

FORENZIČKA ANALIZA LOG DATOTEKA

Angelina Galetin, dipl. inž. informatiku

angelina@neobee.net

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 datoteke i to na WindowsUpdate.log datoteku, kao datoteku operativnog sistema Windows. Beležena su neki događaji i analiziran je njihov zapis u WindowsUpdate.log datoteku. 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 WindowsUpdate.log datoteka znači za digitalnu forenziku i na koji način ona može da se iskoristi.

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

1. UVOD

Log datoteka (dnevnik rada) predstavlja zapis događaja u računarskom sistemu ili mreži. Svaki zapis sadrži informacije relevantne za specifičan događaj, validni ili invalidni pokušaji prijavljivanja, korišćenje resursa kao što su kreiranje, otvaranje ili brisanje datoteka. 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. Log datoteke sadrže veliki broj različitih informacija, te ih možemo podeliti u nekoliko kategorija u odnosu na servise koji su instalirani.

- *Sigurnosni softver (programi zaštite).* Najčešće se koristi za detekciju aktivnosti malicioznih programa, te zaštitu sistema i podataka. Predstavlja glavni izvor sigurnosnih log datoteka. Tipovi sigurnosnog softvera su: Softver za zaštitu od malicioznih programa, Softveri za detekciju i sprečavanje upada u sistem-*IDPS (Intrusion Detection and Prevention Systems)*, Softver za kontrolu udaljenog pristupa, *Web proxy*, Softver za upravljanje ranjivostima, Autorizacioni serveri, Ruteri, Zaštitne barijere (*Firewalls*), Mrežni karantinski serveri.
- *Log datoteke operativnog sistema.* Operativni sistemi beleže različite informacije koje se odnose na sigurnost. Najčešće se susrećemo sa: Sistemskim događajima (*events*), Kontrolni zapisi (tragovi).
- *Log datoteke nastale korišćenjem aplikacija.* Operativni sistemi i sigurnosni softver služe da obezbede zaštitu za aplikacije koje skladište, omogućavaju obradu i pristup podacima. Najčešće se koriste *off-the-shelf* komercijalne aplikacije (*COTS*) kao što su e-mail serveri i klijenti, web serveri i klijenti, fajl

serveri i klijenti, te serveri i klijenti baze podataka. Često se koriste i *off-the-shelf* poslovne aplikacije (*GOTS*) kao što su podrška finansijskom menadžmentu, proceduralni sistem, ERP (*Enterprise Resource Planning*) i CRM (*Customer Relationship Planning*) sistemi za planiranje resursa itd. Pored ovih, koriste se i aplikacije koje se namenski kreiraju za određene potrebe.

1.1. KONFIGURISANJE LOG DATOTEKA

Administrator sistema mora konfigurisati log datoteke da bi se evidentirale neophodne informacije u željenom formatu i na definisanoj lokaciji. Takođe, 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. Naime, svaka pojedinačna log datoteka sadrži informacije iz više izvora. Na primer, log datoteka operativnog sistema sadrži informacije samog operativnog sistema, sigurnosnog softvera, te informacije nastale korišćenjem aplikacija. Za svaki prepoznati izvor log datoteke, administrator mora odrediti koji tip događaja svaki izvor log datoteke mora ili bi trebalo da beleži. Takođe, administrator mora da odredi koje karakteristike podataka moraju ili bi trebalo da budu beležene za svaki tip događaja. Administratorska sposobnost da konfiguriše svaki izvor log datoteka zavisi od mogućnosti koje nudi određeni tip izvora log datoteka. Konfigurisanje izvora log datoteka možemo razvrstati u tri kategorije:

1. *kreiranje izvora log datoteka,*
2. *čuvanje i uništavanje izvora log datoteka i*
3. *zaštita izvora log datoteka.*

2. ANALIZA I FILTRIRANJE LOG DATOTEKA

Dobra analiza log podataka je najizazovniji, a istovremeno i najznačajniji korak. Iako je analiza log podataka veoma težak i obiman posao, automatizacija analize log podataka donekle može biti dobar put da se analiza log podataka izvršava u kraćem vremenskom periodu i da daje relevantne rezultate.

2.1. 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 podatka. Najbolji način za razumevanje log podataka jeste da se pregled i analiza vrše periodično i konstantno (na primer, svaki dan). Cilj je da se obezbedi razumevanje tipičnih log podataka, obuhvatajući najbitnije log podatke za sistem. Dnevni pregledi podataka bi trebalo da uključuju one podatke koji se smatraju važnim, te one koji nisu u potpunosti razumljivi. Upravo ovakva analiza log podataka zahteva najviše vremena i predstavlja najveći izazov. Vremenom, kada osnovne aktivnosti postanu već jasne, dnevni pregledi i analize zahtevaju manje vremena i fokus analize 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. Zbog toga 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. Drugi izveštaj je bitno generisati da bi se obezbedilo prepoznavanje podataka koji su najbitniji.

2.2. PRIORITET LOG PODATAKA

Određivanje prioriteta analize log podataka je veoma izazovan posao. Neki izvori log podataka dodeljuju svoje prioritete za svaki podatak. Svaki izvor log podataka ima svoju skalu za određivanja prioriteta log podatka. Zbog toga je veoma teško porediti prioritete log podataka sa različitih izvora. Takođe, kriterijum za određivanje prioriteta podataka zavisi od potreba i zahteva, a nemoguće je da su svi zahtevi i potrebe kompanija jednaki,

što dodatno otežava tumačenje prioriteta podataka. Svaka kompanija bi trebalo da odredi svoje kriterijume za određivanje prioritete podataka prilikom analize. Kriterijumi za određivanje prioriteta trebalo bi da budu: tip podataka, novi tip podataka, izvor log podataka, izvor ili destinacija IP adrese, vreme u danu ili dan u nedelji, učestalost. Da bi određivanje prioriteta log podataka bilo uspešno, potrebno je obezbediti povezanost log podatka da bi se obezbedio njihov kontekst. Ako se pojavi isti podatak na dva različita izvora, povezanost tih podataka bi obezbedilo sigurnije prepoznavanje i bilo bi više podataka koji ukazuju na napade, nego što bi bilo sa jednog izvora. Još jedna prednost korišćenja povezanosti prilikom određivanja prioriteta je korišćenje informacija poznatih ranjivosti operativnog sistema i aplikacija da bi se obezbedio veći prioritet za određeni log podatak koji je povezan sa tim ranjivostima.

2.3. KOMPARACIJA ANALIZE LOG PODATAKA SA SISTEMSKOG I INFRASTRUKTURNOG NIVOA

Analiza je veoma slična sa oba aspekta - sistemskog i infrastrukturnog. Glavna razlika je u tome što je za infrastrukturne administratore (mrežne administratore) log analiza primarna odgovornost, dok je za administratore sistema log analiza sekundarna odgovornost. Sa obzirom na to infrastrukturni administratori vrše log analizu koja se dešava svaki dan, dok sistemski administratori vrše log analizu periodično, sa obzirom na potrebe i kritične momente. Takođe, infrastrukturni administratori imaju pristup osetljivijim alatima za analizu. Bez obzira na to koliko je analize izvršeno od strane infrastrukturnih administratora, administratori sistema najčešće moraju da izvrše određene analize.

- Analiza podataka koji su od velike važnosti za sistem, a sa infrastrukturnog nivoa nisu od velike važnosti;
- Analiza podataka sa izvora log podataka koji nisu dostupni sa stanovišta infrastrukturnog nivoa;
- Analiza podataka čiji kontekst ne može biti razumljiv sa bilo kog drugog nivoa osim sa sistemskog.

Administratori sistema mogu vršiti analizu korišćenjem određenih alata i tehnika. U nekim sistemima, pogotovu u onim sa više izvora podataka, infrastrukturna analiza bi trebalo da se vrši lokalno, a da se tu čuvaju podaci sa svih sistemskih izvora podataka. U drugim sistemima posebno za obavezne log formate, administratori mogu vršiti analizu za svaki izvor log podataka posebno koristeći specijalizovane log preglede, redukcione alate i slične alate koji omogućavaju lakšu analizu. Još jedna mogućnost je da se log podaci eksportuju u jedinstvenu bazu log podataka i da se korišćenjem upita dolazi do željene analize. Upiti predstavljaju odličan način za filtriranje log podataka za analizu. Ako je moguće automatizovati proces analize, moglo bi biti izvodljivo kreiranje svakodnevnih izveštaja i njihovo prezentovanje administratorima na pregled. Administratori mogu vršiti dalje potrebno istraživanje značajnih događaja identifikovanih u izveštajima. Da bi izvršili uspešno preglede i analizu, sistemski i infrastrukturni administratori bi, na osnovu znanja i iskustva, trebalo da imaju dobro razumevanje sledećeg:

- Poznavanje politike organizacije, tako da ne dođe do njenog narušavanja
- Poznavanje sigurnosnog softvera, uključujući tipove događaja koji prepoznaje svaki softver
- Poznavanje logovanja svakog pojedinačnog operativnog sistema i glavnih aplikacija sa svim mogućnostima i karakteristikama

- Poznavanje karakteristika uobičajenih tehnika napada, posebno na koji način te tehnike bi mogle biti beležene u svakom sistemu
- Poznavanje softvera za analizu, kao što su log pregledi, redukcionu log skriptovi ili upiti.

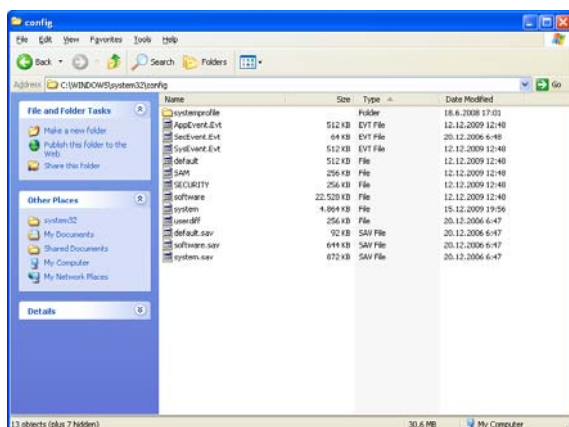
Organizacije često zahtevaju od sistem administratora da izveštavaju infrastrukturne administratore o rezultatima njihovih analiza. Ovo može pomoći da se sistemskim administratorima obezbedi siguran način analize log podataka. Informacije u izveštajima su veoma bitne infrastrukturnim administratorima, jer oni nemaju uvid u model aktivnosti na sistemskom nivou. Infrastrukturni administratori mogu proslediti sistem administratorima iskustvena znanja stečena iz izveštaja, tako da oni budu u stanju da lakše prepoznaju slične aktivnosti u sistemu. Infrastrukturni administratori bi takođe trebalo da kreiraju izveštaje koji sumiraju kako rezultate njihove analize, tako i rezultate izveštaja sistemskih administratora. Pravovremeno deljenje iskustva među administratorima, kao i obaveštavanje menadžmenta o rezultatima izveštaja ukazuje na neophodnost dobrog organizovanja upravljanja log datotekama u cilju poboljšanja poslovanja i sigurnosti informacija organizacije.

2.4. STUDIJA SLUČAJA: UPOTREBA FORENZIČKOG ALATA KOMANDNE LINIJE ZA ANALIZU LOG DATOTEKA WINDOWS OS

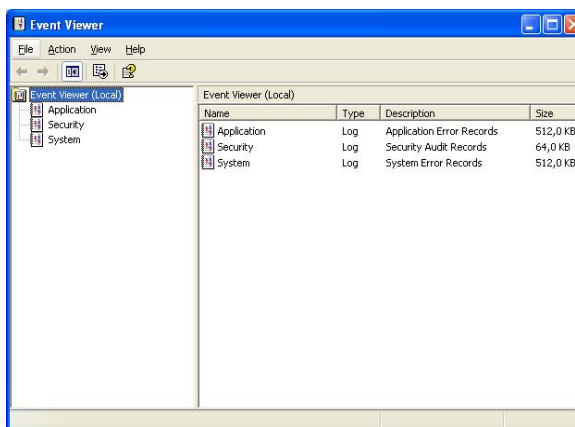
Da bi log datoteke bile korisne potrebno je izvršiti njihovu analizu. Mogućnost tumačenja log datoteka je veoma bitna operacija koja pre svega obezbeđuje sigurnost sistema. Log datoteke mogu da daju dovedu do rešenja za mnoge probleme koji se javljaju u sistemu.

2.4.1 WINDOWS LOG DATOTEKE

Nekim log datotekama Windows operativnog sistema mogu da pristupaju samo administratori. Takva je na primer Security Event Log datoteka. Drugim log datotekama, one koje se generišu korišćenjem aplikacija, može da pristupi bilo koji korisnik. Windows operativni sistem generiše tri log datoteke: SysEvent.Evt, SecEvent.Evt i AppEvent.Evt. Svaka od njih se čuva kao posebna datoteka. Takođe, svakoj od njih se može pristupiti ako se prati putanja C:\WINDOWS\system32\config.



Slika 1. Llog datoteke SysEvent.Evt, SecEvent.Evt



Slika 2. Event Viewer

Windows operativni sistem generiše i datoteku događaja (*logevent*) koja se nalazi na sledećoj lokaciji Start-> Control Panel -> Administrative Tools -> Event Viewer. Ovde se nalaze poruke koje ukazuju na događaje koji su se desili u sistemu. Za analizu log datoteka

postoje programi koji omogućavaju lakši i brži način čitanja svakog novog upisa u log datoteku.

2.4.2 WINDOWSUPDATE.LOG DATOTEKA

U Windowsupdate.log datoteci se nalaze informacije o svim transakcijama koje generiše Widows Update klijent. Da bi se pristupilo Windowsupdate.log datoteci potrebno je iz Start menija odabrati opciju Run i uneti Windowsupdate.log. Ova datoteka sadrži sledeće informacije:

Datum	Vreme	PID	TID	Komponenta	Tekst
2005-06-01	18:30:03	992	810	Misc	= Logging initialized
2005-06-01	18:30:03	992	810	Misc	= Process:
2005-06-01	18:30:03	992	810	Misc	= Module:

Tabela 1. Informacije u Windowsupdate.log datoteci

Veoma je bitno prepoznati koji servis je izvršio upis u Windowsupdate.log datoteku. Postoje tri takva servisa sa različitom identifikacijom (*CallerID*).

```
2005-06-01      18:30:33  992    58c    Agent    *****
2005-06-01      18:30:33  992    58c    Agent    ** START ** Agent: Finding
updates [CallerId = WindowsUpdate]
2005-06-01      18:30:33  992    58c    Agent    *****
```

Slika 3. Log podaci nastali upisom servisa WindowsUpdate

```
2005-06-22      13:02:11 1000    594    Agent    *****
2005-06-22      13:02:11 1000    594    Agent    ** START ** Agent: Finding
updates [CallerId = MicrosoftUpdate]
2005-06-22      13:02:11 1000    594    Agent    *****
```

Slika 4. Log podaci nastali upisom servisa MicrosoftUpdate

```
2005-06-02      11:37:18  992    4e8    Agent    *****
2005-06-02      11:37:18  992    4e8    Agent    ** START ** Agent: Finding
updates [CallerId = AutomaticUpdates]
2005-06-02      11:37:18  992    4e8    Agent    *****
```

Slika 5. Log podaci nastali upisom servisa AutomaticUpdates

Automatic Updates servis opisuje osnovna servisna podešavanja sa sledećim informacijama: verzija servisa, direktorijum koji je korišćen, tip pristupa, proxy, status konekcije.

```
2005-06-01      18:30:03  992    810    Service *****
2005-06-01      18:30:03  992    810    Service ** START ** Service: Service
startup
2005-06-01      18:30:03  992    810    Service *****
2005-06-01      18:30:03  992    810    Agent    * WU client version 5.8.0.2468
2005-06-01      18:30:03  992    810    Agent    * SusClientId = '071ffd36-f490-
4d63-87a7-f7b11866b9fb'
2005-06-01      18:30:03  992    810    Agent    * Base directory:
C:\WINDOWS.0\SoftwareDistribution
2005-06-01      18:30:03  992    810    Agent    * Access type: Named proxy
2005-06-01      18:30:03  992    810    Agent    * Default proxy: test:80
2005-06-01      18:30:03  992    810    Agent    * Network state: Connected
2005-06-01      18:30:03  992    7a0    Agent    ***** Agent: Initializing
Windows Update Agent *****
```

Slika 6. Osnovna servisna podešavanja servisa AutomaticUpdates

Ukoliko se pojavi neka greška na Windows Update Web stranici, potrebno je otvoriti Windowsupdate.log datoteku i pronaći tu grešku pretragom po ključnim rečima FATAL ili WARNING. U sledećem primeru je najpre pronađena ključna reč FATAL, a potom je prepoznata greška is 0x80072EEF i kada je pronađena reč WARNING uvidelo se koje je greška u pitanju. U posmatranom primeru proxy server "Test" je prouzrokovao grešku.

```

2005-06-02      04:32:01  992      158      Setup      FATAL: IsUpdateRequired failed
with error 0x80072eef
2005-06-02      04:32:01  992      158      Misc       WARNING: Send failed with hr =
80072eef.
2005-06-02      04:32:01  992      158      Misc       WARNING: SendRequest failed with
hr = 80072eef. Proxy List used: <Test:80 > Bypass List used : <(null)> Auth Schemes used :
<NTLM;Negotiate (NTLM or Kerberos);>
2005-06-02      04:32:01  992      158      Misc       WARNING: WinHttp:
SendRequestUsingProxy failed for
<http://update.microsoft.com/v6/windowsupdate/redir/wuredir.cab>. error 0x80072eef

```

Slika 7. Pronalaženje greške u Windowsupdate.log datoteci

Neki od osnovnih zapisa u Windowsupdate.log datoteku su:

```

2005-06-01      18:30:03  992      810      Service    *****
2005-06-01      18:30:03  992      810      Service    ** START ** Service: Service
startup
2005-06-01      18:30:03  992      810      Service    *****

```

Slika 8. Startovanje servisa

```

2005-06-01      18:30:03  992      810      Agent      * WU client version 5.8.0.2468
2005-06-01      18:30:03  992      810      Agent      * SusClientId = '071ffd36-f490-
4d63-87a7-f7b11866b9fb'
2005-06-01      18:30:03  992      810      Agent      * Base directory:
C:\WINDOWS.0\SoftwareDistribution
2005-06-01      18:30:03  992      810      Agent      * Access type: Named proxy
2005-06-01      18:30:03  992      810      Agent      * Default proxy: test:80
2005-06-01      18:30:03  992      810      Agent      * Network state: Connected
2005-06-01      18:30:03  992      7a0      Agent      ***** Agent: Initializing
Windows Update Agent *****
2005-06-01      18:30:03  992      7a0      Agent      ***** Agent: Initializing
global settings cache *****
2005-06-01      18:30:03  992      7a0      Agent      * WSUS server: <NULL>
2005-06-01      18:30:03  992      7a0      Agent      * WSUS status server: <NULL>
2005-06-01      18:30:03  992      7a0      Agent      * Target group: (Unassigned
Computers)

```

Slika 9. Dostupni parametri Windows Update-a

```

2005-06-01      18:30:09  3948      918      Misc       ===== Logging initialized
(build: 5.8.0.2469, tz: -0700) =====
2005-06-01      18:30:09  3948      918      Misc       = Process: C:\Program
Files\Internet Explorer\iexplore.exe
2005-06-01      18:30:09  3948      918      Misc       = Module:
C:\WINDOWS.0\system32\wuweb.dll

```

Slika 10. Pristup korisnika na Windows Update Web stranicu korišćenjem Internet Explorer-a i ActiveX kontrola

Sledeći primer ilustruje pokušaj ažuriranja operativnog sistema. Proces je prekinut i zabeleženi su podaci u WindowsUpdate.log datoteci.

```

2009-12-19      21:30:45+0100      1136      4b0      WUCheckForUpdatesAtShutdown
failed, hr=8024A000

```

Slika 11. Traženje dostupnih ažuriranja od strane Windows Update

```

2009-12-19      21:31:02+0100      840      34c      Service received logoff
notification

```

Slika 12. Prekinuto ažuriranje

```

2009-12-19      21:31:18+0100      840      888      AU Restart required....

```

Slika 13. Automatic Update zahteva restatovanje

```

2009-12-19      21:31:18+0100      520      4ec      WUAutoUpdateAtShutdown failed,
hr=8024A000

```

Slika 14. Windows Update nije izvršen i javljena je greška

```

2009-12-19      21:31:18+0100      840      418      AU is disabled, not initializing
any handlers

```

Slika 15. Automatic Update je onemogućen

3. ZAKLJUČAK

U radu je radi ilustracije korišćena WindowsUpdate.log datoteka sa nekoliko prikaza događaja koji mogu da se dese. Izazvani su i neki namerni prekidi da bi se videlo kako se ti događaji beleže u ovoj log datoteci.

Poseban je akcenat stavljen na čitanje WindowsUpdate.log datoteke. Predstavljeno je na koji način može da se dođe do određenih podataka iz WindowsUpdate.log datoteke.

U nedostatku *free* alata za analizu log datoteka i neraspoloživosti licenciranih alata, korišćen je forenzički alat komandne linije (DOS komande) koje se nalaze u operativnom sistemu Windows.

Sa aspekta digitalne forenzike, može se zaključiti da su log datoteke, njihova analiza i filtriranje veoma značajne za prikupljanje podataka o događajima koji su se desili u računarskom sistemu ili mreži. Pre svega, potrebno je dobro konfigurisati kreiranje log datoteke da bi ona bila čitljiva i da bi se analiza vršila dovoljno brzo. Dobra analiza i filtriranje log datoteka može digitalnog forenzičara usmeriti na pravi put u istrazi i ukazati na to kada su se desili neki događaji relevantni za istragu kao i ko je izazvao te događaje.

WindowsUpdate.log datoteka nudi mnogo podataka koji mogu biti od velike koristi, ali za detaljnu analizu je potrebno koristiti složenije alate za analizu i filtriranje bezbednosno relevantnih log događaja. Dobro konfigurisanje, analiza i filtriranje log događaja ima mnoštvo prednosti kao što je smanjenje kompleksnosti analize, ali treba biti i veoma obazriv je moguće isfiltrirati značajan bezbednosni događaj i time dobiti pogrešni zaključci u forenzičkoj analizi.

4. LITERATURA

1. Kent K., Souppaya M., *Guide to Computer Security Log Management*, National Institute of Standards and Technology, Gaithersburg, 2006.
2. Qiao S., Zhang H., *An Automatic Logfile Analyzer for Parallel Programs*, University Hamilton, Canada
3. *Installing and Administering Internet Services*, HP 9000 ,Networking, Edition 8, 2000
4. <http://en.wikipedia.org>, *Log managment and intelligenc*, <http://en.wikipedia.org>
5. <http://en.wikipedia.org> *Server log*, <http://en.wikipedia.org>
6. <http://en.wikipedia.org>, *Web log analaysi*, <http://en.wikipedia.org>
7. <http://en.wikipedia.org>, *Data logging*, <http://en.wikipedia.org>
8. <http://en.wikipedia.org>, *Common log format*, <http://en.wikipedia.org>
9. <http://en.wikipedia.org>, *Syslog*, <http://en.wikipedia.org>
10. <http://en.wikipedia.org> , *List of web analysis software*, pristupljeno decembra 2009.
11. <http://www.stonehenge.com>, *Logfile analysis*, pristupljeno decembra 2009.
12. <http://www.exacttrend.com>, pristupljeno decembra 2009.
13. <http://www.velocityreviews.com>, pristupljeno decembra 2009.
14. <http://www.httpd.apache.org>, pristupljeno decembra 2009.
15. <http://www.loganalysis.com>, pristupljeno decembra 2009.

LOG DATA FORENSIC ANALYZING

Abstract: Everything that happens in a computer system or network should be evident and save the information relevant to a specific occurance. Log file is a record of the activities occured in a computer system or network. Originally, log files were used for solving problems of a computer system, but today log files have much more functions. They are used for optimazing the systems and networks, following a user's acts and generating datas which are useful for researching of mallicious programme activities. For these reasons log files become very significant from phisical forensic perspective. In the first part of the research project, a theoretical review of the basic datas about log files and their analysis is made. In the second part, there is a stress on log files, especially a WindowsUpdate.log file as a file of an operative system. It is adduced what could be found as a record in this file as well as in what way specific records could be found and

interpreted. It is ascertained what WindowsUpdate.log file means for digital forensic and in what way it could be used.

Key words: Log file, log file analyses, forensic importance of a log file analyses, WindowsUpdate.log file