

UNIVERZITET „SINGIDUNUM”

**Departman za poslediplomske
MASTER STUDIJE**

**Studijski program:
Savremene informacione tehnologije**

**Forenzika USB i Compact Flash memorijskih
uređaja**

Mentor:
dr Gojko Grubor

Kandidat:
Tasić Aleksandar
M9394/08

Sažetak

Računarska tehnologija je najmoćnija i najfleksibilnija tehnologija ikada smišljena. Upravo iz ovog razloga, računarstvo je promenilo sve: gde i kako radimo, gde i kako učimo, kupujemo, glasamo, koristimo medicinske usluge, provodimo slobodno vreme, ratujemo, družimo se, ali je dovelo i do pojave novih motiva – napada na informacione sisteme, na privatnost, ali i teške zločine. Razvoj prenosivih memorija, posebno USB fleš i prenosivih kartica, doveo je do menjanja mesta gde se digitalni dokaz može naći. Iz straha, s'jedne strane, a intelektualnog rivalstva s'druge, dolazi do eksplozije interesa za digitalnu istragu prenosivih memorija, samim tim poznavanje načina njihovog rada i mogućnosti.

U slučajevima bezbednosnih incidenata, u koje su uključene prenosive memorije, pravilno prikupljanje relevantnih podataka može značajno povećati verovatnoću dolaženja do informacija o tome ko je izvršilac napada, odakle je napad izvršen, na koji način je napad izvršen i sl. Stalno praćenje noviteta na polju prenosivih memorija omogućava valjanu akviziciju dokaza sa njih. Sve veći broj načina za zaštitu podataka, na njima, otežava i u usporava rad forenzičara i zahteva nova napredna znanja. Digitalni dokazi u mnogo ranjiviji od fizičkih pa je veštom napadaču lakše da ih ukloni, a nepažljivo i nestručno vođenje istrage takođe može dovesti do gubitka ključnih podataka.

Ključne reči: fleš, forenzika, istraga, usb fleš, fleš memorija, memorijske kartice

Naučna oblast: Informatika

Uža naučna oblast: Digitalna forenzika

Abstract

Computer technology is the most powerful and most flexible technology ever developed. From this reason, computing has changed everything: where and how we work, where and how we learn, buy, vote, use of medical services, spend free time, fight, friendship, and led to the appearance of new motives - the attacks on information systems, to privacy, but also serious crimes. Development of portable memory, especially the USB flash card, and memory card, has resulted in changing the place where the digital evidence can be found. From fear, from one side, and intellectual rivalry from another, comes to the explosion of interest in digital investigations portable memory, and the knowledge of how they work and their opportunities.

In the case of security incidents which involving portable memory, regular collection of relevant data can significantly increase the likelihood of obtaining the information about who is the perpetrator of the attack, where the attack was carried out, how the attack was carried out and the like. Constant monitoring of innovations in the field of portable memory acquisition provides valuable evidence on them. An increasing number of ways to protect data on them and makes it difficult and slow down the work of forensic and requires new advanced knowledge. Digital evidence has many more vulnerable of physical and for attacker is easier to remove them, and carelessly and unprofessionally conduct acquisitions may also lead to the loss of important data.

Keywords: flash, forensic, investigation, USB flash, flash memory, memory card

Scientific field: Computer Science

Specific sci-field: digital forensic

Sadržaj:

1	Metodologija naučnog istraživanja	1
1.1	Uvodne napomene	1
1.2	Predmet istraživanja	3
1.3	Hipotetički okvir istraživanja	4
1.4	Ciljevi i zadaci istraživanja	4
1.5	Metodi i tok istraživačkog procesa	5
2	Digitalna forenzika	6
2.1.1	Akvizicija	7
2.1.2	Smernice rada	8
3	USB fleš i CF memorijski uređaji	9
3.1	Fleš memorija	9
3.1.1	Poreklo: istorija i razvoj fleš memorije	10
3.1.2	Principi rada fleš memorije	11
3.1.3	NOR fleš memorija	14
3.1.4	NAND fleš memorija	15
3.1.5	Ograničenja fleš memorije	16
3.1.6	Fleš fajl sistemi	16
3.1.7	Kapacitet fleš memorije	17
3.1.8	Brzina fleš memorije	17
3.1.9	Oštećenje podataka na fleš memoriji	17
3.2	USB fleš	17
3.3	Kompaktne fleš memorijske kartice – CompactFlash	18
3.4	mmC i SD kartice	19
3.4.1	mmC Mobile	20
3.4.2	Mini Secure Digital (SD) kartica	20
3.4.3	MMC (Multi Media Card)	21
3.4.4	Micro SD	21
3.5	Ostali tipovi prenosivih memorijskih uređaja	22
3.5.1	SmartMedia	22
3.5.2	xD-Picture Card	22
3.5.3	IBM Microdrive	23
3.5.4	Sony MemoryStick	23
3.5.5	Disk on module	24
3.5.6	SDXC (eXtended Capacity)	24
4	USB i CF u praksi	25
4.1	Korišćenje USB fleš memorije	25
4.1.1	Prenos ličnih podataka	25
4.1.2	Automatsko prikupljanje podataka	25
4.1.3	Širenje zlonamernog softvera	26
4.1.4	Audio plejeri	26
4.1.5	ReadyBoost	26
4.1.6	Forenzički alat	26
4.2	Korišćenje memorijskih kartica	27
4.2.1	Prenosivi računari	27
4.2.2	Digitalni aprati i kamere	27
4.2.3	Mobilni telefoni, PDA uređaji	27
4.2.4	Čitači memorijskih kartica (Memory Card Reader)	28
4.3	Sigurnost podataka na fleš memorijama	28
5	Forenzika USB i CF uređaja	30

5.1	Utvrđivanje relevantnih činjenica	30
5.2	Izrada procene uspešnosti.....	30
5.3	Kreiranje kopije podataka	30
6	Prikupljanje i provera digitalnih dokaza	32
6.1	Pravilno prikupljanje digitalnih dokaza	32
6.1.1	Otkrivanje tipa memorije	33
6.1.2	Pronalaženje odgovarajućeg alata.....	33
6.1.3	Kopiranje podataka	37
6.1.4	Utvrđivanje autentičnosti kopiranih podataka	38
6.1.5	Pravljenje forenzičkih duplikata	40
7	Alati za akviziciju USB i CF memorija	41
7.1	Alati za zaštitu podataka na memorijama USB i CF tipa.....	41
7.1.1	Hardverska zaštita	41
7.1.2	Softverska zaštita	42
7.2	Uobičajni alati za forenzičku akviziciju.....	45
7.2.1	EnCase	46
7.2.2	FTK.....	47
7.2.3	DriveSpy	47
7.2.4	Helix.....	47
7.2.5	Caine	48
7.2.6	Deft	49
7.2.7	dd.....	49
7.2.8	VMware	49
7.2.9	Ostali alati	49
7.2.10	Nenamenski alati u forenzičkoj primeni	51
8	Studije slučaja	53
8.1	Akvizicija podataka sa fleš diska	53
8.1.1	Utvrđivanje tipa memorije	53
8.1.2	Priprema starilinih medija.....	53
8.1.3	Forenzičko kopiranje	54
8.2	Pristup podacima na zaključanim memorijama	55
8.2.1	Otkrivanje zaštite	55
8.2.2	Otključavanje memorije.....	56
8.3	Praćenje USB uređaja povezanih na računar	58
8.3.1	Linux OS.....	59
8.3.2	Windows OS	60
8.3.3	Povratak podataka sa oštećene USB fleš memorije.....	62
8.3.4	TestDisk	63
8.3.5	Recuva.....	64
8.3.6	GetDataBack	65
8.3.7	Stellar Phoenix Windows Data Recovery	66
9	Diskusija dobijenih rezultata.....	68
10	Zaključak.....	70
11	Litratūra.....	71
11.1.1	Neautorizovani izvori	72
11.1.2	E – izvori	72
12	Lista pojmova.....	74

Spisak slika:

Slika 1: Distribucija podataka u 2008 godini.....	1
---	---

Slika 2: Forenzika u istoriji.....	8
Slika 3: Intelov NOR fleš.....	10
Slika 4: NAND fleš firme Infineon.....	11
Slika 5: Arhitektura fleš memorije.....	12
Slika 6: Fleš memorija ugrađena u USB flash drive.....	12
Slika 7: Blok dijagram fleš memorije.....	13
Slika 8: Fleš memorija.....	14
Slika 9: NOR memorijski čipovi.....	14
Slika 10: NAND memorijski cip.....	15
Slika 11: NAND fleš disk (spreman za zamenu sadašnjih hard diskova).....	16
Slika 12: Spoljašnji izgled jednog USB fleša.....	18
Slika 13: CF memorijska kartica.....	19
Slika 14: MMC Mobile kartica i adapter.....	20
Slika 15: Dimenzije Mini SD i SD katiće.....	21
Slika 16: Multi media Card Slika 17: MMC mikro kartica.....	21
Slika 18: Micro SD kartica sa adapterom.....	22
Slika 19: SmartMedia kartica.....	22
Slika 20: xD Picture Card.....	23
Slika 21: IBM microdrive.....	23
Slika 22: Memory Stick PRO Duo i adapter za nju.....	24
Slika 23: Disk on module.....	24
Slika 24: Čitači memorijskih kartica.....	28
Slika 25: Različite veličine istog medija u Windows OS.....	34
Slika 26: UltraBlock USB Write Blocker.....	35
Slika 27: Acelab Flash reader i Soft Center Flash reader.....	36
Slika 28: Forensic duplicator.....	37
Slika 29: Enkripcija flash diska u Windows 7 OS uz pomoć BitLocker tehnologije..	43
Slika 30: Enkriptovan fleš disk u Windows 7 (levo) i Windows XP (desno).....	43
Slika 31: Osnovni prozor programa PenProtect.....	44
Slika 32: Interfejs programa ProDiscover.....	50
Slika 33: Informacije o disku – predmetu istrage.....	53
Slika 34: Priprema sterilnog medija.....	54
Slika 35: Air - Automated Image and Restore interfejs.....	54
Slika 36: Obaveštenje o zaključanoj memoriji.....	56
Slika 37: Pregled fajlova zaključane memorije u alatu WinHex.....	56
Slika 38: Passware Kit Forensic 10.1.....	57
Slika 39: Passware FireWire Memory Imager.....	58
Slika 40: Linux terminal prozor sa informacijama o povezanom fleš disku.....	59
Slika 41: Linux syslog datoteka sa informacijama o povezanom fleš disku.....	59
Slika 42: Windows Device Manager.....	60
Slika 43: Windows XP setupapi.log fajl.....	61
Slika 44: USBDeview.....	61
Slika 45: Podešavanje proizvođačkih unosa.....	62
Slika 46: Izemljeni podaci Transcend fleš diska.....	62
Slika 47: Interfejs programa TestDisk.....	64
Slika 48: Recuva.....	65
Slika 49: Proces oporavka u programu GetDataBack.....	66
Slika 50: Stellar Phoenix Windows Data Recovery.....	67
Slika 51: Easeus Data Recovery.....	67

1 METODOLOGIJA NAUČNOG ISTRAŽIVANJA

1.1 Uvodne napomene

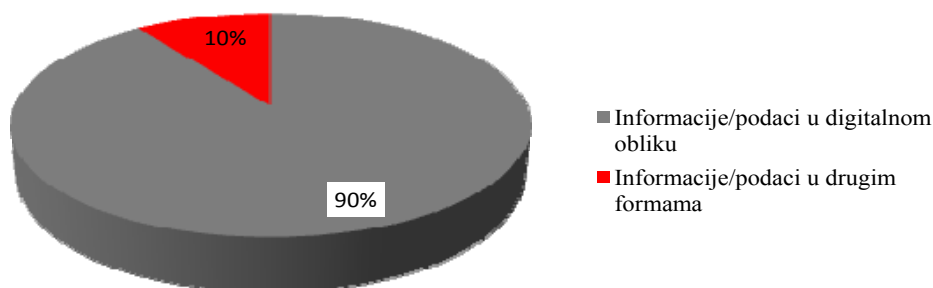
„Tražeći početak, čovek postaje rak. Istoričar gleda unazad;
konačno i veruje unazad.

Hoćeš li da ideš zajedno sa mnom? Ili da ideš predamnom?
Ili sâm za sebe.. Valja znati šta hoćeš, i da hoćeš.”¹

Sve osobine, zbog kojih će čitaoc uočiti ovo delo, objašnjavaju se okolnosti iz kojih je nastalo. Uzimajući u obzir vreme njegovog nastajanja, istraživanje na ovu temu postaje neizbežno. Danas kada su USB flash diskovi postali deo „standardne opreme“, kada se ljudi pre izlaska iz kuće češće pitaju jesu li poneli flash, nego ključeve i kada uzmemo u obzir da je po nekim istraživanja čak 90% informacija distribuirano u elektronskom obliku (slika 1), značaj poznavanja načina funkcionisanja USB memorija predstavlja realnost svakog ko i pokušava da se bavi digitalnom forenzikom.

Distribuiranje informacija i podataka u SAD u 2008.

istraživanje Berkeley Univerziteta



Slika 1: Distribucija podataka u 2008 godini

Dame i gospodo! Ne znamo koliko svaki pojedinac među vama zna o forenzici, flash memorijama i sl. iz vlastitih čitalačkih napora, ili iz priče drugih. Ipak, usuđujemo se pretpostaviti barem toliko, da znate šta je i kako izgleda USB fleš disk, gde se on danas koristi, kao i osnovne elemnte modernih računara ne bi li razumeli rečnik ovog rada. Međutim korisničko iskustvo nije dovoljno, ako se fleš memorijska skladišta gledaju kroz forenzički aspekt. Sve veći broj memorijskih uređaja koji se pojavljuju poslednjih nekoliko godina, primorava kompjuterske forenzičare da se prilagode novonastaloj situaciji. Tome doprinosi podatak da dve od najviše korišćenih tipova memorije jesu compact flash (u daljem tekstu CF) i njima slične kartice i USB flash memorijske kartice (u daljem tekstu USB flash). Iako ne pripadaju standardnim hard diskovima, one lako simuliraju njihov rad, te se sve više podataka, posebno onih privremene prirode nalazi na njima.

¹ Fridrih Niče, Sumrak idola

Forenzika USB i CF uređaja postaje sve više aktuelnost i potreba. Noviteti koji se na ovom polju javljaju skoro svakodnevno, stavljaju ovaj deo računarske forenzike u prvi plan. To što je sve više podataka na ovim memorijama ne bi predstavljalo problem, da nije sve više alata za zaštitu tih podataka, koji na muke stavljaju svakoga ko sa njih treba da prikupi dokaze. Nažalost unapređenja na polju enkripcije koji su doneli mnogi proizvođači hardvera, ali i softvera, nastalih prvenstveno objavljivanjem novih operativnih sistema kompanije Microsoft, nisu ispratili na odgovarajući način kompanije koje se bave izradom alata i softvera za digitalnu forenziku. Mnogi softverski alati koji će biti opisani u radu, nisu „službeni“ (u Republici Srbiji ne postoji zvanično priznat alat za digitalnu forenziku), već predstavljaju često i hakerske načine dolaska do podataka. Postoje različiti izvori koji obrađuju ovu oblast, različiti softverski i hardverski alati. Naša istraživanja imaju okvir propisanih načela vezanih za ostale vidove memorijskih uređaja, a primeri iz prakse potvrđuju su da se tih načela treba držati i kada se radi sa prenosivim memorijama.

U prvom delu – **Uvod** izneli smo razloge našeg istraživanja, osnovne metodološke postavke, ukazali na značaj i aktuelnost istraživanja, a zatim izneli **Predmet istraživanja**, ustanovili ciljeve i polazišta, postavili hipoteze i opisali strukturu rada.

Drugi deo koji nosi naziv **Digitalna forenzika** objašnjava koja su polja istraživanja i čime se bavi ta naučna disciplina. Kroz primere korišćenja, pokazali smo u kojim je segmentima danas prisutna digitalna forenzika, a zatim koje su tendencije njenog razvoja u svetu i kod nas.

Treći deo **USB fleš i CF memorijski uređaji** – analizira tok razvoja fleš memorija, i razloge njihovog omasovljivanja. Zatim se daje jasan uvid u način rada fleš memorije, kao osnove memorijskih uređaja koje obrađujemo. Posle toga posmatramo zasebno sve danas popularne formate prenosivih memorija. Najpre se daje uvid u rad USB memorija, zatim Compact Flash, a na kraju ostalih vidova fleš memorija, koji mogu biti predmet forenzičke istrage. Kroz uvođenje u izgled i elemente memorija date su i osnovne smernice za digitalne forenzičare.

Četvrti deo – **USB i CF u praksi**, daje pregled svih najpoznatijih slučajeva korišćenja ovih memorijskih uređaja i razloge zbog kojih su one bitne za digitalnu forenziku.

Peti deo **Forenzika USB i CF memorija** predstavlja osnovne smernice digitalnim forenzičarima za analizu tih tipova uređaja. Prikazan je samo hardverski aspekt, dok alati za analizu sadržaja nisu predmet ovog rada.

U šestom delu – **Prikupljanje i provera digitalnih dokaza**, posvetili smo se konceptu i valjanim metodama kojih se treba držati tokom akvizicije USB i CF memorijskih uređaja. Svaki ključni korak tokom procesa akvizicije posebno je objašnjen, uz primere iz prakse i objašnjenjem zašto se ni na koji način ne sme zaobići.

U sedmom delu – **Alati za akviziciju USB i CF memorija** najpre se bavimo i posebno analiziramo razne metode zaštite podataka na memorijama ovog tipa, ukazujući da je poznavanje načina njihovog rada bitno isto koliko i poznavanje specijalnih alata za forenziku. Zatim prikazujemo najpoznatije uobičajne alate koji se koriste za digitalnu forenziku, posebno obraćajući pažnju na njihovu funkciju u procesu forenzike prenosivih memorijskih uređaja. Na kraju dajemo pregled

nekolicine softverskih alata, čija osnovna namena nije digitalna forenzika, ali itekako mogu koristiti u procesu akvizicije dokaza.

Osmi deo – **Akvizicija u praksi** predstavlja primer rada na akviziciji USB flash memorije. Prateći sve korake, uz upotrebu ranije prikazanih alata, dajemo osnovne smernice digitalnim forenzičarima kao i načine kojima mogu doći do pravih dokaza, koji postaju neoborivi u bilo kom pravnom procesu. Obrađuju se studije slučaja, sa kojima se forenzičari susreću u praksi, kao što su akvizicija diska, akvizicija oštećenog ili zaključanog diska itd.

Deveti deo rada predstavljaju **diskusije dobijenih rezultata**, a deseti **zaključak**, izveden iz prethodno navedenih ciljeva, hipoteza i analiza konkretnih primera u praksi.

Korišćena literatura i lista pojmova pomenutih u radu čine jedanaesti i dvanaesti deo rada.

1.2 Predmet istraživanja

Predmet našeg istraživanja jeste digitalna forenzika USB i CF memorija, njihove mogućnosti, tipovi i sve veći značaj koje imaju u pronalaženju digitalnih dokaza, kao i borbi protiv kompjuterskog kriminala, koji predstavlja veliki problem današnjeg sveta. Pored toga istraživaćemo istoriju pojave tih tipova memorija, njihov razvoj, način rada, razloge sveprisutnosti, kao i samu prirodu digitalne forenzike, kao naučne discipline.

Pre svega treba znati da je računarska (digitalna, kompjuterska) forenzika postupak prikupljanja i analize podataka na način da se ne utiče na njihovu originalnost ili uništenje, što je više moguće, u svrhu rekonstrukcije podataka ili događaja koji su se dogodili u prošlosti na nekom kompjuterskom sistemu. Razumevanje i poznavanje tipa memorije pomaže u proceni rasporeda informacija, načina gubitaka ili uništavanja, ali za nas najbitnije načine da se dođe do njih, i očuva njihov integritet kako bi mogli da ih analiziramo.

Postoji li univerzalan obrazac kojim možemo uspešno formulisati načine sprovođenja forenzike digitalnih dokaza za prenosivih memorija? Da li se mogu izvući opšti zaključci koji se mogu primeniti u raznovrsnim situacijama? Kako uspešno saznati da li je memorija zaštićena i na koji način? Zašto koristiti forenzičke alate? Traganje za odgovorima na ova pitanja bila su neposredni povod za predmet našeg istraživanja.

Predmet našeg rada je proces forenzike prenosivih memorija. Takođe posebno se bavimo alatima kojima se forenzičar koristi u tokom procesa forenzike.

1.3 Hipotetički okvir istraživanja

Hipotetički okvir istraživanja sastoji se od sledećih hipoteza:

Generalna hipoteza:

Poznavanje tipa USB fleš i CF memorije i odgovarajućih forenzičkih alata za akviziciju dokaza, koja mora se sprovesti na određeni način, omogućava analizu podataka uskladištenih na njima, kao i povratak obrisanih, sakrivenih i privremenih datoteka koje normalno nisu vidljive, dok u suprotnom zaobilaženje i bilo kakva improvizacija dovode do greške i oborivosti dokaza.

Posebna hipoteza:

- Prenosive memorije su sveprisutne, lako se brišu, sakrivaju i time kompromituju dokaze na njima
- Najveći deo modernih prenosivih memorija za skladištenje podataka zasniva se na istom ili sličnom principu.
- Tehnologija koja se primenjuje prilikom upisa/čitanja podataka se razlikuje od proizvođača do proizvođača i ona u znatnoj meri otežava proces spašavanja podataka.
- Podaci se na USB flash i CF memorije smeštaju potpuno drugačije nego u hard diskovima.
- Alati za zaštitu podataka na prenosivim memorijama otežavaju i često čine nemogućim proces akvizicije.
- Većina najpoznatijih i dokazanih forenzičkih alata nije ispratila novitete na polju prenosivih memorija.
- Poznavanje savremenih načina zaštite i dostupnih alata čiji primarni cilj nije digitalna forenzika, pomaže akviziciju podataka na valjan način.

1.4 Ciljevi i zadaci istraživanja

U našem istraživanju fokusirali smo se na forenziku USB i CF memorijskih uređaja, analizu slučaja uz pomoć softverskih alata na dva najpopularnija i najkorišćenija operativna sistema Linux i MS Windows. Posebno je dat akcenat na to da mogući dokazi prikupljeni preko navedenih metoda i alata budu neoborivi. Sadržaj rada prilagođen je čitaocima koji već poznaju osnove računarske forenzike, pojam digitalnog dokaza itd., pa se nismo posebno bavili time na koje dokaze treba obratiti pažnju u procesu akvizicije

Naučni cilj ovog istraživanja jeste opis činjenica kojima pre svega želimo da dodemo do odgovora na pitanja koja glase: Zbog čega je danas bitna digitalna forenzika? Kakav značaj imaju prenosive memorije u pronalaženju digitalnih dokaza? Na koji način treba vršiti akviziciju dokaza sa prenosivih memorijskih uređaja? Kojima alatima to učiniti? Kako ostvariti neoborivost dokaza na sudu? Koje su najsavremenije

metode forenzike USB i CF memorija? Otvaranje tih pitanja u zadatoj koncepciji imaju za cilj naučni opis forenzičkog pogleda na USB i CF memorije.

Društveni cilj istraživanja je da dokažemo praktičnu primenu i potvrdimo neophodnost forenzičke analize USB flash i CF memorija pri rešavanju slučajeva kompjuterskog kriminala. Informacija da se sve više kompjuterskih virusa širi putem USB flash diskova, koji su se pokazali kao pun pogodak, jer se one sve više koriste za razmenu velikih količina podataka i po mnogima su glavni uzrok širenja virusa, čini istraživanje na ovu temu posebno zanimljivom.

Poseban značaj istraživanja je u tome što se u našoj zemlji niko nije bavio ovom tematikom, iako se danas većina visokotehnoloških kriminalnih aktivnosti obavlja upravo uz korišćenje USB memorija.

1.5 Metodi i tok istraživačkog procesa

Složenost predmeta istraživanja zahteva primenu:

- Od analitičkih osnovnih metoda: metod analize, metod apstrakcije, metode specijalizacije i metod dedukcije
- Od sintetičkih osnovnih metoda: sinteza, konkretizacija, generalizacija i indukcija.
- Od opštenaučnih metoda – hipotetičko – deduktivne metode, analitičko deduktivne metode, komparativnu.

Primenom ovih metoda kako govore dosadašnji rezultati istraživanja moguće je validno ostvarenje naučnog i društvenog cilja istraživanja. Pristup istraživanju je integrativan, sintetički, u tom smislu ni jednom metodološkom postupku se ne daje isključiva prednost.

U prikupljanju podataka biće primenjeni: ispitivanje dobijenih eksperimentalnih rezultata i metoda analize sadržaja dokumenata. Analiza će biti ostvarena na nekoliko nivoa:

- Na nivou sekundarne analize rezultata ranijih istraživanja i adekvatne literature,
- Na nivou izvornih podataka proizvođača memorijskih uređaja
- Na nivou izvornih podataka proizvođača forenzičkih alata.
- Na nivou istraživanja autora

Polazeći od postavljenih hipoteza i ciljeva istraživanja proistekla je struktura samog rada.

2 DIGITALNA FORENZIKA

„Odeljenje za kompjuterske zločine policije u Maineu je uspeo da spase devetogodišnju devojčicu iz Džordžije, za koju se veruje da je četiri godine seksualno zlostavljana.

Pedofil je na Internet postavio slike zlostavljanja, nakon čega je tim za kompjutersku forenziku uspeo pronaći proizvođača aparata kojim je slikano, vreme slikanja, zatim proizvođača prekrivača za krevet u hotelskoj sobi sa fotografija.

Nakon toga su uspeali da dođu do hotela u Džordžiji kome su prostirke prodane i pregledana je lista gostiju hotela. Kako se nije moglo utvrditi u kojoj se sobi tačno odigrao zločin, pronađeni svi gosti koji su u vreme fotografisanja gostovali u hotelu, a zatim prešlo se na pretragu njihovih stanova i kuća. Nakon pretrage krug se suzio na samo nekoliko ljudi koji poseduju aparat koji po proizvođaču odgovara osumnjičenom. Iako je prošlo već nekoliko meseci uz pomoć digitalne forenzike sprovedene nad memorijskim karticama aparat krivaca je pronađen. Pedofil je uhapšen i očekuje suđenje.“²

Šta zapravo rade kompjuterski forenzičari? Digitalna forenzička analiza (DFA) je postupak utvrđivanja činjenica nad digitalnim medijima primenom različitih metoda. Najčešće se koristi u postupcima sudskog dokazivanja, a sastoji se od niza analitičkih metoda za otkrivanje, prikupljanje, ispitivanje i skladištenje podataka, a često podrazumeva ispitivanje kompjuterskih sistema kako bi se utvrdilo njihovo korišćenje u ilegalnim ili neautoriziranim aktivnostima poput krađe poslovnih tajni, uništavanja intelektualnog vlasništva, prevare, dečije pornografije...

Dokazi prikupljeni forenzičkim metodama se mogu koristiti u raznim vrstama istraga kompjuterskog kriminala:

- u građanskim parnicama za razvode, zlostavljanja i diskriminaciju
- u slučajevima gde pravna lica zahtevaju prikupljanje dokaza u pitanjima zloupotrebe službenog položaja, pronevere ili krađe intelektualne svojine
- osiguravajuća društva koja traže dokaze u vezi sa prevarama osiguranja, zloupotrebe smrti, prava zaposlenog i slučajevima u vezi sa premijama osiguranja, itd.

Digitalni dokazi su neophodni u širokom spektru istraga kompjuterskog kriminala, a kompjuterska forenzika se koristi različitim metodama u cilju otkrivanja podataka koji počivaju unutar kompjuterskog sistema ili za oporavak obrisanih, kriptovanih ili oštećenih podataka. Svaka informacija može biti od značaja u procesu otkrivanja ili osporavanja tvrdnji.

Kompjuterska forenzika predstavlja relativno novo polje nauke i tokom godina dobijala je razne nazive poput „digitalna forenzika“ i „analiza medija“. Tek pre nekoliko godina prepoznata je činjenica da svi digitalni uređaji ostavljaju deliće

² Casopis „Australian PC Authority“, jun 2008. god.

informacija. Ovi delići predstavljaju značajan dokaz u raznim vrstama istraga. Zainteresovanost za ovu problematiku se prvo javila kod profesionalaca iz oblasti krivičnog prava i obaveštajnih službi, dok su informatičari i civilno pravo sa entuzijazmom prihvatili ovaj novi izvor informacija.

ASCLD-LAB³ je 2003. godine prepoznao digitalni dokaz kao ravnopravnu forenzičku disciplinu. Iako je relativno nova disciplina ona ima potencijal da značajno utiče na specifične tipove istraga i krivičnih gonjenja. Zajedno sa prihvatanjem kompjuterske forenzike kao legitimnog postupka analize dokaza dolazi i do povećanog interesovanja za obučavanje i edukaciju na ovom polju. Trenutno postoji više od trideset koledža i univerziteta samo u Americi koji obavljaju edukaciju na ovom polju. U našoj zemlji još uvek je malo obrazovnih institucija koje se bave ovom oblašću (Univerzitet Singidunum i Fakultet organizacionih nauka iz Beograda). Tome s' jedne strane doprinosi slaba informatička razvijenost, ali neprepoznavanje značaja digitalne forenzike od strane vodećih naučnih institucija.

Kompjuterska forenzika se značajno razlikuje od tradicionalnih forenzičkih disciplina. Za početak, alati i tehnike koje ova disciplina zahteva su relativno lako dostupni svakome ko želi da sprovede forenzičku analizu. Nasuprot tradicionalnim forenzičkim analizama od kompjuterskih istražitelja se zahteva ispitivanje na svakoj fizičkoj lokaciji a ne samo u kontrolisanim uslovima.

Digitalnu (računarsku forenziku) mnogi autori, a posebno pojedinci i kompanije koji se njom bave dele na tri osnovna dela: **intervenciju**, prikupljanje podataka i dokaza – **akviziciju** i **analizu**. Iako se analiza smatra najobimnijom, prava stručnost forenzičara se ogleda upravo u akviziciji digitalnih dokaza. Nažalost više je alata za analizu, nego alata za akviziciju podataka, možda baš iz razloga, jer je često teže obaviti akviziciju, nego analizu.

2.1.1 Akvizicija

Šta zapravo predstavlja akvizicija? Akvizicija predstavlja sakupljanje i pretragu, otkrivanje i identifikaciju digitalnih dokaza. Ona je dosta analogna uzimanju otisaka prsta sa mesta zločina u „običnoj“ forenzici. Uopšteno predstavlja zadatak forenzičara da uz proverene alate (softverske ili hardverske), poštujući metodologiju, napravi originalnu kopiju HDD, CD, FD, USB memorije i iz nje izvuče sve moguće dokaze i preda ih na analizu.

USB i CF memorijski uređaji imaju nekoliko odlika po kojim se razlikuju od standardnih memorijskih uređaja. Osim karakteristika, kao što su fizička veličineža, način rada i sl. u digitalnoj i forenzici oni imaju veliku važnost i kao fizički dokazi. Za razliku od hard diskova koji se najčešće nalaze u unutrašnjosti računara i koji su, u većini slučajeva, izvori isključivo digitalnih dokaza, prenosive memorije na sebi imaju i brojne otiske prstiju, jer se češće prenose „iz ruke u ruku“, a i lako je utvrditi ko je zadnji imao u rukama tu memoriju. Veoma je bitno rukovanje sa ovim uređajima i uzimanje svih vrsta fizičkih dokaza pre same digitalne forenzike. Čak i sitna fizička oštećenja na konektorima mogu biti dokaz koji će osuditi ili osloboditi osumnjičenog. U svetu je poznato više slučajeva dokazivanja umešanosti u kriminalne radnje

³ The American Society of Crime Laboratory Directors/Laboratory Accreditation Board

povezane sa dečijom pornografijom, kada je kao dokaz prihvaćen nalaz forenzičara koji su na osnovu sitnih (mikroskopskih) oštećenja na memorijskoj kartici utvrdili da su korišćene u određenom fotografskom aparatu. Naime raspored konektora, način ubacivanja i mesto na kome se memorijska kartica nalazi, ostavljaju na kartici različita oštećenja, makar se radilo i o dva aparata iz iste serije.

2.1.2 Smernice rada

Tokom istraživanja o računarskom kriminalu u izvršenom uz pomoć USB i CF memorija, kao i drugim kriminalnim aktivnostima gde se dokaz nalazio na ovim uređajima došlo se do dva smera rada. Jedan je svakako akvizicija, pretraga podataka na memorijama, a druga je dokazivanje moguće veze određene prenosive memorije i određenog računara. Za svaku od ovih problema dat je primer i način na koji se može dokazati ili opovrgnuti postojeća sumnja.

Peti vek pre nove ere



„Pretraga podataka će biti teža nego što smo zamislili“

Slika 2: Forenzika u istoriji

3 USB FLEŠ I CF MEMORIJSKI UREĐAJI

“Američka vojska je privremeno zabranila korišćenje USB diskova i ostalih prenosivih uređaja za snimanje podataka nakon što je na njihovoj mreži primećeno širenje računarskog crva.

Takva zabrana može otežati rad bilo koje organizacije, a posebno vojske, jer na mnogim lokacijama gde vojska deluje nije moguće prebacivati datoteke e-poštom ili drugim "online" metodama. Najverovatniji uzročnik problema jeste varijanta crva SillyFDC koja se može širiti putem mreže, ali i putem uređaja za snimanje podataka. U slučaju zaraze, crv ima mogućnost preuzimanja dodatnog zlonamjernog koda s Interneta te može instalirati "keyloggere", botnet agente, spyware i sl. neželjene programe. Sigurnosni stručnjaci se slažu da je mera zabrane prikladna za navedeni računarsko – sigurnosni incident te upozoravaju na važnost antivirusne provere prenosivih medija za smeštanje podataka. Takođe, preporučuju isključivanje mogućnosti automatskog pokretanja programa prilikom priključivanja USB diskova, CD-a, DVD-a i ostalih prenosivih medija.“⁴

"Snimi mi na fleš", je fraza koja je postala deo svakodnevnog govora. Svesni smo da mnogi ljudi danas sve svoje digitalne podatke čuvaju uz sebe, u svom džepu na na popularnim flaševima. Samim tim digitalni forenzičari moraju se prilagoditi novonastalim uslovima i kao što su se nekad upoznivali sa mehanikom rada hard diskova, danas se moraju upoznati sa načinom rada flash memorija.

Šta je zapravo USB fleš? USB fleš, ili kako mu je pravo ime, USB Memory Drive ili Keydrive, je mali prenosni uređaj za skladištenje podataka koji koristi flash memoriju (flash memory) i USB konektor. Priključuju se u normalan tip-A USB priključak, bilo na kompjuteru ili na USB hub-u. Uređaj se napaja preko USB priključka na PC-u i nije mu potrebno spoljno napajanje.

Za razliku od ostalih prenosivih medija za skladištenje podataka, USB fleš koristi poluprovodničku tehnologiju (čipove) za čuvanje podataka. Ovo ih čini otpornim na fizička oštećenja i prašinu. Njihov kapacitet se menjao, od početnih 16MB do današnjih nekoliko gigabajtova. U 2003 većina USB fleševa je radila na USB 1.0/1.1 standardu sa brzinom od 12 Mb/s. Od 2004 novi USB fleševi podržavaju USB 2.0 interfejs, sa maksimalnom brzinom čitanja od oko 100 Mb/s i nešto sporijom brzinom upisivanja podataka. U idealnim uslovima, ovako sačuvani podaci mogu opstati oko 10 godina, ali se ipak kao forenzički dokaz uzimaju podaci ne stariji od 6 meseci.

3.1 Fleš memorija

Fleš memorija je računarska memorija koja može da čuva podatke čak i kada nije pod naponom, a može se brisati i reprogramirati elektronskim putem. Zasnovana je na tehnologiji memorijskih kartica kao što su memorijske kartice za digitalne foto aparate, *palmtop* računare, mobilne telefone, konzole za video igrice, audio plejere itd. Za razliku od EEPROM-a⁵, brisana je i reprogramirana u blokovima koji su

⁴ Izvor: +CERT.hr, 20.11.2008., <http://www.cert.hr/>

⁵ eng. Electrically Erahable Programmabile Read Only Memory

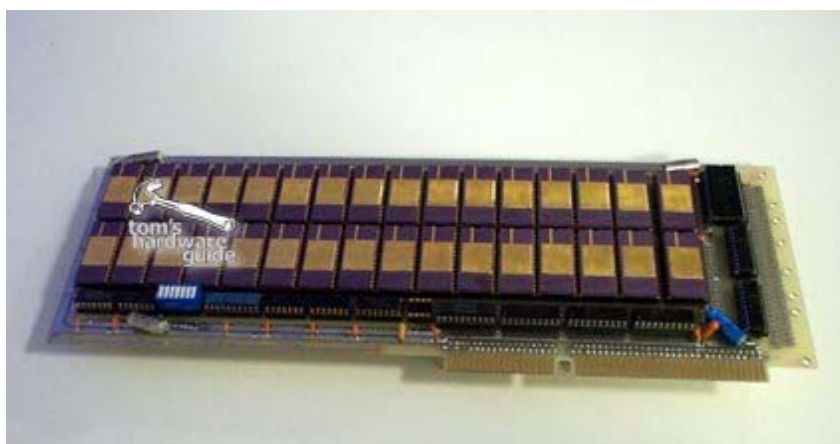
sačinjeni od višestrukih lokacija. Fleš memorija košta mnogo manje od EEPROM-a, i baš zbog toga, ova tehnologija memorijskih kartica je postala dominantna na tržištu od kako se pojavio USB flash drive, koji se koristi za čuvanje i razmenu podataka između računara.

Pored karakteristike da joj nije potrebno električno napajanje za čuvanje podataka, fleš memorija nudi i brz pristup podacima. Još jedna vrlo važna karakteristika fleš memorije je i ta što ima bolju otpornost, na kinetičke skokve u odnosu na hard diskove. Gotovo je fizički neuništiva kada je upakovana u neku memorijsku karticu, koju koristi digitalni uređaj.

3.1.1 Poreklo: istorija i razvoj fleš memorije

Intel je bila prva kompanija koja je proizvela *to produce* fleš memoriju i uvela je na tržište. U 1988. godini, ova grupacija je lansirala 256-bitni fleš čip - veliki kao kutija za cipele. Intel je prikazao prednosti "ugrađene memorije" koristeći jedan od starih magnetofona, koji bi lako mogao da napuni manji kofer.

Intelov pronalazak je bio takozvani NOR fleš, razvijen iz EPROM i EEPROM tehnologija za čipove i opremljen interfejsom za SRAM memoriju (slika 3). NOR fleš je imao brzine upisivanja i brisanja koje bi se mogle smatrati sporim prema današnjim standardima i mogao je da izdrži samo mali broj ciklusa upisivanja (oko 100 000). On je bio primenjivan u oblastima gde su se stalno uskladišteni podaci samo povremeno i retko menjali. Na primer, operativni sistemi digitalnih centrala ili mobilnih telefona su bili smešteni u jedinicama NOR fleš memorija.



Slika 3: Intelov NOR fleš

Za razliku od prethodnih tehnologija, fleš je omogućio da se brišu ili skladište podaci na više mesta u jednom koraku; to je predstavljalo ogromnu prednost u brzini. Ipak, čak i danas, trajna priroda ove memorije smatra se jednom od njenih najvećih prednosti.

Druga vrsta fleš memorije je NAND fleš, projektovan 1989. godine u kompaniji Toshiba, i uspostavljen kao jeftinija i brža alternativa NOR flešu. Toshiba je takodje bila prva kompanija koja je koristila naziv fleš (*Flash*). U poredjenju sa NOR, NAND tehnologija je ponudila deset puta veći broj ciklusa upisivanja, i veće brzine i za skladištenje i za brisanje podataka. Memorijske ćelije u NAND memoriji su upola manje od onih u NOR memoriji. To za rezultat ima u najmanju ruku teorijsku manju cenu NAND memorije: manje dimenzije ćelije omogućavaju da se na datom prostoru

ima veći kapacitet, što istovremeno znači i manju cenu za kupca i veću dobit za proizvođača (slika 4).



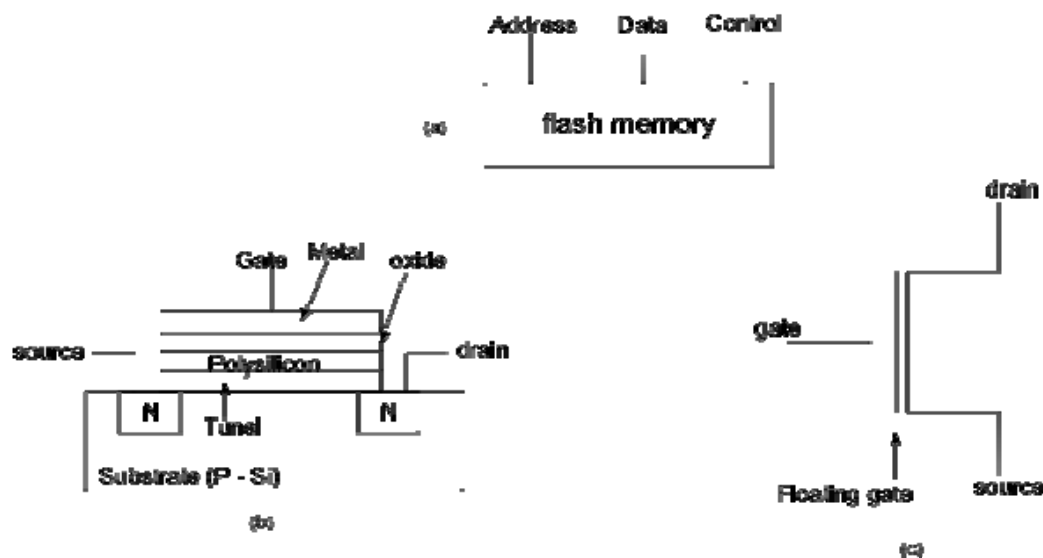
Slika 4: NAND fleš firme Infineon

Prema proizvođaču fleša firmi M-Systems, NAND briše podatke za četiri milisekunde, dok NOR zahteva pet sekundi za isti proces. Razlog za ovo su veće dimenzije NOR blokova. – od 64 do 128 KB. Suprotno tome, NAND pristupa blokovima veličine između 8 i 32 KB. Zbog svoje bolje performanse, NAND se obično koristi u memorijskim karticama – kao što su Compact-Flash, SmartMedia, SD, MMC, xD i PC kartice, USB flash...

3.1.2 Principi rada fleš memorije

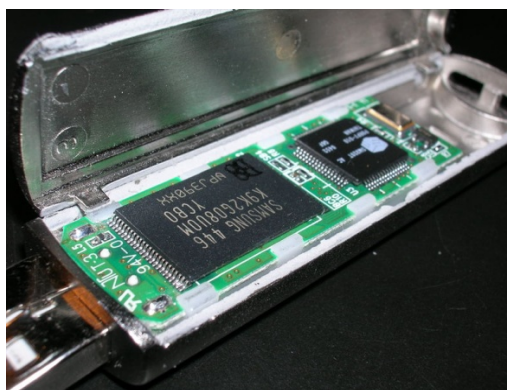
Fleš memorija smešta informacije u redove FTG-a (Floating Gate Transistor) koji se nazivaju "ćelijama", i svaki od njih smešta po jedan bit informacije. Uređaji novijih generacija, koji koriste fleš memoriju, mogu da smeštaju više od jednog bita informacija po ćeliji, koristeći više od dva nivoa električnog punjenja, i svaka sledeća informacija je smeštena na "lebdećem" ulazu ćelije. Kod fleš-a, svaka ćelija izgleda slično kao i ćelija kod standardnog MOSFET-a (Metal Oxide Semiconductor Field-Effect Transistor), osim što ima dva ulaza umesto jednog. Jedan ulaz (gate), kao i kod ostalih MOS tranzistora, je kontrolni ulaz (CG), a drugi ulaz je lebdeći ulaz (FG), izolovan jednim oksidnim slojem koji se nalazi svuda oko njega. Lebdeći ulaz se nalazi između kontrolnog ulaza i podloge. Pošto je lebdeći ulaz izolovan njegovim oksidnim slojem, bilo koji elektron koji se nađe na njemu ostaje zarobljen tu, i na taj način smešta informaciju. Kada se elektroni nalaze na lebdećem ulazu, oni modifikuju (delimično prekidaju) električno polje koje se javlja sa kontrolnog ulaza, što modifikuje naponski impuls (V_t) ćelije. Na taj način, kada je ćelija "očitanja" postavljanjem određenog naponskog impulsa na kontrolnom ulazu, trenutno električno stanje će ili proticati ili neće pročitati, u zavisnosti od naponskog impulsa (V_t) ćelije, koji je kontrolisan od strane broja elektrona na lebdećem ulazu. Ovo prisustvo ili odsustvo trenutnog električnog stanja je detektovano i prevedeno u nule (0) i jedinice (1), reprodukujući tako smešteni podatak (slika 5).

U uređajima koji smeštaju više od jednog bita informacija po ćeliji (tzv. multilevel cell device), količina trenutnog proticanja će biti detektovana, da bi se utvrdio broj elektrona smeštenih na lebdećem ulazu.



Slika 5: Arhitektura fleš memorije

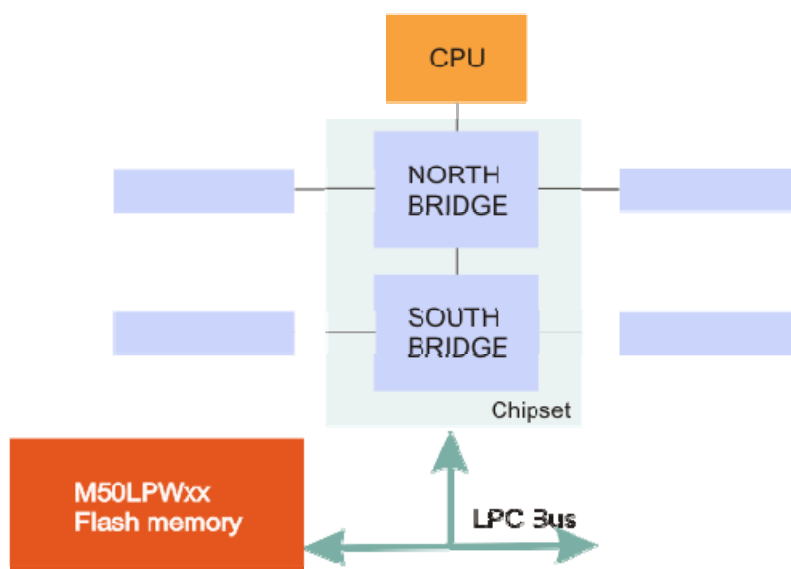
Da bi memorijska ćelija bila programirana, fleš kontrola dovodi kratak naponski impuls. Ovo okida lavinski proboj u memorijskom tranzistoru koji puni lebdeći ulaz (tzv. hot-electron injection). Na ovaj način, 1 Mbitni čip fleš memorije može biti programiran za dve sekunde, za razliku od normalnih EEPROM⁶-ova, međutim, brisanje čipa se izvršava istovremeno. Tokom brisanja, kontrola fleš memorije koristi trenutno prebacivanje brisanja za slanje impulsa brisanja u celo polje memorijske ćelije, pa se brišu sve memorijske ćelije. Vreme brisanja za celu fleš memoriju je oko jedne sekunde. To svakako predstavlja problem forenzičarima, jer praktično znači da se prepisivanjem, briše i ne može rekonstruisati prethodni sadržaj.



Slika 6: Fleš memorija ugrađena u USB flash drive

⁶ Erasable Programmable Read-Only Memory

Centralni deo fleš memorije je matrica memorijskih ćelija. Ćelije su adresirane baferom adrese, koji prima signale adrese i prenosi ih do sektora redova i kolona, naizmenično. Fleš memorije ne izvršavaju multipleksiranje adrese. Dekoderi redova i kolona selektuju jednu liniju reči i jedan, ili više parova bitskih linija, kao i u uobičajenom memorijskom čipu. Čitljivi podatak izlazi preko ulazno/izlaznog bafera podataka, ili se upisuje u adresiranu memorijsku ćeliju ovim baferom preko U/I ulaza (slika 7).



Slika 7: Blok dijagram fleš memorije

Procesi očitavanja, brisanja i programiranja se kontrolišu dvobajtnim instrukcijama, koje eksterni mikroprocesor upisuje u registar instrukcija fleš kontrole. Za tipičnu fleš memoriju dostupne su sledeće instrukcije:

- Čitanje memorije (Read Memory): fleš memorija obezbeđuje podatke preko pinova podataka
- Očitavanje identifikatora memorije (Read Identifier Code): fleš memorija obezbeđuje kôd na pinovima podataka, koji označavaju vrstu i verziju čipa
- Podešavanje brisanja/brisanja (Set-up Erase/Erase): priprema fleš memoriju za proces brisanja i izvršava brisanje
- Brisanje-potvrđivanje (Erase-Verify): briše sve memorijske ćelije i potvrđuje ovaj proces
- Podešavanje programiranja / programiranje (Set-up Program/Program): priprema programiranje pojedinačnih memorijskih ćelija i izvršava ovaj proces
- Programiranje – potvrđivanje (Program-Verify): izvršava programiranje i potvrđuje ovaj proces

- Resetovanje (Reset): resetuje fleš memoriju u definisano početno stanje.



Slika 8: Fleš memorija

Fleš memorija (slika 8) ima karakteristiku da je non – volatile odnosno da ne gubi podatke koji su upisani na nju nakon što nestane napajanje, kao što je slučaj sa klasičnom radnom memorijom u računaru.

U zavisnosti od toga od kojih je kola realizovana svaka memorijska ćelija, fleš čipovi se svrstavaju u dve osnovne kategorije NOR i NAND.

3.1.3 NOR fleš memorija

NOR fleš se pojavio prvi, a njegovu komercijalizaciju pokrenuo je Intel. Fleš tipa NOR (slika 9) nudi sporije čitanje i pisanje, ali i urednu strukturu adrese i podataka tako da je moguće pristupiti bilo kojoj lokaciji na memorijskom čipu, na sličan način kao kod radne memorije. Zbog toga je ovaj tip memorije pogodan za skladištenje podataka koje nije potrebno često osvežavati, kao što je recimo BIOS ili pak firmware u raznim elektronskim uređajima.



Slika 9: NOR memorijski čipovi

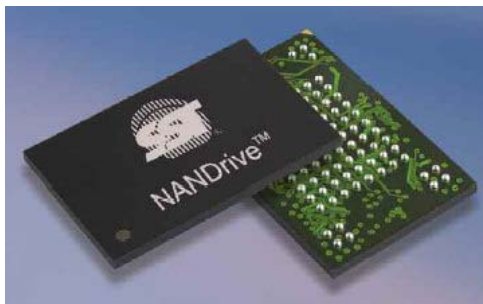
U široj upotrebi kod prenosnih uređaja, pre svega mobilnih telefona, do sada je uglavnom bila NOR Fleš memorija koja polako počinje da gubi korak u trci sa NAND tipom.

Sa aspekta digitalne forenzike NOR tip nije do skoro bio zanimljiv, međutim poslednjih godina, sa rastom potrebe za forenzikom mobilnih telefona porasla je i potreba za forenzičkim istraživanjem tog tipa. Podatak koji ide u korist je da se većina mobilnih telefona, najvećih svetskih proizvođača zasnivala na NOR tipu. Danas se situacija promenila, ali dve trećine mobilnih telefona u upotrebi, koristi NOR tip za smeštanje podataka, kao što su SMS poruke, imenici, podsetnici...

3.1.4 NAND fleš memorija

NAND tip fleš memorije je predstavljen 1989. godine od strane Samsunga i TOSHIBE. Ovaj tip memorije je u poslednjih nekoliko godina doživeo izuzetnu ekspanziju, uz gustinu pakovanja koja se duplira svake godine, u skladu s Murovim zakonom⁷. Ima znatno nižu cenu proizvodnje od NOR fleša, brže čitanje i pisanje, veću gustinu pakovanja memorijskih ćelija osetno veću izdržljivost u pogledu količine maksimalnog broja pristupa memoriji odnosno maksimalnog broja pisanja/brisanja memorije.

NAND fleš je arhitektura sa sekvencijalnim pristupom koja segmentira memoriju na veći broj stranica, obično obima 256 ili 512 bajtova. Svakoj stranici se pristupa kao diskretnoj jedinici. Zbog ovoga, NAND fleševi ne obezbeđuju proizvoljan interfejs kakav je slučaj sa NOR flešom. I pored veće složenosti interfejsa, NAND fleševi se karakterišu većom gustinom u odnosu na NOR fleševe, što ih čini idealnim za čuvanje velike količine podataka. Za slučaj da se programi čuvaju u NAND flešu, pre izvršenja oni se moraju napuniti u RAM prostor, iz razloga što NAND stranično organizovana arhitektura nije pogodna za proizvoljno čitanje/upis od strane mikroprocesora. NAND fleševi (slika 10) se standardno koriste u potrošačkoj elektronici kao memorijske kartice, kakav je slučaj sa digitalnim fotoaparatima. NAND fleševi, kao komponente su takođe dostupne kao diskretne komponente za stalno memorisanje velike količine podataka kod digitalnih sistema.



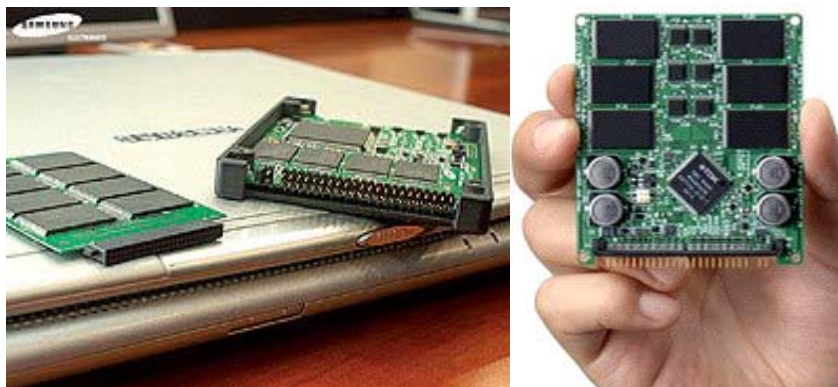
Slika 10: NAND memorijski cip

Kompanije Intel i Micron Technology predstavile su brže NAND fleš memorije, za koje tvrde da omogućavaju pet puta veću brzinu prenosa podataka, od aktuelnih NAND fleš memorija. Nove memorije se zovu ultrabrze NAND memorije (High-Speed NAND Flash). Radi se o jednoćelijskim fleš memorijama, kapaciteta 8 GB koje omogućavaju brzinu čitanja podataka od 200 MB/s, odnosno brzinu upisivanja od

⁷ Pre tačno 45 godina, inženjer Gordon Mur, jedan od osnivača firme Intel, najvećeg svetskog proizvođača kompjuterskih čipova, napisao je novinski članak u kome je izneo da će se broj pojedinačnih elektronskih elemenata na jednom čipu svake godine udvostručavati.

100 MB/s. Aktuelne NAND memorije omogućavaju brzinu čitanja podataka od 40 MB/s, odnosno brzinu upisivanja od 20 MB/s.

Danas je u toku postepeni prelazak klasičnih hard-diskova na nove, ultrabrze fleš diskove koj se za sada sreću samo u po nekim modelima prenosnih računara, kao i u uređajima koji zahtevaju manje količine memorije poput digitalnih video-kamera (slika 11).



Slika 11: NAND fleš disk (spreman za zamenu sadašnjih hard diskova)

Iako novi tip još uvek nije zaživeo, pre svega jer cena ne odgovara komercijalnom tržištu, predviđa se da će u skorijoj budućnosti sve zasnivati na fleš memoriji, tj. da će magnetni hard diskovi otići u zasluženu penziju. Takav sled događaja ide u prilog tezi da će se na polju digitalne forenzike sve više tražiti stručnjaci, koji će iz oštećenih, namerno obrisanih i sl. fleš memorija uspevati da otkriju korisne podatke.

3.1.5 Ograničenja fleš memorije

Ono što ograničava fleš memoriju je to što se mora brisati jedan po jedan “blok“. Ovo generalno svim bitovima u ćeliji dodeljuje vrednost 1. Počevši od sveže obrisanih blokova, svaka lokacija unutar tog bloka može biti programirana. Ipak, čim se bitu jednom dodeli vrednost 0, samo brisanjem celog bloka, bitu se može promeniti vrednost ponovo na 1. Drugim rečima, fleš memorija nudi nasumičan pristup operacije čitanja i programiranja, ali ne može da ponudi bilo kakav nasumičan pristup ponovnom pisanju (rewrite) ili operaciji brisanja.

U odnosu na hard disk, fleš memorija ima konačan broj ciklusa za brisanje i pisanje (erase write cycles) tako da se ovo mora malo ozbiljnije uzeti u obzir, pogotovo ako na nekom USB fleš drive-u imamo instaliran neki operativni sistem. Ipak većina komercijalnih USB memorija uglavnom garantuje 1 milion ciklusa.

3.1.6 Fleš fajl sistemi

Zbog posebnih karakteristika fleš memorije, njena upotreba je najefikasnija ako se koristi pod posebno dizajniranim fajl sistemima. Osnovni koncept “ispod haube“ fajl sistema je: kada magacin fleša treba da se ažurira, fajl sistem će napisati novu kopiju promenjenih podataka na svež blok, postaviće nove pokazivače (pointer-e), i obrisati stari blok kada bude imao vremena. Jeda od starijih fleš fajl sistema bio je Microsoft-ov FFS2, koji je korišćen za rad pod MS-DOS-om. Oko 1994. PCMCIA Industry

Group⁸ je odobrila FTL (Flash Translation Layer) specifikaciju, koja je dozvoljavala fleš uređaju da izgleda kao FAT disk. Drugi komercijalni sistemi, kao što je FlashFX kompanije Datalight, su bili tako kreirani da bi izbegli probleme sa patentima FTL-a. JFFS je bio prvi specifični fleš fajl sistem za Linux, koji je ubrzo zamenjen fajl sistemom JFFS2, a 2003. se pojavio YAFFS. Ove fleš fajl sistem, u malom broju, uglavnom koriste digitalne kamere, foto aparati i sl. uređaji.

Danas se u 76% slučajeva digitalni forenzičari susreću sa *pseudo* FAT fajl sistemom za skladištenje podataka na fleš memorijama, ali su sve brojniji i oni na kojima je NTFS fajl sistem i brojni drugi sistemi koji podržavaju fleš memorije. Istražiteljima to može predstavljati problem, jer se struktura fajlova često razlikuje od onih u Windows i Linux fajl sistemima.

3.1.7 Kapacitet fleš memorije

Svaki čip fleš memorije doseže kapacitet od kilobit-a (128 byte-a) do nekoliko gigabita (1,073,741,824 bit-a). Čipovi su uglavnom sakupljeni zajedno kako bi se postigao što veći kapacitet memorije.

3.1.8 Brzina fleš memorije

Uređaji koji koriste fleš memoriju su dostupni na različitim brzinama. Neki su optimizovani za brzinu od 2MB sekundi, 12MB po sekundi itd. Ostale memorijske kartice su rangirane po 100x, 130x, 200x, itd. Za takve kartice, 1x znači da je brzina prenosa podataka 150KB po sekundi, tj. brzina kojom su prvi CD uređaji mogli da prenose informacije.

3.1.9 Oštećenje podataka na fleš memoriji

Najčešći razlog zbog kojeg dolazi do oštećenja podataka je taj što nekada ljudi uklone uređaj sa fleš memorijom (USB fleš drajv na primer) u toku pisanja podataka na nju. Situacija bi bila još gora ako uz to ne bi koristili i odgovarajući fajl sistem, ili ako bi usledila asinhronizacija (gde podatak i dalje čeka da bude napisan, a uređaj je već uklonjen).

3.2 USB fleš

Fleš memorija je postala dominantna na tržištu od kako se pojavio USB flash drive, koji se koristi za čuvanje i razmenu podataka između računara, i sve pohvale koja je fleš memorija pokupila krajem 20. veka pa sve do danas, dolaze upravo od USB flaš drive-a. USB flash drive je mobilan i moćan memorijski uređaj: mali, lagan, prenosiv, sa mogućnošću pisanja i brisanja podataka. Krajem 2000. godine počela je prodaja prve USB fleš memorije, koju danas popularnije zovemo USB stick, a prvi USB stick koji je proizveden imao je kapacitet od 8 MB. Od tada pa do danas kapacitet USB stickova rastao je iz godine u godinu tako da ih danas možemo pronaći sa kapacitetom od 128MB do 64GB. USB stick danas je jedan od najpopularnijih načina za prenos podataka jer je vrlo jednostavan za korišćenje. Danas, maksimalan kapacitet USB fleš drive-a je zvanično 320GB, a pre samo godinu dana kapacitet od 8GB se smatrao

⁸ Personal Computer Memory Card International Association, grupacija koja je razvila standarde plug-in uređaja, za laptop računare, veličine kreditne kartice

luksuzom. Kapacitet je ograničen samo u zavisnosti od trenutne “gustine“ fleš memorije.

Svaki USB fleš uređaj se sastoji od nekoliko osnovnih elemenata. To su u prvom redu NAND fleš memorijski čip i USB kontroler koji računaru ili nekom drugom uređaju omogućava pristup fleš memoriji. Ostatak čine generator takta, dodatni kontakti za programiranje i testiranje uređaja pri proizvodnji, led dioda za indikaciju rada i na kraju sama štampana pločica na koju su sve ove komponente integrisane. Na štampanoj pločici je i fizički USB konektor kojim se uređaj priključuje na računar (slika 12).



Slika 12: Spoljašnji izgled jednog USB fleša

USB flash drive ima velike prednosti u odnosu na ostale prenosive memorijske uređaje kao što su magnetne diskete i trake, ali i optičke memorije (CD, DVD). Kompaktniji su, generalno brži, mogu da nose veliku količinu podataka, i veoma su pouzdani (fizički pre svega). Moderni operativni sistemi tipa Linux, Mac OS, i Windows, imaju hardversku podršku za uređaje poput USB fleš memorija.

3.3 Kompaktne fleš memorijske kartice – CompactFlash

Najveći problem, koji se u praksi javio, je mešanje i svođenje na isto MMC i SD katica sa CompactFlash memorijama. Neretko čak i stručnjaci pod CF smatraju MMC i SD kartice. Posledica toga je i da se ovaj rad, čiji je predmet istraživanja prvenstveno CF tip memorija bavi i drugim „sličnim“ tipovima memorija, jer se oni češće mogu naći u upotrebi. Sa aspekta forenzike nikada ne sme doći do sumnje koja je kartica u upotrebi. Osnovna razlika je što CF uključuje i kontroler koji upravlja radom memorije, koji je ekvivalent standardnom IDE sistemu.

Danas se svuda mogu pronaći kompaktne fleš memorijske kartice kapaciteta do 8 GB i Secure Digital (SD) kartice od 4 GB. Iako su sasvim male, njihova veličina ih i dalje čini nepogodnim za upotrebu u ultra malim uređajima kao što su mobilni telefoni, pametni telefoni, PDA (personalni digitalni asistent) itd.

Trenutno se najčešće mogu sresti CF (Compact Flash) kartice, veličine kutije za šibice, koje imaju do 8 GB memorijskog prostora i SD (Secure Digital) kartice veličine poštanske markice, kapaciteta do 4 GB, a uskoro bi trebalo da se pojavi i model od 8 GB. Compact Flash (slika 13) je omiljeni medijum za skladištenje podataka u digitalnim foto aparatima, ali ima i aparata koji primaju MicroDrive diskove firme Hitachi, u čijim CF kućištima su ugrađeni hard diskovi veličine jednog inča.



Slika 13: CF memorijska kartica

MMC (Multimedia Card) je preteča SD kartice. Ova dva uređaja izgledaju gotovo isto, ali MMC kartica nema zaštitu ni za pisanje ni za kopiranje, ali je tanja. MMC kartice se i danas mogu sresti u nekim uređajima, pogotovo u nekim modelima mobilnih telefona firme Nokia. Forenzičari se u radu sa memorijskim uređajima, takođe sreću u velikom broju sa Memory Stick karticama i xD karticama za slike firme Olympus, kao naslednicima sada već zastarelog formata SmartMedia.

Da bi se prihvatile zamenljive memorijske kartice u manjim uređajima, postali su neophodni i manji faktori forme. Zato se i MMC i SD kartice prave u smanjenim formatima poznatim kao MMC Mobile (Reduced Size) i MiniSD, respektivno. MMC Mobile je veličine samo jedne polovine SD kartice, dok Mini SD kartice zauzimaju samo 36% tog prostora.

Kompakt fleš podržava najveće brzine prenosa (do 30 megabajta u sekundi) i najveće kapacitete (do 32 GB, uskoro i više). Verzija 3.0 podržava brzine prenosa do 66 megabajta u sekundi. Ove specifikacije dopuštaju maksimalne brzine čak do 137 gigabajta u sekundi ili minimalne od 16 megabajta u sekundi. Zatim, kompakt fleš radi pri naponu od 3,3V do 5V, što dalje omogućava lako rukovanje i raznovrsne implementacije.

CF interfejs koristi 50 pinova, ali je ipak kompatibilan i sa PCMCIA-ATA. Ovo se značajno razlikuje od ostalih standarda koje je CF brzo potukao na tržištu. Laka kompatibilnost sa ATA je rezultat srećne podudarnosti da CF kartice koriste isti kontroler kao i ATA urđaji.

Postoji nekoliko vrsta CF kartice, koje se razlikuju po veličini i omogućavaju i druge primene osim kod uređaja za skladištenje podataka zasnovanih na memoriji. Kartice tipa I i II se mogu razlikovati po debljini: prva je 3,3, a druga 5 mm. (Microdrive firme Hitachi je, jednostavno, suviše debeo da bi stao u omotač od 3,3 mm).

3.4 mmC i SD kartice

Oba formata (mmC i SD) su danas lako dostupna svuda, od prodavnica kamera do supermarketa. Dimenzije njihovih površina iznose 24 x 32 mm (0,94 x 1,26 inča). Lakše orijentacije radi, jedan ugao im je blago zasečen i za razliku od Smart Media kartica, ove kartice je teško slučajno pogrešno postaviti, a interfejs ima 9 pina i to tri pina su za napajanje (2 uzemljenja), jedan je za komande, tri su za podatke i jedan za

sinhronizaciju, jer je ovaj interfejs takođe i magistrala. zajedno sa poslednjim pinom za detektovanje kartice.

Razlike između ova dva tipa kartice su u detaljima. MMC je stariji i jednostavniji medijum za skladištenje za mobilne uređaje, što objašnjava njegovu debljinu od samo 1,0 mm. SD kartice sadrže minijaturni prekidač koji se može da pokrene zaštitu od upisivanja zasnovanu na hardveru. Zato su ove kartice nešto deblje (2,1 mm), što objašnjava zašto MMC kartica može da radi u priključnici ili čitaču za SD karticu, a obrnuto u većini slučajeva nije moguće.

SD kartice nameću zastareli sistem za zaštitu od kopiranja, koji su zajedničkim snagama razvile firme IBM, Intel, Matsushita, i Toshiba, poznat pod nazivom 4C CPRM (Copyright Protection for Recordable Media – zaštita od kopiranja za upisive medijume - 4C je, najverovatnije, skraćenica za "četiri kompanije"). SD karticama se može pristupiti samo pomoću ovlašćenih uređaja. Ukoliko forenzičar za to ima pravi softver, u mogućnosti je da napravi ograničen broj kopija podataka.

3.4.1 mmC Mobile

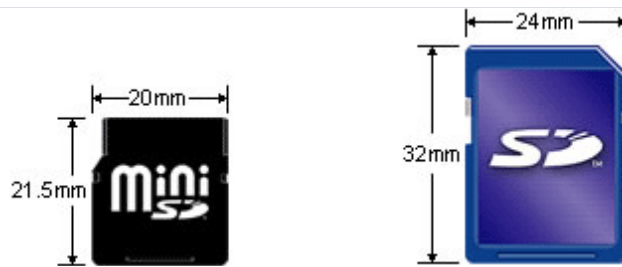
MMC Mobile (slika 14) je smanjena verzija MMC kartice dimenzija 18 x 24 x 1,4 mm, ili 0,71 x 0,94 x 0,06 inča. Ona koristi 13 umesto 9 kontakata da bi prilagodila širine magistrala od 1,4 ili 8 bita i da bi omogućila brzine prenosa podataka od preko 50 megabajta u sekundi. MMC Mobile uređaji su unazad kompatibilni sa standardnim MMC karticama i mogu se postaviti u MMC slotove pomoću običnog adaptera. Za forenzičare je veoma bitno napomenuti, da se MMC Mobile kartica jednostavno prikači na adapter, češće nego što se u njega ubacuje, kao što je to slučaj sa MiniSD karticom. Teoretski, maksimalni kapacitet za MMC Mobile kartice je 1 GB, dok su miniSD danas dostupne sa kapacitetom od 4GB.



Slika 14: MMC Mobile kartica i adapter

3.4.2 Mini Secure Digital (SD) kartica

Sa dimenzijama od 20 x 21,5 mm (0,79 x 0,85 inča), MiniSD je značajno manja od standardne SD kartice, ali je, sa izuzetkom mehaničkog prekidača za zaštitu od upisivanja, identična sa svojim većim prethodnikom (slika 15). Njena debljina takođe je smanjena, sa 2,1 mm (0,08 inča) to 1,4 mm (0,06 inča). Da bi se pristupilo njenom sadržaju sa PC računara, potreban je odgovarajući adapter, koji može da prilagodi ovu karticu. Njen maksimalni kapacitet trenutno iznosi 9 GB.



Slika 15: Dimenzije Mini SD i SD kartice

3.4.3 MMC (Multi Media Card)

Sa dimenzijama od 14 x 12 x 1,1 mm (0,55 x 0,47 x 0,04 inča), Samsungova MMCmicro (slika 17) kartica nešto je veća od MicroSD kartice. Ali, pored ovih proporcija, reč "veća" zvuči gotovo smešno. Očigledno je da je unutra skrivena SLC fleš kartica, što dokazuje i činjenica da su njeni nivoi na-pona napajanja 3,3 ili 1,8 V. Maksimalni ka-pacitet trenutno iznosi 4 GB, ali to će se sigurno povećati u skorije vreme.



Slika 16: Multi media Card

Slika 17: MMC mikro kartica

3.4.4 Micro SD

Micro SD kartica poznata je i kao TransFlash Sa dimenzijama od samo 15 x 11 x 1 mm (0,59 x 0,43 x 0,04 inča), MicroSD kartica može poneti tiulu "najmanje memorijske kartice na svetu". Firma SanDisk je preuzela ovaj format, koji je originalni proizvođač izbacio na tržište pod imenom TransFlash. Slično tome, MicroSD (slika 18) nudi iste karakteristike i funkcije kao i standardna SD kartica, mada uz nešto sporije performanse. Međutim, ona se sjajno uklapa čak i u najmanje modele mobilnih telefona, a ni njen maksimalni kapacitet od 4GB nije baš tako mali. Do kraja ove godine, SanDisk obećava memorije sa 16GB.



Slika 18: Micro SD kartica sa adapterom

3.5 Ostali tipovi prenosivih memorijskih uređaja

3.5.1 SmartMedia

SmartMedia kartice (slika 19) su od 1995. razvijane u kompaniji Toshiba, i originalno su bile poznate kao Solid State Floppy disk. Danas ove memorijske kartice nisu više u upotrebi, pre svega jer su imale maksimalan kapacitet od 128MB (planirano je, ali nikada ostvareno 256MB). Osim toga njene dimenzije od $45.0 \times 37.0 \times 0.76$ mm nisu joj davale veliku prednost na tržištu. Najveći problem prilikom rekonstrukcije podataka sa njih, javio se jer su se proizvodile u dva različita tipa – na radnoj voltaži od 5V i novije sa radnom voltažom od 3,3V. Greška forenzičara da noviji tip stavi u stariji čitač, može da dovede do trajnog gubitka podataka. Danas se mogu naći adapteri koji omogućavaju da uređaji predviđeni sa za rad sa SmartMedia rade sa xD karticama.



Slika 19: SmartMedia kartica

3.5.2 xD-Picture Card

xD Picture kartice (xd – extreme Digital) razvile su kompanije Olympus i Fujifilm, a na tržištu su se pojavile u julu 2002. godine. Njene dimenzije su $20 \text{ mm} \times 25 \text{ mm} \times 1.78 \text{ mm}$. Iako su prvenstveno razvijene za digitalne aparate, danas su prisutne u uređajima za digitalno snimanje glasa i mp3 uređajima. Prilikom forenzike xD kartica (slika 20) treba razlikovati 3 tipa kartica. Prvi, najstariji i najsporiji M tip, koji koristi Multi Level Cell (MLC) arhitekturu i teoretski može da dosegne 8GB, drugi najčešće

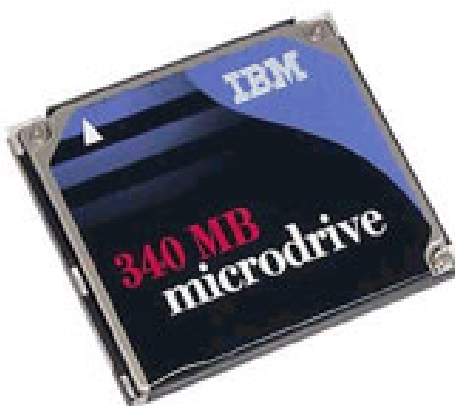
korišćeni H format i najnoviji M+ format koji radi 1.5 puta brže od M formata i kao H format ima maksimalnih 2GB.



Slika 20: xD Picture Card

3.5.3 IBM Microdrive

IBM-ov Microdrive (slika 21) nije tipični predstavnik prenosive *nonvolatile* memorije, budući da se zapravo radi o minijaturnom hard disku. Microdrive ima standardni CompactFlash+ Type II slot koji se koristi na svim prenosivim uređajima, poput digitalnih fotoaparata. U kombinaciji s PC Card adapterom koji se dobija uz Microdrive, ovaj minijaturni tvrdi disk može se koristiti na svakom laptop računar.



Slika 21: IBM microdrive

3.5.4 Sony MemoryStick

Sony je velika kompanija koja ima snage da progura vlastiti "standard" na području memorijskih kartica. Dimenzija 50.8x21.4x2.7 mm, MemoryStick je mala pločica koja se koristi u velikom broju uređaja, a ponajviše u Sonyjevima digitalnim fotoaparatima i kamerama. MemoryStick koristi 10-pinski konektor i serijski način prijenosa podataka. Nova verzija kartice, MemoryStick Duo je dimenzija 20x31x1.6 mm. Kako bi ostala kompatibilna sa "starim" memorijskim karticama, Duo kartica dolazi s adapterom koji je prilagođava starim dimenzijama. Nove dimenzije pre svega su bile potrebne zbog tržišta ručnih računara (PDA) i mobilnih telefona. U decembru 2006. godine Sony je proizveo Memory Stick PRO-HG, najbrža varijanta ovih

kartica, spremna za korišćenje u najnovijim modelima kamera i digitalnih aparata (slika 22).



Slika 22: Memory Stick PRO Duo i adapter za nju

3.5.5 Disk on module

Disk on Module (DOM) je fleš memorijska kartica (slika 23) sa IDE 40/44 konektorom te se samim tim može koristiti za direktno povezivanje na matičnu ploču. Najveće memorije ovog tipa imale su 16GB, sa tendencijom rasta, ali je njihova proizvodnja prestala. Razlog prestanka proizvodnje ponajviše je u pojavi adapte, kojim se CF karice povezuju na IDE interfejs.



Slika 23: Disk on module

3.5.6 SDXC (eXtended Capacity)

SDXC kartice predstavljaju najnoviji standard memorijskih kartica, i samim tim drastično povećavaju mogućnosti i zahteve prosečnih korisnika, kojima je sada omogućeno da bez ikakvih problema snimaju video u visokoj rezoluciji, i smeste svoj višegodišnji foto-na njih. SDXC memorijska kartica podržava kapacitet do 2TB (2 tera-bajta = 2000 GB) i brzinu upisa i čitanja od neverovatnih 104 MB/sec. Da bi sve ovo postigla SDXC kartica koristi Microsoft-ov exFAT standard upisa. SDXC kartica će zadržati dimenzije koje su imale SD i SDHC kartice, i odgovaraće uređajima koji su ih koristili ako im mogućnosti dozvoljavaju da podrže znatno veće kapacitete i brzine.

4 USB I CF U PRAKSI

Danas je svima jasno da ova minijturna čuda postaju neizbežna. Svojim rasprostranjivanjem sa tržišta polako izbacuju hard diskove i CD/DVD diskove. Količina podataka koja se na njima nalazi iz dana u dan je sve veća. Međutim ta rasprostranjenost može da izazove i neke negativne posledice. Svako ko želi da prokrijumčari ili ukrade podatke, a da pritom ne bude otkriven, može veoma lepo da iskoristi ove mikro kartice, iz jednostavnog razloga što može da se desi da ih uobičajene sprave za detektovanje uopšte ne registruju.

4.1 Korišćenje USB fleš memorije

4.1.1 *Prenos ličnih podataka*

Danas se usb fleš ponajviše koristi da bi se sačuvali i nosili sa sobom lični podaci, kao što su dokumenti, slike, audio – video zapisi, sačuvani podaci o napredovanju u igrici... Osim toga oni preuzimaju prevlast u još nekim sferama... Jedan od primera jeste pojava takozvanih „Portabl aplikacija“ uz pomoć kojih se na fleš disku može naći i baza mail poruka, istorija posećenih stranica i sl.

Sve niža cena fleš memorija dovela je do toga da se neretko sreću veličine od 16GB. Ako uzmemo u obzir da prosečan MS Word dokument od deset stranica ima veličinu od oko 60kB, znači da potencijalno možete snimiti 280000 dokumenata, ili 3 miliona stranica, na jednom disku. Takva priuštivost, prenosivost i kapacitet tih uređaja stavili su ih na među dva najveća rizika za kompanije, ali i pojedince. Krađa fleš diska predstavlja krađu intelektualnog vlasništva vlasnika, ali često i trajni gubitak podataka. Kada jednom padnu u pogrešne ruke, ovi podaci mogu otići u konkurentske kompanije, u javnost, ili čak da posluže za krađu identiteta. Evropska agencija za sigurnost mreža i zaštitu podataka (ENISA) procenila je nedavno da je šteta pri svakoj krađi informacija sa USB fleš uređaja oko 7000 evra, kada je reč o pojedincima, ili čak 1,3 miliona kada su u pitanju kompanije ili državne institucije. U zaključaku tog istraživanja ENISA, je kao meru zaštite predložila, kompanijama i institucijama da uvedu pravilo da se zabrani korišćenje ličnih USB memorijskih uređaja na radnom mestu.

Moderni forenzički alati mogu, u slučaju da se sumnja da je neko uz pomoć USB fleš memorije ukrao poverljive podatke otkriti kada je bio spojen na kompjuter, proizvođača, serijski broj, ali i što je najbitnije i podatke iako je korisnik pokušao da ih obriše.

4.1.2 *Automatsko prikupljanje podataka*

Bez nekog velikog iskustva prosečni korisnik internet može lako doći do programa koji će njegov fleš disk pretvoriti u takozvanog USB lopova. Gotovih rešenja je na sve strane, a ne mora se biti veliki programer, a da se napravi *autorun* fajl, koji će pokrenuti softver koji će sa žrtvinog računara pokupiti sve šifre, chat istoriju, otvorene portove... Najveću popularnost imaju alati firme NirSoft, ali postoje i firme koje kao gotov proizvod prodaju USB kradljivce mnogo većih mogućnosti. Takvi programi mogu u rukama digitalnog forenzičara postati i dobar alat, ali su slučajevi takvog korišćenja još uvek retki, pre svega jer se tako prikupljeni podaci ne mogu smatrati valjanim dokazima.

4.1.3 Širenje zlonamernog softvera

Prema izveštaju firme Sophos 4. po redu način širenja računarskih virusa i crva u 2008. godini jeste uz pomoć prenosnih memorijskih uređaja. Možda najbizarniji primer ovakvog načina prenosa zloćudnih programa koji se dogodio tokom 2008. godine je onaj kada su astronauti iz NASA-e nepažnjom preneli crv W32.Gammima.AG putem USB memorije na internacionalnu svemirsku stanicu. Antivirusni program je, srećom, detekovao zlonamerni program, ali su posledice mogle biti katastrofalne.

4.1.4 Audio plejeri

Mnoge kompanije prave audio plejere u obliku USB flash drive – a. Štaviše USB plejeri trenutno imaju monopol u toj oblasti. Najpopularniji audio plejer u ovakvom obliku je iPod, kompanije Apple Computer's. Većina tih uređaja ima u sebi i funkciju za snimanje glasa, te se dokazi u audio obliku često mogu naći i na njima. Iako sami ti audio zapisi na sudu nisu valjani dokazi, digitalni forenzičar može pomoću ostalih podataka koji se nađu snimljeni na njima dokazati njihovu pripadnost osumnjičenom licu. Neke kompanije, kao što je Sony, pokušale su da razviju posebne fajl sisteme i formate muzičkih zapisa (kompresija) za svoje uređaje, ali su ubrzo izgubile bitku, pred uređajima koji se pri priključivanju na PC ponašaju kao najobičniji USB flash, a reprodukuju muziku u najpopularnijim formatima (mp3, wma...). Ipak zbog nemalog broja uređaja koji zahtevaju posebne programe za pristup njihovom sadržaju, koji su još uvek u upotrebi, prilikom forenzičke analize treba posebno obratiti pažnju na model uređaja, jer se iz uobičajnih Windows alata ne mogu otkriti svi zapisi.

4.1.5 ReadyBoost

Windows Vista poseduje novu tehnologiju koja u teoriji poboljšava njene performanse i donose novo iskustvo u interakciji sa smim operativnim sistemom, a zasniva se na korišćenju USB fleš diskova. U pitanju je *ReadyBoost* mehanizam, koji redukuje vreme potrebno za pokretanje popularnih aplikacija. ReadyBoost, dozvoljava proširivanje sistemske memorije priključivanjem USB 2.0 fleš memorije. Iako se brzina transfera preko USB 2.0 ne može porediti sa brzinama modernih hard diskova, vreme pristupa flash memoriji praktično ne postoji, što čini ove naprave jeftinom keš memorijom. Iako su podaci na ovaj način smešteni na USB fleš praktično nekorisni, sve veća popularnost među korisnicima i pojava korisničkih aplikacija koji omogućavaju rad te tehnologije na operativnom sistemu *Windows XP*, za istražitelje digitalnih dokaza biće sve zanimljiviji.

4.1.6 Forenzički alat

Do skora ne zamenjivi mediji prilikom digitalne forenzike Live CD i DVD diskovi polako gube primat, pred naježdom USB fleš memorija. USB disk može poslužiti za podizanje Live operativnog sistema, tj. sistema koji neće ugoziti podatke na postojećem čvrstom disku računara, ali se danas najčeće koristi za pravljenje duplikata digitalnog mesta krivičnog dela. Takođe u popravci računara i backupu podataka USB memorije postaju nezaobilazni alat. Često se na njima drži neki antivirus program kao i ostali programi za softversko održavanje sistema i sistemske administraciju. Kompanija SanDisk predstavila je USB fleš koji automatski *pravi backup podataka* na mreži tako da, za slučaj da se on pokvari ili izgubi, datotekama se jednostavno može pristupiti putem Interneta.

4.2 Korišćenje memorijskih kartica

4.2.1 Prenosivi računari

Gotovo da ne postoji prenosivi računar na tržištu koji na sebi nema ugrađen čitač raznih tipova memorijskih kartica, pored standardnih USB priključaka. Iako sa tim funkcionalnostima laptop računara memorijske kartice mogu da budu i vrsta medijuma za prenos podataka, najčešće se ne koriste u te svrhe, već korisnici ugrađene čitače koriste za brži prenos podataka unetih drugim uređajima, ponajviše digitalnim aparatima i mobilnim telefonima

4.2.2 Digitalni aparati i kamere

Samim pomenom CF memorija, većina upoznata sa terminologijom, automatski pomisli na digitalne aparate. Iako do skoro nije bilo jasno ko je vođa, a ko pratioc, danas je jasno da se razvojem digitalnih aparata, sve većim kavalitetom slika koje mogu da izrade, javlja sve veća potreba za memorijama koje oni koriste. Njihove sve manje dimenzije naravno su razlog za minimiziranje memorijskih kartica.

Digitalni aparati i kamere postali su, u poslednje vreme, alat za izvršavanje krivičnog dela. Forenzičari u svetu svakog dana pokušavaju, istragom podataka na memorijskim karticama, da dođu do krivca, najčešće u oblasti dečije pornografije. Često je ovakva vrsta istrage veoma teška, jer počinioци krivičnih dela lako sakrivaju memorijske kartice. Problem forenzičarima predstavlja i način usnimavanja podataka, fajl sistemi na karticama (najčešće FAT 12), jer se oni dosta razlikuju kod svakog proizvođača digitalnih aparata.

4.2.3 Mobilni telefoni, PDA uređaji

Mobilni telefoni i PDA uređaji svakodnevno dobijaju „bitku“ sa stonim PC računarima. Kalendar, adresar i lista tekućih zadataka, pojavom PDA uređaja predstavljaju potpuno rešenje za optimizaciju i lakšu organizaciju vremena. Iako većina korisnika, iskorišćava samo mali broj mogućnosti ovih uređaja, PDA polako ulazi u sferu multifunkcionalnosti, koji uz sve veću ponudu softvera i moćniji hardver mogu omogućiti "krstarenje" Internetom, prezentacije ili čak bežičnu administraciju udaljenih mreža. Neki noviji modeli mobilnih telefona ne zaostaju u pogledu funkcionalnostii za PDA uređajima. Šta sve forenzičar može naći pretragom tih uređaja?

Zbog ograničenosti veličine, rešenje za smeštanje podataka u mobilnim telefonima i PDA, nađeno je upravo u minijaturnim memorijskim karticama. Iako većina mobilnih telefona ima svoju memoriju, takođe zasnovanu na fleš tipu, zahtevima korisnika za stalnim proširivanjem, proizvođači izlaze u susret dodavanjem slotova za memorijske kartice. MMC kartice su do skoro bile osnovni tip koji se sretao, najviše u mobilnim telefonima, marke Nokia i Sony Ericsson, dok se proizvođači danas najviše odlučuju za Micro SD kartice.

Većina modernih mobilnih telefona ima i funkciju fotografisanja, često takvu da zadovoljavaju i profesionalne zahteve. Samim tim i oni mogu zameniti digitalne aparate, pa forenzičari podobno moraju ispitati slike uskladištene na njihovim memorijama.

Iako su gotovo svi moderni mobilni i PDA uređaji opremljeni USB portovima za sinhronizaciju sa PC računarima, u praksi se pokazalo da većina korisnika koristi čitače memorijskih kartica za transfer podataka, prvenstveno zbog brzina prenosa.

4.2.4 Čitači memorijskih kartica (*Memory Card Reader*)

Čitači memorijskih kartica (slika 24) su uređaji koji se koriste za pristup podacima na memorijskim karticama, koje koriste razni uređaji kao što su digitalne kamere i aparati, igračke konzole, mobilni telefoni itd.



Slika 24: Čitači memorijskih kartica

Vrste čitača – Čitači se mogu podeliti po načinu spajanja na unutrašnje (interne) i spoljašnje (eksterne). Druga vrsta podele je s obzirom na mogućnosti za čitače sa samo jednim slotom, serijske čitače i multi čitače.

Čitači sa samo jednim slotom (Single Slot Card Reader) mogu čitati podatke sa samo jedne određene vrste kartica (npr. SD)

Serijski čitači (Series Card Readers) imaju više portova, ali isto samo za jednu vrstu memorijskih kartica (npr. 4x SD).

Multi čitači (Multi-Card Readers) su danas najrašireniji čitači memorijskih kartica. Ovi čitači mogu čitati više vrsta memorijskih kartica kao što su Compact Flash I (CF-I), Compact Flash II (CF-II), Secure Digital (SD), Memory Stick (MS), XD-Picture (XD), MultiMedia Card (MMC), SmartMedia (SM/SMC), MiniSD, MicroSD, SDHC, MMC Plus, MMC Mobile, MicroDrive, Memory Stick Pro Duo, MagicStore Drive itd. (npr. 12-in-1)

Čitači se spajaju na računar najčešće preko USB ili Firewire porta dok se na prenosive računare mogu ubaciti u PCMCIA ili ExpressCard slot.

4.3 Sigurnost podataka na fleš memorijama

Većina korisnika koji za prenos podataka koriste USB fleš ne razmišlja mnogo o sigurnosti podataka koji su snimljeni na njemu. Ipak ima onih kojima je sigurnost na prvom mestu. U upotrebi je više različitih rešenja koja mehanički štite fleš diskove i memorijske kartice. Proizvođači u svojoj ponudi imaju rešenja i za one koji ne žele da podaci koji su snimljeni na USB flešu dođu u pogrešne ruke. Nekada se sve svodilo samo na prekidač kojim bi se zabranio upis, ali zbog njegove beskorisnosti prestalo sa proizvodnjom takvih rešenja. Najnovija rešenja pružaju 256 bitnu hardversku enkripciju podataka. Neretko je moguće čak i kreirati višestruka zaštićena područja koja su zaštićena posebnom lozinkom ili otiskom prsta na skupljim uređajima. Podaci

se u ta područja mogu jednostavno kopirati i biće automatski kriptovani u „letu“. Kao dodatak ugrađena tome, u mnoge, je ugrađena „*File Shredder funkcija*“ koja uklanja sve tragove obrisanih podataka. Na taj način nije ih više moguće rekonstruirati posebnim forenzičkim programima već su obrisani zauvek. Do sada su bili podržani isključivo Windows sistemi, a sada i Mac korisnici mogu iskoristiti mogućnosti koje nude drajvovi sa povišenim stepenom bezbednosti podataka.

Osim hardverskih postoje i mnoga softverska rešenja kao što je *USB Lock AP* kompanije Advanced Systems International koji prebacivanjem samo 3 fajla na USB disk omogućava iste funkcionalnosti kao i hardverska zaštita. U slučaju da se želi potpuna zabrana rada sa USB memorijama malom izmenom u Windows registry bazi može se omogućiti neometan rad ostalih USB uređaja, koji se priključuju na PC, a zabraniti korišćenje fleš diskova.

5 FORENZIKA USB I CF UREĐAJA

„Pojava USB diskova tvrtkama je donijela velike probleme zbog potencijalne krađe podataka. Jednog dana, kada djelatnik ode iz tvrtke, tim podacima može čak i ucjenjivati tvrtku.“⁹

Šta treba da zna forenzičar pre nego što se usmeri na rad sa prenosivim uređajima? Do prenosivih memorija teško je doći, zbog njihove veličine. Tehnikama pronalaska se nećemo baviti u ovom radu, već samo metodama koje forenzičari trebaju da primene kada već imaju memorijski uređaj „u rukama“. Sa forenzičkog aspekta važno je da forenzičar pouzdano identifikuje tip medijuma sa kojim radi. Jedna od mogućnosti je pažljivo ispitivanje nalepnice na medijumu, ali i ovo nije sigurna metoda, jer može predstavljati zamku. Forenzičar ne sme da pretpostavlja koji je tip kartice u upotrebi. Svakako uvek mora imati na umu da ako osumnjičeni ima neki tip nestandardne memorije, najverovatnije ima i čitač za nju. Osim standardnih metoda koje se primenjuju pri digitalnoj forenzici forenziku USB memorija treba obaviti u tri faze.

5.1 Utvrđivanje relevantnih činjenica

Pre pristupanja pravljenja slike prenosive memorije kao digitalnog dokaza digitalni forenzičar treba da utvrdi i sve detalje neophodne za kompletan opis budućeg posla. Posebnu pažnju treba usmeriti na tip i oznaku memorije, specijalne oznake, vrste enkripcije ako postoje, vrstu fajl sistema, tipove potrebnih datoteka i sl.

5.2 Izrada procene uspešnosti

U ovoj fazi forenzičar mora da utvrdi da li je osumnjičeno lice obrisalo tj. pokušalo da uništi digitalne dokaze, te ne osnovu ranije utvrđenih činjenica pravi procenu uspešnosti oporavka podataka u svrhu obezbeđivanja validnosti oporavljenih podataka kao dokaza pred sudom.

5.3 Kreiranje kopije podataka

Većina fleš memorijskih uređaja izgleda slično – memorijski čip prati odgovarajući kontroler. Ova dva elementa čine praktično ceo uređaj odnosno memoriju. Memorijski čip je u skoro svim vrstama memorijskih kartica, USB flash diskova kao i većini drugih digitalnih uređaja baziran na NAND tehnologiji i dolazi u klasičnom TSOP-48 kućištu. Svakako činjenica da algoritam upisa/čitanja podataka razlikuje od proizvođača do proizvođača, u znatnoj meri otežava proces spašavanja podataka.

Iako veliki broj poznavaoaca računarske tehnologije smatra da je spašavanje podataka sa ovih memorija nemoguće, ta izjava je tačna samo u slučaju kada je memorijski čip uništen (slomljen ili pregoreo). Ovo se naravno odnosi na memorije nad kojima nije izvršeno namerno prepisivanje podataka ili memorije koje imaju izvesne hardverske ili softverske sisteme zaštite. Što se ostalih hardverskih problema tiče daleko je veća verovatnoća otkaz kontrolera, odnosno čipa koji je zadužen za upis podataka u memoriju kao i za čitanje podataka. U tom slučaju postoje velike šanse, da se uz pomoć odgovarajućeg forenzičkog alata ostvari 100% uspeh spašavanja podataka.

⁹ „Poslovni savjetnik – magazin za menadžere i preduzetnike“, broj 36, novembar 2007, Zageb, Hrvatska

Prisutni kontroler određuje algoritam kao i veličinu segmenta za upis i čitanje podataka. Potrebno je “razbiti” algoritam. Algoritam koji je primenjen predstavlja zaštićeni mehanizam, odnosno patentiran je od strane proizvođača i nije javno dostupan.

Prilikom pravljanja slike (ogledala) forenzičar mora da obrati pažnju na to da se podaci na memorije smeštaju potpuno drugačije nego u hard diskovima. Celokupna memorija je podeljena na “strane”, veličina strane kao i način smeštanja zavisi od tipa algoritma koji je primenjen. Takođe raspored strana u okviru same memorije nije linearan, u zavisnosti od tipa primenjenog algoritma postoji više mogućih varijanti mix-a samih strana.

U slučaju da je potrebno izvršiti forenziku nad oštećenim memorijama zasnovanim na fleš tipu ili obrisanim podacima treba izvršiti sledeće:

- Odvojiti memorijski čip od oštećenog uređaja
- Pročitati sve sektore memorije i kreirati identičnu “sliku” memorije
- Detektovani određeni mix strana memorije
- Otkloniti mix
- Primenom adekvatnog algoritma sve stranice spojiti u jednu celinu

Nakon ovog procesa moguć je logički pristup podacima. Odnosno neophodno je odrediti parametre primenjenog fajl sistema (90% slučajeva FAT12) i nakon toga restaurirati logičku strukturu i kopirati podatke.

Izuzeci od opisanog postupka postoje. Mini i Micro SD kartice ne poseduju kontroler, a neki uređaji imaju enkriptovane strane u okviru memorija koje je nemoguće dekriptovati u slučaju otkaza kontrolera.

6 PRIKUPLJANJE I PROVERA DIGITALNIH DOKAZA

„Ne postoje neosvojive tvrđave, postoje samo loši napadači.“¹⁰

„Ne obara se svako drvo prvim udarcem.“¹¹

Osnova digitalne forenzike nije da tvrdite da su se na fleš disku, nađenom kod jednog od zaposlenih, kriju informacije koje bi mogle da ugroze rad kompanije. Uspešnost istrage ogleda se u tome, koliko uspešno je forenzičar uspeo da digitalne forenzičke dokaze prebaci sa jedne na drugu lokaciju, bez kontaminacije, a zatim na valjan način dokaže sudiji i poroti da se taj dokaz našao baš tu i da je za to kriv baš taj radnik. Bez nekih osnovnih postupaka u samom startu dokazi mogu biti odbačeni ili se može dovesti u pitanje njihova valjanost. Iako pojmovi koje smo ovde opisali možda deluju isuviše jednostavni boljim poznavaocima informatičke struke, oni su sastavni deo rada većine vrhunskih forenzičara.

6.1 Pravilno prikupljanje digitalnih dokaza

Akvizicija digitalnih dokaza je najvažniji deo dobre forenzičke istrage, pa se dokazi moraju prikupiti na najprofesionalniji mogući način. Primarnu stvar u procesu akvizicije digitalnih dokaza, sa USB i CF memorijskih uređaja, predstavlja pravljenje sigurne kopije podataka, bez ikakve promene na njima tokom tog procesa. U zavisnosti od tipa memorije na kojoj se vrši akvizicija, njene veličine, tipa i sl. zavisi i na kom mediju se pravi sigurnosna kopija. Karakteristično za prenosive memorije je da je često teško utvrditi veličinu same memorije (pogrešna nalepnica, kućište...), ali se sa sigurnošću gotovo uvek može utvrditi o kojoj se memoriji radi. Naravno od forenzičara se očekuje da poznaje sve moguće tipove ovih uređaja.

Osim načina rada sa medijima i digitalnim dokazima na njima najvažnija stvar u toku akvizicije dokaza jeste pravljenje dokumentacije i pridržavanje određene metodologije rada. Pravilna i već dokazana metodologija najverovatnije će dovesti do željenog i valjanog rezultata, a bez dokumentovanja svakog koraka teško je kasnije braniti dokaze otkrivene u istrazi.

Uopštena metodologija prilikom akvizicije podataka sa prenosivih memorija je:

1. Otkrivanje tipa memorije
2. Pronalaženje odgovarajućeg alata (softverskog ili hardverskog) za rad sa tim memorijskim uređajima
3. Kopiranje podataka
4. Utvrđivanje autentičnosti kopiranih podataka
5. Pravljenje duplikata duplikata

¹⁰ Napoleon I Bonaparta

¹¹ Kineska poslovice

U digitalnoj forenzici postoji pravilo koje treba poštovati i zapamtiti: **Original dodirni jednom, kopiju dva puta, a radnu kopiju onoliko puta koliko ti bude potrebno.**

6.1.1 Otkrivanje tipa memorije

Prvi korak u akviziciji jeste utvrđivanje tipa memorije. Ranije smo dali pregled svih do sada poznatih tipova prenosivih memorija. Na tržištu su se u međuvremenu pojavili prenosivi diskovi koji podržavaju serijsku vezu sa računarom tipa USB 3.0, ali se oni osim brzine prenosa tj. kontrolera ne razlikuju od dosadašnjih uređaja.

Dovoljno neupućenima može delovati da je ovaj posao lak, posebno kada su u pitanju prenosive memorije, jer one uglavnom na svojoj spoljašnjosti imaju upisano ime proizvođača i veličinu, a upravo to može biti krucijalna greška. Šta ako je zlonamerni vlasnik namerno promenio kućište i postojeću memoriju ubacio u drugo kućište? To i nije naročito težak posao za kriminalce, ali jeste za forenzičare koji trebaju da utvrde koja je memorija u pitanju i koliki je njen kapacitet. Većina proizvođača ima isto kućište za svoje memorije proizvedene u istoj seriji, a već odavno je u forenzici standardnih magnetnih memorija poznat slučaj sakrivenih particija. Iako se najčešće na memorijama USB i CF tipa nalazi samo jedna particija poznat je i slučaj terorista iz Avganistana koji su poverljive informacije prenosili na ovim uređajima, iako su svaki put bili pregledani.

Greška detektiva koji su obavljali posao pregleda ovih uređaja nažalost usledila je kasno. Naime teroristi su sa sobom nosili fleš memorije na čijem kućištu je bilo upisano da su veličine 64mB. Prilikom pregleda detektivi su uvek nalazili samo muzičke numere u mp3 formatu, koje su popunjavale veći deo od 64mB. Teroristi su osim lažiranja kućišta memorije koristili i mogućnost da se „slika“ eng, image nekog manjeg diska nasnimi na veći, koji pri tome, najčešće u operativnim sistemima Windows dobijaju sve odlike manje memorije. Kasnije su na odredištu uz pomoć softverskih alata, neretko i forenzičkih, kopirali podatke sakrivene na preostalom delu diska. Čak i da bi se tu zaštitili koristili su slike u formatu jpg, u kojima su bile sakrivene bitne informacije. Za ovu prevaru forenzičari su saznali tek nakon istrage sprovedene posle terorističkih napada na Ameriku, u septembru 2001. godine.

Postoje razni načini sa svojim vrlinama i manama za izbegavanje ovakvih slučajeva. Neki autori koji se bave forenzikom smatraju da je dovoljno doći do tipa memorijskog čipa, sa njega preuzeti serijski broj i ime kompanije koja ga je proizvela pa zatim od nje dobiti sve potrebne podatke. Taj način jeste donekle siguran (rizik uvek postoji), ali često je i veoma spor.

Najsporiji, ali najsigurniji način jeste skidanje memorijskog čipa, a zatim čitanje svih sektora i kreiranje identične slike. Međutim u poslednje vreme tom načinu forenzičari sve manje pribegavaju, jer je u upotrebi dosta kriptovanih fleš memorija, gde ovakav postupak odvajanja memorije od kontrolera dovodi do gubljenja podataka.

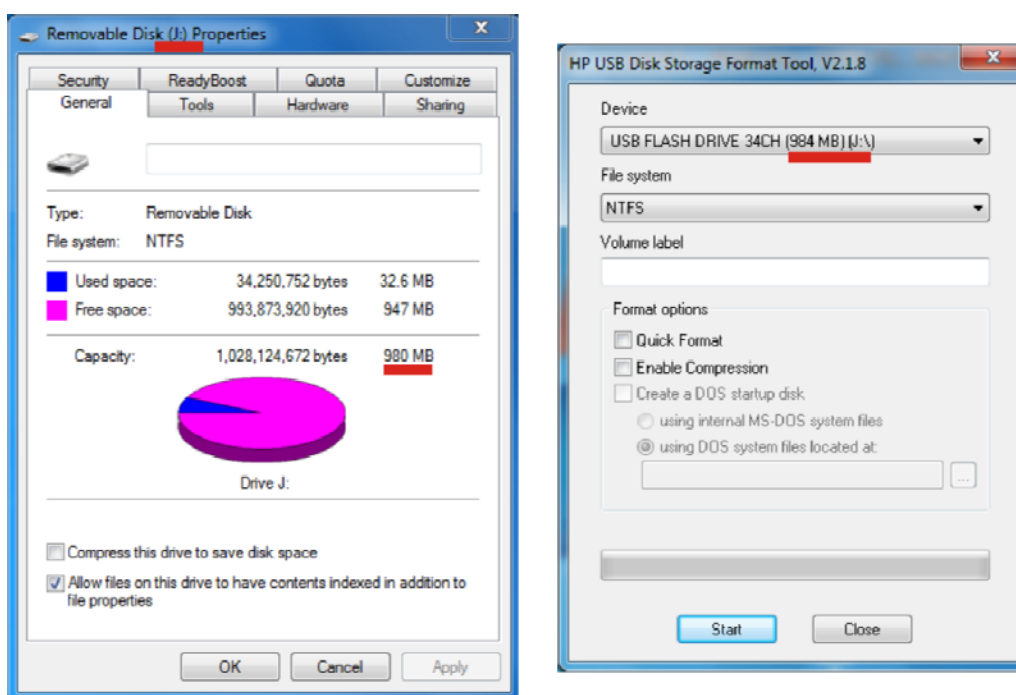
Za potebe istrage proizvođači izlaze u susret i daju sve moguće informacije, ali samo ako im to zatraži vlada neke države, mada i to nije uvek siguran put.

6.1.2 Pronalaženje odgovarajućeg alata

Tokom akvizicije vrši se takozvano bit po bit kopiranje podataka. U ovom, neretko teškom i dugotrajnom procesu treba iskopirati svaki bit originalnog medija, od

fizičkog starta do fizičkog kraja. Koncept je u teoriji lak, ali u praksi često veoma težak, posebno kada forenzičar nema odgovarajući alat. Naravno, kao osnova svega u forenzici prenosivih memorija, od forenzičara se očekuje da poseduje odgovarajući konektor za različite tipove medija. Zato uvek treba imati prave čitače, jer se bitni podaci mogu izgubiti, ako npr. forenzičar za rad sa memorijskim karticama korisiti čitač koji pri povezivanju na računar simulira postojanje USB fleš diska.

Operativni sistemi lociraju prostor na memorijama priključenim na računar, ali uvek postoji mali deo memorije koji nije pristupačan operativnom sistemu. Na primer, Microsoft Windows, fleš memorije većiine 1GB često vidi kao uređaje sa manje od 1000MB¹² prostora, kao što je prikazano na slici 1.



Slika 25: Različite veličine istog medija u Windows OS

Ovaj dokaz ne znači da se „ekstra“ prostoru ne može pristupiti uz pomoć određenih softverskih alata već, već da operativni sistem to ne može da uradi.

Kako operativni sistem, posebno Windows, ne rade na ovaj način, za rad sa memorijama potreban je odgovarajući alat. Postoje brojni Windows alati kao što su EnCase i FTK, kao i brojni alati koji rade u Linux okruženju. Ako se forenzičar dobro snalazi pod Linuxom (npr. njegova komanda „dd“) to je velika prednost, a ako ne uvek treba da ima na umu neke od ovih alata.

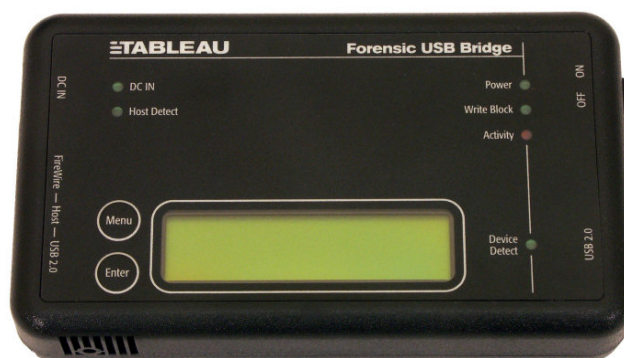
FTK/EnCase/Paraben: Softverski alati koji rade na većini operativnih sistema (Windows, Linux, Mac). Samim tim što poseduju grafički interfejs dosta su lakši za korišćenje od većine drugih alata...

¹² 1GB = 1024MB, ali većina proizvođača kapacitet memorijskih uređaja sa oznakama od 1gB pravi u kapacitetu od 1000mB

Hex editori/ Sistemski alati: Softverski alati za dublje pretraživanje fajl sistema i njihovih fajlova. Napredniji forenzičari uz pomoć ovih alata mogu da dođu do mnogih rezultata, ali je za rad sa njima potrebno odlično poznavanje strukture fajlova.

Duplikatori diskova: Hardverski alati koji na veoma pouzdan i brz način vrše dupliciranje sadržine diskova.

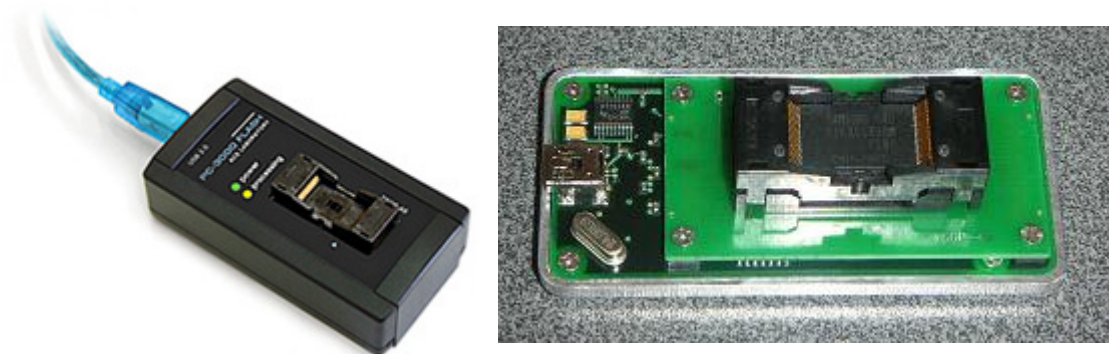
Zaštitnici od upisivanja: Hardverski alati (slika 26) na koje se priključuju memorijski uređaji pre povezivanja na računar. Oni omogućavaju pregledanje sadržaja diskova bez rizika da će se desiti ikakva izmena originala



Slika 26: UltraBlock USB Write Blocker

Zaštita od upisivanja je predstavlja jedanu od najbitnijih činilaca forenzičke akvizicije. Zaštiti prenosivu memoriju od upisivanja često je dosta teško, iako mnoge poseduju i ugrađene mehanizme za to. Sadržaj na memorijskoj kartici u fotografskom aparatu ili mobilnom uređaju, neće biti isti nakon gašenja i ponovnog paljenja. Zato je veoma bitan i način na koji se takve memorije uzimaju sa lica mesta. Forenzičar se često može naći u nedoumici šta da uradi. Univerzalna pravila ne postoje, ali nekoliko opštih se uvek treba držati. Svakako, uređaj ne sme biti na silu isključen sa kompjutera. Ako je u pitanju USB fleš disk, čak iako je u toku njegovo formatiranje, ne treba na silu prekinuti taj proces. Veći je rizik da će u tom slučaju doći do otkaza memorije, nego da će podaci uz pomoć nekog forenzičkog alata biti spašeni.

Uvek treba imati na umu da su flash diskovi i memorijske kartice preosetljive na električna pražnjenja, a problematično isključivanje sa napajanja može dovesti do otkaza. Na te probleme treba dodati i ograničen broj upisa u svaku memorijsku lokaciju, zbog čega je algoritam upisa komplikacija sama za sebe. Implementarni algoritmi „štede“ memorijske lokacije i „troše“ ih ravnomerno. Najveći problem je u tome što kod ovih memorija najčešće otkazuje kontroler, pa se sadržaj čipa mora isčitati sa specijalnim alatima (slika 27), koji uz pomoć implementiranih operacija emuliraju rad kontrolera. Čak i sa ovim uređajim posao zna da bude veoma težak, a razlog tome je veliki broj proizvođača, nepostojanje standarda i relativno kratak period eksploatacije.



Slika 27: Acelab Flash reader i Soft Center Flash reader

Sterilni mediji

Odabir odgovarajućeg softverskog ili hardverskog alata, ma koliko on bio dobar neće značiti ništa ako se za pravljenje kopija ne koriste takozvani sterilni mediji. Zamislite da na video kaseti gde je snimljen neki igrani film, snimate dečiji rođendan. Prilikom gledanja kasete odmah nakon završetka rođendanskog snimka, nastaviće se deo filma koji nije presnimljen. Upravo ista situacija različitog miksa desiće se i ako se ne koristi odgovarajući medij.

Postoje brojni softveri za brisanje sadržaja medija (naravno misli se na višestruko upisivanje nasumičnih nizova bitova). Korišćenje ovih softvera je neophodno da se ne bi desilo da cela istraga „padne u vodu“. Ovi alati su najčešće deo svakog, iole boljeg softverskog alata za digitalnu forenziku, ali se na internetu lako mogu naći nezavisni alati kao što su:

LSoft Technologies Hard Drive Eraser (www.lsoft.net): Besplatan alat koji zadovoljava sve zahteve Ministarstva odbrane SAD

Blancco Data Cleaner (www.blancco.com): Alat nije besplatan, pruža malo lakši rad, i takođe zadovoljava standarde koje je propisala Vlada SAD¹³.

Eraser (www.eraser.heidi.ie): Besplatan alat, čiji autori tvrde da poseduje algoritme kojima nudi čak i više propisanih standarda.

Većina alata¹⁴ koji se mogu naći posao brisanja podataka radi poprilično dobro, jer u principu sve što treba da urade jeste da prepisu preko memorijskog uređaja. Jedini problem može da se javi u vezi vremena koje je potrebno da obave taj posao.

¹³ Ne postoje standardi propisani od strane Vlade Republike Srbije

¹⁴ Dosta informacija u vezi sigurnog brisanja podataka sa medija *eng. wipe* može se naći na internet stranicama Američkog nacionalnog instituta za standarde i tehnologiju (NIST) na adresi: http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

6.1.3 Kopiranje podataka

Podaci tj. dokazi se sa prenosivih memorija mogu preuzeti na više načina, ali samo par njih su forenzički. Korišćenje različitih tehnika prvenstveno diktiraju okolnosti same forenzičke istrage i alat koji forenzičar poseduje. Često je u istrazi najteža odluka raditi na terenu, ili u laboratoriji.

U procesu kopiranja podataka treba se držati sledećih pravila:

1. Sa sigurnošću **utvrditi tip medija** na kome se vrši forenzika.
2. Naći isti tip medija, pripremiti ga („sterilizovati“), a ako to nije moguće odlučiti se za najbolju moguću zamenu. Moguće je i pripremiti prostor na fiksnoj memoriji računara tj. dodatnim memorijama, gde bi se kopija smestila u fajl.
3. Koristiti blokatore upisa

U zavisnosti na tip alata sa kojim se radi treba izvršiti blokadu upisa na memoriju na kojoj se nalaze dokazi. Najveći broj hardverskih duplikatora (slika 28) poseduje priključak na kojem je upis u memoriju onemogućen. U svakom slučaju, pre forenzike treba dobro proučiti mogućnosti alata i pročitati uputstvo proizvođača.



Slika 28: Forensic duplicator

Pri kopiranju uz korišćenje računara, i softverske alate, forenzičar mora dobro da poznaje prirodu operativnog sistema i mogućnosti softvera. U praksi su se najbolje pokazale „live“ verzije operativnih sistema, posebno pripremljene za forenziku (Helix, CAIN, Deft...), koje neće ništa upisati na fizički medij, osim ako to korisnik ne zahteva. Softverski forenzički alati poseduju blokatore upisa, ali treba biti oprezan, jer različito funkcionišu na različitim verzijama Windows operativnog sistema.

Forenzičar koji radi na Windows OS (XP, Vista, 7) može sam da blokira upis na prenosive memorije promenom u Registry bazi sledećim koracima:

1. **Priprema rezervne (back up) kopije Registry baze uz pomoć RegEdit alata:**
Otvaranje RegEdit:
 - a. *Klik na Start→Run (prečica Start+R na tastaturi)*
 - b. *U dialog box, ukucati regedit i stisnuti Enter*
 - c. *Za čuvanje već podešenih Registry podešavanja, odabrati File→Export*
2. Otići na **Computer/HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control**
3. **Desni klik na Control, a zatim odabrati New→Key. Imenovati ga kao StorageDevicePolicies**
4. **Desni klik u StorageDevicePolicies i zatim New→DWORD. Imenovati ga kao WriteProtect , a zatim stisnuti Enter.**
5. **Desni klik na WriteProtect i podešavanje vrednosti na 1 omogućiće zabranu upisa na prenosive memorije.**

Reverzno ovom procesu dovoljno je da se DWORD vrednost podesi na 0, ili da se vrati već postojeća kopija Registry baze.

4. **Korišćenje forenzičkog alata**
 Nakon što je sve uspešno povezao i proverio kontakte, forenzičar pristupa kopiranju podataka uz pomoć softvera ili hardverskog alata.
5. **Uklanjanje memorijskog uređaja**
 Kada alat završi posao kopiranja, bez dojava o bilo kakvoj greški u toku procesa, uređaj treba ukloniti i staviti ga na sigurno.
6. **Pravljenje radne kopije**
 Ako su ranije akcije uspešno izvedene, postoji slika memorijskog uređaja bilo na drugom uređaju, bilo u fajlu treba pristupiti pravljenju radne kopije, za koju se u svakom slučaju preporučuje da bude na što sličnijem uređaju, radi što boljeg utvrđivanja činjenica u daljoj istrazi.

6.1.4 Utvrđivanje autentičnosti kopiranih podataka

Podaci u digitalnom obliku se veoma lako mogu izmeniti, pa je u ozbiljnom forenzičkom procesu bitno dokazati da se nije dogodila ni jedna izmena u procesu akvizicije i analize. Zbog toga definisano je nekoliko načina da se dokaže integritet dokaza nakon što su prošli niz ruke forenzičara.

Primarni model koji koriste većina forenzičkih softvera, da bi zaštitili integritet dokaza, jeste korišćenje takozvanog *checksum* – a, koji najprostije rečeno predstavlja vršenje kalkulacija nad celim dokaznim materijalom i dobijanje odgovarajućeg *sum* – a (*sum* eng. – *rezultat* srb.). Kada se podaci prebace na računar na kome se vrši analiza, potpuno iste operacije se vrše nad kopiranim podacima, i ako se rezultati isti, može se

zaključiti da nije došlo do promene podataka. Moderni softveri za izradu checksum – a ne koriste jednostavne algoritme (nekada je to bila samo XOR operacija nad nizom bitova), jer ih je često lako prevariti ili zaobići i samim tim ugroziti integritet istrage.

Ključno za dobijanje dobre *hash* vrednosti jeste korišćenje kriptografskog heširanja – algoritma koji se može koristiti samo u jednom smeru. Drugim rečima ne postoji način da se reverznim inženjeringom dobiju originalni podaci, na osnovu izračunate vrednosti. Kriptografski hash algoritmi su dizajnirani tako da operaciju pokrenu na početku bloka podataka, a zatim formiraju fiksne nizove bitova. Teoretski šanse da dve različite vrednosti imaju istu vrednost nakon primene hash algoritma nalaze se u rangu 2^{65} .

U toku izrade ovog rada, dva najpoznatija hash algoritma ipak su probijena, ali statistički šansa da se desi tako nešto je skoro ravna nuli, pa je samim tim i rizik prihvatljiv. Međutim što se više povećava snaga računara, time je i rizik veći.

Trenutno dva najkorišćenija kriptografska algoritma su MD5 i SHA.

Message – Digest algorithm 5 (MD5): Najčešće korišćen kriptografski algoritam, koji je u upotrebi još od 1991. godine. Iako su nađeni brojni propusti MD5 se još uvek koristi, jer ni drugi nisu besprekorni.

Secure Hash Algorithm (SHA): Algoritam razvijen od Američke agencije za nacionalnu bezbednost (NSA), kao jedna od mogućih zamena za MD5. Iako je sigurniji od MD5 i na njemu su otkriveni brojni propusti. Zbog povećane sigurnosti većina forenzičara je prešla upravo na ovaj standard.

Kao primer rada, MD5 algoritma daćemo primer generisane heš vrednosti jednog bloka podataka, tj. jednog string – a. Da bi uočili razliku u jednom smo koristili i mala i velika slova, a u drugom samo mala.

```
MD5 Hash: „Digitalna forenzika“ = b401395554bc1c68bbe9e82eb79e103c  
MD5 Hash: „digitalna forenzika“ = ac27e5915c02d938bae08746b8567991
```

Primetna je ogromna razlika između dva ista stringa u kojima je razlika samo u tome koriste li ili ne velika slova interpunkcije. Čak i kada su promenjena dva bajta (ne bita) rezultat će biti različit, što praktično znači da ako se hash vrednosti dokaznog materijala pre i posle analize poklapaju ne postoji ikakva promena na podacima. Ipak postoje momenti kada se hash vrednosti razlikuju i kada te razloge moramo objasniti.

Dva uobičajna slučaja su:

Medij sa koga su preuzeti podaci je oštećen (u lošem stanju): Problem se najčešće javlja kada forenzički softver pogrešno generiše hash vrednosti sa originalnog medija, jer je on oštećen i nemoguće je pročitati sve njegove delove. U ovom scenariju bitno je dokazati oštećenost originalnog medija.

Oprema za prenos podataka je loša: Slučaj koji se dešava najčešće kada su u pitanju memorijske kartice sa kojih se podaci čitaju uz pomoć eksternih čitača. Iako i su i originalni medij i medij na koji se kopira u redu, kabl ili uređaj za zaštitu od upisivanja nisu u redu. Ovaj slučaj se događa mnogo ređe od prvog, a rešenje treba

naći u zameni (popravci) opreme ili softveru koji će na osnovu uočenih nepravilnosti generisati ispravnu heš vrednost.

Slučajevi nepoklapanja heš vrednosti u praksi su retki, ali forenzičar mora biti spreman i upoznat i sa tim mogućnostima. Osnovna ideja prilikom izrade većine bitstream kopija jeste generisanje checksum izveštaja o izvornom mediju i njegovo poređenje sa podacima kopiranim na odredište.

U praksi se to radi na sledeći način:

1. Softver primenjuje algoritam na originalnom mediju i generiše rezultat.
2. Nakon prenosa podataka softver generiše rezultat za kopirane podatke.
3. Softver vrši upoređivanje dobijenih rezultata da bi se osiguralo da se poklapaju.

Ako je poklapanje uspešno, podaci nisu izmenjeni ni u kom pogledu. Međutim, ako do poklapanja ne dođe forenzičar zna da transver nije uspešan i da je možda došlo do oštećenja eventualnih digitalnih dokaza tokom transvera.

Kao što smo ranije naveli u svetu digitalne forenzike prenosivih medija može doći do problema u slučaju ponovnog uključivanja memorije u pogon, nakon pravljenja „slike“. Heš vrednosti podataka sa memorijskih kartica iz mobilnih telefona, PDA uređaja, fotoaparata gotovo sigurno će se razlikovati, ukoliko samo dođe do paljenja tih uređaja sa karticom unutar njih. Za neke modele PDA uređaja utvrđeno je da se hash vrednost menja u toku jedne sekunde, tj. svaki put kada se uradi osvežavanje slike o memoriji. U nekim slučajevima, koji su svoj epilog dobili na sudu, sud je priznao kao valjane dokaze i onda kada je došlo do razlike, međutim treba itekako voditi računa, jer se vrednost dokaza rapidno smanjuje, on postaje „klimav“, ukoliko postoje nepoklapanja.

6.1.5 Pravljenje forenzičkih duplikata

Ranije smo objasnili da nepostojanje kopije originalnog digitalnog dokaza najčešće dovodi do propadanja istrage. Problem se javlja kada dođe do neke neželjene akcije na kopiji. Kako bi forenzičar opet došao do nje, on mora da kontaminira original, a neki put je to nemoguće, jer je memorija potpuno uništena. Da bi se ovo izbeglo prva forenzička kopija (image) originalnog dokaza u daljem procesu koristi se kao original, a za potrebe istrage koriste se njene kopije. Ovo se čini iz dva razloga. Prvi i osnovni jeste taj da je uvek moguće sračunati heš vrednos i uporediti je, a drugi je postojanje prve kopije u formatu forenzičkog softvera, sa koga će uvek biti rekonstruisana.

7 ALATI ZA AKVIZICIJU USB I CF MEMORIJA

Ključna stvar u digitalnoj forenzici je poznavanje, razumevanje i efikasnost u upotrebi svih forenzičkih alata koji su na raspolaganju. Danas postoje mnogi softveri, ali i hardverska rešenja, koji u svom nazivu ili definiciji imaju reč forenzika (eng. forensic). Međutim, kada je reč o memorijama fleš tipa situacija nije baš zadovoljavajuća. Često je do bitnih podataka lakše doći uz pomoć besplatnih programa koje su razvili kompjuterski entuzijasti ili alatom kome osnova nije računarska forenzika. Čini se da vrtoglav porast popularnosti fleš memorija kompanije koje se bave forenzikom nisu ispratili. Takođe primetno je da brojni „vrhunski“ forenzički alati nisu ispratili ni razvoj operativnih sistema i alata za zaštitu podataka na prenosivim memorijama. Zbog svega toga, u toku razvoja ovog rada, isprobali smo mnoge zaštitne alate i alate sa kojima je moguće zaobići tu zaštitu. Sve alate za Windows okruženje isprobali smo na Windows 7 operativnom sistemu, poštujući pravilo da forenzički alat mora da bude savremen barem onoliko koliko su i standardna okruženja korisnika računara tj. potencijalnih visokotehnoloških kriminalaca.

7.1 Alati za zaštitu podataka na memorijama USB i CF tipa

Omasovljavanje prenosivih memorija neminovno je dovelo do toga da je sve više bitnih podataka na njima. Malo je vremena prošlo, od kada su one služile samo za razmenu programa, filmova i slika, do trenutka, kada se često, cela dokumentacija neke kompanije nalazi na njima. S obzirom na danas sveprisutnu mobilnost ljudi to je dovelo do olakšanja, jer one uvek mogu biti uz vlasnika na bilo kom mestu. Međutim zbog njihove veličine donele su i veliku opasnost da padnu u tuđe ruke. Kompanije koje izrađuju softvere za zaštitu podataka spremno su dočekle tu opasnost i pripremile brojne softvere. Nedugo zatim i sami proizvođači memorija pozabavili su se ovim problemom i doneli niz načina od samog hardvera do softverskih rešenja. Koliko je ova oblast značajna pokazuje i to što je najveći svetski proizvođač softvera, kompanija Microsoft, u svoja dva poslednja operativna sistema (Vista i 7) ugradila alat za zaštitu podataka prenosivih memorija. Problem forenzikara je što i „loši momci“ koriste ove alate.

7.1.1 Hardverska zaštita

Enkripcije zasnovane na hardveru verovatno su najsigurniji način da se zaštite podaci na prenosivim memorijama. Ovi sistemi su posebno dizajnirani od strane proizvođača memorije i veoma je teško probiti ih, jer se ceo sistem zaštite nalazi unutar kontrolera i veza unutar nje same. Posao forenzikara pri pristupu podacima na njima, daleko je teži od pokretanja par softvera koji će probiti šifru. Ako se desi ovaj slučaj, a podaci na memoriji su ključni dokaz najbolje je kontaktirati proizvođača uređaja, jer bilo kakva intervencija, čak i pokušaj pravljenja kopije može aktivirati okidač koji će uništiti sve podatke.

Sve enkripcije podataka (hardverske i softverske) danas se uglavnom zasnivaju na AES algoritmu (Advanced encryption standard). Jedini način da se razbije ovaj tip zaštite jeste da lozinku istovremeno napadne više hiljada kompjutera, svaki posebnom lozinkom ne bi li došli do odogvarajuće. Ovaj metod poznat je kao „brute force“ i jedini je način da se otvore datoteke šifrovane AES algoritmom. Hardverski tip enkripcije podataka manje je osteljiv na ovaj tip napada, jer forenzikar ne može da softverski zaobiđe ovaj algoritam i vidi podatke. Da bi pokušao niz napada, forenzikar

mora da napravi veliki broj kopija, a to je gotovo nemoguće. Kao dodatak većini uređaja sa hardverskom zaštitom, ugrađena je „File Shredder“ funkcija koja će ukloniti sve tragove obrisanih podataka. Na taj način nije ih više moguće rekonstruirati forenzičarskim alatima, već su obrisani zauvek.

7.1.2 Softverska zaštita

Zaštita podataka softverskim putem, je na sreću forenzičara još uvek češći slučaj koji se može sresti u praksi. Glavni razlog ovome je cena. Naime postoje i besplatni softveri za zaštitu podataka, ili oni koji dolaze uz operativne sisteme. Razbiti takve algoritme i doći do podataka, lakše je nego kada su podaci zaštićeni hardverski (na nekim memorijama i otiskom prsta vlasnika). Forenzičar u svakom slučaju mora dobro da poznaje makar najpoznatije softvere za zaštitu, jer se na različitim operativnim sistemima može desiti da se uređaji odazivaju.

DriveCrypt

DriveCrypt je po izboru većine korisnika i informatičkih stručnjaka najobuhvatniji, najsigurniji i pritom za korišćenje lak alat za zaštitu celokupnih diskova. Prednosti koje poseduje u odnosu na ostale alate su:

- Javno dostupni algoritmi
- Radi na svim vrstama operativnih sistema
- Celokupan program (dva fajla) zauzima 1mb
- Cena koštanja
- Minimalni gubici u slučaju oštećenja

Zbog jakih algoritama za enkripciju koje koristi, flash memorije kriptovane DriveCrypt alatom, predstavljaju veliki problem za forenzičare. Iako postoji mogućnost da se brutalnim napadom dođe do podataka, taj posao se i pored mogućnosti današnjih računara ipak čini nemogućim. Poznat je slučaj kada je FBI, u nemogućnosti razbijanja PGP šifre, šefu mafije S. Scrafu iz Filadelfije, provalio u računar i instalirao keylogger alat, jer je jedino tako moglo da se dođe do podataka. Taj slučaj se dogodio još 2000te godine, a FBI je od tada više razvijao u špijunske softvere, nego u alate za razbijanje šifara.

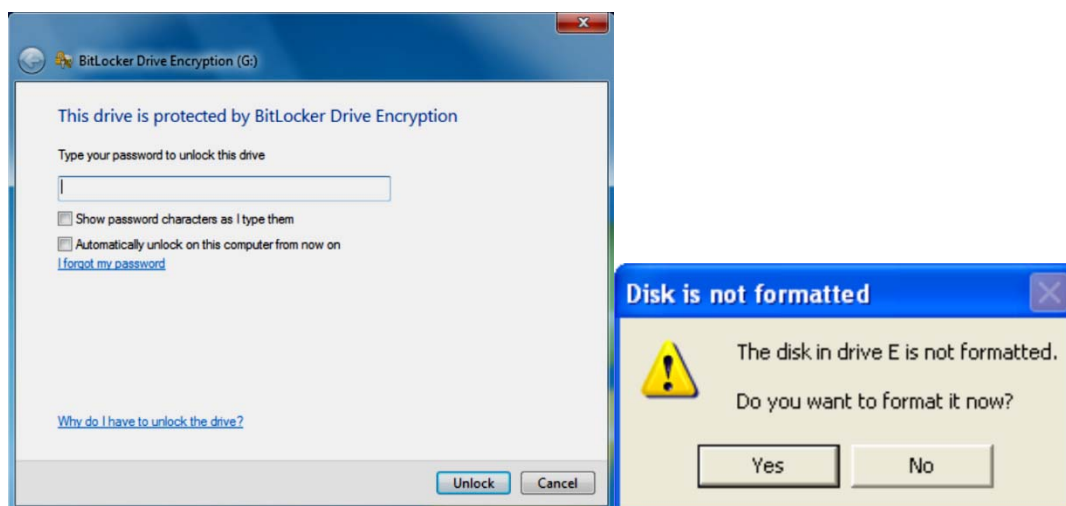
BitLocker

BitLocker je jedna od najnovijih tehnologija zaštitu memorija (ne samo prenosivih), ali je njena raširenost ubrzo pretekla sve prethodnike. Naravno taj podatak nije nimalo čudan, jer iza nje stoji kompanija Microsoft, koja ovaj vid zaštite isporučuje besplatno uz operativne sisteme Vista i Windows 7 (Enterprise i Ultimate edicije), kao i uz serverski operativni sistem verzije 2008. Radi se o 128 bitnoj AES enkripciji u kombinaciji sa još nekoliko tehnologija koje dopunjuju nedostatke AES enkripcije, koja se primenjuje na celom disku, formatirnom u NTFS fajl sistemu particionisanja. BitLocker (slika 29) je zamišljen i kao zaštita samog računara, pružajući mogućnost da se od USB prenosive memorije napravi „ključ“ za ulaz u sistem, ali i kao zaštita samih podataka na memoriji.



Slika 29: Enkripcija flash diska u Windows 7 OS uz pomoć BitLocker tehnologije

Veliki problem pri primeni ove tehnologije na zaštitu podataka na memorijama jeste nekopitabilnost sa ostalim verzijama Windows operativnog sistema. Takođe BitLocker u Vista OS i Win 7 OS imaju sličnosti jedino u imenu, mada će Windows 7 prepoznati uređaj zaključan u Visti. U forenzičkoj struci zabeležena je greška forenzičara (slučaj u republici Hrvatskoj), koji su za prenosivu memoriju pomislili da je oštećena, jer su svi operativni sistemi i forenzički alati kojima su raspolagali pokazivali da podaci ne postoje (slika 30).



Slika 30: Enkriptovan fleš disk u Windows 7 (levo) i Windows XP (desno)

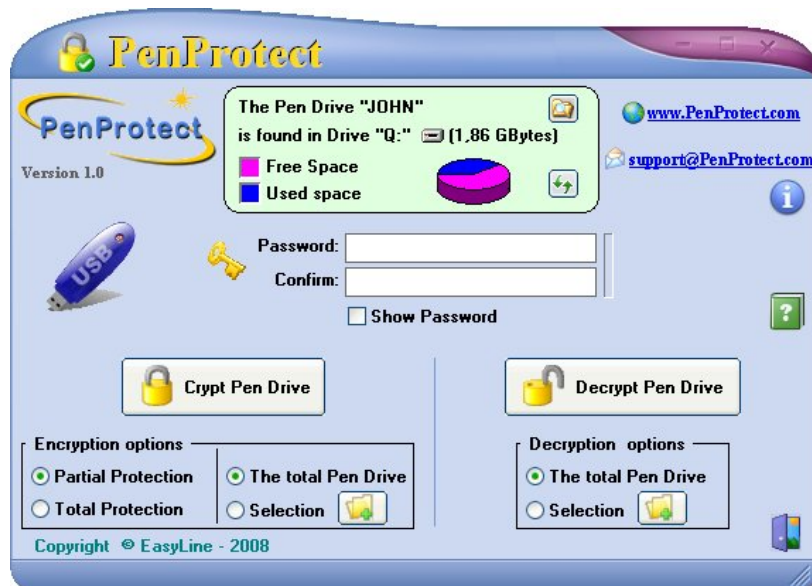
Nažalost greška nije mogla da se ispravi i zbog nepoštovanja procedure, jer alati za pravljenje forenzičkih duplikata, čak i oni stariji, bez greške kopiraju podatke i sa ovih zaštićenih uređaja.

BitLocker je ipak enkripcija koju je moguće probiti¹⁵ i doći do podataka, ali forenzičar mora biti jako oprezan sa ovim memorijama.

¹⁵ Kompanija Passware, Inc objavila je sredinom decembra meseca 2009. godine da je prvi put uspešno probila Windows 7 BitLocker zaštitu. Krajem marta 2010. realaizovan je i algoritam koji taj posao radi.

Ostali vidovi softverskih zaštita

Danas je u upotrebi veliki broj softvera za zaštitu podataka (slika 31). Slobodna enciklopedija Wikipedia je prepoznala čak 82 softvera koji rade sa prenosivim memorijama. Širok spekter ovih alata, ne znači da su oni toliko u upotrebi. Na sreću forenzičara samo mali broj korisnika ih koristi, jer se za ozbiljniju zaštitu i ne mogu koristiti. Većina njih je kompatibilna sa svim operativnim sistemima, samim tim i primamnjiva za korišćenje, a ugalvnom rade na principu sakrivenih direktorijuma.



Slika 31: Osnovni prozor programa PenProtect

Najčešći slučaj u praksi je postojanje izvršne datoteke (verovatno na root direktorijumu memorije), koja se pokreće pri povezivanju memorije za računar i prepoznavanja od strane operativnog sistema. Nakon ukucavanja šifre korisnik može da koristi datoteke. Ova zaštita se lako zaobilazi, jer se uporedo sa razvojem enkripcije razvijaju i alati za dekripciju. Za forenzičara nije teško da otkrije koji je tip enkripcije u pitanju, jer sama izvršna datoteka nosi informacije o softveru i njegovom proizvođaču.

Treba napomenuti da se softverski vid zaštite primenjuje na USB flash memorijama. Memorije CF tipa, kao i ostale memorijske kartice nemaju toliko mogućnosti, što najviše zavisi od aparata u kome se one koriste. Moguće ih je zaključati, naravno, ali proizvođači uređaja u kojima se koriste nude načine da se šifre zaobiđu. Ipak problem je otkriti i u kom uređaju je ona zaključana (ako uređaj nije prisutan), ali se spisak može smajiti utvrđivanjem vrste particije na njoj.

Brute force napadi

Brute force napadi se takođe nazivaju i iscrpnim pretraživanjem, jer se temelje na apsolutnom i ravnopravnom pretraživanju i isprobavanju svih mogućih kombinacija. Takvi napadi očito ne mogu biti efikasni, tj. moraju zahtevati ili velike resurse za isprobavanje velikog broja različitih kombinacija ili veliku količinu vremena dovoljnu da se sa manjim resursima sprovedu isprobavanja svih kombinacija. U stvarnoj

primeni to znači da je cena resursa potrebnih za rešavanje nekog problema ovom metodom često veća nego što vredi samo rešenje.

Brute force napad ne treba zameniti s drugim sličnim vrstama napada koje raznim metodama reduciraju broj mogućih rešenja za isprobavanje. Brute force metodom isprobavaju se sva moguća rešenja bez obzira na nelogičnost nekih od njih. Na primer ako se uzme klasični problem „8 kraljica“ u kojem je potrebno postaviti 8 kraljica na šahovsku ploču, ali na takav način da nijedna od njih ne napada drugu, brute force tehnika će za rešenje problema isprobati svih $64! / 56! = 178,462,987,637,760$ mogućih rešenja. Nekom drugom metodom kao što je npr. backtracking broj ispitanih kandidata pre pronalaska rešenja bio bi znatno manji. Naime, backtracking je derivacija brute force tehnike koja se može primieniti u situacijama kada su ispitivani scenariji donekle povezani.

„Rupe“ u sistemima za zaštitu podataka na prenosivim memorijama

Kao što smo, ranije, više puta naglasili poznavanje aktuelnih metoda zaštite i modela prenosivih memorija najveći je alat u forenzičkoj istazi. Naravno to se ne odnosi samo na podatke proizvođača memorija i kompanija koje se bave digitalnom forenzikom, već i na konstantno praćenje i „druge strane“ tj. hakera koji pronalaze greške i metode zaobilaženja zaštita.

Januara 2010, na hakerskim sajtovima pojavila se vest da je uspešno probijena hardverska zaštita USB fleš diskova. Svakako najporaznija činjenica za proizvođače (SanDisk, Kingston, Verbatim), bilo je to da se radilo o uređajima koji su dobili FIPS 140-2 nivo sigurnosti¹⁶ i validaciju od organizacije NIST koja radi pri Vladi SAD.

Takođe i softverska zaštita, koju kao neprobojnu reklamiraju većina najpoznatijih svetskih proizvođača, davno je probijena, uz pomoć greške u arhitekturi samog sistema zaštite. Naime ovi proizvodi koriste softver koji se izvršava na host računaru, da bi se proverila ispravnost lozinke korisnika, a zatim šalju signal do uređaja da se otključa. Ovaj način rada nije siguran, a stručnjak kompanije SySS¹⁷ GmbH uspeo je da napravi jednostavan softverski alat za otključavanje većine uređaja sa ovim vidom zaštite.

7.2 Uobičajni alati za forenzičku akviziciju

Softvere za forenzičku akviziciju moguće je podeliti u više kategorija. Mi smo ih podelili na osnovu vrste poslova koje obavljaju tokom akvizicije. Naravno tu su multifunkcionalni alati i kao i posebne distribucije softvera koje sa sobom nose više alata. Opisane alate testirali smo na istom računaru, koristeći nekoliko memorija.

¹⁶ Federal Information Processing Standard – najviši standard bezbednosti, koji moraju da zadovolje uređaji da bi bili korišćeni u agencijama Vlade Sjedinjenih Američkih država

¹⁷

http://www.syss.de/fileadmin/ressources/040_veroeffentlichungen/dokumente/SySS_knackt_SanDisk_USB-Stick.pdf

http://www.syss.de/fileadmin/ressources/040_veroeffentlichungen/dokumente/SySS_knackt_Kingston_USB-Stick.pdf

Osnovno pravilo u digitalnoj forenzici je da forenzički računar mora biti „čist“. Međutim stalno čišćenje sistema, i brzina rada nisu srazmerne, pa se zato razvijeni brojni načini da se taj problem reši. Najpoznatije i najprimenljivije rešenje među forenzičarima jesu „žive“ live distribucije operativnih sistema. To su operativni sistemi koji sve što im je potrebno za rad smeštaju u radnu memoriju računara (RAM) tako da nikako ne utiču na podatke na čvrstim memorijama. Kroz godine razvile su se i brojne distribucije koje su isključivo namenjene forenzičarima tj. dolaze sa brojnim forenzičarskim alatima. Najpoznatije distribucije su svakako: Helix, Caine, Deft, FBIFC... Sve one zasnivaju se na Linux operativnom sistemu, ali su se razvila i okruženja koja rade pod Windows OS, kao što je Windows FD.

Broj korisnika Microsoft operativnih sistema i sve veći broj forenzičarskih alata koji rade pod njima, doveo je do razvoja još nekih načina za vršenje akvizicije. Uz pomoć bespaltnih programa, moguće je pripremiti Windows instalaciju, koja će uključivati i sav softver koji je potreban za rad. Tako je za svega pola sata spreman računar kome je HDD formatiran, ima sveže instaliranu verziju Windows OS – a i sve forenzičaru potrebne alate.

Napredak računarske tehnologije, moćne konfiguracije, olakšavaju posao forenzičara i uz pomoć virtuelizacije. Forenzičaru se nudi da na jednom kompjuteru ima više instaliranih operativnih sistema tj. više virtualnih računara, koji se ponašaju kao zasebni i po pogledu softvera, ali što je još bitnije i hardvera.

7.2.1 EnCase

EnCase je programski alat namanjen forenzičkoj istrazi digitalnih dokaza firme Guidance Software. Svojom pojavom EnCase platforma je promenila način sprovođenja istrage sigurnosnih incidenta na računarskim sistemima i postala *de facto* standard. Na osnovu ovog softvera, kompanija Guidance Software se svrstala među tri vodeće svetske IT kompanije. EnCase se danas koristi kao najnapredniji sigurnosni alat, a kao standard su ga prihvatile većina vodećih kompanija i organizacija poput Rolls-Roycea i NATO-a. Takođe alat se široko koristi pri primeni zakona u komercijalnim preduzećima za analizu i akviziciju podataka. Smatra se jednim od najboljih, a svakako je najčešće korišćen.

EnCase program (postoje i hardverski EnCase alati) omogućava i olakšava sudskim veštacima i IT stručnjacima istraživanje slučajeva, akviziciju i analizu dokaznog materijala. Posедуje kvalitetan grafički interfejs, koji omogućava bolji i lakši pregled različitih fajlova kao što su obrisani fajlovi, fajl “slack” i “unallocated data”. Ono što je svakako najvažnije za IT veštace jeste da ne omogućava izmenu podataka preuzetih sa korumpiranog računara.

EnCase se danas isporučuje u više varijacija, a aktuelna verzija osnovnog alata je 6. Starije verzije se mogu naći na internetu, ali do najnovije je veoma teško doći, jer je čak i kupovina dozvoljena samo obrazovnim i vladinim institucijama. Takva politika je i razumljiva, jer se u ranijem periodu ovaj moćni alat često koristio i u kriminalne svrhe. Ipak, pri izradi rada imali smo mogućnost da isprobamo i najnoviju verziju alata, koja se nije previše brzinom i kvalitetom akvizicije prenosivih medija, izdvojila u odnosu na druge komercijalne i nekomercijalne alate. Zanimljivo je da se za autentifikaciju svih novijih EnCase verzija koristi USB dangle drive, koji bukvalno predstavlja ključ kojim se otključava softver. Njega nije moguće duplirati uz pomoć EnCase alata, ali ostali softveri taj posao rade bez ikakvih većih problema. Što se tiče

modernih sistema zaštite prenosivih medija, EnCase uspešno zaobilazi BitLocker zaštitu postavljenu u Vista operativnom sistemu kao i starije PGP zaštite.

7.2.2 *FTK*

Forensic Toolkit je jedan od najstarijih forenzičkih softvera. Zahvaljujući grafičkom interfejsu i radu na Windows operativnom sistemu postao je veoma popularan među forenzičarima. Njegov integralni deo, FTK Imager je možda i najpoznatiji softverski alat za „bit po bit“ kopiranje, koji svoju popularnost, osim nesumnjive funkcionalnosti duguje tome što se zasebno besplatno može preuzeti sa interneta¹⁸.

Slike diskova napravljene FTK Imager programom (ne FTK Imager Lite) priznate su na sudu kao valjani dokaz. Osim toga FTK obejedinjuje sve ostale postojeć formate za pravljenje forenzičkih kopija. Naime, on će sa lakoćom otvoriti i slike napravljene EnCase – om, SMART – om i sl. pa čak i .vmdk fajlove koji predstavljaju sliku radne memorije virtualne mašine.

7.2.3 *DriveSpy*

DriveSpy je forenzički alat za DOS operativni sistem, koji je razvila kompanija Digital Intelligence. Iako nema razvijen grafički interfejs, alat je dosta popularan među forenzičarima, jer sadrži samo 11kb i mlako se uklapa na bilo koju disketu, a kamoli medij većeg kapaciteta. Inače, radi se o alatu koji proširuje osnovne MS-DOS funkcije, a sadrži sve potrebno za kopiranje i ispitivanje sadržaja diska. Dodatne funkcije su i kreiranje MD5 heša za kopirani disk, particiju, ili izabrane datoteke sigurno brisanje diska, praznog prostora, particije.

Alat do skora nije imao podršku za prenosive memorije (aktuelna verzija 3.0 poseduje), tj. DOS OS ih nije prepoznavao. Ipak poslednja verzija sadrži dodatak koji pokreće upravljačke programe i omogućava pristup i rad sa USB fleš diskovima, dok po rečima autora softvera, pristup ostalim memorijskim karticama zavisi od proizvođača, čitača, tipa i sl.

7.2.4 *Helix*

Helix je možda najpoznatija forenzičarska distribucija. Svoju popularnost, između ostalog, Helix je duguje i tome što je do poslednje verzije (objavljene u martu 2009.) bio potpuno besplatan. Njegova najnovija verzija, koja se za razliku od prethodnih, koje su se zasnivale na Knoppix distribuciji, zasniva se na Ubuntu Linuxu u najpovoljnijem obliku košta 239 dolara godišnje (isključivo za akademske institucije).

Helix spada u grupu softvera namenjenih radu direktno sa CD-ROM medija. Bez obzira o kojoj se osnovnoj verziji Linux OS radi, Helix je modifikovan na način da nikad ne koristi swap particiju i da prepoznaje skoro sve moguće fajl sisteme. Važna funkcionalnost Helix distribucije je i mogućnost pokretanja u obliku samostalne aplikacije na Windows operativnim sistemima. Pri tome su raspoloživi različiti alati namenjeni u forenzičke svrhe. Tom funkcionalnošću Helix je razdeljen u program koji analizira podignute Windows sisteme i Linux operativni sistem koji se samostalno podiže.

¹⁸ www.accessdata.com/downloads.html

Linux bootable alati Helix distribucije

Alat	Opis
<i>The Sleuth Kit</i>	Kolekcija Unix alata koji se pokreću sa komandne linije i služe za pretragu čvrstih (i prenosivih) memorija
<i>dc3dd</i>	Specijalna verzija standardnog alata za pravljenje duplikata diskova, koja omogućuje hešovanje podataka, brojnim algoritmima, u letu.
<i>dcfldd</i>	Verzija standardnog Unix alata za pravljenje duplikata diskova, specijalno razvijena od starne ministarstva odbrane SAD
<i>LinEn</i>	Linux verzija EnCase alata, koja praktično simulira standardnu DOS verziju
<i>aimage</i>	Advanced Imager – grafičko okruženje za pravljenje duplikata diskova sa brojnim mogućnostima za hešovanje podataka

Windows alati

Alat	Opis
FTK Imager	Deo profesionalnog FTK (Forensic Toolkit) alata, specijalizovan za pravljenje duplikata u Windows okruženju.
Mdd	Memory dd – alat za pravljenje duplikata zatečenog stanja radne memorije
Win32dd	Pravljenje forenzičkih kopija pod Windows OS
winen	Starija verzija EnCase alata, bez posebnih funkcionalnosti, osim pregledanja HEX vrednosti
WFT	Alat za živu forenziku Window sistema, poseduje funkcionalnosti prikupljanja i pretraživanja podataka i automatskog izveštavanja

7.2.5 Caine

Caine distribucija, javila se kao besplatna alternativa, nakon što je Helix distribucija postala komercijalna. Nastala iz želje italijanskih forenzičara da najednom mestu sakupe većinu dostupnih besplatnih softvera za digitalnu forenziku, CAINE je ubrzo postao glavni alat velikog broja forenzičara. Kao i Helix poseduje veliki broj alata na live Linux distribuciji i alate namenjene za Windows operative sisteme. Posebna prednost CAIN – a je što se, sa zvaničnog sajta grupe, koja ga razvija, može preuzeti instalaciona verzija namenjena podizanju sa USB uređaja. Zbog velikog broja alata nećemo ih posebno navoditi.

7.2.6 *Deft*

Deft forenzička distribucija takođe je delo italijanskih stručnjaka i može se besplatno preuzeti sa interneta. Pored live distribucije Linux operativnog sistema, poseduje i Windows alate, a u odnosu na druge alate posebno ga izdvaja to što ima mnogo veću bazu upravljačkih programa za sve vidove hardvera, što itekako olakšava rad. Aktuelna verzija 5.x dolazi sa velikim brojem Windows i Linux alata, što besplatnih, što par starijih i probnih verzija komercijalnih alata, koji mogu predstavljati kompletnu paletu potrebnih za jednog forenzičara.

7.2.7 *dd*

dd je standardan Unix/Linux alat, koji je u većini slučajeva, za početnike, sinonim za pravljenje kopije diskova. Iako razvijen da "konvertujete ili kopira fajlove"¹⁹, ovaj program (komanda) se najčešće koristi za pravljenje slike diskova ili particija. Danas postoje brojne varijacije ove alatke (*dd for Windows* npr.), sa mogućnošću pokretanja na raznim operativnim sistemima, kao i i par njih koje poseduju mogućnost hešovanja podataka. Kopije podataka napravljene ovim alatom na sudu ipak mogu biti valjane, ako i samo ako postoji neki dodatni alat za verifikaciju dokaza.

7.2.8 *VMware*

VMware je popularan proizvod za virtuelizaciju (VMware Vorkstation 7.x je aktuelna verzija) koji omogućava kreiranje pseudo računara i pseudo mreža, koji za sve koriste hardver jednog sistema. Ova mogućnost ima mnoge prednosti. Na primer, može se podesiti gost operativni sistem, instalirati potrebni forenzički alati, od njega napraviti slika sistema, raditi na njemu, a po potrebi uvek dovesti u prekonfigurisano stanje. Sa njega je moguće, izvršiti sve vrste ispitivanja, uključujući instaliranje i praćenje zlonamernih programa, ponavljanje sigurnosnog incidenta itd.

„U toku rada na WMware računarau (stanici) postoji mogućnost da se rad „zamrzne“. Tako suspendovanom sistemu, sadržaj fizičke memorije se nalazi u datoteci sa ekstenzijom *.vmem.. Format ove datoteke veoma je sličan dd image fajlovima, koji se dobijaju forenzičkom akvizicijom, uz pomoć ranije opisanih alata, tako da se može dalje tumačiti i analizirati.“²⁰

Kada su u pitanju prenosive memorije, VMware nudi opciju da uređaj uopšte nema kontakt sa računarom domaćinom. Praktično, ukoliko korisnik to želi, VMware će, ako je instaliran na operativnom sistemu kompanije Microsoft, blokirati svaku vezu između uređaja i tog operativnog sistema. Ipak, iako proizvođači tvrde da nema ikakvih šansi da dođe do kontakta, treba primeniti Write Protect (vidi 6.1.3) zaštitu na operativnom sistemu sa kojeg se podiže VMware stanica.

7.2.9 *Ostali alati*

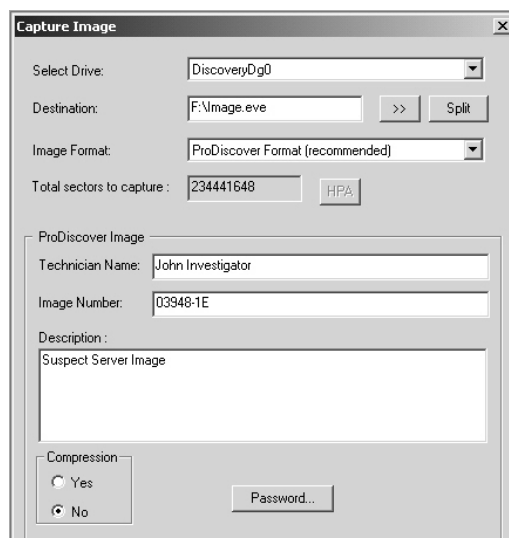
U današnjem, razvijenom, tržištu veliki je broj kompanija koji pokušavaju uspešno, ili bezuspešno da se nađu među onima koje proizvode forenzičke softverske alate. Posebno, veliki je broj onih alata koji se bave samo pravljenjem forenzičkih kopija, jer to i nije veliki programerski zadatak, a kôd brojnih, već opisanih alata, može se

¹⁹ <http://linukrevievs.org/man/dd/>

²⁰ VMware as a forensic tool - www.forensicfocus.com/vmware-forensic-tool

naći na internetu. Najčešće jedina prednost ovih alata je lepši, intuitivniji grafički interfejs koji i početnicima omogućava rad. Među ovim najpoznatiji alati, koji rade i sa prenosivim memorijama su:

- Forensic Replicator, razvijen od strane kompanije Paraben Forensic Tools, može se kupiti zasebno, a sastavni je deo forenzičkog softvera koji razvija ova kompanija
- Norton Ghost, koji razvija kompanija Symantec, nije pravljen kao forenzički alat, ali se kopije uzete ovim programom smatraju prihvatljivim na sudu²¹
- SafeBack – DOS alat sa mogućnošću SHA256 hešovanja podataka. Razvila ga je kompanija New Technologies Inc.
- SMART, Linux alat koji je razvila kompanija ASR Data Acquisition & Analysis. Posедуje inzvaredan grafički interfejs, slikovito prikazuje diskove, njihovu popunjenost i tok kopiranja podataka. Poseduje dva moda rada, brži, bez hešovanja podataka, koji je dobar za pravljenje forenzičkih kopija i sporiji uz hešovanje svih kopiranih podataka.
- WinHex, alat kompanije X-Ways Software Technology AG, služi za akviziciju i analizu dokaza, jer osim mogućnosti za kopiranje i verifikaciju dokaza, poseduje i HEX editor koji omogućava analizu podataka.
- ProDiscover (slika 32), alat koji ima možda najprostiji grafički interfejs od svih pomenutih. Razvija ga kompanija Technology Pathways, a prepoznatljiv je po tome što poseduje sve najmodernije sisteme za verifikaciju podataka.



Slika 32: Interfejs programa ProDiscover

²¹ Podatak važi za SAD

7.2.10 Nenamenski alati u forenzičkoj primeni

Broj softvera koji se može legalno ili putem takozvanih warez / torrent sajtova preuzeti svakodnevno raste. Programeri se zarade ili slave radi trude da on-line objave alate sa novim funkcijama, koji donose izvesnu prednost u odnosu na one koji taj softver ne koriste. Digitalna forenzika je specifična oblast, koja pre svega zahteva odlično poznavanje računarske tehnologije i praćenje svega što se novo objavi, posebno na „hakerskoj sceni“. Mnogi propusti, zapravo većina njih, uočeni su tek nakon napada hakera, a mnogi hakeri poput Rusa Kasperskog, postali su najcenjenije ličnosti u oblasti zaštite. U poslu, forenzičari digitalnih medija moraju se ponekad poslužiti alatima koji ne samo da nisu forenzičarski, već pripadaju grupi hakerskih alata, jer je to često jedini način da se uđe u trag ili dokaže kompjuterski kriminal. Među velikim brojem nenamenskog softvera, koji može poslužiti u forenzičke svrhe izdvojili smo proizvode dve kompanije čiji alati uveliko čekaju u redu da postanu zvanični forenzički alati, jer se uveliko i više od onih verifikovanih koriste u praksi. Problem verifikacije je i vreme potrebno da se provere svi segmenti programa, otkrije količina greške i njen uticaj na dokaze.

ElcomSoft

Elcomsoft je pionir među privatnim kompanijama koje su se bavile računarskom tehnologijom u Rusiji. Osnovana je 1990 godine u Moskvi u cilju proizvodnje komercijalnog softvera. Međutim nakon upada hakera u program koji je proizvela kompanija počinje da se bavi IT bezbednošću, ali na poseban način, koji danas naziva etičko hakovanje (*ethical hack*). Danas se njeni alati koriste u mnogim vojnim i obaveštajnim agencijama u širokom spektru kompjuterskog kriminala.

Najpoznatiji alati ove kompanije izrađeni su, prema njenim rečima da pomognu korisnicima da saznaju zaboravljenu lozinku za pristup sistemu, dokumentu, arhivi ili da npr. „provere sigurnost svoje bežične mreže“. Naravno ti softveri uveliko koriste hakerima da se dokopaju poverljivih podataka, ali i forenzičarima u praktično istu svrhu, samo za druge potrebe.

Praktično ne postoji aplikacija čije lozinke ne otkrivaju alati ElcomSoft-a, tako da su nezamenjivi u forenzičkoj analizi. Prilikom akvizicije prenosivih memorija, najkorisniji su alati za razbijanja PGP šifara i zaključanih NTFS particija, koji čak imaju i opciju deljenja tog posla sa drugim računarima putem mreže.

Passwordare

Kompaniju Passwordare osnovali su 1998. godine bivši radnici savezne američke agencije za borbu protiv kompjuterskog kriminala. Od samog početka izrađuju softver za razbijanje lozinke kako za privatne potrošače tako i za kompanije. Jedan od najvećih uspeha ove firme je to što ju je kompanija Adobe unajmila kao zvaničnog partnera za proveru sigurnosti njihovih programa, a par puta je to činio i za sam Microsoft.

Iako njihovi softveri rade sa dosta uspeha nikada nisu bili prihvaćeni kao forenzički, već su čak nekoliko puta i odgovarali na sudu zbog omogućavanja pojedincima da uz njihove alate naruše bezbednost drugih korisnika. U kompaniji te probleme pravdaju ljubomorom bivših kolega, ali ma koliko su se trudili da u nazive svojih proizvoda stave reč forenzika, tek njihov poslednji proizvod Passwordare Kit Forensic 10, ima

prave odlike forenzičkog softvera, pa je samim tim i uvršćen u zvanični program obuke forenzičara (Certified Computer Examiner). Zanimljivost je da su se pretodne verzije svodile na probijanje šifara različitih datoteka i windows logon šifara (prvi u svetu), a da je preseljenjem razvojnog odeljenja u Moskvu i zapošljavanjem ruskih stručnjaka, alat dobio mogućnosti izrade forenzičke kopije, otkrivanja šifara zaključanih memorija i sl.

NirSoft

U pominjanju alata koji mogu doprineti forenzici, a to im nije standardna namena, mora se pomenuti i programer Nir Sofer. Niko sa sigurnošću ne može da tvrdi da li je to njegovo pravo ime, ili samo pseudonim kojim se predstavlja na svom sajtu www.nirsoft.net

Sajt je prava zbirka raznoraznih alata, koji su namenjeni otkrivanju sačuvanih loziznki. Programi nisu ni na koji način hakerski, već samo imaju automatizovane procese upakovane u grafički interfejs putem kojih dolaze do informacija koje već postoje sačuvane u Windows operativnim sistemima.

8 STUDIJE SLUČAJA

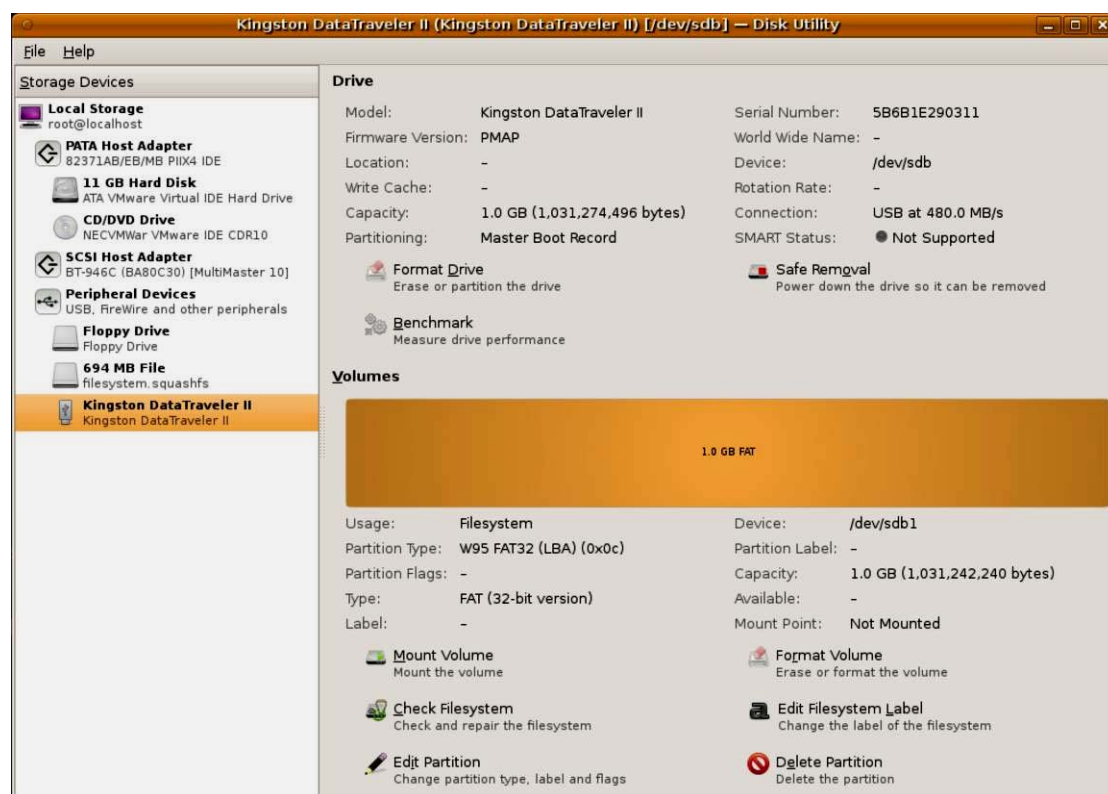
8.1 Akvizicija podataka sa fleš diska

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

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

8.1.1 Utvrđivanje tipa memorije

Prvi zadatak pri akviziciji bio je utvrđivanje stvarne veličine memorije i priprema sterilnih medija. Vizuelnim posmatranjem utvrđeno je da je u pitanju USB memorija fleš tipa, proizvođača Kingston, veličine 1GB. Do tog podatka došli smo ne samo omatranjem memorije u oklopu, već smo oklop uklonili, a zatim podatke pročitati sa čipa. Te podatke još jednom smo proverili i softverski uz pomoć alata DiskUtility (slika 33).



Slika 33: Informacije o disku – predmetu istrage

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

8.1.2 Priprema starilinih medija

Najidealnija situacija bila bi kada bi bili u mogućnosti da imamo još dve potpuno iste memorije, ali to je retko moguće. Kako je nemoguće nabaviti istovetni fleš disk, za

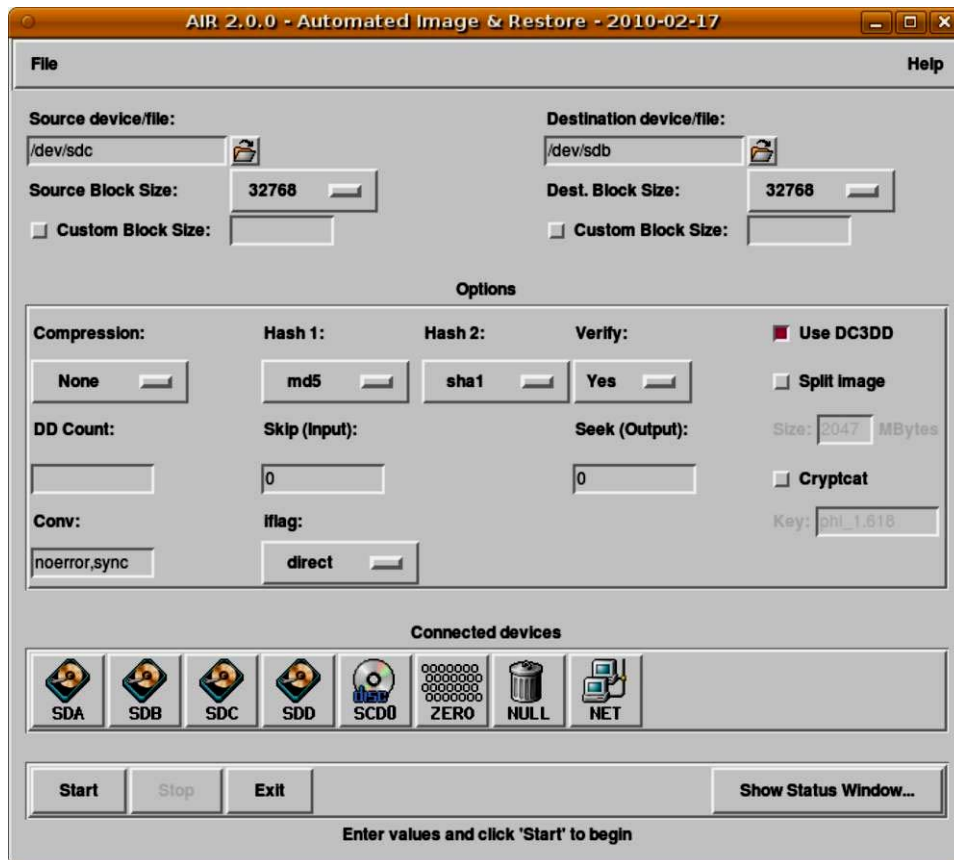
kopije smo odabrali dve memorije istog kapaciteta kao što je i memorija koju ispitujemo. Pre procesa kopiranja bit po bit, iako većina alata tokom tog procesa narušava prethodno stanje, memorije je potrebno formatirati. Sam fajl sistem nije toliko bitan, koliko je bitno uništiti postojeće podatke na memoriji, ali smo se mi odlučili da ne dodelimo ni jedan (slika 34).



Slika 34: Priprema sterilnog medija

8.1.3 Forenzičko kopiranje

Nakon što su sve pripreme izvršene prelazi se na pravljenje forenzičkih kopija. Za taj deo akvizicije odabrali smo AIR (Automated Image and Restore). Program poseduje sve potrebne mehanizme za forenzičko kopiranje kao što je pravljenje MD5 iSHaX heševa i detaljno izveštavanje (slika 35).



Slika 35: Air - Automated Image and Restore interfejs

Dobijene vrednosti heš-a moraju se zapisati, ne bi li proverili da li je sve u redu nakon formiranja radne kopije. Ako se heš vrednosti dobijene sa radne kopije i originala poklapaju, proces akvizicije je završen i možemo pristupiti analizi.

Osim na fizičke medije, programi za forenzičko kopiranje nude i pravljenje slike u vidu fajla, najčešće ekstenzije .dd. Ovu ekstenziju lako je otvoriti u programima za forenzičku analizu, a npr. uz alat WinImage moguće ga je konvertovati u .iso format.

8.2 Pristup podacima na zaključanim memorijama

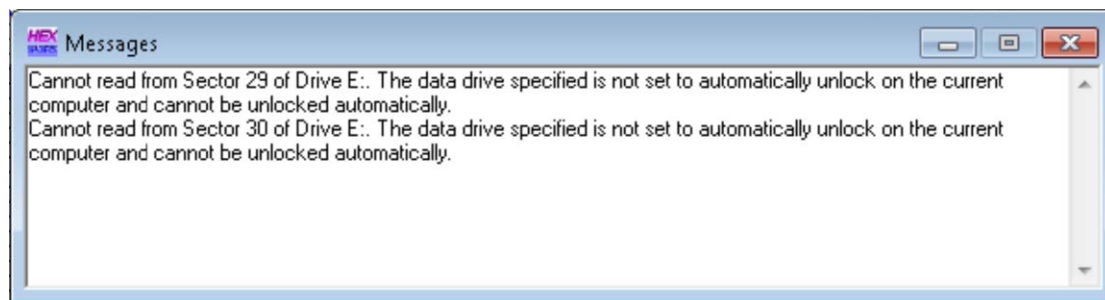
U želji da onemoguće pristup podacima na prenosivim memorijama kriminalci ih često zaključavaju. Dokazi nisu prisutni samo na fleš diskovima onih koji se bave kompjuterskim kriminalom već uopšte. U literaturi o forenzici prenosivih memorija, neizbežan je primer iz 2001. godine kada su istražitelji FBI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

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

8.2.1 Otkrivanje zaštite

Svakako najbitnije nakon forenzičkog kopiranja jeste otkrivanje da zaštita postoji. Neretko dolazi do greške i neiskusni forenzičari zaključanu memoriju, posebno kada se radi o enkripcijama na celom disku, kakva je BitLocker, smatraju oštećenom. EnCase alat uspešno detektuje Winows Vista BitLocker zaštitu i poseduje alat za njeno razbijanje, dok onu postavljenu u Windows 7 sistemu vidi kao oštećenu memoriju. Da bi se greške svele na minimum moraju se ispratiti svi principi akvizicije dokaza, a sama zaštita i njeno razbijanje spadaju u domen forenzičke analize.

Bit Locker zaštita lako je primetna u alatima za analizu. Pri eksperimentu, izvršili smo forenzičko kopiranje fizičke memorije u fajl, a zatim ga analizirali, forenzičkim alatom WinHex (slika 36). Najnovija verzija ovog alata pri pokušaju otvaranja logičkog diska jasno pokazuje da je memorija zaključana, a pri fizičkom sve što se na njoj nalazi, odnosno fajlovi koji operativnom sistemu jasno pokazuju kako da njome upravlja i aktivira sistem za otključavanje (slika 37).



Slika 36: Obaveštenje o zaključanoj memoriji

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
(Root directory)		16.0 KB					969
ar-SA_BitLockerToGo.exe.mui	mui	8.5 KB	07/14/2009 01:55:30	07/14/2009 01:55:30	07/14/2009	SHR	1001
autorun.inf	inf	116 B	07/13/2009 21:21:48	06/10/2009 22:43:12	07/13/2009	SHR	1025
bg-BG_BitLockerToGo.exe.mui	mui	8.5 KB	07/14/2009 01:55:28	07/14/2009 01:55:28	07/14/2009	SHR	1033
BitLockerToGo.exe	exe	250 KB	07/14/2009 00:12:58	07/14/2009 02:26:16	07/14/2009	SR	1057
COV 0000.BL	BL	32.0 KB	11/06/2010 02:23:32	11/06/2010 02:23:32	11/06/2010	SHR	2281
cs-CZ_BitLockerToGo.exe.mui	mui	8.0 KB	07/14/2009 01:55:26	07/14/2009 01:55:26	07/14/2009	SHR	1561
da-DK_BitLockerToGo.exe.mui	mui	8.5 KB	07/14/2009 01:55:26	07/14/2009 01:55:26	07/14/2009	SHR	1577
de-DE_BitLockerToGo.exe.mui	mui	9.5 KB	07/14/2009 01:55:36	07/14/2009 01:55:36	07/14/2009	SHR	1601
el-GR_BitLockerToGo.exe.mui	mui	10.0 KB	07/14/2009 01:55:28	07/14/2009 01:55:28	07/14/2009	SHR	1625
en-US_BitLockerToGo.exe.mui	mui	8.0 KB	07/14/2009 01:55:34	07/14/2009 01:55:34	07/14/2009	SHR	1649
es-ES_BitLockerToGo.exe.mui	mui	8.5 KB	07/14/2009 01:55:28	07/14/2009 01:55:30	07/14/2009	SHR	1665
et-EE_BitLockerToGo.exe.mui	mui	8.0 KB	07/14/2009 01:55:26	07/14/2009 01:55:26	07/14/2009	SHR	1689
fi-FI_BitLockerToGo.exe.mui	mui	8.5 KB	07/14/2009 01:55:22	07/14/2009 01:55:24	07/14/2009	SHR	1705
fr-FR_BitLockerToGo.exe.mui	mui	9.0 KB	07/14/2009 01:55:24	07/14/2009 01:55:24	07/14/2009	SHR	1729
FSCK0000.000	000	4.0 MB	11/06/2010 02:23:32	11/06/2010 02:23:32	11/06/2010	SHR	2345
FSCK0000.001	001	460 MB	11/06/2010 02:23:32	11/06/2010 02:23:32	11/06/2010	SHR	10537
FSCK0000.002	002	0 B	11/06/2010 02:23:32	11/06/2010 02:23:32	11/06/2010	SHR	
FSCK0000.003	003	0 B	11/06/2010 02:23:32	11/06/2010 02:23:32	11/06/2010	SHR	
FSCK0000.004	004	0 B	11/06/2010 02:23:32	11/06/2010 02:23:32	11/06/2010	SHR	
FSCK0000.005	005	0 B	11/06/2010 02:23:32	11/06/2010 02:23:32	11/06/2010	SHR	
FSCK0000.006	006	0 B	11/06/2010 02:23:32	11/06/2010 02:23:32	11/06/2010	SHR	

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
000C5200	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00
000C5210	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00
000C5220	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000C5230	00	00	00	00	00	00	00	00	00	00	00	00	B8	00	00	00
000C5240	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68
000C5250	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F
000C5260	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20
000C5270	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00
000C5280	01	75	F5	D9	45	14	9B	8A	45	14	9B	8A	45	14	9B	8A
000C5290	4C	6C	0F	8A	44	14	9B	8A	4C	6C	0A	8A	44	14	9B	8A
000C52A0	52	69	63	68	45	14	9B	8A	00	00	00	00	00	00	00	00
000C52B0	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	01	00
000C52C0	76	BF	5B	4A	00	00	00	00	00	00	00	00	E0	00	02	21
000C52D0	0B	01	09	00	00	00	00	00	00	20	00	00	00	00	00	00
000C52E0	00	00	00	00	00	10	00	00	00	10	00	00	00	00	00	10
000C52F0	00	10	00	00	00	02	00	00	06	00	01	00	06	00	01	00
000C5300	05	00	00	00	00	00	00	00	00	30	00	00	00	02	00	00
000C5310	36	0B	01	00	02	00	40	05	00	00	10	00	00	00	10	00
000C5320	00	00	10	00	00	10	00	00	00	00	00	00	10	00	00	00
000C5330	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000C5340	00	10	00	00	08	1E	00	00	00	00	00	00	00	00	00	00
000C5350	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000C5360	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000C5370	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000C5380	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000C5390	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000C53A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Sector 1577 of 953281 Offset: C5200 = 77 Block: n/a Size: n/a

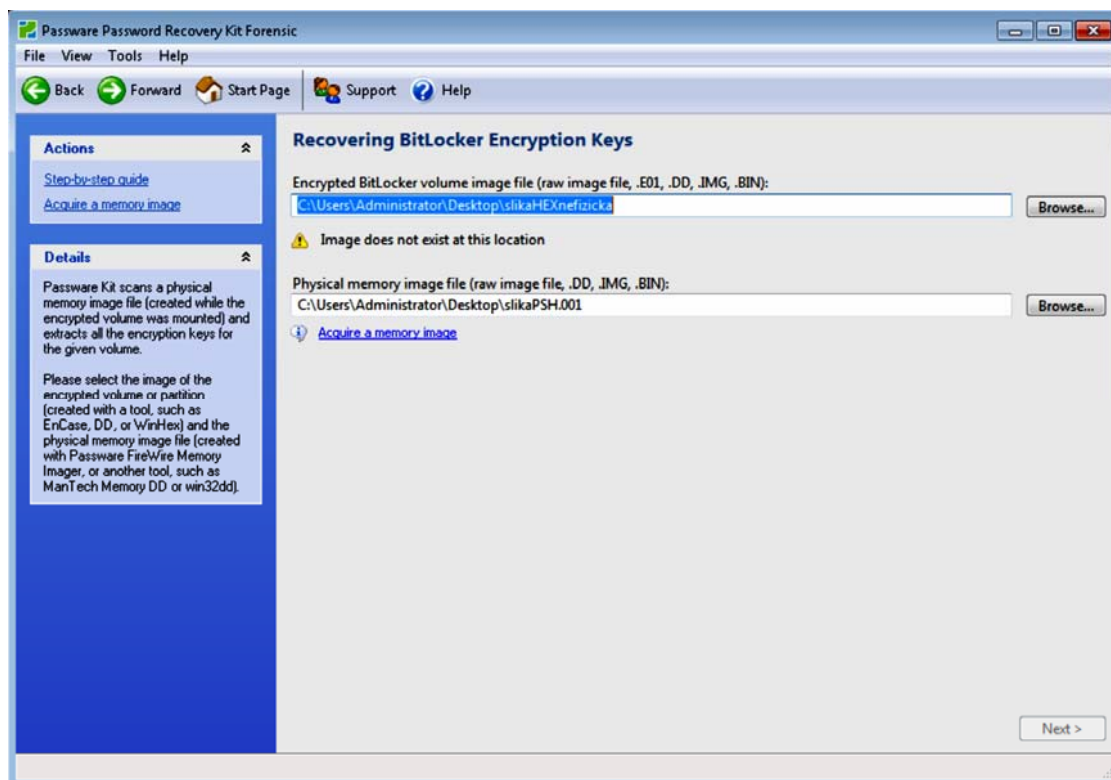
Removable medium 1, Partiti. 0% free
File system: FAT32
[Read-only mode]
Alloc. of visible drive space:
Cluster No.: 78
da-DK_BitLockerToGo.exe.mui
Snapshot taken 73 min. ago
8 Bk (s): 77
Physical sector No.: 1640
Logical sector No.: 1577
Used space: 465 MB
487,579,648 bytes
Free space: 4.0 KB
4,096 bytes
Total capacity: 465 MB
488,079,872 bytes
Bytes per cluster: 4,096
Free clusters: 1
Total clusters: 119,039
Bytes per sector: 512
Usable sectors: 952,312
First data sector: 969

Slika 37: Pregled fajlova zaključane memorije u alatu WinHex

8.2.2 Otključavanje memorije

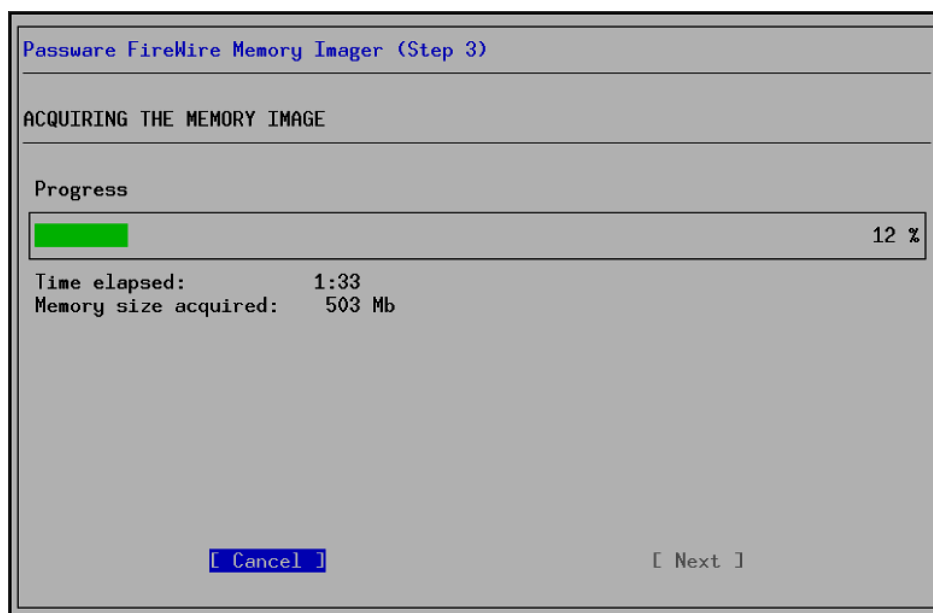
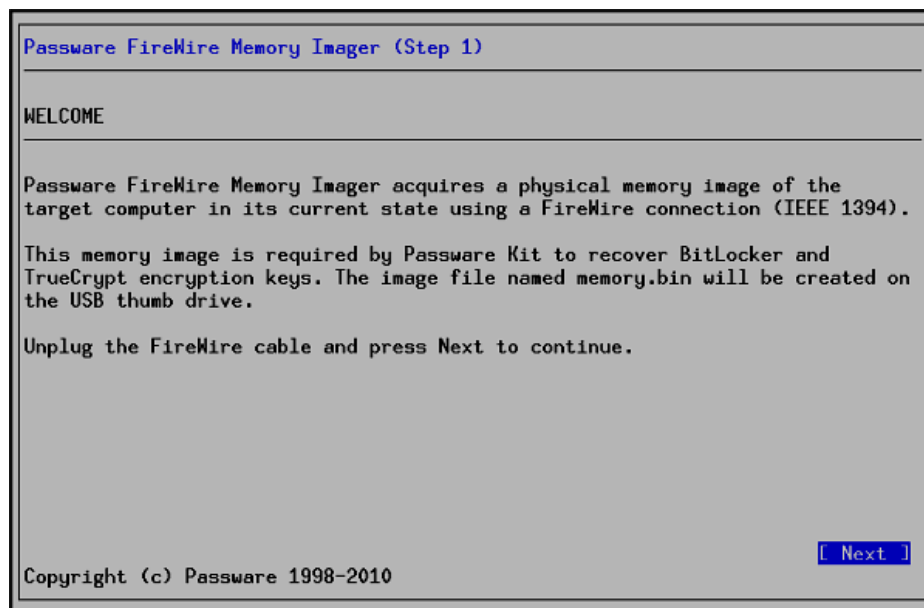
Jedini alat koji trenutno može otključati memoriju zaključanu BitLocker je ne-forenzički alat kompanije PassWare – Passware Kit Forensic 10.1 (slika 38). Iako u svom nazivu ima forenziku, on nije priznat forenzički alat, ali je ovo jedan od načina kompanije da se eventualno uključi u taj posao.

Za postupak otključavanja alat zahteva dve fizičke kopije diska, jer se sam proces otključavanja vrši upoređivanjem. Jedna od potrebnih kopija pravi se uz pomoć standardnih alata kao što su EnCase i WinHex, a druga uz pomoć Passware FireWire Memory Imager-a. Iako naznačava da se druga kopija može izraditi i drugim alatima kao što je win32dd, svaki pokušaj da sa takvim kopijama dođemo do željenog rezultata program je prekidao.



Slika 38: Passware Kit Forensic 10.1

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



Slika 39: Passware FireWire Memory Imager

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

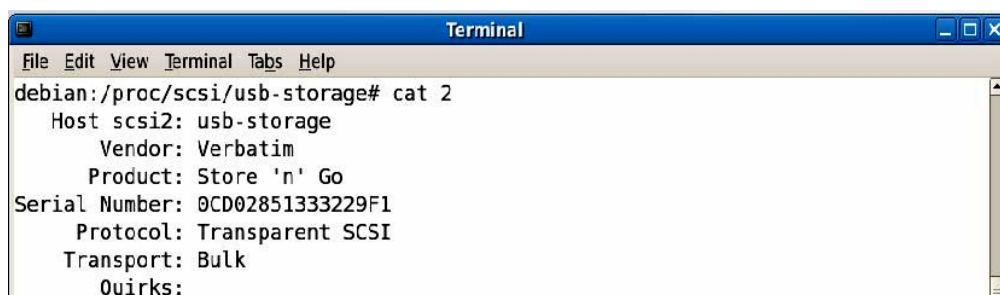
8.3 Praćenje USB uređaja povezanih na računar

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

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

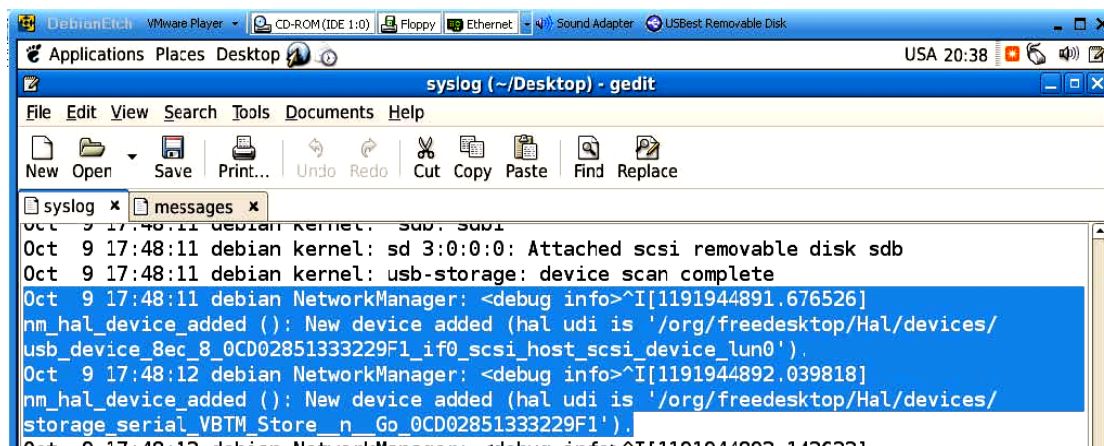
8.3.1 Linux OS

Na Linux operativnim sistemima identifikatori USB fleš diskova su jasni, konkretni i dosledni (slika 40). Pored informacije o proizvođaču uređaja postoje i jasne informacije koje ukazuju na sve one informacije vezane za sam disk (veličina, serijski broj, serija...). Da bi dokazali ovu tvrdnju povezali smo na računar sa instaliranim Linux (Debian) sistemom fleš disk u dva navrata. Najpre prvi put kada je u svom logu on i upisao informacije o uređaju, a zatim drugi put nakon dve nedelje.



Slika 40: Linux terminal prozor sa informacijama o povezanom fleš disku

Prikupljene informacije, koj se inače nalaze u messages.log i syslog.log datotekama uporedili smo ne bi li dokazali da su svi identifikatori isti za taj uređaj (slika 41).



Slika 41: Linux syslog datoteka sa informacijama o povezanom fleš disku

Poređenjem informacija na slici 40 i 41, informacije kao što su serijski broj, skraćenica od imena proizvođača (VBTM za Verbatim) i ime proizvoda (Store_n_Go) u potpunosti se slažu. Ova informacija ne samo da je uspešno sačuvana, već se u potpunosti slaže sa informacijama koje smo daljim ispitivanjem dobili o istom proizvodu na Windows operativnim sistemima.

8.3.2 Windows OS

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

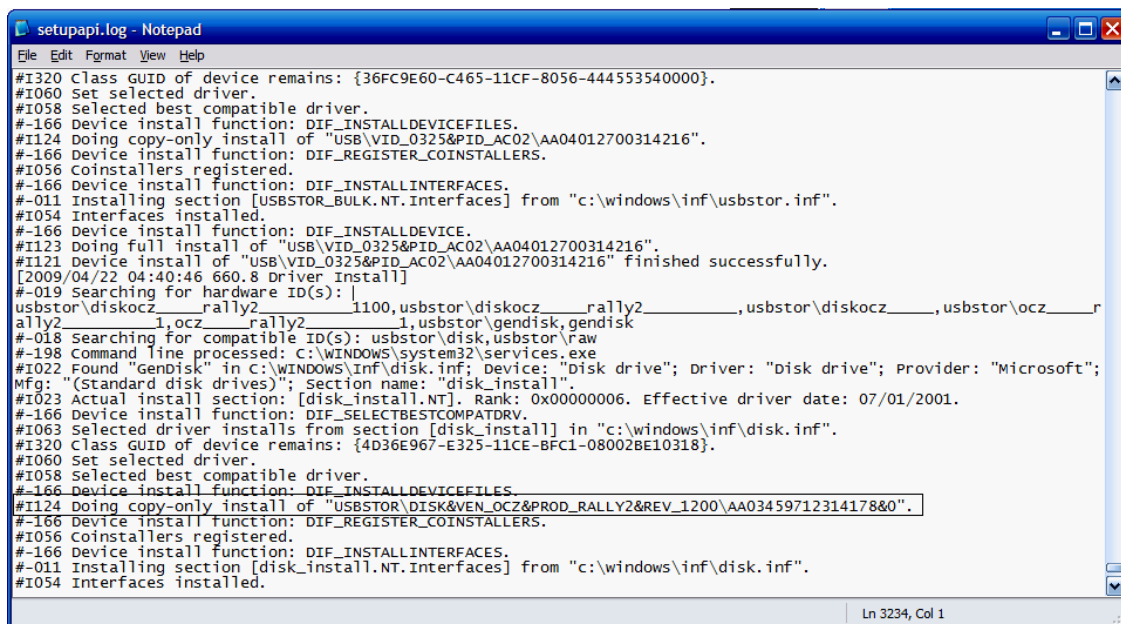
Informacije na osnovu kojih se vrši pretraživanje u *usbstor* datoteci nalaze se u hardveru. Na Windows sistemima identifikator uređaja koji se formira je u formatu `USB\VID_v(4)&PID_d(4)&REV_r(4)`. Po informacijama kompanije Microsoft *v(4)* je četvorocifreni broj proizvođača, dodeljen od strane nadležnih komisija, *d(4)* – broj koji proizvođač dodeljuje uređaju, a *r(4)* je revizija koda (Microsoft 2007). Ilustrovano na određenom uređaju u device manager-u (slika 42) „`USB\VID_08EC&PID_0008\0CD02851333229f1`“, gde je 08EC kod proizvođača, 0008 kod proizvođača, a 0CD0 je revizioni kod. Svi identifikatori su jedinstveni i predstavljaju ID uređaja (Device Instance ID).



Slika 42: Windows Device Manager

Najviše informacija za forenzičara u Windows operativnim sistemima nalazi se u registry bazi. Windows registry skladišti sve informacije o svim aspektima računara kao što su hardver, aplikacije, korisnici... Najbitnije za forenzičara je da na zna šta i gde da traži. Što se USB uređaja tiče najviše informacija se nalazi na lokaciji `HKEY_LOCAL_MACHINE\System\ControlSet00x\Enum\USBSTOR`. Na toj lokaciji nalaze se informacije o svim uređajima koji su putem USB veze ikad povezivani na računar sa Windows sistemom. Pretraživanjem ključeva, lako se može doći do informacija o povezanim USB fleš memorijama, na osnovu njihovog Device Instance ID – a.

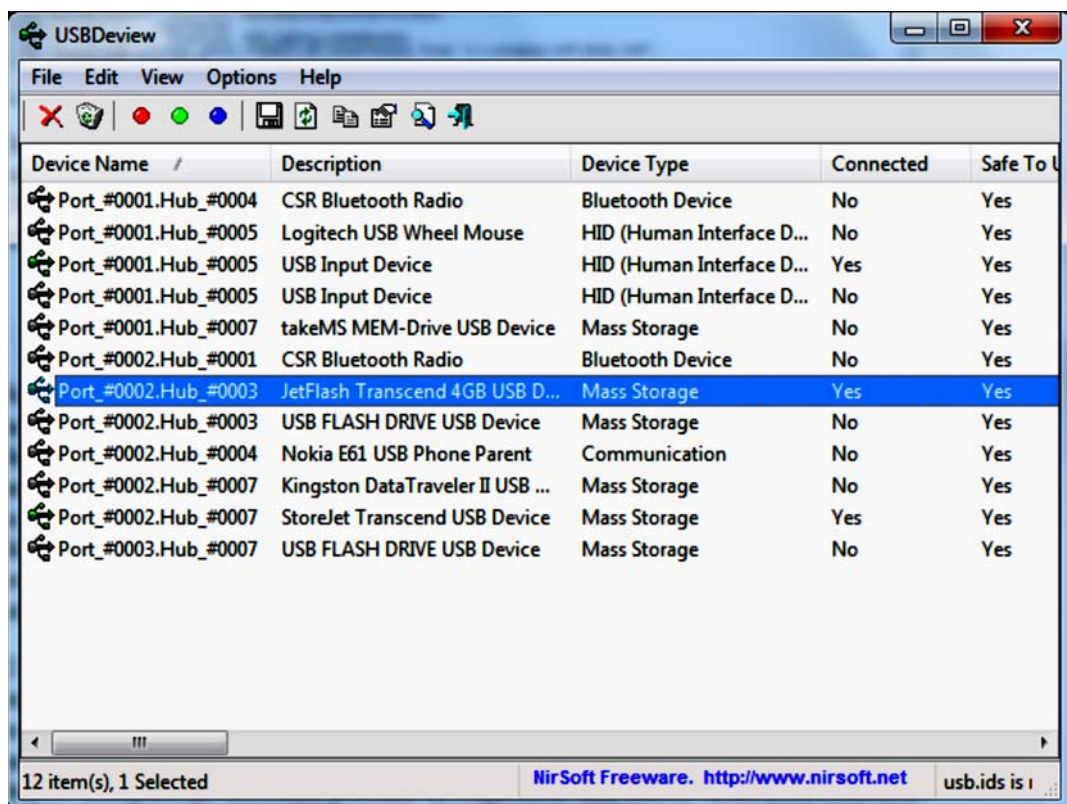
Sajt www.anti-forensics.com koji se bavi načinima za uništenje digitalnih dokaza, navodi brisanje USBSTOR ključa u registry bazi kao drugog po važnosti za uklanjanje dokaza na Win OS, odmah nakon brisanja Windows hibernacionog fajla. Takođe kada se radi o operativnom sistemu Windows XP, treba imati u vidu i fajl *setupapi.log* (slika 43), koji se nalazi u root-u windows operativnog sistema, u kome se takođe nalaze svi zapisi vezani za povezane uređaje.



```
#I320 Class GUID of device remains: {36FC9E60-C465-11CF-8056-444553540000}.
#I060 Set selected driver.
#I058 Selected best compatible driver.
#-166 Device install function: DIF_INSTALLDEVICEFILES.
#I124 Doing copy-only install of "USB\VID_0325&PID_AC02\AA04012700314216".
#-166 Device install function: DIF_REGISTER_COINSTALLERS.
#I056 Coinstallers registered.
#-166 Device install function: DIF_INSTALLINTERFACES.
#-011 Installing section [USBSTOR_BULK.NT.Interfaces] from "c:\windows\inf\usbstor.inf".
#I054 Interfaces installed.
#-166 Device install function: DIF_INSTALLDEVICE.
#I123 Doing full install of "USB\VID_0325&PID_AC02\AA04012700314216".
#I121 Device install of "USB\VID_0325&PID_AC02\AA04012700314216" finished successfully.
[2009/04/22 04:40:46 660.8 Driver Install]
#-019 Searching for hardware ID(s):
usbstor\diskocz____rally2____1100,usbstor\diskocz____rally2____,usbstor\diskocz____,usbstor\ocz____r
ally2____1,ocz____rally2____1,usbstor\gendisk,gendisk
#-018 Searching for compatible ID(s): usbstor\disk,usbstor\raw
#-198 Command line processed: C:\WINDOWS\system32\services.exe
#I022 Found "gendisk" in C:\WINDOWS\inf\disk.inf; Device: "Disk drive"; Driver: "Disk drive"; Provider: "Microsoft";
Mfg: "(Standard disk drives)"; Section name: "disk_install".
#I023 Actual install section: [disk_install.NT]. Rank: 0x00000006. Effective driver date: 07/01/2001.
#-166 Device install function: DIF_SELECTBESTCOMPATDRV.
#I063 Selected driver installs from section [disk_install] in "c:\windows\inf\disk.inf".
#I320 Class GUID of device remains: {4D36E967-E325-11CE-BFC1-08002BE10318}.
#I060 Set selected driver.
#I058 Selected best compatible driver.
#-166 Device install function: DIF_INSTALLDEVICEFILES.
#I124 Doing copy-only install of "USBSTOR\DISK&VEN_OCZ&PROD_RALLY2&REV_1200\AA03459712314178&0".
#-166 Device install function: DIF_REGISTER_COINSTALLERS.
#I056 Coinstallers registered.
#-166 Device install function: DIF_INSTALLINTERFACES.
#-011 Installing section [disk_install.NT.Interfaces] from "c:\windows\inf\disk.inf".
#I054 Interfaces installed.
```

Slika 43: Windows XP setupapi.log fajl

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

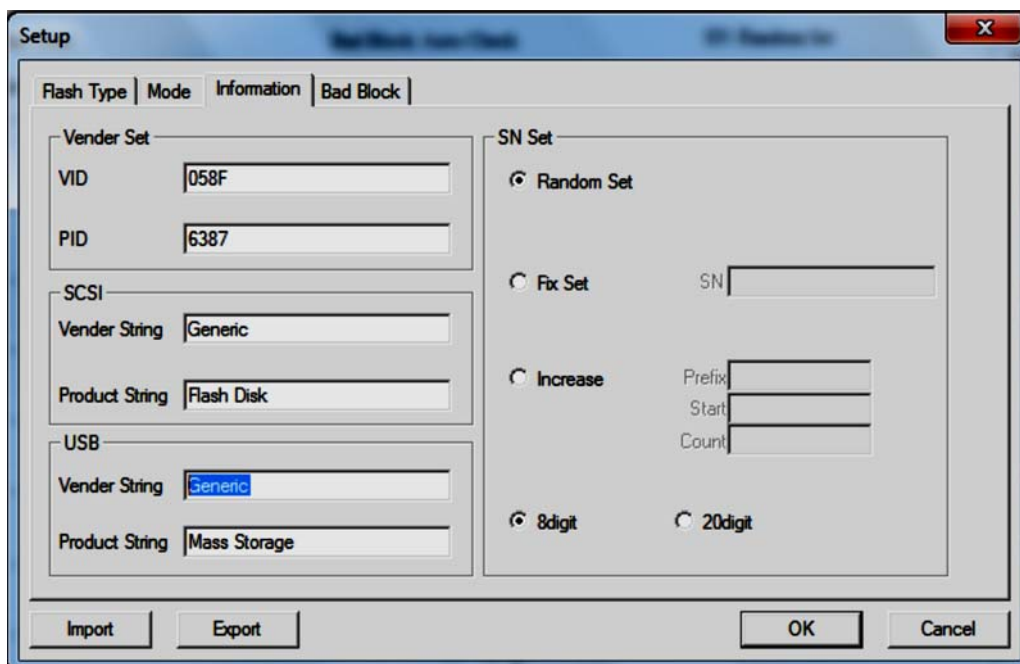


Device Name	Description	Device Type	Connected	Safe To U
Port_#0001.Hub_#0004	CSR Bluetooth Radio	Bluetooth Device	No	Yes
Port_#0001.Hub_#0005	Logitech USB Wheel Mouse	HID (Human Interface D...	No	Yes
Port_#0001.Hub_#0005	USB Input Device	HID (Human Interface D...	Yes	Yes
Port_#0001.Hub_#0005	USB Input Device	HID (Human Interface D...	No	Yes
Port_#0001.Hub_#0007	takeMS MEM-Drive USB Device	Mass Storage	No	Yes
Port_#0002.Hub_#0001	CSR Bluetooth Radio	Bluetooth Device	No	Yes
Port_#0002.Hub_#0003	JetFlash Transcend 4GB USB D...	Mass Storage	Yes	Yes
Port_#0002.Hub_#0003	USB FLASH DRIVE USB Device	Mass Storage	No	Yes
Port_#0002.Hub_#0004	Nokia E61 USB Phone Parent	Communication	No	Yes
Port_#0002.Hub_#0007	Kingston DataTraveler II USB ...	Mass Storage	No	Yes
Port_#0002.Hub_#0007	StoreJet Transcend USB Device	Mass Storage	Yes	Yes
Port_#0003.Hub_#0007	USB FLASH DRIVE USB Device	Mass Storage	No	Yes

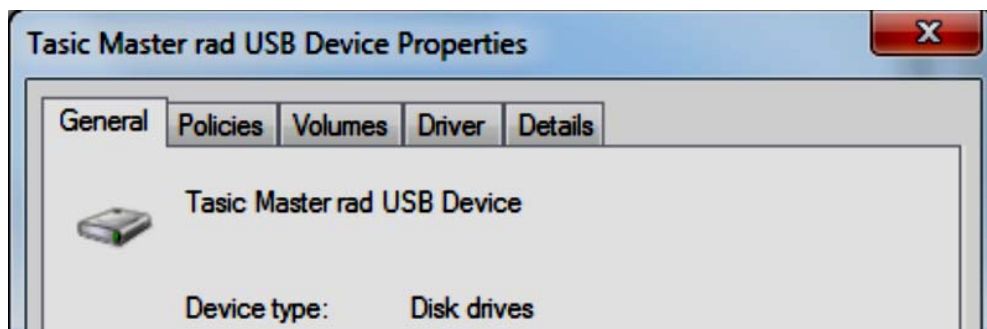
Slika 44: USBDeview

Iako postoje svi ovi identifikatori u sistemu, u današnje vreme se ne mogu koristiti previše. Razlog tome, osim uništavanja dokaza jeste i to što danas postoji veliki broj

NO NAME proizvođača, koji ne popunjavaju sve potrebne podatke tj. pre proizvodnje ne kontaktiraju „USB Implementers Forum²²“ – fondaciju postojećih proizvođača. Osim toga jedna ruska hakerska grupa na svom forumu za sve članove koji joj prilože nešto, nudi besplatan softverski alat za izmenu firmware-a fleš memorija. Njime se mogu zameniti svi identifikatori (slika 45 i 46), a i formatiranjem potpuno iskoristiti sav memorijski potencijal, često namerno zanemaren zbog politike cena po kojima se prodaju memorije.



Slika 45: Podešavanje proizvođačkih unosa



Slika 46: Izemljeni podaci Transcedent fleš diska

8.3.3 Povratak podataka sa oštećene USB fleš memorije

Neretko se dešava da forenzičari imaju posla sa fleš memorijama koje su oštećene iz raznoraznih razloga. U praksi se pokazalo da često dolazi do oštećenja zbog slabog/neujednačenog napona na USB kontrolerima, ali i namerno prilikom nasilnog prekida transvera podataka. Nažalost mnogi forenzički alati nemaju mehanizam za rad sa takvim memorijama, pa treba prenebenuti i ostalim alatima koji su dostupni. Ovi

²² www.usb.org

alati najčešće su pravljani za povratak podataka sa formatiranih fleš memorija, pa u tu svrhu mogu poslužiti i forenzičarima, jer mnogi kompjuterski kriminalci, najčešće, osim fizičkog sakrivanja, pribegavaju formatiranju, ne bi li uništili dokaze na njima.

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

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

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

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

8.3.4 TestDisk

Namena programa TestDisk, čiji je autor Christophe Grenier, kako mu ime kaže prvenstveno nije povraćaj podataka, već testiranje rada svih vrsta čvrstih memorija. Ipak, alat se smatra najmoćnijim za povraćaj podataka, posebno sa prenosivih memorija, ali i za rad sa njim potrebno je veliko znanje, poput toga kakav je fajl sistem memorije koja se testira tj. iz koje treba povratiti podatke (slika 47). Program radi pod svim poznatim operativnim sistemima, a interfejs je u komandnom modu.

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

Pri našem eksperimentu najnovija verzija programa povratila je većinu datoteka ispravno, ali sama struktura nije mogla da se razazna, jer su imena direktorijuma označena brojevima. Povratak podataka od trajao je kraće nego u bilo kom drugom programu, koji smo isprobali, te je najduži proces upravo bio podešavanje programa.

Velika prednost za forenzičare jeste i veličina programa koja iznosi svega 1.44MB (prilagođena veličini floppy diska), a program poseduje ugrađen sistem za izveštavanje.

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

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

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

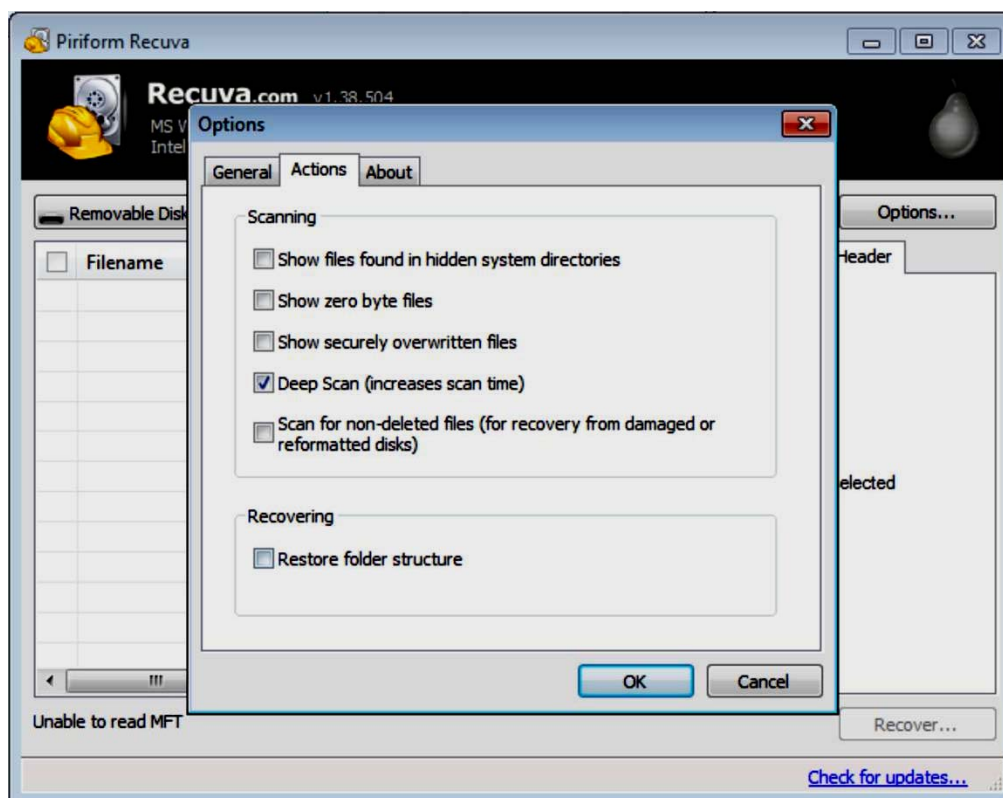
Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a drive to be 'Non-partitioned'.
```

Slika 47: Interfejs programa TestDisk

8.3.5 Recuva

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

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

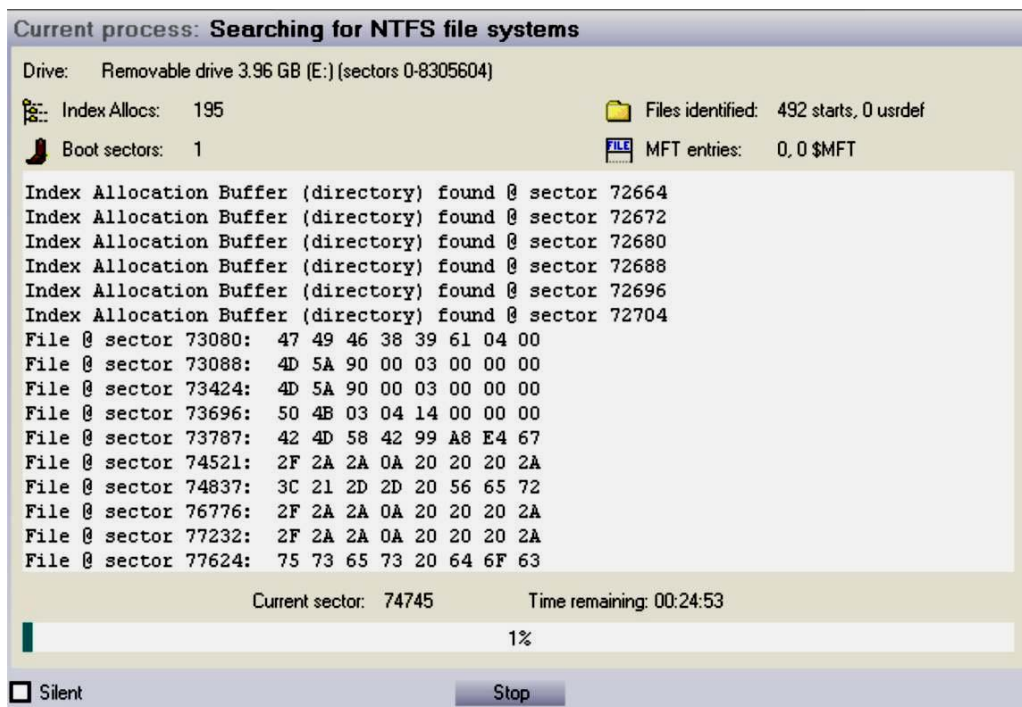


Slika 48: Recuva

8.3.6 GetDataBack

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

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



Slika 49: Proces oporavka u programu GetDataBack

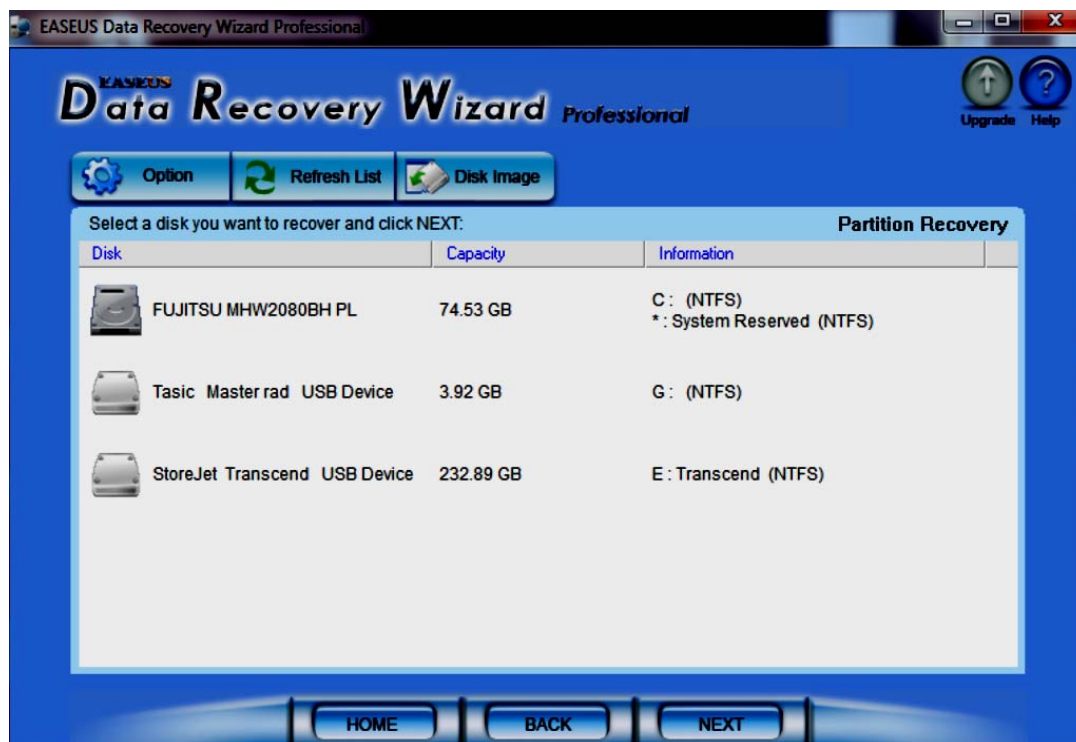
8.3.7 Stellar Phoenix Windows Data Recovery

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

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



Slika 50: Stellar Phoenix Windows Data Recovery



Slika 51: Easeus Data Recovery

9 DISKUSIJA DOBIJENIH REZULTATA

„Kad god neki programer kaže: „Niko se neće mučiti oko toga”, nađe se klinac u Finskoj raspoložen da se pomuči.“²³

Sve rasprostranjenija upotreba računara i razvoj kompjuterske tehnologije doprineo je lakšem obavljanju mnogih poslova, ljudima olakšao mnoge aspekte života, doprineo lakšoj i bržoj komunikaciji, ali uporedo sa tim omogućio veće zloupotrebe u smislu pojava novih kriminalnih radnji i inoviranja načina izvršenja klasičnih krivičnih dela. Prisustvo kompjuterskog kriminala predstavlja izuzetno opasnu pretnju po čitavo društvo, pa stoga treba mu pristupiti krajnje ozbiljno. Značaj ove oblasti ima više dimenzija kao što su politička, vojna, ekonomska, socijalna, etička itd.

Razvoj memorijski uređaja zasnovanih na fleš memoriji, pad njihove cene, neizbežno su promnili i polja istraživanja kojima se digitalna forenzika bavi. Većina udžbenika, knjiga, uputstva i web sajtova koji se bave digitalnom forenzikom, još uvek sve svodi na itraživanje podataka na magnetnim hard diskovima i optičkim medijumima. Situacija na polju prenosivih memorija u poslednjih 2 godine sve njih šalje u istoriju. Na internetu se može naći pregršt alata za forenziku tih uređaja, ali još uvek nema sveobuhvatnih, ili onih koji se bave isključivo tim memorijama. Razlog tome može se ogledati i u tome što za istraživanje podataka i pravljenje vernih slika, mogu iskoristiti alati namenjeni hard diskovima (npr. EnCase forenzičkim alatom može se napraviti imidž fleš kartice), jer fleš memorije, emuliraju njihov rad. Međutim, kao što se iz samog rada može videti, često ti alati ne mogu biti dovoljni, jer se podaci na fleš memorije smeštaju drugačijim principom.

U našem istraživanju došli smo do zaključka da je za forenzičara jako bitno poznavanje tipa memorije koju istražuje. Često je tokom istrage najbitije da na mestu krivičnog dela, istražitelj uoči ovakve memorije, jer su neki tipovi često jedva vidljivi golim okom. Samim tim, ako istražitelj ne zna šta da traži neće ni naći.

Naša istraživanja kako podataka dobijenih od proizvođača memorija, tako i literature i web sajtova koji se bave ovom tematikom, pa čak i različitih internet foruma nedvosmisleno potvrđuju jednu od postavljenih hipoteza rada, a to je da savremena digitalna forenzika mora da bude upoznata sa svim tipovima memorijskih uređaja da bi mogla da analizira podatke uskladištene na njima. Osim toga zaključili smo da je iako je došlo do pokušaja uništavanja digitalnih dokaza, neretko moguć povratak obrisanih i sakrivenih podataka.

Analogno svemu navedenom, poštujući podatke dobijene kroz istraživanje možemo definisati pravila kojih se forenzičari moraju držati kada su u pitanju USB i CF memorijski uređaji. Kroz primere korišćenja prenosivih memorija došli smo do zaključka da su one sveprisutne, te da će u narednom periodu predstavljati osnovni predmet istraživanja digitalne forenzike.

Broj internet stranica, foruma, publikacija koji se bave forenzikom je isuviše mali, s obzirom na prisustvo i značaj koji ova disciplina ima. U prilog tome ide i to što je

²³ Aleks Mejfild

većina alata isuviše skupa i van domašaja običnog sveta. Ipak sve je više i entuzijasta koji uz pomoć dostupnih nekomercijalnih alata uspeavaju da urade nešto na tom polju, držeći se strogih pravila računarske forenzike. Računarska forenzika zajedno sa napretkom tehnologije stalno se menja. Savakako to se najviše vidi kada su u pitanju flash, CF i srodne memorije. Danas nije neobično videti 250 različitih memorija tog tipa u prodavnicama fotoaparata i kamera ili u prodavnicama za snabdevanje kancelarija. Zbog sveprisutnosti i popularnosti koje ovih dana doživljavaju ovaj vid skladištenja podataka, forenzičarima ne preostaje ništa drugo, već da rad na njima stave u prvi plan. Ipak do danas ne postoji jasno definisan metod prikupljanja dokaza sa njih. Digitalni dokazi mogu na USB i CF memorijama su vrlo ranjivi, zbog čega postoji velika opasnost da budu uništeni ili oštećeni. Zbog toga je pre pristupa akviziciji potrebno razraditi planirane postupke i dobro poznavati alate.

Proučavajući literaturu, web sajtove koji se ovom tematikom bave, analizirajući studije slučajeva i primere iz prakse došli smo do zaključka da je akvizicija dokaza prioritetan cilj dobre forenzičke istrage.

10 ZAKLJUČAK

U ovom radu je sistematizovan materijal vezan za forenziku USB i CF memorijskih uređaja sa svim njegovim najvažnijim temama. Objasnen je način funkcionisanja prenosivih memorija i mesta korišćenja, a ušlo se i u problematiku oštećenih i zaključenih memorija i načinima ekstradicije dokaza sa njih.

Dat je prikaz raznolikosti prenosivih memorija i načina njihovog rada kao i potpun uvid u trenutno popularne formate fleš memorija. Na srpskom jeziku trenutno ne postoji jedinstven pregled svih ovih formata, a i pregledi se najčešće mogu naći jedino u vidu novinskih članaka, stručni pregledi ne postoje, a bilo kakva stručna objašnjenja se svode na novinske atrafile, sa tek po kojom informacijom.

Prikazani su komparativni, kao i dobijeni eksperimentalni rezultati. U radu su spomenuti i ne-forenzički alati i procedure dolaska do digitalnih dokaza. Date su definicije osnovnih termina, navedeni principi i standardi i kriterijumi iz oblasti forenzičke akvizicije digitalnih dokaza. Navedeni su osnovni problemi sa kojima se susreću forenzičari uz definicije šta je to digitalna istraga, šta je kompjuterski kriminal, zašto su toliko popularni i zbog čega su od velike važnosti za budućnost. Takođe, je dat pregled osnovnih karakteristika kompjuterskog kriminala, koje su mu pojavne forme i u kojim vidovima se ispoljava uz korišćenje prenosivih memorijskih uređaja.

Ovaj rad donosi efikasan i proveren metod akvizicije dokaza sa prenosivih memorija. Najpre, opisana je potreba za standardizacijom i definisanjem osnovnih načela kojih se treba držati u radu sa prenosivim memorijama. Hronološki su navedeni su i osnovni problemi na koje nailaze forenzičari u radu sa tim uređajima, rešenja za njih i alati koji se pritom koriste. Iako je pomenut veliki broj alata, više puta je naglašeno, da je za njihovo funkcionalno korišćenje potrebno veliko sistemsko predznanje i poznavanje osnovnih metoda forenzičke akvizicije.

Sprovedena istraživanja potvrdila su postavljenu glavnu hipotezu o forenzičkoj akviziciji dokaza sa USB i CF memorija. Takođe, poštujući podatke dobijene kroz istraživanje, opise alata za zaštitu prenosivih memorija, alata koji mogu pomoći tokom akvizicije i podataka proizvođača potvrđene su i posebne hipoteze.

11 LITERATURA

- [1] AccessData[®] - *FTK official guide*, AccessData Corporation, 2008
- [2] Alt.computer.security, *Enkripcija o zaštita podataka*, Beograd, 2009
- [3] Anastasijević S., *Advanced Encryption Standard*, Visoka tehnička škola Kragujevac, Kragujevac 2009
- [4] Anzaldúa R., Volonino L., *Computer Forensics For Dummies*, Wiley Publishing, Inc., Indianapolis 2008
- [5] Axelson J. *USB Mass Storage – Designing and Programming Devices and Embedded Hosts*, Lakeview Research LLC, Madison 2006
- [6] Bez, R.; Camerlenghi, E.; Modelli, A.; Visconti, A. *Introduction to flash memory*, IEEE 2003
- [7] Bunting S., Wei W. „The Official EnCase Guide“, Wiley Publishing, Inc., Indianapolis 2006
- [8] Carrier B. *File System Forensic Analysis*, Addison Wesley Professional, New York 2005
- [9] Carvey H., *Windows Forensic Analysis*, Syngress Publishing, Inc, USA 2009
- [10] Dmitrović A. *Forenzika – „Tehnički i socijalni aspekti*, knjiznica.irb.hr/nippur1/kolokviji/aco%20dmitrovic/c1_2dmitrovic.pdf
- [11] Grubor G., TRIBINA – *ZNAČAJ DIGITALNE FORENZIKE u rešavanju kompjuterskog incidenta i borbi protiv kompjuterskog kriminala*, Udruženje IT Veštak, Beograd
- [12] Jelić Z. *Gde su granice?*, Časopis „Svet“ – specijalno izdanje br. 1 „Svet kompjutera“, Politika, Beograd 1984.
- [13] Jones K., Bejtlich R., Curtis W., Rose C. *Real Digital Forensics*, Addison Wesley, New York 2005
- [14] Kim, K.; Koh, G.H. (2004-05-16), *Future Memory Technology including Emerging New Memories*, 24. Konferencija posvećena Mikroelektronici – Zbornik radova, Srbija i Crna Gora 2004
- [15] Kostić Z, Grubor G., *Alati za forenzičku analizu*, Sinergija Revija, Univerzitet Sinergija, Bljeljina 2009
- [16] Milosavljević M., Grubor G. *Digitalna forenzika – udžbenik*, Univerzitet Singidunum, Beograd 2009
- [17] Miljević M. *Skripta iz metodologije naučnog rada*, Filozofski fakultet, Univerzitet u Istočnom Sarajevu, Pale 2007

- [18] Mitnik K. *Umeće provale*, Mikro knjiga, Beograd 2005
- [19] Mitnik K. *Umetnost obmane*, Mikro Knjiga, Beograd 2004
- [20] Oparica G, *Računarlina forenzika*, InSig2, Zagreb 2007
- [21] *Pregled sigurnosnih incidenata u 2008. godini*, CCERT-PUBDOC-2009-02-254, www.cert.hr 2009
- [22] Schmid P., Roos A. *Will memory card take over the enterprise?*, Tom's Hardware (www.tomshardware.com) 2008
- [23] Solomon M., Barrett D., Broom B. *Computer Forensics – JumpStart*, SYBEX Inc, San Francisko, London 2005
- [24] Stojčev M, Mihajlović D., Paunović P. *Programiranje i čitanje memorije Am29F010 pomoću mikrokontrolera PIC16F877 – skripta*, Elektronski fakultet, Univerzitet u Nišu, Niš 2008
- [25] Vacca J., *Computer Crime Scene Investigation*, Charles river media, INC., Boston, Massachusetts 2005
- [26] Vermezović M. *Osnovi računarske tehnike – Skripta*, Fakultet za poslovnu informatiku, Univerzitet Singidunum, Beograd 2004.
- [27] Wiles J. *TechnoSecurity's Guide to E-Discovery and Digital Forensics*, Syngress Publishing, Inc, Burlington 2007

11.1.1 Neautorizovani izvori

- [1] B92 Tehnopolis, www.b92.net/tehnopolis
- [2] Benchmark Srbija, www.benchmark.rs
- [3] CERT.hr nacionalno središte za računalnu sigurnost, www.cert.hr
- [4] CET čitalište, www.cet.co.yu/CETcitaliste
- [5] How Stuff Works, www.howstuffworks.com
- [6] IT Exclusive, www.itx.ba
- [7] Kompjuter Biblioteka, www.kombib.rs
- [8] Mikro Elektronika, www.mikroe.com
- [9] Slobodna Enciklopedija, www.wikipedia.org

11.1.2 E – izvori

- [1] www.area51warez.info
- [2] www.articlesnatch.com

- [3] www.datasolutions.co.rs
- [4] www.digitalforce.org
- [5] www.digitalintel.com
- [6] www.elitesecurity.org
- [7] www.enterwarez.net
- [8] www.ethicalhacker.net
- [9] www.flashboot.ru
- [10] www.hackforums.net
- [11] www.katz.cd
- [12] www.old.pdfchm.com
- [13] www.rapidserbia.com
- [14] www.rdm.kiev.ua
- [15] www.sistemic.srce.hr
- [16] www.sizzledcore.com
- [17] www.usb.org
- [18] www.videoportal.hr
- [19] www.yu-fitness.com/forum/

12 LISTA POJMOVA

CF (CompactFlash) – format memorijske kartice koji je prvi predstavio i proizveo SanDisk još 1994 godine. Postoje dva tipa CF kartica: tip I (3.3mm debljine) i tip II (5mm debljine). Do 2004 je bio najzastupljeniji format kod digitalnih fotoaparata dok se danas zadržao kod dSLR aparata.

DRAJVER - program koji omogućava drugom programu (operativnom sistemu najčešće) da komunicira sa hardverskim uređajem. Drajver sadrži instrukcije i informacije kako da se neki hardver kontroliše, te kako njemu pristupiti. Bez drajvera računar ne bi mogao raditi. Drajver možemo nazvati posrednikom između hardvera i softvera.

FAT – File Allocation Table, ili „tabela razmeštanja datoteka“ je sistem organizacije podatka na memoriji. Bio je osnova operativnog sistema DOS i Windows 95. Zamenio ga je noviji FAT32 sa većom mogućnošću adresiranja. Danas se može sresti na prenosivim memorijskim karticama.

Firmware – upravljački softver digitalnih uređaja, najčešće smešten na fleš memoriji NOR tipa.

IEEE-1394 – poznatiji kao „FireWire“. Konektor za povezivanje digitalnih uređaja kao što su digitalni kamkorderi, skeneri, digitalni fotoaparati i kompjuteri.

IDE – Interfejs za priključivanje diskova na računar. Sa obzirom da se kontroler nalazi na samom disku, računaru nije potrebna dodatna kontrolerska kartica

Laptop – mobilni (prenosivi) računar

Live CD/DVD – CD na kome je nasnimljen operativni sistem (najčešće Linux). Ne zahteva korišćenje hard diska, već sve potrebno za rad smešta samo u radnoj memoriji računara

Memory Stick – format memorijske kartice koji je proizveo Sony. Ovaj format je tokom godina unapređivan tako da su iz njega proistekli ostali formati koje koriste Sony-jevi uređaji:

Microdrive – minijaturni hard disk spakovan u CompactFlash tip II kućište. Služi isto kao CF tip II memorijska kartica. Nedostatak je veća potrošnja električne energije u odnosu na obične CF kartice zbog pokretanja mehanike hard diska kao i veća osetljivost na temperaturu i fizička oštećenja.

MMC – format memorijske kartice koju koriste pojedini digitalni fotoaparati i stariji mobilni telefoni. Istog oblika i dimenzija kao SD memorijske kartice

MP3, WMA – Audio format, MP3 – MPEG 1, layer 3. Muzika kompresovana ovim algoritmom pogodna je za skidanje sa interneta na PC i razne MP3 playere. Budući da se muzička informacija smanjuje i više od 10 puta, koristi se uglavnom kao muzika za PC-e, u automobilu. WMA – Windows Media Audio je razvio Microsoft kao pandam popularnom mp3 formatu. Nije otvoren, pa samim tim nije stekao toliku popularnost kao mp3.

Palmtop – prenosivi računar, koji može stasti u ruku

PDA – Personal Digital Assistant, što u prevodu znači "lični digitalni pomoćnik", i predstavlja minijaturni kompjuter, koji staje najčešće na dlan, čije su osnovne namene skladištenje svakodnevnih podataka, razmena e-maila, prenos fajlova, reprodukcija multimedije i dr.. Prvim se PDA uređajem smatra 1993. godine na tržište izbačen Appleov Newton MessagePad. Najpopularniji PDA uređaji danas jesu Windows Mobile Pocket PC, BlackBerry, Palm, Symbian UIQ itd. Neke karakteristike zbog kojih su postali popularni jesu: ekran osjetljiv na dodir (kod većine), jednostavan način unosa teksta...

RAM - (Random Access Memory) Predstavlja memoriju koja svoju primjenu nalazi uglavnom kao radna memorija na računarima, PDA i Smartphone uređajima, ali i ostalim elektronskim uređajima. Najprihvatljiviji su oblici provodničke memorije.

ROM - Read Only Memory – kod prenosivih kompjutera ROM se upisuje standardni Firmware, odnosno one aplikacije koje nisu promjenjive, tj. ostaju stalno u uređaju, čak i nakon hard reseta. Ova memorija nije dinamična kao RAM. CD-ROM i DVD-ROM. Kad se na njih upišu podaci, oni se više ne mogu menjati.

SD (Secure Digital) – u današnje vreme najpopularniji format memorijske kartice.

SDHC (Secure Digital High Capacity) – novi SD format memorijske kartice (SD 2.0) koji omogućava kapacitete preko 2 GB.

USB - (Universal Serial Bus). Najrasprostranjeniji sistem ili vrsta serijskog priključka za računare i opremu koja se spaja na njih (kamere, fotoaparati, mobilni telefoni, fleš diskovi, miševi...). Danas je ovaj način povezivanja postao standard za povezivanje PC-a i elektronskih uređaja, jer pruža velike brzine prenosa podataka - do 480 MBit/s.

USB fleš – najpopularniji vid prenosive memorije. Povezuje se na USB port računara, a memorija je zasnovana na fleš tipu.

Virus – program koji ometa ispravan rad računara, a ponekad dovodi do gubitka svih podataka. Danas postoje razni vidovi, ovih zlonamernih programa, koji ugrožavaju svaki vid prenosa informacija, posebno putem interneta ili prenosivih memorija.

Windows – operativni sistemi za PC računare koje je razvila softverska kompanija Microsoft. Većina računara u svetu svoj rad zasniva upravo na ovim sistemima.

xD – tip memorijske kartice koji su razvili Fujifilm i Olympus za upotrebu u svojim digitalnim aparatima i kamerama