Matkapuhelimen JTAG-louhinta halutun datan noutamiseksi siitä

Valokuvien noutaminen mobiililaitteesta

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus
kevät 2023

Celia Kujamäki

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutus Tiivistelmä

Tekijä Celia Kujamäki Vuosi 2023

Työn nimi Matkapuhelimen JTAG-louhinta halutun datan noutamiseksi siitä
Valokuvien noutaminen mobiililaitteesta

Ohjaaja Ismo Turve

TIIVISTELMÄ

Opinnäytetyön tarkoituksena oli selvittää mitä JTAG-menetelmällä tarkoitetaan, mikä on JTAG-standardi ja miten JTAG-louhinta suoritetaan kohdelaitteisiin. Tavoitteena oli luoda selkeä suomenkielinen selvitys aiheesta ja jäsennellä aihe ymmärrettävään muotoon, jolloin lukija pystyisi ymmärtämään JTAG-menetelmän myös osana mobiiliforensiikan menetelmiä.

Opinnäytetyö on tutkimuksellinen ja sen tietopohja koostuu digitaalisen ja mobiiliforensiikan alustamisesta, jotka antavat pohjan JTAG:lle. JTAG osassa käsitellään menetelmän taustaa, perehdytään JTAG-standardiin ja miten menetelmä toimii mobiililaitteen piirilevyn tasolla. Lisäksi teoriaosuudessa kuvaillaan JTAG-louhinnan prosessi ja louhinnassa käytettävien flasher työkalujen perustietoja. Viimeisessä teorialuvussa kerrotaan lyhyesti JTAG-louhintaa sivuavista aiheista, jotka täydentävät lukijan kokonaisymmärrystä laajemmasta kokonaisuudesta. Teoriaa tukevaa aineistoa tuotettiin suorittamalla JTAG-louhinta kahteen mobiililaitteeseen. Tutkimuksessa käytettiin monimenetelmällistä tutkimustragediaa, jossa yhdistetään sekä teoreettista tutkimusta että sovellettua konstruktiivista tutkimusta.

Tutkimuksessa havaittiin, että JTAG-louhinnan prosessi on hienovaraista, jonka tähden tutkijoilta vaaditaan tarkkuutta etenkin hyppylankojen kiinni juottamisessa. Opinnäytetyö ei saavuttanut haluttuja tavoitteita louhinnan onnistumisen kannalta. Työstä saatiin hyödyllistä näyttöä, miten asiat voivat mennä väärin JTAG-louhinta prosessin aikana.

Avainsanat Digitaalinen forensiikka, mobiiliforensiikka, JTAG-standardi, JTAG-louhinta, flasher box.

Sivut 74 sivua ja liitteitä 1 sivu

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology Abstract

Author Celia Kujamäki Year 2023

Subject Mobile phone's JTAG extraction for retrieving desired data
Recovering photos from mobile device

Supervisor Ismo Turve

ABSTRACT

The purpose of the thesis was to find out what is meant by the JTAG method, what is the JTAG standard and how JTAG extraction is performed on the target devices. The goal was to create an explanation of the topic in Finnish and structure the topic to an understandable form, so that the reader would be able to understand the JTAG method also as part of mobile forensics methods.

The thesis is research-based and its knowledge base consists of initialization of digital and mobile forensics, which provide the basis for JTAG method. The JTAG part discusses the background of the method, introduces the JTAG as a standard and how the method works at the level of the mobile device's circuit board. In addition, the theory part describes the process of JTAG extraction and the basic information on the flasher tools used in the extraction. In the last theory chapter, the topics related to JTAG extraction are described, which complete the reader's overall understanding of the larger topic. Supporting material part was produced by performing JTAG extraction on two mobile devices. The research used a multi-method research strategy, which combined both theoretical research and applied constructive research.

The study found that the process of JTAG extraction is delicate, which is why researchers are required to be precise, especially when soldering the jumper wires. The thesis research did not achieve the desired results in terms of JTAG extraction success. Nevertheless, the work provided the knowledge of the difficulties in JTAG extraction process.

Keywords Mobile Forensics, JTAG standard, JTAG extraction, Flasher box, Digital Forensics

Pages 74 pages and appendices 1 page

Sanasto

FORENSIIKKA	Tietorikosten tutkiminen tai rikostekninen tutkimusta.
MOBIILILAITE	Kannettava laite, joka soveltuu tiedon siirtoon ja käsittelyyn.
IR	Incident Response, tietoturvan poikkeamiin vastaaminen,
CSIRT	Computer Security Incident Response Team.
IEEE	Kansainvälinen tekniikan alan järjestö, keskeinen standardoija.
I/O	Input/output, mikä tahansa datansiirto operaatio laitteessa.
RAJASKANNAUS	Mikropiirien testaustapa, joka suoritetaan JTAG:in kautta.
KETJUTUS	Daisy Chain, laiteita kytketty yhteen peräkkäin tai renkaaksi.
JTAG-KÄSKYT	JTAG Instructions, ”ohjeistus” rajaskannauksen suorittamiselle.
FSM	Finite-state Machine, äärellinen automaatti.
JTAG-YHDISTÄJÄ	JTAG Connector.
JTAG-ADAPTERI	JTAG Adapter, myös nimillä Intelligence Card, JTAG interface.
IC	Integrated circuit, mikropiiri.
PCB	Printed Circuit Board, piirilevy.
CHIP	Siru, mikrosiru, piirisiru.
PIN	Nasta piirilevyssä.
RAM	Random-access memory, hajasaantimuisti. Usein keskusmuisti.
FLASH-MUISTI	Puolijohdemuisti, haihtumaton muisti.
HYPPYLANKA	Johtokytkentä kontaktipinnasta toiseen kuparijohdolla/jumperilla.
BGA	Ball grid array, mikropiirin asennustapa piirilevylle.
TSOP	Thin small outline package, mikropiirin asennustapa piirilevylle.
ISP	In-system programming, laitteen sisäisenohjelmointi.

Sisällys

Kuvat ja taulukot

Liitteet

Liite 1 Aineistonhallintasuunnitelma

1 Johdanto

Opinnäytetyössä selvitetään yhden mobiiliforensiikan tutkimusmenetelmän taustaa, sen arkkitehtuuria ja toimintaa käytännössä. JTAG-louhintaa käytetään silloin kun mobiililaitteeseen ei pääse manuaalisesti sisään esimerkiksi siksi, että laite on suojattu salasanalla tai laitteen näyttö on vaurioitunut. Menetelmänä JTAG:ia käytetään pääasiassa mobiililaitteiden piirilevyjen mikropiirien toimivuuden testaamiseen ja se on laajasti käytössä monien matkapuhelinvalmistajien tehtaissa. Menetelmää hyödynnetään myös matkapuhelinten korjauksessa huomattavassa määrin, kun kyse on mobiililaitteiden tietoturvan ja suojauskeinojen vahvistamisesta murtoja vastaan.

Kiinnostukseni aiheeseen heräsi kyberturvallisuuden opintojen aikana, jolloin kävimme läpi muun muassa erilaisia digitaalisen forensiikan haaroja. Aiheesta löytyy runsaasti hajautettua tietoa internetistä ja englanninkielisistä digitaalisen forensiikan oppikirjoista, mutta tämä tieto on usein varsin vaikeaselkoista, mikä hankaloittaa itse JTAG-menetelmän ymmärtämistä. Tavoitteenani on siis luoda selkeä suomenkielinen kuvaus JTAG-louhinnasta, sillä sellaista ei opinnäytetyöni tekohetkellä ole.

Opinnäytetyö pyrkii vastaamaan seuraaviin tutkimuskysymyksiin:

- Mitä on digitaalinen forensiikka ja mobiiliforensiikka?
- Mikä on JTAG-standardi?
- Mitä on JTAG-louhinta ja miten louhinta suoritetaan?
- Mikä on ”flasher box” työkalu?

2 Tutkimuksen tavoite ja tarkoitus

Työn tavoite on selvittää ja selkeyttää lukijalle, mitä JTAG-louhinnalla oikein tarkoitetaan ja miten tämä louhinta toimii käytännössä. Aihetta alustetaan ensin teoriaosuudessa käymällä läpi ensin taustatietoa digitaalisen forensiikasta ja mobiiliforensiikasta, jolloin lukija, joka ei ole täysin perehtynyt näihin aiheisiin saa selkeän kokonaiskuvan aiheesta. Merkittävin osuus teoriasta on osuus, jossa pyritään selittämään JTAG-standardi, JTAG toiminta piirilevyllä, itse JTAG-louhinnan selostus ja siihen liittyvät seikat. Lisäksi teoria osuudessa käydään lyhyesti läpi JTAG-louhintaa sivuavat ja täydentävät aiheet, joihin lukija saattaisi törmätä liittyen tähän aiheeseen.

Teoriaa tuetaan työn käytännönosuudella, jossa suoritetaan ja dokumentoidaan JTAG-louhinta prosessi kahteen mobiililaitteeseen askel askeleelta. Opetusnäkökulmasta katsoen tavoitteena on antaa lukijalle mahdollisimman selkeä ymmärrys JTAG-louhinnasta mobiiliforensiikan menetelmänä ja siitä, miten se tapahtuu käytännössä. Käytännönosuuden teknisenä tavoitteena on palauttaa mobiililaitteista tiedostoja, joihin ei enää pääse manuaalisesti käsiksi itse laitteelta.

Työssä hyödynnetään teoreettista tutkimusstrategiaa, koska työ on vahvasti tutkimuksellinen opinnäytetyö. Tutkimusmenetelminä toimii myös sovellettu konstruktiivinen tutkimusote, jonka keskeinen idea on löytää ratkaisu tiettyyn ongelmaan. Vaikka konstruktiivista tutkimusotetta käytetään pääasiassa innovointiin ja suunnittelun osana, pystyn soveltamaan sitä jonkin verran omassa tutkimuksessani: olemassa keskeinen ongelma, johon vastataan laajan teoreettisen tutkimuksen ja käytännön kautta. (Oppariapu, 2016; *Teoreettinen tutkimus — Jyväskylän yliopiston Koppa*, n.d.-a)

Työtä ja tutkimuksen tuloksia ja aineistoa pystytään jatkossa hyödyntämään mahdollisesti kyberturvallisuuden opettamisessa selkeänä suomenkielisenä selvityksenä yhteen mobiiliforensiikan yleisimmistä tutkimusmenetelmistä, sillä tästä aihealueesta ei ole saatavissa juurikaan suomenkielistä materiaalia.

3 JTAG osana digitaalisen forensiikan menetelmiä

Rikostekninen tutkimus on ollut aina tärkeä osa rikostapausten selvittämisessä. Teknologian ja käytäntöjen kehittyessä tutkimuksesta on tullut yhä tarkempaa ja yksityiskohtaisempaa. Itse rikostekninen tiede on kehittynyt jatkuvasti yhteiskunnan muutosten mukana, jotta tutkijat soveltaisivat aina täsmällisempiä tieteellisiä periaatteita oikeustieteellisten ongelmiin faktojen löytämiseksi ja toteamiseksi. (Årnes, 2018, s. 2)

3.1 Digitaalinen forensiikka

Digitaalisen forensiikan tai digitaaliforensiikan alku pystytään jäljittämään tietokoneiden keksimisestä ja yleistymisestä lähtien, jolloin viranomaiset alkoivat huomioida tietokoneiden yleistyvän käytön myös rikollisten parissa. Tekniikan ja teknologian kehittyessä ovat myös nämä rikosteknisen tutkimuksen menetelmät kehittyneet tarkemmiksi ja laajentuneet uusiin tarpeisiin. (Gogolin, 2021, s. 1) Etenkin 1990-luvulta lähtien monet viranomaistahot, kuten Yhdysvaltojen liittovaltion poliisi (FBI) alkoivat sisällyttää digitaalisista forensiikkaa tutkimusmenetelmiinsä, ja nykyisin se on tärkeä osa laajempaa rikosteknistätutkimusta ja yksi osa-alue rikosteknistä tiedettä. (Johansen, 2022, s. 52)

Digitaalista forensiikkaa ei hyödynnetä yksinomaan rikosoikeudellisissa puitteissa, vaan myös muilla tahoilla kuten julkisella sektorilla sekä yksityisomistuksessa olevissa yrityksissä ja organisaatioissa (Årnes, 2018, s. 5). Näissä tapauksissa sitä hyödynnetään osana organisaation tietoturvapoikkeaman hallintaa (Incident Response), jolloin esimerkiksi organisaation CSIRT (Computer Security Incident Response Team) kutsutaan tutkimaan ja analysoimaan digitaalista aineistoa tietoturvahäiriöstä hyödyntäen digitaalisen forensiikan tietotaitoa, työkaluja ja tekniikoita. Esimerkiksi jos kyseessä on pahaa tarkoittava hyökkäys organisaation sisältä päin, digitaalisen forensiikkan avulla voidaan mahdollisesti löytää syyllinen tapaukseen. Kuitenkin tutkijoiden pitää huomioida oman maansa lait tiedostoja käsitellessään kuten esimerkiksi mihin heillä saa olla pääsy. (Johansen, 2022, s. 47)

Digitaalinen forensiikka on digitaalista rikosteknistä tutkimusta, jonka avulla pyritään paljastamaan ja tulkitsemaan sähköistä tietoa esimerkiksi tietokoneen haihtumattomasta flash-muistista. Prosessin aikana tunnistetaan, säilytetään, analysoidaan ja dokumentoidaan näitä digitaalisia todisteita niin, että todisteet ovat esitettävissä tarvittaessa tuomioistuimelle tai niillä voidaan estää suunniteltuja operaatioita. Tieteenalana digitaalinen forensiikka on oikeustieteen ala, jossa keskitytään tietokoneverkkorikollisuuteen liittyvien sähköisten laitteiden tietojen talteenottoon ja tutkimiseen. Tavoitteena on säilyttää kaikki mahdolliset todisteet niiden alkuperäisimmässä muodossa oletetusta rikosvälineestä tai epäillyn laitteelta. (Årnes, 2018, ss. 4–5)

Tutkimuksen kohteita ovat nykyisin erilaiset digitaaliset laitteet, ei vain pelkästään tietokoneet. Näitä ovat muun muassa printterit, mobiililaitteet, pelijärjestelmät, sovellukset, GPS, biometriset tunnistuslaitteet, älytabletit ja flash-asemat, mutta myös Internet of Things -laitteet, autojen sähköiset järjestelmät ja kaikki muut ohjelmoitavissa olevat laitteet. Huomioitavaa myös on, että Big Data eli jäsentelemätön massadata on suuri informaation lähde rikosteknisille tutkijoille, sillä kyseinen tietomassa sisältää esimerkiksi sähköpostitiedostoja ja mobiililaitteiden tekstiviestejä. (Gogolin, 2021, s. 1)

Näiden erilaisten tutkimuskohteiden kautta digitaalisen forensiikan voi jakaa viiteen eri haarautumaan, jotka ovat tietokonerikostekninen tiede, mobiiliforensiikka, tietokoneverkkoliikenteen rikostekninen tiede, rikostekninen strukturoidun datan analyysi ja tietokantojen rikostekninen tarkastelu.

3.1.1 Digitaalisen forensiikan haasteet

Yleisiä haasteita digitaaliforensiikalle ovat esimerkiksi datan muuttumattomuuden varmistaminen, pilvipalveluiden käytön yleistyminen, jolloin rikolliset voivat hyödyntää näiden palveluiden ketterää käyttötapaa, virtualisointityökalut, kovalevyjen kehittyminen sekä internetin kansainvälisyys. Haasteisiin kuuluvat myös maiden eriävät lait, jotka saattavat rajoittaa rikosteknistä tutkimusta. (Gogolin, 2021, ss. 7–11)

Myös anti-forensiikka eli anti-forensics hankaloittaa rikosteknistätutkimusta, sillä kyseisellä menetelmällä pyritään estämään tiedostojen rekonstruktio tutkimuksen analyysivaiheessa

muun muassa piilottamalla, tuhoamalla tai muuttamalla mahdollista todistusaineistoa käyttökelvottomaksi (Gogolin, 2021, s. 9). Eräs tällainen työkalu on Drive Wiper, joka poistaa tiedostot laitteen levyltä (EC-Council, 2022).

3.1.2 Tutkimukseen soveltuva laboratorioympäristö

Olipa kyseessä minkä tahansa digitaalinen forensiikan haaran prosessi, tutkimus on suoritettava hallitussa laboratorioympäristössä.

Ympäristön täytyy olla tiukasti hallittu ja suojattu ulkopuolisilta. Tällöin pystytään turvaamaan muun muassa todistusaineiston eheys, luotettavuus ja saatavuus. Ilmanlaatu tulee myös ottaa huomioon, sillä laitteet ja todistusaineisto voivat olla herkästi alttiina kosteudelle. Todistusaineiston liikehdintää pystytään hallitsemaan ja kirjaamaan tarkemmin ylös rajaamalla keillä on pääsy tiloihin, ja ketkä saavat olla tekemisissä aineiston kanssa. Todistusaineiston säilyttäminen lukollisessa kaapissa on suositeltavaa silloin, kun niitä ei käsitellä. Rajatussa ympäristössä pystytään hallitsemaan todistusaineiston liikehdintää ja valvomaan pääsyä tiloihin sekä ketkä saavat olla kosketuksissa aineiston kanssa. Laitteiden avaamiseen tarvitaan erilaisia työkaluja kuten ruuvitalttoja ja leikkureita. Tutkijat tarvitsevat tiedon keräämiseen ja käsittelyyn forensiikkaan erikoistuneita laitteita kuten ison muistin omaavia tietokoneita rikosteknistätutkimusta varten, muita erityislaitteita ja tietokoneita, joilla tutkijat pääsevät internettiin. (Johansen, 2022, ss. 61–63)

Tutkijoilla on myös käytössä erilaisia ohjelmia, joilla he pääsevät jäsentelemään ja lukemaan tutkittavan kohteen tietoja. Ohjelmia on saatavilla kaupallisesti ja avoimen lähdekoodin ohjelmina. On myös erillisiä ohjelmia, joita ei ole tarkoituksella luotu digitaaliseen forensiikkan käyttöön, mutta niitä voi hyödyntää silti. Yksi näistä on pakettianalysaattori ohjelma Wireshark, jolla on mahdollista kaapata, tallentaa ja analysoida tietoliikennettä. (Johansen, 2022, s. 63)

Suositeltavaa on, että tutkijoilla olisi valmiina salkku, jossa olisi tarvittavat välineet digitaalisen rikosteknisentutkinnan suorittamiseen työympäristön ulkopuolella esimerkiksi suoraan tapahtumapaikalla (Johansen, 2022, s. 68).

3.2 Mobiiliforensiikka

Mobiiliforensiikka on yksi digitaalisen forensiikan haaroista, jossa keskitytään digitaalisten todisteiden palauttamiseen mobiililaitteelta luotettavilla rikosteknisillä menetelmillä niin, ettei laitteessa oleva tieto muutu. Digitaalisella todisteella tarkoitetaan tietoa, joka on tallennettu, vastaanotettu tai lähetetty tutkinnassa olevasta elektronisesta laitteesta. Todisteet voivat olla muun muassa laitteesta löytyvät yhteystiedot, puhelulokit, sähköpostit, laitteella otetut videot, erilaiset dokumentit, IMEI-koodit, kalenteri, SMS-tekstiviestit, MMS-mediat, GPS-sijaintitiedot, sosiaalisen median sovellukset ja jopa poistetut tiedot. (Gogolin, 2021, s. 65; Packt, 2014a)

Matkapuhelimen ja mobiililaitteiden käytön jatkuvasti kasvaessa on mobiiliforensiikan rooli korostunut entistä enemmän osana rikosteknistä tutkimusta. Esimerkiksi pelkästään vuodesta 2016 vuoteen 2021 älypuhelimien käyttäjä määrä on kaksinkertaistunut noin 3 miljoonasta yli 6 miljoonaan Statican tutkija Petroc Taylorin mukaan ja tulee jatkossa jatkamaan kasvuaan (*Smartphone Subscriptions Worldwide 2027*, n.d.). Aikaisemmin mobiiliforensiikan tutkimus rajoittui paljolti vain manuaaliseen tutkimukseen niin, että tutkimuksen dokumentointi oli vaivanloista ja hidasta. Tämä johtikin teknologian kehittyessä uusien työkalujen kehittämiseen mobiiliforensiikan tukemiseksi. Tulevaisuudessa mobiiliforensiikan tutkimus on laajentumassa myös autojen, älytalojen ja dronien rikostekniseen tutkimukseen. (Packt, 2014a)

Vaikka mobiililaitteella viitataan usein matkapuhelimiin, sillä voidaan tarkoittaa myös kämmentietokoneita (PDA), GPS-laitteita ja muita älylaitteita kuten tabletteja. Myös kannettavat musiikkisoittimet luetaan mobiililaitteiksi. (*Mobiiliopas - Mobiililaitteet*, n.d.)

Mobiililaitteen tutkintaprosessi jakaa joitakin piirreitä digitaalisen forensiikan käsittelyprosessin kanssa, mutta mobiiliforensiikan työkalut käyttävät täysin erilaisia menetelmiä. Digitaalisen forensiikan ja mobiiliforensiikan erot tulevat myös esiin tutkittavina olevista laitteista. Suurimmat erot ovat mobiililaitteiden koko ajan muuttuva luonne verrattavissa tietokoneiden staattiseen olemukseen, ja tietokoneiden on isompi tallennuskapasiteetti verrattuna mobiililaitteisiin. (Gogolin, 2021, ss. 65, 71)

3.2.1 Mobiiliforensiikan haasteita

Mobiililaitteiden rikostekniseen tutkimukseen kohdistuu lukuisia haasteita, jotka eriävät digitaalisen forensiikan haasteista. Suurimmat haasteet voidaan jakaa neljään osaan:

Laitteistoeroavaisuudet: Markkinoilla on nykyään paljon erilaisia mobiililaitteita eri valmistajilta. Täten mobiililaitteet käyttävät usein toisistaan täysin eriäviä käyttöjärjestelmiä, omaavat erillisiä ominaisuuksia ja ovat erilaisia laitteita malliltaan. Mobiililaitteiden jatkuva kehitys vaikeuttaa tutkijoiden työtä, sillä heidän täytyy pystyä mukautua nopeasti näihin muutoksiin ja päivittää tutkimusmenetelmiä samanaikaisesti ajan tasalle. (Gogolin, 2021, s. 67; Packt, 2014a)

Tietoturvallisuus: Nykyaikaiset mobiililaitteet on suojattu käyttäjien tietosuojan kiristyessä paremmin kuin ennen. Lisäksi mobiililaitteet ovat kryptattuja laitteistotasosta aina ohjelmistotasoon. Tämä tarkoittaa sitä, että tutkijoiden täytyy siis esimerkiksi murtaa laitteen lukitus päästäkseen käsiksi mobiililaitteella olevaan dataan. Haasteena tähän ovat eriävät suojausmekanismit eri valmistajien laitteissa: esimerkiksi Apple-laiteet ovat tunnettuja hyvin vankasta salauksestansa ja vahvasta tietoturvan vaalimisesta. (Packt, 2014a)

Tietojen säilyttäminen muuttumattomana: Tärkeimpiä asioita niin mobiiliforensiikassa kuin myös forensiikassa on todistusaineiston säilyttäminen muuttumattomina. Tätä vaikeuttaa mobiililaitteiden dynaaminen luonne, jolloin niiden toiminta on riippuvainen verkkoyhteyksistä, laitteen tilasta sekä laitteessa mahdollisesti olevista sovelluksista. Esimerkkejä tästä ovat mobiililaitteen erilaiset taustaprosessit, joista jotkut voivat pyöriä myös laitteen olleessa sammutettuna ja haihtuvan RAM-muistin tyhjeneminen, kun mobiililaite sammutetaan. Jotkin mobiililaitteessa olevat sovellukset voivat ajoitetusti pyyhkiä sovellusdatan automaattisesti usein juuri tietoturvallisuuden takaamiseksi käyttäjälle. On olemassa myös riski, että tutkijat itse voivat tahattomasti muuttaa laitteessa olevia tietoja esimerkiksi aktivoimalla tehdasasetusten palauttamisen tutkimuksen aikana. (Gogolin, 2021, ss. 67–68; Packt, 2014a)

Resurssien rajoitukset: Mobiililaitteiden määrän kasvaessa tutkimuksiin tarvittavien työkalulaitteiden ja niiden lisäosien, kuten USB-kaapeleiden ja latureiden tarve on myös

kasvanut. Olemassa ei ole myöskään yhtä ainoaa työkalua, jolla olisi tuki kaikkien mobiililaitteiden tutkimiseen. Tästä johtuen tutkijat käyttävät useampaa kuin vain yhtä työkalua tutkinnan aikana. Haasteena ovat sopivan työkalun valinta tutkimuksen suorittamiseen ja mahdolliset lisäkulut uusista laitehankinnoista. (Gogolin, 2021, s. 69; Packt, 2014a)

Mobiiliforensiikassa tulee vastaan myös samoja lisähaasteita kuin digitaalisessa forensiikassa. Näitä ovat esimerkiksi anti-forensiikan tekniikat mobiililaitteiden tietojen poistamiseksi etäältä sekä erilaiset lainsäädännölliset rajoitteet, joihin tutkijat voivat törmätä. (Packt, 2014a)

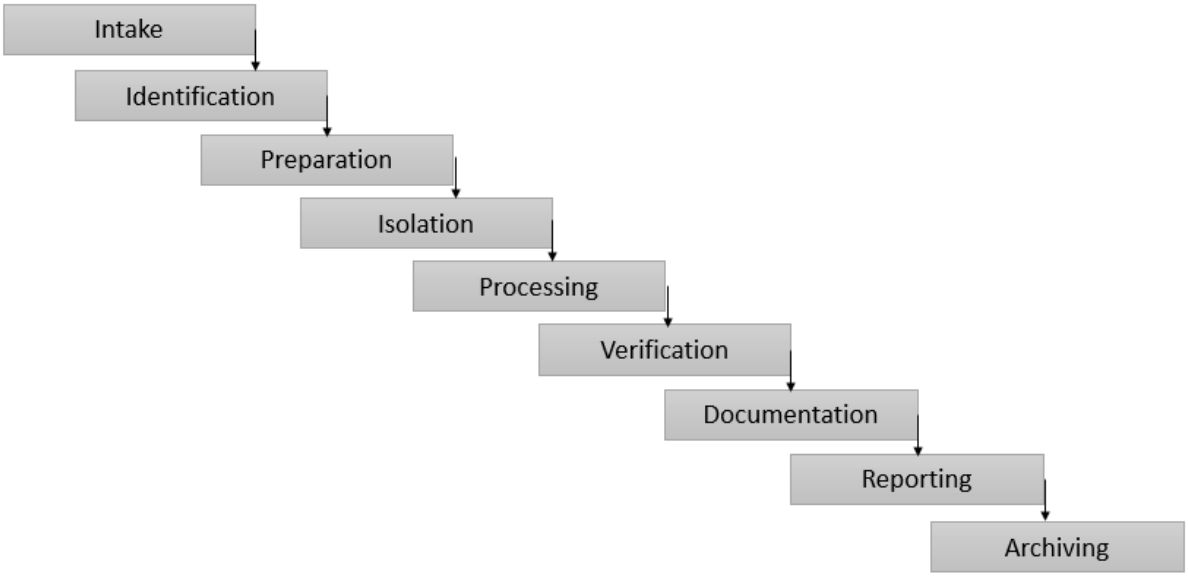
3.2.2 Todistusaineiston käsittelyprosessi

Tutkimusmenetelmät ja todistusaineiston käsittelyprosessi voi vaihdella tutkittavasta mobiililaitteesta toiseen, sillä olemassa ei ole yhtä vakiintunutta käytäntöä mobiililaitteen tutkimista varten. Yleisesti mobiiliforensiikan prosessi on jaettu kolmeen pääluokkaan, jotka ovat takavarikointi, hankita ja tutkimus- ja analysointivaihe. (Packt, 2014a)

Tutkijat tarvitsevat jäsennellyn prosessimallinuksen, jolla he voivat suorittaa tutkimuksen täsmällisesti vahingoittamatta mahdollista todistusainetta laitteessa. Ennen suunnitellun prosessin käyttöönottoa sen eri vaiheet pitää testata ja hyväksyttää samoin kuin myös dokumentoida ne. Prosessin malli tukee todistusaineiston dokumentointia ja mahdollistaa tutkimuksen toistettavuuden. (Packt, 2014a)

Jokaiseen prosessin mallinukseen täytyy sisällyttää seuraavia vaiheita (Kuva 1):

Kuva 1 Todistusaineiston käsittelyprosessi (Packt, 2014b)



Todisteen vastaanottaminen (Intake) on koko prosessin aloittamisvaihe. Vaihe koostuu paperitöistä ja pyyntölomakkeiden laatimisesta. Näihin dokumentteihin kirjataan muun muassa kuka on mobiililaitteen omistaja ja minkä tyyppisessä tapahtumassa laite on ollut osallisena, mutta myös mitä tietoja on pyydetty noudettavaksi laitteelta ja tutkimuksen tavoitteet. (Packt, 2014a)

Tärkein on hallussapitoketjun (chain of custody) dokumentoinnin aloittaminen. Hallussapitoketju on dokumentti, josta käy ilmi kaikki todistusaineistoon liittyvä tieto tutkimuksen aloituksesta sen loppuun kronologisessa järjestyksessä. Alussa siihen kirjataan, missä kunnossa ja tilassa mobiililaite on ollut löytöhetkellä. (Packt, 2014a)

Jatkossa hallussapitoketjuun kirjataan, kuka on käsitellyt todistusaineistoa tutkimuksen aikana kuten myös miksi, mihin ja milloin se on siirretty. Myös tutkimuksen löydökset tulee kirjata tarkasti ja nämä tiedostot tulisi hashata todistusaineen muuttumattomuuden varmistamiseksi. Näin pyritään säilyttämään todistusaineiston luotettavuus, eheys ja saatavuus. Ilman hallussapitoketjun dokumentaatiota todistusainetta ei voida käyttää oikeudessa. (Packt, 2014a)

Tunnistusvaiheessa (Identification) tutkijoiden pitää huomioida seuraavat asiat laitetta tutkiessa, jotka ovat:

Laillinen auktoriteetti eli mihin tutkijoilla on laillinen oikeus koskea. Etsintälupa määrittää muun muassa sen, mihin tiedostoihin laitteen sisällä tutkijoilla on oikeus päästä ja millä rajoitteilla tutkimus etenee. Tutkijoiden tulee selvittää tutkinnan tavoitteet eli kuinka syvällisesti laitetta tarvitsee tutkia sillä, joskus tähdellinen todistusaineisto löytyy vähemmälläkin tutkinnalla, ja varmistaa laitetietojen dokumentointi eli laitteen valmistaja, malli ja muut tunnistettavuustiedot. Heidän tulee tutkia laitteen erilliset tallennusmediat, kuten esimerkiksi lisämuistikortti on syytä tutkia. Tutkijoiden tulee kerätä muut mahdolliset todistusaineistot mobiililaitteesta: esimerkiksi sormenjäljet ja muut mahdolliset jäljet ennen tutkinnan alkua, jolloin vältytään muun todistusaineiston saastumiselta. (Packt, 2014a)

Valmistautumisvaiheessa (Preparation) tutkijat kartoittavat, mitä työkaluja ja metodeja he tarvitsevat mobiililaitteen tutkimista varten. Valinnat perustuvat mobiililaitteen laitetietoihin, saatavilla oleviin resursseihin, mobiililaitteen tyypin ja tutkimuksen tavoitteisiin. (Packt, 2014a)

Mobiililaitteen eristys (Isolation) on tärkeää, sillä mobiililaitteet ovat jatkuvassa kommunikaatiossa verkkojen kanssa. Näitä ovat muun muassa matkapuhelinverkot, bluetooth ja Wi-Fi. Laite pitää eristää verkosta ennen hankinta- ja tutkimusvaihetta, jolloin laitteeseen ei tule enää uutta dataa eikä siitä pystytä poistamaan tiedostoja etänä. (Packt, 2014a)

Eristäminen voi tapahtua asettamalla laite radiotaajuudelta suojaavaan kankaaseen ja asettamalla laite lentokonetilaan, jolloin laitteen kommunikaatiokanavayhteys otetaan pois päältä. Lentokonetila estää laitteen tietojen poistamisen etäältä, mutta jos laitteeseen ei päästä manuaalisesti sisään tätä ei voida tehdä. (Packt, 2014a)

Vaihtoehtoinen tapa eristää mobiililaite verkosta on käyttää Faradayn pussia (Kuva 2) tai häkkiä. Faradayn pussi estää mobiililaitteen signaalien kulkemisen verkkoon ja sen täytyy pysyä suljettuna. Huomioitavaa on tosin, että kun laite asetetaan Faradayn pussiin se alkaa automaattisesti etsiä yhteyttä verkkoon, joka kuluttaa laitteen virta. Tämän ongelman ratkaisu on laitteeseen kiinnitetty varavirtalähde, joka laitetaan laitteen mukana Faradayn

häkkiin tai pussiin. Ennen pussiin laittoa kannattaa tarkistaa vielä laitteen asetuksista, ettei laite voi mennä suojattuun tilaan. (Gogolin, 2021, ss. 70, 73; Packt, 2014a)

Kuva 2 Faradayn pussi (”Faraday Bag”, 2023)

Eristyksen jälkeen mobiililaitteen tutkinta eli **prosessointi** (Prosessing) voi alkaa. Tiedon hankintavaiheessa hyödynnetään erilaisia menetelmiä ja työkaluja. Usein tutkijat käyttävät useampaa kuin vain yhtä tutkinta menettelemään tietojen keräämiseen mobiililaitteelta, jotta he saisivat mahdollisimman paljon dataa mobiililaitteelta. Esimerkiksi yksi työkalu on täydellinen tekstiviestien louhimiseen, kun taas toinen soveltuu loistavasti sähköpostin seulomiseen. Eri työkalujen käytön tarkoitus on siis täydentää toisiaan. Jos taas mobiililaitteen mukana on löydetty muistikortteja tai muita ulkoisia tallennusmedioita, ne pitää tutkia erikseen, jotta laitteen tietojen eheys ja luotettavuus eivät muuttuisi. (Gogolin, 2021, s. 69; Packt, 2014a)

Tutkijoille on myös erittäin tärkeä selvittää mobiililaitteen käytettyjen toimintojen ja sovellusten mahdolliset aikaleimat ja mahdolliset sijaintitiedot. Nämä tiedot yleensä täydentävät rikosteknisten työkalujen löydöksiä ja selkeyttävät tapauksen tapahtumaketjua. (Gogolin, 2021, s. 76)

Varmistusvaiheessa (Verification) tutkijoiden täytyy varmentaa saadun datan oikeus. Varmentamiseen on olemassa eri tapoja, jotka ovat:

Tutkijat vertaavat saatua dataa alkuperäiseen dataan laitteessa. Tällöin on tärkeää varmistaa, ettei laitteessa oleva tieto ole muuttunut tai tule muuttumaan. Tutkijat voivat käyttää myös useampaa kuin yhtä tutkimusmenetelmää ja näillä vertailla saatua dataa. Tai alkuperäisestä datasta tehdään tiiviste (hash), jota verrataan sitä saadun datan tiivisteisiin, jolloin kaikki mahdolliset muutokset näkyvät heti. (Packt, 2014a)

Keskeisenä asiana prosessin aikana on kaiken mahdollisen tiedon **dokumentointi ja raportointi** (Documenting and reporting). Tutkimuksen päätteeksi tulokset vertaisarvioidaan. Dokumentoinnin kuuluu sisältää vähintään seuraavat tiedot: kuvaus laitteen fyysisestä kunnosta, valokuvat laitteesta ja sen erillisistä osista, laitteen tila hankintavaiheessa, seloste tutkinnassa käytetyistä laitteista, laitteen tunnistetiedot, saadun digitaalisen todistusaineiston seloste ja sen vertaisarviointi. (Packt, 2014a)

Tutkimusraportin esitys (Presentation) on toiseksi viimeinen vaihe prosessissa. Tutkimuksesta ja sen tuotoksista on tehtävä raportti, jonka kuuluu olla selkeä ja yksiselitteinen. Tällöin sitä voidaan hyödyntää oikeudessa ja raportti voidaan esitellä myös muille tutkijoille. Tapauksen kulusta tehdään aikajana, jolla pystytään osoittamaan, mitä milloinkin on tapahtunut. (Packt, 2014a)

Saadun datan säilöminen ja **arkistointi** (Archiving) on viimeinen, mutta tärkeä osa prosessia. Tällöin varmistetaan todistusaineiston saatavuus myöhempää käyttöä varten tulevaisuudessa. Esimerkiksi tekniikoiden ja menetelmien kehittyessä eteenpäin tutkijat voivat suorittaa tutkinnan uudestaan saaden uutta dataa, jota voidaan verrata jo arkistoidun datan kopioon. Myös oikeudenkäynnit voivat kestää vuosia ja tuomioistuimet voivat vaatia todistusaineistojen säilyttämistä puhumattakaan siitä, että syyteenalainen voi valittaa tuomiosta myöhemmin, jolloin tapaus otetaan uudelleen tutkintaan. (Packt, 2014a)

3.2.3 Työkalujen luokitusjärjestelmä

Mobiiliforensiikassa on tapana eritellä ja luokitella sen aihealuetta joko laitteiden teknisten ominaisuuksien mukaan tai millä tavalla tutkinnassa päästään käsiksi laitteessa oleviin tiedostoihin, joka on kaikkein selkein tapa ryhmitellä aihetta. (Årnes, 2018, s. 207)

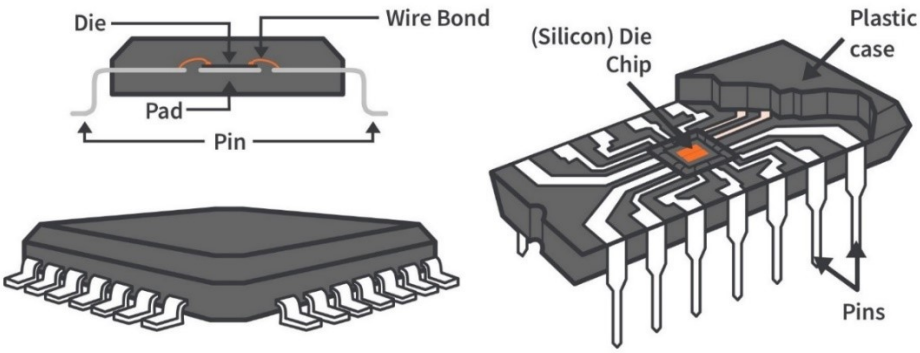
Olemassa on viisi erilaista tapaa eli työkalua, joilla tutkijat saavat tiedot kohdelaitteesta. Nämä ovat manuaalinen menetelmä, looginen menetelmä, hex dumping /JTAG -, chip-off- ja micro read -menetelmä. Menetelmiä usein kuvataan käyttäen pyramidia (Kuva 3), jolloin kaikkein haastavin menetelmä huipulla, mutta samalla lähimpänä kohdelaitteen raakaa dataa. (Årnes, 2018, s. 208)

Kuva 3 Työkalujen luokitusjärjestelmä (*LIGS University*, 2019.)

Manuaalisessa menetelmässä tutkijoilla on pääsy suoraan kohdelaitteeseen sen käyttöliittymän kautta eli esimerkiksi heillä on tiedossa epäillyn puhelimen salasana, jolloin he pääsevät puhelimen sisään suoraan. Loogisessa menetelmässä kohdelaitteelle on jollakin tavalla saatu yhteys rikostekniseltä työasemalta joko langallisesti käyttäen liitäntää laitteiden välillä tai langattomasti esimerkiksi bluetoothia käyttäen, jolloin laitteelle lähetetään komentoja halutun datan saamiseksi siitä takaisin.

Hex Dump/JTAG -menetelmässä tutkijat käyttävät debuggaus käyttöliittymää, jolla luetaan kohdelaitteen raakaa flash-muistia suoraan itse laitteelta. Chip-off menetelmässä kohdelaitteen muistisiru irrotetaan fyysisesti laitteen piirilevystä ja tämä muistisiru luetaan tähän tarkoitukseen erikoistuneilla työkaluilla. Menetelmä vaatii vahvaa osaamista ja tietämystä alasta. Kaikkein vaativin on mikro read menetelmä, jolloin kohdelaitteen mikropiiristä luetaan yksittäisiä portteja silikonisen die-piiristä Kuvassa 4. Tähän menetelmään on olemassa omat erikoistuneet laitteet. (Årnes, 2018, s. 208)

Kuva 4 Mikropiirin osat (*Maestre*, 2021)



Nämä viisi tapaa päästä käsiksi mobiililaitteen dataan voidaan vielä luokitella kolmeen ryhmään perustuen millä metodeilla ne lähestyvät tiedostojen saamista kohdelaitteelta. Nämä luokat ovat yksiselitteisesti manuaalinen taso, looginen taso ja fyysinen taso. Fyysisellä tasolla tarkoitetaan suoraa lukuyhteyttä kohdelaitteen flash-muistiin. (Årnes, 2018, s. 208)

3.3 JTAG

JTAG eli Joint Test Action Group on standardoitu mobiililaitteiden rajaskannaustapa, jolla matkapuhelinvalmistajat muun muassa testaavat piirilevyjen osien toimivuutta ja debuggaavat löydettyjä ongelmia laitteesta laitteen JTAG-käyttöliittymän kautta. JTAG:in kautta on myös mahdollista lukea raakaa flash-muistia prosessorin läpi ja sen avulla voidaan saada myös luettavaksi laitteen haihtuva muistia kuten RAM-muistia. Huomioitavaa kuitenkin on, että laitteen tulee olla päällä menetelmää käyttäessä, sillä menetelmä käyttää prosessoria päästäkseen käsiksi muihin osiin laitteessa. Menetelmän käyttö on myös runsaasti aikaa vievää. (Easttom, 2021, ss. 139–140)

Vaikka menetelmä oli alun perin tarkoitettu mikropiirien, sirujen ja piirilevyjen testaustavaksi, kyseisen menetelmän käyttäjät huomasivat myöhemmin, että tätä voisi hyödyntää rikosteknisissä puitteissa. JTAG:in rajaskannausta käytetään mobiiliforensiikan menetelmänä, koska sillä pystytään ohittamaan puhelimen käyttöjärjestelmä ja kaikki sen mahdolliset suojauskeinot, joihin kuuluvat muun muassa PIN-koodit, salasanat, salasanakuviot ja biometriset tiedot, kuten sormenjälkitunnistus. Eli jos tutkijat eivät pääse laitteeseen sisään manuaalisesti eikä loogista menetelmää voi hyödyntää, heillä on muitakin vaihtoehtoja päästä sisälle kohde laitteeseen. (Easttom, 2021, s. 139)

JTAG-käyttöliittymää on välillä todella haastavaa löytää, koska valmistajat eivät halua ulkopuolisten tahojen tunkeutuvan heidän laiteisiinsa. Monissa laitteissa JTAG on voitu ottaa pois käytöstä tai laitteeseen on lisätty turvakeinoja niin, ettei kuluttajilla ole helppoa pääsyä laitteeseen JTAG-louhintaa käyttäen. Tällöin monet tutkijat käyttävät JTAG sijaan ISP-louhintaa. (Farley, 2019)

3.3.1 Tausta

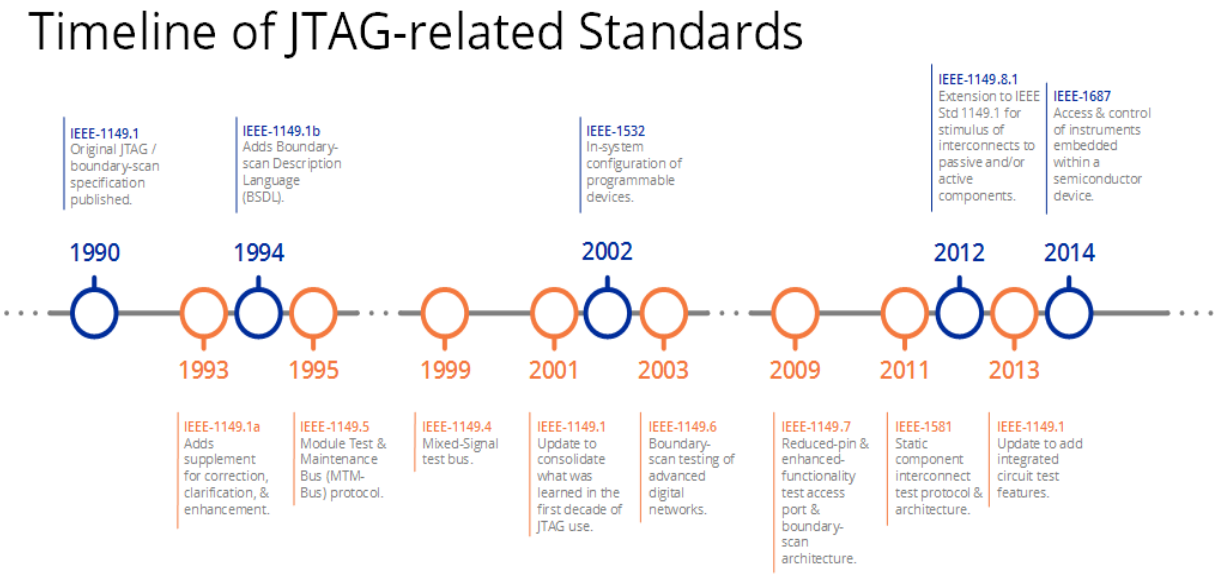
JTAG:in historia alkaa 1980-luvulta, jolloin Joint Test Action Group perustettiin kehittämään spesifiä rajaskannaustestaustapaa mikropiirien, eritoten muistipiirien, testaamiseen ja kehittämiseen. Tämä alkuperäinen menetelmä standardoitiin myöhemmin vuonna 1990 nimellä IEEE Std. 1149.1–1990. Standardi IEEE 1149.1 tunnetaan myös nimillä JTAG-standardi, rajaskannaustesti ja JTAG. (Corelis Jtag, 2013)

Vuosien mittaan standardia on kehitetty eteenpäin alkuperäisen spesifikaation selventämiseksi, korjaamiseksi ja parantamiseksi. Tärkeä täydennys tähän standardiin julkaistiin vuonna 1994, jolloin BSDL, eli Boundary-Scan Description Language, lisättiin standardiin mukaan (Easttom, 2021). Tämä täydennyksen jälkeen standardia on otettu käyttöön globaalisti suurissa elektroniikantuotavissa organisaatioissa.

Perusstandardi, johon sisäistettiin viimeiset kymmenen vuoden kehitykset vuodesta 1990 lähtien, virallistettiin vuonna 2001. Tämänhetkinen standardi IEEE 1149.1 on vuodelta 2013, jolloin pyrittiin parantamaan JTAG:n pääsyä mikropiirien ominaisuuksiin. Tulevaisuudessa JTAG tulee pitämään myös sisällään 3D-piiri (3d-ic), järjestelmätason ja nopean testauksen laajentaen standardia entisestään. (Corelis Jtag, 2013)

Joitakin erillisiä JTAG pohjaisia standardeja on myös julkaistu: nämä lisäävät tiettyjä testausominaisuuksia pohjastandardiin kuten IEEE 1532, joka on standardi ohjelmoitavien laitteiden konfiguroinnille, tai IEEE 1687, joka on vaihtoehtoinen standardi mikropiirien ominaisuuksien käyttämiseksi (Kuva 5.) (Corelis Jtag, 2013)

Kuva 5 JTAG kehityksen aikajana (Corelis Jtag, 2013)



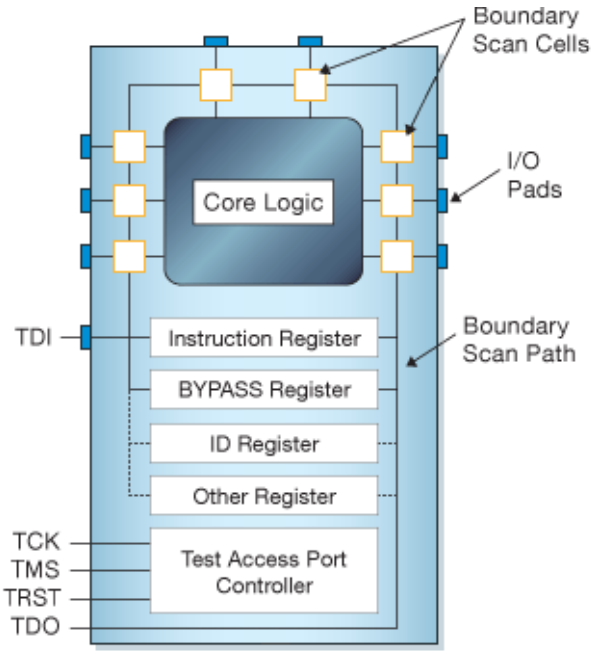
3.3.2 IEEE1149.1 eli määrittelevä JTAG-standardi

IEEE 1149.1 on standardi, joka määrittelee koko JTAG:in. Huomioitavaa on, että tämä standardi ei määrittele, miten JTAG:ia hyödynnetään forensiikassa, mutta antaa kattavan teknisen ymmärryksen JTAG:sta standardina. (Easttom, 2021, s. 137)

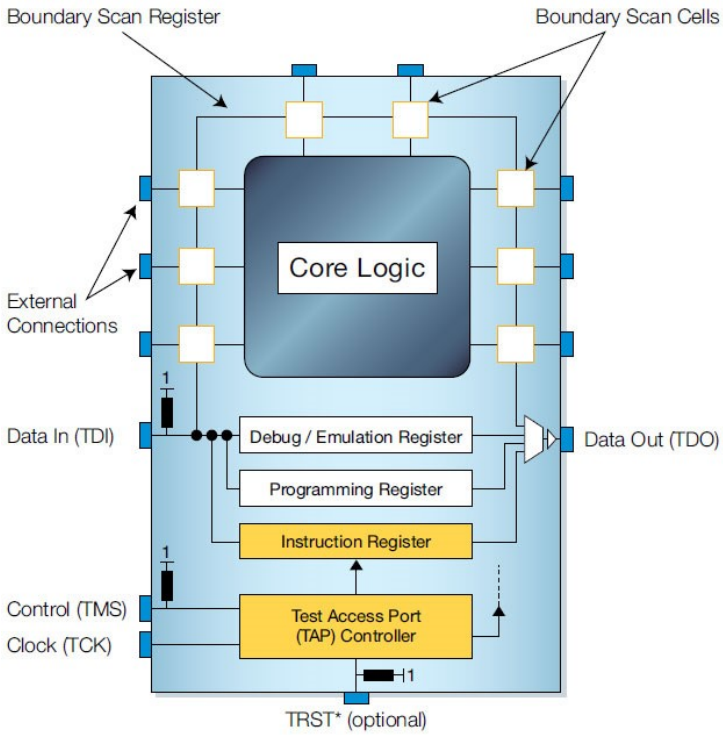
Standardi määrittelee, miten mikropiiri (IC) skannauslogiikan kuuluisi toimia, jotta eri komponenttien, järjestelmien ja testaustyökalujen välinen yhteensopivuus säilyisi. Nämä mikropiirit on kiinnitetty piirilevyyn (PCB) joko nastoilla tai juotinpalloilla. (Corelis JTAG Tutorial, n.d.)

Nämä mikropiirit koostuvat **rajaskannaussoluista** järjestelmälogiikan ja signaalinastojen välillä (Kuva 6 ja Kuva 7.) Jokainen näistä rajasoluista omaa testausominaisuuksia: jotkut solut ottavat vastaan dataa, jotkut lähettävät dataa ulospäin ja jotkut ovat kaksisuuntaisia. Yhdistettynä toisiinsa nämä rajaskannaussolut muodostavat **rajaskannausrekisterin** (BSR), johon päästään käsiksi JTAG-käyttöliittymän kautta. (Corelis JTAG Tutorial, n.d.)

Kuva 6 JTAG-arkkitehtuuri, yksinkertaistettu malli (XJTAG Tutorial, n.d.)



Kuva 7 JTAG-arkkitehtuuri, tarkennettu malli (XJTAG, n.d.)



Standardin mukaisesti **JTAG-käyttöliittymä eli TAP (Test Access Point)** koostuu neljästä signaalista ja yhdestä valinnaisesta palautussignaalista, jotka esitellään Taulukko 1 (Easttom, 2021, s. 143; Årnes, 2018, s. 223).

Taulukko 1 JTAG TAP:sit

PIN	Nimi	Kuvaus
TDI	Test Data In	Käytetään tietojen lataamiseen rajaskannaussoluihin, käskytysrekisteriin tai yhteen tietorekistereistä.
TDO	Test Data Out	Käytetään tietojen lukemiseen rajaskannaussoluista tai käskytys- ja tietorekistereistä
TCLK	Test Clock	Ajastaa valittua tilaa joko TMS HIGH tai TMS LOW bittiä käyttäen niin, että tietyssä valitussa tilassa tilakone etenee (TMS HIGH) tai siirtyy kohti nollaustilaa (TMS LOW)
TMS	Test Module Select	Hallinnoi FSM, josta valitaan käskytila tai datatila.
TRST	Test reset	Pakottaa FSM:än käynnistymään uudelleen.

TAP on ensisijainen liitäntä JTAG-testiohjaimeen, jolla on pääsy laitteen sisäiseen ydinlogiikkaan. Signaalit näkyvät **rajaskannausrekisterissä eli BSR:ssä**. BSR toimii päärekisterinä rajaskannaussoluihin kulkevalle tiedolle. **Siirtorekisteri** yhdistää TDI:n ja

TDO:n ilman, että joutuisi kulkemaan BSR:n kautta. (Gallagher, 2020.; Corelis JTAG Tutorial, n.d.)

Standardiin kuuluvat myös **käskyt**, joita kaikkien JTAG-menetelmää mukailevien laitteiden pitää noudattaa jossain muodossa. Nämä käskyt esitellään Taulukko 2. (Corelis JTAG Tutorial, n.d.)

Taulukko 2 JTAG-käskyt

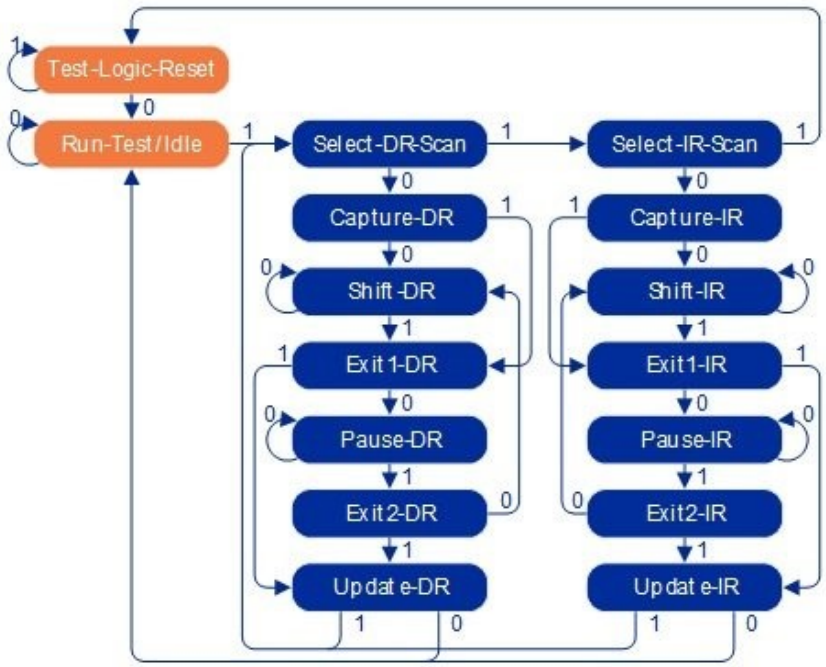
Nimi	Kuvaus
EXTEST	Käskyä käytetään kytkennän testaamiseen eli käsky suorittaa ”ulkoisen” rajaskannaustestauksen käyttäen rajaskannaussoluja. ”Ulkoisessa” testitilassa rajaskannauksen ulosottosolut ohjaavat testitietoa laitteen nastoihin ja syöttösolut keräävät tietoa laitteen nastoista.
SAMPLE/PRELOAD	Käskyä käytettäessä laite suorittaa rajaskannauksen samalla, kun laite pysyy toimintakunnossa.
BYPASS	Käsky lyhentää rajaskannausketjun pituutta eliminoimalla kaikki laitteet, joita ei tarvita kyseisen toiminnan aikana. Käyttää siirtorekisteriä toiminnon suorittamiseen.

Näiden komentojen lisäksi on olemassa muita suositeltuja standardoituja käskyjä kuten IDCODE, CLAMP/HIGHZ, IC_RESET, mutta myös vaihtoehtoisia käskyjä kuten RUNBIST, INTEST ja USERCODE. Yleisesti kuvailtuna käskyt yhdistelevät eri tietorekistereitä TDI/TDO polulle. (Gallagher, 2020.)

Käskytysrekisteri (Instruction Register eli IR) on rekisteri, joka sallii TAP ohjaimen toiminnan siirtorekistereihin, rajaskannausrekistereihin ja muihin rekistereihin käyttäen eri käskyjä. IR suorittaa myös sille annetut käskyt. (ScienceDirect Topics, n.d.)

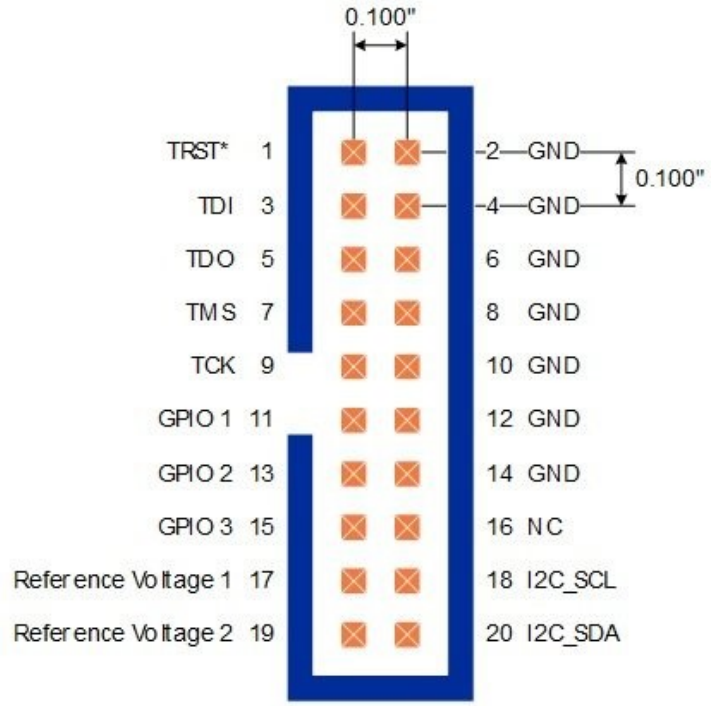
JTAG-arkkitehtuurin keskeinen osa on **TAP-ohjain**. Tämä ohjain on FSM (Finite-state machine) eli äärellinen automaatti, joka pitää kirjaa siitä, mitä käskyjä lähetetään JTAG-porteille. Ohjain hallitsee siirtymätapahtumien ajoitusta ja pysäytystä sekä hallitsee tiedonkulkua rinnakkaisrekisterien ja ohjaus- ja tietorekisterien siirtorekisterien välillä. FSM sisältää kuusitoista eri tilaa (Kuva 8), joita hallitsevat TCK ja TSM signaalit. (Corelis JTAG Tutorial, n.d.)

Kuva 8 JTAG TAP -ohjaimen diagrammi (Corelis JTAG Tutorial, n.d.)



JTAG-yhdistäjälle (Kuva 9) ei ole olemassa vain yhtä standardia, kuten ei myöskään sille, minne JTAG-käyttöliittymä on aseteltu piirilevyllä. Olemassa on lukuisia tapoja kiinnittää mobiililaite flasher boxiin, ja monessa yhdistäjä on flasher boxissa kiinni. Yleensä yhdistäjä on perinteinen male header -pistoke (Kuva 10.) Laite, joka kommunikoi JTAG-käyttöliittymän kautta, tarvitsee 4–5 TAP:in lisäksi virtaa ja maadoituksen. Yhdistäjät käyttävät usein tiedossa olevia suosittuja nasta-asetelmia, kuten ARM-20 tai ARM-14, joita löytyy tietyiltä sivustoilta kuten esimerkiksi ”jtagtest.com.” (Gallagher, 2020.)

Kuva 9 Tyypillinen JTAG-yhdistäjän malli (Corelis JTAG Tutorial, n.d.)



Kuva 10 JTAG-yhdistäjä, moduuliadapteri (*ModJTAG - JTAG Connector Adapter Module*, n.d.)

3.3.3 JTAG toiminta käytännössä

Kuten aikaisemmin mainittu, JTAG-arkkitehtuuri on kehitetty alun perin testaamaan piirilevylle asetettuja mikropiirien välisiä liitäntöjä ilman vaivalloisia testiantureita. Testaus JTAG:illa vähentää myös kustannuksia ja antaa parempaa diagnostiikkaa laitteesta kuin vanhemmilla testimenetelmillä. (Corelis ”What is JTAG?”, 2023)

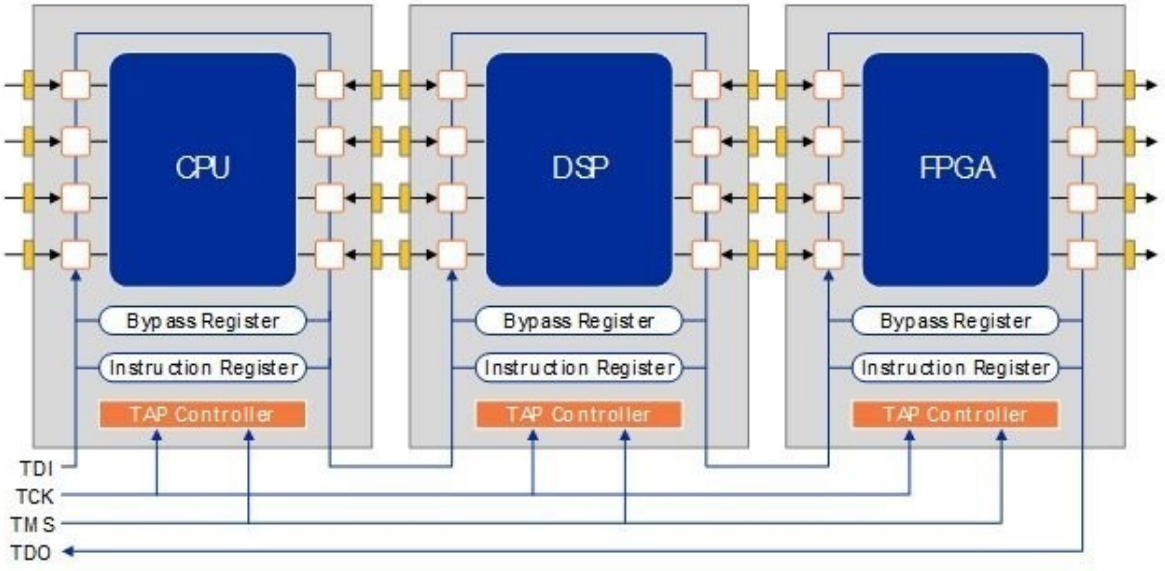
Rajaskannaussolut toimivat kahdessa tilassa: normaalitila ja testitila. JTAG-käyttöliittymästä suoritetaan näitä testejä ja hallinnoidaan datan kulkua rajasoluille. **Rajaskannaus** tapahtuu käyttäen sarjatietopolkua, jota kutsutaan tarkistuspoluksi tai tarkistusketjuksi. (”Corelis What is JTAG?”, 2023)

TAP TDI lähetetään dataa tarkistuspolun kautta rajaskannaussoluihin, josta tieto kulkeutuu rajasolusta rajasoluun tarkistuspolkua pitkin. Rajaskannauksessa pystytään lukemaan arvo suoraan rajasolun ulkoiselta I/O eli Input/output -piiriltä. Nämä arvot kaapataan ja siirretään tarkistuspolkua pitkin sarjassa JTAG-käyttöliittymän TDO kautta ulos, jolloin niitä voidaan vertailla odotettuihin arvoihin. Vertailussa tulos on joko hyväksytty tai hylätty, ja näin testaajat pystyvät löytämään toimimattomat piirit.(EEVblog, 2013; Corelis ”What is JTAG?”, 2023)

Rajasoluille voi myös antaa arvoja suoraan. Tällä ominaisuudella voi esimerkiksi testata ulkoista muistia, jonka osat ovat asetettu rajasolujen eri I/O-nastoihin rajaskannausta varten. Rajaskannausta voi myös käyttämään lukemaan ”live dataa” laiteohjelmiston ollessa toiminnassa ja havainnoida, miten arvot muuttuvat rajasoluissa. (EEVblog, 2013)

Rajaskannauksella on käytössä kaksi päätestiä piirilevyntestaamiseen. Koko piirilevyntestaamiseksi JTAG omaavat mikropiirit voidaan ketjuttaan toisiinsa TDI:n ja TDO:n kautta (Kuva 11), ja ne jakavat TLCK, TMS ja TRST sisään tulevan datan. (Årnes, 2018, s. 222)

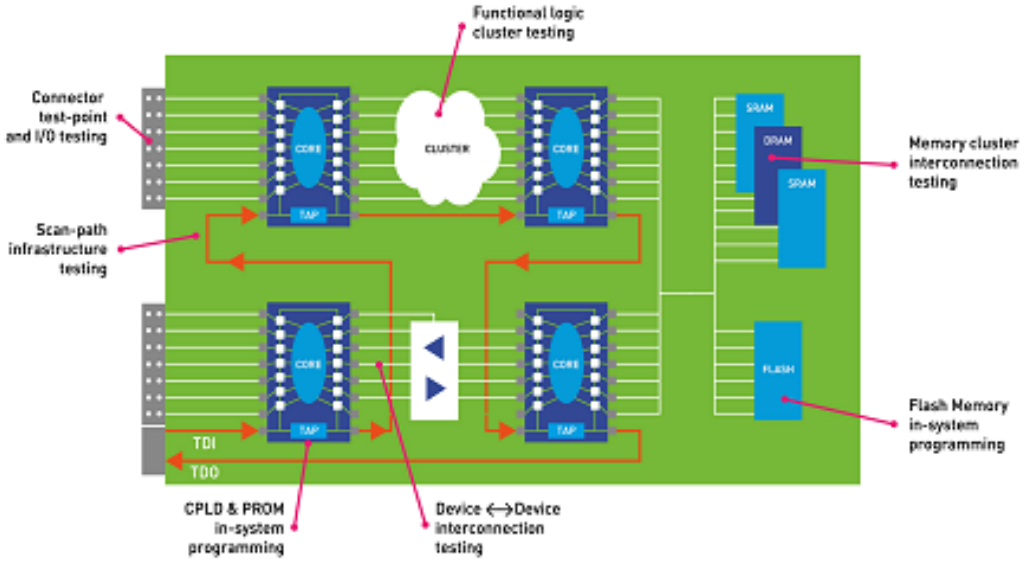
Kuva 11 Rajaskannauksen ketjutus (Corelis JTAG Tutorial, n.d.)



JTAG-liitäntätestillä tarkistetaan, että laitteen piirilevyn yhteydet ja liitännät ovat samat kuin määritellyssä piirisuunnittelussa. JTAG-liitäntätestissä eli yhteenkytkentätestissä kaksi rajaskannaukseen yhteensopivaa piirilevynlaitteita on yhdistetty neljällä ”verkolla” toisiinsa. Laite A sisältää neljä lähtöpaikkaa, josta lähtee neljä ennalta määrättyä arvoa laitteeseen B. Tällä tavalla vian voi havaita helposti, jos joku neljästä ”verkosta” ei vastaa oikein takaisin. (Corelis ”What is JTAG?”, 2023)

JTAG tukee myös järjestelmän sisäistä ohjelmointia (ISP), piirin sisäistä emulointia (ICE) ja muita testausominaisuuksia. Myös flash-muistin lukeminen ja ohjelmointi onnistuvat JTAGin kautta, kun käyttöliittymä keskustelee CPU:n kautta flash-muistille (Kuva 12.) Standardi huomioi myös laitekohtaiset käskyt ja rekisterit, joita voidaan käyttää lisäominaisuuksina, kun mikropiirejä testataan tai tutkitaan. (Corelis ”What is JTAG?”, 2023)

Kuva 12 Rajaskannauksen yleiskatsaus piirilevyllä, ketjutettu (”Boundary-Scan”, n.d.)



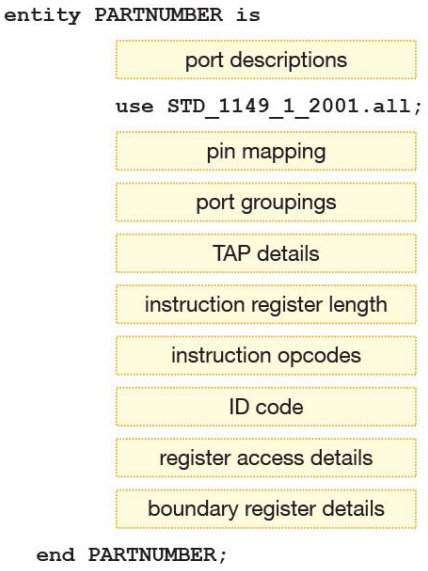
3.3.4 BSDL - Boundary-Scan Description Language

BSDL on laitteistoa kuvaava kieli, jota käytetään elektroniikan testaukseen JTAG:issa. Se antaa käyttäjälle kuvauksen laitteen tärkeistä ominaisuuksista, joilla rajaskannaustestaus suoritetaan onnistuneesti (Kuva 13.) (Easttom, 2021, s. 141)

Näitä ovat laitteen rajaskannaus funktioiden ominaisuudet kuten mitä JTAG-standardeja tuetaan kyseisessä laitteessa, mitkä rajaskannaussolut yhdistyvät mihinkin nastaan, laitteen TAP:it ja saatavilla olevat käskyt ja mihin rekistereihin niillä on pääsy. Myös piirin suunnitteluhuomautukset käyvät ilmi BSDL tiedoston kuvauksesta.

BSDL-formaattia on myös laajennettu pitämään sisällään muun muassa proseduraalisen kuvauskielen (PDL) ja tietoja elektronisen piirin tunnisteesta (ECID). (Corelis JTAG Tutorial, n.d.)

Kuva 13 BSDL-tiedoston pääelementit (XJTAG, n.d.)



Kieli on olemassa standardoituna, koska jokaisella piirilevyllä on oma piirilevysuunnittelija, joka soveltaa rajaskannausstandardia hieman eri tavalla. Täten etenkin TAP:sit on ilmaistava ymmärrettävällä, yksiselitteisellä ja käyttökelpoisella tavalla, jotta yhtenäisyys säilyy laitteesta riippumatta. (Corelis BSDL Tutorial, 2016)

Alun perin BSDL oli tarkoitettu olemaan vain osa VHSIC Hardware Description Language:n (VHDL), joka on laitteistokuvauskieli, alijoukkoa. Sittemmin BSDL formaattia on laajennettu muilla piirteillä ja näin se ei ole enää tiukasti VHDL vaatimustenmukainen. VHDL on ohjelmistokieli, joka kuvaa laitteiston toimintaa ja rakennetta tekstimuotoisesti. Sitä käytetään esimerkiksi ohjelmoitavien porttimatriisien ja sovelluskohtaisten integroitujen piirien (ASIC) laitteiston kuvauskielenä, mutta kieli soveltuu myös rajatusti rajaskannaukseen sillä, se määrittelee myös piirejä. (Corelis JTAG Tutorial, n.d.)

3.4 JTAG-louhinta

Tutkinta alkaa **mobiililaitteen purkamisella.** Purkaminen on täysin riippuvainen mobiililaitteen mallista ja valmistajasta, joten on erittäin suositeltavaa hyödyntää internetistä löytyviä purkuohjeita. Laitteen purkuvaiheessa on suositeltavaa käyttää turvalaseja ja muita tarpeellisiksi todettuja turvavälineitä. Matkapuhelimen akkua käsiteltäessä on noudatettava varovaisuutta, koska vahingoittunut litiumioniakku voi pahimmassa tapauksessa pullistua ja syttyä tuleen tai räjähtää. JTAG-louhinta menetelmän käyttö alkaa heti mobiililaitteen purun jälkeen.

Ensimmäisenä **etsitään TAP:sit eli JTAG-käyttöliittymä piirilevyltä**. Eri mobiililaite merkkien ja mallien TAP merkinnät ovat löydettävissä internetistä, etenkin vanhempien mallien laitteiden. Joskus TAP:sit on merkattu selkeästi tekstillä, ei kuitenkaan aina, ja ne ovat yleensä joko 5–6 nastan rivissä tai kahdessa rivissä, jossa on 10–20 nastaa. Kun mahdolliset TAP kandidaatit on löydetty piirilevyltä, tutkijat voivat hyödyntää yleismittaria tarkempien TAP:sien varausten kartoittamiseen ja verrata löydöksiä suosituimpiin TAP mallinuksiin. Tutkijat voivat myös hyödyntää Jtagulator työkaluja TAP:sien löytämiseen. (Make Me Hack, 2020)

Löytämisen jälkeen **hyppylangat** sijoitetaan ja juotetaan kiinni haluttuihin kohtiin JTAG-adapteriin ja TAP:seihin mobiililaitteessa (CFTT, 2019.). Tämä on usein haastavaa ja pikkutarkkaa työtä muun muassa siksi, että nastat ovat pieniä. Juotettaessa vaijereita kiinni tinalla tulee käyttää suojavälineitä kuten aikaisemmin mainittuja suojalaseja ja käsitellä varoen kuumaa juotinkolvia.

Tämän jälkeen **JTAG-adapteri kiinnitetään flasher boxiin**. Flasher boxin tulee olla tutkimuksen suorittavassa tietokoneessa kiinni ennen tietokoneen päälle laittoa, näin flasher -ohjelma havahtuu boxin läsnäoloon. **Piirilevyyn kytketään virrat päälle,** jotta prosessori alkaisi toimia. Monien osien toiminnot piirilevyllä ovat riippuvaisia prosessorista. (CFTT, 2019.)

Tärkeä osa tutkimusta on testata louhinnassa käytettävä flasher box ennen kuin sitä aikoo käyttää tutkittaviin laitteisiin. Tutkijoiden tulee tietää, miten flasher työkalu toimiin ja ettei

sen toiminnassa löydy virheitä. Näin tutkijat eivät tietämättään paina väärää nappulaa, joka voisi yli kirjoittaa tietoja tai palauttaa tehdasasetukset kohdelaitteelle. (Årnes, 2018, s. 237)

Flasher -ohjelmaa käyttämällä tutkijat aloittavat muistin louhinnan mobiililaitteesta ja luovat tästä flash-muistin datasta **muistidumpin tai binäärikuvan**. Tämä voi viedä paljon aikaa, koska ohjelma käy läpi kaikki mahdolliset tiedot flash-muistista. Ei ole yllättävää, että louhinta venyy yli viiteen tuntiin. Louhinnan jälkeen tutkijat pääsevät **tutkimaan louhittua dataa** ja analysoimaan sitä mahdollisilla lisälaitteilla. (Joe Grand, 2018)

Täytyy kuitenkin huomioida, ettei JTAG:in käyttö ole helppoa etenkään nykyaikaisissa mobiililaitteissa, sillä monet valmistajat ovat tunnistaneet nämä selkeiksi hyökkäysalustoiksi laitteisiinsa. Näin ollen laitetestaaja on voinut ottaa JTAG:in kokonaan pois käytöstä laitteetta tai se on suojattu muulla tavoin ja piilotettu ulkopuolisilta tahoilta. Esimerkiksi Apple-laitteissa JTAG ei toimi ja ne tarvitsevat usein juuri iOS:iin erikoistuneet flasher työkalut Apple-laitteiden korjaamiseen. JTAG-käyttöliittymän voi yrittää ottaa käyttöön uudelleen, mutta monesti tämä epäonnistuu. Tämän takia monet tutkijat käyttävät ISP-louhintaa, jos JTAG-louhinta ei ole mahdollista suorittaa. (says, 2019)

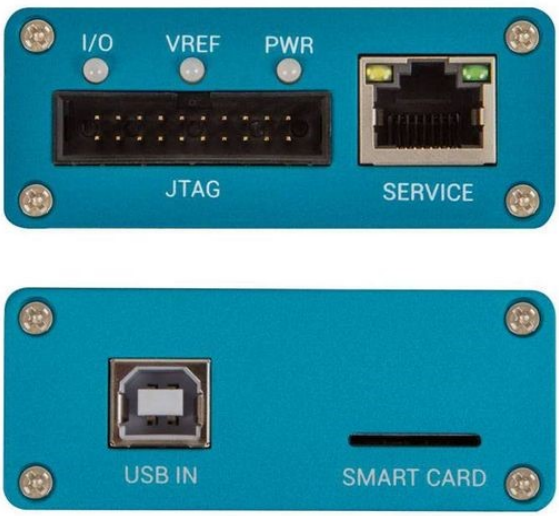
3.4.1 Flasher Box

Yleensä nämä laitteet ovat tarkoitettuja puhelinkorjausliikkeiden käyttöön. Nämä liikkeet eivät ole varsinaisia virallisia palvelukeskuksia (Årnes, 2018, s. 237). Huomioitavaa siis on, ettei kaikkia flasher-työkaluja voi välttämättä hyödyntää mobiiliforensiikassa, sillä jotkin niistä voivat olla kehitettyjä jotain sellaista tarvetta varten, joka eriää mobiiliforensiikan tarpeista.

Flasher boxit (Kuva 14) ovat metallisia laatikon mallisia laitteita, joissa on merkkivaloja ja sekä portteja. Flash boxi on kooltaan yleensä noin kymmenen senttimetriä leveä ja noin viisitoista senttimetriä pitkä. (GSMServer, 2017)

SERVICE eli SERVICE CABLE -porttia käytetään liittämään mobiililaitteita COM (UART) liittymän kautta flasher boxiin. JTAG-portti yhdistää laitteet toisiinsa käyttäen JTAG-käyttöliittymään. Flasher boxit käyttävät yleensä USB IN-porttia ja USB-liitintä, jolla ne ovat kytkettyinä tietokoneeseen, virtajohtona, jolloin ylimääräistä virtajohtoa ei tarvita. Osassa flash boxeja on myös paikka toimikortille ja USB HUB -portti, jolla boxi kiinnitetään muihin USB-laitteisiin, kuten muistitikkua muistuttavat donglet. USB HUB- portti ei ole tarkoitettu puhelinhuoltotoimenpiteisiin. Toimikortteja taas käytetään monesti estämään ohjelman luvatonta käyttöä ja niillä kehittäjät pystyvät tunnistamaan laitteen heidän ohjelmiensa palvelimilta. (GSMServer, 2017)

Kuva 14 Flasher boxin tyypilliset piirteet (GSMServer, 2017)



Flasher boxeja on harvoin ostettavissa verkkokauppojen ulkopuolelta ja lisäksi tulee myös suhtautua varauksella verkkosivustojen tarjontaan: liian sinisilmäinen ei pidä olla. Luotettavimmat ja toimintavarmimmat boxit ovat ostettavissa joko valmistajan omilta verkkosivuilta tai valmistajan käyttämien luotettavien jälleenmyyjien verkkosivuilta.

Aidon ja luotettavan flasher boxin tunnistaa muun muassa siitä, että laitteella on selkeä sarjanumero, ja kyseessä on tunnettu merkki ja malli, joka on laajasti käytössä. Tällöin näille tuotteille on myös saatavilla tukea käyttäjäfoorumeilta kuten myös valmistajan sivuilta. Laadukkaalle tuotteelle myönnetään myös asianmukainen takuu. Laadukkaan tuotteen merkkinä on myös se, että kyseisiä laitteita käytetään laajasti muun muassa mobiiliforensiikassa tai puhelinkorjausliikkeissä. (Al-Zarouni, 2007, s. 3)

Flasher boxien tunnettuja malleja ovat muun muassa RIFF Box (Kuva 15), Octoplus Box Pro (Kuva 16), ORT Box ja Easy JTAG Box (Kuva 17.) (Easttom, 2021, ss. 145–147)

Kuva 15 RIFF boxit ovat laajasti käytössä olevia flasher boxeja ja luotetumpia työkaluja (*Riff Box 2*, n.d.)

Kuva 16 Octoplusbox Pro on uusin flasher box Octoplusbox tiimiltä, jotka tekevät jatkuvaa työtä palvelun kehittämiseksi (GSMServer, n.d.)

Kuva 17 Easy JTAG box, mahdollisesti tunnetuin ja luotetuin flasher box markkinoilla, jolla on tiettyjä lisäominaisuuksia Samsung laitteita varten (*Z3X Easy-Jtag Plus Full Upgrade Set*, n.d.)

On olemassa monenlaisia flasher työkaluja ja usein ne pystyvät käsittelemään monenlaisia mobiililaitteita. Jotkin flasher boxit ovat rajoitettuja mobiililaite tyyppi-, malli- ja/tai valmistajakohtaisiksi (Kuva 19), joten ennen ostopäätöksen tekoa on aina parasta tarkistaa mihin kaikkiin laitteisiin työkalu on yhteensopiva (Kuva 18.) (GSMServer, 2017)

Kuva 18 Tuotteen Octoplus Pro Box with 7 in 1 Cable/Adapter Set (Activated for Samsung + LG + eMMC/JTAG) yhteensopivat puhelinmerkit (GSMServer, n.d.)

Box is compatible with the following models of Cell phones	ZTE Alcatel LG Samsung Sony Sony Ericsson

Kuva 19 IP-Box2 oli flasher työkalu iPhonien ja iPadien korjaamiseksi, mutta työkalun valmistus on jo lopetettu (GSMServer, n.d.)

Usein flasher boxit tarvitsevat aktivoinnin toimiakseen, joka on yleensä uniikki koodi, jonka käyttäjä kirjoittaa flasher boxin käyttöohjelmaan asennusvaiheessa. Tämä riippuu kyseisen tuotteen valmistajasta. (Octoplus Support, 2014)

Laiteiden mukana tulee usein myös setti erilaisia kaapeleita ja tarvittavia osia toimintojen suorittamiseen mobiililaitteelle, mutta on aina hyvä varmistaa flash boxin koko tuotekuvaus ennen lopullista ostopäätöstä. (GSMServer, 2017)

Riippuen käyttötarkoituksesta ja ominaisuuksista boxien hinnat vaihtelevat yleensä 100 eurosta noin 500 euroon, jolloin flasher boxit ovat edullisemmasta päästä mahdollisista mobiiliforensiikan laitteista puhuessa. Kustannustehokkuutensa vuoksi flasher boxit ovat etenkin pienille rikosteknisille yrityksille hyvä hankinta muiden tutkimuslaitteiden rinnalle. (Guarino, 2011)

Flasher boxeilla voi avata operaattoreiden rajoittamien laitteiden lukituksia tai kirjoittaa myös laiteohjelmiston yli, lisäämällä muun muassa ominaisuuksia, kuten kieliä, joita laite ei alun perin olisi tukenut. Myös SIM-kortin rajoitusten avaaminen on mahdollista, tosin vain vanhemmissa matkapuhelinmalleissa. (Guarino, 2011)

Tärkein omaisuus, etenkin mobiiliforensiikan ja korjausliikkeiden näkökulmasta, on flash boxien kyky lukea flash-muistia laitteelta antaen näin mahdollisuuden palauttaa laitteen muistin. (Årnes, 2018, s. 237)

Flasher boxeilla voi myös ylikirjoittaa mobiililaitteen IMEI-koodia (International Mobile Equipment Identity), joka on uniikki 15 numeromerkin sarjanumero, jolla mobiililaite tunnistetaan verkosta. Varjopuolena tähän mahdollisuuteen liittyy sen väärinkäytön mahdollisuus, koska IMEI-koodin muutos vaikeuttaa puhelimen jäljitettävyyttä. (Al-Zarouni, 2007, s. 3)

Vaikka JTAG-louhinta on pääasiassa puhelinkorjausliikkeiden ja mobiiliforensiikan tutkijoiden käytössä, voi tätä silti soveltaa rikollisiin toimiin. Teoriassa kuka tahansa pystyy ostamaan internetin verkkokaupasta flasher työkalun ja käyttämään sitä esimerkiksi varastettuihin mobiililaitteisiin lukeakseen niiden flash-muistin tai palauttaakseen laiteiden tehdasasetukset.

3.4.2 Flasher Box -ohjelmat

Flasher boxin käyttöön tarvitaan laitekohtaiset käyttöohjelmat, joka ovat usein ladattavissa valmistajan omilta verkkosivuilta. Ohjelmat asennetaan louhinnan suorittavaan tietokoneeseen, joka kytketään kiinni flash boxiin. On kuitenkin myös huomioitava, että jotkut ohjelmat ovat yhteensopivia tietyille tietokoneen käyttöjärjestelmille, kuten esimerkiksi vain Windows -käyttöjärjestelmille. (Octoplus Box, n.d.)

Jotkut ohjelmat tarvitsevat myös toimivan internet yhteyden toimiakseen ja flash boxin päivitysten ylläpitämiseen (Al-Zarouni, 2007, s. 3).

Ohjelmilla on usein tyypillinen graafinen käyttöliittymä, jossa on erilaisia painikkeita ja valintoja eri toiminnoille, esimerkiksi IMEI-koodin korjauspainike tai flash-muistin jäsentelypainike.

Valmistajat tarjoavat usein tiettyyn tarkoitukseen tehtyjä ohjelmia, kuten FRP ohjelman tai JTAG-ohjelman. Yleensä kuitenkin FRP ohjelmat ovat lukittuna ostettavien krediittien takana, joita käytetään eri ominaisuuksien käyttämiseen ohjelmassa, esimerkiksi TMB/SPCS koodin purkamiseen tietyiltä mobiililaite malleilta. (Octoplus Box, n.d.)

On todella yleistä, ettei flash boxin mukana tule manuaalisia ohjeita, vaan itse ohjelman käyttöön ohjeet löytyvät valmistajan sivuilta. Suositeltavaa on käyttää hyödykseen tuotteeseen keskittyneitä foorumeita ja mahdollisia ohjevideoita, joita löytyy internetistä.

3.5 JTAG-louhintaan liittyvät aiheet

JTAG-menetelmä on sidoksissa muihin aiheisiin ja sitä sivuaa useita aiheita, jotka täydentävät tutkijoiden tietämystä mobiiliforensiikasta ja JTAG-työkalujen käytöstä. Näitä ovat muun muassa ISP-louhinta, flasher donglet ja chip-off-menetelmä.

3.5.1 ISP-louhinta vaihtoehtona JTAG-louhinnalle

ISP-louhinta muistuttaa paljon JTAG-louhintaa tavalla, jolla mobiililaitteen muistiin ja tietoihin päästään laitteen piirilevyn kautta juottamalla johdot haluttuihin nastoihin. ISP on järjestelmän sisäistä ohjelmointia, jota toisinaan kutsutaan sisäiseksi sarjaohjelmoimiseksi (ICSP). ISP käyttäen ohjelmoidaan piirilevyn eri ominaisuudet niiden asennuksen jälkeen. Sitä voi hyödyntää myös laiteohjelmistopäivitysten toimittamiseen mikro-ohjaimiin ja niihin liittyvien prosessorien muistiin. ISP kommunikoi erilaisten mikropiirien kanssa. (Farley, 2019; ”In-System Programming”, 2023)

ISP väistää laitteen suojaukset kuten JTAG, mutta se ei pysty purkamaan laitteen salausta, ja ISP käyttöön tarvitaan flasher box tai muu flasher työkalu. On haastavaa löytää oikeat, pienet nastat laitteen piirilevyltä, sillä tähän ei ole olemassa standardia, jota kaikkien mobiililaitevalmistajien kuuluisi noudattaa. Internetistä löytyy monia referenssejä erilaisille mobiililaitemallille ja -versiolle. Nämä ISP nastat ovat usein paljon pienempiä kuin JTAG:in TAP:sit, jolloin louhijoilla on käytössään hienovaraisempi juotoskolvi ja mahdollisesti myös suurennuslasi. (Farley, 2019)

ISP nastat ovat: **Data 0** eli konfiguraatioon tarvittava I/O nasta, joka pääasiallisesti toimii datan syöttö nastana, **CLK** eli kello, joka ajastaa toimintaa, **CMD** eli annettava komento nasta, **GND** eli maadoitus, **VCC** noin 2.8 – 3.3 Volt ja **VCCq 1.8 Volt**. Volttinastat antavat virtaa muille nastoille toiminnon suorittamiseksi ja luovat tarvittavat käyttöliittymät eMMC:lle. (Farley, 2019)

3.5.2 Flasher Donglet lyhyesti

Olemassa on myös flasher dongleja (Kuva 20), joita käytetään mobiililaitteiden korjaamiseen. Flasher box valmistajat myyvät myös näitä boxien ohella. Flasher dongleilla voi purkaa, ylikirjoittaa tai korjata laitteen IMEI-koodin tai poistaa FRP:in (Factory Reset Prevention) eli tehdasasetusten eston, joka on käytössä Android-laitteilla. On myös olemassa dongleita, jotka ovat kehitetty tiettyä tarkoitusperää kuten FRP:in poistoa varten. (GSMServer, 2017)

Kuva 20 Octoplus Samsung dongle (GSMServer, 2017)

3.5.3 Chip-off menetelmästä lyhyesti

Chip-off menetelmällä, kuten JTAG-louhinnalla, pystytään lukemaan tietoja suoraan mobiililaitteelta ohittaen samalla käyttöjärjestelmän ja kaikki mahdolliset suojauskeinot, joita laitteella on. Usein chip-off menetelmä voidaan mieltää niin sanotusti lisäominaisuutena JTAG:ia suorittavalle flasher boxille, vaikka käytännössä se eritellään omaksi mobiiliforensiikan menetelmäksi (Easttom, 2021, ss. 148–149). Toisin kuin JTAG-louhintamenetelmässä, chip-off menetelmässä kohdelaite yleensä romuttuu käyttökelvottomaksi muistipiirin irrottamisen aikana. (Årnes, 2018, s. 246)

Chip-off on haastava mobiiliforensiikan menetelmä, sillä se vaatii käyttäjältä laajaa tietotaitoa, kehittyneitä resursseja, laitteita ja paljon aikaa. Menetelmä edellyttää myös, että käyttäjä käyttää tietolomaketta muistimoduuleista. (Årnes, 2018, s. 246)

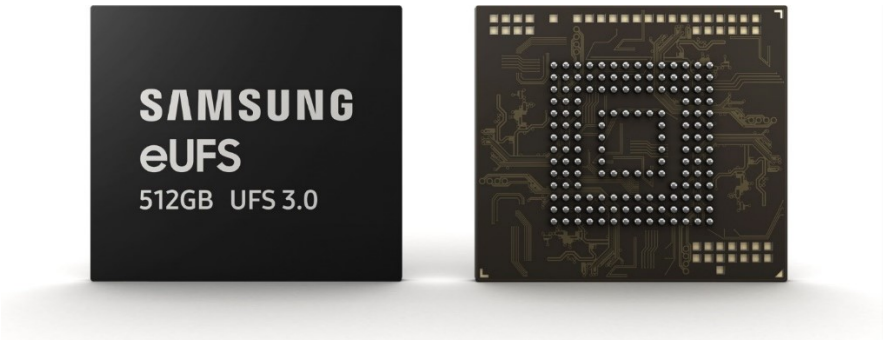
Muistipiirit ovat usein pakattuina piirilevyyn käyttäen juotepalloverkkosarjaa (BGA), jolloin juotekohdat ovat juotekynän ulottumattomissa muistipiirin alla (Kuva 22), tai TSOP:ia (Thin

Small Outline Package), jolloin muistipiiri on pinta-asennettu juottamalla muistipiirin ”jalat” kiinni piirilevyyn (Kuva 21.) (Årnes, 2018, s. 216)

Kuva 21 TSOP mikropiiri (Simms International plc, 2019.)

Toisin kuin JTAG-louhinnassa, muistipiirit pitää irrottaa kokonaan piirilevystä, jotta niiden flash-muisti voidaan lukea. Jos TSOP:in haluaa irrottaa laitteesta, tutkijan pitää poistaa ”jalkojen” juotos ja samalla olla rikkomatta niitä. BGA tyylisen muistipiirin irrottaminen mobiililaitteesta on usein hyvin hellävarainen ja työläs prosessi. (Årnes, 2018, s. 216)

Kuva 22 BGA mikropiiri (Samsung Newsroom, 2019)



Ensimmäinen vaihtoehto BGA-muistipiirin irrottamiseen on käyttää juotetyöasemaa, mutta tällöin täytyy huomioida mahdollisuus, että jotkin piirilevyn komponentit voivat vaurioitua. Toinen vaihtoehto on leikata muistipiiri irti piirilevystä ja hioa varovasti jäljelle jäänyt piirilevyn pois muistipiirin alta tähän erikoistuneella koneella, kunnes juotepallot tulevat näkyviin. (Årnes, 2018, ss. 217–218)

Seikka, joka yhdistää JTAG-louhinnan ja chip-off menetelmän on, että molemmat käyttävät hyödykseen flasher-työkaluja flash-muistin lukemiseen. Tavanomaisella flasher boxille on

olemassa lisäosia (Kuva 23), joilla pystytään lukemaan eMMC ja UFS tyyppisiä BGA-muistipiirejä, ja näille on olemassa erillisiä ohjelmia muistipiirien lukemiseen. (Årnes, 2018, s. 238)

Kuva 23 Flasher työkalun lisäosa, chip -lukija (*UFS socket 254/153/95 for Easy jtag plus box*, n.d.)

Olemassa on myös täysin muistipiireihin erikoistuneita rikosteknisiä laitteita kuten Alankomaiden rikostutkinnan laitoksen MTK (Memory Toolkit) -laite (Kuva 24.) Nämä laitteet ovat ainoastaan viranomaisten käytössä ja ne ovat optimoitavissa monenlaisille muistipiireille. (Årnes, 2018, s. 220)

Kuva 24 MTK laite Alankomaiden rikostutkinnan laitoksessa (Veiligheid, 2017)

4 Matkapuhelimien JTAG-louhinta

Ennen louhinnan alkua on syytä tutustua paremmin flasher boxiin ja flasher ohjelmaan. Tähän kuuluu aina myös työkalujen testaus, joten tulen testaamaan käytössä olevan flasher boxin ja sen käyttöohjelma.

Testilaitteena toimi Samsung J5 (SM – J500FN) (Kuva 25), jonka näyttö on mennyt rikki. Purkamisen aikana huomattiin, ettei laitteessa ole näkyvillä JTAG-käyttöliittymää. Laitteessa on yksi mahdollinen kohta, joka saataisi olla JTAG-käyttöliittymä, mutta tästä osasta ei löytynyt tietoa internetistä. Jouduttiin siis käyttämään ISP-louhintaa flasher boxin testaamiseksi.

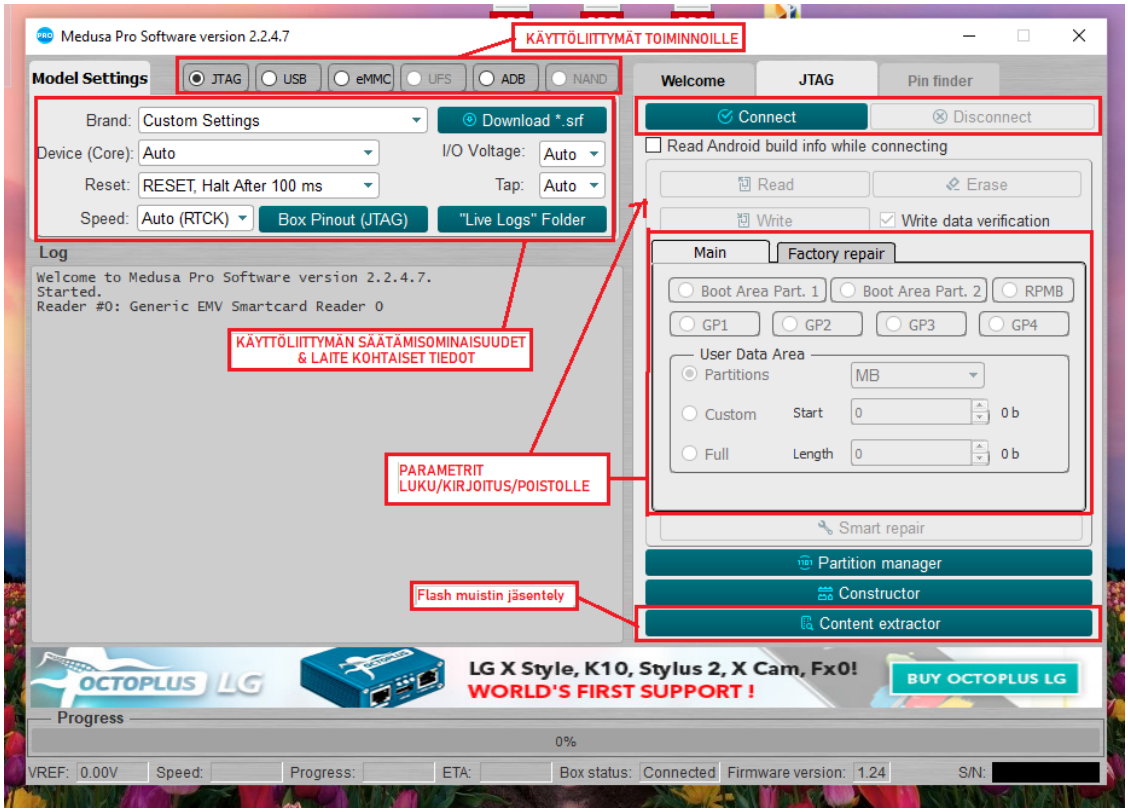
Kuva 25 Testausvaiheen toteutus ja testilaite

Testausvaiheessa kävi ilmi, että Octoplus Pro boxin toimikortti ei toiminut. Tämä vika esti käyttöohjelman käytön kokonaan ja tämä viivästytti itse louhinnan aloittamista. Lopulta oltiin yhteydessä valmistajan tukipalveluun ja paljastui, että erehdyksessä toimikorttia oli päivitetty sen maksimimäärän. Tämän takia toimikorttia ei pidä päivittää, ellei käyttöohjelma pyydä tekemään niin. Flasher boxin valmistajat lisäsivät ystävällisesti kortille päivittämisyrityksiä ja tämä korjasi ongelman.

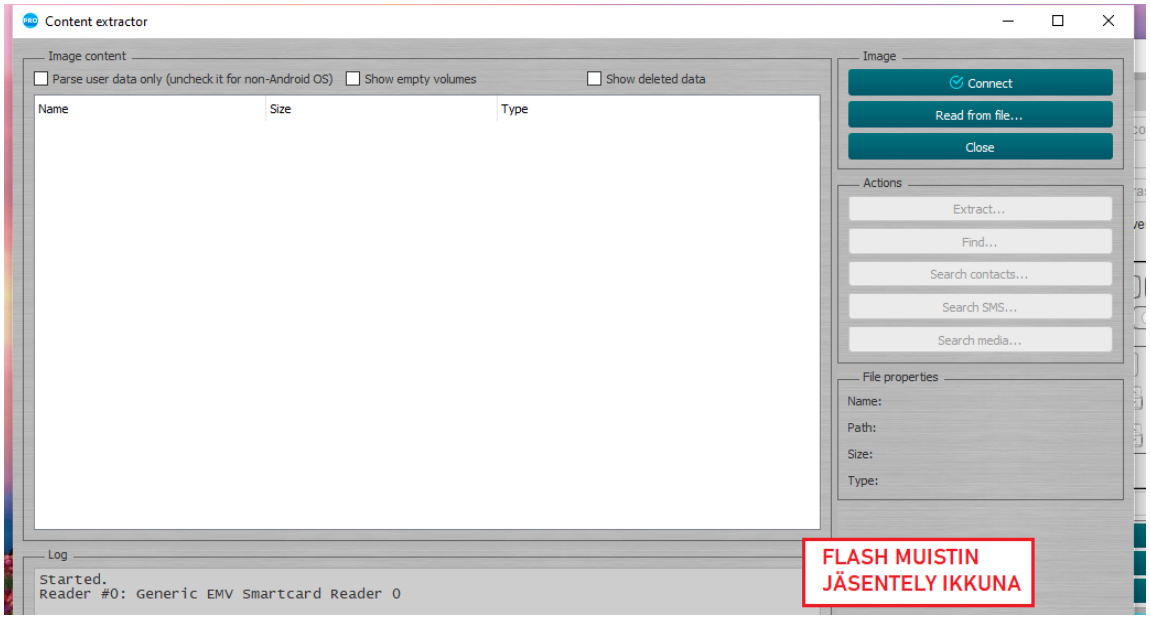
Kuitenkaan itse louhintaominaisuutta ei onnistuttu testaamaan, koska yksi ISP-nasta oli poltettu käytössä olleella juotoskolvilla. Itse ohjelma toimii moitteita kuten myös työkalut louhintaa varten.

Octoplus Pro boxin käyttöliittymä on miellyttävä ja selkeä käyttää louhintatarkoitukseen sekä JTAG- (Kuva 26) että eMMC (Kuva 28) eli ISP-näkymässä. ISP-näkymästä löytyy myös ohjeet ISP-nastojen löytämiseen eri puhelinmalleista (Kuva 29), joita ohjelma tukee. Tähän louhintaohjelmaan on myös käyttöohjeet valmistajan sivuilla: https://octoplusbox.com/en/info/octoplus-pro-software-user-manual/

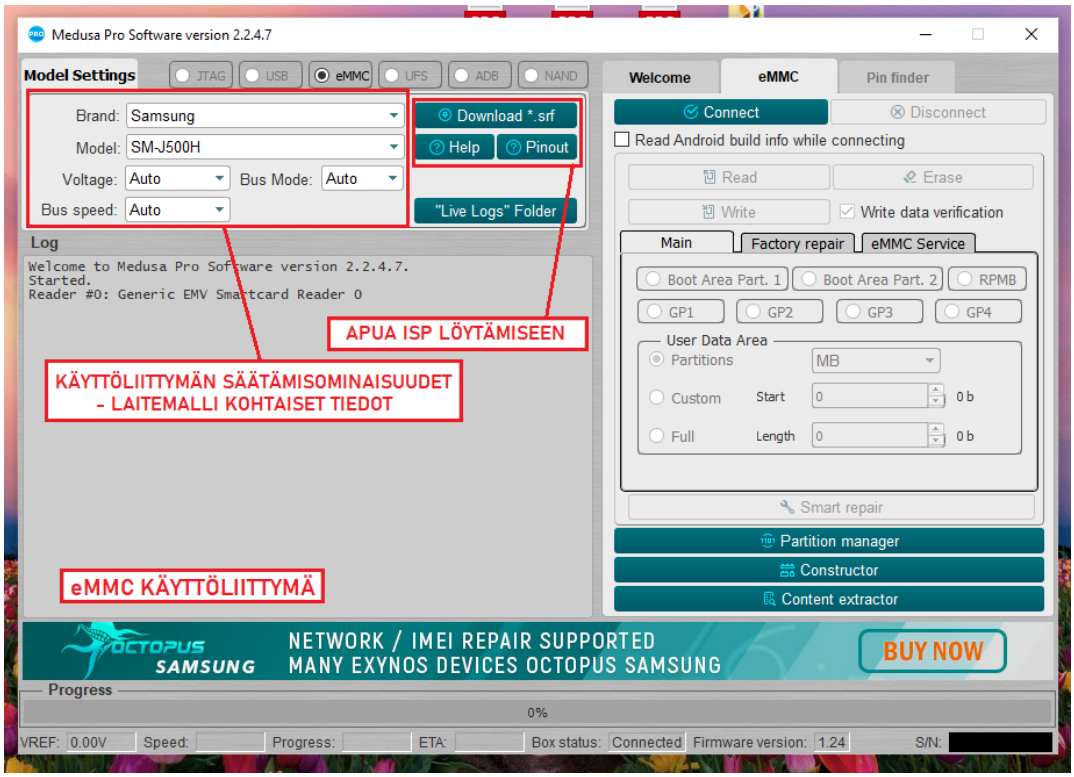
Kuva 26 Octoplus Pro Box - JTAG ohjelma ja ominaisuudet merkattuna



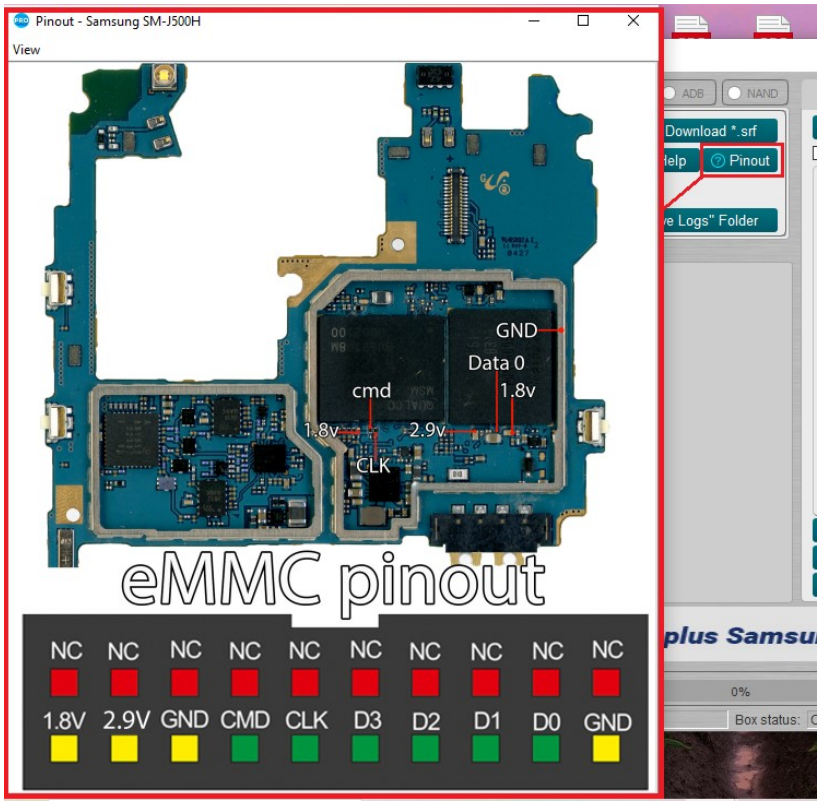
Kuva 27 JTAG-käyttöohjelman flash-muistin jäsentely ominaisuus



Kuva 28 eMMC ohjelman ominaisuudet merkattuna



Kuva 29 ISP nastojen löytämisapu eMMC ohjelman näkymässä



4.1 Kohdelaitteiden esittely

JTAG-louhinnan kohteina ovat matkapuhelimet Honor 8X ja Sony Xperia Z. Huomioitavaa on, että molemmat laitteet ovat olleet pois käytössä jo tovin, ja se on voinut vaikuttaa laitteiden järjestelmiin.

4.1.1 Kohdekännykkä 1

Honor 8X (Kuva 30) on vuonna 2018 julkaistu Huawein älypuhelin. Kooltaan puhelin on 160,4 × 76,6 × 7,8 mm ja se painaa 175 grammaa. Honor 8X on lähes kokonaan lasia, sen 6,5 tuuman näyttö käyttää Gorilla Glass 3- lasia ja takakansi on myös lasia. Takakannessa on sormenjälkitunnistin ja 20 MP takakamera. Puhelin toimii Android-käyttöjärjestelmällä. RAM-muistia on 4 Gt ja flash -muistia 64 Gt.

Huomioitavaa on, että kohdelaiteen näyttöä on aikaisemmin yritetty korjata, joten laitteen takakansi ja piirilevynsuoja on irrotettu ennen tutkimuksen aloittamista. Laitteeseen tiettävästi saa virrat päälle.

Kuva 30 Honor 8x -älypuhelin

4.1.2 Kohdekännykkä 2

Sony Xperia Z (Kuva 31) on vuonna 2013 julkaistu Sonyn valmistama älypuhelintuoteperhe, jota ei enää myydä. Laitteen malli on Sony Xperia Z C6603, joka julkaistiin vuonna 2014. Kooltaan puhelin on 139 × 71 × 7,9 mm ja se painaa 146 grammaa. Sen näyttö on 5 tuumainen. C6603 on pölynkestävä, roisketiivis ja vedenkestävä, ja se on lähes kokonaan lasia muovista runkoa lukuun ottamatta. C6603 takakamera on 20 MP. Puhelin toimii Android käyttöjärjestelmällä. RAM-muistia on 2048 MB ja flash -muistia 16 GB.

Kohdelaitteen näyttö ei toimi, mutta virran kytkeminen päälle onnistuu. Takakansi irrotetaan lämmittämällä sitä, jolloin liima alkaa hellittää otettaan siitä ilman, että takakansi murenisi lasisiruiksi.

Kuva 31 Sony Xperia Z

4.2 Kohdekännykkä 1:n JTAG-louhinnan raportointi

Kohdekännykkä 1:n purkaminen onnistuu helposti ja ripeästi käyttäen apuna Wit Rigsin kuvaamaa purkuohjetta: Wit Rigs (Ohjaaja). (2019, tammikuuta 26). *Huawei Honor 8X Teardown | Disassemble*. https://www.youtube.com/watch?v=ZgMboENpa90

Näyttöä ei tarvitse irrottaa laitteistosta, sillä puhelimen piirilevyyn pääsee käsiksi takakannen irrottamalla (Kuva 32.) Akku on myös valmiiksi irrotettu pois käytöstä. Ruuvaamalla piirilevynsuojan irti pääsee käsiksi piirilevyyn (Kuva 33.) Tämän jälkeen irrotetaan kamera, etuanturi ja muut kiinni olevat nauhat piirilevystä.

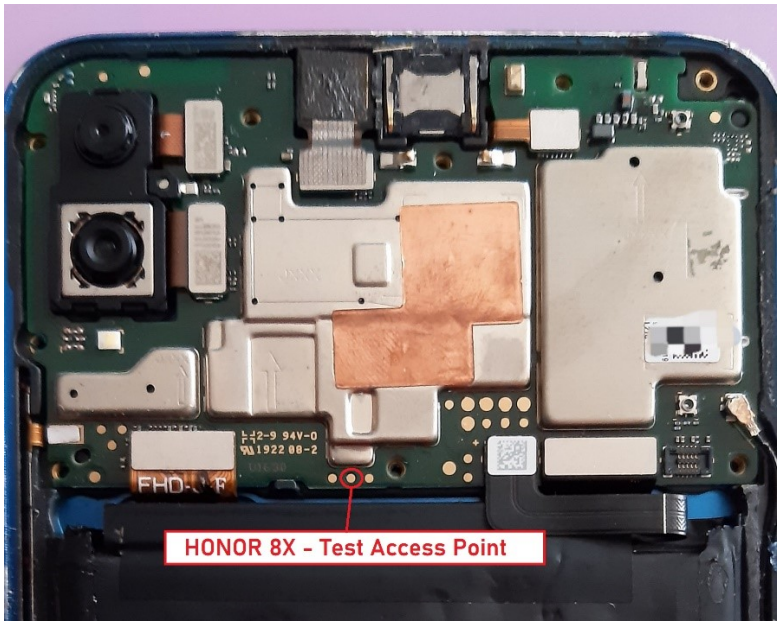
Kuva 32 8x takakannen irrotus

Kuva 33 8x piirilevyn suojan irrottaminen

Purkamisen jälkeen lähdetään etsimään mahdollista JTAG-käyttöliittymää Honor 8x:sta. Etupään piirilevy tarkastetaan molemmilta puolilta, mutta käyttöliittymää ei löydy, jonka jälkeen tarkistetaan internetistä, onko 8x:n nastoja jo kartoitettu. Etsimisen jälkeen joudutaan toteamaan, ettei Honor 8x:ssä ole selkeää JTAG-käyttöliittymää. Honor 8x käyttää pääasiassa ISP-liittymää.

Internetin avulla löytyy Honor 8x:n Test Access Point (Kuva 34), mutta sen tiedoista ei käy ilmi, voiko sitä käyttää laitteen louhimisessa. Sitä käytettäneen laitteen vianetsinnässä ja korjaamisessa.

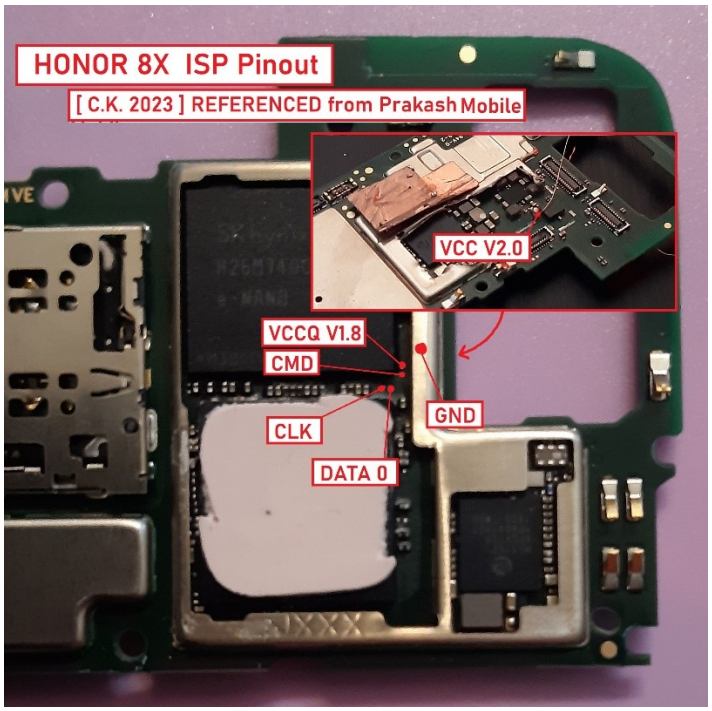
Kuva 34 8x Test Access Point



Testimielessä päätettiin kuitenkin käyttää ISP:ä louhinnassa JTAG:in sijaan, sillä ISP:ä voidaan myös hyödyntää louhinnassa. Honor 8x:n ISP:t löytyvät vaivattomasti internetin avustuksella. Koska haluttuihin nastoihin on haastavaa päästä käsiksi, mikropiirin päällinen puhdistettiin liimasta ja metallikehykset leikattiin leikkureilla (Kuva 35.) ISP-nastat ovat tässä tapauksessa piirilevyn molemmilla puolilla (Kuva 36.)

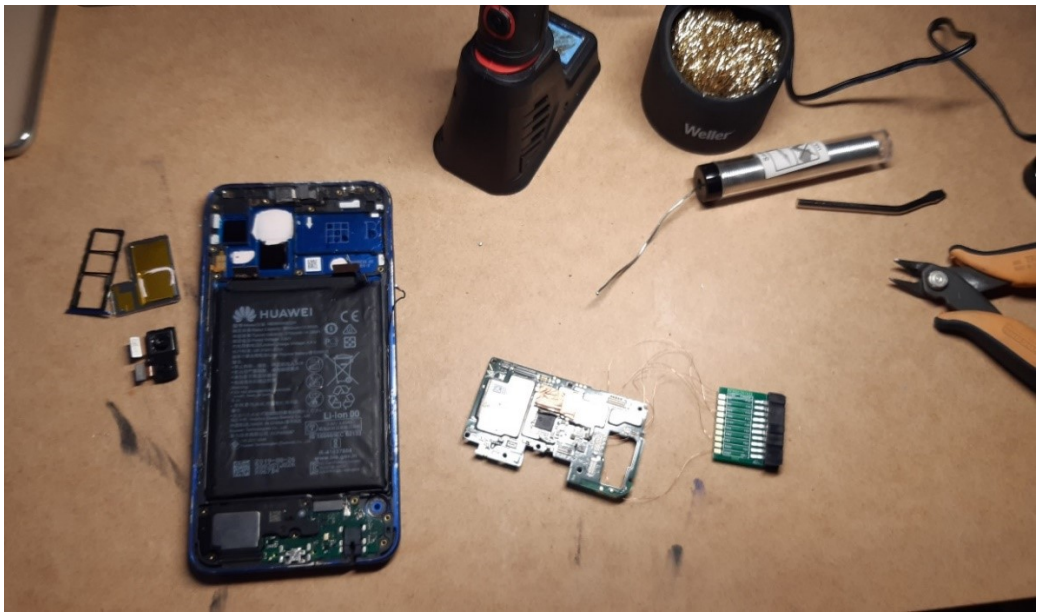
Kuva 35 8x piirilevyn toinen puoli

Kuva 36 Honor 8x ISP pinout

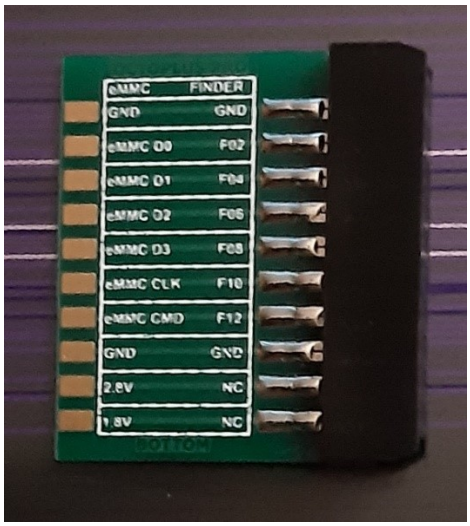


Hyppylankojen kiinnitys (Kuva 37) osoittautuu hankalaksi ja erittäin turhauttavaksi, koska juotettavat langat ovat todella kevyitä. On myös mahdollista, että käytettävän juotoskolvin kärki on liian iso näin pienien nastojen juottamiseen. Hyppylangat saadaan kuitenkin juotettua kiinni ISP- nastoihin ja JTAG-adapteriin (Kuva 38.)

Kuva 37 Hyppylangat juotettuna kiinni 8x:n piirilevyn ISP:hin ja JTAG-adaperiin



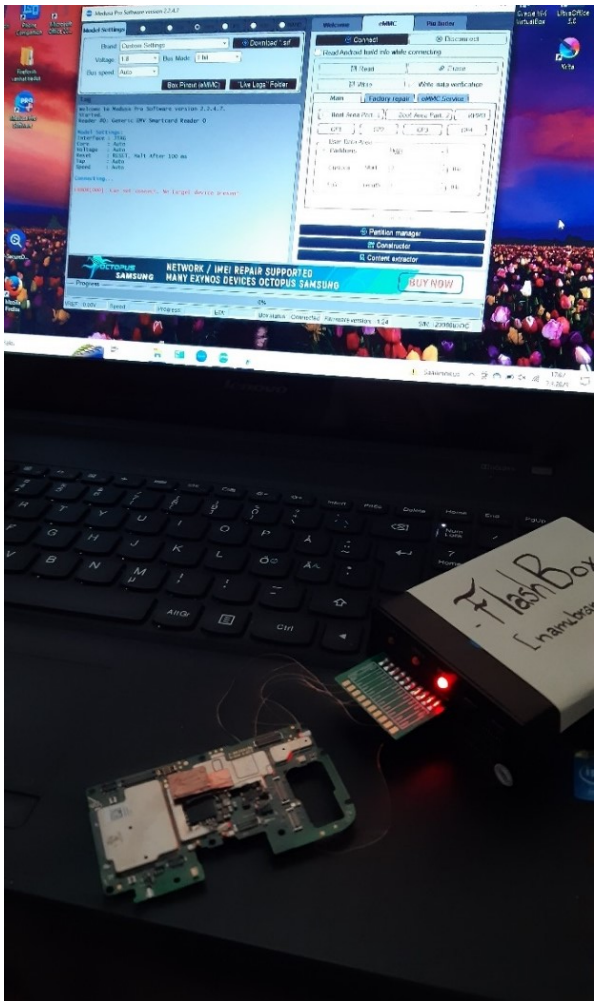
Kuva 38 JTAG-adapterin eMMC puoli



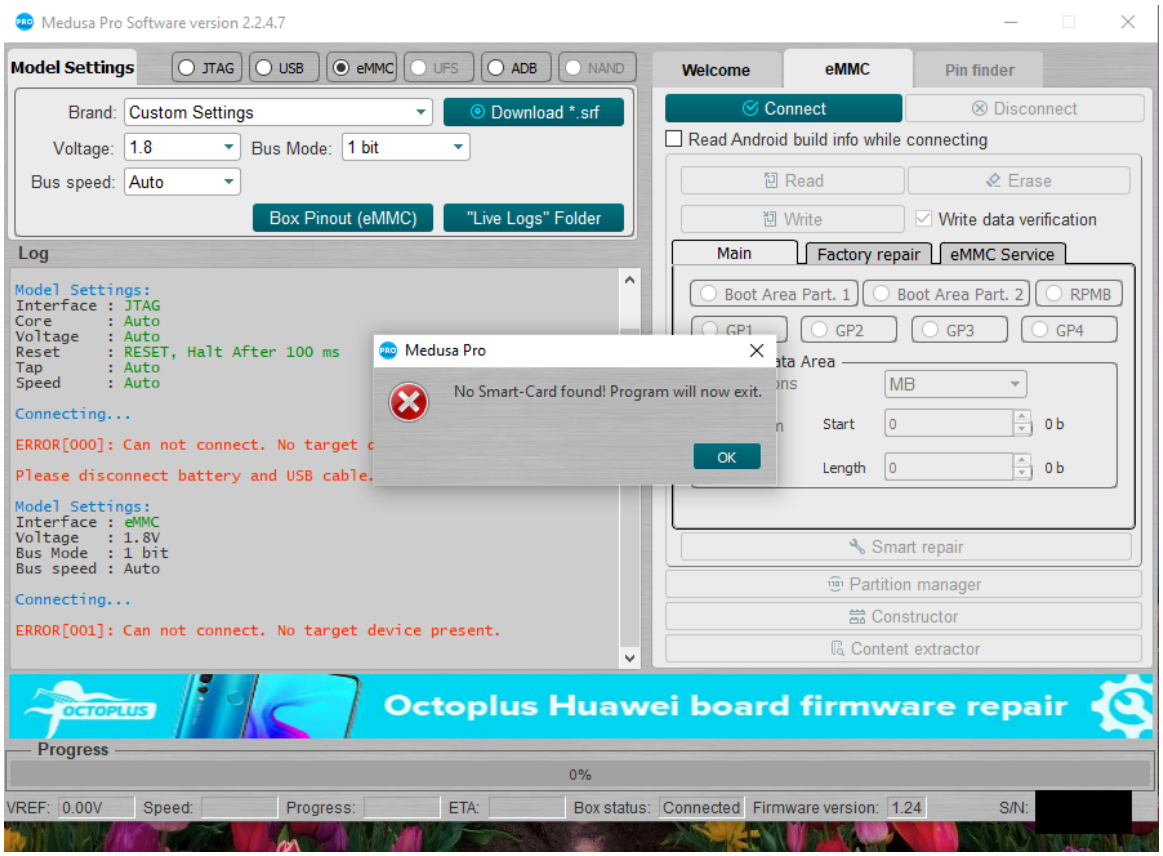
Flasher box kytketään koneeseen ja JTAG-ohjelma käynnistetään. Työkalua testataan muutaman kerran ilman adapterin kiinnitystä ajamalla JTAG-liittymän itsekseen. Kaikki vaikuttaa olevan kunnossa, joten JTAG-adapteri kiinnitetään flasher boxiin kiinni. Käynnistettäessä eMMC-ominaisuuden näytölle tulee viesti, ettei ohjelma löydä kohdelaitetta, mutta myös se, ettei käytettävä flasher box tue Huawei-laitteita. Flasher boxissa oleva toimikortti määrittää, mitä malleja työväline tukee. Rajoitukset tulevat yleensä ilmi flasher boxin ostovaiheessa.

Kohdekännykkä 1:lle ei voida suorittaa minkään muotoista louhintaa. Tutkimus päättyy tähän (Kuva 40.)

Kuva 39 8x kiinni flasher boxissa



Kuva 40 Flasher box ei tue tämän merkin mobiililaitteita

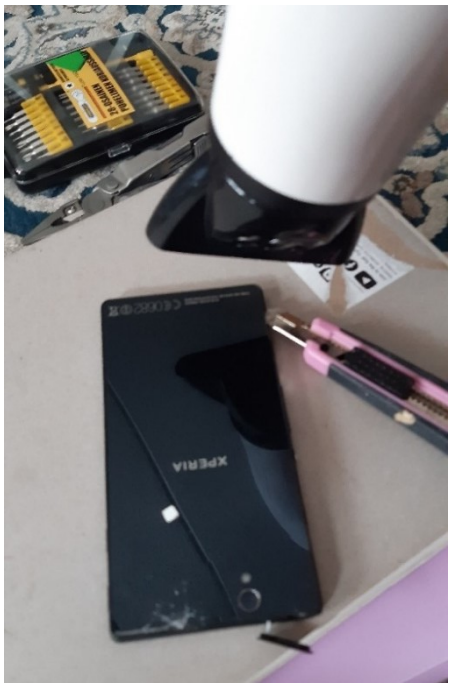


4.3 Kohdekännykkä 2:n JTAG-louhinnan raportointi

Kuva 41 Työkalut puhelimien purkamiseen

Kohdekännykkä 2:n purkaminen on kohdekännykkä 1:een verraten työteliäämpään, koska laitetta ei ole aikaisemmin yritetty purkaa. Purkaminen aloitetaan irrottamalla takakansi, joka on kiinnitetty liimalla kiinni niin lujasti, ettei kuluttaja pystyisi sitä helposti itse avaamaan. Takakannen irrottamiseen voi käyttää puhelimien korjaamiseen tehtyä kuumenninta, mutta tavallinen hiustenkuivaajakin käy. Lämpö sulattaa liiman ja kansi saadaan avattua. Turvallisuussyistä ei ole suositeltavaa käyttää mattoveistä puhelimien purkamiseen, vaan on parasta käyttää metallilastaa tai muoviplektraa.

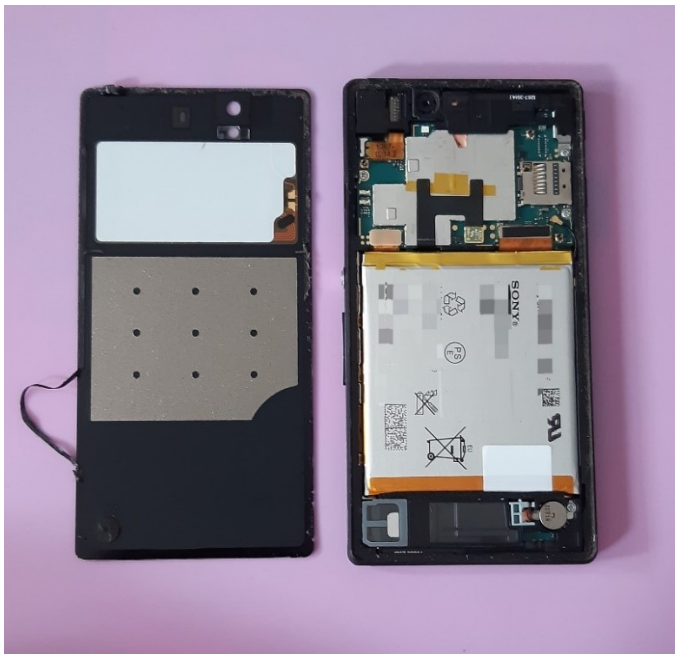
Kuva 42 Älypuhelimen takakannen irrotus



Kannen irrottua, Sony Xperia Z purku tapahtuu pitkälti myötäillen Rounded - YouTube kanavan Sony Xperia Z purkuvideota: Rounded (Ohjaaja). (2013, maaliskuuta 8). *Sony Xperia Z repair, disassembly manual*. https://www.youtube.com/watch?v=jNrtamZuf7E

Laitteen purkaminen on huomattavasti yksinkertaisempaa kuin kohdekännykkä 1:n juuri Xperia Z:n pelkistetyn olemuksen vuoksi. Molemmissa laitteissa on samantyyppinen litiumioniakku, joka kiinnittyy saman tapaan laitteeseen. Suojakotelo ja kamerat irrotetaan yläosasta.

Kuva 43 Xperia Z kannen irrotus



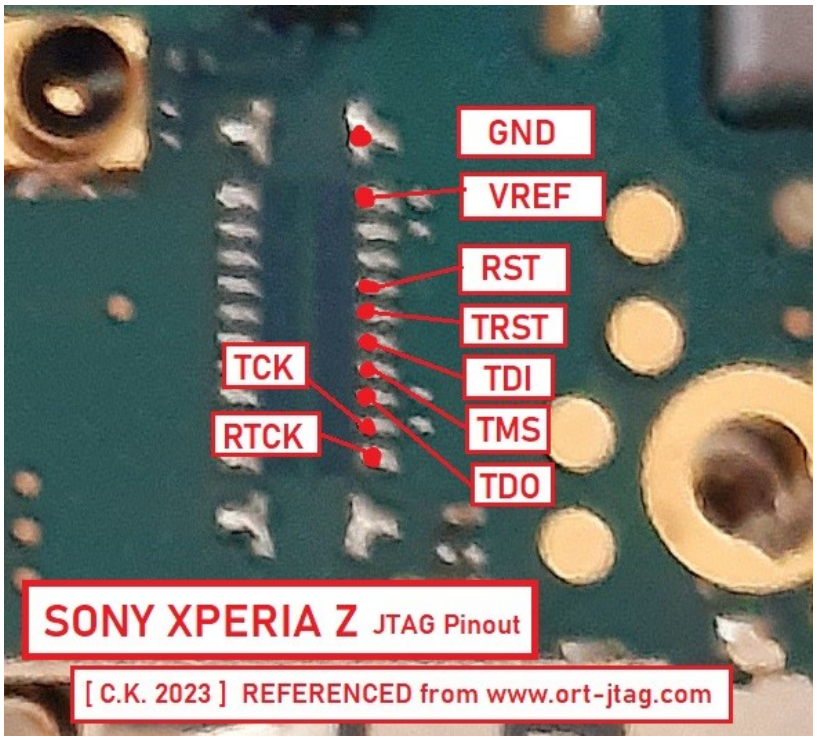
Kuva 44 Xperia Z helposti louhintaa häiritsevien osien irrottaminen

Kuva 45 Xperia Z ja työpiste

JTAG-käyttöliittymä löytyy tällä kertaa heti internetin avustuksella piirilevyn etuosasta kahdessa jonossa sirukotelon yläpuolelta. Nastojen tunnistamiseen ei internetistä löydy muita lähteitä kuin vain ORT JTAG:n asetelma. Koska ORT box on yksi tunnetuista flasher boxeista, joita on käytössä puhelinkorjausliikkeissä, päätetään luottaa tähän asetelmaan.

Kuva 46 Xperia Z:n JTAG-käyttöliittymä

Kuva 47 Sony Xperia Z JTAG pinout



JTAG-käyttöliittymän nastojen tunnistuksen jälkeen lähdetään kiinnittämään hyppylangat kiinni laitteeseen. Tällä kertaa hyppylangat kiinnitetään jo valmiiksi JTAG-adapteriin, jotta niitä ei sekoittaisi heti kiinnitettäessä puhelimeen.

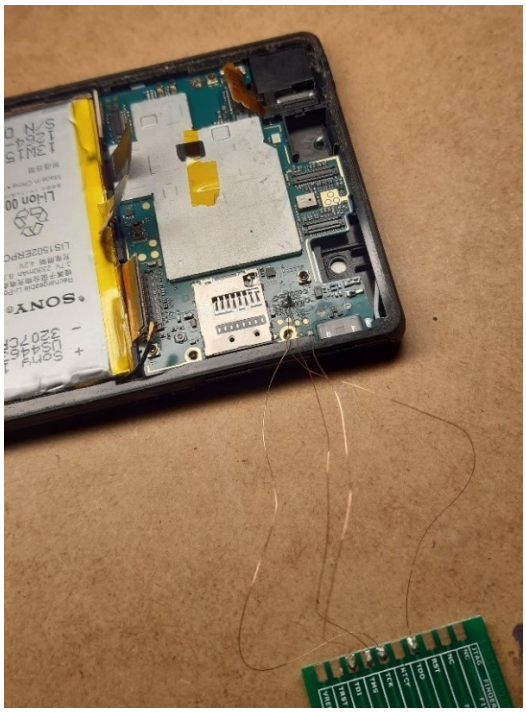
Kuva 48 Hyppylankojen kiinni juotto JTAG-adapteriin

Kuva 49 JTAG-adapterin JTAG puoli

Juottamisen helpottamiseksi käytetään maalarinteippiä pitämään hyppylankoja paikoillaan. Langat asetellaan yksi kerrallaan oikeaan järjestykseen nastoille ja langat teipataan kiinni piirilevyn kulmaan. Tämän jälkeen hyppylangat juotetaan kiinni nastoihin onnistuneesti.

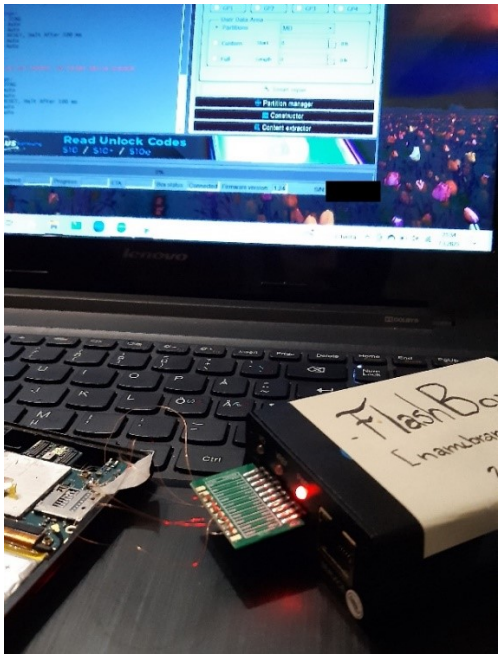
Kuva 50 Hyppylankojen asettelu ja juotto JTAG-käyttöliittymään

Kuva 51 Hyppylangat on juotettu



Kun TDI, TDO, TMS ja TCLK on juotettu, tarkistetaan vielä flasher box -ohjelman uudestaan. Tässä vaiheessa huomataan, että tämä ohjelma käyttää myös TRST, RST ja RTCK toiminnoissaan, joten hyppylangat juotetaan käyttäen jälleen maalarinteippiä tukena näihin nastoihin ja ne kiinnitetään JTAG-adapteriin. Ensin testataan, toimiiko ohjelma normaalisti ilman adapteria ja tämän jälkeen kiinnitetään adapteri jälleen flasher boxiin.

Kuva 52 Xperia Z liitettynä flasher boxiin

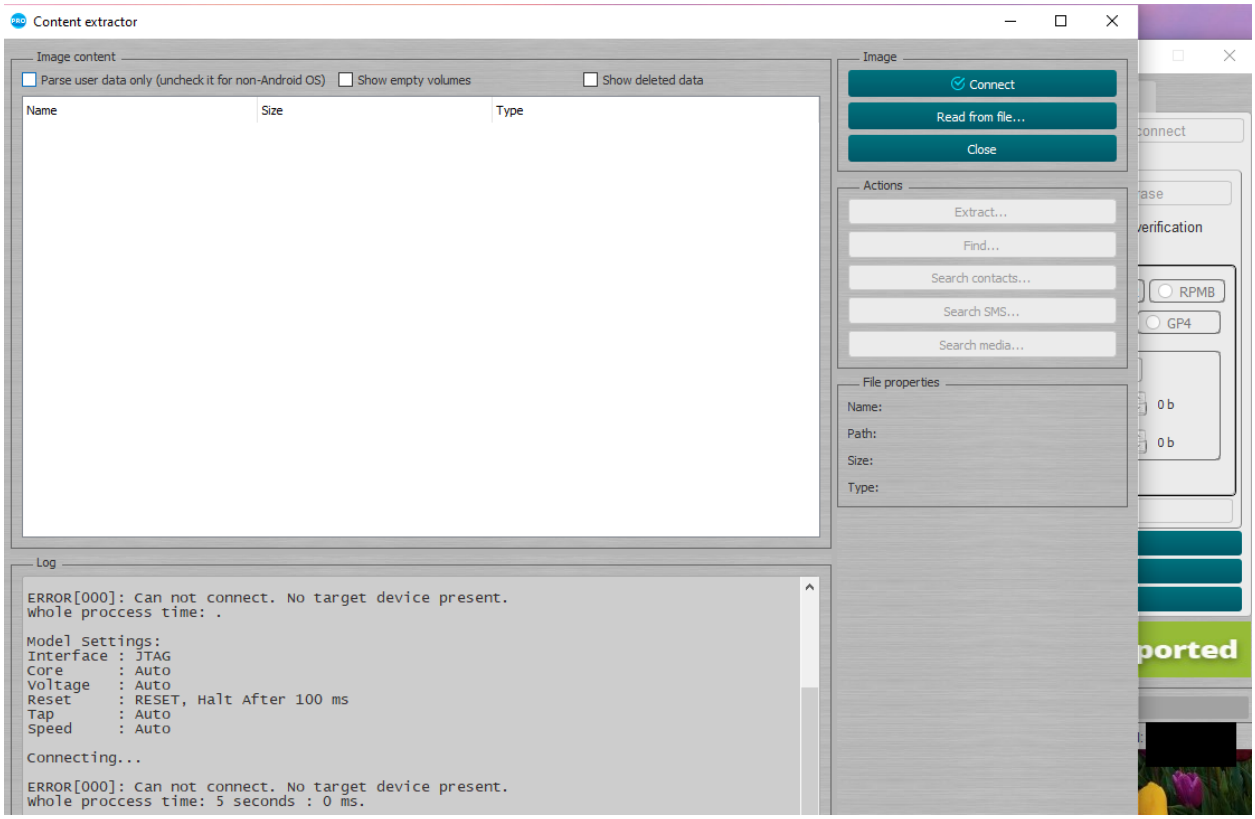


Ohjelma käynnistyy, mutta se ei löydä kohdelaitetta: ”ERROR[000]: Can not connect. No target device present” (Kuva 53). Tätä lähdetään tutkimaan. Tästä tietystä virhemerkinnästä ei löydy paljolti tietoa GSM-tukifoorumeilta, sillä suurin osa tämän tyypin virheistä on eMMC- liittymän virheitä, ja osa JTAG:iin liittyvästä keskustelusta on jo vanhentunut.

Keskusteluista pystytään kuitenkin soveltamaan eMMC-virheen 001 mahdollisia syitä tähän tilanteeseen. Todennäköisesti yksi nastoista on palanut juotosprosessin aikana. Tiettävästi tämä ongelma olisi mahdollista korjata, mutta en koe osaamiseni siihen vielä riittävän.

Tämä tarkoittaa, että louhintaa ei voida suorittaa loppuun ja tutkinta päättyy tähän.

Kuva 53 Louhintaa ei voida suorittaa yhteys ongelman vuoksi



5 Johtopäätökset ja pohdinta

Vaikka louhinnat eivät tuottaneetkaan tulosta, voidaan todeta molempien tapausten toimivan hyvinä esimerkkeinä siitä, mitä voi tapahtua louhinnan aikana ja miten prosessi etenee käytännössä.

JTAG-louhinta on erittäin hienovarainen prosessi, johon tarvitaan tietotaitoa, käytännöntaitoa ja kärsivällisyyttä. JTAG-käyttöliittymät ovat usein hyvin pienikokoisia ja vaikeasti löydettävissä, mikäli sellainen on mobiililaitteen piirilevyllä.

Jatkossa tulee myös perehtyä etukäteen erilaisten laitteiden louhintamahdollisuuksiin, sillä osassa laitteita ei ole nykyisin selkeästi löydettävissä olevaa TAP-käyttöliittymää tai vain ISP-louhinta on mahdollista. Myös se, tukeeko flasher työkalu louhittavan mobiililaitteen mallia tulee tarkistaa. Niin ikään muiden oheistyökalujen, kuten juotoskolvien sopivuus ennen juottamistyön aloittamista on syytä varmistaa, sillä näin vältetään osa louhinnan aikana tapahtuvista juotosvahingoista.

6 Yhteenveto

Tutkimuskysymyksiin onnistuttiin vastaamaan, vaikkei JTAG-louhinta tuottanutkaan toivottua tulosta. Opinnäytetyöstä selviää, mitä digitaalisella forensiikalla ja mobiiliforensiikalla tarkoitetaan, mitä JTAG-menetelmällä ja standardilla tarkoitetaan, ja miten JTAG-louhinta suoritetaan kohdelaitteisiin.

Opin paljon tutkiessani JTAG-menetelmää ja perehtyessäni lähdemateriaaleihin. Aineistoa löytyy valtava määrä, mutta tiedon keräämistä vaikeutti muun muassa se, että yhdestä ominaisuudesta kirjoitetaan usealla eri termillä. Esimerkiksi JTAG-adapterista puhutaan muun muassa ”Inteligence Card” tai ”JTAG interface.” Kirjalliset lähteet olivat todella laajoja ja mieleenpainuvia.

Sain myös uutta tietoa rikosteknillisestä tutkimuksesta ja sen käytännöistä, kuten esimerkiksi digitaalisen todistusaineiston oikeanlaisen käsittelystä tai miten matkapuhelimen löytötila voi vaikuttaa sen sisältämään tietoon. Muun muassa se, että laite otetaan varomattomasti pois suolavedestä voi vaikuttaa laitteen piirilevyyn välittömästi. Opin myös lisää piirilevyistä ja mikropiireistä, kuten myös siitä, miten hyppylankoja juotetaan kiinni laitteisiin.

Toivon myös, että tästä työstä on apua jatkossa kyberturvallisuuden opinnoissa, kun perehdytään erilaisiin mobiiliforensiikan menetelmiin tai että työ lisäisi aiheen saavutettavuutta aiheesta kiinnostuneille lukijoille.

Jatkosuunnitelmana on suorittaa ainakin yksi onnistunut JTAG-louhinta matkapuhelimeen, ja tehdä tästä prosessista lisädokumentaatio. Tätä onnistuneen louhinnan dokumentaatiota voidaan myöhemmin käyttää tämän opinnäytetyön lisämateriaalina opetusmielessä.

7 Lähdeluettelo

Al-Zarouni, M. (2007). Introduction to mobile phone flasher devices and considerations for their use in mobile phone forensics [PDF]. *5th Australian Digital Forensics Conference*, *Edith Cowan University*, December 3rd 2007. https://doi.org/10.4225/75/57AD5EDD7FF34

Basic Overview of JTAG, ISP, and Chip Off Extractions | Farley Forensics. (2019, huhtikuuta 10). https://farleyforensics.com/2019/04/10/basic-overview-of-jtag-isp-chipoff-extractions/, http://www.farleyforensics.com/2019/04/10/basic-overview-of-jtag-isp-chipoff-extractions/

Boundary-Scan. (n.d.). *JTAG* [kuva]. Noudettu 2. maaliskuuta 2023, osoitteesta https://www.jtag.com/boundary-scan/

Boxes and Dongles: Everything You Need to Know (Part 1). (n.d.-a). GsmServer. Noudettu 8. helmikuuta 2023, osoitteesta https://gsmserver.com/en/articles-and-video/boxes-and-dongles-part-1/

Boxes and Dongles: Everything You Need to Know (Part 1) [kuva]. (n.d.-b). GsmServer. Noudettu 8. helmikuuta 2023, osoitteesta https://gsmserver.com/en/articles-and-video/boxes-and-dongles-part-1/

BSDL & SVF File Formats. (n.d.). *XJTAG* [kuva]. Noudettu 8. helmikuuta 2023, osoitteesta https://www.xjtag.com/about-jtag/bsdl-files/bsdl-and-svf-file-formats/

BSDL Tutorial. (2016, syyskuuta 28). *JTAG Boundary-Scan, In-System Programming, & Bus Analyzers - Corelis*. https://www.corelis.com/education/tutorials/bsdl-tutorial/

CFTT - JTAG and Chip-Off 2019.pdf. (n.d.). Noudettu 8. helmikuuta 2023, osoitteesta https://www.nist.gov/system/files/documents/2020/08/21/CFTT%20-%20JTAG%20and%20Chip-Off%202019.pdf

Corelis Jtag (Ohjaaja). (2013, lokakuuta 4). *What is JTAG and why use it? (FULL Presentation)*. https://www.youtube.com/watch?v=uQs32JjZrhs

Differences in advance data extraction methods from the mobile phone [kuva]. (n.d.). Noudettu 8. helmikuuta 2023, osoitteesta https://ligsuniversity.com/blog/differences-in-advance-data-extraction-methods-from-the-mobile-phone

Easttom, C. (2021). *An in-Depth Guide to Mobile Device Forensics*. Taylor & Francis Group. http://ebookcentral.proquest.com/lib/hamk-ebooks/detail.action?docID=6715713

EC-Council. (2022, maaliskuuta 24). Five Anti-Forensic Techniques Used to Cover Digital Footprints. *Cybersecurity Exchange*. https://www.eccouncil.org/cybersecurity-

exchange/computer-forensics/anti-forensic-techniques-used-to-cover-digital-footprints/

EEVblog (Ohjaaja). (2013, heinäkuuta 27). *EEVblog #499—What is JTAG and Boundary Scan?* https://www.youtube.com/watch?v=TlWlLeC5BUs

Everything you need to know about NAND Flash [kuva]. (n.d.). Noudettu 8. helmikuuta 2023, osoitteesta https://www.rs-online.com/designspark/everything-you-need-to-know-about-nand-flash

Faraday bag. (2023). Teoksessa *Wiktionary* [kuva]. https://en.wiktionary.org/w/index.php?title=Faraday_bag&oldid=70924144

Gogolin, G. (2021). *Digital Forensics Explained*. Taylor & Francis Group. http://ebookcentral.proquest.com/lib/hamk-ebooks/detail.action?docID=6469109

Guarino, A. (2011, lokakuuta 2). *Use of flasher boxes for mobile forensics – Strange loops*. http://www.studioag.pro/en/2011/10/le-flasher-box-per-lanalisi-forense-dei-cellulari/

Instruction Decoder—An overview | ScienceDirect Topics. (n.d.). Noudettu 27. helmikuuta 2023, osoitteesta https://www.sciencedirect.com/topics/engineering/instruction-decoder

In-system programming. (2023). Teoksessa *Wikipedia*. https://en.wikipedia.org/w/index.php?title=In-system_programming&oldid=1140202943

Introduction to JTAG and the Test Access Port (TAP)—Technical Articles. (n.d.). Noudettu 8. helmikuuta 2023, osoitteesta https://www.allaboutcircuits.com/technical-articles/introduction-to-jtag-test-access-port-tap/

IP-Box 2 [kuva]. (n.d.). GsmServer. Noudettu 8. helmikuuta 2023, osoitteesta https://gsmserver.com/en/ip-box-2/

Joe Grand (Ohjaaja). (2018, joulukuuta 27). *Extracting Firmware from External Memory via JTAG*. https://www.youtube.com/watch?v=IadnBUJAvks

Johansen, G. (2022). *Digital Forensics and Incident Response: Incident Response Tools and Techniques for Effective Cyber Threat Response*. Packt Publishing, Limited. http://ebookcentral.proquest.com/lib/hamk-ebooks/detail.action?docID=30284025

JTAG Connectors and Interfaces—Technical Articles. (n.d.). Noudettu 2. maaliskuuta 2023, osoitteesta https://www.allaboutcircuits.com/technical-articles/jtag-connectors-and-interfaces/

KONSTRUKTIIVINEN TUTKIMUS. (2016, tammikuuta 9). *Oppariapu*. https://oppariapu.wordpress.com/konstruktiivinen-tutkimus/

Make Me Hack (Ohjaaja). (2020, maaliskuuta 29). *#03—How To Find The JTAG Interface—Hardware Hacking Tutorial*. https://www.youtube.com/watch?v=_FSM_10JXsM

Mobiiliopas—Mobiililaitteet. (ei pvm.). Noudettu 10. maaliskuuta 2023, osoitteesta https://sites.google.com/site/avomobiiliopas/mobiililaitteet

ModJTAG - JTAG connector adapter module [kuva]. (n.d.). Kamami.Pl. Noudettu 2. maaliskuuta 2023, osoitteesta https://kamami.pl/en/jtag-accessories/184708-modjtag.html

Octoplus Dongle Samsung + LG Lite [kuva]. (n.d.). GsmServer. Noudettu 8. helmikuuta 2023, osoitteesta https://gsmserver.com/en/octoplus-dongle-samsung-plus-lg-lite/

Octoplus Pro Box with 7 in 1 Cable/Adapter Set (Activated for Samsung + LG + eMMC/JTAG) [kuva]. (n.d.). GsmServer. Noudettu 8. helmikuuta 2023, osoitteesta https://gsmserver.com/en/octoplus-pro-box-with-7-in-1-cable-adapter-set-activated-for-samsung-plus-lg-plus-emmc-jtag/?currency=2

Octoplus Pro Software - User Manual - Octoplus Box: Decoding and repairing tool. (n.d.). Octoplusbox. Noudettu 8. helmikuuta 2023, osoitteesta https://octoplusbox.com/en/info/octoplus-pro-software-user-manual/

Octoplus Server Credits - Octoplus Box: Decoding and repairing tool. (n.d.). Octoplusbox. Noudettu 8. helmikuuta 2023, osoitteesta https://octoplusbox.com/en/products/credits/

Octoplus Support (Ohjaaja). (2014, lokakuuta 2). *How to activate Octoplus/Octopus LG*. https://www.youtube.com/watch?v=-K-7Mxgfo1Q

Packt. (2014a, heinäkuuta 10). *Introduction to Mobile Forensics*. Packt Hub. https://hub.packtpub.com/introduction-mobile-forensics/

Packt. (2014b, heinäkuuta 10). *Introduction to Mobile Forensics*. Packt Hub. https://hub.packtpub.com/introduction-mobile-forensics/

Riff Box 2 [kuva]. (n.d.). Fonefunshop Ltd. Noudettu 8. helmikuuta 2023, osoitteesta https://www.fonefunshop.com/Riff-Box-2.html

Samsung Electronics Doubling Current Smartphone Storage Speed as it Begins Mass Production of First 512GB eUFS 3.0 [kuva]. (n.d.). Noudettu 8. helmikuuta 2023, osoitteesta https://news.samsung.com/global/samsung-electronics-doubling-current-smartphone-storage-speed-as-it-begins-mass-production-of-first-512gb-eufs-3-0

says, B. G. V. T. (2019, heinäkuuta 21). Securing the JTAG Interface. *ASSET InterTech*. https://www.asset-intertech.com/resources/blog/2019/07/securing-the-jtag-interface/

Smartphone subscriptions worldwide 2027. (n.d.). Statista. Noudettu 23. helmikuuta 2023, osoitteesta https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Technical Guide to JTAG - Corelis JTAG Tutorial. (n.d.). Noudettu 8. helmikuuta 2023, osoitteesta https://www.corelis.com/education/tutorials/jtag-tutorial/jtag-technical-primer/

Technical Guide to JTAG - XJTAG Tutorial. (n.d.). Noudettu 2. maaliskuuta 2023, osoitteesta https://www.xjtag.com/about-jtag/jtag-a-technical-overview/

Teoreettinen tutkimus—Jyväskylän yliopiston Koppa. (ei pvm.-a). Noudettu 8. maaliskuuta 2023, osoitteesta https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/teoreettinen-tutkimus

Teoreettinen tutkimus—Jyväskylän yliopiston Koppa. (ei pvm.-b). Noudettu 8. maaliskuuta 2023, osoitteesta https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/teoreettinen-tutkimus

UFS socket 254/153/95 for Easy jtag plus box [kuva]. (n.d.). Noudettu 8. helmikuuta 2023, osoitteesta https://es-la.facebook.com/sharkgsm2366

Veiligheid, M. van J. en. (2017, maaliskuuta 13). *NFI Memory Toolkit—Products and services—Netherlands Forensic Institute* [Webpagina]. Ministerie van Justitie en Veiligheid. https://www.forensicinstitute.nl/products-and-services/forensic-products/nfi-memory-toolkit

What is an IC & Why is There a Global Chip Shortage? [kuva]. (2021, marraskuuta 9). CircuitBread. https://www.circuitbread.com/ee-faq/what-is-an-ic-and-why-is-there-a-massive-global-chip-shortage

What is JTAG? A guide to the IEEE-1149.1 standard. (2023, tammikuuta 1). *JTAG Boundary-Scan, In-System Programming, & Bus Analyzers - Corelis*. https://www.corelis.com/education/tutorials/jtag-tutorial/what-is-jtag/

What is JTAG and how can I make use of it? - XJTAG Tutorial. (n.d.). *XJTAG*. Noudettu 27. helmikuuta 2023, osoitteesta https://www.xjtag.com/about-jtag/what-is-jtag/

Z3X Easy-Jtag Plus Full Upgrade Set [kuva]. (n.d.). GsmServer. Noudettu 8. helmikuuta 2023, osoitteesta https://gsmserver.com/en/z3x-easy-jtag-plus-full-upgrade-set/

Årnes, A. (Toim.). (2018). *Digital forensics*. John Wiley & Sons Inc.

Liite 1: Aineistonhallintasuunnitelma

Tutkimusaineisto, eli mobiililaitteet tullaan säilyttämään suojatussa työympäristössä, johon ei ole ulkopuolisilla pääsyä. Tutkimusaineistoa ei tulla siirtämään muualle työympäristössä taatakseen datan muuttumattomuuden ja laitteiden hyvän kunnon. Työympäristönä toimii oma asuntoni. Mobiililaitteista tullaan ottamaan kuvia, mutta kaikki viivakoodit ja muu tieto, josta puhelimen pystyisi tunnistamaan, anonymioinaan. Nämä kuvat ovat itse otettuja.

Työssä käytettävän flasher boxin nimi on piilotettu käytännön osan dokumentaation kuvissa, jotka olen itse ottanut. Nimi on piilotettu kyseisen flasher box valmistajan pyynnöstä.

Louhittava aineisto tullaan säilyttämään tutkintaan käytettävällä koneella ja louhinnasta saatu aineisto tullaan varmuuskopioimaan muistitikulle. Jos aineistosta otetusta kuvasta näkyy muita asioita kuin louhinnan kohdemateriaalia, ne tullaan anonymioinaan. Myös mobiililaitteen omistajan mahdolliset henkilötiedot kuten kuvat, joista pystyy päättelemään sijainnin ynnä muuta, piilotetaan.

Tutkimusaineisto eli tutkittavat mobiililaitteet luovutetaan takaisin omistajilleen tutkimuksen päätyttyä. Louhittu aineisto tuhotaan vuoden päästä opinnäytetyön hyväksymispäivästä.