LXIX Konferencija ETRAN, Čačak, 9 - 12. Jun 2025.

# Digitalna forenzika u savremenom svetu: od sajber napada do sudnice

Slađana Pantelić
*Fakultet informacionih tehnologija*
*Metropolitan univerzitet*
Beograd, Republika Srbija
sladjana.pantelic@metropolitan.ac.rs

**Apstrakt:** U digitalno doba, kada se veliki deo našeg privatnog i poslovnog života odvija putem tehnologije, digitalna forenzika postaje ključna alatka u borbi protiv sajber kriminala. Ovo predavanje osvetljava ulogu digitalne forenzike u savremenom društvu – od prvih koraka u otkrivanju i analizi sajber napada, pa sve do upotrebe digitalnih dokaza u pravnim postupcima. Biće reči o osnovnim principima digitalne forenzike, vrstama digitalnih tragova, tehnikama prikupljanja i očuvanja dokaza, ali i izazovima sa kojima se forenzičari suočavaju u okruženju koje se brzo menja. Poseban akcenat biće stavljen na aktuelne pretnje, forenziku u cloud i mobilnim sistemima, kao i na značaj zakonodavnog okvira i etike u forenzičkoj praksi.

**Ključne reči:** digitalna forenzika, sajber napadi, digitalni dokazi, forenzička analiza, prikupljanje i očuvanje dokaza, pravni postupci, etika, zakonodavni okvir

## I. UVOD

U savremenom društvu, gde se tehnologija brzo razvija, sajber kriminal postaje sve sofisticiraniji i teži za otkrivanje. Sa pojavom naprednih digitalnih alata i tehnika, digitalna forenzika se etablirala kao ključna disciplina u borbi protiv sajber kriminala i kao neophodan alat za rešavanje pravnih sporova. Digitalna forenzika uključuje sakupljanje, analizu i očuvanje digitalnih dokaza koji se mogu koristiti u sudskim postupcima. Od otkrivanja sajber napada do primene dokaza u sudnicama, digitalna forenzika ima ključnu ulogu u procesu dokazivanja i obezbeđivanju pravde.

## II RAZUMEVANJE DIGITALNE FORENZIKE

Digitalna forenzika se može definisati kao naučna metoda za istraživanje i analizu podataka sa računara, mobilnih uređaja, mrežnih sistema i drugih digitalnih uređaja, sa ciljem otkrivanja kriminalnih aktivnosti ili neovlašćenog ponašanja. Ovaj proces obuhvata različite tehnike analize podataka, sakupljanje dokaza i očuvanje integriteta dokaza, kako bi se omogućilo njihovo korišćenje u sudskim postupcima.

Digitalna forenzika je široka oblast koja uključuje različite specijalizovane grane, kao što su:

- Forenzika računara: Analiza podataka sa računara, uključujući hard diskove i memorijske uređaje.
- Forenzika mobilnih uređaja: Istraživanje podataka sa pametnih telefona i drugih mobilnih uređaja.
- Forenzika mreža: Analiza mrežnog saobraćaja, identifikacija napada i praćenje saobraćaja u realnom vremenu.
- Cloud forenzika: Praćenje podataka u oblačnim sistemima i rešavanje specifičnih problema koji nastaju zbog distribucije podataka u više geografskih lokacija.

Ove različite grane digitalne forenzike omogućavaju stručnjacima da istraže različite tipove kriminalnih aktivnosti, od hakovanja i sajber napada do prevara na internetu i internog zlostavljanja podataka.

## III SAJBER NAPADI I NJIHOVI DIGITALNI OTISCI

Sajber napadi su postali jedan od najčešćih oblika kriminala u savremenom svetu. Od jednostavnih phishing napada do sofisticiranih napada poput ransomware-a, sajber kriminalci koriste napredne tehnike za obmanu i krađu podataka. U svakom od ovih napada, ostaju određeni digitalni tragovi, koji mogu pomoći istražiteljima da identifikuju napadače i rekonstruiraju događaje.

Sl. 1. Primeri različitih tehnika analize digitalnih dokaza.

Vrste sajber napada

- Phishing: Napadi u kojima napadači pokušavaju da prevare korisnike da otkriju svoje lične podatke (npr. lozinke ili brojeve kreditnih kartica) putem lažnih e-mailova ili web stranica.
- Ransomware: Maliciozni softver koji zaključava podatke na računaru ili mreži i zahteva otkupninu za njihovo otključavanje.



ISBN 978-86-6200-032-3 ©2025 AM & ETRAN
https://doi.org/10.69994/69E25056

- DDoS (Distributed Denial of Service) napadi: Napadi u kojima napadači preplavljuju mrežu ili server sa lažnim saobraćajem, čime uzrokuju prekid u radu usluga.
- Malware: Različiti oblici zlonamernog softvera koji mogu infekovati računare, mobilne uređaje ili mreže i koristiti ih za krađu podataka ili dalja oštećenja.

Digitalni tragovi sajber napada

Kada se desi sajber napad, napadači često ostavljaju tragove u obliku log fajlova, IP adresa, metadata i drugih podataka, koji mogu biti ključni za istraživanje. Forenzičari koriste specijalizovane alate za prikupljanje ovih podataka sa uređaja i mrežnih sistema, a zatim ih analiziraju kako bi rekonstruisali napad i identifikovali počinioce.

Na primer, analiza log fajlova može otkriti vremenske pečate (timestamps), koji mogu pomoći u utvrđivanju tačnog vremena kada je napad počeo, kao i IP adrese koje su korišćene za pristup sistemu. Takođe, analiza metapodataka sa fajlova može pomoći u identifikaciji neovlašćenih izmena ili manipulacija podacima.

Sl. 2. Digitalni dokaz i primena analize.

## IV FORENZIČKE METODE I ALATI U ANALIZI DIGITALNIH DOKAZA

Za pravilno sprovođenje digitalne forenzike, stručnjaci koriste različite metode i alate koji omogućavaju preciznu analizu podataka. Neki od najpoznatijih alata uključuju:

- EnCase: Popularni alat za forenzičku analizu računara koji omogućava duboku analizu hard diskova i drugih medija.
- FTK (Forensic Toolkit): Alat koji omogućava analizu digitalnih dokaza sa računara, mobilnih uređaja i mreža.
- X1 Social Discovery: Alat za analizu podataka sa društvenih mreža, koji može pomoći u prikupljanju informacija relevantnih za istrage.
- Wireshark: Alat za analizu mrežnog saobraćaja koji omogućava praćenje aktivnosti napadača i identifikaciju neovlašćenih pristupa.


Sl. 3. Različiti forenzički alati za analizu digitalnih dokaza.

Pored ovih alata, forenzičari koriste digitalne slike (disk image) kako bi očuvali integritet podataka. Ove slike omogućavaju analizu podataka bez rizika od njihove manipulacije.

## V DIGITALNA FORENZIKA U PRAVNOM SISTEMU

Jedan od ključnih aspekata digitalne forenzike je njena uloga u pravnom sistemu.

Digitalni dokazi se sve češće koriste u pravnim postupcima, ne samo u slučajevima sajber kriminala, već i kod prevara, ucena, pa čak i ubistava. Uređaji kao što su mobilni telefoni, računari i nadzorne kamere često sadrže ključne informacije - lokaciju osumnjičenih, prepiske, ili čak direktne dokaze o izvršenju dela.

Zbog toga je važno da digitalna forenzika poštuje stroga pravila očuvanja dokaza. Svaki korak mora biti dokumentovan i izveden u skladu sa zakonskim procedurama, kako bi dokazi bili prihvaćeni na sudu. Digitalni forenzičari često svedoče kao stručni svedoci, objašnjavajući nalaze sudijama i porotama.

Sl. 4. Pravilni postupak očuvanja digitalnih dokaza.

Digitalni dokazi mogu imati presudnu ulogu u dokazivanju krivice ili nevinosti u sudskim postupcima. Međutim, postavljanje digitalnih dokaza pred sud može biti izazovno zbog:

- Verifikacije autentičnosti: S obzirom na to da digitalni dokazi mogu biti lako manipulirani, veoma je važno da forenzičari koriste odgovarajuće metode za očuvanje integriteta podataka.
- Pravna validnost: U mnogim zemljama, zakoni o digitalnim dokazima su još uvek u fazi razvoja. Na primer, zakonodavstvo poput GDPR-a u Evropskoj uniji postavlja dodatne prepreke za prikupljanje podataka, posebno kada se radi o zaštiti privatnosti.

Iako postoje izazovi, digitalni dokazi se sve više prihvataju u sudnicama. Mnoge sudske odluke u savremenom svetu oslanjaju se na digitalnu forenziku, jer omogućava jasnu i preciznu rekonstrukciju događaja, što može biti ključ za donošenje pravične presude.

## VI PRAVNA I ETIČKA PITANJA U DIGITALNOJ FORENZICI

Digitalna forenzika ne samo da se bavi tehničkim izazovima, već i pravnim i etičkim pitanjima. Neka od glavnih pitanja koja se postavljaju su:

Sl. 5. Zaštita privatnosti.

- Zaštita privatnosti: Kako balansirati između potrebe za prikupljanjem digitalnih dokaza i zaštite prava na privatnost?
- Zakonodavne prepreke: Kako različiti zakoni, kao što su GDPR ili zakoni o zaštiti podataka, utiču na prikupljanje i upotrebu digitalnih dokaza?
- Upotreba veštačke inteligencije: Kako veštačka inteligencija utiče na forenzičke istrage, posebno u kontekstu predviđanja i prepoznavanja obrazaca ponašanja napadača?

## VI ANTIFORENZIKA

Sa razvijem oblasti digitalne forenzike, vremenom je došlo do razvoja i oblasti antiforenzike. Antiforenzika (ili anti-forenzička tehnologija) je skup metoda, tehnika i alata koji se koriste za ometanje, prikrivanje, uništavanje ili izobličavanje digitalnih dokaza, s ciljem da se onemogući ili oteža digitalna forenzika – tj. istraga digitalnih tragova od strane istražnih organa ili analitičara.

Glavni ciljevi antiforenzike su:

1. sakrivanje postojanja podataka,
2. modifikovanje ili uništavanje podataka,
3. zavaravanje forenzičkih alata ili stručnjaka,
4. zamagljivanje identiteta korisnika.

Najčešće antiforenzičke tehnike su:

| Tehnika | Objašnjenje |
|---|---|
| **Brisanje i prepisivanje podataka** | Korišćenje alata za bezbedno brisanje (npr. shred, BleachBit) koji prepisuju sektore više puta da bi se onemogućio oporavak. |
| **Šifrovanje fajlova ili celih diskova** | Korišćenje alata poput VeraCrypt ili BitLocker za zaštitu sadržaja. Bez lozinke, podaci su nečitljivi. |
| **Steganografija** | Sakrivanje podataka unutar drugih fajlova (npr. u slikama ili audio fajlovima). |
| **Manipulacija vremenskim oznakama (timestamp)** | Promena vremena kreiranja, pristupa ili modifikacije fajlova kako bi se zbunila istraga. |
| **Rootkitovi i malware** | Instalacija softvera, koji prikriva aktivnosti ili prisustvo zlonamernih fajlova i procesa. |
| **Anonimizacija i lažni tragovi** | Korišćenje mreža kao što su Tor, VPN-ova, ili čak ubacivanje lažnih logova kako bi se prikrila lokacija ili identitet. |

Antiforenzika može imati legitimne primene (npr. zaštita privatnosti, šifrovanje ličnih podataka), ali se često koristi u ilegalne svrhe – poput prikrivanja tragova kibernetičkog kriminala.

U mnogim jurisdikcijama, korišćenje antiforenzike u kontekstu istrage (npr. uništavanje dokaza) može se smatrati ometanjem pravde**.**

## VII ZAKLJUČAK

Digitalna forenzika je ključni alat u borbi protiv savremenog sajber kriminala. Sa napretkom tehnologije i sve sofisticiranijim napadima, digitalna forenzika postaje sve važnija u procesu prikupljanja, analize i primene dokaza u sudskim postupcima. Iako postoje izazovi, kao što su pravna pitanja i zaštita privatnosti, digitalna forenzika i dalje predstavlja temelj za održavanje sigurnosti i pravde u digitalnom svetu.

## LITERATURA


[1] Matt Bishop, Introduction to Computer Security, Addison-Wesley, 2004.

[2] W. Stallings, L. Brown, Computer Security: Principles and Practice, Prentice Hall, 2008.

[3] M. Stamp, Information Security, Principles and Practice, John Wiley & Sons, 2006.

[4] Peter G. Smith, Linux Network Security, (Charles River Media Networking/Security, 2005.

[5] Daniel J. Barrett, Richard E. Silverman, Robert G. Byrnes, Linux Security Cookbook, Publisher: O'Reilly Media, 2003.

[6] Principles and Practice, Prentice Hall, Upper Sadle River, 2005.

[7] Managment Handbook, 6th edition, Auerbach Publications, 2006. Charles P. Pfleeger, Shari Lawrence Pfleeger, Security in Computing, Prentice Hall,2006.

[8] https://www.cs.purdue.edu/homes/ninghui/courses/426_Fall10/handouts/426_Fall10_lect21.pdf

[9] https://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76

[10] https://en.wikibooks.org/wiki/The_Computer_Revolution/E_commerce/B2C

[11] https://computer.howstuffworks.com/computer-forensic.htm

[12] https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems

[13] https://www.thegeekstuff.com/2010/08/snort-tutorial/

[14] https://www.thegeekstuff.com/2011/01/iptables-fundamentals/

[15] https://www.networkworld.com/article/2255950/lan-wan/chapter-1--types-of-firewalls.html

[16] https://www.offensive-security.com/metasploit-unleashed/

[17] http://nmap.org/bennieston-tutorial/

[18] https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture10.pdf.