**Forenzična analiza operacijskega sistema Linux**

**Avtorji:** Žiga Elsner, Primož Bajželj, Uroš Kastelic, Željko Plesac, Jan Varljen;

Contents

[Povzetek: 1](#_Toc324972925)

[Abstract: 1](#_Toc324972926)

[Uvod v forenzično analizo 1](#_Toc324972927)

[Priprava na analizo 2](#_Toc324972928)

[Forenzična analiza omrežja 3](#_Toc324972929)

[DIGITALNI DOKAZI NA TCP/IP PLASTEH 4](#_Toc324972930)

[Fizična/povezavna plast 4](#_Toc324972931)

[Omrežna in transportna plast 5](#_Toc324972932)

[Aplikacijska plast 5](#_Toc324972933)

[Zaključek 6](#_Toc324972934)

# Povzetek:

Težko bi si pred 15 leti in več zamislili, da bodo računalniki nekoč osrednji cilj forenzične preiskave. V drugem desetletju 21. stoletja, ko pa je človek postal zelo odvisen od računalnikov se to zdi kot nekaj nujno potrebnega. V tem članku bo opisanih nekaj osnovnih principov analize računalniške forenzike z operacijskim sistemom linux.

Ključne besede: forenzična analiza, preiskava diskov, preiskava omrežij, preiskava brskalnikov

# Uvod v forenzično analizo

Znanost forenzične analize je strokovno orientirana za zbiranje in analizo dokazov. Tehnologija, ki se pri tem uporablja pa obsega računalnike ter programsko opremo. Kraj zločina obsega računalnik, omrežje ter naprave na katere je priklopljen.

Delo forenzičnega preiskovalca, da kar najbolje zbere in preiskuje izvore dokazov kot so diski, zgodovine, prenosne medije in drugi. Pri tem je zelo pomembno, da se ohrani čimveč podatkov v originalni obliki ter, da se kar najbolje obnovi dogodke, ki so se pojavili ob določenem kaznivem dejanju.

Vsako dejanje, ki se zgodi je lahko drugačno in v enem primeru lahko obsega zgolj nek računalnik medtem, ko v drugem lahko obsega cele računalniške sisteme z ogromno količino podatkov z kompliciranem obsegom dogodkov.

Preiskovanje se lahko v začetku velikokrat izkaže kot iskanje igle v senu, saj je lahko veliko stvari skritih. Prav tako velja, da ne obstaja nek recept, ki korak za korakom pove kaj je potrebno narediti, ampak se je situaciji potrebno sprotno prilagajati.

Pomembno je, da pri vsaki preiskavi skrbno popisujemo vsak korak naše preiskave - na kakšen način smo pridobili dokaze, katere programe in tehnike smo pri tem uporabili. To je pomembno, da lahko tretja oseba ponovi celotni postopek še enkrat in pridobi enake rezultate. Prav tako nam to lahko v kasnejšem obdobju pomaga, da se spomnimo ter postopek, če je le to potrebno povemo na sodišču. Poleg tega pa nam lahko te zapiski pomagajo ob podobnih primerih, kar lahko znatno zmanjša stroške preiskave primera in sojenja nekega računalniškega kaznivega dejanja.

Za forenzično analizo je pomembno, da si za to pripravimo temu namenjen računalniški sistem s katerim bomo čimbolj učinkovito prišli do želenih rezultatov. Le ta naj bi med drugim omogočal analizo diskov, preiskovanje omrežij, brskalnikov, zgodovine in drugo. Primer takega sistema bi lahko bil sestavljen iz sledečih komponent:

* računalnik s hitrim procesorjem,
* matično ploščo z vsaj tremi IDE kontrolerji za trde diske, cd in dvd enote,
* podporo za prenosne medije kot so npr. USB ključki,
* vsaj dva velika trda diska, katera imata dovolj prostora za operacijski sistem, forenzična orodja ter za kopiranje particij ter izbrisanih datotek iz dokaznega računalnika,
* SCSI kartico, ki omogoča priključitev diskov, magnetnih trakov, skenerjev, printerjev,
* magnetne trakove, ki omogočajo shranjevanje velikih particij,
* sistem mora imeti celotno podporo za omrežje na katerem pa ni zagnana nobena omrežna storitev razen SSH (ki se uporablja za prenos datotek in zavarovan oddaljen mrežni dostop),
* operacijski sistem linux, kjer je ena boljših izbir Red Hat Linux - Shrike (linux izberemo, ker ima precej boljšo podporo od drugih operacijskih sistemov).

Zelo priročen pa je prenosni računalnik (ne mac), ki omogoča, da "forenzični laboratorij" prinesemo kar na mesto zločina.

# Priprava na analizo

Pred začetkom analize sistema je potrebno slediti istim osnovnim korakom za pripravo sistema:

* V nekaterih primerih je pred razstavljanjem in premikanjem računalniški sistem potrebno slikati. To je potrebno že v osnovi, ko je v nekaterih primerih potrebno slikati kraj zločina oz. v drugih primerih, ko je potrebno dokumentirati komponente sistema, kar nam kasneje omogoča vrnitev sistema v prvotno stanje.
* Potrebno je pisati dnevnik preiskave v katerega se čimbolj podrobno zapisuje celoten potek dela. Le ta vključuje datum začetka preiskave ter začetek in konec določene aktivnosti. Zelo pomembno je tudi beleženje morebitnih prekinitev med aktivnostmi. Tak pristop služi sprotnemu ustvarjanju poročila, ki je bolj konsistentno in detajlno kot, če bi ga spisali na koncu. Taki podrobni zapiski bodo občutno boljše pripomogli k predstavi celotnega zločina, kot pa velika količina dokazov, ki se lahko naberejo tudi pri najmanjših računalniških zločinih.
* Preden zaključimo sistem je priporočljivo zbrati osnovne informacije o disku, ki ne bo več spremenjen s strani tretje osebe. Pod to spada zgradba datotečnega sistema (/etc/fstab), katerega prikaz lahko vidimo na sliki 'fstab.png', ime gostitelja in IP naslove iz (/etc/hosts), ki so prikazani na sliki 'hosts.png', naprave (/var/log/dmesg) in sistemska sporočila (/var/log/syslog). To lahko najlažje naredimo s tar arhivom kot je prikazano na sliki 'sys\_log.png'.
* V kolikor je možno je nujno potrebno narediti kopijo celotnega diska ter delati na kopiji in ne na originalu! Če delamo na originalu obstaja velika možnost, da zaradi majhne napake uničimo dokazno gradivo. Original moramo hraniti na varnem mestu, kjer ga ni možno uničiti ali spremeniti.
* Ob začetku je potrebno priklopiti disk na prosta IDE vrata in zagnati sistem. Ob tem moramo biti zelo previdni, da ne uničimo diska. Če nimamo prostih IDE vmesnikov potem izklopimo CD-ROM enoto iz IDE vmesnika in nanj priključimo ta disk. V BIOSu je morda potrebno tudi preklopiti avtomatsko detekcijo tipa diska.
* Zatem moramo identificirati particije na disku z uporabo ukaza "fdisk". Pri tem ukaza ne smemo uporabljati v interaktivnem načinu, saj s tem lahko spremenimo particijsko tabelo. Prikaz uporabe ukaza oz. identifikacijo particij lahko vidmo na sliki 'partition\_table.png'. Pri tem lahko opazimo lastnosti diska ter npr. predvidevamo, da je na /dev/sda1 linux sistem.
* Zaradi varnostnih razlogov moramo generirati MD5 vsoto vsake particije, dobiti bitno sliko diska in preveriti s prej dobljenimi vsotami. (mt, dd, 5/27, morda potrebno še dodati). Če se vsote ne ujemajo pomeni, da se je lahko pokvaril le en bit, kar pa se lahko pojavi npr. zaradi slabih sektorjev ali napake pri samem kopiranju.
* Zatem je potrebno pripeti particijo za katero menimo, da je sistemska particija, ki pa je ne smemo spreminjati. Particijo pripnemo z ukazom "mount -r /dev/sda /mnt" in pri tem uporabimo samo bralni način. Iz pripete particije izpišemo vse datoteke z ukazom "ls -lat /mnt", kjer nato lahko tudi ugotovimo ali gre res za sistemosko particijo. Z pregledom "/mnt/etc/passwd" si lahko izpišemo uporabniške račune, ki so bili ustvarjeni do sedaj. Pri tem smo pozorni na sumljiva imena. Te zapise si shranimo zato, da se kadarkoli kasneje lahko vrnemo nazaj in začnemo preverjati sledi določenega uporabnika. Iz teh zapisov lahko naredimo različne predpostavke o znanju vsiljivca ali lastnika računalnika ter pri tem pazimo, saj so lahko bili le ti tudi načrtno uporabljeni kot diverzija za pravo zlorabo.
* Poskušati moramo zgraditi pomembne dogodke jih povezati z določenimi aktivnostmi ter slediti do njihovega izvora. Po možnosti poskušamo tudi ponoviti napadalčeve korake in s tem odkriti njegov pravi namen ter ugotoviti s katerimi orodji in sistemi je izvedel napad.

Od tu naprej pa se lahko začne forenzična analiza preiskave sistema z standarnimi UNIX orodji.

# Forenzična analiza omrežja

Do nedavnega je veljalo, da je bilo pri preiskavi potrebno preverjati zgolj računalnik in predvsem disk posameznika. V zadnjem času, ko pa je omrežje postalo svetovno razširjeno in velika večina ljudi uporablja e-maile, socialna omrežja, internetne trgovine, pretakanje preko spleta in druge omrežne storitve je pregledovanje postalo precej bolj prepleteno tudi z omrežjem. Forenzični preiskovalci se morajo tako naučiti še enega področja in poznati različna orodja. Med drugim morajo poznati standarde za internetne protokole, brskalnike, e-maile, prenos datotek kar jim je še dodatno oteženo zaradi hitro razvijajočega področja. Možno je celo, da preiskovalci sploh nimajo dostopa do posameznega računalnika s čimer celotna analiza poteka preko spleta oz spletnih storitev in s pomočjo internetnih ponudnikov, kreditnih kartic, telefonskih pogovorov in drugo.

Postopki preiskovanja trdega diska za digitalnimi dokazi so dobro definirani. Ko pa se srečamo z omrežjem pa lahko nastopijo nepričakovane ovire. Podatkov na omrežju je ogromno in so dinamični, kar nam onemogoča zajem celotnega stanja v določenem trenutku. V nasprotju z preiskovanjem enega računalnika preiskovalci ne morejo preprosto izklopiti celotnega interneta, saj morajo kljub preiskavi zagotavljati, čimbolj nemoteno delovanje omrežja. Poleg tega to tudi ne bi bilo smiselno, saj bi se ob izklopu izgubili vsi podatki. Naslednja težava je, da je na omrežju praktično nemogoče izolirati kraj zločina, saj kriminalec napada iz večih mest hkrati.

Porazdelitev na večjih delih omrežja pa je lahko tudi pozitivno, saj je tako težko uničiti vse dokaze. Podjetja velikokrat delajo varnostne kopije, ki jih hranijo na različnih lokacijah, kar pomeni, da po vsej verjetnosti ne bodo uničili vseh podatkov.

UNIX sistemi so večinoma konfigurirani tako, da beležijo in hranijo uporabniške podatke za datoteke, e-maile in gesla za oddaljene dostope. Zato je pametno iskati sledi za oddaljene dostope na omrežju, ki lahko vodijo do dodatnih virov dokazov. Prvotnega pomena je, da se to naredi kar se, da hitro še predno se sledi izgubijo.

UNIX sistemi v "/etc/hosts" pogosto hranijo spisek povezav, ki pogosto komunicirajo med sabo. Za UNIX okolje so značilni lokalni in omrežni skupni diski, kateri so hranjeni v "/etc/fstab", saj so avtomatično pripeti ob zagonu. Podobna informacija se nahaja tudi v "/etc/mtab" in "/proc/mounts", ki pa hranita tudi informacije o pripetih napravah preostalih posameznih uporabnikov. Poleg NFS se lahko s pomočjo Samba orodij dostopa tudi do drugih omrežnih virov na Windows okolju. UNIX računalnike lahko konfiguriramo tako, da sistemske podatke pošiljamo na oddaljen sistem s spremembo v datoteki "/etc/rsyslog.conf","/etc/syslog.conf". To naredimo z dodajanjem vrstice "\*.\* @IP:PORT". Podobno velja za tiskanje, kjer se hranijo informacije v datotetki "/etc/printcap".

Pri tem postopku je pomembno, da na oddaljene lokacije dostopamo fizično po standardnih postopkih in ne brez pravne podlage.

## DIGITALNI DOKAZI NA TCP/IP PLASTEH

TCP/IP je skupni jezik vseh omrežij, osnova interneta in je poznan kot de facto standard. Je enostavnejši od OSI modela in med sabo združi nekatere plasti. Razdeljen je na 4 plasti:

* Aplikacijska plast vsebuje naslednje protokole: telnet, ftp, http, smnp, smtp in druge.
* Transportna plast ima protokole: TCP, UDP, ICMP.
* Mrežna plast ima internetni protokol (IP).
* Fizična in povezavna plast pa ima ARPANET, paketni radio in LAN.

Naloga fizične plasti je, da skrbi za fizični prenos podatkov. Mrežna plast skrbi za transparentno pošiljanje podatkov med mrežami. Dostava pri tem ni zagotovljena, niti vrstni red dostave. Povezava s povezavnim slojem je protokol ARP. Prenosna plast skrbi za povezavni in brezpovezavni način delovanja. TCP predstavlja tok podatkov med procesom na različnih računalnikih. Aplikacijska plast služi uporabi standardnih (npr. pošta, splet, IRC in drugo) in nestandardnih aplikacij. Te aplikacije uporabljajo storitve spodnjih plasti.

Dokaze sicer lahko dobimo iz več naprav kot so računalniki, usmerjevalniki in drugih.

### Fizična/povezavna plast

Fizična in povezavna plast nudi temelj za vse mapkar najdemo na omrežju.

Najbolj pogost način za zbiranje dokazov na omrežju je ti. prisluškovanje omrežju. Ta način zbiranja dokazov je primerljiv s tistim, ko naredimo kopijo trdega diska.

* Z orodjem »ifconfig« lahko skonfiguriramo omrežne naprave. Uporablja se predsem ob zagonu za nastavitev vmesnikov ter kasneje za preverjanje ali nastavljanje. Z ukazom "ifconfig -a" lahko preverimo stanje vseh naprav. S tem tudi vidimo IP in MAC naslove.
* Orodje "arp" se uporablja za nastavljanje oz. prikaz ARP tabele relacij med IP in MAC naslovi. Omogoča tudi brisanje oz. dodajanje zapisov. ARP oz. Address Resolution Protocol sicer služi preslikavi naslovov iz omrežne v povezavno plast.

Naslove računalnikov lahko dobimo tudi iz ARP tabel ali zgodovine DHCP na usmerjevalniku. DHCP med drugim hrani informacije o MAC naslovu, IP naslovu, času dodelitve in odvzema ter imenu računalnika.

### Omrežna in transportna plast

Vsak komunikacijski sistem potrebuje mehanizem naslavlanja. Pogosto, ni pa nujno je potreben tudi nek sistem preverjanja, da je sporočilo prišlo na cilj. Omrežna in transportna plast sta skupaj odgovorni za pravilno dostavljanje paketov. Veliko količino shranjenih informacij se pridobi prav iz teh dveh plasti, kar nam zelo služi v digitalnem preiskovanju. Pomembni na tej plasti so predvsem IP naslovi in z njimi povezana DNS imena, ki nam pomagajo določiti izvor zločina.

* Orodje "nslookup" nam omogoča pretvorbo med IP naslovom in DNS imenom, kar lahko vidimo na sliki 'nslookup.png'.
* Z "dig" lahko poizvedujemo o pripadajočih DNS strežnikih. Občasno pri tem lahko dobimo tudi informacije o drugih računalnikih, ki uporabljajo DNS strežnik, a strežniki tega večinoma ne dopuščajo, saj napadalci lahko to s pridom izkoriščajo.
* Druge še zelo uporabno orodje je tudi "traceroute", ki nam omogoča sledenje paketov po vozliščih, ki jih obišče paket, da doseže ciljni IP. To nam v digitalnem preiskovanju lahko pride zelo prav, saj večinoma poti ostajajo iste kar nam omogoča, da naredimo dodatno preiskovanje na vozliščih ali DNS strežnikih, kjer se dodatno beležijo podatki o prenosih.
* Aplikacije za svojo delovanje uporabljajo določena vrata. Za preverjanje ali pa določena aplikacija deluje lahko uporabimo orodje "nmap". To orodje nam dodatno omogoča tudi npr. odkrivanje operacijskega sistema ali verzij programov, ki so lahko povezani tudi z določenimi varnostnimi luknjami. V začetku nam lahko zelo dobro služi za odkrivanje karakterističnih značilnosti v omrežju.
* Orodje "netstat" nam lahko izpiše aktivne povezave našega računalnika, kar nam ob pomoči orodja "nmap" lahko služi kot določanje aktivivnih aplikacij kot je npr. VNC ali skupni vir z drugim računalnikom. Na ta način lahko pridemo do dodatnih virov informacij, ki jih je potrebno raziskati.

### Aplikacijska plast

* Pri preiskovanju na omrežjih je lahko velika količina podatkov nerelevantnih za določen primer. V tem primeru je pametno dobiti zgolj podatke, ki nas zanimajo, kjer si pomagamo npr. z filtriranjem glede na čas, IP naslov, neuspešne poskuse prijave ali glede na primer primerne kriterije. Primer lahko vidimo na sliki 'filter\_tcpdump.png', ki uporablja nativno orodje linuxa oz. 'filter\_tshark.png', ki uporablja orodje tshark.

# Zaključek

V tem članku(?) smo opisali različne aspekte digitalne forenzike s strani operacijskega sistema linux. Digitalna forenzika je področje, ki je sicer že zelo definirano, a se zaradi hitrega razvoja ves čas pojavljajo nove stvari…..blablabla

Zločini zahtevajo pravico, ki pa mora biti pravična in razumna.