

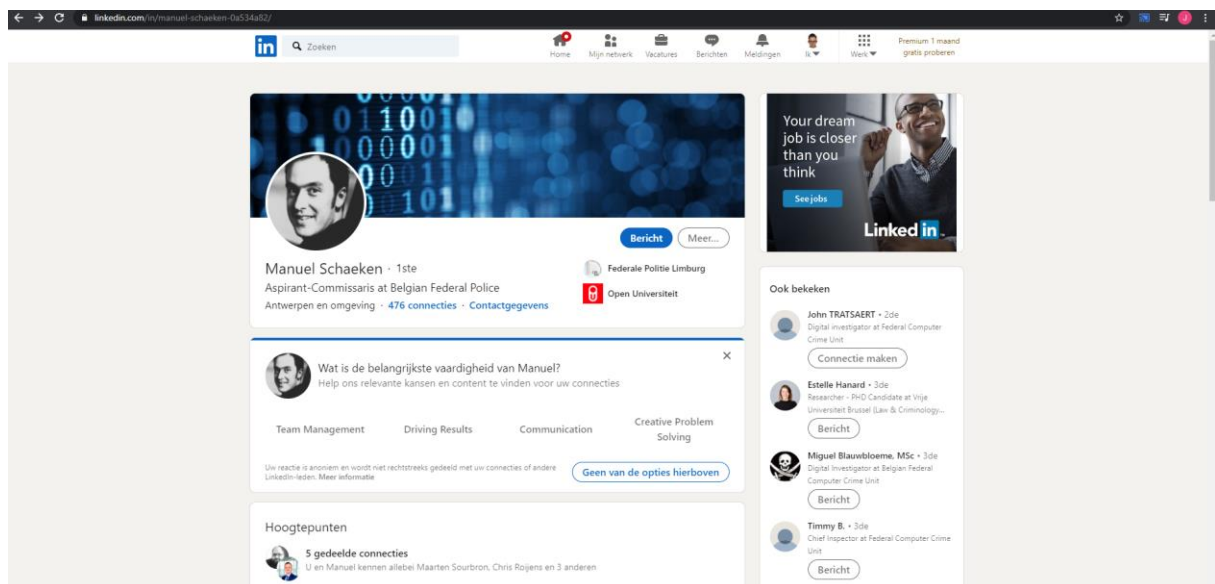
RCCU: Uitdagingen in de wereld van e-forensics & Cybercrime

Op woensdag 16 december 2020 vond het seminarie plaats over de uitdagingen in de wereld van *e-forensics* en cybercrime.

Mijn verwachtingen lagen toch wel zeer hoog. Ik ben namelijk zeer geboeid door e-forensics en cybercrime. Vroeger, toen ik nog een klein jongetje was, droomde ik ervan om later als politieagent aan de slag te gaan. Mijn grootste droom is cybercrime-specialist binnen de federale politie.

Ik zou graag uitleg willen krijgen hoe het nu precies in zijn werk gaat bij de cybercrime unit van de politie. Wat doen ze precies? Is het zwaar? Worden er ook moorden geanalyseerd? Met welke uitdagingen worden ze geconfronteerd?

De spreker heet Manuel Schaeken en is afkomstig van de Kempen. De link naar zijn LinkedIn-profiel is <https://www.linkedin.com/in/manuel-schaeken-0a534a82/>.



Hij vertelde dat de cybercrime unit een afdeling is binnen de federale gerechtelijke politie en dat ze zowel voor de federale als lokale politie werken. Meneer Schaeken wist ons te vertellen dat hij hoofdinspecteur en afdelingshoofd is van de cybercrime unit. Toen hij afstudeerde is hij als *software developer* aan de slag gegaan en daarna is hij zelfs *software manager* geweest. Hij werkt nu bij de politie omdat zijn papa ook bij de politie werkte. Een aantal krantenartikels over cybercrime zijn onder andere: “Hacker steelt gegevens van half miljoen patiënten”, “Man doet zich voor als escortdame en steelt 100 000 euro” en “Amsterdamse student aangehouden in Belgisch hackdossier”.

Er bestaan twee wetboeken. Eén ervan is het strafwetboek waarin de straffen staan en het tweede is het strafvordering wetboek. In dit tweede staat beschreven hoe je met een magistraat dient om te gaan en hoe de processen werken. Een derde aspect dat er in beschreven wordt is waar je je aan dient te houden. Dus met andere woorden, wat mag je wel en niet doen. Meneer Schaeken zei dat je het strafwetboek jaarlijks dient te studeren. Dit had ik eigenlijk wel niet verwacht. De wetgeving

tussen de verschillende landen is ook totaal anders. Zo heeft Amerika andere wetten dan wij hier in België.

Manuel gaf ons een mooie anekdote. Hij vertelde dat hij eens in het buitenland was en toen hadden ze een huiszoeking gedaan met de agenten van dat land. Gedurende de huiszoeking troffen ze de man aan in zijn huis. De programma's waarmee hij werkte om informatie te vergaren stonden nog open op zijn computer. Zodanig hadden ze de man op heterdaad betrapt.

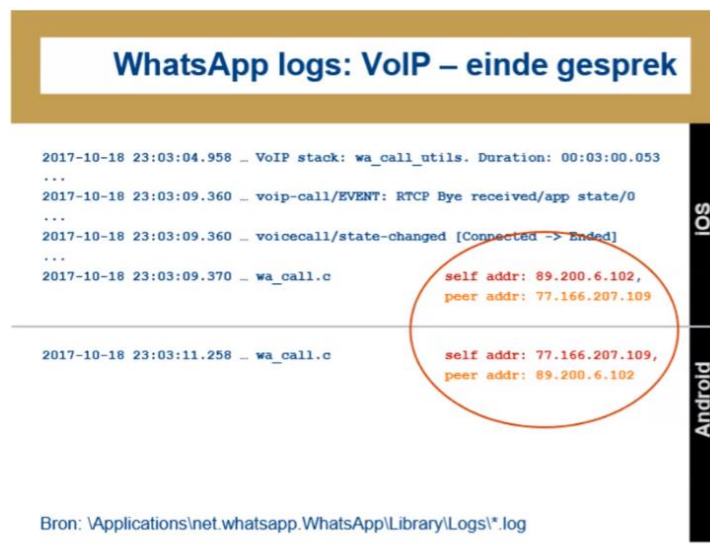
Verder worden er ook moorden onderzocht. Dit had ik wel niet verwacht. Ik dacht altijd dat de cybercrime unit van de politie enkel en alleen cybercriminelen opspoorde en zo uitzocht wat ze mispeuterden. Als er nu ergens een moord gebeurt en er ligt bijvoorbeeld een mobiele telefoon of een laptop bij de plaats delict, dan wordt de cybercrime unit opgeroepen. Dan gaan zij deze toestellen onderzoeken.

Wanneer er nu een moord gepleegd wordt gaan de onderzoekers binnen de cybercrime unit soms naar de rechtbank om aan de rechter uit te leggen wat ze gevonden hebben. Verder dienen ze de bewijzen ook te documenteren voor de grondrechters.

Uiteraard bevat elk onderzoek een onderzoeksleider. Dit is het ministerie van Justitie. Zij geven bijvoorbeeld de opdracht om een mobiel toestel te onderzoeken of het opvragen van de gegevens van een Facebookaccount. Daarnaast geven ze ook toestemming om een huiszoeking te doen.

Wat ik totaal niet verwachtte is dat je een maximum aantal toestellen per persoon mag meenemen gedurende een huiszoeking.

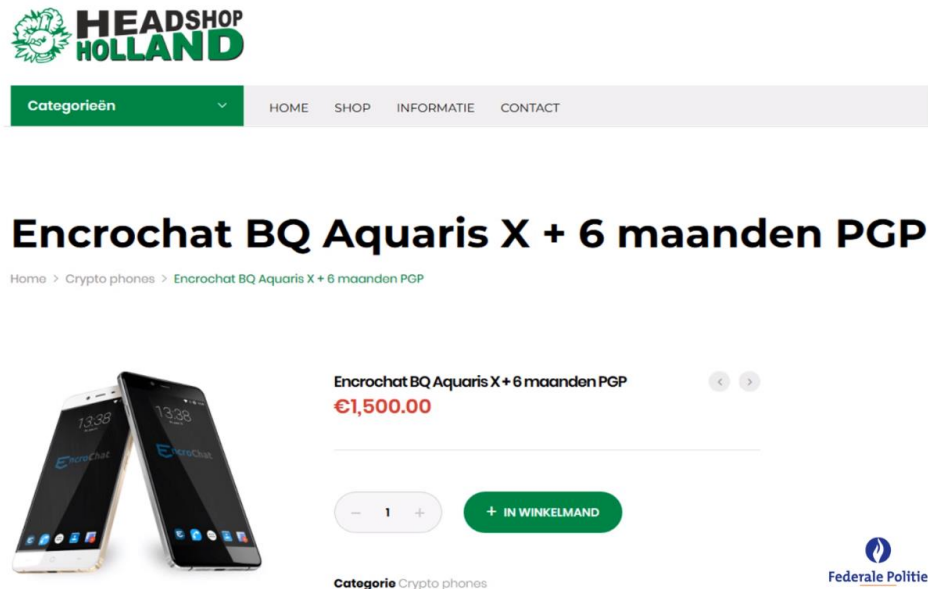
Bij forensisch onderzoek is het belangrijk dat alles onderzocht wordt. Zo kunnen bijvoorbeeld Whatsapp gesprekken achterhaald worden.



Ook harde schijven kunnen volledig onderzocht worden. Soms gooien criminelen de harde schijven kapot omdat ze denken dat deze dan niet onderzocht kunnen worden maar dat is een grote tegenvaller.

Mobile forensics bestaat ook. Dit komt vaak voor in de criminele wereld. Zo kunnen contacten, memo's, oproepen, berichten, afbeeldingen, video's enzoverder achterhaald worden.

Criminelen gebruiken smartphones die enorm hard op iPhones lijken. De data op deze toestellen kan van op afstand verwijderd worden. Manuel zei dat je eigenlijk een fake omgeving ziet als je het toestel gebruikt maar van hier uit kan je naar de echte omgeving gaan. Onderstaande afbeelding bevat zo'n dergelijke smartphone.



Deze mobiele toestellen worden dan in een zakje gestopt in een correcte omgeving om te voorkomen dat de toestellen van op een afstand worden leeggemaakt. Zo kunnen de toestellen verder onderzocht worden.



Wat ik totaal niet verwachtte is dat de cybercrime unit van de politie ook wagens onderzoekt bij een ongeval. Zo kan men te weten komen waar het voertuig geweest is, welke handelingen er met het voertuig zijn gesteld en wie er in het voertuig zat. Dit aspect wordt ook wel automotive genoemd. Bij een zwaar ongeval, waarbij de auto volledig kapot is, is dit niet altijd makkelijk.

De meeste voertuigen bevatten systemen waarmee je je smartphone kan connecteren. Zo kan men de contacten, berichten en de oproepen onderzoeken.

Het laatste aspect dat de heer Schaeken ons uitlegde zijn de verschillende vormen van cybercrime. Deze kende ik al omdat ik deze al heb geleerd tijdens de lessen "Security Essentials" en "Security Advanced". Toch ga ik ze even kort toelichten.

Een voorbeeld van zo een cybercrime is informatica senu lato. Dit is een vorm informatiecriminaliteit. Hierbij worden inbreuken gepleegd op de auteurswetgeving (uploaden en downloaden van bestanden). Ook kinderporno en racisme zijn aspecten dat tot informatiecriminaliteit behoren.

Vervolgens heb je ransomware. De laatste jaren is er een toename van deze cybercrime ten opzichte van bedrijven. Het gaat immers om vertrouwelijke en kritische gegevens en als je je gegevens terug wilt halen moet je uiteraard betalen met de cryptomunt Bitcoin.

Een voorbeeld van ransomware is Wannacry.



Wat ik niet wist is dat er ook "TrumpLocker" bestaat. Hiermee kunnen bestanden op je computer geëncrypteerd worden en als je ze terug wilt dan zal je moeten betalen in TrumpCoin.

TrumpCoin V1 to V2 Swap

Send V1 Coins Here:

Please send in a single transaction

TPAkyU6ZsJq9MsExjcm86DuBb0GUSHf5

Provide the info using the form below

V2 coins are sent manually

Email *

oob@mail.com

Swap Amount *

0.00000000

V2 Address *

TMY2H1QvWyykPbJ22x1tM8w7seFQnV

V1 TXID *

18634dc1347bwd7d7bca4c3288b643ba8d4d0315a878a093a573bd0c1243c

☐ I'm not a robot

Submit

This is the address you will send your original V1 Trump Coins to from your original wallet

Add your email address here

Type in the exact amount of V1 Trumps your sending

Supply a new address from your new Wallet. This is the address we will send Trump Coins V2

Provide the Transaction ID. This is the TXID from your original wallet

The form is a receipt of the transaction. All your things are sending into an address as you normally do with any coin. Except your supplying us with some details and a return address. From your new wallet we will send you V2 Trumps Coins.

De laatste vorm van cybercrime dat besproken werd is (spear-)phishing. Hierbij wilt de hacker gevoelige informatie zoals wachtwoorden, gebruikersnamen of creditcard gegevens achterhalen doormiddel van fictieve websites of door e-mails te versturen met een phishing link in.

Dit seminarie vind ik het leukste en meest interessante van het totaal seminars dat ik heb gevolgd. Dit komt grotendeels doordat ik geboeid ben door het security aspect. Vooral de cybercrime unit van de federale overheid spreekt mij enorm hard aan. Vroeger droomde ik ervan om politieagent te worden. Sinds kort wil ik deel uitmaken van de cybercrime unit. Daarom had ik ook gesolliciteerd voor een stage bij de RCCU en politiezone CARMA.

Ik heb weer wat zaken bijgeleerd maar soms was het wat moeilijker om te volgen. Dit vind ik persoonlijk niet zo erg omdat de heer Schaeken natuurlijk ook veel wilde uitleggen.

De heer Schaeken vertelde zeer boeiend. Daarom was ik zeer geboeid door de informatie en zaken die we kregen voorgeschoteld.

Het meest interessante aan dit seminarie vond ik de uitleg omtrent hoe de cybercrime unit nu precies werkt en wat ze doen. Daarnaast vond ik het ook erg boeiend om meer uitleg te krijgen omtrent forensisch onderzoek binnen informatica.

Ten slotte heb ik ook nieuwe informatie gekregen wat betreft cybercrime unit. Ze onderzoeken auto's bij een ongeval, moorden, doen huiszoekingen en dragen zelfs een wit pak bij huiszoekingen.

Ik dacht altijd dat de cybercrime unit enkel en alleen personen opspoorden maar dat is dus niet zo.

Het seminarie eindigde met het werkveld binnen de unit. Zo kregen we te horen dat er elk jaar vacatures uitgezonden worden omdat de cybercrime unit onderbemand is.

Laat ons hopen dat ik ooit als onderzoeker binnen de cybercrime unit van de politie kan werken.

