Polisen

Protokollbilaga

Åklnr
AM-174292-20

Signerat av

Signeringsdatum

ÖREBRO TINGSRÄTT
Rotel 7
INKOM: 2022-06-02
MÅLNR: B 6266-20
AKTBIL: 977

Enhet
Region Bergslagen, Grova brott 1 PO Örebro

Handläggare (Protokollförare)
Lisa Rehn

Datum

Bitr. handläggare
Gunilla Sköld

Undersökningsledare
Karin Lindell

Polisens diarienummer
5000-K1490612-20

Personer i ärendet

Förtursmål	Beslag	Målsägande vill bli underrättad om tidpunkt för huvudförhandlingen
Nej		Nej
Ersättningsyrkanden		Tolk krävs

Misstänkt (Efternamn och förnamn)	Personnummer
Walczak, Jakub Krzysztof	19850204-0952

Delgiven information om förenklad delgivning vid ett personligt möte genom att skriftlig information överlämnats

Underrättelse om utredning enligt RB 23:18a Underrättelsesätt, misstänkt	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
Ordinär			2022-04-01
Försvarare Richard Backenroth, förordnad 2021-01-12			2021-04-01

Underrättelsesätt, försvarare	Resultat av underrättelse mt	Resultat av underrättelse försv
Ordinär		

Misstänkt (Efternamn och förnamn)	Personnummer
Bogebrink, Tommy Eric Rickard	19741206-6297

Delgiven information om förenklad delgivning vid ett personligt möte genom att skriftlig information överlämnats

Underrättelse om utredning enligt RB 23:18a Underrättelsesätt, misstänkt	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
Ordinär			2022-04-01
Försvarare Melkemichel, Jack, förordnad 2021-06-07			2022-04-01

Underrättelsesätt, försvarare	Resultat av underrättelse mt	Resultat av underrättelse försv
Ordinär		

Misstänkt (Efternamn och förnamn)	Personnummer
Brzozowiec, Pawel	19871101-9698

Delgiven information om förenklad delgivning vid ett personligt möte genom att skriftlig information överlämnats

Underrättelse om utredning enligt RB 23:18a Underrättelsesätt, misstänkt	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
Ordinär			2022-04-01
Försvarare Jerzy Misiowiec, förordnad 2020-12-06			2022-04-01

Underrättelsesätt, försvarare	Resultat av underrättelse mt	Resultat av underrättelse försv
Ordinär		

Misstänkt (Efternamn och förnamn)	Personnummer
Michalski, Jakub	19841204-7675

Delgiven information om förenklad delgivning vid ett personligt möte genom att skriftlig information överlämnats

Underrättelse om utredning enligt RB 23:18a	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd

Underrättelsesätt, misstänkt			
Ordinär			2022-04-01
Försvarare Ulf G V Tollhage, förordnad 2021-02-01			2022-04-01
Underrättelsesätt, försvarare Ordinär	Resultat av underrättelse mt		Resultat av underrättelse försv

Misstänkt (Efternamn och förnamn) Jovanovic, Alexander	Personnummer 19550203-2617
Delgiven information om förenklad delgivning vid ett personligt möte genom att skriftlig information överlämnats	

Underrättelse om utredning enligt RB 23:18a Underrättelsesätt, misstänkt	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
Ordinär			2022-04-01
Försvarare Larsson, Martin, förordnad 2022-02-08			2022-04-01
Underrättelsesätt, försvarare Ordinär	Resultat av underrättelse mt		Resultat av underrättelse försv

Misstänkt (Efternamn och förnamn) Lindberg, Jens Erik Lennart	Personnummer 19620527-0017
Delgiven information om förenklad delgivning vid ett personligt möte genom att skriftlig information överlämnats	

Underrättelse om utredning enligt RB 23:18a Underrättelsesätt, misstänkt	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
Ordinär			2022-04-01
Försvarare Patric Lindblom, förordnad 2020-12-06			2022-04-01
Underrättelsesätt, försvarare Ordinär	Resultat av underrättelse mt		Resultat av underrättelse försv

Misstänkt (Efternamn och förnamn) Glowka, Michal Andrzej	Personnummer 19921019-
Delgiven information om förenklad delgivning vid ett personligt möte genom att skriftlig information överlämnats	

Underrättelse om utredning enligt RB 23:18a Underrättelsesätt, misstänkt	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
Ordinär			2022-04-01
Försvarare Janette Stjernström, förordnad 2020-12-06			2022-04-01
Underrättelsesätt, försvarare Ordinär	Resultat av underrättelse mt		Resultat av underrättelse försv

Notering

Innehållsförteckning

Diarienr	Uppgiftstyp	Sida
	Övergripande information / rättslig info	
5000-K642266-21	PM NOA, övergripande information gällande ANOM	5
	Memorandum United states, översatt till svenska	7
	Beslut om överlämnande av JID information	9
	Beslut om överlämnande av JID information	11
5000-K1490612-20	Beslut om överlämnande av JID information	13
	Beslut om överlämnande av JID information	14
	Teknisk information	
5000-K642266-21	Teknisk information om OP Trojan Shield, FBI (sv)	15
	Rapport, Beskrivning av information i ANOM-data	69
	Hantering av material	
	Rapport, Svensk polis hantering av ANOM-data	101
	PM NFC, Positionsdata i ANOM	125
	PM NFC, beräkning av JID	128
	PM IMEI knutet till JID	129
	Analysresultat NFC - ljudmeddelanden	130
	Utdrag från ANOM	132
	Engelska orginaldokument	
	Memorandum United states	137
	Teknisk information om OP Trojan shield, FBI	139
	Personalia	
	Bilaga skäligen misstänkt, Bogebrink, Tommy Eric Rickard	196
	Personalia, Bogebrink, Tommy Eric Rickard	197
	Bilaga skäligen misstänkt, Brzozowiec, Pawel	198
	Personalia, Brzozowiec, Pawel	199
	Bilaga skäligen misstänkt, Glowka, Michal Andrzej	200
	Personalia, Glowka, Michal Andrzej	201

Bilaga skäligen misstänkt, Jovanovic, Alexander..... 202
Personalia, Jovanovic, Alexander..... 203
Bilaga skäligen misstänkt, Lindberg, Jens Erik Lennart..... 204
Bilaga skäligen misstänkt, Michalski, Jakub..... 205
Personalia, Michalski, Jakub..... 206
Bilaga skäligen misstänkt, Walczak, Jakub Krzysztof..... 207

Polisen

PM

Datum
2021-11-16

Diarienr (åberopas)
5800-128/2020

Polismyndigheten
Nationella operativa avdelningen

Anom

Inledning

Svensk polis har sedan hösten 2020 medverkat i ett internationellt samarbete där vi fått möjlighet att ta del av information från en krypterad kommunikationstjänst.

Den information som lämnats till svensk polis har hanterats av underrättelseenheten vid Nationella operativa avdelningen (NOA).

Bakgrund

Under de senaste åren har krypterade kommunikationstjänster såsom EncroChat och Sky ECC använts som medel för att kommunicera i kriminella syften. Båda har numera upphört att fungera. Parallellt med dessa tjänster har det uppstått en efterfrågan för ett motsvarande system inom den grova organiserade brottsligheten.

FBI har sedan 2019 utvecklat ett krypterat kommunikationssystem som kallas ”ANOM”. Detta har marknadsförts mot kriminella organisationer som ett ”nytt sofistikerat system med enheter som var omöjliga att dekryptera av rättsväsendet”.

I praktiken var dock systemet uppbyggt på ett sätt som gjorde att alla meddelanden som skickades kunde dekrypteras av FBI. En kopia av alla meddelanden har tillgängliggjorts för FBI via en server i tredje land.

Sedan oktober 2019 har FBI och en arbetsgrupp som arbetar med brottsbekämpning på Europol tagit del av meddelanden i systemet. Kommunikationen innehåller meddelanden, fotografier, videoljud, och annan digital information

Varje användare har tilldelats ett unikt ID (Jabber Identification) som inte kan ändras. FBI har en lista över alla JID-nr, både aktiva och inaktiverade.

Kommunikationstjänsten har primärt använts av ledande personer i kriminella organisationer för att samordna narkotikahantering och penningtvätt i ett flertal länder.

Svensk polis har löpande fått ta del av kommunikationen mellan enheter som kunnat knytas till svenska användare i underrättelsesyfte men inte fått använda informationen för brottsutredning.

Avslut

Under våren 2021 startades en operation vid Europol där ett antal länder samverkat runt den tillgängliga informationen från plattformen.

Svensk åklagare har skickat framställningar om rättslig hjälp till USA innehållande begäran om att få använda materialet i svenska förundersökningar.

Informationsinsamlingen avslutades den 7 juni 2021. Detta genom att den tekniska lösningen togs ner och enheterna kan inte längre kommunicera på plattformen.

Letterhead Memorandum (Rev. 02-05-15) **EJ SEKRETESSBELAGT//REL TO USA, SWE**

USA:s Justitiedepartement (United States Department of Justice)

Federal Bureau of Investigation

Spårningsnr: 198842817
Ärendenr:SD-2864529
Prioritet: Rutin
Datum: 9 december 2021

Office of the Legal Attaché
United States Embassy
Dag Hammarskjolds Vag 31
SE-115 89, Stockholm

Nationella Operativa Avdelningen
Sektionen för internationellt polissamarbete
P.O. Box 12256
SE-102 26, Stockholm

TILL: Sambandsman

(U) SÅVIDA INTE ANNAT ANGES ELLER I EN SÄRSKILD SKRIVELSE UTTRYCKLIGEN AV HUVUDKVARTERET FÖR FEDERAL BUREAU OF INVESTIGATION (FBI)MEDGES, ÄR UPPGIFTERNA I DETTA DOKUMENT ENDAST AVSEDDA ATT ANVÄNDAS I UNDERRÄTTELSE- OCH SPÅRSYFTE, OCH ERA MYNDIGHETER FÅR INTE ANVÄNDA DESSA UPPGIFTER I DOMSTOLSFÖRFARANDEN, SPRIDA UPPGIFTERNA TILL MYNDIGHETER, PERSONER ELLER ENHETER I ANDRA STATER, ELLER VIDTA ÖPPNA UTREDNINGSÅTGÄRDER (INBEGRIPET MEN INTE BEGRÄNSAT TILL FORMELLA RÄTTSLIGA PROCESSER ELLER DIREKTKONTAKT MED DE PERSONER/ENHETER ELLER DERAS MEDHJÄLPARE DET HÄNVISAS TILL) PÅ GRUNDVAL AV UPPGIFTERNA I DETTA DOKUMENT.

(U//REL TO USA, SWE) Lämna kompletterande upplysningar rörande den rättsliga myndighet som använts i samband med Trojan Shield-utredningen.

(U//REL TO USA, SWE) Oaktat ovan angivna förbehåll, får uppgifterna i detta dokument användas i underrättelsesyfte, brottsbekämpande åtgärder, eller i rättsliga förfaranden. Uppgifterna som anges i detta dokument får i tillämpliga fall spridas till andra myndigheter i ert land, men de får inte spridas till tredjelands myndigheter eller enheter utan uttryckligt tillstånd från Federal

Bureau of Investigation. Vidare, gör Federal Bureau of Investigation inte gällande att ytterligare stöd ska tillhandahållas (t.ex. kompletterande uppgifter, autentisering, bevismaterial)med kopplingar till dessa uppgifter; ni får, emellertid, använda dessa uppgifter för att begära ytterligare information eller bistånd genom FBI:s juridiske attaché i ert land.

(U//REL TO USA, SWE) Efter diskussioner med USA:s federala åklagarmyndighet (United States Attorney's Office (USAO), beskrev USAO, med följande ordalydelse, den rättsliga grunden för Trojan Shield-operationen:

(U//REL TO USA, SWE) De tekniska metoder som inom Trojan Shields-operationen tillämpades för att driva Anomplattformarna var rättsenliga enligt Amerikas förenta staters lagstiftning och de platser dit plattformarna förlagts. Det stora flertalet av de personer som använde Anom var inte amerikanska medborgare och befann sig inte i USA. Det fjärde tillägget i USA:s konstitution gäller inte för de personerna. Därtill, var det inget av de mellan utländska användare utbytta meddelanden som passerade genom USA:s infrastruktur, dessa omfattades sålunda inte av avlyssningslagen (the Wiretap Act), 18. U.S.C §§ 2510 och följande.

(U//REL TO USA, SWE) Det tredjeland som var värd för Anom-servern ligger i EU och detta tredjeland använde sig av egen rättsprocess för att erhålla ett domstolsbeslut som godkänner att meddelanden som dirigerats till servern kopieras. Tredjelandet lämnade in meddelandena till Federal Bureau of Investigation i enlighet med en begäran om ömsesidig rättslig hjälp (MLAT). Eftersom tredjelandet följde sitt lands lag, kan Förenta staterna förlita sig på de uppgifter som erhållits angående meddelanden mellan utländska användare.

Med vänliga hälsningar

Michael S. Butsch

Polisen

Beslut om överlämnande av JID information

Signerat av

Signerat datum

Enhet	Diarienr
Region Bergslagen, Grova brott 1 PO Örebro	5000-K642266-21

Orginalhandlingens förvaringsplats	Datum	Tid
	2022-03-15	13:21

Involverad personal	Funktion
Andreas Börjesson	Uppgiftslämnare

Berättelse

Överflyttat till Åklagarkammaren i Örebro, nytt AM nummer:

AM-174292-20

ÅKLAGARMYNDIGHETEN
Nationella åklagaravdelningen
Riksenheten mot internationell och organiserad

Kammaråklagare Ewamari Häggkvist

Datum
2021-06-04
Ert datum

Sida 1 (1)
Dnr
AM-72527-21
Er beteckning

BESLUT 2021-06-04

All tillgänglig information rörande följande Jabber Identification (JID) och användarnamn

JID	**Användarnamn**
08075e	Mr.Lansky
b1d66e	Zedd
6e142c	soko

överlämnas till AM-84674-21 (åklagare Thomas Willén).

Ewamari Häggkvist

Postadress
Box 57
101 21 Stockholm

Gatuadress

Telefon
+46 10 562 50 00

Telefax

E-post

Webbadress
www.aklagare.se

Polisen

Beslut om överlämnande av JID information

Signerat av

Signerat datum

Enhet	Diarienr
Region Bergslagen, Grova brott 1 PO Örebro	5000-K642266-21

Orginalhandlingens förvaringsplats	Datum	Tid
	2022-03-15	13:26

Involverad personal	Funktion
Andreas Börjesson	Uppgiftslämnare

Berättelse

Överflyttat till Åklagarkammaren i Örebro, nytt AM nummer:

AM-174292-20

ÅKLAGARMYNDIGHETEN
Nationella åklagaravdelningen
Riksenheten mot internationell och organiserad

Kammaråklagare Ewamari Häggkvist

Datum
2021-06-04
Ert datum

Sida 1 (1)
Dnr
AM-72508-21
Er beteckning

BESLUT 2021-06-04

All tillgänglig information rörande följande Jabber Identification (JID) och användarnamn

JID	**Användarnamn**
56d3f9	Microsoft
7ed648	Microsoft Arcane
aee441	Teamster
225375	Teamsters

överlämnas till AM-84674-21 (åklagare Thomas Willén).

Ewamari Häggkvist

Postadress
Box 57
101 21 Stockholm

Gatuadress

Telefon
+46 10 562 50 00

Telefax

E-post

Webbadress
www.aklagare.se

ÅKLAGARMYNDIGHETEN
Nationella åklagaravdelningen
Riksenheten mot internationell och organiserad

Kammaråklagare Ewamari Häggkvist

Datum
2021-06-22
Ert datum

Dnr
AM-72527-21
Er beteckning

BESLUT 2021-06-22

All tillgänglig information rörande följande Jabber Identification (JID) och användarnamn

JID	**Användarnamn**
3373c4	1919
53b744	szwed blond
83b7cd	seneca
0f9f08	Gunner
2a1cbc	hollow
04522e	Uptown
6afdde	Messi
374fbf	ANOM Sweden
9e96d9	ragnar

överlämnas till AM-174292-20 (åklagare Karin Lindell).

Ewamari Häggkvist

Postadress
Box 57
101 21 Stockholm

Gatuadress

Telefon
+46 10 562 50 00

Telefax

E-post

Webbadress
www.aklagare.se

ÅKLAGARMYNDIGHETEN
Nationella åklagaravdelningen
Riksenheten mot internationell och organiserad

Kammaråklagare Ewamari Häggkvist

Datum
2021-10-13
Ert datum

Dnr
AM-72527-21
Er beteckning

BESLUT 2021-10-13

All tillgänglig information rörande följande Jabber Identification (JID) och användarnamn

JID	**Användarnamn**
c94b76	

överlämnas till AM-174292-20 (åklagare Karin Lindell)

Ewamari Häggkvist

Postadress
Box 57
101 21 Stockholm

Gatuadress

Telefon
+46 10 562 50 00

Telefax

E-post

Webbadress
www.aklagare.se

Teknisk information om Operation Trojan Shield

Senast uppdaterad: 31 augusti 2021

INNEHÅLLSFÖRTECKNING

1. ÖVERSIKT ÖVER SERVRAR OCH NÄTVERK 5

1.1 XMPP-server 5

1.2 Server i tredje land 5

1.3 Google-servrar 5

1.3.1 Överföring 5

1.3.2 Proxy 6

1.4 AWS GovCloud 6

1.4.1 Säkerhet 6

1.4.2 Frontend 6

1.4.3 Ingestion-1 (I1) 6

1.5 Aktivitet i meddelandenätverket 6

2. SKAPANDE AV NYA DATAPAKET 7

2.1 Kryptering av data 8

2.2 Hur databasens skillnadsdump skapades 8

2.3 Hur listan med bilagor fastställs från skillnadsdumpen 8

2.4 Hur bilagor kopierades från fillagringen 9

2.5 Skapa det krypterade paketet 9

3. ÖVERFÖRING FRÅN SERVERN I DET TREDJE LANDET TILL ÖVERFÖRINGSSERVERN 9

3.1 Program som överför data till överföringsservern 9

4.ÖVERFÖRING FRÅN ÖVERFÖRINGSSERVERN TILL AWS GOVCLOUD 10

4.1 Automatisering av program för att överföra data 10

5. BEARBETNING AV KRYPTERADE PAKET 10

5.1 Avkryptering av GPG-paket 10

5.2 Extrahering av den nya MySQL-databasdumpen och bilagor från arkivet 10

5.3 Inmatning av databasdumpen till en tillfällig databas 10

6. AVKRYPTERINGSPROCESSEN 10

6.1 Avkryptering av krypterade fält i databasen 10
6.1.1 Uppdatering av sökvägar för bilagor så att de är korrekta 11

6.2 Avkryptering av alla filer i bilagor 11

7. BEARBETNING AV LJUDFILER 11

7.1 Konvertera ljudfiler till användbart format 11

7.2 Ändring av tonhöjd i ljudfiler om nödvändigt 11

8. DATABASÖVERSIKT 11

8.1 Ärenden/syndikat 11
8.1.1 Grupper av enhetsanvändare (JID) 12

8.2 Användare av granskningsplattformen 12
8.2.1 Allmänna användare 12
8.2.3 Super users 12
8.2.4 Administratörer 12

8.3 Förteckningen 12

8.4 Grupper 13
8.4.1 Avsaknad av gruppinformation 13

8.5 Produkter 13
8.5.1 Produkter i detalj 13

8.6 Meddelanden 15
8.6.1 Fel i meddelandens tidszon 16

8.7 Relationer 16
8.7.1 Relation produkt till meddelande 17
8.7.2 Relation mellan användare och åtkomst till ärenden 17
8.7.3 Relationen mellan JID och ärenden 17
8.7.4 Relationen mellan JID och grupper 17

9. INMATNINGSPROCESS 18

9.1 Mata in ny information i förteckningen 18

9.2 Infoga nya grupper 18
9.2.1 Infoga ny gruppinformation 19

9.2.2 Infoga uppdateringar om medlemskap i grupper 19

9.3 Inmatning av meddelanden *19*
9.3.1 Initialisering 19
9.3.2 Infoga meddelanden 19
9.3.4 Tilldela meddelanden till produkter 20

9.4 Inmatning av produkter *21*
9.4.1 Skapa produkter per ärende 21

9.5 Export efter inmatning *22*

10. WEBBAPPLIKATION/GRANSKNINGSPLATTFORM 22

10.1 Kontroll av användaråtkomst i Hola iBot *22*
10.1.1 Åtkomstkontroll för LEEP (Law Enforcement Enterprise Portal) 22
10.1.2 Åtkomstkontroll i Hola iBot 22

10.2 Ärenden i Hola iBot *25*
10.2.1 Ärendets hemsida 25

10.3 Produktsidan *26*

10.4 Produktsidan *27*
10.4.1 Grupp-ID-visning 29
10.4.2 Meddelanden med bilagor (PTT, bild, video, anteckning) i Hola iBot 29
10.5 Översättningar 31

10.6 Förteckningssidan *33*

10.7 JID-profil *34*
10.7.1 Information om enhetsanvändaren (JID) 35

10.8 Andra sidor *38*
10.8.1 Sökning 38
10.8.2 Sök i anteckningar 39
10.8.3 Alla bilder 39
10.8.4 Blockerade 40

11. MLAT-EXPORT 40

11.1 Hämtning av alla bifogade filer *40*

11.2 Hämtning av slutlig MySQL-databasdump *40*

11.3 Skapa MLAT-exporter *40*

BILAGA A 41

A.1 Kryptering med offentlig nyckel *41*

A.2 Hash *41*

A.3 ANØM-PLATTFORMEN *42*
A.3.1 End-to-end-kryptering 42

A.4 Portalen *43*

A.5 Enheter *44*

A.5 Nätverksanslutning till plattformen *45*

A.6 MDM-komponenten *45*

A.7 ANØM-applikationen *46*

A.8 Data spelas in från plattformen *49*

A.8.2 Metadata för meddelanden 50

A.9 Autentisering och integritet *51*

1. ÖVERSIKT ÖVER SERVRAR OCH NÄTVERK

För Operation Trojan Shield (OTS) krävdes servrar på flera nivåer för dataöverföring, lagring och granskning.

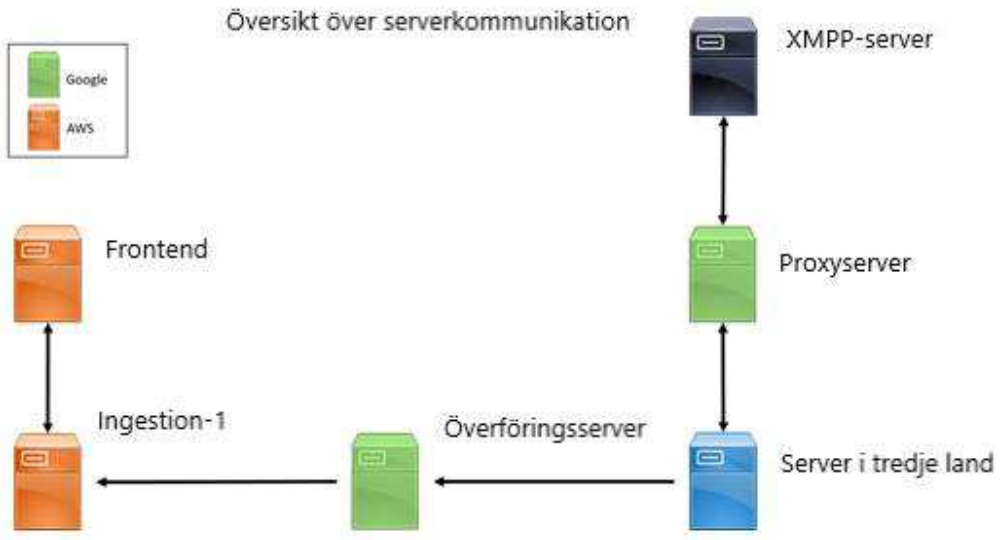


Diagram 1.A

1.1 XMPP-server

XMPP är ett öppet standardprotokoll för snabbmeddelanden som möjliggör chattar mellan flera parter. Det har stöd för multimedia som röst, bilder och video. Vem som helst kan köra en egen XMPP-server och nätverk och bygga vidare på det befintliga ramverket. Appen ANØM innehöll en funktion som innebar att när ett meddelande skickades så skickade appen, via en XMPP-server, automatiskt en dold kopia av meddelandet till ett ghostanvändar-ID, ”bot”. Den här processen var inte synlig för den användare som skickade meddelandet, och den användaren visste inte heller om att processen ägde rum.

1.2 Server i tredje land

En server anskaffades av brottsbekämpande myndigheter i ett tredje land i oktober 2019 för att samla in de dolda kopiorna av meddelanden som skickades till ghostanvändaren ”bot” i enlighet med beskrivning i bilaga A.8 - 59. Servern ägdes, drevs och underhölls av det tredje landet fram tills dess att operationen avslutades.

1.3 Google-servrar

Ett hemligt Google Cloud-konto registrerades för att skapa Google Compute Engines, en tjänst som Google Cloud erbjuder för att skapa och köra virtuella datorer i Google Cloud. De behövdes för att överföra data och tillhandahålla en proxyserver för servern i det tredje landet.

1.3.1 Överföring

Överföringsservern var en konfigurerad Google Compute Engine. Dess enda syfte var att överföra data från servern i det tredje landet till servern Ingestion-1 (I1) i AWS GovCloud.

1.3.2 Proxy

Proxyservern sattes upp som en Google Compute Engine. Servern fungerade som reläserver för alla meddelanden som skickades mellan ANØM-nätverket (XMPP-servern) och uppsamlingsservern i det tredje landet. På så sätt fick man privat kommunikation till ANØM-nätverket från tredjepartsservern.

1.4 AWS GovCloud

Inom AWS GovCloud West konfigurerades, drevs och underhölls EC2-servrar (Elastic Compute Cloud) för OTS.

1.4.1 Säkerhet

AWS-miljön skannas varje månad efter sårbarheter och andra felkonfigurationer som kan utgöra hot. Alla EC2-servrar i AWS GovCloud kör en förstärkt version av operativsystemet CentOS. Båda EC2-servrarna skannas efter sårbarheter och patchas. Skanningen efter sårbarheter och patchningen genomförs enligt de riktlinjer (Security Technical Implementation Guides, STIG) som ges ut av Defense Information Systems Agency (DISA).

1.4.2 Frontend

Frontend-servern fungerade som webbserver för granskningsapplikationen Hola iBot. Mer information om granskningsapplikationen Hola iBot finns i avsnitt 10.

1.4.3 Ingestion-1 (I1)

Ingestion-1 (I1) var den mottagare dit nya datapaket från servern i det tredje landet skickades för behandling och granskning. Den fungerar också som databas och filserver för visning och granskning av data.

1.5 Aktivitet i meddelandenätverket

Som nämns i bilaga A.8 - 59 togs de data som samlades in från plattformen emot som dolda kopior. I diagram 1.B visas en översikt över dataflödet i nätverket för inhämtning av dessa meddelanden.

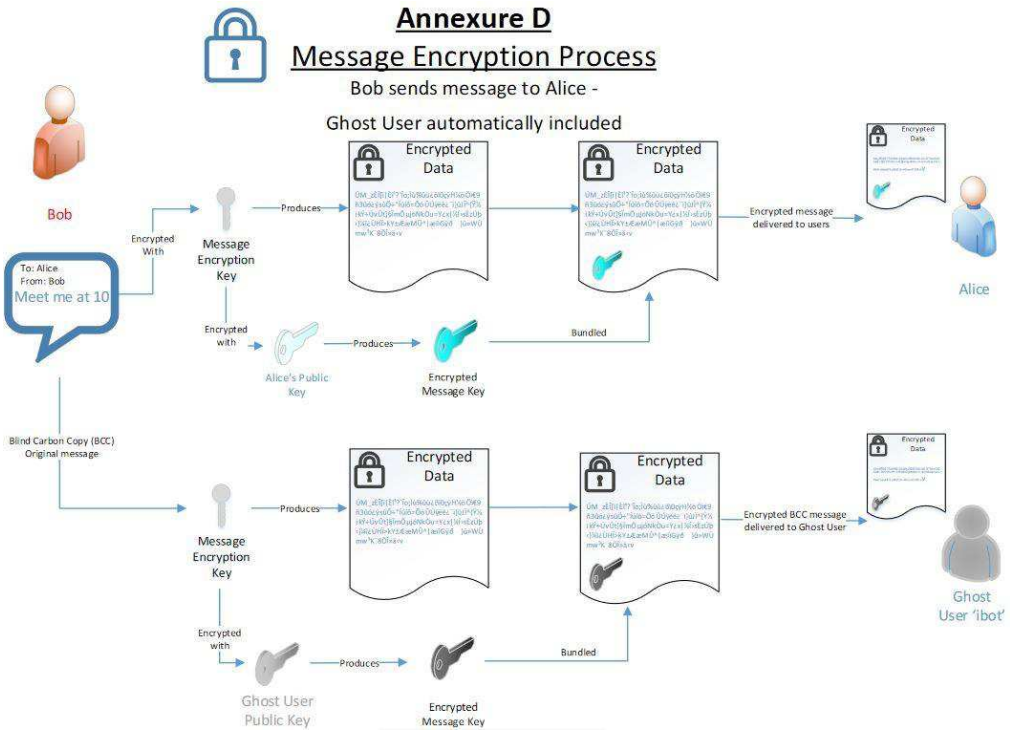


Diagram 1.B

2. SKAPANDE AV NYA DATAPAKET

Tack vare ett avtal om ömsesidig rättshjälp kunde data överföras från det tredje landet varje måndag, onsdag och fredag. En process som gjorde att enbart nya data skickades togs fram och överlämnades till det tredje landet. Följande är en lista över data som bearbetades till nya datapaket:

- MySQL-databasposter:
  - Meddelanden
    - Ett unikt meddelande-ID
      - UUID som unikt identifierar ett enskilt meddelande
    - Avsändare
      - Den avsändande användarens användar-ID (JID)
    - Mottagare
      - Den mottagande enhetens användar-ID (JID) eller grupp-ID (GID)
    - Platsinformation
      - Latitud och longitud bifogades varje meddelande (om enheten tillhandahöll sådan information).
      - Om platsinformation angavs så krypterades den.
    - Mobile Country Code (MCC)
      - Den MCC som meddelandet skickades från
    - Tid
      - Tiden då meddelandet skickades enligt avsnitt 8.6.1
    - Tonhöjdsjustering för ljud
      - Om meddelandet var ett ptt-meddelande (Push To Talk) bifogades ett

värde till bilagan som kunde användas för att ta bort den tonhöjdsjustering som utfördes i appen enligt bilaga A.7.1.4 – 57)

- Typ
  - Varje meddelande kan vara någon av följande typer:
    - text, vidarebefordrat, kontakt
      - Betyder att fältet ”innehåll” innehåller krypterad text
    - ptt, video, bild, anteckning
      - Anger att fältet ”innehåll” innehåller sökvägen till den fil som avsändaren skickade, med filnamnet [unikt meddelande-ID].[bilagans filnamnstillägg]
- Innehåll
  - Om meddelandetypen var ”text”, ”kontakt” eller ”vidarebefordrat” var innehållet krypterat
  - Om meddelandetypen var ”ptt”, ”video”, ”bild” eller ”anteckning” hade fältet sökvägen till den skickade bilagan i klartext

- Förteckning
  - Enhetsanvändar-ID
    - En unik identifierare för en enhetsanvändare
  - Smeknamn
    - Krypterat smeknamn som angavs av användaren
- Gruppinformation
  - Grupp-ID (GID)
    - En unik identifierare för en grupp enheter
  - Gruppnamn
    - Krypterat namn på gruppen som angavs av användaren

- Filer
  - Ljud-, bild-, video- och anteckningsfiler namngavs enligt följande: [Unikt meddelande-ID].[bilagans filnamnstillägg]

2.1 Kryptering av data

Mottagna data (bilagor, innehåll/textmeddelanden, platsinformation, smeknamn och gruppnamn) krypterades med end-to-end-kryptering enligt XMPP-protokollet (Extensible Messaging and Presence Protocol). På servern i det tredje landet avkrypterades data i tillfällig lagring (RAM) vid mottagandet, och sedan krypterades samma data igen med en kombination av asymmetrisk RSA-kryptering och symmetrisk AES-kryptering innan de sparades på disk. Inga data i klartext sparades på servern i det tredje landet. Den privata nyckeln för avkryptering (vad avser RSA) lagrades på I1-servern i AWS GovCloud.

2.2 Hur databasens skillnadsdump skapades

Processen för att erhålla nya data gick ut på att hitta enbart nya data i MySQL-databasen (se ovan för listan över poster som hämtades från databasen). Skillnaden mellan den senaste fullständiga databasdumpen och den nya/aktuella fullständiga databasdumpen kallades internt för ”skillnadsdumpen” (”difference-dump”). Processen inleddes genom att en ny MySQL-databasdump skapades. Databasdumpen från den förra överföringen och den nya databasdumpen användes som indata till ett program. Programmet beräknade skillnaden mellan den förra databasdumpen och den nuvarande och genererade en MySQL-dump med enbart nya data. Se diagram 2.A för en visuell beskrivning av processen.

2.3 Hur listan med bilagor fastställs från skillnadsdumpen

I processen användes skillnadsdumpen för att samla in de nya bilagorna genom att kontrollera fältet ”innehåll” i alla meddelanden som hade sökvägar. Se avsnitt 2 för mer information om var sökvägar lagras som enheter. Som nämndes ovan placerades filnamnen i fältet ”innehåll” om typen inte var ”text”, ”kontakt” eller ”vidarebefordrat’.

2.4 Hur bilagor kopierades från fillagringen

Bilagor lagrades krypterade direkt på servern och programmet som hämtade de nya bilagorna använde sökvägen från fältet ”innehåll” enligt beskrivning i avsnitt 2.3 och kopierade bilagorna till en tillfällig lagringsplats för att skapa paketen.

2.5 Skapa det krypterade paketet

För att paketera MySQL-dumpen med nya data och bilagor komprimerades filerna i en arkivfil med filnamnsillägget ”.tar.gz”. Arkivfilen krypterades med asymmetrisk GnuPG-kryptering (GPG), vilket gjorde att filnamnstillägget ”.gpg” lades till i slutet på arkivets namn. Efter att det krypterade paketet hade skapats hashades det med hashalgoritmen MD5. En hashfunktion är en matematisk process där indata, ”meddelandet”, bearbetas till ett ”sammandrag av meddelandet” eller ett hashvärde med fast längd. Det anges ofta som hexadecimala tecken med siffrorna 0 till 9 och bokstäverna A till F. Hashfunktioner används ofta för dataverifiering genom att identifiera om data har förändrats, eftersom det är mycket osannolikt att två olika ”indatameddelanden” resulterar i samma hashvärde. MD5-hashvärdet sparades till en fil för överföring. I diagram 2.A ges en översikt över paketeringsprocessen.

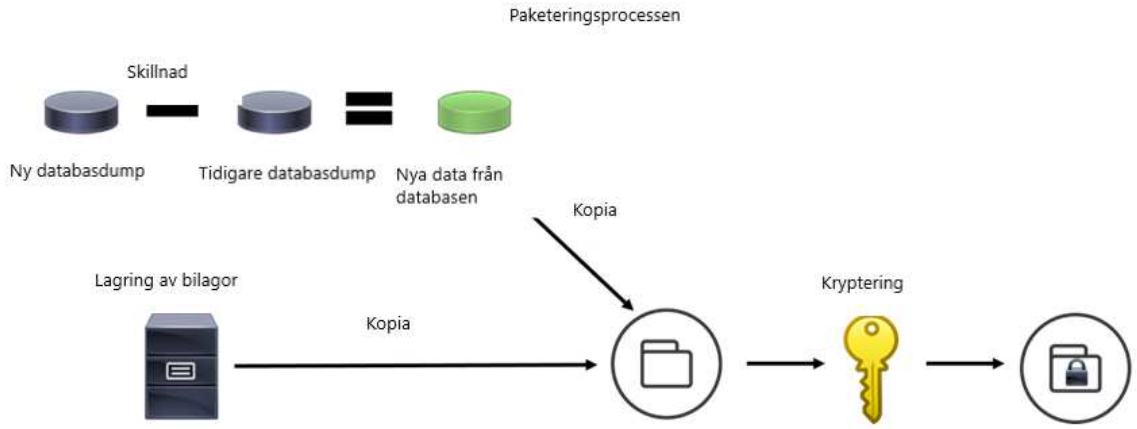


Diagram 2.A

3. ÖVERFÖRING FRÅN SERVERN I DET TREDJE LANDET TILL ÖVERFÖRINGSSERVERN

Det tredje landet körde manuellt ett program som genomförde den behandling av nya data som beskrivs i avsnitt 2.

3.1 Program som överför data till överföringsservern

Varje måndag, onsdag och fredag körde det tredje landet ett program som förpackade och skickade nya data. Programmet skickade MD5-hashvärdet följt av det krypterade paketet med nya data till den hemliga Google Compute Engine-överföringsserver som beskrivs i avsnitt 1.3.1.

4. ÖVERFÖRING FRÅN ÖVERFÖRINGSSERVERN TILL AWS GOVCLOUD

Överföringsservern vidarebefordrade automatiskt mottagna data till I1-servern i AWS GovCloud efter att ha kontrollerat integriteten (genom verifiering av hashvärdet).

4.1 Automatisering av program för att överföra data

När överföringsservern tog emot nya krypterade paket letade den efter filer som slutade med ”.gpg” i den inboxkatalog dit data överfördes. Det indikerade att ett nytt datapaket var klart att överföras till I1 i AWS GovCloud. Programmet beräknade sedan MD5-hashvärdet för .gpg-filen och jämförde det med det MD5-hashvärde som hade överförts av servern i det tredje landet. Om hashvärdena stämde överens betydde det att överföringen hade lyckats och det krypterade paketet vidarebefordrades till I1 i AWS GovCloud.

5. BEARBETNING AV KRYPTERADE PAKET

Varje krypterat paket överfördes till en tilldelad plats på I1 i AWS GovCloud. Genom en automatiserad uppgift kontrollerades om det fanns nya data på platsen. Om nya data hittades på platsen påbörjades inmatningsprocessen på servern.

5.1 Avkryptering av GPG-paket

Först avkrypterades det krypterade paketet med MySQL-data (databasen) samt bilagorna så att dataarkivet (databasen och bilagor till meddelanden) skulle bli tillgängliga. Som nämndes ovan användes asymmetrisk GPG-kryptering för att skydda arkivet med data, så en privat nyckel som enbart var tillgänglig på I1-servern användes för att avkryptera paketet.

5.2 Extrahering av den nya MySQL-databasdumpen och bilagor från arkivet

Efter avkrypteringen extraherades arkivet till filsystemet, vilket gjorde MySQL-datan (databasen) och bilagorna tillgängliga för vidare behandling.

5.3 Inmatning av databasdumpen till en tillfällig databas

I1-servern använde två databaser för behandling av inkommande data. En av dessa databaser, iBot_enc, var en tillfällig lagringsplats för nya data som hade tagits emot från servern i det tredje landet. Här sparades nya MySQL-data tillfälligt för behandling. Nya data behövde avkrypteras, normaliseras och bearbetas in i den andra databasen så att frontend-webbapplikationen Hola iBot kunde visa dessa data.

6. AVKRYPTERINGSPROCESSEN

För att avkryptera och normalisera inkommande data matades databasdumpen in i en databas på I1-servern enligt beskrivningen i avsnitt 5.3.

6.1 Avkryptering av krypterade fält i databasen

Enligt beskrivning i avsnitt 2 krypterades följande fält i databasdumpen:

- Meddelanden
  - Innehåll (om typen är ”text”, ”kontakt” eller ”vidarebefordrat”)
  - Platsinformation (om det finns sådan)
- Förteckning
  - Enhetsanvändarens visningsnamn (se avsnitt 8.3)
    - Kallas också smeknamn, användarnamn, alias
- Gruppinformation
  - Gruppnamn

Med avkrypteringsprocessen avkrypterades fältet ”innehåll” för alla meddelanden utan bilagor direkt

på plats (dvs. det krypterade innehållet ersattes med avkrypterat innehåll) med hjälp av den privata nyckeln för den krypteringsprocess som användes av servern i det tredje landet enligt beskrivning i avsnitt 2.1.

6.1.1 Uppdatering av sökvägar för bilagor så att de är korrekta

När krypterade bilagefiler kom till servern i det tredje landet sparades hela filens sökväg i klartext i fältet ”innehåll” i databasen, om filen var av typen bilaga. Sökvägen avsåg servern i det tredje landet men det här databasfältet användes på samma sätt på I1-servern för att tillhandahålla bilagor för granskning på frontend-webbservern. För att göra bilagorna tillgängliga uppdaterades sökvägen i fältet ”innehåll” till den sökväg där de skulle placeras på I1-servern efter avkryptering och konvertering (om det behövdes).

6.2 Avkryptering av alla filer i bilagor

Efter att sökvägarna i fältet ”innehåll” hade uppdaterats korrekt avkrypterades alla nya filer i bilagor med den privata nyckeln för krypteringsprocessen som användes av servern i det tredje landet enligt beskrivningen i avsnitt 2.1. Genom avkrypteringsprocessen för bilagorna placerades de avkrypterade filerna på rätt plats så att de blev tillgängliga för frontend-webbservern och kunde visas i webbapplikationen Hola iBot.

7. BEARBETNING AV LJUDFILER

Ljudfilerna som kom från servern i det tredje landet behövde bearbetas ytterligare innan de kunde göras tillgängliga i webbapplikationen Hola iBot.

7.1 Konvertera ljudfiler till användbart format

Om en bilaga var en ljudfil (vilket indikerar ett push to talk-meddelande) konverterades ljudfilen, under avkrypteringsprocessen, från filformatet Ogg Opus (OPUS) till filformatet Waveform Audio (WAV). Detta gjordes eftersom webbläsare saknar stöd för OPUS-filer, medan WAV-filer kan spelas upp internt i de flesta moderna webbläsare.

7.2 Ändring av tonhöjd i ljudfiler om nödvändigt

Som nämndes i bilaga A.7.1.4 – 57 fanns det i ANØM-applikationen en möjlighet att justera tonhöjden för det inspelade meddelandet. Användaren hade möjlighet att höja (”helium”) eller sänka (”jellyfish”) tonhöjden i PTT-meddelanden. Tillsammans med varje tonhöjdsjusterat PTT-meddelande skickades också ett värde som representerade den justerade tonhöjden. Värdet användes för att ändra tillbaka tonhöjden, vilket gav en justerad ljudfil. Den tonhöjdsjusterade ljudfilen är tillgänglig för användare av granskningsplattformen Hola iBot, men originalljudfilen sparas också. För närvarande är det dock inte möjligt att återskapa originalljudfilen. Det har inte tagits fram en process för att återskapa originalljudfilen.

8. DATABASÖVERSIKT

Resten av inmatningsprocessen, efter den process som beskrivs i avsnitt 6 och 7, går ut på att omorganisera data i en sekundär databas (iBot_dec). Databasen iBot_dec är den databas som används i frontend-webbapplikationen Hola iBot. I följande avsnitt beskrivs layouten för de viktigaste iBot_dec-tabellerna, liksom interna relationer. Alla tabeller i iBot-dec beskrivs inte i det här avsnittet, men de beskrivs i senare avsnitt om det behövs.

8.1 Ärenden/syndikat

Den centrala komponenten för organisering i databasen iBot_dec är ”ärenden” eller ”syndikat”. I databasen har ärenden ett ärende-ID och ett namn. Ärende-ID är en unik identifierare för ärendet, och namnet är en möjlighet för administratörer att ge ärendet ett namn som är lätt att komma ihåg.

Ärenden har i huvudsak fått namn efter slumpmässigt utvalda gudar och gudinnor i romersk och grekisk mytologi. I databasen finns en tabell med namnet ”ärenden”, där beskrivande information lagras om ärenden.

8.1.1 Grupper av enhetsanvändare (JID)

Ärenden är ett sätt att organisera enhetsanvändare (JID) som ofta pratar med varandra i grupper. De är också ett sätt för användare av granskningsplattformen att skapa en organisationsstruktur.

8.2 Användare av granskningsplattformen

FBI-medarbetare och andra personer från brottsbekämpande myndigheter som övervakar data på plattformen får först ett CJIS LEEP-konto (Law Enforcement Enterprise Portal), men de behöver sedan ytterligare åtkomstbehörigheter för att komma åt granskningsplattformen. För att få dessa behörigheter behöver ett konto skapas i databasen iBot_dec.

Det finns tre huvudsakliga typer av användare i databasen:

- Allmänna användare
- Super users
- Administratörer

I databasen finns en tabell med namnet ”användare”, där beskrivande information lagras om granskningsplattformens användare.

8.2.1 Allmänna användare

Användarna är utredande personal och stödpersonal från FBI och andra brottsbekämpande myndigheter som arbetar med utredningar i Operation Trojan Shield. De har tillgång till produktsidorna för den specifika utredning som de har getts åtkomst till. Produkter i databasen beskrivs närmare i avsnitt 8.5. Här kan de granska, markera och skapa anteckningar om produkter. Allmänna användare kan också komma åt och använda funktionerna i förteckningen. Se avsnitt 8.3 för mer information om förteckningen.

8.2.3 Super users

Super Users är chefer på FBI som ansvarar för utredningar i Operation Trojan Shield. De har tillgång till kommunikationsdata relaterade till deras utredningar på samma sätt som allmänna användare. Super users kan också skapa allmänna användare och ge dem åtkomst till utredningar som de leder.

8.2.4 Administratörer

Administratörer är FBI-personal som är ansvariga för drift, underhåll och övervakning av granskningsplattformen Hola iBot. De granskar behörighetsförfrågningar för att kontrollera att användare har tillräckligt goda skäl för att få åtkomst till Hola iBot och ger användare av granskningsplattformen åtkomst till systemet. Administratörer kan också ge åtkomst till utredningar åt allmänna användare och super users. De har också tillgång till system för att skapa nya ärenden/syndikat.

8.3 Förteckningen

I förteckningen finns all information om enhetsanvändare (JID). Det är en unik lista över alla användare av ANØM-plattformen för vilka data har tagits emot. I databasen finns iBot_dec finns en tabell med namnet ”förteckning”, där beskrivande information lagras om enhetsanvändarna:

- Unik identifierare för enhetsanvändare (JID)
    - Varje användare i ANØM identifieras med en unik identifierare (användar-ID), som tekniskt kallas för en Jabber Identifier (JID). Från början hade användar-ID formen av 6 alfanumeriska tecken (till exempel ”aab2c3”) som genererades automatiskt från

enhetens IMEI-nummer (International Mobile Equipment Identity number) (bilaga A.3 – 19 och A.7.1.1 – 46).

- Enhetsanvändarens visningsnamn
  - Användaren av enheten kunde ange ett ”visningsnamn” (som också kallas smeknamn, användarnamn eller alias), som kunde ändras när användaren ville. Det förändrade inte deras användar-ID (JID) på plattformen (bilaga A.7.1.2 – 47)
- Verkligt namn
  - Om en enhetsanvändares verkliga identitet kunde fastställas genom granskning av innehållet finns det ett utrymme där den kan anges.
- Biografi
  - I granskningsplattformen går det att ange ytterligare information som har samlats in om en enhetsanvändare som kan vara bra att ha med i deras JID-profil. JID-profilen diskuteras närmare i avsnitt 10.7.
- Plats
  - Om man under granskning av en enhetsanvändares eller andra användares innehåll upptäcker en förmodad plats för en enhetsanvändare går det att ange den informationen i granskningsplattformen.

8.4 Grupper

Enligt beskrivningen i bilaga A.7.1.4 – 51 kunde en enhetsanvändare också skicka end-to-end-krypterade meddelanden till en grupp av ANØM-användare, och varje användare i den gruppen kunde se de andra medlemmarna i gruppen. Grupper fick också namn som enhetsanvändarna kunde definiera. Mer information om grupper finns i bilagan, avsnitt A.7.1.4 – 51.

Databasen iBot_dec hade en tabell med namnet ”grupper”, som rymmer följande information:

- Grupp-ID (GID)
  - GID är en sträng alfanumeriska tecken som unikt identifierar en grupp.
  - GID:n tilldelas på samma sätt som JID:n, på XMPP-servern.
- Namn
  - Det användardefinierade namnet på en grupp.
- Infogad
  - Datumet för det nya datapaket som först innehöll information om gruppen. Mer

information om hur enhetsanvändare är kopplade till grupper finns i avsnitt 8.7.4.

8.4.1 Avsaknad av gruppinformation

Gruppinformation samlades inte alltid in under den period då datapaket togs emot från det tredje landet. Informationen om grupper i databasen är därför inte fullständig.

8.5 Produkter

Produkter är synonymt med konversationer som finns i varje nytt datapaket. En produkt representerar en konversation mellan två eller flera enhetsanvändare i ett ärende under tidsperioden mellan det föregående datapaketet och datapaketet med den nuvarande produkten.

8.5.1 Produkter i detalj

En ny unik uppsättning produkter skapas med varje nytt datapaket som tas emot från det tredje landet för varje ärende. Mer information om hur produkter skapas finns i avsnitt 9.

I databasen iBot_dec finns en tabell som heter ”produkter”. I den tabellen finns följande information:

- Ärende-ID
  - Varje produkt som skapas har en en-till-en-relation med ett ärende.
  - Den unika identifieraren för det ärende/syndikat som produkten tillhör lagras i produkttabellen i form av ett positivt heltal.
- Produkt-ID (PID)
  - En unik identifierare för produkten i form av ett positivt heltal.
- Produktanteckning
  - Användare av granskningsplattformen kan lägga till anteckningar i produkter.
  - Anteckningarna läggs till i det här fältet.
- Skapad datum
  - Nya datapaket tas emot från det tredje landet varje måndag, onsdag och fredag.
  - Eftersom nya uppsättningar produkter skapas varje gång ett nytt datapaket tas emot sparas också datumet då produkten genererades, vilket är detsamma som datumet då det nya datapaketet skapades.
- MCC-sträng
  - En unik lista över de olika MCC-koder (Mobile Country Codes) som används av enheterna i produkten.
- JID-sträng
  - En lista i alfabetsordning med unika identifierare för enhetsanvändare (JID) som skickade eller tog emot meddelanden i produkten.
- Antal meddelanden
  - Antalet meddelanden i produkten.
- JID 1
  - Den första avsändaren av ett meddelande i produkten.
- JID 2
  - Den andra deltagaren eller JID i produkten om produkten inte är en grupprodukt.
- Grupp-ID (GID)
  - Gruppens unika identifierare om produkten är en grupprodukt
- Är dubblett
  - Det här värdet är antingen 1 eller 0 (1 = dubblett, 0 = inte dubblett).
  - Som nämnts ovan har varje produkt en en-till-en-relation med ett ärende.
    - Om en eller flera JID i en produkt inte alla tillhör samma ärende eller syndikat (t.ex. JID 123456 tillhör ärende Alfa och JID 789100 tillhör ärende Bravo) skapas en produkt för varje ärende.
    - Produktens meddelanden och deltagare kommer att vara samma, men det kommer att skapas en produkt för varje ärende som en JID i produkten hör till.
    - Se avsnitt 8.7.3 för mer information om relationer mellan JID och ärenden i databasen och avsnitt 9 för mer information om inmatningsprocessen.
- Känd grupp
  - Det här värdet är antingen 1 eller 0 (1 = databasen har information om gruppen, 0 = databasen har inte information om gruppen).
  - Som nämndes ovan i avsnitt 8.4.1 samlades gruppinformation inte alltid in på servern i

det tredje landet.

- Om gruppinformation saknas kan inte granskningsplattformen Hola iBot visa gruppens identifierare och gruppnamnet, och eventuellt inte **alla** gruppmedlemmar.
- Men produkterna bildas direkt från meddelandena och medlemmarna i konversationen/gruppen fastställs av avsändare och mottagare av meddelanden.
- Även om databasen inte innehåller gruppinformation kommer JID-strängen alltså ändå att spegla medlemmarna i konversationen/produkten.

8.6 Meddelanden

MySQL-skillnadsdumpen i det nya datapaketet som togs emot från det tredje landet innehöll en enda tabell för meddelanden. Mer detaljerad information om inmatningsprocessen för meddelanden finns i avsnitt 9. Det finns fyra tabeller i databasen iBot_dec med meddelandeinnhåll och associerade metadata:

- ”textmeddelande”
  - I den här tabellen finns avkrypterade textmeddelanden, kontaktmeddelanden, vidarebefordrade meddelanden och textkomponenter i anteckningsmeddelanden.
  - I tabellen finns även fältet ”från anteckning”, vilket anger att texten i fältet ”innehåll” kommer från ett meddelande av typen anteckning.
    - Se avsnitt 9.3.2.2.2 för mer information om hur meddelanden av typen anteckning matas in i databasen.
- ”ptt-meddelande”
  - I den här tabellen finns sökvägar (på I1-servern) för avkrypterade, konverterade och tonhöjdsjusterade (vid behov) push-to-talk-meddelanden.
- ”videomeddelande”
  - I den här tabellen finns sökvägar (på I1-servern) för avkrypterade videomeddelanden.
- ”bildmeddelande”
  - I den här tabellen finns sökvägar (på I1-servern) för avkrypterade bildmeddelanden och bildkomponenter i anteckningsmeddelanden.
  - I tabellen finns även fältet ”från anteckning”, vilket anger att bilden som finns i sökvägen i fältet ”innehåll” kommer från ett meddelande av typen anteckning.
    - Se avsnitt 9.3.2.2.2 för mer information om hur meddelanden av typen anteckning matas in i databasen.

I alla fyra tabeller finns följande metadatafält:

- Meddelande-ID (MID)
  - En unik identifierare för ett meddelande i form av ett positivt heltal.
  - MID delas av alla fyra tabellerna.
    - Om t.ex. MID 5 visas i ptt-meddelande så visas inte samma MID någon annanstans.
- Ursprungligt meddelande-ID
  - En annan unik identifierare för ett meddelande som kommer från de nya datapaketen.
  - En unik sträng av tecken som representeras som ett UUID (Universally Unique Identifier).
  - Detta meddelande-ID sparades med varje meddelande som servern i det tredje landet tog emot som en dold kopia.
  - Detta meddelande-ID beskrivs närmare i bilaga A.8.2 – 64.a.

    - MID skapades i databasen iBot_dec för att skapa en enhetlig standard för primära nycklar i databasen.
        - T.ex. PID:n som positiva heltal, ärende-ID:n som positiva heltal osv.
- Datum för infogande
    - Datum för infogande är det datum då datapaketet som innehöll meddelandet matades in i databasen.
- MCC (Mobile Country Code)
    - MCC för den avsändande enheten vid tidpunkten då meddelandet skickades.
- Är grupp
    - Det här värdet är antingen 1 eller 0 (1 = meddelandet skickades till en grupp, 0 = meddelandet skickades inte till en grupp).
    - Om meddelandet är ett gruppmeddelande (värdet 1) innehåller fältet mottagare det grupp-ID (GID) som meddelandet skickades till.
- Avsändare
    - Den avsändande enhetens användar-ID (JID)
- Tid
    - Tiden då meddelandet skickades enligt avsnitt 8.6.1.
    - Ett meddelande som skickades den 6 juni 2021 kl. 22.00 Pacific Time skulle i databasen ha tiden och datumet angivet som kl. 05.00 den 7 juni 2021 UTC.
- Platsinformation
    - Om platsinformation (latitud och longitud) mottogs med ett meddelande lagrades latitud och longitud med varje meddelande i var och en av de fyra tabellerna.

8.6.1 Fel i meddelandens tidszon

På grund av en felkonfiguration på servern i det tredje landet varierade meddelandenas tidszoner under inhämtningsperioden. Följande tidsramar visar den korrekta konverteringen av tidsstämplar för meddelanden:

- Tidsram 1
    - 1 oktober 2019 – 27 oktober 2019: UTC – 3
- Tidsram 2
    - 27 oktober 2019 – 29 mars 2020: UTC – 2
- Tidsram 3
    - 29 mars 2020 – 18 september 2020: UTC – 3
- Tidsram 4
    - 18 september 2020 – operationens slut: UTC

8.7 Relationer

I följande avsnitt definieras de relationer i iBot_dec som motsvarar alla de tabeller som definieras i avsnitt 8.1-8.6. Alla de tabeller som definieras i avsnitt 8.7 har många-till-många-relationer, och de följer denna namngivningskonvention:

Användare **tilldelad_till** *ärende*

Där text i kursiv stil är tabeller med en nyckel (den unika posten i tabellen användare identifieras unikt av användar-ID) och texten i fet stil anger att tabellen har sammansatta nycklar (den unika posten i tabellen tilldelad_till identifieras unikt med både ett användar-ID och ett ärende-ID).

8.7.1 Relation produkt till meddelande

I databasen iBot_dec finns en tabell som heter ”har_meddelande”. I den tabellen finns följande information:

- Produkt-ID (PID)
  - En unik identifierare för produkten i form av ett positivt heltal som meddelandet i samma rad med värden är relaterad till.
- Meddelande-ID (MID)
  - En unik identifierare för meddelandet i form av ett positivt heltal som produkten i samma rad med värden är relaterad till.
- Typ
  - Den meddelandetyp som hänvisas till med meddelande-ID i samma rad med värden.
- Markering
  - Varje meddelande kan ha markeringen ”inte markerad”, ”relevant”, ”inte relevant” eller ”privat”.
- Ursprungligt meddelande-ID
  - Den unika teckensträng i form av ett UUID (Universally Unique Identifier) som unikt identifierar ett meddelande. Härrör från det ursprungliga datapaket som meddelandet hörde till.

8.7.2 Relation mellan användare och åtkomst till ärenden

Användare av granskningsplattformen får explicit åtkomst till ärenden av administratörer. Relationen mellan användare av granskningsplattformen och ärenden hanteras genom tabellen ”tilldelad_till”. Tabellen ”tilldelad_till” innehåller följande attribut:

- LEEP-användarnamn
  - Användarnamnet för den Hola iBot-användare som har åtkomst till det ärende som identifieras i samma rad med värden.
- Ärende-ID
  - Ärende-ID för det ärende som Hola iBot-användaren i samma rad med värden har åtkomst till.

8.7.3 Relationen mellan JID och ärenden

Enhetsanvändare (JID:n) tilldelas till ärenden som ett sätt att gruppera dem med andra enhetsanvändare som ofta kommunicerar med varandra, enligt beskrivning i 8.1.1. Eftersom många enhetsanvändare kan motsvara många ärenden är sådana relationer möjliga i tabellen ”tillhör”. Tabellen ”tillhör” innehåller följande attribut:

- Enhetsanvändar-ID
  - JID för den användare som är relaterad till ärende-ID:t i samma rad med värden
- Ärende-ID
  - Det ärende-ID som motsvarande JID är relaterat till.
- Datum för skapande
  - Det datum då relationen skapades i databasen iBot_dec.

8.7.4 Relationen mellan JID och grupper

Enhetsanvändare (JID:n) läggs till i grupper av gruppadministratörer i applikationen ANØM. JID:n kan vara medlemmar i många grupper, och grupper kan ha många JID:n som är medlemmar. Denna relation är alltså tillåten i tabellen ”medlem_i”. Tabellen ”medlem_i” innehåller följande attribut:

- Enhetsanvändar-ID
  - JID för den användare som är medlem i den grupp som identifieras i samma rad med värden
- Grupp-ID (GID)
  - GID för den grupp som motsvarande JID är medlem i.

9. INMATNINGSPROCESS

Efter avkrypteringen av alla krypterade innehållsfält, smeknamn i förteckningen, gruppnamn och bilagor, liksom justering av sökvägar i fältet ”innehåll” för meddelanden av typen ptt, video, bild eller anteckning fortsätter inmatningsprocessen med de steg som beskrivs i det här avsnittet (avsnitt 9). I det här avsnittet beskrivs processen för att överföra data på I1 från databasen iBot_enc (där nya datapaket sparades tillfälligt) till databasen iBot_dec, som ger granskningsplattformen tillgång till nya data.

Förutsättningarna för att inleda inmatningsprocessen anges i avsnitt 5-7:

- Avkryptera det krypterade nya datapaketet
- Extrahera dataarkivet
  - Filer i bilagor
  - MySQL-skillnadsdumpen
    - Enligt beskrivningen i avsnitt 2.2 innehåller skillnadsdumpen bara nya eller annorlunda data.
- Mata in MySQL-skillnadsdumpen i den tillfälliga databasen iBot_enc
- Avkryptera alla krypterade fält i databasen
- Korrigera sökvägar i alla fält i databasen som hänvisar till filer i bilagor
- Avkryptera alla filer i bilagor
- Konvertera och tonhöjdsjustera ljudet, om det behövs

9.1 Mata in ny information i förteckningen

De första dataposterna som infogas i databasen iBot_dec är förteckningsinformationen. Följande process används för att lägga till ny information i förteckningen:

1. Läs in alla nya förteckningsdata från iBot_enc (nya MySQL-data)
2. För varje ny post i förteckningen:
   a. Kontrollera om enhetsanvändar-ID:t (JID) redan finns i tabellen ”förteckning” i iBot_dec
   b. Om enhetsanvändaren redan finns indikerar det att användaren har ändrat sitt visningsnamn för enhetsanvändare.
      i. Om det nya visningsnamnet inte stämmer överens med det gamla visningsnamnet uppdateras det nya visningsnamnet i tabellen ”förteckning” i iBot_dec.
   c. Om enhetsanvändaren inte existerar indikerar det att det är en helt ny användare. Användaren läggs till i tabellen ”förteckning” i iBot_dec och en relation läggs till för enhetsanvändaren så att den motsvarar ärendet ”OKÄND”.
      i. Ärendet ”OKÄND” är ett standardärende där alla nya enhetsanvändare (JID) och enheter placeras tills dess att man hittar ett ärende eller ett syndikat där de kan placeras.

Eventuella fel som uppstår när enhetsanvändares visningsnamn uppdateras eller när användaren infogas i tabellen ”förteckning” loggas.

9.2 Infoga nya grupper

9.2.1 Infoga ny gruppinformation

Ny information om grupper i ANØM-plattformen matas in efter den nya förteckningsinformationen. Följande process används för att lägga till ny gruppinformation:

1. Läs in alla nya gruppdata från iBot_enc (nya MySQL-data)
2. För varje grupp i nya data:
    a. Grupp-ID (GID), gruppnamn och datum för infogande matas in i tabellen ”grupper” i databasen iBot_dec.

9.2.2 Infoga uppdateringar om medlemskap i grupper

Medlemmar lades till i grupper på ANØM-plattformen av gruppadministratörer, och dessa uppdateringar togs emot i MySQL-skillnadsdumpen. Följande process används för att uppdatera relationen gruppmedlemskap:

1. Läs in alla nya data om gruppmedlemskap från iBot_enc (nya MySQL-data)
2. För varje ny relation mellan grupp-ID (GID) och enhetsanvändar-ID (JID):
    a. GID och JID matas in i tabellen ”medlem_i” i databasen iBot_dec.

9.3 Inmatning av meddelanden

Efter att förändringar i förteckningen och grupper har uppdaterats i databasen inleds processen för att mata in meddelanden. Det här är den primära inmatningsmekanismen som gör det möjligt att granska data i form av produkter (konversationer). Inmatning av meddelanden följer den process som beskrivs i det här avsnittet (9.3).

9.3.1 Initialisering

Innan nya data matas in initialiseras vissa komponenter.

9.3.1.1 Svart lista

Den svarta listan är en radavgränsad textfil som separerar JID:n. I filen finns JID:n vars skickade meddelanden är svartlistade från att matas in i databasen iBot_dec. Svartlistningsfunktionen kommer att beskrivas närmare i ett framtida tillägg.

9.3.1.2 Tillfällig datastruktur för konversationer

Datastrukturen som ska innehålla alla unika konversationer och de meddelanden som motsvarar dem initialiseras. Det här är de data som används för att skapa produkter efter att alla nya meddelanden har gåtts igenom.

9.3.1.3 Tillfällig datastruktur för ärende-till-JID

Det här är en datastruktur med en lista över JID:n som hör till varje ärende i databasen. Datastrukturen kommer att användas senare för att skapa korrekta produkter. Den skapas från data i tabellen ”tillhör”.

9.3.1.4 Hämta senaste meddelande-ID (MID)

Genom att hämta det senast infogade meddelande-ID:t (MID) får man fram det meddelande-ID (MID) som är först i de nya data, eftersom MID är stigande positiva heltal.

9.3.1.5 Läs in nya meddelanden

De nya meddelandena läses in från iBot_enc (nya MySQL-data) för att infogas.

9.3.2 Infoga meddelanden

För varje meddelande genomförs sedan resten av åtgärderna i avsnitt 9.3.2.

9.3.2.1 Infoga metadata

I databasen iBot_dec finns en tabell med namnet ”metadata” som innehåller de data som har gemensamma attribut från alla de fyra meddelandetabeller som beskrivs i avsnitt 8.6. Tabellen ”metadata” innehåller följande attribut:

- Meddelande-ID (MID)
- Ursprungligt meddelande-ID
- Tid
- Avsändare
- Mottagare
- Mobile Country Code (MCC)
- Är grupp
- Typ
- Platsinformation

Alla attributen ovan definieras i avsnitt 8.6 i avsnittet om metadata. Alla metadataattribut infogas för alla meddelanden oavsett meddelandetyp.

9.3.2.2 Infoga efter typ

Inmatningsprocessen skiljer sig åt beroende på meddelandetyp.

9.3.2.2.1 Meddelanden av typerna ”text”, ”kontakt” och ”vidarebefordrat”

Om meddelandetypen är ”text”, ”kontakt” eller ”vidarebefordrat” kopieras fältet ”innehåll” från meddelandetabellen i iBot_enc till fältet ”innehåll” i tabellen ”textmeddelande” i iBot_dec. Värdet i fältet ”innehåll” avkrypterades genom stegen i avsnitt 6.1.

9.3.2.2.2 Meddelanden av typen ”anteckning”

Om meddelandetypen var ”anteckning” avkrypterades anteckningsbilagan. Efter avkrypteringen visas anteckningsbilagor som komprimerade ZIP-filer som innehåller text- och bildfiler. Filerna fördelas ut i tabellerna ”textmeddelande” och ”bildmeddelande”.

Först extraheras ZIP-filerna för bearbetning. För varje extraherad fil fastställs först huruvida filen är en textfil eller en bildfil. Om det är en textfil läses texten och infogas i fältet ”innehåll” i tabellen ”textmeddelande”. Om det däremot är en bildfil kopieras bildfilen till den katalog som användes för att skicka bilder till frontend-webbapplikationen, och en datapost infogas i tabellen ”bildmeddelande”.

Alla poster som infogades i ”textmeddelande” eller ”bildmeddelande” fick attributet ”från anteckning” uppdaterat till värdet 1 för att visa att texten/bilden är en komponent från en anteckning.

9.3.2.2.3 Meddelanden av typerna ”ptt”, ”bild” och”video”

Om meddelandetypen är ”ptt”, ”bild” eller ”video” kopieras fältet ”innehåll” direkt från meddelandetabellen i iBot_enc till motsvarande meddelandetabell (beroende på typ) i iBot_dec. Sökvägarna i fältet ”innehåll” korrigerades på plats och uppdaterades till de nya sökvägar som användes av frontend-webbapplikationen för granskning. Mer information om hur sökvägarna uppdateras finns i avsnitt 6.1.1.

9.3.4 Tilldela meddelanden till produkter

Efter att tabellen metadata har fyllts på och infogandet i tabeller efter typ har slutförts placeras meddelandet i en konversation med hjälp av den tillfälliga datastruktur som initialiserades i avsnitt 9.3.1.2.

Den här datastrukturen innehåller en kapslad unik lista med konversationer som alla innehåller deltagarna (JID) i konversationen, MCC-koder (Mobile Country Codes) som meddelandena skickades från, meddelande-ID (MID) och meddelandetypen (”text”, ”ptt”, ”video” osv.).

Efter att alla meddelanden har placerats i en konversation är processen för nya meddelanden klar och användandet av den tillfälliga databasen iBot_enc avslutas.

9.4 Inmatning av produkter

När konversationsdata har fyllts i är produkterna redo att skapas för det nya datapaketet. I resten av avsnitt 9.4 bearbetas varje unik konversation i den tillfälliga datastruktur som innehöll meddelanden.

9.4.1 Skapa produkter per ärende

För varje ärende verkställs stegen under 9.4.1.1 för konversationen.

9.4.1.1 Om JID i konversationen tillhör ett ärende

Om en enhetsanvändare som är deltagare i den aktuella konversationen tillhör det aktuella ärendet gås stegen 9.4.1.1.1- 9.4.1.1.3 igenom.

9.4.1.1.1 Skapa produkt för ärenden

Om 9.4.1 och 9.4.1.1 har genomgåtts för den aktuella konversationen skapas en produkt för det aktuella ärendet. Följande värden infogas baserat på tillfälliga datastrukturer och nuvarande status för inmatningskoden:

- Ärende-ID
- Skapad datum
- MCC-sträng (Mobile Country Code)
- Enhetsanvändar-ID-sträng (JID)
- Antal
- Grupp-ID (GID) – om det behövs
- Känd grupp – Om gruppinformation hittades under skapandet av produkten (genom sökning i tabellen ”grupper”) sätts det här värdet till 1.

9.4.1.1.2 Skapa relation för meddelande och JID till produkt

Som nämndes i avsnitt 8.7.1 är meddelanden associerade med produkter genom användning av tabellen ”har_meddelande”. Efter att produkten har skapats för det aktuella ärendet associeras alla meddelanden i den tillfälliga konversationsdatastrukturen med produkten genom att deras meddelande-ID:n (MID) infogas i ”har_meddelande” tillsammans med det produkt-ID (PID) som infogades.

Det finns en tabell i databasen iBot_dec som heter ”del_av” som kopplar enhetsanvändar-ID:n (JID) till produkt-ID:n (PID). Då skapas en tabell som informerar systemet om att en specifik användare har skickat meddelanden som syns i en produkt. Den tabellen innehåller följande attribut:

- Enhetsanvändar-ID
- Produkt-ID (PID)

Tabellen fylls också i när en ny produkt skapas.

9.4.1.1.3 Tilldela standardmarkering till produkt

Det finns en tabell i databasen iBot_dec med namnet ”har_markering” där textbaserade

markeringar kopplas till produkter. Produkter kan markeras i granskningsplattformen Hola iBot av Hola iBot-användare. Tabellen ”har_markering” innehåller följande attribut:

- Produkt-ID (PID)
- Markering
    - En textbaserad markering som kan sättas på en produkt.
    - Markeringen kan t.ex. vara inte granskad (standardmarkering), relevant eller inte relevant.

Standardproduktmarkeringen inte granskad infogas i tabellen ”har_markering” för den produkt som genereras.

9.5 Export efter inmatning

Krypterade exporter skickades automatiskt via SFTP (Secure File Transfer Protocol) till länder som omedelbart behövde granska nya data i datapaket. Dessa krypterade exporter innehöll en JSON-fil (JavaScript Object Notation) för varje ärende som landet ifråga hade getts åtkomst till. JSON-filen innehöll alla produktdata för det tidigare inmatade datapaketet.

10. WEBBAPPLIKATION/GRANSKNINGSPLATTFORM

Hola iBot är den anpassade webbapplikation som har skapats och drivs av FBI i San Diego och som fungerar som granskningsplattform för alla data som har tagits emot från ANØM-plattformen.

10.1 Kontroll av användaråtkomst i Hola iBot

De användarroller för granskningsplattformen som definieras i avsnitt 8.2 är roller för användare av Hola iBot. Som har nämnts tidigare måste alla användare i avsnitt 8.2 först få konton i LEEP (Law Enforcement Enterprise Portal).

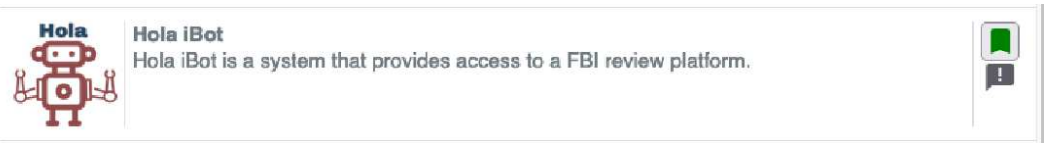
10.1.1 Åtkomstkontroll för LEEP (Law Enforcement Enterprise Portal)

LEEP (Law Enforcement Enterprise Portal) är en portal som brottsbekämpande myndigheter (även internationella sådana) och andra underrättelsegrupper kan få konton i. När avdelningen som ger åtkomst har granskat den ansökande användaren ges användaren åtkomst till listan med applikationer/verktyg. Ett av dessa är granskningsportalen Hola iBot.

LEEP använder gemensamma metoder för autentisering av användare, t.ex. tvåfaktorautentisering (2FA), säkerhetsbilder och säkerhetsfrågor.

10.1.2 Åtkomstkontroll i Hola iBot

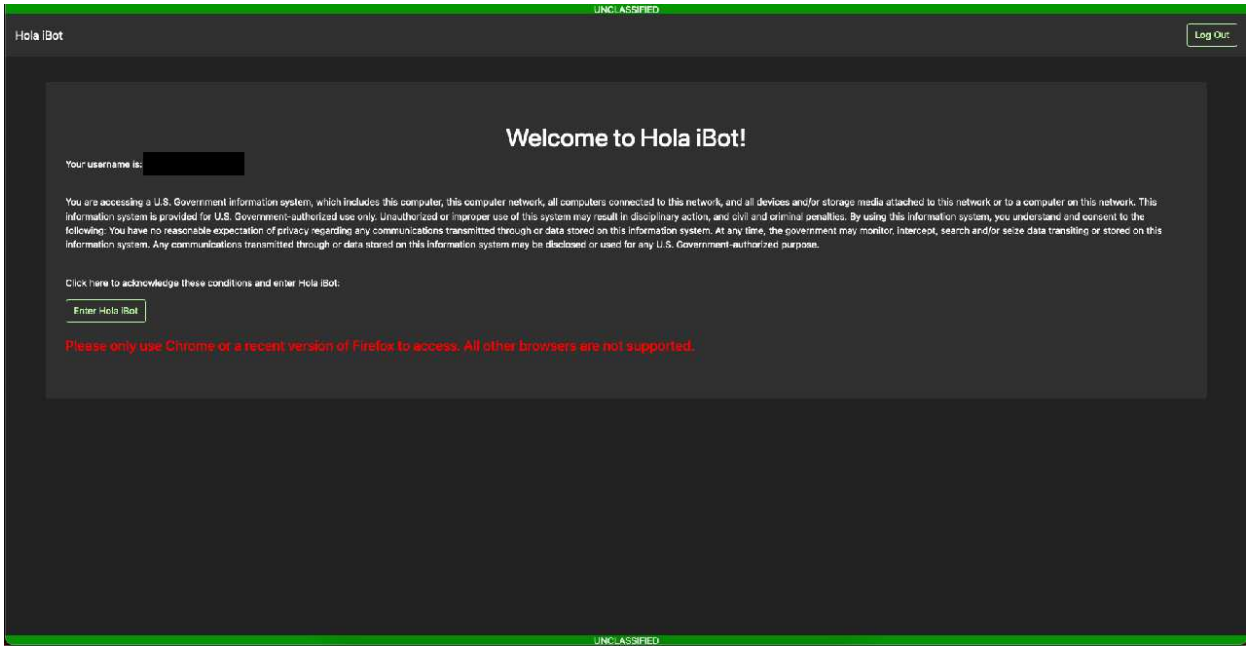
När en användare har autentiserat sig genom den LEEP-administrerade inloggningsprocessen kan användaren öppna applikationen Hola iBot genom att klicka på applikationen i listan som visas i skärmbilden nedan.



Skärmbild 10.A

När man klickar på applikationen Hola iBot skickas en SSO-begäran (single sign-on) i SAML (Security Assertion Markup Language) till frontend-servern för webbapplikationen. SAML är ett protokoll som gör det möjligt för identitetsleverantörer att skicka autentiserade inloggningsuppgifter till en annan tjänst, och det är så Hola iBot autentiserar användare.

Användaren av granskningsplattformen ges bara åtkomst till systemet om de finns upptagna i tabellen ”användare” som omnämns i avsnitt 8.2. Om de ges behörighet till applikationen hälsas de av varningsmeddelandet i skärmbild 10.B.

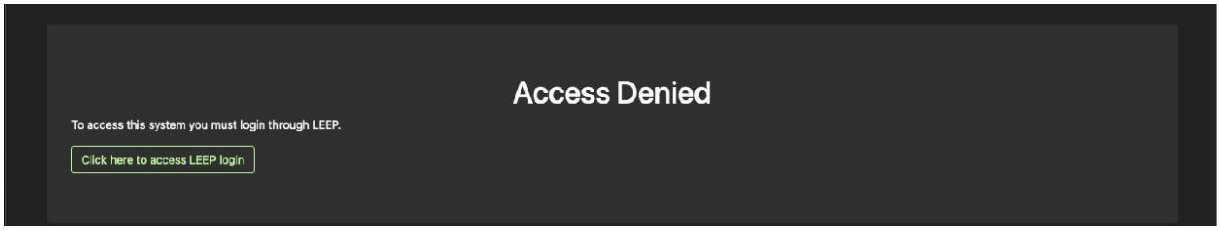


Skärmbild 10.B

Texten i varningsmeddelandet är följande (översatt till svenska):

> *Du ansluter till ett informationssystem som ägs av USA:s federala regering. Det omfattar den här datorn, det här datornätverket, alla datorer som är anslutna till det här nätverket och alla enheter och/eller lagringsmedia som är anslutna till det här nätverket eller till en dator i det här nätverket. Informationssystemet tillhandahålls enbart för användning som är godkänd av USA:s federala regering. Obehörig eller oriktig användning av systemet kan leda till disciplinära åtgärder samt civil- och straffrättsliga sanktioner. Genom att använda det här informationssystemet förstår du och ger ditt samtycke till följande: Du kan inte förvänta dig någon form av personlig sekretess gällande någon form av kommunikation som genomförs på det här systemet, eller gällande data som lagras på det. USA:s federala regering kan när som helst övervaka, avläsa, genomsöka och/eller beslagta data som passerar igenom eller lagras på det här informationssystemet. All kommunikation som skickas, och alla data som lagras, på det här informationssystemet kan röjas eller användas för vilket syfte som helst som är godkänt av USA:s federala regering.*

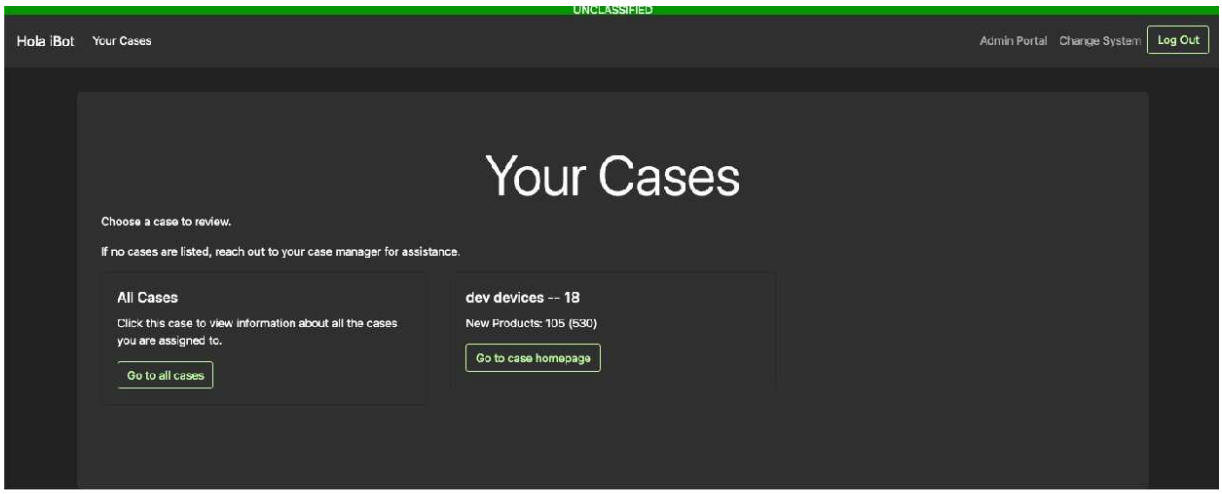
Om användaren inte finns i databasen ser de en generisk sida om nekad åtkomst. Den sidan visas i skärmbild 10.C.



Skärmbild 10.C

10.2 Ärenden i Hola iBot

Om användaren får åtkomst till systemet genom LEEP-autentisering och explicit åtkomst till databasen Hola iBot kommer användaren till sin hemsida, där det visas en lista med ärenden som användaren har fått explicit åtkomst till. I skärmbild 10.D visas hemsidan för en användare som har åtkomst till ett enda ärende, ”dev devices”, med ärende-ID 18.



Skärmbild 10.D

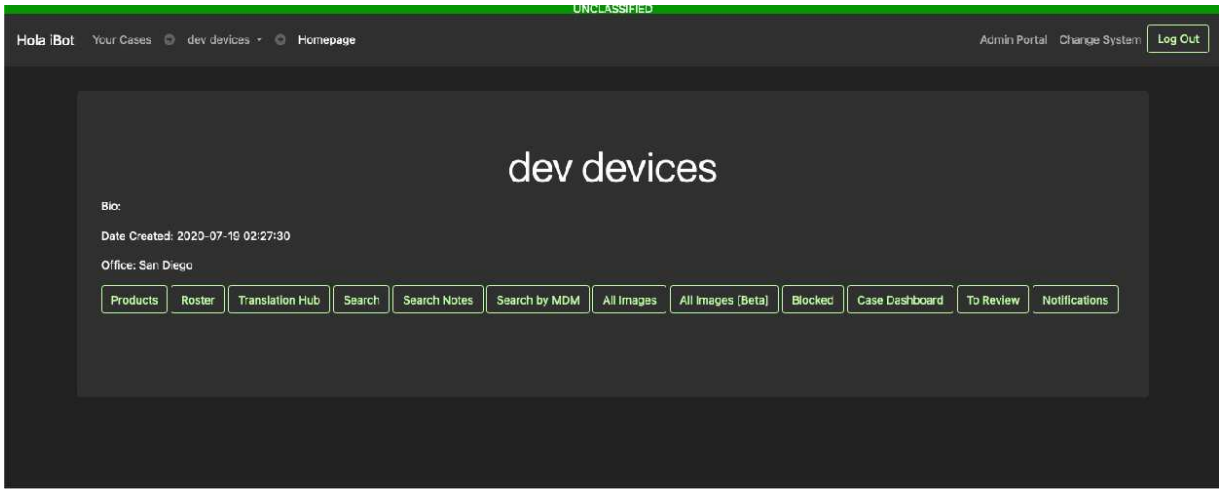
Listan med ärenden som visas på hemsidan baseras på tabellen ”tilldelad_till” enligt beskrivningen i avsnitt 8.7.2 ovan.

Vid visning av ett enda ärende filtreras data på de återstående sidorna till enbart de enhetsanvändare (JID) som är kopplade till ärendet i tabellen ”tillhör” (relationen mellan JID och ärende-ID), enligt beskrivningen i avsnitt 8.7.3.

Användarna har också alternativet ”alla ärenden”. Om det alternativet väljs blir de återstående sidorna ifyllda med alla data som användaren av granskningsplattformen har åtkomst till.

10.2.1 Ärendets hemsida

När en användare av granskningsplattformen har navigerat till ett ärende visas hemsidan för det ärendet. På ett ärendes hemsida visas flera alternativ. Ett exempel på en hemsida för ett ärende visas i skärmbild 10.E.



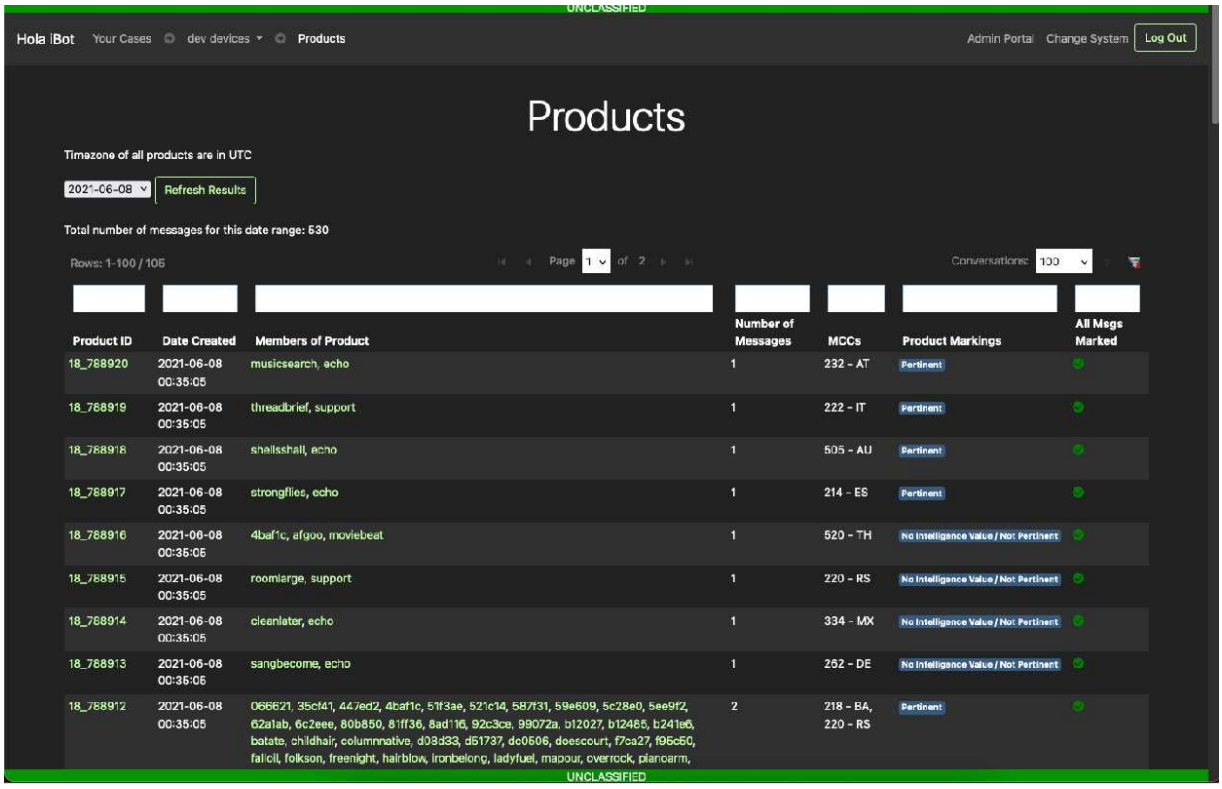
Skärmbild 10.E

I resten av avsnitt 10 beskrivs alternativen på ärendets hemsida närmare.

10.3 Produktsidan

Produktsidan är den sida som användare går till för att visa konversationerna i ärendet. Se avsnitt 8.5 för mer information om produkter och avsnitt 9.4 för mer information om hur produkter skapas.

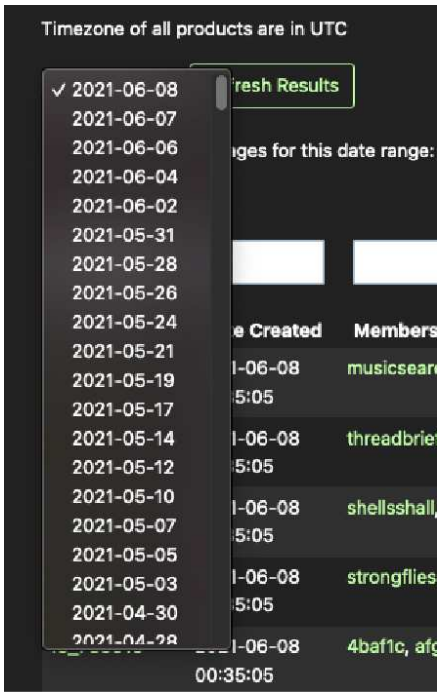
Produkter är unika konversationer för ett ärende som togs emot i ett datapaket. I skärmbild 10.F visas produktsidan för ärendet ”dev devices”.



Skärmbild 10.F

I nedrullningsmenyn överst till vänster där ”2021-06-08” är ifyllt finns en lista med datum då nya

datapaket togs emot:



Skärmbild 10.F.1

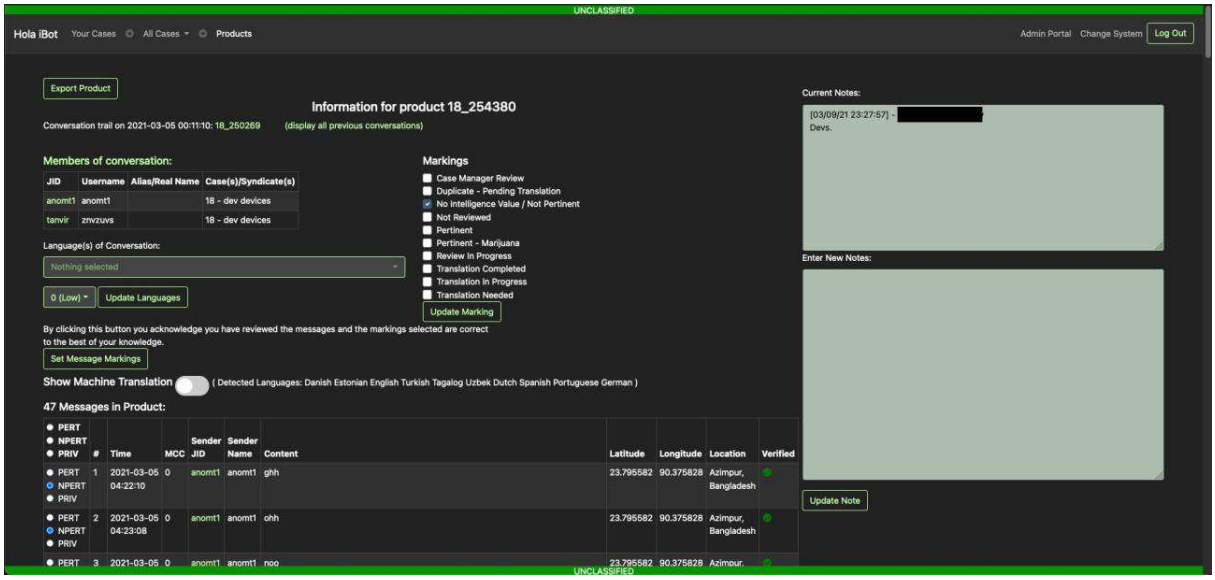
Listorna med produkter är unika per överföringsdatum. Som visas i skärmbild 10.F visas inte produkt-ID (PID) under ”Product ID” i listan över produkter. Det ”Product ID” som visas för användaren anges med ärende-ID följt av understreck och sedan det faktiska produkt-ID:t (PID). Det är ett enklare sätt att universellt hänvisa till produkter och det blir enklare att veta vilka ärenden som produkten hör till.

Resten av data som visas på den här sidan hämtas från tabellerna ”produkter”, ”har_markering” och ”har_meddelande”.

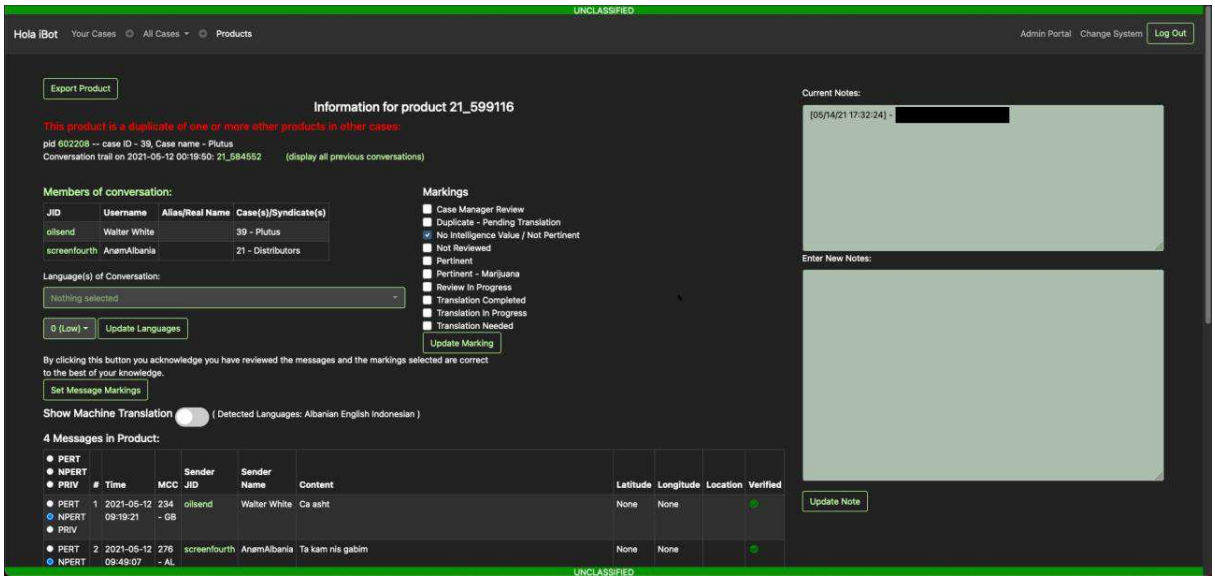
- “Date Created”
  - hämtas från fältet för skapandedatum i tabellen ”produkt”
- ”Members of Product”
  - hämtas från fältet ”JID-sträng” i tabellen ”produkt”
  - Alla JID:n som visas i den här kolumnen är länkade till JID-profilen.
    - Se avsnitt 10.7 för mer information om JID-profilen.
- ”Number of Messages”
  - hämtas från fältet ”antal” i tabellen ”produkt”
- ”MCCs”
  - hämtas från fältet ”MCC-sträng” i tabellen ”produkt”
- ”Product Markings”
  - hämtas från tabellen ”har_markering”, som relaterar produkten till en textbaserad markering
- ”All Msgs Marked”
  - hämtas genom att köra en sökfråga mot tabellen ”har_meddelande” för att testa om alla meddelanden har en markering som inte är standard

10.4 Produktsidan

Länkarna under ”Product ID” går till produktsidan, där meddelandena för produkten visas som på skärmbild 10.G och 10.G.1.



Skärmbild 10.G



Skärmbild 10.G.1

På produktsidan visas många olika typer av information för användaren av granskningsplattformen. Produktsidan visar följande information (se skärmbild 10.G och 10.G.1):

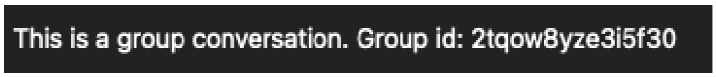
- Huruvida produkten som visas är en dubblett av en produkt i ett annat ärende.
    - I skärmbild 10.G.1 visas ett exempel på en produkt som är en dubblett, och där finns också en länk till den motsvarande dubbletten.
- Deltagarna i konversationen
    - Dessa sammanställs under inmatningsprocessen som beskrivs i avsnitt 9.4.1.1.
- De språk som granskningsplattformens användare har lagt till för produkten.

- Flera språk kan läggas till i listan.
- Språklistan motsvarar inlämnade översättningar.
  - Mer information finns i avsnitt 10.5.1.

- De markeringar som har lagts till för produkten
- De meddelandemarkeringar som granskningsplattformens användare har ställt in
- Anteckningar som har skapats om produkten (höger ruta).
  - När en anteckning väl har skapats kan den inte tas bort, utan den flyttas istället till rutan ”Current Notes” med en tidsstämpel som visar när den skapades samt användarnamnet för den användare av granskningsplattformen som lade till anteckningen.
  - Dessa anteckningar motsvarar fältet ”produktanteckning” i tabellen ”produkter”.
- Alla översättningar som har lagts till i produkten baserat på det språk som lades till syns längst ned på produktsidan.

10.4.1 Grupp-ID-visning

Om produkten motsvarar en grupp kommer följande att visas om det finns gruppinformation i databasen iBot_dec:



Skärmbild 10.G.2

10.4.2 Meddelanden med bilagor (PTT, bild, video, anteckning) i Hola iBot

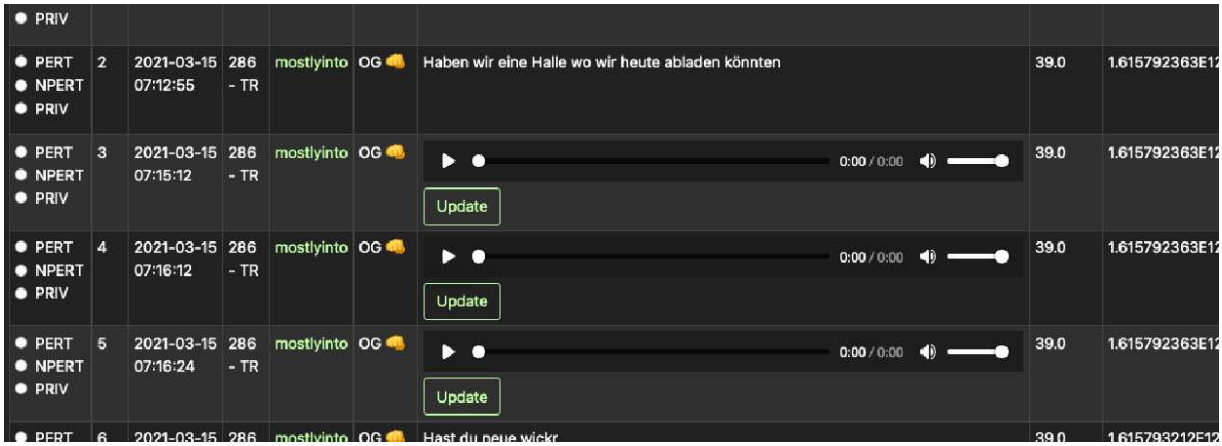
Alla meddelanden med bilagor visas inline, som textmeddelanden. Meddelanden med bilagor kan också ha en markering som tilldelas av användare av granskningsplattformen. I databasen iBot_dec finns en tabell med namnet ”bilaga_har_markering” som gör det möjligt att markera bilagor med textbaserade beskrivningar. Tabellen ”bilaga_har_markering” innehåller följande Fält:

- Meddelande-ID (MID)
  - Det MID som den textbaserade beskrivningen motsvarar
- Markering
  - Den textbaserade beskrivningen av markeringen

Markeringarna av bilagor kan ställas in på produktsidan av granskningsplattformens användare.

10.4.2.1 PTT-meddelanden (push-to-talk) i Hola iBot

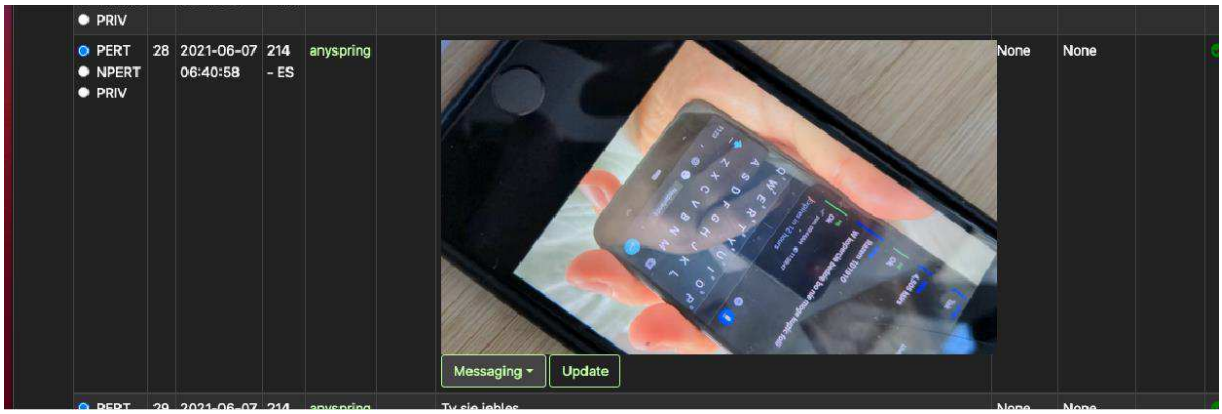
I skärmbild 10.G.3 visas ett exempel på några PTT-meddelanden.



Skärmbild 10.G.3

10.4.2.2 Bildmeddelanden i Hola iBot

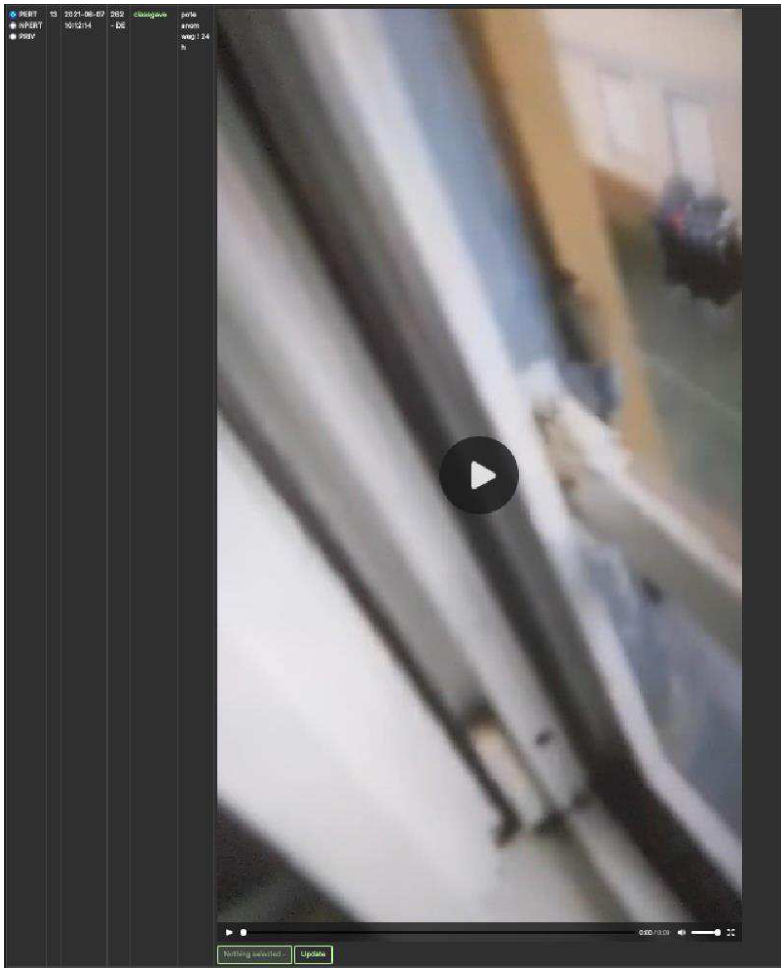
I skärmbild 10.G.4 visas ett exempel på ett bildmeddelande som visas inline.



Skärmbild 10.G.4

10.4.2.3 Videomeddelanden i Hola iBot

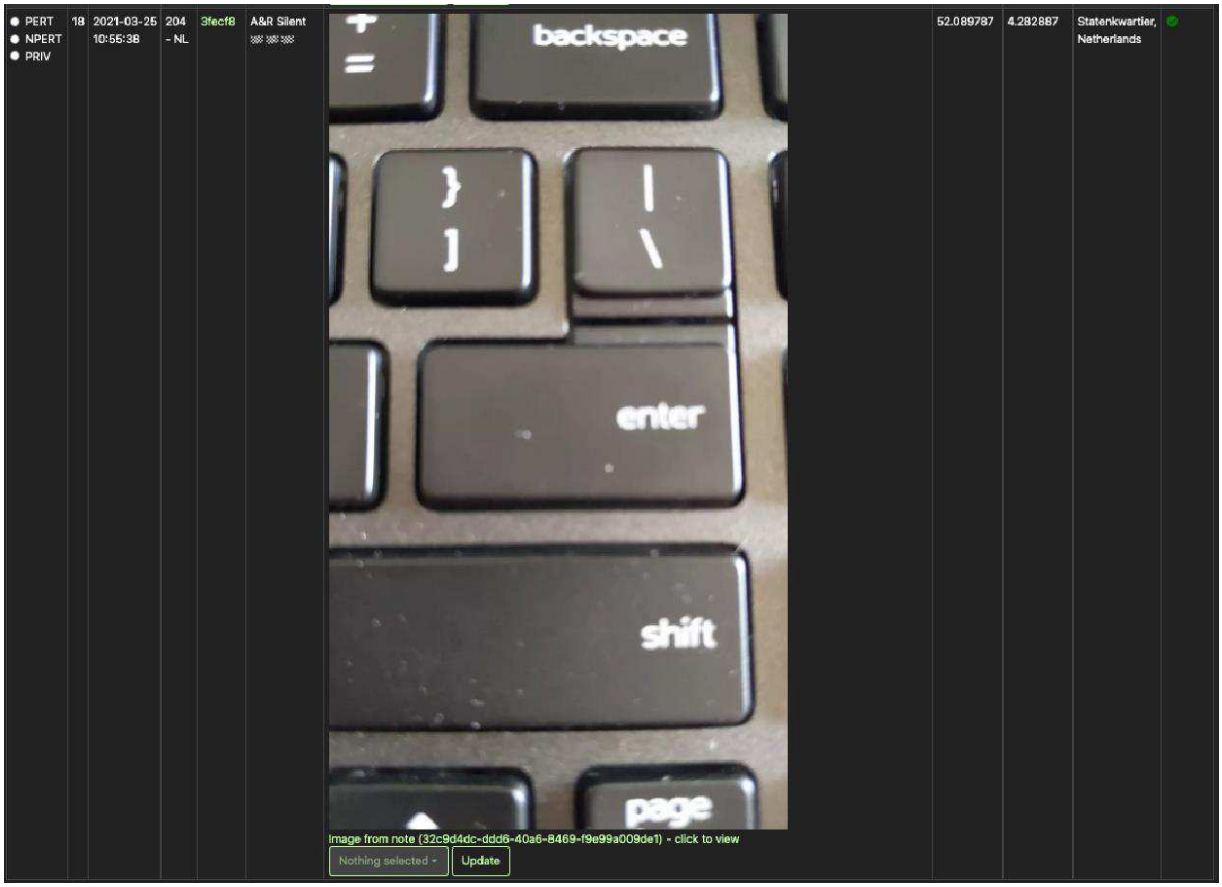
I skärmbild 10.G.4 visas ett exempel på ett videomeddelande i Hola iBot.



Skärmbild 10.G.5

10.4.2.4 Anteckningsmeddelanden i Hola iBot

I skärmbild 10.G.6 visas ett exempel på en bildkomponent för en anteckning som visas inline som ett meddelande.



Skärmbild 10.G.6

Texten ”Image from note ([Original Message ID]) – click to view” anger att bilden kommer från ett anteckningsmeddelande.

10.5 Översättningar

Om en produkt har tilldelats ett språk med hjälp av nedrullningsmenyn i skärmbild 10.G och 10.G.1 skickas produkten automatiskt på översättning. På grund av de många-till-många-relationer som språk har med produkter finns en tabell med namnet ”har_språk” i databasen för att skapa dessa relationer. Tabellen ”har_språk” har följande attribut:

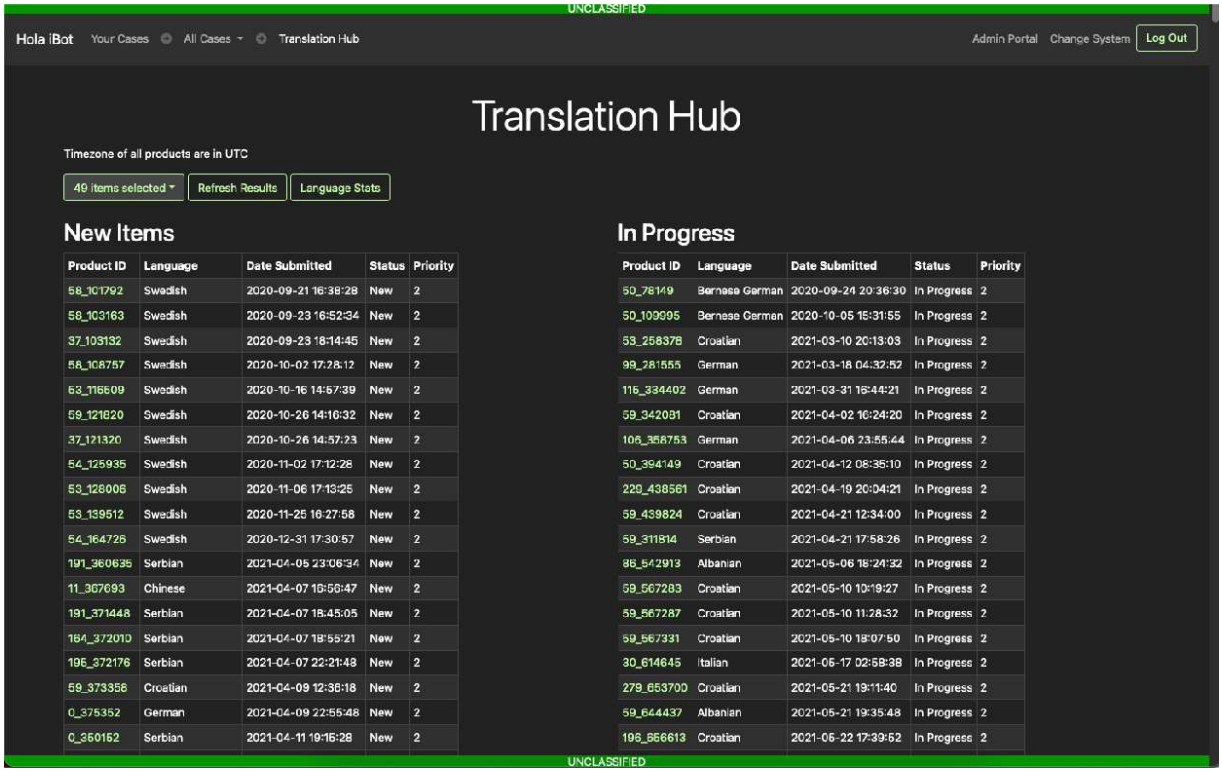
- Språk
  - Namnet på språket som tilldelas till produkten.
  - Exempel: ”engelska”, ”spanska”
- Produkt-ID (PID)
  - PID för den produkt som språket tilldelas till.
- Status
  - Det här fältet visar status på översättningen.
  - Det här fältet kan anges till ”ny”, ”pågående” eller ”klar”.
- Prioritet

- Det här fältet anger prioritet på översättningsbegäran.
- Inskickad av
  - I det här fältet anges det användarnamn på granskningsplattformen som lade till språket i produkten.
- Översättning
  - Det här är det värde som lingvisterna anger för översättningen av produkten.
- Datum för inskickande
  - Anger det datum då språket lades till för produkten
- Ärende-ID
  - Det ärende-ID som produkten motsvarar i raden av värden
- Färdigställd av
  - Det användarnamn i granskningsplattformen som angav fältet ”status” till ”klar”

När ett språk har lagt till för en produkt går det att visa produkt-ID, ärende-ID och språknamn på sidan Translation Hub.

10.5.1 Translation Hub

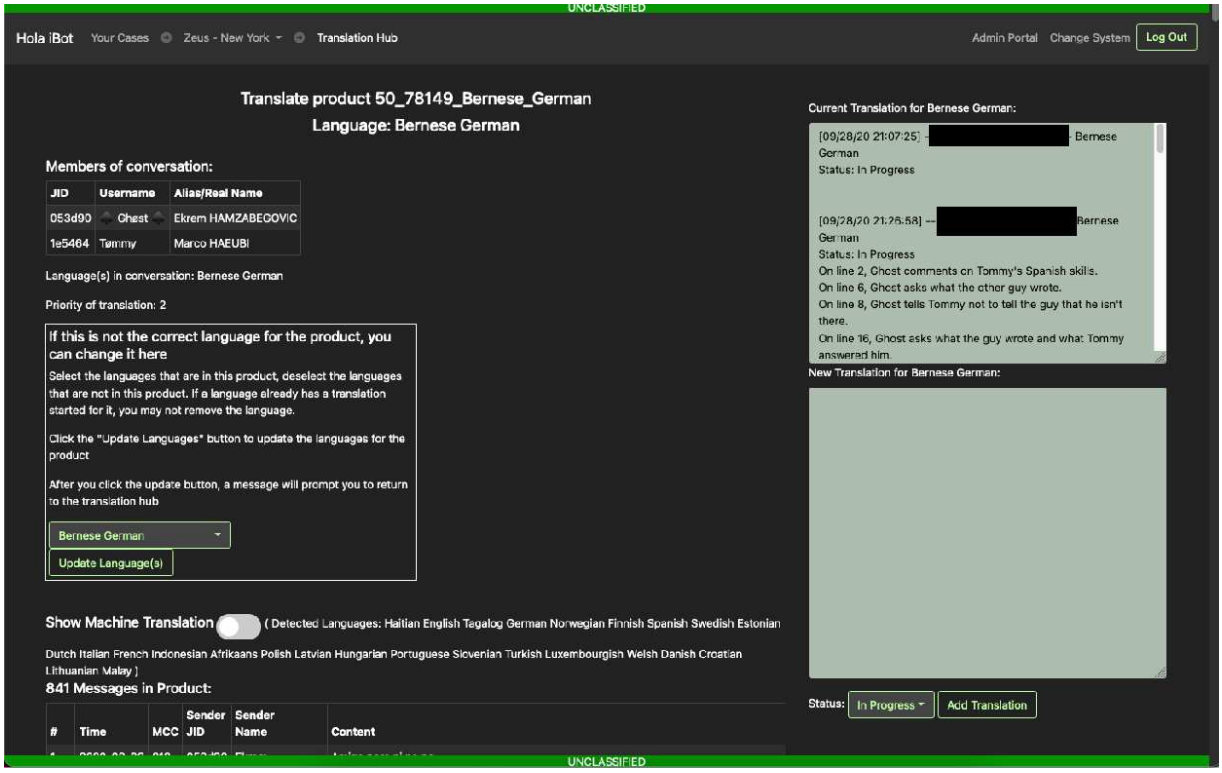
I Translation Hub finns alla översättningar som har lämnats in av användare för produkter. Skärmbild 10.H visar Translation Hub.



Skärmbild 10.H

De två listorna visar status från tabellen ”har_språk” för motsvarande produkt-ID (PID). Om en översättningsförfrågan i tabellen ”har_språk” har statusen ”klar” visas den inte längre i de två listorna.

Efter att ha klickat på en länkad produkt i Translation Hub visas en sida som liknar produktsidan, se skärmbild 10.I.



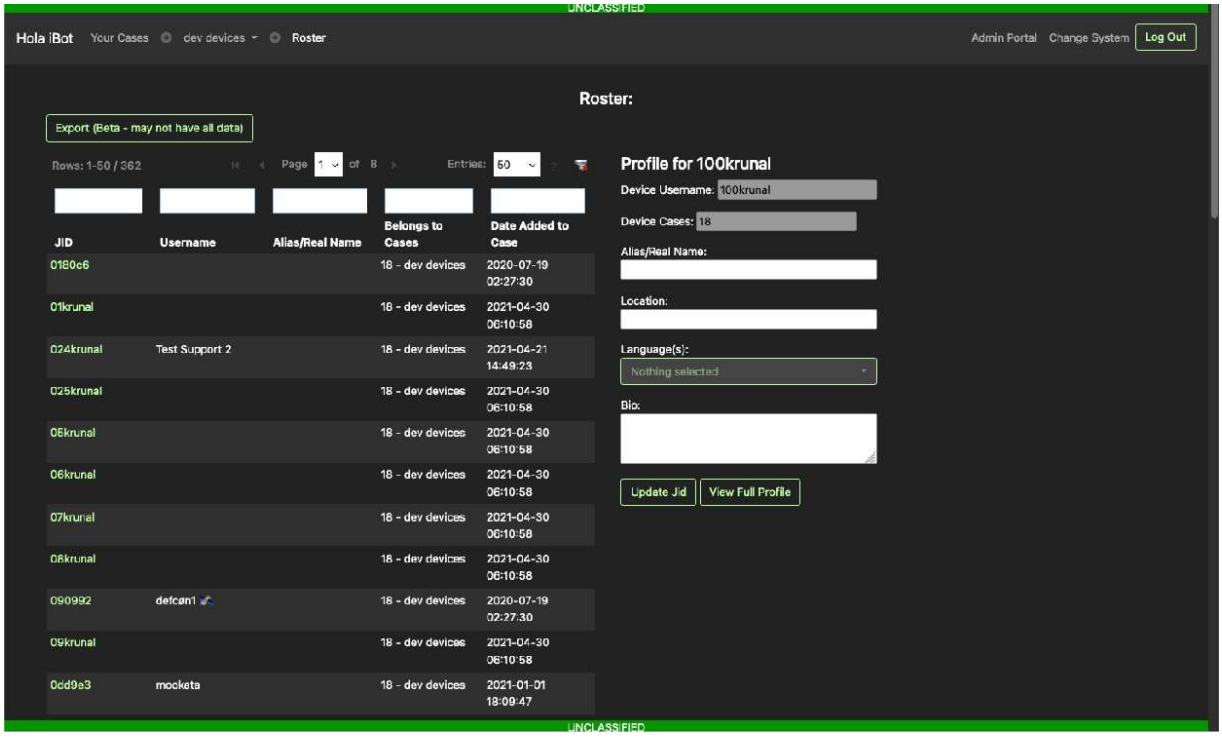
Skärmbild 10.I

På den här sidan lägger översättare till översättningar av produkter. I rutan till höger i skärmbild 10.I kan användare lägga till översättningar. När en översättning läggs till fungerar det som när en användare av granskningsplattformen lägger till anteckningar i produkter. De flyttas till textrutan ”Current Translation for [namn på språket]”. Översättningar som redan har skickats in och flyttats till den andra rutan kan inte uppdateras. De loggas också med en tidsstämpel och användarnamnet för den användare av granskningsplattformen som lade till översättningen.

Alla anteckningar som har lagts till för motsvarande produkt via produktsidan visas längst ned på översättningssidan.

10.6 Förteckningssidan

Sidan som visar förteckningen visar en lista med enhetsanvändare (JID) som har en relation med ett ärende i tabellen ”tillhör”. I skärmbild 10.J visas ett exempel på en förteckningssida för ärendet ”dev devices”.



Skärmbild 10.J

Sidan är delad vertikalt i två rutor.

I den vänstra rutan visas listan med enhetsanvändare (JID) med deras användarnamn (enhetsanvändarnas visningsnamn), verkligt namn (angett av granskningsplattformens användare om det har uppdagats under utredningen), motsvarande ärenden (enligt tabellen ”tillhör”) och datumet då de lades till i ärendet (enligt tabellen ”tillhör”).

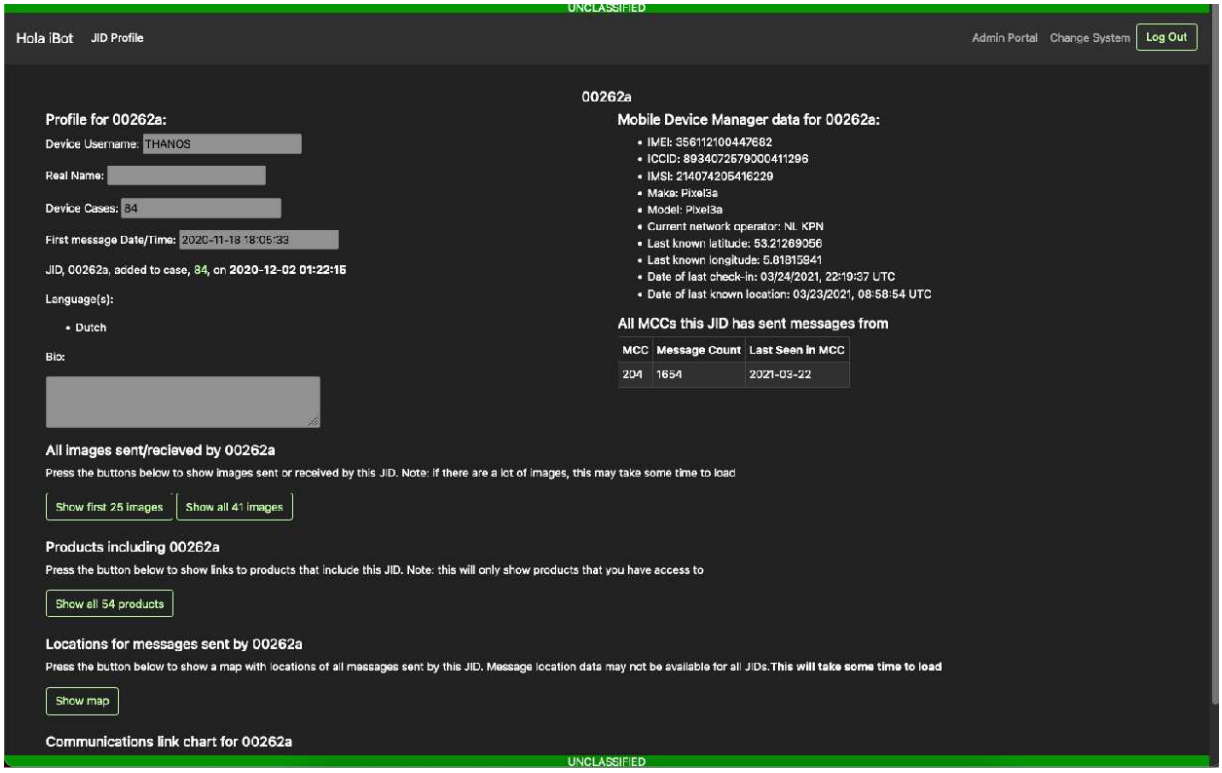
Det går att klicka på varje rad i tabellen och då fylls den högra rutan på med följande ytterligare information, som kan redigeras:

- Alias/verkligt namn
- Plats
- Språk
- Biografi

I avsnitt 8.3 finns mer information om fälten i förteckningen.

10.7 JID-profil

Det går att länka till JID-profilen från ett antal olika sidor. Ett exempel på en JID-profil visas i skärmbild 10.K.



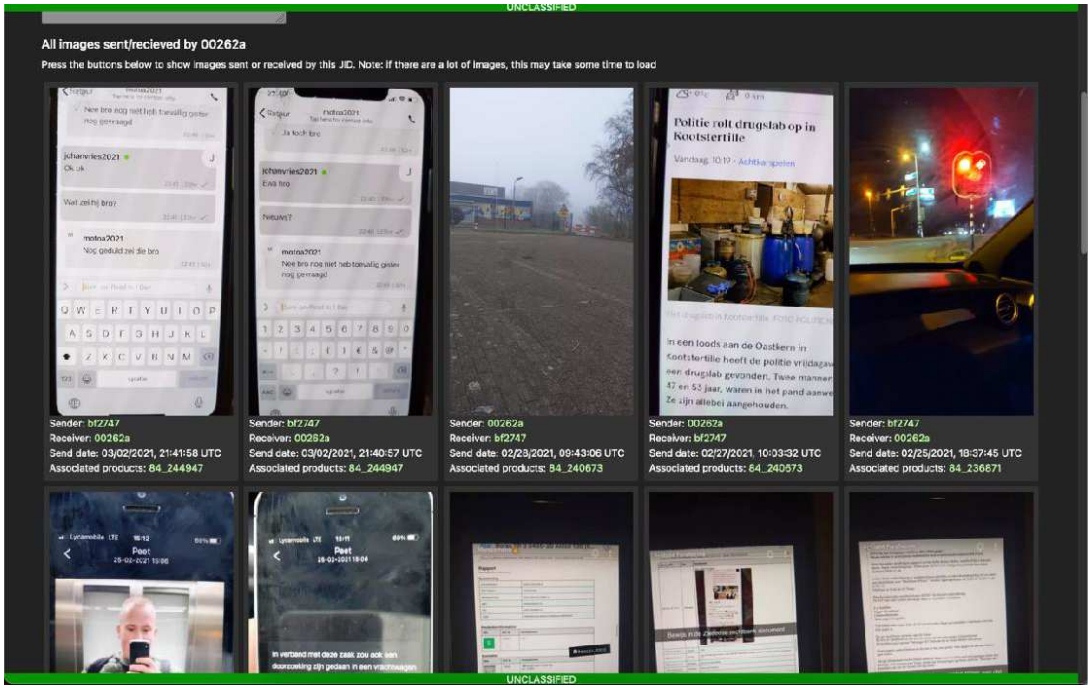
Skärmbild 10.K

Resten av avsnitt 10.7 hänvisar till skärmbild 10.K.

10.7.1 Information om enhetsanvändaren (JID)

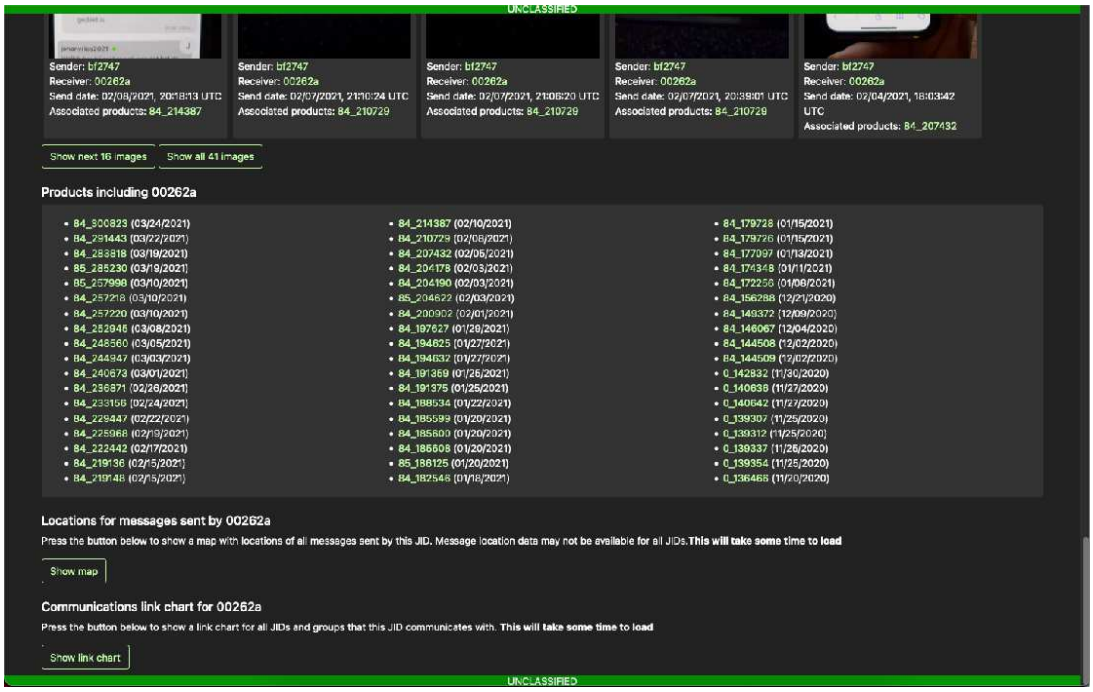
Alla förteckningsdata om enhetsanvändaren (JID) visas på JID-profilsidan. Det finns andra data som också kan hämtas från JID-profilsidan, t.ex.:

- Bilder som har skickats av enhetsanvändaren.
  - ”All images sent/received by 00262a” i skärmbilden.



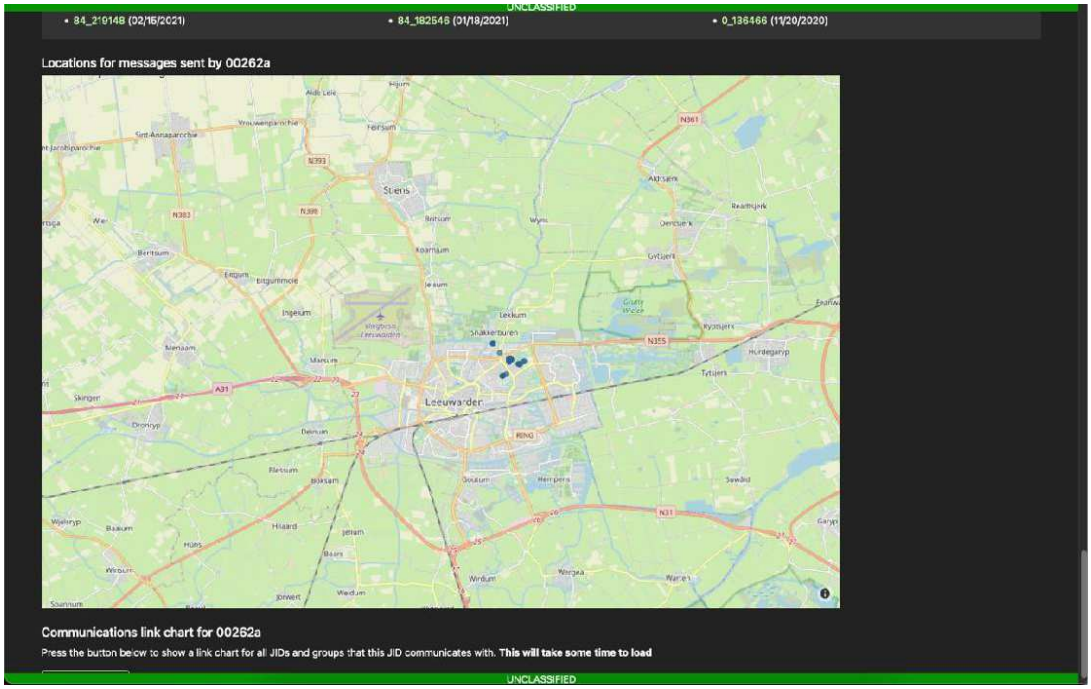
Skärmbild 10.K.1

- Produkter som användaren skickade eller tog emot meddelanden i.
  - "Products including 00262a" i skärmbilden.



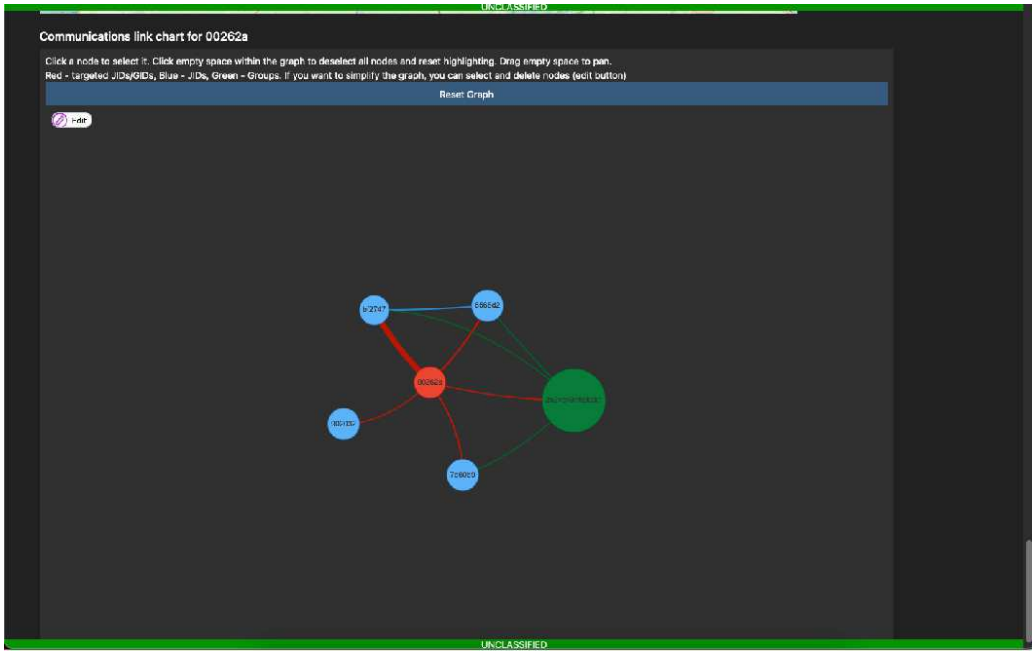
Skärmbild 10.K.2

- Om GPS-data för meddelanden var tillgängliga visas de. Mer information finns i bilaga A, 8.2.
  - ”Locations for messages sent by 00262a” i skärmbilden.



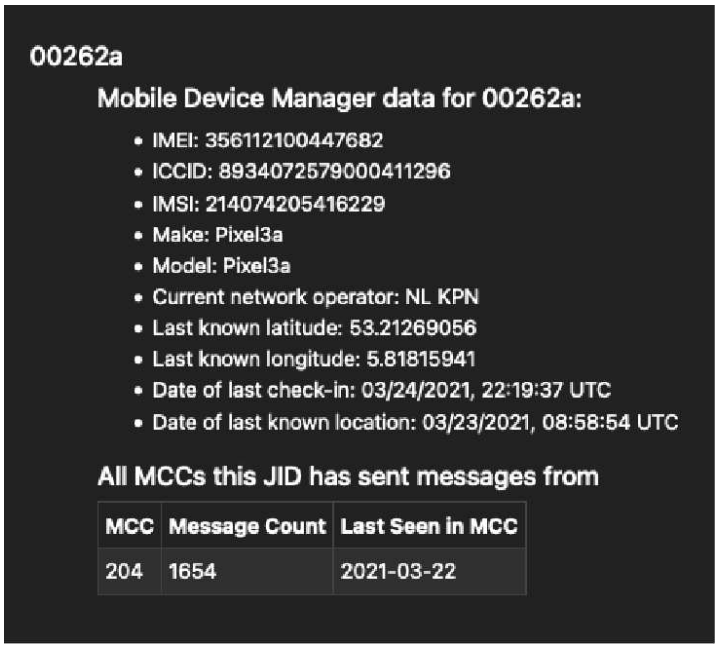
Skärmbild 10.K.3

- En interaktiv kommunikationskarta med länkar.
  - ”Communications link chart for 00262a” i skärmbilden.
  - Om man hovrar över en nod visas JID för avsändaren, ärende och senaste MCC.
  - Om man dubbelklickar på noden skickas användaren av granskningsplattformen till JID-profilen för den valda noden.



Skärmbild 10.K.4

- MDM-information (Mobile Device Manager)
  - Enligt beskrivningen i bilaga A.5 – 24.a hanterades ANØM-plattformen av en MDM-applikation, och en del av informationen från MDM-portalerna matades in i databasen iBot_dec i syfte att tillhandahålla ytterligare information om enhetsanvändare.
  - I skärmbild 10.K.5 visas en förstorad skärmbild av MDM-data för JID:t i skärmbild 10.K.



Skärmbild 10.K.5

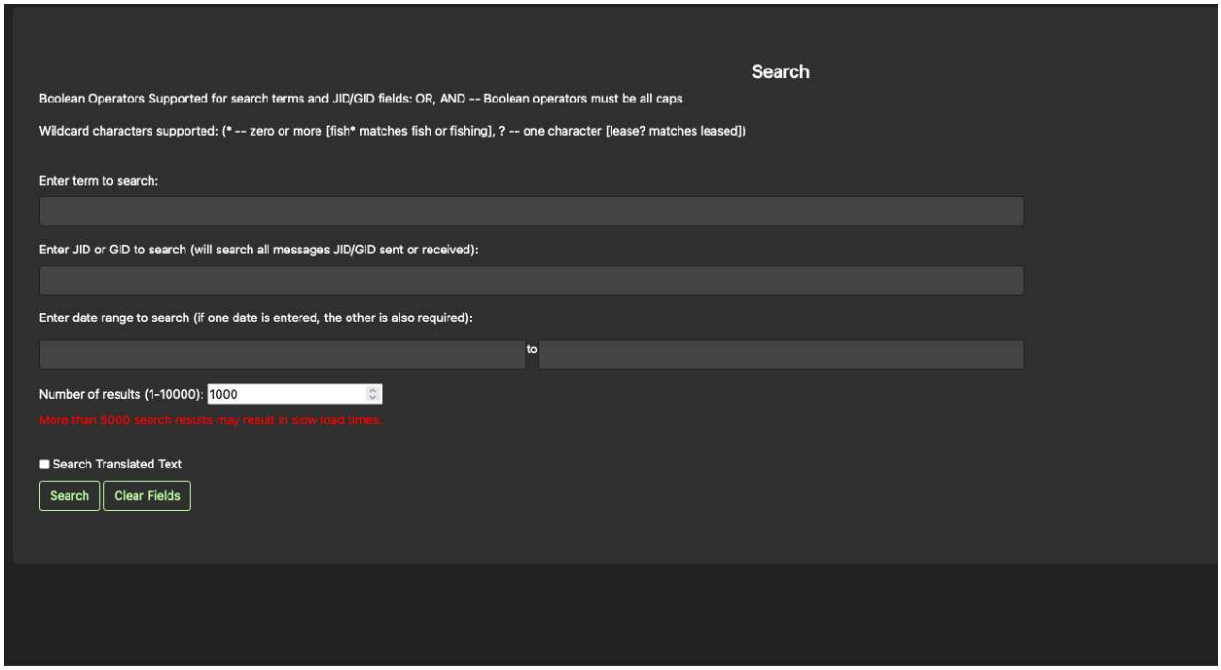
10.8 Andra sidor

10.8.1 Sökning

På söksidan kan man söka i:

- fältet ”innehåll” för meddelanden.
- enhetsanvändar-ID (JID).
- grupp-ID (GID).

Det går också att ange datumintervall för att filtrera resultaten.



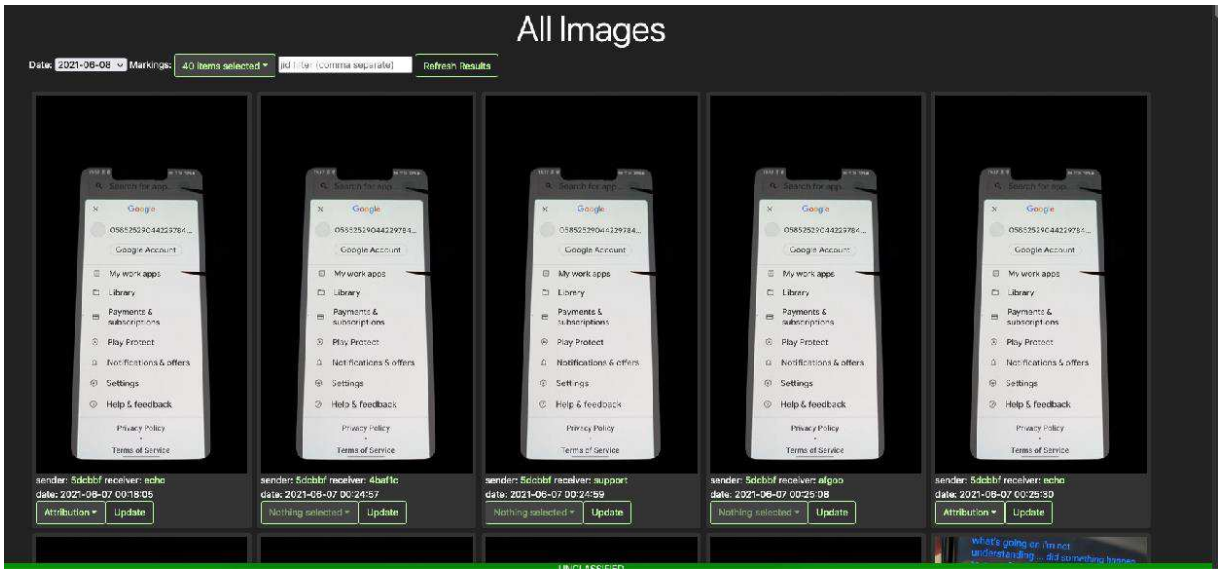
Skärmbild 10.L

10.8.2 Sök i anteckningar

När användare av granskningsplattformen lägger till anteckningar blir de sökbara via sidan Sök i anteckningar. Den har ett gränssnitt som liknar söksidan.

10.8.3 Alla bilder

På sidan Alla bilder visas alla bilder inom ramen för nuvarande åtkomstkontroller, och det går att bläddra igenom dem, markera dem med bilagemarkeringar och visa dem.



Skärmbild 10.M

10.8.4 Blockerade

En lista med meddelanden som blockerades enligt beskrivning i 9.3.1.1. Mer information kommer i en framtida bilaga.

Alla andra navigerbara sidor, baserat på användarroll (se avsnitt 8.2), används av granskningsplattformens administratörer och för andra utredningssyften.

11. MLAT-EXPORT

MLAT-förfrågningar hanteras av FBI:s field office i San Diego. De skickas in av olika länder för en lista med enhetsanvändare (JID). Förberedelser gjordes för MLAT-förfrågningarna genom att flera steg vidtogs för att skapa en automatiserad process som kunde exportera data på ett säkert sätt.

11.1 Hämtning av alla bifogade filer

Ett steg i förberedelserna var att hämta alla bifogade filer från I1-servern i AWS GovCloud. Dessa bifogade filer lagras på en arbetsstation på FBI:s field office i San Diego, som kan skapa automatiska exporter.

11.2 Hämtning av slutlig MySQL-databasdump

När nya datapaket färdigställdes den 08.06.2021 skapades en fullständig MySQL-databasdump som hämtades inför skapandet av exporter. Tidsstämplar för alla exporterade meddelanden anges i tidszonen Pacific Time.

11.3 Skapa MLAT-exporter

En sökning görs i databasen, enligt en lista på enhetsanvändare (JID), efter alla meddelanden som har skickats eller mottagits och som är relevanta för enhetsanvändaren. Meddelandena lagras tillfälligt i en andra databas som kopieras in i en .sql-fil som bifogas svaret på förfrågan. Den innehåller också alla konversationer med efterfrågade JID:n oavsett vilket syndikat (ärende) de är placerade i.

En extern enhet förbereds med LUKS-kryptering och ett lösenord som skickas i förväg till de som skickade MLAT-förfrågan. .sql-filen kopieras till den krypterade enheten tillsammans med en lista på de enhetsanvändare (JID) som efterfrågades.

Listan med bifogade filer sparas till en fil medan data bearbetas och den filen går igenom en andra process som kopierar varje bifogad fil till den krypterade enheten.

Efter att stegen som beskrivs i det här avsnittet har gåtts igenom är MLAT-exporten klar och kan skickas till det begärande landet.

BILAGA A

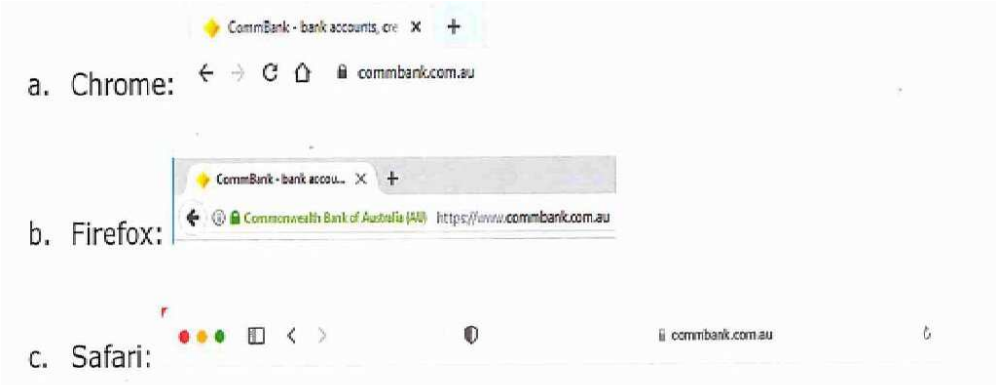
A.1 Kryptering med offentlig nyckel

1. Kryptering innebär att information kodas så att den inte kan läsas av någon som saknar medlen för att avkryptera den. Kryptering med offentlig nyckel är en krypteringsmetod där två olika nycklar, den ”offentliga” och den ”privata”, används för att kryptera och avkryptera information. De två nycklarna hör ihop matematiskt så att information som har krypterats med den ena bara kan avkrypteras med den andra. Samma nyckel kan inte användas till att kryptera och sedan avkryptera samma information. Det innebär att information som har krypterats med den offentliga nyckeln är säker så länge som den privata nyckeln är skyddad. Den är oläslig för alla som inte har den privata nyckeln.

2. Kryptering med offentlig nyckel har många tillämpningsområden och är vanligt på internet. TLS (Transport Layer Security) är ett exempel på kryptering med offentlig nyckel.

3. TLS är en ofta använd säkerhetsmekanism som skyddar data som skickas till många webbplatser. Om den används visas ett litet hänglås i webbläsarens adressfält. Hänglåset kan ofta ses på webbplatser som tillhör t.ex. banker, webbaserad e-post och Google, vilket gör att användare kan vara säkra på att informationen som de skickar till webbplatsen är säker. Den här formen av transportsäkerhet gör också att data som skickas mellan en server och en klient inte kan avlyssnas av en tredje part under överföringen. Alla webbplatser som du besöker där hänglåsikonen visas i adressfältet på webbläsaren använder kryptering med offentlig nyckel för att skydda dina data.

4. Exempel på hur hänglåsikonen visas på webbplatsen för Commonwealth Bank of Australia i webbläsarna Chrome, Firefox och Safari:



5. Eftersom kryptering med offentlig nyckel kräver mycket processorkraft används den i allmänhet inte för att kryptera stora mängder data. Ett annat alternativ är att använda en symmetrisk nyckel, den så kallade sessionsnyckeln i TLS, för att kryptera data och sedan använda kryptering med offentlig nyckel för att kryptera själva nyckeln. Den krypterade nyckeln infogas sedan i krypterade data. Innehavaren av den privata nyckeln kan sedan avkryptera den symmetriska nyckeln och använda den till att avkryptera data.

A.2 Hash

6. En ”hashfunktion” är ett matematiskt förhållande där indata av godtycklig storlek” (det så kallade ”meddelandet”) bearbetas till utdata med fast storlek (”sammandrag av meddelande” eller ”hashvärde”). Vissa hashfunktioner kan användas för kryptering. Bland dessa finns algoritmfamiljen Secure Hash Algorithm 2 (”SHA-2”) som utvecklades av USA:s National Security Agency and publicerades av USA:s Department of Commerce som en del av

FIPS (Federal Information Processing Standards). De är offentligt tillgängliga på internet.

7. SHA-2-algoritmerna kan användas för att verifiera integriteten för data (däribland datorfiler) eftersom det är väldigt osannolikt att två olika meddelanden ger samma hashvärde som utdata. Det gäller även om ett meddelande har förändrats, vilket ger ett annorlunda meddelande. Det här förklaras i FIPS Publication 180-4:

   > *De hashalgoritmer som specificeras i den här standarden betecknas som säkra eftersom det, för en algoritm, är matematiskt omöjligt att 1) hitta ett meddelande som motsvarar ett visst hashvärde eller 2) hitta två olika meddelanden som resulterar i samma hashvärde. Alla förändringar av ett meddelande kommer med mycket hög sannolikhet att resultera i ett annat hashvärde. Det i sin tur leder till att verifieringen misslyckas...*

8. Algoritmen MD5 (Message Digest 5) anses inte längre lämplig för krypteringsändamål, men den används ofta för sådana syften som att skapa checksum-värden för att kontrollera att data inte oavsiktligt har blivit korrupta. Den representeras ofta med 32 hexadecimala tecken (siffrorna 0 till 9 och bokstäverna A till F).

9. En hash är konstruerad för att vara en irreversibel process, eftersom den producerar ett hashvärde med fast längd för meddelandeindata av en given längd. En enkel liknelse är att ta summan av två tal (t.ex. 23 + 78 = 101). Det är extremt svårt att fastställa exakt vilka två tal som användes för att komma fram till utdata (101), men det går att arbeta sig igenom varenda tänkbar kombination för att identifiera de kombinationer som ger den summan. Processen kallas ”brute force” och varje hittad kombination är en ”hash-kollision”. Om ekvationen som gav summan görs ännu mer komplicerad – t.ex. genom att man använder multiplikation, subtraktion och division förutom den ursprungliga additionen – skulle det bli mycket svårare och ta längre tid att identifiera sifferkombinationerna. Det skulle också leda till en mindre underuppsättning av tänkbara ursprungliga indatavärden.

10. Eftersom hashfunktionerna är så komplicerade ägnar matematiker och kryptoanalytiker mycket tid åt att försöka omvända funktionen för att bevisa att det verkligen är en envägsfunktion. Det enda sättet att identifiera ett ursprungligt indatameddelande från ett hashvärde är därmed att genomföra en brute force-process, och det är en alltför komplicerad uppgift för att vara praktiskt genomförbar.

A.3 ANØM-PLATTFORMEN

11. Kommunikationsnätverket ANØM ger end-to-end-kryptering av meddelanden i ett slutet nätverk mellan ANØM-användare. Att nätverket är slutet innebär att den end-to-end-krypterade kommunikationen bara kan ske mellan ANØM-användare. Det är en prenumerationsbaserad tjänst som kräver att man köper smartphones som är särskilt konfigurerade att kommunicera på ANØM, och bara telefoner som har konfigurerats på rätt sätt kan användas för kommunikationen.

12. FBI anlitade tredje parter för att konfigurera och driva ANØM, inklusive att vara primärt ansvariga för att utveckla applikationen samt att hantera och underhålla infrastrukturen för funktionerna i ANØM (ANØM-administratörer).

A.3.1 End-to-end-kryptering

13. End-to-end-kryptering är en typ av kryptering där meddelandenas innehåll bara kan läsas av de parter som deltar i kommunikationen, och ofta används kryptering med offentlig nyckel i sådana sammanhang.

14. Med end-to-end-kryptering säkerställer man att innehållet i det ursprungliga

meddelandet inte kan läsas av leverantören av meddelandetjänsten eller någon annat system eller nätverk från tredje part som meddelandet skickas genom. Meddelandetjänster med end-to-end-kryptering finns på stora plattformar som t.ex. Apple iMessage, Facebook Messenger och WhatsApp, samt meddelandeplattformen Telegram.

15. Utan end-to-end-kryptering kan andra parter än avsändaren och de avsedda mottagarna se och läsa det ursprungliga meddelandet. Exempel på tillämpningar där end-to-end-kryptering normalt inte används är t.ex. e-posttjänster, där tjänsteleverantören kan läsa e-postmeddelanden som sparats i en personlig ”inkorg”, SMS och fax, där nätverksleverantören som tillhandahåller infrastrukturen mellan parterna också kan läsa innehållet i meddelandet när det passerar genom dess infrastruktur. Ett vykort som skickas via traditionell posthantering är ett icke-tekniskt exempel på hur vem som helst kan läsa meddelandet på dess väg från avsändaren till mottagaren.

16. ANØM använder XMPP (Extensible Messaging and Presence Protocol) för kommunikationen mellan deltagarna i ANØM. XMPP är erkänt av branschen och är ett offentligt tillgängligt ramverk som kan modifieras, anpassa och byggas ut efter behov.

17. Med ANØM kan deltagarna skicka end-to-end-krypterade meddelanden – bestående av text och bilagor som t.ex. bilder, videor, anteckningar och korta röstmeddelanden – till andra ANØM-användare.

18. Varje användare i ANØM identifieras med en unik identifierare (användar-ID), som tekniskt kallas för en Jabber Identifier (JID). Från början hade detta användar-ID formen av 6 alfanumeriska tecken (till exempel ”aab2c3”) och det genererades automatiskt från enhetens IMEI-nummer (International Mobile Equipment Identity number).

19. Enhetens IMEI-nummer kombinerades med en fast uppsättning tecken (en så kallad ”saltsträng”) för att skapa ett indatavärde. Indatavärdet genomgick en hashprocess i algoritmen MD5. De sista sex tecknen i det hashvärde som genererades var enhetens användar-ID och användarens lösenord var hela hashvärdet. Processen genomfördes automatiskt av ANØM-appen som använda detta användar-ID och lösenord för automatisk autentisering mot ANØM-servrarna.

20. Det är möjligt att beräkna användar-ID-t för ett visst IMEI eftersom MD5-processen, inklusive saltvärdet, är känd för AFP.

A.4 Portalen

21. Portalen var en webbplats som lanserades i januari 2021 av ANØM-operatören. Där kunde man hantera slutanvändares konton, enheter och abonnemang.

22. Åtkomst till portalen var generellt begränsad till återförsäljare av enheter och ANØM-administratörer, och den hade funktioner för att konfigurera nya enheter så att de skulle fungera i ANØM, ta bort en enhet eller genomföra en fjärrensning av en enhet. Åtkomsten till portalen skyddades av ett användarnamn och ett lösenord, och användaren var också tvungen att ansluta via en VPN-anslutning (Virtual Private Network) som bara var tillgänglig för dem som hade auktoriserats av ANØM-operatören.

23. På grund av förändringar i operativsystemet Android gick det från december 2020 inte längre att använda IMEI-numret till att automatiskt generera användar-ID. Formatet på användar-ID ändrades därför så att det genererades automatiskt i portalen. I den här processen består användar-ID av två slumpmässigt valda ord på engelska som satts samman. ”LITTLE” och ”FISH”

skulle t.ex. ge användar-ID:t ”LITTLEFISH”.

A.5 Enheter

24. Enheter som användes på ANØM bestod av smartphones som körde operativsystemet Android och som:

    a. Hade registrerats i en privat MDM-applikation (Mobile Device Management) som konfigurerades och kontrollerades av ANØM-administratörer. Med MDM-applikationen kunde administratörerna tillhandahålla eller begränsa vissa funktioner på enheterna.

    b. Hade den specialbyggda end-to-end-krypterade kommunikationsapplikationen (appen) installerad. Appen var bara tillgänglig på enheter som hade registrerats i MDM-applikationen.

25. Enheterna förbereddes innan de levererades till användaren. Förberedelserna innebar att den programvara som krävdes för att enheten skulle kunna komma åt och kommunicera via ANØM installerades och konfigurerades. Bilagorna B och C är två dokument som gavs ut av ANØM-administratörerna som riktlinjer för att förbereda enheterna. Förberedelserna omfattade:

    a. Installation av rätt version av operativsystemet, om det behövdes.

    b. Vid behov installation av ett aktivt SIM-kort (Subscriber Identity Module), som normalt hade köpts in från en av följande internationella leverantörer av mobilnätverk: Jersey Telecom (JT), Telefonica eller POD Group. SIM-korten behövde inte registreras i enhetsanvändarnas namn.

    c. Installation av MDM-applikationen och registrering av enheten i MDM.

    d. När registreringen i MDM var klar installerades ANØM-appen automatiskt på enheten.

    e. Om den installerade ANØM-appen var av en version som hade släppts senare än i januari 2021 behövde man använda portalen för att få ett automatiskt genererat användar-ID och lösenord som unikt kunde identifiera enheten i ANØM. Det krävdes inte för tidigare versioner av ANØM-appen, enligt förklaring i punkt 41.

    f. För de enheter som inte automatiskt kunde generera ett användar-ID och lösenord behövde ANØM-appen konfigureras med användar-ID och lösenord.

26. Slutanvändaren betalade en abonnemangsavgift till återförsäljaren för den period som han eller hon vill vara en aktiv användare av plattformen.

27. För de flesta ANØM-användare fanns det inga andra sätt att kommunicera på enheterna. Traditionella funktioner på mobiltelefoner, som t.ex. röst- eller videosamtal, SMS, appar för sociala medier, internetsurf och e-posttjänster, kunde inte användas på de tillhandahållna enheterna eftersom det förhindrades av MDM-inställningarna.

28. Den 8 juni 2021 hade bara 73 av ungefär 12 500 enheter förmågan att ringa i traditionell bemärkelse eller att surfa på internet via den installerade ToR-webbläsaren (The Onion Router). Det var tillåtet i MDM-inställningarna för en specifik grupp användare, så kallade COPE-användare (”Corporate Owned, Personally Enabled”).

29. Eftersom ANØM kördes på ett slutet nätverk, använde en privat app och krävde specifika

autentiseringsuppgifter gick det inte att oavsiktligt skicka ett meddelande via plattformen från en normal mobiltelefon.

30. Varje mobil enhet kan unikt identifieras genom dess IMEI-nummer. IMEI-numret är ett nummer med 15 siffror (14 siffror plus en kontrollsiffra) som ger information om enhetens märke, modell och serienummer. IMEI-numret är ofta tryckt på enheten.

31. De första 8 siffrorna i IMEI-numret kallas för TAC (Type Allocation Code) och identifierar enhetens märke (tillverkare) och modell. De efterföljande 6 siffrorna är enhetens serienummer, och den sista siffran är en kontrollsiffra som beräknas med Luhn-algoritmen.

32. IMEI-numret 358503082383242 består t.ex. av:

    a. TAC-numret 35850308, som identifierar IMEI-numret som tillhörande en Samsung Galaxy Note 8 och

    b. serienumret 238324 och

    c. kontrollsiffran 2.

33. Medan ANØM var i drift tillhandahölls enheter av olika märken och modeller. De vanligaste var Google Pixel, Samsung Galaxy och Xiaomi. Alla enheter körde en version av operativsystemet Android.

A.5 Nätverksanslutning till plattformen

34. Enligt beskrivningen i punkt 42.b.ii kan enheter tillhandahållas till slutanvändaren med ett internationellt SIM-kort som möjliggör internationell roaming över ett mobilnätverk i det land där enheten används. Slutanvändaren kan också köpa ett eget SIM-kort från en leverantör av telekommunikationstjänster.

35. Eller så kan enhetsanvändaren ansluta sig till ett tillgängligt WiFi-nätverk istället för att använda mobildata.

A.6 MDM-komponenten

36. För driften av ANØM användes två MDM-applikationer med tillhörande infrastruktur, MobileIron and FieldX. Båda MDM-applikationerna har liknande kärnfunktioner enligt beskrivningen nedan.

37. MDM-komponentens roll var att tillhandahålla och verkställa vissa enhetsfunktioner genom tillämpning av en MDM-policy som angavs av ANØM-administratörerna. Sådana funktioner kunde t.ex. vara att:

    a. Initiera en ”fjärrfabriksåterställning” av en enhet, vilket innebar att alla data raderades från enheten, inklusive appar.

    b. Verkställa en lösenordspolicy för enheten genom att se till att lösenordet uppfyllde vissa krav på komplexitet, t.ex. minsta längd och teckenuppsättningar.

    c. Förhindra att ”utvecklaralternativ” aktiverades, vilket hade kunnat göra det möjligt för en användare att aktivera USB-felsökning eller andra alternativ som kunde användas för att kringgå begränsningar för enheterna eller på andra sätt manipulera enheten.

    d. Upprätthålla en säker startinläsare som säkerställde att bara det operativsystem för mobila enheter som hade godkänts för plattformen fick köras, vilket därmed upprätthöll enhetens integritet och säkerhet.

e. Förhindra installation av ej betrodda eller ej godkända applikationer och därmed säkerställa att endast applikationer som var tillgängliga via MDM-komponenten för ANØM kunde installeras och köras på enheten.

f. För FieldX MDM: se till att ANØM-appen uppdaterades automatiskt.

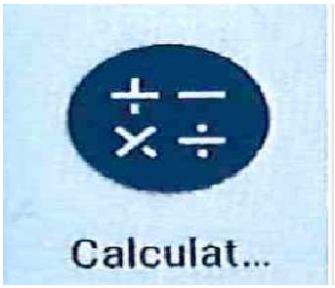
g. Rapportera information om enheten med jämna mellanrum, t.ex. enhetens unika IMEI-nummer, efterlevnad av MDM-policyn, enhetens startinläsare och version av operativsystemet samt enhetens status, t.ex. batterinivå och ledigt minnesutrymme.

38. MDM-komponenten använde funktioner som är en del av operativsystemet Android på enheten, kommunicerade med MDM-servrar för att rapportera enhetens status och hämtade policyer som skulle verkställas på enheten.

A.7 ANØM-applikationen

39. ANØM-applikationen (appen) finns på enheten men är dold i form av en fungerande kalkylatorapp. Varken appikonen eller kalkylatoretiketten avslöjar applikationens verkliga syfte. Om enheten undersöks av en ovetande användare finns det inget som visar att det finns en applikation för krypterade meddelanden på enheten.

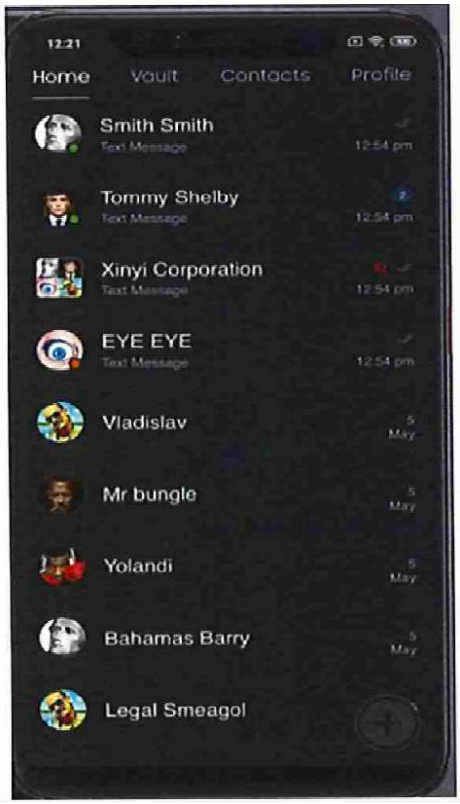
40. Här är ett exempel på appikonen som den såg ut på vissa enheter (ikonens utseende varierade beroende på version av operativsystemet):



41. När appen startas ser användaren ett gränssnitt som fortfarande ser ut som en kalkylator:

42. Kalkylatorn fungerar som förväntat, dvs. användaren kan mata in matematiska funktioner och det korrekta resultatet matas ut.

43. Men om användaren anger en hemlig PIN-kod och sedan håller ned lika-med-tecknet (=) visas den verkliga plattformsapplikationen:



44. Förutom PIN-koden för åtkomst till appen finns även en PIN-kod för nödlägen. Om den senare anges tillsammans med en nedtryckning av lika-med-tecknet raderas all information från appen.

45. PIN-koden för nödlägen kan t.ex. ges till en obehörig användare av enheten om ägaren tvingas eller frivilligt går med på att öppna appen. Appen öppnas som vanligt, men alla data raderas från appen. Ett exempel är om brottsbekämpande myndigheter tar enheten i beslag och kräver att få veta PIN-koden för åtkomst. Den behöriga användaren kan då istället uppge PIN-koden för nödlägen och därmed få det att se ut som att han eller hon samarbetar med utredningen, men i

själva verket raderas eventuellt bevismaterial.

A.7.1 ANØM-applikationsattribut

A.7.1.1 Identifierare för användare

46. Varje användare av plattformen identifieras med ett unikt användar-ID. Bara en enhet vid varje given tidpunkt kunde komma åt ANØM med ett visst användar-ID.
När användar-ID:t och lösenordet hade angetts i appen uppdaterade appen automatiskt lösenordet som var associerat med det användar-ID:t i ANØM. Det uppdaterade lösenordet sparades av appen för senare inloggningar, men det visades aldrig för och var inte känt av användaren som angav värdena. Försök att logga in på en annan enhet med tidigare lösenordet och användar-ID:t misslyckades, och lösenordet behövde återställas till ett känt värde för att det skulle lyckas.

A.7.1.2 Användarens visningsnamn

47. Enhetens användare kunde ange ett ”visningsnamn” (som också kallas smeknamn eller alias), som kunde ändras när användaren ville. Det förändrade inte deras användar-ID på plattformen. Det här liknar ”Från”-namnet som visas i e-postmeddelanden, som normalt skiljer sig från e-postadressen som ofta är användarnamnet.

A.7.1.3 Valvet

48. I valvet kan användaren på ett säkert sätt lagra anteckningar och bilder på enheten. Dessa data krypteras så att de bara kan kommas åt från enheten, och inga data i valvet skickas vidare om inte användare inkluderar dem som en bilaga till ett meddelande.

49. Anteckningar som sparas i valvet kan innehålla en rubrik samt brödtext eller en punktlista. Bilder som sparas i valvet eller som tas med enhetens kamera kan också infogas i anteckningar.

A.7.1.4 Meddelanden

50. En användare kan skicka ett end-to-end-krypterat meddelande till en annan ANØM-användare, förutsatt att de känner till mottagarens användar-ID.

51. En användare kan också skicka end-to-end-krypterade meddelanden till en grupp av ANØM-användare, och varje användare i den gruppen kan se de andra medlemmarna i gruppen. Gruppen kan ha en etikett som fungerar som ett namn på gruppen och som kan anges av gruppadministratören – normalt den som skapade gruppen – eller andra medlemmar som har fått administratörsbehörigheter för gruppen. Det här fungerar på ett liknande sätt som gruppchattar i andra meddelandeapplikationer som WhatsApp, Signal, Telegram och Facebook Messenger.

52. Ett meddelande, antingen till en enda användare eller till en grupp av användare, kan bestå av ett textmeddelande, en bild (t.ex. ett foto som togs med kameran på enheten), en video som spelats in med kameran på enheten, ett kort röstmeddelande (PTT – push-to-talk) eller en anteckning från enhetens valv.

53. Meddelanden kan vara på olika språk. För att kunna stödja olika språks teckenuppsättningar kan datorapplikationer använda Unicode som ett sätt att representera symboler och text från de flesta av världens skriftsystem. Unicode har ett unikt nummer för varje tecken, oavsett plattform, enhet, applikation eller språk. Det görs genom att tecken uttrycks som ett kodnummer och inte som glyfer. De arabiska tecknen ”ا ب و” skulle t.ex. representeras som ”\u0627\u0628\u0648” i Unicode. Så kallade ”emojis” kan också uttryckas som Unicode-värden. T.ex. är ”\u1F603” Unicode-värdet för emojin ”😃”. Sådana Unicode-värden måste konverteras tillbaka till de rätta tecknen för att de ska kunna läsas.

Applikationer kan tolka Unicode-värdet och visa tecknen istället för koden.

54. Det går att citera ett meddelande genom att välja det i en konversation och trycka på svara-knappen, eller vidarebefordra det till andra mottagare genom att välja det och trycka på dela-knappen. När det görs kan deltagarna i konversationen visuellt se att meddelandet har citerats eller vidarebefordrats eftersom det visas som ett citerat block i det skickade meddelandet.

55. Till skillnad från andra meddelandeapplikationer som t.ex. WhatsApp eller Telegram hade ANØM-appen inte några indikatorer för att ange om ett meddelande hade tagits emot eller lästs av mottagaren.

56. Möjlighet att ändra tonhöjd

    57. Avsändaren av ett ljudmeddelande kan justera tonhöjden på inspelningen innan den spelas in, antingen upp (alternativet ”Helium” i appen) eller ned (alternativet ”Jellyfish” i appen), vilket maskerar det verkliga ljudet i avsändarens ljudklipp för mottagaren. Avsändaren kan också välja att inte ändra tonhöjd.

A.7.1.5 Självförstörande meddelanden

58. Avsändaren av ett meddelande av någon av de typer som beskrivs ovan kan också ange en ”självförstörandetimer” för det meddelandet. Genom att ange en sådan tid tas meddelandet bort från alla enheter som har mottagit det när den inställda tidsperioden löper ut.

A.8 Data spelas in från plattformen

59. ANØM-appen hade en funktion som innebar att när ett meddelande skickades så skickade appen automatiskt en dold kopia av meddelandet till ett ghostanvändar-ID, ”bot”. Den här processen var inte synlig för den användare som skickade meddelandet, och användaren visste inte heller om att processen ägde rum.

60. Processen med den automatiska dolda kopian ledde till att en kopia av meddelandet krypterades och skickades till ghostanvändar-ID:t ”bot”. Datorer med en applikation som var kompatibel med plattformen tog emot de krypterade meddelanden som skickades till användar-ID:t ”bot”.

61. Processen för det var precis likadan som plattformens normala beteende när ett meddelande skickades, med undantag för att meddelanden som skickades till ghostanvändar-ID:t inte var synliga för de andra deltagarna i kommunikationen.

62. I avsnitt 1.5 finns ett diagram som visar meddelandeflödet och krypteringsprocessen för ett hypotetiskt meddelande som skickas från Alice till Bob, inklusive den dolda kopian och krypteringen för ghostanvändar-ID:t ”bot”.

63. A.8.1 Innehåll i meddelanden
64. Meddelanden som skickas med plattformen har oftast följande, eller en kombination av följande, attribut. De är synliga för både avsändare och mottagare:

    a. Självförstörelsetid – Anges av avsändaren när meddelandet skickas och definierar hur länge ett meddelande finns kvar innan det tas bort automatiskt från båda enheterna när tiden har löpt ut. Tiden syns på både avsändarens och mottagarnas enheter längst ned i varje meddelande. Den kan anges till 30 sekunder, 5 eller 30 minuter, 1 eller 12 timmar eller 1, 3 eller 7 dagar.

    b. Avsändare – användar-ID och visningsnamn för den avsändande enheten.

    c. Mottagare – Mottagarna av ett meddelande kan identifieras genom att visa deltagarna i

meddelandetråden i fråga. Liksom i andra populära chattapplikationer som t.ex. WhatsApp, Telegram och Facebook Messenger visas de som separata poster i en meddelandelista.

d. Innehåll – Meddelandets innehåll som kan bestå av text eller en bilaga som ljud, bild, video eller anteckning.

e. Tid – Tid och datum i GMT (Greenwich Mean Time) enligt den avsändande enheten när ett meddelande skickades. Det visas på enheten i den inställda tidszonen. Ett meddelande som skickades den 10 juni 2020 kl. 11. 00 Perth-tid skulle t.ex. ha datum och tid kl. 03. 00 den 10 juni 2020 GMT. En enhet i Sydney skulle visa den tiden som kl. 13. 00 den 10 juni 2020. Enheter med ett aktivt SIM-kort synkroniserade sin tid via NTP (Network Time Protocol) till det operatörsnätverk som den var ansluten till.

    i. Se avsnitt 8.6.1 för information om tidszonsavvikelser.

A.8.2 Metadata för meddelanden

65. Meddelanden som skickades via ANØM innehöll ytterligare metadata som inte var synliga varken för avsändaren eller mottagaren av ett meddelande. Vissa av fälten inkluderades för att vara till hjälp för brottsbekämpande myndigheter. På grund av förändringar och tillägg skickades inte alla metadatafälten nedan med varje meddelande:

    a. Ett unikt meddelande-ID – Ett UUID (Universally Unique Identifier) som genererades automatiskt av den avsändande enhetens applikation då ett meddelande skickades. Det visades varken för avsändaren eller mottagarna av ett meddelande. Det här är en komponent i XMPP-ramverket.

    b. IMEI – På enheter som körde operativsystemet Android i version 9 eller lägre inkluderades IMEI-numret som metadata med varje meddelande för användning av brottsbekämpande myndigheter.

    c. MCC/MNC – Enheter med ett aktivt SIM-kort som var registrerade på ett mobilt kommunikationsnätverk skickade den MCC-kod (Mobile Country Code) och den MNC-kod (Mobile Network Code) som enheten för närvarande var uppkopplad mot. De siffrorna skickades med som metadata med meddelandet för användning av brottsbekämpande myndigheter.

    d. Platsinformation – Efter en uppdatering av appen i april 2020 försökte appen ta fram platsinformation via Androids API Location Manager. Om det gick att fastställa en plats inkluderades latitud, longitud, noggrannhet och tidpunkten för platsbestämningen som metadata med meddelandet för användning av brottsbekämpande myndigheter. Ibland kunde appen inte hitta en fullständig och korrekt GPS-plats. När det hände inleddes den hämtade GPS-punkten ofta med siffrorna 39,0 och pekade på en plats utanför Fijis kust i södra Stilla Havet.

    e. Tonhöjdsjustering för ljud – Om meddelandet innehöll en ljudbilaga inkluderades metadata som angav värdet för tonhöjdsjusteringen för användning av brottsbekämpande myndigheter.

    f. Citerade eller vidarebefordrade meddelanden – Om ett meddelande innehöll ett citat eller var ett vidarebefordrat meddelande innehöll det nya innehållet i meddelandet det citerade eller vidarebefordrade innehållet, som också kunde innehålla information som användar-ID för den ursprungliga avsändaren och tidpunkten för det ursprungliga meddelandet. Det här var en funktion i ANØM-appen. Andra meddelandeapplikationer

som t.ex. WhatsApp, Signal, Telegram och Facebook Messenger har en liknande funktion för att citera och vidarebefordra meddelanden.

A.9 Autentisering och integritet

66. Eftersom ANØM-appen uppdaterade lösenordet vid den första inloggningen förhindrade den enheter från att autentisera och skicka meddelanden i ett annat ANØM-användar-ID:s namn. Mer information kommer i en framtida bilaga.

67. Fram tills förändringen av formatet för användar-ID i december 2020 var användar-ID direkt relaterat till enhetens IMEI-nummer, vilket ytterligare begränsade möjligheterna att skicka ANØM-meddelanden.

68. Om en enhet ”fabriksåterställdes”, antingen via MDM eller direkt på enheten, togs alla data och applikationer – även MDM-appen och plattformsappen – bort från enheten.

69. Om PIN-koden för nödlägen angavs togs alla data, inklusive sparade inloggningsuppgifter, bort från appen. Därmed kunde användaren inte komma åt eller kommunicera via ANØM.

70. Om någon av dessa processer genomfördes behövde användar-ID och lösenordet återställas innan enheten kunde användas för att komma åt ANØM igen. Vid en fabriksåterställning behövde enheten ometableras.

ORDLISTA

- **AES-kryptering**: Symmetrisk kryptering (med enkel nyckel) som användes för den andra delen av återkrypteringen av inhämtade data.
- **ANØM**: En kommunikationsplattform med end-to-end-kryptering som använde särskilda mobiltelefonenheter med en anpassad, installerad meddelandeapplikation för att kommunicera inom ett slutet nätverk.
- **API (Application Programming Interface)**: Ett programvarugränssnitt som oftast används med dator-till-dator-interaktion där en klientdator initierar en förfrågan som besvaras av serverdatorn som kör API:t, vilken normalt returnerar data till den klientdator som skickade förfrågan.
- **AWS GovCloud**: Amazon Web Services molninfrastruktur där webbapplikationen Hola iBot och data relaterade till Operation Trojan Shield lagrades.
- **Startinläsare**: Den första programvara som körs på en mobiltelefon när enheten slås på eller startas om. Den initialiserar maskinvaran och läser in operativsystemet, t.ex. Android.
- **Ärenden**: Kallas också syndikat. Det här är den centrala komponenten för relationer i databasen iBot_dec.
- **Skillnadsdump**: Nya eller ändrade data mellan två MySQL-databasdumpar. Det är metoden för hur det tredje landet tog fram nytt innehåll ur hela databasen då det skickade nya datapaket.
- **Elastic Compute Cloud (EC2)**: Datorresurser som ägs av AWS och som kan hyras för att köra datorprogram.
- **End-to-end-kryptering**: Kryptering där data krypteras mellan två ändpunkter och där endast de ändpunkterna har förmåga att avkryptera data. Data kan inte avkrypteras av de servrar och nätverk som data passerar mellan de två ändpunkterna.
- **XMPP (Extensible Messaging and Presence Protocol)**: XMPP är ett öppet standardprotokoll för snabbmeddelanden som möjliggör chattar mellan flera parter. Det har stöd för multimedia som röst, bilder och video. Vem som helst kan köra en egen XMPP-server och nätverk och bygga vidare på det befintliga ramverket.
- **Ghostanvändar-ID (”bot”)**: Det användar-ID till vilket ANØM-applikationen på mobila enheter skickade en dold kopia av alla meddelanden som skickades från den enheten.
- **GPG (GnuPG)**: Möjliggör kryptering av data och signering av kommunikation.
- **Google Compute Engine**: En tjänst från Google Cloud som gör det möjligt att skapa och köra virtuella datorer i Google Cloud.
- **Hash (MD5, SHA-2)**: En hashfunktion är en matematisk process där indata, ”meddelandet”, bearbetas till ett ”sammandrag av meddelandet” eller ett hashvärde med fast längd. Det anges ofta som hexadecimala tecken med siffrorna 0 till 9 och bokstäverna A till F. Hashfunktioner används ofta för dataverifiering genom att identifiera om data har förändrats, eftersom det är mycket osannolikt att två olika ”indatameddelanden” resulterar i samma hashvärde.
- **Hola iBot**: Den anpassade webbapplikation som skapades och drevs av FBI i San Diego och som fungerade som granskningsplattform för alla data som togs emot från plattformen ANØM.

- **iBot_dec**: Databasen som skickade data till granskningsplattformen Hola iBot. Innehåller data som samlades in på plattformen ANØM och skickar den för granskning.
- **iBot_enc**: Den tillfälliga databas där nya datapaket förvarades när nya data togs emot från servern i det tredje landet.
- **Servern Ingestion-1 (I1)**: Den AWS GovCloud EC2 som körde inmatningsprocessen (avsnitt 9), sparade filer som bifogats till meddelanden och skickade data till databasen iBot_dec.
- **IMEI (International Model Equipment Identifier)**: Ett 15-siffrigt nummer som tilldelas en mobil enhet och som kan användas som identifierare. Det består av ett 8-siffrigt TAC-nummer (Type Allocation Code) som visar enhetens märke och modell, ett 6-siffrigt serienummer och en kontrollsiffra (sista siffran) som beräknas med Luhn-algoritmen.
- **Platsinformation**: Information som identifierar en plats (som kan vara en region eller ett område). Den består normalt av värden för latitud och longitud samt en tidsstämpel i UTC för den tid då platsen fastställdes. Platsen kan fastställas med GNSS (Global Navigation Satellite Systems) som t.ex. GPS eller GLONASS, eller fastställas utifrån information om närliggande mobilmaster och WiFi-åtkomstpunkter.
- **MCC (Mobile Country Code)**: MCC-koden identifierar unikt ursprungslandet för mobilabonnenten och är de tre första siffrorna i IMSI-numret (International Mobile Subscriber Identity) som lagras på SIM-kortet. Australien har t.ex. MCC-värdet 505.
- **MDM (Mobile Device Management)**: En programvaruapplikation som består av en mobil enhetskomponent och en serverkomponent som ofta används för att tillämpa vissa funktioner på enheter, så kallade policyer, för att förbättra enheternas integritet, säkerhet och användarvänlighet. MDM-applikationer har ofta också möjligheten att tömma enheter på information på distans.
- **MNC (Mobile Network Code)**: MNC-koden består av två eller tre siffror som identifierar mobilabonnentens mobilnätverk. Det är de två eller tre siffrorna som följer på MCC-koden som tillsammans utgör IMSI-numret (International Mobile Subscriber Identity) som lagras på SIM-kortet. Följande exempel kommer från australiska mobilnätoperatörer (inte ett heltäckande exempel): Telstra har 01, Optus har 02och Vodafone har 03.
- **MySQL-dump**: En logisk säkerhetskopia av alla tabeller, inklusive innehåll, i en MySQL-databas.
- **Nytt datapaket**: Ett paket med nya data hämtade från ANØM-plattformen som skickades av det tredje landet till I1-servern.
- **Portal**: En webbplats som nås via internet med en VPN-anslutning (Virtual Private Network). Man loggar in med ett giltigt användarnamn och lösenord från ANØM-administratörerna och kan då hantera ANØM-slutanvändares enheter, konton och användar-ID:n.
- **Proxy**: En server som fungerar som ett relä för all nätverkstrafik mellan två datorer eller servrar.
- **Kryptering med offentlig nyckel**: Ett system för kryptering och avkryptering där ett par matematiskt relaterade nycklar används för att kryptera och avkryptera innehåll. Den ”offentliga” nyckeln kan användas för att kryptera innehåll som bara den ”privata” nyckeln kan avkryptera, och tvärtom. Samma nyckel kan inte användas för att avkryptera innehåll som krypterades med den.
- **RAM**: Tillfällig lagring i en dator. T.ex. lagrades alla tillfälliga datastrukturer i RAM-minne

inför inmatningen.

- **RSA-kryptering:** En typ av PKI-kryptering som delvis användes för återkryptering av inhämtade data.
- **SIM (Subscriber Identity Module)**: SIM-kortet är ett fysiskt integrerat kretskort som lagrar IMSI-numret (International Mobile Subscriber Identity) och dess relaterade autentiseringsnyckel, som används för att unikt identifiera och autentisera en mobilabonnent (slutanvändare) i ett mobilt nätverk. SIM-kortet har också ett unikt serienummer som kallas ICCID (Integrated Circuit Card Identifier) och som kan vara tryckt på SIM-kortet.
- **TLS (Transport Layer Security)**: En implementering av kryptering med offentlig nyckel som ofta används för att säkra information som skickas till och från webbplatser, t.ex. banker, e-post och sökmotorer på internet. Man kan se att det används genom att det visas en bild av ett låst hänglås i webbläsarens adressfält. TLS kan också användas för att göra annan kommunikation säker, t.ex. snabbmeddelandeapplikationer och VoIP-kommunikation (Voice over Internet Protocol).
- **Unicode**: Unicode är en metod för att representera symboler och text från de flesta av världens skriftsystem. Det görs genom att tecken uttrycks som ett nummer och inte som glyfer. ”Emojis” är en vanlig typ av glyf som skulle uttryckas med Unicode-värdet i t.ex. meddelandeapplikationer men som visas för avsändaren och mottagaren som en glyf.
- **USB-felsökning**: Möjligheten att ansluta en dator till en mobil enhet via en USB-kabel (Universal Serial Bus) och interagera med operativsystemet i den mobila enheten. Det kan användas till att lägga till eller ta bort data från enheten, läsa loggar eller installera och ta bort applikationer. Det kan också användas till att byta operativsystem på en mobil enhet eller installera processer som körs med höjda behörigheter – så kallad ”rooting”.
- **Användar-ID (JID)**: Ett användarnamn som unikt identifierade en användare på ANØM-plattformen. Från början bestod det av sex tecken hämtade från siffrorna 0 till 9 och bokstäverna A till F, och senare blev det två slumpmässigt valda engelska ord som kombinerades.
- **VPN (Virtual Private Network)**: En nätverksapplikation som används för att kryptera data som skickas över en ej betrodd nätverksanslutning, vanligtvis internet. VPN användes traditionellt till att via en internetanslutning ”utöka” ett privat nätverk, dvs. ett nätverk som inte är åtkomligt om man inte är direkt uppkopplad mot det, exempelvis ett företagsnätverk. På så sätt kan en fjärransluten enhet komma åt webbplatser, filer, data och tjänster som inte är tillgängliga utanför det privata nätverket. VPN kan även användas för att dölja en användares identitet eller deras aktivitet på internet från användarens internetleverantör.
- **XMPP**: *Se Extensible Messaging and Presence Protocol (XMPP)*

A605.834-2021

IT-avdelningen

Anøm

Beskrivning av information i Anom-data

Rapport
Version 2.0
2022-02-28

A605.834-2021

Utgivare
Polismyndigheten
Tfn 114 14
E-post kansli.registrator@polisen.se
www.polisen.se

Produktion Polismyndigheten, 2022-02-28

Diarienr. A605.844/2021

A605.834-2021

Tryck Polisens tryckeri

Sammanfattning

Polismyndighetens IT-avdelning har på uppdrag av Polisens nationella operativa avdelning (NOA) utvecklat och applicerat en metod för hantering av det material som inkommit i operation Trojan Shield som berör dekrypterad information från kommunikationstjänsten Anom.

Det här dokumentet beskriver *innehållet,* bestående av meddelanden, användarkonton och metadata, i den dekrypterade informationen.

För beskrivning av Polisens *hantering* av dekrypterad information från Anom hänvisas till dokumentet ”*A605.844/2021 Beskrivning av Polisens hantering av Anom-data*”

Revisionshistorik

Datum	Version	Kommentar	Avsändare
2021-09-21	1.0	Initial version	IT-avdelningen
2022-02-28	2.0	Större bearbetning med förtydliganden och tillägg av flertalet kapitel.	IT-avdelningen

Innehållsförteckning

SAMMANFATTNING ..... **I**

REVISIONSHISTORIK ..... **I**

INNEHÅLLSFÖRTECKNING ..... **II**

1 INLEDNING **1**

1.1 Bakgrund 1

1.2 Syfte 1

1.3 Hänvisning till OTS Technical Details 1

2 INNEHÅLL I MLAT-EXPORTER **2**

2.1 Databasstruktur 2

2.2 Databasinformation 3

2.2.1 Has_message 3

2.2.2 Ptt_message 4

2.2.3 Image_message & video_message 4

2.2.4 Text_message 5

2.2.5 Product 5

2.2.6 MDM_Data 6

2.2.6.1 Kompletterande MDM-information 7

2.2.7 Roster 7

3 RELEVANTA OBSERVATIONER AV MLAT-MATERIALET **8**

3.1 Produkter 8

3.2 Textformat 8

3.2.1 Vidarebefordrade meddelanden 8

3.2.2 Svar på meddelanden 10

3.2.3 Valvbilagor 11

3.3 Tidsförskjutning 13

3.3.1 Tidszonsdifferens 13

3.3.1.1 Exempel korrigering av tidszonsdifferens 14

3.3.2 Tidzonsförskjutning 16-17 februari 2021 14

3.3.3 Övrig tidsförskjutning 15

3.3.3.1 Exempel övrig tidsförskjutning 15

3.4 Shmid är gemensamt för meddelanden och deras attachments 16

3.5 Platsinformation 16
3.5.1 Tillförlitlighet MCC 16
3.5.1.1 Exempel MCC 16
3.5.2 Misslyckad positionering – Felaktig Longitud 17
3.5.2.1 Exempel misslyckad positionering – Felaktig longitud 17
3.5.3 Misslyckad positionering – Trunkerade koordinater 18
3.5.3.1 Exempel misslyckad positionering – Trunkerade koordinater 18
3.5.4 Positionering visar tidigare känd plats 19
3.5.4.1 Exempel positionering visar tidigare känd plats 19
3.6 MDM och Roster – Statisk information 19
3.7 Användandet av flera enheter 20
3.8 Användaren bot 20
4 KÄLLFÖRTECKNING 21

1 Inledning

1.1 Bakgrund

Sammanlagt har 16 länder ingått i insatsen med namnet Trojan Shield/OTF Greenlight. I Europa har arbetet letts av Sverige och Nederländerna i samarbete med Europol.

Den krypterade plattformen Anom, har använts av kriminella för att kunna planera, koordinera och utföra brott. Plattformen skapades och administrerades i det dolda av FBI. I takt med att liknande tjänster som ”*Encrochat*” och ”*Sky ECC*” upphörde övergick allt fler kriminella aktörer till att kommunicera på denna plattform.

Enligt FBI har över 27 miljoner meddelanden skickats via plattformen av över 200 kriminella nätverk mellan oktober 2019 och juni 2021 [1].

Efter att plattformen avvecklades i juni 2021 har Polismyndigheten av FBI försetts med exporter av meddelanden och annan information från plattformen i enlighet med det ömsesidiga juridiska biståndsavtalet (MLAT) mellan USA och EU.

1.2 Syfte

Dokumentet syftar till att beskriva innehållet av det material som mottagits i MLAT. Den första delen (avsnitt 2) beskriver vad rubrikerna och tabellinnehållet betyder. Den andra delen (avsnitt 3) utgörs av observationer som gjorts vid hantering av materialet, som är relevanta för att förstå det på ett korrekt sätt.

1.3 Hänvisning till OTS Technical Details

I detta dokument finns flertalet hänvisningar till det tekniska dokument som är framtaget av FBI gällande Operationen Trojan Shield (OTS) [2]. Det tekniska dokumentet finns i en engelsk och en svensk version. Hänvisningar till respektive kapitel och eventuellt avsnitt är densamma i både det svenska och det engelska dokumentet. Dessa hänvisningar betecknas med kursiv stil *OTS kap. <kapitel>.<avsnitt> <svensk rubrik>*. Exempelvis: *OTS kap. 8.1 Ärenden/syndikat.*

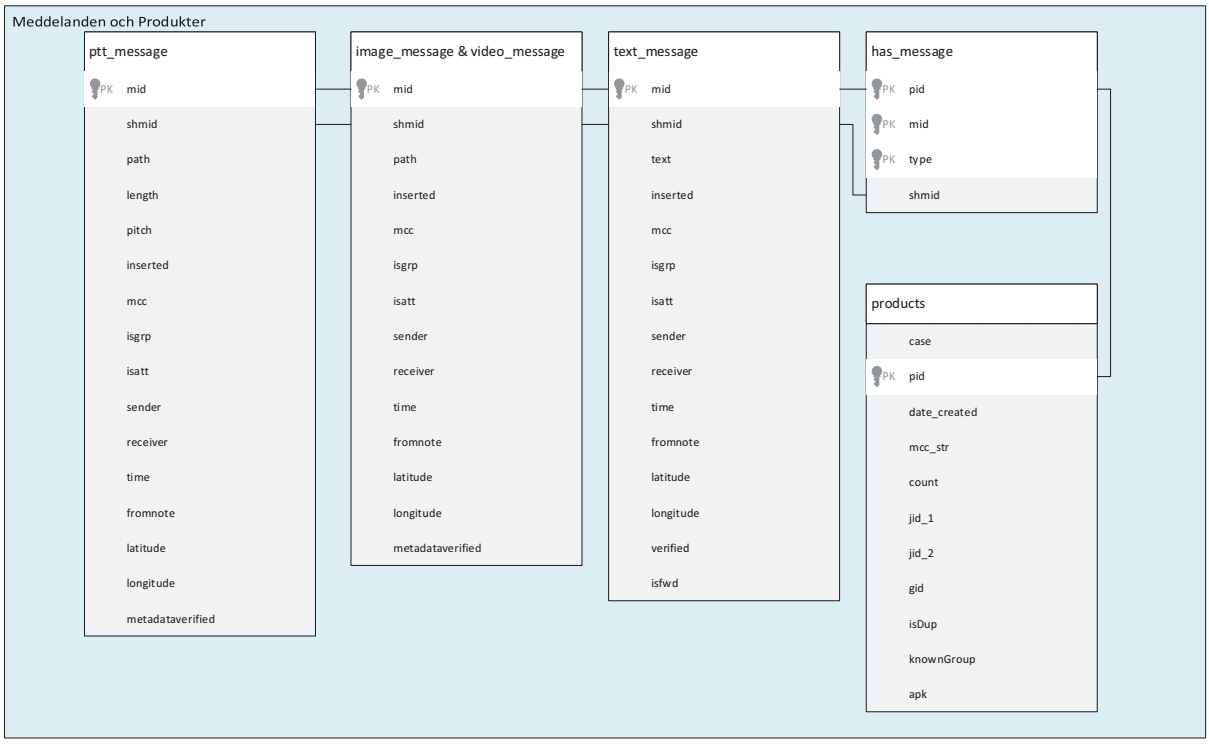
2 Innehåll i MLAT-exporter

2.1 Databasstruktur

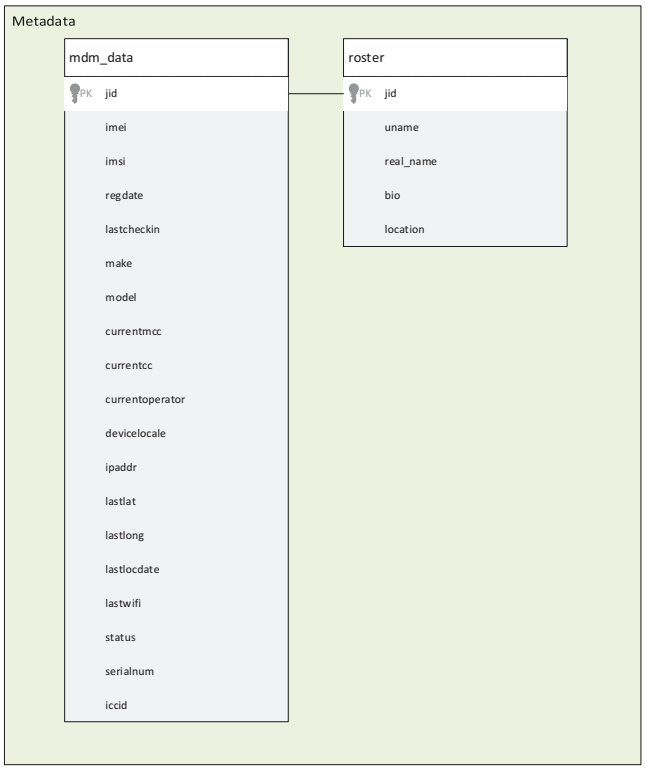
Varje MLAT-export innehåller instruktioner för att bygga upp en SQL-databas innehållandes följande tabeller:

```
has_message
ptt_messages
image_messages
video_messages
text_messages
products
mdm_data
roster
```

Nedan är en visualisering av databas-strukturen samt dess relationer



Figur 1 Databasstruktur meddelanden



Figur 2 Databasstruktur metadata

2.2 Databasinformation

Nedan följer en kort beskrivning av tabeller och dess innehåll.

2.2.1 Has_message

Tabellen beskriver relationerna mellan produkter och meddelanden och innehåller följande fält:

Fält	Betydelse/tolkning
pid	Produkt-ID för aktuell mid
mid	Meddelande-ID
type	Typ av meddelande. Kan vara 1:text, 2:bild, 3:push-to-talk/ljud, 4:video.
shmid	Meddelande UUID

2.2.2 Ptt_message

Tabellen innehåller samtliga ljudmeddelanden genererade av plattformens push-to-talk (PTT)-funktion. Dessa meddelanden kunde även förvrängas med hjälp av en tonhöjdsjustering.
Tabellen innehåller följande fält:

Fält	Betydelse/tolkning
mid	Meddelande-ID, återfinns även i has_message.
shmid	Meddelande-UUID, återfinns även i has_message.
path	Sökväg till aktuell media-fil.
length	Tomt fält.
pitch	Ursprunglig tonhöjd på meddelandet.
inserted	Tid och datum då meddelandet lästes in Ingestion-1, *OTS kap. 1.4.3 Ingestion-1.*
mcc	Mobile Country Code för meddelandet.
isgrp	Anger om meddelandet är en del av en gruppkonversation.
isatt	Anger om meddelandet är en bilaga till ett annat meddelande.
sender	Sändande JID på meddelandet.
reciever	Mottagande JID och/eller grupp (gid).
time	Tid då meddelandet skickades.
latitude	Latitud för den enhet som skickat meddelandet.
longitude	Longitud för den enhet som skickat meddelandet.
metadataverified	Tomt fält.

2.2.3 Image_message & video_message

Tabellen innehåller samtliga meddelanden där bilder eller videoklipp ingick.
Tabellen innehåller följande fält:

Fält	Betydelse/tolkning
mid	Meddelande-ID, återfinns även i has_message.
shmid	Meddelande-UUID, återfinns även i has_message.
path	Sökväg till aktuell media-fil.
inserted	Tid och datum då meddelandet lästes in Ingestion-1, *OTS kap. 1.4.3 Ingestion-1.*
mcc	Mobile Country Code för meddelandet.
isgrp	Anger om meddelandet är en del av en gruppkonversation.
isatt	Anger om meddelandet är en bilaga till ett annat meddelande.
sender	Sändande JID på meddelandet.
reciever	Mottagande JID och/eller grupp (gid).
time	Tid då meddelandet skickades.
fromnote	Anger om meddelandet är skickat från enhetens ”valv”.
latitude	Latitud för den enhet som skickat meddelandet.
longitude	Longitud för den enhet som skickat meddelandet.
metadataverified	Tomt fält.

2.2.4 Text_message

Tabellen innehåller samtliga meddelanden innehållandes enbart text.
Tabellen innehåller följande fält:

Fält	Betydelse/tolkning
mid	Meddelande-ID, återfinns även i has_message.
shmid	Meddelande-UUID, återfinns även i has_message.
text	Textinnehåll i meddelande. Textinnehållet kan anta olika format och beskrivs närmre under 3.1 textformat.
inserted	Tid och datum då meddelandet lästes in Ingestion-1, *OTS kap. 1.4.3 Ingestion-1.*
mcc	Mobile Country Code för meddelandet.
isgrp	Anger om meddelandet är en del av en gruppkonversation.
isatt	Anger om meddelandet är en bilaga till ett annat meddelande.
sender	Sändande JID på meddelandet.
reciever	Mottagande JID och/eller grupp (gid).
time	Tid då meddelandet skickades.
latitude	Latitud för den enhet som skickat meddelandet.
longitude	Longitud för den enhet som skickat meddelandet.
verified	Tomt fält.
isfwd	Anger om meddelandet är ett vidarebefordrat meddelande.

2.2.5 Product

Tabellen innehåller information om de trådar/produkter som genererats i exporter.
Tabellen innehåller följande fält:

Fält	Betydelse/tolkning
case_id	Det case/syndikat aktuell produkt tillhör. Ytterligare information om syndikat återfinns i OTS kap. 1.4.3 Ingestion.
pid	Produkt-ID, återfinns även i has_message.
date_created	Datum och tid då produkten skapats.
mcc_str	Mobile Country Code för samtliga meddelanden som skickats i produkten.
jid_str	Samtliga JID som skickat eller tagit emot meddelanden i produkten.
count	Antalet meddelanden i produkten.
jid_1	Ena parten vid tvåpartskommunikation, tomt vid gruppkonversation.
jid_2	Andra parten vid tvåpartskommunikation, tomt vid gruppkonversation.
gid	Grupp-ID vid flerpartskommunikation, tomt vid tvåpartskommunikation.
isDup	Tomt fält.
knownGroup	Tomt fält.
apk	Grupp-ID

2.2.6 MDM_Data

Tabellen innehåller information om Anom-enheter hämtat från plattformens Mobile Device Management-verktyg. Tabellen innehåller följande fält:

Fält	Betydelse/tolkning
jid	Aktuellt JID, återfinns tabellen Roster.
imei	Senast kända International Mobile Equipment Identity för enheten.
imsi	Senast kända International Mobile Subscriber Identity för SIM-kortet.
regdate	Datum då enheten registrerades i MDM-plattformen.
lastcheckin	Senast enheten syntes av MDM-plattformen.
make	Märke på enheten.
model	Modell på enheten.
currentmcc	Senast kända Mobile Country Code.
currentcc	Senast kända Country Code.
currentoperator	Senast kända teleoperatör.
currentphone	Senast kända telefonnummer.
devicelocale	Senast kända språk- och regionsinställningar på enheten.
ipaddr	Senast kända IP-address.
lastlat	Senast kända latitud.
lastlong	Senast kända longitud.
lastlocdate	Tid och datum för senast kända position.
lastwifi	Senast kända Wifi enheten kopplats till.
status	Status enheten förmedlade till MDM vid senaste incheckning.
serialnum	Serienummer på enheten.
Iccid	Integrated circuit card identifier på SIM-kortet.

2.2.6.1 Kompletterande MDM-information

Den 2021-11-16 delgavs kompletterande information om Anom-enheter. Tabellen innehåller följande fält:

Fält	Betydelse/tolkning
JID	Aktuellt JID, återfinns tabellen Roster.
IMEI	Samtliga kända International Mobile Equipment Identity för enheten.
ICCID	Samtliga kända Integrated circuit card identifier på SIM-kort.
Last Known Latitude	Senast kända latitud för enheten
Last Known Longitude	Senast kända longitud för enheten
Last Location Reported Time	Tid och datum för senast kända position.
Serial Number	Serienummer på enheten
Network Carrier	Senast kända teleoperatör
IMSI	Samtliga kända International Mobile Subscriber Identity för SIM-kort.
Model	Modell på enheten.
Last Seen	Senast enheten syntes av MDM-plattformen.

2.2.7 Roster

Tabellen innehåller känd information om brukaren av en JID. Tabellen innehåller följande fält:

Fält	Betydelse/tolkning
jid	Aktuellt JID, återfinns i tabellen MDM_Data
uname	Senast kända alias för aktuell JID
real_name	Det namn en användare av Hola iBot senast registrerat för aktuell JID
bio	Den beskrivning en användare av Hola iBot senast registrerat för aktuell JID
location	Den plats en användare av Hola iBot senast registrerat för aktuell JID

Användare av Hola iBot var polisanställda som ingick i operationen Trojan Shield som manuellt matade in denna information, vilket beskrivs ytterligare i *OTS kap 10.7 Förteckningssidan.*

3 Relevanta observationer av MLAT-materialet

Vid hanteringen av MLAT-materialet har följande observationer kunnat göras som är relevanta för en korrekt förståelse av materialet.

3.1 Produkter

Under Operation Trojan Shield skapades nya datapaket varje måndag, onsdag och fredag, *OTS kap. 2. Skapande av nya datapaket*. Samtliga konversationer mellan två individer eller i en grupp delades in i produkter, även kallat trådar eller chattslingor. Dessa förseddes med både case_id och pid. En produkt från syndikat 12 med pid 34567 presenteras som 12_34567. Dessa produkter innehåller samtliga meddelanden skickade i konversationen sedan senaste exporttillfället och löper således mellan två till tre dagar.

3.2 Textformat

Meddelanden som skickas via Anom kan antingen återfinnas som ren text, eller som något av de format som presenteras i avsnittet. Dessa är samtliga skrivna som JavaScript Object Notation (JSON).

Text i JSON innehåller normalt inga radbrytningar. Nedan exempel har radbrutits för ökad läsbarhet.

Varje kategori av meddelande finns i två versioner beroende på vilken tidsperiod meddelandet har blivit inläst till Anom-plattformen.

3.2.1 Vidarebefordrade meddelanden

När en användare vidarebefordrar ett meddelande från en konversation till en annan användare presenteras detta som en vidarebefordran (engelska: forward). Meddelanden som vidarebefordras kan presenteras på två sätt.

Vidarebefordringar inlästa till och med 2020-09-09 innehåller enbart text och presenteras som följande exempel:

```
forward_prefix
{
 "forward_message_time":     1633354850,
 "forward_message_text":     "hej",
 "forward_mes-               "abc123"
 sage_user_jid":
}
```

Värdetabell:

Fält	Betydelse/tolkning
forwarded_message_time	Tidsstämpel i Unix Time.
forward_message_text	Vidarebefordrat innehåll.
forward_message_user_jid	Den JID som meddelandet vidarebefordrats från.

Vidarebefordringar inlästa från och med 2020-09-11 möjliggör övriga typer av innehåll och presenteras som följande exempel:

```
forward_prefix
{
 "forward_message_time":     1633354850,
 "forward_mes-               "abc123",
 sage_user_jid":
 "forward_message_body":     "hej",
 "forward_message_type":     "TEXT”,
 "forward_message_uuid":     "123e4567-e89b-12d3-a456426614174000"
}
```

Värdetabell:

Fält	Betydelse/tolkning
forwarded_message_time	Tidsstämpel i Unix Time.
forward_message_user_jid	Den JID som meddelandet vidarebefordrats från.
forward_message_body	Den text eller kontaktinformation som vidarebefordrats. Om forward_message_type är IMAGE, VIDEO, PTT eller NOTE finns inte detta fält i meddelandet.
forward_message_type	Anger vilken sorts meddelande som vidarebefordrats. Fältet kan anta följande värden: TEXT, IMAGE, VIDEO, PTT, CONTACT och NOTE och avgör om det vidarebefordrade meddelandet är text, bild, video, ljud, kontaktinformation eller en anteckning.
forward_message_uuid	UUID på vidarebefordrat meddelande. Detta UUID är inte detsamma som meddelandets shmid.

3.2.2 Svar på meddelanden

När en användare svarar på ett specifikt meddelande i befintlig konversation representeras detta som ett citat (engelska: quote). Citat i konversationer kan presenteras på två sätt.

Meddelanden inlästa till och med 2020-12-21 (med ett fåtal undantag) presenteras som följande exempel:

```
quote_prefix
{
 "quote_message_time":       1633354850,
 "quote_message_text":       "Hur mår du?",
 "quoted_text":              "Jag mår bra",
 "quote_message_user_jid":   "abc123",
 "message_uid":              "123e4567-e89b-12d3-a456-426614174000"
}
```

Värdetabell:

Fält	Betydelse/tolkning
quote_message_time	Tidsstämpel i Unix Time.
quote_message_text	Det meddelande som har besvarats.
quoted_text	Det svar som getts.
quote_message_user_jid	Den JID som skickat det meddelande som har besvarats.
message_uid	UUID på det meddelande som besvarats. Detta UUID är inte detsamma som meddelandets shmid.

Meddelanden inlästa från och med 2020-12-25 (med vissa undantag) innehåller ytterligare metadata och innehåller förutom ovan även följande fält

```
quote_prefix
{
 "quote_message_time":       1633354850,
 ⋮
 "isQuotedMessageDeleted":   true,
 "isEdited":                 false,
}
```

Värdetabell:

Fält	Betydelse/tolkning
quote_message_time	Tidsstämpel i Unix Time.
isQuotedMessageDeleted	Anger om det besvarade meddelandet har raderats. Kan anta värdet true (sant) eller false (falskt).
isEdited	True/False. Anger om det besvarade meddelandet har redigerats.

3.2.3 Valvbilagor

När en användare skickar med en bilaga från det så kallade valvet presenteras det som en valvbilaga (engelska: vault attachment). Bilagor kan vara anteckningar och bilder, *OTS A.7.1.3 Valvet.* Valvbilagor kan presenteras på två vis.

Valvbilagor skickade till och med 2020-12-23 presenteras som följande exempel:

```
{
 "mIsSelected":              true,
 "passwordChecked":          false,
 "archived":                 true,
 "attachmentsList":          [],
 "attachmentsListOld":       [],
 "checklist":                false,
 "content":                  "",
 "creation":,
 "lastModification":,
 "locked":                   false,
 "reminderFired":            false,
 "title":                    "",
 "trashed":                  false
}
```

Värdetabell:

Fält	Betydelse/tolkning
mIsSelected	True/False, innebörd i dagsläget okänd.
passwordChecked	True/False, innebörd i dagsläget okänd.
archived	True/False, innebörd i dagsläget okänd.
attachmentsList	Detta fält innehåller i förekommande fall en lista med bilagor skickade i meddelandet.
attachmentsListOld	Detta fält är tomt i samtliga meddelanden.
checklist	Anger om innehållet är en checklista.
content	Detta fält innehåller i förekommande fall textinnehåll.
creation	Tid i Unix time som bilagan skapades.
lastModification	Tid i Unix time som bilagan senast ändrades.
locked	True/False, innebörd i dagsläget okänd.
reminderFired	True/False, innebörd i dagsläget okänd.
title	Bilagans titel.
trashed	True/False, innebörd i dagsläget okänd.

Meddelanden inlästa från och med 2020-12-23 presenteras som följande exempel.

```
{
 "mIsFromVault":              true,
⋮
}
```

Värdetabell:

Fält	Betydelse/tolkning
mIsFromVault	True/False, innebörd i dagsläget okänd.

Övriga fält som ovan.

3.3 Tidsförskjutning

3.3.1 Tidszonsdifferens

I källmaterialet för MLAT-exporter är samtliga tidsstämplar angivna som tidsformatet UTC. På grund av en misskonfiguration i en av servrarna som extraherat Anom-data har tidszonen för vissa meddelanden felaktigt tolkats som UTC fast den i själva verket varit en annan tidszon. FBI har identifierat olika tidsfönster som gäller för meddelanden *OTS kap. 8.6.1 Fel i meddelandens tidszon*. Meddelanden som är inlästa i respektive fönster är angivna som UTC men skall konverteras enligt nedan:

- Tidsram 1

  Meddelanden inlästa mellan 1 oktober 2019 och 27 oktober 2019: UTC -3

- Tidsram 2

  Meddelanden inlästa mellan 27 oktober 2019 och 29 mars 2020: UTC -2

- Tidsram 3

  Meddelanden inlästa mellan 29 mars 2020 och 18 september 2020: UTC -3

- Tidsram 4

  Meddelanden inlästa efter 18 september 2020: UTC

3.3.1.1 *Exempel korrigering av tidszonsdifferens*

Följande fyra exempelmeddelanden är inlästa 2020-08-28 och 2020-08-31 vilket framgår i kolumn MESSAGE_INSERTED. Dessa meddelanden faller således inom tidsram 3 (29 mars 2020 – 18 september 2020) och skall därför tolkas som UTC -3. I källmaterialet visas följande tidsstämplar:

	A	B	C	D	S
1	MESSAGE_TIME	MESSAGE_SENDER	MESSAGE_DECODED	MESSAGE_RECEIVER	MESSAGE_INSERTED
2	2020-08-27 17:48:46	Exempel1	Hej	exempel2	2020-08-28 00:11:09
3	2020-08-27 17:50:01	Exempel2	Hej på dig	Exempel1	2020-08-31 00:11:10
4	2020-08-27 17:50:15	Exempel1	Hur går det?	Exempel2	2020-08-31 00:11:10
5	2020-08-27 17:51:04	exempel2	Det går bra tack.	Exempel1	2020-08-31 00:11:10

Figur 3 – Exempel korrigering av tidszonsdifferens – originaltid.

Konvertering till svensk sommartid (UTC+2) sker genom addition av fem timmar:

	A	B	C	D	S
1	MESSAGE_TIME	MESSAGE_SENDER	MESSAGE_DECODED	MESSAGE_RECEIVER	MESSAGE_INSERTED
2	2020-08-27 22:48:46+0200	Exempel1	Hej	exempel2	2020-08-28 00:11:09
3	2020-08-27 22:50:01+0200	Exempel2	Hej på dig	Exempel1	2020-08-31 00:11:10
4	2020-08-27 22:50:15+0200	Exempel1	Hur går det?	Exempel2	2020-08-31 00:11:10
5	2020-08-27 22:51:04+0200	exempel2	Det går bra tack.	Exempel1	2020-08-31 00:11:10

Figur 4 – Exempel korrigering av tidszonsdifferens – korrekt svensk tid

I Polisens analysverktyg som hanterar och presenterar källmaterialet skedde automatisk korrigering av tidszon enligt ovan den 2021-09-30. Innan detta datum justerades samtliga tidsstämplar på meddelanden i analysverktyget från UTC till svensk tid vilket medför att urklipp och exporter av material som hämtats från analysverktyget innan 2021-09-30 presenterar tidsstämplar två till tre timmar felaktigt jämfört med svensk tid, beroende på i vilken tidsram det aktuella meddelandet blev inläst.

I källmaterialet har ingen tidszonsjustering utförts. Korrigerad tidsangivelse presenteras enligt ISO8601[3] där tidsangivelse presenteras med ett efterföljande plus- eller minustecken och tidszonsangivelse.

3.3.2 *Tidzonsförskjutning 16-17 februari 2021*

Det har i materialet identifierats ytterligare en tidzonsförskjutning för meddelanden skickade den 16 - 17 februari 2021. Detta förklaras genom att det vid den tiden förelåg ett problem i infrastrukturen som hanterade inläsning av nya meddelanden från servern i tredje land. På grund av detta skedde inläsning av nya data manuellt vilket kan ha orsakat tidzonsförskjutning på grund av mänsklig faktor. Exakt vilken tidzonsförskjutning det rör sig om och under vilka exakta tider har inte kunnat identifieras, men det finns flera exempel som tyder på att tidsstämpeln är satt två timmar efter att meddelandet i verkligheten skickats, exempelvis att ett meddelande har tidsstämpeln 17 feb 2021 01:21 (svensk tid) men i innehållet i meddelandena refererar de till att klockan är 23 (den 16 februari 2021). Efter den 17 februari 2021 åtgärdades problemen och tidsförskjutningen ser ut att upphöra någon gång under dagen den 17 februari 2021.

3.3.3 Övrig tidsförskjutning

Det har i materialet uppmärksammats en förskjutning i tid som yttrar sig på så sätt att vissa meddelandens tidsstämpel är satt 5–10 minuter innan meddelandet faktiskt har skickats.

Det har uppmärksammats genom analys av bilder där en tidsstämpel kunnat uppfattas, t.ex. bilder på klockor eller mobiltelefoner med synlig klocka samt genom matchning av tidsangivelsen i vidarebefordrade meddelanden och deras original.

Vid djupare analys har följande uppmärksammats:

- Från juni till slutet av augusti är differensen mellan fem och sju minuter.
- Från slutet av augusti till slutet av september är differensen oftast åtta minuter.
- Från slutet av september till den 7 oktober är differensen nio minuter.
- Från den 8 oktober till den 15 december är differensen tio minuter.
- Den 15 december 2020 upphör differensen.

3.3.3.1 Exempel övrig tidsförskjutning

Ett meddelande med tidsstämpel 2020-09-17 17:21:41 (svensk tid) innehåller en bild av en mobiltelefon där klockan visar 17:30, en differens på ca 8 minuter. Meddelandet bör därför i verkligheten ha skickats åtta minuter senare än dess tidsstämpel visar.

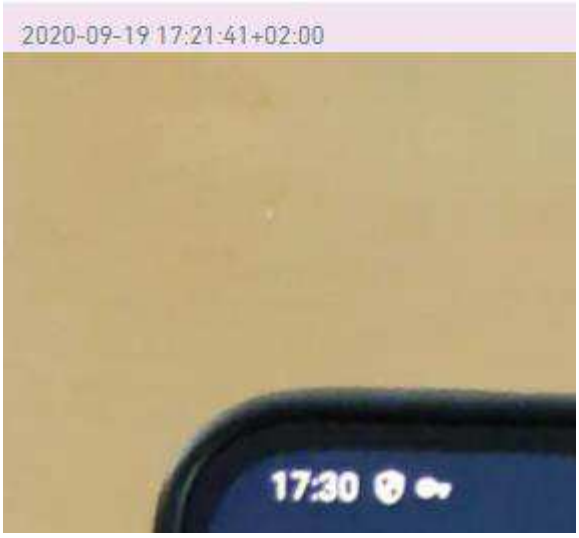


Fig 3. Tidsförskjutning exempel 1

Ett meddelande med tidsstämpel 2020-09-19 11:34:05 (svensk tid) innehåller en bild av en mobiltelefon där klockan visar 11:42, en differens på ca 8 minuter. Meddelandet bör därför i verkligheten ha skickats åtta minuter senare än dess tidsstämpel visar.

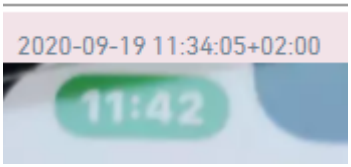


Fig 4. Tidsförskjutning exempel 2

3.4 Shmid är gemensamt för meddelanden och deras attachments

Enligt filen ”*data_information.txt*” ([5] Bilaga 1) framgår det att shmid skall vara ett UUID. Det har uppmärksammats i databaserna att flera rader kan ha samma shmid. Detta uppstår när ett bild-, text- eller ljudmeddelande är en bilaga (eng. attachment) till ett annat meddelande. Vid denna situation får samtliga meddelanden samma unika shmid. Meddelande-id, Mid, är alltid unikt för ett unikt meddelande.

3.5 Platsinformation

3.5.1 Tillförlitlighet MCC

För enheter innehållandes ett aktivt SIM-kort som var uppkopplat mot ett mobilnät försågs det skickade meddelandet med aktuell Mobile Country Code (MCC) för den sändande enheten (Appendix 8.2c [1]). En jämförelse av denna MCC mot textinnehåll samt GPS-position ger att denna MCC inte alltid är helt tillförlitlig. Detta yttrar sig som en fördröjning av byte mellan äldre MCC till ny MCC när enheten färdas från ett land till ett annat.

3.5.1.1 Exempel MCC

Nedan tabell innehåller exempel på koordinater och MCC från meddelanden där plats och MCC inte överensstämmer.

Message - Mcc	Message – Longitude	Message - Latitude	Land – MCC	Land - Koordinater
240	-4.511279	36.599588	Sverige	Spanien
240	-4.511137	36.599613	Sverige	Spanien
240	-4.511137	36.599613	Sverige	Spanien
240	-4.511226	36.599503	Sverige	Spanien
240	-4.621791	36.544923	Sverige	Spanien
240	-4.511296	36.599615	Sverige	Spanien
240	-4.511596	36.599373	Sverige	Spanien
240	-4.511298	36.599735	Sverige	Spanien

3.5.2 Misslyckad positionering – Felaktig Longitud

Efter en uppdatering i april 2020 försökte Anom-applikationen få fram enhetens position i samband med att meddelanden skickades. Detta kunde ibland misslyckas (*OTS A.8.2.d*), vilket resulterade i positionsvärden på följande vis:

Värdet för latitud är satt till ett heltal, t.ex. 59.0.

Värdet för longitud är satt till ett mycket stort tal, t.ex. 1617786553.

Värdet för longitud är vid det tillfället troligen en tidsstämpel i Unix Time.

3.5.2.1 Exempel misslyckad positionering – Felaktig longitud

Nedan tabell visar på exempel där meddelandets position visas felaktigt. Observera att bokstaven E i detta fall symboliserar multiplikation med den specificerade tiopotensen. 1.616779411E12 skall tolkas som $1.616779411x10^{12}$.

Message – Time	Message - Longitude	Message - Latitude
2021-03-26 17:23:42+0100	1.616779411E12	59.0
2021-03-26 17:54:17+0200	1.617206019E12	59.0
2021-03-26 20:57:19+0100	1.616529358E12	59.0
2021-03-26 20:59:04+0100	1.61652912E12	59.0
2021-03-30 15:16:22+0100	1.616508937E12	59.0
2021-04-07 13:20:54+0200	1.617794386E12	59.0
2021-04-24 14:58:07+0100	1.616594251E12	59.0

3.5.3 Misslyckad positionering – Trunkerade koordinater

Ett annat förekommande exempel på hur positionering har misslyckats kan ses genom trunkering av värdet på koordinater i materialet. Denna trunkering yttrar sig genom att värdet för longitud trunkeras från vänster och saknar värde för heltal. Det värde som presenteras är istället värdet på decimalerna. På liknande men omvänt sätt har värdet för latitud trunkerats från höger och saknar värde för decimalerna. Det värde som presenteras är enbart värdet på heltalet.

3.5.3.1 Exempel misslyckad positionering – Trunkerade koordinater

Nedan tabell visar på exempel där meddelandets position visas felaktigt. Observera att enheten i det här fallet delvis rapporterat korrekta koordinater, 29.008981, 41.078515 och delvis trunkerade dito, 8981.0, 41.0. Se även fig 5 för en visualisering över trunkeringen.

Message - Time	Message - Longitude	Message - Latitude
2020-10-16 10:26:38+0200	8981.0	41.0
2020-10-16 10:26:53+0200	8981.0	41.0
2020-10-16 10:27:47+0200	29.008981	41.078515
2020-10-16 10:28:11+0200	29.008981	41.078515
2020-10-16 10:28:14+0200	29.008981	41.078515
2020-10-16 13:42:53+0200	8476.0	41.0
2020-10-16 13:42:54+0200	8476.0	41.0

Kommentar	Message - Latitude	Message - Longitude	Message - Time
Trunkerade koordinater	41.0	8981.0	2020-10-16 10:26:38+0200
Trunkerade koordinater	41.0	8981.0	2020-10-16 10:26:53+0200
Korrekta koordinater	41.078515	29.008981	2020-10-16 10:27:47+0200
Korrekta koordinater	41.078515	29.008981	2020-10-16 10:28:11+0200
Korrekta koordinater	41.078515	29.008981	2020-10-16 10:28:14+0200
Trunkerade koordinater	41.0	8476.0	2020-10-16 13:42:53+0200
Trunkerade koordinater	41.0	8476.0	2020-10-16 13:42:54+0200

Fig 5. Trunkerade koordinater, visualisering över trunkering.

3.5.4 Positionering visar tidigare känd plats

När position hämtas via Android Location Manager kan hämtningen i vissa fall misslyckas varpå den senast kända positionen hämtas istället. Detta beskrivs i detalj i dokumentet ”Positionsdata i meddelanden skickade med applikationen ANØM”, A673.978/2021.

3.5.4.1 Exempel positionering visar tidigare känd plats

Nedan meddelanden visar på ett tillfälle då enhetens position inte kunnat uppdateras. Klockan 13:49 fastställs positionen till 16.489885, 59.596813. Enheten har sedan dess flyttats (enligt annan information i utredningen) men ny position registreras inte förrän klockan 18:50.

Message - Time	Message - Longitude	Message - Latitude
2021-05-19 13:49:19+0200	16.489735	59.596842
2021-05-19 13:49:39+0200	16.489885	59.596813
2021-05-19 13:50:23+0200	16.489885	59.596813
2021-05-19 17:32:59+0200	16.489885	59.596813
2021-05-19 18:04:08+0200	16.489885	59.596813
2021-05-19 18:50:33+0200	17.221353	59.640529
2021-05-19 18:52:16+0200	17.161794	59.64619

3.6 MDM och Roster – Statisk information

Innehåll i tabeller MDM och Roster innehåller den senast kända informationen. En användare av Anom kan använda sig av flera olika enheter med skilda IMEI-nummer såväl som olika SIM-kort. Tabellerna Roster och MDM innehåller den information som var aktuell vid slutet av operation Trojan Shield. Den kompletterande MDM-informationen som behandlas i kap 2.2.6.1 innehåller samtliga kombinationer av enheter aktuellt JID brukat.

Under operation Trojan Shield försågs Polismyndigheten med datapaket varje måndag, onsdag och fredag. Datapaketen innehöll samtliga meddelanden genererade sedan den senaste exporten. Meddelanden var försedda med det alias aktuellt JID hade vid exporttillfället. Det resulterar i att byten av alias i regel visas i materialet upp till tre dagar *tidigare* än de i verkligheten skett. I vissa fall har det observerats att ett nytt alias inte visas i materialet förrän flera veckor *efter* att bytet i verkligheten har skett. På grund av att alias endast kontrollerades vid specifika tillfällen är det möjligt att vissa alias saknas i materialet.

3.7 Användandet av flera enheter

Vid initial uppsättning av ett nytt användarkonto i Anom genererade en återförsäljare ett unikt JID som kontrollerades mot en databas för att säkerställa att JID var unik och inte tidigare brukats inom Anom. Efter att det nya användarkontot satts upp tillhandahölls ett nytt lösenord till återförsäljaren.

Efter att en brukare av JID loggat in på en enhet ändrades det ursprungliga lösenordet till ett slumpmässigt genererat 256 tecken långt nytt lösenord.

Innan uppdatering till Android 10 som skedde under december 2020 var det inte möjligt för ett JID att logga in på en annan enhet än den som initialt sattes upp av återförsäljare eller administratör.

Från och med denna uppdatering var det möjligt för ett JID att använda sig av en annan enhet än den som initialt satts upp till detta JID.

För att kunna logga in på ytterligare en enhet krävdes att en återförsäljare först nollställde lösenordet. Vid nollställning av lösenordet blev eventuell redan inloggad enhet utloggad efter fem minuters inaktivitet och nekad möjligheten att logga in på nytt.

Mellan januari till mars 2021 var det möjligt för ett JID att vara inloggat på två enheter samtidigt, förutsatt att:

- En administratör eller återförsäljare återställde lösenordet för aktuell JID innan varje ny inloggning.
- Att den första enheten var aktiv så att den automatiska utloggningen inte skedde.
- Att enheten var uppdaterad till Android 10 eller senare.

Att en och samma JID var inloggad på två enheter var en sällsynt företeelse som vanligtvis orsakades av en oerfaren återförsäljare som var obekant med återställningsprocessen.

I slutet av mars 2021 justerades lösningen för att förhindra att ett och samma JID kunde använda fler enheter samtidigt. Uppdateringen innebar att en eventuell redan aktiv enhet loggades ut i samma ögonblick som en ny enhet loggades in. *OTS Bilaga Klonade enheter*

3.8 Användaren bot

Applikationen Anom innehöll en funktion som innebar att när ett meddelande skickades så skickades det även automatiskt en dold kopia av meddelandet till en dold/fiktiv användare med användarnamnet ”bot”. Den här processen var inte synlig för den användare som skickade meddelandet, och den användaren visste inte heller om att processen ägde rum. *OTS Kap 1. ÖVERSIKT ÖVER SERVRAR OCH NÄTVERK.*

Under perioden 2021-05-05 – 2021-06-07 förekommer det i materialet meddelanden adresserade till användaren ”bot”. Detta beror på en felaktig uppdatering av Anom som drogs tillbaka.

4 Källförteckning

[1] https://polisen.se/aktuellt/nyheter/2021/juni/155-frihetsberovade-i-storsta-insatsen-hittills-mot-organiserad-brottslighet/ [Hämtat 2021-10-07]

[2] Teknisk information om Operation Trojan Shield [Översatt version, senast uppdaterad 31 augusti 2021]

[3] https://www.iso.org/iso-8601-date-and-time-format.html [Hämtat 2021-12-16]

[4] https://xmpp.org/rfcs/rfc3921.html#session [Hämtat 2021-12-29]

[5] A605.844/2021 Beskrivning av Polismyndighetens hantering av Anom-data

A605.844/2021

polisen.se

Polisens IT-avdelning

Telefon 114 14

e-post registrator@polisen.se

Polisen

A605.844/2021

IT-avdelningen

Anom

Beskrivning av Polismyndighetens hantering av Anom-data

Rapport

Utgivare
Polismyndigheten
Tfn 114 14
E-post kansli.registrator@polisen.se
www.polisen.se

Produktion Polismyndigheten, 2021-09-21
Upplaga [XX] ex

Diarienr. AXX
Tryck Polisens tryckeri

Sammanfattning

Detta dokument innehåller en beskrivning av Polismyndighetens metod och hantering av materialet som inkommit i operation Trojan Shield som berör avkrypterad information från kommunikationstjänsten Anom.

Information har inkommit i form av hårddiskar, där varje hårddisk innehåller data från en gruppering av användare, även kallat syndikat.

Ovan nämnda databaser innehåller meddelanden och bilagor dessa användare skickat i plattformen. Dessa databaser är även försedda med metadata kring dessa meddelanden och användare.

Dokumentet beskriver materialets format och struktur. Information om själva innehållet, den dekrypterade informationen beskrivs i dokumentet *”Beskrivning av information i Anom-data”*

I detta dokument finns flertalet hänvisningar till dokumentet *”Teknisk information om Operation Trojan Shield”* som vidare beskriver materialet och dess hantering innan det kom Polismyndigheten till handa.

Innehållsförteckning

SAMMANFATTNING ..... **I**

INNEHÅLLSFÖRTECKNING ..... **II**

1 INLEDNING **1**
1.1 Bakgrund 1
1.2 Syfte 1
1.3 Hänvisning till OTS Technical Details 1

2 MLAT EXPORTER **1**
2.1 Beskrivning och hantering av fysiskt media 2
2.2 Innehåll fysiskt media 2
2.2.1 Maskininstruktioner 2
2.2.2 Bifogade filer 3
2.2.3 Metadata 4

3 DELNINGSFÖRFARANDE **4**

4 BEHANDLING AV INFORMATION **4**
4.1 Extrahering från databas per JID 4
4.2 Filformat – TSV 4
4.3 Textkodning i Base64 4
4.4 Hänvisning till Media 4
4.5 Deduplicering av meddelanden 4
4.5.1 Anledning till deduplicering 5
4.5.2 Metod 5
4.5.3 Verifiering 5
4.6 Alias-information 5
4.7 Dekodning och presentation av källmaterial 5
4.7.1 Per databas 6
4.7.1.1 <JID>-image-messages & <JID>-video-messages 8
4.7.1.2 <JID>-text-messages 8
4.7.1.3 <JID>-ptt-messages 8
4.7.1.4 <JID>-jids-from-all-relevant-products 8
4.7.1.5 <JID>-mdm_data 8
4.7.1.6 <JID>-roster 8
4.7.1.7 Metadata-query-for-<databas>.sql 8
4.7.2 Dedup 8
4.7.3 Media 9

5 KÄLLFÖRTECKNING **9**

6 BILAGOR **10**

BILAGA 1 – DATA_INFORMATION.TXT **11**

BILAGA 2 – FÄLTORDNING TSV-FILER **1**
<JID>-image-messages & <JID>-video-messages 1
<JID>-text-messages 2
<JID>-ptt-messages 3
<JID>-mdm_data 4
<JID>-roster 4

BILAGA 3 EXEMPEL DATABASFRÅGOR **5**
Bild-meddelanden 5
Ljud-meddelanden 5
Text-meddelanden 5
Video-meddelanden 5
Deltagande JID:ar 5

1 Inledning

1.1 Bakgrund

Sammanlagt har 16 länder världen över ingått i insatsen som gått under namnet Trojan Shield/OTF Greenlight. I Europa har arbetet letts av Sverige och Nederländerna i samarbete med Europol.
Den krypterade plattformen Anom, som nu har avvecklats, har använts av kriminella för att planera, koordinera och kunna utföra brott.

Plattformen skapades och administrerades i det dolda av FBI. I takt med att liknande tjänster som ”*Encrochat*” och ”*Sky ECC*” upphörde övergick allt fler kriminella aktörer till att kommunicera på denna plattform.

Enligt FBI har över 27 miljoner meddelanden skickats via plattformen av över 200 kriminella nätverk mellan oktober 2019 och juni 2021. [1]

Efter att plattformen avvecklades i juni 2021 har Polismyndigheten av FBI försetts med exporter av meddelanden och annan information från plattformen i enlighet med det ömsesidiga juridiska biståndsavtalet (MLAT) mellan USA och EU.

1.2 Syfte

Dokumentet syftar till att beskriva innehållet i de exporter FBI försett polismyndigheten med samt hur dessa har behandlats inom Polisen. Dokumentet beskriver även hur extrahering av information ur exporter för hantering inom FU genomförts.

1.2.1 Avgränsning

Dokumentet syftar inte till att beskriva innehåll i exporter. Detta sker i det separata dokumentet ”*Beskrivning av information i Anom-data”*

1.3 Hänvisning till OTS Technical Details

I detta dokument finns flertalet hänvisningar till det tekniska dokument som är framtaget för Operationen Trojan Shield (OTS) [2]. Det tekniska dokumentet finns i en engelsk och i en svensk version. Hänvisning till respektive kapitel och eventuellt avsnitt är detsamma i både det svenska och det engelska dokumentet. För tydlighetens skull kommer dessa hänvisningar betecknas med kursiv stil *OTS kap. <kapitel>.<avsnitt> <svensk rubrik>*. Exempelvis: *OTS kap. 8.1 Ärenden/syndikat.*

2 MLAT exporter

Material som begärts från USA via MLAT har inkommit som enheter (externa hårddiskar och USB-enheter) med exporter. Dessa har skickats till Sverige och mottagits av Justitiedepartementet och/eller Åklagarmyndighetens Riksenhet mot internationell och organiserad brottslighet (RIO). Dessa enheter har sedan vidarebefordrats till Polismyndigheten för fortsatt hantering. För mer information om MLAT-exporter se *OTS kap. 11 MLAT-export*.

2.1 Beskrivning och hantering av fysiskt media

Polismyndigheten har totalt mottagit åtta externa hårddiskar och fyra USB-minnen innehållandes rådata.

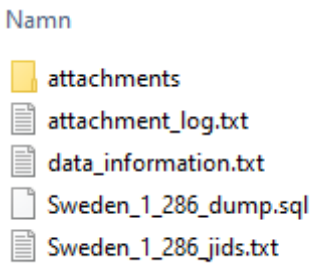
Samtliga enheter har efter ankomst speglats och hanterats enligt gängse rutiner av IT-forensik 1, Utredningsenheten, Polisregion Stockholm.

2.2 Innehåll fysiskt media

Varje fysiskt media utgör en export av ett så kallat syndika. För ytterligare information om syndikat och dess uppdelning hänvisas till *OTS kap. 8.1 Ärenden/syndikat*. De 8 externa hårddiskarna utgör initiala exporter och de 4 USB-minnen utgör tilläggsexporter för vissa syndikat.

För varje enhet finns denna uppsättning av filer

- En katalog innehållandes bilagor i form av ljud-, video-, och bildmaterial (Attachments).
- Information om vilka bilagor som förekommer i ovan katalog (attachment_log.txt).
- Beskrivning av dataformatet (data_information.txt).
- Instruktioner för upprättande av databas (Sweden_<*syndikat*>_dump.sql)
- En förteckning av de
- Information om vilka bilagor som förekommer.



Figur 1. Exempel på filstruktur innehåll, syndikat 286

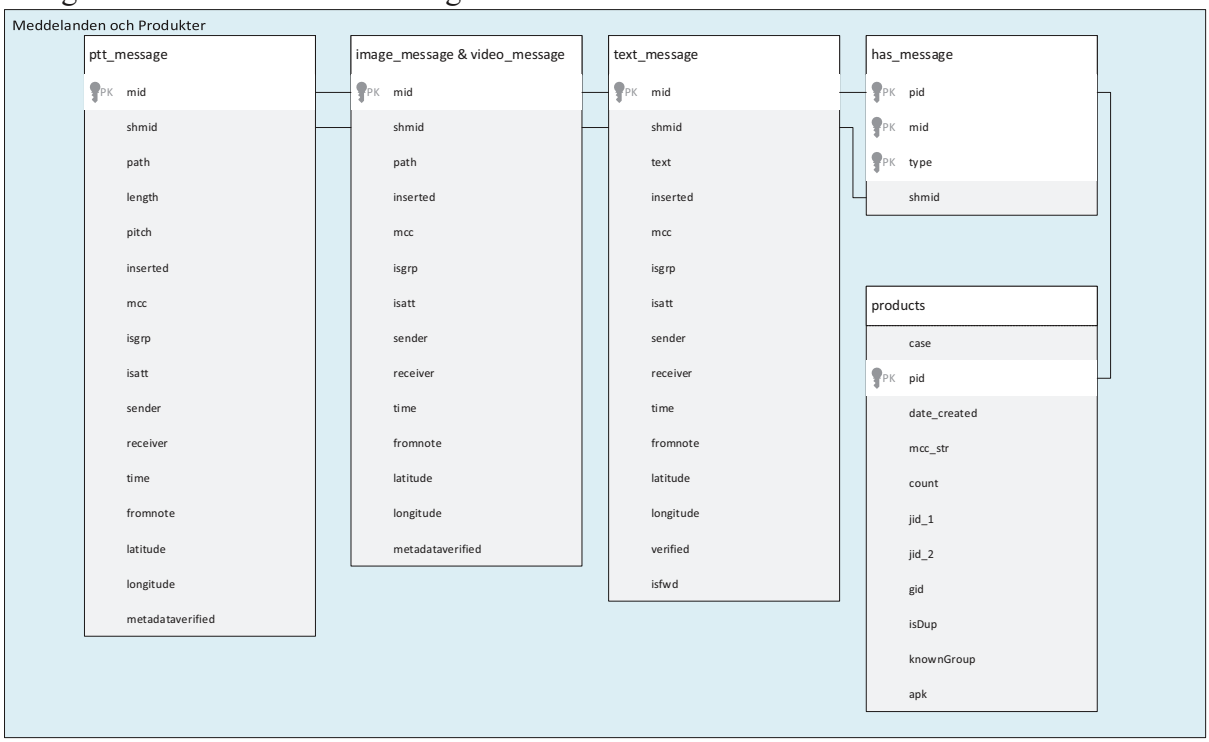
2.2.1 Maskininstruktioner

I filen Sweden<syndikat>_dump.sql återfinns instruktioner för att skapa en MySQL[3]-databas innehållandes följande tabeller:

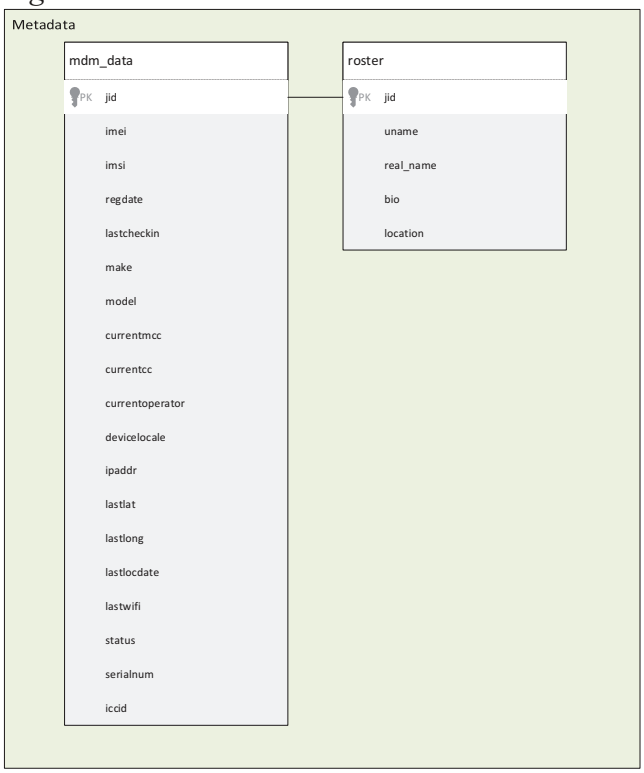
- Has_message
- Image_message
- Mdm_data
- Products
- Ptt_message
- Roster
- Text_message
- Video_message

I filen ”*data_information.txt*” (bilaga 1) återfinns fördjupad information om tabellernas struktur och innehåll. Detta fördjupas ytterligare i *OTS kap.8 Databasöversikt*

Se figur 2 och 3 för en visualisering av databas-strukturen samt dess relationer



Figur 2 Databasstruktur meddelanden



Figur 3 Databasstruktur metadata

2.2.2 Bifogade filer

I katalogen attachments återfinns tre underordnade kataloger

- Audio

- Video
- Images

I dessa finns all media som skickats i konversationer som attribuerats till syndikatet.

I filen ”*attachment_log.txt*” återfinns information om huruvida exporten av media tillhörande syndikatet har lyckats eller misslyckats. Totalt sett har 192 bilagor misslyckats.

2.2.3 Metadata

I filen ”*Sweden_<syndikat>_jids.txt*” återfinns samtliga s.k. Jabber Identification, även förkortat till JID, som attribuerats till syndikatet.

3 Delningsförfarande

Efter delningsbeslut av exportägande åklagare registreras vilken/vilka JID/s det specifika ärendet skall ta del av. Därefter delas följande information:

- Samtliga meddelanden från samtliga konversationer där aktuell JID deltar som sändare eller mottagare.
- MDM-information om aktuell JID.
- Roster-information om aktuell JID.

4 Behandling av information

4.1 Extrahering från databas per JID

Efter delningsbeslut från exportägande åklagare genomförs ett antal databasfrågor mot de olika databaserna. Exempel på dessa databasfrågor återfinns i bilaga 3.

4.2 Filformat – TSV

Samtliga databasfrågor blir sedan presenterade i ett antal tabb-separerade filer som sparas med filändelsen ”.tsv”. Dessa kan öppnas i valfritt program för textbehandling och beskrivs mer detaljerat nedan.

4.3 Textkodning i Base64

Textmeddelanden lagras som en BLOB (Binary Large OBject) [4] i databasen. Vid export konverteras detta till Base64 [5], vilket är en textbaserad representation av det binära objektet. Ingen information går förlorad vid denna konvertering.

4.4 Hänvisning till Media

För varje enskilt meddelande som innehåller media finns en referens till motsvarande fil i MLAT-exportens attachments-katalog.

4.5 Deduplicering av meddelanden

Deduplicering är en form av komprimering i syfte att endast presentera unikt data. Meddelanden från Anom har kunnat deduplicerats så att läsare av dessa endast behövt se varje unikt meddelande en gång. Fördjupning och tillvägagångssätt presenteras nedan.

4.5.1 Anledning till deduplicering

En enskild konversation kan förekomma i flera av de exporterade databaserna. Detta beror oftast på att deltagande JID:ar ingår i flera syndikat vilket medför att flera identiska kopior av konversationer förekommer för dessa JID:ar

4.5.2 Metod

Varje enskilt meddelande är försett med ett unikt meddelande-id (”mid”). Eftersom det unika meddelandet förekommer flera gånger blir dessa kombinerade till endast en rad med hänvisning till vilka konversationer/produkter detta meddelande deduplicerats ifrån.

4.5.3 Verifiering

En kontroll av att varje duplicerad konversation innehåller exakt samma meddelanden har genomförts.

4.6 Alias-information

Användare av Anom kan förse sin JID med ett eget Alias. Information om vilket Alias en JID använt sig av återfinns i Roster-tabellen. Att observera är att denna information är den som var aktuell vid slutfasen av Operation Trojan Shield.

En användare av Anom kan använt sig av andra Alias än detta historiskt.

Under operation Trojan Shield försågs Sverige löpande med meddelanden exporterade från ”hola iBot” *OTS kap.9.5 Export efter inmatning.* Dessa exporter skedde måndagar, onsdagar och fredagar. Meddelanden i exporter innehåller information om vilket Alias aktuell JID använt vid export-tillfället. Om en JID bytt Alias flera gånger mellan exporttillfällen har detta inte kunnat fastställas.

Efter deduplicering av innehållet har därför varje enskilt meddelande som avsänts från en i ärendet förekommande JID kunnat förses med det Alias JID:en använt för detta meddelande.

4.7 Dekodning och presentation av källmaterial

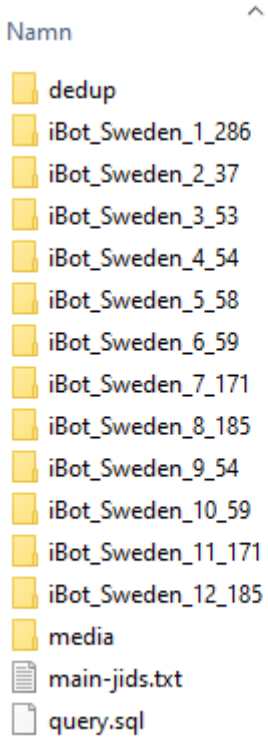
Samtliga TSV-filer med rådata från databasexport och all hänvisat media har levererats till förundersökning för vidare analys.

Förutom detta har även resultatet av deduplicering och Alias-information levererats i egna TSV-filer.

För att underlätta läsning av materialet har varje TSV-fil konverterats till Excel-format. I detta har Base64-texten konverterats till läsbar text samt länkar till hänvisat media infogats. Dessa Excel-filer har även försetts med en rubrikrad. Följande kataloger och filer återfinns:

- En katalog per databas där material extraherats. Dessa har försetts med löpnummer 1-12.
- En katalog med resultat av deduplicering och Alias-innehåll.
- En katalog innehållandes media som aktuell JID skickat och tagit emot

- En text-fil ”main-jids.txt” där aktuell JID framgår.
- En sql-fil ”query.sql” som innehåller den databasfråga som ställts för att generera TSV-filer.



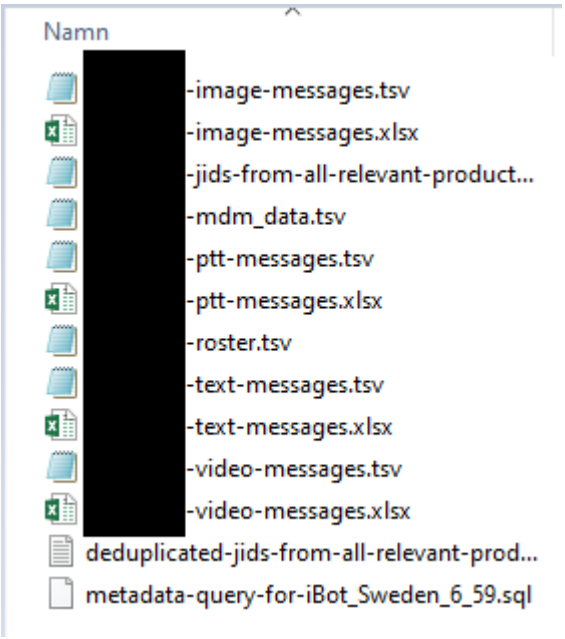
Figur 4 Katalogstruktur exporter

Nedan följer en beskrivning av innehållet i ovan nämnda kataloger.

4.7.1 Per databas

Följande filer återfinns i varje katalog med databasexporter. Dessa finns alltid som TSV oavsett om filen har innehåll eller inte och är ett direkt resultat av databasexport.

Om filen har innehåll har det även skett en konvertering till ett format som är läsbart i Excel. I de fallen har varje fält försetts med en rubrikrad.



Figur 5 Innehåll per databas för en JID. Denna JID har maskerats.

Kolumnerna är uppbyggda på följande vis:

<TABELL>_<FÄLT>

T.ex. innehåller kolumnen “HAS_MESSAGE_MID” fältet ”*mid*”, hämtat från tabellen ”*has_message*” i aktuell databas. Fördjupad information om innehållet i fälten återfinns i [1]

Nedan återfinns beskrivning över innehåll i TSV-filer. Dessa fält är tabb-separerade. Om ett värde inte finns för fältet representeras detta med ”\N”.

I Excel-versioner av dokumenten har informationen försetts med rubrikrad. I Excelfiler innehållandes meddelanden har hänvisning till media försetts med klickbar hyperlänk till aktuellt media.

För fältordning i TSV-filer, se bilaga 2.

4.7.1.1 <JID>-image-messages & <JID>-video-messages

Innehåller samtliga meddelanden och metadata innehållandes bild- respektive videomaterial där aktuell JID varit sändare eller mottagare.

4.7.1.2 <JID>-text-messages

Innehåller samtliga meddelanden och metadata innehållandes text-material där aktuell JID varit sändare eller mottagare.

4.7.1.3 <JID>-ptt-messages

Innehåller samtliga meddelanden och metadata innehållandes ljud-material där aktuell JID varit sändare eller mottagare.

4.7.1.4 <JID>-jids-from-all-relevant-products

Innehåller samtliga JID:ar som förekommer i exporterat material. Denna information återfinns även deduplicerat i en separat textfil ”deduplicated-jids-from-all-relevant-products.txt”

4.7.1.5 <JID>-mdm_data

Innehåller samtlig tillgänglig Mobile Device Management-information för aktuell JID

4.7.1.6 <JID>-roster

Innehåller samtlig tillgänglig roster-information för aktuell JID

4.7.1.7 Metadata-query-for-<databas>.sql

Innehåller den SQL-fråga som ställts mot aktuell databas för att extrahera informationen till Roster och MDM.

4.7.2 Dedup

I katalogen dedup återfinns resultatet av deduplicering och tillfogande av Alias-information på meddelanden. I de fall ett deduplicerat meddelande har flera värden i något av fälten är dessa separerade med semikolon. Fältrubriker i TSV-filer är identiska med de icke deduplicerade filerna. En kolumn ”SENDER_ALIAS” har lagts till efter ordinarie kolumner i varje fil. Denna kolumn innehåller det Alias den JID som är aktuell för exporten använt i enlighet med kap 4.6.
I katalogen finns även en fil *main-alias.tsv* som innehåller tre kolumner:

- Alias
- JID
- mid

Detta är en förteckning över samtliga Alias aktuell JID använt på aktuellt meddelande (mid). Denna är samma mid som återfinns i kolumnerna
HAS_MESSAGE_MID
MESSAGE_MID

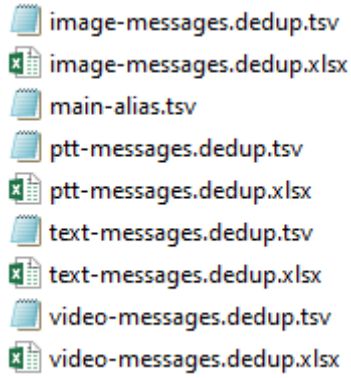


Fig 6, Innehåll dedup

En eventuell felkälla till dessa Alias är om aktuell JID bytt Alias under tiden mellan exporter har detta inte registrerats, se 4.6

4.7.3 Media

Innehåller tre kataloger, audio, images, videos. Dessa innehåller de ljudklipp, bilder och filmklipp som har skickats i meddelanden. Dessa hänvisas till genom ett Universally Unique IDentifier (UUID) [6]

5 Källförteckning

[1] https://polisen.se/aktuellt/nyheter/2021/juni/155-frihetsberovade-i-storsta-insatsen-hittills-mot-organiserad-brottslighet/ [Hämtat 2021-10-07]

[2] Teknisk information om Operation Trojan Shield [Översatt version, senast uppdaterad 31 augusti 2021]

[3] MySQL 8.0 Reference Manual, What is MySQL? https://dev.mysql.com/doc/refman/8.0/en/what-is.html [Hämtat 2021-09-21]

[4] MySQL 8.0 Reference Manual, Data Types https://dev.mysql.com/doc/refman/8.0/en/blob.html [Hämtat 2021-09-21]

[5] IETF RFC 3548, https://datatracker.ietf.org/doc/html/rfc3548 [Hämtat 2021-09-21]

[6] IETF RFC 4122, https://datatracker.ietf.org/doc/html/rfc4122 [Hämtat 2021-09-23]

6 Bilagor

Bilaga 1 – Data_information.txt

The following is information about the data stored on this drive.

Contained on this drive are the following files/directories:

- data_information.txt
- <countryname_number>_jids.txt
- <countryname_number>_dump.sql
- attachments/
  - images
  - videos
  - audio

The attachment_log.txt contains the attachments that were included in the export. If 'success' is shown next to the attachment filename, this means the attachment will be in the attachments directory. If 'failure' is next to the attachment filename, we do not have the attachment.

The sql dump contains the following schema, this has been commented explaining the fields, many of the fields are replicated or obvious:

```
CREATE TABLE `has_message` (
  `pid` int(11) NOT NULL,                    //product ID
  `mid` int(11) NOT NULL,                    //message ID
  `type` varchar(20) NOT NULL,               //1 is text, 2 is image, 3 is ptt, 4 is video
  `shmid` varchar(50) DEFAULT NULL,
 PRIMARY KEY (`pid`,`mid`,`type`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;

CREATE TABLE `image_message` (
  `mid` int(11) NOT NULL,                          //message ID
  `shmid` varchar(50) NOT NULL,                    //message UUID
  `path` varchar(100) NOT NULL,                    //image file name
  `inserted` timestamp NOT NULL DEFAULT current_timestamp(),
  `mcc` varchar(20) NOT NULL,
  `isgrp` int(2) NOT NULL DEFAULT 0,               //if it's from a group message
  `isatt` int(2) NOT NULL DEFAULT 0,
  `sender` varchar(50) NOT NULL,
  `receiver` varchar(50) NOT NULL,
  `time` timestamp NOT NULL DEFAULT current_timestamp(),
  `fromnote` int(2) NOT NULL DEFAULT 0,            //if it's from a note attachemt
  `latitude` varchar(512) DEFAULT NULL,
  `longitude` varchar(512) DEFAULT NULL,
```

```
  `metadataverified` int(2) NOT NULL DEFAULT 0,
  PRIMARY KEY (`mid`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
CREATE TABLE `mdm_data` (
  `jid` varchar(50) NOT NULL,
  `imei` varchar(50) DEFAULT NULL,
  `imsi` varchar(50) DEFAULT NULL,
  `regdate` timestamp NOT NULL DEFAULT '0000-00-00 00:00:00',
  `lastcheckin` timestamp NOT NULL DEFAULT '0000-00-00 00:00:00',
  `make` blob DEFAULT NULL,
  `model` blob DEFAULT NULL,
  `currentmcc` varchar(20) DEFAULT NULL,
  `currentcc` varchar(20) DEFAULT NULL,
  `currentoperator` blob DEFAULT NULL,
  `currentphone` varchar(20) DEFAULT NULL,
  `devicelocale` blob DEFAULT NULL,
  `ipaddr` varchar(50) DEFAULT NULL,
  `lastlat` varchar(512) DEFAULT NULL,
  `lastlong` varchar(512) DEFAULT NULL,
  `lastlocdate` timestamp NOT NULL DEFAULT '0000-00-00 00:00:00',
  `lastwifi` blob DEFAULT NULL,
  `status` varchar(512) DEFAULT NULL,
  `serialnum` varchar(50) DEFAULT NULL,
  `iccid` varchar(100) DEFAULT NULL,
  PRIMARY KEY (`jid`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1;
CREATE TABLE `products` (
  `case_id` int(11) NOT NULL,                    //syndicate ID
  `pid` int(20) NOT NULL AUTO_INCREMENT,         //product ID
  `date_created` timestamp NOT NULL DEFAULT current_timestamp(),
  `mcc_str` blob NOT NULL,
  `jid_str` blob NOT NULL,
  `count` int(11) NOT NULL DEFAULT 0,            //num messages in product
  `jid_1` varchar(50) DEFAULT NULL,
  `jid_2` varchar(50) DEFAULT NULL,
```

```
  `gid` varchar(100) DEFAULT 'NULL',
  `isDup` int(2) NOT NULL DEFAULT 0,                    //is it a duplicate product
  `knownGroup` int(11) DEFAULT NULL,
  `apk` varchar(100) DEFAULT NULL,
  PRIMARY KEY (`pid`),
  KEY `idx_products_pid` (`pid`),
  KEY `idx_products_jid1` (`jid_1`),
  KEY `idx_products_jid2` (`jid_2`)
) ENGINE=InnoDB AUTO_INCREMENT=677525 DEFAULT CHARSET=utf8mb4;
CREATE TABLE `ptt_message` (
  `mid` int(11) NOT NULL,
  `shmid` varchar(50) NOT NULL,
  `path` varchar(100) NOT NULL,
  `length` varchar(20) DEFAULT NULL,
  `pitch` varchar(10) NOT NULL,                         //original pitch of the ptt message
  `inserted` timestamp NOT NULL DEFAULT current_timestamp(),
  `mcc` varchar(20) NOT NULL,
  `isgrp` int(2) NOT NULL DEFAULT 0,
  `isatt` int(2) NOT NULL DEFAULT 0,
  `sender` varchar(50) NOT NULL,
  `receiver` varchar(50) NOT NULL,
  `time` timestamp NOT NULL DEFAULT current_timestamp(),
  `latitude` varchar(512) DEFAULT NULL,
  `longitude` varchar(512) DEFAULT NULL,
  `metadataverified` int(2) NOT NULL DEFAULT 0,
  PRIMARY KEY (`mid`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
CREATE TABLE `roster` (
  `jid` varchar(50) NOT NULL,
  `uname` blob NOT NULL,          //user assigned name
  `real_name` blob DEFAULT NULL,  //attribuited name by monitors
  `bio` blob DEFAULT NULL,
  `location` blob DEFAULT NULL,
  PRIMARY KEY (`jid`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

```
CREATE TABLE `text_message` (
  `mid` int(11) NOT NULL,
  `shmid` varchar(50) NOT NULL,
  `text` mediumblob NOT NULL,                //text of the message
  `inserted` timestamp NOT NULL DEFAULT current_timestamp(),
  `mcc` varchar(20) NOT NULL,
  `isgrp` int(2) NOT NULL DEFAULT 0,
  `isatt` int(2) NOT NULL DEFAULT 0,
  `sender` varchar(50) NOT NULL,
  `receiver` varchar(50) NOT NULL,
  `time` timestamp NOT NULL DEFAULT current_timestamp(),
  `fromnote` int(2) NOT NULL DEFAULT 0,
  `latitude` varchar(512) DEFAULT NULL,
  `longitude` varchar(512) DEFAULT NULL,
  `verified` int(2) NOT NULL DEFAULT 0,
  `isfwd` int(2) NOT NULL DEFAULT 0,
  PRIMARY KEY (`mid`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
CREATE TABLE `video_message` (
  `mid` int(11) NOT NULL,
  `shmid` varchar(50) NOT NULL,
  `path` varchar(100) NOT NULL,
  `inserted` timestamp NOT NULL DEFAULT current_timestamp(),
  `mcc` varchar(20) NOT NULL,
  `isgrp` int(2) NOT NULL DEFAULT 0,
  `isatt` int(2) NOT NULL DEFAULT 0,
  `sender` varchar(50) NOT NULL,
  `receiver` varchar(50) NOT NULL,
  `time` timestamp NOT NULL DEFAULT current_timestamp(),
  `latitude` varchar(512) DEFAULT NULL,
  `longitude` varchar(512) DEFAULT NULL,
  `metadataverified` int(2) NOT NULL DEFAULT 0,
  PRIMARY KEY (`mid`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

Bilaga 2 – Fältordning TSV-Filer

<JID>-image-messages & <JID>-video-messages

Följande fältordning återfinns i TSV-fil:
HAS_MESSAGE_PID
HAS_MESSAGE_MID
HAS_MESSAGE_TYPE
HAS_MESSAGE_SHMID
MESSAGE_MID
MESSAGE_SHMID
MESSAGE_PATH
MESSAGE_INSERTED
MESSAGE_MCC
MESSAGE_ISGRP
MESSAGE_ISATT
MESSAGE_SENDER
MESSAGE_RECEIVER
MESSAGE_TIME
MESSAGE_FROMNOTE
MESSAGE_LATITUDE
MESSAGE_LONGITUDE
MESSAGE_METADATAVERIFIED
PRODUCTS_CASE_ID
PRODUCTS_PID
PRODUCTS_DATE_CREATED
PRODUCTS_MCC_STR
PRODUCTS_JID_STR
PRODUCTS_COUNT
PRODUCTS_JID_1
PRODUCTS_JID_2
PRODUCTS_GID
PRODUCTS_ISDUP
PRODUCTS_KNOWNGROUP
PRODUCTS_APK

<JID>-text-messages

Följande fältordning återfinns i TSV-fil:
HAS_MESSAGE_PID
HAS_MESSAGE_MID
HAS_MESSAGE_TYPE
HAS_MESSAGE_SHMID
MESSAGE_MID
MEE_SHMID
MESSAGE_CONTENT
MESSAGE_INSERTED
MESSAGE_MCC
MESSAGE_ISGRP
MESSAGE_ISATT
MESSAGE_SENDER
MESSAGE_RECEIVER
MESSAGE_TIME
MESSAGE_FROMNOTE
MESSAGE_LATITUDE
MESSAGE_LONGITUDE
MESSAGE_METADATAVERIFIED
MESSAGE_ISFWD
PRODUCTS_CASE_ID
PRODUCTS_PID
PRODUCTS_DATE_CREATED
PRODUCTS_MCC_STR
PRODUCTS_JID_STR
PRODUCTS_COUNT
PRODUCTS_JID_1
PRODUCTS_JID_2
PRODUCTS_GID
PRODUCTS_ISDUP
PRODUCTS_KNOWNGROUP
PRODUCTS_APK

<JID>-ptt-messages

Följande fältordning återfinns i TSV-fil:
HAS_MESSAGE_PID
HAS_MESSAGE_MID
HAS_MESSAGE_TYPE
HAS_MESSAGE_SHMID
MESSAGE_MID
MESSAGE_SHMID
MESSAGE_PATH
MESSAGE_LENGTH
MESSAGE_PITCH
MESSAGE_INSERTED
MESSAGE_MCC
MESSAGE_ISGRP
MESSAGE_ISATT
MESSAGE_SENDER
MESSAGE_RECEIVER
MESSAGE_TIME
MESSAGE_LATITUDE
MESSAGE_LONGITUDE
MESSAGE_METADATAVERIFIED
PRODUCTS_CASE_ID
PRODUCTS_PID
PRODUCTS_DATE_CREATED
PRODUCTS_MCC_STR
PRODUCTS_JID_STR
PRODUCTS_COUNT
PRODUCTS_JID_1
PRODUCTS_JID_2
PRODUCTS_GID
PRODUCTS_ISDUP
PRODUCTS_KNOWNGROUP
PRODUCTS_APK

<JID>-mdm_data

Följande fältordning återfinns i TSV-fil:
MDM_JID
MDM_IMEI
MDM_IMSI
MDM_REG_DATE
MDM_LAST_CHECKIN
MDM_MAKE
MDM_MODEL
MDM_CURRENT_MCC
MDM_CURRENT_CC
MDM_CURRENT_OPERATOR
MDM_CURRENT_PHONE
MDM_DEVICE_LOCALE
MDM_IPADDR
MDM_LAST_LAT
MDM_LAST_LONG
MDM_LAST_LOC_DATE
MDM_LAST_WIFI
MDM_STATUS
MDM_SERIAL_NUM
MDM_ICCID

<JID>-roster

Följande fältordning återfinns i TSV-fil:
JID
SENDER_ALIAS
REAL_NAME
BIO
LOCATION

Bilaga 3 Exempel databasfrågor

Vid varje enskild export av JID ställs följande frågor mot varje enskild databas. Resultatet flyttas sedan till tidigare beskrivna kataloger

Bild-meddelanden

```
SELECT *
FROM has_message
INNER JOIN image_message ON image_message.mid = has_message.mid
LEFT JOIN products ON has_message.pid = products.pid
WHERE convert(jid_str USING utf8) LIKE '%<JID>%'
INTO OUTFILE '/var/lib/mysql-files/<JID>-image-messages.tsv';
```

Ljud-meddelanden

```
SELECT *
FROM has_message
INNER JOIN ptt_message ON ptt_message.mid = has_message.mid
LEFT JOIN products ON has_message.pid = products.pid
WHERE convert(jid_str USING utf8) LIKE '%<JID>%'
INTO OUTFILE '/var/lib/mysql-files/<JID>-ptt-messages.tsv';
```

Text-meddelanden

```
SELECT has_message.pid, has_message.mid, has_message.type, has_message.shmid, text_message.mid,
text_message.shmid, TO_BASE64(text_message.text) AS base_64text, text_message.inserted,
text_message.mcc, text_message.isgrp, text_message.isatt, text_message.sender, text_message.receiver,
text_message.time, text_message.fromnote, text_message.latitude, text_message.longitude,
text_message.verified, text_message.isfwd, products.case_id, products.pid, products.date_created, prod-
ucts.mcc_str, products.jid_str, products.count, products.jid_1, products.jid_2, products.gid, products.isDup,
products.knownGroup, products.apk
FROM has_message
INNER JOIN text_message on text_message.mid = has_message.mid
LEFT JOIN products on has_message.pid = products.pid
WHERE convert(jid_str USING utf8) LIKE '%<JID>%'
INTO OUTFILE '/var/lib/mysql-files/<JID>-text-messages.tsv';
```

Video-meddelanden

```
SELECT *
FROM has_message
INNER JOIN video_message on video_message.mid = has_message.mid
LEFT JOIN products on has_message.pid = products.pid
WHERE convert(jid_str USING utf8) LIKE '%<JID>%'
INTO OUTFILE '/var/lib/mysql-files/<JID>-video-messages.tsv';
```

Deltagande JID:ar

```
select convert(jid_str USING utf8) as jid_str_utf8
from products
WHERE convert(jid_str USING utf8) LIKE '%<JID>%'
GROUP BY jid_str_utf8
INTO OUTFILE '/var/lib/mysql-files/<JID>-jids-from-all-relevant-products.tsv';
```

polisen.se

Polismyndigheten
Telefon 114 14
e-post kansli.registrator@polisen.se

Polisen

Polisen

PM

Datum
2021-11-19

Informationsklass
Öppen information

Diarienr (åberopas)
A673.978/2021

Polismyndigheten
Nationellt Forensiskt Centrum
Linköping

Positionsdata i meddelanden skickade med applikationen ANØM

Detta är en analys av hur applikationen ANØM hämtar positionsdata som sedan visas tillsammans med ett specifikt meddelande. Funktionen finns till viss del beskrivet i dokumentet Teknisk information om Operation Trojan Shield (OTS) [1]. De positioner som är uppenbart felaktiga, exempelvis när ett av positionsvärdena är ett heltal, omfattas inte av denna analys.

> Platsinformation – Efter en uppdatering av appen i april 2020 försökte appen ta fram platsinformation via Androids API Location Manager. Om det gick att fastställa en plats inkluderades latitud, longitud, noggrannhet och tidpunkten för platsbestämningen som metadata med meddelandet för användning av brottsbekämpande myndigheter. Ibland kunde appen inte hitta en fullständig och korrekt GPS-plats. När det hände inleddes den hämtade GPS-punkten ofta med siffrorna 39,0 och pekade på en plats utanför Fijis kust i södra Stilla Havet.
>
> **Punkt 65.d under avsnitt A.8.2 i Teknisk information om OTS [1]**

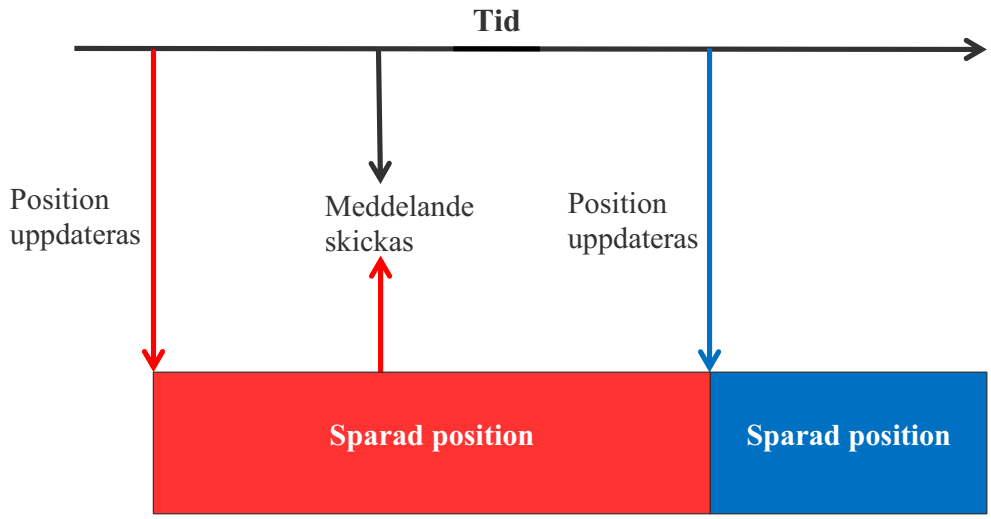
Teknisk analys

Android Location Manager ger en applikation access till systemets platstjänster. Enligt [1] använder ANØM-applikationen denna funktion sedan april 2020. Efter analys av applikationen[1] kan det konstaterats att för att få positionsdata används metoden `requestLocationUpdates` i Android Location Manager. Metoden är väldokumenterad och beskrivs nedan.

> Det kan ta lite tid att få den första platsuppdateringen beroende på de förhållanden som enheten befinner sig i. För att dra fördel av sparade positioner kan applikationen överväga att använda metoderna getLastKnownLocation eller getCurrentLocation.
>
> **Förklaring av metoden requestLocationUpdates [2]**

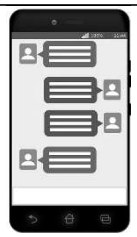
Applikationen får periodvis uppdateringar om enhetens position från Android-systemet (se Figur 1). När ett meddelande skickas är positionen som skickas med den senast mottagna. För att bestämma position i ANØM-applikationen används både signaler från lokala nätverk och GPS. Två scenarion på hur enheten uppdaterar senast kända position är visualiserade i Tabell 1 och Tabell 2.

[1] Anom-applikationen har uppdaterats flertalet gånger. Analys har utförts på en enskild version. Bedömningen av NFC är att detta inte påverkar slutsatsen i detta dokument.

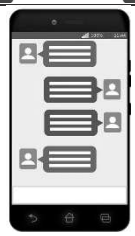


Figur 1 - När ett meddelande skickas används den senast sparade positionen

Tabell 1 - Exempel där koordinater överensstämmer

Exempel 1		**Tid**
Person A befinner sig på ett kafé i Västerås.		2021-05-01 15:00
Telefonen får en automatisk uppdatering om nuvarande position via GPS. Koordinaterna 59.61080, 16.54971 (Västerås) sparas i telefonens ”senast kända position”.		2021-05-01 15:10
Person A sitter fortfarande på kaféet och skriver ett meddelande i applikationen ANØM. Applikationen hämtar uppgiften om ”senast kända position” och skickar koordinaterna tillsammans med meddelandet. Genom att Person A fortfarande befinner på kaféet så stämmer koordinaterna i meddelandet bra överens med den plats från där meddelandet skickas.		2021-05-01 15:20

Tabell 2 - Exempel där koordinater inte överensstämmer

Exempel 2		Tid
Person B befinner sig vid Kalmar centralstation.		2021-06-10 10:00
Telefonen får en automatisk uppdatering om nuvarande position via GPS. Koordinaterna 56.66146, 16.36004 (Kalmar) sparas i telefonens ”senast kända position”.		2021-06-10 10:06
Person A kliver på ett tåg till Göteborg. Under resan har telefonen svårt att uppdatera sin position.		
Väl framme i Göteborg sänder Person A iväg ett meddelande i applikationen ANØM. Koordinatuppgifterna i telefonens ’senast kända position” har inte uppdaterats. Person B befinner sig inte längre i Kalmar. Koordinaterna i meddelandet överensstämmer inte med den faktiska plats där meddelandet skickas ifrån.		2021-06-10 15:20
Telefonen får en automatisk uppdatering om nuvarande position via GPS. Koordinaterna 57.70677, 11.96939 (Göteborg) sparas i telefonens ”senast kända position”.		2021-06-10 15:22

Slutsats

Positionsdata som finns knutet till ett ANØM-meddelande är en sparad position som enheten befunnit sig på vid ett tidigare tillfälle. Meddelandet kan skickas från en position som skiljer sig från den position som visas i meddelandet. Utan tid när positionen uppdaterades bör positionsdata hanteras med försiktighet.

Referenser

[1] Teknisk information om Operation Trojan Shield (2021-08-31)
[2] Location Manager – Android Developers (2021-11-18). https://developer.android.com/reference/android/location/LocationManager#requestLocationUpdates(java.lang.String,%20android.location.LocationRequest,%20java.util.concurrent.Executor,%20android.location.LocationListener)

Polisen

PM

Datum 2022-01-26

Informationsklass
Öppen

Diarienr (åberopas) A053.007/2022

Polismyndigheten
Nationellt Forensiskt Centrum
Informationstekniksektionen

I dokumentet *Teknisk information om Operation Trojan Shield* [1] finns beskrivet hur ANØM-applikationen beräknade JID utifrån enhetens IMEI. Enligt dokumentet beräknades JID utifrån enhetens IMEI fram till december 2020, därefter ändrades formatet då det skedde förändringar i operativsystemet Android.

KAP. A3 punkt 18 - Teknisk information om Operation Trojan Shield [1]
Varje användare i ANØM identifieras med en unik identifierare (användar-ID), som tekniskt kallas för en Jabber Identifier (JID). Från början hade detta användar-ID formen av 6 alfanumeriska tecken (till exempel ”aab2c3”) och det genererades automatiskt från enhetens IMEI-nummer (International Mobile Equipment Identity number).

Kapitel A3 punkt 19 - Teknisk information om Operation Trojan Shield [1]
Enhetens IMEI-nummer kombinerades med en fast uppsättning tecken (en så kallad ”saltsträng”) för att skapa ett indatavärde. Indatavärdet genomgick en hashprocess i algoritmen MD5. De sista sex tecknen i det hashvärde som genererades var enhetens användar-ID och användarens lösenord var hela hashvärdet. Processen genomfördes automatiskt av ANØM-appen som använda detta användar-ID och lösenord för automatisk autentisering mot ANØM-servrarna.

Kapitel A4 punkt 23 - Teknisk information om Operation Trojan Shield [1]
På grund av förändringar i operativsystemet Android gick det från december 2020 inte längre att använda IMEI-numret till att automatiskt generera användar-ID. Formatet på användar-ID ändrades därför så att det genererades automatiskt i portalen. […]

Nationellt Forensiskt Centrum har analyserat ANØM-applikationen och tagit fram ett verktyg i två olika versioner [2, 3] för att beräkna ett potentiellt JID utifrån ett givet IMEI. Verktygets funktion har verifierats via stickprov av kända kombinationer av JID/IMEI. NFC har ingen kunskap om det finns undantag i de enheter som tilldelats JID eller vilka enheter som har den nya respektive den gamla tilldelningen av JID.

Referens

[1] Teknisk information om Operation Trojan Shield (2021-08-31)
[2] Beräkna JID från IMEI 210921.xlsm (Tidigare versioner av Office)
[3] Beräkna JID från IMEI 211119 Office2019.xlsm

Polisen

PM 1 (1)

Polismyndigheten
Nationella operativa enheten
Emil Andersson

Datum
2021-12-15

Informationsklass
BS

Diarienr (åberopas)
5000-K642266-21
5000-K1490612-20

Promemoria gällande koppling mellan JID och IMEI

Utifrån frågeställning gällande koppling mellan JID och IMEI från region Bergslagen i två förundersökningar har information sedan tidigare erhållits från FBI i USA.

Följande kopplingar kan enligt FBI göras:

5000-K642266-21
JID: 08075e IMEI: 351773114076729
JID: b1d66e IMEI: 356112100561565
JID: 6e142c IMEI: 356339112327442

5000-K1490612-20
JID: 3373c4 IMEI: 351773113342718
JID: 6afdde IMEI: 351773113608670
JID: 0f9f08 IMEI: 356339112331311

Polisen

Elektroniskt underskriven av Dan Nyberg 2021-10-13 08:05

Nationellt forensiskt centrum - NFC 1(2)
Analysbesked

Datum	Vårt diarienummer
2021-10-13	2021020626
Ert datum	Er beteckning
2021-10-06	5000-AM-174292-20

Polismyndigheten
Grova Brott PO Örebro
Lisa Rehn
Box 1804
701 18 Örebro

Uppdragsgivare
Polismyndigheten

Materialförteckning
Av materialförteckningen framgår även använd metodik.

Undersökningsmaterial

Beteckning	*Materialbeskrivning*
Ljudfiler	3 ljudfiler där en röstförvrängarfunktion önskas tas bort. Filnamn "0ca45f01-4ebb-440c-95fa-b10696201bbe-pitchfixed.wav", "954cb3dd-e364-4c8e-8ce0-ad7c2380bbb8-pitchfixed.wav", "a4b00fe7-775c-46a1-a134-b0324e725080-pitchfixed.wav". Uppdragsgivarens beteckning: Ljudfiler Forums materialnr: 202102062601 Materialhantering: Digital arkivering. Metodik: 795

Standardförfarande och metoder som har använts anges med dokumentbeteckning.
Standardförfarande och metoder som ingår i laboratoriets ackreditering enligt ISO/IEC 17025 är markerade med asterisk (*).
För förklaring av dokumentbeteckningar hänvisas till laboratoriets hemsida på IntraPolis eller Internet.
Önskas mer information kontakta ärendeansvarig.

Polismyndigheten
Nationellt forensiskt centrum - NFC
581 94 Linköping • Tel 010-562 80 20 vxl • Fax 013-14 57 15
E-post registrator.nfc@polisen.se • www.nfc.polisen.se

Polisen

Elektroniskt underskriven av Dan Nyberg 2021-10-13 08:05

Nationellt forensiskt centrum - NFC 2(2)
Analysbesked

Datum	Vårt diarienummer
2021-10-13	2021020626
Ert datum	Er beteckning
2021-10-06	5000-AM-174292-20

Ändamål
Ändamålet är att försöka få bort den eventuella röstförvrängningen som återfinns på de tre inskickade ljudfilerna.

Undersökningsrelaterad information
Undersökningsmaterialet besitter inte någon av de två förväntade röstförvrängningarna som återfinns hos ANOM applikationen. Troligen är den artefakt som kan höras på inspelningarna en teknisk defekt som uppstår vid processen av röstförvrängning och återställande av denna.

Undersökning
Det inskickade materialet har bearbetats på olika sätt för att minska inverkan av iakttagen artefakt. Dels genom addering av efterklang och ökning av hastigheten på ljudmaterialet, för att maskera inverkan av artefakten. Vidare har materialet tekniskt fönstrats-om i ett försök att minska artefaktens inverkan på ljudsignalerna.

Resultat
Ingen av de testade lösningarna har fungerat och därmed avslutas undersökningen.

Handläggning
Undersökningen har utförts av forensikern Dan Nyberg och teknikern Ronny Max.

Frågor beträffande undersökningen och eventuell kallelse till rättegång ställs i första hand till forensikern Dan Nyberg (ärendeansvarig/ansvarig handläggare), direkttelefon 010-562 84 54.

Dan Nyberg
Forensiker

Vid återgivande av denna redovisning ska detta i normalfallet göras i sin helhet. Om utdrag ur redovisningen återges i annat dokument ska detta följas av en tydlig hänvisning till ursprungsdokumentet.

Polismyndigheten
Nationellt forensiskt centrum - NFC
581 94 Linköping • Tel 010-562 80 20 vxl • Fax 013-14 57 15
E-post registrator.nfc@polisen.se • www.nfc.polisen.se

Om utdrag från ANØM

AM-174292-20

Andreas Börjesson Polisregion Bergslagen

2022-03-15

Polisen

Allmänt om ANOM och dess funktioner
Utifrån det tekniska dokument om plattformen ANOM som erhållits från FBI kan ANOM beskrivas på följande, förenklade, sätt.

För de flesta ANOM-användare fanns det inga andra sätt att kommunicera på enheterna än krypterat med andra ANOM enheter. Funktioner på mobiltelefoner, som t.ex. röst- eller videosamtal, SMS, appar för sociala medier, internetsurf och e-posttjänster, kunde inte användas. Den 8 juni 2021 var det bara 73 av ungefär 12 500 enheter som hade tilldelats specialförmågan att ringa i traditionell bemärkelse eller att surfa på internet via den installerade ToR-webbläsaren.

Varje ANOM enhet hade ett unikt ID nummer, kallat ”JID”, som inte gick att ändra. Användaren kunde välja ifall den ville ha ett Alias. Ett valt Alias gick att ändra.

Med ANOM kunde man skicka meddelanden i form av text, ljud, video och bild. Utöver det fanns det möjlighet att skicka sparade anteckningar och kontakter.

Det fanns även en funktion för att ”citera” och ”vidarebefordra” meddelande som skickats. Funktionerna fungerade liknande som på andra meddelandeapplikationer t.ex. whatsApp eller Facebook messenger.

Viss information som t.ex. bilder och anteckningar kunde sparas i ett lagringsutrymme kallat ”vault” i den fysiska enheten.

Kommunikation på ANOM skedde i vanlig chatt eller i skapade gruppchattar där ANOM enheter bjudits in att delta. För att systemet skulle särskilja gruppchattar från varandra tilldelades varje gruppchat automatiskt ett individuellt ID nummer kallat ”GID”, Grupp-ID. Den användare som skapade gruppchatten kunde manuellt döpa gruppchatten till eget valt namn så användarna lättare kunde hålla isär sina gruppchattar. Det namn som respektive gruppchat eventuellt döpts till av användare syns inte som rubrik i erhållet material från FBI.

För en fullständig och teknisk beskrivning av ANOM hänvisas till dokumentet ”Teknisk information om operation Trojan Shield”.

Om utdrag av chattar i ärendet
Det inhämtade ANOM material i ärendet är omfattande. Det finns ca 370 000 skickade meddelanden. Ett urval har gjorts för att begränsa materialet till det som bedömts vara relevant för brottet som utreds.

Innehåll från ANOM kan, likt innehåll från en sedvanlig mobiltelefon, visualiseras på olika sätt. I detta fall presenteras kommunikationen med pratbubblor. Det kan även visualiseras i exempelvis Excelformat.

Polisen

Om gruppchattar i ärendet.
Det förekommer flera gruppchattar i detta ärende och funktionen har bland annat använts för både strategisk och operativ styrning av brottsligheten. Det är två ihållande konversationer i formen ”gruppchat” som har identifierats fylla en sådan funktion. Dessa sträcker sig över hela brottsperioden, rör var för sig samma tema och involverar i stort samma personer över tid, även om någon person faller ifrån eller kommer till. De gruppchattar som löper efter varandra och som polis menar ingår i dessa två typer av konversationer presenteras som ”*Firmachatt*” respektive ”*Oilgroup*” eller ”Oljegruppen”.

Om försättsblad till utdrag
Ett försättsblad har gjorts av polis för att markera när ett nytt utdrag av chatt presenteras och för att förtydliga vad som omfattas i urvalet. Vid gruppchat har ett nytt försättsblad gjorts vardera gång ett automatiskt Grupp ID tilldelats.

Försättsbladet visar**:**

- Grupp ID nummer vid gruppchat
- Tidsperiod som urvalet avser. Dvs. all konversation under vissa dagar, under en dag eller mellan specifika klockslag.
- Alla involverade JID:ar i aktuell chat / gruppchatt
- Det eventuella Alias som förekommer under tiden för chatten.
- Vem, utifrån polisiär brukaranalys, som är identifierad som användare av aktuell JID

Om presentation av innehåll i chattutdrag.
I respektive meddelanden står först avsändande JID-nr, tidpunkt för utskick och därefter följer innehåll.

Exempel skickat text meddelande:

56d3f9 2021-06-02 07:18:12+02:00
Hej bror

Exempel vidarebefordrat meddelande:

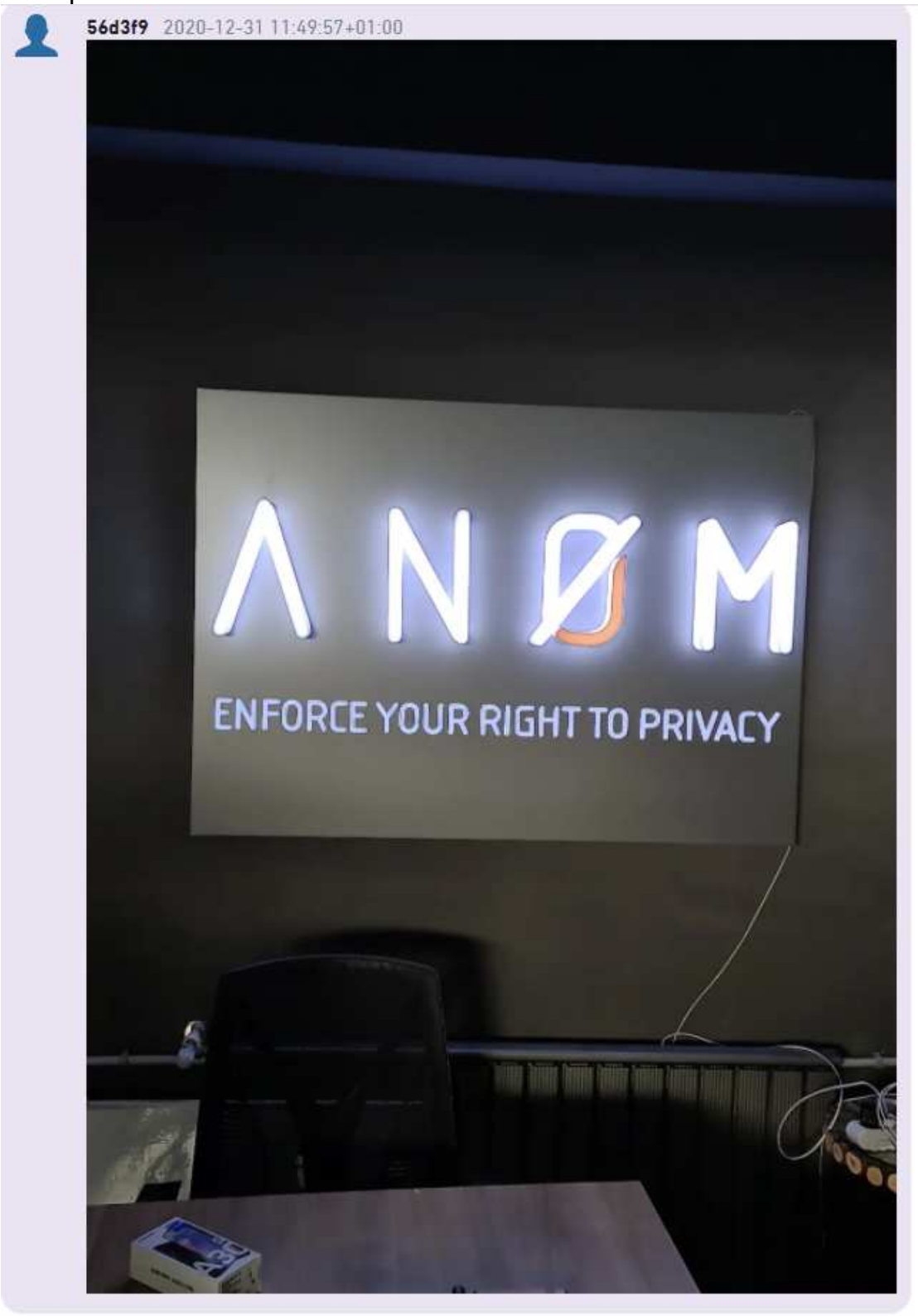
56d3f9 2021-04-09 13:33:54+02:00
forward_prefix{"forward_message_time": 1617967666148, "forward_message_user_jid": "6e4be3", "forward_message_body": "They close at 17:00", "forward_message_type": "TEXT", "forward_message_uuid": "8bb3770e-d5a9-408a-9821-2ad1c5ef6da6"}

Exempel citerat meddelande:

56d3f9 2021-04-05 12:09:49+02:00
quote_prefix{"quote_message_time":1617615372208,"quote_message_text":"Bror hur myckeg btc skicka jag till dig för tjack\n","quoted_text":"Ska kolla bror","quote_message_user_jid":"whateven","message_uid":"e6f90758-e770-41eb-8dd3-91af97ba7bef","isQuotedMessageDeleted":false,"isEdited":false}

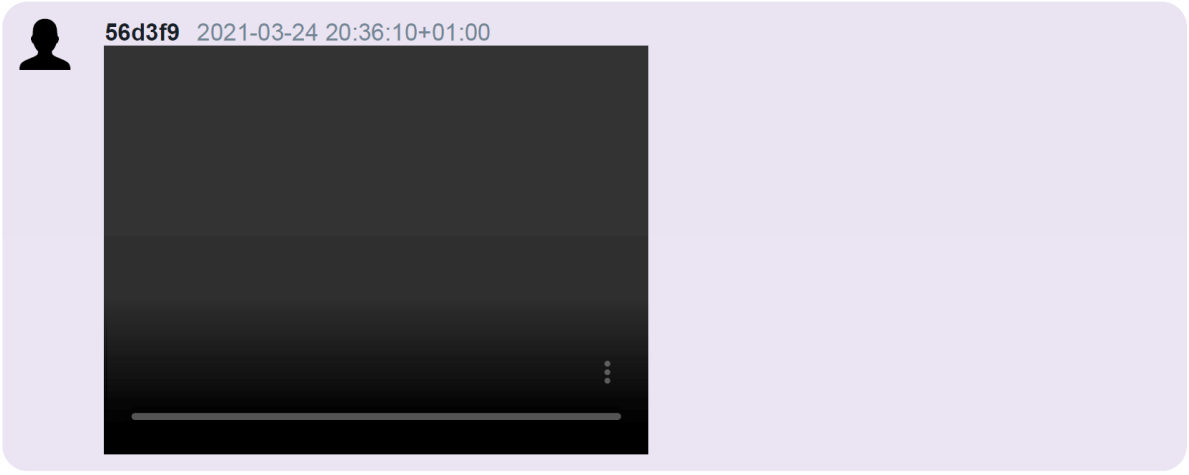
Polisen

Exempel skickad bild:



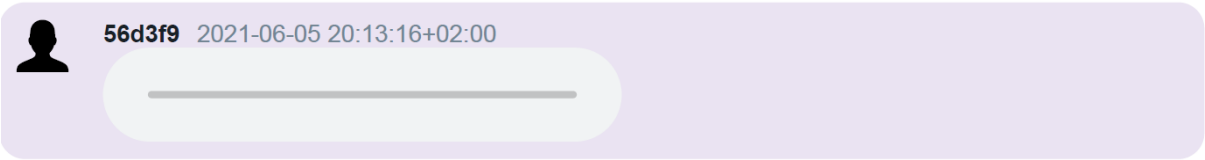
Polisen

Exempel skickad video:



Exempel skickade ljudfiler:
Skickade ljudfiler visualiseras på två olika sätt i denna presentation. Anledningen till två olika visualiseringar är tekniska begränsningar vad gäller utskrift med denna presentationsform. Det har inget med själva funktionen eller innehållet att göra.

Exempel 1



Exempel 2

Letterhead Memorandum (Rev. 02-05-15)

UNCLASSIFIED//REL TO USA, SWE

United States Department of Justice

Federal Bureau of Investigation

Tracking #: 198842817
Case File #: SD-2864529
Precedence: Routine
Date: 09-Dec-2021

Office of the Legal Attaché
United States Embassy
Dag Hammarskjölds Väg 31
SE-115 89, Stockholm

National Operations Department
International Police Cooperation Division
P.O. Box 12256
SE-102 26, Stockholm
ATTN: Liaison Officer

(U) UNLESS OTHERWISE PROVIDED HEREIN OR EXPRESSLY AUTHORIZED BY FEDERAL BUREAU OF INVESTIGATION (FBI) HEADQUARTERS IN A SEPARATE COMMUNICATION, THE INFORMATION IN THIS DOCUMENT IS FOR INTELLIGENCE AND LEAD PURPOSES ONLY, AND YOUR GOVERNMENT MAY NOT USE THE INFORMATION IN ANY LEGAL PROCEEDINGS, DISSEMINATE THE INFORMATION TO ANY OTHER GOVERNMENT, PERSON OR ENTITY, OR TAKE ANY OVERT INVESTIGATIVE STEPS (INCLUDING BUT NOT LIMITED TO FORMAL LEGAL PROCESS OR DIRECT CONTACT WITH REFERENCED PERSONS/ENTITIES OR THEIR ASSOCIATES) BASED ON THE INFORMATION IN THIS DOCUMENT.

(U//REL TO USA, SWE) To provide additional information about the United States legal authority utilized during the Trojan Shield investigation.

(U//REL TO USA, SWE) Notwithstanding the above caveat, the information in this document may be used for intelligence purposes, for overt law enforcement actions, or in legal proceedings. The information contained herein may be disseminated to other agencies within your Government as appropriate, but it may not be disseminated to third party Governments or entities without the express permission of the Federal Bureau of Investigation. Further, the Federal Bureau of Investigation makes no representations as to any additional assistance (e.g. supplementary

information, authentication, testimony) relating to this information; however, you may use this information to request additional information or assistance through your country's FBI Legal Attaché.

(U//REL TO USA, SWE) After discussions with the United States Attorney's Office (USAO), Southern District of California, the following language was drafted by the USAO to describe the legal basis for the Trojan Shield operation:

(U//REL TO USA, SWE) Operation Trojan Shield's technique of operating the Anom platform was lawful under the laws of the United States and where the platform was hosted. The vast majority of individuals who used Anom were not United States citizens and were not located in the United States. The United States Constitution's Fourth Amendment does not apply to these individuals. Additionally, none of the messages exchanged only between foreign users traversed United States infrastructure, so they did not implicate the Wiretap Act, 18 U.S.C. §§ 2510 et seq.

(U//REL TO USA, SWE) The third country that hosted the Anom server is in the European Union and the third country utilized its own judicial process to obtain a court order authorizing the copying of messages routed to the server. The third country provided the messages to the Federal Bureau of Investigation pursuant to a Mutual Legal Assistance Treaty request. Because the third country followed its laws, the United States can rely on the data obtained regarding communications between foreign users.

Sincerely,

Michael S. Butsch

Operation Trojan Shield
Technical Details

Last Updated: August 31, 2021

TABLE OF CONTENTS

1. OVERVIEW OF SERVERS AND NETWORKING 4

1.1 XMPP Server 4

1.2 Third-Party Country Server 4

1.3 Google Servers 5
1.3.1 Transfer 5
1.3.2 Proxy 5

1.4 AWS GovCloud 5
1.4.1 Security 5
1.4.2 Front-End 5
1.4.3 Ingestion-1 (I1) 5

1.5 Messaging Network Activity 5

2. NEW DATA PACKAGE CREATION 6

2.1 Encryption of Data 7

2.2 How the Difference-Dump of the Database was Created 7

2.3 How the List of Attachments is Determined Based on the Difference-Dump 8

2.4 How Attachments were Copied from File Storage 8

2.5 Creation of the Encrypted Package 8

3. TRANSFER FROM THIRD-PARTY COUNTRY SERVER TO TRANSFER SERVER 8

3.1 Program that Transfers Data to Transfer Server 9

4. TRANSFER FROM TRANSFER SERVER TO AWS GOVCLOUD 9

4.1 Automated Program to Transfer Data 9

5. ENCRYPTED PACKAGE PROCESSING 9

5.1 Decrypt GPG Package 9

5.2 Extract New MySQL Database Dump and Attachments from Archive 9

5.3 Ingest Database Dump Into Temporary Database 9

6. DECRYPTION PROCESS 9

6.1 Decryption of Encrypted Fields Within Database 9

6.1.1 Update Attachment Paths to be Correct 10

6.2 Decryption of All Attachment Files 10

7. AUDIO FILE PROCESSING 10

7.1 Convert Audio Files to Usable Format 10

7.2 Pitch Change Audio Files if Needed 10

8. DATABASE OVERVIEW 11

8.1 Cases/Syndicates 11

8.1.1 Groupings of Device Users (JIDs) 11

8.2 Review Platform Users 11

8.2.1 General Users 11

8.2.3 Super Users 11

8.2.4 Admins 11

8.3 The Roster 12

8.4 Groups 12

8.4.1 Lack of Group Information 13

8.5 Products 13

8.5.1 Products in Detail 13

8.6 Messages 14

8.6.1 Message Time Zone Discrepancy 15

8.7 Relationships 16

8.7.1 Product to Message Relationship 16

8.7.2 User to Case Access Relationship 16

8.7.3 JID to Case relationship 17

8.7.4 JID to Group Relationship 17

9. INGESTION PROCESS 17

9.1 Insert new Roster Information 18

9.2 Insert new Groups 18

9.2.1 Insert New Group Information 18

9.2.2 Insert Group Membership Updates 18

9.3 Message Ingestion *18*
9.3.1 Initialization 18
9.3.2 Insert Messages 19
9.3.4 Assigning Messages to Products 20

9.4 Product Ingestion *20*
9.4.1 Product Creation Per Case 20

9.5 Post-Ingestion Exports *21*

10. WEB APPLICATION/REVIEW PLATFORM 22

10.1 User Access Controls within Hola iBot *22*
10.1.1 Law Enforcement Enterprise Portal (LEEP) Access Control 22
10.1.2 Hola iBot Access Control 22

10.2 Cases in Hola iBot *24*
10.2.1 Case Homepage 24

10.3 Products Page *25*

10.4 Product Page *28*
10.4.1 Group ID Display 29
10.4.2 Attachment Messages (PTT, Image, Video, Note) in Hola iBot 29
10.5 Translations 32

10.6 Roster Page *34*

10.7 JID Profile *35*
10.7.1 Information About the Device User (JID) 36

10.8 Other Pages *40*
10.8.1 Search 40
10.8.2 Search Notes 41
10.8.3 All Images 41
10.8.4 Blocked 42

11. MLAT EXPORTING 42

11.1 All Attachment Files Pulled Down *42*

11.2 Final MySQL Database Dump Pulled Down *42*

11.3 MLAT Export Creation *42*

APPENDIX A 43

A.1 Public Key cryptography *43*

A.2 Hashes *43*

A.3 THE ANØM PLATFORM *44*
A.3.1 End-to-end encryption 44

A.4 The Provisioning Portal *45*

A.5 Handsets *46*

A.5 Network connectivity to the platform *47*
A.6 The Mobile Device Management Component *47*
A.7 The ANØM Application *48*
A.8 Data Recorded from the Platform *52*
A.8.2 Message meta-data 53
A.9 Authenticity and Integrity *53*

1. OVERVIEW OF SERVERS AND NETWORKING

Operation Trojan Shield (OTS) required servers at several levels to provide data transfer, storage, and review.

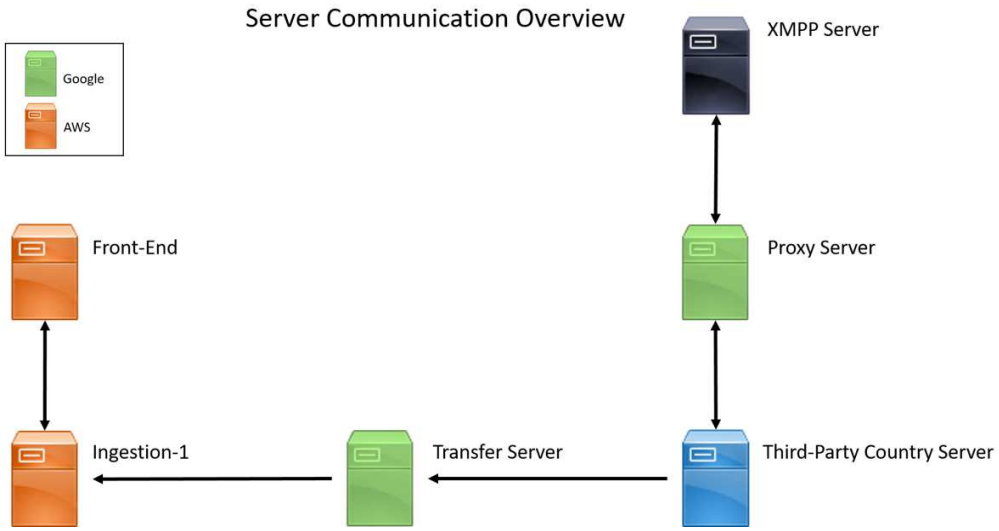


Diagram 1.A

1.1 XMPP Server

XMPP is an open standard protocol for instant messaging, which can facilitate multi-party chats, supporting multimedia such as voice, images, and video. Anyone is free to run their own XMPP server and network and build upon the framework that is provided. The ANØM app included a feature whereby when a message was sent, the app, via XMPP server, automatically sent a 'blind carbon copy' of the message to a ghost user ID, 'bot'. This process was not visible to the sending user, nor were they aware that this process occurred.

1.2 Third-Party Country Server

A server was provisioned by law enforcement from a third-party country in October of 2019 for collecting the blind carbon copy messages sent to the ‘bot’ ghost user as referenced in Appendix A.8 - 59. This server was owned, operated, and maintained by the third-party country until the end of the operation.

1.3 Google Servers

A covert Google Cloud account was provisioned for the creation of Google Compute Engines, a service that Google Cloud provides to create and run virtual machines within Google Cloud, needed for transferring data and providing a proxy server for the third-party country's server.

1.3.1 Transfer

The transfer server was a configured Google Compute Engine. Its only purpose was to transfer data received from the third-party country's server, into the Ingestion-1 (I1) server within AWS GovCloud.

1.3.2 Proxy

The proxy server was provisioned as a Google Compute Engine. The server acted as a relay of all messages between the ANØM network (XMPP server) and the third-party country's collection server. This provided private communications to the ANØM network from the third-party server.

1.4 AWS GovCloud

Within AWS GovCloud West, two Elastic Compute Cloud (EC2) servers were provisioned, operated and maintained for OTS.

1.4.1 Security

The AWS environment is scanned on a monthly basis for vulnerabilities and other misconfigurations that could pose as threats. Each EC2 server within AWS GovCloud runs a hardened version of the CentOS operating system. Both EC2 servers are also scanned and patched for vulnerabilities. The vulnerability scanning and patching is performed in accordance with Security Technical Implementation Guides (STIGs) that the Defense Information Systems Agency (DISA) publishes.

1.4.2 Front-End

The front-end server was designated as the web server for the Hola iBot review application. More details on the Hola iBot review application can be found in section 10.

1.4.3 Ingestion-1 (I1)

Ingestion-1 (I1) was the destination of new data packages from the third-party country's server for processing and review. It also operates as a database and file server for the display and review of data.

1.5 Messaging Network Activity

As mentioned in Appendix A.8 - 59, the data collected from the platform was received as "blind carbon copy" messages. Diagram 1.B shows an overview of the networking data flow for the collection of these messages.

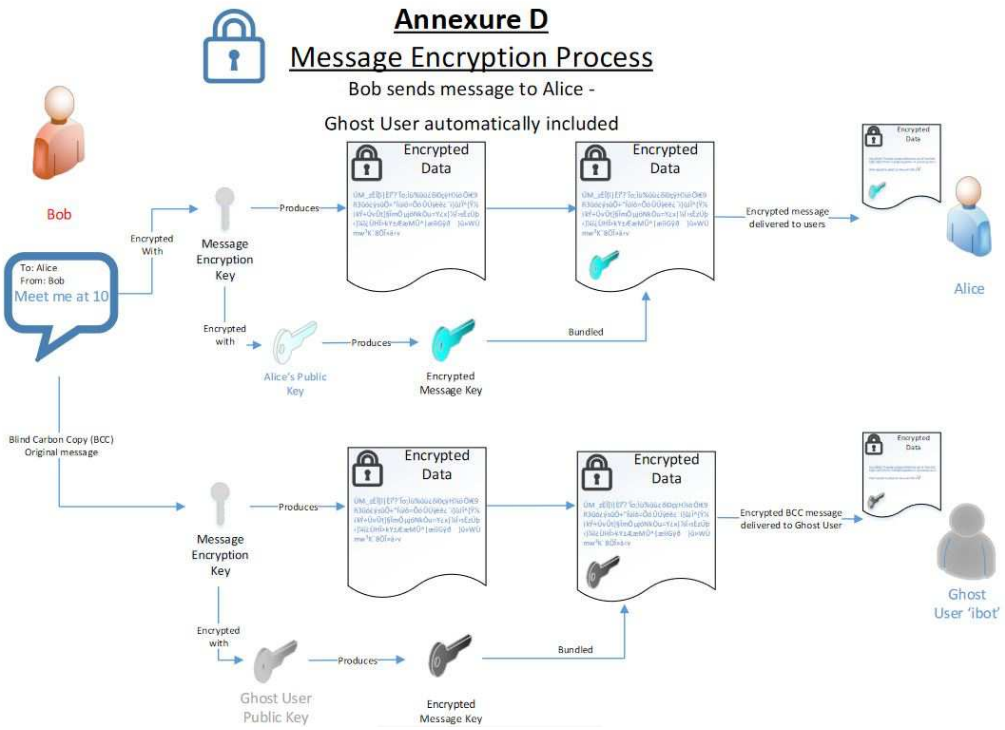


Diagram 1.B

2. NEW DATA PACKAGE CREATION

A mutual legal assistance treaty (MLAT) allowed for transfer of data every Monday, Wednesday, and Friday from the third-party country. A process to obtain only new data was developed and provided for use by the third-party country. The following is a list of data that was processed into the new data packages to be sent:

- MySQL Database Items:
  - Messages
    - A Unique Message ID
      - UUID that uniquely identifies an individual message
    - Sender
      - The User ID (JID) of the sending user
    - Receiver
      - The User ID (JID) or Group ID (GID) of the receiving entity
    - Location information
      - Latitude and Longitude would be attached to each message (if the device provides it).
      - If location information is provided, it will be encrypted.
    - Mobile Country Code (MCC)
      - The MCC that the message was sent from
    - Time
      - The time the message was sent according to section 8.6.1

        - Audio Pitch Adjustment
            - If the message was a Push-To-Talk (ptt) message, a value was sent along with the attachment that provides a way to reverse the pitch adjustment performed on the app as referenced in Appendix A.7.1.4 – 57)
        - Type
            - Each message could be one of the following:
                - text, forwarded, contact
                    - Designates that the 'content' field will contain encrypted text
                - ptt, video, image, note
                    - Designates that the 'content' field will contain the path of the file sent by the sender with the file name [Unique Message ID].[attachment extension]
        - Content
            - If the message type was 'text', 'contact', or 'forwarded', the content was encrypted
            - If the message type was 'ptt', 'video', 'image', or 'note', the field had the plaintext path of the attachment sent
    - Roster
        - Device User ID (JID)
            - A unique identifier for a device user
        - Nickname
            - Encrypted, user-entered nickname
    - Group Information
        - Group ID (GID)
            - A unique identifier for a group of devices
        - Group Name
            - Encrypted, user-entered name of the group
- Files
    - Audio, Image, Video, and Note files were named as the following: [Unique Message ID].[attachment extension]

2.1 Encryption of Data

The data received (attachments, content/text messages, location information, nicknames, and group names) was encrypted using the end-to-end encryption scheme as described in the Extensible Messaging and Presence Protocol (XMPP). On the third-party country's server, the data was decrypted in temporary storage (RAM) upon receipt, and the data was encrypted again using a combination of RSA asymmetric encryption and AES symmetric encryption before being written to disk. No plaintext data was stored on the third-party country's server. The private key for decrypting (in regards to RSA) was stored on the I1 server within AWS GovCloud.

2.2 How the Difference-Dump of the Database was Created

The process to obtain new data included finding only new data in the MySQL database (see above for list of entities obtained from the database) between the last full database dump and the new/current full database dump, internally called a "difference-dump". The process started by creating a new MySQL database dump. A program used the database dump taken from the previous transfer and the new database dump as input. The program performed a difference between the previous database dump

and the current, which generated a MySQL dump with only new data. Reference Diagram 2.A for a visual representation of the process.

2.3 How the List of Attachments is Determined Based on the Difference-Dump

The process used the difference-dump to gather the new attachments by referencing the 'content' field of all messages that have paths. See section 2 for more information about where paths are stored as entities. As mentioned previously, the file names were placed in the 'content' field if the type was not 'text', 'contact', or 'forwarded'.

2.4 How Attachments were Copied from File Storage

Attachments were stored in an encrypted state directly on the server, and the program that retrieved the new attachments utilized the path from the 'content' field as referenced in section 2.3, and copied the attachments to a temporary storage location for packaging.

2.5 Creation of the Encrypted Package

In order to package the MySQL dump with new data and attachments, the files were compressed into an archive file with the extension '.tar.gz'. The archive file was encrypted with GnuPG (GPG) asymmetric encryption, which appended the extension '.gpg' to the end of the archive. After the encrypted package was properly constructed, it was hashed using the MD5 hashing algorithm. A hash function is a mathematical process whereby the data input, or 'message', is processed into a 'message digest' or hash value of fixed length. It is commonly represented as hexadecimal characters which consist of the numbers 0 to 9, and letters A-F. Hash functions are often used for data verification to identify if data has been altered, due to the very high improbability that two different input 'messages' will result in the same hash value. The MD5 hash was saved to a file to be transferred. Diagram 2.A demonstrates an overview of the packaging process.

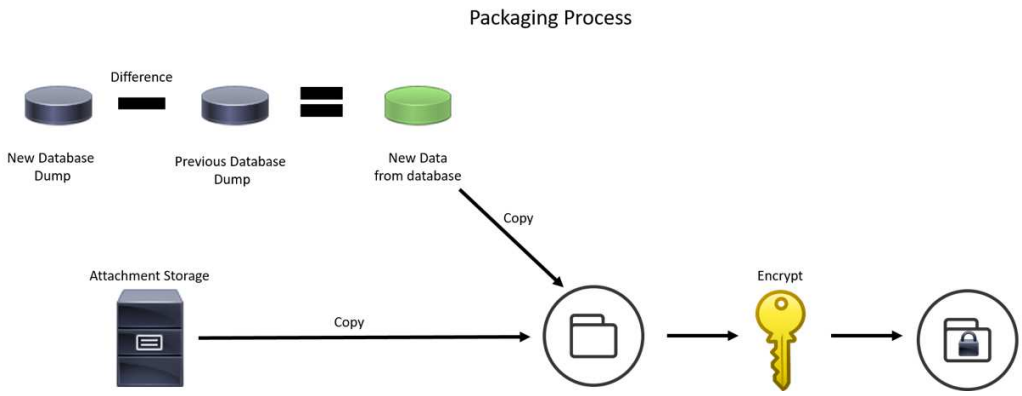


Diagram 2.A

3. TRANSFER FROM THIRD-PARTY COUNTRY SERVER TO TRANSFER SERVER

A program was manually run by the third-party country that performed the new-data processing as described in section 2.

3.1 Program that Transfers Data to Transfer Server

Each Monday, Wednesday, and Friday, a program was run by the third-party country that packaged and sent the new data. The program sent the MD5 hash, followed by the encrypted package of new data to the covert Google Compute Engine transfer server as referenced in section 1.3.1.

4. TRANSFER FROM TRANSFER SERVER TO AWS GOVCLOUD

The transfer server automatically forwarded the data received into the I1 server located in AWS GovCloud after checking the data integrity (verifying the hash).

4.1 Automated Program to Transfer Data

As the transfer server received new encrypted packages, it checked the inbox directory where data was uploaded for any files ending in '.gpg'. This indicated that a new package of data was ready to be transferred into I1 located in AWS GovCloud. The program then calculated the MD5 hash of the '.gpg' file, and it was compared to the result to the MD5 hash uploaded by the third-party country's server. If the hashes matched, this indicated a successful transfer, and the encrypted package was forwarded into I1 within AWS GovCloud.

5. ENCRYPTED PACKAGE PROCESSING

Each encrypted package was transferred to a designated location on I1 within AWS GovCloud. An automated task would check the location for new data. If new data was found in the location, the ingestion process would begin on the server.

5.1 Decrypt GPG Package

First, the encrypted package of MySQL data (database) and attachment files were decrypted so that the archive of data (database and message attachments) would be available. As mentioned before, GPG asymmetric encryption was used to protect the archive of data, so a private key, only available on the I1 server, was used to decrypt the package.

5.2 Extract New MySQL Database Dump and Attachments from Archive

After decryption, the archive was extracted to the file system, making the MySQL data (database) and attachments available for continued processing.

5.3 Ingest Database Dump Into Temporary Database

The I1 server utilized two databases for processing of incoming data. One of these databases, iBot_enc, was the temporary storage for new data received from the third-party country's server. This is where the new MySQL data was temporarily stored for processing. The new data needed to be decrypted, normalized, and processed into the other database so that the front-end web application, Hola iBot, had the ability to display the data.

6. DECRYPTION PROCESS

In order to decrypt and normalize the incoming data, the database dump was ingested into a database on the I1 server, as mentioned in section 5.3.

6.1 Decryption of Encrypted Fields Within Database

As mentioned in section 2, the following fields within the database dump were encrypted:

- Messages

    - Content (if type is ‘text’, ‘contact’, or ‘forwarded’)
    - Location information (if provided)
- Roster
    - Device user display name (reference section 8.3)
        - Also referred to as nickname, username, alias
- Group Info
    - Group name

The decryption process decrypted all non-attachment messages’ ‘content’ field in-place (replacing the encrypted content with the decrypted content), utilizing the private key associated with the encryption process followed by the third-party country’s server as mentioned in section 2.1.

6.1.1 Update Attachment Paths to be Correct

When receiving the encrypted attachment message files on the third-party country’s server, the entire plaintext path of the file was stored in the ‘content’ field of the database if the type was an attachment. This path was relative to the third-party country’s server, but this field in the database was used similarly on the I1 server to serve attachments for review on the front-end web server. In order to make the attachments accessible, the path in the ‘content’ field was updated to the path they would be placed on the I1 server following decryption and conversion (if needed).

6.2 Decryption of All Attachment Files

After the paths in the ‘content’ field were updated correctly, the processing code decrypted all new attachment files using the private key associated with the encryption process followed by the third-party country’s server as mentioned in section 2.1. The attachment decryption process placed the decrypted files in the correct location to be accessed by the front-end web server for view in the Hola iBot web application.

7. AUDIO FILE PROCESSING

The audio files received from the third-party country’s server needed additional processing for them to become available for listening within the Hola iBot web application.

7.1 Convert Audio Files to Usable Format

While the decryption process runs, if an attachment was an audio file (indicating a push-to-talk message), the audio file would be converted from the Ogg Opus (OPUS) File Format to a Waveform Audio (WAV) File Format. This is due to browsers not supporting OPUS files, while WAV files can be played natively in most modern web browsers.

7.2 Pitch Change Audio Files if Needed

As mentioned in Appendix A.7.1.4 – 57, the ANØM application provided the capability of adjusting the pitch of the message recorded. The user had the ability to shift the pitch of PTT messages up ('Helium’) or down (‘Jellyfish’). With each pitch-adjusted PTT message sent, a value that represented the adjusted frequency was also sent. This value was used to reverse the pitch, which would provide an adjusted audio file. While the pitch-adjusted audio file is made available to users of the Hola iBot review platform, the original audio file is also retained. While the original audio file is something that was retained, it's currently not available for retrieval. A process to retrieve the original audio files has not been developed.

8. DATABASE OVERVIEW

The remainder of the ingestion process after the processes described in sections 6 and 7 involves reorganizing the data into a secondary database (iBot_dec). The iBot_dec database is the database used by the front-end Hola iBot web application. The following section describes the layout of the primary iBot_dec tables, as well as relationships within. While not all tables within iBot_dec are described in this section, they will be introduced as needed in later sections.

8.1 Cases/Syndicates

The iBot_dec database's central component for organization is "cases" or "syndicates". Within the database, cases have a case ID and a name. The case ID is a unique identifier for the case, and the name provides a space for administrators to enter an easy-to-remember identifier for the case. Cases were predominantly named after randomly chosen Roman and Greek Gods and Goddesses. Within the database, there is a table named 'cases', where descriptive information is stored regarding cases.

8.1.1 Groupings of Device Users (JIDs)

Cases provide the means to organize device users (JIDs) that frequently talk to each other into groups. They also provide organization for review platform users.

8.2 Review Platform Users

Upon obtaining a CJIS Law Enforcement Enterprise Portal (LEEP) account, FBI employees and other individuals from law enforcement agencies monitoring data within the platform will need additional access permissions to be granted before accessing the review platform. These permissions are granted through the creation of an account that exists within the iBot_dec database.

Three main types of users exist within the database:

- General Users
- Super Users
- Admins

Within the iBot_dec database, there is a table named 'users', where descriptive information is stored regarding review platform users.

8.2.1 General Users

Users are FBI and other law enforcement agency investigative and support personnel working on Operation Trojan Shield investigations. For the specific investigation for which they have been granted access, they can access the products pages. Products are described more in the database in section 8.5. This is where they can review, mark, and submit notes on products. General Users are also able to access and use the features on the roster. Reference section 8.3 for more information about the roster.

8.2.3 Super Users

Super Users are FBI supervisors responsible for Operation Trojan Shield investigations. They can access the communications data related to their investigations as General Users can. Super Users can also create and grant General Users access to investigations under their supervision.

8.2.4 Admins

Administrators are FBI personnel responsible for the operation, maintenance, and oversight of the Hola iBot review platform. They vet access requests to ensure users have adequate justifications for accessing Hola iBot and grant review platform users access to the system. Administrators can also grant access to

investigations for any General Users or Super Users. Additionally, they can access systems to create new cases/syndicates.

8.3 The Roster

The Roster is the location of all device user (JID) information. It is a unique list of every user of the ANØM platform that data has been received for. Within the iBot_dec database, there is a table named 'roster', where the following information is stored regarding device users:

- Unique device user identifier (JID)
  - Each user on ANØM is identified by a unique user identifier (user ID), known technically as a Jabber Identifier (JID). Initially, this user ID took the form of 6 alpha-numeric characters (for example 'aab2c3') and was automatically generated based on the handset International Mobile Equipment Identity (IMEI) number (Appendix A.3 – 19 and A.7.1.1 – 46).
- Device user display name
  - The user of the handset could set a 'display name' (also known as a nickname, username, alias, or handle), which could be changed whenever the user desires. This would not change their user ID (JID) on the platform (Appendix A.7.1.2 – 47)
- Real Name
  - If discovered through reviewing content of a device user, there is a space for entering a true identity for a user.
- Bio
  - The review platform allows for entering in any additional information gathered about a device user that may be useful to include on their JID profile. The JID profile is discussed further in section 10.7.
- Location
  - If discovered through reviewing content of a device user or other users, there is a space for review platform users to enter the assumed location of a device user.

8.4 Groups

As referenced in Appendix A.7.1.4 – 51, A device user could also send end-to-end encrypted messages to a group of ANØM users, and each user in that group was able to see the other members of the group. Groups were also given names that the device users would define. More information about groups can be found in the Appendix, section A.7.1.4 – 51.

The iBot_dec database contained a table named 'groups', which has the following information:

- Group ID (GID)
  - The GID is a string of alphanumeric characters that uniquely identify a group.
  - GIDs are assigned similar to JIDs, at the XMPP server.
- Name
  - The user-created label or name for a group
- Inserted
  - The date of the new data package that initially contained information on the group

For information about how device users are linked to groups, see section 8.7.4.

8.4.1 Lack of Group Information

Throughout the reception of data packages from the third-party country, group information was not always collected. This would cause a lack of information about groups within the database.

8.5 Products

Products are synonymous with conversations contained within each new data package. A single product represents a conversation between two or more device users assigned to a case, over the period of time between the previous data package and the data package the current product corresponds to.

8.5.1 Products in Detail

A new unique set of products are created with each new data package received from the third-party country for each case. More information about how products are created can be found in section 9.

There is a table within the iBot_dec database named ‘products’. This table contains the following information:

- Case ID
  - Each product that is created has a one-to-one relationship with a case.
  - The case/syndicate unique identifier that the product belongs to is stored within the product table, represented as a positive integer.
- Product ID (PID)
  - A unique identifier for the product, represented as a positive integer.
- Product Note
  - Review platform users can add notes to products.
  - This field is where the notes are added.
- Date Created
  - New data packages are received from the third-party country every Monday, Wednesday, and Friday.
  - Since new sets of products are created each time a new data package is received, the date of which the product was generated is also saved, which corresponds to the date the new data package was created.
- MCC String
  - A unique list of the different Mobile Country Codes used by the devices within the product
- JID String
  - An alphabetized list of device user unique identifiers (JIDs) that sent or received messages within the product
- Message Count
  - The number of messages that correspond to the product
- JID 1
  - The first sender of a message within the product
- JID 2
  - The other participant or JID in the product if the product is not a group product
- Group ID (GID)
  - The group unique identifier if the product is a group product

- Is Duplicate
  - This value will be either 1 or 0 (indicating whether it is a duplicate (1) or it is not a duplicate (0)).
  - As said before, each product has a one-to-one relationship with a case.
    - If one or more of the JIDs within a product do not all belong to the same case or syndicate (I.E. JID 123456 belongs to case Alpha and JID 789100 belongs to case Bravo), a product will be created for each case.
    - The messages and participants of the product will all be the same, but there will be a product created for each case a JID within the product belongs to.
    - See section 8.7.3 for more information about JID to Case relationships within the database and section 9 for more information about the ingestion process.
- Known Group
  - This value will be either 1 or 0 (indicating whether our database has information about the group (1) or not (0)).
  - As previously mentioned in section 8.4.1, group information was not always collected on the third-party country's server.
    - This would prevent the Hola iBot review platform from displaying the group identifier, the group name, and potentially **all** of the group members.
    - However, the products are formed directly from the messages, and the members of the conversation/product are determined by the senders and receivers of messages.
    - Thus, if the database does not contain group information, the JID String will still reflect the members of the conversation/product.

8.6 Messages

The MySQL difference-dump within the new data package received from the third-party country contained a single table for messages. Details on the ingestion process for messages are provided in section 9. There are four tables in the iBot_dec database that contain message content and metadata associated:

- 'text_message'
  - This table contains decrypted text messages, contact messages, forwarded messages, and text components of note messages.
  - This table also contains the 'from note' field, indicating that the text in the 'content' field is derived from a note message type.
    - Reference 9.3.2.2.2 for more information about how note message types are ingested to the database.
- 'ptt_message'
  - This table contains the paths (on the I1 server) of decrypted, converted, and pitch-adjusted (if needed) push-to-talk messages.
- 'video_message'
  - This table contains the paths (on the I1 server) of decrypted video messages.
- 'image_message'
  - This table contains the paths (on the I1 server) of decrypted image messages and image components of note messages.

    - This table also contains the 'from note' field, indicating that the image that can be found at the path within the 'content' field is derived from a note message type.
        - Reference section 9.3.2.2.2 for more information about how note message types are ingested to the database.

All four tables contain the following metadata fields:

- Message ID (MID)
    - A unique identifier for a message represented as a positive integer
    - The MID is shared across all four tables
        - Ex. if MID 5 appears in ptt_message, that is the only place the MID will appear
- Original Message ID
    - Another unique identifier for a message, which is inherited from the new data packages.
    - A unique string of characters, represented as a Universally Unique Identifier (UUID).
    - This message ID was stored with each message the third-party country's server received as a 'blind carbon copy'.
    - This message ID is described further in Appendix A.8.2 – 64.a.
    - The MID was created within the iBot_dec database to provide a uniform standard of primary keys within the database.
        - I.E. PIDs as positive integers, case IDs as positive integers, etc.
- Inserted Date
    - The inserted date corresponds to the date in which the data package containing the message was ingested to the database.
- Mobile Country Code (MCC)
    - The MCC of the sending device at the time of the sent message
- Is Group
    - This value is either 1 or 0 (indicating whether the message was sent to a group (1) or not (0)).
    - If the message is a group message (value of 1), the receiver field contains the group ID (GID) that the message was sent to.
- Sender
    - The sending device user's ID (JID)
- Time
    - When the message was sent according to the timeframe in 8.6.1.
    - For example, a message sent on June 6, 2021 at 10:00 pm Pacific Time, the database would have the time and date as 5:00am on June 7, 2021 UTC.
- Location Information
    - If location information (latitude and longitude) was received with a message, the latitude and longitude would be stored with each message in each of the four tables.

8.6.1 Message Time Zone Discrepancy

Due to a misconfiguration on the third-party country's server, the time zones of messages varied throughout the collection period. The following timeframes provide insight into the correct conversions of timestamps for messages:

- Timeframe 1

    - October 1, 2019 – October 27, 2019: UTC – 3
- Timeframe 2
    - October 27, 2019 – March 29, 2020: UTC – 2
- Timeframe 3
    - March 29, 2020 – September 18, 2020: UTC – 3
- Timeframe 4
    - September 18, 2020 – End of operation: UTC

8.7 Relationships

The following sections define the relationships within iBot_dec that correspond to all tables defined in sections 8.1-8.6. The tables defined in section 8.7 all correspond to many-to-many relationships, and they follow a naming convention of this example:

User **assigned_to** *case*

Where the italicized are single-keyed tables (unique entity of the user table is uniquely identified by the user_id), and the bold indicates a composite-keyed table (unique entity of the assigned_to table is uniquely identified by both a user ID and case ID).

8.7.1 Product to Message Relationship

There is a table within the iBot_dec database named 'has_message'. This table contains the following information:

- Product ID (PID)
    - A unique identifier for the product, represented as a positive integer, that the message in the same row of values is related to.
- Message ID (MID)
    - A unique identifier for the message, represented as a positive integer, that the product in the same row of values is related to.
- Type
    - The type of the message that is referenced by Message ID in the same row of values.
- Marking
    - Each message allows the marking of 'Not Marked', 'Pert', 'Not Pert', or 'Priv'.
- Original Message ID
    - The unique string of characters, represented as a Universally Unique Identifier (UUID), that uniquely identifies a message, inherited from the original data package from which the message corresponds.

8.7.2 User to Case Access Relationship

Review platform users are granted explicit access to cases by administrators. The relationships for review platform users to cases is managed by a table named 'assigned_to'. The 'assigned_to' table contains the following attributes:

- LEEP Username
    - The username of the Hola iBot user that has access to the case identified in the same row of values.
- Case ID

- The case ID of the case that the Hola iBot user in the same row of values has access to

8.7.3 JID to Case relationship

Device users (JIDs) are assigned to cases to group them amongst other device users that frequently communicate together, as mentioned in 8.1.1. Since many device users can correspond to many cases, the 'belongs_to' table allows for these relationships. The 'belongs_to' table contains the following attributes:

- Device User ID (JID)
  - The JID of the user that is related to the case ID within the same row of values
- Case ID
  - The case ID that the corresponding JID is related to.
- Date Added
  - The date the relation was created in the iBot_dec database.

8.7.4 JID to Group Relationship

Device users (JIDs) are added to groups by group administrators within the ANØM application. JIDs can be members of many groups, and groups can have many JIDs that are members. Thus, the 'member_of' table allows for this relationship. The 'member_of' table contains the following attributes:

- Device User ID (JID)
  - The JID of the user that is a member of the group identified in the same row of values.
- Group ID (GID)
  - The GID of the group that the corresponding JID is a member of.

9. INGESTION PROCESS

Following the decryption of all encrypted content fields, roster nicknames, group names, and attachments, and the adjustment of paths within content fields of messages that are of type ptt, video, image, or note, the ingestion process will continue by following the steps defined within this section (section 9). This section describes the process of transitioning data on I1 from the iBot_enc database (where the new data packages were temporarily stored) to the iBot_dec database, which permits the review platform code access to the new data.

The prerequisite to begin the ingestion process is sections 5-7:

- Decrypt the encrypted new data package
- Extract the archive of data
  - Attachment files
  - MySQL difference-dump
    - As mentioned in section 2.2, the difference-dump only contains data that is new or different.
- Ingest the MySQL difference-dump into the iBot_enc temporary database
- Decrypt all encrypted fields within the database
- Fix paths of all fields in the database that reference attachment files
- Decrypt all attachment files
- Convert and pitch-adjust audio, if necessary

9.1 Insert new Roster Information

The first data inserted to the iBot_dec database is the roster information. The following is the process for adding new roster information:

1. Load all new roster data from iBot_enc (new MySQL data)
2. For each new roster entry:
    a. Check to see if the device user ID (JID) already exists in the iBot_dec 'roster' table
    b. If the device user already exists, this indicates that the user changed their Device User Display Name.
        i. If the new display name does not match the old display name, the new display name is updated in the 'roster' table of iBot_dec.
    c. If the device user doesn't exist, this indicates a completely new user. The user is added to the 'roster' table of iBot_dec, and a relationship is added for the device user to correspond to the "UNKNOWN" case.
        i. The "UNKNOWN" case is a default case for all new device users (JIDs) and for devices to remain until a case or syndicate is found to place them.

Any errors updating the device user display name or inserting the user into the 'roster' table are logged.

9.2 Insert new Groups

9.2.1 Insert New Group Information

New information regarding groups on the ANØM platform is inserted after new roster information. The following is the process for adding new group information:

1. Load all new group data from iBot_enc (new MySQL data)
2. For each new group from the new data:
    a. The group ID (GID), group name, and the inserted date is inserted into the 'groups' table within the iBot_dec database.

9.2.2 Insert Group Membership Updates

Members were added to groups on the ANØM platform by administrators of groups, and these updates were received in the MySQL difference-dump. The following is the process of updating the group membership relation:

1. Load all new group membership data from iBot_enc (new MySQL data)
2. For each new group ID (GID) to device user ID (JID) relationship:
    a. The GID and JID are inserted into the 'member_of' table within the iBot_dec database.

9.3 Message Ingestion

After changes to the roster and groups are updated within the database, the process to ingest messages starts. This is the primary ingestion mechanism that allows for data to be reviewed in the form of products (conversations). Message ingestion follows the process described in this section (9.3).

9.3.1 Initialization

Before ingesting new data, some components are initialized.

9.3.1.1 Blacklist

The blacklist is a line-delimited text file separating JIDs. This file contains JIDs whose messages sent are blacklisted from being ingested to the iBot_dec database. The blacklisting feature will be further described in a future addendum.

9.3.1.2 Conversation Temporary Data Structure

The data structure to hold all unique conversations and the messages that correspond to them is initialized. This will be the data used for forming products after cycling through each new message.

9.3.1.3 Case to JID Temporary Data Structure

This is a data structure that maintains a list of JIDs that correspond to each case within the database. This data structure will be later used for forming products correctly. It is formed from data residing within the 'belongs_to' table.

9.3.1.4 Retrieve Last Message ID (MID)

Getting the last inserted Message ID (MID) provides the starting Message ID (MID) for the new data, as MID is an ascending positive integer.

9.3.1.5 Load New Messages

The new messages are loaded from iBot_enc (new MySQL data) to be inserted.

9.3.2 Insert Messages

For each message, the remainder of section 9.3.2 is performed.

9.3.2.1 Metadata Insertion

Within the iBot_dec database, a table named 'metadata' exists that contains the data that has common attributes from all four message tables as referenced in section 8.6. The metadata table has the following attributes:

- Message ID (MID)
- Original Message ID
- Time
- Sender
- Receiver
- Mobile Country Code (MCC)
- Is Group
- Type
- Location Information

The attributes above have all been defined in section 8.6 under the metadata section.

Regardless of message type, all of the metadata attributes are inserted for each message.

9.3.2.2 Insert by Type

The ingestion process differs by type of message.

9.3.2.2.1 Text Messages, Contact Messages, and Forwarded Messages

If the message type is 'text', 'contact', or 'forwarded', the 'content' field from the iBot_enc messages table is copied into the 'content' field in the iBot_dec 'text_message' table. The value in the 'content' field was already decrypted by the steps in section 6.1.

9.3.2.2.2 Note Messages

If the message type was 'note', the note attachment would be decrypted. After being decrypted, note attachments are revealed as compressed ZIP files that contain text and image files. These files are parceled out into the 'text_message' and 'image_message' tables respectively.

First, the ZIP files are extracted for processing. For each extracted file, a determination whether the file is a text file or image file is made, and if it is a text file, the text would be read and inserted to the 'content' field of the 'text_message' table. However, if it was an image file, the image file would be copied to the directory which images are served to the front-end review web application, and an entry of data would be inserted to the 'image_message' table.

In all entries to 'text_message' or 'image_message', the 'from note' attribute would be updated to a value of 1 to indicate the text/image is a component from a note.

9.3.2.2.3 Push-to-Talk, Image, and Video Messages

If the message type is 'ptt', 'image', or 'video', the 'content' field would be copied directly from the iBot_enc messages table into the iBot_dec corresponding message table based on the type. The paths in the 'content' field were fixed in-place and updated to the new paths which the front-end review web application utilizes. More information on the paths being updated can be found in section 6.1.1.

9.3.4 Assigning Messages to Products

After the message metadata and type-based table insertion have completed, the message is assigned to a conversation, utilizing the temporary data structure initialized in section 9.3.1.2.

This data structure contains a nested unique list of conversations, each of which have the members (JIDs) of the conversation, the mobile country codes (MCCs) that messages were sent from, the message ID (MID), and the message type ('text', 'ptt', 'video', etc).

After assigning each message to a conversation, the loop over the new messages is complete, and the usage of the temporary iBot_enc database concludes.

9.4 Product Ingestion

After the conversation data is finished populating, the products are ready to be created for the current new data package. The remainder of section 9.4 processes each unique conversation in the temporary data structure that had message(s).

9.4.1 Product Creation Per Case

For each case, the steps under 9.4.1.1 are executed on the conversation.

9.4.1.1 If JID in conversation belongs to case

If a device user that is a member of the current conversation belongs to the current case, 9.4.1.1.1-9.4.1.1.3 are completed.

9.4.1.1.1 Generate Product for Case

If 9.4.1 and 9.4.1.1 are satisfied for the current conversation, a product will be created for the current case. The following values are inserted based on temporary data structures and the current status of the ingestion code:

- Case ID
- Date Created
- Mobile Country Code (MCC) String
- Device User ID (JID) String
- Count
- Group ID (GID) – if necessary
- Known Group – If group information was found during product creation (by querying the 'groups' table), this will be set to 1

9.4.1.1.2 Create Message and JID Relation to Product

As mentioned in 8.7.1, messages correspond to products through the use of the 'has_message' table. After creating the product for the current case, the messages within the temporary conversation data structure are all associated with the product by inserting their message IDs (MIDs) into 'has_message', along with the product ID (PID) that was inserted.

There is a table within the iBot_dec database named 'part_of' that links device user IDs (JIDs) to product IDs (PIDs). This creates a table that informs the system that a specific device user sent messages that appear in a product. This table has the following attributes:

- Device User ID (JID)
- Product ID (PID)

This table is also be populated upon creation of a new product.

9.4.1.1.3 Assign default marking to product

There is a table within the iBot_dec database named 'has_marking' that links text-based markings to products. Products can be marked within the Hola iBot review platform by users of Hola iBot. The has_marking table has the following attributes:

- Product ID (PID)
- Marking
    - A text-based marking that can be assigned to a product.
    - Examples include "Not Reviewed (default)", "Pertinent", "Not Pertinent".

The default product marking of 'Not Reviewed' is inserted to the 'has_marking' table for the currently generated product.

9.5 Post-Ingestion Exports

Encrypted exports were automatically sent over Secure File Transfer Protocol (SFTP) to countries that required immediate review of new data received from data packages. These encrypted exports contained a JavaScript Object Notation (JSON) file for each case the requested country has been given access to. This JSON file contains all product data for the previously ingested data package.

10. WEB APPLICATION/REVIEW PLATFORM

Hola iBot is the custom web application built and operated by San Diego FBI to serve as the review platform of all data received from the ANØM platform.

10.1 User Access Controls within Hola iBot

The review platform user roles defined in section 8.2 are roles of the users of Hola iBot. As stated before, the users in section 8.2 must all be provisioned accounts within the Law Enforcement Enterprise Portal (LEEP).

10.1.1 Law Enforcement Enterprise Portal (LEEP) Access Control

The Law Enforcement Enterprise Portal (LEEP) is a portal that law enforcement agencies (including international) and other intelligence groups can be provisioned accounts. Once the applying user is vetted by the provisioning department, the user will have access to the list of applications/tools, one of which is the Hola iBot review portal.

LEEP also follows common security practices for authenticating users, such as two-factor authentication (2FA), security pictures, and security questions.

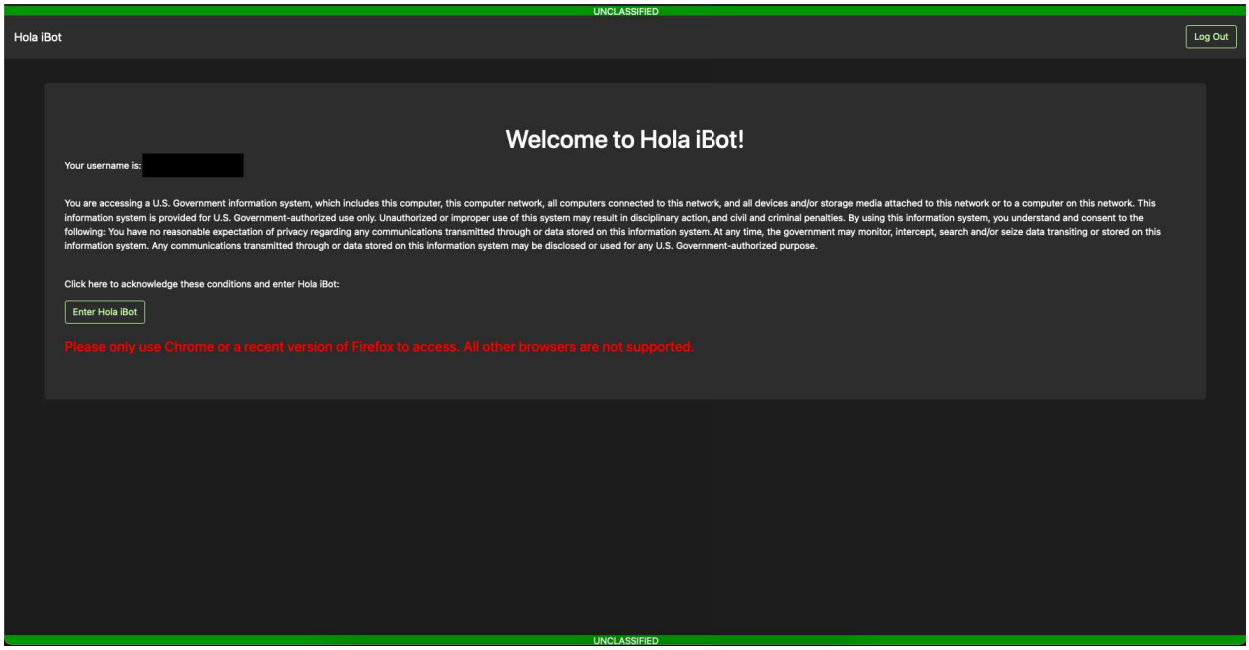
10.1.2 Hola iBot Access Control

After a user authenticates through the login process that LEEP administers, the user will have the ability to visit the Hola iBot application by clicking the application in the list as shown in the screenshot below.

Screenshot 10.A

After clicking the Hola iBot application, a single-sign-on (SSO) request using the Security Assertion Markup Language (SAML) is sent to the front-end web application server. SAML is a protocol that allows identity providers to pass authenticated credentials to another service, which is how Hola iBot authenticates users.

The review platform user is only granted access to the system if they exist within the 'users' table cited in section 8.2. If they are granted permission to the application, they will be greeted with the warning banner shown in screenshot 10.B.

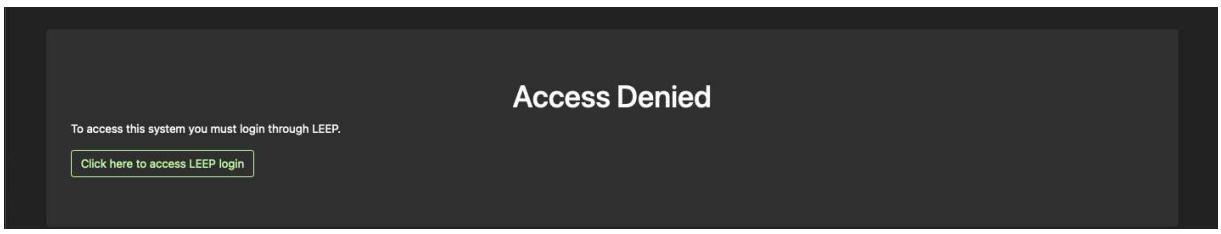


Screenshot 10.B

The text of the banner is the following:

> *You are accessing a U.S. Government information system, which includes this computer, this computer network, all computers connected to this network, and all devices and/or storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, and civil and criminal penalties. By using this information system, you understand and consent to the following: You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system. At any time, the government may monitor, intercept, search and/or seize data transiting or stored on this information system. Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.*

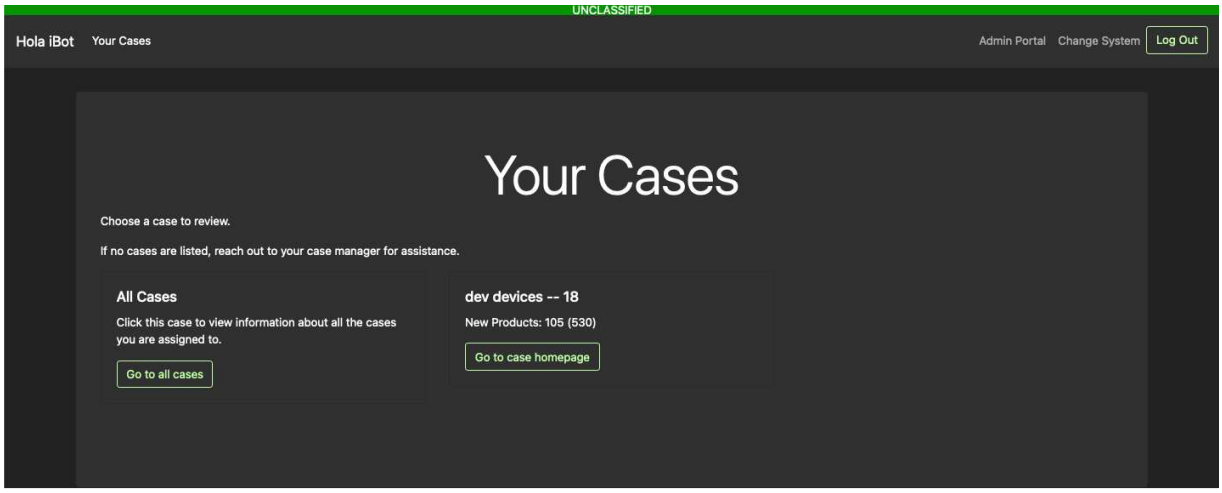
If the user does not exist in the database, they are presented with a generic invalid access page. This page can be viewed in Screenshot 10.C



Screenshot 10.C

10.2 Cases in Hola iBot

Assuming the user has been granted access to the system through LEEP authentication and Hola iBot explicit database access, the user is navigated to their homepage, where a list of cases they have been given explicit access will be displayed. Screenshot 10.D portrays the homepage of a user with access to a single case, named “dev devices” with a case ID of 18.



Screenshot 10.D

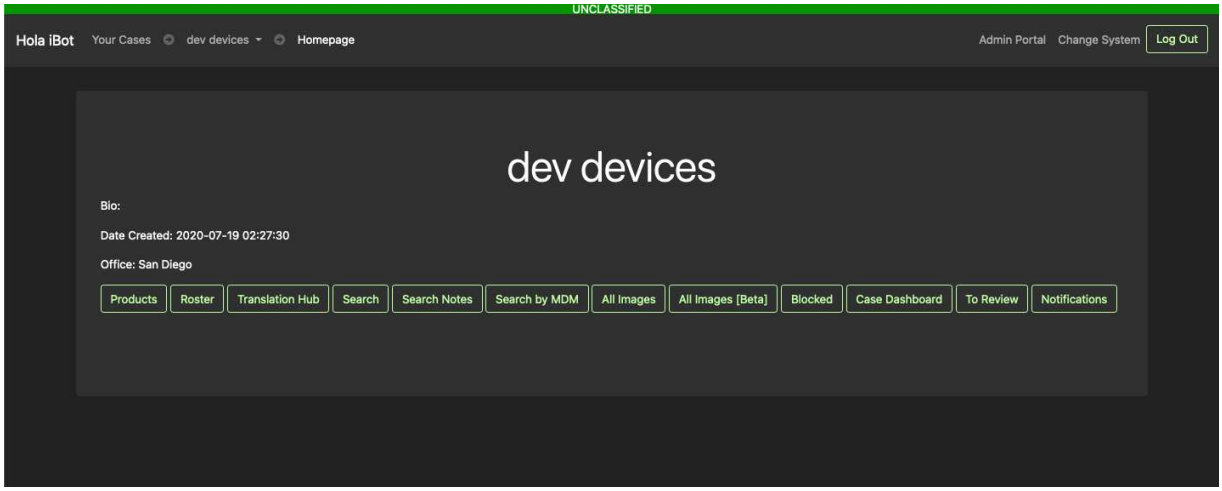
The list of cases displayed on the homepage are displayed based on the ‘assigned_to’ table, as previously described in section 8.7.2.

When visiting a single case, the data in the remaining pages is filtered to only device users (JIDs) that correspond to the case within the ‘belongs_to’ table (JID to case ID relationship), as mentioned in section 8.7.3.

Every user is also shown an option for “All Cases”. When selecting this option, the data in the remaining pages is populated with all data the review platform user has access to.

10.2.1 Case Homepage

After navigating to a case, the case homepage is displayed for the review platform user. Several options are presented after navigating to a homepage for a case. A sample case homepage is displayed in Screenshot 10.E.



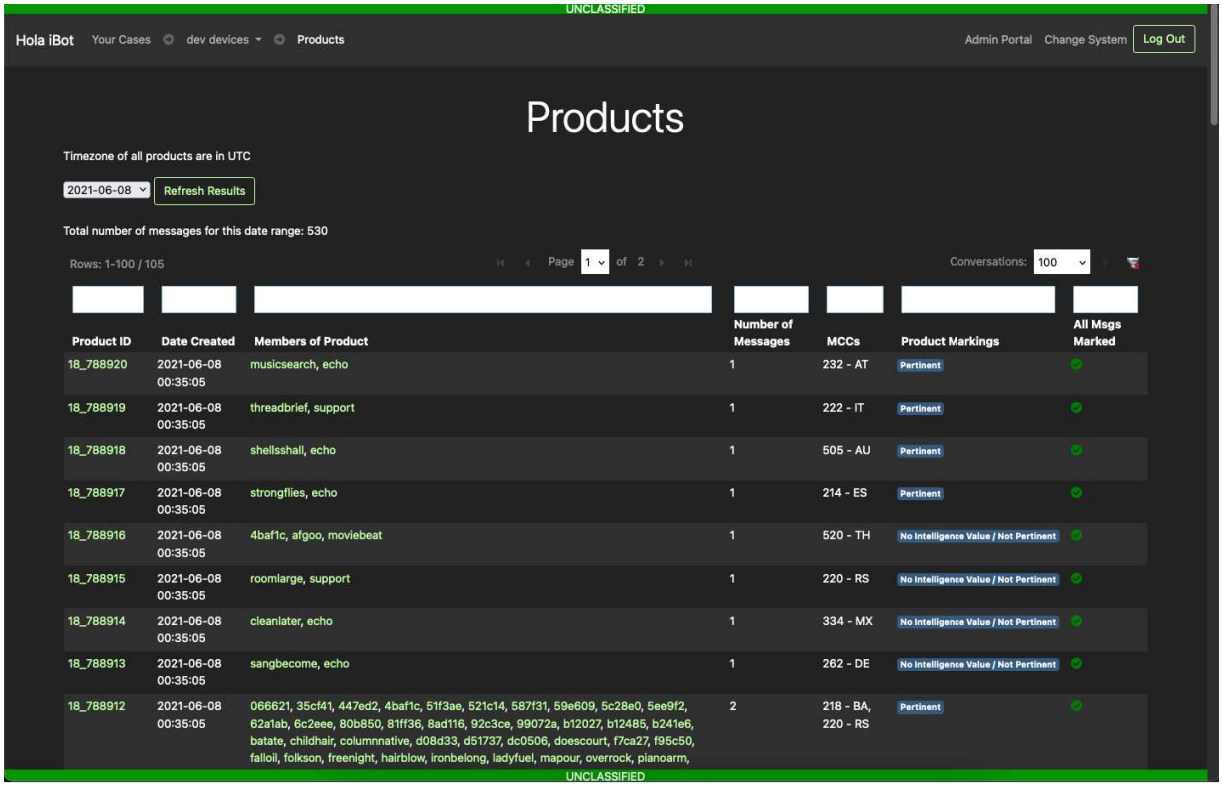
Screenshot 10.E

The remainder of section 10 further describes each of the options displayed on the case homepage.

10.3 Products Page

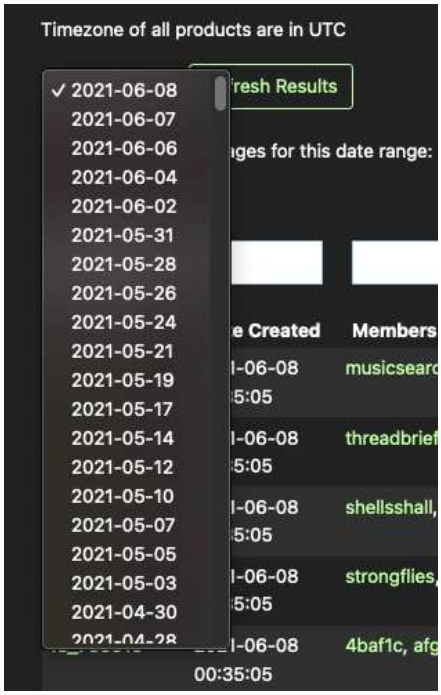
The Products Page is where users navigate to view conversations for the case. See section 8.5 for more information about products and section 9.4 for information about how products are created.

Products are unique conversations for a case that were received for a data package. Screenshot 10.F shows the Product Page for the “dev devices” case.



Screenshot 10.F

The drop-down menu option in the top left populated with “2021-06-08” expands a list of dates that new data packages were received:



Screenshot 10.F.1

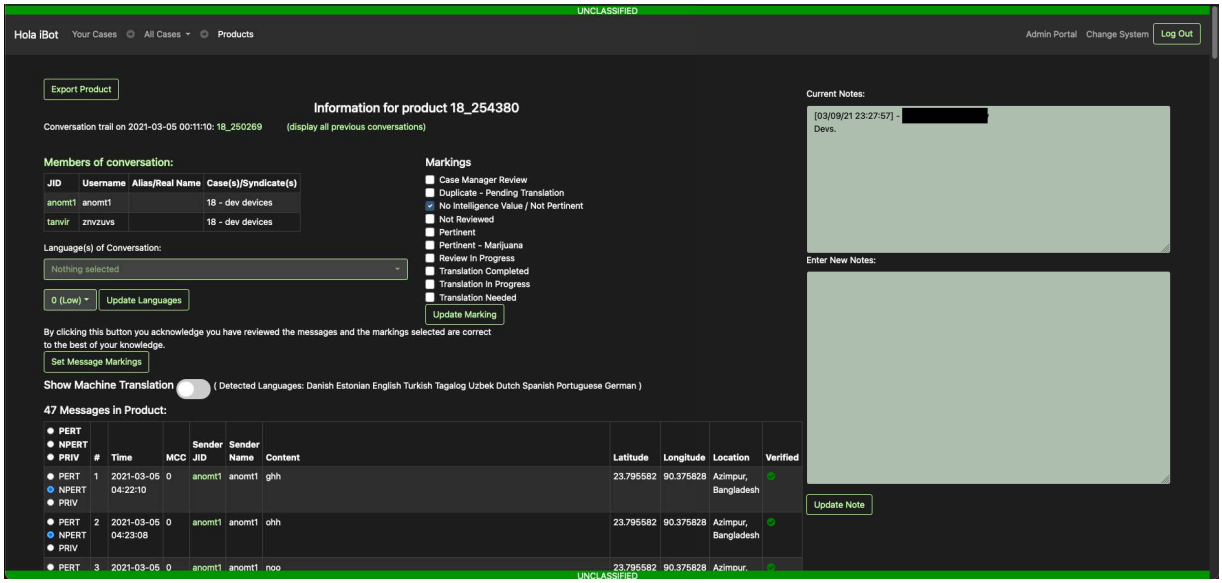
Lists of products are unique, per drop date. As also observed in Screenshot 10.F, the product ID (PID) is not shown under “Product ID” in the list of products. The “Product ID” shown to the user is denoted by case ID, followed by an underscore, followed by the actual product ID (PID). This provides an easier method of universally referencing products and knowing which cases the products belong to.

The rest of the data displayed on this page within the table is gathered from the ‘products’, ‘has_marking’, and ‘has_message’ table.

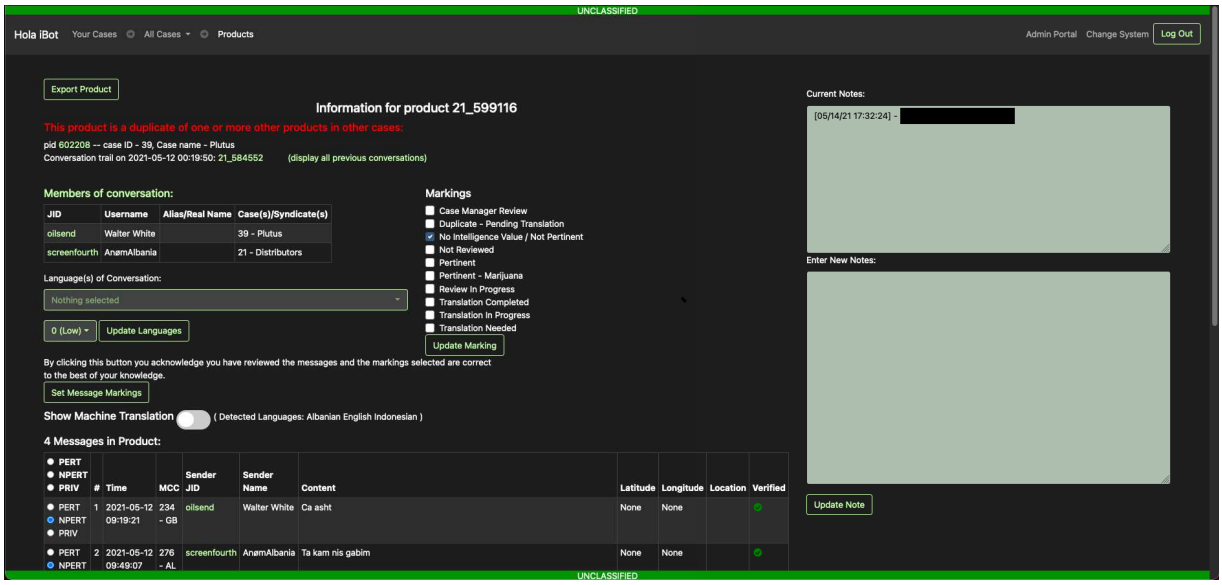
- “Date Created”
  - populated by the ‘date created’ field in the ‘product’ table
- “Members of Product”
  - populated by the ‘JID String’ field in the ‘product’ table
  - The JIDs displayed in this column are all linked to the JID profile.
    - See section 10.7 for more information about the JID profile.
- “Number of Messages”
  - populated by the ‘count’ field in the ‘product’ table
- “MCCs”
  - populated by the ‘MCC String’ field in the ‘product’ table
- “Product Markings”
  - populated by the ‘has_marking’ table, which will relate the product to a text-based marking
- “All Msgs Marked”
  - populated by querying the ‘has_message’ table to test whether all messages have a marking that is not the default

10.4 Product Page

The “Product ID” links will open the product page, which displays the messages for the product, as shown in Screenshot 10.G and 10.G.1.



Screenshot 10.G



Screenshot 10.G.1

The product page displays many different components of information for the review platform user. Referencing Screenshot 10.G and 10.G.1, the product page displays the following information:

- Whether or not the product being referenced is a duplicate of a product within another case
    - Screenshot 10.G.1 shows an example of a duplicate product, which will also provide a link to the corresponding duplicate product.

- The members of the conversation
    - These are compiled during the ingestion process as referenced in section 9.4.1.1.
- The languages that have been added to the product by review platform users
    - This list allows for multiple languages to be added.
    - The languages list corresponds to translation submissions.
        - See section 10.5.1 for more information.
- The markings that have been added to the product
- The message markings that have been set by the review platform users
- Notes that have been created about the product (right pane).
    - Once added, notes cannot be removed, as they will move to the “Current Notes” text area with a timestamp that the note was created and the username of the review platform user that added the note.
    - These notes correspond to the ‘product note’ field in the ‘products’ table.
- All translations that have been added to the product based on the language that was added will appear at the very bottom of the product page.

10.4.1 Group ID Display

If the product corresponds to a group, the following will be displayed if group information is in the iBot_dec database:

Screenshot 10.G.2

10.4.2 Attachment Messages (PTT, Image, Video, Note) in Hola iBot

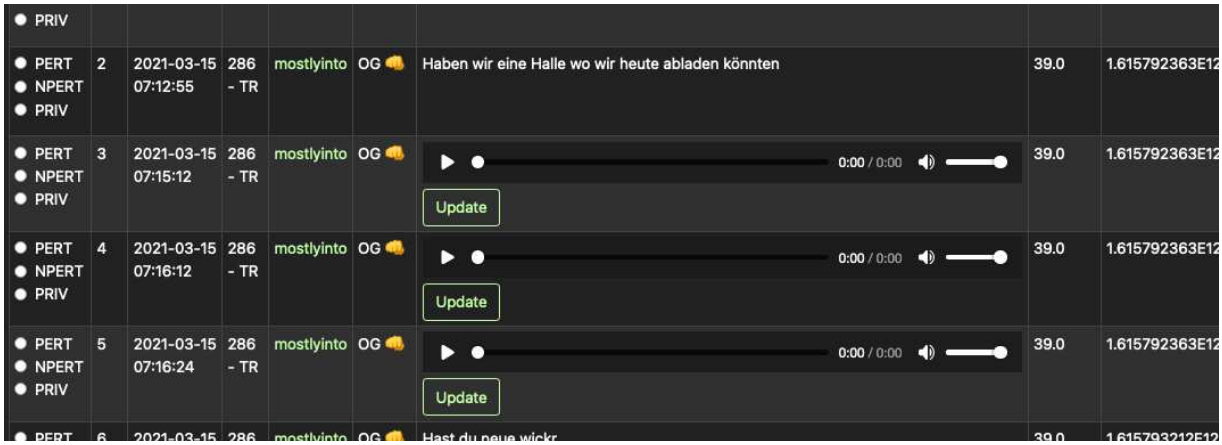
Attachment messages are all displayed inline as text messages are. Attachment messages can also have a marking that review platform users assign. Within the iBot_dec database there is a table named ‘attachment_has_marking’, which allows for marking attachments with text-based descriptions. The ‘attachment_has_marking’ table has the following fields:

- Message ID (MID)
    - The MID that the text-based description corresponds to
- Marking
    - The text-based description of the marking

These attachment markings can be set on the product page by review platform users.

10.4.2.1 Push-to-Talk Messages (PTT) in Hola iBot

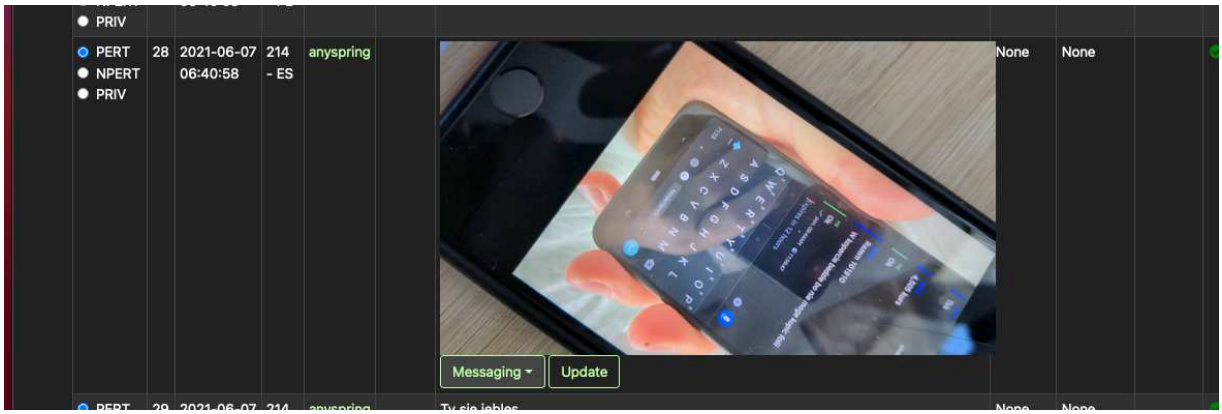
Screenshot 10.G.3 shows an example of a few PTT messages.



Screenshot 10.G.3

10.4.2.2 Image Messages in Hola iBot

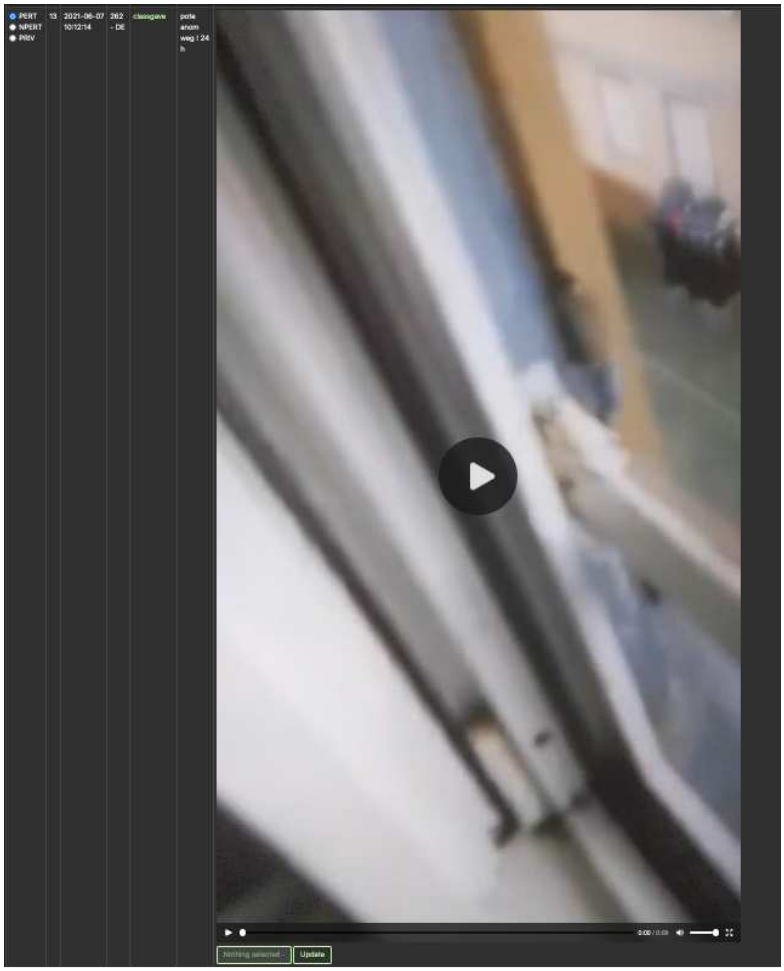
Screenshot 10.G.4 shows an example of an image message displayed inline.



Screenshot 10.G.4

10.4.2.3 Video Messages in Hola iBot

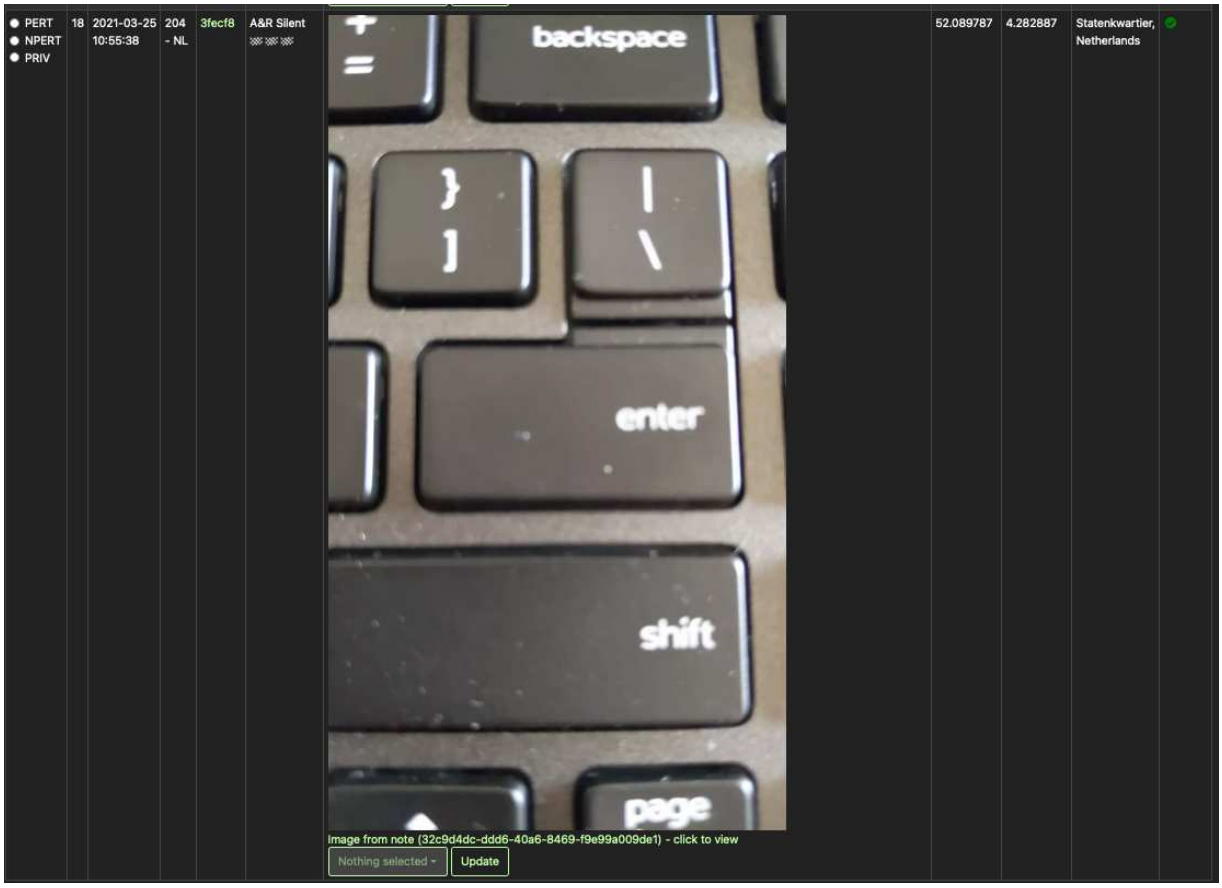
Screenshot 10.G.5 shows an example of a video message in Hola iBot.



Screenshot 10.G.5

10.4.2.4 Note Messages in Hola iBot

Screenshot 10.G.6 shows an example of an image component of a note displayed inline as a message.



Screenshot 10.G.6

The text “Image from note ([Original Message ID]) – click to view” indicates that the image was derived from a note message.

10.5 Translations

If a product has been assigned a language by utilizing the dropdown in Screenshot 10.G and 10.G.1, the product is automatically submitted for translation. Due to the many-to-many relationship that languages have with products, a table named ‘has_language’ exists in the database for creating these relationships. The ‘has_language’ table has the following attributes:

- Language Name
  - The name of the language that is being assigned to the product
  - Examples include “English” and “Spanish”
- Product ID (PID)
  - The PID of the product that the language is being assigned to
- Status
  - This field indicates the status of the translation.
  - This field can be set to either “New”, “In Progress”, or “Completed”.
- Priority
  - This field reflects the priority of the translation request.
- Submitter

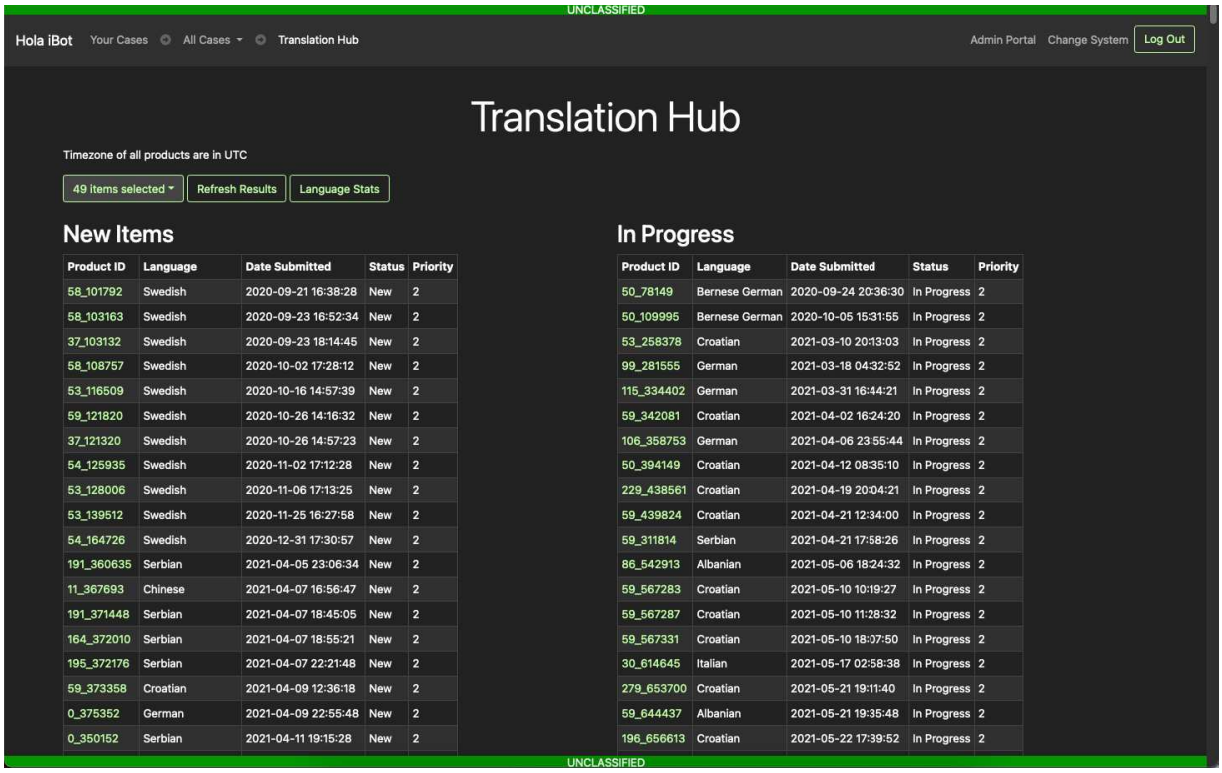
- This is populated with the review platform username that added the language to the product.

- Translation
  - This is the value that linguists will enter for the translation of the product.
- Date Submitted
  - Corresponds to the date the submitter added the language to the product
- Case ID
  - The case ID the product in the row of values corresponds to
- Completed By
  - The review platform username that set the 'status' field to "Completed"

Once a language is added to a product, the product ID, case ID, and language name will be viewable on the Translation Hub page.

10.5.1 Translation Hub

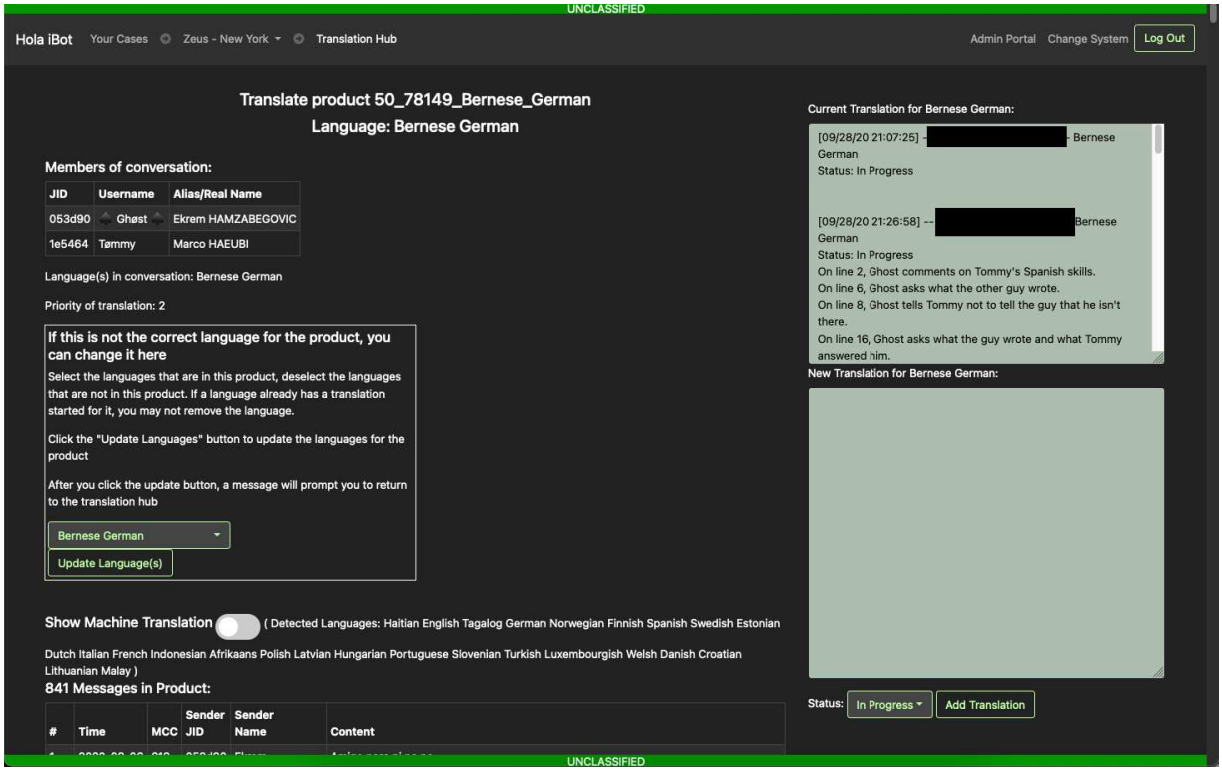
The Translation Hub contains all user-submitted translations for products. Screenshot 10.H contains an example view of the Translation Hub.



Screenshot 10.H

The two lists indicate the status from the 'has_language' table for the corresponding product ID (PID). If a translation request in the 'has_language' table has a status of "Completed", it will no longer be displayed in the two lists.

After clicking a linked product from the Translation Hub, a page similar to the product page will be displayed, as shown in Screenshot 10.I.



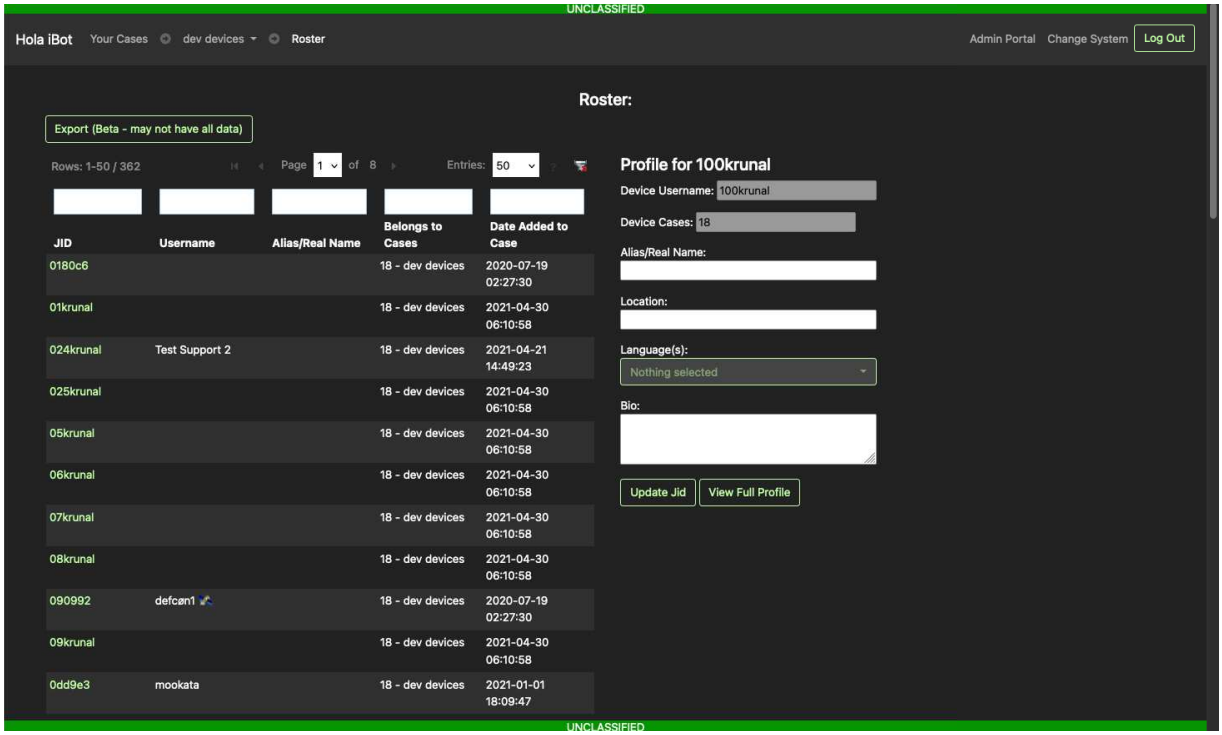
Screenshot 10.I

This page is specifically used by linguists for adding translations of products. The pane on the right-hand side of Screenshot 10.I shows the space where users can add translations. Once a translation is added, it is similar to when review platform users add notes to products. They move to the “Current Translation for [name of language]” text area. Translations cannot be updated that have already been submitted and moved to the other pane. They are also logged with a timestamp and username of the review platform user that added the translation.

All notes that have been added to the corresponding product through the product page are visible at the bottom of the translation page.

10.6 Roster Page

The page that displays the roster shows a list of device users (JIDs) that have a relation to a case in the ‘belongs_to’ table. Screenshot 10.J displays an example roster page for the “dev devices” case.



Screenshot 10.J

The page is separated vertically into two panes.

The left pane displays the list of device users (JIDs) with their Username (device user display name), real name (entered by review platform users if discovered through investigations), corresponding cases (reference the 'belongs_to' table), and the date they were added to the case (reference the 'belongs_to' table).

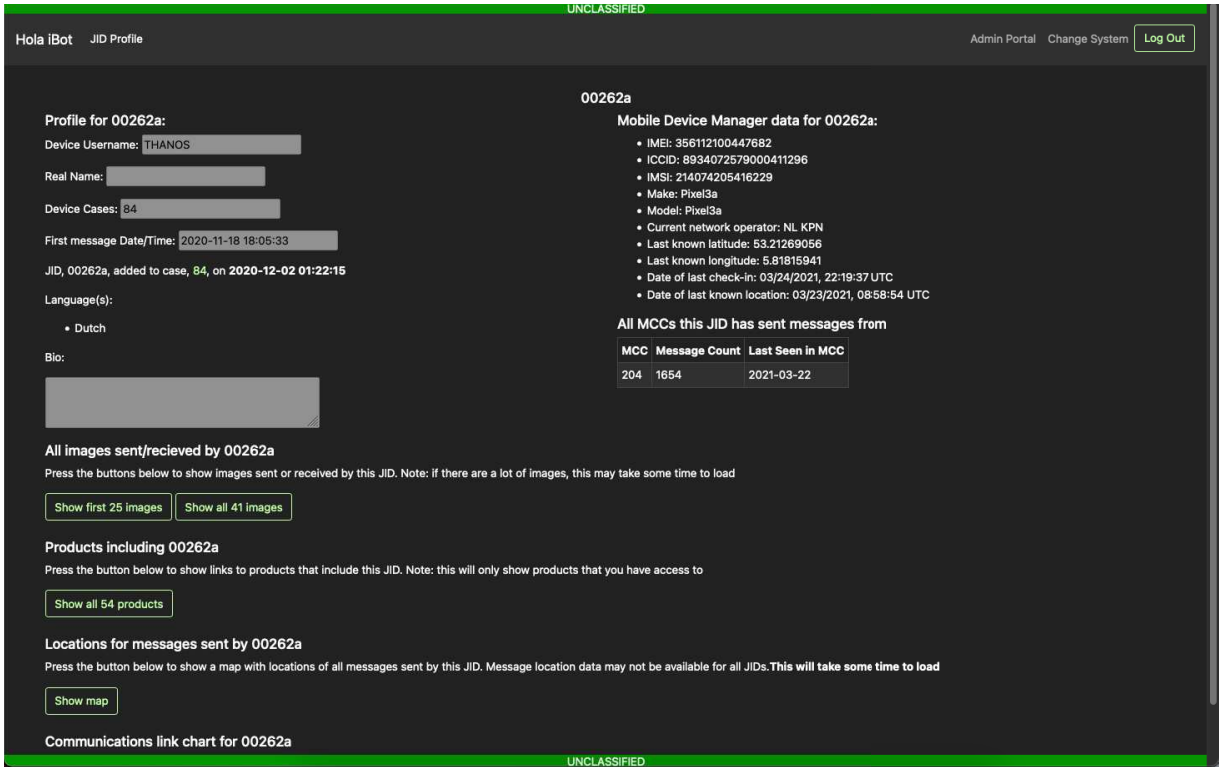
Each row in the list is clickable and will populate the right pane with the following additional information that can be edited:

- Alias/Real Name
- Location
- Language(s)
- Bio

Section 8.3 has additional information regarding the fields in the roster.

10.7 JID Profile

The JID profile can be linked to from a number of different pages. An example JID profile is shown in Screenshot 10.K.



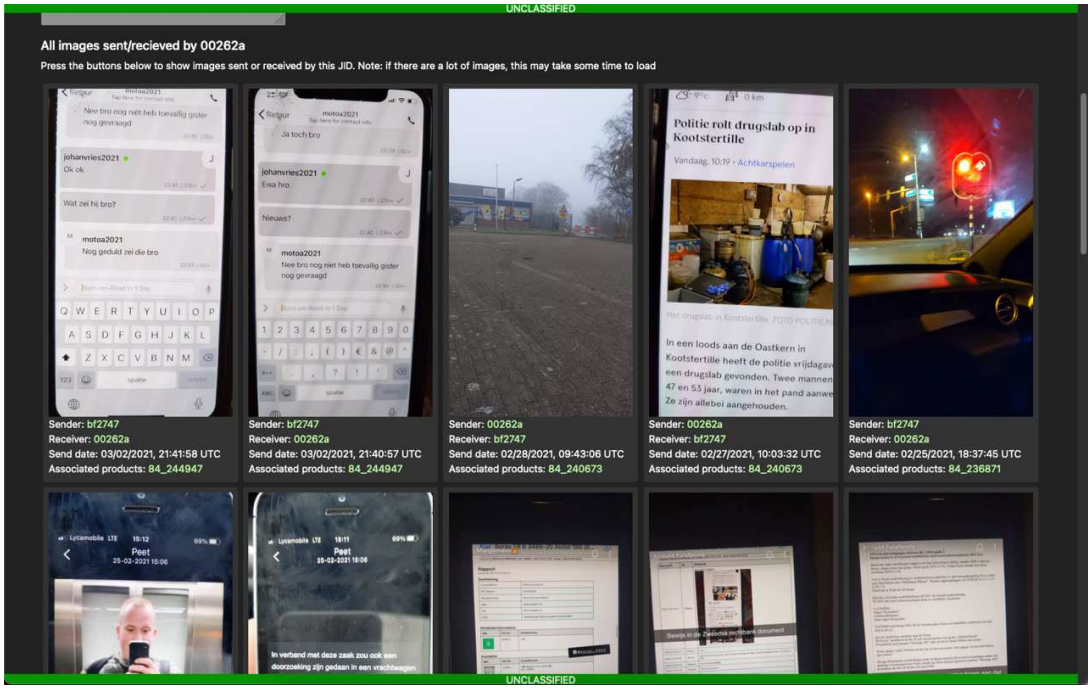
Screenshot 10.K

The remainder of section 10.7 references Screenshot 10.K.

10.7.1 Information About the Device User (JID)

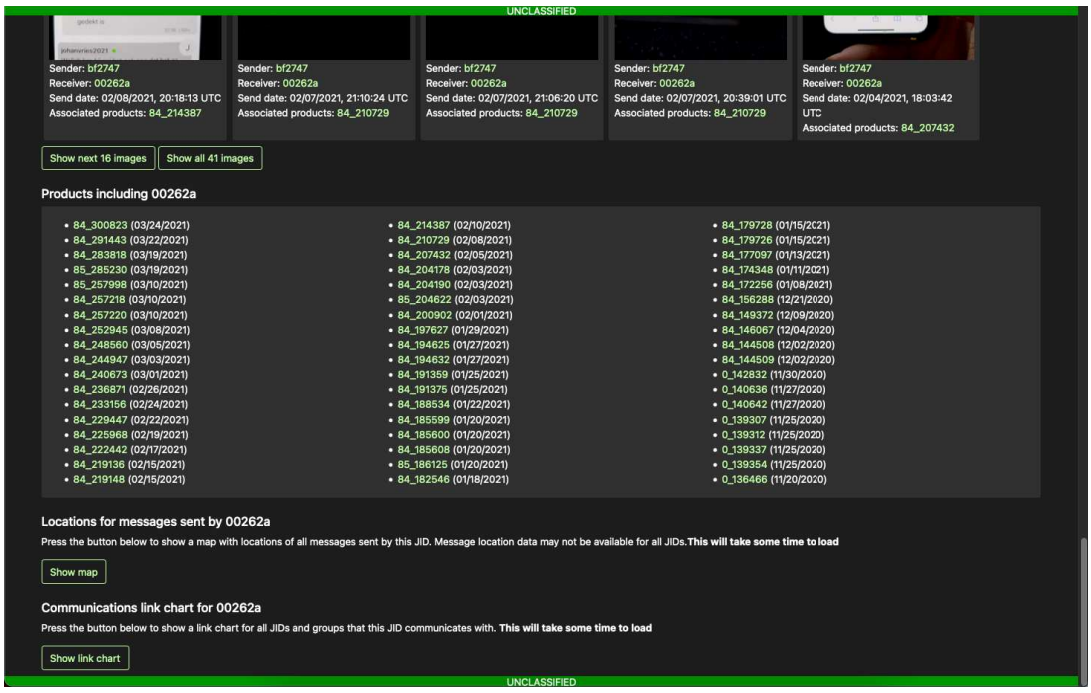
All roster data on the device user (JID) will be displayed on the JID profile page. There is additional data that can be retrieved from the JID profile page as well, such as

- Images sent by the device user.
    - “All images sent/received by 00262a” in the referenced screenshot



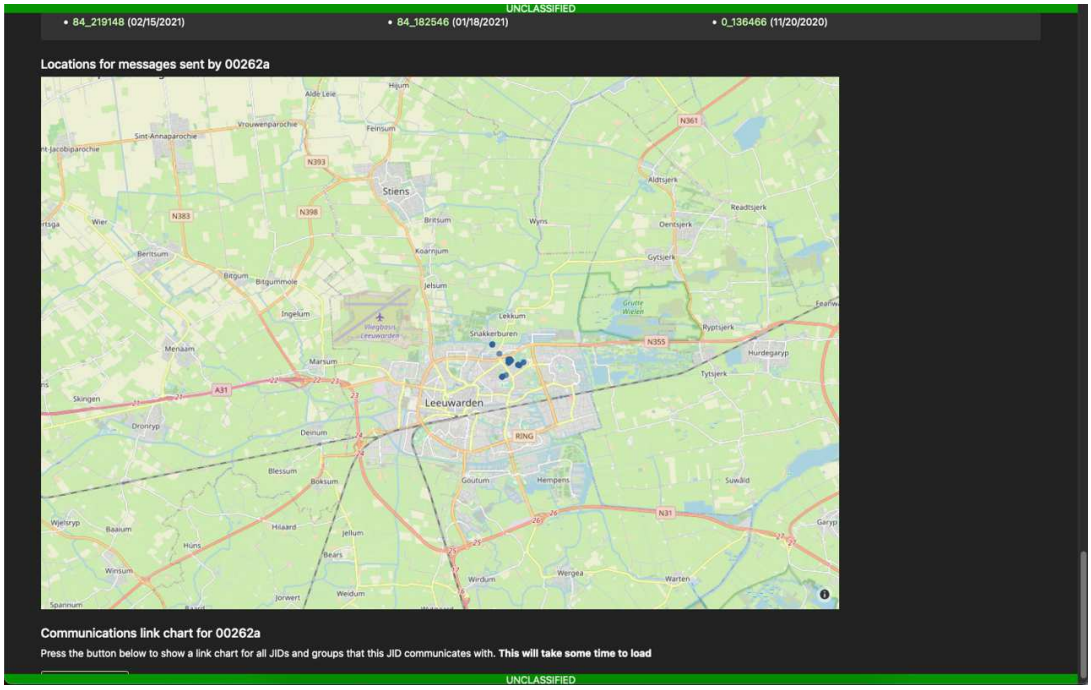
Screenshot 10.K.1

- Products that the user had sent or received messages in
  - "Products including 00262a" in the referenced screenshot



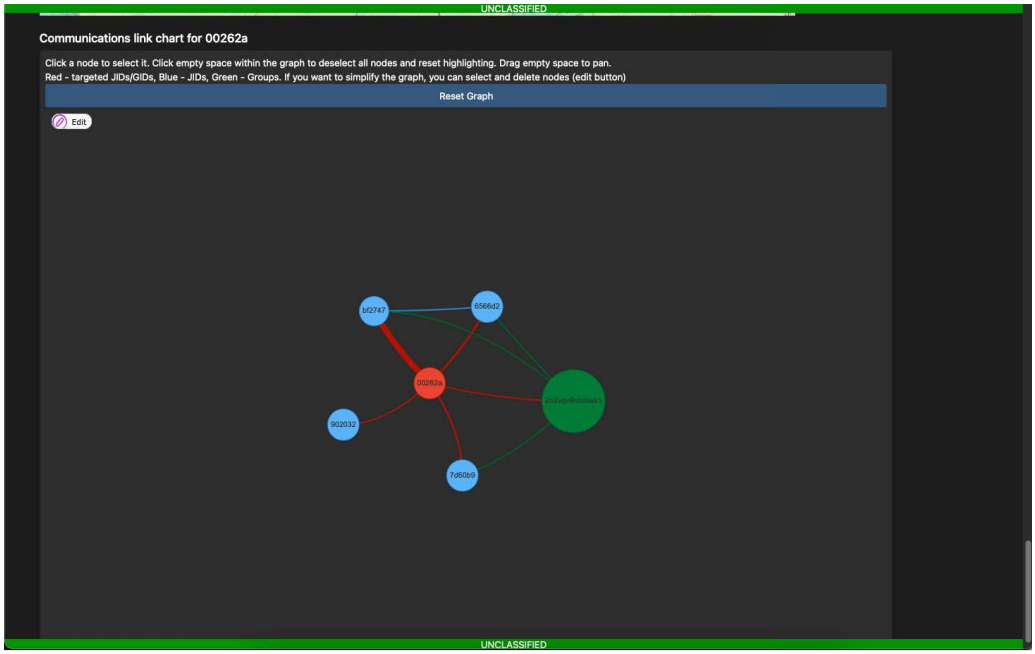
Screenshot 10.K.2

- If GPS data for messages was available it was displayed. Additional information can be found in Appendix A, 8.2.
    - “Locations for messages sent by 00262a” in the referenced screenshot



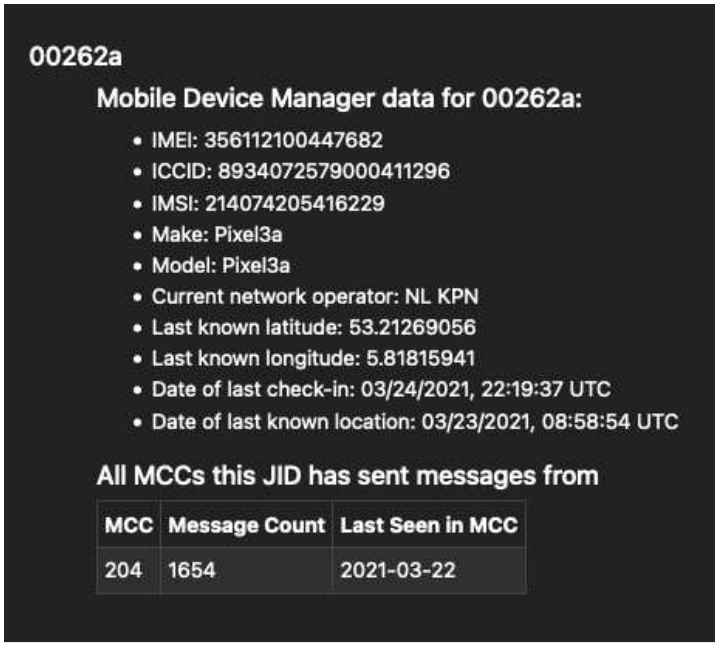
Screenshot 10.K.3

- A communications interactive link chart
    - “Communications link chart for 00262a” in the referenced screenshot
    - When hovering over a node, it displays the sending JID, case, and last MCC.
    - If double-clicked, the review platform user is navigated to the JID profile of the selected node.



Screenshot 10.K.4

- Mobile Device Manager (MDM) Information
  - As referenced in Appendix A.5 – 24.a, the ANØM platform was managed by a mobile device manager, and some of the information from the from MDM portals was ingested into the iBot_dec database for the purposes of providing additional information about device users.
  - Screenshot 10.K.5 shows a magnified screenshot of the MDM data for the JID in Screenshot 10.K.



Screenshot 10.K.5

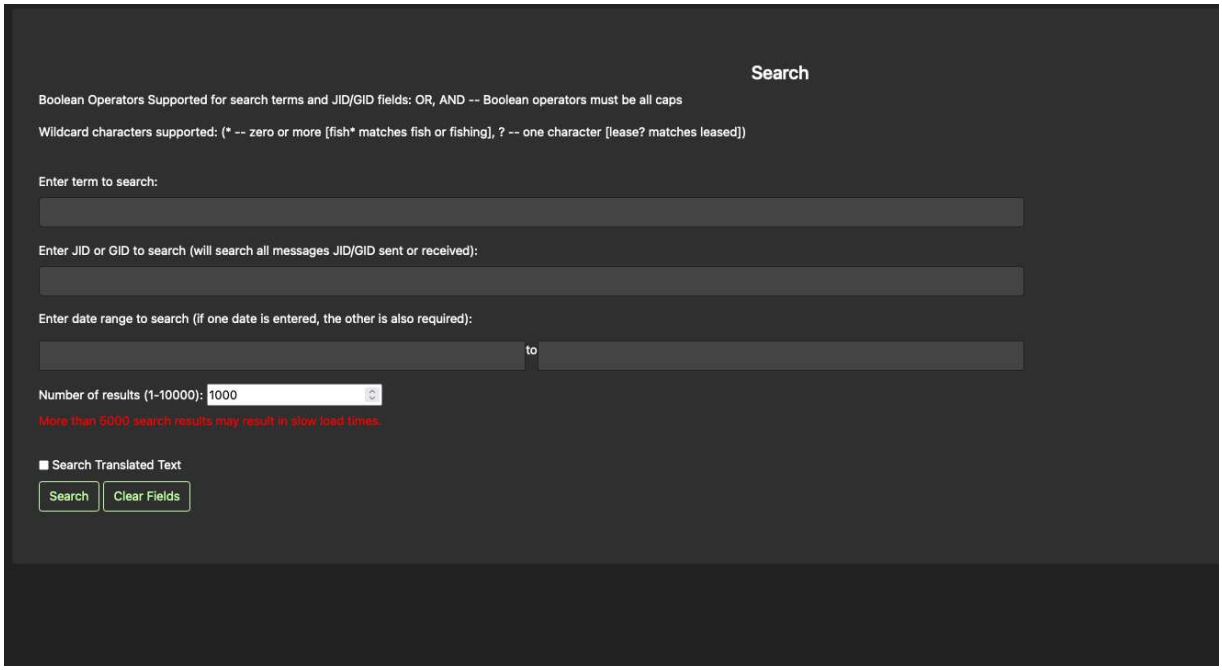
10.8 Other Pages

10.8.1 Search

The search page allows for searching within

- the ‘content’ field of messages.
- device user IDs (JIDs).
- group IDs (GIDs).

Date ranges can also be applied to filter results provided.



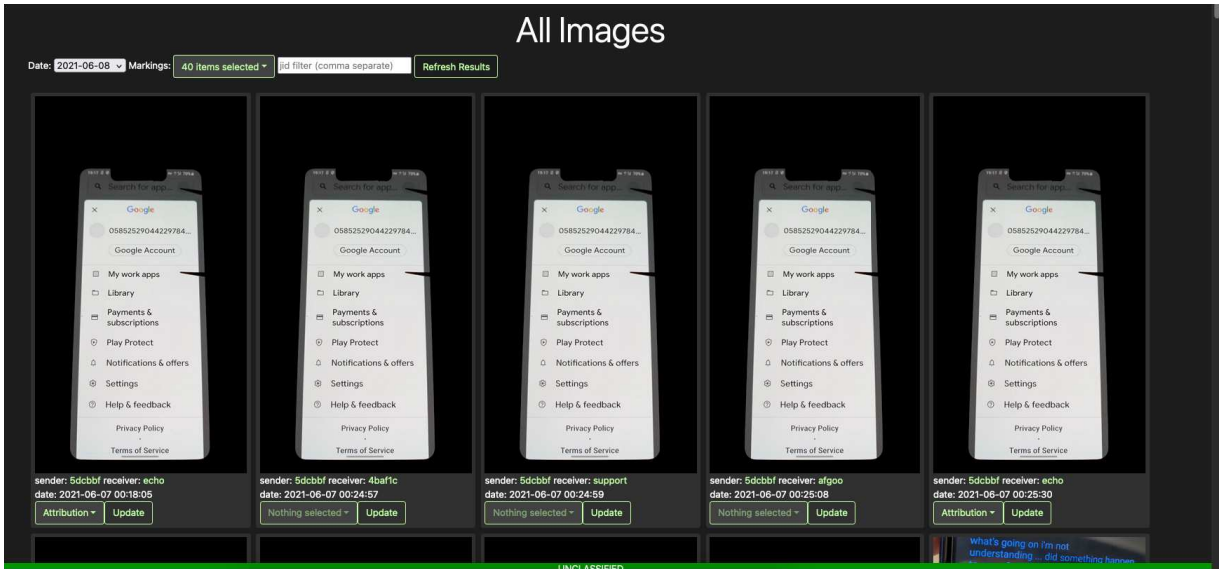
Screenshot 10.L

10.8.2 Search Notes

When review platform users add notes, they also become searchable through the Search Notes page. It has a similar interface to the Search page.

10.8.3 All Images

The All Images page provides a display page of all images within the scope of current access controls can be scrolled through, marked with attachment markings, and viewed.



Screenshot 10.M

10.8.4 Blocked

A list of messages that were blocked as described in 9.3.1.1. Additional information can be found in a future addendum.

All other pages that are navigable based on user role (reference section 8.2) are used for review platform administrators and other investigative purposes.

11. MLAT EXPORTING

MLAT requests are fulfilled by the San Diego FBI Field Office. They are submitted by different countries for a list of device users (JIDs). In order to prepare for these MLAT requests, several steps were taken to create an automated process of exporting data in a secure fashion.

11.1 All Attachment Files Pulled Down

For preparing for these requests, all attachment files were pulled down from the I1 server within AWS GovCloud. These attachment files are stored on a workstation at the San Diego FBI Field Office that can automatically create the exports.

11.2 Final MySQL Database Dump Pulled Down

Upon completion of new data packages on 6/8/2021, a full MySQL Database Dump was created and pulled down in preparation of creating exports. Timestamps of all messages exported are in Pacific Time.

11.3 MLAT Export Creation

Given a list of device users (JIDs), the database will be queried for all messages sent or received, pertinent to the device user. These messages are temporarily stored in a second database that is dumped to a '.sql' file to be added to the request fulfillment. This also includes any conversations containing the requested JID regardless of syndicate (case) assignment.

An external drive is prepared with LUKS encryption, protected with a password pre-shared with the MLAT requesters. The '.sql' file is copied to the encrypted drive, along with a list of device users (JIDs) that were requested.

The list of attachments is saved to a file while processing the data, and this file is enumerated with a second process copying each attachment file to the encrypted drive.

Following the steps described in this section will result in an MLAT export ready to be sent to the requesting country.

APPENDIX A

A.1 Public Key cryptography

1. Encryption involves encoding information so that it cannot be read by anyone who does not possess the means to decrypt it. Public Key (PK) cryptography is a recognized encryption approach whereby two different keys, referred to as the 'public' key and the 'private' key, are used to encrypt and decrypt information. These two keys are mathematically related, such that information encrypted using one can only be decrypted using the other. A single key cannot be used to encrypt and then decrypt the same information. This means that information encrypted using the public key is secure so long as the private key is protected. It will be illegible to anyone who lacks the private key.

2. PK cryptography has many applications and is commonplace on the Internet, Transport Layer Security (TLS) is an example of the implementation of PK cryptography.

3. TLS is a commonly used security mechanism that protects data exchanged with many internet websites and can be identified by the presence of a padlock icon in the address bar of a web browser. For example, the padlock icon is often present on websites such as banks, webmail, and Google, assuring the user the information they exchange with the site is secure. This transport security further prevents data that is being exchanged between a server and a client from being observed in transit by a third party. Any website that you visit where the padlock icon is displayed in the address bar of the web browser is using PK cryptography to protect your data.

4. Examples of the padlock icon displayed in the address bar when visiting the Commonwealth Bank of Australia website, for the Chrome, Firefox and Safari web browser applications are shown for reference:

5. Because PK cryptography requires significant processing power, it is not generally used to encrypt large amounts of data. A recognized alternative to this is to use a symmetric key, known as the session key in TLS, to encrypt the data and then use PK cryptography to encrypt this key. The encrypted key is then bundled with the encrypted data. The holder of the private key can then decrypt the symmetric key, and subsequently use it to decrypt the data.

A.2 Hashes

6. A ' hash ' function is a mathematical relationship, whereby input data of arbitrary size (referred to as the 'message') is processed into output data of fixed size (referred to as the 'message digest' or ' hash value'). Some hash functions have cryptographic applications. These include the

Secure Hash Algorithm 2 ('SHA-2') family of algorithms developed by the US National Security Agency and published by the US Department of Commerce as part of the Federal Information Processing Standards (FIPS), which are publicly available on the Internet.

7. The SHA-2 algorithms can be used to verify the integrity of data (including computer files) because it is highly improbable that two different messages will correspond to the same hash value. This includes where one message has been altered, resulting in a different message. This is explained in FIPS Publication 180-4:

> *The hash algorithms specified in this Standard are called secure because, for an algorithm, it is computationally infeasible 1) to find a message corresponds to a given message digest, or 2) to find two different messages that produce the same message digest. Any change to a message will, with a very high probability, result in a different message digest. This will result in a verification failure...*

8. The Message Digest 5 (MD5) algorithm, although no longer considered suitable for cryptographic purposes, is suitable and commonly used for purposes such as creating checksum values to verify against unintentional data corruption. It is often represented as 32 hexadecimal characters, which consist of the numbers 0 to 9, and the letters A to F.

9. A hash is designed to be an irreversible process, as it produces a fixed-length message digest for any given length message input. A simple example analogy is to take the sum of two numbers, which produces a result (for example: 23 + 78 = 101). It is extremely difficult to determine exactly which two numbers were used to produce the output result (101), but one could work through every single combination to identify combinations that do. This process would be known as a 'brute force', and each combination found would be known as a 'hash collision'. If you further complicated the equation that produces the result - for example, including multiplication, subtraction and division, in combination with the original addition - this would in turn make identifying number combinations much more difficult and time consuming. This further complication would also result in a lower subset of potential original input values.

10. Given the complexity of the hashing functions, mathematicians and crypto-analysts spend a lot of time trying to reverse the function, to prove that it is indeed a one-way function. This results in the only remaining way to identify an original input message from a hash digest is to undertake a brute force attempt, which is a prohibitively lengthy process.

A.3 THE ANØM PLATFORM

11. The ANØM communications network (ANØM) provides end-to-end encrypted, closed- network messaging capability between users of ANØM. By closed- network, I mean that the end-to-end encrypted communications can only occur between users of ANØM. It is a subscription-based service, requiring the purchase of smartphones (handsets) which are specifically configured to communicate on ANØM, and only handsets that have been accordingly set up can participate.

12. The Federal Bureau of Investigation enlisted third parties to setup and operate ANØM, including primary responsibility for development of the application, management and maintenance of the infrastructure to facilitate the ANØM functionality (ANØM administrators).

A.3.1 End-to-end encryption

13. End-to-end encryption refers to an encryption scheme where message content can only be read by the parties involved in the communication, typically involving the implementation of Public Key cryptography.

14. End-to-end encryption ensures that the original message content is not able to be read by the provider of the messaging service, or any third-party system or network which the message may be transmitted over. End-to-end encrypted messaging is implemented and available on recognized platforms such as Apple's iMessage; Facebook's Messenger and WhatsApp platforms; and the Telegram messaging platform.

15. Without end-to-end encryption, parties that are not the sender and intended recipients can access and read the original message. Examples where end-to-end encryption is not commonly implemented include Email services, where the service provider can read emails stored within an individual 'mailbox'; SMS communications, and facsimiles, where a network provider who operates infrastructure between the parties can also view the original content of the message as it transits their infrastructure. A postcard, sent via traditional public postal mail services, is a non-technical example of how without end-to-end encryption, anyone can read the message during its journey from the sender to the intended recipient.

16. ANØM uses Extensible Messaging and Presence Protocol (XMPP) to enable communications between participants of ANØM. XMPP is an industry recognized and publicly available framework that can be modified, adapted and built upon as required.

17. ANØM enables participants to send end-to-end encrypted messages - consisting of text and attachments such as images, videos, notes and short voice messages - to other users on ANØM.

18. Each user on ANØM is identified by a unique user identifier (user ID), known technically as a Jabber Identifier (JID). Initially, this user ID took the form of 6 alpha-numeric characters (for example 'aab2c3') and was automatically generated based on the handset International Mobile Equipment Identity (IMEI) number.

19. The handset IMEI number was combined with a fixed set of characters (known as a 'salt'), to create an input value. The input value was hashed using the MD5 algorithm. The last six characters of the resulting hash was the handset user ID, and the user password was the entire hash value. This process was performed automatically by the ANØM app, which used this user ID and password to automatically authenticate with ANØM servers.

20. It is possible to calculate a user ID for a given IMEI, as the MD5 hash process, including the salt value, is known to AFP.

A.4 The Provisioning Portal

21. The provisioning portal (the portal) was a website set up in January 2021 by the ANØM operator, and enabled the management of end-user accounts, handsets and subscriptions.

22. Access to the portal was limited generally to handset resellers and ANØM administrators, providing functionality to set-up new handsets for operation on ANØM; retire a handset; or initiate a remote wipe of a handset. Access to the portal was protected by a username and password, and also required the authorized user to connect via a Virtual Private Network (VPN) connection, which was only available to those authorized by the ANØM operator.

23. In December 2020, due to changes in the Android Operating System, the IMEI number was not able to be used to automatically generate the user ID. As a result, the user ID format was changed to be automatically generated by the provisioning portal. In this new process, the user ID consisted of two random English words combined together, for example: "LITTLE" and " FI SH", would create the user ID " LITTLEFISH ".

A.5 Handsets

24. Handsets used on ANØM consisted of mobile smartphones running the Android mobile operating system that:

    a. Have been enrolled into a private Mobile Device Management (MDM) application, set up and controlled by the ANØM administrators. The MDM essentially enabled the administrators to facilitate or limit certain features on the handsets; and

    b. Have the ANØM end- to-end custom encrypted communications application installed (the app). The app is only available to handsets that had been enrolled into the MDM.

25. Handsets were provisioned prior to being delivered to the intended user. By provisioned, I mean installation and configuration of the required software and settings to enable the handset to access and communicate using ANØM. Included as Annexure B and C are two documents that were provided by the ANØM administrators as guides for the provisioning process. Provisioning includes:

    a. Installation of the required version of mobile operating system, if required;

    b. If required, provision of an active Subscriber Identity Module (SIM) card, typically sourced from one of the following international mobile network telecommunications providers: Jersey Telecom (JT), Telefonica or POD Group. These SIM cards were not required to be registered in the name of the handset user;

    c. Install the MDM application and enroll the handset into the MDM;

    d. Upon successful enrolment into the MDM, the ANØM app was automatically installed onto the handset;

    e. If the installed ANØM app was a version released later than January 2021, use of the provisioning portal was required to obtain an automatically generated user ID and password to uniquely identify the handset on ANØM. This was not required for earlier versions of the ANØM app, as explained at paragraph 41; and

    f. For handsets that could not automatically generate a user ID and password, manually configure the ANØM app with the user ID and password.

26. The end-user pays the reseller a subscription fee for the period of time for which they desire to remain an active user of the platform.

27. For the majority of users of ANØM, there were no other means of communicating via these handsets. Traditional features associated with mobile handsets, such as voice/video calling, Short Message Service (SMS) messages, social media applications, and access to public internet websites and email services, cannot be used on a provisioned handset, as the ability to do so is prevented by the MDM.

28. As of 8 June 2021, there were only 73 of approximately 12,500 total handsets that did have the ability to make phone calls in the traditional sense, or browse the internet via an installed 'ToR' (The Onion Router) browser application. The ability to do so was allowed by the MDM for a specific group of users referred to as 'Corporate Owned, Personally Enabled' (COPE).

29. Due to the closed-network nature of ANØM, the private app, and specific authentication credentials required, it was not possible to inadvertently send a communication across the platform from a normal mobile phone handset.

30. Each mobile handset can be uniquely identified by its International Mobile Equipment Identity (IMEI) number. The IMEI is a 15-digit number, comprising 14 digits plus a check digit, which provides information about the handset make, model and serial number. The IMEI can often be found physically printed or located on the handset.

31. The· first 8 digits of an IMEI are known as the Type Allocation Code (TAC), which identify the make (manufacturer) and the model of a handset. The next 6 digits are the device serial number, with the final digit being a check digit calculated using the Luhn algorithm.

32. As an example, the IMEI 358503082383242 would consist of:

    a. A TAC of 35850308, which identifies this IMEI as belonging to a Samsung Galaxy Note 8; and

    b. A serial number of 238324; and

    c. A check digit of 2.

33. During the course of ANØM's operation, there have been a variety of different handset makes and models provisioned, the most common being either Google Pixel, Samsung Galaxy or Xiaomi. All handsets were running a version of the Android operating system.

A.5 Network connectivity to the platform

34. As stated at paragraph 42.b.ii, handsets may be provided to the end-user with an international SIM card, which would provide international roaming data using a mobile network located within the host country where the handset is operating. Alternatively, an end-user can utilize a SIM card from a mobile telecommunications provider they have sourced.

35. The handset user may also elect to connect to any available wireless data (WiFi) n.et work, instead of using a mobile network data connection.

A.6 The Mobile Device Management Component

36. During the operation of ANØM, there were two MDM applications and associated infrastructure utilized, MobileIron and FieldX. Both MDM applications provide similar core functionality as described below.

37. The role of the MDM component was to provide and enforce certain handset features via the application of an 'MDM policy', set by the ANØM administrators. Examples of such features include, but are not limited to:

    a. Initiate a remote 'factory reset' of a handset, which would erase all data, including applications, from the handset;

    b. Enforcement of a device password policy, ensuring that the password meets complexity requirements such as minimum length and character sets;

    c. Prevent enabling ' developer options', which would facilitate a user to enable 'USB debugging' amongst other available options, that could be used to circumvent handset restrictions, or otherwise tamper with the handset's integrity;

d. Maintaining a secured handset boot loader, which ensures only the platform approved mobile handset operating system is allowed to run, ensuring handset integrity and security;

e. Prevent installation of untrusted or unapproved applications, which ensures only applications available through the ANØM MDM can be installed and run on the handset;

f. In the case of the FieldX MDM, ensuring the ANØM app is updated automatically;

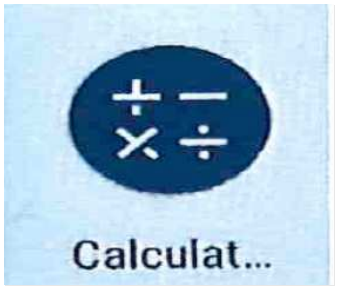
g. Reporting handset information periodically, such as but not limited to, unique handset IMEI, compliance with MDM policy, handset boot loader and operating system versions, and handset status such as battery and internal storage levels.

38. The MDM component utilizes functionality that is part of the core Android mobile operating system on the handset, communicating with MDM servers to report handset status, and retrieve policies to enforce on the handset.

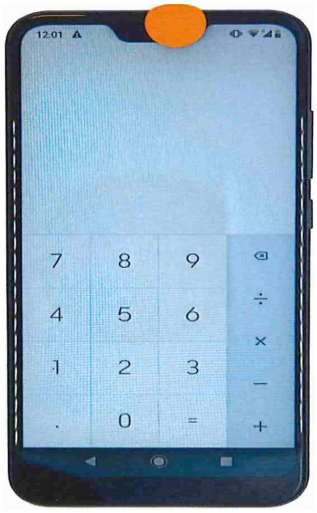
A.7 The ANØM Application

39. The ANØM application (the app) appears on the handset, under the disguise of a working 'calculator' application. Both the app icon, and calculator label, do not reveal the application's true purpose. Examination by an unknowing user would not indicate the presence of an encrypted messaging application.

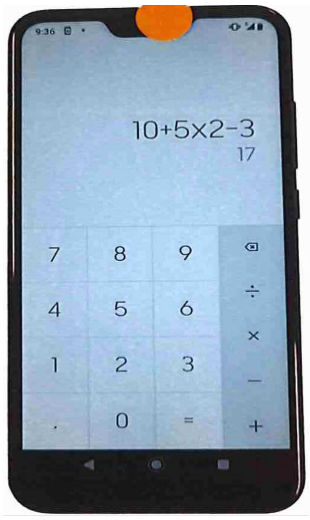
40. An example of the app icon, as would have appeared on some handsets is shown (the style of icon was dependent on the operating system version):



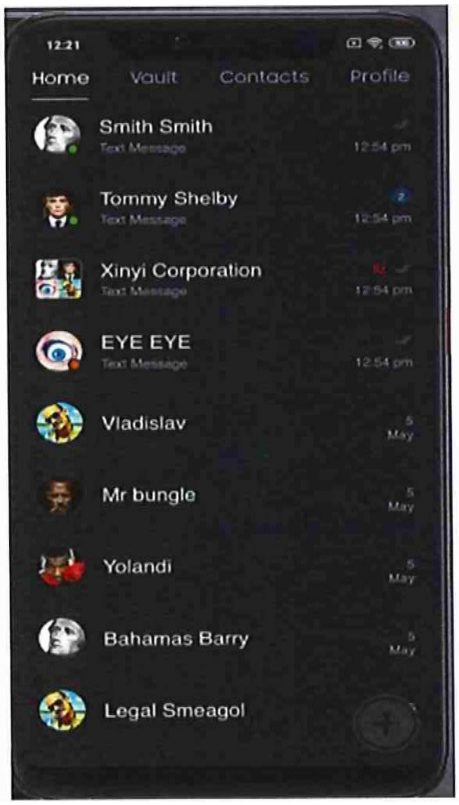
41. Once the app is launched, the user is presented with an interface that continues to reflect that of a calculator:



42. This calculator functions as expected, in that a user can enter mathematical functions, and the correct result is returned.



43. If the user enters a secret personal identification number (PIN) (access PIN), and then presses and holds the equals ('=') symbol, the true platform application appears:



44. Along with the app access PIN, there also exists a 'duress' PIN, which if used instead of the access PIN, along with a long press on the equals symbol, initiated a deletion of all information from within the app.

45. The app duress PIN could, for example, be provided to an unauthorized user of the handset if the owner is coerced or otherwise agreed to voluntarily unlock the app. While access to the app would still occur, all data would be deleted from within the app. An example of where this might occur is if law enforcement were to seize the phone and require the access PIN, the authorized user could instead provide the duress PIN, resulting in the appearance of cooperation but in fact would trigger the removal of any potential evidentiary material.

A.7.1 ANØM Application Attributes

A.7.1.1 User Identifier

46. Each user of the platform is identified by a unique user ID. Only one handset, at any given point, could access ANØM as a particular user ID. Once the user ID and password were entered into the app, the app automatically updates the password associated with that ANØM user ID. This updated password is stored by the app for subsequent login, however it is never presented or known to the user who entered the values. Attempts to login on another handset with the previously known password and user ID would fail, and need the password to be reset to a known value to succeed

A.7.1.2 User Display Name

47. The user of the handset can set a 'display name' (also known as a nickname, alias, or handle), which can be changed whenever the user desires. This does not change their user ID on the plat

form. This is similar to the "From" name displayed in emails that typically differs from the email address, which is often the username;

A.7.1.3 Vault

48. The vault enables the user to store notes and images on the device securely. This data is encrypted such that it is only accessible from the handset, and no data in the vault is transmitted unless the user includes it as an attachment to a message.

49. Notes stored in the vault can contain a title, along with body text or an itemized list. Images stored in the vault, or taken using the handset camera, can also be included in the body of notes.

A.7.1.4 Messages

50. A user can send an end-to-end encrypted message to another user on ANØM, providing they know the intended recipient's user ID;

51. A user can also send an end-to-end encrypted message to a group of ANØM users, and each user in that group can see the other members of the group. This group can have a label, naming the group, which can be set by any group administrator, who is typically the creator of the group, and any other members that have been granted administrator privileges for that group. This is similar to how a group chat in other messaging applications such as WhatsApp, Signal, Telegram, and Facebook Messenger function

52. A message, either to a single user or a group of users, can consist of a text message, an image (for example, a photo taken by the handset camera), a video obtained using the device's camera, a short voice (also known as Push- To-Talk, or PTT) message, or a 'notes' document from the device vault;

53. Messages can contain different languages. In order to support various language character sets, computer applications can use Unicode as a method for representing symbols and text from most of the world's writing systems. Unicode provides a unique number for every character, no matter what platform, device, application or language. It does so by expressing characters as a code number, not a glyph. For instance, the Arabic characters "ا ب و "would be represented as "\u0627\u0628\u0648" in Unicode. Symbols commonly known as 'emojis' can also be expressed as a Unicode value. For instance, "\u1F603" is the Unicode value for the emoji "😃". These Unicode values need to be converted back into the correct characters in order to be legible. Applications may interpret the Unicode characters and display the character, rather than its code;

54. A message can be quoted by selecting it in a conversation and pressing the 'reply' button, or forwarded to other recipients by selecting it and pressing the 'share' button. When this occurs, the parties to the message can visually see that the message has been quoted or forwarded, as it will appear as a quoted block within the sent message;

55. Unlike other messaging applications such as WhatsApp, or Telegram, the ANØM app did not provide indicators if a message had been received or read by the parties;

56. Audio pitch-shifting ability

57. The sender of an audio message has the option to adjust the pitch of the recording prior to it being made, either up (option known as 'Helium' in the app) or down (option known as 'Jellyfish'

in the app), which disguises the true sound of the sender's audio to the recipient. The sender can also opt for no pitch-shift to occur;

A.7.1.5 Self-Destructing Messages

58. The sender of any message type described above can also nominate to set a 'self-destruct' timer for that message, known as a 'burn time'. Setting the burn-time would remove the message from any handset which has received the message once the timer period has elapsed.

A.8 Data Recorded from the Platform

59. The ANØM app included a feature whereby when a message was sent, the app automatically sends a 'blind carbon copy' of the message to a ghost user ID, 'bot'. This process was not visible to the sending user, nor were they aware that this process occurred.

60. The automatic blind carbon copy process resulted in a copy of the message encrypted for, and sent to, the ghost user ID 'bot'. Computers running an application compatible with the platform received these encrypted messages addressed to the 'bot' user ID.

61. This process was identical to the normal platform app behavior when a message is sent, with the exception that the messages sent to the ghost user ID were not visible to the other parties of the communication.

62. A diagram depicting the message flow, and the encryption process for a hypothetical message sent from Alice to Bob, including the blind carbon copy and encryption for the ghost user ID 'bot', is included in Section 1.5.

63. A.8.1 Message contents
64. Messages that are sent using the platform usually have the following, or a combination of the following, attributes that are visible to both sender and recipients:

    a. Burn Time - This is set by the sender at the time of sending a message and defines how long a message will exist before being automatically deleted from both devices once that time has 'elapsed. It is visible on both the sender and recipient handsets, at the bottom of each message. It can be set to 30 seconds; 5 or 30 minutes; 1 or 12 hours; or 1, 3 or 7 days;

    b. Sender - The sending handset user ID and display name;

    c. Recipients - The recipients to a message can be identified by viewing the parties in the relevant message thread, which like other common chat applications such as WhatsApp, Telegram, and Facebook Messenger, appear as separate items in a message list;

    d. Content - The message content, which can consist of text or an attachment such as audio, an image, video or note.

    e. Time - The time and date in Greenwich Mean Time (GMT) according to the sending handset, when a message was sent. This would be displayed on the handset in the configured time zone. For example, a message sent on 10 June 2020, at 11: 00 am Perth time, would have the time and date as 3: 00 am on 10 June 2020 GMT. A handset in Sydney would present this time as being 1: 00 pm on 10 June 20 20 . Handsets which had an active SIM card would synchronize their time via Network Time Protocol (NTP) to the telecommunications carrier network to which it is connected.

i. See section 8.6.1 for time zone discrepancies.

A.8.2 Message meta-data

65. Messages sent over ANØM included additional meta-data that was not visible to either the sender or recipients of a message via the app . Some of these fields were included for the benefit of Law Enforcement Agencies (LEA). Due to changes and enhancements not all the following meta-data fields, or combinations of, were sent with each message:

    a. A Unique Message ID - A Universally Unique Identifier (UUID), automatically generated by the sending handset application at the time a message is sent, and is not displayed to either the sender, or recipients of a message. This is a component of the XMPP framework;

    b. IMEI - On handsets running the Android operating system version 9 or less, the IMEI number was included as meta-data with each message for LEA use;

    c. MCC / MNC - On handsets that contained an active SIM card, and were currently registered to a mobile telecommunications network, the Mobile Country Code (MCC), and Mobile Network Code (MNC), to which the handset is currently connected. These numbers were included as meta-data with the message for LEA use;

    d. Location Information - Following an app update in April 2020, the app would attempt to obtain a location via the Android Location Manager Application Programming Interface (API). If a location could be ascertained, the latitude, longitude, accuracy, and location acquisition time values, were included as meta-data with the message for LEA use. Occasionally, the app was unsuccessful in obtaining a complete and accurate GPS location. When this occurred, the GPS point collected often began with 39.0 and resolved to an area off the coast of Fiji in the South Pacific Ocean;

    e. Audio pitch adjustment - If the message contained an audio attachment, then meta-data which indicates the value of pitch-shift performed was included as meta-data with the message for LEA use;

    f. Quoted or forwarded messages - If the message contains a quote, or is a forwarded message, then the new message content will contain the quoted or forwarded content, which may also include information such as the original sender user ID, and the original message time. This was a feature of the ANØM application, and messaging applications such as WhatsApp, Signal, Telegram and Facebook Messenger have a similar feature to quote and forward messages.

A.9 Authenticity and Integrity

66. The ANØM app behavior of updating a user ID password upon initial successful login, effectively prevents another handset from authenticating and being able to send messages purporting to be another ANØM user ID. Additional information will be included in a future addendum.

67. Until the user ID format change in December 2020, the user ID was directly related to the IMEI number of the handset, further limiting the ability for ANØM messages to be sent

68. If a handset was 'factory reset', initiated either from the MDM, or on the handset itself, all data and applications - including the MDM and platform app - was removed from the handset.

69. If the app duress PIN was entered, all data, including the saved login information, was removed from the app. This would result in the user being unable to access or communicate on ANØM.

70. If either of these processes occurred, then the user ID and password would need to be reset before the handset could be used to access ANØM again. In the case of a factory reset, the handset would need to be reprovisioned.

GLOSSARY

- **AES Encryption**: Symmetric (single-key) encryption that was used for the other part of the re-encryption of data collected.
- **ANØM**: An end-to-end encrypted communications platform, utilizing dedicated mobile phone handsets with a custom messaging application installed to communicate within a closed network of participants.
- **Application Programming Interface (API)**: A software interface, commonly utilized with computer-to-computer interaction, whereby a client computer initiates a request, which is responded to by the server computer running the API, typically returning data to the requesting client computer.
- **AWS GovCloud**: Amazon Web Services cloud infrastructure where the Hola iBot web application and data related to Operation Trojan Shield was stored.
- **Boot Loader**: The first item of software that runs on a mobile phone handset upon device power up or reboot, which initializes the hardware and loads the mobile Operating System, for example, Android.
- **Cases**: Also known as Syndicates. This is the central component of relationships within the iBot_dec database.
- **Difference-Dump**: The new or changed data between two MySQL database dumps. This is how the third-party country parceled out new content from the entire database when sending new data packages.
- **Elastic Compute Cloud (EC2)**: AWS-owned computing resources that can be rented for the purpose of running computer applications.
- **End-to-end encryption**: An encryption scheme whereby data is encrypted between two end points, and only those end points have the ability to decrypt the data. The servers and networks that relay the data between the two end points are not capable of decrypting the data.
- **Extensible Messaging and Presence Protocol (XMPP)**: XMPP is an open standard protocol for instant messaging, which can facilitate multi- party chats, supporting multimedia such as voice, images and video. Anyone is free to run their own XMPP server and network and build upon the framework that is provided.
- **Ghost User ID ('bot')**: The user identifier to which the AN0MANØM application installed upon mobile handsets would send a blind carbon copy of each message which was sent from that handset.
- **GnuPG (GPG)**: allows for data encryption and signing for communications.
- **Google Compute Engine**: A service that Google Cloud provides to create and run virtual machines within Google Cloud.
- **Hash (MD5, SHA-2)**: A hash function is a mathematical process whereby the data input, or 'message', is processed into a 'message digest' or hash value of fixed length. It is commonly represented as hexadecimal characters which consist of the numbers Oto 9, and letters A-F. Hash functions are often used for data verification to identify if data has been altered, due to

the very high improbability that two different input 'messages' will result in the same hash value.

- **Hola iBot**: Custom web application built and operated by San Diego FBI to serve as the review platform of all data received from the ANØM platform.
- **iBot_dec**: The persistent database that serves data to the Hola iBot review platform. Contains data collected on the AN0MANØM platform, and presents it for review
- **iBot_enc**: The temporary database which would hold new data packages when new data was received from the third-party country's server.'
- **Ingestion-1 Server (I1)**: The AWS GovCloud EC2 that ran the Ingestion process (section 9), retained the attachment files of messages, and served the iBot_dec database
- **International Model Equipment Identifier (IMEI)**: A 15-digit number assigned to a mobile handset which can be used as an identifier. It consists of an 8-digit Type Allocation Code (TAC) that reports the manufacturer and model of the handset, a 6-digit serial number, and the last number being a 'check digit' using the Luhn algorithm.
- **Location Information**: Information that identifies a location, which may be a region or area, and typically consists of latitude and longitude values as well as a timestamp in Universal Co-ordinated Time (UTC) of the location fix. The location may be obtained from Global Navigation Satellite Systems (GNSS), such as GPS or GLONASS, or determined based on information about nearby mobile cell towers and WiFi access points.
- **Mobile Country Code (MCC)**: The Mobile Country Code uniquely identifies the country of origin for the mobile subscriber, and is the first three digits that make up the International Mobile Subscriber Identity (IMSI) number, securely stored within the Subscriber Identity Module (SIM) card. For example, Australia has the MCC value of 505.
- **Mobile Device Management (MDM)**: A software application, consisting of a mobile device component, and a server component, which is commonly used by entities that wish to enforce certain device features, known as a 'policy', to assist in device integrity, security and useability. MDM's also commonly possess the ability to remotely wipe a device to prevent information
- **Mobile Network Code (MNC)**: The Mobile Network Code can consist of two or three digits which identifies the home mobile network for the mobile subscriber. It is the two or three digits following the MCC that make up an International Mobile Subscriber Identity (IMSI) number, securely stored within the Subscriber Identity Module (SIM) card. The following are Australian mobile netw9rk operator example values (not a comprehensive example); Telstra is 01, Optus is 02, and Vodafone is 03.
- **MySQL Dump**: a logical backup of all tables, including content, within a MySQL Database.
- **New Data Package**: A package of new data collected from the ANØM platform sent by the third-party country to the I1 server.
- **Portal**: A website accessible over the internet, with the use of a private Virtual Private Network connection, requiring a valid username and password provided by the ANØM administrators, to assist with the ANØM end-user device, account and user ID management.
- **Proxy**: A server that acts as a relay of all network traffic between two computers or servers

- **Public Key Cryptography/ Public Key Encryption**: An encryption and decryption scheme whereby a pair of keys that are mathematically related are used to encrypt and decrypt content. The 'public' key can be used to encrypt content, which only the 'private' key can decrypt, and vice-versa. The same key cannot be used to decrypt content that was encrypted by it.
- **RAM**: Temporary computer storage. For example, this is where all temporary data structures would be stored for ingestion.
- **RSA Encryption:** A type of PKI encryption scheme that was used for part of the re-encryption of data collected.
- **Subscriber Identity Module (SIM)**: The Subscriber Identity Module is a physical integrated circuit card that securely stores the International Mobile Subscriber Identity (IMSI) number and its related authentication key, used to uniquely identify and authenticate a mobile subscriber (end-user) to a mobile network. The SIM card also contains a unique serial number, known as the Integrated Circuit Card Identifier (ICCID) which may be printed on the SIM card itself.
- **Transport Layer Security (TLS)**: An implementation of Public Key Cryptography, commonly used to secure information exchanged with internet websites such as banking, email and internet search engines. Its use can be identified by the presence of a closed padlock icon present in the address bar of a web browser. TLS can also be used to secure communications for other purposes, such as instant messaging applications and Voice over Internet Protocol (VoIP).
- **Unicode**: Unicode is a method for representing symbols and text from most of the world's writing systems. This is achieved by expressing characters as a number, not the glyph. 'Emojis' are a common glyph that would be expressed using the Unicode value for example in messaging applications but presented to a human as the glyph.
- **USB Debugging**: The ability to connect a computer to a mobile handset via a Universal Serial Bus (USB) interface cable, and interact with the mobile operating system. It can be used to add or remove data from a handset, read logs, or install and remove applications. It can also be used to replace the operating system on a mobile handset, or install processes that run with elevated privileges - also known as 'root' a device.
- **User ID (JID)**: A username that uniquely identified a user on the AN0MANØM platform. Initially comprising of six characters consisting of the numbers Oto 9, and letters A to F; later, this became two random English words combined together.
- **Virtual Private Network (VPN)**: A networking application used to encrypt data exchanged over an untrusted network connection, commonly the Internet. VPN's were traditionally used to ‘extend' a private network, that is one not accessible if not directly connected such as a corporate network of computers, over an Internet connection. This would enable a remote device to access websites, files, data and services that are not accessible outside the private network. VPN's can also be used to masquerade the identity or destination of a user's internet activity from their Internet Service Provider (ISP).
- **XMPP**: *See Extensible Messaging and Presence Protocol (XMPP)*

Polisen

Bilaga - Skäligen misstänkt

Enhet	Diarienr
Region Bergslagen, Grova brott 1 PO Örebro	5000-K642266-21

Skäligen misstänkt person	Personnr
Bogebrink, Tommy Eric Rickard	19741206-6297

Identifierad	Kontrollsätt	Kommentar
Ja	Annat	Annat

Polisen

Personalia och dagsbotsuppgift

Utskriftsdatum
2022-03-28

Namn			Personnummer
Bogebrink, Tommy Eric Rickard			19741206-6297
Tilltalsnamn	Kallas för	Öknamn	Kön
Tommy			Man
Födelseförsamling	Födelselän	Födelseort utland	
Karlstad	Värmlands län		
Medborgarskap	Hemvistland	Telefonnr	
Sverige		0762303906: Mobiltelefon	
Adress			
Renstiernas Gata 23 116 31 Stockholm			
Folkbokföringsort		Senast kontrollerad mot folkbokföring	
		2020-03-24	

Föräldrars/Vårdnadshavares namn och adress (beträffande den som inte fyllt 20 år)

Utbildning

Yrke / Titel

Arbetsgivare | Telefonnr

Anställning (nuvarande och tidigare)

Arbetsförhet och hälsotillstånd

Kompletterande uppgifter

Uppgiven inkomst	Bidrag	Hemmavarande barn under 18 år
Försörjningsplikt		Skulder
Förmögenhet		

Kontroll utförd

Taxerad inkomst	Taxeringsår
Taxeringskontroll utförd av	Datum - -

Polisen

Bilaga - Skäligen misstänkt

Enhet	Diarienr
Region Bergslagen, Grova brott 1 PO Örebro	5000-K1490612-20

Skäligen misstänkt person	Identifierad	Anledning	Personnr
Brzozowiec, Pawel	Nej	Personen ej närvarande	19871101-9698

Polisen

Personalia och dagsbotsuppgift

Utskriftsdatum
2022-03-28

Namn			Personnummer
Brzozowiec, Pawel			19871101-9698
Tilltalsnamn	Kallas för	Öknamn	Kön
			Man
Födelseförsamling	Födelselän	Födelseort utland	
		Wlodawa	
Medborgarskap	Hemvistland	Telefonnr	
Polen		0739338344: Mobiltelefon	
Adress		+48511822920: Annat telefonnummer mamma	
Skonbergavägen 5 LGH 1201			
589 41 Linköping			
Folkbokföringsort		Senast kontrollerad mot folkbokföring	
Linköping		2021-04-27	

Föräldrars/Vårdnadshavares namn och adress (beträffande den som inte fyllt 20 år)

Utbildning

Yrke / Titel

Arbetsgivare | Telefonnr

Anställning (nuvarande och tidigare)

Arbetsförhet och hälsotillstånd

Kompletterande uppgifter

Uppgiven inkomst	Bidrag	Hemmavarande barn under 18 år
420000	0	0
Försörjningsplikt		Skulder
-		0
Förmögenhet		
0		

Kontroll utförd

Taxerad inkomst	Taxeringsår
366100	2019
Taxeringskontroll utförd av	Datum
Utr. E. Lundby	2020-06-05

Polisen

Bilaga - Skäligen misstänkt

Enhet	Diarienr
Region Bergslagen, Grova brott 1 PO Örebro	5000-K1490612-20

Skäligen misstänkt person	Personnr
Glowka, Michal Andrzej	19921019-

Identifierad	Kontrollsätt	Kommentar
Ja	Pass (utländskt)	Polskt pass

Polisen

Personalia och dagsbotsuppgift

Utskriftsdatum
2022-03-28

Namn			Personnummer
Glowka, Michal Andrzej			19921019-
Tilltalsnamn	Kallas för	Öknamn	Kön
			Man
Födelseförsamling	Födelselän	Födelseort utland	
Medborgarskap	Hemvistland	Telefonnr	
Adress			
Folkbokföringsort		Senast kontrollerad mot folkbokföring	
		- -	

Föräldrars/Vårdnadshavares namn och adress (beträffande den som inte fyllt 20 år)

Utbildning

Yrke / Titel

Arbetsgivare | Telefonnr

Anställning (nuvarande och tidigare)

Arbetsförhet och hälsotillstånd

Kompletterande uppgifter

Uppgiven inkomst	Bidrag	Hemmavarande barn under 18 år
Försörjningsplikt		Skulder
Förmögenhet		

Kontroll utförd

Taxerad inkomst	Taxeringsår
Taxeringskontroll utförd av	Datum
	- -

Polisen

Bilaga - Skäligen misstänkt

Enhet	Diarienr
Region Bergslagen, Grova brott 1 PO Örebro	5000-K642266-21

Skäligen misstänkt person	Personnr
Jovanovic, Alexander	19550203-2617

Identifierad	Kontrollsätt	Kommentar
Ja	Annat	Annat

Polisen

Personalia och dagsbotsuppgift

Utskriftsdatum
2022-03-28

Namn			Personnummer
Jovanovic, Alexander			19550203-2617
Tilltalsnamn	Kallas för	Öknamn	Kön
			Man
Födelseförsamling	Födelselän	Födelseort utland	
		Arandjelovac Bukovic	
Medborgarskap	Hemvistland	Telefonnr	
Sverige		086003652: Hemtelefon	
Adress		0734345558: Mobiltelefon	
Forelltorget 2 LGH 1402			
141 47 Huddinge			
Folkbokföringsort		Senast kontrollerad mot folkbokföring	
Huddinge		2021-04-20	

Föräldrars/Vårdnadshavares namn och adress (beträffande den som inte fyllt 20 år)

Utbildning

Yrke / Titel

Arbetsgivare | Telefonnr

Anställning (nuvarande och tidigare)

Arbetsförhet och hälsotillstånd

Kompletterande uppgifter

Uppgiven inkomst | Bidrag | Hemmavarande barn under 18 år

Försörjningsplikt | Skulder

Förmögenhet

Kontroll utförd

Taxerad inkomst | Taxeringsår

Taxeringskontroll utförd av | Datum

- -

Polisen

Bilaga - Skäligen misstänkt

Enhet	Diarienr
Region Bergslagen, Grova brott 1 PO Örebro	5000-K1490612-20

Skäligen misstänkt person	Personnr
Lindberg, Jens Erik Lennart	19620527-0017

Identifierad	Kontrollsätt	Kommentar
Ja	Annat	Res bild

Polisen

Bilaga - Skäligen misstänkt

Enhet	Diarienr
Region Bergslagen, Grova brott 1 PO Örebro	5000-K1490612-20

Skäligen misstänkt person	Identifierad	Anledning	Personnr
Michalski, Jakub	Nej	Personen ej närvarande	19841204-7675

Polisen

Personalia och dagsbotsuppgift

Utskriftsdatum
2022-03-28

Namn			Personnummer
Michalski, Jakub			19841204-7675
Tilltalsnamn	Kallas för	Öknamn	Kön
Jakub			Man
Födelseförsamling	Födelselän	Födelseort utland	
		Elblag	
Medborgarskap	Hemvistland	Telefonnr	
Polen		0767090380: Mobiltelefon	

Adress
c/o Radek Rykowski
Bäckgårdsvägen 4
143 42 Vårby

Folkbokföringsort	Senast kontrollerad mot folkbokföring
	2019-11-12

Föräldrars/Vårdnadshavares namn och adress (beträffande den som inte fyllt 20 år)

Utbildning

Yrke / Titel

Arbetsgivare	Telefonnr

Anställning (nuvarande och tidigare)

Arbetsförhet och hälsotillstånd

Kompletterande uppgifter
Jakub uppger att han har skulder men kan inte ange hur mycket.

Uppgiven inkomst	Bidrag	Hemmavarande barn under 18 år
180000	0	0
Försörjningsplikt		Skulder
2		
Förmögenhet		
0		

Kontroll utförd

Taxerad inkomst	Taxeringsår
79400	2017
Taxeringskontroll utförd av	Datum
Sanne Wessman	2020-11-23

Polisen

Bilaga - Skäligen misstänkt

Enhet	Diarienr
Region Bergslagen, Grova brott 1 PO Örebro	5000-K1490612-20

Skäligen misstänkt person	Identifierad	Anledning	Personnr
Walczak, Jakub Krzysztof	Nej	Personen ej närvarande	19850204-0952

Polisen

Underrättelse/Delgivning jml RB 23:18a

Enhet
Region Bergslagen, Grova brott 1 PO Örebro

Ärende

Diarienr
5000-K1490612-20

Handläggare
Rehn, Lisa

Gärning
Synnerligen grovt narkotikabrott med mera

Berörd person

Personnr	Efternamn	Förnamn
19871101-9698	Brzozowiec	Pawel

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd	Delgiven info. om ev. förenklad delgivning
		2022-04-01	2022-02-22

Underrättelsesätt
Ordinär

Notering
Inlämnat till häktet

Erinran

Försvarare

Namn
Jerzy Misiowiec

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
		2022-04-01

Underrättelsesätt
Ordinär

Notering
Finns för upphämtning i reception polishuset Örebro, Järnvägsgatan 3, enligt överenskommelse.

Erinran

Polisen

Underrättelse/Delgivning jml RB 23:18a

Enhet
Region Bergslagen, Grova brott 1 PO Örebro

Ärende

Diarienr
5000-K1490612-20

Handläggare
Rehn, Lisa

Gärning
Synnerligen grovt narkotikabrott med mera

Berörd person

Personnr	Efternamn	Förnamn
19841204-7675	Michalski	Jakub

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd	Delgiven info. om ev. förenklad delgivning
		2022-04-01	

Underrättelsesätt
Ordinär

Notering
Inlämnad till häktet

Erinran

Försvarare

Namn
Ulf G V Tollhage

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
		2022-04-01

Underrättelsesätt
Ordinär

Notering
Finns för upphämtning i reception polishuset Örebro, Järnvägsgatan 3, enligt överenskommelse.

Erinran

Polisen

Underrättelse/Delgivning jml RB 23:18a

Enhet
Region Bergslagen, Grova brott 1 PO Örebro

Ärende

Diarienr
5000-K642266-21

Handläggare
Rehn, Lisa

Gärning
Synnerligen grovt narkotikabrott med mera

Berörd person

Personnr	Efternamn	Förnamn
19741206-6297	Bogebrink	Tommy Eric Rickard

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd	Delgiven info. om ev. förenklad delgivning
		2022-04-01	

Underrättelsesätt
Ordinär

Notering

Erinran

Försvarare

Namn
Melkemichel, Jack

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
		2022-04-01

Underrättelsesätt
Ordinär

Notering
Finns för upphämtning i reception polishuset Örebro, Järnvägsgatan 3, enligt överenskommelse.

Erinran

Polisen

Underrättelse/Delgivning jml RB 23:18a

Enhet
Region Bergslagen, Grova brott 1 PO Örebro

Ärende

Diarienr
5000-K1490612-20

Handläggare
Rehn, Lisa

Gärning
Synnerligen grovt narkotikabrott med mera

Berörd person

Personnr	Efternamn	Förnamn
19921019-	Glowka	Michal Andrzej

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd	Delgiven info. om ev. förenklad delgivning
		2022-04-01	

Underrättelsesätt
Ordinär

Notering
Inlämnat till häktet

Erinran

Försvarare

Namn
Janette Stjernström

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
		2022-04-01

Underrättelsesätt
Ordinär

Notering
Finns för upphämtning i reception polishuset Örebro, Järnvägsgatan 3, enligt överenskommelse.

Erinran

Polisen

Underrättelse/Delgivning jml RB 23:18a

Enhet
Region Bergslagen, Grova brott 1 PO Örebro

Ärende

Diarienr
5000-K1490612-20

Handläggare
Rehn, Lisa

Gärning
Synnerligen grovt narkotikabrott med mera

Berörd person

Personnr	Efternamn	Förnamn
19620527-0017	Lindberg	Jens Erik Lennart

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd	Delgiven info. om ev. förenklad delgivning
		2022-04-01	2021-12-06

Underrättelsesätt
Ordinär

Notering
Inlämnat till häktet

Erinran

Försvarare

Namn
Patric Lindblom

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
		2022-04-01

Underrättelsesätt
Ordinär

Notering
Finns för upphämtning i reception polishuset Örebro, Järnvägsgatan 3, enligt överenskommelse.

Erinran

Polisen

Underrättelse/Delgivning jml RB 23:18a

Enhet
Region Bergslagen, Grova brott 1 PO Örebro

Ärende

Diarienr
5000-K642266-21

Handläggare
Rehn, Lisa

Gärning
Synnerligen grovt narkotikabrott med mera

Berörd person

Personnr	Efternamn	Förnamn
19550203-2617	Jovanovic	Alexander

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd	Delgiven info. om ev. förenklad delgivning
		2022-04-01	

Underrättelsesätt
Ordinär

Notering
Inlämnad till häktet

Erinran

Försvarare

Namn
Larsson, Martin

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
		2022-04-01

Underrättelsesätt
Ordinär

Notering
Finns för upphämtning i reception polishuset Örebro, Järnvägsgatan 3, enligt överenskommelse.

Erinran

Polisen

Underrättelse/Delgivning jml RB 23:18a

Enhet
Region Bergslagen, Grova brott 1 PO Örebro

Ärende

Diarienr
5000-K1490612-20

Handläggare
Rehn, Lisa

Gärning
Synnerligen grovt narkotikabrott med mera

Berörd person

Personnr	Efternamn	Förnamn
19850204-0952	Walczak	Jakub Krzysztof

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd	Delgiven info. om ev. förenklad delgivning
		2022-04-01	

Underrättelsesätt
Ordinär

Notering
Inlämnat till häktet

Erinran

Försvarare

Namn
Richard Backenroth

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
		2021-04-01

Underrättelsesätt
Ordinär

Notering
Finns för upphämtning i reception polishuset Örebro, Järnvägsgatan 3, enligt överenskommelse.

Erinran