Police

Research fase Telegram

Stage

Abstract

In dit document wordt de opbouw en werking van Telegram samen met enkele tegen hangende technologieën besproken. Ook wordt er dieper ingegaan op het gebruik van bepaalde onderzoekstechnieken en het gebruik van Telegram in het algemeen.

Viktor Nagels (FGP ant)

Viktor.Nagels@Police.belgium.eu

Jentel Liekens (FGP ant)

Inhoudsopgave

Wat is Telegram? 4
Telegram vs Telegram Premium 4
Functionaliteiten van Telegram 4
Groep chats 4
Kanalen 5
Spraak- en video oproepen 6
Bestanden delen 6
Verwijderen van berichten 6
Bots 7
Verschillende apparaten 7
Geheime chats 7
Locatie sharing 8
Spraakberichten 8
Werking van Telegram 8
Technologieën Encryptie 8
Server-to-client encryptie 8
End-to-end encryptie 10
Cache opslag 11
OSI Model 11
Export Data 12
Tegenhangers van Telegram 12
Onderzoektechnologieën (OSINT) 14
Geogramint 14
Installatie 15
Wat is Telegram API? 15
Aanmaken API Key 15
Gebruik van Geogramint 17
Telepathy 18
Scan op locatie 18
theHarvester 19
Commando 19
Resultaat 20
Hunter 20
Werking 21

Maltego 21
Resultaat ..... **Error! Bookmark not defined.**
Universal Search bot Telegram 21
Telegram beveiligingsinstellingen 22
Accountinstellingen 22
Telefoonnummer 22
Vergrendelen van de applicatie 22
Berichten automatisch verwijderen 22
Privacy instellingen 22
Account verwijderen 22
Opslaggebruik 23
Gespreksinstellingen 23
Groepstype 23
Chatgeschiedenis 23
Rechten 23
Zichtbaarheid leden / administrators 23
Onderzoek open source code 24
iOS 25
Verschillen tussen web, app en desktop 25
Uitlezingen 25
Mogelijkheden uitlezen Android 26
Wat kan men terugvinden? 26
Gerecupereerde berichten lege cache 26
Gerecupereerde berichten bij uitgelogd account 27
Gerecupereerde berichten na externe verwijdering 28
Gerecupereerde berichten met pincode 28
Uitlezingen met 2FA 28
Mogelijkheden uitlezen iOS 28
Verstuurde berichten 28
Metadata 28
Flowchart 29
Exporteren chats + scripts 30
Sessie overname 30
Bronnen 30

Wat is Telegram?[1] [2]

Telegram is een Cloud gebaseerde instant messaging- en voice-over-IP-service. Het werd opgericht door Pavel en Nikolai Durov. Telegram werd gelanceerd op 14 augustus 2013 en is sindsdien een van de populairste berichten-apps ter wereld geworden.

Met Telegram kunnen gebruikers tekstberichten, foto's, video's en andere bestanden verzenden en ontvangen. Het ondersteunt ook spraak- en video-oproepen, groep chats met maximaal 200.000 leden en kanalen.

Het belangrijkste kenmerk van Telegram is de nadruk op privacy en veiligheid. De app maakt gebruik van end-to-end-codering om gebruikersgegevens te beschermen. Telegram heeft ook een functie "Geheime chats" waarmee gebruikers berichten kunnen verzenden die, indien gewenst, na een bepaalde tijd automatisch worden verwijderd.

Telegram is beschikbaar op alle grote platforms, waaronder Android, iOS, Windows, macOS en Linux. De app is gratis te downloaden en te gebruiken en geeft geen advertenties weer en verkoopt geen gebruikersgegevens aan derden. In de volgende punten gaan we dieper ingaan op de werking van deze applicatie en enkele varianten hiervan bespreken.

Telegram vs Telegram Premium[3]

Er bestaat ook een premiumversie van Telegram. Dit is de betalende versie, maar voor iemand met malafide activiteiten is dit geen interessant aanbod. De extra voordelen zijn vooral bedoeld voor bedrijven en niet voor individuen. Als je hier meer over wilt weten, kun je naar de tabel in de bijlage kijken.

Functionaliteiten van Telegram[4]

Groep chats[5] [6]

Binnen Telegram zijn er verschillende soorten groepen die je kunt maken, waaronder openbare, privé- en geheime groepen.

Een openbare groep is toegankelijk voor iedereen op Telegram en kan worden gevonden door te zoeken op trefwoorden of door te bladeren door de lijst met openbare groepen. Iedereen kan deelnemen aan een openbare groep en alle berichten zijn zichtbaar voor alle leden van de groep.

Een privégroep is alleen toegankelijk via een uitnodigingslink die de beheerder van de groep verstuurt. De link kan worden gedeeld met specifieke personen, en alleen degenen die de link hebben ontvangen, kunnen deelnemen aan de groep.

---

[1] https://nl.wikipedia.org/wiki/Telegram_(applicatie)
[2] https://www.telegram.org/
[3] Bijlage Research Telegram: Wat is Telegram -> Telegram vs Telegram premium (pagina 4)
[4] https://telegram.org/blog/topics-in-groups-collectible-usernames/nl?ln=a
[5] Bijlage Research Telegram: Functionaliteiten van Telegram -> Groep Chats (pagina 4)
[6] https://www.hoewerktdeapp.nl/telegram/hoe-werkt-telegram/hoe-maak-ik-een-nieuwe-groep-aan/

Berichtenten die in een privégroep worden geplaatst, zijn alleen zichtbaar voor de leden van de groep.

Een geheime groep is de meest beperkte vorm van groep chats in Telegram. Deze groepen zijn niet zichtbaar voor zoekopdrachten en kunnen alleen worden gevonden via een uitnodigingslink. De berichten die in een geheime groep worden geplaatst, zijn end-to-end versleuteld, wat betekent dat alleen de afzender en de ontvanger de inhoud van het bericht kunnen zien.

Alle soorten groepen in Telegram kunnen worden aangepast met verschillende functies, zoals het instellen van beheerders, het beperken van wie berichten kan plaatsen, het instellen van de groepsafbeelding en het aanpassen van de instellingen voor meldingen. Ook ondersteunt Telegram veel handige functies, zoals het delen van media, het versturen van bestanden, het maken van polls en nog veel meer.

In de praktijk komen we eigenlijk alleen openbare groepen tegen waar seksueel getinte content wordt verspreid of groepen waarin men verdovende middelen verkoopt. Op de afbeeldingen in de bijlage vind je enkele voorbeelden hiervan.

Kanalen[7]

Telegram-kanalen zijn een functie van de Telegram-app waarmee gebruikers inhoud kunnen publiceren en delen met een onbeperkt aantal volgers. Kanalen worden vaak gebruikt door bedrijven, organisaties en individuen om nieuws, updates en informatie te delen met hun volgers.

Het verschil tussen een Telegram-kanaal en een Telegram-groep is dat kanalen bedoeld zijn voor éénrichtingsverkeer. Dat betekent dat alleen de beheerder van het kanaal berichten kan plaatsen, terwijl de volgers alleen de inhoud kunnen bekijken en erop kunnen reageren via de commentaarfunctie. Telegram-kanalen bieden veel voordelen, waaronder:

1. Onbeperkte volgers: In tegenstelling tot groep chats, is er geen limiet op het aantal volgers dat een kanaal kan hebben. Dit maakt kanalen ideaal voor bedrijven en organisaties die een groot publiek willen bereiken.
2. Eenvoudig te beheren: Aangezien alleen de beheerder van het kanaal berichten kan plaatsen, is het beheren van een kanaal relatief eenvoudig en efficiënt.
3. Directe communicatie: Kanalen stellen gebruikers in staat om rechtstreeks te communiceren met hun volgers zonder de noodzaak van een tussenpersoon zoals e-mail of sociale media.
4. Analytics: Telegram-kanalen bieden uitgebreide analyses van het bereik en de betrokkenheid van uw kanaal, zodat u uw publiek beter kunt begrijpen en uw contentstrategie kunt optimaliseren.

Over het algemeen zijn Telegram-kanalen een krachtige en veelzijdige tool die gebruikers kunnen gebruiken om informatie te delen, hun publiek te vergroten en direct te communiceren met hun volgers.

[7] https://respond.io/blog/telegram-channels#:~:text=Telegram%20Channels%20allow%20you%20to,send%20messages%20to%20your%20subscribers.

Spraak- en video oproepen[8] [9]

Telegram biedt ook de mogelijkheid voor gebruikers om spraak- en video-oproepen te maken, waardoor het een volwaardig alternatief is voor andere communicatie-apps.

De spraak- en video-oproepen op Telegram zijn end-to-end versleuteld, wat betekent dat de inhoud van uw oproepen privé blijft en alleen door deelnemers kan worden gehoord of gezien. Telegram ondersteunt ook groeps-spraakoproepen met maximaal 1000 deelnemers.

Bestanden delen[10] [11]

Telegram staat bekend om zijn uitstekende mogelijkheden voor het delen van end-to-end versleutelde bestanden tot 2gb groot. Het stelt gebruikers in staat om verschillende soorten bestanden te delen, zoals afbeeldingen, video's, audio-opnamen, documenten, presentaties, spreadsheets en nog veel meer.

Telegram biedt ook een functie voor het delen van bestanden genaamd Telegram Bots. Telegram-bots zijn geautomatiseerde chatbots die gebruikers kunnen gebruiken om snel bestanden te delen. U kunt bijvoorbeeld een bot gebruiken om afbeeldingen of video's van internet te zoeken en deze vervolgens naar een chat te sturen.

Ten slotte biedt Telegram een cloudopslagfunctie genaamd Telegram Cloud, waarmee gebruikers hun bestanden in de cloud kunnen opslaan. Dit betekent dat u toegang heeft tot uw bestanden vanaf elk apparaat, zelfs als u geen toegang heeft tot uw telefoon of computer.

Verwijderen van berichten

Telegram biedt gebruikers de mogelijkheid om berichten uit individuele chats of groepen te verwijderen. Wanneer u een bericht in Telegram verwijdert, wordt het zowel van uw apparaat als van het apparaat van de ontvanger verwijderd. Het is echter belangrijk op te merken dat hiermee alleen het bericht van de apparaten wordt verwijderd en niet van de servers van Telegram.

Het is ook vermeldenswaard dat Telegram een zelfvernietigingsfunctie biedt voor berichten die in geheime chats worden verzonden. Deze functie verwijdert het bericht automatisch na een bepaalde tijd, variërend van 1 seconde tot 1 week. Dit zorgt ervoor dat het bericht slechts een beperkte tijd beschikbaar is en voor niemand toegankelijk is nadat het is verwijderd.

Het is echter belangrijk om te onthouden dat het verwijderen van berichten niet noodzakelijkerwijs betekent dat ze volledig verdwenen zijn. In sommige gevallen kunnen berichten nog steeds toegankelijk zijn via back-ups of op een andere manier. Bovendien weerhoudt het verwijderen van berichten andere gebruikers er niet van screenshots te maken of de inhoud van het bericht op een andere manier op te nemen.

---

[8] https://www.makeuseof.com/telegram-video-calls-features/

[9] https://indianexpress.com/article/technology/techook/telegram-how-to-make-video-or-voice-calls-mobile-web-desktop-version-7154554/

[10] https://telegram.org/blog/shared-files

[11] https://www.youtube.com/watch?v=QMZtZrZDNBY

Bots[12] [13] [14]

Telegram Bots zijn geautomatiseerde chatbots die zijn ontworpen om te werken binnen de Telegram-app. Ze zijn programmeerbaar en kunnen worden geconfigureerd om te reageren op berichten, specifieke taken uit te voeren en te communiceren met gebruikers.

Telegram Bots kunnen verschillende functies vervullen, zoals het versturen van nieuws, het beheren van taken, het maken van reserveringen, het genereren van memes, het spelen van games, het opzoeken van informatie op het web en nog veel meer. Ze kunnen ook worden gebruikt om gebruikers te helpen met het beheren van groepen of kanalen en het stroomlijnen van de communicatie.

Telegram Bots zijn vrij eenvoudig te maken. Er is een publieke API beschikbaar op hun website, samen met de nodige documentatie.

Verschillende apparaten[15]

Een van de voordelen van Telegram is de mogelijkheid om de app op meerdere apparaten tegelijkertijd te gebruiken. Dit betekent dat u Telegram kunt gebruiken op uw smartphone, tablet, computer of zelfs op het web, en toegang heeft tot al uw berichten en chats vanaf elk apparaat.

Dit wordt mogelijk gemaakt door de cloud gebaseerde opslag van Telegram. In tegenstelling tot sommige andere messaging-apps, slaat Telegram al uw berichten, media en bestanden op in de cloud, in plaats van alleen op uw apparaat. Dit betekent dat uw gegevens altijd beschikbaar zijn, ongeacht welk apparaat u gebruikt.

Bovendien biedt Telegram ook de functie genaamd "Actieve sessies". Dit geeft u de mogelijkheid om te zien welke apparaten momenteel zijn ingelogd op uw Telegram-account en op afstand toegang te krijgen tot uw sessies.

Geheime chats[16]

Geheime chats zijn een functie in Telegram waarmee gebruikers berichten kunnen uitwisselen met end-to-end encryptie. Dit betekent dat alleen de afzender en de ontvanger de inhoud van de berichten kunnen lezen en niemand anders, inclusief Telegram zelf.

Er zijn enkele belangrijke verschillen tussen geheime chats en reguliere chats in Telegram. Ten eerste worden geheime chats alleen op het apparaat van de afzender en ontvanger opgeslagen en niet in de cloud. Dit betekent dat als u een nieuw apparaat gebruikt om toegang te krijgen tot Telegram, u geen toegang heeft tot uw oude geheime chats. Ten tweede, omdat er geen back-up van de geheime chats is, kunt u geen multimedia-bestanden verzenden of ontvangen in een geheime chat.

---

[12] https://core.telegram.org/bots/api
[13] https://core.telegram.org/bots/features
[14] https://chatbotslife.com/what-is-a-telegram-bot-reasons-to-use-bot-for-telegram-46b0d0579337
[15] https://www.youtube.com/watch?v=tQNt_93HuRo
[16] https://www.gadgetsnow.com/faqs/what-is-secret-chat-in-telegram/articleshow/81323630.cms

Locatie sharing[17]

Telegram biedt een locatie delen-functie waarmee gebruikers hun huidige locatie met anderen kunnen delen.

Spraakberichten

Met Telegram kunnen gebruikers spraakberichten verzenden en ontvangen. Spraakberichten kunnen in realtime worden opgenomen en verzonden of vooraf worden opgenomen en als bestand worden verzonden.

Spraakberichten op Telegram zijn end-to-end versleuteld, wat betekent dat alleen de afzender en de ontvanger toegang hebben tot de berichten en deze kunnen afspelen. Met Telegram kunnen gebruikers ook spraakberichten verzenden zonder beperking van de lengte.

Werking van Telegram[18] [19]

Technologieën Encryptie[20][21]

Telegram maakt gebruik van verschillende encryptietechnologieën om de privacy en beveiliging van gebruikers te waarborgen. Enkele van de belangrijkste technologieën die Telegram gebruikt om berichten te encrypteren worden hieronder besproken.

Het is belangrijk om te benadrukken dat deze technologieën alleen werken als de juiste instellingen zijn geconfigureerd. Het is daarom belangrijk om de privacy-instellingen van uw Telegram-account te controleren om ervoor te zorgen dat u de gewenste vormen van encryptie gebruikt. In onderstaande punten gaan we deze technologieën in detail bespreken.

Server-to-client encryptie

Server-to-client encryptie is een beveiligingsprotocol dat wordt gebruikt om de communicatie tussen een server en een client te beveiligen. Bij dit protocol wordt de data die tussen de server en client wordt uitgewisseld versleuteld, zodat alleen de partijen die toegang hebben tot de juiste sleutel de data kunnen decoderen en begrijpen.

Telegram gebruikt deze encryptie voor berichten die worden verzonden van de servers van hen. Naar de eindgebruikers. Hierbij wordt gebruik gemaakt van hun eigen MTProto-protocol. In het onderstaande puntje gaan we dieper in op de werking van dit protocol.

---

[17] https://famisafe.wondershare.com/location-sharing/how-to-share-location-on-telegram.html

[18] https://www.kaspersky.com/blog/telegram-why-nobody-uses-secret-chats/46889/

[19] https://www.kaspersky.nl/blog/telegram-privacy-security/26592/

[20] Bijlage Research Telegram: Werking van Telegram -> Technologieën Encryptie (pagina 5 - 6)

[21] https://www.leap.expert/telegram-security-is-telegram-safe-why-crypto-companies-use-telegram/

MTProto

MTProto (Mobile Telegram Protocol) is een encryptieprotocol dat specifiek is ontwikkeld voor Telegram. Het werd in 2013 ontworpen en geïmplementeerd door de oprichter van Telegram, Pavel Durov, en zijn team van ontwikkelaars.

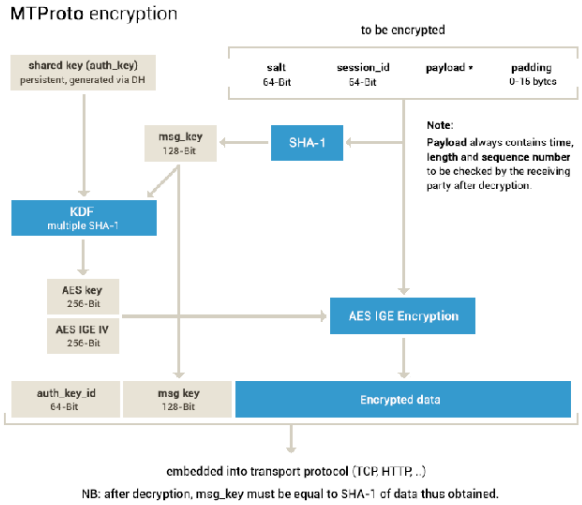
Het MTProto-protocol is een combinatie van verschillende encryptie- en beveiligingsmethoden en heeft als doel een hoge mate van veiligheid en privacy te bieden voor de communicatie van Telegram-gebruikers. Het protocol maakt gebruik van symmetrische AES- en RSA-encryptie, evenals een verscheidenheid aan hashing- en authenticatiemechanismen.

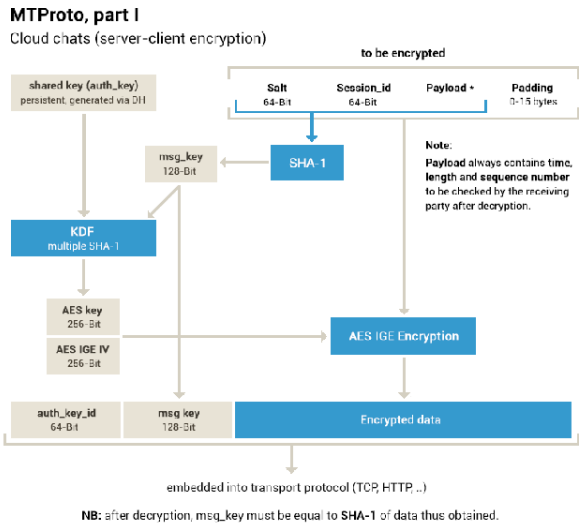
Een belangrijk kenmerk van het MTProto-protocol is dat het niet alleen end-to-end-encryptie biedt voor één-op-één chats en geheime chats, maar ook voor groep chats en kanalen. Dit betekent dat alle berichten die worden verzonden en ontvangen in Telegram-groep chats en kanalen zijn versleuteld.

MTProto heeft nog verschillende andere belangrijke kenmerken die het tot een effectief protocol voor veilige communicatie maken. Deze kenmerken omvatten:

- End-to-end versleuteling: MTProto versleutelt alle berichten en gegevens die tussen clients en servers worden verzonden, zodat alleen de beoogde ontvanger de berichten kan ont sleutelen en lezen.
- Meerdere lagen van versleuteling: MTProto gebruikt zowel symmetrische als asymmetrische versleuteling en Diffie-Hellman sleuteluitwisseling om meerdere lagen van versleuteling te bieden en te beschermen tegen aanvallen. Dit zorgt ervoor dat alleen de bedoelde ontvanger toegang heeft tot de verzonden berichten. Dit omvat het gebruik van verschillende encryptiesleutels voor elk bericht en het genereren van tijdelijke sleutels voor het decoderen van berichten.
- Perfecte voorwaartse geheimhouding: MTProto ondersteunt perfecte forward secrecy, wat betekent dat zelfs als een aanvaller de privésleutel zou bemachtigen, hij niet in staat zou zijn berichten uit het verleden te ont sleutelen.
- Sterke versleutelingsalgoritmen: MTProto gebruikt sterke versleutelingsalgoritmen, waaronder 256-bit Advanced Encryptie Standard (AES), om de veiligheid van de over het netwerk verzonden gegevens te waarborgen.
- Beveiligingsmaatregelen tegen aanvallen: Telegram heeft talrijke beveiligingsmaatregelen geïmplementeerd om te beschermen tegen aanvallen, waaronder het verwijderen van berichten aan de serverzijde, authenticatie met twee factoren en de mogelijkheid om de integriteit van berichten te verifiëren

Hoewel het MTProto-protocol door Telegram wordt geprezen vanwege zijn hoge veiligheidsniveau en snelle prestaties, is het ook onderwerp van enige controverse en kritiek. Sommige beveiligingsexperts hebben bijvoorbeeld bezorgdheid geuit over de gesloten aard van het protocol en het gebrek aan onafhankelijke audits van de code. Toch blijft Telegram een populaire berichten-app met veel gebruikers die waarderen dat de app sterk inzet op privacy en beveiliging.





End-to-end encryptie [22]

End-to-end encryptie (E2EE) is een beveiligingsmethode die wordt gebruikt om de privacy en vertrouwelijkheid van communicatie te beschermen. Bij end-to-end encryptie worden berichten versleuteld op het apparaat van de verzender en vervolgens gedecodeerd op het apparaat van de ontvanger, zonder dat een tussenpersoon of derde partij de inhoud van het bericht kan lezen of onderscheppen.

Deze encryptie wordt gebruikt voor de zogenaamde ‘geheime chats’. Deze chats zijn tussen twee gebruikers en worden niet opgeslagen op de telegram servers. De encryptie is een samenstelling van AES-256, RSA 2048 en Diffie-Hellman-sleuteluitwisseling. Over deze technologieën kan je in de onderstaande punten meer te weten komen.

Symmetrische AES-encryptie[23] [24] [25]

Symmetrische AES-encryptie is een geavanceerde technologie voor gegevensversleuteling die door Telegram en vele andere toepassingen wordt gebruikt om de privacy en veiligheid van gebruikers te waarborgen. AES staat voor "Advanced Encryptie Standard" en is een methode voor het coderen van gegevens die door de Amerikaanse overheid is ontwikkeld. Je kan afbeeldingen over de werking terugvinden in de bijlage.

RSA-encryptie[26] [27]

RSA-encryptie is niet symmetrisch. In tegenstelling tot symmetrische encryptie, maakt RSA gebruik van twee verschillende sleutels: een openbare sleutel en een privésleutel.

---

[22] https://www.wired.co.uk/article/telegram-encryption-end-to-end-features

[23] https://www.cdvibenelux.com/nl/wat-is-aes-encryptie-en-hoe-werkt-het/

[24] https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption#:~:text=The%20AES%20Encryption%20algorithm%20(also,together%20to%20form%20the%20cipher text

[25] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[26] https://www.techtarget.com/searchsecurity/definition/RSA#:~:text=RSA%20is%20a%20type%20of,is%20used%20to%20decrypt%20it.

[27] https://en.wikipedia.org/wiki/RSA_(cryptosystem)

Het gebruik van RSA-encryptie is ook handig voor het verifiëren van de identiteit van de ontvanger, omdat de openbare sleutel van de ontvanger meestal door een vertrouwde autoriteit wordt geverifieerd voordat deze wordt gebruikt. Dit betekent dat de verzender er zeker van kan zijn dat het bericht alleen kan worden gelezen door de beoogde ontvanger en niet door een andere persoon of entiteit. Je kan hier nog een visuele voorstelling van zien in de bijlage.

Diffie-Hellman-sleuteluitwisseling [28] [29]

Diffie-Hellman-sleuteluitwisseling is een cryptografisch protocol waarmee twee partijen die elkaar niet kennen, veilig een gemeenschappelijke geheime sleutel kunnen uitwisselen die vervolgens kan worden gebruikt voor symmetrische encryptie.

Cache opslag[30][31]

Cache-opslag is een tijdelijke opslagplaats voor gegevens die regelmatig worden gebruikt door een computerprogramma of een besturingssysteem. Het doel van cache-opslag is om de snelheid van de computer te verhogen door het verminderen van de toegangstijd tot de gegevens.

Hier staan dus ook nog bestanden in van Telegram. Op het moment van documenteren vond ik enkel de media terug. De chat berichten staan hier ook, maar wel geëncypteerd. In bijlagen kan je zien hoe deze mappenstructuur eruitziet.

OSI Model

Hieronder kan je een samenvatting terugvinden die de systemen die telegram gebruikt beschrijft, gesorteerd op basis van het OSI-model.

OSI	Technologie
Layer 7 (Application)	High-level RPC API
Layer 6 (Presentation)	Type Language
Layer 5 (Session)	MTProto session
Layer 4 (Transport)	-MTProto transport protocol -MTProto obfuscation (optional) -Transport Protocol - TCP - Web socket - Web socket over HTTPS - HTTP - HTTPS UDP
Layer 3 (Network)	IP
Layer 2 (Data link)	MAC/LLC
Layer 1 (Physical)	-IEE 802.3 -IEEE 802.11 -…

[28] https://nl.wikipedia.org/wiki/Diffie-Hellman-sleuteluitwisselingsprotocol
[29] https://meneer.depuydt.eu/tag/diffie-hellman/
[30] Bijlage Research Telegram: Werking van Telegram -> Cache opslag (pagina 6 - 7)
[31] https://www.itgeared.com/where-does-telegram-save-files-on-android/

Export Data

Dankzij deze functie kun je alle persoonlijke gegevens van je eigen account downloaden. Hier worden alle chats weergegeven, inclusief je eigen verstuurde berichten, alle soorten media, contacten en meest gebruikte contacten. De export heeft ook een handige grafische gebruikersinterface (HTML-pagina), waardoor het gemakkelijk is om alle gegevens terug te vinden. Houd er echter rekening mee dat verwijderde berichten niet worden opgenomen in de export.

Tegenhangers van Telegram[32]

In de tabel hieronder vind je een overzicht van enkele tegenhangers van Telegram terug net zoals de voor- en nadelen hiervan. In bijlage vind je van al de besproken technologieën een gedetailleerde uitleg terug.

App	Systemen	Voordelen/nadelen
Suresport	Android en iOS	+ End-to-end encryptie + Sterke versleuteling + Anoniem te gebruiken + Zelfvernietigende berichten + Veilige opslag van berichten - Weinig gebruikers
Signal	iOS, Android, Windows, MacOS en Linux	+ Open source + Geen advertenties + End-to-end encryptie + Sterke versleuteling + Zelfvernietigende berichten + Veilige opslag van berichten + Bescherming tegen MITM-technieken - Geen publieke groepen - Telefoonnummer vereist - Weinig gebruikers
Wire	Android, iOS, Windows, Linux, MacOS en via je browser	+ End-to-end encryptie + Veel functionaliteiten + Zelfvernietigende berichten + Veilige opslag van berichten - Weinig gebruikers - Weinig bescherming tegen - MITM-technieken - Registreert gedragsgegevens
Threema	Android, iOS, MacOS, Windows, Linux	+ Geen advertenties + Open Source

[32] Tegenhangers van Telegram (pagina 8 - 17)

		+ End-to-end encryptie + Zelfvernietigende berichten + Veilige opslag van berichten + Volledige anonimiteit - Betalend - Beperkte compatibiliteit - Weinig gebruikers
Element	IOS, MacOS, Android, Windows, Linux, F-Droid en via browser	+ End-to-end encryptie + Veel functionaliteiten + Open-source software + Gebruikers-ID's in plaats van telefoonnummers + Gebruiksvriendelijke desktop-app - Weinig gebruikers
Viber	Android, iOS, Windows, macOS en Linux	+ End-to-end encryptie + Veel functionaliteiten + Veel gebruikers - Geen zelfvernietigende berichten - Vraagt toegang tot je contacten - Geen anoniem gebruik - Connection Logs
Wickr	Android, iOS, Windows, macOS en Linux	+ End-to-end encryptie + Goede beveiliging + Veilige Bestandsvernietiging + Zelfvernietigende berichten/ bestanden + Cross platform - Weinig functionaliteiten - Betaalde delen - Closed source software
Whatsapp	IOS, Android, Windows, macOS en via browser	+ 2FA + Melding inlogpoging + Verdwijnende berichten + End-to-end encryptie + Encrypted back-ups + Veel gebruikers - Geen E2EE chat back-ups - Verzamelt persoonsgegevens - Afhankelijk van het internet
WeChat	IOS, Android, Windows, macOS en via browser	+ Eenvoudig gebruik + Multifunctioneel

		+ Veel gebruikers - Slechte veiligheid bij betaling - Niet compatibel (enkel Chinees en Engels) - Censuur
Messenger	IOS, Android, Windows, macOS en web	+ 2FA + Meldingen inlogpogingen + Integratie met andere diensten + End-to-end encryptie + Veel gebruikers - Voice, video geen E2EE - Beperkte controle gegevens - Beperkte ondersteuning oudere apparaten - Verzamelt persoonsgegevens - Afhankelijk van internet
Snapchat	Android, IOS en via browser	+ Tijdelijke content + Betrouwbaar + End-to-end encryptie + Veel gebruikers - Security - Verzamelen informatie - Beperkte ondersteuning voor oudere apparaten - Afhankelijk van internet

Onderzoektechnologieën [33](OSINT)

Geogramint[34] [35]

Een eerste onderzoek technologie die ik heb gebruikt, is de Geogramint-tool. Deze tool zal verschillende Telegram-accounts in de buurt van een aangeduide locatie achterhalen. Geogramint is dus een OSINT-tool die de API van Telegram gebruikt om gebruikers en groepen in de buurt te vinden. De tool is geïnspireerd door Tejado's Telegram Near Map, die niet langer wordt onderhouden. Het doel van deze applicatie is om een gebruiksvriendelijker alternatief te bieden.

Geogramint vindt alleen Telegram-gebruikers en -groepen die de functie 'In de buurt' hebben geactiveerd. Standaard is deze gedeactiveerd. De tool wordt volledig

[33] https://www.telegramdb.org/
https://tgstat.com/
[34] Bijlage Research Telegram: Onderzoektechnologieën (OSINT) -> Geogramint (pagina 18)
[35] https://github.com/Alb-310/Geogramint

ondersteund op Windows en gedeeltelijk ondersteund op Mac OS- en Linux-distributies.

Installatie

Voor we deze tool verder kunnen gebruiken, dienen we deze eerst te installeren. Het is belangrijk om te zorgen dat je Git, Python en pip3 geïnstalleerd hebt alvorens je verder kan gaan met de installatie van Geogramint. In de onderstaande stappen gaan we er dus vanuit dat deze al correct zijn geïnstalleerd en worden louter de stappen voor de installatie van Geogramint besproken.

Clone de directory naar je systeem met het commando: 'git clone https://github.com/Alb-310/Geogramint.git '.

De volgende stap in het installatieproces is het installeren van alle nodige requirements met het commando: 'pip3 install -r requirements.txt'.

Als laatste stap binnen deze installatie kunnen we ervoor kiezen om ofwel de GUI modus of de CLI-modus te starten. Als je de GUI modus wilt starten kies je voor het commando: 'python3 geogramint.py' en voor de CLI-modus kies je voor het commando: 'python3 geogramint.py --help'

Wat is Telegram API?[36]

Met de Telegram API kunnen ontwikkelaars communiceren met de Telegram-server en verschillende functies van Telegram gebruiken om bots en andere toepassingen te ontwikkelen. Dit is mogelijk omdat Telegram een open-source platform is dat API's aanbiedt waarmee ontwikkelaars kunnen communiceren met de Telegram-servers.

Een van de belangrijkste functies die via de Telegram API kunnen worden gebruikt, is het verzenden en ontvangen van berichten. Ontwikkelaars kunnen hierdoor verschillende soorten bots en automatiseringen maken die berichten versturen en ontvangen.

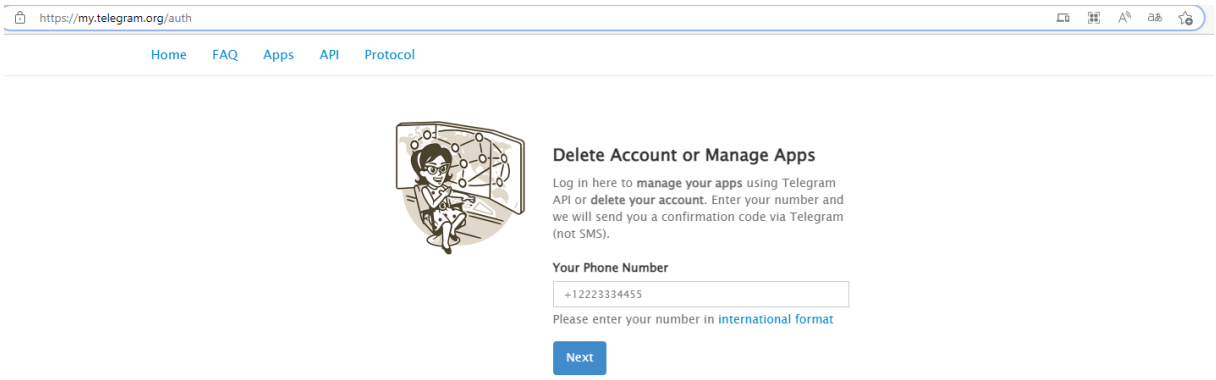
Tot slot ondersteunt de Telegram API het uploaden en downloaden van bestanden en het delen van mediabestanden zoals foto's en video's. Bovendien kunnen ontwikkelaars real-time updates ontvangen via webhooks, waardoor bots en andere toepassingen real-time gegevens kunnen ontvangen en verwerken. Dit maakt het mogelijk om op maat gemaakte oplossingen te bouwen die aansluiten bij specifieke behoeften.

Aanmaken API Keys

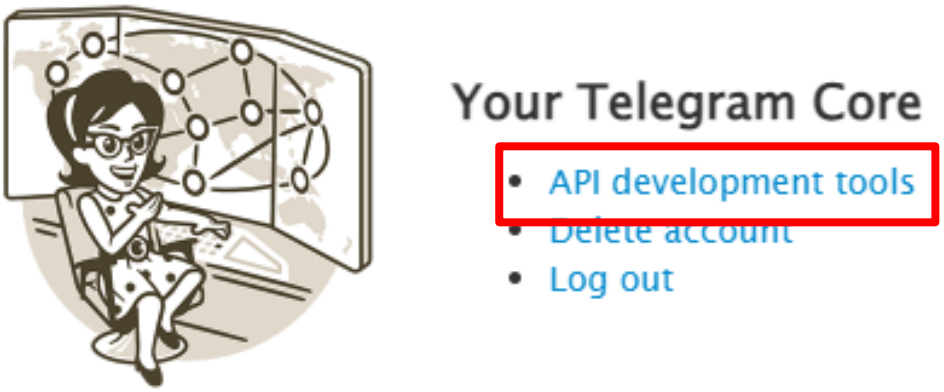
De volgende stap in het opzetten van Geogramint is het aanmaken van je API key. Deze zul je nodig hebben om überhaupt later met de applicatie te kunnen werken. In de onderstaande stappen kan je lezen hoe je deze key bekomt.

1. Als eerste stap moeten we naar de website “https://my.telegram.org/” gaan. Hier geef je het telefoonnummer van je telegram account in.

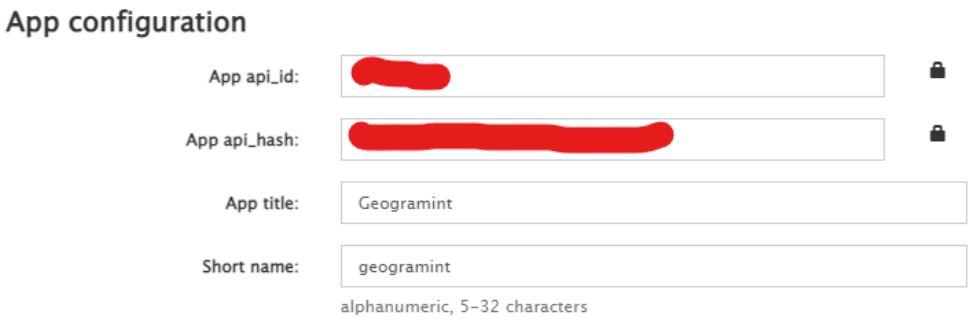
[36] https://core.telegram.org/



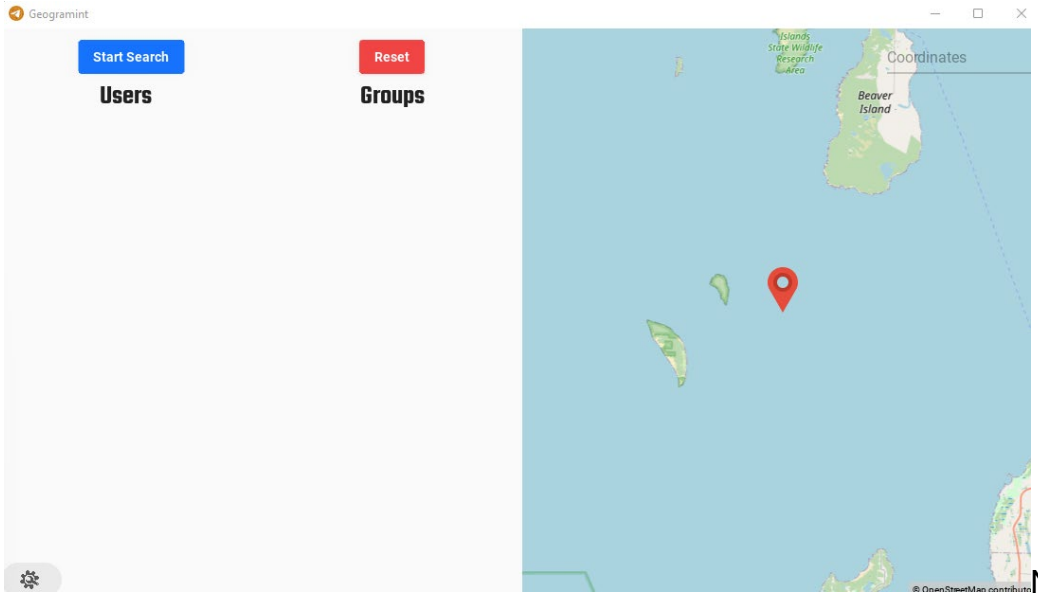
2. In de tweede stap dien je naar de subtab “API-development tools te gaan.



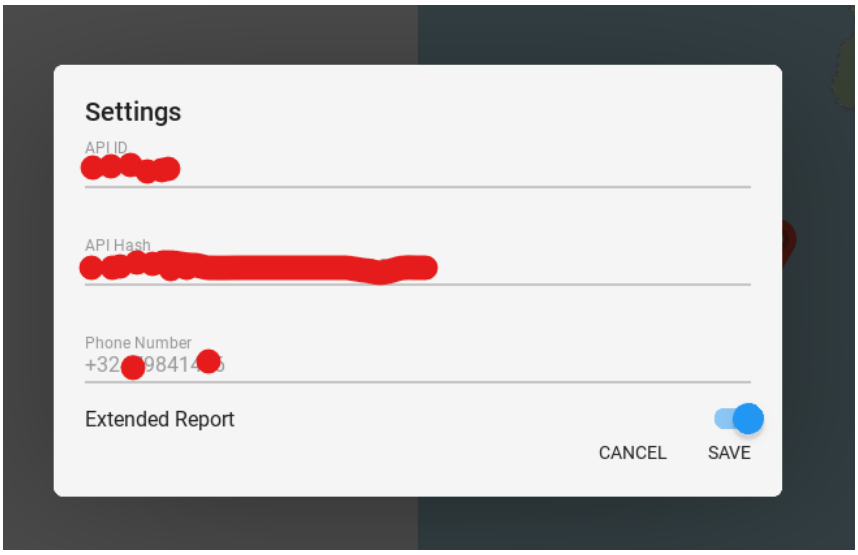
Op deze plaats zal je de gewenste API-codes die we nodig hebben voor Geogramint terugvinden. Dit kan je ook zien op de onderstaande afbeelding.



3. Nu we deze gegevens hebben kunnen we de laatste stap voor we met Geogramint kunnen werken uitvoeren. Hiervoor moeten we verder gaan op de derde stap van de installatie. Ik heb er dus voor gekozen om dit met aan de hand van de GUI te doen. Wanneer we dit commando uitvoeren zullen we dus een nieuw scherm krijgen waarop onderstaande informatie te zien is.

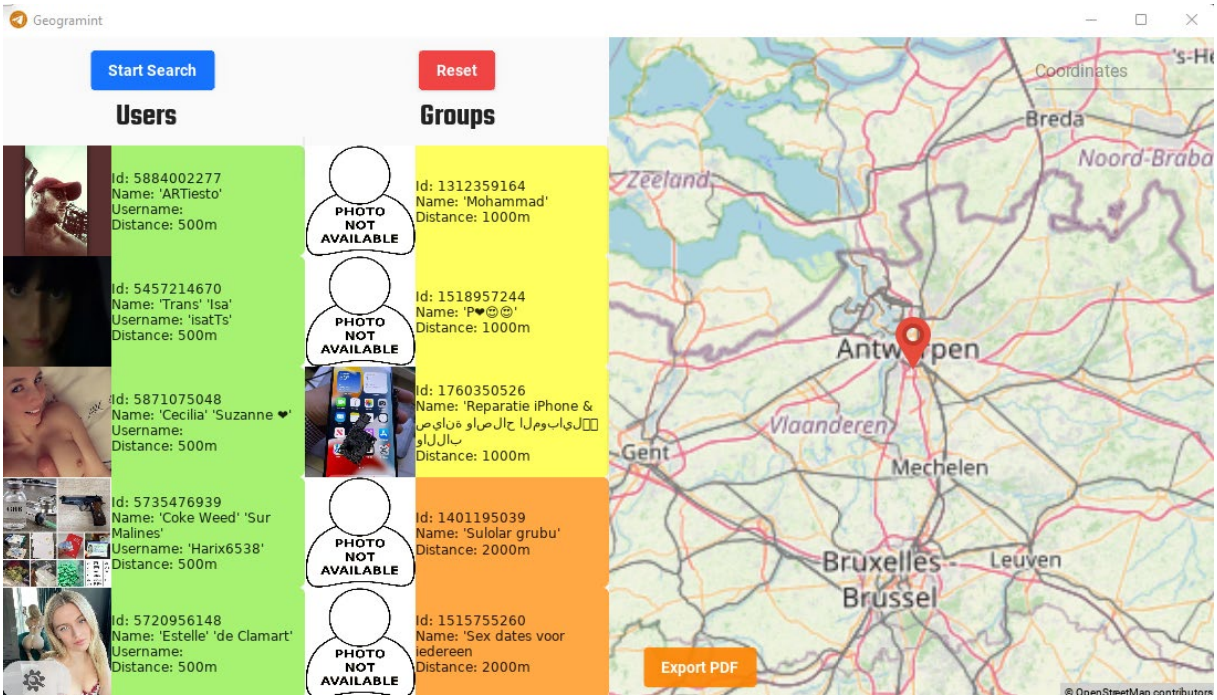


Nu we dit hebben kunnen we de API toevoegen door links van onder op het tandwieltje te klikken. Hier vullen we dus de gegevens die we juist bekomen hebben in.



Gebruik van Geogramint

De applicatie is heel eenvoudig in gebruik. Met de kaart aan de rechterkant van de applicatie kan je zoeken naar een specifieke locatie waar je wilt filteren op Telegram accounts. Door op “Start Search” te klikken zal je starten met zoeken naar de groepen en personen die er op die locatie aanwezig zijn.



Het is ook een optie om dit alles in een overzichtelijk pdf-bestand te plaatsen. Als we dit bestand dan openen zien we dat de profiel foto, het account ID, de voornaam, de achternaam, de gebruikersnaam, eventueel een beschikbaar gsm-nummer en de afstand van de geselecteerde locatie. Op de afbeelding in de bijlage kan je zien hoe zo een rapport er zou uit zien. We zijn er momenteel nog niet helemaal uit of deze locatie wordt bepaald van het IP-adres (niet heel nauwkeurig) of op basis van de locatie (wel nauwkeurig). Hiervoor zal er verder onderzoek moeten gedaan worden.

Telepathy[37] [38]

Telepathy is een OSINT-toolkit waarmee onderzoekers, analisten en digitale onderzoekers Telegram-chats kunnen onderzoeken.

Telepathy wordt beschouwd als het "Zwitserse zakmes van Telegram-tools", omdat het OSINT-analisten, onderzoekers en digitale onderzoekers in staat stelt Telegram-chats te archiveren (inclusief antwoorden, media-inhoud, opmerkingen en reacties), ledenlijsten te verzamelen, gebruikers op locatie te zoeken, top-posters in een chat te analyseren, doorgestuurde berichten te mappen en nog veel meer.

Telepathy kan in ons geval een handige tool zijn, vooral wanneer je op zoek bent naar specifieke Telegram-gebruikers op basis van hun ID of gebruikersnaam (let op: je moet de gebruikers-ID hebben of de gebruiker moet een gebruikersnaam hebben ingesteld). Als je eenmaal de ID of gebruikersnaam hebt, kun je een scan uitvoeren en krijg je waardevolle informatie terug.

Scan op locatie

Telepathy biedt ook de mogelijkheid om coördinaten in te voeren, waarna je een lijst terugkrijgt van Telegram-gebruikers die zich binnen dat gebied bevinden (mits de optie

[37] Bijlage Research Telegram: Onderzoektechnologieën (OSINT) -> Telepathy (pagina 19 - 21)
[38] https://github.com/jordanwildon/Telepathy

"Laat mij zien" is ingeschakeld). Je ontvangt vervolgens een tabel met alle gebruikers-ID's en de afstand tussen hun locatie en de ingevoerde coördinaten.

TheHarvester[39] [40] [41]

TheHarvester is een OSINT-tool (Open Source Intelligence) die wordt gebruikt om informatie te verzamelen over e-mailadressen, subdomeinen, IP-adressen, open poorten en URL's van een bepaalde domeinnaam. Het kan handig zijn voor beveiligingsonderzoekers, pentesters en iedereen die geïnteresseerd is in het verzamelen van informatie over een specifieke entiteit of organisatie.

Met theHarvester kun je zoeken naar informatie in verschillende zoekmachines, zoals Google, Yahoo, Bing, PGP-servers, LinkedIn, enzovoort. Het heeft ook de mogelijkheid om brute force te gebruiken om e-mailadressen te vinden op basis van een domeinnaam en een woordenlijst. De tool heeft de mogelijkheid om resultaten op te slaan in verschillende formaten, zoals txt, html, xml, csv enzovoort.

Hier zijn enkele voorbeelden van hoe theHarvester kan worden gebruikt:

- Zoek naar e-mailadressen die gekoppeld zijn aan een bepaalde domeinnaam. Dit kan handig zijn bij het opsporen van mogelijke doelwitten voor phishing-aanvallen.
- Zoek naar sub domeinen die zijn gekoppeld aan een bepaalde domeinnaam. Dit kan handig zijn bij het identificeren van de scope van een webapplicatie-penetratietest.
- Zoek naar open poorten en services die worden uitgevoerd op een bepaalde IP-adres. Dit kan handig zijn bij het identificeren van kwetsbaarheden in het netwerk.
- Zoek naar informatie over een bepaalde persoon of organisatie op verschillende sociale media-platforms en andere onlinebronnen. Dit kan handig zijn bij het identificeren van de online aanwezigheid van een entiteit.

Hoewel theHarvester een krachtige tool kan zijn, is het belangrijk om het verantwoord te gebruiken en alleen te gebruiken voor legitieme doeleinden. Ongeoorloofde toegang tot informatie kan leiden tot strafrechtelijke vervolging.

Commando

Je kan hiermee werken aan de hand van het “theHarvester” commando binnen kali. Aan de hand van onderstaande lijst van opties kan je het commando zo aanpassen dat je het resultaat naar wens krijgt.

- **-d**: Domain to search or company name.
- **-b**: Data source: baidu, bing, bingapi, dogpile, google, googleCSE, googleplus, google-profiles, linkedin, pgp, twitter, vhost, yahoo, all.
- **-s**: Start in result number X (default: 0).

[39] Bijlage Research Telegram: Onderzoektechnologieën (OSINT) -> theHarvester (pagina 22)

[40] https://www.cybervie.com/blog/what-is-the-harvester/

[41] https://www.kali.org/tools/theharvester/

- **-v**: Verify hostname via DNS resolution and search for virtual hosts.
- **-f**: Save the results into an HTML and XML file (both).
- **-n**: Perform DNS reverse query on all ranges discovered.
- **-c**: Perform DNS brute force for the domain name.
- **-t**: Perform DNS TLD expansion discovery.
- **-e**: Use this DNS server.
- **-l**: Limit the number of results to work with (bing goes from 20 to 20 results, google 100 to 100, and pgp does not use this option).
- **-h**: Use SHODAN database to query discovered hosts.

Resultaat

Ik heb persoonlijk gebruik gemaakt van twee verschillende commando's om te kijken naar de resultaten in verband met Telegram. Zo heb ik gebruik gemaakt van het commando "theHarvester -d telegram.org -b bing " om specifieke resultaten via bing te krijgen. Dit kan je ook zien op de afbeelding in de bijlage.

Hunter[42]

Hunter is een OSINT-tool die wordt gebruikt voor het verzamelen van informatie over e-mailadressen. Het kan handig zijn voor beveiligingsonderzoekers, pentesters en iedereen die geïnteresseerd is in het vinden van informatie over een specifiek e-mailadres of domein.

Met Hunter kun je zoeken naar informatie over een e-mailadres, zoals de bijbehorende domeinnaam, open poorten, enzovoort. Het heeft ook de mogelijkheid om e-mailadressen te valideren en om te bepalen of een e-mailadres geldig is of niet. De tool heeft de mogelijkheid om resultaten op te slaan in verschillende formaten, zoals CSV, XLS en JSON.

Hier zijn enkele voorbeelden van hoe Hunter kan worden gebruikt:

- Zoek naar e-mailadressen die gekoppeld zijn aan een bepaald domein. Dit kan handig zijn bij het vinden van potentiële doelwitten voor een phishing-aanval.
- Zoek naar informatie over een bepaald e-mailadres, zoals de bijbehorende domeinnaam en open poorten. Dit kan handig zijn bij het identificeren van de online aanwezigheid van een bepaalde entiteit.
- Valideer e-mailadressen om te bepalen of ze geldig zijn of niet. Dit kan handig zijn bij het schoonmaken van mailinglijsten en het voorkomen van spam.

Het gebruik van Hunter moet verantwoordelijk en legaal zijn. Het is belangrijk om te onthouden dat het verzamelen van informatie over iemand zonder hun toestemming illegaal kan zijn en kan leiden tot juridische vervolging. Het is ook belangrijk om het beleid van het bedrijf waarvoor je werkt te respecteren en alleen de tool te gebruiken voor legitieme doeleinden.

[42] Bijlage Research Telegram: Onderzoektechnologieën (OSINT) -> Hunter (pagina 22)

Werking

Je kan Hunter eenvoudig gebruiken via de site hunter.io waar je met een account eenvoudig gebruik kunt maken van de opties van deze OSINT-tool. We hebben deze tool gebruikt om alle e-mailadressen binnen het domein telegram.org te zoeken. Je kan het resultaat hiervan zien op een afbeelding in de bijlage.

Maltego[43]

Maltego is een krachtige OSINT (Open Source Intelligence) tool waarmee gebruikers informatie kunnen verzamelen en analyseren over verschillende doelen en entiteiten. De tool is ontworpen om te werken met grote en complexe datasets, waardoor gebruikers in staat zijn om snel en efficiënt inzicht te krijgen in de relaties tussen verschillende informatiebronnen.

Met Maltego kunnen gebruikers gegevens verzamelen uit verschillende bronnen, zoals sociale media, online forums, nieuwsartikelen, databases en meer. De tool maakt gebruik van een visualisatie-gebaseerde interface die de gebruiker in staat stelt om complexe relaties en patronen te identificeren tussen verschillende entiteiten en informatiebronnen.

Maltego biedt een uitgebreide set van functies, waaronder de mogelijkheid om gegevens te transformeren en te manipuleren om de informatie beter te begrijpen en te analyseren. Gebruikers kunnen ook hun eigen plug-ins en API's integreren in de tool om de functionaliteit uit te breiden en aangepaste workflows te creëren.

Op de afbeeldingen in bijlage kan je zien hoe het visuele overzicht voor Telegram eruitziet.

Universal Search bot Telegram[44]

UniversalSearchRobot is een Russische bot op het Telegram-platform die gebruikers kan helpen bij het zoeken naar informatie op het internet. Deze bot is ontworpen als een Open Source Intelligence (OSINT) tool en kan gebruikt worden om informatie te vinden over specifieke personen, zoals hun telefoonnummers, gebruikersnamen en e-mailadressen.

Met behulp van de UniversalSearchRobot bot kunnen gebruikers snel en gemakkelijk toegang krijgen tot verschillende zoekmachines en databases, waaronder Google, Bing, Shodan, HaveIBeenPwned en Hunter. Dit stelt gebruikers in staat om informatie te verzamelen over een persoon of organisatie en eventuele online kwetsbaarheden op te sporen.

Een van de belangrijkste kenmerken van de UniversalSearchRobot bot is de mogelijkheid om te zoeken op verschillende zoektermen. Dit omvat het zoeken op basis van telefoonnummers, e-mailadressen, gebruikersnamen IP-adres. Door simpelweg een zoekopdracht in te voeren in de bot, kan de gebruiker een overzicht krijgen van alle beschikbare informatie die relevant is voor de zoekterm.

---

[43] Bijlage Research Telegram: Onderzoektechnologieën (OSINT) -> Maltego (pagina 23 - 24)

[44] Bijlage Research Telegram: Onderzoektechnologieën (OSINT) -> Universal Search bot (pagina 25 - 26)

Telegram beveiligingsinstellingen

Accountinstellingen

Telefoonnummer

Bij het aanmaken van een nieuw Telegram-account is het vereist om een geldig telefoonnummer te gebruiken. Dit telefoonnummer wordt vervolgens altijd gebruikt om in te loggen op Telegram. Omdat een telefoonnummer kan worden gekoppeld aan een specifiek persoon, heeft Telegram sinds 6 december 2022 een nieuwe functie geïntroduceerd. Deze functie maakt gebruik van telefoonnummers vanaf de blockchain. Via anonieme telefoonnummers die beschikbaar zijn op het platform fragment1, is het nu mogelijk om anonieme Telegram-accounts aan te maken.

Vergrendelen van de applicatie

Telegram geeft de gebruiker ook de optie om twee-staps-verificatie (2FA) te gebruiken. Dit maakt het voor een potentiële hacker enorm lastig om binnen te breken in een account. Echter moet de gebruiker deze optie zelf handmatig inschakelen. Ook krijgt de gebruiker de optie om bij het openen van de app, eerst een toegangscode in te geven. Ook deze optie moet wederom handmatig door de gebruiker aangevinkt worden.

Berichten automatisch verwijderen

Telegram heeft ook een functie om specifiek gekozen groepen automatisch te verwijderen na loop van tijd. De gebruiker kan zelf dit termijn instellen.

Privacy instellingen

De gebruiker krijgt de optie om zijn gegevens openbaar te tonen, of juist verborgen te houden. Volgende gegevens komen in aanmerking:

- Telefoonnummer
- Online status
- Profielfoto
- Berichten forwarden (naar account)
- Oproepen
- Groepen & Kanalen
- Spraakberichten

Bij elk van deze gegevens kan de gebruiker kiezen uit volgende keuzes: Iedereen, mijn contacten en niemand. Er kunnen ook gebruikers toegevoegd worden met “uitzondering” voor deze instellingen.

Account verwijderen

Er is een optie mogelijk om het eigen Telegram-account, automatisch te verwijderen na verloop van tijd. De gebruiker kan er zelf voor kiezen wat deze tijdspanne is.

Opslaggebruik

De gebruiker heeft een overzicht over wat er allemaal wordt opgeslagen op zijn/haar apparaat. Ook kan de gebruiker in kwestie de cache gegevens vanuit de app bekijken. Hierbij heeft de gebruiker ook de optie om deze te verwijderen, of specifieke data te verwijderen.

Gespreksinstellingen

Groepstype

Bij het aanmaken van een groep, kan de administrator kiezen of dat de groep openbaar vindbaar is, of privé blijft. Achteraf kan deze optie nog steeds veranderd worden. Als het om een individueel gesprek gaat, kunnen beide account ervoor kiezen om chatberichten en media na verloop van tijd, automatisch verwijderd worden. Dit kan echter niet in een groepsgesprek.

Chatgeschiedenis

Wanneer er een nieuw lid in een groep terecht komt, kan die de geschiedenis van deze groep bekijken. De administrator kan ervoor kiezen of dat het de hele geschiedenis is, of de laatste 100 verstuurde berichten.

Rechten

De administrator kan de rechten van de leden in een groep zelf aanpassen. Hij/zei krijgt hier volgende opties voor:

- Tekstberichten sturen
- Media versturen (elke media optioneel)
- Gebruikers toevoegen
- Berichten vastzetten
- Chatinformatie wijzigen

Hier kunnen ook leden met uitzondering op worden toegevoegd.

Zichtbaarheid leden/ administrators

De administrator kan ervoor kiezen om de leden in een groep onzichtbaar te maken. Echter kan dit alleen bij groepen over de 100 man. Ook kan de administrator ervoor zorgen dat hijzelf onzichtbaar wordt als administrator.

Accountinstellingen	Gespreksinstellingen
Anonieme nummer (blockchain)	Openbaar/privé
Two step authentication	Chatgeschiedenis
Toegangscode	Automatische verwijderende berichten
Gesprekken automatische verwijderen	Rechten
Privacy instellingen - Telefoonnummer - Status - Forward berichten - Profielfoto - Groepen/kanalen - Spraakberichten	Zichtbaarheid leden/administratie

Account verwijderen	
Betaalgeschiedenis verwijderen	

Onderzoek open source code[45]

Telegram heeft ervoor gekozen om de broncode van de app beschikbaar te stellen als open source, waardoor ontwikkelaars de mogelijkheid hebben om de app aan te passen, verbeteren en te integreren met andere toepassingen.

De broncode van Telegram is beschikbaar op GitHub[46], een platform voor softwareontwikkeling. Het is beschikbaar onder de GPLv3-licentie, wat betekent dat ontwikkelaars de vrijheid hebben om de code te gebruiken, te wijzigen en te distribueren.

Telegram biedt ook een open API aan, waarmee ontwikkelaars bots en andere toepassingen kunnen ontwikkelen die communiceren met de Telegram-app. De API is beschikbaar op de website van Telegram.

Telegram is geschreven in verschillende programmeertalen, waaronder C++, Java, Python en Objective-C. De app maakt gebruik van de MTProto-encryptieprotocol om de beveiliging en privacy van gebruikers te waarborgen.

De broncode van Telegram wordt regelmatig gecontroleerd op beveiligingsproblemen en kwetsbaarheden door de Telegram-beveiligingsgemeenschap. Het openstellen van de broncode stelt gebruikers en ontwikkelaars in staat om feedback te geven en bugs en andere problemen te melden aan het Telegram-ontwikkelingsteam. Dit kan leiden tot verbeteringen en updates van de app.

Hoewel Telegram over het algemeen een open-source platform is, zijn er enkele delen van de code die niet openbaar beschikbaar zijn gesteld.

Een van deze delen is de server-side code die wordt gebruikt om de Telegram-servers te beheren. Dit deel van de code is niet openbaar beschikbaar gesteld en wordt beheerd door de ontwikkelaars van Telegram zelf.

Daarnaast zijn er enkele delen van de client-side code die niet open-source zijn, zoals de code voor de geheime chat-functie. Deze functie maakt gebruik van end-to-end-encryptie om de privacy van gebruikers te waarborgen.

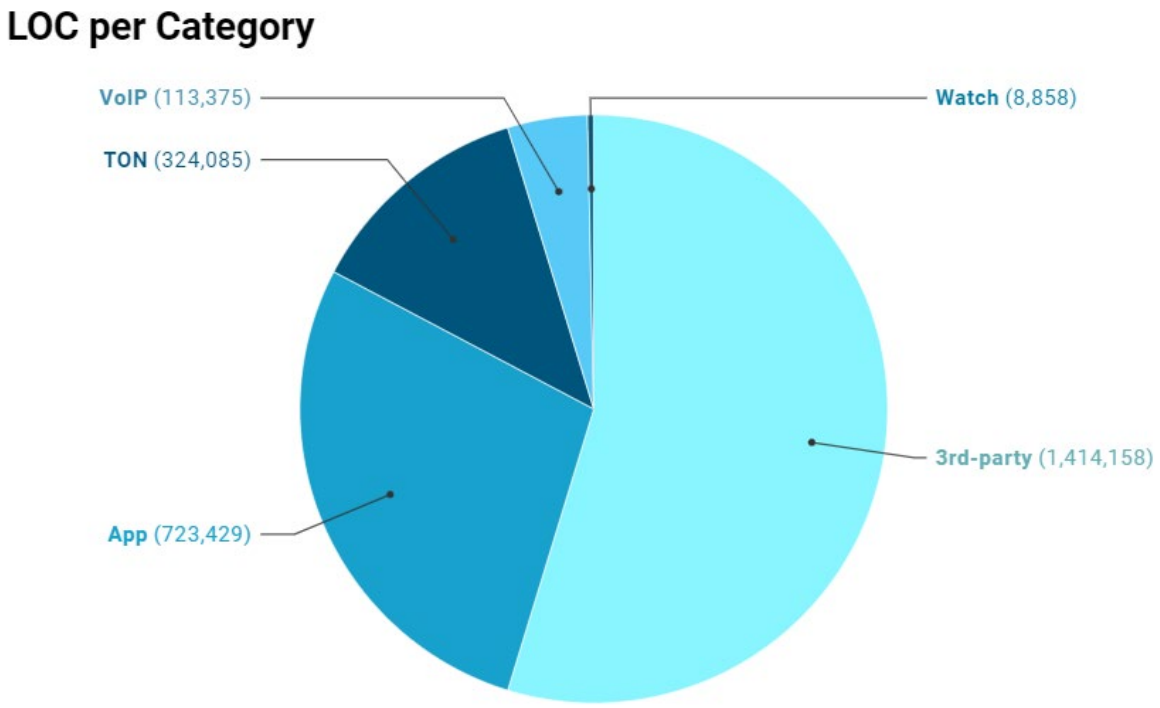
De reden waarom deze delen van de code niet openbaar beschikbaar zijn gesteld, is omdat het Telegram-team van mening is dat deze delen van de code hun intellectuele eigendom zijn en dat het openbaar beschikbaar stellen van deze code de veiligheid van het platform in gevaar zou kunnen brengen.

[45] https://grg.pw/2018/04/telegram-is-down-again-a-deep-look-at-their-infrastructure/
[46] Https://github.com/telegramdesktop/tdesktop

IOS

Telegram-iOS organiseert de broncode in meer dan 200 sub modules met meer dan twee miljoen regels code. De modules kunnen in 5 categorieën worden ingedeeld

- **App**, modules die de belangrijkste functies van de app ondersteunen, zoals foundation utils, UI, netwerk, enz.
- **VoIP**, de functie voor spraakoproepen die eind maart 2017 werd uitgebracht. **TON**, de experimentele integratie met het nieuwe blockchain platform.
- **3rd-party**, de andere open-source projecten waar het van afhankelijk is.



Verschillen tussen web, app en desktop

De keuze tussen Telegram Web, Telegram App en Telegram Desktop hangt af van je voorkeuren en behoeften. Telegram Web is handig als je Telegram wilt gebruiken zonder iets te installeren, terwijl de app en desktop-versie handig zijn als je meer functies en extra voordelen nodig hebt, zoals push-notificaties en integratie met andere functies op je apparaat.

Uitlezingen[47]

Om meer te weten te komen over wat de exacte mogelijkheden zijn voor het uitlezen van informatie die van Telegram afkomstig is hebben we de proef op de som genomen. In de onderstaande punten kan je terugvinden wat we exact gedaan hebben om dit te testen en wat dat de verschillende uitkomsten hier nu uiteindelijk mee zijn. Dit is zowel voor Android

[47] Bijlage Research Telegram: Uitlezingen (pagina 27 - 35)

Mogelijkheden uitlezen Android

De vaststellingen uit dit onderzoek zijn afkomstig van de startgegevens die je in de tabel in bijlage kan terugvinden. Hierin staat alle nodige informatie die je nodig hebt om een overzicht te krijgen over de startinformatie.

Wat kan men terugvinden?

Volgens de collega's van mobile forensics zal men verschillende zaken kunnen terugvinden, afhankelijk van de stand van het toestel. Als men toegang heeft tot de telefoon kan men alle verstuurde berichten, foto's en audiofragmenten terugvinden. Men is in sommige gevallen ook in staat om materiaal dat verwijderd is terug te halen, als het apparaat deze zelf nog niet heeft verwerkt.

In de onderstaande tabel kan je een overzicht zien van wat wij effectief terugvonden. Dit resultaat bevestigt dus ook deze uitspraken.

Type chat	Type bericht	Gevonden?
Tekst	Standaard	**Heimelijk**
Foto	Standaard	
Tekst	Groep met admin rechten	
Foto	Groep met admin rechten	
Tekst	Groep zonder admin rechten	
Foto	Groep zonder admin rechten	
Tekst	Standaard	
Foto	Standaard	
Tekst	Secret	
Foto	Secret	
Tekst	Zelfvernietigend	
Foto	Zelfvernietigend	
Tekst	Achteraf verwijderd	
Foto	Achteraf verwijderd	

Gerecupereerde berichten lege cache

Type chat	Type bericht	Gevonden?
Tekst	Standaard	**Heimelijk**
Foto	Standaard	
Tekst	Groep met admin rechten	
Foto	Groep met admin rechten	
Tekst	Groep zonder admin rechten	
Foto	Groep zonder admin rechten	
Tekst	Standaard	
Foto	Standaard	
Tekst	Secret	
Foto	Secret	
Tekst	Zelfvernietigend	

Foto	Zelfvernietigend	
Tekst	Achteraf verwijderd	
Foto	Achteraf verwijderd	

Een andere optie die bekeken is een uitlezing met een juist verwijderd cachegeheugen van de telefoon. Het resultaat dat je hierbij kan bekomen zie je in de tabel hieronder.

De conclusie die je hierbij kan vormen is dat zo goed als alle tekstberichten worden teruggevonden. Enkel de achteraf verwijderde en zelfvernietigende tekstberichten en foto's vinden we niet meer terug. Bij de foto's zelf kan je enkel zien dat er een foto verstuurd is geweest maar niet meer om welke foto het gaat.

Gerecupereerde berichten bij uitgelogd account

Nog een andere optie die we bekeken hebben is een uitlezing nadat het account uitgelogd was. Bij dit soort uitlezingen kan je geen data terugvinden. Wanneer we terug inloggen krijgen we echter wel terug data te zien. Het resultaat hiervan kan je in de tabel hieronder terugvinden.

Type chat	Type bericht	Gevonden?
Tekst	Standaard	**Heimelijk**
Foto	Standaard	
Tekst	Groep met admin rechten	
Foto	Groep met admin rechten	
Tekst	Groep zonder admin rechten	
Foto	Groep zonder admin rechten	
Tekst	Standaard	
Foto	Standaard	
Tekst	Secret	
Foto	Secret	
Tekst	Zelfvernietigend	
Foto	Zelfvernietigend	
Tekst	Achteraf verwijderd	
Foto	Achteraf verwijderd	

Een belangrijke iets om te weten is dat er nog enkele stappen dienen uitgevoerd te worden alvorens we effectief data terug kunnen vinden.

1) De eerste stap die dat we dienen uit te voeren is het laten versturen van een sms naar het nummer van het telegram account. Dit dient om je account terug in te loggen aangezien telegram niet van een wachtwoord gebruik maakt.
2) Vervolgens dien je iedere chat aan te klikken en ver genoeg door te scrollen zodat alle berichten terug kunnen inladen. Deze stappen zijn essentieel om effectief data terug te vinden.

We kunnen dus concluderen dat er bij een uitgelogd account geen data zal worden teruggevonden en dat men na het inloggen de chats nog gaat moeten inladen alvorens we deze bij de uitlezing gaat terugvinden. Echter is het belangrijk om te weten dat hiervoor andere bevelschriften gelden.

Gerecupereerde berichten na externe verwijdering

Een andere optie die we onderzocht hebben is een uitlezing nadat er berichten extern waren verwijderd. De resultaten die hieruit zijn gekomen zijn identiek aan deze die uit de uitlezing met een lege cache komen. Het is dus belangrijk om te onthouden dat je, als het telegram account uitgelogd is, eerst een uitlezing doet alvorens je de chats volledig inlaad. Hierna doe je dan nog een uitlezing met de chats wel ingeladen. Dit komt omdat, als een foto het laatst verstuurd of ontvangen bericht was, deze eventueel extern verwijderd zou kunnen zijn waardoor je deze niet zou kunnen terugvinden. Te allen tijde dus twee uitlezingen doen om zeker te zijn is de boodschap.

Verwijdering met "nieuwe" simkaart

We hebben ook gekeken wat het resultaat zou zijn als dat de verdacht een nieuwe simkaart zou aanvragen en berichten zou verwijderen aan de hand hiervan. We kunnen concluderen dat ook hier de resultaten weer gelijkaardig zijn aan de uitlezing met de lege cache. Hier dient rekening mee gehouden te worden in toekomstige uitlezingen van dit kaliber.

Gerecupereerde berichten met pincode

Een andere optie die we onderzocht hebben is een uitlezing waarbij dat Telegram vergrendeld is met een pincode. Dit bevatte tegen alle verwachtingen in nog altijd alle berichten zoals we terugvonden bij onze allereerste uitlezing. We vinden dus ook nog de verwijderde berichten en alle foto's terug.

Uitlezingen met 2FA

Een laatste optie die we onderzocht hebben is het effect van twee-factorauthenticatie op een uitlezing. Echter zal dit nooit effect hebben op de resultaten van de uitlezing. Twee-factorauthenticatie zal enkel effect hebben wanneer men opnieuw dient in te loggen. Het toestel uitschakelen heeft hierop dus ook geen invloed. Wanneer we echter voor de eerste keer op een apparaat inloggen of we zijn uitgelogd op ons account zullen we nu een wachtwoord moeten invoeren en een code die we via sms ontvangen. Dit wachtwoord zal in sommige gevallen dus eerst achterhaald moeten worden alvorens we het toestel zouden kunnen uitlezen.

Mogelijkheden uitlezen iOS

Op het moment van documenteren, was er geen mogelijkheid om uitlezingen te testen op IOS-apparaten.

Verstuurde berichten

In de tabel in bijlage kan je een overzicht terugvinden van alle berichten die dat zijn verstuurd. Je kan erin terugvinden wie dat het bericht verstuurd heeft, wie het heeft ontvangen en of het bericht in een groep is verstuurd. Ook is er nog een kolom voorzien met bijkomende informatie.

Metadata

Voor het testen van de metadata bij een foto hebben we zowel gebruik gemaakt van foto's genomen door een iOS toestel, een Android toestel als ook foto's genomen via

de telegram applicatie zelf. Deze foto's zijn vervolgens van en naar het toestel dat wordt uitgelezen gestuurd om zo te zien wat er met de metadata binnen Telegram gebeurt. We kunnen hierbij concluderen dat elke foto, hoe hij ook verstuurd wordt, geen metadata opslaat nadat hij via Telegram is verstuurd. Dit is hetzelfde resultaat zowel bij het Android toestel als bij het iOS toestel.

Type foto	Type toestel	Metadata?
Camera	IOS	**Heimelijk**
Camera	Android	
Camera telegram	IOS	
Camera telegram	Android	
Afbeelding internet	IOS	
Afbeelding internet	IOS	

Flowchart

Wanneer je een toestel wenst uit te lezen kan je onderstaand flowchart volgen om tot het ideale scenario te komen om het toestel uit te lezen. Het is echter wel belangrijk dat je eerst toegang tot het toestel hebt en dat je het bij aanvang van dit flowchart in vliegtuigstand zet om data verlies te vermijden.

Exporteren chats + scripts

Je kunt nu eenvoudig je Telegram-chats exporteren via de app. Om dit te doen, open je de Telegram-app op je apparaat en volg je deze stappen: Navigeer naar de chat die je wilt exporteren en tik op het menu-icoon (meestal drie verticale stippen) in de rechterbovenhoek van het chatscherm. Kies vervolgens de optie "Exporteren chatgeschiedenis". Je krijgt de keuze om de chat te exporteren met of zonder mediabestanden. Selecteer de gewenste optie en selecteer waar je de geëxporteerde chat wilt opslaan, zoals je interne opslag, cloudopslag of een andere locatie. Bevestig je keuze en wacht tot het exporteerproces is voltooid. Dit kan enige tijd duren, afhankelijk van de grootte van de chatgeschiedenis en de bijgevoegde media.

Bovendien zijn er speciale scripts beschikbaar die je kunnen helpen bij het downloaden van alle user Ids en mediabestanden. Deze scripts zijn te vinden op de Git Bucket van de CCU. Met behulp van deze handige functionaliteit kun je niet alleen je chats exporteren, maar ook belangrijke bestanden veiligstellen en een back-up maken van je waardevolle informatie.

Sessie overname

In het externe document “Overname_Telegram_Sessie” kan je terugvinden hoe dat je een sessie kan overnemen op zwel een mobiel apparaat als op een desktop.

Bronnen[48]

Je kan alle gebruikte bronnen terugvinden in de bijlage.

[48] Bijlage Research Telegram: Onderzoektechnologieën (OSINT) -> theHarvester (pagina 35 - 38)