RAČUNARSKA FORENZIKA U ANALIZI I ISTRAŽIVANJU CYBER NAPADA / COMPUTER FORENSICS IN ANALYSIS AND RESEARCH CYBER ATTACKS

Ajla Hurem[1]
[1]Internacionalni univerzitet Travnik, Aleja-Konzula Meljanac bb. 72270 Travnik,
Bosna i Hercegovina,
e-mail: ajla.hurem98@gmail.com

Pregledni članak
UDK / UDC 004:343.98

Sažetak
Kako moderna tehnologija napreduje, tako i kibernetičke prijetnje postaju sve sofisticiranije, a računarska forenzika igra ključnu ulogu u istraživanju i analizi cyber napada. Ovaj rad istražuje primjenu računarske forenzike tokom i nakon napada, fokusirajući se na faze oporavka, analize napada i povezivanje kriminalaca s napadima. Računarska forenzika ne služi samo za identifikaciju napada, već i za razumijevanje metoda napadača, čime doprinosi prevenciji budućih prijetnji i osiguravanju pravne odgovornosti. Rad razmatra osnovne pojmove računarske forenzike, s naglaskom na očuvanje integriteta dokaza i izazove koji se javljaju pri analizi digitalnih podataka. Poseban fokus stavlja na alate i tehnike koje se koriste u istraživanju različitih vrsta cyber prijetnji. Također se razmatraju tehnički i pravni izazovi, poput problema šifriranja, zaštite privatnosti i složenosti u analizi digitalnih dokaza. U zaključku, rad ističe važnost daljnjeg razvoja računarske forenzike u borbi protiv sofisticiranih cyber prijetnji, naglašavajući potrebu za novim alatima, tehnikama i metodologijama koje će omogućiti efikasniju zaštitu, oporavak i jaču sigurnost u digitalnom okruženju.
Ključne riječi: Računarska forenzika, Cyber napadi, Cyber prijetnje
JEL klsifikacija: O33

Abstract
As modern technology advances, so do cyber threats, and computer forensics plays a key role in investigating and analyzing cyberattacks. This paper explores the application of computer forensics during and after cyberattacks, focusing on the phases of recovery, attack analysis, and linking perpetrators to the attacks. Computer forensics not only helps identify attacks but also provides insights into the methods used by attackers, contributing to the prevention of future threats and ensuring legal accountability. The paper examines the fundamental concepts of computer forensics, emphasizing the preservation of evidence integrity and the challenges encountered in analyzing digital data. It places special focus on the tools and techniques used in investigating various types of cyber threats. The paper also discusses the technical and legal challenges, such as encryption issues, privacy protection, and the complexities involved in digital evidence analysis. In conclusion, the paper highlights the importance of further developing computer forensics in the fight against increasingly sophisticated cyber threats, emphasizing the need for new tools, techniques, and methodologies to enable more effective protection, recovery, and enhanced security in the digital environment.
Keywords: *Computer forensics, Cyber attacks, Cyber threats*
JEL classification: O33

UVOD

S razvojem informacionih tehnologija, digitalni svijet postao je neizostavan dio savremenog društva, nudeći nove mogućnosti za komunikaciju, rad i razmjenu informacija. Međutim, uporedo sa benefitima, raste i prijetnja u vidu cyber kriminala, čiji je uticaj sve ozbiljniji i složeniji. Cyber napadi predstavljaju jednu od najopasnijih prijetnji modernom društvu, jer mogu izazvati ogromne finansijske gubitke, narušiti povjerenje u institucije, pa čak i ugroziti nacionalnu bezbjednost. U takvom kontekstu, računarska forenzika postala je ključno oruđe za analizu i istraživanje ovih incidenata. Računarska forenzika predstavlja specijalizovanu oblast digitalne nauke koja se bavi identifikacijom, prikupljanjem, očuvanjem i analizom digitalnih dokaza u svrhu istraživanja i rješavanja kriminalnih aktivnosti koje uključuju informacionu tehnologiju. Njena primjena nadilazi tradicionalno shvatanje kriminalistike, jer omogućava istraživačima da otkriju tragove napadača, rekonstruišu lanac događaja, identifikuju ranjivosti u sistemima i pruže dokaze koji su prihvatljivi na sudu. Uloga računarske forenzike naročito dolazi do izražaja u kontekstu istraživanja cyber napada, koji su postali učestaliji i sofisticiraniji zahvaljujući napretku tehnologije. Napadi poput ransomware-a, DDoS napada, phishing kampanja i naprednih upornjih prijetnji zahtijevaju brzu, preciznu i pouzdanu reakciju. Računarska forenzika omogućava ne samo razotkrivanje prirode napada i njegovih posljedica, već i prevenciju sličnih incidenata u budućnosti. Cilj rada je da pruži sveobuhvatan uvid u značaj i mogućnosti računarske forenzike u analizi cyber napada, identifikuje ključne metode i alate koji se koriste u ovoj oblasti, i predloži strategije za unapređenje praksi. Pored toga, rad se osvrće na buduće trendove u oblasti računarske forenzike, uključujući ulogu vještačke inteligencije i mašinskog učenja u analizi velikih količina podataka i detekciji anomalija. Važnost ove teme ogleda se u činjenici da cyber kriminal postaje sve značajnija prijetnja, kako za pojedince i kompanije, tako i za čitave države. Razumijevanje i primjena računarske forenzike ključni su za jačanje kapaciteta za otkrivanje i borbu protiv ovih prijetnji, kao i za unapređenje digitalne bezbjednosti na globalnom nivou. Ovaj rad predstavlja doprinos naučnoj zajednici, pružajući temelj za buduća istraživanja i praktičnu primjenu u oblasti računarske forenzike i cyber bezbjednosti.

1.OSNOVE CYBER NAPADA

Cyber napadi predstavljaju pokušaje, ili realizovane radnje, kojima se narušava bezbjednost informacionih sistema, kompromituje privatnost ili izaziva šteta korisnicima digitalnih tehnologija. Ovi napadi se mogu realizovati kroz različite tehnike, alate i taktike, zavisno od ciljeva i motivacija napadača. Razumijevanje osnova cyber napada ključno je za unapređenje mjera zaštite i efikasnu primjenu računarske forenzike u istraživanju i prevenciji. Cyber napadi se mogu klasifikovati prema njihovim ciljevima, tehnikama i nivou sofisticiranosti. Najčešći oblici napada uključuju:

1. **Malware napadi**
2. **Phishing napadi**
3. **DDoS (Distributed Denial of Service)**
4. **Napadi na aplikacije i web stranice**

5. **Advanced Persistent Threats (APT)**

Napadači koriste niz tehnika kako bi realizovali svoje ciljeve. Neke od najčešćih tehnika uključuju:

1. **Društveni inženjering**
2. **Eksploatacija ranjivosti**
3. **Upotreba botneta**
4. **Lateralno kretanje u mreži**

Računarska forenzika igra ključnu ulogu u istraživanju cyber napada. Forenzički eksperti analiziraju digitalne tragove kako bi:

- Identifikovali način na koji je napad izvršen.
- Utvrdili obim kompromitacije podataka i sistema.
- Pronašli dokaze koji mogu pomoći u identifikaciji napadača i pokretanju pravnih postupaka.
- Razvili strategije za sprečavanje sličnih napada u budućnosti.

Analiza cyber napada često uključuje prikupljanje log fajlova, mrežnih tokova, memorijskih podataka i malicioznih fajlova, što omogućava rekonstrukciju napada i detekciju metoda koje su napadači koristili.

2.METODOLOGIJA RAČUNARSKE FORENZIKE

Računarska forenzika je disciplinovan proces koji zahtijeva strukturirani pristup u prikupljanju, analizi i očuvanju digitalnih dokaza. Cilj je da se osigura integritet dokaza kako bi bili prihvaćeni u pravnim postupcima i korišteni za otkrivanje činjenica u vezi sa incidentima u informacionim sistemima. Metodologija računarske forenzike oslanja se na precizne korake, stroga pravila i alate koji omogućavaju pouzdano sprovođenje istrage.

2.2.PROCES PRIKUPLJANJA DIGITALNIH DOKAZA

Prikupljanje digitalnih dokaza ključno je za uspjeh forenzičke istrage. Ovaj proces podrazumijeva sljedeće korake:

1. **Identifikacija dokaza**

Prvi korak u forenzičkoj analizi je identifikacija izvora dokaza, što može uključivati računare, mobilne uređaje, servere, mrežnu opremu, baze podataka i cloud servise. Digitalni dokazi mogu uključivati log fajlove, mrežne tokove, e-mail prepiske, fajlove na disku, keš memoriju i meta podatke.

2. **Zaštita mjesta incidenta**

Mjesto incidenta se mora osigurati kako bi se spriječilo narušavanje dokaza. Pristup uređajima i mrežama treba ograničiti kako bi se očuvao integritet podataka.

3. **Prikupljanje podataka**

Koriste se specijalizovani alati za kopiranje podataka na način koji čuva originalni sadržaj. Tehnike prikupljanja uključuju kreiranje forenzičke kopije (bitstream copy), koja predstavlja tačnu repliku originalnog medija. Tokom prikupljanja podataka dokumentuju se svi koraci i radnje, uključujući vrijeme, mjesto i osobe koje su bile prisutne.

4. **Čuvanje dokaza**

Digitalni dokazi moraju biti zaštićeni od manipulacije, oštećenja i neovlaštenog pristupa. Za čuvanje dokaza koristi se specijalna oprema, poput zaštićenih kontejnera i uređaja za zaštitu od elektromagnetnih smetnji.

2.3. OSIGURAVANJE LANCA NADLEŽNOSTI ("CHAIN OF CUSTODY")

Osiguravanje lanca nadležnosti ključno je za pravnu validnost digitalnih dokaza. Lanac nadležnosti predstavlja dokumentovani zapis koji prati tok dokaza od trenutka prikupljanja do korištenja u sudskom postupku. Cilj ovog procesa je da se očuva integritet dokaza i spriječe manipulacije.

2.3.1. Alati i tehnike za analizu podataka

Digitalna forenzika koristi raznovrsne alate i tehnike kako bi se izvršila detaljna analiza dokaza. Neki od najvažnijih alata uključuju:

1. **EnCase**

EnCase je jedan od najpoznatijih alata za digitalnu forenziku. Omogućava prikupljanje, analizu i prezentaciju dokaza. Koristi se za analizu fajlova na računarima, mobilnim uređajima i mrežnim sistemima. Nudi mogućnosti rekonstrukcije fajlova, analize e-mailova i pretraživanja izbrisanih podataka.

2. **FTK (Forensic Toolkit)**

FTK je alat koji omogućava brzu i efikasnu analizu velikih količina podataka. Podržava analizu diskova, fajlova, mrežnih podataka i elektronske prepiske. Ima ugrađene funkcije za dešifrovanje i analizu ključnih reči.

3. **Wireshark**

Wireshark je alat za analizu mrežnog saobraćaja. Omogućava prikupljanje i analizu mrežnih paketa, identifikaciju anomalija i praćenje aktivnosti napadača. Često se koristi u istraživanju DDoS napada, analizi malvera i detekciji neovlaštenog pristupa.

4. **Autopsy i Sleuth Kit**

Ovi alati omogućavaju dubinsku analizu fajlovnih sistema. Koriste se za analizu izbrisanih fajlova, particija i meta podataka.

2.4.OSNOVNI PRINCIPI VALIDNOSTI DOKAZA U SUDSKIM POSTUPCIMA

Da bi digitalni dokazi bili prihvaćeni u sudu, moraju zadovoljiti određene kriterijume validnosti:

Autentičnost: Dokaz mora biti autentičan i nesumnjivo povezan sa incidentom koji se istražuje.
Integritet: Integritet dokaza se obezbeđuje korištenjem kontrolnih zbirki (hash vrijednosti, kao što su MD5 ili SHA-256). Ako se hash vrijednost dokaza promijeni, to ukazuje na manipulaciju.
Pouzdanost: Metodologije i alati korišteni za prikupljanje i analizu dokaza moraju biti pouzdani i široko prihvaćeni u forenzičkoj zajednici.
Zakonitost: Dokazi moraju biti prikupljeni u skladu sa zakonima i regulativama kako bi bili prihvaćeni u pravnom postupku.
Reproduktivnost: Rezultati forenzičke analize moraju biti reproduktivni, tj. nezavisni istraživači bi trebalo da dobiju iste rezultate ako koriste istu metodologiju.

3.ANALIZA I ISTRAŽIVANJE CYBER NAPADA

Analiza i istraživanje cyber napada ključni su procesi u digitalnoj forenzici, jer omogućavaju razumijevanje prirode napada, rekonstrukciju događaja, identifikaciju počinioca i preduzimanje mjera za sprečavanje sličnih incidenata. Ovi procesi zahtijevaju sistematičan pristup, korištenje specijalizovanih alata i tehničku ekspertizu kako bi se istražio svaki aspekt napada i obezbijedili validni digitalni dokazi. Rekonstrukcija cyber napada podrazumijeva detaljno analiziranje svih dostupnih informacija kako bi se utvrdio način na koji je napad izvršen, koje su tehnike korištene i kakve su posljedice napada. Logovi su osnovni izvor podataka o događajima u informacionom sistemu. Sistemski logovi, mrežni logovi i logovi aplikacija sadrže informacije o vremenu, IP adresama, korisničkim sesijama i greškama koje mogu ukazati na tok napada. Na primjer, logovi web servera mogu otkriti pokušaje SQL injekcija, dok mrežni logovi mogu ukazati na DDoS napad ili upad u mrežu. Mrežni tokovi bilježe komunikaciju između uređaja i mogu ukazati na anomalije poput neobičnog saobraćaja, velikih količina podataka koje izlaze iz mreže ili neautorizovanih konekcija. Prikupljeni podaci se organizuju u hronološkom redoslijedu kako bi se rekonstruisala vremenska linija događaja. Ovaj proces uključuje kombinaciju informacija iz logova, memorijskih dump-ova, diskova i mrežnih tokova. Na primjer, vremenska linija može pokazati kada je zlonamerni fajl ubačen u sistem, kako je aktiviran i koje je promjene izazvao. Jedan od glavnih ciljeva analize cyber napada je identifikacija izvora prijetnje. Analiza IP adresa koje su učestvovale u napadu može pomoći u otkrivanju lokacije napadača. Međutim, napadači često koriste proxy servere, VPN-ove ili botnete kako bi prikrili svoj identitet, što otežava direktnu identifikaciju. Meta podaci u dokumentima, e-mailovima ili fajlovima mogu otkriti informacije o autoru ili uređaju koji je koristio fajl. Na primjer, Word dokument može sadržavati informacije o autoru, datumu kreiranja ili softveru korištenom za izradu fajla. Reverse DNS pretraga može pomoći u identifikaciji domena povezanih sa IP adresama, dok WHOIS alati pružaju informacije o registraciji domena. Napadači često ostavljaju tragove na mreži, poput poruka na forumima,

blogovima ili društvenim mrežama. Ove informacije mogu pomoći u povezivanju određenih aktivnosti sa identitetom napadača.

3.1.UPOTREBA SANDBOX TEHNOLOGIJE ZA ANALIZU MALICIOZNIH FAJLOVA

Sandbox tehnologija je ključni alat u istraživanju zlonamjernog softvera (malvera). Sandbox okruženje omogućava izolovano pokretanje sumnjivih fajlova ili aplikacija kako bi se analiziralo njihovo ponašanje bez rizika za stvarni sistem. Sandbox omogućava posmatranje akcija malvera, poput kreiranja fajlova, izmjene registara, mrežnih konekcija i šifrovanja podataka. Na primjer, ransomware će pokušati da šifruje fajlove u izolovanom okruženju, otkrivajući svoje metode rada. IoC su tragovi koje malver ostavlja, poput određenih domena koje koristi, IP adresa, fajlova koje kreira ili ključnih reči. Analiza IoC omogućava brže otkrivanje i blokiranje malvera u budućim incidentima. Alati poput Cuckoo Sandbox i FireEye omogućavaju automatizovanu analizu malicioznih fajlova, smanjujući vrijeme potrebno za istraživanje. Sandbox tehnologija omogućava istraživačima da testiraju malver i eksploite bez ugrožavanja stvarnog sistema ili mreže.

3.2.TEHNIKE PRAĆENJA HAKERA I POVRATNE ANALIZE

Praćenje hakera i povratna analiza (engl. *backtracking*) predstavljaju složen proces kojim se nastoji otkriti identitet napadača i njihova infrastruktura. Malveri često komuniciraju sa C2 serverima kako bi primili komande ili proslijedili ukradene podatke. Analizom mrežnog saobraćaja i DNS upita, istraživači mogu otkriti lokaciju i konfiguraciju C2 servera. Honeypoti su namjerno ranjivi sistemi dizajnirani da privuku napadače i zabilježe njihove aktivnosti. Ovi sistemi pružaju vrijedne informacije o tehnikama i alatima koje napadači koriste. Reverse engineering malvera može otkriti informacije o njegovom autoru, poput korištenih jezika, kôda i stilova programiranja. Na primjer, određeni kodovi ili fraze u malveru mogu ukazivati na geografski ili kulturni identitet autora. OSINT alati omogućavaju prikupljanje informacija iz javno dostupnih izvora, uključujući društvene mreže, forume i blogove. Napadači ponekad ostavljaju tragove o svojim aktivnostima na "dark webu" ili forumima za hakersku zajednicu. Praćenje hakera često zahtijeva saradnju sa međunarodnim organizacijama, obzirom da napadači mogu djelovati iz različitih jurisdikcija. Organizacije poput INTERPOL-a i CERT timova igraju ključnu ulogu u globalnim naporima za identifikaciju i hapšenje cyber kriminalaca.

3.3.ULOGA VJEŠTAČKE INTELIGENCIJE I MAŠINSKOG UČENJA U FORENZIČKOJ ANALIZI

Sa porastom količine digitalnih dokaza, vještačka inteligencija (AI) i mašinsko učenje (ML) postali su ključni alati za automatizaciju i unapređenje forenzičkih analiza. AI omogućava brzo pretraživanje velikih datasetova, uključujući log fajlove, e-mail prepiske i mrežne tokove. Mašinsko učenje se koristi za identifikaciju obrazaca u podacima, poput ponavljajućih aktivnosti napadača. Algoritmi mašinskog učenja mogu otkriti anomalije u mrežnom saobraćaju, koje često ukazuju na napade ili sumnjive aktivnosti. Na primjer, neuobičajeni

obrasci pristupa podacima ili naglo povećanje mrežnog saobraćaja mogu signalizirati pokušaj eksfiltracije podataka. AI alati analiziraju ponašanje malicioznih fajlova kako bi klasifikovali nove vrste malvera. Algoritmi se obučavaju na osnovu karakteristika poznatih malvera kako bi prepoznali nove prijetnje. Mašinsko učenje se koristi za analizu velikih kolekcija tekstualnih dokaza, poput e-mailova i prepiski. Algoritmi mogu identifikovati ključne fraze, emocionalne tonove i potencijalne indikatore kompromitacije. Korištenjem historijskih podataka o napadima, AI može predvidjeti buduće prijetnje i preporučiti mjere za unapređenje bezbjednosti sistema.

3.4.ANALIZA MOBILNIH UREĐAJA I IOT SISTEMA

Mobilni uređaji i IoT (Internet of Things) sistemi postali su ključni izvori digitalnih dokaza zbog svoje sveprisutnosti u svakodnevnom životu i poslovanju. Analiza mobilnih uređaja obuhvata pristup podacima sa SIM kartica, internog skladišta, cloud naloga, aplikacija i mrežnih logova. Alati poput Cellebrite i XRY omogućavaju preuzimanje podataka sa mobilnih telefona, čak i kada su šifrovani. Ključni podaci uključuju SMS poruke, pozive, geolokacijske informacije, fotografije i pretrage na internetu. IoT uređaji (pametni termostati, kamere, pametni zvučnici, itd.) čuvaju vrijedne digitalne dokaze poput vremenskih žigova, aktivnosti uređaja i mrežnih logova. Analiza IoT sistema zahtijeva specifične alate i tehnike jer ovi uređaji koriste raznovrsne protokole i arhitekture. Šifrovanje podataka, različiti standardi hardvera i softvera, kao i dinamična priroda IoT uređaja, otežavaju analizu. Čuvanje podataka u cloud okruženju takođe može otežati pristup i validaciju dokaza.

3.5.REVERSE ENGINEERING MALICIOZNIH PROGRAMA

Reverse engineering (obrnuti inženjering) malicioznih programa ključan je proces u razumijevanju prirode i funkcionalnosti zlonamjernog softvera. Cilj je analizirati kôd malvera kako bi se otkrile njegove namjere, mehanizmi djelovanja i moguće slabosti. Korištenjem alata poput IDA Pro i Ghidra, istraživači analiziraju binarne fajlove kako bi rekreirali njihov izvorni kôd. Ovo omogućava razumijevanje logike malvera i njegovih funkcionalnih komponenti. Malver se pokreće u kontrolisanom okruženju kako bi se posmatralo njegovo ponašanje u realnom vremenu. Dinamička analiza otkriva koje fajlove malver kreira, koje procese pokreće i kako komunicira sa spoljnim serverima.

Analiza statičkih karakteristika malvera, poput strukture fajlova, heder informacija i enkriptovanih sekcija, pruža uvid u njegov dizajn i potencijalne ranjivosti. Reverse engineering otkriva algoritme šifrovanja i mehanizme zaštite koji se koriste za sakrivanje aktivnosti malvera. Ovo omogućava analizu šifrovanih fajlova i komunikacija koje malver koristi. Na osnovu analize malvera, kreiraju se sigurnosni potpisi koji omogućavaju alatima za detekciju malvera da prepoznaju i blokiraju slične prijetnje u budućnosti.

4.IZAZOVI I OGRANIČENJA DIGITALNE FORENZIKE

Digitalna forenzika suočava se sa brojnim izazovima koji proizlaze iz tehničkih, pravnih i etičkih aspekata modernog digitalnog okruženja. Sve veći obim digitalnih podataka, napredne

tehnologije enkripcije, kao i konflikti između privatnosti i bezbjednosti, značajno otežavaju proces istrage i analize cyber incidenata. Enkripcija je ključni alat za zaštitu privatnosti i sigurnosti podataka, ali predstavlja jedan od najvećih izazova u digitalnoj forenzici. Ona omogućava šifrovanje podataka na način koji ih čini nečitljivim bez odgovarajućeg ključa za dešifrovanje. Moderni algoritmi enkripcije, poput AES (Advanced Encryption Standard) i RSA, koriste složene matematičke operacije koje čine dešifrovanje bez ključa praktično nemogućim. Enkripcija podataka na diskovima (npr. BitLocker, FileVault) i mrežnoj komunikaciji (TLS, VPN) otežava pristup digitalnim dokazima. Servisi za razmjenu poruka poput WhatsApp-a, Signal-a i Telegram-a koriste end-to-end enkripciju, što znači da čak ni servis ne može da pristupi sadržaju poruka. Ovo značajno otežava prikupljanje podataka u slučaju kriminalnih istraga. Ransomware šifruje podatke žrtve i zahtijeva otkup za dešifrovanje. Analiza ovakvih slučajeva često zahteva složenu kriptografsku ekspertizu i može biti neuspješna bez pristupa ključu. Postoje specijalizovani alati za "force attack" napade na šifrovane podatke, poput Passware Kit i ElcomSoft, ali oni zahtijevaju značajne resurse i vrijeme. Analiza memorije (RAM) može pomoći u identifikaciji enkripcijskih ključeva koji su aktivni tokom rada uređaja. U mnogim zemljama, forenzičari se oslanjaju na sudske naloge za dešifrovanje uređaja. Međutim, postoji debata o balansu između prava na privatnost i potreba za sprovođenjem zakona.

4.1.PROBLEM PRIVATNOSTI U DIGITALNIM ISTRAGAMA

Digitalne istrage često zadiru u lične podatke pojedinaca, što otvara pitanja privatnosti i etike. Mnogi pravni sistemi priznaju pravo na privatnost kao osnovno ljudsko pravo. Forenzičke istrage mogu uključivati pristup e-mailovima, porukama, fotografijama, zdravstvenim podacima i finansijskim transakcijama, što može biti sporno ako nije striktno opravdano. Sve više podataka se čuva na cloud platformama, što zahtijeva pristup serverima koji se često nalaze u drugim jurisdikcijama. Ovo može stvoriti pravne konflikte između zemalja koje imaju različite zakone o zaštiti podataka. Tehnike poput "dragnet surveillance" (masovnog nadzora) često rezultiraju prikupljanjem podataka velikog broja ljudi, uključujući i nevine korisnike. Ovo izaziva zabrinutost zbog potencijalne zloupotrebe ili curenja podataka.

Postoji potreba za balansiranjem između forenzičke analize i transparentnosti postupaka kako bi se zaštitila prava pojedinaca. Alati za automatizaciju analize, ako nisu pravilno kontrolisani, mogu dovesti do netačnih rezultata ili pretjeranog narušavanja privatnosti.

4.2.BRZI TEHNOLOŠKI RAZVOJ I PROBLEMI ZASTARJELIH METODA

Brz razvoj tehnologije predstavlja ozbiljan izazov za forenzičke stručnjake, koji se često suočavaju sa zastarjelim alatima i metodama. Savremeno digitalno okruženje uključuje širok spektar uređaja (pametni telefoni, IoT uređaji, autonomna vozila), od kojih svaki zahtijeva specifične alate i metode analize. Alati zastarjevaju brzo jer se operativni sistemi i hardver stalno ažuriraju. Stariji forenzički alati možda neće podržavati analizu podataka sa novih uređaja ili sistema, pa nova enkripcijska tehnologija može biti nespojiva sa postojećim alatima. Zlonamerni softver postaje sve sofisticiraniji, koristeći tehnike poput polimorfizma i enkripcije

kako bi izbjegao detekciju. Forenzičari moraju stalno razvijati nove metode za prepoznavanje i analizu ovakvih prijetnji. Mnoge organizacije i agencije nemaju dovoljno resursa za nabavku novih alata i obuku stručnjaka, što može dovesti do zaostajanja u forenzičkim sposobnostima u poređenju sa naprednim tehnikama koje koriste kriminalci.

4.3.PRAVNA I ETIČKA PITANJA

Forenzička analiza digitalnih dokaza nosi sa sobom brojne pravne i etičke izazove koji se tiču očuvanja ljudskih prava, legitimnosti dokaza i etičkog postupanja. Digitalni dokazi moraju biti prikupljeni u skladu sa zakonom kako bi bili prihvaćeni na sudu. Očuvanje lanca nadležnosti (chain of custody) ključni je aspekt pravne validnosti. Cyber kriminal često uključuje više zemalja, što izaziva probleme jurisdikcije i primjene zakona. Na primjer, forenzičari iz jedne zemlje možda neće imati pravo da pristupe serverima u drugoj zemlji. Stvaranje "backdoor" pristupa za šifrovane sisteme radi olakšavanja forenzičkih istraga izaziva debatu o bezbjednosti i privatnosti. Takvi pristupi mogu biti zloupotrebljeni od strane kriminalaca ili autoritarnih režima. AI alati za analizu podataka mogu rezultirati pristrasnim zaključcima ako nisu pravilno dizajnirani i testirani. Takođe postoji zabrinutost zbog mogućnosti automatizovanog donošenja odluka koje utiču na prava pojedinaca. Forenzičari moraju biti obučeni ne samo u tehničkim vještinama, već i u razumijevanju etičkih i pravnih implikacija svojih postupaka. Održavanje integriteta i nepristrasnosti ključni je element profesionalne etike u ovoj oblasti.

ZAKLJUČAK

Računarska forenzika je ključna u borbi protiv cyber kriminala i zaštiti digitalnih podataka. Tehnološki napredak i rast složenosti cyber napada povećali su potrebu za naprednim metodama analize digitalnih dokaza. Forenzičari sada mogu precizno identifikovati izvore napada i analizirati njihove taktike, što pomaže u razjašnjavanju okolnosti napada.

Zbog toga što se digitalni dokazi brzo brišu ili modifikuju, pravilno prikupljanje i očuvanje podataka postaje od presudnog značaja, kako za analize, tako i za pravne postupke. Međutim, forenzika se suočava sa izazovima kao što su enkripcija, koja otežava pristup podacima, te etička i pravna pitanja vezana za privatnost i ljudska prava. Razvoj naprednih alata za analizu malvera, kao i upotreba vještačke inteligencije i mašinskog učenja, biće ključni za efikasnost istraživanja. Takođe, rast upotrebe IoT uređaja stvara nove izazove u analizi podataka. Iako

mnoge zemlje imaju zakonske okvire za forenziku, globalna saradnja i harmonizacija zakonodavstva su od ključne važnosti u borbi protiv transnacionalnog cyber kriminala. Budućnost računarske forenzike zavisi od stalnog razvoja novih tehnologija, edukacije stručnjaka i prilagodbe zakonodavnim promjenama, kako bi se suočili sa sve dinamičnijim digitalnim prijetnjama.

LITERATURA

[1] Cohen, M. E. (2017), Digital Forensics and Cyber Crime: 9th International Conference, ICDF2C 2017, New York: Springer.

[2] Easttom, C. (2020), Computer Security and Digital Forensics, Indianapolis: Pearson.

[3] Kennesaw, G. (2011), Malware Forensics: Investigating and Analyzing Malicious Code, Waltham: Syngress Publishing.

[4] Lynch, C., & Lenz, R. (2013), Investigating Internet Crime: A Handbook for Forensic Professionals, Boca Raton: CRC Press.

[5] Nelson, B., Phillips, A., & Steuart, F. (2018), Guide to Computer Forensics and Investigations, 6th ed., Boston: Cengage Learning.

[6] Peltier, T. R. (2016), Information Security Risk Analysis, 3rd ed., Boca Raton, FL: CRC Press.

[7] Stallings, W. (2017), Cryptography and Network Security: Principles and Practice, 7th ed., Boston: Pearson.