HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Helix forenzička distribucija

CCERT-PUBDOC-2006-08-164

CARNet CERT u suradnji s LS&S

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

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

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

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

Sadržaj

1. Uvod

Helix operacijski sustav spada u grupu sustava namijenjenih podizanju sa CD-ROM medija. To je posebna inačica poznate Knoppix Linux distribucije, koja je za razliku od drugih preinaka prilagođena za forenzičku analizu i reagiranje na incidentne (izvanredne) situacije. U tu svrhu, Helix je modificiran na način da nikad ne koristi *swap* particiju te da prepoznaje iste datotečne sustave koji su podržani i u Knoppix distribuciji (ext2, ext3, vfat, ntfs), ali također i xfs, reiser, jfs te mnoge druge datotečne sustave.

Važna funkcionalnost Helix distribucije je i mogućnost pokretanja u obliku samostalne aplikacije na Windows operacijskim sustavima. Pri tome su raspoloživi različiti alati namijenjeni za forenzičke svrhe u opsegu od 90MB. Tom funkcionalnošću Helix je razdijeljen u program koji analizira podignute Windows sustave te u Linux operacijski sustav koji se samostalno podiže.

Ovaj dokument opisuje načine pokretanja Helix sustava, rad Helix-a na Windows operacijskim sustavima te rad u obliku Linux operacijskog sustava.

Slika 1: Helix distribucija

2. Pokretanje Helix sustava

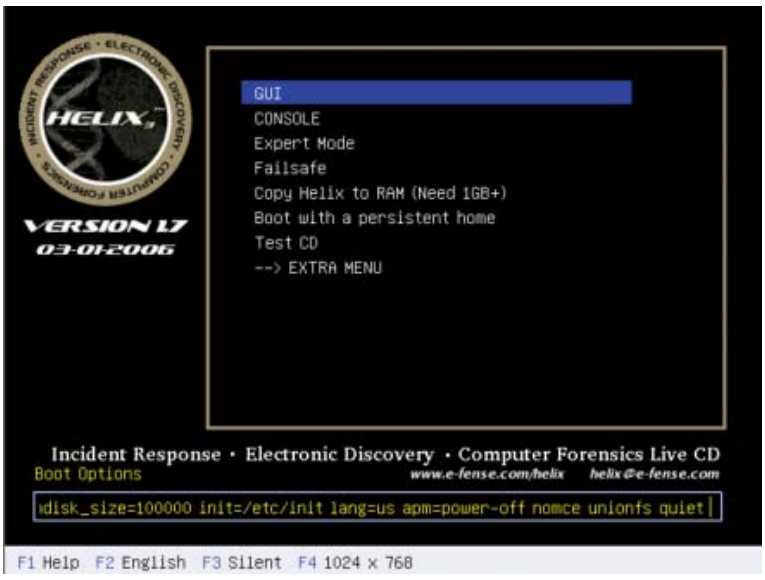
Helix se pokreće izravno sa CD medija te ga nije potrebno instalirati. Distribuciju je moguće preuzeti na stranici proizvođača [1], a trenutno je aktualna inačica 1.7.
Samu distribuciju moguće je koristiti na dva načina: kao Linux operacijski sustav kojim se analizira isključeni sustav, te kao aplikaciju pokrenutu pod Windows operacijskim sustavom pomoću koje se analizira rad uključenog sustava.
Helix sadrži statične binarne datoteke za Linux, Solaris i Windows operacijske sustave, koristeći GNU i Cygwin alate. Također su dostupni i mnogi drugi forenzički alati. Iako je mnogo alata dostupno preko grafičkog sučelja, velik je broj i onih koji su dostupni samo iz komandne linije.

2.1. Pokretanje na Windows operacijskim sustavima

Pri radu u Windows okruženju moguće je samo umetnuti Helix CD te kretanjem kroz njegov sadržaj pokrenuti potrebne forenzičke aplikacije. Sve binarne datoteke koje se koriste su statične tj. pokreću se isključivo sa CD medija i ne koriste nikakve dodatne biblioteke ili datoteke sustava na kojem su pokrenute.
Druga mogućnost pri radu na Windows operacijskim sustavima je korištenje `Helix.exe` aplikacije. Ukoliko je na računalu omogućeno automatsko pokretanje (eng. *autorun*), nakon umetanja CD-a, Helix aplikacija se automatski pokreće. U slučaju kada je automatsko pokretanje isključeno, aplikaciju je potrebno pokrenuti ručno. Nakon što se pokrene `Helix.exe`, korisniku je dostupno grafičko sučelje koje olakšava rad s dostupnim alatima.

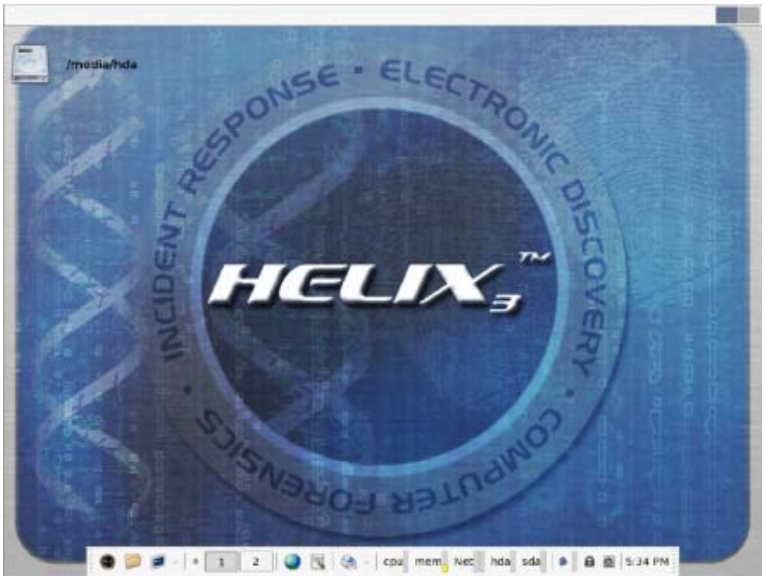
2.2. Pokretanje kao Linux operacijskog sustava

Jedna od najvećih prednosti Helix distribucije je to što se pokreće kao samostalan operacijski sustav. Helix distribuciju moguće je pokretati na svim računalima zasnovanima na x86 arhitekturi.



Slika 2: Izbornik Helix distribucije

Prilikom podizanja operacijskog sustava s Helix CD-a, moguće je mijenjati velik broj parametara. Kompletan popis parametara s njihovim značenjem dostupan je u dokumentaciji koja se nalazi na CD-u i koju je moguće preuzeti sa stranica proizvođača [2]. Nakon podešavanja potrebnih parametara potrebno je pritisnuti tipku ENTER nakon čega će početi podizanje sustava.
Po završetku podizanja sustava automatski će se pokrenuti X Windows okruženje. Helix koristi Xfce grafičko okruženje zbog njegove jednostavnosti i svestranosti. Većina potrebnih stvari dostupna je preko Helix-ovog izbornika i trake sa zadacima na dnu ekrana. Detaljnije upute za korištenje Xfce okruženja moguće je pronaći na stranicama Xfce-a [3].



Slika 3: Grafičko okruženje Helix Linux varijante

Odabirom Helix-ovog izbornika dobiva se pristup velikom broju naredbi i podizbornika. Ovaj izbornik također se aktivira desnim klikom na radnu površinu. U glavnom dijelu izbornika dostupni su:

1. *Run Program* – za pokretanje aplikacija,
2. *Terminal* – za otvaranje komandne linije,
3. *Mount Manager* – upravitelj koji omogućuje korisniku upravljanje uređajima koji su montirani i
4. *Rescan Devices* – pruža mogućnost pristupa uređajima koji nisu bili automatski otkriveni prilikom pokretanja sustava.

Slika 4: Helix-ov izbornik

Osim ovih osnovnih operacija u izborniku se nalaze i određeni podizbornici:

1. forenzika (eng. *Forensics*) – u ovom izborniku sadržani su alati za forenzičku analizu računala te podizbornik s dokumentacijom za određene alate,
2. rješavanje incidenata (eng. *Incidennt Response*) – ovdje se nalaze samo tri alata: Ethereal za analizu mrežnih protokola te dva antivirusna programa – ClamAV i F-Prot,
3. uredske aplikacije (eng. *Office*) – sadrži osnovne uredske aplikacije za uređivanje teksta, pregled pdf datoteka, tablični kalkulator i program za izradu prezentacija,
4. multimedijske aplikacije (eng. *Multimedia*) - u ovom izborniku se nalaze programi za snimanje CD-a, pregledavanje slika, gledanje video zapisa i slušanje audio zapisa, te programi za kontrolu zvuka,

5. sistemski alati (eng. *System Tools*) - osnovni sistemski alati poput alata za particioniranje diskova, pretraživanje diskova, formatiranje disketa, snimanje *screenshot*-ova i sl., i
6. Helix-ovi alati (eng. Helix Tools) - u ovom izborniku se nalaze alati potrebni za osnovnu konfiguraciju računala pa se tako ovdje mogu konfigurirati printeri, mrežne kartice, modemi, ADSL konekcije, pokretati osnovni servisi (samba, syslog, ssh, ...)..

Osim alata dostupnih preko izbornika, postoji velik broj alata koji su dostupni samo iz komandne linije.

3. Helix na Windows operacijskim sustavima

Helix je na Windows operacijskim sustavima moguće koristiti na tri načina. Jedan je pokretanjem grafičkog sučelja pomoću `Helix.exe` izvršne datoteke, drugi je korištenjem komandne linije Helix-a, a treći je izravno pokretanjem pojedinih programa koji su sadržani u Helix distribuciji korištenjem Windows Explorer programa. Preduvjet za pokretanje na zadnji način je da ti programi moraju imati grafičko sučelje.

Kao što je prethodno spomenuto, Helix se na Windows operacijskim sustavima izvršava kao zasebna aplikacija. Pri tome se prati aktivno stanje Windows sustava, tj. aktivni procesi, koji se kontinuirano mijenjaju, a tome dodatno doprinose i alati koji se pokreću s Helix CD-a. Ipak, pošto se gašenjem sustava mogu izgubiti važni forenzički podaci, mogućnost pokretanja forenzičkih alata tijekom rada sustava je veoma korisna. Helix za Windows sustave se može koristiti za prikupljanje informacija sa sustava koji se ne smiju gasiti, a to su uglavnom poslužitelji.

Svi pokrenuti alati pokreću se s privilegijama korisnika koji je trenutno prijavljen na sustavu. Ukoliko trenutni korisnik ima ograničena prava, na sustavu postoji mogućnost nepravilnog izvršavanja nekih alata. Iz tog se je razloga ponekad potrebno prijaviti na sustav s ovlastima administratora kako bi se osigurao nesmetan rad i potpuna funkcionalnost.

3.1. Administracijsko sučelje za Windows sustave

Administracijsko sučelje Helix Windows aplikacije, testirano je na Windows 98SE, NT4, 2000 i XP operacijskim sustavima. Važno je napomenuti da se za pokretanje grafičkog sučelja koriste neke DLL datoteke sustava na kojem se pokreće Helix pokreće. Potrebne DLL datoteke nije moguće uključiti u Helix CD zbog različitosti između pojedinih inačica samih Windows operacijskih sustava.

Slika 5: Grafičko sučelje pod Windows operacijskim sustavom

Samo grafičko sučelje podijeljeno je u više dijelova:

- *Preview System Information* – prikazuje se verzija operacijskog sustava te sažete informacije o diskovima i mrežnim sučeljima. Također je dostupan i popis svih aktivnih procesa na sustavu.

- *Acquire a „live" image of a Windows System using dd* – služi za izradu kopija čvrstih diskova, disketa ili sadržaja memorije te za spremanje istih na CD, DVD ili drugo računalo na mreži, korištenjem dd (eng. *Disk Duplicator*) alata.
- *Incindent Response tools for Windows System* – u ovom djelu je dostupno 20 alata koji se pokreću izravno sa CD medija u svrhu forenzičke analize.
- *Documents pertaining to Incident Response, Computer Forensics, Computer Security & Computer Crime* – pristup dokumentaciji koja sadrži osnovne upute za korištenje Helix distribucije i osnovne upute za prikupljanje forenzičkih podataka.
- *Browse contents of the CD-ROM and Host OS* – jednostavni preglednik sadržaja diskova koji prikazuje osnovne podatke za svaku odabranu datoteku (ime datoteke, datum kreiranja, datum zadnje izmjene, datum zadnjeg pristupa, CRC, MD5 i veličinu datoteke).
- *Scan for Pictures from a live system* – pretražuje zadani disk ili direktorij i prikazuje sve pronađene slike. Ova opcija podržava velik broj grafičkih formata.

3.1.1. Pregled sistemskih informacija

Unutar sučelja za pregled sistemskih informacija (eng. *Preview System Information*), raspoložive su osnovne informacije o sustavu:

- administrator (*Admin*) – informacija o tome je li trenutno prijavljeni korisnik administrator,
- administratorska prava (*Admin Rights*) – informacija o tome da li trenutno prijavljeni korisnik ima administratorska prava,
- mrežne kartice - NIC (eng. *Network Interface Card*) – MAC adresa mrežne kartice. Ukoliko je vrijednost „000000000000" kartica je vjerojatno u „promiskuitetnom" modu i moguć je slučaj u kojem hvata sav mrežni promet,
- IP – trenutna IP adresa,
- popis svih diskova koji mogu biti CD, DVD, čvrsti, uklonjivi i sl., a za koje su opisani tip i veličina.

Nakon stranice s osnovnim informacijama, moguće je otvoriti i slijedeća stranicu s informacijama koje prikazuju trenutno aktivne procese. Klikom na trokutić desno od ikone stranice, mijenjaju se stranice.

Slika 6: Popis aktivnih procesa na sustavu

Dvostrukim odabirom nekog od aktivnih procesa nudi se mogućnost ubijanja istog.
Ukoliko je računalo bilo metom napada, moguća je situacija u kojoj je originalni *Task manager* koji prikazuje aktivne procese izmijenjen kako ne bi prikazivao zlonamjerne procese. Kako se Helix pokreće sa CD medija, on ne može biti izmijenjen pa bi trebao biti u mogućnosti prikazati sve procese.

3.1.2. Kreiranje kopija diskova i memorije na Windows sustavima korištenjem dd alata

Na sučelju za kreiranje kopija diskova i memorije na Windows sustavima korištenjem dd (eng. *Disk Duplicator*) alata (eng. *Acquire a „live" image of a Windows System using dd*) raspoloživa su dva alata namijenjena stvaranju slike (eng. *image*) diska ili fizičke memorije. Na prvoj stranici nalazi se grafičko sučelje komandno-linijskog programa dd, dok se na drugoj stranici nalazi program FTK Imager from AccessData. FTK Imager je u mogućnosti kreirati samo kopije diskova, dok `dd` može kreirati i kopije fizičke memorije. Također, dd alat je u mogućnosti snimiti kopiju na mrežnim uređajima, dok FTK Imager može snimati kopije samo na lokalne uređaje.

Prilikom korištenja `dd` programa u padajućem izboru moguće je odabrati disk koji se želi preslikati, destinaciju gdje je potrebno spremiti kopiju, naziv kopije, veličinu spremanih blokova podataka. Ostale mogućnosti su:

- *Attached/Shared* – uključivanjem ove mogućnosti kopija se sprema na lokalni ili mrežni disk,
- *Netcat* – ova mogućnost isključuje prethodnu, a sama omogućuje izravno slanje kopije na Netcat poslužitelj koji se nalazi na mreži, a kao preduvjet potrebno je specificirati IP adresu poslužitelja,
- Razdijeli kopiju (eng. *Split Image*)– omogućuje dijeljenje kopije ukoliko veličina kopije premašuje kapacitet medija na koji ju se sprema.

Nakon unosa svih željenih parametara pritiskom na opciju *Acquire* otvorit će se komandna linija u koju je potrebno zalijepiti naredbu te pritisnuti tipku Enter kako bi se ona izvršila.

Nakon uspješnog izvršenja naredbe kreiraju se 3 datoteke:

1. `ime_datoteke.dd` – datoteka koja sadrži kopiju diska,
2. `ime_datoteke.dd.md5` – datoteka s MD5 kodom kopije i
3. `Audit.log` – datoteka sa zapisom naredbe i njezinog ispisa.

Slika 7: Grafičko sučelje `dd` programa

Za pokretanje FTK Imagera potrebno je odabirom trokutića otvoriti drugu stranicu na kojoj su prikazane osnovne informacije o alatu te odabrati opciju *Imager*. Program posjeduje detaljnu dokumentaciju koja je dostupna preko izbornika *Help*.

3.1.3. Alati za rješavanje incidenata na Windows sustavima

Sučelje s alatima za rješavanje incidenata na Windows sustavima (eng. *Incindent Response tools for Windows System*) pruža pristup brojnim aplikacijama za rješavanje incidenata. Sveukupno su tri stranice s alatima koje se mijenjaju pomoću trokutića pokraj ikone.

Slika 8: Dio alata dostupnih iz grafičkog sučelja

Dostupni alati su:

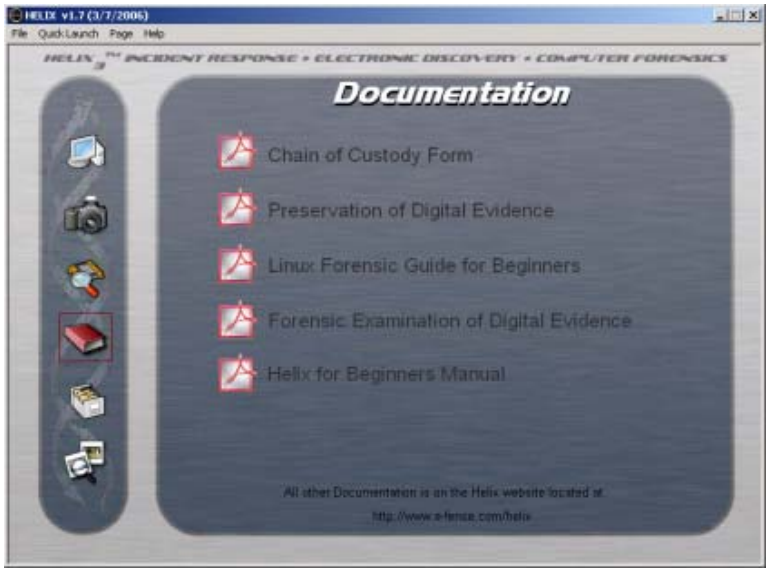
- Windows Forensic Toolchest (WFT) –alat koji pruža automatsko reagiranje na incidente na Windows sustavima i kako bi prikupio informacije koje su važne za sigurnost. To je u osnovi forenzički poboljšana ljuska koja je u mogućnosti pokretati druge programe i proizvesti HTML izvještaj.
- Incident Response Collection Report (IRCR2) – skripta koja poziva druge alate za prikupljanje i analiziranje podataka na Windows sustavima. Većina alata je orijentirana k prikupljanju podataka. Osnovna ideja ICRCR2 skripte je ta po kojoj program može pokrenuti bilo tko te rezultat poslati stručnjaku na daljnju analizu.
- First Responder's Evidence Disk (FRED) – prikuplja veliku količinu podataka o sustavu te ih sprema u tekstualnu datoteku. Podatke je moguće spremiti na disketu, Netcat poslužitelj ili na bilo koji drugi disk na sustavu.
- First Responder Utility (FRU) – namijenjen je prikupljanju promjenjivih podataka na sustavu „žrtvi". Aktualna inačica je komandno-linijski program imena FRUC. FRUC sve podatke šalje računalu na mreži na kojem je pokrenut FSP (eng. *Forensic Server Project*).
- Security Reports (SecReport) – čine ga dva komandno-linijska alata namijenjena skupljanju informacija vezanih uz sigurnost na Windows sustavima te za usporedbu izvještaja bilo da se radi o izvještajima dva različita računala ili o izvještajima istog računala u različitim vremenima. Izvještaji se spremaju u XML formatu. Alat je, osim u forenzici, koristan i u svakodnevnoj provjeri sigurnosti sustava.
- Md5 Generator – generira MD5 sažetak bilo koje datoteke na sustavu.
- Command Shell – Helix grafičko sučelje automatski otkriva i pokreće odgovarajuću komandnu liniju. Dostupne su sve standardne naredbe kao i mnogi forenzički alati sadržani na CD-u.
- File Recovery – ovaj program namijenjen je otkrivanju i oporavku obrisanih datoteka. Podržan je rad s FAT 12/16/32 i NTFS datotečnim sustavima. Program je u mogućnosti automatski prepoznati particije na disku čak i ukoliko je *boot* sektor ili FAT oštećen ili izbrisan.
- Rootkit Revealer – program je u mogućnosti otkriti sve *rootkit*-ove navedene na www.rootkit.com. *Rootkit* je niz zlonamjernih programa koji izmjenjuju operacijski sustav kako ih se ne bi moglo otkriti tradicionalnim načinima. Na primjer, isti mogu modificirati Windows Explorer i `dir` naredbu kako korisnik ne bi mogao vidjeti direktorij u kojem je *rootkit* instaliran.
- VNC (eng. *Virtual Network Computing*) poslužitelj – program za udaljenu kontrolu koji omogućuje pregled i interakciju s računalom (poslužiteljem) pomoću jednostavnog programa (preglednik) na računalu koje se nalazi bilo gdje na Internetu.

- Putty SSH – PuTTY je slobodna implementacija Telnet i SSH2 protokola za Win32 i Unix platforme koja sadrži i emulaciju xterm terminala. Ovaj program omogućuje korisniku prijavljivanje na udaljeno računalo i izvršavanje naredbi na njemu.
- Screen Capture (HoverSnap) - besplatan program za snimanje slika računala s podrškom za jpg, png, bmp i gif formate. Njegovim korištenjem moguće je napraviti sliku cijelog ekrana, aktivnog programa ili određenog dijela ekrana. Također, slike je moguće automatski prebaciti preko FTP protokola.
- Messenger Password –omogućuje oporavak zaporki iz slijedećih *instant messenger* programa: MSN Messenger, Windows Messenger (na Windows XP), Yahoo Messanger (inačice 5.x i 6.x), ICQ Lite 4.x/2003, AOL Instant Messenger (samo starije inačice), AOL Instant Messenger/Netscape, Trillian, Miranda i GAIM.
- Mail Password Viewer – omogućuje otkrivanje zaporki i drugih detalja korisničkih računa u slijedećim programima za pregledavanje elektroničke pošte: Outlook Express, Microsoft Outlook 2000 (samo POP3 i SMTP računi), MS Outlook 2002/2003 (POP3, IMAP, HTTP i SMTP računi), IncrediMail, Eudora, Netscape 6.x/7.x, Mozilla Thunderbird, Group Mail Free, Yahoo! Mail (ukoliko je zaporka spremljena u Yahoo Messenger-u), Hotmail/MSN (ukoliko je zaporka spremljena u MSN Messenger-u), Gmail (ukoliko je zaporka spremljena u Gmail Notifier aplikaciji). Za svaki korisnički račun prikazuju se slijedeći podaci: ime računa, aplikacija, adresa elektroničke pošte, poslužitelj, tip poslužitelja (POP3/IMAP/SMTP), korisničko ime i zaporka.
- Protect Storage Viewer – omogućuje prikazivanje zaporki koje su spremili Internet Explorer, Outlook Express i MSN Explorer. Program prikazuje samo zaporke trenutno prijavljenog korisnika i nema mogućnost prikazivanja zaporki ostalih korisnika.
- Network Password Viewer - preglednik mrežnih zaporki. Prilikom pristupanja dijeljenom disku na mreži ili prijavljivanjem na .NET Passport korisnički račun, Windows operacijski sustavi omogućuju spremanje zaporke za kasniju upotrebu. Network Password Viewer omogućuje otkrivanje svih mrežnih zaporki spremljenih na računalu i to: zaporke za prijave na udaljena računala na LAN-u, zaporke za račune elektroničke pošte na Exchange poslužitelju (spremljene od strane Outlooka 2003), zaporke MSN messenger računa (samo do inačice 7.0).
- Registry Viewer (RegScanner) - alat za pretraživanje registra Windows operacijskih sustava, pronalaženje vrijednosti koje zadovoljavaju zadane kriterije te njihovo prikazivanje na jedinstvenoj listi.
- Asterisk Logger – alat za otkrivanje zaporki. Mnoge aplikacije poput CuteFTP-a, VNC-a, IncrediMail-a, Outlook Expressa i drugih omogućuju spremanje zaporki za kasniju upotrebu u istima. Unesene zaporke se ne prikazuju na zaslonu, već je umjesto stvarne zaporke prikazan niz zvjezdica ('*****'). Ovaj alat omogućuje prikaz zaporki koje se nalaze iza niza zvjezdica.
- IE History Viewer – ovaj alat pretražuje povijesne (eng. *history*) datoteke na računalu i prikazuje listu svih URL-ova posjećenih u zadnjih nekoliko dana. Moguće je odabrati jednu ili nekoliko URL-ova te ih ukloniti iz *history* direktorija ili ih spremiti u tekstualnu, HTML ili XML datoteku. Također je moguće pregledavati povijesne datoteke ostalih korisnika na računalu.
- IECookiesView - aplikacija koja prikazuje detalje o svim web kolačićima (eng. *cookies*) koje Internet Explorer sprema na računalo. Osim prikaza informacija moguće je: sortirati listu po bilo kojem polju, pronalaziti web kolačiće prema imenu web stranice, brisanje neželjenih web kolačića, spremanje sadržaja web kolačića u tekstualnu datoteku, prikaz web kolačića drugih korisnika.
- MozillaCookiesView - alternativa standardnom Cookie Manager alatu raspoloživom u Netscape i Mozilla preglednicima. Alat prikazuje detalje o svim web kolačićima te omogućuje spremanje liste u tekstualnu, HTML i XML datoteku. Također, omogućuje brisanje, izradu sigurnosnih kopija i oporavak obrisanih web kolačića iz sigurnosnih kopija.

3.1.4. Dokumentacija povezana s računalnom forenzikom, sigurnošću, kriminalom i rješavanjem incidenata

Ovaj dio (eng. *Documents pertaining to Incident Response, Computer Forensics, Computer Security & Computer Crime*) pruža korisniku pristup nekim korisnim dokumentima u PDF obliku. Dokumenti sadržani na CD-u su:

- Plan nadzora (eng. *Chain of Custody Form*) – primjer obrasca korištenog od strane e-fense.inc za praćenje postupanja s digitalnim dokazima.
- Očuvanje digitalnih dokaza (eng. *Preservation of Digital Evidence*) – dokument koji pojašnjava metode čuvanja digitalnih dokaza. Priroda digitalnih dokaza čini ih inherentno krhkima. Podaci mogu biti izbrisani ili promijenjeni bez traga usporavajući istražiteljevu potragu za istinom. Napori prvog istražitelja su kritični kako bi se osiguralo da su dokazi prikupljeni i sačuvani na jednostavan, siguran i forenzički zdrav način. Ovaj dokument opisuje neke od izazova s kojima se prvi istražitelji suočavaju kao i neke od strategija kako se nositi s njima. Autor dokumenta je Jesse Kornblum, specijalni agent Ureda američkih zračnih snaga za specijalne istrage.
- Vodič kroz Linux forenziku za početnike (eng. *Linux Forensic Guide for Beginners*) – jedan od prvih i najopširnijih vodiča za korištenje Linux operacijskih sustava u forenzici. Autor dokumenta je Barry J. Grundy, specijalni agent NASA-inog Ureda za opću istragu, odjel za računalni kriminal. Iako ovaj dokument nije specifično orijentiran prema Helix operacijskom sustavu, isti može poslužiti kao izvor pozadinskih informacija za one koji su voljni pokretati Helix Linux operacijski sustav.
- Forenzičko pregledavanje digitalnih dokaza (eng. *Forensic Examination of Digital Evidence*) – dokument je objavilo američko Ministarstvo pravde 2004. godine. Dokument pruža detaljan vodič za digitalne forenzičke istražitelje kako prikupiti, obraditi i dokumentirati digitalne dokaze.
- Helix dokumentacija za početnike (eng. *Helix for Beginners Manual*) – ovaj dokument je vrlo iscrpna dokumentacija Helix distribucije. Osim na CD-u dostupna je i na web stranicama proizvođača [2].



Slika 9: Dokumentacija sadržana na Helix CD-u

3.1.5. Pregledavanje sadržaja CD medija i računala

Kroz ovo sučelje (eng. *Browse contents of the CD-ROM and Host OS*) otvara se jednostavni preglednik datoteka koji će istražitelju pružiti osnovne informacije o njima. Moguće je pregledavati datoteke sa CD medija, ili s računala koje se analizira. Preglednik prikazuje: ime datoteke, datume kreiranja, zadnjeg pristupa i zadnje izmjene, atribute, CRC, MD5 ključ i veličinu datoteke.

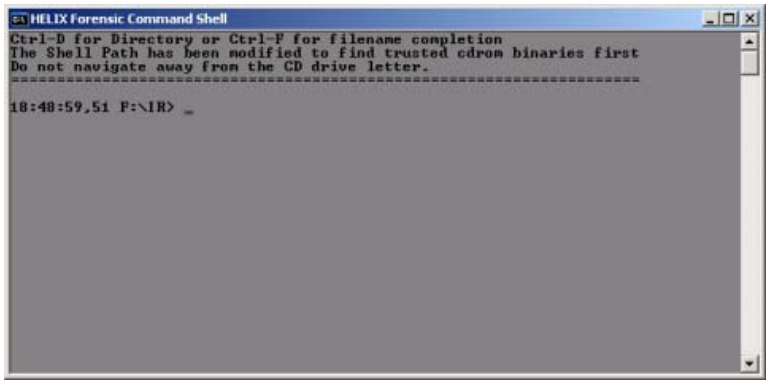
Zbog sam prirode Windows operacijskog sustava, prilikom prvog odabira datoteke (na bilo kojem mediju na kojem je omogućeno pisanje) prikazat će se datum zadnjeg pristupa. Ukoliko se ista datoteka odabere ponovno biti će prikazano vrijeme prethodnog pristupa. Ovo je osobina Windows operacijskih sustava koju nije moguće lako spriječiti.

3.1.6. Traženje slika na analiziranom sustavu

Unutar ovog izbornika (eng. *Scan for Pictures from a live system*) raspoloživ je alat koji istražitelju omogućuje brzo pretraživanje sustava u potrazi za sumnjivim slikama. Podržani su mnogi formati datoteka koje se na Windows sustavima prikazuju kao *thumbnail*-ovi.

3.2. Komandna linija za Windows sustave

Komandnu liniju je osim iz grafičkog sučelja moguće pokrenuti i izvršavanjem CMD.EXE aplikacije smještene unutar odgovarajućeg poddirektorija u `ir\` direktoriju na CD-u. Direktoriji su odijeljeni prema inačici Windowsa.
Nakon pokretanja komandne linije izvršavanjem CMD.EXE potrebno je izvršiti i datoteku za konfiguraciju okoline kako bi se varijable okoline i putanje podesile za CD, a ne za sustav. Naredba koju je potrebno za to izvršiti iz komandne linije je: `cmdenv.bat`.



Slika 10: Helix-ova komandna linija

Uz određene alate s grafičkim sučeljem koji su raspoloživi za izvršavanje kroz komandnu liniju (Windows Forensic Toolchest – wft, Incident Response Collection Report - ircr, First Responder's Evidence Disk – fred, First Responder Utility - fruc, Security Reports – secreport) raspoloživi su i ostali programi koji se također pokreću preko komandne linije:

- 2hash-v0-2w9x i 2hash-v0-2wxp – programi za istovremeno računanje MD5 i SHA1 sažetaka (Windows 9x i XP),
- AccessEnum – alat za pregled datotečnog sustava i sigurnosnih postavki Windows registra,
- AFind – program za pronalaženje zadnjeg pristupanja NTFS datotečnom sustavu,
- Attacker – program za „prisluškivanje" TCP/UDP portova,
- Audited – pronalazi datoteke kojima je pristupano na NTFS datotečnom sustavu,
- Autoruns – prikazuje programe koji su konfigurirani na način da se pokreću tijekom podizanja sustava ili prijavljivanja korisnika,
- Autorunsc – komandno-linijska inačica Autoruns programa,
- Bintext – pretraživač tekstualnih datoteka,
- Bopping – program za izvršavanje `ping` naredbe prema Back Orifice poslužitelju,
- browselist – prikazuje računala na mreži i njihovu ulogu,
- CIScan – identificira potencijalno ranjive Cisco uređaje,
- cmdline – prikazuje procese, ID-ove procesa, putanje te parametre komandne linije,
- cryptcat – inačica netcat mrežnog analizatora nadograđen s *twofish* enkripcijom,
- DACLchk – snima zapise iz registra te ih sortira po vremenu,
- Datetime – prikazuje sistemsko vrijeme i datum,
- dd – duplikator diskova za Unix,

- DiskView – prikazuje grafičku mapu diska,
- DSScan – skenira višestruke raspone IP adresa u potrazi za ranjivim računalima,
- dumpuser – sprema korisnička imena i informacije,
- EFSDUMP – sprema informacije o Win2k kriptiranim datotekama,
- efsview – prikazuje korisnike koji imaju obični ključ za dekripciju za EFS (eng. *Encrypting File System*) kriptirane datoteke,
- etherchange – program za promjenu mrežne adrese ili mrežnog adaptera u Windows sustavima,
- filehasher – računa MD5 ili SHA sažetak za datoteku,
- Filemon – nadgleda i prikazuje aktivnost datotečnog sustava u realnom vremenu,
- FileStat – prikazuje za datoteku alocirani diskovni prostor,
- Filewatch – prikazuje različite informacije o datotekama (koje datoteke su nove, koje nedostaju i sl.),
- foremost – program koji obnavlja datoteke na temelju njihovih zaglavlja i drugih internih informacija,
- Fpipe – pre-usmjerivač TCP/UDP portova,
- Fport – alat za mapiranje procesa na TCP/IP portove,
- galleta – alat za analizu web kolačića Internet Explorer preglednika,
- gplist – prikazuje informacije o primijenjenim grupnim politikama,
- gsd – prikazuje DACL (eng. *Discretionary Access Control List*) za bilo koji Windos NT servis,
- Handle – grafički preglednik DLL datoteka,
- HFind – skriveni pronalazač datoteka s prikazom zadnjeg vremena pristupa,
- Hunt – brojač SMB dijeljenih blokova i pronalazač administratora,
- iplist – prebrojava IP adrese računala,
- Listdlls – ispisuje sve DLL datoteke koje se trenutno koriste,
- listmodules – prikazuje module (EXE i DLL) koji su trenutno učitani u proces,
- Livekd – prikazuje Microsoft-ov analizator jezgre sustava (*kernel debugger*),
- lns – traži NTFS nizove,
- LogonSessions – prikazuje aktivne sesije,
- lsadump2 – sprema LSA (eng. *Local Security Authority*) povjerljive informacije,
- macmatch – traži datoteke na temelju njihovog MAC vremena bez mijenjanja istih,
- md5deep – alat za računanje MD5 sažetka s mogućnošću rekurzivnog rada s direktorijima,
- md5sum – generator MD5 sažetka,
- MessengerScan – pregledava sustav tražeći ranjivosti u MS Messenger programu,
- nbname – dekodira i prikazuje NetBIOS ime prometa,
- nc – Netcat – mrežni analizator,
- NTFSINFO – prikazuje informacije za NTFS disk,
- NTLast – oporavlja informacije za prijavljivanje na sustav,
- openports – pregledava sve otvorene TCP i UDP portove,
- pasco – alat za analizu Internet Explorer preglednika,
- pdd – alat za izradu forenzičkih kopija (eng. *images*) na Palm OS platformi,
- periscope – inspektor PE (eng. *Portable Executable*) datoteka,
- pmdump – sprema sadržaj memorije procesa u datoteku,
- Procexp – prikazuje datoteke, ključeve iz registra te ostale objekte koje proces drži otvorenim,
- procinterrogate – prikazuje popis procesa, pridružene DLL datoteke i MD5 sažetak svake DDL datoteke,
- promiscdetect – provjerava ukoliko je mrežna kartica u „promiskuitetnom“ modu,
- Psexec – izvršava udaljene procese,
- Psfile – prikazuje datoteke koje su otvorene s udaljenog računala,
- Psgetsid – prikazuje SID računala ili korisnika,
- Psinfo – prikazuje ključne informacije o lokalnom ili udaljenom Windows sustavu,
- Pskill – ubija lokalni ili udaljeni proces,

- Pslist – prikazuje informacije o procesima i dretvama,
- Psloggedon – prikazuje korisnike koji su prijavljeni na sustav,
- Psloglist – preglednik log zapisa,
- Pspasswd – alat za promjenu zaporke na lokalnom sustavu,
- Psservice – preglednik i nadzornik servisa,
- Psshutdown – naredba za gašenje sustava,
- Pssuspend – naredba za zaustavljanje i nastavljanje procesa,
- pstoreview – prikazuje sadržaj zaštićene pohrane,
- Psuptime – prikazuje koliko dugo sustav radi od zadnjeg podizanja,
- pwdump2 – sprema SAM (eng. *Security Account Manager*) bazu,
- PwDump3e – dohvaća LM (eng. *LAN Manager*) ključeve-sažetke s poslužitelja,
- reg - komandno-linijski alat za manipuliranje Windows registrom,
- Regmon – prikazuje koje aplikacije pristupaju registru,
- rifiuti – program za analizu *Recycle bin* direktorija za obrisane datoteke,
- rmtshare – komandno-linijski alat koji omogućuje postavljanje i brisane udaljenih dijeljenih blokova,
- ServiceList – popis pokrenutih servisa,
- Serviselist – alat za ispitivanje stanja servisa s radne stanice ili poslužitelja,
- Sfind – alternativa find alatu, namijenjen traženju podataka,
- sha1deep – alat za izračun SHA1 sažetaka s mogućnošću rekurzivnog rada s direktorijima,
- sha256deep – alat za izračun SHA256 sažetaka s mogućnošću rekurzivnog rada s direktorijima,
- Showin – prikazuje informacije pojedinog prozora,
- sid2user – pretvara SID u User ID,
- SI – komandno-linijski preglednik portova,
- Streams – prikazuje koji NTFS sustavi imaju pridružene *stream*-ove,
- strings – alat za traženje ANSI i UNICODE nizova slova u binarnim slikama,
- tcpvcon i Tcpview – preglednici otvorenih TCP i UDP portova
- tigerdeep – alat za izračun rekurzivnog ključa za *Tiger* algoritam,
- Trout – sadrži traceroute i whois programe,
- user2sid – pretvara User ID u SID,
- UserDump – naredba komandnog retka za spremanje osnovnih informacija o korisniku,
- volume_dump – prikazuje informacije o logičkim particijama na disku,
- whirpooldeep – alat za izračun rekurzivne *whirlpool* sume,
- winfo – ispituje sustav o različitim informacijama,
- winrelay – TCP/UDP pre-usmjerivač za IPv4 i IPv6 i
- wipe – alat za sigurno brisanje datoteka.

4. Helix kao Linux operacijski sustav

Velika prednost Helix distribucije je to što se može pokretati kao samostalan Linux operacijski sustav. Time je moguće analizirati ugašena računala bez interferencije sa spremljenim informacijama. Pri tome se svi diskovi spajaju samo s opcijom čitanja kako se ne bi modificirale postojeće informacije.
U svrhu forenzičke analize, Helix raspolaže velikim brojem Linux programa i alata koji su opisani u narednim poglavljima.

4.1. Alati s grafičkim sučeljem

Odabirom Helix-ovog osnovnog izbornika pa zatim podizbornika *Forensics* moguće je pokrenuti slijedeće alate:

- Adepto – grafičko sučelje za dd/dcfldd/sdd dizajnirano s namjerom pojednostavljenja kreiranja forenzičkih bit kopija (eng. *bit images*). Program omogućuje: automatsko otkrivanje IDE i SCSI diskova, CD-ROM-ova i traka, izbor korištenja dd, dcfldd ili sdd alata, provjeru originala i kopije pomoću MD5 i SHA1 sažetaka, kompresiju i de-kompresiju kopija

gzip i bzip2 algoritmima, spremanje kopije na mrežu preko netcat/cryptcat ili Samba, dijeljenje kopije na manje dijelove te detaljno logiranje aktivnosti.

- AIR (eng. *Automated Image and Restore*) – grafičko sučelje za dd i dcfldd naredbe dizajnirano s namjerom jednostavnijeg kreiranja forenzičkih bit kopija. Program omogućuje iste funkcionalnosti kao i prethodno opisni Adepto.
- EnCase Linen Acquisition Tool – alat za prihvaćanje podataka s drugih uređaja.
- Retriever - alat za traženje video i foto datoteka, ali i općenito pretraživanje montiranih diskova. Nakon skeniranja montiranog diska program može sve pronađene datoteke prebaciti na USB ili lokalni disk ili ih otvoriti za pregledavanje.
- Autopsy – ovaj alat je grafičko sučelje za komandno-linijske alate iz paketa *The Sleuth Kit*. Zajedno mogu analizirati Windows i UNIX diskove te datotečne sustave (NTFS, FAT, UFS1/2, Ext2/3). Diskove je moguće analizirati na upaljenom sustavu, ali i na posebnom sustavu predviđenom za analizu.
- pyFlag (eng. *Python Forensic and Log Analysis GUI*) - alat namijenjen pretraživanju i analiziranju log datoteka korištenjem web sučelja. PyFlag koristi bazu podataka kako bi spremio informacije iz log zapisa te na taj način osigurao brzo pretraživanje i analiziranje.
- Regviewer – preglednik Windows registar datoteka. Program nije ovisan o nijednoj platformi pa omogućuje i pregled Windows registar datoteka iz *nix sustava.
- Hexeditor (GHex) – jednostavni binarni editor. Program omogućuje pregledavanje i editiranje binarnih datoteka u ASCII i HEX formatu.
- Xfce Diff – grafičko sučelje za GNU diff i patch naredbe. Pomoću ovog alata moguće je vrlo lako uspoređivati datoteke ili direktorije. Također je moguće izraditi zakrpe za razlike između pojedinih direktorija.
- xhfs – je grafičko sučelje za pregledavanje i kopiranje datoteka na HFS (Macintosh) formatiranim diskovima.

U podizborniku *Incident response* dostupni su alati:

- Ethereal – alat otvorenog koda za pregledavanje mrežnog prometa. Koristi se za ispitivanje, analizu, razvoj programa i protokola i edukaciju. Program može primati podatke izravno s mreže ili iz datoteke u koju su spremljeni. Podaci mogu biti primani s Ethernet, FDDI, PPP, Token-Ringa, IEEE 802.11 i drugih mreža. Primljene podatke moguće je pregledavati iz grafičkog sučelja ili preko TTY (eng. *Telecommunications Device for the Deaf*) moda - „Tethereal".
- F-prot (*F-Prot Antivirus for Linux*) – program koji je posebno razvijen kako bi učinkovito eliminirao viruse koji prijete radnim stanicama na Linux operacijskim sustavima. Pruža potpunu zaštitu od makro virusa i ostalih zloćudnih programa poput trojanaca. Program je u mogućnosti otkriti preko 200.000 virusa i zloćudnih programa. Također je dostupna i komandno-linijska inačica.
- ClamAV – antivirusno rješenje za UNIX. Dizajniran je za pregledavanje elektroničke pošte na poslužiteljima. Program pruža fleksibilni servis (eng. *daemon*), komandno-linijski skener, i napredni alat za automatsko ažuriranje baze podataka o virusima preko Interneta.

4.2. Alati komandne linije

Osim alata dostupnih iz grafičkog sučelja, Helix Linux sadrži mnoštvo alata dostupnih iz komandne linije. To su:

- 2hash – alat za paralelno izračunavanje MD5 i SHA1 sažetaka,
- bmap – program za spremanje, otkrivanje i brisanje podataka iz praznog prostora datoteke,
- chaosreader – aplikacija za otkrivanje tcpdump logova i dohvat podataka,
- chkrootkit – alat za otkrivanje *rootkit*-ova,
- chntpw – program za resetiranje zaporki za korisničke račune na Windows NT, 2000 i XP operacijskim sustavima,
- dcfldd – unaprijeđena inačica GNU dd alata za kreiranje kopija (eng. *image*) diskova,
- e2recover – alat za povrat izbrisanih datoteka na Ext2 datotečnom sustavu,
- fatback – alat za povrat izbrisanih datoteka na FAT12/16/32 datotečnim sustavima,

- faust.pl – skripta za analizu datoteka nađenih nakon upada na računalo,
- fenris – grafički analizator (eng. *debugger*) i obratni prevodilac (eng. *decompiler*),
- foremost – program za oporavak datoteka na temelju njihovog zaglavlja i unutarnje strukture,
- f-prot – komandno-linijska inačica F-prot antivirusnog alata za Linux,
- ftimes – alat za prikupljanje podataka o direktorijima i datotekama,
- galleta – program za analizu Internet Explorer web kolačića,
- glimpse – alat za brzo pretraživanje i indeksiranje datoteka,
- grepmail – program za pretraživanje sandučića elektroničke pošte pomoću regularnih izraza,
- logfinder.py – alat za pronalaženje datoteka koje bi mogle biti log zapisi,
- logsh – program za interaktivno pregledavanje log zapisa,
- lshw – alat za prikazivanje informacija o sklopovlju,
- mac_grab.pl – skripta za prikaz osnovnih informacija o direktorijima i datotekama,
- mac-robber – alat za prikupljanje podataka iz alociranih datoteka,
- md5deep – program za izračunavanje MD5 sažetaka s mogućnošću rekurzivnog rada na direktorijima,
- outguess – univerzalni steganografski alat,
- pasco – alat za forenzičku analizu Internet Explorer preglednika,
- rifiuti – program za analizu *Recycle Bin* direktorija na Windows sustavima,
- rkhunter – alat za otkrivanje *rootkit*-ova,
- scalpel – program za otkrivanje datoteka na temelju zaglavlja,
- sdd – poboljšana inačica dd alata,
- sha1deep i sha256deep – programi za računanje SHA1 i SHA256 sažetka s mogućnošću rekurzivnog rada na direktorijima,
- stegdetect – alat za automatsko pronalaženje steganografskih sadržaja u slikama i
- wipe – alat za sigurno brisanje datoteka.

5. Zaključak

Helix forenzička distribucija pruža odličan spoj malih sistemskih zahtjeva i velikog broja alata za prikupljanje i analiziranje podataka potrebnih za forenzičku analizu. Iako na CD-u postoji veliki broj forenzičkih alata, za njihovo funkcionalno korištenje potrebno je veliko sistemsko predznanje. Ipak, Helix distribucija raspolaže i upute u kojima se nalaze objašnjeni svi alati te njihovo korištenje, ali i osnove forenzičke analize.

Opcija pokretanja Helix distribucije kao zasebne aplikacije na Windows sustavima, kao i opcija pokretanja Helix distribucije u obliku samostalnog Linux operacijskog sustava, omogućavaju administratorima ispitivanje kako upaljenih Windows sustava koji se ne smiju gasiti, tako i ugašenih sustava koji se ne smiju paliti.

Potrebno je naglasiti da je Helix distribucija u potpunosti besplatna te da je većina programa sadržanih u njoj otvorenog koda.

6. Reference

[1] Helix distribucija, http://www.e-fense.com/helix/, kolovoz, 2006.

[2] Dokumentacija za korištenje Helix distribucije, http://www.e-fense.com/helix/Docs/Helix0307.pdf, kolovoz, 2006.

[3] Dokumentacija za korištenje Xfce grafičkog okruženja, http://www.xfce.org/documentation/docs-4.2/xfce4-use.html, kolovoz, 2006.

[4] Knoppix distribucija, http://www.knoppix.net, kolovoz 2006.