

Inhoud

1	Leeswijzer.....	5
2	Rapportage.....	6
2.1	Algemeen.....	6
2.2	Titel Rapport.....	7
2.3	Zaakgegevens.....	7
2.4	Te onderzoeken materiaal.....	8
2.5	Verkregen informatie.....	9
2.6	Vraagstelling.....	9
2.7	Onderzoek.....	9
2.8	Resultaten.....	9
2.9	Interpretatie.....	10
2.10	Conclusie.....	10
2.11	Interne rapporten.....	10
2.12	Voorlopige rapportage.....	10
2.13	Opmaak.....	10
3	Onderzoeksvoorstel.....	11
3.1	acceptatiecriteria en deskundigenbenoeming.....	11
4	Standaardformuleringen.....	12
4.1	Rapportage (algemeen).....	12
4.2	Digitale technologie (algemeen).....	13
4.3	Crypto.....	14
4.4	Hardware en firmware.....	14
4.5	Harde schijven.....	16
4.6	Minidisk.....	16
4.7	Simkaarten.....	17
4.8	Mobiele netwerken.....	17
4.9	Zakagenda's.....	18
4.10	Microsoft Windows.....	18
4.11	Onderzoeksapparatuur.....	19
4.12	Onderzoekssoftware.....	19
5	Standaard voetnoten.....	23
6	Standaard onderzoeken.....	30

1 Leeswijzer

De notatie *{vervanging}* betekent dat dit stuk vervangen dient te worden in de uiteindelijke tekst. De formattering van het te vervangen deel is al toegepast.

2 Rapportage

De volgende documenten vormen de basis voor het gebruik van de RNS rapportagetemplate:

QOL-00551 KPM Rapportagerichtlijnen (werkvoorschrift)

Dit document beschrijft hoe je de rapportage-template moet gebruiken en wat je precies moet invullen op het voorblad bij de zaakgegevens etcetera. Daarnaast beschrijft dit document hoe je moet omgaan met datums en tijden, aantallen en hoeveelheden in lopende tekst, etcetera;

QOL-00900 Stylesheet Sjabloon RNS rapport

Dit document beschrijft de formattering, regelafstanden, lettertypen etcetera die gebruikt moeten worden in de rapportage template.

2.1 Algemeen

Voor het gehele rapport geldt:

- Zet letterlijke aanhalingen cursief en tussen dubbele aanhalingstekens (onder meer in de hoofdstukken *Verkregen informatie* en *Vraagstelling*);
- Gebruik actieve zinnen, bv "het NFI heeft", "Bijlage 3 beschrijft", "Tabel 1 geeft weer";
- Gebruik geen spreektaal;
- Voorkom lastig taalgebruik, bv:
 - ook i.p.v. *eveneens*;
 - over i.p.v. *betreffende*;
 - die i.p.v. *welke*;
 - daarom i.p.v. *als gevolg hiervan*;
 - met i.p.v. *met behulp van*;
 - van i.p.v. *d.d.*;
 - etcetera;
- Begin iedere paragraaf met de essentie van die paragraaf;
- Praat over "sporen van";
- Praat over "één-op-één-kopieën van gegevensdragers in de PC" i.p.v. "de PC";
- NFI 1^e keer altijd voluit schrijven;
- Samenstellingen schrijf je aan elkaar, evt. m.b.v. een "-", bv "SMS-berichten";
- Zorg dat zinnen en met name de titel niet voor dubbele interpretatie mogelijk is. Bijv. "data-analyse naar aanleiding van ontbrekende financiële administratie bij onderzoek naar het faillissement van instelling X" kan ook opgevat worden als dat het NFI de financiële administratie deels heeft kwijt gemaakt;
- Hanteer "op" voor geheugendrager en "in" voor bestand;
- Als er verwezen wordt beeldmateriaal wordt er altijd "afbeeldingen" gebruikt, in alle andere gevallen "bestanden". Zo voorkom je dat dit niet door elkaar loopt (m.n. in KP-onderzoek);
- Bij de term "marge" moet er rekening mee worden gehouden dat dat beide kanten op kan (plus en min).

2.1.1 DT-specifieke formattering en lettertypen

Het standaard lettertype voor normale tekst is Verdana 9. Het standaard fixed-width lettertype is Consolas 9.

Omschrijving	Lettertype en schrijfwijze	Voorbeelden
SIN nummer	Verdana 9, altijd tussen	[AAAA1111NL]

	blokhaken	
Merk, Model, Type	Verdana 9, cursief	<i>HTC Desire S</i>
Achterhaalde wachtwoorden	Consolas 9, dikgedrukt	Pa\$\$w0rd
Letterlijke verwijzing SVO	Verdana 9, tussen enkele aanhalingstekens	'GSM-telefoon van de verdachte'
IMEI-nummer	Consolas 9	123456789012345
Telefoonnummer	Consolas 9	06-12345678 +31(6)12345678
Pukcode	Consolas 9	12345678
Dienstaanbieder	Verdana 9, cursief	<i>Vodafone</i>
Hashes	Consolas 9, lowercase, na iedere 4 karakters een spatie	dfd1 a341 0cd8 16a4 88d3 7345 2342 12d3
Bestandsnamen	Consolas 9	index.dat Hashes.txt
IP-adressen	Consolas 9	123.45.67.89 2001:610:b10:a:214:4ff:fe3:65
Naamgeving/verwijzing SVO	Consolas 9	KOPIE_COMPAQ KOPIE_PC_OMA
Programma's	Consolas 9	Excel
Toelichting: Indien een SIN-nummer bij een apparaat wordt genoemd, plaatst dit dan achter de omschrijving (ook hier tussen blokhaken).		

Enkele algemene tips:

- Gebruik non-breaking spaces (shift-ctrl-spatie) voor referenties naar genummerde stukken, bijvoorbeeld hoofdstuk 1, bijlage 2, paragraaf 3.
- Gebruik non-breaking spaces (shift-ctrl-spatie) voor aantallen, bv 23 harde disk, 12 simkaarten.
- Gebruik non-breaking hyphen (shift-ctrl-min) voor referenties naar genummerde stukken waarbij een min-teken in de nummering zit, bijvoorbeeld S-1, DF-1-456-T, NFI-1-2.
- Rommel niet met de pagina-indeling;
- Pas de stijlen aan, niet de stijl van losse tekstfragmenten (m.a.w. gebruik Word zoals het bedoeld is);
- Definieer een nieuwe stijl voor een nieuwe formattering;
- Kijk pas naar de pagina-einden en paragraaf en -tabelafbrekingen als het hele rapport af is.

2.2 Titel Rapport

Neem in de titel/introductie van het rapport op dat het om een "vermeend" misdrijf gaat, tenzij dit te gekunsteld/te lang wordt.

2.3 Zaakgegevens

Gebruik de volgende zaakgegevens voor DT-rapporten.

2.3.1 Afhandeling SVOs

Vul bij afhandeling SVOs in:

- separaat retour (standaard, SVOs worden los van het rapport teruggestuurd);
- ingesloten retour (als de SVOs bij het rapport retour gaan);
- reeds retour op dd-mm-jjjj;
- opgelegd (als ze niet retour worden gestuurd, bij voorbeeld in geval van een kopie van tapdata);
- vernietigd.

Als de SVOs gedemonteerd zijn, voeg dan de volgende tekst toe:

Tijdens het onderzoek zijn de stukken van overtuiging (gedeeltelijk) gedemonteerd. Het NFI beschikt niet over de middelen om deze stukken van overtuiging na het onderzoek volledig in de oorspronkelijke staat terug te brengen. Geretourneerde elektronische apparatuur kan daarom na onderzoek niet meer functioneren, sneller defect raken of niet meer voldoen aan de door de fabrikant opgegeven specificaties.

Als er bewijsbestanden zijn gemaakt van aangeleverde SVOs, voeg dan de volgende tekst toe:

In de loop van het onderzoek zijn door het Nederlands Forensisch Instituut bewijsbestanden gemaakt van de door de opdrachtgever aangeleverde digitale bewijsstukken. Deze bewijsbestanden zijn tot drie maanden na de tekendatum van het rapport op te vragen bij het Nederlands Forensisch Instituut, afdeling Digitale Technologie en Biometrie.

2.3.2 Overige informatie

Als er eerder is gerapporteerd vermeld bij overige informatie dan voor iedere eerder aanvraag:

In aanvraag {aanvraagnummer} van deze zaak is op {datum} gerapporteerd.

Als er eerder een vooronderzoek is gedaan vermeld bij overige informatie dan voor iedere eerder vooronderzoek:

In aanvraag {aanvraagnummer} van deze zaak is op {datum} een onderzoeksvoorstel gedaan waarin {aantal} onderzoeksmogelijkheden zijn besproken.

Als het rapport slecht een deel van de onderzoeksvragen behandelt:

Dit rapport behandelt de onderzoeksvragen over {het apparaat}. De overige onderzoeksvragen worden apart of zijn apart gerapporteerd.

Voorbeeld:

In aanvraag 001 van deze zaak is op 1 september 2010 gerapporteerd. In aanvraag 002 van deze zaak is op 6 april 2011 een onderzoeksvoorstel gedaan waarin vier onderzoeksmogelijkheden zijn besproken.

2.4 Te onderzoeken materiaal

Als een transportschijf is aangeleverd, neem dan op bij de toelichting in de tabel: Op de transportschijf [{SIN-nummer}] zijn de te onderzoeken gegevens bij het Nederlands Forensisch Instituut (NFI) aangeleverd. De transportschijf zelf is geen onderwerp van onderzoek.

Als er door het NFI SVOs zijn afgesplitst, zet deze dan in een aparte tabel onder een genummerde paragraaf met titel 'Afgesplitst door het NFI'.

Bij gebruikmaking van een verwijzing, bv. KOPIE_XXX naar een SVO, neem dan op bij de toelichting in de tabel:

In het vervolg van dit rapport verwijst {verwijzing} naar de één-op-één-kopie [{SIN-nummer}] van de harde schijf afkomstig uit computer {type en model}.

2.5 Verkregen informatie

Voor het hoofdstuk *Verkregen informatie* geldt:

- Informatie staat in het dossier, neem deze informatie één-op-één over, inclusief typ- en taalfouten, bij kleine relevante fouten vermelden dat "hier is aangenomen dat....bedoeld wordt";
- Verwijs niet naar notulen van een gesprek, maar naar het gesprek zelf.

- Soms maakt een kleine toelichting over de aanleiding van deze zaak of de context een verhaal al snel veel logischer.

2.6 Vraagstelling

2.6.1 *Bron van de vraagstelling*

Maak altijd duidelijk waar de vraag precies staat. Neem de vraag letterlijk over uit de bron.

Voorbeeld:

Onderstaande vraagstelling is afkomstig van het aanvraagformulier van 7 juli 2011: {vraagstelling}

2.6.2 *Aanpassen naar PDC*

Indien een vraag vaag is omschreven en er een PDC omschrijving beschikbaar is, bijvoorbeeld:

De vraag "{vage vraag}" is aangepast naar de standaard vraagstelling in de Producten en Diensten catalogus van het NFI: 'Maak een één-op-één kopie van de gegevensdrager SVO [{SIN-nummer}]'.

2.6.3 *Interpretatie van de vraagstelling*

In geval dat de vraagstelling interpretatie vereist, maak dat dan expliciet:

De vraagstelling is als volgt geïnterpreteerd:
{geïnterpreteerde vragen}

In geval er extra vragen beantwoord worden, maak dan duidelijk welke dit zijn en waarom ze zijn toegevoegd. Bijvoorbeeld:

In onderzoeken waarbij een digitale videorecorder wordt aangeleverd, noteren wij in de regel ook de *systeemtijd*. Wij hebben daarom de vraagstelling uitgebreid met de volgende vraag:

Wat zijn de systeemtijden van de videosystemen?

2.7 Onderzoek

Voor het hoofdstuk *Onderzoek* geldt:

- Houd de beschrijving van het onderzoek zo algemeen mogelijk, zonder in te gaan op de details van de zaak;
- Zeg eerst altijd waarom je een onderzoeksstap zet en leg daarna pas uit wat het onderzoek inhoudt.

2.8 Resultaten

Voor het hoofdstuk *Resultaten* geldt:

- Neem alle resultaten op, laat niets achterwege;
- Geen resultaat is ook een resultaat;
- Maak alles expliciet, onderzochte SVOs per stap, bekeken bestanden, etcetera;
- Beschrijf alles objectief;
- Alles in dit hoofdstuk moet reproduceerbaar zijn;
- Geen interpretatie!

2.9 Interpretatie

Voor het hoofdstuk *Interpretatie* geldt:

- Neem alleen de relevante sporen op;
- Sluit geen scenario's uit (bias);
- Let op de prosecutor's fallacy!

2.10 Conclusie

Voor het hoofdstuk *Conclusie* geldt:

- Herhaal de vragen en geef per vraag een antwoord;
- Geef op gesloten vragen een gesloten antwoord (Ja/Nee), gevolgd door een toelichting.
- Hou in de gaten of de vraagstelling van de aanvrager aansluit op de conclusie die je gaat geven. Tijdens het onderzoek kan blijken dat de conclusie een heel andere richting op gaat, maar als je daar pas tijdens het schrijven van het rapport aandacht aan besteed moet je op het laatste moment om een andere vraagstelling vragen.

2.11 Interne rapporten

Plaats dit op en het voorblad:

Intern Rapport

2.12 Voorlopige

rapportage

Bij het maken van een voorlopig rapport moet je altijd aan het begin én aan het eind de volgende disclaimer opnemen:

De waarneming(en), bevinding(en) en/of conclusie(s), als vermeld in dit rapport, hebben nadrukkelijk een voorlopig karakter, waaraan geen definitieve conclusies verbonden mogen worden. Aangezien op dit moment nog niet alle onderzoeksresultaten bekend zijn, volgt - na dit voorlopig rapport - een formeel NFI-rapport (met definitieve conclusies).

In verband met de kans op selectieve citering zullen de conclusies in de rapportage in overeenstemming met disclaimer ook een duidelijk voorlopig karakter moeten krijgen.

2.13 Opmaak

Moeilijke termen kunnen in een verklarende woordenlijst, of een voetnoot of in een kader. Zet een enkele term met een korte uitleg in een voetnoot. Veel termen met een korte uitleg in een verklarende woordenlijst. Een enkele of een paar termen met een lange uitleg in een kader bij het eerste gebruik van de term.

3 Onderzoeksvoorstel

3.1 acceptatiecriteria en deskundigenbenoeming

WEL NODIG?

Indien gewenst is dat één of meerdere van de hiervoor beschreven onderzoeksmogelijkheden uitgevoerd wordt, dan moet dit onderzoeksvoorstel met aankruising van de gewenste keuzes geretourneerd worden naar het NFI met een NFI-aanvraagformulier. Voor deze nieuwe aanvraag is geen deskundigenbenoeming vereist; de geschetste onderzoeksmogelijkheden behoren tot de categorie onderzoeken die behoren tot de voorfase in het opsporingsonderzoek, met in het bijzonder het ontcijferen van vertaalde gegevens. Zie voor meer informatie het ambtsbericht van 11 juli 2011, uitgegeven door het College van Procureurs-Generaal (kenmerk PaG/B&S/15798).

NIET NODIG?

Indien gewenst is dat één of meerdere van de hiervoor beschreven onderzoeksmogelijkheden uitgevoerd wordt, dan moet dit onderzoeksvoorstel met aankruising van de gewenste keuzes geretourneerd worden naar het NFI met een NFI-aanvraagformulier. Voor deze nieuwe aanvraag is een deskundigenbenoeming vereist; de geschetste onderzoeksmogelijkheden behoren tot de categorie (...), met in het bijzonder het (...). Zie voor meer informatie het ambtsbericht van 11 juli 2011, uitgegeven door het College van Procureurs-Generaal (kenmerk PaG/B&S/15798).

4 Standaardformuleringen

4.1 Rapportage (algemeen)

4.1.1 *Geaccrediteerde procedures*

Met het programma rdd is, aan de hand van geaccrediteerde NFI-procedure QOL-00008, een één-op-één-kopie gemaakt van harde schijf [{SIN-nummer}].

4.1.2 *Onderzoek demontage*

Door deze methode kan [het apparaat] defect raken. Daarom is het onderzoek met toestemming van de verbalisant uitgevoerd.

4.1.3 *Werking onveranderd*

Na het onderzoek is geconstateerd dat de werking van [het apparaat] niet is veranderd.

4.1.4 *Afhandeling defecte harde schijf*

Harde schijf [{SIN-nummer}] is defect. Het aanzetten van harde schijf [{SIN-nummer}] kan (nog meer) onherstelbare schade en/of gegevensverlies tot gevolghebben.

4.1.5 *SVO-degradatie*

Tijdens het onderzoek zijn de stukken van overtuiging (gedeeltelijk) gedemonteerd. Het NFI beschikt niet over de middelen om deze stukken van overtuiging na het onderzoek volledig in de oorspronkelijke staat terug te brengen. Geretourneerde elektronische apparatuur kan daarom na onderzoek niet meer functioneren, sneller defect raken of niet meer voldoen aan de door de fabrikant opgegeven specificaties.

4.1.6 *Verklarende woordenlijst in bijlage*

Bijlage {bijlagenummer} bevat een verklarende woordenlijst met enkele technische termen. Cursief gedrukte termen worden nader verklaard in deze woordenlijst.

4.1.7 *Resultaten in bijlage*

Alle uitgelezen gegevens zijn opgenomen in bijlage [bijlagenummer].

4.1.8 *Hashes*

Op de {cd of dvd}-recordable staat een bestand met de naam hashes.txt. Dit bestand bevat de bestandskenmerken van alle bestanden op de {cd of dvd}-recordable. Bijlage {bijlagenummer} beschrijft het forensisch gebruik van bestandskenmerken. De MD5-, SHA-1 en SHA-256-bestandskenmerken van bestand hashes.txt zijn:

```
MD5:      dfd1 a341 0cd8 16a4 88d3 7345 xxxx xxxx
SHA-1:    7085 1565 85ab 7de0 f751 c498 4986 8dfb xxxx xxxx
SHA-256:  0785 35bc 1565 85ab 7de0 bc48 a761 4976
           4986 58fe 341b 8dfb 5cba 7126 xxxx xxxx
```

4.1.9 *Entropie*

In de informatietheorie is (Shannon-)entropie een maat voor de informatiedichtheid van een bericht (of een bestand). Een bepaald soort bestand heeft een vaak typerende entropie. Bij bijvoorbeeld veel tekstdocumenten is de entropie vrij laag, terwijl de entropie van gecijferde of gecomprimeerde bestanden meestal zeer hoog is.

4.1.10 Base64

Met base64 codering kunnen binaire (8-bit) tekens omgezet worden naar een beperkte set van (7-bit) ASCII-tekens. ASCII staat voor American Standard Code for Information Interchange en is een standaard om een aantal letters, cijfers, leestekens en andere symbolen te representeren. De beperkte ASCII-set bestaat uit de volgende tekens:
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/. .

4.2 Digitale technologie (algemeen)

4.2.1 ASCII

ASCII is een veelgebruikte manier om tekst digitaal te representeren.

4.2.2 AVI

AVI staat voor Audio Video Interleave. Het is ontwikkeld door Microsoft. Het is een veelgebruikt formaat voor audio en video bestanden.

4.2.3 Cookie

Een cookie is een stukje tekst dat een webpagina aan een webbrowser kan sturen om op te slaan op de harde schijf van een gebruiker. De webbrowser stuurt de opgeslagen informatie bij een volgend bezoek weer terug. Zo wordt informatie over de internetgebruiker bijgehouden en worden de verschillende bezoeken van een gebruiker aan elkaar gekoppeld.

4.2.4 Image

Eén-op-één-kopie

4.2.5 Indexeren

Een index van een groep digitale gegevens is een lijst van woorden met de locaties waarop die woorden in de groep gegevens voorkomen. Een index van een groep gegevens is analoog aan een (trefwoorden)register van een boek, al bevat een index van een groep digitale gegevens meestal alle locaties waarop dat woord voorkomt en een (trefwoorden)register alleen de belangrijkste locaties.

Het zoeken van een woord in een index is meestal vele malen sneller dan het zoeken van dat woord in de originele groep digitale gegevens. Wanneer een grote groep digitale gegevens meerdere malen moeten worden onderzocht, kan het voordelen hebben om eerst een index te maken.

4.2.6 IP-adres

Een IP-adres (ook wel IP-nummer) is een Internet Protocol-adres dat een computer identificeert die een verbinding heeft met een computernetwerk zoals bijvoorbeeld het Internet.

4.2.6.1 Gebruik (lang)

Op dit moment komen ip-adressen in twee versies voor: versie 4 (IPv4) en versie 6 (IPv6). Een IPv4-adres wordt met 32 bits gerepresenteerd, een IPv6-adres met 128 bits. IPv4 adressen worden gerepresenteerd door vier getallen tussen 0 en 256, gescheiden door een punt (b.v. 10.0.29.1). IPv6 adressen worden gerepresenteerd door acht hexadecimale getallen, gescheiden door een dubbele punt. Eventuele 'voorloopnullen' mogen weggelaten worden (b.v. 2001:0610:0b10:000a:0214:4fff:fe23:6510 wordt 2001:610:b10:a:214:4fff:fe23:6510). Omdat IPv6-adressen momenteel zelden gebruikt worden binnen de Nederlandse ISP (Internet Service Provider) wereld, is ervoor gekozen om alleen IPv4-adressen te zoeken.

4.2.6.2 Gebruik (kort)

Op dit moment komen ip-adressen in twee versies voor: versie 4 (IPv4) en versie 6 (IPv6). Een IPv4-adres wordt met 32 bits gerepresenteerd, een IPv6-adres met 128 bits. Omdat IPv6-adressen momenteel zelden gebruikt worden binnen de Nederlandse ISP (Internet Service Provider) wereld, is ervoor gekozen om alleen IPv4-adressen te zoeken.

4.2.7 JPEG

JPEG staat voor Joint Photographic Experts Group. Het is een door het ISO gestandaardiseerde methode voor compressie van digitale plaatjes.

4.2.8 MPEG

De ISO MPEG standaarden zijn internationale standaarden die te maken hebben met compressie, decompressie, verwerken en gecodeerde representatie van (digitale) video en/of audio. Deze standaarden zijn ontwikkeld door de Moving Picture Experts Group (MPEG).

4.3 Crypto

4.3.1 Aanvullende informatie

In dit onderzoek is geprobeerd een of meerdere wachtwoorden te achterhalen om zo een of meer digitaal gecijferde gegevens te kunnen ontsleutelen. Tot op heden is dit niet gelukt. Indien gewenst kan, met een nieuwe aanvraag, op het NFI verder gezocht worden naar wachtwoorden om de gegevens alsnog te ontsleutelen.

4.3.2 Signatures

Signatures (ook wel *magics of magic numbers* genoemd) zijn vaste termen die over het algemeen op vaste locaties in een bestand staan. Signatures worden door programmatuur gebruikt om bestanden te kunnen identificeren.

4.4 Hardware en firmware

4.4.1 FTL en FAT-BS

Gegevens in het NAND-flashgeheugen zijn ingedeeld met behulp van twee opslagmechanismen. Op laag niveau verzorgt een flash translation layer (FTL) de vertaling van fysieke geheugenlocaties in het halfgeleidergeheugen naar logische datablokken. Een niveau hoger vertaalt een FAT bestandsstelsel (FAT-BS) deze logische datablokken naar bestanden en mappen.

4.4.2 BIOS (Basic Input Output System)

Het BIOS (Basic Input Output System) is de eerste software die wordt gedraaid als een PC wordt aangezet. Het BIOS bevat onder andere een functie om de systeemklok uit te lezen. Het BIOS van een PC corrigeert niet automatisch de systeemtijd bij een overgang van zomer- naar wintertijd of andersom. Daarnaast kan het BIOS onder andere het interne geheugen testen en de gebruiker laten kiezen tussen het opstarten van besturingssystemen.

4.4.3 BIOS-wachtwoord

Een BIOS-wachtwoord is een wachtwoord dat kan worden ingesteld op een computer om te voorkomen dat derden, zonder kennis van dit wachtwoord, instellingen kunnen wijzigingen in de (hardware)configuratie van de computer. Een opstartwachtwoord voorkomt dat derden zonder kennis van dit wachtwoord de computer kunnen opstarten.

4.4.4 Besturingssysteem

Het besturingssysteem maakt het de gebruiker mogelijk programma's te draaien op een computer. Het besturingssysteem verzorgt onder andere de communicatie met toetsenbord, muis, modem, webcam, netwerk, etc. Voorbeelden van besturingssystemen zijn MS-DOS, Microsoft Windows 95/98/Me/NT/2000/XP, Unix, Linux, BSD en Apple MacOS. Moderne besturingssystemen (zoals de recente Windows-besturingssystemen) corrigeren de systeemtijd automatisch bij een overgang van zomer- naar wintertijd of andersom.

4.4.5 Digitale videosystemen

De videorecorder {merk en type} is een digitale videorecorder die de opgenomen beelden opslaat op een interne harde schijf {merk en type}. Als er geen beschikbare ruimte meer op de harde schijf is, worden de oudste beelden overschreven door de nieuwe beelden.

4.4.6 Herallocatie

Wanneer een harde schijf bij het lezen van een sector een fout registreert zal de harde schijf zelfstandig een of meerdere malen de sector proberen te lezen. Wanneer de fout zich blijft herhalen en ernstig genoeg is, kan de schijf besluiten om de gelezen sector te heralloceren. Heralloceren van een sector houdt in dat de fysieke locatie die hoort bij het adres (sector nummer) waar de fout is opgetreden te verwisselen met een andere fysieke locatie in een speciaal voor dit doel gereserveerd gedeelte van de harde schijf. Dit heeft tot gevolg dat de sector weer bruikbaar wordt voor gegevensopslag. Als de harde schijf de inhoud van de sector die de fout bevatte nog kan reconstrueren kan de nieuwe fysieke locatie de gereconstrueerde inhoud krijgen van de defecte sector. Deze reconstructie vindt plaats met de beschikbare foutcorrectie informatie. Wanneer de schijf de inhoud niet meer kan reconstrueren krijgt de sector de inhoud van de nieuwe fysieke locatie (meestal volledig gevuld met de bytewaarde 0).

4.4.7 Sectoren

Een sector is de kleinste adresseerbare eenheid gegevens op een harde schijf, meestal 512 bytes groot.

In bijlage {bijlagenummer} zijn de posities van deze sectoren opgenomen.

4.4.8 Systeemtijd

Een PC bevat een interne klok, de systeemklok. Deze klok is aangesloten op een batterij en loopt door als de PC uitstaat. De systeemklok van een PC corrigeert de systeemtijd niet automatisch bij een overgang van zomer- naar wintertijd of andersom. De tijd die de systeemklok aangeeft heet de systeemtijd.

4.4.9 Timeserver

Een timeserver is een computer die is ingericht om de juiste tijd bij te houden. Een timeserver stelt deze tijd via een netwerk beschikbaar aan andere computers. Er zijn meerdere timeservers beschikbaar op het Internet.

4.5 Harde schijven

4.5.1 Controller

Een controller is elektronica die deel uitmaakt van een harde schijf. De controller van een harde schijf zorgt voor de juiste besturing van de mechanische delen van de harde schijf. De gegevens die door een harde schijf worden opgeslagen bevinden zich niet in de controller. Als een controller niet of niet goed werkt, dan zijn de gegevens op de harde schijf niet of niet goed te benaderen.

4.5.2 *Controller, vervanging*

Om de gegevens op de harde schijf [{SIN-nummer}] weer te kunnen benaderen is de defecte controller vervangen. De vervangende controller is afkomstig van een harde schijf die hetzelfde merk en modelnummer heeft als [{SIN-nummer}].

Om [{SIN-nummer}] weer in oorspronkelijke staat te herstellen is de originele, defecte controller na het kopiëren van de data teruggeplaatst op het SVO.

4.5.3 *Flash-disk*

Een flash-disk is een harde schijf in de vorm van een chip.

4.5.4 *Ramp*

parkeerstandaard

4.5.5 *Unallocated clusters / niet-toegewezen bestandsruimte*

Unallocated clusters zijn die gebieden van een harde schijf die op het moment van veiligstellen niet gebruikt worden voor de opslag van bestanden. Deze unallocated clusters kunnen data bevatten van bestanden die voor de veiligstelling gewist zijn.

Bij het verwijderen van bestanden blijft de bestandsinhoud in eerste instantie op de harde schijf aanwezig. De ruimte die deze data inneemt wordt echter beschikbaar gesteld voor opslag van nieuwe bestanden. Wanneer na het verwijderen van bestanden nieuwe bestanden op de harde schijf worden gezet, kan de data van de verwijderde bestanden geheel of gedeeltelijk worden overschreven. De verwijderde bestanden die na het overschrijven in de unallocated clusters zijn gevonden zijn dan niet meer compleet.

4.6 **Minidisk**

4.6.1 *Lege table of contents (TOC)*

Een audio-opname wordt bij opslag op een minidisc eerst gecomprimeerd. Hierna wordt de opname verdeeld in blokken op de minidisc geplaatst. Het is mogelijk dat blokken niet opeenvolgend op een minidisc worden opgeslagen maar gefragmenteerd over de disc verdeeld worden. De plaats van deze blokken en tot welke opname ze behoren, wordt bijgehouden in een table of contents (TOC), die ook op de minidisc staat. In deze TOC worden ook andere parameters van een opname bijgehouden, zoals de titel of de lengte van de opname. Als opnames worden verwijderd, wordt in feite alleen de TOC gewijzigd. Het is met de door het NFI gehanteerde methode niet mogelijk om de TOC te herstellen, maar in de meeste gevallen is het wel mogelijk om de audio data blokken één voor één terug te halen. Daarbij worden alle teruggehaalde data blokken toegewezen aan één enkele opname ook als die afkomstig zijn van meer dan één originele opname. Indien op deze manier gefragmenteerde blokken worden teruggehaald is het mogelijk dat delen van opnamen door elkaar staan. Dit is ook een van de beperkingen van deze methode. Hierop dient de resulterende opname gecontroleerd te worden.

Uit onderzoek bleek dat de table of contents (TOC) van de MiniDisk [{SIN-nummer}] leeg was. Met een door het NFI ontwikkelde methode is het mogelijk om alle data die op een MiniDisk staat terug te halen. Deze methode is toegepast op MiniDisk [{SIN-nummer}], en alle data aanwezig op de MiniDisk is terug gezet op een andere MiniDisk.

4.7 Simkaarten

4.7.1 *Mobiele telefoon met simkaart*

De mobiele telefoon van het merk *{merk}*, model *{model}* [*{SIN-nummer}*] heeft het IMEI-nummer (International Mobile Equipment Identity) *{IMEI-nummer}*. In de mobiele telefoon is een *{landaanduiding}* simkaart aanwezig met het nummer *{telefoonnummer}*, uitgegeven door dienstaanbieder *{dientaanbieder}*.

4.7.2 *Simkaart uitlezen*

De simkaart is uitgelezen met behulp van een chipkaartlezer en door het Nederlands Forensisch Instituut ontwikkelde programmatuur.

4.7.3 *Niet-beveiligde simkaart*

Deze simkaart is niet beveiligd met een pincode.

4.7.4 *Door verbalisant verstrekte pukcode*

Deze simkaart is beveiligd met een onbekende pincode. Met behulp van de pukcode *{pukcode}* is de pincode gewijzigd in 0000. Deze pukcode is door de verbalisant verstrekt.

4.7.5 *Sim zonder pukcode*

De opdrachtgever heeft afgezien van het verkrijgen van een pukcode.

4.7.6 *Sim-kloon*

Met het ICCID-nummer en het IMSI-nummer is een simkaart geconfigureerd voor onderzoek aan de mobiele telefoon [*{SIN-nummer}*]. Deze simkaart is zodanig geconfigureerd dat de kans op het overschrijven van mogelijk in de mobiele telefoon aanwezige gegevens wordt geminimaliseerd.

4.8 Mobiele netwerken

4.8.1 *Afzien van toestemming voor het uitlezen van netwerkgegevens*

De opdrachtgever heeft afgezien van het verkrijgen van toestemming van de dienstaanbieder voor het uitlezen van in het netwerk opgeslagen aan de mobiele telefoon gerelateerde gegevens.

4.8.2 *Opvragen netwerkgegevens bij dienstaanbieder*

Gegevens behorend bij het abonnement zijn bij de dienstaanbieder opgevraagd met een mobiele telefoon van het Nederlands Forensisch Instituut met daarin simkaart [*{SIN-nummer}*].

4.8.3 *Machtiging uitlezen gegevens uit netwerk*

Het Nederlands Forensisch Instituut beschikt over een machtiging artikel 126ng/ug lid 1 jo 126nd/ud Sv voor het uitlezen van in het netwerk opgeslagen aan de mobiele telefoon gerelateerde gegevens.

4.8.4 *Uitlezen voicemail*

Er zijn voicemailberichten opgenomen, behorend bij het telefoonabonnement. Deze voicemailberichten zijn opgenomen met behulp van simkaart [*{SIN-nummer}*] en een mobiele telefoon van het Nederlands Forensisch Instituut. De opgenomen gegevens zijn als geluidsbestand opgenomen in bijlage *{bijlagenummer}*.

4.8.5 *Uitlezen telefoongeheugen*

In het telefoongeheugen opgeslagen (gewiste) gegevens zijn vervolgens uitgelezen met behulp van een door het Nederlands Forensisch Instituut ontwikkelde methode.

4.8.6 *Handmatig uitlezen van telefoongegevens*

Via het gebruikersmenu toegankelijke gegevens zijn handmatig uitgelezen.

4.8.7 *Met programmatuur uitlezen van telefoongegevens*

In de telefoon opgeslagen gegevens zijn uitgelezen met door het Nederlands Forensisch Instituut ontwikkelde programmatuur.

4.8.8 *Maken geheugenkopie uit telefoon*

Er is een methode ontwikkeld voor het maken van een geheugenkopie van het niet vluchtige geheugen uit een mobiele telefoon van het merk *{merk}*, model *{model}*. Deze methode is, na validatie op een zelfde model uit de referentieverzameling van het Nederlands Forensisch Instituut (NFI), toegepast op de mobiele telefoon [*{SIN-nummer}*].

4.9 **Zakagenda's**

De elektronische zakagenda van het merk *{merk}*, model *{model}* [*{SIN-nummer}*] is beveiligd met een wachtwoord. Met een door het Nederlands Forensisch Instituut ontwikkelde methode is het wachtwoord achterhaald. Het wachtwoord blijkt te bestaan uit *{aantal}* tekens, te weten *{wachtwoord}*.

In de elektronische zakagenda aanwezige gegevens zijn vervolgens uitgelezen en omgezet naar een op een PC leesbaar formaat. Dit is gebeurd met voor dit type elektronische zakagenda's commercieel verkrijgbare software. De gegevens zijn opgenomen in bijlage *{bijlagenummer}*.

4.10 **Microsoft Windows**

4.10.1 *Registry*

Windows-besturingssystemen houden gebruikers- en configuratie-informatie bij in een configuratiedatabase. Deze database wordt meestal registry (register) genoemd. De inhoud van de registry wordt, verspreid over meerdere bestanden, op de harde schijf opgeslagen.

4.10.2 *Restore point / herstelpunt*

Een herstelpunt is een mechanisme van het besturingssysteem Windows XP en opvolgende versies dat voorkomt dat belangrijke bestanden bij calamiteiten verloren gaan. Bepaalde soorten bestanden worden, bijvoorbeeld als ze verwijderd worden, naar een herstelpunt gekopieerd zodat ze in geval van nood nog teruggehaald kunnen worden. Bij het maken van een dergelijk herstelpunt krijgt het bestand een andere naam. De oorspronkelijke naam wordt bewaard in het logboek van het herstelpunt.

4.11 **Onderzoeksapparatuur**

4.11.1 *Cleandesk*

Een cleandesk is een stofarme werkplek. Het mechanische binnenwerk van harde schijven is zeer gevoelig voor stofdeeltjes. Stofdeeltjes kunnen zorgen voor schade aan het binnenwerk en hiermee gepaard gaand gegevensverlies. Harde schijven worden geproduceerd in dergelijke stofarme ruimtes. Onderzoek aan het binnenwerk van harde schijven wordt bij het NFI in een cleandesk gedaan.

4.11.2 *DCF77-klok*

Een DCF77-klok is een klok die zich synchroniseert met het tijdsignaal van een radiozender in Mainflingen, nabij Frankfurt in Duitsland. Het tijdsignaal uit

Mainflingen is gerelateerd aan een atoomklok. Het DCF77-tijdssignaal wordt in West-Europa gebruikt om klokken en horloges automatisch op tijd te laten lopen.

4.11.3 *PC3000*

PC3000 bestaat uit apparatuur en programmatuur bestemd voor de analyse en reparatie van harde schijven.

PC3000 is gebruikt om het defect van harde schijf [{SIN-nummer}] te lokaliseren.

4.11.4 *Memory Toolkit*

Als de MTK gebruikt wordt dan kan er het beste een korte samenvatting van die techniek in het rapport komen om de boel te verduidelijken: "Met een door het NFI ontwikkelde methode wordt een exacte kopie van alle data op de geheugenchip gemaakt, zonder dat deze data wordt veranderd. Ook gewiste data die nog niet overschreven is, wordt gekopieerd."

4.12 **Onderzoekssoftware**

In het onderzoek is gebruik gemaakt van de volgende apparatuur en programmatuur:

- EnCase, versie {versie}, ontwikkeld door het Amerikaanse bedrijf Guidance Software;
- Rdd, versie {versie}, ontwikkeld door het Nederlands Forensisch Instituut;
- DeepSpar Disk Imager (DDI), versie {versie}, ontwikkeld door het Canadese bedrijf DeepSpar Data Recovery Systems;
- Ilook, versie {versie}, ontwikkeld door Elliot Spencer en de Fiscale Opsporingsdienst van de Amerikaanse belastingdienst;
- MMPC (Media Merge Personal Computer), versie {versie}, ontwikkeld door Emag Solutions;
- PC3000 ISA, IBM DTLA-utility versie {versie}, ontwikkeld door het Russische bedrijf ACE Laboratory;
- PC3000 PCI, versie {versie}, ontwikkeld door het Russische bedrijf ACE Laboratory;
- een cleandesk, merk Brecon model 9 CL 9 AL type crossflow, voldoet aan klasse 5 van iso-norm 14644-1;
- als-niet-laatste-item-dan-een-punt-komma;
- laatste regel eindigt met een punt.

4.12.1 *BestCrypt*

BestCrypt, versie {versie}, ontwikkeld door {versie}. BestCrypt wordt gebruikt om digitale gegevens te versleutelen. Met BestCrypt kunnen de gegevens ook weer ontsleuteld worden, mits men het juiste wachtwoord weet. Het bestand waar BestCrypt de gecijferde gegevens in opslaat wordt een container genoemd.

4.12.2 *DeepSpar Disk Imager*

DeepSpar Disk Imager (DDI) bestaat uit apparatuur en programmatuur bestemd voor het op een efficiënte manier lezen van gegevens van harde schijven die (deels) defect zijn. DDI maakt voor de opslag van de gelezen gegevens gebruik van een tweede harde schijf; deze harde schijf noemen we in dit rapport DOELSCHIJF Deze DOELSCHIJF is voorafgaand aan het onderzoek leeggemaakt, dat wil zeggen volledig beschreven met bytes met de waarde nul.

Bij het kopiëren van een harde schijf met DDI kunnen leesfouten optreden. Sectoren die niet kunnen worden gelezen, worden door het programma DDI in de gemaakte

kopie vervangen door bekende gegevens. Dit noemen we een 'vervangende sector'. Een vervangende sector bevat 32 maal de volgende tekst: " <unreadable> ".

4.12.3 *EnCase*

EnCase, versie {versie}, ontwikkeld door het Amerikaanse bedrijf Guidance Software. EnCase is een veelgebruikt forensisch onderzoeksprogramma. Met EnCase kunnen gegevens van diverse digitale gegevensdragers zoals harde schijven en cd-recordables onderzocht worden. EnCase gebruikt zogeheten bewijsbestanden (Eng: *Evidence Files*) om de te onderzoeken gegevens in op te slaan.

4.12.4 *File Monitor*

File Monitor, versie {versie}, ontwikkeld door het Amerikaanse bedrijf Sysinternals. File Monitor is een programma dat systeemactiviteit bijhoudt en afbeeldt. Het is hier gebruikt voor het monitoren van diverse acties op bestanden, zoals openen, lezen en schrijven.

4.12.5 *IDA Pro*

IDA Pro (Interactive DisAssembler PROfessional) is een multi-processor dis-assembleer programma en wordt gebruikt om de werking van programmatuur te analyseren. Meer informatie over IDA Pro is te vinden op www.hex-rays.com.

4.12.6 *JAD*

Jad, Java Decompiler, versie {versie}, ontwikkeld door Pavel Kouznetsov. Met Jad is het mogelijk om de originele Java broncode die gebruikt is om een programma te maken (compileren) terug te krijgen (te decompileren).

4.12.7 *MMPC*

MMPC is een forensisch programma dat tapes kan lezen. Het herkent standaard de opslagmethode van veel verschillende merken backup-software.

4.12.8 *Paint Shop Pro*

Paint Shop Pro, versie {versie}, ontwikkeld door Jasc Software. Paint Shop Pro wordt gebruikt om digitale plaatjes te manipuleren. Deze versie van Paint Shop Pro ondersteunt 32 verschillende soorten formaten.

4.12.9 *PGP*

PGP (Pretty Good Privacy), versie {versie}, ontwikkeld door Network Associates. PGP wordt onder andere gebruikt om digitale gegevens zoals bestanden en e-mails te versleutelen. Om de bestanden te ontsleutelen moet men vaak de beschikking hebben over de juiste geheime sleutel (secret key). Zo'n geheime sleutel is beveiligd met een wachtwoord (passphrase).

4.12.10 *PhotoRescue*

PhotoRescue, versie {versie}, is een commercieel programma om gewiste foto's terug te halen.

4.12.11 *Rdd*

Rdd, versie {versie}, is een forensisch kopieerprogramma. Het is gebruikt om een één-op-één-kopie van [{SIN-nummer}] te maken.

4.12.12 *Skyhook*

Het bedrijf 'skyhook wireless' heeft, veelal in opdracht van bedrijven als Apple en Google, met auto's door Nederland gereden en geadministreerd op welke locaties welke draadloze toegangspunten zichtbaar zijn. Bij de publieke online-dienst van

'skyhook wireless' is via de openbaar gemaakte API opgevraagd of elk gevonden MAC-adres een bekende locatie heeft.

4.1.13 *TrueCrypt*

Met TrueCrypt, versie {versie}, kunnen digitale gegevens op verschillende manieren versleuteld worden onder bescherming van een wachtwoord. TrueCrypt is gratis te verkrijgen. Zie voor meer informatie www.truecrypt.org.

4.1.14 *UltraEdit-32*

UltraEdit-32, versie {versie}, ontwikkeld door het Amerikaanse bedrijf IDM Computer Solutions. UltraEdit-32 is een programma dat bestanden in zowel tekstvorm als hexadecimale vorm kan laten zien en eventueel kan laten aanpassen. Het is hier gebruikt om machinecode te bekijken en aan te passen.

4.1.15 *VideoMach*

VideoMach, versie {versie}, ontwikkeld door Gromada.com. VideoMach is geschikt voor het maken en converteren van audio en/of video. Het is hier gebruikt om van stilstaande plaatjes videofilms te maken.

4.1.16 *VMWare*

VMWare is een Amerikaans bedrijf dat zich gespecialiseerd heeft in ontwikkeling op het gebied van virtualisatie en cloud infrastructure. VMWare ontwikkelt onder meer de programmatuur VMWare Workstation. Met VMWare Workstation is het mogelijk om op één computer (Eng: *host computer*) meerdere besturingssystemen (Eng: *guest operating systems*) gelijktijdig te kunnen laten draaien; alle in een eigen (eventueel afgeschermd) omgeving. Een dergelijk besturingssysteem wordt door VMWare Workstation opgeslagen in een bestand dat virtuele machine (Eng: *virtual machine*) wordt genoemd. Meer informatie over VMWare is te vinden op www.vmware.com/nl.

4.1.17 *Windows Media Player*

Windows Media Player, versie {versie}, ontwikkeld door Microsoft. Windows Media Player is een universele media speeler voor het afspelen van diverse formaten audio en video.

4.1.18 *WinZip*

WinZip, versie {versie}, wordt gebruikt voor het archiveren en/of comprimeren van één of meerdere bestanden. Het resultaat hiervan is een nieuw bestand, het archiefbestand, waar de bestanden in opgeslagen zijn. Een optie tijdens het archiveren en/of comprimeren is het toekennen van een wachtwoord aan het archiefbestand. Zonder invoering van een correct wachtwoord kunnen de opgeslagen bestanden in het archiefbestand niet worden ingezien.

4.1.19 *Hex Workshop*

Hex Workshop, versie {versie}, is een programma dat bestanden in hexadecimale vorm kan tonen en eventueel kan aanpassen. Het is in dit onderzoek gebruikt om de inhoud van onbekende gegevens te onderzoeken.

4.1.20 *XIRAF*

XIRAF, versie {versie}, is een forensisch onderzoeksprogramma ontwikkeld door het NFI. Met XIRAF kunnen gegevens van diverse digitale gegevensdragers zoals harde schijven en cd-recordables onderzocht worden. XIRAF is gebruikt om de bewijsbestanden te analyseren.

5 Standaard voetnoten

Onderstaande tabel bevat standaard voetnootteksten.

Steekwoord	Omschrijving
7 bits codering	7 bits codering wordt toegepast om een sms-bericht kleiner te maken. I.p.v. dat een karakter, zoals een a, 8 bits inneemt, neemt deze nu maar 7 bits in.
ASCII / Unicode	ASCII en Unicode zijn twee veel gebruikte standaarden voor het opslaan van (letter)tekens in een computer. Zie o.a. http://www.unicode.org/standard/ (bezocht op {datum})
AT-commando's	AT-commando's zijn ontwikkeld voor communicatie tussen een computer en een modem. Deze commandoset is later uitgebreid met commando's om bijvoorbeeld sms-berichten te versturen en telefoonlijsten uit te lezen, zodat ze ook geïmplementeerd kunnen worden op mobiele telefoons.
Basisstation	Deze beschrijving is een vereenvoudiging van de werkelijkheid. Een zendmast is onderdeel van een basisstation. Een basisstation is gedefinieerd als het geheel van antennes, kabels en elektronische zend- en ontvangapparatuur bestemd voor de radio-elektrische dekking van een gegeven geografische zone. Een basisstation bevat in het algemeen meerdere antennes in verschillende richtingen. Elke antenne verzorgt de dekking van een specifieke geografische zone, ook wel cel genoemd.
Batterij clip	Een hulpmiddel om elektrisch verbinding te maken met een 9 Volt blokbatterij.
Bestandskenmerken	De vakbijlage Forensisch gebruik van bestandskenmerken beschrijft het forensisch gebruik van bestandskenmerken.
Bluetooth MAC adres	Het adres van de bluetooth interface
Bluetooth zichtbaar	In de bedieningssoftware van een apparaat met een bluetooth communicatie mogelijkheid kan men veelal kiezen uit de modus zichtbaar of niet zichtbaar. Als een apparaat in de modus niet zichtbaar staat wordt hij niet gevonden als er naar bluetooth apparaten gezocht wordt, bij zichtbaar wel.
CDR	Een CDR (van het Engels: Call Detail Record) bevat gegevens zoals het afzendertelefoonnummer, het bestemmingstelefoonnummer, aanvangsdatum, tijdstip en tijdsduur van een gesprek en de identificatienummers van de cellen waar de verbinding begon en eindigde. Een printlijst is een selectie uit alle bij een telecommunicatiedienstaanbieder aanwezige CDRs. Bijvoorbeeld alle verbindingen van of naar een bepaald telefoonnummer in een bepaalde periode.
cemail.vol	In het bestand cemail.vol worden e-mail-, MMS- en SMS-berichten opgeslagen.
Condensator	Een condensator is een elektronisch component voor opslag van elektrische energie.
CRC	Een CRC (van het Engelse Cyclic Redundancy Check) code is een code waarmee fouten in data overdracht gedetecteerd kunnen worden. Bij het zenden van data wordt een CRC code mee gezonden. Bij ontvangst van de data wordt de CRC code opnieuw berekend over de ontvangen data en vergeleken met de ontvangen code. Als de ontvangen en berekende codes van elkaar verschillen is er een overdrachtfout geconstateerd.
Datasheet	Datasheet: Gegevensblad behorende bij een technische component. In een datasheet wordt aan de hand van het typenummer van de component de functionaliteit en de aansluiting van de component met de buitenwereld in detail beschreven.
Die	Een die is een rechthoekig stukje halfgeleidermateriaal met een specifieke elektrische schakeling, dat tijdens productie wordt gezaagd uit een grotere plak halfgeleidermateriaal. Een chip kan meerder dies met schakelingen bevatten.

FDT - Leidraad rapporteren

DIL	DIL (Dual In Line) is a type of housing of an integrated circuit (IC). In a DIL IC, two rows of connection pins stick out on either side of the housing.
DIL	DIL (van het Engels: Dual In Line), is een type behuizing van een geïntegreerde schakeling (zie IC) waarbij de aansluitpennen in twee rijen tegenover elkaar uit de zijkant van de behuizing steken.
Duo SIM adapter	Dit is een speciale adapter waarin twee simkaarten kunnen worden geplaatst die afzonderlijk van elkaar kunnen worden gebruikt, zonder dat de telefoon hoeft te worden geopend.
EEPROM	EEPROM (van het Engels: Electrically Erasable Programmable Read Only Memory), een elektrisch wisbaar en -programmeerbaar halfgeleidergeheugen dat gegevens vasthoudt zonder dat daarvoor energievoorziening nodig is.
EEPROM	EEPROM (Electrically Erasable Programmable Read Only Memory), a nonvolatile memory. Nonvolatile memory retains its data contents, even without power-supply.
EWf-formaat	Het EWf-formaat (Eng: <i>Expert Witness Format</i>) is een bestandsformaat voor het opslaan van één-op-één-kopieën. Dit formaat wordt onder andere gebruikt door het forensisch onderzoeksprogramma EnCase. Het NFI gebruikt voor dit bestand ook wel de term EnCase-bewijsbestand.
Experimenteerprint	Een experimenteerprint is een printplaat(je) met een raster van contactgaten die in een regelmatig patroon door middel van koperbanen zijn verbonden. Hierop kunnen door middel van ingestoken componenten en soldeerverbindingen in korte tijd semi-permanente (experimentele) schakelingen worden gerealiseerd.
FIF 3GP	FIF en 3GP headers zijn bij een Nokia 6230 aanwezig in bestanden van met de telefoon gemaakte beeld en video opnamen.
Firmware	Firmware is de programmatuur voor de besturing van een mobiele telefoon.
Flash wear	Flash geheugen heeft de eigenschap dat afzonderlijke geheugenblokken een beperkt aantal keren (10.000 tot 100.000 maal) gewist kunnen worden. Dit wordt veroorzaakt door slijtage (Eng: <i>wear</i>) die optreedt tijdens het wissen. Versleten blokken kunnen nog wel gegevens bevatten en worden uitgelezen, maar niet meer opnieuw foutloos worden beschreven.
Flash bestandsysteem	Een flash bestandsysteem is een bestandsysteem dat is opgeslagen in zogenaamd Flash geheugen. Dit bestandsysteem heeft veel overeenkomsten met bestandssystemen zoals die gebruikt worden op harde schijven en kan vaak ook op vergelijkbare wijze onderzocht worden.
Flashgeheugen	Flashgeheugens zijn niet-vluchtige halfgeleidergeheugens. Een niet-vluchtig halfgeleidergeheugen houdt gegevens vast, ook zonder energievoorziening. Twee veelgebruikte benamingen voor flashgeheugen zijn NOR-flash en NAND-flash, vernoemd naar de technologie die wordt gebruikt om een data eenheid op te slaan.
	Met een door het Nederlands Forensisch Instituut (NFI) ontwikkelde methode is een gegevenskopie gemaakt van het in de mobiele telefoon aanwezige NOR flashgeheugen. Voetnoot: Voor meer informatie over deze methode, zie het hoofdstuk "Physical Extraction" in het artikel "Forensic Data Recovery from Flash Memory" http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf (bezocht op DD-MM-YYYY).
Gps	Gps is de afkorting van 'global positioning system', een wereldomvattend systeem voor locatiebepaling via zogenaamde gps-ontvangers.
Header	Een header staat aan het begin van een computerbestand en beschrijft de eigenschappen van dat bestand.
Hexadecimale notatie	De notatie 0x voor een getal geeft aan dat dit een hexadecimale weergave van een getal is.

FDT - Leidraad rapporteren

History	Via het menu-onderdeel history kan een lijst van eerder gebruikte posities geraadpleegd worden. De posities in deze lijst hoeven niet per se als bestemming gekozen te zijn. Als een positie als bestemming gekozen is hoeft deze bestemming niet per se ook bereikt te zijn.
I2C	I2C is een communicatie protocol dat veel gebruikt wordt in elektronischakelingen voor communicatie tussen IC's, bijvoorbeeld tussen microcontroller en geheugen
IC	Een IC (van het Engels: Integrated Circuit, ook wel chip genoemd) is een in halfgeleider materiaal geïntegreerde elektronische schakeling. Voor een uitgebreide populaire beschrijving, zie bijvoorbeeld nl.wikipedia.org/wiki/Integrated_circuit (bezocht op [DATUM])
IC	IC = Integrated Circuit, an electronic component containing a small semiconductor wafer on which thousands or millions of very tiny electronic components are fabricated.
IC voet	Een IC-voet wordt gebruikt om elektronische componenten (met name IC's) makkelijk te kunnen vervangen zonder dat hiervoor gesoldeerd hoeft te worden.
ICCID	ICCID is het identificatienummer van de simkaart.
Image	De term image verwijst naar een bestand dat minimaal alle beschikbare digitale (gebruikers-)gegevens bevat van een gegevensdrager. Het NFI gebruikt de term één-op-één-kopie voor een dergelijk bestand.
IMEI	IMEI (van het Engels: International Mobile Station Equipment Identity) staat voor het unieke identificatienummer dat iedere GSM-telefoon (of ander mobiel apparaat binnen GSM) verplicht is te bevatten.
IMSI	IMSI (van het Engels: International Mobile Subscriber Identity) is het nummer waarmee iedere abonnee uniek is te identificeren binnen het complete internationale GSM netwerk.
JPG	De extensie jpg (van het Engels: Joint Photographic Experts Group) wordt gebruikt voor bestanden met afbeeldingen opgeslagen volgens de zogenaamde JPEG-standaard. Zie http://www.jpeg.org/jpeg/
Kabelschoen	Een kabelschoen is een platte, klemmende stekerverbinding die zeer trillingsbestendig is en daarom veel wordt gebruikt voor het maken van elektrische verbindingen in auto's en machines. De stekerpool wordt om de aan te sluiten draad geklemd met een speciale tang.
Keyframe	Keyframes zijn beelden uit een video-opname die volledig zichtbaar zijn te maken zonder dat er andere frames uit dezelfde opname voor nodig zijn.
Keyframe	Keyframes zijn frames in een .3gp bestand, met een zogenaamde mp4v container, die geen referentie hebben naar een ander frame, deze frames bevatten het hele beeld zoals het door dat frame wordt weergegeven.
Klemconnector	Klemconnectoren worden vaak gebruikt als luidsprekeraansluiting. Door op een hendel te duwen opent een klemcontact, waarin een (ongec/soleerd) draad(eind) kan worden gestoken. Bij het loslaten van de hendel sluit het klemcontact zich weer, waarbij de ingestoken draad zowel elektrisch wordt aangesloten als ook mechanisch wordt vastgezet.
Knoopcel	Een knoopcel is een schijfvormige batterij
LED	Een LED (van het Engels: Light Emitting Diode) is een energie zuinig halfgeleiderlampje, vaak gebruikt als controlelampje.
Magneetstrip spoor	De magneetstrip op een bankpas bevat drie magneetsporen, ook wel tracks genoemd tracks. Spoor 1 bevat informatie voor het gebruik als credit card. Spoor 2 bevat de informatie die nodig is voor buitenlands gebruik van een bankpas. Als de informatie van spoor 2 van een bankpas gekopieerd wordt naar een andere magneetstrippas, dan kan met deze kopie in het buitenland worden betaald of geld opgenomen. Spoor 3 bevat informatie voor binnenlands betalingsverkeer.

FDT - Leidraad rapporteren

Metadata	Metadata zijn gegevens (data) die karakteristieken van andere gegevens bevatten. De hier bedoelde metadata in het telefoongeheugen bevat geen gebruikersgegevens maar kan wel worden gebruikt om gebruikersgegevens te achterhalen.
microcontroller	Een microcontroller (μ -Controller, μ C) is een computer waarbij alle benodigde componenten, zoals de centrale rekeneenheid, geheugen en randapparatuur, in één IC geïntegreerd zijn. Zie voor verdere uitleg bijvoorbeeld http://nl.wikipedia.org/wiki/Microcontroller (bezocht op {datum})
mp3 speler	Elektronisch apparaat waarmee audiobestanden (vaak muziek) afgespeeld kunnen worden, genoemd naar een veel gebruikt opslagformaat voor audio
Multimedia gegevens	Voorbeelden van multimedia gegevens zijn foto's, video's en muziek
Multimeter	Een multimeter of universeelmeter is de benaming van een elektrisch meetinstrument waarmee grootheden als spanning, stroom, weerstand mee gemeten kunnen worden.
NAND-flashgeheugen	NAND-flash is een type flash geheugen: een niet-vluchtig halfgeleidergeheugen vaak toegepast voor de opslag van multi-media data.
NOR-flashgeheugen	NOR-flash is een type flash geheugen: een niet-vluchtig halfgeleidergeheugen vaak toegepast voor de opslag van firmware of losse gegevens zoals telefoonnummers of sms berichten .
Neon signaal lamp	Een neon(signaal)lamp is een lagedruk gasontladingslamp
NVM	Niet-vluchtig geheugen (van het Engels: Non Volatile Memory, NVM), geheugen dat zijn informatie behoudt zonder dat het geheugen van energie wordt voorzien.
Oscilloscoop	Een oscilloscoop (kortweg scoop) is een meetinstrument waarmee elektrisch signaalvormen bekeken en gemeten kunnen worden
OneNAND	OneNAND flashgeheugen is een merknaam voor flashgeheugen dat gebruikmaakt van NAND-flash opslagtechnologie maar waarvan de lees- en schrijfkarakteristieken vergelijkbaar zijn met NOR-flash.
OTP EPROM	OTP EPROM (van het Engels: One-Time Programmable Erasable Programmable Read-Only Memory), een niet vluchtig halfgeleidergeheugen dat eenmalig kan worden geprogrammeerd en daarna niet meer kan worden gewijzigd.
PAL	PAL (van het Engels: Phase Alternating Line) is een standaard voor analoge video overdracht
Parkeerstandaard (Ramp)	De parkeerstandaard (Eng: <i>ramp</i>) is een onderdeel van een harde schijf dat zorgt voor het ophangen van de lees-/schrijfkoppen wanneer de harde schijf niet in gebruik is.
PCB	Een printplaat is een drager voor elektronische componenten, waarbij de koperen bedrading op de drager is aangebracht, .
PCB, printplaat	Een PCB (van het Engels: Printed Circuit Board), ook wel printplaat genoemd, is een kunststof plaatje waarop een patroon van koper is aangebracht, veelal met fotochemische etstechnieken. Op dit koperpatroon kunnen de elektronische componenten gesoldeerd worden zodat het koper patroon de elektrische verbindingen legt tussen de componenten.
PDU	PDU-formaat is een formaat waarin sms-berichten worden verstuurd. De sms-berichten die zijn verstuurd en ontvangen worden in deze mobiele telefoon ook opgeslagen in het PDU-formaat.
Protocol analyser	Een protocol analyser is een apparaat en/of programmatuur waarmee communicatie protocollen inzichtelijk kunnen worden gemaakt. Bijvoorbeeld het protocol waarmee wordt gecommuniceerd met een geheugenchip van een telefoon.
Piezo ontsteker	Met een piezo ontsteker kan elektrische lading worden opgewekt door het uitoefenen van drukkracht. Deze ontstekers worden bijvoorbeeld gebruikt in sommige gasaanstekers.

RAM	RAM (van het Engels: Random Access Memory), ook wel RAM geheugen genoemd, is geheugen dat willekeurig toegankelijk is voor lees- en schrijf acties, waarbij iedere geheugenlocatie even snel bereikt kan worden (in tegenstelling tot bijvoorbeeld een harde schijf). RAM is een vorm van vluchtig geheugen, het verliest zijn gegevens wanneer de voedingsspanning wegvalt.
Reed-contact	Een reed-contact of magneetschakelaar is een elektrisch schakelcontact in een glazen behuizing
Relais	Relais: elektromagnetische schakelaar.
Security Block	Het security block is een elektronica schakeling in een betaalautomaat die ervoor zorgt dat een ingetoetste pincode gecijferd wordt, zodanig dat de pincode veilig via datacommunicatiekanalen naar een bank verstuurd kan worden ter controle van deze pincode. Deze elektronica is ingegoten in een harde kunststof, om manipulatie van deze elektronica te voorkomen of tijdig te detecteren.
Servo	Een servo is een klein kastje met een daaruit stekend armpje. De beweging van dit armpje is afhankelijk van een elektronisch signaal dat het kastje aanstuurt. Servo's worden typisch gebruikt voor het op afstand laten bewegen van onderdelen van modellen, b.v. roeren van modelschepen en modelvliegtuigen, of het stuur van een modelauto.
Servomotor	Een servo(motor) is een motor waarvan de hoekverdraaiing afhankelijk is van een aangeleverd signaal. Dit signaal is in de modelbouw vaak de vertaling van de stand van een bedieningshendel. Op die manier kan de mechanische stand van deze bedieningshandel via draad of via een radiografische verbinding worden overgebracht naar een mechanische verdraaiing op een willekeurige andere plaats. Zo volgt bijvoorbeeld de stand van het rolroer van een modelbouwvliegtuig de stand van een hendel op de zender die het vliegtuig bestuurt.
Silicon die	The silicon die is the functional part inside the IC. The die is packed into a package, often made of epoxy.
SVO	Stuk Van Overtuiging, bewijsmateriaal
TFAT	Voor een beschrijving van het TFAT bestandsysteem zie bijvoorbeeld http://msdn.microsoft.com/en-us/library/aa915463.aspx (bezoekt op 12 maart 2009)
Thumbnail	Een thumbnail bestand bevat een afbeelding waarmee het beginbeeld van een video-opname op het beeldscherm van een telefoon wordt weergegeven.
Thyristor	Thyristor: elektronische schakelaar zonder bewegende delen.
tijdstippen	Alle in deze rapportage vermelde tijdstippen zijn gerelateerd aan de interne klok van de mobiele telefoon [1.001] en komen niet noodzakelijk overeen met de daadwerkelijke tijd.
Timing advance 0-2	Het betreft hier het timing advance interval 0-2 wat overeenkomt met een afstand van 0-1100 meter.
Timing advance 2-8	Het betreft hier het timing advance interval 2-8 wat overeenkomt met een afstand van 1100-4400 meter, zie ook de laatste zinnen in de paragraaf "veldmetingen".
TRIAC	Een TRIAC (van het Engels: TRIode Alternating Current switch) is een halfgeleider bouwsteen waarmee (wissel)stromen kunnen worden geschakeld.
Unicode	Unicode is een internationale standaard voor de identificatie van grafische tekens en symbolen. De standaard voorziet alle tekens en symbolen ('karakters') van alle geschreven talen van een nummer. In tegenstelling tot de oudere ASCII standaard waarmee maar een beperkt aantal karakters is te representeren, ondersteunt Unicode alle gebruikte schriften (zoals het Arabische alfabet en Chinese karakters).
Tulp2g versie	Tulp2g versie informatie staat in de bijlage
Windows CE store	In een Windows CE Smartphone is het niet-vluchtig geheugen opgedeeld in een aantal zogenoemde stores. Elke store is bedoeld voor het opslaan van bepaalde typen informatie. Een store bevat een Windows CE filesysteem en kan gebruikersgegevens bevatten. De overige stores bevatten firmware componenten.

XML openen	Xml bestanden zijn te openen met behulp van een webbrowser, bijvoorbeeld Internet Explorer van de firma Microsoft.														
Waarschijnlijk	De verbale term is afkomstig uit een standaard reeks van termen (de linkerkolom in onderstaande tabel). Deze reeks van verbale termen wordt gebruikt wanneer de onderzoeker geen of onvoldoende getalsmatige gegevens heeft om een numeriek oordeel expliciet te kunnen onderbouwen. De gebruikte verbale term is onder meer gebaseerd op vakkennis en ervaring opgedaan in (zaken)onderzoek. Om de transparantie voor de lezer en de uniformiteit tussen verschillende deskundigen te bevorderen heeft het NFI de verbale termen numeriek gedefinieerd. Deze definities worden uitgedrukt in ordegrootten die in de rechterkolom staan in onderstaande tabel. Bijvoorbeeld: met de term 'iets waarschijnlijker' wordt bedoeld dat de kans op het waarnemen van de onderzoeksresultaten twee tot tien keer groter wordt geacht wanneer de ene hypothese waar is, dan wanneer de andere hypothese waar is. <table border="1"> <thead> <tr> <th>Verbale term</th><th>Ordegrootte bewijskracht</th></tr> </thead> <tbody> <tr> <td>ongeveer even waarschijnlijk</td><td>1-2</td></tr> <tr> <td>iets waarschijnlijker</td><td>2-10</td></tr> <tr> <td>waarschijnlijker</td><td>10-100</td></tr> <tr> <td>veel waarschijnlijker</td><td>100-10.000</td></tr> <tr> <td>zeer veel waarschijnlijker</td><td>10.000-1.000.000</td></tr> <tr> <td>extreem veel waarschijnlijker</td><td>> 1.000.000</td></tr> </tbody> </table> De conclusie verwoordt de bewijskracht van de resultaten ten aanzien van de hypothesen. De conclusie geeft niet de kans weer dat een bepaalde hypothese waar is. Die kans hangt namelijk ook af van overig bewijs en informatie buiten het forensische expertiseterrein en valt daardoor buiten de reikwijdte van dit rapport. Zie voor meer informatie over deze wijze van concluderen de vakbijlage "De reeks waarschijnlijkheidstermen van het NFI". Deze is onder meer te vinden op de NFI website www.forensischinstituut.nl.	Verbale term	Ordegrootte bewijskracht	ongeveer even waarschijnlijk	1-2	iets waarschijnlijker	2-10	waarschijnlijker	10-100	veel waarschijnlijker	100-10.000	zeer veel waarschijnlijker	10.000-1.000.000	extreem veel waarschijnlijker	> 1.000.000
Verbale term	Ordegrootte bewijskracht														
ongeveer even waarschijnlijk	1-2														
iets waarschijnlijker	2-10														
waarschijnlijker	10-100														
veel waarschijnlijker	100-10.000														
zeer veel waarschijnlijker	10.000-1.000.000														
extreem veel waarschijnlijker	> 1.000.000														
Waarschijnlijk	http://nfiweb/040_dossiers/waarschijnlijkheidstermen/waarschijnlijkheidstermen.aspx														
	Een locatie die is opgeslagen in het geheugen van de GPS ontvanger en die wordt verkregen door gegevens in te voeren, te bewerken of te berekenen, of door een huidige positie op te slaan.														
	Een door de gebruiker gedefinieerde lijst van één of meer waypoints waarop genavigeerd kan worden.														
	Een lijst van één of meer locaties (trackpoints) die ontstaat doordat de GPS ontvanger min of meer regelmatig de positie in het geheugen wegschrijft.														
	De positie die de GPS ontvanger als laatste heeft kunnen bepalen aan de hand van de signalen van de GPS satellieten.														
	Dit serienummer is mogelijk terug te vinden in PCbs waarop deze mp3 speler aangesloten is geweest.														
	Opgenomen geluid wordt in dit type apparaat opgeslagen in zogenaamd wav formaat, een veelgebruikt opslagformaat voor audio														

FDT - Leidraad rapporteren

	Een lijst van één of meer locaties (trackpoints) die ontstaat doordat de ontvanger min of meer regelmatig de huidige positie in het geheugen wegschrijft.
	Bij harde schijven is het gebruikelijk om sectoren te tellen vanaf nul; de eerste sector is dan sector 0; de tweede sector, sector 1, enz.

6 Standaard onderzoeken

6.1.1 *Onderzoek naar cookietijden*

Een cookie is een stukje tekst dat een webpagina aan een webbrowser kan sturen om op te slaan op de harde schijf van een gebruiker. De webbrowser stuurt de opgeslagen informatie bij een volgend bezoek weer terug. Zo wordt informatie over de internetgebruiker bijgehouden en worden de verschillende bezoeken van een gebruiker aan elkaar gekoppeld.

Cookies hebben een verlooptijd die aangeeft tot wanneer het cookie geldig is. Een veel voorkomende procedure is dat de server de verlooptijd van het cookie berekent door bij de huidige tijd (van de serverklok) een constante waarde op te tellen. Deze constante waarde is vaak een mooie ronde tijdsduur, bijvoorbeeld 10 jaar. Als deze constante waarde bekend is, dan kan de waarde van de serverklok bepaald worden aan de hand van de verlooptijd in een cookie. In het algemeen wordt de computerklok van een server regelmatig gesynchroniseerd met een tijdserver.

Cookies hebben een aanmaaktijd die wordt bepaald aan de hand van de systeemklok van de computer. De berekende waarde van de serverklok wordt vergeleken met de aanmaaktijd van het cookie op de lokale harde schijf. Het verschil tussen deze tijden is het verschil tussen de lokale computerklok en de serverklok op het moment dat het cookie aangemaakt is. Op deze manier wordt een indicatie verkregen van de mate waarin de lokale computerklok dezelfde tijd aangaf als de computerklok van de server.