Forenzička analiza mobilnih terminalnih uređaja alatom NowSecure Forensics

Brletić, Luka

Undergraduate thesis / Završni rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:923823

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository







SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Luka Brletić

FORENZIČKA ANALIZA MOBILNIH TERMINALNIH UREĐAJA ALATOM NOWSECURE FORENSICS

ZAVRŠNI RAD

Zagreb, 2016.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

FORENZIČKA ANALIZA MOBILNIH TERMINALNIH UREĐAJA ALATOM NOWSECURE FORENSICS

FORENSIC ANALYSIS OF MOBILE TERMINAL DEVICES USING NOWSEURE FORENSICS TOOL

Mentor: Siniša Husnjak, mag. ing. traff.

Student: Luka Brletić
JMBAG: 0135227800

Zagreb, kolovoz 2016.

FORENZIČKA ANALIZA MOBILNIH TERMINALNIH UREĐAJA ALATOM NOWSECURE FORENSICS

SAŽETAK

Forenzička analiza mobilnih terminalnih uređaja se provodi kako bi se s uređaja prikupili podaci koji mogu biti presudni za sudske postupke. Ovisno o vrsti mobilnih terminalnih uređaja koriste se različite vrste ekstrakcija podataka i različiti alati. NowSecure Forensics je jedan od takvih alata koji omogućuje analizu mobilnog terminalnog uređaja. U usporedbi sa sličnim alatima ističe se po svojim karakteristikama, ali ima nedostatke. U ovom radu na dva primjera provedena je digitalna forenzička analiza mobilnih terminalnih uređaja inačicom Now Secure Forensics Community Edition. Pomoću rezultata analize procijenjene su mogućnosti alata i situacije u kojima je najpogodnije koristiti spomenuti alat, odnosno u kakvom okruženju daje najbolje rezultate.

KLJUČNE RIJEČI: mobilni terminalni uređaj; digitalna forenzička analiza; ekstrakcija podataka

SUMMARY

Forensic analysis of mobile terminal devices is carried out in order to collect data from devices that may be critical for the court proceedings. Depending on the type of mobile terminal devices various types of data extraction and different tools will be used. NowSecure Forensics is one of the tools which allows analysis of the mobile terminal device. Compared to similar tools it stands out for its characteristics, but has drawbacks. In this thesis digital forensic analysis of mobile terminal devices is carried out in the two examples with the NowSecure Forensics Community Edition version. Using the result of the analysis tool features and situation in which it is the most appropriate to use the tool are evaluated, and the environment for gaining best results is estimated.

KEY WORDS: mobile terminal device; digital forensic analysis; data extraction

SADRŽAJ

1. Uvod 1

2. Postupci i metode ekstrakcije podataka 3

2.1. Ručna, logička i datotečna ekstrakcija podataka 4

2.2. Fizička, JTAG i *chip-off* ekstrakcija podataka 5

2.2.1. Fizička ekstrakcija podataka 5

2.2.2. Ekstrakcija podataka JTAG metodom 6

2.2.3. *Chip-off* ekstrakcija podataka 6

2.3. Ostale metode ekstrakcije 7

3. Karakteristike alata NowSecure Forensics 9

3.1. NowSecure Forensics Community Edition verzija 9

3.2. Osnovne karakteristike 10

3.2.1. Skeniranje i *root* otključavanje MTU-a 10

3.2.2. Logička i datotečna ekstrakcija 12

3.2.3. Ekstrakcija sigurnosne kopije i fizička ekstrakcija 13

3.3. Napredne karakteristike 14

3.3.1. Otključavanje zaslona MTU-a 15

3.3.2. Prikaz podataka na karti i vremenskoj crti 16

3.3.3. Funkcija pretraživanja 18

3.4. Zakonska regulativa – zaštita osobnih podataka 19

4. Usporedba mogućnosti s drugim alatima forenzičke analize 21
4.1. Usporedba mogućnosti forenzičkih alata 21
4.2. Karakteristike odabranih forenzičkih alata 23
5. Forenzička analiza mobilnih terminalnih uređaja 25
5.1. Forenzička analiza MTU-a Sony Xperia Miro 25
5.2. Forenzička analiza MTU-a Sony Xperia Z1 30
6. Zaključak 36
Literatura 37
Popis kratica 39
Popis slika 40
Popis tablica 41

1. UVOD

Suvremeni svijet postaje sve više digitaliziran i ljudima se nudi mnoštvo digitalnih sadržaja koje nemaju vremena konzumirati i time se sadržaj i njegova konzumacija premješta na mobilne terminalne uređaje (MTU). MTU omogućuju ljudima konzumiranje digitalnog sadržaja i istovremeno ih ne ograničava u njihovom kretanju zbog mobilne prirode takvih uređaja. Sva komunikacija, koja je neophodna za socijalni aspekt čovjeka, ima svoj digitalni oblik bilo to pošta, razgovori, poruke, ploče s obaviješću ili reklamni paneli.

Kako je korištenje MTU-a u današnjem digitalnom svijetu neophodno ako osoba želi ostati u toku s najnovijim događajima bez obzira gdje se nalazila i/ili ako želi biti uvijek dostupna, to znači kako i osobe s malicioznim namjerama i/ili osobe koje mogu biti sudionici u nekom kaznenom djelu također koriste MTU. MTU se može koristiti i kao sredstvo napada na informacijsko-komunikacijske (IK) sustave, kao sredstvo koordinacije takvog napada, ali i u tradicionalnim kaznenim djelima. Komunikacija takvih osoba može otkriti puno o njima, gdje su se nalazili, koji im je cilj te može otkriti njihove buduće namjere.

Kako bi se analizirala komunikacija, kao i digitalni sadržaj, malicioznih osoba potrebno je provesti digitalnu forenzičku analizu njihovog MTU-a. Forenzičke znanosti su one koje su važne pred sudovima jer omogućuju sudovima da utvrde relevantne činjenice za svoje postupke. E-forenzika ili digitalna forenzika su postupci, procedure i metode u prikupljanju i analizi entiteta u IK sustavu.

MTU je razliku od osobnog računala sadrži privatniji sadržaj i u većini slučajeva vlasnik MTU-a takav sadržaj dijeli samo s jako bliskim osobama. Tako forenzička analiza MTU-a može ponuditi oslobađajuće dokaze obrani ili osuđujuće dokaze tužitelju. Kako bi se pribavili takvi dokazi, potrebno je koristiti alate za digitalnu forenziku koji su u mogućnosti analizirati sve ili većinu vrsta suvremenih MTU-a.

Jedan od takvih alata je NowSecure Forensics i njegova inačica Now Secure Forensics CE (engl. *Community Edition*). Baziran na Linux platformi u mogućnosti je vršiti više vrsta ekstrakcije podataka, prikazati dobivene podatke grafovima, pretražiti sadržaj ključnom riječi te čak zaobilaziti i/ili probijati zaštite na MTU-u kao što je zaslon zaključan lozinkom i PIN (engl. *Personal Identification Number*) brojem. Nakon što je analiza završena izrađuje se izvještaj koji se kasnije može koristiti u druge svrhe.

U ovom radu će biti analizirane mogućnosti i karakteristike alata NowSecure Forensics i njegove CE inačice. U drugom poglavlju će biti objašnjene različite metode

ekstrakcije podatka kako bi se kroz rad moglo razlikovati između mogućnosti različitih alata. Zatim će u trećem poglavlju biti navedene karakteristike alata NowSecure Forensics, odnosno njegove inačice NowSecure Forensics CE. Treće poglavlje je napravljeno uz legitimnu inačicu spomenutog alata te je svaka opisana mogućnost koja je dostupna u CE verziji testirana u okruženju alata koristeći MTU.

U četvrtom poglavlju će se mogućnosti alata NowSecure Forensics CE usporediti s drugim alatima za forenzičku analizu MTU-a i time ocijeniti njegova korisnost. U petom poglavlju će biti provedena forenzička analiza dvaju MTU-a na temelju hipotetskih primjera koji bi se mogli susresti u stvarnosti. Svaki korak opisan u primjerima u petom poglavlju je bio proveden nad uređajima i na slikama su prikazani podaci koju su dobiveni postupcima forenzičke analize MTU-a.

Cilj ovog rada je uspješno testiranje, detaljan prikaz mogućnosti i uporaba alata NowSecure Forensics CE kao i usporedba karakteristika s drugim programskim alatima za digitalnu forenzičku analizu mobilnih terminalnih uređaja.

2. POSTUPCI I METODE EKSTRAKCIJE PODATAKA

Ekstrakcija podataka je postupak prikupljanja podataka, iz medija s podacima, za daljnju obradu i/ili pohranu. U digitalnoj forenzičkoj analizi MTU-a ovaj postupak je nužan u većini slučajeva kako bi se došlo do dokaza ili drugih podataka koji upućuju na daljnje dokaze, [1].

Postupak ekstrakcije podataka s MTU-a ponajprije ovisi o količini podataka koju istraživač forenzičkog procesa želi izvući iz MTU-a. Najjednostavnijim metodama se može dobiti najmanje podataka, ali su najbrže, dok se najkompliciranijim metodama može dobiti najviše podataka, ali je cijeli postupak dugotrajan, zahtijeva posebne uvjete u kojima se mora obavljati i skupu opremu te stručno osoblje i zbog toga je ujedno i rezervirano za službe kao što je policija i vojska i velike privatne tvrtke koje se bave digitalnom forenzičkom analizom. Omjer relativne težine ekstrakcije i brzine je prikazan na slici 1 gdje je najbrža ručna, kojom se prikuplja najmanje podataka, i najsporija metoda Mikro Čitanje (engl. *Micro Read)*, kojom se ujedno i prikuplja najviše podataka, [2].



Slika 1. Usporedba brzine ekstrakcije i količine dobivenih podataka, [3]

Glavne metode ekstrakcije, odnosno one najviše zastupljenije će biti navedene i objašnjene u dva dijela. Prvi dio će obuhvaćati metode koje ne zahtijevaju nikakav dodatni hardver i nije im potreban dodatan softver za izvedbu kao i metode koje imaju minimalne zahtjeve za dodatnim softverom za izvedbu analize koji se ne nalazi na MTU-u i zahtijevaju minimalno osposobljavanje ili osposobljavanje uopće nije potrebno provesti. U drugom dijelu će biti navedene i objašnjene metode koje zahtijevaju dodatan hardver, napredniji softver koji je rijetko dostupan besplatno, i za te metode potrebno je duže

osposobljavanje stručnjaka koji će vršiti forenzičku analizu MTU-a. Metode koje ne spadaju u ove dvije kategorije zbog svojih karakteristika će biti objašnjene zasebno.

2.1. Ručna, logička i datotečna ekstrakcija podataka

Ručna ekstrakcija podataka se vrši preko sučelja MTU-a na kojemu se izvodi forenzička analiza. Istraživač forenzičkog procesa pregledava sadržaj MTU-a, njegove postavke i ostali sadržaj koji je dostupan običnom korisniku koristeći navigaciju kroz datotečni sustav koji MTU pruža svojim grafičkim sučeljem.

Sa svakim prikazom nove informacije na ekranu uzima se slika ekrana pomoću dodatnog fotoaparata. Time se sprema sadržaj ekrana na drugom, vanjskom uređaju, kako bi se mogao iskoristiti u sudskom procesu. Ovakva vrsta ekstrakcije je najjednostavnija i ne zahtijeva dodatna stručna znanja. Ručna ekstrakcija se može provesti samo ako je MTU otključan jer inače istraživač forenzičkog procesa ne može pristupiti sadržaju. Ovakva vrsta ekstrakcije ne zahtijeva nikakvo osposobljavanje, moguće ga je provesti sa svim vrstama MTU-a dok god su otključani, i nisu potrebni dodatni kabeli, [4].

Nedostatak je što se ovime ne može očuvati integritet uređaja i nije moguće pristupiti obrisanim podacima kao i onim podacima koji nisu vidljivi pomoću sučelja MTU-a. Također ova vrsta ekstrakcije zahtijeva puno vremena jer se sve provodi ručno.

Logička ekstrakcija je vrsta ekstrakcije koja kopira podatke s logičkih jedinica za pohranu na MTU-u, kao što su mape i datoteke i sustavna particija memorije. Prednost ovakve ekstrakcije u usporedbi s ručnom je automatsko prikupljanje podataka čime ih istraživač forenzičkog procesa može brže prikupiti s MTU-a, [1].

Sučelje preko kojeg se odvija logička ekstrakcija je najčešće tvorničko sučelje MTU-a kojeg je ugradio proizvođač i služi za sinkronizaciju podataka s osobnim računalom što je u većini slučajeva USB (engl. *Universal Serial Bus*) kabel. Koristeći AT (engl. *Attention Commands*) naredbe preko sučelja s uređajem se pokreće ekstrakcija podataka.

Ovakva vrsta ekstrakcije ne zauzima veliki prostor za pohranu prikupljenih podataka, ali u slučaju da nisu pronađeni nikakvi relevantni podaci za sudski proces za koji istraživač forenzičkog procesa vrši analizu druge vrste ekstrakcije su poželjnije. Logična ekstrakcija ne prikuplja podatke koji su izbrisani jer se takvi podaci ne prikazuju u mapama MTU-a, odnosno logička ekstrakcija ne prikuplja podatke sa dijela memorije

koji nije dodijeljen. Logička ekstrakcija nije u mogućnosti zaobići zaključan ili zaštićen uređaj, [1].

Po količini dohvaćenih podataka između logičke i fizičke nalazi se datotečna ekstrakcija. Datotečna ekstrakcija dohvaća sve datoteke koje su pohranjene na dijelu memorije MTU-a koji se smatra zauzetim. Datotečnom ekstrakcijom je moguće vidjeti raspored sustava datoteka MTU-a, koje aplikacije su instalirane, povijest pregleda stranica u Internet pregledniku i SMS poruke i ostale komunikacijske zapise.

Datotečna ekstrakcija čitanjem SQLite baze podataka i koristeći SQL naredbe dolazi do adresa na kojima se nalaze podatci. Pri zapisivanju podatka na memoriju uređaja adresa memorije gdje je podatak zapisan će se smatrati zauzetom dok korisnik MTU-a ne odluči izbrisati podatak. Pri tom postupku podatak se ne briše, već samo adresa u memoriji gdje se podatak nalazi. Podatak će ostati netaknut dok se drugi podatak ne zapiše na isto mjesto. Tako je moguće doći do nekih podataka koje je korisnik izbrisao, ali na njihovu lokaciju nije zapisan novi podatak. Datotečna ekstrakcija ne može doći do podataka ako je provedeno formatiranje memorije MTU-a, [5].

2.2. Fizička, JTAG i *chip-off* ekstrakcija podataka

Iduće tri vrste ekstrakcija zahtijevaju veće ulaganje u hardver i softver kako bi se uspješno provele. Fizička zahtijeva napredniji softver dok ostale dvije ekstrakcije zahtijevaju dodatan hardver koji će se koristiti u procesu. Osim toga potrebna je i veća razina stručnog znanja eksperta forenzičkog procesa. Zbog navedenih razloga iduće tri ekstrakcije će se obraditi odvojeno od ručne, datotečne i logičke ekstrakcije podataka.

2.2.1. Fizička ekstrakcija podataka

Fizička ekstrakcija je kopiranje i svakog bita koji se nalazi na cijelom fizičkom mediju na kojem se vrši analiza. Najveća prednost ovakve ekstrakcije je obuhvaćanje izbrisanih podataka. Nakon preuzimanja svakog bita sa uređaja potrebno je dekodirati dobivene podatke kako bi se iz njih dobile informacije, [6].

Ova vrsta ekstrakcije je jedna od najzahtjevnijih jer je potrebno zaobići sigurnosne mehanizme koji omogućuju samo uređaju na kojem je medij pohranjen manipulaciju podacima. Zbog toga je fizička ekstrakcija rijetko dostupna u besplatnim alatima zbog potrebnog tehničkog znanja i dostupna je u gotovo svim profesionalnim alatima. Fizička ekstrakcija se vrši preko USB kabela ili neke druge veze s uređajem koji je uključen i ne zahtijeva nikakvu modifikaciju uređaja, [1].

2.2.2. Ekstrakcija podataka JTAG metodom

JTAG (engl. *Joint Test Action Group*) je organizacija osnovana 1985. godine za postavljanje novih industrijskih standarda u elektroničkoj industriji. Specificirali su poseban ulaz za uklanjanje grešaka na procesorima koji ne zahtijeva pristup sistemskim adresama i podatkovnim sabirnicama pod nazivom standard IEEE 1149.1, poznatiji po imenu JTAG. Time je moguće pomoću posebnih priključaka na procesoru pristupiti podacima na uređaju. U zadnjoj fazi testiranja uređaja JTAG pinovi se koriste za provjeru ispravnosti procesora. Pri normalnom radu uređaja JTAG pinovi su automatski isključeni, [7].

Za JTAG ekstrakciju podataka potrebno je u većini slučajeva ukloniti bateriju MTU-a kako bi se rastavio uređaj i pristupilo procesoru pa je potrebno koristiti vanjsko napajanje. Također je potrebno fizički se spojiti na pinove procesora kako bi se omogućilo serijsko sučelje. Pomoću JTAG pinova se vrši ekstrakcija memorije s uređaja kako bi se stvorila forenzička slika na kojoj je moguća daljnja analiza.

Prednosti JTAG metode su višestruke, s tim da je najveća prednost to što je opasnost od korumpiranja podataka tijekom ekstrakcije minimalna, jer JTAG koristi vlastite registre. Ova metoda je neovisna o OS-u MTU-a. Druga prednost je to što JTAG zaobilazi sve sustave zaštite na razini grafičkog sučelja uređaja, što uključuje pinove, alfanumeričke lozinke i uzorke za otključavanje cijelog ili dijelove uređaja, [8].

Ovakva vrsta ekstrakcije je zahtjevna po tome što zahtjeva dodatnu opremu i cijeli postupak nije uvijek isti za sve uređaje. Neki proizvođači se mogu odlučiti na fizičko uklanjanje JTAG pinova na procesorima ili razvijanje vlastitog softvera kojeg koriste na JTAG sučelju. Čak i ako procesor ima na sebi JTAG pinove, nisu uvijek označeni i teško ih je naći. Time se stvara dodatna zapreka koju je potrebno zaobići pri forenzičkoj analizi. Cijeli postupak je spor zbog toga što se mora oprezno rukovati sa procesorom uređaja, [9].

2.2.3. *Chip-off* ekstrakcija podataka

Chip-off je metoda forenzičke ekstrakcije podataka koja uključuje fizičko uklanjanje *flash* memorije uređaja na kojem se vrši analiza. Uklanjanje memorije s matične ploče MTU-a se vrši termičkim postupkom. Pri provođenju ovog postupka postoji opasnost oštećivanja memorije.

Nakon uklanjanja *flash* memorije vrši se ekstrakcija slike uređaja. Kako bi se ovo postiglo potrebno je koristiti čitač memorije uređaja. Potrebni su upravljački programi za

svaku vrstu memorije i ako oni nisu dostupni trebaju se isprogramirati što može biti veoma zahtjevno ako podaci o unutarnjoj strukturi nisu dostupni.

Prednosti ovakve ekstrakcije je što rad sa svim vrstama memorije i zaobilazi sve vrste zaštite osim enkripcije podataka, što ne predstavlja problem ako se iz memorije usporedno i dobavi enkripcijski ključ. *Chip-off* vrši ekstrakciju cijele memorije i zadržava integritet podataka. Najveća prednost ove metode je što se može uspješno obaviti sa oštećenim MTU-em, [4].

Chip-off zahtijeva još veća ulaganja u opremu nego je to slučaj kod JTAG-a jer samo specijalizirani softver nije dovoljan. Pri vađenju memorije moguće ju je oštetiti i neki dokazi se mogu izgubiti. Također nije moguće vratiti MTU u stanje prije ekstrakcije što predstavlja problem ako zakoni zemlje u kojoj se vrši digitalna forenzička analiza zahtijevaju da se MTU-i vrate u prvobitno stanje. Unatoč navedenim nedostatcima, *chip-off* je jedina opcija u uvjetima gdje je uređaj teško oštećen i ostale metode forenzičke analize nisu moguće kao i u uvjetima gdje je MTU funkcionalan, ali procesor nema JTAG pinove i nije moguće probiti zaštitu MTU-a.

2.3. Ostale metode ekstrakcije

Jedna od najpopularnijih metoda ekstrakcije kada skuplje metode nisu dostupne, jest korištenje takozvane Kutije za Bljeskanje (engl. *Flasher Box*, FB) memorije MTU-a. FB se inače koristi za dijagnostiku i servisiranje MTU-a kao što je dodavanje jezičnih postavki uređaja i mijenjanje regionalnih postavki uređaja. FB nije namijenjen za forenziku, niti je ikad bio zamišljen kao takav pa se ova metoda svrstava pod ostale metode.

Zbog svojih svojstava FB-ovi se mogu koristiti za pristup podacima uređaja i mijenjanje IMEI-a i uklanjanje ograničenja za samo jednog operatera. FB se koristi za nisku razinu pristupa podacima, odnosno pristupa podacima zaobilazeći operativni sustav (OS) MTU-a. Za priključivanje uređaja na FB se koristi fizički kabel i nije potrebno nikakvo odlemljivanje ili uklanjanje memorije sa uređaja.

Prednosti su što je u mogućnosti dobaviti skrivene i izbrisane datoteke, kao i mogućnost obaviti ekstrakciju na oštećenom MTU-u. Forenzičku analizu pomoću FB-a je moguće napraviti na zaključanim uređajima kao i na onim MTU-ima koji nemaju SIM (engl. *Subscriber Identity/Identification Module*) karticu. Veliki nedostatak FB, onaj koji postoji jer FB nikad nije zamišljen kao sredstvo za forenzičku analizu, je taj što postoji velika opasnost za integritet podataka. Također nije moguće utvrditi integritet podataka nakon ekstrakcije jer se kopira bit po bit uređaja i prikupljeni podaci nemaju nikakvu strukturu. Jedan od glavnih razloga zašto nije preporučljivo koristiti FB je to što osim čitanja

podataka imaju i mogućnost pisanja podatak na MTU-u čime se gubi vjerodostojnost dokaza, [4].

Jedna od najmanje zastupljenih metoda ekstrakcije podataka u današnjem IK okruženju je ekstrakcija podataka uređaja sa njegove sigurne kopije u Okruženju Računalstvo u Oblaku (engl. *Cloud Computing* ,CC). Kako sigurnost postaje sve više aktualna tako sve više sigurnosnih propusta dolazi na vidjelo. Jedan od takvih sigurnosnih propusta je aktiviranje ažuriranja kopije podataka na uređaju koji se spremaju u CC.

Glavni izazov predstavlja virtualizirano okružje CC-a u kojem je teško doći do podatka određenog MTU-a. Uz to CC je veoma distribuirano okruženje, sva računala nisu na istoj geografskoj lokaciji. Osim podatka koji su s MTU-a kopirani u CC potrebno je doći i do mrežnih zapisa od CC kako bi se utvrdilo kada je podatak dospio na CC. Uz to nema do sada nikakvih forenzičkih alata koji bi omogućili ovakvu ekstrakciju podataka sa CC te ona ovisi o dobroj volji tvrtke koja je vlasnik CC. Prednosti su što se na ovaj način mogu dobaviti podaci sa MTU-a čija lokacija i stanje nisu uopće poznati, [10].

Micro Read je metoda ekstrakcije podataka koja uključuje pregled memorije uređaja pod elektronskim mikroskopom. Ova metoda je veoma spora, zahtijeva sofisticiranu tehničku opremu (elektronski mikroskop) i potreban je tim stručnjaka kako bi se provela. Zbog navedenih razloga ova vrsta ekstrakcije se provodi na razini državnih institucija u slučajevima velikih profila, kada je ugrožena nacionalna sigurnost, i to samo kada su sve druge metode ekstrakcije neuspješne. *Micro Read* također zahtijeva visoku razinu poznavanja građe uređaja nad kojim se vrši analiza.

Prema dostupnim informacijama u nacrtu uputa za provođenje forenzičke analize MTU-a koje je izdao Nacionalni Institut za Standarde i Tehnologiju (engl. *National Institute for Standards and Technology,* NIST) SAD-a u rujnu 2013. godine, nema dostupne komercijalne opreme za *Micro Read* i nema službe za provođenje zakona u SAD-u koja koristi tu metodu. Ovime se može zaključiti kako je *Micro Read* metoda napuštena jer su tijekom vremena metode nižih razina poboljšane te su potpune potisnule potrebu za provođenjem ekstrakcije metodom *Micro Read*, [11].

3. KARAKTERISTIKE ALATA NOWSECURE FORENSICS

NowSecure Forensics je alat za forenzičku analizu i ekstrakciju podataka s MTU-a koji je napravljen i osmišljen od tvrtke NowSecure. Alat je napravljen na Santoku Linux distribuciji koja je namijenjena za forenziku mobilnih uređaja.

Nudi mogućnosti kao što je puna fizička i logička ekstrakcija podataka što uključuje i datotečnu ekstrakciju kao i ekstrakciju sigurnosne rezerve podataka. Također ima mogućnosti otključati privremeno ili trajno lozinu, uzorak i PIN na Android uređajima ako je uključeno uklanjanje pogreški preko USB kabela.

3.1. NowSecure Forensics Community Edition verzija

Pri odabiru alata za forenzičku analizu MTU-a ovoga rada potrebno je bilo razvrstati kriterije koje su potrebni za izradu ovog rada. Alat treba zadovoljiti potrebe nekoga tko još nije imao iskustvo rada forenzičke analize MTU-a i time alat mora biti dovoljno jednostavan za osobu koja ulazi u područje forenzičke analize, [12].

Prvi od tih kriterija je da alat mora biti suvremen i sa svojim mogućnostima mora biti u toku sa tehnologijom današnjih MTU-a. Alati kao što su BitPim su odmah izuzeti jer ne podržavaju MTU-e proizvedene poslije 2009. godine. Rad na zastarjelim alatima nema nikakvog smisla jer ne pružaju nikakvo novo znanje i njihove metode su zastarjele i više se ne mogu upotrijebiti.

Drugi kriterij je da alat mora imati dostupnu besplatnu verziju, ili u najboljem slučaju cijeli biti dostupan bez naplate i pretplate. Time je većina profesionalni alata odmah izuzeta kao što su MOBILedit i MOBILedit! Enterprise, XRY i Cellebrite.

Treći kriteriji obuhvaća besplatne alate i probne verzije profesionalnih alata, odnosno njihove licence. Probna verzija mora trajati dovoljno dugo kako bi se mogao izraditi kvalitetan rad i uz to mora imati glavne značajke alata za forenzičku analizu MTU-a. Ovim zadnjim kriterijem je izuzeta probna verzija MOBILedit Forensics alata zbog njegovog kratkog trajanja od tjedan dana. Sve navedene kriterije zadovoljava alat NowSecure Forensics CE.

NowSecure Forensics CE je verzija koja je namijenjena ne-komercijalnoj uporabi, i kao takva nema neke značajke zbog kojih bi se mogla upotrijebiti u komercijalnu svrhu. NowSecure Forensics CE verzija je zbog svoje namjene besplatna i dostupna je svima koji je žele isprobati. Time je CE verzija prigodna za ovaj rad, jer će se koristiti u istraživačke svrhe, [13]. Značajke koje su izuzete kod CE, a ugrađene su u punu verziju

su fizička ekstrakcija podataka na Android uređajima, logička ekstrakcija iOS uređaja, automatsko generiranje izvještaja, i sastavljanje podataka iz fragmenata kada metapodaci[1] nisu dostupni. Tim izuzetcima je profesionalni program za forenzičku analizu MTU-a spušten na razinu besplatnog programa zadržavši osnovne značajke koje su potrebne za provođenje forenzičke analize MTU-a.

CE se preuzima u obliku kopije virtualnog stroja (engl. *Virtual Machine*, VM) Santoku Linux-a koja ima instaliranu najnoviju verziju NowSecure Forensics CE. Unutar toga se nalazi i dodatni alati za forenziku MTU-a, kao što je Exif Tool i Android Brute Force Encryription. Zbog svega navedenog NowSecure Forensics CE je najbolji izbor alata pomoću kojeg će se obaviti forenzička analiza MTU-a i tijekom toga opisati karakteristike alata za potrebe ovoga rada. Njegove karakteristike se mogu podijeliti na osnovne, one koje su dostupne kod većine sličnih alata, i napredne.

3.2. Osnovne karakteristike

Osnovne karakteristike alata NowSecure Forensics su [13]:

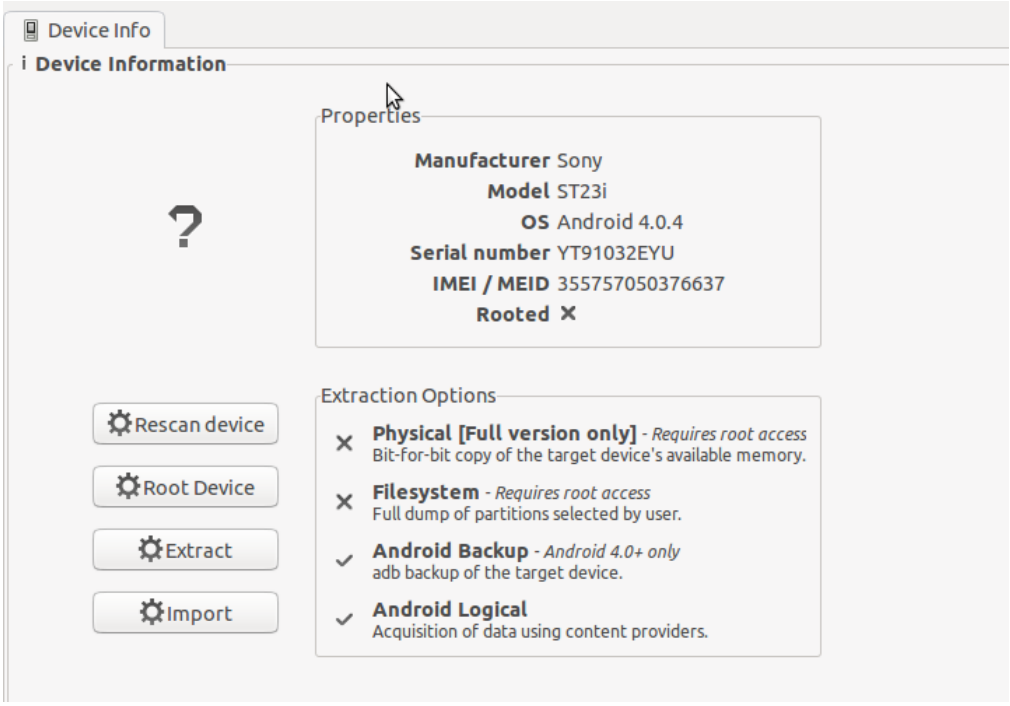
- skeniranje MTU-a pomoću USB veze i otkrivanje specifikacija MTU-a
- *root*[2] otključavanje uređaja
- logička ekstrakcija podataka s Android uređaja
- datotečna ekstrakcija podataka s Android uređaja
- ekstrakcija podataka sa sigurnosne kopije Android uređaja
- unos dodatnih podataka za analizu kao što je Android sigurnosna kopija, Android datotečni sustav, Samsung Kies sigurnosna kopija i iTunes sigurnosna kopija

3.2.1. Skeniranje i *root* otključavanje MTU-a

Skeniranje se pokreće automatski pri spajanju uređaja USB kabelom na osobno računalo na kojemu je pokrenut NowSecure Forensics CE. Skeniranje otkriva osnovne informacije o uređaju kao što je proizvođač uređaja, model uređaja, OS uređaja, serijski broj uređaja, IMEI (engl. *International Mobile Equipment Identity*)/MEID (*engl.* Mobile Equipment Identifier), vremensku zonu na koju je podešen MTU i detektira je li uređaj

[1] Metapodatci su podatci o podatcima, opisuju karakteristike digitalnih podataka
[2] *Root* otključavanje MTU-a označuje postupak pomoću kojega se uklanjaju tvorničke zaštite s MTU-a kako bi se uređaj mogao koristiti u svrhe za koje nije bio prvotno namijenjen.

root otključan ili ne. Navedene informacije se mogu vidjeti na slici 2, gdje su prikazane informacije MTU-a Sony Xperia Miro.



Slika 2. Prikaz osnovnih informacija prikupljenih s MTU-a

Skeniranjem se stječe prvotni uvid u uređaj na kojem će se vršiti analiza. Na temelju dobivenih informacija osoba koja provodi analizu planira sljedeći korak. U slučaju u kojem uređaj nije otkriven, može se ručno pokrenuti ponovno skeniranje uređaja. Ako uređaj i dalje nije uspješno skeniran potrebno je ažurirati program kako bi se osvježila baza podataka uređaja ili uređaj nije kompatibilan s tom verzijom alata.

Serijski broj i IMEI su u stanju povezati specifičan uređaj sa određenim korisnikom i mobilnim operaterom, uspoređujući rezultate s vanjskom bazom podataka kao što je baza podataka mobilnog operatera. Informacije OS označuju i verziju OS što je važno kod načina na koje će se vršiti ekstrakcija podataka jer zadnje verzije OS mogu biti otporne na neke metode. Također služe i za pronalaženje CVE registriranih sigurnosnih propusta te verzije OS-a kako bi se uređaj mogao *root* otključati i kako bi se zaobišla zaštita na uređaju, kao što je lozinka ili uzorak, u svrhu provođenja forenzičke analize.

Root otključavanje uređaja se vrši instaliranjem privremene aplikacije s *root* pristupom na sam uređaj preko USB veze kada je uključeno USB uklanjanje pogrešaka pod naprednim postavkama na Android uređaju. Za ovaj postupak uređaj ne smije imati

lozinku ili ona mora biti probijena postupkom koji će se objasniti u idućem dijelu poglavlja. Alat automatski ponudi rješenje ovisno o uređaju nakon čega korisnik bira rješenje i time *root* otključa uređaj. Za najnovije uređaje ovo možda neće biti moguće jer još nisu otkriveni sigurnosni propusti koji bi to omogućavali.

Nakon što je uređaj *root* otključan moguće je izvršiti datotečnu ekstrakciju koja vrši punu ekstrakciju particija MTU-a koje odabere korisnik. Također je moguće vršiti fizičku ekstrakciju Android uređaja, ali u CE verziji to nije moguće.

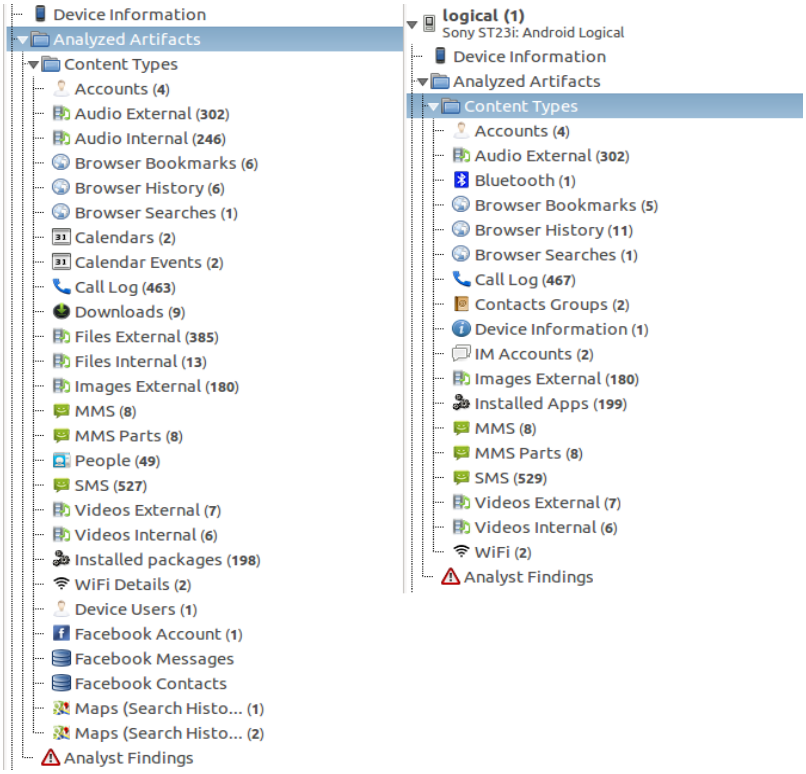
3.2.2. Logička i datotečna ekstrakcija

Datotečna ekstrakcija je po brzini u alatu NowSecure Forensics CE druga, odmah poslije logičke ekstrakcije, ali je u stanju izvući puno veće količine podataka. Navedeni podaci uključuju korisničke račune na MTU-u, audio i video datoteke, označene web stranice, označeni datumi na kalendaru, povijest poziva, preuzimane datoteke, datoteke u memoriji uređaja i vanjskoj memoriji, MMS-ovi, SMS-ovi, popis ljudi i njihove informacije iz imenika, instalirani paketi koji odgovaraju određenim aplikacijama, detalji o svim Wi-Fi vezama na koje se uređaj spajao, kao što su lozinke i njihovi nazivi, Facebook korisnički računi i oznake na Google kartama.

Iz navedenog se može puno saznati o MTU-u, za što je bio korišten, kao i o njegovom korisniku. Bitno je napomenuti kako je većina ovakvih informacija dostupna samo ako nisu izbrisane. Neke binarne datoteke kao što su nazivi instaliranih aplikacija će biti zapisane u SQLite bazi podataka uređaja čak i nakon što su izbrisane, ali to je zato jer baza podataka nakon brisanja aplikacije neće izbrisati metapodatke.

Korištenjem logičke ekstrakcije se može doći do relevantnih podatka kao što su Wi-Fi mreže, korisnički računi uređaja i ostali korisnički računi, ali samo ako nisu izbrisani. To je zato zbog načina na koji logička ekstrakcija funkcionira te nije restrikcija samog alata. Prednost logičke ekstrakcije je to što nije potrebno *root* otključavanje MTU-a i moguće je doći do nekih podataka kao što korisnički računi na novijim MTU-ima koje još nije moguće otključati.

Navedeno pretpostavlja da je omogućeno USB rješavanje pogreški. U većini slučajeva to nije prepreka jer prema istraživanju iz 2014. godine koje je proveo Google-ov inženjer za sigurnost Elie Bursztein na 1500 korisnika, čak 52% korisnika ne zaključava svoje MTU-e kako je prikazano u [14]. Ako je uređaj kao dokaz nije preuzet ugašen USB otključavanje uređaja je moguće uključiti bez ikakve sigurnosne prepreke. Jedina prepreka koja može postojati kod logičke ekstrakcije je ta ako je MTU bio često brisan.



Slika 3. Usporedba dobivenih podataka datotečnom ekstrakcijom (lijevo) i logičkom ekstrakcijom (desno)

Na slici 3 se vidi usporedba logičke (desna strana slike) i datotečne ekstrakcije (lijeva strana slike) kada je uređaj bio često brisan. Logička ekstrakcija dohvaća usporedivo manje podataka i ne dohvaća podatke iz Facebook aplikacije, ali je dohvatila popise poziva i SMS poruke. Također logička ne dohvaća preuzete datoteke s interneta.

3.2.3. Ekstrakcija sigurnosne kopije i fizička ekstrakcija

Ekstrakcija podataka pomoću pokretanje sigurnosne kopije MTU-a funkcionira samo na Android uređajima i to na verzijama iznad 4.0. Razlog tome je što *adb* (engl. *Android Debug Bridge*) naredbe kojima se pokreće izrada sigurnosne kopije je moguće izvršiti samo u navedenim verzijama Android OS-a. Postupak će pokrenuti upit na ekranu MTU-a gdje će OS postaviti pitanje želi li korisnik izvršiti izradu sigurnosne kopije. Ako se odgovori na ovo pitanje negativno, ekstrakcija neće uspjeti jer se ona vrši tijekom postupka izrade kopije.

Sigurnosna kopija uređaja se sprema na osobno računalo pomoću USB kabela te se ovim postupkom uređaj zavara kako je spojen na legitimno računalo i time započinje sve podatke slati alatu NowSecure Forensics CE. Android sigurnosna verzija radi kopiju svih

aplikacija instaliranih na uređaj, kao i svih onih datoteka koje su vidljive u datotečnoj strukturi uređaja. Time izbrisane datoteke i aplikacije neće biti prikupljene jer Android neće kopirati ono što smatra praznim prostorom u memoriji uređaja. Iako je navedeno kako ova vrsta ekstrakcije radi na verzijama Android OS-a iznad 4.0, autor nije uspio pokrenuti ovu vrstu ekstrakcije na MTU-u s Android OS-om 4.0.4 i alat je iznio poruku kako ekstrakcija nije uspjela. Ovu ekstrakciju je moguće izvršiti nad već izrađenom sigurnosnom kopijom MTU-a, koju je potrebno naknadno prije toga unijeti u program koristeći opciju za to.

Ovakve situacije u kojima forenzički alat nije u mogućnosti izvršiti ekstrakciju su puno češće nego u slučaju autora jer osobe koje su bile vlasnici MTU-a na kojima je potrebno izvršiti forenzičku analizu koriste sve dostupne metode kako bi otežali cijeli postupak. Nakon što sve ostale metode ne uspiju preostaje fizička ekstrakcija koja je jedna od dviju najopsežnijih ekstrakcija po količini podataka, druga bi bila JTAG.

Fizička ekstrakcija kopira bit po bit sa memorije uređaja i kao takva zahtijeva *root* otključani uređaj. Bit po bit kopiranje kopira i onaj prostor memorije koji bi datotečna ekstrakcija smatrala praznim i time se dolazi do većine izbrisanih podataka. Fizička ekstrakcija u alatu NowSecure Forensics CE nije moguća i zahtijeva punu verziju programa i MTU mora biti *root* otključan.

Cijeli postupak fizičke ekstrakcije je veoma dugotrajan i zahtijeva najviše vremena od svih mogućih vrsta ekstrakcije podataka. Zauzvrat tome ovaj način ekstrakcije dohvaća najviše podataka iz MTU-a i u stanju je dohvatiti izbrisane podatke.

3.3. Napredne karakteristike

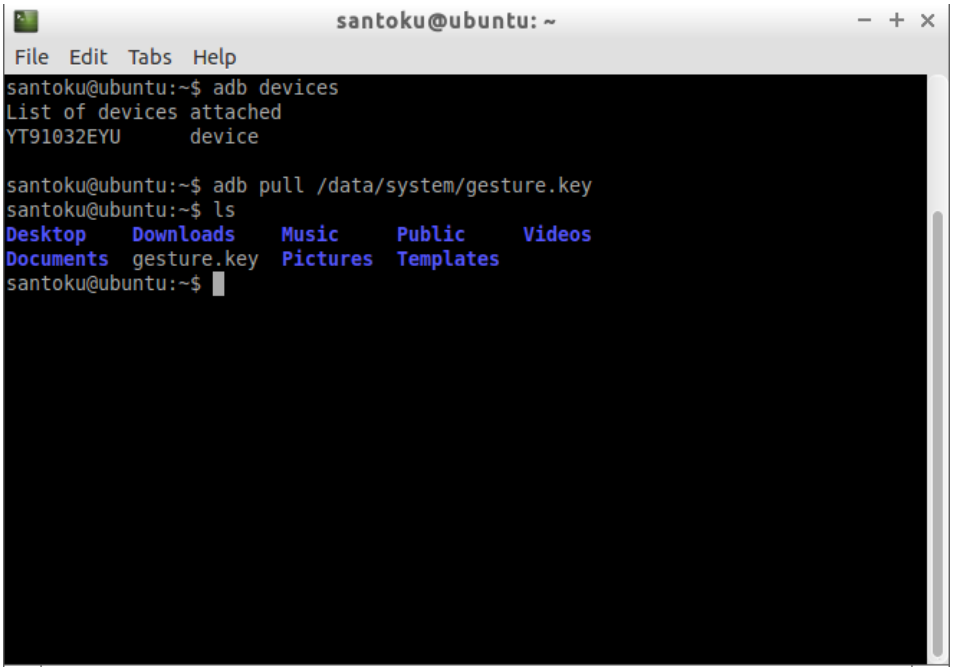
NowSecure Forensics CE nudi mnoge napredne funkcije koje omogućuju lakšu preglednost prikupljenih podataka, organiziranje prikupljenih podatka po datumu, vrsti i/ili ključnoj riječi. Druge funkcije kao što su *Gesture Key Decode* i *Unlock Screen* omogućuju otključavanje Android MTU-a ako je uređaj zaključan lozinkom ili uzorkom.

Još jedna od naprednih karakteristika je mogućnost unosa i izvoza projekata, odnosno skeniranih podataka s MTU-a. Kod svakog novog skeniranja korisnik može odabrati naziv projekta, vremensku zonu te broj trenutnog dokaza. Svaka od ovih karakteristika će biti objašnjena ukratko.

3.3.1. Otključavanje zaslona MTU-a

Gesture Key Unlock omogućuje otkrivanje uzorka kojim je MTU zaključan i time omogućava otključavanje uređaja. Postoje dva načina na koje se MTU može otključati i svaki zahtjeva *root* otključani uređaj. Prvi način zahtijeva da se pomoću adb naredbi preuzme *gesture.key* datoteka s MTU-a. Ta datoteka sadrži sha1 *hash*[3] od 20 bajta koji će se onda početi dekriptirati. Drugi način je ručni unos sha1 *hash*-a od 20 bajta u za to predviđeno polje za unos nakon čega počinje dekripcija.

Kako bi se došlo do datoteke *gesture.key* na *root* otključanom MTU-u koristi se Santoku konzola i niz od par naredbi. Prva naredba *adb devices* će prikazati popis svih MTU-a koji su trenutno spojeni preko USB kabela. U prvom retku će odmah biti vidljiv serijski broj uređaja. Idućom adb naredbom *adb pull /data/system/gesture.key* će datoteka *gesture.key* biti kopirana i spremljena u početnoj mapi. Zadnjom Linux naredbom *ls* će se ispisati sadržaj početne mape i time se može potvrditi da je datoteka preuzeta. Cijeli postupak je vidljiv na slici 4.



Slika 4. Prikaz niza naredbi u Linux terminalu za kopiranje datoteke s uzorkom sa MTU-a na računalo

[3] *Hash* je niz nasumično generiranih znakova fiksne veličine koji se dobije nakon provođenja funkcije enkripcije jednog ili više podataka

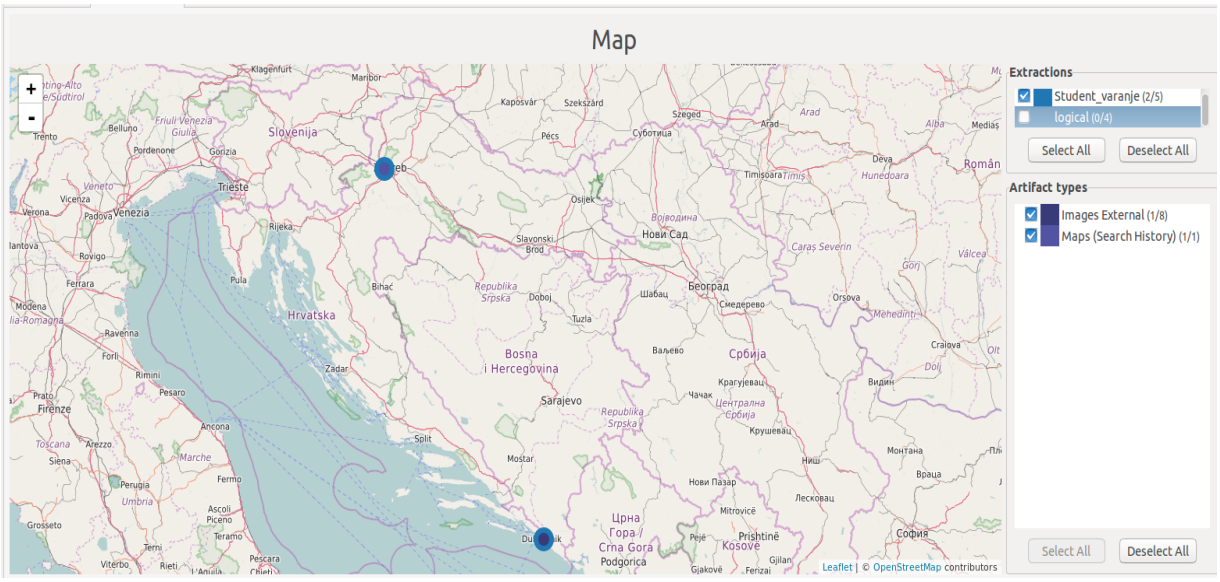
Nakon preuzimanja datoteke *gesture.key* sa MTU-a na računalo moguće je istu odabrati za dekripciju kako bi se došlo do uzorka kojim će se otključati MTU. Za nekoliko sekundi uzorak će biti prikazan na monitoru u obliku znamenki u brojčanoj matrici. Navedeni postupka vrijedi samo za Android MTU-e.

U slučaju u kojem uređaj nije *root* otključan, moguće je pomoću JTAG metode doći do slike uređaja i onda iz te slike uređaja izvući *gesture.key* datoteku. Ovo je nužno samo u slučaju u kojem uređaj nije *root* otključan.

Još jedna od naprednijih funkcija je *Unlock Screen* koja ima mogućnost otključavanja zaslona Android MTU-a koji je zaključan nizom znamenaka, za razliku od zaslona koji je zaključan uzorkom. Cijeli postupak se svodi na instaliranje aplikacije koja će otključati zaslon MTU-a. Za ovaj postupak uređaj mora biti *root* otključan jer se u protivnom aplikacije neće uspješno instalirati. Nakon što se aplikacija instalira na ekranu MTU-a pojavi se upit za otključavanje zaslona. Nakon što korisnik potvrdi otključavanje pritiskom na tipku zaslon se otključa. U slučaju u kojemu uređaj nije moguće *root* otključati jer nije uključen USB rješavanje pogreški ova metoda nije u mogućnosti otključati zaslon i potrebno je koristiti JTAG.

3.3.2. Prikaz podataka na karti i vremenskoj crti

Jedna od naprednijih karakteristika ovog alata je funkcija lokacije koja automatski preuzete datoteke s MTU-a koje imaju GPS (engl. *Global Positioning System*) oznaku, je u stanju prikazati na karti. Ovo je korisno ako osoba koja je koristila MTU nije isključila GPS lociranje na fotografijama jer se u tom slučaju sve fotografije spremaju s GPS informacijama na uređaj. Osim prikaza na karti, biti će i prikazane mape gdje je svaka datoteka snimljena na MTU-u te odabirom na svaku datoteku moguće ju je pregledati.

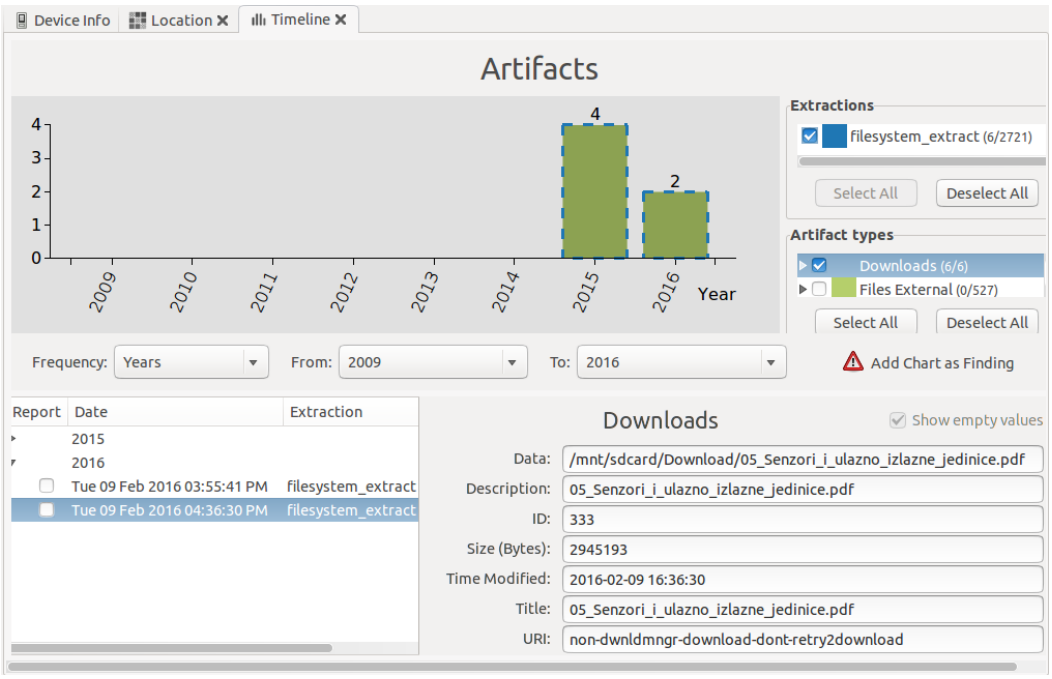


Slika 5. Prikaz dviju GPS lokacija koje su očitane iz fotografija

Na slici 5 su prikazane s plavim krugovima takve informacije za dvije fotografije koje su došle tvornički s uređajem. Jedna lokacija je na području Grada Zagreba dok je druga na području Dubrovnika. Iako su fotografije tvorničke, sa sobom i dalje nose GPS koordinate pa ih je moguće prikazati na karti.

Osim što je prikupljene podatke moguće prikazati prostorno, sve podatke je moguće i prikazivati vremenski na vremenskoj crti. Vremenska crta će prikazati sve podatke u rasponu od najstarijeg podatka prikupljenog s uređaja, pa sve do najnovijih podataka koji su nastali netom prije forenzičke analize. Podatke na vremenskoj crti je moguće filtrirati po tipu podatka ili po vremenskom razdoblju. Time je moguće doći do određenog tipa podatka u određenom vremenskom razdoblju kao što je SMS poruka poslana na specifičan datum. Odabirom podatka na vremenskoj crti se otkrivaju njegovi detalji, kao što vidi na slici 6 gdje je odbrana PDF datoteka koja je preuzeta s interneta.

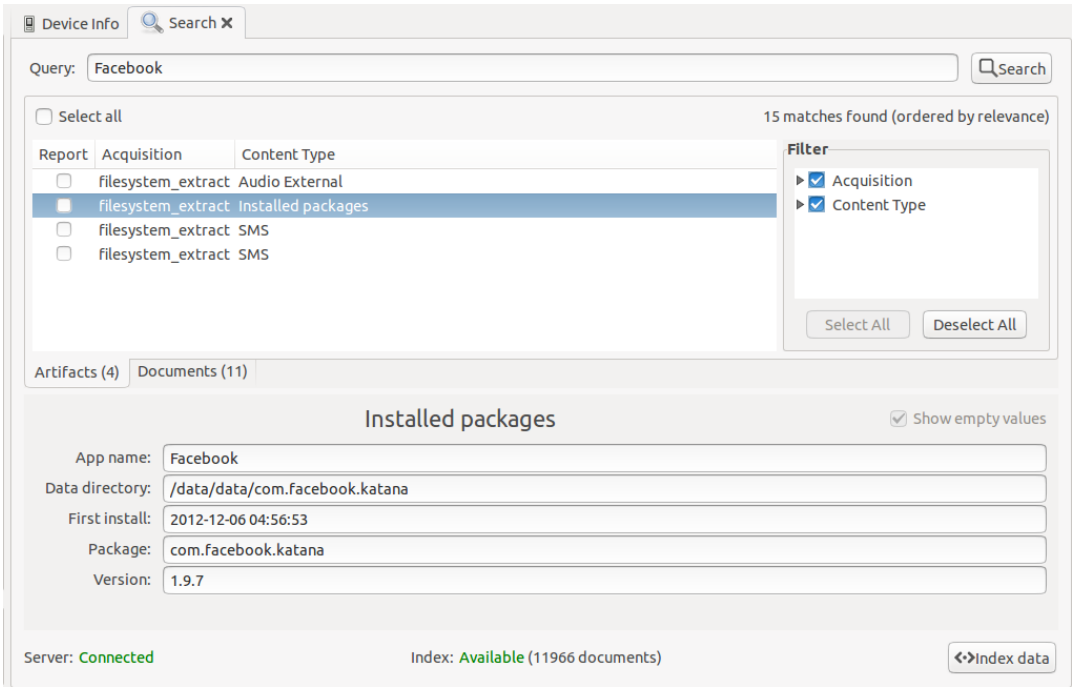
S obzirom na to kako je identifikacijski broj odabrane datoteke 333, a prije nje na vremenskoj crti nema drugih preuzimanja može se zaključiti kako je osoba koje je koristila MTU obrisala svu povijest preuzimanja skupa s dotičnim datotekama, što se može vidjeti na istoj slici. Ovakvi zaključci se mogu puno lakše i brže iznijeti sa grafičkim prikazom kao što je vremenska crta nego što bi to bio slučaj s tekstualnim sučeljem.



Slika 6. Prikaz vremenske crte i njenog grafičkog sučelja

3.3.3. Funkcija pretraživanja

Funkcija pretraživanja je napredna karakteristika koja omogućuje pretraživanje prihvaćenih podataka s MTU-a. Pretraživanje se vrši pomoću ključne riječi i obuhvaća i zaglavlja podataka, odnosno metapodatke, kao i tijelo podataka, odnosno sadržaj podatka. Tako je primjerice pretraživanje s ključnom riječi „Facebook“ kao rezultate između ostalog iznijelo dodatne aplikacijske pakete za „Facebook“ aplikaciju, kao i dvije SMS poruke koje u svojem sadržaju imaju ključnu riječ što se može vidjeti na slici 7. Dobivene su i informacije kada je pojedina aplikacija prvi put instalirana na MTU.



Slika 7. Prikaz rezultata dobivenih pretragom ključne riječi

Pretraživanje ključnih riječi isto tako omogućuje odabir koju vrstu sadržaja korisnik želi pretraživati pa se tako može ograničiti samo na SMS poruke, popis poziva, popis kontakata u imeniku, audio i/ili video datoteke, povijest Internet preglednika itd. Na ovaj način moguće je brzo pretraživanje kompletnog preuzetog sadržaja MTU-a kako bi se došlo do relevantnih podataka koji zanimaju korisnika.

3.4. Zakonska regulativa – zaštita osobnih podataka

U Republici Hrvatskoj u članku 2. Zakonu o zaštiti osobnih podataka (NN 103/03, 118/06, 41/08, 130/11, 106/12) definirani su izrazi osobni podatak, obrada osobnih podataka i zbirka osobnih podataka.

Osobni podataka je svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati; osoba koja se može identificirati je osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na osnovi identifikacijskog broja ili jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet, [15].

Obrada osobnih podatka je svaka radnja ili skup radnji izvršenih na osobnim podacima, bilo automatskim sredstvima ili ne, kao što je prikupljanje, snimanje, organiziranje, spremanje, prilagodba ili izmjena, povlačenje, uvid, korištenje, otkrivanje

putem prijenosa, objavljivanje ili na drugi način učinjenih dostupnim, svrstavanje ili kombiniranje, blokiranje, brisanje ili uništavanje, te provedba logičkih, matematičkih i drugih operacija s tim podacima, [15].

Zbirka osobnih podatka je svaki strukturirani skup osobnih podatka koji je dostupan prema posebnih kriterijima, bilo centraliziranim, decentraliziranim, ili raspršenim na funkcionalnom ili zemljopisnom temelju i bez obzira na to da li je sadržan u računalnim bazama osobnih podatka ili se vodi primjenom drugih tehničkih pomagala i ručno, [14].

Prema navedenom se može zaključiti kako će svaki pristup podacima na MTU biti pristup osobnim podacima korisnika, odnosno vlasnika tog MTU-a i time će spadati pod domenu spomenutog zakona. Forenzička analiza takvog MTU-a, primjerice s alatom NowSecure Foresics CE, će spadati pod obradu osobnih podataka i strogo će biti podčinjena ovom zakonu i pravilima koje taj zakon propisuje.

Nadalje, u članku 6. Zakona o zaštiti osobnih podataka regulira se obrada osobnih podataka; Osobni podaci mogu se prikupljati u svrhu s kojom je ispitanik upoznat, koja je izričito navedena i u skladu s zakonom i mogu se dalje obrađivati samo u svrhu u koju su prikupljeni, odnosno u svrhu koja je podudarana sa svrhom prikupljanja. Daljnja obrada osobnih podatka u povijesne, statističke ili znanstvene svrhe neće se smatrati ne nepodudarnom, pod uvjetom da se poduzmu odgovarajuće zaštitne mjere, [15].

Prema tome digitalna forenzička analiza MTU-a, kao što bi bilo korištenje alata NowSecure Forensics CE, bi bila obrada osobnih podatka i ako se ne provodi uz privolu osobe kojoj pripadaju osobni podaci bila bi izvan zakona. U članku 8. su definirani slučajevi kada je dopuštena obrada osobnih podatka i ako se provodi u okviru uspostave, ostvarenja ili zaštite potraživanja propisanih zakonom tada je dopuštena.

U tom kontekstu, digitalna forenzička analiza MTU-a je dozvoljena samo ako se provodi za druge slučajeve koji su propisani zakonom, kao što je službena policijska istraga, ili ako se provodi uz privolu vlasnika, odnosno korisnika MTU-a. Kako bi se zadovoljili ti uvjeti za potrebe ovoga rada autor ovog rada je koristio isključivo svoj uređaj te uređaje koje je pridobio uz privolu njihovih vlasnika.

4. USPOREDBA MOGUĆNOSTI S DRUGIM ALATIMA FORENZIČKE ANALIZE

U idućem poglavlju će analizirati i usporediti mogućnosti i karakteristike alata NowSecure Forensics CE, MOBILedit Forensics, Cellebrite UFED Physical Analyzer, Cellebrite UFED Logical Analyzer i SecureView Mobile Forensics. Analizirati će se nedostaci i prednosti pojedinih alata kao i njihove dostupnosti.

Zatim će se objasniti karakteristike svakog alata, jer unatoč tome što je svaki alat dizajniran za forenzičku analizu MTU-a svaki je prilagođen za drugačijeg korisnika, tako su MOBILedit Forensics i NowSecure Forensics više usredotočeni na organizacije i osobe koje se bave digitalnom sigurnošću dok su Cellebrite UEFD alati dizajnirani za napredne korisnike kao što su državne institucije i istraživačke institucije.

Svaki forenzički alat se razlikuje i po tome na kojim sve platformama je dostupan, neki su dizajnirani kao samostojeće platforme na Linux distribucijama dok su drugi alati napravljeni kao programi koji se mogu instalirati na Windows OS i iOS.

4.1. Usporedba mogućnosti forenzičkih alata

Iz tablice 1 vidljivo je kako je alat NowSecure Forensics CE napravljen za korisnike koji su početnici u području digitalne forenzičke analize MTU-a. To je vidljivo po nedostacima naprednijih mogućnosti, uz zadržavanje osnovnih mogućnosti koje su potrebne za izvođenje forenzičke analize.

Tablica 1.Usporedba mogućnosti različitih alata za forenzičku analizu MTU-a

KARAKTERISTIKE	FORENZIČKI ALATI				
	NowSecure Forensics CE	**MOBILedit Forensics**	**Cellebrite UFED Logical Analyzer**	**Cellebrite UFED Physical Analyzer**	**SecureView Mobile Forensics**
Mogućnost root otključavanja	DA	DA	DA	DA	DA
Zaobilaženje zaključanog zaslona	DA	DA	DA	DA	DA
Prikupljanje izbrisanog sadržaja	NE	DA	DA	DA	DA
Pretraživanje pomoću ključne riječi	DA	DA	DA	DA	DA
Android logička ekstrakcija	DA	DA	DA	DA	DA
Android datotečna ekstrakcija	DA	DA	DA	DA	DA
Android fizička ekstrakcija	NE	DA	NE	DA	DA
iOS logička ekstrakcija	NE	DA	DA	DA	DA
iOS fizička ekstrakcija	NE	NE	NE	DA	DA
Izrada izvještaja	NE	DA	DA	DA	DA
Kloniranje SIM kartice	NE	DA	DA	DA	NE
Analiziranje MTU-a koristeći bežične tehnologije	NE	DA(Wi-Fi, Bluetooth, IrDA)	NE	NE	NE
Podržava druge OS-e osim Andorida i iOS-a	NE	DA (Symbian, Windows Phone)	DA	DA	NE
Detektira malware	NE	NE	DA	DA	NE

Izvor: [16], [17], [18], [19]

Cellebrite UFED ima dvije inačice, jednu manje naprednu, sposobnu samo za logičke ekstrakcije i drugu sa svim mogućnostima i u stanju izvršiti fizičke ekstrakcije podataka. Cellebrite UFED forenzički alati su jedini od nabrojanih koji imaju mogućnost detekcije nepoćudnih programa (engl. *malware*). Razlog tome je što je Cellebrite UFED namijenjen državnim i profesionalnim institucijama u čijim okruženjima postoji mogućnost nalaženja *malware* programa na MTU-ima, [16], [17].

Od svih nabrojanih samo MOBILedit Forensics forenzički alat ima mogućnost spajanja s MTU-ima pomoću bežičnih tehnologija Wi-Fi, Bluetooth i IrDA. Također je u mogućnosti analizirati stariju generaciju MTU-a, takozvane Symbian uređaje. Kako je tehnologija infracrvenog prijenosa veoma zastarjela može se zaključiti kako MOBILedit Forensics pruža jednaku mogućnost analize starijih MTU-a kako i MTU-a najnovije generacije, [18].

SecureView Mobile Forensics ima mogućnost analize samo Android i iOS MTU-a, a nema detekciju *malware*-a i ne može klonirati SIM kartice. SecureView Mobile Forensics je alat koji je više fokusiran na analizu i prikaz preuzetih podataka. Tako nudi mogućnost vremenske crte, grafova i listi i ima mogućnost pronalaženja fotografija na MTU-u na temelju slične fotografije koju korisnik odabere. Također je u stanju automatski izraditi grafove internet aktivnosti korisnika i aktivnosti korištenja MTU-a, [19].

Na prvi pogled svi spomenuti alati su napredniji od NowSecure Forensics CE alata, ali ti alati nisu dostupni bez naplate i time su daleko nedostupniji osobi koja se želi upoznati s forenzičkom analizom MTU-a. Također alati kao Cellebrite UFED su dostupni odabranim institucijama i nije ih moguće nabaviti u pojedinim zemljama.

4.2. Karakteristike odabranih forenzičkih alata

MOBILedit Forensics je alat za forenzičku analizu MTU-a koji ima mogućnost izvršiti forenzičku analizu preko USB kabela, Wi-Fi, Bluetooth i IrDA (engl. *Infrared Data Association*). Koristi se kao samostojeći alat koji se instalira na Windows računalo i odmah je dostupan za korištenje. S mogućnošću kloniranja SIM kartice alat može bez poteškoća zaobilaziti SIM zaključane MTU-e. Alat ima mogućnost ekstrakcije podataka o MTU-u s iOS OS iz iTunes sigurnosne kopije za razliku od NowSecure Forensics CE koji tu mogućnost ima samo za Android MTU-e.

MOBILedit Forensics podržava mnoštvo MTU-a, od starijih tipova telefona sve do novijih tipova pametnih telefona. Na svim vrstama MTU-a je moguća fizička ekstrakcija podataka te alat ima mogućnost izrade izvještaja u različitim formatima koji se onda mogu uvesti u druge forenzičke alate. Fizička analiza svih vrsta uređaja i mogućnost kloniranja

SIM kartica stavljaju ovaj forenzički alat ispred NowSecure Forenscis CE. Glavni nedostatak je to što nije dostupan kao freeware inačica i time je daleko izvan dosega osobama koje tek ulaze u područje digitalne forenzičke analize, [18].

SecureView Mobile Forensics je forenzički alat koji se može koristiti na Windows platformi kao samostojeći alat, kao mobilna verzija programa ili u paru s uređajem za forenzičku analizu NUC od iste tvrtke. Ima mogućnost analize iOS i Android uređaja, ali ne podržava starije uređaje koji ne spadaju u kategoriju pametnih telefona. Fizičkom ili logičkom ekstrakcijom podataka s uređaja prikuplja podatke kao što su SMS/MMS poruke, popis poziva, kontakata i popis događaja u kalendaru telefona i podatke izbrisane od strane korisnika MTU-a. Sa prikazom podatka na vremenskoj crti, kao i grafovima prikupljenih podataka i pretragom fotografija konkurira mogućnostima NowSecure Forensics CE, ali nema mogućnost *root* otključavanja MTU-a i otključavanja zaslona bez dodatnog uređaja te je potrebno izvršiti JTAG ekstrakciju kako bi se otključao zaslon MTU-a, [19].

Cellebrite UFED Logical Analyser je alat za forenzičku analizu MTU-a koji je osmišljen kao manje sposoban alat od Cellebrite UFED Physical Analyser-a. U stanju je izvršiti samo logičku analizu uređaja, ali zato ima niz dodatnih mogućnosti. Jedna od dodatnih mogućnosti uključuje prijevod GPS koordinata u adrese kako bi se lakše povezali podaci iz MTU-a s lokacijama. Uz popis samih instaliranih aplikacija alat iz samih aplikacija prikuplja podatke te je u stanju pretražiti uređaj kako bi otkrio zlonamjeran softver. Prikazom podataka na karti i vremenske crte , opcijom pretraživanja sadržaja te ostalim dodatnim mogućnostima nadmašuje NowSecure Forensics CE. Najveći nedostatak je što nema mogućnosti druge vrste ekstrakcije osim logičke, [16].

Cellebrite UFED Physical Analyser je forenzički alat od tvrtke Cellebrite koji nudi više mogućnosti od UFED Logical Analyser-a te je daleko više sposobniji nego NowSecure Forensics CE. Uz fizičku analizu MTU-a ima i mogućnost ekstrakcije podataka iz sigurnosnih kopija kao što je iCloud te ekstrakciju izbrisanih podataka iz nedodjeljenog prostora sa memorije MTU-a. Uz navedeno UFED Physical Analsyer može prikupiti izbrisane slike s MTU-a, i to u slučaju u kojemu su samo fragmenti izvornih podataka ostali na MTU-u. Alat ima mogućnost dodavanja novih modula pisanih u Python programkom jeziku kao i dekodiranje raznih vrsta aplikacija. Uz sve to zadržava sve mogućnosti Logical Analyser-a. Uz navedeno UFED Physical Analyser je najbolji alat po svojim mogućnostima od nabrojanih alata i daleko nadmašuje mogućnosti NowSecure Forensics CE, [17].

5. FORENZIČKA ANALIZA MOBILNIH TERMINALNIH UREĐAJA

U ovom poglavlju će biti obrađene, korak po korak, forenzičke analize MTU-a. Analize su informativnog karaktera, svi pronađeni podaci su unaprijed postavljeni na MTU. Događaji koji će biti navedeni kao svrhe analize su izričito fiktivnog karaktera i nisu povezani sa stvarnim događajima. Forenzička analiza će biti provedena nad Android uređajima Sony Xperia Miro i Sony Xperia Z1 alatom NowSecure Forensics CE.

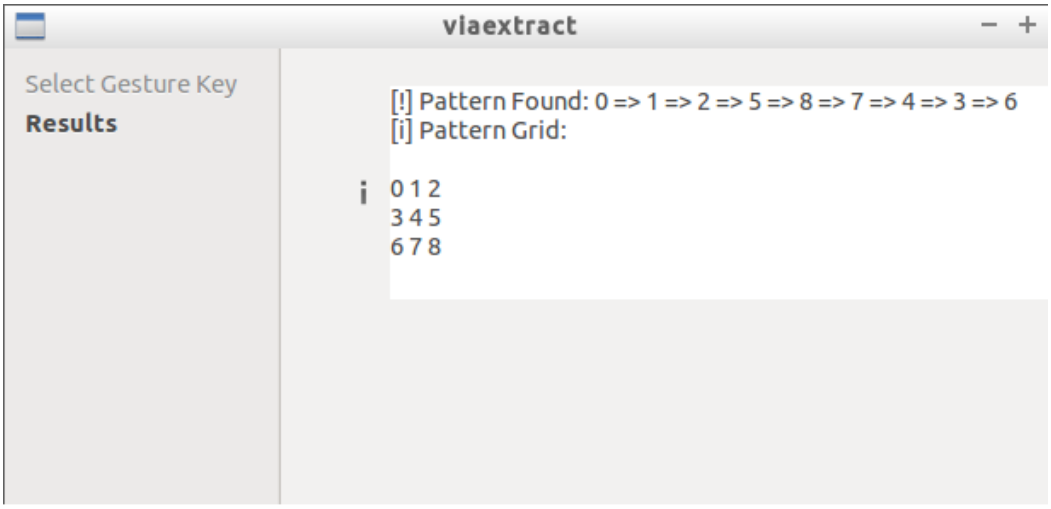
5.1. Forenzička analiza MTU-a Sony Xperia Miro

Za prvi primjer biti će analiziran MTU Sony Xperia Miro s OS Android 4.0.4. Kao razlog analize biti će postavljen fiktivni događaj u kojemu se fiktivnog studenta optužilo za varanje na ispitu. Studenta se optužuje kako je tijekom ispita koristeći svoj MTU pristupio internet stranicama na kojima se nalazio nastavni materijal i time povrijedio vlastite obveze koje su utvrđene pravilnikom o stegovnoj odgovornosti studenata, [20].

Kako bi se utvrdila točnost tvrdnje kako je student varao na ispitu obaviti će se forenzička analiza njegovog MTU-a i obaviti pretraga povijesti Internet preglednika kao i povijest preuzetih datoteka. MTU je zaključan s uzorkom, ali je utvrđeno kako je USB rješavanje pogreški uključeno što će omogućiti otključavanje i analizu sadržaja.

Prvi korak će biti priključivanje MTU-a s USB kabelom na računalo na kojemu se nalazi instaliran NowSecure Forensics CE. Zatim će se pokrenuti program za forenzičku analizu gdje će se potvrditi model MTU-a i na početnom zaslonu programa će se prikazati osnovne informacije na temelju kojih se donosi odluka o vrsti ekstrakcije koju je moguće provesti.

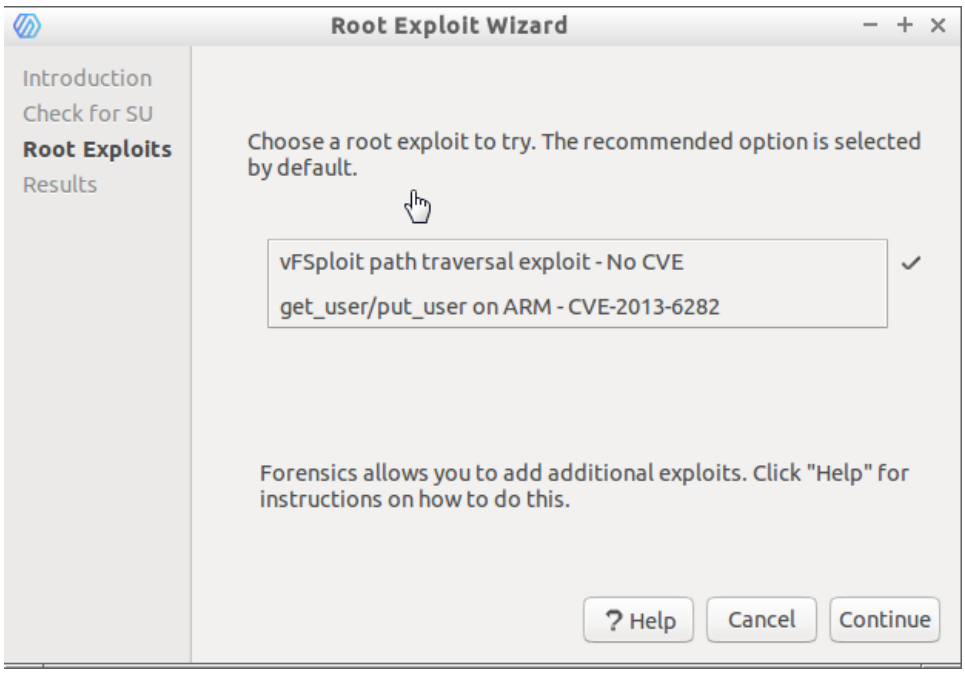
Kako bi se obavila datotečna ekstrakcija biti će potrebno *root* otključati uređaj za što će biti potrebno otključati zaslon uređaja. Naredbom *adb pull data/system/gesture.key* će se datoteka koja sadrži *hash* za dešifriranje prebaciti na računalo. Koristeći Gesture Key Decoder nad prenesenom datotekom uzorak će se dekriptirati u manje od jedne sekunde. Na slici 8 se vidi pronađeni uzorak. Brojevi u matrici prikazuju određeno polje uzorka dok je iznad njih naveden redoslijed kojim se povezuju.



Slika 8. Rezultat dekripcije datoteke s uzorkom

Nakon što se otključa zaslon MTU-a u njegovim postavkama se ukloni zaključavanje zaslona i uključi se opcija koja sprječava gašenje zaslona dok je uređaj na punjenju. Ovo će omogućiti lakše rukovanje uređajem i spriječiti njegovo zaključavanje. Kako bi se provela datotečna ekstrakcija uređaj će biti potrebno *root* otključati. Odabirom te opcije u sučelju će se otvoriti skočni prozor u kojem će se odabrati metoda *root* otključavanja. U ovom slučaju je odabrana prva ponuđena metoda, *vFSploit path traversal exploit – No CVE* kao što se vidi na slici 9.

Ako nije moguće *root* otključati MTU ovim postupkom izabere se metoda koja je iduća na popisu. Ovisno o OS i proizvođaču MTU-a biti će ponuđene različite metode *root* otključavanja uređaja. U slučaju u kojemu nijedna metoda nije uspješna potrebno je napraviti JTAG ili *chip-off* ekstrakciju što nije slučaj u ovom primjeru.



Slika 9. Mogućnost odabira između više sigurnosnih propusta za *root* otključavanje MTU-a

Nakon što je uređaj *root* otključan, datotečna ekstrakcija može početi. Pri pokretanju se postavljaju ime i broj dokaza te vremenska zona u kojoj se vrši analiza. Vremenska zona služi za bolje organiziranje vremenske crte i metapodataka koji nose oznaku vremena. U ovom primjeru ime dokaza je „Student_varanje“ dok je broj dokaza „1“. Ovakva funkcija imenovanja olakšava organiziranje svih dokaza kada se provodi više ekstrakcija nad jednim MTU-em. Prosječno vrijeme trajanje u ovom slučaju je iznosilo oko dvadesetak minuta, za MTU na kojem se nalazilo oko 6 GB podataka.

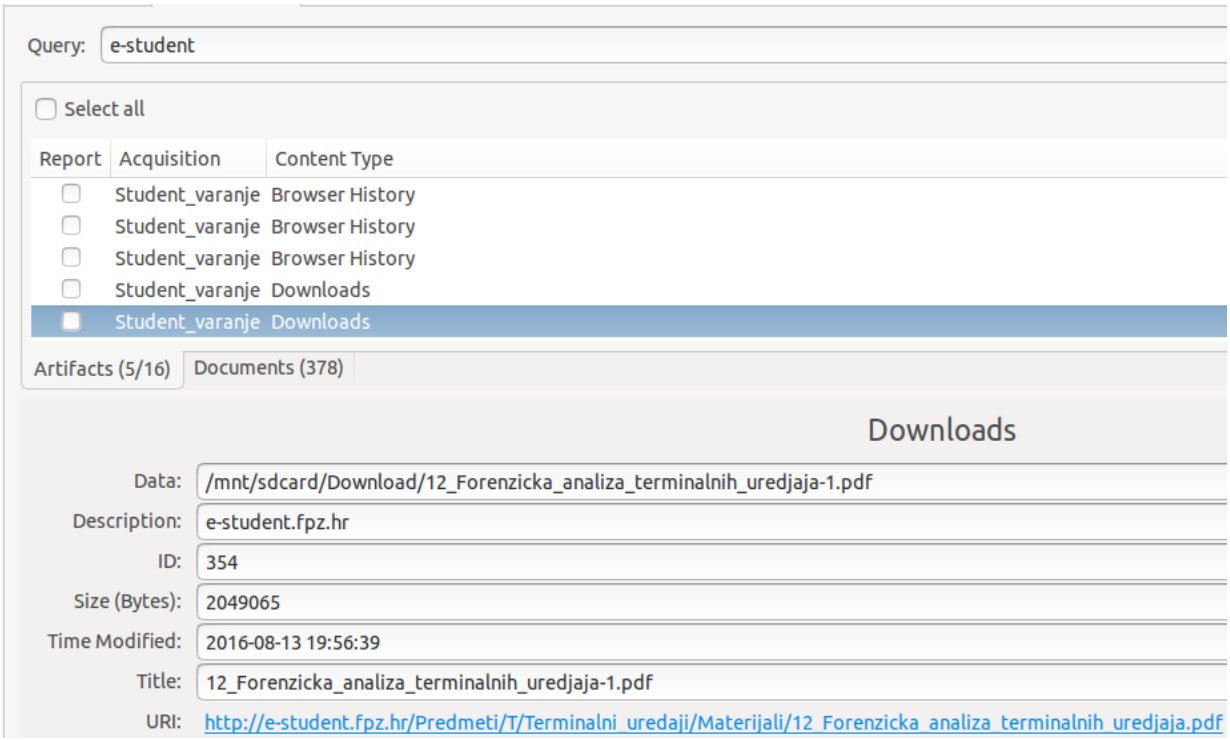
Ovisno o modelu MTU-a i količini podataka vrijeme ekstrakcije može jako varirati, čak i do nekoliko sati kod MTU-a velikog kapaciteta trajne memorije. Moguće je i provesti više vrsta ekstrakcije i rezultati svake će biti poredani jedni ispod drugih u izborniku na lijevoj strani. Na slici 10 se vide dobiveni podaci nakon datotečne ekstrakcije.

File	File Path	Size
org.mozilla.firefox-1.apk	data/app/org.mozilla.firefox-1.apk	37.7 MB
libchromeview.so	system/lib/libchromeview.so	23.9 MB
framework-res.apk	system/framework/framework-res.apk	17.0 MB
com.android.vending-1.apk	data/app/com.android.vending-1.apk	14.7 MB
com.mireo.dontpanic.vipnavigacija.apk	system/etc/customization/applications/com.mireo.dontp...	12.2 MB
com.foxit.mobile.pdf.lite-1.apk	data/app/com.foxit.mobile.pdf.lite-1.apk	11.8 MB
full_model.bin	system/vendor/pittpatt/models/recognition/face.face.y0-...	11.4 MB
framework.odex	system/framework/framework.odex	11.2 MB
textinput-chn.apk	system/app/textinput-chn.apk	10.3 MB
OfficeSuitePro_SE_Viewer.apk	system/etc/product/applications/OfficeSuitePro_SE_View...	9.2 MB
Settings.apk	system/app/Settings.apk	9.1 MB
data@app@com.estrongs.android.pop-1.apk@classes.dex	data/dalvik-cache/data@app@com.estrongs.android.pop...	8.6 MB

Slika 10. Dio popisa binarnih podataka nakon datotečne ekstrakcije MTU-a Sony Xperia Miro

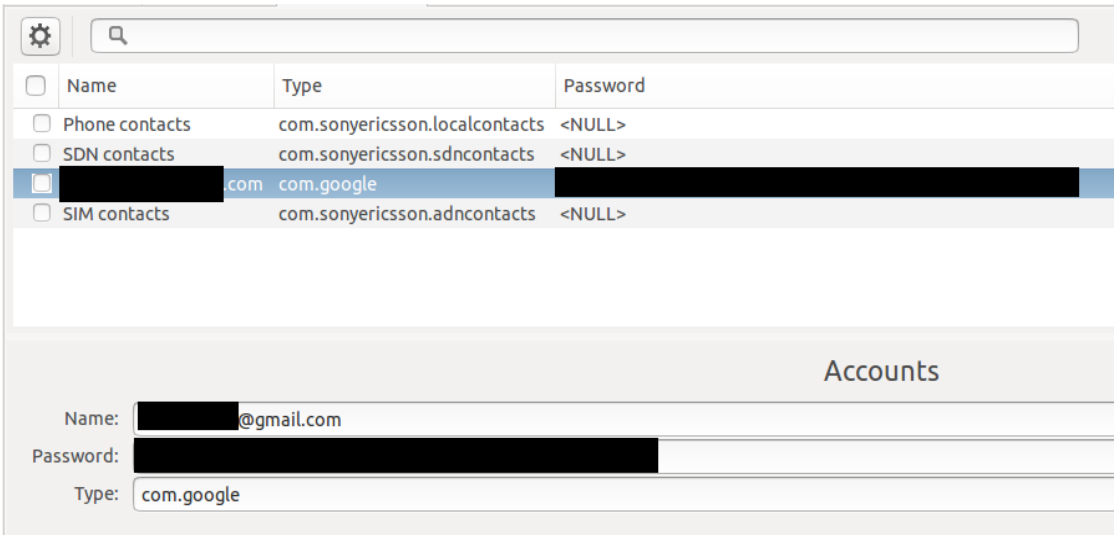
Alat pokazuje ukupan broj od 3431 binarnih podataka dohvaćenih s MTU-a. Svi ti podaci su smješteni u odgovarajuće kategorije, ali njihov pojedinačni pregled bi oduzeo puno vremena. Zbog toga će se koristiti mogućnost pretraživanja ključne riječi. Kao ključna riječ će se upisati „e-student“ u polje za pretraživanje jer je to ime web stranice s nastavnim materijalima. Nakon toga će se pregledati dobiveni rezultati za preuzete datoteke s interneta kao i povijest Internet pretraživanja.

Na slici 11 se može vidjeti kako su sa web stranice e-studenta preuzete PDF datoteke na MTU. Pri odabiru jednog od ponuđenih rezultata na dnu ekrana će se prikazati više informacija. Prvo polje prikazuje put do mape na MTU-u na kojemu je taj podatak spremljen. Drugo polje opisuje podatak dok treće polje prikazuje njegov identifikacijski broj. Četvrto i peto polje prikazuju veličinu podatka u bajtovima i datum i vrijeme preuzimanja podatka. Zadnja dva polja prikazuju ime podatka kako se prikazuje na MTU-u i adresu web stranice s koje je preuzet podatak.



Slika 11. Prikaz preuzetih datoteka i povijesti internet pretraživanja koje odgovaraju ključnoj riječi "e-student"

Ako se vrijeme preuzimanja poklapa s vremenom polaganja ispita to dokazuje varanje na ispitu. Kako bi se dodatno povezao identitet studenta s MTU-em koji je imao tijekom ispita, pod korisničkim računima se pretražuje e-mail koji pripada studentu koji dokazuje kako je student koristio MTU. Korisnički računi koji su korišteni se mogu vidjeti na slici 12, zbog privatnosti autora dio e-mail adrese je cenzuriran.



Slika 12. Korisnički računi koji su bili korišteni na MTU-u

Osim imena korisničkog računa prikazani su i njegova lozinka, ali u enkriptiranom obliku. Prikazuje se i vrsta korisničkog računa, koji može biti SIM kontakt, telefonski kontakt ili u ovom slučaju, e-mail kontakt vlasnika MTU-a. Ako je ovime pronađeno dovoljno dokaza digitalni forenzički proces se smatra završenim i USB veza između MTU-a i računala se može prekinuti.

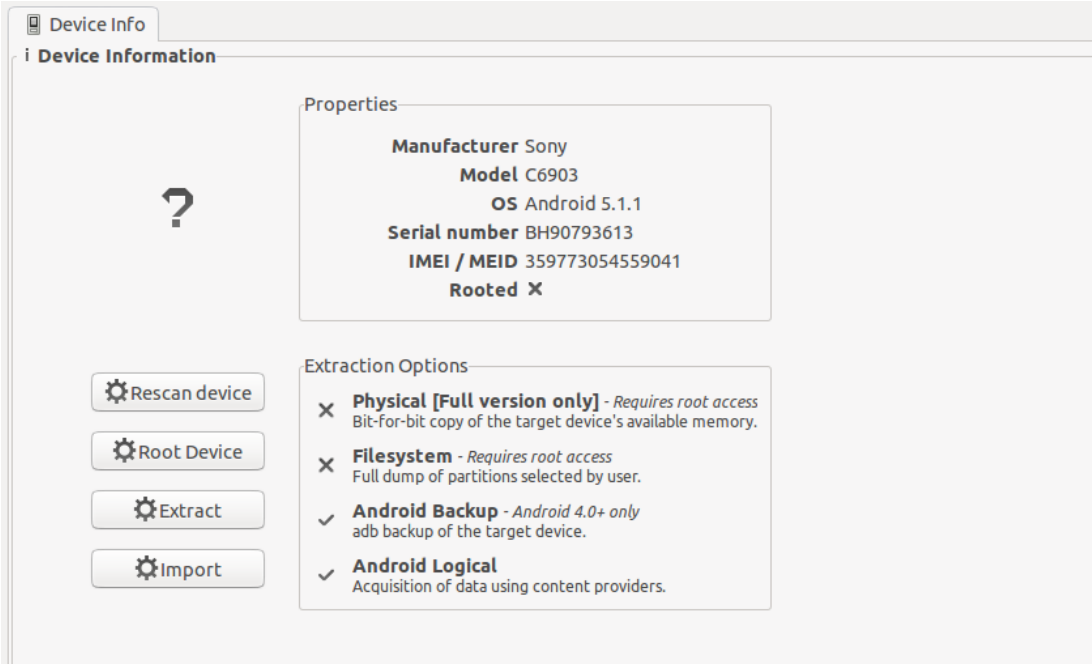
5.2. Forenzička analiza MTU-a Sony Xperia Z1

Drugi primjer uključuje analizu MTU-a Sony Xperia Z1. Ovaj uređaj dolazi s Android 5.1.1 OS-om koji je moderniji od OS-a MTU-a iz prijašnjeg primjera i zbog toga ga NowSecure Forensics CE nije u stanju *root* otključati. Time je u mogućnosti nad njim izvršiti samo logičku ekstrakciju i ekstrakciju sigurnosne kopije podataka.

Kao hipotetski primjer analize biti će postavljeni sljedeći događaji; unutar zaštićenog prostora tvrtke koja se bavi informatičkim poslovanjem ostavljen je sumnjiv MTU. MTU je imao uključen Wi-Fi i Bluetooth bežičnu komunikaciju, ali nije bio spojen niti na jednu Wi-Fi mrežu unutar tvrtke. Sumnja se kako je MTU korišten od nepoznate strane kako bi skupljao podatke o mreži tvrtke u čijim se prostorima nalazio.

Kako bi se dokazale predložene sumnje izvršiti će se logička ekstrakcija podataka uređaja. Na MTU-u će se tražiti instalirane aplikacije koje se koriste u analizi Wi-Fi i Bluetooth bežičnih mreža kao i popis svih korisničkih računa kako bi se otkrio vlasnik uređaja. MTU ima uključeno rješavanje pogreški pomoću USB kabla što uvelike olakšava pristup.

Prvi korak uključuje spajanje MTU-a s USB kabelom na računalo kao i kod prvog primjera. Nakon što se na ekranu ispišu osnovne informacije o uređaju, kao što se vidi na slici 13, odmah se uočava kako datotečna i fizička ekstrakcija nisu moguće jer zahtijevaju *root* otključavanje uređaja. Logička ekstrakcija će preuzeti manje podataka, ali će i dalje biti dovoljna za popis svih instaliranih aplikacija, kao i popis korisničkih računa na uređaju.



Slika 13. Prikaz osnovnih informacija prikupljenih s MTU-a Xperia Z1

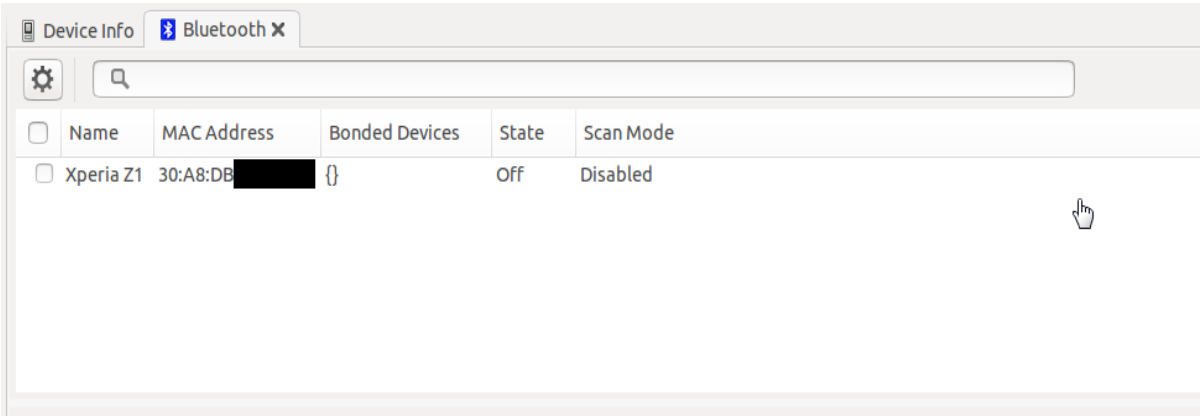
Na slici 14 se vidi dio popisa tekstualnih datoteka koje su preuzete logičkom ekstrakcijom MTU-a. Sve datoteke su zapisane u JSON (engl. *JavaScript Object Notation*) formatu, to je standard za tekstualni format za organizaciju podataka, [21].

Među ovim podacima u JSON formatu nalazi se popis svih audio datoteka, oznake i povijest Internet preglednika, popis poziva, popis kontakata, popis slika, popis instaliranih aplikacija i svi ostali podaci prikupljeni s MTU-a. Među ostalim podacima nalazi se i datoteka s informacijama o Bluetooth povezivanju. Uočljivo je kako je prikupljeno manje binarnih podataka nego kada se usporedi s datotečnom ekstrakcijom iz prijašnjeg primjera, gotovo svi podaci su u tekstualnom JSON obliku.

File	File Path	Size	Children	Binary?	Preview	File Type	MIME Type
Accounts.json	Accounts.json	323.0 B		×		Text	application/json
Audio External.json	Audio External.json	5.0 kB		×		Text	application/json
Bluetooth.json	Bluetooth.json	219.0 B		×		Text	application/json
Browser Bookmarks.json	Browser Bookmarks.json	96.1 kB		×		Text	application/json
Browser History.json	Browser History.json	96.1 kB		×		Text	application/json
Browser Searches.json	Browser Searches.json	435.0 B		×		Text	application/json
Call Log.json	Call Log.json	422.0 B		×		Text	application/json
Contacts ContactMethods.json	Contacts ContactMethods.json	335.0 B		×		Text	application/json
Contacts Extensions.json	Contacts Extensions.json	93.0 B		×		Text	application/json
Contacts Groups.json	Contacts Groups.json	562.0 B		×		Text	application/json
Contacts Organizations.json	Contacts Organizations.json	126.0 B		×		Text	application/json
Contacts Phones.json	Contacts Phones.json	331.0 B		×		Text	application/json
Contacts Settings.json	Contacts Settings.json	121.0 B		×		Text	application/json
cpro_info.json	cpro_info.json	4.5 kB		×		Text	application/json
Device Information.json	Device Information.json	791.0 B		×		Text	application/json
getprop.json	getprop.json	26.1 kB		×		Text	application/json
Image Thumbnails External.json	Image Thumbnails External.json	471.0 B		×		Text	application/json
Image Thumbnails Internal.json	Image Thumbnails Internal.json	143.0 B		×		Text	application/json
Images External.json	Images External.json	1.7 kB		×		Text	application/json
Images Internal.json	Images Internal.json	352.0 B		×		Text	application/json
Installed Apps.json	Installed Apps.json	189.4 kB		×		Text	application/json
MMS Parts.json	MMS Parts.json	192.0 B		×		Text	application/json

Slika 14. Prikaz svih tekstualnih datoteka preuzetih logičkom ekstrakcijom

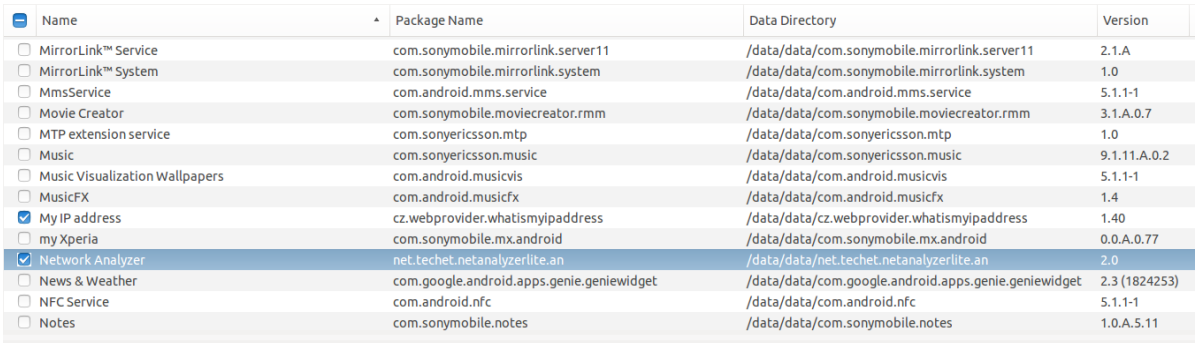
Bluetooth MAC adresu uređaja je moguće pronaći pretragom s ključnom riječi ili klikom na oznaku „Bluetooth“ u lijevom izborniku. Navedena Bluetooth MAC adresa se uspoređuje s MAC adresom uređaja koji je pokušavao uspostaviti Bluetooth veze s drugim uređajima unutar tvrtke. Navedena MAC adresa se vidi na slici 15, zadnja tri para MAC adrese su cenzurirana kako se ne bi koristila za maliciozne namjere.



Slika 15. Bluetooth MAC adresa MTU-a Sony Xperia Z1

U trećem koraku se analiziraju instalirane aplikacije na MTU-u kako bi se utvrdilo ima li među njima aplikacija koje bi se mogle koristiti za skeniranje Bluetooth i Wi-Fi mreža. Na slici 16 su s plavim kvadratićem označene aplikacije *„Network Analyzer*“ i „*My IP*

tools“ koje služe za skeniranje IP mreža. Uz ime aplikacije prikazani su i njihova mjesta u mapama na MTU-u i njihove verzije. Osim navedene dvije aplikacije pronađene su još i aplikacije „*PingTools*“, „*Fing*“ i „*WifiMap*“ za skeniranje i mapiranje Wi-Fi mreža te „*BlueScan*“ i „*Signal Sniffer*“ za skeniranje Bluetooth uređaja. Navedeno potvrđuje kako je uređaj korišten od nepoznate strane za skeniranje spektra za bežičnu komunikaciju od nepoznate strane.

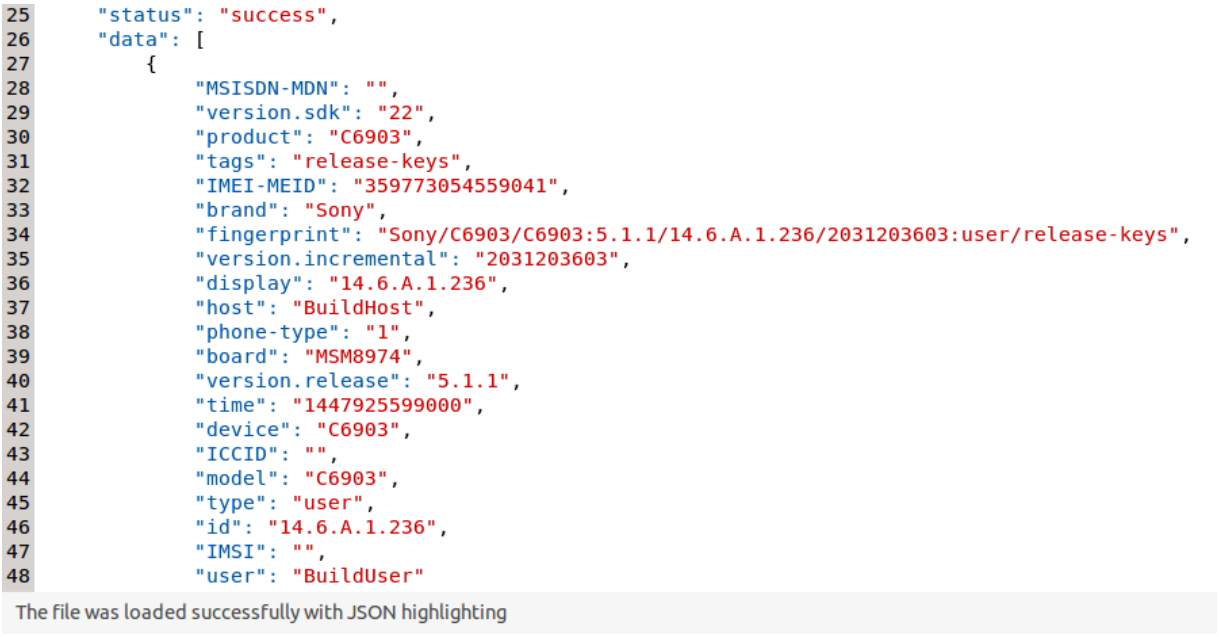


Name	Package Name	Data Directory	Version
MirrorLink™ Service	com.sonymobile.mirrorlink.server11	/data/data/com.sonymobile.mirrorlink.server11	2.1.A
MirrorLink™ System	com.sonymobile.mirrorlink.system	/data/data/com.sonymobile.mirrorlink.system	1.0
MmsService	com.android.mms.service	/data/data/com.android.mms.service	5.1.1-1
Movie Creator	com.sonymobile.moviecreator.rmm	/data/data/com.sonymobile.moviecreator.rmm	3.1.A.0.7
MTP extension service	com.sonyericsson.mtp	/data/data/com.sonyericsson.mtp	1.0
Music	com.sonyericsson.music	/data/data/com.sonyericsson.music	9.1.11.A.0.2
Music Visualization Wallpapers	com.android.musicvis	/data/data/com.android.musicvis	5.1.1-1
MusicFX	com.android.musicfx	/data/data/com.android.musicfx	1.4
My IP address	cz.webprovider.whatismyipaddress	/data/data/cz.webprovider.whatismyipaddress	1.40
my Xperia	com.sonymobile.mx.android	/data/data/com.sonymobile.mx.android	0.0.A.0.77
Network Analyzer	net.techet.netanalyzerlite.an	/data/data/net.techet.netanalyzerlite.an	2.0
News & Weather	com.google.android.apps.genie.geniewidget	/data/data/com.google.android.apps.genie.geniewidget	2.3 (1824253)
NFC Service	com.android.nfc	/data/data/com.android.nfc	5.1.1-1
Notes	com.sonymobile.notes	/data/data/com.sonymobile.notes	1.0.A.5.11

Slika 16. Instalirane aplikacije na MTU-u Xperia Z1

Preostaje još utvrditi identitet, ili barem lokaciju korisnika. Pod korisničkim računima uređaja dobavljena je e-mail adresa koja je korištena kao Google korisnički računa za „*Google Play*“ trgovinu kako bi se preuzele prije navedene aplikacije. Korisnički račun je najvjerojatnije privremen te je potrebno još identifikacijskih faktora pronaći na uređaju. To se može obaviti pretraživanjem povijesti pretraživanja.

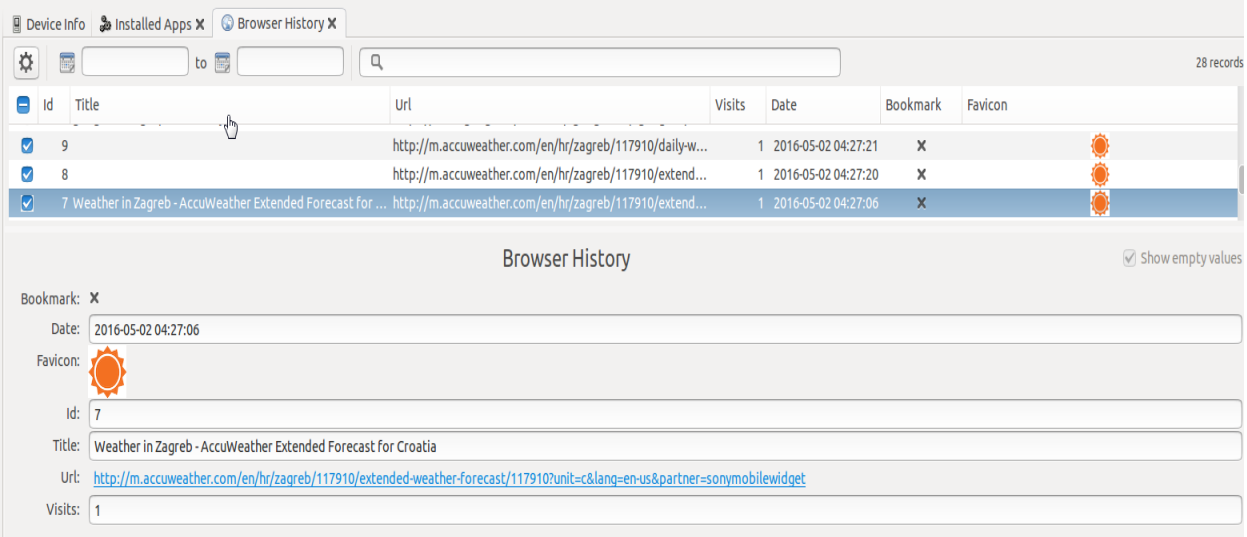
Na slici 17 su prikazane detaljne informacije o uređaju koje su zapisane u jednoj od dohvaćenih tekstualnih datoteka. Ovakve informacije također mogu poslužiti za daljnju identifikaciju vlasnika. Među njima se nalazi serijski broj MTU-a, IMEI/MEID, ime proizvođača MTU-a, verzija OS-a, vrsta matične ploče i tip korisničkog računa.



Slika 17. Prikaz prikupljenih informacija koje mogu poslužiti za daljnu identifikaciju vlasnika MTU-a

Na slici 18 se vidi povijest pretraživanja MTU-a, na njegovom tvornički ugrađenom Internet pregledniku. Pri pažljivom pregledavanju nađeni su API (Aplication Programing Interface) pozivi na Internet adresu za aplikaciju „AccuWeather“. Aplikacija dolazi tvornički ugrađena u MTU i njena svrha je skupljanje i prikaz vremenskih prognoza za područje u kojem se MTU nalazi. Kako bi to postigla, aplikacija preko interneta šalje upite za prognozu matičnim serverima s nazivom lokacije na kojoj se trenutno MTU nalazi.

Takva lokacija je vidljiva u web adresi i pojaviti će se u povijesti Internet preglednika što je vidljivo sa slike 18. Na kraju URL-a (Uniform Resource Locator) vidljiv je dio „=sonymobilewidget“ što potvrđuje kako se radi o API pozivu aplikacije, uz podatak kako je posjet Internet adresi izvršen u ranim jutarnjim satima.



Slika 18. Povijest internet pretraživanja i prikaz API poziva aplikacije za vremensku prognozu

Iz navedenog se može zaključiti kako je vlasnik MTU-a koristio uređaj kako bi skenirao bežične mreže komunikacije tvrtke koja se bavi informatičkim poslovanjem. Također se saznalo kako se vlasnik nalazio na području grada Zagreba te njegova privremena e-mail adresa za pristup uslugama tvrtke Google. Iako se počinitelj nije identificirao direktno, dobivene informacije će tijelima za provođenje zakona biti dovoljne za daljnju istragu.

6. ZAKLJUČAK

Forenzička analiza MTU-a je dugotrajan proces koji puno ovisi o vanjskim faktorima kao što je generacija uređaja na kojem se vrši analiza, vrsta OS, stanje uređaja, odnosno koliko je uređaj fizički ili softverski bio oštećen, te najvažnije od svega, s kojim programskim alatom se vrši forenzička analiza. Alati s najmanje funkcija s veoma očuvanih MTU-a mogu izvući jako malo podataka dok najbolji alati s jako oštećenih MTU-a mogu izvući veliku količinu podataka.

S time u vezi treba uzeti u obzir kako su mogućnosti alata proporcionalni njegovoj ekonomskoj vrijednosti, pa tako najbolje alate imaju državne službe i institucije i velike korporacije koje se bave sigurnošću IK sustava. Nasuprot tome alati za forenzičku analizu MTU-a koji imaju najmanje mogućnosti su uglavnom dostupni za besplatno preuzimanje s Interneta. NowSecure Forensics CE unatoč tome ne spada u zadnju kategoriju, sa svojim mogućnostima konkurira skupljim alatima dok je dostupan besplatno uz registraciju. NowSecure Forensics CE ima dvostruku funkciju, na prvom mjestu služi kao uvid u naprednije mogućnosti svoje pune inačice NowSecure Forensics, dok na drugom mjestu osobama koji ulaze u područje forenzičke analize MTU-a služi kao izvrsna početna točka.

Uz vidljiv porast korištenja MTU-a u suvremenom svijetu nezaobilaznim postaje mogućnost izvršiti forenzičku analizu nad tim uređajima kako bi se došlo do podataka koje ti MTU-i sadrže. Tako je forenzička analiza MTU-a postala dio svake ozbiljnije istrage što pak zahtijeva veći broj stručnjaka iz tog područja.

NowSecure Forensics CE zbog nedostatka značajki nije povoljan za korištenje u stvarnim slučajevima, ali može poslužiti kao izvrstan alat za obuku ljudi na području forenzičke analize MTU-a. Forenzička analiza je veoma kompleksan proces za koji je potrebno interdisciplinarno iskustvo za što je pak potrebno dugo vremensko razdoblje kako bi se steklo. NowSecure Forensics CE omogućuje bilo kome korištenje čime studenti pa i učenici srednjih škola mogu steći početno znanje koje dalje mogu usavršavati na profesionalnim alatima kao što je potpuna inačica NowSecure Forensics.

LITERATURA

[1] E. R. Mumba and H. S. Venter, "Mobile forensics using the harmonised digital forensic investigation process," 2014 Information Security for South Africa, Johannesburg, 2014, pp. 1-10.doi: 10.1109/ISSA.2014.6950491

[2] Bommisetty S., Tamma R., Mahalik H. (2014) Introduction to Mobile Forensics: Practical mobile forensic approaches, *Practical Mobile Forensics*[online], UK: Pack Publishing Limited Dostupno na: https://www.packtpub.com/mapt/book/Application%20Development/9781783288311/1 [20.08.2016]

[3] http://www.nist.gov/forensics/upload/2-Brothers-NIST-2014_Slides-23-Pages-2.pdf [19.08.2016]

[4] K. A. Alghafli, A. Jones and T. A. Martin, "Forensics data acquisition methods for mobile phones," Internet Technology And Secured Transactions, 2012 International Conference for, London, 2012, pp. 265-269.

[5] http://www.cellebrite.com/Pages/file-system-extraction-of-mobile-data [19.08.2016]

[6] T. B. Tajuddin and A. A. Manaf, "Forensic investigation and analysis on digital evidence discovery through physical acquisition on smartphone," 2015 World Congress on Internet Security (WorldCIS), Dublin, 2015, pp. 132-138. doi: 10.1109/WorldCIS.2015.7359429

[7] https://standards.ieee.org/findstds/standard/1149.1-2013.html [19.08.2016]

[8] Be Van Ngo, P. Law and A. Sparks, "Use of JTAG boundary-scan for testing electronic circuit boards and systems," 2008 IEEE AUTOTESTCON, Salt Lake Cirty, UT, 2008, pp. 17-22. doi: 10.1109/AUTEST.2008.4662576

[9] G. G. N. Kumar, G. Cousins and M. Sprayberry, "JTAG debug tool for efficient debugging on V93K," Electronics Packaging Technology Conference (EPTC 2013), 2013 IEEE 15th, Singapore, 2013, pp. 407-409.doi: 10.1109/EPTC.2013.6745752

[10] N. Samet, A. Ben Letaïfa, M. Hamdi and S. Tabbane, "Forensic investigation in Mobile Cloud environment," Networks, Computers and Communications, The 2014 International Symposium on, Hammamet, 2014, pp. 1-5.doi: 10.1109/SNCC.2014.6866510

[11] National Institute for Standards and Technology (2013) *Guidelines on Mobile Device Forensics(Draft)* Gaithersburg U.S. Department of Commerce Dostupno na: http://www.nist.gov/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf [19.08.2016]

[12] https://www.nowsecure.com/forensics/ [20.08.2016]

[13] https://www.nowsecure.com/forensics/community/ [20.08.2016]

[14]https://www.elie.net/blog/security/survey-most-people-dont-lock-their-android-phones-but-should#.UzKKs9zKZZh [20.08.2016]

[15] Zakon o zaštiti osobnih podataka (pročišćeni tekst zakona, Narodne Novine, br. 103/03, 118/06, 41/08, 130/11, 106/12)

[16]http://www.cellebrite.com/Media/Default/Files/Forensics/Features-Lists/UFED-Physical-Analyzer-FeaturesList.pdf [21.08.2016]

[17]http://www.cellebrite.com/Media/Default/Files/Forensics/Features-Lists/UFED-Logical-Analyzer-FeaturesList-1.pdf [21.08.2016]

[18]http://www.mobiledit.com/forensic-features [21.08.2016]

[19]http://secureview.us/buy.html [21.06.2016]

[20]http://www.fpz.unizg.hr/DatotekeFPZ/Pravilnik_o_stegovnoj_odgovornosti_studenata_FPZ.pdf [31.08.2016]

[21]http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-404.pdf [31.08.2016]

POPIS KRATICA

ADB	(Android Debug Bridge) standardizirano sučelje za ispravljanje pogrešaka na Android uređajima
AT	(Attractive Commands) standard naredbi za operacije kao što je uspostavljanje poziva, biranje broja i mijenjanje parametara konekcije
CC	(Cloud Computing) dijeljenje resursa između računala u „oblaku“
CE	(Community Edition) izdanje napravljeno besplatno za širi dio zajednice
FB	(Flasher Box) Kutija za bljeskanje
GPS	(Global Positioning System) globalni sustav za navigaciju
IMEI	(International Mobile Equipment Identity) međunarodni broj mobilne opreme
IrDA	(Infrared Data Association) set protokola za infracrvenu komunikaciju
JSON	(JavaScript Object Notation) standard za organizaciju podataka u tekstualnom obliku
JTAG	(Joint Test Action Group) organizacija za postavljanje industrijskih standarda
MEID	(Mobile Equipment Identifier) identifikator mobilne opreme
NIST	(National Institute for Standards and Technology) Nacionalni Institut za Standarde i Tehnologiju
PIN	(Personal Identification Number) osobni identifikacijski broj
SIM	(Subscriber Identity/Identification Module) modul za identifikaciju pretplatnika
USB	(Universal Serial Bus) standard za povezivanje elektroničkih uređaja kabelom
VM	(Virtual Machine) virtualizacija računala i OS koja se pokreće u specijaliziranom programu na drugom računalu

POPIS SLIKA

Slika 1. Usporedba brzine ekstrakcije i količine dobivenih podataka 3

Slika 2. Prikaz osnovnih informacija prikupljenih s MTU-a 11

Slika 3. Usporedba dobivenih podataka datotečnom ekstrakcijom (lijevo) i logičkom ekstrakcijom (desno) 13

Slika 4. Prikaz niza naredbi u Linux terminalu za kopiranje datoteke s uzorkom sa MTU-a na računalo 15

Slika 5. Prikaz dviju GPS lokacija koje su očitane iz fotografija 17

Slika 6. Prikaz vremenske crte i njenog grafičkog sučelja 18

Slika 7. Prikaz rezultata dobivenih pretragom ključne riječi 19

Slika 8. Rezultat dekripcije datoteke s uzorkom 26

Slika 9. Mogućnost odabira između više sigurnosnih propusta za *root* otključavanje MTU-a 27

Slika 10. Dio popisa binarnih podataka nakon datotečne ekstrakcije MTU-a Sony Xperia Miro 28

Slika 11. Prikaz preuzetih datoteka i povijesti internet pretraživanja koje odgovaraju ključnoj riječi "e-student" 29

Slika 12. Korisnički računi koji su bili korišteni na MTU-u 30

Slika 13. Prikaz osnovnih informacija prikupljenih s MTU-a Xperia Z1 31

Slika 14. Prikaz svih tekstualnih datoteka preuzetih logičkom ekstrakcijom 32

Slika 15. Bluetooth MAC adresa MTU-a Sony Xperia Z1 32

Slika 16. Instalirane aplikacije na MTU-u Xperia Z1 33

Slika 17. Prikaz prikupljenih informacija koje mogu poslužiti za daljnu identifikaciju vlasnika MTU-a 34

Slika 18. Povijest internet pretraživanja i prikaz API poziva aplikacije za vremensku prognozu 35

POPIS TABLICA

Tablica 1.Usporedba mogućnosti različitih alata za forenzičku analizu MTU-a.....22