Polisen

Protokollbilaga

Åklnr
AM-54003-21

Signerat av
Jörgen Eriksson

Signeringsdatum
2021-10-29 09:30

Arkiv/Åkl. ex

Enhet
Polisregion Bergslagen, Grova brott 1 PO Örebro

Handläggare (Protokollförare)
Jörgen Eriksson

Datum
2021-10-29

Undersökningsledare
Anna Maria Larsson

Polisens diarienummer
5000-K402690-21

Personer i ärendet

Förtursmål	Beslag	Målsägande vill bli underrättad om tidpunkt för huvudförhandlingen
Annat förtursmål	Finns	Nej
Ersättningsyrkanden		**Tolk krävs**
Finns ej		

Misstänkt (Efternamn och förnamn)	Personnummer
Yavuz, Zafer	19880913-0977

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

Underrättelse om utredning enligt RB 23:18a Underrättelsesätt, misstänkt	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
Skriftligt	2021-10-08	2021-10-25	2021-10-28
Försvarare Neo Barsoum Barstedt, förordnad 2021-04-11	2021-10-08	2021-10-25	2021-10-25

Underrättelsesätt, försvarare	Resultat av underrättelse mt	Resultat av underrättelse försv
Skriftligt	Ej erinran	Ej avhörts

Notering

Innehållsförteckning

Diarienr	Uppgiftstyp	Sida
	Information Anom	
5000-K402690-21	Information från krypterad kommunikationstjänst	3
	Om utdrag från ANOM i ärendet	5
	Brukande analys	
	Brukaranalys JID adcf1d	10
	Chattar	
	Om urval av chattar	35
	11 mars, om potentiell lagerhållare	36
	5-8 april, om och med kurir och lagerhållare	43
	Gruppchatt 7 april för kontakt med utl. leverantör	55
	Gruppchatt 7 april, handledning av svensk kurir	65
	Gruppchatt 7 april för, att sammanföra kurirer	75
	9-11 april, om förlust av 90 st tjack i Örebro	83
	11 april, om förlust av 85 st av 120	86
	12 april. Om förlust av 90 "tjack", 35 hann gå ut	88
	5-6 maj, om polisens tillslag av 85 kg	93
	Teknisk information om Operation Trojan Shield	
	Teknisk information om Operation Trojan Shield	98
	Beslut Anom	
	Beslut om överlämnande till AM-54003-21 2021-06-22	152
	Beslut om överlämnande till AM-54003-21 2021-06-22	153
	Personalia	
	Bilaga skäligen misstänkt, Yavuz, Zafer	154
	Personalia, Yavuz, Zafer	155

Polisen

PM

Datum
2021-06-08

Diarienr (åberopas)

Polismyndigheten
Nationella operativa avdelningen

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.

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.

Polisen

Utdrag från ANØM

Polisregion Bergslagen

2021-10-04

Polisen

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

För de flesta ANOM-användare fanns det inga andra sätt att kommunicera på enheterna än krypterat med andra ANOM enheter.

Funktioner på mobiltelefoner, som t.ex. röst- eller videosamtal, SMS, appar för sociala medier, internet-surf och e-posttjänster, kunde inte användas. Den 8 juni 2021 var det bara 73 av ungefär 12 500 enheter som hade tilldelats special-förmågan att ringa i traditionell bemärkelse eller att surfa på internet via den installerade ToR-webbläsaren.

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

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

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

Viss information som t.ex. bilder och anteckningar kunde sparas i ett lagringsut-rymme kallat ”vault” i sin fysiska enheten.

Kommunikation skedde i chattar med annan ANOM enhet eller i skapade gruppchattar där flera ANOM enheter bjudits in att delta. För att särskilja olika gruppchattar tilldelades de automatiskt ett individuellt Grupp ID ”GID” i syste-met. Det namn som respektive gruppchat eventuellt döpts till syns inte i erhållet material.

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

Polisen

Om utdrag av chattar i ärendet
Det inhämtade ANOM materialet i detta ärende är omfattande. Det finns ca 300 000 skickade meddelanden. Ett urval har gjorts för att begränsa materialet till det som bedömts vara relevant för brottet som utreds.

Innehåll från ANOM kan, likt innehåll från en sedvanlig mobiltelefon, visualiseras på olika sätt. I detta fall presenteras kommunikationen med pratbubblor där varje JID har en egen färg. Det kan även visualiseras i exempelvis Excel-format.

Om försättsblad i presentationen
Ett försättsblad har gjorts av polis för att markera när ett nytt utdrag av chatt presenteras och för att förtydliga vad som omfattas i urvalet.

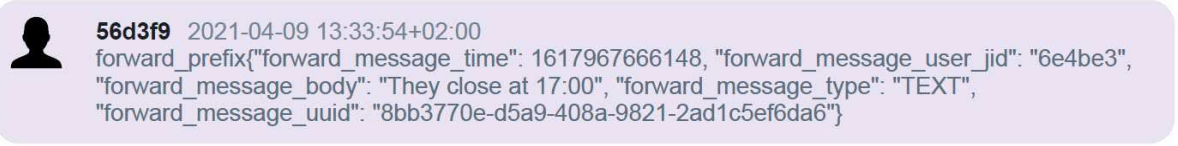
Försättsbladet visar**:**

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

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

Ex. skickat text meddelande:

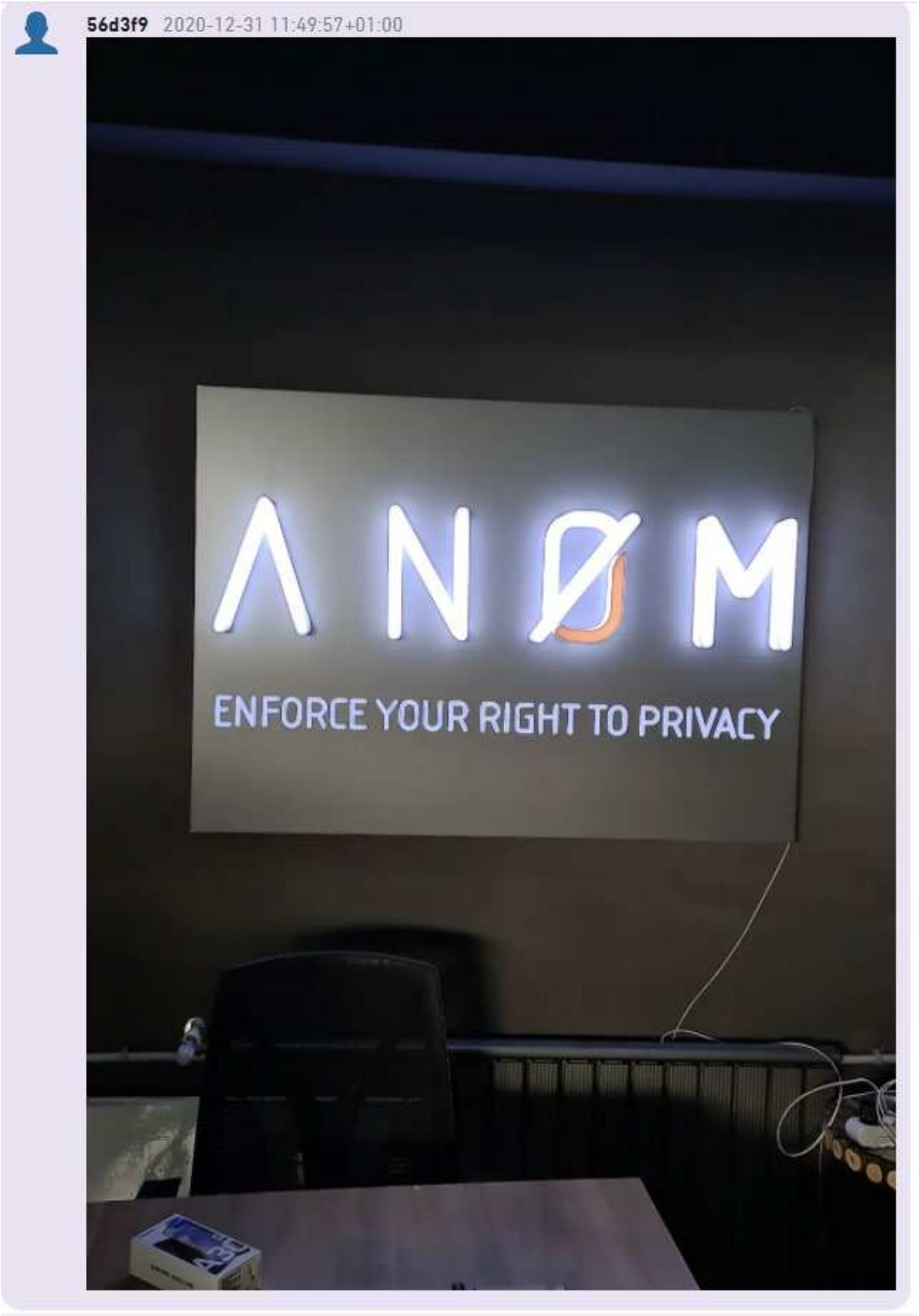
Ex. vidarebefordrat meddelande:



Ex. citerat meddelande:

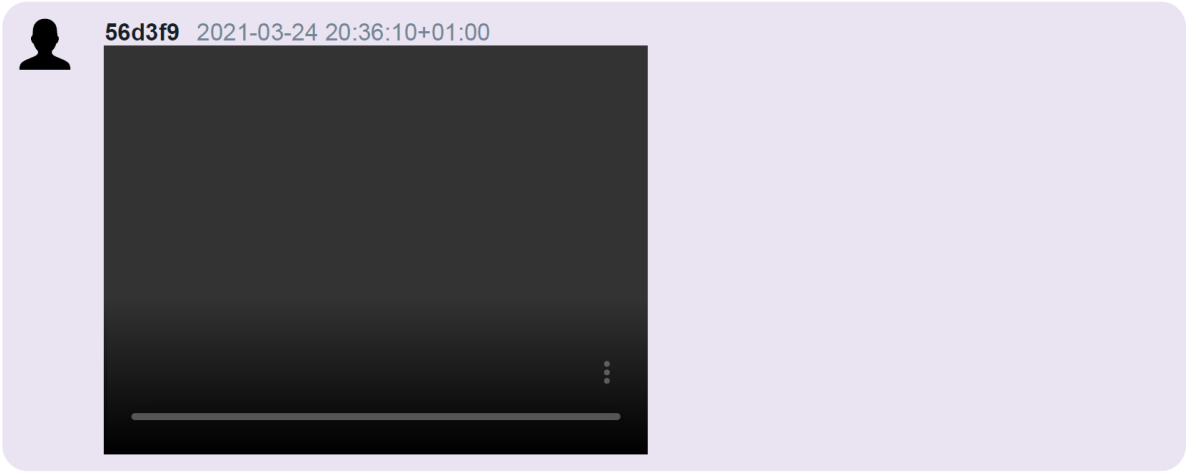
Polisen

Ex. skickad bild:

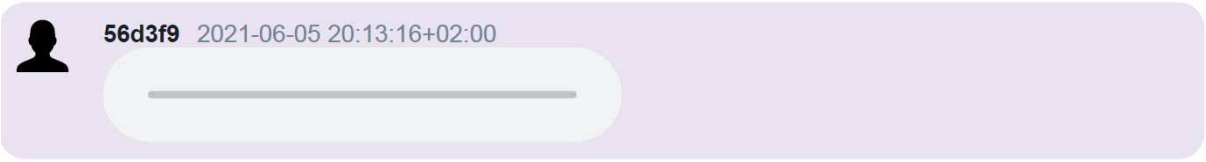


Polisen

Ex. skickad video:



Ex. skickad ljudfil:



Polisen

Brukaranalys JID adcf1d

Signerat av

Signerat datum

Enhet	Diarienr
Polisregion Bergslagen, Grova brott 1 PO Örebro	5000-K402690-21

Orginalhandlingens förvaringsplats	Datum	Tid
	2021-10-07	09:45

Involverad personal	Funktion
Madelene Malkani	Uppgiftslämnare

Berättelse

Brukaranalys av JID adcf1d.

Brukaranalys

adcf1d

PO Örebro, Utredningssektionen, Grova Brott

Operativ Analytiker Madelene Malkani

2021-10-05

PO Örebro, Utredningssektionen, Grova Brott.

Innehåll

1 Inledning 3

1.1 Syfte 3

1.2 Metod och data 3

2 Misstänkt Zafer Yavuz 4

2.1 Adress och Relationer 4

2.1 Telefon 4

3 Brukaranalys 6

3.1 2021-03-11 6

3.2 2021-04-06 7

3.3 2021-04-07 8

3.1 2021-04-11 21

3.2 2021-05-05 22

3.3 Telefonnummer 46761384095 23

4 Slutsats 23

1 Inledning

Operation Trojan Shield var en internationell polisoperation som pågick fram till 7 juni 2021. Operationen startade 2018 då amerikanska FBI utvecklade den krypterade plattformen ANOM. Plattformen marknadsfördes mot kriminella nätverk och organisationer som ett nytt kommunikationssystem som omöjligt att dekryptera av rättsväsendet. Ett stort antal kriminella individer anammade den krypterade plattformen och använde denna för kommunikation sinsemellan för att kunna utför brottslighet. Flera insatser mot brott kunde utföras av rättsväsendet baserat på underrättelser från plattformen. I samband med att operationen avslutades, den 7 juni, greps mer än 800 personer i 16 olika länder i världen och material från plattformen tilldelades flera förundersökningar i Sverige.

Utifrån informationen från den krypterade plattformen ANOM har det framkommit uppgifter om att JID **adcf1d** brukats den 7 april 2021 i samband med att narkotika hämtats på en adress i Årsta för att sedan påträffats i Zafer Yavuzs lägenhet på Engelbrektsgatan 52 i Örebro.

1.1 Syfte

Syftet med denna analys är att undersöka vilken fysisk person som den 7 april 2021 brukade JID **adcf1d**.

1.2 Metod och data

I brukaranalysen har material använts som delgivits förundersökningen från den krypterade kommunikationsplattformen Anom, vars information tilldelats svensk polis. Information från JID **adcf1d** har gåtts igenom för perioden 2021-03-11 till 2021-05-06. Materialet presenteras nedan i form av chattmeddelande och bilder i en kronologisk tidslinje.

Övriga data som används i analysen är:

- Telefonextrahering 2021-5000-BG44022-1tillhörande Zafer Yavuz.
- Förhör.
- Information från polisens interna system PMF(Polisens multifråga), PIL(Polisens informationslösning) samt VTR (Vägtrafikregistret)

2 Misstänkt Zafer Yavuz

2.1 Adress och Relationer

Namn: Zafer Yavuz

Personnummer: 1988-09-13–0977

Folkbokföringsadress: Engelbrektsgatan 52, 70213 Örebro[1]

Fordon: Inga fordon registrerade.[2]

Arbetsplats: Underleverantör Cap Gemini Sverige AB till EON. Arbete som mätvädersoperatör[3][4]

2.1 Telefon

Telefontyp: Okänd

IMEI: *

JID nr: adcf1d

Användarnamn: Havana

Brukarperiod: 7 april 2021

[1] PMF 2021-09-16
[2] VTR Vägtrafikregistret 2021-10-05.
[3] Förhör Zafer Yavuz 2021-04-23, Förhörsledare J. Eriksson
[4] Registerurdrag från Skatteverket 2021-09-17

PO Örebro, Utredningssektionen, Grova Brott.

(2021-04-19) [5]

[5] Foton från daktning från 2021-04-19

PO Örebro, Utredningssektionen, Grova Brott.

3 Brukaranalys

3.1 2021-03-11

Chattkonversation mellan JID whateven och **adcf1d** där en person beskrivs som jobbar inom elverket och bor mitt i ”stan”.[6] Troligen är det en person som beskrivs som ska hjälpa till att lagerhålla något och vara undercover person. Zafer Yavuz bor på Engelbrektsgatan 52 som man kan påstå ligger centralt i Örebro.[7] Zafer Yavuz arbetar hos en underleverantör till EON.[8]

[6] Protokollbilaga Chat 11 mars om potentiell lagerhållare.
[7] Information från PIL 2021-10-01
[8] Förhör Zafer Yavuz 2021-04-23, Förhörsledare J. Eriksson

3.2 2021-04-06

JID whateven skickar chattmeddelande till **adcf1d** att **adcf1d** ska ge ”dom” **adef1d**:s anom telefon.[9] Troligen är det en annan person som ska låna telefonen av nuvarande brukare.

Chattkonversation mellan JID whateven och **adcf1d**. **Adcf1d** skriver att **adcf1d** ska lämna över telefonen till sin vän nu.[10]

[9]Protokollbilaga, chatt 5-8 april, om och med kurir och lagerhållare.
[10]Protokollbilaga, chatt 5-8 april, om och med kurir och lagerhållare.

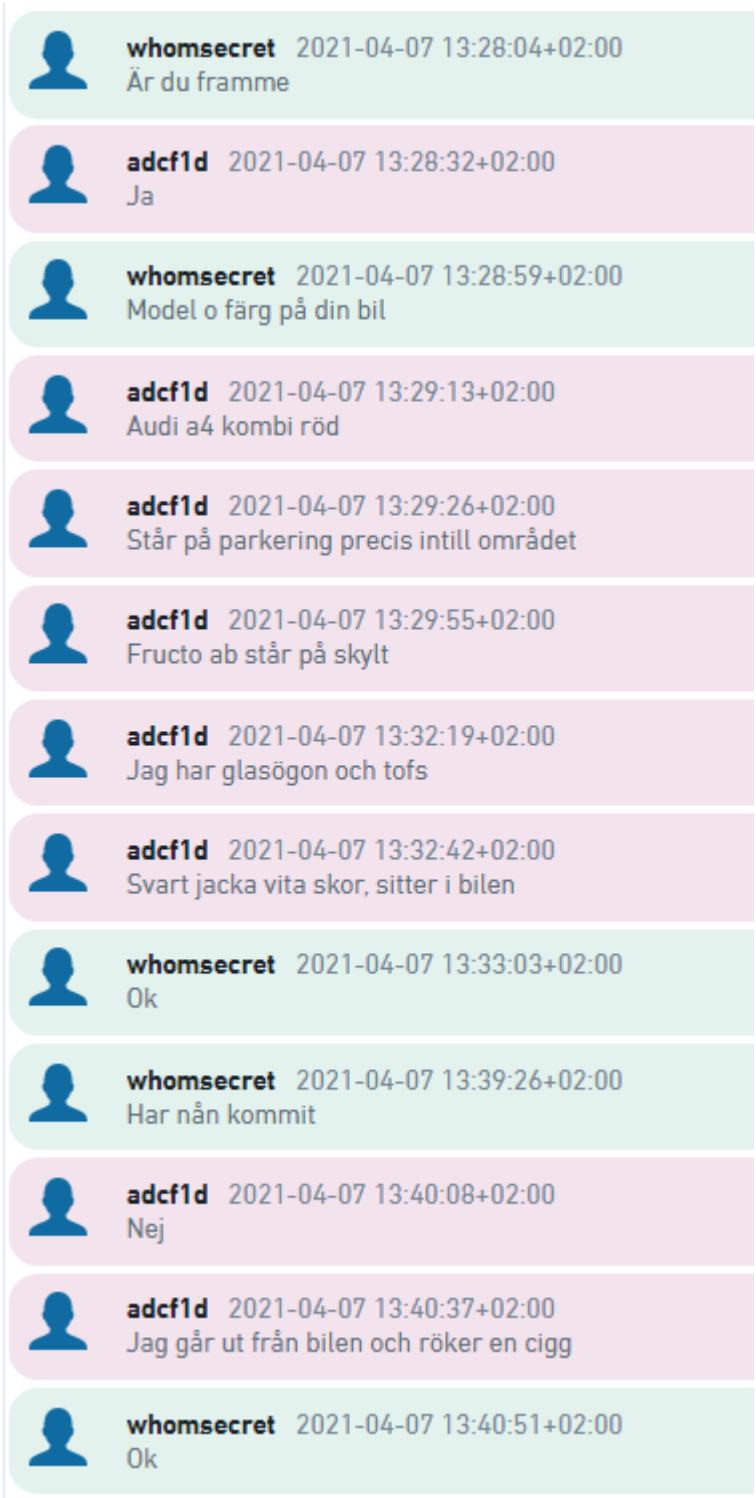
3.3 2021-04-07

Chattkonversation mellan JID whomsecret och **adcf1d**. **Adcf1d** uppger i konversationen att **adcf1d** har en röd Audi kombi.[11] Zafer Yavuz bror har en röd audi kombi som Zafer Yavuz brukar använda.[12][13]

[11] Protokollbilaga, Gruppchatt 7 april, handledning av svensk kurir
[12] Förhör Zafer Yavuz 2021-04-23, Förhörsledare J. Eriksson
[13] Information från VTR 2021-10-07

PO Örebro, Utredningssektionen, Grova Brott.

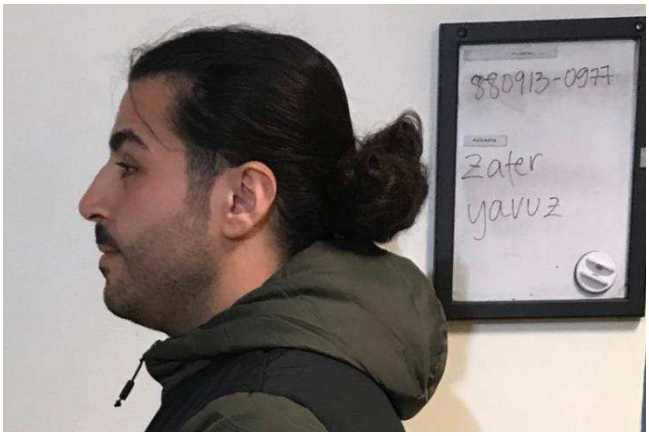
Chattkonversation nedan mellan JID whomsecret och **adcf1d**. Whomsecret vill ha **adcf1d**:s modell och färg på bilen som körs. **Adcd1d** uppger åter att **adcd1d** kör en röd Audi A4. Zafer Yavuz bror äger en röd Audi A4 som Zafer Yavuz uppger i förhör att han brukar använda.[14][15]



[14] Protokollbilaga, Gruppchatt 7 april, handledning av svensk kurir
[15] Förhör Zafer Yavuz 2021-04-23, Förhörsledare J. Eriksson

PO Örebro, Utredningssektionen, Grova Brott.

Brukaren av JID **adcf1d** beskriver sig också i ovan chattkonversationen ha glasögon, tofs, svart jacka och vita skor.[16] Bild nedan är tagen på Zafer Yavuz i arresten i Örebro 2021-04-10.[17] På bilden som togs vid gripandet har han en hårtofs vilket skulle kunna stämma överens med beskrivning av brukaren til JID **adcf1d** 2021-04-07.



[18]

Från telefonextraheringen 2020-5000-BG44022-1 tillhörande Zafer Yavuz finns en bild nedan att Zafer Yavuz använder glasögon när han kör bil. [19] I chattmeddelandet från JID **adcf1d** bekrivs att brukaren vid tillfället har glasögon.[20]

[16] Protokollbilaga, Gruppchatt 7 april, handledning av svensk kurir
[17] Gripandefoto 2021-04-10.
[18] Gripandefoto 2021-04-10.
[19] Undersökningsprotokoll Apple Iphone 8, 2020-5000-BG44022-1
[20] Protokollbilaga, Gruppchatt 7 april, handledning av svensk kurir

PO Örebro, Utredningssektionen, Grova Brott.

Chattkonversation mellan JID **adcf1d** och whomsecret. **Adcf1d** beskriver vart **adcf1d** parkerat. Whomsecret vill ha en bild på parkeringen.[21]

[21] Protokollbilaga, Gruppchatt 7 april, handledning av svensk kurir

Bild skickas från JID **adcf1d** klockan 14:06:14 på den bil som troligen brukare av **adcf1d** använder och var den parkerats. Bilden är på en röd audi registreringsnummer CLJ 189, registrerad på Zafer Yavuz bror Ramazan Yavuz.[22]

Personbil med registreringsnummer CLJ189 är också den personbil som Zafer Yavuz greps vid 2021-04-10 och som ägs av hans bror Ramazan Yavuz.[23]

[22] Information från VTR 2021-09-29
[23] PM Stopp och kontroll Zafer Yavuz 2021-04-10, M Boije

Bild skickas från JID **adcf1d** klockan 14:08. Bilden är med största sannolikhet tagen innifrån förarplatsen i en röd bil.[24] Med största sannolikhet är det brukare av **adcf1d** som sitter i bilen som tar fotot.

[24] Protokollbilaga, Gruppchatt 7 april, handledning av svensk kurir

PO Örebro, Utredningssektionen, Grova Brott.

Chattmeddelande mellan JID whomsecret och **adcf1d** där whomsecret vill ha en bättre bild över parkeringen.[25]

JID **Adcf1d** svarar ok och skickar därefter en bild.

Bild skickas från JID **adcf1d** 2021-04-07 klockan 14:08.[26] Bilden föreställer en mindre parkering utanför troligen företagslokaler samt att man kan urskilja en röd bil.

[25] Protokollbilaga, Gruppchatt 7 april, handledning av svensk kurir
[26] Protokollbilaga, Gruppchatt 7 april, handledning av svensk kurir

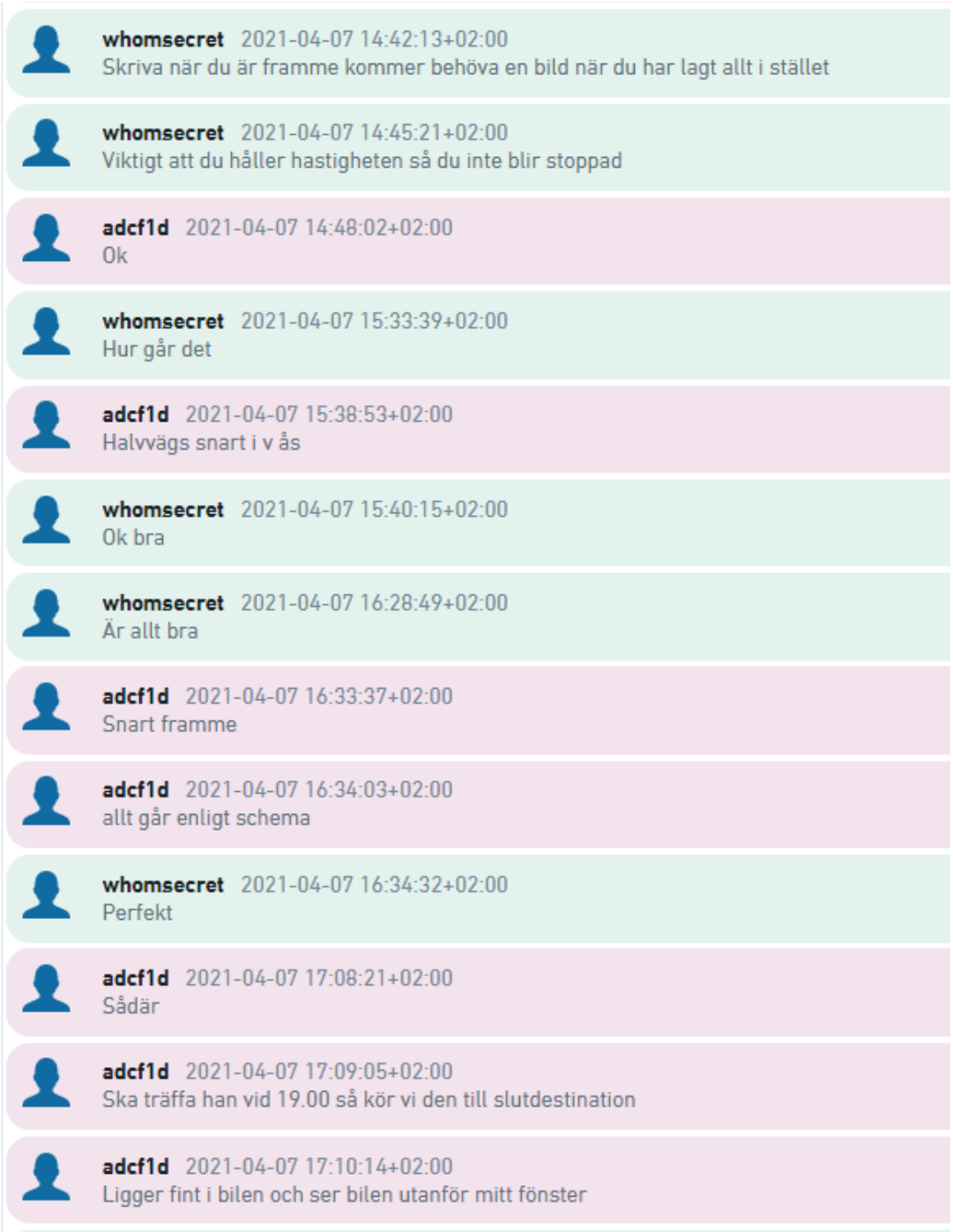
PO Örebro, Utredningssektionen, Grova Brott.

Chattkonversation nedan mellan JID **adcf1d** och whomsecret kan bekräfta att det är **adcf1d**:s bil som är parkerad till höger och att **adcf1d** som troligen sitter i bilen och väntar.[27]

[27] Protokollbilaga, Gruppchatt 7 april, handledning av svensk kurir

PO Örebro, Utredningssektionen, Grova Brott.

Chattkonversation mellan whomsecret och JID **adcf1d** där det beskrivs hur **adcf1d** uppmanas att skicka bild när **adcf1**d är framme och allt lagt i ”stället”. [28] Adcf1d skriver att adcf1d är snart i v ås som troligen menas Västerås. Västerås ligger på halva sträckan mellan Stockholm och Örebro.



[28] Protokollbilaga, Gruppchatt 7 april, handledning av svensk kurir

PO Örebro, Utredningssektionen, Grova Brott.

Chattkonversationen mellan JID whateven och **adcf1d.** Whateven uppmanar adcf1d att räkna och ta bild.[29]

[29] Protokollbilaga, Chatt 5-8 april, om och med kurir och lagerhållare.

PO Örebro, Utredningssektionen, Grova Brott.

Chattmeddelande skickas från JID **adcf1d** om att de va två stora bags o en stor icakasse och två tunga kartonger.[30]

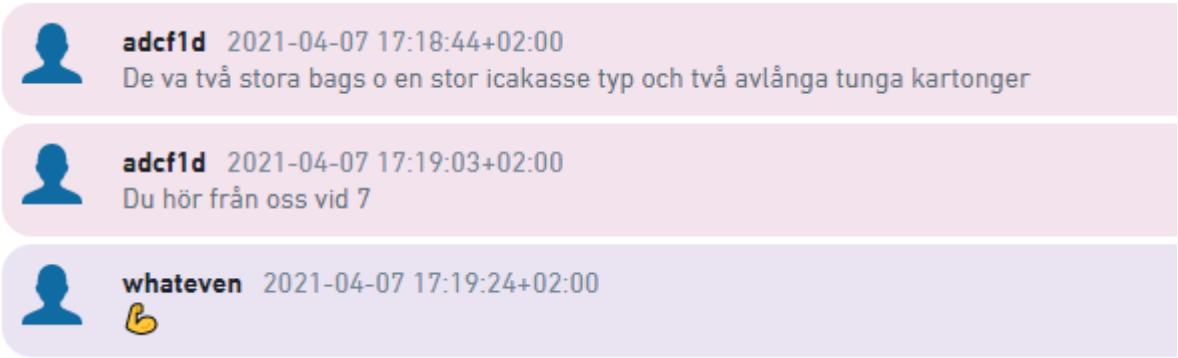


Bild skickas från JID **adcf1d** nedan från uppmaning av whateven i tidigare chattkonversation. 2021-04-07 19:43:50. [31] På bilden kan man se narkotika med brunt mönster på samt en grön heltäckningsmatta i bakgrunden. Även en stålstång med skruv synd i bakgrunden i högra hörnet.

[30] Protokollbilaga, Chatt 5-8 april, om och med kurir och lagerhållare.
[31] Protokollbilaga, Chatt 5-8 april, om och med kurir och lagerhållare.

PO Örebro, Utredningssektionen, Grova Brott.

Bild nedan är från tekniska rotel på Polisen. Bilden är på narkotikan som beslagstogs på Engelsbrektsgatan 25B.[32]

Den högra amfetaminkakan på bilden ovan överensstämmer bra med den bild som JID **adcf1d** skickar i chattmeddelande med det bruna kaffemönstret 2021-04-07 19:43:50. Nedan visas en jämförelse mellan amfetaminkakorna från de två bilderna.

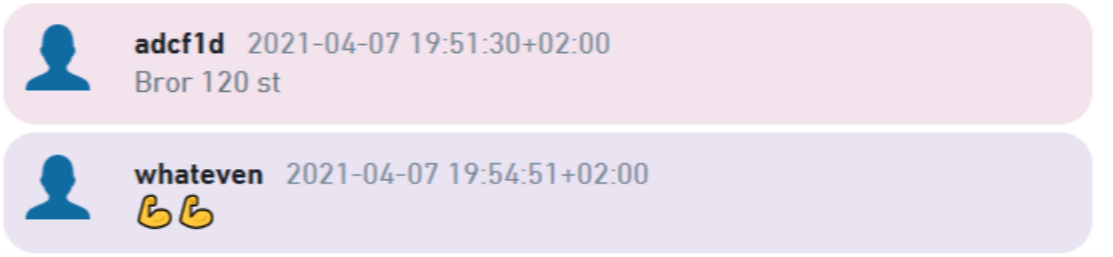
[32] Fotografier av tekniska roteln av narkotikabeslag, 2021-09-24

Bild nedan är från brottplatsundersökningen 2021-04-10 från lägenheten på Engelbrektsgatan 25B.[33]

Den gröna heltäckningsmattan som finns i bakgrunden på bilden som JID **adcf1d** skickar 2021-04-07 19:43:50 stämmer bra överens med heltäckningsmatta från husrannsakan 2021-04-10 från Engelbrektsgatan 25B. Man kan även se den grå stålstång (röd ruta) som är ett skoställ som finns med på tidigare bild som JID **adcf1d** skickar 2021-04-07 19:43:50.

[33] Fotografier över bostaden, initiala husrannsakan 2021-04-12

Chattkonversation mellan JID **adcf1d** och whateven. **Adcf1d** verkar ha räknat narkotikan och fått det till 120 stycken, troligen 120 paket.[34] **Adcf1d** har uppmanats i tidigare chattkonversation att räkna när **adcf1d** kommit fram.



3.1 2021-04-11

Vid tillslaget 2021-04-10 hittas ca 85kg amfetamin hemma hos Zafer Yavuz.[35] I chattkonversation mellan JID whateven och 7b7ef3 kan man ev styrka att 35 kg av partiet på 120kg har delats ut.[36]

[34] Protokollbilaga, Chatt 5-8 april, om och med kurir och lagerhållare.
[35] NFC analys av narkotika
[36] Protokolbilaga Chatt 9-11 april, om förlust av 90 st tjack i Örebro

PO Örebro, Utredningssektionen, Grova Brott.

3.2 2021-05-05

Chattkonversation mellan JID 225375 och JID whateven där man frågar efter namnet på ”han som ramla i örebro”.

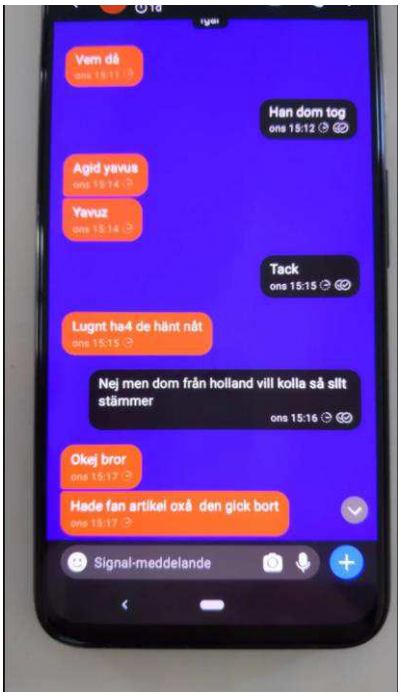
225375 2021-05-05 12:42:19+02:00
Har gurkan namnet på han som ramla i örebro ?

225375 2021-05-05 12:42:50+02:00
Vill ta ut häktning visa till min vän

whateven 2021-05-05 12:45:35+02:00
Nej
Han vet inte vem det är
Det var mina killar

whateven 2021-05-05 12:45:54+02:00
Jag väntar namn

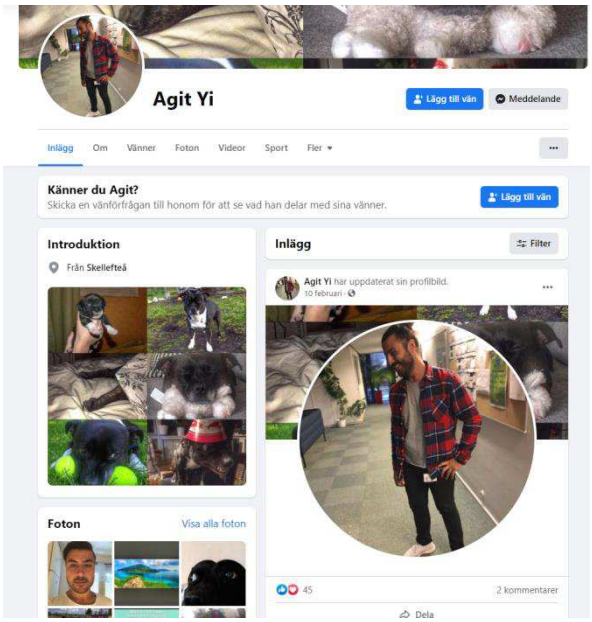
Bild skickas dagen efter från JID whateven 2021-05-06 klockan 9:29:09. [37]Bilden föreställer ett fotografi på en chattkonversation från en telefon angående en Agid Yavus som skulle vara ”han som dom tog”. Troligen menas den person som Polisen gripit 2021-04-10.[38]



[37] Protokollbilaga Chatt 5-6 maj, om polisens tillslag av 85 kg
[38] Gripande 2021-04-10.

PO Örebro, Utredningssektionen, Grova Brott.

Zafer Yavuz kallar sig Agit på facebook[39] och har även Agit tatuerat på ena armen[40].



3.3 Telefonnummer 46761384095

Från analys av samtalslista för nummer 46761384095 brukare Zafer Yavuz kan man se ett inkommande samtal klockan 10:27 till 46761384095 från Bravida Sverige som pågår i 1:54 minuter. Nästa inkommande samtal är 17:01från 46762728205 Robin Yavuz som varar i 37 sekunder. Mellan dessa tider finns inga utgående eller inkommande samtal eller sms.[41]

4 Slutsats

Mot bakgrund av ovanstående uppgifter är slutsatsen att Zafer Yavuz är med största sannolikhet brukare av JID **adcf1d** 2021-04-07. Beskrivningen av den person som använder **adcf1d** för denna tidpunkt överensstämmer mycket bra med Zafer Yavuz då han har tofs, bär

[39] Information från facebook 2021-10-01
[40] Foton från daktning, 2021-04-19
[41] Analys samtalslista 2021-04-07 Zafer Yavuz, J Pegers.

glasögon, jobbar hos en underleverantör till ett elverk och bor i centrala delarna i Örebro. Zafer Yavuz använder sin brors bil, röd Audi som finns med på ett flertal bilder i materialet och som han också grips vid. Zafer Yavuz har ca 85 kg amfetamin i sin lägenhet vid gripandet 2021-04-10. 6 april 2021 skriver ordinarie brukaren för JID **adcf1d** att telefon kommer lämnas över till en vän. Efter gripandet spekuleras om vem den gripne var och namnet Agit framkommer. Namnet Agit är tatuerat på Zafer Yavuz arm och han har även det namnet på facebook.

Från Zafers Yavuz samtalslista kan man också se att det finns ett glapp på samtal och sms mellan klockan runt 10:27 till 17:01. Troligen används istället JID **adcf1d** under denna tid att kommunicera med.

Polisen

Om urval av chattar

I erhållet material från ANOM finns kommunikation som rör narkotikhandel i stor omfattning. Det finns chattar som berör allt från beställning, införsel, logistik och försäljning av amfetamin.

Följande konversationer bedöms handla om mottagande, transport och förvar i Sverige av det parti på 120 kg amfetamin som utreds i ärendet.

- 11 Mars, om potentiell lagerhållare
- 5-8 april, om och under en period med, inhemsk kuir /lagerhållare i sverige den (chat mellan JID adcf1d och whateven)
- 7 april med utländsk leverantör för att få information om insmuggling och transportörs position. (GID gon2aiomoroi6)
- 7 april med inhemsk mottagare/kurir för att få information om position och ge direktiv om överlämnande. (GID 5v4lmf1glxxw2)
- 7 april för att smmanföra utländsk smugglare/kurir med inhemsk kurir/lagerhållare. (GID 3fmvnxnzesuutS)
- 9-11 april. Om förlust av 90 st ”tjack” i Örebro och att man han dela ut 35 (chat mellan whateven och 7b7ef3)
- 11 april kl 16:08 till 16:10. Förlust av 85st av ursprunglinga 120 nämns i diskussion (chat mellan whomsecret och 4f3887)
- 12 april. Om förlust av 90 ”tjack” som legat i lager i tre dagar. 35 hann delas ut innan . (chat mellan whateven och buslost)
- 5-6 maj. Diskussion om polisens tillslag av 85 kilo amfetamin. (chat mellan whateven och 225375)

Polisen

Chat

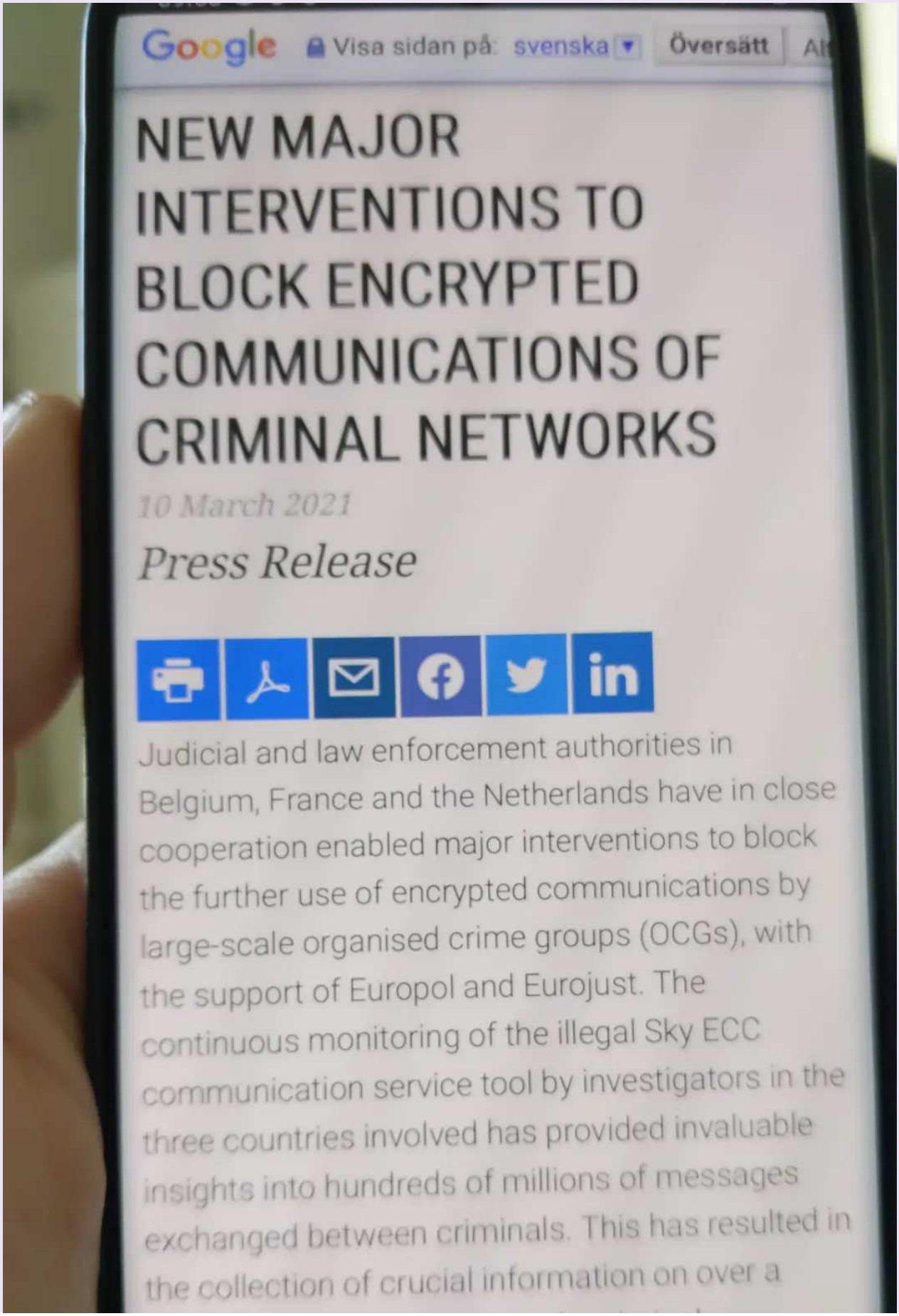
2020-03-11

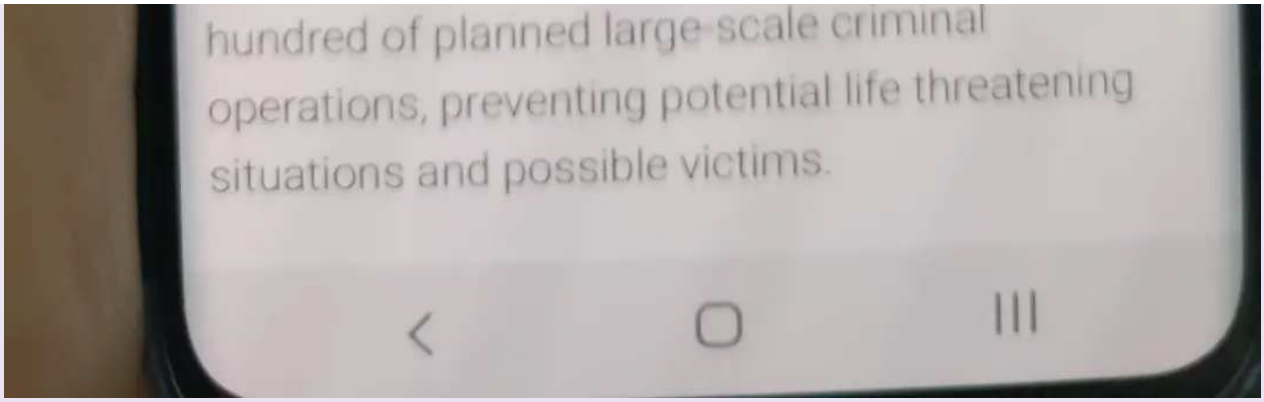
JID	Alias	Användare enligt brukaranalys
whateven	worldwide	?
adcf1d	havana	?

Showing all 19 messages.

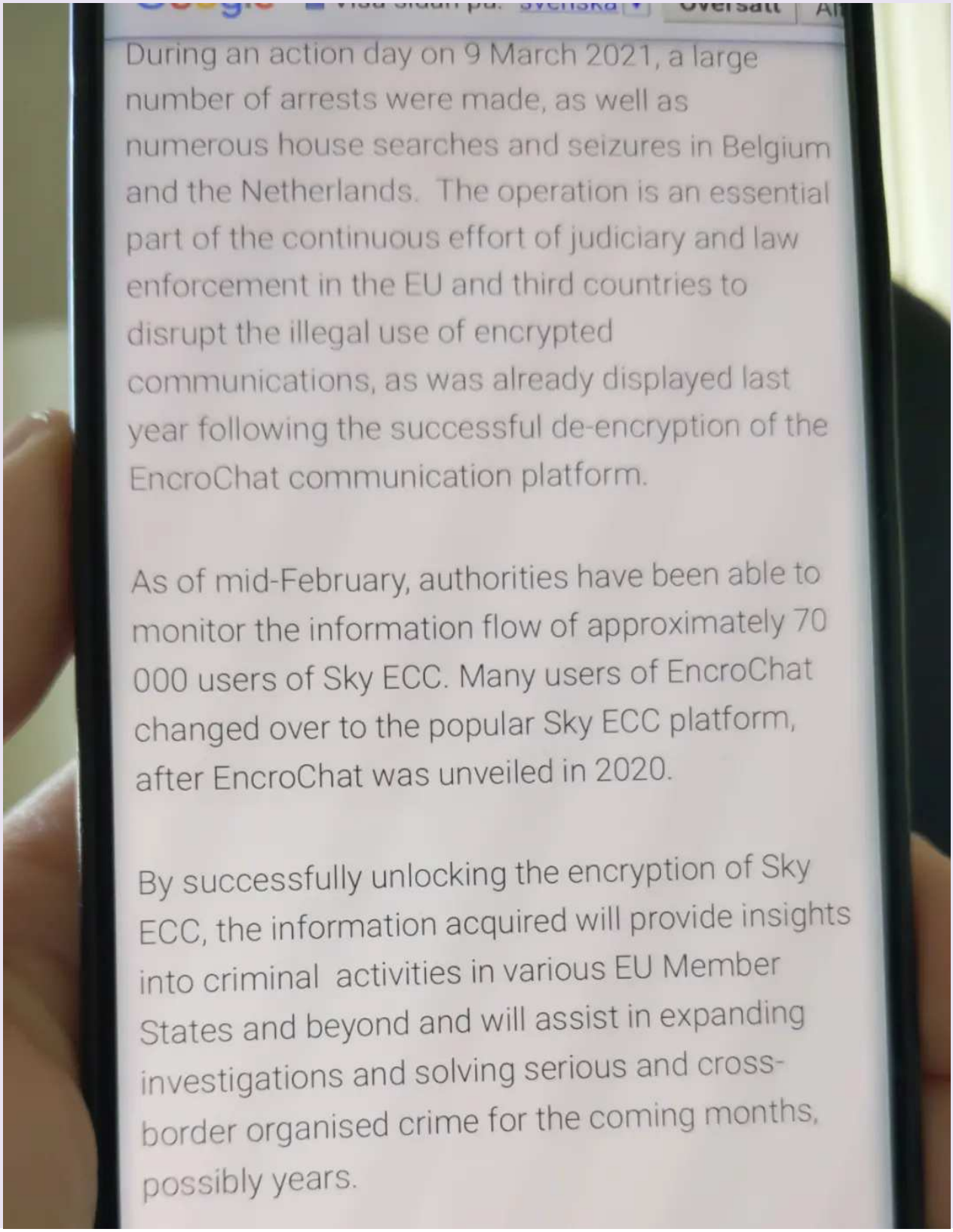
Thread 54_266747

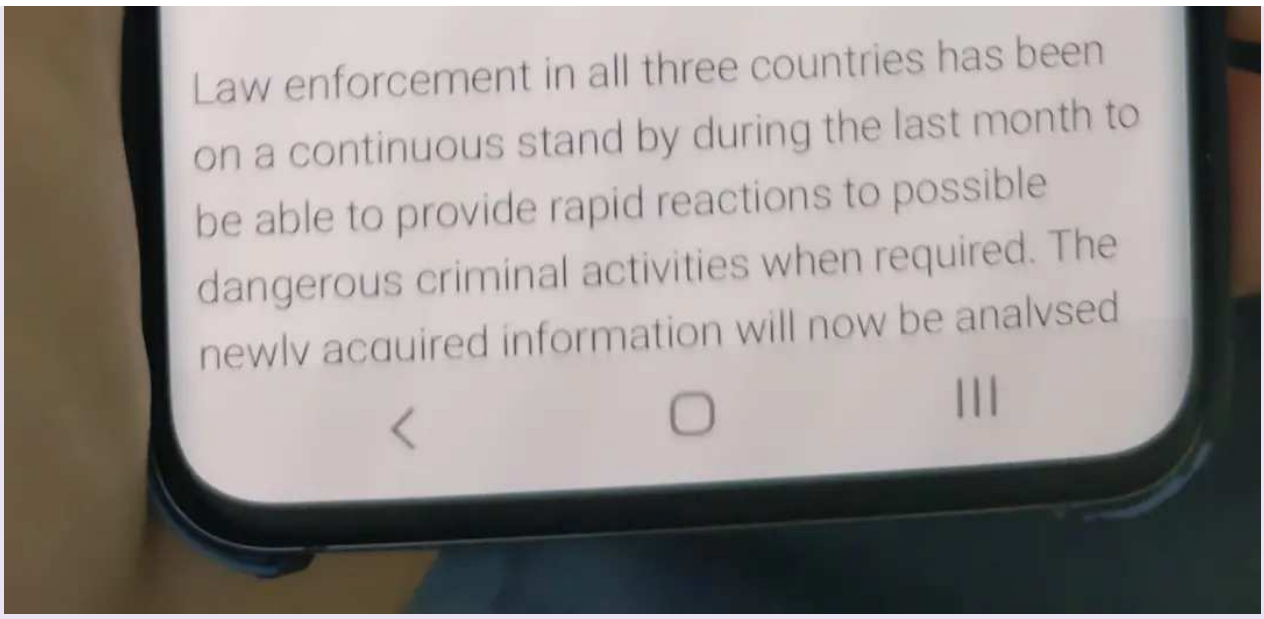
whateven 2021-03-11 10:00:36+01:00



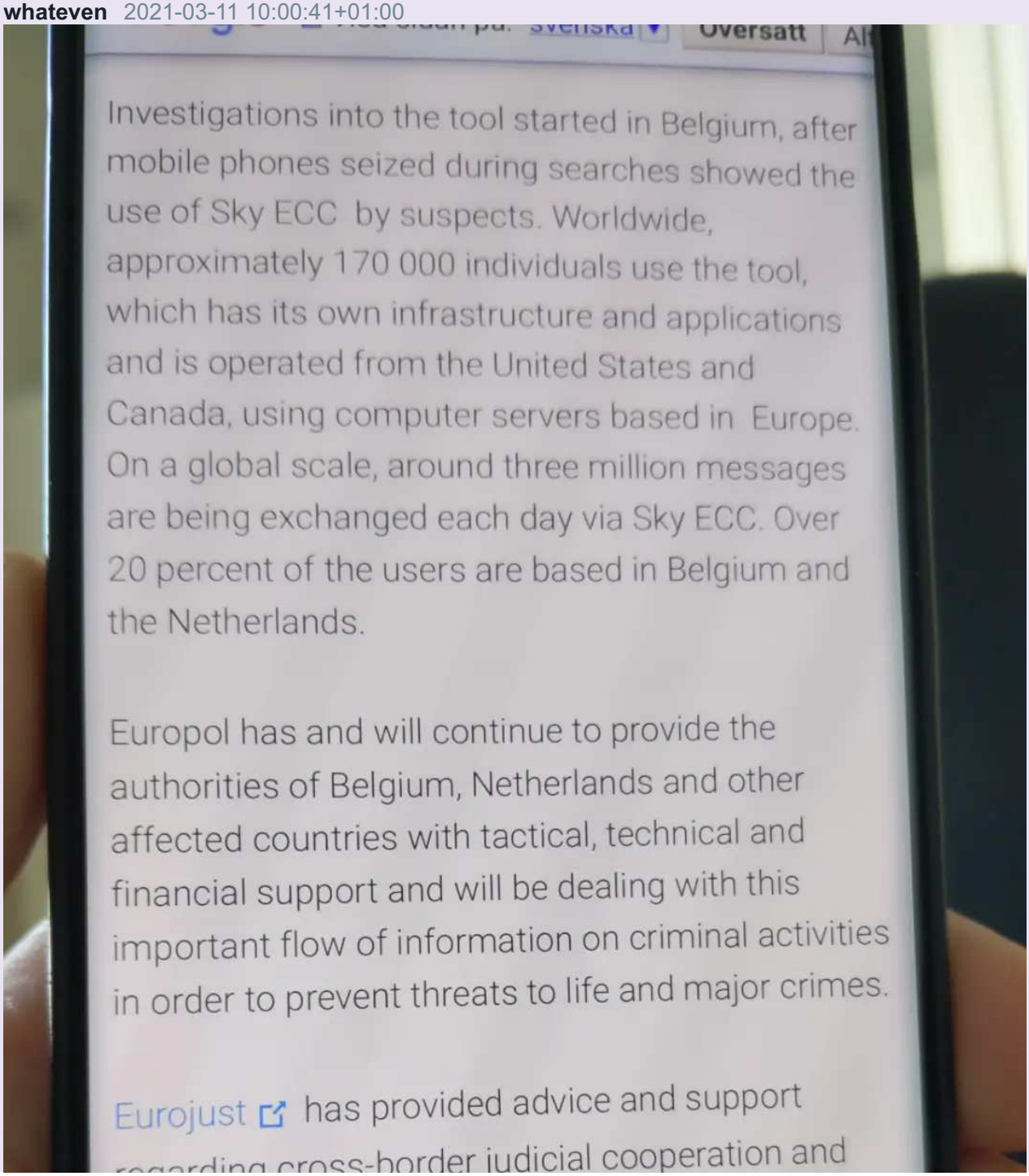


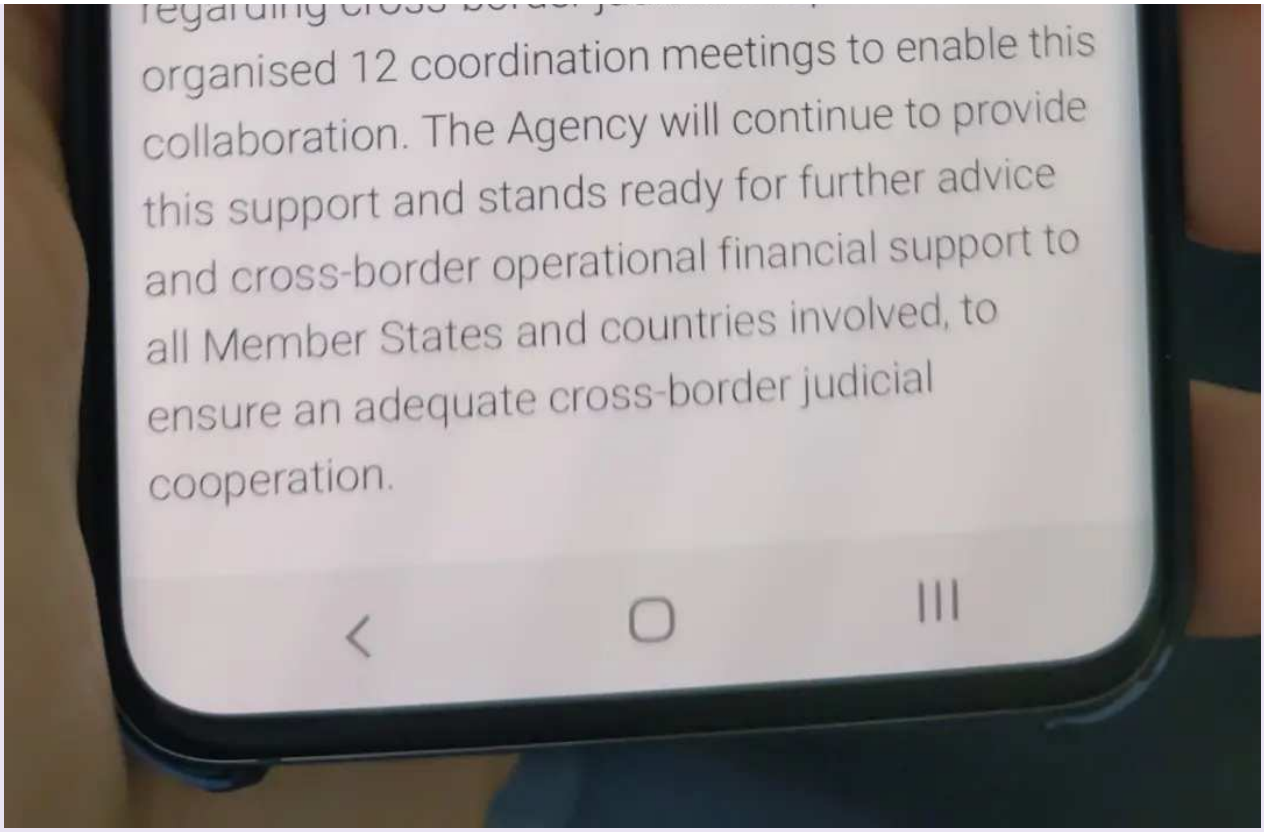
whateven 2021-03-11 10:00:38+01:00



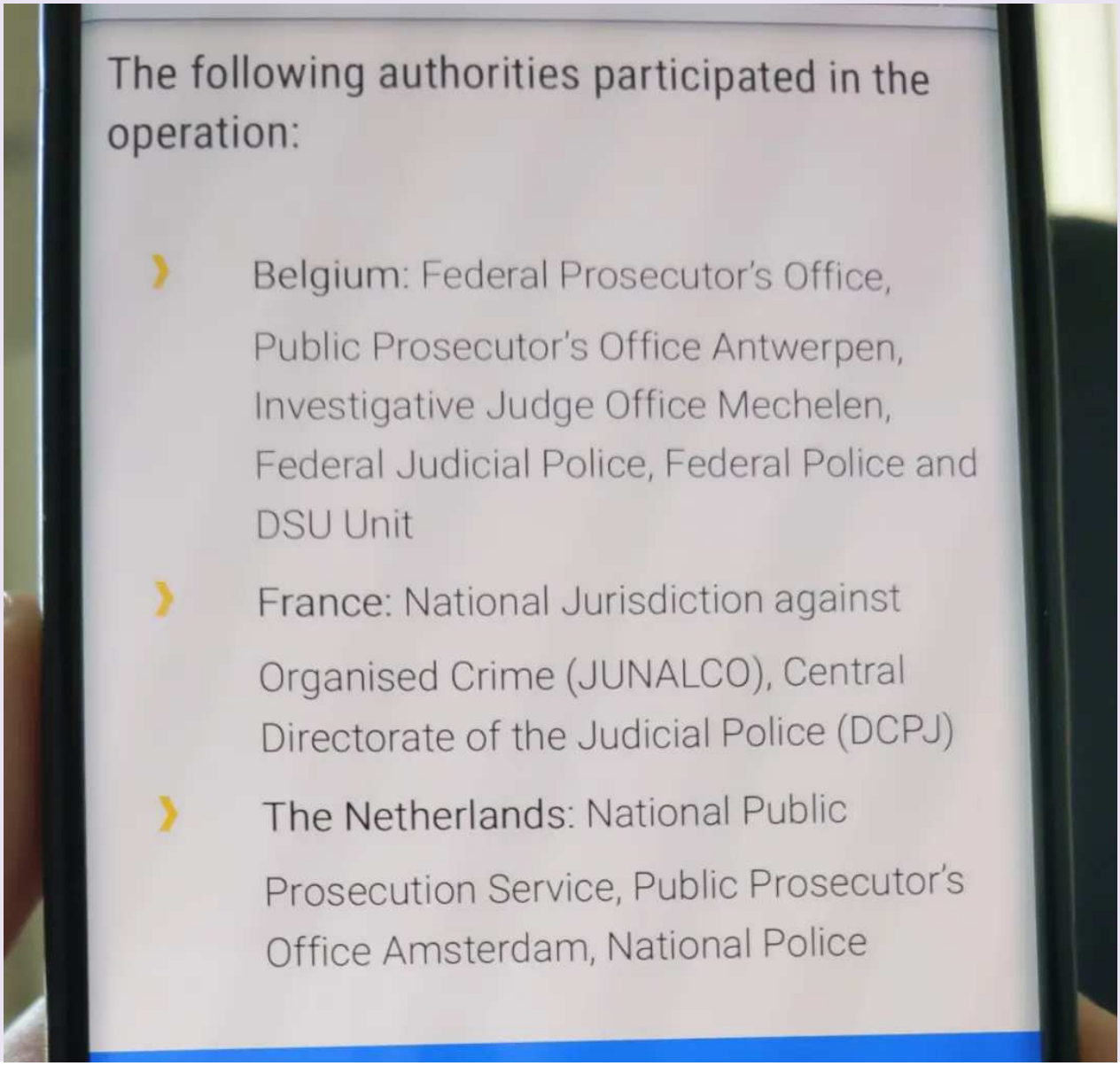


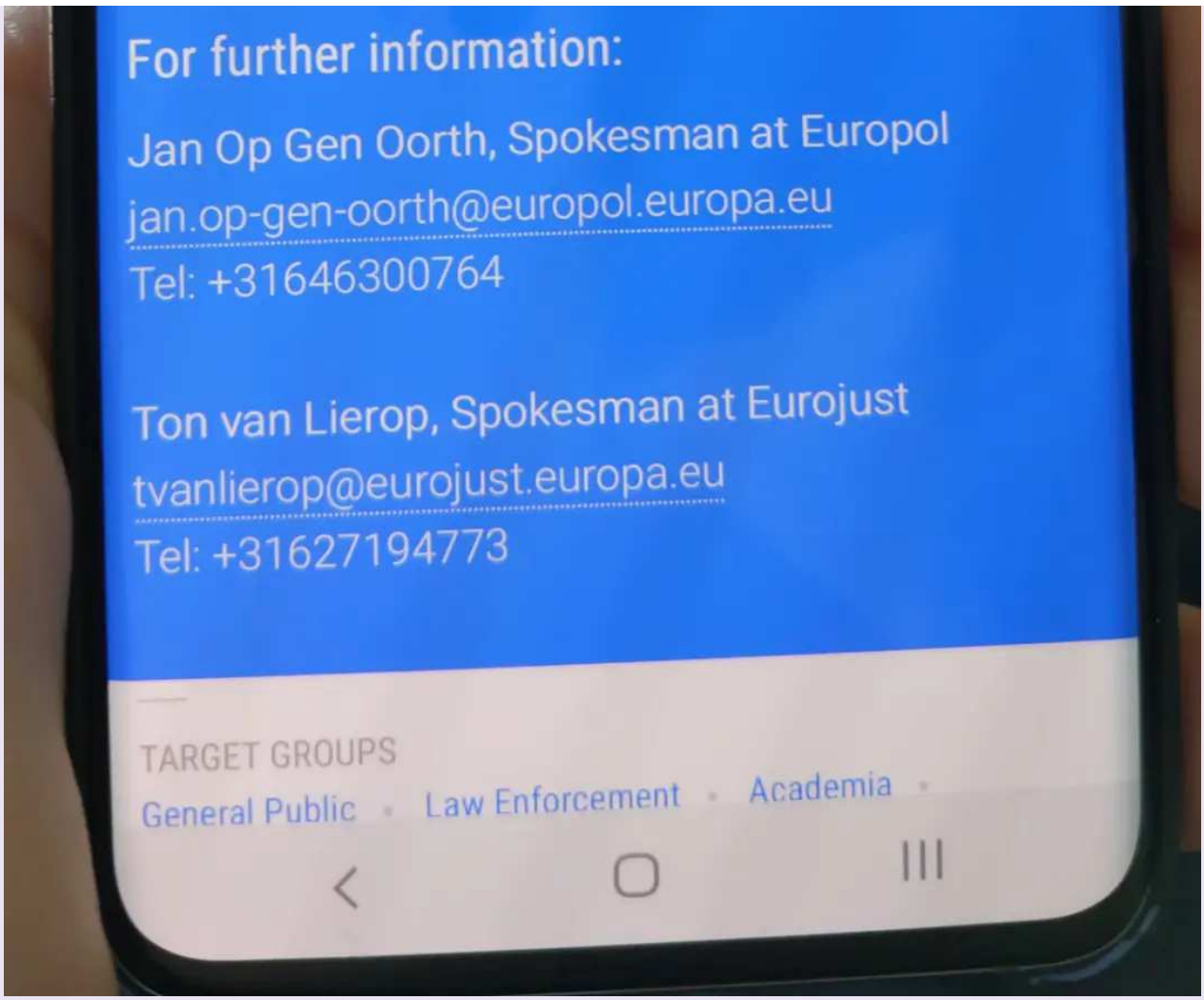
whateven 2021-03-11 10:00:41+01:00





whateven 2021-03-11 10:00:43+01:00





adcf1d 2021-03-11 12:07:42+01:00
Bror kommer på lördag eller söndag

adcf1d 2021-03-11 12:07:54+01:00
Hinner de bli av innan jag k8mmer

whateven 2021-03-11 12:07:58+01:00
💪

adcf1d 2021-03-11 12:08:14+01:00
Dom väntar på svar

whateven 2021-03-11 12:08:23+01:00
Kan han lösa etr stort garagw där liten lastbil går i

adcf1d 2021-03-11 12:09:07+01:00
Svårt bror killen bor mitt i stan

whateven 2021-03-11 12:09:19+01:00
Ok

adcf1d 2021-03-11 12:09:20+01:00
Jobbar inom elverket

adcf1d 2021-03-11 12:09:47+01:00
Undercover person

De blir inte av? 2021-03-11 12:10:55+01:00

whateven 2021-03-11 12:11:39+01:00
Jo bror bara lire uppskjutet pga env

whateven 2021-03-11 12:11:45+01:00
Sky

adcf1d 2021-03-11 12:12:11+01:00
Fattar

adcf1d 2021-03-11 12:12:41+01:00
Bror

adcf1d 2021-03-11 12:13:17+01:00
Tänkte helst blir av innan jag kommer

Polisen

Chat

2020-04-05 till 2020-04-08

JID	Alias	Användare enligt brukaranalys
adcf1d	Havana	Zafer Yavuz Den 7 april Övrig tid oidentiferad
whateven	Worldwide	?

Showing all 123 messages.

Thread 54_366243

Thread 54_377615

whateven 2021-04-05 15:54:17+02:00
Bror tjacket onsdsg torsdag

adcf1d 2021-04-05 18:05:47+02:00
Okej bror

adcf1d 2021-04-05 18:06:04+02:00
Säg lite innan bara så dom hinner åka ditåt

whateven 2021-04-06 16:11:25+02:00
forward_prefix{"forward_message_time": 1617658845159, "forward_message_user_jid": "whateven", "forward_message_body": "Bror har du något numer eller nått till någon som kanske kan hjölpa min vän att hitta killen", "forward_message_type": "TEXT", "forward_message_uuid": "5e3eb6eb-a57c-4791-b231-0c8d8227d968"}

whateven 2021-04-06 16:11:26+02:00
forward_prefix{"forward_message_time": 1617659341819, "forward_message_user_jid": "drawnsent", "forward_message_body": "D e min nära bror som satt med killen bror han ringer honom o ringer honom men han svarar inte", "forward_message_type": "TEXT", "forward_message_uuid": "3a50a9cd-d8c9-4114-8657-4671c6f1cebe"}

whateven 2021-04-06 16:11:26+02:00
forward_prefix{"forward_message_time": 1617659098241, "forward_message_user_jid": "drawnsent", "forward_message_body": "Du mena den där grejen blåsningen lr", "forward_message_type": "TEXT", "forward_message_uuid": "c077ea8b-988e-4e5f-a538-4517449f161c"}

whateven 2021-04-06 16:11:26+02:00
forward_prefix{"forward_message_time": 1617659357122, "forward_message_user_jid": "drawnsent", "forward_message_body": "Har daglig kontakt med han", "forward_message_type": "TEXT", "forward_message_uuid": "d3dd3f47-b629-42c2-be6a-dbae52d246e6"}

whateven 2021-04-06 16:11:26+02:00
forward_prefix{"forward_message_time": 1617659206347, "forward_message_user_jid": "whateven", "forward_message_body": "A bror", "forward_message_type": "TEXT", "forward_message_uuid": "9962d311-f6c4-4daa-9a6b-19cefb5d0c7a"}

whateven 2021-04-06 16:11:26+02:00
forward_prefix{"forward_message_time": 1617659381586, "forward_message_user_jid": "whateven", "forward_message_body": "Ok bror", "forward_message_type": "TEXT", "forward_message_uuid": "4d91c409-64ba-4ada-b2f5-93a03e297a59"}

whateven 2021-04-06 16:11:26+02:00
forward_prefix{"forward_message_time": 1617658856062, "forward_message_user_jid": "whateven", "forward_message_body": "Någon som känner han", "forward_message_type": "TEXT", "forward_message_uuid": "accd4ed9-1fec-486c-b3b4-7617b0ab9aee"}

whateven 2021-04-06 16:11:27+02:00
forward_prefix{"forward_message_time": 1617660729875, "forward_message_user_jid": "drawnsent", "forward_message_body": "Så fort han får tag i han tror min broder att han kommer komma till han då e d löst bror", "forward_message_type": "TEXT", "forward_message_uuid": "bc027246-03a1-4aa9-b3d1-50ad3d25090e"}

whateven 2021-04-06 17:42:11+02:00
Bror

whateven 2021-04-06 17:42:17+02:00
Är dom redo imprgon

whateven 2021-04-06 17:42:44+02:00
Anom har inte kommit en

whateven 2021-04-06 17:43:03+02:00
Du får ge dom din

whateven 2021-04-06 17:43:16+02:00
Så länge så sköter jag allt med dom

adcf1d 2021-04-06 17:47:31+02:00
När imorgon bror

adcf1d 2021-04-06 17:47:36+02:00
Tid

whateven 2021-04-06 18:03:32+02:00
Vet ej tid

whateven 2021-04-06 18:03:45+02:00
Jag skriver när jag har info

adcf1d 2021-04-06 19:20:03+02:00
Okej bror

adcf1d 2021-04-06 19:20:15+02:00
Men de är hundra imorgon

whateven 2021-04-06 20:14:33+02:00
Ja imorgon eller torsdsg

adcf1d 2021-04-06 22:02:23+02:00
Okej bror

adcf1d 2021-04-06 22:02:52+02:00
Måst2 veta nån timme innan

adcf1d 2021-04-06 22:03:02+02:00
De tar 1,5 upp

whateven 2021-04-06 22:13:32+02:00
💪

adcf1d 2021-04-06 23:09:51+02:00
Bror kommer lämna tel till min vän nu så han kommer ha den

whateven 2021-04-06 23:19:46+02:00
Ok bror

whateven 2021-04-07 08:00:39+02:00
God morgon

adcf1d 2021-04-07 08:01:47+02:00
God morgon

whateven 2021-04-07 08:20:35+02:00
Bra dubär aktiv jag väntat på tid och adress

adcf1d 2021-04-07 08:24:51+02:00
Absolut. Bara att meddela direkt när du vet så åker jag

whateven 2021-04-07 10:53:20+02:00

whateven 2021-04-07 10:53:50+02:00
Åk nu bror

whateven 2021-04-07 10:54:01+02:00
Stockholm

whateven 2021-04-07 10:55:17+02:00
Hans lur strulade innan du skulle vara där 12 😂😂

adcf1d 2021-04-07 10:55:18+02:00
Okej ska klä på mig och åker inom 1 min

whateven 2021-04-07 10:55:31+02:00
Så skynda iallfalla så gått du kan

whateven 2021-04-07 11:00:10+02:00
Jag gör en grupp med min vän

whateven 2021-04-07 11:00:21+02:00
Jag kommer vara uppdagen

adcf1d 2021-04-07 11:05:41+02:00
Okej låter bra

whateven 2021-04-07 11:32:04+02:00
Bror

whateven 2021-04-07 11:32:10+02:00
Kolla gruppen

adcf1d 2021-04-07 11:35:00+02:00
Kör bil bror

adcf1d 2021-04-07 11:35:04+02:00
Kollarnu

whateven 2021-04-07 11:36:06+02:00
Bästa

adcf1d 2021-04-07 11:36:12+02:00
Hur kommer jag till gruppen jao

whateven 2021-04-07 11:36:55+02:00
Gå in på chatar

whateven 2021-04-07 11:36:59+02:00
Så finns den där

whateven 2021-04-07 11:37:12+02:00
018♡♡♡

whateven 2021-04-07 11:37:16+02:00
Så heter den

adcf1d 2021-04-07 11:37:58+02:00
Bara våran chatt som syns

whateven 2021-04-07 11:38:31+02:00
Ok gör om nu

whateven 2021-04-07 11:38:41+02:00
Eller

whateven 2021-04-07 11:38:46+02:00
Kolla kontakter

whateven 2021-04-07 11:38:52+02:00
Där ligger den

whateven 2021-04-07 11:39:35+02:00
018♡

adcf1d 2021-04-07 11:40:48+02:00
Nu jag ser

whateven 2021-04-07 11:41:04+02:00
Kung

adcf1d 2021-04-07 17:16:45+02:00
Bror

adcf1d 2021-04-07 17:17:00+02:00
Skulle svara på de han skrev med gruppen försvann

whateven 2021-04-07 17:17:22+02:00
Jag radera den

adcf1d 2021-04-07 17:17:26+02:00
Ok

whateven 2021-04-07 17:17:46+02:00
Kan du räkna alla sen å ta bild

adcf1d 2021-04-07 17:18:03+02:00
Ja absolut

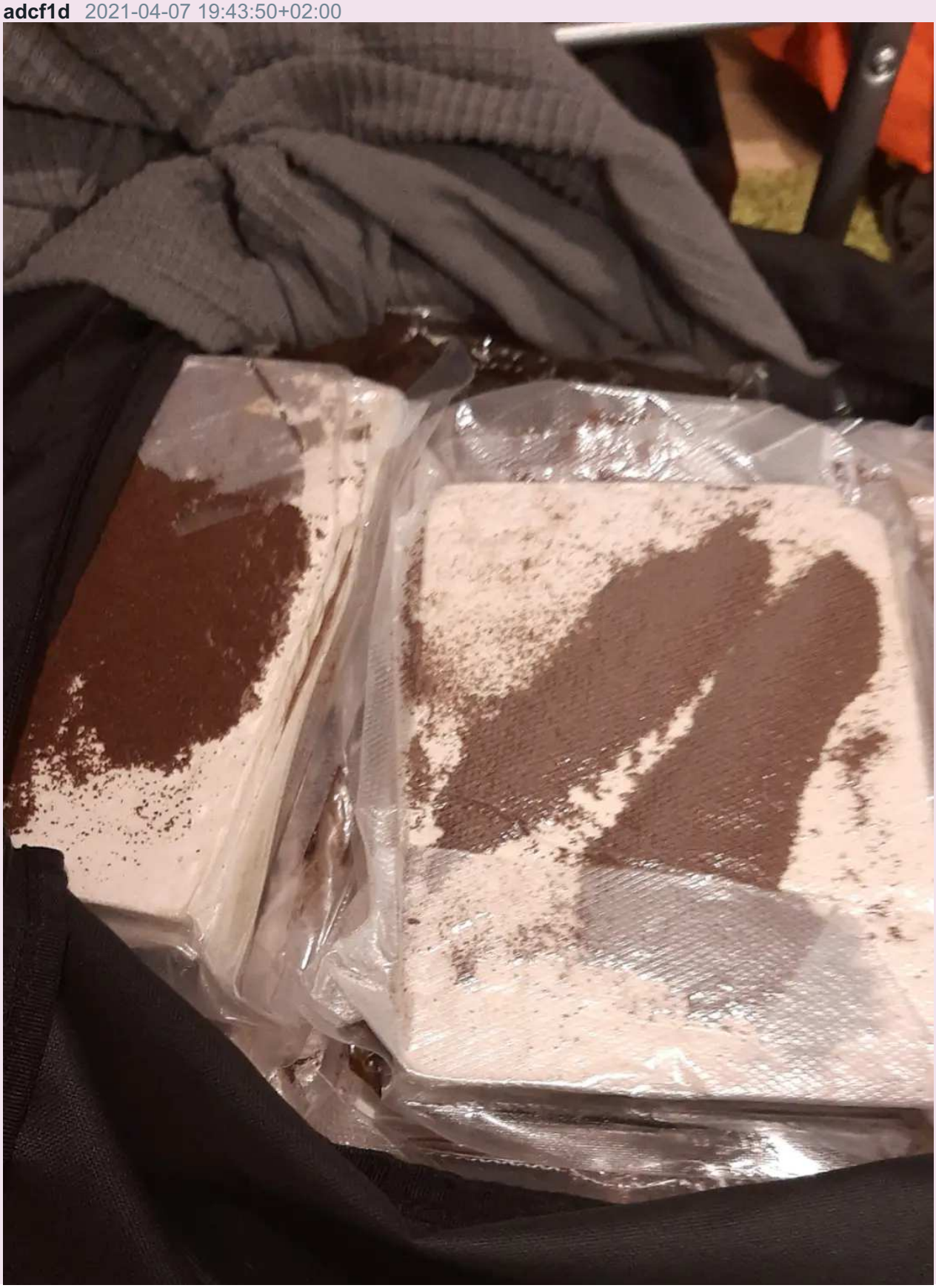
whateven 2021-04-07 17:18:17+02:00
💪

adcf1d 2021-04-07 17:18:44+02:00
De va två stora bags o en stor icakasse typ och två avlånga tunga kartonger

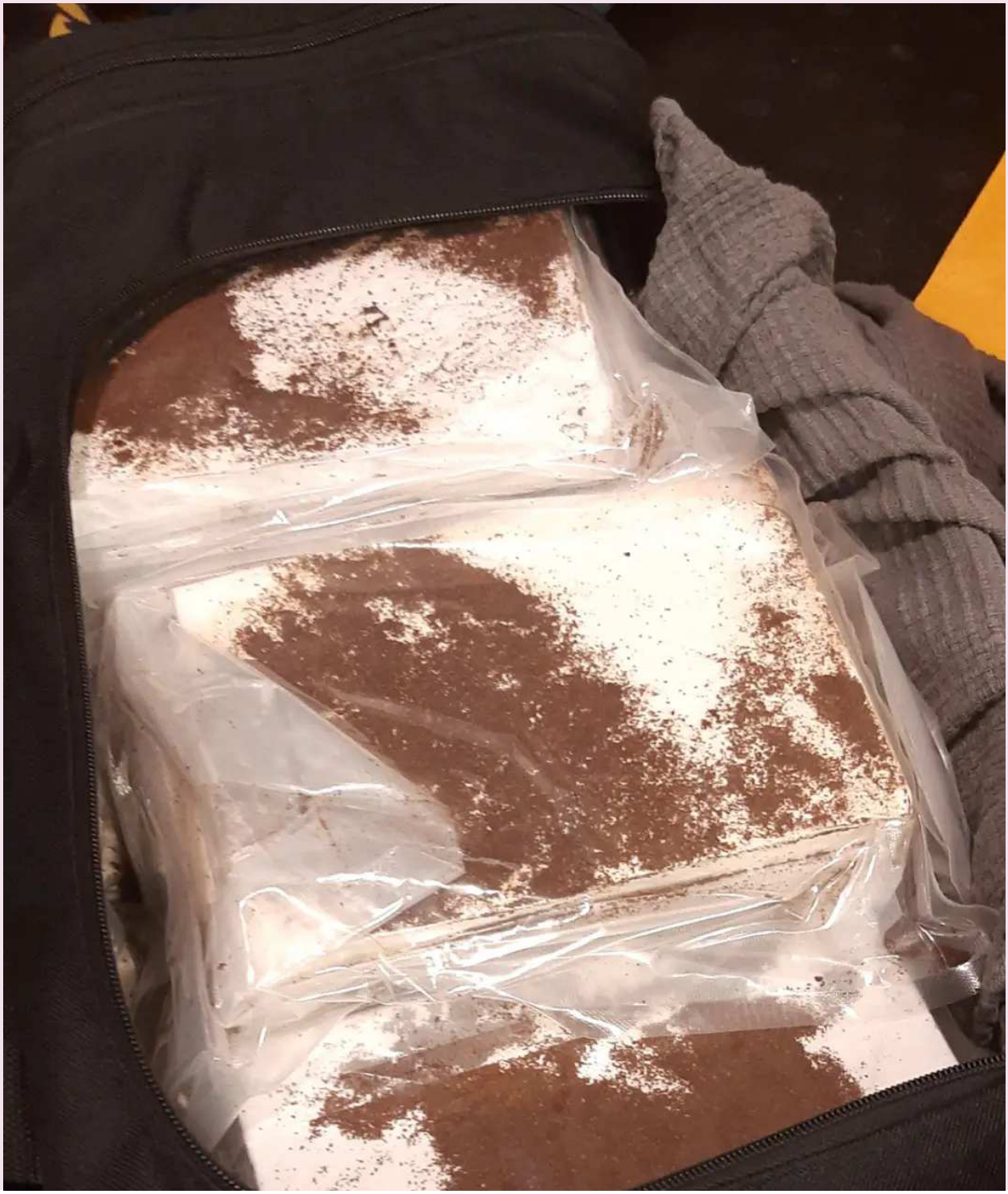
adcf1d 2021-04-07 17:19:03+02:00
Du hör från oss vid 7

whateven 2021-04-07 17:19:24+02:00
💪

adcf1d 2021-04-07 19:43:50+02:00



adcf1d 2021-04-07 19:44:00+02:00



adcf1d 2021-04-07 19:51:30+02:00
Bror 120 st

whateven 2021-04-07 19:54:51+02:00
💪💪

whateven 2021-04-08 12:15:12+02:00
Hej

whateven 2021-04-08 12:25:38+02:00
Tja

adcf1d 2021-04-08 13:12:08+02:00
Hej

whateven 2021-04-08 13:12:44+02:00
20st till malmö går det att fixa idag

adcf1d 2021-04-08 13:13:24+02:00
Malmö

adcf1d 2021-04-08 13:21:53+02:00
Behöver adress

adcf1d 2021-04-08 13:22:04+02:00
Ska kolla tåg tider nu

adcf1d 2021-04-08 13:24:51+02:00
Vi tar bilen istället

whateven 2021-04-08 13:30:00+02:00
Ja ta bil

whateven 2021-04-08 13:30:18+02:00
Bror om dom stoppar er vet vår vän då vart lager är

adcf1d 2021-04-08 13:30:54+02:00
Bror skicks4 nån annan nu

whateven 2021-04-08 13:31:18+02:00
Va då

adcf1d 2021-04-08 13:31:28+02:00
Inte samma kille som har gömt allt

whateven 2021-04-08 13:32:09+02:00
Ok bästa

whateven 2021-04-08 13:32:19+02:00
När börjag han

whateven 2021-04-08 13:33:35+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_type": "IMAGE", "forward_message_uuid": "bc8c2ac0-74ac-48a5-9a5e-53bc0362347d"}

adcf1d 2021-04-08 13:33:45+02:00
Bror han e framme i Malmö 19,50

adcf1d 2021-04-08 13:34:00+02:00
Han får åka tåg

whateven 2021-04-08 13:36:49+02:00
Ok gillar inte tåg

whateven 2021-04-08 13:37:03+02:00
Men som du vill

whateven 2021-04-08 13:37:54+02:00
Bättre ha en chafför som kör ut allt

adcf1d 2021-04-08 13:40:54+02:00
Tänker mindre risk

adcf1d 2021-04-08 13:41:05+02:00
Bil kan bli stoppad

adcf1d 2021-04-08 13:41:15+02:00
När de är så långt

whateven 2021-04-08 13:43:03+02:00
Ja men så längw killen är grön så är det lungt

whateven 2021-04-08 13:43:10+02:00
Men som du vill

whateven 2021-04-08 13:43:17+02:00
Bara han inte missar tåg

adcf1d 2021-04-08 13:43:27+02:00
Nej bror

adcf1d 2021-04-08 13:43:41+02:00

Behöver en adress med nr

adcf1d 2021-04-08 13:43:53+02:00
Han kommer ta taxi ditt

whateven 2021-04-08 13:44:18+02:00
Yes fixar

adcf1d 2021-04-08 13:45:04+02:00
Kommer lämna över telefonen nu till

whateven 2021-04-08 13:45:36+02:00
Ok så jag har direkt lontakt

adcf1d 2021-04-08 13:45:44+02:00
Exakt

whateven 2021-04-08 15:32:20+02:00
Tja är du på tåget

adcf1d 2021-04-08 15:33:02+02:00
Yes

whateven 2021-04-08 15:33:08+02:00
💪💪

adcf1d 2021-04-08 15:33:28+02:00
👊💯

whateven 2021-04-08 19:25:08+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_body": "Whw193 grå saab 93
Den står på miten av den gatan jag skicka det är inga hus där", "forward_message_type": "TEXT", "forward_message_uuid": "e74c6e97-54ef-4045-8d3c-9fb8aca7b19d"}

adcf1d 2021-04-08 19:27:13+02:00
Yes

whateven 2021-04-08 19:56:21+02:00
Hur går det

whateven 2021-04-08 19:56:41+02:00
Lägg väskan i bilen å skriv när det ät klart

adcf1d 2021-04-08 19:57:45+02:00
Bror de långt med taxi va

adcf1d 2021-04-08 19:58:12+02:00
Sitter i Cab nu från C

whateven 2021-04-08 19:59:41+02:00
Har ingen aning

adcf1d 2021-04-08 19:59:58+02:00
Okej men på g nu skriver när de klart

whateven 2021-04-08 20:00:36+02:00

Ta inte samma cab tbx

adcf1d 2021-04-08 20:25:29+02:00
Klart

whateven 2021-04-08 20:25:46+02:00
Bästa

Polisen

Gruppchat

Grupp ID: gon2aiomoroi6

2020-04-07

JID	Alias	Användare enligt brukaranalys
225375	TEAMSTERS	?
403c28	-	?

hread 83_376523/21_374675/59_373383

225375 2021-04-07 07:31:18+02:00
Good morning

225375 2021-04-07 07:31:36+02:00
quote_prefix{"quote_message_time":1617750699750,"quote_message_text":"🚮\n","quoted_text":"😜","quote_message_user_jid":"403c28","message_uid":"adeb4409-dc19-4ea5-b092-d9e0cb846ae7","isQuotedMessageDeleted":false,"isEdited":false}

225375 2021-04-07 07:34:07+02:00
So 13.00 ?

403c28 2021-04-07 07:34:56+02:00
Yes around that time

Im waiting time details now

225375 2021-04-07 07:35:16+02:00
You never sleep peaky

225375 2021-04-07 07:35:27+02:00
😳

225375 2021-04-07 07:35:35+02:00
Always online always ready

403c28 2021-04-07 07:35:51+02:00
Yes bro

403c28 2021-04-07 07:36:26+02:00
They just text that they are safe over the border

They now drive to stockholm

403c28 2021-04-07 07:36:40+02:00
I give you the adress around 11 okay bro

225375 2021-04-07 07:38:18+02:00
OK thanks

403c28 2021-04-07 07:39:03+02:00
quote_prefix{"quote_message_time":1617773733837,"quote_message_text":"Always online always ready\n","quoted_text":"💪","quote_message_user_jid":"225375","message_uid":"f6743c81-8106-4294-9e44-200287c1ffcf","isQuotedMessageDeleted":false,"isEdited":false}

225375 2021-04-07 07:47:05+02:00
I go spa maat

225375 2021-04-07 07:47:22+02:00
We speak in 2-3 hours

403c28 2021-04-07 07:47:51+02:00
Okay bro

403c28 2021-04-07 07:48:10+02:00

Enjoy

225375 2021-04-07 09:23:45+02:00
I'm back

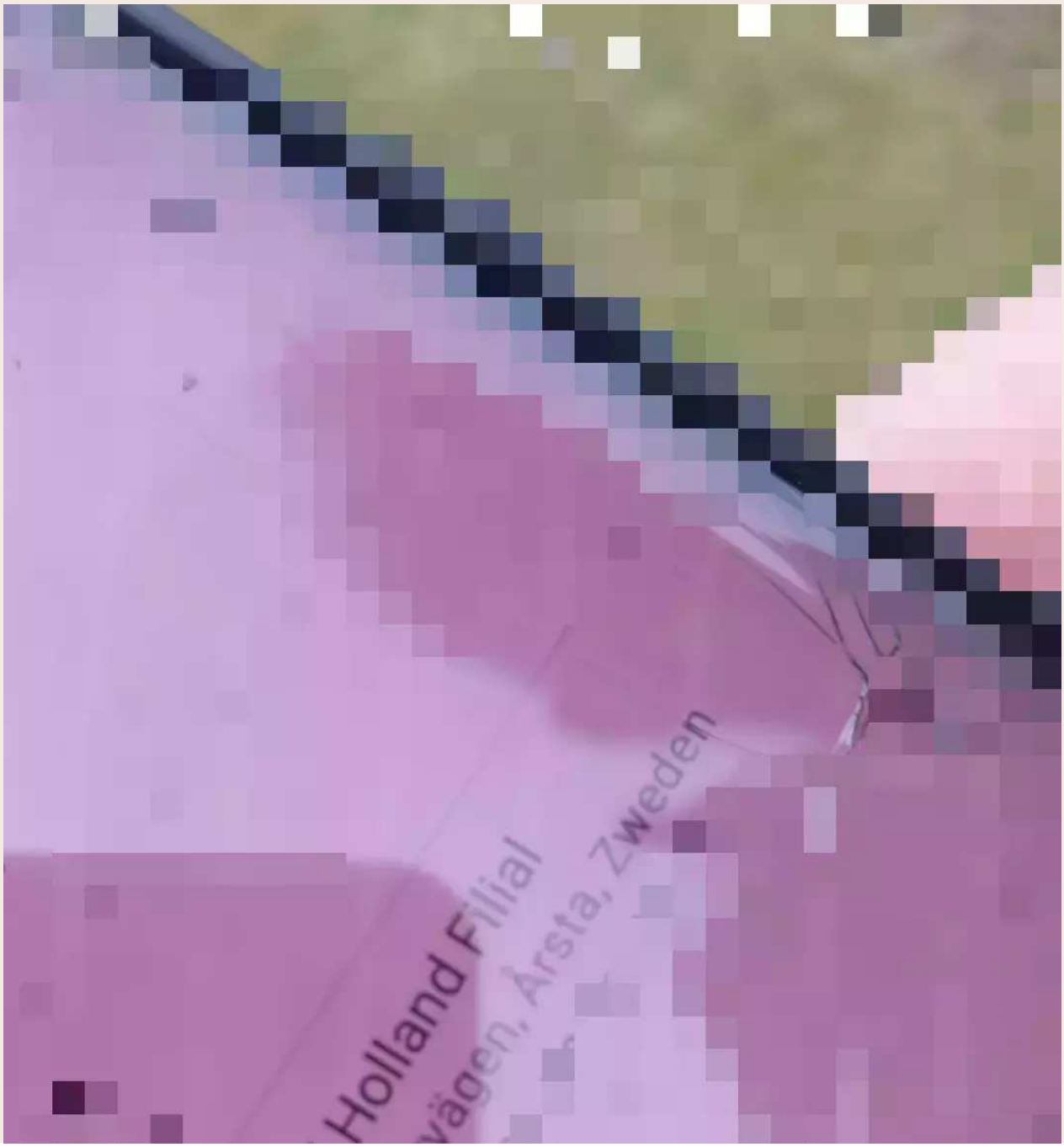
403c28 2021-04-07 09:24:20+02:00
Big boss

403c28 2021-04-07 10:18:28+02:00
Bro whats happen with the token guy? I send token friday, than he should call monday because of weekend.
Now its wednesday still nobody called.. And iff i ask i get no answer..

225375 2021-04-07 10:19:51+02:00
He call today he say yesterday 100%

403c28 2021-04-07 10:19:59+02:00
Okay

403c28 2021-04-07 10:45:09+02:00



403c28 2021-04-07 10:47:09+02:00
Your guys have to say " Rolex " to Truck Driver

225375 2021-04-07 11:24:40+02:00
OK what time

403c28 2021-04-07 11:55:45+02:00
13:30

403c28 2021-04-07 12:26:41+02:00
Bro

225375 2021-04-07 12:34:05+02:00
Yes

225375 2021-04-07 12:34:06+02:00
Top

403c28 2021-04-07 12:34:57+02:00
Okay

225375 2021-04-07 13:22:15+02:00
How we recognise the truck bro ?

403c28 2021-04-07 13:22:56+02:00
White with red i think. But let me ask hold on

225375 2021-04-07 13:32:36+02:00
Audi a4 kombi röd

225375 2021-04-07 13:32:47+02:00
Red a4 combi my guy have

403c28 2021-04-07 13:32:59+02:00
Okay

225375 2021-04-07 13:41:21+02:00
Bro tell me how its going 🙏

225375 2021-04-07 13:41:29+02:00
My guy is there

403c28 2021-04-07 13:41:31+02:00
Let me call driver.

403c28 2021-04-07 13:41:35+02:00
Okay perfect.

403c28 2021-04-07 13:41:38+02:00
Hold.on

225375 2021-04-07 13:44:43+02:00
Ok

403c28 2021-04-07 13:49:55+02:00
Wait a few minutes bro he little bit delayed

403c28 2021-04-07 14:03:51+02:00
He is there mate

403c28 2021-04-07 14:04:19+02:00
Can you ask where your guys exactly are?

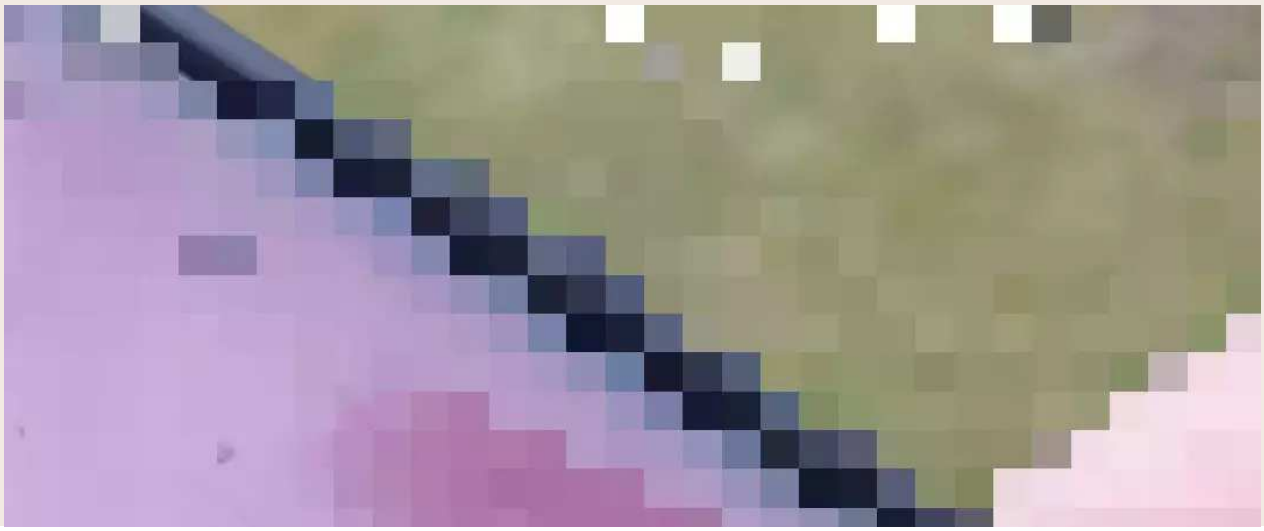
225375 2021-04-07 14:04:34+02:00
There bro

225375 2021-04-07 14:04:48+02:00
What truck is it

403c28 2021-04-07 14:05:05+02:00
Guy with blue tshirt

403c28 2021-04-07 14:05:17+02:00
Hes exactly at this sign

403c28 2021-04-07 14:05:28+02:00



403c28 2021-04-07 14:06:53+02:00
can you guys send picture where they are

225375 2021-04-07 14:12:50+02:00

403c28 2021-04-07 14:13:25+02:00
Perfect. Wait

225375 2021-04-07 14:14:25+02:00
How does the truck look

34a584 2021-04-07 14:15:15+02:00
He comes walk en take them

403c28 2021-04-07 14:16:34+02:00
He is next to you

403c28 2021-04-07 14:16:42+02:00
He send me exact same picture

225375 2021-04-07 14:16:47+02:00
Who comes walking

403c28 2021-04-07 14:16:53+02:00

225375 2021-04-07 14:17:00+02:00
I send my guy walking or your guy come

403c28 2021-04-07 14:17:11+02:00
Red truck bro

403c28 2021-04-07 14:17:17+02:00
Next to you

225375 2021-04-07 14:19:53+02:00
You see the
Red Audi a4

403c28 2021-04-07 14:25:01+02:00
Bro you and my guy send both the same picture.. You have to stand next each other.. I dont understand hahaah 😂🤦

403c28 2021-04-07 14:25:07+02:00
Big red truck

403c28 2021-04-07 14:25:19+02:00
Okay its done i hear

403c28 2021-04-07 14:26:07+02:00
All good bro?

34a584 2021-04-07 14:26:07+02:00
Your hear the same bro?

403c28 2021-04-07 14:26:16+02:00
Yes he send me a 👍

225375 2021-04-07 14:26:52+02:00
Its done bro?

225375 2021-04-07 14:27:02+02:00
OK

403c28 2021-04-07 14:27:02+02:00
Yes . pls ask your guys also

403c28 2021-04-07 14:27:13+02:00
My guy say all good nice weekend 👍

225375 2021-04-07 14:27:59+02:00
😎😎😎😎

225375 2021-04-07 14:28:01+02:00
Then its goodv

225375 2021-04-07 14:28:05+02:00
Then its good

403c28 2021-04-07 14:28:15+02:00
Good brother

Polisen

Gruppchat

Grupp ID: 5v4lmf1glxxw2

2020-04-07

JID	Alias	Användare enligt brukaranalys
whomsecret	”fyra gurkor”	?
whateven	worldwide	?
adcf1d	Havana	Zafer Yavuz

Showing all 94 messages.

Thread 54_377544

whomsecret 2021-04-07 11:04:10+02:00
Hejsan

whomsecret 2021-04-07 11:04:59+02:00
Är du där havana ?

whomsecret 2021-04-07 11:29:18+02:00
?

whateven 2021-04-07 11:39:14+02:00
Han verkar inte hitta gruppen

adcf1d 2021-04-07 11:40:56+02:00
Så

whomsecret 2021-04-07 11:41:39+02:00
forward_prefix{"forward_message_time": 1617788499039, "forward_message_user_jid": "whomsecret", "forward_message_type": "IMAGE", "forward_message_uuid": "b5693f59-40ca-411c-b95f-4b5a83895787"}

whomsecret 2021-04-07 11:41:52+02:00
Åk till denna adress

whomsecret 2021-04-07 11:42:10+02:00
Nu på en gång

adcf1d 2021-04-07 11:42:11+02:00
Yes

adcf1d 2021-04-07 11:42:25+02:00
Är på vägen redan

whomsecret 2021-04-07 11:42:36+02:00
Ok bra

whomsecret 2021-04-07 11:44:16+02:00
Kodord rolex

whomsecret 2021-04-07 11:45:46+02:00
När är du framme

adcf1d 2021-04-07 11:53:28+02:00
Ok

adcf1d 2021-04-07 11:53:51+02:00
1,30 typ

adcf1d 2021-04-07 11:54:01+02:00
Ligger på gasen

whomsecret 2021-04-07 11:55:27+02:00
Stressa inte onödigt bli stoppad

whomsecret 2021-04-07 11:55:54+02:00
Bätrre köra försiktigt

adcf1d 2021-04-07 12:06:43+02:00
Ok

adcf1d 2021-04-07 12:57:02+02:00
Framme o 20

whomsecret 2021-04-07 12:57:42+02:00
Ok

whomsecret 2021-04-07 13:07:30+02:00
Glöm inte kodord Rolex

adcf1d 2021-04-07 13:08:58+02:00
Ok

adcf1d 2021-04-07 13:17:42+02:00
Är på macken nu

adcf1d 2021-04-07 13:17:58+02:00
Ska köra in på adressen

adcf1d 2021-04-07 13:18:13+02:00
Vart ska jag ställa mig?

adcf1d 2021-04-07 13:18:22+02:00
Har en röd Audi kombi

whomsecret 2021-04-07 13:28:04+02:00
Är du framme

adcf1d 2021-04-07 13:28:32+02:00
Ja

whomsecret 2021-04-07 13:28:59+02:00
Model o färg på din bil

adcf1d 2021-04-07 13:29:13+02:00
Audi a4 kombi röd

adcf1d 2021-04-07 13:29:26+02:00
Står på parkering precis intill området

adcf1d 2021-04-07 13:29:55+02:00
Fructo ab står på skylt

adcf1d 2021-04-07 13:32:19+02:00
Jag har glasögon och tofs

adcf1d 2021-04-07 13:32:42+02:00
Svart jacka vita skor, sitter i bilen

whomsecret 2021-04-07 13:33:03+02:00
Ok

whomsecret 2021-04-07 13:39:26+02:00

Har nån kommit

adcf1d 2021-04-07 13:40:08+02:00
Nej

adcf1d 2021-04-07 13:40:37+02:00
Jag går ut från bilen och röker en cigg

whomsecret 2021-04-07 13:40:51+02:00
Ok

adcf1d 2021-04-07 13:42:21+02:00
Innan man kör in på området där alla grossister finns så finns det en bilparkering direkt till höger

adcf1d 2021-04-07 13:42:29+02:00
Där står jag

whomsecret 2021-04-07 13:42:47+02:00
Ok jag väntar på svar

adcf1d 2021-04-07 13:43:49+02:00
Ok

whomsecret 2021-04-07 14:00:38+02:00
När som dom är där

adcf1d 2021-04-07 14:01:16+02:00
Okej bram

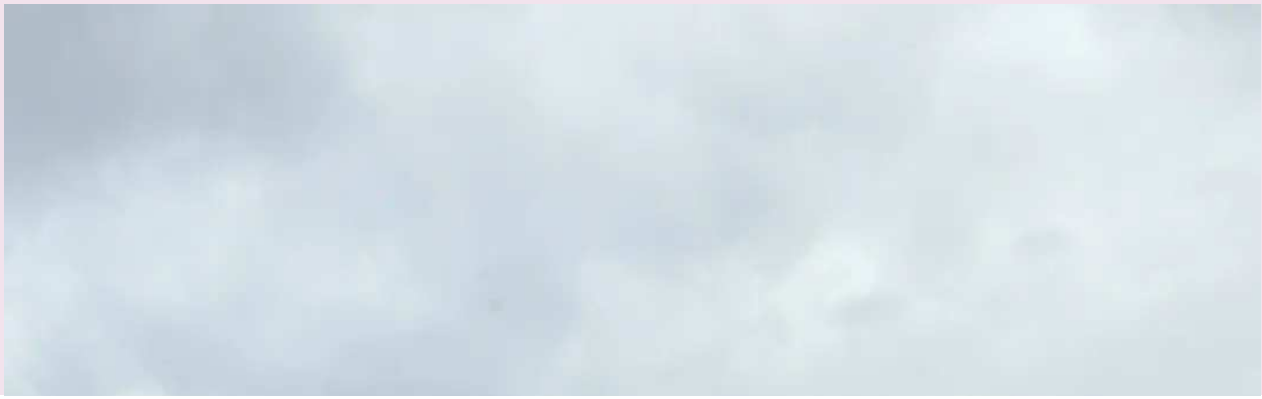
whomsecret 2021-04-07 14:05:20+02:00
Vart står du exakt

whomsecret 2021-04-07 14:05:27+02:00
Kan du skicka bild

adcf1d 2021-04-07 14:06:14+02:00

adcf1d 2021-04-07 14:07:07+02:00
Innan man kör in på området

adcf1d 2021-04-07 14:08:29+02:00



whomsecret 2021-04-07 14:09:49+02:00
Kan du ta en bäytre bild ute ifrån när man kommer in i parkwringen

adcf1d 2021-04-07 14:10:29+02:00
Ok

adcf1d 2021-04-07 14:11:45+02:00

adcf1d 2021-04-07 14:11:45+02:00
Där

adcf1d 2021-04-07 14:11:57+02:00
Röd Audi till höger

whomsecret 2021-04-07 14:12:05+02:00
Ok

whomsecret 2021-04-07 14:15:38+02:00
Glöm inte kod rolex

whomsecret 2021-04-07 14:15:50+02:00
Du kan gå till bilen

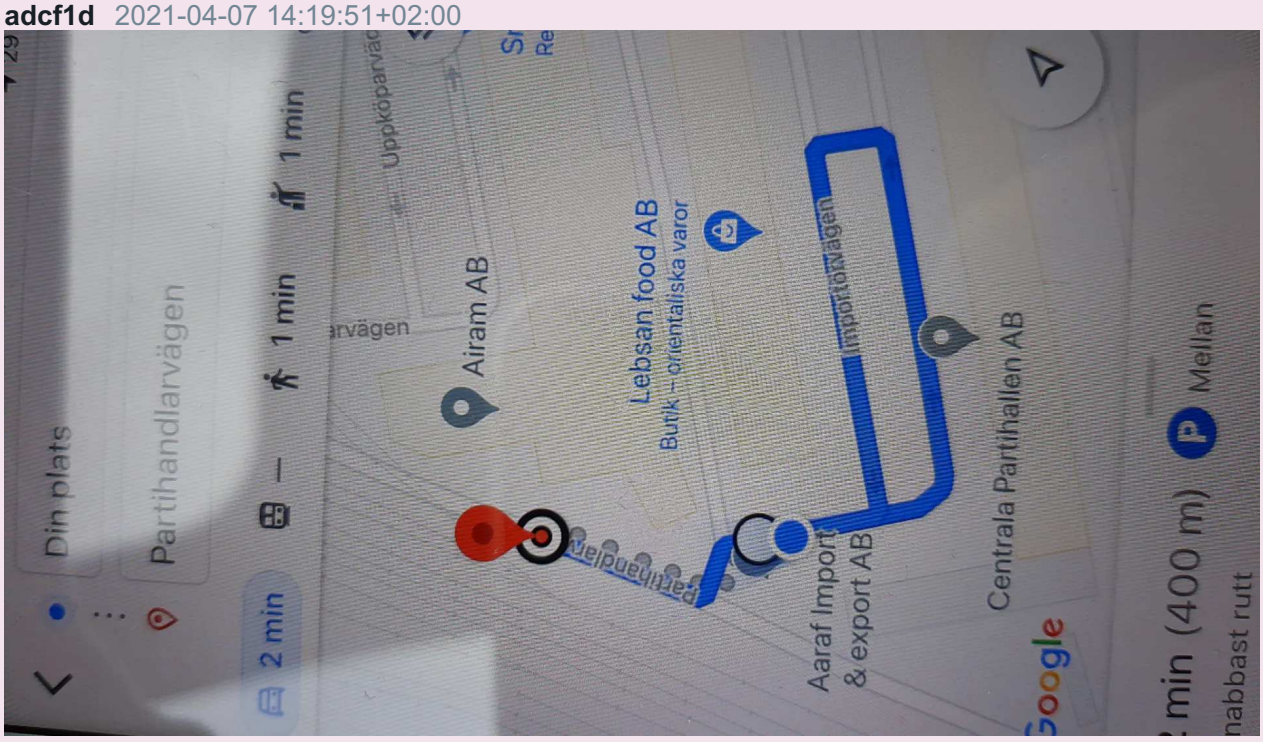
adcf1d 2021-04-07 14:16:13+02:00
Sitter i bilen

adcf1d 2021-04-07 14:16:22+02:00
Ok

whomsecret 2021-04-07 14:18:21+02:00
Är du exakt på den adressn

adcf1d 2021-04-07 14:19:13+02:00
Ja

adcf1d 2021-04-07 14:19:51+02:00



adcf1d 2021-04-07 14:20:09+02:00
Ska jag ta ett varv in på området ?

whomsecret 2021-04-07 14:20:19+02:00
Ser du röd lastbil

adcf1d 2021-04-07 14:20:27+02:00
Ja

whomsecret 2021-04-07 14:20:31+02:00
Dey är deb

adcf1d 2021-04-07 14:20:41+02:00
Vit container

adcf1d 2021-04-07 14:20:42+02:00
Ok

whomsecret 2021-04-07 14:20:58+02:00
1 sekund

whomsecret 2021-04-07 14:21:16+02:00
Gå fram säg rolex

adcf1d 2021-04-07 14:27:24+02:00
Så

adcf1d 2021-04-07 14:27:34+02:00
Ska jag åka tillbaka där jag kom ifrån?

adcf1d 2021-04-07 14:28:30+02:00
Allt är i min bil nu

whateven 2021-04-07 14:30:10+02:00
Yes

whomsecret 2021-04-07 14:30:32+02:00
Kör försiktig

adcf1d 2021-04-07 14:30:50+02:00
Ok

whomsecret 2021-04-07 14:42:13+02:00
Skriva när du är framme kommer behöva en bild när du har lagt allt i stället

whomsecret 2021-04-07 14:45:21+02:00
Viktigt att du håller hastigheten så du inte blir stoppad

adcf1d 2021-04-07 14:48:02+02:00
Ok

whomsecret 2021-04-07 15:33:39+02:00
Hur går det

adcf1d 2021-04-07 15:38:53+02:00
Halvvägs snart i v ås

whomsecret 2021-04-07 15:40:15+02:00
Ok bra

whomsecret 2021-04-07 16:28:49+02:00
Är allt bra

adcf1d 2021-04-07 16:33:37+02:00
Snart framme

adcf1d 2021-04-07 16:34:03+02:00
allt går enligt schema

whomsecret 2021-04-07 16:34:32+02:00
Perfekt

adcf1d 2021-04-07 17:08:21+02:00
Sådär

adcf1d 2021-04-07 17:09:05+02:00
Ska träffa han vid 19.00 så kör vi den till slutdestination

adcf1d 2021-04-07 17:10:14+02:00
Ligger fint i bilen och ser bilen utanför mitt fönster

whomsecret 2021-04-07 17:11:54+02:00
Ok glöm inte skicka bild sen

whomsecret 2021-04-07 17:12:06+02:00
Där dom ska va sen

whomsecret 2021-04-07 17:12:18+02:00
När kan du åka gbg

Polisen

Gruppchat

Grupp ID: 3fmvnxnzesuutS

2020-04-07

JID	Alias	Användare enligt brukaranalys
225375	TEAMSTERS	?
whomsecret	”fyra gurkor”	?
whateven	worldwide	?

Thread 54_377587/59_373396

225375 2021-04-07 07:38:26+02:00
Va redo

225375 2021-04-07 07:38:40+02:00
tp e inne i sverige

whateven 2021-04-07 07:58:31+02:00
💪

225375 2021-04-07 10:45:42+02:00
forward_prefix{"forward_message_time": 1617785138316, "forward_message_user_jid": "225375", "forward_message_type": "IMAGE", "forward_message_uuid": "f5f3d7a0-d3b2-4322-baf7-8f450fdbdfcf"}

225375 2021-04-07 10:45:59+02:00
Ser ni ?

225375 2021-04-07 10:46:03+02:00
Kl 11?

whateven 2021-04-07 10:52:44+02:00
Men bror hur ska det gå kl 11

whateven 2021-04-07 10:53:41+02:00
Kl är 11 nu

225375 2021-04-07 11:24:53+02:00
E dina killar på plats

225375 2021-04-07 11:25:06+02:00
forward_prefix{"forward_message_time": 1617785231950, "forward_message_user_jid": "403c28", "forward_message_body": "Your guys have to say " Rolex " to Truck Driver", "forward_message_type": "TEXT", "forward_message_uuid": "5b4940b6-659a-4a95-b167-3ca50ee8b883"}

whomsecret 2021-04-07 11:26:20+02:00
Micro det behövs tid du sa till sista sekunden

whomsecret 2021-04-07 11:26:50+02:00
Väntar svar från han som ska hämta dom

225375 2021-04-07 11:27:00+02:00
Bros

225375 2021-04-07 11:27:04+02:00
Skojar due

225375 2021-04-07 11:27:09+02:00
Jag sa onsdag

225375 2021-04-07 11:27:13+02:00
Kl 13

225375 2021-04-07 11:27:25+02:00

Nu sa Dom det kan bli tidigare

whomsecret 2021-04-07 11:27:41+02:00
Du sa bara onsdag

whateven 2021-04-07 11:27:58+02:00
Ja du sa bara onsdag

whateven 2021-04-07 11:28:23+02:00
Å jag fråga igår blir det imorgon jag fick inget svar

225375 2021-04-07 11:28:37+02:00
Upp

225375 2021-04-07 11:28:37+02:00
Scrolla

225375 2021-04-07 11:28:47+02:00
quote_prefix{"quote_message_time":1617717688015,"quote_message_text":"Tomorrow around 1pm be in Stockholm.. They keep me updated about times etc. And i send exact adress in the morning.","quoted_text":"Här står.det","quote_message_user_jid":"225375","message_uid":"b3f217bf-91fc-493b-8543-14f8ce38e8a0","isQuotedMessageDeleted":false,"isEdited":false}

225375 2021-04-07 11:28:53+02:00
Skickade igår

whateven 2021-04-07 11:29:00+02:00
Ok sorry

whateven 2021-04-07 11:29:03+02:00
Har missat

225375 2021-04-07 11:29:10+02:00
👌🙏

whateven 2021-04-07 11:29:32+02:00

225375 2021-04-07 11:30:35+02:00
OK bror men låt oss môta den

225375 2021-04-07 11:30:40+02:00
🤓

whateven 2021-04-07 11:31:19+02:00
Han är påbäg bror

225375 2021-04-07 11:31:50+02:00
Ok

225375 2021-04-07 11:56:39+02:00
forward_prefix{"forward_message_time": 1617789349798, "forward_message_user_jid": "403c28", "forward_message_body": "13:30", "forward_message_type": "TEXT", "forward_message_uuid": "b9a75c23-edbb-4516-97e0-fb61fffe3341"}

225375 2021-04-07 12:34:21+02:00
Kl 13.30 kod ord Rolex

whomsecret 2021-04-07 12:35:00+02:00
👍

whomsecret 2021-04-07 12:57:51+02:00
Framme om 20min

whomsecret 2021-04-07 12:58:30+02:00
Hur ser den ut är det samma som sist

225375 2021-04-07 12:59:14+02:00
Nej en annan

whomsecret 2021-04-07 13:00:19+02:00
Hur ska jag beskriva för han

225375 2021-04-07 13:00:39+02:00
Moment

225375 2021-04-07 13:27:14+02:00
E han på stället

whomsecret 2021-04-07 13:29:06+02:00
Ja

whomsecret 2021-04-07 13:29:24+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_body": "Audi a4 kombi röd", "forward_message_type": "TEXT", "forward_message_uuid": "5dbd7ad0-c765-4aa7-b014-f72f7bcf12f1"}

whomsecret 2021-04-07 13:29:56+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_body": "Står på parkering precis intill området", "forward_message_type": "TEXT", "forward_message_uuid": "0e72583a-9ebf-408d-8609-f9a418b2b296"}

whomsecret 2021-04-07 13:32:57+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_body": "Fructo ab står på skylt", "forward_message_type": "TEXT", "forward_message_uuid": "e4631a0c-1d7b-45a5-9161-dea442357250"}

whomsecret 2021-04-07 13:40:22+02:00
Hur går det

225375 2021-04-07 13:50:51+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_body": "Wait a few minutes bro he little bit delayed", "forward_message_type": "TEXT", "forward_message_uuid": "b091da5c-1a17-4f7f-a079-885b65de61d2"}

225375 2021-04-07 14:04:24+02:00
Han e där

225375 2021-04-07 14:04:38+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_body": "Can you ask where your guys exactly are?", "forward_message_type": "TEXT", "forward_message_uuid": "fb412ec1-0f0e-45b7-be27-79d549ec0d7d"}

whomsecret 2021-04-07 14:06:37+02:00

whomsecret 2021-04-07 14:06:37+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_type": "IMAGE", "forward_message_uuid": "756bdc67-530c-47a5-b6f0-42ed9d4f1bd7"}

whomsecret 2021-04-07 14:07:24+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_body": "Innan man kör in på området", "forward_message_type": "TEXT", "forward_message_uuid": "37070c2e-4831-4fe1-a4ed-13acc0ed8e78"}

225375 2021-04-07 14:08:20+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_body": "can you guys send picture where they are", "forward_message_type": "TEXT", "forward_message_uuid": "456c85f7-be6c-46c0-9722-122a1705fcce"}

225375 2021-04-07 14:08:44+02:00
?

whomsecret 2021-04-07 14:08:55+02:00
Jag skickade bild

whomsecret 2021-04-07 14:12:00+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_type": "IMAGE", "forward_message_uuid": "77b579ca-ac5d-4234-ae2b-51595e105e39"}

whomsecret 2021-04-07 14:12:46+02:00
Det står en röd audi a4 där också

225375 2021-04-07 14:13:06+02:00
Ok

225375 2021-04-07 14:14:32+02:00
Code rolex

whomsecret 2021-04-07 14:15:23+02:00
Ok

225375 2021-04-07 14:17:17+02:00
Ni e på samma ställe

225375 2021-04-07 14:17:30+02:00
Dom e.brevid varandra

225375 2021-04-07 14:17:46+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_body": "Red truck bro", "forward_message_type": "TEXT", "forward_message_uuid": "f61887c7-6dca-4e19-8a89-b36d4da09ac5"}

225375 2021-04-07 14:17:46+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_body": "Next to you", "forward_message_type": "TEXT", "forward_message_uuid": "fb38d9d3-52d0-449b-a097-1a1d935b5c34"}

whomsecret 2021-04-07 14:18:48+02:00
Han säger det är exakt innan området

225375 2021-04-07 14:19:37+02:00
Vem säger

225375 2021-04-07 14:19:41+02:00
Ser han röda lastbilen

whomsecret 2021-04-07 14:20:38+02:00
A

whomsecret 2021-04-07 14:20:43+02:00
Han ser den

whomsecret 2021-04-07 14:20:47+02:00
Är dey den

225375 2021-04-07 14:21:07+02:00
Bra kan han gå fram säga rolex

225375 2021-04-07 14:26:49+02:00
Klart ?

225375 2021-04-07 14:27:17+02:00
Mina säger det e klart

225375 2021-04-07 14:27:25+02:00
🤝

225375 2021-04-07 14:27:34+02:00
Bekräfta gurkan🙏

whateven 2021-04-07 14:30:34+02:00
Klart

whateven 2021-04-07 14:30:39+02:00
💪💪

225375 2021-04-07 14:37:03+02:00
Ok

225375 2021-04-07 14:37:16+02:00
Kan Dom ta kort när det e i stash

whomsecret 2021-04-07 14:38:28+02:00
Absolut

whomsecret 2021-04-07 14:38:40+02:00
Ska dom räkna allt

225375 2021-04-07 14:38:52+02:00
120 kilo e det

whomsecret 2021-04-07 14:39:02+02:00
Ok

whomsecret 2021-04-07 14:39:26+02:00
Plus dom andra 2 också vist

225375 2021-04-07 14:39:31+02:00
Bäst att ta alla drop I gruppen så vi hjälps åt att hålla kolll

225375 2021-04-07 14:39:37+02:00
😉😎🙏

225375 2021-04-07 14:40:01+02:00
quote_prefix{"quote_message_time":1617799168743,"quote_message_text":"Plus dom andra 2 också vist\n","quoted_text":"Nästa onsdag 60 kilo tjack och 2 Ladd","quote_message_user_jid":"whomsecret","message_uid":"b346b00b-5959-4a7e-b36a-5f74799b6bb7","isQuotedMessageDeleted":false,"isEdited":false}

225375 2021-04-07 14:40:07+02:00
Nu bara 120 kilo tjack

whomsecret 2021-04-07 14:40:11+02:00
Ok

225375 2021-04-07 15:22:23+02:00
E han inte I stash

225375 2021-04-07 15:22:50+02:00
E det uppdelat att det e stash på ett ställe och han som kör ut inte e kopplad

225375 2021-04-07 15:23:09+02:00
Vilken dag kan vi köra malmö och GBG ?

whateven 2021-04-07 15:37:35+02:00
Han är inte hemma en
Skriver direkt

225375 2021-04-07 15:44:25+02:00
Kör han till örebro ?

225375 2021-04-07 15:44:37+02:00
Hur ska vi boka utkörningar

225375 2021-04-07 15:44:42+02:00
quote_prefix{"quote_message_time":1617802659232,"quote_message_text":"Han är inte hemma en\nSkriver direkt\n","quoted_text":"Ok","quote_message_user_jid":"whateven","message_uid":"25f7719c-5e34-4eb9-9865-3007dc957524","isQuotedMessageDeleted":false,"isEdited":false}

225375 2021-04-07 17:12:10+02:00
E allt OK Mina vänner

whomsecret 2021-04-07 17:12:24+02:00
Allt är bra

whomsecret 2021-04-07 17:12:34+02:00
Han är framme

225375 2021-04-07 17:13:02+02:00
Har han räknat

whomsecret 2021-04-07 17:13:49+02:00
Han ska göra om en stund

whateven 2021-04-07 17:13:58+02:00
Nej han har parkerat bilen å väntar på att stash ska hämta bilen och räkna

whateven 2021-04-07 17:14:18+02:00

Det blir lite senare

225375 2021-04-07 17:15:09+02:00

Bästa gillar när det låter komplicerat det känns säkert

Polisen

Chat

2020-04-09 till 2020-04-11

JID	Alias	Användare enligt brukaranalys
whateven	worldwide	?
7b7ef3		?

Showing all 26 messages.

Thread 54_391096

whateven 2021-04-09 09:10:10+02:00
Våran båt på spansla sidan är ute å väntar bror

7b7ef3 2021-04-09 14:41:41+02:00
Va säger dom bror

whateven 2021-04-09 14:43:57+02:00
Spanien båten är ute å väntar

7b7ef3 2021-04-09 14:44:23+02:00
Okej så dom ska köra nu på Dan?

whateven 2021-04-09 14:45:17+02:00
Nej trpr dom väntar
Men dom hållwr på för fullt

7b7ef3 2021-04-10 00:27:36+02:00
Har Du hört nå nytt bror

whateven 2021-04-10 11:17:02+02:00
Ska träffa dom idag

whateven 2021-04-10 21:59:47+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_body": "OK pal please", "forward_message_type": "TEXT", "forward_message_uuid": "6a6f15ec-a559-44a3-ab98-1d9b3794a71a"}

whateven 2021-04-10 21:59:47+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_body": "My boy go mpw stay with guy while we work", "forward_message_type": "TEXT", "forward_message_uuid": "0174d0e6-6009-4eff-b915-199075cbcc08"}

whateven 2021-04-10 21:59:52+02:00
forward_prefix{"forward_message_time": -1, "forward_message_user_jid": "", "forward_message_type": "IMAGE", "forward_message_uuid": "f9c497da-39d1-4646-b395-09c8c0b810bf"}

whateven 2021-04-10 22:00:35+02:00
Så trött på det här brorf

whateven 2021-04-10 22:48:44+02:00
Kommer köra 2,5 bara me den båten bror

7b7ef3 2021-04-11 18:33:46+02:00
Sho bror

whateven 2021-04-11 18:36:33+02:00
Sho brori

7b7ef3 2021-04-11 18:42:32+02:00
Va händer är allt bra

Nej inte bra torska 90st tjack 2021-04-11 18:50:53+02:00

7b7ef3 2021-04-11 19:01:57+02:00
Knas

7b7ef3 2021-04-11 19:01:59+02:00
Vart

whateven 2021-04-11 19:02:22+02:00
Örebro

whateven 2021-04-11 19:02:43+02:00
Tur jag han dela ut 35

7b7ef3 2021-04-11 19:03:34+02:00
Ouf jobbigt bror

whateven 2021-04-11 19:04:00+02:00
A men standard

whateven 2021-04-11 19:04:05+02:00
😂😂

7b7ef3 2021-04-11 19:04:17+02:00
Låt oss ses sen så vi kan gå igenom

whateven 2021-04-11 19:25:32+02:00
Ok bror
Har du panik 😂

7b7ef3 2021-04-11 19:59:50+02:00
Haha nej bara tappat hoppet

Polisen

Chat

20-04-11 kl 16:08 till 20-04-11 kl 16:10

JID	Alias	Användare enligt brukaranalys
whomsecret	”fyra gurkor”	?
4f3887		?

Showing 14 matches out of 95 message(s).Show all

Thread 54_391062

4f3887 2021-04-11 16:08:04+02:00
Varför den e päsh väll

4f3887 2021-04-11 16:08:09+02:00
Hälften va inte er

whomsecret 2021-04-11 16:08:23+02:00
Men ändå

4f3887 2021-04-11 16:08:31+02:00
Hur många e de?

whomsecret 2021-04-11 16:08:35+02:00
85st

4f3887 2021-04-11 16:08:43+02:00
Som e er?

whomsecret 2021-04-11 16:08:49+02:00
Allt va 120

4f3887 2021-04-11 16:09:02+02:00
Är de eran risk?

4f3887 2021-04-11 16:09:06+02:00
Dom alla?

whomsecret 2021-04-11 16:09:18+02:00
Inte alla va jag vet

whomsecret 2021-04-11 16:09:27+02:00
Vår halva bara

4f3887 2021-04-11 16:09:36+02:00
Ja men 40 st

whomsecret 2021-04-11 16:09:48+02:00
De är äbdå mycket

whomsecret 2021-04-11 16:10:28+02:00
Ingen aning skulle gå förbi för att kolla varför man inte svara mig allt spärrat

Polisen

Chat

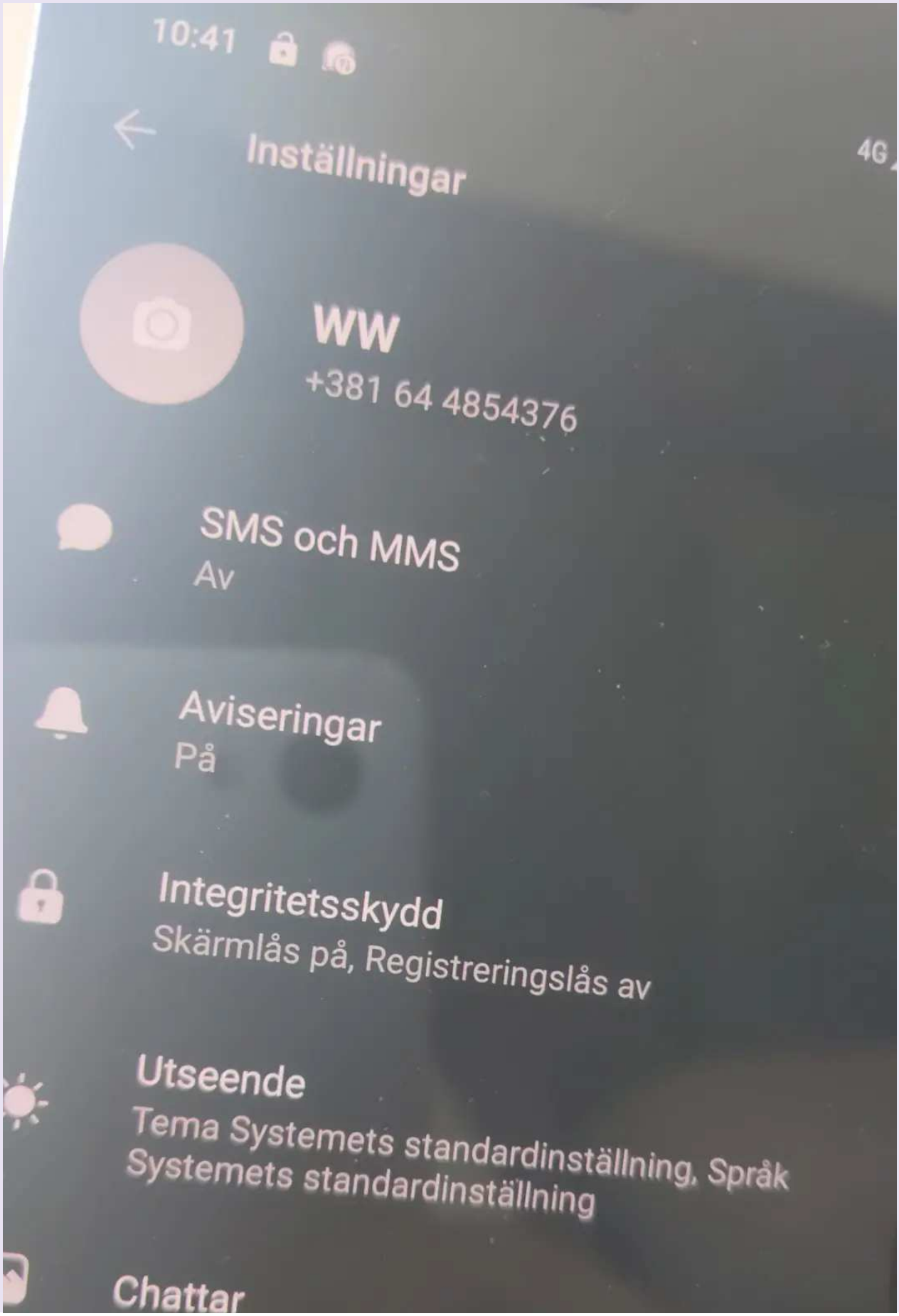
2020-04-12

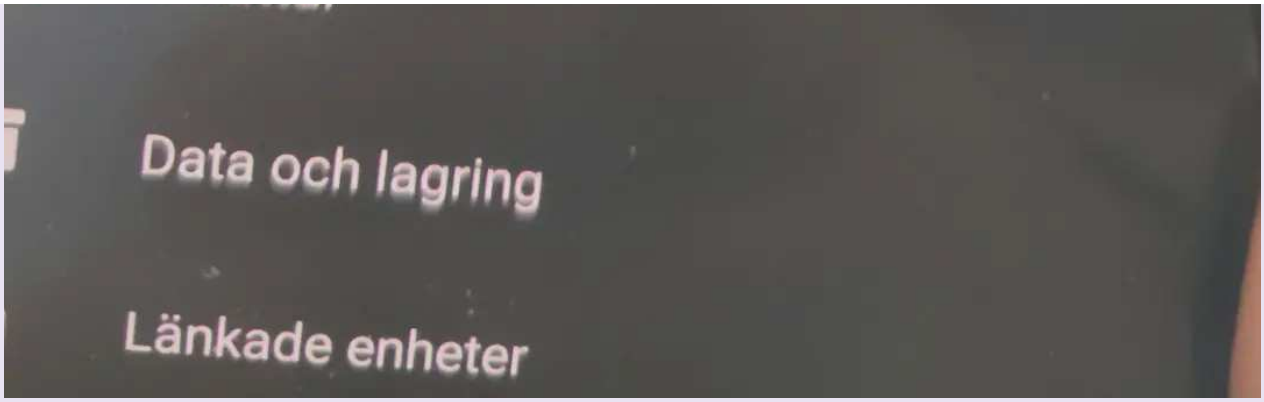
JID	Alias	Användare enligt brukaranalys
whateven	worldwide	?
buslost		?

Showing all 20 messages.

Thread 54_404074

whateven 2021-04-12 10:42:55+02:00





buslost 2021-04-12 10:44:38+02:00
Är det nya?

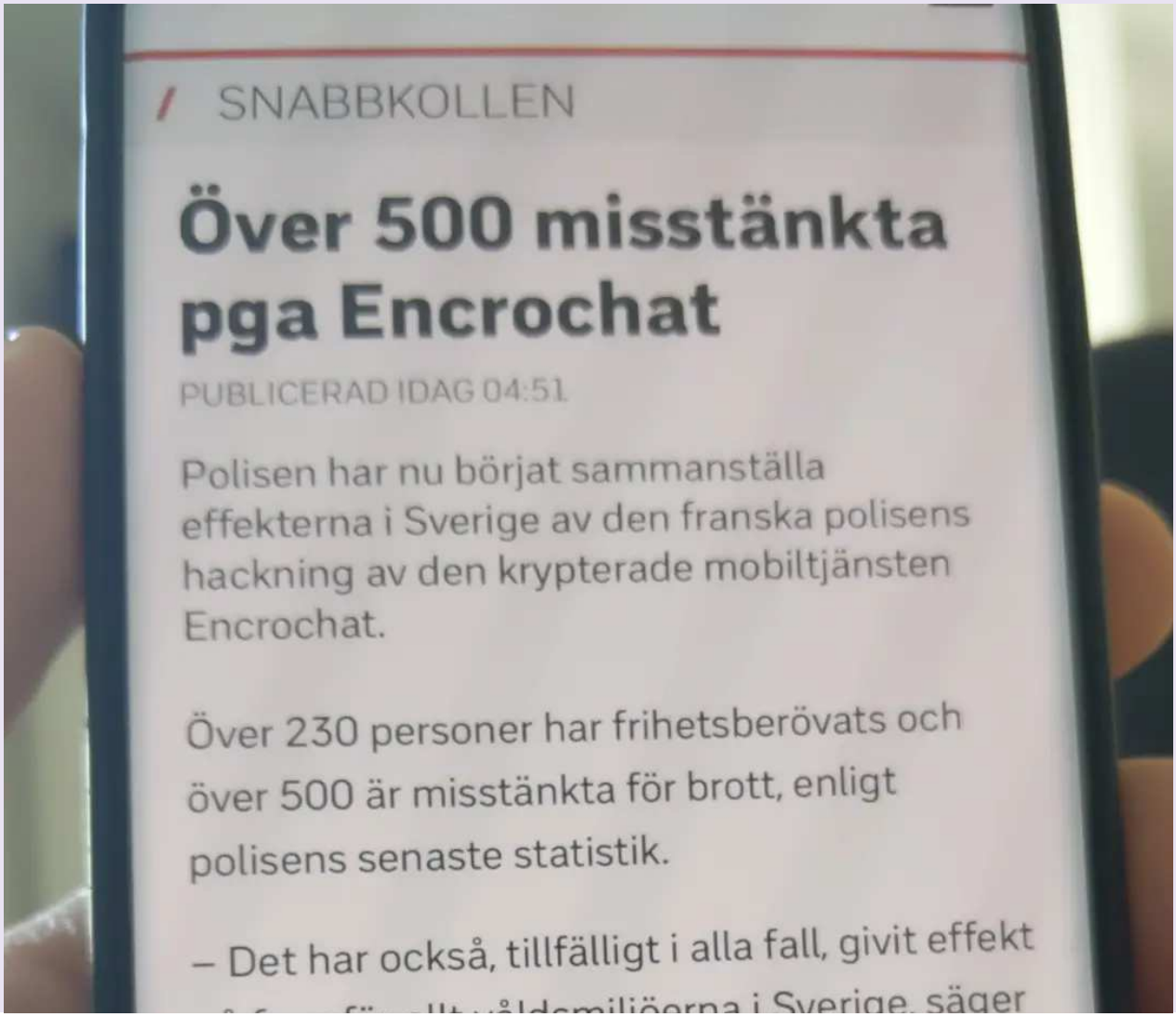
whateven 2021-04-12 10:51:28+02:00
Yes

buslost 2021-04-12 10:52:06+02:00
Det går inte att se videon, den laddas inte ner

whateven 2021-04-12 10:53:08+02:00
Aha skjut iväg appen å prova igen

buslost 2021-04-12 10:53:45+02:00
Den försvann nu haha

whateven 2021-04-12 10:56:06+02:00


SNABBKOLLEN

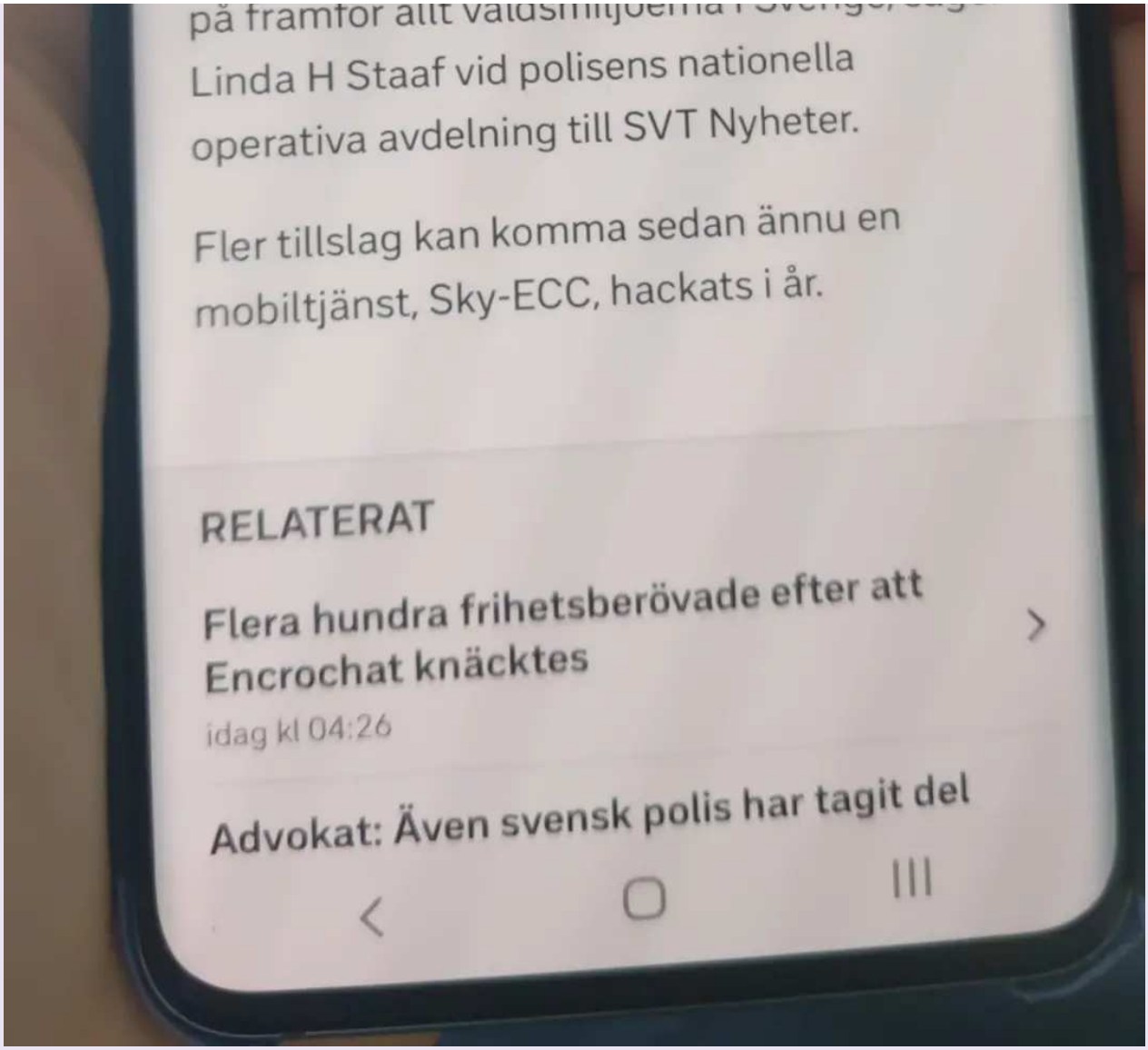
Över 500 misstänkta pga Encrochat

PUBLICERAD IDAG 04:51

Polisen har nu börjat sammanställa effekterna i Sverige av den franska polisens hackning av den krypterade mobiltjänsten Encrochat.

Över 230 personer har frihetsberövats och över 500 är misstänkta för brott, enligt polisens senaste statistik.

– Det har också, tillfälligt i alla fall, givit effekt



buslost 2021-04-12 12:50:16+02:00
Bror va har hänt?

whateven 2021-04-12 13:13:55+02:00
Torska stash igår 90 tjack

buslost 2021-04-12 13:14:12+02:00
Abo

whateven 2021-04-12 13:14:13+02:00
Fattar ej hur helt nytt stash

buslost 2021-04-12 13:14:17+02:00
Fucking kuk

whateven 2021-04-12 13:14:22+02:00
3 dagar

buslost 2021-04-12 13:15:13+02:00
Den var där 3 dagar?

whateven 2021-04-12 13:23:13+02:00
Ja exakt

whateven 2021-04-12 13:23:28+02:00

Jag han dela ut 35st bara

buslost 2021-04-12 13:24:22+02:00
Fan asså

buslost 2021-04-12 13:24:37+02:00
Var det nytt stash men samma arbetare?

whateven 2021-04-12 13:51:18+02:00
Ja men nya arbetare mr

whateven 2021-04-12 13:51:20+02:00
Me

Polisen

Gruppchat

Chat

2020-05-05 till 2020-05-06

JID	Alias	Användare enligt brukaranalys
225375	TEAMSTERS	?
whateven	worldwide	?

Sista meddelandet där inte innehåll visas är en ljudfil

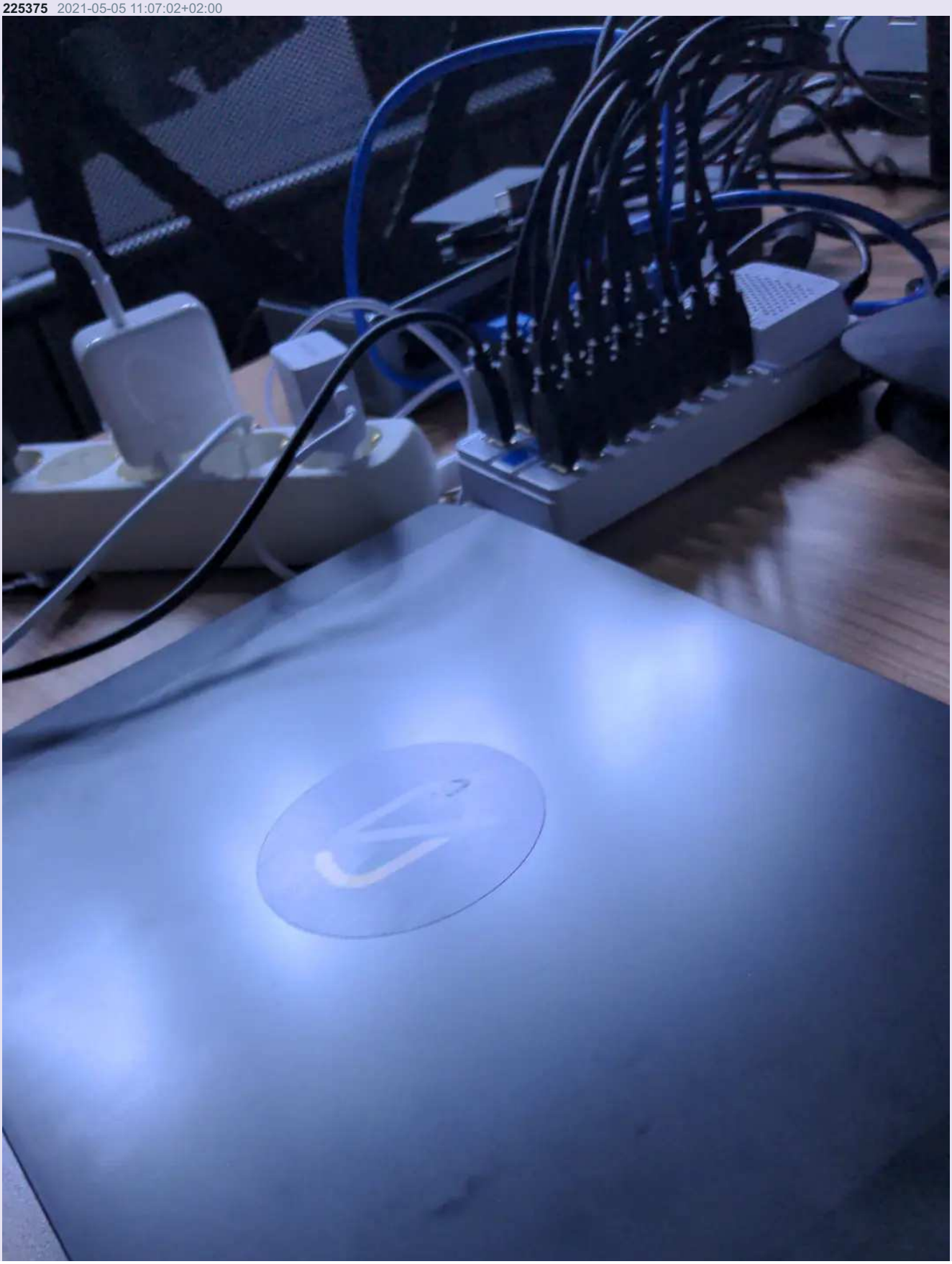
Showing all 34 messages.

Thread 54_556602/59_552840

whateven 2021-05-05 10:33:12+02:00
God morgon lever du

225375 2021-05-05 11:06:27+02:00

225375 2021-05-05 11:07:02+02:00



225375 2021-05-05 11:07:28+02:00
Har lite ångest bror gör anom grejer för att glömma 😃

whateven 2021-05-05 11:13:27+02:00
Bästa

225375 2021-05-05 11:57:24+02:00
Vilken tid kan vi ringa varandra ?

225375 2021-05-05 12:00:22+02:00
Bror kan du be btc ringa mig och gå igenom siffror

whateven 2021-05-05 12:02:37+02:00
Yes ber han ringa
Bror skit i att ringa nu blir nojjig nått ät helt fel

225375 2021-05-05 12:10:01+02:00
Jag behöver först gå igenom med btc viktigt bror . sen kan jag och du gå igenom på anom

225375 2021-05-05 12:10:39+02:00

225375 2021-05-05 12:42:19+02:00
Har gurkan namnet på han som ramla i örebro ?

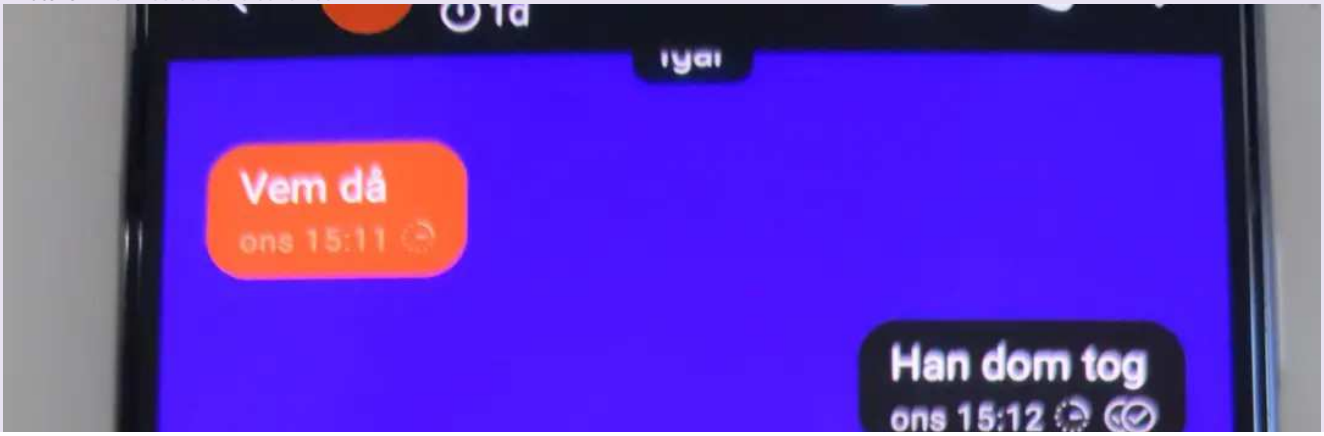
225375 2021-05-05 12:42:50+02:00
Vill ta ut häktning visa till min vän

whateven 2021-05-05 12:45:35+02:00
Nej
Han vet inte vem det är
Det var mina killar

whateven 2021-05-05 12:45:54+02:00
Jag väntar namn

225375 2021-05-05 22:57:36+02:00
quote_prefix{"quote_message_time":1620211529660,"quote_message_text":"Jag väntar namn\n","quoted_text":"OK bror","quote_message_user_jid":"whateven","message_uid":"d46c4950-0a31-4593-879f-2065b12263e2","isQuotedMessageDeleted":false,"isEdited":false}

whateven 2021-05-06 09:29:09+02:00



225375 2021-05-06 09:32:51+02:00
quote_prefix{"quote_message_time":1620286125314,"quote_message_text":"https://anom-one.s3-accelerate.amazonaws.com/832391f13a2e9b767df2a442d6a873bf3f0ccb61bde555756f0c8ce741793007/35089558-911f-4ec7-a6ce-1fec524cdb42.webp#34e43234066eb8f3d0ac7829fd816a061248b3236e99ee9f618a61800e1732a9f7647a0062f2f910f29a3eb0ba601626|50684|1080|1920\n","quote_message_user_jid":"whateven","message_uid":"35089558-911f-4ec7-a6ce-1fec524cdb42","isQuotedMessageDeleted":false,"isEdited":false}

Detta e senaste eller 85 kilo tappet ?

whateven 2021-05-06 09:57:58+02:00
Yes

whateven 2021-05-06 09:58:05+02:00
85kg

225375 2021-05-06 12:22:13+02:00
Läget med dig bror

225375 2021-05-06 12:45:22+02:00
Har du tid?

225375 2021-05-06 12:45:42+02:00
Btc svarar ej jag pratar hellre med dig 😀

whateven 2021-05-06 12:48:28+02:00
Hahaha
Va händer brir

225375 2021-05-06 12:59:34+02:00
Bror btc duckar mig hahahahaha

225375 2021-05-06 12:59:49+02:00
Ska bara äta bror skriver

225375 2021-05-06 17:48:42+02:00
Addar dig från min btc lur

whateven 2021-05-06 17:54:56+02:00
Ok bror

225375 2021-05-06 17:55:34+02:00
Jag e btc bror

225375 2021-05-06 17:55:59+02:00
Ska ha en lur med alla räkningar och listor den e sepperat

whateven 2021-05-06 18:00:07+02:00
Shitt hur orkar du

225375 2021-05-06 18:01:20+02:00

225375 2021-05-06 18:01:38+02:00

225375 2021-05-06 18:01:46+02:0

Teknisk information om Operation Trojan Shield

Senast uppdaterad: 31 augusti 2021

INNEHÅLLSFÖRTECKNING

1. ÖVERSIKT ÖVER SERVRAR OCH NÄTVERK 5

1.1 XMPP-server 5

1.2 Server i tredje land 5

1.3 Google-servrar 5

1.3.1 Överföring 5

1.3.2 Proxy 6

1.4 AWS GovCloud 6

1.4.1 Säkerhet 6

1.4.2 Frontend 6

1.4.3 Ingestion-1 (I1) 6

1.5 Aktivitet i meddelandenätverket 6

2. SKAPANDE AV NYA DATAPAKET 7

2.1 Kryptering av data 8

2.2 Hur databasens skillnadsdump skapades 8

2.3 Hur listan med bilagor fastställs från skillnadsdumpen 8

2.4 Hur bilagor kopierades från fillagringen 9

2.5 Skapa det krypterade paketet 9

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

3.1 Program som överför data till överföringsservern 9

4.ÖVERFÖRING FRÅN ÖVERFÖRINGSSERVERN TILL AWS GOVCLOUD 10

4.1 Automatisering av program för att överföra data 10

5. BEARBETNING AV KRYPTERADE PAKET 10

5.1 Avkryptering av GPG-paket 10

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

5.3 Inmatning av databasdumpen till en tillfällig databas 10

6. AVKRYPTERINGSPROCESSEN 10

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

6.2 Avkryptering av alla filer i bilagor 11

7. BEARBETNING AV LJUDFILER 11

7.1 Konvertera ljudfiler till användbart format 11

7.2 Ändring av tonhöjd i ljudfiler om nödvändigt 11

8. DATABASÖVERSIKT 11

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

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

8.3 Förteckningen 12

8.4 Grupper 13
8.4.1 Avsaknad av gruppinformation 13

8.5 Produkter 13
8.5.1 Produkter i detalj 13

8.6 Meddelanden 15
8.6.1 Fel i meddelandens tidszon 16

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

9. INMATNINGSPROCESS 18

9.1 Mata in ny information i förteckningen 18

9.2 Infoga nya grupper 18
9.2.1 Infoga ny gruppinformation 19

9.2.2 Infoga uppdateringar om medlemskap i grupper 19

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

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

9.5 Export efter inmatning *22*

10. WEBBAPPLIKATION/GRANSKNINGSPLATTFORM 22

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

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

10.3 Produktsidan *26*

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

10.6 Förteckningssidan *33*

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

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

11. MLAT-EXPORT 40

11.1 Hämtning av alla bifogade filer *40*

11.2 Hämtning av slutlig MySQL-databasdump *40*

11.3 Skapa MLAT-exporter *40*

BILAGA A 41

A.1 Kryptering med offentlig nyckel *41*

A.2 Hash *41*

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

A.4 Portalen *43*

A.5 Enheter *44*

A.5 Nätverksanslutning till plattformen *45*

A.6 MDM-komponenten *45*

A.7 ANØM-applikationen *46*

A.8 Data spelas in från plattformen *49*

A.8.2 Metadata för meddelanden 50

A.9 Autentisering och integritet *51*

1. ÖVERSIKT ÖVER SERVRAR OCH NÄTVERK

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

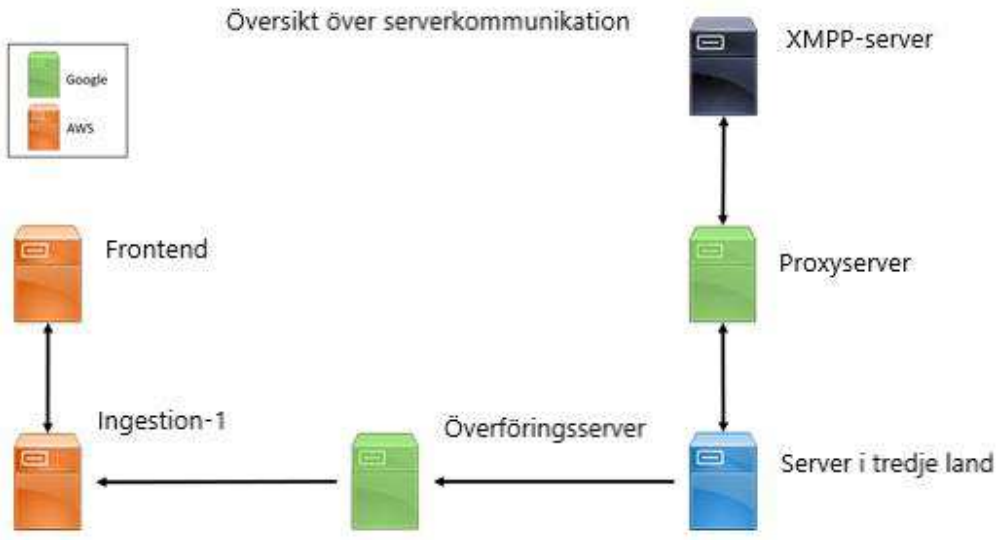


Diagram 1.A

1.1 XMPP-server

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

1.2 Server i tredje land

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

1.3 Google-servrar

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

1.3.1 Överföring

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

1.3.2 Proxy

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

1.4 AWS GovCloud

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

1.4.1 Säkerhet

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

1.4.2 Frontend

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

1.4.3 Ingestion-1 (I1)

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

1.5 Aktivitet i meddelandenätverket

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

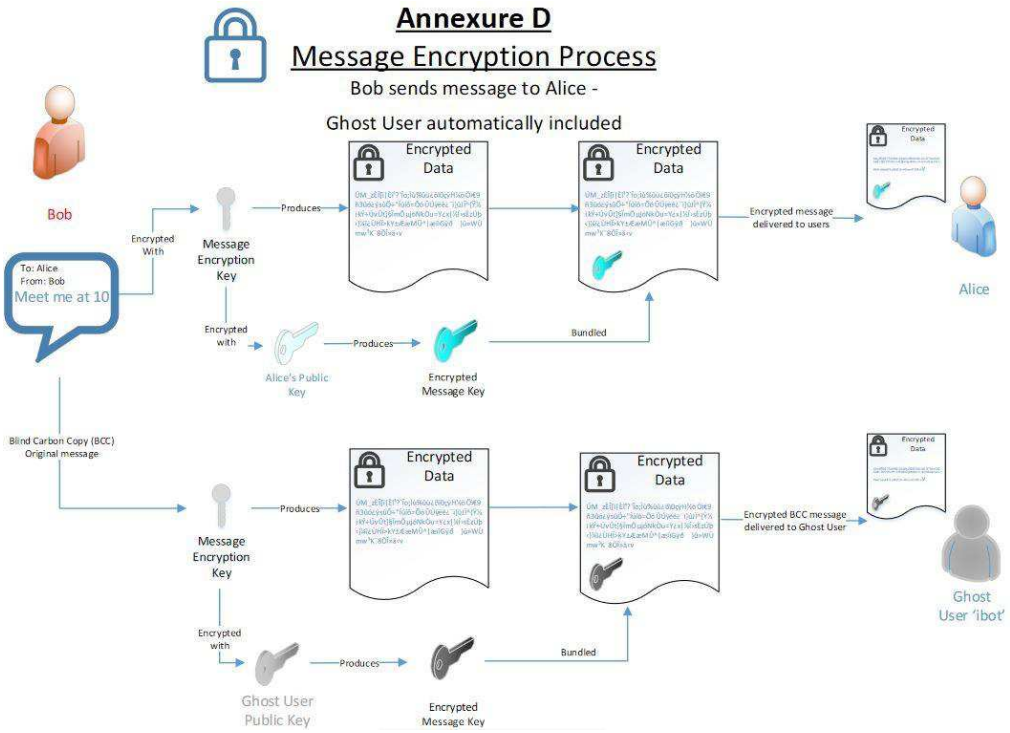


Diagram 1.B

2. SKAPANDE AV NYA DATAPAKET

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

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

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

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

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

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

2.1 Kryptering av data

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

2.2 Hur databasens skillnadsdump skapades

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

2.3 Hur listan med bilagor fastställs från skillnadsdumpen

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

2.4 Hur bilagor kopierades från fillagringen

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

2.5 Skapa det krypterade paketet

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

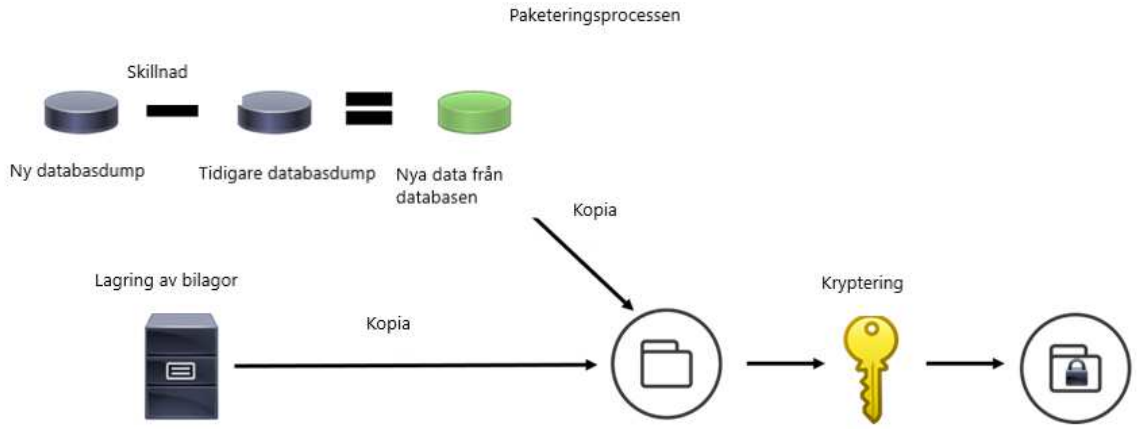


Diagram 2.A

3. ÖVERFÖRING FRÅN SERVERN I DET TREDJE LANDET TILL ÖVERFÖRINGSSERVERN

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

3.1 Program som överför data till överföringsservern

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

4. ÖVERFÖRING FRÅN ÖVERFÖRINGSSERVERN TILL AWS GOVCLOUD

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

4.1 Automatisering av program för att överföra data

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

5. BEARBETNING AV KRYPTERADE PAKET

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

5.1 Avkryptering av GPG-paket

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

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

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

5.3 Inmatning av databasdumpen till en tillfällig databas

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

6. AVKRYPTERINGSPROCESSEN

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

6.1 Avkryptering av krypterade fält i databasen

Enligt beskrivning i avsnitt 2 krypterades följande fält i databasdumpen:

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

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

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

6.1.1 Uppdatering av sökvägar för bilagor så att de är korrekta

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

6.2 Avkryptering av alla filer i bilagor

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

7. BEARBETNING AV LJUDFILER

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

7.1 Konvertera ljudfiler till användbart format

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

7.2 Ändring av tonhöjd i ljudfiler om nödvändigt

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

8. DATABASÖVERSIKT

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

8.1 Ärenden/syndikat

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

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

8.1.1 Grupper av enhetsanvändare (JID)

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

8.2 Användare av granskningsplattformen

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

Det finns tre huvudsakliga typer av användare i databasen:

- Allmänna användare
- Super users
- Administratörer

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

8.2.1 Allmänna användare

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

8.2.3 Super users

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

8.2.4 Administratörer

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

8.3 Förteckningen

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

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

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

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

8.4 Grupper

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

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

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

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

8.4.1 Avsaknad av gruppinformation

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

8.5 Produkter

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

8.5.1 Produkter i detalj

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

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

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

det tredje landet.

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

8.6 Meddelanden

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

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

I alla fyra tabeller finns följande metadatafält:

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

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

8.6.1 Fel i meddelandens tidszon

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

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

8.7 Relationer

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

Användare **tilldelad_till** *ärende*

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

8.7.1 Relation produkt till meddelande

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

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

8.7.2 Relation mellan användare och åtkomst till ärenden

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

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

8.7.3 Relationen mellan JID och ärenden

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

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

8.7.4 Relationen mellan JID och grupper

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

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

9. INMATNINGSPROCESS

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

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

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

9.1 Mata in ny information i förteckningen

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

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

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

9.2 Infoga nya grupper

9.2.1 Infoga ny gruppinformation

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

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

9.2.2 Infoga uppdateringar om medlemskap i grupper

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

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

9.3 Inmatning av meddelanden

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

9.3.1 Initialisering

Innan nya data matas in initialiseras vissa komponenter.

9.3.1.1 Svart lista

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

9.3.1.2 Tillfällig datastruktur för konversationer

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

9.3.1.3 Tillfällig datastruktur för ärende-till-JID

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

9.3.1.4 Hämta senaste meddelande-ID (MID)

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

9.3.1.5 Läs in nya meddelanden

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

9.3.2 Infoga meddelanden

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

9.3.2.1 Infoga metadata

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

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

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

9.3.2.2 Infoga efter typ

Inmatningsprocessen skiljer sig åt beroende på meddelandetyp.

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

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

9.3.2.2.2 Meddelanden av typen ”anteckning”

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

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

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

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

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

9.3.4 Tilldela meddelanden till produkter

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

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

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

9.4 Inmatning av produkter

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

9.4.1 Skapa produkter per ärende

För varje ärende verkställs stegen under 9.4.1.1 för konversationen.

9.4.1.1 Om JID i konversationen tillhör ett ärende

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

9.4.1.1.1 Skapa produkt för ärenden

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

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

9.4.1.1.2 Skapa relation för meddelande och JID till produkt

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

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

- Enhetsanvändar-ID
- Produkt-ID (PID)

Tabellen fylls också i när en ny produkt skapas.

9.4.1.1.3 Tilldela standardmarkering till produkt

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

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

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

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

9.5 Export efter inmatning

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

10. WEBBAPPLIKATION/GRANSKNINGSPLATTFORM

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

10.1 Kontroll av användaråtkomst i Hola iBot

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

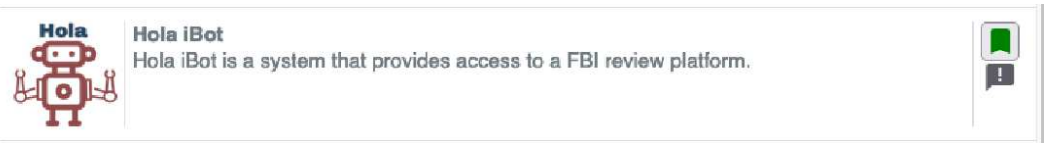
10.1.1 Åtkomstkontroll för LEEP (Law Enforcement Enterprise Portal)

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

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

10.1.2 Åtkomstkontroll i Hola iBot

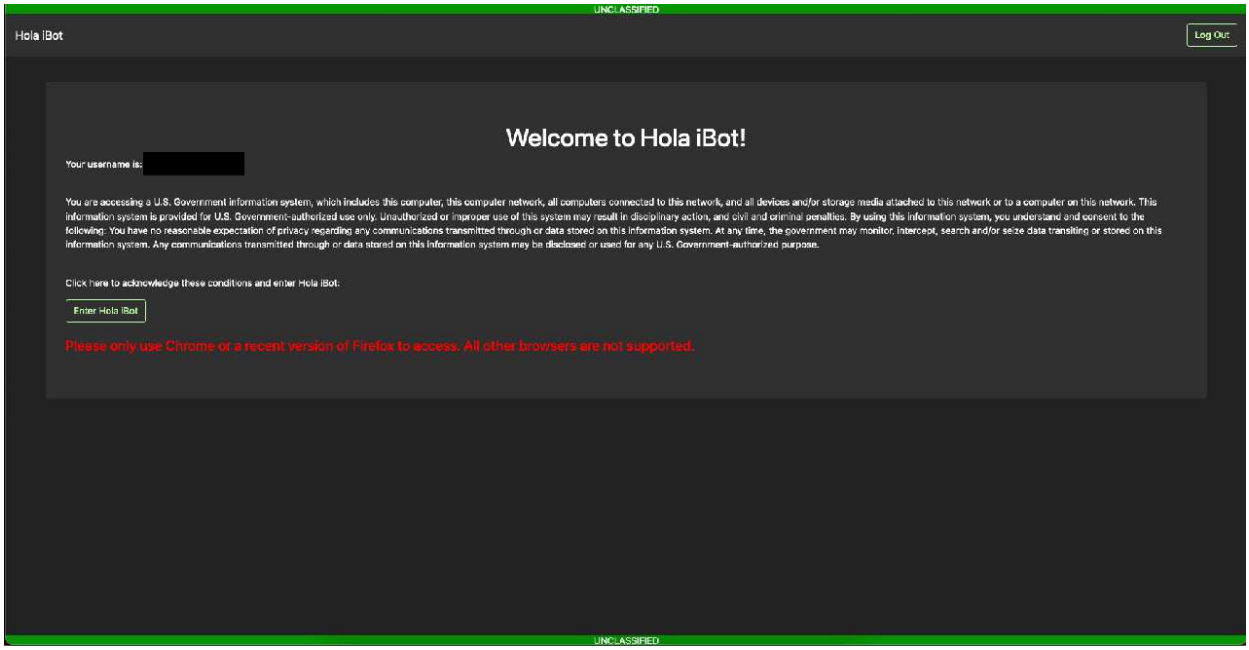
När en användare har autentiserat sig genom den LEEP-administrerade inloggningsprocessen kan användaren öppna applikationen Hola iBot genom att klicka på applikationen i listan som visas i skärmbilden nedan.



Skärmbild 10.A

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

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

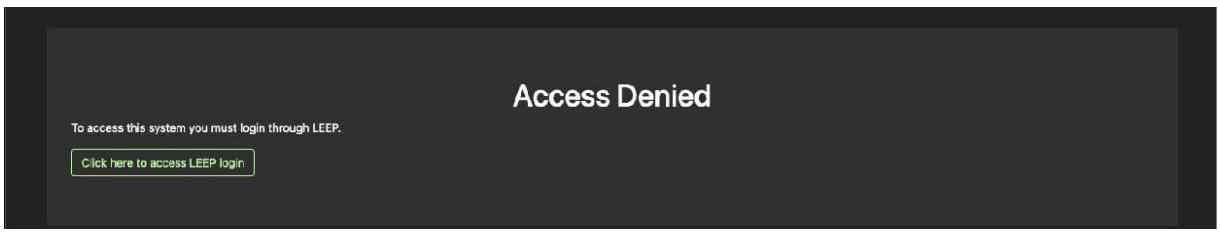


Skärmbild 10.B

Texten i varningsmeddelandet är följande (översatt till svenska):

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

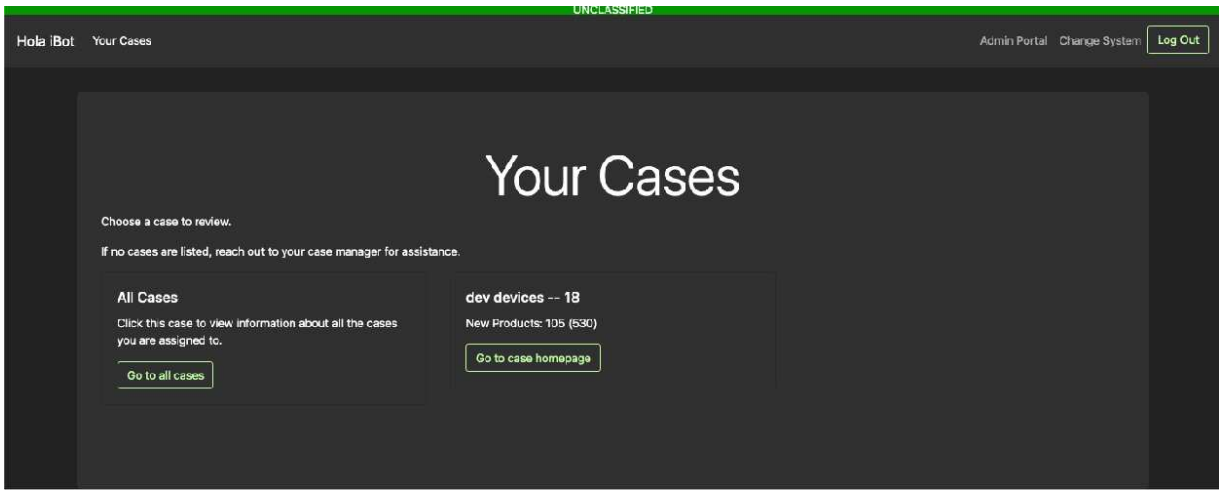
Om användaren inte finns i databasen ser de en generisk sida om nekad åtkomst. Den sidan visas i skärmbild 10.C.



Skärmbild 10.C

10.2 Ärenden i Hola iBot

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



Skärmbild 10.D

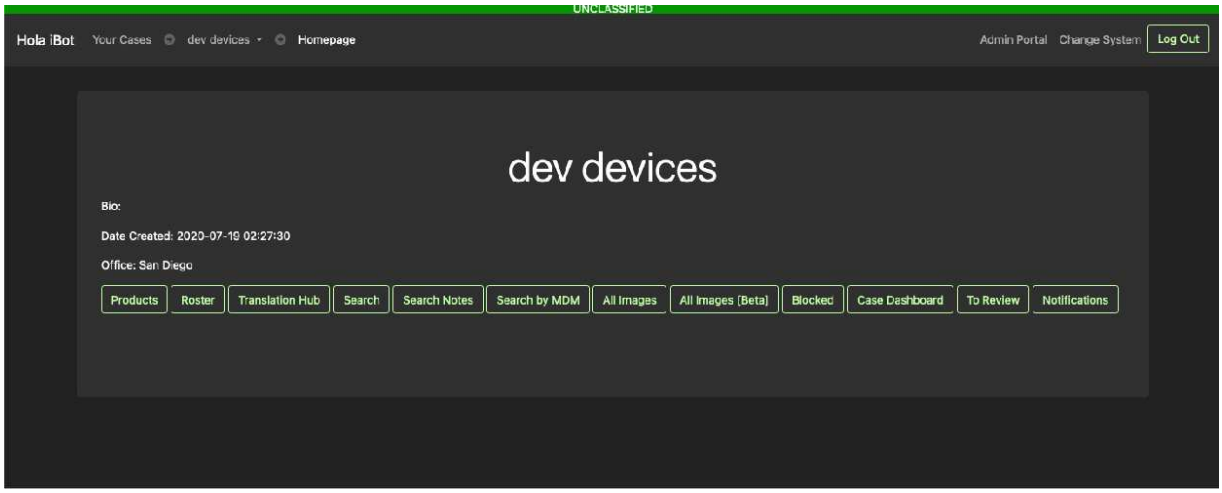
Listan med ärenden som visas på hemsidan baseras på tabellen ”tilldelad_till” enligt beskrivningen i avsnitt 8.7.2 ovan.

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

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

10.2.1 Ärendets hemsida

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



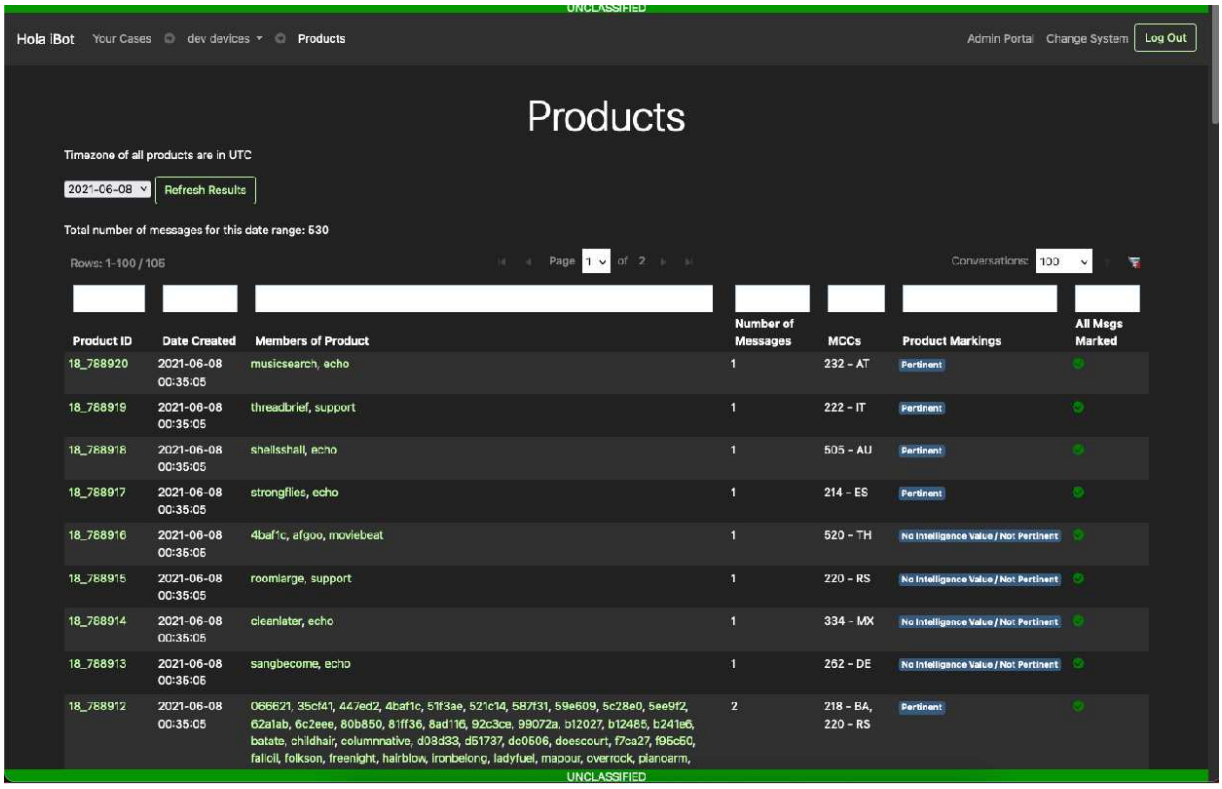
Skärmbild 10.E

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

10.3 Produktsidan

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

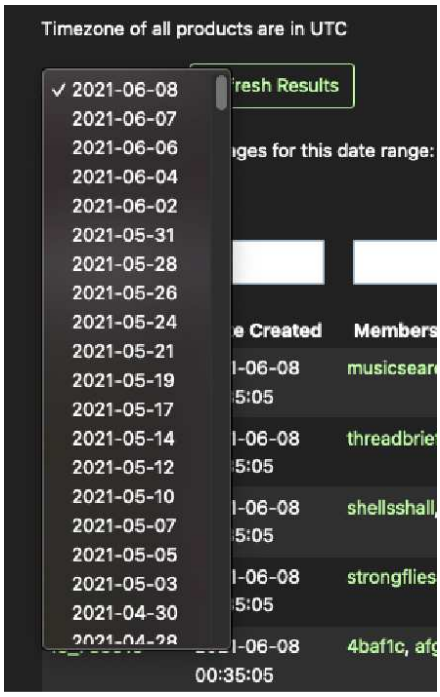
Produkter är unika konversationer för ett ärende som togs emot i ett datapaket. I skärmbild 10.F visas produktsidan för ärendet ”dev devices”.



Skärmbild 10.F

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

datapaket togs emot:



Skärmbild 10.F.1

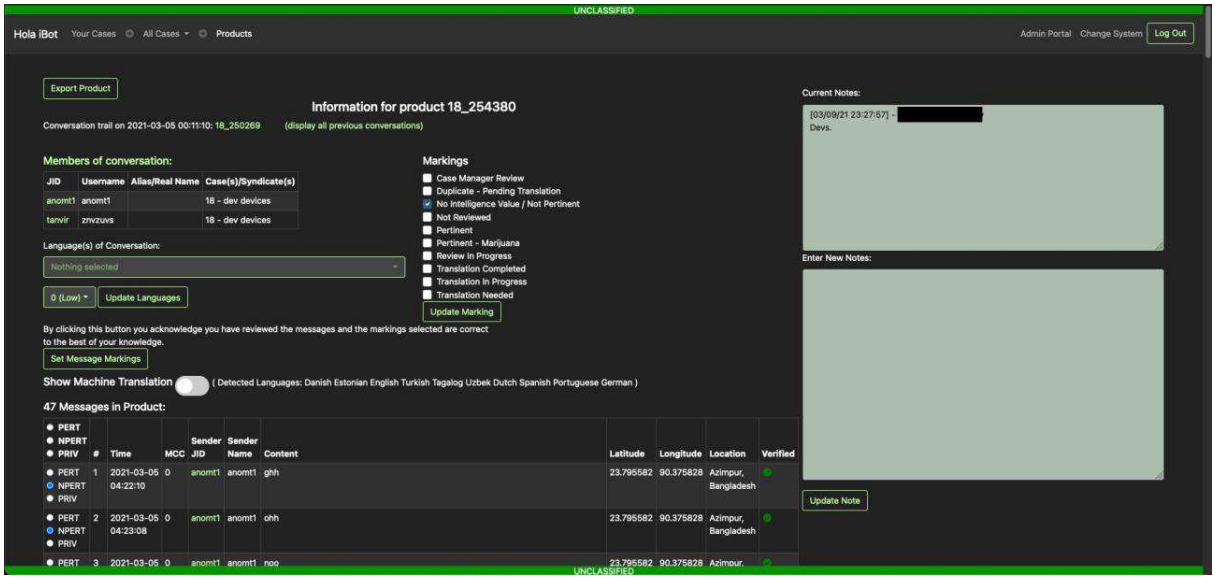
Listorna med produkter är unika per överföringsdatum. Som visas i skärmbild 10.F visas inte produkt-ID (PID) under ”Product ID” i listan över produkter. Det ”Product ID” som visas för användaren anges med ärende-ID följt av understreck och sedan det faktiska produkt-ID:t (PID). Det är ett enklare sätt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

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

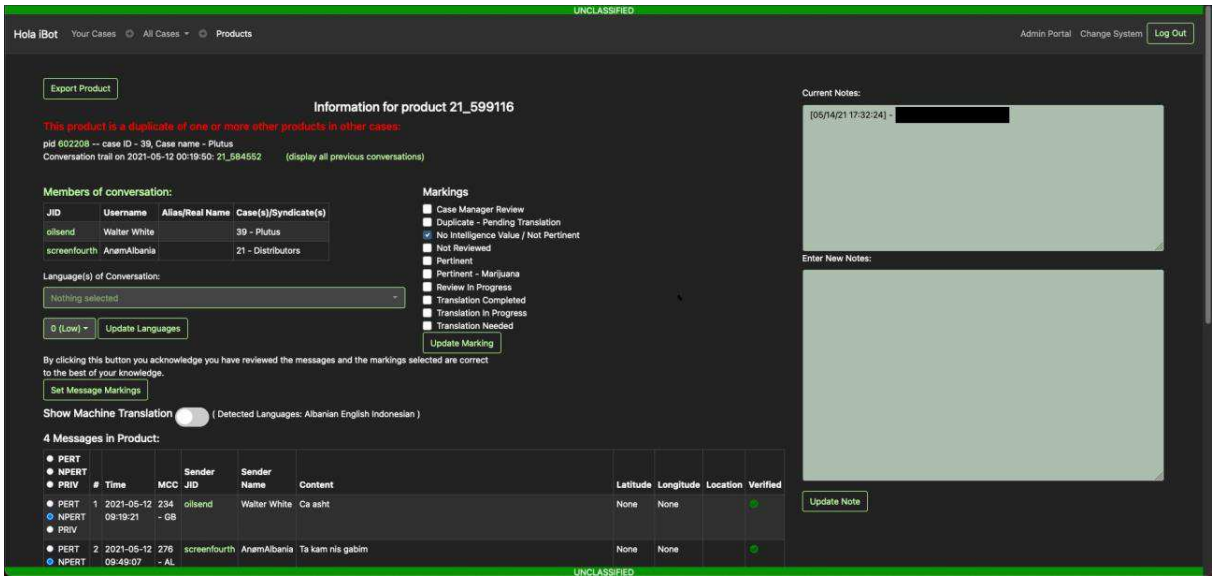
- “Date Created”
  - hämtas från fältet för skapandedatum i tabellen ”produkt”
- ”Members of Product”
  - hämtas från fältet ”JID-sträng” i tabellen ”produkt”
  - Alla JID:n som visas i den här kolumnen är länkade till JID-profilen.
    - Se avsnitt 10.7 för mer information om JID-profilen.
- ”Number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

10.4 Produktsidan

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



Skärmbild 10.G



Skärmbild 10.G.1

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

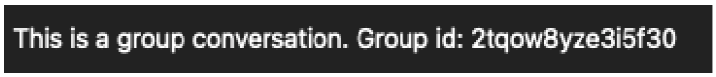
- Huruvida produkten som visas är en dubblett av en produkt i ett annat ärende.
    - I skärmbild 10.G.1 visas ett exempel på en produkt som är en dubblett, och där finns också en länk till den motsvarande dubbletten.
- Deltagarna i konversationen
    - Dessa sammanställs under inmatningsprocessen som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

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

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

10.4.1 Grupp-ID-visning

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



Skärmbild 10.G.2

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

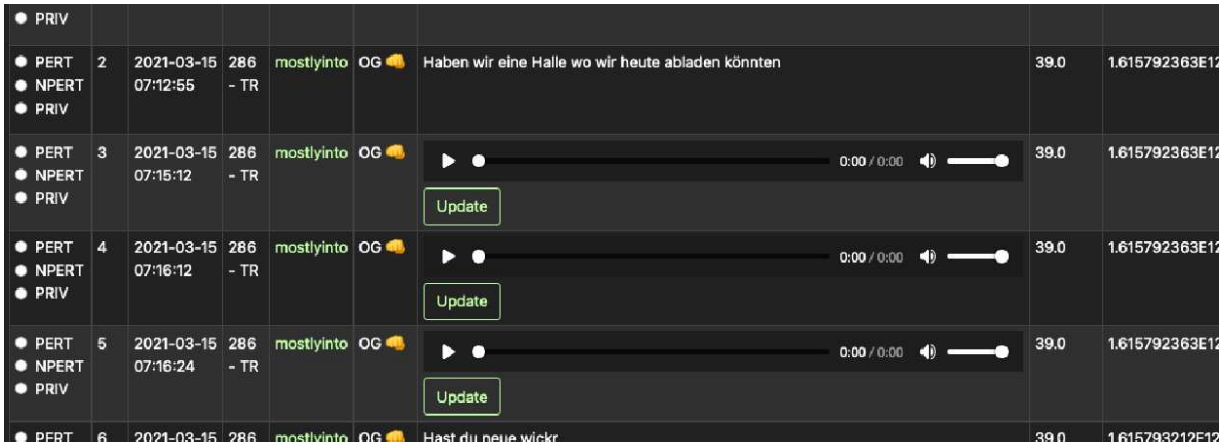
Alla meddelanden med bilagor visas inline, som textmeddelanden. Meddelanden med bilagor kan också ha en markering som tilldelas av användare av granskningsplattformen. I databasen iBot_dec finns en tabell med namnet ”bilaga_har_markering” som gör det möjligt att markera bilagor med textbaserade beskrivningar.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

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

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

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

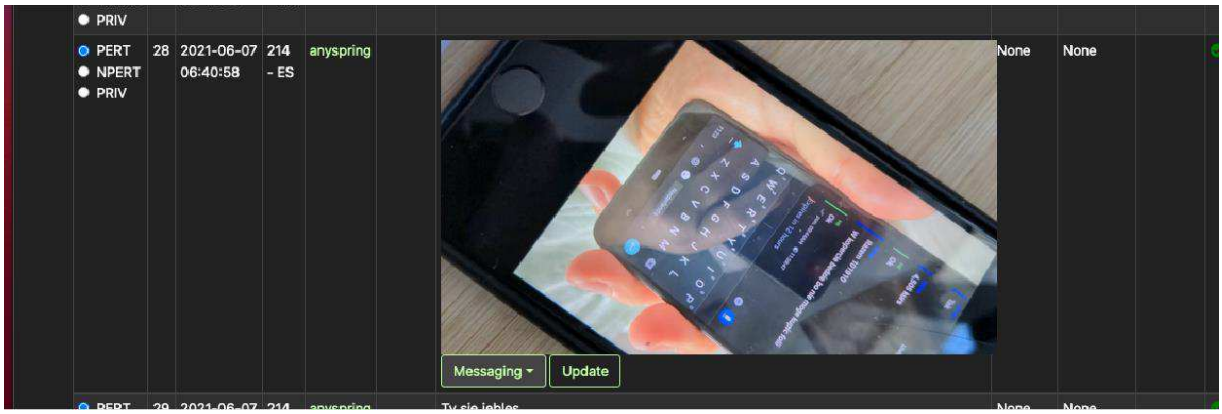
I skärmbild 10.G.3 visas ett exempel på några PTT-meddelanden.



Skärmbild 10.G.3

10.4.2.2 Bildmeddelanden i Hola iBot

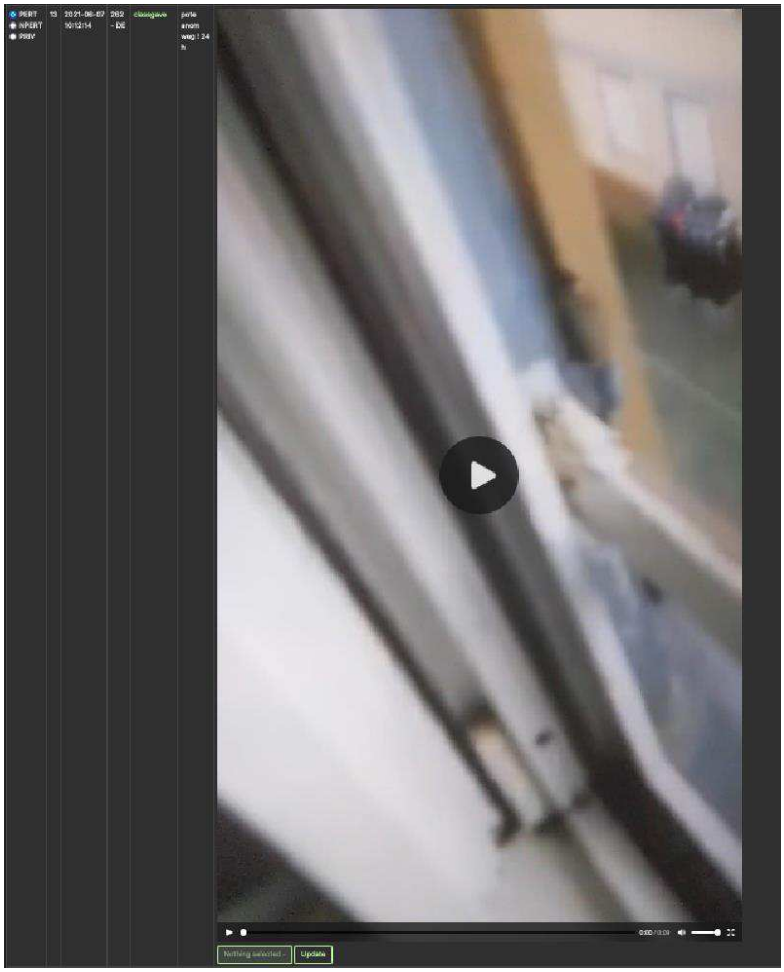
I skärmbild 10.G.4 visas ett exempel på ett bildmeddelande som visas inline.



Skärmbild 10.G.4

10.4.2.3 Videomeddelanden i Hola iBot

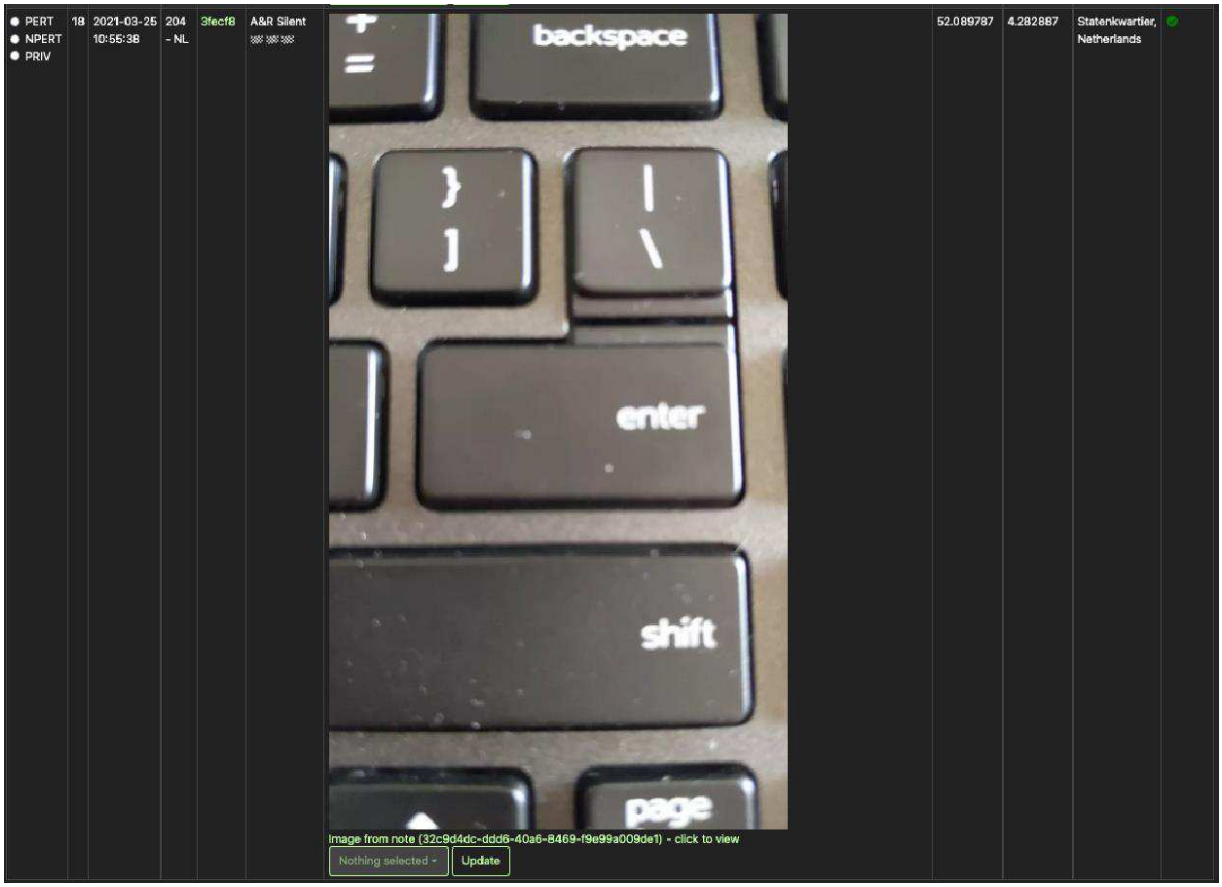
I skärmbild 10.G.4 visas ett exempel på ett videomeddelande i Hola iBot.



Skärmbild 10.G.5

10.4.2.4 Anteckningsmeddelanden i Hola iBot

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



Skärmbild 10.G.6

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

10.5 Översättningar

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

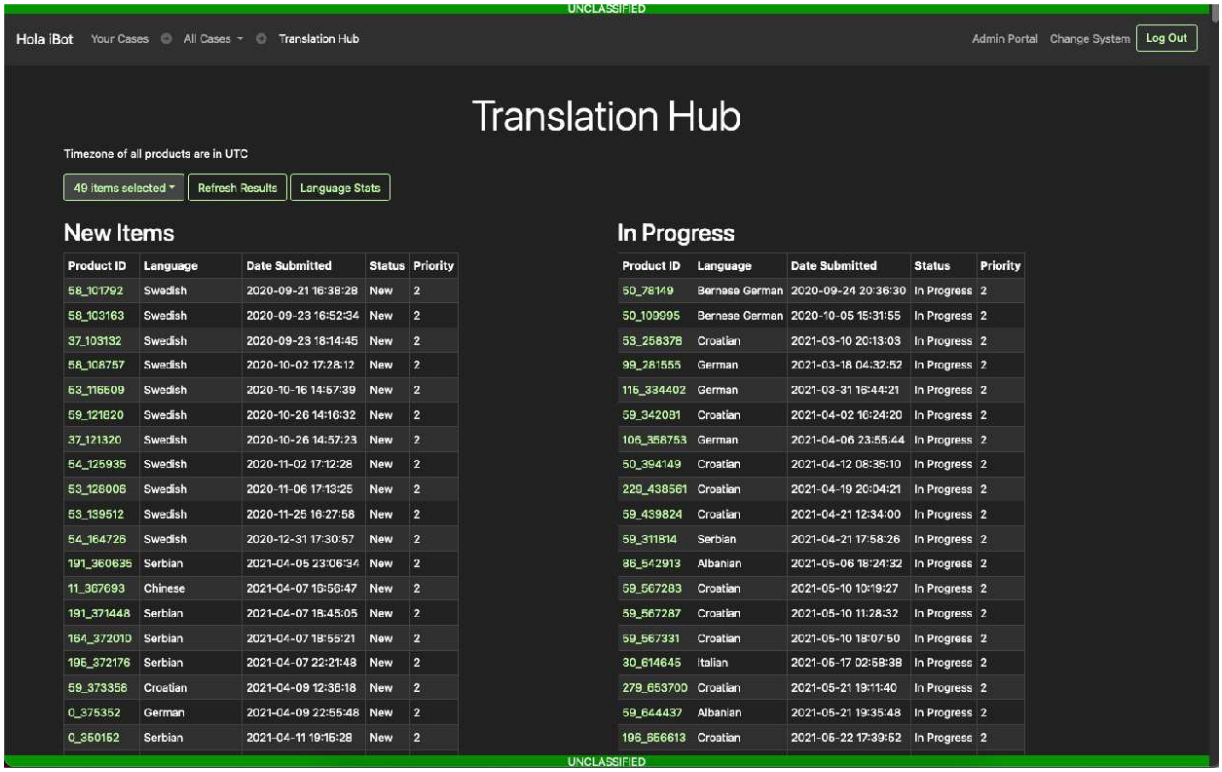
- Språk
  - Namnet på språket som tilldelas till produkten.
  - Exempel: ”engelska”, ”spanska”
- Produkt-ID (PID)
  - PID för den produkt som språket tilldelas till.
- Status
  - Det här fältet visar status på översättningen.
  - Det här fältet kan anges till ”ny”, ”pågående” eller ”klar”.
- Prioritet

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

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

10.5.1 Translation Hub

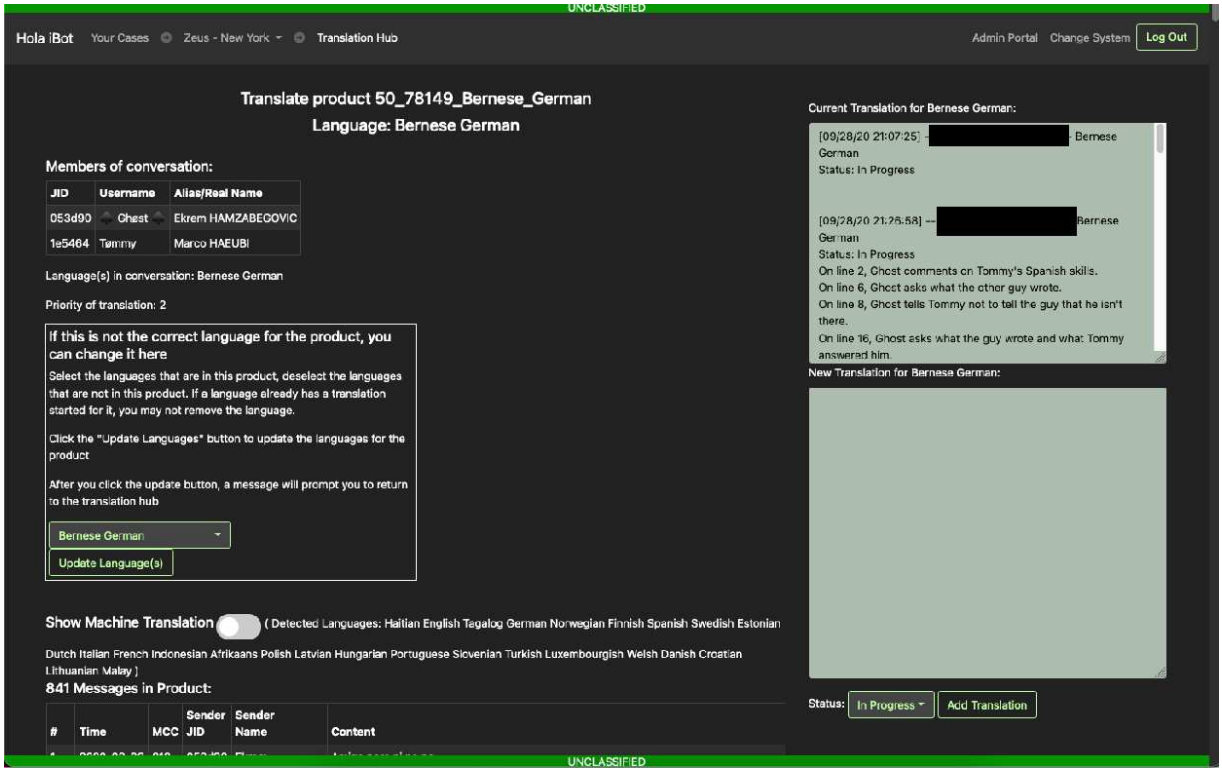
I Translation Hub finns alla översättningar som har lämnats in av användare för produkter. Skärmbild 10.H visar Translation Hub.



Skärmbild 10.H

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

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



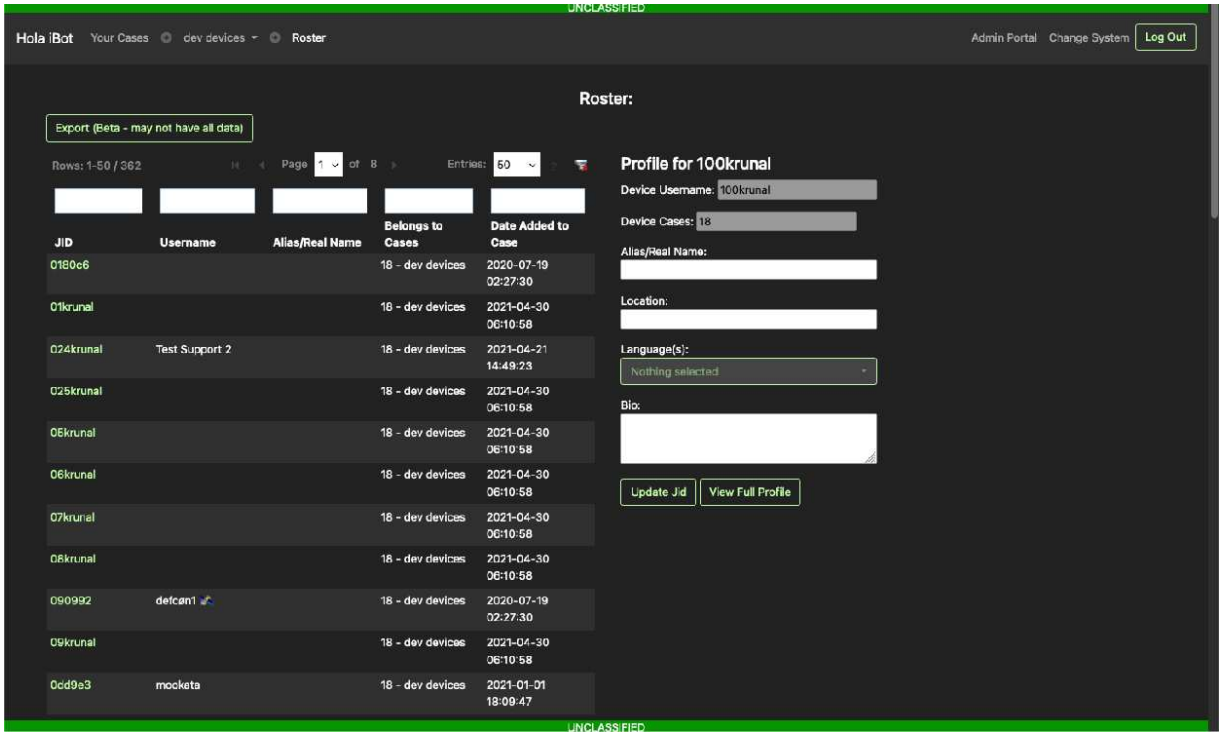
Skärmbild 10.I

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

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

10.6 Förteckningssidan

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



Skärmbild 10.J

Sidan är delad vertikalt i två rutor.

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

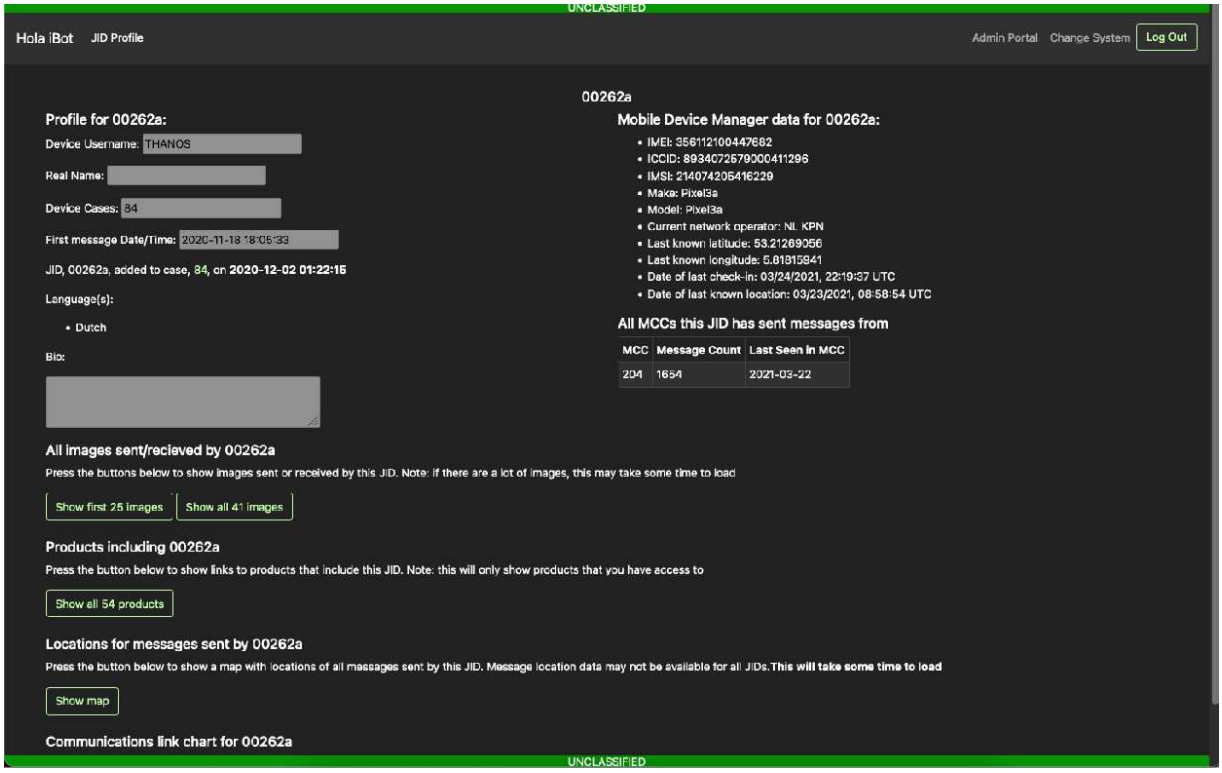
Det går att klicka på varje rad i tabellen och då fylls den högra rutan på med följande ytterligare information, som kan redigeras:

- Alias/verkligt namn
- Plats
- Språk
- Biografi

I avsnitt 8.3 finns mer information om fälten i förteckningen.

10.7 JID-profil

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



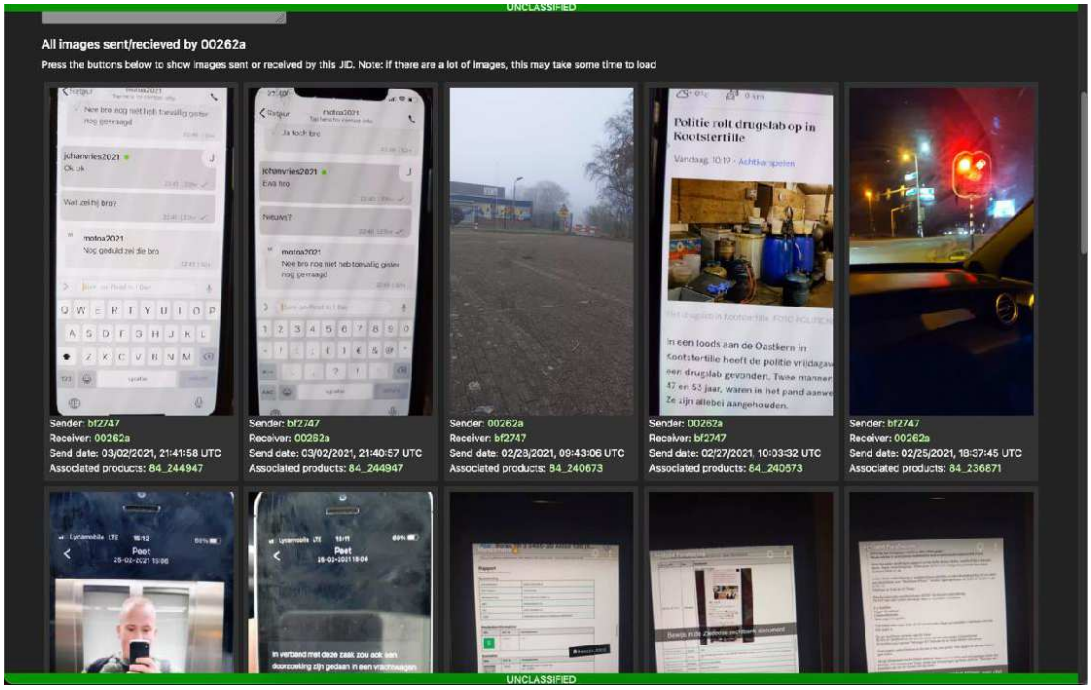
Skärmbild 10.K

Resten av avsnitt 10.7 hänvisar till skärmbild 10.K.

10.7.1 Information om enhetsanvändaren (JID)

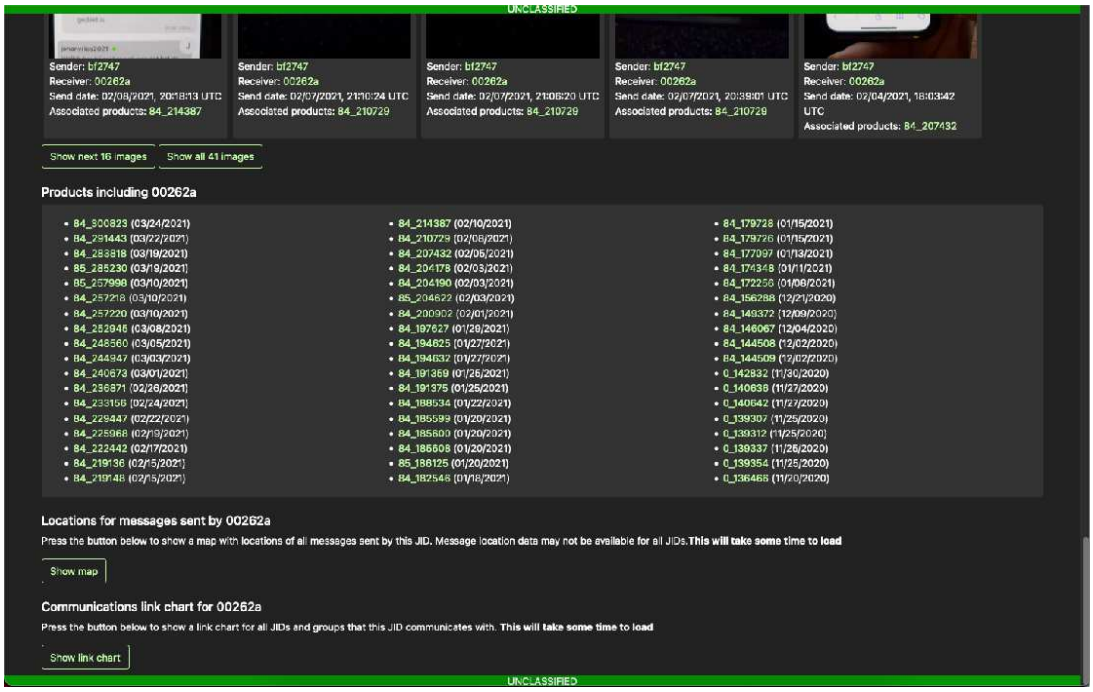
Alla förteckningsdata om enhetsanvändaren (JID) visas på JID-profilsidan. Det finns andra data som också kan hämtas från JID-profilsidan, t.ex.:

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



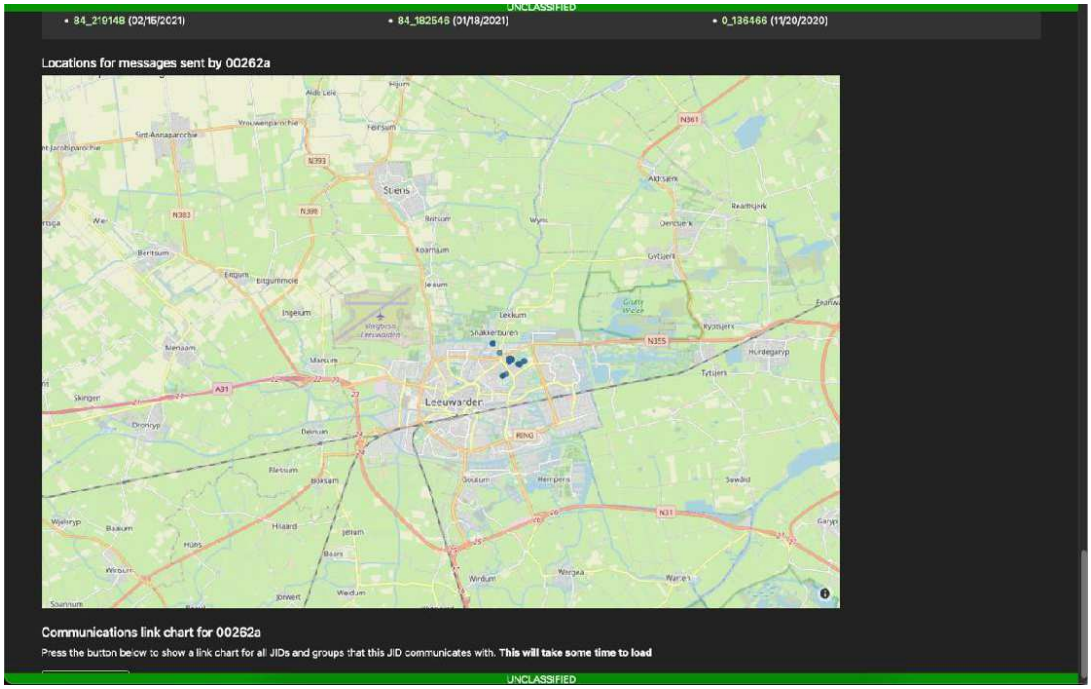
Skärmbild 10.K.1

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



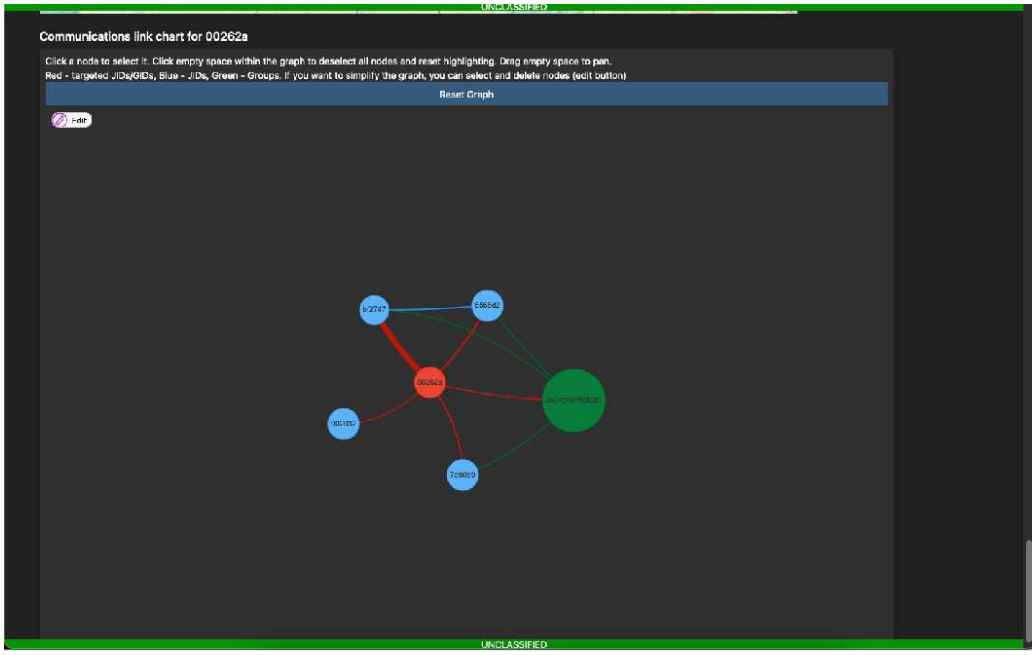
Skärmbild 10.K.2

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



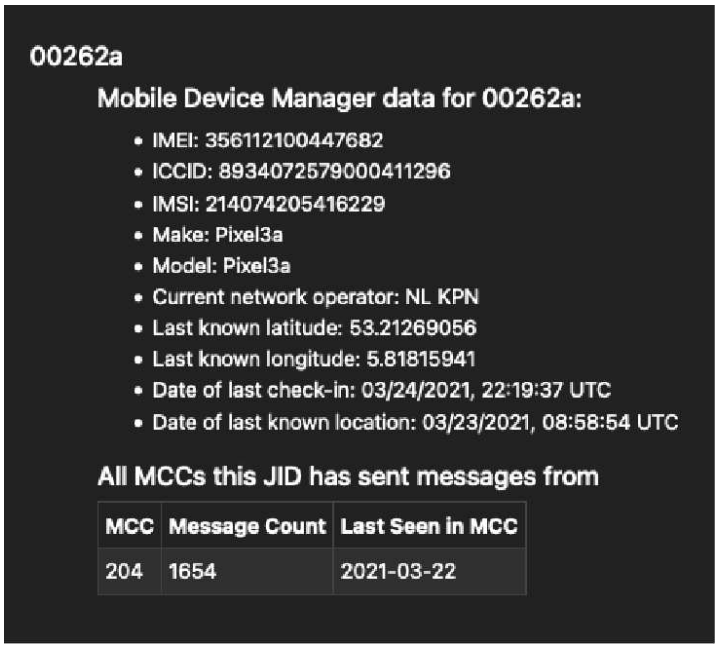
Skärmbild 10.K.3

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



Skärmbild 10.K.4

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



Skärmbild 10.K.5

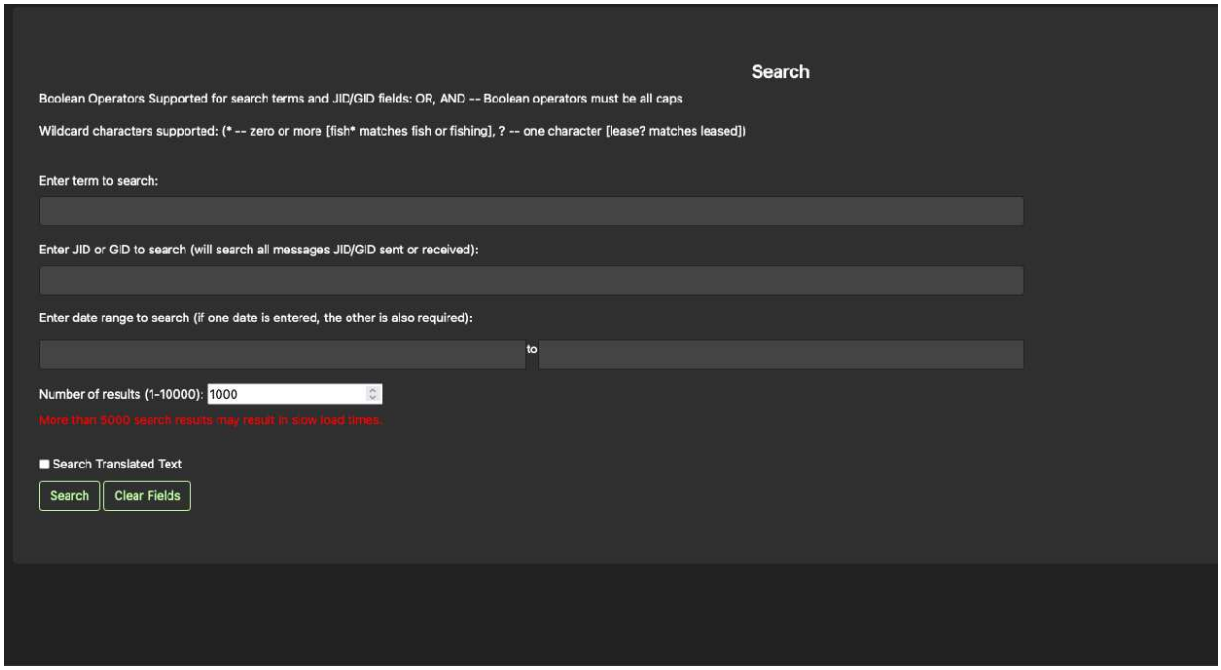
10.8 Andra sidor

10.8.1 Sökning

På söksidan kan man söka i:

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

Det går också att ange datumintervall för att filtrera resultaten.



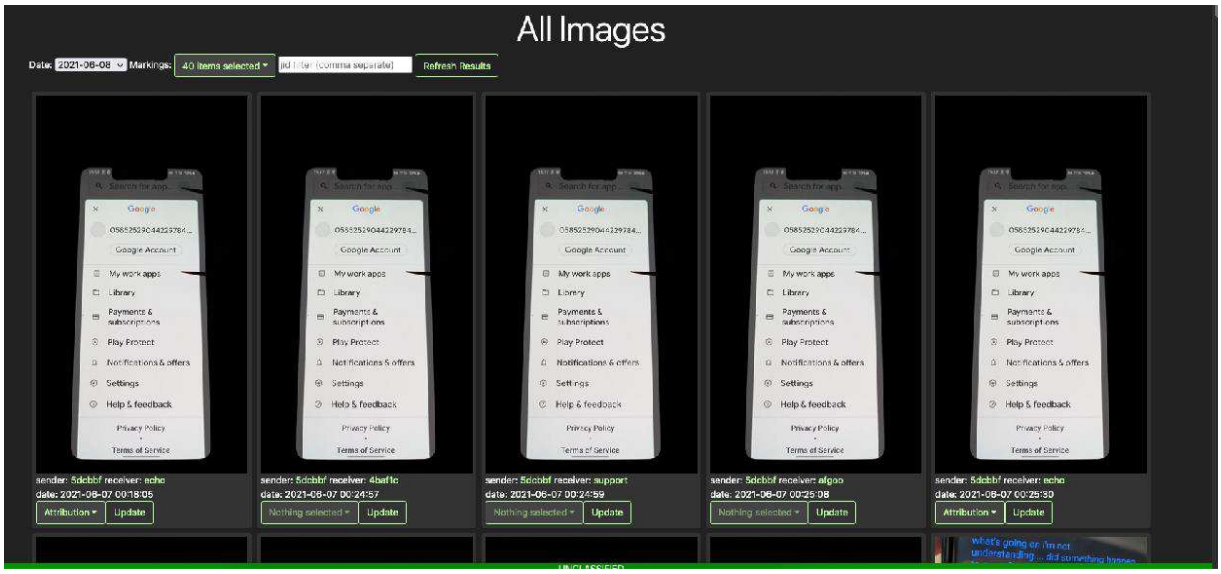
Skärmbild 10.L

10.8.2 Sök i anteckningar

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

10.8.3 Alla bilder

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



Skärmbild 10.M

10.8.4 Blockerade

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

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

11. MLAT-EXPORT

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

11.1 Hämtning av alla bifogade filer

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

11.2 Hämtning av slutlig MySQL-databasdump

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

11.3 Skapa MLAT-exporter

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

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

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

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

BILAGA A

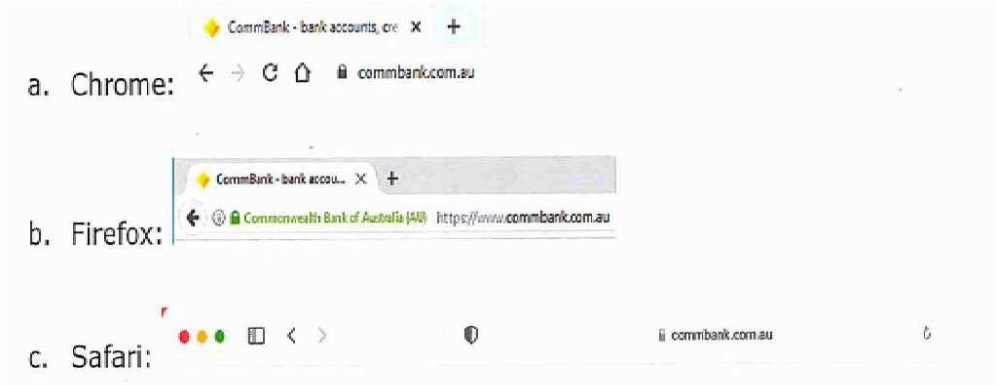
A.1 Kryptering med offentlig nyckel

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

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

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

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



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

A.2 Hash

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

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

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

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

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

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

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

A.3 ANØM-PLATTFORMEN

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

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

A.3.1 End-to-end-kryptering

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

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

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

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

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

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

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

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

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

A.4 Portalen

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

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

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

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

A.5 Enheter

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    b. serienumret 238324 och

    c. kontrollsiffran 2.

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

A.5 Nätverksanslutning till plattformen

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

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

A.6 MDM-komponenten

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

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

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

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

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

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

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

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

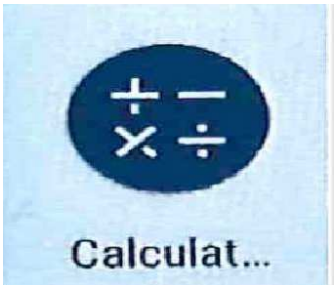
g. Rapportera information om enheten med jämna mellanrum, t.ex. enhetens unika IMEI-nummer, efterlevnad av MDM-policyn, enhetens startinläsare och version av operativsystemet samt enhetens status, t.ex. batterinivå och ledigt minnesutrymme.

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

A.7 ANØM-applikationen

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

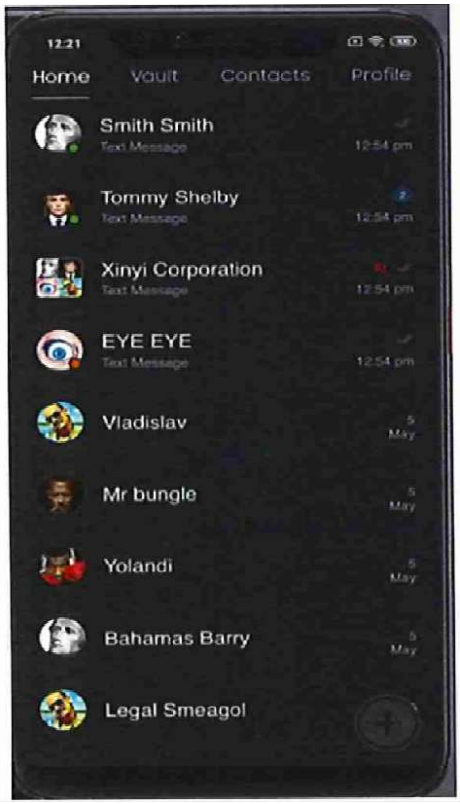
40. Här är ett exempel på appikonen som den såg ut på vissa enheter (ikonens utseende varierade beroende på version av operativsystemet):



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

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

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



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

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

själva verket raderas eventuellt bevismaterial.

A.7.1 ANØM-applikationsattribut

A.7.1.1 Identifierare för användare

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

A.7.1.2 Användarens visningsnamn

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

A.7.1.3 Valvet

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

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

A.7.1.4 Meddelanden

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

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

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

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

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

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

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

56. Möjlighet att ändra tonhöjd

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

A.7.1.5 Självförstörande meddelanden

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

A.8 Data spelas in från plattformen

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

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

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

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

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

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

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

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

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

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

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

    i. Se avsnitt 8.6.1 för information om tidszonsavvikelser.

A.8.2 Metadata för meddelanden

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

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

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

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

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

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

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

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

A.9 Autentisering och integritet

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

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

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

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

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

ORDLISTA

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

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

inför inmatningen.

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

ÅKLAGARMYNDIGHETEN
Nationella åklagaravdelningen
Riksenheten mot internationell och organiserad

Kammaråklagare Ewamari Häggkvist

Datum
2021-06-22
Ert datum

Dnr
AM-72527-21
Er beteckning

BESLUT 2021-06-22

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

JID	**Användarnamn**
whateven	Worldwide
04522e	Uptown
whomsecret	“fyra gurkor”
adcf1d	Havana
b1d66e	Zedd

överlämnas till AM-54003-21 (åklagare Inger Sandström).

Ewamari Häggkvist

Postadress
Box 57
101 21 Stockholm

Gatuadress

Telefon
+46 10 562 50 00

Telefax

E-post

Webbadress
www.aklagare.se

ÅKLAGARMYNDIGHETEN
Nationella åklagaravdelningen
Riksenheten mot internationell och organiserad

Kammaråklagare Ewamari Häggkvist

Datum
2021-06-22
Ert datum

Dnr
AM-72508-21
Er beteckning

BESLUT 2021-06-22

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

JID	**Användarnamn**
56d3f9	Microsoft
225375	Teamsters
c3b5d4	rampage

överlämnas till AM-54003-21 (åklagare Inger Sandström).

Ewamari Häggkvist

Postadress
Box 57
101 21 Stockholm

Gatuadress

Telefon
+46 10 562 50 00

Telefax

E-post

Webbadress
www.aklagare.se

Polisen

Bilaga - Skäligen misstänkt

Enhet	Diarienr
Polisregion Bergslagen, Grova brott 1 PO Örebro	5000-K402690-21

Skäligen misstänkt person	Personnr
Yavuz, Zafer	19880913-0977

Identifierad	Kontrollsätt	Kommentar
Ja	Körkort (svenskt)	

Polisen

Personalia och dagsbotsuppgift

Utskriftsdatum
2021-10-29

Namn			Personnummer
Yavuz, Zafer			19880913-0977
Tilltalsnamn	Kallas för	Öknamn	Kön
			Man
Födelseförsamling	Födelselän	Födelseort utland	
		Izmir	
Medborgarskap	Hemvistland	Telefonnr	
Sverige		0736199074: Hemtelefon e-anmälan 5000-K556	

Adress
Engelbrektsgatan 52 LGH 1002
702 13 Örebro

Folkbokföringsort	Senast kontrollerad mot folkbokföring
Örebro	2021-02-17

Föräldrars/Vårdnadshavares namn och adress (beträffande den som inte fyllt 20 år)

Utbildning

Yrke / Titel

Arbetsgivare | Telefonnr

Anställning (nuvarande och tidigare)

Arbetsförhet och hälsotillstånd

Kompletterande uppgifter

Uppgiven inkomst	Bidrag	Hemmavarande barn under 18 år
300000	Pågående skuldsanering hos kronofogden.	
Försörjningsplikt		Skulder
		450000
Förmögenhet		

Kontroll utförd

Taxerad inkomst	Taxeringsår
347700	2020
Taxeringskontroll utförd av	Datum
Pinsp. P. Wirolainen	2021-04-11

Underrättelse/Delgivning jml RB 23:18a

Enhet
Polisregion Bergslagen, Grova brott 1 PO Örebro

Ärende

Diarienr
5000-K402690-21

Handläggare
Eriksson, Jörgen

Gärning
Synnerligen grovt narkotikabrott

Berörd person

Personnr	Efternamn	Förnamn
19880913-0977	Yavuz	Zafer

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd	Delgiven info. om ev. förenklad delgivning
2021-10-08	2021-10-25	2021-10-28	

Underrättelsesätt
Skriftligt

Notering

Resultat av underrättelsen/delgivningen
Ej erinran

Försvarare

Namn
Neo Barsoum Barstedt

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
2021-10-08	2021-10-25	2021-10-25

Underrättelsesätt
Skriftligt

Notering
FU-protokoll översänt via krypterad e-post till advokaten

Resultat av underrättelsen/delgivningen
Ej avhörts