



Protokollbilaga

Åklnr
AM-76985-21

Signerat av

Arkiv/Åkl. ex

Enhet

Region Syd, Grova brott 1 PO S Skåne

Handläggare (Protokollförare)

Petra Bagge

Bitr. handläggare

Maria Hagefjord

Undersökningsledare

Thomas Ahlstrand

Polisens diarienummer

5000-K654768-21

Signerat av
Doha 8Datum: 2022-01-28
2021-12-09
AKTBIL: 145

Personer i ärendet

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

Notering

Protokollbilaga 1

Innehållsförteckning

Diariernr	Uppgiftstyp	Sida
	Tekniska dokument Anom	
5000-K654768-21	Information från krypterad kommunikationstjänst.....	3
	Beskrivning av information i Anom-data.....	5
	Polismyndighetens hantering av Anom-data.....	22
	Yttrande Positionsdata i meddelanden skickade med Anom.....	46
	Teknisk information om Operation Trojan Shield.....	49
	Presentation av bearbetat material Anom	
	Presentation av Anom material, bearbetning mm.....	103
	Brukaranalys Anom	
	<i>Oscar Thomsen</i>	
	Brukaranalys Oscars telefon -2893.....	108
	Brukaranalys JID 8191be.....	112
	<i>Atif Perviz</i>	
	Brukaranalys JID c3b5d4.....	123



Polisen

Polismyndigheten
Nationella operativa avdelningen

PM

Datum
2021-06-08

Diariennr (åberopas)

1 (2)

Information från krypterad kommunikationstjänst

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.

Nationella operativa avdelningen

2021-06-08

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 klockan 02.00 natten mot den 7 juni 2021. Detta genom att den tekniska lösningen togs ner och enheterna kan inte längre kommunicera på plattformen.

A605.834/2021

IT-avdelningen

Anøm

Beskrivning av information i 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

Diariennr. AXX

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.

Detta dokument beskriver den innehållet i den dekrypterade informationen. Detta innehåll består av meddelanden, användarkonton och metadata kring dessa.

För beskrivning av Polisens hantering av dekrypterad information från Anom hänvisas till dokumentet ”*Beskrivning av Polisens hantering av Anom-data*”

Innehållsförteckning

SAMMANFATTNING	I
INNEHÅLLSFÖRTECKNING	II
1 INLEDNING	1
1.1 Bakgrund.....	1
1.2 Syfte	1
2 INNEHÅLL I MLAT EXPORTER	1
2.1 Databasstruktur	1
2.2 Databasinformation.....	3
2.2.1 Has_message.....	3
2.2.2 Ptt_message	3
2.2.3 image_message & video_message	4
2.2.4 text_message.....	4
2.2.5 Product.....	5
2.2.6 MDM_Data.....	5
2.2.7 Roster.....	6
3 ATT NOTERA KRING INFORMATION FRÅN MLAT	6
3.1 Textformat	6
3.1.1 Vidarebefordrade meddelanden	7
3.1.2 Svar på meddelanden	7
3.1.3 Valvbilagor	8
3.2 Tidsförskjutning.....	9
3.2.1 Tidzonsdifferens	9
3.2.2 Övrig tidsförskjutning	10
3.3 Shmid är gemensamt för meddelanden och dess attachments	10
3.4 Platsinformation	10
3.4.1 Tillförlitlighet MCC.....	10
3.4.2 Misslyckad GPS Positionering.....	10
3.5 MDM och Roster – Statisk information.....	11

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 det material som mottagits i MLAT.

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*.

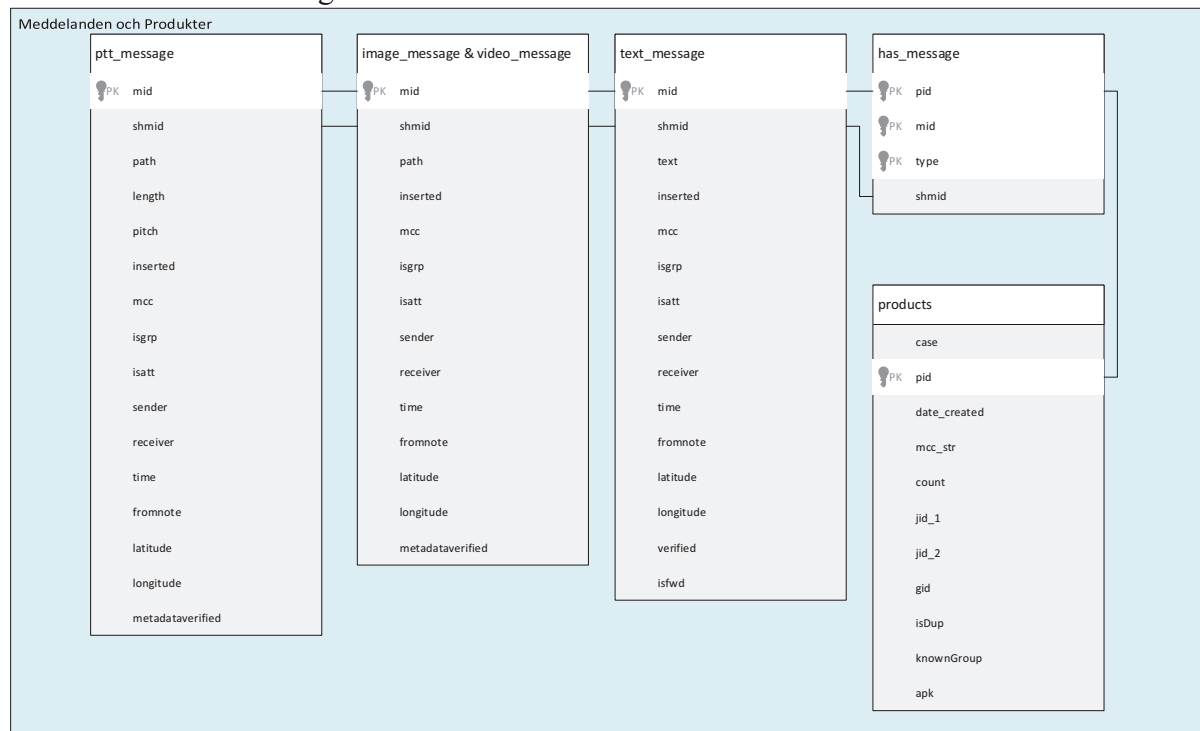
2 Innehåll i MLAT exporter

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.

Innehåller följande fält:

- pid – Produkt-ID för aktuell mid
- mid – Meddelande-ID
- type – Typ av meddelande, 1 är text, 2 är bild, 3 är ptt/ljud 4 är 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.

Innehåller följande fält:

- 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
- Receiver – Mottagande JID och/eller grupp (gid)
- Time – Tid då meddelandet skickades
- Latitude – Latitude för den enhet som skickat meddelandet
- Longitude – Longitude 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.

Innehåller följande fält:

- 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
- Receiver – Mottagande JID och/eller grupp (gid)
- Time – Tid då meddelandet skickades
- Fromnote – Anger om meddelandet är skickat från enhetens ”Valv”.
- Latitude – Latitude för den enhet som skickat meddelandet
- Longitude – Longitude för den enhet som skickat meddelandet
- Metadataverified - Tomt fält

2.2.4 text_message

Tabellen innehåller samtliga meddelanden innehållandes enbart text.

Innehåller följande fält:

- Mid – Meddelande-ID, återfinns även i has_message.
- Shmid – Meddelande-UUID, återfinns även i has_message
- text – text-innehåll i meddelande. Detta text-innehåll kan anta olika format beroende på typ av innehåll. Dessa format beskrivs under 3.1 textformat
- Inserted – Tid och datum då meddelandet lästes in Ingestion-1, *OTS kap. 8.1 Ärenden/syndikat*
- 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
- Receiver – Mottagande JID och/eller grupp (gid)
- Time – Tid då meddelandet skickades
- Latitude – Latitude för den enhet som skickat meddelandet
- Longitude – Longitude 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.

Innehåller följande fält:

- 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 – Antal 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**

Innehåller information om Anom-enheter hämtat från plattformens Mobile Device Management-verktyg.

Innehåller följande fält:

- Jid – Aktuell JID, återfinns tabellen Roster
- Imei – Senast kända International Mobile Equipment Identity för enheten
- Imsi – Senast kända International Mobile Subscriber Identity för SIM-kort i enheten
- 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 teleoperator.
- Currentphone – Senast kända telefonnummer.
- Devicelocale – Senast kända språk- och regionsinställningar på enheten
- Ipaddr – Senast kända IP-adress
- 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

2.2.7 Roster

Innehåller känd information av brukaren av en JID.

Innehåller följande fält:

Jid – Aktuell 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

3 Att notera kring information från MLAT

Vid hanteringen av exporter från MLAT har följande uppmärksammats

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.

3.2 Textformat

Meddelanden som skickas via ANOM kan antingen återfinnas som ren text, eller som något av följande format. 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's plattform.

3.2.1 Vidarebefordrade meddelanden

När en användare vidarebefordrar ett meddelande från en konversation till en annan presenteras detta som en vidarebefordran (eng. forward).

Meddelanden som vidarebefordrats från en konversation till en annan kan presenteras på två vis

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

```
forward_prefix
{
  "forward_message_time":1633354850, (Tidsstämpel i så kallad Epoch Unix Time)
  "forward_message_text":"hej", (Vidarebefordrat innehåll)
  "forward_message_user_jid":"abc123" (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, (Tidsstämpel i så kallad Epoch Unix Time)
  "forward_message_user_jid": " abc123" (Den JID som meddelandet vidarebefordrats från)
  "forward_message_body": "hej, (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": "TEXT", (Anger vilken sorts meddelande som vidarebefordrats. Fältet kan anta följande värden: TEXT|IMAGE|VIDEO|PTT|CONTACT|NOTE och avgör då om det vidarebefordrade meddelandet är text, bild, video, ljud, kontaktinformation eller en anteckning.",
  "forward_message_uuid": "123e4567-e89b-12d3-a456-426614174000" (UUID på vidarebefordrat meddelande)
}
```

3.2.2 Svar på meddelanden

När en användare svarar på ett meddelande i befintlig konversation representeras detta som ett citat (eng: 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, (Tidsstämpel i så kallad Epoch Unix Time),
  "quote_message_text":"Hur mår du?", (Det meddelande som har besvarats)
  "quoted_text":"Jag mår bra", (Det svar som getts)
  "quote_message_user_jid":"abc123" (Den JID som skickat det meddelande som har besvarats)
  , "message_uid":"123e4567-e89b-12d3-a456-426614174000" (UUID på det meddelande som besvarats)
}
```

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, (Tidsstämpel i så kallad Epoch Unix Time),
  ...
  "isQuotedMessageDeleted":true, (Anger om det besvarade meddelandet raderats. Kan anta värde true (sant) eller false (falskt).
  "isEdited":false , (Anger om det besvarade meddelandet redigerats. Kan anta värde true (sant) eller false (falskt).
}
```

3.2.3 Valvbilagor

När en användare skickar med en bilaga från det så kallade valvet presenteras detta som en valvbilaga (eng Vault attachment). Dessa bilagor kan vara anteckningar och bilder, *OTS A.7.1.3 Valvet*.

Valvbilagor kan presenteras på två sätt

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

```
{
  "mIsSelected":true, (Detta fält kan anta värdet true och false. Innebörden är i dagsläget okänd)
  "passwordChecked":false, , (Detta fält kan anta värdet true och false. Innebörden är i dagsläget okänd)
  "archived": true, , (Detta fält kan anta värdet true och false. Innebörden är 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":false, (Anger om innehållet är en checklista)
  "content":"", (Detta fält innehåller i förekommande fall text-innehåll)
  "creation":, (Detta fält innehåller den tid bilagan skapades, i UNIX Time)
  "lastModification":, (Detta fält innehåller den tid bilagan senast ändrades, i UNIX Time)
  "locked":false, (Detta fält kan anta värdet true och false. Innebörden är i dagsläget okänd)
  "reminderFired": false, (Detta fält kan anta värdet true och false. Innebörden är i dagsläget okänd)
  "title":"", (bilagans titel)
  "trashed": false (Detta fält kan anta värdet true och false. Innebörden är i dagsläget okänd)
}
```

Meddelanden inlästa från och med 2020-12-23 presenteras som ett liknande objekt:

```
{
  "mIsFromVault": true, (Detta fält kan anta värdet true och false. Innebörden är i dagsläget okänd)
  ...
  (Övriga fält som ovan)
}
```

3.3 Tidsförskjutning

3.3.1 Tidzonsdifferens

I MLAT exporter är samtliga inlästa tidsstämplar i UTC.

På grund av en misskonfiguration i en av de servrar som extraherat Anom-data har tidzonen för vissa meddelanden felaktigt tolkats som UTC. FBI har identifierat olika tidsfönster som gäller för meddelanden *OTS kap. 8.6.1 Fel i meddelandens tidzon*. Meddelanden som är inlästa i respektive fönster är angivna som UTC men är 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

3.3.2 Övrig tidsförskjutning

Det har i materialet uppmärksammats en förskjutning i tid som yttrar sig på så sätt att meddelanden verkar ha skickats ca 5-10 minuter innan meddelandets tidsstämpel. Detta är baserat på kontroll av bilder där en tidsstämpel kunnat uppfattas, t.ex. bilder på klockor eller mobiltelefoner med synlig klocka. 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.

3.4 Shmid är gemensamt för meddelanden och dess attachments

Enligt filen ”*data_information.txt*” (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 ett 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 inte alltid är helt tillförlitlig. Framför allt gäller detta vid gränstrakter och när en användare nyligen färdats från ett land till ett annat.

3.5.2 GPS Positionering

Efter en uppdatering i april 2020 försökte Anom-applikationen få fram enhetens position i samband med meddelanden som skickades. Detta kan ibland misslyckas. (*OTS A.8.2.d*) När detta misslyckas resulterar detta 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 de tillfället troligen en tidsstämpel i UNIX Time (Tid i sekunder sedan 1/1 1970 UTC)

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.

Under operation Trojan shield försågs Polismyndigheten med datapaket varje måndag, onsdag och fredag. Dessa datapaket innehöll samtliga produkter genererade sedan den senaste exporten. I dessa produkter var meddelanden försedda med det Alias aktuell JID hade vid export-tillfället.

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]

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

Diariennr. 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.

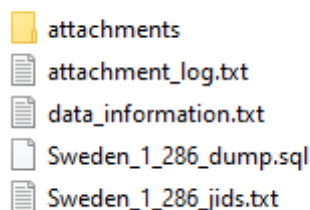
2.2 Innehåll fysiskt media

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 tillägsexporter 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.

Namn



```

attachments
attachment_log.txt
data_information.txt
Sweden_1_286_dump.sql
Sweden_1_286_jids.txt
  
```

Figur 1. Exempel på filstruktur innehåll, syndikat 286

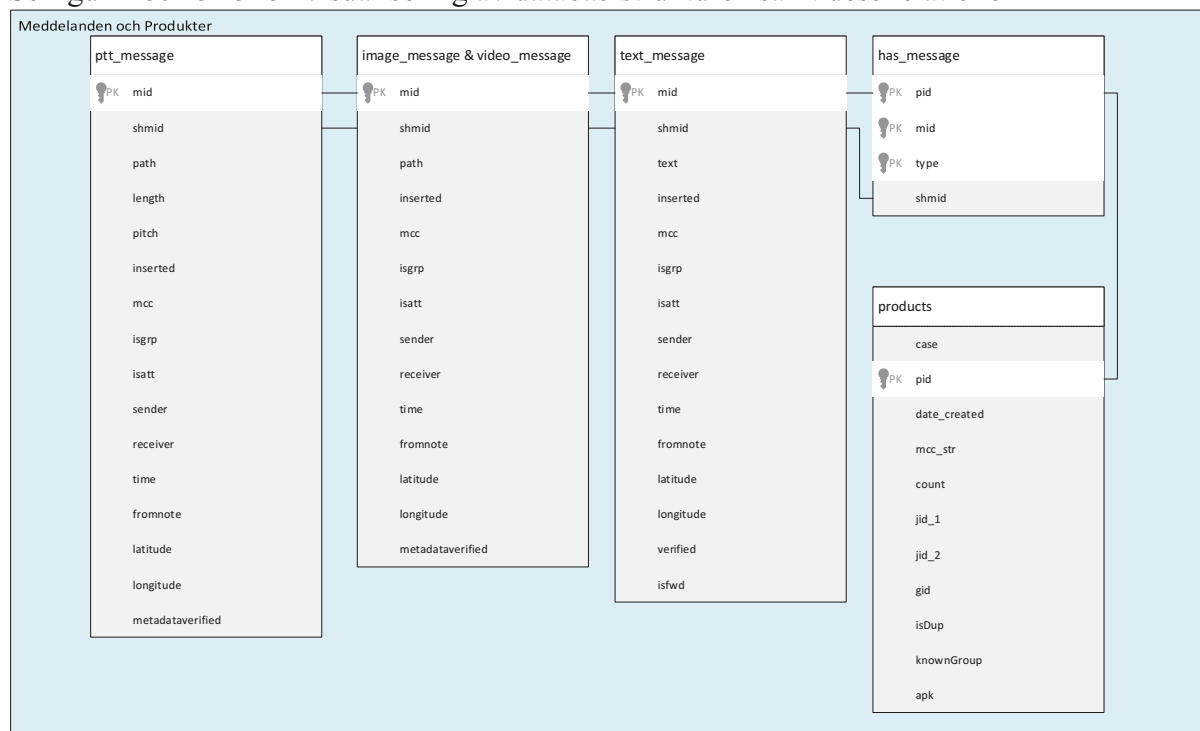
2.2.1 Maskininstruktioner

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

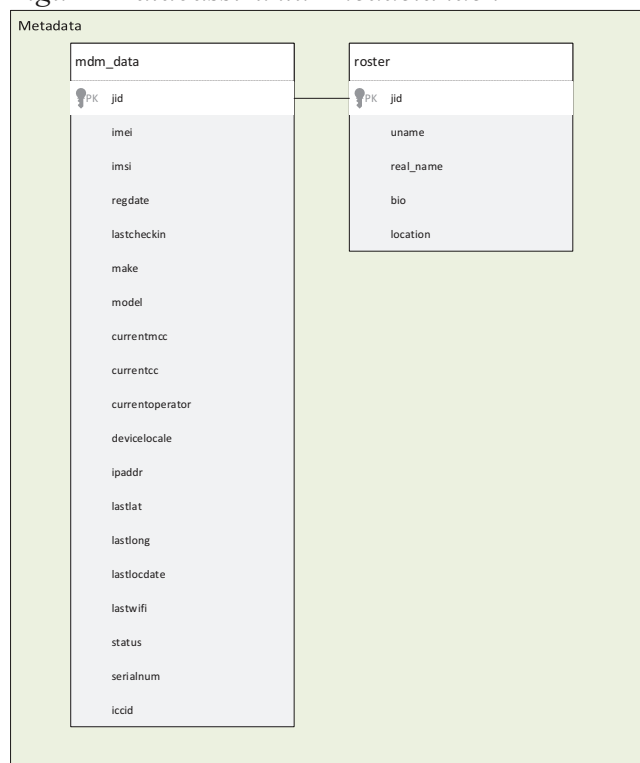
- Has_message
- Image_message
- Mdm_data
- Products
- Ptt_message
- Roster
- Text_message
- Video_message

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 dedupliceras 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 förse med det Alias JID:en använt för detta meddelande.

4.7 Dekodning och presentation av källmaterial

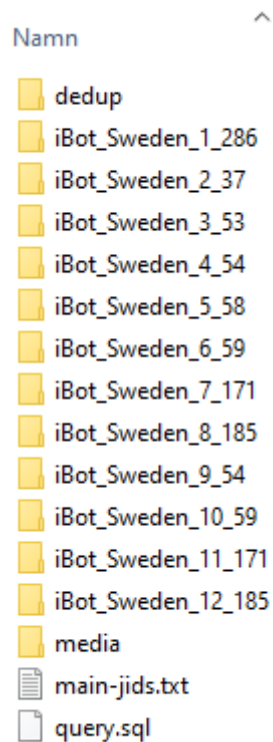
Samtliga TSV-filer med rådata från databasexport och all hänvisat media har levererats till förundersökning för vidare analys.

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.



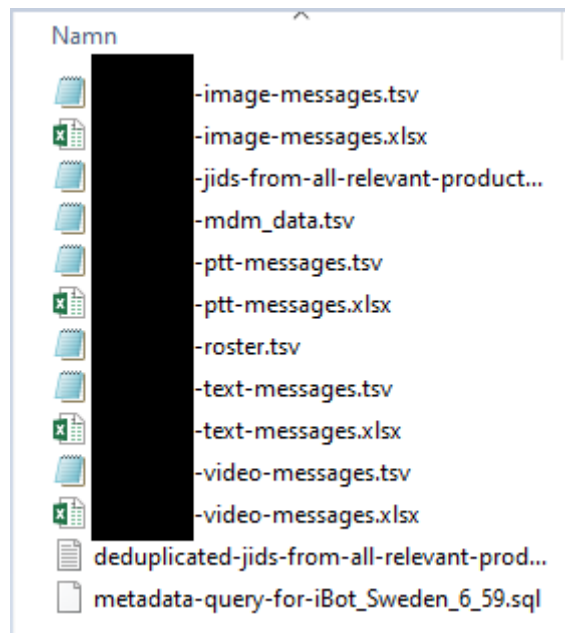
Figur 4 Katalogstruktur exporter

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

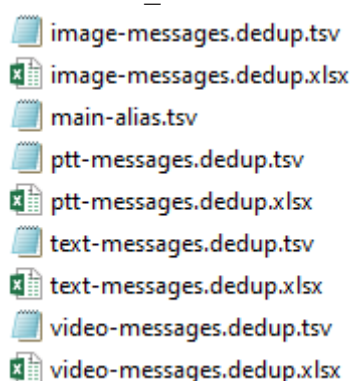


Fig 6, Innehåll dedup

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,
```

```

`metadaverified` 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,

`device locale` 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,

`metadaverified` 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, //attributed 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_METADATA_AVERIFIED
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_METADATA_AVERIFIED
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_METADATA_AVERIFIED
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

Polismyndigheten
Nationellt Forensiskt Centrum
Linköping

PM

1 (3)

Datum
2021-11-19

Informationsklass
Öppen information

Diariernr (åberopas)
A673.978/2021

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

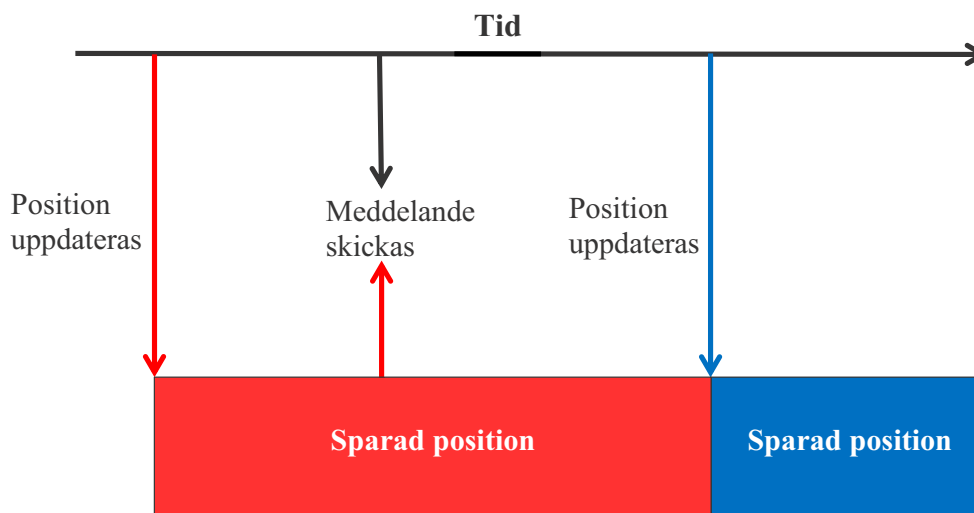
Android Location Manager ger en applikation access till systemets platstjänster. Enligt [1] använder ANØM-applikationen denna funktion sedan april 2020. Efter analys av applikationen¹ kan det konstaterats att för att få positionsdata används metoden `requestLocationUpdates` i Android Location Manager. 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\(java.lang.String,%20android.location.LocationRequest,%20java.util.concurrent.Executor,%20android.location.LocationListener\)](https://developer.android.com/reference/android/location/LocationManager#requestLocationUpdates(java.lang.String,%20android.location.LocationRequest,%20java.util.concurrent.Executor,%20android.location.LocationListener))

OFFENTLIGT // FOUO



Teknisk information om Operation Trojan Shield

Senast uppdaterad: 31 augusti 2021

INNEHÅLLSFÖRTECKNING

1. ÖVERSIKT ÖVER SERVVAR 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

OFFENTLIGT // FOUO

OFFENTLIGT // FOUO

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

OFFENTLIGT // FOUO

OFFENTLIGT // FOUO

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

OFFENTLIGT // FOUO

<i>A.5 Nätverksanslutning till plattformen</i>	<i>45</i>
<i>A.6 MDM-komponenten.....</i>	<i>45</i>
<i>A.7 ANØM-applikationen</i>	<i>46</i>
<i>A.8 Data spelas in från plattformen</i>	<i>49</i>
<i>A.8.2 Metadata för meddelanden</i>	<i>50</i>
<i>A.9 Autentisering och integritet</i>	<i>51</i>

OFFENTLIGT // FOUO

OFFENTLIGT//FOUO

1. ÖVERSIKT ÖVER SERVVAR OCH NÄTVERK

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

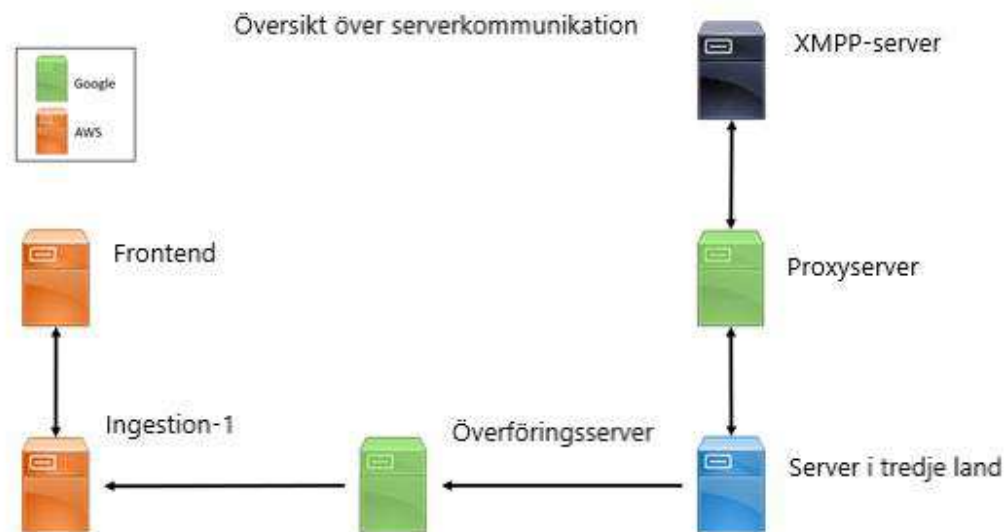


Diagram 1.A

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.

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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.

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

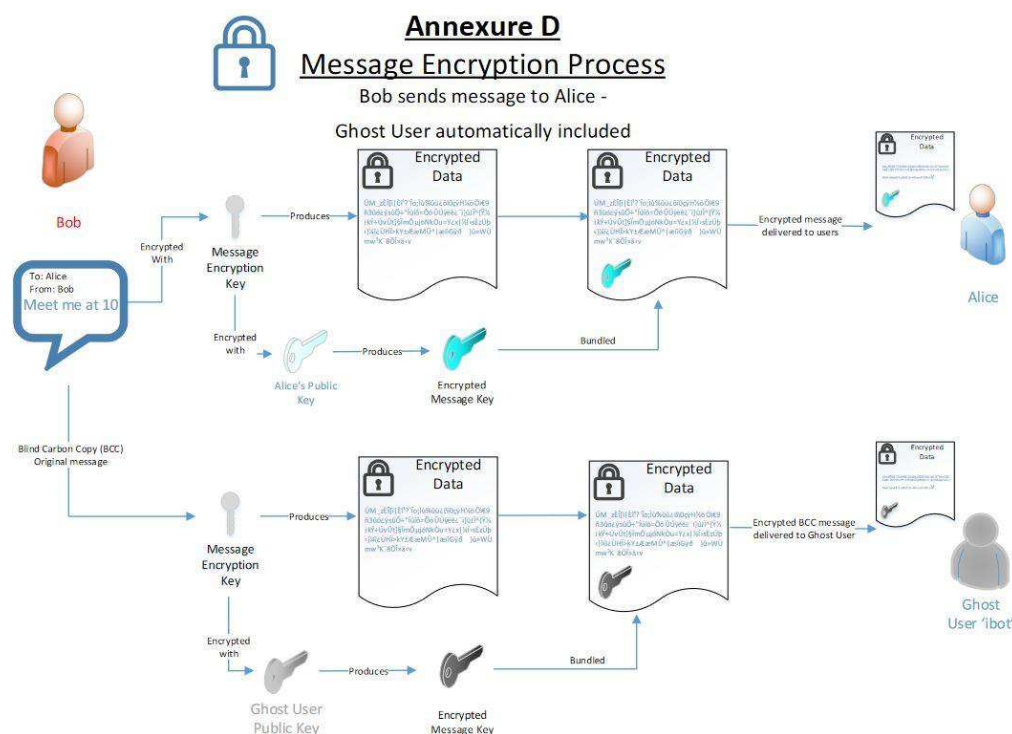


Diagram 1.B

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

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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 [unik meddelande-ID].[bilagens filnamnstillägg]
- Innehåll
 - Om meddelandetyper var "text", "kontakt" eller "vidarebefordrat" var innehållet krypterat
 - Om meddelandetyper 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].[bilagens 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

OFFENTLIGT//FOUO

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 paketet.

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 filnamnsillägget ".pgp" 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.

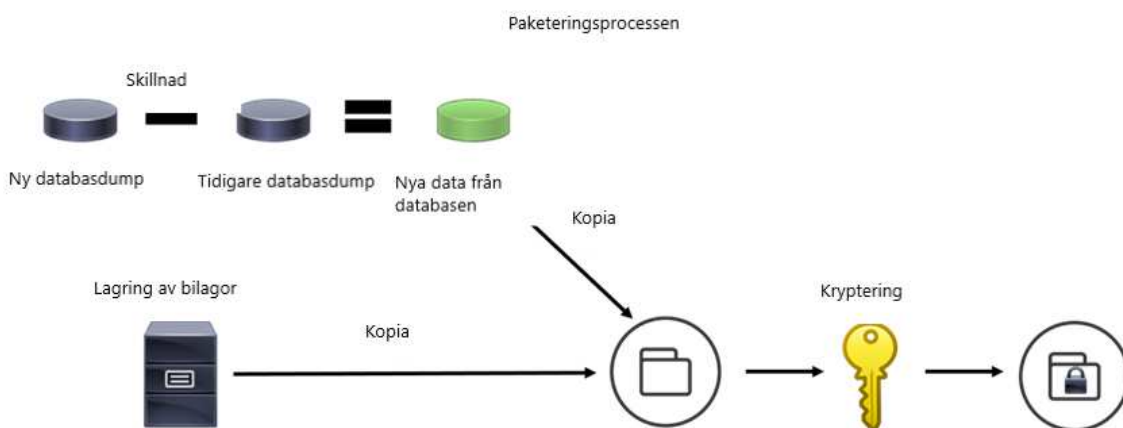


Diagram 2.A

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.

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

4. ÖVERFÖRING FRÅN ÖVERFÖRINGSSERVERN TILL AWS GOV CLOUD

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 ".pgp" 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 .pgp-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

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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.

OFFENTLIGT//FOUO

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

OFFENTLIGT//FOUO

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.

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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 gruppprodukt.
- Grupp-ID (GID)
 - Gruppens unika identifierare om produkten är en gruppprodukt
- 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

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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 meddelandeinnehåll 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 datapaketet.
 - 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.

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

- 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).

OFFENTLIGT//FOUO

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:

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

- 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

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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 senaste 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.

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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.

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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 meddelandetyper ("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 går 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 genomgått 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

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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. tvåfaktoraautentisering (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.



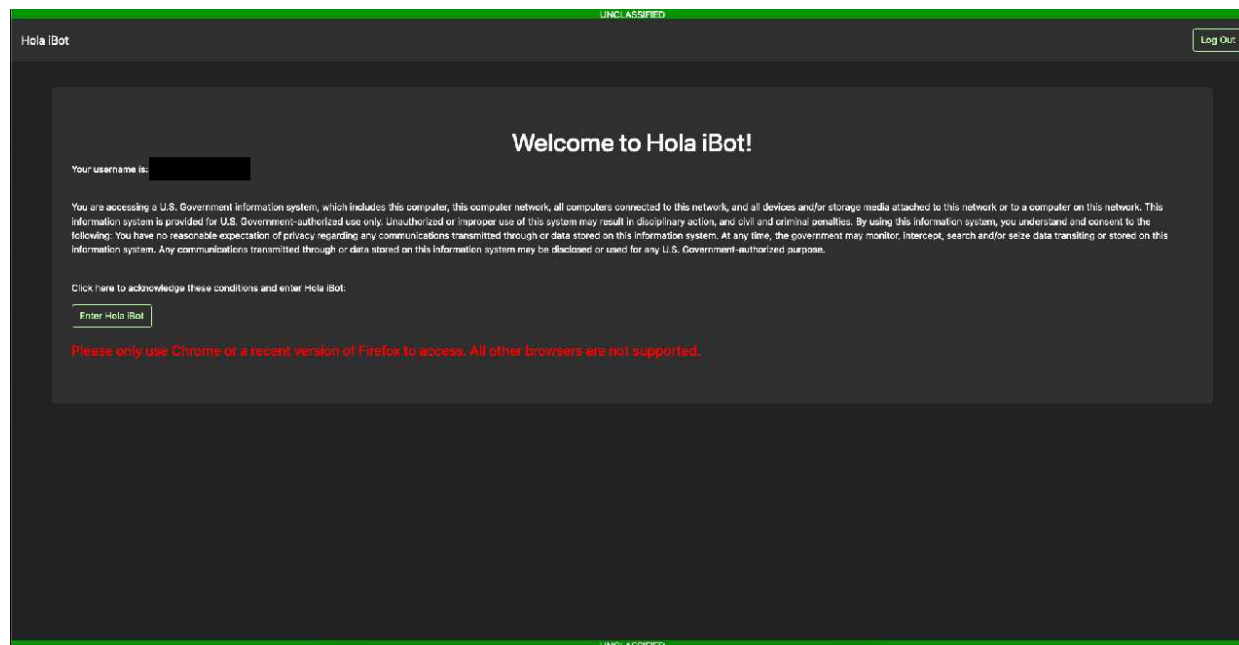
Skärmbild 10.A

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.

OFFENTLIGT//FOUO

OFFENTLIGT // FOUO

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.

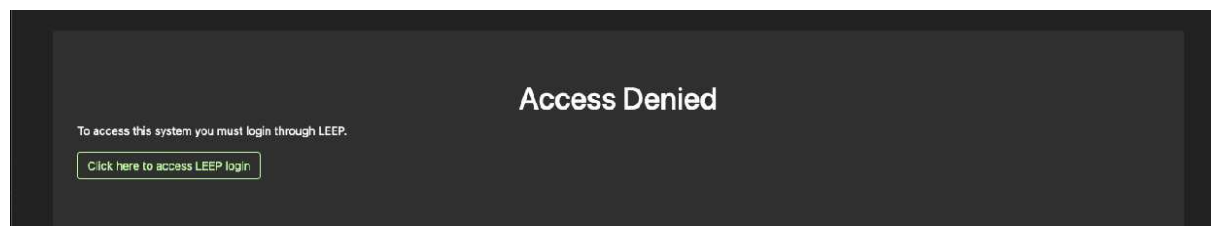


Skärmbild 10.B

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.



OFFENTLIGT // FOUO

OFFENTLIGT//FOUO

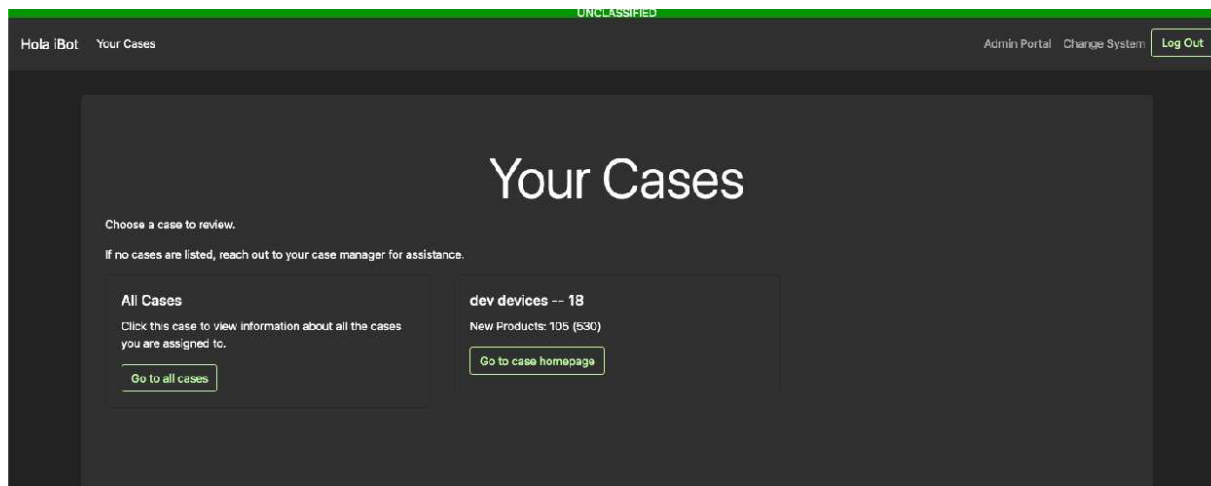
Skärmbild 10.C

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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.

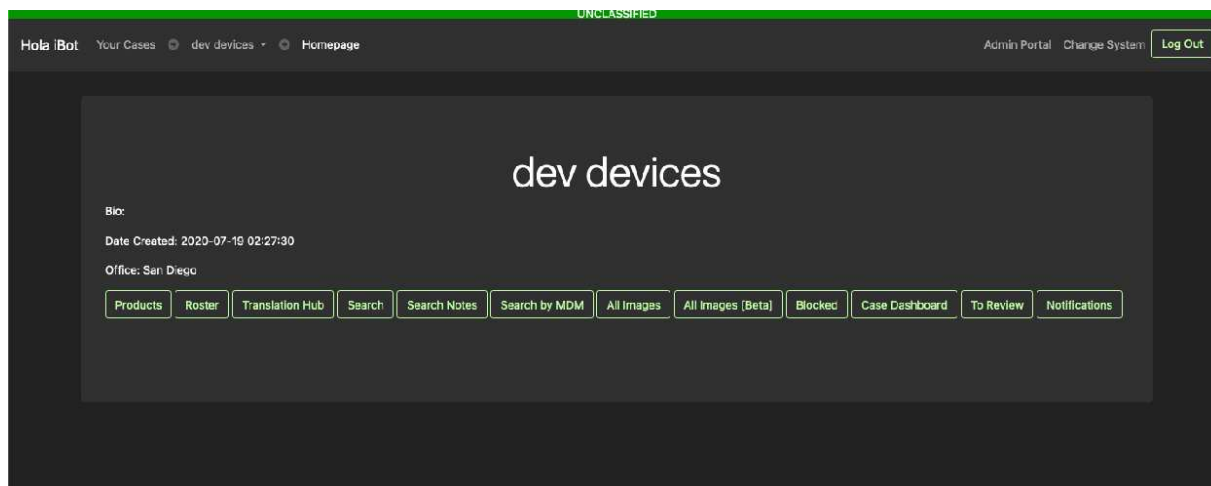
Användarna har också alternativet "alla ärenden". Om det alternativet väljs blir de återstående sidorna ifyllda med alla data som användaren av granskningsplattformen har åtkomst till.

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.

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO



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”.

Product ID	Date Created	Members of Product	Number of Messages	MCCs	Product Markings	All Mags Marked
18_788920	2021-06-08 00:35:05	musicsearch, echo	1	232 - AT	Pertinent	✓
18_788919	2021-06-08 00:35:05	threadbrief, support	1	222 - IT	Pertinent	✓
18_788918	2021-06-08 00:35:05	shellshall, echo	1	505 - AU	Pertinent	✓
18_788917	2021-06-08 00:35:05	strongfiles, echo	1	214 - ES	Pertinent	✓
18_788916	2021-06-08 00:35:05	4bafic, afgoo, moviebeat	1	520 - TH	No Intelligence Value / Not Pertinent	✓
18_788915	2021-06-08 00:35:05	roomlarge, support	1	220 - RS	No Intelligence Value / Not Pertinent	✓
18_788914	2021-06-08 00:35:05	cleanlater, echo	1	334 - MX	No Intelligence Value / Not Pertinent	✓
18_788913	2021-06-08 00:35:05	sangbecome, echo	1	252 - DE	No Intelligence Value / Not Pertinent	✓
18_788912	2021-06-08 00:35:05	066621, 35c4d1, 447ed2, 4bafic, 51f3ae, 521c14, 587f31, 59e609, 5c28e0, 5ee9f2, 62a1ab, 6c2eee, 80b850, 81ff36, 8ad116, 92c3ca, 99072a, b12027, b12485, b241e6, batate, childhair, columnmotive, d03933, d61737, de0606, deescourt, f7ca27, f85c50, falcil, folkson, freenlight, hairblow, ironbelong, ladyfuel, mapour, overcock, piandern,	2	218 - BA, 220 - RS	Pertinent	✓

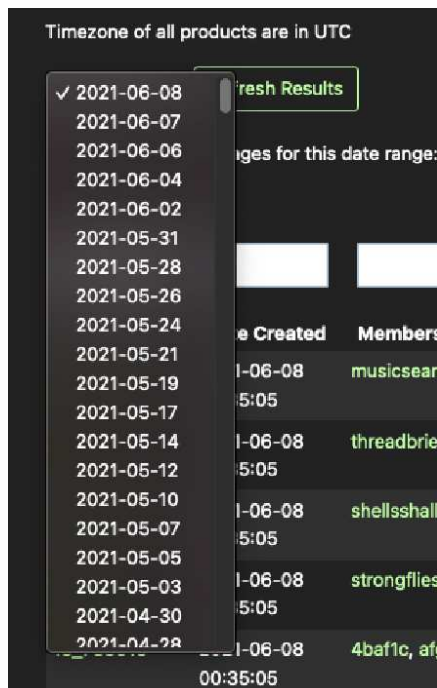
Skärmbild 10.F

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

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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

Information for product 18_254380

Conversation trail on 2021-03-05 00:11:10: 18_250269 (display all previous conversations)

Members of conversation:

JID	Username	Alias/Real Name	Case(s)/Syndicate(s)
anomt1	anomt1		18 - dev devices
tanvir	zhvzvuv		18 - dev devices

Language(s) of Conversation:

Nothing selected

Markings

- ☐ Case Manager Review
- ☐ Duplicate - Pending Translation
- ☒ No Intelligence Value / Not Pertinent
- ☐ Not Reviewed
- ☐ Pertinent
- ☐ Pertinent - Marijuana
- ☐ Review In Progress
- ☐ Translation Completed
- ☐ Translation In Progress
- ☐ Translation Needed

47 Messages in Product:

PERT	NPRT	PRIV	#	Time	MCC	JID	Sender Name	Content	Latitude	Longitude	Location	Verified
●	●	●	1	2021-03-05 04:22:10	0	anomt1	anomt1	ghh	23.795582	90.375828	Azimpur, Bangladesh	●
●	●	●	2	2021-03-05 04:23:08	0	anomt1	anomt1	ohh	23.795582	90.375828	Azimpur, Bangladesh	●
●	●	●	3	2021-03-05 0	0	anomt1	anomt1	noo	23.795582	90.375828	Azimpur	●

Skärmbild 10.G

Information for product 21_599116

This product is a duplicate of one or more other products in other cases:
pid 602208 -- case ID - 39, Case name - Plutus
Conversation trail on 2021-05-12 00:19:50: 21_584552 (display all previous conversations)

Members of conversation:

JID	Username	Alias/Real Name	Case(s)/Syndicate(s)
olssend	Walter White		39 - Plutus
screenfourth	AnamAlbania		21 - Distributors

Language(s) of Conversation:

Nothing selected

Markings

- ☐ Case Manager Review
- ☐ Duplicate - Pending Translation
- ☒ No Intelligence Value / Not Pertinent
- ☐ Not Reviewed
- ☐ Pertinent
- ☐ Pertinent - Marijuana
- ☐ Review In Progress
- ☐ Translation Completed
- ☐ Translation In Progress
- ☐ Translation Needed

4 Messages in Product:

PERT	NPRT	PRIV	#	Time	MCC	JID	Sender Name	Content	Latitude	Longitude	Location	Verified
●	●	●	1	2021-05-12 09:19:21	- GB	olssend	Walter White	Ca sht	None	None		●
●	●	●	2	2021-05-12 09:49:07	- AL	screenfourth	AnamAlbania	Ta kam nis gabim	None	None		●

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.

OFFENTLIGT//FOUO

- 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.

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

Skärmbild 10.G.2

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

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

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

● PRIV									
● PERT ● NPERT ● PRIV	2	2021-03-15 07:12:55	286 - TR	mostlyinto	OG 🗨️	Haben wir eine Halle wo wir heute abladen könnten	39.0	1.615792363E12	
● PERT ● NPERT ● PRIV	3	2021-03-15 07:15:12	286 - TR	mostlyinto	OG 🗨️	▶ ● 0:00 / 0:00 🔊 ▬ Update	39.0	1.615792363E12	
● PERT ● NPERT ● PRIV	4	2021-03-15 07:16:12	286 - TR	mostlyinto	OG 🗨️	▶ ● 0:00 / 0:00 🔊 ▬ Update	39.0	1.615792363E12	
● PERT ● NPERT ● PRIV	5	2021-03-15 07:16:24	286 - TR	mostlyinto	OG 🗨️	▶ ● 0:00 / 0:00 🔊 ▬ Update	39.0	1.615792363E12	
● PERT ● NPERT ● PRIV	6	2021-03-15 07:16:24	286 - TR	mostlyinto	OG 🗨️	Hast du neue wäke	39.0	1.615792363E12	

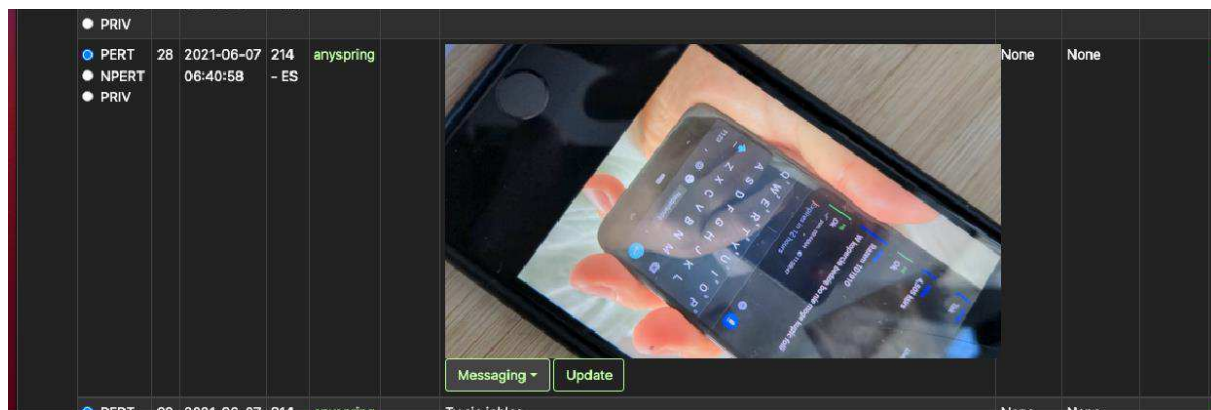
29

OFFENTLIGT//FOUO

Skärmbild 10.G.3

10.4.2.2 Bildmeddelanden i Hola iBot

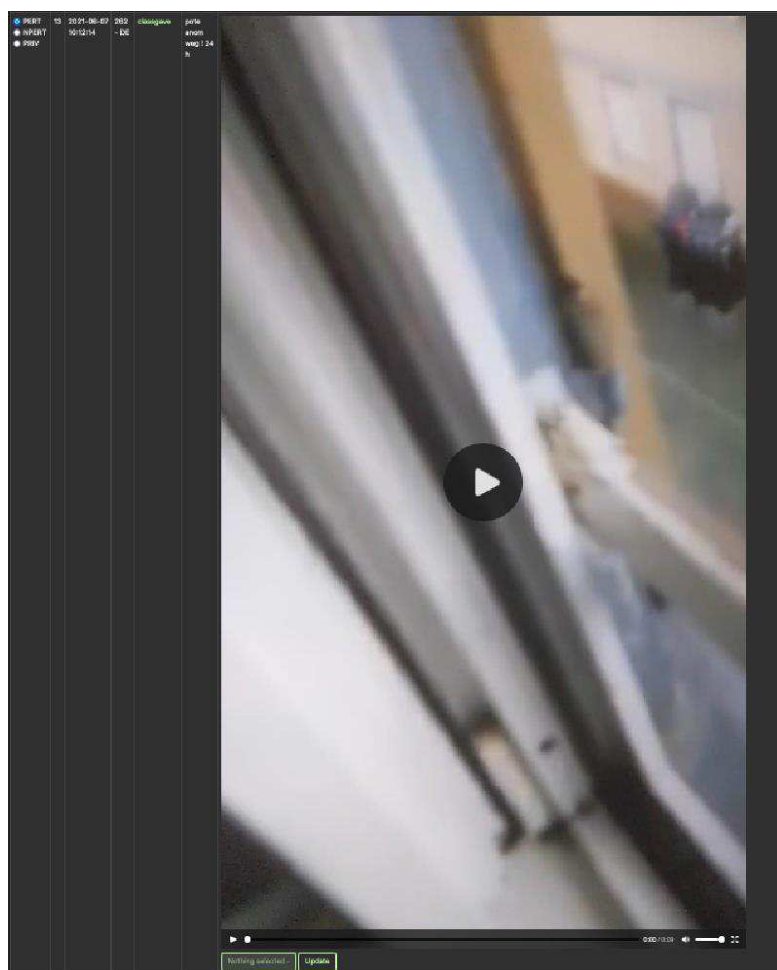
I skärmbild 10.G.4 visas ett exempel på ett bildmeddelande som visas inline.



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.



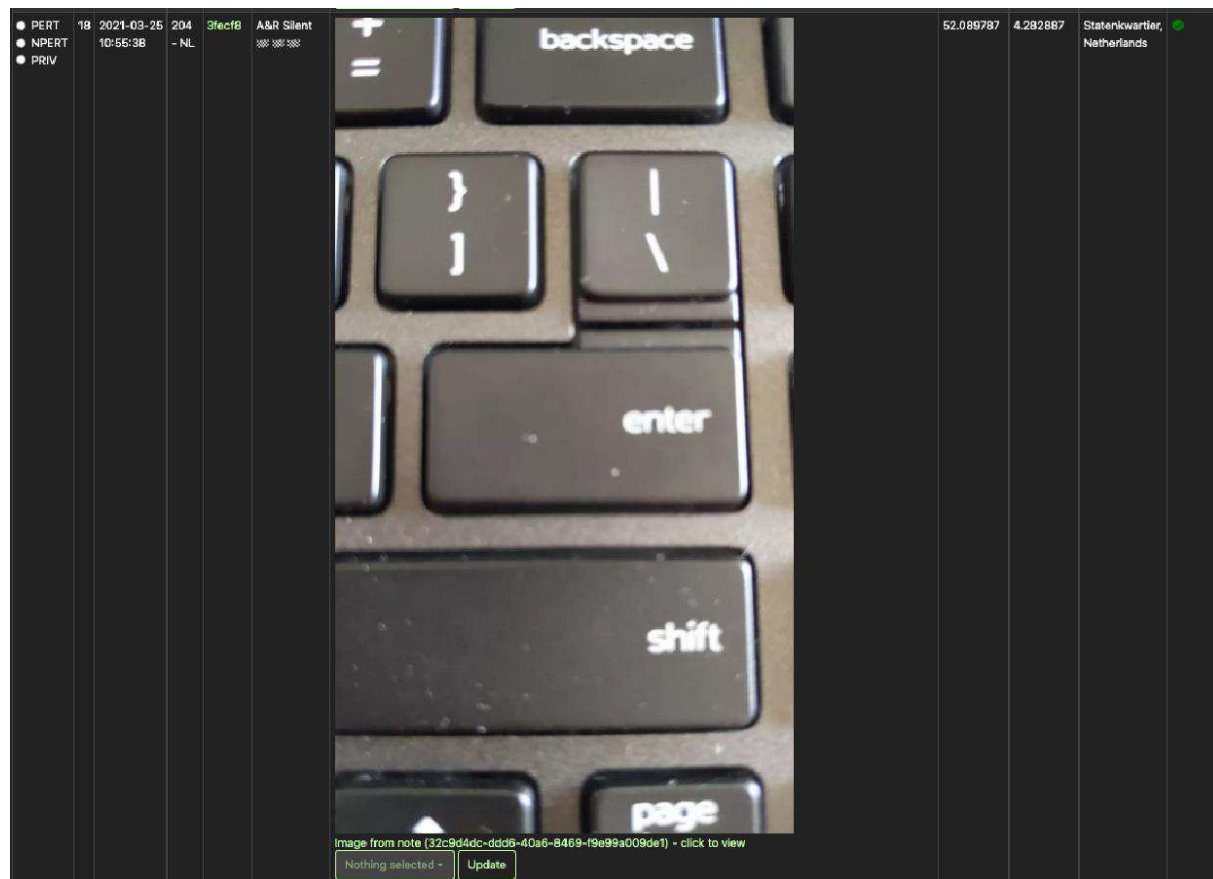
Skärmbild 10.G.5

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

- 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.

UNCLASSIFIED

Hola iBot Your Cases All Cases Translation Hub Admin Portal Change System Log Out

Translation Hub

Timezone of all products are in UTC

49 items selected Refresh Results Language Stats

New Items					In Progress				
Product ID	Language	Date Submitted	Status	Priority	Product ID	Language	Date Submitted	Status	Priority
58_10792	Swedish	2020-09-21 16:38:28	New	2	50_78149	Bernese German	2020-09-24 20:36:30	In Progress	2
58_103163	Swedish	2020-09-23 16:52:34	New	2	50_100095	Bernese German	2020-10-05 15:31:55	In Progress	2
37_103132	Swedish	2020-09-23 18:14:45	New	2	53_258378	Croatian	2021-03-10 20:13:03	In Progress	2
58_106757	Swedish	2020-10-02 17:28:12	New	2	99_281555	German	2021-03-18 04:32:52	In Progress	2
63_116509	Swedish	2020-10-16 14:57:39	New	2	115_334402	German	2021-03-31 18:44:21	In Progress	2
59_121820	Swedish	2020-10-26 14:10:32	New	2	59_342031	Croatian	2021-04-02 10:24:20	In Progress	2
37_121320	Swedish	2020-10-26 14:57:23	New	2	105_358753	German	2021-04-06 23:55:44	In Progress	2
54_125935	Swedish	2020-11-02 17:12:26	New	2	50_394149	Croatian	2021-04-12 08:35:10	In Progress	2
53_126006	Swedish	2020-11-06 17:13:25	New	2	220_438561	Croatian	2021-04-19 20:04:21	In Progress	2
53_139512	Swedish	2020-11-25 16:27:58	New	2	59_439824	Croatian	2021-04-21 12:34:00	In Progress	2
54_164726	Swedish	2020-12-31 17:30:57	New	2	59_311814	Serbian	2021-04-21 17:58:26	In Progress	2
191_360635	Serbian	2021-04-05 23:06:34	New	2	86_542913	Albanian	2021-05-06 18:24:32	In Progress	2
11_367693	Chinese	2021-04-07 10:55:47	New	2	59_567283	Croatian	2021-05-10 10:19:27	In Progress	2
191_371448	Serbian	2021-04-07 18:45:05	New	2	59_567287	Croatian	2021-05-10 11:28:32	In Progress	2
184_372010	Serbian	2021-04-07 18:55:21	New	2	59_567331	Croatian	2021-05-10 18:07:50	In Progress	2
196_372176	Serbian	2021-04-07 22:21:48	New	2	30_614645	Italian	2021-05-17 02:58:38	In Progress	2
59_373358	Croatian	2021-04-09 12:36:18	New	2	279_653700	Croatian	2021-05-21 19:11:40	In Progress	2
0_375352	German	2021-04-09 22:55:48	New	2	59_644437	Albanian	2021-05-21 19:35:48	In Progress	2
0_350152	Serbian	2021-04-11 10:16:28	New	2	108_856613	Croatian	2021-05-22 17:33:52	In Progress	2

UNCLASSIFIED

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.

OFFENTLIGT//FOUO

Translate product 50_78149_Bernese_German
Language: Bernese German

Members of conversation:

JID	Username	Alias/Real Name
053d90	Chest	Ekrem HAMZABEGOVIC
1e5464	Tommy	Marco HAEUBI

Language(s) in conversation: Bernese German
Priority of translation: 2

If this is not the correct language for the product, you can change it here
Select the languages that are in this product. deselect the languages that are not in this product. If a language already has a translation started for it, you may not remove the language.
Click the "Update Languages" button to update the languages for the product
After you click the update button, a message will prompt you to return to the translation hub

Bernese German
Update Language(s)

Show Machine Translation (Detected Languages: Haitian English Tagalog German Norwegian Finnish Spanish Swedish Estonian Dutch Italian French Indonesian Afrikaans Polish Latvian Hungarian Portuguese Slovenian Turkish Luxembourgish Welsh Danish Croatian Lithuanian Malay)

841 Messages in Product:

#	Time	MCC	JID	Sender Name	Content
1	09/28/20 21:07:25	000000	000000	Ghost	Tommy

Current Translation for Bernese German:

[09/28/20 21:07:25] -- [Redacted] Bernese German
Status: In Progress

[09/28/20 21:26:58] -- [Redacted] Bernese German
Status: In Progress
On line 2, Chest comments on Tommy's Spanish skills.
On line 6, Ghost asks what the other guy wrote.
On line 8, Ghost tells Tommy not to tell the guy that he isn't there.
On line 16, Ghost asks what the guy wrote and what Tommy answered him.

New Translation for Bernese German:

Status: In Progress Add Translation

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.

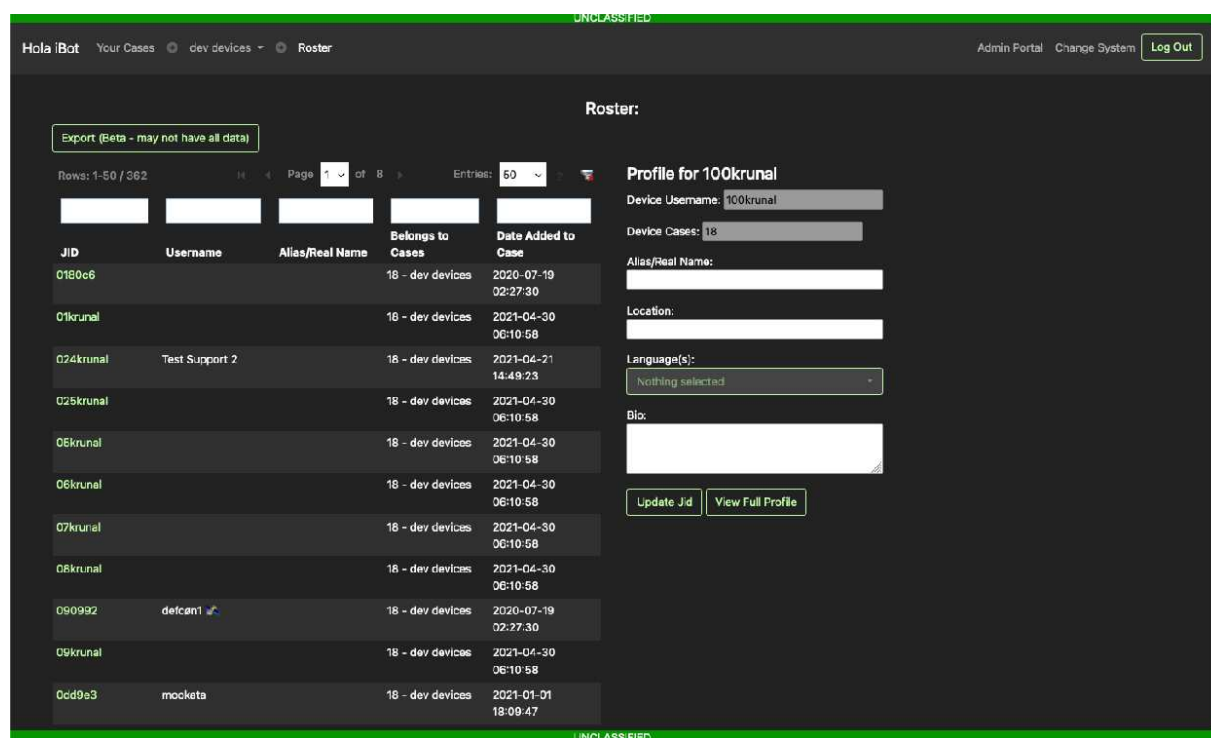
Alla anteckningar som har lagts till för motsvarande produkt via produktsidan visas längst ned på översättningssidan.

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".

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO



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.

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

UNCLASSIFIED

Hola iBot JID Profile Admin Portal Change System Log Out

00262a

Profile for 00262a:

Device Username: THANOS

Real Name: [REDACTED]

Device Cases: 84

First message Date/Time: 2020-11-18 18:05:33

JID, 00262a, added to case, 84, on 2020-12-02 01:22:16

Language(s):

- Dutch

Blot: [REDACTED]

All images sent/received by 00262a

Press the buttons below to show images sent or received by this JID. Note: if there are a lot of images, this may take some time to load

Show first 25 images Show all 41 images

Products including 00262a

Press the button below to show links to products that include this JID. Note: this will only show products that you have access to

Show all 54 products

Locations for messages sent by 00262a

Press the button below to show a map with locations of all messages sent by this JID. Message location data may not be available for all JIDs. This will take some time to load

Show map

Communications link chart for 00262a

Mobile Device Manager data for 00262a:

- IMEI: 356112100447682
- ICCID: 8934072679000411296
- IMSI: 214074205416229
- Make: Pixel3a
- Model: Pixel3a
- Current network operator: NL KPN
- Last known latitude: 53.21269056
- Last known longitude: 5.01915841
- Date of last check-in: 03/24/2021, 22:19:37 UTC
- Date of last known location: 03/23/2021, 08:58:54 UTC

All MCCs this JID has sent messages from

MCC	Message Count	Last Seen in MCC
204	1654	2021-03-22

UNCLASSIFIED

Skärmbild 10.K

Resten av avsnitt 10.7 hänvisar till skärmbild 10.K.

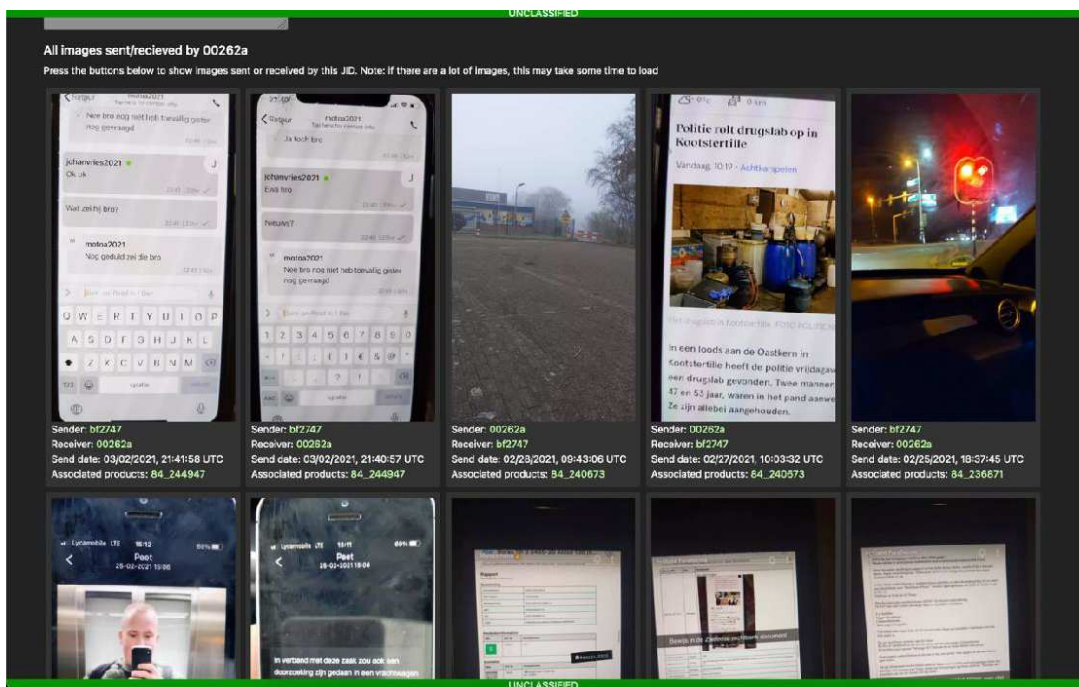
10.7.1 Information om enhetsanvändaren (JID)

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.

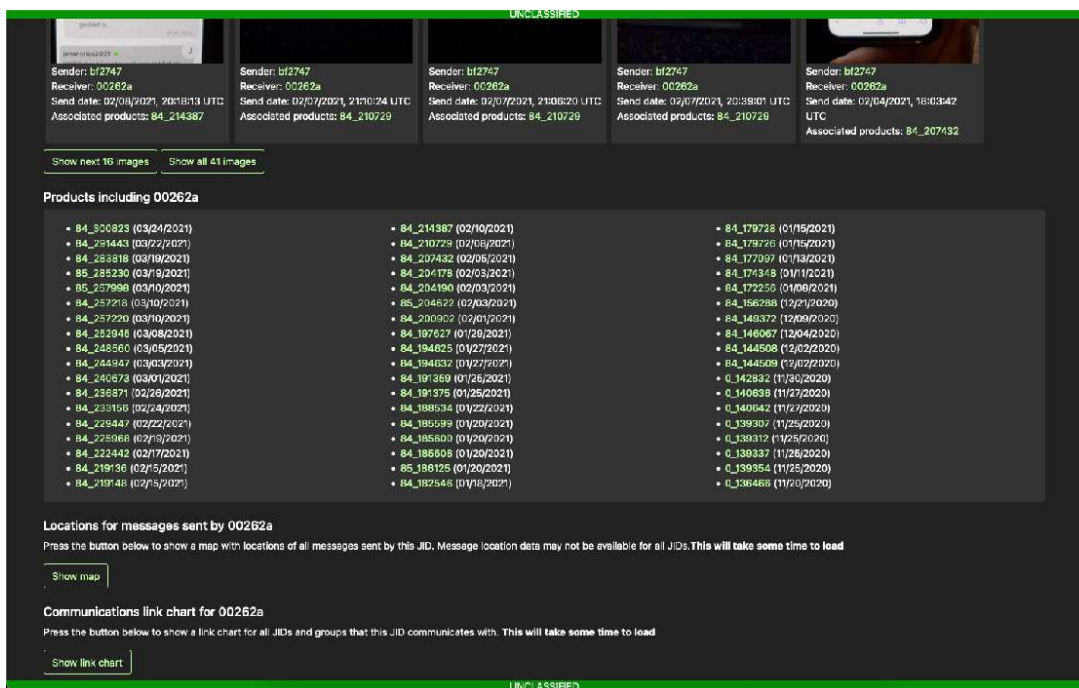
OFFENTLIGT//FOUO

OFFENTLIGT//FOUO



Skärmbild 10.K.1

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

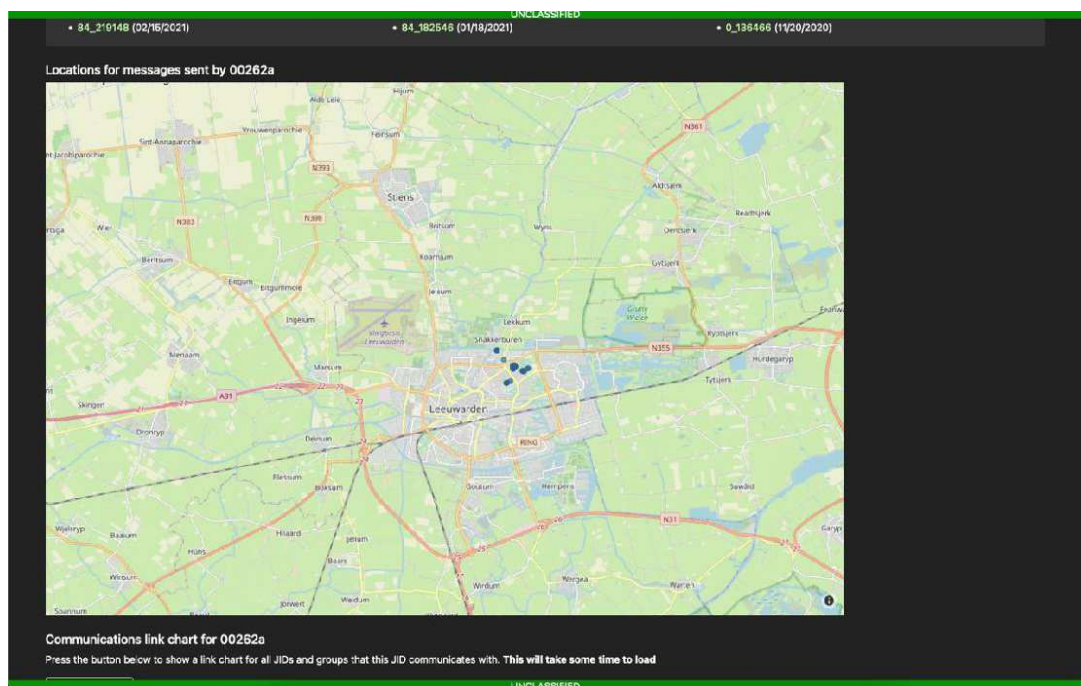


Skärmbild 10.K.2

OFFENTLIGT//FOUO

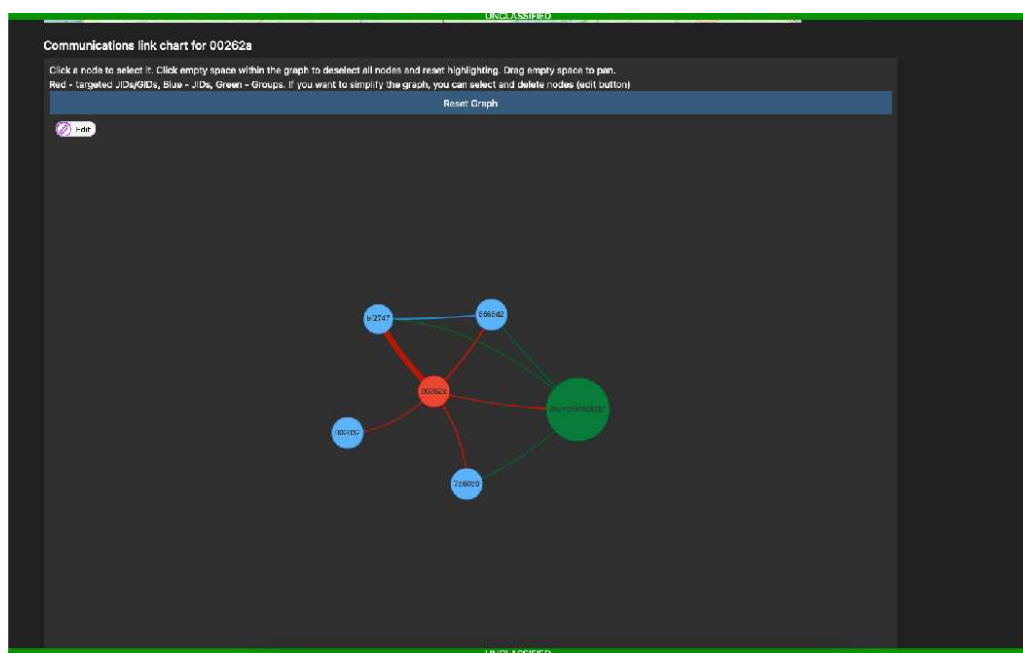
OFFENTLIGT//FOUO

- 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.

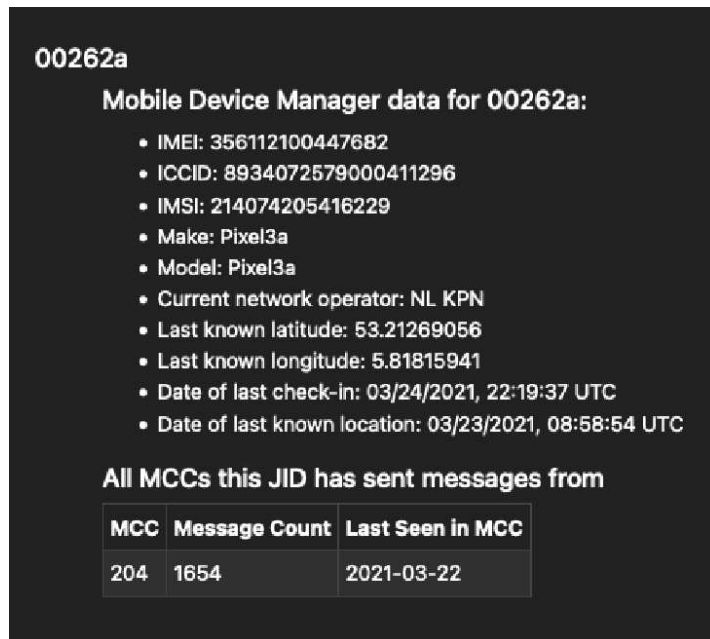


OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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 förstord 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.

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

Search

Boolean Operators Supported for search terms and JID/GID fields: OR, AND -- Boolean operators must be all caps

Wildcard characters supported: (* -- zero or more [fish* matches fish or fishing], ? -- one character [lease? matches leased])

Enter term to search:

Enter JID or GID to search (will search all messages JID/GID sent or received):

Enter date range to search (if one date is entered, the other is also required):

Number of results (1-10000): 1000

More than 5000 search results may result in slow load times.

☐ Search Translated Text

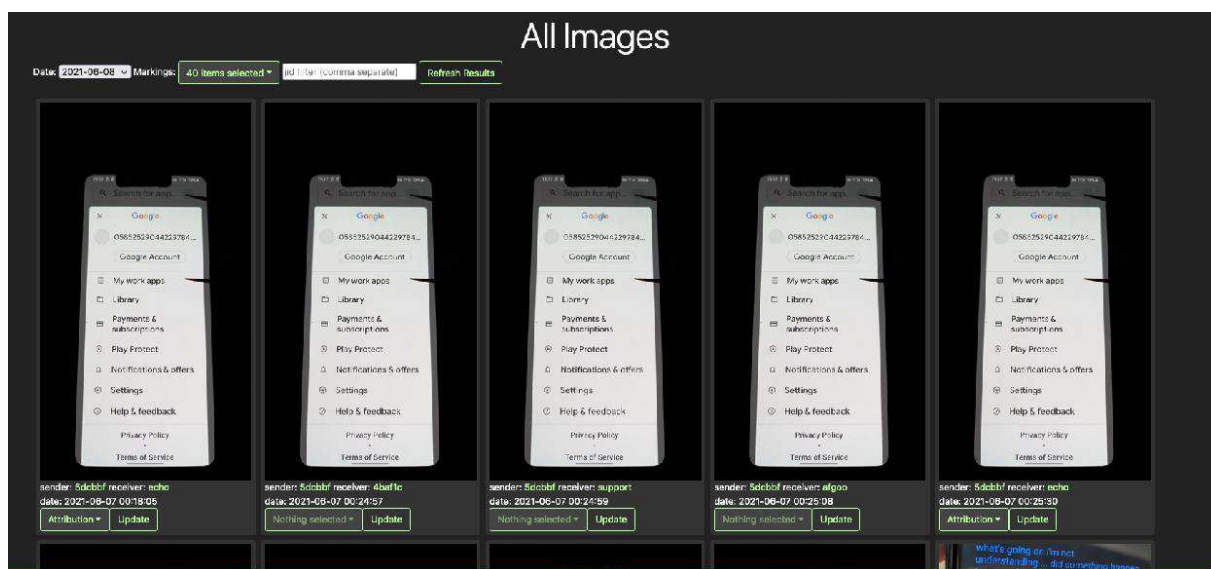
Skärmbild 10.L

10.8.2 Sök i anteckningar

När användare av granskingsplattformen 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

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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 gått igenom är MLAT-exporten klar och kan skickas till det begärande landet.

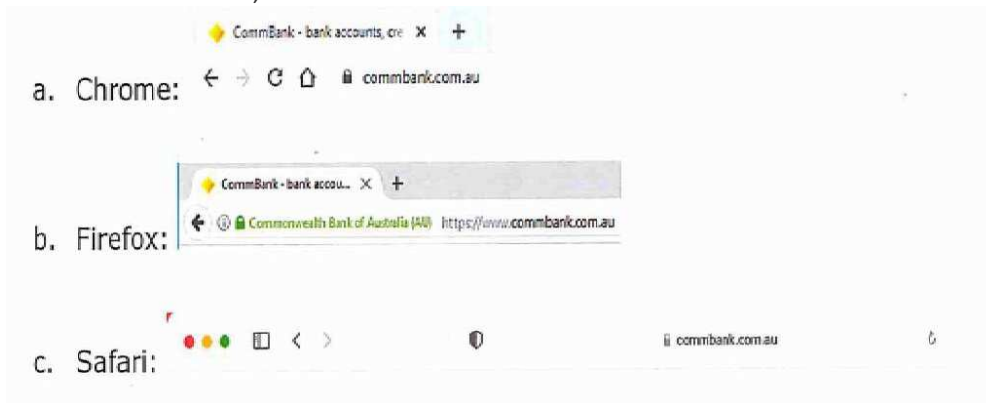
OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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 anlidade 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

OFFENTLIGT//FOUO

- 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 använde 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 fjärrrensning 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"

OFFENTLIGT//FOUO

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

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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. Slut användaren 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 lösenordspolitik 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.

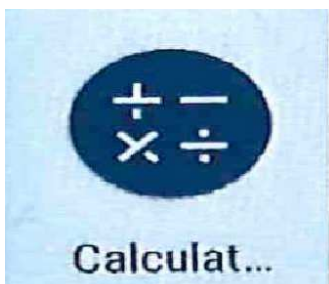
OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

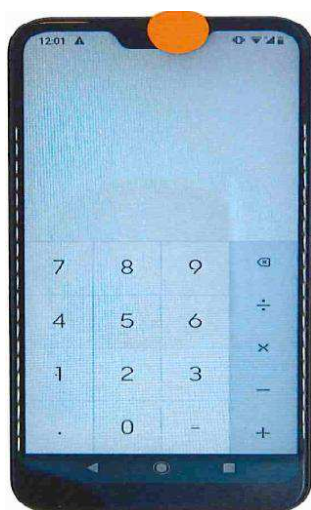
- e. Förhindra installation av ej betrodda eller ej godkända applikationer och därmed säkerställa att endast applikationer som var tillgängliga via MDM-komponenten för ANØM kunde installeras och köras på enheten.
 - f. För FieldX MDM: se till att ANØM-appen uppdaterades automatiskt.
 - g. Rapportera 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:



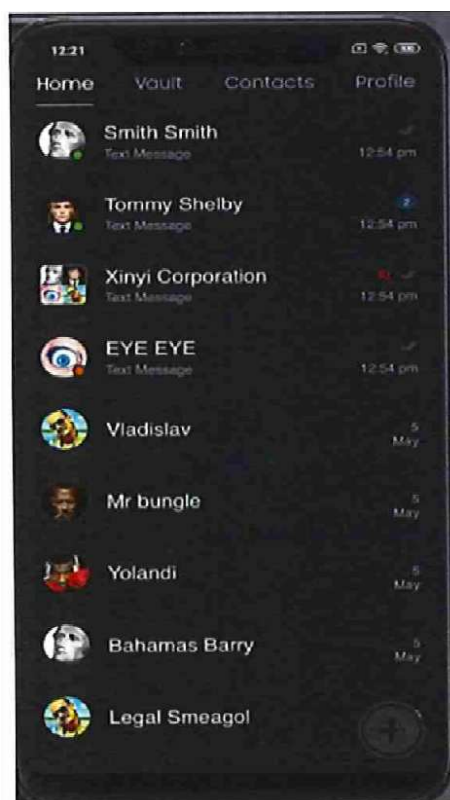
42. Kalkylatorn fungerar som förväntat, dvs. användaren kan mata in matematiska funktioner och det korrekta resultatet matas ut.

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO



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



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

OFFENTLIGT//FOUO

OFFENTLIGT // FOUO

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 emoji "😡". Sådana Unicode-värden måste konverteras tillbaka till de rätta tecknen för att de ska kunna läsas.

OFFENTLIGT // FOUO

OFFENTLIGT//FOUO

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 "självförstörelsetimer" 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

OFFENTLIGT//FOUO

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

OFFENTLIGT//FOUO

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.

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

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.

OFFENTLIGT//FOUO

OFFENTLIGT//FOUO

- **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 02 och 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

OFFENTLIGT//FOUO

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)**

OFFENTLIGT//FOUO



PM
Presentation av AnOm-material
 Sammanställt av
 Daniel Klein, Analytiker

5000-K654768-21 mfl.
 2021-12-09 11:27
 Region Syd
 Polisområde Södra Skåne

Färgsättning

I presenterade AnOm-chattar har respektive AnOm-identitet (JID), knuten till en viss person, färglagts med en egen färg. Detta för att det ska vara lättare att läsa materialet och kunna följa vem som skickar till vem.

Ljudfiler

I AnOm har det funnits möjlighet för användare att spela in ljudfiler/röstmeddelanden och skicka till andra AnOm-användare. Dessa ljudfiler är oftast relativt korta, mellan 2 - 30 sekunder. I rapporter i ärendet presenteras dessa ljudfiler med en utskrift av röstmeddelandet tillsammans med övriga chattar – detta för att göra materialet lättare att läsa i ett sammanhang.

Vidarebefordrade meddelanden

I AnOm har det funnits möjlighet för användarna att vidarebefordra meddelanden, både vad gäller text-, ljud-, video- och bildmeddelanden. Detta innebär att det funnits en funktion i telefonerna för att skicka vidare ett meddelande, som man fått eller skickat i en chatt, till en annan chatt. I inhämtade AnOm-chattar visas vidarebefordrade meddelanden lite ”klumpigt” och kan upplevas ostrukturerat och svåräst, detta på grund av att textfältet innehåller programmeringskod som användarna av AnOm sannolikt inte fått upp på sin telefons skärm i samband med att dessa meddelanden mottagits eller skickats.

I rapporter i ärendet har koden raderats för att i meddelandefältet endast ange den text eller typ av fil som vidarebefordrats och vilken användare som ursprungligen skickade meddelandet. Vid vidarebefordrade bilder/filmer/ljudklipp framgår i regel inte vilken fil det är som skickats. Dessa meddelanden har därför i rapporter fått texten ”*okänt innehåll*”.

Citerade meddelanden

I AnOm har det funnits möjlighet för användarna att i ett svar välja att citera det meddelandet som man svarar på. Liksom vid vidarebefordrade meddelanden innehåller dessa meddelanden kod som gör dem svåräst. I rapporter i ärendet visas endast texten som citerats samt det svar som meddelandet innehåller.

Syftet med att bearbeta vidarebefordrade och citerade meddelanden har varit att göra materialet lättare att läsa. På följande sidor presenteras exempel på hur denna typ av meddelanden har bearbetats.

Exempel på vidarebefordrat textmeddelande.....	2
Exempel på vidarebefordrad bildfil.....	3
Exempel på vidarebefordrad ljudinspelning.....	4
Exempel på citerat meddelande	5



PM
Presentation av AnOm-material
 Sammanställt av
 Daniel Klein, Analytiker

5000-K654768-21 mfl.
 2021-12-09 11:27
 Region Syd
 Polisområde Södra Skåne

Exempel på vidarebefordrat textmeddelande

Obearbetat textinnehåll från AnOm:

Time	Sender	Receiver	Message - Text
2021-03-17 14:29:16	8191be	c3b5d4	Vit polo
2021-03-17 14:34:51	c3b5d4	56d3f9	forward_prefix{"forward_message_time": 1615987801937, "forward_message_user_jid": "8191be", "forward_message_body": "Vit polo", "forward_message_type": "TEXT", "forward_message_uuid": "c1f1191a-9de1-46d8-9fbb-ffbb43dc600f"}

I exempel ovan skickas kl. 14:29:16 meddelandet med texten "Vit polo" från 8191be till c3b5d4. C3b5d4 vidarebefordrar sedan kl. 14:34:51 samma meddelande till 56d3f9.

I rapporten i ärendet presenteras materialet ovan på följande sätt:

Time	Sender	Receiver	Message - Text
2021-03-17 14:29:16	8191be	c3b5d4	Vit polo
2021-03-17 14:34:51	c3b5d4	56d3f9	Vidarebefordrat meddelande från 8191be: "Vit polo"



PM
Presentation av AnOm-material
 Sammanställt av
 Daniel Klein, Analytiker

5000-K654768-21 mfl.
 2021-12-09 11:27
 Region Syd
 Polisområde Södra Skåne

Exempel på vidarebefordrad bildfil

Obearbetat textinnehåll från AnOm:

Time	Sender	Receiver	Text/Media
2021-01-14 21:05:55	c3b5d4	225375	Its look like unprofessional stone hihi
2021-01-14 21:06:49	225375	c3b5d4	I will tell them next time make bricks
2021-01-14 21:07:00	225375	c3b5d4	But quality is very high
2021-01-14 21:07:08	c3b5d4	225375	forward_prefix{"forward_message_time": 1610310061813, "forward_message_user_jid": "56d3f9", "forward_message_type": "IMAGE", "forward_message_uuid": "e2e97d0a-ea7f-4f30-b33f-a198f1ad95aa"}
2021-01-14 21:07:54	c3b5d4	225375	forward_prefix{"forward_message_time": 1610310063562, "forward_message_user_jid": "56d3f9", "forward_message_type": "IMAGE", "forward_message_uuid": "1e5e56fb-57fb-4299-bc3c-9ccb3c96302"}
2021-01-14 21:08:31	c3b5d4	225375	Its should look like this Haha but ok

I exempel ovan vidarebefordrar c3b5d4 kl. 21:07:08 och kl. 21:07:54 bildfiler (IMAGE) till 225375.

Bilderna har c3b5d4 ursprungligen fått från 56d3f9.

Det går inte i materialet att utläsa vilka bildfiler som skickats och det anges därför ”*Okänt innehåll*” i rapporten.

I rapporten i ärendet presenteras materialet ovan på följande sätt:

Time	Sender	Receiver	Text/Media
2021-01-14 21:05:55	c3b5d4	225375	Its look like unprofessional stone hihi
2021-01-14 21:06:49	225375	c3b5d4	I will tell them next time make bricks
2021-01-14 21:07:00	225375	c3b5d4	But quality is very high
2021-01-14 21:07:08	c3b5d4	225375	Vidarebefordrad bildfil från 56d3f9. *Okänt innehåll*
2021-01-14 21:07:54	c3b5d4	225375	Vidarebefordrad bildfil från 56d3f9. *Okänt innehåll*
2021-01-14 21:08:31	c3b5d4	225375	Its should look like this Haha but ok



PM
Presentation av AnOm-material
 Sammanställt av
 Daniel Klein, Analytiker

5000-K654768-21 mfl.
 2021-12-09 11:27
 Region Syd
 Polisområde Södra Skåne

Exempel på vidarebefordrad ljudinspelning

Obearbetat textinnehåll från AnOm:

Time	Sender	Receiver	Text/Media
2021-03-12 23:25:58	56d3f9	c3b5d4	Ljudfil: f91b07dc-6f10-4c2d-a435-c74833cd83ed-pitchfixed.wav
2021-03-12 23:25:58	c3b5d4	56d3f9	I have to tell him now I get things soon so he don't buy from other
2021-03-12 23:26:28	c3b5d4	8191be	forward_prefix{"forward_message_time": 1615584046362, "forward_message_user_jid": "56d3f9", "forward_message_type": "PTT", "forward_message_uuid": "928b12fd-956f-465e-8d84-97f69d8c6a88"}

I exempel ovan skickar 56d3f9 en ljudfil till c3b5d4 kl. 23:25:58.

c3b5d4 vidarebefordrar kl. 23:26:28 en ljudfil (PTT-PushToTalk) till 8191be.

Man kan tänka sig att ljudfilen som vidarebefordras är den samma som ursprungligen kom från 56d3f9 kl. 23:25:58 – men det går inte i materialet att utläsa om det är samma ljudfil och det anges därför **"*Okänt innehåll*"** i rapporten.

I rapporten i ärendet presenteras materialet ovan på följande sätt:

Time	Sender	Receiver	Text/Media
2021-03-12 23:25:58	56d3f9	c3b5d4	Ljudfil: f91b07dc-6f10-4c2d-a435-c74833cd83ed-pitchfixed.wav Utskrift: <i>*vi skriver ut vad som sägs i ljudfilen*</i>
2021-03-12 23:25:58	c3b5d4	56d3f9	I have to tell him now I get things soon so he don't buy from other
2021-03-12 23:26:28	c3b5d4	8191be	Vidarebefordrad ljudfil från 56d3f9. *Okänt innehåll*



PM
Presentation av AnOm-material
 Sammanställt av
 Daniel Klein, Analytiker

5000-K654768-21 mfl.
 2021-12-09 11:27
 Region Syd
 Polisområde Södra Skåne

Exempel på citerat meddelande

Obearbetat textinnehåll från AnOm:

Time	Sender	Receiver	Text/Media
2021-01-14 16:11:43	c3b5d4	225375	He is swedish driver and stash guy
2021-01-14 16:12:14	225375	c3b5d4	quote_prefix{"quote_message_time": 1610637186799,"quote_message_text ":"He is swedish driver and stash guy\n","quoted_text":"Perfect bro","quote_message_user_jid":"c3b5d4","message_uid":"0d6f6f2e-4882-4972-a13c-3085edf1dea9","isQuotedMessageDeleted":false,"isEdited":false}

I exempel ovan använder 225375 kl. 16:12:14 en funktion i AnOm-chatt där han först citerar det tidigare meddelandet från c3b5d4 och sedan skickar med ett svar.

I rapporten i ärendet presenteras materialet ovan på följande sätt:

Time	Sender	Receiver	Text/Media
2021-01-14 16:11:43	c3b5d4	225375	He is swedish driver and stash guy
2021-01-14 16:12:14	225375	c3b5d4	Quote: He is swedish driver and stash guy Message: Perfect bro



Brukaranalys
46720322893
Sammanställt av
Daniel Klein, Analytiker

5000-K654847-21
2021-09-07
Region Syd
Polisområde Södra Skåne

1 Brukaranalys av telefonnummer 46720322893

Nedan uppgifter visar på att Oscar Thomsen är den som brukat telefonnummer 46720322893.

1.1. Telefon i beslag från Oscar, 2021-5000-BG62924-1

I samband med gripandet av Oscar 2021-05-21 togs en Samsung-telefon i beslag från Oscar. Den IT-forensiska undersökningen har visat att det senaste telefonnumret som brukades i telefonen var 46720322893.

1.2. Swish

46720322893 är registrerat på den misstänkte Oscar Thomsen på betaltjänsten Swish.

1.3. 46720322893 i kontaktböcker

I Mathilda Johanssons telefon (beslag 2021-5000-BG101183-1) ligger telefonnummer 46720322893 sparad under namnet "Oscar💎❤️".

I Ann-Helen Falks telefon (beslag 2021-5000-BG62947-1) ligger telefonnummer 46720322893 sparad under namnet "Oscar T".

1.4. Kontakter i HÖK-listan

Det har från teleoperatören inhämtats trafikhistorik för 46720322893 för perioden 2020-12-03 – 2021-05-21. Under denna period sker flest kontakter med nedan tre telefonnummer. Brukarna har kopplats till respektive telefonnummer då de är registrerade med dessa på betaltjänsten Swish.

Telefonnummer	Antal trafikhändelser	Identifierad brukare	Relation till Oscar
46707450820	649	Eva-Karin Marie Lindberg	mamma
46768940340	570	Mathilda Johansson	vän
46760732533	501	Madeléne Thomsen	syster



Brukaranalys
46720322893
 Sammanställt av
 Daniel Klein, Analytiker

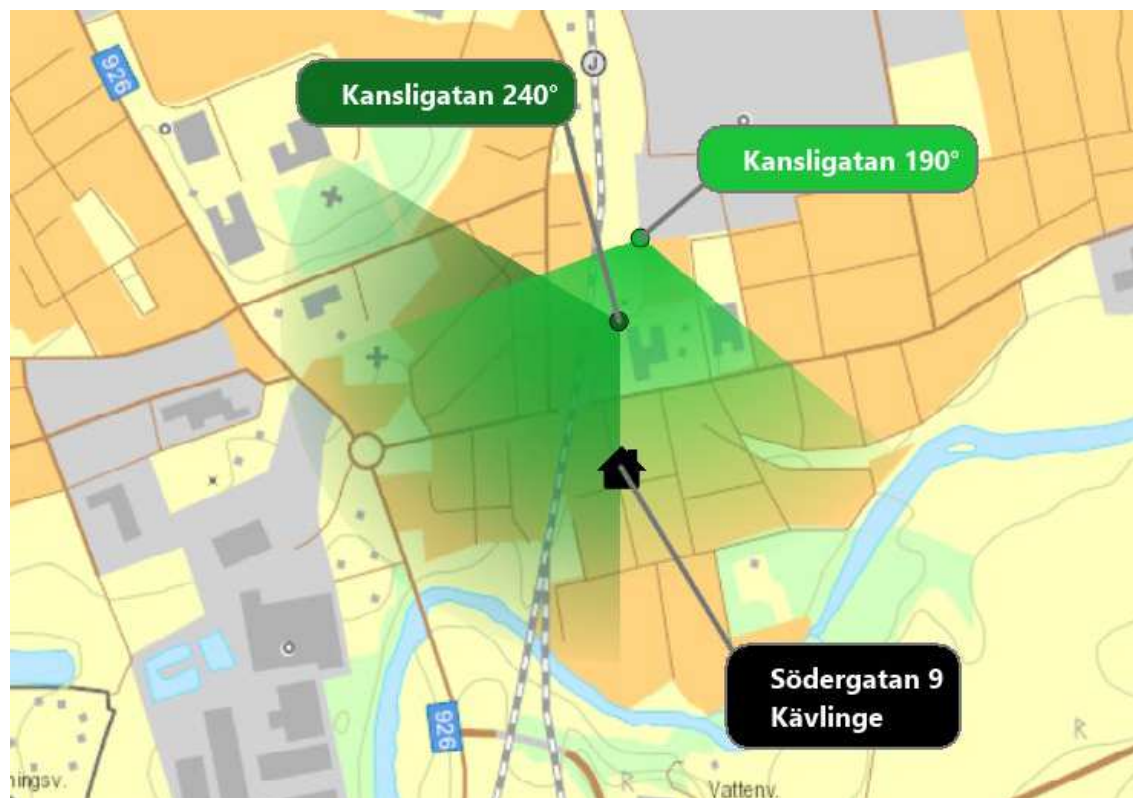
5000-K654847-21
 2021-09-07
 Region Syd
 Polisområde Södra Skåne

1.5. Mest frekvent förekommande basstationer

Det har från teleoperatören inhämtats trafikhistorik för 46720322893 för perioden 2020-12-03 – 2021-05-21, materialet ger från 2021-02-09 information om vilka basstationer som telefonnumret kopplar upp mot. På grund av lagringsdirektiv saknas information om basstationer längre tid tillbaka.

Nedan presenteras de fem mest förekommande basstationerna som 46720322893 kopplar upp mot. Telefonnumret kopplar absolut mest frekvent upp mot basstationerna *Kansligatan 240°* och *Kansligatan 190°*. Basstationerna är belägna i Kävlinge och ger täckning mot den adress där den misstänkte Oscar har sin bostad, Södergatan 9. Basstationerna och deras täckningsriktning illustreras på karta nedan.

Basstationer	Antal uppkopplingar	% Antal uppkopplingar
Kansligatan 240°	530	17%
Kansligatan 190°	528	17%
Planteringen/Skogsgatan 280°	231	7%
Helsingborg S 120°	152	5%
Blentarp 10°	145	5%





Extraction Report - Apple iPhone

Utdrag från Ann-Helens telefon (BG62947-1) - Kontaktboken

Contacts (2)

#	Contact	Timestamp	Entries	Addresses	Notes	Deleted
1	Name: Oscar T Source: Recents Source Extraction: File System Source file: DarArchive/root/private/var/mobile/Library/Recents/Recents-wal : 0x17CE07 (Table: contacts; Size: 1821072 bytes)		Phone: +46720322893			
2	Name: Oscar T Source Extraction: File System Source file: DarArchive/root/private/var/mobile/Library/AddressBook/AddressBook.sqlitedb : 0x88E4B (Table: ABPerson, ABMultiValue; Size: 806912 bytes) DarArchive/root/private/var/mobile/Library/CoreDuet/People/interactionC.db-wal : 0x12431E (Table: ZCONTACTS; Size: 3633872 bytes)	Created: 2020-12-23 16:18:31(UTC+1) Modified: 2020-12-24 10:05:40(UTC+1)	User ID: User ID A1A3FADE-2560-42CE-B2D6-5CFF3D428917:ABPerson Identifier +46720322893 Phone: General 0720322893		InteractionC: incoming interaction count: 6 InteractionC: incoming interaction count: 14 InteractionC: outgoing interaction count: 10	



Cellebrite
www.cellebrite.com

Extraction Report - Apple iPhone

Utdrag från Mathildas telefon (BG101183-1) - Kontaktboken

Contacts (2)

#	Contact	Timestamp	Entries	Addresses	Notes	Deleted
1	Name: Oscar Source file: Mathildas iPhone/mobile/Librar y/Recents/Recents : 0x1F40F (Table: contacts; Size: 180224 bytes)		Phone: +46720322893			
2	Name: Oscar Source file: Mathildas iPhone/mobile/Librar y/AddressBook/Addr essBook.sqlitedb : 0x56A71 (Table: ABPerson, ABMultiValue; Size: 454656 bytes) Mathildas iPhone/mobile/Librar y/CoreDuet/People/i nteractionC.db : 0x2F2BF (Table: ZCONTACTS; Size: 3076096 bytes)	Created: 2021-02-08 21:27:26(UTC+1) Modified: 2021-03-02 22:00:42(UTC+1)	User ID: User ID CCB3B89E-D592-4919- 942D-5455BD36C6A3:ABPerson Identifier +46720322893 Phone: General 0720322893		InteractionC: incoming interaction count: 88 InteractionC: incoming interaction count: 112 InteractionC: outgoing interaction count: 178	



Brukaranalys
An0m-enhet 8191be
Sammanställt av
Daniel Klein, Analytiker

5000-K654847-21 mfl.
2021-12-06
Region Syd
Polisområde Södra Skåne

1 Brukaranalys av An0m-enhet 8191be

Nedan uppgifter visar på att Oscar Thomsen är den som brukat An0m-enheten med identitetsnummer 8191be.

1.1. 2020-11-18 Fotograferad An0m-chatt anträffad i Oscars Samsung-telefon

Från Oscar Thomsen togs en Samsung-telefon i beslag (BG62924-1). I telefonen har det anträffats ett utgående chatt-meddelande där det bifogats en bild. Bilden visar en telefonskärm som har fotograferats och på skärmen visas en chatt mellan "Rampage" och "Me" (telefonens brukare).

Samma chatt som har fotograferats har anträffats i det inhämtade An0m-materialet och det framgår där att den som i den avfotograferade chatten angavs som "Me" är 8191be.

1.2. 2021-01-14 Film med välliknande tatuering

8191be skickar 2021-01-14 en film på An0m som visar hur en person hanterar ett vitt pulver på ett kakelgolv. Man får uppfattningen av att det är personen på filmen som själv spelar in filmen. Personen bär svarta handskar, men en tatuering syns på handen och nedre delen av armen. Den misstänkte Oscar Thomsen har välliknande tatueringar.

NFC slutsats av jämförelse mellan person som visas på filmen och bild på Oscars tatueringar ger att *"Resultaten talar starkt för att personen på bilden i material Sax+tatuering.PNG är densamma som mannen på bilderna i material Jämförelsebilder tatuering (Grad +3)."* (NFC Sakkunnigutlåtande 2021015484)





Brukaranalys
AnOm-enhet 8191be
 Sammanställt av
 Daniel Klein, Analytiker

5000-K654847-21 mfl.
 2021-12-06
 Region Syd
 Polisområde Södra Skåne

1.3. 2021-01-22 c3b5d4 skickar bild på den som ska åka upp på måndag

I AnOm-chatt 2021-01-22 diskuterar man att en person ska åka upp till Stockholm måndagen den 25 januari och i samband med detta skickas ett fotografi på den misstänkte Oscar Thomsen. Utifrån material i AnOm-chatt för 8191be sker en resa till Stockholm 2021-01-25. Övervakning på Centralstationen och uppgifter i HÖK-lista för Oscars telefonnummer 46720322893 visar att Oscar Thomsen är uppe i Stockholm samma dag vid tidpunkter som korrelerar med uppgifterna i AnOm-chatten.



1.4. 2021-01-25 Tågresä

2021-01-25 05:09 skickar 8191be meddelandet "God morgon tar tåget nu".

Inhämtad HÖK-lista för 46720322893, visar att det 2021-01-25 mellan 05:03-05:07 inkommer SJ-biljett (SJBILJ) till telefonnumret.

Utdrag från AnOm-chatt

Time	Sender	Receiver	Text / Media
2021-01-25 05:09:57	8191be	c3b5d4	Godmorgon tar tåget nu

Utdrag från HÖK-lista för Oscars telefonnummer 46720322893

Typ	Datum	Tid	A_Part (Från)	B_Part (Till)
SMS	2021-01-25	05:03:09	SJBILJ	46720322893
SMS	2021-01-25	05:04:27	SJBILJ	46720322893
SMS	2021-01-25	05:07:01	SJBILJ	46720322893
SMS	2021-01-25	05:07:02	SJBILJ	46720322893



Brukaranalys
An0m-enhet 8191be
 Sammanställt av
 Daniel Klein, Analytiker

5000-K654847-21 mfl.
 2021-12-06
 Region Syd
 Polisområde Södra Skåne

1.5. 2021-01-25 Uppgifter om tågresor i An0m samt i chatt med Oscar

I An0m chatt skriver 8191be 2021-01-25 13:59 "Yes är i Hässleholm kl 4 så hämtar dennis hängis mig där och kör mig till hbg".

I A-H Falks mobiltelefon har det anträffats en chatt med Oscar Thomsens konto. I chatten skriver personen 2021-01-25 14:45 "Jag är snart hemma igen eller ja jag är i Hässleholm kl 4". Hon frågar "Ska du till hbg sen eller?" och får 17:28 svaret "Yes är där snart".

Inhämtad HÖK-lista för telefonnummer 46720322893, som är knutet till Oscar Thomsen, visar att det 2021-01-25 11:02-16:12 sker kontakter med ett telefonnummer som via betaltjänsten Swish är registrerat på en Dennis Karlsson. Dennis är folkbokförd i Hyllinge som är beläget cirka 10 kilometer öster om Helsingborg.

Utdrag från An0m-chatt

Time	Sender	Receiver	Text / Media
2021-01-25 13:57:28	7d4d4c	8191be	Är du på väg hem?
2021-01-25 13:59:33	8191be	7d4d4c	Yes är i hässleholm kl 4 så hämtar dennis hängis mig där och kör mig till hbg

Utdrag från chatt anträffad i Falks mobiltelefon (beslag BG62947-1).

Tidpunkt	Från	Till	Text
2021-01-25 14:38:24	A-H Falk	Oscar Thomsen	Framme än?
2021-01-25 14:45:52	Oscar Thomsen	A-H Falk	Jag är snart hemma igen eller ja jag är i Hässleholm kl 4
2021-01-25 14:48:21	A-H Falk	Oscar Thomsen	Skönt det i alla fall
2021-01-25 14:51:09	A-H Falk	Oscar Thomsen	Ska du till hbg sen eller?
2021-01-25 17:28:11	Oscar Thomsen	A-H Falk	Yes är där snart

Utdrag från HÖK-lista för Oscars telefonnummer 46720322893

Typ	Datum	Start Tid	Stopp Tid	Längd	A_Part (Från)	Namn	B_Part (Till)	Namn
Samtal	2021-01-25	11:02:04	11:02:04	00:00:00	46720322893	Oscar	46708182188	Dennis
Samtal	2021-01-25	11:50:41	11:50:44	00:00:04	46720322893	Oscar	46708182188	Dennis
SMS	2021-01-25	11:50:59			46720322893	Oscar	46708182188	Dennis
SMS	2021-01-25	11:51:47			46720322893	Oscar	46708182188	Dennis
Samtal	2021-01-25	11:57:45	11:58:44	00:00:59	46708182188	Dennis	46720322893	Oscar
SMS	2021-01-25	16:05:37			46708182188	Dennis	46720322893	Oscar
SMS	2021-01-25	16:12:57			46720322893	Oscar	46708182188	Dennis



Brukaranalys
AnOm-enhet 8191be
Sammanställt av
Daniel Klein, Analytiker

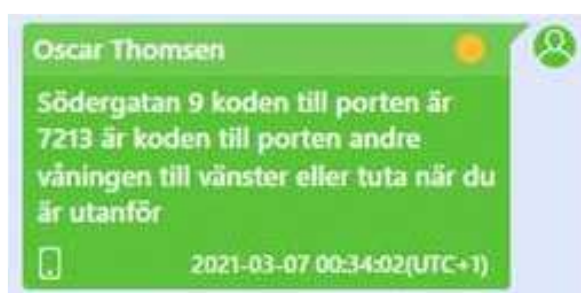
5000-K654847-21 mfl.
2021-12-06
Region Syd
Polisområde Södra Skåne

1.6. 2021-03-20 Portkod till Södergatan 9

2021-03-20 20:36 skickar 8191be en ljudfil på AnOm. På ljudfilen säger en mansperson:

"Be dom gå ut till porten istället, denna gången, port 9. Koden är 7213 in. Så möter jag dem i porten istället, för det fungera inte att vi springer där ute."

I Oscar privata Samsung-telefon, beslag BG62924-1 har det anträffats ett utgående meddelande, daterat 2021-03-07 00:34, där det står: *"Södergatan 9 koden till porten är 7213 är koden till porten andre våningen till vänster eller tuta när du är utanför"*.



Den misstänkte Oscar Thomsen var vid tillfället boende på Södergatan 9 i Kävlinge.

1.7. Uppgifter som visar att ytterligare en person brukat 8191be

Vid fyra olika datum (2021-03-18, 2021-03-26, 2021-04-12, 2021-04-13) skickas meddelanden på danska från 8191be. Uppgiften visar på att det sannolikt är en annan person än Oscar som brukar AnOm-telefonen med 8191be vid dessa tillfällen, då det i meddelande från telefonen framgått att Oscar har svårt att förstå danska. 2021-03-20 18:40:14 skickas AnOm-meddelandet *"Men där står väl inget om det fattar inte riktigt danska 😊"*

En analys av material i ärendet visar att det vid samtliga dessa fyra datum finns uppgifter som visar på att Oscar är tillsammans med Ali Aghazadeh i närtid till att meddelanden på danska skickas från AnOm-telefonen 8191be. Ali är danskspråkig.

Detta material presenteras i en separat rapport.

I övrigt har det inte anträffats något material som visar på att någon annan än Oscar brukat 8191be.


Cellebrite

www.cellebrite.com

Extraction Report - Google Android Generic

Utdrag från Oscars Samsung-telefon (BG62924-1) - Chattmeddelande med bifogad bild

Chats (1)

#		Deleted
1	Start Time: 2020-10-19 14:57:52(UTC+2) Last Activity: 2021-05-21 15:50:14(UTC+2) Number of attachments: 79 Source: WhatsApp Source file: Universal_Android Access.zip/data/data/com.whatsapp/databases/msgstore.db : 0x210FF5 (Table: call_log, messages, chat_list; Size: 8196096 bytes) Universal_Android Access.zip/data/data/com.whatsapp/databases/wa.db : 0x24A5A (Table: wa_contacts; Size: 163840 bytes) Universal_Android Access.zip/data/data/com.whatsapp/shared_prefs/registration.RegisterPhone.xml : 0x198 (Size: 706 bytes) Universal_Android Access.zip/data/data/com.whatsapp/shared_prefs/com.whatsapp_preferences_light.xml : 0x19C6 (Size: 8670 bytes) Body file: chat-1.txt Participants:  46737815260@s.whatsapp.net Ali  46720322893@s.whatsapp.net O (owner) Identifier: 46737815260@s.whatsapp.net	

From: 46720322893@s.whatsapp.net O (owner)

To: 46737815260@s.whatsapp.net Ali

Attachments:



Size: 104556
File name: IMG-20201118-WA0003.jpg
Path: https://mmg.whatsapp.net/d/t/AsAz2QOU2C9UIGm0uLRFVj9xnjdp8srW-TTCYivE8vK8.enc

Participant	Delivered	Read	Played
46737815260@s.whatsapp.net Ali	2020-11-18 21:45:30(UTC+1)		

Status: Delivered

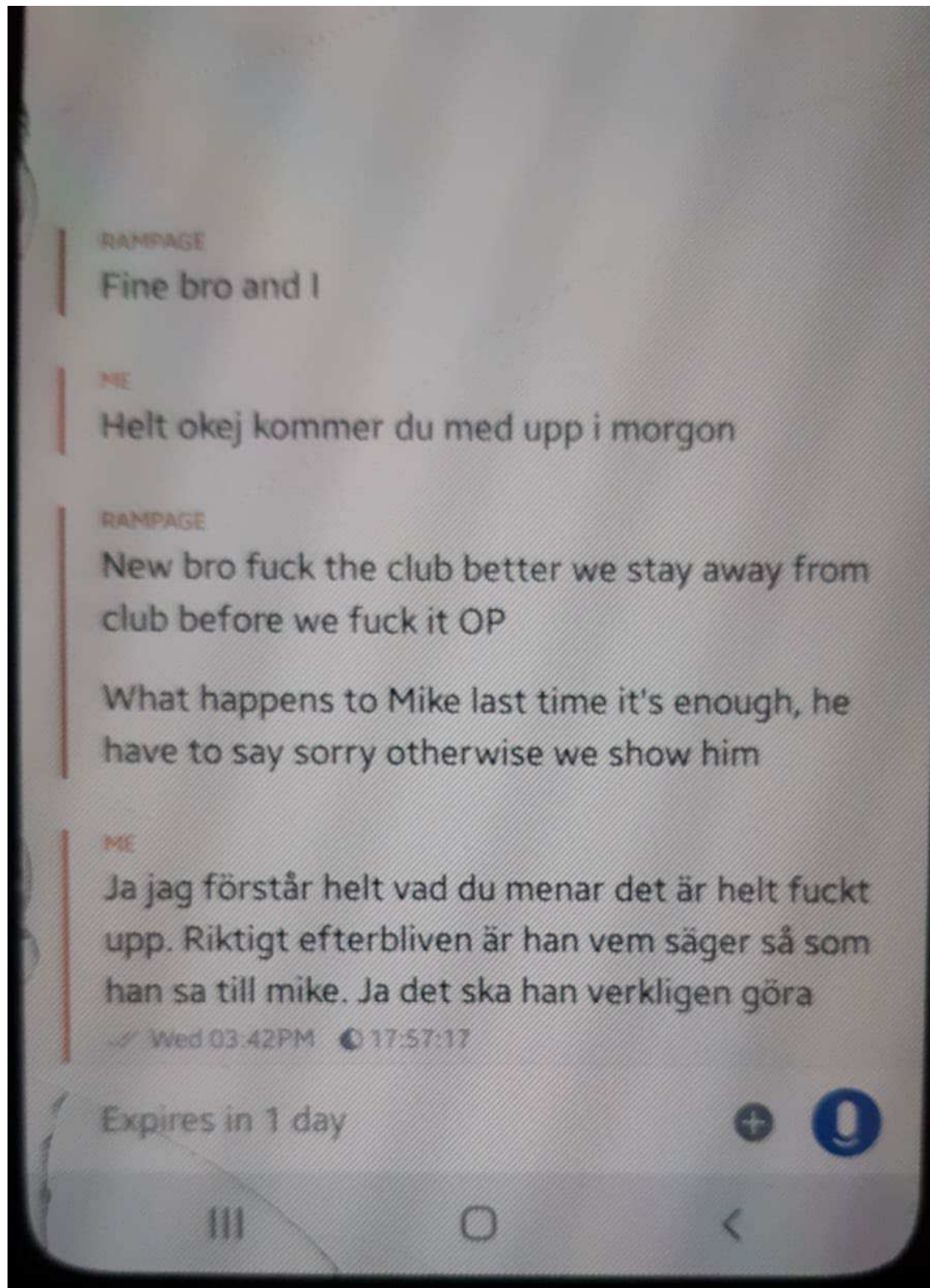
Platform: Mobile

2020-11-18 21:45:27(UTC+1)

Source Info:
Universal_Android Access.zip/data/data/com.whatsapp/databases/msgstore.db : 0x27F941 (Table: messages; Size: 8196096 bytes)
Universal_Android Access.zip/data/data/com.whatsapp/shared_prefs/registration.RegisterPhone.xml : 0x198 (Size: 706 bytes)
Universal_Android Access.zip/data/data/com.whatsapp/shared_prefs/com.whatsapp_preferences_light.xml : 0x19C6 (Size: 8670 bytes)
Universal_Android Access.zip/data/data/com.whatsapp/databases/wa.db : 0x24A5A (Table: wa_contacts; Size: 163840 bytes)
Universal_Android Access.zip/data/media/0/WhatsApp/Media/WhatsApp Images/Sent/IMG-20201118-WA0003.jpg : (Size: 104556 bytes)

Foto anträffat i bifogat meddelande från Oscars telefon

IMG-20201118-WA0003.jpg



Utdrag från An0m – chatt 2021-11-18 mellan 8191be och c3b5d4



c3b5d4 2020-11-18 00:54:41+01:00
Fine bro and I



8191be 2020-11-18 00:55:37+01:00
Helt okej kommer du med upp i morgon



c3b5d4 2020-11-18 00:56:37+01:00
New bro fuck the club better we stay away from club before we fuck it OP



c3b5d4 2020-11-18 00:57:50+01:00
What happens to Mike last time it's enough, he have to say sorry otherwise we show him



8191be 2020-11-18 15:32:12+01:00
Ja jag förstår helt vad du menar det är helt fuckt upp. Riktigt efterbliven är han vem säger så som han sa till mike. Ja det ska han verkligen göra



Cellebrite
www.cellebrite.com

Extraction Report - Apple iPhone

Utdrag från Oscars Samsung-telefon (BG62924-1) - Chatt med Ann-Helen

Chats (1)

#		Deleted
1	Start Time: 2020-01-13 22:39:29(UTC+1) Last Activity: 2021-05-18 21:15:07(UTC+2) Number of attachments: 20 Source: Facebook Messenger Account: 100000468048741 Source file: DarArchive/root/private/var/mobile/Containers/Shared/AppGroup/3163E83E-3F44-410A-95AF-8E57A6C373D1/lightspeed-100000468048741.db : 0x8A0B0D (Table: messages, contacts; Size: 9854976 bytes) Source Extraction: File System Body file: chat-1.txt Participants:  505928359 Oscar Thomsen  100000468048741 Ann-Helen Falk (owner)	

From: 100000468048741 Ann-Helen Falk

Jobbar. Vad gor du?

Status: Sent

Platform: Mobile

2021-01-25 13:47:40(UTC+1)

Source Extraction:
File System
Source Info:
DarArchive/root/private/var/mobile/Containers/Shared/AppGroup/3163E83E-3F44-410A-95AF-8E57A6C373D1/lightspeed-100000468048741.db : 0x82707C (Table: messages; Size: 9854976 bytes)

From: 505928359 Oscar Thomsen

Aker trakigt tag fett drygt

2021-01-25 13:52:33(UTC+1)

Source Extraction:
File System
Source Info:
DarArchive/root/private/var/mobile/Containers/Shared/AppGroup/3163E83E-3F44-410A-95AF-8E57A6C373D1/lightspeed-100000468048741.db : 0x827117 (Table: messages; Size: 9854976 bytes)

From: 100000468048741 Ann-Helen Falk

Forstar jag

Status: Sent

Platform: Mobile

2021-01-25 13:55:51(UTC+1)

Source Extraction:
File System
Source Info:
DarArchive/root/private/var/mobile/Containers/Shared/AppGroup/3163E83E-3F44-410A-95AF-8E57A6C373D1/lightspeed-100000468048741.db : 0x8271BD (Table: messages; Size: 9854976 bytes)

From: 100000468048741 Ann-Helen Falk

Framme an?

Status: Sent

Platform: Mobile

2021-01-25 14:38:24(UTC+1)

Source Extraction:
File System
Source Info:
DarArchive/root/private/var/mobile/Containers/Shared/AppGroup/3163E83E-3F44-410A-95AF-8E57A6C373D1/lightspeed-100000468048741.db : 0x827252 (Table: messages; Size: 9854976 bytes)

From: 505928359 Oscar Thomsen

Jag ar snart hemma igen eller ja jag ar i Hassleholm kl 4

2021-01-25 14:45:51(UTC+1)

Source Extraction:
File System
Source Info:
DarArchive/root/private/var/mobile/Containers/Shared/AppGroup/3163E83E-3F44-410A-95AF-8E57A6C373D1/lightspeed-100000468048741.db : 0x8272E5 (Table: messages; Size: 9854976 bytes)

From: 100000468048741 Ann-Helen Falk

Skont det i alla fall

Status: Sent

Platform: Mobile

2021-01-25 14:48:21(UTC+1)

Source Extraction:
File System
Source Info:
DarArchive/root/private/var/mobile/Containers/Shared/AppGroup/3163E83E-3F44-410A-95AF-8E57A6C373D1/lightspeed-100000468048741.db : 0x8273A9 (Table: messages; Size: 9854976 bytes)

From: 100000468048741 Ann-Helen Falk

Ska du till hbg sen eller?

Status: Sent

Platform: Mobile

2021-01-25 14:51:09(UTC+1)

Source Extraction:
File System
Source Info:
DarArchive/root/private/var/mobile/Containers/Shared/AppGroup/3163E83E-3F44-410A-95AF-8E57A6C373D1/lightspeed-100000468048741.db : 0x827446 (Table: messages; Size: 9854976 bytes)

From: 505928359 Oscar Thomsen

Yes ar dar snart

2021-01-25 17:28:11(UTC +1)

Source Extraction:

File System

Source Info:

DarArchive/root/private/var/mobile/Containers/Shared/AppGroup/3163E83E-3F44-410A-95AF-8E57A6C373D1/lightspeed-100000468048741.db : 0x8274E6 (Table: messages; Size: 9854976 bytes)



Cellebrite
www.cellebrite.com

Extraction Report - Google Android Generic

Utdrag från Oscars Samsung-telefon (BG62924-1) - Chattmeddelande om portkod

Chats (1)

#		Deleted
1	Start Time: 2021-01-23 22:56:04(UTC+1) Last Activity: 2021-04-08 10:59:34(UTC+2) Number of attachments: 5 Source: Facebook Messenger Source file: Universal_Android Access.zip/data/data/com.facebook.orca/databases/threads_db2 : 0x3F37E5 (Table: messages, threads; Size: 15728640 bytes) Universal_Android Access.zip/data/data/com.facebook.orca/app_light_prefs/com.facebook.orca/authentication : 0xD0 (Size: 1170 bytes) Universal_Android Access.zip/data/data/com.facebook.orca/databases/omnistore_505928359_v01.db : 0x28A748 (Size: 10280960 bytes) Body file: chat-1.txt Participants:  100041688524817 Moffe Glad  505928359 Oscar Thomsen (owner) Identifier: 100041688524817	

From: 505928359 Oscar Thomsen (owner)

Södergatan 9 koden till porten är 7213 är koden till porten andre våningen till vänster eller tuta när du är utanför

Platform: Mobile

2021-03-07 00:34:02(UTC +1)

Source Info:
Universal_Android Access.zip/data/data/com.facebook.orca/databases/threads_db2 : 0x5C3CFA (Table: messages; Size: 15728640 bytes)



Brukaranalys
An0m-enhet c3b5d4
Sammanställt av
Daniel Klein, Analytiker

5000-K654847-21

2021-12-13

Region Syd
Polisområde Södra Skåne

1 Brukaranalys av An0m-enhet c3b5d4

Nedan uppgifter visar på att Atif Pervez/Perviz är den som brukat An0m-enheten med identitetsnummer c3b5d4.

1.1. 2020-08-09 Motpart säger "Atif" på skickad ljudfil

2020-08-09 11:53 skickar motparten 8191be ett röstmeddelande till c3b5d4. I inspelningen säger personen *"Jaja inga problem, inga problem. Han var jätteglad i alla fall och han sa nästa runda han har 20 30. Jag sa till honom 'du får ta det med Atif, fixa med honom, han vet bäst', han bara 'okej'".*

C3b5d4 svarar 25 sekunder senare genom att skicka ett inspelat röstmeddelande tillbaka till 8191be där han säger *"Du ska inte ta, *ohörbart* mitt namn på telefon bror"*.

1.2. 2020-08-25 Bild skickas från c3b5d4

2020-08-25 skickar c3b5d4 en bild till en oidentifierad motpart. Personen i förgrunden ser ut att hålla kameran/telefonen och en mansperson i bakgrunden riktar en knuten näve mot kameran som om han höll i en pistol och ena fingret på avtryckaren, 10 sekunder efter bilden skickar c3b5d4 även textmeddelandet "the killer".

Nedan en bildjämförelse mellan bilden skickad från An0m c3b5d4 (personen i vit tröja) och bild inhämtad från SIS på Raja Atif Pervez 19830628.



Källa: SIS



Brukaranalys
An0m-enhet c3b5d4
 Sammanställt av
 Daniel Klein, Analytiker

5000-K654847-21
 2021-12-13
 Region Syd
 Polisområde Södra Skåne

1.3. 2020-10-29 Telefonnummer 0046739018616

2020-10-29 framgår i ett meddelande till c3b5d4 att "Bess" vill ha telefonnumret till c3b5d4. C3b5d4 svarar med textmeddelandet "0046739018616".

Time	Sender	Receiver	Text
2020-10-29 21:20:34	8191be	c3b5d4	Bess är här och vill ha dit nummer
2020-10-29 21:21:12	c3b5d4	8191be	Ok wait
2020-10-29 21:21:54	c3b5d4	8191be	0046739018616

Vid kontroll 2021-08-26 är telefonnummer 46739018616 registrerat på betaltjänsten Swish på personen Thy-Tam Tine Do. Personen är en kvinna med Danskt medborgarskap som är registrerad som utvandrad från Sverige 2021-07-01. Raja Atif Pervez med personnummer 830628- är registrerad som make till Thy-Tam Tine Do.

Enligt en Promemoria upprättad 2020-07-24 i annat ärende (K841379-20) framkommer uppgifter från anställd vid Gränspolissectionen i Malmö om att Atif Perviz uppgett att han bor hos sin danska fru Thy Tam Tine Do i Malmö. I bifogade resehandlingar till samma promemoria framgår att efternamnet där stavas Pervez.

I promemoria i ärendet 5000-K581825-21 omnämns de olika identiteter som förekommit för Atif, och att det är samma person som brukat personnummer 830628- och 19800261-. *PM Angående identiteten på Atif Pervez, 2021-08-30, S Svensson.*

1.4. 2020-12-01 RIA-överföring

2020-12-01 skriver en oidentifierad motpart att c3b5d4 ska skicka över sitt konto och kod för en banktransaktion. C3b5d4 svarar med meddelandetexten "Raja atif pervez" och "Malmo sweden". Motparten frågar om han inte har något kontonummer. C3b5d4 svarar att han inte vill ha på bank utan att det ska skickas på "RIA money transfer".

Time	Sender	Receiver	Text
2020-12-01 11:01:37	3c77a5	c3b5d4	Give me account and sort code and I will bank today
2020-12-01 14:16:16	c3b5d4	3c77a5	Raja atif pervez
2020-12-01 14:16:20	c3b5d4	3c77a5	Malmo swedan
2020-12-01 14:27:50	3c77a5	c3b5d4	Bro don't you have account number and sortcode
2020-12-01 14:28:05	3c77a5	c3b5d4	Which company you want me to send from
2020-12-01 14:31:30	c3b5d4	3c77a5	Not good in bank bro
2020-12-01 14:31:54	c3b5d4	3c77a5	Just send me from RIA money transfer
2020-12-01 14:41:03	3c77a5	c3b5d4	That's what I was thinking
2020-12-01 14:41:22	3c77a5	c3b5d4	I will go post office after work



Brukaranalys
An0m-enhet c3b5d4
 Sammanställt av
 Daniel Klein, Analytiker

5000-K654847-21
 2021-12-13
 Region Syd
 Polisområde Södra Skåne

2020-12-01 14:41:55	c3b5d4	3c77a5	Ok bro thanks
2020-12-01 14:46:06	3c77a5	c3b5d4	Thank u bro
2020-12-01 16:11:39	3c77a5	c3b5d4	Yo
2020-12-01 16:13:45	3c77a5	c3b5d4	I am going to send in morning I will leave money with Usman tonight he will bank it because I finish at 6 and won't make post office today
2020-12-01 16:14:16	3c77a5	c3b5d4	He will go post office tomorrow morning

1.5. 2021-01-14 Telefonnummer 0046734141971

2021-01-14 ber användare av An0m-enheten 225375 om att c3b5d4 ska skicka sitt telefonnummer så att de har en "Backup-kontakt". C3b5d4 skickar då textmeddelande tillbaka med texten "0046734141971".

Time	Sender	Receiver	Text
2021-01-14 16:02:15	225375	c3b5d4	Bro
2021-01-14 16:02:30	225375	c3b5d4	Send me your signal number
2021-01-14 16:02:33	225375	c3b5d4	Please
2021-01-14 16:02:44	225375	c3b5d4	We must have backup contact
2021-01-14 16:06:59	c3b5d4	225375	Ok br
2021-01-14 16:07:52	225375	c3b5d4	Send it here i call you in 1 hour
2021-01-14 16:10:13	c3b5d4	225375	0046734141971

Enligt uppgift i Polisens utredningssystem Dur2 är telefonnumret knutet till 830628-Raja Atif Pervez i samband med annan utredning.

Även i tidigare omnämnd Promemoria, upprättad 2020-07-24 i ärendet K841379-20, framgår att Atif lämnat telefonnummer 0734141971 som sitt eget till anställd vid Gränspolissektionen i Malmö.

I promemoria i ärendet 5000-K581825-21 omnämns de olika identiteter som förekommit för Atif, och att det är samma person som brukat personnummer 830628- och 19800261-. *PM Angående identiteten på Atif Pervez, 2021-08-30, S Svensson.*



Brukaranalys
An0m-enhet c3b5d4
 Sammanställt av
 Daniel Klein, Analytiker

5000-K654847-21
 2021-12-13
 Region Syd
 Polisområde Södra Skåne

1.6. 2021-05-05 c3b5d4 tilltalas som "Atif"

2021-05-05 benämner en oidentifierad motpart c3b5d4 som "Atif" då det i ett textmeddelande skrivs: *"But Atif do you have any good contacts on weed? Not hash"*.

Time	Sender	Receiver	Text
2021-05-05 23:38:47	sportlisten	c3b5d4	But Atif do you have any good contacts on weed? Not hash
2021-05-05 23:39:01	c3b5d4	sportlisten	Who need it
2021-05-05 23:39:06	sportlisten	c3b5d4	Got a frieend that is big in Malmö he needs a new contact
2021-05-05 23:39:23	c3b5d4	sportlisten	Swedish guy or Arab
2021-05-05 23:39:37	sportlisten	c3b5d4	Swedish

1.7. Resor

2020-07-28 – 2020-08-17 Spanien

Enligt meddelanden på An0m ska brukaren av c3b5d4 åka till Spanien under slutet av juli 2020 och stanna under 2-3 veckor.

2020-07-28 15:13 skriver c3b5d4 att hen är på flygplatsen i Göteborg och ska flyga till Barcelona om ungefär en timme.

Inhämtade uppgifter från PIU visar att 1983-06-28 Rajaatif Pervez hade en plats bokad på flight FR5125 med avgång 2020-07-28 19:30 från Göteborg till Barcelona.

Fredagen 2020-08-14 uttrycker c3b5d4 att hen fortfarande är i Spanien, men har som plan att komma till Sverige på måndag.

Söndagen 2020-08-16 meddelar c3b5d4 att hen kommer till flygplatsen i Göteborg kl. 10 imorgon (2020-08-17).

Måndagen 2020-08-17 12:17 skriver c3b5d4 att han är hemma.

Inhämtade uppgifter från PIU visar att 1983-06-28 Rajaatif Pervez hade en plats bokad på flight från Malaga till Göteborg, med beräknad ankomst till Göteborg 2020-08-17 10:20.

Time	Sender	Receiver	Text
2020-07-26 14:34:32	c3b5d4	dbab0f	I am going to Spain on Tuesday
2020-07-26 17:08:25	dbab0f	c3b5d4	Bro where u will go to marbella ??



Brukaranalys
An0m-enhet c3b5d4
 Sammanställt av
 Daniel Klein, Analytiker

5000-K654847-21

2021-12-13

Region Syd
 Polisområde Södra Skåne

2020-07-26 17:08:34	dbab0f	c3b5d4	U will stay there ??
2020-07-26 17:09:31	c3b5d4	dbab0f	I will stay at hotel bro
2020-07-26 17:09:47	c3b5d4	dbab0f	In marbella
2020-07-26 17:10:02	c3b5d4	dbab0f	I will stay there 2 ,3 weeks
2020-07-26 17:10:33	c3b5d4	dbab0f	Police on me her that's why I wana relax little there

Time	Sender	Receiver	Text
2020-07-28 09:10:17	c3b5d4	aee441	I come to Barcelona today and try to come to Costa tomorrow
2020-07-28 09:15:48	c3b5d4	aee441	I go to airport now bro
2020-07-28 09:16:33	c3b5d4	aee441	Yes I come to Barcelona today
2020-07-28 09:16:48	c3b5d4	aee441	Ok bro
2020-07-28 14:41:59	aee441	c3b5d4	Brate moj have you landed ?
2020-07-28 15:13:04	c3b5d4	aee441	No bro I fly from gothenburg I'm in airport
2020-07-28 15:13:46	c3b5d4	aee441	Fly about one hour

Time	Sender	Receiver	Text
2020-08-14 06:25:03	dbab0f	c3b5d4	Bro you still in sp
2020-08-14 06:25:12	dbab0f	c3b5d4	Ww are coming next week bro
2020-08-14 10:12:57	c3b5d4	dbab0f	I am still her bro I was sick I could not go back to malmo
2020-08-14 10:13:14	c3b5d4	dbab0f	But my plan is going back on Monday
2020-08-14 10:31:32	c3b5d4	aee441	I come back Monday for some paper work in Sweden
2020-08-16 13:24:15	c3b5d4	dbab0f	Ok bro perfect I am also back tomorrow morning 10 o clock gotneborg airport
2020-08-16 13:24:52	c3b5d4	aee441	Yes bro I come gothenburg air port 10 o clock norning
2020-08-17 12:17:21	c3b5d4	aee441	He Brata I am home

2020-11-22 – 2020-11-24 Portugal

I An0m-materialet saknas meddelanden för c3b5d4 under perioden 2021-11-22 – 24. 2021-11-25 får c3b5d4 frågan "How is portugal". C3b5d4 svarar att han är tillbaka i Malmö.

Uppgifter från PIU ger att Rajaatif Pervez 1983-06-28 var bokad på flight med avgång 2020-11-22 16:25 från Arlanda med destination Lissabon, Portugal. Han var vidare bokad 2020-11-23 09:25 från Lissabon till Bilbao, Spanien.



Brukaranalys
An0m-enhet c3b5d4
 Sammanställt av
 Daniel Klein, Analytiker

5000-K654847-21

2021-12-13

Region Syd
 Polisområde Södra Skåne

Uppgifter från PIU ger även att 1983-06-28 Raja Pervez var bokad på flyg med avgång 2020-11-24 15:25 från Lissabon till Amsterdam, och på flyg med avgång 2020-11-24 20:50 från Amsterdam till Göteborg. Ankomst till Göteborg 2020-11-24 22:20.

Time	Sender	Receiver	Text
2020-11-21 21:17	56d3f9	c3b5d4	How are you
2020-11-21 21:17	56d3f9	c3b5d4	I need to talk to you
2020-11-21 21:18	c3b5d4	56d3f9	Fine bro call me

Time	Sender	Receiver	Text
2020-11-25 23:41	c3b5d4	56d3f9	Hej bro
2020-11-25 23:41	56d3f9	c3b5d4	My brother
2020-11-25 23:41	56d3f9	c3b5d4	How is portugal
2020-11-25 23:41	56d3f9	c3b5d4	Maybe we open restaurant there and stop ● the other bizzniz 😊👉
2020-11-25 23:42	c3b5d4	56d3f9	Fine bro lan back in malmo
2020-11-25 23:42	c3b5d4	56d3f9	Hahaha



Brukaranalys
An0m-enhet c3b5d4
 Sammanställt av
 Daniel Klein, Analytiker

5000-K654847-21
 2021-12-13
 Region Syd
 Polisområde Södra Skåne

2021-02-06 – 2021-02-28 Pakistan

I An0m-chatt 2021-02-28 skriver c3b5d4 att hen är på flygplatsen i London och att han fått vänta länge i Turkiet på grund av missad flight.

Inhämtade uppgifter från PIU ger att RAJA PERVEZ 1983-06-28 var bokad på flyg 2021-02-06 från Arlanda till Qatar. 2021-02-07 var samma person bokad för vidare flyg från Qatar till Pakistan (Islamabad).

Uppgifterna ger vidare att samma person var bokad 2021-02-26 på flight från Pakistan (Lahore) till Turkiet (Istanbul) och vidare samma dag med flyg till Göteborg.

Uppgift i ärendet ger att Atif i samband med inresan 2021-02-26 till Landvetter blir avisad och inte får komma in i Sverige. Atif uppvisade i samband med detta ett pakistanskt pass. *PM Angående identiteten på Atif Pervez, 2021-08-30, S Svensson*

Vidare uppgift från PIU ger att Atif dagen efter, 2021-02-27, är bokad på flight från Göteborg tillbaka till Pakistan, via Turkiet. Uppgifter från PIU tyder dock på att passageraren sannolikt inte brukade denna resebokning.

Inhämtade uppgifter från PIU har inte visat på hur Atif kom tillbaka till Sverige.

Time	Sender	Receiver	Text
2021-02-28 17:20:21	c3b5d4	56d3f9	I just get my fone I lose my baggage In airport, I'm in London now bro
2021-02-28 17:22:40	c3b5d4	56d3f9	I am fine bro come yesterday night long flights wait long time in turkey because I miss my flight Friday and then I wait the day after take new one
2021-02-28 17:23:00	c3b5d4	56d3f9	I pick up my baggage 1 hour ago

Utdrag från inhämtade uppgifter från PIU - Raja Atif Pervez 1983-06-28

Passenger Last Name	Passenger First Name	Passenger Middle Name	Passenger Date Of Birth	Flight Airline Code	Flight Code	Flight ETD (Departure)	Flight Origin Airport	Flight ETA (Arrival)	Flight Destination Airport
PERVEZ	RAJAATIF		1983-06-28	FR	5125	2020-07-28 19:30	GOT	2020-07-28 22:35	BCN
PERVEZ	RAJAATIF		1983-06-28	FR	2524	2020-08-17 06:35	AGP	2020-08-17 10:20	GOT
PERVEZ	RAJAATIF		1983-06-28	TP	0789	2020-11-22 16:25	ARN	2020-11-22 19:45	LIS
PERVEZ	RAJAATIF		1983-06-28	TP	1062	2020-11-23 09:25	LIS	2020-11-23 12:35	BIO
PERVEZ	RAJA	ATIF	1983-06-28	KL	1696	2020-11-24 15:25	LIS	2020-11-24 19:35	AMS
PERVEZ	RAJA	ATIF	1983-06-28	KL	1163	2020-11-24 20:50	AMS	2020-11-24 22:20	GOT
PERVEZ	RAJA	ATIF	1983-06-28	KL	1152	2020-12-08 06:00	GOT	2020-12-08 08:20	AMS
PERVEZ	RAJA	ATIF	1983-06-28	KL	1695	2020-12-08 12:35	AMS	2020-12-08 14:35	LIS
PERVEZ	RAJA	ATIF	1983-06-28	QR	0168	2021-02-06 15:25	ARN	2021-02-06 23:35	DOH
PERVEZ	RAJA	ATIF	1983-06-28	QR	0614	2021-02-07 02:40	DOH	2021-02-07 08:00	ISB
PERVEZ	RAJA	ATIF	1983-06-28	TK	0715	2021-02-26 06:40	LHE	2021-02-26 13:05	IST
PERVEZ	RAJA	ATIF	1983-06-28	TK	1799	2021-02-26 14:45	IST	2021-02-26 16:50	GOT
PERVEZ	RAJA	ATIF	1983-06-28	TK	1798	2021-02-27 11:30	GOT	2021-02-27 17:00	IST
PERVEZ	RAJA	ATIF	1983-06-28	TK	0714	2021-02-27 23:45	IST	2021-02-28 07:15	LHE

Bedömning om resebokningar brukats eller ej:

I detta fall bedömer vi att samtliga resebokningar ovan *sannolikt* eller *högst sannolikt* har brukats, förutom:

- 1) KL1152 2020-12-08 i V9RHCJ där koden NO SHOW förekommer (betyder "resenär dök inte upp", se kolumn AI)
- 2) TK1798 2021-02-27 i R4M2RE där incheckningsinformation saknas helt

Redogörelse för begränsningar med PNR-data:

Svenska PIU är anslutna till 36 flygbolag som tillsammans täcker upp till 90 procent av all flygtrafik till/från Sverige.

Det innebär att det finns en risk att personen har rest med något flygbolag som inte är anslutna till PIU.

Under önskad sökperiod hade vi 32 flygbolag anslutna under hela perioden.