Digitalna forenzika

Šeruga, Dona

Master's thesis / Diplomski rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, University of Zagreb, Faculty of Humanities and Social Sciences / Sveučilište u Zagrebu, Filozofski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:131:825262

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
SMJER INFORMATIKA (ISTRAŽIVAČKA)
Ak. god. 2019./2020.

Dona Šeruga

Digitalna forenzika

Diplomski rad

Mentor: prof.dr.sc. Krešimir Pavlina

Zagreb, rujan 2020.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Dona Šeruga
(potpis)

Prije svega zahvaljujem se mentoru, prof. dr. sc. Krešimiru Pavlini na savjetima i smjernicama koje mi je dao tijekom izrade ovog rada te na iskazanom povjerenju i volji.

Zahvaljujem se i profesorima s Odsjeka za informacijske i komunikacijske znanosti Filozofskog fakulteta u Zagrebu na prenesenom znanju i vještinama koje sam stekla tijekom studija.

Također, zahvaljujem se kolegama i prijateljima koji su uvijek bili uz mene, bez kojih godine studiranja ne bi bile iste.

I za kraj, posebno se zahvaljujem svojoj obitelji na neizmjernoj podršci i razumijevanju kroz cijelo obrazovanje.

Sadržaj

1. Uvod

Društvene mreže, pametni uređaji, umjetna inteligencija, kriptovalute – prije dvadesetak godina bez svega toga se moglo živjeti, a danas je to naša svakodnevica. Podaci su jezgra tih koncepata, a informacije proizašle iz tih podataka su veoma vrijedne. Svijet se nekoć temeljio na ratovima, onim fizičkim, a danas smo svjedoci novih vrsta ratova – onih u digitalnom svijetu. Na tržištu se ratuje informacijama, a terorizam je dobio novi oblik – kibernetički. Broj napada svakim danom raste, a da toga nismo ni svjesni. Više se bojimo za podatke, slike, brojeve, poruke nego za nešto materijalno, poput uređaja. Tim Berners-Lee je jednom izjavio: „Podaci su ono što nam je vrijedno i opstat će duže nego sami sustavi.“ Ipak, nećemo uvijek sami sudjelovati u životnom vijeku naših podataka. Možemo ih čuvati, kopirati, napraviti sigurnosne kopije, ali to jednom neće biti dovoljno. Naići će netko s crnim šeširom i podaci, za koje smo mislili da su sigurni, će nestati.

Iz tog razloga, potrebna je digitalna forenzika - zanimanje koja će nam osigurati izgubljene podatke i otkriti krivca, odnosno zločinca. Za svaki kibernetički napad, zločin ili prijetnju postoji forenzičar koji će provesti digitalnu istragu, ali i za svakog forenzičara postoje protumjere koja otežavaju istragu. Koristeći alate, hardverske i softverske prirode, digitalni forenzičar u nekoliko koraka obavlja samu istragu, a pri tome upotrebljava različite tehnike i metode. Digitalni dokazi su temelj istrage te ih je potrebno detaljno i pažljivo analizirati. Kako bi postao uspješan u svojoj karijeri, budući digitalni forenzičar bi trebao proći formalno ili neformalno obrazovanje, kako bi dobio teorijska znanja i praktične vještine koje će kasnije moći koristiti. Pored svega toga, digitalna forenzika je u bliskom odnosu s pravom, pa je potrebno poznavati zakone i druge regulative te legislative. U Hrvatskoj se digitalna forenzika tek razvija, ali trenutno stanje predviđa svijetlu budućnost.

2. Računalna sigurnost i kibernetički kriminal

Čovječanstvo se suočilo s velikim brojem ratova, bolesti i prirodnim katastrofama, ali to nisu jedine prijetnje koje čovjeku ugrožavaju osjećaj sigurnosti. Pojavom Interneta, javljaju se i nove vrste prijetnji – one u digitalnom svijetu. Kibernetička prijetnja (eng. *cyberthreat*) je mogućnost iskorištavanja ranjivosti u svrhu napada na računalo, računalni sustav ili mrežu.[1] Kako bi se osigurali od tih prijetnji i napada, potrebno je poznavati osnove računalne sigurnosti. Računalna sigurnost (eng.*computer security)* je definirana kao mogućnost zaštite računalnih sustava i informacija od štete, krađe i neovlaštenih pristupa. To je proces sprječavanja i otkrivanja neovlaštenog pristupa na računalnom sustavu. Računalna sigurnost osigurava povjerljivost, integritet i dostupnost cjelokupnog računalnog sustava. Osim računalne sigurnosti, javljaju se i pojmovi informacijska sigurnost (eng.*information security*) i kibernetička sigurnost (eng.*cyber security*). Informacijska sigurnost je zaštita informacija od neovlaštenog pristupa, izmjene i brisanja, dok je kibernetička sigurnost zaštita računalnih sustava koji komuniciraju putem mreže.[2] Ugrožavanjem navedenih tipova sigurnosti javlja se nova vrsta zločina – kibernetički. Kibernetički zločin (eng.*cybercrime*) je vrsta zločina u kojem je računalo objekt napada ili se ono koristi u svrhu napada. Kibernetički zločinci (eng. *cybercriminals*) mogu koristiti računalne tehnologije kako bi pristupili osobnim podacima, poslovnim tajnama ili koristili Internet u zlonamjerne svrhe. Kibernetički zločin najčešće uključuje krađu bankovnih podataka, krađu identiteta ili neovlašteni pristup računalu. [3] Također, javlja se problematična vrsta kibernetičkog zločina, a to je kibernetički terorizam (eng.*cyberterrorism*). Kibernetički terorizam se odnosi na stvaranje prijetnji koje su namijenjene promjenama društvenog uređenja, zastrašivanju šire javnosti ili utjecaju na političko odlučivanje, zbog unapređenja političkih, vjerskih, rasnih ili ideoloških razloga, utjecajem na integritet, povjerljivost i/ili dostupnost informacija, informacijskih sustava i mreža ili neovlaštenim radnjama vezanim za nadzor informacijskih i komunikacijskih tehnologija fizičkih procesa u stvarnom svijetu.[4] Upravo zbog pojave ovakvih prijetnji i zločina, uspostavljaju se mnoge sigurnosne i zakonodavne ustanove.

---

[1] Cyberthreat. Techopedia. Dostupno na: https://www.techopedia.com/definition/25263/cyberthreat (28.03.2020)

[2] Choudary, A. What is Computer Security? Introduction to Computer Security. Edureka! Dostupno na: https://www.edureka.co/blog/what-is-computer-security/ (28.03.2020.)

[3] Cybercrime. Techopedia. Dostupno na: https://www.techopedia.com/definition/2387/cybercrime (28.03.2020.)

[4]Cyber Terrorism. CIPedia. Dostupno na: https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Cyber_Terrorism (28.03.2020.)

3. Digitalna forenzika

Digitalna forenzika dio je forenzične znanosti (eng. forensic science). Forenzika je primjena znanosti u rješavanju pravnih problema, odnosno integracija prava i znanosti.[5] U forenzici se primjenjuju znanosti poput toksikologije, psihologije, patologije, optometrije, lingvistike, geologije, inženjeringa, botanike, informatike i mnogih drugih koje zajedno predstavljaju poddiscipline same forenzike. Jedna od tih poddisciplina je digitalna forenzika.[6] Ponekad nazvana i računalnom te kibernetičkom forenzikom, digitalna forenzika podrazumijeva primjenu računalne znanosti i istraživačkih procedura u pravne svrhe, a uključuje analizu digitalnih dokaza prikupljenih nakon istrage i matematičkih potvrđivanja, korištenjem ispravnih alata, ponovljivosti, izvještaja i stručne prezentacije.

Osim prijenosnih i osobnih računala, digitalna forenzika istražuje i zločine počinjene nad mobilnim uređajima, mrežama i tehnologijama u oblaku. Također, analizira i fotografije, video i audio zapise u analognom i digitalnom obliku. Analiza se provodi zbog vjerodostojnosti, usporedbe i poboljšanja. Digitalna forenzika se koristi u različitim okruženjima, uključujući kaznene istrage, građanske parnice, obavještajne i administrativne poslove.[7] Bavi se i slučajevima poput krađe intelektualnog vlasništva, industrijske špijunaže, prijevare, zlouporabe Interneta i elektroničke pošte na radnom mjestu, raznim krivotvorenjima, stečajnim istragama i pitanjima usklađenosti s propisima.[8] Izazovi na koje nailazi uključuju povećanje broja uređaja i dostupnosti Interneta, lako dostupni alati za hakiranje, velike količine podataka za obradu i tehnološke promjene koje zahtijevaju ažuriranje ili promjene rješenja. Prednosti digitalne forenzike su osiguranje integriteta računalnog sustava, predočavanje dokaza na sudu, efikasnost pronalaženja zločinaca u cijelom svijetu, pomaže očuvati novčana i materijalna dobra neke organizacije i omogućuje prikupljanje, obradu i tumačenje činjeničnih dokaza potrebnih u pravnom postupku. Nedostaci korištenja digitalne forenzike su prihvaćanje digitalnih dokaza kao vjerodostojnih na sudu, bez ikakvih izmjena, izrada i pohrana elektroničkih zapisa je skupa, pravnici trebaju biti informatički pismeni te alati korišteni u istrazi moraju biti u skladu s određenim standardima kako bi bili prihvaćeni na sudu.

[5] Sammons, J. (2014). The Basics of Digital Forensics (2nd ed.). Syngress. (28.03.2020.)
[6] What is Forensics?. CrimeSceneInvestigatorEDU.org. Dostupno na: https://www.crimesceneinvestigatoredu.org/what-is-forensic-science/ (28.03.2020.)
[7] Sammons, J. (2014). The Basics of Digital Forensics (2nd ed.). Syngress. (28.03.2020.)
[8] What is Digital Forensics? History, Process, Types, Challenges. Guru99. Dostupno na: https://www.guru99.com/digital-forensics.html (28.03.2020.)

3.1. Povijest digitalne forenzike

Forenzika je znanost koja je prisutna preko sto godina, ali pojam digitalne forenzike javlja se tek 1980-ih, pojavom prvih osobnih računala i zlonamjernih programa. Neki od prvih alata korištenih u digitalnoj forenzici su bili razvijeni u laboratorijima Saveznog istražnog ureda (eng. *Federal Bureau of Investigation*) Sjedinjenih Američkih Država. Ondje je 1984. godine osnovan program magnetskih medija (eng. *Magnetic Media program*), koji je kasnije preimenovan u CART (eng. *Computer Analysis and Response Team*), a danas svima poznat kao CERT (eng. *Computer Emergency and Response Team*) ili CSIRT (eng. *Computer Security Incident Response Team*). CART je tada imao malu ulogu u istragama. Četiri godine kasnije, nastaje neprofitna organizacija IACIS (eng. *International Association of Computer Investigative Specialists*), koja se sastoji od računalnih stručnjaka koji podučavaju i treniraju buduće digitalne forenzičare, a 1995. godine formira se IOCE (eng. *International Organization on Computer Evidence*), kojoj se cilj približiti organizacije koje se aktivno bave digitalnim i multimedijskim dokazima zbog komunikacije i suradnje kako bi doprinijeli kvaliteti i konzistentnosti forenzičke zajednice.

Krajem 1990-ih, broj kibernetičkih zločina raste te države G8 objavljuju da zakonodavni službenici moraju biti trenirani i opremljeni kako bi se mogli baviti zločinima koji uključuju digitalne tehnologije, također uspostavljaju se i međunarodna načela, smjernice i procedure vezane za prikupljanje digitalnih dokaza. Prvi regionalni FBI laboratorij za digitalnu forenziku uspostavljen je 2000. godine u San Diegu.[9] Do danas polje digitalne forenzike se rapidno razvija, broj organizacija i konferencija raste, razvijaju se novi i bolji alati, a ovo polje neće ni prestati rasti budući da se promet na Internetu svakodnevno povećava, kao i broj zlonamjernih napada. Zbog tog razloga, potrebno je povećati svijest o kibernetičkim zločinima u cijelom svijetu, kako bi se pravni standardi i zakoni vezani za digitalne istrage počeli razvijati i primjenjivati.[10]

[9] Prasad, A., Pande, J. (2016). Digital Forensics. Uttarakhand Open University. (29.03.2020.)
[10] Pollitt, M. (2010). A History of Digital Forensics. Advances In Digital Forensics VI, 3-15. Dostupno na: https://doi.org/10.1007/978-3-642-15506-2_1 (29.03.2020.)

4. Podjela digitalne forenzike

Digitalna forenzika dijeli se u nekoliko grana, ovisno o uređaju ili sustavu koji prenosi digitalne dokaze ili o samom digitalnom dokazu. Tako postoji računalna forenzika, forenzika mobilnih uređaja, mrežna forenzika i forenzika baza podataka. Neke grane su manje razvijene ili su jednostavno poddiscipline većih grana, a to su forenzika medija za pohranu, forenzika zlonamjernih programa, forenzika elektroničke pošte, forenzika tehnologija u oblaku, *live* forenzika, forenzika društvenih mreža i forenzika interneta stvari. Nastankom novih različitih grana digitalne forenzike, razvija se i antiforenzika koja otežava pojedinu digitalnu istragu.

4.1. Računalna forenzika

Računalna forenzika često se miješa s digitalnom forenzikom, jer se pojam digitalno asocira s računalima. Računalna forenzika je zapravo identifikacija, očuvanje, prikupljanje, analiza i izvještavanje o dokazima koji su nađeni primarno na računalima, stolnim i prijenosnim te njihovim prijenosnim medijima u svrhu istrage i pravnih postupaka.[11] Ova znanost se smatra najstarijom granom digitalne forenzike te osim navedenih uređaja uključuje i memoriju računala, tvrde diskove, operacijske sustave i zapise (eng. *logs*), odnosno kompletnu periferiju i komponente računala. Jedan od glavnih poslova računalne forenzike je vraćanje obrisanih datoteka.[12] Računalni forenzičar se obvezuje pratiti procedure i pristupiti računalu žrtve kibernetičkog napada nakon slučaja, dizajnirati procedure na mjestu zločina kako bi osigurao legitimne, nekoruptirane dokaze, prikupiti podatke i kopirati ih te vratiti obrisane datoteke i particije kako bi iz njih izdvojio validne i relevantne dokaze. Također, mora pružiti smjernice za analiziranje samih dokaza i zapisa, proizvesti izvješće o cjelokupnoj istrazi koju je proveo, očuvati dokaze i predstaviti te dokaze na sudu kao stručni svjedok.[13] Neki od razloga za primjenu računalne forenzike su analiza računala optuženika, oporavak podataka u slučaja kvara računala, analiza računalnog sustava nakon napada i prikupljanje dokaza protiv zaposlenika za kojeg tvrtke smatraju da se bave ilegalnim aktivnostima.[14]

[11] Different types of digital forensics. Open Learn. Dostupno na: https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.3 (03.04.2020.)
[12] Categories of Digital Evidence. Infosec. Dostupno na: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/ (03.04.2020.)
[13] Prasad, A., Pande, J. (2016). Digital Forensics. Uttarakhand Open University. (03.04.2020.)
[14] Računalna forenzika. Nacionalni CERT. Dostupno na: https://www.cert.hr/racunalna-forenzika/ (03.04.2020.)

4.2. Forenzika mobilnih uređaja

Mobilni uređaju su nešto o čemu danas svi ovisimo. Koristimo ih svakodnevno, u raznolike svrhe. Dvije stavke definiraju mobilne uređaje, a to su mobilnost i povezanost na Internet. Oni moraju biti lagani, prenosivi i kompaktni. Mobilni uređaji mogu biti povezani na Internet bežičnom mrežom, mrežom pružatelja mobilne usluge ili lokalnom mrežom (eng. *Local Area Network*) te je bitno da imaju mogućnost komunikacije. Zbog svih današnjih mogućnosti, mobilni uređaje se nazivaju ručnim računalima. Evolucija mobilnih uređaja krenula je od prvih dlanovnika (eng. *Personal Digital Assistant*), preko tableta i GPS-a (eng. *Global Positioning System*), mobilnih telefona, odnosno današnjih pametnih telefona[15] pa do nekolicine uređaja u svijetu Internet stvari (eng. *Internet of Things*). Neki od tih uređaja su pametni satovi, narukvice i dronovi, ali i uređaji poput pametnih televizora, mikrovalnih pećnica i frižidera.. Neke od tih inovacija nemaju aspekt mobilnosti, ali su povezani, pa ih zato možemo shvatiti kao mobilne uređaje.

Pametni telefoni se smatraju telefonima s fiksnim sposobnostima, ali s mogućnošću preuzimanja dodatnih aplikacija u svrhu proširenja funkcionalnosti uređaja. Potreba za forenzikom mobilnih uređaja se javlja naglim rastom korisnika pametnih telefona, ali i mobilnih telefona općenito. Ove godine broj korisnika mobilnih telefona u svijetu, uključujući i pametne telefone, iznosi 4,78 milijardi.[16] Mobilni uređaji mogu sadržavati osobne podatke korisnika, poslovne tajne, ali i dokaze zločina, pa se iz tog razloga pojavljuje forenzika mobilnih uređaja. Izazovi kod mobilnih uređaja su različite inačice operacijskih sustava, nestandardizirane funkcionalnosti pohrane podataka, različita sučelja za povezivanje na uređaj i masovna proizvodnja novih uređaja. Izazovi forenzike mobilnih uređaja uključuju nestandardiziranost procedura i prikupljanja dokaza, nemogućnost forenzičkih alata da prikupe sve podatke, nepostojanje alata za sve mobilne uređaje, različitost kabela i priključaka te problem znakova u jeziku koji nisu po ASCII standardu (eng. *American Standard Code for Information Interchange*). Aplikacije također stvaraju problem za forenzičare. Broj aplikacija se konstantno povećava, postoje različite inačice aplikacije i svako ažuriranje donosi neke promjene. Podaci koji se mogu prikupiti s mobilnih telefona su zapisi poziva, SMS i MMS poruke, kontakti, slike te video i audio zapisi. Dodatni podaci se mogu prikupiti s pametnih telefona, a to su aplikacije za: dopisivanje, elektroničku poštu,

[15] Mobile Device. Techopedia. Preuzeto sa: https://www.techopedia.com/definition/23586/mobile-device (04.04.2020.)
[16] How Many Smartphones Are In The World? BankMyCell. Dostupno na: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world (04.04.2020.)

društvene mreže, navigacijske usluge i geolokaciju, video igre, financijske aplikacije i podaci o trgovini, knjige i usluge u oblaku. Pitanja koja se postavljaju su: koje podatke je bitno prikupiti, koji je profil korisnika koji se istražuje i treba li uzeti u obzir druge povezane uređaje.

Proces forenzike mobilnih uređaja ima tri koraka: zapljena, prikupljanje i analiza. U pravnom smislu zapljena mobilnih uređaja je jednaka zapljeni ostalih digitalnih uređaja. Mobilni uređaji su uglavnom zaplijenjeni dok su upaljeni te zbog očuvanja dokaza transportiraju se u istom stanju kakvom su nađeni. Problem kod upaljenih uređaja je što su i dalje spojeni na mrežu te tako omogućavaju prepisivanje (eng. *overwrite*) starih podataka i dokaza. Kako bi se to spriječilo, mobilni uređaj se prenosi u Faraday vreći ili kavezu. Ova metoda onemogućava korištenje mobilnog uređaja, odnosno korištenje njegovog zaslona na dodir (eng. *touch screen*) i tipkovnice. Drugi nedostatak ove metode je to što će mobilni uređaj pokušavati uspostaviti povezanost na mrežu te će to dovesti do pražnjenja baterije. Preporučuje se da se uređaj stavi u zrakoplovni način ili da se klonira njegova SIM kartica (eng. *subscriber identity module card*). Drugi korak je prikupljanje dokaza s mobilnog uređaja, koje se uglavnom izvodi na upaljenim uređajima. Prikupljanje se odnosi na prikupljanje informacija o mobilnoj mreži, podataka o proizvođaču (serijski brojevi, kodovi proizvodnje) i karakteristikama mobilnog uređaja (operacijski sustav, metode za bežični pristup, aplikacije, poruke). Zadnji korak procesa je analiza, koja uključuju tehničko ispitivanje uređaja i prikupljanje podataka s istih. Podaci se prikupljaju sa SIM kartica, memorijskih kartica i sa samog uređaja. Analiza se može vršiti na velikom broju vrsta podataka – tekstualnim (poruke), grafičkim (slike), audio-vizualnim (video) i audio podacima (zvučni zapisi). Pojavom pametnih telefona broj podataka na uređajima se iznimno povećao. Forenzičari danas mogu analizom mobilnog uređaja osuditi zločinca samo na temelju dokaza koje su prikupili na uređaju. Unutarnja i vanjska memorija te zapisi poziva i poruka mogu se analizirati kako bi se stekao uvid u aktivnosti korisnika uređaja te saznati s kim je korisnik komunicirao.[17] Potreba za forenzičarima mobilnih uređaja itekako postoji, baš iz tog razloga što takvi mali uređaji nose tolike količine informacija i podataka.

[17] Prasad, A., Pande, J. (2016). Digital Forensics. Uttarakhand Open University. (04.04.2020.)

4.3. Mrežna forenzika

Pojavom Interneta i napada na mrežu, nastaje i mrežna forenzika kao jedna od najbitnijih i najpotrebnijih grana digitalne forenzike. Mrežna forenzike se odnosi na istraživanje i analiziranje informacija o mreži ili događaja na mreži, kako bi se otkrio izvor sigurnosnih napada ili incidenata.[18] Većina današnjih računalnih napada događa se na mreži. Žrtve mrežnih napada uključuju vladu, elektrane, financijske i zdravstvene ustanove, podatkovne centre, a prijetnje su terorističke organizacije i individualci. Za razliku od drugih grana, mrežna forenzika je kompleksnija jer se dokazi, koji su potrebni u istragama, mogu podijeliti kroz velik broj uređaja, ali i, geografski gledano, cijelim svijetom. Drugi izazov mrežne forenzike je veličina podataka koja, ovisno o veličini mreže organizacije, može biti nemoguća za prikupiti.[19] Iako nije moguće snimiti sve podatke koji prolaze kroz mrežu, posao mrežnog forenzičara je izdvojiti one bitne koji mogu služiti kao dokazi, spremiti njihove sigurnosne kopije kako bi ih se kasnije moglo obraditi i analizirati.

Mrežni forenzičar mora poznavati OSI (eng. *Open System Interconnection*) i TCP/IP (eng. *Transmission Control Protocol/Internet Protocol*) modele računalnih mreža, druge mrežne protokole i mrežne komponente. Metode mrežne forenzike variraju, pa ih stručnjaci dijele u dvije kategorije: „uhvati ono što možeš“ (eng. *catch-it-as-you-can*) i „stani, gledaj i slušaj“ (eng. *stop, look and listen*). „*Catch-it-as-you-can*“ je metoda zapisivanja svih paketa koji prolaze kroz određenu mrežu i naknadna analiza tih paketa. Ova metoda zahtjeva više prostora za pohranu. „*Stop, look and listen*“ je metoda zapisivanja svakog paketa posebno, gdje se samo određeni podaci pohranjuju za buduću analizu. Ovaj pristup zahtjeva manje prostora za pohranu, ali potreban je jači procesor kako bi se mogao nastaviti pratiti dolazni promet.[20]

Mrežna forenzika odnosi se na prikupljanje i analizu onih dokaza koji su rezultat komunikacije na mreži. Neki od mrežnih dokaza su elektronička pošta, IM sesije (eng. *instant messaging session*), aktivnosti, kolačići i povijest preglednika te zapisnici paketa. Izvori mrežnih dokaza mogu biti bežične pristupne točke (eng. *wireless access point*), mrežni usmjernici (eng. *router*) i centralni poslužitelji. Prikupljanje mrežnih dokaza je veliki izazov

[18] Network Forensics. Techopedia. Dostupno na: https://www.techopedia.com/definition/16122/network-forensics (05.04.2020.)
[19] Sammons, J. (2014). The Basics of Digital Forensics (2nd ed.). Syngress. (05.04.2020.)
[20] Network Forensics. Search Security. Dostupno na: https://searchsecurity.techtarget.com/definition/network-forensics (05.04.2020.)

zbog lociranja samih dokaza, sadržaja dokaza, privatnosti podataka, zbrinjavanja uređaja bez ispada na mreži i prihvatljivosti standarda u zakonima pravnog sustava.[21]

4.4. Forenzika baza podataka

Baze podataka su organizirani skupovi podataka kojima je lako pristupiti i koje je moguće izmjenjivati, brisati i ažurirati. Organizacije koriste baze podataka za pohranu, upravljanje i prikupljanje podataka iz baze. Kako bi se moglo pristupiti bazi podataka, danas se koriste mnogi sustavi za upravljanje bazama podataka (eng. *database management system*).[22] Baze podataka su bitna komponenta većine tvrtki i organizacija te je potrebno ostvariti visoku razinu sigurnosti same baze, jer jedan kibernetički napad može ugroziti poslovanje cijele tvrtke. Napadi na baze i krađe podataka postaju učestaliji te je stoga potrebna intervencija digitalnog forenzičara specijaliziranog za baze podataka.

Forenzika baza podataka je polje digitalne forenzike koje se fokusira na detaljnu analizu baze podataka, uključujući njezinog sadržaja, zapisnika, metapodataka i podataka ovisno o vrsti baze.[23] Forenzičari baze podataka bave se sljedećim problemima: prestanak rada baze podataka, brisanje podataka iz baze podataka, nedosljednosti u bazi podataka i otkrivanje sumnjivih radnji korisnika. Kako se podaci ne bi ugrozili, forenzičari će koristiti bazu podataka dostupnu samo za čitanje (eng. *read-only database*) ili identičnu kopiju baze podataka, koju će detaljno analizirati. Zatim je potrebno rekonstruirati podatke i zapise koji nedostaju, ako je došlo do brisanja tih podataka. Nakon toga će forenzičar dešifrirati podatke i utvrditi moguće uzroke kvara. Također, provjerit će aktivnosti korisnika i izolirat će sumnjive i ilegalne radnje. Forenzičari baza podataka koriste dvije metode u svojim istragama: dobavljanje zapisa (eng. *record carving*) i obnavljanje baze podataka (eng. *database reconstruction*). Dobavljanje zapisa je proces prikupljanja valjanih redaka podataka iz oštećene ili koruptirane baze podataka. Ovaj proces zahtjeva suvremene alate koji omogućuju rekonstrukciju podataka koji se nalaze u metapodacima baze. Obnavljanje baze podataka je proces u kojem forenzičar pokušava popraviti bazu u tolikoj mjeri da može izvući

[21] Davidoff, S., Ham, J. (2012). Network forensics: Tracking Hackers through Cyberspace. Upper Saddle River, New Jersey: Prentice Hall. (07.04.2020.)
[22] Database (DB). Techopedia. Dostupno na: https://www.techopedia.com/definition/1185/database-db (10.04.2020.)
[23] Chopade, R., & Pachghare, V. (2019). Ten years of critical review on database forensics research. Digital Investigation, 29, 180-197. Dostupno na: https://doi.org/10.1016/j.diin.2019.04.001 (10.04.2020.)

osnovne informacije iz nje. To je moguće analiziranjem zapisnih datoteka (eng. *log files*) baze i korištenjem algoritma koji omogućuje vraćanje zapisa u prošlo stanje.[24]

4.5. Ostale grane digitalne forenzike

Osim osnovnih grana digitalne forenzike, postoje još i grane koje se koriste rjeđe ili se njihove metode istrage već koriste u osnovnim granama. Forenzika medija za pohranu (eng. *disk forensics*) je grana digitalne forenzike koja se bavi prikupljanjem podataka s medija za pohranu, pretraživanjem aktivnih, izmijenjenih ili obrisanih datoteka.[25] Mediji za pohranu podataka se odnose na tvrde i SSD (eng. *solid state drive*) diskove, memorijske kartice, *flash drive,* poslužitelje i USB (eng. *Universal Serial Bus*) memorije. Metode koje se koriste u ovoj grani digitalne forenzike su obrada i analiza diska, metapodataka, datoteka i mapa, skrivenih i obrisanih datoteka i mapa te zapisnika (eng. *registry logs*).[26]

Forenzika zlonamjernih programa (eng. *malware forensics*) je grana digitalne forenzike koja se bavi identifikacijom i analizom zlonamjernog koda, virusa, Trojanskih konja i crva. Forenzičari moraju znati prepoznati i razlikovati adware, spyware, viruse, crve, trojanske konje, *rootkitove, backdoor* programe, *keyloggere*, *browser hijackere* i ransomware. Analiza zlonamjernih programa može biti statična ili dinamična. Statična analiza zlonamjernih programa je proces pretraživanja datoteka bez praćenja uputa, u kojoj se može otkriti je li program zlonamjeran i koje su njegove funkcionalnosti. Ova metoda je jednostavna i brza, ali nije korisna kod sofisticiranih zlonamjernih programa. Dinamična analiza zlonamjernih programa je proces pokretanja zlonamjernog programa kako bi se analizirale aktivnosti i funkcionalnosti programa.[27]

Forenzika elektroničke pošte (eng. *e-mail forensics*) se bavi oporavljanjem i analizom elektroničke pošte, uključujući obrisanu elektroničku poštu, kalendare i kontakte.[28] Pri tome se analiziraju zaglavlje, poslužitelji, mrežni uređaji, programi za slanje elektroničke pošte,

[24] What Is Database Forensics? Infosec. Dostupno na: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/application-forensics/overview-types-of-database-forensics/ (10.04.2020.)
[25] What is Digital Forensics? History, Process, Types, Challenges. Guru99. Dostupno na: https://www.guru99.com/digital-forensics.html (11.04.2020.)
[26] Disk Forensics. CyberImmersions. Dostupno na: https://www.cyberimmersions.com/digital-forensics/disk-forensics/ (11.04.2020.)
[27] Overview Of Malware Forensics. Infosec. Dostupno na: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/application-forensics/overview-of-malware-forensics/ (11.04.2020.)
[28] What is Digital Forensics? History, Process, Types, Challenges. Guru99. Dostupno na: https://www.guru99.com/digital-forensics.html (11.04.2020.)

otisci pošiljatelja te privitci.[29] Forenzika tehnologija u oblaku (eng. *cloud forensics*) je grana mrežne forenzike koja se bavi istragom kibernetičkih napada, kršenjem zakona i pravila te oporavljanjem podataka s tehnologija u oblaku. Izazovi s kojima se ovi forenzičari susreću su arhitektura oblaka, analiza podataka na oblaku, prikupljanje podataka, pravna pitanja i standardi.[30]

Live forenzika je grana digitalne forenzike koja se bavi analizom pokrenutih uređaja, kojoj je cilj prikupiti promjenjive podatke koje je moguće izgubiti ukoliko je uređaj ugašen. Promjenjivi podaci (eng. *volatile data*) su podaci koji su digitalno pohranjeni, a postoji vjerojatnost da će biti obrisani, prepisani ili promijenjeni u kratkom vremenu zbog interakcije čovjeka ili samog računala. Forenzičar mora znati prepoznati i razlikovati dvije vrste promjenjivih podataka: promjenjive podatke na fizičkom računalu poput otvorenih mrežnih veza, aktivnih procesa i usluga te privremenih memorija (eng. *cache*) i kratkotrajne, prolazne podatke (eng. *transient data*) koji nisu zapravo promjenjivi, ali im se može pristupiti samo na mjestu događaja.[31]

Forenzika društvenih mreža (eng. *social network forensics*) je grana digitalne forenzike koja je relativno mlada i nova. Digitalni dokazi koje je moguće prikupiti s društvenih mreža su od velike važnosti u pravnom sustavu jer mogu pružati ključne informacije o zločinu i osobi koja ga je počinila. Forenzika društvenih mreža se bavi prikupljanjem informacija s društvenih mreža, računalnim istraživanjem i analizom. Prikupljene informacije je potrebno pohraniti, analizirati i očuvati kako bi se mogle iskoristiti na sudu. Izazov je pronaći relevantne podatke u moru informacija, jer se oni, osim na društvenim mrežama mogu nalaziti na povezanim stranicama, blogovima i portalima. Najveći problem forenzike društvenih mreža je prikupiti dokaze bez kršenja zakona i uredbi, poput GDPR-a (eng. *General Data Protection Regulation*) i ToS-a (eng. *Terms of Service*). Također, teško je raditi s podacima i mrežama koje su aktivne (eng. *live*) pa se forenzičari koriste alatima za arhiviranje sadržaja.[32]

[29] Email Forensics: Investigation Techniques. Forensics Focus. Dostupno na: https://articles.forensicfocus.com/2019/02/15/email-forensics-investigation-techniques/ (11.04.2020.)
[30] Areas Of Study. Infosec. Dostupno na: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/ (11.04.2020.)
[31] Live Data Forensics. Council of Europe. Dostupno na: https://www.coe.int/en/web/octopus/blog/-/blogs/live-data-forensics-or-why-volatile-data-can-be-crucial-for-your-cases/ (11.04.2020.)
[32] Introduction to Social Network Forensics. Infosec. Dostupno na: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/hybrid-and-emerging-technologies/social-network-forensics/#gref (11.04.2020.)

Još jedna mlada grana digitalne forenzika je forenzika Interneta stvari (eng. *IoT forensics*). Forenzičar Interneta stvari mora poznavati tehnologije Interneta stvari, mreže i tehnologije u oblaku. Izazovi s kojima se susreće ova grana digitalne forenzike su brojni. Najveći izazov predstavlja prikupljanje podataka pa tako i njihova lokacija, budući da su uređaji Interneta stvari povezani na razne načine, pa se podaci mogu nalaziti u oblaku, na mobilnom uređaju ili na drugim uređajima. Drugi izazov je životni vijek podataka na uređajima, budući da ih je moguće lako prepisati. Internet stvari zahtjeva tehnologiju u oblaku, a korisnici su često anonimni pa je teško pronaći zločinca. Manjak sigurnosti je još jedan problem s kojim se susreće ova nova tehnologija. Također, svakim danom razvijaju se nove vrsta uređaja Interneta stvari, pa to predstavlja još jedan izazov za ovu granu digitalne forenzike.[33]

4.6. Antiforenzika

Budući da se digitalna forenzika počela primjenjivati svugdje u svijetu, kibernetički zločinci su razvili načine kojima mogu otežati istragu i prikriti svoje tragove. Antiforenzika je skup metoda koje se koriste za prevenciju znanstvenih metoda u zakonodavstvu, a koje provode policijske agencije.[34] Prema tome, digitalna antiforenzika je skup metoda i tehnika koje se koriste za ugrožavanje procesa digitalne forenzike, manipulacijom sustava i narušavanjem digitalnih dokaza.[35] Također, antiforenzikom se manipuliraju, brišu ili izmjenjuju digitalni dokazi, kako bi se analiza istih otežala, produžila ili virtualno onemogućila.[36]

Sakrivanje podataka je jedna od tehnika koju koriste antiforenzičari. Podaci se mogu sakriti promjenom imena datoteke ili ekstenzija, sakrivanjem datoteka u nepovezane direktorije, sakrivanjem datoteka unutar drugih datoteka i enkripcijom datoteke. Enkripcija ili šifriranje je proces pretvaranja podataka u šifre, koje nisu razumljive neovlaštenim osobama. Osim datoteka, moguće je šifrirati i cijele sustave datoteka (eng. *file system*), tvrde i ostale diskove na uređaju te mrežne protokole. Korištenje kompliciranih kriptografskih algoritama znatno otežava i produljuju posao digitalnog forenzičara. Najkorišteniji algoritmi za šifriranje su RSA (Rives-Shamir-Adleman) i AES (*Advanced Encryption Standard*) algoritmi. RSA je asimetričan algoritam koji koristi ključeve od 1024 do 4096 bitova, a sastoji se od javnog

[33] Alabdulsalam, S., Schaefer, K., Kechadi, T., & Le-Khac, N. (2018). Internet of Things Forensics – Challenges and a Case Study. Advances In Digital Forensics XIV, 35-48. Dostupno na: https://doi.org/10.1007/978-3-319-99277-8_3 (13.04.2020.)
[34] Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. Digital Investigation, 3, 44-49. Dostupno na: https://doi.org/10.1016/j.diin.2006.06.005 (13.04.2020.)
[35] Ćosić, J., Ćosić, Z., Bača, M. (2010). Digitalna antiforenzika – manipulacija procesom digitalne istrage. 18. TELEKOMUNIKACIONI FORUM TELFOR 2010. Dostupno na: https://www.bib.irb.hr/601475 (13.04.2020.)
[36] Sammons, J. (2014). The Basics of Digital Forensics (2nd ed.). Syngress. (13.04.2020.)

ključa za šifriranje i privatnog ključa za dešifriranje. AES je simetričan algoritam koji koristi ključeve od 128, 192 ili 256 bitova u blokovima od 128 bitova, a sastoji se od jednog ključa koji ima ulogu šifriranja i dešifriranja.[37] Steganografija je još jedna od metoda antiforenzike koja se koristi za sakrivanje podataka. Steganografija je sakrivanje podataka unutar obične poruke otkrivanjem podataka na destinaciji. Stego datoteka se sastoji od nosioca i tereta, nosioc je datoteka u kojoj se nalazi tajna poruka (npr. slika, audio ili video zapis, tekstualni dokument), a teret (eng. *payload*) je tajna poruka koja se nalazi u nosiocu. Jedan od izazova steganografije kojem se suprotstavlja digitalni forenzičar je težina otkrivanja tereta. Ukoliko digitalni forenzičar ipak uspije otkriti teret, izazov mu predstavlja i dobavljanje samog tereta bez poznavanja aplikacije i šifre kojom je sakriven podatak. Metoda koja se koristi u antiforenzici je i uništavanje podataka. Uništavanje podataka se vrši na nekoliko načina: brisanjem diska (eng. *drive wiping*), defragmentacijom diska (eng. *drive defragmentation*), uništavanjem metapodataka ili fizičkim uništavanjem.[38] Brisanje diska se odnosi na prepisivanje podataka na disku u tolikoj mjeri da ih je nemoguće vratiti. Defragmentacija diska je proces premještanja dijela podataka kako bi se ubrzao rad računala. Defragmentacija također može dovesti do prepisivanja i uništavanja podataka.[39] Uništavanje metapodataka je proces prepisivanja bajtova unutar datoteke koje dovodi do brisanja metapodataka. Posljednja metoda uništavanja podataka je fizičko uništavanje uređaja na kojem se nalaze podaci ili dokazi. Demagnetizacija je jedna od tehnika fizičkog uništavanja, a to je proces smanjenja ili uklanjanja magnetskog polja, kako bi došlo do uništenja podataka na tvrdom disku ili rjeđe, na disketama i magnetskim vrpcama.[40]

Antiforenzika računalnih mreža je skup metoda koje ugrožavaju ili usporavaju istragu mrežnog forenzičara. Neke od tehnika koje se koriste u antiforenzici računalnih mreža su tuneliranje (eng. *tunneling*), *onion* umjeravanje (eng. *onion routing*) i zavaravanje (eng. *spoofing*). Tuneliranje koristi enkapsulaciju kako bi se dozvolila privatna komunikacija putem javne mreže. Paketi bez sumnje putuju javnom mrežom. Kibernetički zločinci koriste virtualne privatne mreže (VPN) koje tuneliranjem omogućuje prikrivanje tragova i dokaza. Kako bi se organizacije obranile od takvih napada, potrebno je kontinuirano pratiti mrežne

[37] What is the Strongest Encryption Today? TechNadu. Dostupno na: https://www.technadu.com/strongest-encryption/37596/ (13.04.2020.)
[38] Anti-Forensics. Infosec. Dostupno na: https://resources.infosecinstitute.com/anti-forensics-part-1/ (13.04.2020.)
[39] Sammons, J. (2014). The Basics of Digital Forensics (2nd ed.). Syngress. (13.04.2020.)
[40] Anti-Forensics. Infosec. Dostupno na: https://resources.infosecinstitute.com/anti-forensics-part-1/ (13.04.2020.)

veze. *Onion* usmjeravanje je proces slanja šifriranih paketa u slojevima, poput slojeva luka, kako bi poslana poruka ostala anonimna. *Onion* usmjeravanje se koristi kod anonimnih preglednika za pretraživanje *deep web-a.* Obrnuto usmjeravanje se koristi za obranu od *onion* usmjeravanja, ali je dugotrajno. Zavaravanje je proces sakrivanja komunikacije kako bi se dobio pristup neovlaštenim sustavima ili podacima. Može se koristiti na elektroničkoj pošti, pozivima i mrežnim stranicama. Postoje IP (eng. *Internet Protocol*), MAC (eng. *Media Access Control*), ARP (eng. *Address Resolution Protocol*) i DNS (eng. *Domain Name System*) zavaravanje. IP i DNS zavaravanje može dovesti do distribuiranog uskraćivanja usluge (eng. *Distributed Denial of Service*). Kod IP zavaravanja napadači koriste drugačije IP adrese, kako bi prikrili vlastite. MAC zavaravanje se koristi za prikrivanje vlastite MAC adrese, korištenjem lažne adrese.[41] Upravo zbog pojave antiforenzike, digitalni forenzičari moraju tražiti nove metode, tehnike i alate kako bi uspješno obavljali svoj posao.

[41] 6 Anti-forensic techniques that every cyber investigator dreads. EC-Council. Dostupno na: https://blog.eccouncil.org/6-anti-forensic-techniques-that-every-cyber-investigator-dreads/ (13.04.2020.)

5. Alati u digitalnoj forenzici

U digitalnoj forenzici postoji velik broj alata, od kojih su neki razvijeni za specifičnu namjenu, a neki se upotrebljavaju u različite svrhe. Alati mogu biti hardverske ili softverske prirode, komercijalni ili otvorenog koda. Bitno je napomenuti, budući da je razvijen velik broj alata, dobra forenzička praksa je koristiti više alata za istu svrhu zbog potvrđivanja dokaza. Alati imaju svoje prednosti i nedostatke, ali kako bi se uopće mogli koristiti, potrebno ih je odobriti. Nacionalni institut za standarde i tehnologiju (eng. *National Institute of Standards and Technology* – NIST) je prije nekoliko godina pokrenuo projekt za testiranje alata koji se koriste u digitalnoj forenzici. Cilj tog projekta je uspostaviti metodologiju za testiranje softverskih alata u digitalnoj forenzici, razvijanjem specifikacija, procedura testiranja, kriterija, skupova testova i uređaja za testiranje. Svaki alat mora se odobriti kada je ažuriran ili promijenjen, neovisno je li hardverske ili softverske prirode.[42]

5.1. Hardver

Hardver su svi fizički elementi računala, elektroničkog sustava ili uređaja. U kontekstu digitalne forenzike hardver kao alat uključuje uređaje za kloniranje, uređaje za prijenos mobilnih telefona, uređaje za blokiranje pisanja, prijenosne memorije za pohranu, adaptere, kablove i ostalo. Dobro opremljeno računalo je najbitniji dio istrage digitalnog forenzičara. Takvo računalo mora posjedovati nekoliko višejezgrenih procesora, što više radne memorije te brze tvrde diskove sa što više memorije. Programeri softvera digitalne forenzike objavljuju minimalne i preporučene hardverske zahtjeve. Što se tiče mobilnih uređaja, kako je ranije navedeno, proizvođači nisu standardizirali kabele, pa digitalni forenzičar pri ruci mora imati sve aktualne i stare kabele i konektore. U digitalnoj forenzici je nužno klonirati uređaje i diskove radi očuvanja fizičkog medija. Iz tog razloga, forenzičari koriste uređaje za kloniranje hardvera. Takvi uređaji mogu klonirati više tvrdih diskova i tako ubrzavaju proces istrage. Također, omogućuju zaštitu od zapisivanja, odnosno modificiranja i brisanja podataka.[43] Uređaji za prijenos mobilnih telefona se nazivaju Faraday vreće ili kavezi. Mobilni telefon koji se nalazi u Faraday vreći nije u mogućnosti komunicirati s vanjskim bežičnim uređajima, zbog presretanja radio valova. U mobilnoj forenzici se još koriste čitači SIM kartica, koji se mogu nalaziti u računalu ili biti samostalna USB sučelja.[44]

[42] Sammons, J. (2014). The Basics of Digital Forensics (2nd ed.). Syngress. (18.04.2020.)
[43] Sammons, J. (2014). The Basics of Digital Forensics (2nd ed.). Syngress. (18.04.2020.)
[44] Prasad, A., Pande, J. (2016). Digital Forensics. Uttarakhand Open University. (18.04.2020.)

5.2. Softver

Softver je svaki program koji zadaje računalu neke zadatke, a pokreće se na osobnim računalima, mobilnim telefonima, tabletima i ostalim pametnim uređajima.[45] Danas postoji veliki broj alata koji se koriste u digitalnoj forenzici. Digitalni forenzičar će koristiti alate kako bi prikupio podatke iz sustava, računala ili mreže bez da izmjeni podatke na samom sustavu. Neki alati uključuju funkcionalnosti koje se drže upravo ovog principa. Alati mogu imati određenu namjenu i limitirane funkcionalnosti, ali postoje i alati koji imaju širok obujam funkcija i mogućnosti. U smislu digitalne forenzike, softver se dijeli na komercijalne alate i alate otvorenog koda. Faktori pri odabiru alata su trošak, funkcionalnosti, mogućnosti i podrška.[46] Alati u digitalnoj forenzici se koriste za dešifriranje, analizu datoteka, analizu registra, prikupljanje i sigurnosnu kopiju medija, analizu elektroničke pošte, analizu i prikupljanje mrežnih paketa, *live* analizu i otkrivanje plagijata. [47]

5.2.1. Komercijalni softver

Komercijalni softver se odnosi na svaki softver ili program koji je dizajniran i razvijen za licenciranje ili prodaju krajnjim korisnicima ili koji se koristi u komercijalne svrhe.[48] Neke od mogućnosti koje komercijalni softver nudi su blokiranje zapisivanja, kloniranje diskova, prikupljanje forenzičko značajnih dokaza, očuvanje dokaza šifriranjem, oporavak skrivenih i obrisanih datoteka, udaljeno i *live* prikupljanje dokaza, analiza radne memorije, preslikavanje (eng. *image mounting*), napredno pretraživanje i filtriranje podataka te metapodataka, označavanje datoteka i sektora (eng. *bookmarking*), otkrivanje zaporki i automatsko generiranje izvješća. EnCase Forensic (https://www.guidancesoftware.com/encase-forensic), Forensic Toolkit (http://accessdata.com/products-services/forensic-toolkit-ftk) i X-Ways Forensics (http://www.x-ways.net/forensics/) su među najkorištenijim komercijalnim programima u digitalnoj forenzici.

EnCase je skup alata za digitalnu forenziku kojeg je razvila tvrtka Guidance Software. Alat je razvijen za Windows operacijski sustav, ali postoji inačica i za UNIX sustave. Najčešće se koristi za preslikavanje, čitanje sustava datoteka, vraćanje izgubljenih particija i obrisanih datoteka. EnCase Forensic ima mogućnost označavanja dokaza i ispisivanja izvještaja.

[45] Software. Techopedia. Dostupno na: https://www.techopedia.com/definition/4356/software (18.04.2020.)
[46] Sammons, J. (2014). The Basics of Digital Forensics (2nd ed.). Syngress. (18.04.2020.)
[47] Commercial Computer Forensics Tools. Infosec. Dostupno na: https://resources.infosecinstitute.com/category/computerforensics/introduction/commercial-computer-forensics-tools/ (18.04.2020.)
[48] Commercial Software. Techopedia. Dostupno na: https://www.techopedia.com/definition/4245/commercial-software (18.04.2020.)

Pretraživač ima mogućnost dobavljanja i indeksiranja podataka te pretraživanja izraza, a može pretraživati i nedodijeljeni prostor u heksadecimalnim vrijednostima. Postoji i EnCase Portable koji je prenosivi hardver, a funkcionalnosti uključuju podizanje računala i kalkulaciju *hash* vrijednosti.[49] Također, razvili su i alat za mobilne uređaje EnCase Mobile Investigator koji nudi podršku za velik broj mobilnih uređaja i operacijskih sustava i optičko prepoznavanje znakova.[50] Osim navedenih alata, razvili su i EnForce Risk Manager, EnCase Endpoint Security, EnCase eDiscovery i EnCase Endpoint Investigator.[51]

Forensic Toolkit (FTK) je skup alata za digitalnu forenziku koji je razvila tvrtka AccessData. FTK sadrži lakšu inačicu FTK Imager koja se koristi za preslikavanje fizičkog ili logičkog diska, ali i particije na USB disku. Format koji se koristi u ovom alatu ima ekstenziju .adf što označava AccessData format. FTK Imager ima mogućnosti pregledavanja podataka i vraćanja datoteka ovisno o tome jesu li prepisane, a prenosiv je pa se može koristiti na pokrenutim uređajima.[52] FTK je temeljen na bazi podataka, odnosno svi podaci se spremaju u jednu centralnu bazu, što omogućuje timski rad nad samo analizom i istragom.[53]

X Ways Forensics je skup alata koji se koristi u digitalnoj forenzici i razvijen je za Windows operacijski sustav. Također je prenosiv, kao i prethodno navedeni alati. Podržava preslikavanje i kloniranje diska te dobavljanje datoteka. Može čitati razne formate datoteka poput expert witness file formata (.ewf) i virtual machines image-a (.vmdk). X-Ways Forensics je integrirani softver, a uz njega su razvijena još tri specijalizirana alata: X-Ways Investigator, WinHex i X-Ways Imager. X-Ways Investigator se koristi za istragu, analizu dokumenata i stvaranje izvještaja. WinHex je inačica koja je koristi za uređivanje heksadecimalnih vrijednosti i diska, a X-Ways Imager se koristi za preslikavanje diska.[54]

[49] Commercial Computer Forensics Tools. Infosec. Dostupno na: https://resources.infosecinstitute.com/category/computerforensics/introduction/commercial-computer-forensics-tools/ (18.04.2020.)
[50] EnCase Mobile Investigator. Guidance Software. Dostupno na: https://www.guidancesoftware.com/encase-mobile-investigator (18.04.2020.)
[51] Software. Guidance Software. Dostupno na: https://www.guidancesoftware.com/software (18.04.2020.)
[52] Commercial Computer Forensics Tools. Infosec. Dostupno na: https://resources.infosecinstitute.com/category/computerforensics/introduction/commercial-computer-forensics-tools/ (18.04.2020.)
[53] Forensic Toolkit (FTK). Access Data. Dostupno na: https://accessdata.com/products-services/forensic-toolkit-ftk (18.04.2020.)
[54] X-Ways Forensics: Integrated Computer Forensics Software. X-Ways. Dostupno na: http://www.x-ways.net/forensics/ (18.04.2020.)

5.2.2. Softver otvorenog kôda

Softverom otvorenog kôda smatra se onaj softver kojega je moguće besplatno i slobodno dijeliti, postoji pristup izvornom kôdu kojega krajnji korisnici mogu uređivati i ne smije se zabraniti korištenje samog softvera. Jedna od prednosti korištenja softvera otvorenog kôda u digitalnoj forenzici je obrazovanje forenzičara – u svrhu školovanja, budući forenzičari se samostalno mogu educirati na alatima koji su besplatni i otvoreni za korištenje. Osim što je besplatan, softver otvorenog kôda je često prenosiv i fleksibilan. Prenosivi softver je moguće nositi i koristiti od sustava do sustava. Prenosivost označava gdje će se koristiti softver, a fleksibilnost kako će se koristiti – na lokalnom sustavu ili udaljeno, na jednom ili više sustava. Još jedna prednost softvera otvorenog kôda je što je besplatan, što omogućuje korisnicima komercijalnog softvera pokrivanje funkcija koje taj softver nema ili za potvrđivanje nalaza i operacija komercijalnog softvera. Najveća prednost je pristup samom kôdu programa, kojeg je moguće naknadno uređivati i nad kojim se mogu otkrivati i otklanjati pogreške.[55] Softveri otvorenog kôda u digitalnoj forenzici su izdani pod GPL licencom (eng. *General Public License*), što znači da su alati besplatni i otvorenog kôda, kao i svi naknadni derivati, koji također moraju biti pod istom licencom.[56] Besplatni softveri su uglavnom za specifičnu namjenu, za razliku od komercijalnih koji mogu biti sveobuhvatni. Neki od softvera otvorenog koda za digitalnu forenziku su The Sleuth Kit i Autopsy (http://www.sleuthkit.org/), Wireshark (https://www.wireshark.org/) i Volatility (https://www.volatilityfoundation.org/).

The Sleuth Kit je skup alata za analizu sustava datoteka. Nastao je na temelju Coroner's Toolkit-a, alata za forenzičku analizu UNIX sustava. Coroner's Toolkit nije bio prenosiv i nije imao podršku za ostale operacijske sustave, pa je kasnije The Sleuth Kit to nadomjestio.[57] The Sleuth Kit se sastoji od alata za analizu datotečnog sustava i alata za upravljanje medijima za pohranu. Alati su neovisni o operacijskom sustavu, a mogu i procesuirati obrisane te sakrivene sadržaje. Alat za upravljanje medijima za pohranu se koristi u svrhu istraživanja diskova i lociranje particija. Autopsy je grafičko korisničko

[55] Altheide, C., Carvey, H. (2011). Digital forensics with Open Source Tools. Syngress. (19.04.2020.)
[56] Commercial Computer Forensics Tools. Infosec. Dostupno na: https://resources.infosecinstitute.com/category/computerforensics/introduction/commercial-computer-forensics-tools/ (19.04.2020.)
[57] Altheide, C., Carvey, H. (2011). Digital forensics with Open Source Tools. Syngress. (19.04.2020.)

sučelje unutar TSK-a, koje olakšava istragu. Mogućnosti Autopsy-ija uključuju upravljanje slučajem, pretraživanje ključnih riječi, analiza vremenske linije i filtriranje hash funkcija.[58]

Wireshark je softver otvorenog koda za analizu mrežnog prometa, paketa i protokola. Koristi se za otklanjanje poteškoća na mreži, analizu, razvoj komunikacijskih protokola i u obrazovanju. Razvio ga je Gerald Combs 1998. godine, pod imenom Ethereal, a 2006. godine zbog autorskih prava mijenja ime u Wireshark. Wireshark radi na većini platformi i operacijskih sustava, poput Windows-a, UNIX-a, MacOS-a, Solaris-a, FreeBSD-a i NetBSD-a. Iako Wireshark ima svoje grafičko sučelje, postoji i Tshark, inačica temeljena na terminalu. Funkcionalnosti ovog alata su duboka analiza velikog broja mrežnih protokola, dobavljanje paketa uživo, pregled paketa, filtriranje, analiza VoIP-a (eng. *Voice over Internet Protocol*), usklađenost formata datoteka i podrška za dešifriranje protokola.[59]

Volatility je skup alata otvorenog kôda za analizu memorije. Primarni alat unutar okvira (eng. *framework*) je Python skripta koja omogućava niz dodataka za analizu pohrane. Volatility okvir se može koristiti na bilo kojem operacijskom sustavu koji podržava Python. Volatility se fokusira na analizu podataka u radnoj memoriji. Također, koristi se u analizi zlonamjernih programa i u odgovaranju na incidente (eng. *incident response*). Ovaj skup alata je razvijen kako bi upoznao stručnjake s tehnikama i složenošću prikupljanja promjenjivih podataka u pohrani. Volatility nema svoje sučelje već se pokreće putem terminala ili naredbenog retka.[60]

[58] Open Source Digital Forensics. Sleuth Kit. Dostupno na: http://www.sleuthkit.org/index.php (19.04.2020.)
[59] About Wireshark. Wireshark. Dostupno na: https://www.wireshark.org/ (19.04.2020.)
[60] Volatility. Volatility Foundation. Dostupno na: https://www.volatilityfoundation.org/ (19.04.2020.)

5.2.3. Linux distribucije

Osim navedenih alata, digitalni forenzičari često koriste neke alate i distribucije operacijskog sustava Linux. Linux distribucije u digitalnoj forenzici su DEFT, CAINE (https://www.caine-live.net/) i Kali Linux (https://www.kali.org/). DEFT (*Digital Evidence and Forensics Toolkit*) je distribucija koja je 2019. obustavljena. DEFT je razvijen na GNU/Linux i DART (*Digital Advanced Response Toolkit*) skupu alata. Osim pune inačice, postoji i lakša inačica DEFT Zero, koja ne podržava mogućnosti poput analize mobilnih uređaja i otkrivanja zaporki. Ova distribucije se može koristiti uživo, odnosno kad bi gašenje sustava uzrokovalo gubitak podataka. DEFT nudi alate protiv zlonamjernih programa, za oporavak podataka i zaporki, preslikavanje, mobilnu i mrežnu forenziku te za izvještavanje.

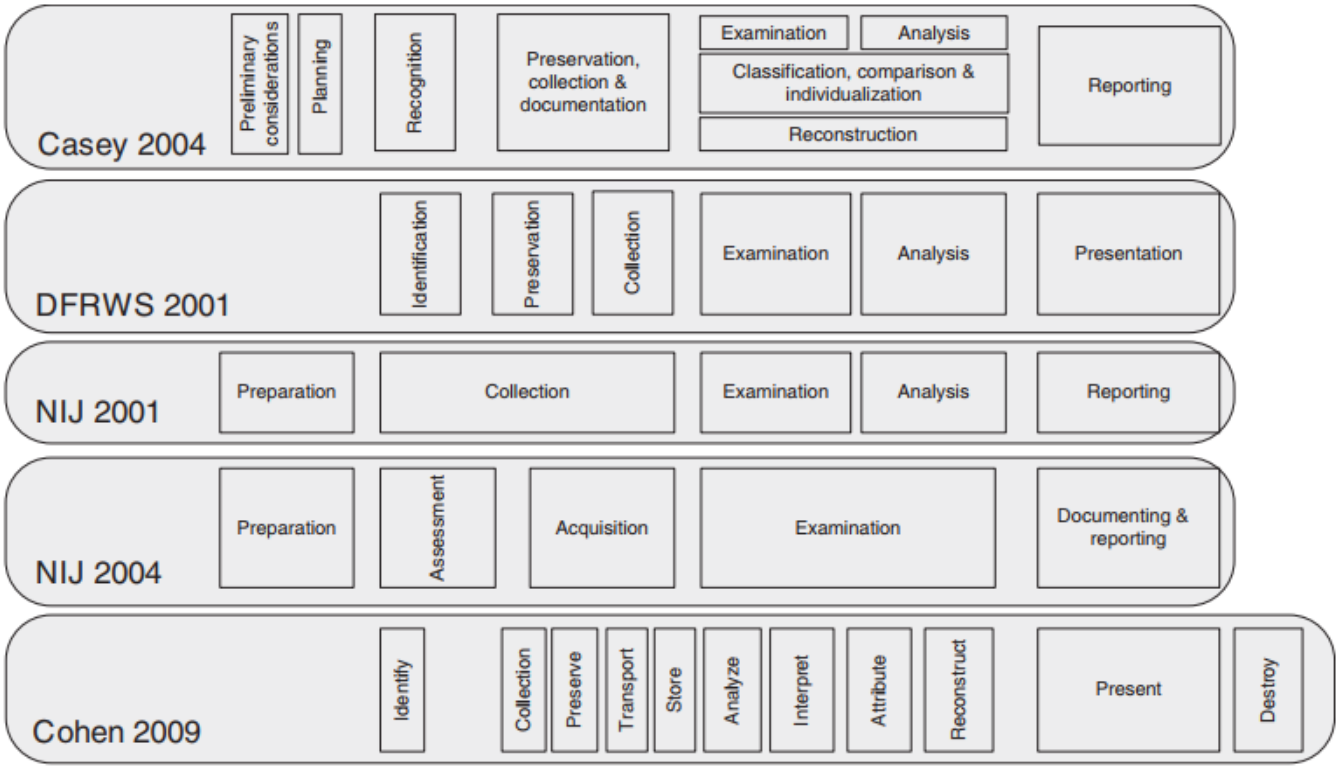
CAINE (*Computer Aided INvestigative Environment*) je distribucija koja je nastala kao dio projekta digitalne forenzike u Italiji. CAINE nudi alate za digitalnu forenziku i ima mogućnost instaliranja već spomenutih alata poput Autopsy-ija. Alati na ovoj distribuciju se mogu koristiti za analizu diska, forenziku pohrane i baza podataka, mobilnu i mrežnu forenziku.

Kali je poznata Linux distribucija zasnovana na Debianu, koja se koristi u računalnoj sigurnosti i digitalnoj forenzici. Razvijen je kao distribucija BackTrack za penetracijsko testiranje do 2015. kada je preimenovan u Kali. Kali je popularna distribucija i u antiforenzici, budući da sadržava nekolicinu alata koji se mogu koristiti u svrhe kibernetičkih napada. Osim što se može koristiti kao cjelokupni operacijski sustav na računalu, moguće ga je instalirati i na uređaje.[61] Alati za Kali su poredani po kategorijama: prikupljanje informacija, analiza ranjivosti, napadi na bežičnu mrežu, mrežne aplikacije, iskorištavanje ranjivosti, testiranje izdržljivosti (eng. *stress testing*), alati za forenziku, njuškanje i ometanje (eng. *sniffing and spoofing*), napadi na zaporke, pristup održavanju, obrnuto inženjerstvo, hakiranje hardvera i alati za izvještavanje. Neki od alata za forenziku su Volatility, Guymager, Dumpzilla i Cuckoo. Guymager se koristi za preslikavanje podataka unutar medija, Dumpzilla se koristi za prikupljanje relevantnih informacija s preglednika, a Cuckoo za analizu zlonamjernih programa.[62]

[61] Operating systems and open source tools for digital forensics. Packt. Dostupno na: https://subscription.packtpub.com/book/networking_and_servers/9781788625005/1/ch01lvl1sec13/operating-systems-and-open-source-tools-for-digital-forensics (20.04.2020.)
[62] Kali Linux Tools Listing. Kali Tools. Dostupno na: https://tools.kali.org/tools-listing (20.04.2020.)

6. Metodologija digitalne istrage

Forenzički i znanstveni proces se koristi u istragama digitalne forenzike. Mnogi stručnjaci u polju ga definiraju kao korake ili faze koje digitalni forenzičari poduzimaju od početka incidenta do izvještavanja o dokazima.[63] Stručnjaci se ne mogu složiti oko standardnog modela procesa u digitalnoj forenzici, ali je najčešće potrebno šest koraka kako bi se provela potpuna digitalna istraga: priprema, prepoznavanje, prikupljanje, očuvanje, analiza i prezentacija.



Slika 1: Usporedba modela procesa u digitalnoj forenzici

[63] Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press. (28.04.2020.)

6.1. Priprema

Priprema (eng. preparation) je prva faza procesa u digitalnoj istrazi, a podrazumijeva planiranje radnji koje će se provesti za efektivnu istragu i prikupljanje potrebnih izvora i materijala. Priprema slijedi odmah nakon samog incidenta. Ova faza se mora provesti prije same istrage, kako bi forenzičari bili sigurni da imaju potrebnu infrastrukturu i tehnologije za provođenje istrage. U fazi pripreme incident se mora pronaći i identificirati radi procjene rizika i prijetnji. Prije svega je potrebno komunicirati s ostalim službenicima na slučaju. Ukoliko je potrebno, forenzičar treba nabaviti nalog za pretres te ostale potrebne suglasnosti i dozvole. Također, mora pripremiti papirologiju za dokumentaciju slučaja. Priprema podrazumijeva i razvijanje plana, uključujući politike, procedure, zadatke službenika i tehničke zahtjeve. Potrebno je uspostaviti strategiju za prikupljanje i očuvanje dokaza i specificirati korake za istraživanje i analizu tih dokaza, odnosno pripremiti sve što je potrebno da bi se iduće faze procesa realizirale.[64]

6.2. Prepoznavanje

Prepoznavanje (eng. *identification*) je druga faza procesa digitalne istrage. Prepoznavanje se temelji na jednom od najbitnijih načela forenzike, a to je Locardovo načelo razmjene (eng. *Locard's exchange principle*). Locardovo načelo razmjene pretpostavlja da ukoliko dva objekta dođu u kontakt, ostavit će trag jedno na drugom, odnosno u forenzici, zločinac ne može otići s mjesta zločina bez da ostavi trag i bez da ponese nešto sa sobom. Ovo načelo se ne odnosi samo na fizički, već i na digitalni svijet. Na primjer, ako pojedinac pretražuje nešto na mrežnom pregledniku, poslužitelj ili vatrozid mogu zabilježiti njegovu IP adresu, a preglednik može spremiti kolačiće. Treba biti oprezan jer kao i fizički, digitalni dokazi mogu biti privremeni i nestati iz memorije. Locardovo načelo može pomoći pri prepoznavanju potencijalnih izvora dokaza.[65] Faza prepoznavanja se odnosi na samo pronalaženje izvora dokaza, kao što su mjesto zločina, unutar tvrtke ili na Internetu. Osim utvrđivanja lokacije izvora, faza prepoznavanja uključuje i određivanje osoba zaposlenih u tvrtki koja je žrtva incidenta ili osoba koje imaju veze s tehnologijom koja je napadnuta. Potrebno je razgovarati s administratorima, čuvarima i korisnicima te otkriti imaju li ikakve relevantne informacije.[66]

[64] Abdalla, S., Hazem, S., & Hashem, S. (2007). Guideline Model for Digital Forensic Investigation. Annual ADFSL Conference on Digital Forensics, Security and Law. Dostupno na: https://commons.erau.edu/adfsl/2007/session-7/2 (28.04.2020.)
[65] Johansen, G. (2020). Digital Forensics and Incident Response (2nd ed.). Packt Publishing. (28.04.2020.)
[66] Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press. (28.04.2020.)

6.3. Prikupljanje

Prikupljanje (eng. *acquisition*) je treća faza procesa digitalne istrage u kojoj forenzičar prikuplja identificirane dokaze na pokrenutom ili ugašenom sustavu. Bitno je napraviti kopije zapisa, diskova, izvještaja ili pristupnih zapisa te pružati valjane i legitimne kopije potpunih zapisnika koje je moguće iskoristiti na sudu. Osim digitalnih zapisa, prikupljanje se odnosi i na fizičke uređaje poput tvrdih diskova, optičkih medija, kartica za pohranu, digitalnih fotoaparata, mobilnih uređaja, ali i samih računala, kao i pripadajućih komponenti i periferija. Kada je to moguće, potrebno je napraviti radnu kopiju, u suprotnom s originalnim medijem treba rukovati pažljivo radi očuvanja integriteta i podataka.[67]

Za prikupljanje na upaljenom ili pokrenutom sustavu treba uspostaviti prioritete u smislu promjenjivosti (eng. *volatility*). Prioriteti slijede od najviše promjenjivih podataka u memoriji do najmanje promjenjivih, pa bi trebalo prikupiti prvo zapisnike, privremenu memoriju, tablice usmjeravanja i ARP tablice, statistike jezgre, tablice procesa, a kasnije podatke o fizičkoj konfiguraciji i mrežnoj topologiji, medije za arhiviranje i drugo. Osim što treba paziti na promjenjivost, potrebno je spriječiti vanjske smetnje i pokretanje programa na računalu. Također, treba analizirati stvarno stanje sustava sa što manje promjena. Prikupljanje se vrši nadzorom mreže, sustava i kamerama. Mrežni dokazi se prikupljaju iz izvora kao što su sustavi za otkrivanja upada (eng. *intrusion detection system*), usmjernika, vatrozida i poslužitelja. Kako bi se očuvao integritet informacija, potrebno je koristiti alate za blokiranje pisanja prije samog preslikavanja diska, a dobro je napraviti barem dvije kopije diska. Naravno, treba svaki korak pažljivo i detaljno dokumentirati.

Drugi scenarij je sustav koji je već ugašen pa su radnje kod prikupljanja nešto drugačije. Ukoliko je sustav već ugašen, nikad se ne bi trebao paliti jer će to ugroziti cijelu istragu. Potrebno je odrediti strukturu, model i veličinu diska, koristiti alate za blokiranje pisanja, isključiti i preuzeti uređaje za pohranu kada je to moguće, napraviti najmanje dvije kopije diska i napraviti dokumentaciju cijelog procesa.[68]

[67] Altheide, C., Carvey, H. (2011). Digital forensics with Open Source Tools. Syngress. (28.04.2020.)
[68] Abdalla, S., Hazem, S., & Hashem, S. (2007). Guideline Model for Digital Forensic Investigation. Annual ADFSL Conference on Digital Forensics, Security and Law. Dostupno na: https://commons.erau.edu/adfsl/2007/session-7/2 (28.04.2020.)

6.4. Očuvanje

Očuvanje (eng. *preservation*) je četvrta faza procesa digitalne istrage. Nakon identifikacije dokaza, potrebno je dokaze čuvati od bilo kakve promjene ili brisanja. Očuvanje se odnosi na sprječavanje promjena nad digitalnim dokazima, koje uključuje izolaciju sustava na mreži, spremanje relevantnih zapisnih datoteka i prikupljanje promjenjivih podataka, koji bi nestali ukoliko se sustav ugasi. Kod zapisnih datoteka potrebno je uključiti kontrole koje čuvaju datoteke od izmjena ili uklanjanja. Sustavi se mogu izolirati na mreži putem fizičkih ili logičkih kontrola, kontrola za pristup mreži ili kontrola periferije. U ovoj fazi je bitno da korisnici ili drugi sudionici ne koriste sustav koji se promatra, kako ne bi namjerno ili nenamjerno ugrozili dokaze. [69]

6.5. Analiza i ispitivanje

Analiza i ispitivanje (eng. *analysis and examination*) je predzadnja i najbitnija faza digitalne istrage. Prikupljeni podaci se analiziraju i preispituju kako bi se utvrdilo je li zločin počinjen i mogu li poslužiti kao dokazi na sudu. Ova faza se odnosi na samu interpretaciju digitalnih dokaza. Ispitivanje je izdvajanje i pregledavanje informacija iz prikupljenih dokaza, kako bi bili spremni za analizu. Forenzička analiza je primjena znanstvenih metoda i kritičkog razmišljanja kako bi odgovorili na sljedeća pitanja: tko, što, gdje, kada, kako i zašto?[70] Tko ili što je kreiralo, uredilo, promijenilo, poslalo, primilo ili ugrozilo podatke i s kim je povezano? Gdje su podaci pronađeni i kako su dospjeli tamo gdje jesu te znamo li gdje su relevantni događaji locirani? Kada su podaci kreirani, pristupljeni, izmijenjeni, primljeni, poslani, pregledani, obrisani i pokrenuti te znamo li kada su se relevantni događaji odvijali i što se na sustavu u istom vremenskom periodu događalo? Kako je podatak nastao na mediju, odnosno kako je kreiran, prenošen, izmijenjen i korišten te znamo li kako su se odvijali relevantni događaji? Koje su povezane informacije i datoteke s podacima koje istražujemo?[71]

U fazi analize i ispitivanja forenzičari dolaze do krajnjih rezultata istrage, odnosno dolazi se do zaključka u kojem su povezani prikupljeni i analizirani podaci koji tvore početak, radnju i završetak incidenta te služe kao legitimni dokazi koji će se kasnije iskoristiti na sudu. Neke od metoda su vremenska analiza, analiza skrivenih podataka i analiza datoteka i aplikacija.

[69] Johansen, G. (2020). Digital Forensics and Incident Response (2nd ed.). Packt Publishing. (28.04.2020.)
[70] Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press. (28.04.2020.)
[71] Computer Forensics: Digital Forensic Analysis Methodology. Crime Scene Investigator Network. Dostupno na: https://www.crime-scene-investigator.net/computer-forensics-digital-forensic-analysis-methodology.html (28.04.2020.)

Vremenska analiza je proces određivanja vremenskog perioda u kojem se zločin, napad ili incident dogodio. Stvara se vremenska crta razvoja događaja, pregledavaju se metapodaci ili zapisnici – podaci o posljednjim izmjenama i pristupima, vremenu nastanka, promjeni statusa i drugo. Analiza skrivenih podataka može ukazati na vlasništvo ili namjeru, pretraživanjem podataka s izmijenjenim ekstenzijama ili kriptiranih i komprimiranih datoteka. Analiza datoteka i aplikacija se odnosi na pregledavanje sadržaja datoteke, identificiranje operacijskog sustava, utvrđivanje povezanosti datoteka i pregledavanje korisničkih postavki. Takvom analizom izvode se zaključci o sustavu i korisniku. Potrebno je dokumentirati svaki korak, jer je ova faza ključan dio digitalne istrage.[72]

6.6. Prezentacija

Prezentacija (eng. *presentation*) je posljednja faza procesa digitalne istrage koja se odnosi na izvještavanje o prethodnim fazama i rezultatima analize i ispitivanja. Izvještaj povezuje zaključke analize, dokaza i dokumentacije, sadrži vrijeme i datum analize te detaljan opis rezultata dobivenih ispitivanjem. Izvještaj mora sadržavati detaljnu dokumentaciju alata, procesa i metodologije. Složenost izvještaja ovisi o namjeni, a osim u pravne svrhe, piše se i izvještaj koji ide tvrtki koja je bila napadnuta. Kada je istraga zaključena, rezultati se prezentiraju pravnicima i sucu. Rezultate je potrebno obrazložiti jednostavnim terminima, neovisno o razini tehnološkog znanja pravnika i ostalih sudionika.[73]

Izvještavanje činjenica u digitalnoj forenzici mora biti jasno, sažeto i objektivno, dok pisani izvještaj mora biti temeljit, precizan i objektivan. Elementi izvještaja digitalne istrage su izvršni sažetak, nalazi, priloženi izvještaji i zaključak. Svrha izvršnog sažetka je detaljno opisati rezultate analize i istrage, jednostavnim, netehnološkim izrazima i terminima. Svrha nalaza je detaljno opisati tehničke aspekte analize s dijagramima, grafikonima i fotografijama. Priloženi izvještaj se sastoji od dodatnih relevantnih informacija koje su veoma detaljno opisane, a može sadržavati podatke poput poruka i elektroničke pošte. Zaključak pruža subjektivnu analizu i mišljenja stručnjaka te ne smije sadržavati nikakve nove informacije i podatke. Savjetuje se da izradu izvještaja nadgleda nekoliko osoba koje su stručne u području kako bi mogli izvršiti reviziju. [74]

[72] Računalna forenzika. Nacionalni CERT. Dostupno na: https://www.cert.hr/racunalna-forenzika/ (28.04.2020.)
[73] Računalna forenzika. Nacionalni CERT. Dostupno na: https://www.cert.hr/racunalna-forenzika/ (28.04.2020.)
[74] Digital Forensic Process—Presentation. DriverSavers Data Recovery. Dostupno na: https://drivesaversdatarecovery.com/blog/digital-forensic-process-presentation/ (28.04.2020.)

7. Metode i tehnike

Digitalni forenzičari koriste niz metoda i tehnika kada provode istragu, prikupljaju dokaze i analiziraju ih. Dvije metode su ključne u digitalnoj forenzici, a to su odgovor na incident i elektroničko otkriće.

7.1. Metode

Odgovor na incident (eng. *incident response*) je proces suočavanja organizacije s digitalnim incidentom. Organizacija je sigurna ako ima već pripremljene mjere koje se tiču svake faze procesa. Kada organizacija prvi put uoči događaj povezan sa zlonamjernom aktivnošću, tada nastaje incident. Takvo uočavanje može biti u obliku sigurnosnog upozorenja unutar organizacija ili upozorenja o potencijalnim sigurnosnim propustima od treće strane. Nakon upozorenja, organizacija samostalno analizira incident kroz mjere ograničavanja, kako bi informacijski sustav nastavio s radom.

Proces odgovora na incident započinje s pripremom, koju slijedi otkrivanje, pa analiza, ograničavanje, zatim iskorjenjivanje i oporavak te aktivnosti nakon incidenta i tako u krug. Priprema je ključni dio istrage, pa tako i samog odgovora na incident. Kritični dio pripreme je složiti plan odgovora na incident, s potrebnim osobljem, procesima, procedurama i alatima. Otkrivanje (eng. *detection*) je kompleksni dio odgovora na incident. Ovisno o veličini organizacije, broj dnevnih događaja može biti jako velik. Događaji mogu biti normalne poslovne aktivnosti ili pokazatelji potencijalne opasnosti. Organizacije koriste sustave za sigurnosne incidente i upravljanje događajima (eng. *security incident and event management system*), koje je potrebno često ažurirati skupovima pravila za određivanje potencijalnih incidenata. Otkrivanje je dio odgovora na incident u kojem organizacija prvi put postane svjesna o zlonamjernom ponašanju događaja. Otkrivanje zlonamjernih događaja može biti unutar organizacije, od vanjskih izvora ili od strane korisnika. Vanjski izvori poput davatelja usluge Interneta (eng. *Internet service provider*) ili službe za očuvanje reda i sigurnosti (eng. *law enforcement agency*) mogu otkriti zlonamjerne aktivnosti unutar mreže organizacije te kontaktirati i savjetovati ih. Isto tako, korisnici i zaposlenici mogu naići na zlonamjerne aktivnosti i prijaviti ih nadležnima. Kada je incident otkriven, osoblje iz organizacije ili provjerena vanjska tvrtka započinje s fazom analize. U ovoj fazi, prikupljaju se podaci o događajima u sustavu. Ovisno o vrsti incidenta, analiza može trajati od nekoliko sati do nekoliko dana. Nakon prikupljanja, provode se ispitivanja. Alatima se utvrđuje što se dogodilo, na što je incident utjecao, jesu li drugi sustavi uključeni i jesu li ukradeni

povjerljivi podaci. Cilj analize je otkriti uzrok incidenta i rekonstruirati incident do otkrivanja. Ograničavanje (eng. *containment*) je faza koju je potrebno provesti nakon analize incidenta. Organizacije provode mjere kako bi smanjile daljnje širenje prijetnji. Strategije ograničavanja su različite, a neke od njih su zaključavanje priključaka (eng. *port*) i IP adresa na vatrozidima ili isključivanje mrežnog kabela iz zaraženog sustava. Svaka vrsta incidenta uključuju različitu strategiju ograničavanja, ali dobro je imati nekoliko opcija kako bi zaustavili širenje prijetnje. Iskorjenjivanje i oporavak dolazi nakon ograničavanja incidenta. Organizacija uklanja prijetnju na sustavu ili mreži. U slučaju zlonamjernih programa, rješenje je pojačani antivirusni program. U drugim slučajevima, sustavi se moraju počistiti i preslikati, a također potrebno je i uklanjanje ili mijenjanje korisničkih računa. Programe je potrebno ažurirati i zakrpati (eng. *patch*), a operacijske sustave i aplikacije ponovno instalirati. Ukoliko postoje sigurnosne kopije, treba vratiti podatke s lokalnih sustava. Na kraju se provodi sveobuhvatno pretraživanje ranjivosti kako bi organizacija bila sigurna da su sve prijetnje uklonjene. Aktivnosti nakon incidenta uključuju potpunu reviziju incidenta s uključenim sudionicima i događajima. Revizije su bitne kako bi istaknule specifične zadatke i radnje koje su imale pozitivan ili negativan utjecaj na rezultate odgovora na incident. U ovoj fazi se završava i pisani izvještaj o incidentu. Izvještaj sadrži potpunu dokumentaciju radnji tijekom incidenta, kako bi se mogao iskoristiti u pravne svrhe. Dokumentacija mora biti detaljna i imati prikaz niza događaja s fokusom na uzrok problema te ako je pisana tehnološkim terminima, oni moraju biti objašnjeni kako bi vanjski sudionici i pravnici razumjeli o čemu se radi. Na kraju je potrebno ažurirati plan odgovora na incident s novim informacijama dobivenim nakon dokumentacije i izvještaja o incidentu, kako bi sljedeći put organizacija bila spremna.[75] Brzi i efektivni odgovor na incident je ključan kod kibernetičkih napada, zbog zaustavljanja daljnjih učinaka na sustav, očuvanja ugleda organizacije, očuvanja dokaza i osiguravanja od ponovnog napada. Zajednički cilj timova digitalne forenzike i odgovora na incident je očuvanje digitalnih dokaza i optužba zločinaca, ako slučaj dođe na sud. Digitalni forenzičari često sudjeluju u procesu analize digitalnih dokaza zajedno s timom odgovora na incident, koji moraju prikupiti dokaze na način da to učine potpuno i legalno te ih na pravilan način očuvaju. Uloga digitalnog forenzičara u analizi incidenta je da pomogne u shvaćanju cijelog događaja.[76]

[75] Johansen, G. (2020). Digital Forensics and Incident Response (2nd ed.). Packt Publishing. (07.05.2020.)
[76] Understanding Digital Forensics In Cyber Penetration Testing and Incident Response. Lineal. Dostupno na: https://www.linealservices.com/understanding-digital-forensics-in-cyber-penetration-testing-and-incident-response/ (07.05.2020.)

Elektroničko otkriće (eng. *electronic discovery*) je proces traženja, lociranja, osiguravanja i pretraživanja elektroničkih podataka kako bi se mogli iskoristiti kao dokazi na sudu. Budući da je podataka previše, potrebno je odvojiti irelevantne podatke od relevantnih i tako smanjiti broj podataka. Jedan način je uklanjanje duplikata poznat kao deduplikacija, kojom alati za elektroničko otkriće identificiraju duplikate pomoću hash funkcije. Drugi način je identifikacija poznatih podataka, kojom se uspoređuju bijele liste (eng. *white list*) koje sadrže hash funkcije uobičajenih datoteka koje nisu relevantne za istragu. Ovaj način se još naziva deNISTiranje (eng. *deNISTing*) prema Nacionalnom institutu za standarde i tehnologiju (NIST) koji je razvio Nacionalnu biblioteku preporuka za softver (eng. *National Software Reference Library*). Biblioteka sadrži hash vrijednosti standardnih datoteka i uobičajenih aplikacija. U sljedećem koraku je potrebno istaknuti predmete bitne za istragu. Takvi predmeti prolaze detaljnu analizu i mogu sadržavati bitne metapodatke poput vremenskih i geografskih oznaka te autora. Za filtriranje podataka koristi se metoda pretraživanja ključnih riječi. Ovisno o alatu, moguće je pretraživati od jedne riječi do kompleksnih logičkih Boolean upita, ali nedostatak ove metode je višeznačnost riječi. Elektroničko otkriće je formalizirano kroz referentni model koji je sličan procesu digitalne istrage. Referentni model elektroničkog otkrića (eng. *Electronic Discovery Reference Model*) se sastoji od devet iterativnih procesa, u kojima se radnje ili događaji mogu ponavljati onoliko puta koliko je potrebno da bi rezultati u sljedećoj fazi bili usavršeni. Prva faza je upravljanje informacijama, u kojoj se organizacija priprema za proces elektroničkog otkrića, kako bi umanjila rizike i troškove. Identifikacija je faza u kojoj je potrebno locirati potencijalne izvore elektronički pohranjenih informacija. Očuvanje i prikupljanje je treća faza. Očuvanje je proces osiguravanja elektronički pohranjenih informacija od neprikladnih izmjena ili uništenja, a te informacije se zatim prikupljaju za daljnje korištenje u elektroničkom otkriću. Četvrta faza se sastoji od procesiranja, pregleda i analize. Procesiranje je smanjenje broja elektronički pohranjenih informacija i ako je potrebno, pretvaranje u formate koji bi olakšali pregled i analizu. Pregled se odnosi na procjenu relevantnosti i prioriteta informacija, a analiza na procjenu sadržaja i konteksta informacija. Peta faza uključuje proizvodnju, odnosno dostavljanje elektronički pohranjenih informacija drugim sudionicima u prikladnom obliku, koristeći prikladne načine isporuke. Posljednja faza je predstavljanje elektronički pohranjenih informacija publici, kako bi se otkrile nove informacije, potvrdile postojeće činjenice ili uvjerila publika.[77]

[77] Lawton, D., Stacey, R., Dodd, G. (2014). eDiscovery in digital forensic investigations. Centre for Applied Science and Technology (CAST). (07.05.2020.)

7.2. Tehnike

7.2.1. Penetracijsko testiranje

Penetracijsko testiranje je proces ispitivanja učinkovitosti mjera zaštite sustava i mreže neke tvrtke, na način da se proaktivno i promišljeno traže ranjivosti. Vještine digitalne forenzike su ključne u penetracijskom testiranju. Timovi digitalne forenzike pružaju korisne povratne informacije o nađenim ranjivostima, jer su se već susreli s njima u istragama. Takve informacije mogu biti temelj specifičnim penetracijskim testovima. Također, znanje digitalnih forenzičara se traži u raznim specijalističkim vježbama. Iako stručnjaci digitalne forenzike i stručnjaci penetracijskog testiranja imaju mnoge vještine koje su im zajedničke, digitalni forenzičari su oni koji bolje razumiju protokole i standarde te znaju pristupiti i tumačiti podatke s velikog broja uređaja. Osim toga, forenzički timovi su obučeni kako bi s lakoćom mogli pronaći uzorke i povezanosti. Iz tih razloga, digitalni forenzičari pomažu u rješavanju specifičnih izazova, povećavajući učinkovitost rezultata penetracijskog testiranja.[78]

7.2.2. Rudarenje podataka

Rudarenje podataka je proces analiziranja skrivenih uzoraka podataka, prema različitim perspektivama za kategorizaciju u korisne informacije, koje se prikupljaju i sastavljaju u zajedničkim mjestima poput skladišta podataka.[79] U kontekstu digitalne forenzike, rudarenje se odnosi na korištenje forenzičkih tehnika na velikom skupu podataka kako bi se našli relevantni uzorci ili manipuliranje velikim skupovima podataka kako bi se izvukle korisne informacije. Rudarenje podataka se koristi u poslovnim trendovima, zbog digitalizacije poslovnih operacija i povećanja obujma podataka. U digitalnoj forenzici, stručnjaci moraju prepoznati relevantne podatke tehnikama rudarenja podataka, kao što su čišćenje (eng. *pruning*) i grupiranje (eng. *clustering*). Iako rudarenje podataka nije forenzička tehnika, korisna je u istrazi jer štedi vrijeme, odnosno poznavanje tehnika rudarenja podataka može biti od velike važnosti u istragama koje ovise o vremenu.[80]

---

[78] Understanding Digital Forensics In Cyber Penetration Testing and Incident Response. Lineal. Dostupno na: https://www.linealservices.com/understanding-digital-forensics-in-cyber-penetration-testing-and-incident-response/ (08.05.2020.)

[79] Data Mining. Techopedia. Dostupno na: https://www.techopedia.com/definition/1181/data-mining (08.05.2020.)

[80] Forensics Tehniques Part 2. Infosec. Dostupno na : https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/forensic-techniques-part-2/ (07.05.2020.)

7.2.3. Ostale tehnike

Još neke od tehnika koje se koriste u digitalnoj forenzici su analiza grafičkih slika (eng. *graphical image analysis*), povezivanje događaja (eng. *event correlation*), testiranje u sigurnosnoj okolini (eng. *sandboxing*), kriptoanaliza i stegoanaliza (eng. *steganalysis*). Analiza grafičkih slika je prikupljanje informacija iz slika u svrhu forenzičke istrage. Slike mogu sadržavati metapodatke, MIME oznaku (eng. *Multipurpose Internet Mail Extension*) za identificiranje vrste podatka i geografsku oznaku lokacije. Također, analizom se može utvrditi je li slika izmijenjena. Povezivanje događaja je analiza zapisa aktivnosti mreže kako bi se uspostavio redoslijed događaja. Stručnjaci u digitalnoj forenzici analiziraju zapise aktivnosti određene mreže koji sadrže detalje o prometu na mreži, kako bi otkrili koji događaj je doveo do kvara, propusta ili ugrožavanja sigurnosti. Testiranje u sigurnosnoj okolini je proces u kojem se sumnjivi programi pokreću u izoliranom okruženju. Sigurnosni okviri su sigurna virtualna okruženja koja se koriste za testiranje programa iz neutvrđenih izvora i nadziranje prijetnji nepouzdanih programa. Takvi virtualni strojevi nemaju pristup mreži kako bi ograničili širenje virusa. Kriptoanaliza i stegoanaliza se odnosi na dešifriranje podataka koji su sakriveni kriptografijom ili steganografijom. Dešifriranje podataka je jedna od najstarijih tehnika koja se koristila prije izuma računala. Kriptoanaliza je proces dešifriranja podataka koji su skriveni šifrom, a stegoanaliza je proces traženja skrivenih podataka u običnim porukama ili datotekama. Razlika ovih tehnika je u tome kako je poruka šifrirana, odnosno podaci skriveni kriptografijom nemaju smisla i pojedinac može shvatiti da je poruka šifrirana, dok steganografija skriva podatke u smislenim porukama, tekstualnim i zvučnim datotekama te najčešće slikama.[81]

[81] Forensics Tehniques Part 2. Infosec. Dostupno na : https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/forensic-techniques-part-2/ (07.05.2020.)

8. Digitalni forenzičar

Digitalni forenzičar ima nekoliko bitnih obaveza kada provodi istragu. On je taj koji potvrđuje ili odbacuje tvrdnju o tome je li mreža, izvor ili sustav ugrožen. Zatim, određuje veličinu štete nastale napadom i odgovora na pitanja poput tko, što, kada, gdje, kako i zašto. Prikuplja podatke na pravilan način i analizira dokaze, nakon čega piše izvještaj o istrazi. Na kraju, predstavlja dokaze i slučaj na sudu. Drugim riječima, vodi se metodologijom procesa digitalne istrage.[82] Digitalni forenzičar je netko tko ima želju pratiti dokaze i riješiti slučaj virtualno. Kada se dogodi neki kibernetički napad u tvrtki, moguće je da dođe do krađe podataka te tada digitalni forenzičar otkriva kako je napadač dobio pristup mreži, gdje je napao mrežu i što je napravio na mreži, odnosno je li ukrao neke podatke ili postavio zlonamjerni program. U takvoj situaciji, uloga digitalnog forenzičara je vratiti podatke poput dokumenata, fotografija i elektroničke pošte s tvrdih diskova ili drugih uređaja za pohranu, koji su obrisani, oštećeni ili izmijenjeni. Drugi nazivi su istražitelj zločina informacijske sigurnosti, inženjer/ istražitelj/ stručnjak/ analitičar/ ispitivač/ tehničar digitalne forenzike, stručnjak za računalne ili digitalne zločine. Zadaci digitalnog forenzičara su identifikacija, dobivanje pristupa i osiguravanje uređaja ili sustava, rekonstrukcija, kopiranje podataka, vraćanje informacija te procjena vjerodostojnosti i cjelovitosti podataka, dokumentiranje metapodataka, prikupljanje podataka na legalan način, osiguravanje kontrole bilježenja istrage, osiguravanje dokaza i pisanje strukturiranih izvještaja prihvatljivih na sudu, svjedočenje na sudu, provođenje istrage u skladu s državnim zakonima i međunarodnim forenzičkim standardima te savjetovanje i treniranje osoblja u forenzici. Također, bavi se i nadgledanjem i testiranjem sigurnosti mreže ili sustava pojedine tvrtke ili organizacije. Iz tog razloga, mora biti u toku s aktualnim, prošlim i budućim temama kibernetičke sigurnosti. Također, trebao bi savjetovati tvrtke, organizacije i agencije o ranjivostima sustava i mjerama zaštite. I na kraju, trebao bi usavršavati svoje vještine i dijeliti svoje znanje s kolegama.[83] Digitalni forenzičar bi trebao imati želju za stalnim učenjem i usavršavanjem u informacijskim tehnologijama, dobre komunikacijske i analitičke vještine te vještine u rješavanju problema, ali i iskustvo u informatici ili kriminalistici.[84]

[82] Prasad, A., Pande, J. (2016). Digital Forensics. Uttarakhand Open University. (16.05.2020.)
[83] How to become a Computer Forensics Investigator. Infosec. Dostupno na : https://resources.infosecinstitute.com/job-titles/computer-forensics-investigator/ (16.05.2020.)
[84] Computer Forensics Investigator: Career Guide. Criminal Justice Degree Schools. Dostupno na: https://www.criminaljusticedegreeschools.com/criminal-justice-careers/computer-forensics-investigator/ (16.05.2020.)

8.1. Formalno obrazovanje

Zakoni i primjena prava su drugačiji u Americi nego u Europi, ali i ustroj kriminalističkih agencija se znatno razlikuje. Popularnost digitalne forenzike u Americi raste te se otvaraju obrazovne ustanove i studijski programi vezani za digitalnu forenziku. Neki od fakulteta koji nude diplomski studij su Sveučilište Carnegie Mellon u Pennsylvaniji, Sveučilište John Hopkins u Marylandu, Sveučilište Purdue u Indiani, Sveučilište u Bostonu i Rochester institut tehnologije u New Yorku. Ovi fakulteti nude kolegije: moderna kriptografija, mrežna sigurnost, etičko hakiranje, privatnost na računalu, operacijski sustavi, teorija kompleksnosti, arhitektura računala, dizajn i analiza algoritama, penetracijsko testiranje i druge.[85] U Europi također postoje obrazovne ustanove na kojima je moguće završiti studij za digitalnu forenziku. Sveučilišta u Engleskoj nude studije poput preddiplomskog studija računalne sigurnosti i forenzike na Sveučilištu Greenwich u Londonu, diplomskog studija istrage kibernetičkog zločina na Sveučilištu u Lancashireu i poslijediplomskog studija računalstva na Sveučilištu u Birminghamu. Također, postoje i studiji u Irskoj, Škotskoj, Walesu, Norveškoj, Švedskoj i Nizozemskoj. Njemačka ima poslijediplomski studij digitalne forenzike na nekoliko sveučilišta.[86] U Hrvatskoj je 2018. godine pokrenut prvi diplomski stručni studij Informacijske sigurnosti i digitalne forenzike. Kompetencije koje student stječe završetkom ovog studija su primjena informacijsko-komunikacijskih tehnologija, implementacija, upravljanje i organiziranje sustavima informacijske zaštite, organiziranje i upravljanje digitalno forenzičkim analizama i primjena zakonskih osnova informacijske sigurnosti i digitalne forenzike. Neki od kolegija koje ovaj studij nudi su mrežna forenzika, forenzika zlonamjernih programa i mobilnih uređaja, informacijska sigurnost, sigurnost web aplikacija i sigurnost računalnih mreža, zakonska osnova digitalne forenzike, primijenjena kriptografija, etičko hakiranje, skripte i objektni jezici za forenziku.[87] Osim navedenog studija, Fakultet elektrotehnike i računalstva u Zagrebu i Sveučilišni odjel za forenzične znanosti na Sveučilištu u Splitu nude kolegij Računalna forenzika na diplomskoj razini.[88]

[85] Best Masters in Computer Forensics Degrees. College Choice. Dostupno na: https://www.collegechoice.net/rankings/best-masters-in-computer-forensics-degrees/ (16.05.2020.)
[86] Education. Forensics Focus. Dostupno na: https://www.forensicfocus.com/education/#europe (16.05.2020.)
[87] Digitalna forenzika – diplomski. Tehničko veleučilište u Zagrebu. Dostupno na: https://www.tvz.hr/studiji/digitalna-forenzika/diplomski (16.05.2020.)
[88] Program. Sveučilišni odjel za forenzične znanosti. Dostupno na: http://forenzika.unist.hr/Nastava/Diplomskisveu%c4%8dili%c5%a1nistudijforenzike/Program/tabid/498/Default.aspx (16.05.2020.)

8.2. Neformalno obrazovanje

Osim formalnog obrazovanja, postoji i neformalno, koje uključuje razne tečajeve, ispite i certifikate. Ono može biti u učionici, laboratoriju, uživo, a danas su sve popularniji tečajevi i certificiranja na mreži, odnosno *online*. EC-Council ili International Council of E-Commerce Consultants je među vodećim organizacijama za certificiranje u kibernetičkoj sigurnosti. Nudi certificiranje iz dvadesetak područja kibernetičke sigurnosti, a najpoznatiji programi su etički haker, analitičar sigurnosti, penetracijski tester, arhitekt za obranu mreže i računalni forenzičar. Osim certificiranja, EC-Council drži i svoje *online* sveučilište i nudi preddiplomski i diplomski studij kibernetičke sigurnosti. Neki od kolegija na preddiplomskoj razini su osnove sigurnosti informacijskih sustava, pravna pitanja u kibernetičkoj sigurnosti, kontrola pristupa, kibernetičko ratovanje, socijalna psihologija i osnove programskog jezika Python. Diplomski studij ima pet specijalizacija: analitičar sigurnosti, arhitekt sigurnosti oblaka, digitalna forenzika, upravljanje incidentima i trajnost poslovanja te izvršno rukovodstvo u osiguravanju informacija.[89] EC-Council u suradnji s visokim učilištem Algebra nudi nekoliko programa za certificiranje u Zagrebu. Trenutno su aktualna certificiranja za etičkog hakera, analitičara sigurnosti i licenciranog penetracijskog testera te digitalnog forenzičara. Također, u ponudi još imaju certificiranje za sigurnog programera i sigurnog korisnika računala.[90] Osim službenih ustanova, postoje i platforme za *online* učenje, koje nude video zapise, video pozive, vježbe i literaturu u sklopu tečajeva. Neke od tih platforme nude i diplome za završetak tečajeva, ali te diplome imaju manju vrijednost od certifikata. Neke od tih platformi su Udemy (https://www.udemy.com/) i LinkedIn Learning platforma (https://www.linkedin.com/learning/). Obrazovanje je prvi korak u karijeri digitalnog forenzičara, bilo ono formalno ili neformalno, potrebno je kako bi digitalni forenzičar uspješno izvršio svoje obaveze i zadatke.

[89] Degrees. EC-Council. Dostupno na: https://www.eccouncil.org/ (17.05.2020.)
[90] EC-Council. Algebra. Dostupno na: https://www.algebra.hr/certifikacijski-seminari/tag/ec-council/ (17.05.2020.)

9. Digitalni dokazi

Digitalni dokazi su ključni dio svake istrage u digitalnoj forenzici. U pravu dokazi su neke činjenice, potvrđenja ili zaključci koji proizlaze iz ukupne procesne građe i koji zajedno utječu na izricanje odluke ili presude.[91] Digitalni ili elektronički dokazi su informacije pohranjene ili prenošene u digitalnom obliku koje se mogu iskoristiti na suđenju. Prije nego što digitalni dokaz bude prihvaćen na sudu, mora se odrediti je li relevantan te vjerodostojan. Također, mora se odrediti je li kopija dokaza prihvatljiva ili je potreban izvorni dokaz. Digitalni dokazi određuju povezanost napadača, žrtve i mjesta zločina. Dva pravila su povezana s digitalnim dokazima, a to su Locardovo načelo i pravilo najboljeg dokaza. Kao što je već navedeno, Locardovo načelo određuje da će zločinac nesvjesno ostaviti nekakav trag na mjestu zločina. Pravilo najboljeg dokaza je uspostavljeno kako ne bi došlo do izmjene dokaza, namjerno ili nenamjerno. Ono navodi da sud daje prednost izvornim dokazima, prije kopija. Kopija će se prihvatiti ukoliko zadovolji sljedeće uvjete: izvorni dokaz je izgubljen ili uništen u vatri, poplavi ili drugoj prirodnoj katastrofi, a može uključivati i nemarnost zaposlenika ili osoblja. Drugi uvjet je da je izvorni dokaz uništen u normalnom tijeku radnog procesa, a treći da je izvorni dokaz u vlasništvu treće strane koja je izvan sudske moći. Pravilo je olakšano na način da se duplikati mogu prihvatiti, osim ukoliko dolazi do pitanja vjerodostojnosti ili ukoliko prihvaćanja duplikata u okolnostima ne bi bilo pošteno.

Karakteristike digitalnih dokaza su prihvatljivost, pouzdanost, potpunost i vjerodostojnost. Osim navedenog, moraju biti i uvjerljivi i razumljivi sudcima. Prihvatljivost znači da dokaz mora biti potvrđen u zakonima. Mora postojati povezanost dokaza i činjenica. Digitalni dokazi često nisu prihvaćeni na sudu, jer su prikupljeni bez odobrenja. Neke pravne nadležnosti zahtijevaju nalog za prikupljanje, zapljenu i analizu digitalnih dokaza. To predstavlja problem jer se mogu pronaći dokazi drugih zločina, koji nisu povezani s trenutnom istragom. Pouzdanost se odnosi na sam izvor ili porijeklo dokaza. Digitalni dokaz je potpun ukoliko dokazuje radnje zločinca i tako pomaže u zaključivanju istrage. Vjerodostojan dokaz je stvaran dokaz i povezan je sa zločinom ili incidentom. Forenzičar mora dokazati vjerodostojnost digitalnog dokaza tako da objasni pouzdanost računalne opreme, način na koji su osnovni podaci izvorno uneseni, mjere koje su proveli kako bi osigurali točnost unesenih podataka, metode pohrane podataka i predostrožnosti koje sprječavaju gubitak podataka, pouzdanost računalnih programa koji obrađuju podatke i mjere

[91] Dokaz. Enciklopedija Leksikografskog zavoda Miroslav Krleža. Dostupno na: http://enciklopedija.lzmk.hr/clanak.aspx?id=8423 (22.05.2020.)

koje su proveli da bi potvrdili točnost programa.[92] Digitalni dokazi su često skriveni poput otisaka prstiju, mogu premašiti pravne granice lako i brzo, osjetljivi su i moguće ih je lako izmijeniti, oštetiti ili uništiti te ponekad ovise o vremenu. Oni su temelj procesa digitalne istrage jer je potrebno identificirati, prikupiti, očuvati, dokumentirati, analizirati i prenijeti digitalne dokaze. [93]

9.1. Izvori digitalnih dokaza

Računalni sustavi su jedan od izvora digitalnih dokaza, a oni mogu biti otvoreni računalni sustavi, komunikacijski sustavi i ugrađeni računalni sustavi (eng. *embedded computer system*). Otvoreni računalni sustavi su zapravo računala ili sustavi koji se sastoje od tvrdih diskova, tipkovnica i ekrana, poput prijenosnih računala, stolnih računala ili poslužitelja. Zbog povećanja mogućnosti pohrane, ovi sustavi su bogati izvori digitalnih dokaza. Jedna datoteka može sadržavati niz informacija, poput toga kada i gdje je napravljena te tko ju je napravio. Komunikacijski sustavi su tradicionalni telefonski sustavi, bežični telekomunikacijski sustavi, Internet i mreže općenito. Telekomunikacijski sustavi su izvor SMS/MMS poruka, dok je Internet izvor elektroničke pošte. Informacije o tome kada je poruka ili pošta poslana, tko ju je poslao i što sadrži, su jako bitne u digitalnoj istrazi. Kako bi došli do nekih dokaza, digitalni forenzičari moraju analizirati i zapise na poslužitelju i usmjerniku. Ugrađeni računalni sustavi su mobilni uređaji, pametne kartice i drugi pametni ugrađeni uređaji. Mobilni uređaji sadrže podatke o komunikaciji, fotografije, video i audio zapise. Sustavi za navigaciju sadrže informacije o tome gdje se uređaj ili vozilo nalazilo. Mikrovalne pećnice i drugi kuhinjski aparati danas funkcioniraju bežično, putem mreže, i oni su bitan izvor digitalnih dokaza.[94]

Digitalni dokazi s računalnih sustava mogu biti datoteke koje je korisnik kreirao (eng. *user-created files*), zaštitio (eng. *user-protected files*), datoteke koje je računalo kreiralo i ostale datoteke. Datoteke koje je korisnik kreirao su razni adresari, audio i video zapisi, kalendari, baze podataka, dokumenti i tekstualne datoteke, datoteke elektroničke pošte, slikovne i grafičke datoteke, proračunske tablice i druge datoteke povezane s radnjama korisnika. Datoteke koje je korisnik zaštitio često su znak sakrivanja dokaza. Korisnik može šifrirati datoteke ili sakriti ih na čudna mjesta na disku pod drugačijim imenom. To su datoteke koje su kompresirane, šifrirane, sakrivene, preimenovane, zaštićene šifrom ili datoteke nastale

[92] Prasad, A., Pande, J. (2016). Digital Forensics. Uttarakhand Open University. (22.05.2020.)
[93] Ashcroft, J. (2001). Electronic Crime Scene Investigation: A Guide for First Responders. U.S. Dept. of Justice, Office of Justice Programs, National Institute of Justice. (22.05.2020.)
[94] Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press. (22.05.2020.)

steganografijom. Datoteke koje je računalo kreiralo su sigurnosne kopije, konfiguracijske datoteke, kolačići, skrivene datoteke, datoteke povijesti, zapisne datoteke, sustavne datoteke i privremene datoteke. Ostali dokazi na računalima su računalno vrijeme, datum i zaporka, obrisane datoteke, skrivene particije, metapodaci, ostale particije, rezervirani prostori, nedodijeljeni prostor, informacije o softveru i drugi. Mobilni uređaji su izvor dokaza poput imenika, poruka, kalendara, poziva, dokumenata, elektroničke pošte, osobnih podataka, slikovnih, audio i video zapisa. Mrežni uređaji poput mrežne kartice, usmjernika, preklopnika i poslužitelji su izvor dokaza poput MAC i IP adresa, konfiguracijskih datoteka, topologija, tablica usmjeravanja i otvorenih priključaka. Globalni pozicijski sustav je izvor dokaza poput adrese korisnika, zadnjih destinacija, zapisa putovanja, koordinata destinacija i drugih.[95]

9.2. Izazovi

Prikupljanje digitalnih dokaza je posao digitalnog forenzičara koji se mora obavljati s velikom opreznošću. Taj dio istrage nailazi na mnoge izazove. Za početak, digitalni dokazi su vrsta dokaza koji su neuredni i kompliciran za rukovati. Na primjer, tvrdi disk se sastoji od velike količine nerazvrstanih podataka, odnosno pomiješanih informacija koje su naslagane jedna na drugu. Samo dio tih informacija će biti relevantan za istragu, pa je potrebno izvući korisne dijelove, spojiti ih i prevesti ih u oblik koji se može protumačiti. Drugi izazov je što su digitalni dokazi apstrakcija nekog digitalnog objekta ili događaja. Na primjer, kada osoba naredi računalu da izvrši neki zadatak poput slanja elektroničke pošte, ona vidi samo dio onoga što se dogodilo, odnosno samo poruku elektroničke pošte i zapis poslužitelja. Također, vraćanje obrisanih datoteka s medija za pohranu pomoću forenzičkog alata uključuju nekoliko slojeva apstrakcije od magnetskih polja na disku do slova i brojeva koje vidimo na ekranu. To znači da nikad ne vidimo stvarne podatke nego samo prikaz tih podataka te svaki sloj apstrakcija može predstaviti nove pogreške. Treći izazov je taj što digitalni dokazi ovise o okolnostima, što otežava povezivanje računalne aktivnosti s pojedincem. Iz tog razloga, digitalni dokaz mora biti jedna cijela komponenta čvrste istrage. Ako istraga ovisi o jednom zasebnom obliku ili izvoru digitalnog dokaza, poput vremenskih oznaka na datotekama, onda je slučaj neprihvatljiv. Bez dodatnih informacija bi se moglo raspravljati o tome je li netko drugi koristio računalo u isto vrijeme, pogotovo ako računalo nema zaporku ili ima slab sigurnosni mehanizam. Moguće je manipulirati digitalnim dokazima te ih je lako za uništiti, što predstavlja još jedan izazov za digitalne forenzičare. Zločinci mogu namjerno izmijeniti

[95] Ashcroft, J. (2001). Electronic Crime Scene Investigation: A Guide for First Responders. U.S. Dept. of Justice, Office of Justice Programs, National Institute of Justice. (22.05.2020.)

ili uništiti dokaze, a forenzičari slučajno kod prikupljanja. Digitalni dokazi imaju i svojstva koja ublažavaju takve probleme. Najbolja praksa je izrada kopije dokaza za analizu, kako ne bi došlo do izmjene ili uništenja dokaza. Također, postoje alati koji mogu odrediti je li dokaz izmijenjen tako što se uspoređuje s originalnom kopijom. Treće svojstvo je težina uništavanja digitalnih dokaza, odnosno iako je datoteka obrisana ili tvrdi disk formatiran, digitalne dokaze je moguće vratiti. Također, iako zločinac pokuša uništiti digitalne dokaze, moguće je da ne uništi sigurnosne kopije i ostatke dokaza za koje nije bio svjestan da postoje.[96]

9.3. Analiza dokaza

Digitalni dokazi se mogu analizirati na tri načina: vremenskom, relacijskom i funkcionalnom analizom. Vremenska analiza je proces povezivanja poznatih događaja s oznakama datuma i vremena digitalnog objekta. Rezultat povezivanja je vremenska crta aktivnosti na računalu ili drugom uređaju. Relacijska analiza je proces utvrđivanja povezanosti digitalnih objekata s različitim elementima istrage. Povezanost ili jačina povezanosti se utvrđuje brojem veza među objektima. Objektima se pridodaje vrijednost zajedničkim karakteristikama te oni s visokim vrijednostima dijele zajedničke karakteristike, odnosno imaju bolju povezanost.

Funkcionalna analiza je proces u kojem se dokumentiraju načini funkcioniranja objekata. Također, moguće je izrađivanje dijagrama i grafikona funkcija kako bi se otkrile sličnosti i veze između objekata. Digitalni forenzičar može koristiti sve tehnike analize kako bi dokazao zločin, ali mora biti objektivan. Svaki dokaz mora biti provjeren i potvrđen, mora biti vezan za osumnjičenika i ne smije biti dvosmislen. Analiza dokaza određuje vlasništvo, upotrebu, pristup i znanje o dokazu. Bitno je odrediti vezu između dokaza i osumnjičenika, a forenzičar bi uvijek trebao pokušati dokazati vlasništvo samog dokaza. Također, bitno je odrediti na koji način je osumnjičenik koristio dokaz. Forenzičar mora dokazati da je osumnjičenik pristupio samom dokazu te na koji način je to napravio. Ponekad nije moguće dokazati vlasništvo, upotrebu i pristup dokazu pa digitalni forenzičar mora demonstrirati kako je osumnjičenik imao saznanja o dokazu.[97]

[96] Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press. (22.05.2020.)
[97] King, G. (2006). A Forensic Investigation Plan and Cookbook. SANS Institute. (22.05.2020.)

10. Digitalna forenzika i pravo

Digitalna forenzika, kao relativno mlada grana forenzike, nije široko prihvaćena u pravnom sustavu, zakonima i legislativama. Ipak, neki pravni sustavi su donijeli zakone koji se tiču kibernetičkog kriminala, privatnosti i sigurnosnih napada općenito. Takvi zakoni donose stroga pravila vezana za optužbe počinitelja i postupke rukovanja s dokazima, kao što su prikupljanje i prikazivanje dokaza na sudu. U svijetu se počelo primjenjivati i pravo informatičkih tehnologija ili kibernetičko pravo. Kibernetičko pravo pokriva uglavnom bilo kakve oblike digitalnih informacija, uključujući kibernetičku sigurnost i elektroničko poslovanje. Kibernetičko pravo uključuje i Internet pravo, koje obuhvaća zločine nastale korištenjem Interneta. U nekim pravosuđima postoje zakoni o cenzuri naspram slobode izražavanja, pristupu informacija i privatnosti podataka.[98]

Zločini koji su obuhvaćeni kibernetičkim zakonima mogu se svrstati u tri kategorije: seksualni zločini, zločini protiv osoba i prijevare, odnosno drugi financijski zločini. Najčešće putem Interneta, seksualni zločini su dječja pornografija, odnosno iskorištavanje i zlostavljanje djece te prostitucija. Zločini protiv osoba su smrt, nasilje u obitelji, krađa podataka, prijetnje, uznemiravanje i uhođenje, putem elektroničke pošte, društvenih medija ili općenito putem Interneta. Prijevare i financijski zločini su aukcijske prijevare, upadi u računalo, ekonomske prijevare, iznude, kockanje, krađa identiteta, prodaja droge i drugih ilegalnih opojnih sredstava, piratstvo i telekomunikacijske prijevare.[99]

[98] Prasad, A., Pande, J. (2016). Digital Forensics. Uttarakhand Open University. (30.05.2020.)
[99] Ashcroft, J. (2001). Electronic Crime Scene Investigation: A Guide for First Responders. U.S. Dept. of Justice, Office of Justice Programs, National Institute of Justice. (30.05.2020.)

10.1. Europa

Države u Europi imaju različit pravni sustav od onog u Americi. Neke se države drže općeg prava (eng. *common law*), dok su druge usvojile sustav građanskog prava (eng. *civil law*). Europske unija i Vijeće Europe zahtijevaju implementaciju smjernica kibernetičkog prava od svojih država članica. Vijeće Europe je 2001. godine sastavilo Konvenciju o kibernetičkom zločinu, a ona se primjenjuje od 2004. godine. Osim europskih država, Konvenciju su potpisale i države Sjeverne i Južne Amerike, Afrike i Azije. Konvencija o kibernetičkom kriminalu je međunarodni standard postupanja s kibernetičkim kriminalom i digitalnim dokazima. Koristi se kao smjernica za uspostavljanje nacionalnih legislativa o kibernetičkom zločinu te kao okvir za međunarodnu suradnju među članicama. Konvencija previđa kriminalizaciju ponašanja poput ilegalnog pristupa, ometanja podataka i sustava, prijevara putem računala i dječje pornografije te alate za učinkovitu istragu kibernetičkog zločina i osiguravanje digitalnih dokaza.[100] Konvencija razlikuje tri vrste kibernetičkog zločina: zločin u kojem je računalo objekt napada, zločin u kojem je računalo sredstvo napada i zločin u kojem je računalna mreža okolina napada. Zločini u kojima je računalo objekt napada su hakiranje, ilegalno prisluškivanje, smetnje podataka i sustava i zloupotreba uređaja. Zločini u kojima je računalo sredstvo napada su krivotvorenje i razne prijevare. Zločini u kojima je računalna mreža okolina zločina su dječja pornografija, internetsko mamljenje (eng. *online grooming*) i zločini vezani za rasizam. Ostali zločini kojima je obuhvaćena Konvencija su kršenje autorskih prava i kibernetičko maltretiranje. Ujedinjeno Kraljevstvo je 1990. godine donijelo Odluku o zloupotrebi računala, koja pokriva neovlašteni pristup računalu, neovlašteni pristup s namjerom da se počini ili olakša daljnji zločin ili djelo i neovlaštene izmjene na računalu. Europska unija je 2001. godina donijela Okvirnu odluku (eng. *Framework Decision*), koja uključuje suzbijanje prijevara i krivotvorenja te prekršaje vezane za računala i druge uređaje. Tri godine kasnije dodane su odredbe o borbi protiv dječje pornografije, zbog povećanja takvih zločina na Internetu. Lisabonski ugovor potpisan 2007. godine od strane država članica Europske unije je poništio Okvirnu odluku i donio nove smjernice za suzbijanje kibernetičkog zločina. Lisabonski ugovor pokriva sljedeća polja zločina: terorizam, krijumčarenje ljudima, seksualno zlostavljanje žena i djece, krijumčarenje droge i oružja, korupciju, organizirani zločin i kibernetički zločin.[101]

[100] The Budapest Convention on Cybercrime: International Criminal Law and the use of Treaties. Lexology. Dostupno na: https://www.lexology.com/library/detail.aspx?g=4220b287-ac07-4a33-a711-bee235721d9f (30.05.2020.)
[101] Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press. (30.05.2020.)

10.2. Sjedinjene Američke Države

Sjedinjene Američke Države su federalni sustav, pa se iz tog razloga pravo koje se tiče kibernetičkog zločina dijeli u federalno i državno pravo. Federalno pravo je jedinstven, sveobuhvatan sustav koji se primjenjuje na teritorijalnom pravosuđu Sjedinjenih Država. Državno kibernetičko pravo je drugačije, zakoni koji se tiču kibernetičkog zločina svih država se primjenjuju jedino unutar teritorijalnog pravosuđa države. Zakon o računalnim prijevarama i zlouporabi je donesen 1986. godine kao dio federalnog prava. Od tada je proširen raznim dopunama i izmjenama, zbog napredovanja tehnologija i ispravljene su neke stavke koje se postojala u ranijim inačicama Zakona. Zakon primarno zabranjuje neovlašten pristup računalu i mreži. Također, pokriva i zločine poput prenošenja zlonamjernih programa, napade uskraćivanjem usluge, trgovanje zaporkama i korištenje računala u svrhu prijevare ili iznude.

Jedan od članaka Zakona govori o nekoliko mogućih prekršaja. Prvi se odnosi na svjesno prenošenje programa, informacija, kôda ili naredbe zbog namjere da se ošteti računalo. Također, odnosi se na one koji izrađuju i šire viruse, crve i druge vrste zlonamjernih programa te na one koji distribuirano uskraćuju uslugu. Drugi prekršaj se odnosi na hakiranje ili neovlašteni pristup računalu ili računalnom sustavu. Zločin može biti namjerno pristupanje računalu bez odobrenja i namjerno izazivanje štete i namjerno pristupanje računalu bez odobrenja i slučajno izazivanje štete. Oba prekršaja se odnose na pristup vanjske osobe, koja nema ovlasti pristupati računalu ili sustavu. Još jedan prekršaj je trgovanje zaporkama ili sličnim informacijama kojima se može pristupiti računalu, a uključuje i proizvodnju, korištenje, posjedovanje ili trgovanje uređajima za neovlašteni pristup. Prekršaj je i korištenje računalnih tehnologija da bi se počinila iznuda. Ostali veći zločini pokriveni federalnim zakonima su krađa identiteta, dječja pornografija, kršenje autorskih prava i ekonomski prekršaji. Državno pravo određuje zločine neovlaštenog pristupa, prenošenja zlonamjernih programa, uskraćivanja usluge, računalne prijevare, krađe i iznude te zločine počinjenih nad djecom na razini pojedine države. Pravni sustav također slijedi ustavno pravo koje se odnosi na sveukupni teritorij država te na ustave unutar pojedine države. Ustavno pravo uključuje kibernetičke zločine kroz Četvrti i Peti amandman. Četvrtim amandmanom ograničavaju se mjesta pretraživanja i prikupljanja dokaza, a Peti amandman zabranjuje vladi prisiljavanje pojedinca na svjedočenje koje ga optužuje. Drugim riječima, Četvrti amandman stvara pravo slobode od nerazumnih pretraga i zapljena. Pretraga ili zapljena su razumni kada se provode temeljem zakonitog naloga za pretres ili uhićenje, jer pretraga predstavlja napad privatnosti

pojedinca, dok zapljena predstavlja miješanje u tuđe posjedovanje i korištenje njegove imovine. Peti amandman govori o tome da se nikoga ne može natjerati da bude svjedok protiv samog sebe, odnosno smatra se privilegijom protiv samoinkriminacije. Primjenjuje se kada je pojedinac prisiljen dati izjavu koja inkriminira samog sebe.[102]

Iz razloga što je kibernetički zločin temeljen na takvim zakonima, digitalni forenzičari moraju biti pažljivi i precizni kod prikupljanja dokaza i predstavljanja slučaja na sudu. Još jedan zakon se tiče kibernetičkih zločina, a to je Zakon o elektroničkim komunikacijama i privatnosti (eng. *Electronic Communication and Privacy Act - ECPA*), utemeljen 1986. godine. Temelji se na Federalnom zakonu o prisluškivanju (eng. *Federal Wiretap Act*) iz 1968. godine. Zakon o elektroničkim komunikacijama i privatnosti brani prava korisnika telekomunikacijskih usluga. Drugim riječima, ograničava prava davatelja telekomunikacijskih usluga na način da ne smije dati informacije o korisnikovim komunikacijama, sadržaju tih komunikacija i aktivnosti na mreži. Ipak, postoji nekoliko iznimaka u ovom Zakonu. Prva iznimka je da primatelj komunikacije može odobriti otkrivanje same komunikacije. Druga iznimka je da sudska naredba ili nalog za pretraživanje može odobriti otkrivanje informacija o komunikaciji. Treća iznimka je nesvjesno prikupljanje sadržaja komunikacije od strane davatelja usluge, a sadržaj uključuje ilegalne aktivnosti. Četvrta iznimka se odnosi na pravo davatelja usluge da štiti svoju imovinu ili uslugu. Posljednja iznimka govori da davatelj usluge smije dati sadržaj komunikacije vladinim agencijama, kada je nesvjesno prikupio sadržaj i kada vjeruje da postoji hitan slučaj i da osoba ozbiljno ozlijeđena.[103] Zakon je dorađen Zakonom o komunikacijskoj podršci za provođenje prava (eng. *Communications Assistance for Law Enforcement Act – CALEA*) 1994. godine, koje naglašava potrebu za tim da davatelji usluge osiguraju dostupnost svoje mreže agencijama za provođenje prava, zbog provođenja ovlaštenog nadzora.[104] Nakon napada na Svjetski trgovački centar (eng. *The World Trade Centar*) 11. rujna 2001. godine, Zakon je nadopunjen Patriotskim zakonom Sjedinjenih Američkih Država (eng. USA Patriot Act) i ponovno je obnovljen 2006. godine. Dvije godine kasnije, dodane su izmjene iz FISA zakona (eng. *Foreign Intelligence Surveillance Act*), koji je korišten kao pravni temelj Edwardu Snowdenu pri otkrivanja nadzornih programa 2013. godine.

[102] Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press. (31.05.2020.)
[103] King, G. (2006). A Forensic Investigation Plan and Cookbook. SANS Institute. (31.05.2020.)
[104] Johansen, G. (2020). Digital Forensics and Incident Response (2nd ed.). Packt Publishing. (31.05.2020.)

11. Primjena digitalne forenzike u Hrvatskoj

Digitalna forenzika se proširila po cijelom svijetu, pa tako i po Hrvatskoj. Razlog tome je što se broj kibernetičkih napada i računalno-sigurnosnih incidenata povećava. Nacionalni CERT (eng. *Computer Emergency Response Team*) je početkom godine počeo upozoravati na povećanje broja računalnih napada za vrijeme epidemije koronavirusa. Kibernetički napadači su koristili tehnike poput phishinga, privitaka sa zlonamjernim sadržajem, lažne poveznice i mrežne stranice, zlonamjerna preuzimanja i druge tehnike, povezane s informacijama i sadržajem o koronavirusu kako bi uspješno napali pojedince i tvrtke.[105] Iako Nacionalni CERT izdaje razna upozorenja, obrazuje građane i obrađuje računalno-sigurnosne incidente, ne obavlja posao digitalnog forenzičara. CERT je organizacija koja reagira na računalno-sigurnosne incidente te preventivnim djelovanjem radi na poboljšanju računalne sigurnosti informacijskih sustava. Nacionalni CERT se ne bavi operativnim rješavanjem problema i brigom o sigurnosti pojedinih sustava, kažnjavanjem problematičnih korisnika, arbitražom u sporovima i pokretanjem kaznenih prijava.[106] To su aktivnosti kojima se bavi pravosuđe, službe za očuvanje javnog reda i sigurnosti, a među kojima je i digitalna forenzika. Razvoj digitalne forenzike u Hrvatskoj raste, a to je vidljivo u djelatnostima zakonodavnih službi i privatnih tvrtki, ali i u obrazovanju, otvorenjem specijalističkog diplomskog studija Informacijska sigurnost i digitalna forenzika na Tehničkom veleučilištu u Zagrebu te raznim konferencijama u području digitalne forenzike. Tehničko veleučilište u Zagrebu i tvrtka iStart IT u suradnji sa Zagrebačkim inovativnim centrom organiziraju konferencije o kibernetičkoj sigurnosti i digitalnoj forenzici. Prošle godine teme su bile implementacija digitalnog laboratorija, tehnike sigurnog programiranja, kibernetička sigurnost u big data okruženju i druge.[107] Tvrtka INsig2 organizira svake godine internacionalnu konferenciju DataFocus, koja se sastoji od tri tematske cjeline: pravna, istražiteljska i tehnička. Pravna se sastoji od predavanja o pravnom aspektu prikupljanja, obrade i predstavljanja digitalnih dokaza u kaznenim i upravnim postupcima, istražiteljska se sastoji od predavanja o tehničkom aspektu pronalaženja, očuvanja i obrade digitalnih dokaza, a tehnička se sastoji od prezentacija o proizvodima, uslugama i trendovima iz područja digitalne forenzike.[108]

[105] Budite oprezni - COVID-19 iskorištava se i u kibernetičkim napadima. Nacionalni CERT. Dostupno na: https://www.cert.hr/budite-oprezni-covid-19-iskoristava-se-i-u-kibernetickim-napadima/ (04.06.2020.)
[106] O Nacionalnom CERT-u. Nacionalni CERT. Dostupno na: https://www.cert.hr/onama/ (04.06.2020.)
[107] Konferencija kibernetička sigurnost i digitalna forenzika. iStart IT. Dostupno na: http://www.cyber-security-conf.istart-it.hr/ (04.06.2020.)
[108] DataFocus. INsig2. Dostupno na: https://www.insig2.com/hr/konferencija/datafocus (04.06.2020.)

11.1. Zakonske regulative

Zakoni, kao i u svijetu, također imaju velik utjecaj na digitalnu forenziku u Hrvatskoj. Hrvatska je 2002. godine ratificirala Konvenciju o kibernetičkom kriminalu Europskog vijeća.[109] Osim Konvencije, 2015. godine donesena je i Nacionalna strategija kibernetičke sigurnosti. Strategija, zajedno s Akcijskim planom provedbe nastoje postići nekoliko ciljeva: sustavni pristup u primjeni i razvoju nacionalnog zakonodavnog okvira kako bi se uzela u obzir nova, kibernetička dimenzija društva, provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora, uspostavljanje učinkovitijeg mehanizma razmjene, ustupanja i pristupa podacima potrebnim za osiguravanje više razine opće sigurnosti u kibernetičkom prostoru, jačanje svijesti o sigurnosti svih korisnika kibernetičkog prostora, poticanje razvoja usklađenih obrazovnih programa, poticanje istraživanja i razvoja, u području e-usluga i sustavni pristup međunarodnoj suradnji u području kibernetičke sigurnosti. Strategija se odnosi na sljedeća područja kibernetičke sigurnosti: elektronička komunikacijska i informacijska infrastruktura i usluge, koja je podijeljena na javne elektroničke komunikacije, elektroničku upravu i elektroničke financijske usluge, kritična komunikacijska i informacijska infrastruktura i upravljanje kibernetičkim krizama, kibernetički kriminalitet, zaštita podataka, tehnička koordinacija u obradi računalnih sigurnosnih incidenata, međunarodna suradnja i obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru.[110]

Europska unija je 2016. godine donijela NIS direktivu (eng. Network and Information Systems), koja propisuje sustavno upravljanje kibernetičkom sigurnošću nacionalnih infrastruktura. Hrvatska je direktivu uvela izglasavanjem Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Zakon zahtjeva uspostavu tehničkih i organizacijskih mjera za zaštitu ključne infrastrukture u skladu s rizicima. Zakon se primjenjuje na osam sektora: energetika, prijevoz, bankarstvo, infrastrukture financijskog tržišta, zdravstveni sektor, opskrba i distribucija vode, digitalna infrastruktura i poslovne usluge za državna tijela. Osim Zakona, propisana je i Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Zakon daje generalni okvir za usklađivanje, a Uredba donosi nekoliko konkretnih tehničkih i organizacijskih mjera za

[109] Chart of signatures and ratifications of Treaty 185. Council of Europe. Dostupno na: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=27HuKgpK (04.06.2020.)

[110] Kibernetička sigurnost. Ministarstvo unutarnjih poslova. Dostupno na: https://mup.gov.hr/istaknute-teme/nacionalni-programi-i-projekti/nacionalne-strategije/kiberneticka-sigurnost/222335 (04.05.2020.)

implementacije te načina provedbe tih mjera. Generalno, od samih operatora se očekuje da uspostave i održavaju sustave upravljanja kibernetičkom sigurnošću kako bi osigurali što kvalitetniju zaštitu od kibernetičkih napada.[111]

Ostali zakoni u području kibernetičke sigurnosti i digitalne forenzike su Zakon o informacijskoj sigurnosti, Zakon o tajnosti podataka, Opća uredba o zaštiti podataka i Zakon o pravu na pristup informacijama. Zakon o informacijskoj sigurnosti definira pojam, mjere i standarde informacijske sigurnosti, područja informacijske sigurnosti, te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti.[112] Zakon o tajnosti podataka definira pojam klasificiranih i neklasificiranih podataka, stupnjeve tajnosti, postupak klasifikacije i deklasifikacije, pristup klasificiranim i neklasificiranim podacima, njihovu zaštitu i nadzor nad provedbom samog Zakona.[113] Opća uredba o zaštiti podataka osigurava zaštitu pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka.[114] Zakon o pravu na pristup informacijama definira pravo na pristup informacijama i ponovnu uporabu informacija koje posjeduju tijela javne vlasti, načela i ograničenja prava na pristup informacijama i ponovnu uporabu informacija, postupak za ostvarivanje i zaštitu prava na pristup informacijama i ponovnu uporabu informacija.[115]

11.2. Provedba digitalne forenzike

U Hrvatskoj se područjima digitalne forenzike i kibernetičke sigurnosti bave tijela nacionalne sigurnosti, službe javne uprave, tvrtke i detektivske agencije. Sigurnosno-obavještajna agencija navodi kao neka od područja rada kibernetičku i informacijsku sigurnost. Hrvatska je moguća meta kibernetičkih napada, a namjere napadača su prikupljanje podataka o sigurnosnim, političkim, gospodarskim i drugi procesima i prikupljanje podataka organizacija asociranih s Hrvatskom. Sigurnosno-obavještajna agencija aktivno sudjeluje u otkrivanju i suzbijanju državno sponzoriranih kibernetičkih napada. Također je zadužena za otkrivanje i sprječavanje neovlaštenog ulaska u zaštićene informacijske i komunikacijske sustave državnih tijela te odavanje klasificiranih podataka. Zbog tog razloga, intenzivno surađuje s tijelima javne vlasti, državnim institucijama te drugim institucijama i ustanovama, poput

[111] NIS Direktiva. Infigo. Dostupno na: https://www.infigo.hr/nis-direktiva-s124?t=1 (04.06.2020.)
[112] Zakon o informacijskoj sigurnosti. (NN 79/2007). Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html (04.06.2020.)
[113] Zakon o tajnosti podataka. (NN 79/2007). Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2483.html (04.06.2020.)
[114] Zakon o provedbi Opće uredbe o zaštiti podataka. (NN 42/2018). Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html (04.06.2020.)
[115] Zakon o pravu na pristup informacijama. (NN 25/2013). Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2013_02_25_403.html (04.06.2020.)

Vlade Republike Hrvatske, Uredom Vijeća za nacionalnu sigurnost, Zavodom za sigurnost informacijskih sustav, Ministarstvom unutarnjih poslova i drugima.[116] Početkom godine Europska unija je donijela odluku o dodjeli financijskih sredstava za provedbu projekta: „Jačanje kapaciteta MUP-a u borbi protiv svih oblika kibernetičkog kriminaliteta“. Cilj projekta je nabaviti potrebnu opremu i računalne alate za efikasno izvršavanje naloga za pretragom elektroničkih dokaza. Cilj edukacije je podizanje kompetencija policijskih službenika za uspješno suzbijanje kibernetičkih zločina.[117] Ministarstvo unutarnjih poslova ima Službu kibernetičke sigurnosti koja djelomično obavlja poslove digitalne forenzike, a Centar za forenzična ispitivanja, istraživanja i vještačenja „Ivan Vučetić“ ima specijaliziranu Službu za digitalnu forenziku. Služba kibernetičke sigurnosti sudjeluje u primjeni i razvoju nacionalnog zakonodavnog okvira kibernetičke sigurnosti, sustavno analizira, prati i izučava fenomenološki i etiološki aspekt kaznenih djela visokotehnološkog kriminaliteta, neposredno provodi složena kriminalistička istraživanja u domeni kaznenih djela počinjenih na štetu i pomoću računalnih sustava i mreža, kriminaliteta počinjenog zlouporabom sredstava plaćanja te iskorištavanja djece za pornografiju, ali obavlja i forenzičku analizu digitalnih dokaza.[118] Služba za digitalnu forenziku obavlja poslove vještačenja digitalnih zapisa na računalima, telefonima i svim medijima za pohranu digitalnih podataka, također poslove vezane uz izradu zakonskih i podzakonskih propisa iz djelokruga rada Službe i poslove vezane uz izradu i provedbu programa stručne osposobljenosti djelatnika.[119] Među tvrtkama koje se bave digitalnom forenzikom ističe se INsig2. Tvrtka se bavi razvojem i izradom rješenja vezanih za integriranu sigurnost te pružanjem stručnog savjetovanja i usluga u području digitalne forenzike. Njihova sigurnosna rješenja objedinjuju sklopovske i programske platforme, za privatni i javni sektor, tijela za provedbu zakona, obrambene snage, pravna tijela, međunarodne organizacije, tehnološki sektor, banke, javno zdravstvo i druge. Od područja digitalne forenzike pružaju razne usluge poput savjetovanja, obrazovanja i opremanja laboratorija.[120]

---

[116] Područja rada. Sigurnosno-obavještajna agencija. Dostupno na: https://www.soa.hr/hr/podrucja-rada/ (10.06.2020.)

[117] Aktivnosti u sklopu projekta „Jačanje kapaciteta MUP-a u borbi protiv svih oblika kibernetičkog kriminaliteta. Ministarstvo unutarnjih poslova. Dostupno na: https://mup.gov.hr/vijesti/aktivnosti-u-sklopu-projekta-jacanje-kapaciteta-mup-a-u-borbi-protiv-svih-oblika-kibernetickog-kriminaliteta/285974 (10.06.2020.)

[118] Uprava kriminalističke policije. Ravnateljstvo policije. Dostupno na: https://policija.gov.hr/uprava-kriminalisticke-policije/415 (10.06.2020.)

[119] Centar za forenzična ispitivanja, istraživanja i vještačenja "Ivan Vučetić". Ministarstvo unutarnjih poslova. Dostupno na: https://mup.gov.hr/centar-za-forenzicna-ispitivanja-istrazivanja-i-vjestacenja-ivan-vucetic-281610/281610 (10.06.2020.)

[120] Profil kompanija. INsig2. Dostupno na: https://www.insig2.com/hr/o-nama/kompanijski-profil (10.06.2020.)

12. Istraživački rad – Stavovi studenata o digitalnoj forenzici

Nakon definiranja područja digitalne forenzike, njezine primjene u svijetu i u Hrvatskoj, za potrebe ovog rada provedena je anketa „Stavovi studenata o digitalnoj forenzici“. Ciljana skupina bili su studenti fakulteta u Hrvatskoj, tehničkih, ali i netehničkih usmjerenja. Cilj istraživanja bio je dobiti uvid u informiranost studenata o digitalnoj forenzici, njihov stav o tome postoji li potreba za digitalnom forenzikom u Hrvatskoj, utječe li na privatnost podataka i kakvo je stanje kibernetičke sigurnosti u doba epidemije koronavirusa. Anketa se sastoji od četiri dijela: osobni podaci, kibernetička sigurnost u Hrvatskoj, privatnost podataka i kibernetička sigurnost u doba epidemije koronavirusa. Iz toga proizlaze četiri pretpostavke: studenti nisu dovoljno informirani o zakonima i tijelima koja se bave digitalnom forenzikom u Hrvatskoj, smatraju da je kibernetička sigurnost u Hrvatskoj ugrožena, da utječe na privatnost i da epidemija utječe na sustav kibernetičke sigurnosti. Metodom ankete i analizom dobivenih podataka, potvrđuju se ili odbijaju prethodno postavljene pretpostavke. Anketa je provedena mrežnim putem, većinom društvenim mrežama i elektroničkom poštom, a izrađena je putem alata Google Forms. Ukupno je ispitano 168 studenata, s različitih fakulteta iz cijele Hrvatske. Na početku ankete prikupljaju se osobni podaci (spol, razina studija, fakultet i smjer), kako bi anketa zadržala neku razinu anonimnosti, a koji se koriste za analizu i statistiku rezultata. Istaknuto je da je anketa anonimna te da se podaci koriste isključivo u svrhu istraživanja u diplomskom radu.

12.1. Anketna pitanja

Anketa se sastoji od ukupno 17 pitanja, od kojih se prva tri odnose na osobne podatke – spol, razinu studija te fakultet i smjer koji student pohađa. Drugi dio ankete je vezan za kibernetičku sigurnost u Hrvatskoj. Ispituje se informiranost studenata o tome tko provodi mjere protiv kibernetičkih napada, postoji li odjel za digitalnu forenziku te provode li se mjere protiv kibernetičkih napada temeljito i u dovoljnom broju. Također, od studenata se traži da označe regulative vezane za kibernetičku sigurnost. Zadnja tri pitanja vezana su uz ocjenjivanje učestalosti kibernetičkih napada, njihovih meta i motiva napada u Hrvatskoj.

Sljedeći dio vezan je za digitalnu forenziku i privatnost podataka. Ispituje se stav o utjecaju digitalne forenzike na privatnost građana te subjektivna mišljenja o tome bi li dopustili praćenje uređaja u svrhu poboljšanja mjera obrane kibernetičke sigurnosti i o tome mogu li državne službe pristupiti pojedinim podacima bez odobrenja.

Posljednji dio vezan je za kibernetičku sigurnost u doba epidemije koronavirusa. Ispituje se stav studenata o ugroženosti kibernetičke sigurnosti za vrijeme epidemije te povećanju broja napada od početka epidemije. Također, traži se subjektivno mišljenje o tome treba li više uložiti u sustav kibernetičke sigurnosti u doba epidemije. Za kraj, traži se od studenata da označe neke od kibernetičkih napada za koje su čuli ili kojih su bili žrtva, a vezani su ili su se dogodili za vrijeme epidemije.

12.2. Rezultati

Anketu je ispunilo ukupno 168 ispitanika, od kojih je najveći broj s Filozofskog fakulteta u Zagrebu. Od ostalih fakulteta, ispitanici su studenti s Fakulteta elektrotehnike i računarstva u Zagrebu, Tehničkog veleučilišta u Zagrebu, Fakulteta prometnih znanosti u Zagrebu, Pravnog fakulteta u Zagrebu i drugih. Od 168 ispitanika 84 (50%) ih pohađa preddiplomski studij, 79 (47%) ih pohađa diplomski studij, a 5 (3%) ih pohađa poslijediplomski studij. Njih 94 (56%) je ženskoga spola, dok ih je 74 (44%) muškoga spola.

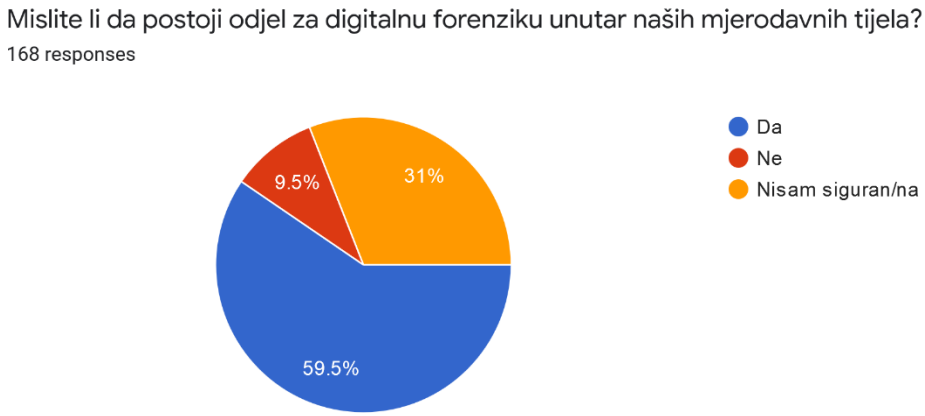
12.2.1. Kibernetička sigurnost u Hrvatskoj

1. Prema Vašem mišljenju, tko provodi mjere protiv kibernetičkih napada u Hrvatskoj?

Ovo je bilo otvoreno pitanje te su studenti mogli napisati bilo koju instituciju, tijelo ili tvrtku. Najčešći odgovori su Sigurnosno-obavještajna agencija, Ministarstvo unutarnjih poslova, policija, Nacionalni CERT, CARNET, SRCE, Vojna sigurnosno-obavještajna agencija, razni odjeli unutar policije, odjeli unutar privatnih tvrtki, Zavod za sigurnost informacijskih sustava, vojska i vlada.

2. Mislite li da postoji odjel za digitalnu forenziku unutar naših mjerodavnih tijela?

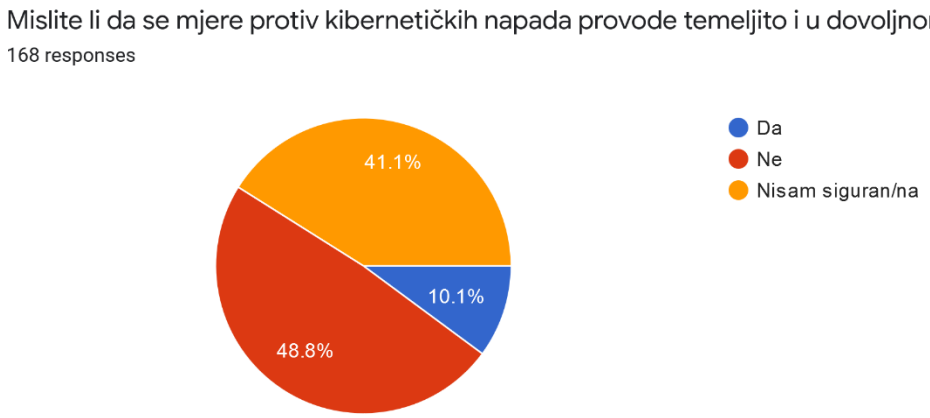
Od 168 ispitanika, 100 (59.5%) ih je potvrdilo s „da“, 52 (31%) ih nije sigurno, a 16 (9.5%) ispitanika ne smatra da postoji odjel za digitalnu forenziku u Hrvatskoj.



Graf 1: Omjer odgovora na drugo pitanje

3. Mislite li da se mjere protiv kibernetičkih napada provode temeljito i u dovoljnom broju?

Od 168 ispitanika, njih 82 (48.8%) ne smatra da se mjere protiv kibernetičkih napada provode temeljito i u dovoljnom broju, 69 (41.1%) ih nije sigurno, dok svega njih 17 (10.1%) smatra da se mjere provode temeljito i u dovoljnom broju.



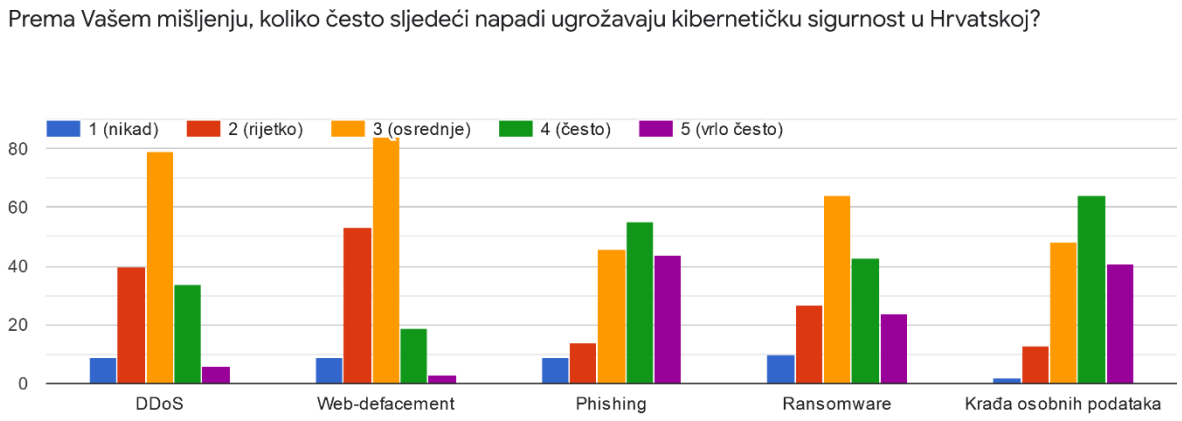
Graf 2: Omjer odgovora na treće pitanje

4. Označite regulative o kibernetičkoj sigurnosti za koje ste čuli:

Navedene regulative su Uredba i Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja usluga (2018) te Konvencija o kibernetičkom kriminalu (2001) te jedna je kućica u koju se može upisati slobodan odgovor (ostalo). Ovo je pitanje višestrukog odabira. Uredbu su označila 43 ispitanika (25.6%), Zakon 44 ispitanika (26.2%), Konvenciju 36 ispitanika (21.4%), a ostalo 83 ispitanika (49.4%). Od ostalih odgovora, pojavljuju se Zakon o informacijskoj sigurnosti te Opća uredba o zaštititi podataka. Osim toga, većina ih je odgovorilo da nisu upoznati s navedenima regulativama.

5. Prema Vašem mišljenju, koliko često sljedeći napadi ugrožavaju kibernetičku sigurnost u Hrvatskoj?

Navedeni napadi su distribuirano uskraćivanje usluge (eng. *distributed denial of service*), uništavanje mrežne stranice (eng. *web-defacement*), *phishing* kampanje, ransomware zlonamjerni programi i krađa osobnih podataka te je moguće odabrati više odgovora. Većina studenata smatra da navedeni napadi uglavnom osrednje ugrožavaju kibernetičku sigurnost u Hrvatskoj, ali i da su najčešći napadi krađa osobnih podataka te phishing kampanje.



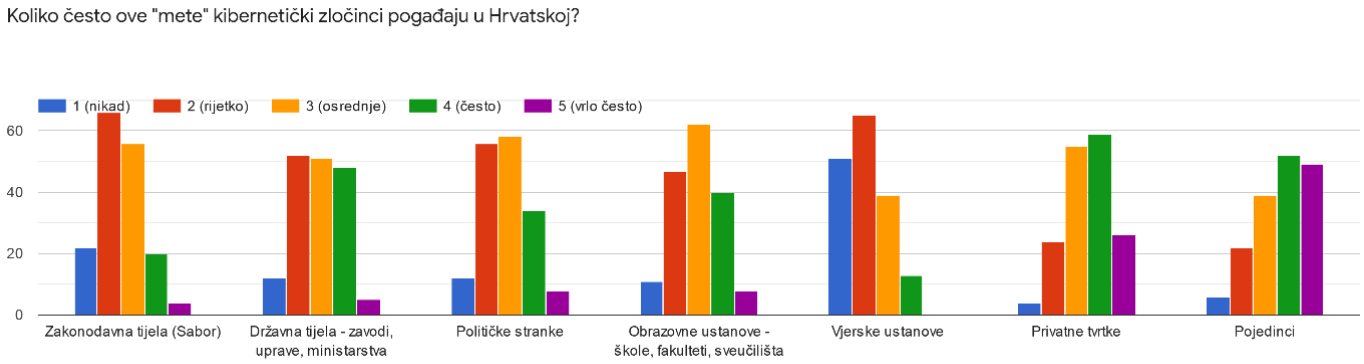
Graf 3: Prikaz odgovora na peto pitanje

	DDoS	Web-defacement	Phishing	Ransomware	Krađa osobnih podataka
1 (nikad)	9 (5.36%)	9 (5.36%)	9 (5.36%)	10 (5.95%)	2 (1.19%)
2 (rijetko)	40 (23.81%)	53 (31.54%)	14 (8.33%)	27 (16.07%)	13 (7.74%)
3 (osrednje)	79 (47.02%)	84 (50%)	46 (27.38%)	64 (38.1%)	48 (28.57%)
4 (često)	34 (20.24%)	19 (11.31%)	55 (32.74%)	43 (25.59%)	64 (38.1%)
5 (vrlo često)	6 (3.57%)	3 (1.79%)	44 (26.19%)	24 (14.29%)	41 (24.4%)

Tablica 1: Tablični prikaz rezultata iz petog pitanja

6. Koliko često ove "mete" kibernetički zločinci pogađaju u Hrvatskoj?

Ponuđeni odgovori su zakonodavna tijela (Sabor), državna tijela (zavodi, uprave, ministarstva), političke stranke, obrazovne ustanove (škole, fakulteti, sveučilišta), vjerske ustanove, privatne tvrtke i pojedinci. Studenti smatraju da su najčešće mete kibernetičkih napada u Hrvatskoj pojedinci, privatne tvrtke i državna tijela, a najrjeđe vjerske ustanove.



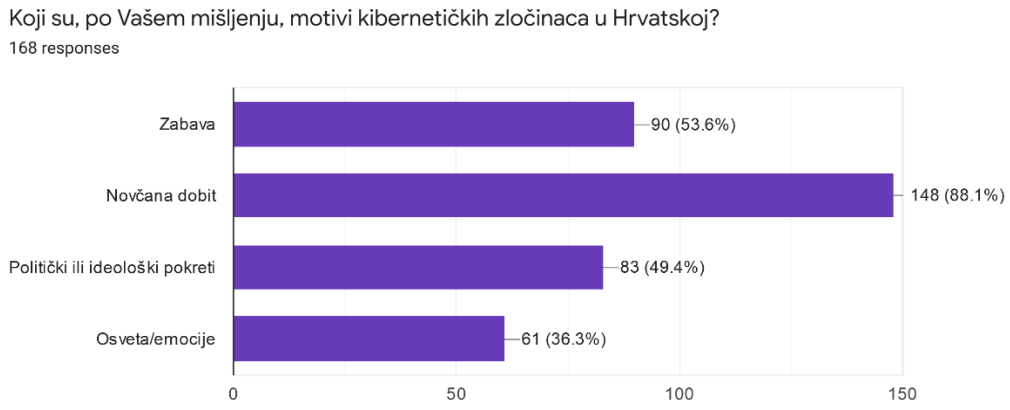
Graf 4: Prikaz odgovora na šesto pitanje

	Zakonodavna tijela	Državna tijela	Političke stranke	Obrazovne ustanove	Vjerske ustanove	Privatne tvrtke	Pojedinci
1 (nikad)	22 (13.1%)	12 (7.14%)	12 (7.14%)	11 (6.55%)	51 (30.36%)	4 (2.38%)	6 (3.57%)
2 (rijetko)	66 (39.29%)	52 (30.95%)	56 (33.33%)	47 (27.98%)	65 (38.69%)	24 (14.29%)	22 (13.1%)
3 (osrednje)	56 (33.33%)	51 (30.36%)	58 (34.53%)	62 (36.9%)	39 (23.21%)	55 (32.74%)	39 (23.21%)
4 (često)	20 (11.9%)	48 (28.57%)	34 (20.24%)	40 (23.81%)	13 (7.74%)	59 (35.12%)	52 (30.95%)
5 (vrlo često)	4 (2.38%)	5 (2.98%)	8 (4.76%)	8 (4.76%)	0 (0%)	26 (15.47%)	49 (29.17%)

Tablica 2: Tablični prikaz rezultata iz šestog pitanja

7. Koji su, po Vašem mišljenju, motivi kibernetičkih zločinaca u Hrvatskoj?

Ovo je također pitanje višestrukog odabira. Najviše studenata smatra da je motiv kibernetičkog napada novčana dobit (88.1%), a najmanje (36.3%) da su to osveta/emocije.

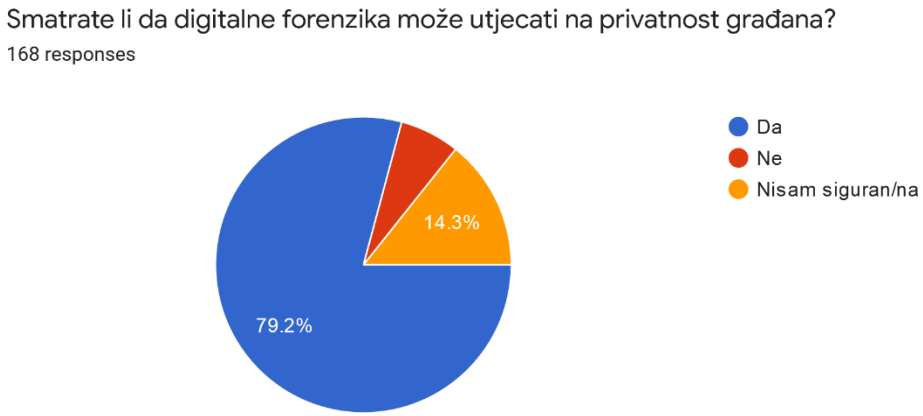


Graf 5: Prikaz odgovora na sedmo pitanje

12.2.2. Privatnost podataka

8. Smatrate li da digitalne forenzika može utjecati na privatnost građana?

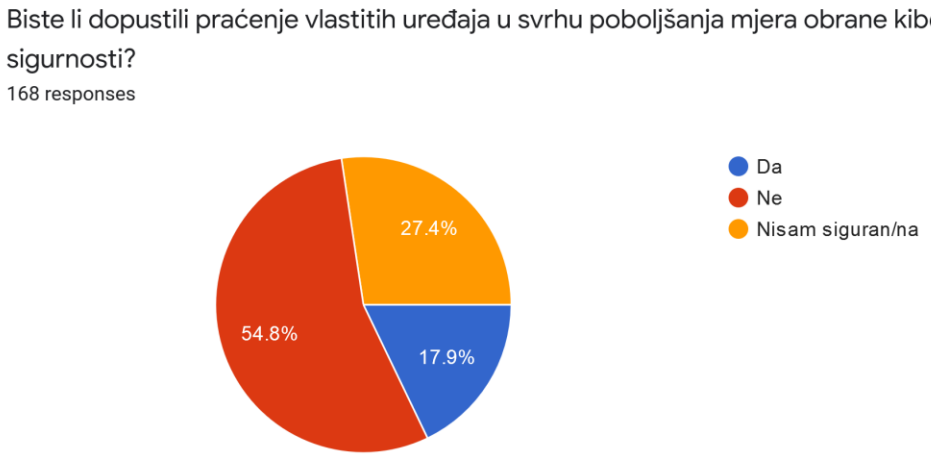
Čak 79.2% studenata smatra da digitalna forenzika može utjecati na privatnost građana, dok ih 14.3% nije sigurno, a 6.5% ne smatra da može utjecati.



Graf 6: Omjer odgovora na osmo pitanje

9. Biste li dopustili praćenje vlastitih uređaja u svrhu poboljšanja mjera obrane kibernetičke sigurnosti?

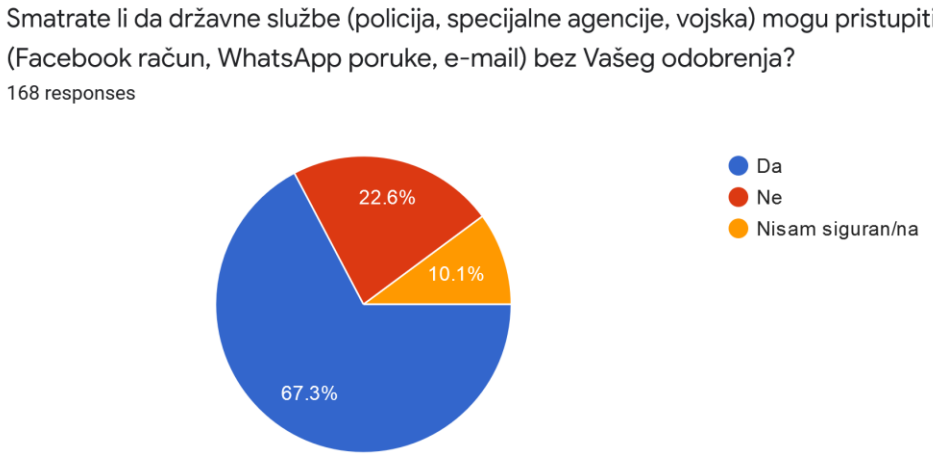
Što se tiče praćenja vlastitih uređaja u svrhu poboljšanja mjera obrane kibernetičke sigurnosti, 54.8% studenata ne bi pristalo na takvu mjeru, 27.4% ih nije sigurno, a samo 17.9% studenata bi pristalo.



Graf 7: Omjer odgovora na deveto pitanje

10. Smatrate li da državne službe (policija, specijalne agencije, vojska) mogu pristupiti Vašim podacima (Facebook račun, WhatsApp poruke, e-mail) bez Vašeg odobrenja?

Većina studenata (67.3%) smatra da državne službe mogu pristupiti njihovim podacima bez odobrenja, dok ih 22.6% ne smatra, a 10.1% ih nije sigurno.

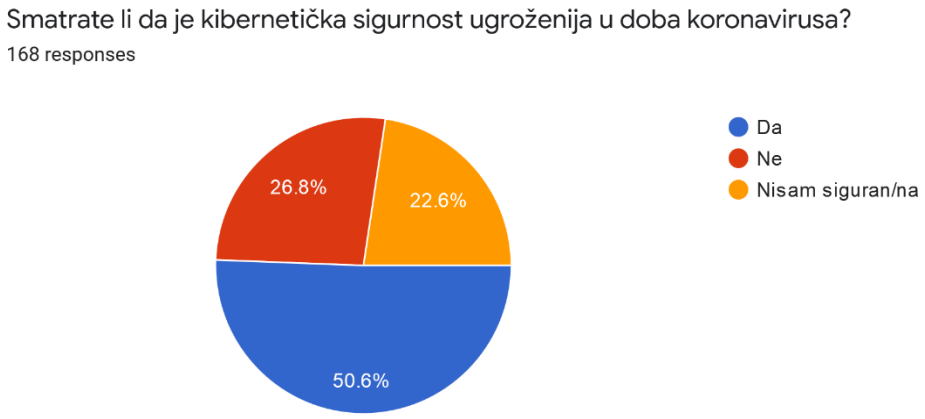


Graf 8: Omjer odgovora na deseto pitanje

12.2.3. Kibernetička sigurnost u doba koronavirusa

11. Smatrate li da je kibernetička sigurnost ugroženija u doba koronavirusa?

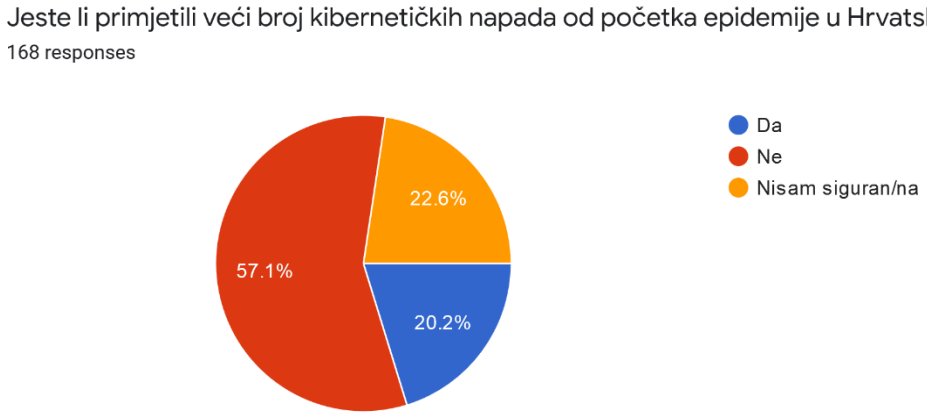
Za vrijeme epidemije koronavirusa javljaju se novi kibernetički napadi, a 50.6% studenata smatra da je kibernetička sigurnost u to vrijeme ugroženija. 26.8% ne smatra da je kibernetička sigurnost ugroženija, dok ih 22.6% nije sigurno oko te izjave.



Graf 9: Omjer odgovora na jedanaesto pitanje

12. Jeste li primijetili veći broj kibernetičkih napada od početka epidemije u Hrvatskoj?

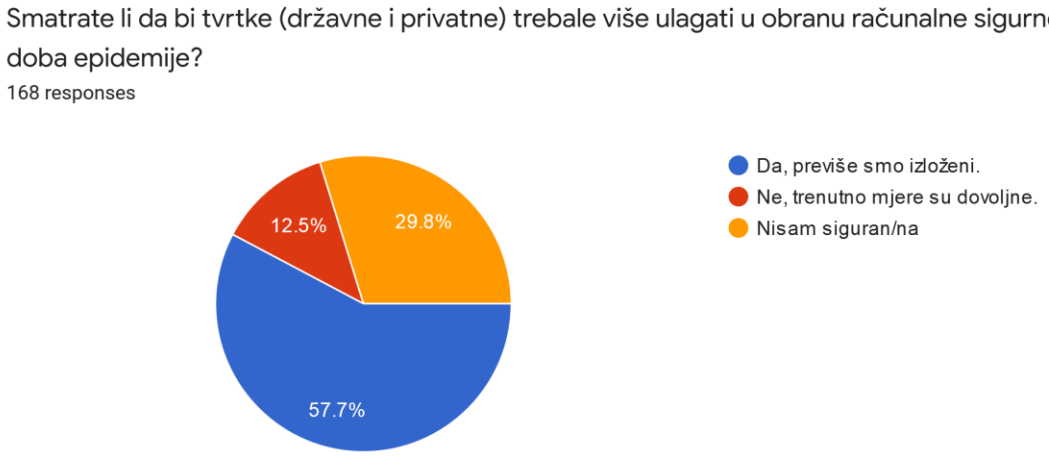
Povezano sa zadnjim pitanjem, 57.1% studenata nije primjetilo veći broj kibernetičkih napada od početka epidemije u Hrvatskoj, tek ih je 20.2% primijetilo, a 22.6% nije sigurno.



Graf 10: Omjer odgovora na dvanaesto pitanje

13. Smatrate li da bi tvrtke (državne i privatne) trebale više ulagati u obranu računalne sigurnosti u doba epidemije?

Što se tiče samog povećanja obrane od kibernetičkih napada za vrijeme epidemije, 57.7% studenata smatra da bi tvrtke trebale više ulagati u samo obranu, 12.5% smatra da su trenutno mjere dovoljne, a 29.8% ih nije sigurno.



Graf 11: Omjer odgovora na trinaesto pitanje

14. Označite napade za koje ste čuli ili bili žrtva za vrijeme epidemije?

Ovo je pitanje višestrukog odabira, a ponuđeni su CARNET DDoS (50%), spam i phishing kampanje o koronavirusu (51.8%), krađa podataka putem WhatsApp-a (36.9%), fake mrežne stranice o koronavirusu (60.7%) i slobodan odabir (ostalo). Od ostalih odgovora navedeni su krađa novčanih iznosa s bankovnih računa, hakerski napad na INA-u i napadi putem Zoom-a.

13. Zaključak

U zadnjih nekoliko godina povećava se broj novih i sofisticiranih načina ugroze kibernetičke sigurnosti. Iz tog razloga pojavljuje se potreba za većom razinom obrane i boljim mjerama sprječavanja prijetnji i napada. Digitalna forenzika je rješenje za to, jer podrazumijeva primjenu računalne znanosti i istraživačkih metoda u pravne svrhe. Ova grana forenzike uključuje prikupljanje, očuvanje, analizu i prezentaciju digitalnih dokaza, korištenjem odgovarajućih alata, metoda i tehnika. Ovisno o uređaju ili vrsti digitalnog dokaza, digitalna forenzika dijeli se na: računalnu forenziku, forenziku mobilnih uređaja, mrežnu forenziku i forenziku baza podataka. Osim navedenih, postoje još i derivati navedenih grana poput forenzike medija za pohranu, forenzike tehnologija u oblaku i drugih. Kibernetički zločinci razvijaju nove metode i alate kojima bi otežali digitalnu istragu i nazivaju se antiforenzičarima. Digitalni forenzičari koriste niz alata u samoj istrazi, a oni mogu biti hardverske ili softverske prirode, komercijalni ili otvorenog kôda, specijalizirani ili sveobuhvatni. Metode povezane s digitalnom forenzikom su odgovor na incident i elektroničko otkriće, a tehnike koje se koriste su penetracijsko testiranje, rudarenje podataka, analiza grafičkih slika, povezivanje događaja, testiranje unutar sigurnosnog okvira, kriptoanaliza i stegoanaliza. Kako bi netko postao digitalnim forenzičarem, trebao bi proći obuku i formalno ili neformalno obrazovanje. Odlike digitalnog forenzičara su ambicioznost u informacijskim tehnologijama, dobre komunikacijske i analitičke vještine te vještine u rješavanju problema, a trebao bi imati i iskustvo u informatici ili kriminalistici. Potrebno je poznavati i niz legislativa i regulativa, jer digitalna forenzika nije toliko prihvaćena u pravnom sustavu, a može naići na mnoge prepreke poput ugrožavanja privatnosti i potrebe za nalogom kod digitalne istrage. U Hrvatskoj se razvijaju odjeli digitalne forenzike unutar policije i Ministarstva unutarnjih poslova, ali postoje i privatne tvrtke koje obavljaju poslove vezane za digitalnu forenziku. Istraživačkim radom utvrdili su se stavovi studenata o stanju digitalne forenzike u Hrvatskoj. Studenti smatraju da iako postoje tijela koja obavljaju digitalne istrage, mjere protiv napada kibernetičke sigurnosti su nedovoljne. Oni nisu dovoljno informirani o zakonima vezanim za kibernetičku sigurnost, niti o specifičnim tijelima koja se bave digitalnom forenzikom. Također, smatraju da ona može utjecati na privatnost, ne bi dopustili praćenje vlastitih uređaja, ali vjeruju da državne službe svejedno pristupaju podacima bez njihovog znanja. Polovica ih smatra da je kibernetička sigurnost ugroženija za vrijeme epidemije koronavirusa te da bi trebali više ulagati u obranu tijekom same epidemije.

14. Literatura

Popis literature

1. Altheide, C., Carvey, H. (2011). Digital forensics with Open Source Tools. Syngress.
2. Ashcroft, J. (2001). Electronic Crime Scene Investigation: A Guide for First Responders. U.S. Dept. of Justice, Office of Justice Programs, National Institute of Justice.
3. Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press.
4. Davidoff, S., Ham, J. (2012). Network forensics: Tracking Hackers through Cyberspace. Upper Saddle River, New Jersey: Prentice Hall.
5. Johansen, G. (2020). Digital Forensics and Incident Response (2nd ed.). Packt Publishing.
6. King, G. (2006). A Forensic Investigation Plan and Cookbook. SANS Institute.
7. Lawton, D., Stacey, R., Dodd, G. (2014). eDiscovery in digital forensic investigations. Centre for Applied Science and Technology (CAST).
8. Prasad, A., Pande, J. (2016). Digital Forensics. Uttarakhand Open University.
9. Sammons, J. (2014). The Basics of Digital Forensics (2nd ed.). Syngress.

Popis internetskih izvora

1. 6 Anti-forensic techniques that every cyber investigator dreads. EC-Council. Dostupno na: https://blog.eccouncil.org/6-anti-forensic-techniques-that-every-cyber-investigator-dreads/
2. Abdalla, S., Hazem, S., & Hashem, S. (2007). Guideline Model for Digital Forensic Investigation. Annual ADFSL Conference on Digital Forensics, Security and Law. Dostupno na: https://commons.erau.edu/adfsl/2007/session-7/2
3. About Wireshark. Wireshark. Dostupno na: https://www.wireshark.org/
4. Aktivnosti u sklopu projekta „Jačanje kapaciteta MUP-a u borbi protiv svih oblika kibernetičkog kriminaliteta. Ministarstvo unutarnjih poslova. Dostupno na: https://mup.gov.hr/vijesti/aktivnosti-u-sklopu-projekta-jacanje-kapaciteta-mup-a-u-borbi-protiv-svih-oblika-kibernetickog-kriminaliteta/285974
5. Alabdulsalam, S., Schaefer, K., Kechadi, T., & Le-Khac, N. (2018). Internet of Things Forensics – Challenges and a Case Study. Advances In Digital Forensics XIV, 35-48. Dostupno na: https://doi.org/10.1007/978-3-319-99277-8_3
6. Anti-Forensics. Infosec. Dostupno na: https://resources.infosecinstitute.com/anti-forensics-part-1/
7. Areas Of Study. Infosec. Dostupno na: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/
8. Best Masters in Computer Forensics Degrees. College Choice. Dostupno na: https://www.collegechoice.net/rankings/best-masters-in-computer-forensics-degrees/
9. Budite oprezni - COVID-19 iskorištava se i u kibernetičkim napadima. Nacionalni CERT. Dostupno na: https://www.cert.hr/budite-oprezni-covid-19-iskoristava-se-i-u-kibernetickim-napadima/
10. Categories of Digital Evidence. Infosec. Dostupno na: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/
11. Centar za forenzična ispitivanja, istraživanja i vještačenja "Ivan Vučetić". Ministarstvo unutarnjih poslova. Dostupno na: https://mup.gov.hr/centar-za-forenzicna-ispitivanja-istrazivanja-i-vjestacenja-ivan-vucetic-281610/281610

12. Chart of signatures and ratifications of Treaty 185. Council of Europe. Dostupno na: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=27HuKgpK

13. Chopade, R., & Pachghare, V. (2019). Ten years of critical review on database forensics research. Digital Investigation, 29, 180-197. Dostupno na: https://doi.org/10.1016/j.diin.2019.04.001

14. Choudary, A. What is Computer Security? Introduction to Computer Security. Edureka! Dostupno na: https://www.edureka.co/blog/what-is-computer-security/

15. Commercial Computer Forensics Tools. Infosec. Dostupno na: https://resources.infosecinstitute.com/category/computerforensics/introduction/commercial-computer-forensics-tools/

16. Commercial Software. Techopedia. Dostupno na: https://www.techopedia.com/definition/4245/commercial-software

17. Computer Forensics Investigator: Career Guide. Criminal Justice Degree Schools. Dostupno na: https://www.criminaljusticedegreeschools.com/criminal-justice-careers/computer-forensics-investigator/

18. Computer Forensics: Digital Forensic Analysis Methodology. Crime Scene Investigator Network. Dostupno na: https://www.crime-scene-investigator.net/computer-forensics-digital-forensic-analysis-methodology.html

19. Cyber Terrorism. CIPedia. Dostupno na: https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Cyber_Terrorism

20. Cybercrime. Techopedia. Dostupno na: https://www.techopedia.com/definition/2387/cybercrime

21. Cyberthreat. Techopedia. Dostupno na: https://www.techopedia.com/definition/25263/cyberthreat

22. Ćosić, J., Ćosić, Z., Bača, M. (2010). Digitalna antiforenzika – manipulacija procesom digitalne istrage. 18. TELEKOMUNIKACIONI FORUM TELFOR 2010. Dostupno na: https://www.bib.irb.hr/601475

23. Data Mining. Techopedia. Dostupno na: https://www.techopedia.com/definition/1181/data-mining

24. Database (DB). Techopedia. Dostupno na: https://www.techopedia.com/definition/1185/database-db

25. DataFocus. INsig2. Dostupno na: https://www.insig2.com/hr/konferencija/datafocus

26. Degrees. EC-Council. Dostupno na: https://www.eccouncil.org/

27. Different types of digital forensics. Open Learn. Dostupno na: https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.3

28. Digital Forensic Process—Presentation. DriverSavers Data Recovery. Dostupno na: https://drivesaversdatarecovery.com/blog/digital-forensic-process-presentation/

29. Digitalna forenzika – diplomski. Tehničko veleučilište u Zagrebu. Dostupno na: https://www.tvz.hr/studiji/digitalna-forenzika/diplomski

30. Disk Forensics. CyberImmersions. Dostupno na: https://www.cyberimmersions.com/digital-forensics/disk-forensics/

31. Dokaz. Enciklopedija Leksikografskog zavoda Miroslav Krleža. Dostupno na: http://enciklopedija.lzmk.hr/clanak.aspx?id=8423

32. EC-Council. Algebra. Dostupno na: https://www.algebra.hr/certifikacijski-seminari/tag/ec-council/

33. Education. Forensics Focus. Dostupno na: https://www.forensicfocus.com/education/#europe

34. Email Forensics: Investigation Techniques. Forensics Focus. Dostupno na: https://articles.forensicfocus.com/2019/02/15/email-forensics-investigation-techniques/

35. EnCase Mobile Investigator. Guidance Software. Dostupno na: https://www.guidancesoftware.com/encase-mobile-investigator

36. Forensic Toolkit (FTK). Access Data. Dostupno na: https://accessdata.com/products-services/forensic-toolkit-ftk

37. Forensics Tehniques Part 2. Infosec. Dostupno na : https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/forensic-techniques-part-2/

38. Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. Digital Investigation, 3, 44-49. Dostupno na: https://doi.org/10.1016/j.diin.2006.06.005

39. How Many Smartphones Are In The World? BankMyCell. Dostupno na: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

40. How to become a Computer Forensics Investigator. Infosec. Dostupno na : https://resources.infosecinstitute.com/job-titles/computer-forensics-investigator/

41. Introduction to Social Network Forensics. Infosec. Dostupno na: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/hybrid-and-emerging-technologies/social-network-forensics/#gref

42. Kali Linux Tools Listing. Kali Tools. Dostupno na: https://tools.kali.org/tools-listing

43. Kibernetička sigurnost. Ministarstvo unutarnjih poslova. Dostupno na: https://mup.gov.hr/istaknute-teme/nacionalni-programi-i-projekti/nacionalne-strategije/kiberneticka-sigurnost/222335

44. Konferencija kibernetička sigurnost i digitalna forenzika. iStart IT. Dostupno na: http://www.cyber-security-conf.istart-it.hr/

45. Live Data Forensics. Council of Europe. Dostupno na: https://www.coe.int/en/web/octopus/blog/-/blogs/live-data-forensics-or-why-volatile-data-can-be-crucial-for-your-cases/

46. Mobile Device. Techopedia. Preuzeto sa: https://www.techopedia.com/definition/23586/mobile-device

47. Network Forensics. Search Security. Dostupno na: https://searchsecurity.techtarget.com/definition/network-forensics

48. Network Forensics. Techopedia. Dostupno na: https://www.techopedia.com/definition/16122/network-forensics

49. NIS Direktiva. Infigo. Dostupno na: https://www.infigo.hr/nis-direktiva-s124?t=1

50. O Nacionalnom CERT-u. Nacionalni CERT. Dostupno na: https://www.cert.hr/onama/

51. Open Source Digital Forensics. Sleuth Kit. Dostupno na: http://www.sleuthkit.org/index.php

52. Operating systems and open source tools for digital forensics. Packt. Dostupno na: https://subscription.packtpub.com/book/networking_and_servers/9781788625005/1/ch01lvl1sec13/operating-systems-and-open-source-tools-for-digital-forensics

53. Overview Of Malware Forensics. Infosec. Dostupno na: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/application-forensics/overview-of-malware-forensics/

54. Područja rada. Sigurnosno-obavještajna agencija. Dostupno na: https://www.soa.hr/hr/podrucja-rada/

55. Pollitt, M. (2010). A History of Digital Forensics. Advances In Digital Forensics VI, 3-15. Dostupno na: https://doi.org/10.1007/978-3-642-15506-2_1

56. Profil kompanija. INsig2. Dostupno na: https://www.insig2.com/hr/o-nama/kompanijski-profil

57. Program. Sveučilišni odjel za forenzične znanosti. Dostupno na: http://forenzika.unist.hr/Nastava/Diplomskisveu%c4%8dili%c5%a1nistudijforenzike/Program/tabid/498/Default.aspx

58. Računalna forenzika. Nacionalni CERT. Dostupno na: https://www.cert.hr/racunalna-forenzika/

59. Software. Guidance Software. Dostupno na: https://www.guidancesoftware.com/software

60. Software. Techopedia. Dostupno na: https://www.techopedia.com/definition/4356/software

61. The Budapest Convention on Cybercrime: International Criminal Law and the use of Treaties. Lexology. Dostupno na: https://www.lexology.com/library/detail.aspx?g=4220b287-ac07-4a33-a711-bee235721d9f

62. Understanding Digital Forensics In Cyber Penetration Testing and Incident Response. Lineal. Dostupno na: https://www.linealservices.com/understanding-digital-forensics-in-cyber-penetration-testing-and-incident-response/

63. Uprava kriminalističke policije. Ravnateljstvo policije. Dostupno na: https://policija.gov.hr/uprava-kriminalisticke-policije/415

64. Volatility. Volatility Foundation. Dostupno na: https://www.volatilityfoundation.org/

65. What Is Database Forensics? Infosec. Dostupno na: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/application-forensics/overview-types-of-database-forensics/

66. What is Digital Forensics? History, Process, Types, Challenges. Guru99. Dostupno na: https://www.guru99.com/digital-forensics.html

67. What is Forensics?. CrimeSceneInvestigatorEDU.org. Dostupno na: https://www.crimesceneinvestigatoredu.org/what-is-forensic-science/

68. What is the Strongest Encryption Today? TechNadu. Dostupno na: https://www.technadu.com/strongest-encryption/37596/

69. X-Ways Forensics: Integrated Computer Forensics Software. X-Ways. Dostupno na: http://www.x-ways.net/forensics/

70. Zakon o informacijskoj sigurnosti. (NN 79/2007). Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html

71. Zakon o pravu na pristup informacijama. (NN 25/2013). Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2013_02_25_403.html

72. Zakon o provedbi Opće uredbe o zaštiti podataka. (NN 42/2018). Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html

73. Zakon o tajnosti podataka. (NN 79/2007). Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2483.html

Popis slika

Popis tablica

Popis grafikona

Digitalna forenzika

Sažetak

Digitalno doba donosi nam mnoge prednosti, ali i nedostatke, poput ugrožavanja sigurnosti podataka i informacija. U ovom radu bavit ću se temom digitalne forenzike, kojoj je cilj očuvanje i analiziranje podataka i informacija proizašlih iz neke kriminalne aktivnosti na bilo kojem obliku informacijskog sustava.

Digitalni forenzičari koriste niz alata i metoda kako bi istragu učinili jednostavnijom i bržom. Objasnit ću navedene stavke, kao i potrebne vještine i znanja koje digitalni forenzičar mora imati kako bi uspješno odradio svoj posao.

Usporedit ću primjenu digitalne forenzike u svijetu s primjenom u Republici Hrvatskoj. Za istraživanje ću provesti anketu koja prikazuje koliko su studenti upoznati s digitalnom forenzikom i postoji li potreba za njom u Hrvatskoj.

Ključne riječi: digitalna forenzika, kibernetički kriminal, informacijski sustav, informacija, podatak

Digital Forensics

Summary

Digital age comes with many advantages, as well as disadvantages, such as compromising data and information security. Throughout this paper, I will write about digital forensics, the aim of which is to preserve and analyze data and information derived from some criminal activity on any form of information system.

Digital forensic experts use a variety of tools and methods to make the investigation simpler and faster. I will write about those tools and methods, as well as the necessary skills and knowledge that a digital forensics expert should have in order to successfully do his job.

I will compare the use of digital forensics in the world with its application in Republic of Croatia. For the research, I will conduct a survey that will show how well students are familiar with digital forensics and whether it is needed in Croatia.

Key words: digital forensics, cyber-crime, information system, information, data