



**UNIVERZITET SINGIDUNUM
SAVREMENE INFORMACIONE TEHNOLOGIJE**

MASTER STUDIJE

Master rad:

**Značaj proaktivne forenzike za
bezbednost informacionih sistema**

MENTOR:
Docent dr. Gojko Grubor

KANDIDAT:
Andrijana Đoković

Beograd, mart 2013.

Sažetak: Svaki događaj koji se desio u računarskom sistemu ili računarskoj mreži bi trebalo evidentirati i sačuvati informacije relevantne za specifičan događaj. Log datoteka predstavlja zapis događaja u računarskom sistemu ili mreži. Prvobitno, log datoteke su korišćene za rešavanje problema računarskog sistema, ali danas log datoteke imaju mnogo više funkcija. Koriste se za optimizovanje sistema i mreža, praćenje ponašanja korisnika i generisanje podataka korisnih za istraživanje aktivnosti malicioznih programa. Samim tim log datoteke dobijaju na značaju sa aspekta digitalne forenzike. U prvom delu istraživačkog projekta izvršen je teorijski pregled osnovnih podataka o log datotekama i njihovoj analizi. U drugom delu je akcenat stavljen na analizu log datoteka i beleženi su neki događaji i analiziran je njihov zapis. Predočeno je šta sve može da se nađe kao zapis u ovoj datoteci kao i na koji način mogu određeni zapisi da se pronalaze i tumače. Zaključeno je šta log datoteka znači za digitalnu forenziku i na koji način ona može da se iskoristi. Sa Log fajlovim treba raditi pažljivo, jer je Log osetljiv fajl i lako se mogu menjati podaci i u njih hakeri lako ulaze.

Ključne reči: Log datoteka, analiza log datoteke, forenzički značaj analize log datoteke.

Summary: Each event that took place in a computer system or computer network should be recorded and information relevant to a specific event should be preserved. The log file is a record of events in a computer system or a network. Initially, the log files are used for troubleshooting a computer system, but now the log files have many more functions. They are used to optimize the system and network, for monitoring user behavior and to generate data useful for investigating activities of malicious programs. Therefore the log files are becoming more important in terms of digital forensics. In the first part of a research project carried out a theoretical overview of the basic information about the log files and analysis. At the second part, the focus was on analysis of the log files and some events were recorded and their record was analyzed. It was demonstrated what can be found as a record in this file and how can a certain records be found and interpreted. It is presented what log file means for digital forensics and how it can be used. Log files should be handled with care because Log file is sensitive and the data can be easily altered and hackers can easily access.

Keywords: log file, log file analysis, forensic significance analysis of log files.

Sadržaj:

1	Metodologija istraživačkog projekta.....	6
1.1.	Uvodne napomene i obrazloženje rada	6
1.2.	Predmet istraživanja.....	7
1.3.	Ciljevi i zadaci istraživanja.....	8
1.4.	Hipotetički okvir istraživačkog rada.....	8
1.5.	Metode, tehnike i tok istraživačkog procesa.....	10
2.	Maliciozni napad na Informacione sisteme	12
2.1.	Uvod.....	12
2.3.	Evolucija malicioznih pretnji.....	19
2.4.	Mehanizmi prostiranja.....	20
2.5.	Tehnike samoodržavanja.....	21
2.6.	Identifikacija i odbrana od malicioznih napada	22
2.7.	Tehnike za ublažavanje posledica malicioznih napada.....	24
2.8.	Tehnike mrežnih nivoa	27
2.9.	Prevođenje adrese iz mreže (Network Address Translation-NAT)	31
3.	Istraga Wireless napada	34
3.1.	Tehnologije Wireless mreža	34
3.2.	Napad na bežičnu mrežu	37
3.2.	Mrežna forenzika u wireless okruženju.....	40
4.	Digitalni Forenzički dokazi i alati.....	43
4.1.	Digitalni dokaz	44
4.2.	Prihvatljivost digitalnih dokaza u sudnici	47
4.3.	Alati za digitalnu forenzičku istragu.....	48
4.4.	Metodologije za testiranje alata za digitalnu forenziku.....	50

5. Značaj proaktivne forenzike za bezbednost Informacionih sistema.....	55
5.1. Teorijske osnove	55
5.2. Slojevit pristup kod detekcije spoljašnje pretnje i proaktivne forenzike.....	58
5.3. Mrežna forenzika i istraga Log fajlova	60
5.3.1. Analiza mrežnih podataka.....	60
5.4. Log fajlovi.....	61
5.5. Konfigurisanje Log datoteka	63
5.6. Potraga za dokazima	63
5.7. End-to-End forenzička istraga	64
5.8. Log fajlovi kao dokazi.....	65
5.9. Ispitivanje upada i bezbednost događaja.....	66
5.10. Prednost razumevanja Log datoteka	67
5.11. Tačnost log fajlova.....	68
5.12. Pregled Web Log-a	70
5.13. Istraga FTP Servera.....	73
5.14. Istraga Apache logova	74
5.15. Istraživanje statičke i dinamičke IP adrese	75
5.16. Checklist za Web bezbednost.....	76
5.17. Alati za istragu Web napada	78
6. Studije slučajeva.....	84
6.1. Studija slučaja 1: Primena istraživanja podataka u digitalnoj forenzici...90	
6.1.1 Istraga autora e-mejla (<i>Mining E-mail Authorship</i>)	
6.1.2 Autorska kategorizacija	
6.1.3 Mašinska podrška za vektorsku klasifikaciju	
6.1.4 E-mail dokumenti, atributi i eksperimentalne metodologije	
6.2. Studija slučaja 2: Analiza Windows Log	
datoteke.....	87
Zaključak.....	106

1 Metodologija istraživačkog projekta

1.1. Uvodne napomene i obrazloženje rada

Od kada se desila pojava računarskih mreža, a samim tim i njen brz napredak i umrežavanje u sistem globalne mreže zvane Internet, sa tim dolazi i do zloupotrebe i narušavanja njene funkcionalnosti u komunikaciji i prenosu informacija. Sve je veći broj napada sa Interneta, slanjem malware-a od strane hakera, i drugih kompjuterskih kriminalaca. Računarske mreže Internet tipa daju brojne prednosti i omogućavaju veću efikasnost rada i smanjenje troškova, ali imaju i svoje mane, jer predstavljaju kritičnu tačku bezbednosti. Naglo je porastao broj napada na računarske mreže, pa se samim tim i povećao sam finansijski gubitak usled tih napada. Pored finansijske dobiti, postoje i razni drugi motive za napade, kao što je krađa poverljivih podataka, ili njihovo oštećenje, kao i oštećenje samih aplikacija i sistema. Sve ovo spada u kompjuterski kriminal, i daljim otkrivanjem dokaza bavi se grana nauke- Digitalna forenzika. "Pod kompjuterskim kriminalom se podrazumeva krivično delo prema krivičnom zakonu nacionalne države. U kompjuterskom kriminalu, računari se koriste kao alat za predmet napada, krađe, izmene i uništenja podataka."¹

Cilj same istrage ovakvog vida kriminala, je sličan klasičnoj istrazi, a to je dobijanje neoborivih i čvrstih dokaza za pravosudne organe, koji će osumnjičenog ili osuditi ili osloboditi na osnovu njih. "Digitalna forenzika je relativno malada nauka, koja se vrtoglavom brzinom razvija, jer radi sa osetljivim podacima koji su i pritom lako promenljivi. Ova nauka obezbeđuje primenu pri sakupljanju, čuvanju, identifikaciji, analizi, dokumentovanju i prezentaciji dokaza, koji će poslužiti u rekonstrukciji događaja nastalog krivičnog dela."² Za pravosudnu prihvatljivost digitalnih dokaza osnovne prepreke su osetljivost i promenljivost digitalnih podataka i inherentna posrednost digitalnih dokaza. Neposredni dokaz u slučaju kompjuterskog kriminala je gotovo nemoguće obezbediti, ali je moguće izgraditi neoboriv

¹ Milosavljević M., Grubor G., *Digitalna forenzika, Univerzitet Singidunum, Beograd 2008, str 12*

² Milosavljević M., Grubor G., *Digitalna forenzika, Univerzitet Singidunum, Beograd 2008, str 14*

digitalni dokaz bez “pukotina” koji se dobija na osnovu niza posrednih digitalnih dokaza. U zvaničnoj istrazi kompjuterskog kriminala, u toku prikupljanja, analize i prezentacije digitalnih dokaza, moraju se imati u vidu određeni principi. Praksa je pokazala da je najbolji način formiranje tima od tri profesionalca i to: zvaničnog organa istrage, tužioca i eksperta u oblasti Informaciono-komunikacionog sistema. Često se dešava da ekspert iz ove oblasti bude i veštak na sudu. Današnje usmeravanje na serversko okruženje, centralizovano nadgledanje kao i druge “beneficije” ponudice korisnicima jednostavniji, sigurniji i brži rad, ali pod uslovom da računar koriste u legalne svrhe.

Spoljašnja pretnja je pretnja bezbednosti računara kao rezultat zloupotrebe sistema od strane pojedinca ili organizacije. Sama proaktivna digitalna forenzika podrazumeva smanjenje štete izazvane napadom kroz proaktivnu pripremu okruženja, pre faze incidenta, a u cilju postizanja spremnosti organizacije za digitalnu forenzičku istragu. Osnovni rezultat ovakvog pristupa jeste brzo reagovanje na incident, ublažavanje njegovih posledica i podizanje kvaliteta zaključaka forenzičke analize [izolovanje faze incidenta proaktivne digitalne forenzike korišćenjem adaptivnog virtuelnog okruženja]. Prikupljanje podataka sa računarskih sistema, na kojima su identifikovani bezbednosni incidenti, je kompleksan zadatak čije pravilno izvođenje može uticati na uspeh predstojećeg forenzičkog procesa. Biti proaktivan definiše se kao kontrolisanje situacije pre nego što se ona dogodi. Savremeni proaktivni sistema za detekciju i sprečavanje upada u sistema obezbeđuju inteligentnu tehniku za hvatanje napadača poznatu kao ćup medra (honeypot). Ove tehnike omogućavaju hvatanje hakera u napadnutom sistema, nakon utvrđivanja njegovog prisustva.

U ovom radu obrađena je tema značaja proaktivne forenzike za bezbednost informacionih sistema. Dati su primeri u pristupu digitalnog forenzičara na log fajlove. Objašnjene su određene vrste spoljnih napada, analiza mrežnih podataka, određene istrage na serverima, kao i sama Web bezbednost.

1.2. Predmet istraživanja

U ovom radu, predmet istraživanja je značaj proaktivne forenzike na bezbednost informacionih sistema, uloga *Log* fajlova koji zapisuju događaje kao što su validni i nevalidni

pokušaji prijavljivanja i korišćenja resursa. Svaki kompjuter u organizaciji ima odvojeni sigurnosni *Log* koji zapisuje događaje koji su se desili na lokalnom kompjuteru. Na samim Domen kontrolerima se nalazi sigurnosni log u kome se nalaze informacije vezane za aktivne direktorijume. U ovom radu će biti i objašnjen značaj ovih fajlova, jer su oni izvor informacija i mogu biti različitog tipa kao što su sistemski logovi, aplikacioni logovi, mrežni logovi i ovo su neki od najčešćih logova. Biće objašnjeni i određeni pokušaji napada na sisteme, kao i načini odbrane od istih.

U ovom radu je korišćen program **Splunk** za obradu *Log* fajlova. U prvom delu rada izvršen je teorijski pregled i upoznavanje sa *log* datotekama i njihova analiza. U daljem radu je izvršena analiza log datoteka. Beležena su događanja i analiziran je njihova zapis. Predstavljeno je šta sve može da se nađe kao zapis u datoteci i na koji način mogu određeni zapisi da se pronalaze i tumače.

1.3. Ciljevi i zadaci istraživanja

Glavni cilj ovog rada je da se prikaže značaj proaktivne forenzike u zaštiti informacione imovine.

Poseban cilj ovog rada je da se istakne značaj *Log* fajlova (dnevnika rada) za otkrivanje stvarnih uzroka povrede politike zaštite Informacionih sistema, kao i same uloga proaktivne forenzike u otkrivanju načina i samih počinioaca krivičnih dela.

1.4. Hipotetički okvir istraživačkog rada

S obzirom na obim i dubinu ovog rada, postavljene su četiri opšte i četiri radne hipoteze.

Opšta hipoteza 1: Za forenzičku analizu napada na sisteme i mreže potrebno je dobro poznavanje same mreže i sistema, što virtuelnog, što pravog, jer ono nudi velike mogućnosti

korišćenja koje je pozitivno, ako se pravilno koriste sva posešavanja, ali takođe može i izazvati velike posledice, ako administrator ne vodi računa i ne bude detaljno obučen da prepozna napade. Sve ovo može biti pogubno za podatke, ali i same sisteme.

Radna hipoteza 1.1: Od posebnog značaja je pristup digitalnih forenzičara samim sistemima, kako bi svi podaci ostali sačuvani. Pristupom na servere, sisteme i ostale mrežne uređaje, mogu se prikupiti značajne informacije vezane za dokaze o nekom krivičnom delu. Sa svim prikupljenim dokazima kreira se slučaj događaja koji mora imati čvrste dokaze koji će potom biti predstavljeni pred sudom ili direktorima kompanija. U zavisnosti o kojem incidentu je reč, istragu mogu pokrenuti javna bezbednost koju predstavlja tužilaštvo, policija, bezbednosne agencije, vojska ili korporacijska istraga koju predstavlja menadžment same kompanije.

Opšta hipoteza 2: Digitalna forenzika ima određene metode kako otkriva napade i kako se bori sa raznim izazovima. Pre svega koje vrste alata mogu da se koriste i načini na koje ona dolazi do određenih dokaza, objašnjeni su u radu.

Radna hipoteza 2.1: Od posebnog značaja su način pristupa i dokazivanje krivičnog dela. Kao i alati kojima će se dokazi prezentovati na sudu, zato je od vitalnog značaja da istražitelj dobro poznaje način rada softvera.

Opšta hipoteza 3: Za borbu protiv zlonamernih korisnika koji pokušavaju da eksploatišu mrežu i sisteme, kako bi kompromitovali podatke, potrebno je poznavati softvere za zaštitu sistema, način uzimanja dokaza, ako je već došlo do napada, i postupak obrade donetih dokaza, radi prezentovanja na sudu i oslobađanja ili kažnjavanja optužene strane. Pri obradi podataka jako je bitno poznavati i pravne propise, kako bi podaci bili validni na sudu.

Opšta hipoteza 4: Kako postoje alati za dobijanje dokaza kod nekog slučaja, tako postoje i alati koji omogućavaju uklanjanje istih. Te alate koriste lica koja vrše ne zakonite aktivnosti, a mogu ih kreirati i programirati u zavisnosti kakve posledice za sobom žele da ostave. Lica koja koriste anti forenzičke alate isto tako koriste za napade maliciozne softvere.

Hipoteza 4.1: Od posebnog je značaja pristup mreži i mrežnim uređajima kao i samim sistemima u kojima se nalaze dragoceni podaci. Istraga počinje fizičkim pristupom lokalitetu,

potom prikupljanjem fizičkih dokaza i sve do trenutka kada digitalni forenzičar mora da izvrši istragu nad digitalnim podacima. Tada mora voditi računa o svim mogućim anti-forenzičkim manipulacijama od strane lica koje je izazvalo incident, kao ne bi bio doveden u zabludu.

1.5. Metode, tehnike i tok istraživačkog procesa

Metoda naučnog istraživanja je sistematski, kritični, kontrolisan i ponovljeni proces sticanja novih znanja, neophodnih za identifikovanje, određivanje i rešavanje naučnog problema. U naučnom istraživanju u ovom radu primenjeni su sledeći glavni principi:

- ▶ *Sistematičnost* – dobra uređenost istraživanja i obezbeđivanje prirodnog i logičkog sleda procesa,
- ▶ *Kontrolisanost* – sprovođenje istraživanja u što moguće boljim i nadziranim uslovima, kako bi se isključila alternativna rešenja i
- ▶ *Kritičnost* – sve važne tvrdnje o pojavama, procesima, odnosima i svojstvima moraju se ozbiljno, iskreno i strogo procenjivati, proveravati i obrazložiti.

Na osnovu podele naučnog istraživanja, a prema prirodi istraživanja postoje: teorijska i empirijska, a prema cilju istraživanja na: fundamentalna i primenjena. Prema funkciji istraživanja na: eksplorativna i usmerena na proveravanje hipoteza. U ovom radu biće primenjena fundamentalna i primenjena istraživanja. Fundamentalna istraživanja koriste se radi sticanja novih znanja o ovoj oblasti koja će biti obrađena, a primenjena radi sticanja novih znanja i rešavanja hipotezama postavljenih problema u ovoj naučnoj oblasti.

Na početku rada je objašnjen način funkcionisanja proaktivne digitalne forenzike, objašnjeni su problemi definisani kao kompjuterski incidenti i načini odbrane od njih. Takođe, definisan je cilj istraživanja. Kao verifikacija dela teorije napada i odbrane računarskog sistema ili mreže. Istraživanje je izvršeno kroz faze pristupa slučaju, uglavnom teorijskog i opisanog karaktera, prikupljanja i obrade podataka Log fajlova i izvođenje zaključka.

U ovom radu korišćene su različite metode istraživanja i verifikacije procesa digitalne forenzičke istrage da bi se došlo do određenih saznanja, otkrili i izložili naučni principi, koji se primenjuju u digitalnoj forenzici.

Od opštih naučnih metoda korišćene su statistička metoda, analitičko- deduktivana metoda. Takođe su korišćene osnovne, opšte metode društvenih nauka: pozitivistička metoda, metoda razumevanja, komparativna metoda i dijalektička metoda

Od posebnih naučnih metoda i tehnika primenjene su: analitičko – sintetička metoda, metoda apstrakcije i konkretizacije, metoda generalizacije, metoda klasifikacije, kao i metoda spoznaje i dijalektičkog jedinstva indukcije i dedukcije.

Tehnike istraživanja predstavljaju sistematsko i svrsishodno jedinstvo postupaka i instrumenata. Ovaj deo naučnog metoda podrazumeva: ocenu, sređivanje, obradu podataka i zaključivanje na osnovu njih. U tom smislu, postoji povezanost i međuzavisnost između metoda prikupljanja i obrade podataka, odnosno dokaznih materijala i informacija do kojih se došlo istraživanjem.

Tok istraživanja, kao prvi logičan korak uključuje prikupljanje potrebne literature o metodologiji naučnog istraživanja u dogotalnoj forenzičkoj istrazi sa težištem na sisteme i mreže i same softvere za odbranu od napada u svetu komunikacionih tehnologija, klasičnoj forenzičkoj istrazi, digitalnoj forenzilkoj istrazi. Zatim, istraživanje dobijenih podataka iz literature i materijala preuzetih iz raznih izvora, kroz faze otkrivanja, opisivanja i objašnjenja određenih faza digitalne forenzičke istrage u zavisnosti od situacije i primene. Rad je struktuiran u određene celine i svaka od njih konkretno objašnjava kroz koje faze prolazi sistem pri napadu, način odbrane od napada, kao i postupku prikupljanja podataka kada do incidenta dođe.

2. Maliciozni napadi na Informacione sisteme i njegove razvojne pretnje

Zlonamerni softveri (malware) kao što su crvi, virusi i trojanci su sada među najlakšim priznatim pretnjama kompjuterskih sistema. Zapravo malware je bio glavni problem za kompjutersku bezbednost i svakako je dominirao PC scenom, jer masovno korišćenje Interneta počelo je 90-ih godina. Međutim počeci problema sa malware-om datiraju znatno pre toga. Precizno poreklo Trojanskog konja je nepoznat, dok pojava pojava crva i virusa se može povezati sa najranijim razmišljanjima o napadima na računare. Postoji „Ćelijski automat“ (Fon Nijman, 1948). Ovi „automati“ su uveli određeni koncept i informacije mogu biti kodirane sa jednostavnim pravilima na takav način da je u stanju da samostalno ponavlja operacije i širi se u celom sistemu. Ovaj koncept je korišćen od strane Watso-a i Crick-a kada su pet godina kasnije objavili strukturu DNK molekula koji kodira informacije koje se koriste da ponove organske forme života. Nekih 30 godina kasnije prvi kompjuterski virus koristi termin za opisivanje replikacije koda unutar IT sistema.

Rasprava u ovom poglavlju ima za cilj da ispita nastanak i razvoj zlonamernih pretnji i način odbrane od njih. Sledeći odeljak predstavlja i neke osnovne terminologije i ističe na neki način nadmoć nekih od njih. Obraduje se i deo motiva zbog kojih se pišu i puštaju u opticaj malware, kao i koji je razlog za pretnju. Ispituju se i načini na koji je malware evoluirao, fokusirajući se na tehnike koje se mogu koristiti da se naškodi sistemu. Pošto se identifikuje pretnja, moraju se identifikovati i različite mere koje treba razmotriti u cilju otkrivanja i sprečavanja malware-a, uključujući mere zaštite kako na nivou sistema i mreža tako i na sveobuhvatnu strategiju zaštite.

2.1. Pozadina

Na opštem nivou termin „malware“ može da označava bilo koji deo računarskog koda koji ima zlonamerni ili neželjeni efekat na IT sisteme ili mreže. Iako bukvalno postoje hiljade pojedinačnih primera zlonamernih programa, ključne kategorije su sledeće:

- ▶ **Virusi:** koristi program koji ulazi u sistem takozvani prevoznik, koji inficira radni materijal kao što su diskovi, datoteke ili dokumenta. Oni se krišom spajaju sa programima. Virus nosi „teret“ koji će aktivirati u nekom trenutku nakon pokretanja, i izazvati neželjene efekte, koji su u nemalom broju pogubni po dokumenta. Treba napomenuti da termin „virus“ se često koristi kao generička oznaka za sve oblike zlonamernih programa, ali on u svim slučajevima to nije. Takvi termini se najčešće javljaju u medijskom kontekstu i izveštajima.

Postoji nekoliko vrsta virusa:

- ▶ Virus koji inficiraju fajlove- Tradicionalni oblik računarskog virusa, je infektor fajla koji se skriva u kodu drugog programa. Oni su pre pojave Interneta i makro virusa bili uzročnici skoro 85% svih infekcija. Zaraženi program može da bude poslovna aplikacija, pomoćni program ili čak i igra – bitno je samo da program bude izvršan, obično sa ekstenzijom EXE, COM, SYS, BAT ili PIF. Kada se zaraženi program pokrene, kod virusa se učitava u sistemsku memoriju, obično prije nego što se učita kod programa. Virus tada traži druge fajlove koje može da zarazi i umeće se u njih, a takođe isporučuje svoj sadržaj u skladu sa načinom na koji je programiran. Potom vraća kontrolu host programu koji završava učitavanje i prikazuje se na ekranu.³

U zavisnosti od načina na koji inficiraju fajlove, virusi fajlova mogu se podeliti u nekoliko kategorija:

- ▶ Parazitski virusi – menjaju sadržaj inficiranih fajlova, ali tako da ti fajlovi i dalje ostanu kompletno ili delimično upotrebljivi. U većini slučajeva, originalni kod se pomera naviše ili naniže kako bi se napravio prostor za kod virusa
- ▶ Virus koji prepisuju sadržaj fajla – prepisuju originalni programski kod svojim kodom. Na taj način uništavaju originalni programski kod i program više ne može da funkcioniše.
- ▶ Virus sa neprimetnom ulaznom tačkom – (*EPO-Entry-Point Obscuring*) umeće u program samo kod koji pokreće kod virusa. Instrukcija koja pokreće kod virusa obično

³ Garrison Clint P., (2010), *Network, Internet, and Cloud Computing*

se izvršava pod specifičnim programskim uslovima, tako da virus može duže vreme ostati aktivan.

- ▶ Prateći virusi – kreiraju klon host fajla koji se zatim pokreće umesto originalnog fajla. Ovi virusi mogu da preimenuju ciljani fajl, a originalni naziv da dodele zaraženom klonu ili da promene DOS putanju tako da vodi do zaraženog fajla.
- ▶ Link virusi – ne menjaju fizički sadržaj host fajla, već kada se on pokrene primoravaju operativni sistem da pokrene i kod virusa. To se postiže modifikovanjem prvog klastera host fajla, tako da ukazuje na klaster koji sadrži kod virusa.

Virusi koji inficiraju fajlove mogu, takođe biti i statički ili polimorfni.

Statički virusi se nikada ne menjaju, tj, kod virusa ostaje isti kroz sve infekcije.

Polimorfni virusi se mogu menjati prilikom prelaska sa jednog sistema na drugi, tako da ga je teško otkriti. Takođe, virusi mogu kombinovati infekciju fajlova zajedno sa infekcijom boot sektora.

Najlakši način za detektovanje virusa koji inficiraju fajlove je praćenje veličine fajlova. Antivirusni programi takođe poseduju i druge načine za identifikovanje ovih virusa.

Virusi koji inficiraju boot sektor – Smešteni su na delu diska koji se učitava u memoriju prilikom podizanja sistema (na floppy disku to je boot sektor, a za hard disk ekvivalentna oblast poznata kao Master Boot Record - MBR). Kada se jednom učita, virus može da zarazi druge diskove koje računar koristi. Ovi virusi mogu biti izuzetno destruktivni – ako oštete ili prepisu boot sektor hard diska, mogu da spreče kompletno startovanje računara, a mogu i da unište određene ili sve podatke sa hard diska. Oni su bili naročito aktuelni u vreme masovnog korišćenja floppy diskova, kada se virus prenosio sa floppy diska na hard disk (i obratno) i tako se širio. Danas je češći slučaj tzv. hibridnog virusa koji sadrži komponentu za inficiranje boot sektora zajedno sa infektorom fajla, Trojancem ili kodom crva.

U opštem slučaju, virusi boot sektora se lako identifikuju i uklanjaju. Tipični virus boot sektora usporava boot rutinu i često prikazuje neuobičajene poruke na ekranu računara. Antivirusni programi pronalaze ove viruse skeniranjem boot sektora. Većina virusa ima identifikujući tekst koji se inače ne nalazi u boot sektoru (odnosno MBR kodu). Na pojavu infekcije, takođe, ukazuje i promena veličine MBR koda, jer prisutstvo virusa utiče na povećanje njegove veličine (standardni MBR kod zauzima manje od polovine sektora na hard disku, a većina virusa je znatno veća).

Makro virusi – To su virusi kreirani pomoću makro jezika koji koriste brojne softverske aplikacije. Makroi su manji programi koji se kreiraju za visoko specifične zadatke u okviru aplikacije i napisani su pseudo programskim jezikom dizajniranim za rad sa aplikacijom (npr. Visual Basic for Applications (VBA) koji se koristi u Microsoft-ovim aplikacijama). Makro virusi se ne aktiviraju otvaranjem aplikacije, već tek nakon otvaranja zaraženog dokumenta (npr. otvaranjem zaraženog Word fajla). Da bi se to postiglo većina ovih virusa koristi makroe koji se automatski izvršavaju svaki put kada se dokument otvori (ili nakon specifične akcije programa), bez traženja dozvole ili akcije korisnika. Makro virus tada može da briše tekst, preimenuje ili briše fajlove i sl. Većina ovih virusa se kopira na standardni templejt (default template) aplikacije (npr. u Microsoft Word-u to je templejt Normal, pod nazivom normal.dot), tako da svi novokreirani dokumenti bivaju zaraženi.

Skript virusi – Ovi virusi su zasnovani na skript jezicima (Visual Basic Script – VBS, JavaScript i dr.), koji liče na makro pseudo-programске jezike, a koji se koriste na Web sajtovima i nekim kompjuterskim aplikacijama. Oni se često izvršavaju automatski sa otvaranjem Web stranice ili HTML e-maila. Napomenimo da se makro virusi mogu svrstati u grupu skript virusa, ali je način njihovog distribuiranja (preko dokumenata) drugačiji od ostalih skript virusa (preko zaraženih Web stranica, e-mail poruka, fajlova pripojenih e-mail porukama i Internet Relay Chat – IRC sesija).

- ▶ Crvi : ima sličnosti sa virusom u smislu prenošenja u umreženom sistemu. Oni se razlikuju po tome što su u stanju da se samostalno šire, za razliku od virusa. Crvi koriste mrežnu povezanost između sistema i nekada može da se proširi kao potpuno automatizovana aktivnost, kao što je skeniranje slučajnih IP adresa ili iskorišćavanje propusta u zaštiti pri ulasku u daljinske sisteme. Crv je kompjuterski program koji se kopira sa jedne mašine na drugu, obično bez eksplicitne akcije korisnika. Šire se preko mreže (automatskim slanjem e-mail, IRC ili instant poruka). Isporučuju destruktivne sadržaje ili samo zagušuju mrežu samopropagiranjem. Najskriveniji su tzv. mrežni crvi. Najčešće koriste propuste u Web serverima i browserima. Dok funkcionišu, ovi programi postoje samo u sistemskoj memoriji tako da ih je teže identifikovati od pomenutih crva fajlova. Crvi skeniraju mrežu kompanije ili Internet, tražeći drugi računar sa specifičnim propustom po pitanju zaštite. Brzo se repliciraju, a mreža zaražena crvom može da se obori za nekoliko sati

- ▶ Trojanci: naziv je dobio po drevnom konju koji se koristio kod Grka kako bi izvršili napad na Troju. Ova kategorizacija malicioznog softvera se odnosi na programe koji korisnici ne primete, jer se pretvaraju da obavljaju neku aktivnost, ali na kraju pokazuju da su naneli neku štetu.

Tu su i razni drugi uslovi i okolnosti koje možemo sresti kod opasnih i štetnih kodova, uključujući i štetne zamke, vremenske bombe koje se pokreću posle određenog vremenskog perioda ili kada se proteklo određeno vreme, datum koji su podešeni, logičke bombe, koje se aktiviraju određenim događajem ili nizom događaja koji se javljaju u sistemu. Malware je konstantno jedan od najviših nivoa bezbednosnih pretnji.

Malware je konstantno jedan od najjačih pretnji i mnoga istraživanja pokazuju da je tako. A jedna od značajnijih stvari je i ta da se korisnici sada više susreću sa malwarima, jer se koristi Internet kao transportni medijum. Zbog toga je malware distribucija postala brža i opasnija. U 2000 godini statistika je pokazala da se u proseku na svakih 790 e-mail poruka nalazila i jedna koja je sadržala virus, u 2004 je na svakih 16 e-mailova postojala jedna koja je sadržala u sebi virus, danas je taj broj veći. Na osnovu ove statistike da se izbegnu zaražene poruke znatno su pale. Imajući u vidu tako nagle promene, jasno je da oni koji stvaraju malware postižu stalni napredak, naglašavajući time važnost efikasnog otkrivanja i preventivne strategije kako bi se korisnici zaštitili na vreme.

2.2. Motivacije za napad

Pre nego što se osvrnemo na to šta malware može da uradi, potrebno je razmotriti ulogu ljudi koji pišu zlonamerne softvere. Razumevanje njihovih tehnika i motiva za napade, mogu nam u mnogome pomoći kako da se odbranimo od njih.

Tipični motivi mogu da se klasifikuju prema jednoj ili više sledećih razloga:

- ▶ Da vide koliko daleko se može proširiti njihova tvorevina ili koliko pažnju ona može privući

- ▶ Koliku štetu ili oštećenje ona može proizvesti, što može biti razlog napada na pojedinca, organizaciju ili režim
- ▶ Da bi se postigao osećaj moći nad onima koji su žrtve
- ▶ Malware koriste kao sredstvo za određeni vid lične koristi
- ▶ Nekada da bi se pružile „lekcije“ ljudima o bezbednosti, pružajući time praktičnu ilustraciju administratorima na kojim mestima i koliko je slaba zaštita nekog sistema.
- ▶ I jedan od najčešćih motiva je da vidi šta se može postići sa savremenim softverima, mrežnim tehnologijama i dr.

Iako je komunikacija sa programerima malware-a jako retka, postoje neki komentari koji daju uvid u njihov način razmišljanja. Neki od tih su da bi se proverila tehnička izdržljivost novih načina pristupa, ili da bi se dokazala i pokazala ranjivost i propusti neke platforme ili sistema koji su ciljne grupe napada. Objavljen je intervju sa bivšim piscem virusa Marekom Strihavkom, bivšim članom grupe 29a, pričao je o ciljevima i motivima za pisanje virusa:

„Svrha 29a je oduvek bila tehnički napredak, pronalazak i inovacija kao i tehnička zanimljivost virusa... uvek sam pokušavao da dođem do nečega novog što nikada ranije nije viđeno. Kodirao sam viruse za platforme čiju sam otpornost na viruse morao proveriti. Tu se ne radi o bilo kojoj vrsti „sajberterorizma“.

Nešto direktnije opravdanje dolazi od strane Onela de Guzman, samopriznatog pisca malware-a i navodi da je stvorio čuvenog zloglasnog Loveletter crva. De Guzmanov cilj je bio da se dokaže na neki način Microsoftova krivica za incidente jer se crv oslanjao na sposobnost da iskoristi slabosti Outlook e- mail klijenta.

„Za programere kao što smo mi, to nije pogrešno... ja sam korisnik, ja kupujem proizvod. Ako ga koristim na pogrešan ili nepravilan način, zašto bih ja bio kriv?“

Pored takvih mišljenja, takođe je moguće dobiti indikacije autora ili motive iz poruka koje često kriju u svojim tvorevinama. Možda i ne iznenađuju s obzirom na moć i ego-orjentisane motive mnogih njihovih stvaralaca, jedan od najčešćih oblika poruke odnosi se na hvalisanje o sopstvenoj veštini za stavljanje malware-a. Kao primer možemo uzeti sledeću poruku koja se odlaže u sistem direktorijumu (pod nazivom „msg15.txt.“) nakon inficiranja.

*„Lucky Av’s :P. Autor Sessar dobija IT bezbednosni posao i mi ćemo raditi sa Mydoom, na P2P crvima i iskoristiti te kodove. Takođe ćemo izvršiti napade na mcafee, trendmicro i dr. Ovo će biti dan D. Kada Beagle i Mydoom izgube mi ćemo obustaviti sve naše aktivnosti. <== dakle gde je Skynet sada? Lol
Ovo će oboriti W32. Scan P2P Worm.“⁴*

U ovom slučaju, tekst je ismejavanje rivala crva NetSky i najavljivanje pretnji različitim antivirusnim kompanijama. Takođe dešava se da autori prenesu poruke koje pokušavaju da opravdaju njihove postupke.

Na primer, kod iz Blaster-a avgusta 2003. godine sadržao je sledeću poruku:

*„Samo hoću da ti kažem volim te!
Billy Gates zašto bi ovo bilo moguće? Prestani da zarađuješ novac i popravi svoj softver!!“*

U međuvremenu poruka ugrađena u kod crva Klez pojavila se oktobra 2001 i sadrži sledeći tekst:

*„ Žao mi je da to učinim, ali ne želi da kaže izvini.
Ja samo želim dobar posao, i moram da podržim svoje roditelje.
Sada možeš da vidiš moje tehničke sposobnosti.
Kolika je sada moja plata? Ne više od 5.500 dolara.
Šta mislite o tome?
Možete li mi pomoći?“*

Iz ovih primera je jasno, da je motivacija relativna za svakog programera malware-a. Međutim motivaciju možemo otkriti iz onoga što malware pokušava da napadne i uradi. Neki od malware-a pokušavaju da onesposobe i iskoriste zadnja vrata sistema kako bi nastavili dalji upad. Upad na ovakav način može onesposobiti čitav sistem, i ili iskoristiti nekoliko hiljada računara kako bi preuzeo kontrolu nad njima i kako bi oni počeli da rade kao roboti. Većina napada se koristi u finansijske svrhe. Jedan pristup može da iznajmi čitavu mrežu da bi ga koristio kao sredstvo za slanje neželjene pošte i zaobilaženje IP

⁴ Garrison Clint P., (2010), Network, Internet, and Cloud Computing

adresa sa crne liste. Druga opcija je iznuda, značajne žrtve u tom pogledu su sajtovi za kockanje, koji su prijavljivali da su mete Ruskog organizovanog kriminalnog sindikata.

2.3. Razvoj pretnji

Pošto je ustanovljeno postojanje malwarea i njegove pretnje, ovde se razmatra o načinu njegovog evoluiranja tokom vremena. Ovde se osvrćemo najviše na crve i viruse koji su i ujedno jedna od najvećih pretnji. Trojanski konji još uvek imaju značajno prisustvo iako priroda njihove pretnje nije fundamentalno evoluirala oni su ustanju da urade sve što se može uraditi, mada postoji potencijalno ograničen pristup privilegijama. Jedna od najznačajnijih promena je put kojim mogu doći do sistema. S obzirom na ugradnju Trojanac se nekada oslanja na ručnu akciju prenosa od strane korisnika koji toga nije ni svestan. Crvi se automatski ubacuju u sistem. Crvi i virusi su u svojim razvijanjima dosta napredovali u smislu infiltracije, mehanizama kao i rezultatima akcije na određenom ciljanom sistemu. Distribucija se najlakše dešava od strane Interneta, poslednjih petnestak godina smo svedoci nekih posebnih faza:

- ▶ Ranih 90-tih virusi su se prenosili razmenom diskova i tako se širili između sistema
- ▶ Sredinom 90-ih zlonamernim programima je omogućeno da budu ugrađeni u fajlove koje korisnici razmenjuju jedni sa drugima
- ▶ Kasnih 90-ih automatsko funkcionisanje pošte omogućilo je napredovanje širenja virusa.
- ▶ Danas je to izbegavanje i iskorišćavanje propusta glavni način omogućavanja širenja virusa.

Maliciozni napad datira još dalje od tog perioda. Prvi poznati slučajevi virusa mogu se pratiti od 1982. godine. Autor 15-godišnji Ričard Skrenta, napravio je virus koji se prenosi između mašina, inficiranjem disketa i učitavanjem u memoriju svaki put kad se sistem pokrene, sa zaraženog diska. Posle 50-og puta virus bi prikazao poruku kao na donjoj slici.

```
Elk Cloner:  The program with a personality  
  
It will get on all your disks  
It will infiltrate your chips  
Yes it's Cloner!  
  
It will stick to you like glue  
It will modify ram too  
Send in the Cloner!
```

Slika 1. Poruka koja se pojavljuje u Elk Cloner virusu

Izvor: Mining E-mail autorship, publikacija, 2008,

Ovaj virus nije činio ništa, da namerno poremeti korisnike ili oštetiti njihov sistem. Iako je današnji termin „virus“, takav termin nije postojao kada se ovaj program pojavio. Tek dve godine kasnije, za ovakvo ponašanje softver, dobija današnje ime.

„Virus“ se sada često koristi kao termin da obuhvati sve oblike malware-a. Zajedno sa hakerima po kompjutersku bezbednost imaju i ljudi koji ne štite računare i sisteme na valjan način.

2.4. Mehanizmi prostiranja

Svi malware-i zahtevaju sredstva kako bi pronašli put ka sistemima „žrtvama“. U slučaju crva i virusi imaju sposobnost da prenesu deo urođene funkcionalnosti sa aplikacija unutar i između sistema što je i ključ daljih infekcija. U principu postoje razne tehnike i metode koje se mogu koristiti za širenje virusa:

- ▶ masovno slanje
- ▶ eksploatacija ranjivosti sistema
- ▶ napad na nezaštićenu mrežu

Treba znati da malware programeri prate razvijanje tehnologije, platformi i na osnovu toga razvijaju i unapređuju svoje softvere.

- ▶ E-mail. Od kasnih 90-tih godina, e-mail poruka se pokazala kao izuzetno moćan metod distribucije malware-a. Iako je prvobitno postojao jedan način razmene i širenja virusa, sada to korisnici mogu to da naprave razmenom e-pošte u kombinaciji sa automatizovanim funkcijama i time zaraze velike mreže. Ove tehnike uključuju Melissa-u, Word 97 mikro virus 1999 godine, LoveLetter, crv zasnovan na Visual Basis kodu.
- ▶ *Peer-to-Peer* (P2P) mreže: početkom 2000-ih došlo je do rasprostiranja i popularnosti ovih mreža, koje mogu da sadrže softver, kao što je KaZaA i Morpheus, koji su postali naročito značajni kao izvor nelegalnih softvera, muzike i drugih piratskih medijskih datoteka. Oni su postali prirodna meta zlonamernih programa, čiji autori shvatili da se mogu iskoristiti kao distributivni kanal koji će maskirati malware-a i prikazati ga kao drugi sadržaj i tako zavarati korisnika da ga preuzmu u uverenju da su preuzeli nešto drugo.
- ▶ *Instant Mesaging (IM)* ovaj vid poruka postao je popularan kao aplikacija korisna i kod kuće i na radnom mestu, omogućavajući lične razgovore kao i pogodan način kontakta i razmene informacija u okviru organizacije. Za malware-a ona je služila da se ostvari još jedan potencijalni kanal za napad na kompanijske mreže.
- ▶ *Blogovi*: sa popularnošću blogova, napadačima je omogućen novi vid napada u vidu kreiranja lažnih blogova i njihovih lokacija., zbog kojih će sistem posetioca biti ugrožen kada ih poseti radi nekih značajnih tema.

Sve ovo ilustruje oportunističku prirodu autora malware-a, a činjenica da su oni podešeni da pronalaze nove načine da bi prevarili žrtve. Autori koriste svoje softvere kako bi pokazali svoju domišljatost i svetu prikazali svoju kreativnost. U neku ruku oni žele publicitet.

2.5. Tehnike samoodržavanja

Jedna od najvažnijih osobina za dobar maliciozni napad je ta da se on mora teško otkriti i uništiti. Za taj cilj programeri malware-a su osmislili niz tehnika dizajniranih tako da prikriju postojanje svojih kreacija u okviru sistema i da otežju zadatak antivirusnim paketima.

- ▶ *Stealh* tehnika: zlonamerni napad može da koristi metod sakrivanja dokaza o svom postojanju i time poveća šanse za izbegavanje detekcije. Na primer, ako je virus zarazio izvršni program, veličina fajla koji je napadnut neizbežno se menja. Virus može pokušati da prikrije ovu promenu.
- ▶ Polimorfizam: virus je dizajniran tako da komplikuje funkciju i zadatak antivirusnih softvera. Glavni način detekcije malware-a je potpis, polimorfni malver se šifrue različito za svaku infekciju, da bi se izbegao konzistentni detektovani potpis.
- ▶ Metamorfizam: iako polimorfni maliciozni napad može usvojiti različite maske, u osnovi ostaje kod. Nasuprot ovom, metamorfni malver ima sposobnost da se koriguje, radi tako da može da rastavi kod, vrši preraspodelu u posebne blokove koda, a zatim može ponovo da se sastavi da bi dao novu instancu. Najpoznatiji primer je Evol crv.
- ▶ Ofanzivna bezbednost: imajući u vidu da su mnogi sistemi sada opremljeni antivirusnim i drugim oblicima zaštite, sve češće se pojavljuju virusi koji pokušavaju da tu zaštitu zaobiđu i da je osujete. Nekoliko tehnika je razvijeno. Na primer, crv Gaobot pokušava da blokira pristup preko veze za bezbednost Web sajtova i time spreči da zaražen sistem dobije bezbednosnu zaštitu koja bi omogućila detekciju i uklanjanje crva. On takođe održava listu od preko 420 procesa koji prestaje ako se detektuje njegova prisutnost na sistemu. Pojedini crvi pokušavaju da izbrišu različite Windows stavke registratora kako bi se sprečila povezanost sa bezbednosnim softverom kada se sam sistem pokreće.

2.6. Identifikacija i odbrana od malicioznih napada

Većina antivirusnih sistema je zasnovana na metodologiji identifikovanja virusa, kroz razne tehnike skeniranja, a potom se vrši izolacija i onda uklanjanje. Skeneri koriste antivirusni mehanizam koji ima jednu ili više faza:

- ▶ Jednostavno skeniranje: ovaj vid otkriva nepravilne bajtove koji se koriste od starne malicioznih napada.
- ▶ Kompleks skeniranja: on je zasnovan na jednostavnom skeniranju, tačnije otkriva i identifikuje nepravilnosti i omogućava prevenciju od trenutnog malware-a.
- ▶ Algoritamsko skeniranje: on generiše algoritam koji se koristi za otkrivanje određenih virusa.
- ▶ Kod emulacije: ovaj vid se oslanja na korišćenje virtuelne mašine koja oponaša okruženje. Virus izvršava u ovom virtuelnom okruženju napad, i biva pronađen i uklonjen
- ▶ Heuristička analiza: ovaj vid zaštite se koristi za sumnjive kombinacije koda i često se koristi kao filter za algoritamsko skeniranje.
- ▶ Neuronske mreže: ovaj vid se koristi da bi se smanjio broj lažnih uzbuna proizvedenih tokom upotrebe heurističke analize. Neuronske mreže mogu biti „obučene² da otkrivaju samo one kombinacije koda koje su zaista zlonamerne i koje predstavljaju najveće pretnje.

Jednom identifikovan maliciozni napad kroz upotrebu gore navedenih tehnika za skeniranje, mora biti izolovan i ako je zaražen sistem mora biti očišćen i popravljen. Na opštem nivou, antivirusni sistem se oslanja na poznavanje lokacija i veličina zlonamernog koda. Ukoliko je malver polimorfni, on mora biti prvo dešifrovan, a većina modernih antivirusnih sistema imaju generički dekriptor, koji se oslanja na pomenute tehnike. Uprkos sofisticiranosti i kompleksnosti otkrivanja malware-a njihovo otkrivanje i tehnike, antivirusni sistemi su i dalje u velikoj meri ograničeni na identifikaciju pretnji. Redovno ažuriranje antivirusnih proizvoda sa novim potpisima je od vitalnog značaja za zaštitu od napada na sistem. Nepravilna upotreba antivirusnog softvera može značajno da onespособi potpunu zaštitu sistema od pretnji. Zato je i jako bitno da su radnici obučeni za pravilno korišćenje softvera za zaštitu.⁵

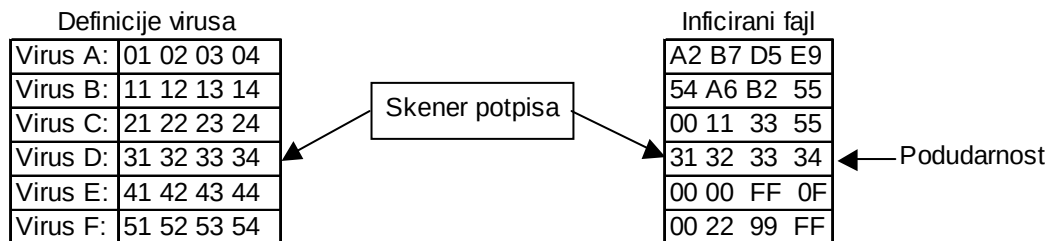
⁵ Seminarski rad, *Zaštita mreže od napada virusa*, Sveučilište Zagreb.

2.7. Tehnike za ublažavanje posledica malicioznih napada

Postoje i druge tehnike, koje se koriste za ublažavanje štete, pri pretnjama od strane malicioznih napada. Ove tehnike uključuju:

- ▶ Skeniranje potpisa
- ▶ Kontrola pristupa sistemu
- ▶ Provera integriteta
- ▶ Blokiranje ponašanja
- ▶ Heurističko skeniranje
 - ◆ Filtriranje sadržaja
 - ◆ *Sandboxing*
 - ◆ Analiza ponašanja

Skeniranje potpisa – Primarni metod detektovanja poznatih virusa koji koriste antivirusni programi naziva se skeniranje potpisa. Ovaj metod proverava da li u sadržaju skeniranog fajla postoje unapred definisane jedinstvene sekvence binarnih kodova poznatih virusa (prikazano na slici 2.)



Slika 2. Identifikacija poznatog virusa skeniranjem potpisa

Izvor: Zaštita mreže od napada virusa, Sveučilište Zagreb.

Kodovi poznatih virusa se nalaze u bazi podataka antivirusnog programa. U slučaju podudarnosti, program označava fajl kao inficiran i preduzima odgovarajuću akciju.

Danas postoje virusi kod kojih kod mutira prilikom repliciranja, dok neke mutacije bivaju i kriptovane. Na taj način, javlja se potreba da fajlovi sa potpisima (fajlovi u kojima se nalaze definicije virusa) antivirusnih programa uključuju i odgovarajuće algoritme za dekriptovanje. Situacija se dodatno komplikuje sa pojavom tzv. polimorfnih virusa koji generišu slučajne rutine za enkripciju.

Kontrola pristupa je ugrađena u sistem da bi ograničila prava korisnika i aplikacija. Njihova svrha je da obezbede tajnost podataka o sistemu. Po svojoj zlonamernoj prirodi malver može da dođe integriteta podataka i tada je u stanju da uđe u sistem sa svim pravima koja odgovaraju korisnicima i aplikacijama.

Za razliku od kontrole pristupa, **provera integriteta** se oslanja na činjenicu da malware pravi kompromis kod integriteta programa. Nažalost, sposobnost sistema da proveriti sve instalirane programe da nisu menjani je ograničen. Alternativa skeniranju potpisa je provera integriteta. Ova starija tehnika je relativno jednostavna, jer se traže samo promene u veličini individualnih fajlova. Fajlovi na hard disku se skeniraju i registruju sa njihove veličine. Svaki sledeći put kad se pokrene provera integriteta vrši se poređenje veličine fajlova sa prethodno memorisanim veličinama i u slučaju razlike, program ukazuje na moguću infekciju. Ova metoda je dobra za testiranje fajlova koji imaju fiksnu veličinu, ali je beskorisna u slučaju fajlova čija se veličina često menja. Drugim rečima, provera integriteta može biti korisna za odbranu od virusa koji inficiraju fajlove, ali ne za odbranu od makro i skript virusa.

Blokiranje ponašanja se oslanja na činjenicu da zlonamernost često iniira aktivnosti kojih korisnik nije ni avestan ili mu nisu poznate, kao što je primera radi povezivanje aplikacija. Blokatori ponašanja otkrivaju takve akcije i upozoravaju korisnika da li to namerava zaista da uradi. Mada za neke korisnike većina ovakvih poruka je iritirajuća, pa na njih nekada obrate pažnju, a nekada ne. Ovi blokatori mogu izbeći spore infekcije malvera tj. da se njihovo izvršavanje dešava jedino kada korisnik nesvesno daje dozvolu za obavljanje određenih akcija. Blokiranje ponašanja je posebno korisno u saradnji sa heurističkom analizom, kada je blokiranje akcija transparentno korisniku.

Heurističko skeniranje – Heurističko skeniranje je jedna od najčešće korišćenih alternativa skeniranju potpisa. Ova vrsta skeniranja ne traži viruse, već ponašanje karakteristično za viruse. Drugim rečima, heuristički skener ne zavisi od specifičnih potpisa virusa, već traži opšte kodne sekvence koje se obično pronalaze samo u kodovima virusa, a ne i u legitimnim programima. Na primer, ako heuristički skener pronade da deo koda u programu pokušava da promeni Windows Registry, program se označava kao mogući virus. Na ovaj način moguće je otkriti i nepoznate viruse tj. one za koje ne postoji definicija (registrovani potpis).

Postoji nekoliko različitih načina za implemetaciju heurističkog skeniranja. Oni obično daju slične rezultate, a različiti antivirusni programi najčešće, pored standardnog skeniranja potpisa, koriste neki od njih. To su:

- ◆ Filtriranje sadržaja – Ovo je jedan od najtradicionalnijih metoda za heurističko skeniranje. Filtar sadržaja upoređuje osnovni kod svih dolazećih programa sa ugrađenom bazom pravila. Antivirusni softver, ustvari, traži samo ono što podseća na kod virusa zadužen za neku sumnjivu akciju. Na primer, ako pronade programski kod zadužen za brisanje EXE fajla, generiše poruku o mogućoj infekciji.
- ◆ Sandboxing – Sandboxing je interesantan pristup skeniranju virusa po tome što dozvoljava pokretanje dolazećeg programa unutar virtuelnog sandbox-a (eng. ograđeni prostor sa peskom – ustvari zaštićeno okruženje unutar koga se program može pokrenuti bez bojazni od oštećenja ostalog dela sistema). Sandbox simulira operativno okruženje računara (virtuelni računar), a sandboxing softver traži specifične aktivnosti pokrenutog programa. Ako se pojave takve aktivnosti (pokušaj brisanja fajlova, modifikovanje postavki operativnog sistema, editovanje Registry-a, itd.), softver daje upozorenje o fajlu koji potencijalno sadrži virus. Send-boxing je relativno skoriji proizvod koji omogućava da se samo pouzdani programi mogu pokrenuti na živi sistem. Svi ostali rade na izolovanim „virtuelnim podsistemima“. Zbog toga infekcija virusima ne utiče na „živi“ sistem, ali se može detektovati i izolovati u podsistemima. Neki zlonamerni programi mogu da iskoriste „živi“ sistem i izbegnu *send box*. Međutim on može da nađe primenu i spregu sa drugim sigurnosnim rešenjima. Korisnikovo obrazovanje je vitalna prva linija odbrane od virusa. Korisnici moraju da budu svesni rizika otvaranja pojedinih sajtova,

reklama i e-pošte od strane nepouzdatih izvora i od strane nepouzdatih sajtova za preuzimanje određenih sadržaja. Kao i obični korisnici, administratori moraju biti još oprezniji i svesniji rizika od napada i moraju dobroznati kako zaštititi sisteme.

- ◆ Analiza ponašanja – Analizom ponašanja se ne proveravaju programski kodovi, već se prati ponašanje celokupnog sistema. U zavisnosti od toga kako sistem reaguje na specifični program, softver za analizu ponašanja može da utvrdi da li je u toku napad virusa ili hakera. Softver se, dakle, izvršava u pozadini, prati rad sistema i reaguje na svako odstupanje od standardnih operativnih procedura. U slučaju da neka operacija (komanda) ne zadovoljava heuristički test, ona biva blokirana, a sistem i dalje nastavlja da funkcioniše.

2.8. Tehnike mrežnih nivoa

Na nivou mreže, odbrana od malware-a može uključiti i korišćenje lista za kontrolu pristupa ruterima, port blokiranja firewall-a, raspoređivanje mrežnih sistema za detekciju upada i upotreba *honeypots-a* kao i rano upozoravanje sistema. Mrežne skretnice mogu se posmatrati kao prva linija odbrane od malware-a. One mogu biti korisne u prevenciji *denial of service* napada i pokušaja prostiranja malware-a. Treba istaći da su i sami ruteri predmet ranjivosti i moraju biti dobro obezbeđeni, jer u budućnosti oni će biti ciljne grupe za eksploataciju sa potencijalnim razarajućim rezultatima.

Zaštitni zidovi su od vitalnog značaja odbrane od malware-a. Njihovim korišćenjem mnogi virusi mogu se sprečiti da izvrše upad u sistem. Oni blokiraju portove za sve neiskorišćene usluge i time sprečavaju značajnu količinu saobraćaja i smanjuju rizik od napada. Međutim firewall ne može lako blokirati saobraćaj na portovima kao što je TCP 80 koji se koristi za web servis. Firewall mora biti deo slojevite odbrane. Mnoge organizacije koriste tunele za daljinski pristup mrežama (VPN), oni dobijaju svoj lični firewall, ali postaju i jako ranjive. Treba imati u vidu da firewall ima svoje slabosti i zbog toga postaje sve više meta napadača.

Firewalli održavaju Internet konekciju što je moguće bezbednijom tako što ispituju i nakon toga odobravaju ili odbijaju svaki pokušaj povezivanja privatne mreže i spoljnih mreža,

kao što je Internet. Oni omogućavaju centralizaciju svih bezbednosnih servisa na spoljnim mašinama koje su optimizovane i posvećene zadatku zaštite.

Po prirodi, firewalli kreiraju "uska grla" (bottlenecks) između unutrašnjih i spoljnih mreža. Razlog za to je što sva saobraćajna tranzicija između ovih mreža mora proći kroz jednu tačku kontrole. Ovo je mala cena za bezbednost. S obzirom na to da su spoljne zakupljene linije relativno spore u poređenju sa brzinama modernih računara, zastoje prouzrokovani firewall-ima može biti kompletno transparentan. Većini korisnika su relativno jeftini firewall uređaji više nego dovoljni da se povežu sa Internetom. Za poslovne potrebe i potrebe ISP-a (Internet Service Provider - Dobavljač Internet usluga), čiji je Internet saobraćaj na mnogo višem nivou, razvijeni su ekstremno brzi (i skupi) firewall-vi, koji su u mogućnosti da opsluže i najzahtevnije privatne mreže.

Firewall-vi primarno funkcionišu koristeći tri osnovna metoda:

- Filtriranje paketa - Odbacuje TCP/IP pakete neautentifikovanih hostova kao i pokušaje povezivanja na neautentifikovane servise.
- Network Address Translation (NAT) - Prevodi IP adrese unutrašnjih hostova i tako ih skriva od spoljnog praćenja. Ovaj metod se naziva i maskiranje IP adrese (IP address masquerading).
- Proxy servisi - Uspostavljaju konekcije na visokim aplikacionim nivoima za unutrašnje domaćine u cilju da se kompletno prekine konekcija mrežnog sloja između unutrašnjih i spoljnih domaćina.⁶

Moguće je korišćenje uređaja ili servera koji obavljaju samo jednu od navedenih funkcija; na primer, može se koristiti usmerivač (ruter) koji obavlja filtriranje paketa, kao i proxy server na posebnoj mašini. Na ovaj način, filter za pakete mora propustiti saobraćaj kroz proxy server ili se proxy server mora nalaziti van unutrašnje mreže, bez zaštite koju pruža filtriranje paketa. Oba načina su opasnija od korišćenja samo jednog firewall proizvoda koji obavlja sve bezbednosne funkcije u isto vreme. Većina firewalla takođe obavlja dva podjednako važna bezbednosna servisa:

⁶ Seminarski rad, *Zaštita mreže od napada virusa*, Sveučilište Zagreb.

- ◆ Šifrovana autentifikacija - Omogućava korisnicima na javnim mrežama da dokažu svoj identitet firewallu, u cilju sprečavanja pristupa privatnim mrežama sa spoljnih lokacija.
- ◆ Virtualno privatno umrežavanje (VPN_- Uspostavlja bezbednu konekciju između dve privatne mreže preko javnog medijuma kao što je Internet. Ovo omogućava korišćenje Interneta fizički odvojenim mrežama bez zakupljivanja direktnih linija. VPN-i se takođe nazivaju šifrovanim tunelima.

Takođe, neki firewall-vi obezbeđuju dodatne servise kao što su:

- ◆ Skeniranje virusa – Pretražuju se dolazeći nizovi podataka u potrazi za virusima. Ažuriranje servisa liste virusa zahteva pretplatu kod proizvođača firewalla.
- ◆ Filtriranje prema sadržaju - omogućava da se unutrašnjim korisnicima blokira pristup određenim tipovima sadržaja.

Opisaćemo detaljnije pet primarnih funkcija koje većina firewalla pokriva:

► Filtriranje paketa

Prvi Internet firewall-vi su bili jednostavni filteri paketa. Filtriranje paketa i danas ostaje jedna od ključnih funkcija firewalla. Filteri upoređuju mrežne protokole (kao što je IP) i pakete transportnih protokola (kao što je TCP) sa pravilima regulisanim u bazi podataka i prosleđuju samo one koji potpadaju pod kriterijum specificiranih pravila. Filteri mogu biti implementirani ili u ruterima ili u okviru TCP steka na serveru. Oni koji su implementirani unutar usmerivača (ruter) sprečavaju da saobraćaj sumnjivog porekla stigne do određene mreže, dok moduli TCP filtera jednostavno sprečavaju tu specifičnu mašinu da odgovara na saobraćaj sumnjivog porekla.

Firewall pravila (dozvoljeni portovi)
TCP port 80 (Web)
TCP port 25 (Mail)
TCP port 21 (FTP)

Tabela 1. Filtriranjem Internet konekcije sprečava se neželjeni saobraćaj

Izvor: Zaštita računarskih mreža, Podgorica

Neka od tipičnih pravila koja filteri slede su:

- ◆ Odbacuju dolazeće zahteve za konekciju, ali dozvoljavaju zahtevima za izlaznu konekciju da prođu.
- ◆ Eliminišu TCP pakete upućene na portove koji ne bi trebalo da budu raspoloživi za Internet (kao što je port za NetBIOS sesiju), ali dozvoljavaju prolaz paketima koji bi trebalo da su raspoloživi (kao što je SMTP). Većina filtera može tačno odrediti koji saobraćaj ide na određeni server - na primer, SMTP saobraćaj bi trebalo kroz port 25 da ide samo na IP adresu servera za poštu (mail server)
- ◆ Zabranjuje zahtev za pristup dolazeće konekcije određenim IP opsezima

Unutrašnjim klijentima je uglavnom dozvoljeno da kreiraju konekcije ka spoljnim hostovima, a spoljni hostovi su uobičajeno sprečeni u iniciranju pokušaja konekcije. Kada unutrašnji host odluči da inicira TCP konekciju, on šalje TCP poruku na IP adresu i broj porta javnog servera. U inicirajućoj konekcionoj poruci, TCP kaže udaljenom serveru koja mu je IP adresa i na kom portu sluša odgovor (na primer, localhost:2050). Spoljni server tada šalje odgovor, transmitujući ga do datog porta gde ga unutrašnji host očekuje. Pošto firewall proverava sve podatke koji su razmenjeni između ta dva hosta, on zna da je konekciju inicirao unutrašnji host, koji je povezan na svoj unutrašnji mrežni nterfejs, zna IP adresu tog hosta i zna na kom portu očekuje odgovor. Firewall zatim pamti da treba da dozvoli spoljnom hostu, čija se adresa nalazi u konekcionoj poruci, da vrati saobraćaj na IP adresu unutrašnjeg hosta samo na port koji je određen. Kada učesnici u sesiji zatvore TCP konekciju, firewall briše unose u svojoj tablici stanja (memorija u kojoj se nalazi stanje konekcija) i time prekida mogućnost udaljenom hostu da dalje komunicira sa unutrašnjim. Ukoliko unutrašnji host prestane da odgovara pre zatvaranja TCP konekcije (na primjer, zbog prekida veze) ili ako protokol koji je u pitanju ne podržava sesije (na primjer, UDP), firewall će ukloniti unos u tablicu stanja konekcije nakon programiranog isteka vremena od nekoliko minuta.

Filtriranje ne rešava u potpunosti problem bezbednosti na Internetu. Kao prvo, IP adrese računara u filteru su predstavljene u dolazećem saobraćaju, što pojednostavljuje određivanje tipa i broja Internet hostova u filteru, kao i praćenje napada na ove adrese. Filtriranje ne sakriva identitet domaćina u filteru. Pored toga, filteri ne mogu proveriti sve fragmente jedne IP poruke, zasnovane na protokolima višeg nivoa, kao što su TCP zaglavlja, iz razloga što

zaglavlje postoji samo u prvom fragmentu. Podeljeni fragmenti nemaju informacije o zaglavlju i mogu biti upoređeni samo sa IP pravilima, koja uobičajeno dozvoljavaju nešto saobraćaja kroz filter. Ovo omogućava greškama u odredišnim IP stekovima računara na mreži da se eksploatišu i mogu omogućiti komunikacije sa Trojanskim konjem instaliranim negde na mreži. Savremeniji firewallovi podržavaju povratak fragmentovanih podataka u pređašnje stanje i nakon toga primenu firewall pravila na njih. Konačno, filteri nisu dovoljno složeni za proveru legitimnosti protokola u okviru paketa mrežnog sloja. Na primer, filteri ne ispituju HTTP pakete, sadržane u TCP paketima, radi utvrđivanja da li oni sadrže elemente, kojima hakeri gađaju web pretraživač ili web server na kraju konekcije. Većina pokušaja modernog hakerisanja zasnovana je na iskorišćavanju ovih servisa viših slojeva TCP/IP steka, iz razloga što su firewalli gotovo eliminisali uspešno hakerisanje na mrežnom sloju, ako izuzmemo neugodne napade tipa "odbijanje izvršenja servisa" (DoS, denial-of-service).

2.9. *Prevođenje adrese iz mreže (Network Address Translation-NAT)*

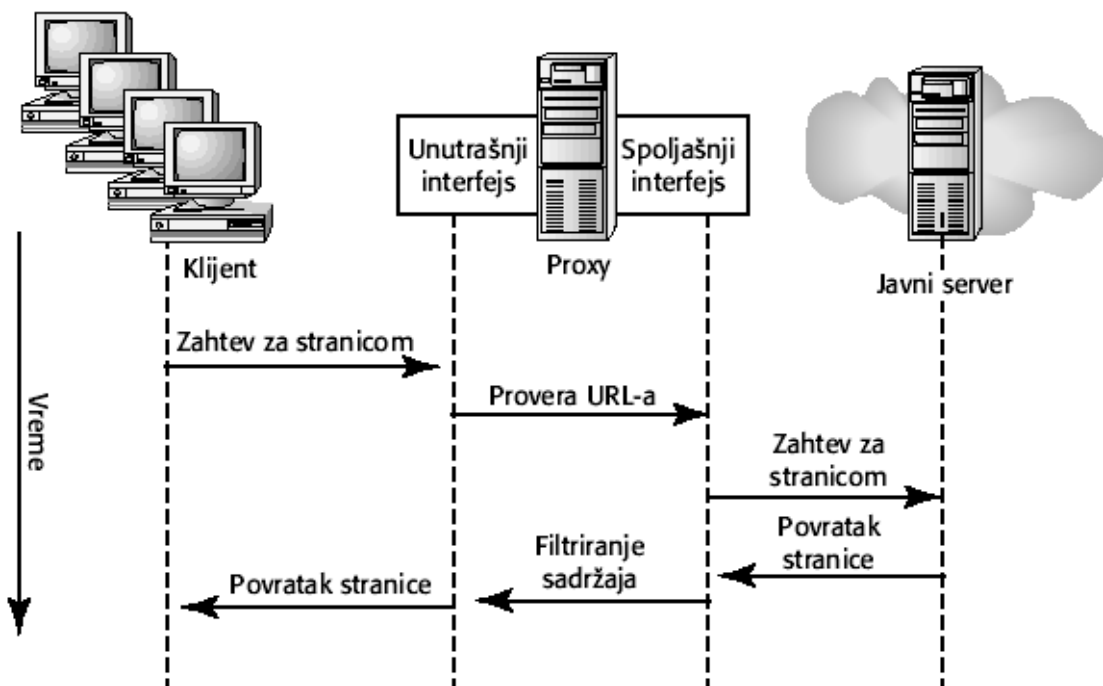
Prevođenje adrese iz mreže rešava problem skrivanja unutrašnjih hostova. NAT je zapravo proxy mrežnog sloja: jedan host čini zahteve u ime svih unutrašnjih hostova. Na taj način on skriva njihov identitet na javnoj mreži. Napomenimo, da većina savremenih operativnih sistema obezbeđuje ovu funkciju kao deo samog operativnog sistema.

NAT skriva adrese unutrašnjih hostova, konvertujući ih u adresu firewalla. Firewall zatim ponovo šalje podatke unutrašnjih hostova, koristeći sopstvenu IP adresu. Korišćenjem TCP broja porta, uspeva da prati koje se konekcije na javnom delu podudaraju sa hostovima na privatnom delu mreže. Gledano sa Interneta, sav saobraćaj sa lokalne mreže izgleda kao da dolazi sa jednog, ekstremno zaposlenog računara.

Prevođenje IP adresa omogućava korišćenje bilo kog opsega IP adresa na unutrašnjoj mreži, čak i ako se te adrese već koriste negde na Internetu. Takođe, NAT dozvoljava multipleksiranje jedne javne IP adrese kroz celu mrežu.

NAT rešava mnoge probleme Internet konekcija, ali ne sprovodi potpunu kontrolu podataka kroz firewall. Moguće je, na primer, da neko uz pomoć mrežnog monitora pregleda saobraćaj koji dolazi iz firewalla i na osnovu dobijenih informacija zaključi da firewall prevodi adrese drugih mašina. Hakeri na ovaj način mogu dobiti informacije potrebne za otimanje TCP konekcija ili za prolaz kroz firewall lažnom konekcijom.

Proxy aplikativnog sloja (nivoa) ovo sprečava. On omogućava potpunu zabranu protoka podataka protokolima mrežnog nivoa, a propušta saobraćaj baziran samo protokolima višeg (aplikativnog) nivoa, kao što su HTTP, FTP i SMTP. Proxy aplikativnog sloja je specifično klijentsko-serverska kombinacija za protokol koji se koristi. Na primjer, web proxy je kombinacija web servera i web klijenta. Serverski deo protokola proxya prihvata konekcije klijenata unutrašnje mreže, dok se klijentski deo protokola povezuje na javni server. Kada klijentski deo proxya primi podatke od javnog servera, serverska strana proxy aplikacije šalje podatke krajnjem unutrašnjem klijentu. Slika 3. prikazuje kako se ovaj proces odvija.



Slika 3. Funkcionisanje Web proxy servera

Izvor: Zaštita računarskih mreža, Podgorica

Proxy serveri primaju zahteve sa privatne mreže i ponovo ih generišu na javnoj mreži. Kada klijent zaštićene mreže inicira zahtev prema serveru javne mreže, proxy server preuzima taj konekcioni zahtev i povezuje se na server javne mreže u ime klijenta zaštićene mreže. Oni, takođe, prosleđuju odgovor javnog servera klijentu na unutrašnjoj mreži.

Razlika između NAT i filtera sa jedne strane i aplikativnih proxya (kao što je Microsoft Proxy Server) sa druge strane je u tome što su klijentske aplikacije za Internet (uobičajeno) unapred podešene za komunikaciju sa proxyem. Na primer, unošenje adrese web proxya u Internet Explorer na korisničkom računaru prouzrokuje da Internet Explorer šalje sve zahteve tom proxy serveru, umesto da sam razrešava adrese i uspostavlja direktne konekcije.

Aplikativni proxy ne mora biti pokrenut na firewallu - bilo koji server unutar ili izvan lokalne mreže može imati ulogu proxy servera. Ipak, ukoliko se želi postići dobra bezbednost mreže, trebalo bi postaviti i firewall i proxy. Mora postojati i neki tip filtriranja podataka zbog zaštite proxy servera od napada usmerenih preko mrežnog sloja tipa "denial of service" (kao što je "ping of death"). Ukoliko se proxy ne pokreće na firewallu, neophodno je otvoriti kanal kroz taj firewall. Preporučljivo je, ipak, da firewall obavlja i funkciju proxya kako bi se sprečilo prosleđivanje paketa javnog dela mreže u lokalnu mrežu.

Bezbedniji proxy-ji su u mogućnosti da izvode filtriranje aplikativnog sloja za određeni saobraćaj. Na primer, neki firewall HTTP proxy traže Java ili ActiveX oznake u HTML stranicama koje ukazuju na ugneždene aplete i zatim ih uklanjaju. Ovo sprečava da aplet bude izvršen na klijent kompjuteru i eliminiše rizik slučajnog učitavanja Trojanskog konja.

Proxy-ji mogu raditi samo sa specifičnim naročitim aplikacijama. Na primer, moraju se posebno imati proxy softverski moduli za HTTP, FTP, Telnet. Pošto ovi protokoli evoluiraju (naročito HTTP), moraju se redovno ažurirati određeni proxy softverski moduli.⁷

⁷ *Zaštita računarskih mreža, Podgorica*

3. Istraga Wireless napada

U ovom delu rada, biće objašnjen napad na Wireless mrežu kao i istraživanje ovakve vrste napada. U ovom poglavlju će biti fokus na istraživanje bežičnih napada. Ovde se razmatraju različite vrste bežičnih tehnologija dostupnih, kao i različite vrste napada.

3.1. Tehnologije Wireless mreža

Rast tehnologija bežičnog umrežavanja, je dao povoda za mnoga pitanja o bezbednosti, ova vrsta tehnologije je postala jako popularna zbog svoje praktičnosti i cene, koja je relativno niska. Bežične lokalne mreže (WLAN) omogućavaju radnicima da pristupe digitalnim resursima, bez da budu vezani za određenu prostoriju. Često je jeftinije i lakše da podesimo bežičnu mrežu, nego da se koriste kablovi kroz čitavu organizaciju. Sledi spisak nekih od najrasprostranjenijih vidova bežične mrežne tehnologije:

- ▶ Bluetooth
- ▶ Infrared
- ▶ Wireless USB
- ▶ Wi-Fi
- ▶ WiMAX
- ▶ Satellite
- ▶ ZigBee

Bluetooth

Bluetooth IEEE 802.15 je protokol za bežičnu razmenu podataka na malim udaljenostima sa fiksnih i mobilnih uređaja, što čini lične bežične mreže, personal area network (PAN). Nastao je kao alternativa RS232 prenosu podataka pomoću kabla. Moguća je konekcija više uređaja na ovu mrežu, uz prevazilaženje problema sinhronizacije. Razvojem specifikacije za ovaj

standard se bavi Bluetooth Special Interest Group. Od 1994 god. Dosada je bilo više verzija ovog standarda, verzije 1.0 i 1.0B su nekompatibilne sa ostalim verzijama, a verzije 1.1, 1.2, 2.0 i 2.1 su međusobno kompatibilne. Bezbednost Bluetooth komunikacije je prema objavljenim radovima, na više načina ugrožavana. Prednost ovakvog načina komunikacije su niska cena uređaja, mala snaga zračenja, koje je u principu štetno za ljudsko zdravlje, niska potrošnja energije.

Wireless USB

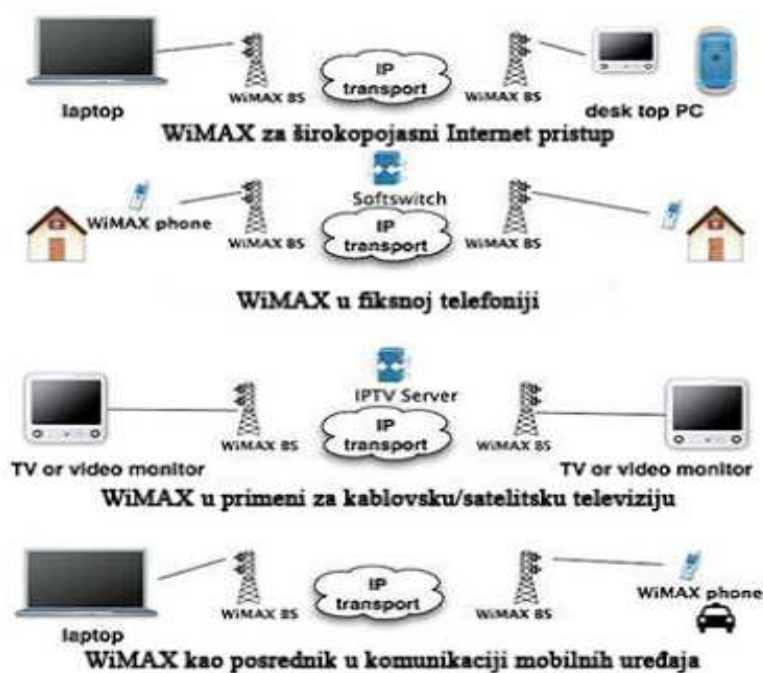
On je kratkog dometa, visoke propusne moći, radio komunikacioni protokol, kreiran od strane Wireless USB Promote Group. On se zasniva na Ultra-WideBand zajedničkoj radio platformi, koja je u stanju da pošalje 480Mbit/s na rastojanjima od 3 metra i 110Mbit/s na rastojanju do 10 metara. Dizajnirane je da radi 3.1 na 10.6 GHz frekvencionom opsegu, iako lokalna regulativa može da ograniči pravno operativni opseg za svaku zemlju.

ZigBee IEEE 802.15.4.

Je specifikacija za komunikacioni protokol koji koristi digitalni radio prenos sa niskom potrošnjom energije. Zasnovana je na IEEE 802.15.4 standardima i namenjena je za bežične personalne mreže (WPANs). Tehnologija definisana ovom specifikacijom je namenjena da bude jednostavnija i jeftinija od ostalih WPAN, kao što je Bluetooth, i primenjuje se kao RF prenos za mali protok podataka, dug vek baterijskog napajanja i kao bezbedna mreža. ZigBee radi na ISM opsegu 868MHz u Evropi i 915 MHz u SAD i Australiji, kao i na 2.4GHz u celom svetu. Jednostavna rešenja u tehnologiji donose niže cene uređaja. Proizvođači opreme nude integrisane varijante sa radio uređajem procesorom ili mikrokontrolerom, čak i sa kompletnim softverom. Najnovija verzija ZigBee specifikacije iz 2007 godine ima dva profila. Jedan za kućnu i manje zahtevnu komercijalnu upotrebu koji koristi RAM memorije i drugi je tzv. ZigBee Pro koji pruža znatno veće mogućnosti kao što je multi-casting, rutiranje many-to-one, poboljšanu bezbednost korišćenjem Symmetric-Key Key Exchange. Oba profila rade u mesh mrežama i rade sa svim ostalim profilima. ZigBee uređaja. Izrazita primena ovog standarda je u senzorskim mrežama.

WiMAX standard

Sve veća potražnja za širokopojasnim pristupom Internetu dovodi do prezasićenja postojeće zemaljske infrastrukture oličene u telefonskim paricama ili koaksijalnim kablovima u smislu kapaciteta bitskog protoka. Povećanje brzine pristupa se može ostvariti uvođenjem optičkih kablova do svakog doma. Poznato je da bilo koji telekomunikacioni operater ima najveće troškove prilikom uspostave takozvane *last-mile* infrastrukture iz razloga što je samo postavljanje kablova jako skupo. Pojam *last-mile* se odnosi na vezu između lokalne centrale operatora i samog korisnika. Kao rešenje se nameće korišćenje visoko efikasnog bežičnog standarda za pristup kao što je WiMAX.⁸



Slika 4. WinMax

Izvor : CET Čitalište 67 – Novembar 2007. WiMAX – dipl. ing. Dejan Petković

Ovaj standard je baziran na standardu IEEE 802.16, omogućava širokopojasni pristup baziran na IP Internet protokolu za mobilne i fiksne bežične korisnike kako u urbanom okruženju, tako i u ruralnim oblastima. IEEE 802.16 standard je razvijen kako bi omogućio vezu između bazne stanice i korisnika između kojih ne postoji direktna optička vidljivost, sa dometom između tri i deset kilometara.

⁸ dipl. ing. Dejan Petković, CET Čitalište 67 – Novembar 2007. WiMAX

Da bi mrežna oprema bila odobrena kao WiMAX-kompatibilna, mora da zadovolji striktne testove WiMAX foruma, i kao takva nudi pristupnu brzinu od 40 Mbps po kanalu. Za mobilne korisnike, koji uključuju PDA i Notebook računare, očekuje se kapacitet od oko 15Mbps unutar oblasti do 3 km u prečniku. WiMAX forum je organizacija proizvođača - globalnih lidera na polju telekomunikacija i IT tehnologija, i za cilj ima razvoj globalne platforme za širokopojasne IP-bazirane bežične servise. Ključ uspeha WiMAX standarda leži u kompatibilnosti uređaja različitih proizvođača. To će omogućiti veliku rasprostranjenost uređaja, i neće obavezivati operatora da opremu kupuje od samo jednog proizvođača.

3.2. Napad na bežičnu mrežu

Postoje razne vrste bežičnih napada. Slede neke metode koje hakeri koriste da bi olakšali ovu vrstu napada.

- ▶ *Wardwing*: je tehnika koju hakeri koriste da bi pronašli nesigurne bežične mreže, dok krstare net-om.
- ▶ *Warflying*: slično predhodnoj vrsti napada, ali uključuju „letenje“ okolo u potrazi za otvorenom bežičnom mrežom.
- ▶ *Warchalking*: uključuje korišćenje određenih simbola kako bi se postavio poseban simbol koji će ukazati da u obližnjem delu postoji bežična mreža koja nudi pristup Internetu.

Pasivni napad

Je vrsta napada gde neovlašćeni korisnik prati komunikaciju za prikupljanje informacija. Na primer, prisluškivanje mrežnog saobraćaja je jedna vrsta pasivnog napada. Prisluđkivač lako eksploatiše mrežni saobraćaj koristeći alate, kao što su: *Network Monitor* ili *AirSnort*. Pasivne napade je teško detektovati ili identifikovati. Oni su često simetrični, što znači da napadač

može da prati komunikaciju u oba smera. Neki drugi primeri pasivnih napada su analiza saobraćaja i praćenje saobraćaja.

Elektronske emanacije

One su elektromagnetni talasi zračenja koje emituje elektronski uređaj tokom operacije. Bežična tehnologija je predmet ovih emanacija. Napadač može da presretne emanaciju i da korišćenjem shvati kako da stekne odgovarajuće akreditivne kako bi se pridružio bežičnoj mreži. Glavni problem je u tome što administrator mreže ne može da identifikuje da je napadač presreo signal.

Aktivni napad

Aktivni napadi na bežičnoj mreži su slični onima na žičnim mrežama, u kojima napadač pokušava da promeni ili kompromituje i korumpira podatke ili usluge na mreži. Ove vrste napada uključuju preplavljanje podacima, obmane i neovlašćeni pristup. Informacije koje sakuplja usled pasivnog napada, napadač može sebi da olakša aktivan napad na mrežu.

Denial-Of-Service napad

Bežični sistemi imaju iste ranjive protokole koji su podložni DoS napadima koji pogađaju i žične mreže. Oni su takođe podložni i drugim vrstama DoS napada, jer se signali koji se koriste za prenos podataka preko mreže lako mogu kompromitovati i narušiti. Glavni cilj DoS napada je da se uskrati pristup mrežnim uslugama i resursima. Teško je pratiti takve napade na bežičnoj mreži. Režim napada DoS varira, on uključuje potrošnju, izmenu i fizičko uništavanje mrežnih komponenti ili resursa. Sledi spisak nekih uobičajenih napada:

- ▶ Potrošnja resursa: ovo podrazumeva korišćenje resursa sistema uključujući sledeće:
 - Protokol: uljez može da preusmeri pakete na mrežu kako bi se potrošio dostupan protokol na mreži
- ▶ Memorija : ovo se postiže nepotrebnim e-mailovima, izazivajući time punjenje memorije i deljenje datoteka na nevažne fascikle

- ▶ Izmena resursa ili informacija. Menjanje konfiguracije mašine može da spreči korisnika da koristi sam računar.
- ▶ Fizičko uništavanje računarskih/mrežnih elemenata. Ova vrsta napada se tiče uništavanja fizičkih elemenata, kao što su računari i ruteri.

Rezultat DoS napada su jako pogubni, jer zbog ovakve vrste napada vreme i novac se jako puno gube, jer su usluge organizacije koja je napadnuta nedostupni.

Man-In-The Middle napad

Ovo je napad kada se narušava pravilnik pristupa informacijama koje se prenose između pošiljaoca i primaoca. Prenos može biti nesiguran, jer informacija nije šifrovana. U takvim slučajevima, postoji mogućnost menjanja podataka od strane provalnika.

Postoji nekoliko vrsta ovog napada:

- ▶ Prisluškivanje: ovo je pasivna tehnika. Napadač presreće podatke koji se prenose između jednog ka drugom sistemu. Bezbednosni mehanizmi kao što su IPSec, SSH, SSL mogu sprečiti prisluškivanje.
- ▶ Manipulacija : je proširen korak prisluškivanja. O ovom tipu napada, napadač manipuliše podacima koje je presreo u toku komunikacije. Ova manipulacija može biti izvedena pomoću tehnika kao što je ARP „trovanje“

Otmica i modifikovanje bežične mreže

U bežičnoj mreži, TCP/IP paket ide kroz svičeve, rutere i wireless pristupne tačke. Svaki uređaj posmatra IP adresu odredišta i proverava tu adresu u listi lokalnih IP adresa. Ova tabela je dinamički izrađena na osnovu saobraćaja koji prolazi kroz uređaj i iz Address Resolution Protocol šalje obaveštenja za priključivanje uređaja na mrežu. Ukoliko odredišna IP adresa nije u tabeli uređaja, ona prolazi dalje. Međutim, ne postoji provera identiteta ili verifikacija važenja paketa koji uređaj primi. Zlonamerni korisnik može slati poruke, usmeravanja uređaja i pristupne tačke navodeći da je njegova MAC adresa povezana sa poznatim IP adresama. Sav

saobraćaj koji ide preko tih uređaja je namenjen za krađu i otimanje IP adrese koja će stići na računar zlonamernog korisnika.

Udruženje Wireless pristupne tačke i uređaja

Bežična pristupna tačka je čvor konfigurisan da dozvoli bežičnom uređaju da pristup na lokalnu mrežu. WAPs je samo priključen na switch ili na Ethernet hub. Pristupna tačka ima svoj domet. Postoje dve metode koje obezbeđuju određeni nivo bezbednosti između uređaja i WAP sa kojim je povezan:

- ▶ **MAC filtriranje:** MAC adresa ima 12 karaktera – 48 bita napisanih u heksadecimalnoj notaciji., to je jedinstvena hardverska adresa određenog sistema. MAC adresa se koristi u data-link sloju mreže. Samo oni uređaji sa MAC adresama sa bele liste je dozvoljen pristup na mreži.
- ▶ **Preshared key :** ili upotreba enkripcije: bežični uređaj i pristupna tačka koriste zajednički tajni ključ. *Checksum* se dodaje svakom paketu koji se prenosi preko mreže. Ukoliko je paket oštećen, onda se vrednost checksum-a menja, i to je lako identifikovati za upad. Uređaj kreira u paketima vektor koji je u kombinaciji sa ključem za šifrovanje paketa. Na prijemnom kraju isti ključ se koristi za dešifrovanje paketa.

3.2. Mrežna forenzika u wireless okruženju

Slede koraci koji su uključeni u obavljanje forenzičkog ispitivanja u bežičnom okruženju:

- ▶ Nabavljanje naloga za pretres
- ▶ Identifikovanje bežičnog uređaja
- ▶ Dokumentovanje podataka
- ▶ Otkrivanje bežične veze
- ▶ Mapa bežične zone i „žarišta“

- ▶ Povezivanje na bežičnu mrežu
- ▶ Analiza bežičnih podataka
- ▶ Generisanje izveštaja

Nabavljanje naloga za pretres

Istražitelj treba da obezbedi nalog za pretres uređaja na licu mesta, kako računara tako i bežične prateće opreme. Istražitelj može da izvrši forenzičku analizu samo na onim delovima opreme koji su navedeni u nalogu. Treba biti oprezan da se ne napravi previd kod uređaja koji se ne nalaze u istoj prostoriji.

Identifikovanje Wireless uređaja

Istražitelj treba da identifikuje sve različite bežične urešaje koji su povezani na mreži. On ili ona treba da provere fizičke lokacije na sledećim bežičnim hardverima:

- ▶ Wireless ruterima
- ▶ Bežične pristupne tačke
- ▶ Mežičnim modemima
- ▶ Bežičnim mrežnim adapterima
- ▶ Repetitorima
- ▶ Hard diskove
- ▶ Antene

Traženje dodatnih uređaja

Da si pronašli dodatne bežične uređaje na mreži, istražitelj mora da stavi svoj računar u prometni mod i početi sa slanjem podataka. Ovo može naterati aktivnu bežičnu opremu na ponovno povezivanje na podrazumevanu bežičnu pristupnu tačku, koja će biti preusmerena na forenzički računar. Airplay je bežični alat koji se koristi pri kreiranju specijalnih paketa podataka koji se ubacuju i bežični protok.

Detektovanje bežične pristupne tačke

Istražitelji mogu da koriste sledeće tehnike za pronalaženje bežične pristupne tačke:

- ▶ Ručno detektovanje: on treba da konfiguriše neku vrstu mobilnog uređaja slično kao ručni PC ili laptop. Za njeno otkrivanje istražitelj treba da fizički poseti područje gde se ona nalazi.
- ▶ Aktivno bežično skeniranje: ono podrazumeva emitovanje poruka i čekanje na odgovor od uređaja u opsegu. Sastoji se od slanja okvira zahteva za sondiranjem sa bežičnog klijenta. Klijenti šalju sondirajuće okvire kad aktivno traže mrežu, koji sadrže ili SSID mreže kojoj se klijent želi pridružiti. Cilj aktivnog sondiranja je lociranje pristupnih tačaka kroz koje se klijent može priključiti na mrežu. Nakon što je pristupna tačka s odgovarajućim SSID-om pronađena, klijent preduzima autentifikacijske i asocijacijske korake pridruživanja mreži kroz tu pristupnu tačku.
- ▶ Tehnika pasivnog bežičnog skeniranja – predstavlja proces soluskiivanja okvira na svakom kanalu određeno vreme. Beacon okvire šalju pristupne tačke, infrastrukturni mod ili klijent- ad-hoc mod. U konfiguracijama u kojima postoji više pristupnih tačaka, SSID one mreže kojoj se klijent želi pridružiti može biti odaslan s više pristupnih tačaka. Klijent će tada pokušati da se pridruži mreži kroz pristupnu tačku sa najjačim signalom.

4. Digitalni Forenzički alati – Nova generacija

Izbor alata je od suštinskog značaja u procesu digitalne forenzičke istrage. Samo oni alati koji daju tačne, potpune i pouzdane rezultate mogu obezbediti digitalne dokaze koji su prihvatljivi na sudu. U procesu selekcije alata veliki značaj pridaje se ispunjavanju uslova validacije i verifikacije, ali je od izuzetnog značaja i njegova upotrebljivost u konkretnoj istrazi.

Proces i izbor alata za digitalnu forenzičku istragu još uvek predstavlja izazov i nedovoljno je istražena tema u oblasti digitalne forenzike. Izbor adekvatnog alata koji će biti korišćen za digitalnu forenzičku istragu u velikoj meri utiče na ishod u sudnici. Iako je cilj jasan – dobijanje validnih digitalnih dokaza prihvatljivih na sudu, u praksi se pokazuje da do toga nije nimalo lako doći.

Validni digitalni dokaz treba da potkrepi dokaze iznete u sudnici, da dokaže krivicu ili oslobodi osumnjičenog. Mora biti pouzdan i doprinositi istrazi. Pošto je digitalni dokaz rezultat alata i metoda koje je odabrao i primenio digitalni forenzičar može se tvrditi da upravo od njegove stručnosti i dobrog izbora alata zavisi konačan ishod. Zbog nedostatka konkretnih propisa česta zamerka na sudu je usmerena na rezultate istrage koji nisu dovoljno naučno potkrepljeni kao i na to da direktno ne ukazuju na donete zaključke. Iz tih razloga je sve veći broj pokušaja da se poluautomatizuju alati za ekstrakovanje i analizu dokaza bez neophodnog suštinskog poznavanja rada alata.⁹

Digitalni forenzičari imaju pristup širokom spektru alata, kako komercijalnim, tako i onim koji su *open-source*, koji pomažu u očuvanju i analizi digitalnih dokaza. Nažalost, većina današnjih forenzičkih alata podbacuju u radu na nekoliko načina:

- ▶ Nisu u stanju da se izbore sa većim kapacitetom od ciljanih uređaja, akko kapaciteti rastu na stotine gigabajta ili terabajta, tradicionalni pristup koristi jednu stanicu kako bi izveo digitalnu istragu protiv jednog izvornog dokaza, ako što je hard disk.
- ▶ Veći ciljevi će zahtevati i sofisticiranije tehnike analize, kao što je na primer automatizovana kategorizacija slika. Na tržištu se pojavljuju alati, koji će moći da isprate rad kompjutera visokih performansi, poslužiće za dobijanje sofisticiranih dokaza, sve će ovo uticati da se temeljnije izvršavaju poslovi digitalnih forenzičara.

⁹ Kaurin Tanja, et., *Smernice za izbor alata digitalne forenzike*

U ovom poglavlju će biti objašnjeno delovanje i principi rada alata.

Širok spektar alata za digitalnu forenziku, kao što su komercijalni i *open-source*, su na raspolaganju forenzičarima. Ovi alati u različitom stepenu pružaju, određeni nivo apstrakcije koji omogućava da istražitelj bezbedno napravi kopije digitalnih dokaza i obavi rutinsku istragu, bez da bude preplavljen detaljima koji su bespotrebni ili su na niskoj lestvici kao dokazi. Mnogi postojeći alati pružaju intuitivan korisnički interfejs koji pretvara istragu u nešto nalik na struktuirani proces. Na žalost sadašnja generacija digitalnih forenzičkih alata podbacuje na nekoliko načina. Tradicionalni pristup korišćenja jedne stranice i izvršavanja istrage protiv nje, neće biti u potpunosti aktivan, jer postoje terbjati podataka, a za dobijanje čvrstih dokaza potrebna je sofisticiranija tehnika.

Ono što je potrebno da bi se neki forenzički alat koristio u istrazi, je da bude sertifikovan i priznat od državnih sudskih organa, kako bi digitalni dokazi bili validni u sudskom procesu.

U odeljku je dat pregled značajnijih inicijativa usmerenih na pokušaje standardizacije procesa validacije alata za digitalnu forenziku. U odeljku je objašnjen pojam digitalnog dokaza, njegove osnovne karakteristike i prihvatljivost na sudu. Digitalni dokaz je posmatran kao rezultat odabranog alata za digitalnu forenzičku istragu, pa su iz tog razloga navedeni uslovi koje digitalni dokaz treba da ispuni kako bi se na sudu smatrao prihvatljivim. U daljem delu su u kratkim crtama objašnjeni alati za digitalnu forenziku, njihova namena i podela. I dalje se prelazi na suštinu rada – prezentovanje smernica koje su prisutne u naučnim krugovima i imaju za cilj standardizaciju validacije i verifikacije alata za digitalnu forenziku.

4.1. Digitalni dokaz

Prema *National Institute of Justice-NIJ* (Electronic Crime Scene Investigation, 2008, p.ix) digitalni dokaz je definisan kao informacija i podatak od značaja za istragu, koji je uskladišten, primljen ili poslat preko elektronskog uređaja.

Druga definicija predložena od strane *Scientific Working Group on Digital Evidence* SWGDE (2009) kaže da je digitalni dokaz svaka informacija koja ima dokazujuću vrednost koja je uskladištena ili se prenosi u digitalnom obliku.

Zaključak je da digitalni dokaz može biti svaka informacija koja je generisana, obrađivana, uskladištena ili prenesena u digitalnom obliku, koju sud može smatrati merodavnom, tj. svaka binarna informacija, sastavljena od digitalnih 0 i 1, uskladištena ili prenesena u digitalnoj

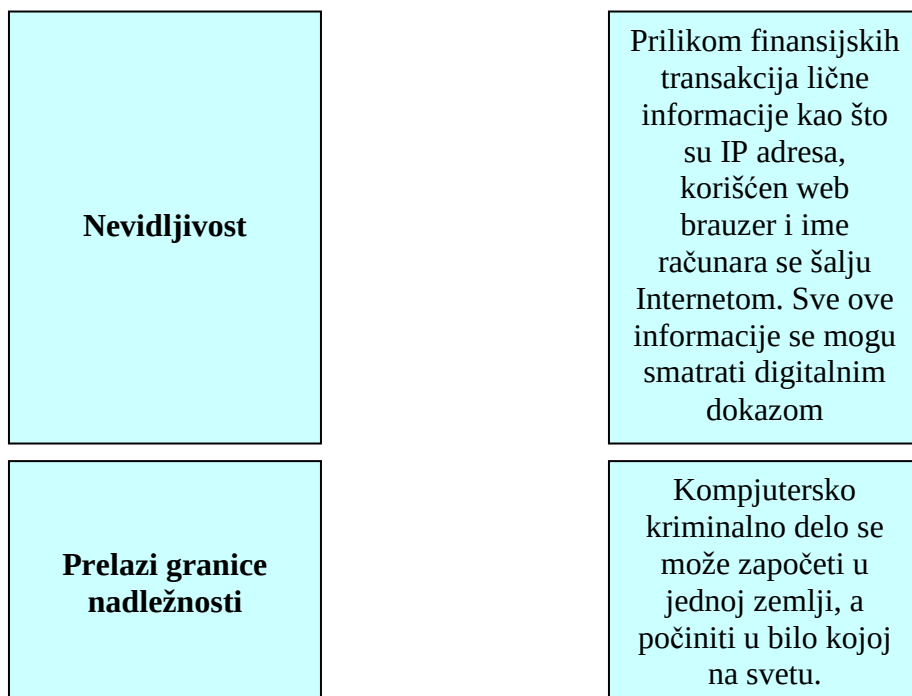
formi, kao i druge moguće kopije originalne digitalne informacije koje imaju dokazujuću vrednost i na koje sud se može osloniti, u kontekstu forenzičke aktivizacije, analize i prezentacije.

Digitalni dokaz se formira iz gomile posrednih stvarnih dokaza od kojih se ni jedan ne sme isključiti iz bilo kog razloga. Dokazi se moraju međusobno dopunjavati i ne smeju imati takozvane pukotine za donošenje zaključaka odnosno za utvrđivanje čvrstog digitalnog dokaza.

Digitalni dokaz je potreban ali ne i dovoljan uslov za građenje slučaja. Ovakvi dokazi su krhke prirode i lako mogu biti modifikovani, uništeni i izgubljeni. Upravo zbog njihove prirode nije dovoljno samo postojanje dokaza koji je rezultat forenzičkog alata i primenjenih forenzičkih tehnika već njihovo prihvatanje na sudu zahteva ispunjavanje određenih uslova.

U tabeli 5. predstavljeno je pet karakteristika digitalnog dokaza kako bi se bolje razumela njegova prihvatljivost na sudu kao i razlozi zbog kojih digitalni dokaz mora proći kroz različite testove kako bi bio validan. Uočljivo je da se integritet i tačnost digitalnih dokaza lako mogu kompromitovati.

Karakteristike digitalnog dokaza	Opis
Tehnološka naprednost	Prikupljanje i analiza digitalnih dokaza može biti izuzetno teški, jer često zahtevaju najnovije naučne metode i tehnologije
Fleksibilnost	Digitalni dokaz se može sastojati od svih vrsta elektronskih informacija.



Slika 5. Osnovne karakteristike digitalnog dokaza

Izvor: James Liang, Evaluating A selection of Tools for Extraction of Forensics, School of Computing and Mathematical Science, New Zealand, 2010.

U martu 1998. godine, International Organization of Computer Evidence (IOCE) je odlučio da formuliše međunarodne principe za postupke koji se odnose na digitalne dokaze, kako bi se obezbedila usklađenost metoda i prakse među narodima i garantovala mogućnost korišćenja digitalnih dokaza prikupljenih od strane jedne države u sudu druge države. Uzevši u obzir da upravo kod kriminalnih radnji počinjenih računarom raste stopa onih koji su izvršeni u više različitih zemalja čest je slučaj da prilikom istrage dolazi do razmene digitalnih dokaza.¹⁰

Da bi se digitalni dokazi što efikasnije razmenjivali, moraju biti zadovoljeni glavni principi:

- ▶ Konzistentnost sa pravosudnim sistemima u svakoj državi,
- ▶ Upotreba uobičajenog i razumljivog jezika
- ▶ Posedovanje trajne vrednosti
- ▶ Međunarodna prihvatljivost i priznavanje

¹⁰ James Liang, *Evaluating A selection of Tools for Extraction of Forensics*

- ▶ Ulivaju poverenje i štite integritet digitalnih dokaza
- ▶ Primenljivost na sve digitalne dokaze
- ▶ Primenljivost na pojedinca, zvanične agencije i najviši nacionalni nivo.

Iako je IOCE, propisala opšte principe i procedure za usaglašavanje metoda i praktičnih rešenja u vezi digitalnih dokaza, još uvek nigde u svetu ne postoji verifikacija zvaničnih istražnih organa, forenzičkih analitičara i pravosudnih organa, podjednako kvalifikovanih u svojim oblastima, da objektivno i tačno vode istragu, forenzičku akviziciju, analizu, dokazni postupak i prezentaciju digitalnih dokaza na sudu.

4.2. *Prihvatljivost digitalnih dokaza u sudnici*

Postojanje digitalnog dokaza odnosno, izvorno posmatrajući, postojanje kompjuterskog kriminala je unelo pometnju u dotadašnje procedure sudskog veštačenja i svedočenja. Forenzičar, umesto svedoka koji je lično video ili iskusio ono o čemu svedoči, postaje svedok iz druge ruke jer prezentuje digitalni dokaz koji se po tradicionalnim tumačenjima može smatrati posrednim dokazom.

Američko pravosuđe ima detaljan skup pravila i polisa u vezi prihvatljivosti bilo kog tipa dokaza i predstavlja trend kome teži pravosuđe većeg broja zemalja. Dva glavna uslova, u okviru američkog pravosuđa, za prihvatanje dokaza na sudu su:

- ▶ Federal Rules of Evidence koji se primenjuju na sve vrste dokaza i
- ▶ Daubert Challenge za naučnu prezentaciju dokaza od strane eksperta.

Pravilo najboljeg dokaza „the best evidence rules“ je definisano u tačkama 1001 do 1008. Po pravilima se najboljim dokazom koji treba biti korišćen na sudu smatra original, kopija nije dovoljna. Kada se radi o digitalnim dokazima tu pravilo 1001 definiše da se svaki štampani ili neki drugi izlaz čitljiv po viđenju ukoliko tačno odražava podatke može smatrati originalom.

Pravilo 901 je od izuzetne važnosti upravo za digitalne dokaze jer se odnosi na identifikaciju i autentifikaciju dokaza. Pod tačnim rezultatom podrazumeva se dokaz koji je proizvod

automatskog procesa a sistem je automatski autentičan ukoliko se pokaže da daje precizne rezultate.

Pravilo 702 se odnosi na eksperta-veštaka koji na sudu prezentuje dokaze. Takva osoba mora posedovati ekspertsko znanje, veštine, obuku ili obrazovanje iz konkretne oblasti. U svom svedočenju mora se oslanjati na pouzdane podatke i primenjivati pouzdane principe i metode na konkretne činjenice vezane za slučaj.¹¹

Drugi standard

Od 1923 do 1993 prihvatljivost naučnih dokaza testirana je Fraye standardom. Od 1993. Koristi se Daubert standard za prihvatljivost. Postoje četiri opšte kategorije Daubertovog procesa koje se koriste prilikom procene procedure korišćene za analizu dokaza, ali se često u literaturi navodi i peti:

- ▶ Da li teorija ili tehnika mogu biti testirane?
- ▶ Da li je poznata potencijalna stopa greške i njena egzistencija?
- ▶ Da li je tehnika objavljivana i dostupna javnosti?
- ▶ Da li je prihvaćena od strane relevantnih naučnih krugova?
- ▶ Da li postoje i da li su primenjeni standardi?

4.3. Alati za digitalnu forenzičku istragu

Za dobijanje digitalnih dokaza u forenzičkom postupku postoji mnogo razvijenih tehnika i alata koji se danas koriste, a njihov velik značaj povezan je sa činjenicom da je „danas preko 90 posto svih novih informacija proizvedeno u digitalnom obliku“, i da se takvo bogatstvo mora na adekvatan način kontrolisati, nadgledati i čuvati.

Razvoj forenzičkih alata usavršavao se kroz tri generacije. Prvu generaciju su sačinjavali razni alati za: slike, dokumenta, pretraživanje i oporavak sistema; drugu generaciju su činili posebno dizajnirani i razvijeni profesionalni alati (Encase, SANS, Helix itd.), kao i veliki broj besplatnih alata otvorenog koda koji se mogu naći i preuzeti sa Interneta; treću generaciju

¹¹ Kaurin Tanja, et., *Smernice za izbor alata digitalne forenzike*

čine inteligentni alati koji u realnom vremenu, bezbedno i efikasno nadgledaju celokupan mrežni saobraćaj.

Ono što je potrebno da bi se neki forenzički alat koristio u istrazi, je da bude sertifikovan i priznat od državnih sudskih organa, kako bi digitalni dokazi bili validni u sudskom procesu.

Uobičajena je sledeća podela alata:

Prema načinu implementacije:

- ▶ Hardverski
- ▶ Softverski alati

Prema tipu koda:

- ▶ Otvorenog koda
- ▶ Licencirani

Prema platformi na kojoj rade:

- ▶ Windows platforma i
- ▶ Linux platforma

Prema oblasti upotrebe:

- ▶ Forenzika računarske mreže
- ▶ Forenzika računarskog sistema
- ▶ Analiza drugih digitalnih uređaja
- ▶ Forenzika softvera.

Prema fazi procesa koji obavljaju u forenzičkoj istrazi:

- ▶ Formiranje sterilnih medijuma,
- ▶ Formiranje fizičke kopije čvrstog diska

- ▶ Oporavak podataka
- ▶ Dešifrovanje podataka
- ▶ Analiza digitalnog materijala
- ▶ Formiranje dokumentacije.

4.4. Metodologije za testiranje alata za digitalnu forenziku

Trend ubrzane pojave novih forenzičkih alata nameće potrebu za standardizacijom. Svakodnevno raste broj slučajeva u kojima se koriste digitalni dokazi. S obzirom da se nove tehnologije i novi alati stalno pojavljuju izuzetno je težak zadatak neprekidno biti u toku. Kako bi se na pravi način digitalni dokazi predstavili na sudu naučni principi o validnosti i prihvatljivosti dokaza moraju biti ispunjeni. Da bi se ti uslovi ispunili moraju postojati opšte prihvaćene smernice za ispitivanje forenzičkih alata. Na taj način bi se ukazalo na mogući procenat greške i dovelo do veće pouzdanosti analize digitalnih dokaza.

Koncept verifikacije i validacije softvera (V&V) je nastao krajem '60-tih. Tokom godina razvijani su razni modeli i standardi. Prema IEEE (1990) Standardni rečnik termina u softverskom inženjerstvu validaciju definiše kao „proces evaluacije sistema ili komponente u toku ili na kraju procesa razvoja kako bi se utvrdilo da li zadovoljava navedene zahteve“. Drugim rečima razvijen softver treba da zadovolji unapred postavljene zahteve.

Verifikaciju IEEE (1990) definiše kao „proces evaluacije sistema ili komponenti za utvrđivanje da li proizvod u datoj razvojnoj fazi zadovoljava uslove postavljene na početku te faze“. Može se reći da je verifikacija proces koji potvrđuje usklađenost softverskog alata sa zadatim specifikacijama.

Poštovanje V&V standarda omogućava dobru osnovu za prilagođavanje afirmisanih modela zahtevima digitalne forenzike.

U tekstu koji sledi izdvojene su neke od inicijativa predložene od akademske zajednice u svrhu pouzdane procene alata koji omogućavaju solidne osnove za veštačenje.

CFTT

Nacionalni institut za standarde i tehnologiju (NIST) je pokrenuo projekat pod nazivom „Projekat testiranja alata za računarsku forenziku“(CFTT). Cilj projekta je: utemeljenje metodologije za testiranje softvera za računarsku forenziku specificiranjem alata, testiranjem procedura, kriterijuma i hardvera. Rezultat projekta je opšta metodologija testiranja softvera za digitalnu forenziku koja se u velikoj meri zasniva na smernicama standarda ISO/IEC 17025 koji daje opšte zahteve za kompetentnost laboratorija za ispitivanje i kalibraciju.

Opšti pristup definisan NIST metodologijom:

- ▶ utvrđivanje kategorije forenzičkih zahteva
- ▶ identifikacija zahteva za određenu kategoriju
- ▶ razvoj testa provere tačnosti u skladu sa potrebama
- ▶ razvoj test koda za proveru tačnosti
- ▶ identifikacija relevantnih slučajeva testiranja
- ▶ razvoj procedura i metoda testiranja
- ▶ izveštaj rezultata testiranja

Na bazi ove metodologije u okviru CFTT projekta je testiran veliki broj alata i objavljeni su izveštaji testiranja. Opšta zapažanja NIST CFTT projekta su:

- ▶ Da je teško definisati i kvantifikovati stopu greške;
- ▶ Greška može imati teorijsku stopu greške;
- ▶ Implementacija algoritma može imati greške;
- ▶ Izvršenje procedure može imati grešku koja utiče na rezultat.

Testovi koje sprovodi CFTT su rigorozni i za druge organizacije izuzetno teški za ponavljanje zbog ogromne količine zadataka koji se izvršavaju. Na osnovu izveštaja CFTT projekta programeri mogu uočiti u kom smeru trebaju poboljšavati alate a korisnici dobijaju kvalitetne informacije na osnovu kojih mogu izabrati adekvatne alate. Za ostale zainteresovane strane izveštaji omogućavaju bolje razumevanje mogućnosti alata i pravnicima približavaju prihvatljivost digitalnost dokaza.

SWDGE Recommendations for Validation Testing

Drugačiji pristup dolazi od Scientific Working Group on Digital Evidence (SWGDE) koji su umesto testa specifikacije razvili smernice za testiranje validacije i šablone koji mogu biti od pomoći zainteresovanim stranama ili agencijama za sprovođenje zakona.

Smernice predstavljene u “2009-01-15 SWGDE Recommendations for Validation Testing Version v1.1” [11] su zapravo lista akcija koje treba sprovesti kako bi se kompletirao proces validacije. Smernice koje preporučuje SWDGE uključuju svrhu testiranja, obim, metodologiju, izbor test slučajeva.¹²

Testiranje po metodi predloženoj od Lynn M. Batten i Lei Pan

Nedostaci CFTT projekta su što su javno dostupni rezultati testiranja samo za najpoznatije alate kao i taj što je potrebno značajno vreme da se nakon pojavljivanja alata taj alat testira i pojave rezultati. To je glavni razlog zbog kog se novorazvijeni forenzički alati teško prihvataju.

Sa ciljem pomoći digitalnim forenzičarima prilikom izbora forenzičkih alata Lynn M. Batten i Lei Pan-a u svom radu “Testing Digital Forensic Software Tools Used in Expert Testimony” su dali predlog eksperimentalnog okvira. Namera je da se rezultati mogu koristiti od strane veštaka kako bi se opravdao izbor alata i eksperimentalne postavke, unapred izračunali troškovi testiranja i obezbedili kvalitetni rezultati. Proces počinje izborom alata koji će biti testiran, izborom važnih parametara i njihovim podešavanjem.

To se postiže u sledećim koracima:

- ▶ Na osnovu ovih alata i parametara vrši se izbor testiranja.
- ▶ Identifikacija outlejera jer se greška u eksperimentu može pojaviti zbog ljudske greške ili netačnog alata za merenje.
- ▶ Smanjenje negativnog uticaja outlejera na bezbedan nivo tako da je moguće doneti korektan zaključak.

¹² Kaurin Tanja, et., *Smernice za izbor alata digitalne forenzike*

U poslednjoj fazi testiranja ispitivač dobija kompletan set zapažanja koja treba obraditi adekvatnim statističkim alatima.

A Common Evaluation Scheme For Forensic Software (COSEFOS)

Grupa autora iz Nemačke je na Sixth International Conference on IT Security Incident Management and IT Forensics prezentovala rad u kome je ponudila svoje rešenje A Common Evaluation Scheme For Forensic Software (COSEFOS).

Ovo rešenje u osnovi ima dva cilja:

1. Ispitivanje adekvatnosti svakog pojedinačnog alata za digitalnu forenziku. Njegova Efikasnost, kvalitet rezultata i potencijalne greške.
2. Istražiti integraciju u forenzičkom procesu. Ovim je uključeno i moguće sudsko odobrenje za prikupljene podatke.

U tabeli 2. nalazi se predložena šema.

Uočljiva je podela na Hard-criteria i Soft-criteria. Provera ispunjenja Hard-criteria je moguća testiranjem i nepromenjiva je za određenu verziju određenog alata. Sa druge strane Softcriteria nisu merljivi, subjektivni su, zavise od sudije i nije moguće dodeliti im čak ni težinske faktore. Hard-criteria obuhvata tri grupe kriterijuma Must, Should i Can. Must-criteria, se odnosi na osnovnu funkcionalnost softvera i ukoliko nije zadovoljena zaključuje se da softver nije pogodan za istragu. Po preporuci autora ovde treba ispitati:

- ▶ reproduktivnost rezultata,
- ▶ moguće greške koje se mogu pojaviti,
- ▶ učestalost tih grešaka i
- ▶ njihov značaj.

Hard-Criteria	Soft-Criteria
Must-Criteria Osnovne funkcije Should-Criteria Logovanje Zaštita integriteta prikupljenih podataka Zaštita autentičnosti prikupljenih podataka Zaštita poverljivosti prikupljenih podataka Ograničenje pristupa prikupljenim podacima Zaštita integriteta izvora podataka Can-Criteria Heterogenost sistema Minimalizacija neophodnih sistemskih zahteva Open source	Opšte prihvatanje u okviru stručne javnosti Objavljivanje metoda Standardi za korišćenje aplikacije Razlog istrage Odlično poznavanje aplikacije

Tabela 2. Predložena šema za COSEFOS

Izvor: M. Hildebrant, S. Kiltz, and J. Dittmann, "A common scheme for evaluation of forensic software"

Reproduktivnost rezultata je najvažnija mogućnost koju treba da ponudi forenzički alat. Ukoliko se određeni alat ponaša nedeterministički smatra se neadekvatnim za forenzičke istrage jer nije moguće utvrditi validnost rezultata.

Soft-criteria su neophodni za sudske istrage. Moguće je imati potrebne alate u okviru samog forenzičkog softvera ili koristiti spoljne. Prva opcija je bolja jer bi se na taj način ispunio uslov 901 Federal Rules of Evidence.

Konačno, Can-criteria su motivisani potencijalnim pretnjama za forenzički softver. Ovo je opciona skup kriterijuma. Njima je moguće pozabaviti se tokom istrage, kako bi se npr. omogućila detaljnija istraga.

5. Značaj proaktivne forenzike za bezbednost Informacionih sistema

5.1. Teorijske osnove

Digitalna forenzika je relativno mlada nauka. Od pojave računara i njihovog povezivanja došlo je do stvaranja informacionog i globalnog okruženja . Sada jedan deo populacije je sve ovo iskoristio u pogrešne svrhe i da na nezakonit način koristi računare kao i Internet. Tada se pojavljuje Digitalna forenzika kao nauka, da bi sprečila svako nezakonito delo koje je bilo u planu da se učini, ili da nađe nepobitne dokaze o već učinjenom delu. Kako su se razvijali računari, a samim tim i njihovo povezivanje, tako se razvijala i digitalna forenzika. Takođe se moralo voditi računa i o obrazovanju i edukovanju forenzičara. Digitalna forenzika se i dan danas razvija, jer je relativno mlada nauka i uvek mora pratiti inovacije koje se uvode u svetu računara, informacionih sistema i na samoj Globalnoj mreži. Takođe mora pratiti i prikupljati razna saznanja, a najviše pratiti antiforenzičko razvijanje kako bi mogla lakše i brže da prikuplja dokaze i da stane na put nezakonitim delima.

U ovom radu se opisuje rad proaktivne forenzike, kao i sam uticaj antiforenzičkih alata, jer sa druge strane postoji osoba koja je izazvala incident, koja može biti needukovana, ali moramo imati u vidu da može biti i jako dobar poznavalac napada, pa samim tim i znati kako u određenom trenutku da upotrebi aqnti forenzički alat. Kada se spomenu kateorije kompjuterskog kriminala, onda se može reći da su to sredstva kojima se napad izvršio, kako hardverski uređaji, tako i softverska rešenja nehik programera koji mogu da olakšaju napad, ali koja takođe mogu da nannesu ogromne štete kako pojedincu tako i velikim kompanijama. Skladištenje informacija je bitna stavka za digitalnog forenzičara, jer pomoću njih on može izvući potrebne informacije o delu koje je nezakonito izvršeno i to može biti dokaz za osumnjičenog. Neki od tipova kompjuterskog kriminala može biti neovlašćen pristup drugom računaru, bazi podataka, ali takođe i zloupotreba lozinki kao i kompjuterska špiunaža. Ljudi koji rade kaoo digitalni forenzičari moraju se konstantno edukovati, jer u suprotnom postojaće problema pri prikupljanju dokaza koji su u većini slučajeva apstraktni. Dokazi su uglavnom binarni, koriste se 0 i 1. Skup binarnih brojeva čine niz, a njime se mogu opisati razni folderi kao i fajlovi koji sadrže aplikacije, slike ili neke druge dokumente koji su bitni dokazi i koji

mogu da se uklone pomoću određenih alata, zato forenzičar mora biti dobro edukovan da zna kako da reaguje u određenim situacijama kako bi došao do dokaza, a samim tim i do osuđivanja počinioca za nezakonito delo.

Digitalni dokaz je svaka informacija koja ima dokazujuću vrednost, a koja je uskladištena ili snimljena u digitalnoj – binarnoj formi. Ovom vrstom dokaza se smatraju i informacije koje mogu biti i prenešene sa jednog na drugi računar ili nekog drugog prenosivog uređaja. Postoji i originalni digitalni dokaz, a njega čini svaka informacija koja se nalazi snimljena na računaru koji je fizički privremeno oduzet u toku istrage i biće iznešen na sud, kao dokazni materijal. Duplikat digitalnog dokaza u njega spadaju svi digitalni dokazi koji su kopirani sa originalnog digitalnog dokaza. Kako postoje digitalni dokazi, tako postoje i fizički koji mogu biti prikupljeni na licu mesta gde se odvijao incident. Kombinovanjem dokaza mora se voditi računa da se celokupan slučaj incidenta opiše., kako bi prikupljeni dokazi bili validni i neoborivi pred sudom. Opis procedure mora imati svaki digitalni dokaz koji opisuje korake i mere opreza pod kojim se digitalni dokaz koristio u istrazi. Postoje ograničenja koja opisuju opremu koja nije validna kada se vrši ispitivanje. Forenzički alati moraju biti prihvatljivi pred sudom, merodavni su : EnCase i FTKImager.

Ljudi koji koriste forenzičke alate su:

- ▶ Istražitelji – koriste brojne alate kao i tehnike
- ▶ IKT profesionalac – koristi mali broj forenzičkih alata i tehnika i to uglavnom iz njima bliskih oblasti
- ▶ Tim ili ekipa – koriste veliki broj alata i tehnika, jer su obučeni da prate različite kompjuterske incidente.

Proaktivna digitalna forenzika (ProDF) predstavlja proširenu granu standardne digitalne forenzičke istrage, čiji je osnovni cilj da se organizacija pripremi za digitalnu forenzičku istragu, ili za testiranje otpornosti sistema na napad, i to pre nego što dođe do napada.

Proaktivna digitalna forenzička istraga (ProDF) obezbeđuje neophodne procese, procedure, tehnologije i sveobuhvatne digitalne dokaze. Neophodno je razmotriti sledeće ciljeve proaktivne digitalne forenzičke istrage:

- ▶ Sremnost za digitalnu forenzičku istragu
- ▶ Poboljšanje upravljačke strukture u organizaciji

- ▶ Poboljšanje Info Sec/IT performansi sa korišćenjem odgovarajućih alata digitalne forenzike za poboljšanje efikasnosti i efektivnosti u organizaciji.

Model digitalne forenzičke istrage se takođe često pominje i predlažu se različite dimenzije elemenata i većina modela se koncentriše na pitanja:

- ▶ Ko?
- ▶ Šta?
- ▶ Zašto?
- ▶ Kako?
- ▶ Kada?
- ▶ Gde?

Predlažu se sledeće dimenzije za digitalnu forenzičku istragu:

- ▶ Upravljanje – odgovor na pitanje “Zašto”, razmatra upravljanje objektima, parametrima i bave se upravljanjem rizika i operativnim rizicima,
- ▶ Pravo – odgovor na pitanje “Zašto” i bavi se saglasnošću,
- ▶ Ljudi – odgovor na pitanje “Ko”
- ▶ Procesi – odgovor na pitanja “Kako”, “Kada”, i “Gde” i povezuju korišćene aplikacije i tehnologije.

Pored proaktivne forenzičke istrage postoje još dve komponente digitalne forenzičke istrage:

- ▶ **Aktivna ili “live”** digitalna forenzička istraga (ActDF) koja predstavlja sposobnost organizacije da prikupi relevantne dokaze (CDE), zatim da se umanjí efekat incidenta koji je u toku i omogućuje uspešnu istragu.
- ▶ **Reaktivna ili “dead”** digitalna forenzička istraga (ReDF) sastoji se od analitičkih i istraženih tehnika koje se koriste za zaštitu, identifikaciju, dokumentaciju, analizu i interpretaciju digitalnih medija koji su digitalno sačuvani i sakupljeni kao dokaz za olakšanje ili pomoć u rekonstrukciji incidenta.

Aktivna i reaktivna komponenta digitalne forenzičke istrage razlikuju po načinu upravljanja dokazima, procesima, alatima i primenjenim protokolima istrage. Istraga zahteva korišćenje forenzičkih alata i njihovu primenu u celokupnom toku istrage. Forenzički alati kao i tehnike digitalnog forenzičara, koriste se u slučajevima kada treba da se eliminiše očiglednost, postavljanje hipoteza o napadu, rekonstrukcije krivičnih dela i otkrivanje traga do osumnjičenog računara. Tada se vrši analiza određenog računara, ali i onih računara koji su neposredno korišćeni u toku nezakonite radnje. Najbitnije je da se svi dokazi prikupe i celokupni sadržaj predate zvaničnim organima, ako je ugrožena javna ili državna bezbednost. Digitalni dokazi su apstraktni i s njima se može lako manipulirati raznim operacijama koje mogu da dupliraju ili da ih uklone sa samog računara. Forenzički procesi ispitivanja i analize u digitalnoj forenzičkoj istrazi, zasnivaju se na informacijama koje su nekompletne ili ih proizvodi forenzički alat koji sam može biti kompromitovan. Primena forenzičkih tehnika takođe utiče na analizu. U klasičnoj digitalnoj forenzici, neaktivna ili statička forenzika, u procesu ispitivanja gubi se većina informacija iz radne memorije (RAM).¹³

5.2. Slojevit pristup kod detekcije spoljašnje pretnje i proaktivne forenzike

Spoljašnja pretnja, je pretnja na samu bezbednost računara i ona je rezultat neovlašćenog pristupa i zloupotrebe, od strane korisnika ili organizacija. Spoljašnji napad može biti destruktivan i napadač često ima pogodan pristup organizacijama i resursima samih računara. Jedan od napada je upad u sisteme detekcije, kao crne kutije i forenzičke alate. Rano otkrivanje i dokumentovanje prekršaja spoljašnjih upada, je od vitalnog značaja za forenzičare. Sam IDS možda neće biti pogodan za ovo korišćenje iz sledećih razloga:

- ▶ Tačnost detekcije: na IDS može prevideti realne pretnje ili problem oko upozorenja na normalni događaj. Potpis na bazi ID (SID) identifikuje obrasce ali ne uspeva da uhvati put ponašanja. Anomalija zasnovana na ID je osetljiva na lažne alarme zbog teškoća u razlikovanju napada od brojnih anomalija. Lažni negativni su više štetni nego lažne uzbune zbog njihove destruktivne prirode. Lažne uzbune su manje hitni

¹³ Bayuk Jennifer, (2010), *Cyber Forensics Understanding Information Security Investigation*

problemi, ali ništa manje problematični jer troše resurse potrebne za njihovu verifikaciju. Lažno pozitivan može zatražiti IDS da sakupi beskorisne podatke.

► Troškovi: razlikujemo ID srodne troškove u:

- ◆ Troškove oštećenja
- ◆ Odgovor troškova
- ◆ Operativni troškovi

Prikupljanje podataka o sumnjivim korisnicima je skupo i pri tom treba voditi računa da se sam korisnik ne uznemorava. Treba u većini slučajeva naći kompromis između cene i preciznosti detekcije. Praćenje je popularna strategija i koristi se za detekciju. U idealnom slučaju IDS treba da koristi i prati najmanju moguću količinu sistemskih resursa na hostu ili mreži. Isto tako tajno prikupljanje podataka i aplikacija, forenzički alati treba da ih što bolje detektuju. Njegovi operativni troškovi treba da budu svedeni na minimum da ne bi uticali na normalnu upotrebu sistema i da bi se ipak postigli željeni rezultati. Spoljnje pretnje karakteriše više stvari: kvalitet, dizajn i pretpostavka. Zlonamerni činilac cilja da ima više znanja i mogućnosti za praktični pristup od čoveka koji brani sistem. Zbog takvih pristupa, on nekada mora koristiti nove tehnike napada ili poboljšati stare tehnike, ali administrator mora voditi računa o tome i imati mogućnosti da preduhitri napadača.

Pošto je proaktivna bezbednost nesavršena i nekada stvara greške, računarski bezbednosni sistem mora da ima sposobnost da prikupi i sačuva važne dokaze koji se kasnije mogu staviti u razmatranje zbog krivičnog gonjenja.

Termin „Proaktivna forenzika“ je korišćen od strane nekih komercijalnih proizvođača forenzičkih proizvoda. Softveri pomažu pri procesu istrage i proaktivne mrežne aktivnosti. Mada ova definicija može da se proširi i u izgradnju, projektovanje i konfigurisanje sistema koji je najviše podložan analizama digitalne forenzike.

5.3. Mrežna forenzika i istraga Log fajlova

Mrežna forenzika snima i analizira događaje na mreži kako bi otkrila izvor napada. Snimanje mrežnog saobraćaja, preko mreže je jednostavnije u teoriji, ali je u praksi jako složen. To se dešava zbog velike količine podataka koji protiču kroz mrežu i složenosti prirode Internet protokola. Snimanje mrežnog saobraćaja uključuje mnoge resurse, pa neke podatke je nemoguće snimiti. Istražitelj treba da napravi rezervnu kopiju snimljenih podataka da bi se oslobodio prostor za čuvanje podataka za buduće analize.

5.3.1. Analiza mrežnih podataka

Analiza snimljenih podataka je jako dugotrajan proces. Iako postoji puno automatizovanih alati za analizu podataka, koje istražitelji mogu i da koriste u ove svrhe, ponekad oni nisu dovoljni, jer ne postoje nepogrešive metode za odstranjivanje lažnog saobraćaja generisanog od strane napadača, i prepoznavanje pravog saobraćaja. Presuda forenzičara je kritična, jer se postoji šansa da neki od forenzičkih alata da lažno pozitivan rezultat istrage. Istražitelj treba da izvrši forenziku mrežnog saobraćaja, i same mreže da bi odredio tip napada preko mreže i da uđe u trag krivcu. Istražitelj treba da prati odgovarajuće istražne procedure tako da dokazi budu validni na sudu.¹⁴

Mrežna forenzika može otkriti sledeće informacije:

- ▶ Put napada
- ▶ Koje tehnike napadač koristi
- ▶ Tragove i dokaze

Mrežni forenzičar ne može i ne sme uraditi sledeće:

- ▶ Samo rešiti slučaj

¹⁴ Garza Dave, Kane Matthew, et, *Computer Forensic Investigation Wireless Networks and Devices*.

- ▶ Koristiti link osumnjičenog za napad

Proces upada su sledeći:

Mrežni napadači mogu ući u sistem koristeći sledeće metode:

- ▶ Nabranje: ovo je proces prikupljanja informacija o mreži koje mogu da pomognu napadaču da napadne mrežu. Ovaj metod se uglavnom obavlja preko Interneta.

Sledeće informacije se prikupljaju tokom popisivanja:

- ▶ Topologija mreže
- ▶ Spisak hostova
- ▶ Mrežna arhitektura i vrsta saobraćaja (npr: TCP, UDP i IPX)
- ▶ Potencijalni propusti u host sistemima
- ▶ Ranjivosti: napadač identifikuje potencijalne slabosti u sistemu, mreži i elementima mreže, a zatim pokušava da iskoristi te ranjivosti, za ranjivosti može koristiti razne skenere.

5.4. Log fajlovi

Log datoteka je zapis događaja u računarskom sistemu ili mreži. Svaki zapis sadrži informacije relevantne za specifičan događaj, uspešne ili neuspešne pokušaje prijavljivanja, korišćenje resursa kao što su kreiranje, otvaranje ili brisanje datoteka. *Log* datoteke su prvobitno korišćene za rešavanje problema računarskog sistema, ali danas se koriste u mnogo veće svrhe jer imaju mnogo više funkcija. Koriste se za optimizovanje sistema i mreža, za praćenje ponašanja korisnika i generisanje podataka korisnih za istraživanje aktivnosti malicioznih programa. Vremenska evidencija je najbolji dokaz za zaključivanje o incidentu. Ako se obezbedi dokaz o vremenskoj liniji upada u sistem, u svim Log fajlovima mrežnih uređaja i napadnutog računara, onda je čvrst dokaz za slučaj. Treba imati na umu da se vreme i datum lako menjaju, pa je potrebno ovaj dokaz podupreti sa drugim dokazima iz napadnutog

računara. Log fajlovi se mogu smatrati za očevice digitalnog krivičnog dela i moraju biti obezbeđeni ukoliko postoji pretnja da mogu biti izbrisani, pre nego što se sistem fizički iskopira. Sistemski log fajlovi obezbeđuju brojne dokaze o upadima u mrežu i host računare. Ova vrsta dokaza ima svoja ograničenja: Mora se na sudu dokazati da log fajl nije izmenjen. Log datoteke sadrže veliki broj različitih informacija, te ih možemo podeliti u nekoliko kategorija u odnosu na servise koji su instalirani.

- *Sigurnosni softveri (programi zaštite)* – najčešće se koriste za detekciju aktivnosti malicioznih programa, kao i zaštitu sistema i podataka. Predstavlja glavni izvor sigurnosnih log datoteka.

Tipovi sigurnosnih softvera su:

- ▶ Softver za zaštitu od malicioznih programa,
 - ▶ Softver za detekciju i sprečavanje upada u sistem – IDPS (*Intrusion Detection and Prevention System*),
 - ▶ Softver za kontrolu udaljenog pristupa,
 - ▶ Web proxy,
 - ▶ Softver za upravljanje ranjivostima,
 - ▶ Autorizacioni server,
 - ▶ Ruteri,
 - ▶ Zaštitne barijere (*Firewalls*),
 - ▶ Mrežni karantinski serveri.
- *Log datoteke operativnog sistema.* OS beleži različite informacije koje se odnose na sigurnost. Najčešće se susrećemo sa: sistemskim događajima, kontrolnim zapisima.
 - *Log datoteke nastale korišćenjem aplikacija.* OS i sigurnosni softver služe da obezbede zaštitu za aplikacije koje skladište, omogućavaju obradu i pristup podacima. Najčešće se koriste *off-the-shelf* komercijalne aplikacije, kao što su e-mail serveri i klijenti, fajl serveri i klijenti, serveri baze podataka. Često se koriste i aplikacije ove vrste, kao što su podrška finansijskom menadžmentu, proceduralni sistem, ERP, i dr.

5.5. Konfigurisanje Log datoteka

Administrator sistema mora konfigurisati log datoteke, da bi se evidentirale neophodne informacije u željenom formatu i na definisanoj lokaciji. Potrebno je obezbediti da se te informacije i čuvaju određeni vremenski period. Konfigurisanje *log* datoteka je veoma složen i zahtevan proces. Prvo što administrator treba da otkrije jeste koji izvor podataka za log datoteke koristi svaka pojedinačna log datoteka. Svaka log datoteka sadrži informacije iz više izvora. Log datoteka operativnog sistema, sadrži informacije samog operativnog sistema, sigurnosnog softvera, i informacije koje su nastale korišćenjem aplikacija. Za svaki prepoznati izvor log datoteke, administrator mora odrediti koji tip događaja svaki izvor log datoteke mora ili treba da beleži. Administrator mora da odredi koje karakteristike podataka moraju ili bi trebalo da budu beležene za svaki tip događaja. Sposobnost administratora da konfiguriše svaki izvor log datoteka, zavisi od mogućnosti koje nudi određeni tip izvora log datoteka.¹⁵

Konfigurisanje izvora log datoteka možemo razvrstati u tri kategorije:

1. Kreiranje izvora log datoteka,
2. Čuvanje i uništavanje izvora log datoteka
3. Zaštita izvora log datoteka

5.6. Potraga za dokazima

Istražitelj može naći dokaze prateći sledeće opcije:

- ▶ Pomoću napadnutog računara i intermedijalnih računara. Ovo je vrsta dokaza u obliku fajlova, okruženja podataka i alata.
- ▶ Pomoću *firewall-a* istražitelj može pogledati na disku zaštitnu barijeru, ako je on bio žrtva napada, istražitelj ga tretira kao bilo koji drugu zaštitnu barijeru pri prikupljanju dokaza.

¹⁵ Garza Dave, Kane Matthew, *Computer Forensics Investigation Wireless Networks and Devices*

- ▶ Pomoću napadnutog računara, istražitelj može doći do dokaza u log fajlovima, datotekama, promenama konfiguracije datoteka, ostacima trojanskih datoteka, datotekama koje se ne podudaraju sa *hash* podešavanjima, alatima, virusima i ekstenzijama nepoznatih fajlova.

5.7. *End-to-End forenzička istraga*

Ova forenzička istraga obuhvata sledeće osnovne procedure od početka do kraja:

- ▶ end-to-end koncept: on prati sve elemente napada, uključujući i to kako je napad počeo, koji se uređaji koriste prilikom napada, a koji su napadnuti.
- ▶ Lociranje dokaza: kada istražitelj zna koji su uređaji korišćeni prilikom napada, i pomoću toga oni mogu tražiti dokaze. I dalje analiziraju te dokaze da bi saznali više o samom napadu i napadaču.
- ▶ Klopka za prikupljanje mrežnih dokaza: dokazi mogu biti izgubljeni za nekoliko sekundi tokom analize log-a jer se sama struktura stabla poremeti. Ponekad dozvola za prikupljanje dokaza sa određenih izvora nije potrebna kao što je ISP- Ovaj proces može potrajati, što povećava šanse za gubitak dokaza.

Ostale zamke uključuju sledeće:

- ▶ Istražitelj ili administrator mreže može zameniti računar ili mrežne aktivnosti za aktivni napad
- ▶ Nekad može biti praznine u lancu dokaza
- ▶ Zapisi nekada mogu biti dvosmisleni, nepotpuni ili nekada može da se desi da neki dokazi nedostaju.
- ▶ Nekada se može desiti da i drugi narodi budu uključeni u istrau. Ovo može stvoriti neke probleme oko pravnih i političkih pitanja oko istrage.

- ▶ Analiza događaja: istražitelj ispituje sve informacije, pravi korelaciju svih događaja ili podataka iz različitih izvora da bi dobio kompletnu sliku nekog napada i dokaza.

5.8. Log fajlovi kao dokazi

Log fajlovi su primarni za snimanje aktivnosti korisnika na sistemu, kao i na samoj mreži. Istražitelj može otkriti izvor nelegalnih aktivnosti koristeći dnevnike. Osnovni problem sa log fajlovima je da se oni mogu lako menjati. Napadač može lako ubaciti lažne ulaske u ove fajlove.

Istražitelj mora biti u stanju da dokaže na sudu da je prijavljena verzija softvera za korišćenje ispravna. Ponekad kompjuterski zapisi su teško prihvatljivi kao dokaz, oni moraju da ispunjavaju određene kriterijume da bi bili prihvaćeni. Tužilaštvu moraju biti predstavljeni na odgovarajući način i samo svedočenje mora dokazati da su ovi dokazi tačni, pouzdani i potpuno verodostojni originalu. Svedok mora da overi evidenciju računarskih podataka koji se iznose kao dokazni materijla.

Zakovitost korišćenja Log fajlova

Slede neka od pravnih pitanja koji se bave kreiranjem i korišćenjem logova koje organizacije i istražitelji moraju imati na umu:

- ▶ Log mora biti kreiran istovremeno sa događajem pod istragom
- ▶ Log fajlovi se ne mogu dirati
- ▶ Stručno lice mora evidentirati informacije. Programi rade snimanja, a kasnije programeri i sistem administratori obrađuju podatke
- ▶ Nasumične zbirke podataka nisu prihvatljive
- ▶ Log pokrenut nakon incidenta ne ispunjava uslove

- ▶ Ako organizacija počinje redovno vođenje evidencije, to će se kasnije moći koristiti kao dokazni materijal
- ▶ Kvalifikovani svedok mora svedočiti o tačnosti evidentiranih podataka. Ovo je proces potvrde identiteta. On mora znati koji se softver koristio pri istrazi i koliko su zapisi pouzdani. Oni moraju znati koja se hardverska i softverska platforma koristi u toku istrage.
- ▶ Odbrana može dati priliku da se ispita verodostojnost podataka i zapisa. organizacija može pokazati da su relevantni programi poslovna tajna, organizaciji može biti dozvoljeno da ih zadrži kao tajne.
- ▶ Originalne kopije kao podaci imaju prednost.

5.9. Ispitivanje upada i bezbednost događaja

Ranije je rečeno da pregled log fajlova može da otkrije upad ili napad na sistem. Monitoring za upad i događaje koji ne poštuju bezbednost je neophodan da bi se ušlo u trag napadačima. Ispitivanje upada i bezbednost događaja uključuje i pasivne i aktivne poslove. Upad koji se koristi posle napada zove se post-napad i koristi se za detektovanje upada i njegovo otkrivanje. U tim slučajevima kontrola log datoteke je jedini način koji se može iskoristiti da bi se otkrio napad. Pasivne tehnike za detekciju upada uključuju preled evidencije događaja. Istražitelj pregleda i analizira podatke o događajima i pokušava da nađe obrazac napada. S druge strane postoje napadi koji se lako otkrivaju čim krene njihovo odvijanje. Ovaj tip detekcije napada je poznat kao **aktivna** detekcija upada. Koristeći ovu metodu administrator ili istražitelj prati korake napadača i traži poznate obrasce napada da bi blokirao izvršenje napada.

Detekcija upada je proces praćenja neovlašćenih aktivnosti korišćenjem tehnika, kao što su ispitivanje korisnika akcije, bezbednost, revizija podataka. Postoje razne vrste upada, uključujući i neovlašćen pristup fajlovima i sistemu, crve, trojance, kompjuterske viruse, napade pomoću prelivanja bafera, preusmeravanja identiteta, prisluškivanje mrežnog saobraćaja. Ovi napadi se mogu takođe pojaviti i u vidu uskraćivanja usluga ili oštećenja podataka. Upad može rezultirati promenom korisničkih prava i promenom bezbednosti

datoteka, instaliranjem trojanskih datoteka ili nepravilnog pristupanja podacima. Administratori koriste razne tehnike za detekciju upada, uključujući u to procenu sistemskih loova i podešavanja, kao i postavljanje zaštitnih zidova, antivirusnih softvera za specijalizovanu detekciju neovlašćenih upada. Administrator mora da istraži svaki neovlašćeni ili zlonamerni ulazak na mrežu ili host.

5.10. Prednost razumevanja Log datoteka

Da bi se izvela log analiza, potrebno je poznavati aktivnosti vezane za svaki sistem. Neki od log podataka su veoma jednostavni za razumevanje, dok su drugi krajnje komplikovani. Za ovo postoji više razloga:

- ▶ **Poznavanje konteksta.** Značenje log podataka zavisi od konteksta. Potrebno je da administratori dobro poznaju kako je definisan kontekst. Kontekst određuje ispravnost pouzdanosti log podataka. Administratori računarske mreže pomažu administratorima računarskog sistema pri analizi log podataka pojašnjavajući kontekst.
- ▶ **Nejasne poruke.** Log podaci mogu sadržati kodove ili poruke koje su značajne za prodavce softvera, ali ne i za administratore. Koristeći **SIEM** (*Security Information and Event Management*) softver za analizu log datoteka smanjuje se broj ovakvih poruka.

U nekim slučajevima nije moguće postići potpuno razumevanje log podataka. Izvor log podataka nekada ne može da zabeleži neophodne podatke za obezbeđivanje konteksta za razumevanje log podataka. Najbolji način za razumevanje ovih podataka jeste da se pregled i analiza vrše periodično i konstantno. Cilj je da se obezbedi razumevanje tipičnih log podataka, obuhvatajući najbitnije log podatke za sistem. Dnevni pregled podataka bi trebalo da uključuju one podatke koji se smatraju važnim. Upravo ovakva analiza log podataka zahteva najviše vremena i predstavlja najveći izazov. Vremenom, kada osnovne aktivnosti postanu već jasne, dnevni pregled i analiza zahtevaju manje vremena i fokus analiza se usmerava na najbitnije log podatke, što dovodi do kvalitetnije analize log podataka.

Razumevanje log podataka je olakšan u toliko što proces analize log podataka može da se automatizuje. Određivanjem koji tipovi log podataka su važni, a koji nisu, administratori mogu da konfigurišu filtere log podataka prilikom automatizacije. Ovim se omogućava da maliciozni programi budu odmah prepoznati i prikazani. Filtriranje je bitno da bi se obezbedilo da ručna analiza administratora bude prioriteta na odgovarajući način. Filtriranje bi trebalo da bude konfigurisano tako da omogući administratorima da za odgovarajući broj podataka izvrše ručnu analizu. Najbolja tehnika je da postoje dva izveštaja, jedan za podatke koji su najbitniji, drugi za one koji nisu u potpunosti razumljivi. Oba izveštaja je potrebno generisati periodično, ali bi prvi izveštaj trebalo da bude od veće važnosti. Drugo izveštaj je bitno generisati da bi se obezbedilo prepoznavanje podataka koji su najbitniji.

5.11. Tačnost log fajlova

Tačnost IIS log datoteka određuje njihov kredibilitet. Tačnost, ovde znači da su fajlovi predstavljeni kao stvarni ishod aktivnosti vezanih za IIS servere pod istragom. Bilo koja modifikacija na disku izaziva validnost delog log fajla koji se predstavlja kao osumnjičeni.

Da bi se osigurala tačnost log fajla administrator mreže mora prijaviti sve. Određena polja u IIS log datotekama možda izgledaju manje značajna, ali svako polje može da napravi veliki doprinos kao dokaz. Mrežni administrator treba da konfiguriše svoj server IIS log fajlovima i da snimi svako polje koje je na raspolaganju.

IIS logove mora da evidentira kao i podatke o korisnicima WEB-a, tako da podaci daju nagoveštaje o tome da li je napad došao od prijavljenih korisnika na sistem ili nekog drugog korisnika ili sistema. Napadač koristi zadnja vrata proxy-a da napadne druge sisteme.

Sledeći koraci objašnjavaju kako omogućiti prijave za IIS Web/FTP server i promene lokacija na log fajlovima:

- ▶ Pokreće se Internet Service Manager
- ▶ Odabiraju se podešavanja na Web/FTP serveru
- ▶ Selektuje se Web lokacija ili FTP check box
- ▶ Bira se W3C Extend Log File format sa padajuće listre

- ▶ Odlazi se na Properties.
- ▶ Kliknete na karticu Extended Properties, i shodno tome postavljaju se sledeća svojstva:
 - o Korisničko ime
 - o Metod
 - o URI stem
 - o HTTP status
 - o Win32 status
 - o User agent
 - o IP adresa servera
 - o Port servera
- ▶ Biramo Daily za New Long Time Period koji se nalazi ispod opšte kartice Svojstva
- ▶ Biramo Use local time za imenovanje datoteka
- ▶ Menja se direktorijum log datoteke na lokaciji
- ▶ Provera da NTFS bezbednosne postavke imaju sledeća podešavanja:
 - o Administratori imaju punu kontrolu
 - o System- potpuna kontrola.

Vreme zadržavanja

Sa vremenskim Windows servisima, mrežni administratori mogu sinhronizovati IIS servere i povezati ih na spoljni izvor vremena. Administrator mreže može sinhronizovati samostalni server na spoljni izvor vremena, postavljanjem određenih stavki registara:

Key: HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\

Setting: Type

Type: REG_SZ

Value: NTP

Key: HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\

Setting: NtpServer

Type: REG_SZ

Value: ntp.xsecurity.com

5.12. Pregled Web Log-a

Ivor, priroda i vreme nekog napada, može se odrediti analizom log fajlova samog kopmpromitovanog sistema.

Windows 2003 server ima sledeće logove:

- ▶ Primenu dnevnika, skladištenje događaja vezanih za aplikacije koje rade na serveru
- ▶ Evidencija bezbednosnih događaja i skladištenje događaja vezanih za reviziju
- ▶ Sistem dnevnika, skladištenje događaja vezanih za Windows komponente i usluge
- ▶ Direktorijum servis dnevnika, skladištenje aktivnog direktorijuma i dijagnostiku informacija o greškama.
- ▶ File Replication Service log, skladištenje aktivnog direktorijuma datoteka o događajima.
- ▶ Service Specific log, skladištenje događaja vezanih za određene usluge ili aplikacije.

Log fajlovi imaju HTTP statusne kodove koji su specifični za određene vrste incidenta. Oni su navedeni u HTTP-u i specifični su za sve Web servere. Ovi kodovi su trocifreni brojevi, gde prva cifra identifikuje klasu odgovora. Statusni kodovidovi su klasifikovani u pet kategorija, kao što je prikazano u tabeli 3.

Status Code	Description
1XX	Continue or request received
2XX	Success
3XX	Redirection
4XX	Client error
5XX	Server error

Tabela 3. Statusni kodovi: tri cifre podeljene u pet kategorija

Izvor: Bayuk Jennifer, (2010), *Cyber Forensics Understanding Informatio Security Investigation*

Nije neophodno da se razume definicija specifičnih HTTP statusnih kodova koliko je važno da se razumeju klase ovih kodova. Statusni kodovi jedne klase, treba da budu tretirani na isti načina kao bilo koji kodovi iz te klase.

Log bezbednost

Web servisi koji rade na IIS ili Apache-u rizikuju brisanje log fajlova, od strane bilo kog napadača, koji ima pristup Internetu i serveru jer se fajlovi čuvaju na samom Web servisu.

Network logging je metod za bezbedno održavanje dnevnika. Mrežni IDS može prikupljati aktivne zahteve na mreži, ali oni ne uspevaju da se usklade sa SSL zahtevima. Zbog toga napadači koriste HTTPS koji ne mogu biti priznati od strane IDS-a. *Proxy* server snima detaljne informacije o svakom zahtevu, koji je izuzetno dragocen za istragu Web napada.

Kada se istražuju log fajlovi, informacije se čuvaju na jednostavnom formatu sa sledećim poljima:

- ▶ Vreme/ Datum
- ▶ Izvor IP adrese
- ▶ HTTP izvorni kod
- ▶ Zahtevani resursi.

Istraživanje Web napada

Da bi se istražili Web napadi, istražitelj treba da sledi sledeće korake:

- ▶ Analiza Web servera, FTP servera i lokalne systemske log fajlove da bi potvrdio napad na Web.
- ▶ Proverava informacije log fajlova koje su utisnute u vezi sa vremenom napada, IP adresu, HTTP statusni kod i zahtevani resurs.
- ▶ Identifikovanje prirode napada, neophodno je razumeti prirodu napada, u suprotnom to bi otežalo zaustavljanje napada u početnim fazama. Ako se na vreme ne zaustavi, napad može izmaći kontroli i naneti štetu velikih razmera.
- ▶ Proveravanje da li neko pokušava da isključi mrežu ili pokušava da izvrši upad na sistem,
- ▶ Lokalizuje izvor
- ▶ Koristi *Firewall* i IDS logove da bi se identifikovao izvor napada. IDS i *Firewall* monitoring i mrežni saobraćaj vode evidenciju o svakom unosu. Oni pomažu da se izvrši identifikacija pokušaja napada na host.
- ▶ Bokiranje napada. Kada se utvrdi kako je napadač ušao u sistem, treba blokirati taj port kako bi se sprečio dalji upad.
- ▶ Kada su kompromitovani sistemi identifikovani, treba da se isključe sa mreže kako ne bi nanosili dalje štetu.
- ▶ Pokretanje istrage preko IP adrese. Pre nego što pokuša da napadne FTP, napadač obavlja kompletno skeniranje portova. To podrazumeva povezivanje na TCP i UDP portove, na ciljanom sistemu da bi se omogućilo prisluškivanje i da bi se dobila slika stanja sistema i aplikacija koje se koriste.¹⁶

¹⁶ Bayuk Jennifer, (2010), *Cyber Forensics Understanding Information Security Investigation*

5.13. Istraga FTP Servera

FTP serveri su potencijalni bezbednosni problemi, jer su izloženi spoljnjim interfejsima. Oni preko interneta podržavaju anonimne pristupe javnim resursima. Njih treba stalno ažurirati sa svim OS i Nos dostupnim zakrpama. Sve usluge osim FTP-a treba da budu onemogućene, ili uklonjene. Kontakt sa internet mrežom, na FTP serveru preko zaštitnog zida treba da bude ograničen i kontrolisan preko ACL stavki, da bi se sprečio saobraćaj od mreže. FTP serveri pružaju usluge na internoj mreži i nisu imuni na napad, pa zbog toga administratori moraju da razmotre uspostavljanje kontrole pristupa, uključujući korisnička imena, lozinke i SSL protokol za autentifikaciju.

Neke odbrambene mere koje treba primenjivati na FTP serverima uključuju sledeće:

- ▶ Zaštita sistemskih datoteka servera
- ▶ Izolacija FTP direktorijuma
- ▶ Stvaranje preavila za ovlašćenja i kontrole pristupa
- ▶ Redovni pregled logova
- ▶ Redovni pregled sadržaja direktorijuma za detekciju neovlašćenih fajlova i neovlašćene upotrebe.

Istraga IIS logova

Sve posete log fajlovima nalaze se u :

<%systemroot%\logfiles

Ako se ne koristi proxy, onda IP adresa može biti prijavljena. Primer vezan za log fajlove koji se nalaze na URL adresi:

[illegible]

5.14. Istraga Apache logova

Apache server ima dve evidencije:

- ▶ The error log
- ▶ The access log

Apache server čuva dijagnostičke informacije i poruke o greškama koje nađe tokom obrade zahteva i čuva ih kao: **error_log** u UNIX-u i **error. Log** u Windows-u. Podrazumevana putanja ove datoteke u UNIX-u je : **/usr/local/apache/logs/error_log.** Ovo je veoma bitna stvar za istražitelje i važan je deo dokaza. Razmotrićemo sledeće stavke grešaka u dnevniku:

[Sat Dec 11 7:12:36 2004] [error] [client 202.116.1.3]

Objačnjenje:

Klijent je poslao ispravno host zaglavlje. Prvi element *Error log-a* je dan, datum, vreme i godina poruke.

Drugi element pokazuje ozbiljnost greške.

Treći element pokazuje IP adresu klijenta koji generiše greške

Poslednji element je sama poruka.

Zahtevi procesirani od strane Apache servera se nalaze u *Access log-u* i čuvaju se zajedno.

Podrazumevana putanja za ovaj fajl je : `/usr/local/apache/logs/access_log` u **UNIX-u**.

Razmotrimo sledeći primer:

127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326

Prvi element u dnevniku prikazuje IP adresu klijenta.

Drugi je informacija koja sadrži identitet

Crtica ukazuje da informacija nije bila dostupna.

Treći element je uputstvo ID korisnika.

Četvrti element je datum i vreme.

Peti element je ulaz u log fajl, to je datum u dvostrukim navodnicima.

Šesti element je stanje pod kojim server šalje do klijenta poruke i

Sedmi element je veličina objekta koji se šalje klijentu.¹⁷

5.15. Istraživanje statičke i dinamičke IP adrese

IP adrese mogu biti statički ili dinamički dodeljene korišćenjem DHCP servera. ISP obezbeđuje pristup Internetu, velikoj bazi klijenata kojima obično dodeljuje dinamičke IP adrese. DHCP log datoteka skladišti informacije u vezi IP adresa dodeljenih određenom hostu u određeno vreme. Statičke IP adrese određenog hosta mogu se naći uz pomoć alata kao što su : **Nslookup, WHOIS, Traceroute, ARIN i NeoTrace.**

- ▶ **Nslookup** je ugrađen program koji se često koristi da pronade servere internet domena, one informacije se koriste za pronalaženje i identifikaciju DNS infrastrukture.
- ▶ **Tracetoute** utvrđuje geografsku lokaciju sistema. On može dati detaljan put IP paketa između dva sistema.
- ▶ **NeoTrace** daje informacije preko mape sveta. Ona prati putanju mreže od domaćina, do ciljanog mesta preko Interneta.

¹⁷ Grance Tim, et, Nist, Guide to Computer and Network Data Analysis: Applying Forensic Tehniques to Incident Response

- ▶ **WHOIS** baza podataka može da se koristi za identifikaciju vlasnika Web lokacije. Koristi se upit sledeće sadržine: **whois -h <host name> <identifier>**

5.16. Checklist za Web bezbednost

Da bi se povećala bezbednost Web-a istražitelj ili administrator treba da utvrde da li je sledeći spisak zadataka izvršen:

- ▶ Uveriti se da korisnički nalozi nemaju slabosti ili da im nedostaju lozinke
- ▶ Blokiranje neiskorišćenih otvorenih portova
- ▶ Proveravanje da li postoje neki od različitih Web napada.
- ▶ Proveriti da li IDS ili IPS su raspoređeni
- ▶ Koristiti skenere da bi se sprečili određeni ilegalni upadi
- ▶ Testiranje Web lokacije i SSL-a.
- ▶ Dokument sa spiskovima tehnika, uređaja, politike je neophodan korak za bezbednost.

U tabeli 4. prikazan je broj prijavljenih slučajeva, različitih vrsta Web napada:

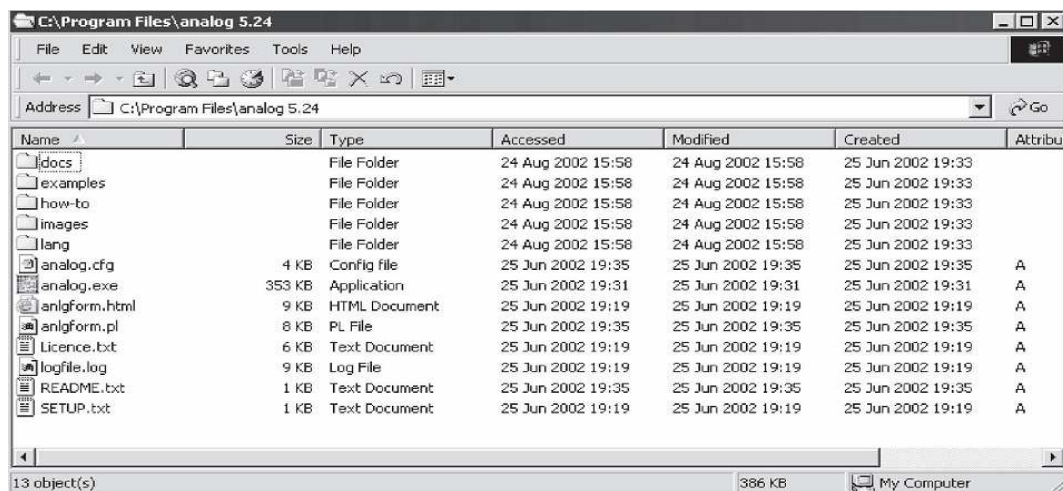
Attack Method	Total 2005	Total 2006	Total 2007
Attack against the administrator/user (password stealing/sniffing)	48,005	207,323	141,660
Share misconfiguration	39,020	39,629	67,437
File Inclusion	119,305	146,082	61,011
SQL Injection	36,253	47,212	35,407
Access credentials through Man in the Middle attack	26,427	21,209	26,648
Other Web Application bug	60,383	6,529	18,048
FTP Server intrusion	38,945	55,011	17,023
Web Server intrusion	38,975	20,059	12,409
DNS attack through cache poisoning	7,341	9,131	9,747
Other Server intrusion	1,4732	16,050	8,050
DNS attack through social engineering	4,719	5,659	7,585
URL Poisoning	2,997	7,888	8,931
Web Server admin module intrusion	9,497	17,260	8,890
Remote administrative panel access through brute forcing	2,738	4,898	6,007
Routing after attacking the Firewall	989	4,308	0,127
SSH Server intrusion	2,644	14,740	9,723
RFC Server intrusion	1,821	5,793	5,618
Routing after attacking the Router	1,520	4,897	5,257
Remote service password guessing	939	7,008	5,106
Telnet Server intrusion	1,863	6,253	4,753
Remote administrative panel access through password guessing	1,914	6,416	4,753
Remote administrative panel access through social engineering	769	5,472	3,127

Webserver defaced	Year 2005	Year 2006	Year 2007
Apache	308,291	486,294	519,439
IS/6.0	72,338	180,926	113,938
IS/5.0	92,616	65,304	23,654
Unknown	4,974	0,605	15,741
Zeus	1,059	508	1,972
UOTB	0	1308	1,920
IS/4.0	5,840	3,952	1,149
nginx	136	670	729
IS/5.1	540	412	358
RapidSite	158	110	244
SonataServer	4	557	178
A-NETEX RobustWeb	4	4	92
Zope	106	67	80
LiteSpeed	3	150	55
OpenWebServer	50	181	50
EnterpriseDataPath	15	15	41
Lighttpd	25	30	37
DanahHTTPd Server	52	89	35
Eoa	5	59	25
SilverStream Server	35	40	20
SAITBAR	0	18	17
Indy	8	20	15
SunONE WebServer	188	670	12

Tabela 4. Broj prijavljenih vrsta Web napada

Izvor: Grance Tim, et, (August 2005), Nist, *Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response*

Na slici jedan je prikazano analogno analiziranje log fajlova:



Slika 6. Analogno analiziranje log fajlova

Izvor : <http://www.analog.cx/how-to/index.html>. Accessed 2/2007

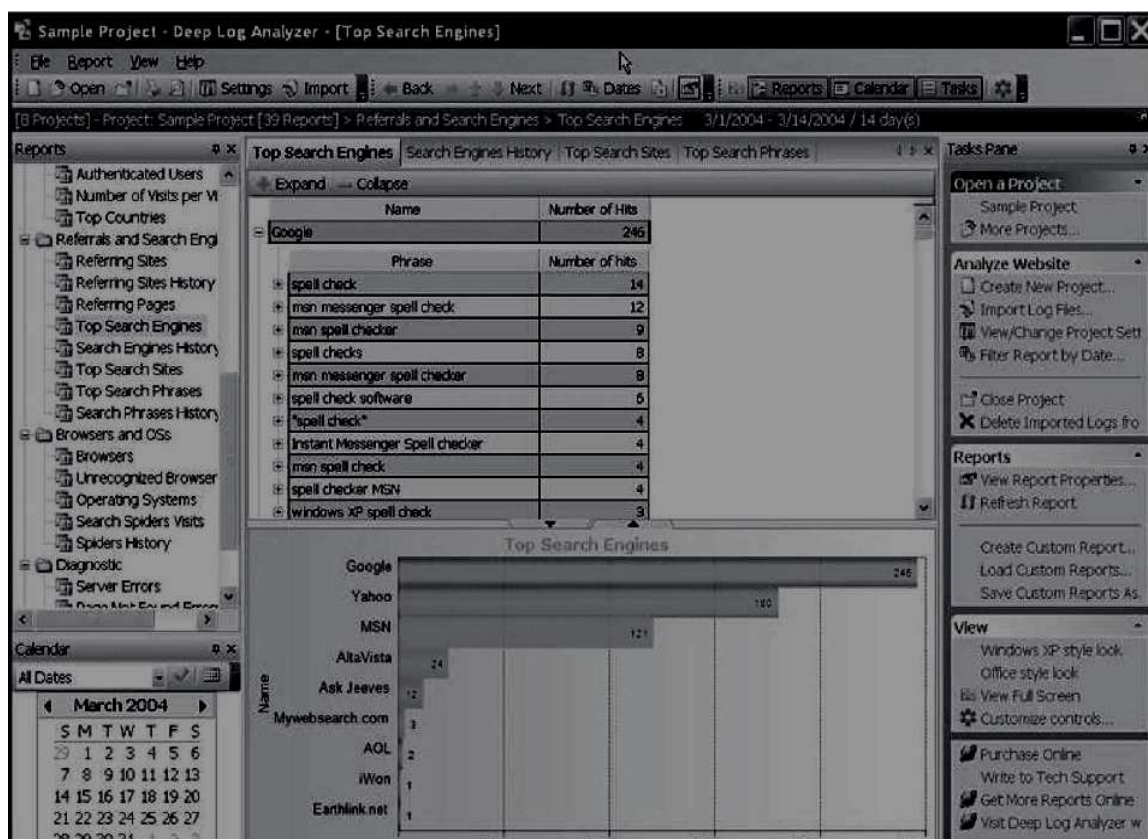
5.17. Alati za istragu Web napada

Analogna analiza ima sledeće karakteristike:

- ▶ Pokazuje podatke kao što su : Koliko često se posećuju određene stranice.
- ▶ Kreira HTML, tekst, ili e-mail izveštaje sa Web servera o saobraćaju
- ▶ Generiše izveštaje na 32 jezika
- ▶ Radi na bilo kom operativnom sistemu.
- ▶ Brz je, skalabilan i konfigurabilan.

Dubinska analiza Log fajlova

Ona vrši analizu logova za male i srednje Web lokacije. To je prikazano na slici 7. i ima sledeće karakteristike:



Slika 7. Duboka analiza Logova je posebno dizajniran za male i srednje Web lokacije

Izvor: <http://www.analog.cx/how-to/index.html>. Accessed 2/2007.

Karakteristike su sledeće:

- ▶ Određuje gde je poseta napravljena, i poslednja stranica koju su posetili pre odlaska sa mreže.
- ▶ Analiza ponašanja posetilaca na određenoj Web lokaciji
- ▶ Daje čitavu statistiku korišćenja Web lokacije
- ▶ Omogućava kreiranje prilagođenih izveštaja
- ▶ Predstavlja naprednu statistiku Web lokacije i izveštaje web analitike sa interaktivnom navigacijom i samim hijerarhijskim prikazom
- ▶ Analizira log fajlove sa svih popularnih Web servera
- ▶ Preuzima log fajlove preko FTP.
- ▶ Prikazuje zbirni izveštaj iz izabranog opsega datuma
- ▶ Poredi izveštaje za različite vremenske intervale
- ▶ Automatizuje uobičajene zadatke preko skripti, koje mogu biti periodično zakazane za izvršenje
- ▶ Koristi Access MDB bazu podataka, za skladištenje informacija koje su izvučene iz Log fajlova, tako da korisnici mogu da upišu svoje upite, ako je potrebno
- ▶ Moguće je obraditi ažurirane log fajlove, koji generišu izveštaje u formatu HTML automatskog rasporeda.

Postoji i server log analiza i ona se koristi za analiziranje servera promenom IP adrese u imenu domena. Uhost fajlovima svaka lonija, koja ne počinje sa # je u sledećem formatu:

ipaddress status count name

IP adresa je standardna, stanje je 0 ako je dobro ime ili *h_error value* ako nije

Count broji koliko je puta pristupljeno hostu

Name je DNS ime hosta

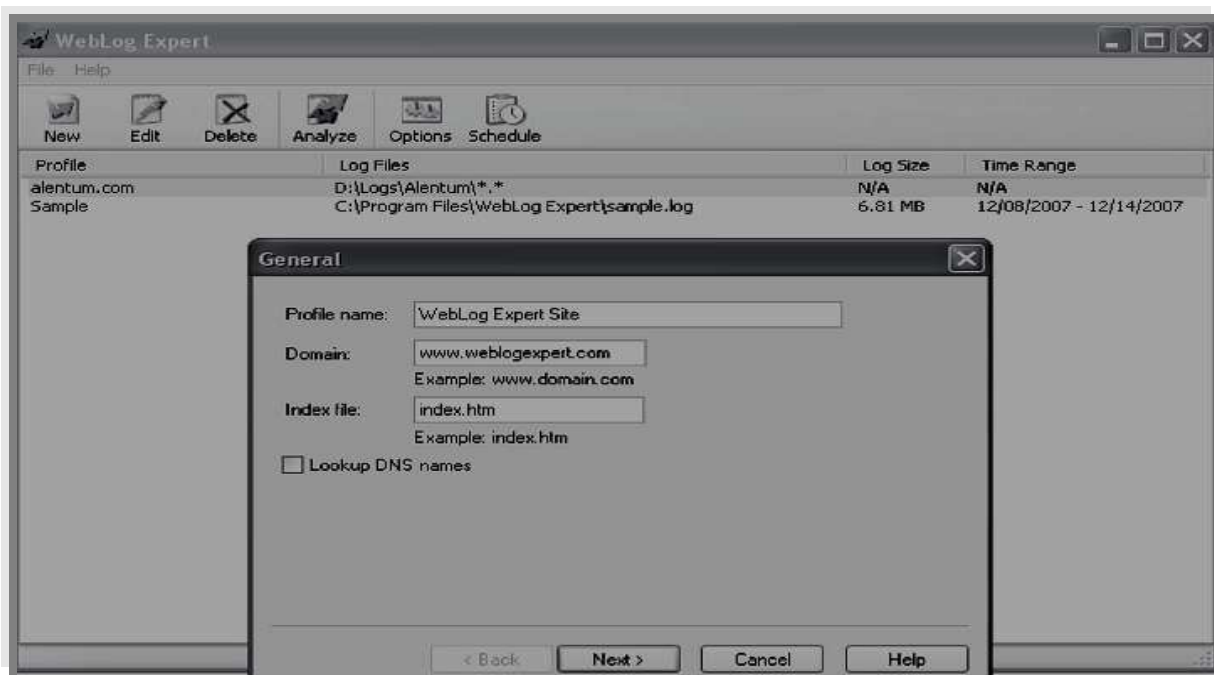
Server log analizira da je verziju log fajla sa imenom dokumenta (ako je potrebno) i IP adrese koje su pretvorene u DNS imena.

Postoji i *WebLog Expert* koji daje informacije o posetiocima lokacije, uključujući i statistiku aktivnosti, pristupa datotekama, putanjama preko sajta, pozivanim stranicama, pretraživačima, operativnim sistemima i mnogim drugim. Program daje HTML izveštaje uključujući tabele i grafikone. Može analizirati logove Apache-a i IIS Web servera. Njegov interfejs takođe uključuje ugrađenog čarobnjaka za brzu pomoć, kao i lako kreiranje i analizu sajta profila.

WebLog Expert prijavljuje sledeće:

- ▶ Opštu statistiku
- ▶ Statističke aktivnosti po satima, danima, danima u nedelji, i mesecima
- ▶ Statistiku pristupa stranicama, datotekama, slikama, direktorijumima, upitima, virtuelnim domenima
- ▶ Informacije o domenima najvišeg nivoa, zemljama, državama, gradovima, organizacijama i autentifikacijama korisnika.
- ▶ Browser-e, operativne sisteme i spiders statistike
- ▶ Informacije o greškama sa informacijama o grešci 404
- ▶ WebLog Experts je napravio filtere za host, upite, reference, statusne kodove operativnog sistema, browser-e, korisničke agente, dan u nedelji, sate, zemlje, države, gradove i virtuelne domene.
- ▶ On takođe ima i filtere za posetioce koji pristupaju određenim datotekama, posetiocima koji su došli sa određene URL adrese.

Na sledećoj slici je dat primer WebLog Expert-a.



Slika 8. Primer WebLog Experta

Izvor: <http://www.analog.cx/how-to/index.html>. Accessed 2/2007.

WebLog Expert ima sledeće karakteristike:

- ▶ Radi pod Windows-om
- ▶ Podržava Apache i IIS logove
- ▶ Automatski detektuje log format
- ▶ Može preuzimati logove preko FTP i HTTP-a
- ▶ Ima dnevnik preuzetih log fajlova
- ▶ Može kreirati HTML, PDF, i CSV izveštaje

- ▶ Podržava izveštaje na više jezika.
- ▶ Podržava stranu za preuzimanje
- ▶ Može da *upload*-je izveštaje preko FTP-a i šalje ih preko e-mail-a
- ▶ Ima IP mapiranu bazu podataka zemalja
- ▶ Posедуje bazu podataka gradova, država i organizacija
- ▶ Podržava *command-line* mod.

Pored ovog programa, postoji i *AlterWind Log analizator*

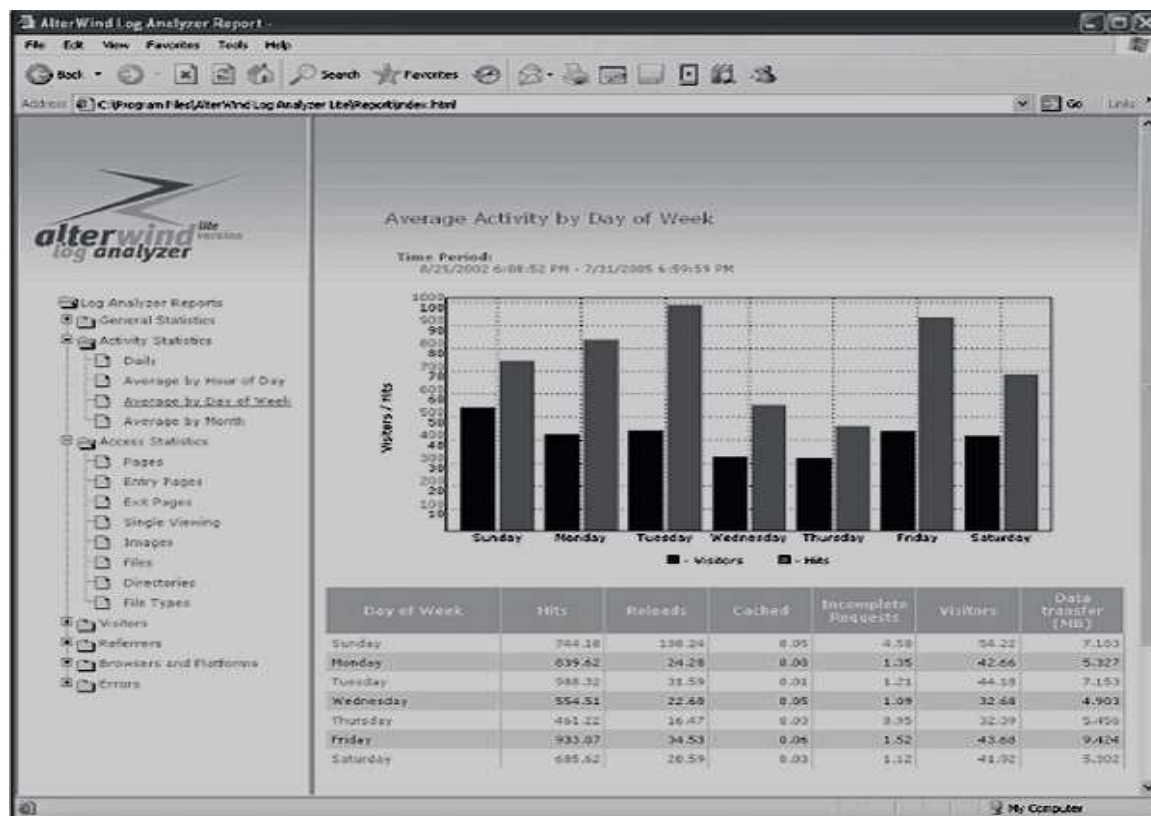
On dolazi u tri verzije:

1. Professional
2. Standard
3. Lite

On generiše izveštaje za Web optimizaciju sajta pretraživača.

Verzija *Lite* je besplatan alat Web analizator. Ova verzija prikazuje samo osnovne karakteristike na Web sajtu.

Ovaj program prikazan je na sledećoj slici.



Slika 9. AlterWind Log Analizator dolazi u tri verzije

Izvor: <http://www.alterwind.com/loganalyzer/>. Accessed 2/2007.

Ima sledeće karakteristike:

- ▶ Automatsku detekciju standardnih formata log fajlova
- ▶ Automatsko dodavanje log datoteka na listu dnevnika
- ▶ Sposobnost da promeni dizajn izveštaja
- ▶ Podržava komandne linije
- ▶ Sposobnost da se prilagodi unetim podacima u izveštaj
- ▶ Simultana analiza velikog broja log fajlova.

6. Studije slučaja

Rad se bavi pristupom digitalnog forenzičara Log datotekama. U log datotekama je zapis događaja u računarskom sistemu ili mreži. Koriste se za optimizovanje sistema i mreža, praćenje ponašanja korisnika i generisanje podataka korisnih za istraživanje aktivnosti malicioznih programa.

Slučajevi opita treba da prikažu ali i opišu istrage pri forenzičkoj analizi Log datoteka. Uzeta je WindowsUpdate.log datoteka, koja je datoteka samog Windows operativnog sistema. Beleženi su neki događaji i analiziran je njihov zapis u ovoj log datoteci. Predočeno je šta se sve može naći kao zapis u ovoj datoteci i na koji se način određeni zapisi mogu tumačiti.

6.1.1. Istraga autora e-mejla (Mining E-mail Authorship)

U ovom delu je obrađena istraga o učenju autorskog prava identifikacijom i kategorizacijom slučaja e-mail dokumenata. Korišćene su razne e-mail karakteristike dokumenata, kao što su strukturne karakteristike i lingvistički dokazi u saradnji sa Support Vector Machine koju koriste za pisanje algoritama.

S' brzim porastom kompjuterske tehnologije, industrije i dr. mnoge vlade su postale zavisne od upotrebe elektronske pošte, kao svrsishodan i ekonomski oblik komunikacije, preko Interneta ili Intraneta. E-mail se koristi u mnogim situacijama, kao na primer u razmeni i emitovanju poruka, dokumenata i za obavljanje elektronske trgovine. Nažalost može takođe biti i zloupotrebljen za distribuciju neželjene pošte, (obično se naziva *spam*). U nekim sličajevima, zlonamerni pošiljalac će pokušati da sakrije svoj pravi identitet kako bi se izbeglo njegovo otkrivanje. Na primer, adresu pošiljaoca je moguće falsifikovati ili usmeriti preko anonimnog servera e-pošte, ili e-mail sadržaja i informacija u zaglavlju i tako prikriti pravi identitet pošiljaoca.

Kao rezultat rastuće e-mail zloupotrebe, efikasne automatizovane metode za analizu sadržaja e-poruka i identifikovanje ili autorizaciju-Autori ovih poruka postaju imperativ. Osnovni ciljevi su da se klasifikuju neki podaci kao pripadnici, posebno autor i ako je moguće i dobiti niz karakteristika koje ostaju relativno konstantne, za veliki broj elektronske pošte napisane

od strane autora. Identifikovanje takve kategorizacije ističe i inherentne poteškoće sa kojima se sušćavaju autori kategorizacija, jer se očekuje da karakteristike pisanja evoluiraju u vremenu i izmene u različitim kontekstima. Na primer sastav formalnih e-mail-ova će se razlikovati od onih neformalnih (sama promena vokabulara). Čak i u kontekstu neformalnih e-poruka može biti nekoliko kompozicijskih stilova (na primer: za lične odnose, za radne odnose i sl.). međutim ljudi su bića navika i imaju određene lične osobine koje imaju tendenciju trajanja. Svi ljudi imaju jedinstvene ili skoro jedinstvene obrasce ponašanja, biometrijske attribute i dr. Stoga se pretpostavlja da su neke karakteristike koje se odnose na jezik, sastav u pisanju, kao što su posebni sintaksički i strukturalni raspored osobina, obrasci korišćenja rečnika i neobična uporeba jezika ili prekomerna upotreba cifara, velikih i malih slova, stilske i substilske karakteristike ostaju relativno konstantne. Identifikovanje i učenje ovih karakteristika su glavni izazovi u autorstvu kategorizacije.¹⁸

Kategorizacija autorskih prava, se može izvršiti korišćenjem različitih pristupa.

Prvi najjednostavniji metod je korišćenje demena eksperta za identifikaciju nove e-mail poruke i dokumenta i dodeliti ih dodro zaštićenoj autorskoj kategorizaciji. To može potrajati i biti skupo i možda najvažnije ograničenje je to što ne daje stalnu meru o stepenu zaštite, sa kojima je raspodela napravljena.

Drugo, domen stručnjak može da uspostavi skup osnovnih pravila koja se mogu koristiti za klasifikaciju novih e-mail dokumenata. Nažalost u mnogim slučajevima skup pravila može biti veliki i glomazan i obično mora često da se ažurira i ne može da se prilagodi promenama u sadržaju dokumenata ili autorskim karakteristikama.

Slična oblast autorskoj kategorizaciji je tekst kategorizacija koja pokušava da kategorizuje skup tekstualnih dokumenata na osnovu svog tipa sadržaja. Tekstualna kategorizacija pruža podršku za širok spektar aktivnosti u informacionom *miningu* i u upravljanju informacijama. Ona se može primeniti i koristiti za podršku, preuzimanje dokumenata generisanjem kategorije potrebne za preuzimanje dokumenata. Mnogi metodi koji automatski koriste pravila predloženi su za kategorizaciju teksta. Većina ovih tehnika se zasniva na *bag of words* ili vektorski prikaz reči u kome svaka funkcija u tekstualnom dokumentu odgovara jednoj reči, a zatim koristi za učenje. Primer su neuronske mreže, *Bayesian pristup*, ili mašinska vektorska podrška koja klasifikuje tekstualni dokument.

¹⁸ Oliver, *Mining E-mail Authorship*, Information Technology Division, Defence Science and Technology Organisation

6.1.2. Autorska kategorizacija

Formalno autorska kategorizacija je zadatak utvrđivanja autorskog dela. Posebno je interesantna kategorizacija tekstualnog dela, obično na osnovu drugih tekst uzoraka nastalih od strane istog autora. Pretpostavljamo da je samo jedan autor odgovoran za pravljenje tekstualnih priloga, više autora nije uzimano u obzir. Autorska kategorizacija je podskup opštijih problema zvanih „Autorska analiza“. Ova analiza obuhvata i druge različite delove, kao što su autorska karakterizacija i otkrivanje sličnosti. Autorsku kategorizaciju određuje autor ili karakteristike koje određuje autor koji je proizveo deo posla. Primer karakteristike uključuje obrazovanu i kulturnu pozadinu. Slično detekciji izračunava stepen sličnosti između dva ili više delova rada bez nužnog identifikovanja autora. Sama sličnost se koristi u otkrivanju plagijata, ovde se uključuje potpuna ili delimična replika dela rada sa ili bez dozvole od strane originalnog autora. Detekcija plagijata pokušava da otkrije sličnost između dva suštinski različita dela, ali nisu u mogućnosti da utvrde da li su nastala od istog autora. Autorska analiza ima veliki broj primena, uključuje se identifikovanje autora u literaturi, u programskom kodu, u forenzičkim analizama u krivičnim predmetima.

Možda najopsežnija i sveobuhvatna primena autorske analize je, u literaturi i u objavljenim člancima. Postoje studije koje pokušavaju da reše neke Šekspirove radove i bilo je pokušaja da se pokaže da Šekspir nije autor ovih radova već da ih je stvorio Edvard De Vere. Korišćene su autorske funkcije kao što su neobična dikcija, učestalost pojedinih reči, izbor same rime, isame navike rastavljanja reči. Važna vrsta dokaza koja se može koristiti da se utvrdi autorstvo je lingvistički dokaz koji je karakterističan za jezičke navike koje su jedinstvene pri identifikaciji autora. Smatra se da su pojedini lingvistički dokazi dinamički generisani i podsvesno korišćeni pri stvaranju samog jezika. Jezički obrasci ili podstilske karakteristike generišu se van svesne kontrole nekog autora. Kombinacija podstilskih funkcija mogu biti proizvoljne i jedinstvene za nekog autora.

Programski kod autorskog prava je istražen od strane nekih korisnika, u kontekstu softverske krađe i plagijata, softverskog autorskog praćenja i samog otkrivanja upada. Softver za praćenje autora omogućava identifikovanje autora određenog fragmenta koda iz velikog skupa programera koji rade na softverskom projektu. Ovo može biti jako korisno za autore za softversku nadogradnju i održavanje. Autorstvo računarskog virusa ili Trojanca može biti

identifikovan na sličan način. Ispitivanjem specifični karakteristika ili mernih jedinica u stilu samog programiranja omogućava da se identifikuju autori određenih dela programskog koda, na sličan način koji se koristi za otkrivanje lingvističkih dokaza kod autora slobodnog teksta. Programi metrike kao što su štamparske karakteristike (upotreba malih i velikih slova i mnoštva programskih izveštaja i dr.) stilske metrike, programske strukture, postavljanje komentara, simboli, odaju samog autora.

Forenzička analiza teksta ili forenzička lingvistika pokušavaju da identifikuju tekst i autora u cilju krivične istrage. Tekstualna analiza *Unabomber manifesto* je najpoznatiji primer forenzičke lingvistike. U ovom slučaju *manifesto* i osumnjičeni bombaš koriste skup sličnih karakteristika, kao što je karakterističan rečnik, pokreti i dr.

E-mail dokumenti imaju nekoliko karakteristika koje čine autorsku kategorizaciju malim izazovom u poređenju sa dužim formalnim tekstualnim dokumentima kao što su književna dela ili objavljeni članci. Prvo, kompozicija i stil se koriste u formulisanju e-mail dokumenta često drugačiji od normalnih tekstualnih dokumenata koje su napisali isti autori. Nekada publikacija ne mora biti ista kao i kad je poslata e-mail-om, jer su mail dokumenti uglavnom kraći i neki delovi mogu biti isečeni zbog nekih gramatičkih grešaka. Autorov stil pisanja e-mailova je često kombinacija formalnog pisanja, govora i transkripta. Drugo, autorska kompozicija u e-mailovima može da varira u zavisnosti od primaoca i može da se koriguje veoma brzo tokom vremena. Ali neke određene osobine kao što su posebna sintaksa, struktura rečenice, izgled obrazaca, rečnik pri pisanju, neobična jezička upotreba, stilske i podstilske karakteristike ostaju relativno konstantne za obeležje svakog autora.¹⁹

6.1.3. Mašinska podrška za vektorsku klasifikaciju

Osnovni koncepti za podršku *Vector machines* (SVM) su razvijeni od strane Vapnika. Koncept SVM-a je zasnovan na ideji strukturalne minimizacije rizika, koji minimizira generalizaciju grešaka koja je ograničena skupom grešaka i termina koji zavise od *Vapnik-Chervonenkis* (VC). Za razliku od mnogih drugih učenja algoritama, određeni parametri se koriste u SVM-u i zavise od ograničenja koja razdvajaju podatke i ne zavisi od broja ulaznih

¹⁹ Grance Tim, et, Nist, *Guide to Computer and Network Data Analysis: Applying Forensic Tehniques to Incident Response*

funkcija. Tako SVM nema zahteve u smanjenju broja funkcija kako bi se izbegao problem prekoračenja. Ovo je prednost u kontekstu visoke dimenzionalne aplikacije, kao što su tekstualni dokumenti i autorska kategorizacija. SVM zahteva primenu algoritama za optimizaciju minimizacije postupaka koji može biti računarski skupo.

6.1.4. E-mail dokumenti, atributi i eksperimentalne metodologije

Dokumenta koja se koriste u eksperimentalne evaluacije autorske kategorizacije sadrži ukupno 274 dokumenta i entitet autora. Podaci se koriste za dobijanje baze podataka kao i pitanja koja treba rešiti, posebno problem privatnosti. U bazu su uključeni privatni e-mail-ovi, a uklonjeni su mailovi sa temama koje doprinose samo minimalne osobine za verifikaciju autora. Telo svake poruke je podešeno da ukloni ako je prisutan deo teksta tipa pozdrava ili potpisa. Međutim, postojanje, lokacija i tip poruka neke od njih se zadržavaju kao ulaz u određene kategorije (donja slika).

<i>Author Category</i>	<i>Number of E-mail Documents</i>	<i>Document Size (Number of words)</i>	
		<i>Minimum</i>	<i>Maximum</i>
A	87	3	323
B	51	0	112
C	73	19	440
D	45	3	680
E	18	30	298

Slika 10. Pregled statistike e-mail dokumenata korišćenih u eksperimentu

Izvor: Nist- Guid to Computer and Network Data Analysis

Broj atributa, uključujući i strukturne karakteristike, obrasce upotrebe rečnika, stilske i podstilske karakteristike izdvojeni su iz svake e-mail poruke i navedeni su u tabeli.

<i>Attribute</i>	<i>Attribute Type</i>
1	Total number of words
2	Average length of words (number of characters)
3	Number of sentences
4	Average length of sentences
5	Number of lines
6	Number of blank lines
7	Average length of lines (number of characters)
8	Number of characters
9	Number of upper-case characters
10	Number of digits
11	Number of tabs
12	Reply status
13	Ratio of short words to total number of vocabulary words
14	Ratio of words used once to total number of vocabulary words
15-38	Function word attributes

Tabela 5. Tabela dokumentovanih E-mail atributa

Izvor: Mining E-mail Authorship, publikacija, 2008

olivier.devel@dsto.defence.gov.au

SVM samo izračunava dvosmernu kategorizaciju Q dvosmerni klasifikacioni model koji su generisani, gde je Q broj autorske kategorizacije (za naše e-maile je Q=5) i svaka SVM kategorizacija je primenjena Q puta. Ovo je proizvelo Q dvosmernu matricu. SVM je testiran na 192 dokumenta 70% od tih je dokumenata je podešeno, a 82 su nevidljivi.

Da bi se ocenila uspešnost kategorizacije na e-mail dokumentu koristi se tačnost opziva (R) i preciznost (P) i performanse mere najčešće zaposleni u pronalaženju informacija i teksta.

Preciznost (P) se definiše:

$$P = \frac{\text{BROJ TAČNIH KATEGORIJSKIH ZADATAKA}}{\text{UKUPAN BROJ ZADATIH KATEGORIJA}}$$

$$R = \frac{\text{BROJ TAČNIH KATEGORIJSKIH ZADATAKA}}{\text{UKUPAN ISPRAVAN BROJ ZADATIH KATEGORIJA}}$$

6.2. Studija slučaja 2: Analiza Windows Log datoteka

Da bi Log datoteke bile korisne, potrebno je izvršiti njihovu analizu. Tumačenje log datoteka je jako bitno, jer obezbeđuje sigurnost samog sistema, one su veoma bitne jer mogu dovesti do rešenja mnoge probleme koji se javljaju na sistemima i mrežama. Dobra analiza log datoteka je najznačajniji i najbitniji korak. Ovo je veoma obiman i težak posao. Da bi se uradila log analiza, potrebno je dobro poznavanje aktivnosti vezanih za sistem. Neke log datoteke su veoma jednostavne, dok su druge jako komplikovane. Značenje log podataka zavisi od konteksta. Administratori moraju dobro poznavati kontekst definisanosti. Log podaci mogu sadržati kodove ili poruke koje su značajne za prodavce softvera.

Postoji nekoliko vrsta log fajlova:

- ▶ Access.log
- ▶ Error.log
- ▶ Reffer.log
- ▶ Search.log
- ▶ Rotation.log (Apache)
- ▶ Piped. Log (Apache)

Acess.log beleži sve pristupi nekoj web strani ili serveru.

Error.log sadrži sve greške kod pritupa bez obzira gde su nastale i na čijoj strani.

Reffer.log sadrži adrese dolaznih strana ili linkove preko kojih su posetioči došli na sajt.

Search.log da li je poseta naše strane usledila kao rezultat nekog web pretraživača, i preko koje ključne reči je taj pretraživač izbacio neku od naših strana sajta.

Rotation.log služi za rotaciju log fajlova, ili otvaranje novih a da ne dođe do prekida rada servera.

U nekim slučajevima nije moguće postići potpuno razumevanje log podataka. Najbolji način da se log podaci razumeju jeste da se pregled i analiza vrše periodično i konstantno. Dnevni pregled treba da uključuje podakte koji su od bitnog značaja i one koji nisu u potpunosti razumljivi. Ovakve analize log datoteka oduzimaju jako puno vremena i predstavljaju najveći izazov.

Danas je razumevanje log podataka u neku ruku olakšano, jer je automatizovano.

Određivanjem koji tipovi log datoteka su važni administratori mogu da konfigurišu filtere podataka prilikom automatizacije. Ovim postupkom se povećava šansa da se maliciozni programi prepoznaju i odmah budu prikazani.

Administratori sistema mogu vršiti analizu korišćenjem određenih alata i tehnika. U nekim sistemima infrastrukturna analiza bi trebalo da se vrši lokalno. Jedan od mogućnosti da se log podaci ubace u bazu log podataka, jeste korišćenje upita jer se sa njim dolazi do željene analize. Upiti predstavljaju način filtriranja log podataka za analizu.

Pojedinim log datotekama operativnog sistema Windows mogu pristupiti samo administratori. Takva je Security Event Log datoteka. Drugim log datotekama koje se generišu korišćenjem aplikacija, može pristupiti sam korisnik.

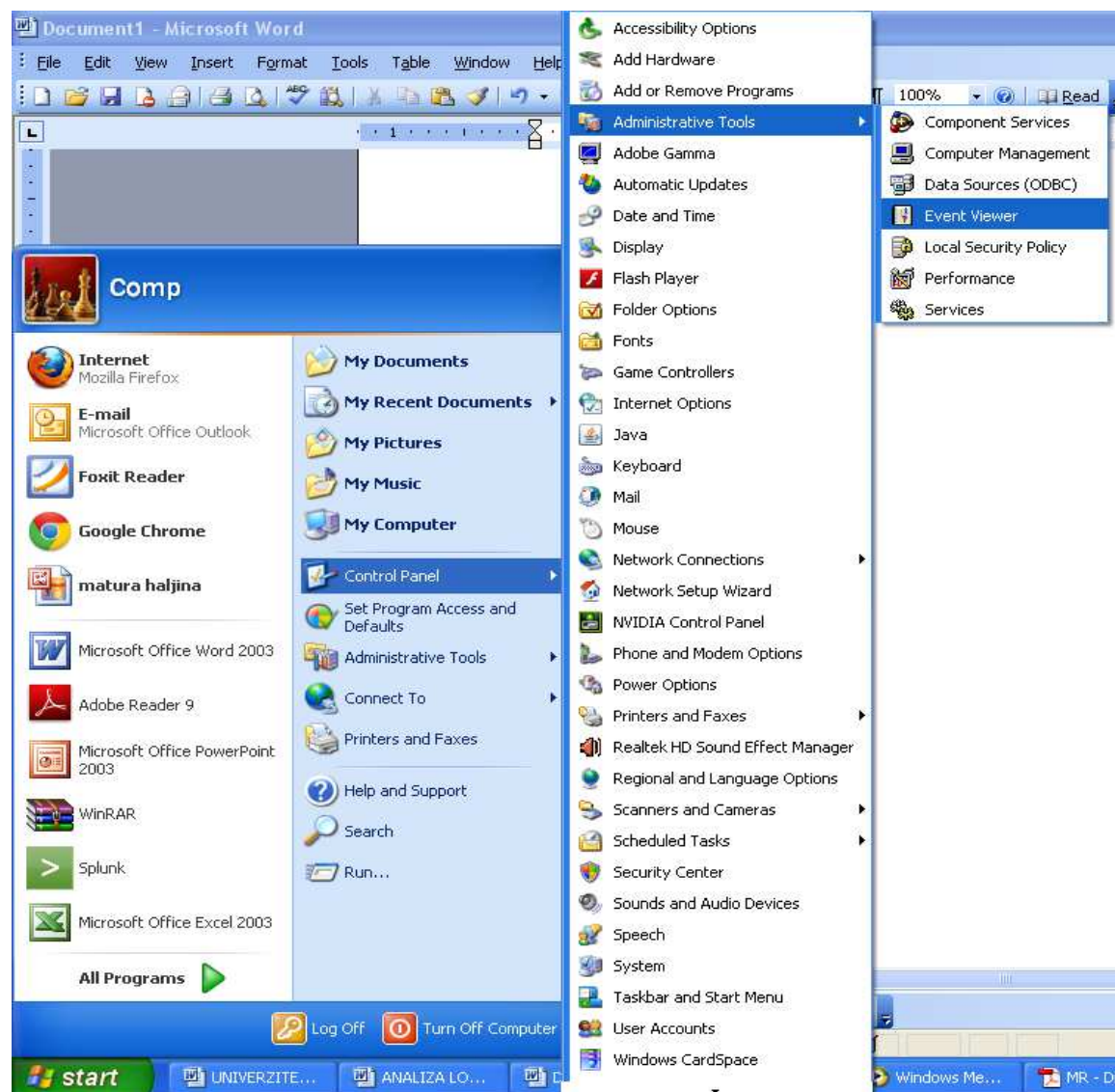
Windows OS vrši generisanje tri log datoteke:

- ▶ SysEvent.Evt
- ▶ SecEvent.Evt
- ▶ AppEvent.Evt

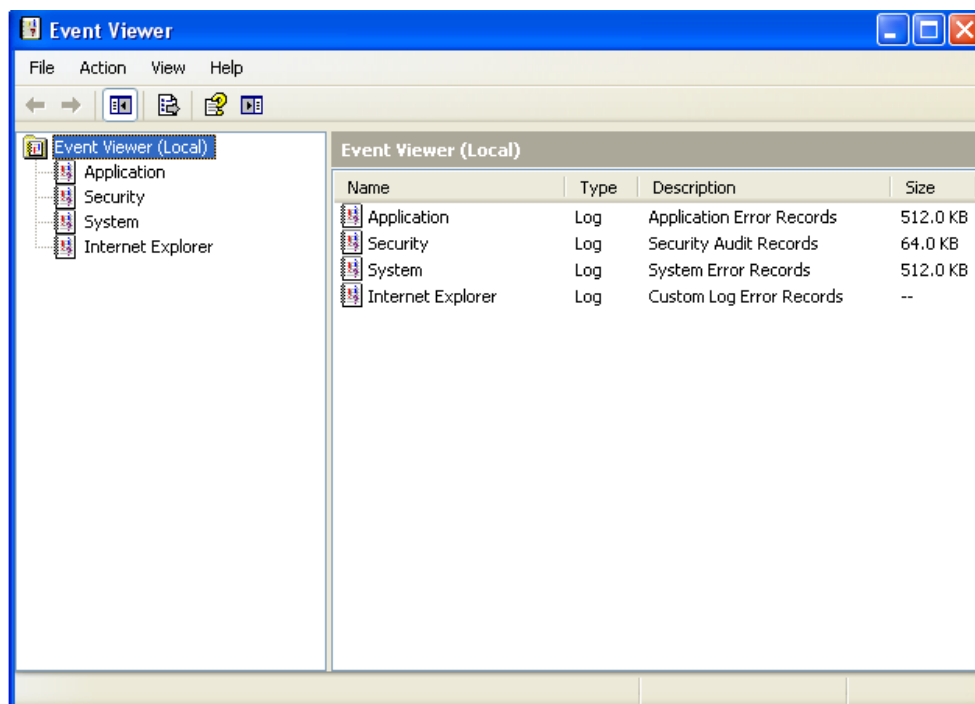
Svaka od njih se čuva kao posebna datoteka, i svakoj od njih se može pristupiti ako se prati putanja:

C:\Windows\system32\config.

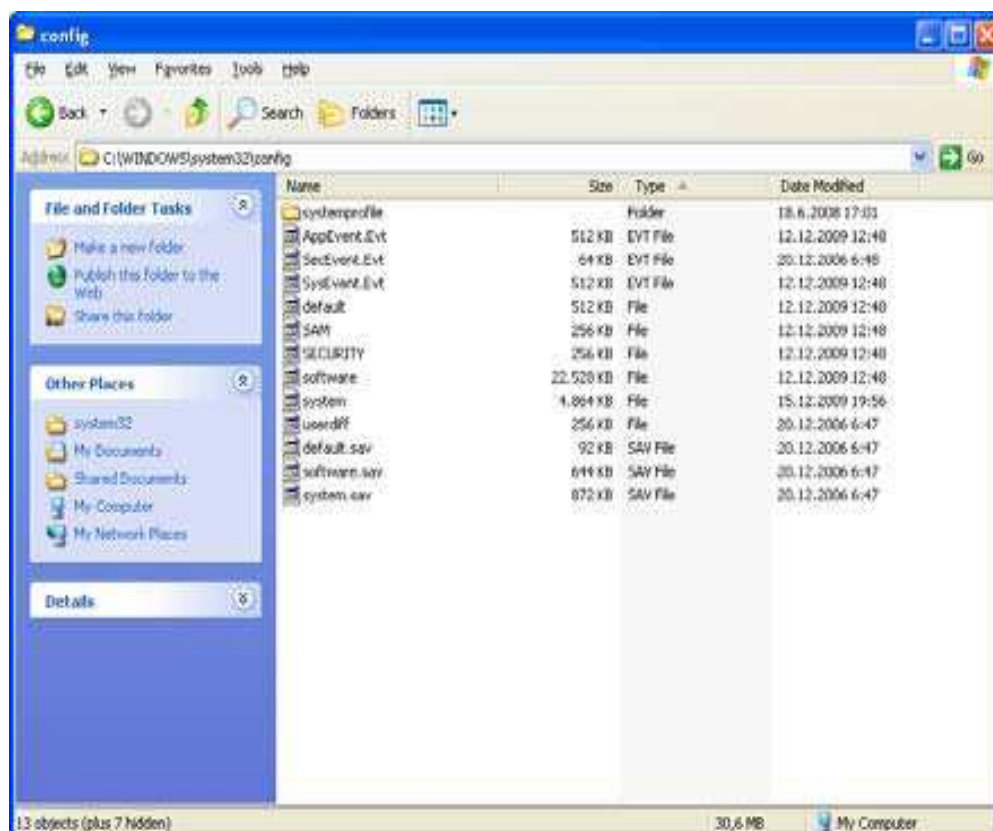
Do ovih datotek se dolazi sledećim putem:



Slika 11. Putanja do Log datoteka SysEvent.Evt,SecEvent.Evt



Slika 12: Prozor u kome se nalaze datoteke – Event Viewer



Slika 13 : log datoteke SysEvent.Evt, SecEvent.Evt

Operativni sistem Windows generiše i datoteku događaja koja se nalazi na gore objašnjenoj lokaciji.. Ovdje se nalaze poruke koje ukazuju na događaje koji su se odvijali na sistemu.

Ova datoteka sadrži sledeće informacije:

```

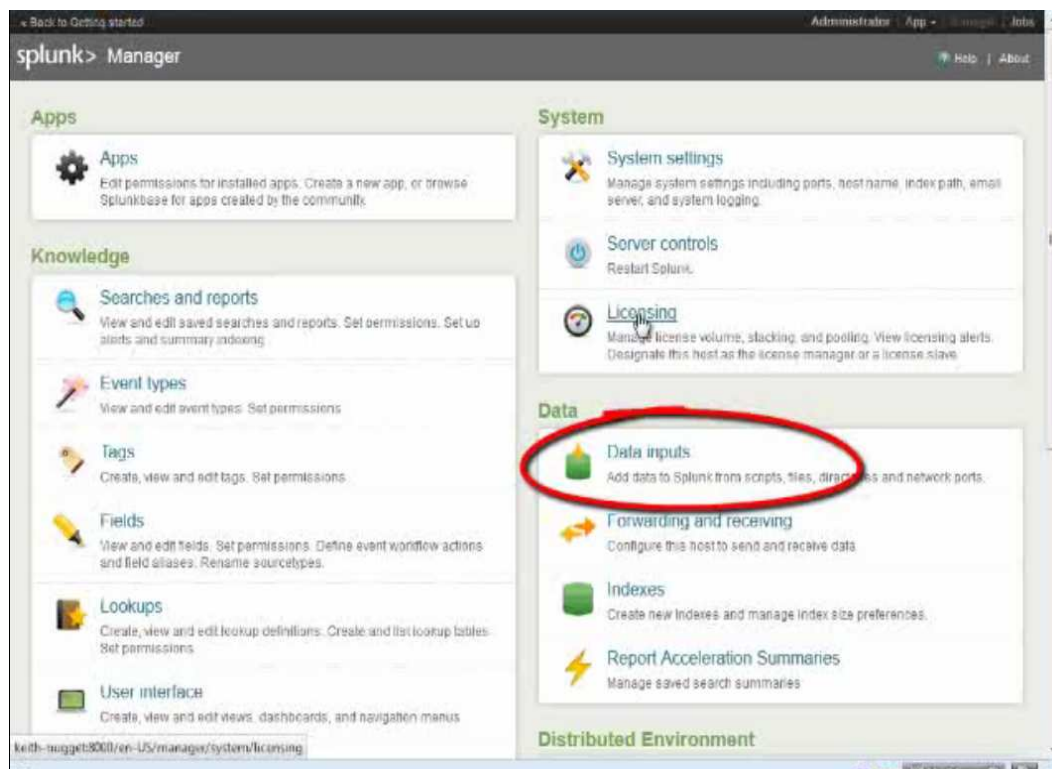
WinEdit 7.1 (Unregistered Copy) : [C:\WINDOWS\WindowsUpdate.log]
File Edit Search Insert Document Project View Tools Macros Accessories TeX Options Window Help
WindowsUpdate.log Doc2 Doc3
2012-08-17 17:03:00:296 1616 8a8 Agent * Added update (3ABE760C-4578-4C94-A1CB-BF1DF019EFE4).100 to search result
2012-08-17 17:03:00:296 1616 8a8 Agent * Added update (596ADB47-108D-482D-85BA-A513621434B7).100 to search result
2012-08-17 17:03:00:296 1616 8a8 Agent * Added update (E8169F6D-525A-4809-9B1A-E1806CBB0073).100 to search result
2012-08-17 17:03:00:296 1616 8a8 Agent * Added update (7079BEEB-6120-4AFD-AD07-FB4DFA284FBE).100 to search result
2012-08-17 17:03:00:296 1616 8a8 Agent Update (A566B4B1-D44F-46F8-A862-64EFA6684948).100 is pruned out due to potential supersession
2012-08-17 17:03:00:296 1616 8a8 Agent Update (A2E271BC-57AE-44C3-8BFF-919D81299B5D).100 is pruned out due to potential supersession
2012-08-17 17:03:00:296 1616 8a8 Agent * Added update (C683FDC6-3997-4D12-AA8B-49AE57031FE6).100 to search result
2012-08-17 17:03:00:296 1616 8a8 Agent Update (DFBE25B4-06A4-4267-8AB0-5E05460DEC6B).100 is pruned out due to potential supersession
2012-08-17 17:03:00:296 1616 8a8 Agent Update (127A8A76-D873-4D58-993B-F02A2BD9DDF6).100 is pruned out due to potential supersession
1570 2012-08-17 17:03:00:296 1616 8a8 Agent * Added update (768119E9-6732-4DFA-B241-BE26DB65AD08).100 to search result
2012-08-17 17:03:00:296 1616 8a8 Agent * Found 14 updates and 13 categories in search; evaluated appl. rules of 603 out of 1281 deployed
2012-08-17 17:03:00:343 1616 8a8 Agent *****
2012-08-17 17:03:00:343 1616 8a8 Agent ** END ** Agent: Finding updates [CallerId = ]
2012-08-17 17:03:00:343 1616 8a8 Agent *****
2012-08-17 17:03:00:343 1616 8a8 Agent ** START ** Agent: Finding updates [CallerId = AutomaticUpdates]
2012-08-17 17:03:00:343 1616 8a8 Agent *****
2012-08-17 17:03:00:343 1616 8a8 Agent * Online = No; Ignore download priority = No
2012-08-17 17:03:00:343 1616 8a8 Agent * Criteria = "IsHidden=0 and IsInstalled=0 and DeploymentAction='Installation' and IsAssigned=1 or
1580 2012-08-17 17:03:00:343 1616 8a8 Agent * ServiceID = (9482F4B4-E343-43B6-B170-9A65BC822C77) Windows Update
2012-08-17 17:03:00:343 1616 8a8 Agent * Search Scope = (Machine)
2012-08-17 17:03:00:406 2324 hcc COMAPI >>-- RESUMED -- COMAPI: Search [ClientId = <NULL>]
2012-08-17 17:03:00:421 2324 hcc COMAPI - Updates found = 14
2012-08-17 17:03:00:421 2324 hcc COMAPI -----
2012-08-17 17:03:00:421 2324 hcc COMAPI -- END -- COMAPI: Search [ClientId = <NULL>]
2012-08-17 17:03:00:421 2324 hcc COMAPI -----
2012-08-17 17:03:01:125 1616 8a8 Agent Update (DFBE25B4-06A4-4267-8AB0-5E05460DEC6B).100 is pruned out due to potential supersession
2012-08-17 17:03:01:125 1616 8a8 Agent Update (127A8A76-D873-4D58-993B-F02A2BD9DDF6).100 is pruned out due to potential supersession
2012-08-17 17:03:01:125 1616 8a8 Agent * Added update (768119E9-6732-4DFA-B241-BE26DB65AD08).100 to search result
1590 2012-08-17 17:03:01:125 1616 8a8 Agent * Found 1 updates and 13 categories in search; evaluated appl. rules of 449 out of 1281 deployed
2012-08-17 17:03:01:125 1616 8a8 Agent *****
2012-08-17 17:03:01:125 1616 8a8 Agent ** END ** Agent: Finding updates [CallerId = AutomaticUpdates]
2012-08-17 17:03:01:125 1616 8a8 Agent *****
2012-08-17 17:03:01:140 1616 bc0 AU >>## RESUMED ## AU: Search for updates [CallId = (3B8D9B12-5E51-4ABD-ABE6-EFEA5951AF28)]
2012-08-17 17:03:01:140 1616 8a8 Report REPORT EVENT: (A967D6B3-24C6-4457-9CA8-9227C8ED4FAE) 2012-08-17 17:03:00:343+0200 1 147 101

```

Slika 14 : Izgled log datoteke WindowsUpdate.log

Ona sadrži sledeće informacije:

- Datum
- Vreme
- PID
- TID
- Komponentu
- Tekst

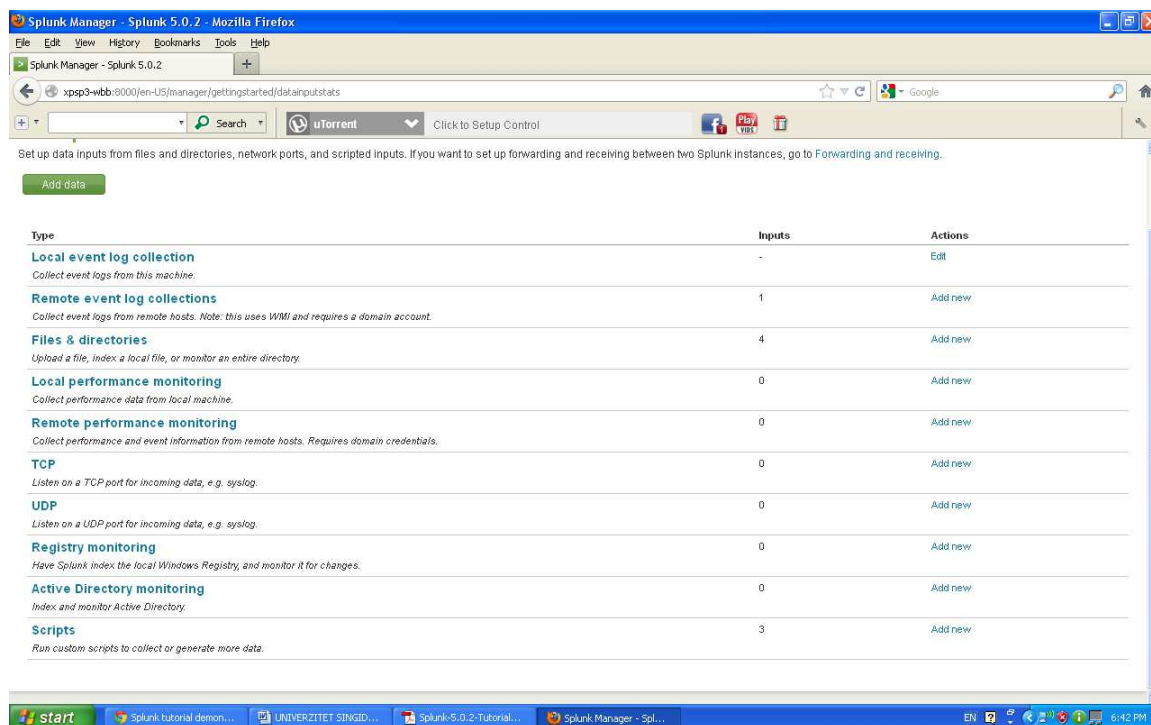


Slika 15: Izgled prozora za rad u Splunk programu

Dalje vršimo izbor log datoteka koje ćemo analizirati u ovom programu. Sledeći prozor slika 16. nam daje spisak svih skupljenih aktivnosti u poslednje vreme.

Kada se izvodi konfigurisanje, podaci se ubacuju u sistem, tražena aplikacija je polazna tačka za analizu. Bilo koji indeksirani termin za pretragu može da posluži kao polazna tačka za pretraživanje, koji kasnije može da se poboljša prema uputstvu sa ekrana.

Splunk automatski indeksira sve podatke, uključujući i složene multi-line aplikacije logova, što vam omogućava da pretražujete po svim podacima, bez potrebe za prilagođenim konektorima i bez ograničenja baznim šemama. U Splunk-u možete brzo da pretražujete i izveštaje o podacima jer on ih tumači i daje kompletniji kontekst.



Slika 16. Spisak skorašnjih aktivnosti

Splunk je sistem za čuvanje i analizu istorije. Princip rada može da se svrsta kao rad servera Splunk, on skladišti indekse i omogućava vam analizu i evidenciju koje su kreirane i prenose se na server. Postoji poseban program koji je u stanju da brzo i efikasno šalje obaveštenja logova servera, preko tehnologija kao što su NFS/SMB ili SNMP. Pod Windows-om Splunk može uzeti podatke iz Windows događaja, performansi ili registara.

U procesu indeksiranja dnevnika linije su podeljene po oblastima, kao što su: „Ime=vrednost“, zatim se uz pomoć specijalnog SPL zahteva može raditi sa ovim poljima, sortiranje, kreiranje polja za formiranje tabela, pregled spoljnog rečnika, na primer iz SQL baze podataka, i naravno da se izgradi niz grafikona.

Splunk sve evidencije koje čuva na sistemu i mogu biti na raspolaganju u bilo koje vreme. Splunk još nazivaju i „Google za log“. Interfejs Splunk-web može da napravi panele od kojih se razvijaju sopstvene Splunk aplikacije. U Splunk-u postoji App.Store, gde postoji more gotovih konfiguracija za sve popularniju analizu sistema, na primer: UNIX syslog, Apache log, Microsoft Exchange i dr.

U ovom delu rada prikazan je prvi primer koji se može kasnije ponoviti, to je dovoljno za preuzimanje i instaliranje Splunka na sistem. Tradicionalni dnevnici se koriste za analizu podataka.

Evo primera skripta koji će za nekoliko minuta snimiti dnevnike poruka:

```
require 'date'

duration = 60*1

update_period = 0.5

i = 0 while i <= duration do

  progress = i * 100.0 / duration

  msg = "%s progress=%05.2f\n" % [DateTime.now, progress]

  puts msg open("logs/my.log", 'a') { |f| f << msg }

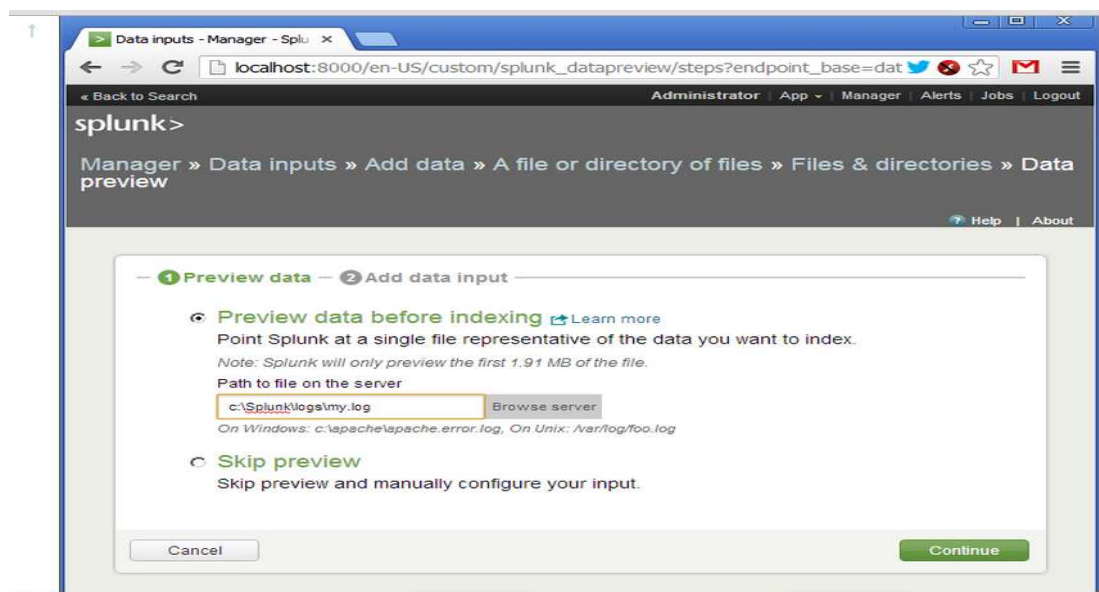
  i = i + update_period sleep update_period

end
```

Posle ovog skripta primer dnevnika će izgledati kao na sledecoj slici:

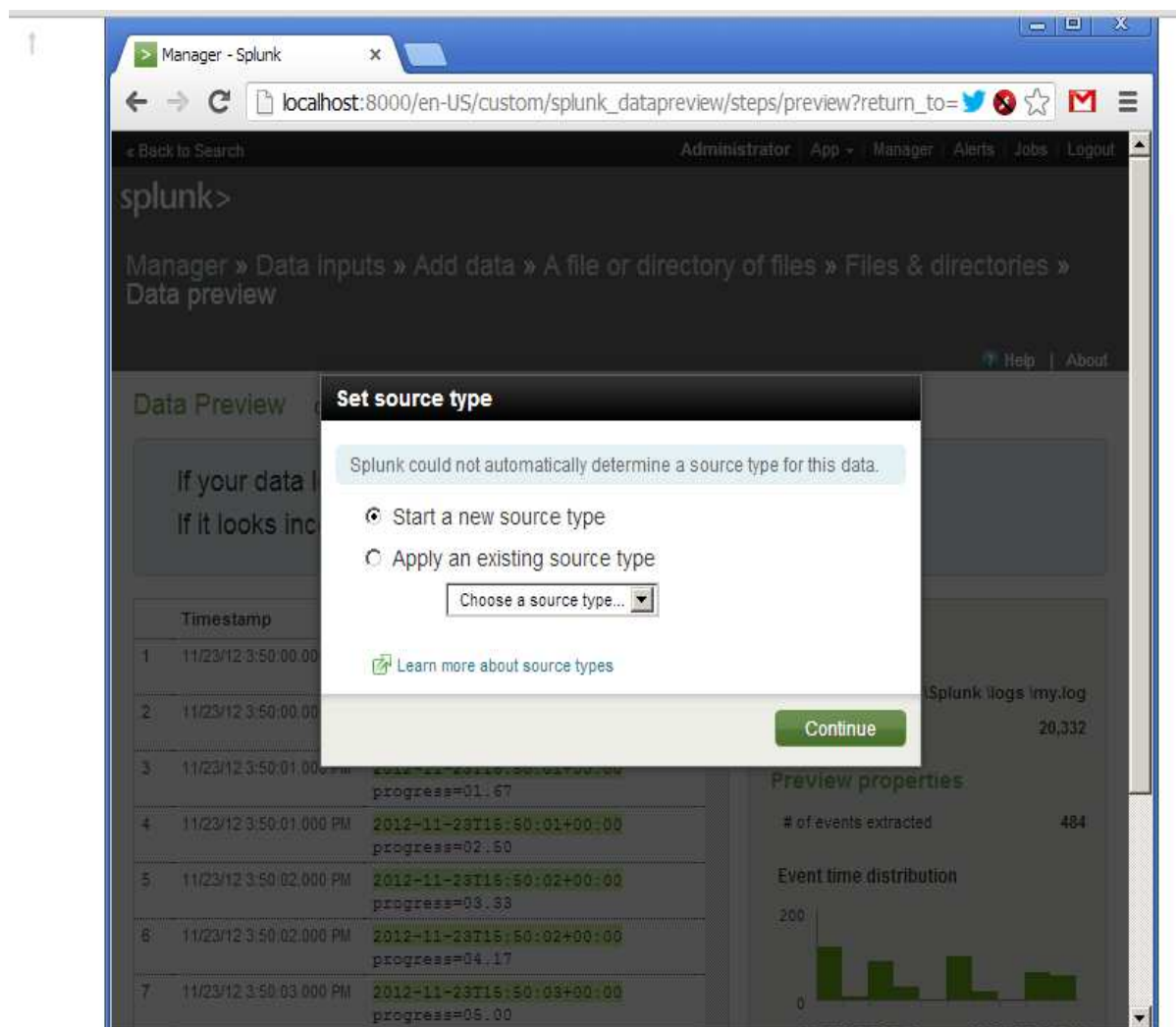
```
2012-11-23T15:58:54+00:00 progress=45.00
2012-11-23T15:58:55+00:00 progress=45.83
2012-11-23T15:58:55+00:00 progress=46.67
2012-11-23T15:58:56+00:00 progress=47.50
2012-11-23T15:58:56+00:00 progress=48.33
2012-11-23T15:58:57+00:00 progress=49.17
2012-11-23T15:58:57+00:00 progress=50.00
```

Prvo što je potrebno jeste prijavljivanje na stranicu Splunk programa, zatim odlazak do menija **Menager** -> **Data Inputs** -> **Add data** -> **A file or directory or files**. Ovde se određuje ime datoteke ili direktorijuma gde se nalazi naš log. Sledeća slika prikazuje tu putanju.



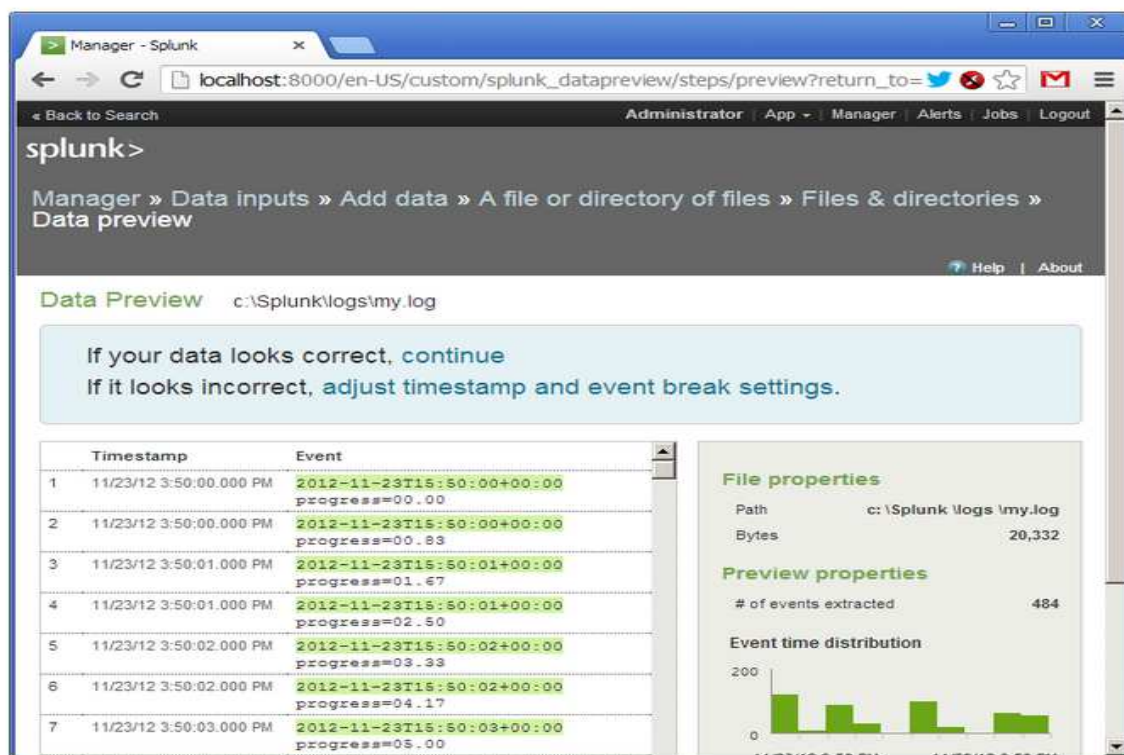
Slika 17. Putanja do izbora datoteka

Kao što je već rečeno, do grananje u Splunk-u se može doći na razne načine. Svaki izvor ima i stabla koja mogu biti samostalno obrađena.



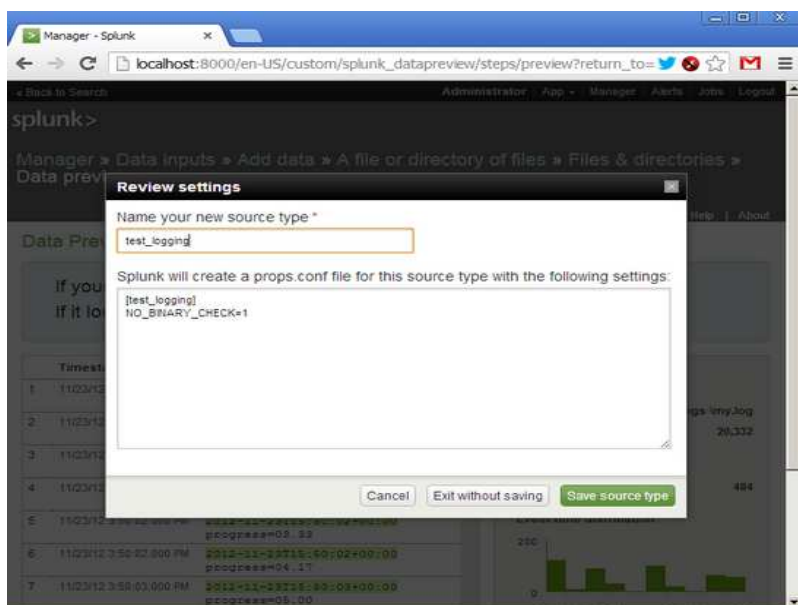
Slika 18 Biranje novog izvora podataka

Vidimo da Splunk „hvata“ fajl i da raščlanjava string polja. Splunk razume dosta datum i vreme formata. Sledeća slika to potvrđuje.



Slika 19: Prepoznavanje formata datum i vreme

Sledeća stavka nam je zadavanje imena našim izvorima - «test_logging» i čuvanje podešavanja.

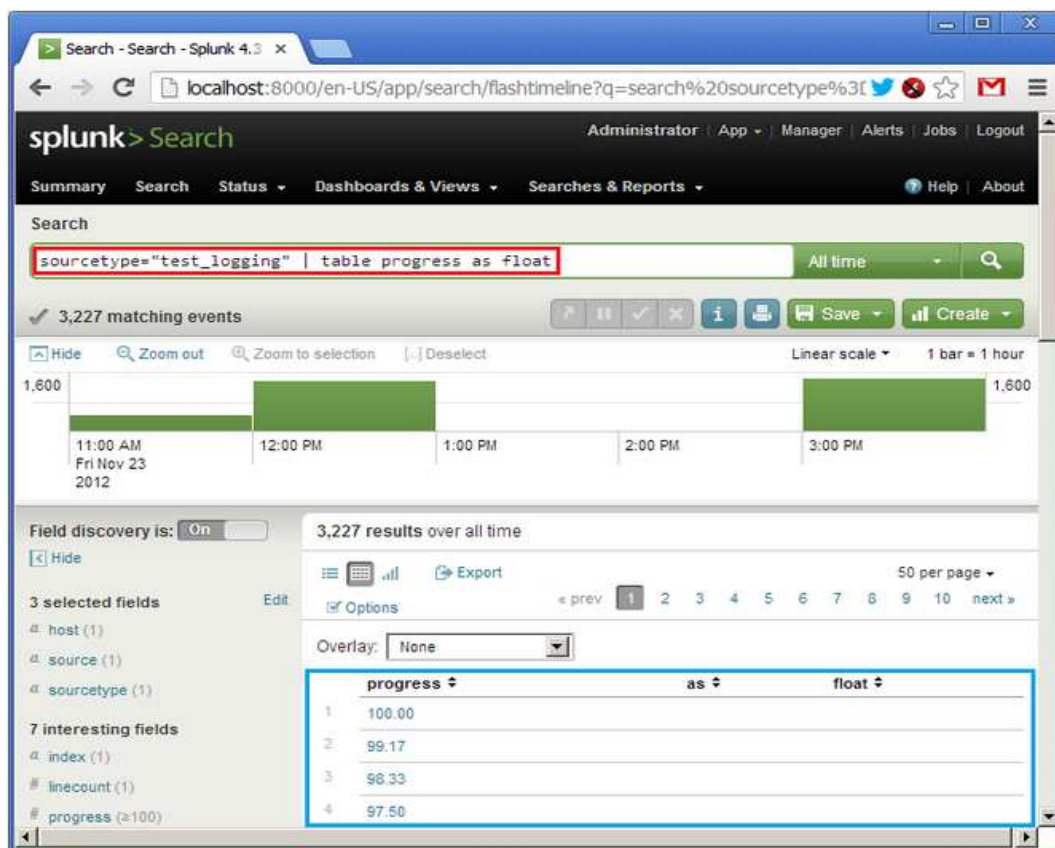


Slika 20. Izvršavanje testiranja

Vraćamo se na početnu stranicu i unosimo Search za pretragu našeg prvog upita koristeći SPL.

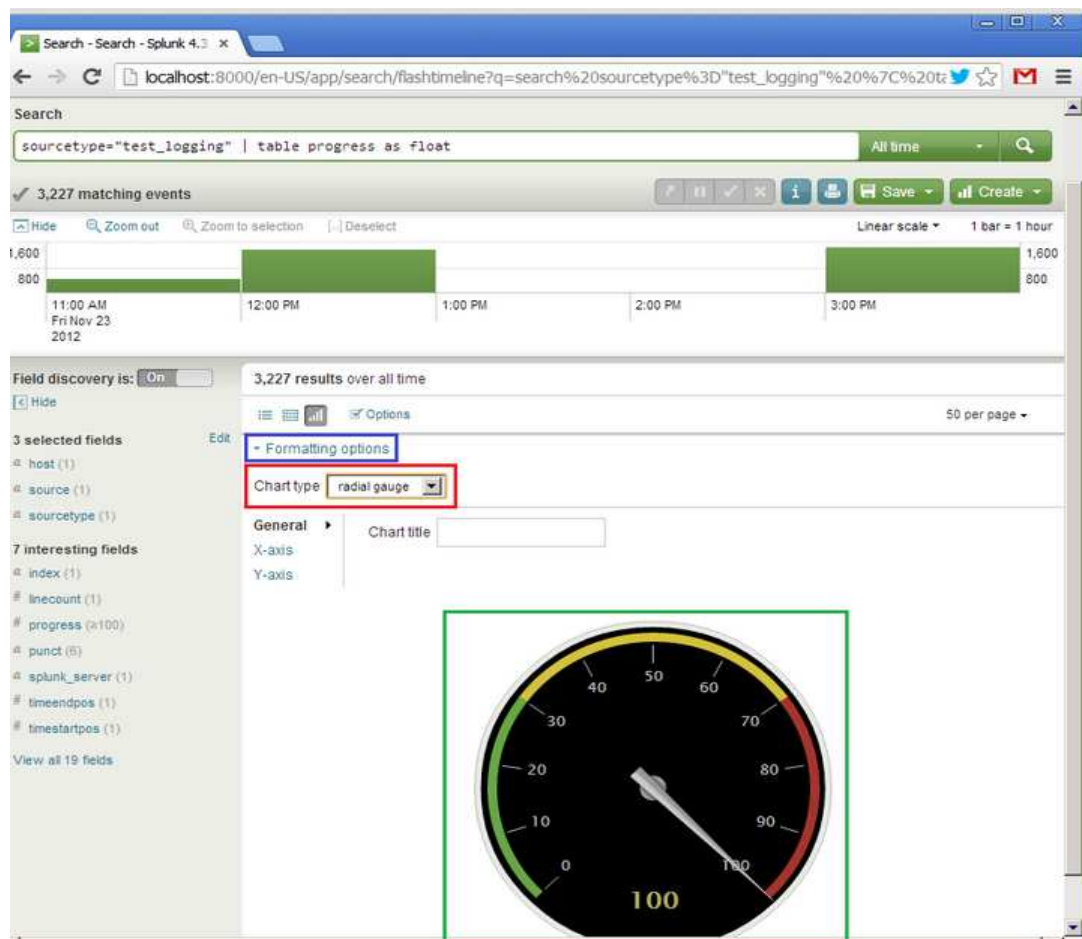
```
sourcetype=«test_logging» | table progress as float
```

Uzimamo dnevnik iz «test_logging», pravimo tabelu koja dodaje kolonu iz oblasti «progress». Ispod vidimo rezultate upita. U UNIX – u SPL princip rada jedne operacije je ulaz u sledeću.



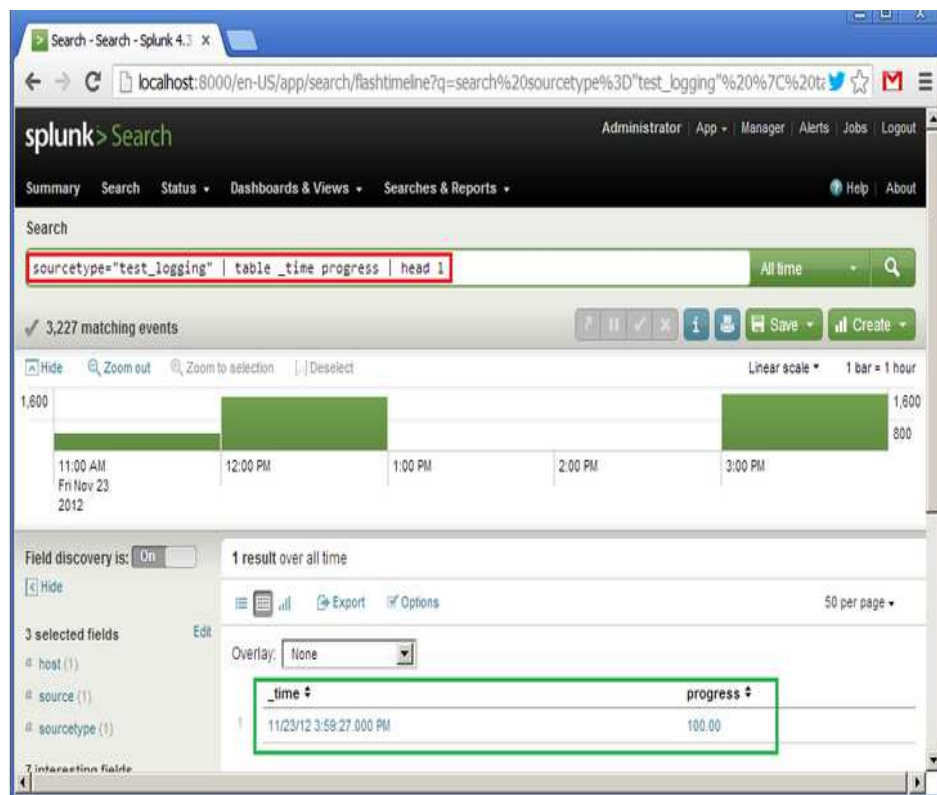
Slika 21. Izgled prozora kod testiranje Logging

Posle ovog prozora i izvođenja testiranja, možemo preći na grafički prikaz. Pošto postoji samo jedno polje koje prikazuje procentualnu vrednost 100% , možemo koristiti polje brzinoera, gde će igla pokazati trenutnu vrednost. Kliknućemo na dugme „Formatting options“ i izabrati tip stavki odnosno grafikona „radijalni kolosek“ (radial gauge), koji će biti označen crvenom bojom.



Slika 22. Grafički prikaz korišćenja logova pomoću „radial gauge-a“

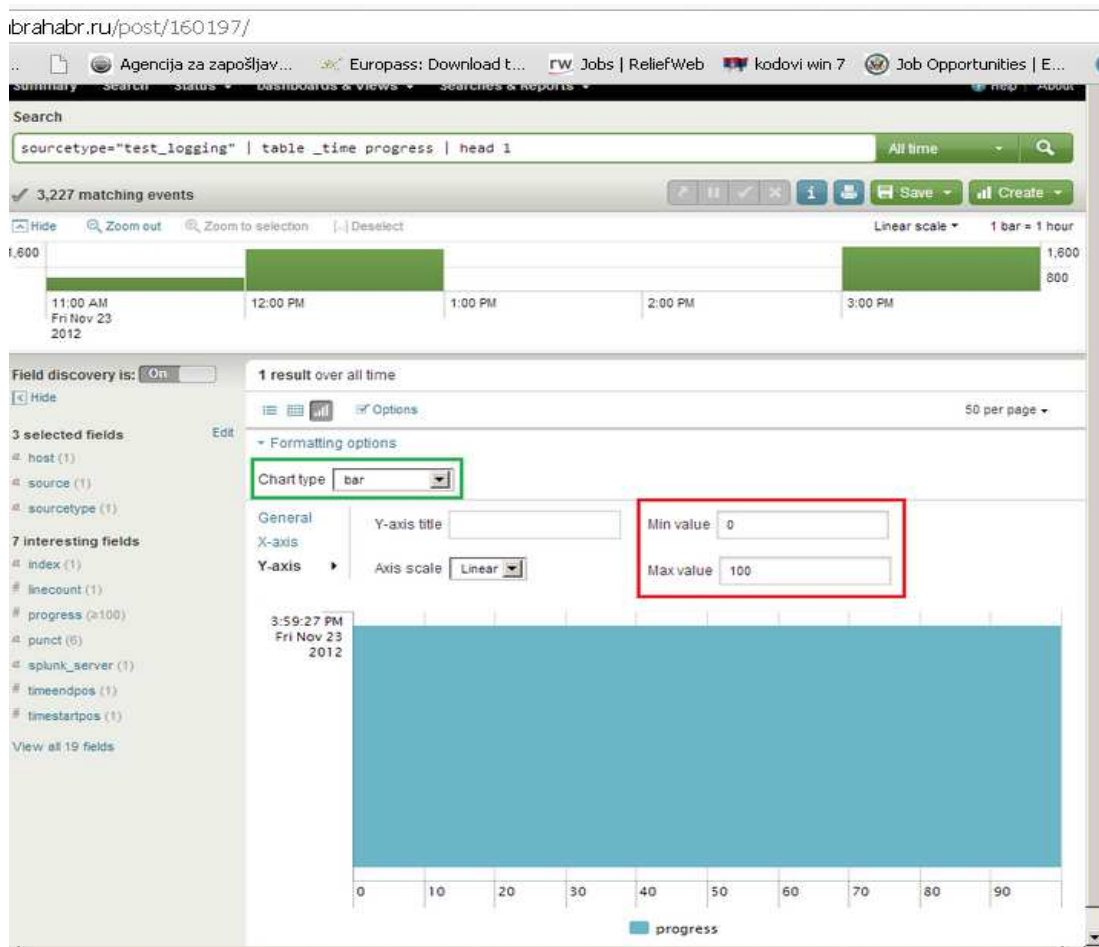
Prvi podatak je spreman, sada ćemo radi eksperimenta ćemo stvoriti još jedan. On će pokazati vrednosti napretka polja, ali sa horizontalnim indikatorom, krećući se sa leva na desno. Upit bi onda izgledao kao na slici, na sledeći način:



Slika 23. Testiranje vrednosti po horizontalnom indikatoru.

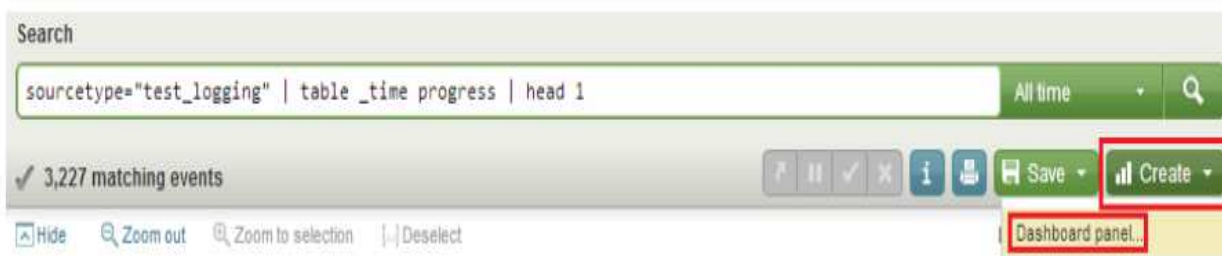
Sledeće je odlazak do opcije „**Formatting options**“ gde biramo opciju „**bar**“ (zelena boja) na Y osi i podešavamo interval od 0 do 100. Ovde X osa ide vertikalno, to pokazuje „time“ a osa Y po horizontali koja pokazuje polje „progress“. Zbog zahteva sa ranijih slika pokazuje vrednost 100, a naš horizontalni indikator smo u potpunosti ofarbali.

Ovo je prikazano na sledećoj slici.



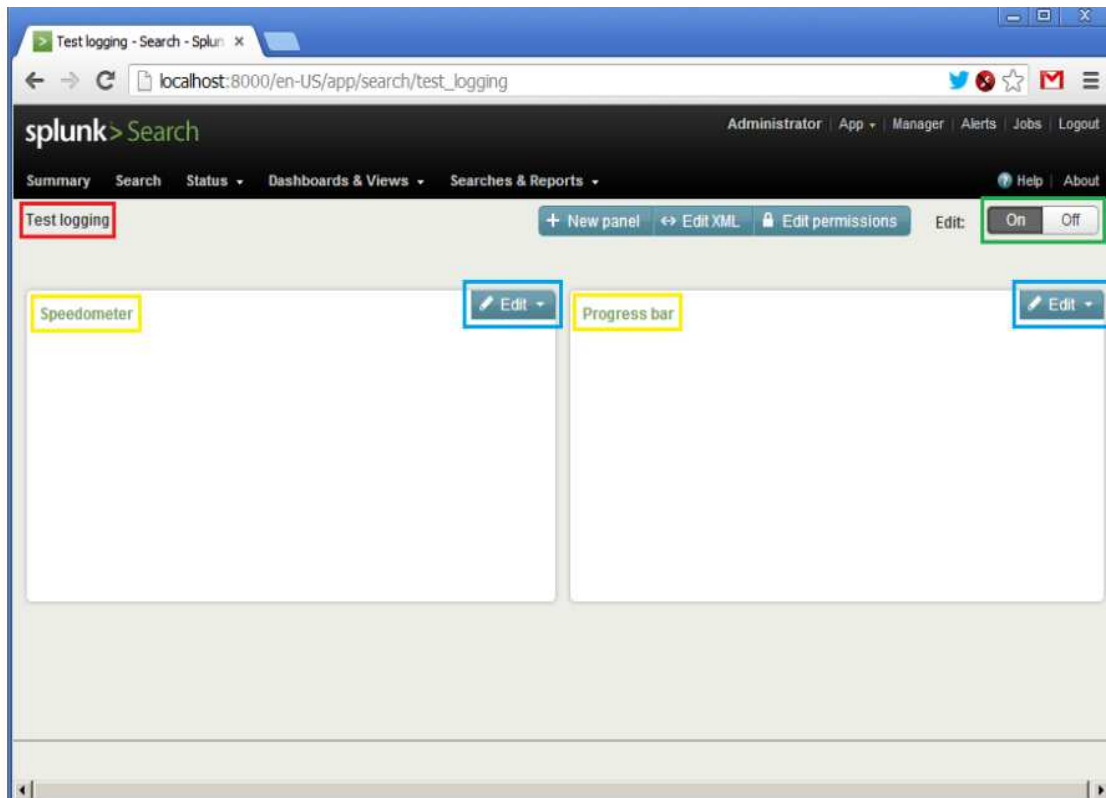
Slika 24. Podešavanje po Y osi i prikaz minimalne i maksimalne vrednosti.

Propušten je prvi vidžet, pomoću brzinomera, otklanjanje grešaka u upitu i njihovih vizuelnih predstavljanja možemo skladištiti u obliku „Dashboard panel“. Da bi smo to uradili idemo na opciju „Create“ i „Dashboard panel“ i čuvamo podešavanja. Pokrećemo naš prvi zadatak „Speedometer“ i drugi „Progress bar“.



Slika 25: Pokretanje prvog zadatka

Kada se skladišti prvi vidžet, biće zatraženo kreiranje tabele. Opcija „Test logging“ je poziva. Kada budemo čuvali drugi zadatak, vidžet dodaje već postojeću tablu.



Slika 26: Dodavanje zadatka i kreiranje dodatnih panela

Dok podaci nisu dostupni, paneli su prazni. Vidimo naziv panela, imena dodataka, aktivne digmiće i dugme „Edit“ koji dodaje upite ili vizuelne prikaze, i vrši osvežavanje intervala oko jedne sekunde.

Moderni sistemi za nadzor „iz kutije“ omogućava nam da pratimo skoro sve učinke pojedinačnih čvorova u sistemu, ali takođe imaju i niz značajnih nedostataka kao što je znanje sve o jednom čvoru sistema kao celine, oni nemaju mogućnost da rukovode sistemskim greškama sa vremenskim ograničenjima koja su manja od 10 po sekundi. Ako se sistem kreće iznad jednog od parametara sistema, to nije za uzbunu, postoji mogućnost da je sam čvor na mreži pod povećanim opterećenjem ili je neki od programa promenio svoj algoritam u praćenju pojedinih čvorova, i nemoguće je pratiti pojedine čvorove postepeno.

Zaključak

Računarska tehnologija se naglo razvija poslednjih godina. Računari postaju sve brži i dosta jeftiniji nego pre, pa samim tim i pristupačniji sve većem broju ljudi. Dolazi do sve većeg broja podataka koji se kreću mrežom, koja je nezamenljiv deo poslovne infrastrukture i predužeca.

Zbog svega toga problemu sigurnosti se mora posvetiti posebna pažnja. Zahtevi koji se odnose na sigurnost informacija unutar neke organizacije značajno su se promenili u nekoliko poslednjih decenija. Pre nego što su se počeli masovno primenjivati uređaji za obradu podataka, podaci koji su smatrani značajnim za organizaciju, štitili su se fizičkim i administrativnim merama.

Od kada se desila pojava računarskih mreža, a samim tim i njen brz napredak i umrežavanje u sistem globalne mreže zvane Internet, sa tim dolazi i do zloupotrebe i narušavanja njene funkcionalnosti u komunikaciji i prenosu informacija. Sve je veći broj napada sa Interneta, slanjem malware-a od strane hakera, i drugih kompjuterskih kriminalaca. Računarske mreže Internet tipa daju brojne prednosti i omogućavaju veću efikasnost rada i smanjenje troškova, ali imaju i svoje mane, jer predstavljaju kritičnu tačku bezbednosti. Naglo je porastao broj napada na računarske mreže, pa se samim tim i povećao sam finansijski gubitak usled tih napada. Pored finansijske dobiti, postoje i razni drugi motive za napade, kao što je krađa poverljivih podataka, ili njihovo oštećenje, kao i oštećenje samih aplikacija i sistema.

Spoljašnja pretnja je pretnja bezbednosti računara kao rezultat zloupotrebe sistema od strane pojedinca ili organizacije. Sama proaktivna digitalna forenzika podrazumeva smanjenje štete izazvane napadom kroz proaktivnu pripremu okruženja., pre faze incidenta, a u cilju postizanja spremnosti organizacije za digitalnu forenzičku istragu.

Osnovni izvor podataka potencijalnih izvora dokaza jeste Log datoteka. Log je osetljiv fajl, u njemu se menjaju podaci i napadač lako može da ih menja.

Literatura:

- [1] Bayuk Jennifer, (2010), *Cyber Forensics Understanding Information Security Investigation*, Stivens Institute of technology Castle Point on Hudson, 518 Babbo Center, USA, jennifer@bayuk.com
- [2] Garrison Clint P., (2010), *Network, Internet, and Cloud Computing*, Corporate Drive, Burlington, MA, USA, Page: 6-40.
- [3] Garza Dave, Matthew Kane, et, (2010) *Computer Forensics Investigation Wireless Networks and Devices*, Clifton Park, NY, USA. Page: 19-35. www.cengage.com.
- [4] Garza Dave, Kane Matthew, et, (2010), *Computer Forensics Investigation Network Intrusions & Cyber Crime*, Clifton Park, NY, USA, Page: 27-40, www.cengage.com.
- [5] Grance Tim, et, (August 2005), *Nist, Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response*, Information Technology Laboratory National Institute of Standards and Technology Gaithersburg.
- [6] Hildebrant M., Kiltz M., and J. Dittmann, (10-12 May 2011) *A common scheme for evaluation of forensic software*, Proc. Sixt International Conference on IT Security Incident Management and IT Forensics – IMF, Stuttgart, Page. 92-106
- [7] Kanellis Panagiotis, et, (2006), *Forensic Science in Cyberspace*, Information Society, S.A., Greece, Univesity of Peloponnese, Greece. Page: 19-28.

- [8] Kaurin Tanja, et, (Mart 2012), *Smernice za izbor alata digitalne forenzike*, INFOTEH- Jahorina, Fakultet za pravne i poslovne studije, Novi Sad, Srbija, tanja.milosevic@useens.net.
- [9] Liang James, (2010), *Evaluating A selection of Tools for Extraction of Forensics*, School of Computing and Mathematical Science, New Zeland.
- [10] Milosavljevic, M., i Grubor G., (2009), *Istraga kompjuterskog kriminala*, Univerzitet Singidunum, Beograd.
- [11] Nikkel Bruce, (May 2006), *The Role of Digital Forensics within a Corporate Organization*, IBSA Conference, Vienna.
- [12] Petković D., (Novembar 2007), *WinMax*, CET Čitalište 67.
- [13] Timčenko Valentina, et, (4-5 decembar 2012), *Primena Forenzičke analize u sistemima zaštite savremenih IP mreža*, XXX Simpozijum o novim tehnologijama-PosTel, Institut Mihajlo Pupin, Beograd.
- [14] Vel Oliver, *Mining E-mail Authorship*, Information Technology Division, Defence Science and Technology Organisation, P.O.Box 1500, Salisbury, Australia, oliver.devel@dsto.defence.gov.au
- [15] *Zaštita Mreža od napada virusa*, Sveučilište Zagreb.
- [16] <http://www.analog.cx/how-to/index.html>. Accessed 2/2007.

