FBIM Transactions
DOI 10.12709/fbim.07.07.01.06

SAVREMENA RAČUNARSKA FORENZIKA I FORENZIČKI ALATI

MODERN COMPUTER FORENZICS AND FORENZIC TOOLS

Zoran Čekerevac
Poslovni i pravni fakultet, „Union – Nikola Tesla“ Univerzitet, Beograd, Srbija

Zdenek Dvorak
University of Žilina, Faculty of Security Engineering, Žilina, Slovakia

Lyudmila Prigoda
Maykop State Technological University, Maykop, Russian Federation

JEL Category: **C88, L86**

Apstrakt

Sve veća upotreba računara i na njima zasnovanih uređaja i opreme omogućila je znatna poboljšanja u funkcionisanju preduzeća i ustanova, ali i pojedinačnih korisnika. Istovremeno su se pojavili i rizici zbog njihove nepravilne upotrebe ili zloupotrebe. Do gubitka ili krađe podataka može doći na najrazličitije načine, od greške u radu korisnika, do pojedinačnih ili masovnih napada zlonamernih napadača. Neke od problema je moguće rešiti upotrebom alata samog operativnog sistema ili korišćenog softvera, a za pojedine situacije, kada je (ne)delo već izvršeno, potrebno je koristiti specijalne, namenske forenzičke alate. U slučaju potrebe za sudskim veštačenjem, zadatak forenzičara postaje još kompleksniji, jer uz otkrivanje uzroka, forenzičar mora da pruži i valjane dokaze da je delo učinjeno i (ako je moguće) ko ga je učinio, ali i da sam artefakt ostavi u nepromenjenom stanju da bi mogla da se izvrše i druga forenzička istraživanja bilo u vezi sa drugim razlozima bilo da ih izvrši druga institucija (ili drugi forenzičar). Zbog toga, a i zbog drugih razloga, neophodno je korišćenje specijalizovanih forenzičkih alata. U ovom radu se posle uvodnog dela u kome se razmatraju forenzika i antiforenzika, kratka istorija i savremena zakonska regulativa, kao i izazovi u vezi sa forenzikom i alatima, detaljnije razmatraju računarski forenzički alati. Akcenat je stavljen na besplatne forenzičke alate. U zaključcima rada su sumirani stavovi o forenzici i forenzičkim alatima i ukazano na pravce budućeg razvoja, posebno u vezi sa masovnijom primenom Interneta stvari.

Ključne reči: *forenzika, antiforenzika, IT alati, računari, Internet stvari, bezbednost, zaštita.*

Adresa autora zaduženog za korespodenciju:
Zoran Čekerevac
zoran@cekerevac.eu

Abstract

Increased use of computers and devices and equipment based on them has made significant improvements in the functioning of companies and institutions, but also individual users. At the same time, risks have arisen due to their improper use or misuse. The loss or theft of data can occur in a variety of ways, from a user's error to an individual or mass attacks of malicious attackers. Some of the problems can be solved using the operating system's or application software's tools, but for specific situations, when the misdoing has already been done, it is necessary to use special, dedicated forensic tools. In case of need for judicial expertise, the task of forensic experts becomes even more complex, as with the detection of causes, the IT forensic expert must provide valid evidence that the act was done and (if possible) who made it, but also left the artifact in an unchanged state that other forensic research could be carried out either in connection with other reasons, or by another institution (or another forensic expert). Therefore, and for other reasons, it is necessary to use specialized forensic tools. In this paper, after the introductory part, which examines forensics and anti-forensics, short history and contemporary legislation, as well as the challenges associated with forensics and tools, the computer forensic tools are discussed in greater detail. The accent is placed on free forensic tools. The conclusions of the paper summarize views on forensics and forensic tools and point out the directions for future development, especially in connection with the massive use of the Internet of Things.

Keywords: *Forensics, anti-forensics, IT tools, computers, IoT, security, protection.*

1 UVOD

Neverovatno brz razvoj računara i softvera i masovnost njihove upotrebe poslednjih par decenija i perspektive daljeg ubrzanog razvoja, pre svega kroz „Internet stvari“ (IoT), donele su mnoge blagodeti čovečanstvu i otvorile nove mogućnosti daljeg napretka, ali su sa sobom donele i mnogobrojne izazove koji su nepovratno promenili svet i način rada i razmišljanja. Sa jedne strane, svaki pojedinac ima (praktično) neograničene mogućnosti za komunikaciju, za sticanje novih saznanja, prikupljanja podataka o svemu i svačemu, za daljinsko upravljanje ličnim uređajima, pa i velikim postrojenjima, zabavu i još mnogo šta. I dok mu to kao korisniku sasvim odgovara, u jednom trenutku se i on može pojaviti kao objekat interesovanja, što mu u najmanju ruku može biti neprijatno. Tada poželi da sve ono što je ranije sa ponosom ili lakomisleno objavljivao, nekako obriše, skloni ili sakrije. Sa druge strane, sa povećanjem broja uređaja koje koristi, raste i mogućnost da se neki od njih ošteti ili da postane nefunkcionalan iz najrazličitijih razloga. Sa pristupom Internetu i korišćenjem Internet resursa raste i opasnost od zlonamernih napada na korisničke podatke, pa čak i napada na funkcionisanje celih, fizičkih, postrojenja. Kada se sve ovo ima u vidu, lako je zaključiti da su potrebe korisnika veoma raznovrsne i da ih je, najverovatnije, teško u potpunosti zadovoljiti.

Tabela 1. Neki od nedavnih slučajeva gubitka podataka

Datum	**15.07.2017.**	**01.05.2017.**	**06.03.2017.**	**13.06.2017.**
Žrtva	Equifax	Motor Vehicles Department in Kerala	River City Media	Deep Root Analytics
Broj zapisa	147.700.000	200.0000.000	1.340.000.000	198.000.000
Šta je ukradeno	Krađa identiteta	Krađa podataka o registraciji vozila	Krađa e-mail adresa	Krađa identiteta
Ko je izvršilac	Maliciozni spoljašnji napadač	Maliciozni spoljašnji napadač	Greška administratora	Greška administratora
Vrsta vlasnika podataka	Kreditni biro	Država	Marketing organizacija	Republikanski Nacionalni Komitet
Država	SAD	Indija	SAD	SAD
Ocena rizika	10	9,9	9,8	9,6

Izvor: (Breach Level Index, 2018)

Gubici podataka su svakodnevni, a Breach Level Index pokazuje više od 9.728.017.988 podataka koji su izgubljeni ili ukradeni od 2013. do 17.08.2018. To govori da se 55 zapisa gubi svake sekunde. Samo 4% izgubljenih zapisa su zapisi kod kojih je korišćena enkripcija. (Breach Level Index, 2018)

Neka od najvećih gubljenja podataka su slučajevi: JP Morgan Chase, Bank of America, HSBC, TD Bank, Target, Tumbler, Home Depot, MySpace, eBay, Adobe System Inc, iMesh, a neki od nedavnih slučajeva su prikazani u tabeli 1.

Juniper Research (Smith, 2015) sugeriše da će do 2019. godine IT kriminal kompanije koštati preko 2 biliona dolara. Zbog toga će se povećati i zahtevi za računarskom forenzičkom ekspertizom.

Aktivnosti u oblasti zaštite podataka su obično podeljene u dve osnovne grupe, preventivne mere i forenzičke mere. Preventivnim merama se nastoji da se negativni uticaji preduprede. Za ove svrhe se koriste različite mere zaštite, od zaštitnog zida (fajervola) i antivirusnih programa, do redovnih bekapa. Kada je šteta već učinjena, na red dolazi forenzika, koja po definicija predstavlja proces otkrivanja i tumačenja elektronskih podataka sa ciljem da "sačuva bilo koji dokaz u svom najoriginalnijem obliku dok vrši strukturiranu istragu sakupljanjem, identifikacijom i validacijom digitalnih informacija u svrhu rekonstrukcije prošlih događaja" (Techopedia, 2016). Forenzika i forenzički alati se mogu koristiti i preventivno, u cilju provere zaštite sistema, ali ta primena, kao ni preventivne mere u zaštiti računarskih sistema, ovde neće biti razmatrani.

1.1 Forenzika i antiforenzika

Donedavno se moglo govoriti sa velikom tačnošću da je forenzika nauka koja se bavi pronalaženjem razloga zašto nešto više nije kako treba. I ta bi se definicija tada mogla preneti i na računarsku forenziku. Danas to više tako verodostojna definicija, jer se pored računara u oblasti digitalne forenzike pojavljuju i mnogi drugi učesnici kao višestruki operativni sistemi, mreže, uređaji za umrežavanje, serveri za različite namene, baze podataka, softverske aplikacije… Naravno, ne treba gubiti iz vida nadirući IoT. Predmet ovog rada je računarska forenzika u užem smislu i prvenstveno će biti razmatrani računari i podaci koji se u njima nalaze.

U mnogim slučajevima korisnici računara imaju interes da unište sve ili neke zapise tako da se ne mogu oporaviti i pročitati. Mada je to najčešći slučaj kod nedozvoljenih aktivnosti, to može da bude i legalna i legitimna potreba korisnika u slučajevima kada otuđuje opremu koja još ima upotrebnu vrednost ili je menja novom. Zato se može reći da uz forenziku, vrlo često, paralelno ide i antiforenzika koja po definiciji ima suprotne ciljeve. Kada se govori o antiforenzici, obično se razmišlja o tome da ona služi da počisti tragove napada, zlonamerne upotrebe i tragove upada, da na neki način spreči rad forenzičkih alata ili da ga uspori do neisplativosti. Međutim, antiforenzika može i da posluži kao metod odbrane od krađe podataka. Posebna vrsta upotrebe antiforenzike je provera sposobnosti i pravilnosti rada računarskih forenzičkih alata i podsticanje njihovih kreatora na dalji rad i usavršavanje alata.

Ako se zanemare ekstremni slučajevi IT kriminala, koji uzgred i retko stižu u sudove, većina slučajeva iz sudske prakse se svodi na potvrđivanje ili pobijanje sumnje da je neki korisnik zloupotrebio pravo pristupa i preuzeo i/ili preneo podatke koje nije smeo, da je komunicirao sa nekim ili da je izvršio neku transakciju, napravio neku fotografiju ili dokument u određenom trenutku ili vremenu i slično. Vrlo često se u praksi IT veštaka javljaju slučajevi da su akteri samouki ili delimično obučeni, pa je rad veštaka time olakšan. Međutim, zbog raznovrsnosti korišćenih uređaja i po vrsti i po karakteristikama i po proizvođačima, rad IT veštaka postaje svakim danom sve kompleksniji. U slučajevima kada se radi o vrhunskim IT ekspertima, teško je naći odgovarajućeg IT veštaka, pa čak i veoma razvijeni timovi moraju tražiti pomoć specijalizovanih veštaka negde u svetu.

1.2 Kratka istorija i zakonska regulativa

IT forenzika je po svojoj suštini jedna od grana dobro poznate forenzičke nauke koja teži da prikupi sve moguće dokaze vezane za neki događaj, samo što se ovde radi o digitalnom svetu, o prikupljanju nula i jedinica, koje predstavljaju meta-podatke, datoteke dnevnika, IP adrese i slično. Računari i njihova intenzivna primena su novijeg datuma, pa je i IT forenzika mlada nauka. U početku, u prvoj polovini sedamdesetih godina

bilo je malo računara, pristup računarima je bio ograničen na vrlo mali broj ljudi, načini prenosa podataka su bili ekstremno neudobni i, objektivno, veća pažnja je bila posvećena njihovoj fizičkoj bezbednosti nego sadržajima koje su posedovali ili mogli da poseduju. Zbog toga se privatnošću i računarskom bezbednošću bavio samo mali broj ljudi. Šta više, ni zakon nije prepoznavao delo računarskog kriminala. Pojavom personalnih računara i razvojem računarskih mreža situacija se naglo menja, pa je moguće reći da je prekretnicu predstavljao Zakon o računarskom kriminalu Floride iz 1978. godine (Norman, 1978). Ovim zakonom su prepoznati prvi računarski zločini u SAD i uključeni su u zakonodavstvo protiv dela neovlašćenog brisanja ili modifikacije računarskih podataka. Uskoro su usledili drugi zakoni kao Američki Federalni zakon o računarskim prevarama i zlostavljanju (Cole, 2012) i britanski Zakon o računarskim zloupotrebama (Computer Misuse Act, 1990). Posle toga su usledile dugotrajne, deceniju duge, diskusije uglavnom oko prepoznavanja kompjuterskih zločina kao ozbiljnih pretnji ličnoj, organizacionoj i nacionalnoj bezbednosti. 2004. godine Naučna radna grupa za digitalne dokaze (SWGDE), objavila je "Najbolje prakse za računarsku forenziku" (SWGDE, 2004). Ovo izdanje je doživelo bitnu reviziju 2013. godine i minimalne korekcije 2014. godine.

2005. godine publikovan je standard ISO 17025 „Opšti zahtevi za kompetentnost laboratorija za ispitivanje i laboratorija za etaloniranje“ (ISO/IEC 17025, 2005) koji je kasnije revidiran 2017. godine. U Republici Srbiji su obe verzije standarda prevedene i objavljene kao SRPS ISO/IEC 17025:2006 i 2017, uz korekciju Ispr.1:2018. Ovi standardi i uputstva pomogli su publikovanje najboljih praksi računarskih forenzičara, specijalista, i pokrenuli mnoge forenzičke kompanije da kreiraju nova softverska rešenja koja su mogla da idu u korak sa novim zahtevima. U Republici Srbiji je IT kriminal dobio svoju zakonsku regulativu u obliku Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala (NSRS, 2005). Republika Srbija je potpisala i Konvenciju o sajber kriminalu i Dodatni protokol uz Konvenciju u Helsinkiju 2005. godine.

1.3 Izazovi za forenzičare i forenzičke alate

Tipični forenzički proces ima nekoliko različitih faza (n.d., 2018): zaplenu, forenzičku akviziciju, analizu i izradu izveštaja zasnovanog na prikupljenim podacima. U slučaju javnog sektora, rad IT forenzičara se najčešće svodi na podržavanje ili odbacivanje hipoteze pred krivičnim ili građanskim sudovima, ali mnogo raznovrsnije je angažovanje IT forenzičara u privatnom sektoru i u istraživanju upada u sisteme. Tu su zadaci toliko raznovrsni da se forenzičari vrlo često fokusiraju na samo jednu ili nekoliko podgrupa digitalne forenzike kako bi mogli da ostvare odgovarajući nivo znanja. Iako zadaci forenzičara mogu da budu vrlo slični, ili, čak, isti, forenzika se najčešće grubo deli prema vrsti posmatranih uređaja, pri čemu se izdvajaju računarska forenzika, forenzika mobilnih uređaja, forenzika u mreži, forenzička analiza podataka i forenzika baza podataka. Forenzika mobilnih uređaja doživljava najintenzivniji rast pre svega zbog enormnog rasta broja korišćenih mobilnih uređaja.

IT forenzičari se u praksi susreću sa različitim slučajevima. Jedan od slučajeva je slučaj skrivanja podataka. Napadači pokušavaju da naprave tajni ulaz (tzv. zadnja vrata, „back door“), ali da bi ostao tajni, potrebno je sakriti podatke o njegovom postojanju, bilo šifrovanjem, steganografijom ili kombinacijom više tehnika. Najbazičniji načini skrivanja podataka, koji ne zahtevaju posebne IT veštine, su premeštanje datoteka, korišćenje skrivenog medijuma, preimenovanje datoteka i ekstenzija, deljenje datoteka na manje segmente i njihovo smeštanje na različite lokacije. Nešto kompleksniji metod je šifrovanje datoteka, meta-podataka o datotekama, pa i čitavih diskova. Steganografija koristi princip da je najlakše sakriti papir među papirima. Naime, glavni uslov je da se zapis ne razlikuje po svom spoljašnjem izgledu od okruženja. Praktično, maskira se i postavlja među regularne, korisne, zapise. Jedan od načina je čista eliminacija izvora podataka o napadu. Na mesto napada se dovede zlonamerni kod, raspakuje se, iskoristi, a potom zapakuje i ukloni sa mesta napada. Na sličan način se mogu koristiti virtualne mašine, anonimni identiteti, preusmeravanje sistemskih poziva, itd.

Druga grupa slučajeva sa kojima se sreću IT forenzičari su slučajevi brisanja podataka. Kod

potpunih amatera vlada uverenje da je dovoljno samo obrisati određenu datoteku. Oni malo obučeniji znaju da im to ne daje nikakvu zaštitu, pa pribegavaju povratnom ili (za sada) nepovratnom brisanju svih podataka i/ili fizičkom uništavanju medijuma kako bi se obrisali svi tragovi. Najjednostavniji način brisanja podataka je ponovno pisanje drugih podataka preko postojećih podataka. Ovaj način ne garantuje da prethodni zapis neće biti u potpunosti ili delimično nečitljiv. Za sigurnije brisanja podataka postoje aplikacije koje ceo disk popunjavaju nulama ili jedinicama, ili, čak, omogućavaju višestruko pisanje i brisanje, tako je da praktično nemoguće povratiti početne podatke. Manje destruktivni programi ciljaju samo na sektore koje treba ukloniti. Tako se samo kod sektora na kojima postoje forenzički tragovi vrši ponovni upis podataka. Ovaj postupak je znatno kompleksniji, zahteva nadzor i ne briše sve meta-podatke. U slučaju magnetnih diskova, moguće je uraditi potpunu demagnetizaciju diska što omogućava potpuno brisanje diska, ali pri tome disk mora biti fizički dostupan, a može postati i potpuno neupotrebljiv. A, ako se želi potpuno uništavanje diska postoje mnoge druge, jeftinije, fizičke i hemijske metode.

Treću grupu slučajeva čini zametanje tragova, zamagljivanje situacije. Tu su na raspolaganju brojne mogućnosti, od brisanja tragova, do postavljanja raznih brojnih tragova koji ne vode nikuda, do postavljanja beznačajnih izmena na datotekama čije će uzaludno izučavanje oduzeti mnogo vremena. Promene zaglavlja datoteka, uz promenu vremenskog žiga i brisanje dnevnika zapisa, u suštini predstavlja vrlo efikasan metod koji pravi skoro nepremostive probleme IT veštaku pri izradi valjanog izveštaja o veštačenju. U tu svrhu mogu se koristiti i neki besplatni open-source programi.

Četvrta grupa slučajeva sa kojima se susreću IT forenzičari su slučajevi direktnih napada na alate i tehnike koje forenzičari koriste. Ovo su retki slučajevi i zahtevaju posebnu pripremu i posebna znanja napadača kako o računaru koji napada, tako i o onima koji ga štite, kao i alatima koje koriste. Svaki forenzičar ima svoj omiljeni alat, a svaki alat ima svoje slabosti. Ovo su ipak situacije sa kojima se sudski veštaci retko susreću i ovde neće biti detaljnije razmatrani.

2 RAČUNARSKI FORENZIČKI ALATI I OPREMA

Zadatak sudskog veštačenja je da sudu pruži relevantne informacije o učinjenom ili neučinjenom delu, a alati su najbolji prijatelji IT veštaka. Omogućavaju im da iz šume podataka izvuku ono što im je važno. Pored toga, da bi se dobili verodostojni podaci, veštak mora da ispoštuje određenu proceduru.

U slučaju veštačenja sadržaja hard diska (HD), prvo što IT veštak radi je uklanjanje hard diska iz računara i njegovo povezivanje na uređaj za onemogućavanje novih upisa na HD. Na taj način je sprečeno svako brisanje podataka ili naknadno upisivanje podataka na HD, a omogućeno čitanje i kopiranje zapisa sa HD. Za kopiranje sadržaja diska sa tačnošću do nivoa bita mogu se koristiti razni alati i platforme kao što su Digital Forensics Framework, Open Computer Forensics Architecture, CAINE (Computer Aided Investigative Environment), X-Ways Forensics, SANS Investigative Forensics Toolkit (SIFT), EnCase, itd., mada mnogo profesionalnih forenzičara više voli da umesto neke sveobuhvatne platforme koristi grupu forenzičkih alata po svom sopstvenom izboru. Na taj način iz bogate ponude softverskih rešenja biraju samo ono što im je potrebno za ekspertize za koje su se specijalizovali.

Karakteristike i mogućnosti profesionalnih forenzičkih alata se razlikuju prvenstveno zbog razlika u njihovim osnovnim namenama, ali se očekuje da veliki softverski paketi podržavaju heširanje svih datoteka i celog diska, vremenske i datumske žigove, akviziciju i filtriranje podataka, te učitavanje bekapa iOS-a i analizu njegovih podataka. Za razliku od državnih institucija, privredne organizacije obično nisu zainteresovane za iščitavanje RAM memorije, kao i za mogućnost prethodnog pregleda zapisa. Razlog je vrlo jednostavan, jer kompanije obično ne raspolažu ni odgovarajućim stručnim kadrom koji bi mogao da realizuje te aktivnosti.

Da bi se omogućila efikasnija i uspešnija ispitivanja i istrage, programeri su kreirali mnogo različitih računarskih forenzičkih alata, koji bi se u zavisnosti od toga čemu su namenjeni, mogli podeliti na (Shankdhar, 2018):

- alati za snimanje diska i podataka,
- alati za pregled i oporavak fajlova,
- alatke za analizu datoteka,

- alati za analizu registara,
- Internet analitički alati,
- alati za analizu e-pošte,
- alati za analizu mobilnih uređaja,
- OS analitički alati,
- mrežni forenzički alati i
- forenzički alati za baze podataka

U ovu podelu se svakako mogu dodati i:

- alati za ekstrakciju meta-podataka iz dokumenata,
- anti-forenzički alati i
- alati za sigurno brisanje podataka.

Podela alata bi se mogla izvršiti i sa drugih tački gledišta, u zavisnosti od toga da li su proaktivni ili namenjeni za upotrebu posle samog događaja, kojim su operativnim sistemima i uređajima namenjeni, kao i mnogo detaljnije, na osnovu delova uređaja za koje su specijalizovani, no to ovde neće biti učinjeno. Jedna od bitnih, nezaobilaznih, podela je podela na besplatne i na one koji se plaćaju. S obzirom na dostupnost forenzičkih alata ovde ćemo pažnju posvetiti besplatnim alatima.

Kvalitet forenzičkih alata je postao vrlo visok tako da se uz njihovu primenu do sticanja osrednjih forenzičkih veština može stići relativno brzo. Interesovanje za vrhunske eksperte u računarskoj forenzici postaje sve ređe kako zbog kvaliteta forenzičkih alata, tako i zbog boljeg obrazovanja bilo da je ono realizovano kroz specijalne treninge ili kroz univerzitetsko obrazovanje. Toliko je velika konkurencija za obuku i sertifikaciju u organizacijama za obuku na komercijalnom nivou da su neke neprofitne organizacije kao što je napustile tržište. Nedavno je Internet Systems Consortium (ISC)[2] objavio da je napustio sertifikat CCFP (*Certified Cyber Forensics Professional*), jedini takav sertifikat u svetu koji je zahtevao ili značajno iskustvo (šest godina) ili univerzitetsku diplomu. (Stephenson, 2017)

Pre analize nekih od forenzičkih alata, neizostavno je konstatovati da je uvek dobro imati na raspolaganju više alata, pa makar oni radili skoro iste stvari. To je dobro i za forenzičare, ali i za proizvođače forenzičkih alata.

Prateći razvoj forenzičkih alata može se zapaziti da se od nekadašnjih pojedinačnih specijalizovanih alata došlo do sveobuhvatnih platformi koje obuhvataju mnoštvo različitih alata koji su međusobno povezani i koji omogućavaju glatko prelaženje sa jednog na drugi, iz jedne oblasti u drugu. Međutim, današnje takve platforme su ipak retke, a zbog mnoštva novih proizvoda i alata nije nemoguće da će u jednom trenutku postati same sebi prepreka daljem razvoju. Pored toga, može se zapaziti i da neki ne-forenzički alati kao npr. SIEM-i (*Security Information and Event Management*) počinju da dobijaju forenzičke zadatke. I to nam može pomoći da razumemo realnost digitalne forenzike.

U tabeli 2 je prikazano deset popularnih forenzičkih alata po slučajnom rasporedu. Treba imati u vidu da njihov položaj u tabeli ne odražava njihov značaj u forenzičkoj praksi. Pored toga, treba naglasiti i da ne postoje egzaktni kriterijumi kojima se može doći do „najboljeg forenzičkog alata“. U tabeli su pored kratkog opisa prikazane i osnovne karakteristike i URL adrese sa kojih je moguće preuzeti softver.

Tabela 2 Deset besplatnih forenzičkih alata

R.Br.	Naziv alata	Opis	Osnovne karakteristike	URL
1	**SIFT - SANS Investigative Forensic Toolkit**	SIFT ima mogućnost ispitivanja diskova, tj. podataka, na nivou bajtova direktno sa hard diska ili bilo kojeg drugog uređaja za skladištenje, više fajl sistema i formata dokaza. U osnovi je baziran na Ubuntuu i predstavlja Live CD uključujući i alate za koji su potrebni za detaljnu forenzičku istragu. Najbolja stvar oko SIFT alata je to što je slobodan i "Open Source".	- Ubuntu LTS 14.04 Base. - 64-bit base system. - Bolje korišćenje memorije. - Automatsko ažuriranje DFIR paketa i prilagođavanja. - Najnovije forenzičke alati i tehnike. - VMware Appliance spreman za forenziku. - Kompatibilnost između Linux-a i Windows-a. - Opcija za samostalno instaliranje putem (.iso) ili korišćenje preko VMware Player/Workstation. - Onlajn dokumentacija na ReadTheDocs - Podrška za Expanded Filesystem.	https://digital-forensics.sans.org/community/downloads

R.Br.	Naziv alata	Opis	Osnovne karakteristike	URL
2	**Nmap**	Nmap ("Netvork Mapper") je besplatan i open source (licencirani) alat za otkrivanje mreže i reviziju bezbednosti. Mnogi sistem i mrežni administratori takođe smatraju ga korisnim za inventarisanje mreže, upravljanje vremenskim planovima za nadogradnju usluge i nadzor nad vremenom rada hosta ili usluge. Nmap koristi sirove IP pakete kako bi utvrdio koji su hostovi dostupni na mreži, koje usluge (naziv aplikacije i verzija) hostovi nude, koje operativne sisteme (i verzije OS-a) pokreću, koje vrste paketnih filtera i zaštitnih zidova su u upotrebi i desetine drugih karakteristika. Dizajniran je za brzo skeniranje velikih mreža, ali radi dobro i sa pojedinačnim hostovima. Nmap radi na svim većim računarskim operativnim sistemima, a službeni binarni paketi su dostupni za Linux, Windows i Mac OS X. Pored klasične Nmap izvršne komandne linije, Nmap paket uključuje napredni pregledač GUI i pregled rezultata (Zenmap), fleksibilnu alatku za prenos, preusmeravanje i debagovanje podataka (Ncat), uslužni program za upoređivanje rezultata skeniranja (Ndiff) i alatku za generisanje paketa i analizu odgovora (Nping). Nmap je proglašen za "Sigurnosni proizvod godine" od strane Linux žurnala, Info World-a, LinuxQuestions.Org i Codetalker Digest.	- Fleksibilan: Podržava desetine naprednih tehnika za mapiranje mreža. - Moćan: Nmap se koristi za skeniranje ogromnih mreža sa bukvalno stotinama hiljada mašina. - Prenosiv: Podržani su većini operativnih sistema, uključujući Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIKS, Mac OS X, HP-UKS, NetBSD, Sun OS, Amiga itd. - Lak za upotrebu: Dostupne su i tradicionalne komandne linije i grafičke verzije (GUI). - Besplatan: Nmap je dostupan za besplatno preuzimanje, a dolazi i sa punim izvornim kodom koji možete modifikovati i distribuirati pod uslovima licence. - Dobro dokumentovan. - Podržan: Nmap nema garanciju, ali, dobro ga podržava zajednica programera i korisnika. - Nagrađivan: Nmap je osvojio brojne nagrade. - Popularan: Uključen je u mnoge operativne sisteme (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, itd.).	https://www.magnetforensics.com/free-tool-encrypted-disk-detector/
3	**Volatility Framework**	Volatility Framework je platforma objavljena od strane Black Hat-a. Neposredno se odnosi na Advance Memory Analysis & Forensics. Advance Memory Analysis & Forensics u osnovi analiziraju RAM memoriju žrtvinog računara. Ova memorija je nestabilna i njen se sadržaj može promeniti samim startovanjem računara. Analiza ovih podataka se može izvršiti upotrebom Volatility Framework-a. Ovaj okvir je omogućio praćenje procesa rada i stanja bilo kog sistema korišćenjem podataka pronađenih u RAM-u. On takođe omogućava jedinstvenu platformu za forenzička istraživanja u u cilju povećanja efikasnosti. Njega koriste policijski organi, odbrambene snage, ali i komercijalni istražitelji širom sveta	- Jedinstveni, kohezioni okvir - To je Open Source GPLv2 - Napisan je u Pitonu (Python) - Pokreće Windows, Linux ili Mac - Proširiv i podržava API skripte - Odlični kompleti funkcija zasnovani na reversnom inženjerstvu i specijalizovanim istraživanjima - Sveobuhvatna pokrivenost formata datoteka - Brzi i efikasni algoritmi - Ozbiljna i moćna zajednica - Forenzički/IR/malver fokusiran	https://www.darknet.org.uk/2016/09/volatility-framework-advanced-memory-forensics-framework/
4	**Sleuth Kit (+Autopsy)**	The Sleuth Kit (+Autopsy) podržava interfejs baziran na komandnoj liniji. Korisnici/klijenti izdaju komande programskom programu uzastopnim redovima teksta, na isti način kao komande u programskom jeziku. Sleuth Kit omogućava korisnicima da ispituju imidže žrtvinih diskova i da oporavljaju oštećene datoteke. Obično se koristi u Autopsy zajedno sa mnogim drugim "Open Source" ili komercijalnim	- Multi-User rad: zajednički rad više forenzičara u složenijim slučajevima. - Analiza vremenske linije: Prikazuje sistemske događaje u grafičkom interfejsu kako bi se identifikovala aktivnost. - Pretraživanje ključnih reči: ekstrakcija teksta i indeksirani pretraživači omogućavaju pronalaženje datoteka u kojima se pominju specificirani izrazi.	https://www.sleuthkit.org/

R.Br.	Naziv alata	Opis	Osnovne karakteristike	URL
		alatima. Autopsy® zajedno sa Sleuthkit-om je program baziran na GUI-u. Omogućava korisniku da ispituje hard diskove i pametne telefone sa boljom efikasnošću od drugih alata.	- Veb artefakti: Ekstrakcija veb aktivnost iz uobičajenih pretraživača kako bi se identifikovala korisnikova aktivnost. - Analiza registra: koristi RegRipper za identifikaciju nedavno posećenih dokumenata i USB uređaja. - LNK fajl analiza: Identifikuje prečice i dokumenta kojima je pristupljeno. - Analiza elektronske pošte: analizira poruke MBOX formata, kao što je Thunderbird. - EXIF: Ekstrakcija geolokacija i informacije o kameri iz JPEG datoteka. - Sortiranje datoteka po tipovima: Grupisanje datoteka po tipovima za pronalaženje svih slika ili dokumenata. - Media plejbek: omogućava pregled video zapisa i slika u aplikaciji bez spoljnih pregledača. - Thumbnail pregledač: Prikazuje sličice slika za brzi pregled slika.	
5	**Caine (Computer Aided Investigative Environment)**	CAINE (Computer Aided INvestigative Environment Live USB/CD/DVD) je izgrađen na Linuks okruženju. To je u stvari Live CD sa nizom forenzičkih alata. S obzirom da je najnovija verzija CAINE izgrađena na Ubuntu Linux LTS, MATE i LightDM, svako ko je upoznat sa njima ne mora da ulaže dopunske napore da bi mogao da koristi CAINE.	- CAINE Interface – korisnički interfejs koji okuplja neke dobro poznate forenzičke alate, od kojih su mnogi otvorenog koda. - Ažurirano i optimizirano okruženje za vođenje forenzičke analize. - Poluautomatski generator izveštaja.	https://www.caine-live.net/
6	**Xplico**	Xplico je Open Source mrežni forenzički alat koji može rekonstruisati sadržaj bilo kojih akvizicija izvršenih od strane sniffera za pakete, kao što su Wireshark, ettercap itd. Ovaj alat može izvući i rekonstruisati sadržaj sa bilo kog mesta. Xplico je podrazumevano instaliran u nekim od digitalnih forenzika i testiranja penetracije operativnih sistema Kali Linux, BackTrack i drugim.	- Podržani protokoli: HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IPv4, IPv6. - Port Independent Protocol Identification (PIPI) za svaki protokol aplikacije. - Multithreading - tehnika pomoću kojeg jedan set koda može koristiti nekoliko procesora u različitim fazama izvršenja. - Izlazni podaci i informacije u SQLite bazi podataka ili MySQL bazi podataka i/ili datotekama. - Svakom podatku koji je Xplico ponovo sklopio asocirana je XML datoteka koja jednoznačno identifikuje tokove i pcap koji sadrži ponovno sastavljene podatke. - Nema ograničenja veličine podataka za unos ili broja ulaznih datoteka (jedina granica je veličina HD). - Modularnost. Svaka Xplico komponenta je modularna.	https://www.xplico.org/
7	**X-Ways Forensics**	X-Ways Forensics je napredno radno okruženje koje forenzičari masovno koriste. Jedan od problema sa kojim se suočava stručnjak pri korišćenju nekog forenzičkog alata jeste nedostatak resursa, spor rad, nemogućnost da se dođe do svih lokacija sa podacima. Toga kod X-Ways nema. Ovaj forenzički alat je jednostavan i potpuno prenosiv i može se	- Kloniranje diska i izrada imidž datoteka. - Mogućnost čitanja strukture particioniranja i strukture fajl sistema u sirovim (.dd) imidž datotekama, ISO, VHD i VMDK imidžima. - Potpuni pristup diskovima, RAID-u i imidžima veličine veće od 2TB.	http://www.x-ways.net/forensics/

R.Br.	Naziv alata	Opis	Osnovne karakteristike	URL
		nositi na USB memorijskom elementu. Ne zahteva nikakvu dodatnu instalaciju na Windows sistemima.	- Automatska identifikacija izgubljenih/izbrisanih particija. - Pregled i izmena binarnih struktura podataka pomoću šablona. - Rekurzivan pregled svih postojećih i izbrisanih datoteka u svim poddirektorijima.	
8	**Bulk Extractor**	Bulk_extractor skenira sliku diska, datoteku ili direktorijum datoteka i izvlači korisne informacije ne obraćajući pažnju na strukturu datotečnog sistema. Na taj način dobija u brzini rada i u mogućnosti da paralelno obrađuje različite delove diska. U praksi, program deli disk na stranice i obrađuje jednu stranicu na svakom dostupnom jezgru. To znači da mašine sa više jezgara obrađuju disk približno toliko puta brže koliko imaju jezgara u poređenju sa mašinama sa jednim jezgrom (Garfinkel, 2013). Bulk_ektractor je takođe temeljan. Testiranje je pokazalo da postoji značajna količina komprimiranih podataka u nedodeljenim područjima datotečnog sistema koju propusti većina danas korišćenih forenzičkih alata, ali ne i bulk_extractor. Još jedna od prednosti je što se može koristiti za obradu praktično svakog digitalnog medijuma. Za pregled rezultata poseduje automatizovane alate.	Bulk_extractor - je alat za forenziku podataka na disku. Skenira medije i izdvaja prepoznatljive sadržaje. - deli disk na 16M "stranice" (blokove) i obrađuje svaku stranicu nezavisno. - ispituje svaki bajt da vidi da li je to početak "kodiranog" regiona. - ima tri faze rada: ekstrakcija; stvaranje histograma; naknadna obrada. - pokreće se iz komandne linije i kreira direktorijum "funkcionalnih datoteka" i rezultata. - GUI radi na Windows, Mac i Linux operativnim sistemima.	http://www.softpedia.com/get/Compression-tools/Bulk-Extractor.shtml
9	**Mandiat Redline**	RedLine je popularan alat za analizu memorije i datoteka, a prikuplja informacije o procesima koji se odvijaju na hostu i upravljačkim programima iz memorije, i druge podatke kao što su meta podaci, podaci iz registara, zadaci, usluge, informacije o mreži i Internet istorija kako bi se kreirali odgovarajući izveštaji. Redline®, FireEie-ova besplatna sigurnosna alatka, pomoću analize memorije i datoteka, pruža korisnicima istraživačke mogućnosti pri traženju znakova zlonamerne aktivnosti i izradi profila procene pretnji.	- Temeljno vrši reviziju i prikuplja sve programe i upravljačke programe iz memorije, meta podatke datotečnog sistema, podatke iz registra, evidencije događaja, informacije o mreži, usluge, zadatke i veb istoriju. Analizira i prikazuje uvezene podatke o reviziji, uključujući i mogućnost filtriranja rezultata oko datog vremenskog okvira. - Ubrzava analizu memorije dokaznim alatima za analizu malvera zasnovano na relativnom prioritetu. - Izvodi IOC (Indicators of Compromise) analize. - Snabdeven setom IOC-ova, Redline Portable Agent se automatski konfiguriše da prikupi podatke potrebne za izvođenje i prikaz rezultata IOC analize.	https://www.mandiant.com/resources/download/redline
10	**Linux 'DD'**	DD dolazi podrazumevano uz većinu danas dostupnih Linux distribucija (npr. Ubuntu, Fedora). Ovaj alat može se koristiti za različite forenzičke zadatke kao što su forenzičko brisanje diskova i stvaranje sirovog imidža diska. DD je veoma moćan alat koji može imati razorne efekte ako se ne koristi sa pažnjom. Modifikovana „dd“ verzija 'dc3dd' uključuje i funkcije koje su dodate posebno za zadatke digitalne forenzičke nabavke.	DC3DD predstavlja dodatak GNU dd programa. Ova verzija ima nekoliko funkcija namenjenih forenzičkoj akviziciji podataka. Najznačajniji dopunski sadržaji uključuju: Prikupljanje digitalnih dokaza "hashing on-the-fly", deljenje izlaznih datoteka, šablone za pisanje izveštaja, merač napredovanja i verifikaciju datoteka.	https://sourceforge.net/projects/dc3dd/

3 ZAKLJUČAK

Računarska ili digitalna forenzika, iako mlada grana, zahvaljujući ubrzanom razvoju informacionih tehnologija i softvera i hardvera poslednjih godina dobija veliki zamah u svom razvoju. Posebno veliki pomak se očekuje sa masovnom primenom Interneta stvari (IoT). Svaki korisnik računara se nebrojeno puta našao u situaciji da preuzima ulogu IT forenzičara, bilo da traži zagubljeni dokument ili fotografiju na hard disku ili u svoj arhivi, bilo da traži razlog neregularnog rada svog računara. Navedene situacije koje se mogu rešiti upotrebom alata korišćenog operativnog sistema, iako brojne, samo su mali deo ukupnih potreba. Na nivou sudskih IT veštaka zadaci su kompleksniji i odgovorniji. Sudski IT veštaci imaju zadatak da otkrivaju i opisuju informacije sadržane na digitalnom artefaktu ili njihovom stanju ili postojanju pri čemu digitalni artefakti uključuju mobilne telefone, računarske mreže, računarske sisteme, hard diskove, DVD- i CD-ove i druge uređaje za skladištenje podataka, kao i elektronska dokumenta i datoteke poput e-pošte, JPEG ili PNG slika, PDF dokumenata, itd. Za takve aktivnosti su neophodni i odgovarajuća stručnost i odgovarajući alati. Logično je očekivati da komercijalni programi pružaju veće forenzičke mogućnosti, da su pouzdaniji i da pružaju garanciju kvaliteta. S druge strane, takvi programi su relativno glomazni, skupi i neisplativi većini korisnika, razvija ih ograničen broj eksperata, a iako korisnik očekuje garanciju, dobija garanciju za kupljeni softver, ali ne i garanciju za rezultate rada kupljenog softvera. Za rešavanje većine forenzičkih zadataka vrlo uspešno se nametnula mogućnost korišćenja besplatnih forenzičkih alata. Besplatni forenzički alati su svakim danom sve brojniji i bogatije opremljeni, sposobni da urade najširi spektar zadataka, čak se i ugrađuju kao podrazumevane komponente pojedinih operativnih sistema, a koristi ih i usavršava brojna korisnička zajednica. Za svaku od aktivnosti može se naći jedan ili više odgovarajućih alata čijom se upotrebom ili paralelnom upotrebom može uspešno doći do rezultata.

Iako su mu na raspolaganju brojni alati, IT veštak ima veoma težak zadatak u svom radu. Većina digitalnih dokaza se nalazi tamo gde im je teško prići. U prvom redu se tu misli na privremene datoteke i privremene memorije, kao i na obrisane datoteke bilo da su one poruke elektronske pošte, dokumenta u najrazličitijim formatima ili obrisane particije diska. Sami počinioci zlonamernih aktivnosti pokušavaju da zametnu tragove. Da zadatak forenzičara bude teži dopunski „se trude“ sam operativni sistem i njegovi alati. Da bi olakšao rad korisniku operativni sistem se širi po memoriji, masovno generiše nove i pamti stare podatke prepisujući nove preko starih zapisa uništavajući dokaze. Zato se sa dobrom dozom sigurnosti može reći da se najkvalitetniji dokazi nalaze u oblastima koje su nedostupne standardnim alatima operativnog sistema.

Na osnovu trendova u razvoju računara i opreme može se reći da će do rasta potrebe za forenzičarima i forenzičkim alatima doći rastom upotrebe Interneta stvari. Pored nesumnjivih blagodeti primene ove tehnologije, pojaviće se i niz novih slabih tačaka koje treba štititi od napada ili istraživati posledice napada i pronalaziti izvršioce.

CITIRANA DELA

Breach Level Index. (2018, avgust 17). *Data Breach Statistics*. Preuzeto sa Breach level index: https://breachlevelindex.com/

Cole, B. (2012, juni). *Computer Fraud and Abuse Act (CFAA).* Preuzeto sa TechTarget: https://searchcompliance.techtarget.com/definition/The-Computer-Fraud-and-Abuse-Act-CFAA

Computer Misuse Act. (1990). Preuzeto sa legislation.gov.uk: https://www.legislation.gov.uk/ukpga/1990/18/contents

Garfinkel, S. L. (2013). Digital media triage with bulk data analysis and bulk_extractor. *Computers & Security*(32), 56-72.

ISO/IEC 17025. (2005). *General requirements for the competence of testing and calibration laboratories.* ISO.

n.d. (2018, mart). *Forensic Software: Everything You Need to Know About Computer Forensics*. Preuzeto sa Disk Drill: https://www.cleverfiles.com/howto/computer-forensic.html

Norman, J. (1978, maj 30). *Probably the First U. S. Legislation against Computer Crimes (1978).* Preuzeto sa HistoryofInformation: http://www.historyofinformation.com/expanded.php?id=3888

NSRS. (2005). Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala. *Sl. glasnik RS*(61).

Shankdhar, P. (2018, mart 26). *22 Popular Computer Forensics Tools [Updated For 2018]*. Preuzeto sa Infosec Institute: https://resources.infosecinstitute.com/computer-forensics-tools/

Smith, S. (2015, maj 12). *Cybercrime will Cost Businesses Over $2 Trillion by 2019*. Preuzeto sa Juniper research: https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

Stephenson, P. (2017, oktobar 02). *It's forensic tools time again*. Preuzeto sa SC Magazine: https://www.scmagazine.com/its-forensic-tools-time-again/article/696487/

SWGDE. (2004). *SWGDE Best Practices for Computer Forensics.* Washington DC: SWGDE.

Techopedia. (2016, Sep 14). *Digital Forensics.* Preuzeto sa techopedia: https://www.techopedia.com/definition/27805/digital-forensics

Datum prve prijave: 27.08.2018.
Datum prijema korigovanog članka: 20.11.2018.
Datum prihvatanja članka: 27.03.2019.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Čekerevac, Z., Dvorak, Z., & Prigoda, L. (2019, 04 15). Savremena računarska forenzika i forenzički alati. (Z. Čekerevac, Ur.) *FBIM Transactions, 7*(1), 50-60. doi:10.12709/fbim.07.07.01.06

*Style – **Chicago** Sixteenth Edition:*

Čekerevac, Zoran, Zdenek Dvorak, i Lyudmila Prigoda. 2019. „Savremena računarska forenzika i forenzički alati.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 50-60. doi:10.12709/fbim.07.07.01.06.

*Style – **GOST** Name Sort:*

Čekerevac Zoran, Dvorak Zdenek i Prigoda Lyudmila Savremena računarska forenzika i forenzički alati [Časopis] // FBIM Transactions / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 50-60.

*Style – **Harvard** Anglia:*

Čekerevac, Z., Dvorak, Z. & Prigoda, L., 2019. Savremena računarska forenzika i forenzički alati. *FBIM Transactions,* 15 04, 7(1), pp. 50-60.

Style – **ISO 690** Numerical Reference:

Savremena računarska forenzika i forenzički alati. **Čekerevac, Zoran, Dvorak, Zdenek i Prigoda, Lyudmila.** [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, FBIM Transactions, T. 7, str. 50-60.