

WiFi Probe Requests

Tussenrapportage

projectnaam: WiFi Probe Requests

contactpersoon: [REDACTED]

10.2.e.

datum: 2014-01-19

versie: 22: d1f79e1fdeff

Inleiding

Dit document is een tussenrapportage voor het 'WiFi Probe Requests'-project en besluit fase 1 van dat project. Het informeert over de behaalde doelen en de financiële status. Daarnaast bevat het een discussie over fase 2 en een doorkijk naar hoe de resultaten van het onderzoek kunnen worden vertaald naar de praktijk. In dit document wordt meermaals verwezen naar het projectvoorstel.

1. Resultaten fase 1

1.1 Wetenschappelijk rapport

Over de bevindingen in het onderzoek is een wetenschappelijk rapport opgesteld. Dit is produkt 1, zoals genoemd onder paragraaf 1.4 in het projectplan:

1. Een wetenschappelijk rapport dat de geteste parameters en hun invloed op de spoorvorming beschrijft.

Met het rapport, meegeleverd met dit document, lost het NFI de prestatieverplichting voor fase 1 in. Het rapport is momenteel onder dubbelblinde *peer review*, die versie heeft een blinde colofon.

1.2 Verloop in vogelvlucht

Uit het onderzoek is duidelijk geworden hoe de sporen ontstaan. Hieruit volgt ook een vrij duidelijk beeld van onder welke omstandigheden dit soort sporen verwacht kunnen worden in het veld, en welke maatregelen er genomen kunnen worden om ze te conserveren. Zoals u kunt lezen in het wetenschappelijk rapport komen de sporen in veel situaties voor. Ze zijn echter ook erg kwetsbaar; de sporen kunnen overschreven worden door andere signalen uit de ether. Het is juist op de meer afgelegen plekken dat het type spoor zijn nut zou kunnen bewijzen, te meer omdat het op dat soort plaatsen juist ontbreekt aan meer traditionele sporen — cameraregistraties, ooggetuigen etc.

Het onderzoek is iets breder dan in de aanvraag uitgevoerd om ook een ander frametype — beacon frames — te onderzoeken. De spoorvorming rond deze frames werkt analoog aan die rond probe request frames, maar de beacon frames kunnen andere tactisch bruikbare informatie opleveren.

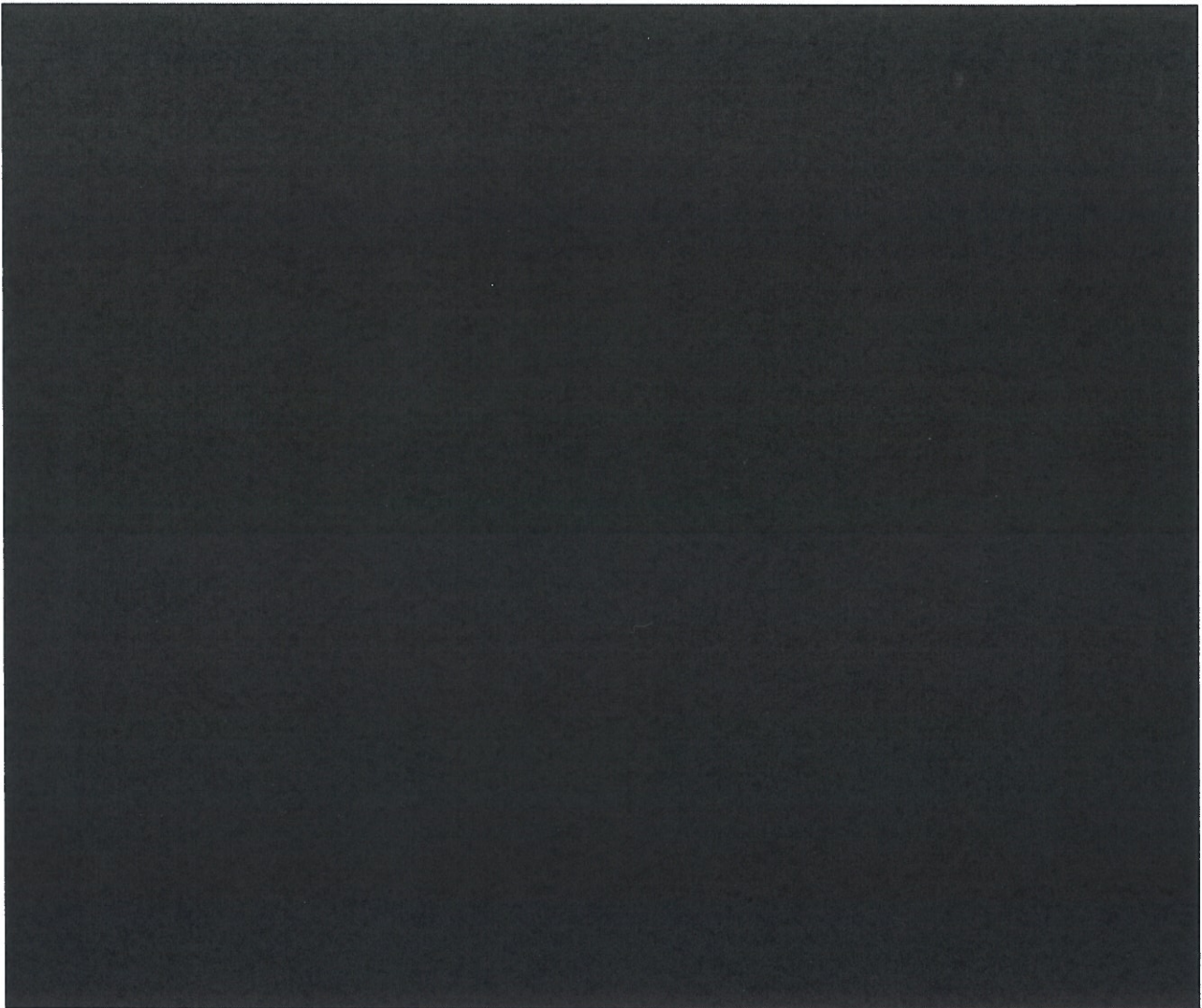
Een aantal experimenten moest worden overgedaan omdat sommige Faraday-kooien bleken te lekken in de gebruikte frequentieband. Een opvallend bijresultaat van het onderzoek is dat we een eenvoudige en kostenefficiënte kooidoormetmethode denken te kunnen ontwikkelen op basis van de in de experimenten gebruikte opstelling.

Een voor fase 2 zeer relevante bevinding is dat het vrij eenvoudig blijkt te zijn om sporen uit een geheugendump te halen - ze zijn erg goed herkenbaar. Doelstelling 2, die eigenlijk in fase 2 bereikt zou moeten worden, is daarmee nu al bereikt. Een voorgesteld produkt van fase 2 — extractiesoftware — is daarom irrelevant geworden.

De workshop over het onderzoek op de Themadagen Digitale Opsporing is erg goed bezocht, en is vanwege de grote vraag twee keer gehouden. De discussie over wat met de onderzoeksresultaten moet worden gedaan draait om de volgende twee punten:

1. Hoe kunnen de situaties herkend worden waarin relevante informatie nog bewaard zijn?
2. Hoe kan voorkomen worden dat *first responders* een plaats delict contamineren en sporen beschadigen?

2. Financiën



Buiten scope verzoek

3. Vertaling naar praktijk

In het onderzoek is duidelijk geworden dat er een kans ligt voor dit spoortype, maar dat om goed gebruik van het spoor mogelijk te maken een antwoord moet worden gevonden op de twee centrale vragen uit de discussie met de doelgroep, hier herhaald:

1. Hoe kunnen de situaties herkend worden waarin relevante informatie nog bewaard zijn?
2. Hoe kan voorkomen worden dat *first responders* een plaats delict contamineren en sporen beschadigen?

Vraag 1

Voor de beantwoording van de eerste vraag zien wij mogelijkheden voor een technische oplossing; een simpele draagbare sensor, door iedereen te gebruiken, die de signalen uit de ether analyseert en (met een lampje) een simpel "ja/nee" antwoord kan geven op de vraag: "heeft het zin om in deze omgeving rekening te houden met sporen van signalen uit de ether?". Op het moment dat dat het geval is, kan een coördinator worden ingeschakeld die de volgorde waarin sporen worden veiliggesteld bepaalt, en zorgdraagt voor het bewaken van radiostilte op een plaats delict.

Intern loopt bij het NFI een kwaliteitsverbeteringstraject dat radio-lekken en -contaminaties in onze opslagruimte voor bewijsmateriaal moet signaleren. In het kader van dat traject is een zeer kostenefficiënt apparaat (€70) ontwikkeld op basis van goed verkrijgbare massaproduceerde consumentenapparatuur. Dat platform kan eenvoudig worden aangepast voor deze nieuwe taak.

Vraag 2

Deze vraag is vele malen moeilijker te beantwoorden dan de eerste vraag. Het gaat hierbij om bewustwording, voorlichting, en het opstellen van protocollen. De afdeling Digitale Technologie heeft hiervoor partners nodig binnen de politie-organisaties, en kan daarnaast een samenwerking opzetten met het Mobiel Forensisch Team van het NFI. Op dit moment weten we nog niet of de organisaties die dichterbij het veld zitten mogelijkheden zien.

Resumerend

Fase 2 zoals aanvankelijk voorgesteld in het projectplan is, ondanks de onderzoeksresultaten die de aanwezigheid van het spoortype bevestigen, niet meer relevant. Omdat we in principe technische mogelijkheden zien om het spoortype te benutten, zouden we graag proberen om ketenpartners te vinden die aanpassingen aan de werkwijze in het veld kunnen en willen bewerkstelligen. Daar zou een nieuw projectvoorstel uit voort kunnen komen, waarbij meerdere partners zijn betrokken.