Invazivne metode za ekstrakciju podataka mobilnih uređaja

Đurić, Matko

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Matko Đurić

INVAZIVNE METODE ZA EKSTRAKCIJU PODATAKA MOBILNIH UREĐAJA

ZAVRŠNI RAD

Zagreb, 2020.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 26. ožujka 2020.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Terminalni uređaji**

ZAVRŠNI ZADATAK br. 5779

Pristupnik: **Matko Đurić (0135250024)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Invazivne metode za ekstrakciju podataka mobilnih uređaja**

Opis zadatka:

Objasniti forenzičku analizu mobilnih uređaja. Sistematizirati forenzičke metode za ekstrakciju podataka mobilnih uređaja. Prikazati invazivne metode za ekstrakciju podataka. Objasniti hardverska i softverska rješenja invazivnih metoda za ekstrakciju podataka. Prikazati izazove forenzičke analize i mogućnosti invazivnih metoda.

Mentor:

dr. sc. Siniša Husnjak

Predsjednik povjerenstva za završni ispit:

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

ZAVRŠNI RAD

INVAZIVNE METODE ZA EKSTRAKCIJU PODATAKA MOBILNIH UREĐAJA

INVASIVE METHODS FOR DATA EXTRACTION OF MOBILE DEVICES

Mentor: dr. sc. Siniša Husnjak

Student: Matko Đurić

JMBAG: 0135250024

Zagreb, rujan 2020.

INVAZIVNE METODE ZA EKSTRAKCIJU PODATAKA MOBILNIH UREĐAJA

SAŽETAK

Ovaj završni rad prikazuje značajke metoda za ekstrakciju podataka iz mobilnih terminalnih uređaja. Također su opisana različita programska i sklopovska rješenja koja se koriste u procesu forenzičke analize. Stalnim razvojem digitalnih tehnologija, a posebice mobilnih terminalnih uređaja, došlo je do pojave novih digitalnih dokaza koji postaju sve važniji segment forenzičkih istraga. Digitalni podaci, odnosno digitalni dokazi su krhke prirode te ih je u današnje vrijeme moguće lako prikriti i modificirati pomoću dostupnih tehnologija. Kako bi se pronašli svi relevantni digitalni dokazi potrebno je koristiti napredne invazivne metode za ekstrakciju podataka. U ovom radu analizirane su invazivne metode za ekstrakciju podataka te su utvrđene prednosti i nedostaci njihovog korištenja. Provedenom analizom definirano je kada i na koji način upotrebljavati neku od invazivnih metoda za ekstrakciju podataka.

KLJUČNE RIJEČI: mobilni uređaji; forenzika; invazivne metode; ekstrakcija podataka

SUMMARY

This bachelor's thesis shows features of methods for data extraction of mobile devices. It also describes various software and hardware solutions used in the forensic analysis process. Due to constant development of digital technologies and especially mobile devices, new digital evidence emerged and are becoming an increasingly important segment of forensic investigations. The nature of digital data is fragile and nowadays it is possible to easily modify it with the help of available technologies. In order to find all relevant evidence, it is necessary to use advanced invasive methods for data extraction. This thesis analyzed invasive methods for data extraction and identified the advantages and disadvantages of their use. The analysis defined when and how to use one of the invasive methods for data extraction.

KEY WORDS: mobile; forensics; invasive methods; data extraction

Sadržaj

1. Uvod

Mobilni terminalni uređaji predstavljaju dinamički sustav koji digitalnim forenzičarima predstavlja niz izazova prilikom ekstrakcije podataka i analize tih podataka kao digitalnih dokaza. Razvojem novih tehnologija i stalnim napretkom postojećih tehnologija mobilni terminalni uređaji postaju sve kompleksnija cjelina zbog toga što sadrže razne ugrađene podsustave i koriste različite inačice operativnih sustava. Stvaranje forenzičkog alata koji bi posjedovao mogućnost analize svih trenutno dostupnih terminalnih uređaja predstavlja kompleksan proces iz razloga što se uz razvoj takvog alata razvija i tehnologija izrade samih terminalnih uređaja.

Ekstrakcija podataka predstavlja postupak dobave digitalnih dokaza iz različitih izvora u cilju daljnje obrade i pohrane. Navedeni postupak je najzahtjevniji, a istovremeno i najvažniji korak u provođenju forenzičke analize. Načini i metode provođenja ovog postupka opisani su u trećem i četvrtom poglavlju. Dostupnost metoda kojima će se provoditi ekstrakcija ovisi o korištenim hardverskim i softverskim rješenjima.

Predmet analize ovog završnog rada su invazivne metode za ekstrakciju sadržaja mobilnih uređaja. Invazivne metode opisane su u trećem i četvrtom poglavlju, dok su u šestom poglavlju navedene mogućnosti i izazovi pojedine invazivne metode.

Cilj i svrha izrade ovog diplomskog rada je analiza mogućnosti invazivnih metoda za ekstrakciju podataka mobilnih uređaja te opis njihovog provođenja.

Završni rad sastoji se od 7 poglavlja:

1. Uvod
2. Općenito o forenzičkoj analizi mobilnih uređaja
3. Sistematizacija forenzičkih metoda za ekstrakciju podataka mobilnih uređaja
4. Prikaz invazivnih metoda za ekstrakciju podataka
5. Hardverska i softverska rješenja invazivnih metoda
6. Izazovi forenzičke analize i mogućnosti invazivnih metoda
7. Zaključak

U drugom poglavlju definirani su pojmovi digitalne i mobilne forenzike, objašnjen je osnovni princip mobilne forenzike te su definirani i objašnjeni koraci forenzičke analize mobilnih uređaja.

Trećim poglavljem opisane su osnovne i napredne metode ekstrakcije podataka.

Invazivne metode podrazumijevaju fizičko rastavljanje elektroničkih uređaja koji se ispituju te su detaljnije opisane u četvrtom poglavlju. Za svaku invazivnu metodu definirani su i opisani koraci koji se provode u forenzičkoj analizi.

Peto poglavlje prikazuje različite implementacije softverskih i hardverskim rješenja za mobilnu forenziku. Svako navedeno rješenje je ukratko opisano te su navedene osnovne značajke.

Šesto poglavlje obuhvaća analizu izazova forenzičke analize i opisuje mogućnosti pojedine invazivne metode. Definirani su pojmovi destruktivnih i nedestruktivnih metoda te su za svaku metodu navedene neke od mogućnosti koje nude kada se koriste za ekstrakciju podataka. Izazovi forenzičke analize koji su navedeni ukratko su objašnjeni.

2. Općenito o forenzičkoj analizi mobilnih uređaja

U današnje vrijeme mobilni terminalni uređaji (MTU) sve manje se koriste za pozivanje, a sve više za komunikaciju putem društvenih mreža. Većina korisnika nije svjesna da se podaci kao što su kontakti, tekstualne poruke, popis poziva, elektronička pošta i razni privitci pohranjuju u memoriji MTU-a. Podaci kao što su informacije o geolokaciji i memoriranim zaporkama za razne servise se također pohranjuju i mogu biti od velikog značaja ukoliko je potrebno provesti istragu, [1].

Digitalna forenzika je grana forenzičke znanosti koja se bavi istraživanjem i oporavkom podataka koji su pohranjeni u memoriji digitalnih ili elektroničkih uređaja. Jedna od podvrsta digitalne forenzike je i forenzika mobilnih uređaja koja se bavi prikupljanjem i oporavkom podataka, odnosno potencijalnih digitalnih dokaza sa MTU-a u skladu s načelima forenzičke znanosti. Pod pojmom mobilne forenzike u većini slučajeva misli se na forenziku pametnih telefona iako se pod pojmom mobilnih uređaja podrazumijevaju klasični MTU, pametni MTU, tableti i mnogi drugi terminalni uređaji, [2].

Osnovno načelo mobilne forenzike i digitalne forenzike općenito je očuvanje integriteta informacija. Prilikom provođenja postupaka i metoda mobilne forenzike navedeno načelo se izuzetno teško može poštovati. Problemi koji se javljaju, a zbog kojih je ponekad teško poštovati načelo digitalne forenzike su krhkost samih podataka i zahtjevi pojedinih forenzičkih metoda za ekstrakciju podataka. Krhkost podataka može biti problem zbog toga što se podaci mogu lako prepravljati, a samim time u pitanje je dovedena i njihova vjerodostojnost. Razne forenzičke metode za ekstrakciju podataka zahtijevaju vezu između forenzičkog alata i uređaja prilikom provođenja ekstrakcije, te se tada ne može uključiti način rada samo za čitanje, [3].

Forenzička analiza MTU-a sastoji se od nekoliko koraka, [1]:

- Zapljenjivanje uređaja – Oduzimanje uređaja predstavlja prvi korak u procesu forenzičke istrage te podrazumijeva očuvanje integriteta informacija koje se postiže mrežnom izolacijom samog uređaja. Mrežna izolacija se omogućuje korištenjem Faraday vrećice koja blokira signale bežičnih tehnologija kao što su mobilne mreže, Bluetooth i WiFi. Nakon što se zaplijenjeni uređaj pohrani u Faraday vrećicu, potrebno je osigurati izvor vanjskog napajanja ukoliko je uređaj bio uključen, zbog mogućnosti da se uređaj sam isključi.
- Ekstrakcija podataka – U ovom koraku forenzičke istrage koriste se različite metode za ekstrakciju podataka iz MTU-a. Metoda ekstrakcije koja će se koristiti ovisit će o

modelu uređaja, fizičkom stanju uređaja i alatima koje posjeduje forenzički istraživač koji provodi istragu. Metode za ekstrakciju podataka MTU-a biti će objašnjenje u idućim poglavljima.

- Analiza podataka – Zadnji je korak u forenzičkoj istrazi te podrazumijeva analizu svih prikupljenih podataka koristeći neki od forenzičkih alata. Prilikom analize podataka koji nisu bili izbrisani preporučljivo je provesti ručni pregled istih na samom uređaju kako bi se utvrdila vjerodostojnost digitalnih dokaza.

3. Sistematizacija forenzičkih metoda za ekstrakciju podataka mobilnih uređaja

Ekstrakcija podataka je proces prikupljanja podataka iz različitih vrsta medija, za daljnju analizu i pohranu, [4]. Cilj provođenja ekstrakcije podataka je dobava podataka koji nisu dostupni prilikom uobičajenog pregledavanja uređaja. Ovisno o potrebama istrage metode ekstrakcije razlikuju od slučaja do slučaja.

Slika 1. Sistematizacija metoda ekstrakcije podataka

Izvor [5]

Slika 1 prikazuje piramidalnu sistematizaciju metoda ekstrakcije podataka. Donji dio prikazane piramide sastoji se od metoda ekstrakcije koje ne zahtijevaju veliku količinu tehničkih napora kao i upotrebu složenih forenzičkih procesa i alata dok gornji dio piramide prikazuje metode ekstrakcije koje provode forenzički stručnjaci primjenjujući napredne tehničke vještine te forenzičke alate i procese.

Proces ekstrakcije podataka MTU-a često se sastoji od kombinacije zahtjevnih i jednostavnih metoda ekstrakcije. Pomoću jednostavnih metoda podaci se ekstrahiraju u jako kratkom vremenskom periodu, ali njihova količina je ograničena i relativno mala. Ovisno o složenosti slučaja, forenzički ispitivači primorani su osim jednostavnih metoda koristiti i napredne metode ekstrakcije kojima se povećava obujam dobavljivih podataka. Napredne tehnike, osim povećanja količine podataka donose i povećanje vremenskog perioda potrebnog za ekstrakciju tih podataka. Prikazane metode biti će objašnjene u nastavku poglavlja, dok će invazivne metode ekstrakcije podataka biti dodatno opisane u slijedećem poglavlju.

3.1. Ručna ekstrakcija

Ručna ekstrakcija podataka predstavlja najjednostavniju metodu, a provodi se nad MTU-ima koji su podvrgnuti forenzičkoj analizi. Postupak ekstrakcije podataka sastoji se od procesa pregledavanja sadržaja MTU-a od strane istražitelja i korištenja fotoaparata za uzimanje slike ekrana MTU-a. Za lakšu provedbu ručne ekstrakcije istražitelji mogu koristiti alate koji im omogućuju brže provođenje cjelokupnog procesa, a jedan od takvih alata prikazan je na slici 2.

Slika 2. EDEC Eclipse alat za provođenje ručne ekstrakcije, [6]

Prednost korištenja metode ručne ekstrakcije podataka je podržanost svih modela MTU-a i mogućnost provedbe ekstrakcije bez korištenja dodatnih alata i priključaka. Kao glavni nedostaci ove metode izdvojeni su nemogućnost očuvanja integriteta podataka, kao i nemogućnost ekstrakcije svih podataka iz MTU-a. Ukoliko je MTU nad kojim se provodi forenzička analiza zaplijenjen u isključenom stanju ili je zaštićen zaporkom, metodu ručne ekstrakcije podataka nije moguće provesti, [7].

3.2. Logička ekstrakcija

Logička ekstrakcija je metoda akvizicije podataka terminalnih uređaja koja uključuje povezivanje uređaja na forenzičko sklopovlje putem odgovarajućeg sučelja ili korištenjem bežičnih komunikacijskih tehnologija kao što su Bluetooth i infracrvena tehnologija. Proces ekstrakcije započinje povezivanjem uređaja i forenzičkog alata, najčešće putem tvorničkog sučelja uređaja koje se analizira. Nakon uspješnog uparivanja forenzički će alat proslijediti niz instrukcija prema procesoru terminalnog uređaja, koji će na njih odgovoriti tako što će započeti prosljeđivati podatke iz pohrane uređaja prema radnoj stanici istražitelja, [4].

Logičkom ekstrakcijom kopiraju se podaci sa logičkih adresa pohrane uređaja. Logičke adrese pohrane sadrže razne mape i datoteke, ali pristup izbrisanim podacima nije moguć iz razloga što se oni nalaze u ne dodijeljenom području u koje ova metoda nema pristup. Upravo zbog automatiziranog prikupljanja podataka, glavna prednost ove vrste ekstrakcije je brzina provođenja cjelokupnog procesa. Neki od nedostataka ove metode su količina memorije potrebne za pohranu ekstrahiranih podataka i mogućnost promjene integriteta podataka prilikom procesa ekstrakcije, [8].

3.3. Ekstrakcija datotečnog sustava

Metoda ekstrakcije datotečnog sustava sa tehničkog aspekta predstavlja potkategoriju logičke ekstrakcije. Ovom vrstom ekstrakcije podataka mogu se ekstrahirati veće količine podataka jer se cjelokupni sadržaj datotečnog sustava kopira na računalo istraživača. Ekstrakcijom datotečnog sustava osim uobičajenih podataka, moguće je dobaviti podatke kojima se ne može izravno pristupiti putem korisničkog sučelja uređaja.

Oporavak izbrisanih podataka sa MTU-a koristeći navedenu metodu ekstrakcije moguć je ukoliko je uređaj koji se analizira pokretan operativnim sustavom Android ili iOS. Oba operativna sustava temeljena su na platformi SQLite baze podataka. Oporavak podataka iz baze podataka moguć je kroz sinkronizacijsko sučelje, a pristup izbrisanim podacima ovisit će o tome da li su logički blokovi unutar kojih su bili zapisani podaci ponovno pušteni u upotrebu ili ne, [9].

3.4. Fizička ekstrakcija

Potpuna forenzička analiza mobilnog uređaja moguća je jedino uz provedbu fizičke akvizicije podataka. Fizička ekstrakcija provodi se korištenjem alata i metoda mobilne forenzike. Fizička slika podataka se iz memorije uređaja izdvaja naprednim tehnikama ekstrakcije koje izdvajaju svaki bit memorijskog modula. Korištenjem navedene metode omogućuje se kopiranje dodijeljenog i ne dodijeljenog prostora, kao i izbrisanih podataka, [10].

Zbog problematike zaobilaženja sigurnosnih mehanizama, fizička ekstrakcija u pravilu zahtjeva korištenje plaćenih profesionalnih rješenja. Proces ekstrakcije podataka ovom metodom ne zahtjeva izvođenje bilo koje vrste prepravke na samom uređaju koji se analizira. Fizička ekstrakcija se realizira uspostavom veze između uređaja i alata kojim će se provesti proces ekstrakcije podataka, [1].

3.4.1. Flash Box metoda ekstrakcije

Kada forenzički ispitivači imaju ograničene financijske resurse, tj. kada skuplje metode ekstrakcije podataka nisu dostupne koristi se *Flash Box* metoda ekstrakcije. Osnovna namjena *Flasher Box* uređaja je dijagnostika i popravak mobilnih uređaja te su oni prvenstveno razvijeni za pružatelje mobilnih uređaja. Sa stajališta mobilne forenzike ova se alternativna metoda koristi za pristup *flash* memoriji i čitanju pohranjenog sadržaja. Pristup memoriji uređaja ostvaruje se putem JTAG ili servisnog priključka na matičnoj ploči MTU-a, dok je sučelje samog *Flasher Box* uređaja većinom RJ-45, [11].

Korištenjem navedene metode za ekstrakciju podataka moguće je izdvojiti skrivene i izbrisane podatke te je ekstrakciju također moguće provesti na oštećenim mobilnim uređajima. Prednost korištenja *Flasher Box* uređaja je potpuno izdvajanje i analiza *hex dump-a* koji predstavlja bit po bit kopiju sadržaja memorije uređaja koji se ispituje. Osim navedene, prednost korištenja ove metode je i potreba za relativno malim financijskim resursima u odnosu na druge komercijalne metode ekstrakcije, [11].

Narušavanje i provjera integriteta podataka dobivenih ovom metodom ekstrakcije predstavljaju veliki nedostatak. Opasnost za integritet podataka proizlazi iz činjenice da navedena metoda nikada nije bila zamišljena kao sredstvo za provođenje forenzičke analize. Također, postoji mogućnost da se ovom metodom osim kopiranja i čitanja podataka iz memorije uređaja zapišu novi podaci u memoriju i time se naruši vjerodostojnost izdvojenih digitalnih dokaza.

Ova fizička metoda ekstrakcije podataka zbog navedenih nedostataka i mogućih opasnosti nije namijenjena za mobilnu forenziku, a nikada nije niti bila zamišljena kao metoda koja će se koristiti u mobilnoj forenzici.

3.4.2. JTAG metoda ekstrakcije

JTAG (*eng. Joint Test Action Group*) predstavlja standard kojim se definira implementacija jedinstvenog ulaznog sučelja koje se koristi za otklanjanje grešaka u sklopovlju MTU-a. Ekstrakcija podataka korištenjem ove metode vrši se povezivanjem forenzičkog alata na TAP (*eng. Test Access Port*) priključke MTU-a. Navedena metoda ekstrakcije koristi se kada je potrebno zaobići implementirane mehanizme zaštite te ona pripada skupini invazivnih metoda ekstrakcije podataka MTU-a iz razloga što je za njeno provođenje potrebno fizički rastaviti MTU, [12].

JTAG metodom ekstrakcije podaci se ekstrahiraju pomoću serijskog sučelja koje se omogućuje fizičkim priključivanjem na pinove procesora. Jedna od prednosti korištenja ove metode je visoki stupanj očuvanja integriteta informacija zbog korištenja vlastitih registara, a osim očuvanja integriteta informacija prednosti JTAG metode ekstrakcije su i to što ne ovisi o operativnom sustavu MTU-a te ima mogućnost zaobilaženja svih softverskih mehanizama zaštite uređaja. Proces ekstrakcije ovom metodom je dugotrajan, a kako bi se uopće mogao koristiti potrebna je odgovarajuća dodatna oprema. Iako je JTAG kao standard definirao implementaciju ulaznog sučelja, mnogi proizvođači uklanjaju JTAG pinove ili ih ne označuju kako bi otežali provođenje procesa ekstrakcije, [12].

3.4.3. ISP Chip-off ekstrakcija

ISP (*eng. In-System Programming*) metoda ekstrakcije predstavlja invazivnu ali nedestruktivnu metodu ekstrakcije. Ekstrakcija podataka MTU-a pomoću ove metode dostupna je ukoliko uređaj koji se analizira koristi eMMC (*eng. Embedded MultiMedia Controller*) memorijski čip za pohranu podataka. Navedeni memorijski čip zapravo je memorijski modul jer se sastoji od MMC (*eng. MultiMedia Card*) sučelja, *flash* memorije i kontrolera koji su upakirani u jedinstveni BGA (*eng. Ball Grid Array*) čip, [1].

ISP metoda se koristi u slučajevima kada je potrebno zaobići sigurnosne mehanizme uređaja koji ne podržavaju JTAG. Omogućuje ekstrahiranje jednake količine podataka kao i chip-off metoda ekstrakcije, ali za razliku od nje nije potrebno uklanjati memorijski modul te je samim time manja mogućnost od fizičkog oštećenja memorijskog modula. Forenzički analitičari odlučuju se na korištenje ove metode zbog toga što je isplativija u odnosu na chip-

off metodu, količina resursa i alata za provedbu je također manja u odnosu na chip-off, dok je brzina ekstrakcije podataka puno veća u odnosu na JTAG metodu, [13].

3.4.4. Chip-off ekstrakcija

Chip-off metoda ekstrakcije je varijacija fizičke ekstrakcije podataka kod koje se podaci ekstrahiraju izravno s memorijskog čipa MTU-a. Proces ekstrakcije vrši se fizičkim uklanjanjem memorijskog čipa s matične ploče uređaja, a pomoću čitača čipova ili nekog forenzičkog alata provodi se ekstrakcija i analiza podataka zapisanih u uklonjenom memorijskom čipu.

Navedenom metodom moguće je ekstrahirati sve vrste podataka te je moguće zaobići gotovo sve mehanizme zaštite uređaja. Jedini mehanizam zaštite koji nije moguće zaobići je enkripcija podataka, ali se navedeni mehanizam može naknadno otkloniti ukoliko se ekstrahira enkripcijski ključ sa memorijskog čipa. Prednost korištenja ove metode ekstrakcije podataka je očuvanje integriteta informacija te mogućnost akvizicije podataka sa oštećenih uređaja, [14].

Chip-off metoda ekstrakcije podataka vremenski je jako iscrpljujuća i zahtjeva adekvatno obučeno osoblje za provođenje procesa ekstrakcije. Odabir ove metode uobičajeno se dešava nakon što su provedene sve ostale metode ekstrakcije, a rezultat njihovog provođenja nije zadovoljavajući. Prilikom provođenja ekstrakcije podataka ovom metodom postoji mogućnost od fizičkog oštećivanja memorijskog čipa, što znači i trajni gubitak podataka te je zbog toga ova metoda zadnji odabir svakog stručnjaka.

3.4.5. Micro Read

Micro Read metoda ekstrakcije podrazumijeva ručno analiziranje sadržaja memorijskih čipova korištenjem visoko softificiranih elektronskih mikroskopa. Proces ekstrakcije podataka svodi se na čitanje stanja elektroničkih sklopova i prevođenja istih u 0 i 1 kako bi se mogao odrediti znak koji je zapisan u uređaju korištenjem ASCII koda, [10].

Ovom metodom ekstrakcije moguće je ekstrahirati podatke s fizički oštećenih memorijskih čipova te se ista koristi u rijetkim slučajevima kao što je ugroza nacionalne sigurnosti. Prednost korištenja ove metode je mogućnost ekstrakcije svih podataka zapisanih u memoriji uređaja i dobivanje percepcije o procesima koji se dešavaju unutar MTU-a, [2]. Veliki financijski izdaci i vrijeme potrebno za ekstrakciju dovelo je do zanemarivanja Micro Read-a dok su alternativna rješenja u obliku metoda nižih razina sve više napredovala. Tržište alata mobilne forenzike trenutno ne nudi rješenja za ovu metodu, što govori da se s vremenom ova metoda izbacila iz upotrebe.

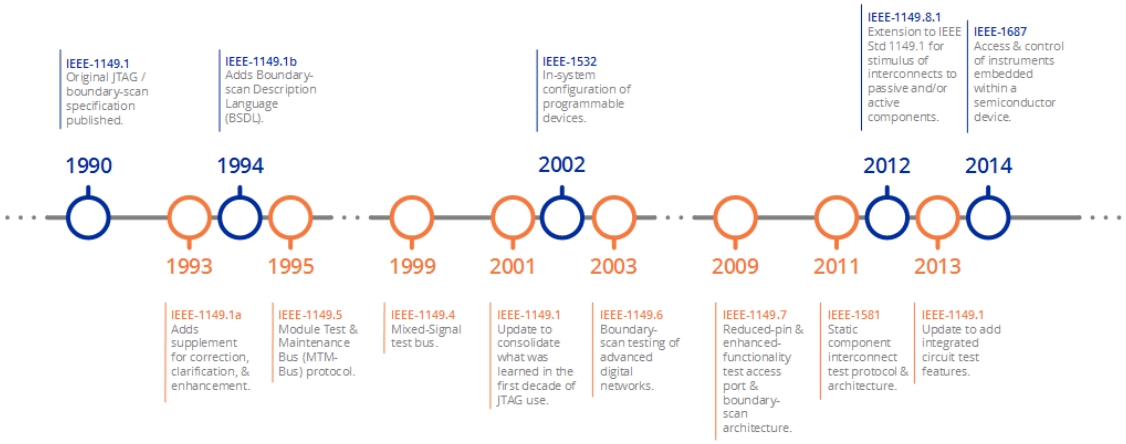
4. Prikaz invazivnih metoda za ekstrakciju podataka

Invazivne metode fizičke ekstrakcije zahtijevaju fizičko rastavljanje uređaja kako bi se omogućio pristup SoC-u (*eng. System on a chip*). Metode ekstrakcije podataka kojima je moguće dobaviti informacije sa memorijskog modula su :

1. JTAG
2. ISP - eMMC
3. *Chip-off*

4.1. JTAG metoda ekstrakcije

JTAG je udruga elektroničkih industrija osnovana s ciljem razvoja metode za provjeru i ispitivanje dizajna tiskanih pločica. Izvorni JTAG standard razvila je 1990. godine IEEE (*eng. Institute of Electrical and Electronics Engineers*) udruga pod nazivom IEEE 1149.1. Tri godine nakon izvornog standarda objavljena je revizija koja je poboljšala, prepravila i pojasnila izvornu verziju standarda. Godinu dana kasnije objavljena je dodatna dopuna kojom se dodao standardni jezik za opisivanje graničnog jezika. Definiranjem BSDL (*eng. Boundary-Scan Description Language*) jezika omogućio se automatizirani razvoj testova koji potiče usvajanje standarda od strane velikih proizvođača elektronike. Razvojem tehnologije stvaraju se nove prilike za korištenje JTAG-a. Razvoj standarda koji omogućuju proširivanje područja primjene JTAG tehnika bio je istodoban sa razvojem novih tehnologija, [15].



Slika 3. Razvoj JTAG-a, [15].

Tijek razvoja JTAG standarada prikazan je na slici 3 na kojoj se mogu vidjeti neki od značajnijih standarda poput IEEE 1149.6 i 1149.7. Standard pod nazivom 1149.6 objavljen je 2003. godine i odnosi se na granično testiranje sofisticiranih digitalnih mreža. Navedeni

standard poznatiji kao Dot6 standard predstavlja nadogradnju izvornog JTAG standarda koji definira BSDL ekstenzije koje podržavaju napredne digitalne mreže poznatije pod pojmom LVDS (*eng. Low Voltage Differential Signals*), [16]. Standard objavljen 2009. godine koji se naziva cJTAG razvijen je zbog sve veće potražnje za testiranjem tiskanih pločica i sustava modernih elektroničkih uređaja. IEEE 1149.7 standard nadograđuje izvorni JTAG standard kako bi ispunio zahtjeve novih tehnologija te se njime omogućuje provođenje osnovne JTAG tehnike ispitivanja na modernim elektroničkim uređajima, [17].

Način ekstrakcije podataka JTAG metodom je invazivan jer je za provođenje postupka ekstrakcije potrebno fizički ukloniti unutarnje napajanje uređaja s ciljem pristupanja procesoru ali nije destruktivan. Pristup procesoru omogućuje se putem serijskog sučelja koje se ostvaruje fizičkim povezivanjem na određene pinove procesora.

JTAG sučelje koristi niz signalnih pinova kojima podržava rad graničnog skeniranja. Svaki signalni pin zadužen je za obavljanje određene funkcije korištenjem slijedećih signala, [18] :

- TCK (*eng. Test Clock*) – Signal takta koji definira brzinu rada TAP kontrolera. Promjenom napona na ovom pinu insinuira se da kontroler provede određenu radnju. Bržom izmjenom naponskih stanja povećava se operativna brzina TAP kontrolera kojim se upravlja.
- TMS (*eng. Test Mode Select*) – Izmjenom naponskog stanja na ovom pinu definira se proces koji će JTAG izvršiti.
- TDI (*eng. Test Data In*) – Korištenjem ovog signalnog pina unose se podaci u logiku uređaja. Ulazni signal se uzorkuje uzlaznim bridom TCK signala.
- TDO (*eng. Test Data Out*) – Podaci koji se nalaze na ovom signalnom pinu predstavljaju izlazne podatke iz logike uređaja. Signal na ovom pinu se uzorkuje padajućim bridom TCK signala.
- TRST (*eng. Test Reset*) – Dodatni signalni pin koji omogućuje resetiranje JTAG-a u početno stanje.

JTAG standard definira niz instrukcija graničnog skeniranja koje moraju biti dostupne za uređaj nad kojim se želi provesti ekstrakcija podataka pomoću ove metode. U nastavku će biti opisane slijedeće instrukcije, [19] :

- BYPASS – Ovom instrukcijom uzrokuje se povezivanje TDI i TDO signalnih pinova preko jednobitnog registra koji omogućuje testiranje drugih uređaja s minimalnim zaglavljem.
- EXTEST – TDI i TDO signalni pinovi se pomoću ove instrukcije povezuju na BSR (*eng. Boundary Scan Register*) registar koji omogućuje prijenos informacija između izlaznih ili ulaznih pinova uređaja.
- SAMPLE/RELOAD – Ovom instrukcijom dolazi do povezivanja TDI i TDO signalnih pinova na BSR registar. Za vrijeme provođenja ove instrukcije omogućen je pristup BSR registru korištenjem operacije za skeniranje podataka. Osim za pristup uzorku ulaznih i izlaznih podataka, ova instrukcija koristi se za pred učitavanje testnih podataka.

JTAG metoda ekstrakcije koristi se kada ekstrakcija slike uređaja nije izvediva forenzičkim alatima. Najčešći problem zbog kojeg ekstrakcija forenzičkim alatima nije moguća je nemogućnost podizanja operativnog sustava uređaja. Proces ekstrakcije fizičke slike uređaja korištenjem JTAG metode sastoji se od sljedećih koraka, [10]:

- Identifikacija TAP pinova – Identifikacija JTAG priključka na tiskanoj pločici uređaja može biti zahtjevna. Postupak pronalaženja priključka započinje analiziranjem dokumentacije uređaja, a ukoliko se ovim postupkom lokacija priključka ne pronađe potrebno je koristiti neki od alata koji omogućuje pronalaženje istog.
- Povezivanje na JTAG priključak – Nakon uspješne identifikacije TAP pinova potrebno se povezati na iste. Povezivanje na pinove moguće je korištenjem JTAG priključka ili zalemljivanjem vodiča na same pinove. Nakon ostvarivanja konekcije JTAG kontrolera sa pinovima potrebno je priključiti kontroler na forenzičku radnu stanicu.
- Ekstrakcija podataka – Proces ekstrakcije podataka izvršava se korištenjem softverskog rješenja koje podržava ekstrakciju putem JTAG metode. Pokretanjem postupka ekstrakcije dobaviti će se binarna slika uređaja.
- Odvajanje i sastavljanje uređaja – Završetkom ekstrakcije podataka iz mobilnog uređaja potrebno je odspojiti konektor priključen na TAP pinove ili odlemiti zalemljene žice. Slijedi čišćenje tiskane pločice od ostataka lema i sastavljanje uređaja. Ukoliko se sastavljanje uređaja provede prema pravilima, uređaj će ostati funkcionalan.
- Analiza podataka – Zadnji korak u procesu ekstrakcije podataka JTAG metodom je analiza dobavljenih podataka. Ekstrahiranu binarnu sliku potrebno je otvoriti kroz neki

od forenzičkih alata za analizu. Analizom podataka mogu se oporaviti izbrisani podaci i ekstrahirati postojeći, a također je moguće provesti rezbarenje podataka.

4.2. ISP metoda ekstrakcije

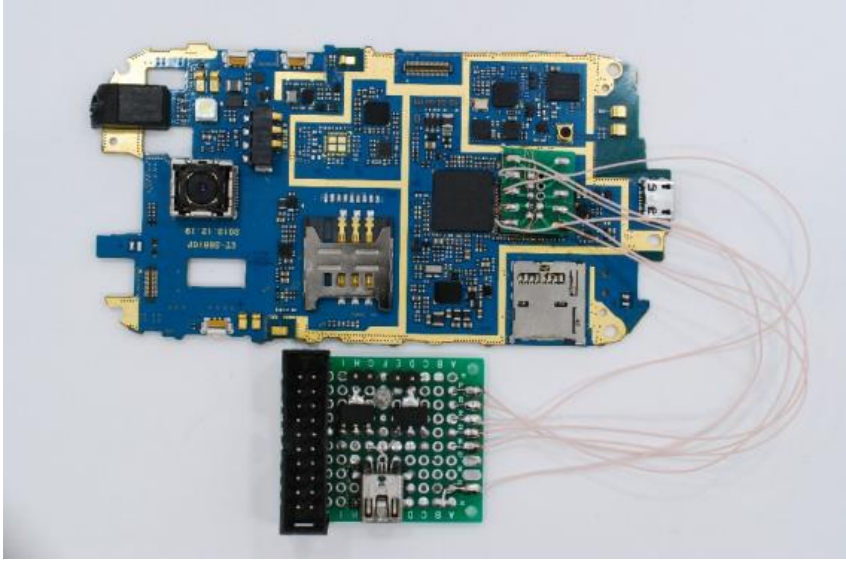
ISP sa forenzičkog stajališta predstavlja praksu povezivanja forenzičkih alata na memorijski čip s ciljem preuzimanja cjelokupnog sadržaja pohranjenog na memorijskom modulu. ISP kao i JTAG metoda predstavlja invazivnu nedestruktivnu metodu ekstrakcije. Zbog navedenog JTAG i ISP metode su vrlo slične ali bitna razlika manifestira se u brzini izdvajanja podataka. ISP metoda zaobilazi povezivanje s procesorom i izravno se spaja na memorijski modul. Osim bržeg odvijanja izdvajanja podataka moguće je analizirati uređaje koji ne podržavaju JTAG metodu.

ISP metoda ekstrakcije podataka primjenjuje se na svim elektroničkim uređajima koji koriste eMMC memorijske module. Izdvajanje navedenom metodom zahtijeva djelomično rastavljanje uređaja kako bi se identificirali i kasnije u procesu koristili TAP pinovi za pristup memorijskom modulu. TAP pinovi koji se koriste za pristup memorijskom čipu puno su manjih fizičkih dimenzija u odnosu na JTAG pinove te je za povezivanje na iste potrebno koristiti preciznije alate.

Provođenje ISP ekstrakcije odvija se istim tijekom kao što je objašnjeno u JTAG potpoglavlju. Problem koji može nastati je da na matičnoj ploči nisu označeni TAP pinovi i da JTAG nije podržan. Forenzički stručnjak u tom slučaju ima nekoliko opcija. Prva opcija je identifikacija TAP pinova pomoću ugrađenog softvera *flash box* uređaja. Ukoliko navedeni način identifikacije nije uspješan ispitivač će morati informacije o lokacijama TAP pinova saznati iz alternativnih izvora ako postoje ili će identifikaciju provesti ručno. TAP pinovi koji se koriste za provođenje ekstrakcije ISP metodom su, [20] :

- CMD – Koristi se za unos naredbi i dobivanje odgovora na iste
- DATA0 – Ovaj pin se koristi za transport podataka
- CLK – Pin koji generira signal takta
- VCC – Napon napajanja jezgre, iznosi 3.3V
- VCCQ – Napon napajanja za ulaze i izlaze, iznosi od 1.8V do 3.3V
- GND – Ovaj pin predstavlja uzemljenje.

Ručna identifikacija se provodi korištenjem *flash box* uređaja i ispitne sonde. Ispitna sonda se postavlja na otpornik koji vodi do samog TAP pina, nakon postavljanja ispitne sonde potrebno je pričekati povratnu informaciju *flasher box* uređaja. Ukoliko testirani pin nije odgovarajući, uređaj će odgoditi ispitivanje za nekoliko sekundi. Pronalaženjem odgovarajućeg pina potrebno je na njega zalemiti vodič kako bi se proces ručne identifikacije mogao nastaviti. Pronalaženjem svih potrebnih TAP pinova omogućuje se daljnji proces ekstrakcije. Na slici 4 prikazana je matična ploča na kojoj su identificirani TAP pinovi i koja je spremna za daljnje korake. Konektor koji je priključen na matičnu ploču uređaja potrebno je priključiti na *flash box* uređaj. *Flash box* uređaj se zatim povezuje na radnu stanicu forenzičkog ispitivača putem koje je moguće provesti ekstrakciju podataka korištenjem programskog rješenja *flash box* uređaja.



Slika 4. Prikaz pripremljenog uređaja za provođenje ISP izdvajanja, [5].

Na slici 4 prikazana je matična ploča mobilnog uređaja nad kojom su provedeni procesi identifikacije TAP pinova i priključivanje adaptera na iste. Nakon izvršenih radnji potrebno je adapter priključiti na *flash box* uređaji koji je povezan na računalo forenzičkog ispitivača te korištenjem ugrađenog softvera provesti izdvajanje podataka.

4.3. Chip-off metoda ekstrakcije

Chip-off je napredna tehnika akvizicije podataka iz mobilni uređaja. Proces ekstrakcije podataka zahtijeva rastavljanje uređaja i uklanjanje memorijskog čipa korištenjem specijaliziranih alata, a uklonjeni memorijski modul postavlja se u čitač pomoću kojeg se izdvajaju pohranjeni podaci.

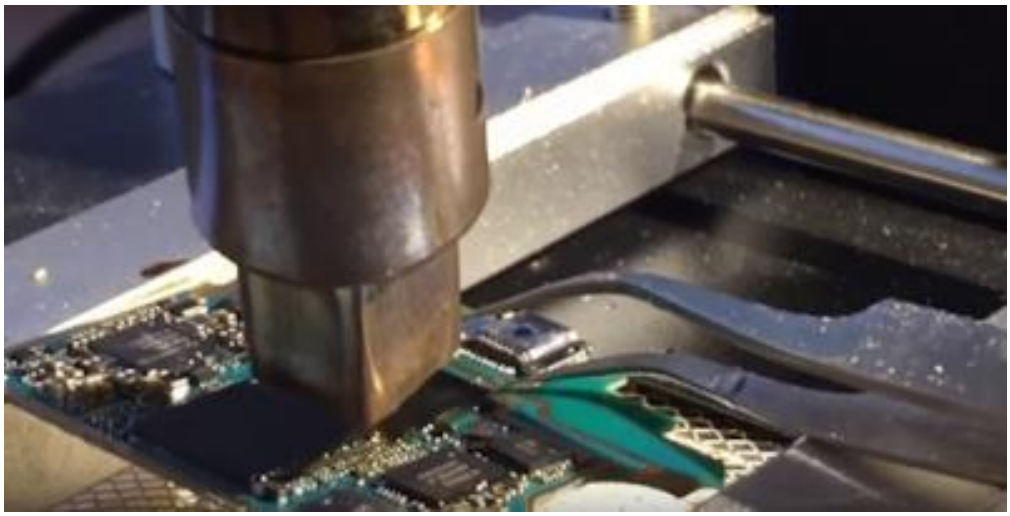
Chip-off je učinkovita ali destruktivna metoda i uobičajeno se koristi kao zadnja solucija za izdvajanje podataka. Ova vrsta ekstrakcije neovisna je o tipu memorije korištene u zaplijenjenom uređaju i pruža mogućnost zaobilaženja gotovo svih implementiranih sigurnosnih mehanizama. U odnosu na neinvazivne metode ekstrakcije, *chip-off* metoda zadržava integritet informacije i ekstrahira potpunu fizičku sliku memorijskog modula, [21].

Proces ekstrakcije podataka ovom metodom podijeljen je u četiri koraka:

1. Fizičko uklanjanje memorijskog modula.
2. Čišćenje i možebitni popravak memorijskog čipa.
3. Ekstrakcija pohranjenih podataka.
4. Analiza dobavljenih podataka.

4.1.1. Fizičko uklanjanje memorijskog modula

Postupak fizičkog uklanjanja memorijskog modula zahtjeva rastavljanje uređaja i korištenje specijalizirane opreme ili lemilice za uklanjanje samog memorijskog čipa sa matične ploče uređaja. Osim korištenja topline, odnosno lemilice potrebno je koristiti kemijska sredstva pomoću kojih će se ukloniti ostaci ljepila.



Slika 5. Odvajanje memorijskog čipa, [22].

Proces odvajanja memorijskog čipa s matične ploče uređaja započinje prethodnim zagrijavanjem cjelokupne matične ploče s ciljem omekšavanja vezivnog sloja između memorijskog modula i matične ploče. Nakon što je proces zagrijavanjem matične ploče završio, započinje se sa procesom uklanjanja memorijskog čipa koji je prikazan na slici 5. Nakon uspješnog odvajanja memorijskog čipa, memorijski je čip potrebno ostaviti da se ohladi te prijeći na slijedeći korak, [22].

4.1.2. Čišćenje i popravak memorijskog čipa

Nakon što je memorijski čip odvojen s matične ploče potrebno ga je postaviti ispod mikroskopa. Za proces čišćenja čipa potrebni su pasta za odlemljivanje, lemilica i alkohol. Pomoću paste za odlemljivanje i lemilice uklanja se vezivni sloj, a nakon što je vezivni sloj uklonjen potrebno je pomoću četkice i alkohola očistiti ostatke s memorijskog čipa. Kada je memorijski čip očišćen potrebno ga je osušiti te se nakon toga može prijeći na proces ekstrakcije podataka iz čipa.

4.1.3. Ekstrakcija podataka

Za ekstrakciju podataka s memorijskog čipa koristi se odgovarajući čitač čipa. Nakon što je čip pravilno postavljen u čitač potrebno je čitač povezati s forenzičkom radnom stanicom. Ekstrakcija podataka provodi se korištenjem nekog od softvera koji podržava čitanje podataka sa uklonjenih čipova.

4.1.4. Analiza podataka

Dobavljeni podaci iz prošlog koraka su sirovi i potrebno ih je analizirati pomoću nekog od dostupnih komercijalnih forenzičkih alata.

Ekstrakcija korištenjem *chip-off* metode pruža brojne prednosti, a neke od njih su podržavanje uređaja koji su zaključani ili fizički uništeni kao i uređaja koji ne posjeduju JTAG priključke te potpuna i vremenski brza ekstrakcija podataka. Korištenje ove metode može biti besmisleno na uređajima koji enkripciju podataka imaju uključenu prema zadanim postavkama. Za provođenje cjelokupnog postupka ekstrakcije forenzički stručnjak mora biti upoznat sa svim izazovima koje ova metoda ekstrakcije podataka donosi, [22].

5. Hardverska i softverska rješenja invazivnih metoda

Provođenje forenzičkih istraživanja u području digitalne forenzike podrazumijeva istraživanje mnoštva digitalnih uređaja i izvora podataka. Forenzički stručnjaci prilikom izvršavanja analize oduzetih uređaja imaju mogućnost korištenja svih njima dostupnih forenzičkih alata. Zbog visoke cijene forenzičkih alata, većina forenzičkih stručnjaka i agencija koje se bave analizom mobilnih uređaja ih ne posjeduje. Zbog navedenog razloga vremenski period potreban za potpunu analizu oduzetih uređaja ovisi o dostupnim forenzičkim alatima. Ukoliko postoji agencija koja posjeduje većinu forenzičkih alata, ona će imati mogućnosti provedbe analize uređaja u puno kraćem vremenskom roku u odnosu na samostalnog forenzičkog stručnjaka čiji su resursi ograničeni, [23]. U ovom poglavlju istražiti će se dostupna sklopovska rješenja za invazivne metode te će biti navedena neka od softverskih rješenja kojima se analizira ekstrahirana slika uređaja dobivena korištenjem invazivnih metoda.

5.1. JTAG i ISP sklopovska rješenja

JTAG i ISP metode ekstrakcije također zahtijevaju fizičko rastavljanje uređaja, a sam proces fizičkog rastavljanja uređaja te alati koji se koriste za provedbu istog objašnjeni su ranije u ovom poglavlju. Nakon što je uređaj koji se ispituje rastavljen potrebno je identificirati JTAG TAP priključke na matičnoj ploči uređaja. Na identificirane TAP priključke potrebno je priključiti odgovarajući JTAG konektor. Ukoliko mobilni uređaj koji se ispituje ne posjeduje TAP priključke koji podržavaju izravno spajanje pomoću JTAG konektora, potrebo je koristiti JTAG konektor koji sa jedne strane posjeduje vodiče koji se moraju precizno zalemiti na odgovarajuće pinove na matičnoj ploči. Nakon izvršavanja navedenog procesa, JTAG kabel je potrebno priključiti na JTAG programator. Jedan od JTAG programatora dostupnih na tržištu prikazan je na slijedećoj slici.

Slika 6. JTAG programator, [24].

Ekstrakcija podataka sa uređaja koji se ispituje provodi se kroz programsko rješenje određenog JTAG programatora. Programsko rješenje najčešće je u obliku aplikacije za operativni sustav Windows. Ugrađeno programsko rješenje predstavlja jednostavno sučelje za oporavak podataka s uređaja.

VR Table prikazan je na idućoj slici i predstavlja alternativno sklopovsko rješenje za provođenje nedestruktivnih metoda ekstrakcije. Ovo sklopovsko rješenje omogućuje forenzičkim ispitivačima izdvajanje podataka s raznih elektroničkih uređaja. *VR Table* opremljen je ručicama koje sadrže vrlo precizne ispitne sonde koje se priključuju na TAP pinove na matičnoj ploči uređaja koji se ispituje.

Slika 7. *VR Table* uređaj,[25].

Prednosti korištenja ovog sklopovskog rješenja u odnosu na uobičajene alate su jednostavnost korištenja, brzina i preciznost provedbe, mogućnost provođenja raznih nedestruktivnih metoda te ekstrakcija podataka s memorijskih modula bez potrebe za lemljenjem i odlemljivanjem.

Provođenje ekstrakcije podataka ISP metodom odvija se na isti način kao i JTAG metoda, jedina razlika u provođenju ove dvije metode je mjesto pristupa na matičnoj ploči. Dok JTAG metoda podrazumijeva priključivanje na ugrađeni priključak, ISP metoda ekstrakcije koristi pinove koji zaobilaze komunikaciju s procesorom te omogućuju izravnu interakciju s memorijskim modulom.

5.2. Chip off sklopovska rješenja

Ekstrakcija podataka korištenjem *chip-off* invazivne metode zahtjeva korištenje raznih alata. Proces izdvajanja fizičke slike s uređaja korištenjem navedene metode sastoji se od nekoliko koraka. Prvi korak ekstrakcije je fizičko rastavljanje uređaja prilikom čega se koriste razni odvijači, puhala vrućeg zraka, vakuumske hvataljke za staklo i sl.

Drugi korak prilikom provođenja ekstrakcije *chip-off* metodom je fizičko uklanjanje memorijskog modula sa matične ploče uređaja koji se ispituje. Za provođenje ovog koraka potrebna je lemna stanica. Nakon uspješnog uklanjanja memorijskog modula s matične ploče najčešće je potrebno provesti proces reparacije pinova memorijskog modula. Navedeni proces provodi se korištenjem *reballing* alata. Komplet za provođenje navedenog procesa prikazan je na idućoj slici.

Slika 8. Komplet za *reballing* proces, [26].

Treći korak ekstrakcije podataka ovom metodom zahtjeva korištenje adaptera i čitača *flash* memorije. Adapteri i čitači često su odvojeni uređaji, ali postoje i ugrađene varijante. Adapteri memorijskih modula su uređaji koji omogućuju prihvat odvojenog memorijskog modula. Čitači memorijskih modula većinom podržavaju sve vrste memorijskih modula, ali zahtijevaju korištenje adaptera koji su namijenjeni za njih.

Slika 9. USB čitač memorijskih modula, [27].

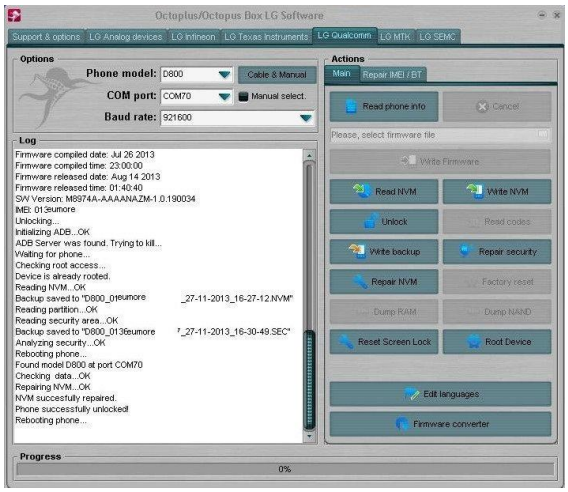
Na slici 9 prikazan je USB čitač čipova sa ugrađenim adapterom za određenu vrstu čipova. Navedeni adapter jednostavan je za upotrebu iz razloga što ne zahtijeva dodatne kablove za povezivanje na radnu stanicu forenzičkog istraživača.

Ekstrakcija i analiza izdvojenih podataka posljednji je korak ekstrakcije podataka *chip-off* metodom. Ovaj koraka podrazumijeva korištenje softverskih rješenja koja će biti opisana kasnije u ovom poglavlju.

5.3. Softverska rješenja

Nakon provedbe fizičkog dijela procesa ekstrakcije podataka potrebno je prijeći na programski dio. Programski dio ekstrakcije podataka podrazumijeva korištenje ugrađenih programskih rješenja različitih čitača čipova, kao i dodatnih programskih rješenja koja su dostupna na tržištu.

Pomoću ugrađenih programskih rješenja moguće je izdvojiti fizičku sliku podataka iz memorije uređaja. Analiza dobivenih podataka provodi se korištenjem nekog od dostupnih forenzičkih alata. Na slici 10 prikazano je sučelje programskog rješenja čitača čipova.



Slika 10. Sučelje ugrađenog programskog rješenja, [28].

Nakon ekstrakcije podataka iz memorije uređaja, dobivene podatke potrebno je analizirati. Za analizu podataka najčešće se koriste softverska rješenja forenzičkih alata. U sljedećim potpoglavljima biti će definirane značajke programskih rješenja za analizu ekstrahiranih podataka pomoću gore navedenih metoda.

5.3.1. Cellebrite UFED Physical Analyzer

UFED Physical Analyzer je programsko rješenje tvrtke *Cellebrite*. Navedeni alat pruža podršku širokom rasponu digitalnih uređaja, aplikacija i servisa u oblaku. Dolazi sa opsežnim setom alata i mogućnosti kojima pruža potporu dublje analize podataka.

Značajke ovog programskog rješenja za mobilnu forenziku su, [29]:

- Pristup širokom rasponu aplikacija, uređaja i tipova podataka – *UFED Physical Analyzer* pruža potporu za više od jedanaest tisuća aplikacija i inačica uređaja.
- Jednostavno korisničko sučelje – Razni vizualni dodaci nadzorne ploče omogućuju forenzičkim stručnjacima da se usredotoče na važne dijelove forenzičke istrage.
- Vremenska vizualizacija događaja – Napredna grafička vremenska crta omogućuje stvaranje temeljitog opisa događaja i pruža mogućnost pozicioniranja na određeni dio vremenskog odsječka koji je važan za proces forenzičke istrage.
- Oporavak izbrisanih podataka – Ovo programsko rješenje nudi mogućnost rezbarenja ne dodijeljenog prostora iz memorije uređaja. Time se omogućuje oporavak izbrisanih informacija i datoteka.
- Pregled podataka aplikacije u izvornom obliku – Omogućuje se stvaranje emulacije određene aplikacije s ciljem lakšeg analiziranja izdvojenih podataka.
- Analiza podataka pohranjenih na oblaku – Korištenjem inačice *UFED Cloud* moguće je izdvojiti podatke društvenih mreža i sigurnosnih kopija pohranjenih u oblaku.
- Analiza prevedenog sadržaja – *UFED Phyisical Analyzer* nudi potporu u obliku prijevoda na zahtjev. Korištenjem navedene mogućnosti forenzički istražitelji mogu analizirati tekstualni sadržaj zapisan na nekom njima nepoznatom jeziku.
- Stvaranje jednostavnih izvještaja – Svaki sudionik forenzičkog procesa koristeći adekvatan alat može pristupiti objavljenim izvještajima te ih upotrijebiti za svoje potrebe u vidu forenzičke analize.

5.3.2. Oxygen Forensic Detective

Tvrtka *Oxygen Forensics* pruža razna rješenja u mobilnoj forenzici. Alati ove tvrtke pružaju najnaprednije metode za ekstrakciju digitalnih dokaza i alate za analizu dokaza u svrhu provođenja forenzičke istrage.

Značajke programskog tješenja *Oxygen Forensics Detective*, [30] :

- Vremenska crta – Ova značajka omogućuje analizu svih događaja pohranjenih na uređaju koji su u jednoj listi. Događaji se mogu analizirati za jedan ili više uređaja te se mogu filtrirati prema unesenim postavkama. Kartica geolokacije pruža uvid u geografske koordinate svakog događaja i informacije koja se analizira.
- Analiza socijalne povezanosti uređaja – Nudi se mogućnost stvaranja grafa koji opisuje društvene veze između vlasnika uređaja i njegovih kontakata ili drugih uređaja.
- Kategorizacija slika – Kategorizacija slika pohranjenih na uređaju omogućuje istražiteljima da prilikom unosa izdvojenih podataka definiraju prioritete. Provođenjem analize slika dobiva se izvještaj sa brojem podudarajućih slika za svaku vrstu fotografija.
- Prepoznavanje lica – Ova značajka omogućuje istražiteljima da provedu proces prepoznavanja lica na pohranjenim fotografijama.
- Zapis karata – Ovo programsko rješenje izdvaja podatke o geolokaciji iz svih izvora podataka dostupnih na mobilnom telefonu. Omogućuje identificiranje često posjećenih mjesta i lokacije na kojima se određeni uređaji često nalaze. Forenzički stručnjaci prilikom analize mogu pomoću ove značajke vizualizirati kretnje uređaja u određenom vremenskom periodu.
- Pretraživanje datoteka – Omogućuje se pretraživanje različitih podataka na uređaju.
- Analiza aplikacija – Ova značajka istražiteljima omogućuje provedbu analize svake aplikacije pomoću ugrađenog analizatora.

5.3.3. Elcomsoft Mobile Forensic Bundle

Tvrtka *Elcomsoft* razvila je paket programskih rješenja za mobilnu forenziku koji omogućuje ekstrakciju i analizu podataka sa mobilnih uređaja pokretanih operativnim sustavima iOS i BlackBerry. Neke od glavnih značajka ovog paketa programskih rješenja su, [31] :

- Fizička, logička i ekstrakcija preko zraka – Ova značajka omogućuje forenzičkim istražiteljima da provedu ekstrakciju podataka sa iOS uređaja pomoću svih dostupnih metoda ekstrakcije za iste.
- Ekstrakcija Google računa – Omogućuje se ekstrakcija velikih količina podataka pohranjenih u oblaku i stvaranje izvještaja koji je razumljiv čovjeku.
- Ubrzavanje procesa pomoću grafičke kartice – Navedena značajka koristi se prilikom razbijanja zaporki kojima su zaštićene sigurnosne kopije.

5.3.4. Belkasoft Evidence Center

Korištenjem ovog programskog rješenja istražitelji na relativno jednostavan način mogu izdvojiti, analizirati i pohraniti digitalne dokaze iz različitih digitalnih uređaja, RAM memorija i mrežnih servisa za pohranu. *Belkasoft Evidence Center* programsko rješenje automatizirano analizira izdvojene podatke te istražiteljima prikazuje forenzički najrelevantnije dokaze.

Značajke ovog programskog rješenja su, [32] :

- Potpuno automatizirana ekstrakcija i analiza za praktički sve vrste digitalnih dokaza
- Rezbarenje uništenih i skrivenih podataka
- Trenutna analiza RAM memorije
- Potreba za bilo kakvim predznanjem je minimalna
- Mogućnost pretraživanja sadržaja višestrukih slučajeva
- Ekstrakcija podataka na daljinu
- Mogućnost dekriptiranja šifriranih sigurnosnih kopija.

6. Izazovi forenzičke analize i mogućnosti invazivnih metoda

U ovom poglavlju definirat će se izazovi forenzičke analize koji proizlaze iz činjenice da se podacima pohranjenima na mobilnim uređajima može jednostavno pristupiti te da se mogu sinkronizirati na više uređaja, što znači da mogu biti pohranjeni ne više lokacija. Jedan od najvećih forenzičkih izazova je nestabilnost podataka te je za očuvanje istih potrebno uložiti puno više napora.

Korištenjem određene metode za ekstrakciju podataka dobivaju se razne mogućnosti za izdvajanje različitih vrsta podataka i zaobilaženja implementiranih sigurnosnih rješenja. Mogućnosti *chip-off*, JTAG i ISP metoda za ekstrakciju biti će navedene u idućem dijelu ovog poglavlja.

6.1. Izazovi forenzičke analize

Polje mobilne forenzike u stalnom je napretku i podrazumijeva korištenje raznih novih tehnologija koje pružaju mogućnost pristupa podacima s MTU-a. Zbog progresivnog razvoja tehnologije sve više protuzakonitih radnji prisutno je u digitalnom svijetu, a pritom ostaju zabilježeni tragovi koji mogu postati važni digitalni dokazi u provedbi istrage.

U ovom potpoglavlju opisani su neki od izazova koje forenzički stručnjaci susreću u svakodnevnom provođenju forenzičkih istraga.

- Root otključavanje uređaja – Operativni sustav prema zadanim podešavanjima korisnicima dodjeljuje niži stupanj privilegija korištenja uređaja. Pomoću *root* otključavanja korisnik dobiva administrativne ovlasti kojima se omogućuje pristup procesima operativnog sustava koji nisu dostupni korisnicima koji nemaju administrativne ovlasti. *Root* otključavanjem uređaja gubi se garancija proizvođača i postoji mogućnost ugroze sigurnosti zbog korištenja uređaja sa dostupnim svim administrativnim ovlaštenjima. Prilikom provođenja forenzičke analize uređaja istraživač će ovisno o metodi ekstrakcije koju koristi biti primoran izvršiti *root* otključavanje uređaja. Navedeni proces provodi se kako bi se mogle dobaviti informacije potrebne za daljnji napredak forenzičke analize. Proces ekstrakcije podataka korištenjem nekog forenzičkog alata koji zahtjeva *root* otključavanje može postati jako zahtjevan zbog raznolikosti dostupnih uređaja koji imaju različite značajke. Ukoliko istražitelj odluči provesti *root* otključavanje uređaja koji je zaplijenjen, ostvarit će mogućnost provedbe puno opsežnije ekstrakcije podataka, [33].

- Odabir logičke ili fizičke ekstrakcije podataka – Mobilna forenzika posjeduje dvije osnovne vrste ekstrakcije podataka, fizičku i logičku. Fizička ekstrakcija podrazumijeva izvadak fizičke slike memorije koja sadrži obje vrste podataka; trenutne podatke i izbrisane podatke. Podaci koji se dobave procesom fizičke ekstrakcije nalaze se u sirovom obliku te ih je potrebno dodatno prevoditi u ovisnosti od korištenog datotečnog sustava. Logička ekstrakcija provodi se instruiranjem procesora uređaja da kopira sve dostupne datoteke iz datotečnog sustava. Podaci koji se dobave ovom metodom ekstrakcije su aktivni korisnički podaci kao što su slike, kontakti, popisi poziva i slično. Odabir odgovarajuće metode za ekstrakciju podatak ovisi o faktorima kao što su vrijeme dostupno za provođenje ekstrakcije, vrsta podataka koja se želi dobaviti i temeljitost provođenja odabrane metode ekstrakcije podataka.
- Sigurnosni mehanizmi – Sigurnosni mehanizmi koriste se s ciljem zaštite podataka MTU-a. Mehanizmi koji se koriste variraju od jednostavnijih u obliku zaštite zaporkom ili PIN kodom do složenijih mehanizama poput enkripcije podataka. Ukoliko je oduzeti uređaj zaštićen zaporkom potrebno je koristiti adekvatno softversko rješenje kako bi se dobavila informacija. MTU koji koristi enkripciju podataka nastoji onemogućiti dobavu pohranjenih podataka. Procesom enkripcije izvorni zapis podataka se izmjenjuje korištenjem enkripcijskog algoritma, [34]. Vrsta enkripcije koja se provodi može biti simetrična enkripcija i enkripcija korištenjem javnog ključa. Simetrična enkripcija koristi jedan ključ za provedbu procesa enkripcije i dekripcije podataka. Ukoliko je enkripcijski ključ pohranjen na uređaju, moguće je provesti njegovu ekstrakciju i dekriptirati štićeni sadržaj. Enkripcija pomoću javnog ključa podrazumijeva korištenje javno dostupnog ključa za provođenje enkripcije podataka i drugog ključa koji je dostupan određenim korisnicima kako bi se kriptirani sadržaj otključao.
- Operativni sustav mobilnog uređaja - Provođenje forenzičke analize postaje zahtjevnije zbog svakodnevnog povećanja inačica mobilnih operativnih sustava. Istražitelji najčešće nailaze na operativni sustav Android, dok su operativni sustavi iOS, BlackBerry i Windows nešto rjeđa pojava u forenzičkoj analizi. Navedeni operativni sustavi i njihove različite inačice se pokreću na velikom broju uređaja te je zbog toga ekstrakcija podataka čak i sa istog operativnog sustava različite težine.
- Hardverske razlike – Tržište mobilnih uređaja preplavljeno je različitim modelima različitih proizvođača uređaja. Svaki proizvedeni mobilni uređaj sastoji se od mikroprocesora, memorijskog modula, zaslona osjetljivog na dodir i raznih dodatnih

modula. U stvarnosti mobilni uređaji sadrže sve navedene elemente ali se međusobno bitno razlikuju prema fizičkoj veličini, ugrađenom hardveru, operativnom sustavu i značajkama. U današnje vrijeme trend razvoja novih uređaja je progresivan te od forenzičkih stručnjaka zahtijeva neprestano informiranje o novim izazovima koji se nameću i mogućnostima provedbe ekstrakcije sa određenim forenzičkim alatima za svaki uređaj.

- Pohrana podataka u oblaku – Kapacitet pohrane mobilnih uređaja nerijetko je ograničen te korisnici svoje podatke pohranjuju na mrežnim servisima. Podaci koje korisnici najčešće pohranjuju na servise u oblaku su sigurnosne kopije koje sadrže veliku količinu podataka koja može sadržavati bitne informacije za daljnji napredak forenzičke analize. Ekstrakcija navedenih podataka iz servisa za pohranu u oblaku od iznimne je važnosti ukoliko je uređaj koji je oduzet neispravan ili zaključan. Dobava podataka pohranjenih u oblaku je ograničena zbog implementiranih raznih sigurnosnih mehanizama i pravnih ograničenja. Za provedbu ekstrakcije u oblaku potrebno je koristiti specijalizirana softverska rješenja.
- Metode antiforenzike – Antiforenzika je skup postupaka i tehnika koje se izvršavaju s ciljem skrivanja tragova i zapisa ili brisanja podataka. Anti-forenzičke metode se osim za navedene zlonamjerne radnje koriste za unaprjeđivanje forenzičkih postupaka i razvoj novih ili već prisutnih forenzičkih alata, [35]. Skrivanje podataka je metoda antiforenzike kojom se podaci od iznimne važnosti za forenzičku istragu skrivaju te samim time produžuju vrijeme potrebno za otkrivanje takvih dokaza. Ovom se metodom podaci ne žele uništiti već se pokušava dokaze učiniti manje vidljivima tijekom procesa forenzičke istrage. Brisanje podataka najčešće je korištena antiforenzička metoda koja podrazumijeva fizičko uništavanje memorije kako bi se obrisali svi podaci koji mogu biti od koristi u forenzičkoj analizi. Osim fizičkog uništavanja memorije, podatke je moguće obrisati zapisivanjem novih podataka preko postojećih ili zapisivanjem točno definiranih vrijednosti na određene sektore memorije kako bi se onemogućio povratak izvorni podataka, [35]. Skrivanje tragova je metoda čiji je cilj preusmjeravanje tijeka forenzičke istrage. Ovom se metodom omogućuje skrivanje tragova počinitelja korištenjem raznih alata za čišćenje tragova aktivnosti, metoda za zamjenu IP adresa i sl. Napadi na forenzičke alate predstavljaju posljednju vrstu antiforenzičkih metoda, a podrazumijevaju napade i zavaravanje forenzičkih alata koji se koriste u digitalnoj istrazi. Softverska rješenja koja se koriste za navedene radnje

imaju mogućnost promjene sistemskog vremena, brisanja sadržaja pregledavanja i predmemorije, [36].

- Zlonamjerni programi – Uređaj koji se ispituje može sadržavati zlonamjerni kod koji se može prenijeti na ostale uređaje putem žične ili bežične veze, [10].
- Dostupnost forenzičkih alata – Niti jedan forenzički alat nije u mogućnosti podržati sve zahtijevane funkcije i uređaje. Navedeno nije izvedivo iz jednostavnog razloga što na tržištu postoji vrlo velik broj uređaja od kojih je samo nekolicina podržana od strane nekog alata mobilne forenzike. Forenzički ispitivač koji provodi istragu najvjerojatnije ne posjeduje sve dostupne alate mobilne forenzike te se zbog toga javlja potreba za korištenjem kombinacije raznih alata kako bi se ekstrahirala maksimalna količina podataka, [37].
- Pravna pitanja – Mobilni uređaji mogu biti uključeni u protuzakonite radnje koje prelaze državne granice. Kako bi proveo istragu takvih slučajeva, forenzički stručnjak mora biti upoznat sa prirodom nezakonite radnje i zakona pojedine države unutar koje je ta radnja počinjena, [10].

6.2. Mogućnosti invazivnih metoda

Invazivne metode ekstrakcije podataka predstavljaju dio mobilnih forenzičkih postupaka čiji je početni uvjet fizičko rastavljanje zaplijenjenog uređaja. Ova vrsta mobilnih forenzičkih metoda može se podijeliti u dvije skupine. Prva skupina invazivnih metoda za ekstrakciju podataka je skupina nedestruktivnih metoda u koju pripadaju JTAG i ISP. Osim spomenutih nedestruktivnih metoda postoje destruktivnije metode ekstrakcije podataka kao što je *chip-off*. Takve metode smatraju se destruktivnim metodama zato što postoji velika vjerojatnost od nemogućnosti ponovnog korištenja mobilnog uređaja.

Mogućnosti izdvajanja podataka JTAG metodom:

- Izdvajanje ekstrakcije podataka sa mogućnošću ponovnog korištenja uređaja
- Izdvajanje podataka iz uređaja koje drugi forenzički alati ne podržavaju
- Ekstrakcija zaporkom zaštićenih uređaja
- Izdvajanje slike fizički oštećenih uređaja, uspješnost ekstrakcije je manja u odnosu na *chip-off* metodu ekstrakcije

Mogućnosti izdvajanja podataka ISP metodom:

- Izdvajanje sadržaja s eMMC memorijskih modula
- Provođenjem ekstrakcije podataka iz uređaja i ponovnim sklapanjem, uređaj će biti moguće koristiti
- Visoka brzina ekstrakcije
- Izdvajanje slike uređaja koji nisu podržani od strane drugih forenzičkih alata
- Ekstrakcija podataka iz fizički oštećenih uređaja, uspješnost izdvajanja podataka veća je u odnosu na JTAG metodu

Mogućnosti ekstrakcije podataka *chip-off* metodom:

- Izdvajanje slike uređaja koji su zaštićeni zaporkom
- Ekstrahiranje podataka iz uređaja koji nisu podržani od strane forenzičkih alata
- Izdvajanje slike fizički oštećenih uređaja
- Podržanost ekstrakcije uređaja koji koriste vlastite operativne sustave
- Visoka brzina ekstrakcije

7. Zaključak

Forenzička analiza mobilnih terminalnih uređaja je u stalnom porastu, jer digitalne tehnologije napreduju svakodnevno. Sukladno razvoju digitalnih tehnologija raste i broj nezakonitih radnji. Kako bi se smanjio rast nezakonitih radnji povezanih sa mobilnim tehnologijama potrebno je razvijati forenzičke tehnologije koje će to onemogućiti. Jedan od najefikasnijih načina suzbijanja kriminalnih radnji je forenzička analiza koja u relativno kratkom roku otkriva identitet počinitelja i pronalazi digitalne dokaze od velike važnosti.

Provođenjem forenzičke analize forenzički stručnjak mora nastojati poštovati osnovna načela forenzičke znanosti, što znači da sam istražitelj mora biti visoko kvalificiran, tj. mora biti adekvatno obučen za rad u nekom od forenzičkih rješenja i mora biti dobro upoznat sa problematikom slučaja koji istražuje iz svih gledišta. Alati za forenzičku analizu prvenstveno služe kao pomagalo koje istražitelju olakšava izdvajanje i analizu podataka koji su potencijalni digitalni dokazi od velike važnosti. Mogućnosti forenzičkih alata ovise o stručnosti istražitelja koji njima rukuje i o njihovoj financijskoj vrijednosti. Besplatni ili jeftiniji forenzički alati u odnosu na one puno skuplje imaju ograničene mogućnosti.

Provedbom forenzičke analize nad mobilnim terminalnim uređajem korištenjem invazivnih metoda ekstrakcije moguće je izdvojiti podatke koji nisu vidljivi drugim forenzičkim metodama za ekstrakciju. Podaci koji se dobave invazivnim metodama često su značajniji u odnosu na podatke dobivene nekom od osnovnih metoda za ekstrakciju podataka.

Literatura

[1] Afonin O, Katalov V. Mobile Forensics – Advanced Investigative Strategies. Birmingham: Packt Publishing Ltd.; 2016.

[2] National Institute for Standards and Technology (2013) Guidelines on Mobile Device Forensics(Draft) Gaithersburg U.S. Department of Commerce Preuzeto sa: http://www.nist.gov/forensics/research/upload/draft-guidelines-on-mobile-deviceforensics.pdf [Pristupljeno: rujan 2020.]

[3] https://infoteh.etf.ues.rs.ba/zbornik/2018/radovi/RSS-3/RSS-3-6.pdf [Pristupljeno: rujan 2020.]

[4] https://www.researchgate.net/publication/287723267_Mobile_forensics_using_the_harmonised_digital_forensic_investigation_process [Pristupljeno: rujan 2020.]

[5] Forenzika mobilnih uređaja mogućnosti i izazovi iOS & Android. Preuzeto sa: https://infoteh.etf.ues.rs.ba/zbornik/2018/radovi/RSS-3/RSS-3-6.pdf [Pristupljeno: rujan 2020.]

[6] https://edecdf.com/products/eclipse-3-pro-kit?variant=30205372268626 [Pristupljeno: rujan 2020.]

[7] Forensics Data Acquisition Methods for Mobile Phones. Preuzeto sa: https://www.researchgate.net/publication/261465980_Forensics_data_acquisition_methods_for_mobile_phones [Pristupljeno: rujan 2020.]

[8] Android Forensic Logical Acquisition. Preuzeto sa: https://resources.infosecinstitute.com/android-forensic-logical-acquisition/#gref [Pristupljeno: rujan 2020.]

[9] Your Mobile Device – The Best Piece of Evidence in an Investigation. Preuzeto sa: https://www.alvarezandmarsal.com/insights/your-mobile-device-best-piece-evidence-investigation#:~:text=File%20System%20Acquisition%3A%20A%20file,using%20a%20SQLite%20database%20platform [Pristupljeno: rujan 2020.]

[10] Tamma R, Skulkin O, Mahalik H, Bommisetty S. Practical mobile forensics : A hands-on guide to mastering mobile forensics for the iOS, Android, and the Windows phone platforms. Birmingham: Packt Publishing Ltd.; 2018.

[11] Use of flasher boxes for mobile forensics. Preuzeto sa: http://www.studioag.pro/en/2011/10/le-flasher-box-per-lanalisi-forense-dei-cellulari/ [Pristupljeno: rujan 2020.]

[12] Use of JTAG boundary-scan for testing electronic circuit boards and systems. Preuzeto sa: https://www.researchgate.net/publication/224344598_Use_of_JTAG_boundary-scan_for_testing_electronic_circuit_boards_and_systems [Pristupljeno: rujan 2020.]

[13] ISP (In-System Programming) training. Preuzeto sa: https://teeltecheurope.com/computer-forensic-training/isp/ [Pristupljeno: rujan 2020.]

[14] JTAG Forensics. Preuzeto sa: http://www.binaryintel.com/services/jtag-chip-off-forensics/jtag-forensics/ [Pristupljeno: rujan 2020.]

[15] What is JTAG?. Preuzeto sa: https://www.corelis.com/education/tutorials/jtag-tutorial/what-is-jtag/ [Pristupljeno: rujan 2020.]

[16] What is the IEEE 1149.6 Standard?. Preuzeto sa: https://www.keysight.com/main/editorial.jspx?cc=HR&lc=eng&ckey=2060779&nid=-11143.0.00&id=2060779 [Pristupljeno: rujan 2020.]

[17] cJTAG IEEE 1149.7 Standard. Preuzeto sa: https://www.electronics-notes.com/articles/test-methods/boundary-scan-jtag-ieee1149/compact-cjtag-ieee-1149-7.php [Pristupljeno: rujan 2020.]

[18] JTAG Explained: Why "IoT", Software Security Engineers, and Manufacturers Should Care. Preuzeto sa: https://blog.senr.io/blog/jtag-explained [Pristupljeno: rujan 2020.]

[19] Technical Guide to JTAG. Preuzeto sa: https://www.xjtag.com/about-jtag/jtag-a-technical-overview/ [Pristupljeno: rujan 2020.]

[20] Investigation of JTAG and ISP Techniques for Forensic Procedures. Preuzeto sa: https://comserv.cs.ut.ee/home/files/pappas_cybersecurity_2017.pdf?study=ATILoputoo&reference=BE2138E95B31179324FF14E71176FCDB482D24DD [Pristupljeno: rujan 2020.]

[21] Napredni forenzički postupci: Chip-off. Preuzeto sa: https://digitalna-forenzika.com/napredni-forenzicki-postupci-chip-off/ [Pristupljeno: rujan 2020.]

[22] How to Save Lost Data from a Dead Phone Using Chip-Off Data Recovery. Preuzeto sa: https://flashfixers.com/recover-data-dead-phone-chip-off-data-recovery/ [Pristupljeno: rujan 2020.]

[23] Tools up: the best software and hardware tools for computer forensics. Preuzeto sa: https://www.group-ib.com/blog/digital_forensics_tools [Pristupljeno: rujan 2020.]

[24] https://z3x-team.com/ [Pristupljeno: rujan 2020.]

[25] VR-Table. Preuzeto sa: https://www.teeltech.com/mobile-device-forensic-hardware/vr-table/ [Pristupljeno: rujan 2020.]

[26] Reballer Kit. Preuzeto sa: https://teeltechcanada.com/digital-forensic-equipment/chip-off/reballer-kit/ [Pristupljeno: rujan 2020.]

[27] Mobile Forensics Tool-Chip off. Preuzeto sa: http://www.meltak.com/Product-MobileForensicsTool.html [Pristupljeno: rujan 2020.]

[28] Octoplus/Octopus box LG software. https://octoplus-octopus-box-lg-software.software.informer.com/ [Pristupljeno: rujan 2020.]

[29] https://www.cellebrite.com/en/physical-analyzer/ [Pristupljeno: rujan 2020.]

[30] 10 Analytical Features Available in Oxygen Forensic Detective. Preuzeto sa: https://blog.oxygen-forensic.com/10-analytical-features-available-in-oxygen-forensic-detective/ [Pristupljeno: rujan 2020.]

[31] Elcomsoft Mobile Forensic Bundle. Preuzeto sa: https://www.elcomsoft.com/emfb.html [Pristupljeno: rujan 2020.]

[32] 10 Reasons To Use Belkasoft Evidence Center. Preuzeto sa: https://belkasoft.com/10-reasons-to-use [Pristupljeno: rujan 2020.]

[33] Smartphone Forensic Challenges. Preuzeto sa: https://www.researchgate.net/publication/336221775_Smartphone_Forensic_Challenges [Pristupljeno: rujan 2020.]

[34] 10 challenges in mobile forensics. Preuzeto sa: https://www.t3k.ai/allgemein-en/10-main-challenges-in-mobile-forensics2/ [Pristupljeno: rujan 2020.]

[35] Digitalne antiforenzičke tehnike. Preuzeto sa: https://sigurnostnamrezi.wordpress.com/2015/12/08/digitalne-antiforenzicke-tehnike/ [Pristupljeno: rujan 2020.]

[36] Digitalna antiforenzika–manipulacija procesom digitalne istrage. Preuzeto sa: https://www.researchgate.net/publication/279175024_Digitalna_antiforenzika-manipulacija_procesom_digitalne_istrage [Pristupljeno: rujan 2020.]

[37] The Forensic Process Analysis of Mobile Device. Preuzeto sa: https://ijcsit.com/docs/Volume%206/vol6issue05/ijcsit20150605150.pdf [Pristupljeno: rujan 2020.]

Popis kratica

ASCII	American Standard Code for Information Interchange
BGA	Ball Grid Array
BSDL	Boundary scan description language
BSR	Boundary Scan Register
eMMC	Embedded MultiMedia Controller
IEEE	Institute of Electrical and Electronics Engineers
ISP	In-System Programming
JTAG	Joint Test Action Group
LVDS	Low Voltage Differential Signals
MMC	MultiMedia Card
MTU	Mobilni terminalni uređaj
SoC	System on a chip
TAP	Test Access Port
TCK	Test Clock
TDI	Test Data In
TDO	Test Data Out
TMS	Test Mode Select
TRST	Test Reset

Popis slika

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **Invazivne metode za ekstrakciju podataka mobilnih uređaja**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 8.9.2020

Matko Đurić

(potpis)