DIGITALNA FORENZIČKA ISTRAGA U KORPORACIJSKOJ ZAŠTITI INFORMACIJA

DIGITAL FORENSIC INVESTIGATION IN COORPORATION INFORMATION SECURITY

Gojko Grubor, Angelina Galetin, Univerzitet Singidunum

Sažetak

Na tržištu postoji veliki broj forenzičkih alata koji lako mogu zbuniti forenzičara pri odabiru odgovarajućeg za konkretan zadatak. U ovom istraživačkom projektu izvršena je kratka revizija procesa digitalne forenzičke analize i osnovnih karakteristika i tipično zahtevanih funkcionalnosti softverskih forenzičkih alata. Zatim su analizirane osnovne funkcionalnosti FTK softverskog forenzičkog alata. FTK predstavlja skup forenzičkih alata koji može da izvrši više koraka digitalne forenzičke istrage. Koristeći FTK forenzički alat prikazan je tok forenzičke istrage od akvizicije do izveštavanja pri čemu su analizirane karakteristike svakog koraka istrage i beležene prednosti, ali i nedostaci FTK forenzičkog alata. Za potrebe verifikacije značaja forenzičke istrage u korporacijskoj zaštiti informacija korišćena su dva USB uređaja, od kojih je jedan zaražen malicioznim programom, a drugi nije. Verifikacija je izvršena na tri različita slučaja akvizicije i analize dva USB uređaja. Prikazani su rezultati verifikacije i jasno istaknute prednosti i nedostaci FTK forenzičkog alata, prihvaćenog od strane pravosudnih organa većine država.

Ključne reči: digitalna forenzika, forenzički alat, akvizicija, analiza, fizička kopija

Abstract

There are a great number of forensic tools which can easily make confusion for a forensics expert choosing the appropriate tool for a particular process. In the researching project the revision of a digital forensic analysis process and the basic characteristics and typical requested functionalities of the forensic software tools was made. Then, the basic functionalities of FTK forensic software tool were analyzed. The FTK is a set of forensic tools which can be used through numerous steps of a digital forensic investigation. Using the FTK forensic tool, the flow of a digital forensic investigation is presented, from the acquisition to the reporting. In this process, characteristics of each phase of the investigation was analyzed and the advantages and disadvantages of the FTK forensic tool were recorded. The two USB memory devices are used for the purpose of verification digital forensic in coorporate information cecurity. One of them was infected by malware. Doing acquisition and making analysis of these two USB memory devices on the three different cases, the verification was made. The results of verification and the advantages as well as disadvantages of the FTK forensic tool, accepted by the laws of majority countries, were made and clearly emphasized.

Key words: *digital forensic, forensic tool, aquisition, analysis, fisical copy*

1. UVOD

Razvojem internet tehnologija i povećanim umrežavnjem lokalnih i korporacijskih računarskih mreža, rastu i brojni napadi i zloupotrebe od narušavanja regularnih servisa do svih oblika kompjuterskog kriminala. Napade mogu izazvati maliciozni programi koji kruže Internetom ili neposredno hakeri, krakeri, vandali ili kompjuterski teroristi. Razlozi za pojavu napada iz samih mreža organizacija i sa Interneta su različiti - od sticanja finansijske i druge dobiti do izazova, znatiželje, samopotrvđivanja, krađe informacija, špijunaže pa i klasičnih neprijateljskih opreracija sa ciljem uništavanja informacione infrastrukture i druge informacione imovine.

Pod kompjuterskim kriminalom u najširem smislu podrazumevaju se krivična dela prema krivičnom zakonu nacionalne države, u kojoj su na bilo koji način uključeni računarski sistemi i mreže. Glavni cilj istrage kompjuterskog kriminala je, kao i u slučaju klasičnog kriminala, izgraditi za pravosudne organe neoboriv, čvrst dokaz, i/ili dokaz za oslobađanje osumnjičenog, i/ili pravedno sankcionisanje počinioca krivičnog dela, [8]. Da bi se obezbedio digitalni dokaz potrebno je iz niza posrednih dokaza doći do

informacija u digitalnom obliku koje imaju dokazujuću vrednost, a koja je uskladištena ili prenesena u takvom obliku. Istragu digitalnih dokaza i kompjuterskog kriminala, bez alternative u doglednom vremenu, obezbeđuju tehnike i alati digitalne forenzičke nauke (uspostavljene 1999).

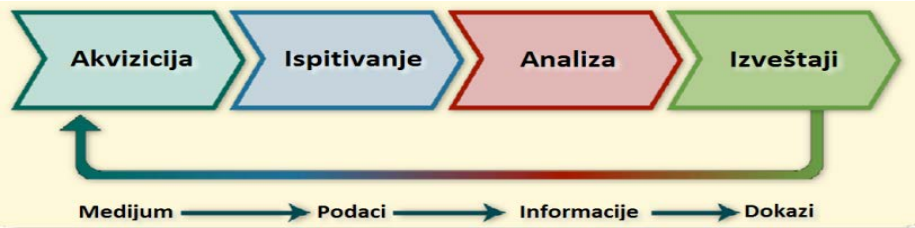
Digitalna forenzička istraga jednako je značajna za javnu forenziku državnih organa i korporacijsku istragu kompjuterskog incidenta. Korporacijski tim za upravljanje kompjuterskim incidentom može otkriti i potpuno otkloniti uzroke incidenta, samo primenom forenzičkih tehnika i alata. Ovo je posebno značajno, ako se uzmu u obzir brojni sofisticirani, antiforenzički metodi i tehnike kojima se služe autori malicioznih programa u cilju zaštite od antivirusnog programa, administratora i korisnika. Sve antiforenzičke aktivnosti mogu se svrstati u samozaštitu od detekcije zasnovane na potpisima, analize kôda od strane antivirusnih stručnjaka, detekcije malicioznog programa u sistemu i ometanje funkcionalnosti antivirusnih programa, barijera i drugih programa za zaštitu. Zato je uloga digitalnog forenzičara u korporacijskom timu za upravljanje kompjuterskim incidentom - nezamenljiva.

U ovom radu je verifikovana primena FTK forenzičkog alata, široko prihvaćenog u brojnim pravosudnim sistemima u svetu za otkrivanje dokaza malicioznog virusnog napada, uključujući rut tehnike za prikrivanja prisustva malicioznog programa. Demonstrirane su forenzičke tehnike akvizicije i komparativne analize forenzičkog imidža dva USB memorijska uređaja od kojih je jedan nezaražen, a drugi zaražen test virusom.

2. DIGITALNA FORENZIČKA VERIFIKACIJA NAPADA MALICIOZNIM PROGRAMOM

2.1. Proces digitalne forenzike

Digitalna forenzička nauka koristi naučno dokazane metode za identifikaciju, akviziciju, ispitivanje, analizu (dokazivanje) i izveštavanje (ekspertsko svedočenje, veštačenje, prezentaciju pred sudom) kao i za dokumentovanje digitalnih podataka (Sl. 1), [8].



Sl. 1. Proces digitalne forenzičke istrage

Dobro su diferencirane dve taksonomije digitalne forenzičke istrage, u odnosu na **objekat primene**: digitalnu forenziku računarskog sistema (kompjutersku forenziku) i digitalnu forenziku računarske mreže, uključujući i Internet (kibernetičku forenziku) i u odnosu na **oblasti primene** na: javnu (zvaničnu) i privatnu (korporacijsku), [7], 10].

Akvizicijom sakupljeni potencijalni digitalni dokazi predstavljaju serije bajtova podataka sa fizičkog čvrstog diska (HD) računara ili mrežnog uređaja, uzetih sa najnižih apstraktnih slojeva računarskog sistema. Takvi podaci su veoma teško razumljivi za ljudski interpretaciju, što je glavni faktor kompleksnosti digitalne forenzike. Da bi se ovi podaci mogli interpretirati, potrebno ih je prevesti tako da budu razumljivi za ljudsku interpretaciju. Postupak prevođenja vrši se pomoću forenzičkih alata za prevođenje kroz jedan ili više slojeva apstrakcije sve dok binarni podaci ne postanu razumljivi. Namena alata za digitalnu forenzičku analizu je da tačno predstavi sve podatke na sloju apstrakcije i u formatu koje forenzičar može efektivno koristiti za identifikaciju dokaza. Zahtevani sloj apstrakcije zavisi od veštine forenzičara i zahteva istrage, [8].