Polisen

Protokollbilaga

Åklnr
AM-54003-21

Signerat av
Jörgen Eriksson

Arkiv/Åkl. ex

Enhet
Polisregion Bergslagen, Grova brott 1 PO Örebro

Signeringsdatum
2021-10-29 09:32

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**

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	2021-10-22	2021-10-26	2021-10-28
Försvarare Neo Barsoum Barstedt, förordnad 2021-04-11	2021-10-22	2021-10-26	2021-10-26

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

Notering

Innehållsförteckning

IT-avdelningen

Anom

Beskrivning av Polismyndighetens hantering av Anom-data

Rapport
Version 1.0
2021-10-19

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

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

Diarienr. AXX
Tryck Polisens tryckeri

Sammanfattning

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

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

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

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

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

Innehållsförteckning

1 Inledning

1.1 Bakgrund

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

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

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

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

1.2 Syfte

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

1.2.1 Avgränsning

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

1.3 Hänvisning till OTS Technical Details

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

2 MLAT exporter

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

2.1 Beskrivning och hantering av fysiskt media

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

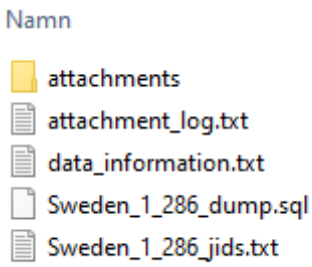
Samtliga enheter har efter ankomst speglats och hanterats enligt gängse rutiner av IT-forensik 1, Utredningsenheten, Polisregion Stockholm.

2.2 Innehåll fysiskt media

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

För varje enhet finns denna uppsättning av filer

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



Figur 1. Exempel på filstruktur innehåll, syndikat 286

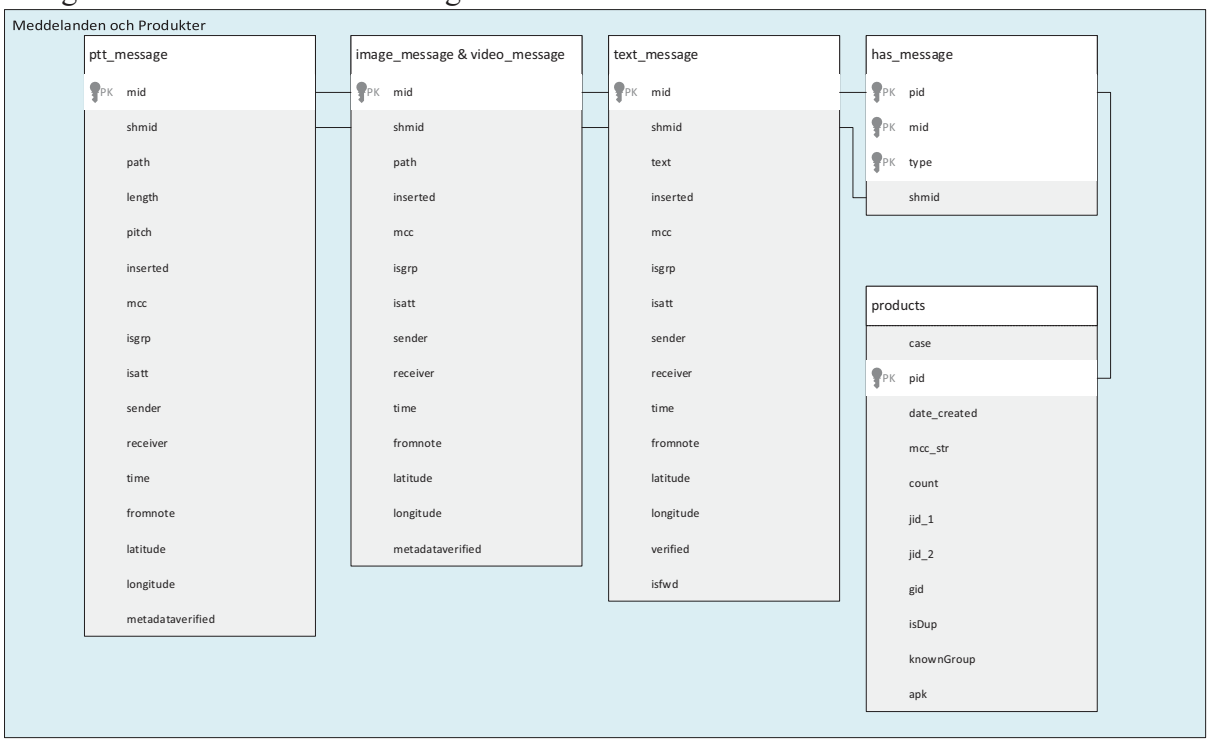
2.2.1 Maskininstruktioner

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

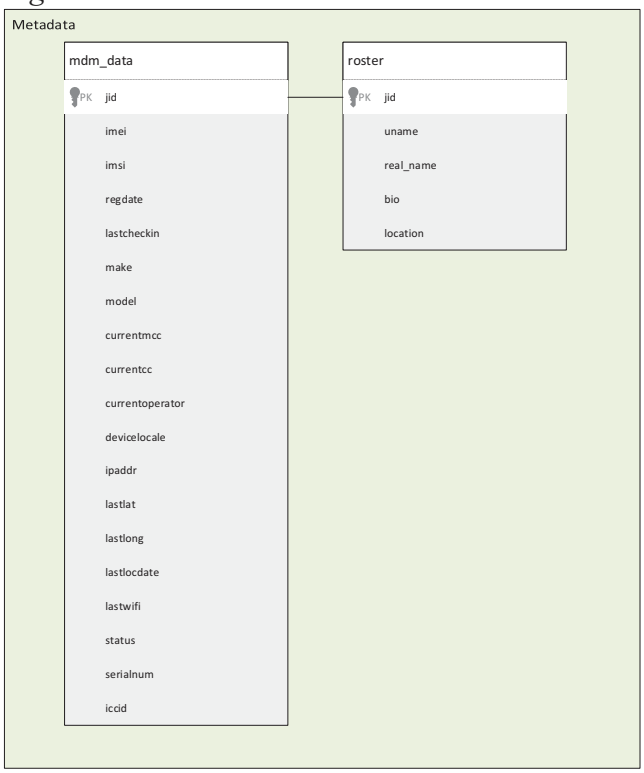
- Has_message
- Image_message
- Mdm_data
- Products
- Ptt_message
- Roster
- Text_message
- Video_message

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

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



Figur 2 Databasstruktur meddelanden



Figur 3 Databasstruktur metadata

2.2.2 Bifogade filer

I katalogen attachments återfinns tre underordnade kataloger

- Audio

- Video
- Images

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

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

2.2.3 Metadata

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

3 Delningsförfarande

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

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

4 Behandling av information

4.1 Extrahering från databas per JID

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

4.2 Filformat – TSV

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

4.3 Textkodning i Base64

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

4.4 Hänvisning till Media

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

4.5 Deduplicering av meddelanden

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

4.5.1 Anledning till deduplicering

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

4.5.2 Metod

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

4.5.3 Verifiering

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

4.6 Alias-information

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

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

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

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

4.7 Dekodning och presentation av källmaterial

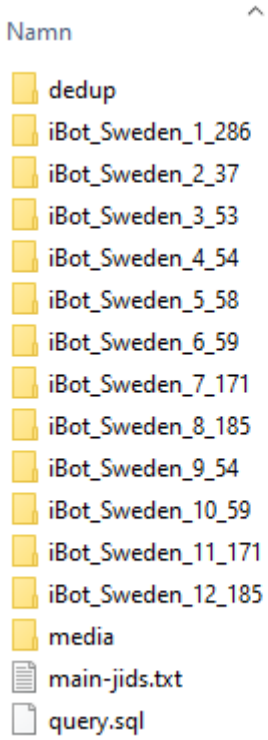
Samtliga TSV-filer med rådata från databasexport och all hänvisat media har levererats till förundersökning för vidare analys.

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

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

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

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



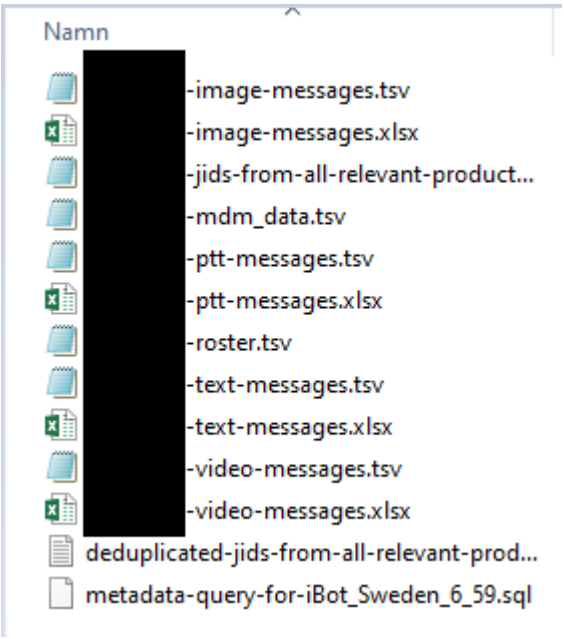
Figur 4 Katalogstruktur exporter

Nedan följer en beskrivning av innehållet i ovan nämnda kataloger.

4.7.1 Per databas

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

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



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

Kolumnerna är uppbyggda på följande vis:

<TABELL>_<FÄLT>

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

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

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

För fältordning i TSV-filer, se bilaga 2.

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

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

4.7.1.2 <JID>-text-messages

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

4.7.1.3 <JID>-ptt-messages

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

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

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

4.7.1.5 <JID>-mdm_data

Innehåller samtlig tillgänglig Mobile Device Management-information för aktuell JID

4.7.1.6 <JID>-roster

Innehåller samtlig tillgänglig roster-information för aktuell JID

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

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

4.7.2 Dedup

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

- Alias
- JID
- mid

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

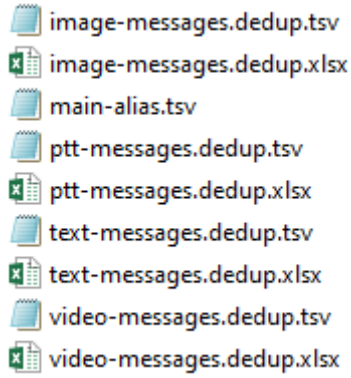


Fig 6, Innehåll dedup

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

4.7.3 Media

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

5 Källförteckning

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

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

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

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

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

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

6 Bilagor

Bilaga 1 – Data_information.txt

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

Contained on this drive are the following files/directories:

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

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

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

```
CREATE TABLE `has_message` (
  `pid` int(11) NOT NULL,                    //product ID
  `mid` int(11) NOT NULL,                    //message ID
  `type` varchar(20) NOT NULL,               //1 is text, 2 is image, 3 is ptt, 4 is video
  `shmid` varchar(50) DEFAULT NULL,
 PRIMARY KEY (`pid`,`mid`,`type`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
CREATE TABLE `image_message` (
  `mid` int(11) NOT NULL,                          //message ID
  `shmid` varchar(50) NOT NULL,                    //message UUID
  `path` varchar(100) NOT NULL,                    //image file name
  `inserted` timestamp NOT NULL DEFAULT current_timestamp(),
  `mcc` varchar(20) NOT NULL,
  `isgrp` int(2) NOT NULL DEFAULT 0,               //if it's from a group message
  `isatt` int(2) NOT NULL DEFAULT 0,
  `sender` varchar(50) NOT NULL,
  `receiver` varchar(50) NOT NULL,
  `time` timestamp NOT NULL DEFAULT current_timestamp(),
  `fromnote` int(2) NOT NULL DEFAULT 0,            //if it's from a note attachemt
  `latitude` varchar(512) DEFAULT NULL,
  `longitude` varchar(512) DEFAULT NULL,
```

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

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

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

Bilaga 2 – Fältordning TSV-Filer

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

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

<JID>-text-messages

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

<JID>-ptt-messages

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

<JID>-mdm_data

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

<JID>-roster

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

Bilaga 3 Exempel databasfrågor

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

Bild-meddelanden

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

Ljud-meddelanden

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

Text-meddelanden

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

Video-meddelanden

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

Deltagande JID:ar

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

polisen.se

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

Polisen

IT-avdelningen

Anøm

Beskrivning av information i Anom-data

Rapport
Version 1.0
2021-10-19

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

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

Diarienr. AXX
Tryck Polisens tryckeri

Sammanfattning

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

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

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

Innehållsförteckning

1 Inledning

1.1 Bakgrund

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

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

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

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

1.2 Syfte

Dokumentet syftar till att beskriva det material som mottagits i MLAT.

1.3 Hänvisning till OTS Technical Details

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

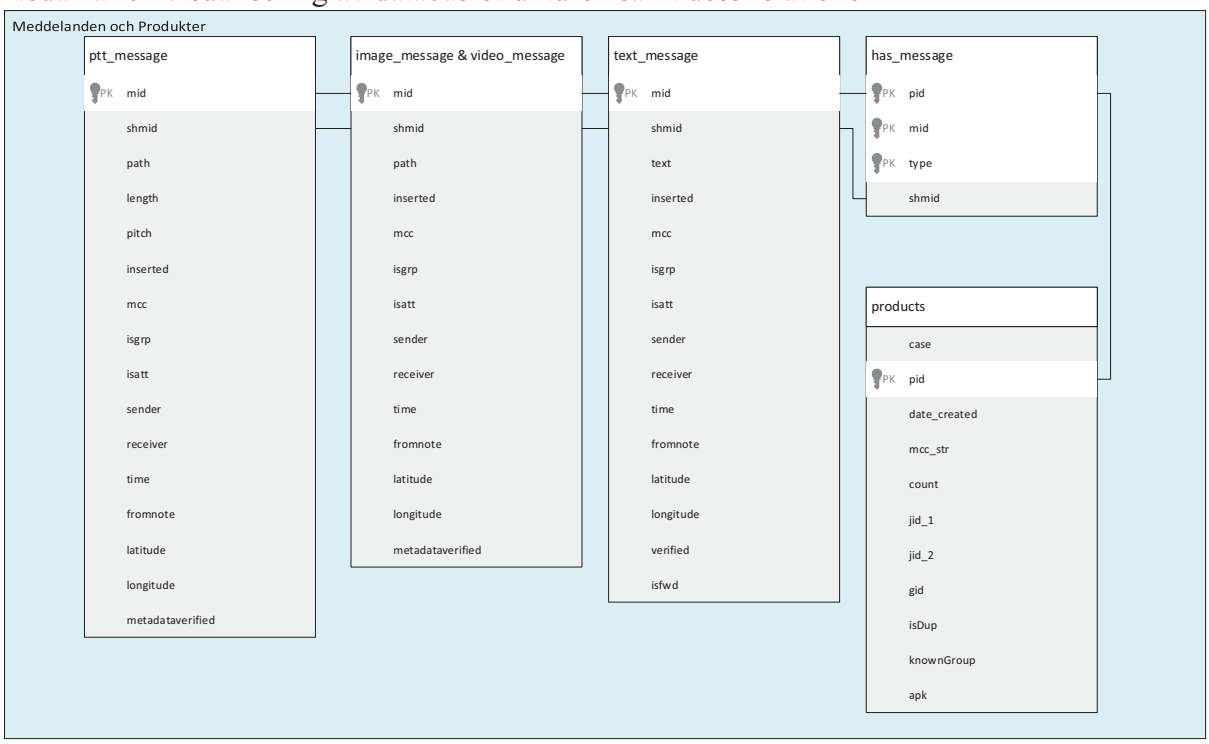
2 Innehåll i MLAT exporter

2.1 Databasstruktur

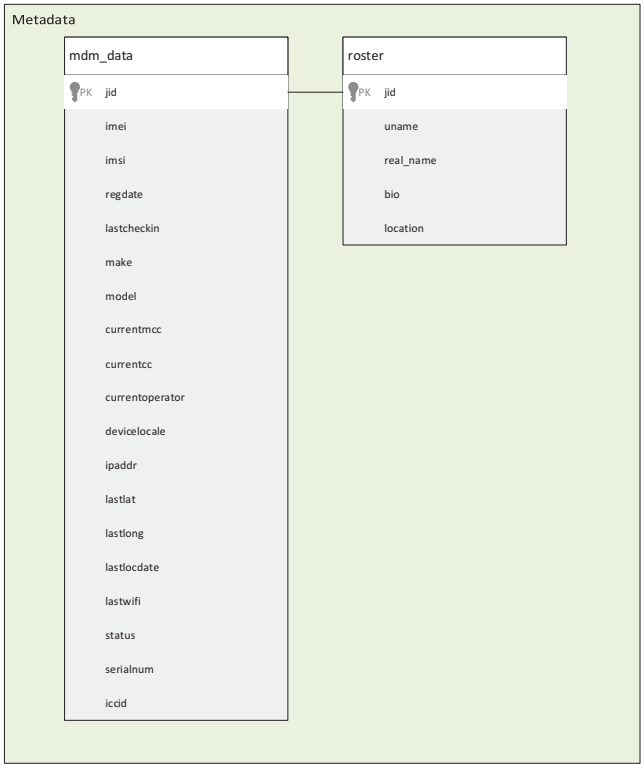
Varje MLAT-export innehåller instruktioner för att bygga upp en SQL-databas innehållandes följande tabeller:

- Has_message
- Ptt_messages
- Image_messages
- Video_messages
- Text_messages
- Products
- Mdm_data
- Roster

Nedan är en visualisering av databas-strukturen samt dess relationer



Figur 1 Databasstruktur meddelanden



Figur 2 Databasstruktur metadata

2.2 Databasinformation

Nedan följer en kort beskrivning av tabeller och dess innehåll.

2.2.1 Has_message

Tabellen beskriver relationerna mellan produkter och meddelanden.
Innehåller följande fält:

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

2.2.2 Ptt_message

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

- Mid – Meddelande-ID, återfinns även i has_message.
- Shmid – Meddelande-UUID, återfinns även i has_message
- Path – Sökväg till aktuell media-fil.
- Length – Tomt fält
- Pitch – Ursprunglig tonhöjd på meddelandet.
- Inserted – Tid och datum då meddelandet lästes in Ingestion-1, *OTS kap. 1.4.3 Ingestion-1*
- Mcc – Mobile Country Code för meddelandet
- Isgrp – Anger om meddelandet är en del av en gruppkonversation.
- Isatt – Anger om meddelandet är en bilaga till ett annat meddelande
- Sender – Sändande JID på meddelandet
- Receiver – Mottagande JID och/eller grupp (gid)
- Time – Tid då meddelandet skickades
- Latitude – Latitude för den enhet som skickat meddelandet
- Longitude – Longitude för den enhet som skickat meddelandet
- Metadataverified - Tomt fält

2.2.3 image_message & video_message

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

- Mid – Meddelande-ID, återfinns även i has_message.
- Shmid – Meddelande-UUID, återfinns även i has_message
- Path – Sökväg till aktuell media-fil.
- Inserted – Tid och datum då meddelandet lästes in Ingestion-1, *OTS kap. 1.4.3 Ingestion-1*
- Mcc – Mobile Country Code för meddelandet
- Isgrp – Anger om meddelandet är en del av en gruppkonversation.
- Isatt – Anger om meddelandet är en bilaga till ett annat meddelande
- Sender – Sändande JID på meddelandet
- Receiver – Mottagande JID och/eller grupp (gid)
- Time – Tid då meddelandet skickades
- Fromnote – Anger om meddelandet är skickat från enhetens ”Valv”.
- Latitude – Latitude för den enhet som skickat meddelandet
- Longitude – Longitude för den enhet som skickat meddelandet
- Metadataverified - Tomt fält

2.2.4 text_message

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

- Mid – Meddelande-ID, återfinns även i has_message.
- Shmid – Meddelande-UUID, återfinns även i has_message
- text – text-innehåll i meddelande. Detta text-innehåll kan anta olika format beroende på typ av innehåll. Dessa format beskrivs under 3.1 textformat
- Inserted – Tid och datum då meddelandet lästes in Ingestion-1*, OTS kap. 8.1 Ärenden/syndikat*
- Mcc – Mobile Country Code för meddelandet
- Isgrp – Anger om meddelandet är en del av en gruppkonversation.
- Isatt – Anger om meddelandet är en bilaga till ett annat meddelande
- Sender – Sändande JID på meddelandet
- Receiver – Mottagande JID och/eller grupp (gid)
- Time – Tid då meddelandet skickades
- Latitude – Latitude för den enhet som skickat meddelandet
- Longitude – Longitude för den enhet som skickat meddelandet
- Verified - Tomt fält
- Isfwd – anger om meddelandet är ett vidarebefordrat meddelande

2.2.5 Product

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

- Case_id – Det case/syndikat aktuell produkt tillhör. Ytterligare information om syndikat återfinns i *OTS kap. 1.4.3 Ingestion*
- Pid – Produkt-ID, återfinns även i has_message.
- Date_created – Datum och tid då produkten skapats
- Mcc_str – Mobile Country Code för samtliga meddelanden som skickats i produkten
- Jid_str – Samtliga JID som skickat eller tagit emot meddelanden i produkten
- Count – Antal meddelanden i produkten
- Jid_1 – Ena parten vid tvåpartskommunikation, tomt vid gruppkonversation.
- Jid_2 – Andra parten vid tvåpartskommunikation, tomt vid gruppkonversation.
- Gid – Grupp-ID vid flerpartskommunikation, tomt vid tvåpartskommunikation.
- isDup – Tomt fält
- knownGroup – Tomt fält
- apk – Grupp-ID

2.2.6 MDM_Data

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

- Jid – Aktuell JID, återfinns tabellen Roster
- Imei – Senast kända International Mobile Equipment Identity för enheten
- Imsi – Senast kända International Mobile Subscriber Identity för SIM-kort i enheten
- Regdate – Datum då enheten registrerades i MDM-plattformen.
- Lastcheckin – Senast enheten syntes av MDM-plattformen
- Make – Märke på enheten
- Model – Modell på enheten
- Currentmcc – Senast kända Mobile Country Code
- Currentcc – Senast kända Country Code
- Currentoperator – Senast kända teleoperator.
- Currentphone – Senast kända telefonnummer.
- Devicelocale – Senast kända språk- och regionsinställningar på enheten
- Ipaddr – Senast kända IP-address
- Lastlat – Senast kända latitud
- Lastlong – Senast kända longitud
- Lastlocdate – Tid och Datum för senast kända position.
- Lastwifi – Senast kända Wifi enheten kopplats till.
- Status – Status enheten förmedlade till MDM vid senaste inchekning
- Serialnum – Serienummer på enheten
- Iccid - integrated circuit card identifier på SIM-kortet

2.2.7 Roster

Innehåller känd information av brukaren av en JID.
Innehåller följande fält:
Jid – Aktuell JID, återfinns i tabellen MDM_Data
Uname – Senast kända Alias för aktuell JID
Real_name – Det namn en användare av Hola iBot senast registrerat för aktuell JID
Bio – Den beskrivning en användare av Hola iBot senast registrerat för aktuell JID
Location – Den plats en användare av Hola iBot senast registrerat för aktuell JID

3 Att notera kring information från MLAT

Vid hanteringen av exporter från MLAT har följande uppmärksammats

3.1 Produkter

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

3.2 Textformat

Meddelanden som skickas via ANOM kan antingen återfinnas som ren text, eller som något av följande format. Dessa är samtliga skrivna som JavaScript Object Notation (JSON).

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

Varje kategori av meddelande finns i två versioner beroende på vilken tidsperiod meddelandet har blivit inläst till Anom's plattform.

3.2.1 Vidarebefordrade meddelanden

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

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

Vidarebefordringar inlästa fram till och med 2020-09-09 innehåller enbart text och presenteras som följande exempel:
forward_prefix
{
"forward_message_time":1633354850, (Tidsstämpel i så kallad Epoch Unix Time)
"forward_message_text":"hej", (Vidarebefordrat innehåll)
"forward_message_user_jid":"abc123" (Den JID som meddelandet vidarebefordrats från)
}

Vidarebefordringar inlästa från och med 2020-09-11 möjliggör övriga typer av innehåll och presenteras som följande exempel:
forward_prefix
{
"forward_message_time": 1633354850, (Tidsstämpel i så kallad Epoch Unix Time)
"forward_message_user_jid": " abc123" (Den JID som meddelandet vidarebefordrats från)
"forward_message_body": "hej, (Den text eller kontaktinformation som vidarebefordrats, om forward_message_type är IMAGE, VIDEO, PTT eller NOTE finns inte detta fält i meddelandet.)
"forward_message_type": "TEXT", (Anger vilken sorts meddelande som vidarebefordrats. Fältet kan anta följande värden: TEXT|IMAGE|VIDEO|PTT|CONTACT|NOTE och avgör då om det vidarebefodrade meddelandet är text, bild, video, ljud, kontaktinformation eller en anteckning.",
"forward_message_uuid": "123e4567-e89b-12d3-a456-426614174000" (UUID på vidarebefordrat meddelande. Detta UUID är inte detsamma som meddelandets shmid)
}

3.2.2 Svar på meddelanden

När en användare svarar på ett meddelande i befintlig konversation representeras detta som ett citat (eng: quote).

Citat i konversationer kan presenteras på två sätt

Meddelanden inlästa till och med 2020-12-21 (med ett fåtal undantag) presenteras som följande exempel:
quote_prefix
{
"quote_message_time":1633354850, (Tidsstämpel i så kallad Epoch Unix Time),
"quote_message_text":"Hur mår du?", (Det meddelande som har besvarats)
"quoted_text":"Jag mår bra", (Det svar som getts)
"quote_message_user_jid":"abc123" (Den JID som skickat det meddelande som har besvarats)
,"message_uid":"123e4567-e89b-12d3-a456-426614174000" (UUID på det meddelande som besvarats. Detta UUID är inte detsamma som meddelandets shmid)
}

Meddelanden inlästa från och med 2020-12-25 (med vissa undantag) innehåller ytterligare metadata och innehåller förutom ovan även följande fält
quote_prefix
{
"quote_message_time":1633354850, (Tidsstämpel i så kallad Epoch Unix Time),
...
"isQuotedMessageDeleted":true, (Anger om det besvarade meddelandet raderats. Kan anta värde true (sant) eller false (falskt).
"isEdited":false , (Anger om det besvarade meddelandet redigerats. Kan anta värde true (sant) eller false (falskt).
}

3.2.3 Valvbilagor

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

Valvbilagor kan presenteras på två sätt

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

{
"mIsSelected":true, (Detta fält kan anta värdet true och false. Innebörden är i dagsläget okänd)
"passwordChecked":false, , (Detta fält kan anta värdet true och false. Innebörden är i dagsläget okänd)
"archived": true, , (Detta fält kan anta värdet true och false. Innebörden är i dagsläget okänd)
"attachmentsList":[], (Detta fält innehåller i förekommande fall en lista med bilagor skickade i meddelandet)
"attachmentsListOld":[], (Detta fält är tomt i samtliga meddelanden)
"checklist":false, (Anger om innehållet är en checklista)
"content":"", (Detta fält innehåller i förekommande fall text-innehåll)
"creation":, (Detta fält innehåller den tid bilagan skapades, i UNIX Time)
"lastModification":, (Detta fält innehåller den tid bilagan senast ändrades, i UNIX Time)
"locked":false, (Detta fält kan anta värdet true och false. Innebörden är i dagsläget okänd)
"reminderFired": false, (Detta fält kan anta värdet true och false. Innebörden är i dagsläget okänd)
"title":"", (bilagans titel)
"trashed": false (Detta fält kan anta värdet true och false. Innebörden är i dagsläget okänd)
}

Meddelanden inlästa från och med 2020-12-23 presenteras som ett liknande objekt:
{
"mIsFromVault": true, (Detta fält kan anta värdet true och false. Innebörden är i dagsläget okänd)
...
(Övriga fält som ovan)
}

3.3 Tidsförskjutning

3.3.1 Tidzonsdifferens

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

- Tidsram 1
  Meddelanden inlästa mellan 1 oktober 2019 och 27 oktober 2019: UTC -3
- Tidsram 2
  Meddelanden inlästa mellan 27 oktober 2019 och 29 mars 2020: UTC -2
- Tidsram 3
  Meddelanden inlästa mellan 29 mars 2020 och 18 september 2020: UTC -3
- Tidsram 4
  Meddelanden inlästa efter 18 september 2020: UTC

3.3.2 Övrig tidsförskjutning

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

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

3.4 Shmid är gemensamt för meddelanden och dess attachments

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

3.5 Platsinformation

3.5.1 Tillförlitlighet MCC

För enheter innehållandes ett aktivt SIM-kort som var uppkopplat mot ett mobilnät försågs det skickade meddelandet med aktuell Mobile Country Code (MCC) för den sändande enheten (Appendix 8.2c [1]). En jämförelse av denna MCC mot textinnehåll samt GPS-position ger att denna inte alltid är helt tillförlitlig. Framför allt gäller detta vid gränstrakter och när en användare nyligen färdats från ett land till ett annat.

3.5.2 Positionering

Efter en uppdatering i april 2020 försökte Anom-applikationen få fram enhetens position i samband med meddelanden som skickades. Detta kan ibland misslyckas. (*OTS A.8.2.d*) När detta misslyckas resulterar detta i positionsvärden på följande vis:
Värdet för latitud är satt till ett heltal, t.ex. 59.0
Värdet för longitud är satt till ett mycket stort tal, t.ex. 1617786553.
Värdet för longitud är vid de tillfället troligen en tidsstämpel i UNIX Time (Tid i sekunder sedan 1/1 1970 UTC)

3.6 MDM och Roster – Statisk information

Innehåll i tabeller MDM och Roster innehåller den senast kända informationen. En användare av Anom kan använda sig av flera olika enheter med skilda IMEI-nummer såväl som olika SIM-kort. Tabellerna Roster och MDM innehåller den information som var aktuell vid slutet av operation Trojan shield.

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

4 Källförteckning

[1] https://polisen.se/aktuellt/nyheter/2021/juni/155-frihetsberovade-i-storsta-insatsen-hittills-mot-organiserad-brottslighet/ [Hämtat 2021-10-07]
[2] Teknisk information om Operation Trojan Shield [Översatt version, senast uppdaterad 31 augusti 2021]

polisen.se

Polisens IT-avdelning
Telefon 114 14
e-post registrator@polisen.se

Polisen

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
2021-10-22	2021-10-26	2021-10-28	

Underrättelsesätt
Skriftligt

Notering

Resultat av underrättelsen/delgivningen
Ej erinran

Försvarare

Namn
Neo Barsoum Barstedt

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
2021-10-22	2021-10-26	2021-10-26

Underrättelsesätt
Skriftligt

Notering
Protokollbilaga skickad via krypterad e-post till försvararen

Resultat av underrättelsen/delgivningen
Ej avhörts