jamk.fi

Mobiiliforensiikan nykytilakartoitus

Ville Kylämies

Opinnäytetyö
Joulukuu 2019
Tekniikan ala
Insinööri (AMK), Tieto- ja viestintätekniikka
Kyberturvallisuus

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Kylämies, Ville	Opinnäytetyö, AMK	joulukuu 2019
	Sivumäärä 63	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: Kyllä

Työn nimi
Mobiiliforensiikan nykytilakartoitus

Tutkinto-ohjelma
Tieto- ja viestintätekniikka, Kyberturvallisuus

Työn ohjaaja(t)
Immonen, Jani
Mieskolainen, Matti

Toimeksiantaja(t)
Marko Vatanen
JYVSECTEC

Tiivistelmä

JYVSECTEC:llä oli tarve selvittää ja vertailla erilaisia avoimia forensiikkatyökaluja Android- ja iOS -laitteiden tiedostojen haltuunottoon ja analysointiin.

Työssä implementoitiin kaksi virtualisoitua forensiikkatyöasemaa, joihin asennettiin käyttöjärjestelmäkohtaisia forensiikkatyökaluja ja -ohjelmistoja. Työssä tutkittiin kolmea Android-laitetta, joihin oli luotu testidataa tutkimusta varten.

Opinnäytetyössä selvitettiin nykypäivän mobiililaitteiden forensiikalle asettamat haasteet, sekä avoimia työkaluja hyödyntämällä luottamuksellisen ja tutkinnan kannalta oleellisen tiedon etsimisen tutkittavasta laitteesta. Toimeksiantaja sai tietoa siitä, mitkä ovat ajankohtaisimmat toimintatavat mobiililaitteiden tutkinnassa.

Takavarikoidun laitteen haltuunotto ja luottamuksellisen tiedon tutkinta edellyttää tutkijoilta jonkin laitteessa sijaitsevan tietoturvahaavoittuvuuden hyödyntämistä pääkäyttäjäoikeuksien saamiseksi. Laitteiden kehittyessä yhä tietoturvallisemmiksi lukittuun laitteeseen pääsy on edelleen haastavin osuus mobiiliforensiikassa. Täysin haltuun otetusta laitteesta asiantuntevan tutkijan on mahdollista palauttaa kaikki tieto.

Avainsanat (asiasanat)
Forensiikka, Android, iOS, mobiiliforensiikka, tietorikollisuus

Muut tiedot

jamk.fi

Description

Author(s)	Type of publication	Date
Kylämies, Ville	Bachelor's thesis	December 2019
	Number of pages 63	Language of publication: Finnish
		Permission for web publication: x

Title of publication

Mapping the state of mobile forensics

Degree programme

Information and Communications Technology

Supervisor(s)

Immonen, Jani

Mieskolainen, Matti

Assigned by

Vatanen, Marko

JYVSECTEC

Abstract

The thesis was assigned by Jyväskylä Security Technology which works alongside JAMK University of Applied Sciences as an independent cyber security operator. The purpose was to research and compare different open source mobile forensic tools and their effectiveness for Android and iOS data acquisition and analysis.

Two forensic workstations were implemented in virtualized platform with OS-specific forensic software as well as three physical Android devices for research purposes. Dummy data was generated within the test devices to demonstrate the use of forensic tools.

The study results describe the obstacles of modern-day mobile forensics, best practices for open source mobile forensics as well as the sensitive information to look for in devices with the combination of different forensic techniques and tools.

Acquiring the seized device's data requires the analyst to exploit a vulnerability within the device to gain privileged access and extract the sensitive data, which remains the greatest challenge in mobile forensics. With the devices constantly evolving, forensic analysts are required to implement more creative techniques to access a locked device. Once a device has been fully acquired, the most limiting factor comes down to the analyst's technical expertise to look for data relevant to the investigation.

Keywords ()

Mobile forensics, Android, iOS, cyber crime

Miscellaneous (Confidential Information)

Sisältö

Kuviot

Taulukot

Lyhenteet

ADB	Android Debug Bridge
APFS	Apple File System
API	Application programming interface
APT	Advanced Persistent Threat
ART	Android Runtime
CIRT	Computer Incident Response Team
CoC	Chain of custody
COW	Copy-on-write
CVE	Common Vulnerabilities and Exposures
FBE	File-Based Encryption
FDE	Full-Disk Encryption
FTK	Forensic Toolkit
HAL	Hardware Abstraction Layer
IEEE	Institute of Electrical and Electronics Engineers
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
iOS	iPhone operating system
JTAG	Joint Test Action Group
JYVSECTEC	Jyväskylä Security Technology
LKM	Loadable Kernel Module
OSE	Open Source Edition
SDK	Software Development Kit
TSK	The Sleuth Kit

1 Johdanto

1.1 Mobiili- ja älylaitteiden merkitys nykypäivänä

Älylaitteiden ja etenkin älypuhelinten viime vuosina räjähdysmäisesti kasvanut määrä on muuttanut ihmisten tavan hoitaa päivittäisiä asioitaan. Niistä on tullut osa jokapäiväistä elämää. Nämä helposti ja edullisestikin saatavilla olevat laitteet mahdollistavat puhelujen ja tekstiviestien lisäksi Internetin ja muiden sähköisten palveluiden käytön lähes missä ja milloin tahansa. Pienestä koostaan huolimatta älypuhelimiin mahtuu hyvin suuri määrä erilaisia toimintoja ja ominaisuuksia. Niillä voidaan ottaa valokuvia ja videoita, maksaa laskuja, tarkastella pankkitietoja, potilastietoja ja lähes mitä tahansa muuta luottamuksellista tietoa. Älypuhelimia ja muita mobiililaitteita käytetään myös laajasti sosiaalisessa mediassa tiedon ja median jakamiseen, esimerkiksi Instagramissa, Facebookissa ja Twitterissä. Tämä tarkoittaa myös sitä, että puhelin sisältää mahdollisesti paljon luottamuksellista tietoa käyttäjästään. Älypuhelinta voisi kutsua ihmisen nykyaikaiseksi päiväkirjaksi. Bankmycellin statistiikan mukaan älypuhelinten käyttäjiä on tällä hetkellä noin 2,7 miljardia ympäri maailmaa. Määrän odotetaan kasvavan lähes kolmeen miljardiin vuoteen 2020 mennessä ja siitä edelleen kymmenin prosentin vuosikasvulla. (How many phones are in the world? 2019.)

Älypuhelinten lisääntyminen, niiden laajat toiminnallisuudet sekä niiden sisältämä kiinnostava data ovat aiheuttaneet myös sen, että niitä käytetään yhä enemmän rikolliseen toimintaan. Tästä on syntynyt lisääntynyt tarve mobiiliforensiikalle, jolla tarkoitetaan mobiililaitteen rikosteknistä tutkimista lain sallimissa olosuhteissa käyttäen hyväksyttyjä toimintatapoja (Ayers, Brothers & Jansen 2014).

Laitevalmistajat pyrkivät tekemään laitteistaan mahdollisimman tietoturvallisia loppukäyttäjän tietojen ja yksityisyyden suojaamiseksi. Useat eri käyttöjärjestelmät ja säännölliset tietoturvapäivitykset hankaloittavat forensiikkatyötä, koska laitteisiin murtautuminen ja niiden tutkiminen edellä mainituista syistä vaikeutuvat. Laitevalmistajat eivät myöskään välttämättä luovuta viranomaisille tietoja (vaikka siihen pys-

tyisivät), joilla nämä pystyisivät ohittamaan tietoturvapäivityksen tai jonkin muun esteen (kuten pääsykoodi). Esimerkiksi vuonna 2015 tapahtuneen San Bernardinon joukkoammuskelun tutkinta. FBI halusi Applen kehittävän ohjelmiston, jonka avulla he pystyisivät avaamaan epäillyn ampujan iPhonen, joka oli suojattu PIN-koodilla. Apple ei suostunut tähän vedoten tietoturvariskiin, joka uhkaisi kaikkia iPhonen käyttäjiä, jos päivitys vuotaisi vääriin käsiin. FBI ilmoitti myöhemmin löytäneensä kolmannen osapuolen, jonka avulla matkapuhelin saatiin avattua, mutta sieltä ei loppujen lopuksi löytynyt tutkinnan kannalta hyödyllistä tietoa. (Apple vs. the FBI -- 2016.)

Yksi suurimmista mobiiliforensiikan haasteista on se, että dataa voidaan hallinnoida, varastoida ja synkronoida useiden eri laitteiden välillä (tietoihin pääsee näin ollen käsiksi monesta paikasta). Lisäksi datan ollessa haihtuvaa (engl. volatile) ja se, että se voidaan poistaa etänä, aiheuttaa lisää vaivannäköä tutkijoilta tietojen säilyttämiseksi. (Bommisetty, Mahalik, Skulkin & Tamma 2018.) Myös lukuisat täysin erilaiset käyttöjärjestelmät ja arkkitehtuurit edellyttävät spesifiä osaamista tietyn laitteen tai valmistajan saralla.

1.2 Toimeksiantaja

Opinnäytetyön toimeksiantaja oli Jyväskylä Security Technology (JYVSECTEC). JYVSECTEC on Suomen johtava itsenäinen kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus. Se toimii osana Jyväskylän Ammattikorkeakoulun IT-instituuttia. JYVSECTEC tarjoaa organisaatioille kyberharjoituksia, tietoturvatestausta, tutkimustyötä ja konsultointia. Sen tavoitteena on kiihdyttää valmiuksia ja teknistä kehittämistä nykypäivän tietoturvauhkia vastaan. (Secure exercise environment 2019.)

JYVSECTEC on kehittänyt kyberturvallisuuden kehitysympäristön RGCE:n (Realistic Global Cyber Environment), joka on todenmukainen harjoitteluympäristo, joka jäljittelee oikeaa verkkoa ja sitä voidaan käyttää kyberturvallisuuden harjoittelemiseen ja kyberuhkien simuloimiseen (Secure exercise environment 2019).

1.3 Tehtävät ja tavoitteet

Toimeksiantajalla oli tarve selvittää, mikä on mobiiliforensiikan tämänhetkinen tilanne ja miten nopeasti kehittyvän teknologian haasteisiin pystytään vastaamaan. Työn painopiste on Androidin forensiikassa ja sen tutkimista hyödyntäen avoimia työkaluja, sekä samalla vertaillen niitä. Lisäksi työssä käydään läpi sekä Androidin, että iOS:n forensiikkaprosessi kartoitetaan iOS:lle saatavilla olevia forensiikkatyökaluja.

2 Forensiikka ja kyberturvallisuus

2.1 Kyberturvallisuus

Kyberturvallisuudesta puhuttaessa tarkoitetaan monesti tietoturvauhkien torjumista ja ennaltaehkäisyä. Forensiikka ja tietoturvapoikkeamien hallinta (engl. Incident response) pyrkii tunnistamaan ja ymmärtämään jo tapahtuneen tietoturvaloukkauksen keinot ja tarkoitusperät.

2.1.1 APT (Advanced Persistent Threat)

Advanced Persistent Threat -käsitteellä tarkoitetaan hyvin resursoituja ja koulutettuja tahoja, jotka suorittavat pitkäkestoisia tietoturvahyökkäyksiä erilaisiin hyvin luottamuksellisiin taloudellisiin, patentoituihin tai kansalliseen turvallisuuteen liittyviin tahoihin. (Amin, Cloppert & Hutchins n.d.) Ne ovat kohdistettuja ja monimutkaisia verkkohyökkäyksiä, jotka hyödyntävät useita eri hyökkäysvektoreita sulautuen muun verkkoliikenteen joukkoon. Yleensä APT-hyökkäyksillä pyritään saamaan pääsy luottamuksellisiin tietoihin tai häiritsemään toimintaa.

2.1.2 Cyber Kill Chain -malli

Kill chain tarkoittaa systemaattista prosessia, jossa pyritään vaikuttamaan vastustajaan haluttujen vaikutusten aikaansaamiseksi. Se on Lockheed Martinin alun perin so-

tilaskäyttöön kehitetty konsepti hyökkäyksen rakenteen muodostamiseksi. Siitä tehtiin vuonna 2011 vastaavanlainen yleinen rakenne kyberhyökkäyksen toteuttamiseksi digitaalista kohdetta vastaan, myös Lockheed Martinin toimesta. Tietoturvahyökkäyksen onnistumiseksi jokaisen ketjun vaiheen täytyy onnistua, tai ketju katkeaa ja hyökkäys epäonnistuu. Kuviossa 1 on kill chainin eri vaiheet.

Kuvio 1. Cyber kill chain -malli (Lockheed Martin n.d.)

Cyber Kill Chain -mallin eri vaiheet:

1. Reconnaissance (Tiedustelu): Tunkeutuja suunnittelee hyökkäystään tutkimalla ja tunnistamalla potentiaalisia kohteita. Hän yrittää ymmärtää millä keinoin hän pääsee päämääräänsä. Tyypillisiä keinoja ovat sähköpostiosoitteiden kerääminen, työntekijöiden tunnistaminen. Kohteilta yritetään kalastella tietoja esimerkiksi tekstiviesteillä tai puheluilla.
2. Weaponization (Aseistaminen): Tunkeutuja kehittelee haittaohjelman ja piilottaa sen esimerkiksi PDF-tiedostoon tai Office-dokumenttiin.
3. Delivery (Jakelu): Haittaohjelma toimitetaan kohteeseen. Lockheed Martinin (n.d). CIRT-tiimin mukaan kolme yleisintä toimitustapaa ovat sähköpostiliitteet, verkkosivut ja USB-mediat. Erilaiset kanssakäymiset sosiaalisessa mediassa ovat myös suosittuja tapoja levittää haittaohjelmia.
4. Exploitation (Hyödyntäminen): Tunkeutuja väärinkäyttää jotain haavoittuvuutta saadakseen pääsyn kohteeseen hyödyntämällä ohjelmisto-, laitteisto- tai ihmishaavoittuvuutta. Tunkeutuja hyödyntää esimerkiksi mahdollista nollapäivähaavoittuvuutta tai ohjaa käyttäjän klikkaamaan hämärää hyperlinkkiä.
5. Installation (Asentaminen): Haittaohjelma asentuu kohteeseen ja samalla sinne aukeaa takaovi (backdoor), jolla voidaan ohittaa autentikointi ja ylläpitää oikeuksia järjestelmässä.

6. Command and Control (C2) (Jakeluverkko): Haittaohjelma avaa kanavan hyökkääjän ja uhrin välille, joka mahdollistaa väärinkäytön etänä. Yleisimmät C2-kanavat ovat verkko-, DNS- ja sähköpostiprotokollat. Hyökkääjä suorittaa erilaisia forensiikan vastaisia toimia esimerkiksi muuttelemalla aikaleimoja eri tapahtumille.
7. Actions on objectives (Tavoitteiden toteuttaminen): Tässä vaiheessa, kun aikaisemmat vaiheet on saatu suoritettua, on tunkeutujan mahdollista suorittaa toimia alkuperäisen tavoitteensa saavuttamiseksi. Tyypillisesti tunkeutuja kerää tietoa uhrista tai yrittää edetä syvemmälle järjestelmään. (Amin, R. Cloppert, M. & Hutchins, E n.d.)

2.2 Forensiikan käsite

Englannin kielen termi forensic science on määritelmänä tieteellisten periaatteiden soveltamista oikeusasioihin (Johansen 2017, 27). Sen yksi osa-alueista on digitaaliforensiikka tai digitaalinen forensiikka (engl. Digital forensics). Tällä tarkoitetaan jonkin laitteen tutkintaa rikostutkijoiden toimesta todistusaineiston löytämiseksi. Forensiikkatyöstä vastaa yleensä jokin kaupallinen forensiikan toimija tai virkavalta. Tutkijat analysoivat sähköistä todistusaineistoa erilaisia työkaluja ja tekniikoita hyödyntäen.

Esimerkkitapauksia, joissa voidaan tarvita forensiikkaa:

- Todistusaineiston kerääminen oikeudenkäyntiä varten
- Kyber- ja APT-uhkien aiheuttamien loukkausten tutkinta
- Yrityksissä tapahtuvat tutkinnat
    - Immateriaalioikeudet
    - Tietovarkaudet
    - Resurssien väärinkäyttö
    - Kyberhyökkäykset
    - Auditointi
    - Työpaikkakiusaaminen (Hoog 2011.)

2.3 Mobiiliforensiikka

2.3.1 Yleistä

Mobiiliforensiikka on digitaalisen forensiikan haara, jossa keskitytään mobiililaitteiden tutkintaan. Muita digitaalisesta forensiikasta haarautuneita alueita ovat esimerkiksi pilvipalveluiden forensiikka tai verkkoforensiikka. Mobiiliforensiikka on tullut enemmissä määrin käyttöön vasta vuosituhannen vaihteessa, jolloin matkapuhelimet alkoivat olemaan saatavilla kuluttajille laajemmin. Matkapuhelimia on toki käytetty rikolliseen toimintaan jo aiemmin, mutta takavarikoitujen laitteiden tutkinta rajoittui lähinnä valokuvien ottamiseen puhelimen näytöstä, joka oli aikaa vievä ja tehoton tapa tutkia päätelaitetta. Nämä vaatimukset johtivat erilaisten kaupallisten työkalujen kehittämiseen. (Bertè, Marturana, Me, & Tacconi 2011.)

Mobiiliforensiikan toimintaperiaate ja forensiikkaprosessi poikkeavat merkittävästi esimerkiksi tavallisen Windows-pohjaisen tietokoneen kiintolevyn tutkinnasta ja analysoinnista. Suurin ero on se, että tietokoneiden kiintolevyiltä tutkittavat tiedot pysyvät enimmäkseen staattisina. Mobiililaitteet sen sijaan ovat hyvin dynaamisia. Niiden toiminta on riippuvaista verkkoyhteydestä ja sovelluksista. On siis tärkeää, että laite ja rauta säilytetään mahdollisimman hyvin siinä tilassa, missä ne olivat esimerkiksi takavarikointihetkellä. Laite eristetään sähkömagneettiselta säteilyltä siihen tarkoitetulla suojapussilla (Faraday bag), ettei se vahingossakaan yhdistä avoimiin verkkoihin ja ettei tätä kautta tiedostoja onnistuta poistamaan etänä. Laite on syytä pitää virroissaan, jotta vältytään PIN-koodin kyselyltä. Tämä aiheuttaisi lisää haasteita tutkijoille (Introduction to Mobile Forensics 2014).

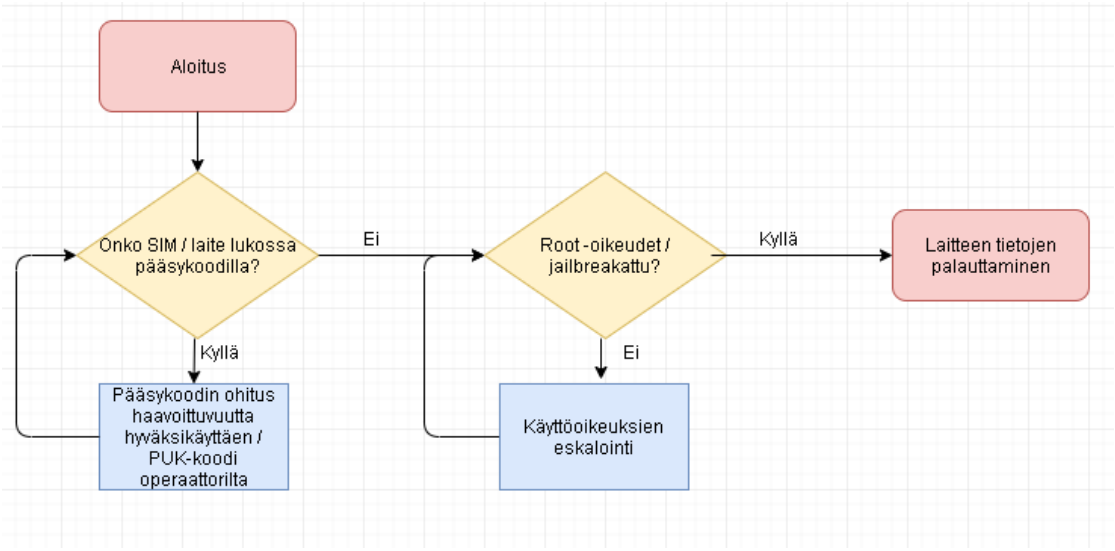
2.3.2 Mobiiliforensiikassa esiintyviä haasteita

Mobiililaitteiden tutkintaan liittyy ainutlaatuisia haasteita, joita ei esiinny digitaaliforensiikassa esimerkiksi tietokoneiden kiintolevyjen tutkinnassa.

- Laitteistoeroavaisuudet: Markkinoilla on hyvin suuri määrä erilaisia mobiililaitteita, jotka ovat laitteistoltaan, ominaisuuksiltaan ja arkkitehtuuriltaan täy-

sin erilaisia. Nopea tuotekehityssykli edellyttää tutkijoilta mukautumista haasteisiin ja pysymistä ajan tasalla ajankohtaisimmista tutkintamenetelmistä. (Skulkin, Tamma, & Tindall 2019.)

- Tietojen säilyminen muuttumattomina: Yksi tärkeimmistä säännöistä forensiikassa on se, että todistusaineisto pitää pyrkiä säilyttämään muuttumattomana. Tämä ei kuitenkaan täysin toimi mobiiliforensiikassa, sillä laitteen tila muuttuu jatkuvasti. Esimerkiksi laitteen sammuessa RAM-muisti tyhjenee ja käynnissä olevassa laitteessa pyörii jatkuvasti taustaprosesseja. Useimmiten tutkinta edellyttää laitteen pitämistä käynnissä. (Skulkin ym. 2019.)
- Forensiikkatyökalujen tuki: Mobiililaitteille ei ole yhtä työkalua, josta löytyy tuki kaikille mobiililaitteille. Näin ollen tutkijalla pitää olla hallussaan useita työkaluja kaikkien tarpeellisten toimintojen suorittamiseksi. Oikean työkalun valinta voi olla haastavaa, ja kaupalliset forensiikkatyökalut ovat hyvin kalliita.
- Tietoturva: Käyttäjien tietosuojan kiristyessä myös mobiililaitteiden tietoturvaan kiinnitetään yhä enemmän huomiota. Ennen kuin tutkija voi analysoida laitetta, hänen täytyy pystyä esimerkiksi ohittamaan laitteen pääsykoodi. Nykypäivän laitteet ovat täysin kryptattuja ja hyvin vaikeita murtaa. Kuviossa 2 on laitteen haltuunoton vaiheet. Pääsykoodin ohittamisen onnistuminen riippuu hyvin paljon laitteen käyttöjärjestelmän versiosta, asetuksista ja tutkijan teknisistä kyvyistä. (Bommisetty ym. 2018.)

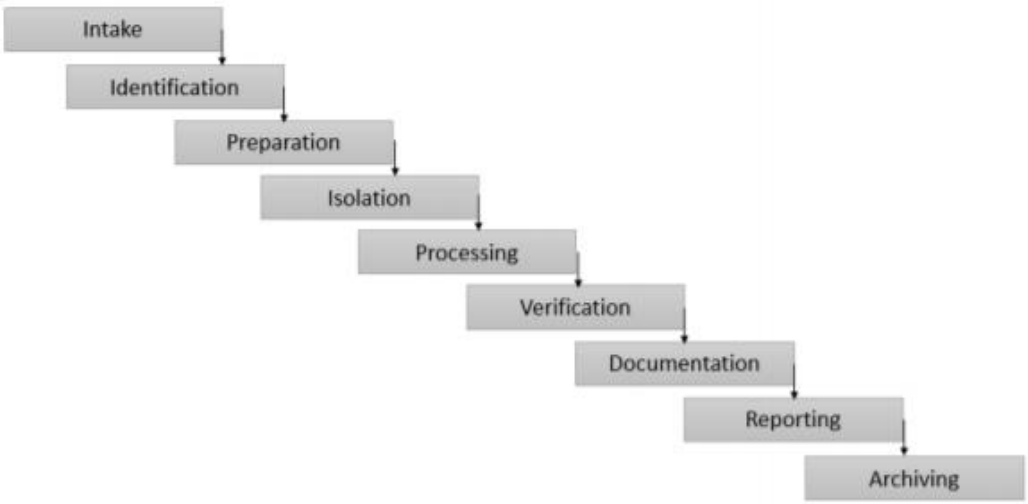


Kuvio 2. Täydellisen haltuunoton edellytykset

2.3.3 Sähköisen todistusaineiston käsittelyprosessi

Todisteiden poiminta ja rikostekninen tutkinta vaihtelee riippuen laitteesta. Johdonmukaisen tutkintaprosessin noudattaminen laitteesta riippumatta kuitenkin auttaa tutkijaa varmistamaan sen, että kaikki todistusaineisto on hyvin dokumentoitu ja perusteltu. Tutkijan pitää pystyä perustelemaan, miksi jokin löydös on hänen mielestään oikeaa todistusaineistoa. Mobiililaitteiden tutkintaan ei kuitenkaan ole vielä olemassa standardisoitua toimintatapaa. (Bommisetty ym. 2018.)

Kuviossa 3 on kuvailtu todistusaineiston käsittelyprosessi.



Kuvio 3. Todistusaineiston käsittelyprosessi (Murphy n.d.)

Todisteiden vastaanottamisvaihe (intake phase)

Prosessi käynnistyy vastaanottamisvaiheella, jossa tehdään paperityöt dokumentoimalla hallussapitoketju (chain of custody), omistajuustiedot ja tapahtuman tyyppi, jossa laite on ollut mukana. Hallussapitoketju luodaan rikospaikalta kerätystä todistusaineistosta kronologisessa järjestyksessä ottaen huomioon sen, mitä todistusaineistoa löytyi, kuka aineistoa on käsitellyt, missä kunnossa aineisto on ollut löytöhetkellä sekä todistusaineiston tarkka sijainti. Rikospaikka on tutkittavissa vain rajoitetun ajan, joten pienetkin yksityiskohdat pitää ottaa huomioon. Hallussapitoketjua voidaan hyödyntää myöhemmin oikeudessa, mutta vain jos se on tehty oikein. (Murphy n.d.)

Tunnistamisvaihe (identification phase)

Tunnistamisvaiheessa pitää ottaa aina huomioon seuraavat seikat:

- Laillinen auktoriteetti
    - Oikeuskäytänteet mobiililaitteiden tutkinnasta muuttuvat jatkuvasti
    - Laitteen tutkinta suoritettava etsintäluvan rajoitteiden mukaisesti
- Tutkinnan tavoitteet
    - Tutkija tekee ratkaisun siitä, kuinka syvällisesti laitetta on tarvetta tutkia. Riittävät todisteet voi saada kevyemmälläkin tutkinnalla
- Laitteen valmistaja, malli sekä muut tunnistettavuustiedot
    - Laitteen tunnistaminen auttaa valitsemaan oikeat työkalut ja tutkintamenetelmät
- Laitteen ulkoiset mediat
    - Jos laitteessa on esimerkiksi lisämuistikortti, myös se on syytä tutkia
- Muut mahdolliset todistusaineistot
    - Laitteesta otettava sormenjälkitunnisteet ja muut mahdolliset jäljet (Murphy n.d.)

Valmistautuminen (preparation phase)

Valmistautumisvaiheessa kartoitetaan tarvittavat työkalut ja menetelmät perustuen laitemalliin, käyttöjärjestelmään ja sen versioon, tutkinnan tavoitteisiin sekä laitteen ulkoisiin medioihin. (Murphy n.d.)

Eristäminen (isolation phase)

Mobiililaitteet ovat riippuvaisia verkoista (matkapuhelinverkot, bluetooth, Wifi), joten laite on syytä eristää kaikista verkoista tutkinnan ajaksi. Näin ollen laitteeseen ei tule uutta dataa ja siitä ei pystytä poistamaan dataa etänä. Esimerkiksi kadonneen iPhonen pystyy tyhjentämään helposti etänä, jos ominaisuus on otettu käyttöön ennen laitteen katoamista. Eristämiseen käytetään Faradayn häkkiä, joka estää ulkopuolelta tulevan sähkömagneettisen säteilyn. (Murphy n.d.)

Prosessointi (processing phase)

Prosessointivaiheessa laitetta tutkitaan valmistautumisvaiheessa tehtyjen valintojen

mukaisesti. Mahdolliset muistikortit pitää tutkia erikseen, ettei laitteen kiintolevyllä olevat tiedot tai aikaleimat muutu. Fyysisen tutkinnan avulla laitteesta on mahdollista saada kopioitua kaikki data (myös poistettu data). Lisäksi se aiheuttaa vähiten muutoksia laitteen muistiin. (Murphy n.d.)

Varmistaminen (verification phase)
Kun laitteen tutkinta on suoritettu, pitää varmistaa ovatko saadut tiedot tarkkoja. Varmistustapoja on useita. Esimerkiksi laitteesta kaivettuja ja siirrettyjä tietoja voidaan verrata laitteessa oleviin tietoihin; pitää kuitenkin olla tarkkana, ettei laitteen tietoja muuta ja näin ollen poista tai muuta todistusaineistoa. Toinen tapa tarkistaa on tiivistää (Engl. hash) saadut tiedot ja verrata niiden tiivistettä alkuperäiseen dataan, jonka pitäisi pysyä muuttumattomana. Lisäksi tietoja voidaan tutkia eri työkaluilla ja verrata, löytyykö niistä erilaisuuksia. (Murphy n.d.)

Dokumentointi ja raportointi (Documentation and reporting phase)
Tutkija dokumentoi tekemisiään jatkuvasti tutkinnan edetessä. Ainakin seuraavat asiat kirjataan ylös tutkintaa tehdessä:

- Tutkinnan aloittamisen kellonaika ja päivämäärä
- Laitteen fyysinen kunto
- Valokuvat laitteesta ja yksittäisistä komponenteista
- Oliko puhelin käynnissä vai sammutettuna tutkintaa aloitettaessa
- Laitteen tunnistetiedot (valmistaja, malli ym.)
- Tutkinnassa käytetyt työkalut
- Tutkinnan aikana löydetyt tiedot (Murphy n.d.)

Esitys (presentation phase)
Tutkija tekee raportin tekemästään työstä, jota voidaan esitellä muille tutkijoille ja jota voidaan hyödyntää oikeudessa. Väärinkäyttäjän toimista tehdään aikajana, jolla voidaan perustella, mitä milloinkin on tapahtunut. Löydökset raportoidaan lyhyesti ja selkeästi. (Murphy n.d.)

Arkistointi (archiving phase)
Laitteesta saatu data säilytetään ja arkistoidaan mahdollista myöhempää käyttöä var-

ten. Jotkut oikeuskäsittelyt kestävät pitkään ja tuomioistuimet vaativat tietojen säilyttämistä. Syytetyt henkilöt saattavat myös valittaa tuomioista, jolloin tiedot saatetaan ottaa uudelleen tutkintaan. (Murphy n.d.)

2.3.4 Työkalujen luokitusjärjestelmä

Tunnistettaessa laitteen analysointiin soveltuvia työkaluja tutkijan kannattaa hyödyntää Sam Brothersin vuonna 2009 kehittämää luokitusjärjestelmää (Ks. kuvio 4.) Se pyrkii lajittelemaan työkalut ja metodit siihen kategoriaan, jota niillä on mahdollista suorittaa. Siirryttäessä ylemmäs järjestelmässä tutkinnasta tulee teknisempää, vaikeampaa ja enemmän aikaa vievää ja työkalut kallistuvat. Metodit ovat kuitenkin tehokkaampia, tutkittava tieto säilyy paremmin muuttumattomana ja sen käyttö todistusaineistona on helpommin perusteltavissa eli tieto on forensisesti luotettavampaa (engl. Forensically sound).

Kuvio 4. Työkalujen luokitusjärjestelmä (Brothers, 2014)

Manuaalisella palauttamisella tarkoitetaan käytännössä laitteen selailua, jota voi tehdä lähes jokaisella matkapuhelimella. Tutkija käy läpi puhelimen tietoja tutkimalla niitä puhelin kädessään ja dokumentoi löydetyt tiedot valokuvaamalla puhelimen näyttöä. Suurin riskitekijä on inhimillinen virhe tai huolimattomuus. Virheiden välttämiseksi tutkijalla on syytä olla muistilista asioista, jotka tällä menetelmällä pystytään löytämään.

Looginen palauttaminen ja haltuunotto on laitteen tiedostojen kopioimista työasemaan. Loogista palauttamista tehdään kiinnittämällä laite työasemaan esimerkiksi USB:n tai Bluetoothin kautta. Työasemalta pystytään antamaan erilaisia komentoja laitteeseen. Laite tulkitsee komennon ja tämän pohjalta palauttaa tietoa takaisin työasemaan tutkijan analysoitavaksi. Suurin osa forensiikkatyökaluista toimii luokituspyramidin tällä kerroksella. Looginen tutkinta on melko helppoa ja nopeaa, ja sillä pystytään saamaan paljon tietoa tarvitsematta välttämättä lainkaan luokitusjärjestelmän vaativampia kerroksia. Toisaalta looginen analysointi saattaa muuttaa tutkittavan laitteen tietoja, mikä vaikuttaa suoraan todistusaineiston eheyteen. (Tamma ym. 2018.) Looginen tutkinta ei edellytä root-oikeuksia tutkittavaan laitteeseen, mutta USB-vianetsintä pitää olla kytkettynä (root-oikeuksilla varustetusta laitteesta saa kuitenkin enemmän tietoa palautettua).

Luokitusjärjestelmän kolmannessa kerroksessa (Hex dump) laitteelle tehdään fyysinen palauttaminen. Koko laitteesta, tai vaihtoehtoisesti jostain tietystä kiintolevystä tai osiosta, luodaan identtinen kopio, joka sisältää kaikki tiedostot, poistetut tiedostot sekä käyttämättömän tilan (engl. Slack space). Tämä toimenpide on verrattavissa digitaaliforensiikassa esimerkiksi kiintolevystä luotavaan levykuvaan ja sillä pystytään palauttamaan myös poistettuja tiedostoja. Fyysinen palauttaminen edellyttää root-oikeuksia (Android) tai jailbreakin (iOS) toimiakseen, sillä kaikkia tiedostoja ei ilman niitä pystytä käsittelemään. Käytännössä tämä palauttaa kaiken datan laitteesta, joten tutkintaa rajoittaa ainoastaan tutkijan kyky osata etsiä ajankohtaista aineistoa.

Neljännessä kerroksessa (engl. Chip off) laitteesta irrotetaan muistipiiri kokonaan juottamalla ja sitä tutkitaan joko muistikortinlukijan avulla tai toisella puhelimella. Toimenpide on kallis ja vaatii rautatason osaamista tutkijalta, sillä muistipiiri voi rikkoutua helposti. Näistä syistä alemmilla kerroksilla on syytä yrittää tehdä kaikki toimenpiteet, ennen kuin muistipiiriä aletaan irrottamaan. Joskus piirin irrottaminen ja analysointi on ainut keino löytää todistusaineistoa, jos esimerkiksi puhelin on muuten rikkoutunut, mutta muistipiiri on säilynyt ehjänä. (Tamma ym. 2018.)

Viidennellä tasolla (engl. Micro read) käytetään tehokasta mikroskooppia lukemaan piirissä olevien fyysisten porttien tilaa. Jokainen portti joudutaan katsomaan kerrallaan, joten prosessi on hyvin kallis ja aikaa vievä. (Ayers, Brothers & Jansen 2014.)

Viidennen tason tutkinta on harvinaista, ja siitä on tällä hetkellä kehnosti dokumentaatiota saatavilla.

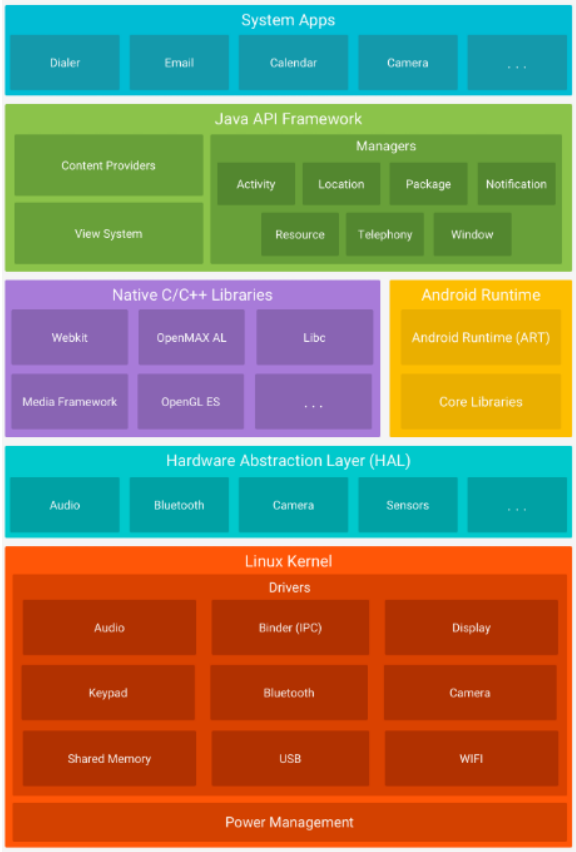
JTAG on IEEE:n kehittämä edistyksellinen laitteen haltuunottotapa. Se on alun perin suunniteltu testikäyttöön laitteen valmistusvaiheessa. Sitä voidaan käyttää myös forensiikassa fyysisen levykuvan palauttamiseen. JTAGia käytetään usein silloin, kun tutkittavan laitteen pääsykoodia ei pystytä ohittamaan. Laitteeseen yhdistetään muistipiirejä ja laitteessa olevia testiportteja (engl. Test Access Ports) hyödyntämällä prosessoria ohjeistetaan lähettämään tiedot liitettyihin muistipiireihin. (Skulkin ym. 2019.)

2.4 Android

2.4.1 Yleistä

Androidin historia kulkeutuu vuoteen 2003, kun Andy Rubin, Rich Miner, Nick Sears ja Chris White perustivat Android Inc. yrityksen Kaliforniassa. Rubinin mukaan Androidin tarkoitus oli sallia fiksummat mobiililaitteet, jotka ovat enemmän tietoisia omistajansa sijainnista ja mieltymyksistä. (Google’s Android OS -- 2011.) Google osti Android Inc:n vuonna 2005 ja julkisti käyttöjärjestelmän vuonna 2007. Ensimmäinen kaupallinen Android-laite T-Mobile G1 julkaistiin syyskuussa 2008. Androidin uusin versio, Android 10, julkaistiin syyskuussa 2019.

Android on Linuxiin pohjautuva ohjelmistopino (engl. Software stack), joka toimii kerroksittain. Androidin pääkomponentit ovat kuvailtuna kuviossa 5.



Kuvio 5. Androidin arkkitehtuuri (Android n.d)

Android-käyttöjärjestelmä on suurimmilta osin Linux-kernelin päälle suunniteltu, johon Google on tehnyt joitakin arkkitehtuurillisia muutoksia. Linux on siirrettävä alusta ja se voidaan helposti kääntää erilaiselle laitteistolle toimivaksi. Androidin ydintoiminnot, kuten prosessit, muisti, turvallisuus, ja verkot ovat Linux kernelin hallinnoimia. Kernelissä sijaitsevat ajurit vastaavat myös rautatason käskyjen muuntamisesta ohjelmistomuotoon. Esimerkiksi kameralla kuvaa otettaessa kameran ajuri lähettää käskyn kuvan ottamiseksi ja sen tallentamiseksi kuvagalleriaan. (Tamma ym. 2018.)

Laitteiston abstraktiokerros (engl. Hardware abstraction layer) mahdollistaa korkeamman tason Java API:n viitekehyksen toiminnan laitteiston kanssa. Abstraktiokerros koostuu kirjastomoduuleista, jotka luovat rajapinnan jollekin tietylle komponentille (kuten Bluetooth tai kamera). (Skulkin ym. 2019.)

Monet Android-järjestelmien ydinkomponentit on tehty natiivikoodista, jotka tarvitsevat C tai C++-kielillä kirjoitettuja kirjastoja. Android hyödyntää Javan viitekehyksen ohjelmointirajapintoja vapauttaakseen näiden kirjastojen toiminnallisuuksia laitteen sovelluksille.

Uudemmissa Android-laitteissa (versiosta 5.0 alkaen) jokainen applikaatio toimii ART:ssä sekä omana prosessinaan, että instanssinaan. ART ajaa useita virtuaalikoneita suorittamalla DEX-tiedostoja, jotka on optimoitu käyttämään vähän muistia. (Android n.d.)

Java API -viitekehystä käytetään Android-laitteiden perustoimintojen käsittelemiseen, kuten puheluiden tai resurssien hallinnoimiseen. Se mahdollistaa myös sovelluskehityksen käyttämällä modulaarisia järjestelmäkomponentteja (Skulkin ym. 2019).

Androidin arkkitehtuurin ylin kerros, eli järjestelmäapplikaatiokerros (engl. System apps layer) sisältävää Androidin ydinsovellukset esimerkiksi puhelimen käyttämiseksi. Nämä sovellukset tulevat esiasennettuina laitteen mukana. Järjestelmäapplikaatioita voi peruskäyttäjän lisäksi hyödyntää myös sovelluskehittäjät, jotka voivat käyttää niiden toiminnallisuuksia oman sovelluksensa kehittämisessä. Android varastoi kaikki tiedot osioihin.

2.4.2 Tietojärjestelmät

Androidin tietojärjestelmät voidaan jakaa kolmeen eri kategoriaan:

- Flash-tietojärjestelmät
    - YAFFS2
    - F2FS
    - RFS

Flash-muistilla tarkoitetaan haihtumatonta muistia, joka on mahdollista tyhjentää ja uudelleenohjelmoida ns. muistilohkoihin. Flash-muistin luonnosta johtuen sille on kehitetty erillisiä tietojärjestelmiä epätoivottujen ilmiöiden (kuten write amplification) välttämiseksi. YAFFS2 on avoin, yhden säikeen tietojärjestelmä. Uusimmat kernelit eivät tue enää tätä tietojärjestelmää, sillä sen tiedetään olevan pullonkaula moniydinjärjestelmissä. F2FS on alun perin Samsungin kehittämä tietojärjestelmä, mutta myös muut OEM:t, kuten Huawei ja OnePlus ovat alkaneet käyttämään sitä jossain määrin. Kyseessä on nopea tietojärjestelmä, joskin pidemmässä juoksussa siinä aiheutuu tiedostojen pirstoutumista ja tämä hidastaa laitteen toimintaa.
RFS on ainoastaan Samsungin laitteissa käytetty tietojärjestelmä, joka perustuu FAT16/32:een.

- Mediapohjaiset tietojärjestelmät
    - EXT (2/3/4)
    - VFAT

EXT-tietojärjestelmä julkaistiin ensimmäisen kerran vuonna 1992. Kyseessä on virtuaalitietojärjestelmä, joka abstraktiota hyödyntäen tarjoaa käyttöliittymän kernelin ja tietojärjestelmän välillä. EXT3 tukee journalointia, jolla järjestelmän eheys saadaan säilytettyä, vaikka laitteelle tulisi esimerkiksi äkillinen virtakatkos. EXT4:n suurin ero EXT3:een on se, että se tukee paljon suurempia tiedostokokoja sekä tuplasti suuremman määrän alihakemistoja. VFAT on laajennus aikaisempiin FAT16 ja FAT32-tietojärjestelmiin. VFAT:n avulla voidaan hallinnoida Android-laitteen FAT32-osiossa sijaitsevia tietoja. (Tamma ym. 2018.)

- Pseudo-tietojärjestelmät
    - rootfs
    - procfs
    - sysfs
    - tmpfs

Rootfs-tietojärjestelmä sisältää kaikki tiedot, joita tarvitaan laitteen käynnistymiseksi. Procfs sisältää tietoa kernelistä, kuten tietorakenteet ja prosessit. Laitteen konfigu-

raatiotiedot sijaitsevat sysfs-tietojärjestelmässä. Laitteen väliaikaistiedostot tallennetaan RAM:iin ja tmpfs-tietojärjestelmään, joka on olennaista forensiikan kannalta. Laitteen uudelleen käynnistyessä RAM tyhjentyy, joten tieto on syytä varmuuskopioida tai tutkia ennen sitä.

2.5 Android-forensiikka

Android-laitteita tutkittaessa haastavin osuus ei niinkään ole tietojen palauttaminen tai analysointi, vaan pääsy tietoihin. Järjestelmäpäivitykset tuovat mukanaan uusia tietoturvapäivityksiä, jotka vaikeuttavat entisestään forensiikan tutkijan työtä.

2.5.1 Root

Unix-käyttöjärjestelmissä pääkäyttäjää kutsutaan rootiksi. Rootilla on täydet oikeudet järjestelmään ja sillä voi esimerkiksi poistaa Android-laitteelle asetettuja rajoituksia tai ylikellottaa prosessoria. Forensiikan näkökulmasta root on hyvin tärkeä ominaisuus, sillä rootatusta laitteesta saadaan tutkittua paljon enemmän tietoa kuin roottaamattomasta laitteesta. Android-laitteen roottaus tuo mukanaan haasteita forensiikkaan. Laitteen roottaaminen edellyttää käynnistyslataimen (engl. Bootloader) avaamista, jonka laitevalmistaja on lukinnut estääkseen muunnellun käyttöjärjestelmän asentamisen. Roottaaminen on tietoturvariski, koska käyttöoikeuksien lisääntyminen mahdollistaa myös esimerkiksi haittaohjelmille suuremmat oikeudet, jos tällainen laitteeseen joutuu. Käynnistyslataimen avaaminen palauttaa laitteen tehdasasetuksille ja näin ollen hävittää laitteesta kaiken datan. Monet forensiikkatatoimijat hyödyntävät laitteista löytyviä tietoturva-aukkoja, joiden avulla niihin saadaan root ilman, että laitetta joudutaan tyhjentämään. Avoimilla työkaluilla tämä on hyvin vaikeaa.

Esimerkki Androidin tietoturvahaavoittuvuudesta väliaikaisen rootin saamiseksi on Project Zeron lokakuussa 2019 julkistama use-after-free-haavoittuvuus CVE-2019-2215. Use-after-free-haavoittuvuus mahdollistaa mielivaltaisen koodin suorittamisen laitteesta vapautuneesta muistista. Haavoittuvuus sijaitsee useissa eri valmistajien (kuten Huawei, LG ja Samsung) laitteissa. Haavoittuvuuteen julkaistiin korjauspäivitys viikon sisällä sen julkistamisesta, mutta korjaaminen vaatii tietoturvapäivityksen

asentamisen laitteeseen. Haavoittuvuus mahdollistaa laitteen roottaamisen ilman, että OEM-Unlock:ia tarvitsee kytkeä päälle. Haavoittuvuuden hyödyntäminen edellyttää Androidin tietoturvakerrosten ohittamista, mutta haavoittuvuuden ollessa kernelissä tietoturvakerrokset voidaan melko helposti ohittaa. (Hernandez 2019; CVE-2019-2215.)

2.5.2 Android-laitteista löydettäviä jälkiä

Sovellukset sisältävät paljon luottamuksellista tietoa Android-laitteissa. Sovellukset jakautuvat niin esiasennettuihin, valmistajakohtaisiin, operaattorikohtaisiin kuin käyttäjän asentamiin sovelluksiin. (Skulkin ym. 2019.) Kaikki laitteeseen asennetut sovellukset voidaan nähdä osoitteesta *data/system/packages.xml*.

Laitteista on löydettävissä mm. seuraavia tietoja:

- Puhelulokit
- Teksti- ja multimediaviestit
    - Osittaiset viestit (mmsparts)
- Yhteystiedot
- Selainhistoria
- Sijaintitiedot
- Laitteeseen asennetut sovellukset
- Some-sovellusten tiedot
- Varmuuskopiot
- Kalenteritiedot
- Kuvat ja videot

Android käyttää useita eri osioita (engl. Partition) tiedostojen varastoimiseen. Userdata-osio sisältää forensiikan kannalta tärkeimmät tiedot käyttäjän puhelimella tekemistä toimenpiteistä. Sinne tallentuu tekstiviestit, puhelulokit, yhteystiedot, asennetut sovellukset, sovellusten sisältämät tiedot ja asetukset. Kuviossa 6 on listattu Galaxy S5-puhelimen osiot, joista userdata on osio *mmcblk0p23*. Userdata sijaitsee

/data -hakemistossa ja vaatii root-oikeudet tietojen tarkastelemiseen ja siirtämiseen. /data -hakemistoa kutsutaan laitteen sisäiseksi tallennustilaksi.

```
root@s5neolte:/ # ls -l /dev/block/platform/13540000.dwmmc0/by-name/
lrwxrwxrwx root     root              2019-10-31 13:02 BOOT -> /dev/block/mmcblk0p10
lrwxrwxrwx root     root              2019-10-31 13:02 BOTA0 -> /dev/block/mmcblk0p1
lrwxrwxrwx root     root              2019-10-31 13:02 BOTA1 -> /dev/block/mmcblk0p2
lrwxrwxrwx root     root              2019-10-31 13:02 CACHE -> /dev/block/mmcblk0p21
lrwxrwxrwx root     root              2019-10-31 13:02 CARRIER -> /dev/block/mmcblk0p8
lrwxrwxrwx root     root              2019-10-31 13:02 CDMA-RADIO -> /dev/block/mmcblk0p13
lrwxrwxrwx root     root              2019-10-31 13:02 CPEFS -> /dev/block/mmcblk0p4
lrwxrwxrwx root     root              2019-10-31 13:02 DNT -> /dev/block/mmcblk0p16
lrwxrwxrwx root     root              2019-10-31 13:02 EFS -> /dev/block/mmcblk0p3
lrwxrwxrwx root     root              2019-10-31 13:02 HIDDEN -> /dev/block/mmcblk0p22
lrwxrwxrwx root     root              2019-10-31 13:02 OTA -> /dev/block/mmcblk0p12
lrwxrwxrwx root     root              2019-10-31 13:02 PARAM -> /dev/block/mmcblk0p9
lrwxrwxrwx root     root              2019-10-31 13:02 PERSDATA -> /dev/block/mmcblk0p18
lrwxrwxrwx root     root              2019-10-31 13:02 PERSISTENT -> /dev/block/mmcblk0p17
lrwxrwxrwx root     root              2019-10-31 13:02 RADIO -> /dev/block/mmcblk0p14
lrwxrwxrwx root     root              2019-10-31 13:02 RECOVERY -> /dev/block/mmcblk0p11
lrwxrwxrwx root     root              2019-10-31 13:02 RESERVED2 -> /dev/block/mmcblk0p19
lrwxrwxrwx root     root              2019-10-31 13:02 SYSTEM -> /dev/block/mmcblk0p20
lrwxrwxrwx root     root              2019-10-31 13:02 TOMBSTONES -> /dev/block/mmcblk0p15
lrwxrwxrwx root     root              2019-10-31 13:02 USERDATA -> /dev/block/mmcblk0p23
```

Kuvio 6. Listaus Android-puhelimen osioista

Android-laitteissa on ulkoinen tallennustila, jossa sijaitsee /sdcard -hakemisto. Nimestään huolimatta laitteessa ei välttämättä ole ollenkaan SD-muistikorttia, vaan sille on varattu erillinen kiinteä tallennustila. Hakemistoon tallentuvat laitteen kameralla otetut valokuvat, joten sieltä voi löytyä forensiikan kannalta kiinnostavaa sisältöä. Hakemiston käyttö ei edellytä root-oikeuksia laitteeseen.

SQLite on avoin ja suosittu tietokantaformaatti, jota käytetään monissa mobiililaitteissa jäsenneltyyn tiedon varastoimiseen (Skulkin ym. 2019). Android hyödyntää SQLite-tietokantoja siihen tarkoitetuilla API:lla. Tietokannat sisältävät hyvin paljon forensisesti kiinnostavaa tietoa. Jokaiselle sovellukselle on oma tietokanta, joka sijaitsee polussa */data/sovelluksen_nimi/databases*.

2.5.3 Muistin forensiikka

Android-laitteiden muistin tutkinta on vielä puutteellisesti dokumentoitua ja tästä syystä hyvin haastavaa. Mobiililaitteita ja laitevalmistajia on tuhansia, eivätkä saatavilla olevat työkalut tue läheskään kaikkia laitteita. Tuen puute suurimmalle osalle laitteista johtuu siitä, että työkalut (kuten LiME) pitää kääntää tutkittavan laitteen

kernelin lähdekoodille / konfiguraatiotiedostolle toimivaksi. Lähdekoodia ja konfiguraatiotiedostoa ei ole aina saatavilla. (Liu, Liu, Yang & Zhuge n.d.)

Muistin palauttamiseen työkalut hyödyntävät ladattavia kernel-moduuleja (engl. Loadable kernel module). Työpöytäversioissa tämä onnistuu melko helposti, sillä LKM voidaan kääntää samalla Linux-jakelulla ja kernel-versiolla. Androidille prosessiin ei ole valmiita ohjelmistoja saatavilla, vaan LKM-moduuli pitää kääntää ristiin samalla työkaluketjulla (engl. Toolchain), jota käytettiin tutkittavan laitteen kernelin kääntämiseen. Tämä johtaa helposti yhteensopivuusongelmiin useiden työkaluketjujen ollessa saatavilla. (Broenner, Höfken & Schuba 2016.) Myöskään kalliilla kaupallisilla forensiikkatyökaluilla ei tällä hetkellä ole tukea muistin forensiikalle.

Androidin haihtuvan muistin forensiikka ei ole käytännöllistä monissa tapauksissa, sillä se edellyttää root-oikeuksia laitteeseen ja laitteen roottaamiseksi se on yleensä uudelleenkäynnistettävä. Laitteen uudelleenkäynnistäminen tyhjentää RAM-muistin ja näin ollen sitä ei voida tutkia. Toisaalta, jos tutkittavassa laitteessa on valmiiksi root-oikeudet, RAM-muistista pitäisi tehdä välittömästi levykuva, jos mahdollista. (Skulkin ym. 2019, 155.)

2.5.4 Androidin forensiikkatyökaluja

Taulukossa 1 on listattu Androidin forensiikassa käytettäviä avoimia työkaluja.

Taulukko 1. Androidin avoimia forensiikkatyökaluja

AFLogical OSE
Android SDK
Autopsy & The Sleuth Kit
FTK Imager
Magnet ACQUIRE
Dd
WhatsApp Viewer
LiME
Volatility
AMExtractor

AFLogical OSE on NowSecure:n kehittämä, tietojen palauttamiseen tarkoitettu työkalu, jolla voidaan helposti palauttaa laitteesta puhelulokit, kontaktit ja teksti-, sekä multimediaviestit. Työkalun käyttö ei vaadi root-oikeuksia laitteeseen, mutta USB-vianetsintä pitää olla päällä toimiakseen ja sovellus pitää asentaa myös tutkittavaan laitteeseen ADB:lla. Lisäksi kehittäjän mukaan laitteessa tulee olla erillinen SD-kortti, jolle tiedot siirretään ja sitä kautta kopioidaan työasemaan. Työkalu hyödyntää sisällöntarjoajia (engl. Content provider), joita käytetään tietojen jakamiseen eri sovellusten välillä. Tästä sijainnista sovellukset pääsevät käsiksi dataan. Ohjelmistosta on olemassa paremmin varusteltu versio AFLogical LE, jolla voidaan palauttaa kaikki looginen data. Kehittäjä tarjoaa LE-versiota ilmaiseksi viranomaiskäyttöön.

Android SDK on kokoelma kehitystyökaluja Android-sovelluskehitykseen. Lisäksi se on välttämätön forensiikan kannalta, sillä sen avulla voidaan kommunikoida laitteen ja työaseman välillä:

- apkanalyzer:llä voidaan tarkastella APK-tiedostoja. Sillä voidaan esimerkiksi nähdä sovelluksen ID, versiokoodi, versionimi, tarkastella manifestitiedoston sisältöä, DEX-tiedostoja, kuvia, sekä merkkijonoja.
- ADB on SDK:n mukana tuleva komentorivityökalu, jolla pystytään ohjaamaan ja hallinnoimaan Android-laitetta. ADB:tä käytetään sovelluskehityksessä mm. vikojen etsimiseen (debugging). Forensiikan näkökulmasta hyöty on se, että sillä voi kopioida tiedostoja tutkittavasta laitteesta ja tutkijalla on käytettävänään komentokehote. Tutkittavalla laitteella täytyy olla kytkettynä päälle USB-vianetsintä tutkittavan laitteen asetuksista, jotta ADB:tä voidaan käyttää. ADB:llä voidaan siirtää tiedostoja tietokoneelle *pull*-komennolla.
    - ADB dumpsys:llä voidaan tarkastella eri prosessien ja palveluiden tilaa. Sillä voidaan esimerkiksi nähdä, milloin milläkin Google-käyttäjällä on kirjauduttu laitteeseen (jos käytössä useampi käyttäjä) ja mihin WIFI-verkkoihin laitteella on kirjauduttu. Lisäksi sen avulla näkee, milloin jokin sovellus on käyttänyt oikeuksia, joihin sillä on sallittu pääsy.
    - ADB:llä voidaan luoda sovellusten tiedoista varmuuskopiot suoraan työasemalle ADB:n yli. Nämä varmuuskopiot eivät sisällä chat-sovellusten tietoja eivätkä Googlen sovellusten tietoja.

Dd-komennolla voidaan tehdä kopio koko järjestelmästä, eli käytännössä se on tietojen fyysistä palauttamista (palauttaen myös poistetut tiedostot). Dd löytyy Linuxista ja Androidista natiivina.

The Sleuth Kit (TSK) on kokoelma erilaisia komentorivityökaluja, joita käytetään levykuvien analysointiin. Sen avulla voidaan analysoida volyymien ja tietojärjestelmien dataa. Autopsy on graafinen käyttöliittymä TSK:hon. Autopsyä käyttävät eri armeijat, viranomaiset kuin yksityiset tutkijatkin.

FTK Imager on AccessDatan kehittämä työkalu, jolla on mahdollista sekä palauttaa, että analysoida aineistoa. Sillä voidaan luoda identtinen kopio tutkittavasta laitteesta forensisen eheyden ja luotettavuuden säilyttämiseksi.

Magnet Acquire on Magnet Forensics:n kehittämä ohjelmisto levykuvien tekemiseen iOS- tai Android-laitteesta. Se on saatavilla ilmaiseksi forensiikan ammattilaisten tai

viranomaisten käyttöön hakemuksen täyttämällä, joskaan opiskelijat eivät voi hakea ohjelmistoa itsenäisesti. Acquire:lla on mahdollista tehdä molemmille käyttöjärjestelmille looginen palautus ja Androidille lisäksi fyysinen palautus. Ohjelmassa on sisäänrakennettuja exploitteja käyttöoikeuksien eskalointiin (engl. Privilege escalation), joiden avulla laitteelle saadaan root-oikeudet, mutta on täysin laitekohtaista, toimiiko se. Laitteelle, jolla on jo root-oikeudet, saadaan helposti tehtyä fyysinen palautus. (How to Image a Smartphone with Magnet ACQUIRE 2019.)

WhatsApp Viewer on työkalu, jolla voidaan purkaa WhatsAppin varmuuskopioiden salaus sillä edellytyksellä, että käyttäjällä on hallussaan salausavain. Avain sijaitsee laitteessa osoitteessa */data/data/com.whatsapp/files/key* ja pääsyyn vaaditaan root-oikeudet laitteeseen.

Linux Memory Extractor (LiME) on Joe Sylven vuonna 2012 julkaisema LKM-työkalu, jolla voidaan palauttaa haihtuva RAM-muisti Linux-pohjaisista laitteista. Se pyrkii minimaaliseen vuorovaikutukseen käyttäjän ja kernelin välillä, jotta laitteesta haltuun otettu muisti on forensisesti luotettavaa. (Spreitzenbarth & Uhrmann 2016, 141.) LiMEn käytettävyys on rajallista, sillä sen käyttöön vaaditaan tutkittavan laitteen kernelin lähdekoodi ja kernelin konfiguraatiotiedosto. Laitevalmistajat julkaisevat lähdekoodeja ladattavaksi Internetistä, mutta läheskään kaikille laitteille sitä ei ole saatavilla ja LiMEä ei silloin voida käyttää.

2.6 iOS

2.6.1 Yleistä

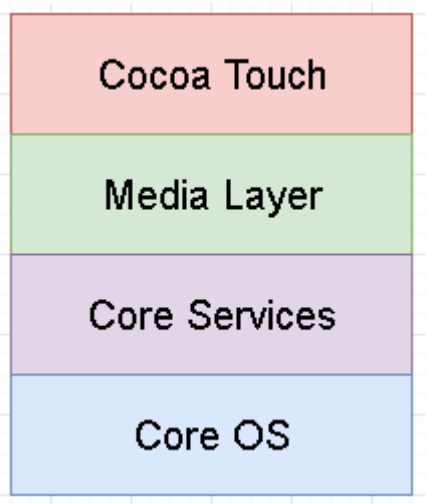
iOS on Applen kehittämä käyttöjärjestelmä. Se oli aluksi nimeltään iPhone OS, mutta muutettiin myöhemmin iOS:ksi kuvastamaan paremmin universaalia käyttöjärjestelmää Applen laitteissa (Bommisetty ym. 2018). iOS julkaistiin samaan aikaan kuin ensimmäinen iPhone, kesäkuussa 2007. iOS 13 julkaistiin 19. syyskuuta 2019.

iOS pohjautuu macOS X:ään, mutta siinä on muutamia merkittäviä eroavaisuuksia:

- Arkkitehtuuri on ARM-pohjainen Intel x86_64:n sijaan

- Mac OS X:n kernel perustuu avoimeen lähdekoodiin, iOS on suljettu
- Muistin hallinnointi on tiukempaa
- Järjestelmä on kovennettu eikä se salli pääsyä alla oleviin ohjelmointirajapintoihin (API) (Bommisetty ym. 2018.)

iOS koostuu neljästä abstraktiokerroksesta (Ks kuvio 7). Tämä mahdollistaa sovellusten kehittämisen eri valmiuksilla varustetuille laitteille.



Kuvio 7. iOSn arkkitehtuurin kerrokset

Cocoa Touch sisältää tarvittavat ohjelmistokehykset sovellusten visuaalisten käyttöliittymien kehittämiseen. Lisäksi se mahdollistaa käyttöjärjestelmän moniajon, ydinanimaation (engl. Core animation) ja kosketusnäytön käyttämisen. (Epifani & Stirparo 2016, 44.)

Media Layer koostuu grafiikka-, ääni- ja video-ohjelmistokehyksistä, jotka mahdollistavat laitteen multimediaominaisuudet (Bommisetty ym. 2018).

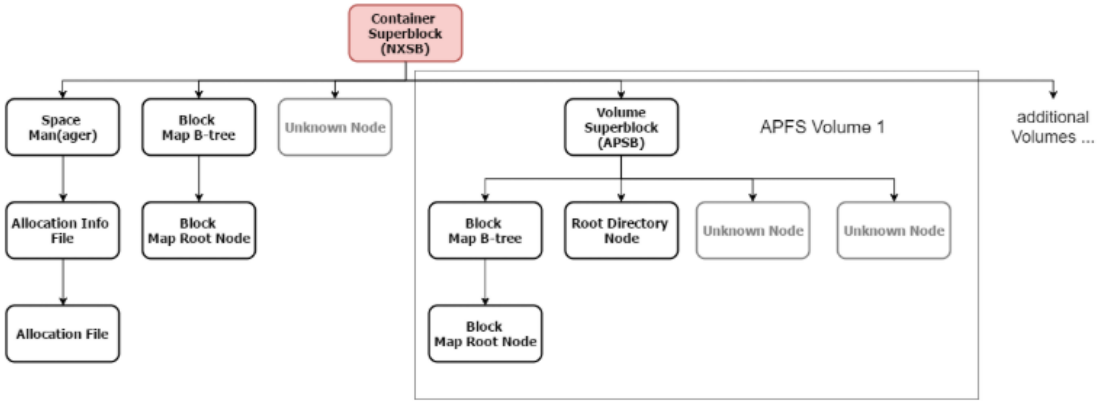
Core Services tarjoaa sovelluksille välttämättömät järjestelmäpalvelut, kuten sijainnin, SQLite-tietokannat, iCloud-pilvipalvelun ja sosiaalisen median ominaisuudet (Bommisetty ym. 2018).

Core OS rakentuu matalan tason välttämättömistä toiminnallisuuksista, kuten tietojärjestelmä, muistinhallinta, tietoturva, virranhallinta, verkotus ja kryptaus (Epifani ym. 2016, 44).

2.6.2 Tietojärjestelmät

APFS

APFS on Applen uusin tietojärjestelmä, joka julkaistiin vuonna 2017. Se korvasi vanhemman, yli 20vuotta sitten julkaistun HFS+ -tietojärjestelmän. APFS tuli käyttöön iOS:n versiosta 10.3 ja macOS:n versiosta 10.12.4 alkaen. APFS:stä on tehty Applelle universaali tietojärjestelmä, ja se pystyy korvaamaan kaikki aiemmat Applen laitteissa käytössä olevat tietojärjestelmät. APFS on jäsennelty yhteen konttiin (container), joka voi sisältää useampia volyymejä. Kuviossa 8 on kuvailtu APFS:n rakenne.



Kuvio 8. APFS:n rakenne (Plum 2017)

Rakenteen elementit alkavat 32-bittisellä otsakelohkolla (engl. block header), joka alkaa Fletcherin algoritmia käyttävällä tarkistussummalla ja sisältää myös lohkon ID:n ja lohkotyypin (Plum 2017.) Lisäksi otsakelohko sisältää copy-on-write -version lohkosta; jokainen lohko kopioidaan ennen kuin muutoksia tehdään säästäen edellisen version lohkosta. Näin ollen forensiikkaa tutkiessa voi löytyä kiinnostavia jälkiä (engl. artifact), sillä vanhoja lohkoja ei päällekirjoiteta. (Plum 2017.)

Kontin superlohko (superblock), sisältää tietoa lohkon koosta, lohkojen lukumäärästä, osoittimen tilanhallintaan (engl. space manager), kaikkien volyymien lohkojen ID ja lisäksi osoittimen B-puuhun (engl. B-tree), jossa on merkittynä jokaisen volyymin ID sekä offset. B-puu hallinnoi useita solmuja, ja ne sisältävät juurisolmun offsetin. Offsetillä tarkoitetaan etäisyyttä kahden pisteen tai elementin välillä. Solmuja (engl. node) käytetään varastoimaan erilaisia kohtia muistissa (engl. entry). Ne voivat olla osa B-puuta tai itsenäisiä. Solmut voivat sisältää vakiokokoisia tai joustavia kohtia. (Plum 2017.)

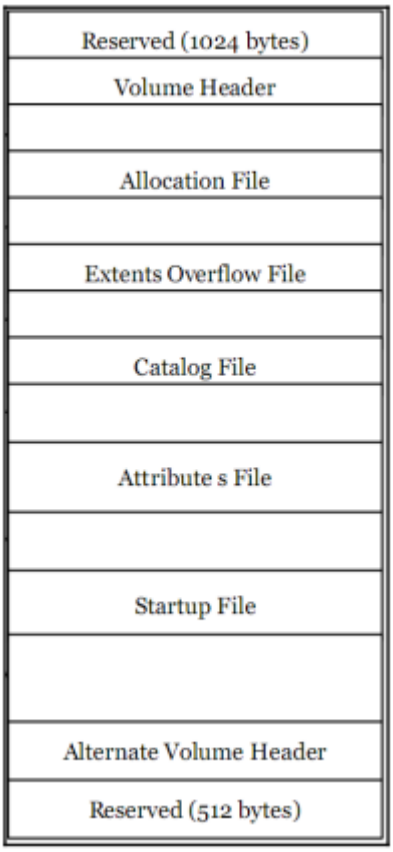
Tilanhallintaa käytetään hallinnoimaan allokoituja lohkoja kontin sisällä. Lisäksi se varastoi vapaiden lohkojen lukumäärän ja osoittimen allokaation infotiedostoon. Allokaation infotiedosto itsessään sisältää allokaatiotiedoston pituuden, version ja offsetin. (Plum 2017.)

Volyymin superlohko sisältää volyymin nimen, ID:n ja aikaleiman. Viimeisimpänä tietojärjestelmän rakenteessa ovat allokaatiotiedostot, jotka ovat yksinkertaisia bittikarttoja, eikä niillä ole ollenkaan otsaketta tai tyyppi-ID:tä. (Plum 2017.)

HFS+

HFS+ -tietojärjestelmä julkaistiin vuonna 1998 vanhemman HFS-tietojärjestelmän korvaajaksi. Se mahdollistaa 32-bittisten lohkojen osoitteet 16-bittisten sijaan ja tietojärjestelmän objektien nimeämiseen käytetään Unicodea (maksimissaan 255 merkin pituiset nimet) (Epifani & Stirparo 2016, 51). Tietojärjestelmästä on myös olemassa päivitetty versio HFSX, joka mahdollistaa merkkikokoriippuvaiset tiedostonimet.

HFS+ -tietojärjestelmän volyymit koostuvat kuudesta merkittävästä tietorakenteesta, jotka sisältävät tarvittavat tiedot datan hallinnoimiseen. (Ks kuvio 9.)



Kuvio 9. HFS+ volyymin tietorakenne (Epifani & Stirparo 2016)

- Reserved (1024 bytes): Tavut on varattu käynnistämiseen tarkoitetulle tiedolle.
- Volume header määrittelee volyymin perusrakenteen, allokaatioblokkien koon ja käytettyjen sekä käyttämättömien blokkien lukumäärän.
- Allocation file sisältää bittikartan käytetyistä ja käyttämättömistä blokeista volyymin sisällä.
- Extents Overflow tallentaa blokit, jotka otetaan käyttöön tiedoston käyttäessä enemmän kuin kahdeksan blokkia
- Catalog file määrittelee tietojärjestelmän kansioiden rakenteen ja sitä käytetään jonkin tietyn kansion tai tiedoston sijainnin tunnistamiseen
- Attribute file sisältää tiedoston muokattavat attribuutit.
- Startup file sisältää tiedot, jotka tarvitaan järjestelmän käynnistämiseen
- Alternate Volume header on volume headerin varmuuskopio, jota käytetään levyn korjaamiseen vikatilanteissa

- Reserved (512 bytes): Varatut tavut, joita käytetään laitteen valmistusvaiheessa (Epifani & Stirparo 2016, 51.)

2.7 iOS-forensiikka

2.7.1 Yleistä

iOS-laitteet sisältävät kaksi loogista osiota, joista toinen varastoi käyttöjärjestelmän käynnistämiseen tarvittavat tiedostot kuten kernel levykuvat ja konfiguraatiotiedostot. Toista osioita käytetään käyttäjäkohtaisten asetusten ja sovellusten, kuten kuvien, videoiden ja kontaktien varastoimiseen. Forensiikan näkökulmasta jälkimmäinen osio on kiinnostava, sillä se sisältää kaikki käyttäjän laitteella tekemät toimenpiteet ja niistä syntyvän datan. (Reddy 2019.)

2.7.2 Jailbreak

iOS:n jailbreakilla tarkoitetaan iOS-laitteiden rajoitteiden poistamista. Se mahdollistaa pääkäyttäjän oikeudet laitteeseen, sovellusten, laajennusten ja teemojen asentamisen App Storen ulkopuolelta. Jailbreakia ei luokitella forensisesti luotettavaksi toimenpiteeksi, koska se muuttaa laitteen tilaa. Se on kuitenkin välttämätönä fyysisen levykuvan saamiseksi tutkittavasta laitteesta. (Reddy 2019, 228.)

Uusissa iPhoneissa jailbreak edellyttää laitteen pääsykoodia, joka tutkijan täytyy tietää. Vaihtoehtoisesti pääsykoodin voi yrittää murtaa kolmannen osapuolen forensiikkatoimija, joskaan sen onnistumisesta ei ole varmuutta. (Epifani & Stirparo 2016, 59.)

2.7.3 iOS:n avoimia forensiikkatyökaluja

iOS:lle on niukasti avoimia työkaluja saatavilla. Ilmaistyökaluilla työskentely on hyvin haasteellista käyttöjärjestelmän ollessa sekä tietoturvallinen, että suljettu.

Libimobiledevice on alustariippumaton kirjasto, joka mahdollistaa kommunikoinnin tietokoneen ja iOS-laitteen tietojärjestelmän välillä. Sillä voidaan esimerkiksi palauttaa tiedostoja, varmuuskopioita sekä tietoa laitteesta. Sovelluksen käyttö ei edellytä jailbreakia laitteeseen. (Libimobiledevice n.d.)

IBackupBot on iTunes-varmuuskopioiden hallinnoimiseen tarkoitettu ohjelmisto. Sillä voidaan analysoida tarkastella iTunesissa sijaitsevia tietokantoja, kuvia, tekstiviestiä, muistiinpanoja, kontakteja sekä puhelulokeja. IBackupBot on Windows-pohjainen sovellus, joten se on yhteensopiva useimpien tutkintatyöasemien kanssa.

3 Tutkimusasetelma

3.1 Tutkimuskysymykset

- Mikä on mobiiliforensiikan tämänhetkinen tilanne?
- Mitä erilaisia avoimia työkaluja on käytettävissä?
- Mitä tutkittavia jälkiä laitteista löytyy?
- Mitä haasteita esiintyy mobiiliforensiikassa?

3.2 Tutkimusmenetelmät

Opinnäytetyön tutkimuskysymyksiin vastataan hyödyntämällä tutkimusotteena laadullista tutkimusta. Kanasen (2015, 70) mukaan laadullinen tutkimus pyrkii ymmärtämään jotakin ilmiötä. Valinnan perusteena on se, että ilmiö on melko uusi, josta on niukasti aikaisempaa tietoa ja tutkimusta, sekä siitä halutaan saada syvempi ymmärrys.

3.3 Tutkimuksen luotettavuus

Opinnäytetyön teoriaosuus perustuu forensiikkaan ja kyberturvallisuuteen liittyvään kirjallisuuteen, aihealueen tunnettujen ja merkittävien ammattilaisten tekemiin julkaisuihin ja vertaisarvioituihin tutkimuksiin, blogikirjoituksiin, sekä muihin luotettavien ja virallisten tahojen tekemiin julkaisuihin (kuten NIST, IEEE ja SANS).

Opinnäytetyössä käytettävät työkalut ja ohjelmistot valitaan sen perusteella, miten luotettavia ja suosittuja ne ovat olleet aiemmissa tutkimuksissa, sekä miten hyvin niitä tuetaan ja kehitetään. Tutkimus toteutetaan avoimilla forensiikkatyökaluilla, eikä käytössä ole kaupallisia työkaluja. Tämä mahdollisesti rajoittaa kykyä tutkia laitteita. Androidin forensiikan tutkinta tapahtuu fyysisille laitteille virtuaalilaitteen sijaan todenmukaisemman kuvan saamiseksi. Tutkimuksessa vertaillaan forensiikkatyökalujen ominaisuuksia rootattujen ja roottaamattomien laitteiden avulla.

4 Android-testilaitteiden tutkinta

4.1 Forensiikkaympäristön implementointi

Tutkintaympäristön tulee olla steriili ja luotettava. Ainoastaan tutkinnassa tarvittavien ohjelmistojen ja työkalujen asentaminen varmistaa sen, että tiedot pysyvät eheinä ja forensisesti luotettavina.

Forensiikkatyöasemat pystytettiin VirtualBox-ympäristöön virtuaalikoneina. Työssä käytettiin sekä Linux, että Windows-työasemia. Osa työssä käytetyistä ohjelmistoista on tuettu ainoastaan toisella käyttöjärjestelmällä tai ominaisuudet ovat puutteellisia, joten erilliset työasemat vaadittiin molemmilla käyttöjärjestelmillä varustettuina. Linux-työasemana käytettiin Ubuntuun pohjautuvaa Santoku-Linuxia. Santoku on NowSecure-nimisen yrityksen kehittämä mobiililaitteiden forensiikkaan ja tietoturvatestaukseen tarkoitettu Linux-versio. Santokusta löytyy esiasennettuina useimpien mobiililaitteiden USB-ajurit, lukuisia avoimia forensiikkatyökaluja, sekä joidenkin kaupallisten forensiikkatyökalujen kokeiluversioita. Käytännössä monet hyödylliset työkalut on koottu yhteen Linux-jakeluun.

Windows-työasemaan asennettiin Windows 10 versio 1809. Tällä työasemalla suoritettiin laitteista palautettujen tiedostojen analysointia johtuen siitä, että Autopsyn käyttöönotto Linuxissa vaatii monimutkaisia toimenpiteitä, eikä FTK Imager ole tuettu Linuxissa ollenkaan. Näiden ohjelmistojen lisäksi työasemaan asennettiin ADB.

Työssä hyödynnettiin kolmea eri testilaitetta forensiikan tutkimiseen. Testilaitteet on esitelty taulukossa 2.

Taulukko 2. Käytetyt testilaitteet

Nimi	**Laitetyyppi**	**Android-versio**
OnePlus 3T	Älypuhelin	9.0.5
Samsung Galaxy S5 Neo	Älypuhelin	6.0.1
Lenovo TB-8704F	Tabletti	7.1.2

Testilaitteista Lenovo ja Samsung on valmiiksi rootattu. Näin ollen tutkittavista laitteista saatavan tiedon määrää pystytään helposti vertailemaan rootatun ja roottaamattoman laitteen välillä. Laitteisiin on luotu testidataa tutkimusta varten.

4.2 Työn toteutuksen vaiheet

Käytännön osuudessa tutkittiin Androidin forensiikkaa käyttäen testilaitteina tablettia, sekä kahta älypuhelinta. Työn aluksi esiteltiin forensiikkaympäristö ja testilaitteet, jonka jälkeen testilaitteista palautettiin erinäisiä tiedostoja sekä levykuvia niihin tarkoitetuilla työkaluilla. Palautettuja tiedostoja analysoitiin saatavilla olevilla analysointityökaluilla.

4.3 Tietojen palauttaminen tutkittavista laitteista

4.3.1 Fyysinen levykuva

Koko laitteesta on mahdollista luoda fyysinen kopio (blokki mmcblk0), tai vaihtoehtoisesti yksittäisestä osiosta. Valtaosa forensiikan kannalta kiinnostavasta datasta löytyy userdata-osiosta. S5:n userdata-osiosta (mmcblk0p23) luotiin kopio käyttäen dd:tä. Lisäksi puhelimeen asennettiin BusyBox, joka on kokoelma Unix-apuohjelmien

pienempiä versioita. BusyBoxin mukana tulee Netcat-työkalu, joka tarvitaan tunnelin muodostamiseksi laitteen ja tutkintatyöaseman välille kopioitavan osion siirtämiseksi. Netcat on vakiona mukana Linuxissa. Osion kopiointi työasemalle tapahtuu kuviossa 10 ohjaamalla puhelimesta tuleva data portin 8888 (vaihtoehtoisesti voi käyttää mitä tahansa porttia väliltä 1023-65535) kautta tiedostoon S5userdata.dd. dd:n siirtonopeus käytetyllä virtuaalikoneella oli hyvin hidasta. 12 gigatavun kokoisen osion siirtämisessä kesti n. 5 tuntia.

```
santoku@santoku-VirtualBox:~/forensics$ adb forward tcp:8888 tcp:8888
santoku@santoku-VirtualBox:~/forensics$ nc 127.0.0.1 8888 > S5userdata.dd
root@s5neolte:/ # dd if=/dev/block/mmcblk0p23 | busybox nc -l -p 8888
```

Kuvio 10. Userdata-osion palauttaminen laitteesta

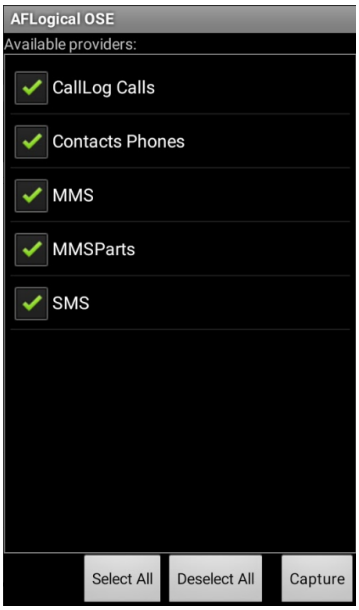
Myös Windows-työasemalla yritettiin tehdä fyysistä palauttamista, mutta dd-komennon suorittaminen ei missään vaiheessa päättynyt luotuaan levykuvan. Komento pysäytettiin manuaalisesti, mutta kumpikaan analysointityökaluista (FTK Imager tai Autopsy) ei kyennyt avaamaan levykuvaa ja ilmoitti sen olevan korruptoitunut. Tämän epäiltiin johtuvan Windowsin ncat-sovelluksesta, joka on korvaava työkalu Netcat:lle. Ncat ei aina toimi odotetulla tavalla, koska se ei ole Windowsin natiivisovellus (Lohrum 2017).

4.3.2 Loogiset tiedostot

Testilaitteesta OnePlus 3T palautettiin loogiset tiedostot käyttämällä AFLogical OSE-työkalua. Laitteessa ei ollut käytössä erillistä SD-muistikorttia, vaikka AFLogical OSE:n dokumentaatiossa muistikortti vaaditaan tietojen palauttamiseksi. Siitä huolimatta tiedostoja kokeiltiin palauttaa ja ne onnistuttiinkin siirtämään testilaitteesta työasemaan. Muistikorttia käytettäessä OSE siirtäisi tiedostot aluksi muistikortille, jonka jälkeen ne siirrettäisiin manuaalisesti tutkintatyöasemalle.

Kun palauttaminen käynnistettiin työasemalta, OSE asentui automaattisesti tutkittavaan laitteeseen ja siihen saatiin käyttöliittymä. Uusien sovellusten asentaminen tut-

kittavaan laitteeseen kuitenkin muuttaa laitteen tilaa ja muutokset on dokumentoitava forensisen eheyden säilymisen kannalta. Kuviossa 11 on OSE:n käyttöliittymä testilaitteen OnePlus 3T näytöllä ja lista tiedostoista, joita oli mahdollista siirtää tutkintatyöasemaan (puhelulokit, yhteystiedot, multimediaviestit ja tekstiviestit).



Kuvio 11. AFLogical OSE -tallennus

AFLogical OSE:n avulla palautettiin myös samat tiedot Galaxy S5-puhelimesta, joka oli rootattu. Laitteesta ei kuitenkaan pystynyt palauttamaan enempää tietoa, sillä tiedostojen sijainti ja palauttaminen ei edellyttänyt roottia laitteeseen eikä näin ollen hyödyttänyt lisätiedon saamisessa.

OnePlus 3T-puhelimesta palautettiin lisäksi ulkoinen tallennustila kuvion 12 mukaisesti.

```
santoku@santoku-VirtualBox:~/forensics$ adb pull /sdcard/
pull: building file list...
```

Kuvio 12. 3T:n ulkoisen tallennustilan looginen palautus

TB-8704F -tabletin /data -hakemistolle suoritettiin looginen palautus BusyBoxia ja Netcattia hyödyntäen. Data ohjattiin portin 8888 kautta forensiikkatyöasemaan (Ks.

Kuvio 13). Kuten fyysisessäkin palautuksessa S5:lle, Windowsin työkalu ncat ei toiminut tässäkään tapauksessa, vaan Linuxilla palautetut tiedostot siirrettiin manuaalisesti Windows-työasemaan analysoitavaksi Autopsyllä ja FTK Imagerilla.

```
 TB8704:/ # busybox tar -cvz /data | busybox nc -l -p 8888
forensics$ adb forward tcp:8888 tcp:8888
forensics$ nc 127.0.0.1 8888 > data.tar.gz
```

Kuvio 13. Lenovo TB-8704F -tabletin /data -hakemiston looginen palautus

4.4 Fyysisesti palautettujen tietojen analysointi

Autopsy

S5-puhelimen levykuva ladattiin Windows-työasemalla Autopsyyn tutkittavaksi. Autopsyssä on valittavana erilaisia moduuleja, jotka etsivät tietyntyyppisiä tiedostoja lähdetiedostosta. Tärkeimpänä Android Analyzer -moduuli, joka mahdollista tekstiviestien, puhelulokien yhteystietojen ja sijaintitietojen palauttamisen laitteesta. Autopsyllä nähdään lisäksi levykuvalla sijaitsevan osion tietorakenne, josta löytyy kaikki palautetut tiedot.

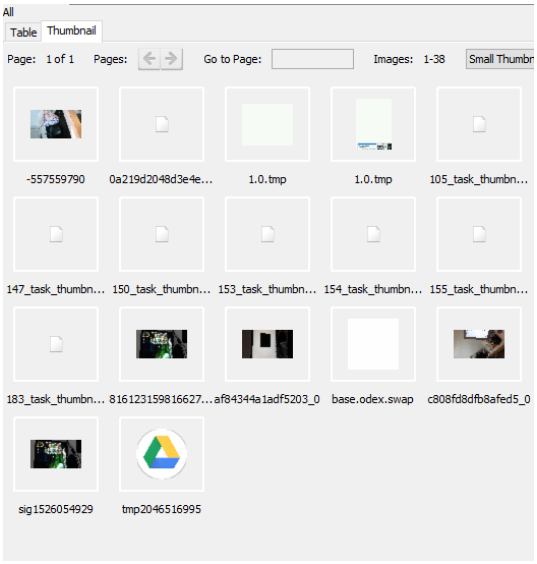
Jokaisesta yksittäisestä tiedostosta on olemassa yhteensä neljä eri aikaleimaa, joiden avulla pystytään näkemään, kun tiedoston tila on jollain tapaa muuttunut (Ks. Kuvio 14).

Modified	2019-11-03 02:22:53 EET
Accessed	2019-11-03 02:22:53 EET
Created	2019-11-03 02:22:53 EET
Changed	2019-11-03 02:22:53 EET

Kuvio 14. Tiedoston aikaleimat

4.4.1 Poistetut tiedostot

Autopsy suodattaa laitteesta poistetut tiedostot helposti tarkasteltaviksi. Kuviossa 15 on laitteesta poistetut kuvat. Listauksesta löytyi Googlen stock-kuvia, sekä Galaxy S5:n kameralla otettuja kuvia. Monet kuvat olivat vaihtaneet tiedostopäätettä (.cnt tai .0), mutta Autopsyn tiedostopääte-moduuli osasi korjata tiedostopäätteet oikeiksi.



Kuvio 15. S5-puhelimesta poistetut kuvat

Jokaista tiedostoa voi tarkastella heksadesimaalimuodossa ja tiedoston otsake (engl. Header) kertoo oikean tiedostotyypin. Esimerkiksi JPG-tiedostot alkavat *ff D8 ff* -otsakkeella (Ks. Kuvio 16) Tämän perusteella voidaan selvittää oikea tiedostopääte, vaikka tiedostopäätettä yritettäisiin vaihtaa hämäystoimenpiteenä.

```
0x00000000: FF D8 FF E1  2D B8 45 78   69 66 00 00  49 49 2A 00    ....-.Exif..II*.
0x00000010: 08 00 00 00  0D 00 00 01   04 00 01 00  00 00 00 12    ................
```

Kuvio 16. Heksadesimaalituloste JPG-tiedostosta

4.4.2 Sovellukset

Testilaitteisiin asennetuista sovelluksista ja applikaatioista tutkittiin, mitä forensiikan kannalta hyödyllistä tietoa niistä voidaan löytää. Työssä tutkitut sovellukset ovat listattuina taulukossa 3.

Taulukko 3. Tutkittavat sovellukset

Facebook / Facebook Messenger
Tekstiviestit, puhelulokit, yhteys-tiedot
WhatsApp
Wifi
Gmail

Facebook

Facebook varastoi tietoa kahteen eri hakemistoon, jotka ovat */data/com.facebook.katana* (Facebook -sovellus) ja */data/com.facebook.orca* (Facebookin Messenger -sovellus). S5-puhelimen fyysisestä levykuvasta tutkittiin Autopsyllä Facebookin SQLite -tietokantoja. Kuviossa 17 on näkymä tietokannasta *contacts_db2*, jossa on listattuna laitteelle liitetyn Facebook -käyttäjän kaikki kontaktit (Facebook-kaverit ja henkilöt, joille on viestitelty). Taulukon ylimmäisellä rivillä ovat käyttäjän omat tiedot. Taulukossa 4 on selitteet tietokannan sarakkeille.

contact_id	fbid	first_name	last_name	display_...	small_pic...	big_pictu...	huge_pic...	communi...	is_messe...	messeng...	added_ti...	is_on_vi...	data	bday_day	bday_mo...
Y29udGFj...	1	[redacted]			https://sc...	https://sc...	https://sc...	0.0	true	14156260...	0	true	{"contactI...	27	8
Y29udGFj...	1				https://sc...	https://sc...	https://sc...	0.0	false	0		true	{"contactI...	0	0
Y29udGFj...	1				https://sc...	https://sc...	https://sc...	0.002000...	true	14157150...		true	{"contactI...	28	4
Y29udGFj...	1				https://sc...	https://sc...	https://sc...	0.002000...	true	15062068...		true	{"contactI...	0	0

Kuvio 17. Facebookin Contacts -taulukko

Taulukko 4. Contacts -tietokannan kenttien nimet ja selitykset

First_name	Kontaktin etunimi
Last_name	Kontaktin sukunimi
Small / big / huge_picture_url	Kontaktin profiilikuvan osoite ja kuva kolmessa eri koossa.
Communication_rank	Arvo, joka kertoo, kuinka paljon käyttäjä on kommunikoinut jonkun kontaktin kanssa. Viestit, julkaisut, tykkäykset ja kommentit kasvattavat tätä arvoa.
Is_messenger_user	Totuusmuuttuja, joka kertoo käyttääkö kontakti Messenger -sovellusta
Messenger_install_time_ms	Tarkka kellonaika epoch -muodossa, jolloin kontakti on asentanut Messenger -sovelluksen
Added_time_ms	Tarkka aika epoch -muodossa, jolloin kontakti on lisätty.
B_day / _month	Kontaktin syntymäpäivä ja -kuukausi
Data	Kaikki aiempien kenttien tiedot löytyvät tästä kentästä. Lisäksi täällä näkyvät kontaktin puhelinnumero ja kotiosoite, jos tämä on asettanut ne näkyville profiilissaan.

Hakemistosta löydettiin kolme muutakin oleellista tietokantaa ja hakemisto välimuistissa sijaitseville kuville:

- savedvideos.db
    - Käyttäjän facebookista tallentamat videot
- newsfeed.db
    - Käyttäjän Facebook-syöte

- notifications.db.
    - Sovelluksen lähettämät ilmoitukset käyttäjälle
- /cache/images
    - Sisältää kuvia käyttäjän syötteestä sekä kontakteista

Messengerin hakemistosta löytyi tietokanta *threads_db2*, josta näkee *messages* -taulukosta käyttäjän keskustelut (Keskustelut oli mahdollista nähdä testitapauksessa vuoteen 2012 saakka). Taulukosta on nähtävissä viestin sisältö, lähettäjä, vastaanottaja, kellonaika epoch-muodossa sekä mahdolliset liitteet. Kuviossa 18 on näkymä *threads_db2* -tietokannasta ja käyttäjän viesteistä. Lisäksi tietokannassa on sarake *coordinates*, josta pitäisi nähdä viestin lähettäneen laitteen tarkat koordinaatit, mutta tätä ei saatu toimimaan. Tämä mahdollisesti aiheutui Facebookin asettamista tietoturva-asetuksista.

msg_id	thread_key	text	sender	times...
mid.$oAAB...	ONE_TO_ONE:1292...	moro ooot...	{"user_key":"FACEBOOK:1[redacted]","name":"[redacted]","email":null,"phone":null,"smsParticipantFbid":null,"is...	13388281...
mid.$oAAB...	ONE_TO_ONE:1292...	juuh	{"user_key":"FACEBOOK:1[redacted]90969","name":"[redacted]","email":null,"phone":null,"smsParticipantFbi...	13388282...

Kuvio 18. Messages -taulukko

Yhteystiedot ja puhelulokit

Käyttäjän yhteystiedot ja puhelulokit sijaitsevat hakemistossa com.android.providers.contacts /databases/-kansion alla contacts2.db ja calllog.db-tietokannoissa.

Tekstiviestit

Tekstiviestejä tutkittiin hakemistosta com.android.providers telephony:

- /files
- databases/
    - Mmssms.db
    - Telephony.db

Kuviossa 19 on laitteessa sijaitsevat tekstiviestit tietokannassa mmssms.db, josta nähdään viesteihin liitetyt puhelinnumerot, aikaleima epoch-muodossa, sekä viestin sisältö. Huomattavaa puhelinnumerokentässä on se, että siitä ei tiedä onko kyseinen numero viestin lähettäjä vai vastaanottaja.

_id	thread_id	address	person	date	date_sent	protocol	read	status	type	reply_pa...	subject	body
2	1	474831		1572472327027	0		1	-1	5			Hidden message \ud83...
3	2	7383819		1572472354936	0		1	-1	5			I have the goods
4	3	956481849		1572517415514	0		1	-1	5			Package delivered
5	4	0504356050		1573040411079	0		1	-1	2			Testiviesti
6	4	0504356050		1573040435947	0		1	-1	2			Baeb

Kuvio 19. SQLite-tietokannan tuloste tekstiviesteistä

Telephony.db-tietokannassa oli kenttä siminfo, josta pystyttiin näkemään laitteessa olleet SIM-kortit ja niiden operaattorit (Ks. Kuvio 20).

_id	icc_id	sim_id	display_...	carrier_n...	name_so...	color	number	display_...	data_roa...	mcc	mnc
1	[redacted]	0	Telia FI	Telia FI	0	-16746133		1	0	244	91

Kuvio 20. Telephony.db-tietokannan SIM-korttitiedot

Whatsapp

Whatsapp varastoi tietoa sekä sisäiseen, että ulkoiseen muistiin. Ulkoiselle muistille Whatsapp tallentaa mediatiedostot, sekä varmuuskopiot. Sisäiselle tallentuu kaikki muu tieto (mm. keskustelut ja yhteystiedot).

Sovelluksesta tutkittiin seuraavia hakemistoja, tietokantoja ja tiedostoja:

- /files/
    - Avatars
- /shared_prefs/
    - Registration.RegisterPhone.xml
    - Registration.VerifySMS.xml
- /databases/
    - Msgstore.db

    - Wa.db
- /sdcard/WhatsApp/
    - Media
    - Databases

Avatars -kansiosta löydettiin kaikkien käyttäjän yhteystietojen profiilikuvat, sekä puhelinnumerot. Lisäksi /files -hakemistossa oli *me* -niminen tiedosto, joka sisälsi käyttäjän Whatsapp-tiliin liitetyn puhelinnumeron.

/shared_prefs/-hakemistosta löydetyistä kahdesta XML-tiedostoista voitiin nähdä Whatsapp-tiliin rekisteröity puhelinnumero, suuntanumero, sekä rekisteröitymisen tarkka kellonaika epoch-muodossa (Ks. Kuvio 21).

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <long name="com.whatsapp.registration.VerifySms.call_countdown_end_time" value="1573583316399" />
    <int name="com.whatsapp.registration.VerifySms.verification_state" value="0" />
    <long name="com.whatsapp.registration.VerifySms.sms_request_failed_retry_time" value="1573583316395" />
</map>
```

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="com.whatsapp.registration.RegisterPhone.phone_number">[redacted]</string>
    <int name="com.whatsapp.registration.RegisterPhone.verification_state" value="0" />
    <int name="com.whatsapp.registration.RegisterPhone.country_code_position" value="-1" />
    <string name="com.whatsapp.registration.RegisterPhone.input_phone_number">[redacted]</string>
    <int name="com.whatsapp.registration.RegisterPhone.phone_number_position" value="10" />
    <string name="com.whatsapp.registration.RegisterPhone.input_country_code">358</string>
    <string name="com.whatsapp.registration.RegisterPhone.country_code">358</string>
</map>
```

Kuvio 21.RegisterPhone.xml ja VerifySMS.xml

Msgstore.db -tietokantaan tallentuu käyttäjän keskustelut. *Chat_list* -taulukossa on listattuna kaikki puhelinnumerot, joiden kanssa käyttäjä on viestitellyt. *Messages* -taulukossa oli tiedot kaikista käyttäjän keskusteluista. Seuraavat kentät olivat oleellisia tutkinnan kannalta

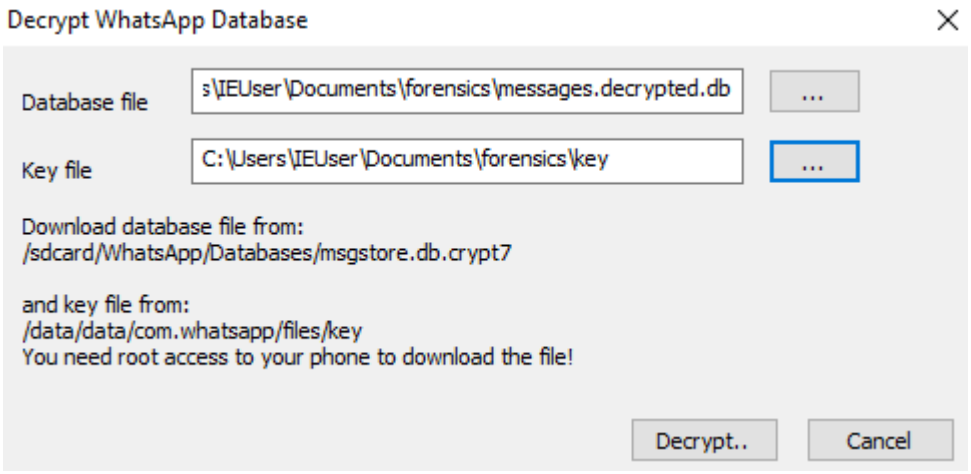
- Key_remote_jid
    - Yhteystiedon puhelinnumero
- Key_from_me
    - Kertoo, oliko käyttäjä viestin lähettäjä vai vastaanottaja (0=vastaanotettu, 1=lähetetty)
- Media_mime_type

- Mahdollisen tiedostopäätteen nimi

- Received_timestamp
  - Kellonaika, jolloin viesti on tullut perille

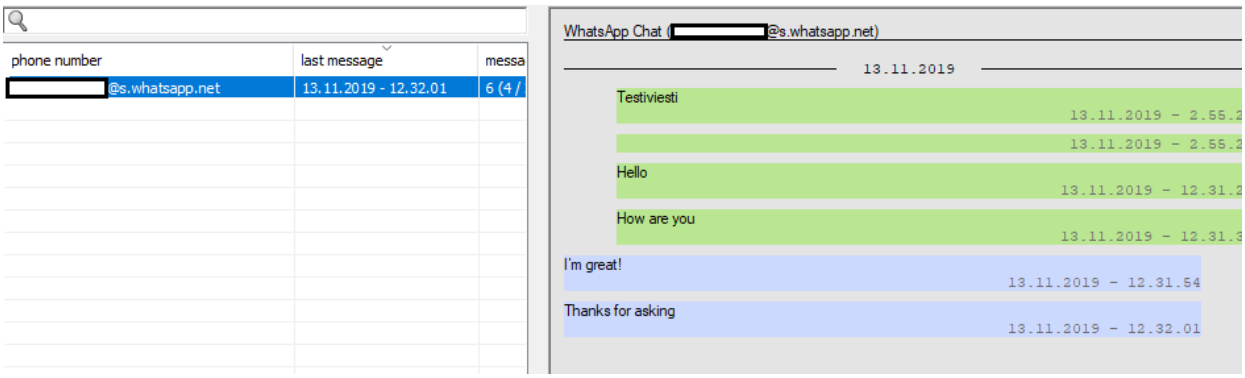
Wa.db -tietokanta sisältää yhteystietojen kontaktitiedot, kuten puhelinnumeron, statustekstin ja nimen.

Whatsappin varmuuskopiot olivat salattuja, mutta ne voidaan purkaa olettaen, että salausavain on hallussa. Se sijaitsee */data/files* -hakemistossa. Testikäyttäjän luoman varmuuskopion salaus purettiin WhatsApp Viewer-ohjelmalla, jonne ladattiin sekä salattu tietokanta, että salausavain (Ks. Kuvio 22).



Kuvio 22. Whatsapp -varmuuskopion salauksen purku

Kuviossa 23 on Viewerin käyttöliittymä ja varmuuskopioitu keskustelu. Viewer listaa keskustelut puhelinnumeroittain.



Kuvio 23. Varmuuskopioitu keskustelu

WiFi

Forensiikan kannalta kiinnostava tietoa WiFistä tutkittiin Autopsyllä tiedostosta /data/misc/wifi/wpa_supplicant.conf josta löytyi langattomat verkot, joihin käyttäjä kirjautuu automaattisesti. Kuviossa 24 on tuloste wpa_supplicant.conf-tiedostosta, josta näkee mm. langattoman verkon nimen, verkkoon asetetun salasanan ja salaustyypin. Tiedostossa näkyvät langattomat verkot ovat sidottuina Google-tiliin, eivätkä laitteeseen. Tallennetut WiFi-verkot eivät siis välttämättä olleet tallennettuina juuri tutkittavaan laitteeseen.

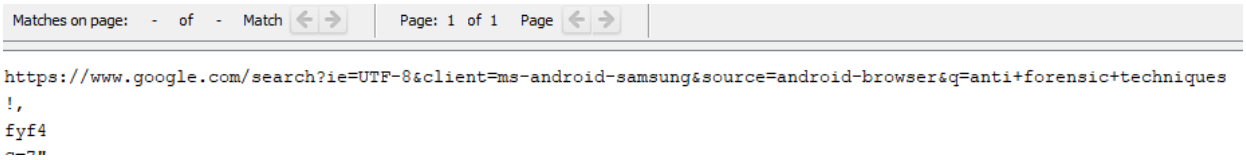
```
network={
        ssid="[redacted]"
        psk="[redacted]"
        key_mgmt=WPA-PSK
        priority=1
        frequency=5180
        autojoin=1
        usable_internet=0
        skip_internet_check=0
        verified_password=1
}
```

Kuvio 24. Laitteen muistissa olevat WiFi-verkot

Gmail

Sijainti: com.google.android.gm

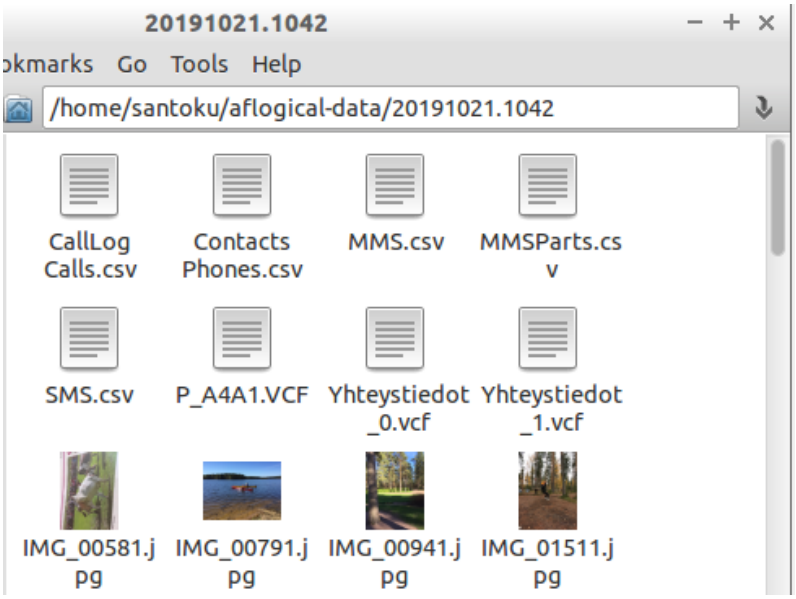
Gmailia tutkittaessa tietokannoista paljastui muutama kiinnostava kohta. Databases-kansiossa oli laitteeseen liitetyn Gmail-tilin sähköpostitietokanta (mailstore.<käyttäjä>@gmail.com.db). Tietokannasta ei löydetty sähköpostiviestejä, mutta merkkijonoja tarkasteltaessa löytyi kuviossa 25 tehty Google-haku.



Kuvio 25. Testikäyttäjän Gmail-tietokannan tarkastelu

4.5 Loogisesti palautettujen tietojen analysointi

AFLogical OSE loi tutkintatyöasemalle palautetuille tiedostoille kansion, johon se tallensi tiedostot senhetkisellä aikaleimalla. Tekstitiedot tallentuivat csv-päätteellä ja niitä voitiin tarkastella millä tahansa editorilla. Lisäksi laitteesta tallentui info.xml -tiedosto, josta löytyi tietoa laitteesta mm. IMEI, IMSI, laitteen teknisiä tietoja ja laitteeseen asennetut sovellukset. Vcf-päätteiset tiedostot ovat laitteella tekstiviestitse lähetettyjä yhteystietoja tai käyntikortteja (Ks. Kuvio 26).



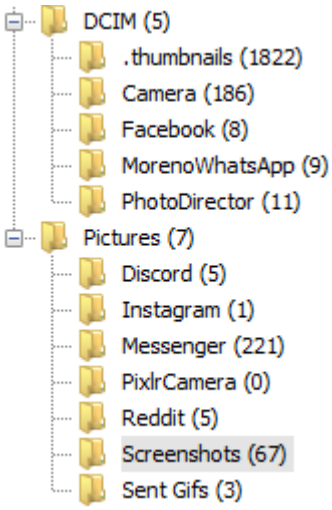
Kuvio 26. AFLogical OSE:lla palautetut tiedostot OnePlus 3T-puhelimesta

Puhelimen puhelokitiedostoa tarkasteltiin kuviossa 27 Gnumeric-taulukkolaskentaohjelmalla, josta nähtiin toisen osapuolen numero, puhelun ajankohta epoch-muodossa, puhelun kesto sekä yhteystiedon nimi.

_id	number	date	duration	type	new	name	numbert	numberlabel
2	[redacted]	1573040510648	0	2	0	[redacted]	2	SIM
1		1573040475028	0	2	0			

Kuvio 27. AFLogical OSE puheloki

Roottaamattomasta 3T-puhelimesta tutkittiin /sdcard-hakemiston sisältöä. Hakemistossa löytyi kameralla otetut kuvat, pikkukuvat eri sovelluksista, viestintäsovelluksilla jaetut/vastaanotetut kuvat, sekä puhelimen näytöstä otetut kuvat. Kuviossa 28 on listattuna kuvien sijainnit ja lukumäärä. Kuvien lisäksi hakemistoon tallentui kaikki laitteella ladatut tiedostot.



Kuvio 28. 3T-puhelimen kuvat

5 Tulokset

Mobiiliforensiikka on aihealueena valtava. Mobiililaitteiden luonnosta johtuen niiden tutkinta on haastavaa. Tutkijat joutuvat mukautumaan laitteiden kehittyessä tietoturvallisimmiksi. Opinnäytetyön lähtökohta oli sinänsä ihanteellinen, koska käytössä oli valmiiksi rootattuja laitteita. Näin ollen niistä oli mahdollista tutkia kaikkea niiden sisältämää tietoa. Rootattuja laitteita on kuitenkin nykypäivänä harvoissa oikeissa tutkintatapauksissa. Monesti on tukeuduttava siihen aineistoon, jota on saatavilla ilman root-oikeuksia tai väliaikaiseen roottiin tietoturvahaavoittuvuutta hyödyntäen, joka sekin on aikaa vievä toimenpide ja ei aina onnistu.

Mobiiliforensiikkaan on saatavilla paljon erilaisia avoimia työkaluja. Monet niistä eivät kuitenkaan ole helposti löydettävissä ja vaativat syvempää etsimistä. Läheskään kaikkien toimivuudesta ei myöskään ole takeita uudempien laitteiden kanssa, sillä

työkaluja päivitetään harvoin. Jotkut kuitenkin toimivat uusimpienkin laitteistoversioiden kanssa, vaikka niitä ei ole vuosiin päivitetty (Esim. AFLogical OSE). Työssä kartoitettiin työkaluja aina laitteiden tietojen palauttamisesta niiden analysointiin.

Avoimia analysointityökaluja on yhteensä kaksi, Autopsy ja FTK Imager. Autopsy todettiin työssä paremmaksi vaihtoehdoksi, sillä Android analyzer-moduulin ansiosta tiedot jäsenneltiin järkevästi sekä käyttöliittymä oli selkeämpi kuin FTK:lla. Näin ollen sitä käytettiin työssä tietojen analysointiin. Autopsyssä on lisäksi sisäänrakennettu SQL-tietokantaohjelma, jolla sovellusten tietokantoja voitiin suoraan tarkastella ilman, että niitä tarvitsi siirrellä ulkoiseen lukijaohjelmaan.

TB-8704f-tabletista palautettuja loogisia tiedostoja tutkittiin myös Autopsyllä. Tablettiin asennettiin samat sovellukset ja applikaatiot, kuin S5-puhelimeen. Tutkittavasta aineistosta ei kuitenkaan löytynyt mitään uutta tietoa, joka olisi tuonut tutkimukselle lisäarvoa. Liitteissä 1 ja 2 on esimerkkitulosteita tabletista tutkituista tiedoista.

Työssä selvitettiin, minkälaisia jälkiä käyttäjän tekemät toimenpiteet jättävät laitteeseen. Androidin sovellusten ja applikaatioiden käytöstä voidaan koostaa paljon tietoa SQLite-tietokantojen avulla. Esimerkiksi Facebookin sisältämä data on selkokielisenä luettavissa ja siitä voidaan päätellä paljon, jos sovellusta on jollain tapaa käytetty hämärään toimintaan. Lähes kaikissa sovelluksissa kansion rakenne on perusperiaatteeltaan samanlainen, joten tiedostojen tutkiminen on siinä mielessä melko vaivatonta. Analysointi on kuitenkin aikaa vievää, sillä sovelluksia saattaa olla asennettuna useita ja analysoitavaa dataa on todella paljon.

Sovellusten hakemistoissa on oleellisten tietokantojen lisäksi paljon muitakin tietokantoja ja tiedostoja, jotka eivät välttämättä varastoi kiinnostavaa dataa. Tutkijan on siis hyvä tietää etukäteen, mistä etsii tietoa. Taulukossa 5 on yhteenveto työssä käytetyistä sovelluksista, sekä tietokannat, joista löydettiin kiinnostavaa dataa.

Taulukko 5. Tietokantojen sijainnit sovelluksissa

Sovellus	**Kiinnostavan datan sijainti**

Facebook	• Data/com.facebook.katana/databases
	  ○ Contacts_db2
	  ○ Savedvideos.db
	  ○ Newsfeed.db
	  ○ Notifications.db

Facebook Messenger	• Data/com.facebook.orca/databases ○ Threads_db2

Tekstiviestit	• Data/com.android.providers.telephony/
	  ○ /files
	  ○ /databases
	  ▪ Mmsms.db
	  ▪ Telephony.db

Puhelulokit / Yhteystiedot	• Data/com.android.providers.contacts/databases
	  ○ Contacts2.db
	  ○ Calllog.db

WhatsApp	• Data/com.whatsapp/
	  ○ /databases
	  ▪ Msgstore.db
	  ▪ Wa.db
	  ○ /files
	  ▪ Avatars
	  ○ /shared_prefs
	  ▪ Registerphone.xml
	  ▪ VerifySMS.xml
	• Sdcard/WhatsApp
	  ○ Media
	  ○ Databases

WiFi	• Data/misc/wifi/ ○ Wpa_supplicant.conf
Gmail	• Data/com.google.android.gm ○ Mail-store.<user>@gmail.com.db

6 Pohdinta & johtopäätökset

Opinnäytetyön tavoitteena oli selvittää toimeksiantajalle nykypäivän mobiiliforensiikassa esiintyviä haasteita, sekä tutkia ja vertailla käytettävissä olevia avoimia työkaluja ja niiden kyvykkyyksiä Android-laitteiden tutkinnassa. Lisäksi työssä oli tarkoitus kartoittaa iOS:lle saatavilla olevat vastaavat työkalut.

Opinnäytetyössä oli käytössä testilaitteina sekä puhelimia, että tabletti. Suurimpana erona matkapuhelimiin oli se, että tabletilla oli mahdollista liittyä ainoastaan langattomaan verkkoon eikä siinä ollut SIM-kortin mahdollisuutta. Tabletin tutkinnasta voitiin siis sulkea pois puhelulokien ja tekstiviestien tarkastelu. Näitä eroavaisuuksia lukuun ottamatta Android-puhelimiin sovellettavaa toimintaperiaatetta voidaan hyödyntää myös tablettien tutkinnassa, sillä kaikki Android-sovellukset ja laitteet varastoivat tiedot samalla tavalla. Tuloksina saatiin kattavasti tietoa ajankohtaisimmista toimintatavoista ja avoimista forensiikkatyökaluista mobiililaitteiden forensiikan tutkimiseen.

Työssä käytetyt forensiikkatyökalut ja -ohjelmistot ovat toki hyvä lähtökohta laitteiden tutkimiseen ja forensiikkaan tutustumiseen, mutta niiden toiminnallisuudet ovat rajalliset ja luotettavampien tulosten saamiseksi on suositeltavaa tukeutua kaupallisiin vaihtoehtoihin. Laitteiden tutkinta ilmaistyökaluilla on pääosin manuaalista, maksulliset työkalut tekevät monet toimenpiteet automaattisesti ja niissä on enemmän toiminnallisuuksia. Automaattista analysointia ei kuitenkaan kannata pitää täysin luotettavana, sillä se voi jättää joitakin kohtia huomioimatta. Dahiyan, Mahajanin & Sanghvin (2013) tekemän tutkimuksen mukaan Cellebrite Physical Analyzer:in automaattinen analysointityökalu ei löytänyt jälkiä Viber-sovelluksesta, mutta manuaalisesti analysoituna merkittävää tietoa löytyi paljon. Ilmaistyökaluja käytettäessä on suurempi riski jättää epähuomiossa jokin tutkinnan kannalta oleellinen kohta huomioimatta. Työssä käytiin läpi kohdat, joilla on mahdollista minimoida inhimillisen virheen aiheuttamat puutteet tutkinnassa.

Työssä oli tarkoituksena tutkia lisäksi Androidin muistin forensiikkaa. Käytettyjen laitteiden ja muistin forensiikkaan tarkoitettujen työkalujen välillä esiintyi kuitenkin yhteensopivuusongelmia valmisteluvaiheessa, eikä laitteista onnistuttu palauttamaan

muistivedoksia. Muistin tutkintaan ei ole olemassa standardisoitua, universaalia toimintatapaa.

Opinnäytetyöstä saadun uuden tutkimustiedon ansiosta toimeksiantaja pystyy tekemään mobiililaitteiden forensiikkatyötä avoimilla työkaluilla parhaiden ja ajankohtaisimpien käytänteiden mukaisesti. Toimeksiantaja sai lisätietoa siitä, mitä eri työkaluja ja ohjelmistoja mobiiliforensiikkaan on saatavilla sekä mistä ja miten tutkittavaa aineistoa kannattaa etsiä.

Tutkimusta on mahdollista jatkokehittää moneen eri suuntaan. Työn toteutus painottui Androidiin iOS:n jäädessä toissijaiseksi. iOS:ään keskittyvästä forensiikasta voidaan tehdä vastaavanlainen tutkimus kartoittamalla saatavilla olevat työkalut sekä vertailla niiden ominaisuuksia. Myös pilvipalveluiden forensiikkaan keskittyvä tutkimus toisi arvokasta lisätietoa aihealueeseen, koska mobiililaitteet varastoivat paljon tietoa pilveen. Lisäksi SIM-korttien erillinen tutkinta voi paljastaa kiinnostavaa tietoa, joita ei laitteesta pystytä näkemään.

Tärkeä, mutta haastava kehityskohde on tietoturvahaavoittuvuuksien tutkiminen sekä Android-, että iOS-laitteista. Tätä voidaan pitää kriittisimpänä ja tärkeimpänä osa-alueena koko mobiiliforensiikassa, sillä laitteen perusteellinen tutkinta edellyttää pääkäyttäjän oikeuksia. Monet forensiikkatoimijat hyödyntävät näitä haavoittuvuuksia pääkäyttäjäoikeuksien saamiseksi ja luottamukselliseen tietoon pääsemiseksi, mutta ne ovat pääosin salassa pidettävää tietoa eikä niitä paljasteta julkisuuteen. Opinnäytetyössä yritettiin haastatella forensiikka-alan ammattilaista liittyen pääosin laitteen roottaamiseen ja pääsykoodin ohittamiseen, mutta kysymyksiin ei voitu vastata vedoten vaitiolovelvollisuuteen. Kysymykset on esitelty liitteessä 3.

Työssä ei käsitelty mobiililaitteiden rautatason (JTAG, Chip Off, Micro read) forensiikkaa, josta on myös mahdollista tehdä laajempaa tutkimusta. Kyseessä on kuitenkin hyvin paljon aikaa, resursseja sekä erityistä osaamista vaativa aihealue.

Testilaitteet eivät sisältäneet varsinaista oikeaa tutkittavaa tietoa, mutta todenmukaista tilannetta simuloitiin luomalla laitteisiin testidataa demonstroimaan työkalujen käyttöä ja ominaisuuksia. Samoja toimintaperiaatteita voidaan soveltaa oikeassakin

forensiikkatutkinnassa. Työtä voivat toimeksiantajan lisäksi hyödyntää muutkin tahot, joita aihealue koskettaa.

Lähteet

Amin, R. Cloppert, M. & Hutchins, E. N.d. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Viitattu 26.9.2019. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Apple vs. the FBI: A complete timeline of the war over tech encryption. Digital Trends Staff. 2016. Viitattu 17.9.2019. https://www.digitaltrends.com/mobile/apple-encryption-court-order-news/

Ayers, R. Brothers, S. & Jansen, W. 2014. Guidelines on Mobile Device Forensics. NIST Special Publication 800-101 Revision 1. Viitattu 24.9.2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

Bertè, R. Marturana, F. Me, G. & Tacconi, S. 2011. A quantitative approach to Triaging in Mobile Forensics. Viitattu 23.10.2019. https://www.researchgate.net/publication/259527921_A_Quantitative_Approach_to_Triaging_in_Mobile_Forensics

Bommisetty, S. Mahalik, H. Skulkin, O. & Tamma, R. 2018. Practical Mobile Forensics. Birmingham: Packt Publishing Ltd.

Broenner, S. Höfken, H. & Schuba, M. 2016. Streamlining Extraction and Analysis of Android RAM Images. Viitattu 30.11.2019. https://pdfs.semanticscholar.org/858d/9452e04ededfc2b036f15424e54456cb7235.pdf

Brothers, S. 2014. NIST Mobile Device Forensics A-Z. Viitattu 20.10.2019. https://www.nist.gov/sites/default/files/documents/forensics/2-Brothers-NIST-2014_Slides-23-Pages-2.pdf

CVE-2019-2215. N.d. Cve.mitre.org. Viitattu 4.12.2019. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2215

Dahiya, M. S. Mahajan, A. Sanghvi, H.P. 2013. Forensic Analysis of Instant Messenger Applications on Android Devices. Viitattu 30.11.2019. https://arxiv.org/ftp/arxiv/papers/1304/1304.4915.pdf

Epifani, M. Stirparo, P. 2016. Learning iOS Forensics. Uud. P. Birmingham: Packt Publishing Ltd.

Google's Android OS: Past, Present, and Future. 2011. Phonearena. Viitattu 29.9.2019. https://www.phonearena.com/news/Googles-Android-OS-Past-Present-and-Future_id21273

Hernandez, G. 2019. Tailoring CVE-2019-2215 to Achieve Root. Viitattu 4.12.2019. https://hernan.de/blog/2019/10/15/tailoring-cve-2019-2215-to-achieve-root/

Hoog, A. 2011. Android Forensics. Syngress.

How many phones are in the world? 2019. Bankmycell.com. Viitattu 17.9.2019. https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

How to Image a Smartphone with Magnet ACQUIRE. Magnet Forensics.com. 2019. Viitattu 22.10.2019. https://www.magnetforensics.com/resources/image-smartphone-magnet-acquire/

Johansen, G. 2017. Digital forensics and Incident Response. Birmingham: Packt Publishing Ltd.

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas: Näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun. Jyväskylä: Jyväskylän ammattikorkeakoulu

Libimobiledevice. N.d. Libimobiledevice:n verkkosivut. Viitattu 2.12.2019. http://www.libimobiledevice.org/

Liu, H. Liu, W. Yang, H. & Zhuge, J. N.d. A Tool for volatile memory acquisition from android devices. Viitattu 30.11.2019. https://hal.inria.fr/hal-01758679/document

Lohrum, M. 2017. Using Windows to Live Image an Android device. Viitattu 7.11.2019. http://freeandroidforensics.blogspot.com/2017/07/using-windows-to-live-image-android.html

Murphy, C. N.d. Developing Process for Mobile Device Forensics. Viitattu 30.9.2019. https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf

Packt. 2014. Introduction to Mobile Forensics. Viitattu 23.11.2019. https://hub.packtpub.com/introduction-mobile-forensics/

Platform Architecture. N.d. Developer.android.com-sivusto. Viitattu 5.11.2019. https://developer.android.com/guide/platform

Plum, J. 2017. APFS filesystem format. Viitattu 29.8.2019. https://blog.cugu.eu/post/apfs/

Reddy, N. 2019. Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations. Apress.

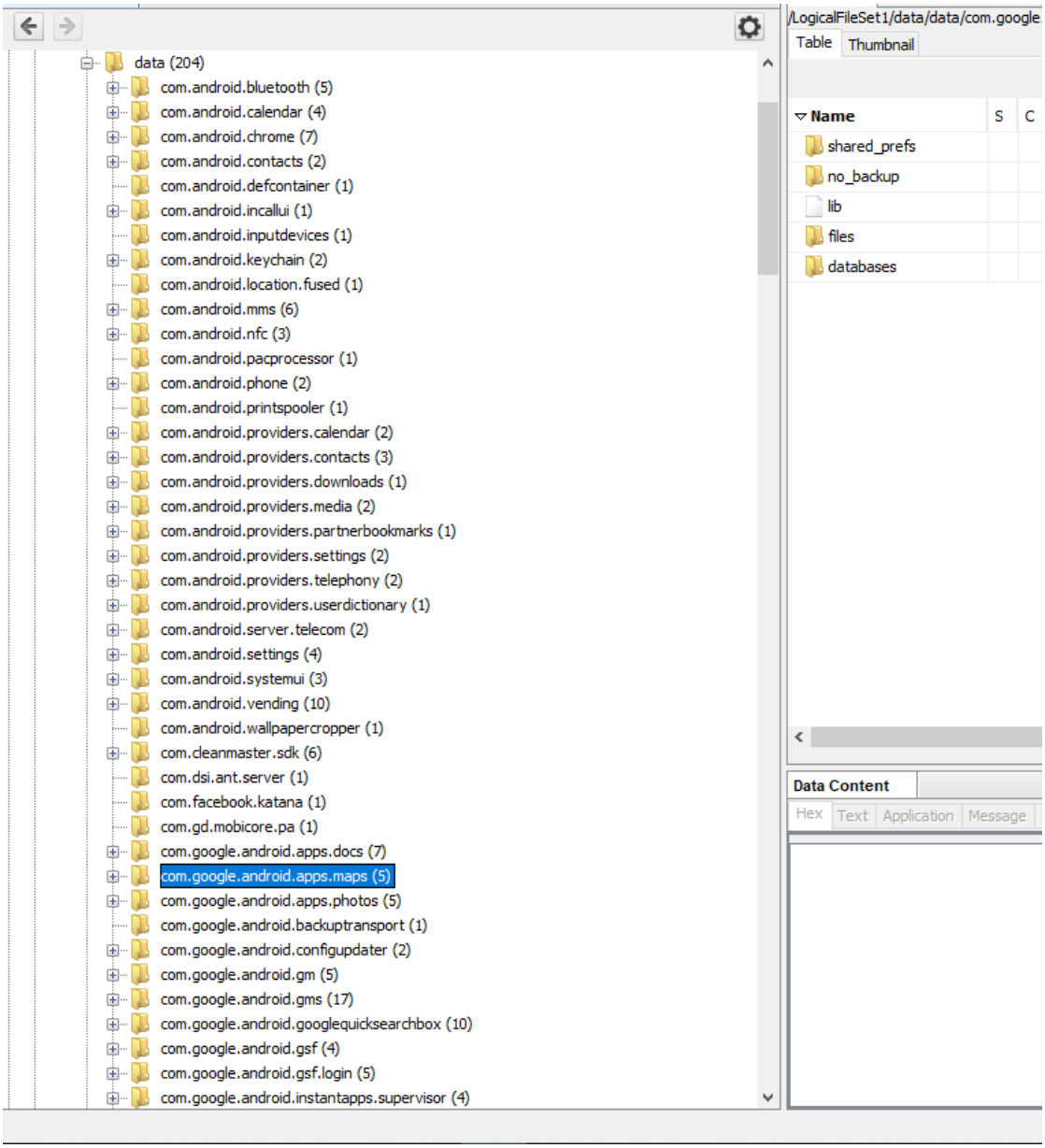
Secure exercise environment. 2019. JYVSECTECin verkkosivut. Viitattu 8.7.2019. https://jyvsectec.fi/cyber-range/overview/

Skulkin, O. Tamma, R. & Tindall, D. 2019. Learning Android Forensics. Uud. P. Birmingham: Packt Publishing Ltd.

Spreitzenbarth, M. & Uhrmann, J. 2015. Mastering Python Forensics. Birmingham: Packt Publishing Ltd.

Liitteet

Liite 1. /userdata-osio tabletista



Liite 2. Tablettiin asennettuja sovelluksia

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<packages>
    <version sdkVersion="23" databaseVersion="3" fingerprint="samsung/s5neoltexx/s5neolte:6.0.1/MMB29K/G903FXXU2BRH2:user/release-keys" />
    <version volumeUuid="primary_physical" sdkVersion="23" databaseVersion="23" fingerprint="samsung/s5neoltexx/s5neolte:6.0.1/MMB29K/G903FXXU1BQC1:use
    <permission-trees>
        <item name="com.google.android.googleapps.permission.GOOGLE_AUTH" package="com.google.android.gsf" />
    </permission-trees>
    <permissions>
        <item name="android.permission.REAL_GET_TASKS" package="android" protection="18" />
        <item name="com.sec.android.app.music.provider.permission.READ_MUSIC_SEARCH_PROVIDER" package="com.sec.android.app.music" />
        <item name="com.sec.android.emergencymode.permission.MODIFY_LOCATION_PROVIDER" package="com.sec.android.emergencymode.service" protection="18" /
        <item name="com.samsung.accessory.permission.TRANSPORTING_NOTIFICATION_ITEM" package="android" protection="2" />
        <item name="com.samsung.android.providers.context.permission.READ_MOVE_LOCATION" package="com.samsung.android.providers.context" protection="18'
        <item name="com.sec.android.permission.PERSONAL_MEDIA" package="com.samsung.android.allshare.service.mediashare" protection="18" />
        <item name="android.permission.REMOTE_AUDIO_PLAYBACK" package="android" protection="2" />
        <item name="android.permission.DOWNLOAD_WITHOUT_NOTIFICATION" package="com.android.providers.downloads" />
        <item name="com.sec.android.app.sns3.permission.RECEIVE_LINKEDIN_BROADCAST" package="com.sec.android.app.sns3" protection="18" />
        <item name="android.permission.sec.MDM_REMOTE_CONTROL" package="android" protection="2" />
        <item name="com.samsung.android.provider.filterprovider.permission.RECEIVE_UPDATE" package="com.samsung.android.app.filterinstaller" protection=
        <item name="com.google.android.apps.photos.permission.C2D_MESSAGE" package="com.google.android.apps.photos" protection="2" />
        <item name="com.sec.permission.BLUETOOTH_DEBUG" package="android" protection="2" />
        <item name="android.permission.INTENT_FILTER_VERIFICATION_AGENT" package="android" protection="18" />
        <item name="android.permission.BIND_INCALL_SERVICE" package="android" protection="18" />
        <item name="com.samsung.android.permission.LAUNCH_ULTRAPOWERSAVING_SERVICE" package="com.sec.android.emergencymode.service" protection="18" />
        <item name="com.samsung.applock.permission.STATUSCHANGED" package="com.android.settings" protection="18" />
        <item name="com.google.android.gms.trustagent.framework.model.DATA_CHANGE_NOTIFICATION" package="com.google.android.gms" protection="2" />
        <item name="android.permission.WRITE_SETTINGS" package="android" protection="1218" />
        <item name="com.google.android.gm.permission.WRITE_GMAIL" package="com.google.android.gm" protection="2" />
        <item name="com.sec.android.fota.permission.PUSH" package="com.sec.android.soagent" protection="18" />
        <item name="com.google.android.vending.verifier.ACCESS_VERIFIER" package="com.android.vending" protection="2" />
        <item name="com.sec.android.app.samsungapps.accesspermission.BILLING_ACTIVITY" package="com.sec.android.app.samsungapps" protection="2" />
        <item name="com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE" package="com.android.vending" />
        <item name="com.sec.android.email.permission.EMAILBROADCAST" package="com.samsung.android.email.provider" protection="18" />
        <item name="android.permission.READ_SMS" package="android" protection="1" />
        <item name="android.permission.CONTROL_KEYGUARD" package="android" protection="2" />
        <item name="com.samsung.android.voicewakeup.permission.READ_SETTING_PROVIDER" package="com.samsung.voiceserviceplatform" />
        <item name="com.samsung.android.providers.context.permission.UPLOAD_APP_FEATURE_SURVEY" package="com.samsung.android.providers.context" protecti
        <item name="com.samsung.android.sdk.email.permission.WRITE_EMAILCONTRACT" package="com.samsung.android.email.provider" protection="18" />
        <item name="com.sec.smartcard.pinservice.permission.SMARTCARD_CRYPTO" package="com.sec.smartcard.manager" protection="18" />
```

Liite 3. Haastattelukysymykset

- Mitä haasteita mobiiliforensiikassa esiintyy?
- Mikä on mobiiliforensiikan tämänhetkinen tilanne teknisen tutkijan näkökulmasta?
    - Pysytäänkö teknologian nopeassa kehityksessä mukana?
- Mitä työkaluja ja tekniikoita viranomaiset/tutkijat käyttävät mobiililaitteiden tutkinnassa?
    - Käytetäänkö open source -työkaluja vai ainoastaan kaupallisia?
- Miten uudempien, kryptattujen laitteiden kanssa toimitaan jos esimerkiksi pääsykoodia ei syystä tai toisesta tiedetä?
- Saako laitteista todistusaineistoa ilman root-oikeuksia?
- Tiettävästi laite tyhjentyy kaikesta datasta kun lukittu bootloader avataan, onko tämä jotenkin ohitettavissa (esim. tietoturvahaavoittuvuutta hyödyntämällä)?