# FORENZIKA RAČUNARSKIH MREŽA

*Ratomir* Đ. Đokić, *Milorad* S. Markagić,
Univerzitet odbrane u Beogradu, Vojna akademija,
Katedra telekomunikacija i informatike, Beograd

DOI: 10.5937/vojtehg61-1493

OBLAST: telekomunikacije, informatika
VRSTA ČLANKA: stručni članak

*Sažetak:*

*Digitalna forenzika predstavlja skup naučnih metoda i postupaka za prikupljanje, analizu i prezentaciju dokaza koji se mogu pronaći na računarima, serverima, računarskim mrežama, bazama podataka, mobilnim uređajima, kao i svim ostalim elektronskim uređajima na kojima je moguće memorisati (sačuvati) podatke.*

*Digitalna forenzika računarskih mreža bavi se analizom digitalnih dokaza koji se mogu naći na serverima ili korisničkim uređajima, a koji su razmenjeni internom ili eksternom komunikacijom preko lokalne ili javne mreže. Takođe, javlja se potreba i za utvrđivanjem mesta i načina nastanka poruke, utvrđivanja identifikacije korisnika, kao i otkrivanjem vrste manipulacija putem logovanja na korisnički nalog. U ovom radu prikazani su osnovni elementi računarskih mreža, programi koji se koriste za komunikaciju i opisane metode prikupljanja digitalnih dokaza i njihove analize.*

*Ključne reči: forenzika, serveri, digitalizacija, računarske mreže.*

## Uvod

Osnovno polje delovanja digitalne forenzike je polje rekonstrukcije oštećenih i pronalaženje skrivenih ili šifrovanih podataka.

Mrežna forenzika, kao deo digitalne forenzike, bavi se bezbednošću mreža, otkrivanjem napada, neovlašćenih pristupa i zloupotrebi mreža.

Sve istrage o napadima na mreže ili neovlašćenim upadima u mrežu tretiraju se kao istrage u polju mrežne forenzike.

Osnovni problemi koji se javljaju prilikom ove istrage jesu kako zaustaviti upad u mrežu, a pritom sačuvati neoštećene dokaze za kasniju analizu ili upotrebu na sudu.

Mrežna forenzika ispituje podatke koji se menjaju u realnom vremenu, sa ogromnim količinama podataka koji se mogu naći u protoku ili memorisati (sačuvati) na mreži bez prekoračenja kapaciteta. Mreže su, u stvari, saobraćajnice digitalnog prenosa podataka velikog kapaciteta, što forenzičku istragu čini veoma teškom i zahtevnom (Caloyannides, 2009).



djokicr@mail.ru

U upotrebi je veliki broj javno dostupnih antiforenzičkih alata, koji po svojoj prirodi nisu namenjeni za nedozvoljene radnje, ali ih korisnici maksimalno eksploatišu, pa se velika količina digitalnih dokaza nepovratno gubi.

## Mesto i uloga forenzike računarskih mreža

Sistemi za otkrivanje upada na mrežu (Intrusion Detection Systems-IDS) mogu pronaći i pratiti mrežne informacije, ali se forenzičkim alatima dopunski može sprovesti analiza vremenskog toka mrežnog saobraćaja, rekonstrukcija elektronskih poruka, analiza metapodataka ili analiza paketa odnosno okvira, da bi se matematičkim metodama dokazalo da podaci nisu promenjeni od momenta kada su pronađeni i snimljeni.

Sledeći aspekt mrežne forenzike je skup forenzičkih softvera koji deluju na mrežu, a imaju iste metode i postupke kao da se vrši forenzička obrada računara. To znači da je moguće sprovesti forenzičku analizu preko mreže, a da pri tome nije neophodan fizički pristup istraživanom uređaju.

Naravno da je veoma važno napomenuti da je forenzička istraga preko mreže tehnološki izvodljiva, ali treba uzeti u obzir zakonska ograničenja, pre svega onih koji regulišu privatnost komunikacija i privatnost podataka o ličnosti.

Svi poznati mrežni sistemi su standardizovani u velikoj meri, pa je time olakšana istraga, jer je moguća primena istih alata prilikom analiza svih sistema i mreža.

Osnovna struktura rada mrežnog forenzičkog sistema zasnovana je na klijent-server odnosu.

Na serverima se nalaze svi podaci, a klijenti spojeni na neki od servera preuzimaju i primaju podatke sa njega. U forenzici računarskih mreža ovaj je model pretrpeo izvesne promene, tako da umesto da klijent komunicira sa serverom, to čini agent. Pri tome agenti ili senzori prenose informacije serveru.

Prilikom upotrebe mrežnih forenzičkih agenata, pri prosleđivanju podataka aktivirane su zaštitne mere koje onemogućavaju menjanje podataka prilikom tranzita i proveru da li su podaci sumnjivi ili sigurni sa tehničko-tehnološkog stanovišta. Agenti se koriste u korisničkim računarima, dok se senzori smeštaju na mrežnoj opremi u usmerivačima ili preklopnicima.

Mrežni forenzički alati mogu se razvrstati u nekoliko grupa.

1. Server za upravljanje i kontrolu (Command and control server)

upravlja operacijama mrežnih forenzičkih alata, pa u većini slučajeva dolazi s GUI programskim paketom preko kojega je moguća jednostavna komunikacija sa svim delovima mrežnog forenzičkog sistema. Iz tog servera postavljaju se programski agenti, akvizicijski parametri, dobavlja se slika, te sve ostale akcije prikupljanja i analize.

2. Server za čuvanje (storage server) služi za čuvanje svih podataka preuzetih sa mrežnih izvora. Podaci prikupljeni od agenata i senzora se ispituju, forenzički autentifikuju i tek tada smeštaju u objekat čuvanja. Velikim količinama podataka na tim serverima upravljaju baze podataka (SQL).

3. Agenti, od kojih većina nije veća od 200 KB, te rade u prikrivenom načinu rada, prikupljaju i podatke koje OS ne vidi ili do kojih nema pristupa, a razmešteni su po istraživanim sistemima ili mrežama. Softver forenzičkih agenata može se maskirati kao jedan od standardno korišćenih programa, a svoje informacije da šalje kriptovano, čak i nasumičnim redosledom kako bi se zamaskirao pravi tok podataka. Ukoliko je potrebno preneti veliku količinu podataka, kako bi njihov prenos ostao neprimećen, forenzički softver se podešava tako da prenos obavlja onda kada je saobraćaj na mreži minimalan.

Većina mrežnih uređaja je standardizovana u interakciji sa drugim mrežnim uređajima, ali unutar svakog tipa takvog uređaja, kao što su usmerivači, preklopnici ili privatna čvorišta (Hub), postoje mnoge varijacije konfiguracija i mogućnosti postavki.

## *Kategorizacija podataka*

Tipovi podataka koji se mogu otkriti koristeći mrežne forenzičke alate variraju od forenzičkih kopija tvrdog diska do dnevnika usmerivača.

Podaci se prikupljaju sa određenih uređaja. To su:

– host računar. Sprovodi se standardna forenzička akvizicija - image uređaja za čuvanje podataka, sadržaj radne memorije, statički dokazi fizički locirani unutar dosega agenata. Svi ovi podaci prebacuju se na forenzički server. Dodatno se sakupljaju i podaci u stvarnom vremenu koji se nalaze u mrežnoj kartici računara. Host računari su radne stanice, ali i serveri (mrežni, server elektronske pošte, serveri baza podataka...).

– usmerivač (Router). Dizajniran je za prenos podataka između mreža. Tipovi informacija koje se nalaze na usmerivaču vezane su uz dnevnike saobraćaja, čuvanje mrežnih razgovora ili dokumenata. Dnevnici saobraćaja sadrže greške koje su se dogodile tokom usmeravanja i statusne informacije komponenti usmerivača. Usmerivači čuvaju određen broj IP i MAC adresa koje vode do ostalih mreža i host računara (Swaminathan, et al., 2009), (Carrier, 2009).

– zaštitni zid (firewall). Sadrži detaljne dnevnike aktivnosti na sistemu, kao što su pokušaji napada, neovlašćenog pristupa, nedostavljanih paketa, bezbednosna pravila, aplikacije koje imaju ili nemaju dozvolu komuniciranja s mrežom ili primanja podataka s mreže, izvore sumnjivih akcija, protokole i servise koji se aktiviraju pri pokušaju neovlašćenog upada, kao i napadačevu IP adresu.

– preklopnik (switch). Korisne informacije nalaze se u sadržajnoj adresabilnoj memoriji (Content addressable memory – CAM). U njoj su smeštene informacije o pridruživanju MAC adresa specifičnim portovima,

kao i podaci o virtualnim lokanim mrežama (Virtual local area netwotk – VLAN). Preklopnici ne vode dnevnike aktivnosti, zbog toga što ne poseduju dovoljno memorijskih ili procesorskih kapaciteta, ali su korisni za dodavanje mrežnih ogledala, koja se koriste za kopiranje tokova podataka u stvarnom vremenu (Swaminathan, et al., 2009), (Caloyannides, 2009).

– sistemi za otkrivanje upada (IDS). U IDS dnevnicima sadržane su sve aktivnosti procenjene kao sumnjive. Ovi dnevnici služe za naknadnu analizu i otkrivanja načina sprečavanja sličnih sumnjivih događaja u budućnosti. U njima su sadržane sledeće informacije: rezultati skeniranja portova, saobraćaj koji dolazi sa nepoznatih portova ili sumnjivih protokola, prepoznate pretnje kao što su crvi, virusi ili neovlašćeni pokušaji pristupa mreži, anonimni pokušaji korišćenja FTP servisa mreže i IP adrese napadača.

– sistem za sprečavanje upada (Intrusion prevention system – IPS).

Sistem blokira ili gasi primećene potencijalne pretnje na mreži. IPS u dnevnicima zapisuje gotovo iste tipove informacija kao i IDS, ali je njegov glavni zadatak analiza podataka na mreži u realnom vremenu i utvrđivanje potencijalnih pretnji sistemu:

– mrežni štampači. U dnevnicima štampača mogu se pronaći dokumenti, slike i ostale informacije poslate na štampanje, ponekad i sa pripadajućim metapodacima. Na većinu današnjih mrežnih štampača moguće je postaviti agenta koji će presretati sve podatke poslane na njega.

– mrežni uređaj za kopiranje. U njegovim se dnevnicima mogu pronaći slične informacije kao i kod mrežnih štampača.

– bežične tačke pristupa (Wireless acess point – WAP). Dnevnici sadrže sve informacije kao i kod žičanog usmerivača, sa dodatkom informacija kao što su SSID i dolazne pristupne veze.

## *Rekonstrukcija događaja sa podacima o saobraćaju na mrežama*

Većina mrežnih forenzičkih alata analiziraju prikupljene podatke i rekonstruišu događaje i vremenski tok automatizovanim procesima, ali je ipak poželjno da istražitelj razume osnovne koncepte i način na koji je alat došao do tih rezultata.

Prvi korak u analizi prikupljenih podataka je korelacija vremenskih oznaka prikupljenih iz različitih izvora, i za iste i za povezane podatke. Dave Mills, Universitiy of Delawear, razvio je protokol koji sinhronizuje sve uređaje na mreži, te time otklanja potrebu ručnog postavljanja vremenskih funkcija svake mrežne komponente. Protokol mrežnog vremena (Network Time Protocol – NTP) održava vremenska podešenja svih mrežnih komponenti tačnosti jedne milisekunde od koordiniranog univerzalnog vremena (Coordinated Universal Time – UTC), (Caloyannides, 2009).

Mrežna komunikacija oslanja se na precizne vremenske oznake kako bi sve izmene podataka funkcionisale ispravno; preciznost je veoma važna u sinhronizovanim mrežama velike brzine, finansijskim softverima, poslovnim komunikacijama, bezbednosnim i vojnim aplikacijama i sl.

Mrežne komponente, osim IDS i IPS i njima sličnih sistema, samo prosleđuju pakete i podatke do njihovog odredišta. IPS sistemi vrše analizu podataka kako bi utvrdili da li postoji pretnja odredišnom računaru, a za podatke se uglavnom brine host računar mreže.

Host računar koristi Transmission Control Protocol/Internet Protocol (TCP/IP) za slaganje tokova podataka u razumnu celinu. Podaci se protokolom razlažu na pakete i šalju do odredišta, gde se sastavljaju korišćenjem sekvencijskih brojeva i potvrda. Istražitelj može ponovo sastaviti pakete uhvaćene na mreži korišćenjem njihovih sekvencijskih brojeva.

## *Prepoznavanje tokova podataka*

Jedan od načina raspoznavanja jednog to  ka podataka od drugog jeste pregled korišćenog protokola pomoću kojeg su podaci poslati. Broj dostupnih protokola zaista je veliki, ali većina proizvođača softvera koristi standardne protokole kako bi se osigurala kompatibilnost u mrežama (Caloyannides, 2009).

Najčešće korišćeni mrežni protokoli su:

– ARP (Address Resolution Protocol): pronalazi MAC adresu na temelju IP adrese drugog hosta,

– ICMP (Internet Control Message Protocol): šalje poruke greške i ostalih informacija,

– IPS (Internet Protocol Security): bezbednosni protokol koji kriptuje ili autentifikuje pakete podataka,

– BitTorrent: koriste ga peer-to-peer mreže za prenos velikih količina podataka,

– DNS (Domain Name System): prevodi IP adrese u lakše čitljiva imena,

– DHCP (Dynamic Host Configuration Protocol): host računari koriste ovaj protokol za dobijanje IP adresa na mreži,

– FTP (File Transfer Protocol): pomaže prelazu podataka sa jednog host računara na drugi, preko mreže,

– HTTP (Hyper Text Transfer Protocol): prenosi podatke kao što su internet stranice sa jednog host računara na drugi,

– IMAP (Internet Message Access Protocol): koristi se u sistemima elektronske pošte,

– NTP (Network Time Protocol),

– POP3 (Post Office Protocol version 3): protokol elektronske pošte koji pribavlja elektronske poruke sa mreže,

– SSH (Secure SHell): stvara siguran kanal između host računara na mreži,

– SMTP (Simple Mail Transfer Protocol): protokol elektronske pošte, korišćen za njeno slanje preko mreže.

## *Mrežni forenzički alati*

Mrežni alati sakupljaju podatke iz već postojećih dnevnika aktivnosti komponenti mreže ili se instaliraju na mrežu radi sakupljanja podataka u realnom vremenu.

## *Mrežni ispitni pristupi*

Test Access Port – TAP, ključni su u mrežama koje sadrže preklopnike, zbog toga što preklopnici prosleđuju podatke samo među portovima koji aktivno komuniciraju.

Mrežni TAP ugrađuje se direktno na mrežni medij, pa može nadzirati sav saobraćaj koji dolazi i izlazi iz preklopnika na svim portovima (Nolan, et al., 2005). Kada podaci stignu do preklopnika, kopira se celi tok podataka, a oni nesmetano nastavljaju put ka odredištu.

Mrežni TAP može se smatrati stostrani hub velike brzine, jer mu ne trebaju IP ili MAC adrese, zbog toga što samo kopira podatke, i to sve od loše formiranih paketa do VLAN informacija. Moguće ga je instalirati na mreže ostvarene optičkim kablovima, standardnim kablovima, pa čak i WAN (Wide Area Network). Omogućava istovremeno kopiranje podataka sa obe strane razmene podataka na mreži. TAP portovi ne zahtevaju dodeljivanje adresa i nevidljivi su svim učesnicima u razmeni podataka na mreži. Time nisu ni podložni napadima, jer čak i ako neko primeti mala kašnjenja prilikom dostave podataka, nema načina da pronađe uzrok. Nedostatak TAP portova jeste da kopiraju sve, pa ukoliko istražilac ne filtrira podatke, memorisanje celokupnog materijala može biti problematično. Drugi nedostatak je da udvostručuje količinu saobraćaja na mreži ukoliko se koristi ista mreža koja se nadzire za prebacivanje podataka na medij za čuvanje.

## *Ogledala*

Mrežni usmerivači i preklopnici koriste višestruke portove. Preslikavanje portova koristi se kada je potrebno svesti saobraćaj na jedan port gde IDS analizira saobraćaj i pronalazi potencijalno opasne podatke ili alat za forenzičku analizu i bezbednost.

Način na koji preklopnik ili usmerivač prenosi podatke sa jednog porta na drugi, i kojom se brzinom radi, ograničavaju i korisnost ogledala (Mirrors). Na mrežama velike brzine gubljenje podataka zbog kolizija i odbačenih podataka povećava se porastom saobraćaja na mreži. Ukoliko se u tom slučaju sav saobraćaj ogleda na jednom portu, mrežni se uređaj zakrči podacima (Nolan, et al., 2005). Najčešća upotreba ogledala na portovima je kopiranje mrežnog saobraćaja određenog računara ili korisnika. Ogledalu je moguće pristupiti sa udaljene lokacije, pa je ranjivo za napade i promene konfiguracija.

### *Promiskuitetni NIC*

Ova metoda prikupljanja i nadziranja podataka se ne koristi baš često. NIC je kartica mrežnog sistema, a dualan spoj na mrežu omogućava nadzor i skeniranje mrežnog saobraćaja. Jedna od prednosti korišćenja ovog tipa TAP-a jeste da je ugrađen direktno u računar istražioca, pa se podaci ne moraju prenositi preko mreže do medija za čuvanje. Ova činjenica predstavlja i njegov nedostatak, jer nije efektivno mobilan.

### *Bežične mreže*

U mrežama ostvarenim kablovima ili optičkim vlaknima informacije su zarobljene u tom kablu, te ukoliko neko želi pristup tim informacijama mora se fizički spojiti na mrežu. Bežične mreže šalju sve informacije vazdušnim putem, i svako sa antenom pri ruci može kopirati i sačuvati poslate podatke (Volonino, Anzaldua, 2008). TAP mora biti pasivan sistem kako bi prikrio svoje postojanje i bio zaštićen od napada. Sa stanovišta uređaja, može se koristiti bilo šta što je sposobno da prima podatke na datoj frekvenciji, kao što su NIC kartice ili primalac radio-frekvencija.

Važan aspekt pregleda mrežnog saobraćaja jeste koji se tip softvera koristi za pregled i analizu podataka. Prenosni računar sa bežičnom karticom može snimati mrežni saobraćaj, jer već poseduje ugrađene protokole koji prevode bežični signal u digitalni kôd koji OS razume.

Program po imenu Kismet koristi NIC kartice i može raditi pod različitim operativnim sistemima. On generiše dnevnike koji su kompatibilni sa većinom IDS i forenzičkih sistema, pa time olakšava analizu prikupljenih podataka. Treba imati na umu da su podaci koji putuju između bežičnih tačaka pristupa paketi. Ali, ako se podaci presretnu pre nego što napuste bežičnu tačku pristupa, ili nakon što stignu u nju, snimaju se u originalnom obliku.

## Zaključak

Današnja komunikacija među pojedincima i organizacijama nezamisliva je bez upotrebe javnih elektronskih mreža. Sa jedne strane, olakšana je komunikacija i broj i količina podataka za prenos se vrtoglavo uvećavaju, a, sa druge strane, razvoj naučne misli, tehnoloških ostvarenja i ogroman broj softverskih alata omogućavaju lak dostup do informacija na mrežama.

Zbog lakoće dostupnosti hardvera i softvera, velikom broju počinilaca kriminalnih radnji omogućen je lak prodor u informacijske mreže.

Zadatak istražioca na ovom polju jeste da se onemogući neprihvatljivo delovanje na mreže ili, ako do njega ipak dođe, da se otkriju efekti učinjene štete i otklone posledice, kao i da se otkrije počinilac.

## *Literatura*

Caloyannides, M. A., 2009, Forensics Is So Yesterday, IEEE Security & Privacy, Vol. 7, No. 2.

Carrier, B. D., 2009, Digital forensics works, IEEE Security & Privacy, Vol. 7, No. 2.

Nolan, R., Branson, J., Wait, C., O'Sullivan, C., 2005, First responders guide to Computer Forensics, CERT.

Swaminathan, A., Min Wu, K. J., Liu, R., 2009, Component Forensics, IEEE Signal Processing Magazine, Vol. 26, No. 2.

Volonino, L., Anzaldua, R., 2008, Computer Forensics, Wiley Publishing Inc.

COMPUTER NETWORKS FORENSICS

FIELD: Telecommunications, IT
ARTICLE TYPE: Professional Paper

*Summary:*

*Digital forensics is a set of scientific methods and procedures for collection, analysis and presentation of evidence that can be found on computers, servers, computer networks, databases, mobile devices as well as on all other devices where data can be stored (saved).*

*Digital forensics of computer networks is an examination of digital evidence that can be found on servers and user devices, when the evidence is exchanged by internal or external communication through local or public networks. There is also a need for identifying sites and modes of message origins, for establishing user identifications, and for detecting types of manipulation by logging into user accounts. This paper presents the basic elements of computer networks, the software used for communication and the methods of collecting digital evidence and its analysis.*

Introduction

*The primary field of activity is the field of digital forensic reconstruction of damaged data and finding hidden or encrypted data.*

*Network forensics as a part of digital forensics deals with network security, intrusion detection, unauthorized access and misuse of networks.*

*All investigations into attacks on the network or unauthorized intrusions into the network are treated as an investigation in the field of network forensics.*

Place and role of the forensics of computer networks

*Network Intrusion Detection Systems (IDS), can find and track network information; forensic tools can be used for additional analyses of time flow of network traffic, for reconstruction of electronic messages, for metadata analyses and for analyses of packets and frames in order to to prove by mathematical methods that data has not been changed from the moment it was found and recorded.*

*Another aspect of network forensics is a set of forensic software that operates on a network and has the same methods and procedures as in computer forensic processing. This means that it is possible to carry out a forensic analysis over a network without being required to have physical access to the examined device.*

Categorization of data

*Data types that can be detected using network forensic tools range from forensic copies of the hard disk to the log router.*

*Data is collected with the following devices: Host computer, Router, Firewall, Switch, Intrusion Detection Systems (IDS), Intrusion Prevention System (IPS), Network printers and Network copiers.*

Reconstruction of events with the data on network traffic

*Most network forensic tools analyse the data and reconstruct events and the time course through automated processes, but it is still advisable for the investigator to understand the basic concepts and the methods which the tool uses to obtain the results.*

*Data flow identifying*

*One way of distinguishing one data flow from another, is a review of the protocol by which data is sent.*

*There are numerous protocols available, but most software vendors use standard protocols to ensure compatibility across networks.*

*Network forensic tools*

*Network tools collect data from existing activity logs of network components, or they are installed on a network with the aim of collecting data in real time.*

Network Test Access

Mirrors

Promiscuous NIC

Wireless networks

*In networks with cables orr optic fibers, the information is captured within the cable, so if someone wants an access to this information they must be physically connected to the network. Wireless networks send all information by air, and anyone with an antenna at hand can copy and save the sent data. A TAP must be a passive system in order to conceal its existence and protect itself against attacks. Regarding devices, anything capable of receiving data at a given frequency, such as NIC cards or radio frequency receivers, can be used.*

Conclusion

*The present communication among individuals and organizations is unthinkable without the use of public electronic networks. On the one hand, communication is facilitated and the number and the amount of*

*data to be transferred are increasing fast; on the other hand, the development of science, technological achievements and a huge number of software tools provide an easy access to information on networks.*

Keywords: *forensics, servers, digitalization, computer networks*.

Datum prijema članka/Paper received on: 08. 02. 2012.
Datum dostavljanja ispravki rukopisa/
Manuscript corrections submitted on: 28. 02. 2012.
Datum konačnog prihvatanja članka za objavljivanje/ Paper accepted for publishing on: 02. 03. 2012.