HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Osnove računalne forenzičke analize

CCERT-PUBDOC-2006-11-174

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Računalna forenzička analiza (RFA) je postupak utvrđivanja činjenica nad digitalnim medijima primjenom različitih metoda. Najčešće se koristi u postupcima sudskog dokazivanja, a sastoji se od niza analitičkih metoda za otkrivanje, prikupljanje, ispitivanje i skladištenje podataka, te često podrazumijeva ispitivanje računalnih sustava kako bi se utvrdilo njihovo korištenje u ilegalnim ili neautoriziranim aktivnostima poput krađe poslovnih tajni, uništavanja intelektualnog vlasništva ili prijevare.

Postupci RFA u mnogo čemu se razlikuju od postupaka klasične forenzičke analize. Kod klasične istrage dovoljno je osigurati mjesto zločina kako bi se zaštitili dokazi, za koje se kaže da se pokoravaju tzv. *„Dead Body"* teoremu (*„It's not going anywhere!"*). Čak i kada su dokazi na neki način ugroženi, moguće ih je zaštititi brzo i bez posebnih znanja, primjerice prekrivanjem otisaka obuće na tlu u slučaju kiše. Kod RFA, situacija je daleko zamršenija. Samo za utvrđivanje prisutnosti dokaza potrebno je provesti sveobuhvatnu analizu sustava, jer na računalu nema rupa od metaka ili mrlja krvi koje bi ukazale na zločin. Digitalni dokazi su ujedno i mnogo ranjiviji od fizičkih pa je vještom napadaču puno lakše ukloniti tragove svoga djelovanja, a nepažljivo ili nestručno provođenje istrage također može rezultirati gubitkom ključnih podataka.

U nastavku teksta kronološkim redoslijedom navedene su i ukratko opisane mogućnosti RFA. Započinje se s razradom postupaka RFA, a zatim slijedi opis postupaka prikupljanja dokaza, s naglaskom na prikupljanje osjetljivih dokaza i kratkim pregledom programskih alata, te metoda analize prikupljenih materijala. Opis postupaka dokumentiranja RFA, koje se provodi tijekom cjelokupnog postupka, raspoloživ je na kraju dokumenta.

2. Izrada postupka računalne forenzičke analize

RFA je zahtjevno područje djelatnosti koje iziskuje posebno obučeno osoblje, razrađenu logističku podršku i značajna financijska sredstva, a sve sa ciljem zadržavanja pravne vjerodostojnosti prikupljenih dokaza. Zbog toga je potrebno detaljno razraditi odgovarajuće postupke RFA.

2.1. Određivanje ciljeva RFA

Razvoj načela rada i postupaka je važan korak u stvaranju tima za RFA. Ovo je moguće učinkovito učiniti određivanjem ciljeva RFA koji obuhvaćaju osnovne funkcije tima bez obzira radilo se o istraživanju zločina na području visoke tehnologije, prikupljanju dokaza ili forenzičkoj analizi.

2.2. Ljudski resursi potrebni za provođenje RFA

Prilikom razrade postupaka RFA potrebno je posvetiti pažnju pitanjima vezanim uz ljudske resurse, kao što su: opis posla, potrebna stručna sprema, radno vrijeme, dežurstva te hijerarhija i struktura tima za provođenje RFA.
Zbog dinamike ovog područja potrebno je neprestano održavati razinu stručnosti članova tima stalnim usavršavanjem djelatnika ili zapošljavanjem novih stručnjaka određenog profila.

2.3. Administrativne pripreme

Osnivanje i djelovanje tima za RFA zahtjeva znatna sredstva, a mnogi od potrebnih izdataka su periodički te je sredstva potrebno osiguravati na godišnjoj osnovi. Potrebno je osigurati radni prostor, opremu, programsku podršku s nužnim nadogradnjama te stalno školovanje osoblja. Korištena programska podrška obično treba biti licencirana, bilo na ime agencije ili članova tima koji ju koriste.

2.4. Zahtjevi za provedbom RFA te prihvaćanje dokaza

Potrebno je izraditi smjernice za predavanje zahtjeva za provedbom RFA te smjernice za prihvaćanje dokaza ako je takav zahtjev uvažen. Ove smjernice se odnose na: formulare sa zahtjevima, načine na koje se zahtjevi predaju, dokumentaciju koju treba priložiti zahtjevu, kriterije prihvaćanja zahtjeva i fizičkih dokaza.

2.5. Upravljanje slučajem

Jednom kada je zahtjev za provedbom RFA uvažen, potrebno je utvrditi kriterije za određivanje prioriteta pojedinih ispitivanja. Takvi se kriteriji mogu odnositi na vrstu zločina, rokove vezane uz sudski proces, potencijalne žrtve, pravna pitanja, postojanost dokaza i raspoloživa sredstva.

2.6. Određivanje postupaka rukovanja dokazima

Potrebno je izraditi smjernice za primanje, obradu, dokumentiranje i rukovanje dokazima i ostalim materijalima povezanim s istragom. Za prihvaćanje dokaza s ilegalnim sadržajima, npr. dječjom pornografijom, mogu biti potrebni posebni nalozi.
Druge forenzičke discipline mogu pronaći dodatne dokaze, kao što su otisci prstiju na kućištu tvrdog diska, vlasi ili vlakna unutar tipkovnice te rukom pisane oznake ili tiskani materijali. Zbog toga je potrebno izraditi postupke za određivanje redoslijeda kojim će se vršiti ispitivanja, kako ne bi došlo do uništavanja dokaza.
Sve tehničke postupke prikupljanja dokaza potrebno je ispitati kako bi se utvrdila njihova ponovljivost i valjanost dobivenih rezultata. Koraci razvoja i ispitivanja ovakvih postupaka trebaju biti dokumentirani i sadržavati:

- određivanje zadatka ili problema,
- prijedlog mogućih rješenja,
- ispitivanje svakog rješenja na poznatom uzorku,
- ocjenjivanje rezultata ispitivanja i
- oblikovanje postupka.

Uz prethodno navedeno, veoma je važno da se izvorni dokazi nikada ne koriste u procedurama testiranja postupaka.

3. Prikupljanje podataka i dokaza

Prikupljanje podataka i dokaza najosjetljiviji je korak RFA. Eventualne pogreške u ovom stupnju mogu značiti nepovratan gubitak dokaza, bilo zbog njihova oštećivanja ili zbog gubitka njihove vjerodostojnosti uslijed neprimjerenih metoda prikupljanja. Zbog toga je potrebno pažljivo isplanirati postupak prikupljanja dokaza, s posebnim naglaskom na ranjive dokaze, te koristiti odgovarajuće programske alate.

3.1. Procjena dokaza

Prije prikupljanja dokaza potrebno je izvršiti temeljitu procjenu danog slučaja i na temelju toga odrediti smjer daljnjeg djelovanja. U okvir takve procjene ulaze nalog za pretraživanje, detalji slučaja, vrsta ispitivanog sklopovlja i programske podrške, potencijalni dokazi koje se traži te uvjeti njihovog prikupljanja.

U razgovoru s voditeljem istrage potrebno je razmotriti:

- primjenu ostalih forenzičkih postupaka nad dokazima (DNA analiza, prikupljanje otisaka prstiju, traženje tragova mehaničke obrade i sl.),
- važnost opreme pronađene uz računalo (npr. kreditne kartice, skeneri, pisači ili digitalne kamere),
- ostale smjerove istrage (npr. traženje podataka od pružatelja Internet usluga, pronalaženje udaljenih spremišta podataka ili poruka elektroničke pošte),
- vrstu potencijalnih dokaza (fotografije, tablice, dokumenti, baze podataka, financijski podaci),
- ostale informacije vezane uz slučaj (korisnička imena, zaporke, računi elektroničke pošte, mrežne postavke, dnevnički zapisi) koje je možda moguće dobiti u razgovoru s administratorima, korisnicima ili zaposlenicima, te
- razinu informatičkog znanja korisnika čije se djelovanje ispituje.

Po dolasku na mjesto potencijalnog zločina potrebno je utvrditi:

- broj i vrste računala,
- prisutnost računalne mreže,
- vrstu i količinu medija za pohranu podataka te dokumentirati gdje su pronađeni,
- postojanje udaljenih spremišta podataka i/ili udaljenih računala,
- korištene komercijalne programske pakete,
- o kojim se operacijskim sustavima radi, te
- intervjuirati sistemske administratore i korisnike.

Prilikom skladištenja pronađenih dokaza potrebno je osigurati njihovu zaštitu od elektromagnetskih smetnji. Stalni izvori napajanja mogu biti potrebni ukoliko se radi o uređajima s baterijskim napajanjem.

3.2. Ranjivost dokaza

Digitalni dokazi su mnogo ranjiviji od konvencionalnih fizičkih dokaza i zbog toga se prilikom rukovanja potrebno pridržavati određenih smjernica kako ih se ne bi uništilo ili oštetilo.

Prvi korak u traženju dokaza na računalu često je njegovo gašenje i transport u laboratorij radi provođenja temeljite analize. Svi podaci nastali tijekom rada računala, koji nisu pohranjeni na tvrdi disk, time su nepovratno izgubljeni.

Ostavljanje računala uključenim ipak ne jamči očuvanje dokaza. Ako je računalo povezano na računalnu mrežu, napadač može s udaljene lokacije izbrisati dnevničke zapise ili, neovisno o vezi na mrežu, programirati njihovo automatsko brisanje. Jednako tako, dobronamjeran korisnik radom na računalu može nesvjesno uzrokovati prepisivanje dokaza.

Uništenje nije jedina opasnost koja prijeti digitalnim dokazima. Nestručnim rukovanjem oni mogu biti oštećeni i tako obezvrijeđeni u potencijalnom sudskom postupku. Ovo se najčešće događa zbog

neinformiranosti korisnika koji, nakon što su uočili zločin, pokušavaju otkriti što se točno dogodilo, te tako utječu na sustav.
Glavne vrste ranjivih dokaza su:

- prijelazni podaci – oni koji se gube gašenjem računala i tu se ubrajaju aktivne mrežne veze ili aplikacije koje se izvode u radnoj memoriji,
- ranjivi podaci – iako pohranjeni na tvrdom disku, lako su izmjenjivi (primjer ovakvih dokaza su vremenske oznake posljednjeg pristupa datoteci ili direktoriju),
- privremeni podaci – podaci koji su pohranjeni na tvrdom disku, a moguće im je pristupiti samo u određenim vremenskim intervalima (primjer su datoteke kriptiranih datotečnih sustava).

Kako bi se ranjivi dokazi očuvali potrebno ih je što prije pohraniti na siguran medij. Tvrdi disk ispitivanog računala nije prikladan za to jer i sam može sadržavati dokaze koji bi na ovaj način mogli biti uništeni ili oštećeni. Prilikom pohrane ranjivih dokaza potrebno je koristiti što manje radne memorije kako bi se očuvao njezin sadržaj.
Diskete su dobar izbor za pohranu ranjivih dokaza zbog svoje raširenosti, niske cijene i jer ih je lako zaštititi od pisanja. Glavni im je nedostatak maleni kapacitet. Umetanje tvrdog diska u ispitivano računalo nije prihvatljivo jer zahtjeva njegovo gašenje. Ne preporuča se niti korištenje USB ili Firewire prijenosnih medija jer se njihovim spajanjem mijenja stanje ispitivanog sustava.
Najbolji način za prikupljanje ranjivih dokaza je uporaba računalne mreže. Kako bi se ispitivano računalo zaštitilo od daljnjih napada i kako bi se prikrila istraga, računalo je po otkriću napada potrebno isključiti s mreže. Njegovim spajanjem na privatno čvorište (eng. *hub*) omogućuje se prijenos podataka. Pri tome drugo računalo, korišteno za prikupljanje dokaza, treba prilagoditi mrežnim postavkama ispitivanog računala.
Prije svega je potrebno dohvatiti i pohraniti sadržaj radne memorije ispitivanog računala i to u manjim paketima kako bi se izbjeglo prepisivanje ostatka radne memorije. Nakon što je sadržaj radne memorije pohranjen može se pristupiti dohvaćanju ostalih podataka, bez ograničenja na veličinu paketa.

3.3. Alati za prikupljanje ranjivih dokaza

Alat za prikupljanje ranjivih dokaza mora zadovoljavati sljedeće kriterije:

1. Forenzički integritet ispitivanog sustava mora biti očuvan. To znači da na takvom sustavu nije dozvoljeno spremanje podataka niti izvođenje aplikacija.
2. Alat autonomno izvodi cjelokupno rukovanje dokazima, bez interakcije korisnika. Ovo je potrebno kako bi se dokazi osigurali od nestručnog rukovanja. Time se ujedno osigurava i vjerodostojnost prikupljenih dokaza jer ih korisnik ne može mijenjati.
3. Alat sakuplja samo dokaze koji bi mogli biti oštećeni ili izgubljeni tijekom ispitivanja sustava ili njegova transporta.
4. Alat izvještava korisnika o otkrivenim tragovima napada. Rezultat razumljiv korisniku potaći će ga na korištenje alata.

Primjer ovakvog alata je FRED (eng. *First Responder's Evidence Disk*) koga je razvila organizacija AFOSI (eng. *Air Force Office of Special Investigations*). Ovo je jednostavan i malen programski paket namijenjen pokretanju s diskete. Glavni zadatak FRED paketa je prikupljanje podataka potrebnih za otkrivanje napada, on bilježi osnovne sistemske veličine (npr. vrijeme i datum), mrežne veze, aktivne procese, aktivne DLL datoteke, otvorene priključke (eng. *port*) i MD5 (eng. *Message-Digest algorithm 5*) vrijednosti važnijih sistemskih datoteka.

3.4. Logičko i fizičko dohvaćanje podataka s diska

Fizičko dohvaćanje podataka podrazumijeva dohvaćanje podataka na fizičkoj razini, bez obzira na datotečni sustav. Logičko dohvaćanje se odnosi na dohvaćanje podataka u ovisnosti o instaliranom operacijskom sustavu, o datotečnom sustavu i/ili prisutnim aplikacijama.
Fizičko dohvaćanje podataka obuhvaća sljedeće metode:

- ispitivanje particijske strukture (koristi se za identifikaciju prisutnih datotečnih sustava te određivanje veličine i sadržaja nezauzetog diskovnog prostora) i

- traženje znakovnih nizova na fizičkom disku, čime se mogu pronaći podaci nevidljivi operacijskom i datotečnom sustavu.

Mogući koraci logičkog dohvaćanja podataka su:

- dohvaćanje podataka o datotečnom sustavu kao što su struktura direktorija, imena, svojstva, veličine i položaji datoteka te vremenske oznake,
- eliminacija poznatih datoteka iz RFA na temelju identifikacijskih brojeva (eng. *hash value*),
- identificiranje datoteka značajnih za RFA na temelju njihova imena, veličine, zaglavlja, sadržaja ili položaja na disku,
- obnavljanje izbrisanih datoteka,
- dohvaćanje komprimiranih, kriptiranih i zaporkama zaštićenih podataka,
- dohvaćanje neiskorištenog prostora iza kraja datoteka (eng. *file slack*),
- dohvaćanje nezauzetog diskovnog prostora.

3.5. Prikupljanje dokaza na Linux operacijskim sustavima

RFA analizu Linux operacijskih sustava moguće je provoditi alatima ugrađenim u operacijski sustav ili specijaliziranim aplikacijama.

3.5.1. Ispitivanje radne memorije

Prvi korak u ispitivanju radne memorije je pohrana njenog sadržaja (eng. *dump*) na neki trajni medij. Kako bi se smanjio utjecaj na ispitivano računalo pohranu je potrebno načiniti korištenjem samo jedne naredbe. Pritom sliku radne memorije nije uputno pohraniti na tvrdi disk ispitivanog računala. Sliku radne memorije moguće je dohvatiti pomoću *dd* naredbe, koja podatke kopira bit po bit, te ju je potom moguće korištenjem *netcat* alata spremiti na udaljeno računalo.

Kod Linux operacijskih sustava radnu memoriju je moguće spremiti u dvije datoteke: `/dev/mem` i `/proc/kcore`. Slika radne memorije se u `/proc/kcore` datoteku sprema u „*ELF core*" formatu što ju čini pogodnom za analizu *gdb* alatom, ali je pri tome slika nešto veća od same radne memorije zbog *ELF* zaglavlja.

Radnu memoriju je moguće spremiti sljedećom naredbom:

```
#mnt/cdrom/dd if=/dev/mem | /mnt/cdrom/nc <IP adresa> <broj porta>
```

Nakon toga moguće je pristupiti pretraživanju spremljene slike radne memorije u potrazi za tragovima digitalnog zločina. Pri tome je nužno dobro poznavanje strukture radne memorije kod Linux operacijskih sustava.

3.5.2. Ispitivanje sadržaja diska

Linux operacijski sustavi imaju ugrađene brojne alate korisne u ispitivanju sadržaja diska. Neki od njih su:

- *dd* – naredba za kopiranje podataka iz jedne datoteke ili uređaja u drugu datoteku ili uređaj,
- *sfdisk* i *fdisk* – naredbe za određivanje strukture diska,
- *grep* – naredba za traženje izraza ili uzoraka u jednoj ili više datoteka,
- *loop device* – omogućuje dohvaćanje (eng. *mount*) slike diska bez snimanja na tvrdi disk,
- *md5sum* i *sha1sum* – omogućavaju stvaranje MD5 ili SHA (eng. *Secure Hash Algorithm*) sigurnosnih suma datoteka ili lista datoteka,
- *file* – čitanjem zaglavlja datoteke određuje njezin tip, bez obzira na ime,
- *xxd* – preglednik binarnih datoteka,
- *ghex* i *khexedit* – preglednici binarnih datoteka namijenjeni *Gnome* i *KDE* grafičkim okruženjima.

Značajan je korak svake RFA analize utvrđivanje vjerodostojnosti prikupljenih podataka. To omogućuju naredbe *md5sum* i *sha1sum* koje za svaku datoteku ili disk stvaraju jedinstven digitalni potpis.

Naredba *dd* stvara točnu kopiju zapisa na fizičkom uređaju s nerezerviranim prostorom i neiskorištenim prostorom iza kraja datoteka. Za razliku od drugih sličnih alata *dd* u stvorenu sliku ne

zapisuje dodatne podatke što ima višestruke prednosti sa stajališta RFA. Pretraživanjem nerezerviranog prostora unutar slike ispitivanog diska pomoću *grep* naredbe moguće je pronaći fragmente teksta ili cijele izbrisane dokumente.
Kombiniranjem naredbe *dd* s naredbom *split*, sliku ispitivanog diska moguće je razložiti na dijelove proizvoljne veličine. To može biti korisno ukoliko sliku treba pohraniti na više CD ili DVD medija ili ako je potrebno ograničiti njezinu veličinu zbog specifičnosti alata korištenih za analizu.
Ako je sadržaj ispitivanog tvrdog diska s više particija pohranjen unutar jedne slike može se javiti i potreba za stvaranjem pojedinačne slike za svaku particiju. Izdvajanjem pojedinih particija olakšava se njihovo pregledavanje, jer je moguće koristiti *loop device* alate.
Prije obnavljanja slike ispitivanog diska potrebno je „očistiti" odredišni disk kako ostaci starih podataka ne bi otežali potragu za dokazima. Čišćenje je moguće izvesti prepisivanjem cijelog diska nulama. Provjeru uspješnog prepisivanja moguće je obaviti naredbom *xxd* s „*autoskip*" parametrom.
Pored spomenutih alata namijenjenih tekstualnom korisničkom sučelju postoji niz grafičkih alata koji RFA čine bržom i jednostavnijom. Dva takva alata su opisana u nastavku.

3.5.3. *Autopsy*

Autopsy programski paket je HTML korisničko sučelje programskog paketa *Sleuthkit* koji predstavlja skup forenzičkih alata namijenjenih tekstualnom korisničkom sučelju. Naredbe *Sleuthkit* paketa su organizirane u slojevima:

1. Sloj datotečnog sustava
   - *fsstat* – vraća statističke podatke o datotečnom sustavu smještenom na disku ili unutar slike diska
2. Sloj imena datoteka
   - *fls* – prikazuje rezervirana i nerezervirana imena datoteka unutar datotečnog sustava
   - *ffind* – traži datotečna imena povezana s određenim metazapisom
3. Podatkovni sloj
   - *dcalc* – koristi se za provedbu RPN (eng. *Reverse Polish Notation*) proračuna
   - *dcat* – omogućuje prikaz bloka podataka iz slike diska
   - *dls* – prikazuje blokove podataka unutar datotečnog sustava
   - *dstat* – jedinstvena zamjena *vmstat*, *iostat* i *ifstat* alata
4. Sloj metapodataka
   - *icat* – omogućuje dohvaćanje blokova podataka iz „*inode*" strukture
   - *ils* – prikazuje sve metazapise
   - *ifind* – omogućuje pretraživanje metazapisa
   - *istat* – vraća statističke podatke o „*inode*" strukturi

Autopsy grafičko korisničko sučelje omogućuje jednostavan pristup funkcionalnostima *Sleuthkit* programskog paketa te organiziranje podataka u „slučajeve".

3.5.4. *SMART for Linux*

SMART je komercijalni programski paket s grafičkim korisničkim sučeljem koji automatski obrađuje slike ispitivanih diskova. Neke od mogućnosti ovog paketa su:

- otkrivanje tragova ilegalnog djelovanja (tzv. „*Knock-and-talk*" istrage),
- izravan ili udaljen pristup i pregled računala,
- analiza neispravnog računala (tzv. „*post mortem*" analiza),
- testiranje i vrednovanje drugih forenzičkih alata,
- pretvorba vlasničkih (eng. *proprietary*) formata za spremanje dokaza i
- usporedbena, tzv. „*baseline*" analiza performansi računalnog sustava.

3.6. Prikupljanje dokaza na Windows operacijskim sustavima

Windows operacijski sustavi najčešće su korišteni operacijski sustavi među korisnicima. Stoga je u nastavku ovog poglavlja analizirana rekonstrukcija obrisanih datoteka te korištenje *Windows Forensics Toolchest* besplatnog alata.

3.6.1. Rekonstrukcija sadržaja „*Recycle Bin*“ direktorija

Brisanjem datoteka one nisu nepovratno izgubljene već se spremaju u „*Recycle Bin*“ direktorij kako bi se umanjile posljedice slučajnog brisanja. Pri tome nastaje INFO2 datoteka s podacima potrebnim za obnavljanje izbrisanih datoteka od kojih neki mogu biti značajni za RFA.

Datotekama premještenim u „*Recycle Bin*“ direktorij ime se mijenja u oblik „*DC#.EXT*“, gdje je # cjelobrojna jedinstvena oznaka izbrisane datoteke, a *EXT* izvorni format izbrisane datoteke, npr. brisanjem datoteke „*DATOTEKA.TXT*“ ona može u „*Recycle Bin*“ direktoriju biti spremljena kao „*DC4.TXT*“. Brisanjem sadržaja spomenutog direktorija briše se i sadržaj INFO2 datoteke te se brojač pobrisanih datoteka (#) postavlja u početno stanje.

U INFO2 datoteku zapisuju se sljedeći podaci o svakoj izbrisanoj datoteci:

- puno ime izvorne datoteke (s položajem u datotečnom sustavu) u ASCII i UNICODE formatu,
- oznaka diska s kojeg je datoteka izbrisana (0x00 za „A:“ disk, 0x01 za „B:“ disk itd.),
- fizička veličina,
- datum i vrijeme brisanja i
- identifikacijski broj.

Analizu obrisanih datoteka moguće je automatizirati korištenjem nekog od specijaliziranih alata, kakav je npr. *Rifiuti* programski paket otvorenog koda.

3.6.2. *Windows Forensics Toolchest*

Ako se područje potrage za dokazima želi proširiti izvan „*Recycle Bin*“ direktorija potrebno je koristiti neki od alata koji to omogućuju. Jedan od njih je *Windows Forensics Toolchest* (WFT) besplatni programski paket koji omogućuje automatsko prikupljanje dokaza, a financiran je dobrovoljnim donacijama korisnika.

WFT predstavlja forenzički unaprijeđenu ljusku za automatsko pokretanje sigurnosnih alata (eng. *batch processing shell*) s mogućnošću stvaranja izvještaja u HTML formatu. Uz pravilnu uporabu i u kombinaciji s odgovarajućim sigurnosnim alatima, ovaj paket omogućuje otkrivanje sigurnosnih incidenata te stvara izvještaj prikladan za uporabu tijekom sudskog procesa. WFT bilježi sve svoje aktivnosti tijekom traženja dokaza i kontinuirano proračunava MD5 kontrolne zbrojeve, čime se osigurava vjerodostojnost njegovih izvještaja.

Tijekom izvođenja sam WFT paket minimalno opterećuje ispitivani sustav: koristi dio radne memorije te čita nekoliko registara. Alati koje WFT poziva nisu nužno tako nezahtjevni pa je potreban pažljiv izbor postavki postupka traženja dokaza.

Kako bi se osigurao forenzički integritet prikupljenih dokaza, potrebno je WFT pokretati sa CD ili USB diska na kojemu se, pored ovog paketa, nalaze kopije alata koje koristi u radu te sigurna kopija „*cmd.exe*“ datoteke, i to inačice jednake onoj na ispitivanom računalu. Konfiguracijska datoteka WFT alata mora sadržavati MD5 sigurnosne zbrojeve svih datoteka korištenih tijekom traženja dokaza.

Tijekom ispitivanja računala u HTML izvještaj se, posebno za svaki od korištenih sigurnosnih alata, bilježi opis alata, MD5 sigurnosni zbroj pokrenute datoteke, korištene naredbe te rezultat i uz njega vezan MD5 sigurnosni zbroj.

3.7. *Helix*

Helix je distribucija *Knoppix* operacijskog sustava prilagođena primjeni u računalnoj forenzici. Kao i sve ostale distribucije *Knoppix* operacijskog sustava, *Helix* je moguće pokrenuti sa CDa, bez instalacije. Neke od ključnih prilagodbi ovog operacijskog sustava primjenama u RFA su:

- *Helix* nikada ne koristi tzv. „*swap*“ prostor,
- *Automount* alat automatski dohvaća sve diskove koje pronađe, ali tako da sve točke dohvaćanja (eng. *mount point*) stvara s parametrima: *ro*, *noatime*, *noexec*, *nodev*, *noauto* i *user*,
- *Helix*, pored datotečnih sustava kojim *Knoppix* ima pristup (*ext2*, *ext3*, *vfat*, *ntfs*), može pristupati *xfs*, *resier*, *jfs* te brojnim drugim datotečnim sustavima,
- u *Helix* su ugrađeni svi dostupni alati otvorenog koda namijenjeni RFA,
- dodana je „*Knock and Talks*“ mogućnost koja omogućuje brzo pretraživanje sustava za potencijalno ilegalnim grafičkim materijalima,

- sadrži okruženje namijenjeno Windows operacijskim sustavima,
- prekrivajući datotečni sustav omogućuje pisanje na CD,
- nadogradnje se izdaju ne rjeđe od svaka tri mjeseca, itd.

Helix podržava dva načina rada. U Windows načinu rada predstavlja standardnu Windows aplikaciju za prikupljanje forenzičkih dokaza bez gašenja računala čime je omogućeno prikupljanje podataka koji bi gašenjem bili izgubljeni, te analiziranje poslužitelja i drugih sustava koje nije dopušteno gasiti. Windows način rada omogućuje pokretanje brojnih forenzičkih alata sa CDa. Ove aplikacije su statičke što znači da tijekom izvođenja ne koriste dodatne programske biblioteke ili datoteke. Time je uklonjena potreba za korištenjem nepouzdanih sistemskih alata ili programskih paketa ispitivanog računala. Ipak, zbog potrebe za pokretanjem pod različitim inačicama Windows operacijskih sustava, koriste se DLL datoteke operacijskog sustava ispitivanog računala.
U Helix sučelje ugrađeni su, među ostalima, i slijedeći alati za analizu Windows operacijskih sustava:

- *George Garners Forensic Acquisition Utility*,
- *Sysinternal* ,
- *Foundstone*,
- *Windows Debugger* i
- *Windows Forensic Toolchest*.

U Linux načinu rada, *Helix* je operacijski sustav pokretan sa CDa koji diskovima ispitivanog računala pristupa isključivo uz ovlasti čitanja.

4. Analiza dokaznih materijala

Poželjno je analizu dokaznih materijala provesti u kontroliranim uvjetima kakve pruža forenzički laboratorij ili neki drugi radni prostor takve namjene. Ako objektivne okolnosti nameću potrebu analize dokaza na mjestu pronalaska, prije pristupanja analizi, treba razmotriti vrijeme, materijalna sredstva i osoblje potrebno za takvu analizu te utjecaj na poslovanje ustanove u kojoj se provodi istraga. Kada je to moguće, analizu je potrebno provoditi nad kopijama dokaza kako bi se izbjeglo nenamjerno oštećivanje originala.
Redoslijed ispitivanja dokaza može se utvrditi prema mjestu pronalaska ili stabilnosti medija na kojima su pohranjeni. Pri tome u obzir treba uzeti posljedice koje su na dokazima mogli ostaviti pakiranje, transport ili skladištenje.
U nastavku su navedene četiri skupine metoda analize prikupljenih dokaza. Rezultati svake od navedenih analiza sami za sebe ne moraju otkrivati puno i zbog toga ih je, u kontekstu istrage, potrebno sagledati kao cjelinu.

4.1. Analiza vremenskog slijeda

Analizom vremenskog slijeda utvrđuje se redoslijed događaja na ispitivanom računalnom sustavu te se time oni povezuju s korisnicima. Ovu analizu moguće je provesti na dva načina. Prvi način se odnosi na analizu metapodataka datotečnog sustava u kojima su zabilježena slijedeće oznake vremena:

- vrijeme stvaranja datoteka,
- vrijeme njihove posljednje promjene, te
- vrijeme posljednjeg pristupa i promjene statusa.

Druga metoda je analiza sistemskih dnevničkih zapisa koji mogu obuhvaćati zapise pogrešaka, instalacijske, mrežne, sigurnosne ili neke druge zapise.

4.2. Pronalaženje skrivenih podataka

Moguće je primijeniti nekoliko metoda za traženje skrivenih podataka:

- usporedbom zaglavlja datoteka i njihovih nastavaka moguće je otkriti nepodudaranja koja ukazuju na prikrivanje podataka,
- podatke je moguće prikriti kriptiranjem, komprimiranjem ili zaštitom zaporkama, pri čemu za RFA korištene zaporke mogu biti jednako značajne kao sadržaj datoteka koje štite,
- pohrana podataka u HPA (eng. *Host-Protected Area*) također može ukazivati na pokušaj njihova prikrivanja.

4.3. Analiza aplikacija i datoteka

Analizom aplikacija i datoteka prisutnih na računalu moguće je utvrditi njegove performanse te razinu informatičkog znanja korisnika. Takva saznanja mogu zatim ukazati na potrebu za dodatnim koracima RFA. Neki od primjera analize aplikacija i datoteka su:

- uočavanje uzoraka u imenima datoteka,
- pretraživanje sadržaja datoteka,
- utvrđivanje broja i vrste prisutnih operacijskih sustava,
- utvrđivanje veza među datotekama i instaliranim aplikacijama,
- identificiranje nepoznatih vrsta datoteka i utvrđivanje njihove važnosti za RFA,
- utvrđivanje odnosa među datotekama, npr. povezivanje zapisa aktivnosti na Internetu s priručnim (eng. *cache*) datotekama ili povezivanje poruka elektroničke pošte s njihovim prilozima,
- ispitivanje korisničkih postavki,
- analiza metapodataka, npr. za tekstualni dokument to mogu biti podaci o autoru, vrijeme posljednje izmjene, broj izmjena te podaci o ispisu ili spremanju, itd.

4.4. Analiza vlasništva nad datotekama

Identificiranje korisnika koji je stvorio, izmijenio ili pristupio određenoj datoteci može biti ključno za istragu. To je moguće učiniti nekom od slijedećih metoda, koje pripadaju i prethodno navedenim skupinama:

- utvrđivanje točnog vremena kada je korisnik imao pristup računalu može omogućiti utvrđivanje vlasništva nad datotekama (analiza vremenskog slijeda),
- smještaj datoteka može otkriti njihova vlasnika (analiza aplikacija i datoteka),
- zaporke za pristup kriptiranim ili zaštićenim datotekama mogu, ukoliko su otkrivene, ukazati na vlasnika zaštićenih datoteka (pronalaženje skrivenih podataka),
- datoteke mogu sadržavati podatke karakteristične za pojedinog korisnika i tako otkriti svoga vlasnika (analiza aplikacija i datoteka).

5. Dokumentiranje i izvještavanje

Istražitelj je odgovoran za potpunost i točnost izvještaja o RFA. Dokumentiranje je proces koji se treba provoditi usporedno s RFA, s preciznim bilježenjem svakog koraka. Dokumentacija mora biti potpuna, točna i sveobuhvatna.

5.1. Vođenje bilježaka

Tijekom cijele istrage potrebno je voditi bilješke u skladu s preporukama institucije u čije ime se istraga provodi. Slijedi nekoliko općenitih uputa koje u tome mogu pomoći istražitelju:

- voditi bilješke tijekom konzultacija s voditeljem istrage ili tužiocem,
- sačuvati kopiju naloga za pretragu,
- sačuvati kopiju prvotnog zahtjeva za pokretanjem istrage,
- sačuvati kopiju dokumentacije o nadležnostima i odgovornostima sudionika istrage,
- voditi bilješke koje omogućuju ponavljanje svih provedenih postupaka,
- u bilješke unositi datum, točno vrijeme, opis i rezultate svakog provedenog postupka,
- dokumentirati neuobičajene okolnosti i u vezi njih poduzete akcije,
- bilježiti podatke kao što su: topologija računalne mreže, popis autoriziranih korisnika, korisničke zaporke i sl.,
- bilježiti sve promjene unesene u ispitivani sustav tijekom provođenja RFA,
- dokumentirati programsku podršku ispitivanog računala: operacijski sustav, instalirane aplikacije te zakrpe i nadogradnje,
- dokumentirati prisutnost udaljenih spremišta podataka, mogućnost pristupa udaljenih korisnika i sigurnosnih kopija, itd.

Ukoliko se tijekom pretrage pronađu materijali koji bi mogli biti značajni za RFA, ali nisu u nadležnosti istrage, to je potrebno dokumentirati te zatražiti ovlasti potrebne za obradbu spomenutih materijala.

5.2. Izvještaj

Oblik i sadržaj izvještaja o RFA ovisi o zahtjevima tijela ili organizacije kojoj se izvještaj predaje. On može sadržavati:

- podatke o organizaciji koja je provela RFA,
- jedinstvenu oznaku slučaja,
- podatke o istražiteljima i njihove potpise,
- datum početka istrage i predaje izvještaja,
- popis ispitanih predmeta s opisom koji uključuje serijski broj, naziv proizvođača i model,
- kratak opis poduzetih koraka RFA,
- rezultate RFA i zaključak.

Ponekada je potrebno izvještaj proširiti sažetkom pronalazaka, detaljnim opisom rezultata RFA te listom priloženih dokumenata i/ili kazalom. Sažetak pronalazaka sadrži kratak pregled rezultata svih ispitivanja provedenih u okviru RFA.

Detaljan opis rezultata RFA se može sastojati od:

- datoteka značajnih za RFA,
- ostalih datoteka koje potvrđuju rezultate analize, uključujući izbrisane datoteke,
- dokaza vezanih uz Internet kao što su analiza Web prometa, dnevnički zapisi, priručne datoteke, poruke elektroničke pošte, aktivnosti na tzv. *usenet* grupama,
- analize grafičkih datoteka,
- dokaza vlasništva koji mogu uključivati licence aplikacija,
- opisa za RFA značajnih programskih paketa pronađenih unutar ispitivanog sustava,
- opisa uočenih tehnika prikrivanja podataka kao što su enkripcija, sakrivanje atributa, sakrivanje particija, nepravilnosti imena datoteka, itd.

6. Zaključak

Kako bi se pronašli tragovi zlonamjernog djelovanja unutar računalnog sustava potrebno je provesti sveobuhvatnu RFA. Digitalni dokazi mogu biti vrlo ranjivi zbog čega postoji opasnost od njihova namjernog uklanjanja ili slučajnog oštećivanja. Zbog toga je prije pristupanja analizi potrebno temeljito razraditi planirane postupke i dobro poznavati korištene alate kako ne bi došlo do oštećivanja ili gubitka dokaza.

Tijekom ispitivanja računalnog sustava potrebno je minimizirati utjecaj na njegovo stanje. To znači da je potrebno izbjegavati njegovo gašenje, pohranu podataka na tvrdom disku, pokretanje aplikacija, mijenjanje mrežnih postavki i sl. Preporuča se korištenje programskih alata pokretanih s diskete ili CDa koji svojim radom ne utječu na ispitivani sustav. Također, prikupljanje dokaza potrebno je započeti dohvaćanjem sadržaja radne memorije te drugih ranjivih podataka.

Metode prikupljanja i analize dokaza moraju biti temeljito ispitane i ponovljive kako bi se rezultatima istrage dala vjerodostojnost potrebna za primjenu u sudskom postupku. Iz istog razloga, svaki je korak RFA potrebno detaljno dokumentirati.

7. Reference

[1] Mariusz Burdach: Digital forenzics of the physical memory, Varšava, 2005.

[2] Jesse Kornblum: Preservation of Fragile Digital Evidence by First Responders, Digital Forensics Research Workshop, 2002.

[3] BJ Gleason, Drew Fahrey: Helix 1.7 for Beginners, e-fense, Inc., 2006.

[4] Barry J. Grundy: The Law Enforcment and Forensic Examiner Introduction to Linux, NASA Office of Inspector General, 2004.

[5] Keith J. Jones: Forensic Analysis of Microsoft Windows Recycle Bin Records, http://www.e-fense.com/helix/Docs/Recycler_Bin_Record_Reconstruction.pdf, studeni 2006.

[6] John Ashcroft, Deborah J. Daniels, Sarah V. Hart: Forensic Examination of Digital Evidence: A Guide for Law Enforcment, U.S. Department of Justice, 2004.

[7] Monty McDougal: Window Forensic Toolchest, http://www.foolmoon .net/security/, studeni, 2006.