UDK: 343.983:004

ALATI ZA DIGITALNU FORENZIKU

*Dragan Ranđelović[1]
Tijana Bogdanović[2]
[1]*Kriminalističko policijska akademija, Beograd, Srbija*
[2]*COING doo, Novi Sad*

Sažetak: Kompjuterska forenzika je naučna disciplina koja se bavi prikupljanjem, očuvanjem, analizom i prezentovanjem podataka koji su elektronski procesirani i uskladišteni na kompjuterskim medijima. Iako je relativno nova disciplina, ona ima potencijal da značajno utiče na specifične tipove istraga i krivičnih gonjenja. Kompjuterska forenzika se značajno razlikuje od tradicionalnih forenzičkih disciplina. Za početak, alati i tehnike koje ova disciplina zahteva, relativno su lako dostupni svakome ko želi da sprovede forenzičku analizu. Nasuprot tradicionalnim forenzičkim analizama, od kompjuterskih istražitelja se zahteva ispitivanje u uslovima koji nisu uvek kontrolisani. Prikupljanje digitalnih dokaza počinje kada se informacija i/ili fizički objekt prikupe ili sačuvaju u očekivanju ispitivanja. Termin „dokaz" implicira da je osoba koja ga je prikupila prepoznata od strane Cuda, kao i sam proces prikupljanja. Podatak ili fizički objekt postaje dokaz jedino kada je prikupljen od strane ovlašćenog lica.
Ključne reči: kompjuterska forenzika, komercijalni i nekomercijalni alati za digitalnu forenziku.

1. Uvod

Termin „kompjuterska forenzika" ili „digitalna forenzika" označava primenu naučnih metoda u cilju identifikacije, prikupljanja i analiziranja podataka uz očuvanje integriteta originalnog dokaza kao i lanca nadležnosti. Kompjuterska forenzika se može definisati i kao proces prikupljanja, očuvanja, analize i prezentovanja digitalnih dokaza.

Digitalni dokazi su osetljivi, lako se brišu, menjaju i time kompromituju. Specijalni forenzički alati omogućavaju povrat i analizu obrisanih, skrivenih i privremenih podataka koji u normalnim uslovima nisu vidljivi.

* E-mail: dragan.randjelovic@kpa.edu.rs

Forenzički alati se koriste zato što digitalni dokazi imaju strukturu kao „santa leda“ – sastoje se od vidljivih dokaza koji se lako pronalaze i moguće ih je otkriti „klasičnim alatima“ (kao što je *Windows Exlorer*) a veći deo dokaza čine obrisani, preimenovani ili skriveni fajlovi za koje su potrebni forenzički alati za identifikaciju (Bishop, 2003; Casey, 2004).

Procedura koja se uglavnom preduzima prilikom forenzičke istrage podrazumeva da se odrede računari koji su predmet istrage, sačuvaju originalni mediji i spreče bilo kakve izmene sadržaja medija. Ako je kompjuter upaljen, preuzima se sadržaj *RAM*-a (*random-access memory*), zatim se kompjuter gasi, bilo redovnim putem, bilo isključivanjem napajanja, prave se kopije svih bitnih medija i forenzička analiza se obavezno vrši na kopijama medija (INsig2, 2003).

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. Neki od vodećih komercijalnih produkata koštaju nekoliko hiljada dolara, dok su drugi besplatni. Opet, priroda forenzičara i cilj istrage određuju alat koji će se koristiti. Uopšteno, istražitelj će koristiti alat da bi prikupio podatke sa sistema (kompjuter ili kompjuterska mreža) bez menjanja podataka na njemu. Ovaj aspekt istrage, izbegavanje menjanja originalnih podataka, jeste osnovni princip kompjuterske forenzike, i neki dostupni alati uključuju funkcionalnost specijalno dizajniranu da podrži ovaj princip. U praksi, nije uvek jednostavno prikupiti podatke bez ikakvog menjanja sistema (čak će i samo gašenje kompjutera, zbog prenosa, prouzrokovati promene na podacima tog sistema), ali iskusan istražitelj će težiti da zaštiti integritet originalnih podataka kad god je to moguće.

Da bi se ovo izvršilo, potrebno je napraviti tačnu kopiju svih podataka sa diska. Ova kopija se naziva slika, a proces akviticija; ova slika je subjekat istrage.

Drugi koncept podrazumeva da se obrisani podaci ili njihovi delovi, mogu povratiti. Uopšteno, kada se podatak obriše on nije fizički nestao sa sistema, nego je samo uklonjen podatak o lokaciji podatka (na hard disku ili drugom mediju). Otuda, podatak može još biti prisutan, ali operativni sistem kompjutera više „ne zna“ za njega. Pravljenjem slike i analizom svih podataka sa diska, ne samo onih koji su poznati operativnom sistemu, moguće je oporaviti podatak koji je bio slučajno ili namerno obrisan (Forensic Focus, 2009).

2. Komercijalni alati

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. U ovom delu opisan je alat *EnCase*, koji je zvanični alat koji koriste američke vlasti, kao i drugi spomenuti alati koji su često upotrebljavaju.

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, 2009).

FTK pokušava da pomogne analitičaru smanjivanjem ogromnih skupova podataka na podskup važnih informacija. *FTK* je komercijalan proizvod razvijen od strane *AccessData*. Najveća prednost *FTK-a* i ono po čemu se izdvaja od ostalih alata za digitalnu forenziku je veoma intuitivan korisnički interfejs koji omogućava jednostavan rad i početnicima (AccessData, 2009).

Vogon International nudi širok spektar komercijalnih softvera za digitalnu forenziku koji su podeljeni na softvere za pravljenje slike, obradu i istragu. Softver za kreiranje slike, pravi tačnu kopiju podataka sa diska koja može biti indeksirana sa softverom za obradu da bi se brže vršila pretraga komponenti istrage. U širokoj ponudi *Vogon* nudi sličnu funkcionalnost kao *EnCase* pojednostavljujući proces pravljenja slike i pretrage.

SafeBack je još jedan komercijalni softver za kompjutersku forenziku često upotrebljavan od strane vlasti širom sveta. *SafeBack* je primarno korišćen za pravljenje slike hard diska Intelovih kompjutera i povratak ovih slika na drugi hard disk. Program je baziran na *DOS*-u (*Disk Operating System*), može se pokrenuti sa flopi diska i namenjen je samo za pravljenje slike, ne uključuje mogućnost analize kao *EnCase* ili *Vogon*-ov forenzički softver (Forensic Focus, 2009).

Neophodno je, pored kratko opisanih softvera za digitalnu forenziku, bar spomenuti i *Ilook Investigator* kao i *HELIX* od *e-fence* koji je varijanta *Knoppix Linux* distribucije.

2.1 EnCase

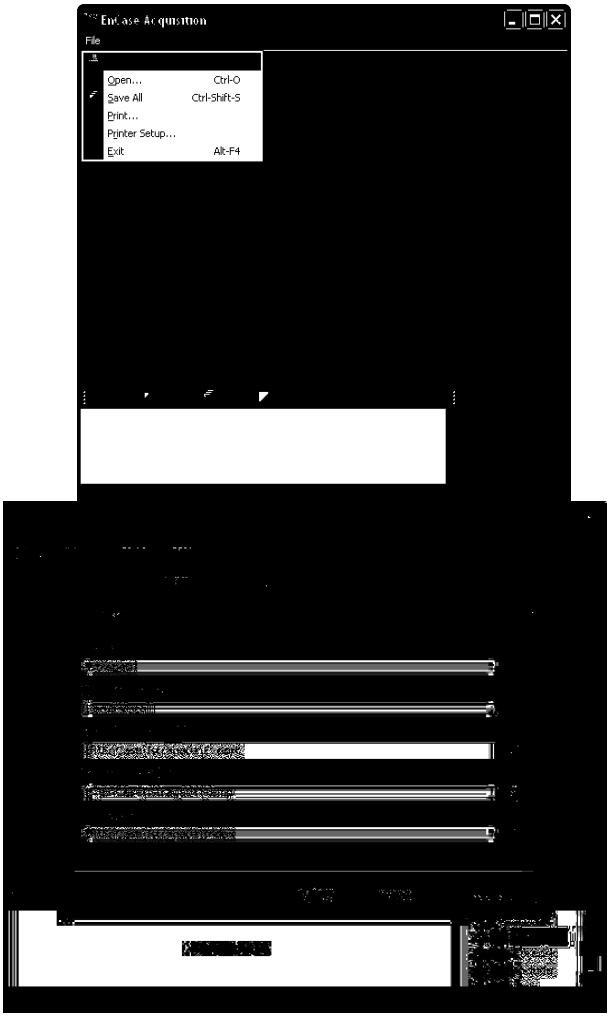
EnCase Forensic, proizvod kompanije *Guidance Software*, jeste industrijski standard u digitalnoj, odnosno računarskoj forenzici i istrazi. Neke od osnovnih prednosti korišćenja *EnCase*-a su dobra tehnička podrška korisnicima, grafički korisnički interfejs, odličan dodatak za kreiranje skripti, velika 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.

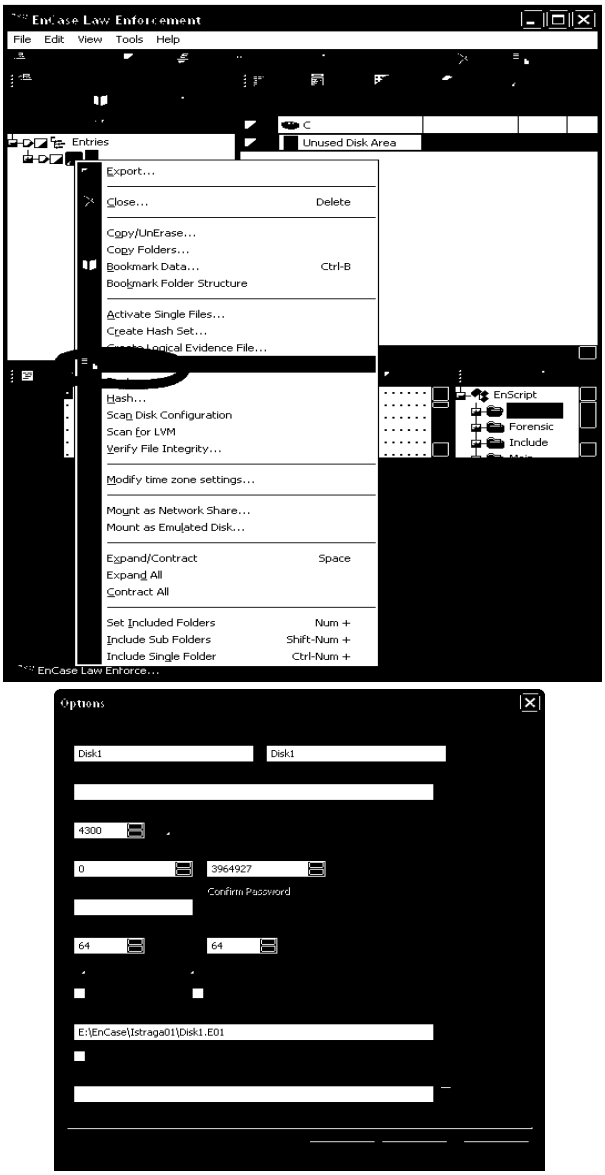
Program *EnCase 6* može da radi na *Windows XPPro*, *Windows 2003 Server* ili *Windows 2000Pro*. Na *Windows Vista* ne rade neki vrlo važni moduli (npr. softverski *write blocker*).

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



Slika 1: Otvaranje novog slučaja i opcije

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.



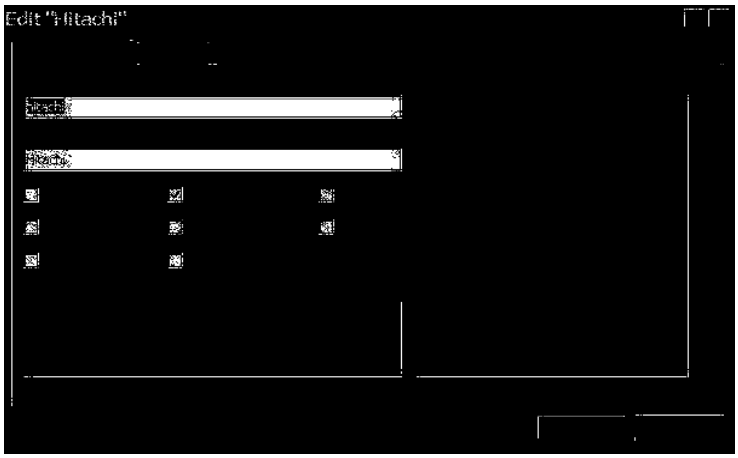
Slika 2: Akvizicija diska i opcije (eSecurityLab, 2009)

Na slici 3 vidi se sadržaj medija čija je slika napravljena.

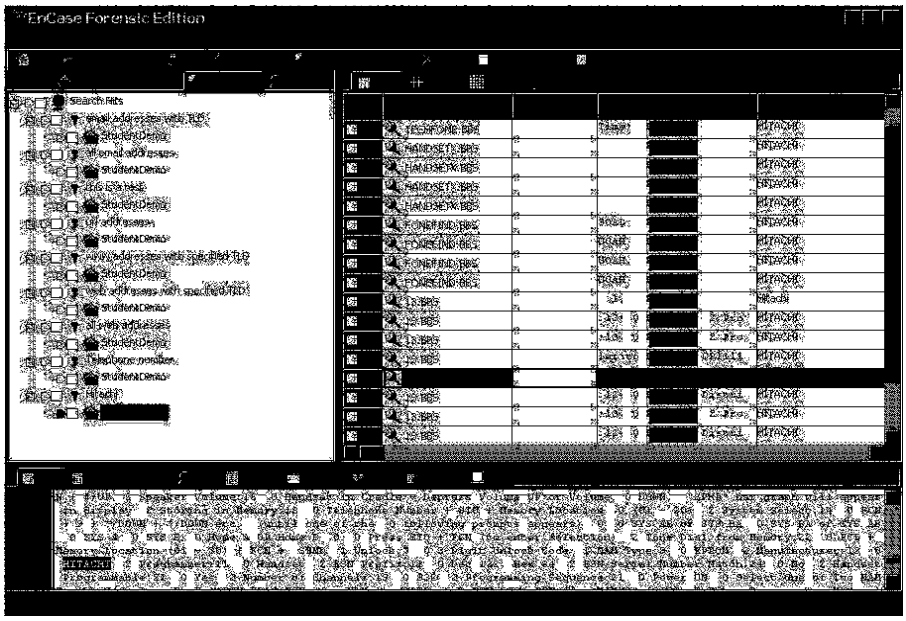
Slika 3: Sadržaj slike

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. Zatim se ovaj fajl može pregledati kao i bilo koji drugi fajl (Jones et al., 2003). Opis *GREP* simbola je dat desno na slici 4.



Slika 4: Podešavanje pretrage



Slika 5: Rezultati pretrage za reč hitachi

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. Ako pritisnete desni taster na saopštenje, možete ga izvesti u *Rich text* formatu *(RFT)* tako da možete iseći i zalepiti značajne podatke u dokumentaciji istražitelja (Jones at al., 2003).

3. Nekomercijali alati

Počeci kompjuterske forenzike su bili na *Unix*-u, a ne na *Windows* operativnom sistemu koji je dostigao veliku popularnost danas. Oni koji su razvijali *Unix*, više su želeli da kreiraju veliki broj malih programa koji se mogu koristiti zajedno da bi izvršili kompleksnije zadatke, nego jedan program koji može da radi sve. I iz ovih malih programa su nastali sofisticirani komercijalni paketi za kompjutersku forenziku. Mali programi se još mogu naći na modernim verzijama *Unix* operativnih sistema i mnogi su dostupni i za *Windows* (McClure, 2006; Pastore, 2007).

U ovom delu su opisana dva alata za kreiranje kopije koji su najpopularniji. *Sleuth kit* sah *Autopsy* i DD.

Treba se spomenuti *The Coroner's Toolkit* koji je kolekcija besplatnih alata dizajniranih da se koriste za forenzičke analize na *Unix* mašinama. *Coroner's Toolkit* je specijalno dizajniran da se koristi u istrazi prilikom kvara kompjutera. Alat uključuje pomoć pri rekonstrukciji aktivnosti uljeza, između ostalog, ispitivanjem vremena pristupa fajlovima i povratkom obrisanih fajlova.

MD5sum se koristi da bi se otkrilo da li je kreirana slika, prava kopija originala. Ova procedura rezultira kreiranjem velikog broja koji se zove „heš" (*hash*), i predstavlja tačnu vrednost koja je određena položajem podataka nađenih na disku (*MD5* se takođe može koristiti i za kreiranje heša za fajlove). U osnovi, ako je disk menjan na bilo koji način, brisanjem ili menjanjem fajlova na primer, pokretanje *MD5* algoritma će rezultovati značajno drugačijom heš vrednosti. Ovo se vidi bez obzira na stepen promene koja je izvršena, čak i kao je promena na jednom bitu informacije velikog hard diska, paket sa podacima će rezultovati novom heš vrednošću. *MD5sum* je besplatan alat za kreiranje *MD5* heš vrednosti koje, komparacijom originalnog diska i kopije, mogu da se koriste u istrazi da bi se osiguralo da je slika prava kopija originala.

Grep je program koji omogućava da se fajlovi pretražuju po delimičnim sekvencama karaktera: reč „sastanak" ili fraza „sastanak je u 4" na primer. Moć *Grep*-a, je u mogućnosti da koristi metakaraktere. Metakarakteri su nekoliko karaktera koji imaju specijalno značenje za *Grep* program i omogućavaju veliku fleksibilnost tokom pretrage. Na primer, metakarakter „.", ako se pretraga formuliše kao „ca.", može se naći „can", „cat", „cab" i tako dalje gde god je prisutna ova sekvenca. *Grep* je dugo bio jedan od najkorisnijih alata za istražitelje dok nije postao standardan program na *Unix* sistemima i takođe je deo *EnCase*-a (Forensic Focus, 2009).

3.1. *DD*

Ovaj program je prvi na listi zbog neverovatne jednostavnosti, a opet izuzetne funkcionalnosti kao forenzički alat (dodatno kao alat za povratak podataka). Ukratko, dd je program za povratak podataka koji može da kopira i konvertuje fajlove, hard diskove, CD, ili bilo koji deo diska pomoću opcija *skip* i *seek*.

Bez obzira na sve ovo, u forenzičkom svetu *DD* se koristi u svrhu kreiranja tačnog duplikata podataka sa medija, i tako omogući sigurnu istragu sakupljenih dokaza. Kada se uz ove mogućnosti zabrani pisanje na hard disk koristeći softver, *DD* postaje alat koji se može koristiti za ekstrakciju duplikata hard diska, bit po bit, koji se posle analiziraju sa forenzičkim programima. Dokle god je medij učitan kao „ro", ne može biti prepisan tokom ekstrakcije štiteći tako dokaz.

Ono što izdvaja *DD* od ostalih programa za pravljenje slike hard diska je što on kopira sve sa hard diska, uključujući i slak (*slack*) prostor i obrisane fajlove. Ako se na primer uzme tek formatiran hard disk od 1 GB, fajl koji će napraviti *DD* će biti takođe 1 GB. Kao rezultat, ovo omogućava drugim alatima da brzo istraže *DD* sliku, što može pomoći da se ubrza proces analize i zaštiti dokaz od slučajnog brisanja. Mnogi drugi programi jednostavno kopiraju „žive" fajlove koji su upotrebljivi i vidljivi uz pomoć bilo

kog kompjutera. Na žalost ovo može da utiče na gubitak većine kritičnih informacija koje su prethodno obrisane.

DD je *Linux* alat i kao takav, očekuje se da je alat sa komandnom linijom. *DD* je više od forenzičkog alata (konverzija slike i povratak podataka) ali se ovde fokusira na pravljenje duplikata odredišta. Uopšteno, istražitelj može da koristi *DD* da napravi sliku hard diska koji je konektovan na kompjuter, ili neki drugi medij koji je učitan na **nix* sistem, kao *backup* fajl ili *RAM*. Kada se konektuje, medij mora biti zaštićen od pisanja, što se postiže unosom *fstab* fajla ili kada je pokrenuto otvaranje, u komandnoj liniji. Prethodne informacije su opšta uputstva za učitavanje hard diska, kreiranje slike i ponovno učitavanje tek kreirane slike za dalju forenzičku istragu.

Potrebno je bar onoliko slobodnog prostora koliko je velik hard disk koji je predmet istrage. Ako se koristi eksterni uređaj, kao što je *USB* uređaj, treba da se pokrene *rescan-scsi-bus.sh*. Ova skripta će olakšati konektovanje i diskonektovanje *USB* uređaja. Kada je jednom pregledan, uređaj se otvara zaštićen od pisanja (*mount –t vfat –o ro,noatime /dev/sda1 /images/case1-hdc1*).

Najsigurniji metod ekstrakcije podataka je da se *DD* koristi bez pokretanja uređaja, ali ovo nije jednostavno kada se radi sa više particija.

Otvara se medij zaštićen od pisanja.

Sledeća komanda se koristi za pravljenje kopije prve particije diska

dd if=/dev/hdc1 of=/home/images/case1-hdc1-c1-badguy.

Kada je slika napravljena, može da se otvori sa sledećom komandom

mount -o ro, loop, noatime /home/images/case1-hdc1-c1-badguy /mnt/case1-hdc1

ro (read-only) – ovo je obavezno prilikom pokretanja bilo kog uređaja; ako dođe do pisanja po uređaju tokom istrage, gubi se vrednost dokaza;

loop – omogućava da se fajl otvara i da mu se jednostavno pristupa;

noatime – onemogućava markiranje vremena poslednjeg pristupa koje se dodaje na otvorene fajlove;

Kada se otvori uređaj to jest slika uređaja, može da se započne istraga upotrebom forenzičkih alata i tehnika (InformIT, 2009).

Postoji više alata koji se obično koriste za kreiranje dokazne slike, kao što su *EnCase* ili *SafeBack*; oni imaju svoje cene, dok je *DD* alat otvorenog koda i ne naplaćuje se. Ono što je specifično kod *DD* komande za kopiranje, jeste da se mogu kopirati uređaji koji su orijentisani kao blokovi, *DD* je sposoban da adresira ove blokove sekvencijalno.

Da bi se kopirao dokazni disk, može se koristiti komanda *dd if=/dev/source of=/dev/destination. If* znači *infile*, označava dokazni disk koji treba da se klonira a *of* znači *outfile*, to jest lokacija gde će se smestiti klon medija. Pored kopiranja hard diska, *DD* kopira i trake, cd/dvd, i drugo. Da bi se shvatilo kako se *DD* može koristiti u forenzičkom svetu, sledi primer.

Ako je dokazni hard disk kapaciteta 20 GB, koristiće se *Linux live CD* na dokaznom kompjuteru, potrebno je i spremiti jedan hard disk kapaciteta minimalno 20 GB, mada je bolje da bude veći, na koji će se klonirati dokazni disk. U ovom slučaju to će biti hard disk od 80 GB.

mount /dev/sda2 /mnt/backupdiskdd if=/dev/sda1 of=/mnt/backupdisk/evid1

Ako nije poznato koliki su blokovi hard diska potrebno je koristiti *ibs/obs* oznake da se pronađe tačna veličina. Pronalaženje tačne veličine ubrzava proces kopiranja.

dd if=/dev/st0 ibs=128 of=/mnt/backupdisk/evid1 obs=1 count=1

Može da se uzme 1 blok veličine 128 od *'st0?* i kreira *'evid1?* izlaz sa veličinom bloka 1. *Count* oznaka se koristi da bi se pročitao samo jedan blok; ovo se radi da bi se *DD* ograničio da koristi jedan blok. Ako se ne podesi veličina, *DD* će nastaviti i potrošiće mnogo vremena. Ovaj primer treba da pokaže da se podešavanjem ulaznog bloka na 128, može pronaći prava veličina bloka osim ako je naravno baš 128. Sa 512, kao standardnom veličinom bloka, pretpostavka da je 128 je loš način da se dođe do stvarne veličine bloka. Izlaz ove komande verovatno će biti poruka o grešci sa pravom veličinom bloka, recimo 1024.

Ako treba prekopirati ceo disk na *CD* ili *DVD* potrebno je podeliti sliku na više delova, na primer kreiranjem četiri slike dokaza od po 1GB.

dd if=/dev/st0 count=4000000 of=/mnt/backupdisk/evid1

dd if=/dev/st0 count=4000000 skip=4000000 of=/mnt/backupdisk/evid2

dd if=/dev/st0 count=4000000 skip=8000000 of=/mnt/backupdisk/evid3

dd if=/dev/st0 count=4000000 skip=12000000 of=/mnt/backupdisk/evid4

dd if=/dev/st0 count=4000000 skip=16000000 of=/mnt/backupdisk/evid5

Sada se 20 GB dokaznog hard diska nalazi na pet odvojenih slika od po 4 GB (što je veličina jednog *DVD-R* diska). Ako se pogledaju komade, može se primetiti da prva komdana uzima 4 GB (*count=4000000*) i kopira ih sa imenom *evid1.* Druga komanda preskače prvih 4 GB (*skip 4000000*) i zatim kopira sledećih 4 GB (*count=4000000*) sa imenom slike *evid2.* Ovde se vidi tačno šta rade oznake *count* i *skip*.

Iz primera se vidi da je *DD* veoma dobar alat za kreiranje fizičke kopije dokaza. Naročito je koristan kada se radi sa velikim diskovima (Stmik Akakom, 2009).

DD za Windows: `dd [bs=SIZE[SUFFIX]] [count=BLOCKS[SUFFIX]] if=FILE of=FILE [seek=BLOCKS[SUFFIX]] [skip=BLOCKS[SUFFIX]] [--size] [--list] [--progress]` ;

bs je veličina bloka; uobičajena veličina bloka na većini uređaja je 512 ali kopiranje će biti znatno brže ako se koristi veća veličina bloka; npr. ako se flopi disk čita sa veličinom bloka od *bs*=1*k count*=1440 traje skoro dvostruko duže nego ako se koristi *bs*=1440*k count*=1; ne treba uzeti ni preveliku veličinu bloka jer *Windows* može ostati bez memorije; 1M je dobra veličina ali i gornja granica. Većina *CD* i *DVD-a* imaju veličinu sektora 2*k,* i neće raditi ako veličina bloka ne može da se podeli sa 2;

skip je opseg koji će se preskočiti na ulaznom fajlu, pre nego što počne čitanje; Budući da je u blokovima, pisaće se opseg *skip * blocksize*; može se koristiti i sufiks *skip*=1*k* tako da će onda preskočiti 1024 blokova.

seek je opseg koji će se pretražiti pre nego što počne da piše izlazni fajl; on je takođe u blokovima pa će opseg biti *seek * blocksize*; može se i ovde koristiti sufiks *seek*=1*k* koji će tražiti 1024 blokova.

count je broj blokova za kopiranje; ako nije određen onda će *DD* da kopira sve dok ne dođe do kraja dokaznog fajla; na mnogim *USB* uređajima ovo nije moguće, tako da treba koristiti *--size* da se pogodi veličina uređaja; mogu se koristiti i sufiksi, *count*=1*k* će kopirati 1024 blokova.

--size je uobičajena komanda kada se *DD* koristi za kopiranje celog uređaja a neće se specificirati veličina, tako da će *DD* čitati dok ne dođe do kraja uređaja; ako se pokuša čitati posle kraja uređaja, vratiće se na početak i javiće grešku; *Windows* ne uradi ovo uvek tako da će *--size* reći *dd* da pronađe veličinu uređaja i omogućiti da ne pređe kraj tokom čitanja;

--list će dati ponuđena imena; na *NT4* moguć je samo metod: *\\?\Device\Harddisk<n>\Partition<n>*; *Partition0* je ceo disk. Na *Windows XP*, neke particije nemaju ime; u ovom slučaju koristi se *Harddisk<n>\Partition<n> ime*. *Windows* 2000 i kasniji imaju imena uređaja koja su jedinstvena i identifikuju disk ili particiju; u većini slučajeva ovo je slovo; na *Windows XP SP2* mnoge particije se ne mogu čitati direktno čak i ako nisu u upotrebi, tada je potrebno prići sa „zadnjih vrata";

--progress se koristi ako se želi gledati napredovanje svakog bloka koji se kopira.

Da bi se sprečilo slučajno prepisivanje pogrešnog diska, treba koristiti sigurnostni filter. Dostupni filteri su:

- fixed – piše samo po fiksnom disku
- removable – piše samo po pokretnom disku
- disk – piše po bilo kojoj vrsti diska
- partition – piše samo po particiji.

Filter se može primeniti ako se *dd.exe* preimenuje u *dd-<filter>.exe*. Na primer, *dd-removable.exe* može pisati samo po pokretnom disku kao što je *USB*, tako da osigurava da ne dođe do slučajnog pisanja po fiksnom disku. Slede neki primeri za upotrebu *DD*-a (*Chrysocome, 2009*):

kreiranje slike flopi diska – dd if=\\.\a: of=c:\temp\disk1.img bs=1440k ;

pisanje slike nazad na flopi disk – dd if=c:\temp\disk1.img of=\\.\a: bs=1440k ;

skidanje .iso sa CD-a – dd if=\\?\Device\CdRom0 of=c:\temp\disc1.iso bs=1M

čitanje particije sa USB memorijskog uređaja – dd if=\\.\Volume{c18588c0-02e9-11d8-853f-00902758442b} of=c:\temp\usb1.img bs=1M ;

čitanje celog USB memorijskog uređaja – dd if=\\?\Device\Harddisk1\Partition0 of=c:\temp\usb2.img bs=1M --size –progress .

3.2. Sleuth Kit i Autopsy

The Sleuth Kit, ranije nazivan *TASK*, jeste kolekcija alata za forenzičku analizu sistema pod *UNIX*-om baziranih na komandnoj liniji. Alati omogućavaju ispitivanje sistemskih fajlova na sumnjivom kompjuteru na nenametljiv način. Alat nije povezan sa operativnim sistemom da bi analizirao sistemske fajlove, takođe prikazuje obrisane i sakrivene sadržaje. *The volume system (media management)* alat omogućava da se ispita forma hard diskova i drugih medija. *Sleuth Kit* podržava *DOS* particije, *Mac* particije, *Sun slices* i *GPT* diskove. Sa ovim alatima moguće je identifikovati gde su locirane particije i kopirati ih tako da mogu biti dalje analizirane. Kada se izvodi kompletna analiza sistema, bolje je koristiti alat sa grafičkim okruženjem a ne sa komandnom linijom. *Autopsy Forensic Browser* je alat u *Sleuth Kit-u* sa grafičkim interfejsom koji omogućava lakši tok istrage. *Autopsy* daje mogućnost menadžmenta slučaja, integritet slike, pretragu po ključnim rečima i ostale automatske operacije.

Ulazni podaci mogu biti slike raznih formata, *raw* (*dd*), *EnCase* slika, *AFF* fajl sistem i druge. Podržava *NTFS, FAT, UFS1, UFS2, EXT2FS, EXT3FS*, i *ISO 9660* fajl sisteme (čak i kada ispitani operativni sistem ne podržava). Alati mogu biti pokrenuti sa „živog" *UNIX* sistema tokom odgovora na incident. Ovi alati će prikazati fajlove koji su skriveni i neće modifikovati vreme pristupa.

Mogućnosti pretrage:

- izlistava alocirane i obrisane *ASCII* i *Unicode* fajlove;
- prikazuje detalje i sadržaj svih *NTFS* atributa;
- prikazuije fajl sistem i *meta-data* strukturu;
- kreira raspored aktivnosti, koji može da se eksportuje;
- pregleda heš u heš bazi podataka, kao što su *NIST NSRL*, *Hash Keeper*, i ostale baze podataka kreirane sa *md5sum* alatom;
- organizuje fajlove prema njihovom tipu (na primer izvršni, slike i dokumenta su odvojeni) a mogu se napraviti stranice sa malim grafičkim slikama za njihovu bržu analizu.

Sleuth Kit je napisan u S i Perl-u a koristi i neke kodove i dizajn od Coroner's Toolkit (TCT). Sleuth Kit je testiran na sledećim sistemima: Linux, Mac OS X, Windows (Visual Studio), CYGWIN, Open & FreeBSD, Solaris.

4. Primeri upotrebe alata za digitalnu forenziku

U sledećem delu biće prikazana upotreba opisanih alata, prvo za analizu slike u ovom slučaju *USB* u *stand alone* režimu sa *Sleuth kit* i *Autopsy* a posle sa *EnCase.*

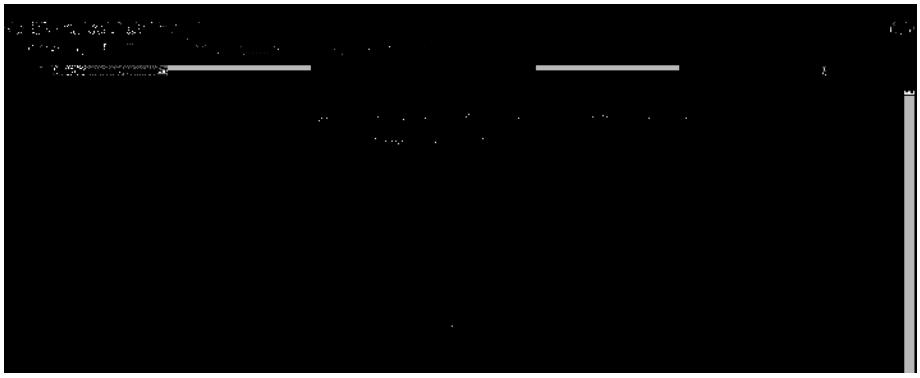
4.1. Forenzička analiza kopije medija sa forenzičkim alatom otvorenog koda

Alati za digitalnu forenziku pomenuti u prethodnim poglavljima testirani su na slici *USB* fleš memorije od 64*MB* na kojem su kreirana dva fajla u *.doc* formatu, *prazan.doc* i *formula.doc*. U fajlu *prazan.doc* piše da je prazan i on je ostao na *USB* fleš memoriji, dok u fajlu *formula.doc* piše da sadrži tajnu formulu i on je zatim obrisan sa *USB* memorije. Slika *USB* memorije napravljena je sa *dd-0.4beta4*. *DD* se pokreće tako što se u *Command Prompt* piše *dd.exe --list* da bi se videlo koje medije sadrži računar. Na *C:* particiji napravljen je folder *dd* u koji će se smestiti slika memorije. Da bi se napravila kopija *USB* memorije tj. slika *USB* memorije, prvo se na samoj memoriji hardverski uključi zaštita memorije od pisanja i brisanja, zatim se u *DD-u* piše: *dd if=\\.\e: of=c:\dd\primer.bin bs=512k*

Na *C* particiji u folderu *DD* pod imenom *primer.bin* napravljena je slika *USB* memorije. Prethodno su instalirani *Sleuth kit* i *Autopsy* uz pomoć *Cygwin-a*. Da bi se instalitao *Sleuth kit* prvo se pokreće fajl *configure* zatim *makefile*. Za instalaciju *Autopsy* komande u *Cygwin*:

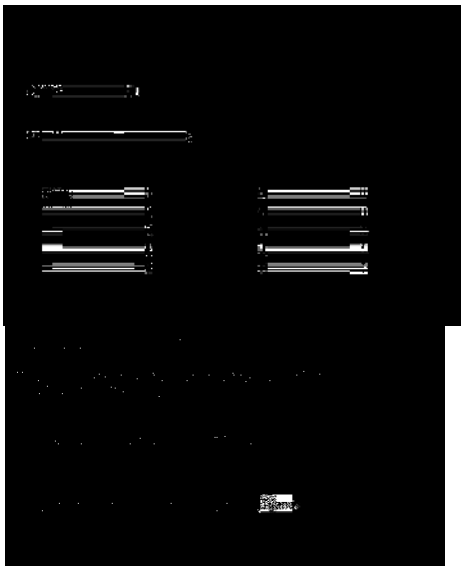
cd '/cygdrive/c/autopsy'
'/cygdrive/c/autopsy/configure'
'/cygdrive/c/autopsy/makefile'
'/cygdrive/c/autopsy/autopsy'

Nakon toga se može pokrenuti pisanjem u *HTML Browser*: *http://localhost:9999/autopsy* . Otvara se *Autopsy* koji izgleda kao na slici 6.

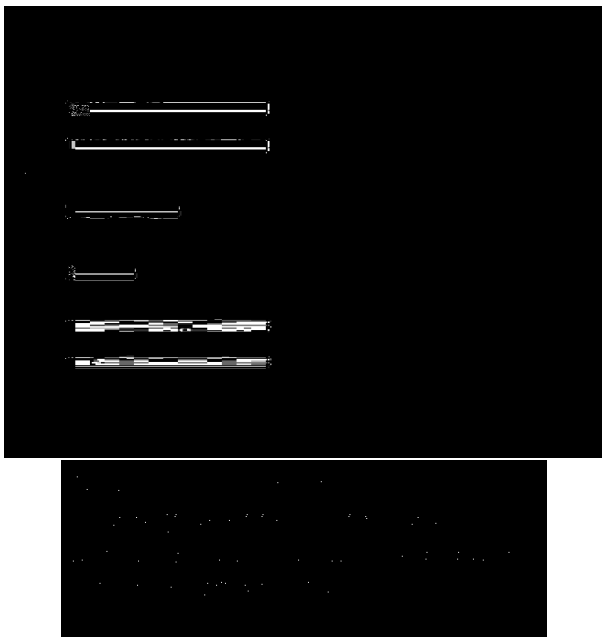


Slika 6: Izgled Autopsy-ja

Da bi se otvorio novi slučaj, potrebno je kliknuti na *New Case*. Dostupne opcije su prikazane na slici 7.



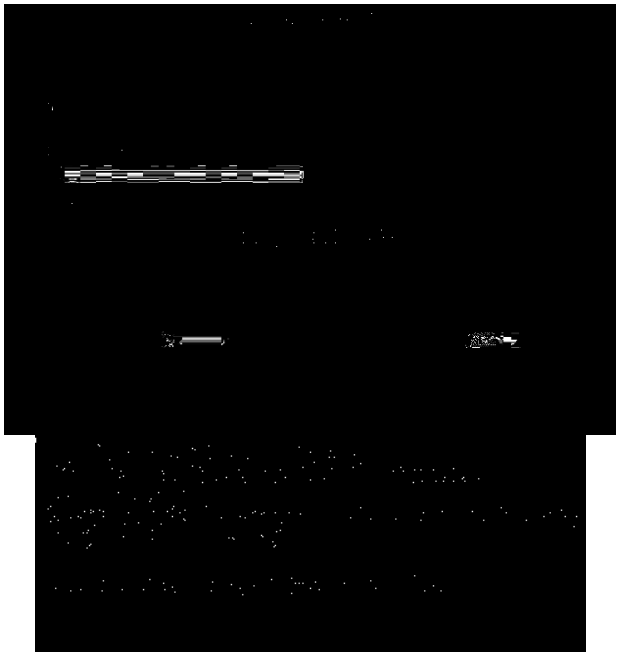
Slika 7: Otvaranje novog slučaja



Slika 8: Opis hosta

Ime slučaja u ovom primeru je *Primer* a ime istražitelja *Tijana*. Moguće je dati opis slučaja, ovo se preporučuje kada se radi o obimnijoj istrazi.

Pre dodavanja slike, može se odabrati da se izračuna MD5 vrednost ili da se doda poznata tako da Autopsy može da izvrši verifikaciju.



Slika 9: Dodavanje slike

Na slici 10 prikazano je da se slika zove *primer.bin* i da je *fat32* formata.

Slika 10: Opcije dostupne nakon dodavanja slike

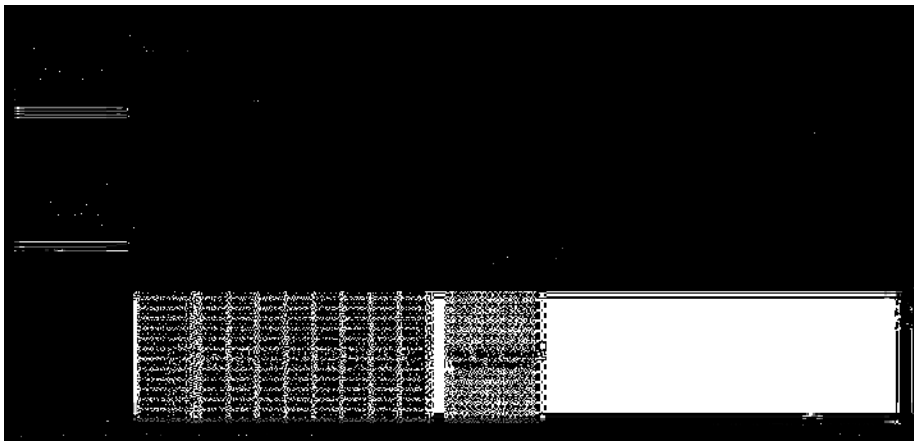
Moguće je videti detalje slike i ekstraktovati stringove kao i obrisani prostor. Opcije nakon ekstrakcije su prikazane na slici 11, analiza fajlova, pretraga po ključnoj reči, tip fajlova i drugo.

Slika 11: Opcije u Autopsy-ju

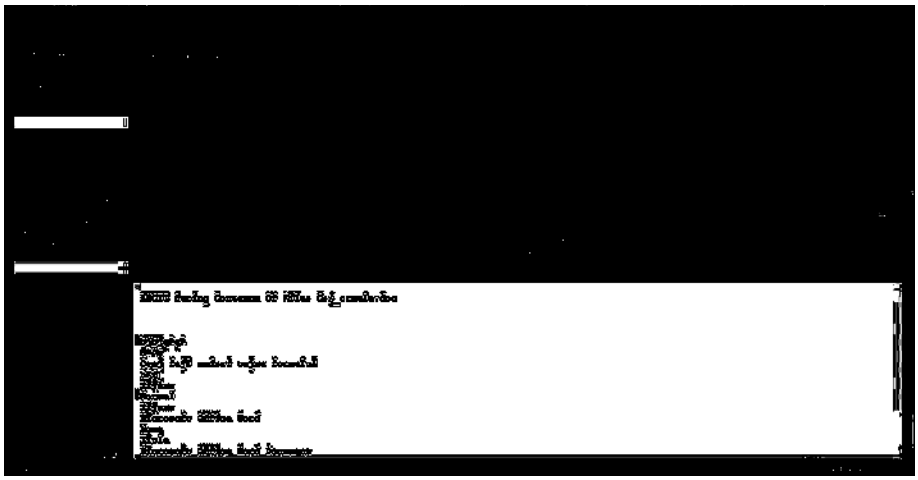
Ako je odabrana alaniza fajlova otvara se sadržaj slike, što je prikazano na slici 12. Fajl označen crvenom bojom je onaj fajl koji je obrisan.

Slika 12: Sadržaj slike

Na slici 13 vidi se *ASCII* prikaz obrisanog fajla *formula.doc* i može da se vidi da u njemu piše *Ovaj fajl sadrži tajnu formulu!.*

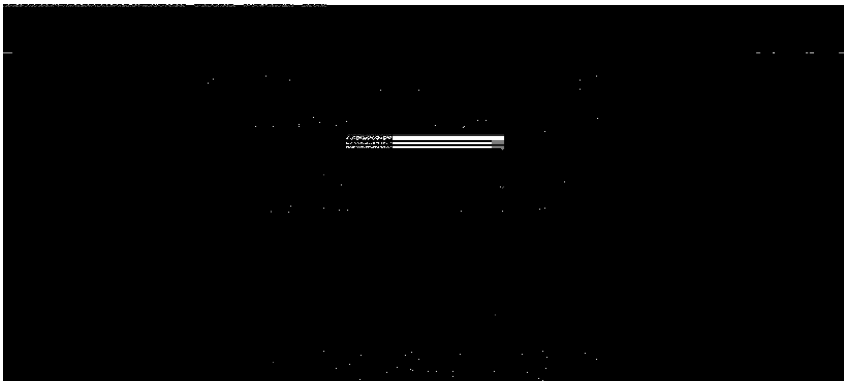


Slika 13: ASCII prikaz fajla formula.doc



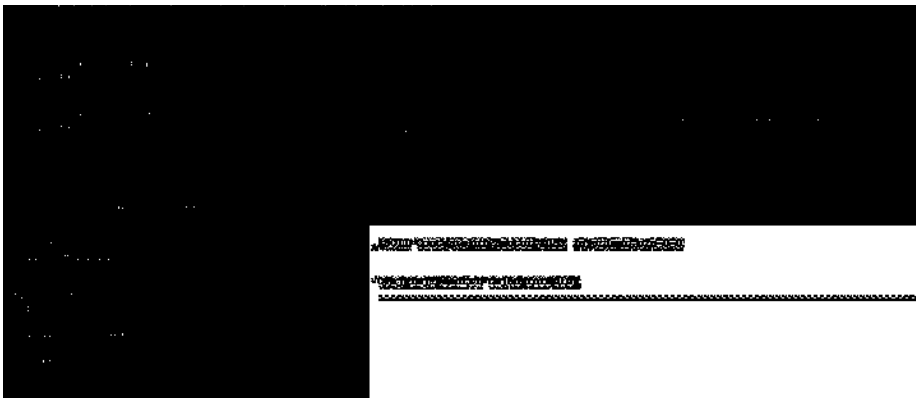
Slika 14: Heksadecimalni prikaz fajla formula.doc

Na slici 15 prikazana je pretraga po ključnoj reči na alociranom i nealociranom prostoru. Ključna reč je *formula*.



Slika 15: Pretraga po ključnoj reči

Na slici 16 su prikazani rezultati pretrage, na levoj strani su rezultati a na desnoj prikaz rezultata i tačna lokacija.

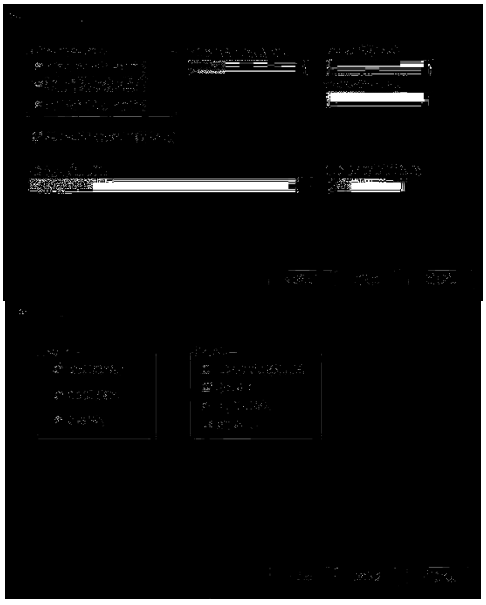


Slika 16: Rezultati pretrage

4.2. Forenzička analiza kopije madija sa komercijalnim forenzičkim alatom

Ista *USB* memorija kapaciteta 64MB capacity koja sadrži fajlove u *.doc* formatu, *prazan.doc* i *formula.doc* je testirana sa EnCase. U fajlu *prazan.doc* je zapisano da je prazan i ostavljen je na *USB* memoriji, dok je fajl *formula.doc* u kojem piše da sadrži tajnu formulu obrisan sa *USB* memorije. Novi slučaj se otvara klikom na *File – New*.

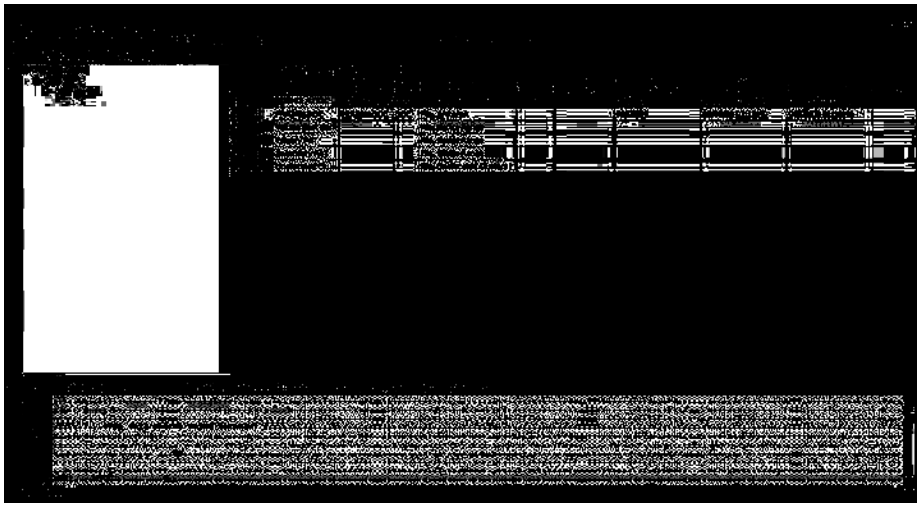
Na slici 17 je prikazana akvizicija *USB* memorije.



Slika 17: Akvizicija USB memorije

Slika je sačuvana u *C:\EVD* named *1.E01*, mada se ovo ne preporučuje ako se radi akvizicija celog hard diska, ali u ovom primeru u pitanju je akvizicija *USB* memorije malog kapaciteta. Odabran je tip kompresije *Good* (sporije i manje).

Na slici 18 se vidi sadržaj slike, moguće je videti da sadrži obrisna fajl sa imenom *_ORMULA.DOC* i fajl *PRAZAN.DOC* koji se i dalje nalazi na *USB* memoriji. Oba fajla su kreirana 02. 08. 2009, prvi u 01:13:48 a drugi 01:13:46 a pisanje je vršeno na *_ORMULA.DOC* u 01:13:24 a na drugom u 01:13:40.



Slika 18: Prikaz slike

Desnim klikom je moguće odabrati *External Viewer* pa se fajlovi mogu pregledati u eksternom pregledaču. U ovom slučaju to je *Microsoft Word*.

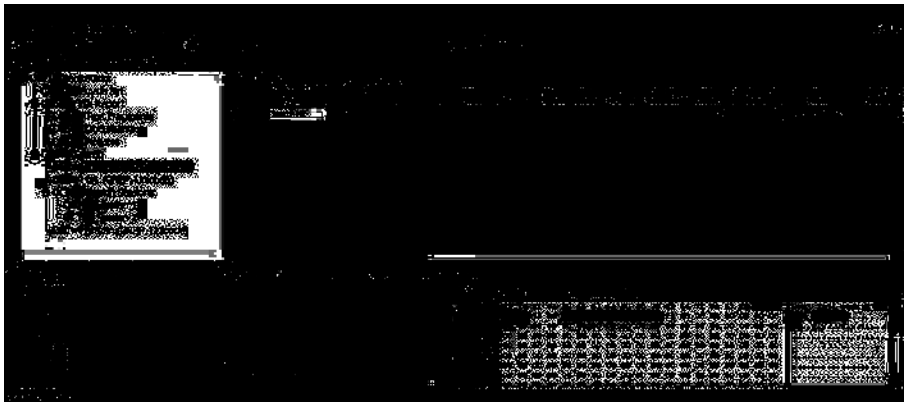
Na slici 19 je prilkazan fajl *_ORMULA.DOC* u *MS Word* i može da se vidi da u njemu piše *Ovaj fajl sadrži tajnu formulu!*.

Slika 19: Prikaz fajla formula.doc u spoljašnjem pregledaču

Zbog malog broja fajlova u ovom slučaju, jednostavno ih je sve pregledati ali važna opcija kada je u pitanju velik broj fajlova je svakako pretraga po ključnoj reči. U ovom primeru prikazanom na slici 20 zadata ključna reč je *formu..*, dok tačka predstavlja bilo koji karakter.

Slika 20: Dodavanje ključne reči

Rezultati pretrage su prikazani na slici 21 i tačna lokacija reči *formula* kao i to da se nalazi na nealociranim klasterima.



Slika 21: Rezultati pretrage za ključnu reč formu..

5. Zaključak

Buran razvoj informacionih tehnologija u današnje vreme, početka dvadeset prvog veka, učinio je da se povećava broj dostupnih forenzičkih alata a mnogi alati su i unapređeni da bi radili sa poslednjim tehnologijama. Cilj izvođenja kompjuterske forenzike nije da postoje dueli konkurentskih tehnologija, već da se sudskim putem goni osoba zbog zločina za koji je optužena. Stoga je važno da i programi otvorenog koda i zatvorenog koda zajedno rade da bi međusobno izvršili validaciju rezultata, tako da bi pravda bila zadovoljena. Ovo znači da oni koji koriste zatvoreni kod treba da imaju na umu da, treba da pokušaju da koriste i druge alate, najpre alate otvorenog koda, da bi tako ocenili svoje rezultate. Ako alat otvorenog koda dobija iste rezultate kao alat zatvorenog koda, može se smatrati da alat otvorenog koda radi ispravno. Kolekcija alata dostupnih istražitelju se stalno povećava i mnogi alati se redovno dopunjavaju od strane onih koji su ih razvili da bi mogli da rade sa poslednjim tehnologijama. Neki alati daju sličnu funkcionalnost ali različiti korisnički interfejs, kao što su alati od *Guidance Software* i *Vogon,* dok su ostali jedinstveni po informacijama koje obezbeđuju. Na istražitelju je da odluči koji će alat koristiti i koji alat je najkompetetniji istragu, uzimajući u obzir prirodu dokaza koji treba da se prikupe i činjenicu da će dokazi biti prezentovani na Sudu. Bez sumnje, porast broja slučajeva gde forenzički alati igraju značajnu ulogu čine ovo polje fascinantno za sve koji učestvuju (Forensic Focus, 2009).

6. Literatura

AccessData, Jun 05, 2009, www.accessdata.com

Bishop, M. (2003). *Computer Security: Art and Science*, Addison-Wesley Professional.

Casey, E. (2004). Computer Crime Investigation Forensic Tools and Technology, London: Elsevier Academic Press.

Chrysocome, Jun 05, 2009, www.chrysocome.net/dd

Carrier, B. (2002). *Open Source Digital Forensics Tools*, Astake Research Report

DataSolutions d.o.o., Maj 22, 2009, www.datasolutions.rs.

EnCase, Jun 05, 2009, www.encase.com

eSecurityLab, Jun 05, 2009, http://esecuritylab.net

Forensic Focus, Jun 01, 2009, www. forensicfocus.com

Đorđević, B., Pleskonjić, D., Maček, N. (2006). *Operativni sistemi:koncepti*, Beograd: Viša elektrotehnička škola.

Howard, M., Lipner, S. (2006). *The security development lifestyle*, Microsoft Press.

InformIT, Avgust 15, 2009, www.informit.com

INsig2 d.o.o., Maj 22, 2009, www.insig2.hr

Jones, K. J., Shema, M., Jonhson, B. C. (2003). *Antihakerski alati*, Čačak: Kompjuter Biblioteka.

Manson, D., Carlin, A., Ramos, S., Gyger, A., Kaufman, M. & Treichelt, J. (2007). *Is the Open Way a Better Way? Digital forensic using Open Source Tools*, Proceedings HICSC'07 Hawai USA, IEEE.

McClure, S., Scambray, J., Kurtz, G. (2006). *Hakerske tajne: zaštita mrežnih sistema*, (prevod). Beograd: Mikro knjiga.
Pastore, M., Dulaney, E. (2007). *Security* +. Miš d.o.o.
Pleskonjić, D., Đorđević, B., Maček, N., Carić, M. (2006). *Sigurnost računarskih mreža*, Beograd: Mikro knjiga.
Stmik Akakom, Jun 05, 2009, www.akakom.ac.id
Salty Brine Software, April 20, 2009, www.saltybrine.com/hexdump32.htm
Sleuthkit, Maj 12, 2009, www.sleuthkit.org
Tanenbaum, A. (2005). *Računarske mreže*. Beograd: Mikro knjiga.
Tanenbaum, A.,& Woodhull, A.(1997). *Operating System Design and Implementation*. CRCPress.
Tanenbaum, A. (2001). *Modern Operating Systems*. Prentice Hall.
Uroš, I. (2008). *Osnovi informatike*, Beograd: Kriminalističko-policijska akademija.

DIGITAL FORENSICS TOOLS

SUMMARY

Computer forensics is a scientific discipline dealing with acquiring, collecting, storing and presenting data that are electronically processed and stored on computer media. Although a relatively new discipline, it has the potential to significantly influence the specific types of investigations and prosecutions. Computer forensics is significantly different than traditional forensic disciplines. First of all, tools and techniques that this discipline demands are relatively easily available to anyone who wants to conduct forensic analysis. Contrary to traditional forensic analysis, computer investigators need to conduct testing that is not always carried out in controlled conditions. Collecting digital evidence begins when information and/or physical objects are collected or stored in anticipation of testing. The term "evidence" implies that the person who has collected it is recognized by the Court, so as the process of collecting evidence. Data or physical objects become evidence only when they are collected by an authorized person.