Centar Informacijske Sigurnosti

TSK - The Sleuth Kit

srpanj 2011.

CIS-DOC-2012-07-056

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

U ovom dokumentu su opisane karakteristike TSK (eng. The Sleuth Kit) alata otvorenog koda s kojim je pojednostavljen proces digitalne forenzike. Digitalna forenzika je grana forenzike koja prikuplja, čuva, analizira i dokumentira digitalne dokaze. Zbog različitosti medija za pohranu podataka digitalna forenzika se dijeli na podgrane. TSK je skup alata za provođenje računalne forenzike, odnosno analiziranje medija za pohranu podataka.

Alat omogućuje korisniku analizu tvrdoga diska ili nekog drugog uređaja za pohranu podataka, neovisno o operacijskom sustavu. Korisnik dobiva prikaz svih datoteka, čak i ako su izbrisane. Uz detaljan popis datoteka korisnik može tražiti, posložiti, pregledavati metapodatke i ostale mogućnosti. Alat omogućuje i vremenski prikaz aktivnosti neke datoteke što je vrlo bitno prilikom analize. Cilj forenzičara je pronaći čim više dokaza jer o tome ovisi rezultat suđenja. Kako bi se uporaba samog programa olakšala i ubrzala napravljeno je grafičko sučelje pomoću kojeg korisnik, umjesto upisa naredbi, upravlja mišem. Forenzičari se umjesto na rad samog programa sada mogu koncentrirati na samu analizu.

Alat TSK je postavio temelje analize digitalnih podataka te se većina današnjih programa temeljni na njemu. Alat je otvorenog koda te na njegovom razvoju sudjeluju brojni programeri. Alat je sastavni dio mnogih Linux distribucija za testiranje sigurnosti te forenzičke analize. Alat se primjenjuje i na većim serverskim sustavima kako bi se moguća nepravilnost odmah zabilježila.

U dokumentu je objašnjen rad samoga alata. U drugom poglavlju je objašnjeno što je to forenzika općenito te je definiran pojam digitalne forenzike. U poglavlju je naveden i postupak provođenja digitalne forenzike te njena osnovna podjela.

U trećem poglavlju je objašnjen rad s alatom. Naveden je popis naredbi te njihova primjena prilikom provođenja analize. Opisan je skup biblioteka koji programerima omogućuje korištenje TSK resursa i funkcija te su navedeni programi koji se temelje na samom alatu.

U četvrtom poglavlju je alat TSK uspoređen s drugim alatima te su navadene prednosti i mane alata.

U petom poglavlju je prikazana povijest alata te njegova budućnost.

Predzadnje i zadnje poglavlje sadrže popis poveznica za dodatne informacije i objašnjenje pojmova. Također su navedeni izvori na temelju kojeg je napisan ovaj dokument.

2. Forenzika

Forenzika je znanost koja primjenom određenih metodologija i tehnika, utvrđuje činjenice potrebne za sudski ili upravni postupak. Značenje riječi forenzika dolazi od latinske riječi *forensis*, što znači „iznositi na sudu, forumu“. Naziv potječe iz starog Rima kada su optuženik i tužitelj javnim govorima na forumu, pokušali uvjeriti skupinu osoba (sudaca) da je njihova verzija događaja istinita. Forenzika je se razvijala stoljećima, a prvi zapis korištenja forenzičkih metoda potječe iz 1248. godine u priručniku kineskog liječnika Hi Duan Yu pod imenom „*the washing away of wrongs*“. Brži razvoj forenzike je započeo 1892. godine kada je se počela koristiti identifikacija pomoću otiska prstiju. U začecima su se forenzikom bavili samo specijalizirani ljudi ili odbor ljudi. U moderno doba se njome bave stručnjaci iz raznih područja, od znanstvenika s područja medicine pa do računalnih inženjera. Kako se radi o vrlo širokom spektru djelatnosti, forenzika se grana na manje podcjeline, kao što su:

- kriminalistička,
- digitalna,
- forenzika arheologije,
- DNA (eng. D*eoxyriboNucleic Acid*)analiza,
- forenzika porijekla.
- forenzika lingvistike,
- forenzika otrovnih sredstava,
- forenzika video analize.

Digitalna forenzika je grana forenzike kojoj je cilj prikupiti, sačuvati i analizirati dokaze u digitalnom obliku. Dokazi u digitalnom obliku su razni zapisi na digitalnim memorijskim uređajima. Dokazi mogu biti slike nepoćudnog sadržaja, kao što je na primjer dječja pornografija, nelegalni videozapisi i zvučni zapisi te tajni ili uvredljivi dokumenti. Digitalna forenzika, se zbog različitih vrsta uređaja koji pohranjuju podatke, dijeli na:

- računalnu forenziku,
- mrežnu forenziku,
- forenziku mobilnih uređaja,
- forenziku baza podataka.

Zbog složenosti samog područja, digitalna forenzika se može podijeliti i po sustavima za koje se primjenjuje. Forenzičar ne može pratiti razvoj različitih sustava, pa se on specijalizira za jedan, na primjer za Linux operacijski sustav ili Android sustav ako se bavi mobilnim uređajima.

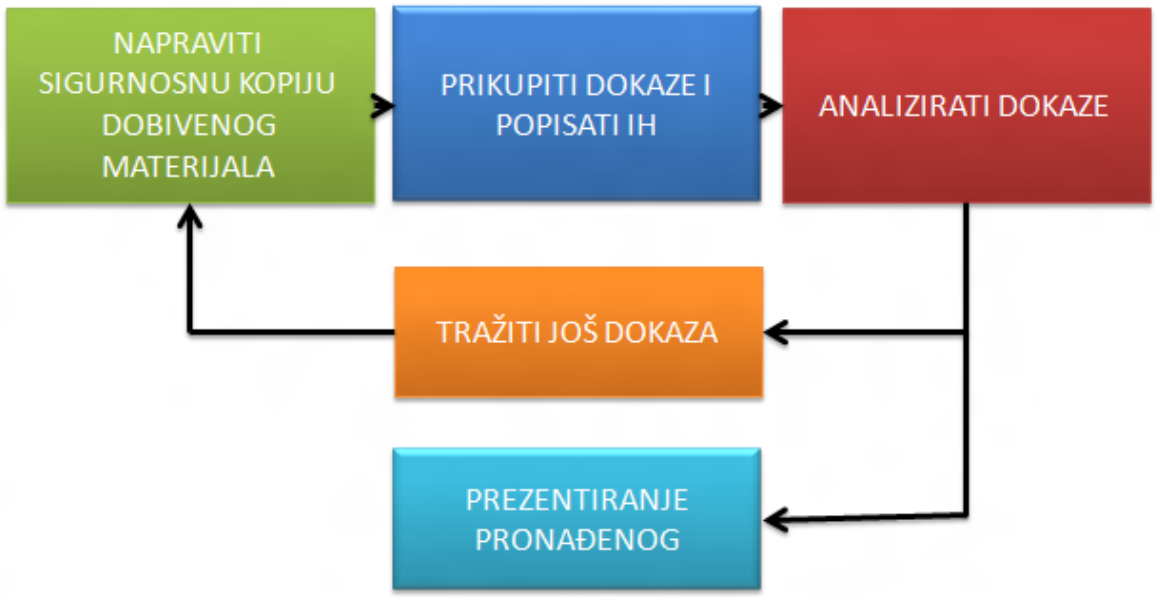
Digitalna forenzika postoji otkako se na računalima pohranjivalo podatke koji se mogu koristiti kao dokaz. U početku se to odnosilo samo na postojane podatke, odnosno podatke koji su sačuvani na tvrdom disku ili nekom drugom mediju, te ostaju na njemu i kada je uređaj ugašen. U današnje vrijeme je izrazito bitan i pregled podataka koji će se izbrisati nakon gašenja računala, na primjer podaci spremljeni u registre, *cache* memoriju ili radnu mermoiju. Ekspanzijom Interneta dolazi do razvoja sigurnosnih sustava s mogućnošću otkrivanja pokušaja proboja u sustav. Administratori sustava moraju biti upoznati s procesom provođenja digitalne forenzike te u slučaju incidenta, prikupiti što više podataka.

Digitalna forezika, osim pravila provođenja, ima zakonske normative. Propisani zakon ovisi od države do države, pa tako u republici Hrvatskoj imamo par zakona vezanih uz prikupljanje digitalih dokaza te zapljenu digitalnih uređaja. Prema članku 257. Zakona o kaznenom postupku okrivljenik je dužan omogućiti pristup računalu ili drugim medijima za pohranu podataka. Također, davatelj telekomunikacijskih usluga je dužan predati ispis mrežnih aktivnosti okrivljenika. Uz navedeno, u članku je spomenuta i potreba očuvanja zaplijenjenog materijala. U članku 263. istoga zakona se nadležnim službama, odnosno sudu daje pravo oduzimanja računale opreme ako za to postoji opravdana sumnja o počinjenju kaznenog djela koji je definiran u članku 334. Uz same zakone, postoje i pravila po kojima se provodi digitalna forenzika. Pravila se indirektno mogu zaključiti iz pravila o primjeni forenzike.

2.1. Proces provođenja digitalne forenzike

Proces provođenja digitalne forenzike je strogo definiran. Nakon što je računalnom kriminalcu zaplijenjeno računalo, sud odabire forenzičara (sudskog vještaka) ili više njih koji provode digitalnu forenziku. Sudski vještak provodi analizu te iznosi svoje mišljenje koje sud prihvati bez propitivanja valjanosti, osim ako optuženik i/ili tužitelj ne zatraže novu forenzičku analizu te se sud s time složi. Sudski vještak preuzima na sebe odgovornost da će sačuvati dokazni materijal u izvornom obliku te da će zabilježiti sve nepravilnosti. Sudski vještak predaje svoje mišljenje tek nakon što je siguran da je sve pronašao jer ishod suđenja ovisi o količini pronađenih dokaza.

Sam proces provođenja analize je prikazan slikom.

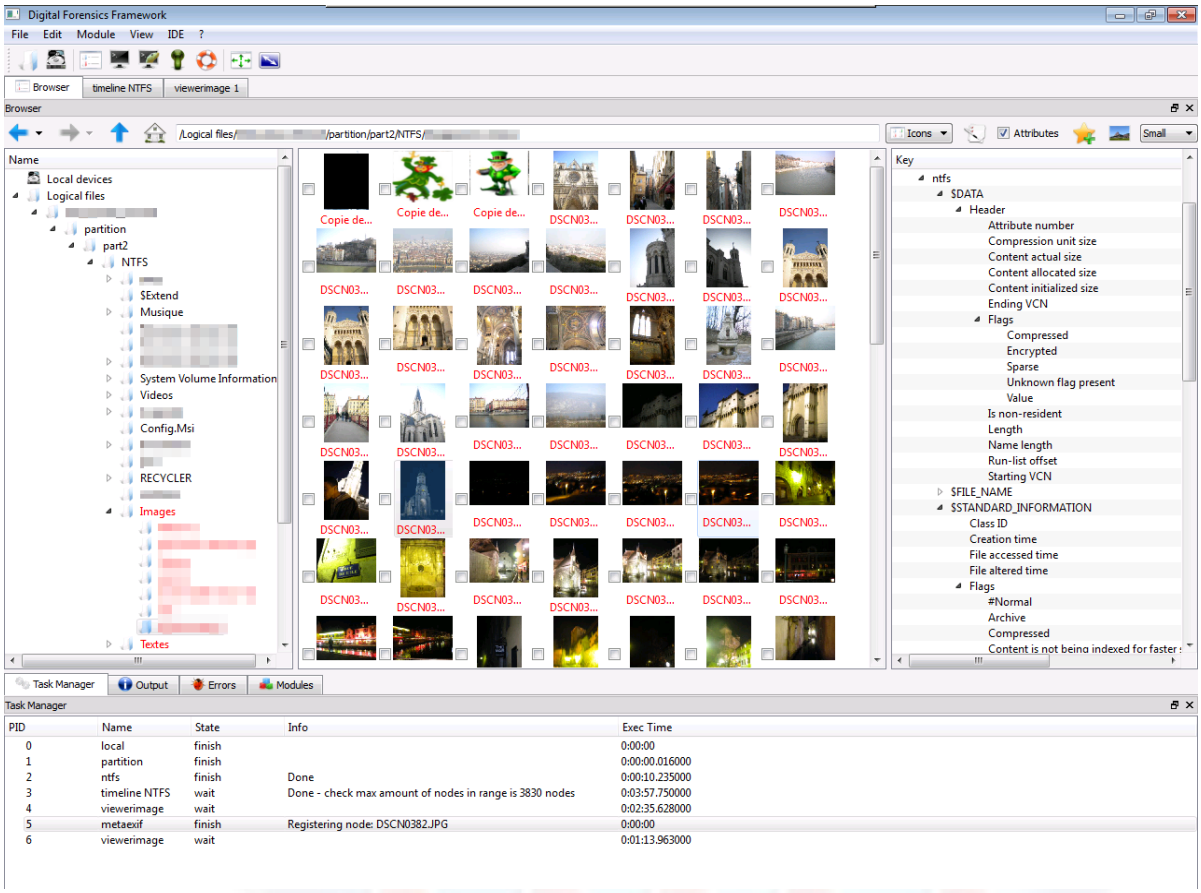


Slika 1. *Proces izvođenja digitalne forenzike*
Izvor: *LSS*

Nakon što sudski vještak dobije dokazni materijal koji je zaplijenjen optuženiku, on radi više sigurnosnih kopija koje će analizirat te time neće promijeniti dokazni materijal. Ako je na primjer optuženik optužen za dječju pornografiju te mu je zaplijenjen tvrdi disk koji sadrži slike (dokaze), onda sudski vještak sve te dokaze prekopira na vlastiti disk te dokazni materijal odloži na sigurno mjesto dok ne analizira prekopirane podatke. Također forenzičar radi sažetak diska koji služi kao provjera je li disk identičan dobivenom. Tijekom analize dobiveni tvrdi disk ili uređaj trebaju biti na sigurnom mjestu te forenzičar mora bilježiti sve otkrivene nepravilnosti. Forenzičar prikuplja i zapisuje nepravilnosti sve dok nije siguran da je prikupio sve dokaze. Ishod presude ovidi o broju prikupljenih dokaza. Prilikom analize podataka, forenzičar može koristi razne alate, kao što su:

- DFF (eng. Digital Forensics Framework) – alat otvorenog koda s mogućnošću analiziranja svih poznatijih operacijskih i datotečnih sustava. Ima vlastito grafičko sučelje koja olakšava njegovu uporabu.
- Hachoir – skup biblioteka namijenjenim Python programerima. Nema definirano grafičko sučelje te ima nešto manji broj opcija od ostalih alata
- Scalpel – program otvorenog koda koji podržava najpoznatije datotečne sustave. Uz standardne mogućnosti, program neke funkcije izvodi uz pomoć grafičkog procesora čime se dobiva na dodatnoj brzini prilikom obrade.

- Autopsy – grafičko sučelje alata TSK čime se složene naredbe pretvaraju u jednostavan odabir opcija



Slika 2. DFF
Izvor: Digital-forensic

3. Alat TSK

Alat TSK je najpoznatiji program za digitalnu forenziku. To je skup alata s kojima se automatizira i pojednostavljuje provedba računalne forenzike. Alat TSK nema grafičko sučelje, već se programom upravlja upisom naredbi u naredbenu liniju (terminal, CMD). Kako bi se uporaba ovog programa pojednostavila napravljen je program Autopsy, koji forenzičaru nudi grafičko sučelje (izbornike) pomoću kojih može uz par klika mišem upravljati alatom TSK. Kako se radi zapravo o istom programu, razumijevanje rada i mogućnosti alata TSK je nužno za rad s programom Autopsy. Alat TSK se sastoji od dva dijela:

- naredbe alata TSK,
- dodatnih biblioteka za programere.

3.1. Naredbe alata TSK

Datotečni sustav je skup alata odnosno biblioteka, koje forenzičaru omogućuju pregledavanje datoteka na tvrdom disku. S ovim alatom je moguće pročitati datoteke koje su izbrisane te datoteke kojima je izmijenjen format. Prethodno spomenuti primjer optuženika čiji je disk s dječjom pornografijom zapljenjen je idealan za objašnjenja samog alata. Prije nego se započne sa samom analizom potrebno je napraviti sigurnosnu kopiju zaprimljenog materijala. To se može napraviti s programom dd[1] sljedećom naredbom:

```
dd if=/dev/sdb of=/home/lss/kopija.dd
```

Gornja naredba će kopirati sve podatke s uređaja (npr. tvrdi disk) sdb u datoteku kopija.dd. Podatke se može kopirati i na drugi tvrdi disk ili usb memoriju, ali je lakša uporaba programa s datotekom. Nakon što je napravljena datoteka možemo je otvoriti sa alatom TSK. Za otvaranje se koriste naredbe mmls i fls.

Mmls naredba prikazuje detaljan popis particija i praznog prostora te vrstu particijske tablice:

```
lss@linux:~$ mmls kopija.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000001   0000000062   0000000062   Unallocated
02:  00:00   0000000063   0007823654   0007823592   Win95 FAT32 (0x0B)
03:  -----   0007823655   0007827455   0000003801   Unallocated
```

Naredba fls prikazuje popis datoteka te stavlja posebnu oznaku na izbrisane datoteke. Svaki datotečni sustav sadrži na svojem početku tablicu, odnosno popis svih datoteka koje se nalaze na njemu. Kada korisnik izbriše neku datoteku, ona se ne uklanja s diska, već se samo miče s liste. Kada naredba fls čita disk, ona ne čita tu listu već na temelju posebnih oznaka za kraj, a time i početak iduće datoteke, zaključuje da se radi o datoteci. Ako je korisnik na mjestu prijašnje datoteke zapisao novu, onda će naredbi fls biti teže, ako ne i nemoguće pročitati prijašnju datoteku.

```
lss@linux:~$ fls -o 63 kopija.dd
r/r * 3:    _ekst.txt
r/r 4:      tekst.txt
r/r 5:      popis.txt
```

[1] dd - UNIX program namijenjen kopiranju bitova podataka. Ime dolazi od riječi *Data Description*, iako se je prvobitno trebao zvati cc (eng. *convert and copy*) ali je ime zauzeto.

Kao što je vidljivo iz primjera, datoteka _ekst.txt je obrisana, a ostale su očuvane. Također naredbi je predan i broj od koje adrese će ispisati, pošto je zaključeno da je prostor prije te adrese prazan, odnosno slobodan (eng. *unallocated*). Kako bi sačuvanu datoteku snimili na vlastiti medij za pohranu koristimo naredbu icat:

```
lss@linux:~$ icat -o 63 -r kopija.dd 4 > kopija_tekst.txt
```

Icat naredbi smo također predali adresu s koje treba tražiti datoteku četiri (svakoj datoteci je dodijeljen broj). Ovu naredbu možemo koristiti i za izbrisanu datoteku samo ako ima pravilnu MD5 vrijednost. Kako bi provjerili je li moguće spasiti neku datoteku koristimo naredbu istat, koja uz navedenu provjeru ispisuje

```
lss@linux:~$ istat -o 63 kopija.dd 3
Directory Entry: 3
Not Allocated
File Attributes: File, Archive
Size: 0
Name: _ekst.txt

Directory Entry Times:
Written: Thu Feb 25 20:33:44 2010
Accessed: Thu Feb 25 00:00:00 2010
Created: Thu Feb 25 20:33:42 2010

Sectors:

Recovery:
File recovery not possible
```

Istat ispisuje na kojoj se poziciji u diskovnoj hjerarhiji nalazi datoteka, prikazuje je li datoteka izbrisana (eng. not allocated) ili očuvana (eng. allocated), koje je vrste datoteka, veličinu, ime, vrijeme zapisivanja, pristupa te stvaranja datoteke, prostor koji zauzima (sketori) te može li se datoteka spasiti ili ne. Vrijeme pristupa, zapisanja i stvaranja datoteke je vrlo bitna informacija. Ako je računalo privremeno bilo kod optužnikovog poznanika ili na servisu te ako se vrijeme vezano za datoteku preklapa s tim vremenom, znači da optuženik nije imao kontakta s njome. Također su bitni i atributi datoteke. Ako je optuženik promijenio nastavak datoteke, npr. slika.jpg je preimenovao u popis.txt, onda ćemo uz pomoć atributa doznati da se zapravo radi o slici. Atribut datoteke se doznaje iz njenog zaglavlja a ne imena, odnosno nastavka. Svaka datoteka na svojem početku sadrži tablicu s podacima o autoru, vremenu nastanka, vrsti datoteke (atribut) i ostale informacije. Vidljivo se ova datoteka ne može spasiti, ali se sa naredbom strings možda može pročitati kao tekst:

```
lss@linux:~$ strings -tx kopija.dd
7e03 mkdosfs
7e46 K           FAT32
7e77 This is not a bootable disk.  Please insert a bootable floppy and
7eba press any key to try again ...
8000 RRaA
81e4 rrAa
8a03 mkdosfs
8a46 K           FAT32
8a77 This is not a bootable disk.  Please insert a bootable floppy and
8aba press any key to try again ...
77e601 EKST   TXT
3 77e610 Y<Y<
77e620 TEKST   TXT
77e630 Y<Y<
77f600 TEKST IZ DATOTEKE!!
```

Ova naredba će dati ispis cijele datotečne slike u obliku teksta. Ako se ni s ovom naredbom ne uspije doznati sadržaj datoteka, onda se ona ne može spasiti (npr. možda je kriptirana).

Ponekad se prilikom analize treba pregledati heksadecimalne vrijednosti datoteke. To se može napraviti s hexdump programom:

```
lss@linux:~$ hexdump -C kopija.dd
```

Program će ispisati heksidecimalne vrijednosti cijelog diska.

Osim naredbi vezanih za samu datoteku alat TSK sadrži i naredbe za otkrivanje informacija o samom datotečnom sustavu i vremenskoj aktivnosti računala.

```
lss@linux:~$ fsstat -o 63 kopija.dd

FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT32
OEM Name: mkdosfs
Volume ID: 0x4b871ef2
Volume Label (Boot Sector):
Volume Label (Root Directory):
File System Type Label: FAT32
Next Free Sector (FS Info): 15300
Free Sector Count (FS Info): 7808288
Sectors before file system: 0
File System Layout (in sectors)
Total Range: 0 - 7823591
* Reserved: 0 - 31
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 32 - 7657
* FAT 1: 7658 - 15283
* Data Area: 15284 - 7823591
** Cluster Area: 15284 - 7823587
*** Root Directory: 15284 - 15291
** Non-clustered: 7823588 - 7823591

METADATA INFORMATION
--------------------------------------------
Range: 2 - 124932930
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 2 - 976039

FAT CONTENTS (in sectors)
--------------------------------------------
15284-15291 (8) -> EOF
15292-15299 (8) -> EOF
```

Iz dobivenih rezultata možemo zaključiti da se radi o FAT32 (eng. *File Allocation table*) što je dobra informacija u slučaju da smo upoznati sa strukturom FAT datotečnih sustava.

Ovim postupkom su opisane najvažnije naredbe ovoga programa. Naredbe se mogu podijeliti prema funkciji koju obavljaju na:

- Naredbe datotečnog sustava – informacije o datotečnom sustavi i strukturi datoteka.
  - ,,Fstat“ – prikazuje detalje (statistiku, strukturu, veličinu, particije) datotečnog sustava.
- Datotečne naredbe – koriste se za prikaz hjerarhije datoteka, njihova imena.
  - „Ffind“ – traži datoteku, bila ona izbrisana ili ne, na temelju naziva,
  - „Fls“ – prikazuje sve datoteke i direktorije.
- Naredbe za metapodatke – služe za prikaz metapodataka.
  - „Icat“ – sprema datoteke na lokalni medij za pohranu, uz pomoć metapodataka (podaci o veličini, imenu datoteke i ostalim podacima),
  - „Ifind“ – traži zadani podatak u metapodacima,
  - „Ils“ – ispisuje metapodatke unutar direktorija,
  - „Istat“ – prikazuje metapodatke o datoteci.
- Naredbe za podatke – skupina naredbi namijenjena upravljanju binarnim podacima (podatke tretira kao skupinu blokova i sektora).
  - „Blkcat“ – prikazuje sadržaj nekog podatka,
  - „Blkls“ – prikazuje podatke na nekom mediju za pohranu (slično fls naredbi),
  - „Blkstat“ – prikazuje statistike podatka,
  - „Blkcalc“ - računa adresu koja sadrži neki podatak (koristi se najčešće kod izbrisanih dijelova medija za pohranu).
- Diskovne naredbe – prikazuju strukturu samog medija za pohranu.
  - „Mmls“ – prikazuje cijelokupnu strukturu medija,

Osim navedenih naredbi, postoje naredbe koje automatiziraju određene procese, kao što su:

- „tsk_comparedir“ – uspoređuje dva datotečna sustava, primjenjivo za pronalazak rootkita[2],
- „tsk_gettimes“ – prikazuje vremensku aktivnost podataka (sat kreiranja i ostalo),
- „tsk_loaddb“ – metapodatke sprema u bazu podataka SQLite[3] ,
- „tsk_recover“ – snima sve podatke (izbrisane i neizbrisane) na lokalni disk.

Kako bi se postupak digitalne analize ubrzao i olakšao naprevljen je program Autopsy. Autopsy je grafičko sučelje alata TSK pisano u HTML (eng. *HyperText Markup Language*) prezentacijskom jeziku. Autopsy se otvara u web pregledniku te korisniku uz pomoć autoamatiziranih radnji prikazuje cjelokupnu diskovnu hjerarhiju materijala za obradu. Korisnik uz pomoć izbornika pokreće navedene naredbe, bez znanja o njihovim imenima te parametrima koje one primaju. Ovim pojednostavljenjem te automatiziranim naredbama alat TSK je postao dostupan široj javnosti. Na slici je prikazan izgled sučelja.

[2] Rootkit – zlonamjerni programi napravljeni da bi preuzeli kontrolu nad operacijskim sustavom tako da nadomjeste sustavske procese i podatke bez znanja korisnika

[3] SQLite – baza podataka temeljena na C programskoj biblioteci

Slika 3. *Autopsy*
Izvor: *Sectools*

Popis svih naredbi naredbi s opisom se može naći na web stranici projekta:

http://wiki.sleuthkit.org/index.php?title=TSK_Tool_Overview

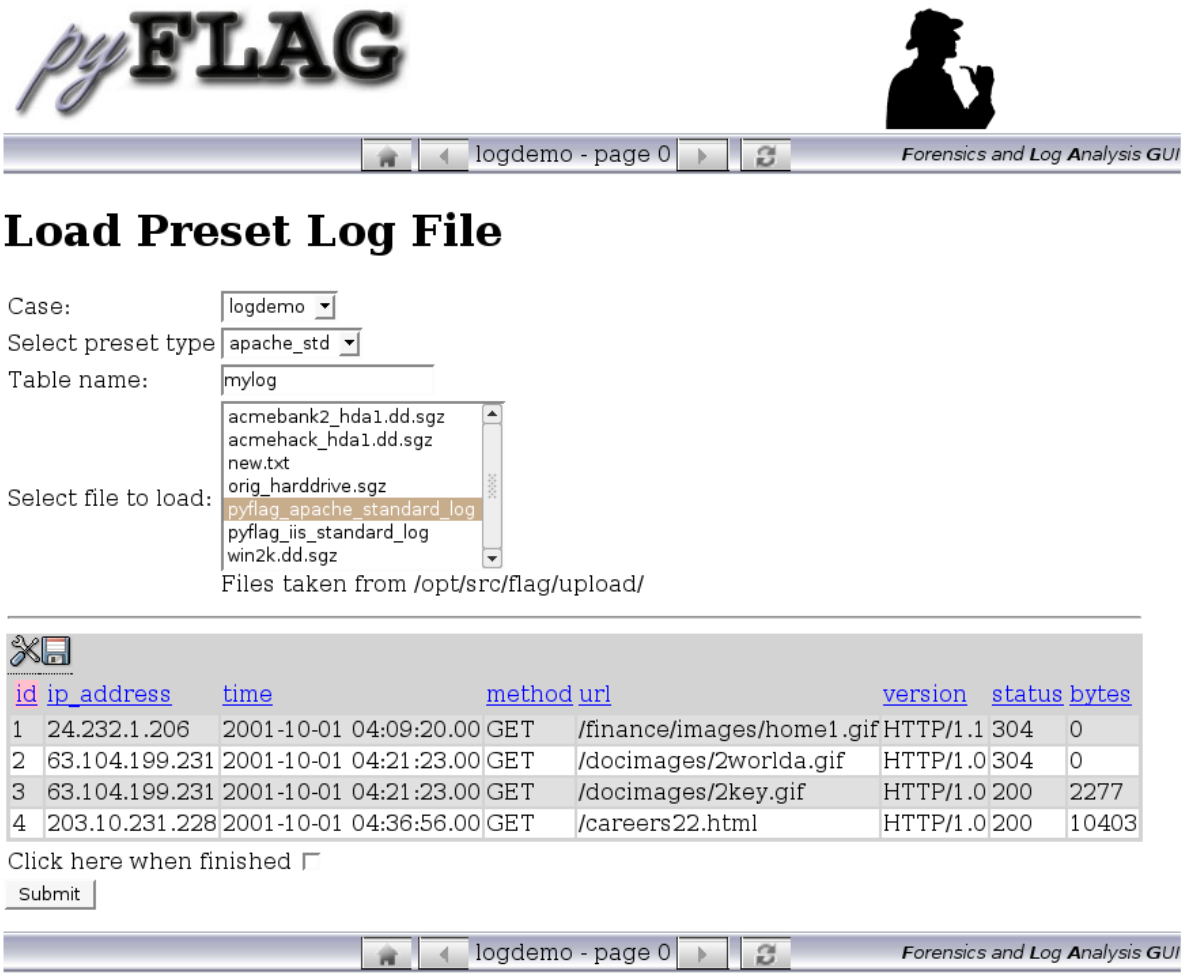
3.2. TSK biblioteke

Izuzev ugrađenih naredbi, alat TSK posjeduje mogućnost dodavanja raznih dodataka čime se povećava opseg programa. Programeri na vrlo jednostavan način, koristeći skup biblioteka - TSK API (eng. application programming interface), mogu programirati vlastite dodatke. Navedeni skup biblioteka je pisan i potpuno kompatibilan s programskim jezikom C , a radi se na boljoj podršci i za ostale programske jezike. Ova mogućnost proširivanja mnogi koriste jer ako, na primjer, trebaju analizirati tvrdi disk osobe optužene za dječju pornografiju, onda je dobro imati automatizirani alat koji daje prikaz svih slika. Uz mogućnost pisanja vlastitih alata, postoje već gotovi alati koji koriste TSK API. Neki od važnijih takvih alata su:

- Fiwalk,
- PyFlag,
- Raw2FS,
- MultiFS,
- SFDumper,
- FUNDL,
- Odyssey Digital Forensic Search.

Fiwalk je program koji metapodatake (podaci o autoru, datumu kreiranja datoteke i slično) nekog programa sprema u XML (eng. Extensible Markup Language) datoteku, a kreirao ga je Simson Garfinkel. PyFlag, prikazan na slici, je grafički program za forenziku mreža, zapisa aktivnosti i memorijsku forenziku. Napravli su ga Michael Cohen i David Collet. Veliki doprinos razvoju

forenzičkih alata je pridonio Nanni Bassetti s alatima: Raw2FS (skup binarnih brojeva pretvara u smislen naziv datoteke), MultiFS (otkriva vrstu datotečnog sustava), SFDumper (omogućuje vraćanje izbrisanih datoteka jednostavnije od alata TSK) i FUNDL (radi slično SFDumperu). Kako bi se lakše našao podatak, bio on unutar datoteke ili sama datoteka, izumljen je Odyssey Digital Forensic Search (ODFS). Zbog svoje lakoće i jakih alata, ODFS je vrlo raširen te drastično ubrzava proces forenzičke analize.



Slika 4. *PyFlag*
Izvor: *PyFlag*

Iako postotoje razni alati koji dolaze sa samim programom, primjetno neki alati nedostaju. Na primjer, unutar alata TSK, nedostaje program s kojim bi se moglo čitati registar operacijskog sustava Windows, kao i alat za čitanje povijesti web preglednika. Ugradnjom ovih alata bi se umanjila potreba korištenje zasebnih programa, odnosno alata.

Više informacija o funkcijama alata TSK koje se mogu koristiti prilikom programiranja se nalaze na stranici projekta:

http://www.sleuthkit.org/sleuthkit/docs/api-docs/

3.3. Podrška

Alat TSK podržava razne formate tvrdih diskova, operacijskih sustava te *hash* funkcija. Trenutne platforme koje alat TSK podržava su:

- Windows sustav,
- Linux sustav,
- OS X sustav,
- Cygwin alat,
- OpenBSD, FreeBSD i ostali BSD sustavi,
- Solaris sustav.

Alat TSK podržava mnoge datotečne sustave:

- NTFS (eng. *New Technology File System*),
- FAT12, FAT16, FAT32 (eng.*Fille Allocation Table*),
- HFS+ (eng. *Hierarchical File System*),
- ISO9660 (eng. International Organization for Standardization),
- Ext2, Ext3 (eng. *Extended file system*),
- UFS1, UFS2, FFS (eng. Unix *file system).*

Uz datotečne sustave, podržava i nekoliko vrsta particija:

- DOS (eng. Disk Operating System) particije,
- GPT (eng. *Globally unique identifier Partition Table*) particije,
- MAC particije,
- BSD (eng. Berkeley Software Distribution) particije,
- SUN VTOC (eng. *Volume table of contents*).

te nekoliko baza podataka:

- NSRL (eng. National Software Reference Library),
- Hashkeeper,
- Md5sum/sha1sum.

Programeri alata TSK rade na široj podršci sustava, posebice datotečnog sustava Ext4. Ovi podaci, koji su više tehničke prirode, su bitni svakom digitalnom forenzičaru jer daju uvid što se sve s programom može analiziarti, a što ne može.

4. Usporedba s ostalim alatima

U novije vrijeme postoje mnogi alati za provođenje digitalne forenzike. Neki od njih su komercijalni (zatvorenog koda i plaćaju se), a neki su besplatni te otvorenog koda čime je omogućeno da se i ostali programeri uključe u razvoj ovih alata. Uz alat TSK još su poznati EnCase, FTK (eng. Forensics toolkit), Microsoft COFEE (eng. Computer Online Forensics Evidence Extractor), OCFA (eng. Open Computer Forensics Arhitecture) i Bulk Extractor.

Kako bi drugi alati mogli konkurirati alatu TSK, rade se brojni dodaci. EnCase je komercijalni program koji dolazi u više inačica, a najbolja je Enterprise inačica. Program uz analiziranje računalnih sustava, ima mogućnost analiziranja tablet računala te pametnih telefona. Datotečni sustav u programu omogućuje pregled preko 1000 formata, uključujući pregled registra operacijskog sustava, što alat TSK ne može. Program ima i vlastitu biblioteku za pisanje dodataka, baš kao i alat TSK. Ostali alati su identični. Alat FTK je, za razliku od programa EnCase, besplatan. Program se može pohvaliti povećom bazom *hash* funkcija, preko 45 milijuna. Također, omogućuje i spašavanje šifri zaključanih programa ili datoteka. Još jedna od prednosti alata je ta što je grafičko sučelje odvojeno od samog programa. Ako dođe do greške ili pada grafičkog sučelja, program će obraditi započeti proces do kraja. Alat podržava preko 700 formata te sve poznate datotečne sustave, kao i Blackberry i Android operacijske sustave. Među alatima ima i algoritme za dekripciju određenih formata te mogućnost otkrivanja pornografskog sadržaja sa slika.

Alat Microsoft COFF je alat namijenjen samo profesionalnim forenzičarima te nije dostupan široj javnosti. Alat može analizirati samo Windows operacijski sustav i sadrži oko 150 alata. Alat OCFA je alat otvorenog koda koji ne posjeduje sve mogućnosti alata TSK. Jedina prednost mu je brzina obrade podatka,

Alat Bulk Extractor je program otvorenog koda, pisan u programskom jeziku C++. Program skenira dokazni materijal te sprema sve pronađene podatke u datoteke. Program prije analize napravi tekstualne datoteke u koje će spremti brojeve kreditnih kartica, konfiguraciju mreže, podatke sa slika, telefonske brojeve, povijest pretrage i još nekolicinu podataka. Nedostatak alata je što ne omogućuje pregled zaprimljenog materijala već samo traži podatke koji su definirani u programu.

Od svih navedenih alata jedino EnCase i FTK alati mogu konkurirati TSK alatu. Alat TSK uz dodatke može analizirati sve što i analiziraju ova dva programa, no nažalost još uvijek nije prisutna podrška za mobilne uređaje.

5. Povijest

Zbog potrebe da se napravi alat za digitalnu forenziku, 2000. godine, programeri Dan Farmer i Wietse Venema objavljuju TCT (eng. The Coroner's Toolkit). Alat je mogao prikazati sve podatke koji se nalaze na disku bili oni izbrisani ili ne. Bio je namijenjen operacijskim sustavima UNIX te je podržavao samo diskovne formate Ext2 i UFS. Nedostatak alata je bila ta što je prikazivao blokove, a ne stvarna imena datoteka, npr: alat bi javio da se od bloka 20 do bloka 50 nalazi tekstualna datoteka, ali nije prikazivao njen naziv. Programer Brian Carrier, 2001. godine, objavljuje alat TCTUtils. Alat TCTUtils je uveo mogućnost prikaza direktorija odnosno imena datoteka te mogućnost traženja po adresi. Ovom je novinom omogućeno korisniku da pregledava vlastiti disk (otvara datoteke, slike, tekst i slično). Integracijom alata TCT i TCTUtils, 2002. godine, nastaje novi alat TASK (eng. The @stake Sleuth Kit) koji je uz mogućnosti oba alata, uveo i podršku za nove diskovne formate, kao što su FAT, NTFS, OS X i Cygwin. Alat TASK se 2003. godine preimenovao u TSK. Kako bi se rad s alatom TSK olakšao napravljen je program Autopsy s HTML (eng. *HyperText Markup Language*) zasnovanim grafičkim sučeljem, što znači da se program pokreće s web preglednikom. HTML sadrži popis pravila kako će se izbornik i gumbi te ostali elementi prikazati u samom web pregledniku.

5.1. Daljnji razvoj

Programeri teže tome da naprave automatiziran alat, koji će bez korisničke interakcije uspijeti obraditi informacije te rezultate prikazati korisniku. Također se teži pojednostavljivanju biblioteka samog programa te širenju podrške za programske jezike C++, Java i Python. Time bi se povećao broj programera koji bi doprinosili izradi alata za digitalnu forenziku. Osim programskih jezika, teži se i podršci za druge datotečne sustave. Kako bi se povećale mogućnosti programa Autopsy, programiraju se dodaci koji bi omogućili pregled registra operacijskog sustava (npr. Windows Registry), pregled Internet povijesti i ostale mogućnost. Veliki napraedak je primjetan i kod sučelja programa Autopsy koji bi se ipak mogao malo više prilagoditi stvarnom datotečnom sustavu, na primjer mogla bi se uvest *drag & drop* tehnika[4]

[4] *Drag & drop* tehnika - korisnik klikom na datoteku i njenim odvlađenjem na drugo mjesto je zapravo kopira

6. Zaključak

Razvojem Interneta se razvija i računalni kriminal, čime se javlja potreba za razvojem alata s kojima će se nelegalne aktivnosti moći uočiti i ukloniti. Digitalna forenzika je jedno od mnogih područja koje nude riješenje na te probleme. Osim forenzičke analize računala i mreža, danas je sve učestalija i forenzika mobilnih uređaja. Pametni telefoni su danas dostupni vrlo velikom broju ljudi te zbog jednostavnijeg korištenja nego računala, vrlo su se brzo raširili.

Danas su zastupljene mnoge vrste računalnog kriminala. Nekoć dok je pristup Internetu bio spor i skup, jedini računalni kriminalci su bile osobe koje su svojim znanjem pokušavali probiti u telekom kompanije. Kako bi se otkrile ovakve vrste napada definirana je mrežna forenzika. Pomoću ove forenzike se ispituje mrežna aktivnost napadača te žrtve kako bi se vidjelo kada je napad izveden i koja je šteta. Nakon što su predstavljeni ,,brzi“ modemi[5] , počinje se javljati nelegalno dijeljenje sadržaja (slike, glazba, a kasnije i filmovi). Kako bi se vidjelo je li je neka osoba posjedovala ili posjeduje nelegalan sadržaj definirana je forenzika računala. U današnje vrijeme su ,,popularni“ i napadi na velike baze podataka, na primjer. napad skupine Anonymous na tvrtku Sony. Kako bi tvrtka Sony otkrila razinu štete korištena je forenzika mreže, računala te baza podataka. U najnovije vrijeme, širenjem mobilnih uređaja kao što su na primjer pametni telefoni, javlja se potreba i za forenzikom takvih uređaja. Moguće da će u budućnosti i alat TSK dobiti ovu mogućnost, pošto je puno veća vjerojatnost da se nelegalni sadržaj pohranjuju na prijenosnom mediju.

Alat TSK je jedan od najvažnijih alata za provođenje digitalne forenzičke analize. Program je postavio temeljne algoritme za traženje izbrisanih datoteka, kao i prepoznavanje vrste datoteka na temelju njenog zaglavlja. Objedinjavanjem velikog broja opcija, alat TSK je postao brz i snažan alat za analiziranje sustava. Popularizaciji alata TSK je pridonio program Autopsy, koji je zapravo grafičko sučelje alata TSK. Program Autopsy je puno jednostavniji za korištenje te se danas češće on koristi prilikom digitalne forenzike. Osim programa Autopsy, razvijeni su mnogi drugi alati koristeći sučelje TSK API, odnosno njegove resurse i funkcije. Vrlo je vjerovatno i da većina današnjih alata za spašavanje podataka koristi alat TSK u svojoj bazi. Alat TSK osim što može čitati izbrisane podatke na temelju oznaka za početak i kraj datoteke, može i iz pročitanih fragmenata (malih djelova) obnoviti većinu datoteke. Najveći problem predstavlja slučaj kada je korisnik izbrisao datoteku i na njeno mjesto nekoliko puta zapisao novu. Tada takvu datoteku nije moguće spasiti, odnosno otkriti. Problem predstavljaju i nove tehnologije koje će se koristiti u SSD[6](eng. *Solid-state drive*) diskovima. Alat TSK je vrlo kvalitetno napravljen skup alata s kvalitetnim algoritmima za spašavanja i prikaz datoteka, ali ima određenih nedostatak koje će programeri ispraviti. Ako zanemarimo ove kozmetičke detalje i ako nedostatke ugrađenih alata kompeziramo korištenjem drugih programa, dobit ćemo idealan program ili programe za digitalnu forenziku.

[5] Modem – uređaj koji modulira signa u blik pogodan za prijenos, a nakon prijenosa ga demodulira u izvorni oblik. Uglavnom služi sa spajanje na Internet ili kao telefaks.

[6] SSD - memorijski uređaji koji ne koriste klasični disk za zapisivanje, već zapisuju na memorijske pločice, slično USB memorijama ili karticama iz digitalnog fotoaparata

7. Leksikon pojmova

Digitalna forenzika

Digitalna forenzika je grana forenzike koja ima cilj prikupljanje, čuvanje, pronalaženje, analizu i dokumentiranje digitalnih dokaza tj. Podataka koji su skladišteni, obrađivani ili prenošeni u digitalnom obliku.

http://hr.wikipedia.org/wiki/Digitalna_forenzika

Alat TSK

Alat TSK (eng. The Sleuth Kit) je skup alata, otvorenog koda, namijenjenih provođenju digitalne forenzike.
http://www.sleuthkit.org/

Autopsy

Program Autopsy je grafičko sučelje alata TSK čija je svrha pojednostaviti proces analiziranja medija za pohranu. Forenzičar uz pomoć ovoga programa ne mora biti upoznat s naredbama samog TSK alata.

http://www.sleuthkit.org/autopsy/

Digital Forensics Framework (DFF)

Alat otvorenog koda za digitalnu forenziku. Alat ima jednostavno grafičko sučelje te ga mogu koristiti profesionalni i obični korisnici. Alat dolazi s vlastitim APIjem čime je omogućeno proširivanje funkcionalnosti samog programa.

http://www.digital-forensic.org/

Hachoir

Hachoir je Python biblioteka koja programerima omogućuje da bilo koji skup binarnih podataka pretvori u smislene datoteke i direktorije.

https://bitbucket.org/haypo/hachoir/wiki/Home

Scalpel

Također jedan od programa koji koristi TSK kao bazu. Program nema grafičko sučelje i nema poseban API.

http://www.digitalforensicssolutions.com/Scalpel/

Autopsy

Alat koji pruža grafičko sučelje TSK programskom paketu. Ima široku podršku, od operacijskih sustava, pa sve do diskovnih formata. Progarm se otvara unutar web preglednika te nudi jednostavno sučelje s kojim se vrlo brzo mogu analizirat materijali.

http://www.cert.hr/node/15263

Datotečni sustav

Datotečni sustav je način pohranjivanja i organiziranja računalnih datoteka. Oni su sastvani dio same jezgre operacijskog sustava.

http://hr.wikipedia.org/wiki/Datotečni_sustav

Aplikacijsko programsko sučelje (API)

API ili sučelje za programiranje aplikacija je skup određenih pravila i specifikacija koje programeri koriste kako bi se mogli služiti uslugama ili resursima operacijskog sutava ili nekog drugog programa.

http://hr.wikipedia.org/wiki/API

C programski jezik

Programski jezik je jezik za pisanje programa koje računalo zna i može izvoditi. Jedan od najpoznatijih jezika na kojem se zasnivaju mnogi drugi jezici je C. C je razvijen u ranim 70-im godinama 20. stoljeća. On spada u proceduralne programske jezike i za njega je definiran ISO standard.

http://hr.wikipedia.org/wiki/C_(programski_jezik)

Java programski jezik

Programski jezik je jezik za pisanje programa koje računalo zna i može izvoditi . Java je objektno orijentirani programski jezik objabljen 1995. Za razliku od drugih programskih jezika, Java programi se izvode u virtualnom okruženju (JVM).

http://hr.wikipedia.org/wiki/Java_(programski_jezik)

Python programski jezik

Programski jezik je jezik za pisanje programa koje računalo zna i može izvoditi. Python je progrsamki jezik visoke razine čiji je cilj stvaranje čitljivog koda. To je objektno orijentirani, imperativni i funkcionalni programski jezik.

http://hr.wikipedia.org/wiki/Python

XML

XML je kratica za Extensible Markup Language, odnosno jezik za označavanje podataka. Ako na primjer želimo neke podatke zapisati u neku tablicu, s ovim je jezikom lakše možemo napraviti. Konkretno bi se tablica mogla napravit i sa drugim alatima, ali bi njen kapacitet bio puno veći i takva tablica bi se mogla otvoriti samo s tim alatom.

http://hr.wikipedia.org/wiki/XML

HTML

HTML je kratica za HyperText Markup Language, odnosno prezentacijski jezik za izradu web stranica. XML je sličan ovom jetiku. Korisnik HTML jezikom oblikuje izgled web stranice ili programskog sučelja koji se otvara web preglednikom (npr. Autopsy).

http://hr.wikipedia.org/wiki/HTML

Windows registar

Registar je baza podataka u sustavu Windows, u kojoj su pohranjene važne informacije o sklopovlju, instaliranim programima te raznim postavkama.

http://windows.microsoft.com/hr-hr/windows-vista/What-is-the-registry

NTFS

New Technology File System je datotečni sustav namijenjen Windows NT sustavima (XP, Vista, 7, 8). NTFS je za razliku od svog prethodnika (FAT) uveo mogućnost ograničavanja pristupa pojedinima mapama te njihovom šifriranju. Podaci o svim datotekama u NTFS sustavu se čuvaju u MFT (Master File Table) tablici.

http://www.informatika.buzdo.com/s345.htm

FAT

File Allocation Table je datotečni sustav razvijen 70-ih godina 20. stoljeća. Zbog svoje jednostavnosti implementacije brzo se proširio te je danas standard za prijenosne memorijske uređaje. FAT je univerzalni datotečni sustav, što znači da ga prepoznaju svi značajniji operacijski sustavi. FAT se zbog svojih ograničenih svojstava ne koristi u sustavima većeg kapaciteta.

http://www.informatika.buzdo.com/s345.htm

HFS+

Hjerarhijski Datotečni Sustav (Hierarchical File System, HFS+) je datotečni sustav kojeg je razvio Apple te se primarno koristi na Machintosh računalima, odnosno uređajima koja koriste Mac OS.

http://en.wikipedia.org/wiki/HFS_Plus

ISO 9660

ISO 9660, poznatiji pod nazivom CDFS (Compact Disc File System), je datotečni sustav za optičke medije (CD,DVD i ostale). Razvijen je od High Sierra Format (HSF) datotečnog sustava koji je načinom rada vrlo sličan FATu i UNUXu. Sustav se sastoj od 24 oktetnih *frame*-ova (okvira), a oni su organizirani u sektor, npr. kod CDa, sektor ima 98 okvira.

http://en.wikipedia.org/wiki/ISO_9660

Ext2, 3 i 4

Ext ili Extended file system (Prošireni datotečni sustav) je datotečni sustav koji se koristi u Linux operacijskom sustavu. Razvijen je 1992. godine po uzoru na UNIX datotečni sustav.

http://en.wikipedia.org/wiki/Extended_file_system

UFS1 i 2

UFS, odnosno UNIX-ov datotečni sustav, je još poznat i pod nazivom Fast File System (FFS). Razvoj ovog datotečnog sustava je tekao zajedno s razvojem UNIX operacijskog sustava.

http://en.wikipedia.org/wiki/Unix_File_System

FFS

Vidi **UFS1 i 2**.

NSRL

National Software Reference Library (Nacionalna programski referentna biblioteka) je američka organizacija koja promovira učikovito korištenje računalne tehnologije u istraživanju računalnih kriminalnih radnji.

http://www.nsrl.nist.gov/

Hashkeeper

Program za izradu baza podataka prilikom forenzičke analize. Koristeći MD5 datotečne algoritme, proračuna hash vrijednosti (numerične vrjednosti datoteke) i otkriva je li datoteka zlonamjerna.

http://en.wikipedia.org/wiki/HashKeeper

Md5sum/sha1sum

Algoritmi koji rade numerički sažetak datoteke. To se koristi kako bi se provijerila autentičnost datoteke, na prijmjer riječ ,,abc“ ima md5 hash vrijednost : 900150983cd24fb0d6963f7d28e17f72 , a riječ ,,abd“ ima : 4911e516e5aa21d327512e0c8b197616.

http://en.wikipedia.org/wiki/Md5sum

http://en.wikipedia.org/wiki/Sha1sum

Ako želite provijerit hash i za ostale riječi:

http://www.md5.cz/

Metapodatak

Metapodaci su podaci o podacima, odnosno oni opisuju karakteristike neke datoteke (nekog podatka). Na primjer kada netko napiše neki dokument, u meta podatke će se spremiti virjeme kada je napisan, ime autora ili inicijali i ostale naznake.

http://hr.wikipedia.org/wiki/Metapodatci

SQLite

SQLite je program za baratanje bazama podataka. Primjenjuje se za web stranice, za aplikacijske podatke ili neke popise na samom mediju za pohranu.

http://hr.wikipedia.org/wiki/SQLite

8. Reference

[1] The Sleuth Kit projekt, http://www.sleuthkit.org/proj.php , srpanj 2012.

[2] The Sleuth Kit, http://www.forensicswiki.org/wiki/The_Sleuth_Kit , srpanj 2012.

[3] System forensics, The Sleuth Kit Part 1 i 2 http://www.sysforensics.org/2012/02/sleuth-kit-part-1-information.html, srpanj 2012.

[4] Brian Carrier: The Sleuth Kit Overview and Automated Scanning Features, http://www.basistech.com/conference/2010/osdf-slides/carrier-sleuthkitoverview.pdf, lipanj 2010.

[5] Slobodan Uzon: Slobabgd tutorijali - Digitalne antiforenzičke tehnike, http://slobabgd.webs.com/Tutorijali/Digitalne%20antiforenzicke%20tehnike.htm , srpanj 2012.

[6] Slobodan Uzon: Slobabgd tutorijali - Uvod u kompjutersku forenziku, http://slobabgd.webs.com/Tutorijali/Uvod%20u%20kompjutersku%20forenziku.htm , srpanj 2012.

[7] Anthony Dowling: Digital Forensics: A Demostration of the Effectiveness of The Sleuth Kit and Autopsy Forensic Browser, http://otago.ourarchive.ac.nz/bitstream/handle/10523/378/ADowlingThesisDigitalForensics.pdf?sequence=1https://diuf.unifr.ch/drupal/tns/sites/diuf.unifr.ch.drupal.tns/files/cmarko-tskintro.pdf , srpanj 2012.

[8] Marina Marčeta: Digitalna forenzika slika http://os2.zemris.fer.hr/ostalo/2010_marceta/Diplomski.htm , travanj 2010.