Visoko sudsko i tužilačko vijeće Bosne i Hercegovine
Visoko sudbeno i tužiteljsko vijeće Bosne i Hercegovine
Високи судски и тужилачки савјет Босне и Херцеговине
High Judicial and Prosecutorial Council of Bosnia and Herzegovina

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Agency for Development and Cooperation SDC

Priručnik o pretresanju kompjuterskih sistema, uređaja za pohranjivanje

kompjuterskih i elektronskih podataka i mobilnih telefonskih aparata

PROJEKAT

Jačanje tužilačkih kapaciteta u sistemu krivičnog pravosuđa

Irhad Kos, Saša Petrović, Jovo Marković

PRIRUČNIK O PRETRESANJU KOMPJUTERSKIH SISTEMA, UREĐAJA ZA POHRANJIVANJE KOMPJUTERSKIH I ELEKTRONSKIH PODATAKA I MOBILNIH TELEFONSKIH APARATA

Autori:

Irhad Kos

Saša Petrović

Jovo Marković

Sarajevo, 2013

PREDGOVOR

U postupanju policijskih organa i tužilaštava bilježi se stalni porast broja pretresa kompjutera i s njim povezanih uređaja, odnosno drugih uređaja koji služe prikupljanju, pohranjivanju i prijenosu podataka. Navedeno je dovelo do potrebe da se predstavnicima agencija za provođenje zakona i tužiocima predstave bitni standardi i smjernice za pribavljanje i očuvanje elektronskih (digitalnih) dokaza, pri čemu bi trebalo prikazati najbolje prakse u snimanju elektronskih (digitalnih) dokaza koje se primjenjuju sa ciljem sprječavanja njihovog onečišćenja ili gubitka, a u skladu sa tehničkim izazovima koje nameće brza evolucija hardvera (hardware) i softvera (software).

Radna grupa za daljnji razvoj dogovorenih uputstava, operativnih priručnika i policijskih obrazaca, formirana u okviru projekta „Podrška pravosuđu u Bosni i Hercegovini – Jačanje tužilačkih kapaciteta u sistemu krivičnog pravosuđa" (Projekat)[1], bila je jednoglasna u ocjeni da je potrebno posvetiti pažnju izradi posebnog priručnika o pretresanju kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka, kao i mobilnih telefonskih aparata, u smislu odredbe člana 51. stav 2. Zakona o krivičnom postupku Bosne i Hercegovine, odnosno analognih odredbi članova ZKP FBiH, RS i BD o pretresanju pokretnih stvari, a na što upućuje i Uputstvo o postupanju i saradnji OSL (policijskih službenika) i tužioca u provođenju radnji dokazivanja tokom istrage (član 11). Navedeno je i preporuka iz izvještaja koji je rezultat istraživanja koje je obavio angažirani stručnjak u saradnji sa projektnim timom, a koje je obuhvatilo razgovore i intervjue sa tužiocima iz svih tužilaštava u BiH, kao i predstavnicima agencija za provedbu zakona.[2]

Projekat "Podrška pravosuđu u Bosni i Hercegovini – Jačanje tužilačkih kapaciteta u sistemu krivičnog pravosuđa" se realizira u saradnji sa brojnim projektnim partnerima, uključujući i policijske organe svih nivoa i nadležnosti.

U okviru projektne komponente B planirane su intervencije u cilju unaprijeđenja saradnje policije i tužilaca, što obuhvata i identifikaciju potreba za zajedničkom edukacijom policije i tužilaca u vođenju krivičnih istraga i shodno tome razvoj edukativnih modula,

[1] Projekat implementira Visoko sudsko i tužilačko vijeće Bosne i Hercegovine, a finansiran je od strane Vlade Švicarske, posredstvom Švicarske agencije za razvoj i saradnju (SDC) – Švicarske kancelarije za saradnju u Bosni i Hercegovini. Vremenski okvir projekta je 1. oktobar 2010. – 31. mart 2014. godine.

[2] Jadranka Lokmič-Misirača: Izvještaj „Stručna procjena i identifikacija ključnih prepreka za efikasnije krivične istrage" izrađen u okviru projekta "Podrška pravosuđu u Bosni i Hercegovini – Jačanje tužilačkih kapaciteta u sistemu krivičnog pravosuđa".

priručnika i brošura. Navedeno je poslužilo kao osnov za angažiranje stručnih lica iz Državne agencije za istrage i zaštitu (SIPA), Ministarstva unutrašnjih poslova Republike Srpske i Federalnog ministarstva unutarnjih poslova – Federalne uprave policije, koja su izradila jedinstveni Priručnik koji se nalazi pred Vama i na osnovu kojeg je planirana realizacija posebnih programa praktične obuke za predstavnike policijskih organa i tužilaštava u Bosni i Hercegovini.

SADRŽAJ

UVOD

Ovaj priručnik je namijenjen svim tužiocima, sudijama i ostalim službenicima u agencijama za sprovođenje zakona, koji se tokom svog rada susreću sa raznim oblicima elektronskog i bilo kojeg drugog kriminala, gdje se potencijalni dokazi o izvršenim kriminalnim radnjama ili namjeri za njihovo izvršenje mogu nalaziti na raznim elektronskim, magnetnim i optičkim uređajima. Priručnik ne obuhvata sve moguće scenarije iz domena tzv. "***cyber***" kriminala već se prevashodno odnosi na očuvanje mjesta izvšenja krivičnog djela iz oblasti visokotehnološkog kriminala, odnosno prepoznavanje, prikupljanje, siguran transport i čuvanje digitalnih dokaza. Svi policijski službenici koji se nađu u ulozi prvih lica koja su došla u dodir sa eventualnim digitalnim dokazima (u daljem tekstu ***kontakt lica***) treba da se prilagode novonastalim okolnostima uzevši u obzir njihovo znanje iz ove oblasti, sveukupno iskustvo u radu sa dokazima, uslove i dostupnu opremu.

Ciljna grupa kojoj je priručnik namjenjen:

- Tužioci koji učestvuju u istragama.
- Svako ko je uključen u vršenje istražnih radnji, a gdje postoje eventualni digitalni dokazi.
- Sva lica koja rade na privođenju potencijalnh počinilaca kao i obradi mjesta izvršenja krivičnog djela, a gdje postoje eventualni digitalni dokazi.
- Sva lica koja nadziru lica uključena u gore navedene istražne radnje.
- Sva lica koja rukovode organizacionim cjelinama čije je osoblje uključeno u gore navedene istražne radnje.

Pojam pretresa i definicija digitalnih dokaza

Pretres digitalnih dokaza, u smislu pretresa predmeta koji sadrže digitalni dokaz, definisan je zakonima o krivičnom postupku:

ZKP BiH u članu 51. stav 2.definiše:

„Pretresanje pokretnih stvari, u smislu odredbe stava (1) ovog člana, obuhvata i pretresanje kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka, kao i mobilnih telefonskih aparata. Lica koja se koriste ovim uređajima dužna su omogućiti pristup, predati medij na kojem su pohranjeni podaci, te pružiti potrebna obavještenja za

upotrebu tih uređaja. Lice koje odbije njihovu predaju može se kazniti prema odredbi člana 65. stav (5) ovog zakona."

ZKP RS u članu 115. stav 2. definiše:

„Pretresanje pokretnih stvari u smislu odredbe stava 1. ovog člana obuhvata i pretresanje kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka kao i mobilnih telefonskih aparata. Lica koja se koriste ovim uređajima dužna su da omoguće pristup, predaju medij na kome su pohranjeni podaci, te pruže potrebna obavještenja za upotrebu tih uređaja. Lice koje odbije njihovu predaju može se kazniti prema odredbi člana 129. stav 5. ovog zakona."

ZKP FBiH u članu 65. stav 2. definiše:

"Pretraga pokretnih stvari, u smislu odredbe stavka 1. ovoga članka, obuhvaća i pretragu kompjuterskih sustava, uređaja za pohranjivanje kompjuterskih i elektronskih podataka, kao i mobilnih telefonskih aparata. Osobe koje se koriste ovim uređajima dužne su omogućiti pristup, predati medij na kojemu su pohranjeni podaci, te pružiti potrebne obavijesti za uporabu tih uređaja. Osoba koja odbije njihovu predaju može se kazniti prema odredbi članka 79. stavak 5. ovoga Zakona."

ZKP Brčko Distrikta Bosne i Hercegovine u članu 51. stav 2. definiše:

"Pretresanje pokretnih stvari, u smislu odredbe stava 1 ovog člana, obuhvata i pretresanje kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka, kao i mobilnih telefonskih aparata. Lica koja se koriste ovim uređajima dužna su da omoguće pristup, da predaju medij na kojem su pohranjeni podaci, te pruže potrebna obavještenja za upotrebu tih uređaja. Lice koje odbije njihovu predaju može se kazniti prema odredbi člana 65. stava 5. ovog zakona."

Radnja pretresa digitalnih dokaza u smislu pretresanja pokretnih stvari, kako to definiše ZKP, podrazumjeva radnje koje će se preduzeti na licu mjesta zajedno sa radnjama pretresa prostorija ili lica, ili kao zasebna radnja pretresa pokretnih stvari i treba je odvojeno posmatrati od analize (vještačenja) u laboratorijskim uslovima.

Radnja pretresa pokretnih stvari, koje sadrže informacije u digitalnom obliku, podrazumjeva da se na licu mjesta izuzmu informacije u obliku koji će biti prihvatljiv kao dokaz

u daljem postupku, a koje bi bilo nemoguće naknadno dobiti, kao i prikupljanje informacija koje će biti od koristi prilikom vještačenja digitalnih dokaza. To znači da prilikom isključenja električne energije (radi oduzimanja pokretnih stvari) neke informacije se nepovratno gube ili u slučajevima kada je oduzimanje pokretnih stvari nemoguće iz razloga što bi to prouzrokovalo ometanje ili prekid rada nekog pravnog subjekta što bi uzrokovalo veliku ili nepopravljivu štetu. Procjenu o postupanju u ovakvim slučajevima vrše stručna lica rukovodeći se interesima istrage, ali i opštedruštvenim interesima.

Primjer: Pretres u prostorijama određene kompanije, kada su sa centralnog servera koji sadrži baze ličnih podataka, zbog nemogućnosti isključenja servera, izuzeti logovi (evidencije o pristupu bazama podataka, pristupu podacima i obradi podataka) koji su kasnije analizirani.

Definicija digitalnog dokaza

Prema međunarodnoj definiciji u oblasti forenzičkih nauka, digitalni dokaz je svaka informacija u digitalnom obliku koja ima dokaznu vrijednost i koja je uskladištena ili prenesena u takvom obliku. Pojam digitalnog dokaza uključuje kompjuterski uskladištene i generisane dokazne informacije, digitalizovane audio i video dokazne signale, signal sa digitalnog mobilnog telefona, informacije sa digitalnih fax mašina i signale drugih digitalnih uređaja. Znači, digitalni dokaz je bilo koja informacija generisana, obrađena, uskladištena ili prenesena u digitalnom obliku na koju se sud može osloniti kao mjerodavnom, tj. svaka binarna informacija, sastavljena od digitalnih 1 i 0, uskladištena ili prenesena u digitalnoj formi, kao i druge moguće kopije orginalne digitalne informacije koje imaju dokaznu vrijednost i na koje se sud može osloniti u kontekstu forenzičke akvizicije, analize i prezentacije.

UREĐAJI KOJI MOGU SADŽAVATI DIGITALNE PODATKE

Kompjuterski sistem sastoji se od harvera i softvera koji rade zajedno kako bi se obradili neki podatci i sastoji se od nekoliko komponenti:

1. Kućište kompjutera poznato i kao centralna procesna jedinica– sadrži RAM memoriju, hard diskove, procesor, CD/DVD ROM i priključke za druge uređaje,
2. periferni uređaji kao što su monitor, tastatura, miš, printer, skener, eksterni hard diskovi, slotovi za memorijske kartice, USB wireless kartice itd.

Kompjuterski sistemi mogu biti u različitim izvedbama kao što su stolni, toranj-uspravni, integrisani zajedno sa monitorom, laptopi, rack-mounted (ormarski), kao na sljedećim slikama:

Slika 1. Pojavni oblici računara

Tablet uređaji

Tablet kompjuter je uređaj kojim se upravlja dodirivanjem displeja, a ne pomoću tastature ili miša. Obično veći od mobilnih telefona ili PDA uređaja. Dolaze u mnogim oblicima i veličinama i obično imaju mogućnost memorisanja u obliku tvrdih-hard diskova ili flash memorije. Postali su vrlo popularni u posljednjih nekoliko godina i mogu biti korisni izvori digitalnih dokaza kao što su razni dokumenti i pristup internet servisima, spajanjem na Internet putem bežične lokalne mreže (WLAN) ili treće generacije mobilnih telekomunikacija (3G).

Slika 2. Primjeri tablet uređaja

Uređaji za skladištenje podataka

Uređaji za pohranu podataka dolaze u mnogim oblicima i veličinama i na različite načine mogu pohraniti i čuvati podatke. Važno je biti svjestan dokaznog potencijala ovih uređaja njihova postojanja i njihove sposobnosti čuvanja ogromne količine podataka. Sljedeća poglavlja sadrže informacije o pojedinostima nekih od tih uređaja.

Hard diskovi i Solid state diskovi SSD

Hard diskovi su glavni uređaji za čuvanje podataka u kompjuterskim sistemima. Sastoje se od elektronike i diskova koji mogu biti od keramike, metala ili stakla na kojima se snimaju podatci. Nije neobično da se na licu mjesta pronađu hard diskovi koji nisu priključeni ili ugrađeni u kompjuterski sistem. SSD diskovi postaju sve više popularni jer pohranjuju podatke na drugačiji način od tvrdih diskova, dok omogučuju priključke i pristup podacima na isti način kao tradicionalni hard diskovi. Dok hard diskovi pohranu podataka vrše na magnetne ploče, a SSD diskovi pohranu podataka vrše pomoću mikročipova koje nemaju pokretnih dijelova. Kao takvi garantuju manju vjerovatnoću kvara zbog udara i nude brži pristup podacima. Ovi uređaji mogu posjedovati veoma vrijedne dokaze.

Slika 3. Primjeri internih hard diskova

Treba naglasiti da pored diskova koji se ugrađuju u kompjuterske sisteme postoje i verzije eksternih diskova sa kućištem a koji se priljučuju najčešće putem USB kabla. Također sve popularniji su diskovi kojima se pristupa putem bežične veze -Wireless. Veoma su pogodni da se koriste kao skrivena skladišta podataka npr. skrivaju se na tavan ili slična skrivena mjesta obzirom da ne trebaju fizičku vezu i obično sadrže podatke koji mogu biti veoma bitni u dokaznom postupku.

Slika 4. Primjeri bežičnih eksternih hard diskova

Optički mediji

Mediji kao Compact Disk (CD), digitalni video disk (DVD) i Blu-ray diskovi (BD), obično se koriste za pohranu velikih video ili audio datoteka, ali i drugih podataka. Na njima se mogu pronaći velike količine podataka koje imaju dokaznu vrijednost.

Treba naglasiti da ove vrste medija postoje u izvedbi koja omogućuje višekratno pisanje i brisanje podataka i nose oznaku CD-RW, DVD-RW. Na takvim medijima mogu se pronaći i podaci koji su predhodno obrisani.

Slika 5. Optički mediji

Memorijske kartice

Memorijske kartice, također poznate kao flash kartice, su uređaji za pohranu digitalnih podataka. Često se koristi u mnogim elektronskim uređajima kao što su digitalne kamere, mobiteli, prijenosni računari , muzički playeri i igraće konzole. Važna karakteristika je da su u stanju zadržati podatke bez napajanja električnom energijom i primjena i kapacitet se konstantno povećava, što znači da može pohraniti ogromne količine podataka, dok su male veličine zbog čega se lako mogu sakriti.

Slika 6. Memorijske kartice

USB uređaji za pohranu podataka

Universal Serial Bus (USB) je standard koji definiše protokole za komunikaciju, povezivanje i napajanje, za uređaje koji će biti povezani s računarima. Od svog izlaska 1990. godine, broj uređaja koji se sada spajaju pomoću ovog protokola je porastao i veliki broj ovakvih uređaja svih vrsta, oblika i veličina sada se koriste za pohranu podataka. Neki primjeri uređaja koji koriste USB protokol nalaze se na sljedećim slikama:

Slika 7. USB uređaji

Pored standardnih oblika USB stikova postoje i u teško prepoznatljivim oblicima zbog čega je potrebno prilikom vršenja pretresa posvetiti posebnu pažnju:

Slika 8. Primjeri specifičnih USB uređaja

Trake za pohranu podataka

Trake za pohranu podataka mnogo češće se sreću u poslovnom okruženju. Koriste se za kreiranje sigurnosnih kopija (Backup) podataka sa servera odnosno sa baza podataka. Najčešći tip koji se koriste trenutno je Linear Tape-Open Tehnologija razvijena 1990-ih kao otvoreni standard. Obzirom da se trake koriste za backup mogu biti korisne u slučajevima kada je potrebna analiza podataka unazad ili ako je izvorni kompjuter – server nedostupan.

Slika 9. Trake za pohranu podataka

Ostali korisnički uređaji koji mogu sadržavati digitalne dokaze

Kontakt lica moraju biti svjesna dokazne vrijednosti i nekih drugih elemenata na mjestu izvršenja krivičnog djela ili u prostorijama koje koriste lica osumnjičena za vršenje istih, a koji su u vezi sa digitalnim informacijama. To su elektronski uređaji i oprema, softver, hardver ili bilo koja druga oprema koja može funkcionisati nezavisno, u konjunkciji sa računarom ili je pridodata nekom računarskom sistemu. Namjena ovih predmeta je olakšavanje pristupa ovlaštenom korisniku ili poboljšanje funkcionalnosti računarskog sistema, samog predmeta ili druge opreme.

Između ostalog tu spadaju:

- Oprema za video nadzor,
- Digitalni foto aparati i video kamere – sadrže memorijske module,
- Digitalni audio snimači (diktafoni) – sadrže memorijske module,
- Digitalni video rekorderi (DVR) – mogu da sadrže memorijske module,
- MP3 i MP4 plejeri – sadrže memorijske module,
- Satelitski digitalni prijemnici i pristupne kartice,
- Konzole video igrica – mogu da sadrže memorijske module,
- Uređaji za čitanje i kloniranje SIM kartica,

- KVM razdjelnici – uređaji koji omogućavaju kontrolu više računara sa jednog monitora (***eng. Keyboard Video Mouse – KVM Switch***),
- GPS prijemnici – sadrže memorijske module,
- Čitači otisaka prstiju,
- Čitači bar kodova,
- ***Bluetooth*** uređaji,
- Uređaji za replikaciju portova – adapteri,
- Razni referentni materijali – knjige koje se tiču uputstava za korištenje raznih softvera i uređaja.

Na sljedećim stranama su prikazane slike nekih od primjera navedenih uređaja uređaja, a u daljem tekstu opis najčešće korištenih uređaja.

Slika 10: Digitalni foto aparati (lijevo) i digitalne video kamere (desno).

Slika 11: Digitalni audio snimači – diktafoni.

Slika 12: Digitalni video snimači (eng. DVR).

Slika 13: Različiti primjeri MP3 i MP4 plejera.

Slika 14: Izgled digitalnog satelitskog prijemnika sa pristupnim karticama.

Slika 15: KVM razdjelnici.

Slika 16: Uređaji za čitanje i kloniranje SIM kartica.

Slika 17: Uređaji za čitanje otisaka prstiju.

Slika 18: Uređaj za čitanje bar kodova.

Slika 19: Uređaji za replikaciju portova.

Potencijalni dokazi: Uređaj ili neki drugi predmet, namjera za njegovo korištenje, njegove funkcije i mogućnosti, kao i bilo koje druge informacije u vezi njih mogu sadržati potencijalne dokaze. Posebnu pažnju treba posvetiti onim uređajima koji sadrže ili mogu sadržati memorijske module koji mogu poslužiti za prikrivanje digitalnih dokaza.

Računarske mreže

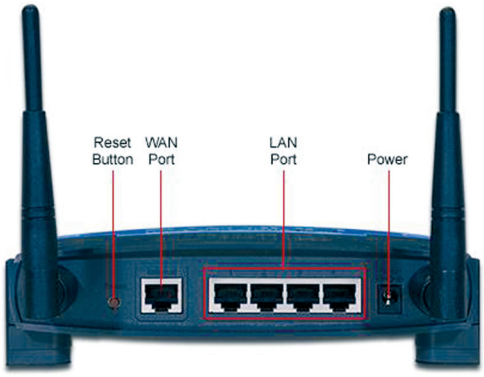
Računarske mreže se sastoje od dva ili više računara povezanih kablovskom ili bežičnom vezom i koji dijele ili su u mogućnosti da dijele razne resurse. Često uključuju štampače i druge periferne uređaje, kao i uređaje za rutiranje podataka kao što je hab ***(eng. Hub)***, razdjelnik ***(eng. Switch)*** ili ruter. Pored navedenih treba obratiti posebnu pažnju i na neke druge komponente i uređaje koji mogu pomoći identifikaciji računarskih mreža ili mogu sadržati digitalne dokaze. To su razne mrežne karte, internet modemi, bežične pristupne tačke (***eng. Wireless Access Point***), usmjerene antene za vezu sa bežičnim jezgrom i sl. Na slikama ispod su prikazani neki od mrežnih uređaja i komponenti.

Hab (slika 20)**,** mrežni razdjelnik (slika 21) i ruter (slika 22) su uređaji čija je uloga omogućavanje uspostavljanja komunikacione mreže između računara, raznih periferala, kamera za video nad-

zor sa jezgrom i slično. Često su na prvi pogled vrlo slični, a razlikuju se po načinu regulisanja saobraćaja u mreži. Mogu biti u kablovskoj izvedbi, kada su sve komponente mreže međusobno povezane mrežnim (UTP/FTP) kablom preko tih uređaja, ili mogu biti u bežičnoj izvedbi. Tada svi uređaji u mreži moraju imati karte za bežični pristup, integrisane ili eksterne. Zajednički naziv za ove uređaje jeste mrežne pristupne tačke ***(eng. Network Access Point)***.

Slika 20: Mrežni hab (eng. Hub).

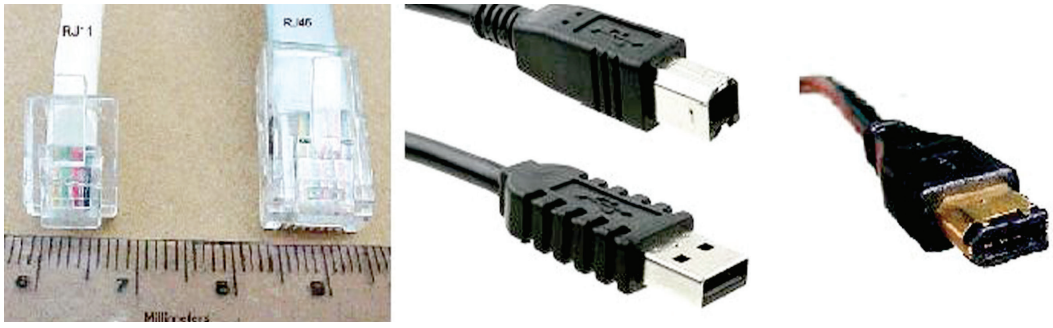
Slika 21: Mrežni razdjelnik sa napajanjem (eng. Switch).



Slika 22: Bežični mrežni ruter (pogled sa leđa).

Uređaji u kablovskoj mreži su povezani pomoću mrežnog (UTP/FTP) kabla na čijim se krajevima nalazi RJ – 45 konektor. Postoje i kablovske izvedbe mreže ili nekih njenih dijelova gdje

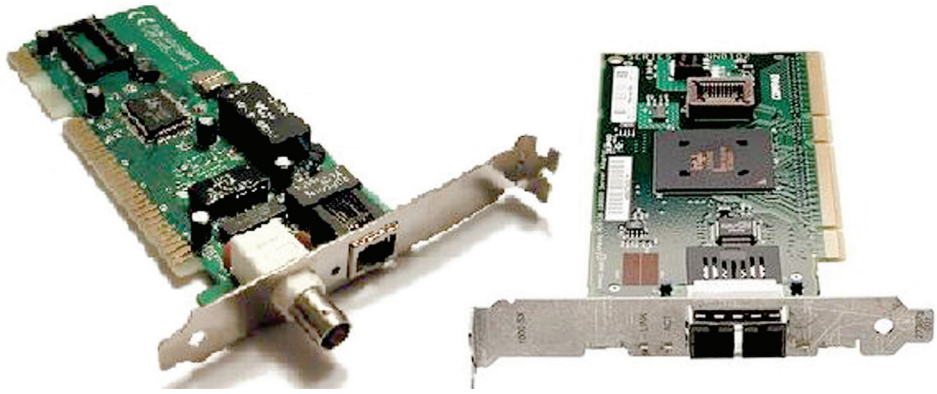
su pojedini uređaji na mrežu povezani pomoću FireWire ili USB konektora, ali je to rijeđe slučaj. RJ – 11 konektor se koristi za telefonske četvorožilne kablove i pomoću njega se isto tako neki uređaji mogu spojiti na mrežu.



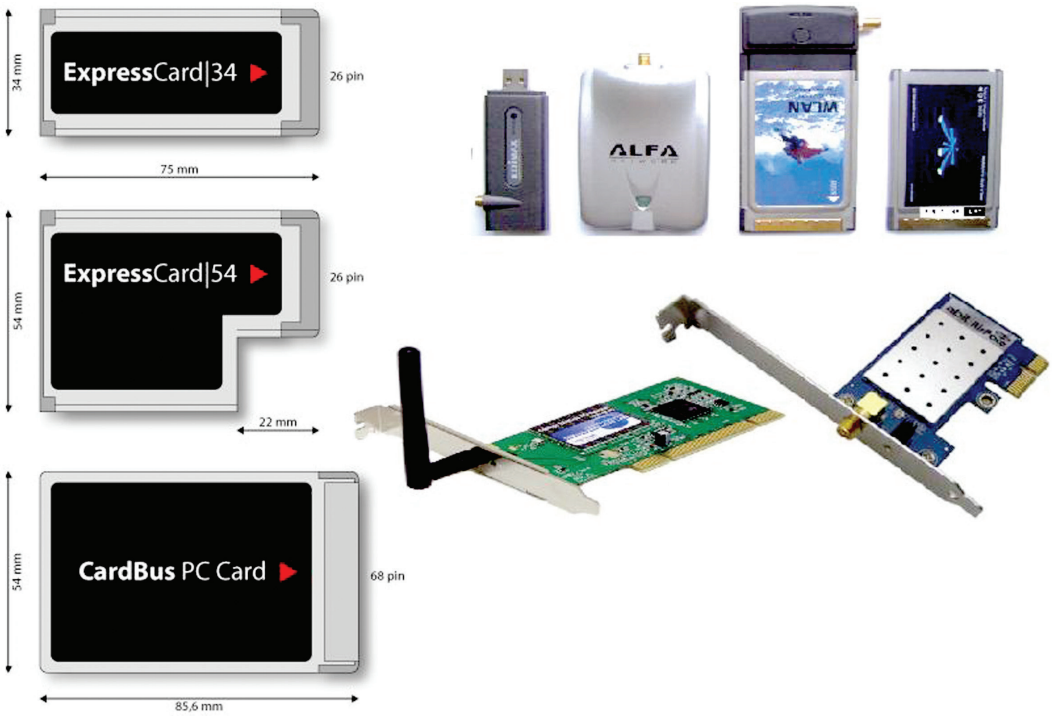
a) **b)** **c)**

Slika 23: Izgled konektora RJ – 11 i RJ – 45 (a), USB (b) i FireWire (c) konektora.

Hardverski dio pomoću kojeg računari i drugi uređaji komuniciraju sa mrežom zove se mrežna karta (slika 24). On predstavlja fizički sloj komunikacije i jednoznačno je određen MAC adresom (***eng. Medium Access Control***). Mogu biti predviđene za kablovsku ili bežičnu komunikaciju. Ako su predviđene za kablovsku vezu, na njima su vidljivi odgovarajući slotovi za gore navedene konektore (slika 23), a ako su predviđene za bežičnu vezu tada imaju vidljivu antenu, slot za antenu ili se USB konekcijom povezuju na računar (slika 25).



Slika 24: Izgled klasičnih mrežnih karti.



Slika 25: Primjeri bežičnih mrežnih karti.

Slika 26: Mobilne mrežne karte koje se na rčunar povezuju pomoću USB, FireWire ili PCMCIA konektora.

Posljednjih godina trend u svijetu je mobilnost uređaja zbog jako snižene cijene u odnosu na prethodne godine. Bez obzira što je većina računara opremljena nekom od mrežnih karti sve je češća pojava da tehnički obučenija kriminogena lica, koja nezakonite radnje čine putem interneta ili se njime služe u planiranju istih, na sve načine pokušavaju da zavaraju trag svojih aktivnosti na internetu. U tu svrhu se sve više koriste mrežne karte sa USB konekcijom pomoću koje se lako priključe na bilo koji računar, preko nje ostvare konekciju na mrežu i na taj način u potpisu ostavljaju MAC adresu različitu od one koju ima mrežna karta ugrađena na računar (slika 30). MAC adresu posjeduju i svi ostali uređaji koji se priključuju na mrežu, a koji korisnicima mreže pružaju određene usluge. Ti uređaji su modemi, mrežni preklopnici, ruteri, štampači, IP video kamere i sl.

Uređaji preko kojih mreža ili računar zasebno ostvaruje vezu sa internetom naziva se modem. U zavisnosti od načina ostvarivanja veze može biti kablovski ili bežični. Ukoliko vezu ostvaruje bežičnim putem tada za ostvarivanje veze koristi signal mobilne telefonije i u svom sklopu ima i slot za umetanje SIM kartice, mada to nije nužno jer kartica može biti i fabrički ugrađena. Tada ima oblik kao USB memorijski stik (slika 28).

Slika 27: Primjer modema.

Dodatna oprema koja može skrenuti pažnju na postojanje bežične internet konekcije može biti i postojanje helikoidne usmjerene antene od bežične mrežne karte (slika 29). Ona je najčešće smještena tako da je na vidljivom mjestu i da ima optičku vidljivost sa antenom nekog od internet provajdera. Takva mjesta su najčešće balkoni ili krovovi kuća.

Slika 28: Modem za vezu preko mobilne telefonije putem SIM kartice.

Slika 29: Usmjerena antena bežične mrežne karte.

Kada je riječ o poslovnom okruženju, lokalne mreže su najčešće ostvarene preko centralnog računara koji se naziva server. Na njemu se tada smještaju svi važniji podaci i korisničke aplikacije i kao takav od posebnog je značaja u procesu istražnih radnji. To su specijalizovani računari koji se na mrežu najčešće spajaju kablovski ali postoje i bežične varijante. Fizičkim izgledom mogu podsjećati na klasične desktop računare, ali i mogu biti specifičnog izgleda, samostalni (slika 30) ili vezani u grupu (***eng. cluster***). Tada su smješteni u specijalne ormare (slika 31).

Slika 30: Fizički izgled servera.

Slika 31: Grupa servera smještenih u specijalne ormare.

Potencijalni dokazi: Umreženi računari i uređaji mogu predstavljati dokaze korisne u samoj istrazi ili sudskom procesu. Podaci koje sadrže takođe mogu biti značajni dokazi i obuhvataju različit softver, dokumenta, slike, elektronsku poštu sa prilozima, baze podataka, finansijske podatke, istoriju internet pretraživanja, razne log fajlove, liste kontakta, i sl. Funkcije uređaja, njihove mogućnosti kao i bilo koje druge informacije važne za identifikaciju računara uključujući internet protokol (IP) adrese pohranjene na njima, te njihove fizičke adrese (***eng. Medium Access Control - MAC***) predstavljaju korisne dokaze.

PRETRES DOKAZA U DIGITALNOM OBLIKU

Prilikom planiranja i realizacije pretresa digitalnih dokaza potrebno je ispoštovati opšte principe, a to su:

1. Planiranje i priprema pretresa digitalnih dokaza (naredbe koje će pokriti sve mrežne lokacije, informacije o lokacijama, šta se očekuje u pretresu, vrsta KD itd.),
2. Prepoznavanje lica mjesta podrazumjeva identifikaciju predmeta koji sadrže digitalne dokaze, da li postoji računarska mreža i gdje se prostire odnosno koji su uređaji u mreži i obezbjeđenje takvih predmeta,
3. Prikupljanje digitalnih dokaza (dump memorije, e-mail, logovi i drugi podaci koje je potrebno prikupiti na licu mjesta),

4. Izuzimanje predmeta koji sadrže informacije o korištenju i pristupu digitalnim dokazima (e-mail adrese, lozinke, zabilješke, upustva o programima i sl.),
5. Izuzimanje predmeta koji sadrže digitalne dokaze (HDD, računari, CD/DVD, MMC, mobiteli, USB itd.),
6. Obilježavanje i pakovanje,
7. Obezbjeđenje i transport.

Sve urađeno tokom obezbjeđivanja, prikupljanja, transporta i čuvanja digitalnih dokaza mora biti u potpunosti dokumentovano, sačuvano i dostupno naknadnoj reviziji.

S obzirom na činjenicu da su digitalni dokazi veoma osjetljivi i lako podložni kontaminaciji, kontakt lica ne bi trebala istraživati niti analizirati iste osim ako nemaju odgovarajuću obuku.

Planiranje pretresa digitalnih dokaza

U zavisnosti od vrste krivičnog djela i procjene osumnjičenih o stručnosti osumnjičenih iz informacionih tehnologija, u mnogome će zavisiti planiranje i pripreme za izvršenje pretresa. Za planiranje i pripremu pretresa, uz konsultacije sa stručnim osobama, potrebno je izvršiti sljedeće radnje i prikupiti informacije:

1. **Informacije prikupljene u toku istrage**, na osnovu kojih bi se mogla izvršiti procjena u kojem obliku bi se mogli pronaći digitalni dokazi i koja vrsta. Ove informacije će odrediti daljnji tok pretresa odnosno koji će se predmeti oduzeti, koje vrste digitalnih dokaza će se izuzimati na licu mjesta ukoliko se predmeti ne mogu izuzeti. Npr.izuzimanje servera koji predstavlja osnov poslovanja firme, čime bi se napravila ogromna šteta u poslovanju, umjesto izuzimanja servera izuzeli bi se samo podaci koji bi se koristili za dalju istragu i dokazni postupak.
2. **Informacije o osumnjičenim.** Navedene informacije su bitne zbog planiranja izvršenja pretresa. Ukoliko se radi o licima koja imaju veliko znanje iz informacionih tehnologija često imaju i pripremljene zaštite kojima veoma lako uništavaju ili učine nedostupnim digitalne dokaze. Zbog navedenog potrebno je izvršiti procjenu da li će pretres početi bez uručenja naredbe i da li će se lice na prevaru udaljiti od digitalnih dokaza kako bi se spriječilo uništenje istih.
3. **Informacije o lokacijama.** Navedene informacije poslužit će za procjenu radnji koje je potrebno izvršiti, lokacija koje treba obuhvatiti naredbom za pretres, da li su lokacije povezane računarskom mrežom, koliko računara se očekuje, da li se radi o firmi, kući ili javnoj lokaciji.

4. **Procjena ljudskih kapaciteta i potrebne opreme.** Na osnovu informacija iz tačke 1., 2. i 3.izvršit će se procjena kapaciteta i rasporeda službenika, kao i opreme potrebne za realizaciju pretresa.
5. **Naredba za pretres pokretnih stvari.** U zavisnosti od okolnosti naredba može biti zasebna ili u sastavu naredbe za pretres prostorija i/ili lica. Ukoliko postoji opasnost od uništenja digitalnih dokaza potrebno je da naredba sadrži odobrenje za početak pretresa bez predhodnog uručenja.

Prepoznavanje lica mjesta incidenta

Prepoznavanje lica mjesta podrazumjeva neposredan početak pretresa. U ovoj fazi bitno je prvenstveno ***„stavljanje pod kontrolu lica zatečenih u prostorijama".*** Ovo podrazumjeva da se hitno pregledaju sve prostorije i zatečena lica udalje od elektronske opreme. Provedba i hitnost navedene radnje je bitna posebno u slučajevima kada osumnjičeni posjeduje visoko znanje iz informacionih tehnologija. Dovoljan je samo jedan klik na tastaturu pa da se pokrene trajno brisanje diska (wipe) ili da se pokrene enkripcija diska koju je naknadno teško ili nemoguće „razbiti". Lica koja koriste računarsku tehniku za izvršenje krivičnih djela često imaju pripremljene „zaštite" koje se u iznenadnim slučajevima mogu veoma lako pokrenuti nakon čega vjerovatno dolazi do trajnog gubitka digitalnih dokaza.

Ukoliko se u toku pregleda prostorija primjeti da je na nekom od računara eventualno pokrenuta procedura brisanja podataka ***(Deleting, Wipe ili Wiping)***, takve uređaje potrebno je hitno isključiti iz napajanja električnom energijom (izvaditi kabl iz utičnice).

Nakon obezbjeđenja uređaja, vizuelno je potrebno ustanoviti da li postoji računarska mreža tj.da li je jedan ili više računara povezano mrežnim kablovima i ustanoviti gdje se završavaju kablovi. Razlog je što u nekim slučajevima postoje kompjuteri koji se nalaze na skrivenim mjestima i služe samo za skladištenje podataka. Ovo se takođe odnosi na eksterne hard diskove koji mogu imati mrežni priključak.

Pored vizuelnog pregleda, ukoliko se zatekne upaljen neki od računara a takođe i ako se ustanovi da postoji bežična (Wireless) mreža, jedan od načina sa se provjeri da li postoje i drugi aktivni uređaji u mreži je i korištenje besplatnog programa u „Nirisoft" paketu programa pod nazivom "Wireless Network Watcher" ili ručnom pretragom kroz operativni sistem računara. U zavisnosti od operativnog sistema računara na sljedeći način moguće je provjeriti koji su uređaji aktivni na mreži:

1. za Windows to je „My network place",
2. za Mac (Apple) sisteme otvoriti Finder i kliknuti ikonicu Network,

3. za Linux sisteme otvoriti „File manager izabrati Places->Network Servers".

Uređaje pronađeni prilikom pretresa osoba skloniti na bezbjedno mjesto van dohvata osumnjičenih osoba do procedure izuzimanja predmeta.

Prikupljanje digitalnih dokaza

Digitalni mediji dijele se u dvije kategorije. Prva kategorija su nepostojani mediji, kojima treba stalni dotok elektriciteta da bi zadržali pohranjene informacije i druga kategorija su postojani mediji koji zadržavaju informacije i nakon gubitka napajanja električnom energijom **Ukoliko nema električne energije u uređaju iz nekog izvora ili baterije, informacije će biti izgubljene.** Jedan primjer nepostojanog medija je radna memorija kompjutera (RAM). Podaci se gube ako nema stalnog dotoka energije (kada se uređaj isključi iz zida ili kada se baterija istroši).

U današnje vrijeme, izvršioci krivičnih djela, sve više koriste kriptografsku zaštitu kako bi onemogučili pristup svojim podacima. Danas se na internetu nudi veliki broj besplatnih alata za enkripciju cjelokupnih medija ili pojedinačnih podataka. Enkripcije su na tako visokom nivou da je često veoma teško razbiti šifru pa čak i nemoguće obzirom da je za dekripciju u prihvatljivom vremenu potrebno obezbjediti ogromne informatičke resurse.

Istrage o provalama u mreže su među tehnički najkomplikovanijim cyber istragama iz više razloga. Prvo, počinioci ove vrste krivičnog djela su često tehnički napredni i znaju niz metoda za sakrivanje svojih aktivnosti. Ove upade sve više vrše organizovane kriminalne grupe radi finansijske dobiti kao i države radi sticanja obavještajnih podatka i tehničkih inovacija. Drugi razlog je distribuirana priroda dokaza kod ove vrste napada, kada se napadne mreža i dokazi se nalaze širom mreže na različitim lokacijama pa i kontinentima. Većina alata koji se koriste za ovakvu vrstu napada pokreću se i nalaze se isključivo u RAM memoriji.

Uzimajući u obzir naprijed navedeno i u zavisnosti od krivičnog djela i procjene službenog lica koje vodi istragu, potrebno je poduzeti sljedeće korake prije gašenja i izuzimanja računara:

- FTK Imager Lite i Win32DD - široko rasprostranjeni programi za kreiranje forenzičke slike radne memorije na aktivnom računaru. Navedeni programski alat pohranjuje cijeli sadržaj RAM-a u binarnu presliku datoteka, a koja se može analizirati korištenjem instrumenata kao što su „EnCase" ili „FTK".
- IRTools i Microsoft Cofee su programske platforme koje sadrže skup otvorenih programskih alata koje su razvili Microsoft i Sysinternals. Navedne grupe programa koriste se za prikupljanje informacija sa mreže i drugih sistema nepostojanih podataka, po-

dataka o operativnom sistemu, kreira sliku onoga što se trenutno nalazi na ekranu itd. Treba naglasiti da ove platforme dozvoljavaju i dodavanje novih programskih alata u zavisnosti od potreba.

- CryptHunter je instrument koji koristi policija da bi otkrila aktivnu upotrebu kriptografske zaštite. On će otkriti montirane kriptografski zaštićene diskove, ali i nemontirane kriptografski zaštićene diskove. Ukoliko je otkrivena kriptografska zaštita pokušati dobiti šifru od osumnjičenog. Ukoliko osumnjičeni ne želi dati šifru, treba ga upozoriti da zakonom o krivičnom postupku može biti kažnjen novčanom kaznom do 50.000 KM ili kaznom zatvora do 90 dana.
- FTK Imager Lite - program pomoću kojeg se može napraviti forenzičku slika sadržaja aktivog diska, svezaka, datoteka ili foldera. Ukoliko je na hard disku otkrivena kriptografska zaštita i ne možemo otkriti šifru onda je preporučljivo uraditi logičku forenzičku sliku (Logical image) kako bi smo obezbjedili bar jedan nivo podataka za naknadnu analizu.

Svaki od navedenih programa može se pokrenuti sa eksternog USB hard diska. USB hard diskovi su poželjniji od USB flash diskova, zbog povećanja prostora za pohranjivanje podataka i veće brzine pisanja.

U dosadašnjoj praksi, ukoliko se zatekne otvoreno elektronsko poštansko sanduće (E-mail), bilo je nedoumica da li se mogu izuzeti poruke koje se nalaze u sandučetu. Obzirom da se poruke nalaze uglavnom na serverima u drugim državama, da je za osumnjičene ili njihove saradnike veoma lako trajno obrisati poruke ili da na drugi način postanu nedostupne, smatralo se da u skladu sa naredbom za pretres kompjutera može se izuzeti sadržaj sandučeta na način da se poruke isprintaju i takođe snime na optički medij u elektronskoj formi.

Ukoliko se vrši pretres u firmama čiji je rad uglavnom vezan za informacioni sistem i gdje bi izuzimanje informatičke opreme uzrokovalo prekid u radu, ukoliko tehničke i druge okolnosti dozvoljavaju moguće je izuzeti samo dio podataka koji će se naknadno koristiti u istrazi.

Izuzimanje predmeta koji sadrže informacije o digitalnim dokazima

Sakupljanje dokaza na licu mjesta ne treba biti ograničeno samo na digitalne dokaze. Osim digitalnih medija, postoje i mnoge druge stvari koje su vrijedne za istragu. Osumnjičeni često bilježe lozinke, IP adrese, korisnička imena, imena datoteka, e-mail adrese sa lozinkom i druge informacije koje mogu biti od vrijednosti za neku istragu. Ovo osobito važi za hakere ili osumnjičene koji pohranjuju datoteke na udaljene kompjutere. Zabilješke nađene na licu mjesta su često jedini znak postojanja drugih izvora digitalnih dokaza. Pošto su hakeri i kriminalci takođe ljudi i njima je često teško da zapamte više lozinki, IP adresa i slične vr-

ste informacija. Kao i kod drugih ljudi, pamćenje osumnjičenih je ograničeno i oni često zapišu ove ključne informacije u lako dostupna mjesta blizu svog radnog prostora. Zbog navedenog veoma je bitno detaljno pregledati neposredno okruženje računara i izuzeti sve ceduljice, rokovnike i slično, gdje bi se mogle nalaziti bitne informacije za naknadnu forenzičku analizu. Naprimjer, može se pronaći korisnički nalog i šifra za elektronsko poštansko sanduće, sa kojima se može nanadno uz naredbu suda za izuzimanjem poštanskih pošiljki izuzeti sadržaj odnosno poruke.

Za tumačenje mnogih vrsta digitalnih dokaza u naknadnoj analizi, može biti korisno pronaći uputstva za upotrebu, softver za instalacije ili druge informacije o softverskim programima koji se nalaze na izuzetim računarima. Nalozi za pretres treba da sadrže dozvolu za legalno sakupljanje ove imovine da bi se osiguralo da kasnija forenzička analiza ima što više informacija potrebnih za tumačenje podataka pronađenih na analiziranom kompjuteru. Uz to, priručnici za upotrebu i softver diskovi mogu ukazati na to gdje se na kompjuteru nalaze informacije interesantne za istragu.

Ne-elektronski dokazi, **ne zaboravite zaplijeniti:**

- Zabilješke i druge štampane materijale,
- Adresare i dnevnike,
- Video i audio kasete,
- Fotografije i dijagrame,
- **Ukoliko se radi o javnom mjestu kao što je internet klub ili slično a potrebno je dokazati da je osumnjičeni koristio određeni računar, bitno je obezbjediti tastaturu i miš kako bi se naknadno moglo izvršiti vještačenje otisaka prstiju**.

Izuzimanje predmeta koji sadrže digitalne dokaze

U predmete koji sadrže digitalne dokaze spadaju svi elektronski uređaji koji posjeduju trajnu ili privremenu memoriju i koji su bili sredstvo izvršenja krivičnog djela. To su uređaji koji su obrađeni u predhodnom poglavlju kao što su računari, mobilni telefoni, USB stikovi, memorijske kartice i drugi uređaji koji posjeduju memoriju.

Prilikom oduzimanja računara, u zavisnosti od prirode krivičnog djela odnosno da li je računar korišten kao sredstvo izvršenja krivičnog djela ili samo sadrži potencijalne dokaze, zavisi i koji predmeti će se izuzeti. Ukoliko je korišten kao sredstvo izvršenja krivičnog djela za koju će sud donjeti odluku o oduzimanju, posmatrajući računar u cjelini izuzet će se centralna procesna jedinica, monitor, tastatura, miš, ali i ostala periferna i mrežna oprema u zavisnosti

da li se radi o krivičnim djelima povrede autorskih prava, kompjuterskog kriminala, falsifikovanja i dr.

Prikupite informacije koje mogu biti od koristi za kasniju analizu:

- Dužina vlasništva,
- Operativni sistem,
- Primarna upotreba,
- Ko su korisnici računara,
- Računi elektronske pošte, korisnička imena i lozinke,
- Antiforenzičke mjere,
- Kriptografska zaštita,
- Datoteke od interesa za istragu,
- Davaoci Internet usluga (provajderi),
- Skladište podataka na nekom drugom lokalitetu,
- Skriveni uređaji za pohranjivanje podataka.

Prilikom izuzimanja računara, zavisno da li je uključen ili isključen, potrebno je slijediti sljedeće korake:

Ako je kompjuter uključen:

- Fotografišite ekran,
- Kreirajte forenzičku kopiju RAM memorije,
- Provjerite aktivne pograme i šta se trenutno dešava,
- Izuzmite sadržaj elektronskog poštanskog sandučeta,
- Provjerite da li ima CD/DVD medija u uređaju,
- Prekinuti vezu s mrežom,
- Ako postoji kriptografska zaštita, kreirati logičke forenzičke kopije diskova,
- Izvucite kabl,
- Zaplijenite i upakujte sve dokaze.

Ako je kompjuter isključen:

- Nemojte ga uključivati,
- Fotografišite ga,
- Dokumentujte da li je povezan na mrežu,
- Isključite i označite kablove,
- Provjerite dali ima CD/DVD medija u uređaju, ako ima izvadite koristeći spajalicu (provjerite da je struja isključena).

Slika 32.

Obzirom da bi svako paljenje računara dovelo do izmjene određenih podataka, čime bi se mogla dovesti u pitanje validnost pronađenih dokaza, kako bi se onemogućilo slučajno ili namjerno paljenje, preporučljivo je koristiti odgovarajuće etikete za utičnice i kablove, kao na slici.

Slika 33.

Prilikom izuzimanja mobilnih telefona, potrebno je slijediti korake:

1. **Za mobilne telefone koji su aktivni sa SIM karticom**:

- Ukucati ***#06#,** broj koji se pojavi na displeju je IMEI broj i unijeti u zapisnik,
- Unijeti u zapisnik na kojoj mreži telekom operatera je aktivan telefon i unijeti u zapisnik,
- Telefon ugasiti a zatim upaliti,
- Ukoliko traži **PIN** kôd, tražiti od lica i kod unijeti u zapisnik,
- Ukoliko traži **SECURITY** kôd, tražiti od lica i kôd unijeti u zapisnik,
- Telefon ugasiti ili ne, zavisi od toga da li je bitno vidjeti ko je zvao u toku ili nakon pretresa obzirom da telekom operateri nisu bilježili propuštene pozive. Međutim treba imati na umu da mobilni telefoni sa operativnim sistemom Android imaju opciju trajnog brisanja podataka koja se aktivira putem interneta. (Ne vaditi bateriju iz razloga što se gubi lista poziva)

Ukoliko lice ne želi dati PIN ili Security kôd, upozoriti ga da Zakonom o krivičnom postupku može biti kažnjen novčanom kaznom do 50.000 KM ili kaznom zatvora do 90 dana.

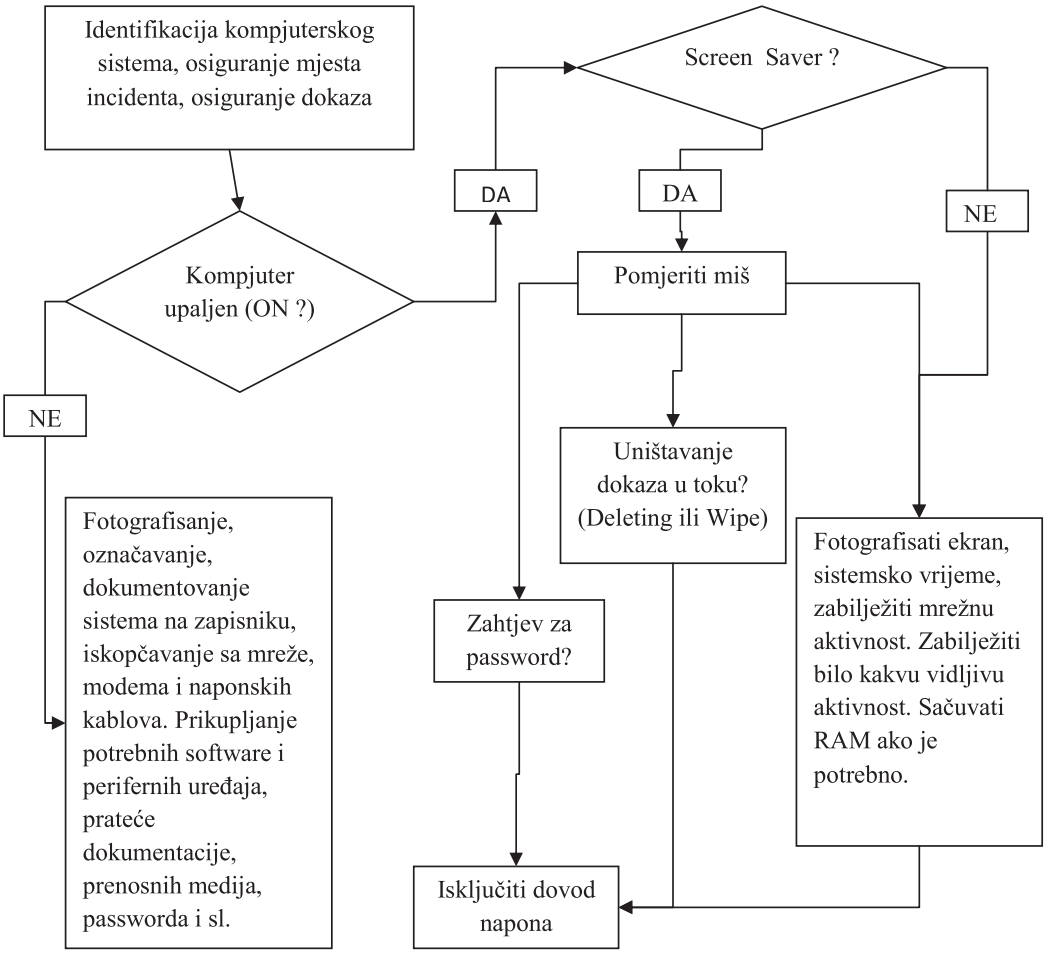
2. **Za mobilne telefone koji nisu aktivni, nemaju SIM karticu**:

- Pokušati upaliti mobilni telefon i ponoviti korake iz tačke 1;
- Ukoliko se telefon ne može upaliti ili nema SIM kartice, izvaditi bateriju i unijeti u zapisnik IMEI broj,

Mobilne telefone, SIM kartice, memorijske kartice, punjače za mobitel i certifikate za SIM kartice, pakovati odvojeno od ostalih predmeta koji se oduzimaju a koji neće biti predmet vještačenja digitalnih dokaza.

Obzirom na laku promjenjljivost digitalnog dokaza ali i promjene podataka na medijima koji sadrže digitalni dokaz, preporučljivo je iako to može predstavljati problem prilikom pretresa (tehnički i vremenski), izraditi HASH broj za cjelokupnu memoriju medija ili samo za određeni fajl ili folder.

Hash funkcija je matematički algoritam koji na osnovu podatka koji se nalaze u fajlu, folderu ili cjelokupnoj memoriji medija, proizvede broj koji se naziva hash vrijednost. Ovaj broj je isti svaki put kada se hash funkcija izračunava na identičnom podatku i predstavlja „otisak prsta digitalnog dokaza". Svaka najmanja promjena na ulaznom podatku hash funkcije za rezultat ima stvaranje potpuno drugačije hash vrijednosti. U kompjuterskoj forenzici hash funkcije potvrđuju tačnost forenzičke slike čime se obezbjeđuje vjerodostojnost dokaza od trenutka izračunavanja HASH broja. MD5 i SHA su dva najčešća hash algoritma koji se koriste u računarskoj forenzici.



Šematski prikaz procesa identifikacije i prikupljanja računara
kao dokaza u digitalnom obliku:

Obilježavanje i pakovanje

Ono što je potrebno naglasiti, prilikom pakovanja predmeta koji sadrže digitalne dokaze kao i koji sadrže informacije o digitalnim dokazima, da se obavezno pakuju odvojeno od drugog dokaznog materijala, kako iz sigurnosnih tako i praktičnih razloga. Prilikom obilježavanja predmeta potrebno je upisati lice od kojeg se izuzima, lokaciju, sprat, po mogućnosti namjenu računara, broj naredbe suda, datum i vrijeme. Tokom pakovanja za transport predmeta koji sadrže digitalne dokaze, trebalo bi poštovati slijedeće procedure:

- Sve prikupljene digitalne dokaze potrebno je pravilno dokumentovati, etiketirati, označiti, fotografisati, te napraviti video zapis ili skicu i popisati ih odnosno napraviti listu, pravilno etiketiranje veza i povezanih uređaja olakšava povezivanje sistema kasnije;
- Treba zaštititi bilo kakve potencijalne tragove ili biološke dokaze koji se nalaze na digitalnim dokazima; digitalne dokaze je potrebno fotografisati prije obrade;
- Sve digitalne dokaze treba pakovati u antistatičkoj ambalaži; plastične kese mogu proizvesti statički elektricitet i omogućiti razvoj vlage i kondenzacije, što može oštetiti ili uništiti digitalne dokaze;
- Digitalne dokaze pakovati na način koji će ih zaštititi od savijanja, grebanja i slično, a pri tom svaku ambalažu označiti na odgovarajući način;
- Telefone ostaviti u stanju u kojem su pronađeni; telefoni se pakuju u ambalažu koja štiti od prijema signala, da bi se spriječila komunikacija;
- Potrebno je sakupiti sva napajanja i adaptere za sve elektronske uređaje koji su oduzeti.

Tokom transporta predmeta koji sadrže digitalne dokaze, trebalo bi da se poštuju sljedeće transportne procedure:

- Digitalne dokaze je potrebno držati dalje od magnetnih polja (npr. od onih koje proizvode radio-predajnici, magneti u zvučnicima ili magneti za montiranje rotacionog svjetla),
- Ostale izvore opasnosti predstavlja uključivanje grijača u sjedištima ili bilo koji uređaj ili materijal koji može proizvesti statički elektricitet, kao što je tepih,
- Držanje digitalnih dokaza u vozilu na duže vreme nije dozvoljeno; toplota, hladnoća i vlaga mogu da oštete ili unište digitalne dokaze,
- Potrebno je uvjeriti se da su računari i elektronski uređaji upakovani i obezbjeđeni tokom prevoza, da bi se spriječila oštećenja od udara i vibracija,
- Bitno je dokumentovati prijevoz digitalnih dokaza, kao i dokumentaciju lanca rukovanja predmetima.

Skladištenje digitalnih dokaza

Soba za pohranjivanje dokaza u digitalnom obliku bi trebala da uključuje kontrolisanu klimu, sa suhim okruženjem, bez mogučnosti pražnjenja statičkog elektriciteta, te blizine uređaja koji emituju magnetna zračenja.

Pristup sobi za dokaze u digitalnom obliku bi trebao biti strogo kontrolisan sa tačnom evidencijom pristupa istoj od strane trećih osoba.

ZAKLJUČAK

Digitalni dokazi su osjetljivi i teško ih je pronaći; koristite obučene istražitelje.

Iako pronalaženje i sakupljanje digitalnih dokaza može biti komplikovano, pravilno obučen forenzički istražitelj posjeduje znanja za obavljanje ovih zadataka. Obučeni forenzički istražitelj zna kako da pravilno zaplijeni, sakupi i obradi digitalne dokaze za sve svoje istrage zahvaljujući obuci, specijalizovanoj opremi i detaljnoj dokumentaciji. Detaljna dokumentacija je izuzetno značajna; ukoliko istražiteljeve radnje nisu detaljno dokumentovane, odbrana može tvrditi da su dokazi uništeni, falsifikovani ili promijenjeni za vrijeme sakupljanja. Dobre bilješke mogu pokazati da procedure korištene za sakupljanje dokaza neće uzrokovati takve promjene. Kod zapljene dokaza sa kompjutera koji je bio uključen kada je pronađen, istražitelj mora preduzeti određene korake prije sakupljanja dokaza (npr. isključiti kompjuter ili sakupiti dokaze iz nepostojane memorije). Ove radnje mogu promijeniti stanje kompjutera ili dokaza a te se promjene moraju objasniti kasnije za vrijeme sudskog procesa. Jasna dokumentacija je osobito važna kada se suđenja održavaju godinama kasnije, nakon što pamćenje istražitelja o događajima više nije potpuno.

RIJEČNIK POJMOVA

Access	Pristup	(1) Mogućnost da se uđe u obezbjeđeno područje. (2) Proces interakcije sa sistemom.
Access Authorization	Dozvola pristupa	Dozvola koja se daje korisnicima, programima ili radnim stanicama.
Access Control	Kontrola pristupa	Niz procedura koje sprovode hardver, softver i administratori kako bi nadzirali pristup, identifikovali korisnike koji traže pristup, registrovali pokušaje ostvarenja pristupa i odobrili ili uskratili pristup.
Alphanumeric Key	Alfanumerički algoritam	Sistem slova, brojeva, simbola i praznih prostora koji sadrži od 1 do 80 znakova.
Anti-static	Antistatički	Onaj koji eliminiše ili smanjuje statički elektricitet.
Application Level Gateway [Firewall]	Maršrutizator Firewalla	Firewall sistem u kojem se usluge pružaju pomoću procesa kojima se održava protokol za kontrolu prenosa podataka. Maršrutizator Firewalla često mijenja adresu upućene poruke tako da se čini da potiče od Firewalla, a ne od internog domaćina (hosta).
Artifacts	Artifakti	Uobičajeni podaci i informacije o vlasniku pohranjene u operativnom sistemu.
Audit	Revizija	Pregled sistema, programiranja i postupka u centru podataka da bi se utvrdila efikasnost kompjuterskih operacija.
Audit Trail	Slijed revizije	Slijed revizije može biti na papiru ili na disku. U sistemima za obezbjeđenje kompjutera, hronološki zapis vremena kada su se korisnici registrovali, aktivnosti koje su obavljali i trajanje različitih aktivnosti i da li je došlo do pokušaja ili izvršenja kršenja bezbjednosti.
Authenticate	Utvrditi vjerodostojnost	Kod umrežavanja, utvrditi vjerodostojnost korisnika ili objekta (tj. komunikacijskog servera).
Authentication	Proces identifikacije korisnika	Proces utvrđivanja legitimnosti sabirnice ili korisnika prije nego što se dozvoli pristup traženim informacijama. Tokom tog procesa korisnik ukucava ime ili broj korisničkog računa (identifikacija) i lozinku (potvrda vjerodostojnosti).

Authentication Tool	Sredstvo za provjeru vjerodostojnosti	Softverski ili hardverski ključ ili token koji se koristi u procesu identifikacije korisnika.
Authentication Token	Token za provjeru identiteta	Prenosivi uređaj koji se koristi u procesu identifikacije korisnika. Token za provjeru identiteta radi na principu pitanje/odgovor, tempirane šifre ili drugim tehnikama. To može obuhvatiti i spiskove jednokratnih šifri na papiru.
Backbone (Network Backbone)	Network Backbone (glavna mreža)	Brza veza ili niz veza koje formiraju glavnu putanju unutar mreže. Naziv je relativnog značenja jer će "kičma" u maloj mreži biti vjerovatno mnogo manja od mnogo veza bez "kičme" u velikoj mreži.
Bagging and Tagging	Pakovanje i obilježavanje dokaza	Proces uzimanja dokaza, uključujući i propisno pakovanje i obilježavanje zaplijenjenih dokaza.
Biometric	Biometrika	Biološka identifikacija osobe. Primjeri su lice, šara zjenice ili mrežnjače, geometrija ruke i glas. Biometrika se ne bavi samo statičnim uzorcima već i akcijom. Dinamika kojom se ispisuje nečiji potpis kao i kucanje na tastaturi mogu biti analizirani.
Biometric Access Control	Kontrola pristupa pomoću biometrike	Svaki način kontrolisanja pristupa pomoću ljudskih mjerila, kao što su otisci prstiju i snimak glasa. Čitači otisaka prstiju su popularni bezbjednosni metod za identifikaciju kod laptop kompjutera.
BIOS	BIOS	Osnovni ulazno/izlazni sistem. Niz osnovnih radnji kojima se uspostavlja hardver u personalni kompjuter i inicira operativni sistem. Prije učitavanja operativnog sistema, BIOS obezbjeđuje osnovne softver drajvere za sve periferne tehnologije koje su dio matične ploče personalnog kompjutera, uključujući tastaturu, miša, monitor i tvrdi disk. Ovi drajveri omogućavaju korisniku podešavanje konfiguracije i dozvoljavaju hardveru pristup tvrdom disku, optičkom disku ili disketi kako bi došao do operativnog sistema. Nakon što je operativni sistem učitan, po pravilu se učitavaju složeniji drajveri koji zamjenjuju rutinu BIOS-a korištenu za inicijaciju sistema. BIOS takođe podržava interne servise kao što su časovnik (vrijeme i datum).
Bitstream image	Kompresovana preslika	Kopija sadržaja tvrdog diska, koja uključuje operativni sistem i instalirane aplikacije.

Bookmark	Obilježivač stranice (bookmark)	Sačuvana lokacija kako bi se kasnije mogla brzo pozvati. Pretraživač weba obezbjeđuje obilježivače stranica (bookmark) koji sadrže adrese (URL) omiljenih sajtova. Većina elektronskih referenci, velike datoteke tekstova i sistemi za pomoć pružaju obilježivače stranica (bookmark) kako bi se označila lokacija koju bi korisnici htjeli da posjete ubuduće.
Boot	Inicijacija sistema	Dovodi do toga da kompjuter počne izvršavati uputstva. Personalni kompjuter i MAC sadrže ugrađene instrukcije u ROM-u ili čipu sa fleš memorijom koje se automatski izvšavaju sa uključivanjem kompjutera. Ove instrukcije tragaju za operativnim sistemom, učitavaju ga i njemu prepuštaju kontrolu. Uključivanje velikog kompjutera može tražiti pritiskivanje više dugmadi i unošenje komandi preko tastature.
Bridge	Most	Uređaj koji međusobno povezuje lokalne mreže sa OSI Slojem veze, filtrirajući i prosljeđujući pakete podataka u skladu sa adresama Kontrole pristupa mediju (MAC).
Browser	Pretraživač weba	Klijent program (softver) koji se koristi da bi se pregledale različite vrste resursa na Internetu.
Budapest Convention	Budimpeštanska konvencija	Alternativno ime za Konvenciju o kibernetičkom kriminalu iz jula 2004.
Burn	Narezati	Narezati optički medij koji se može narezivati samo jednom, kao što su CD-R, DVD-R i BD-R diskovi. Takav disk se smatra narezanim zato što je na njemu nešto snimljeno i ne može se izbrisati ili preko njega snimati. Ovaj izraz se takođe pogrešno koristi za diskove preko kojih se može ponovo snimati, kao što su - CD-RW i DVD-RW, ali ti mediji nisu narezani; oni su snimljeni.
CD-ROM	CD-ROM	Kompakt disk, čitačka memorija. Format kompakt diska koji se koristi za pohranjivanje programa i datoteka. Memorije od 650 MB ili 700 MB, CD-ROM koristi različite formate za snimanje podataka od onih koje koristi CD (CD-DA) iz kojeg se razvio. Audio CD plejer ne može čitati CD-ROM ali CD-ROM drajveri mogu pustiti audio diskove. U personalnom kompjuteru, većina internih CD-ROM uređaja je povezana sa ATA interfejsom na matičnoj ploči, iako su raniji uređaji bili povezani preko SCSI-ja. Uređaji s vanjskim kućištem se povezuju preko USB-ja. U praksi, izraz CD odnosi se na CD formate. Na primjer, izraz "ubacite CD" u stvari znači "ubacite CD-ROM".

Chain of Custody	Evidencija čuvanja dokaza	Pravni izraz koji se odnosi na sposobnost da se garantuje identitet i integritet uzorka (ili podatka) iz zbirke kroz izvještaje o rezultatima testova. To je proces koji se koristi za vođenje i dokumentovanje hronologije čuvanja uzorka (ili podatka). Obrazac za slijed čuvanja dokaza treba da sadrži ime ili inicijale osobe koja je uzela uzorak (ili podatak), svake osobe ili organa koji ga je nakon toga imao u posjedu, datume kada su objekti uzeti ili prebačeni, mjesto prikupljanja, kratak opis predmeta i identifikacioni broj uzorka.
Chat	Ćaskanje (četanje) preko Interneta	Komunikacija između jednog ili više korisnika u realnom vremenu preko tastature na lokalnoj mreži (LAN) ili preko Interneta. Naziva se takođe i ćaskanje uživo, ali je riječ ćaskanje pogrešan naziv jer je riječ o komunikaciji koja nije verbalna, već se odvija putem teksta. Ćaskanje se ostvaruje kucanjem i svaki udarac na tastaturi se prenosi odmah nakon što je tipka pritisnuta ili se šalje cijeli tekst kada korisnik pritisne dugme Enter.
Chat Logs	Dnevnik četanja	Kompjuterske datoteke koje arhiviraju čet razgovor između dvoje ljudi preko kompjutera.
Chat Room	"Čet soba"	Dio websajta ili neka druga usluga na Internetu koja pruža prostor za komunikaciju korisnika sa zajedničkim interesom za komuniciranje u realnom vremenu.
Client/Device	Klijent/uređaj	Hardver koji poziva informacije sa servera.
Cloud Storage	Pohranjivanje podataka online	Online servis za pohranjivanje podataka preko Interneta.
Clustering	Grupisanje u skupine	Grupa nezavisnih sistema koji rade zajedno kao jedan jedini sistem. Tehnologija skupina omogućava grupama servera pristup polju jednog jedinog diska koji sadrži aplikacije i podatke.
Computer Forensic Examination	Forenzičko testiranje kompjutera	Obavlja se u forenzičkim laboratorijama, odjelima za obradu podataka, a u nekim slučajevima, u prostorijama detektivskog odreda. Raspoređivanje osoblja na takve vrste testiranja često se temelji na raspoloživoj ekspertizi, kao i na politici uprave policije. Bez obzira gdje se vrši testiranje, valjano i pouzdano forenzičko testiranje je potrebno. Ovaj zahtjev ne priznaje nikave političke, birokratske, tehnološke ili pravosudne granice.

Content data	Podaci o sadržaju	Suština, svrha ili značenje komunikacije ili drugih podataka.
Convention on Cybercrime	Konvencija o kibernetičkom kriminalu	Ova Konvencija je prvi međunarodni sporazum o krivičnim djelima počinjenim preko Interneta i drugih kompjuterskih mreža, koja se posebno bavi povredom autorskih prava, prevarom uz korištenje kompjutera, dječijom pornografijom i kršenjem bezbjednosti mreža. Takođe sadrži niz ovlaštenja i procedura kao što su pretraživaje kompjuterskih mreža i presretanje razgovora. Njen glavni cilj je sprovođene zajedničke kriminalističke politike usmjerene na zaštitu društva od kibernetskog kriminala, posebno usvajanjem odgovarajućih zakona i jačanjem međunarodne saradnje.
Court Order	Sudski nalog	Nalog koji izdaje nadležni sud koji od neke strane traži da nešto uradi ili da se uzdrži od određene radnje.
CPU	CPU	Centralna procesorska jedinica. Procesorski dio kompjutera. Takođe se naziva procesor, sastoji se iz kontrolne jedinice i aritmetičke logičke jedinice (ALU). Danas se procesori većine kompjutera nalaze u jednom jedinom čipu. CPU i glavna memorija čine kompjuter. Potpun kompjuterski sistem traži dodatne kontrolne jedinice, ulaznu i izlaznu komponentu i uređaje za pohranjivanje podataka, te operativni sistem.
Cryptographic Checksum	Kriptografski kontrolni zbir	Jednosmjerna funkcija koja se primjenjuje na datoteku kako bi se došlo do jedinstvenog otiska datoteke za kasnije reference. Sistem kontrolnog zbira je primarni način za otkrivanje neovlaštenog diranja datotečnog sistema na Unixu.
Data	Podaci	Informacije u bilo kom obliku, na papiru ili u elektronskom obliku. Podaci mogu biti elektronske datoteke, bez obzira na format: baza podataka, tekst, slika, audio i video. Sve što čita i piše kompjuter može se smatrati podacima osim instrukcija u programu koji je aktivan (softver). U svakodnevnoj upotrebi se istovremeno koriste izrazi podaci i informacije. Pored toga, engleska riječ za podatak - data je ustvari množina od riječi datum, a to je takođe podatak. Međutim "data" se na engleskom u praksi koristi i za jedninu - podatak, i za množinu - podaci. Uobičajena je zabluda da je softver takođe podatak. Softver aktivira ili pokreće kompjuter. Podaci se obrađuju. Prema tome, softver omogućava da kompjuter obrađuje podatke.

Data in Motion	Podaci u pokretu	Odnosi se na podatke u stanju transfera s jedne lokacije na drugu, kao što su podaci koji prelaze preko Interneta.
Data Retention	Čuvanje podataka	Pohranjivanje podataka kao rezerva i u istorijske svrhe.
Debian	Debian	Operativni sistem na bazi Linuxa kojeg je napravio Ian Murdock 1993. Funkcioniše na većini glavnih platformi, uključujući i x86, Itanium, PowerPC, SPARC, MIPS i IBM glavni kompjuter, primijećen je na više od 18.000 aplikacija koje prate distribuciju. Verzija 4 Debiana objavljena je u aprilu 2007. Debian je bio inspiracija za nekoliko izvedenih programa.
Decode	Dešifrovati	Pretvoriti šifrovani tekst u obični tekst pomoću šifre.
Decrypt	Dekripcija	Pretvaranje šifrovanog ili kodiranog teksta u obični tekst.
DHCP	DHCP	Dinamični protokol za utvrđivanje konfiguracije kompjutera. DHCP se koristi da automatski utvrdi konfiguraciju mrežnih parametara kompjutera, kao što su IP adrese, DNS serveri, maršrutizator i maska podmreže.
Digital Evidence	Digitalni dokazi	Podaci pohranjeni u binarnom obliku (datoteka, slika, pjesma, dokument, računovodstvena tabela, program, podatak, itd.) koji sadrže informacije koje potkrepljuju ili se odnose na kibernetski zločin o kojem se vodi istraga.
Digital Fingerprint	Digitalni otisak prsta	v. Heš funkcija
Digital Forensics	Digitalna forenzika	Nauka koja se bavi analizom digitalnih objekata kako bi provjerila teorije i/ili odgovorila na pitanja o događajima koji su se desili prilikom reagovanja na incident
Digital Media	Digitalni mediji	Svaki uređaj za pohranjivanje digitalnih podataka. Svi podaci nastali u kompjuteru su digitalni. Sve vrste informacija koje su pohranjene u kompjuteru, uključujući podatke, glas i video.
Digital Storage Device	Uređaj za pohranjivanje digitalnih podataka	Periferni uređaj za pohranjivanje podataka kao što je disk, traka ili fleš memorijska kartica. Tehnologije pohranjivanja obuhvataju magnetske diskove, magnetske trake, optičke diskove i fleš memoriju.

Disk	Disk	Uređaj za pohranjivanje podataka sa direktnim pristupom kao što je disketa, tvrdi disk, magnetski disk, optički disk, kompakt disk CD-ROM i DVD.
Download	Preuzeti	Prebaciti datoteku s mreže. U komunikaciji, presnimiti i učitati podrazumjeva odnos između velikog i malog partnera, u kojem se podaci presnimavaju sa "velikog" servera na korisnikov "mali" kompjuter.
Dual Homed Gateway	Dvomrežni pristupnik	(1) Sistem koji ima dva ili više mrežnih interfejsova, svaki povezan sa različitom mrežom. U konfiguraciji Firewalla, dvomrežni pristupnik obično djeluje tako da blokira ili filtrira dio ili cijeli saobraćaj koji pokušava da prođe između mreža. (2) Primjena Firewalla bez korištenja zaštitnog rutera.
Electronic Evidence	Elektronski dokazi	Digitalni dokazi i uređaji na kojima se pohranjuju digitalni dokazi
Email	Email	Elektronska pošta. Prenos tekstualnih poruka od pošiljaoca do primaoca. Email poruke mogu biti formatizovane i sa grafikom kao što su brošure ili web stranice, poboljšanje koje vole mnogi korisnici ali može kreirati mnogo neželjene pošte i predstavlja bezbjednosni rizik. Korisnici mogu poslati elektronsku poštu jednom ili više primalaca. Pored toga, toj poruci se mogu dodati JPEG fotografije i druge vrste kompjuterskih datoteka. Pošta se šalje na simulirani poštanski sandučić na poštanskom serveru operatera telekomunikacija sve dok se ne presnimi u poštanski sandučić na korisnikovom kompjuteru.
Encrypting Router	Mrežni usmjerivač (rauter) za šifriranje	v. rauter za tuneliranje poruka i krug virtuelne mreže.
Encryption	Kriptografska zaštita	Proces pseudoslučajnog kodiranja datoteka ili programa, promjenom jednog niza znakova u drugi putem alogoritma (kao što je DES alogoritam).
End-to-End Encryption	Enkripcija s kraja na kraj	Enkripcija na izvorištu poruke na mreži, nakon koje slijedi dekripcija na odredištu.
Environment	Okruženje	Skupina vanjskih okolnosti, uslova i događaja koja utiče na razvoj, rad i održavanje sistema.

Ethernet	Eternet	Kablovska tehnologija lokalne mreže (LAN) koja se koristi da poveže kompjutere i druge hardverske uređaje, preko AUI kabla ili koaksijalnog kabla, sa brzinom transfera podataka do 10 Mbps (megabita u sekundi). Specifikacije Eterneta razvio je Istraživački centar Xerox u Palo Altu. Eternet je trenutno mrežna tehnologija u najširoj upotrebi. Brzi Eternet pruža transfer podataka od 100- Mbps (megabita u sekundi).
Evidence Custodian	Čuvar dokaza	Odgovoran za propisno pohranjivanje dokaza i vodi evidenciju o slijedu čuvanja dokaza i drugih evidencija; prima, obilježava, pohranjuje i registruje dokaze, pronađenu imovinu ili imovinu na čuvanju; vodi evidenciju o slijedu čuvanja dokaza sve vrijeme dok je imovina u njegovoj nadležnosti i raspolaže imovinom prema utvrđenim pravilima i propisima Uprave policije; pomaže u pripremi dokaza za sud; može svjedočiti na sudu; fotografiše povrede i osobe u svrhu identifikacije; pribavlja otiske prstiju date prilikom zaposlenja, registracije potrebne prema zakonu ili date u druge svrhe; uništava vatreno oružje, droge i druge predmete u skladu sa državnim i federalnim propisima; vraća imovinu njenim vlasnicima; prebacuje nepotraživanu imovinu za međusektorsku upotrebu ili organizuje njenu prodaju na aukcijama ako je to primjereno; može pomoći tehničaru za dokaze u obavljanju njegovih dužnosti; vodi tačnu evidenciju i priprema izvještaje.
Extranet	Ekstranet	Odnosi se na proširenje LAN-a daljinskim pristupom Internetu ili partnerima van organizacije, kao što su česti snabdjevači i kupci. Ovaj odnos treba proširiti preko vjerodostojne veze do ovlaštenih segmenata LAN-a i često kriptografski zaštititi kako bi se sačuvala privatnost.
Files/ Documents	Datoteke/ dokumenti	Zbirka bajtova pohranjenih kao pojedinačna cjelina na tvrdom disku. Datoteka je najčešći nazivnik za spremnik podataka. Svi podaci i programi, bez obzira na vrstu, pohranjuju se kao datoteke pod određenim imenom koje mora biti jedinstveno unutar fascikle (foldera, direktorija) u kojoj se nalazi na disku. Datoteke sa istim imenom mogu se nalaziti u različitim folderima.
File and Print Sharing	Zajedničko korištenje datoteka i štampača	Opcija koja je na raspolaganju na Windows Network Control Panel koja omogućava kompjuteru da određene foldere ili štampač dijeli s drugim kompjuterima na mreži. Standard je da ta opcija nije uključena.

Firewall	Firewall (Vatreni zid)	Sistem ili kombinacija sistema koji sprovode politiku odobrenja pristupa između dvije ili više mreža. To je primarni metod obezbjeđenja kompjutera od uljeza. Firewall dozvoljava ili blokira dolazeći i odlazeći sabraćaj na privatnoj mreži ili na korisničkom kompjuteru. Firewall je u širokoj upotrebi da bi se korisnicima pružio bezbjedan pristup Internetu kao i da bi se odvojio javni web server kompanije od njene interne mreže. Firewall se takođe koristi da se osiguraju segmenti interne mreže; na primjer, računovodstvena mreža može biti ranjiva na njuškanje unutar preduzeća.
Flash Drive	Fleš disk	Vidi USB disk.
Flash Memory	Fleš memorija	Vrlo popularan, postojan memorijski čip na kojem se mogu memorisati podaci preko podataka. Razvijena iz EEPROM čipa, fleš memoriju je izumila Toshiba i nazvala po njenoj sposobnosti da izbriše blok podataka u trenu (na engleskom "in a flash"). Ironija je da je ova karakteristika brisanja bloka podataka najmanje poželjna i proizvođači pokušavaju da je eliminišu razvojem novijih tehnologija. Izuzetno izdržljiv, fleš je u širokoj upotrebi za pohranjivanje modula kao što su USB diskovi i memorijske kartice za digitalne fotoaparate. Takođe se pakuju i kao samostalni čipovi za ugradnju integralnog kola.
Floppy Connector/ Drive	Konektor/uređaj za disketu	Očitava disketu preko unutrašnjeg ili vanjskog uređaja.
Floppy Disk	Disketa	Disketa je fleksibilan krug od magnetskog materijala sličan magnetskoj traci, osim što se koriste obje strane. Uređaj za čitanje zgrabi centar diskete i vrti je unutar kućišta. Glava za čitanje/pisanje uspostavlja kontakt sa površinom kroz otvor na plastičnoj školjki ili omotu. Diskete se vrte brzinom od 300 RPM, što je 10 do 30 puta sporije od tvrdog diska. One takođe miruju sve dok se ne zatraži transfer podataka. Iako sve diskete izgledaju isto, ono što je na njima zabilježeno određuje njihov kapacitet i kompatibilnost. Svaka nova disketa mora biti formatizirana, čime se bilježe sektori na disku koji sadržavaju podatke.
Forensic Examination	Forenzičko testiranje kompjutera	Tehnički pregled koji čini digitalne dokaze vidljivim i pogodnim za analizu; testiranje izvršeno na dokazima da bi se utvrdilo prisustvo ili odsustvo određenih podataka.

Forensic Image	Forenzička preslika	Fizička kopija diska.
Forensically Clean	Forenzički čist	Disk, traka ili drugi uređaj za pohranjivanje podataka na kojem nema nikakvih podataka i virusa. Na tom mediju nema ni nikakvih ostataka podataka.
Gateway	Poveznik	Most između dvije mreže. Parametar na mrežnoj kontrolnoj tabli koji određuje Internet adresu portala na webu, poznatu kao poveznik ili mrežni usmjerivač (ruter).
Hard drive	Tvrdi disk	Primarni uređaj za pohranjivanje podataka na kompjuteru koji vrti, čita i piše po jednoj ili više fiksnih magnetskih ploča. U praksi, izrazi hard disk drajv, hard disk, i tvrdi disk se koriste kao sinonimi. Tvrdi diskovi su mediji za pohranu podataka na desktop i laptop kompjuterima kao i na serverima i glavnim kompjuterima širom svijeta. Koriste se i u štampačima za pohranjivanje fontova i štampačkih poslova kao i u plejerima digitalne muzike i mnoštvu drugih prenosivih i stacionarnih uređaja kompjuterskog tipa. Iako prenosivi diskovi koji su spakovani u kasete koriste iste medije "tvrdih" diskova i sličnu tehnologiju, oni se uglavnom nazivaju premjestivi diskovi a ne tvrdi diskovi. Izraz tvrdi pravi razliku između tvrdih diskova napravljenih od aluminijuma ili stakla i koji su velikog kapaciteta i disketa napravljenih od plastike koje su malog kapaciteta.
Hardware	Hardver	Mašinerija i oprema (procesori, drajvovi za disk i traku, modemi, tastature, štampači, skeneri, kablovi, itd.) Kada radi, kompjuter je i hardver i softver. Jedan je beskoristan bez drugog. Izrada hardvera određuje komande koje može slijediti, a softveru instrukcije kažu šta da radi.
Hash Value	Heš funkcija	Metod kojim se osigurava tačnost obrađenih podataka. To je ukupno nekoliko polja podataka u datoteci, uključujući i polja koja se normalno ne koriste u kalkulacijama, kao što je broj korisničkog računa. U raznim fazama procesa, heš funkcija se preračunava i upoređuje sa originalom. Ako su neki podaci izgubljeni ili promijenjeni, nepodudaranje rezultata ukazuje na grešku.
Hub	Mrežni čvor	Hardverski uređaj koji povezuje kompjutere na lokalnoj mreži (LAN). Svaki kompjuter se povezuje na mrežni čvor preko Eternet kabla.

Hybrid Gateway	Hibridni poveznik	Neuobičajena kombinacija s usmjerivačima (ruterima) koji vode evidenciju o kompletnom stanju TCP/IP veza ili pregledaju saobraćaj da bi pokušali da otkriju i spriječe napade (može uključiti i Bastion host). Teško ga je dodati, održavati i revidirati.
Image	Preslika	Kopija sadržaja tvrdog diska, koja uključuje operativni sistem i instalirane aplikacije.
Information Systems Technology	Tehnologija informacijskih sistema	Zaštita informacija od slučajnog ili namjernog ali neovlaštenog objelodanjivanja, modifikacije ili uništenja ili onemogućavanja da se obrade te informacije.
Interface	Interfejs	Zajednička granica definisana zajedničkim fizičkim karakteristikama povezivanja, karakteristikama signala i značenjem razmijenjenih signala.
Internet	Internet	Globalni sistem uzajamno povezanih mreža. Nastao na temelju ARPANET-a, rastao je od 1969. da bi postao zajednica vladinih agencija, privatnih organizacija i obrazovnih institucija. Nijedan entitet nije vlasnik Interneta. Većina organizacija ga koriste da bi komunicirale, vršile istraživanja i razmjenjivale podatke i resurse kao što su upravljanje i pohranjivanje podataka. Pojedinci se također uključuju na Internet radi elektronske pošte, vijesti, itd. Internet predstavlja najveću zbirku elektronskih informacija. Pružatelji Internet usluga (provajderi) kontrolišu uspostavljanje veze na Internetu. Provajderi pružaju i naplaćuju pristup Internetu. Pojedinci plaćaju mjesečnu naknadu kompanijama kao što su America Online i dobijaju korisničko ime, lozinku, softver i pristupni telefonski broj. Provajderi nude velikim organizacijama sredstvo za povezivanje njihovih mreža sa Internetom.
Internet Search	Pretraživanje Interneta	Program za pretraživanje Interneta napravljen je tako da traga za informacijama na World Wide Webu. Rezultati pretrage se obično pojavljuju u obliku spiska i obično nazivaju pogoci (hit). Informacije se mogu sastojati od web stranica, slika, podataka i drugih vrsta datoteka. Neki programi za pretraživanje na webu također vade podatke koji su na raspolaganju u bazama podataka ili javnim direktorijima. Za razliku od direktorija na Webu koje održavaju urednici, programi za pretraživanje na webu rade na principu algoritma i ljudskog doprinosa.

IP	IP	Internet protokol. Protokol mrežnog sloja iz skupine TCP/IP protokola (za Internet).
IP Address	IP adresa	Identifikator mrežnog čvora kojeg dodjeljuje menadžer mreže (lokalno ili na daljinu) kako bi dozvolio vanjsku mrežnu komunikaciju. Dodjeljivanje IP adrese je od suštinskog značaja za preusmjeravanje komunikacije na mreži. Svaki uređaj na LAN-u mora imati jedinstvenu IP adresu. Svaka adresa je od suštinskog značaja za rad na Internetu preko globalne mreže. IP adresa je hijerarhijska i ima dva dijela. Prvi dio je identifikator mreže (NETID) koji jedinstveno identifikuje mrežu na globalnom Internetu i koristi se u svrhe preusmjeravanja. Drugi dio je identifikator kompjutera-domaćina (HOSTID) koji jedinstveno identifikuje domaćina (host) na datoj mreži. U prošlosti je Kategorija A adresa imala 8-bita NETID i 24-bita HOSTID, omogućavajući mreže sa vrlo velikim brojem kompjutera-domaćina. Kategorija B adresa ima 16-bita NETID i 16-bita HOSTID, dok Kategorija C adresa ima 24-bita NETID i 8-bita HOSTID. Kategorija D adrese se koriste za odašiljanje iste poruke podgrupi terminala a kategorije C adrese su za eksperimentalne aplikacije. IP adrese se pišu kao četiri grupe brojeva, odvojene tačkama. Na primjer, 131.160.10.240 predstavlja IP adresu Kategorije B. (Adrese IP verzije 4 su duge 32 bita; adrese nove IP verzije 6 su duge 128 bita.)
Intellectual Property	Intelektualno vlasništvo	Ideja, izum ili proces koji proizilazi iz umnog ili intelektualnog rada.
ISP	ISP	Pružatelj Internet usluga. Institucija koja omogućava pristup Internetu u nekom obliku, obično za novac.
Key	Ključ	U kriptografskoj zaštiti, ključ je niz znakova koji se koriste za šifriranje i dešifriranje datoteke. Ključ se može unijeti u dva formata: alfanumerički i kondenzovani (heksadecimalni). Na tržištu obezbjeđenja pristupa mreži, ključ se obično naziva token ili sredstvo za provjeru vjerodostojnosti, uređaj koji se koristi da bi slao pitanja i primao odgovore tokom procesa identifikacije korisnika. Ključevi mogu biti mali, ručni hardverski uređaji slični džepnom digitronu ili kreditnim karticama, ili mogu biti učitani u personalni kompjuter kao zaštićena kopija.

Letter of Rogatory	Formalni zahtjev suda	Formalna međunarodna saradnja uključuje i da jedna zemlja zvanično zatraži pomoć ili informacije od druge.
Linux	Linux	Besplatni softver u širokoj upotrebi koji je operativni sistem kao Unix. Njegov pronalazač Linus Torvalds ga je prvi put objavio 1991. Verzije Linuxa postoje za većinu tipova kompjuterskih hardvera od desktop kompjutera do velikih kompjuter IBM-a. Linux je besplatan i na raspolaganju svakom ko želi da ga ispituje i mijenja sve dok su te promjene dostupne javnosti. Ova karakteristika dovela je do toga da hiljade ljudi rade na različitim aspektima Linuxa i prilagođavanju Linuxa u raznovrsne svrhe od servera do TV-rekordera.
LAN	LAN	Lokalna mreža (LAN). U uzajamno povezanom sistemu kompjutera i perifernih uređaja, korisnici LAN-a razmjenjuju podatke pohranjene na tvrdim diskovima, a mogu i zajednički koristiti štampače povezane na mrežu.
Log	Dnevnik	Dnevnik kompjuterske aktivnosti koji se koristi u statističke svrhe, ali i kao rezervna kopija za ponovno podizanje sistema.
Log in	Prijava	Prijaviti se i ostvariti pristup serverima na mreži, web serverima i drugim kompjuterskim sistemima. Naziva se takođe login ili logon.
Log out	Odjava	Odjaviti se i otići sa servera na mreži, web servera ili drugih kompjuterskih sistema. Naziva se takođe logout ili logoff.
Logging	Evidentiranje	Proces pohranjivanja informacija o događajima koji su se desili na Firewallu ili mreži.
Logical Image	Logička preslika	Kopija particije diska.

MAC Address	MAC adresa	Adresa kontrole pristupa mediju. Jedinstvena fizička adresa koja identifikuje podatke o transmisiji na mreži. MAC adresama koje su pohranjene na mrežnim interfejs karticama (NIC), može se ostvariti pristup na Sloju veze jer se one odnose na adrese fizičkog hardvera. Kada kompjuter na Eternet mreži hoće da pošalje paket podataka drugom kompjuteru koristi MAC adresu kompjutera koji prima paket da bi odredio njegovu putanju. Paket podataka nosi MAC adresu kompjutera koji ga prima. MAC adresa je jedinstvena 48-bitna adresa koju mrežnoj interfejs kartici (NIC) dodjeljuje proizvođač adaptera. Dole je primjer MAC adrese: 00-A0-C9-12-34-56 Prvih osam bitova (00-A0-C9) određuju isporučitelja (Intel). Drugih osam bitova (12-34-56) isporučitelj dodjeljuje mrežnoj interfejs kartici (NIC) kao njenu jedinstvenu identifikaciju.
Mac OSX	Mac OSX	Macintosh operativni sistem (verzija 10). Apple operativni sistem, takođe poznat pod imenom Snow Leopard (snježni leopard).
Malicious code	Zlonamjerni softver	Program koji obavlja funkcije za koje nije dobio dozvolu legitimnog korisnika. U zlonamjerne softvere spadaju virusi, crvi, trojanski konji, logičke bombe i zamke ili klopke (trap).
Malware	Malver	Softver napravljen da uništi, pogorša i na drugi način onemogući normalan rad računarskih sistema.
MD5	MD5	Kriptografski algoritam MD5. Algoritam za izračunavanje heš funkcije.
Metadata	Metapodaci	Informacije koje opisuju karakteristike drugih datoteka, kao što su datum i vrijeme kada je datoteke nastala ili modifikovana ili kada je ostvaren pristup datoteci.

Memory	Memorija	Radni prostor kompjutera: fizički skup dinamičkih RAM (DRAM) čipova. Memorija je glavni resurs u kompjuteru jer ona određuje veličinu i broj programa koji mogu raditi u isto vrijeme, kao i količinu podataka koji se mogu trenutno procesirati. Svo aktiviranje programa i obrada podataka odvija se u memoriji, koja se često naziva glavnom memorijom da bi se razlikovala od memorijskih čipova na integralnom kolu uređaja. Instrukcije za program kopiraju se u memoriju sa diska, trake ili s mreže i onda pozivaju iz memorije u kontrolnu jedinicu kako bi se analizirale i izvršile. Instrukcije upućuju kompjuter da unese podatke u memoriju s tastature, diska, trake, modema ili mreže.
Monitoring	Nadzor	Skraćena verzija kompjuterskog nadzora. Bilježi aktivnost korisnika na kompjuteru. Programi kompjuterskog nadzora utvrđuju koliko vremena zaposleni provodi na različitim zadacima, a moguće i na nezakonitim aktivnostima. Ovi programi mogu zabilježiti kucanje na tastaturi, ćaskanje i slanje trenutačnih poruka preko Interneta, kopirati ekran i Webcam fotografije, a sve to se može lokalno pohraniti ili prebaciti na neko drugo mjesto.
Motherboard	Matična ploča	Nazvana još i sistemska ploča, glavna ploča, osnovna ploča ili logička ploča, je primarno štampano integralno kolo u kompjuteru ili drugim elektronskim uređajima. U modernom desktop kompjuteru, matična ploča se sastoji od procesora (CPU), čipseta, utičnica za memoriju i svih kontrolnih integralnih kola za diskove, tastaturu, miša, mrežu, zvuk i USB. Može imati PCI slot za međupovezivanje adaptera za najsavremeniji ekran i PCI slot za međupovezivanje ostalih perifernih komponenti. Matične ploče laptopa po pravilu imaju ugrađene sve periferne kontrolore.
MP3	MP3	MPEG-1 Audio sloj III. Tehnologija audio kompresije koja je revolucionarizirala digitalnu muziku. Potiče iz audio dijela MPEG-1 i MPEG-2 video specifikacija, MP3 komprimira CD-kvalitet zvuka faktorom od približno 10, pri čemu uglavnom zadržava vjernost originalu. Na primjer, CD traka od 40MB se pretvara u MP3 datoteku od približno 4MB.
MP3 Player	Digitalni audio plejer (MP3 plejer)	Elektronski uređaj koji je u stanju da očitava i emituje datoteke MP3 formata.

Multi-User	Višekorisnički	Sposobnost da se više istovremenih korisnika prijavi i pokrene aplikacije sa jednog jedinog servera.
NetBIOS	NetBIOS	Microsoftov Osnovni ulazno/izlazni sistem za mrežno povezivanje, programski interfejs između adapterskih protokola lokalne mreže i aplikacije. Ovaj interfejs omogućava aplikaciji da raspolaže komunikacijskim sposobnostima LAN-a, a da ne mora da zna LAN-ov protokol.
Network Computing Architecture	Mrežna kompjuterska arhitektura	Kompjuterska arhitektura u kojoj se komponente dinamički presnimavaju s mreže u uređaj klijenta koji će ih aktivirati. Programski jezik Java je srž kompjuterskog rada na mreži.
Network Connectivity	Sposobnost povezivanja s mrežom	Topološki opis mreže koji navodi, sa stanovišta lokacije i količine krugova, međupovezivanje čvorova transmisije.
Network-Level Firewall	Firewall na nivou mreže	Firewall kod kojeg se saobraćaj pregleda na nivou paketa protokola mreže.
Network Monitor	Nadzor mreže	Specijalizovani hardverski uređaj ili softver u desktop ili laptop kompjuteru koji vrši rutinsku inspekciju paketa podataka koji se prenose preko mreže i otkriva probleme. Takođe se naziva njuškalo, njuškalo paketa, analizator paketa, ili analizator protokola, uređaj za nadzor mreže uključuje se u utičnicu na mrežnom čvoru ili prekidaču i za administratora mreže dekodira jedan ili više protokola u format koji čovjek može čitati. Može takođe pohranjivati pakete podataka na disk za dodatnu analizu kasnije.
Network Port	Mrežna utičnica	Virtuelna veza koja omogućava kompjuterima na mreži da šalju i primaju podatke. Svaka aplikacija na mreži ima dodijeljen specifičan broj utičnice. Utičnice se koriste u TCP i UDP protokolima. Utičnice 0-1023 su opšte poznate utičnice (port) rezervisane za server. Utvrđene su usluge koje koriste ove brojeve utičnica (port), kao što je FTP (21 za kontrolu, 20 za podatke), SMTP (25), Telnet (23) i HTTP (80). Utičnice 1024-49151 su registrovane i može ih koristiti svaka aplikacija. Ove utičnice (port) treba koristiti samo nakon što se registruju. Utičnice 49152-65535 su dinamičke utičnice. Ove utičnice (port) može koristiti svaka aplikacija u bilo koju svrhu i nije potrebna prethodna registracija. Spisak TCP/UDP utičnica (port) može se naći na http://www.iana.org / assignments/port-numbers.

NIC	NIC	Mrežna interfejs kartica (NIC). Adapter na kompjuteru koji mu omogućava da se poveže na mrežu. Svaki NIC je napravljen za određenu vrstu mreže koju podržava, kao što je Eternet, prstenasta mreža i Interfejs za slanje podataka preko optičkog kabla (FDDI). Neke kartice se odvojeno uključuju u matičnu ploču, a druge su integrisane u nju. NIC se proizvodi sa tvrdo ožičenim kodom, poznatim kao MAC adresa, jedinstvena za svaku karticu. Kada se NIC instalira u kompjuter ili neki drugi uređaj, MAC adresa odgovara fizičkoj adresi tog kompjutera na mreži. MAC adresa se koristi da bi se identifikovalo pravo odredište za prenošenje paketa podataka preko mreže. Kada kompjuter podnese zahtjev za komunikacijom s mrežom, OS šalje taj zahtjev NIC-u. NIC pretvara zahtjev u odgovarajuću vrstu paketa podataka koji će se poslati preko mreže. On onda nadzire tok saobraćaja na mreži i šalje pakete podataka u odgovarajuće vrijeme kada se ukaže slobodan prostor. Pored pripreme i slanja paketa podataka, NIC takođe provjerava MAC adrese transmisija koje prolaze mrežom da bi utvrdio da li su upućene tom kompjuteru. Ako se adrese podudare, NIC kopira paket podataka za taj kompjuter.
Non-volatile	Postojani	Kada je riječ o kompjuterskoj memoriji, to znači da sadržaj nije izgubljen kad se isključi struja. To ne znači nepromjenjiv, što je obično značenje te riječi, jer se preko mnogih postojanih čipova može ponovo memorisati.
One-Time Password	Jednokratna lozinka	U obezbjeđenju mreže, lozinka koja se izdaje samo jednom kao rezultat bezbjednosnog pitanja/odgovora u procesu identifikacije korisnika. Ne može se ukrasti ili ponovo koristiti za neovlašteni pristup. Takođe nazivane jednoprolazne zakrivke, jednokratne lozinke su jedini poznat tip neslomive kriptografske zaštite.
Online	Na mreži	Povezan, opslužen ili na raspolaganju kroz sistem, posebno kompjuterski ili telekomunikacijski sistem (kao što je Internet); aktivnost koja se obavlja za vrijeme veze s takvim sistemom
Online Account	Korisnički račun na mreži	Formalni poslovni aranžman koji omogućava redovno poslovanje ili pružanje usluga preko Interneta ili sličnog telekomunikacijskog sistema

Open Source	Besplatni softver	Odnosi se na softver koji se distribuira sa svojim izvornim kodom tako da krajnji korisnik, organizacija ili dostavljač može da ga modifikuje u svoje vlastite svrhe. Većina licenci za besplatne softvere omogućava da se oni redistribuiraju bez ograničenja pod istim uslovima navedenim u licenci.
Operating system	Operativni sistem	Sistemski softver koji kontroliše kompjuter i njegove periferne uređaje. Moderni operativni sistemi, kao što je OS Windows i NT, obavljaju mnogo osnovnih funkcija kompjutera.
Optical Media	Optički medij	Poznati i kao optički diskovi, optički mediji su mediji za pohranjivanje sa direktnim pristupom koji se pišu i čitaju pri svjetlu. Najčešći optički diskovi u upotrebi su CD-ovi i DVD-ovi, a postoje tri vrste: samo za čitanje, samo za pisanje i oni preko kojih se može ponovo pisati (memorisati). CD, CD-ROM, DVD-ROM, DVD-Video kao i BD-ROM (Blu-ray) su diskovi samo za čitanje koji su snimljeni u vrijeme proizvodnje i ne mogu se izbrisati. CD-R, DVD-R, DVD+R, BD-R, WORM i magnetno-optički (u WORM modu) diskovi samo za jednokratno pisanje (memorisanje). Oni se snimaju u korisnikovom okruženju i ne mogu se brisati. Preko CD-RW, DVD-RAM, DVD-RW, DVD+RW, BD-RE i MO diskova se može ponovo pisati (memorisati).
Overwrite	Pisati preko postojećih podataka	Bilježiti nove podatke preko postojećih podataka kao što je slučaj kad se snima disk ili ažurira datoteka.
P2P	P2P	Veza ravnopravnih kompjutera
Packet	Paket podataka	Naručena grupa podataka i kontrolnih signala koja se prenosi preko mreže, kao podgrupa neke veće poruke.
Partition	Particija diska	Dio diska ili memorije koji je odvojen po strani u neku svrhu. Na personalnom kompjuteru, mora se napraviti particija novog tvrdog diska prije nego što se može formatizovati za operativni sistem i za taj zadatak se koristi softver Fdisk. On može napraviti jednu particija diska, stvoriti jedno slovo drajv za cijeli disk ili može napraviti više particija, veličine prema vašim zahtjevima. Na primjer, drajvovi C:, D:, i E: mogu biti na istom fizičkom disku, ali za operativni sistem i korisnika funkcionišu kao tri logička drajva.

Password	Lozinka	Tajni kod dodijeljen korisniku. Fraza koju poznaje kompjuterski sistem. Poznavanje lozinke povezano s identifikacijom korisnika smatra se dokazom autorizacije.
PCI Slots	PCI slotovi	Slotovi za međupovezivanje perifernih komponenti. PCI most povezuje PCI sabirnice zajedno za više utičnica (slot).
PDA	PDA uređaj	Personalni digitalni asistent
Peer-to-Peer	Veza ravnopravnih kompjutera	Mrežni protokol za kompjuterske korisnike koji dozvoljava korisnicima međusobno direktno slanje podataka, umjesto preko websajt servera.
Peripheral	Periferni	Bilo koji ulazni i izlazni sistem ili uređaj za pohranjivanje podataka povezan vanjski ili interno na kompjuterski procesor, kao što je monitor, tastatura, štampač, disk, traka, grafički tablet, skener, komandna ručica, padl (kontrolor igre) ili miš.
PIN	PIN	Lični identifikacioni broj. Koristi se za obezbjeđenje kompjutera tokom procesa identifikacije korisnika, poznat je samo korisniku.
Power Connector	Konektor za struju	Električni konektor za povezivanje opreme sa utičnicama u zidu
Promiscuous Mode	Promiskuitetni mod	Način operacija za mrežnu interfejs karticu (NIC) u kojem svaki poslati paket podataka NIC može da primi i čita.
Proxy	Proksi služba	(1) Metod zamjene koda za servisnu aplikaciju sa poboljšanom verzijom koja je mnogo sigurnija. Poželjni metod uslužnih zajednica - npr. Oracla - radije nego individualne aplikacije razvijene iz priključenja na utičnicu. (2) Softverski program koji djeluje u ime korisnika. Tipična proksi služba prihvata vezu od korisnika, donosi odluku o tome da li IP adresa korisnika ili klijenta dozvoljava korištenje proksi službe, možda obavi dodatnu provjeru identiteta korisnika i kompletira vezu sa udaljenom destinacijom u ime korisnika.

Public Key	Javni ključ	U kriptografiji, sistem dualnog ključa u kojem se jedan ključ koristi za enkripciju podataka, a drugi za dekripciju. Pošto poznavanje samo jednog ključa ne donosi poznavanje i drugog ključa, jedan ključ može postati javan dok vlasnik ključa drugi ključ čuva za sebe.
RAM	RAM	Radna memorija kompjutera. Vrsta memorije koja pruža direktan pristup svakom bajtu na čipu.
Registry	Registar	Konfiguracijska baza podataka u svim 32-bitnim verzijama Windowsa koja sadrži parametre za hardver i softver u personalom kompjuteru u kojem je Registar instaliran. Registar se sastoji od SYSTEM.DAT i USER.DAT datoteka. Mnogi parametri koji su prethodno pohranjivani u WIN.INI i SYSTEM.INI datotekama u 16-bitnim verzijama Windowsa (Windows 3.x) su sada u Registru. Registar se može direktno uređivati ali obično se to radi samo za tehnička poboljšanja ili u krajnjoj nuždi. Rutinski pristup je preko kontrolne table u meniju My Computer (moj kompjuter) ili Properties (karakteristike). Desnim klikom miša na gotovo svakoj ikonici u Windowsu doći ćete na meni Properties (karakteristike) tog objekta. Personalni kompjuter sa mnogo aplikacija koje se koriste izvjesno vrijeme može lako imati stotine hiljada ili više upisa u Registru.
Remote Access	Daljinski pristup	Priključenje udaljenog kompjuterskog uređaja preko komunikacijskih veza kao što su redovne telefonske linije ili mrežama širokog dosega da bi se ostvario pristup aplikacijama i informacijama na mreži.
Router	Mrežni usmjerivač (rauter)	Hardverski uređaj ili kompjuterski softver koji međusobno povezuje različite pristupne metode i protokole. Djeluje kao most velike funkcionalnosti; koristi se u mrežama širokog dosega (WAN).
Screened Host Gateway	Poveznik za zaštićeni host-kompjuter	Host-kompjuter na mreži iza zaštitnog rautera. Stepen u kojem se može ostvariti pristup zaštićenom host- kompjuteru zavisi od pravila zaštite u rauteru.
Screened Subnet	Zaštićena podmreža	Izolovana podmreža napravljena iza zaštitnog rautera da bi se zaštitila privatna mreža. Stepen u kojem se može ostvariti pristup zaštićenoj podmreži zavisi od pravila zaštite u rauteru.

Screening Router	Zaštitni rauter	Usmjerivač (rauter) konfigurisan da može da dozvoli ili uskrati saobraćaj koristeći tehnike zasnovane na nizu dozvola koje je instalirao administrator. Komponenta u mnogim zaštitnim zidovima (Firewall) koja se obično koristi za blokiranje saobraćaja između mreže i konkretnih host-kompjutera na nivou IP porta. Nije vrlo bezbjedna, ali se koristi kada je brzina jedini kriterij za donošenje odluka.
Screen name	Korisničko ime	Ime koje odabire korisnik za komunikaciju s drugima na mreži, na Internetu
Secret Key	Tajni ključ	U kriptografskoj zaštiti, jedan ključ (ili lozinka) koji se koristi i za zaključavanje, i za otključavanje podataka. Uporedite s javnim ključem.
Seizure	Pljenidba	Čin, radnja ili proces pljenidbe; zaplijenjena roba. Oduzimanje imovine zakonitim putem.
Server	Server	Kontrolni kompjuter na lokalnoj mreži kojim kontrolišete pristup softvera radnim stanicama, štampačima i drugim dijelovima mreže.
Server-based Computing	Kompjuterske radnje preko servera	Inovativan pristup obavljanju kompjuterskih radnji preko servera kako bi se aplikacije od ključnog značaja za poslovanje dostavljale na uređaje krajnjeg korisnika dok se logika aplikacije sprovodi na serveru i preko mreže se do klijenta prenosi samo korisnički interfejs. Njene prednosti su u upravljanju aplikacijom iz jednog mjesta, univerzalnom pristupu aplikaciji, propusnosti-nezavisnom radu i poboljšanoj sigurnosti za poslovne aplikacije.
Server Farm	Farma servera	Skupina servera povezanih u jedan sistem koji obezbjeđuje centralizovanu administraciju i sposobnost horizontalnog širenja.
SHA	SHA	Sigurni heš algoritam. Algoritam za izračunavanje heš funkcije.
Sign Off	Sign Off (odjava)	Sinonim za drugi engleski izraz za odjavu log out
Sign On	Sign On (prijava)	Sinonim za drugi engelski izraz za prijavu log in

SIM Card	SIM kartica	Modul za identifikaciju pretplatnika (SIM kartica). Prenosna pametna kartica korištena u GSM mobilnim telefonima kao i UMTS telefonima, satelitskim telefonima i nekim CDMA telefonima. Sadrži jedinstven ID i autentifikacijske kodove dodijeljene pretplatniku kao i telefonski broj pretplatnika i podatke koji se odnose na mrežu. Uvedene 1991., SIM kartice se mogu programirati da na ekranu telefona pokazuju meni prema potrebama pretplatnika.
Slave	Slave	Kompjuter ili periferni uređaj kojeg kontroliše neki drugi kompjuter. Na primjer, terminal ili štampač na udaljenoj lokaciji koji samo prima podatke kao sekundarni uređaj (slave). Kada su dva kompjutera povezana preko serijskog ili paralelnih portova za razmjenu datoteka, program za transfer datoteka može odrediti da je jedan kompjuter master a drugi slave.
Smart Card	Pametna kartica	Uređaj veličine kreditne kartice sa umetnutim mikroelektronskim kolom za pohranjivanje informacija pojedinca. To nije ključ ili token kao što se koristi u procesu identifikacije korisnika na daljinu.
SMS	SMS	Usluga slanja kratkih poruka. Uobičajena usluga za slanje kratkih tekstualnih poruka koja je na raspolaganju na mobilnim telefonima i drugim ručnim uređajima. Ukucavanje tekstualne poruke (tekstiranje), čija je dužina ograničena na 160 znakova, može se vršiti na najprostijim mobilnim telefonima sa samo numeričkim tipkama. Neki moderniji mobilni telefoni opremljeni su tastaturom koja simulira pisaću mašinu. Poruke se šalju na obične telefonske brojeve ili kraće brojeve za komercijalnu upotrebu. Kao i kod slanja trenutačnih poruka, SMS prenosi poruku pošiljaoca do primaoca odmah. On takođe pohranjuje i proslijeđuje poruke kasnije ako je primaočev telefon isključen kada je poruka poslata. Cijene SMS razliku se od jednog do drugog nosioca modulacije, koji mogu naplaćivati fiksni mjesečni iznos, naplaćivati po poruci ili to uključiti u plan usluga.
Software	Softver	Instrukcije za kompjuter. Niz instrukcija koje obavljaju određeni zadatak naziva se program. Dvije glavne kategorije softvera su sistemski softver i aplikacijski softver. Sistemski softver se sastoji od kontrolnih programa kao što su operativni sistem i sistem upravljanja bazom podataka. Aplikacijski softver je svaki program koji obrađuje podatke za korisnika (inventar, plate, računovodstvene tabele, procesor teksta, itd.)

SSH	SSH	Secure Shell. Program koji se koristi za uključivanje u drugi kompjuter preko mreže, za izvršavanje komandi u udaljenom kompjuteru i za prebacivanje datoteka s jednog kompjutera na drugi. Obezbjeđuje snažnu potvrdu identiteta korisnika i bezbjednu komunikaciju preko neobezbjeđene mreže. Svrha mu je da zamijeni Telnet, rlogin, rsh i rcp.
Sterile	Forenzički sterilan	Forenzički čist.
Steganography	Steganografija	Sakrivanje poruke unutar slikovne, audio ili video datoteke. Koristi se kao alternativa kriptografskoj zaštiti i iskorištava neupotrebljene bitove unutar strukture datoteke ili bitove kod kojih se uglavnom neće ni otkriti da su mijenjani. Steganografska poruka putuje tajno do svog odredišta, za razliku od kriptografski zaštićenih poruka koje, premda se ne mogu dešifrovati bez ključa za dekripciju, mogu se identifikovati kao enkriptovane.
Storage Media	Mediji za pohranu podataka	Periferni uređaj za pohranjivanje podataka kao što je disk, traka ili fleš memorijska kartica. Tehnologije pohranjivanja obuhvataju magnetske diskove, magnetske trake, optičke diskove i fleš memoriju.
Switch	Prekidač	Uređaj koji ispunjava zahtjeve za bržom vezom i većom propusnosti mreže. Kao i čvorišta, prekidači imaju mnogo utičnica (port). Međutim, samo jedan ili nekoliko kompjutera su povezani sa svakim portom na prekidaču omogućavajući tako veću propusnost za svaki kompjuter. Prekidači pomažu da se poveća brzina mreže time što određuju propusnost za svaki port. Za razliku od njih, čvorišta razmijenjuju propusnost među svim utičnicama (port). Prekidač određuje propusnost svakog porta i usmjerava saobraćaj od porta izvora direktno na port odredišta.
System (operating)	Sistem (operativni)	Glavni kontrolni program kompjutera. Kada se kompjuter uključi, mali program za inicijaciju sistema učitava operativni sistem. Iako se mogu učitati i dodatni moduli po potrebi, glavni dio, poznat kao kernel ostaje u memoriji sve vrijeme. Operativni sistem (OS) određuje standarde za sve aplikacijske programe koji su aktivni na kompjuteru. Aplikacije "razgovaraju" s operativnim sistemom za sve korisničke interfejsove i operacije upravljanja datotekama.

TCP	TCP	Protokol za kontrolu prenosa podataka. Niz pravila (protokol) koji se koristi zajedno sa Internet Protokolom (IP) da bi se poslali podaci u obliku poruke između kompjutera preko Interneta. TCP je poznat kao protokol orijentisan na vezu, što znači da je uspostavljena i održava se veza sve dok poruka ili poruke koje treba da razmijene aplikacijski programi, ne budu razmijenjene na svakom kraju.
TCP/IP	TCP/IP	Protokol o kontroli transmisije/Internet protokol. TCP/IP se koristi za povezivanje kompjutera sa različitim platformama operativnih sistema širom mreže ili serije mreža. Tokom 1970-tih razvilo ga je Američko ministarstvo odbrane i danas je TCP/IP transportni protokol koji koristi Internet. TCP/IP se u stvari sastoji od dva protokola ali predstavlja arhitekturu protokola sastavljenu od desetak protokola. IP je protokol koji se koristi za prebacivanje paketa podataka kroz mrežu i bavi se usmjeravanjem. TCP je protokol od hosta do hosta i pruža pouzdan prenos podataka od jednog kraja do drugog; UDP je takođe protokol od hosta do hosta ali ne garantuje dostavu podataka. Drugi protokoli podržavaju aplikacije krajnjih korisnika kao što su daljinsko prijavljivanje na mrežu (SSH i Telnet), elektronska pošta (SMTP, POP i IMAP), i World Wide Web (HTTP, HTTPS).
Thumb Drive	USB fleš disk	Sinonim za USB fleš drajv.
Token	Token	Sredstvo za provjeru vjerodostojnosti - uređaj koji se koristi da bi se slala pitanja i primali odgovori tokom procesa identifikacije korisnika. Tokeni mogu biti mali, ručni hardverski uređaji slični džepnom digitronu ili kreditnim karticama.
Traffic data	Saobraćajni podaci	Kompjuterski podaci koji se odnose na aktivnost ili komunikaciju putem kompjuterskog sistema, koje proizvodi kompjuterski sistem u lancu komunikacije, ukazujući na porijeklo, odredište, rutu, vrijeme, datum, veličinu i trajanje komunikacije ili vrstu uslužnog servisa.
Tunneling Router	Rauter za tuneliranje poruka	Mrežni usmjerivač (rauter) ili sistem koji je u stanju da usmjerava saobraćaj tako što ga kodira i hermetički zatvara za transmisiju preko nepouzdane mreže za eventualno otvaranje i dekripciju.

UDP	UDP	Krisnički datagram protokol. Jedan od protokola transportnog sloja za prenos podataka koji je dio TCP/IP skupine protokola. UDP je protokol bez uspostavljanja veze jer host-kompjuter koji šalje podatke se ne povezuje sa host-kompjuterom koji ih prima. Host-kompjuter koji prima UDP pakete ne potvrđuje prijem paketa podataka.
Unallocated	Nedodijeljen	Na raspolaganju za pohranjivanje podataka.
Unix	Unix	Kompjuterski operativni sistem (osnovni softver koji je aktivan na kompjuteru ispod programa kao što su word procesor i računovodstvene tabele.) Unix je napravljen tako da ga istovremeno koristi mnogo ljudi; to je operativni sistem sa više korisnika u kojem je ugrađen TCP/IP. To je najčešći operativni sistem za servere na Internetu.
USB	USB	Univerzalna serijska sabirnica. To je hardver interfejs za priključenje perifernih uređaja na kompjuter koji je u najširoj upotrebi. Nakon što se pojavio u personalnim kompjuterima 1997., USB je brzo postao popularan za povezivanje tastature, miša, štampača i tvrdih diskova, zamjenjujući na kraju serijske i paralelne priključke (port) na personalnom kompjuteru. USB uređaji se mogu lako zamijeniti; mogu se uključivati i isključivati dok je kompjuter uključen.
USB Drive	USB disk	(1) Vanjski tvrdi disk ili optički disk koji se uključuje u USB port. (2) Fleš memorijski modul koji se uključuje u USB port kompjutera. Dovoljno mali da može da se zakači na lanac za ključeve, imitira tvrdi disk i dozvoljava da se podaci lako prenose s jednog kompjutera na drugi. Vrlo popularna rezervna kopija i medij za prenos podataka, USB diskovi mogu imati kapacitet i mnogo veći spremnik od CD i DVD na koje se može snimati. Oni su u širokoj upotrebi kao štampani medij za klijente da bi se distribuirali promotivni podaci. Iako je skuplji od CD i DVD koji se koriste u ove svrhe, ljudi po pravilu ponovo koriste ovaj uređaj, a prodavci dobijaju bolju reklamu. Ova vrsta USB uređaja poznata je pod mnogim imenima: fleš drajv, pen drajv, drajv na lančiću za ključeve, ključ drajv, USB ključ, USB stik ili memorijski ključ. Naziv marke se takođe koristi kao generičko ime, kao što su Lexar's JumpDrive i Trek 2000 International's ThumbDrive

User	Korisnik	Svaka osoba u direktnoj interakciji sa kompjuterom.
User ID	Korisnički ID	Jedinstven niz karakteristika koje identifikuju korisnika.
User Identification	Identifikacija korisnika	Proces u kojem korisnik identifikuje nekoga u sistemu kao validnog korisnika. Za razliku od procesa identifikacije korisnika, ovo je proces utvrđivanja da je korisnik zaista stvarni korisnik i da mu je dozvoljeno da koristi sistem.
User Interface	Korisnički interfejs	Tekstualni ili grafički dio aplikacije koji omogućava korisniku da pokreće softver u namijenjenu svrhu, tj. tekstualni interfejs kao što je DOS ili grafički interfejs kao što je Windows.
Virtual Network Perimeter	Krug virtuelne mreže	Mreža koja djeluje kao jedna jedina zaštićena mreža iza Firewalla, koja ustvari obuhvata kriptografski zaštićene virtuelne veze preko nepouzdanih mreža.
Virus	Virus	Segmet koda koji se sam replicira. Virus može a ne mora sadržavati napadne programe ili klopke. Virus je grupa kompjuterskih programskih kodova koja pravi vlastite kopije bez bilo kakve svjesne intevencije čovjeka. Neki virusi rade više od jednostavnog repliciranja; oni mogu pokazivati poruke, instalirati druge softvere ili datoteke, izbrisati softvere ili datoteke, itd. Virus traži prisustvo nekog drugog programa da bi se replicirao. Po pravilu, virusi se šire kačenjem za programe i neke druge datoteke. Na primjer, datoteke formata za Microsoft word procesor i programi računovodstvenih tabela dozvoljavaju uključivanje programa koji se zovu macros, što može biti povoljno tlo za uzgoj virusa.
VoIP	VoIP	Glas preko IP-a. Digitalni telefonski servis koji koristi javni Internet i privatne Network Backbone (glavne mreže) za prenošenje poziva. Obezbjeđena je takođe i podrška javnim telefonskim mrežama (PSTN) tako da VOIP pozivi mogu da potiču i da se završavaju na običnom telefonu. Mnoge kompanije, uključujući Vonage, 8x8 i AT&T (CallVantage), po pravilu nude pozive unutar zemlje za fiksnu cijenu i jeftine troškove poziva po minuti za inostranstvo. Od korisnika se traži da imaju širokopojasni pristup Internetu (kabl ili DSL).

Volatile	Nepostojan	Kad je riječ o kompjuterskoj memoriji, to znači privremena (a ne vrlo promjenljiva, što je uobičajeno značenje te riječi).
Volatile data	Nepostojani podaci	Sadržaj fizičke memorije, mrežna konfiguracija, otvorene veze s drugim kompjuterima, procesne informacije, itd.
VPN	VPN	Virtuelna privatna mreža. VPN se obično odnosi na mrežu u kojoj su neki dijelovi povezani preko javnog Interneta, ali su podaci poslati preko Interneta kriptografski zaštićeni tako da je cijela mreža "virtuelno" privatna.
Web	Web	Dio Interneta kojem se ostvaruje pristup preko korisničkog grafičkog interfejsa i koji sadrži dokumenta koja su često povezana hipervezom - takođe se naziva World Wide Web.
Web browser history	Evidencija o pretraživanju weba	Dnevnik web stranica koje su prethodno posjećivane, pohranjen lokalno na kompjuteru.
Webpage	Web stranica	Dokumenti kodirani standardizovanim opisnim jezikom, HTML-om.
Website	Websajt	Websajt je zbirka web stranica koje su međusobno povezane i vrlo često povezane s drugim websajtovima. Websajt aktivira (domaćin mu je) na web serveru sajt vlasnika, provajdera ili pružatelja Internet usluga (ISP).
Windows Registry	Registar Windowsa	Centralna hijerarhijski struktuirana baza podataka koja se koristi u OS Windows za pohranjivanje informacija koje su neophodne za konfigurisanje sistema za jednog ili više korisnika, aplikacija i hardverskih uređaja. Registar sadrži informacije na koje se Windows stalno poziva tokom rada, kao što su profili za svakog korisnika, aplikacije instalirane na kompjuteru i vrste dokumenata koje svako može napraviti, parametri karakteristika svih ikonica za fascikle (foldere) i aplikacije, hardveri koji postoje na sistemu i priključci (port) koji se koriste.

Wipe	Pobrisati	Potpuno izbrisati podatke iz memorije i sa tvrdog diska.
Write blocker	Blokada pisanja	Elektronski uređaj koji omogućava istražitelju pristup i čitanje podataka na tvrdom disku kompjutera ili drugih uređaja bez mijenjanja podataka, pa se prema tome dokazi čuvaju u njihovom prvobitnom stanju.
WWW	WWW	World Wide Web. Cijela konstelacija resursa do koje se može doći korištenjem Gophera, FTP-a, HTTP-a, Telneta, USENET-a, WAIS-a i nekih drugih softvera.

KORACI KOJE JE POTREBNO PREDUZETI PRILIKOM IZUZIMANJA UREĐAJA KOJI SADRŽE DIGITALNE DOKAZE

Prilikom izuzimanja računara, zavisno da li je uključen ili isključen, potrebno je slijediti sljedeće korake:

Ako je kompjuter uključen:

- Fotografišite ekran,
- Kreirajte forenzičku kopiju RAM memorije,
- Provjerite aktivne pograme i šta se trenutno dešava,
- Izuzmite sadržaj elektronskog poštanskog sandučeta,
- Provjerite da li ima CD/DVD medija u uređaju,
- Prekinuti vezu s mrežom,
- Ako postoji kriptografska zaštita, kreirati logičke forenzičke kopije diskova,
- Izvucite kabl iz računara,
- Zaplijenite i upakujte sve dokaze.

Ako je kompjuter isključen:

- Nemojte ga uključivati,
- Fotografišite ga,
- Dokumentujte da li je povezan na mrežu,
- Isključite i označite kablove,
- Provjerite dali ima CD/DVD medija u uređaju, ako ima izvadite koristeći spajalicu (provjerite da je struja isključena).

Obzirom da bi svako paljenje računara dovelo do izmjene određenih podataka,

čime bi se mogla dovesti u pitanje validnost pronađenih dokaza, kako bi se onemogučilo slučajno ili namjerno paljenje, preporučljivo je koristiti odgovarajuće etikete za utičnice i kablove, kao na slici.

Predmete kao što su USB stikovi, eskterni hard diskovi i sl. nakon gašenja računara iskopčati i posebno zapakovati, nikako lijepiti za računar kao sastavni dio računara.

Prilikom izuzimanja mobilnih telefona, potrebno je slijediti korake:

3. **Za mobilne telefone koji su aktivni sa SIM karticom**:

- Ukucati ***#06#,** broj koji se pojavi na displeju je IMEI broj i unijeti u zapisnik,
- Unijeti u zapisnik na kojoj mreži telekom operatera je aktivan telefon,
- Telefon ugasiti a zatim upaliti,

- Ukoliko traži **PIN** kod, tražiti od lica PIN kod i unijeti u zapisnik,
- Ukoliko traži **SECURITY** kod, tražiti od lica SECURITY kod i unijeti u zapisnik,
- Telefon ugasiti ili ne, zavisi od toga da li je bitno vidjeti ko je zvao u toku ili nakon pretresa obzirom da telekom operateri nisu bilježili propuštene pozive. Međutim treba imati na umu da mobilni telefoni sa operativnim sistemom Android imaju opciju trajnog brisanja podataka koja se aktivira putem interneta. (Ne vaditi bateriju iz razloga što se gubi lista poziva)

Ukoliko lice ne želi dati PIN ili Security kod, upozoriti ga da Zakonom o krivičnom postupku može biti kažnjen novčanom kaznom do 50.000 KM ili kaznom zatvora do 90 dana.

4. **Za mobilne telefone koji nisu aktivni ili nemaju SIM karticu**:

- Pokušati upaliti mobilni telefon i ponoviti korake iz tačke 1;
- Ukoliko se telefon ne može upaliti ili nema SIM kartice, izvaditi bateriju i unijeti u zapisnik IMEI broj.

Mobilne telefone, SIM kartice, memorijske kartice, punjače za mobitel i certifikate za SIM kartice, pakovati odvojeno od ostalih predmeta koji se oduzimaju, a koji neće biti predmet vještačenja digitalnih dokaza.

NACRTI - PRIMJERI

[upisati naziv policijskog organa – zaglavlje dokumenta]

Broj: [upisati broj]
Datum: [upisati datum]

[upisati naziv suda – primaoca zahtjeva]
[upisati mjesto/adresu primaoca]
Sudiji za predhodni postupak

Na osnovu člana 53. stav 2. ZKP BiH/člana 67. stav 2. ZKP FBiH/člana 117. stav 2. ZKP RS/ člana 53. stav 2. ZKP BD [naredba za pretresanje], a u vezi člana 51. stav 1. i člana 52. ZKP BiH/ člana 65. stav 1. i člana 66. ZKP FBiH/člana 115. stav 1. i člana 116. ZKP RS/člana 51. stav 1. i člana 52. ZKP BD [pretresanje stana, ostalih prostorija i pokretnih stvari – pretresanje osobe/ lica], ovlaštene službene osobe [upisati naziv policijskog organa], [ime i prezime policijskog službenika i čin] i [ime i prezime policijskog službenika i čin], po dobijanju odobrenja od [ime i prezime tužioca i naziv nadležnog tužilaštva], u skladu sa članom 55. ZKP BiH/članom 69. ZKP FBiH/članom 119. ZKP RS/članom 55. ZKP BD [sadržaj zahtjeva za izdavanje naredbe za pretresanje], podnose:

Z A H T J E V
za izdavanje naredbe za pretresanje
[prostorija, osoba, predmeta, pmv]

1. Radi pronalaženja, počinitelja, saučesnika, tragova krivičnog djela i predmeta važnih za krivični postupak, predlažem da se izvrši pretresanje, i to:
   1.1. [ime i prezime osobe/lica]
   i/ili
   1.2. [stana/kuće i pratećih objekata – navesti adresu]
   i/ili
   1.3. [pmv]

2. U navedenim pretresima predmet pronalaženja je informatička oprema (kompjuteri, externi hard-diskovi, usb memory stickovi, CD-nosači memorije), kao i svi ostali uređaji koji mogu poslužiti za prijenos podataka u digitalnom obliku, mobilni telefonski aparati, GSM SIM kartice, novac, telefonski certifikati, notesi, bilješke, evidencije, bankovne kartice, oprema za krivotvorenje bankovnih kartica, kao i drugi predmeti koji potiču iz krivičnog djela.

3. Pretres gore navedenih objekata/stvari/osoba/pokretnih stvari/pmv, kao i oduzimanje eventualnih predmeta dokaza, izvršiće ovlaštene službene osobe [navesti].

4. Činjenice koje ukazuju na vjerovatnost da će se pronaći tragovi krivičnog djela i predmeti važni za krivični postupak: [navesti]

Predlažemo da se navedeni pretres izvrši u bilo koje vrijeme i bez prethodne predaje Naredbe, iz razloga:

- što postoji mogućnost da se traženi predmeti lako i brzo unište primjenom metoda anti-forenzičke zaštite, kao što je enkripcija podataka, EMI (elektro-magnetni impuls) usmjeren ka bilo kojem dokazu u elektronskom obliku i sl.

Nadalje, predlažemo da se Naredba za pretresanje i privremeno oduzimanje predmeta izvrši najkasnije 15 dana od dana izdavanja Naredbe za pretresanje, nakon čega će se bez odlaganja vratiti Sudu.

Prilog:
[navesti]

Zahtjev odobrio [ime i prezime ovlaštenog policijskog službenika i čin]

[upisati naziv tužilaštva – zaglavlje dokumenta]

Broj: [upisati broj] [upisati oznaku povjerljivosti i hitnosti]
Datum: [upisati datum]

[upisati naziv suda – primaoca prijedloga]
[upisati mjesto/adresu primaoca]
Sudiji za predhodni postupak

Na broj: [navesti]

Na osnovu člana 35. stav 1. i 2. tačke a), b) i e), članova 51., 52. i 55. i člana 65. stav 1., 2., 3. i 4. ZKP BiH/člana 45. stav 1. i 2. tačke a), b) i e), članova 65., 66. i 69. i člana 79. stav 1., 2., 3. i 4. ZKP FBiH/ člana 43. stav 1. i 2. tačke a), b) i d), članova 1115., 116. i 119. i člana 129. stav 1., 2., 3. i 4. ZKP RS/ člana 35. stav 1. i 2. tačke a), b) i e), članova 51., 52. i 55. i člana 65. stav 1., 2., 3. i 4. ZKP BD, tužilac [navesti naziv tužilaštva], p o d n o s i

P R I J E D L O G
za izdavanje naredbe za pretres stana, ostalih prostorija i pokretnih stvari, pretres lica i privremeno oduzimanje predmeta

I

Radi pribavljanja dokaza u vezi osnova sumnje da su [ime i prezime] i [ime i prezime] počinili krivično djelo [navesti] iz člana ____. KZ-a BiH/FBiH/RS/BD, potrebno je izvršiti pretres stana, ostalih prostorija i pokretnih stvari, pretres lica i privremeno oduzimanje predmeta koje koriste osumnjičeni.

1. lica [ime i prezime], sin [ime], rođen dana [datum] u [mjesto], JMBG: [navesti], sa prijavljenom adresom prebivališta u [mjesto] u ul. [navesti] br. [navesti],
    a) stana koji koristi [ime i prezime] u ul. [navesti] br. [navesti], stan br. [navesti] u naselju [navesti] u [mjesto],

2. lica [ime i prezime], sin [ime], rođen dana [datum] u [mjesto], JMBG: [navesti], sa prijavljenom adresom prebivališta u [mjesto] u ul. [navesti] br. [navesti],
    a) porodične kuće i pomoćnog objekta ul ul. [navesti] br. [navesti], u naselju [navesti] u [mjesto], gdje je prijavljen i gdje prebiva [ime i prezime],
    b) motornog vozila [navesti] koji koristi [ime i prezime].

II

Pretres lica i objekata iz tačke I prijedloga treba izvršiti radi pronalaska i privremenog oduzimanja predmeta koji mogu poslužiti kao dokaz u krivičnom postupku, i to: [navesti predmete oduzimanja] [npr. informatička oprema (kompjuteri, externi hard-diskovi, usb memory stickovi, CD-nosači memorije), kao i svi ostali uređaji koji mogu poslužiti za prijenos podataka u digitalnom obliku, mobilni telefonski aparati, GSM SIM kartice, novac, telefonski certifikati, notesi, bilješke, evidencije, bankovne kartice, oprema za krivotvorenje bankovnih kartica, kao i drugi predmeti koji potiču iz krivičnog djela i mogu poslužiti kao dokaz u krivičnom postupku].

III

Predlažemo da [navesti naziv suda] izvršenje ove naredbe povjeri [naziv policijskog organa / agencije] i [naziv policijskog organa / agencije], uz pomoć – asistenciju ovlaštenih službenih lica [naziv policijskog organa / agencije].

IV

Predlažemo da se pretres i oduzimanje predmeta izvrši u roku od [navesti] dana od dana izdavanja Naredbe Suda i to u vremenskom periodu od 6 do 21 časa / u bilo koje vrijeme, jer postoji osnovana sumnja da pretresanje neće moći biti izvršeno u vremenskom periodu od 6 do 21 sati, iz razloga što postoji mogućnost da se traženi predmeti lako i brzo unište primjenom metoda anti-forenzičke zaštite, kao što je enkripcija podataka, EMI (elektro-magnetni impuls) usmjeren ka bilo kojem dokazu u elektronskom obliku i sl.

V

S obzirom da se ovim Prijedlogom traži pretresanje više fizičkih lica, stanova, ostalih prostorija i pokretnih stvari, te privremena oduzimanja predmeta, potrebno je da [navesti naziv suda] donese više primjeraka Naredbi radi uspješnog okončanja istrage.

O b r a z l o ž e n j e

[obrazložiti]

[ime i prezime tužioca]

Prilog:
[prijedlog/izvještaj policijskog organa/agencije]

[upisati naziv policijskog organa – zaglavlje dokumenta]

Broj: [upisati broj]
Datum: [upisati datum]

[upisati naziv suda – primaoca zahtjeva]
[upisati mjesto/adresu primaoca]
Sudiji za predhodni postupak

Na osnovu člana 95. ZKP BiH/člana 109. ZKP FBiH/člana 160. ZKP RS/člana 95. ZKP BD [određivanje vještačenja], ovlaštene službene osobe [upisati naziv policijskog organa], [ime i prezime policijskog službenika i čin] i [ime i prezime policijskog službenika i čin], po dobijanju odobrenja od [ime i prezime tužioca i naziv nadležnog tužilaštva], podnose:

Z A H T J E V
za izdavanje naredbe za vještačenje računara i računarske opreme
u predmetu [navesti]

1. Radi utvrđivanja sadržaja privremeno oduzetih računara i računarske opreme, odnosno prikupljanja dokaza u predmetu: [navesti], vezano za postojanje osnovane sumnje da je izvršeno krivično djelo [navesti] iz člana ____. KZ-a BiH/FBiH/RS/BD u sticaju sa krivičnim djelom [navesti] iz člana ____. KZ-a BiH/FBiH/RS/BD, predlažemo da se zatraži stručno mišljenje od vještaka ili osobe koja raspolaže stručnim znanjem, odnosno da se istim, n a r e d i

   dostavljanje stručnog mišljenja u pogledu sadržaja privremeno oduzetih računara i računarske opreme i to:
   [navesti]

vezano za tragove izvršenja krivičnog djela [navesti] iz člana ____. KZ-a BiH/FBiH/RS/BD, te krivičnog djela [navesti] iz člana ____. KZ-a BiH/FBiH/RS/BD, ili nekog drugog krivičnog djela, a sadržani su na navedenim privremeno oduzetim predmetima.

2. Svrha preduzimanja ove službene radnje jeste prikupljanja dodatnih dokaza u predmetu: [navesti], a po Nalogu za provođenje istražnih radnji [navesti], broj: [navesti].

3. Stručno mišljenje potrebno je dostaviti u najkraćem roku [upisati naziv tužilaštva], te jedan primjerak istog i policijskim službenicima [upisati naziv policijskog organa], u elektronskom i pisanom obliku.

4. Činjenice koje ukazuju na vjerovatnost da će se pronaći tragovi krivičnog djela i predmeti važni za krivični postupak:
   [navesti]

5. Predlažemo da se Naredba obezbjedi ODMAH, te da se vještaku ili stručnom licu naredi da Stručno mišljenje, dostavi u najkraćem roku [upisati naziv tužilaštva], te jedan primjerak istog i policijskim službenicima [upisati naziv policijskog organa], u elektronskom i pisanom obliku.

Napomena: Gore navedeni predmeti se nalaze u službenim prostorijama [navesti] i isti će biti predati licu koje Sud odredi Naredbom za vještačenje.

Prilog:
Nalog za provođenje istražnih radnji, broj: [navesti]

Zahtjev odobrio tužilac:

[ime i prezime tužioca] [ime i prezime ovlaštenog policijskog rukovodioca]

[upisati naziv tužilaštva – zaglavlje dokumenta]

Broj: [upisati broj]
Datum: [upisati datum]

[upisati naziv primaoca naredbe]
[upisati mjesto/adresu primaoca]

Na osnovu člana 35. stav 2. tačka e) ZKP BiH/člana 45. stav 2. tačka e) ZKP FBiH/člana 43. stav 2. tačka d) ZKP RS/člana 35. stav 2. tačka e) ZKP BD [prava i dužnosti tužioca], člana 96., 97. i 99. ZKP BiH/člana 110., 111. i 113. ZKP FBiH/člana 161., 162. i 164. ZKP RS/ člana 96., 97. i 99. ZKP BD [naredba o vještačenju, dužnosti vještaka i postupak vještačenja] u postupku istrage protiv osumnjičenih [navesti] i dr., zbog krivičnog djela [navesti] iz člana ____. KZ-a BiH/FBiH/RS/BD, a u vezi sa krivičnim djelom [navesti] iz člana ____. KZ-a BiH/FBiH/RS/BD, tužilac donosi

NAREDBU ZA VJEŠTAČENJE

I

Ima se izvršiti informatičko – forenzičko vještačenje.

II

Vještačenje se povjerava [navesti kome se povjerava vještačenje].

III

Predmet vještačenja su privremeno oduzeti predmeti po Potvrdama i to:
Potvrda o privremenom oduzimanju predmeta [navesti izdavaoca potvrde], broj: [navesti] od [datum] na ime [navesti]:

1. [opis računara: marka, serijski broj], označeno kao trag broj: [navesti] (redni broj Potvrde: [navesti]),
2. [opis računara: marka, serijski broj], označeno kao trag broj: [navesti] (redni broj Potvrde: [navesti]),
3. [opis računara: marka, serijski broj], označeno kao trag broj: [navesti] (redni broj Potvrde: [navesti]).

IV

Informatičko – forenzičkim vještačenjem pobrojanih predmeta potrebno je:

1. Sačiniti kopiju tj. kreirati zamrznutu sliku (mirror image) svih hard diskova, optičkih medija i USB memorijskih stikova.

2. Izdvojiti sve podatke u datotekama – fajlovima koji mogu poslužiti kao dokaz u ovom krivičnom postupku i to:
   - postojeće datoteke – fajlove,
   - brisane datoteke – fajlove,
   - oštećene datoteke – fajlove,
   - e-mail adrese, kontaktirane i nekontaktirane,
   - primljene i poslane postojeće e-mail poruke,
   - primljene i poslane brisane e-mail poruke.

3. Izdvojiti:
   - videozapise,
   - mrežne konfiguracije računara – klijenta,
   - instalirane programe, na koji način se uspostavljala komunikacija između klijent – računara i servera na kojima se nalaze baze podataka i tragovi istih,
   - druge vrste komunikacija i tragove istih,
   - istorija pristupa web – stranicama putem Interneta i njihov sadržaj sa posebnim akcentom na [navesti] i [navesti],
   - identifikacije e-mail adresa i eventualne pristupne šifre koje su korištene za pristup istim, te tragove sadržaja e-mail poruka,
   - druge dokaze koji se mogu dovesti u vezu sa predmetnim krivičnim djelima.

4. Iz kategorije specifičnih računara:
   - mrežne konfiguracije računara – klijenta,
   - instalirane programe, na koji način se uspostavljala komunikacija između klijent – računara i servera na kojima se nalaze baze podataka i tragovi istih,
   - druge vrste komunikacije i tragove iste,
   - istorija pristupa web – stranicama putem Interneta i njihov sadržaj sa posebnim akcentom na [navesti] i [navesti],
   - identifikacija e-mail adresa i eventualno pristupnih šifri koje su korištene za pristup istim, te tragovi sadržaja e-mail poruka,
   - evidencije i dokumenti vezano za poslovanje preduzeća [navesti],
   - drugi dokazi koji se mogu dovesti u vezu sa predmetnim krivičnim djelima.

5. Iz kategorije [navesti]:
   - videozapise,
   - mrežne konfiguracije računara – klijenta,
   - instalirane programe, na koji način se uspostavljala komunikacija između klijent – računara i servera na kojima se nalaze baze podataka i tragovi istih,
   - druge vrste komunikacije i tragove iste,
   - istorija pristupa web – stranicama putem Interneta i njihov sadržaj sa posebnim akcentom na [navesti] i [navesti],
   - identifikacija e-mail adresa i eventualno pristupnih šifri koje su korištene za pristup istim, te tragovi sadržaja e-mail poruka,
   - drugi dokazi koji se mogu dovesti u vezu sa predmetnim krivičnim djelima.

6. Iz kategorije [navesti]:
   - mrežne konfiguracije,
   - instalirane programe,
   - baze podataka i sadržaj istih,
   - log – fajlove administracije servera,
   - video – zapise,
   - evidencije i dokumenti vezano za poslovanje preduzeća [navesti],
   - druge vrste evidencija i dokumenata,
   - drugi dokazi koji se mogu dovesti u vezu sa predmetnim krivičnim djelima.

7. Iz kategorije memorijskih stikova, memorijskih kartica, kompakt diskova i dr.:
   - očitati sadržaj istih i izdvojiti sadržaj koji se može dovesti u vezu sa krivičnim djelima koja se stavljaju na teret korisnicima istih i dr.

V

Vještak će konstatovati i sve druge relevantne podatke do kojih dođe tokom vještačenja, a koje vještak smatra potrebnim za pravednu i objektivnu analizu.

VI

Nakon izvršenog vještačenja, vještak je dužan sačiniti Izvještaj koji će sadržavati sljedeće:
1. Dokaze koje je pregledao,
2. Obavljene radnje vještačenja,
3. Stručnu literaturu i druga sredstva koja je vještak koristio u svrhu vještačenja,
4. Druge relevantne podatke koje vještak smatra potrebnim,
5. Obrazloženje kako je vještak došao do određenog mišljenja.

VII

Vještačenje će se izvršiti u najkraćem vremenu koje je neophodno za nevedenu vrstu vještačenja, a vodeći računa o razlozima hitnosti.

VIII

Izvještaj o vještačenju vještak će dostaviti [navesti naziv tužilaštva] u pismenoj formi u 3 primjerka.

IX

Na osnovu člana 99. ZKP BiH/člana 113. ZKP FBiH/člana 164. ZKP RS/ člana 99. ZKP BD [postupak vještačenja] vještak je dužan da predmet vještačenja pažljivo razmotri, da tačno navede sve što zapazi i utvrdi, kao i da svoje mišljenje iznese nepristrasno i u skladu s pravilima nauke i vještine.

Vještak se upozorava da lažno vještačenje predstavlja krivično djelo.

X

U svrhu vještačenja vještaku se predaje Naredba o sprovođenju istrage, broj: [navesti] od [datum] i predmeti vještačenja pobrojani u tački III ove Naredbe.

XI

Vještačenje će se obaviti u prostorijama [navesti].

NAPOMENA: Po obavljenom vještačenju [navesti] će obezbijediti skladištenje gore navedenih predmeta (zbog osjetljivosti premještanja predmeta) do okončanja krivičnog postupka u ovom predmetu, odnosno do nove naredbe ovog Tužilaštva.

U slučaju potrebe i nejasnoća, kontaktirati postupajućeg tužioca [navesti] na broj telefona [navesti].

[ime i prezime tužioca]

[upisati naziv policijskog organa – zaglavlje dokumenta]

Broj: [upisati broj]
Datum: [upisati datum]

[upisati naziv suda – primaoca zahtjeva]
[upisati mjesto/adresu primaoca]
Sudiji za predhodni postupak

Na osnovu člana 72a. ZKP BiH/člana 86a. ZKP FBiH/člana 137. ZKP RS/člana 72a. ZKP BD [naredba operateru telekomunikacija], ovlaštena službena osoba [upisati naziv policijskog organa], [ime i prezime policijskog službenika i čin], po dobijanju odobrenja od [ime i prezime tužioca i naziv nadležnog tužilaštva], podnosi:

Z A H T J E V
za izdavanje naredbe operateru telekomunikacija

1. Radi identifikacije i pronalaženja počinioca krivičnog djela, predlažemo da se pravnom licu [naziv i adresa telekom operatera], kao operateru telekomunikacija naloži dostava podataka o NN licima, koji su koristili sljedeće IP adrese za pristup internetu, kao i svih ostalih podataka koji mogu poslužiti identifikaciji gore navedenih NN lica (ovjerene kopije ugovora o korištenju internet usluga, kopije računa za vrijeme korištenja predmetnih adresa sa navedenom adresom njihove dostave):

   Datum i vrijeme: [navesti]
   IP: [navesti]

2. Predlažemo da se Naredba uruči odgovornom licu u [naziv telekom operatera], odmah po njenom izdavanju, te da se podaci od strane ovog operatera telekomunikacija dostave u najkraćem roku u pisanom i elektronskom obliku, policijskim službenicima [upisati naziv policijskog organa], pozivom na broj i datum ovog akta.

Napomena:
[navesti]

Prilog:
[navesti]

Zahtjev odobrio tužilac:

[ime i prezime tužioca] [ime i prezime ovlaštenog policijskog rukovodioca]

Priručnik o pretresanju kompjuterskih sistema, uređaja za pohranjivanje

kompjuterskih i elektronskih podataka i mobilnih telefonskih aparata

PROJEKAT

Jačanje tužilačkih kapaciteta u sistemu krivičnog pravosuđa