A black background with red text

Description automatically generated

***IT381 Zaštita i bezbednost informacija***

***Domaći zadatak br. 15***

***Ime i prezime: Jovan Pavkovic***

***Broj indeksa: 4442***

**Rešenje domaćeg zadatka**

**Forenzika**

Reč "forenzika" potiče od latinske reči "forensis", što znači "na otvorenom prostoru", a ima korene u reči "forum". Prvobitno značenje je bilo povezano s dešavanjima na otvorenom prostoru ili pred sudom.

Međutim, s vremenom, kada je počela da se široko koristi na engleskom jeziku, dobila je suženo značenje vezano za oblast pravne forenzike i krivične istrage. Danas se pojam forenzike često koristi kako bi opisao naučne metode i tehnike koje se primenjuju u analizi materijala ili podataka kako bi se pružile relevantne informacije u pravnim ili istražnim kontekstima.

Digitalna forenzika predstavlja nauku koja ima za cilj prikupljanje, čuvanje, pronalaženje, analizu i dokumentaciju digitalnih dokaza ili podataka koji su pohranjeni, obrađivani ili prenošeni u digitalnom formatu. Ove aktivnosti obuhvataju različite oblasti, uključujući:

* **Računarska forenzika**: Fokusirana na istraživanje i analizu digitalnih podataka s računara kako bi se otkrili tragovi zloupotreba, zločina ili neovlaštenog pristupa.
* **Forenzika mobilnih uređaja**: Fokusirana na istraživanje mobilnih uređaja poput pametnih telefona i tableta radi identifikacije i analize relevantnih informacija u forenzičke svrhe.
* **Mrežna forenzika**: Bavi se analizom digitalnih podataka koji putuju preko mreže kako bi se otkrili potencijalni sigurnosni incidenti, napadi ili neovlašteni pristupi.
* **Forenzika baza podataka**: Posvećena proučavanju digitalnih podataka u bazama podataka radi otkrivanja nepravilnosti, zloupotreba ili manipulacija.

Ove vrste forenzike koriste se kako bi se otkrili, dokumentovali analizirali digitalni tragovi u svrhu pružanja relevantnih informacija u pravnim, istražnim ili sigurnosnim kontekstima.

Digitalna forenzika ima široku primenu i nije ograničena samo na policijsko-sudske i vojno-obaveštajne samo na policijsko-sudske i vojno-obaveštajne aktivnosti.

**Forenzički alati**

Alati (hardver isoftver) koji se koriste za istragu su alati za detekciju podataka, alati za analizu prikupljenih za detekciju podataka, alati za analizu prikupljenih podataka, alati za proveru autentičnosti itd. Postoji veliki broj različitih softverskih alata koji se mogu preuzeti broj različitih softverskih alata koji se mogu preuzeti besplatno sa Interneta.

Neki alati za digitalnu forenziku dizajnirani su samo za jednu svrhu, dok drugi nude veliki spektar funkcionalnosti. Jedinstvenost svake istrage odrediće koji je alat, iz kompleta alata koji su dostupni istražitelju, najbolji za predmetnu istragu. Postoji velika razlika između forenzičkih alata, kako po funkcionalnosti i kompleksnosti, tako i po ceni.

Postoji veliki broj komercijalnih alata za digitalnu forenziku dostupnih na tržištu. Neki se koriste samo za kreiranje slike medija a neki za analizu tih slika, mada većina komercijalnih alata ima obe mogućnosti i nude još mnogo toga.

EnCase, iz Guidance Software, potpuno je uobličen komercijalni softverski paket, koji omogućava istražitelju da napravi sliku i ispita podatke sa hard diska, pokretnog medija ili PDA. Istraga pomoću EnCase-a počinje korišćenjem softvera da kreira sliku medija koja se zatim analizira. Mogući su pretraga po ključnoj reči, pregled fotografija ili ispitivanje obrisanih fajlova. Mnoge vlasti širom sveta koriste EnCase i to je važan faktor za istražitelje ako postoji mogućnost da će se istraga naći na sudu. EnCase je jedan od najskupljih komercijalnih alata, a popust je omogućen vlastima. EnScripts i prilagodljivi filteri omogućavju istražitelju da brzo pronađe relevantne podatke da dalju obradu sa predefinisanim EnScripts, ili da razvije sopstvene sa EnScript alatom.

EnCase Forensic, proizvod kompanije Guidance Software, jeste industrijski standard u digitalnoj, odnosno računarskoj forenzici i istrazi. Neke od osnovnih prednosti korišćenja EnCase-a su dobra tehnička podrška korisnicima, grafički korisnički interfejs, odličan dodatak za kreiranje skripti, velika baza korisnika, priznavanje forenzičke analize na sudovima i još mnogo toga objedinjenog u jednom alatu. Korišćenjem ovog programa moguće je uraditi kompletnu forenzičku analizu počevši od akvizicije do konačnog izveštaja. Ovo je jedan od najviše upotrebljavanih alata u pravosudnim i policijskim organima, među državnim istražiteljima kao i konsultantima (EnCase, 2009). EnCase radi na Windows operativnom sistemu, ali postoji i Linux verzija (LinEn). U mogućnosti je da radi analizu različitih platformi, od Windows-a, Linux-a i OS X do Solaris-a. Poseduje mnoštvo modula koji automatizuju, ubrzavaju i daju kvalitet istrazi. Program EnCase 6 može da radi na Windows XPPro, Windows 2003 Server ili Windows 2000Pro. Na Windows Vista ne rade neki vrlo važni moduli (npr. softverski write blocker).

Novi slučaj se otvara klikom na File – New. Zatim se dodaju opcije za predmetni slučaj.

A computer screen with text and icons

Description automatically generated with medium confidence

Akvizicija diska se vrši tako što se odabere Acquire, zatim vrsta medija i način na koji je taj medij povezan na kompjuter na kojem je pokrenut EnCase. Podešava se gde će se sačuvati slika koja će biti napravljena, početni i krajnji sektor, vrsta kompresije i drugo.

A screenshot of a computer

Description automatically generated

Na slici se vidi sadržaj medija čija je slika napravljena.

A screenshot of a computer

Description automatically generated

Desnim klikom na fajlove može se odabrati External Viewer da bi se fajl pogledao u izvornom okruženju, tj. programu namenjenom za pregled fajlova određenog tipa. Druga funkcija koju često koriste istražitelji jeste funkcija pretraživanja pomoću ključne reči, koja dozvoljava istražitelju da pretraži brojeve kreditnih kartica, krijumčareni materijal ili druge informacije. EnCase obezbeđuje mehanizam koji izvršava ovaj zadatak u pozadini pa se analitičar može vratiti na posao. Ključna reč se može dodati pritiskanjem jezička Keywords a desnim klikom se dodaje nova ključna reč u New Keyword okvir za dijalog. Može se izabrati opcija Unicode dok se pretražuje dokaz koji je dobijen iz Windows mašine. Funkcionalnost grep podržava složene ključne reči. Mogu se razviti grep stringovi ključne reči da se potraže brojevi kreditnih kartica, na primer, kao što je ####-####-####-####. Dok napreduje pretraživanje, videće se linija napretka u gornjoj oblasti statusa. Rezultati će biti smešteni u jezičku Bookmarks u Search direktorijumu. Rezultati uključuju fajl u kome je pronađena ključna reč, i neke podatke pre i posle lokacije ključne reči u dokazu.

Na primer, Microsoft Office dokumenta sadrže poznata zaglavlja i futere, a ovaj prosec označiće potpis Microsoft Word Document u file.txt fajl ako je otkriveno zaglavlje. Ovo je veoma korisno u slučaju kada subjekt primenjuje ekstenzije fajla da spreči istražitelja.

Druga opcija je otkrivanje direktorijuma koji su izbrisani sa diska. Potrebno je pretražiti ceo disk za „.“ i „..“ kombinacije predstavljaju ulaze direktorijuma. Kada ih EnCase locira, smešta direktorijume u direktorijum pod nazivom Recovered Folders u diskovima koji su otkriveni. Ovaj proces se započinje pritiskom desnog tastera na disk i selekcijom Recover Folders. Ovaj proces pokreće i ažurira svoj status u naslovnoj liniji. EnCase obezbeđuje i mogućnost da se kreiraju skripte koje se mogu izvršavati na dokaznom fajlu. Pritiskom na dugme EScript u traci za alate kreiraju se skripte. Guidance Software je omogućio nekoliko primera EScript kao podrazumevane prilikom instalacije EnCase. Jedna skripta koja je krajnje korisna je Internet History skripta. Ova skripta locira sve fajlove index.dat koje kreira Internet Explorer i sadrži istoriju pretraživača. Više skripti je dostupno preko korisničkog foruma na EnCase sajtu. Kada je učitana skripta koja se želi pokrenuti, potrebno je desnim klikom kliknuti na nju i odabrati Run Script, potrebno je i odabrati gde da snimi saopštenje.

Kada se završi izvršavanje skripte, može se specificirati direktorijum i dva puta pritisnuti fajl index.htm. Ovaj fajl sadržaće indeks stranu za saopštenje. Kada pritisnemo jedan od fajlova koji su nabrojani u indeks strani Internet History saopštenja, vidimo svaki URL koji je otvoren u pretraživaču.

Dve druge korisne skripte su one koje ponovo pokrivaju INFO2 slogove i JPG, GIF i EMF grafičke fajlove. Slogovi INFO2 su fajlovi koji zapisuju informaciju o fajlovima koji su izbrisani iz Recycle Bin u Windows operativnim sistemima. Fajlovi JPG i GIF su grafički fajlovi koji se tipično koriste na web stranama. Fragmenti tih web strana mogu postojati na disku. Skripte smeštaju rezultate u Bookmarks direktorijum, u direktorijumima koji se nazivaju Recovered recycle Bin Records i Recovered Graphics Files, respektivno. Pošto EnCase ne može pregledati svaki fajl koji postoji, treba se povezati sa spoljašnjim pregledačima za različite tipove fajla. Novi spoljašnji pregledači mogu se izvesti biranjem Tools, a zatim Signatures. U jezičku Viewers, mogu se dodati različiti pregledači kao što je Quickview Plus. Nakon što se doda pregledač, kad god se sretne fajl koji se želi pregledati spoljašnjim pregledačem, pritisne se desnim tasterom fajl, izaberite Send To, i izaberite pregledač koji je ustanovljen. EnCase podržava nekoliko režima pregledavanja. Pregled Gallery prikazuje sve grafičke fajlove u direktorijumu. Pregled View obezbeđuje detaljan listing sa atributima kao što su vreme i datum, veličina fajla i drugo. Pregled Timeline prikazuje šemu vremena kreiranje, modifikacije i pristupa izabranih fajlova. Pregled Report nabraja detalje o dokaznom fajlu koji sadrži podatke. Neki fajl ili fragment fajla koji istražitelj bira pritiskom desnog tastera na Bookmarks selektor prikazaće se u saopštenju.