Eindrapportage

WiFi Probe Requests

projectnaam: WiFi Probe Requests
contactpersoon: [redacted] 10.2.e.
datum: 2014-10-15
versie: 30: 5285cefa5c7c

Inleiding

Dit is een eindrapportage voor het project *WiFi Probe Requests*, dat in het kader van het NCTV-programma *Veilig door Innovatie* door het Nederlands Forensisch Instituut is uitgevoerd tussen juli 2013 en november 2014.

Het projectvoorstel behorende bij dit project is bijgevoegd. Het projectvoorstel bevat een inleiding die helpt om de technische en forensische achtergrond van het project te begrijpen. Deze achtergrondinformatie is in beknopte vorm ook terug te vinden in het door NCTV gepubliceerde nieuwsartikel te http://www.nctv.nl/actueel/overig-nieuws/onderzoek-nfi-digitale-wifi-sporen.aspx .

Het probleem waar het project aan tegemoetkomt is verwoord in secties 1.1-1.3 van dat voorstel. In sectie 1.3 ("Doelstelling") worden de projectdoelen genoemd. Het gaat om het verwerven van de volgende *capabilities*:

1. Gegeven informatie over een PD, een inschatting kunnen maken van hoe waarschijnlijk het zal zijn dat er nog sporen van dit type kunnen worden aangetroffen.
2. Een analysemethode voorhanden hebben die, gegeven een geheugendump, aanwezige sporen zichtbaar maakt. De analysemethode moet door opsporingsdiensten gebruikt kunnen worden, de BDE's staan model voor het niveau van de doelgroep.

Het project kende een gefaseerde opzet. Over het verloop en de resultaten van de fasen wordt afzonderlijk gerapporteerd in secties 1 en 2. Sectie 3 behandelt de financiën.

1. Fase 1

In deze fase is wetenschappelijk onderzoek uitgevoerd dat inzicht geeft in de spoorvorming. Tegen verwachting in is gebleken dat het fenomeen vrij algemeen en in uiteenlopende configuraties voorkomt, waardoor het interessant werd om de scope uit te breiden en ook een ander spoortype te onderzoeken — hierdoor kwam een breder scala aan apparatuur (laptops, tablets, mobiele telefoons) onder de aandacht dan alleen de basisstations, en ook een ander type signaal (*beacons*).

1.1 Opdracht

In het projectvoorstel zijn voor deze fase de volgende producten gedefiniëerd:

1. Een wetenschappelijk rapport dat de geteste parameters en hun invloed op de spoorvorming beschrijft.
2. Een schema met een vereenvoudigde versie van de parameterbeschrijving, geschikt voor snelle beantwoording van vragen die zich op plaats delict kunnen voordoen.

Deze komen tegemoet aan het volgende doel (ook genoemd in de inleiding):

1. Gegeven informatie over een PD, een inschatting kunnen maken van hoe waarschijnlijk het zal zijn dat er nog sporen van dit type kunnen worden aangetroffen.

1.2 Verloop

Gedurende de zomer en het najaar van 2013 zijn experimenten uitgevoerd om het mechanisme achter de spoorvorming te achterhalen en te parametriseren.

Op 18 november 2013 zijn de onderzoeksresultaten gepresenteerd op de zgn "Themadagen digitale opsporing", een congres dat jaarlijks door het NFI en verschillende opsporingsorganisaties wordt georganiseerd. Vanwege de belangstelling voor dit onderwerp is de workshop twee maal gegeven. Bijzonder punt van aandacht in discussies waren de omgevingsfactoren (en met name de inschatting daarvan) die van invloed zijn op het spoor, en hoe er op plaatsen delict moet worden opgetreden om het spoor te conserveren.

Op 7 december is een wetenschappelijk artikel ingediend voor de internationale *Digital Forensic Research Workshop*-conferentie (http://dfrws.org). Het artikel is *peer review* gepasseerd en geaccepteerd voor de conferentie, op welke op 8 mei 2014 de resultaten zijn gepresenteerd. Het artikel is uitgegeven door Elsevier als onderdeel van het journal *Digital Investigation*. De publicatie is publiek online beschikbaar: http://dx.doi.org/10.1016/j.diin.2014.03.013 .

1.3 Resultaten

- Product 1, het wetenschappelijk rapport, is gerealiseerd. Het rapport beschrijft naast de in de productdefinitie genoemde onderdelen, ook hoe het spoor zichtbaar gemaakt kan worden, en welke tactische afleidingen in de opsporing gedaan kunnen worden op basis van de blootgelegde sporen.
- Product 2, het schema met een vereenvoudigde parameterbeschrijving, is niet gerealiseerd. Uit het onderzoek is namelijk gebleken dat er, met name voor de apparaten die in de verbrede scope voorkomen, omgevingsfactoren zijn die van grote invloed zijn op de spoorvorming. Echter, er is weinig bekend over in hoeverre met die omgevingsfactoren — voor het gemak: storende signalen, die het spoor laten vervluchtigen — rekening moet worden gehouden. Kortom, er miste nog informatie die nodig zou zijn om beslissingen 'in het veld' te ondersteunen.

1.4 Doelen

De resultaten brengen ons dichter bij doelstelling 1, in zoverre dat bepaalde situaties op voorhand uit te sluiten zijn op basis van de in het wetenschappelijk artikel beschreven parameters. Desalniettemin zou nog meer gedaan kunnen worden gedaan om een vertaling naar de praktijk te maken.

Met de resultaten is doelstelling 2 (zie inleiding) — het voorhanden hebben van een analysemethode die de sporen in een geheugendump blootlegt — ook bereikt. Dat was niet voorzien. Fase 2 zou dienen voor het behalen van dit doel.

2. Fase 2

Uit 1.3 en 1.4 blijkt het volgende. Enerzijds: Fase 2 diende oorspronkelijk om doelstelling 2 te behalen. Echter, die doelstelling (het voorhanden hebben van een analysemethode) is reeds behaald in fase 1. Anderzijds is doelstelling 1 maar ten dele behaald; er zou meer onderzoek kunnen plaatsvinden om een vertaling naar de praktijk te maken.

Daarnaast is ook duidelijk geworden dat, alhoewel het een digitaal spoor betreft, het in eerste aanleg niet de bureaus digitale expertise zijn die worden ingezet op een plaats delict — het kenmerkende van het spoor is nu juist dat élke plaats delict potentieel een digitale component heeft. De BDE's zitten voor de meeste plaatsen delict niet in de lijn. Het spoor, en de omgang ermee in de praktijk, zal via een andere weg onder de aandacht gebracht moeten worden gebracht in de politie-organisatie om conservering op plaats delict te kunnen borgen.

Dit overwegende is op 23 april 2014 een verzoek tot wijziging van de inhoud van fase 2 ingediend. Voorgesteld is om veldmetingen te doen op (historische) plaatsen delict, om op die manier meer inzicht te krijgen in de houdbaarheid van sporen in praktijksituaties, en op die manier verder tegemoet te komen aan doelstelling 1.

Dit verzoek is ingewilligd (kenmerk: 523117; 11 juni 2014).

2.1 Opdracht

Het voor fase 1 gestelde doel blijft staan:

1. Gegeven informatie over een PD, een inschatting kunnen maken van hoe waarschijnlijk het zal zijn dat er nog sporen van dit type kunnen worden aangetroffen.

Daarnaast formuleren we een nieuw, derde doel, dat betrekking heeft op forensisch-organisatorische aspect van de praktijk:

3. De recherche-keten kennis geven om het spoortype in overweging te nemen bij a) het veiligstellen van bewijsmateriaal op een plaats delict en b) het opzetten van een forensisch onderzoek.

2.2 Verloop, resultaten

1. Tussen 11 juni en 9 september is bij politieregio's geïnventariseerd voor historische plaatsen delict met geschikte kenmerken. Uit de regio Midden-Nederland is een lijst met plaatsen delict uit de zaak rond de Utrechtse serieverkrachter beschikbaar gesteld. Op 14 september zijn op zes van die lokaties metingen gedaan.
2. Er is een dataset aangelegd van beacon-signalen van 18046 basisstations. Van deze dataset zijn statistieken berekend die tonen hoe snel er in de opsporing gehandeld moet worden om een tijdsbepaling te kunnen doen.
3. Als case-study is een geheugendump uit een NFI-zaak geanalyseerd op via blootgelegde beacon frames te achterhalen locatie-informatie.
4. De resultaten van punt 1,2 en 3 zijn op 2 oktober 2014 gepresenteerd op een zgn. "Kennisavond". Deze avonden dienen om forensisch coördinatoren en openbaar ministerie voor te lichten over nieuwe ontwikkelingen op forensisch gebied.

2.3 Doelen

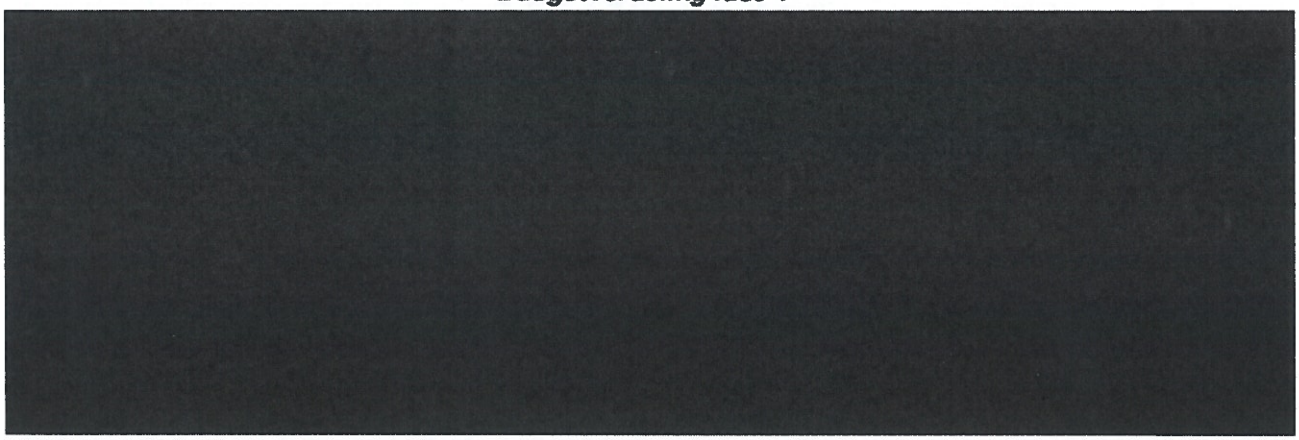
Met resultaat 1 is, voor zover mogelijk, doelstelling 1 bereikt. De veldmetingen wijzen namelijk uit dat door omstandigheden op kleine schaal (lokaal terreinreliëf, begroeïng) binnen gebieden met veel storende signalen lokaal toch vaak plaatsen van radiostilte voorkomen. Op basis van een beschrijving van een plaats delict kan slechts een eerste schifting worden gemaakt, vervolgens kan het beste op een geschikt moment alsnog een veldmeting op plaats delict worden gedaan om een betere inschatting te maken.

Doelstelling 3, met betrekking tot de plaats van het spoortype in de praktijk, is met resultaat 4 behaald. Vroege signalering van een mogelijkheid tot benutten van het spoortype is hierbij het belangrijkst; het NFI kan vervolgens bijstaan in de fasen van veiligstellen en analyse.

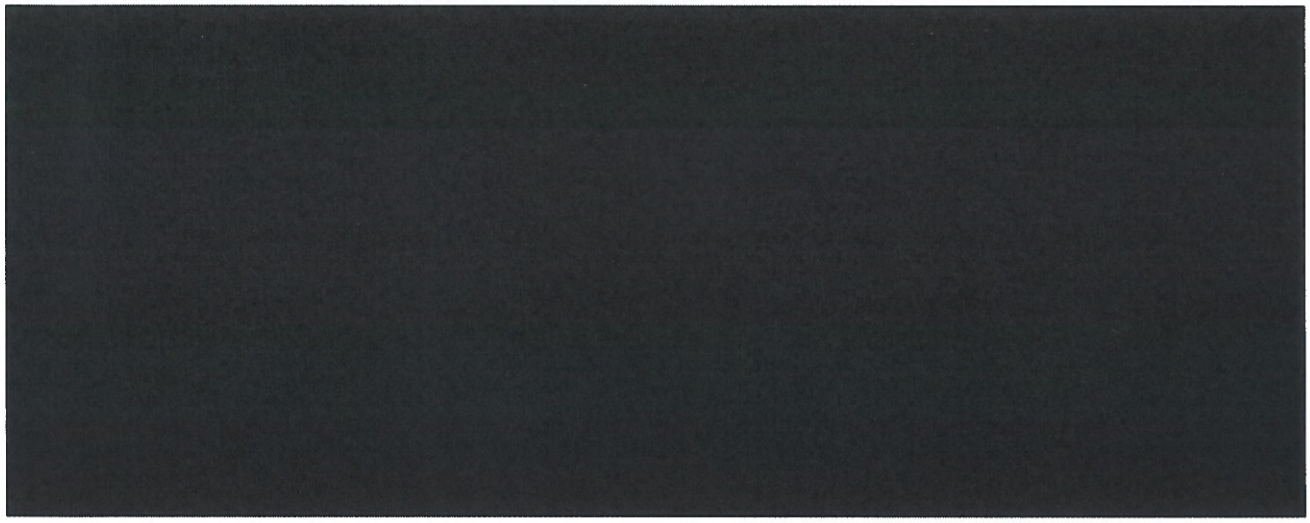
3 Financiën

Fase 1 is binnen begroting afgerond, zij het met andere accenten in de uurbesteding dan geraamd. De presentatie op de DFRWS-conferentie is niet bekostigd uit de projectsubsidie. De uren voor verslaglegging zijn weliswaar onder fase 1 geschaard, maar zijn aangesproken voor alle verslaglegging, ook deze eindrapportage en het wijzigingsverzoek voor fase 2.

Budgetverdeling fase 1



Fase 2 kent een gewijzigde vorm, waarvoor de indeling in posten zoals in de oorspronkelijke budgetraming (voor softwareontwikkeling) niet geschikt is.



Een verzoek tot vaststelling van de subsidie wordt separaat van deze eindrapportage ingediend.

Buiten scope verzoek