



Univerzitet
Singidunum

Fakultet za informatiku i menadžment
SAVREMENE INFORMACIONE TEHNOLOGIJE

MASTER RAD

ISTRAŽNE METODOLOGIJE, TEHNIKE I ALATI ZA DIGITALNU FORENZIČKU ISTRAGU

MENTOR:

Docent dr. Gojko Grubor

KANDIDAT:

Georgijević Uglješa
M9461/08

Beograd, decembar 2010

Abstract

This paper describes the various methodologies, technologies and techniques of computer crime investigations. It also explains the basic relationship between various aspects of computer crime and crime as we had been known until now.

The paper presents the types and distribution tools for digital forensic investigation, and describes the detailed instructions for using one of these tools in practice. The tool described in this paper is ILook Investigator, who is the official tool for investigating computer crime in the United States (FBI, IRS).

Another part of the master thesis is tool for digital forensics "ThumbnailViewer", who is also a practical part of master thesis. Tool that is made can be used in the investigation independently and can be used as an auxiliary tool to existing tools. It was made in Microsoft Visual Studio 2008 (C#).

Key words:

case - slučaj
digital forensic - digitalna forenzika
cyber crime – visoko tehnološki kriminal

Apstrakt:

U ovom radu su opisane razne metodologije, tehnologije i tehnike istrage kompjuterskog kriminala. Takođe su objašnjene osnovne veze između raznih aspekata kompjuterskog kriminala sa kriminalom kakav nam je bio poznat do sada. Rad sadrži i zaključke o prikazanim metodologijama, tehnologijama, i tehnikama kao i preporukama za korišćenje istih.

Predstavljene su vrste i podela alata za digitalnu forenzičku istragu, i opisana su detaljna uputstva za korišćenje jednog od tih alata u praksi. Alat koji je opisan u ovom radu je ILOOK Investigator koji je oficijelni alat za istragu kompjuterskog kriminala u Sjedinjenim Američkim državama (koriste ga FBI, IRS...).

Za praktični deo master rada napravljen je alat za digitalnu forenzičku istragu "Thumbnail pretraživač". Alat koji je napravljen ovom prilikom može se koristiti u istrazi nezavisno od drugih alata a takođe može da se koristi i kao pomoćni alat već postojećim alatima za digitalnu forenzičku istragu. Napravljen je u Microsoft Visual Studio 2008 (C#).

SADRŽAJ

1. METODOLOGIJA ISTRAŽIVAČKOG RADA	5
1.1. Uvodne napomene i obrazloženje rada	5
1.2. Predmet istraživanja	5
1.3. Cilj i zadaci istraživanja	5
1.4. Hipotetički okvir	6
1.5. Metode istraživanja i tok istraživačkog procesa	6
2. METODI I TEHNIKE DIGITALNE FORENZIČKE ISTRAGE	7
2.1. Istorijat	7
2.2. Evolucija istražnih alata	8
2.3. Digitalna forenzička istraga	10
2.4. ULOGA DIGITALNIH DOKAZA	13
2.5. ULOGA KOMPJUTERA U ZLOČINU	15
2.5.1. Hardver kao proizvod kriminalne aktivnosti (Hardware as Contraband or Fruits of Crime)	15
2.5.2. Hardver kao instrument(oruđe) zločina (Hardware as an Instrumentality)	16
2.5.3. Hardver kao dokaz (Hardware as Evidence)	16
2.5.4. Informacija kao proizvod kriminalne aktivnosti (Information as Contraband or Fruits of Crime)	16
2.5.5. Informacija kao instrument(oruđe) zločina (Information as an Instrumentality)	17
2.5.6. Informacija kao dokaz (Information as Evidence)	17
2.6. ISTRAŽNE METODOLOGIJE	18
2.7. ISTRAŽNA METODOLOGIJA Prema Eoghan Casey-u	19
2.7.1. Optužbe ili uzbuna incidentom (Accusation or Incident Alert)	20
2.7.2. Procena vrednosti (Assessment of Worth)	21
2.7.3. Protokoli Incidenta/Mesta zločina (Incident/Crime Scene Protocols)	21
2.7.4. Identifikacija ili zaplena (Identification or Seizure)	22
2.7.5. Čuvanje (Preservation)	24
2.7.6. Oporavak podataka (Recovery)	24
2.7.7. Žetva (Harvesting)	24
2.7.8. Redukcija (Reduction)	25
2.7.9. Organizacija i pretraga (Organization and Search)	25
2.7.10. Analiza (Analysis)	26
2.7.11. Izveštavanje (Reporting)	26
2.7.12. Ubeđivanje i svedočenje (Persuasion and Testimony)	27
2.8. ISTRAŽNA METODOLOGIJA Prema Brian Carreir-u	27
2.8.1. Korporacijski Model Istrage	28
2.8.2. Zvanični model istrage	29
2.9. Model istrage fizičke scene zločina	30
2.10. Integrisani model procesa digitalne forenzičke istrage	31
2.10.1. Faza pripreme	33
2.10.2. Faza razvoja	33
2.10.3. Faza istrage fizičke scene zločina	34
.....	34
Faza istrage fizičke scene zločina	34
2.10.4. Faza istrage digitalne scene zločina	36
2.10.5. Faza provere (kontrole)	39

3. ŽIVOTNI CIKLUS ANALIZE I PRETRAGE DOKAZA.....	41
4. VRSTA FORENZIČKIH ALATA ZA DIGITALNU FORENZIČKU ISTRAGU.....	43
5. ILOOK.....	45
5.1. Izgled ILook ekrana.....	47
5.2. Prozor dokaza (Evidence Window).....	48
5.3. Prozor fajlova: (FileWindow)	50
5.4. Prozor Informacija (InfoWindow).....	51
5.5. Pregled diska	52
5.6. Pregled Fajla (File View).....	55
5.7. Funkcije pregleda sadržaja.....	58
5.8. Dnevnik (Log)	63
5.9. Korišćenje skripti u Ilook-u za automatizaciju, izveštavanje i procesiranje podataka.....	66
5.10. Pregled Infrastrukture Ilook-a	69
5.11. Preporuka u korišćenju ILook tokom istraga.....	71
5.12. Pretraga fajlova.....	76
5.13. Pronalazak fajlova koji su kreirani, modifikovani na određeni datum ili između nekog perioda i statistička vremenska linija sa podacima o promeni fajl sistema tokom njegovog životnog veka.....	76
5.14. Dnevnik Fajl sistema (statistička vremenska linija sa podacima o promeni fajl sistematom tokom njegovog životnog veka)	78
5.15. Pronalazak fajlova po potpisu fajla ili obeležavanje fajlova čija ekstenzija ne odgovara potpisu tih fajlova.....	80
5.16. Funkcije oporavka i pretraživanja ostataka fajlova i samih fajlova	83
5.17. Pronalaženje stvari uz pomoć pretraživača koji su sastavni deo ILook-a.....	86
5.18. Korišćenje funkcija obeležavanja da bi se napravio set dokaznog materijala (“tagging”)	89
6. Windows Thumbnail cache.....	92
6.1. Thumbs.db.....	93
7. Thumbnail pretraživač	93
7.1. Početni ekran	94
7.2. Funkcije Thumbnail pretraživača	98
7.2.1. Pretraga.....	98
7.2.2. Funkcije promena.....	103
7.2.3. Funkcija Kreiraj izveštaj	104
8. Zaključak	107
9. Literatura	110

1. METODOLOGIJA ISTRAŽIVAČKOG RADA

1.1. Uvodne napomene i obrazloženje rada

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

Pored teoretskog dela rada, kao prekičan deo rada napravljen je jedan alat za digitalnu forenzičku analizu Thumbnail pretraživač. Alat se koristi kao sredstvo za pretragu kompjutera, tj. Thumbs.db fajlova na kompjuteru i pregledanje istih kao i pravljenje forenzičkih izveštaja na osnovu tih pregleda.

Za pisanje ovog rada iskorišćena je literatura stranih vrhunskih stručnjaka koji se ovim poslovima bave dugi niz godina.

1.2. Predmet istraživanja

Predmet istraživanja je veza visoko tehnološkog kriminala sa tradicionalnim kriminalom, kao i nove tehnike, tehnologije i metodologije istrage visoko tehnološkog kriminala.

1.3. Cilj i zadaci istraživanja

Kao što su i informacione tehnologije stvar koja je relativno novijeg datuma tako i kriminalne radnje u svetu visoko tehnološkog kriminala i istraga tih kriminalnih radnji je jedna od novosti sa kojima se susrećemo u današnjem svetu. Cilj ovog rada je da nam objasni i približi istragu kompjuterskog kriminala sa tradicionalnom istragom kriminala i da nam objasni vezu između ta dva „sveta“ koja se prožimaju i prepliću kao i stvarni svet sa virtuelnom realnošću. Još jedan od ciljeva ovog rada je da se novim, istražiteljima i naučnicima koji se bave ovom problematikom približe i predstave nove metodologije, tehnologije i tehnike istrage kao jedno od rešenja koja se mogu praktikovati i kojima se

može rukovoditi na terenu i u praksi, kao i da se novi korisnici upute u mogućnosti digitalne forenzike kao primenjene nauke, tako da znaju da postoje mehanizmi koji nam pružaju neku vrstu sigurnosti da počinioci visoko tehnološkog kriminala ipak nisu nedostižni i da iza njihovih kriminalnih radnji ipak ostaju ili digitalni ili fizički ili i jedni i drugi dokazi, koji se mogu dovesti u vezu sa njima.

1.4.Hipotetički okvir

Opšta hipoteza: Nove računarske tehnologije i softveri koji se razvijaju iz dana u dan su podložne raznim napadima i kriminalnim aktivnostima. Digitalna forenzika kao nauka je jedna od novijih nauka pa je još nedovoljno istražena. Svakim danom tehnologije sve više i više napreduju a samim tim moraju da se menjaju i metodologije, tehnike i tehnologije koje služe za istragu kompjuterskog kriminala.

Posebna hipoteza: Praćenjem razvoja novih informacionih tehnologija, operativnih sistema, softvera, novih metodologija istrage kompjuterskog kriminala, tehnika i tehnologija koje služe u istragama možemo obeshrabriti i smanjiti broj novih počinioca visoko tehnološkog kriminala, a i povećati broj rešenih slučajeva istog.

1.5.Metode istraživanja i tok istraživačkog procesa

1. Prikupljanje literature koja se tiče istorijata visoko tehnološkog kriminala, teoretskog dela literature o digitalnoj forenzici, raznih metodologija istrage kompjuterskog kriminala.
2. Sortiranje i iščitavanje iste da bi se izdvojile najsveobuhvatnije i najpraktičnije metodologije, tehnologije i tehnike istrage kompjuterskog kriminala.
3. Pretraga interneta za raznim alatima koji se koriste u digitalnoj forenzici. Isprobavanje mogućnosti alata (svakog pojedinačno).
4. Primenjivanje izabranih metodologija nad virtuelnim slučajevima u sprezi sa raznim setovima alata radi provere funkcionisanja izabranih metodologija i tehnika istrage u praksi.
5. Pravljenje programa za digitalnu forenzičku istragu
6. Izlaganje sopstvenog mišljenja i preporuka.

2. METODI I TEHNIKE DIGITALNE FORENZIČKE ISTRAGE

2.1. Istorijat

Kao odgovor na rast kompjuterskog kriminala, u kasnim osamdesetim i ranim devedesetim godinama agencije reda i zakona u Sjedinjenim Američkim Državama počele su da rade zajedno na razvoju treninga i izgradnji kapaciteta da bi rešile ovaj problem. Ova inicijativa je dovela programa treninga za agencije zakona i reda u centrima ka što su „SEARCH, Federal Law Enforcement Center (FLETC), and National White Collar Crime Center (NW3C)“.

Ujedno Sjedinjene države i druge države uspostavile su specijalizovane grupe radi istrage kompjuterskog kriminala na nacionalnom nivou. Ipak, zahtevi koji su stizali ovim grupama su ubrzo istrošili njihove resurse i došlo je do razvoja regionalnih centara za procesiranje digitalnih dokaza. Ovi regionalni centri su takođe postali preopterećeni, što je dovelo do razvoja jedinica za rukovanje digitalnim dokazima pri lokalnim agencijama reda i zakona. Ovaj rapidni razvoj je rezultirao u piramidalnoj strukturi, prva lica koja odgovaraju na incident sa osnovnim veštinama kolekcije i pregleda digitalnih dokaza koji rešavaju većinu slučajeva, koji su podržani od strane regionalnih laboratorija radi procesiranja komplikovanijih slučajeva, zatim su nacionalni centri koji pomažu kod najzahtevnijih slučajeva, izvode istraživanja, i razvijaju alate koji mogu da se koriste na regionalnim i lokalnim nivoima.

Sa razvojem tehnologije i kompjuterskog kriminala došlo je i do potrebe za specijalizacijom: tehničari digitalnog mesta zločina 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.

Kada je jedna individua odgovorna za prikupljanje, procesiranje i analiziranje digitalnih dokaza, korisno je da se ovi zadaci izvode posebno. Svaka oblast specijalizacije zahteva različite sposobnosti i procedure. Ukoliko se svaka oblast obrađuje posebno lakše se definišu treninzi i standardi u svakoj oblasti. Working Group for Digital Evidence (SWGDE) je izdala vodiče za trening i najbolje prakse. American Society of Crime Laboratory Directors (ASCLD) je predložila zahteve za ljude koji pregledaju digitalne dokaze u forenzičkim laboratorijama (ASCLD 2003). Postoje slični naponi za razvoj pregleda digitalnih dokaza u akreditovanu disciplinu pod internacionalnim standardima (ISO 17025; ENFSI 2003).

Razvoj ovih standarda je napravio potrebu za standardima prakse za individue na polju. Da bi se odgovorilo na ovu potrebu, razvijeni su programi sertifikacije i treninzi da bi se osiguralo da ljudi koji pregledaju digitalne dokaze imaju osobine potrebne da obavljaju svoj posao kompetentno i da prate proverene procedure. Cilj je da se napravi nekoliko nivoa sertifikacije:

1. Ispit opšteg znanja (koji svi moraju da prođu, uključujući i osoblje koje prvo odgovara na incident koje rukuje digitalnim dokazima)
2. Viši sertifikati za individue koje rukuju u mnogo kompleksnijim slučajevima u laboratorijskim uslovima.

2.2. Evolucija istražnih alata

Na početku istraživanja kompjuterskog kriminala bilo je uobičajeno da digitalni istražitelji koriste kompjuter koji je korišten za zločin radi uzimanja dokaza sa njega. Rizici pri ovom pristupu problemu je što prilikom pregleda kompromitovanog sistem sa njega samog može doći do kontaminiranja dokaza na način koji nije moguće opaziti. Uprkos tome postoje programi na UNIX platformi ka ošto je dd koji postoji još od 1980 i koji 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, 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 Internal Revenue Service (IRS) da bi pomogli istražiteljima da procesiraju podatke na kompjuterskim 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 tcpdump i Ethereal 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 počinu neka fizička kriminalna aktivnost (primer. Ukoliko je osumnjičeni koristio internet da bi vršio istragu o kriminalnom aktu koji je načinio (će nčiniti) ili je korišten za neku digitalnu aktivnost u virtuelnom okruženju koja krši polise (npr. u firmi) ili zakon. (npr. Napadač uspe da neautorizovano pristupi kompjuteru, korisnik “skida” sa interneta zabranjeni materijal, ili kada korisnik pošalje preteći e-mail.). Kada se datektuje prekršaj istraga počinje.

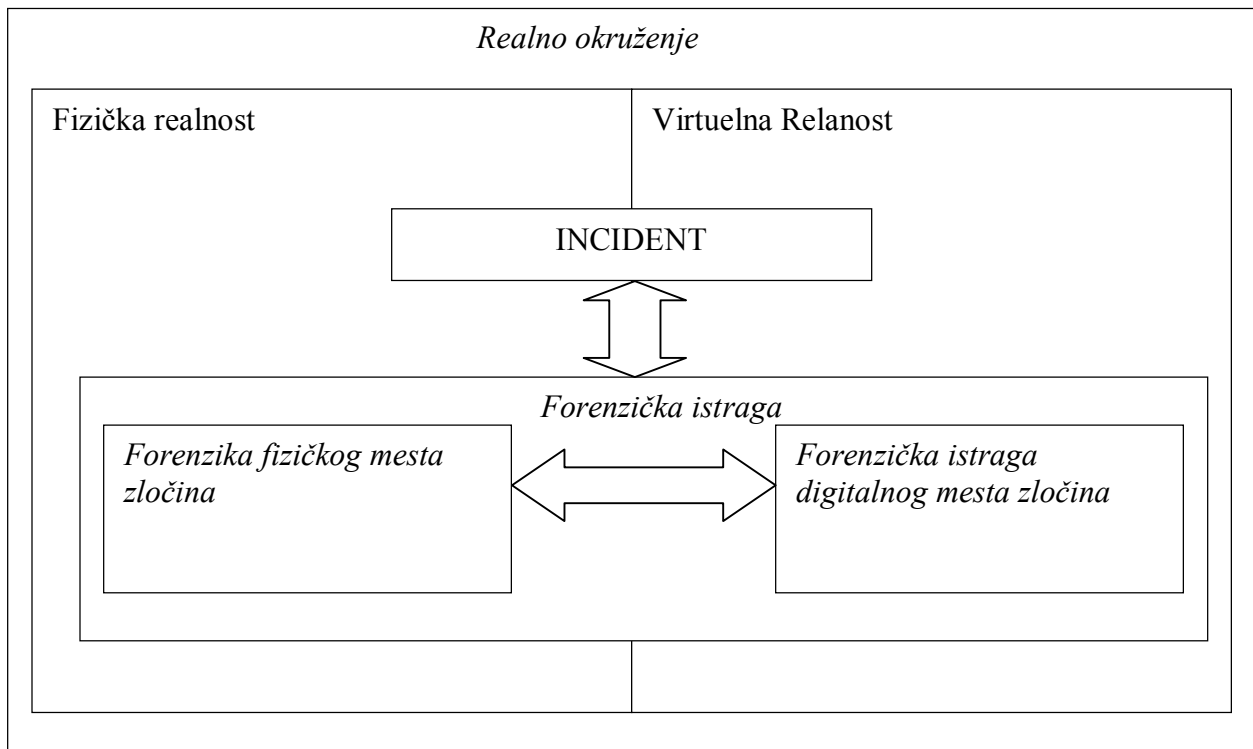
Digitalna istraga je proces gde se razvijaju i testiraju hipoteze koje odgovaraju na pitanja o digitalnim događajima. Ovo se radi koristeći naučne metode gde se razvija hipoteza koristeći dokaze koji su nađeni a zatim se testira hipoteza pretražujući dodatne dokaze koji su u kontradikciji sa hipotezom.

Digitalni dokaz je digitalni objekat koji sadrži pouzdane informacije koje podržavaju hipotezu ili je opovrgavaju.

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.

2.3.Digitalna forenzička istraga

U proteklih par godina sa razvojem digitalne tehnologije kao i interneta (globalne svetske mreže) mesto zločina se seli sve više u virtuelnu realnost. Zašto se seli u virtuelnu realnost? Zato što se pronevere novca kao i razne druge nelegalne radnje mogu lakše izvršiti i to neposredno tj. ne iz prvog lica već preko kompjutera, tj nekog vida mreže(interenta,intraneta). Samim tim pruža težu identifikaciju počinioca. Preko interneta i raznih organizacija koje funkcionišu na internetu tj. u virtuelnooj stvarnosti kao što su kockarnice, E-Gold, MoneyTransfer itd. javlja se mogućnost pranja novca neposredno i vrlo efikasno. Pravne organizacije na svetu imaju sve više slučajeva koji su izvršeni delimično ili celokupno preko interneta ili nekih drugih elektronskih medija. Potrebni su resursi i procedure da bi se efektivno locirali, pretraživali i očuvali svi tipovi elektronskih dokaza. Ovi dokazi variraju od slika dečije pornografije pa do kriptovanih podataka koji se koriste za razne kriminalne aktivnosti. Čak neke istrage koje nisu totalno elektronske prirode u nekim delovima istrage imaju potrebu za analizom digitalnih podataka. Digitalna forenzička istraga je nova diciplina forenzičke istrage koja se bavi upravo otkrivanjem incidenta, konfiskovanjem i akvizicijom, analizom, očuvanjem, i prezentovanjem digitalnih dokaza.



Slika 1. Veze između fizičkog mesta zločina i digitalnog mesta zločina

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 ovaj iako je cilj isti i za istragu fizičkog kriminala. Ovo poglavlje opisuje metodologije, zasnovane na naučnim metodama, da bi pomogli istražiteljima da razotkriju istinu koja služi pravdi. Ova metodologija je dizajnirana da pomogne razvoju alata, standardnih operativnih procedura, i konačno istražnih izveštaja. Ova metodologija je nastala iz iskustava i diskusija u polju. Svaka istraga je jedinstvena pa prema tome ne treba se držati striktno ove metodologije već kao neki početni okvir koji treba da se nadograđuje od slučaja do slučaja.

Istražni proces je deo većeg okvira tj. pravnog okvira (sudstva).

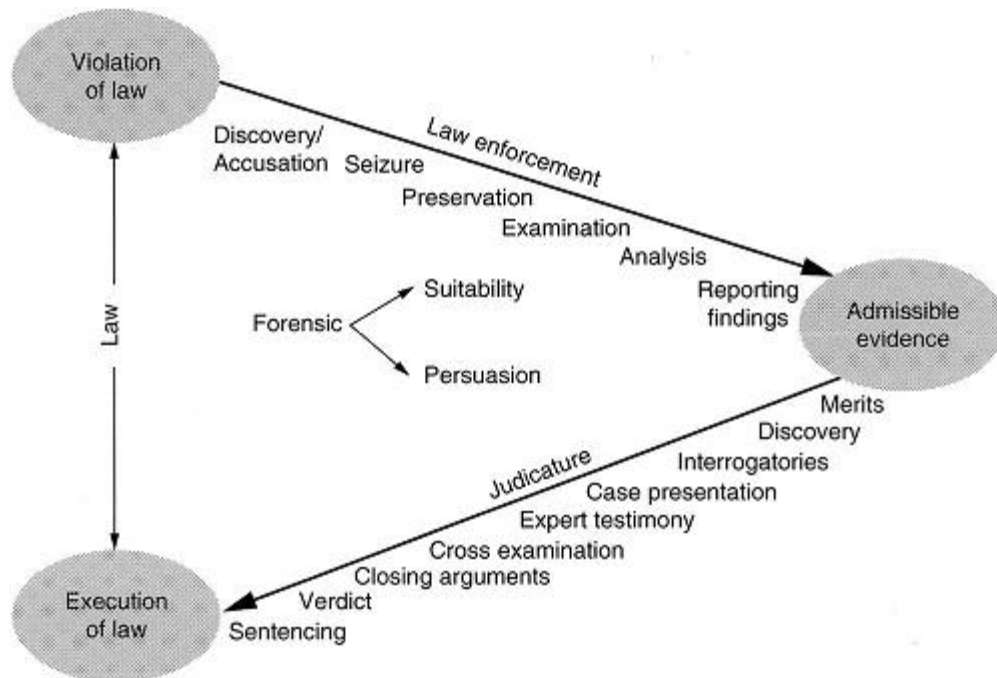


Figura 2: Prikaz procesa rešavanja slučaja [7]

Pojednostavljena metodologija na slici 4.1 je napravljena radi lakšeg sagledavanja mesta aktivnosti njihovih aktivnosti koje utiču na druge potrebne aktivnosti. 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.

Na primer kada log fajlovi ukazuju da je zaposleni zloupotrebio mašinu ali on to uporno poriče, digitalni istražitelj bi trebao detaljno pregledati log fajlove radi znakova koje ukazuju na grešku. Slično, kada velika količina podataka nedostaje sa kompjutera i sumnja se na uljeza, digitalni istražitelji treba da ustanove da li je šteta više povezana sa mogućim greškama na disku ili sa upadom.

Ukoliko su odgovori na ova pitanja potvrdni, fokus se pomera i utvrđuje se šta se desilo, gde, kada, kako, ko je umešan, i zašto. Proces po kojem digitalni dokaz otkriven i primenjen na ova pitanja sastoji se iz nekoliko koraka pri kojima se svaki od njih izvodi po strogim protokolima, proverenim metodama, i u nekim slučajevima proverenim alatima.

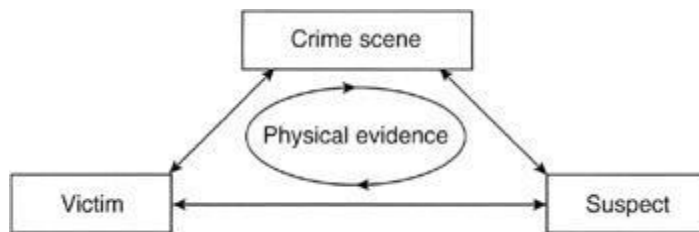
Najvažnije je da uspeh ovog procesa najviše zavisi od iskustva i veština istražitelja, ljudi koji pregledaju dokaze i tehničara mesta zločina koji moraju da sarađuju da bi povezali dokaze zajedno i da bi razvili ubedljivi „*account*“ (sadržaj) prekršaja.

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.

2.4. ULOGA DIGITALNIH DOKAZA

Jedan od glavnih ciljeva u istrazi je povezivanje zločina sa izvršiocem otkrivanjem odgovarajućih veza između počinioca, žrtve, i mesta zločina. Svedoci mogu da identifikuju osumnjičenog ali dokazi o umešanosti individue su obično pouzdaniji. 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 [1].



Slika 3. *Locard's Exchange Principle* [7]

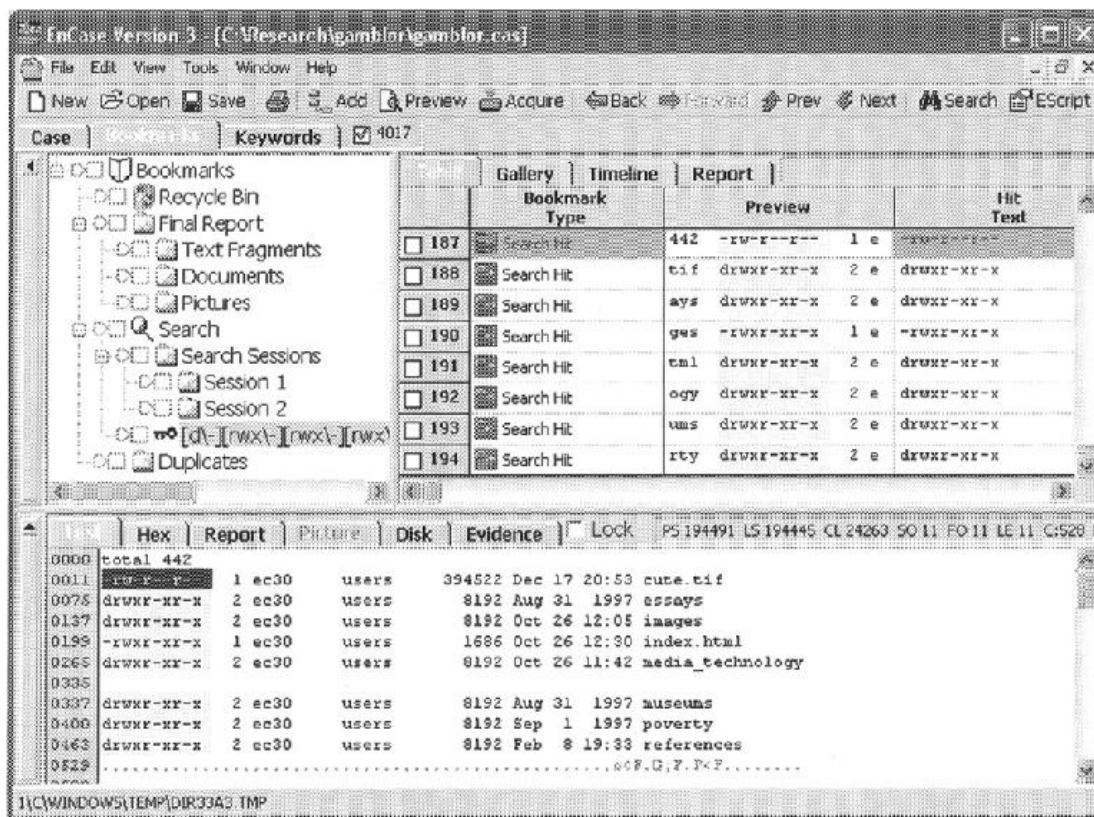
Ovaj tip razmene svrstava dokaze u jednu od dve kategorije:

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

Klasne karakteristike mogu da pomognu istražiteljima npr. da odrede da je Apache Web Server korišten, ili određena šema za e-mail (MIME), ili da je mrežna karta određenog proizvođača korištena.

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*, *SecureCRT*, *SSH* ili neki drugi program prikazivao na ekranu Slika 4. 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 4. Ostaci listinga direktorijuma sa UNIX sistema nađene na Windows kompjuteru koristeći „grep” funkciju u alatu EnCase za pretragu po "[d\-][rwx\-][rwx\-][rwx\-][rwx\-][rwx\-][rwx\-][rwx\-](space)." [7]

2.5. 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 :

1. Hardver kao proizvod kriminalne aktivnosti (*Hardware as Contraband or Fruits of Crime*).
2. Hardver kao instrument (oruđe) zločina (*Hardware as an Instrumentality*).
3. Hardver kao dokaz (*Hardware as Evidence*).
4. Informacija kao proizvod kriminalne aktivnosti (*Information as Contraband or Fruits of Crime*).
5. Informacija kao instrument (oruđe) zločina (*Information as an Instrumentality*).
6. Informacija kao dokaz (*Information as Evidence*).

Ove kategorije nisu međusobno isključive, i neki zločin može da spada u više različitih kategorija.

2002 godine USDOJ je ažuriralo dokument tako da je u skladu sa današnjom tehnologijom i zakonom i izrastao je u uputstvo za "*Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*" (USDOJ 2002). Dok vodiči pridaju istu važnost hardveru i softveru, uputstvo pridaje veću važnost informacionom delu. Ukoliko hardver sam po sebi kao uređaj nije dokaz, oruđe ili plod zločina onda se hardver posmatra kao skladište podataka. Iako je prikupljanje informacija glavni cilj, može biti neophodna i kolekcija hardvera iz različitih razloga.

Zbog unikatnosti legalnih procedura za svaku kategoriju zločina, ovo uputstvo bi trebali pročitati istražitelji, tužioci i advokati odbrane.

Od najvećeg značaja je to što uputstvo ima mrežno-centralni prilaz problemu.

2.5.1. Hardver kao proizvod kriminalne aktivnosti (*Hardware as Contraband or Fruits of Crime*)

Zabranjeni materijal je vlasništvo koje običan građanin ne sme da poseduje. Npr. pod određenim 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 koja je ukradena, ili kupljena koristeći ukradene kreditne kartice.

2.5.2. Hardver kao instrument(oruđe) zločina (Hardware as an Instrumentality)

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 instrument 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. Sudovi u Americi su liberalni po ovom pitanju.

Primeri slučaja iz Amerike:

Primer 1. U slučaju dečije pornografije u gradu New York sud je odlučio da je kompjuter instrument zločina zato što je kompjuter imao mogućnost slanja i primanja slika. (*United States v. Lamb* 1996).

Primer 2. Istočni Okružni Sud iz Virdžinije odlučio je da je kompjuter instrument zločina zato što je sadržao fajl koji je detaljno opisivao rast biljaka marihuane. (*United States v. Real Property* 1991).

2.5.3. Hardver kao dokaz (Hardware as Evidence)

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.

2.5.4. Informacija kao proizvod kriminalne aktivnosti (Information as Contraband or Fruits of Crime)

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.

2.5.5. Informacija kao instrument(oruđe) zločina (Information as an Instrumentality)

Informacija može biti the oruđe 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 krekuju šifre mogu takođe biti instrumenti zločina. Ukoliko ne postoji mogućnost da se prikaže da je informacija imala jednu od značajnijih uloga u zločinu, onda verovatno nema potrebe da se konfiskuje kao instrument zločina.

2.5.6. Informacija kao dokaz (Information as Evidence)

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.

Posle toga koristio sam mobilni i kontaktirao određene osobe. Zapisi o toj komunikaciji mogu da se pribave od mobilnog operatera. U tim zapisima možemo videti ko je sa kim komunicirao i vremena poziva. Sve ove informacije mogu se koristiti kao dokazi u slučaju.

2.6. ISTRAŽNE METODOLOGIJE

U daljem tekstu bih opisao dve metodologije koje mi se čine kao najsveobuhvatnije i najprimenljivije u ovom trenutku. Jedna ima pristup sa pravnog stanovišta, dok druga ima pristup više sa naučnog. Jedna metoda nadopunjuje drugu.

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 korenspodencije fizičke i digitalne istrage.

2.7. ISTRAŽNA METODOLOGIJA Prema Eoghan Casey-u

“Istražni proces se izvodi kroz niz rastućih stepenika prikazanih na *slici 5*. 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.”

Eoghan Casey



Slika 5: Kategorije Istražnog procesnog modela opisane kao niz stepenika.[7]

Kategorije na *slici 5*. bi trebale biti opšte. Jedinstvene metode i alati korišteni u svakoj kategoriji vezuju istražni proces za određeni forenzički domen.

Istražitelj i ispitivač (*investigators and examiners*) 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. U mnogim slučajevima mehanizmi korišteni za struktuiranje, organizovanje, i snimanje detalja o svim događajima i fizičkim predstavama koje se tiču određene istrage su isto važne kao i sama informacija koja se prezentuje. 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.

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.

2.7.1. Optužbe ili uzbuna incidentom (Accusation or Incident Alert)

Svaki 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 se donose zaključci, zasnovani na malom broju dokaza, da li se kriminalni akt dogodio ili nije.

2.7.2. Procena vrednosti (Assessment of Worth)

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.

2.7.3. Protokoli Incidenta/Mesta zločina (Incident/Crime Scene Protocols)

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.

2.7.4. Identifikacija ili zaplena (Identification or Seizure)

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.

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 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 kompatibilne 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 proveru 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

iskrsnu. 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.

2.7.5. Čuvanje (Preservation)

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.

2.7.6. Oporavak podataka (Recovery)

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 počinioaca ukoliko je konkretan dokaz odlučnosti pronađen ili snimljen.

2.7.7. Žetva (Harvesting)

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.

Na primer, optužba koja je povezana sa dečijom pornografijom zahteva vizuelne digitalne dokaze u standardnom kompjuterskom grafičkom 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.

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.

2.7.8. Redukcija (Reduction)

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.

2.7.9. Organizacija i pretraga (Organization and Search)

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.

2.7.10. Analiza (Analysis)

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 prekršioaca. 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 poruk, 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).

2.7.11. Izveštavanje (Reporting)

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 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.

2.7.12. Ubeđivanje i svedočenje (Persuasion and Testimony)

Značajan 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.

2.8. 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.

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; zvanični model procesa istrage.

2.8.1. Korporacijski Model Istrage

U knjizi “*Incident Response*” opisuje se istražni model sa sledećim fazama:

1. **Priprema:** Pripremiti se za incident sa odgovarajućom obukom i infrastrukturom
2. **Detekcija incidenta:** Identifikovati sumnjivi incident.
3. **Prva reakcija:** Potvrditi da se incident dogodio i sakupiti preliminarne, nestabilne dokaze (koji se degradiraju vremenom)
4. **Formulisanje strategije reakcije:** Odrediti reakciju, bazirajući se na saznatim informacijama
5. **Dupliranje:** Napraviti “backup”, fizičku miror sliku sistema
6. **Istraga:** Istražiti sistem zbog identifikacije ko, šta i kako
7. **Implementacija mera zaštite:** Izolovati sumnjiv sistem pre nego što je vraćen u normalni režim rada.
8. **Posmatranje mreže:** Posmatrati mrežu radi identifikacije novih (ponovljenih) napada
9. **Oporavak:** Vratiti sistem u njegovo originalno stanje sa dodatnim merama zaštite
10. **Izveštavanje:** Napraviti dokumentaciju o reakciji na incident (kriminal).
11. **Finalna faza:** Izvršiti reviziju reakcije i izvršiti eventualne promene.

Ova metodologija je adekvatna za korporacijski model istrage.

2.8.2. Zvanični model istrage

Američki “*Department of Justice*” je objavio model procesa istrage u “Vodiču za istragu elektronske scene zločina”. Vodič odgovara fizičkoj sceni zločina, tako da je akcenat stavljen na te potrebe. Malo pažnje je fokusirano na forenzičku analizu digitalnog sistema. Faze modela su sledeće:

- **Priprema:** Pripremiti opremu i alat potreban za istragu.
- **Sakupljanje:** Naći i sakupiti elektronske dokaze.
 - **Osigurati i proceniti scenu:** Obezbediti scenu radi bezbednosti lica i integriteta podatka. U ovoj fazi trebalo bi da se identifikuju potencijalni dokazi.
 - **Dokumentovanje scene:** Dokumentovati fizički opis scene uključujući fotografije kompjutera.
 - **Sakupljanje dokaza:** Uzeti fizički računarski sistem ili napraviti kopiju podataka na forenzičkom sistemu.
- **Pregled:** Tehnički pregled sistema radi nalaženja dokaza.
- **Analiza:** Istražni tim pregleda rezultate tehničkog pregleda radi procene njihove važnosti za slučaj.
- **Izveštaj:** Izveštaj se pravi posle svakog slučaja kompjuterskog kriminala (incidenta). Ovaj model je baziran na standardnoj fizičkoj istrazi scene zločina. Kao i prethodni model ovaj model ne obraća mnogo pažnje na proces forenzičke analize i ne ispunjava naše zahteve modela procesa digitalne istrage.

2.9. Model istrage fizičke scene zločina

Sa aspekta teorije istrage, konsultovana literatura fizičke istrage. Faze fizičke istrage scene zločina su:

1. **Očuvanje, fiksiranje scene zločina:** Prvi korak je da se pomogne povređenima, zatim sledi potraga za osumnjičenima i hapšenje osumnjičenih i zadržavanje svih svedoka. Fizička scena zločina mora biti osigurana, a pristup sceni zločina omogućen samo ovlašćenim licima (istražnim organima, (detektivima), forenzičarima itd.).
2. **Pregled scene zločina:** Detektiv “prolazi” (šeta oko mesta) kroz scenu zločina da bi identifikovao očigledne delove dokaza i dokaze koji su prolazni (kratkotrajni (krv, sluz, pljuvačka itd.)). Početna opažanja (ko, šta, gde, kada, kako) se dokumentuju i kreira se početna teorija (hipoteza slučaja).
3. **Dokumentovanje scene zločina:** Scena zločina se dokumentuje fotografisanjem, skiciranjem i snimanjem video snimaka. Dokaze treba dokumentovati jasno (čisto) potpuno i sakupljati ih za analizu.
4. **Pretraga scene zločina:** Obrasci istrage koriste se da bi se identifikovali dodatni dokazi koji nisu nađeni u pregledu. Teorija razvijena u pretrazi koristi se za pretragu specifičnih dokaza koji nedostaju (npr. oružje kojim je počinjeno ubistvo).
5. **Rekonstrukcija scene zločina:** Događaji koji su se dogodili na mestu zločina određuju se na osnovu izgleda scene zločina, mesta i pozicije fizičkih dokaza, analiziranih rezultata iz forenzičke laboratorije i naučnih metoda primenjenih u istrazi i analizi dokaza.

Ovaj model omogućava kompletnu dokumentaciju mesta zločina i koristi detektivsko iskustvo (iskustvo istražnog organa) da bi se došlo do korisnih dokaza. Svi fizički predmeti ne mogu da se uzmu sa mesta zločina, tako da *Faza Pretrage* mora biti potpuna da bi se sakupili potrebni dokazi, ali ne sme se preopteretiti laboratorija sa predmetima koji nemaju veze sa slučajem.

2.10. Integrirani model procesa digitalne forenzičke istrage

Ovaj model istrage koristi mnoge faze koje su opisane u poglavljima 2.8.1, 2.8.2 i 2.9, ali prilazi problemu sa druge tačke gledišta. Ovaj model koristi teoriju da je kompjuter sam po sebi mesto zločina, nazvan *digitalna scena zločina* i primenjuje tehnike istrage fizičke scene zločina. Istraga fizičke scene zločina koristi zakone prirode da bi našla fizičke dokaze, a istraga digitalne scene zločina koristi kod da bi našla digitalne dokaze.

U istrazi fizičke scene zločina, najpoznatija teorija je *Lokardov zakon razmene*: “Kada dva objekta dođu u kontakt, doći će do razmene materije između njih”. Na primer, dlake i vlakna sa zločinca se često zadržavaju na fizičkoj sceni zločina. Sličan efekat se dešava u digitalnoj sceni zločina. Privremeni fajlovi (datoteke), sadržaj memorije koji je snimljen na disku i izbrisani delovi fajlova mogu postojati zbog delovanja softvera (OS) koji je osumnjičeni koristio i izvršavao. Podatak ulazi i postoji u digitalnoj sceni zločina i ostavlja tragove digitalnog dokaza iza sebe na raznim mestima u memorijskim elementima računarskog sistema (hard disku, memoriji, pokretnim memorijskim elementima itd.). Digitalni forenzičar je prepušten radu operativnog sistema i aplikacija, zato što oni kontrolišu koji dokaz je napisan u memorijskoj lokaciji.

Koristeći koncept da je kompjuter sam za sebe scena zločina, teorija istrage fizičke scene zločina primenjena je na digitalnu forenzičku istragu. Rezultujući model procesa je opisan u sledećem poglavlju, uključujući kratak opis akcija koje treba preduzeti. Forenzička istraga digitalne scene zločina je integrisana sa istragom fizičke scene zločina tako da fizički dokazi mogu biti sakupljeni i povezani sa digitalnom aktivnošću (X) lica. Digitalna scena (X) osumnjičenog zločina može se smatrati za sekundarnu scenu zločina, u odnosu na fizičku scenu zločina.

U ovom polju, postoji mnogo interpretacija i mišljenja za ključne reči. Da bi se sprečila konfuzija, definisaćemo osnovne termine procesa. Postoje brojne definicije za svaki termin i zbog toga sam se opredelio za sledeće, zato što 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 su primeri digitalnog dokaza.

- **Fizička scena zločina:** Fizičko okruženje gde postoje fizički dokazi zločina ili incidenta. Okruženje gde se prvi kriminalni akt dogodio je primarna fizička scena zločina, a sledeće scene su sekundarne fizičke scene zločina. Ova definicija je kreirana prema definiciji koju je definisao *Lee*.
- **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**.

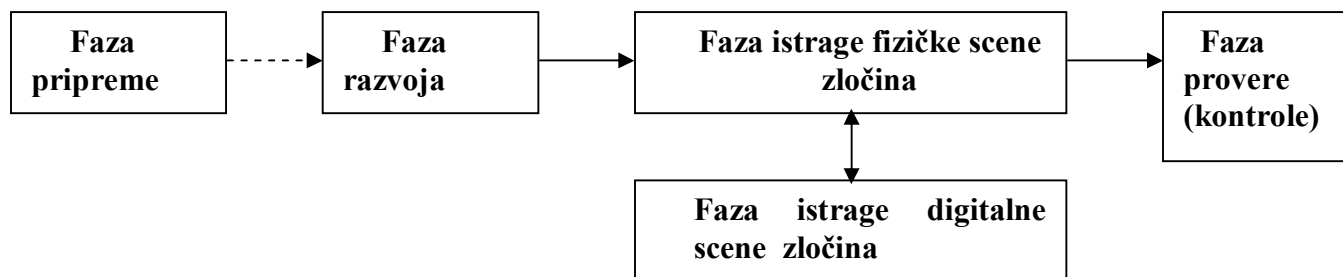
Ovaj model procesa primenjuje se na obe vrste istrage, korporacijsku i zvaničnu. Zbog toga se izrazi “scena zločina” i “incident” koriste u opštem smislu. Pod fizičkom scenom zločina podrazumeva se sto zaposlenog koji je ispitivan od strane organa istrage (*Ljudskih Resursa*), centar podataka koji sadrži kompjuter server, soba za istragu dečije pornografije, ili kola u kojim je čovek ubijen i u kojima na suvozačevom sedištu stoji otvoren laptop. Incident je bilo koja serija događaja koji prouzrokuju da reaguje interventni tim za odgovor ili forenzički tim za prikupljanje dokaza. Ovo uključuje upad u server, izdavanje naloga za pretres kuće osumnjičenog i reagovanje specijalne jedinice MUP-a za borbu protiv visokotehnološkog (kompjuterskog) kriminala na hitni poziv 92.

Pretpostavljamo da je veličina scene zločina inicijalno definisana prirodnim granicama oko poznatih dokaza. Na primer, ukoliko je zločin počinjen u kući, onda kuća i vlasništvo oko nje može biti inicijalna scena fizičkog kriminala, a veličina kasnije može biti povećana ili smanjena zavisno od dodatnih dokaza koji se pronađu. Za kompjuter, inicijalna digitalna scena zločina je tipično virtuelno okruženje kreirano lokalnim operativnim sistemom i hardverom. Svaki kompjuter uključen u incident će verovatno biti zasebna scena zločina.

Termini “pregled (revizija)” i “analiza” koji se koriste u ovom projektnom zadatku, znače da se neki objekat može procesirati u nekom smislu i da se mogu prikupiti informacije iz njega.

Model 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)



Slika 6: Pet grupa faza u procesu istrage.

Prisetimo da se na slici *Faza Istrage Fizičke Scene Zločina* izvodi uporedo sa *Fazom Istrage Digitalne Scene Zločina*. Rezultati *Istrage Digitalne Scene Zločina* koriste se u *Istrazi Fizičke Scene Zločina*.

2.10.1. Faza pripreme

Cilj faze pripreme je da osigura da operacije i infrastruktura mogu u potpunosti podržati (pomoći, omogućiti) istragu. Digitalni i fizički dokazi mogu biti izgubljeni ukoliko nisu prikupljeni i čuvani na pravi način. Ova faza je u stalnom trajanju i nije vezana za bilo koji zločin ili incident.

Operacije faze pripreme obezbeđuje obuku i opremu za lica koja će biti uključena u istragu incidenta. Ovo uključuje obuku interventnog tima za odgovor (eng. “responders”), forenzičkih laboratorijskih analitičara, i lica koja će primati inicijalne (prvobitne) izveštaje o incidentu. Oprema koju interventni tim donosi na scenu zločina mora da bude ispravna i mora biti poslednja tehnologija. Oprema u forenzičkoj laboratoriji za analizu mora, takođe, da bude održavana (na visokom nivou pouzdanosti) i spremna kada podaci o incidentu stignu.

Infrastruktura faze pripreme osigurava da postoje (da se generišu) potrebni podaci da bi se izvršila potpuna istraga, jer ukoliko podaci ne postoje nemoguće je izvršiti istragu. Ova faza se odnosi samo na one koji održavaju okruženje koje bi mogao biti scena zločina. Fizički primeri za ovu fazu su instalacije i raspoređivanje video nadzora i čitača kartica da bi se snimilo ko je bio u tom prostoru za vreme zločina. Digitalni primeri za ovu fazu su slanje log datoteka servera na zaštićeni “log host”, sinhronizacija unutrašnjih satova na serverima sa NTP-om, kreiranje sistema osnovne, optimalne zaštite sa MD5 i održavanje upravljanja promenama baze podataka.

2.10.2. Faza razvoja

Cilj faze razvoja je da obezbedi mehanizam za detekciju i potvrdu incidenta. Zadaci koji se izvode u ovoj fazi dosta se razlikuju između zvaničnog i korporacijskog tima za istragu.

Faza detekcije i obaveštenja je faza kada se incident detektuje i odgovarajući ljudi obaveste o incidentu. Ovo se može obaviti putem poziva 92, preko uzbune mrežnog *Intrusion Detection System*-a (IDS), ili online od strane prerušenog policajca, koji istražuje ilegalne aktivnosti. Ova faza definiše početak procesa istrage.

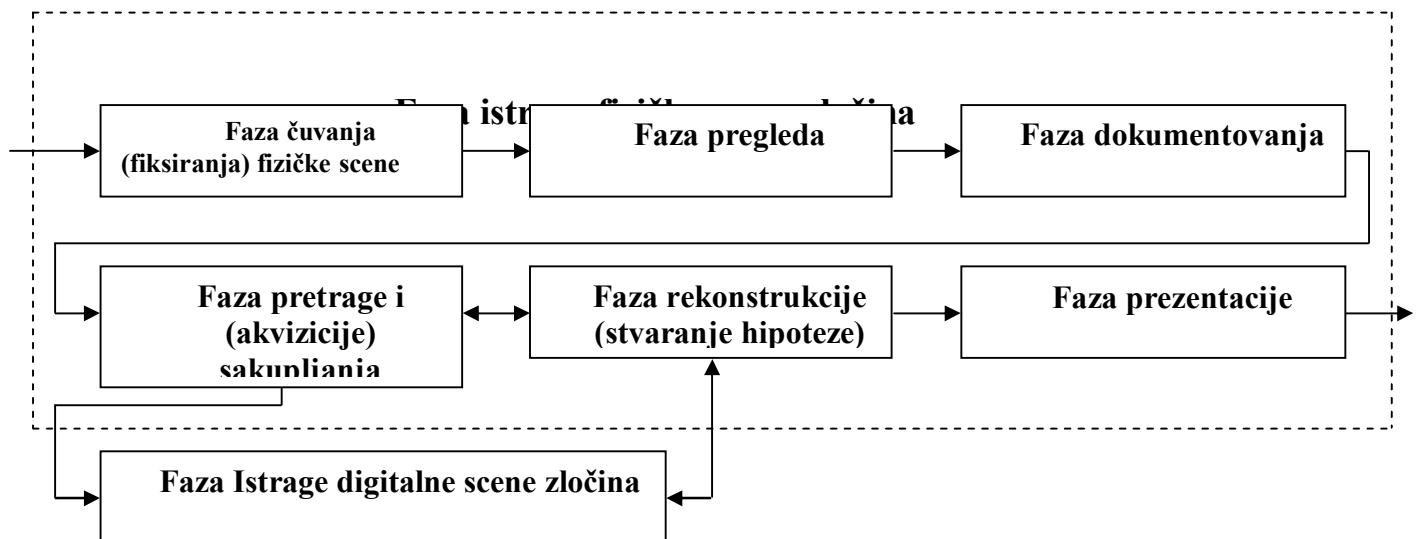
Faza potvrde i autorizacije će nastaviti u različitim smerovima, zavisno od situacije. Cilj ove faze je da dobije autorizaciju (ovlašćenje) da u potpunosti istraži incident i scenu

zločina. Za slučaj zvanične istrage, ovaj korak podrazumeva vađenje naloga za pretres ili drugo legalno odobrenje, koje je potkrepljeno dovoljnim dokazima ili sumnjama.

Za slučaj korporacijskog incidenta, nalozi za pretres nisu potrebni dok god se ne krše prava privatnosti ili slučaj preraste kapaciteta i sposobnosti korporacijskog tima za istragu (npr. međunarodni incident, zahtev za prisluškivanje telefona osumnjičenog, hapšenje i dr.). U situaciji upada u server, ovaj korak uključuje interventni tim za odgovor na incidente koji proverava da li je sistem kompromitovan, tako što gledaju sumnjive aktivnosti na mreži ili traže rootkit-ove po sistemu. U toku ove analize uživo važno je da se prema sistemu ophodi kao prema sceni zločina i da se minimizira uticaj na sistem. Posle potvrde da se incident dogodio, neophodan je pristanak supervizora da bi se preduzele naredne akcije. Za servere čiji je vreme aktivnog rada kritično za kompaniju, odobranje mora da se traži na nivou izvršne vlasti.

2.10.3. Faza istrage fizičke scene zločina

Cilj ove faze je da prikupi, analizira fizičke dokaze i rekonstruiše akcije koje su dovele do incidenta. Jedan od najvažnijih ciljeva forenzičke digitalne istrage je da se identifikuje ljude koji su odgovorni za incidente i zbog toga su potrebni fizički dokazi. Za zvanični model istrage, ekspert za fizičku scenu zločina izvršava većinu ovde navedenih zadataka. U korporacijskoj istrazi, ove zadatke će izvršiti interventni tim za odgovor na kompjuterski incident ili tim za fizičku bezbednost. Faze za istragu fizičke scene zločina prikazane su na slici 2.



Slika 7: Šest faza istrage fizičke scene zločina i interakcija sa istragom digitalne scene zločina

Faza čuvanja (fiksiranja) je ista za svaki tip zločina. Aktivnosti koje se preduzimaju su osiguranje izlaza, pomoć ranjenima, zadržavanje osumnjičenih, i identifikovanje svedoka. U digitalnom incidentu, fizička scena zločina trebalo bi da se osigura koristeći iste procedure kao i kod fizičkog incidenta (koji nije digitalni). U istrazi upada u server, ova faza uključuje identifikovanje, ko je bio u centru za obradu podataka i sprečavanje drugih

da uđu u centar zbog toga što je možda neko od zaposlenih odgovoran za incident. Primetimo da ova faza čuva scenu zločina od izmena da bi se kasnije mogli sakupiti i identifikovati dokazi. Ova faza ne čuva određene delove dokaznog materijala već celokupnu scenu zločina.

Faza pregleda fizičke scene zločina odvija se tako što organ istrage (detektiv, istražitelj) prolazi i opservira scenu zločina i obično je prva osoba koja odgovara na incident. Cilj je da se identifikuju očigledni delovi dokaznog materijala, osetljivi delovi fizičkog dokaza i razvije početna teorija (hipoteza) o zločinu. Na primer, u istrazi ubistva, u ovoj fazi se ide kroz stan i identifikuje kako je napadač ušao, na kom mestu se ubistvo dogodilo i šta se dogodilo sa žrtvom posle ubistva. Osetljivi delovi dokaza bi trebali da se dokumentuju i sakupe odmah da se ne bi oštetili. U digitalnom incidentu, primeri fizičkih dokaza koji su identifikovani u pretrazi uključuju broj i lokaciju kompjutera, koje mrežne konekcije kompjuteri poseduju, PDAs, mobilni telefoni, lozinke (šifre) na papiru, razne zabeleške i odštampani materijali i CD-romovi ili neki drugi prenosivi mediji. Pri završetku ove faze istražni organi će imati ideju kako da obradi fizičku scenu zločina i koje specijalne veštine će mu biti potrebne za obradu. Ukoliko digitalni forenzičar -specijalista za kompjutere nije na uviđaju u tom trenutku, treba ga pozvati da dođe i izvrši forenzičku akviziciju dokaza (uzme dokaze). Kompjuter koji je uključen tj. koji radi i koji je priključen na mrežu može se smatrati za osetljiv (krt) dokaz, jer se digitalni dokazi koji se nalaze u njemu mogu izbrisati pomoću komande sa udaljenog sistema (računarskog). Zbog toga se obavezno koriste neke standardne procedure kao što je isključivanje kompjutera sa mreže (zavisno od vrste platforme: *Windows, Linux/Unix,...*) dok ne počne potpuna forenzička istraga.

Faza dokumentovanja fizičke scene zločina izvodi se tako što se prave fotografije, skice i video snimci scene zločina i fizičkih dokaza. Cilj je da se prikupi što više informacija tako da se razmeštaj i važni detalji scene zločina sačuvaju i zabeleže. Kod digitalnog incidenta važno je da se dokumentuju i fotografiju konekcije na kompjuteru i stanje kompjutera. Takođe bi moglo biti od važnosti da se dokumentuje broj i veličina hard diskova i količina memorije. U nekim slučajevima, MAC adresa hardvera mrežnih karata bi isto trebalo da se sačuva da bi se DHCP logovi mogli koristiti za identifikovanje systemske aktivnosti. Korisno je sačuvati serijske brojeve i “oznake objekata sistema” u ovoj fazi. Da bi se identifikovalo šta treba sačuvati, treba uzeti u obzir da forenzičke laboratorije za analizu ne mogu dobiti originalni fizički hardver, već samo fizičku (mirror) kopiju hard diska. Bilo šta što bi moglo biti od koristi za forenzičku laboratoriju za analizu, ili kasniju rekonstrukciju trebalo bi da se zabeleži. Na kraju *Faze Dokumentacije* izrađuje se konačni izveštaj o incidentu.

Faza pretrage i prikupljanja (akvizicije) dokaza iz fizičke scene zločina obuhvata pretragu i detaljno prikupljanje iz dubine scene dodatnih fizičkih dokaza. Pretraga može biti usmerena prema nestalim delovima fizičkih dokaza, kao što su oružje, ili može biti metodična i ima striktnu šablone pretrage. Svaki tip dokaza treba da ima specifične standardne procedure, za prikupljanje (akvizicije). Za digitalni incident u ovoj fazi traže se dodatni mediji i digitalni uređaji sa mesta zločina. Ova faza takođe uključuje kontaktiranje administratora radi očuvanja i obezbeđivanje logova za pristup (*access logs*) centru podataka, promenljivih logova za “*update*” servera, logove *firewall*-ova, logova IDS, i logove udaljenog pristupa (*remote access logs*). Ovo je poslednja faza koja

se vrši na realnoj sceni zločina. Fizički dokazi koji su prikupljeni sa scene zločina, šalju se u forenzičku laboratoriju radi analize a rezultati se koriste u sledećoj fazi, rekonstrukcije incidenta.

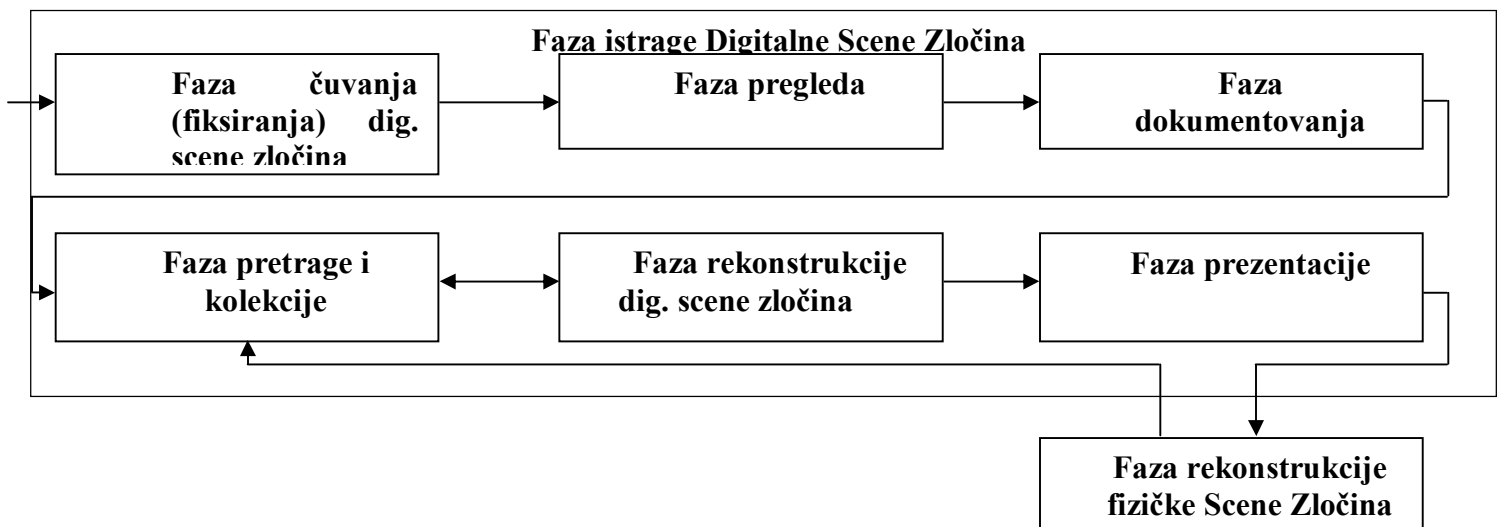
Faza pretrage i prikupljanja dokaza iz fizičke scene zločina je faza u kojoj počinje forenzičke istrage scene zločina. Kompjuterski sistem se smatra za fizički dokaz pa će se i on uzeti kao dokazni materijal gde god je moguće. Procedure prikupljanja bi trebalo da dokumentuju kako da se prikupe važni podaci sa sistema koji je aktivan i kako da se sistem isključi. Faze Digitalne Scene Zločina detaljno su prikazane u sledećem poglavlju.

Faza rekonstrukcije fizičke scene zločina uključuje organizovanje rezultata analize iz prikupljenih fizičkih i digitalnih dokaza i korišćenje fotografija sa scene zločina da bi se razvila teorija (hipoteza) o incidentu. Naučni metod se koristi za rad sa dokazima da bi se mogle testirati teorije o incidentu. Kod digitalnog incidenta, rezultati istrage digitalne scene zločina su u vezi sa fizičkim dokazima da bi se povezala osoba sa digitalnim događajima. Primeri u ovoj fazi su povezivanje logova sa servera u centru podataka sa *login*'ovima u radnoj stanici (napadnutom računaru) i drugim mrežnim uređajima, povezivanje *chat* aktivnosti nađene u sistemu sa aktivnošću prerusenog (maskiranog) detektiva, i povezivanje aktivnosti na kompromitovanom serveru sa aktivnošću na kućnom računarskom sistemu osumnjičenog i mrežnom aktivnošću sačuvanog od strane ISP-a. Da bi imala najveći efekat, ova faza treba da uključi eksperte digitalne forenzičare radi pomoći oko povezivanja i konsultovanja događaja sa više izvora digitalnih dokaza. Primetimo da rekonstrukcija fizičke scene zločina nije isto što i “ponovno kreiranje”, koje podrazumeva izradu fizičkog modela scene zločina .

Faza prezentacije fizičke scene zločina prezentuje fizičke i digitalne dokaze sudu ili upravi korporacije. Ova faza prezentuje dokaze i teoriju koje je razvijena u fazi rekonstrukcije fizičke scene zločina.

2.10.4. Faza istrage digitalne scene zločina

Faza istraga digitalne scene zločina počinje kada su fizički digitalni uređaji prikupljeni kao i fizički dokazi sa fizičke scene zločina ili kada je sačuvani mrežni saobraćaj analiziran radi obezbeđivanja dokaza. Ova faza prilazi kompjuterskom sistemu kao sceni zločina i pretražuje ga radi izvlačenja dokaza. Cilj je da se identifikuju elektronski događaji koji su se dogodili na sistemu i prezentuju istražnom organu fizičke scene zločina. Specijalista za rad sa forenzičkim alatima i tehnikama za analizu vrši forenzičku digitalnu analizu u sledećim fazama. Faze su prikazane na slici 3.



SLIKA 8: Šest faza u forenzičkoj istrazi digitalne scene zločina. Rezultati se vraćaju u istragu fizičke scene zločina.

U ovom modelu, svaki digitalni uređaj se smatra posebnom (odvojenom) fizičkom scenom zločina. Konačni rezultati analize svakog digitalnog uređaja šalju se u *Fazu Rekonstrukcije Fizičke Scene Zločina*, u kojoj će biti identifikovane veze između digitalnih uređaja. Ovo omogućava da se analize različitih tipova uređaja izvrše na različitim mestima. Fizičke scene zločina organizovane su u primarne i sekundarne scene, gde su primarne one gde se prvi kriminalni akt dogodio. Digitalne scene zločina mogu takođe da se organizuje u primarne i sekundarne scene zločina. Na primer, server koji je kompromitovan bio bi primarna scena zločina, a log server koji je bio kompromitovan kasnije zbog izmene log-ova koji su u vezi sa upadom, bio bi sekundarna digitalna scena zločina.

Faza čuvanja digitalne scene zločina sastoji se iz obezbeđivanja ulaza i izlaza ka digitalnoj sceni zločina i očuvanja digitalnih dokaza koji bi se lako mogli promeniti. U fizičkom svetu, ovome odgovara smanjenje broja otiska stopala i sakupljanje fizičkih dokaza koji bi mogli da se vremenom izgube. U digitalnom svetu ovo bi značilo izolaciju sistema od mreže, sakupljanje nestabilnih (lako promenljivih) podataka koji bi mogli biti izgubljeni kada se sistem isključi i identifikovanje bilo kakvih sumnjivih procesa, koji su aktivni u sistemu. Sumnjivi korisnici koji su ulogovani (registrovani) na sistem trebali bi biti registrovani i po mogućstvu ispitani. Log datoteke mogu se smatrati za očevidce zločina i moraju biti obezbeđene ukoliko postoji pretnja da će biti izbrisani pre nego što se sistem fizički iskopira. Primetimo da drugi modeli koriste “čuvanje” u smislu očuvanje digitalnih dokaza. U ovom modelu “čuva se” celokupno digitalno okruženje. U stvari, nijedan digitalni dokaz nije još identifikovan, kada se ova faza izvršava. Jedna od prednosti digitalnog sveta u odnosu na fizički svet je u tome da se digitalno okruženje može lako kopirati. Zato, je uobičajeno u ovoj fazi da se napravi kompletna slika, fizički (mirror) *backup* sistema na forenzičkom računaru da bi se mogao kasnije analizirati u forenzičkoj laboratoriji. Kompletne fizičke kopije diskova očuvaju celokupnu digitalnu scenu zločina, dok kopije koje su samo obični *backup*-ovi sistema čuvaju samo dodeljene podatke u digitalnoj sceni zločina. Kritični sistemi mogu da se povrate posle kreiranja forenzičke fizičke slike tako da se može brzo priključiti na mrežu. Neki slučajevi zahtevaju da originalni hard disk ostane fizički dokaz sve dok je slučaj u toku. Kada monitori mrežnog saobraćaja snime mrežni tok saobraćaja, tada oni imaju efekat čuvanja bezbednog (neizmenjenog) stanja mreže.

Faza pregleda digitalne scene zločina odigrava se u forenzičkoj laboratoriji koristeći jedan od slika, replika scene zločina. Ova faza može da se izvrši na živom sistemu (kompromitovanom sistemu uživo), isto kao i u fizičkom svetu, ali se preferira laboratorijsko okruženje, zato što pruža kontrolisane uslove, a rezultati se mogu ponoviti sa drugom kopijom sistema, ako to zahtevaju sudski organi. Ukoliko se *Faza Pregleda* izvodi na živom sistemu, trebalo bi forenzičku sliku sistema ipak napraviti tako da se bilo koji digitalni dokaz može prikupiti i u kontrolisanom laboratorijskom okruženju. Ova faza se ponekad radi na terenu da bi se utvrdilo da li sistem treba donositi u laboratoriju

na punu forenzičku analizu. Pretrage na terenu obično se izvode na *boot*-ovanom sistemu u sigurnom okruženju tako da digitalni dokazi ostanu nepromenjeni (sa *butabilnog* CD/diskete).

U *Fazi Pregleda* pronalaze se očigledni delovi digitalnih dokaza za datu vrstu zločina. Na primer, u slučaju dečije pornografije istražni organ će prikupiti sve grafičke slike sa sistema i identifikuje one koje bi mogli da se koriste kao dokazi. U upadu na server, istražitelj bi tražio očigledne znakove instalacije *rootkit*-a, analizirao logove aplikacija i tražio nove konfiguracione datoteke. U drugim slučajevima, mogu se analizirati keš i istoriju na *HTML browser*-u. Kada se analizira mrežni saobraćaj o nekom incidentu, ova faza može analizirati saobraćaj zbog okvirnog vremena incidenta i filtrirati (odbaciti) određene portove i hostove. *Faza Pregleda* će pokazati veštinu osumnjičenog i analizirati tehnike koje će biti potrebne u istrazi. Istražni organ u ovoj tački može konsultovati eksperte iz oblasti kriptologije, digitalne forenzičke analize ili eksperte za oporavak podataka (povratak podataka ukoliko su neki nestali ili bili izbrisani).

Faza dokumentovanja digitalne scene zločina sastoji se iz pravilno dokumentovanih digitalnih dokaza koji su akvizicijom nađeni. Tačna (fizička) kopija sistema koja je potrebna u toku *Faze Očuvanja* imaju istu ulogu kao i skice i video zapisi fizičke scene zločina. Svaki deo digitalnog dokaza koji se pronađe u toku forenzičke analize fizičke (mirror) slike sistema mora biti jasno dokumentovan. Ova faza dokumentuje pojedinačne delove dokaza i ne kreira finalni izveštaj o incidentu. Finalni izveštaj forenzičke digitalne analize pravi se u *Fazi Prezentacije*.

Digitalni dokazi mogu postojati u različitim apstraktnim slojevima računarskog sistema i moraju biti dokumentovani prema tome. Na primer, datoteka može biti dokumentovan koristeći njegovo puno ime putanje, *cluster*-e fajl sistema koje datoteka koristi, i sektore na disku koje koristi. Mrežni podaci podaci mogu biti dokumentovani sa izvornom i ciljnom adresom na raznim mrežnim nivoima. Kako su digitalni dokazi promenljivi i mogu ostaviti malo tragova, dodatni koraci bi trebali da se preduzmu da bi se kasnije proverio integritet. Kriptografska heš vrednost, kao što je MD5 ili SHA-1, trebala bi da se primeni na dokaze kada se skupljaju da bi se mogao dokazati integritet na sudu. Lanac neprekidnog čuvanja i nadzora dokaza treba formirati u ovoj fazi, kako bi se dokazi mogli koristiti na sudu. U praksi, *Faza Dokumentovanja* nije posebna faza u digitalnoj istrazi zato što se digitalni dokazi dokumentuju u trenutku pronalaženja (akvizicije).

Faza pretrage i sakupljanja (akvizicije) dokaza sa digitalne scene zločina sastoji se od potpune digitalne forenzičke analize sistema radi izvlačenja digitalnih dokaza. Ova faza koristi rezultate iz *Faze Pretrage* da bi se fokusirala na dodatne tipove analiza. Na primer, u ovoj fazi može se izvršiti pretraga po ključnoj reči ukoliko su ključne reči identifikovane iz drugih dokaza. Nedodeljeni prostori fajl sistema mogu biti ekstrahovani i obrađeni zbog izbrisanih datoteka. Najniži nivo vremenske linije aktivnosti nad datotekama može biti analiziran da bi se pratile korisničke aktivnosti. Svi mrežni paketi koji su sakupljeni softverom za monitoring mrežnog saobraćaja mogu biti analizirani. U nekim slučajevima, može biti prikladno da se pregleda sadržaj svakog klastera (fizička

pretraga) ili svake datoteke (logička pretraga). Kao što postoje različite tehnike pretrage u fizičkoj sceni zločina, tako postoje i različite tehnike za analizu digitalne scene zločina.

Najveći deo vremena istrage potroši se u ovoj fazi. U digitalnom svetu, dokazi su kopirani iz scene zločina, ali nisu uklonjeni sa nje. Za neke tipove kompjuterskih incidenata, uobičajeno je da rade i tehnički i ne-tehnički istražni organi u ovoj fazi, zbog ograničenog broja obučenih organa za digitalnu forenzičku istragu. Na primer, tehnički istražni organi će izvući sve slike iz sistema i poslati ih ne-tehničkim istražnim organima koji će analizirati svaku sliku i identifikovati one koje bi se mogle koristiti kao dokaz. *Faza Pregleda* i *Pretrage* su slične *Fazi Ispitivanja* koji su deo drugih modela.

Faza rekonstrukcije digitalne scene zločina sastoji se iz sastavljanja delova digitalne zagonetke. Digitalni dokazi se mogu razvrstati i proceniti da bi se odredilo koliko je poverljiv i pouzdan. Podaci koji zahtevaju napredne tehnike analize, ko što su izvršne analize ili dešifrovanje, izvode se u ovoj fazi i koriste se njihovi rezultati. Ova faza koristi stroge naučne metode da bi se dokazi testirali i odbacile teorije potencijalno zasnovane na digitalnom dokazu. Ova faza ustanovljava kako je digitalni dokaz dospao tamo i šta njegovo postojanje (prisustvo) znači. Kada digitalni dokaz i dalje nedostaje, Faza Pretrage će nastaviti da identifikuje dodatne dokaze. Na primer, u slučaju upada u server, ova faza će dovesti u vezu eksploataciju ranjivih servisa sa instalacijom *rootkit*-a i razvojem mrežnog *sniffer*-a. Izvorišna IP adresa mrežne konekcije može dovesti do potrebe analize dodatne digitalne scene zločina. Ova faza je slična *Fazi Analize* drugih modela.

Faza prezentacije digitalne scene zločina obuhvata prezentovanje nađenih digitalnih dokaza fizičkom istražnom timu. Rezultate iz digitalne istrage tim za istragu fizičke scene zločina koristi u *Fazi Rekonstrukcije*. Istražni organ fizičke scene zločina integriše rezultate od svake digitalne scene zločina. U ovoj fazi dokumentuju se i prezentuju otkrića određene scene zločina drugim organima istrage. U mnogim slučajevima, fizički i digitalni tim za istragu su isti i informacije se lakše razmenjuju između članova tima.

2.10.5. Faza provere (kontrole)

Finalna faza je **Faza provere** i sastoji se od provere istrage da bi se identifikovale oblasti koje bi se mogle poboljšati. Za digitalni kompjuterski incident, ovo uključuje koliko dobro su izvršene fizička i digitalna istraga svaka za sebe, koliko dobro su urađene fizička i digitalna istraga zajedno i da li postoji dovoljno fizičkih i digitalnih dokaza da bi se rešio slučaj. Rezultat ove faze mogle bi biti nove poboljšane procedure, nova obuka, ili ništa ukoliko je sve ispalo kako je planirano.

3. 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 prikupljanja 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.

4. VRSTA 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 (miror))
- 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

integriranih 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.

5. ILOOK

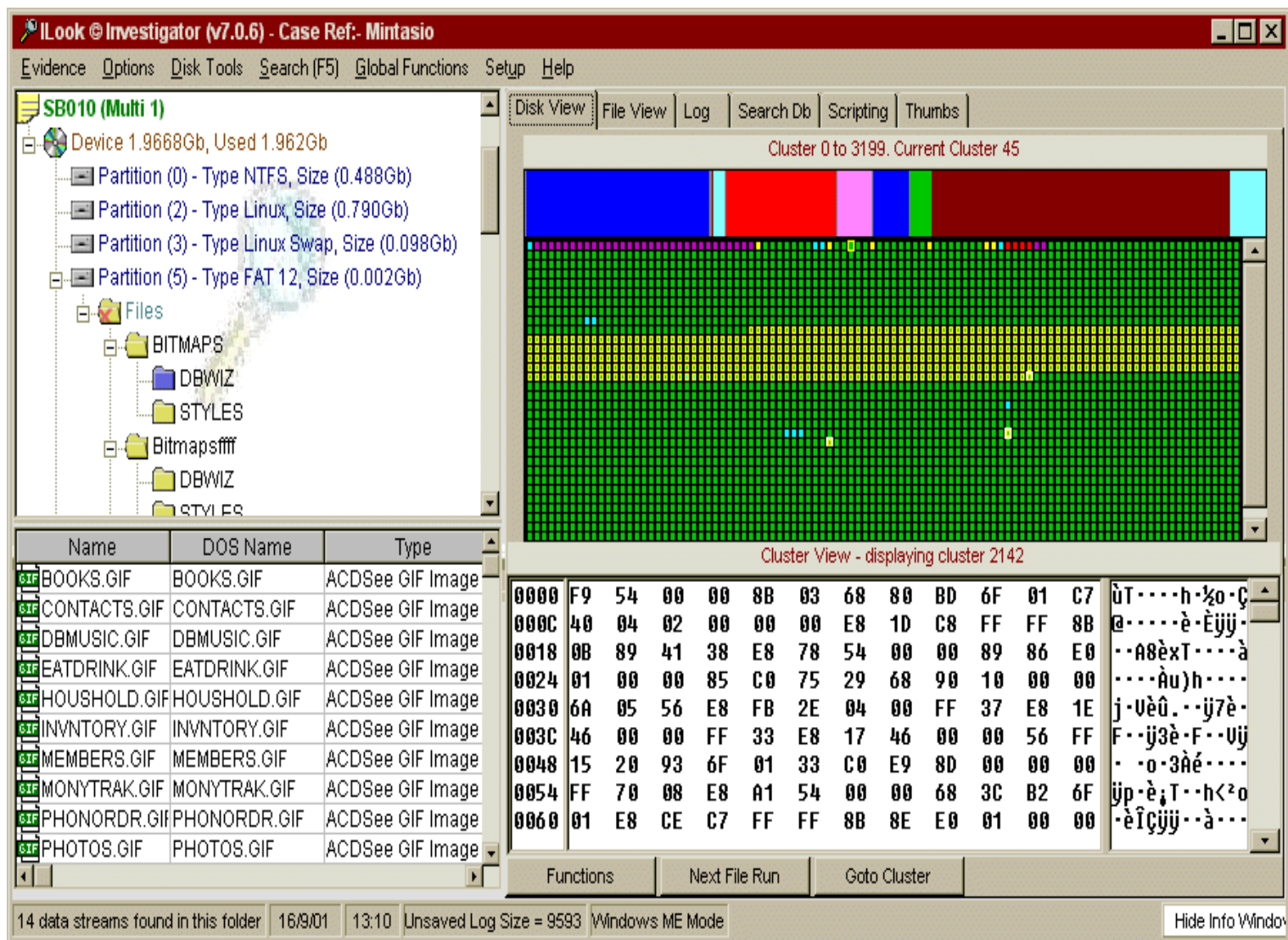
ILook je alat za forenzičku analizu koji pruža mogućnost pretrage i pregleda slike(image) diska koja je uzeta sa zaplenjenog kompjutera. Ima mogućnost pretrage i pregleda sa bilo slike diska koja je uzeta uz pomoć bilo kog sistema za pravljenje slika diska koji pravi bit niz ili bit sliku(bit po bit 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:

6. 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
 - SCO Sys V EAFS
 - SCO Sys V HTFS
 - CDFS
7. Novell Netware NWFS
8. Izgled ekrana je kao Explorer tako da istražitelju pruža mogućnost pregleda i navigacije po fajl sistemu kao što se originalno pojavljuje na kompjuteru osumnjičenog.
9. Granularne extraction facilities pomoću kojih možemo da izdvojimo sve ili deo fajl sistema iz slike diska koja se pregleda.
10. Tri ugrađena moda pretrage (standardni, bulk pretraga and indeksirana pretraga).
11. Autonomna pretraga i indexirajući agenti.
12. Ugrađeni jednostavan textifier.
13. defined viewer Link points to investigator technology.
14. Ugrađena mogućnost gledanja multi-format fajla
15. Podrška za duga imena fajlova
16. Automatizovano procesiranje velikog broja slika i ekstrakcija
17. List generatori Šifara i fraza za šifre.
18. Ugrađeni hex editor sa mogućnostima pretrage.
19. Mogućnosti spasavanja izbrisanih ili oštećenih fajlova.

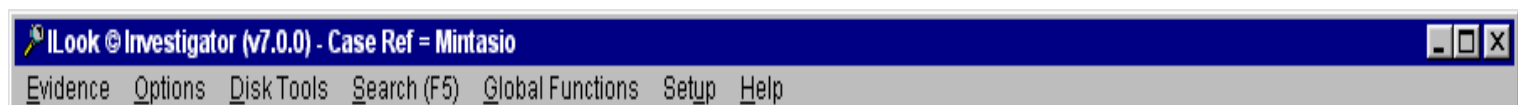
20. Rutine za verifikaciju potpisa fajlova
21. Oporavak Orphaned FAT direktorijuma.
22. Podrška za CRC32, MD5 and SHA1 hash analizu.
23. CRC32, MD5 and SHA1 generatri za sliku (image data) i disk(disk data).
24. Mogućnosti obeležavanja fajlova i pravljenje izveštaja.
25. Mogućnost rukovanja dokazima i mogućnost rukovanja dokazima koje se sastoje iz više slika ili diskova.
26. Alati za rekonstrukciju internet keš-a i mailbox-a (rekonstrukcija i priloga pisama (attachment reconstruction) i pravljenje izveštaja).
27. Alati za vađenje UUE and Base64 attachment-a.
28. Mogućnost direktne istrage na uređajima.
29. Alati koji iz BIOS-a uzimaju sliku diska sa funkcijama MD5 / SHA1 verifikacije i kompresije slike (image).
30. Funkcije filtriranja fajlova i eliminacije istih.
31. Mogućnosti Globalne pretrage između pojedinačnih dokaza.
32. Rezultati pretrage se smeštaju u bazu podataka u odnosu na bilo koju pretragu i bilo koji pojedinačni dokaz.
33. Bitmap slika diska daje detaljan uvid u fizički izgled bilo kojeg selektovanog diska
34. Sveobuhvatni skript jezik, kompajler i runtime engine.
35. Kategorizacija fajlova preko virtuelnih foldera.
36. Ugrađeni thumbnail pretraživač.

5.1. Izgled ILook ekrana



Slika 9. Izgled Ilook ekrana

Glavni meni



Slika 10. 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

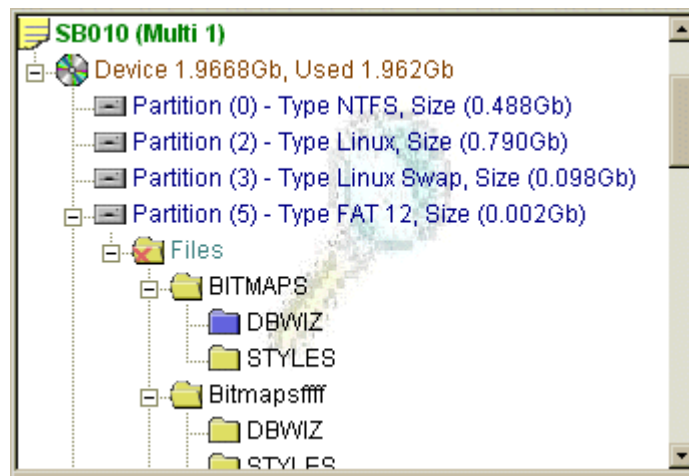
Disk oruđa (Disk Tools) - forenzičke funkcije koje možete koristiti na fajlovima koji se nalaze na diskovima vašeg PC-a ili šerovanim mrežnim folderima.

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

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

Pomoć (Help)

5.2.Prozor dokaza (Evidence Window)



Slika 11. 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:

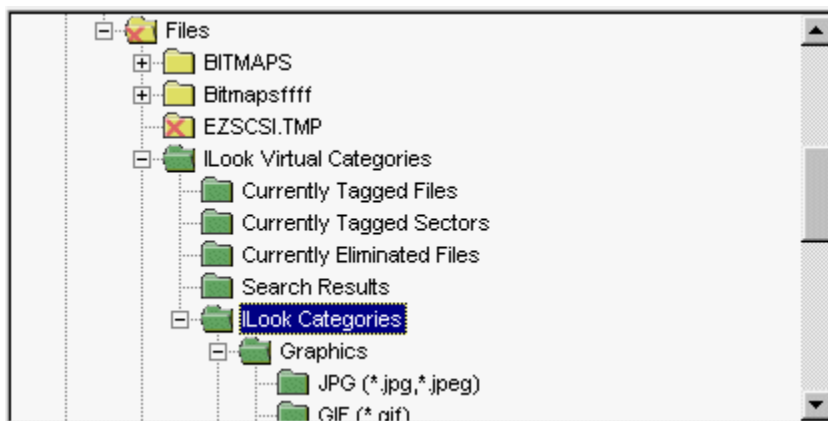
Evidence Item (Dokazna stavka(naziv I broj ukoliko se sastoji iz više njih))

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.

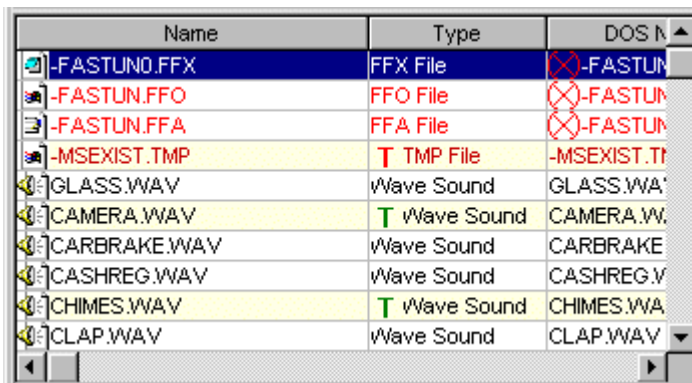


Slika 12. Virtualni folderi

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.

7. **Trenutno eliminisani fajlovi (Currently Eliminated Files)** - lista svih fajlova koji su eliminisani iz selektovane particije, objekti se mogu izbaciti iz liste nazad
8. **Trenutno označeni fajlovi (Currently Tagged Files)** - lista svih fajlova iz selektovane particije
9. **Lista svih označenih sektora (Currently Tagged Sectors)** - lista svih označenih nizova sektora za selektovanu dokaznu stavku.
10. **Izbrisani fajlovi (Undeleted Files)** – lista svih izbrisanih fajlova za selektovanu particiju (fajlovi koje je Ilook povratio iz izbrisanih fajlova).
11. **Ilook Kategorije (Ilook Categories)** – koje nam omogućavaju kategorizaciju i brzi pristup fajlovima iz mapiranog fajl sistema i čija se imena podudaraju sa određenom specifikacijom fajlova. Možemo sami postaviti svoje kategorije desnim klikom na virtuelni folder I izborom odgovarajuće funkcije iz menija. Kada postavimo kategoriju, klikom na kategoriju izlistać se svi fajlovi mapiranog fajl sistema koji se podudaraju sa specifikacijom kategorije fajla.
12. **Kategorije korisnika (User Categories)** – koje nam omogućavaju kategorizaciju fajlova kako mi želimo. Možemo sami postaviti svoje kategorije desnim klikom na virtuelni folder "User Categories", zatim upišemo ime kategorije. Možemo dodeliti bilo koji fajl ovoj grupi tako što ga prvo selektujemo iz liste fajlova, zatim desnim klikom selektujemo odgovarajuću kategoriju na rezultirajućem meniju – fajlovi će biti dodeljeni kategoriji i moći će ih videti tako što izaberete virtuelni folder (fajlovi nisu pomereni sa originalne pozicije). Koristite ove virtuelne foldere kao skladišta za fajlove koje želite da sakupite na jednom mestu. Možemo imati neograničen broj kategorija.
13. **Rezultati pretrage (Search Results)** – sadrži sve pretrage koje su vršene nad fajlovima u odnosu na mapiranu particiju.

5.3.Prozor fajlova: (FileWindow)



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

Slika 13. Prozor fajlova

Prozor fajlova (FileWindow) prikazuje fajlove koji se nalaze u bilo kom folderu selektovanom u Proзору Dokaza (EvidenceWindow - slika gore). 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):

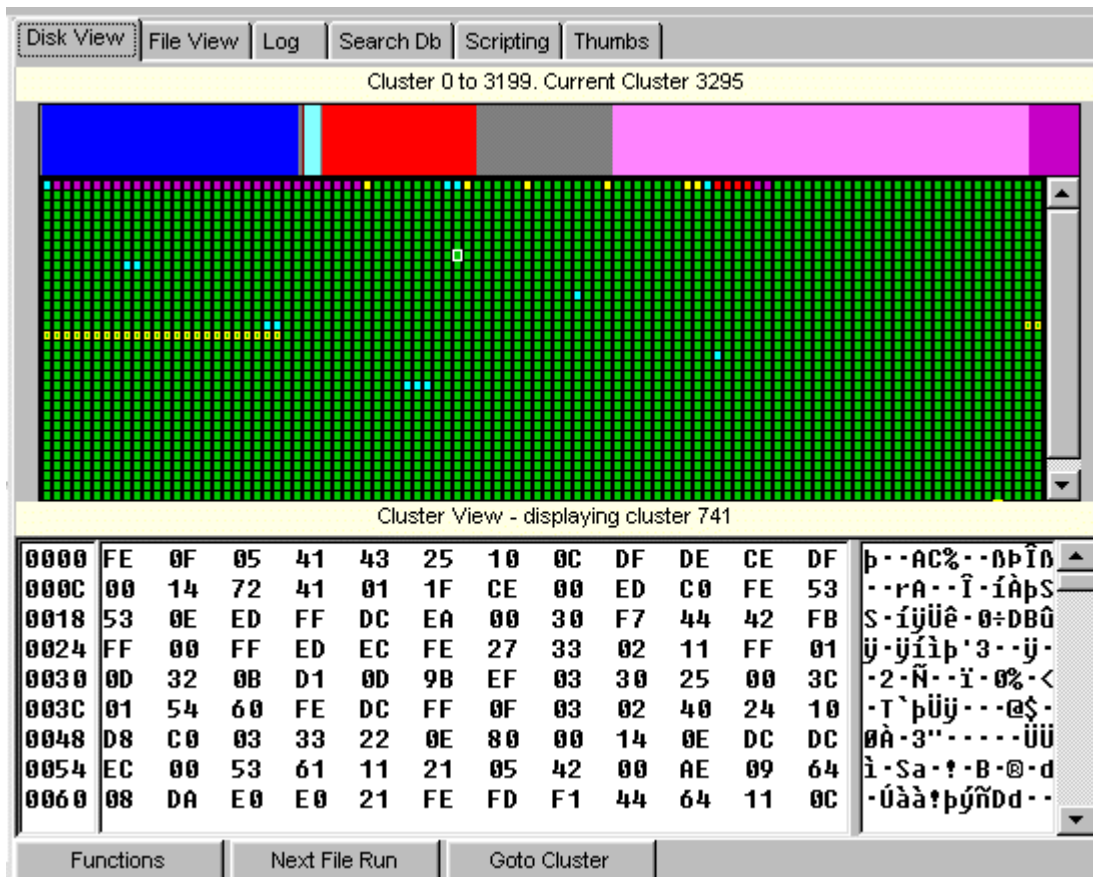
Normalni fajlovi (Normal files) - crni tekst na beloj pozadini

Izbrisani fajlovi (Undeleted files) – crveni tekst na beloj pozadini

Označeni fajlovi (Tagged files) – žuta pozadina (sa zelenim slovom "T" u drugoj koloni za označene noramlne 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 ostaj prema poslednjem redosledu kad god se Ilook ponovo upali. Možemo i sakriti određene kolone ukoliko nam smetaju. To se radi iz Ilook setup-a.

5.4.Prozor Informacija (InfoWindow)



Slika 14. 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.

Kartice:

Pregled diska (Disk View)

Pregled fajla (File View)

Dnevnik (Log)

Pretraga baze podataka (SearchDb)

Skripte (Scripting)

Thumb fajlovi (Thumbs)

5.5.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

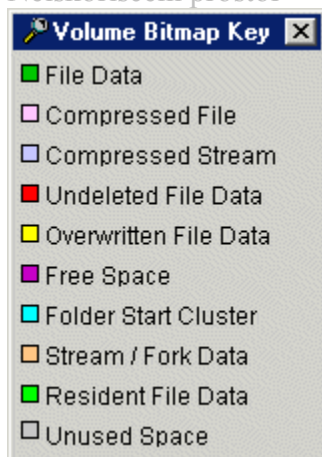
Slobodan prostor

Klaster u kojem počinje folder

Niz podataka

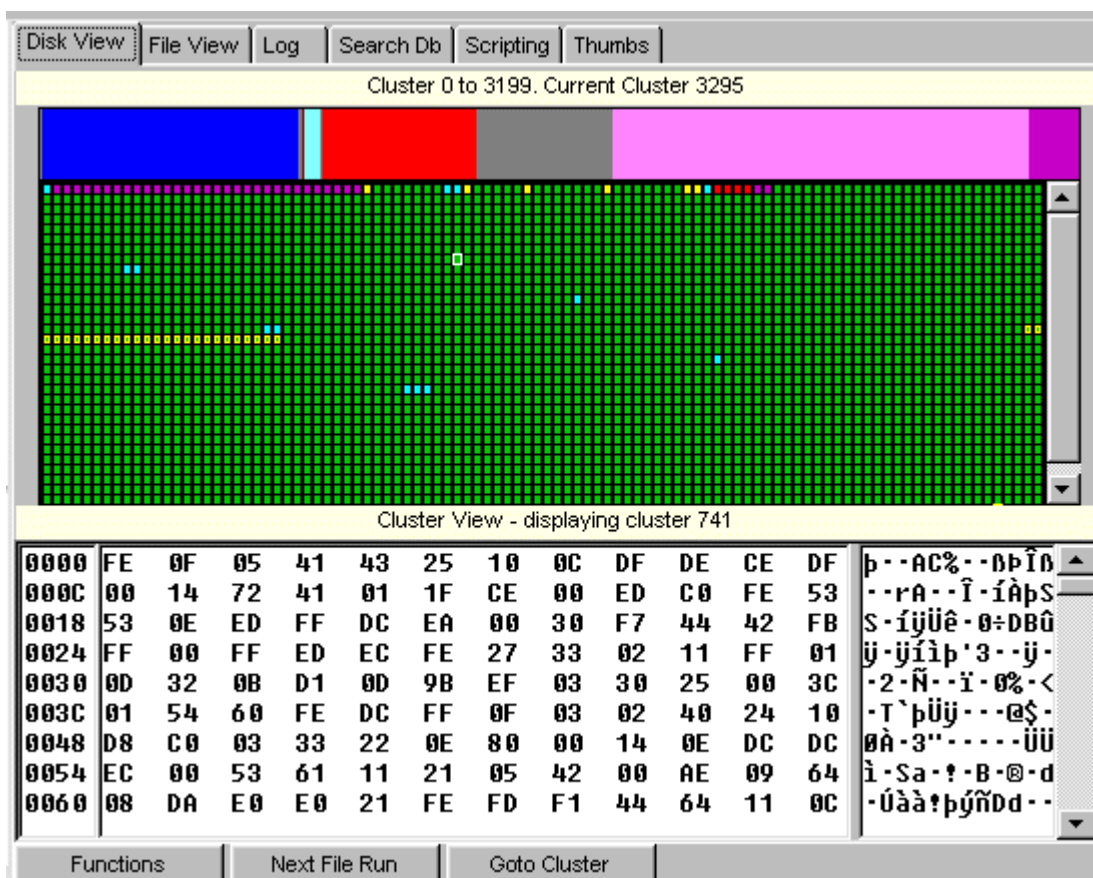
Podaci residentnog fajla

Neiskorišćeni prostor



Slika 15. Legenda

Kada selektujete bilo koji klaster sa mišem (ili korišćenjem navigacijskih dugmića na tastaturi) selektovani klaster će biti učitao 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).

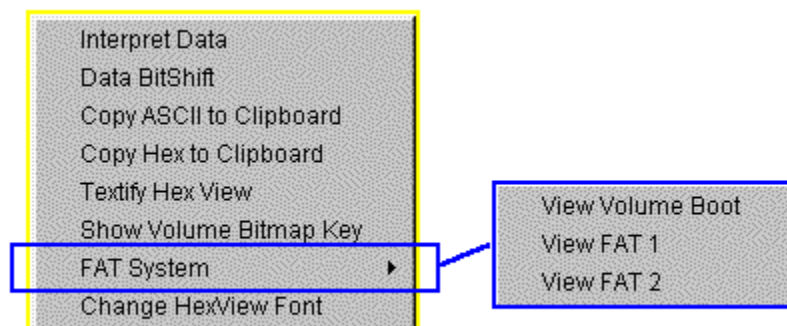


Slika 16. Pregled diska

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 17. Funkcije pregleda diska

Funkcije :

Interpretiranje podataka (Interpret Data) – Interpretiranje podataka za trenutno selektovane bajtove na prozoru klastera kroz različite vremenske formate. Može biti korisno za interpretiranje podataka koji su otkaćeni iz strukture fajlova sistema.

Pomeranje bitova podataka (Data BitShift) – Pomeranje svih podataka u hexadecimalnom zapisu udesno za N bita (N se može definisati između 1 i 7). all data in the hex view right by N bit (ILook will right pad). N is a user definable value in the range of 1 to 7.

Kopiranje ASCII na klipbord (Copy ASCII to Clipboard) – Kopiranje trenutnog ASCII sadržaja koji se nalazi u klaster prozoru na klipbord.

Kopiranje heksadecimalnih vrednosti na klipbord (Copy Hex to Clipboard) -

Kopiranje trenutnog Hex sadržaja koji se nalazi u klaster prozoru na klipbord.

Tekstuelizacija heksadecimalnog pregleda (Textify Hex View) – Izbacuje karaktere koji nisu čitljivi iz klastera i ostavlja normalan tekst, pomaže pri čitanju.

Legenda za sektore (Show Volume Bitmap Key) – Prikazuje šta koja boja klastera predstavlja.

Fat sistem (Fat System) – Pojavljuje se samo kada se selektuju FAT particije. Pruža nam mogućnost pregleda boot sektora FAT particije i FAT tabele .

Promena fonta u heksadecimalnom prozoru (Change HexView Font) – Prolazi kroz klaster sa nizom različitih fontova, možemo da izaberemo onj koji nam najviše odgovara..

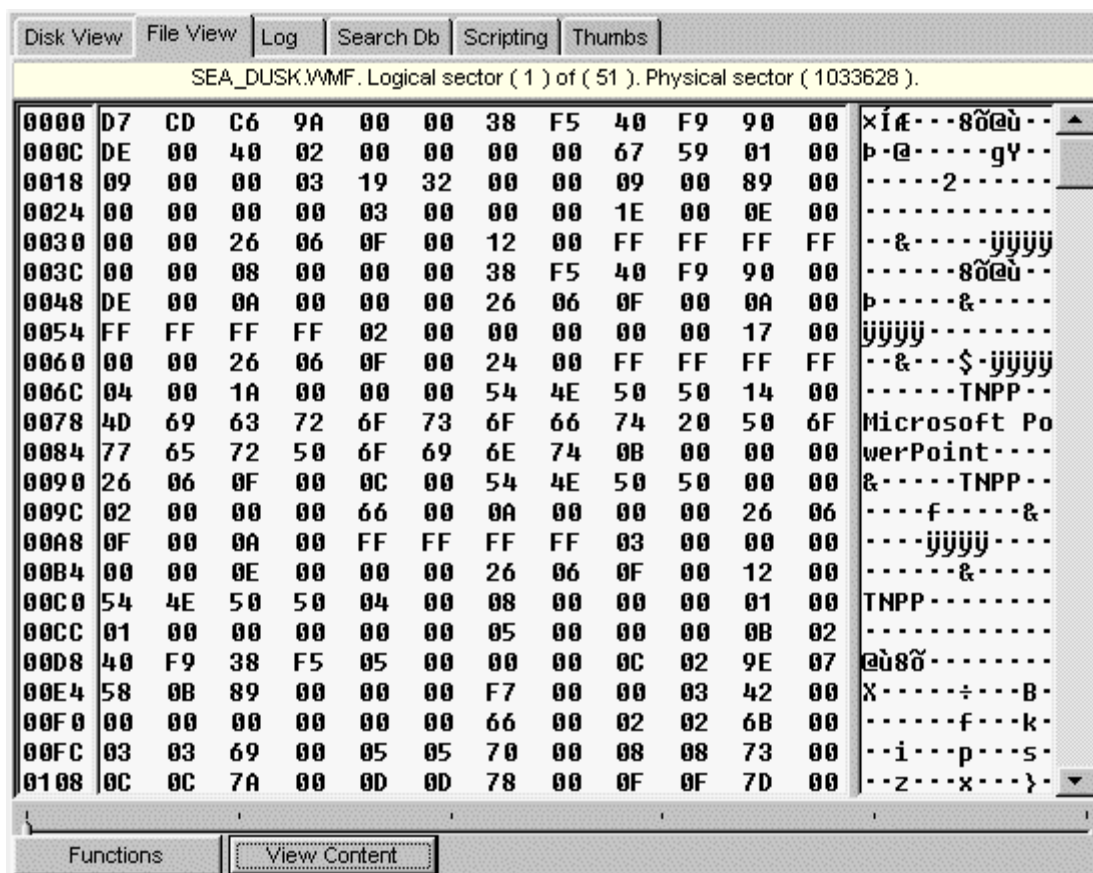
Dugme idi na klaster (The Goto Cluster button): locira bilo koji klaster koji ste upisali i selektuje ga u prozoru pregleda particije i automatski ga učitava u prozor za pregledanje klastera.

5.6. Pregled Fajla (File View)

Prozor za pregled fajla je multifunkcijski prikaz bilo kog fajla selektovanog u **Prozoru 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.

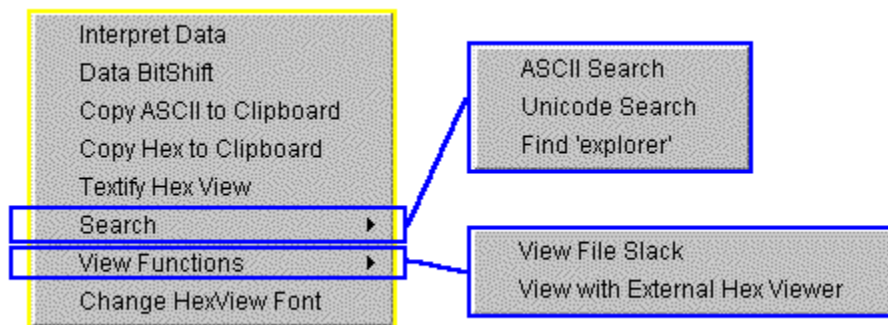
Heksadecimalni prikaz (Hex View)

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 18. Pregled fajla

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



Slika 19. Prozor dokaza

Funkcije:

Interpretiranje podataka (Interpret Data) – Interpretiranje podataka za trenutno selektovane bajtove na prozoru klastera kroz različite vremenske formate. Može biti korisno za interpretiranje podataka koji su otkaćeni iz strukture fajlova sistema.

Pomeranje bitova podataka (Data BitShift) - Pomeranje svih podataka u hexadecimalnom zapisu udesno za N bita (N se može definisati između 1 i 7). all data in the hex view right by N bit (ILook will right pad). N is a user definable value in the range of 1 to 7.

Kopiranje ASCII na klipbord (Copy ASCII to Clipboard) - Kopiranje trenutnog ASCII sadržaja koji se nalazi u klaster prozoru na klipbord.

Kopiranje Hex na klipbord (Copy Hex to Clipboard) - Kopiranje trenutnog Hex sadržaja koji se nalazi u klaster prozoru na klipbord.

Tekstuelizacija heksadecimalnog pregleda (Textify Hex View) - Izbacuje karaktere koji nisu čitljivi iz klastera i ostavlja normalan tekst, pomaže pri čitanju.

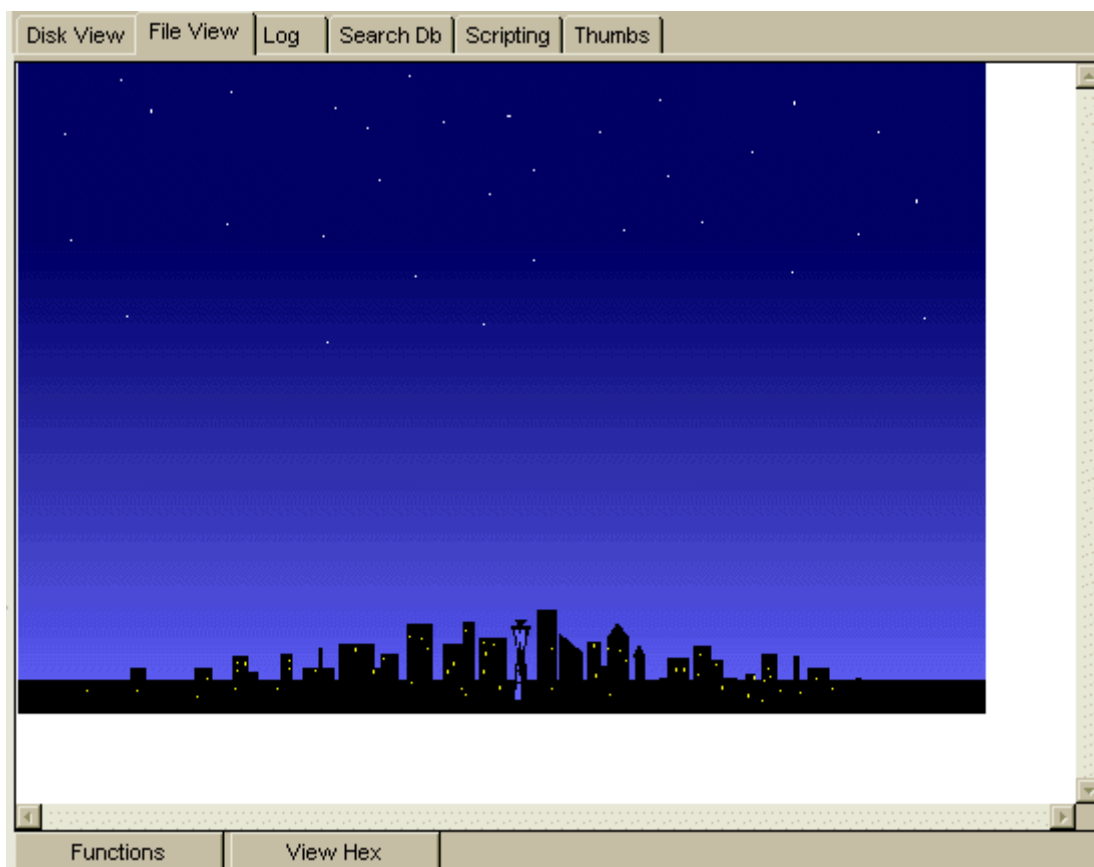
Pretraga (Search) – Omogućava pretragu klastera koje zauzima fajl u odnosu na bilo koje ASCII ili Unicode niz karaktera. Svi pogodci se obeležavaju automatski u heksadecimalnom pregledu fajla (sa F3 se pronalazi sledeći pogodak). Ukoliko smo prethodno obavili standardnu pretragu, rezultati pretrage koju sad obavljamo će biti pridodata već prethodno pokrenutoj standardnoj pretrazi kao dodatni objekat.

Funkcije pregleda (View Functions) – Ove dve funkcije nam omogućavaju pregled “file slack” selektovanog fajla i ekstrakovanje podataka fajla kao i pregledanje istih u nekom od spoljnih heksadecimalnih pregledača.

Promena fonta u heksadecimalnom prozoru (Change HexView Font) – Prolazi kroz klaster sa nizom različitih fontova, možemo da izaberemo onj koji nam najviše odgovara.

Pregled Sadržaja (Content View)

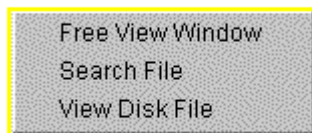
Pregled sadržaja je interpretacija sadržaja fajla bairana na potpisu fajla, ukoliko je podržan pregled fajla biće prikazan ovde. Iz ovog pogleda možete odštampati fajl.



Slika 20. Pregled sadržaja

5.7.Funkcije pregleda sadržaja

Funkcije pregleda sadržaja se koriste preko dugmeta "Functions".



Slika 21. Funkcije pregleda sadržaja

Funkcije:

Pregled u novom prozoru (Free View Window) - Ova funkcija izbacuje sadržaj fajla u novi prozor, radi lakšeg pregledanja istog.

Pretraga (Search) - Omogućava pretragu fajla u odnosu na zadati niz karaktera. Svi pogodci se obeležavaju automatski u heksadecimlnom pregledu fajla (sa F3 se pronalazi sledeći pogodak).

Pregled fajla sa diska (View Disk File) - Ova funkcija nam daje mogućnost učitavanja bilo kog fajla sa bilo kog diska u Ilook radi pregleda sadržaja tog fajla.

Formati fajlova koje je moguće pregledati pomoću Ilook-a:

Tekstualni i grafički formati fajlova:

ANSI Text (7 i 8 bita) Sve verzije
ASCII Text (7 & 8 bita veerzije) Sve verzije
Adobe FrameMaker (MIF) Verzija do 6
Corel WordPerfect for Windows Verzije do 2002
DEC WPS Plus (DX) Verzije do 4.0
DEC WPS Plus (WPL) Verzije do 4.1
DisplayWrite 2 & 3 (TXT) Sve verzije
DisplayWrite 4 & 5 Verzije do 2.0
Enable Verzije 3.0, 4.0 i 4.5
First Choice Verzije do 3.0
Framework Verzija 3.0
HTML Verzije do 3.0
IBM FFT Sve verzije
IBM Revisable Form Text Sve verzije
IBM Writing Assistant Verzija 1.01

JustWrite Verzije do 3.0
Legacy Verzije do 1.1
Lotus AMI/AMI Professional Verzije do 3.1
Lotus Manuscript Verzije do 2.0
Lotus WordPro (Win32 platforms) SmartSuite 96, 97 and Millennium
Lotus WordPro (Non-Windows platforms – samo tekst)
SmartSuite 97 and Millennium edition
MacWrite II Verzije 1.1
MASS11 Verzije do 8.0
Microsoft Rich Text Format (RTF) Sve verzije
Microsoft Word for DOS Verzije do 6.0
Microsoft Word for Macintosh Verzije od 4.0 do 98
Microsoft Word for Windows Verzije do 2002
Microsoft WordPad Sve verzije
Microsoft Works for DOS Verzije do 2.0
Microsoft Works for Macintosh Verzije do 2.0
Microsoft Works for Windows Verzije do 4.0
Microsoft Write Verzije do 3.0
MultiMate Verzije do 4.0
Navy DIF Sve verzije
Nota Bene Verzija 3.0
Novell Perfect Works Verzija 2.0
Novell WordPerfect for DOS Verzije do 6.1
Novell WordPerfect for Mac Verzije 1.02 do 3.0
Novell WordPerfect for Windows Verzije do 7.0
Office Writer Verzija 4.0 to 6.0
PC-File Letter Verzije do 5.0
PC-File+ Letter Verzije do 3.0
PFS:Write Verzije A, B, and C
Professional Write for DOS Verzije do 2.1
Q&A for DOS Verzija 2.0
Professional Write Plus Verzija 1.0
Q&A Write for Windows Verzija 3.0
Samna Word Verzije do Samna Word IV+
SmartWare II Verzija 1.02
Sprint Verzija 1.0
StarOffice Writer (UNIX and Windows) Verzija 5.2
Total Word Verzija 1.2
Unicode Text Sve verzije
Volkswriter 3 & 4 Verzije do 1.0
Wang PC (IWP) Verzije do 2.6
WordMARC Verzije do Composer Plus
WordStar 2000 for DOS Verzije do 3.0
WordStar for DOS Verzije do 7.0
WordStar for Windows Verzija 1.0
XyWrite Verzije do III Plus

Grafički formati fajlova:

Binary Group 3 Fax Sve verzije
 BMP (including RLE, ICO, CUR & OS/2 DIB) Windows
 CDR (if TIFF image is embedded in it) Corel Draw versions 2.0 - 9.0
 CGM - Computer Graphics Metafile ANSI, CALS, NIST, Verzija 3.0
 CMX - Corel Clip Art Format Verzije 5 do 6
 DCX (multi-page PCX) Microsoft Fax
 DRW - Micrografx Designer Verzija 3.1
 DRW - Micrografx Draw Verzije do 4.0
 DXF (Binary and ASCII) AutoCAD Drawing Interchange Format Verzije to 14
 EMF Windows Enhanced Metafile
 EPS Encapsulated PostScript If TIFF image is embedded in it
 FMV - FrameMaker graphics Vector & raster do version 5.0
 FPX - Kodak Flash Pix No specific format
 GDF - IBM Graphics Data Format Verzija 1.0
 GEM - Graphics Environment Manager Metafile Bitmap and Vector
 GIF - Graphics Interchange Format Compuserve
 GP4 - Group 4 CALS Format Type I and Type II
 HPGL - Hewlett Packard Graphics Language Verzija 2.0
 IMG - GEM Paint nema specifičnu verziju
 JFIF (JPEG not in TIFF format) Sve verzije
 JPEG – Joint Photographic Experts Group format Sve verzije
 MET - OS/2 PM Metafile Verzija 3.0
 PBM - Portable Bitmap nema specifičnu verziju
 PCD - Kodak Photo CD Verzija 1.0
 PCX Bitmap PC Paintbrush
 Perfect Works (Draw) Novell version 2.0
 PGM - Portable Graymap nema specifičnu verziju
 PIC – Lotus 1-2-3 Picture File Format nema specifičnu verziju
 PICT1 & PICT2 (Raster) Macintosh Standard
 PIF - IBM Picture Interchange Format Verzija 1.0
 PNG - Portable Network Graphics Internet Format Verzija 1.0
 PNTG MacPaint
 PPM - Portable Pixmap nema specifičnu verziju
 Progressive JPEG nema specifičnu verziju
 PSP - Paintshop Pro (Win32 only) Verzije 5.0, 5.0.1
 RND - AutoShade Rendering File Format Verzija 2.0
 SDW Ami Draw
 Snapshot (Lotus) Sve verzije
 SRS - Sun Raster File Format nema specifičnu verziju
 Targa Truevision
 TIFF Verzije do 6
 TIFF CCITT Group 3 & 4 Fax Systems
 VISO Visio 4 (page preview only), 5, 2000 and 2002
 WBMP nema specifičnu verziju
 WMF Windows Metafile
 WordPerfect Graphics [WPG and WPG2] Verzije do 2.0
 XBM - X-Windows Bitmap x10 compatible

XPM - X-Windows Pixmap x10 compatible
XWD - X-Windows Dump x10 compatible

Tabelarni fajlovi:

Enable verzije 3.0, 4.0 i 4.5
First Choice verzije preko 3,0
Okvirni Verzija 3.0
Lotus 1-2-3 (DOS i Windows) verzije do 5,0
Lotus 1-2-3 za SmartSuite SmartSuite 97and Millenium
Lotus 1-2-3 Charts (DOS i Windows) verzije do 5,0
Lotus 1-2-3 (OS / 2) verzije do 2,0
Lotus 1-2-3 Charts (OS / 2) verzije do 2,0
Lotus Symphony verzije 1.0,1.1 i 2.0
Microsoft Excel za Macintosh verzije 3.0 do 4.0, 98
Microsoft Excel za Windows verzije 2,2 do 2002
Microsoft Excel Charts verzije 2.x preko 7,0
Microsoft Multiplan Verzija 4.0
Microsoft Windows Works verzije do 4,0
Microsoft Works (DOS) verzije do 2,0
Microsoft Works (Macintosh) verzije do 2,0
Mozaik Twin Verzija 2.5
Novell Perfect Works Verzija 2.0
QuattroPro za DOS verzije preko 5,0
QuattroPro za Windows verzije do 2002
PFS: Profesionalni plan Verzija 1.0
SuperCalc 5 Verzija 4.0
SmartWare II Version 1,02
VP Planer 3D Verzija 1.0

“High-End” grafički formati:

AI - Adobe Illustrator Format datoteke verzije preko 7,0
CDR - Corel Draw verzije preko 8,0
DSF - Micrografx Dizajner Windows 95, verzija 6.0
DWG - AutoCAD za crtanje formata verzije 12 do 14
AutoCAD – verzije do 5.1
PDF - Portable Document Format Acrobat verzije 2.1, 3.0, 4.0 i 5.0
PS - Postscript Level 2
PSD - Adobe Photoshop File Format Verzija 4.0

Baze podataka:

Access verzije do 2,0
dBASE verzije do 5,0
DataEase verzija 4.x
DBXL Verzija 1.3
Enable verzije 3.0, 4.0 i 4.5

First Choice verzije preko 3,0
FoxBase Verzija 2.1
Okvirni Verzija 3.0
Microsoft Windows Works verzije preko 4,0
Microsoft Works (DOS) verzije do 2,0
Microsoft Works (Macintosh) kroz 2 verzije. 0
Paradoks (DOS) verzije do 4,0
Paradoks (Windows) verzije do 1,0
Osobni R: BAZA Verzija 1.0
R: 5000 BASE verzije preko 3,1
R: BASE System V Verzija 1.0
Reflex Verzija 2.0
Q & verzije do 2,0
SmartWare II Version 1,02

Programi za pravljenje prezentacija:

Corel Prezentacije verzije 8,0, 9,0 i 2002
Prezentacije Novell verzije 3,0 i 7,0
Harvard Graphics za DOS verzije 2.x & 3.x
Harvard Graphics verzije sustava Windows
Freelance za Windowse 1.0, 2.0, 96, 97, Millenium
Freelance za OS / 2 verzije preko 2,0
Microsoft PowerPoint za Windows verzije do 2002
Microsoft PowerPoint za Macintosh verzije 4.0, 98

Kompresovani i kodirani fajlovi:

GZIP Nema posebnih verzija
LZA compress Nema posebnih verzija
LZH compress Nema posebnih verzija
Microsoft Binder Verzija 7.0, Binder 97
MIME (tekst pošte) Nema posebnih verzija
UU Encode Nema posebnih verzija
UNIX copmpress Nema posebnih verzija
UNIX TAR Nema posebnih verzija
ZIP PKWare verzije do 2.04g

Drugi:

Adobe FrameMaker (text only) 6.0
Executable (EXE, DLL) Nema posebnih verzija
Executable for Windows NT Nema posebnih verzija
MSG (text only) Microsoft Outlook Mail format
Microsoft Project (text only) Project 98
vCard Electronic Business Card Versit Verzija 2.1
WML Compatible with WML specification 5.2
JustSystems Ichitaro Versions 5.0, 6.0, 8.0, 9.0 and 10.0

5.8.Dnevnik (Log)

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.



```
Disk View | File View | Log | Search Db | Scripting
11/03/01 16:46:22 (BF8922) MI002I File deconstructor for file (freeserve.help.webspace.dbx) initiated
11/03/01 16:46:25 (BF8922) MI003I File deconstruction for file (freeserve.help.webspace.dbx) complete
11/03/01 16:46:26 (BF8922) MI002I File deconstructor for file (freeserve.help.webspace.dbx) initiated
11/03/01 16:46:26 (BF8922) MI003I File deconstruction for file (freeserve.help.webspace.dbx) completed
11/03/01 16:46:26 (BF8922) MU023I Finished auto deconstruction check
11/03/01 16:46:26 (BF8922) MU025V Object 52 name changed from CGI available?CGI available?(32) to
11/03/01 16:46:27 (BF8922) MU025V Object 180 name changed from Help?Help?(160) to Help_Help_(16
11/03/01 16:46:27 (BF8922) MU025V Object 188 name changed from Help?Re Help?(168) to Help_Re H
11/03/01 16:46:27 (BF8922) MU025V Object 198 name changed from Zip Files???Zip Files???[178] to Zi
11/03/01 16:46:27 (BF8922) MU025V Object 200 name changed from Zip Files???Re Zip Files???[180] t
11/03/01 16:46:27 (BF8922) MU025V Object 226 name changed from Frontpage, ne1??Frontpage, ne1??
11/03/01 16:46:27 (BF8922) MU025V Object 227 name changed from Frontpage, ne1??Re Frontpage, ne
11/03/01 16:46:28 (BF8922) MU025V Object 298 name changed from Default index page?Re Default ind
11/03/01 16:46:28 (BF8922) MU025V Object 364 name changed from Zip Files???Re Zip Files???[344] t
11/03/01 16:46:28 (BF8922) MU025V Object 442 name changed from How can I lease/buy an IP How can
11/03/01 16:46:29 (BF8922) MU025V Object 453 name changed from How can I lease/buy an IPRe How
11/03/01 16:46:29 (BF8922) MU025V Object 467 name changed from DNS names????Re DNS names???
11/03/01 16:46:30 (BF8922) MU021I Checking for duplicate file names, this may take a few minutes ...
11/03/01 16:46:30 (BF8922) MU023I Finished checking for duplicate file names
11/03/01 16:46:30 (BF8922) MU008I Building the filesystem meta data, please wait ...
11/03/01 16:46:30 (BF8922) MU009I Initialised file system driver
11/03/01 16:46:30 (BF8922) MF005I Finished FileSystem mapping for partition (0)
11/03/01 16:46:30 (BF8922) MF006I Processed - 490 objects (total)
11/03/01 16:46:30 (BF8922) MU001I Calculating partition free space, this may take some time ...
11/03/01 16:46:31 (BF8922) MU003I Finished calculating partition free space
11/03/01 16:46:34 (BF38820) MP019I Starting Partition Traverse
11/03/01 16:46:34 (BF38820) MP020I Image file - E:\images\deconstruct1.000. Size - 798,010
11/03/01 16:46:36 (BF38820) MP021I Reading MBR and master partition table
11/03/01 16:46:36 (BF38820) MP030I Processing boot sector for partition (0)
11/03/01 16:46:36 (BF38820) MF009I Checking FAT integrity for FAT 12 partition (0)
11/03/01 16:46:36 (BF38820) MF010I FAT integrity result on partition (0) - FAT1 = FAT2 = True
11/03/01 16:46:36 (BF38820) MP031I Calculating disk unused space
11/03/01 16:46:37 (BF38820) MP032I Finished calculating disk unused space
11/03/01 16:46:37 (BF38820) MP033I Ending Partition Traverse
11/03/01 16:46:39 (BF38820) FE070I >>>> Textify Free / Unused = Off
11/03/01 16:46:39 (BF38820) FE072I >>>> Extraction Overwrite = Off
11/03/01 16:46:39 (BF38820) FE074I >>>> Fat Ultra Undelete = Off
11/03/01 16:46:39 (BF38820) FE075I >>>> Sector IDs in Sector Dump files = On
11/03/01 16:46:39 (BF38820) FE077I >>>> Force FAT12 map of all floppies = On
11/03/01 16:46:39 (BF38820) MF001I FAT 1 mapping of FAT 12 filesystem on partition (0)
11/03/01 16:46:40 (BF38820) MF004I Mapping status - processed 20 objects. Still indexing
11/03/01 16:46:40 (BF38820) MF004I Mapping status - processed 20 objects. Still indexing
11/03/01 16:46:40 (BF38820) MU121I Started auto deconstruction check, looking for suitable objects
11/03/01 16:46:45 (BF38820) MI002I File deconstructor for file (freeserve.help.webspace.dbx) initiated
11/03/01 16:46:46 (BF38820) MI003I File deconstruction for file (freeserve.help.webspace.dbx) completed
11/03/01 16:46:46 (BF38820) MI002I File deconstructor for file (freeserve.help.webspace.dbx) initiated
11/03/01 16:46:48 (BF38820) MI003I File deconstruction for file (freeserve.help.webspace.dbx) completed
11/03/01 16:46:48 (BF38820) MI002I File deconstructor for file (freeserve.help.webspace.dbx) initiated
11/03/01 16:46:49 (BF38820) MU023I Finished auto deconstruction check
11/03/01 16:46:49 (BF38820) MU025V Object 234 name changed from Requirement 4/12-01[11] to Requi
11/03/01 16:46:49 (BF38820) MU025V Object 241 name changed from Re how's it going?(18) to Re how
11/03/01 16:46:50 (BF38820) MU025V Object 304 name changed from DO YOU KNOW IF YOU ARE BEA
11/03/01 16:46:50 (BF38820) MU025V Object 309 name changed from Fancy a Flutter ? Here's a Tip !!(8
11/03/01 16:46:50 (BF38820) MU025V Object 318 name changed from How can I read the contents name
```

Slika 22. Dnevnik (Log)

Tekst koji se nalazi u Dnevniku je ispisano 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
 - 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 bazu podataka pretraga. Bazu 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.

Disk View	File View	Log	Search Db	Scripting	Thumbs
Search Tag	Date	Search Terms	Searched What ?	Hits	
Sdb-Record	11/03/01 19:28:40	applause <OR> explor <OR> db*	Bulk search of free sectors. Item (MP 100	6	
Trial1	11/03/01 19:28:12	applause <OR> explor <OR> db*	Bulk search of file data. Item (MP 1001a2)	53	
Trial1	11/03/01 19:27:30	explorer	Interactive search of free sectors. Item (M	0	
Sdb-Record	11/03/01 19:27:06	explorer	Interactive search of file data. Item (MP 10	2	
Sdb-Record	11/03/01 19:26:03	db8	Interactive search of unused sectors. Item	0	
Trial2	11/03/01 19:26:01	db8	Interactive search of free sectors. Item (M	0	
Sdb-Record	11/03/01 19:25:34	db8	Interactive search of file data. Item (MP 10	0	

Slika 23. Baza podataka rezultata pretrage

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)** – Ova funkcija nam omogućava da dodamo komentar izabranom rezultatu pretrage.
- **Izveštaj istorije pretrage (Search History Report)** – Ova funkcija služi za prevljenje izveštaja u HTML formatu sa detaljima pretrage za trenutno izabrani dokazni objekat.
- **Pregled rezultata pretrage (View Search Results)** – Ova funkcija prikuplja pogotke pretrage za pretragu koja je selktovana na ekranu rezultata pretrage. Pogotci pretrage se snimaju tokom inicijalne pretrage, tako da ukoliko želimo da vidimo rezultate te pretrage program ne mora opet da pretražuje sliku ili disk.
- **Restartovanje pretrage (Restart Search)** – Ova funkcija je na raspolaganju ukoliko imamo standardne pretrage koje su prekinute. Ova funkcija se koristi da bi se restartovala selektovana pretraga, a pretraga počinje od mesta gde je zaustavljena.
- **Ponovo pokretanje pretrage kao Bulk pretragu (Rerun search as Bulk Search)** – Ova funkcija šalje selektovani set rezultata pretrage kroz “bulk search engine” tako da se rezultati mogu predstaviti preko izveštaja, baze podataka ili CSV fajla u zavisnosti od poslednjeg podešavanja pretrage bulk-a (bulk search settings). Ovo je dobar meto za formatiranje rezultata pretrage radi dalje obrade podataka ili neke probne prezentacije.



Slika 24. funkcije nad bazom rezultata pretrage

5.9. Korišćenje skripti u Ilook-u za automatizaciju, izveštavanje i procesiranje podataka.

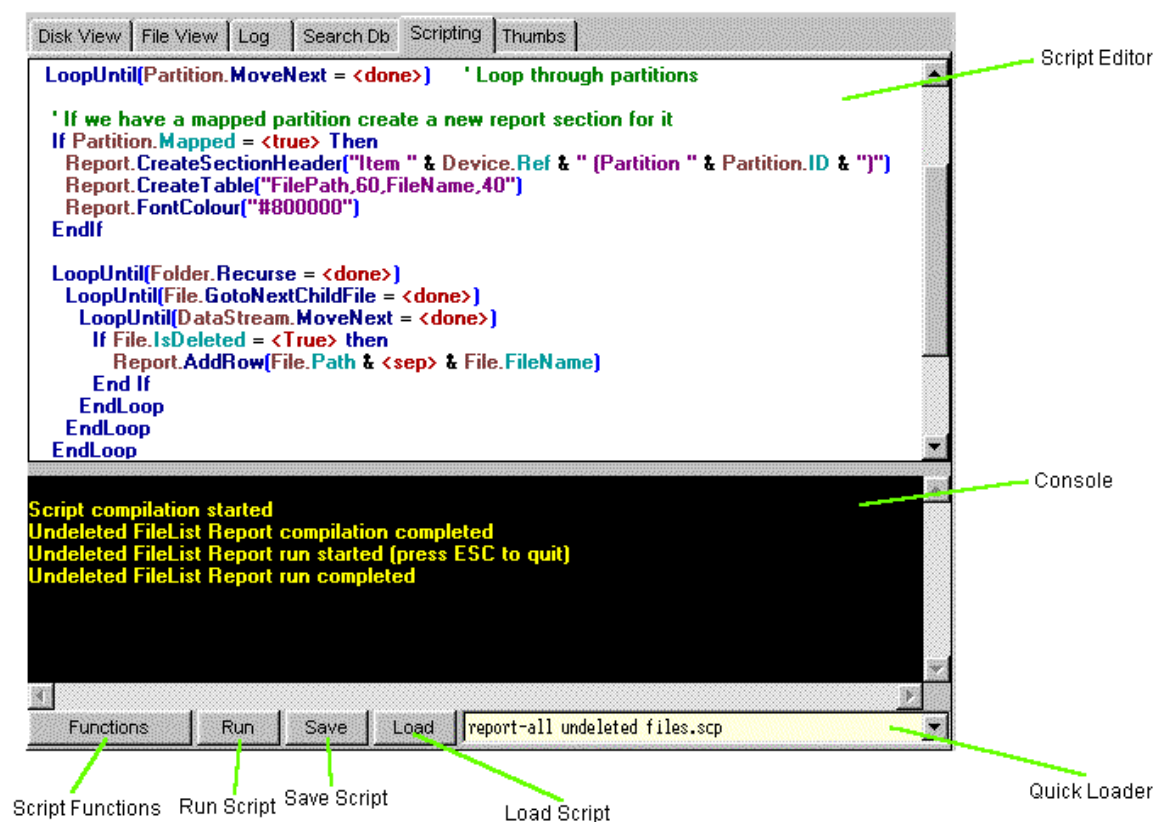
Ilook-ov skript jezik je dizajniran kao alatka koja se lako koristi a koja ima veoma moćne funkcije.

Ilook-ove skripte pružaju mogućnost:

- Automatizacije postupaka koji se ponavljaju
- Procesuiranja podataka na različite i nove načine.
- Pravljenja izveštaja i analiza podataka

Skript jezike je baziran na programskom jeziku "BASIC" samo što je pojednostavljen. Ilook ima u sebi set skripti koje možete menjati po svojoj potrebi.

Pregled



Slika 25. Prozor skripti

Skript prozor za promenu sadržaja skripte (Script Editor) – U ovom prozoru kreirate ili prikazujete vaše skripte. Ilook ispisuje kod u različitim bojama tako da lakše možete da razlikujete objekte, metode, funkcije itd. Ilook takođe obeležava linije koda koje sadrže greške kada pokušate da kompajlirate ili pokrenete skriptu.

Konzola (Console) – Skript "engine" šalje poruke o statusu u ovaj prozor.

Skript funkcije (Script Functions) – Detaljnije u nastavku.

Pokreni skriptu (Run Script) – Pokreće trenutno učitano skriptu, prethodno je kompajlira ukoliko je potrebno.

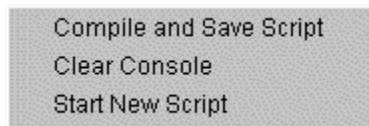
Snimi skriptu (Save Script) - Snima skriptu na disk.

Učitaj skriptu (Load Script) – Učitava novu ili kompajliranu skriptu.

Brzo učitavanje (Quick Loader) – Izlistava sve skripte i kompajlirane skripte koje se nalaze u trenutnom folderu za skripte. Selektovanjem skripte iz padajuće liste automatski učitavate skriptu.

Skripte imaju ".scp" ekstenziju, a kompajlirane skripte imaju ".cx" ekstenziju. Pokretanje skripte se vrši na dugme "Run Script", ukoliko skripta nije kompajlirana Ilook će je u ovom koraku kompajlirati pre nego što je pokrene. Poruke o greškama ukoliko ih postoje biće prikazane u prozoru konzole. Pre izlaska iz program Ilook vas pita da snimate sve nesnimljene promene na skriptama.

Funkcije skripti (Script InfoWindow Functions)



Slika 26. Pfunkcije skripti

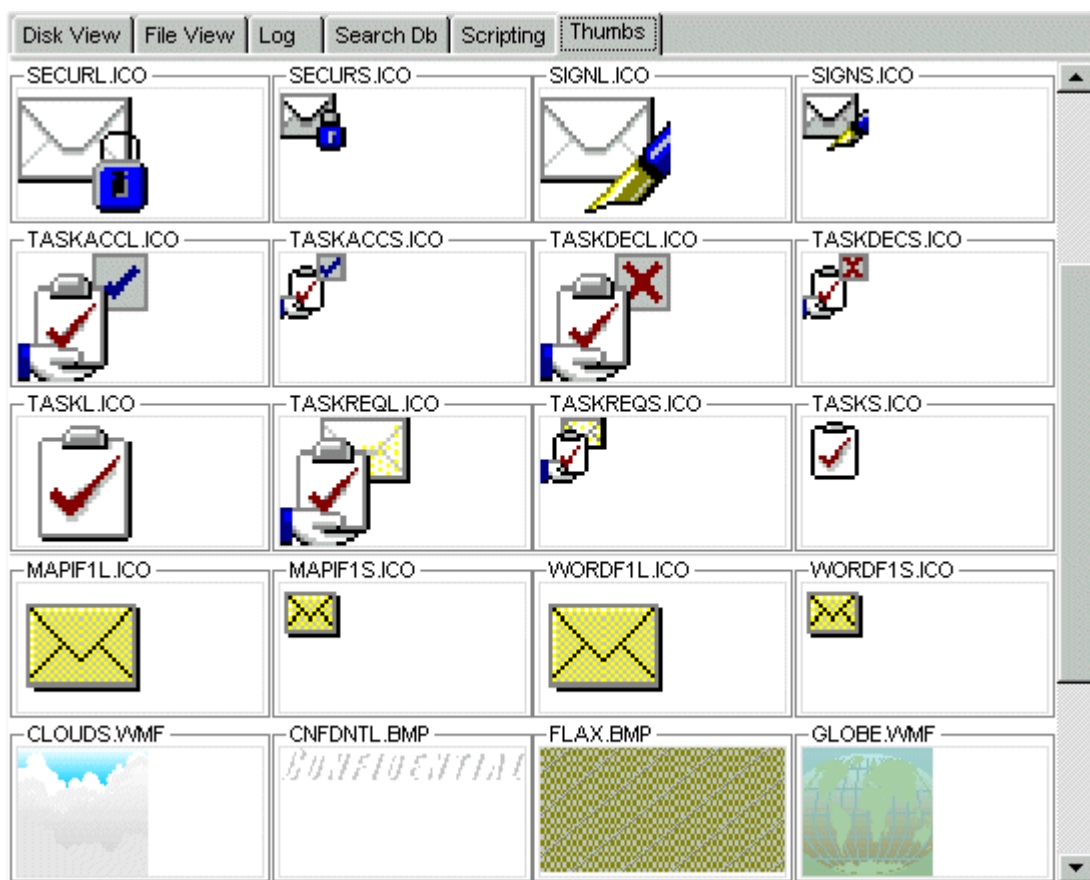
Kompajliraj i snimi skriptu (Compile and Save Script) –

Kompajlira trenutno izabranu skriptu I snima je na disk.

Brisanje teksta iz konzole (Clear Console) – Briše sve poruke koje su trenutno prikazane u konzoli.

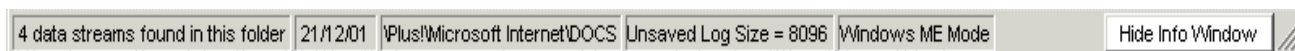
Nova skripta (Start New Script) – Briše sadržaj editor prozora i kreira novu skriptu koristeći postojeći šablon.

Kartica Thumbs (Thumbs InfoWindow) prikazuje listu slika koje se nalaze u selektovanom folderu. Ova funkcija je od velike pomoći pri istragama sistema koje se tiču nelegalnih slika. Koristi se tako što izaberete karticu Thumbs a zatim izaberete bilo koji folder u prozoru dokaza (EvidenceWindow). ILook će prikazati slike I druge fajlove u thumbnail obliku (umanjene verzije velikih slika) . Fajlovi koji nisu podržani za pregledanje od strane Ilooka neće biti prikazani u ovom prozoru. Ukoliko zadržite kursor miša iznad bilo koje thumbnail sličice Ilook će prikazati i naziv fajla. Desnim klikom na prikazanu sličicu fajl će biti prikazan u Prozorau za pregledanje fajlova (File View InfoWindow).



Slika 27. Thumbs

Statusni meni-linija (Status bar)



Slika 28. Statusna meni-linija

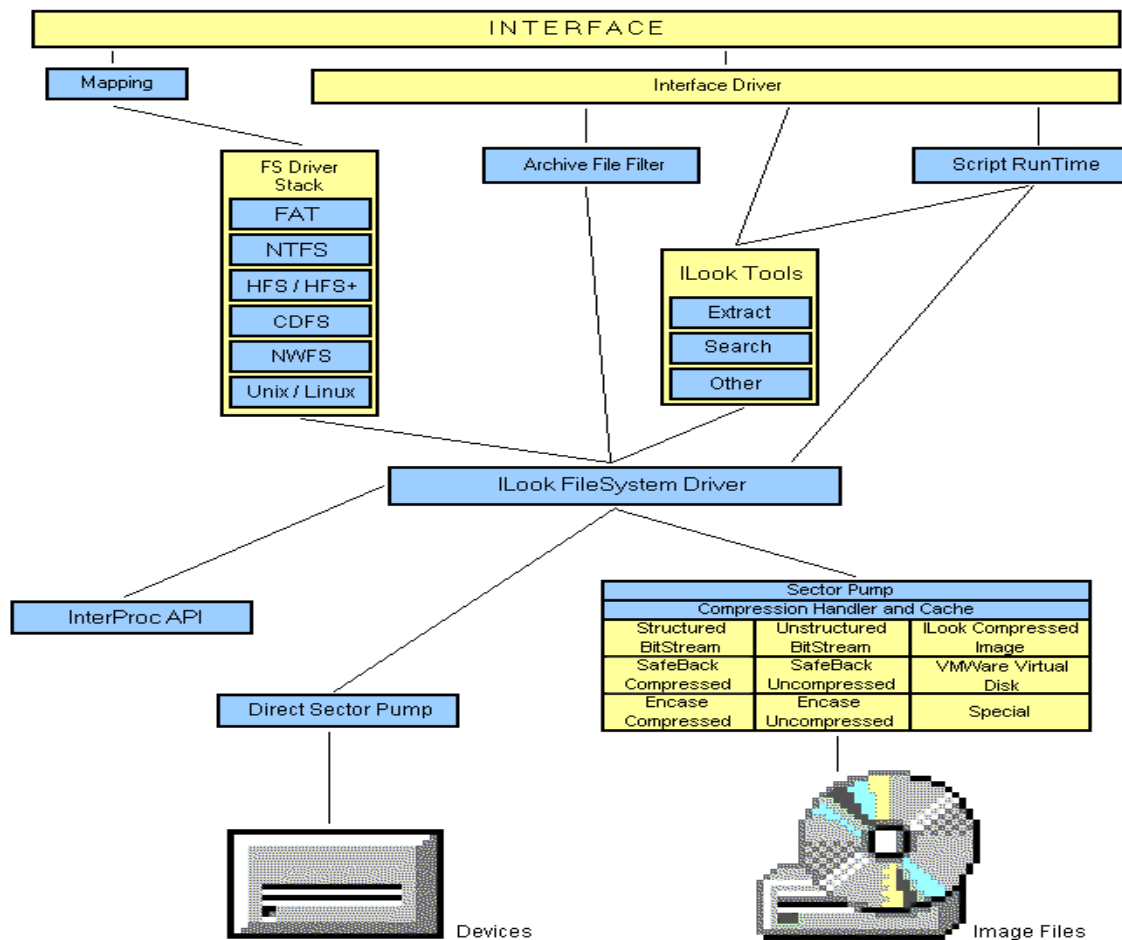
Statusna linija se sastoji od 5 panela informacija:

Panel informacija – detalji povremenih poruka koji se ne zapisuju u dnevnik

- Datum(Date) – trenutni datum u lokalnom formatu datuma
- Putanja(Path) – cela putanja za trenutno selektovani folder u prozoru Dokaza (EvidenceWindow)
- Status dnevnika (Log status) – trenutni broj nesnimljenih podataka u dnevniku(Log fajlu)
- Mod (Mode) – trenutni mod O/S

Statusna linija sadrži i dugme kojim možete sakriti ili ponovo prikazati prozor informacija (InfoWindow).

5.10. Pregled Infrastrukture Ilook-a



Slika 29. Pregled Infrastrukture Ilook-a

Kratko uputstvo za korišćenje Ilook-a

Definisanje dokaza u Ilook-u

1. Pokrenite ILook
2. Pritisnite **F4** da bi ste otvorili Prozor za rukovanje dokazima(evidence management window).
3. Podešavanje postavki novog slučaja (radi se samo jednom na početku svakog slučaja).
 - U delu za definiciju fajla dokaza (**Evidence Definition File**) pritisnite dugme **New (Novi)** i napravite novi EVD fajl. Ovaj fajl sadrži informacije o konfiguracionim informacijama za tekući slučaj. Morate napraviti novi EVD fajl za svaki slučaj koji istražujete.
 - U delu Ime istražitelja (**Investigator's Name / ID**) pritisnite dugme **Change (Promeni)** i napišite vaše ime, po default-u vaše ime biće prikazano za svaki novi deo dokaza u slučaju kao ime istražnog lica (takođe možete za svaki deo dokaza da promenite ovo ime).

- U delu **Case Results Path(Putanja rezultata slučaja)** selektujte local(lokalni disk) ili network drive(mrežni disk) na kojem će te čuvati sve izveštaje ili ekstrahirane podatke iz vaše istrage.
 - U delu **Case Reference (Opis slučaja)** pritisnite dugme **Change (Promena)** i upišite kratak opis za tekući slučaj.
4. Add a new item of evidence (Dodaj novi dokazni objekat) (ovaj deo se mora ponoviti za svaki dokazni objekat koji dodate u slučaj).
- Levi klin na žuto dugme označeno kao **Add Evidence to Case(Dodaj dokaz u slučaj)**, pojaviće se novi dokazni objekat prozoru dokaza (evidence view).
 - Desni klik na boldiranu liniju novog dokaznog objekta i izaberite funkciju **Edit Evidence ID** (Izmeni ID Dokaza), dajte vašem novom delu dokaznog materijala kratak opis.
 - U odeljkui **Evidence Info** (Inforamcije o dokaznom materijalu) novog objekta kliknite desnim dugmetom na **Notes (Zabeleška)** i izaberite funkciju **Edit(Promeni)**, napišite opis za taj deo dokaznog materijala.
 - U odeljku **Image / Device List**(Lista Slika/Uređaja) novog objekta kliknite desnim dugmetom **Image 0** i izaberite funkciju **Select Image Section (Selektujte Sliku)**. Pronađite prvi deo iz vašeg seta slika diska I izaberite taj fajl.Ukoliko ILook prepozna da postoji još delova slika diska Ilook će ih automatski dodati u deo pod nazivom **Image / Device List**.Ukoliko ILook sve delove onda možete da promenite listu manuelno tako što kliknete desnim dugmetom na odeljak **Image / Device List** I selektujete funkcijju **Resize List(Promeni veličinu liste)**.Kada kliknete bićete u mogućnosti da specificirate koliko delova slika imate. Kada to završite onda možete da učitate svaku sliku ponoaosob kao što ste to u početku uradili. Slike diska moraju biti definisane u pravilnom redosledu, najgornji ulaz mora biti prva slika diska i tako dalje do kraja liste.
5. Pritisnite dugme **Apply(Prihvati)** da bi ste snimili promene.

Mapiranje delova digitalnih dokaza

12. Vaši novi delovi dokaznog materijala biće prikazani u prozoru Dokaza (EvidenceWindow) glavnog ekrana. Kliknite desnim dugmetom na zapis i izaberite funkciju “Standard Partition Traverse”. ILook sada uklanja kompresiju slike diska ukoliko je slika diska kompresovana. Posle ovoga Ilook pregleda sliku i traži zapise o ispravnim meta podacima, strukturu diska, kao što su particije.
13. Pritisnite desno dugme na svaku strukturu koju je Ilook izlistao I izaberite funkciju “Map FileSystem”. Ilook će onda mapirati fajl sistem I prikazati strukturu foldera ispod izabrane strukture. Kliknite na folder kako bi ste videli fajlove i I zbrisane fajlove koji pripadaju selektovanom folderu.
14. Zapamtite da snimate mapirani fajl sistem tako da bi ste mogli da ga učitate tokom neke sledeće sesije.

5.11. Preporuka u korišćenju ILook tokom istraga.

Nameštanje računara

Za najbolje rezultate postavite rezoluciju vašeg ekrana(monitora) 1024x768x32bit boju, font bi trebao da bude Small Fonts. Instalirajte MDAC sa Microsoft web sajta.

Filtriranje i isključivanje

Prvo što bi ste trebali uraditi je da iskoristite razne načine filtriranja i isključivanja koje Ilook poseduje da bi ste ograničili količinu materijala koji morate da pregledate I pretražite. Ovo je jedan od najbitnijih delova programa koji morate da svladate. Sa malo vežbe ovim metodama možete da eliminišete 60% ili više objekata fajl sistema i time uštedite veliku količinu vremena. Cilj korišćenja ovih funkcija je da se automatski odvoje podaci koje je kreirao korisnik od podataka koje je kreirao sistem i izbacivanja istih iz pretrage. Ovo ne treba koristiti ukoliko fajlovi koje je kreirao sistem utiču na krajnji rezultat vaše istrage. Ipak u najviše slučaja najverovatnije je da podaci koje je kreirao korisnik imaju najveći značaj za tužioca. Koraci koji moraju da se obave kako bi se ove funkcije pravilno koristile:

1. Nabavite Hashkeeper hash bazu podataka i podesite ILook da zna gde se baza nalazi.
2. Mapirajte fajl sisteme na dokaznim objektima po postupku opisanom u prethodnom delu.
3. Napravite MD5 hash vrednosti svih fajlova.
4. Pokrenite negativnu hash analizu da bi ste eliminisali poznate systemske fajlove.
5. Napravite uključujuće ili isključujuće filtre nad folderima ili fajlovima da bi ste još više smanjili broj fajlova koje treba da pregledate.

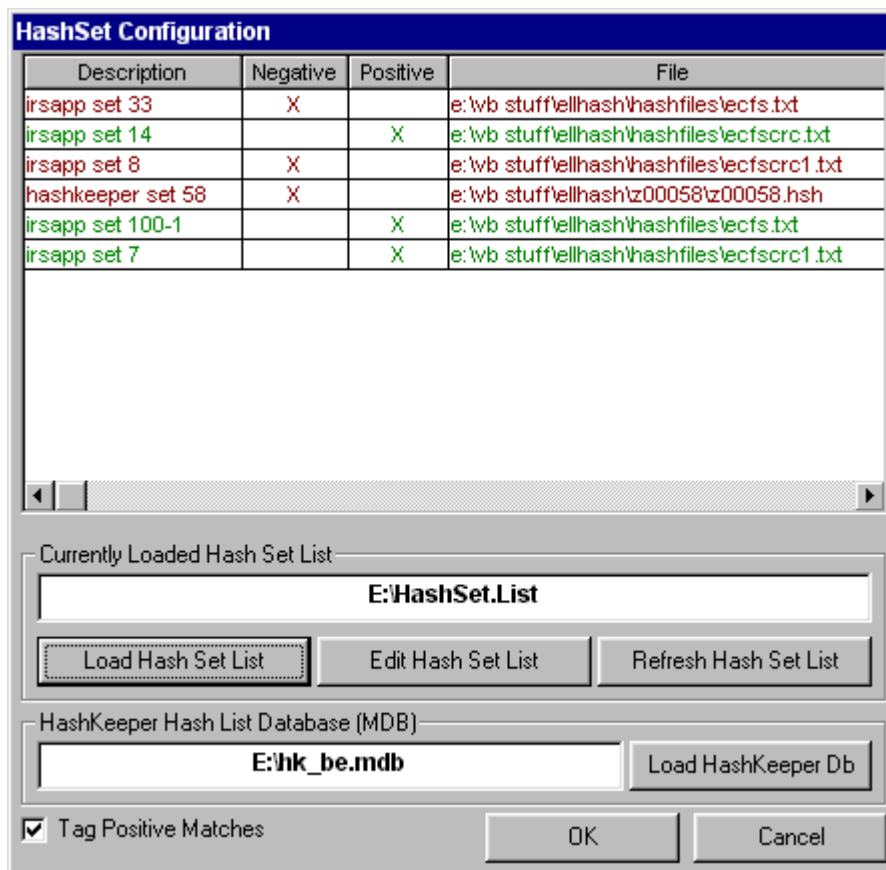
Zapamtite da se fajlovi koje ste isključili neće pojavljivati ni na jednoj listi fajlova tako da možete da se skoncentrišete na pretragu preostalih. Isključeni fajlovi su takođe nevidljivi za pretrage tako da se vreme pretrage fajlova znatno smanjuje.

1. Hashkeeper baza podataka

Hashkeeper je alat za hash-ovanje fajlova koje je napravila US National Drug Intelligence Centre. Hashkeeper se sastoji od velike baze podataka u MS Access formatu koja sadrži nekoliko stotina hiljada hash vrednosti. Ove hash vrednosti su generisane iz hash set fajlova koje pripadaju velikom broju komercijalnih I nekomercijalnih programa I idealne su za isključivanje velikog broja poznatih fajlova iz istrage od onih koje želite da pretražujete. Ovo u mnogome pomaže tako što vam smanjuje broj fajlova koji treba da pretražite. Dodatno hashkeeper takođe ima u sebi hash vrednosti koje us generisane kriptu programima, stego programima i slika

pedofilije. Ove setove možete koristiti za pretrage pozitivne hash analize da bi ste označili fajlove koji mogu biti ključni u vašoj istrazi.

Prozor za konfiguraciju HashSet-a ima dugme Load HashKeeper Db(Učitaj HashKeeper Db). Koristite ovu funkciju kako bi ste locirali I učitali hashkeeper bazu podataka hk_be.mdb – ovaj fajl ne može da bude read-only I ne može da se nalazi na CD-ROM-u. ILook integriše vrednosti iz ove baze podatak sa funkcijama hash analize podataka. Tabela TblHashSet HashKeeper baze podataka ima kolonu koja se zove Notable_Flag. ILook koristi vrednosti iz ove kolone da bi znao da li svaki set treba da se primeni negativno ili pozitivno. Ukoliko je Notable_Flag postavljen za dati hash set onda će ILook taj hash set tretirati kao pozitivan.



Slika 30. Prozor za konfiguraciju HashSet-a

3.MD5, SHA1, CRC32 negativne hash analize

ILook ima implementirane dve funkcije hash analize, pozitivnu i negativnu hash analizu. Negativna hash analiza je dizajnirana da omogući istražitelju da isključi iz istrage velike količine poznatih fajlova, tako da u mnogome smanjuje obim posla. Funkcije za hashiranje fajlova možete naći u menijima particija, foldera i fajlova.

Funkcije negativne hash analize rade tako što upoređuju hash vrednosti fajlova u vašem dokaznom materijalu sa vrednostima u hash setovima podataka i/ili HashKeeper bazi podataka koje su dodeljene negativnim hash funkcijama. Ove vrednosti su obično delovi

određenog operativnog sistema ili neke aplikacije. Cilj ove analize je da se lako uklone fajlovi koji nisu od dokazne vrednosti. Kada se obavi negativna hash analiza preostaje mnogo manji deo fajlova da se proverí, i ostatak fajlova će predstavljati uglavnom fajlove koje su napravljeni, modifikovani ili dopunjeni na disku osumnjičenog.

Pokretanje negativne hash analize

- Pre nego što pokrenete analizu morate prvo izračunati hash vrednosti za grupu fajlova na kojoj ćete da vršite analizu. Funkcije za izračunavanje hash vrednosti fajlova se nalaze na nivoima particija, foldera i fajlova. Ove funkcije se nalaze pod menijem Analysis Functions (Funkcije Analiza) na svakom od navedenih nivoa imožete birati vrstu hash algoritma CRC32, MD5 and SHA1 (ili kombinaciju od ova tri). Morate izabrati vrstu algoritma koja je konfigurisana u hahs setovima koje ste konfigurisali (u odnosu na koje će te da vršite analizu, zapisi HashKeeper baze podataka su vrednosti koje su dobijene MD5 hash algoritmom). Drugim rečima ukoliko vaš hash set sadrži MD5 hahs vrednosti onda morate izračunati MD5 hash vrednosti za sve fajlove koje želite da ukljućite u analizu inače fajlovi za koje nije izračunata hash MD5 vrednost biće preskoćeni.
- Kada ste izračunali vrednosti hash fajlova onda izaberete funkciju Negative Hash Analysis (Negativnu hash analizu) iz menija funkcija Analysis Functions (Funkcije Analize) na nivou particije. Ovo će pokrenuti analizu i izbaciće sve fajlove koji se poklapaju (fajlovi za koje nije izračunata hash vrednost će biti ignosrisani). Funkcije koje se pokreću ubuduće nad particjom neće uzimati u obzir fajlove koji su iskljućeni ovom analizom i nećete ih više videti među fajlovima.
- Možete vrstiti iskljućene fajlove tako što će te izabrati funkciju Reverse Negative Hash Analysis (Povratna Negativna Hash analiza) iz menija Analysis Functions menu (Meni Funkcije Analize) na nivou particije. Ovo će vratiti nazad sve iskljućene fajlove I Ilook će ih prikazati ponovo. Ovu funkciju vraćanja fajlova možete vršiti I na nivou foldera tako što desnim klikom miša na folder izaberete funkciju Unapply File Hash Elimination (Vrati Fajlove koje su eliminisani Hash anlaizom) iz menija Filters (Filteri).

5. Ukljućujući ili iskljućujući filtri nad folderima ili fajlovima

Postoje dva glavna metoda za izdvajanje kolićine fajlova koje treba da pregledate u Ilook. Prva je negativna hash analiza

Drugi metod je Filtering (Filtriranje). Filtriranje je kojim se iskljućuju fajlovi iz dalje istrage tako što se naznači Ilook-u da oni više nisu potrebni. Ilook će izbaciti te fajlove iz Prozora fajlova (File Window) i Prozora rezultata (Results Window).

Filtriranje (Filtering) radi na nivou foldera u prozoru dokaza (Evidence Window) I odnosi se na selektovani folder kao i na sve pod foldere. Pošto ova funkcija radi na nivou foldera moguće je primeniti različite filtere na različite delove fajl sistema. Na ovaj način možete podesite šta da vam prikazuje i smanjite kolićinu fajlova koje pregledate.

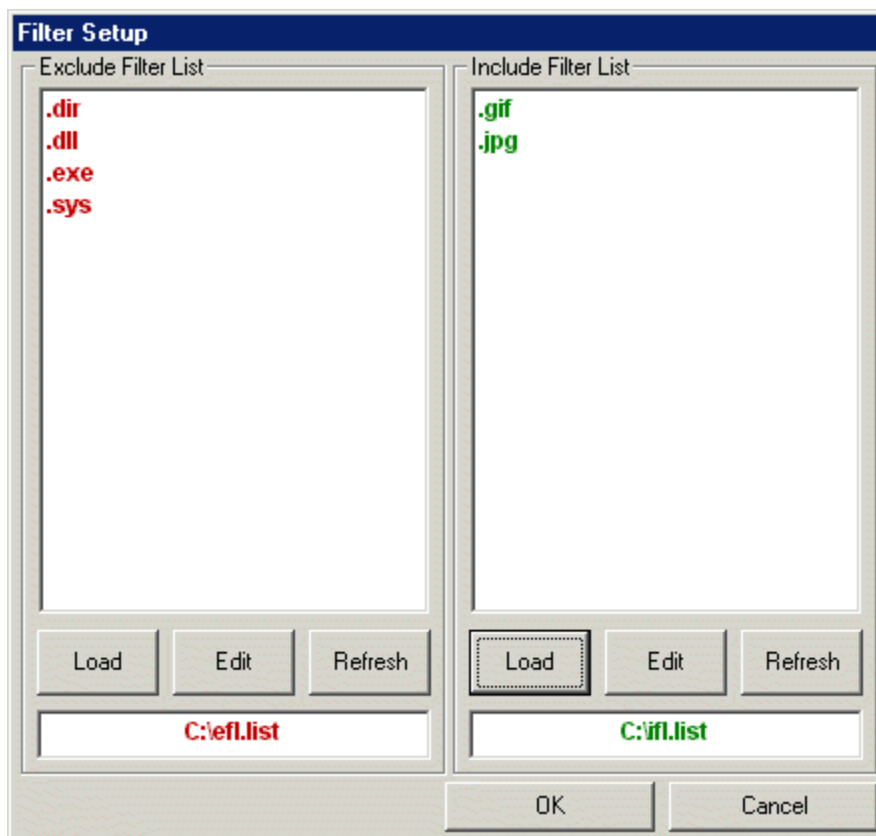
Vrste filtera

Ilook ima 4 filtrirajuća mehanizma :

3. **Include filter(Filter uključivanja)** – filter nad ekstenzijom fajla. Kada je ovaj filter uključen, svi fajlovi koji nemaju ekstenziju koja je upisana u listi ekstenzija filtera biće isključeni iz prikazivanja.
4. **Exclude filter (Filter isključivanja)**– filter nad ekstenzijom fajla. Kada je ovaj filter uključen, svi fajlovi koji imaju ekstenziju koja je upisana u listi ekstenzija filtera biće isključeni iz prikazivanja.
5. **NDF filter (NDF filter)**- ovaj filter je moguće uključiti samo nad particijama koje su pod Unix fajl sistemom. Unix većinu objekata zapisuje kao fajl a ovaj filter isključuje objekte fajl sistema koji nisu pravi fajl (block devices, character devices, symlinks).
6. **Elimination filter (Filter eliminacije)** – Ovaj filter možete sami postaviti I sa njim možete isključiti fajl ili grupu fajlova koje ste prepoznali kao nebitne za vašu istragu. Na ovaj način možete isključiti sve fajlove koje ste već pregledali I time ih isključiti iz svih funkcija pretraga tako da se ne pojavljuju u rezultatima pretraga. Ovaj filter je moguće uključiti u prozoru fajlova (FileWindow), prozoru rezultata (ResultsWindow) desnim klikom miša. Moguće ga je uključiti na nivou foldera u prozoru dokaza (EvidenceWindow).

Podešavanje filtera uključivanja i isključivanja

- Iz Setup menija koji se nalazi u glavnom Ilook-ovom meniju, izaberite funkciju Filter Setup (Podešavanje filtera). Pojaviće se Filter setup dijalog kao na slici.



Slika 31. Prozor za konfiguraciju HashSet-a

- Liste filtera uključivanja i isključivanja su dva obična tekst fajla, i svaki sadrži listu ekstenzije fajlova koji se primenjuju na svaku funkciju. Kada kreirate ova dva fajla treba da naznačite Ilook-u putanje do tih fajlova koristeći dugme Load (Učitaj). ILook će prikazati vaše filtere u odgovarajućem prozoru.
- Dugmići Edit će pokrenuti sistemski editor teksata tako da možete da promenite ekstenzije fajlova koje tražite. Ukoliko izmenite vaše filter fajlove onda možete da koristite refresh dugme da bi te promene učitali u Ilook.
- Na bilo kom folderu bilo kog mapiranog fajl sistema možete pritisnuti desno dugme miša i ući u podmeni menija Filter. Ovde se nalazi dve funkcije pomoću kojih možete da vratite fajlove koje ste isključili negativnom hash analizom ili filterima. Povratak fajlova se odnosi na sve foldere i podfoldere selektovanog foldera.

Filteri nad folderima

Možete primeniti filter foldera nad bilo kojim pravim (koji nije virtuelan) folderom koji Ilook prikazuje u Prozoru dokaza (EvidenceWindow). Filter nad folderom je jedna ili više specifikacija fajlova koja limitira Ilook da prikazuje samo fajlove sa tom specifikacijom kada selektujete filtrirani folder. Na primer ukoliko folder sadrži nekoliko hiljada fajlova različitih tipova a vi želite samo da vidite JPG i GIF fajlove onda treba da

kliknete desnim dugmetom miša na folder zatim selektujete zatim iz menija izaberete funkciju Set Folder Filter(Namesti Folder filter) i upišete "*.jpg, *.doc" u prozoru za filter. Odvojite svaku specifikaciju fajla sa zarezom. Pojaviće se "F" simbol u ikonici za folder tako da nas podseća da je nad folderom uključen filter. Da bi isključili filter, selektujte opet iz menija funkciju Set Folder Filter I izbrišite unete parametre ili kliknite dugme Cancel (Odustani).

5.12. Pretraga fajlova

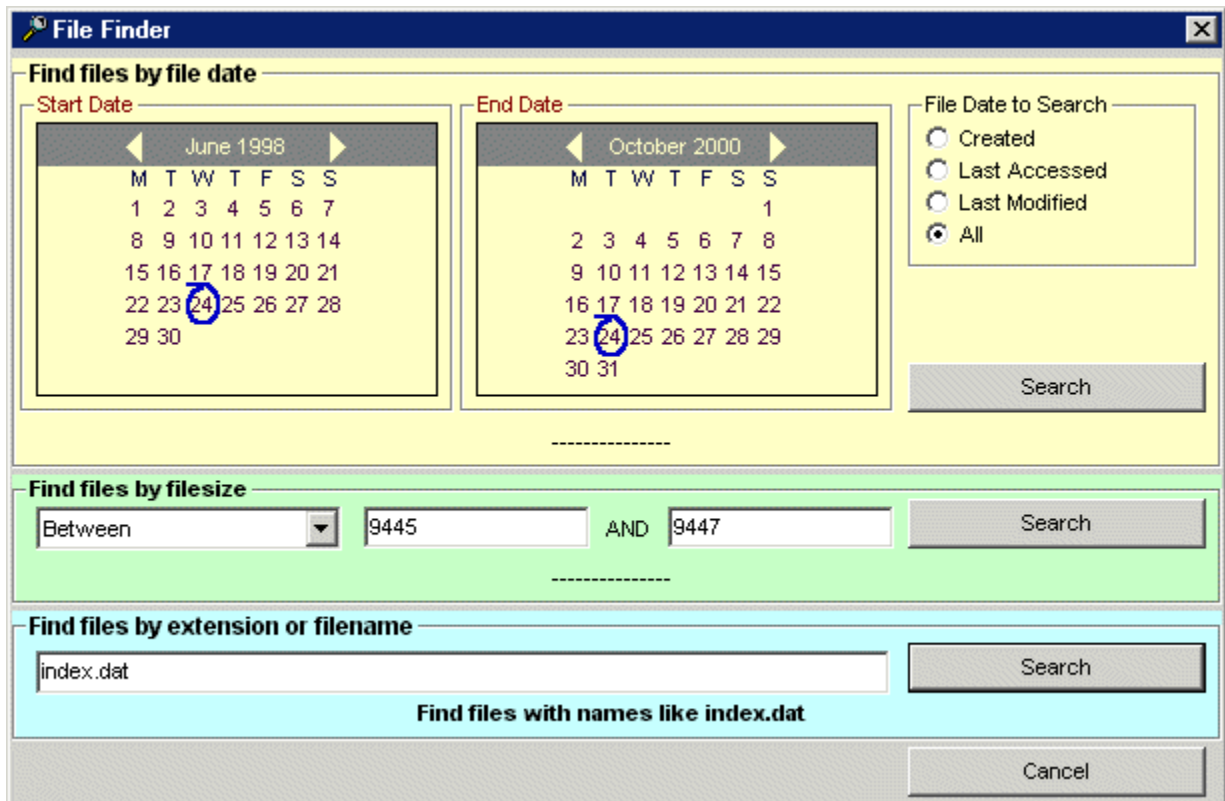
Koristite funkcije Ilook-a da bi pronašli stvari koje vas interesuju, nemojte lutati kroz fajl sistem, koristite ILook da obavi posao.

- Pronalazak fajlova koji su kreirani, modifikovani na određeni datum ili između nekog perioda
- Pronalazak fajlova sa određenim ekstenzijama ili nazivima
- Statistička vremenska linija sa podacima o promeni fajl sistema tokom njegovog životnog veka
- Pronalazak fajlova po potpisu fajla ili obeležavanje fajlova čija ekstenzija ne odgovara potpisu tih fajlova
- Korišćenje pozitivne hash analize za pronalazak poznatih fajlova.
- Pretraga neiskorišćenih delova diska za izbrisanim fajlovima
- Korišćenje mogućnosti pretrage Ilook-a da bi ste obeležili relevantne podatke
- Korišćenje ILook-ovih virtuelnih kategorija, brz metod kojim možete da dobijete brz pregled sistema.

5.13. Pronalazak fajlova koji su kreirani, modifikovani na određeni datum ili između nekog perioda i statistička vremenska linija sa podacima o promeni fajl sistema tokom njegovog životnog veka

Da bi ste pristupili pretrazi pritisnite desni klik miša, na nivou uređaja, uređaja nad kojim želite da izvršite pretragu fajlova i iz menija selektujte funkciju Find files by date, size or name (Pronađi fajlove po datumu, veličini ili nazivu).

Kada pritisnete dugme pojaviće se prozor koji je prikazan dole na slici.



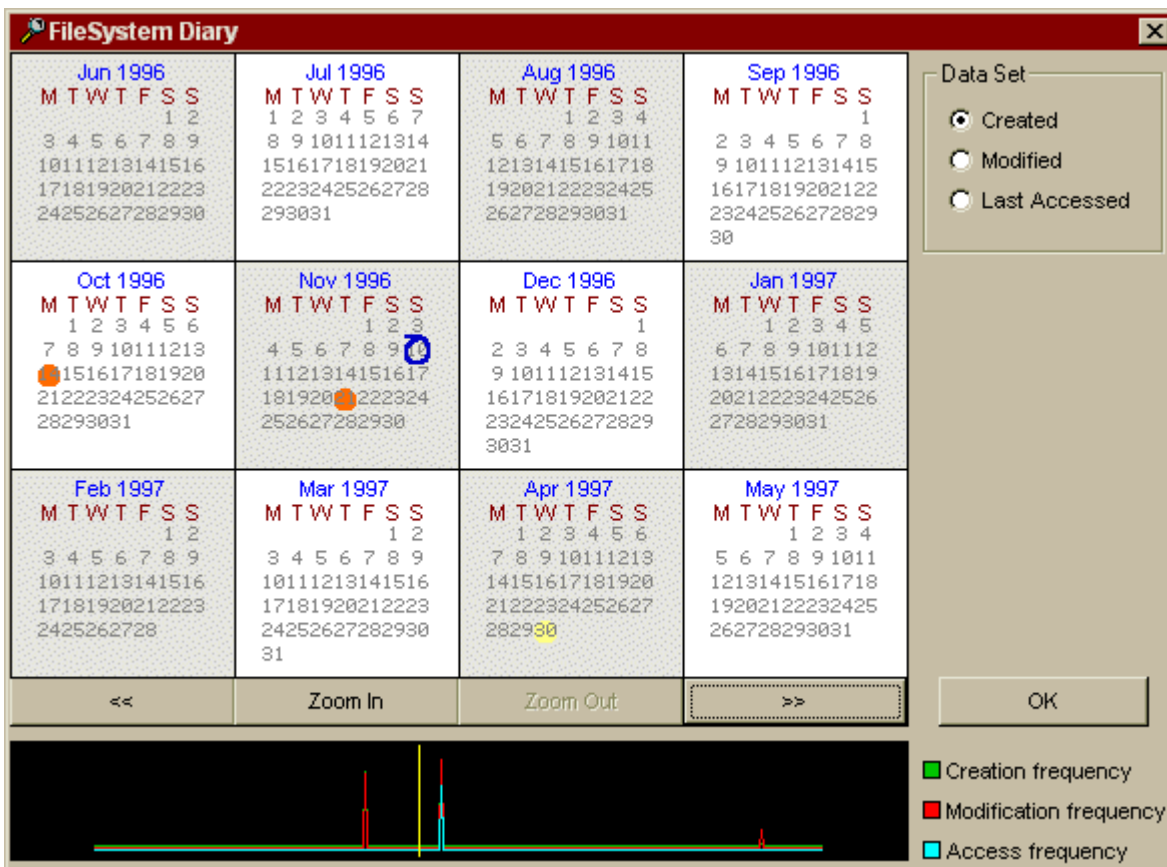
Slika 32. Prozor za pretragu fajlova po datumima

- Pretraga po datumu se vrši u žutom delu ekrana. Na levom kalendaru se izabere datum početka a na desnom datum kraja. U delu ekrana koji je obeležen sa File Date to Search možemo izabrati da li želimo pretragu po datumima kada su fajlovi kreirani, kada im je zadnji put pristupljeno, kada su zadnji put promenjeni ili da gleda po svim ovim parametrima. Posle odabira parametara pretraga se pokreće na dugme Search(Pretraga). Rezultati pretrage se prikazuje u prozoru Rezultata pretrage.
- Pretraga po veličini fajla se vrši u zelenom delu ekrana. Iz padajuće liste izaberite tip poređenja, zatim upišite parametre veličine fajlova koje tražite. Zatim pritisnite dugme Search(Pretraga) i Ilook će započeti pretragu a rezultati pretrage će se prikazati u prozoru rezultata pretrage (search results window).
- Pretraga fajla po imenu fajla se vrši u plavom delu ekrana. U polje možete upisati pun naziv fajla, deo naziva fajla, ili ekstenziju fajla koji tražite. Možete koristiti i znakove u pretragama:
 - ? - zamenjuje bilo koji karakter na poziciji na kojoj se upiše znak
 - *- zamenjuje bilo koji niz karaktera na poziciji na kojoj se upiše znak
 - # - zamenjuje bilo koji numerčki karakter na poziciji na kojoj se upiše znak

Možete tražiti i više različitih naziva fajlova ili ekstenzija fajlova tako što svaki parametar pretrage odvojite zarezom. . Zatim pritisnite dugme Search(Pretraga) i Ilook će započeti pretragu a rezultati pretrage će se prikazati u prozoru rezultata pretrage (search results window).

5.14. Dnevnik Fajl sistema (statistička vremenska linija sa podacima o promeni fajl sistematomkom njegovog životnog veka)

Dnevnik fajl sistema je analiza značajnih datuma koji su snimljeni u odnosu na sve fajlove u odnosu na bilo koji mapirani fajl sistem. Denvniku fajl sistema se pristupa tako što se pritisne desno dugme na particiju i izabere iz menija koji se prikazuje. Slika dole je izgled dnevnika:



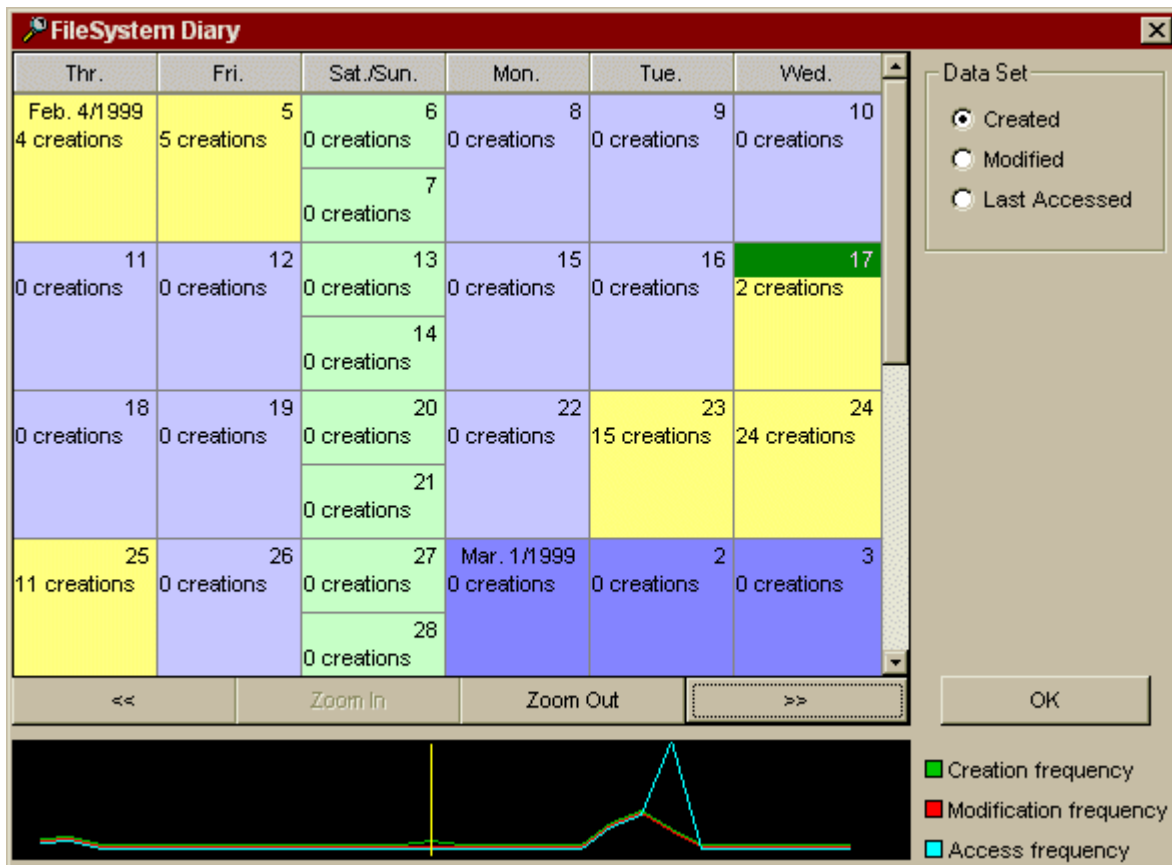
Slika 33. Dnevnik fajl sistema

Ovo je odzumirani izgled(zoomed out). Gornji deo ekrana prikazuje godišnji pregled događanja na fajl sistemu u odnosu na izabranu opciju iz seta podataka (Data Set). Možete izabrati datume kreiranja, modifikovanja ili zadnjeg pristupa fajlovima. Možete skrolovati kalendar na dugmiće << ,>>. Događanja na datumima su prezentovana grafički i prikazana su u tačkama u boji na određene datume. Šema boja:

- Bela - nema aktivnosti
- Svetlo žuta – slaba aktivnost

- Tamno žuta – srednje slaba aktivnost
- Narandžasta – srednja aktivnost
- Svetlo crvena – srednje jaka aktivnost
- Tamno crvena – jaka aktivnost

Donji deo ekrana je analiza učestalosti za sve tri vrste podataka za period od godinu dana koji je prikazan u gornjem delu ekrana. Žuta vertikalna linija se postavlja gde god označite datum u gorenjm delu ekrana tako da možete da s efolusirate na određeni deo vremenske linije. Možete zumirati pregled datuma u četvornedeljni pregled koristeći dugme Zoom In ili duplim klikom na neki datum. Dobićete izgled ekrana kao na slici dole:



Slika 34. Dnevnik fajl sistema

Ovo je zumirani izgled ekrana. Možete skrolovati nedelje preko dugmića << ,>>. Šema značenja boja je ista kao i kod ne zumiranog izgleda ekrana

Možete se vratiti u godišnji izgled klikom na dugme Zoom Out. Ukoliko kliknete dvaput na neki datum u ovom ekranu Ilook će izabrati fajlove koji sadrže podatke za taj datum i prikazati ih u prozoru rezultata pretrage.

5.15. Pronalazak fajlova po potpisu fajla ili obeležavanje fajlova čija ekstenzija ne odgovara potpisu tih fajlova

Ova funkcija pronalazi fajlove tako što upoređuje potpise koji se nalaze u zaglavlju fajla sa poznatim potpisima. Ova funkcija nam pruža brz način za pronalazak skrivenih ili preimenovanih fajlova. Radi tako što upoređuje nekoliko prvih bajtova svakog fajla naspram liste potpisa fajlova koje vi obeležite. Možete koristiti listu predefinisanih fajlova i/ili možete kreirati sami svoju listu.

Funkcija "File Signature Check"(Provera potpisa fajla) skenira svaki fajl u izabranoj particiji za određene tipove fajlova i može da identifikuje sledeće tipove fajlova:

- **Arhive**
 - **.ARJ** (*Archive*)
 - **.ZIP** (*PKZIP archive*)
- **Slike**
 - **.GIF** (*Graphics Interchange Format picture*)
 - **.JPG** (*Joint Photographics Group format picture*)
 - **.PNG** (*Portable Network Graphics format picture*)
 - **.BMP** (*Windows bitmap picture*)
 - **.ART** (*AOL picture*)
- **Filmovi**
 - **.AVI** (*Audio Video digital movie*)
 - **.MPG** (*Motion Picture Group digital movie*)
- **Tekstualne fajlove**
 - **.DOC** (*MS Word v1/2/4/5/6/97*)
 - **.RTF** (*Rich Text Format*)
 - **.WRI** (*Windows Write*)
 - **.WP** (*Word Perfect v5.x*)
- **Tabelarne fajlove**
 - **.XLS** (*MS Excel v3/4/97*)
 - **.WK1** (*Lotus 123 v1/2*)
 - **.WK3** (*Lotus 123 v3*)
 - **.WK4** (*Lotus 123 v4*)
 - **.WKS** (*MS Works Spreadsheet*)
 - **.DIF** (*Data Interchange Format*)
- **HTML fajlove**
 - **.HTM(L)** (*Hyper Text Markup Language scripts*)
- **Formate fajlova koje ste sami kreirali**
 - **Bilo koji**

Pokretanje pozitivne ili negativne provere potpisa

Pozitivna provera potpisa fajlova pregleda potpis svakog mapiranog fajla u odnosu na listu koju specificirate u podešavanjima potpisa (signature setup) i obeležiće svaki fajl koji odgovara selektovanim specifikacijama potpisa. Na primer ukoliko izaberete JPG u podešavanjima potpisa ILook će proveriti svaki fajl, i pronaći svaki koji odgovara selektovanim specifikacijama potpisa bez obzira na stvarno ime ili ekstenzije za bilo koji fajl. Ovo je brz i odličan metod za pronalaženje preimenovanih ili pogrešno imenovanih tipova fajlova. Negativna provera potpisa pregleda sve fajlove sa selektovanim ekstenzijama da bi se proverili da li su to tipovi fajlova koji tvrde da jesu. Ilook će obeležiti bilo koji fajl koji ima ekstenziju koja se ne poklapa sa potpisom fajla.

- Kada kliknete na Pozitivnu ili negativnu proveru potpisa na funkciju u meniju na nivou particije (Positive Signature Check or Negative Signature Check) pojaviće se ekran kao na slici

File Signature Setup

Options

Detect Archives
☐ ARJ and ZIP

Detect Images
☒ PNG, BMP, GIF, JPG and ART

Detect Movies
☐ AVI and MPG

Detect Word Processing Files
☐ MS DOC 1/2/4/5/6/97, RTF, WRI and WP

Detect Spreadsheets
☒ MS XLS 3/4/97, WK1, WK3, WK4, WKS and DIF

Detect HTML
☒ HTML

Detect Custom Files
☒ C:\WB stuff\ELIX\Samples\Signature.List

File Type	File Ext	Signature	Signature Displacement
☒ AOL Graphic File3	.art	4a47030e	1
☒ AOL Graphic File4	.art	4a47040e	1
☒ PGP Disk	.pgd	504750644041494E600100006AF5216F	1
☐ Have file	.hav.	52494646	1
☐ Enhanced meta file	.enf	010000005800	1
☐ Windows meta file	.unf	07CDC6980000	1

Load Custom List Edit Custom List Refresh

OK Cancel

Slika 35. Potpis fajla

- Selektujte koje tipove fajlova želite da proveravate tako što kliknete na polje pored naziva tipa fajla. Opcije u meniju omogućavaju recimo da isključite proveru **.BMP** fajlova.
- Ilook vam omogućava da specificirate bilo koje potpise fajlova koje želite da budu uključeni u funkciju provere potpisa. Kreirajte teks fajl i na svaku liniju specificirajte definiciju za format potpisa fajla. Svaka definicija se sastoji od pet polja, prva tri polja su obavezna. Prvo polje je opis tipa fajla, drugo polje je ekstenzija fajla koji Ilook koristi kada detektuje ovaj tip fajla, treće polje je sam potpis u zaglavlju fajla, četvrto polje je (opciono) pomeranje potpisa fajla unutar zaglavlja (ukoliko se ne upiše ništa u ovo polje početna vrednost je 1), peto polje je (opciono) potpis footer-a fajla. Sva polja moraju da budu razdvojena tačkom i zarezom.

- Za primer koji je prikazan na slici morate napisati sledećih 7 linija u tekstualnom fajlu :
 - **MS Access Db;.mdb;00010000537461**
 - **Outlook Mail Files;.pst;2142444e**
 - **Meta File Graphic;.wmf;d7cdc69a0000**
 - **Jpeg Graphic File;.jpg;ffd8fffee0001a10;1;ffd9**
 - **AOL Graphic File3;.art;4a47030e;1;d0cb0000**
 - **AOL Graphic File4;.art;4a47040e;1;cfc7cb**
 - **PGP Disk;.pgd;504750644D41494E600100006AF5216F;1**
- Učitajte ove definicije potpisa u ILook'-ovu funkciju provere potpisa tako što kliknete dugme **Load Custom List (Učitajte vašu listu)** i selektujete fajl koji ste kreirali. Vaši unosi će se pojaviti u listi **Detect Custom Files (Detektuj listu)**. Odavde možete pojedinačno da selektujete fajlove koje hoćete da uključite u proveru potpisa tako što kliknete na checkbox-ove pored svakog unosa (na početku su svi selektovani). Dugme **Edit Custom List(Promena liste)** pokreće tekst editor u vašem lokalnom sistemu tako da možete da promenite vaš fajl sa ptpisima i tipovima fajlova. Ukoliko promenite vaše liste onda pritisnite dugme refresh da bi se liste učitale u Ilook sa novim podacima.
- Kada podesite proveru potpisa i pritisnete dugme **OK**, ILook će skenirati fajlove na particiji za tipove fajlova koje ste izabrali. Pogotci pri ovoj analizi biće prikazani na ekranu rezultata pretrage (search results screen).
- Ekranu za podešavanje potpisa možete pristupiti preko menija Setup koji se nalazi u glavnom meniju Ilook-ovog ekrana i funkcije **Signature Setup (Podešavanje potpisa)**.

5.16. Funkcije oporavka i pretraživanja ostataka fajlova i samih fajlova

Ilook ove funkcije spasavanja podataka su dizajnirane da oporave fajlove, iz bilo kog uređaja ili slike diska sa bilo kog uređaja, koji su se odvojile od normalne strukture fajl sistem indeksiranja, obično ovi fajlovi ne mogu biti oporavljeni standardnim metodama. Funkcije spasavanja podataka otkrivaju fajlove tako što prolaze kroz sve sektore u potrazi za potpisima poznatih fajlova (potpis fajla se nalazi u prvih nekoliko bajtova fajla i jedinstven je za svaku vrstu fajlova). Postoje dve funkcije za spasavanje podataka prva prolazi samo kroz granice sektora u potrazi za fajlovima dok druga pretražuje svaki bajt u potrazi za specificiranim tipom fajlova.

Funkcija spasavanja podataka skenira celu sliku diska i ima mogućnost pretrage i ekstrakovanja sledećih tipova fajlova:

- **Arhive**
 - **.ARJ** (*arhiva*)
 - **.ZIP** (*PKZIP arhiva*)
- **Slike**
 - **.GIF** (*Graphics Interchange Format picture*)
 - **.JPG** (*Joint Photographics Group format picture*)
 - **.PNG** (*Portable Network Graphics format picture*)
 - **.BMP** (*Windows bitmap picture*)
 - **.ART** (*AOL picture*)
- **Filmovi**
 - **.AVI** (*Audio Video digital movie*)
 - **.MPG** (*Motion Picture Group digital movie*)
- **Program za pisanje**
 - **.DOC** (*MS Word v1/2/4/5/6/97*)
 - **.RTF** (*Rich Text Format*)
 - **.WRI** (*Windows Write*)
 - **.WP** (*Word Perfect v5.x*)
- **Tabele**
 - **.XLS** (*MS Excel v3/4/97*)
 - **.WK1** (*Lotus 123 v1/2*)
 - **.WK3** (*Lotus 123 v3*)
 - **.WK4** (*Lotus 123 v4*)
 - **.WKS** (*MS Works Spreadsheet*)
 - **.DIF** (*Data Interchange Format*)
- **HTML fajlove**
 - **.HTM(L)** (*Hyper Text Markup Language scripts*)
- **Prilagođene formate fajlova (Custom)**
 - **Any**

Upotreba funkcija spasavanja podataka (“Salvage”)

Kada pritisnete na “*Salvage*” funkciju na nivou uređaja bilo kog objekta u Prozoru dokaza prikazaće Vam se sledeći ekran, gde možete podešavati potpise fajlova.

File Signature Setup

Options

Detect Archives
☒ ARJ and ZIP

Detect Images
☒ PNG, GIF, JPG and ART

Detect Movies
☐ AVI and MPG

Detect Word Processing Files
☐ MS DOC 1/2/4/5/6/97, RTF, WRI and WP

Detect Spreadsheets
☐ MS XLS 3/4/97, WK1, WK3, WK4, WKS and DIF

Detect HTML
☐ HTML

Detect Custom Files
☒ C:\WB stuff\ELIX\Samples\Signature.List

File Type	File Ext	Signature	Signature Displacement
☒ MS Access Db	.mdb	00010000537461	1
☒ Outlook Mail Files	.pst	2142444e	1
☒ Meta File Graphic	.wmf	d7cdc69a0000	1
☒ Jpeg Graphic File	.jpg	ffd8ffe000104a464946	1
☒ AOL Graphic File3	.art	4a47030e	1
☒ AOL Graphic File4	.art	4a47040e	1

Load Custom List Edit Custom List Refresh

Salvage Parameters
 Salvage size (Sectors) 340 Salvage Size 170.0Kb

Salvage Type
☒ Sector Boundary
☐ Byte by byte

OK Cancel

Slika 36. Podešavanje funkcija pretrage po potpisu fajla

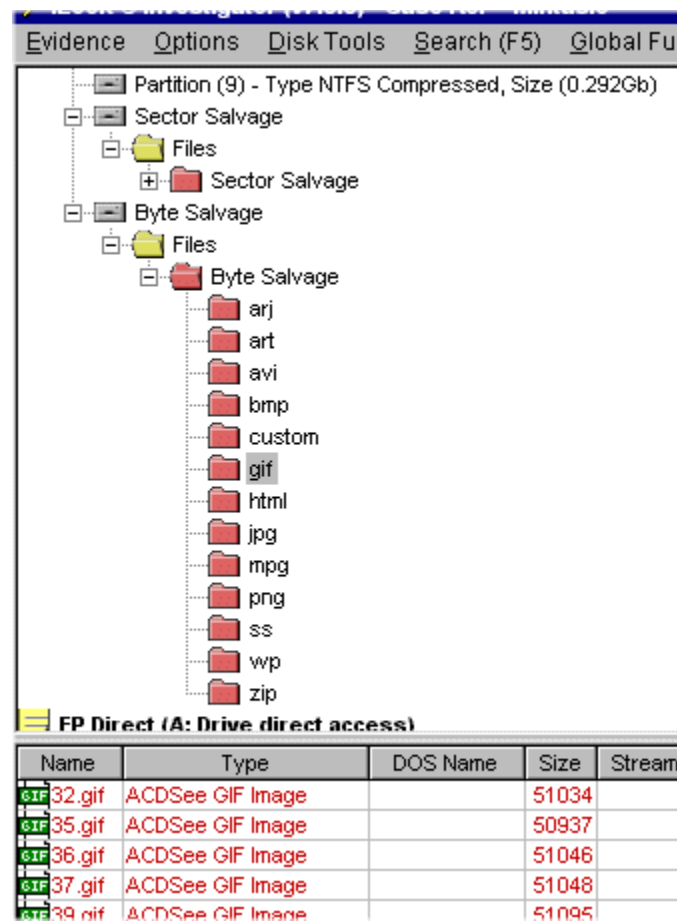
- Izaberite koju grupu fajlova želite da spasete tako što štiklirate kućicu pored naziva tipa fajla. Meni “**Options**” ima mogućnost isključivanja pretrage .BMP fajlova. (Pojavljuje se dosta lažnih pogodaka sa ovim tipom fajlova).
- Meni “**Options**” ima mogućnost izbora pretrage neiskorišćenog prostora u slici diska, ili cele slike diska.
- ILook ima mogućnost specifikacije bilo kojeg potpisa fajla koji želite da uključite u pretragu. Napravite tekstualni fajl i u svaku liniju napišite definiciju potpisa formata fajla. Svaka definicija se sastoji od po pet polja, prva tri polja su obavezna potrebna za normalno funkcionisanje ove funkcije. Prvo polje je opis tipa fajla, drugo je ekstenzija fajla koji želite da ILook koristi kada detektuje ovaj tip fajla, treće polje je sam potpis fajla, četvrto (opciono) je pomeraj zaglavlja fajla unutar podataka (do defaultu je 1), i peto (opciono) je potpis footera fajla. Sva polja moraju biti odvojena znakom ; .
- Za primer sa slike biće Vam potrebno sledećih sedam linija u tekstualnom fajlu:

1. MS Access Db;.mdb;00010000537461

2. Outlook Mail Files;.pst;2142444e
 3. Meta File Graphic;.wmf;d7cdc69a0000
 4. Jpeg Graphic File;.jpg;ffd8fffee0001a10;1;ffd9
 5. AOL Graphic File3;.art;4a47030e;1;d0cb0000
 6. AOL Graphic File4;.art;4a47040e;1;cfc7cb
 7. PGP Disk;.pgd;504750644D41494E600100006AF5216F;1
- Učitajte ove definicije u ILook-ovu funkciju za proveru potpisa tako što će te kliknuti na dugme ***“Load Custom List”*** I odabrati Vaš fajl sa definisanim potpisima. Potpisi će se pojaviti u listi ***“Detect Custom Files list”***. Na ovom mestu možete izabrati pojedinačno fajlove koje želite da uključite u proveru potpisa tako što kliknete na kućice pored inena fajla (po *“defaultu”* su sve selektovane). ***“Edit Custom List”*** dugme će otvoriti Vaš lokalni teks editor tako da možete da izmenite Vaš fajl sa listom potpisom. Ukoliko promenite vašu listu potpisa pritisnite dugme ***“Refresh”*** da bi se promene učitale u Ilook.
 - Morate da izaberete I količinu informacije koje moraju biti spašene nakon što se fajl identifikuje, ovo je potrebno zato što svi formati fajlova nemaju podatak o samoj dužini fajla. Ilook će pokušati da ispravno prikupi .BMP, .PNG and .ZIP fajlove ali drugi fajlovi će biti prikupljeni prema veličinama koje su podešene u delu ***“Salvage Parameters”***. Na Vama je da obezbedite dovoljnu veličinu da bi ste pokrili verovatnu veličinu fajla koji spašavate. Odeljak ***“Salvage Parameters”*** sastoji se od skrolbara I 2 indikatora veličina, pomerajući skrolbar povećavamo ili smanjujemo količinu informacija koji će biti ekstrakovani za svaki spašeni fajl. Prvi parametar predstavlja broj sektora koje bi trebalo da fajl sadrži. Drugi parametar predstavlja veličinu fajla u kilobajtima.
 - **PAŽNJA** – Ovaj proces se odnosi na fajlove koji nisu fragmentisani. Pošto nisu dostupne informacije indeksa fajlsistema za ovu operaciju moguće je da podaci koji pripadaju različitim fajlovima budu grupisani u jedan oporavljen fajl.
 - Na kraju, treba da podesite Ilook da li treba da ograniči pretraživanje na granicama sektora ili treba da proveri svaki bajt podataka. Obično fajlovi kreću na granicama sektora i ograničavajući oporavak fajlova na ovaj način, ubrzava proces pretrage i spašavanja podataka. Provera svakog bajta je dugotrajan proces ali yato može pronaći fajlove koji se nalaze unutar drugih fajlova, kao *“Internet cache dumps and mailboxes”*. Izaberite tip pretrage tako što kliknete na odgovarajuću kućicu u delu ***“Salvage Type”***.
 - Kada ste postavili sve parametre pritisnite dugme ***“OK”*** i ILook će pretražiti podatke u odnosu na zadate parametre..
 - Podešavanju parametra možete pristupiti i iz glavnog menija, tako što izaberete ***“Signature Setup”***.

Ilook kreira virtuelnu particiju za obe vrste pretrage i rezultati pretrage se nalaze na tim virtuelnim particijama. Ove particije su smeštene ispod uređaja nad kojim uradite pretragu. Možete da ih vidite iz “Prozora dokaza”), ispod ovih particija može se nalaziti niz foldera, koji su nazvani po spašenom sadržaju. U svakom folderu nalaze se virtuelni fajlovi koji predstavljaju spašene fajlove. Možete pregledati, obeležavati, pretraživati ili raditi sve radnje koje su moguće i nad bilo kojim fajlovima sa mapiranih fajl sistema. Na slici dole prikazana je kako izgleda struktura foldera i fajlova posle pretrage.

Ilook kreira log fajl koji ima naziv **"Log.txt"** u "root"-u strukture foldera svake virtuelne particije pretrage koja ukazuje na kom fizičkom sektoru bilo koji fajl je detektovan, a za bajt po bajt pretragu, koja su odstupanja u okviru sektora na kojem je potpis fajla pronađen.



Slika 37. Podešavanje funkcija pretrage po potpisu fajla

Možete pokrenuti pretragu na nivou particija tako što će te kliknuti desnim dugmetom miša na naziv particije u prozoru dokaza a zatim izabrati potrebnu funkciju. Na ovom nivou pretraga izgubljenih podataka će se vršiti nad nedodeljenim sektorima(praznim prostorom) selektovane particije pretražujući potpise fajlova koje specificirate.

5.17. Pronalaženje stvari uz pomoć pretraživača koji su sastavni deo Ilook-a

Ilook sadrži tri glavna pretraživača. Pristupa im se preko **"Search"** iz glavnog menija ili preko tipke (F5). U zavisnosti od toga šta želite da postignete koristite taj pretraživač. Rezultati pretrage iz bilo koje pretrage smeštaju se u Ilook-ovu bazu podataka pretraga,

tako da možete da ponovo pregledate rezultate pretrage od bilo koje prethodne pretrage a da ne uključujete pretragu ispočetka.

- **“Slack”** - prostor na kraju alociranih klastera nekog fajla koji se nalaz iza poslednjeg bajta podataka fajla pa do kraja alociranih klastera.
- **“Free”** - ssektori u okviru particije koji nisu alocirani nijednom fajlu
- **“Unused”** - sektori na disku koji nisu alocirani nijednoj particiji
- **Standard** – Ovaj pretraživač služi za brza pretraživanja za jedan ili dva pojma pretrage. Postoji mogućnost pretrage “ASCII, Unicode, Hex ili EBCDIC” reči kroz sledeće grupe podataka:
 - Sve podatke koji su pridruženi slučaju (sve fajlove na particijama, “slack” i “free” prostore i “unused” prostor za sve uređaje koji se nalaze u slučaju)
- **Bulk** - Ovaj pretraživač služi za masovne pretrage do 1000 “ASCII” i “Unicode” pojmova pretrage kroz sledeće grupe podataka :
 - Sve podatke koji su pridruženi slučaju (sve fajlove na particijama, “slack” i “free” prostore i “unused” prostor za sve uređaje koji se nalaze u slučaju)
- **Indexed** - Ovaj pretraživač služi za masovne pretrage bilo koje količine pojmova pretrage kroz sledeće grupe podataka:
 - Sve podatke koji su pridruženi slučaju (sve fajlove na particijama, “slack” i “free” prostore i “unused” prostor za sve uređaje koji se nalaze u slučaju)

Tri izgleda ekrana za standardnu, bulk i indeksiranu pretragu

The screenshot shows a 'Data Search' dialog box with the following sections:

- Search Type:** Radio buttons for 'Standard search' (selected), 'Bulk search', and 'Indexed search'.
- Data Groups:** Radio buttons for 'Search all evidence' (selected), 'Search current device', 'Search current partition', 'Search selected folder', and 'Search selected file(s)'.
- Search What ?**: Checkboxes for 'Files + slack' (checked), 'Tagged files + slack', 'Partition free space', and 'Disk unused areas'.
- Search terms:** Two text input fields; the first contains 'shilling'.
- Search term combination:** Radio buttons for 'Or' (selected) and 'And'.
- Terms type:** Radio buttons for 'ASCII' (selected), 'Unicode', 'Hexadecimal', and 'EBCDIC'.
- Options:** Checkboxes for 'Case Sensitive' and 'Allow Wildcards' (checked).
- Buttons:** 'Use Search Bot' (disabled), 'Auto Tag Search Hits' (checked), 'Search', and 'Cancel'.

Slika 38. Podešavanje funkcija pretrage

Data Search

Search Type ☐ Standard search ☒ Bulk search ☐ Indexed search	Data Groups ☒ Search all evidence ☐ Search current device ☐ Search current partition ☐ Search selected folder ☐ Search selected file(s)	Search What ? ☒ Files + slack ☐ Tagged files + slack ☐ Partition free space ☐ Disk unused areas
---	--	---

Standard **Bulk** Indexed

Load

Edit

Bulk Search Results Output Format

☐ Comma Separated Value (.CSV) ☐ Access Database (.MDB)
☒ Report (.HTM)

☒ Clean up output text ?
☒ Display 1st page when ready ?

Search Type
☒ ASCII
☐ Unicode

Hits Returned
☐ Only first hit
☒ All hits

☐ Use Search Bot ☒ Auto Tag Search Hits Search Cancel

Slika 39. Podešavanje funkcija pretrage

Data Search

Search Type ☐ Standard search ☐ Bulk search ☒ Indexed search	Data Groups ☒ Search all evidence ☐ Search current device ☐ Search current partition ☐ Search selected folder ☐ Search selected file(s)	Search What ? ☒ Files + slack ☐ Tagged files + slack ☒ Partition free space ☒ Disk unused areas
---	--	---

Standard Bulk Indexed

ADF889 ADF890 ADF919

Keywords ==>

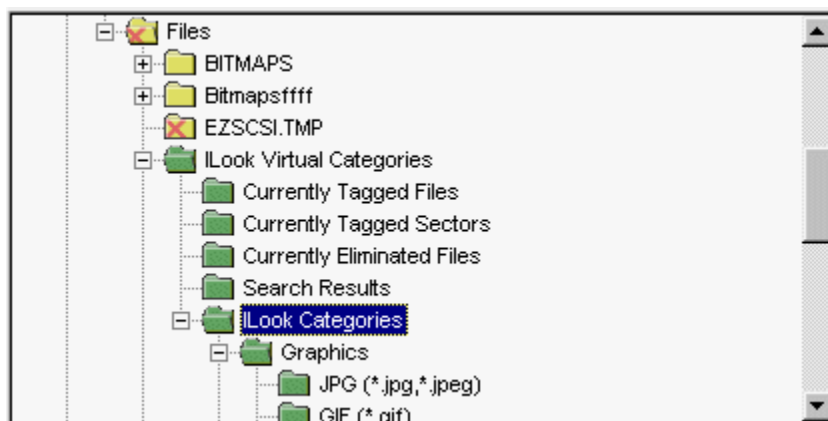
☐ Use Search Bot ☒ Auto Tag Search Hits Search Cancel

Slika 40. Podešavanje funkcija pretrage

5.18. Korišćenje funkcija obeležavanja da bi se napravio set dokaznog materijala (“tagging”)

Ilook poseduje funkciju “tagging” koja pruža mogućnost obeležavanja fajlova, ili grupa sektora koje želite da zapamtite i za koje želite da napišete neki komentar. “Tagging” nam pruža mogućnost brzog i lakog metoda pravljenja seta dokaza koji želimo da pribeležimo radi daljeg procesiranja.

Možete brzo pregledati trenutno eliminisane fajlove, obeležene fajlove i obeležene sektore za bilo koji dokazni objekat tako što se klikne na traženi virtuelni folder koji Ilook smešta u “root” folder svake mapirane particije (ti folderi su obeleženi zelenom bojom).



Slika 41. Podešavanje funkcija pretrage

- **Currently Eliminated Files(Trenutno eliminisani fajlovi)** – lista svih fajlova eliminisanih iz selektovane particije. Eliminirani fajlovi se mogu oporaviti iz ove liste.
- **Currently Tagged Files(Trenutno obeleženi fajlovi)** – lista svih obeleženih fajlova u selektovanoj particiji..
- **Currently Tagged Sectors(Trenutno obeleženi sektori)** – lista svih obeleženih grupa sektora za selektovani dokazni objekat.

Funkcija “**Tag / Untag**” nalazi se na kontekstni menijima koji se otvaraju desnim klikom miša u okviru “File Window” I “Results Window”. Može se obeležiti ili skinuti obeležavanje sa više fajlova odjednom. Zatim Ilook nam nudi polje u koje možemo upisati neki komentar. Po “default”-u, obeleženi fajlovi se prikazuju sa svetlo žutom pozadinom. Skraćenica za obeležavanje fajlova je CTRL+T.

Funkcije koje se mogu raditi nad obeleženim setovima fajlova

1. Prvo što se može uraditi sa obeleženim fajlovima je da se ograniči količina podataka koja se pretražuje u bilo kojoj tekstualnoj pretrazi, što nam štedi veliku količinu vremena.
2. Takođe možete ograničiti ekstrakovanje podataka samo na obeležene fajlove. Ovo je naročito korisno kada želite da ekstrajete samo one informacije koje ste obeležili jer su od značaja za tužilaštvo.
3. Na "Global Functions" meniju glavnog menija, pod delom "Global File Lists" nalazi se funkcija "Global Tagged File List". Ova funkcija prikuplja listu svih obeleženih fajlova iz svih mapiranih dokaznih objekata i prikazuje ih u "ResultsWindow"-u, odakle možete da napravite izveštaj i ekstrajete sve tagovane fajlove u slučaju.
4. Desnim klikom miša na dokaz u prozoru dokaza pojavljuje se Ilook-ov forenzički izveštaj ("forensic report"), kojem se pristupa preko funkcije "Forensic Report" pod grupom "Device Reports". Ukoliko pokrenete ILook će kreirati izveštaj za svaku particiju od dokaza koji su obeleženi ("tagged"). Svi obeleženi fajlovi su povezani preko hiperlinkova ("hyperlinked") sa putanjama ekstrajevanih fajlova koji su obeleženi u istrazi. Na ovaj način možete napraviti set dokaza koji za svaki forenzički izveštaj koji zatim možete ekstrajovati, narezati na disk i predstaviti sudu.
5. Na meniju "Global Functions" glavnog menija, pod izveštajima ("Reports") nalazi se funkcija Forenzički izveštaj ("Forensic Report"). Ukoliko pokrenete Ukoliko pokrenete ILook će kreirati izveštaj za svaku particiju od dokaza koji su obeleženi ("tagged"). Svi obeleženi fajlovi su povezani preko hiperlinkova ("hyperlinked") sa putanjama ekstrajevanih fajlova koji su obeleženi u istrazi. Na ovaj način možete napraviti set dokaza koji za svaki forenzički izveštaj koji zatim možete ekstrajovati, narezati na disk i predstaviti sudu.

Obeležavanje sektora ili grupe sektora

Sektore možete obeležiti sa dva različita mesta, prvo je iz **Prozora Rezultata ("ResultsWindow")** gde bilo koji sektor koji je prikazan posle pretrage možete obeležiti kao i bilo koji fajl. Drugi način je da zadate naredbu preko funkcije **"Tag Disk Sector(s)"** koja se nalazi u podmeniju **"Sector Functions"** na nivou uređaja tako što kliknete desnim dugmetom miša na uređaj. Ova funkcija ima mogućnost pojedinačnog ili grupnog obeležavanja sektora.

- **10** – bilo koji broj sektora (*displacement*)
- **10-31** – raspon sektora (*start displacement to end displacement*)
- **10 for 40** – raspon sektora (*start displacement for a given number of sectors*)

Obeležene sektore možete vratiti u normalu tako što kliknete desnim dugmetom miša na željene sektore koji se nalaze u virtuelnom folderu "**Currently Tagged Sectors**" i izaberete funkciju untag.

6. Windows Thumbnail cache

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

Windows smešta thumbnail-ove grafičkih fajlova, i određenih dokumenata kao i filmova u Thumbnail Cache fajl, uključujući i sledeće formate: JPEG, BMP, GIF, PNG, TIFF, AVI, PDF, PPT and HTML.

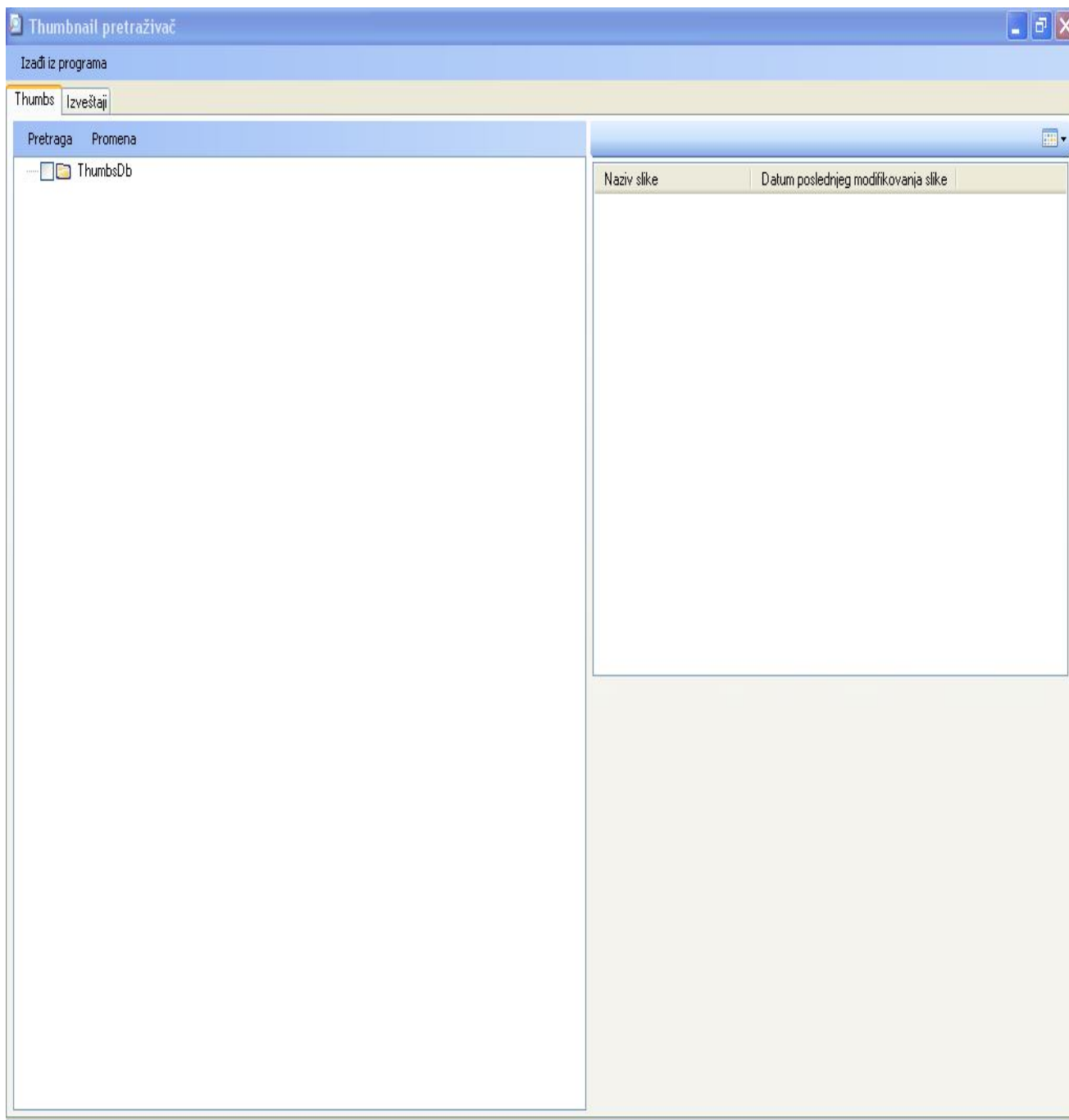
6.1. Thumbs.db

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, nalazi se među slikama. 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 slika koje se nalaze u direktorijumu. Ove slike se smanjuju na maksimalno 96×96 pixels, ili na proporcionalnu minijaturu njihovog originalnog oblika(ovo je kod slika koje nisu kvadratnog oblika) sa 96 pixels na dužoj strani. Svaki folder u kojem su fajlovi prikazani kao Thumbnails or Filmstrip u Windows Exploreru sadržaće i Thumbs.db fajl. Thumbs.db fajl je "OLE Compound Document format". Ovaj format koriste mnogi Microsoft Office proizvodi.

7. Thumbnail pretraživač

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

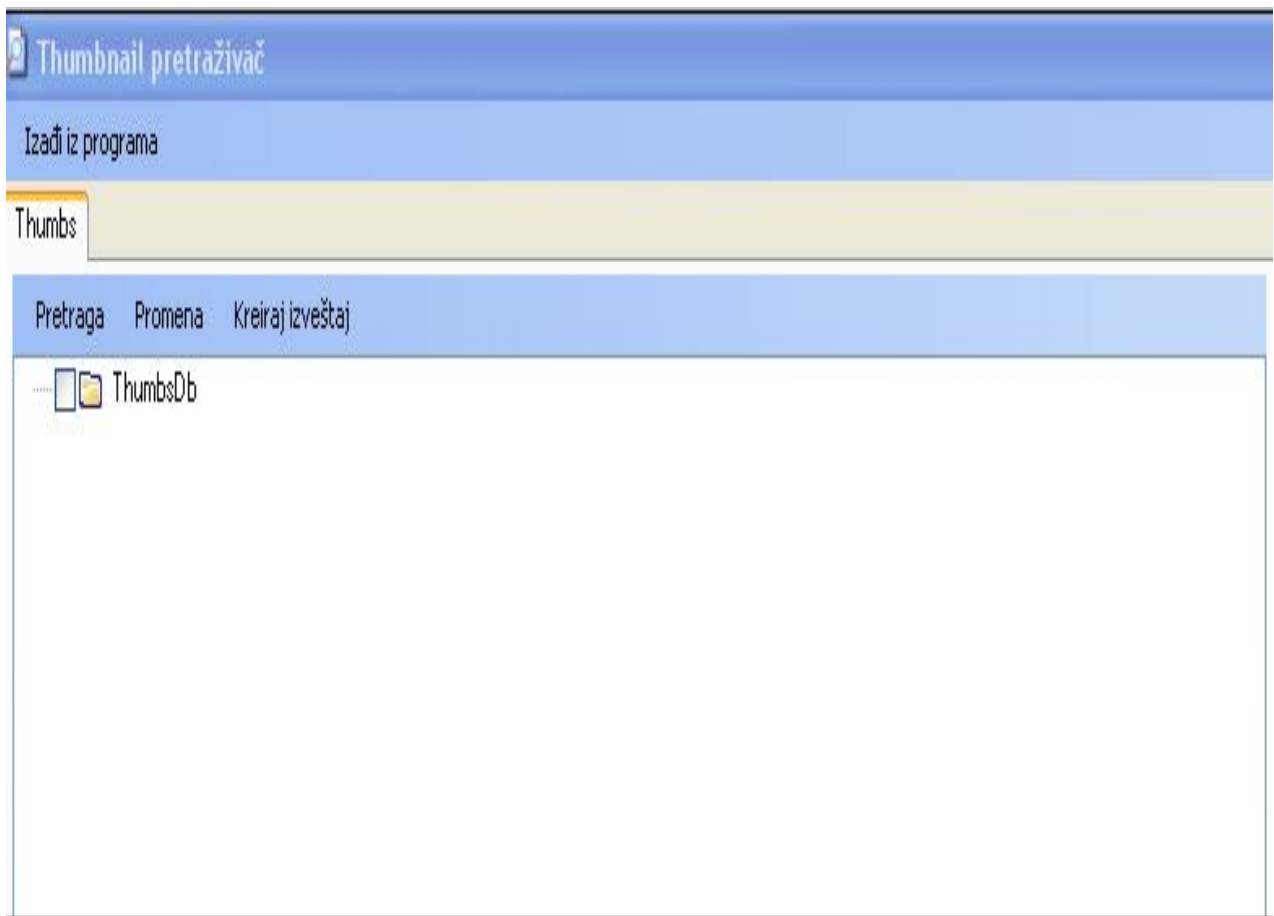
7.1.Početni ekran



Slika 42. Početni ekran alata Thumbnail pretraživač

Ekran Thumbnail pretraživača je podeljen na tri dela:

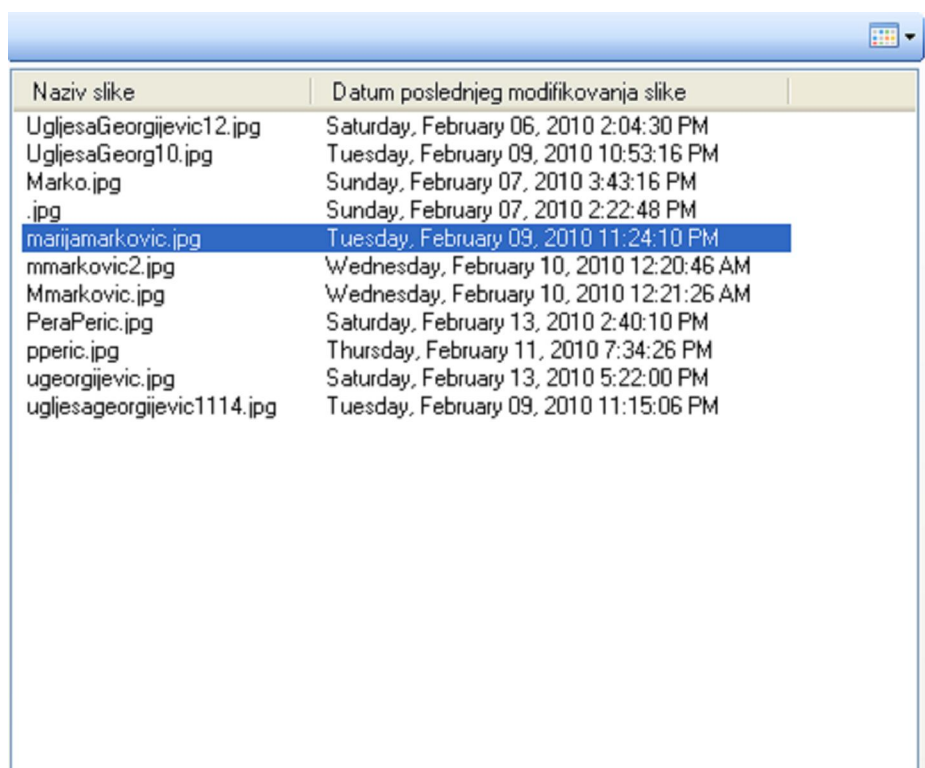
1. Prozor za pregledanje Thumbs.db fajlova (Slika 1.)
2. Prozor za pregledanje sadržaja pojedinačnog Thumbs.db fajla (Pregledanje malih slika iz fajla Slika 2.)
3. Panel za prikaz (koji prikazuje uvećanu kopiju male slike (Slika 3.))



Slika 43. Prozor za pregledanje Thumbs.db fajlova

U desnom gornjem uglu prozora za pregledanje Thumbs.db fajlova imamo osnovne funkcije programa:

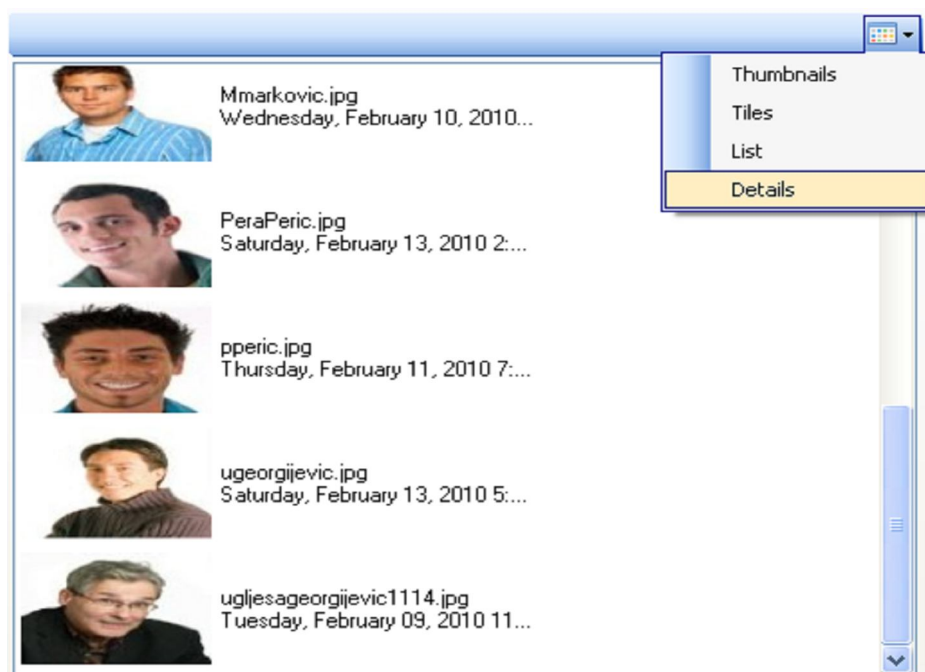
- **Pretraga**
- **Promena**
- **Kreiraj izveštaj**



Naziv slike	Datum poslednjeg modifikovanja slike
UgljesaGeorgijevic12.jpg	Saturday, February 06, 2010 2:04:30 PM
UgljesaGeorg10.jpg	Tuesday, February 09, 2010 10:53:16 PM
Marko.jpg	Sunday, February 07, 2010 3:43:16 PM
.jpg	Sunday, February 07, 2010 2:22:48 PM
marijemarkovic.jpg	Tuesday, February 09, 2010 11:24:10 PM
mmarkovic2.jpg	Wednesday, February 10, 2010 12:20:46 AM
Mmarkovic.jpg	Wednesday, February 10, 2010 12:21:26 AM
PeraPeric.jpg	Saturday, February 13, 2010 2:40:10 PM
pperic.jpg	Thursday, February 11, 2010 7:34:26 PM
ugeorgijevic.jpg	Saturday, February 13, 2010 5:22:00 PM
ugljesageorgijevic1114.jpg	Tuesday, February 09, 2010 11:15:06 PM

Slika 44. Prozor za pregledanje sadržaja pojedinačnog Thumbs.db fajla

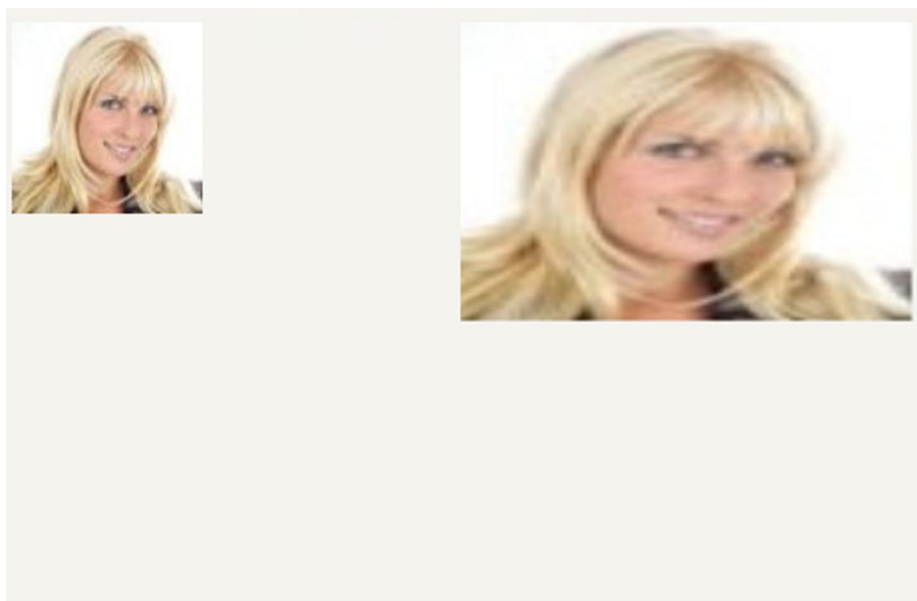
U prozoru za pregledanje sadržaja pojedinačnog Thumbs.db fajla nalaze se informacije vezane za nazive fajlova koji se nalaze u Thumbs.db fajlu (kao što se vidi sa slike postoji naziv fajla, Datum i vreme poslednjeg modifikovanja fajla(slike)). U ovom prozoru možemo i da podešavamo prikaz pregledanja fajlova, klikom na ikonicu u gornjem desnom uglu ekrana i izborom jedne od opcija kao na slici:



Slika 43. Prozor za pregledanje Thumbs.db fajlova sortiranu sa "Tiles"

Od opcija prikaza fajlova na raspolaganju su nam:

- Thumbnails
- Tiles
- List
- Details



Slika 43. Panel za prikaz

Kao što i samo ime govori u ovom panelu se prikazuju fajlovi izabrani iz prozora za pregledanje pojedinačnih fajlova i to u originalnoj veličini u kojoj Windows smešta prikaze u Thumbs.db fajlove i u dva puta većem formatu.

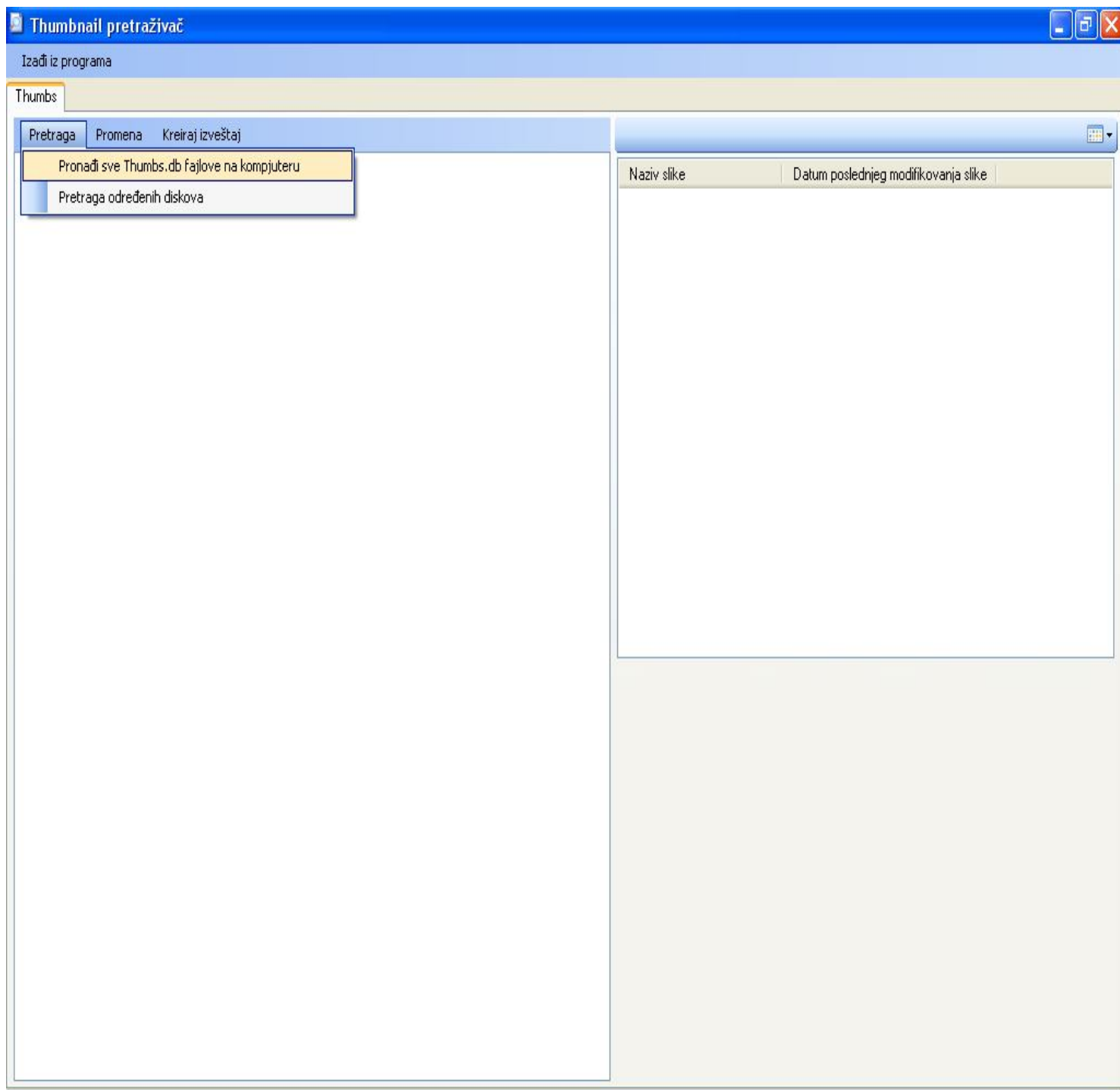
7.2.Funkcije Thumbnail pretraživača

- **Pretraga**
- **Promena**
- **Kreiraj izveštaj**

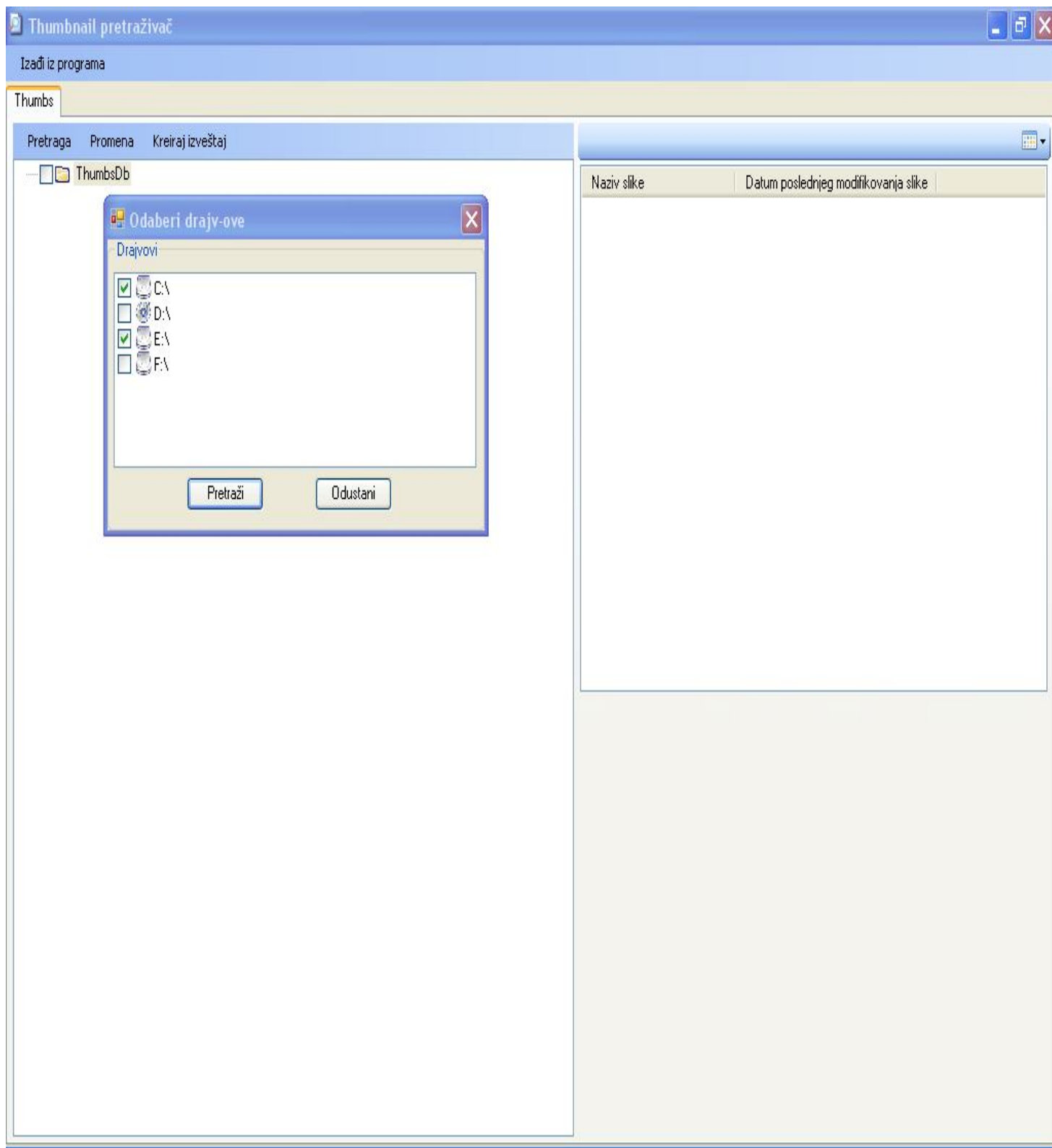
7.2.1. Pretraga

Izborom opcije pretraga prikazuje nam se padajući meni u kojem imamo da odaberemo 2 vrste pretraga:

1. pretraga svih uređaja sa kompjutera (svih hard diskova, cd-ova, usb-uređaja koji su prikazani na kompjuter) sl.1
2. pretraga određenih delova kompjutera sl.2

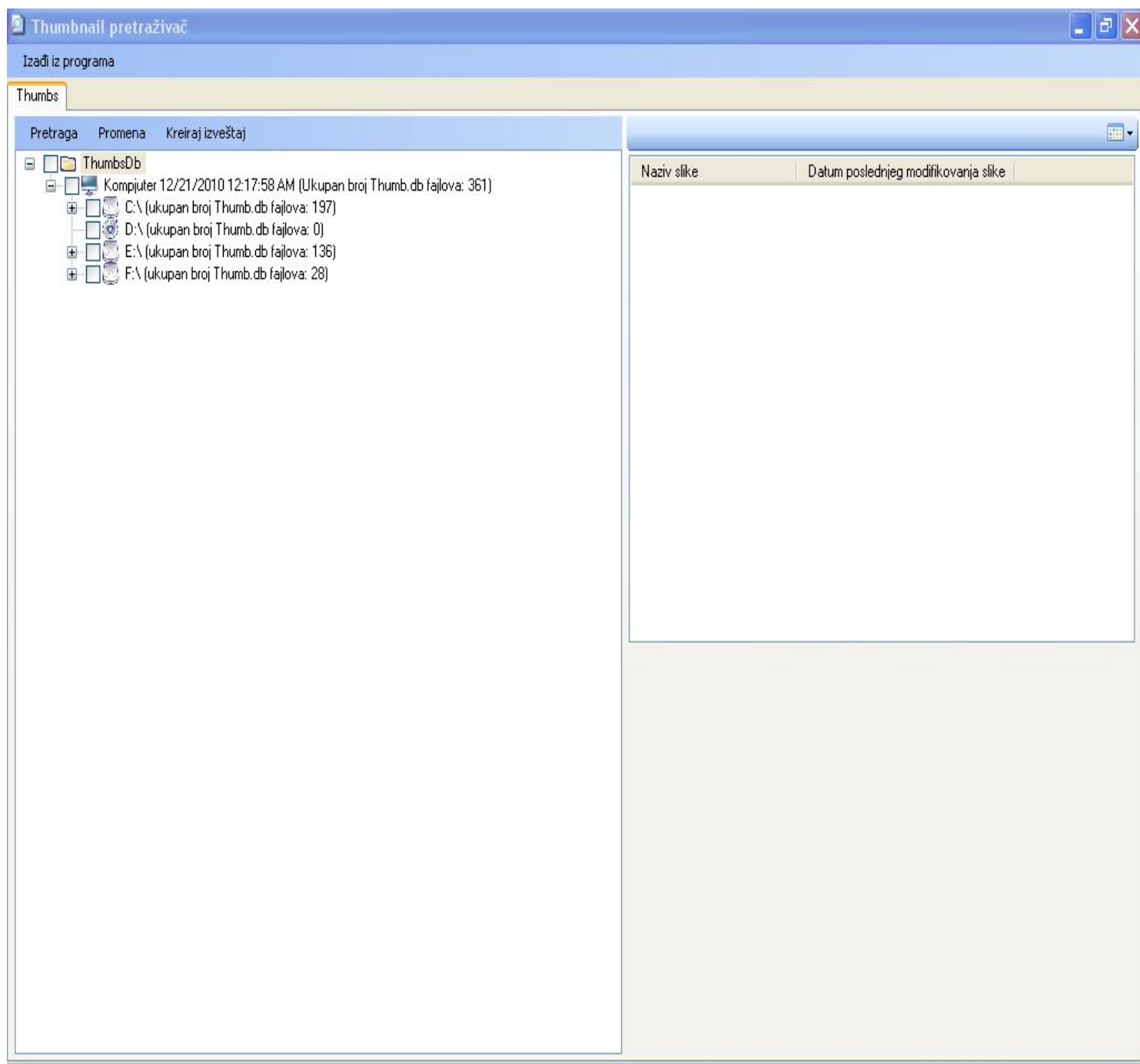


Slika 44. Pretraga svih uređaja



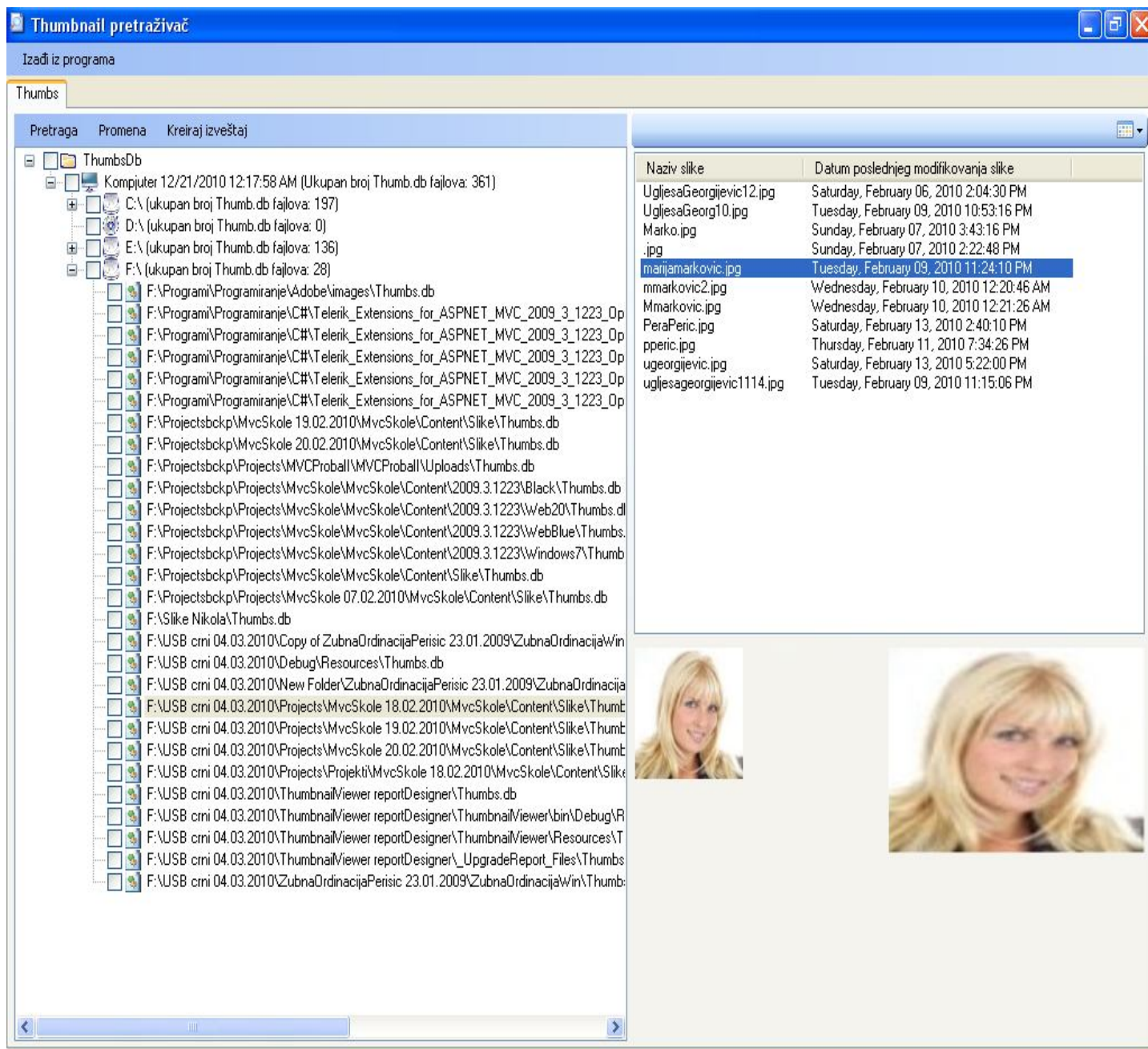
Slika 45. Pretraga određenih delova kompjutera

Posle izabranih opcija sledi prikaz pretrage:



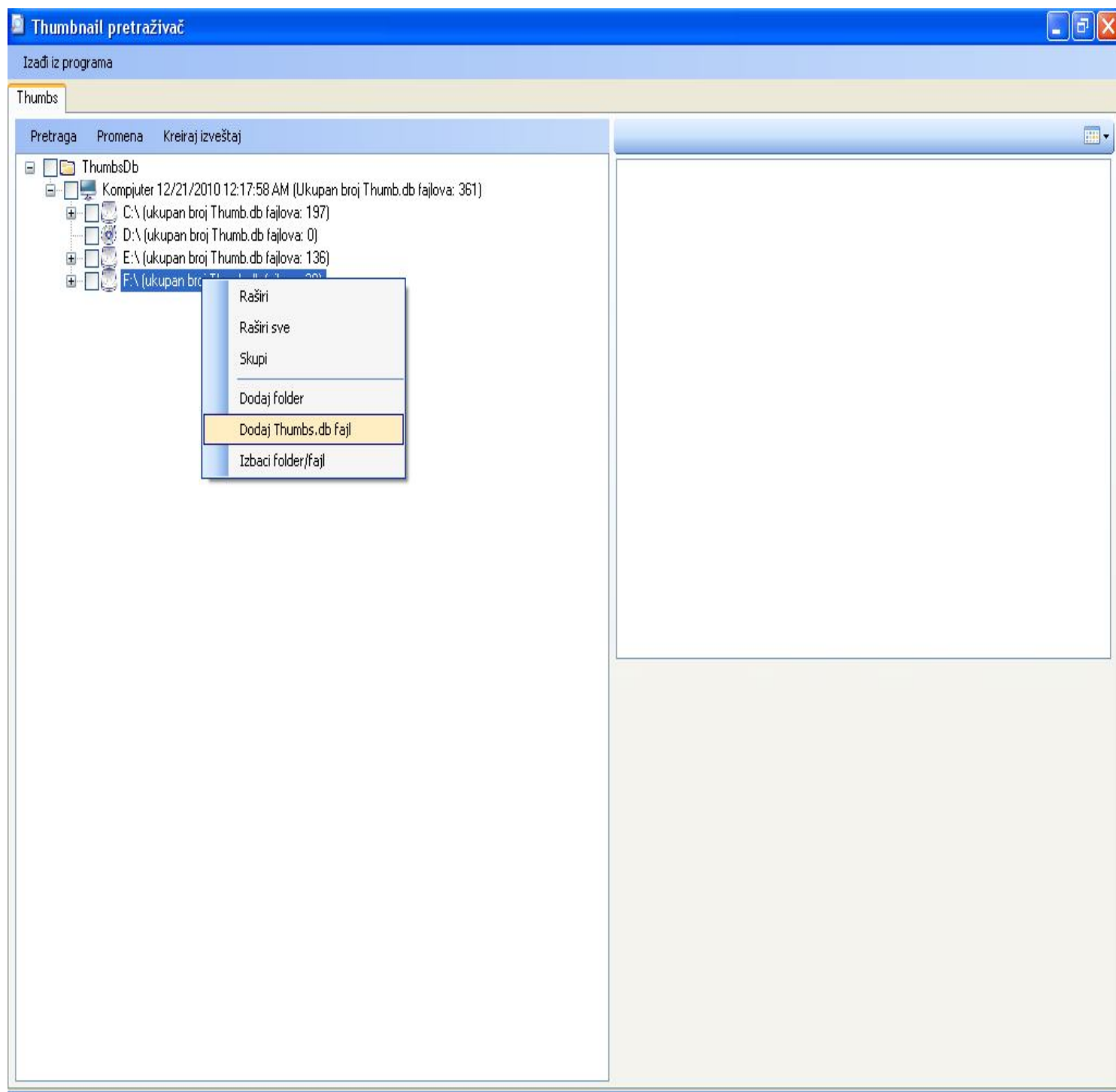
Slika 46. Rezultati pretrage

Prikazuje 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 tj u Prozoru za pregledanje sadržaja pojedinačnog Thumbs.db fajla (Pregledanje malih slika iz fajla Slika 2.). Prikazuje se naziv slike (fajla) i vreme kada je slika (fajl) poslednji put bio modifikovan, a u donjem desnom delu prozora Panel prikazuje nam se thumbnail slika kao i njena uvećana verzija (Sl.4).



Slika 47. Rezultati pretrage

7.2.2. Funkcije promena

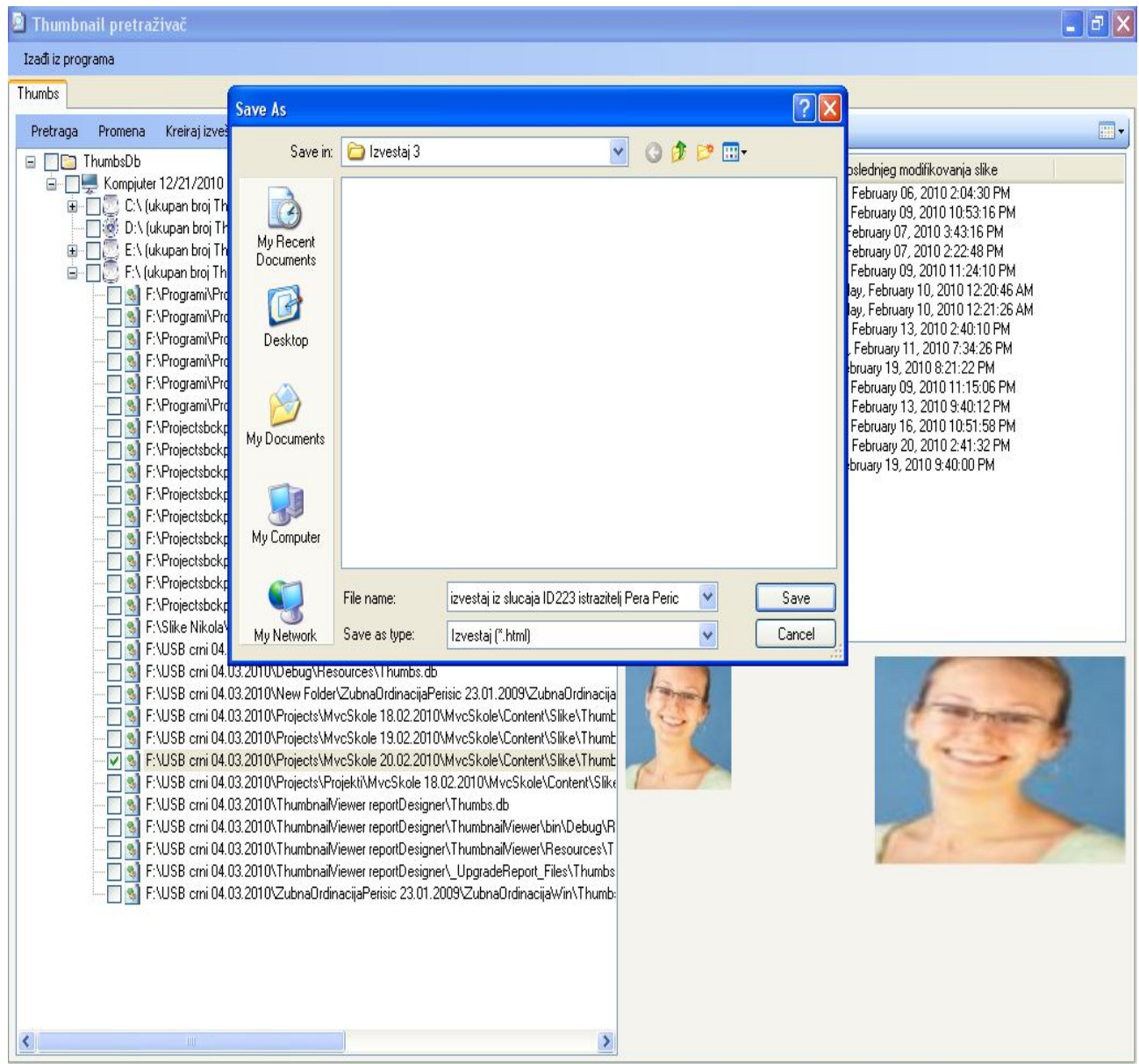


Slika 48. Funkcije “Promena”

Funkcije promena se odnose na kreiranje strukture stabla foldera i naziva foldera u toku istrage(Dodavanje foldera, izbacivanje istih kao i dodavanje novih Thumbs.db fajlova koji se tiču slučaja). Ove funkcije nam omogućavaju organizovanje fajlova i foldera radi lakše pretrage i pregleda fajlova.

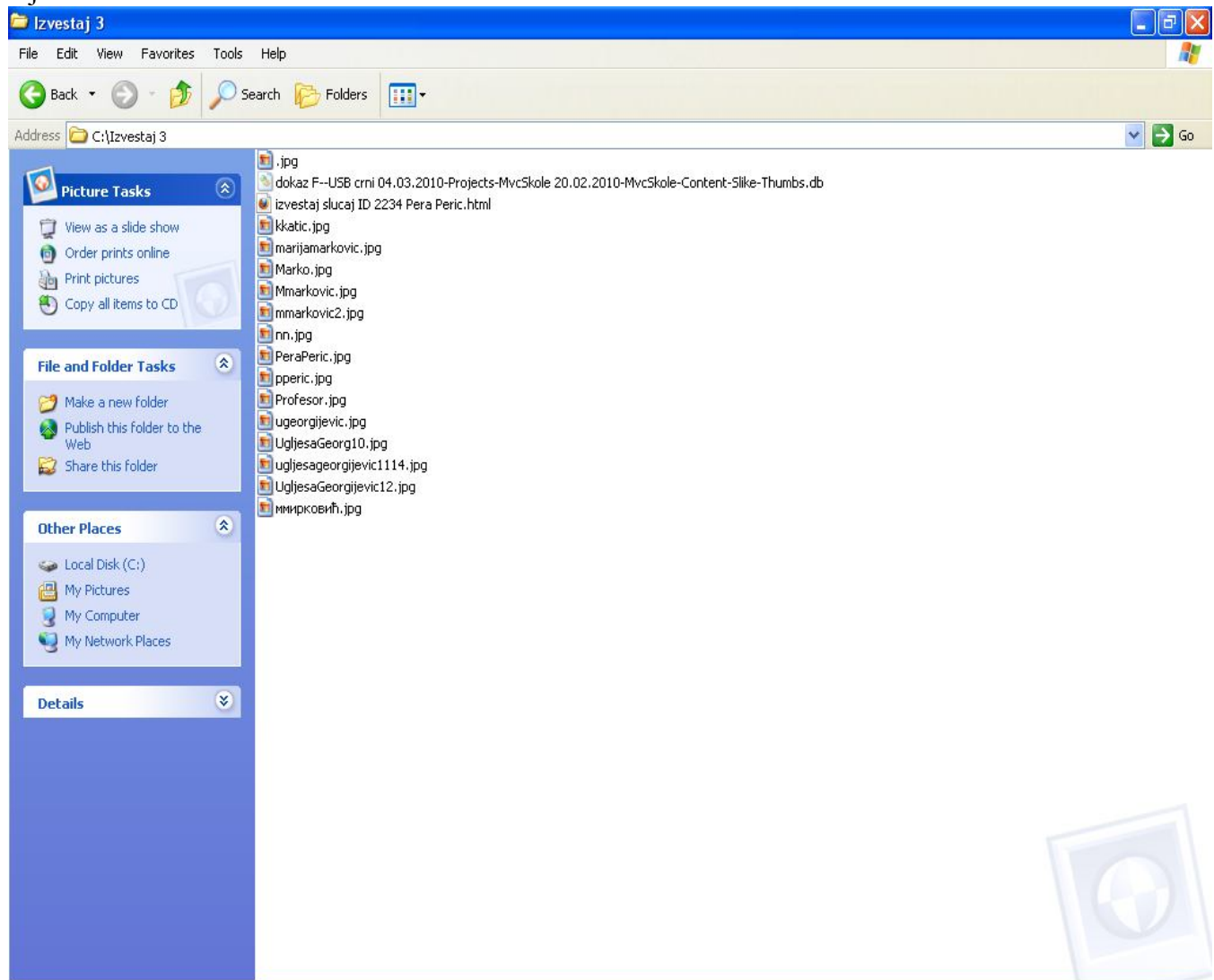
7.2.3. Funkcija Kreiraj izveštaj

Kreiranje izveštaja se vrši tako što se u Prozoru pretrage Thumbs.db fajlova pored naziva fajla, koji su od interesa za istragu, štiklira polje, zatim, izborom funkcije kreiraj izveštaj otvara nam se fajl prozor u kojem biramo destinaciju kreiranja izveštaja kao i naziv samog izveštaja.



Slika 49. Funkcije “Kreiraj izveštaj”

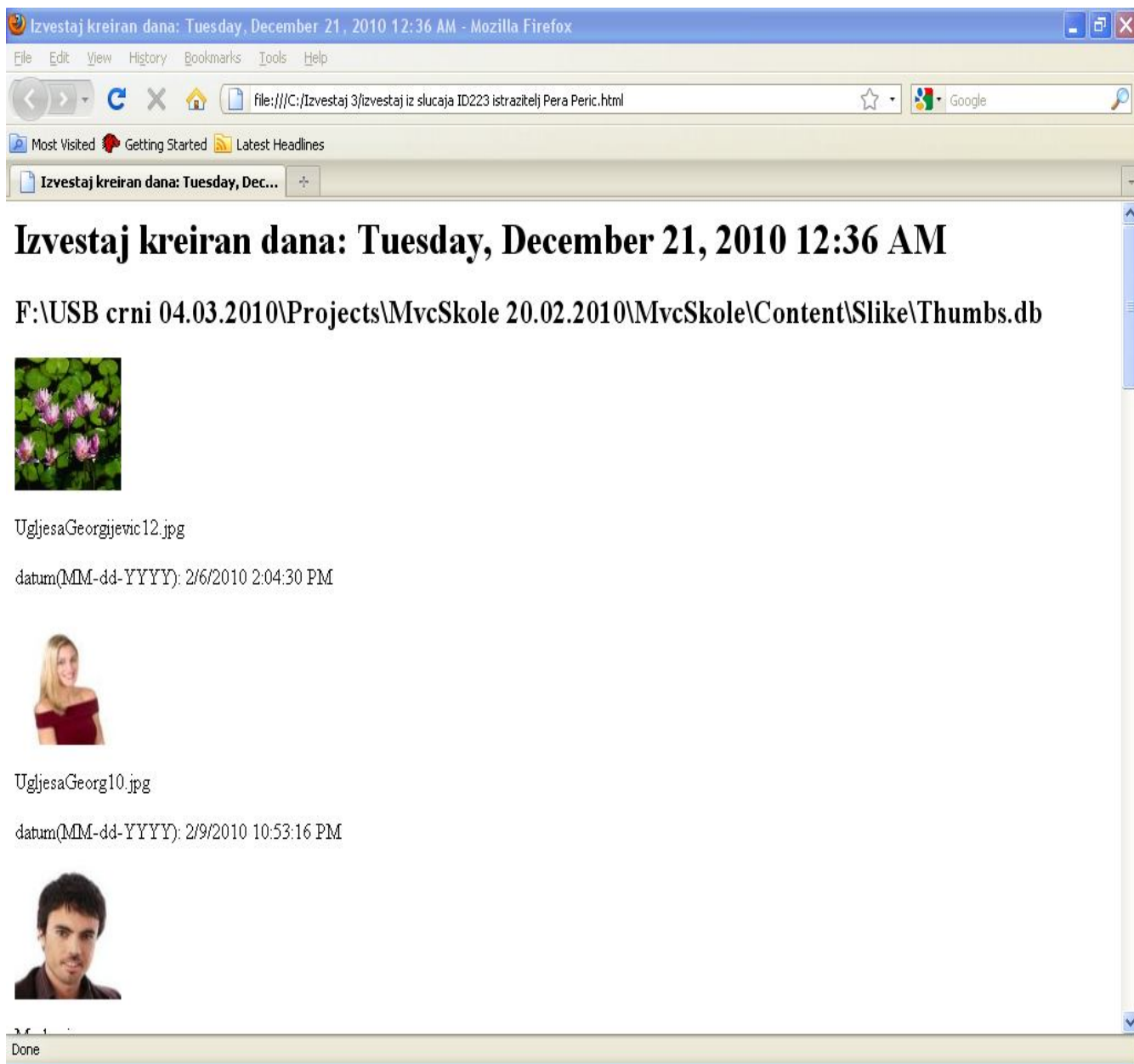
Pritiskom na dugme “Save”, alat kreira izveštaj u izabranom folderu, snima u folder sve slike koje se nalaze u izabranim Thumbs.db fajlovima, i snima izabrane Thumbs.db fajlove u isti folder.



Slika 50. Sadržaj foldera u kojem je napravljen izveštaj

Izveštaj se kreira u formi html-a tako da se može pregledati iz bilo kog Browser-a. Ovako pripremljen izveštaj može se narezati na CD ili prebaciti na neki drugi uređaj radi prikazivanja pri svedočenju.

Izveštaj se automatski prikazuje u Web Browseru nakon pritiska dugmeta “Save”.



Slika 51. Izgled izveštaja

8. Zaključak

Integrirani 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 dokaze 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. Na primer, mnogi interventni timovi za odgovor na incident nemaju zvanične procedure za analiziranje fizičkog prostora oko kompromitovanog servera. U stvarnosti neki nezadovoljni sistem administrator koji ima fizički pristup sistemu, mogao bi sam da izazove incident. 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. Na primer, *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. Slično tome, 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.

9. Literatura

1. Access Data: Forensic Toolkit. Available at: <http://www.accessdata.com/>
2. ASR Data Acquisition and Analysis: SMART. Available at: <http://www.asrdata.com/>
3. Brian Carrier. Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. *International Journal of Digital Evidence*, Winter 2003
4. Brian Carrier. The Sleuth Kit. Available at: <http://www.sleuthkit.org/>
5. David Mills. Network Time Protocol (Version 3). Network Working Group RFC 1305, March 1992.
6. Electronic Crime Scene Investigation: A Guide for First Responders. Available at: <http://www.ncjrs.org>, July 2001.
7. Elliot Spencer *ILook Investigator* <<http://www.ilook-forensics.org>>
8. Eoghan Casey. *Digital Evidence and Computer Crime*. Academic Press, 2000.
9. Eoghan Casey. Error, Uncertainty, and Loss in Digital Evidence. *International Journal of Digital Evidence*, Summer 2002.
10. mr Gojko Grubor . Tema 16: Osnove Kompjuterskog kriminala, Univerziitet Singidunum, Fakultet za poslovnju informatiku.
11. Guidance Software: EnCase Forensic Edition. Available at: <http://www.encase.com/>
12. Henry Lee, Timothy Palmbach, and Marilyn Miller. *Henry Lee's Crime Scene Handbook*. Academic Press, 2001.
13. i2 Ltd: Analyst's Notebook. Available at: <http://www.i2.co.uk/>
14. John Tan. Forensic Readiness. Technical report, @stake, 2001. [28] Brent Turvey. *Criminal*
15. Richard Saferstein. *Criminalistics: An Introduction to Forensic Science*. Pearson, 7 edition, 2000.
16. Ron Rivest. The MD5 Message-Digest Algorithm. Network Working Group RFC 1321, April 1992.
17. Steve Bunting, William Wei, *Encase Certified Examiner Study Guide*. Willey publishing, 2006
18. Secure Hash Standard. National Institute of Standards and Technology, FIPS PUB 180, May1993.
19. Stuart James and Jon Nordby, editors. *Forensic Science: An Introduction to Scientific and Investigative Techniques*. CRC Press, 2003.
20. Tim Grance, Suzanne Chevalier, Karen Kent, Hung Dang, *Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response*, National Institute of Standards and Technology
21. TechnologyPathways:ProDiscoverDFT. Available at: <http://www.techpathways.com/>

Internet

http://www.forensicswiki.org/wiki/OLE_Compound_File
<http://www.forensicswiki.org/wiki/Thumbs.db>
sc.openoffice.org/compdocfileformat.pdf
<http://www.petedavis.net/drupal//index.php?q=node/2>
<http://www.x-ways.net/winhex/manual.pdf>
http://www.dmares.com/maresware/linksto_forensic_tools.htm

PRILOG 1

Operativni sistem	Karakteristike	Procedure gašenja
DOS	Tekst na crnoj pozadini ekrana, obično crne boje. Prompt se sastoji od slova drajvova, kosih crta (backslashes), i obično znaka >; npr, C:\>	Fotografišite ekran i pribeležite sve programe koji su vidljivi da rade ili poruke koje se nalaze trenutno na ekranu. Izvucite kabl za napajanje sa zadnje strane kompjutera.
Windows 3.1	Program menadzer je umesto Windows explorera. Obojena naslovna traka. Standard meni.	Fotografišite ekran i pribeležite sve programe koji su vidljivi da rade ili poruke koje se nalaze trenutno na ekranu. Izvucite kabl za napajanje sa zadnje strane kompjutera.
Windows 95	Start dugme je sa Windows simbolom.	Fotografišite ekran i pribeležite sve programe koji su vidljivi da rade ili poruke koje se nalaze trenutno na ekranu. Izvucite kabl za napajanje sa zadnje strane kompjutera.
Windows NT Workstation	Start dugme je sa Windows simbolom.	Fotografišite ekran i pribeležite sve programe koji su vidljivi da rade ili poruke koje se nalaze trenutno na ekranu. Izvucite kabl za napajanje sa zadnje strane kompjutera.
Windows NT Server	Start dugme je sa Windows simbolom.	Fotografišite ekran i pribeležite sve programe koji su vidljivi da rade ili poruke koje se nalaze trenutno na ekranu. Koristite normalnu proceduru za isključivanje kompjutera.
Windows 98/Me	Start dugme je sa Windows simbolom.	Fotografišite ekran i pribeležite sve programe koji su vidljivi da rade ili poruke koje se nalaze trenutno na ekranu. Izvucite kabl za napajanje sa zadnje strane kompjutera.

Windows 2000	Start dugme je sa Windows simbolom.	Fotografišite ekran i pribeležite sve programe koji su vidljivi da rade ili poruke koje se nalaze trenutno na ekranu. Izvucite kabl za napajanje sa zadnje strane kompjutera.
Windows 2000 Server	Start dugme je sa Windows simbolom.	Fotografišite ekran i pribeležite sve programe koji su vidljivi da rade ili poruke koje se nalaze trenutno na ekranu. Koristite normalnu proceduru za isključivanje kompjutera.
Windows XP	Zeleno Start dugme sa Windows simbolom.	Fotografišite ekran i pribeležite sve programe koji su vidljivi da rade ili poruke koje se nalaze trenutno na ekranu. Izvucite kabl za napajanje sa zadnje strane kompjutera.
Windows 2003 Server	Zeleno Start dugme sa Windows simbolom.	Fotografišite ekran i pribeležite sve programe koji su vidljivi da rade ili poruke koje se nalaze trenutno na ekranu. Koristite normalnu proceduru za isključivanje kompjutera.
Linux/Unix	Ukoliko postoji grafičko okruženje (GUI), potražite (pogledom) Start dugme sa simbolom verzije Linux/Unix ili njihove ikone, kao što su “red hat” ili “fedora” itd. Ukoliko ne postoji grafičko okruženje već je konzolna verzija vidite da li postoji prompt u sledećem obliku: [root@localhost root]# [user@host dir]\$	Fotografišite ekran i pribeležite sve programe koji su vidljivi da rade ili poruke koje se nalaze trenutno na ekranu. Koristite normalnu proceduru za isključivanje kompjutera. U mnogim slučajevima korisnik mora biti root da bi isključio sistem. Ukoliko ste u grafičkom okruženju desni klik miša na desktop površinu i iz kontekstnog menija izaberite Console ili Terminal. Pogledajte da li u konzoli na levom kraju ekrana postoji znak #.

		Ukoliko ne posotji upisite su root. Pitaće vas za šifru. Ukoliko je imate upisite je. Ukoliko nemate moraćete da isključite sistem fizički izvlačenjem kabla za napajanje iz kućišta. Ukoliko ste ipak ušli kao root ukucajte synch;synch;halt i sistem bi trebao da stane.
Macintosh	Apple simbol se nalazi u gornjem levom uglu.	Fotografišite ekran i pribeležite sve programe koji su vidljivi da rade ili poruke koje se nalaze trenutno na ekranu. Zabeležite vreme sa meni linije i simultano zabeležite stanadrdno vreme. Ukoliko Mac radi na OS X, BSD (Linux varijanta) radi kao podsistem. Takođe Mac može raditi kao server (Web server, server baze podataka i e-mail server, itd...). Ukoliko je neki od servera podignut na Mac-u normalna procedura gašenja je sigurnija vearijanta. Za OSX, pritisnite „Apple“ ikonicu i izaberite „ShutDown“ i pitaće vas da potvrdite. Stariji Mac-ovi, pritisnite „Special“ pa onda „ShutDown“. Kada se ugasi izvucite kabl za napajanje.