



Master rad

Forenzika i prevare u digitalnoj tehnologiji sa istražnim metodolgijama,
tehnikama i alatima za kompijuterski kriminal

Mentor:

Prof dr. Kosana Vićentijević

Student:

Nevena Subotić

400244/2013

Beograd, novembar 2014

SADRŽAJ

1.UVOD.....	5
1.2 PREDMET ISTRAŽIVANJA	6
1.3 CILJEVI I ZADACI ISTRAŽIVANJA	6
1.4 HIPOTETIČKI OKVIR ISTRAŽIVANČKOG RADA	7
1.5 METODE I TEHNIKE ISTRAŽIVANJA	7
1.6 STRUKTURA RADA.....	8
2. KOMPIJUTERSKI KRIMINAL	9
2.1 RAZVOJ KOMPIJUTERSKOG KRIMINALA	10
2.2 KARAKTERISTIKE KOMPIJUTERSKOG KRIMINALA	11
2.3 OBLICI KOMPIJUTERSKOG KRIMINALA	11
2.4 TIPOVI KOMPIJUTERSKOG KRIMINALA	12
3.ISTRAGA KOMPIJUTERSKOG KRIMINALA	13
3.1 PROCES ISTRAGE	13
3.2 SIGURNOSNA POLITIKA.....	15
3.3 SIGURNOSNI STANDARDI	16
4.FUNKCIONALNI MODELI DIGITALNE FORENZIČKE ISTRAGE	17
4.1 MODEL INTEGRISANIH PROCESA DIGITALNE FORENZIČKE ISTRAGE	17
4.1.1 Faza pripreme	19
4.1.2 Faza razvoja.....	19
4.1.2.1 Faza detekcije i izveštavanja.....	20
4.1.2.2 Faza potvrde i autorizacije	20
4.1.3 Faza istrage fizičkog mesta krivičnog dela.....	20
4.1.3.1 Faza obezbeđenja fizičkog mesta krivičnog dela.....	20
4.1.3.2 Faza revizije fizičkog mesta krivičnog dela.....	21
4.1.3.3 Faza dokumentovanja fizičkog mesta krivičnog dela	21
4.1.3.4 Faza pretrage i sakupljanja dokaza sa fizičkog mesta krivičnog dela	21
4.1.3.5 Faza rekonstrukcije fizičkog mesta krivičnog dela	21
4.1.4 Faza istrage digitalnog mesta krivičnog dela	22
4.1.4.1 Faza fiksiranja digitalnog mesta krivičnog dela	22
4.1.4.2 Faza pretrage digitalnog mesta krivičnog dela	22
4.1.5 Faza provere	23
5. BEZBEDNOST	23
5.1 ZLONAMERNI SOFTVERI.....	24

5.2 TIPOVI ZLONAMERNIH SOFTVERA	25
5.2.1 Trojanski konj.....	25
5.2.2 Logičke bombe	26
5.2.3 Crvi	26
5.2.4 Virusi	27
5.2.4.1 Virusi koji napadaju sisteme datoteka	27
5.2.4.2 Makro virusi.....	28
5.2.5 Špijunski programi (spyware)	28
5.3 ZAŠTITA OD ZLONAMERNIH PROGRAMA	29
6. HAKERISANJE.....	30
6.1 ETNICKO HAKERISANJE	30
6.1.1. ETIČKI HAKER	30
6.1.2 Deset zapovesti računarske etike	31
7. FORENZIČKI ALATI.....	31
7.1 HARDVERSKI ALATI.....	32
7.1.1. Blokatori upisivanja.....	33
8. SOFTVERSKI ALATI.....	34
8.1 SOFTVERSKI ALAT – ENCASE	34
12 . MEĐUNARODNI RAČUNOVODSTVENI STANDARD 38.....	35
12.1 TUMAČENJE SIC 32	37
13.METODE I TEHNIKE DIGITALNE FORENZIČKE ISTRAGE.....	39
13.1 ISTORIJAT	39
13.2 EVOLUCIJA ISTRAŽNIH ORGANA	40
13.3 DIGITALNA FORENZIČKA ISTRAGA	43
13.4.ULOGA DIGITALNOG DOKAZA.....	45
14. ISTRAŽNE METODOLOGIJE.....	47
14.1 ISTRAŽNE METODOLOGIJE PREMA EOGHAN CASEY-U.....	47
14.1.1. Optužbe ili uzbuna incidentom.....	49
14.1.2 Procena vrednosti	49
14.1.3 Protokoli Incidenta/Mesta zločina	50
14.1.4 Identifikacija ili zaplena	51
14.1.5 Čuvanje.....	53
14.1.6 Oporavak podataka	54
14.1.7 Žetva	54
14.1.8 Redukcija	55
14.1.9 Organizacija i pretraga.....	55
14.1.10 Analiza.....	56
14.1.11 Izveštavanje	56

14.1.12. Ubeđivanje i svedočenje	57
15. Istražna metodologija prema Brian Carreir-u	57
15.1 Korporacijski model istrage.....	58
15.1.1 Uspostavljanje tima za upravljanje kompjuterskim incidentom.....	59
15.1.2 Procedura određivanja karaktera kompijuterskog kriminala.....	61
15.1.3 Model troškova korporacijske forenzičke istrage.....	62
15.2 TIM ZA ISTRAGU KOMPIJUTERSKOG KRIMINALA	64
15.2.1 Interventni tim za korporacijsku istragu kompijuterskog kriminala	64
15.2.2 Formiranje korporacijskog interventnog kibernetičkog tima	64
15.2.3 Metodologija rada kibernetičkih interventnih timova	65
15.2.4 Rezultati korporacijske istrage kompijuterskog incidenta.....	65
15.3 ZVANIČNI MODEL ISTRAGE	66
16.ŽIVOTNI CIKLUS ANALIZE I PRETRAGE DOKAZA	68
17.VRSTE FORENZIČKIH ALATA ZA DIGITALNU FORENZIČKU ISTRAGU	69
18. ILOOK	71
18.1 IZGLED ILOOK-A	73
18.2 PROZOR DOKAZA	74
18.3 PROZOR FAJLOVA	76
18.4 PROZOR INFORMACIJA	77
18.5 PREGLED DISKA	78
18.6 PREGLED FAJLA	81
18.7 DNEVNIK	83
19. WINDOWS THUMBNAIL COCHE	85
19.1 THUMBS	85
19.2 FUNKCIONALNOSTI THUMBNAIL PRETRAŽIVAČA	85
19.3 OSNOVNE FUNKCIONALNOSTI TUMBNAILS PRETRAŽIVAČA	86
20. ULOGA KOMPJUTERA U ZLOČINU	87
20.1 HARDVER KAO PROIZVOD KRIMINALNE AKTIVNOSTI.....	88
20.2 HARDVER KAO INSTRUMENT(ORUĐE) ZLOČINA	88
20.3 HARDVER KAO DOKAZ.....	88
20.4 INFORMACIJA KAO PROIZVOD KRIMINALNE AKTIVNOSTI	89
20.5 INFORMACIJA KAO INSTRUMENT ZLOČINA	89
20.6 INFORMACIJA KAO DOKAZ	89
21. STUDIJA SLUČAJA 1.....	91
21.1 UVOD	92
21.2 OPŠTE KARAKTERISTIKE.....	93
21.3 Način korišćenja	95
22. STUDIJA SLUCAJA 2	100
22.1 UVOD	101

22.2 PROBLEM U FOKUSU	102
22.3 REŠENJE	103
23.STUDIJA SLUČAJA 3	105
23.1 AKVIZICIJA PODATAKA SA FLASH DISKA	106
23.1.1 Utvrđivanje tipa memorije.....	106
23.1.2 Priprema starilinih medija	107
23.1.3 Forenzičko kopiranje	108
23.2 PRISTUP PODACIMA NA ZAKLJUČANIM MEMORIJAMA	108
23.2.1 Otkrivanje zaštite.....	109
23.2.2 Otključavanje memorije	110
23.3 PRAĆENJE USB UREĐAJA POVEZANIH NA RAČUNAR.....	112
23.3.1 Linux OS.....	112
23.3.2 Windows OS.....	113
23.3.3 Povratak podataka sa oštećene USB fleš memorije.....	116
23.3.4 Test Disk.....	117
23.3.5 Recuva	118
23.3.6 GetDataBack.....	118
23.3.7 Stellar Phoenix Windows Data Recovery	119
24. ZAKLJUČAK	120
25.LITERATURA.....	125

1.Uvod

Internet, globalna svetska kompijuterska mreža je za kratak vremenski period od desetak godina evoluirala u moćnu mrežu bez koje se ne može zamisliti život savremenog čoveka. Kada bi ova kompijuterska mreža prestala da funkcionise tek tad bi se shvatio njen značaj i u kojoj meri se protkala u sve pore savremenog društva. Broj korisnika interneta iz godine u godinu beleži eksponencijalan rast broja korisnika i smatra se da ih trenutno ima oko 1,113,408,294 (17,2 %) . Uporedo sa razvojem i implementacijom kompijuterskih mreža u sistem globalne mreže – interneta, rastu i potencijalne opasnosti od različitih napada sa interneta, uključujući brojne maliciozne kodove (programe) i napade ljudskog faktora hakera, vandala i kompijuterskih terorista.

Razlozi za pojavu ovih napada su različiti. Najčešći razlog je sticanje finansijske dobiti, ali i drugi motivi kao što su izazov, znatiželja, samopotvrđivanje krađa informacija, špijunaža i drugi oblici kompijuterskog kriminala. Pod kompijuterskim kriminalom u najširem smislu podrazumevaju se krivična dela prema krivičnom zakonu nacionalne države u kojoj su na bilo koji način uključeni računarski sistemi i mreže. Glavni cilj istrage kompijuterskog kriminala je kao i u slučaju klasičnog kriminala, izgraditi za pravosudne organe neoboriv ili čvrst dokaz , i /ili dokaz za oslobađanje osumnjičenog i /ili pravedno sankcionisanje učinjenog dela.¹ Da bi se obezbedio takav dokaz u slučaju kompijuterskog kriminala potrebno je nizom potrebnih dokaza doći do informacija u digitalnom obliku koje imaju verodostojnu vrednost, a koja je uskladištena ili prenesena u takvom obliku. Ovakve informacije su digitalni dokazi.

U današnje vreme informacione tehnologije su deo naše svakodnevnice. Informaciona tehnologija se prožima kroz sve pore našeg života. Od infrastrukture (strujne stanice, kontrola saobraćaja (semafora), mobilna telefonija, itd.), socijalnog (facebook, twitter itd.), preko saobraćaja (moderna kola u današnje vreme imaju ugrađene kompjutere, avio saobraćaj, železnički saobraćaj), bankarstva (skoro sav novac ovoga sveta je virtuelan, pohranjen kao podatak na računarima) itd. Samim tim ranjivosti informacionih sistema su veliki izazov za razne vrste kriminala, od materijalnog, naučnog, krivičnog pa do terorističkog.

Tema ovog rada je zaštita od zlonamernih programa analiza i vrsta kriminala koji se baziraju na visoko tehnološkom kriminalu kao i upoznavanje vrsta tih kriminalnih radnji, predstavljanje veze između fizičkog kriminala i visoko tehnološkog kriminala kako sa pravnog aspekta tako i sa naučnog aspekta. Upoznavanje termina digitalnih dokaza, i veze između digitalnih i fizičkih dokaza radi lakšeg identifikovanja počinioca zločina.

U radu je opisana i kratka evolucija alata za digitalnu forenzičku istragu kao i praktičnih metoda koji su korišćeni pri ranijim istragama, Neke od tih metoda su unapređene, neke više

¹ Milosavljevic M, Grubor G. Istraga kompijuterskog kriminala Univerzitet Singidunum 2009 str 4

nisu u upotrebi, a neke koje nisu dugo upotrebljavane, opet se vraćaju u upotrebu sa malim izmenama (pregledanje na samim kompromitovanim mašina uživo).

1.2 Predmet istraživanja

U ovom radu bavili smo se kompijuterskim kriminalom i tokom istraživanja i kako da otkrijevo prevare , i pomoću kojih metoda i alata pronaći i prezentovati digitalne dokaze protiv osumnjičenog tako da ti dokazi budu valjani i samim tim prihvaćeni na sudu.

Predmet ovog rada su metode i tehnike koje koriste iztražni organi u saradnji sa dogitalnim forenzičarima, kako bi što bolje i sto brže došli do počinioca zločina. Takođe govori se i o tehnici koju digitalni forenzičari treba da poseduju, a takođe i o neophodnom znanju. Takođe bavili smo se i mestom i ulogom digitalne forenzike kao i upotrebom forenzickih alata u procesu odgovora na identitet u cilju predstavljanja značaja digitalne forenzike za dobru korporacijsku istragu. Početak rada je orijentisan ka objašnjenju pojma kompijuterski kriminal, njegovih pojava oblika i forenzičkih alata koji su korišćeni u istrazi. Sredina rada je orijentisana na istrazne metodologije koje su korišćene da bi se suybio kompijuterski kriminal. Krajnji deo rada se bavi programima koji istražitelji koriste u istrazi kompijuterskog kriminala.

1.3 Ciljevi i zadaci istraživanja

Naučni cilj ovog rada je da se demonstrira sam značaj forenzičke istrage kompijuterske prevare koja nanosi veliku stetu organizaciji kao i da se osvrnemo na nove alate i tehnike koje koristimo i koji nam pomažu u istrazi.

Društveni cilj jeste ukazivanje na važnost istrage kao i na korišćenje alata jer ako korporacijska istraga nije sprovedena dobro i najmanja moguća sitnica nije u skladu sa standardnom procedurom (IOCE) uzimanja forenzičkog imidža može da ugrozi celu istragu i sud može da odbaci dokaze kao nedovoljne.

Cilje je takodje da se pokaze kako smo dosli do relevantnih podataka ,kako tereba da ih čuvamo i prikazemo na sudu.

1.4 Hipotetički okvir istraživančkog rada

Opšta hipoteza

Izvršioi krivičnog dela su uglavnom hakeri koji na bilo koji način pokušavaju da zloupotrebe tuđe računare, mreže ili sisteme. Brojna tradicionalna krivična dela danas koriste računar, posebno kada je u pitanju organizovanje tog krivičnog dela, kao što su dečija pornografija, trgovina drogom, syber terorizam, krađa identiteta na Internetu i razne Internet prevare koje postaju sve češći oblik napada na pojedince. Kompjuterski kriminalci to rade uz pomoć raznih zlonamernih softvera koji se instaliraju na tuđem računaru i na taj način mogu da dođu do potrebnih informacija, mogu i da uspore rad tog sistema ili čak i da ga unište.

Posebna hipoteza

Radna hipoteza je forenzička analiza za otkrivanje internog napada i zloupotrebe od strane zaposlenog sa privilegijama radi pribavljanja vlastite koristi i u kojoj meri je korporacijska istraga podpomogla zvaničnu istragu kompijuterskog kriminala.

Da bi se korisnici zaštitili od kriminala nacionalne države formiraju posebna odeljenja koja se isključivo bave ovim vrstom posla tj kriminalom i to su specijalna odeljenja MUP-A, sudstva i tužilaštva. U samoj borbi protiv kriminala važnu ulogu ima i antivirusna kompanija koja prati maliciozne programe na internetu .

1.5 Metode i tehnike istraživanja

Metoda naučnog istraživanja je sistemski, kritički, kontrolisani i ponovljivi proces sticanja novih znanja, neophodnih za identifikovanje, određivanje i rešavanje naučnog problema. U naučnom istraživanju glavni principi su :

- ❖ Sistematičnost – dobra uređenost istraživanja i obezbeđivanje prirodnog i logičkog sleda procesa.
- ❖ Kontrolisanost – sprovođenje istraživanja u što moguće boljim i nadziranim uslovima, kako bi se isključila alternativna rešenja i
- ❖ Kritičnost – sve važne tvrdnje o pojavama, procesima, odnosima i svojstvima moraju se ozbiljno, iskreno i strogo procenjivati, proveravati i obrazložiti.

U ovom istraživačkom radu korišćene su različite metode istraživanja i verifikacije procesa digitalne forenzičke istrage da bi se došlo do nekih saznanja, otkrili i izložili naučni principi , koji se primenjuju u digitalnoj forenzici. Korišćene su sledeće metode :

1. Analitičke :

- ❖ Analiza
- ❖ Apstrakcija
- ❖ Specifikacija
- ❖ Dedukcija

2. Sintetičke :

- ❖ Sinteza
- ❖ Konkretizacija
- ❖ Generalizacija
- ❖ Indukcija

Tok istraživanja, kao prvi logični korak uključuje prikupljanje literature o metodologiji naučnog istraživanja i digitalnoj forenzičkoj istrazi sa težištem na zvaničnu istragu zatim istraživanje literaturnih podataka i materijala preuzetih iz raznih izvora , kroz faze otkrivanja, opisivanja i objašnjavanja određenih faza digitalne forenzičke istrage.Rad je strukturiran u određene celine .

1.6 Struktura rada

U prvom delu svog projektnog rada obradila sam osnovne podatke o metodologiji društvenih istraživanja ,predmet,ciljeve i zadatke istraživanja.

U drugom delu prvog projektnog rada bavila sam se pitanjima o samom kompjuterskom kriminalu, istraživala koji forenzički alati mogu da se koriste za suzbijanje tog kriminala, kao i dokazi koji mogu da se koriste i prezentuju na sudu.

U prvom delu drugog projektnog rada bavila sam se istorijim digitalne forenzike od njenog nastanka pa sve do danas.Obradila sam takodje i istaražne metodologije prema Eoghan Casez i Braian Carrier-u.

U drugom delu drugog projektnog zadatka obrađivala sam programe koji koriste isrtažni timovi da bi otkrili kompjuterski kriminal i tako došli do validnih podataka koje mogu da podnesu sudu,a da ih sud ne odmaci.

Na kraju samog rada odradila sam tri studije slucaja.

2. Kompjuterski kriminal

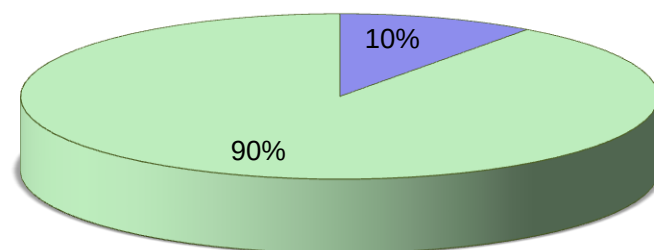
Digitalna ili kompjuterska forenzika se može definisati kao proces prikupljanja , očuvanja , analize i prezentovanja digitalnih dokaza. Digitalna forenzika računarske mreže uključujući i internet ili kiberneticka forenzika² otkriva i sakluplja informacije o tome kako je napadač ili haker dobio pristup računarskoj mreži i računarskom sistemu. Forenzički alati omogućavaju povraćaj i analizu obrisanih, skrivenih i privremenih fajlova kojima se ne može pristupiti na uobičajen način. Ceo izveštaj napravljen na osnovu digitalnih dokaza se koristi na sudu. Korišćenje ovih metoda za potrebe rekonstrukcije događaja okarakterisane su kao kompjuterski kriminal.

Kompjuterski kriminal predstavlja oblik kriminalnog ponašanja kod kojeg se korišćenje kompjuterske tehnologije i informacionih sistema ispoljava kao način izvršenja krivičnog dela ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivično – pravnom smislu relevantna posledica. Kompjuterski kriminal je takođe protivpravna povreda imovine kod koje se računarski podaci s predumišljajem menjaju (manipulacija računara) , razaraju (računarska sabotaza) ili se koriste zajedno s hardverom (krađa vremena) . U kompjuterski kriminal spada svako krivično delo koje je počinjeno uz pomoć računara ili mreže.

Uporedno sa ubrzanom informatizacijom društva i ulaskom interneta u sve oblasti društvenog i privatnog života ljudi , kompjuterski kriminal postaje dominantan oblik zloupotrebe , kršenja zakona i drugih normi ponašanja. Novi oblici napada na računare i računarske mreže javljaju se velikom brzinom, a novi tipovi kompjuterskog kriminala praktično zavise samo od mašte malicioznih napadača.

Procenat otkrivenosti kompjuterskih krivičnih dela

■ Procenat otkrivenih KD ■ Procenat neotkrivenih KD



² Cyber forensic

2.1 Razvoj kompijuterskog kriminala

Šezdesetih godina je bilo izveštavanja o kompijuterskim manipulacijama, sabotazama, špijunažama i nelegalnim korišćenjem računarskih sistema . Sedamdesetih godina su se pojavili prvi ozbiljni zločini ove vrste. Zbog ograničenosti uloge računara u svakodnevnom životu ovi prekršaji su bili usmereni na krađe i prevare vezane za telekomunikacione uloge i prenos elektronskih sredstava. Kasnije sa povećanjem umreženih personalnih računara stvara se potreba za specifičnim zakonima vezanim za ovu vrstu kriminala.

U toku 1984.godine FBI je počeo razvoj laboratorije i programa za ispitivanje kompijuterskih dokaza koji je izrastao u jedinstveni CART (computer analysis and response team) tim , kasnije formiran u mnogim organizacijama u SAD . Danas je trend da se forenzička analiza računara vrši u dobro opremljenoj laboratoriji. Međutim u tom periodu u SAD je oko 70% osposobljenih zvaničnih agencija radilo ovaj posao bez razvijenih procedura za taj rad.

Pojavom digitalnog videa i audia uvodi se pojam digitalnih dokaza.Međunarodna organizacija za kompijuterske dokaze IOCE (international organization on computer evidence) je formirana 1997 godine . Tehnička radna grupa za kompijuterske dokaze TWGDE (technical working group for digital evidence) održala je prvi radni sastanak 17 juna 1998 godine sa ciljem razvoja organizacionih procedura i relevantnih dokumenata za forenzičku istragu digitalnih dokaza.Kompijuterska forenzička analiza za manje od 20 godina pouzdano čuva digitalne podatke, oporavlja izbrisane podatke, rekonstruiše kompijuterske događaje, odvraća napadača, nudi dosta dobrih proizvoda i procedura za podršku.

Kompijuterska forenzička analiza primenjuje se u slučajevima : hakerskog upada, pronevere, pedofilijaskog kruga, imigracione prevare, trgovine drogom, falsifikovanje platnih kartica, piraterija softvera, izbornog zakona, obscenih publikacija,falsifikata, ubistva.seksualnog uznemiravanja, krađe podataka industrijske špijunaže, razonoda.

Savremeni korisnici digitalne forenzike su: policija, vojska,pravosudni sistem (tužilaštvo i pravosuđe), firme koje se profesionalno bave oporavkom podataka iz računara,korporacijee za upravljanje kompijuterskim incidentom.³

³Milosavljević Milan,Grubor Gojko Istraga kompijuterskog kriminala Univezitet Singidunum 2009 ,strana 8

2.2 Karakteristike kompijuterskog kriminala

Kompijuterski kriminal ima svoje specifičnosti u odnosu na druge oblike kriminalnih delovanja, i te karakteristike su :

- ❖ Velika dinamičnost
- ❖ Konstantno širenje na nove oblasti
- ❖ Težina posledica koje nastupaju vršenjem kompijuterskih krivičnih dela
- ❖ Otežano otkrivanje i dokazivanje
- ❖ Specifičan profil učinioca
- ❖ Velike mogućnosti za prikrivanje izvršenog kriminalnog dela

Ove karakteristike posledica su specifičnog ambijenta u kojem se kompijuterski kriminalitet vrši. Taj ambijent karakterišu sledeće osobine:

- ❖ Visoka koncentracija na malom prostoru
- ❖ Proširen prostor kriminalnog delovanja koji za razliku od tradicionalnih vidova kriminaliteta ne zahteva prisustvo izvršioca na licu mesta
- ❖ Skraćeno vreme kriminalnog delovanja s obzirom na automatizovani ambijent čija brzina sprečava nadzor i upravljanje.
- ❖ Postojanje veštih tehnika i metoda koje se izvršavaju istim mehanizmima kao i zakonite, ne ostavljajući tragove i ne ometajući redovan rad sistema
- ❖ Stabilnost rizika s obzirom da se jednom izgrađen modus može veoma dugo koristiti sa potpuno istim, niskim rizikom otkrivanja
- ❖ Jednostavnije mogućnosti upotrebe kompijuterske tehnologije od strane sve većeg broja korisnika

2.3 Oblici kompijuterskog kriminala

Na Destom kongresu Ujedinjenih nacija za prevenciju kriminaliteta I tretman delikvenata, u okviru materijala za sekciju o kriminalu zaključeno je da postoje dve vrste pojavnog oblika kriminalnog ponašanja :

- ❖ **Cyber kriminal u užem smislu** – predstavlja svako nezakonito ponašanje usmereno na elektronske operacije sigurnosti kompijuterskih sistema i podataka koji se u njima obrađuju
- ❖ **Cyber kriminal u širem smislu** – kao svako nezakonito ponašanje vezano za ili u odnosu na kompijuterski sistem i mrežu, uključujući i takav kriminal kakvo je nezakonito posedovanje, nuđenje i distribuiranje informacija preko kompijuterskih sistema i mreža.

U skladu sa Preporukom Saveta Evrope i listom OECD –a iz 1989 odnosno 1985 godine kompijuterski kriminal se deli na :

- ❖ Neuautorizovani pristup kompjuterskom sistemu ili mreži kršenjem mera sigurnosti (haking);
- ❖ Oštećenje kompjuterskih podataka ili programa;
- ❖ Kompjuterske sabotaze;
- ❖ Neovlašćeno presretanje komunikacija od i u kompjuterskim sistemima i mrežama;
- ❖ Kompjuterska špijunaža. Svaki od ovih oblika može se ukrštati sa svakim jer gotovo da ne postoji “čisti” oblik.⁴

Od kompjuterskog kriminaliteta u širem smislu, najčešće se pojavljuju: kompjuterski falsifikati, kompjuterske krađe, tehničke manipulacije uređajima ili elektronskim komponentama uređaja, zloupotrebe sistema plaćanja (kao što su manipulacije i krađe elektronskih kreditnih kartica ili korišćenje lažnih šifri nezakonitim finansijskim aktivnostima.

2.4 Tipovi kompijuterskog kriminala

Tipovi kompjuterskog kriminala:

- ❖ Krađa elektronskih usluga
- ❖ Komunikacija u cilju krivične zavere
- ❖ Piraterija
- ❖ Elektronsko pranje novca
- ❖ Vandalizam i terorizam na Internetu
- ❖ Prodaja i investicija laži
- ❖ Ilegalno presretanje komunikacionih kanala
- ❖ Transfer sredstava za on line prevare

U zavisnosti od tipa pocinjenih dela kompijuterski kriminal može biti :

- ❖ Politički
- ❖ Ekonomski
- ❖ Proizvodnja i distribucija nedozvoljenih i štetnih sadržaja
- ❖ Manipulacija zabranjenim proizvodima, supstancama ,robom
- ❖ Povreda sajber privatnosti

⁴ Džemail Zornić kompijuterski kriminal – zločin i prevencija str 1

3.Istraga kompijuterskog kriminala

Krađa osetljivih podataka i dalje je glavni uzrok nastajanja kompjuterskih incidenata u korporacijama. Ovi incidenti se sve češće događaju od strane zaposlenih u samoj korporaciji što ukazuje na to da je potrebno uvesti niz efikasnih i jasno određenih pravila koja će osigurati i zaštititi materijalne i intelektualne vrednosti organizacije od krađe i uništavanja.

Prilikom istrage kompjuterskog kriminala na računarskim mrežama, u toku prikupljanja, analize i prezentacije digitalnih dokaza moraju se poštovati određeni principi. Najbolja forenzička praksa dokazala je da je najbolje formirati tim sačinjen od profesionalaca: zvaničnog organa istrage, tužioca, eksperta u oblasti informaciono komunikacionog sistema, eksperta u oblasti računarskih mreža, digitalnog forenzičara i dr. po potrebi. U slučaju kompjuterskog kriminala česta je praksa da se zahteva ekspertsko svedočenje ili veštačenje.

Uvođenje sigurnosne politike može biti skup i dugotrajan proces u kojem je potrebno prilagoditi sve delove organizacije da rade sinhronizovano. Korporacijama i institucijama se preporučuje uvođenje sigurnosne politike radi podizanja nivoa sigurnosti kako informacionog sistema, tako i njihovih korisnika. U ovom radu predmet istraživanja je pronalaženje digitalnih dokaza na mrežnim uređajima koji se koriste u korporacijama u cilju forenzičke akvizije na računarskim mrežama i izrada sigurnosne politike za korporaciju sa težištem na rešavanju kompjuterskih incidentata i digitalnu forenzičku istragu kompjuterskog kriminala.

3.1 Proces istrage

Sam process digitalne forenzičke istrage deli se u dve osnovne kategorije:

- ❖ Zvanična (javna) i
- ❖ Korporacijska (privatna) digitalna forenzička istraga
- ❖

Zvanični istražni postupak kompjuterskog kriminala optimalno se odvija u 4 faze, po modelu “korak po korak” u okviru jedne faze. Svaki korak u okviru jedne faze istrage treba da vodi u drugi i da je obezbeđena kontrola aktivnosti u okviru svake faze .

- ❖ Inicijalna istraga,
- ❖ Ulazak u trag napadaču.
- ❖ Otkrivanje identiteta napadača.
- ❖ Hapšenje

Ova istraga uključuje u svoj rad policijske organe , specijalno tužilaštvo i specijalno sudstvo za borbu protiv visokotehnološkog (kompijuterskog) kriminala. Ovi organi treba da rade u skladu sa brojnim zakomima.Takođe zvanični organi istrage kompijuterskog kriminala treba

da rade prema strogo utvrđenim standardima operativnim procedurama (SOP) . U slučaju zvanične istrage istražni organi moraju dobro poznavati i razumeti sve zakone i propise koji se odnose na kompijuterski kriminal, uključujući standarde lokalne procedure za pretragu i utvrđivanje slučaja krivičnog dela kompijuterskog kriminala.

Korporacijska istraga se može smatrati predistražnim postupkom zvanične istrage kompijuterskog kriminala. Odvija se u tri faze:

- ❖ pokretanje istrage,
- ❖ određivanje karaktera kompijuterskog incidenta i
- ❖ analiza prikupljenih digitalnih podataka.

Korporacijsku istragu organizacija može izvršiti sopstvenim timom , iznajmljenim timom ili kombinovanim timom. Praksa je pokazala da se efikasniji rezultati dobijaju izvršavanjem 6 Rosenblattovih koraka:

- ❖ eliminisanje očiglednosti,
- ❖ postavljanje hipoteze o napadu,
- ❖ rekonstruisanje krivičnog dela,
- ❖ otkrivanje traga do osumnjičenog računara,
- ❖ analiza izvornog, ciljnog i posrednog računara i
- ❖ prikupljanje dokaza, nakon čega predati nalaze i dokazne materijale korporacijskim ili zvaničnim organima istrage za dalji postupak.

Rekonstrukcija traga napada predstavlja čitanje log datoteka na celom putu napada, pri čemu se javljaju sledeći problemi:

- ❖ log datoteke su izmenjene, ne postoje ili su neadekvatne,
- ❖ isprekidana zaustavljanja između izvora napada i računara žrtve,
- ❖ uskraćena saradnja administratora posrednih računara,
- ❖ lažiranje IP adresa,
- ❖ izmenjeni log datoteka napadnutog računara ili primenjeni drugi trikovi za maskiranje
- ❖ neovlašćenog pristupa, samo jedan neovlašćeni pokušaj pristupa.

Prikupljanje dokaza i predavanje dokaznog materijala korporacijskim ili zvaničnim organima istrage, vrši se isključivo po odobrenju vlasnika napadnutog sistema i odluci korporacije .

Standarda korporacijska istraga obuhvata :

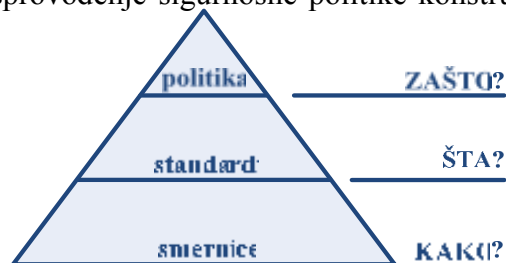
- ❖ Ispitivanje osumnjičenih i svedoka
- ❖ Priprema organa za pretragu
- ❖ Pretres resursa osumnjičenog
- ❖ Provera evidencija log fajlova i ostalih informacija o osumnjičenom
- ❖ Markiranje i sortiranje svog posrednog dokaznog materijala sa detaljnim oznakama o sadržaju i mestom za potpis .lica koje preuzima dokazni material
- ❖ Zaštita od izmene memorisane datoteke sa dokazima
- ❖ Obezbeđenje vremenske evidencije događaja kao čvrstog dokaza
- ❖ Korišćenje forenzičkih alata za verifikaciju događaja kao kriminalnog akta
- ❖ Kontrolna provera svih faza istrage
- ❖ Prikupljanje, analiza i priprema dokaza za glavni pretres
- ❖ Izrada detaljnog izveštaja o istrazi, dokumentovanje i preporuka za dalji postupak

- ❖ Odluka na nivou organizacije : stornirati, nastaviti u organizaciji ili predati slučaj nadležnim organima.

3.2 Sigurnosna politika

Sigurnosna politika predstavlja skup jasno definisanih pravila koji obuhvataju područja na kojima je moguće izvršiti neku vrstu napada .Sigurnosnom politikom jasno se određuju pravila ponašanja i odgovornosti vezane uz informacioni sistem kako bi se minimizovala šteta nastala namernim ili nenamernim delovanjem.

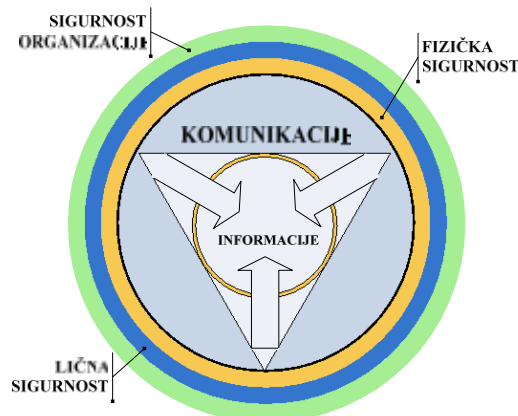
Sigurnosna politika korporacije ili institucije prilagođava se potrebama i nije jednaka za sve. Standard je obavezni postupak ili pravilo koje je izrađeno kako bi učinilo politiku delotvornu, a mora uključivati jedan ili više tehničkih opisa za komponente računara, programe i njihovo rukovanje. Smernice su uopštene izjave, preporuke ili administrativna uputstva koja daju okvirna uputstva za sprovođenje sigurnosne politike konstruisane kako bi se ostvarili ciljevi sigurnosne politike.



Slika 1. Prikaz uklapanja smernica, standarda i sigurnosne politike⁵

Uspostavom sigurnosne politike korisnicima su nametnuta obavezujuća pravila ponašanja koja ograničavaju slobodu pri pregledu poverljivih informacija, kao i pravila za ispravno korišćenje računarske opreme koja je korisniku data na korišćenje, Sigurnosnom politikom se osiguravaju tri svojstva informacija koji sadrže neki sistem :

- ❖ Poverljivost
- ❖ Integritet
- ❖ Dostupnost



Slika 2. Sigurnosne informacione komponente

⁵ http://www.itvestak.org.rs/ziteh_10/zbornik_radova/Nikacevic%20Vladan%20-%20Korporacijska%20istraga%20kompjuterskog%20kriminala.pdf – 20.03 2014

Da bi se zadovoljili propisani standardi sigurnosti informacijski sistemi se dele na tri glavna dela: f

- ❖ računarsku opremu,
- ❖ programe i
- ❖ komunikacije.

Mehanizmi zaštite i sprečavanja su podeljeni na tri osnovna nivoa:

- ❖ fizička sigurnost, pod kojom se smatra sigurnost računarske opreme i podataka,
- ❖ lična sigurnost je zaštita korisnika i poverljivih informacija o korisniku i
- ❖ sigurnost organizacije, koja zavisi od prva dva nivoa.

3.3 Sigurnosni standardi

Sigurnost informacija je podjednako važna malim i velikim, kao i javnim i privatnim organizacijama. Primena tehničkih rešenja, odgovarajuće opreme i proizvoda više nije dovoljna da bi osiguralo odgovarajuće upravljanje sigurnošću informacija. Sigurnost informacija nije isključivi problem informacijskih tehnologija (IT), već je to "poslovni" problem. Opšte je mišljenje da primenom odgovarajućih tehnologija se rešava samo jedan deo problema sigurnosti informacija.

Razvojem, implementacijom i sertifikacijom menadžment sistema za sigurnost informacija ISMS (Information Security Management System) pruža se određeni nivo poverenja kod komitenata menadžmenta, deoničara i zaposlenih da će njihove informacije adekvatno biti zaštićene. Standard ISO 27001 može da se implementira u sve grane industrije, trgovine i pružanja usluga.

Standardi iz ISO/IEC 27000 serije korporacijama pružaju smernice za konstruisanje, primenu i proveru informacijskih sistema čime se osigurava poverljivost, integritet i dostupnost informacionog sadržaja, sistema i procesa unutar organizacije. Za područje sigurnosti informacijskih sistema najčešće se koriste dva standarda :

- ❖ ISO/IEC 27001 i
- ❖ ISO/IEC 27002 (pre 2007. godine poznat kao ISO/IEC 17799:2005).

****ISO/IEC 27001****

Standard ISO 27001 predstavlja sistem zaštite i bezbednosti informacija. Cilj ovog sistema je da osigura sve neophodne kontrole u vezi sa strogo poverljivim, verodostojnim i ograničenim za pristup informacijama, u cilju zaštite informacija i podataka "zainteresovanih strana". Zainteresovane strane kojima je ovaj sistem menadžmenta upućen mogu biti klijenti, organizacije i kompanije, zaposleni, saradnici, ali i društvo u širem smislu.

Serijski standard ISO/IEC 27000 daje jedan harmonizovani pristup upravljanju rizicima kojim su izložene informacione vrednosti u organizaciji kroz razvoj, implementaciju i održavanje menadžment sistema za sigurnost informacija.

Standard se sastoji od 5 delova:

- ❖ Sistem za zaštitu informacija
- ❖ Odgovornost rukovodećih ljudi
- ❖ Unutrašnje provere sistema za zaštitu informacija
- ❖ Provera valjanosti sistema za zaštitu informacija
- ❖ Poboljšanja na sistemu za zaštitu informacija

**** ISO/IEC 27002 (ISO/IEC 17799)****

ISO/IEC 27001 standard definiše koje zahteve neki sistem za zaštitu informacija mora imati, pa za primerene provere navodi upotrebu ISO/IEC 27002 standarda. ISO/IEC 27002 je službeni standard, ali se tumači kao skup smernica koje je moguće upotrebiti. Standard sadrži 39 ciljeva i sastoji se od 12 delova :

- ❖ Procena rizika
- ❖ Sigurnosna politika
- ❖ Organizacija informacione sigurnosti
- ❖ Upravljanje imovinom
- ❖ Zaštita od zaposlenih
- ❖ Fizička zaštita i zaštita od okoline
- ❖ Upravljanje komunikacijama i operacijama

4.Funkcionalni modeli digitalne forenzičke istrage

4.1 Model integrisanih procesa digitalne forenzičke istrage

Model koristi pretpostavke da je kompjuter sam po sebi mesto zločina , nazvan digitalna scena zločina i primenjuje tehnike istrage fizičke scene zločina.Istara fizičke scene zločina koristi zakone prirode i bogata iskustva , da bi otkrila fizičke dokaze ,a istraga digitalne scene koristi kod da bi otkrila digitalne dokaze .

U istrazi fizičkog mesta krivičnog dela najpoznatija primenjena tehnika je Lokardov zakon razmene materije.Sličan efekat se dešava u digitalnoj sceni zločina. Rad digitalnog forenzičara u potpunosti zavisi od rada operativnog sistema i aplikativnih programa, zato što oni nezavisno od korisnika kontrolišu koji dokaz je napisan i u kojem delu memorijskih lokacija.

Koristeći koncept da je kompjuter sam za sebe scena zločina, može se teorija istrage fizičke scene zločina primeniti na digitalnu forenzičku istragu. Forenzička istraga digitalne scene zločina integrisana je sa istragom fizičke scene zločina tako da fizički dokazi mogu biti sakupljeni i povezani sa digitalnom aktivnošću napadača. Digitalna scena osumnjičenog kompjuterskog kriminala može se smatrati za sekundarnu scenu zločina, u odnosu na fizičku scenu zločina.⁶

Da bi se sprečila konfuzija, definišimo osnovne termine procesa, tako da najtačnije odražavaju izabrani pristup problemu:

❖ **Fizički Dokaz:** fizički objekti koji mogu utvrditi da je kriminalni akt počinjen, i koji mogu da omoguće vezu između zločinca i žrtve, ili mogu da omoguće vezu između zločina i izvršioca zločina,. Kompjuter, hard disk, PDA i CD-ROM su primeri fizičkog dokaza.

❖ **Digitalni dokaz:** digitalni podatak koji može potvrditi da je kompjuterski kriminal počinjen i koji može da omogući vezu između kriminala i njegovog izvršitelja,. Podatak u memoriji, na hard disku, ili u mobilnim telefonima primeri su digitalnog dokaza.

❖ **Fizička scena zločina:** fizičko okruženje gde postoje fizički dokazi zločin incidenta. Okruženje gde se prvi kriminalni akt dogodio je primarna fizička scena zločina, a sledeće scene su sekundarne fizičke scene zločina.

❖ **Digitalna scena zločina:** Virtuelno okruženje koje se sastoji od hardvera i softvera gde digitalni dokaz zločina ili incidenta postoji. Okruženje gde se prvi kriminalni akt dogodio je primarna digitalna scena zločina, a sledeće scene se nazivaju sekundarnim digitalnim scenama zločina.⁷

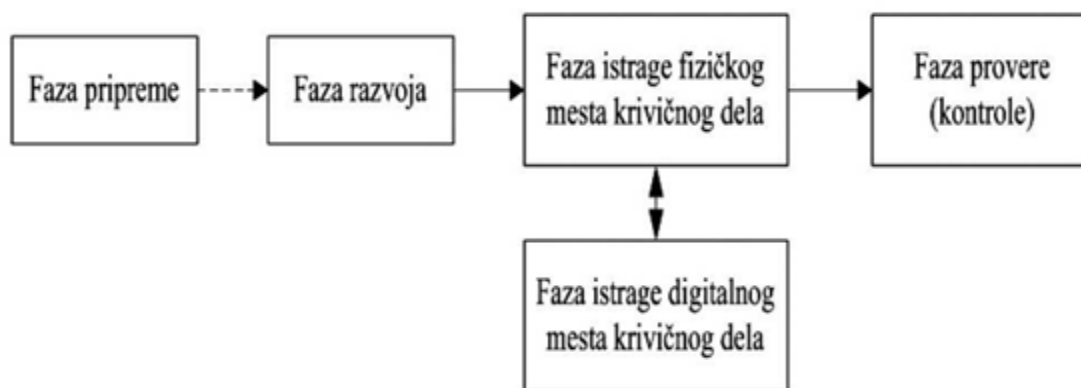
Ovaj model procesa primenljiv je na obe vrste istrage, korporacijsku i zvaničnu.

Zbog toga se izrazi “scena zločina” i “incident” koriste u opštem smislu. Model integrisanih procesa ima 17 faza organizovanih u pet grupa

- ❖ Faza pripreme;
- ❖ Faza razvoja;
- ❖ Faza istrage fizičke scene zločina;
- ❖ Faza istrage digitalne scene zločina;
- ❖ Faza provere (kontrole).

⁶ Milosavljevic M, Grubor D. Istraga kompijuterskog kriminala , Univerzitet Singidunum 2009 , str 54

⁷ http://www.itvestak.org.rs/ziteh_06/Radovi/ZITEH%2006-R07.pdf – 20.03.2014



Slika 3. Faze modela integrisanih procesa digitalne forenzičke analize⁸

4.1.1 Faza pripreme

Digitalni i fizički dokazi mogu biti izgubljeni ukoliko nisu prikupljeni i čuvani na pravi način. Traje u kontinuitetu i nije vezana za bilo koji zločin ili incident. Ova faza ima zadatak da obezbedi potpunu operativnu i infrastrukturnu pripremu i podršku istrazi. Operativna priprema obezbeđuje obuku za lica koja će biti uključena u incident. Infrastruktura faze pripreme obezbeđuje da se generišu potrebni digitalni i drugi podaci da bi se izvršila potpuna istraga. Ukoliko podaci ne postoje nemoguće je izvršiti istragu. Ova faza odnosi se samo na one koji održavaju okruženje koje bi potencijalno moglo biti scena kompjuterskog kriminala.

Fizički primeri za ovu fazu su instalacije i raspoređivanje video nadzora i čitača kartica da bi se snimili pristupi prostoru za vreme kriminalnog akta. Digitalni primeri za ovu fazu su skladištenje log datoteka servera i drugih mrežnih uređaja na zaštićeni "log host", sinhronizacija unutrašnjih satova na serverima i računarima sa NTP (*Network Time Protocol*), kreiranje sistema osnovne zaštite integriteta sa heš algoritmom MD5, i održavanje upravljanja promenama baze log podataka.

4.1.2 Faza razvoja

Cilj ove faze je da obezbedi mehanizam za detekciju i potvrdu incidenta. Zadaci modela koji se izvode u ovoj fazi dosta se razlikuju za zvaničnu i korporacijsku istragu.

⁸ Milosavljevic M. Grubor G. Istraga kompjuterskog kriminala, Univerzitet Singidunum 2009, str 56

4.1.2.1 Faza detekcije i izveštavanja

Cilj ove faze je da detektuje i izveštava odgovorna lica o incidentu. Ovo se može obaviti pozivom 92, preko alarma mrežnog detektora upada- IDS (intrusion detection system) ili online od agenta policije koji istražuje ilegalne aktivnosti. Ova faza definiše početak procesa istrage.

4.1.2.2 Faza potvrde i autorizacije

Cilj ove faze je da se dobije ovlašćenje za istragu incidenta i mesta krivičnog dela. U slučaju zvanične istrage traži se nalog za pretres ili drugo ilegalno odobrenje koje mora da bude potkrepljeno sa dovoljno inicijalnih dokaza. Kod korporacijske istrage nalozi za pretres nisu potrebni dok god ne krše prava privatnosti ili slučaj ne prerasta kapacitete i sposobnosti korporacijskog tima za istragu.

4.1.3 Faza istrage fizičkog mesta krivičnog dela

Ova faza ima cilj da prikupi i analizira fizičke dokaze i rekonstruiše akcije koje su dovele do incidenta. Kao jedan od najvažnijih ciljeva forenzičke digitalne istrage navodi se identifikacija ljudi koji su odgovorni za incidente, i zbog toga su potrebni fizički dokazi. Ovu istragu vrši istražitelj- ekspert za istragu fizičkog mesta krivičnog dela i interventni tim za reagovanje na kompjuterski incident ili tim za fizičko obezbeđenje.

4.1.3.1 Faza obezbeđenja fizičkog mesta krivičnog dela

Ista je za svaki tip krivičnog dela, i osnovne aktivnosti koje sadrži su :

- ❖ Osiguraje izlaza
- ❖ Pomoć ranjenima
- ❖ Zadržavanje osumnjičenih
- ❖ Identifikovanje svedoka

Ova faza obezbeđuje mesto krivičnog dela od izmena da bi se kasnije mogli sakupiti i identifikovali dokazi, i ne čuva samo određene delove dokaznog materijala već celokupno fizičko i digitalno mesto krivičnog dela kompjuterskog kriminala.

4.1.3.2 Faza revizije fizičkog mesta krivičnog dela

Organ istrage bilo da je to zvanični ili korporacijski prolazi i opservira fizičko mesto krivičnog dela i obično je prva osoba koja reaguje na kompjuterski kriminal/ incident. Cilj ove faze je da se identifikuju očigledni delovi dokaznog materijala, osetljivi delovi fizičkog dokaza i razvije početna teorija o krivičnom delu. Digitalni dokazi moraju se odmah dokumentovati i sakupiti da se ne bi oštetili.

4.1.3.3 Faza dokumentovanja fizičkog mesta krivičnog dela

Istražitelj treba da pravi fotografije, skice i video snimke mesta krivičnog dela i dokaza i da detaljno dokumentuje svaku aktivnost u procesu pretrage. Cilj je da se prikupi što više informacija i da se sačuvaju i zabeleže.

4.1.3.4 Faza pretrage i sakupljanja dokaza sa fizičkog mesta krivičnog dela

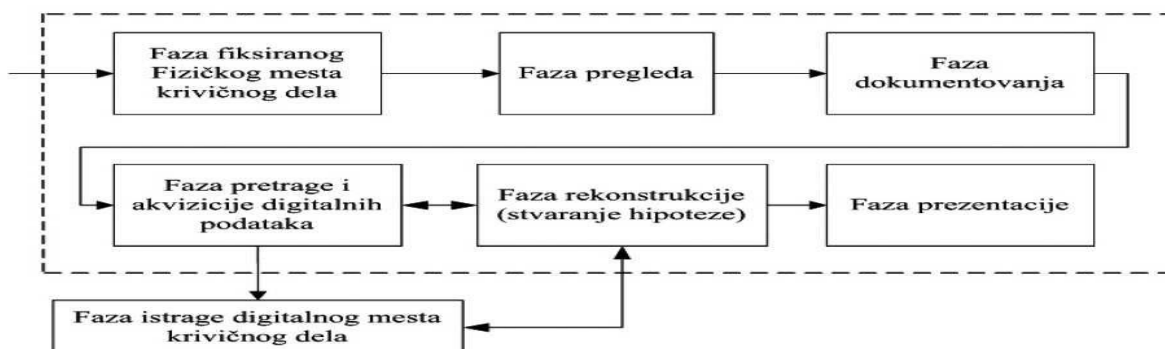
Ova faza obuhvata pretragu i detaljno prikupljanje dodatnih fizičkih dokaza iz dubine fizičkog mesta krivičnog dela. Pretraga može biti usmerena prema nestalim delovima fizičkih dokaza kao što je npr. oružje. Prikupljeni dokazi se šalju u forenzičku laboratoriju radi analize, a rezultati se koriste u sledećoj fazi rekonstrukcije incidenta. U ovoj fazi počinje forenzička istraga digitalnog mesta krivičnog dela. Računarski sistem se smatra fizičkim dokazom pa se i on oduzima kad god je to moguće.

4.1.3.5 Faza rekonstrukcije fizičkog mesta krivičnog dela

Ovde spada organizovanje rezultata analize prikupljenih fizičkih i digitalnih dokaza i korišćenje fotografija sa fizičkog mesta krivičnog dela da bi se razvila hipoteza o incidentu. Kod digitalnog incidenta, rezultati istrage digitalnog mesta krivičnog dela povezuju se sa fizičkim dokazima, da bi se povezala osoba sa digitalnim događajem. U ovoj fazi treba uključiti i konsultovati digitalne forenzičare za pomoć oko povezivanja događaja sa više izvora digitalnih dokaza.

4.1.4 Faza istrage digitalnog mesta krivičnog dela

Počinje kada su fizički digitalni uređaji i drugi dokazni materijali prikupljeni kao fizički dokazi ili kada je sačuvan analizirani mrežni saobraćaj radi obezbeđivanja dokaza. Ova faza prilazi računarskom sistemu kao fizičkom mestu krivičnog dela i pretražuje ga radi izvlačenja digitalnih dokaza. Cilj je da se identifikuju digitalni podaci o događajima na sistemu i prezentuju istražnom organu fizičkog mesta krivičnog dela.



Slika 4. - Faze i interakcija istrage digitalnog mesta krivičnog dela⁹

4.1.4.1 Faza fiksiranja digitalnog mesta krivičnog dela

Ova faza obezbeđuje ulaz ili izlaz ka ili od digitalnog mesta krivičnog dela i zaštitu integriteta digitalnih dokaza koji se lako mogu izmeniti. Ovo predstavlja izolaciju računarskog sistema od računarske mreže, sakupljanje nestabilnih i lako promenljivih podataka koji bi mogli biti izgubljeni kada se sistem isključi i identifikovanje bilo kakvih sumnjivih procesa koji su aktivni u sistemu. Treba registrovati i po mogućstvu ispitati sumnjive korisnike koji su ulogovani na sistem. Log fajlovi se mogu smatrati za očevice digitalnog krivičnog dela i moraju biti obezbeđeni ukoliko postoji pretnja da mogu biti izbrisani pre nego što se sistem fizički iskopira.

4.1.4.2 Faza pretrage digitalnog mesta krivičnog dela

Ova faza se obavlja u forenzičkoj laboratoriji, na jednoj od forenzičkih replika (imidža) digitalnog mesta krivičnog dela. Ukoliko nije moguće privremeno oduzeti kompromitovani sistem, ova faza može da se izvrši i uživo u fizičkom

⁹ Milosavljevic M. Grubor G. Istraga kompijuterskog kriminala, Univerzitet Singidunum 2009, str 59

okruženju sa tehnikama i alatima aktivne akvizice računara u radu, iako je poželjno laboratorijsko okruženje, zato što pruža kontrolisane uslove, a rezultati se mogu ponoviti sa drugom, referentnom replikom sistema, ako to zahtevaju sudski organi .

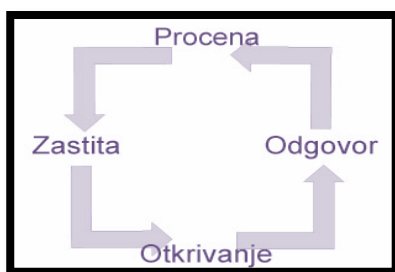
4.1.5 Faza provere

Ovo je završna faza i sastoji se od revizije i kontrole integralnog procesa istrage da bi se identifikovale oblasti koje se mogu poboljšati. Za digitalni kompjuterski incident, ovo obuhvata analizu kvaliteta rada organa istrage, i koliko dobro su izvršene fizička i digitalna istraga svaka za sebe, koliko dobro su urađene zajedno i da li postoji dovoljno fizičkih i digitalnih dokaza da bi se slučaj rešio. Rezultat ove faze mogu biti nove poboljšane procedure istrage, dodatna obuka ili ništa ukoliko je sve ispalo kako je planirano.¹⁰

5. Bezbednost

Bezbednost kao proces se sastoji iz četiri osnovna koraka a to su :

- ❖ Procena
- ❖ Zaštita
- ❖ Otkrivanje
- ❖ Odgovor



Slika 5. Sigurnost kao proces

Procena je priprema za ostale tri komponente. Jako je bitna procena realnog stanja sistema jer greška u proceni može da naškodi svim operacijama koje slede.

Zaštita je sprečavanje ili prevencija. Podrazumeva protiv meru kako bi se smanjila ugroženost sistema. Ukoliko ona zakaže primenjuje se sledeća mera, a to je otkrivanje.

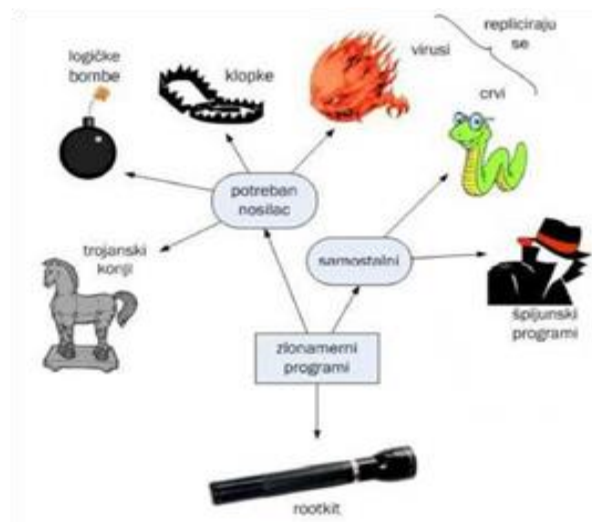
Otkrivanje predstavlja proces identifikacije upada ili incidenta koji se odnosi na bezbednost. I poslednji korak je odgovor.

Odgovor ili reakcija predstavlja proces oporavka tj. lečenja posledica upada.

¹⁰ Milosavljevic M. Grubor G. Istraga kompijuterskog kriminala, Univerzitet Singidunum 2009, str 66

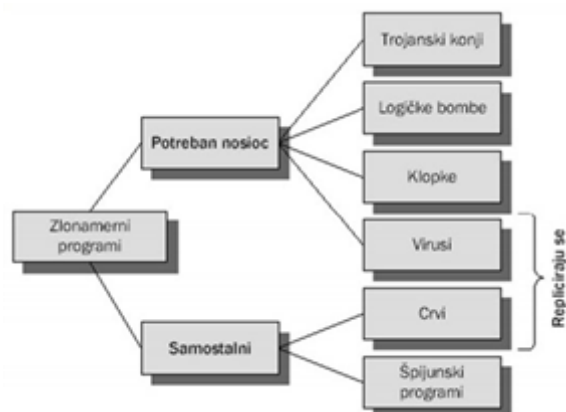
5.1 Zlonamerni softveri

Zlonamerni softver je skup instrukcija koji se pokreću na korisnikovom računar i čine da korisnički računar radi ono što napadač želi. U zlonamerni softver spada svaki program napravljen u nameri da na bilo koji način ošteti umrežen ili neumrežen računar i/ili oteža ili onemogući njegovo korišćenje. Postoje različiti oblici zlonamernih programa – neki zahtevaju nosioce (korisnike programa) dok su neki samostalni, a neki se repliciraju (razmnožavaju), a drugi ne. Zlonamerni programi mogu raditi neprimetno u pozadini, ili usporiti računar i periodično izazvati kočenje ili obaranje sistema. Najveći broj zlonamernih programa namenjen je Microsoft Windows platformama. Zlonamerni programi se distribuiraju pomoću deljenih direktorijuma na mreži, priloga elektronske pošte, otvorenih TCP i/ili UDP portova koji omogućavaju izvršenje udaljenog koda na žrtvi, P2P mreža, IM servisa, drugih zlonamernih programa koji će preuzeti maliciozni kod sa neke lokacije na internetu i instalirati ga na žrtvi.



Slika 6. Zlonamerni softveri

5.2 Tipovi zlonamernih softvera



Slika 7. Vrste zlonamernih programa

Zlonamerni programi se mogu klasifikovati na dva načina.

Prema jednom kriterijumu (da li zahtevaju nosioca, tj program u koji će biti sakriveni) zlonamerni programi se dele na:

- ❖ one koji zahtevaju nosioca (trojanski konji, virusi)
- ❖ samostalne (crvi, špijunski programi).

Prema drugom kriterijumu, zlonamerni programi se dele na:

- ❖ one koji se repliciraju (virusi, crvi)
- ❖ na one koji se ne repliciraju (trojanski konji, logičke bombe).

5.2.1 Trojanski konj

Trojanski konji (ili kraće trojanci) zlonamerni su programi koji se maskiraju i reklamiraju kao korisni programi kako bi se korisnici prevarili tj. naterali da te programe pokrenu.

Ono što trojance razlikuje od virusa i crva je nemogućnost replikacije, tačnije oni se mogu prenositi i sa računara na računar samo putem aktivnosti samog korisnika.

To znači da ovaj tip zlonamernih programa ne poseduje infekcijsku komponentu, tj. funkcije za inficiranje drugih programa. Trojanski konji koji uspevaju da se infiltriraju u sistem, najčešće pokušati da ukradu korisne informacije od korisnika, kao na primer lozinke. Takođe, često korišćena mogućnost trojanaca je takozvani “backdoor” ili omogućavanje neovlašćenog pristupa i kontrole računara od strane neautorizovanog korisnika, a da legitimni korisnik toga nije svestan. Oni prouzrokuju ozbiljne probleme u računarskim sistemima svih veličina. Mnogi trojanci prenose softverske viruse.

U praksi se najčešće pojavljuju sledeće vrste trojanca:¹¹

- ❖ Trojanac koji otvara zadnja vrata – program koji omogućava udaljenom korisniku da pristupi inficiranom računaru, i to najčešće tako da vlasnik računara nije ni svestan posetioca. Nakon inficiranja, napadač može da koristi resurse inficiranog računara u koje spadaju i poverljive informacije kao što su lozinke.
- ❖ Nosioци softvera – realizovani su u vidu trojanskih konja koji se nakon instalacije ponasaju kao magnet za drugi zlonamerni softver.
- ❖ Trojanski proksi server – pretvara inficirani računar u proksi server, čime se udaljenim korisnicima dozvoljava da preko inficiranog računara anonimno pristupe internetu. Time se inficirani računar efikasno pretvara u zombija koji se može iskoristiti za slanje neželjenih poruka ili za učestvovanje u DoS napadu.

5.2.2 Logičke bombe

Jedan od najstarijih vrsta zlonamernih programa. Logička bomba je zlonamerni kod ugrađen u neki koristan program koji će se aktivirati kada se ispune odgovarajući uslovi. Kada se aktivira logička bomba se najčešće ponaša destruktivno. Za posledicu može imati uništavanje datoteka podataka, aplikativnih programa ili operativnog sistema¹². Virus i crvi često sadrže logičke bombe koje će izvršiti neku akciju u unapred određeno vreme ili ako se ispune neki uslovi. Oni koriste ovu tehniku kako bi se neprimetno proširili na druge sisteme. Destruktivne akcije virusa i crva često se izvode uz pomoć logičkih bombi.

5.2.3 Crvi

Zlonamerni softveri poznati pod nazivom crvi koriste računare domaćine da se reprodukuju. Crvi su samostalni programi koji se šire s jednog računara na drugi i za delovanje mu nije potreban domaćin. Kada crv uđe u vaš sistem, on dalje može da putuje sam. Velika opasnost kod crva jeste njihova sposobnost da se umnožavaju u ogromnim količinama. Kada se oslobode, novi crvi se šire veoma brzo, zagušujući mreže, što može da znači da ćete vi (i svi ostali) morati da čekate duplo duže da se otvore Web stranice na Internetu. Crv je potklasa virusa. Crv se obično širi bez pomoći korisnika i sam distribuira sopstvene potpune kopije (možda izmenjene) širom mreža. Može da zauzme memoriju ili propusni opseg mreže toliko da računar prestane da reaguje. Pošto crvima nije potreban „program-domaćin“ ili datoteka da bi putovali, oni takođe mogu da se krišom uvuku u vaš

¹¹ Pleskonjić D. Maček N. Đorđević B: Carić M. Sigurnost računarskih sistema i mreža, Makro knjiga 2007, str 297

¹² Dr Petković A. Forenzička revizija. Novi Sad 2010, str 282

sistem i omogućuje nekome drugome da daljinski kontroliše vaš računar. Sveži primeri crva jesu crvi Sasser i Blaster.

Oni se mogu podeliti u nekoliko osnovnih kategorija u zavisnosti od načina propagacije:

- ❖ Email crvi - najraširenija vrsta crva koja se širi koristeći attachment elektronske pošte. Najčešće funkcioniše na način da se pošalje na sve e-mail adrese koje pronađe na korisničkom računaru (npr. u Outlook adresaru)
- ❖ Instant messaging crvi - ovi crvi šire se putem programa za slanje poruka u realnom vremenu (MSN, ICQ i sl.). jedina razlika u odnosu na email crve je medijum putem koga se crv prenosi.
- ❖ IRC crvi - IRC crvi šire se putem IRC kanala za chat na identičan način kao i email crvi – slanjem zaraženih datoteka ili URL adresa koje vode na inficirane web stranice.
- ❖ File sharing crvi
- ❖ Internet crvi

5.2.4 Virusi

Virus je deo računarskog koda koji se prikači na program ili datoteku tako da može da se prenosi sa računara na računar, šireći pri tom zarazu. On može da ošteti hardver, softver ili podatke. Ne može sam da se reprodukuje ali zato može da osvoji ćelije drugog organizma i upotrebi reproduktivam, mehanizam svake ćelije domaćina da napravi svoju kopiju. Šteta koju mogu da izazovu ide od toga da poneki program postane privremeno neupotrebljiv, dok se ne nađe rezervna zdrava verzija, pa do uništenja logičke strukture diska i gubitka svih podataka i programa sa njega. Za razliku od crva virusi ne koriste mrežne resurse širenja ali se mogu širiti preko mreže kao deo nekog crva.

Virusi se mogu podeliti na nekoliko osnovnih kategorija, u zavisnosti od cilja svog napada :

- ❖ Virus datotečnog sistema
- ❖ Sistemski virusi
- ❖ Multipatite virusi
- ❖ Makro virusi

5.2.4.1 Virusi koji napadaju sisteme datoteka

Virusi ovog tipa za svoje širenje koriste jednu ili više vrsta sistema datoteka. Napadaju i inficiraju isključivo izvršne datoteke računarskih programa (ekstenzije datoteka .exe, .com, .bat, .sys, drv). Većina trajno ostaje u memoriji računara (engl. memory resident) što znači da

će prilikom sledećeg pokretanja neinficirani programi automatski postati inficirani. Prema metodama inficiranja virusi ovog tipa se dela na :

- ❖ Prepisujuće viruse
- ❖ Parazitske viruse
- ❖ Pridružujuće viruse
- ❖ Viruse startnog zapisa

5.2.4.2 Makro virusi

Napisani i ugrađeni su u dokumente koji se otvaraju onim aplikacijama iz paketa Microsoft Office koje koriste tehnologiju povezivanja i ugrađivanja objekata OLE2 (object linking and embedding).¹³ Karakteristika makro virusa je da su oni za razliku od klasičnih virusa, vezani za aplikaciju, a ne za operativni sistem ili platformu

Najrasprostranjeniji su zbog svoje jednostavne izrade i aktiviraju se otvaranjem datoteka (Word, Excel, Point) kad se kod virusa kopira u izvršni kod programa koji ga je otvorio. Prenose se kao izvršna komponenta u neizvršenom fajlu sa podacima. Mogu se proširiti i na druge kompjutere ukoliko se na oba kompjutera koristi dotična aplikacija i vrši se razmena inficiranog dokumenta. Makro virusi mogu se izvršavati na svakoj platformi na kojoj postoji ovakav program (i pripadajući interni jezik). Oni nisu ograničeni na pojedinačne kompjutere ili samo određeni operativni sistem. Podrazumeva se da makro virusi (uključujući i Excel makro viruse), mogu biti automatski detektovani i očišćeni korišćenjem zaštite u realnom vremenu. Zaštita od makro virusa sprovodi se podizanjem makro nivoa sigurnosti na najviši stepen

5.2.5 Špijunski programi (spyware)

Prate vaš rad i o tome obaveštavaju nekog drugog. Prisustvo špijunskog programa je obično teško otkriti. Postoje program koji se namerno instaliraju po firmama kako bi direktori imali uvida u to što im se radi na njihovom kompjuteru. Spyware se razlikuje od virusa i crva u tome što se obično ne replicira. Dizajniran je da iskorištava zaražene kompjutere za komercijalnu dobit. Često osim što krađu vaše informacije krađu i resurse vašeg računara i propusni opseg veze sa internetom. Gotovo da ne postoji podatak na vašem računaru koji spyware ne može prikupiti i poslati zlonamernom napadaču. Simtomi za pojavljivanje spyware-a su :

- ❖ Stalno pojavljivanje iskaćućih reklama
- ❖ Postavke računara su se promenile i ne mogu da se vrate na raniji status
- ❖ Web pretraživač ima dodatne komponente, koje nismo preuzeli

¹³ Pleskonjić D. Maček N. Đorđević B. Carić M. Sigurnost računarskih sistema i mreža
Makro knjiga 2007 , str 308

- ❖ Računar kao da usporava

Vrste spywear –a

- ❖ Adwer
- ❖ Kolačići
- ❖ Internet dialeri
- ❖ Hoaksi
- ❖ Trojanci

Top lista špijunskih programa :

- ❖ GatorCool
- ❖ Web Search
- ❖ 180 search Assisant
- ❖ Cydoor IST bar
- ❖ WhenU Desktop Bar

5.3 Zaštita od zlonamernih programa

Da bi uspeli da računar zaštitimo od zlonamernih progrma potrebno je da na svakom računaru postoje sledeći programi :

- ❖ **Antivirus** – projektovani su da traže viruse, obaveste korisnike kada ih nađu i uklone ih sa zaraženog diska ili fajla.¹⁴ Nadgleda memoriju računara u pokušaju detekcije zlonamernih programa i ukoliko detektuje zlonamerni program ,blokira izvršenje tog programa. Antivirus programi funkcionišu na principu upoređivanja podataka na disku sa podacima o virusima koji se nalaze u bazi antivirusa. Napredniji AV-i imaju razvijen sistem detekcije zlonamernih programa na osnovu njihove delatnosti čak i ako podaci o takvom programu ne postoje u bazi. Baza antivirusa mora sa vremena na vreme da se "update"-uje, tj. da se preuzme novija verzija baze koja sadrži nove detektovane viruse.
- ❖ **Firewall** - predstavlja softver i ima mogućnost da spreči neželjeni prenos podataka preko mreže . Ovakvi programi najčešće onemogućavaju korišćenje bug-ova (grečki) u operativnim sistemima ili nepravilnog podešavanja windows-a koji se mogu zloupotrebiti. Treba biti oprezan u rukovanju sa firewall programima jer se zbog nepravilnog rukovanja može desiti da totalno izgubite vezu sa internetom.
- ❖ **Anti - spayware**

¹⁴ Milosavljević M. Veinovic M. Grubor G. Poslovna informatika, Univerzitet Singidunum 2009,str 282

Korisnici čiji su računari inficirani zlonamernim programima često nisu ni svesni da je njihov računar inficiran i da je zloupotrebljen za dalju distribiciju tih programa. Voditi računa o tome koje Web lokacije posećujete i šta sa njih preuzimate. Pošto se danas zlonamerni programi granaju velikom brzinom veoma je bitno da se ažurira baza Anti virusnog programa pošto se otkrivanjem novih zlonamernih kodova nadograđuje baza virusa koja nakon toga sadrži deskripciju novih zlonamernih programa.¹⁵

Postoje različiti načini na koje se pojedinci i firme štite od nepoželjnih posetilaca ili softvera. Neki od tih načina su:

- ❖ Specijalni programi
- ❖ Mrežne barijere
- ❖ Biometrijska zaštita
- ❖ Etičko hakerisanje

6. Hakerisanje

6.1 Etnicko hakerisanje

Kada se sprovedu sve preporučene mere za zaštitu mreža i informacionih sistema od narušavanja sigurnosti, treba uraditi analizu i proveriti uspešnost zaštite. Osmišljeni su načini ispitivanja koji bi trebalo da pokažu koliko je zaštita pouzdana i efikasna. Međutim, oni koji napadaju mrežu stalno smišljaju nove načine i metode da ostvare svoje ciljeve. Da bi zaštitili mrežu, klijenti često angažuju hakere koji po dogovoru napadaju i proveravaju sigurnost, uz obavezu da svoja saznanja drže u tajnosti, da ih ne zloupotrebe i da ih prenesu samo organizaciji koja ih je angažovala i isključivo u svrhu unapređenja sigurnosti. Takvi hakeri se drugačije nazivaju i „etički hakeri“ ili „hakeri sa belim šeširom“. Oni uglavnom rade u raznim firmama koje se bave bezbednošću sistema. Etičko hakerisanje zahteva dosta strpljenja i vremena.

6.1.1. Etički haker

Etički haker je stručnjak za kompijutersku bezbednost koji je specijalizovan za testiranje sistema i mreža i sprovodi hakerske napade na zahtev vlasnika kompijuterskih sistema kako bi se proverila njihova bezbednost. Naziva se još i „haker sa belim šeširom“. Mnogi od njih su zaposleni u kompanijama koje se bave bezbednošću. Sa druge strane postoje „hakeri sa crnim šeširima“ ili zlonamerni hakeri koji pokušavaju da upadnu u sistem i

¹⁵ Dabić I. Malware, 2010 str 20

ukradu poverljive informacije ili da nanese neku štetu. Etički haker koristi istu metodologiju kao i njegove kolege sa ne tako plemenitim namerama. Razlika između hakera sa belim i crnim šeširima je upravo u motivima, jer etički haker propuste koje otkrije prijavljuje nadležnima, uz eventualne sugestije kako oni mogu biti popravljani, ne koristeći ih na zlonameran način. Smatra se da onim treba da budu osobe od poverenja. Imaju veliko iskustvo u poslu sa računarima i računarskim mrežama kao i u vezi sa programiranjem, instalacijom i administriranjem popularnih operativnih sistema.

Etički haker obavljajući svoj posao traži odgovor na sledeća pitanja:

- ❖ Šta može napadač da vidi na ciljnom sistemu?
- ❖ Šta može napadač da uradi s tim informacijama?
- ❖ Da li je neko primetio napadačev napad ili uspeh?

Na kraju piše izveštaj sa saznanjima koje je prikupio tokom procene i dostavlja je klijentima.

6.1.2 Deset zapovesti računarske etike

Institut za računarsku etiku (the computer ethics institute) je objavio 10 zapovesti računarske etike i rekao „ Ako prekršite neku zapovest nećete otići u pako ali ćete zato otići u zatvor “.

- ❖ Ne koristi računar da povredi drugog
- ❖ Ne mešaj se nepozvan u tuđ rad na računaru
- ❖ Ne njuškaj po tuđim datotekama
- ❖ Ne koristi računar da bi lažno svedočio
- ❖ Ne koristi računar da bi krao
- ❖ Ne koristi komercijalni softver koji nisi platio
- ❖ Ne korsi tuđe računarske resurse bez odobrenja ili nadoknade
- ❖ Ne prisvajaj sebi zasluge za tuđu intelektualnu svojinu
- ❖ Razmisli o posledicama koje će program koji pišeš ili sistem koji projektuješ imati na društvo
- ❖ Koristi računar samo na način koji ne ugrožava druge

7. Forenzički alati

Postoji veliki broj alata za digitalnu forenzičku istragu i analizu. Prilikom istrage i analize mora se jasno utvrditi koji alati će u najkraćem vremenskom periodu pomoći u postizanju odgovarajućeg cilja. To proističe iz aktuelnosti tzv. žive forenzike, online hitnog odgovorana

incident¹⁶. Alati se mogu podeliti u nekolikogrupa, pri čemu, po funkcijama koje obavljaju, ne moraju striktno da pripadaju samo grupi u koju su svrstani. To su :

- ❖ multifunkcionalni alati
- ❖ alati za napad i pregled sistema na net-u
- ❖ otvoreni kod/sistemski alati
- ❖ alati za kreiranje lozinke
- ❖ alati za retorički i incidentni odgovor
- ❖ alati za dupliranje odredišta
- ❖ alati za inspekciju sistema na mreži
- ❖ alati za inspekciju mreže
- ❖ alati za pomoć u istraživanju incidenata
- ❖ alati koji pomažu rekonstrukciju Inter-net aktivnosti
- ❖ uopšteni uređivači i pregledači

Glavni problem u vezi sa forenzičkim alatima su :

- ❖ Bagovi u softveru
- ❖ Promene u OS i hardveru računara
- ❖ Kompleksnost
- ❖ Nedostatak standarda i razvoj standarda
- ❖ Alati sa otvorenim izvornim kodom
- ❖ Počelo testiranje forenzičkih alata

7.1 Hardverski alati

Kako se brzo menjaju informaciono komunikacione tehnologije sistema, tako se zahteva i izbor novih forenzičkih alata za novi hardver. Kako se forenzički hardverski alati, radne stanice i serveri koriste intenzivno, zamenu treba planirati najmanje na dve godine. Snabdevači računarskih sistema nude širok asortiman forenzičkih radnih stanica, koje korisnik treba da prilagodi svojim potrebama. Forenzičke radne stanice se mogu podeliti u tri kategorije:

- ❖ **stacionarna radna stanica** (računarski sistem sa nekoliko kućišta za eksterne hard diskove i mnogo perifernih uređaja visokih performansi),
- ❖ **portabl radna stanica** (laptop računar sa ugrađenim LCD monitorom i

¹⁶ Kostic Z. Grubor G. Alati za digitalnu forenzičku istragu str 113

skoro istim brojem kućišta i perifernih uređaja kao i stacionarna radna stanica),

- ❖ **prenosna radna stanica** (obično laptop ugrađen u transportnu torbu sa manjim brojem perifernih uređaja).¹⁷

Digitalna forenzika bi trebalo da ima dosta različitih forenzičkih alata, softvera i hardvera da bi mogla da se izvrše svi potencijalni zadaci vezani za samu istragu kompijuterskog kriminala. Ako je moguće treba imati po nekoliko konfiguracija za istovremeni rad na različitim slučajevima. Problemi mogu nastati u podršci periferijskim uređajima koji mogu doći u konflikt ili da ne rade. Forenzičar mora da zna koliko periferijskih uređaja može da se poveže na sistem da bi on nesmetano radio. Prilikom odabira radne stanice treba birati onu koja može da omogući najveći broj proširenja.



Slika 8. Hardverski blokatori¹⁸

7.1.1. Blokatori upisivanja

Predstavljaju hardversko- softverske uređaje za sprečavanje upisivanja podataka na ispitani disk. Postoje i softverski i hardverski blokatori. Korišćenjem hardverskih blokatora upisivanja mogu se skinuti digitalni podaci sa brojnih tipova čvrstih diskova, a neki od njih su :

- ❖ IDE čvrsti diskovi 3,5 inča
- ❖ SATA čvrsti diskovi
- ❖ Notebook čvrsti diskovi
- ❖ Toshiba čvrsti diskovi

¹⁷ Milosavljevic M. Grubor G. Istraga kompijuterskog kriminala, Univerzitet Singidunum 2009, str 170

¹⁸ Milosavljevic M. Grubor G. Istraga kompijuterskog kriminala, Univerzitet Singidunum 2009 , str 174

8. Softverski alati

Softverski forenzički alati se dele u dve grupe :

- ❖ Aplikacije komandne linije
- ❖ GUI (graphics user interface) aplikacija

Aplikacije komandne linije su namenjene za izvršavanje samo jednog zadatka, kao što je SaveBack, alat na bazi DOS komandne linije. Za razliku od njih, **GUI aplikacije** su namenjene za obavljanje više forenzičkih funkcija, oni mogu obaviti većinu zadataka akvizicije. U ovu vrstu alata spadaju FTK i EnCase. Najbitnija funkcija ovih alata je ta što mogu u potpunosti da iskopiraju osumnjičeni disk

8.1 Softverski alat – EnCase

EnCase je programski alat namanjen forenzičkoj istrazi digitalnih dokaza. Smatra se jednim od najboljih i najčešće korišćenih softverskih forenzičkih alata. Omogućava i olakšava sudskim veštacima i IT stručnjacima istraživanje slučajeva, akviziciju i analizu dokaznog materijala. Odlikuje ga dobra podrška korisnicima i velika baza korisnika. Korišćenjem programa može se uraditi kompletna forenzička analiza, počevši od akvizicije do konačnog izveštaja. Druga važna osobina EnCase softvera je njegova mogućnost da odradi sliku diska korišćenjem mrežnog patch kablaili serial kabl.

EnCase softver omogućava korisnicima da kreiraju bootdisk koji će zaštititi podatke od toga da budu upisani na neki sumnjivi disk prilikom procesa pokretanja računara. Jednom kada se kompjuter pokrene i krene sa radom, forenzičar može da krene sa pravljenjem slike diska, bilo pomoću patch kabl ili serial kabl.

EnCase alat takođe poseduje mogućnost izveštavanja što omogućava istražiteljima da sačuvaju pronađene ključne reči, slike i da usnime lične komentare u formatu koji je lak za izveštavanje. Na taj način, informacije mogu da se odštampaju ili proslede mail-om pravnim zastupnicima koji su uključeni u slučaj. Međutim, za korišćenje ovog softvera, uglavnom je neophodna detaljna obuka.

12 . Međunarodni računovodstveni standard 38

*** Cilj **

Cilj ovog Standarda je da propiše računovodstvene postupke za nematerijalna sredstva koja nisu posebno obrađena drugim Međunarodnim računovodstvenim standardima. Ovaj Standard zahtijeva da subjekt prizna neko nematerijalno sredstvo ako, i samo ako su ispunjeni određeni uslovi. Ovaj Standard takođe uređuje način određivanja knjigovodstvene vrijednosti nematerijalnih sredstava i zahtijeva određena objavljivanja o nematerijalnim sredstvima

*** Delokrug ***

Ovaj Standard treba primijeniti u računovodstvu nematerijalnih sredstava, osim:

- ❖ nematerijalnih sredstava koja su obuhvaćena nekim drugim standardom
- ❖ finansijskih sredstava, kako su definisana MRS-om 32 -Finansijski instrumenti: Prezentacija
- ❖ pri priznavanju i mjerenju sredstava istraživanja i procjene mineralnih resursa (vidi MSFI 6 -Istraživanje i procjena mineralnih resursa); i
- ❖ izdataka za vađenje minerala, nafte, prirodnog plina i sličnih neobnovljivih resursa

Ovaj standard se ne primjenjuje na:

- ❖ nematerijalna sredstva koja se drže radi prodaje u sklopu redovnog poslovanja
- ❖ odložena porezna sredstva (vidjeti MRS 12 -Porez na dobit)
- ❖ najmove koji potpadaju u djelokrug MRS-a 17 -Najmovi
- ❖ sredstva koja proizlaze iz naknada zaposlenicima
- ❖ finansijska sredstva kao što je definisano MRS-om 39. Priznavanje i mjerenje nekih finansijskih sredstava uređuje i MRS 27 -Konsolidirani i odvojeni finansijski izvještaji
- ❖ MRS28 -Ulaganja u pridružene subjekte i MRS 31 -Udjeli uzajedničkim poduhvatima
- ❖ goodwill koji nastane iz poslovnih spajanja
- ❖ odložene troškove sticanja, kao i nematerijalna sredstva, koja proizlaze iz osiguravačevih ugovornih prava iz ugovora o osiguranju, definisanih u MSFI 4- Ugovori o osiguranjuMSFI 4 postavlja određene zahtjeve objavljivanja za odložene troškove sticanja, ali ne i zahtjeve za objavljivanje za navedena nematerijalna sredstva. Prema tome, zahtjevi objavljivanja iz ovog standarda se odnose i na navedena nematerijalna sredstva.

Nematerijalna sredstva

Subjekti često troše resurse ili stvaraju obaveze radi sticanja, razvoja, održavanja ili poboljšanja nematerijalnih resursa kao što su naučna i tehnička saznanja, projektovanje i implementacija novih procesa ili sistema, licence, intelektualno vlasništvo, tržišno znanje i zaštitni znakovi (uključujući trgovačke marke i izdavačke nazive). Uobičajeni primjeri stvari

obuhvaćenih ovim širokim pojmovima su računarski softveri, patent, autorska prava, filmovi, liste kupaca, založna prava, dozvole za ribarenje, uvozne kvote, franšize, odnosi s kupcima i dobavljačima, odanost kupaca, tržišni udjeli i marketinška prava bućih ekonomskih koristi. Ako neka stavka iz djelokruga ovog Standarda ne ispunjava uslove iz definicije nematerijalnog sredstva, svaki izdatak za sticanje ili interno stvaranje takve stavke se priznaje kao rashod u trenutku njegovog nastanka. Međutim, ako je stavka stećena poslovnim spajanjem, ona čini dio goodwilla koji se priznaje na datum sticanja ,

*** Indetifikacija ***

Definicija nematerijalnog sredstva nalaže da se nematerijalno sredstvo može identifikovati na način da bi se jasno razlikovalo od goodwilla. Goodwill priznat u sklopu poslovnog spajanja je sredstvo koje predstavlja buduće ekonomske koristi od ostalih sredstava stećenih poslovnim spajanjem koja nisu pojedinaćno identifikovana i odvojeno priznata. Buduće ekonomske koristi mogu nastati sinergijom stećenih identifikovanih sredstava ili iz sredstava koja pojedinaćno ne zadovoljavaju kriterije za priznavanje u finansijskim izveštajima.

Nematerijalno sredstvo se priznaje ako, i samo ako:

- ❖ je verovatno da će buduće ekonomske koristi, koje se mogu pripisati sredstvu, priticati subjektu; i
- ❖ se trošak nabavke tog sredstva može pouzdano izmeriti

Nematerijalno sredstvo se poćetno meri po trošku sticanja.

12.1 Tumačenje SIC 32

Subjekt može imati znatne izdatke radi razvoja i ažuriranja svojih web stranica za unutarnji i spoljni pristup. Web sajt oblikovan za spoljni pristup može biti korišteno u razne svrhe, kao promocija i oglašavanje vlastitih proizvoda i usluga, pružanje elektronskih usluga, te prodaja proizvoda i usluga. Web sajt koji ima unutarnji pristup može biti korišteno za pohranjivanje politika subjekta i pojedinosti o kupcima, te pretraživanje odgovarajućih informacija.

Faze razvoja web stranica:

- ❖ Planiranje – uključuje preduzimanje studija izvodljivosti, definišući ciljeve i specifikacije, ocenu pojedinih alternative zbor između njih.
- ❖ Razvoj informatičkih programa i infrastrukture - uključuje sticanje domene, nabavku i razvoj hardvera i operativnog softvera, instaliranje razvijenih informatičkih programa, te naglašeno ispitivanje
- ❖ Razvoj grafičkog dizajna - uključuje dizajniranje izgleda web stranice
- ❖ Razvoj informacionog sadržaja - uključuje kreiranje, pribavljanje, pripremu, i postavljanje informacija, bilo tekstualne ili grafičke prirode, na web mesto pre završetka razvoja web stranica. Ova informacija može biti pohranjena u zasebne baze koje su objedinjene u (ili s pristupom) web mjestu ili kodirane direktno u web stranicu.¹⁹

Kada je razvoj web stranica jednom dovršen, započinje operativna faza. U toku ove faze, subjekat održava i unapređuje informatičke programe, infrastrukturu, grafički dizajn i sadržaj web stranica.

Pitanja koja se javljaju kod računovodstvenog praćenja internih izdataka u vezi sa razvojem i funkcionisanjem sopstvenog web sajta entiteta za interni ili eksterni pristup su :

- ❖ Da li je web sajt interno generisana nematerijalna imovina na koju se odnose na IAS 38
- ❖ Adekvatni računovodstveni postupak sa takvim izdacima

Ovo tumačenje se ne odnosi na kupovinu, razvoj i funkcionisanje hardvera . Takav trošak je pokriven MRS-om 16. Dodatno, kad subjektu nastane izdatak za usluge provajdera internet izdaci se priznaju kao rashod u skladu sa IAS 1.88 i Okvirom kada su usluge izvršene.

MRS 38 se ne koristi za nematerijalna sredstva koja subjekt drži sa namerom prodaje u okviru redovnih poslovnih aktivnosti (vidjeti MRS 2 i MRS 11) niti na lizing koji spade u MRS 17. Prema tome, ovo tumačenje se ne odnosi na izdatke razvoja ili funkcionisanja web

¹⁹ <http://www.mfin.gov.rs/UserFiles/File/MRS/Tumacenje%20SIC-32%20-%20Nematerijalna%20imovina%20-%20Troskovi%20veb-sajta.pdf> – 25.03.2014

stranica (ili softvera web stranice) koje su namenjene za prodaju drugom subjektu. Kad je web sajt iznajmljuje putem operativnog lizinga, davalac lizinga primenjuje ovo tumačenje.

Kad je web sajt unajmljen putem finansijskog lizinga, davalac lizinga primenjuje ovo tumačenje nakon inicijalnog priznavanja iznajmljenog sredstva.

Vlastiti web sajt subjekta razvijen za interni i eksterni pristup, je interno kreirano nematerijalno sredstvo, i kao takvo je pod djelokrugom MRS-a 38.

Web sajt koji je entitet razvio se priznaje kao nematerijalna imovina ako i samo ako pored poštovanja opštih zahteva u vezi s priznavanjem i početnim mjerenje, opisan u MRS 38.21, entitet može zadovolji zahteve iz MRS 38.57. Konkretno, entitet može biti u stanju da zadovolji zahtev u vezi s pokazivanjem kako će web - stranica generisati verovatne buduće ekonomske korististi u skladu sa MRS 38.57 (d), kada, na primjer, web - stranica može generisati prihode, uključujući direktne prihode od mogućnosti da se vrše narudžbe. Entitet ne može pokazati kako će web - stranica, razvijen jedino ili primarno za promociju i oglašavanje njegovih proizvoda usluga i stvoriti buduće ekonomske koristi, i u skladu s tim, svi izdaci u vezi s razvojem takvog web - stranice se priznaju kao rashod kada nastanu.

Interni izdaci u vezi s razvojem i funkcioniranjem web stranice entiteta se računovodstveno obuhvaćaju u skladu sa MRS 38. Priroda svake aktivnosti za koju su izdaci nastali i faza razvoja web stranice ili faza pose razvoja se procenjuju radi određivanja primerenog računovodstvenog post upka.

13. Metode i tehnike digitalne forenzičke istrage

13.1 Istorijat

Kompjuterska forenzika je očuvanje , indentifikacija , ekstrakcija, tumačenje i dokumentacija računarskog dokaza²⁰. Kompjuterska forenzika je disciplina koja ima za cilj da prikupi, sačuva i prezentuje podatke koji su dobijeni sa medija za čuvanje podataka. Digitalna forenzika se kao nauka razvila relativno skoro, spada u mlađe naučne oblasti²¹. Sama forenzika vuče korene još iz Rimskog doba kada su krivične prijave podrazumevale javno iznošenje slučaja u Forumu, gde bi lice optuženo za krivično delo i podnosilac prijave javno raspravljao o ovome a osoba sa boljim argumentom bi pobedila. Sa razvojem tehnologije i kompjuterskog kriminala došlo je i do potrebe za specijalizacijom : tehničari digitalnog mesta koji prikupljaju digitalne dokaze, ljudi koji pregledaju dokaze i istraživači koji analiziraju sve raspoložive dokaze da bi izgradili slučaj. Ove specijalizacije nisu limitirane na policiju i razvijene su i na korporativnom nivou.

Prva škola forenzike je otvorena u Evropi u Lozani (Švajcarska) i to od strane Rudolfa Arčibalda Rajsa. Što se tiče digitalne forenzike istorija je malo drugačija. Sami računari su se pojavili tek sredinom XX veka , i tad još uvek nije postojao internet kao i digitalnog kriminala , pa za forenzikom tog tipa nije bilo potrebe. Početkom osamdesetih godina kada personalni računari postaju sve pristupačniji dolazi do njihove sve veće zloupotrebe tj do povećanja upotrebe kompjutera prilikom izvršenja kriminalnih radnji. Zbog toga je Federalni istražni biro 1984 godine oformio novu jedinicu Computer Analysis and Response Team (CART) koja je imala za cilj da se izbori sa sve većim brojem slučajeva koji su uključivali digitalne dokaze. ASCLO- LAB društvo je 2003 godine prihvatilo pojam digitalne forenzike i značaj digitalnog dokaza u rešavanju zločina. Kanada je prva zemlja koja je 1983 godine donela zakon koji delimično reguliše digitalni zločin, nakon nje sledi Amerika 1986 godine zatim Australija 1989 godine a potom i Engleska 1990 godine. Danas u Sjedinjenim Američkim Državama postoji više desetina koledža koji su specijalizovani za ovu oblast. SAD je trenutno lider u ovoj oblasti²². Prvi zabeležen napad na digitalnu infrastrukturu se desio 1988 godine od strane Roberta Morisa. Sjedinjene Američke Države i druge države uspostavile su

²⁰ The Best Damn Cybercrime and Digital Forensics book Period , Anthony Reyes, Jack Wiles 2007

²¹ <http://www.datasolutions.rs/srp/kompjuterska-forenzika/kompjuterska-forenzika-osnove.html> - 01.06.2014

²² http://en.wikipedia.org/wiki/Digital_forensics -01.06.2014

specijalizovane grupe radi istrage kompijuterskog kriminala na nacionalnom nivou. 1992 godine termin digitalna forenzika počinje da se koristi u stručnoj literaturi od strane Koliera i Spaula. Digitalna forenzika se i dalje suočava sa mnogo nerešenih pitanja. Simon Garinkel je 2010 godine identifikovao probleme sa kojima će se digitalna forenzika susresti u budućnosti.

13.2 Evolucija istražnih organa

Na početku istraživanja kompijuterskog kriminala bilo je uobičajeno da digitalni istražitelji koriste kompjuter koji je korišten za zločin radi uzimanja dokaza sa njega. Rizici pri ovom pristupu problem je što prilikom pregleda kompromitovanog sistema sa njega samog može doći do kontamiranja dokaza na način koji nije moguće opaziti. Uprkos tome postoje programi na UNIX platformi kao što je dd koji postoji još od 1980 godine i može da se koristi radi uzimanja izbrisanih podataka koji se nalaze na hard disku. DD može da se koristi za uzimanje podataka na fizičkom, logičkom ili na file system nivou. 1980-ih nisu široko korišćeni i zato mnoge pretrage digitalnih dokaza u to vreme izvođene su na nivou file system-a, zanemarujući izbrisane podatke.

Tako je bilo do ranih 90-ih godina dok nisu razvijeni alati kao što su SafeBack i DIBS koji omogućavaju kolekciju svih podataka na disku, a da pri tom ne menjaju digitalne dokaze. U isto vreme razvijeni su još neki alati kao što su Maresware i NTI. Razvili su ih pojedinci iz US International Revenue Service (IRS) da bi pomogli istražiteljima da procesiraju podatke na kompijuterskim diskovima. The Royal Canadian Mounted Police (RCMP) je takođe razvila specijalne alate za pregledanje kompjutera. Malo kasnije razvijeni su integrisani alatai za digitalnu istragu kao što su Encase, FTK od AccessData-e, X-ways Forensics, Ilook Investigator, koji još više olakšavaju istražni proces. Ovi alatai omogućavaju efikasniju istragu, i automatizuju uobičajene korake u digitalnoj istrazi koji se moraju preduzeti, prikazuju podatke u grafičkom interfejsu radi lakšeg opažanja važnih podataka. Nedavno je obnovljeno interesovanje za Linux kao platformu za digitalnu istragu i alate kao što su 4n6, Sluethkit i SMART koji su razvijeni sa grafičkim interfejsom takođe. Još sofisticiraniji alati koji vraćaju izbrisane podatke sa hard diskova postoje, ali oni su skupi za korporacije i koriste ih samo snage reda.

Postoji sličan napredak u evoluciji alata za prikupljanje dokaza na komunikacionim sistemima. U kasnim 80-im, objašnjeno je kako da se napravi “slika” mrežnog saobraćaja radi očuvanja istog kao dokaza. Mrežni alati za nadgledanje mreže kao što su tcdumd i Ethernal mogu da se koriste za “hvatanje” mrežnog saobraćaja ali nisu specijalizovani za hvatanje digitalnih dokaza. Komercijalni alati kao što su Carnivore, NetIntercept, NFR Security, NetWitness, and SilentRunner razvijeni su sa integrisanim pretragama, vizualizacijom, i analizirajućim sposobnostima kao pomoć digitalnim istražiteljima radi uzimanja podataka iz mrežnog saobraćaja.

Postoji sličan napredak u evoluciji alata za prikupljanje dokaza sa zatvorenih sistema kao što su mobilni telefoni, PDA uređaji i personalni digitalni asistenti. Uobičajeno je da istražitelji čitaju podatke sa ovih uređaja direktno, ali ovim pristupom se ne mogu čitati izbrisani podaci, ili se ne može pristupiti ovim uređajima uopšte ukoliko su zaštićeni šifrom. Zbog ovih problema razvijeni su alati kao što su ZERT, TULP, and Cards4Labs koji imaju mogućnost pristupa podacima koji su zaštićeni šifrom kao i izbrisanim podacima. Mnogo sofisticiranije tehnike uključujući električne mikroskope koji su u stanju da povrate kriptovane podatke sa zatvorenih sistema postoje ali su veoma skupe za mnoge svrhe. Tokom niza godina, nađene su grške u mnogim alataima za digitalnu forenzičku istragu, koji potencijalno prouzrokuju da dokazi budu izostavljeni ili pogrešno interpretirani. The National Institute of Standards and Testing je testirao neke alate. Nemoguće je testirati sve alate za digitalnu forenzičku istragu i zbog toga je predloženo, radi smanjenja kompleksnosti testiranja alata, da se dozvoli ljudima da vide source code kritičnih komponenata software. Omogućavanje source code-a programerima iz sveta omogućava „testerima“ da steknu bolje razumevanje programa i povećava šansu da se pronađu razne greške. Prihvatljivo je da timovi za razvoj komercijalnih alata žele da drže neke delove svojih programa u tajnosti zbog konkurencije ali određene operacije kao što su kopiranje podataka sa hard diska, su uobičajene i kritični i kao takve bi trebale da budu otvoreni standard. Da bi bili sigurni u neke rezultate moraju da izvrše validaciju svojih rezultata koristeći više alata.

Fokus digitalne istrage je neki digitalni uređaj koji je uključen u kriminalnu aktivnost. Uređaj je korišten da se poćini neka fizićka kriminalna aktivnost (primer. Ukoliko je osumnjićeni koristio internet da bi vršio istragu o kriminalnom aktu koji je naćinio (će nćiniti) ili je korišten za neku digitalnu aktivnost u virtuelnom okruženju koja krši polise (npr. u firmi) ili zakon. (npr. Napadać uspe da neautorizovano pristupi kompjuteru, korisnik “skida” sa interneta zabranjeni materijal, ili kada korisnik pošalje preteći e-mail.). Kada se datektuje prekršaj istraga poćinje.

Digitalna istraga je proces gde se razvijaju i testiraju hipoteze koje odgovaraju na pitanja o digitalnim događajima. Ovo se radi koristeći naućne metode gde se razvija hipoteza koristeći dokaze koji su naćeni a zatim se testira hipoteza pretražujući dodatne dokaze koji su u kontradikćiji sa hipotezom. Obuhvata postupak dolaženja do podataka i utvrđivanja vremena kada su bili uneti, modifikovani, distribuirani, korišćeni, uskladišćeni, sklonjeni, kao vremena kada su fajlovi bili kreirani, postavljeni, punjeni, modifikovani ili kada im se pristupilo.²³

Digitalni dokaz je svaka informacija u digitalnom obliku koja ima dokazujuću vrednost, i koja je ili uskladišćena ili prenesena u takvom obliku²⁴. Pojam digitalnog dokaza uključuje kompjuterski uskladišćene i generisane dokazne informacije, digitalizovani audio i video dokazne signale, signali sa digitalnog mobilnog telefona, informacije na digitalnih fax mašina i signali drugih digitalnih uređaja. Znaći, digitalni dokaz je bilo koja informacija generisana,

²³ Alati za digitalnu forenzićku istragu, Digital forensics tools, Zona Kostić, Gojko Grubor 2008 god.

²⁴ http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-19.pdf -02.06.2014

obrađivana, uskladištena ili prenesena u digitalnom obliku na koju se sud može osloniti kao merodavnom, tj. svaka binarna informacija, sastavljena od digitalnih 1 i 0, uskladištena ili prenesena u digitalnoj formi, kao i druge moguće kopije originalne digitalne informacije koje imaju dokazujuću vrednost i na koje se sud može osloniti, u kontekstu forenzičke akvizicije, analize i prezentacije.

KARAKTERISTIKE DIGITALNOG DOKAZA	OPIS
Tehnološka naprednost	Prikupljanje i analiza digitalnih dokaza mogu biti izuzetno teški jer često zahtevaju najnovije naučne metode i tehnologije. Naučni metodi koji se koriste moraju se konstantno unapređivati kako bi ispratili brz napredak tehnologije.
Fleksibilnost	Digitalni dokaz se može sastojati od svih vrsta elektronskih informacija kao što su slike, video i audio zapis, tekst
Mogućnost umnožavanja i modifikovanja	Digitalni dokazi se mogu lako menjati, skroz modifikovati i umnožavati bez ostavljanja traga. Prilikom mrežnog prenosa Informacija može biti modifikovana ili izgubljena.
Nevidljivost	Prilikom fnansijskih transakcija lične informacije kao što su IP adresa, korišćen web brauzer i ime računara se šalju Internetom. Sve ove informacije se mogu smatrati digitalnim dokazima ukoliko su relevantne i pouzdane.
Prelazi granice nadležnosti	Kompjutersko kriminalno delo se može započeti u jednoj zemlji a počiniti u bilo kojoj na svetu. Shodno tome digitalni dokaz se može nalaziti bilo gde. Različiti lokalni zakoni i nadležnosti su dodatna prepreka za prikupljanje digitlanih dokaza i gonjenje počinilaca.

Tabela I. Osnovne karakteristike digitalnog dokaza

Digitalna forenzička istraga je proces koji koristi nauku i tehnologiju radi analize digitalnih objekata i koji razvija i testira teorije, koje su prihvatljive na sudu, radi dobijanja odgovora o događajima koji su se desili. Digitalna forenzička istraga je uža forma digitalne istrage.

13.3 Digitalna forenzička istraga

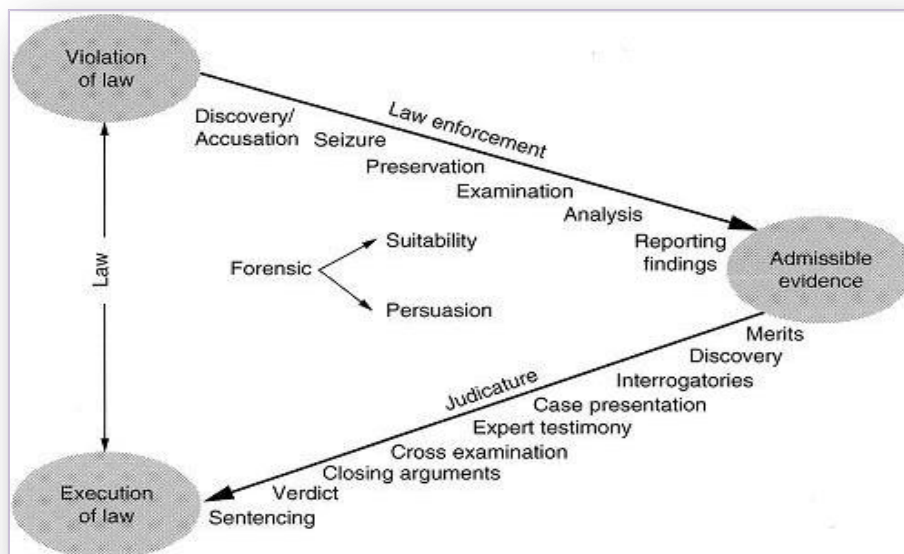
Digitalna forenzička istraga je proces koji koristi nauku i tehnologiju radi analize digitalnih objekata i koji razvija i testira teorije, koje su prihvatljive na sudu, radi dobijanja odgovora o događajima koji su se desili. Digitalna forenzička istraga je uža forma digitalne istrage. Jednako je značajna za javnu forenziku državnih organa i korporacijsku istragu kompjuterskog incidenta. U proteklih par godina sa razvojem digitalne tehnologije kao i interneta (globalne svetske mreže) mesto zločina se seli sve više u virtuelnu realnost. Digitalna forenzička istraga je nova disciplina forenzičke istrage koja se bavi upravo otkrivanjem incidenta, konfiskovanjem i akvizicijom, analizom, očuvanjem, i prezentovanjem digitalnih dokaza. Fokus digitalne istrage je digitalni uređaj koji je uključen u kriminalnu aktivnost. Uređaj je korišćen da se poćini neka fizička kriminalna aktivnost (primer. ukoliko je osumnjićeni koristio internet da bi vršio istragu o kriminalnom aktu koji je načinio ili je korišten za neku digitalnu aktivnost u virtuelnom okruženju koja krši polise (npr. u firmi) ili zakon. (npr. napadać uspe da neautorizovano pristupi kompjuteru, korisnik "skida" sa interneta zabranjeni materijal, ilik adakor isnik pošalje preteći e- mail.). Kada se datektuje prekršaj istraga poćinje.²⁵



Slika 9 : Proces digitalne forenzičke istrage

Kao što se realan svet prepliće sa virtuelnim svetom(virtuelnom realnošću) tako se i forenzička istraga fizičkog mesta zločina prepliće sa forenzičkom istragom digitalnog mesta zločina. Cilj bilo koje istrage je da se otkrije i prezentuje istina o nekom događaju. Usredsređićemo se na digitalnu istragu prevashodno, iako je cilj isti i za istragu fizičkog kriminala. Istražni proces je deo većeg oikvira tj pravnog okvira (sudstva).

²⁵ [http://www.academia.edu/5693529/ISMS_Digital_Forensic - IT Security Management Advanced techniques - Napradne tehnike sigurnosti IS - srpski-10.06.2014](http://www.academia.edu/5693529/ISMS_Digital_Forensic_-_IT_Security_Management_Advanced_techniques_-_Napradne_tehnike_sigurnosti_IS_-_srpski-10.06.2014)



Slika 10 : Prikaz procesa rešavanja slučaja

Istražni proces počinje sa tužbom, i napreduje kroz rukovanje dokazima do jasnih i preciznih objašnjenja činjenica i tehnika u svedočenju eksperata. Ova linearna reprezentacija korisna je za pravljenje procedura i krajnjeg izveštaja koji opisuje svaki korak neke istrage do donošenja odluka. U praksi istrage ne moraju biti linearne, kao što su izvršavanje nekih osnovnih analiza u fazi kolekcije, ili vraćanje na korak prikupljanja ukoliko je analiza ukazala na dodatne dokaze. Istrenirani, iskusni istražitelji će započeti istragu postavljajući sebi niz pitanja u cilju saznanja i odluke da li se zločin ili upad zaista dogodio. Odgovori na ova pitanja odrediće da li će se potpuna istraga nastaviti ili da li su resursi upotrebljiviji za neke druge stvari.

Proces po kojem je digitalni dokaz otkriven i primenjen sastoji se iz nekoliko koraka pri kojima se svaki od njih izvodi po strogim protokolima, proverenim metodama, i u nekim slučajevima proverenim alatima. Najvažnije je da uspeh ovog procesa najviše zavisi od iskustva i veština istražitelja, ljudi koji pregledaju dokaze i tehničara mesta zločina koji moraju da sarađuju da bi povezali dokaze zajedno i da bi razvili ubedljivi „account“(sadržaj) prekršaja.

Efektivnost istražnog procesa u mnogome zavisi od objektivnosti istražitelja. Neki sadržaji mogu da utiču na objektivno razmišljanje istražitelja kao i sličnosti između datog slučaj i nekog slučaja iz prošlosti. Sličnosti između određenih slučajeva mogu dovesti do preranog donošenja zaključaka na osnovu dela pregledanih dokaza, što kasnije može rezultirati

odbijanjem određenih dokaza na sudu kao i čitavog slučaja, zbog toga treba svakom slučaju pristupiti kao unikatnom iako je možda identičan nekom prethodnom. Moraju se ispoštovati sve naučne metode i određeni standardne procedure da bi bili sigurni da smo slučaj procesirali na pravilan način kao i da su sve naše hipoteze i dokazi zasnovani na naučnim metodama.

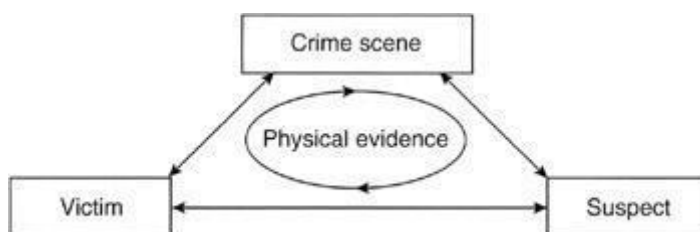
U poslednjem koraku istražnog procesa važno je imati na umu da se mogu pojaviti razlike između naučne i pravne istine koje mogu naići na nerazumevanje kod donosioca odluka. Ova faza je podjednako bitna kao i sve ostale faze. Kada se tehnički dokazi predstavljaju licima koja nemaju nikakvog ili vrlo malog znanja o tehnologijama, metodama koje se koriste radi prikupljanja digitalnih dokaza može doći do nesporazuma i nerazumevanja istih. Da bi se smanjili ovakvi rizici istražni proces kao i dokazi moraju biti jasno prezentovani na sudu.

13.4.Uloga digitalnog dokaza

Glavni cilj istrage u kompjuterskoj incidentnoj situaciji je, kao i slučaju klasičnog kriminala, izgraditi za pravosudne organe neboriv ili čvrst dokaz krivice ili dokaz za oslobađanje osumnjičenog, i/ili pravedno sankcionisanje učinjenog dela. Pojam digitalni dokaz je u ovom radu upotrebljen u smislu “utvrđivanja dokaza zloupotrebe u sistemima u kojima je primenjena digitalna tehnologija”, u širem smislu te reči.²⁶

Digitalni dokaz je potreban ali ne i dovoljan uslov za građenje slučaja.

Jedan od glavnih ciljeva u istrazi je povezivanje zločina sa izvršiocom otkrivanjem odgovarajućih veza između počinioca, žrtve, i mesta zločina. Svedoci mogu da identifikuju osumnjičenog ali dokazi o umešanosti individue su obično pouzdani. Prema „Locard's Exchange Principle” bilo šta, ili bilo ko, ko je bio prisutan na mestu zločina u samoj interakciji sa mestom zločina je odneo nešto sa mesta zločina, a i ostavio je nešto svoje na mestu zločina. Zbog ovoga moguće je dovesti određene dokaze u vezu sa počiniteljem.



Slika 11: Locard's Exchange Principle

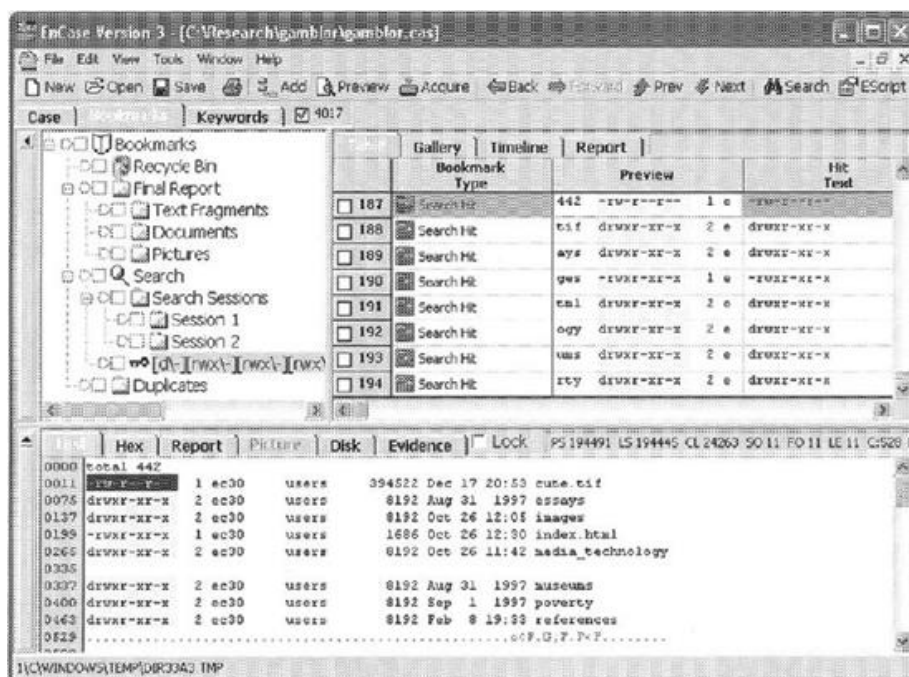
²⁶ http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-19.pdf-10.06.2014

Ovaj tip razmene svrstava dokaze u jednu od dve kategorije:

1. Dokazi sa atributima koji spadaju u grupu klasne karakteristike
2. Dokazi sa atributima koji spadaju u grupu individualne karakteristike

Još jedan primer Locard's Exchange Principle, u digitalnom okruženju. Kada uljez dobije neautorizovan pristup UNIX sistemu sa njegovog ličnog kompjutera, koristeći ukradeni dial-up račun i upload-uje različite alate na UNIX mašinu preko FTP-a (File transfer protocol), alati su tada locirani i na Windows i na UNIX sistemu. Određene karakteristike ovih alata biće iste na oba sistema, uključujući i na neke vremenske pečate i MD5 hash vrednosti.

Windows aplikacija korištena za konekciju na UNIX sistem (npr. Telnet, Secure CRT, SSH) mogu imati ciljnu IP adresu ili hostname. Listing direktorijuma sa UNIX sistema može biti nađen na hard diku uljeza ukoliko su smeštene na disk dok ih je Telnet, Secure CRT, SSH ili neki drugi program prikazivao na ekranu. Ukradeni račun i šifra su verovatno smešteni negde na kompjuteru uljeza, obično u log-u sniffer-a ili na listu ukradenih računa sa različitih sistema. FTP klijent koji je korišten (npr. WS_FTP) može da kreira log transfera alata na server.



Slika 12: Ostaci listinga direktorijuma sa UNIX sistema nađene na Windows kompjuteru koristeći „grep” funkciju u alatu EnCase

14. Istražne metodologije

Istražni proces koji je opisao Eoghan Casey prilazi metodologiji istrage sa pravnog stanovišta, dok metod Brajana Kerijera prilazi istrazi kao procesu same naučne istrage digitalnih dokaza, ne zanimajući ga pravni aspekti istrage.

Istražni proces Eoghan Casey-a ima veći okvir, ali je zato Brajanova metoda detaljnija, što se tiče same digitalne istrage i korenspondencije fizičke i digitalne istrage.

14.1 Istražne metodologije prema Eoghan Casey-u

Istražni proces se izvodi kroz niz rastućih stepenika konstruisanih tako da se pridržava kompletne rigorozne istrage kao i da osigura sigurno rukovanje dokazima i da smanji šanse za greškama koje su proizvod preuranjenih teorija i drugih potencijalnih zamki .Ovaj proces odnosi se na kriminalnu kao i na vojnu i korporacijsku istragu.



Slika 13 : Kategorije istražnog procesnog modela opisane kao niz stepenika

Kategorije na slici 13. bi trebale biti opšte. Jedinstvene metode i alati korišteni u svakoj kategoriji vezuju istražni proces za određeni forenzički domen.

Istražitelj i ispitivač rade zajedno kroz svaki korak u istrazi da bi na kraju prezentovali slučaj kompletno. Odavde će njihov posao preuzeti tužilaštvo ili ovlašćena lica sa viših položaja koji će odrediti u odnosu na iznete dokaze da li će se nastaviti slučaj ili će fokusirati resurse na druge stvari.

Menadžment slučaja igra vitalnu ulogu u slučaju i prolazi kroz sve korake u procesnom modelu. Obezbeđuje stabilnost i omogućava istražiteljima da efektivno povežu sve relevantne informacije zajedno u jednu jasnu celinu.

Faza analize istražnog procesa zasniva se na naučnim metodama. Počinje prikupljanjem činjenica i proverom istih, preko formiranja hipoteza i testiranja, aktivno tražeći dokaze koji osporavaju ili potvrđuju određenu hipotezu, i menjanjem zaključaka ukoliko se pronađu novi dokazi.

Generalno ovaj model omogućava istražiteljima i ispitivačima logičan sled događaja koji pruža:

- ❖ Prihvatanje - koraci i metode su stekle profesionalni konsenzus.
- ❖ Pouzdanost - metodi koji su korišteni mogu da se dokažu da bi potkrepili otkrića.
- ❖ Ponovljivost - proces mogu upotrebiti svi, nezavisno od prostora i vremena.
- ❖ Integritet - mora postojati mogućnost provere stanja dokaza, tj. da je stanje nepromenjeno.
- ❖ Uzrok i posledica - logička konekcija između osumnjičenih i dokaza.
- ❖ Dokumentacija – zapisi su bit dokaza svedočenja (svedočenje eksperata).

Svrha svih šest principa je da se formira što ubedljiviji argument zasnovan na činjenicama, ne na pretpostavkama, i to uzimajući u obzir pravni kriterijum za prihvatljivost.²⁷

Iako je proces opisan kao linearna progresija i koraci u ovoj metodi mogu biti ponovljeni na zahtev profesionalaca koji učestvuju u istrazi iako su oni završeni. Često je od suštinskog značaja da se poboljšaju ili povećaju metodi kao i alati za istragu. Mnogi koraci nisu samo digitalne prirode već mnogi delovi procesa funkcionišu primenjujući i integrišući metode i tehnike iz policijske nauke i kriminalistike kao pomoć. Postoji relacija između uzastopnih koraka. Veza je opisana kao ulaz i očekivani izlaz u svakom koraku, tako što rezultati jednog koraka služe kao ulaz sledećeg koraka.

²⁷ [http://www.academia.edu/5693529/ISMS_Digital_Forensic -
IT Security Management Advanced techniques - Napredne tehnike sigurnosti IS -
srpski-12.06.2014](http://www.academia.edu/5693529/ISMS_Digital_Forensic_-_IT_Security_Management_Advanced_techniques_-_Napredne_tehnike_sigurnosti_IS_-_srpski-12.06.2014)

14.1.1. Optužbe ili uzbuna incidentom

Svakii proces ima polaznu tačku. Ovaj korak može biti prepoznat kao signaliziran kao alarm nekog “intrusion detection” sistema, sistem administrator koji je pregledao neke logove sa servera ili “firewall”-a. Ovaj početni korak može biti i u tradicionalnijem obliku. Kada građanin prijavi moguću kriminalnu aktivnost šalje se istražni tim na fizičko mesto. Ovo mesto može sadržati elektronske naprave koje zahtevaju da jedan deo istrage ide digitalnim putem. Pošto kompjuteri preovlađuju u današnjem svetu postoji velika mogućnost da informacije dobijene iz digitalnih izvora imaju veze sa tradicionalnim kriminalom.

Kada primimo optužbu ili automatizovanu uzbunu o incidentu, važno je da se razmotri izvor i pouzdanost informacije. Važno je da se izmere snage, slabosti i drugi faktori povezani sa izvorom i uključi ljudski faktor kao i digitalni (Individua se žali na maltretiranje zbog pretećih poruka koje joj se prikazuju na ekranu. Uzrok može biti crv/virus. Alarm “Intrusion detection” sistema može prikazati neuspeli pokušaj upada u sistem ili može biti lažan alarm).

Prikupljanje nekih inicijalnih činjenica je potrebno pre nego što se pokrene potpuna istraga. Da bi se prikupili nek osnovne činjenice za pokretanje istrage obično je potrebno ući na mesto zločina (digitalnu mesto) i skenirati ili vrlo pažljivo “prošetati” kroz razne izvore podataka tražeći stavke koje mogu sadržati relevantne informacije.

Ovo je veoma delikatan korak u istrazi zato što svaka akcija na mestu zločina može promeniti dokaze. Takođe ulazak u istragu prerano bez pravilne autorizacije ili protokola može dovesti do kompromitacije čitavog slučaja. Zbog svega ovoga mora se izvesti minimum akcija da bi se odredilo da li je dalja istraga zagarantovana. U ovom koraku s e donose zaključci, zasnovani na malom broju dokaza, da li se kriminalni akt dogodio ili nije.

14.1.2 Procena vrednosti

Osoblje koje je uključeno u istražne aktivnosti obično je zauzeto sa više slučajeva ili ima dužnosti koje su ekvivalentne po važnosti. Davanje istražnih resursa je ograničeno, oni moraju da budu primenjeni tamo gde su najpotrebniji. Kako se ovaj korak u procesu izvodi varira u odnosu na istražna okruženja. U organima reda i mira sve sumnjive kriminalne aktivnosti moraju biti ispitane. U civilnom, poslovnom i vojnom sektoru sumnjive aktivnosti moraju biti ispitane ali politike i kontinuitet operacija često zamenjuje legalne aspekte kao glavno pitanje. Postavljaju se pitanja i pokušava se usmeravanje resursa na ozbiljnije probleme ili tamo gde su najefektniji.

Faktori koji doprinose ozbiljnosti nekog problema su pretnje fizičkih povreda, potencijal znatnih gubitaka, rizik od kompromitovanja ili ometanja sistema na većem nivou. Ukoliko se problem može zaustaviti brzo, ukoliko je malo ili nimalo štete, i ukoliko nema faktora pogoršanja, potpuna istraga ne mora biti sprovedena. Izlaz ovog koraka je odluka koja spada u jednu od dve osnovne kategorije.

Ne zahtevaju se sledeće akcije – sumnja se dokazala kao neopravdana. Raspoloživi podaci i informacije su dovoljni da ukazuju na to da zločin nije učinjen. Ova odluka mora da se dokumentuje sa detaljnim obrazloženjem, izveštajem, a zatim moraju da se resursi ponovo raspodele.

Nastavak primene istražnih resursa zasnovanih na važnosti dokaza pregledanih do ovog koraka zasnovanih na inicijalnim informacijama. Svi incidenti ili optužbe zaslužuju detaljnu inicijalnu istragu. Ova kategorija ima za cilj da nas informiše o različitosti praktičnoj kao i pravnog presedana koja je spojena sa iskustvom istražnog tima. Ekspertiza iz kombinacije iskustva i sertifikovanih treninga igra veliku ulogu u efektivnom rasuđivanju.

14.1.3 Protokoli Incidenta/Mesta zločina

Kada je odobrena potpuna istraga prvi izazov je da se sačuva mesto zločina i dokumentuje stanje i integritet predmeta sa mesta zločina. Da bi se smanjile šanse za grešku, povredu ili previd, koriste se standardni protokoli, prakse i procedure. Kada se sprovodi potpuna istraga prvi izazov je očuvanje i dokumentovanje stanja dokaza (digitalnih ili drugih) na mestu zločina.

Protokoli, prakse, i procedure se moraju primenjivati radi smanjenja procenata grešaka, previda ili povreda. Ko god da je odgovoran za osiguravanje mesta zločina, da li lica koja su prva odgovorila na incident ili digitalni istražitelji, moraju da prate dogovorene protokole. Ovi protokoli moraju da obuhvate i pitanja kao što su očuvanje zdravlja i sigurnosti (ograničavanje izlaganja štetnim materijama kao što su otrovni materijali ili hemikalije u laboratorijama droge ili potencijalno infektivne telesne tečnosti), o kojima se obaveštavaju drugi nadležni organi, i šta mora da se uradi ne bi li se osiguralo mesto zločina.

Proizvod ili izlaz iz ove faze je sigurno mesto zločina, gde je sav sadržaj upisan i snimljen, sa pratećim fotografijama i osnovnim dijagramima da bi se dokumentovale važne oblasti i predmeti. Dokaz je, u suštini, zamrznut na mestu.

Ovo okruženje je osnov za sve dalje korake i predstavlja temelj za sve naredne aktivnosti. Predmeti otkriveni u ovoj fazi ostaju nepromenjeni deo slučaja kroz sve njegove faze. Koraci koji slede služe da se pronađu i dodaju predmeti kao i atributi i detalji, veze, i provere koje su bitne za rekonstrukciju, vremenske odredbe i motive. U ovom koraku se samo identifikuju dokazi za koje se smatra da su od važnosti za slučaj, ne radi se prikupljanje, analiza itd.

14.1.4 Identifikacija ili zaplena

Kada je mesto osigurano, potencijalni dokazi navodnog zločina ili incidenta moraju biti konfiskovani. Jasne procedure i razumevanje potrebnih pravnih kriterijuma su od suštinskog značaja pre nego što se nastavi sa procedurom uspešno. Cilj ove faze nije da se konfiskuje sve što se primeti na mestu zločina (bilo da je to fizičko ili virtuelno) već da se napravi razuman odabir objekata koj treba konfiskovati, i mora se dokumentovati i opravdati svaka aktivnost koja se napravi.

Dokumentacija prati sve korake istražnog procesa ali je najvažnija pri konfiskovanju digitalnih dokaza. Neophodno je da se sačuvaju detalji o svakom delu konfiskovanog dokaza zbog uspostavljanja autentičnosti i lanca odgovornosti. Na primer mnogobrojni objekti i fotografije istih, snimanje serijskih brojeva i dokumentovanja ko je rukovao dokazima, pomaže da se prati odakle je svaki deo dokaza došao i gde je otišao posle prikupljanja. Standardni obrasci i procedure pomažu u održavanju dokumentacije.²⁸

U tradicionalnom kontekstu, konfiskovanje (privremeno oduzimanje) implicira “uzimanje materijala”. U digitalnom svetu, vrši se konfiskovanje predmeta takođe, ali sva stanja ili delovi stanja određenih predmeta mogu da se izgube odmah po konfiskovanju zbog nestabilnosti elektronskih uređaja ili njihovog dizajna. Mnogi moderni kompjuteri imaju velike količine RAM-a (Random Access Memory) gde su podaci o procesima, informacije o stanju mreže i mnoge druge. Kada se sistem isključi trenutni sadržaj RAM memorije je izgubljen i može samo deo informacija da se povрати.

Izlaz ove faze proizilazi iz stanja trijaže. Inventar, ne samo fizičkih elektronskih komponenti nego i svojstva tih komponenti koje ukazuju na moguće mrežno povezivanje između lokalnog i udaljenog uređaja takođe treba biti katalogizovano. Ovo je veoma bitno zato što će dati

²⁸ Srdjan Atanasijević, Digitalna forenzika, Visoka tehnička škola Kragujevac, 2012. skripta str 92

šansu istražiteljima da prikupe važno stanje i karakterne informacije pre nego što se isključi napajanje i izvrši konfiskovanje. Iako istraga garantuje konfiskovanje elektronskih komponenti, trebaju se uzeti u obzir metode i tehnike koje pružaju mogućnost prikupljanja određenih osetljivih sistemskih i mrežnih informacija.

U ovom koraku, dobro trenirano osoblje koje odgovara prvo na incident, mogu da im se daju instrukcije kako da pronađu i zaplene dokaze za kasnije procesiranje koje izvode digitalni istražitelji. Dva korisna dokumenta koji prikazuju efektivne prakse za zaplenjivanje digitalnih dokaza pomenuti su ovde ukratko. Ove informacije mogu biti obrađene tako da budu u skladu sa politikama organizacije i mogu biti korištene kao podsetnik za istražitelje kao procedure, ček-liste, i formulare.

The Good Practices Guide for Computer Based Electronic Evidence, koje je publikovala Asocijacija “Chief Police Officers” u Velikoj Britaniji (NHCTU 2003), pruža početnu tačku za diskusiju inicijalnih koraka o rukovanju digitalnih dokaza. Ovaj vodič je dizajniran da pokrije najuobičajenije tipove kompjutera : elektronske organizatore i IBM kompatabilne laptopove ili desktopove sa modemom. Kao dodatak praktičnim savetima vodič pruža četiri globalna principa koja su od koristi svima koji se bave digitalnim dokazima.

Princip 1: Ne sme se preduzeti nijedna akcija od strane policije ili agenata koja može da promeni podatke koji se nalaze na kompjuteru ili na nekom drugom medijumu koji pruža pomoć na sudu.

Princip 2: U izuzetnim slučajevima gde osoba odredi da je neophodno da pristupi originalnim podacima koje se drže na ciljnom kompjuteru, osoba mora biti kompetentna da to odradi i da pruži obrazloženje i važnost kao i implikacije preduzetih akcija.

Princip 3: Trag provera ili snimak svih procesa primenjenih na kompjuterski dokaz mora biti kreiran i sačuvan. Nezavisna treća strana mora biti u stanju da pregleda te procese i dobije iste rezultate po tim zapisima.

Princip 4: Oficir zadužen za slučaj odgovoran je za primenu kako ovih principa tako i zakonskih. Ovo se odnosi na posedovanje i pristup informacijama koje se nalaze u kompjuteru. Ovi principi moraju da važe za sve koji pristupaju kompjuteru, za ili bilo koje korišćenje uređaja za kopiranje, moraju biti u skladu sa ovim zakonima i principima.

US Department of Justice je napravilo koristan vodič Electronic Crime Scene Investigation: A Guide for First Responders (USDOJ 2001). Ovaj vodič razmatra različite izvore digitalnih

dokaza. Sadrži slike da bi pomogle osoblju koje prvo odgovara na incident, i opisuje kako se kojim rukuje. Ovi dokumenti su korisni za razvijanje standardnih operativnih procedura (SOP) koje pokrivaju jednostavne istrage sa par kompjutera. SOP su neophodne za izbegavanje grešaka, osiguravajući da se najbolji mogući metodi koriste, i povećava verovatnoću da dva forenzička istražitelja dođu do istih zaključaka kada pregledaju dokaze.

Treba imati na umu da digitalni dokazi dolaze u mnogim formama: “audit trails, application logs, badge reader logs, biometrics data, application metadata, Internet service provider logs, intrusion detection system reports, firewall logs, network traffic, and database contents and transaction records (npr. Oracle NET8 or 9 logs)”. S obzirom na ovo identifikovanje i zaplena svih dostupnih digitalni dokaza je težak zadatak. Više tehničkih procedura je potrebno da bi se izašlo na kraj sa velikim serverima ili dokazima koji su rašireni preko mreže. Takođe situacije koje nisu pokrivene nijednom procedurom iskrсну. Zbog ovoga je važno da se razvije solidno znanje forenzike I da se nauči da se primenjuju generalni principi kreativno. Inicijalni intervjui moraju da se izvedu da bi se dobile informacije o tome ko je umešan. Sta ljudi znaju, šta je nepoznato, i koje druge informacije treba da se sakupe.

14.1.5 Čuvanje

Radeći sa konfiskovanim komponentama istražitelji moraju obezbediti nepromenljivost potencijalno osetljivih dokaza. Odgovarajuće akcije moraju biti preduzete radi očuvanja integriteta kako fizičkih tako i digitalnih dokaza. Ključ uspeha ove faze su metode i alati koji se koriste. Njihova tačnost kao i pouzdanost, kao i stručnost istražitelja mogu biti dovedene u pitanje od strane saveta optuženog ukoliko se radi o krivičnom postupku. Istražitelji moraju da obezbede da promenljivo stanje konfiskovanih komponenti bude osigurano tako da ne dođe do bilo kakvih promena. Drugačije rečeno, moraju se preduzeti pravilne akcije kako bi se osigurala nepromenljivost potencijalnih dokaza, digitalnih i fizičkih. Metode i alati igraju ključnu ulogu u ovom procesu. Njihova tačnost i pouzdanost kao i profesionalna upotreba mogu biti predmet ispitivanja suprotne strane ukoliko dođe do podizanja optužnice. Ovi isti kriterijumi daju i strani koja diže optužnicu potrebno poverenje da nastavi sa preporukama svojih istražitelja.

Mnogim stručnjacima u ovom polju ovde počinje prava digitalna istraga. Ovo je generalno prvi korak u procesu koji koristi uobičajene alate određenog tipa. Izlaz iz ove faze je obično grupa dupliranih kopija digitalnih dokaza iz svih izvora. Ovom fazom se postiže to da je originalni materijal katalogizovan i smešten u odgovarajuće kontrolisano okruženje, u nemodifikovanom stanju. Dobijena je identična kopija originalnog materijala koja dalje služi za pregledanje kako se istraga nastavlja.

14.1.6 Oporavak podataka

Pre nego što se uradi potpuna analiza sačuvanih izvora digitalnih dokaza, neophodno je ekstrahovati podatke koji su izbrisani, sakriveni, kamuflirani, ili koji su iz nekih drugih razloga nedostupni za pregledanje koristeći operativni sistem ili specijalni fajl sistem. U nekim slučajevima, može biti neophodno da se rekonstruišu delovi podataka da bi se oporavio neki objekat. Kada je god moguće ovaj proces treba uraditi na kopijama originalnih digitalnih dokaza iz faze čuvanja

U ovom koraku fokus je na oporavku svih nedostupnih podataka bili oni od značaja za slučaj (incident) ili ne. Cilj je da se identifikuju, i ukoliko je to moguće učine vidljivim, svi podaci koji mogu biti prepoznati da pripadaju određenom tipu podataka. Izlaz iz ove faze je maksimalni dostupni sadržaj za istražitelje koji im omogućuje da pređu u sledeću fazu procesa. Pruža najkompletniju vremensku liniju podataka i može pružiti uvid u motive počinioca ukoliko je konkretan dokaz odlučnosti pronađen ili snimljen.

14.1.7 Žetva

Do početka ove faze svi potencijalni digitalni dokazi koji imaju veze sa slučajem ili incidentom su dostupni istražiteljima. Ova faza u procesu je gde stvarna pretraga počinje, gde konkretne činjenice dobijaju oblik koji podržava ili opovrgava hipoteze koje je izgradio istražni tim. Prikuplja se materijala iz očuvanog i oporavljenog izvora. Ovo prikupljanje se vrši po kategorijama dokaza a ne po sadržaju podataka, kontekstu, ili interpretaciji. Istražitelj će tražiti određene kategorije koje imaju određene klasne karakteristike, koje iz iskustva ili treninga, izgledaju ili se zna da su u vezi sa glavnim činjenicama slučaja ili incidenta koje su znane do ove tačke istrage.²⁹

Na primer, optužba koja je povezana sa dečijom pornografijom zahteva vizuelne digitalne dokaze u standardnom kompjuterskom grafičkog formata GIF ili JPEG. Zbog toga istražitelji će najverovatnije tražiti postojanje fajlova određenih karakteristika iz ovih grafičkih formata. U slučajevima incidenta povezanih sa “hakovanjem” istražitelji mogu fokusirati pažnju na kolekciju fajlova ili objekata koji su u vezi sa određenim rootkit-ovima ili grupama izvršnih fajlova (executables), skripti (scripts) i interpretirani kod koji je poznat kao pomoć krakerima u uspešnom kompromitovanju sistema.

²⁹ Srdjan Atanasijević, Digitalna forenzika , Visoka tehnička škola Kragujevac 2012, skripta str 94

Poznavanje tehnologija i alata koji se koriste, zajedno sa razumevanjem osnovnih mehanizama i tehničkih principa koji su uključeni su od najvećeg značaja za ovu fazu. Uobičajeni izlaz su velike organizovane grupe digitalnih podataka koji imaju potencijalne dokaze. To je prvi sloj organizacione strukture koje će istražitelji razložiti u koracima koji slede.

14.1.8 Redukcija

U ovom koraku se sprovode aktivnosti koje pomažu da se eliminišu ili ciljaju specifične objekte prikupljenih podataka potencijalno povezane sa istragom. Ovaj korak je u stvari odvajanje kukolja od žita. Odluka da li da se odstrani ili ostavi bazirana je na eksternim atributima podataka kao što su hash ili “checksum” vrednosti, tipovi podataka itd. Ova faza ostaje fokusirana na opštu strukturu objekta i obično ne zalazi u sadržaj ili kontekst. Rezultat (izlaz) ovog koraka istražnog procesa je najmanja grupa digitalnih informacija koja ima najviše potencijala da sadrži podatke koje imaju istražnu vrednost. Kriterijum koji se koristi za eliminisanje određenih podataka je veoma važan i može biti preispitan od strane sudije, porote, ili bilo kojeg autorizovanog donosioca odluka.

14.1.9 Organizacija i pretraga

Da bi se lakše prošla analiza, savetuje se da se organizuje smanjena grupa materijala iz prethodnog koraka, grupisanje, označavanje, ili drugačije, stavljajući ih u značajne jedinice. U ovom koraku od koristi može biti grupisanje određenih fajlova fizički radi ubrzanja analize. Mogu biti smešteni u grupe koristeći foldere ili odvojene medije za skladištenje ili u nekim slučajevima baze podataka koje ukazuju na katalogizovane fajl sistem objekte za laku i tačne reference izbegavajući korišćenje kapacitete rudimentarnog pretraživanja koje nude najveći broj operativnih sistema.

Primarna svrha ove aktivnosti je lakše pronalaženje i identifikovanje podataka kroz korak analize, koji se kasnije koriste pri kreiranju krajnjih izveštaja i svedočenja. Ova aktivnost može ugraditi različite nivoe tehnologija pretrage radi pomaganja istražitelja u lociranju potencijalnih dokaza. Može se kreirati indeks pretrage radi kreiranja efikasnijih pregleda materijala, zbog pomoći pri identifikovanju relevantnih, irelevantnih, i privilegovanog materijala. Svi alati ili tehnologije koje se koriste u ovom pogledu moraju da prate sve prihvaćene standarde koji postoje. Rezultat ove faze su atributi organizacije podataka koji omogućavaju ponovljivost i tačnost analitičkih aktivnosti koje slede.

14.1.10 Analiza

Ovaj korak obuhvata detaljnu pretragu podataka koji su identifikovani u prethodnim koracima. Tehničari koji su zaduženi za ovaj deo teži će da pregledaju detaljno, unutrašnje attribute podataka, kao što je tekst i njegovo značenje, ili specifični format video i audio zapisa. Klasne i individualne karakteristike pronađene u ovom koraku koriste se u pravljenju veza, određivanju porekla podataka, i konačno lociranju prekršioca. Generalno analiza se sastoji od sledećih kategorija (ali nije ograničena na njih):

- ❖ **Procena situacije (Assessment (content and context))** — Čitljivi (ili vidljivi) digitalni podaci imaju sadržaj koji je moguće pregledati i pomoću njih odrediti faktore kao što su sredstva, motivi i prilike.
- ❖ **Eksperimentisanje (Experimentation)** — Probanje novih neisprobanih metoda i tehnika. Moraju biti zasnovane na naučnoj osnovi. Svako eksperimentisanje mora biti rigorozno dokumentovano tako da zajednica, sudovi, imaju priliku da ih testiraju. Na kraju eksperimenti vode do odbijanja istih ili generalnog prihvatanja.
- ❖ **Fuzija i korelacija (Fusion and correlation)** — Za vreme istrage, informacije se su prikupljene iz mnogih izvora (digitalnih i ne-digitalnih). Cela priča ne može da se sklopi samo od jednih ili drugih informacija. Podaci moraju da se fuzionišu da bi se sklopila cela priča. Primer fuzije bi bila vremenska linija događaja koja se odnosi na određeni slučaj ili incident. Svaki zločin ili incident ima hronološku komponentu gde događaji ili akcije popunjavaju vremenske delove. Ovo nam daje odgovore na pitanja gde, kada, i nekada kako? Vremenski delovi koji predstavljaju sve aktivnosti fuzionišu se iz različitih izvora (digitalnih i ne-digitalnih) kao što su digitalni podaci, zapisi telefonske kompanije, e-mail poruke, izjave osumnjičenih i svedoka. Korelacija ne prati samo hronološki događaje već i vezu između događaja.
- ❖ **Provera (Validation)** — Ovo je izlaz iz faze analize i predstavlja razumna otkrića koja istražitelji predlažu porotnicima ili nekim drugim licima ovlašćenim za donošenje odluka kao pozitivan dokaz za krivično gonjenje ili oslobađajuću presudu.

Greška pri ocenjivanju digitalnih dokaza može da dovede do konfuzije i pogrešnih zaključaka.

Primer ovakvog slučaja (LISER v. SMITH 2003).³⁰

14.1.11 Izveštavanje

Konačni izveštaji trebaju da sadrže važne detalje o svakom koraku istrage, uključujući upućivanje na protokole kojih su se istražitelji pridržavali, metode korišćene u zapleni, dokumentovanju, kolekciji, čuvanju, rekonstrukciji, organizovanju, i pretrazi ključnih dokaza. Veći deo izveštaja bavi se analizama koje su dovele do svakog zaključka ili opisom dokaza

³⁰ Srdjan Atanasijević, Digitalna forenzika, Visoka tehnička škola Kragujevac 2012, skripta str 95

koji podržavaju te zaključke. Nijedan zaključak ne bi trebalo zapisati bez opisa dokaza koji ga podržavaju i analize. Takođe izveštaj prikazuje i objektivnost istražitelja tako što opisuje alternativne teorije koje su odbačene zato što su bile kontradiktorne ili ne podržane dokazima.

14.1.12. Ubeđivanje i svedočenje

Značajana količina truda je potrebna da se pripremi za ispitivanje i prenošenje tehničkih pitanja u jasnom obliku. Zbog toga ,ovaj korak u procesu zahteva tehnike i metode koje se koriste kao pomoć analitičaru ili ekspertu da prevede tehnološke i inženjerske detalje u razumljivu priču za diskusiju sa donosiocima odluka.

15. Istražna metodologija prema Brian Carreir-u

- ❖ Model mora biti zasnovan na postojećoj teoriji fizičke istrage.
- ❖ Model mora da bude praktičan i da sprovodi iste korake koje sledi stvarna istraga.
- ❖ Model mora biti generički (dovoljno opšti) u odnosu na tehnologiju, ne sme biti vezan za tekuću tehnologiju.
- ❖ Model mora biti dovoljno specifičan tako da za svaku fazu mogu da se razviju opšti generalni zahtevi.
- ❖ Model mora biti apstraktan i primenjiv za zvaničnu istragu, korporacijsku istragu, i reakciju na kompjuterski incident.

Za ovaj rad korištena je literatura koja definiše fizičke forenzičke procedure sa ciljem traženja modela koji bi se mogli primeniti na digitalnu forenzičku analizu, kompjuterski incident.

Umesto da tretiramo kompjuter kao neki predmet koji se nalazi na sceni na kojoj se odigrao zločin mi ćemo smatrati kompjuter kao sekundarnu scenu zločina. Gledano sa te tačke gledišta isti principi istrage će biti korišćeni kao kad se ispituje soba u kojoj se dogodio neki zločin, iako će specifične metode i korišćena tehnologija biti različiti.

Druge knjige i naučni radovi su koristili termine poput “Digitalna scena zločina” ili “Kompjuterska scena zločina” za bilo koju scenu zločina u kojoj se nalazi neki kompjuter. Mi ćemo naprotiv koristiti termin “digitalna scena zločina” za digitalno

okruženje koje se nalazi u hardveru i softveru. Postoje drugi radovi koje koriste termin digitalna scena zločina na isti način kao u ovom radu, ali oni ne primenjuju procedure fizičke forenzičke istrage.

Istraga kompjutera ili nekog drugog digitalnog uređaja ima sličnosti sa istragom fizičke scene zločina zbog količine potencijalnih dokaza. Kao što fizička scena može biti obrađena za identifikaciju velikog broja dokaza isto tako i kompjuter, iako je samo jedan fizički predmet, može biti obrađen za identifikaciju mnoštva dokaza kao što su identitet, vlasništvo podataka, vreme i pozicija. Digitalni podaci mogu biti analizirani na isti način kao i fizički dokazi.

Model procesa prezentovan u ovom radu nije prvi model procesa digitalne istrage. Različiti modeli su predloženi u prošlosti i korišćeni za organizaciju procedure digitalne istrage i pisanje materijala za obuku. U novom poglavlju ćemo prezentovati dva modela za forenzičku istragu: korporacijski model i zvanični model procesa istrage.

15.1 Korporacijski model istrage

Korporacijska istraga se može smatrati predistražnim postupkom zvanične istrage kompijuterskog kriminala. Odvija se u tri faze :

- ❖ Pokretanje istrage
- ❖ Određivanje karaktera kompijuterskog incidenta
- ❖ Analiza prikupljenih digitalnih podataka

Praksa je pokazala da se efikasni rezultati dobijaju izvršenjem 6 Rosemblatovih koraka:

- ❖ Eliminisanje očiglednosti
- ❖ Postavljanje hipoteze o napadu
- ❖ Rekonstrukcija krivičnog dela
- ❖ Otkrivanje traga do osumnjičenog računara
- ❖ Analiza izvornog , ciljnog i posrednog računara
- ❖ Prikupljanje dokaza

Nakon ovih šest koraka treba predati analize i prikupljenje dokaze korporacijskom ili zvaničnom organu istrage za dalji postupak.

Rekonstrukcija napada predstavlja čitanje log datoteka na celom putu napada, pri čemu se javljaju sledeći problemi:

- ❖ Log datoteke su izmenjene ,ne postoje ili su neadekvatne
- ❖ Isprekidana zaustavljanja izvora napada i računara žrtve
- ❖ Uskraćena saradnja administratora posrednih računara
- ❖ Lažiranje IP adrese
- ❖ Izmenjena log datoteka napadnutog računara ili primenjeni drugi trikovi za maskiranje neovlašćenog pristupa

- ❖ Samo jedan neovlašćeni pokušaj pristupa ³¹

Prikupljanje dokaza i predavanje dokaznog materijala korporacijskim ili zvaničnim organima istrage vrši se isključivo po odobrenju vlasnika napadnutog sistema i odluci korporacije.

Funkcionalni korporacijski model istražnog postupka može se opisati sledećim fazama:

- ❖ **Priprema za incident:** sa odgovarajućom obukom i infrastrukturom
- ❖ **Detekcija incidenta:** identifikovati sumnjivi incident
- ❖ **Prva reakcija:** prepoznati i potvrditi da se incident dogodio, sakupiti preliminarne, nestabilne i posredne dokaze (koji se vremenom degradiraju)
- ❖ **Formulisanje strategije reakcije:** na bazi poznatih indikatora
- ❖ **Dupliranje:** napraviti fizičku mirror sliku kompromitovanog sistema
- ❖ **Istraga:** ispitati sistem radi identifikacije ko, šta i kako je izvršio napad
- ❖ **Implementacija mera zaštite:** izolovati kompromitovan sistem pre nego što je vraćen u normalni režim rada
- ❖ **Nadzor mreže:** posmatrati mrežu radi identifikacije novih (ponovljenih) napada
- ❖ **Oporavak:** vratiti sistem u originalno stanje sa dodatnim merama zaštite
- ❖ **Izveštavanje:** dokumentovati reakciju na incident (kriminal) i izvestiti
- ❖ **Završna faza:** revidirati saniranje incidenta i eventualno poboljšati proces. ³²

15.1.1 Uspostavljanje tima za upravljanje kompjuterskim incidentom

Korporacijski tim za upravljanje kompjuterskim incidentom treba da bude centralizovan za sve delove korporacije. Tim može biti uspostavljen od kompetentnih zaposlenih koji obavljaju redovne poslovne zadatke, a u timu rade po potrebi i u slučaju glavnog kompjuterskog incidenta. Neki ili svi članovi tima mogu biti iznajmljeni što predstavlja dodatnu ranjivost korporacije. Velike korporacije mogu imati poseban tim samo za digitalnu forenzičku istragu, akviziciju i analizu.

Tim za upravljanje bezbednosnim kompijuterskim incidentom treba da uključi sledeće uloge/profile zaposlenih ili iznajmljenih specijalista:

- ❖ Menadžer zaštite informacija
- ❖ Administrator računarskog sistema/mreže

³¹ http://www.itvestak.org.rs/ziteh_10/zbornik_radova/Nikacevic%20Vladan%20-%20Korporacijska%20istraga%20kompjuterskog%20kriminala.pdf-17.06.2014

³² Uglješa Georgijević, Integrirani model procesa digitalne forenzičke istrage skripta str 3

- ❖ Specijalista za upravljanje i kontrolu bezbednosnog rizika
- ❖ Kontrolor sistema kvaliteta
- ❖ Predstavnici drugih timova
- ❖ Digitalni forenzičar
- ❖ Pravnik organizacije
- ❖ Menadžer za upravljanje ljudskim resursima ³³

Ključni nedostatak centralizovanog upravljanja kompjuterskim incidentom i sistemom zaštite u celini, može biti činjenica da se postepeno klasična paradigma savremenih malicioznih , hakerskih napada sve više pomera na centralizovane entitete za upravljanje zaštitom informacija u korporaciji.

Uspeh uspostavljanja korporacijskog tima za upravljanje kompijuterskim incidentom sa sopstvenim kapacitetima za korporacijsku digitalnu forenzičku istragu u najvećoj meri zavisi od podrške menadžmenta korporacije. Potrebno je ubediti menadžment da je takav tim neophodan za korporaciju i da može doneti vidljive koristi.³⁴

Pažnju treba usmeriti na razvoj opšte spremnosti korporacije da upravlja kompleksnim kompijuterskim incidentom, analogno pripremi za protiv požarnu zaštitu. Praksa zaštite nesumnjivo potvrđuje da je spremnost kompanije da razvijaju i implementiraju svoje adekvatne sisteme zaštite informacija, proporcionalna količini akumuliranog straha menadžmenta od posledica koje su imale druge slične korporacije. Neophodno je je razviti svest o potrebi zaštite i kod drugih grupa zaposlenih uključujući krajnje korisnike, i obezbediti opšte razumevanje i podršku cele organizacije.

Takođe je značajno i uspostavljanje pouzdane, potpune i efikasne komunikacije između zaposlenih i interventnog tima i obrnuto. Treba odrediti odgovorna lica i navesti kontaktne informacije članova tima iz različitih delova IKT sistema i organizacije za potrebe sakupljanja digitalnih dokaza, a takođe i kontaktne informacije sa spoljnim saradnicima i konsultantima. Politika korporacijske digitalne forenzičke istrage treba da zahteva obaveznu obuku za sticanje različitih zvanja i veštine iz oblasti IKT sistema. Sama obuka treba da bude zasnovana na poznavanju metoda i procedura, razumevanju novih forenzičkih tehnika i alata. Cilj je da u samoj organizaciji kao i u samom timu za upravljanje kompjuterskim kriminalom bude što više sertifikovanih članova iz oblasti kao što je CISSP za zaštitu IKT sistema.

³³ Milosavljevic M, Grubor G. Istraga kompijuterskog kriminala, Univerzitet Singidunum 2009 ,str 30

³⁴ Milosavljevic M, Grubor G. Istraga kompijuterskog kriminala Univerzitet Singidunum 2009, str 31

15.1.2 Procedura određivanja karaktera kompijuterskog kriminala

Prosečan kompijuterski incident najčešće nije kriminalni akt. U samom toku predistražnih i istražnih radnji treba verovati indikacijama istrage a ne statističkim pokazateljima. Na osnovu rezultata procesa određivanja karaktera kompijuterskog incidenta, čak i površnog preliminarnog uvida u posledice incidenta, vlasnik sistema donosi odluku da li da nastavi istragu unutar organizacije sopstvenim kapacitetima ili da iznajmi sopstvene saradnike.

Korporacijske, kombinovane ili zvanične istrage karaktera kompijuterskog incidenta treba:

- ❖ Napraviti detaljan izveštaj o svim nalazima, dokumentovati izveštaj i nalaze i dati predlog/preporuku za dalji postupak
- ❖ Dokazne materijale pažljivo markirati obojenom samoljepljivom nalepnicom, sortirati u odvojene koverta sa detaljnim oznakama o sadržaju svake. Oznaka treba da ima mesta za potpis lica koje preuzima dokazni materijal u daljem postupku.
- ❖ Kada se neki fajl memoriše kao digitalni dokaz mora se zaštititi od izmene. Za zaštitu integriteta treba koristiti standardni hash program koji daje jedinstven sažetak fajla. Svaka i najmanja promena u fajlu digitalnog dokaza menja hash vrednost fajla. Zatim se sažetak fajla zajedno sa fajlom digitalnog dokaza šifrira javnim ključem asimetričnog algoritma i memoriše. Tako zaštićen dokaz se kad zatreba dešifrira privatnim ključem i verifikuje se hash vrednost sa istim hash algoritmom.
- ❖ Dobro je u izveštaju pomenuti svaki pojedinačni dokaz pod jedinstvenim brojem evidencije na koverti, što olakšava kasnije snalaženje.
- ❖ Izveštaj treba početi sa kratkim sadržajem incidenta u kojem se opisuje incident, metod istraživanja i generalne zaključke po redosledu izvedenih dokaza.
- ❖ Vremenska evolucija je najbolji dokaz za zaključivanje o incidentu. Ako se obezbedi dokaz o vremenskoj liniji upada u sistem, u svim log fajlovima mrežnih zređaja i napadnutog računara, onda je to čvrst dokaz za slučaj.
- ❖ Najniži rezultat istrage mora biti dovoljan za odluku na nivou organizacije šta dalje uraditi sa istragom. Obustaviti je ili nastaviti u organizaciji ili predati zvaničnim organima. Ta odluka najviše zavisi od prezentacije zaključka i materijalnih dokaza za svaki slučaj.
- ❖ Izveštaj treba završiti sa preporukom kako sprečiti da se incident ne ponovi i šta dalje učiniti sa istražnim postupkom.³⁵

³⁵ Milosavljevic M, Grubor G. Istraga kompijuterskog kriminala Univerzitet Singidunum, 2009 str 32

15.1.3 Model troškova korporacijske forenzičke istrage

Da bi korporacija uspela da uspostavi zahteve za digitalnu forenzičku laboratoriju i rad na terenu treba da sadrži specifikaciju kategorija neophodnih hardverskih i softverskih forenzičkih alata ,kao što su forenzički računarski sistemi za akviziciju, analizu i testiranje,blokatori upisivanja,komercijalni alati zatvorenog izvornog koda,alati Linux otvorenog koda i druga mobilna laboratorijska oprema.

Politika zaštite korporacije na kraju treba da preporuči referentne izvore za obuku iz oblasti digitalne forenzičke istrage kao što su : web lokacije,relativni casopisi i relevantni alati-komercijalni sa zatvorenim izvornim kodom.

Kad se kompjuterski incident dogodi, kritičan faktor je brzina reakcije. U početnoj praksi forenzičke istrage kompijuterskog kriminala, pokazalo se da su podaci otkriveni u toku prvih sedam dana bili kritični za uspešan oporavak.Danas je to vreme znatno kraće i reda je nekoliko časova.

Za donošenje odluke o uključivanju internog ili eksternog tima u digitalnu forenzičku istragu,organizacija treba da razmotri i izbalansira sledeće faktore:

- ❖ Troškove
- ❖ Vreme odgovora
- ❖ Osetljivost podataka³⁶

Jednostavan model troškova forenzičkog ispitivanja digitalnih uređaja pretpostavlja da postoji skup nekompatibilnih a različitih tehnologija i očekivani broj uređaja za forenzičko ispitivanje i da razvoj metoda za forenzičku akviziciju i analizu ima neke fiksne troškove.Pretpostavlja se da su ovi troškovi isti za jednu tehnologiju, iako je u praksi skuplji rezervni inženjering autorskog formata digitalnih podataka , nego razvoj softvera za procesiranje otvorenog standarda.

U ovom modelu mere se troškovi porasta forenzičke akvizicije i analize zbog nekompatibilnosti platformi, odnosno formata .Model pretpostavlja da je $F \gg MC$ pa su ukupni troškovi $c(M)$ za analizu digitalnih uređaja jednaki:

$$C(M) = F * |M| + MC * \sum m_l$$

³⁶ Milosavljevic M, Grubor G. Istraga kompijuterskog kriminala Univerzitet Singidunum, 2009 str 33

gde je :

M- broj nekompatibilnih platformi digitalnih uređaja

i – broj različitih tehnologija digitalnih uređaja

mi – očekivani broj uređaja digitalnih uređaja

F – visoki fiksni troškovi ekstrakcije digitalnih uređaja

MC – marginalni troškovi ispitivanja

U visoko distribuiranom zatvorenom okruženju sa mnogo nekompatibilnih formata, $|M|$ je veliki pa su i uključeni troškovi veliki. Troškovi su mnogo niži ako je sistem baziran samo na nekoliko otvorenih standarda.

Vreme odogovora na sam kompjuterski incident postaje sve kraći. Personal lociran na lokaciji incidenta može inicirati forenzičku istragu znatno brže od iznajmljenog tima. Za fizički distribuirane organizacije personal na lokaciji incidenta može brže reagovati nego tim iz centra organizacije.³⁷

Osetljivost podataka utiče na to da organizacija odustane da angažuje spoljni forenzički tim koji treba za analizu da uzme forenzičku kopiju čvrstog diska i pri tom ima pristup svim podacima, pošto na disku mogu da se čuvaju važne privatne informacije, finansijski izveštaji ili neke druge osetljive informacije.

Forenzičke tehnike i alati korisni su i za mnoge druge tipove zadataka kao što su:

- ❖ Otkrivanje grešaka
- ❖ Monitorisanje log datoteka
- ❖ Oporavak podataka
- ❖ Akvizicija podataka
- ❖ Obaveze po dužnosti/usklađenost sa regulativom

Primarni korisnici forenzičkih alata i tehnika unutar neke organizacije dele se u sledeće grupe:

- ❖ Istražitelj
- ❖ IKT Profesionalci
- ❖ Tim za upravljanje kompjuterskim incidentom

³⁷ Milosavljevic M, Grubor G. Istraga kompjuterskog kriminala Univerzitet Singidunum, 2009 str 35

15.2 Tim za istragu kompijuterskog kriminala

Istragu kompijuterskog kriminala mogu vršiti samo visoko specijalizovani stručni kadrovi u interventnim timovima nadležnih državnih organa sa odgovarajućim kapacitetima. Takav pristup omogućava valjanu istragu i način da se sakupe, sačuvaju i na sudu veštače digitalni dokazi o izvršenom kompijuterskom kriminalu.

15.2.1 Interventni tim za korporacijsku istragu kompijuterskog kriminala

Praksa organizacije je da izvrši vlastitu inicijalnu istragu kompijuterskog incidenta na nivou organizacije, da utvrdi karakter incidenta i tek onda donese odluku o pozivanju zvaničnih organa istrage kompijuterskog kriminala. Uloga korporacijskih organa za istragu zloupotreba u IKT sistemu ograničena je zato što većina organizacija nije dovoljno dobro opremljena odgovarajućim kapacitetima za forenzičku istragu i analizu, i što mnogi organi istrage nemaju sva zakonska ovlašćenja za otkrivanje traga do napadača i zaplenu računarskih sistema napadača kao dokaznog materijala. Jedno od boljih rešenja je da se anganžuje stručni konsultant za inicijalnu istragu, akviziciju i forenzičku analizu digitalnih dokaza i treba voditi istragu vlastitim snagama najmanje do trenutka utvrđivanja prirode incidenta i donošenja odluke o tome da li treba ili ne treba uključivati zvanične organe u sam proces istrage. Može se formirati sopstveni tim za brzo reagovanje i istragu kompijuterskog incidenta, a ako postoji neka praznina u timu popuniti je pridruženim (pomoćnim) članovima – stručnim konsultantom koji je najčešće tehnički ekspert u oblasti zaštite IKT sistema, kontrole sistema zaštite i digitalnim forenzičarom. Konsultant koji se angažuje može biti i privatna informatička firma sa znanjem u ovoj oblasti, kadrovski i materijalno obezbeđeni i osposobljeni za istragu i forenzičku analizu digitalnih dokaza.

15.2.2 Formiranje korporacijskog interventnog kibernetičkog tima

Pojam interventnog kibernetičkog tima odnosi se na CIRT (Computer Incident Response Teams) ili ređe na CERT (Computer Emergency Response Teams) tipove kombinovanih, stručnih timova koje treba formirati, obučiti i sa njima rukovoditi. Oni obavljaju planski prema utvrđenoj politici zaštite sve radnje opisane u slučaju kompijuterskog incidenta. Za formiranje kibernetičkih interventnih CIRT timova treba definisati organizacione i tehničke standarde, radne procedure i standarde dobre prakse, i nabaviti opremu sa potrebnim tehnologijama (tehnikama i forenzičkim alatima).

15.2.3 Metodologija rada kibernetičkih interventnih timova

U istražnom postupku CIRT tim koristi metodologiju kojom obezbeđuje sledeće:

- ❖ Zaštitu prava osumnjičenih do mere koju diktira tekuća politika organizacije.
- ❖ Propisno sakupljanje, čuvanje i dokumentovanje digitalnih dokaza.
- ❖ Donošenje zaključaka sa činjenicama i dokazima.
- ❖ Vođenje kompletne istrage bez izmene digitalnih dokaza i uticaja izvana.
- ❖ Zadržavanje odgovarajuće poverljivosti istrage.
- ❖ Odgovarajuće vođenje istrage da se zaštiti IS organizacije od ponovljenog izlaganja incidentu.
- ❖ Korišćenje standardizovane tehnike i alata za akviziciju (otkrivanje i sakupljanje), forenzičku analizu, skladištenje i čuvanje digitalnih kompjuterskih dokaza. Osnovni alati su: portabl hardversko-softverski alat za bekapiranje i mirorisanje diskova, foto/digitalne kamere i softverski alati za forenzičku analizu.
- ❖ Sakupljanje, označavanje i čuvanje digitalnih dokaza u lancu istrage u skladu sa standardizovanim procedurom.
- ❖ Pripremu i izradu izveštaja za nadležne organe (CIO ili zvanični organ istrage) u skladu sa standardizovanim procedurom.³⁸

15.2.4 Rezultati korporacijske istrage kompijuterskog incidenta

Istraga kompijuterskog kriminala i zloupotreba IKT sistema često se završava bez hapšenja, suđenja i sankcionisanja počinioca. Sve to desava iz više razloga:

- ❖ Gubljenje traga, kada prođe suviše vremena od incidenta i nema dokaza
- ❖ Nekompletnog logovanja, ili uopšte nema logovanja
- ❖ Cena istrage je veća nego gubici nastali usled incidenta i nije rentabilno nastaviti istragu
- ❖ Veliki prostor skrivanja počinioca a incident se dogodio samo jedanput sa malo ili bez imalo dokaza
- ❖ Incident nije sasvim određen, nije jasno da li je, ili nije bezbedonosni incident
- ❖ Ne može se nepobitno ukazati na počinioca i nema dovoljno dokaza
- ❖ Postoji politički, ili drugi pritisak da se istraga zaustavi
- ❖ Zataškivanje istrage³⁹

³⁸ Mr Miodrag Đorđević, dipl. inž. Ministarstvo odbrane SCG, Resursi za istragu kompijuterskog sadržaja skripta str 7

³⁹ Milosavljevic M, Grubor G. Istraga kompijuterskog kriminala Univerzitet Singidunum, 2009str 48

Ako se izvrši i kompletira istraga kompijuterskog incidenta obavezno je da se dostavi izveštaj o istrazi. Izveštaj se dostavlja vlasniku sistema i on dalje odlučuje o sudbini istrage, a takođe može da se dostavi i zvaničnim organima istrage za dalji pravosudni postupak.

15.3 Zvanični model istrage

Ova istraga uključuje policijske organe istrage, specijalno tužilaštvo i specijalno sudstvo za borbu protiv visokotehnološkog (kompjuterskog) kriminala. Ovi organi rade u skladu sa raznim zakonima kao što su : Zakon o krivičnom postupku, Zakon o borbi protiv visokotehnološkog kriminala, Zakon o zaštiti informacija i informacionih sistema, Zakon o digitalnom dokazu, Zakon o elektronskom potpisu, Zakon o elektronskoj trgovini i razni drugi zakoni koji regulišu elektronsko poslovanje .

Zvanični organi istrage treba da rade prema strogo utvrđenim standardnim operativnim procedurama (SOP) za: pretragu, privremeno oduzimanje i ispitivanje računarskih sistema i drugih mrežnih uređaja, akviziciju digitalnih podataka/ dokaza sa različitih platformi i slika u cilju otkrivanja validnih digitalnih dokaza. Istražni organi moraju mnogo dobro da poznaju zakone i propise .

Prilikom utvrđivanja karaktera krivičnog dela, istražni organi traže odgovore na mnoga pitanja kao što su:

1. Šta je bilo sredstvo izvršenja krivičnog dela?
2. Da li su računarski sistem i mreža poslužili kao jednostavan prolaz za izvršavanje krivičnog dela?
3. Da li je u pitanju krađa, provala ili vandalizam u sistemu?
4. Da li je napadač ugrozio nečiju privatnost i druga prava, ili uznemiravao?

Računarski sistem ili mreza se koriste kao sredstvo za izvršenje krivičnog dela, kao što je pištolj kod ubistva.

U izgradnji slučaja krivičnog dela mogu se razlikovati tri glavne faze :

- ❖ postojanje slučaja izvršenja krivičnog dela,
- ❖ istraga krivičnog dela i
- ❖ suđenje.

Opšti proces zvanične istrage se sastoji iz četiri faze, i unutar svake faze se nalazi po nekoliko koraka.

A to su:

- ❖ inicijalna istraga,
- ❖ ulazak u trag napadaču,
- ❖ otkrivanje identiteta napadača,
- ❖ hapšenje.

Zvanični proces istrage kreće od prijave krivičnog dela policiji. Nakon toga istražni organi prikupljaju dokaze za pokretanje tužbe. Zatim policija upoznaje tužioca koji obezbeđuje nalog za istragu od istražnog sudije i pokreće zvaničnu istragu. Sa sudskim nalogom organi istrage mogu legalno privremeno da oduzimaju osumnjičeni računarski sistem ili fizičku sliku čvrstog diska, radi forenzičke akvizicije i analize digitalnih dokaza .

Pre privremenog oduzimanja računarskog sistema, istražitelj dostavlja preliminarne dokaze o osnovanoj sumnji tužiocu za visokotehnološki kriminal i zahteva nalog za pretragu. Specijalni tužilac podnosi specijalnom sudu za visokotehnološki kriminal zahtev za nalog za pretres imovine osumnjičenog u kojem iznosi činjenice o predistražnom postupku i prilaže dokaze. Na osnovu ovog zahteva i dokaza o osnovanoj sumnji, specijalni sudija izdaje nalog za pretres stana i računarskog sistema osumnjičenog .

16. Životni ciklus analize i pretrage dokaza

Analiza i pretraga dokaza slučaja može se odvijati na više načina. Postoje više tipova i zavise od obima slučaja kao i specifičnosti slučaja.

Vodopad: Svi koraci se odvijaju sekvencijalno jedan za drugim. Svaki korak se temeljno sprovodi. Svaki digitalni istražitelj radi na svom slučaju i radi pretrage na svim nivoima i u svim oblastima. Svaki digitalni istražitelj ima alat koji najbolje poznaje. Digitalni istražitelj treba proveriti svoja otkrića upotrebom nekog drugog alata, da bi bio siguran u svoja otkrića. Ovaj model nije najbolji jer se svet digitalne tehnologije mnogo brzo razvija tako da ni jedan digitalni istražitelj ne može da ima znanje iz svih oblasti kao i rad svih alata za digitalnu istragu. Različiti alati pružaju različite mogućnosti pretrage.

Zbog ovih razloga ukoliko je laboratorija za forenzičku istragu u mogućnosti možda treba koristiti više istražitelja koji koriste različite alate na istom slučaju. Ovo je dobro radi same provere alata kao i tehnika prikupljana digitalnih dokaza jer postoji mogućnost upoređivanja dokaza dobijenih različitim metodama, tehnikama, i alatima. (sve tehnike, metode, alati moraju biti zasnovani na naučnim metodama). Kada se završi kompletna pretraga istražitelji upoređuju rezultate i sumiraju otkrića. Moguće je pretraga određenih delova dokaza i na određenom nivou radi dobijanja dodatnih dokaza ili potvrđivanja dobijenih dokaza.

Spirala: Spirala je metod koji omogućava da metod vodopada bude fleksibilniji. Ovo je ciklus koji se sastoji od niza manjih vodopada. Progres se odigrava u manjim koracima i posle svakog koraka se upoređuju rezultati, a zatim se vrši dodatna pretraga radi dobijanja dodatnih dokaza ili radi potvrđivanja dobijenih. Ukoliko je sve ovo završeno može se pristupiti sledećoj spirali u kojoj se izvršava obimnija pretraga i tako dalje dok se ne izvrši kompletna analiza. Ovom metodom, u zavisnosti od slučaja možemo sistem pretražiti brže, ali takođe i mnogo sporije.

Iterativni razvoj: Metod spirale je dobar ali istražitelji imaju potrebu za analizom koja ne traje predugo. Slučaj se može procesirati paralelno u iteracijama dobijajući na brzini. Prikupe se bitne informacije o slučaju, a zatim se slučaj deli u manje celine koje se daju različitim grupama istražitelja. Male grupe istražitelja rade svaki na svojoj iteraciji u isto vreme. Slučaj se analizira brže jer istražitelji rade na različitim delovima slučaja u isto vreme. Na kraju sve informacije se sumiraju i prave upoređivanja između timova. Ukoliko je potrebno, određeni timovi mogu napraviti dodatne pretrage radi dobijanja dodatnih dokaza iz određene oblasti slučaja.

Prednost metode vodopada je u slučajevima gde se materijal koji se pretražuje nalazi u manjim količinama ili se informacije nalaze na jednom sistemu (Windows ili Unix ili Mac). Još jedna prednost je u tome što za ovakvu metodologiju analize nije potreban veliki broj

istražitelja. (1 ili 2). Mane su mu brzina procesiranja slučaja, i nemogućnost jednog istražitelja poznavanja svih operativnih sistema, programa, hardvera i velikog broja alata za pretragu.

Prednost metode spirale je u tome što se posle svakog malog koraka (malog vodopada) radi dodatna provera i pretraga može da se u svakom sledećem preusmeri na pretragu za drugom vrstom digitalnih dokaza. Ova metodologija takođe ne zahteva veliki broj istražitelja ali samimi tim i brzina procesiranja slučaja nije na velikom nivou.

Prednost iterativne metode je u brzini procesiranja slučaja i fleksibilnosti kao i dodatnoj proveru jer više istražitelja koji procesiraju jedan deo informacija sa slučaja vide više i iz različitih uglova. Takođe svaki tim je specijalizovan za određeni deo sistema. Ukoliko je sistem koji se analizira mreže kompjutera neke firme (agencije), postoje sistemi koji su na više različitih operativnih sistema i koriste različite programe. Takođe tu je i veliki broj informacija koje se moraju procesirati. Ovaj metod je dobar ukoliko postoji mogućnost za većim brojem istražitelja koji su specijalizovani u različitim oblastima. Ovaj metod ima prednost u pretragama velikih sistema i odlikuje se velikom brzinom i sigurnošću.

17.Vrste forenzičkih alata za digitalnu forenzičku istragu

Podele: Alata za digitalnu forenzičku istragu na hardverske i softverske alate.

Zatim prema oblasti upotrebe:

- ❖ alati za analiziranje i snimanje mrežnog saobraćaja (tcdump , Ethereal, Carnivore, NetIntercept, NFR Security, NetWitness, and SilentRunner)
- ❖ alati za analiziranje sadržaja pojedinačnog kompjutera (Encase, FTK od AccesData-e, X-ways Forensics, Ilook Investigator)
- ❖ alati za analizu digitalnih uređaja (npr. pda, mobilnih, itd), (ZERT, TULP, and Cards4Labs)

Prema kodu:

- ❖ “Open source” programi(4n6, Sluethkit i SMART...)
- ❖ Licencirani programi(Encase, FTK od AccesData-e, X-ways Forensics, Ilook Investigator , Carnivore, NetIntercept, NFR Security, NetWitness, and SilentRunner)

Prema platformi na kojoj rade:

- ❖ alati koji rade na Windows platformi(Encase, FTK od AccesData-e, X-ways Forensics, Ilook Investigator)
- ❖ alati koji rade na Linux platformi(4n6, Sluethkit...)

Prema fazi procesa koji obavljaju:

- ❖ alati za pravljenje sterilnih medijuma
- ❖ alati za pravljenje kopije dokaza (pravljenje „slike“ sistema (mirror))
- ❖ alati za oporavak podataka
- ❖ alati za dekriptovanje podataka (razbijanje šifara)
- ❖ alati za analizu digitalnog materijala
- ❖ alati za dokumentaciju

Jedan alat može spadati i pod više različitih grupa. Opšte prihvaćeno mišljenje je da svi programi za digitalnu istragu trebaju biti “open source” ali tako ne misle i proizvođači programa, jer bi tim konkurencija imala uvid u određene prednosti nekog programa. Ako ne celi programi da budu “open source” onda bi određeni delovi program trebaju biti, jer se time postiže da istražitelji mogu da provere da li program radi kako treba, da li možda pogrešno interpretira neke rezultate itd. Što više ljudi vidi kod programa moguće je poboljšanje istog kao i ispravka postojećih grešaka jer kao što znamo nijedan program nije bez grešaka. Deo koda koji treba otkriti javnosti je deo programa koji je zadužen za pravljenje “slike” uređaja sa kojeg vršimo akviziciju dokaza jer je ovo osnovni korak koji mora da se radi bez greške. Ukoliko se akvizicija dokaza ne obavi na pravilan način dokazi će biti nevažeći a samim tim i ceo slučaj može biti odbačen na sudu, zato je od velike važnosti da neki delovi programa budu “open source”. Open source programi se ne plaćaju, većina radi na Linux platformi i obično ne pokrivaju sve oblasti digitalne forenzičke istrage. Mora se koristiti više različitih alata. Nemaju podršku i servirs. Licencirani programi se prave za Windows platformu, imaju veći broj modula integrisanih u jedan program samim tim pokrivaju više oblasti digitalne forenzičke istrage. Plaćaju se i nisu nimalo jeftini. I jedni i drugi mogu da se koriste u zvaničnim, korporacijskim, i vojnim istragama. U zavisnosti od kupljenih modula zavisi i stepen korišćenja alata kod licenciranih alata.⁴⁰

⁴⁰ Uglješa Georgijević, Gojko Grubor „Alati za digitalnu forenzičku istragu, skrita strana 2

18. ILOOK

Ilook je alat za forenzičku analizu koji pruža mogućnost pretrage i pregleda slike (image) diska koja je uzeta sa zaplenjenog kompjutera. Ima mogućnost pretrage i pregleda sa bilo slike diska koja je uzeta uz pomoć bilo kog sistema za pravljenje slika diska koji pravi bit niz ili bit sliku(bit po bit kopiju originalnog diska). Mnogi alati, što komercijalni programi, što programi koje koristi državne institucije (milicija, vojska, sudstvo, itd.). Može se koristiti i za pregledanje slika diskova (image) koji su uzeti sa sledećim komercijalnim alatima: Safeback image fajl, EnCase image fajlovi, ISO and CIF CD image fajlovi, VMWare virtual disks and Ilook image fajlovi.

Ilook mogućnosti:

Identifikacija i podrška sledećim fajl sistemima i varijantama:

- ❖ FAT12
- ❖ FAT16
- ❖ FAT32
- ❖ FAT32x
- ❖ VFAT
- ❖ NTFS 4
- ❖ NTFS 5
- ❖ NTFS 4 Compressed •NTFS 5 Compressed •Mac HFS
- ❖ Mac HFS+
- ❖ Linux Ext2FS
- ❖ Linux Ext3FS (journaling variant of Ext2FS) • SCO Sys V AFS
- ❖ Novell Netware NWFS

Izgled ekrana je kao Explorer tako da istražitelju pruža mogućnost pregleda i navigacije po fajl sistemu kao što se originalno pojavljuje na kompjuteru osumnjičenog.

Granularne extraction facilities pomoću kojih možemo da izdvojimo sve ili deo fajl sistema iz slike diska koja se pregleda.

Tri ugrađena moda pretrage (standardni, bulk pretraga and indeksirana pretraga). Autonomna pretraga i indexirajući agenti.

Ugrađeni jednostavan textifier.

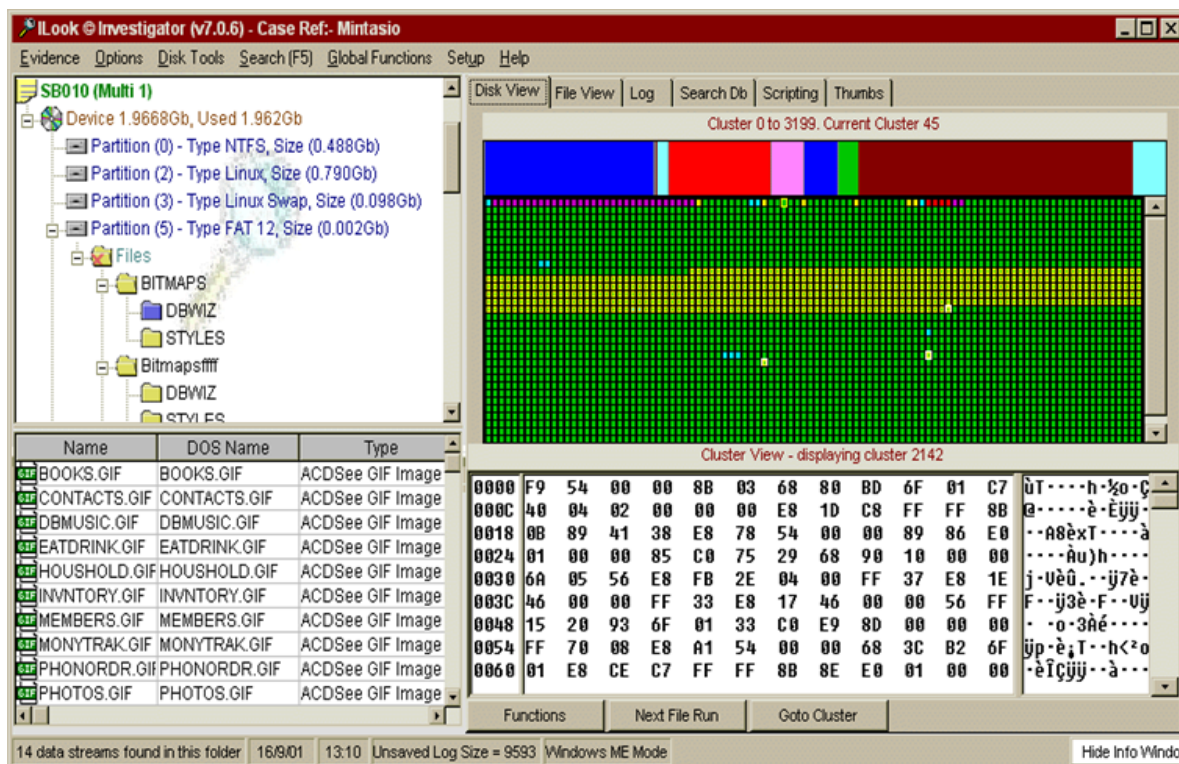
Defined viewer Link points to investigator technology.

Ugrađena mogućnost gledanja multi-format fajla

Podrška za duga imena fajlova

- ❖ Automatizovano procesiranje velikog broja slika i ekstrakcija. List generatori šifara i fraza za šifre.
- ❖ Ugrađeni hex editor sa mogućnostima pretrage.
- ❖ Mogućnosti spasavanja izbrisanih ili oštećenih fajlova.
- ❖ Rutine za verifikaciju potpisa fajlova. Oporavak orphaned FAT direktorijuma.
- ❖ Podrška za CRC32, MD5 and SHA1 hash analizu.
- ❖ CRC32, MD5 and SHA1 generatri za sliku (image data) i disk (disk data). Mogućnosti obeležavanja fajlova i pravljenje izveštaja.
- ❖ Mogućnost rukovanja dokazima i mogućnost rukovanja dokazima koje se sastoje iz više slika ili diskova.
- ❖ Alati za rekonstrukciju internet keš-a i mailbox-a (rekonstrukcija i priloga pisama (attachment reconstruction) i pravljenje izveštaja)).
- ❖ Alati za vađenje UUE and Base 64 attachment-a.
- ❖ Mogućnost direktne istrage na uređajima.
- ❖ Alati koji iz BIOS-a uzimaju sliku diska sa funkcijama MD5 / SHA1 verifikacije i kompresije slike (image).
- ❖ Funkcije filtriranja fajlova i eliminacije istih.
- ❖ Mogućnosti globalne pretrage između pojedinačnih dokaza.
- ❖ Rezultati pretrage se smeštaju u bazu podataka u odnosu na bilo koju pretragu i bilo koji pojedinačni dokaz.
- ❖ 3Bitmap slika diska daje detaljan uvid u fizički izgled bilo kojeg selektovanog diska
- ❖ Sveobuhvatni skript jezik, kompajler i runtime engine.
- ❖ Kategorizacija fajlova preko virtuelnih foldera.
- ❖ Ugrađeni thumbnail pretraživač.

18.1 Izgled ILOOK-a



Slika 16: Izgled ILOOK ekrana



Slika17:Glavni meni

Glavni meni sadrži grupe funkcija koje se odnose na Ilook kao celinu. Funkcije koje se odnose na pojedinačne ili grupe objekata se pokreću desnim klik menijima koji su dostupni ukoliko kliknete desnim dugmetom miša na bilo koji objekat koji se nalazi u “case EvidenceWindow” ili “FileObjectWindow.” Kratak opis funkcija:

Dokaz (Evidence) - rukovanje slučajem i dokazima

Opcije (Options)- brzi pristup opcijama koje utiču na to kako Ilook procesira razna mapiranja i funkcije auto procesiranja

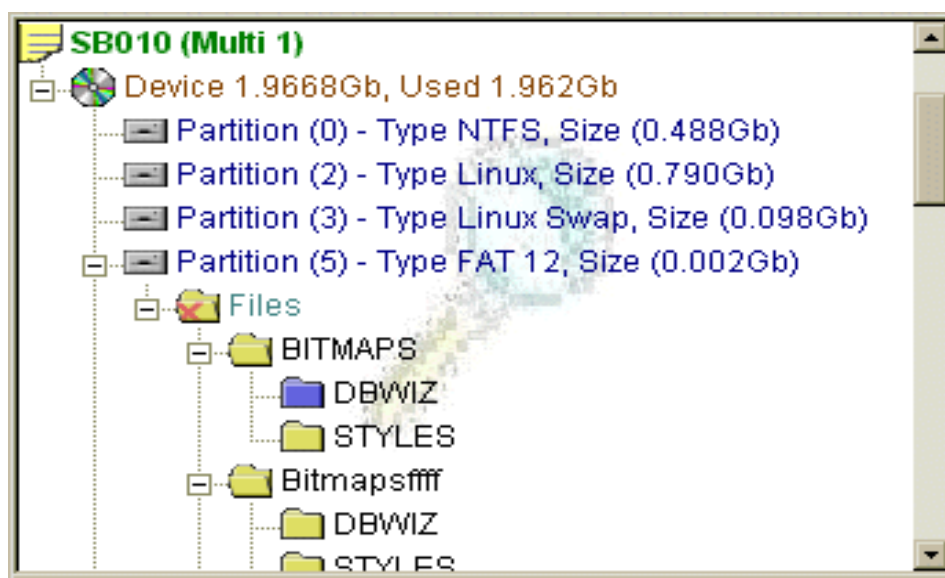
Disk oruđa (Disk Tools) - forenzičke funkcije koje možete koristiti na fajlovima koji se nalaze na diskovima vašeg PC-a ili šerovanim mrežnim folderima.

Pretraga (Search) – pristup ILook Čenginima pretrage i podešavanje pretraga.

Globalne Funkcije (Global Functions) – skladište funkcija koje se upotrebljavaju u odnosu na sve dokazne objekte u slučaju

Pomoć (Help)

18.2 Prozor dokaza

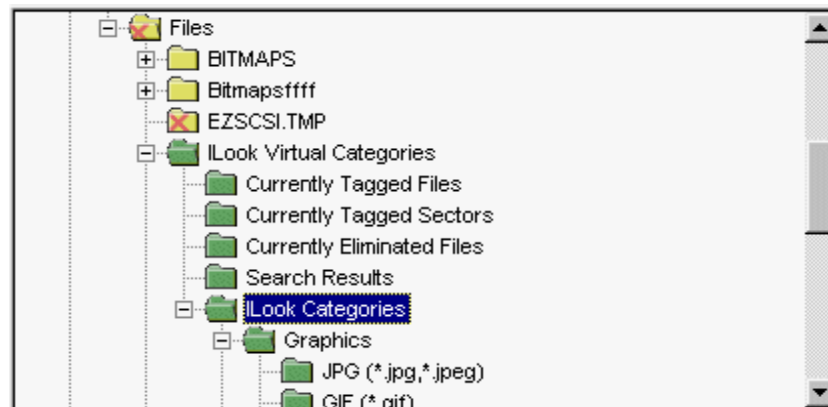


Slika 18: Prozor dokaza

Prozor dokaza prikazuje detalje dokaznih objekata koji su trenutno definisani u Ilook-u za tekući slučaj. Stavke su strukturirane hijerarhijski i svaka dokazna stavka je boldirana i identifikovana vrednostima koje smo im dodelili u ekranu za rukovanje dokazima. Ispod svake stavke su nekoliko grupa informacija koje su takođe hijerarhijski poredane. Generalno podaci su poredani za svaku definisanu stavku na sledeći način:

- ❖ **Evidence Item (Dokazna stavka(naziv i broj ukoliko se sastoji iz više njih))**
- ❖ **One or more device descriptions (Opis jednog ili više uređaja)**
- ❖ **One or more partition descriptions (Opis jedne ili više particija)**
- ❖ **A filesystem mapping (Mapa fajl sistema)**

Funkcijama iz kontekstnog menija se može pristupiti desnim klikom na bilo koji objekat na bilo kom nivou. Mapa fajl sistema (The file system mapping) se sastoji od foldera koji predstavljaju originalnu strukturu diska. Neki folderi su markirani sa crvenim krstom, to znači da ti folderi sadrže u sebi fajlove koji su bili izbrisani.



Slika 19: Virtuelni folderi

Prozor Dokaza (The EvidenceWindow) takođe sadrži i virtuelne foldere koji su pristupačni u svakoj mapiranoj particiji (folderi su zelene boje). Postoje tri virtuelna foldera, koje pravi Ilook u root –u svake particije, koja nam pružaju mogućnost bržeg pregleda fajlova koje smo eliminisali, obeleženih fajlova i obeleženih sektora za bilo koju dokaznu stavku. Klikom na traženi virtuelni folder prikazuje se set podataka.

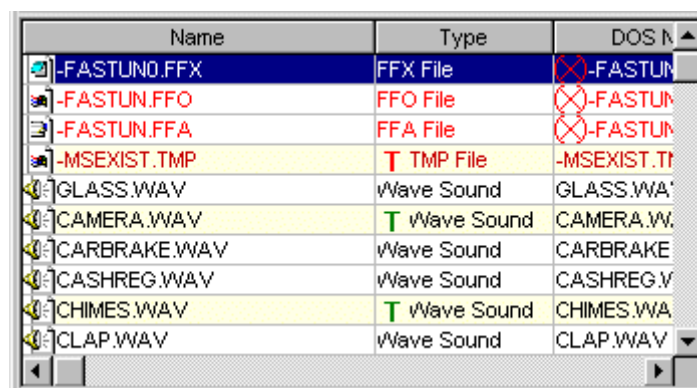
- ❖ **Trenutno eliminisani fajlovi (Currently Eliminated Files)**
- ❖ **Trenutno označeni fajlovi (Currently Tagged Files)**
- ❖ **Lista svih označenih sektora (Currently Tagged Sectors)**
- ❖ **Izbrisani fajlovi (Undeleted Files)**
- ❖ **Ilook Kategorije (ILook Categories)**
- ❖ **1Kategorije korisnika (User Categories).**
- ❖ **Rezultati pretrage (Search Results)**

18.3 Prozor fajlova

Prozor fajlova (FileWindow) prikazuje fajlove koji se nalaze u bilo kom folderu selektovanom u prozoru dokaza (Evidence Window). Izbrisani fajlovi prikazani su ispisani, po početnim podešavanjima (default), sa crvenim tekstom. Kao i kod prozora za dokaze (EvidenceWindow), desni klik na fajl ili grupu fajlova će prikazati funkcijski meni. Po početnim podešavanjima (default), fajlovi koji su prikazani na prozoru fajlova prate sledeće konvencije(mogu se promeniti ukoliko to želimo):

- ❖ Normalni fajlovi (Normal files) - crni tekst na beloj pozadini
- ❖ Izbrisani fajlovi (Undeleted files) – crveni tekst na beloj pozadini
- ❖ Označeni fajlovi (Tagged files) – žuta pozadina (sa zelenim slovom "T" u drugoj koloni za označene normalne fajlove i crveno "T" u drugoj koloni za izbrisane fajlove)

Može se takođe desiti da se u trećoj koloni nalazi crveni krst u krugu, to znači da je fajl skraćen (truncated file). Ovi fajlovi se dešavaju kada Ilook nemože da odredi sve alocirane klastere koji pripadaju tom fajlu. Obično se to dešava na FAT fajl sistemima gde je drugi fajl delimično ili skroz prepisao niz podataka koji pripadaju izbrisanom fajlu ili je niz podataka prešao unakrsni FAT lanac (cross linked FAT chain). Možemo kliknuti na bilo koje zaglavlje kolone da bi sortirali prikazane fajlove u opadajućem ili rastućem redosledu. Možemo takođe promeniti redosled kolona tako što držimo levo dugme miša na zaglavlju kolone a zatim je prevučemo na željeno mesto. Redosled kolona ostaje prema poslednjem redosledu kad god se Ilook ponovo upali. Možemo i sakriti određene kolone ukoliko nam smetaju. To se radi iz Ilook setup-a.

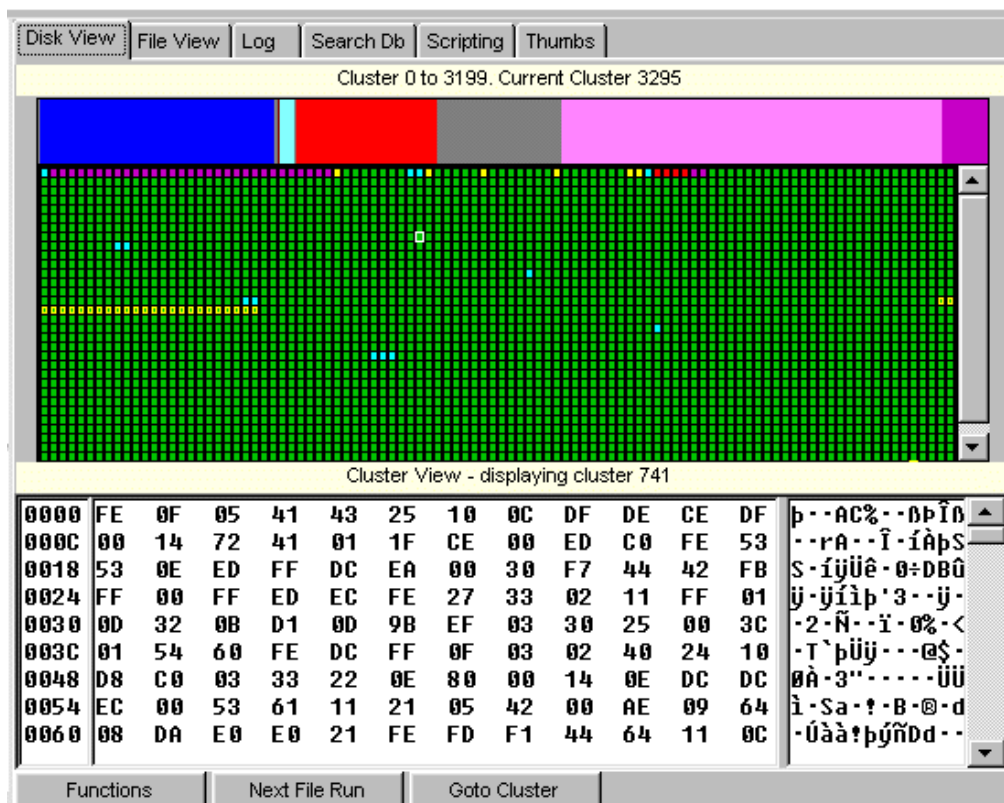


Name	Type	DOS N
-FASTUN0.FFX	FFX File	~~-FASTUN~~
-FASTUN.FFO	FFO File	~~-FASTUN~~
-FASTUN.FFA	FFA File	~~-FASTUN~~
-MSEXIST.TMP	T TMP File	-MSEXIST.TI
GLASS.WAV	Wave Sound	GLASS.WA
CAMERA.WAV	T Wave Sound	CAMERA.W.
CARBRAKE.WAV	Wave Sound	CARBRAKE
CASHREG.WAV	Wave Sound	CASHREG.V
CHIMES.WAV	T Wave Sound	CHIMES.WA
CLAP.WAV	Wave Sound	CLAP.WAV

Slika 20:Prozor fajlova

18.4 Prozor informacija

Prozor informacija (InfoWindow) je grupa od šest kartica (tabova) koja nam daje informacije u odnosu na objekte selektovane u prozoru dokaza i prozoru fajlova. U zavisnosti od izabranih objekata zavisi i promena podataka na ovim karticama u trenutku odabira.



Slika 21: Prozor informacija

Kartice:

- ❖ Pregled diska (Disk View) Pregled fajla (File View) Dnevnik (Log)
- ❖ Pretraga baze podataka (SearchDb) Skripte (Scripting)
- ❖ Thumb fajlovi (Thumbs)

18.5 Pregled diska

Ovaj prozor prikazuje interaktivni pregled površine diska koju je mapirao Ilook, rezultati na ovom ekranu se manjeju u zavisnosti od izbora dokaznog objekta iz prozora dokaza. Prozor izgled diska sastoji se od tri panela informacija:

Pregled diska – najviši ekran, sastoji se od raznih boja, pokazuje slikovni pregled rasporeda particija unutar diska ili slike diska ili uređaja. Ukoliko zadržite kursor preko površine u boji Ilook će izbaciti mali prozor u kome će prikazati informacije o particiji, klikom na obojenu površinu menjamo pregled particije na novu particiju. Neiskorišćeni delovi diska ili uređaja su obeležena sivom bojom, možete kliknuti i na te delove da bi pogledali trenutno nealocirane sektore (ovi delovi su grupisani u klastere veličine 8 sektora po klasteru)

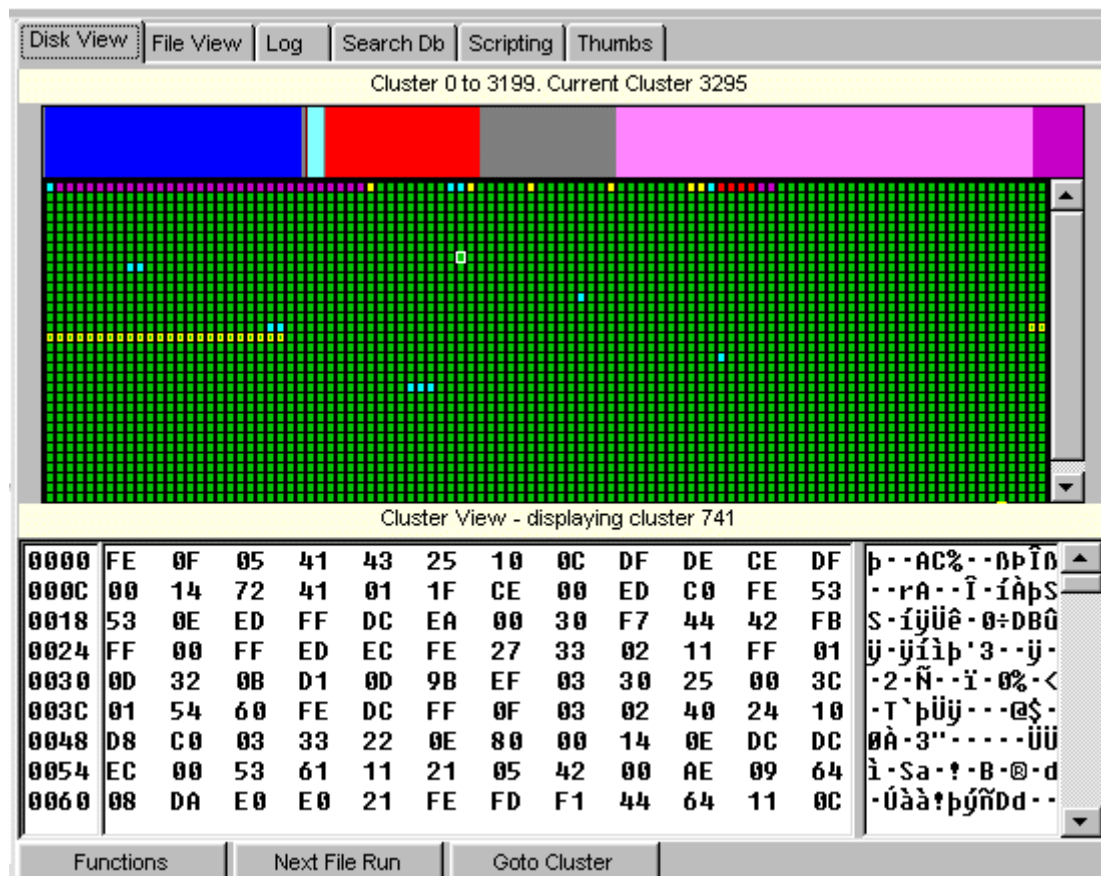
Pregled particije – centralni panel prikazuje u boji izgled trenutno prikazane particije. Informacije u ovom panelu se menjaju u zavisnosti od selekcije u prozoru dokaza ili prozoru pregleda diska. Svaki obojeni blok predstavlja klaster a njegova boja predstavlja kakvu vrstu informacija klaster predstavlja.

- ❖ Podaci - fajl
- ❖ Kompresovani fajl
- ❖ Kompresovani niz podataka
- ❖ Obrisani podaci fajla
- ❖ Prebrisani podaci fajla
- ❖ Slobodan prostor
- ❖ Klaster u kojem počinje folder
- ❖ Niz podataka
- ❖ Podaci residentnog fajla
- ❖ Neiskorišćeni prostor



Slika 22: Legenda

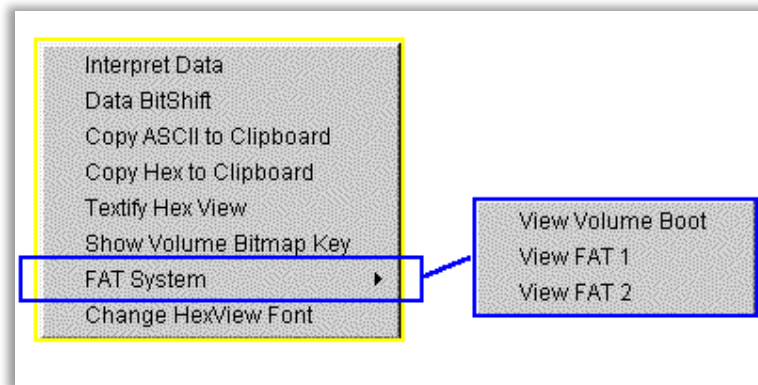
Kada selektujete bilo koji klaster sa mišem (ili korišćenjem navigacijskih dugmića na tastaturi) selektovani klaster će biti učitani u panel za pregled klastera (Cluster View panel). Selektovanjem fajla selektuju se i klasteri koje zauzima taj fajl. Postoji mogućnost i selektovanja određenog broja klastera i njihovo prebacivanje u virtuelni fajl ili direktno kopiranje na disk (selektovanje uz pomoć ctrl+shift + levi klik miša).



Slika 23:Pregled fajla

Pregled klastera (Cluster view) - Donji panel prikazuje sadržinu selektovanog klastera. Funkcije pregleda diska (Disk View Functions)

Funkcijama pregleda diska se prilazi preko dugmeta Funkcije (Functions button).



Slika 24: Funkcija pregleda diska

Funkcije :

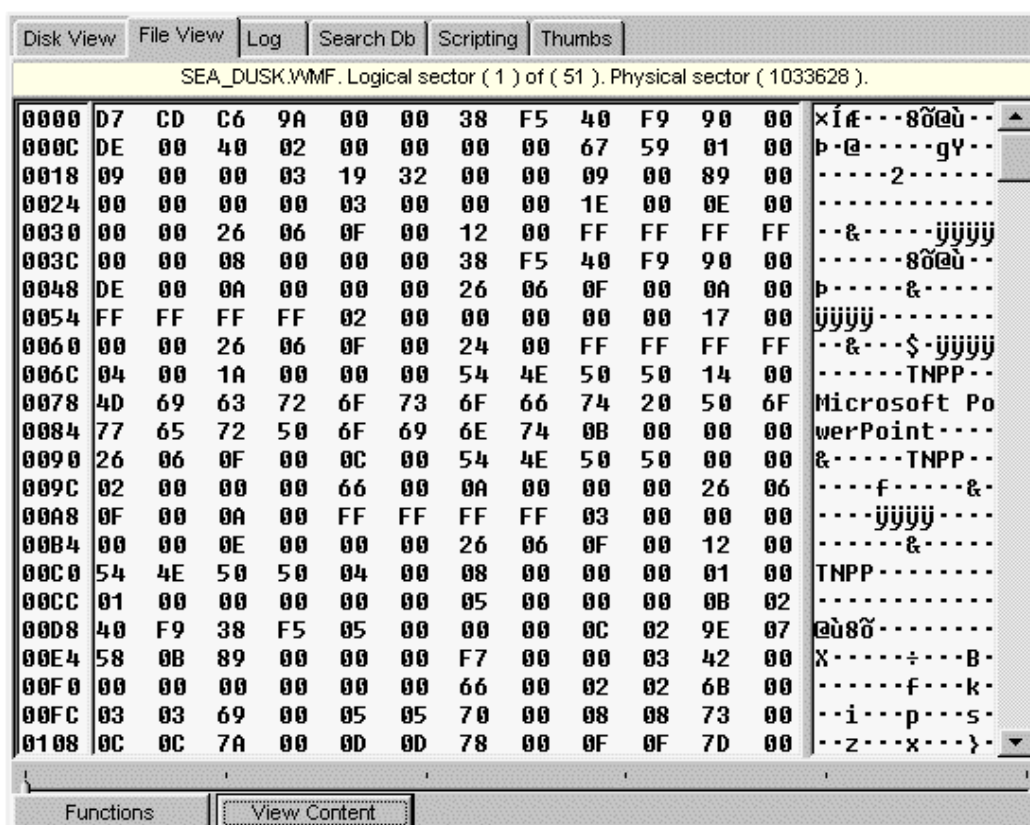
- ❖ **Interpretiranje podataka**
- ❖ **Pomeranje bitova podataka**
- ❖ **Kopiranje ASCII na klipbord**
- ❖ **Kopiranje heksidecimalnih vrednosti na klipbord**
- ❖ **Tekstuelizacija heksadecimalnog pregleda**
- ❖ **Legenda za sektore**
- ❖ **Fat sistem**
- ❖ **Dugme idi na klaster**
- ❖ **Promena fonta u heksadecimalnom prozoru**

18.6 Pregled fajla

Prozor za pregled fajla je multifunkcijski prikaz bilo kog fajla selektovanog u Proзору fajlova (FileWindow). Fajl se može pregledati u heksadecimalnom obliku ili se može prikazati u svom originalnom formatu (ukoliko je prikaz tog tipa fajla podržan od strane Ilook softvera). Promena prikaza fajla se vrši preko dugmeta “View” na dnu ekrana.

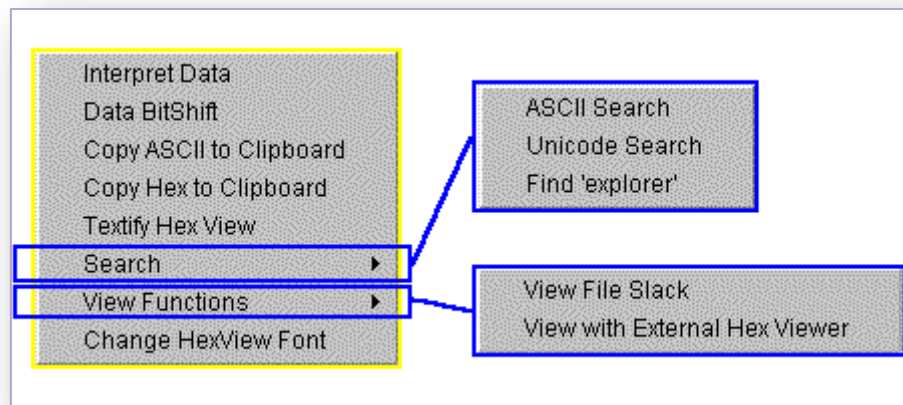
Heksadecimalni prikaz (Hex View)

Heksadecimalni prikaz je prikaz selektovanog fajla po klasterima, podaci su prikazani u kombinovanom Hex / ACSII prozoru. Možete prolaziti kroz klastere a trenutna logička pozicija fajla i fizička lokacija trenutnog sektora se ispisuju u naslovnoj traci prozora.



Slika 25: Pregled fajla

Funkcijama heksadecimalnog pregleda fajla prilazi se preko dugmeta “Functions”.



Slika 26: Prozor dokaza

Funkcije :

- ❖ Interpretiranje podataka
- ❖ Pomeranje bitova podataka
- ❖ Kopiranje ASCII na klipbord
- ❖ Kopiranje Hex na klipbord
- ❖ Tekstuelizacija heksadecimalnog pregleda
- ❖ Pretraga
- ❖ Funkcije pregleda
- ❖ Promena fonta u heksadecimalnom prozoru

18.7 Dnevnik

Prozor dnevnik prikazuje svaki korak koji smo preduzeli tokom sesije (Važno zbog sudskog postupka i zbog mogućnosti ponovne izvedbe istih dokaza). U njemu se upisuju detalji o funkcijama koje smo koristili o informacijama koje su otkrivene i akcijama koje smo preduzeli tokom istrage. Na slici je prikazan izgled dnevnika (Log). To je pomoćna alatka koja služi kao podsetnik, i nije joj svrha da zameni beleške koje pravi istražitelj tokom istrage.

Tekst koji se nalazi u Dnevniku je isписan u različitim bojama. Svaki dokazni objekat ima svoju boju za trenutnu sesiju i svaka akcija koja se uradi nad dokaznim objektom biće zapisana u dnevniku u svojoj odgovarajućoj boji. Boja za svaki dokazni objekat se može promeniti preko prozora dokaza (Evidence Window). Greške su ispisane svetlo crvenom a upozorenja su ispisana tamno crvenom bojom. Upozorenja se generalno odnose na procesiranje koje možda želite da pribeležite. Greške mogu da ukazuju na problem pri procesiranju, ili da je Ilook detektovao ozbiljan problem sa slikom diska ili uređajem koji se istražuje.

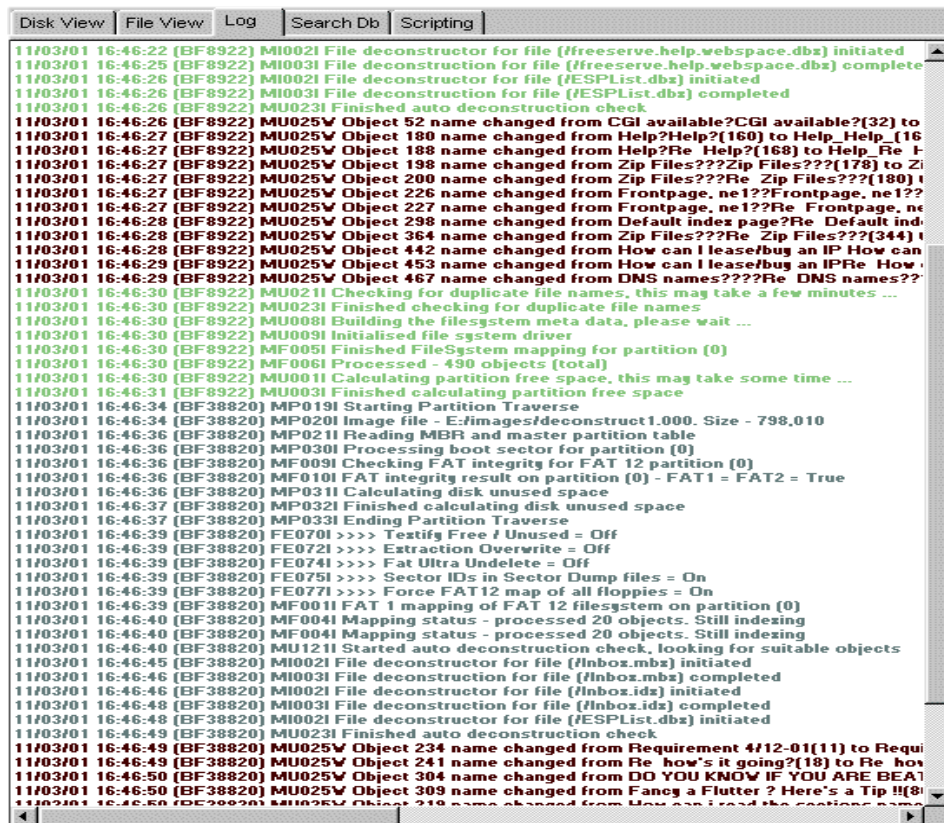
Dnevnik beleži sve važne događaje koji se mogu dogoditi tokom istražne sesije. Sastoji se od brojnih vremenski obeleženih poruka kao što su početak i kraj neke funkcije, informacije o fajl sistemu, poruka o opcijama, grešaka i upozorenja.

Dnevnik se automatski snima u određenim intervalima. Ukoliko gasite sesiju, Ilook Vas pita da snimate poruke koje se nisu automatski snimile tokom sesije. U dnevnik možete i sami da upisujete bilo koje zabeleške koje će vam pomoći pri istrazi.

Standardne poruke dnevnika su u sledećem formatu:

- ❖ Datum (Date) – u lokalnom formatu datuma
- ❖ Vreme (Time) – u lokalnom formatu vremena
- ❖ ID Dokaza (Evidence ID) – indikacija na koji dokazni objekat se poruka odnosi (takođe I boja ukazuje na ID dokaza)
- ❖ ID poruke (Message ID) – grupa od šest karaktera koja se sastoji od:
- ❖ ID Tipa (Type ID) - F = Interaktivni oblik (Interactive form), M = Programski modul (Code module)
- ❖ ID Modula (Module ID) – Jedan karakter koji definiše programsku grupu o Pozicija - 3 broja koja lociraju poruku u Ilook-u
- ❖ Pokazatelj (Flag) - I = Informacija (Information), W = Upozorenje (Warning), E = Greška (Error)
- ❖ Tekst poruke
- ❖ Baza podataka pretraga (Search Results Database InfoWindow – Search Db)

Rezultati standarden, indeksirane ili bulk pretrage za svaki dokazni objekat se upisuju u u bazu podataka pretraga. Bazi podataka pretraga možete pristupiti preko kartice Pretraga Db (Search Db) u Prozoru informacija (Info Window) ili preko virtuelnog foldera Pretraga (Search) u bilo kojem mapiranom fajl sistemu. Sve pretrage su prikazne po datumu pretraga (najnovije pretrage se nalaze na vrhu liste) i ispisane su u nekoj boji koja predstavlja rezultate pretrage. Zelena boja ukazuje da je pretraga završena dok crvena predstavlja da je pretraga zaustavljena od strane korisnika.



Slika 27: Dnevnik

Postoji nekoliko funkcija koje možete pokrenuti u bazi podataka rezultata pretrage. Njima se pristupa desnim klikom na bilo koji zapis.

- ❖ Promena komentara pretrage (Edit Search Tag)
- ❖ Izveštaj istorije pretrage (Search History Report).
- ❖ Pregled rezultata pretrage
- ❖ Restartovanje pretrage (Restart Search)
- ❖ Ponovo pokretanje pretrage kao Bulk pretragu (Rerun search as Bulk Search)

19. Windows Thumbnail cache

Na Windows operativnim sistemima (od verzije Windows 98), thumbnail cache je fajl koji u sebi sadrži thumbnail (sličica, umanjena verzija originalne slike) slike za Windows explorer thumbnail view. Ovakav pristup skladištenja thumbnail slike u fajl omogućava brži prikaz thumbnail-ova slike koje se nalaze u folderu, jer ne moraju da se prerađuju svaki put kada korisnik pristupi nekom folderu koji sadrži slike.

Windows smešta thumbnailove grafičkih fajlova i određenih dokumenata, kao i filmova u Thumbnail Cache fajl, uključujući i sledeće formate: JPEG, BMP, GIF, PNG, TIFF, AVI, PDF, PPT i HTML⁴¹

19.1 Thumbs

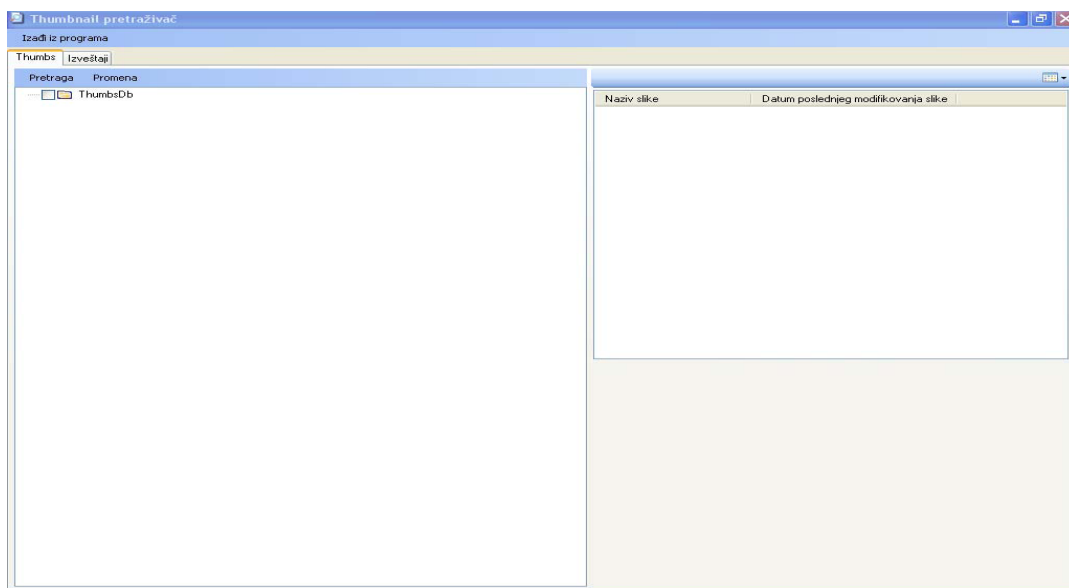
Thumbnail pretraživač je alatka koja može da se koristi u korelaciji sa alatima za digitalnu forenzičku istragu koji nemaju opciju čitanja sadržaja Thumbs.db fajlova, a može da se koristi i kao specijalizovan alat, jer ima ugrađene mehanizme pretrage svih uređaja (HDD, CD, USB..) na računaru.

Thumbs.db fajlovi su smešteni u svaki direktorijum koji sadrži slike ili filmove na Microsoft Windows NT verzijama operativnih sistema pre Viste. Operativni sistem kreira fajl lokalno. Za svaku sliku koja se nalazi u direktorijumu pravi se njena umanjena kopija koja se smešta u Thumbs.db fajl kao mali JPEG fajl, bez obzira na format slike koje se nalaze u direktorijumu. Ove slike se smanjuju na maksimalno 96×96 pixels, ili na proporcionalnu minijaturu njihovog originalnog oblika (ovo je kod slike koje nisu kvadratnog oblika) sa 96 pixels na dužoj strani. Svaki folder u kojem su fajlovi prikazani kao Thumbnails ili Filmstrip u Windows Exploreru sadržaće i Thumbs.db fajl.

19.2 Funkcionalnosti Thumbnail pretraživača

Neki forenzički digitalni alati ne poseduju modul za pregledanje thumbs.db fajlova tj. njihovog sadržaja. ThumbnailViewer je napravljen kao dodatna (pomoćna) alatka tim forenzičkim alatima. ThumbnailViewer pronalazi sve thumbs.db fajlove koji se nalaze na kompjuteru, a ima mogućnost pretrage samo određenih delova kompjutera, kao i prikazivanje sadržaja pojedinačnog thumbs.db fajla.

⁴¹ Uglješa Georgijević, Gojko Grubor „Alati za digitalnu forenzičku istragu, skrita strana 4



Slika 28: Pocetni ekran Tumbnails pretraživača

19.3 Osnovne funkcionalnosti Tumbnails pretraživača

Izborom opcije pretraga prikazuje se padajući meni u kojem se mogu izabrati 2 vrste pretrage:

- ❖ pretraga celog računara, svih HD, CD-ova, USB-uređaja koji su prikačeni na računar ili
- ❖ pretraga određenih delova računara.
- ❖

Prikazuju se datum i vreme pretrage, ukupan broj pronađenih thumbs.db fajlova i uređaji koji su pronađeni i koliko u kojem od njih ima thumbs.db fajlova. Odabirom diska prikazuju se svi thumbs.db fajlovi na tom disku (putanje fajlova). Odabirom nekog thumbs.db fajla prikazuje se sadržaj tog fajla u desnom prozoru programa. Prikazuje se naziv fajla i vreme kada je fajl poslednji put bio modifikovan, a u donjem desnom delu prozora prikazuje se thumbnail slika kao i njena uvećana verzija.

Na osnovu prikaza svih slika sa izabranog, istraživanog medija, forenzičar može izvršiti selekviju slika koje podržavaju osnovanu sumnju za istragu (npr., dečije pornografije, terorističkih aktivnosti itd.). Ovom operacijom forenzičar bitno smanjuje vreme analize imidža, kao i zahtevanu veću procesorsku snagu za analizu thumbnails.⁴²

⁴².http://www.itvestak.org.rs/ziteh_10/zbornik_radova/Georgijevic%20Ugljesa,%20Gojko%20Grubor%20%20Alat%20Alat%20za%20Digitalnu%20forenzicku%20istragu%20Thumbnail%20Viewer.pdf-01.10.2014

20. Uloga kompjutera u zločinu

U roku od četiri godine (od 1994 do 1998) "US Department of Justice (USDOJ)" napravila je set kategorija a po njima i niz vodiča za pretragu i konfiskovanje.(USDOJ 1994, 1998). Ove kategorije prave razliku između hardvera (elektronskih dokaza) i informacija (digitalnih dokaza), koja je bitna kod razvoja raznih procedura.U ovom kontekstu hardver se odnosi na sve fizičke delove računarskog sistema, a informacije se odnose na podatke i programe koji su smešteni na kompjuteru.

Kategorije :

- ❖ Hardver kao proizvod kriminalne aktivnosti (Hardware as Contraband or Fruitsof Crime).
- ❖ Hardver kao instrument (oruđe) zločina (Hardware as an Instrumentality).
- ❖ Hardver kao dokaz (Hardware as Evidence).
- ❖ Informacija kao proizvod kriminalne aktivnosti (Information as Contraband orFruits of Crime).
- ❖ Informacija kao instrument (oruđe) zločina (Information as anInstrumentality).
- ❖ Informacija kao dokaz (Information as Evidence).

Ove kategorije nisu međusobno isključive, i neki zločin može da spada u višerazličitih kategorija.2002 godine USDOJ je ažuriralo dokument tako da je u skladu sa današnjomtehnologijom i zakonom i izrastao je u uputstvo za "Searching and Seizing Computersand Obtaining Electronic Evidence in Criminal Investigations" (USDOJ 2002). Dokvodiči pridaju istu važnost hardveru i softveru, uputstvo pridaje veću važnostinformacionom delu. Ukoliko hardver sam po sebi kao uređaj nije dokaz, oruđe ili plodzločina onda se hardver posmatra kao skladište podataka. Iako je prikupljanje informacijaglavni cilj, može biti neophodna i kolekcija hardvera iz različitih razloga.Zbog unikatnosti legalnih procedura za svaku kategoriju zločina, ovo uputstvo bitrebali pročitati istražitelji, tužioci i advokati odbrane.Od najvećeg značaja je to što uputstvo ima mrežno-centralni prilazproblemu.⁴³

⁴³ Srđan Atanasijević,Digitalna forenzika,Visoka tehnička škola Kragujevac 2012 , skripta 86 str

20.1 Hardver kao proizvod kriminalne aktivnosti

Zabranjeni materijal je vlasništvo koje običan građanin ne sme da poseduje. Npr. pododređenim uslovima zabranjeno je da građanin poseduje uređaj za presretanje elektronskih komunikacija (18 USCS 2512). Klonirani mobilni telefoni i oprema koja se koristi da se isti kloniraju je drugi primer zabranjenog materijala. Plodovi zločina predstavljaju vlasništvo koje je dobijeno kriminalnom aktivnošću kao što je oprema koje je ukradena, ili kupljena koristeći ukradene kreditne kartice.

20.2 Hardver kao instrument(oruđe) zločina

Kada je hardver odigrao važnu ulogu u zločinu onda se on smatra za sredstvo. Ova razlika je bitna jer ukoliko je hardver korišten kao oružje u kriminalnom činu, ovo može dovesti do dodatnih optužbi ili povećanja kazne. Primer je hardver koji je napravljen isključivo u svrhe kriminalnih aktivnosti. Npr. snifer hardver koji je napravljen da prisluškuje mrežu. Sniferi se obično koriste za prikupljanje šifara koje zatim mogu poslužiti za neautorizovan pristup sistemu. Glavni razlog za autorizovanje snaga reda i mira da konfiskuju instrumenti zločina je sprečavanje budućih zločina. Ukoliko ne može da se da argument da je hardver imao ulogu instrumenta u zločinu, onda ga ne bi trebali konfiskovati kao instrument zločina. Uglavnom je na sudovima da odluče da li je neki predmet igrao ključnu ulogu u nekom zločinu.

20.3 Hardver kao dokaz

Ova kategorija hardvera kao dokaza ne spada ni u contraband ni kao instrumentality of a crime. Npr. ukoliko je korišten štampač pri falsifikovanju nekih dokumenata ili novca ima jedinstvene karakteristike štampe koje povezuju hardver sa tim dokumentima, može da se zapleni kao dokaz.

20.4 Informacija kao proizvod kriminalne aktivnosti

Contraband informacija je informacija koju obični građanin ne sme da poseduje. Uobičajena forma informacije koja je zabranjena je softver za šifrovanje. U nekim zemljama ilegalno je posedovati softver koji poseduje jake algoritme za enkripciju zato što taj softver omogućava kriminalcima veliku privatnost. Ukoliko su dokazi koji su potrebni za uspešnu tužbu kriptovani moguće je da ne mogu da se dekodiraju podaci a samim tim dolazi do odbacivanja slučaja usled nedostatka dokaza. Drugi oblik informacija kao proizvod kriminalne aktivnosti su slike dečije pornografije. U ovu grupu još spadaju i ilegalne kopije kompjuterskih programa, ukradene industrijske, trgovačke tajne, šifre, ili bilo kakve informacije dobijene iz kriminalne aktivnosti.

20.5 Informacija kao instrument zločina

Informacija može biti the oruđem kojim je izvršena neka kriminalna aktivnost ukoliko je dizajnirana ili ukoliko je njena svrha da bude sredstvo za kriminalnu aktivnost. Programi koji se koriste kao oruđe za upad u sistem su instrumenti zločina. Ovi programi omogućavaju neautorizovani pristup računarskom sistemu. Programi koji snimaju korisničke šifre pri logovanju na kompjuter mogu biti instrument zločina. Kompjuterski programi koji kreću šifre mogu takođe biti instrumenti zločina. Ukoliko ne postoji mogućnost da se prikaže da je informacija imala jednu od značajnijih uloga zločinu, onda verovatno nema potrebe da se konfiskuje kao instrument zločina.

20.6 Informacija kao dokaz

Mnoge naše dnevne aktivnosti ostavljaju digitalne tragove iza nas. Svi servis provajderi (npr., ISP-ovi, banke, kreditne institucije, telefonske kompanije) vode neke informacije o svojim mušterijama. Ovi podaci mogu da daju važne informacije o kretanju subjekata kao i vremenu određenih aktivnosti.

Na primer pre nego što sam krenuo na posao koristio sam bankomat i podigao određenu sumu novca. Informacije ostaju u log datotekama na serveru banke kao i na kameri koja snima bankomat. Iz ovih informacija možemo izvući informacije o kretanju subjekta. Kada sam stigao na posao primio sam i poslao elektronsku poštu. Iako je sadržaj pošte šifrovan podaci o vremenu i primaocu ostaju zapisani kako na log serveru e-mail provajdera tako i na kompjuteru sa kojeg je pošta poslata. S tim informacijama mogu da se dve osobe dovedu u vezu. Na primer ukoliko sam poslao veliki broj poruka određenoj osobi i dobio odgovore na te sve poruke a, zatim sam uhvaćen u nekom zločinu u za koju sam radio u saradnji sa

osobom sa kojom se dopisujem prethodne informacije služe kao dokazi o planiranju određenog zločina ili naručivanja istog. Ukoliko je osumnjičeni koristio e-mail sa još nekoliko osoba u određenom vremenskom intervalu pre i posle zločina može se tražiti nalog za pregled pošte kao i za pretres ostalih kompjutera koji su korišćeni u komunikaciji sa osumnjičenima. Zatim sam otišao na neke web lokacije koje sadrže materijal o uputstvima za sprovođenje određenog zločina. Sa mog kompjutera kao i sa servera na kome se nalazi web stranica moguće je uzeti adrese kompjutera a zatim od internet provajdera vreme i lokaciju sa koje je osumnjičeni pristupio web strani. S tim podacima možemo dokazati da je osumnjičeni planirao takav zločin.

21. STUDIJA SLUČAJA 1

UVOD

OPŠTE KARAKTERISTIKE

NAČIN KORIŠĆENJA



Slika 29: TeamViewer logo

Izvor: http://www.teamviewer.com/download/teamviewer_manual.pdf

21.1 Uvod

Kako računari postaju sve jeftiniji i potrebni su u gotovo svakom poslu, gotovo da i nema korisnika koji ne poseduje ili ne koristi više od jednog računara. Uzimajući u obzir tu činjenicu, nije teško zamisliti ili bolje reći doći u situaciju da smo neki jako važan dokument zaboravili na nekom računaru koji trenutno nije ispred nas, nebitno da li je situacija kuća ili posao.

Sesti u auto i voziti se sat vremena, od kancelarije do kuće, kako bismo sa računara pokupili jedan fajl koji smo zaboravili staviti na USB suludo je ako su oba računara spojena na Internet. Sve što u tom trenutku trebamo je remote desktop aplikacija poput TeamViewera, kojeg ćemo detaljno obraditi u ovoj studiji slučaja.



21.2 Opšte karakteristike

TeamViewer je proizvod istoimene nemačke kompanije osnovane 2005. godine. Pre par meseci izdata je njegova najnovija 6 verzija. Iako nema mnogo godina iza sebe, sa više od 100 miliona korisnika, u 200 zemlja širom sveta, te 21 jezičkom verzijom, TeamViewer je jedno od najbrže rastućih rešenja za daljinski nadzor i daljinsku prezentaciju. Među partnerima kompanije mogu da se nađu imena kao što su: Porsche, Canon, Intel, IBM, UNICEF, Ford itd.⁴⁴

TeamViewer je jednostavan i praktičan, a istovremeno izuzetno moćan program za kontrolu računara na daljinu. Iako je prvenstveno namenjen za poslovnu primenu, dostupan je i kao besplatna verzija za privatne korisnike, naravno uz izvesna ograničenja. Između ostalih branši, jako je koristan i u ekonomiji gde nalazi primenu u bankarskom, kao i u sektoru osiguranja i sl.⁴⁵

Glavna odlika TeamViewera, podrška na daljinu tokom godina se nije menjala, a svaka nova verzija donosila je nešto novo, kao i unapređenje već postojećih mogućnosti. Od novih funkcija možemo da izdvojimo VoIP (Voice over Internet Protokol) i novi protokol prenosa podataka sa unapređenim „keširanjem“ i metodama kompresije, što čini TeamViewer znatno bržim u odnosu na prethodne verzije kao i dosta jednostavnijim za upotrebu u odnosu na konkurenciju koju čine poznata imena iz svijeta Remote support-a: LogMeIn, Ultra VNC, pcAnywhere...

Glavne odlike TeamViewera i dalje su podrška na daljinu (Remote support), prezentacija (Presentation), prenos podataka (File transfer) i VPN (Virtual Private Network). Njegova prava snaga krije se u činjenici da za uspostavljanje konekcije nije potrebno vršiti podešavanja na samom ruteru, otvarati portove ili podešavati firewall, iz pomenutog razloga je i vrlo popularan za profesionalnu upotrebu npr. u Kompanijama ili Forumima koji se bave sa poslovima održavanja i „čišćenja“ računara (od virusa, trojanaca) i sl.

⁴⁴ <http://www.teamviewer.com/en/company/references.aspx> -05.10.2014

⁴⁵ <http://www.teamviewer.com/en/company/references.aspx>-05.10.2014

Sama konekcija uspostavlja se putem TCP ili UDP protokola, preko glavnih TeamViewer servera, a ostatak konekcije odvija se putem redundantne mreže, preko TCP ili HTTP tunela.

Nakon pokretanja instalacionog paketa, dobijamo mogućnost da instaliramo TeamViewer na hard disk ili da ga pokrenemo kao prenosnu (portable) verziju. Ukoliko izaberemo klasičnu instalaciju, dobijamo mogućnost za izbor tipa licence, opciju za startovanje TeamViewera uz Windows, kao i postavljanje glavne šifre.

Programu je moguće pristupiti iz sistemskog „treja“, a po želji se može integrisati i u Windows programe.

Važno je napomenuti to da je ideja koja stoji iza TeamViewera jednostavnost rukovanja, što je od velikog značaja za one koji se slabije snalaze sa računarima. To ne znači da TeamViewer ne posjeduje više od onoga što je dostupno na prvi pogled. Naprotiv, od opcija koje nisu prikazane u glavnom prozoru možemo da izdvojimo slanje TeamViewer pozivnice prijatelju (ako je definisan imejl klijent) i, mnogo važnije, detaljna podešavanja programa kao što su Proxy, prihvatanje LAN konekcija, obavezna dužina šifre, kao i spisak identifikacionih kodova koji mogu da pristupe vašem računaru (tzv. „whitelist“). Tu su i podešavanja za kontrolu na daljinu, podešavanje prezentacija i VPN-a.

Dok većina konkurenata nudi različite pakete za daljinsku podršku, daljinsko administriranje, obuku i prodaju (ali će te usluge i dodatno naplatiti...), TeamViewer je „all in one“ rešenje za sve što vam treba, TeamViewer uključuje sve pomenute module u jednom jednostavnom i vrlo „povoljnom“ paketu.⁴⁶

Takođe bitno je napomenuti da je TeamViewer jedno vrlo sigurno rješenje. Sve verzije krasi potpuno siguran prijenos podataka sa 256 Bitnom enkripcijom/kodiranjem (isti sigurnosni standard koji se koristi za https / SSL).⁴⁷

⁴⁶ <http://www.teamviewer.com/en/products/benefits.aspx> -05.10.2014

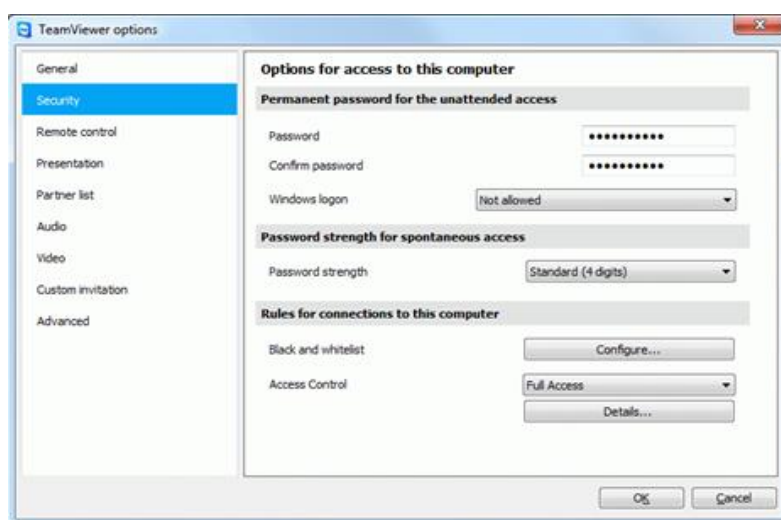
⁴⁷ <http://www.teamviewer.com/en/products/security.aspx> -05.10.2014

21.3 Način korišćenja

TeamViewer je jedan od najboljih i po našem mišljenju najjednostavnijih programa za Remote Desktop (Udaljeni Pristup), bilo da se radi o udaljenoj podršci, prezentaciji, razmeni datoteka. Osim jednostavnosti instalacije i korišćenja, potpuno je besplatan (za nekomercijalnu upotrebu). Ono što sa njim možete napraviti je vrlo brzo pomoći kolegi, prijatelju koji treba pomoć u svakodnevnom radu na računaru (mnogo jednostavnije nego telefonskim putem).

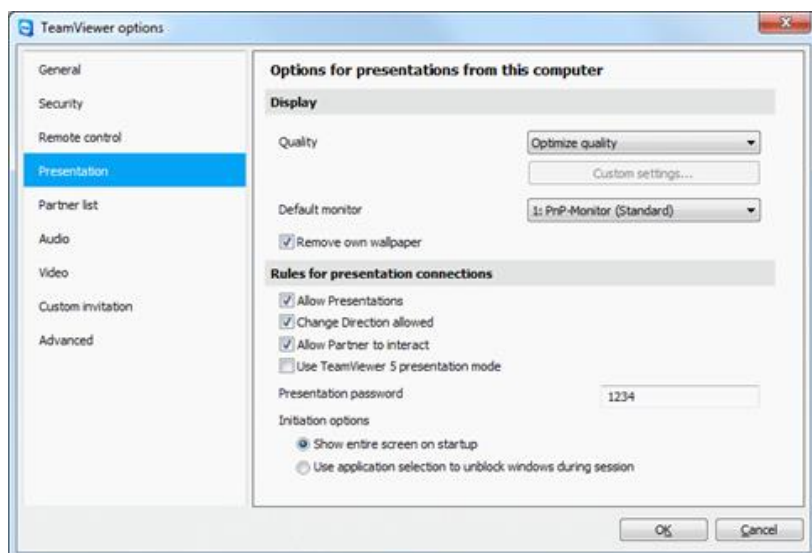
Prvo što se mora napraviti je da na svoj računar skinemo TeamViewer aplikaciju sa oficijelnih stranica i to TeamViewer <http://www.teamviewer.com/en/download/index.aspx>

Nakon što ste ga skinuli i pokrenuli imate mogućnost instalacije ili samo pokretanja programa bez instalacije (što je korisno za računare na kojima nemate administratorske ovlasti za instalaciju dodatnog software-a). Za dalji proces (za slučaj kada ga želimo instalirati na računar) potrebno je samo pažljivo pratiti uputstva i odabrati podešavanja koja nama odgovaraju na datom računaru

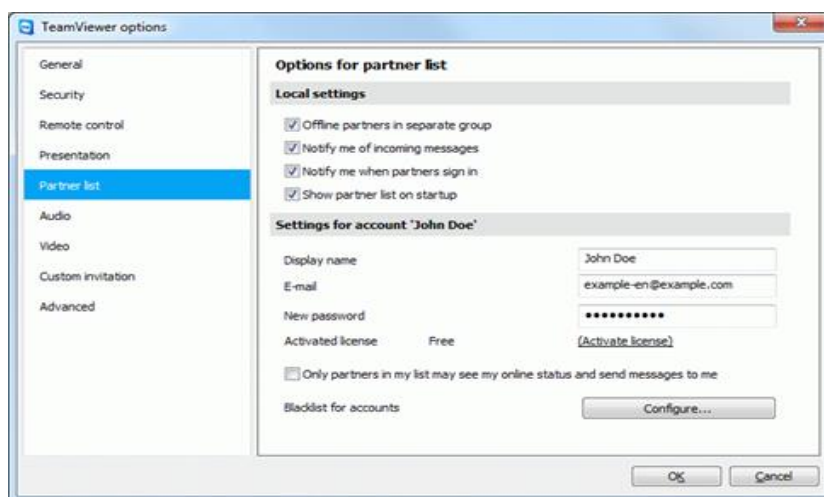


Slika 30 :TimeView postavka 1⁴⁸

⁴⁸ http://www.teamviewer.com/download/teamviewer_manual.pdf -05.10.2014



Slika 31: TimeView postavka⁴⁹

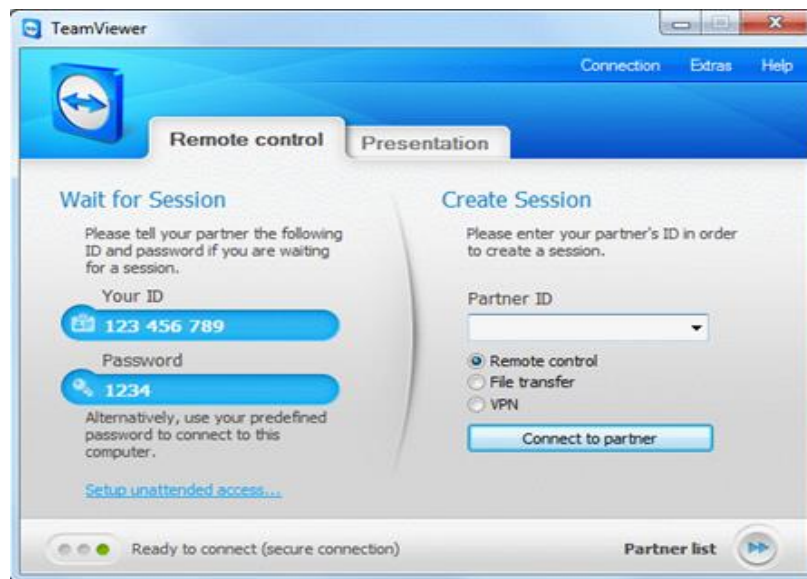


Slika 32: TimeViem postavka 3⁵⁰

Pokretanjem TeamViewer aplikacije u levom delu su vidljivi naš ID i šifra, ukoliko se neko sa istom aplikacijom želi spojiti na naš računar. U desnom delu pod ID upisujemo ID računara na koje se želimo spojiti, te odabiramo način spajanja. Za pokretanje konekcije potrebno je (logično) kliknuti na Connect... nakon čega se otvara novi „prozor“ gde je potrebno unjeti i šifru (koju smo sa ID-om trebali dobiti ranije, npr. od kolege.

⁴⁹ http://www.teamviewer.com/download/teamviewer_manual.pdf -05.10.2014

⁵⁰ http://www.teamviewer.com/download/teamviewer_manual.pdf -05.10.2014



Slika 33: TimeView glavni prozor⁵¹



Slika 34: TeamViewer „prozor“ za unošenje šifre pri konektovanju na računar⁵²

⁵¹ http://www.teamviewer.com/download/teamviewer_manual.pdf -05.10.2014

⁵² http://www.teamviewer.com/download/teamviewer_manual.pdf -05.10.2014

Naravno ista aplikacija ili Customare Modul (Korisnički Modul) TeamViewer QuickSupport mora postojati na računaru na koje se želimo spojiti, što je jednostavnije.⁵³ Jer isti modul je potrebno samo pokrenuti, nema nikakvog dodatnog klikanja, podešavanja. Možete ga poslati i e-mailom...

Pokretanjem korisničkog modula (u varijanti QuickSupport) odmah su vidljivi ID i šifra potrebni za spajanje na taj računar.



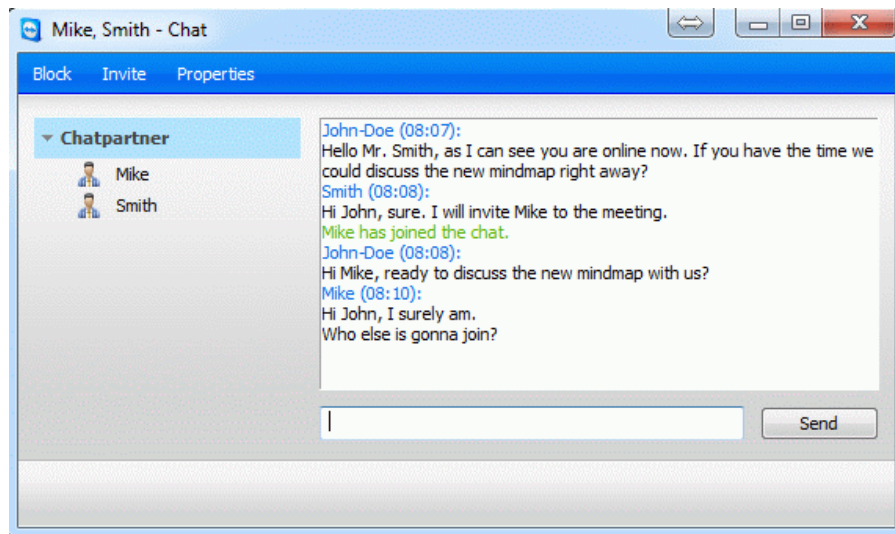
Slika 35: TeamViewer „prozor“ za QuickSupport⁵⁴

Nakon jednostavne instalacije i pokretanja na oba računara (koje želimo povezati) imamo veliki broj mogućnosti i opcija koje nam omogućava TeamViewer: pokretanje prezentacija, prebacivanje fajlova, chat... kao i ona verovatno nakorisnija i najkorištenija „popravlak računara prijateljima“ tj. čišćenje virusa, instalacija drajvera itd. i to sve tako da udaljeni korisnik (prijatelj), koji može biti čak i na drugom kontinentu, vidi sve što radite kao i da u svakom trenutku ima mogućnost da prekine „operaciju“ jednostavnim gašenjem TeamViewer-a.

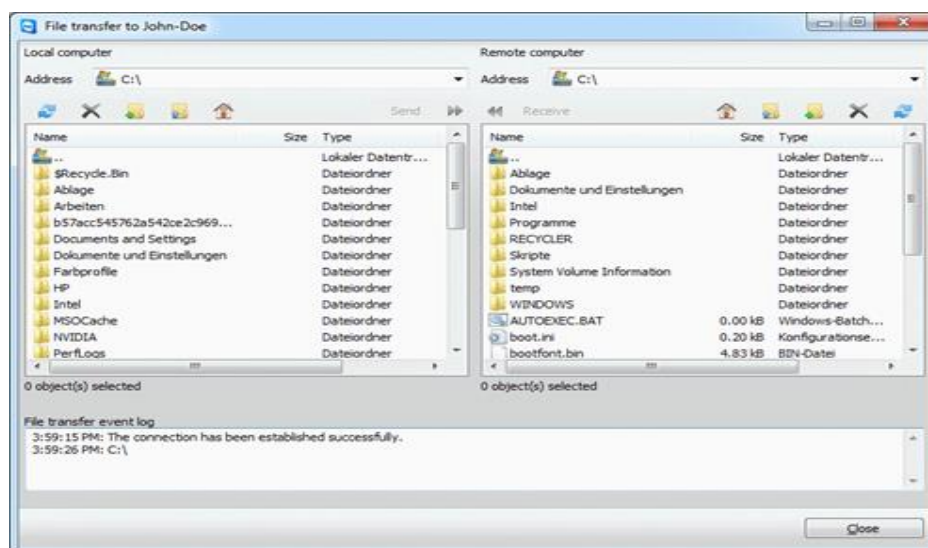
⁵³ http://www.teamviewer.com/download/teamviewer_manual.pdf -05.10.2014

⁵⁴ http://www.teamviewer.com/download/teamviewer_manual.pdf -05.10.2014

Prikaz nekih od funkcija:



Slika 36: TeamViewer Chat⁵⁵



Slika 37: TeamViewer File transfer⁵⁶

⁵⁵ http://www.teamviewer.com/download/teamviewer_manual.pdf -05.10.2014

⁵⁶ : http://www.teamviewer.com/download/teamviewer_manual.pdf -05.10.2014

22. STUDIJA SLUCAJA 2

UVOD

ROBLEM U FOKUSU

REŠENJE

INFORMATIČKI KRIMINAL U EKONOMIJI



22.1 Uvod

Kompjuterski kriminal predstavlja oblik kriminalnog ponašanja, kod koga se korištenje kompjuterske tehnologije i informacionih sistema ispoljava kao način izvršenja krivičnog dela, ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivično-pravnom smislu relevantna posljedica. Kompjuterski kriminal je takođe protivpravna povreda imovine kod koje se računarski podaci sa predumišljajem mjenjaju (manipulacija računara), razaraju (računarska sabotaza), ili se koriste zajedno sa hardverom (krađa vremena).

Kompjuteri i kompjuterska tehnologija se mogu zloupotrebljavati na razne načine, a sam kriminal koji se realizuje pomoću kompijutera može imati oblik bilo kojeg od tradicionalnih vidova kriminala, kao što su krađe, utaje, pronevere, dok se podaci koji se neovlašteno pribavljaju zloupotrebom informacionih sistema mogu na razne načine koristiti za sticanje protivpravne koristi. Pojavni oblici kompjuterskog kriminaliteta su: protivpravno korištenje usluga i neovlašteno pribavljanje informacija, kompjuterske krađe, kompjuterske prevare, kompjuterske sabotaze i kompjuterski terorizam i kriminal vezan za kompjuterske mreže.

.Protivpravno korištenje usluga se sastoji u neovlaštenoj upotrebi kompijutera ili njegovoj ovlaštenoj upotrebi ali za ostvarivanje potreba nekog neovlaštenog korisnika.

Primer neovlašćene upotrebe kompijutera je kada se kompijuter koristi u bilo koje druge svrhe, osim onih koje predstavljaju deo njegove namene u informatičkom sistemu. Prijeri ovlašćene upotrebe kompijutera, ali za potrebe neovlašćenog korisnika, ili radi ostvarenja drugih nedopuštenih ciljeva su npr., u slučaju kada zaposleni u jednoj firmi pribavi podatke za budućeg poslodavca ili kad raspoloživo kompijutersko vreme koristi za obavljanje nekih svojih poslova. Jedan od najčešćih oblika neovlašćene upotrebe kompijutera sa kojim se susreću poslodavci širom sveta jeste zloupotreba Interneta od strane zaposlenih.

Neovlašćeno pribavljanje informacija predstavlja svojevrsnu krađu podataka sadržanih u kompjuterskim sistemima, najčešće u cilju ostvarivanja protivpravne imovinske koristi. Tehničke i tehnološke mogućnosti za neovlašćeno pribavljanje informacija su sa pojavom Interneta postale mnogostruko veće tako da mete mogu biti i vaš lični PC ali i bilo koji povezani ili izolovani kompijuterski sistem.

22.2 Problem u fokusu

Usled velike količine podataka još se čini da je "filmska piraterija" na internetu nerealna. Ta oblast je ipak žestoko napadnuta, počev od 1999. godine kada je mnoštvo hakera krekovalo CSS-zaštite DVD-filmova. Da bi digitalizovana filmska traka mogla da se odmotava ne samo na Apple-sistemu i PC-sistemu, nego i na Open-Source Linux-u, industrijska zaštita od kopiranja stavljena je izvan snage. Od tada besni ogorčena borba - između ostalog o tome, u kojoj meri se ovde radi o (u mnogim državama dozvoljenom) reverzibilnom inženjeringu (Reverse Engineering), a u kojoj o prosto povredi autorskih prava. Borba protiv "softverske piraterije" ima nešto dužu tradiciju. Bussines Software Alliance (BSA) na svojoj austrijskoj web stranici navodi 1996. godinu kao početak borbe protiv pirata, nemačka BSA uprkos svoje kampanjestrha ("Svi imate razloga da budete nervozni"), 2001. godine konstatuje boom internet-piraterije i obelodanjuje 533 mirujuća sajta. Warez-scene (ilegalno kopiranje software-a, termin nastao u USA poznatih sedamsedetih godina - prim.prev.) koje na duge staze nisu podsticane komercijalom već strašću, ukazuju na onu oblast u kojoj su internet-pirati načinjeni mediskim zvezdama, oblast prema kojoj filmska i software-ska piraterija deluju kao bagatela: muzičke fanove na internetu. Sa početkom osamdesetih godina, muzička industrija je u akciji velikih razmera prebacivala posao za konzumente u digitalnu formu. CD (kompakt disk), kao sledbenik LP (longplej ploče) još uvek je bio shvaćen kao fizički nosilac podataka i isto tako malo je čuvan od kopiranja kao i analogna vinilska ploča. Naučnici na Fridrih-Aleksander univerzitetu u Erlangenu su u isto vrijeme, od 1987. godine na tamnošnjem Fraunhofer-Institutu za integrisane ploče (IIS-A) razvili komprimovanje digitalizovanih zvukova. Erlangenški tim je unutar Moving Pictures Expert Group (MPEG) postao vodeće pero u razvoju "MPEG Audio Layer-3", ukratko: MP3, u internacionalnim standardizovanim oznakama. Izvorni encoder bio je mali i komplikovan za korisničku upotrebu - a širio se eksplozivno. Naredni programi koji su vrlo brzo kursirali Shareware, bili su CD-Ripper koji je audio podatke sa nosača zvuka kopirao na hardisk. Sa jeftinom raspoloživošću CD-rezačima i CD-romovima na kojima se mogao unositi zapis, otpala je i poslednja barijera koja je sprečavala identično umnožavanje digitalnih nosača zvuka bez gubitka kvaliteta, što je postao raširen fenomen. Ali pre svega, to je omogućilo internetu da tako nastale kolekcije fajlova svih vrsta i bez fizičkog transporta podataka objedini u respektivne nosače zvuka. Postoji sve više programa koji muzičkim fanovima omogućavaju da preko interneta dođu do muzike. Gigantska zajednica koja više nije bila upućena na školsko dvorište da bi razmenjivala kasete, započela je na internetu živu diskusiju u vezi sa muzikom. Uskoro su se lokalne piratske stanice sa ultra kratkih talasa prebacile na Real Audio Stream. Od 1996. godine, postojala je Internet Chat Groups (IRC) koja je sebi pripisala širenje MP3 fajlova. Muzika je brzo našla put od korisnične mreže do WWW, od tekstualne naredbe do grafičke korisničke površine, od specijalnog znanja do masovnog fenomena. Sve više su programi nalik browserima nudili pristup muzici; inspirisan IRC-om i MP3-mašinama za pretragu, mladi student Šon Fening (Shawn Fenning) je u januaru 1999.

godine u igru uveo istinsku "Killer Application". Kada je startovala beta-verzija njegovog softwara, Napster na download.com, odmah je u maju 1999. godine osnovao Napster.com i tako dao podsticaj strmoglavoj karijeri Peer-to-Peer (P2P) menjanju file-ova. Muzičkoj industriji su bili potrebni meseci da bi samo primetila novinu. Slušaoci su utoliko brže reagovali: prema studiji firme PC Pitstop (koja nije iznosila neodmerene podatke) u jesen 2000. godine software je već bio instaliran na gotovo svakom trećem personalnom računaru priključenom na internet. Prema podacima firme, na Napster je istovremeno pristupalo do milion korisnika. Poređenja radi: kao najveći servis provajder na svetu AOL (America On Line) u vreme najveće posete na mreži, istovremeno gotovo da i nema više do 1,5 miliona korisnika. Na pozadini snažno centralizovane muzičke branše orijentisane prema objektima i još uvek nadasve masovne legalne ponude muzike na mreži, naredne P2P platforme su rasle kao pečurke poslije kiše - Gnutella, Scour, Mojo Nation & Co.

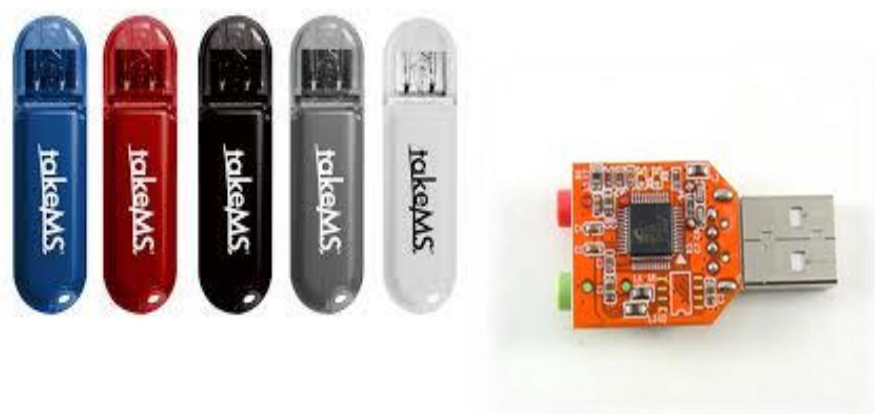
22.3 Rešenje

Brojne firme čekaju, spremne da zarade mnogo novca posredstvom zahteva za sigurnost, zaštitu od kopiranja i nadziranja. "Tehničke mjere" i "Informacije za razumevanje prava" koje su opraštajuće EU-Pravne smjernice 2001. godine u međuvremenu decidirano stavile pod pravnu zaštitu, postaviće na nove osnove nosačima zvuka, videom koji su zaštićeni autorskim pravima. Digital Records Menagement (DRM) nudi mogućnost, da internet od strane "Copyright Industries" prikazan u najužasnijim bojama piratskog raja, postane medijum totalne kontrole. Američki ekspert za ustavno pravo i za prava na internetu Lorens Lesig (Lawrence Lessig) upozorava na, među apologetama interneta, rasprostranjeno verovanje u "prirodu informacija ili informacionih tehnologija". Statički optimizam legendarnih stavova poput "informacija želi da bude slobodna" ili "Mreža interpretira cenzuru kao štetu i odbacuje je", on klasifikuje kao naivni "jeizam" (Is-Is). Riskantno je poći od toga, da internet "jeste, kakav jeste" - jer internet konačno nije šaka puna protokola, kod stvoren od strane čoveka - koji je s vremenom iskusio drastične promene. I zakonodavci su sasvim sigurno svesni da se svet ne sastoji samo od vlasnika prava. Takođe ne zvuči ni naročito verovatno da će korisnici industrije zabave masovno biti spremni da radi slušanja muzike pokažu dozvolu za posedovanje digitalnog oružja ili Dongle (mali hardware koji se konektuje na kompjuter da bi identifikovao neke delove software-a). Koliko dalekosežno bi mogla da ode izgradnja digitalnog sveta u toku "borbe protiv pirata" tumačila su 2001. godine prodorna razmišljanja Intela, IBM-a, Tošibe (Toshiba) i Matsušite (Matsushita), da naprave zaštitu od kopiranja u okviru generičkog hardvera. Da biste kopirali hard disk C na hard disk D, molimo Vas pokažite nam Vašu legitimaciju. Još pre nego što su se zadimili topovi usmereni ka navodnim piratima, svijet je postao kovčeg sa blagom konkvistadora. Uostalom, jedan pogled ka muzici može ponuditi podsticaje za originalne izlaze iz konfuze situacije kako za "konzumente", tako i za Copyright-industriju. Na primjer, historija uspjeha benda "Grateful Dead" započinje kada su muzičari prestali svojim fanovima da uskraćuju autorskim pravima "zabranjene" delove koncerata. Njihov tekstopisac Džon Peri Barlou (John Perry Barlow) uostalom zna da

barem u oblasti umetničkog stvaranja bez daljnjeg nije moguće ne biti "pirat": "Koliko muzičara može iskreno reći da nikada nisu iskoristili nešto čega je bilo i ranije?". I profesionalni protivnici kopiranja počinju da osećaju da je to pitanje prikladno; ponuđač DRM-a Inter Trust je početkom 2001. godine optužio kolege iz Microsoft-a zbog povrede patenta od strane tehnike zaštite od kopiranja ugrađene u Windows Media Player. Iz piratske perspektive posmatrano, to je jedan mnogo obećavajući feedback - ali ipak,naočigled sve češće igre među firmama koje razvijaju hardver i softver u vezi sa optužbama za patente, bilo bi pre nagljeno očekivati da će različiti naraštaji zaštite autorskih prava jedni druge kočiti u tolikoj meri, da između njih još uvek ostane prostora za sasvim normalan napredak. U svakom slučaju, čini se da bi osnovnim mislima zaštite autorskih prava nagrađivanju i podsticanju kreativnosti ,fundamentalno protivrečilo, da razvoj i napredak kao zadatak svih, budu prepušteni samo piratima. Poslednji pogled u prošlost povezan sa nadom, da će nezgrapna antipiratska propaganda ponovo ustupiti mesto začuđujućoj višeslojnosti, koja je u Evropi prije milenijuma bila dovodena u vezu sa "piraterijom". Ključna reč pripada grčkom rječniku: "peirates: morski razbojnici; od pieramai: pokušati, prioniti na posao, truditi se, težiti, preduzeti, odvažiti se; nešto pokušati ili isprobati, proveriti, istraživati; okušati sebe ili svoju sreću u nečemu; odvažiti se na napad, zapodenuti borbu sa nekim; dovesti u iskušenje; truditi se oko nečije naklonosti; udvarati se ljubljenoj, učiti iz iskustva".

23.STUDIJA SLUČAJA 3

Digitalna forenzika usb (flash)memorije i akvizicija podataka



23.1 Akvizicija podataka sa flash diska

Proceduru akvizicije ranije smo teoretski opisali, ali želimo i da napravimo praktično uputstvo. Glavna ideja je bila da uz pomoć dostupnih besplatnih alata izvršimo proces akvizicije, koji ne bi bio oboriv na sudu.

U eksperimentu smo koristili prenosivu fleš memoriju veličine 1GB. Celi proces izveden je uz pomoć CAINE forenzičke distribucije, koja se besplatno može preuzeti sa interneta.

23.1.1 Utvrđivanje tipa memorije

Prvi zadatak pri akviziciji bio je utvrđivanje stvarne veličine memorije i priprema sterilnih medija. Vizuelnim posmatranjem utvrđeno je da je u pitanju USB memorija fleš tipa, proizvođača Kingston, veličine 1GB. Do tog podatka došli smo ne samo posmatranjem memorije u oklopu, već smo oklop uklonili, a zatim podatke pročitali sačipa. Te podatke još jednom smo proverili i softverski uz pomoć alata DiskUtility.



Slika 38: Informacije o disku – predmetu istrage

Naravno zaštita od upisivanja bila je obavezna. Kako je u pitanju forenzička distribucija kojoj je to default vrednost nismo imali posebne potrebe da je aktiviramo.

23.1.2 Priprema starilinih medija

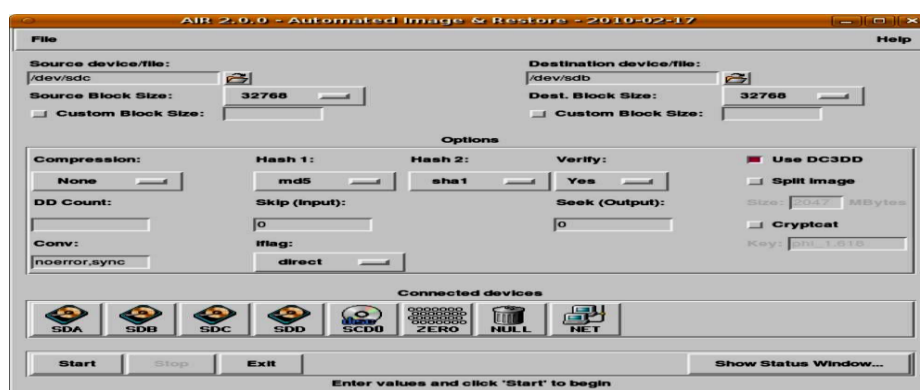
Najidealnija situacija bila bi kada bi bili u mogućnosti da imamo još dve potpuno iste memorije, ali to je retko moguće. Kako je nemoguće nabaviti istovetni fleš disk, za 54 kopije smo odabrali dve memorije istog kapaciteta kao što je i memorija koju ispitujemo. Pre procesa kopiranja bit po bit, iako većina alata tokom tog procesa narušava prethodno stanje, memorije je potrebno formatirati. Sam fajl sistem nije toliko bitan, koliko je bitno uništiti postojeće podatke na memoriji, ali smo se mi odlučili da ne dodelimo ni jedan.



Slika 39: Priprema sterilnog medija

23.1.3 Forenzičko kopiranje

Nakon što su sve pripreme izvršene prelazi se na pravljenje forenzičkih kopija. Za taj deo akvizicije odabrali smo AIR (Automated Image and Restore). Program poseduje sve potrebne mehanizme za forenzičko kopiranje kao što je pravljenje MD5 i SHA heševa i detaljno izveštavanje.



Slika 40: Air - Automated Image and Restore interfejs

Dobijene vrednosti heša moraju se zapisati, ne bi li proverili da li je sve u redu nakon formiranja radne kopije. Ako se heš vrednosti dobijene sa radne kopije i originala poklapaju, proces akvizicije je završen i možemo pristupiti analizi. Osim na fizičke medije, programi za forenzičko kopiranje nude i pravljenje slike uvidu fajla, najčešće ekstenzije .dd. Ovu ekstenziju lako je otvoriti u programima zaforenzičku analizu, a npr. uz alat WinImage moguće ga je konvertovati u .iso format.

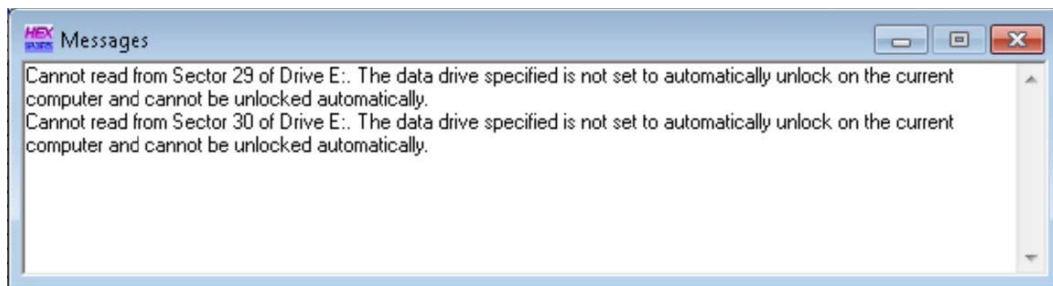
23.2 Pristup podacima na zaključanim memorijama

U želji da onemoguće pristup podacima na prenosivim memorijama kriminalci ih često zaključavaju. Dokazi nisu prisutni samo na fleš diskovima onih koji se bavekompjuterskim kriminalom već uopšte. U literaturi o forenzici prenosivih memorija, neizbežan je primer iz 2001. godine kada su istražitelji FBI došli do fleš diska jednogod šefa mafije, na kome su se nalazili podaci o bankarskim transakcijama, tj. optužujući dokazi. Na njihovu nesreću disk je bio zaključan, pa su paralelno krenuli sa brute force napadom i razvojem keylogger alata. Nakon 3 meseca ne samo da su uspeli da u njegov računar ubace špijunski softver, već je i tim psihologa na osnovuostalih stvari kucanih na računaru došao do potrebne šifre, dok brute force napad nijedao nikakve rezultate. Odluka odeljenja za tehnološki kriminal FBI nakon ovogslučaja bila je da se svi resursi prebace na razvoj špijunskih alata, a obustavi razvoj alata za pronalaženje šifara.

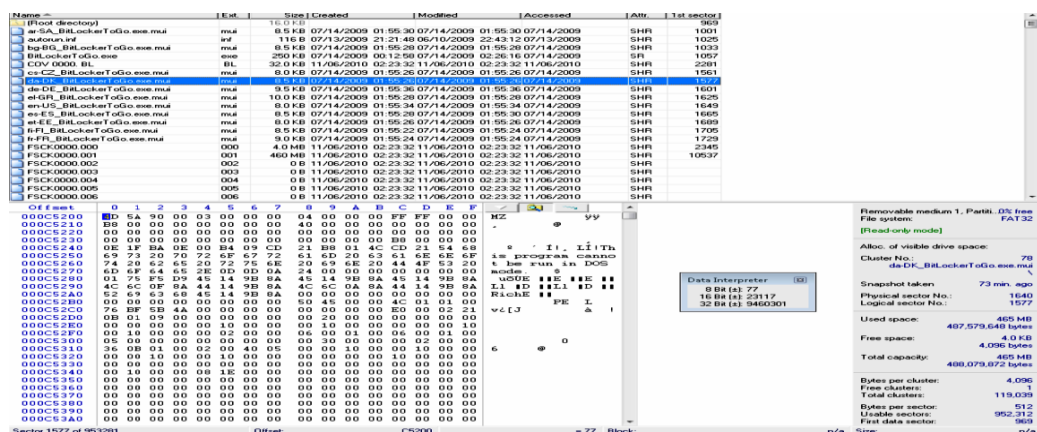
Danas nimalo nije lako ispratiti sveopšti nalet alat za zaštitu svih vidova memorija, ne samo prenosivih. U moru softverskih zaštita izdvajaju se PGP enkripcija i BitLocker, i za koje u svojim operativnim sistemima stoji kompanija Microsoft. Razvoj PGP enkripcije u stopu prate alati ruske kompanije Elcom Soft i po nekom ustaljenom običaju mesec do dva dana od unapređenja, nude način za razbijanje postavljene zaštite. Microsoft se dičio time da je njegova enkripcija neprobojna, ali ni to nije dugo potrajalo. U našem slučaju zaključali smo fleš memoriju veličine 512mb uz pomoć BitLocker alata, dodelili joj šifru za pristup „singidunum“, a zatim pokušali da do te šifre dođemo uz dostupne alate.

23.2.1 Otkrivanje zaštite

Svakako najbitnije nakon forenzičkog kopiranja jeste otkrivanje da zaštita postoji. Neretko dolazi do greške i neiskusni forenzičari zaključanu memoriju, posebno kada se radi o enkripcijama na celom disku, kakva je BitLocker, smatraju oštećenom. EnCase alat uspešno detektuje Windows Vista BitLocker zaštitu i poseduje alat za njeno razbijanje, dok onu postavljenu u Windows 7 sistemu vidi kao oštećenu memoriju. Da bi se greške svele na minimum moraju se ispratiti svi principi akvizicije dokaza, a sama zaštita i njeno razbijanje spadaju u domen forenzičke analize. BitLocker zaštita lako je primetna u alatima za analizu. Pri eksperimentu, izvršili smo forenzičko kopiranje fizičke memorije u fajl, a zatim ga analizirali, forenzičkim alatom WinHex (slika 36). Najnovija verzija ovog alata pri pokušaju otvaranja logičkog diska jasno pokazuje da je memorija zaključana, a pri fizičkom sve što se na njoj nalazi, odnosno fajlovi koji operativnom sistemu jasno pokazuju kako da njome upravlja i aktivira sistem za otključavanje.



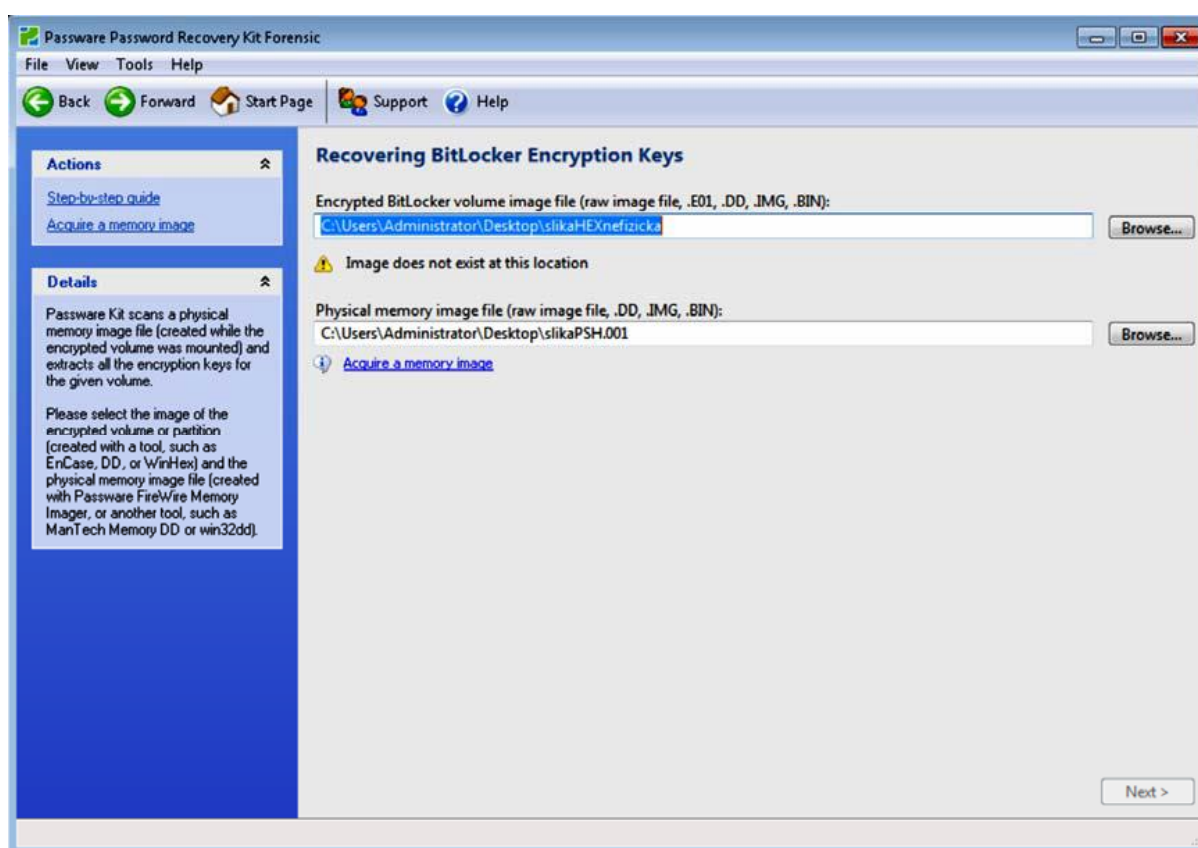
Slika 41: Obaveštenje o zaključanoj memoriji



Slika 42: Pregled fajlova zaključane memorije u alatu WinHex

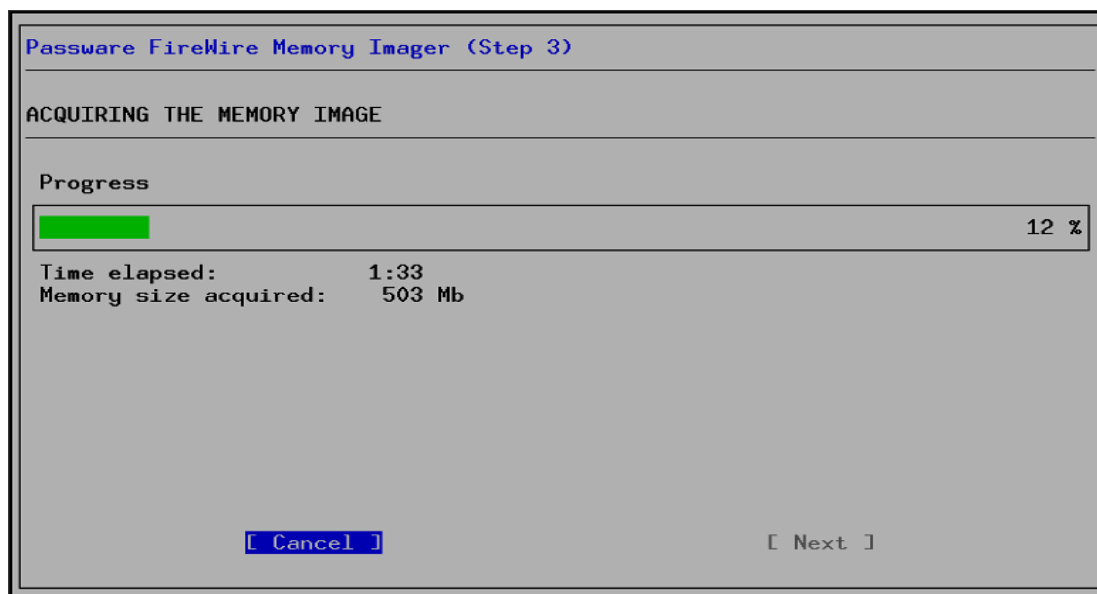
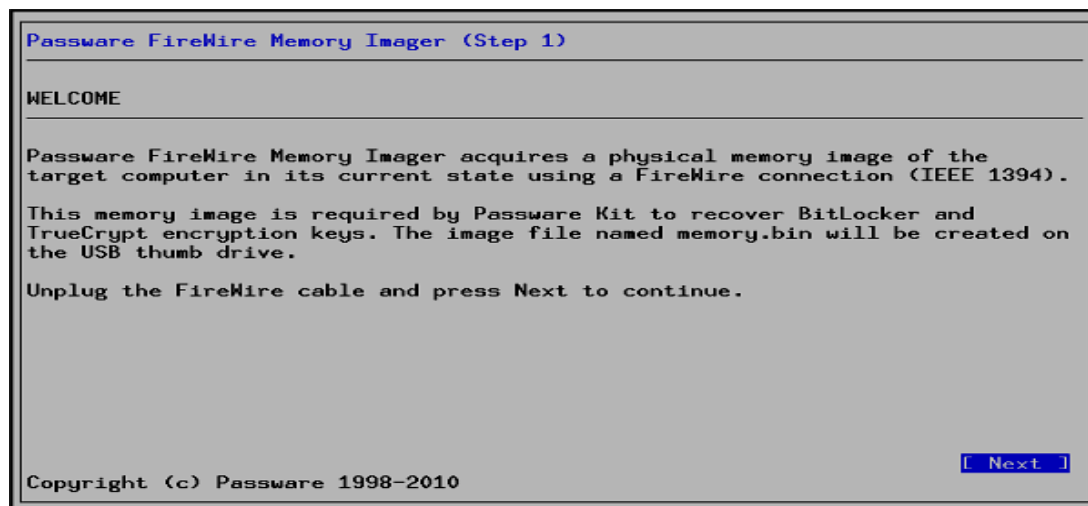
23.2.2 Otključavanje memorije

Jedini alat koji trenutno može otključati memoriju zaključanu BitLocker je neforenzički alat kompanije PassWare – Passware Kit Forensic 10.1 (slika 38). Iako u svom nazivu ima forenziku, on nije priznat forenzički alat, ali je ovo jedan od načina kompanije da se eventualno uključi u taj posao. Za postupak otključavanja alat zahteva dve fizičke kopije diska, jer se sam process otključavanja vrši upoređivanjem. Jedna od potrebnih kopija pravi se uz pomoć standardnih alata kao što su EnCase i WinHex, a druga uz pomoć Passware FireWire Memory Imager-a. Iako naznačava da se druga kopija može izraditi i drugim alatima kao što je win32dd, svaki pokušaj da sa takvim kopijama dođemo do željenog rezultata program je prekidao.



Slika 43: Passware Kit Forensic 10.1

Za dobijanje druge potrebne kopije moraju se upotrebiti dva računara sa FireWire portom. Program sam formatira disk i nasnimava na posebnoj Linux particiji forenzički alat. Zadatak forenzičara je da računar startuje uz pomoć tog diska, a zatim sledi instrukcije (slika 39). Na drugom računaru ne moraju postojati nikakve posebne pripreme, može biti uključen bilo koji operativni sistem. Kako je memorija šifrom zaštićena od upisivanja nije potrebno ni posebno štititi. FireWire ima direktan pristup memoriji, na fizičkom nivou bez kontakta sa operativnim sistemom, a alat sam pronalazi sve fleš diskove povezane na drugi kompjuter. Fizička slika diska smešta se na istom disku sa koga je podignut alat, te se zato uvek mora imati u vidu veličina diska koji se procesuiru i veličina diska na kome je alat.



Slika 44: Passware FireWire Memory Imager

Nakon što su svi potrebni elementi bili spremni, programu je bilo potrebno dvadesetak minuta da dođe do šifre kojom je fleš disk bio zaključan.

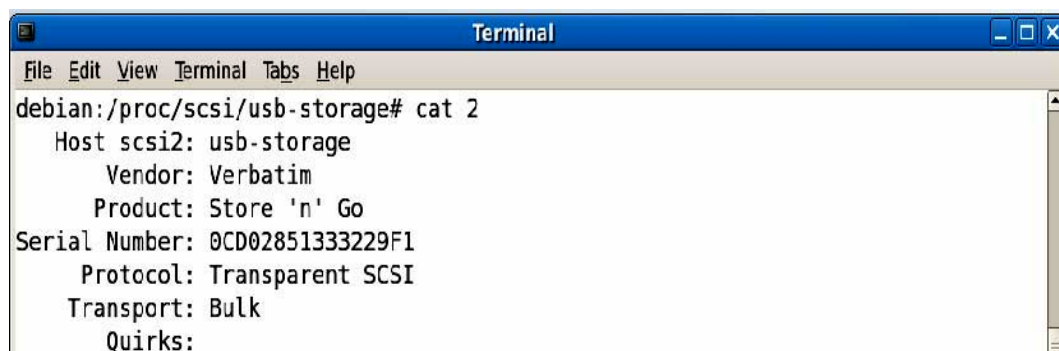
23.3 Praćenje USB uređaja povezanih na računar

U procesu rada računara sa USB uređajima uvek treba imati u vidu važan princip – da će doći do promene u sistemu. Kada se prenosivi disk priključi na Windows operativni sistem, rezidenta informacija o uređaju ostaje u računaru. Takve informacije itekako mogu biti od koristi, kada je bitno dokazati vezu nekog računara sa podacima na određenom fleš disku. Iako, danas, postoji par programa, koji forenzičaru mogu pružiti informacije o USB uređajima koji su ranije ili sada povezani na računar najsigurniji je „pešački“ metod.

Na Windows operativnim sistemima postoje nekoliko identifikatora koji pokazuju da li je neki uređaj bio povezan na univerzalnu serijsku magistralu. Neki od njih su isti za sve uređaje tog tipa, ali postoje i oni jedinstveni. Drugi ključni faktor koji čini te identifikatore važnim forenzičarima, jeste činjenica da se oni mogu pratiti i kada je sistem zatvoren. Stoga se mogu koristiti u forenzičkoj istrazi da identifikuju specifične uređaje.

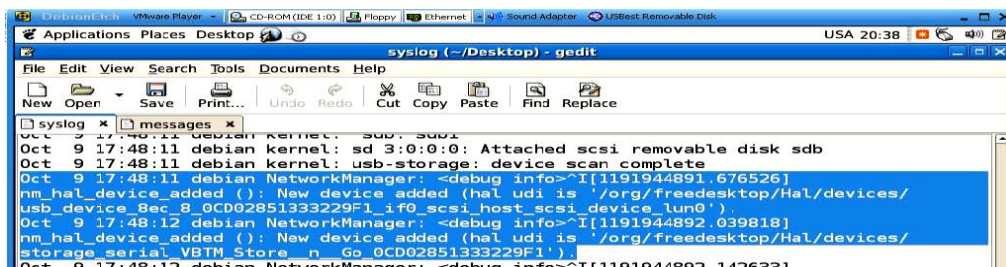
23.1.1 Linux OS

Na Linux operativnim sistemima identifikatori USB fleš diskova su jasni, konkretni i dosledni. Pored informacije o proizvođaču uređaja postoje i jasne informacije koje ukazuju na sve one informacije vezane za sam disk (veličina, serijski broj, serija...). Da bi dokazali ovu tvrdnju povezali smo na računar sa instaliranim Linux (Debian) sistemom fleš disk u dva navrata. Najpre prvi put kada je u svom logu on i upisao informacije o uređaju, a zatim drugi put nakon dve nedelje.



Slika 45: Linux terminal prozor sa informacijama o povezanom fleš disku

Prikupljene informacije, koje se inače nalaze u messages.log i sis log datotekama uporedili smo ne bi li dokazali da su svi identifikatori isti za taj uređaj.



Slika 46: Linux syslog datoteka sa informacijama o povezanom fleš disku

Poređenjem informacija na slici 45 i 46, informacije kao što su serijski broj, skraćenica od imena proizvođača (VBTM za Verbatim) i ime proizvoda (Store_n_Go) u potpunosti se slažu. Ova informacija ne samo da je uspešno sačuvana, već se u potpunosti slaže sa informacijama koje smo daljim ispitivanjem dobili o istom proizvodu na Windows operativnim sistemima.

23.3.2 Windows OS

Operativni sistemi kompanije Microsoft pri uključivanju uređaja u USB port najpre pozivaju informacije uskladištene u USB hub drajveru iz kojeg dobija informaciju o tipu povezanog uređaja. Nakon detekcije tipa uređaja, Windows traži drajvere za sam uređaj, a za sve to potrebno je da ima sve informacije o uređaju. Tom prilikom operativni sistem pravi jedinstvenu deskripciju i jedinstven profil. Nakon formiranja profila Windows traži potrebne instrukcije za rad u usbstor.inf datoteci, zatim preko Windows Update servisa (ako je računar povezan na internet i ako je korisnik to dozvolio ranijim podešavanjima), a ako ne postoji bilo šta za taj uređaj pokreće se generički drajver – generic mass storage device. Informacije na osnovu kojih se vrši pretraživanje u usbstor datoteci nalaze se u hardveru.

Na Windows sistemima identifikator uređaja koji se formira je u formatu USB\VID_v(4)&PID_d(4)&REV_r(4). Po informacijama kompanije Microsoft v(4) je četvorocifreni broj proizvođača, dodeljen od strane nadležnih komisija, d(4) – broj koji proizvođač dodeljuje uređaju, a r(4) je revizija koda (Microsoft 2007). Ilustrovano na određenom uređaju u device manager-u „USB\VID_08EC&PID_0008\0CD0285133229f1“, gde je 08EC kod proizvođača, 0008 kod proizvođača, a 0CD0 je revizioni kod. Svi identifikatori su jedinstveni i predstavljaju ID uređaja (Device Instance ID).

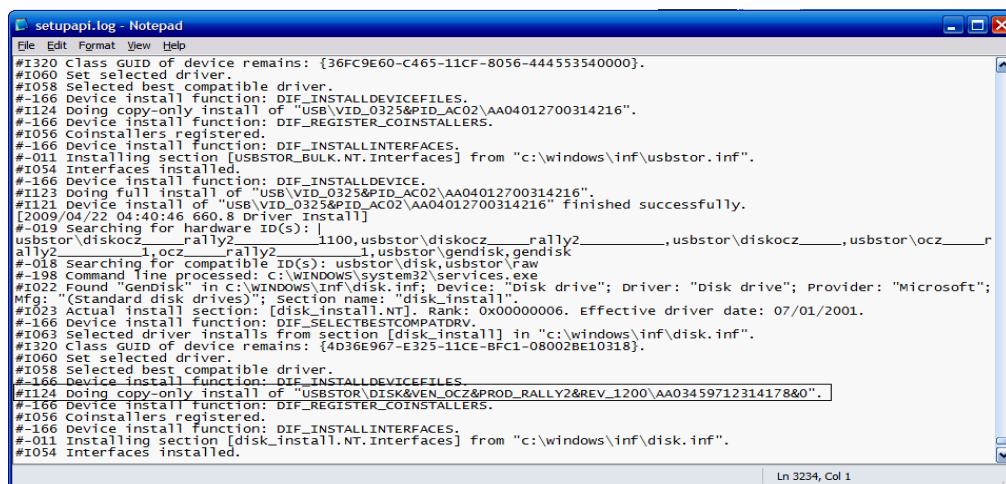


Slika 47: Windows Device Manager

Najviše informacija za forenzičara u Windows operativnim sistemima nalazi se u registry bazi. Windows registry skladišti sve informacije o svim aspektima računara kao što su hardver, aplikacije, korisnici... Najbitnije za forenzičara je da na zna šta i gde da traži. Što se USB uređaja tiče najviše informacija se nalazi na lokaciji.

Na toj HKEY_LOCAL_MACHINE\System\ControlSet00x\Enum\USBSTOR lokaciji nalaze se informacije o svim uređajima koji su putem USB veze ikad povezivani na računar sa Windows sistemom. Pretraživanjem ključeva, lako se može doći do informacija o povezanim USB fleš memorijama, na osnovu njihovog Device Instance ID – a.

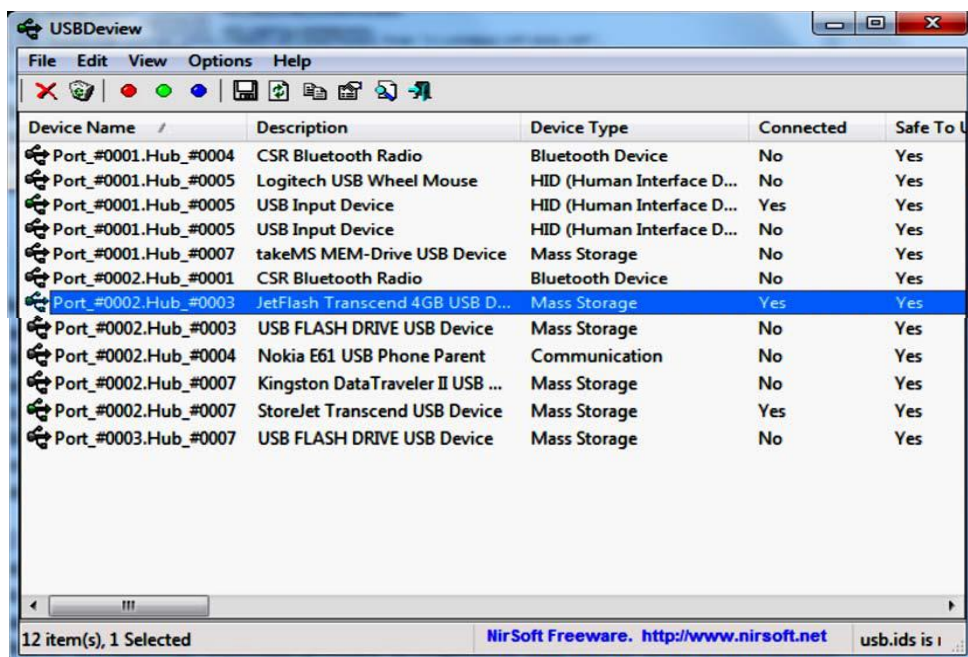
Sajt www.anti-forensics.com koji se bavi načinima za uništenje digitalnih dokaza, navodi brisanje USBSTOR ključa u registry bazi kao drugog po važnosti za uklanjanje dokaza na Win OS, odmah nakon brisanja Windows hibernacionog fajla. Takođe kada se radi o operativnom sistemu Windows XP, treba imati u vidu i fajl setupapi.log koji se nalazi u rootu windows operativnog sistema, u kome se takođe nalaze svi zapisi vezani za povezane uređaje



```
setupapi.log - Notepad
File Edit Format View Help
#I320 Class GUID of device remains: {36FC9E60-C465-11CF-8056-444553540000}.
#I060 Set selected driver.
#I058 Selected best compatible driver.
#-166 Device install function: DIF_INSTALLDEVICEFILES.
#I124 Doing copy-only install of "USB\VID_0325&PID_AC02\AA04012700314216".
#-166 Device install function: DIF_REGISTER_COINSTALLERS.
#I056 Coinstallers registered.
#-166 Device install function: DIF_INSTALLINTERFACES.
#-011 Installing section [USBSTOR_BULK.NT.Interfaces] from "c:\windows\inf\usbstor.inf".
#I054 Interfaces installed.
#-166 Device install function: DIF_INSTALLDEVICE.
#I123 Doing full install of "USB\VID_0325&PID_AC02\AA04012700314216".
#I121 Device install of "USB\VID_0325&PID_AC02\AA04012700314216" Finished successfully.
[2009/04/22 04:40:46 660.8 Driver Install]
#-019 Searching for hardware ID(s):
usbstor\diskocz____rally2____1100,usbstor\diskocz____rally2____,usbstor\diskocz____,usbstor\ocz____rally2____1,ocz____rally2____1,usbstor\gendisk,gendisk
#-018 Searching for compatible ID(s): usbstor\disk,usbstor\raw
#-198 Command line processed: C:\WINDOWS\system32\services.exe
#I022 Found "gendisk" in C:\WINDOWS\inf\disk.inf; Device: "Disk drive"; Driver: "Disk drive"; Provider: "Microsoft"; Mfg: "(Standard disk drives)"; Section name: "disk_install"
#I023 Actual install section: [disk_install.NT]. Rank: 0x00000006. Effective driver date: 07/01/2001.
#-166 Device install function: DIF_SELECTBESTCOMPATDRV.
#I063 Selected driver installs from section [disk_install] in "c:\windows\inf\disk.inf".
#I320 Class GUID of device remains: {4D36E967-E325-11CE-BF01-08002BE10318}.
#I060 Set selected driver.
#I058 Selected best compatible driver.
#-166 Device install function: DIF_INSTALLDEVICEFILES.
#I124 Doing copy-only install of "USBSTOR\DISK&VEN_OCZ&PROD_RALLY2&REV_1200\AA03459712314178&0".
#-166 Device install function: DIF_REGISTER_COINSTALLERS.
#I056 Coinstallers registered.
#-166 Device install function: DIF_INSTALLINTERFACES.
#-011 Installing section [disk_install.NT.Interfaces] from "c:\windows\inf\disk.inf".
#I054 Interfaces installed.
```

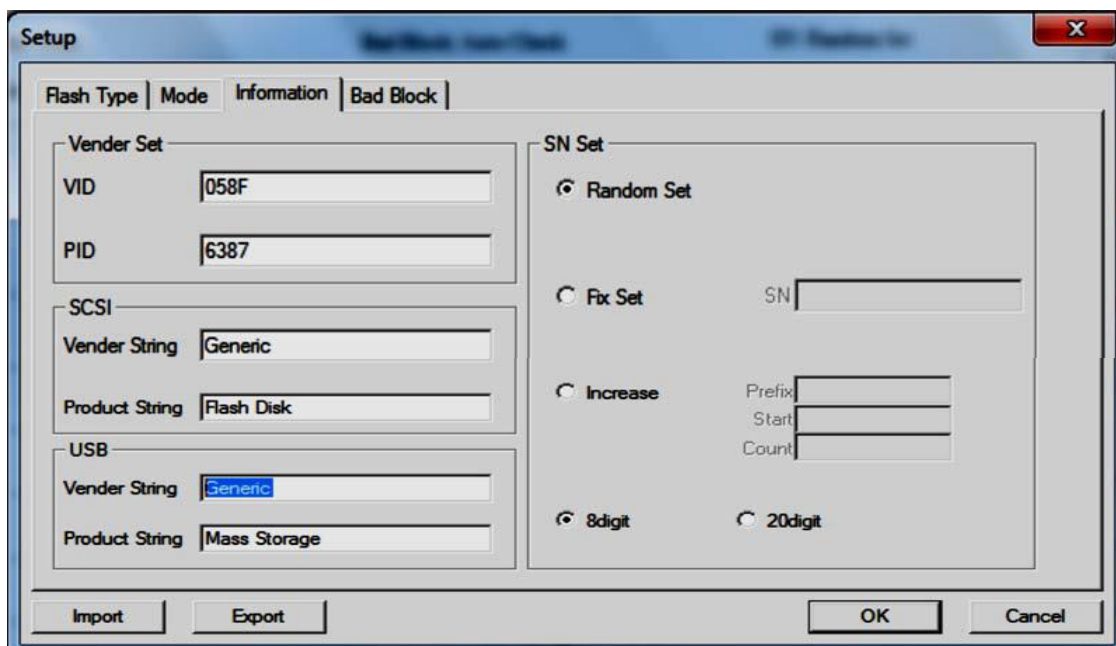
Slika 48: Windows XP setupapi.log fajl

Osim metode pretraživanja registry baze, brojni softverski alati koji pouzdano i sortirano prikazuju sve informacije iz registry baze. Među njima najviše se izdvojio USBDeview, alat kompanije NirSoft, koji osim za pregled dokaza može koristiti i za njihovo uništavanje.



Slika 49: USBDeView

Iako postoje svi ovi identifikatori u sistemu, u današnje vreme se ne mogu koristiti previše. Razlog tome, osim uništavanja dokaza jeste i to što danas postoji veliki broj NO NAME proizvođača, koji ne popunjavaju sve potrebne podatke tj. pre proizvodnje ne kontaktiraju „USB Implementers Forum”⁵⁷ – fondaciju postojećih proizvođača. Osim toga jedna ruska hakerska grupa na svom forumu za sve članove koji joj prilože nešto, nudi besplatan softverski alat za izmenu firmware-a fleš memorija. Njime se mogu zameniti svi identifikatori a i formatiranjem potpuno iskoristiti sav memorijski potencijal, često namerno zanemaren zbog politike cena po kojima se prodaju memorije.



Slika 50: Podešavanje proizvođačkih unosa

⁵⁷ www.usb.org – 16.10.2014



Slika 51: Izemljeni podaci Transcedent fleš diska

23.3.3 Povratak podataka sa oštećene USB fleš memorije

Neretko se dešava da forenzičari imaju posla sa fleš memorijama koje su oštećene iz raznoraznih razloga. U praksi se pokazalo da često dolazi do oštećenja zbog slabog/neujednačenog napona na USB kontrolerima, ali i namerno prilikom nasilnog prekida transvera podataka. Nažalost mnogi forenzički alati nemaju mehanizam za rad sa takvim memorijama, pa treba pristupiti i ostalim alatima koji su dostupni. Ovi alati najčešće su pravljeni za povratak podataka sa formatiranih fleš memorija, pa u tu svrhu mogu poslužiti i forenzičarima, jer mnogi kompjuterski kriminalci, najčešće, osim fizičkog sakrivanja, pribegavaju formatiranju, ne bi li uništili dokaze na njima.

U našem slučaju napravili smo eksperiment, tako što smo najpre presnimili podatke sa jednog USB fleša, zatim ga namerno oštetili, a onda pokušali da povratimo datoteke sa njega. Oštećenja smo pravili i logički prekidanjem kopiranja podataka na NTFS particiji i fizički spajanjem jednosmerene struje od 12V na konektore USB flash drajva. Komparacija oštećenih podataka sa originalom dala nam je tačan uvid u kvalitet ispitanih softverskih alata. Prilikom ocenjivanja alata uzeli smo u obzir još par stavki, kao što su vreme, koje je bilo potrebno za povratak i struktura povraćenih podataka.

Pre svega treba utvrditi da li je memorija stvarno oštećena, a to je često i najveći problem na koji forenzičar nailazi. Postupanje sa memorijom, koja je obeležena kao oštećena ili pak zaključana, svodi se na uhodane principe kojih se treba držati. Kao što smo ranije naveli pre rada treba napraviti kopiju i radnu kopiju memorije. Međutim kod oštećenih memorija to nije baš lak princip, jer u njima postoje sektori koje nije moguće pročitati, te ih alati koji služe za kloniranje, pri kopiranju, često upisuju kao UNREADABLESECTOR (*WinXex alat*). Zbog tih problema treba se držati isključivo fizičkog kopiranja, bez dodatnih upisa od strane alata. Alati koji su imali najmanji procenat greške u ovim postupcima su *Man Tech Memory DD* i *Passware FireWire Memory imager*. Nažalost neki put ni oni sami ne mogu da naprave fizičku kopiju memorije, ili je problem vreme koje je potrebno za akviziciju, pa se mora raditi sa samom memorijom.

Najčešći dokaz da je memorija oštećena, a ne zaključana je obaveštenje operativnog sistema da nije u mogućnosti da otkrije tip fajl sistema koji je aktivan. Ta pojava nije vezana samo za operativne sistem već i za napredne forenzičke alate koje smo isprobali. Univerzalni način ne postoji, ali svakako se preporučuje da u slučaju da na kopiji ni jedan alat ne nalazi nikakav podatak, posebno ne one koji ukazuju na to da je sadržaj zaključan, treba pokušati sa alatima za povraćaj.

Najpoznatiji alat među forenzičarima i može se naći na skoro svakoj forenzičkoj distribuciji jeste TestDisk, a u poslednjim se nailazi i na alat *Recuva*, koji je svoju popularnost stekao još ranije među običnim korisnicima.

23.3.4 Test Disk

Namena programa TestDisk, čiji je autor Christophe Grenier, kako mu ime kaže prvenstveno nije povraćaj podataka, već testiranje rada svih vrsta čvrstih memorija. Ipak, alat se smatra najmoćnijim za povraćaj podataka, posebno sa prenosivih memorija, ali i za rad sa njim potrebno je veliko znanje, poput toga kakav je fajl sistem memorije koja se testira tj. iz koje treba povratiti podatke. Program radi pod svim poznatim operativnim sistemima, a interfejs je u komandnom modu.

Njegova važnost za prenosive memorije je velika u tome što je razvijen, nakon uspeha programa za povraćaj podataka sa memorijskih kartica fotoaparata. Međutim kako je programski kod programa otvorenog tipa, ostale kompanije iskoristile su algoritam za pristup memoriji i od njega razvile programe sa razvijenim grafičkim interfejsom, daleko primamljiviji korisnicima. Osim rada u komandnom modu od korisnici nisu bili zadovoljni time što ranije verzije nisu mogle da povrate imena fajlova.

Pri našem eksperimentu najnovija verzija programa povratila je većinu datoteka ispravno, ali sama struktura nije mogla da se razazna, jer su imena direktorijuma označena brojevima. Povratak podataka od trajao je kraće nego u bilo kom drugom programu, koji smo isprobali, te je najduži proces upravo bio podešavanje programa. Velika prednost za forenzičare jeste i veličina programa koja iznosi svega 1.44MB (prilagođena veličini floppy diska), a program poseduje ugrađen sistem za izveštavanje.

```
TestDisk 6.11.3, Data Recovery Utility, May 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdb - 1031 MB / 984 MiB - USB FLASH DRIVE

Please select the partition table type, press Enter when done.
[Intel] Intel/PC partition
[EFI GPT] EFI GPT partition map (Mac i386, some x86_64...)
[Mac] Apple partition map
[None] Non partitioned media
[Sun] Sun Solaris partition
[XBox] XBox partition
[Return] Return to disk selection

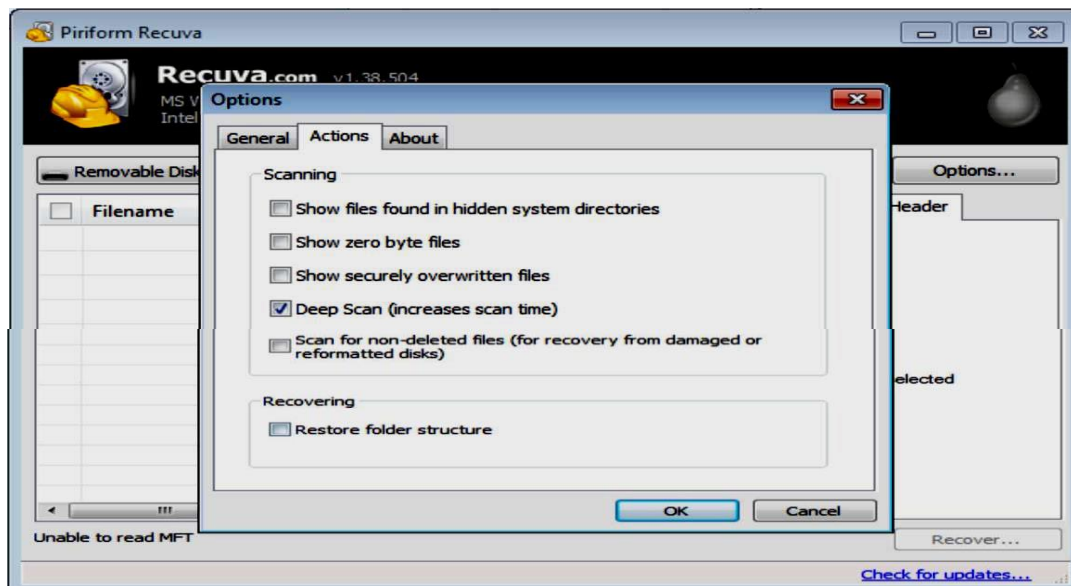
Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a drive to be 'Non-partitioned'.
```

Slika 52: Interfejs programa TestDisk

23.3.5 Recuva

Recuva je najpoznatiji program za povraćaj podataka sa prenosivih memorija. Ipak do skora ga nije bilo na forenzičkim distribucijama, iako su mu rezultati bili odlični. Sam program nije ni namenjen forenzičarima, već običnim korisnicima, na šta pre svega ukazuje njegov grafički interfes. Osim intuitivnog okruženja prednost programa je to što je besplatan.

U našem eksperimentu program je pokazao zavidne rezultate, ali ipak najslabije od svih testiranih alata. Program iz prvog pokušaja nije ni uspeo da povрати podatke, ali su se opcijom DeepScan podaci pojavili, bez strukture fajlova. Ovakvi rezultati produžuju proces analize, jer se na fleš diskovima danas nalazi ogroman broj datoteka. Nepostojanje strukture povraćenih fajlova, autori programa objašnjavaju time da je program uglavnom namenjen memorijskim karticama fotoaparata, gde se uglavnom nalaze samo fotografije.

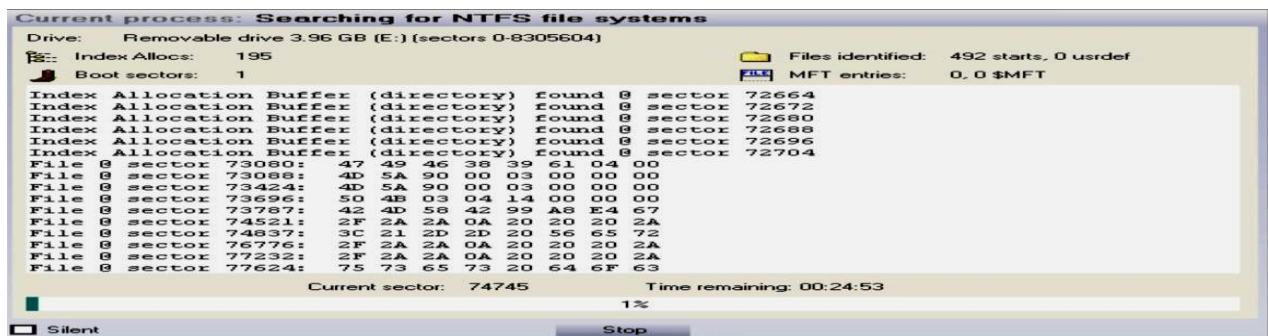


Slika 53: Recuva

23.3.6 Get DataBack

GetDataBack alati među, naprednijim korisnicima računara, koji se ne bave forenzikom, ima najveću popularnost. Program nije namenjen forenzici i poseduje samo dva moda rada – za FAT i NTFS fajl sisteme. Taj nedostatak, kao i činjenica da je alat komercijalnog tipa udaljila ga je od forenzičara.

Eksperiment na našoj memoriji pokazao je odlične rezultate, a jedni problem koji se može pojaviti jeste mod rada programa, jer se treba odlučiti za fajl sistem. Za sve ostalo brine se čarobnjak koji vodi niz proces oporavka podataka. Problem ovog softvera jeste i to što poslednja verzija podržava instalaciju na Windows XP operativnom sistemu, a na novijim ne može da radi ni u compatibility modu, jer poseduje posebne algoritme za pristup memoriji.

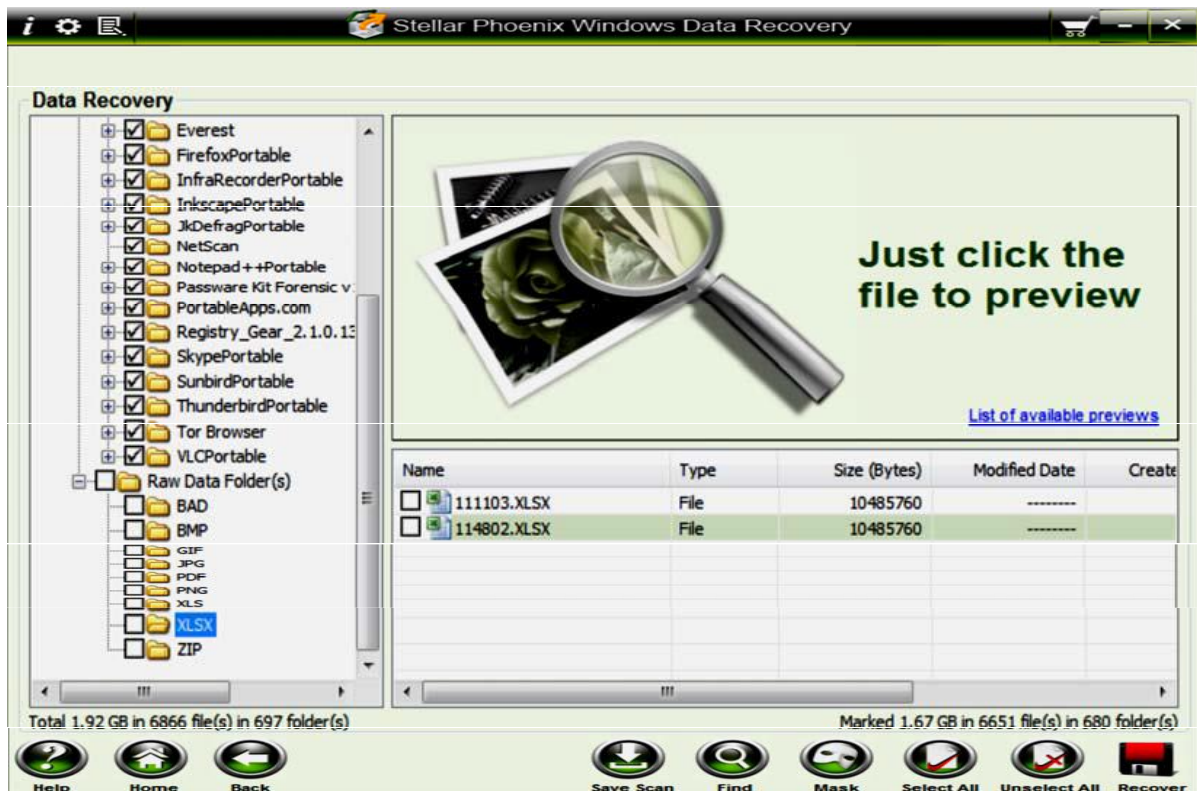


Slika 54: Proces oporavka u programu GetDataBack

23.3.7 Stellar Phoenix Windows Data Recovery

Ne toliko poznat, besplatni softver Stellar Phoenix (slika 50) pokazao se ubedljivo najbolje na našem testu. Ne samo da su svi podaci vraćeni, već je to urađeno u najkraćem roku, a program je napravio i odličan log fajl. Ipak možda i najveća prednost jeste to što je pre nego što je krenuo oporavak podataka, program napravio image fajl fizičke memorije i tako ostavio mogućnost da se kasnije radi bez direktnog „napada“ na memoriju.

Tokom eksperimenta isprobali smo mnoge alate, koji su se različito pokazali, ali osim opisanih podatke su vratili jedino EASEUS Data Recovery Professional, koji takođe ima mogućnost pravljenja forenzičke kopije i povratka sa nje (slika 51), Data Doctor Recovery Pen Drive i Handy Recovery.



Slika 55: Stellar Phoenix Windows Data Recovery

24. Zaključak

Da bi se sprečile prevare forenzičari koriste razne vrste forenzičkih alata poštujući zakone, jer ako se zakoni ne poštuju ni dokazi pred sudom neće biti validni. Moraju da se formiraju institucije koje bi se bavile samo ovom vrstom kriminala. Često da bi se doslo do sto tačnijih i verodostojnih dokaza istražni organi svoje dokaze spajaju sa dokazima do kojih su dosli forenzičari. Međutim kada je reč o računarskim kriminalnim delima mora se imati u vidu da "digitalni dokazi" često nisu jednaki ostalim oblicima fizičkih dokaza u odnosu na koje su osetljiviji i podložni menjaju strukture i sadržaja, te se prema njima treba posebno odnositi. Dokazi mogu potvrditi ili oboriti hipotezu pred sudom pa je njihov integritet ključna stvar u njihovom prihvatanju odnosno odbacivanju pred sudom.

Kroz ovaj rad potvrđena je opšta i posebna hipoteza postavljena na samom početku rada u metodologiji naučnog istraživanja. Cilj eksperimentalnog istraživanja je prikaz gde i kako naći digitalne dokaze koji potvrđuju kompjuterski kriminal koji se može realno dogoditi u kompaniji. Kao rezultat i zaključak eksperimentalnog istraživanja predložena je sigurnosna politika koja definiše digitalnu forenzičku istragu kompjuterskog kriminala i rešavanje sigurnosnih incidenata, skupom pravila, koja omogućavaju i olakšavaju oporavak sistema posle incidenta i time smanjuju uticaj i sprečavaju ponavljanje kompjuterskog incidenta. Kompjuterska forenzika je mnogo šira od samog pružanja izvora potencijalnih dokaza. Ozbiljna korporacijska ustanova treba da uspostavi tim za upravljanje kompjuterskim incidentom i planira obuku, zajedno sa sigurnosnom politikom i procedurama za forenzičku istragu.

Postupci i metodi koji su sprovedeni tokom eksperimentalnog istraživanja sublimirani su u Pravilniku za digitalnu forenzičku istragu kompjuterskog kriminala, a u Pravilniku o rešavanju kompjuterskih incidenata date su smernice za zaposlene u korporaciji.

Preventivne i reaktivne mere zaštite nisu više dovoljne održavanje računarskih sistema i mreža na prihvatljivom nivou rizika. Potrebno je pronaći način da se maliciozni napadi proaktivno spreče, uspešni napadi identifikuju, a posledice i uzroci trajno otklone, kao i da se identifikuje, uhvati i procesira kompjuterski kriminal koji je izvršio napad, što je ključno pitanje kompjuterske forenzike.

Za istragu kompjuterskog kriminala razvijeni su brojni hardverski i softverski forenzički alati. Iako se neki podaci mogu dobiti putem Interneta i telefonskih provajdera servisa, do suštinskih podataka može doći samo korišćenjem forenzičkih alata za pronalaženje i analizu podataka iz „osumnjičenog/korumpiranog” računara i računarskih mreža. Brojni alati za digitalnu forenzičku istragu razvijeni su za akviziciju, analizu ili najčešće obe funkcije.

Za sva-ki slučaj istrage kompjuterskog kriminala potrebno je proceniti koji forenzički alat daje najbolje rezultate. Najvredniji i najko-risniji su uglavnom oni alati koji su multi-funkcionalni, fleksibilni i prikladni za up-otrebu u više različitih scenarija. Alat sampo sebi ne garantuje uspešne rezultate is-trage u kompjuterskoj forenzici, što izazivamnog problema, pa je od ključne važnost stručnost i znanje forenzičara koji se ala-tom koristi. Forenzičar mora dobro pozna- vati operativni sistem koji istražuje (Win-dows, MacOS, Unix, Linux) i fajl-sistem koji se koristi (npr. FAT, NTFS itd.). U tom smislu otvoren je problem odabira alata, njegove funkcije i lica koje će se njime ko-ristiti.

Za svaki pojedinačni slučaj istrage treba odabrati adekvatan alat. Iako treba poštovati generalnu preporuku da digitalne dokaze od trenutka otkrivanja zaključujući sa forenzičkom analizom, treba uvek tretirati kao da će biti prezentovani na sudu, prilikom izbora alata drugačije se rangiraju prioriteta. U slučajevima kada se digitalna forenzika ne radi sa svrhom prezentovanja dokaza u sudskom procesu forenzičar ima veću slobodu izbora i bira alat sa kojim ima najviše iskustva i koji ima najveći faktor upotrebljivosti za konkretan slučaj. Izbor adekvatnog alata ukoliko se rezultati trebaju prezentovati u sudskom procesu može biti zahtevniji posao. S obzirom da izabrani alat mora biti sertifikovan i priznat od strane državnih organa to povlači za sobom da se forenzičar odlučuje za alate koje mora, ne nužno za one koje smatra najboljim.

Integrisani model istrage fizičke i digitalne istrage daje nam tačan pogled na proces digitalne forenzičke istrage i razlike između prikupljanja digitalnih dokaza i digitalne forenzičke analize. Fizička digitalna forenzička analiza odgovara na komparativna pitanja tipa: "Da li su X i Y slični", ili identifikaciona pitanja tipa: "Da li možeš identifikovati X". Postupci koji su potpali pod kategoriju digitalne forenzičke analize širi su i uključuju rekonstrukciju događaja (incidenta). Zbog toga izraz digitalna forenzička analiza mnogo je precizniji (tačniji), iz perspektive ljudi koji analiziraju sistem. Iz perspektive istražnog organa i fizičke scene zločina, koji šalje kompjuter u laboratoriju radi analize, između ostalog, ovaj proces će se verovatno uvek smatrati digitalnom forenzičkom analizom.

Ovaj model takođe prikazuje obim napora koje treba da učiniti da bi se ispravno istražio digitalni incident. Mnogi zvanični organi istrage imaju samo jedno lice koje analizira svaki deo kompjutera. Ovo je analogno slanju jednog zvaničnog organa istrage na fizičku scenu zločina, očekujući da će naći sve vrste dokaza i odraditi tip slučaja. Potrebni su adekvatni resursi (forenzički alati) da bi se kvalitetno istražio digitalni incident.

Kada se sadašnje tehnologije pregledaju prema ovim fazama, vidi se da postojeći digitalni forenzički alati za analizu dozvoljavaju korisniku da vidi digitalnu scenu zločina i prikupi digitalne dokaze iz nje. Forenzički alati se koriste u fazama digitalnog pregleda i pretrage za prikupljanje dokaza. Analize veza i alati za konsolidaciju vremenskih linija događaja pomažu istražnom organu u fazi digitalne rekonstrukcije. Zato, sa ovim modelom mnogi postojeći alati za digitalnu forenzičku analizu mogu se nazvati alati za forenzičku akviziciju (prikupljanje) digitalnih dokaza. Alati za prikupljanje digitalnih dokaza prevode digitalne podatke na neki nivo apstrakcije koji pomaže istražnom organu. Ovi alati koriste inženjerske tehnike, a ne stroge naučne, da bi predstavile podatke istražnom organu.

Vode se debate da li su dokazi skupljeni sa kompromitovanog kompjutera uživo pouzdani. Koristeći ovaj model, za prikupljanje dokaza sa kompromitovanog kompjutera uživo, nije ništa drugačije od skupljanja fizičkih dokaza. Fizička scena zločina se modifikuje kada istražni organ šeta okolo, kao što se digitalna scena zločina modifikuje, kada forenzički istražni organ pokrene softver za prikupljanje digitalnih dokaza. Izazov je da se smanje izmene, razume efekat izmena digitalnih podataka i minimizuje poverenje u operativni sistem u slučaju prikupljanja digitalnih podataka sa sistema uživo.

Ovaj model jasno pokazuje interakciju između fizičkog i digitalnog domena. Mnoge procedure fokusiraju se uglavnom na digitalne dokaze i uključuju osnovne fizičke dokaze kao što su slike spoljašnje strane sistema. Model se sastoji od jednakog broja faza fizičke scene zločina i digitalne scene zločina. Motiv i mogućnost za ovo leži u tome što je krajnji cilj bilo koje digitalne istrage da se povežu digitalne aktivnosti sa čovekom. Zato će fizički dokazi biti potrebni i treba da se uzmu u obzir u toku istrage svakog kompjuterskog incidenta. Digitalna scena zločina može da se smatra sekundarnom scenom zločina fizičke scene zločina.

Fizička scena zločina vrlo je jasna i razumljiva za zvaničnu istragu. Uobičajeno fizička scena zločina manje je razumljiva za digitalnu istragu koje vodi korporacijski istražni organ. Moguće je da preostali fizički dokazi budu izgubljeni, ukoliko ih interventni tim nije otkrio.

Ovaj model pokazuje da se poteškoće sa kojima se digitalni istražni organi susreću slični onima sa kojima se susreću organi fizičke istrage. Faza pregleda i pretrage u oba slučaja moraju da identifikuju korisne delove dokaza. Istražni organ fizičkog kriminala ne može da pošalje svaki fizički objekat u laboratoriju na analizu. Mora da koristi svoje iskustvo da identifikuje šta je uobičajeno (normalno), a šta ne. Organ digitalne istrage ne može da pošalje svaku datoteku sa sistem da bude pregledana i ispitana. Oba organa istrage susreću se sa poteškoćom pronalaženja sitnih delića dokaza, kao što su dlaka na tepihu ili izbrisane datoteke u 100 GB-nom sistemu.

Razdvajanjem procesa analize u fazu pregleda i fazu pretrage, lakše se dokumentuje, shvata i uči proces. Uobičajeni problem za neiskusnog digitalnog istražnog organa digitalnih dokaza je to što ne zna kako da počne Fazu Ispitivanja koju drugi modeli opisuju. Fizički model istrage razdvajanjem Faze Ispitivanja u dve faze čini proces više intuitivnim. Obično digitalna istraga započinje pronalaženjem očiglednih brzih rezultata, (isključivanje nemogućih i nelogičnih), a onda se na njima dalje širi.

Mislim da bi se ovaj model trebao koristiti u praksi jer je sveobuhvatniji u odnosu na druge modele.

ILook kao alata za digitalnu forenzičku istragu kompromitovanih računara se pokazao u praksi kao jedan od najboljih alata sa velikim brojem funkcija koje su od neprocenjivog značaja u digitalnoj forenzičkoj istrazi. Alati kao što su Encase, FTK AccessData, Xway-s forensic, imaju takođe izuzetne karakteristike, ali nisu u upotrebi toliko dugo kao ILook.

Mala je razlika između svih ovih alata, neki imaju neke funkcije koji drugi nemaju ali važi i obratno. Recimo Xways u odnosu na ove druge alate ima jednu veoma zanimljivu funkciju koja je sve popularnija u digitalnoj forenzičkoj istrazi, a to je prikupljanje dokaza sa kompromitovanih uređaja uživo pre gašenja samih uređaja. Ovo je veoma bitna funkcija koji ovi drugi alati nemaju. Prikupljanjem dokaza pre gašenja uređaja može se napraviti slika memorije koja je na današnjim uređajima sve veća. U memoriji se mogu nalaziti razni podaci kao i šifre za pristup određenim podacima koje će se automatski izgubiti pri gašenju računara. Međutim Xways nema funkcije automatizacije određenih procesa istrage koje u mnogome štede resurse.

Što se tiče alata za digitalnu forenzičku istragu, ozbiljan istražitelj bi morao da zna da koristi više različitih alata, u zavisnosti od slučaja do slučaja, a takođe bi morao da isproba rad skoro svakog ozbiljnijeg alata kako bi znao koje su im prednosti a koje mane. Jer u zavisnosti od slučaja do slučaja moraju se birati alati koji najviše pogoduju datom slučaju radi što temeljnije početene akvizicije potencijalnog dokaznog materijala. Što se tiče digitalne forenzičke istrage i pojedinog slučaja, mišljenja sam da se dokazi koji su prikupljeni, i pretraženi u istrazi trebaju proveriti na dva različita alata u svakoj fazi istrage i u svakoj oblasti u zavisnosti od uređaja (pojedinačni kompjuter, telefoni, pda, mrežni uređaji, mreža, serveri...s).

Neki alati za digitalnu forenzičku istragu ne poseduju opciju za pregledanje sadržaja Thumbs.db fajlova, zbog toga je kao praktičan deo master rada urađena aplikacija Thumbanil pretraživač za akviziciju, pretragu i izveštavanje dokaza koji su nastali na kompromitovanim uređajima a nalaze se u Thumbs.db fajlovima.

Thumbanil pretraživač je alatka koja može da se koristi u korelaciji sa alatima za digitalnu forenzičku istragu koji nemaju opciju čitanja sadržaja Thumbs.db fajlova a može se koristiti i kao alat sam za sebe, jer ima ugrađene mehanizme pretrage svih uređaja (HDD,CD,USB..) na kompjuteru. Alat je maksimalno automatizovan i komforan za rad. Postoje i drugi alati koji pretražuju Thumbs.db fajlove, neki su komercijalni (20-40\$), a neki besplatni. Ovaj alat je napravljen kao deo šireg projekta poboljšanja funkcionalnosti raspoloživih forenzičkih alata.

TeamViewer je kompanija koja je za kratko vreme uspjela da ostvari veliki uspjeh na polju pružanja internet podrške, a sertifikat ISO 9001, koji se izdaje na godišnjem nivou, pečat kvaliteta sa pet zvezdica izdat od strane Njemačkog udruženja FAIER (Federal Association of IT Experts and Reviewers), potvrda od FIDUCIA (operater centara za informacionu obradu 800 njemačkih banaka) za upotrebu na bankarskim radnim stanicama itd. predstavljaju čvrstu garanciju bezbednosti i kvaliteta.

Nema sumnje da je TeamViewer sjajan program koji zaslužuje sve pohvale, jedina zamerka je jako visoka cijena komercijalne verzije (za naš standard) od € 499 za Business verziju, preko € 998 za Premium verziju do € 1890 (i to sa popustom) za Corporate verziju.

Elektronsko poslovanje se naglo razvija i danas je u širokoj upotrebi, kako javnosti tako i mnogih kompanija. Ono pruža bezbroj pogodnosti kao što su brzina, veća i kvalitetnija informiranost o proizvodima, dostupnost svima i bezbroj drugih prednosti.

Elektronsko poslovanje, koje se predstavlja kao najperspektivniji oblik poslovanja u budućnosti, ima kao i sve ostalo neke propuste, među kojima je prvo informacijska sigurnost. Problemi se javljaju zbog brzog razvoja takvog načina poslovanja te se nemogu provjeriti svi sigurnosni aspekti njihove primjene. Sve češća je pojava informatičkog kriminala koji se služi informacijskom tehnologijom kao sredstvom napada.

Postoje razne vrste kriminalnih aktivnosti koje su mogu svrstati u četiri osnovne skupine:

Napadi na resurse kompanije - to je neovlašćeno pristupanje informaciskim reursima kmpanije , tj. njenom hardveru i softveru da bi ostvario neku korist na koju nema pravo ili prouzrokovao neku štetu u kompaniji.

Napadi na privatnost i krađe identiteta - to je lažno predstavljanje, neovlašćeno čitanje ili kopiranje tuđih podataka pomoću kojih se može ostvariti neka nepripadajuća korist, uzrokovanje štete u komaniji ili ugrožavanje privatnosti identiteta čiji je otuđio.

Ugrožavanje identiteta podataka - do ovih problema dolazi kad informacije koje kompanija koristi i poruke koje dostavlja nekom drugom gube na pouzdanosti i vrednosti i zbog toga postaju beskorisni.

Ometanje normalnog rada i poslovanja - to je problem u kojem dolazi do smanjenja kvalitete usluge koju bi tvrtka trebala pružiti klijentima, jer nemože obavljati posao na normalan kvalitetan način. Glavni primjer toga je "zasipanje" poslužiteljskog računara (servera) te kompanije sa puno beskorisnih poruka koje uzrokuju njegov slom, pa on nije u mogućnosti obavljanja svoje primarnih zadataka.

25.Literatura

1. Ćurčić B., Dražić R., "Pirati na mreži: kultura elektronskog kriminala", Daniel Print, Novi Sad, 2008
2. Gojko Drubor, tema 16: Osnove kompjuterskog kriminala ,Univerzitet Singidunum
3. Milosavljević Milan, Grubor Gojko, Digitalna forenzika računarskog Sistema, Univerzitet Singidunum,Bgd 2009
4. Milosavljević Milan, Grubor Gojko, Istraga kompijuterskog kriminala, Univerzitet Singidunum,Bgd 2009
5. Mr Miodrag Đorđević, dipl. inž. Ministarstvo odbrane SCG,Resursi za istragu kompijuterskog sadržaja skripta
6. Petkovic Aleksandar, Forenzička revizija.Novi Sad 2010
7. Pleskonjic D. Maček N. Đorđević B. Carić M. Sigurnost računarskih sistema i mreža- Mikro knjiga
8. Radmila Živković, Ponašanje potrošača, Univeritet Singidunum,Bgd 2013, 2009
9. Srdjan Atanasijević , Bezbednost informacionih sistema.,Visoka tehnička škola Kragujevac 2009
10. Srdjan Atanasijević , Digitalna forenzika, Visoka tehnička škola Kragujevac 2009
11. Stuart McClure, Joel Scambray, George Kurtz Hakerske tajne ,Mikro knjiga – prevod petog izdanja
12. Uglješa Georgijević,Integrisani model procesa digitalne forenzičke istrage,skripta
13. Varga M., Ćurko K., Panian Z., Cerić V., Bosilj Vukuši V., Srića V., Požgaj Z., Strugar I., Spremić M., Pejić Bach M., Vlahović N., Jaković B., Informatika u poslovanju, Senat Sveučilišta u Zagrebu, Zagreb, 2007.
14. Zona Kostić, Gojko Grubor, Alati za digitalnu forenzičku istragu, Digital forensics tools,2008 godina
15. Zoran Petrović, Računovodstvena regulative, Univerzitet Singidunum, Bgd 2009

Internet članci

1. http://www.itvestak.org.rs/ziteh_10/zbornik_radova/Zornic%20Dzemail%20-%20%20Racunarski%20kriminal.pdf
2. http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-17.pdf
3. http://www.prafak.ni.ac.rs/files/nast_mat/Kompjuterski_kriminal.pdf
4. http://sr.wikipedia.org/wiki/Kompjuterski_kriminalitet
5. http://www.itvestak.org.rs/ZITEH_12/radovi-12/Forenzicki%20alati%20%20Katarina%20Djordjevic.pdf

6. <http://www.scribd.com/doc/77698542/Alati-za-digitalnu-forenzi%C4%8Dku-istragu>
7. http://www.itvestak.org.rs/ziteh_10/zbornik_radova/Nikacevic%20Vladan%20-%20Korporacijska%20istraga%20kompjuterskog%20kriminala.pdf
8. http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-06.pdf
9. http://en.wikipedia.org/wiki/Digital_forensics
10. http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-19.pdf
11. http://www.itvestak.org.rs/ziteh_06/Radovi/ZITEH%2006-R07.pdf
12. http://www.teamviewer.com/download/teamviewer_manual.pdf
13. <http://www.teamviewer.com/en/company/references.aspx>
14. <http://www.teamviewer.com/en/licensing/index.aspx>
15. <http://www.teamviewer.com/en/products/benefits.aspx>