Current computer Forensic tools

- Computer forensics tools are constantly being developed, updated, patched, and revised. Therefore, checking vendors’ Web sites routinely to look for new features and improvements is important.
- Before purchasing any forensics tools, consider whether the tool can save you time during investigations and whether that time savings affects the reliability of data you recover.

Evaluating Computer Forensics Tool Needs

Some questions to ask when evaluating computer forensic tools:

- On which OS does the forensics tool run?
- Is the tool versatile? For example, does it work in Windows 98, XP, and Vista and produce the same results in all three OSs?
- Can the tool analyze more than one file system, such as FAT, NTFS, and Ext2fs?
- Can a scripting language be used with the tool to automate repetitive functions and tasks?
- Does the tool have any automated features that can help reduce the time needed to analyze data?
- What is the vendor's reputation for providing product support?

…….

- When you search for tools, keep in mind what file types you’ll be analyzing.
- For example, if you need to analyze Microsoft Access databases, look for a product designed to read these files.
- If you’re analyzing e-mail messages, look for a forensics tool capable of reading e-mail content.

Tasks Performed by Computer Forensics Tools

- All computer forensics tools, both hardware and software, perform specific functions. These functions are grouped into five major categories.
- Acquisition
- Validation and discrimination
- Extraction
- Reconstruction
- Reporting

Acquisition

- Acquisition, the first task in computer forensics investigations, is making a copy of the original drive.
- Physical data copy
- Logical data copy
- Data acquisition format
- Command-line acquisition
- GUI acquisition
- Remote acquisition
- Verification

……..

- Some computer forensics software suites, such as AccessData FTK and EnCase, provide separate tools for acquiring an image.
- However, some investigators opt to use hardware devices, such as the Logicube Talon, VOOM HardCopy 3, or ImageMASSter Solo III Forensic unit from Intelligent Computer Solutions, Inc., for acquiring an image.
- These hardware devices have their own built-in software for data acquisition.
- No other device or program is needed to make a duplicate drive; however, you still need forensics software to analyze the data.

………

- Two types of data-copying methods are used in software acquisitions:
- physical copying of the entire drive and
- logical copying of a disk partition.
- The situation dictates whether you make a physical or logical acquisition

………

- All computer forensics acquisition tools have a method for verification of the data-copying process that compares the original drive with the image.
- For example, EnCase prompts you to obtain the MD5 hash value of acquired data,
- FTK validates MD5 and SHA-1 hash sets during data acquisition, and Safe Back runs an SHA-256 hash while acquiring data.
- Hardware acquisition tools, such as Image MASSter Solo, can perform simultaneous MD5 and CRC-32 hashing during data acquisition.
- Whether you choose a software or hardware solution for your acquisition needs, make sure the tool has a hashing function for verification purposes.

Validation and Discrimination

- Two issues in dealing with computer evidence are critical.
- First is ensuring the integrity of data being copied—the validation process.
- Second is the discrimination of data, which involves sorting and searching through all investigation data.
- Many forensics software vendors offer three methods for discriminating data values.

……….

- Hashing
- Filtering
- Analyzing file headers
- Validating data is done by obtaining hash values.This unique hexadecimal value for data, used to make sure the original data hasn’t changed.

……

- The primary purpose of data discrimination is to remove good data from suspicious data.
- Good data consists of known files, such as OS files and common programs (Microsoft Word, for example).
- The National Software Reference Library (NSRL) has compiled a list of known file hashes for a variety of OSs, applications, and images.

Extraction

- The extraction function is the recovery task in a computing investigation and is the most challenging of all tasks to master.
- Recovering data is the first step in analyzing an investigation's data.
- The following sub functions of extraction are used in investigations.
- Data viewing
- Keyword searching
- Decompressing
- Carving
- Decrypting
- Bookmarking

- Many computer forensics tools include a data-viewing mechanism for digital evidence.
- Tools such as ProDiscover, X-Ways Forensics, FTK, EnCase, SMART, ILook, and others offer several ways to view data, including logical drive structures, such as folders and files.

……..

- A common task in computing investigations is searching for and recovering key data facts.
- Computer forensics programs have functions for searching for keywords of interest to the investigation. Using a keyword search speeds up the analysis process for investigators.
- With some tools, you can set filters to select the file types to search, such as searching only PDF documents.
- Another function in some forensics tools is indexing all words on a drive.
- X-Ways Forensics and FTK 1.6x and earlier offer this feature, using the binary index (Btree) search engine from dtSearch.

Reconstruction

- The purpose of having a reconstruction feature in a forensics tool is to re-create a suspect drive to show what happened during a crime or an incident.

- Another reason for duplicating a suspect drive is to create a copy for other computer investigators, who might need a fully functional copy of the drive so that they can perform their own acquisition, test, and analysis of the evidence.

- These are the sub functions of reconstruction:
- Disk-to-disk copy
- Image-to-disk copy
- Partition-to-partition copy
- Image-to-partition copy

….

- There are several ways to re-create an image of a suspect drive. Under ideal circumstances, the best and most reliable method is obtaining the same make and model drive as the suspect drive,
- If the suspect drive has been manufactured recently, locating an identical drive is fairly easy.
- A drive manufactured three months ago might be out of production and unavailable for sale, which makes locating identical older drives more difficult.

- The simplest method of duplicating a drive is using a tool that makes a direct disk-to-disk copy from the suspect drive to the target drive.
- One free tool is the UNIX/Linux dd command, but it has a major disadvantage:
- The target drive being written to must be identical to the original (suspect) drive, with the same cylinder, sector, and track count.

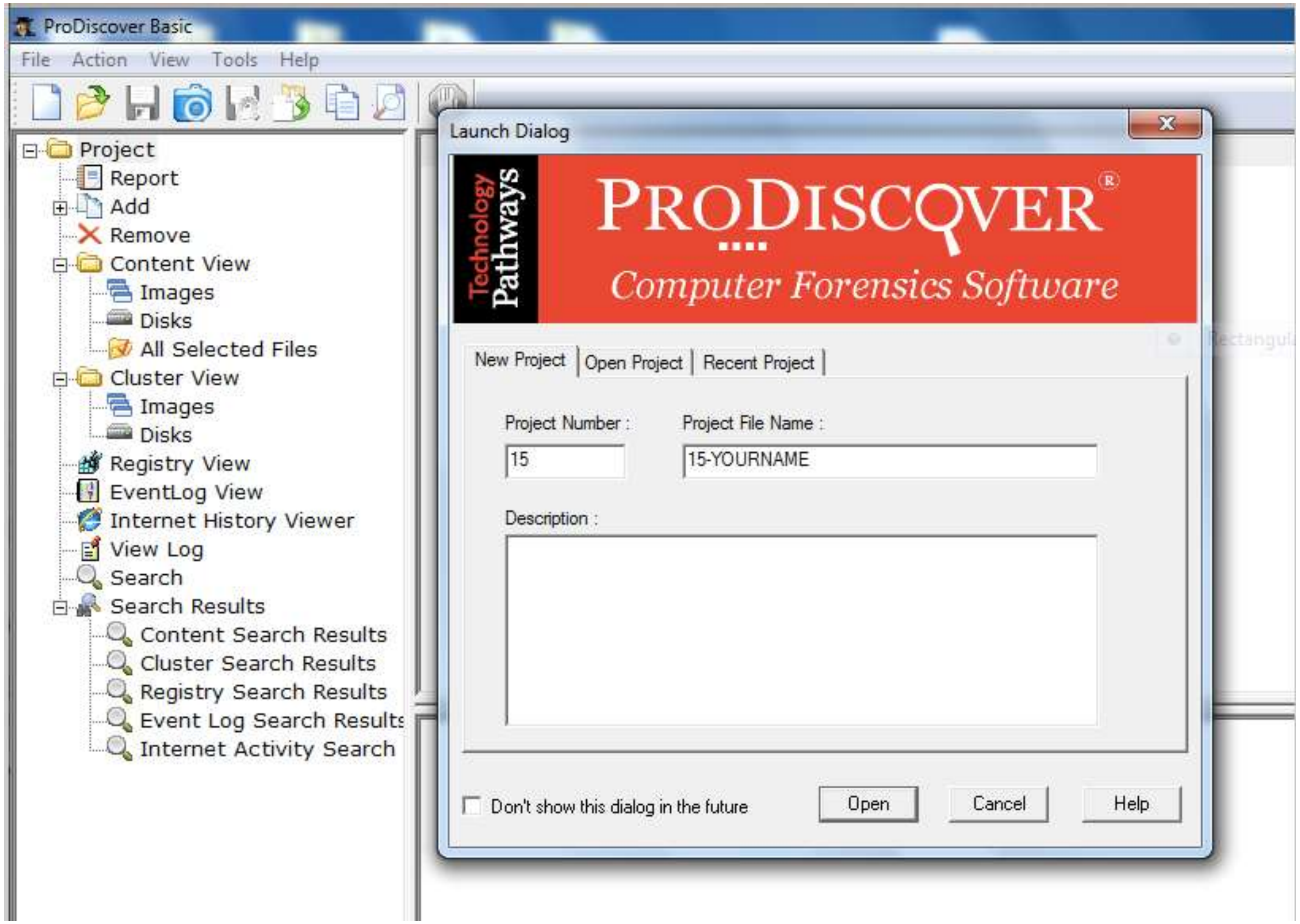
……….

- For a disk-to-disk copy, both hardware and software duplicators are available; hardware duplicators are the fastest way to copy data from one disk to another.
- Hardware duplicators, such as Logicube Talon, Logicube Forensic MD5, and ImageMASSter Solo III Forensics
- Hard Drive Duplicator, adjust the target drive’s geometry to match the suspect drive’s cylinder, sectors, and tracks.

…………

- For image-to-disk and image-to-partition copies, many more tools are available, but they are considerably slower in transferring data.
- The following are some tools that perform an image-to-disk copy:
- SafeBack
- SnapBack
- EnCase
- FTK Imager
- ProDiscover
- X-Ways Forensics

Pro discover



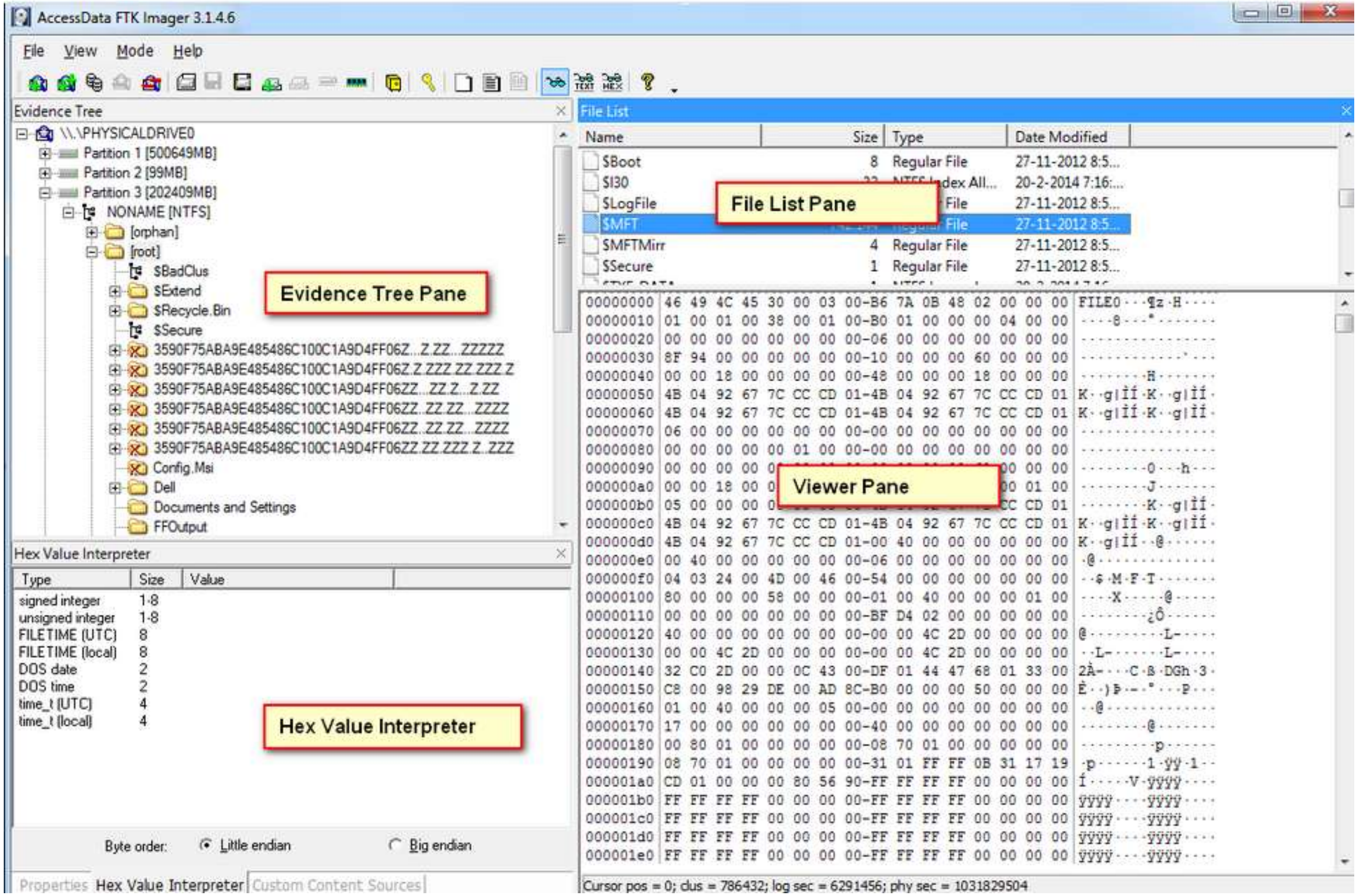
Project Number : 15

Project File Name : 15-YOURNAME

Description :

□ Don't show this dialog in the future

FTk imager



Evidence Tree

```
\\.\PHYSICALDRIVE0
    Partition 1 [500649MB]
    Partition 2 [99MB]
    Partition 3 [202409MB]
        NONAME [NTFS]
            [orphan]
            [root]
                $BadClus
                $Extend
                $Recycle.Bin
                $Secure
                3590F75ABA9E485486C100C1A9D4FF06Z...Z.ZZ...ZZZZZ
                3590F75ABA9E485486C100C1A9D4FF06Z.Z.ZZZ.ZZ.ZZZ.Z
                3590F75ABA9E485486C100C1A9D4FF06ZZ...ZZ.Z...Z.ZZ
                3590F75ABA9E485486C100C1A9D4FF06ZZ..ZZ.ZZ...ZZZZ
                3590F75ABA9E485486C100C1A9D4FF06ZZ..ZZ.ZZ...ZZZZ
                3590F75ABA9E485486C100C1A9D4FF06ZZ.ZZ.ZZZ.Z..ZZZ
                Config.Msi
                Dell
                Documents and Settings
                FFOutput
```

File List

Name	Size	Type	Date Modified
$Boot	8	Regular File	27-11-2012 8:5...
$I30		dex All...	20-2-2014 7:16:...
$LogFile		File	27-11-2012 8:5...
$MFT		File	27-11-2012 8:5...
$MFTMirr	4	Regular File	27-11-2012 8:5...
$Secure	1	Regular File	27-11-2012 8:5...

```
00000000 46 49 4C 45 30 00 03 00-B6 7A 0B 48 02 00 00 00 FILE0···¶z·H····
00000010 01 00 01 00 38 00 01 00-B0 01 00 00 00 04 00 00 ····8···°·······
00000020 00 00 00 00 00 00 00 00-06 00 00 00 00 00 00 00 ················
00000030 8F 94 00 00 00 00 00 00-10 00 00 00 60 00 00 00 ············`···
00000040 00 00 18 00 00 00 00 00-48 00 00 00 18 00 00 00 ········H·······
00000050 4B 04 92 67 7C CC CD 01-4B 04 92 67 7C CC CD 01 K··g|ÌÍ·K··g|ÌÍ·
00000060 4B 04 92 67 7C CC CD 01-4B 04 92 67 7C CC CD 01 K··g|ÌÍ·K··g|ÌÍ·
00000070 06 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000080 00 00 00 00 01 00 00-00 00 00 00 00 00 00 00 00 ················
00000090 00 00 00 00 0                          00 00 00 ········0···h···
000000a0 00 00 18 00 0                          00 01 00 ········J·······
000000b0 05 00 00 00 0                          CC CD 01 ········K··g|ÌÍ·
000000c0 4B 04 92 67 7C CC CD 01-4B 04 92 67 7C CC CD 01 K··g|ÌÍ·K··g|ÌÍ·
000000d0 4B 04 92 67 7C CC CD 01-00 40 00 00 00 00 00 00 K··g|ÌÍ··@······
000000e0 00 40 00 00 00 00 00 00-06 00 00 00 00 00 00 00 ·@··············
000000f0 04 03 24 00 4D 00 46 00-54 00 00 00 00 00 00 00 ··$·M·F·T·······
00000100 80 00 00 00 58 00 00 00-01 00 40 00 00 00 01 00 ····X·····@·····
00000110 00 00 00 00 00 00 00 00-BF D4 02 00 00 00 00 00 ········¿Ô······
00000120 40 00 00 00 00 00 00 00-00 00 4C 2D 00 00 00 00 @·········L-····
00000130 00 00 4C 2D 00 00 00 00-00 00 4C 2D 00 00 00 00 ··L-······L-····
00000140 32 C0 2D 00 00 0C 43 00-DF 01 44 47 68 01 33 00 2À-···C·ß·DGh·3·
00000150 C8 00 98 29 DE 00 AD 8C-B0 00 00 00 50 00 00 00 È··)Þ·-·°···P···
00000160 01 00 40 00 00 00 05 00-00 00 00 00 00 00 00 00 ··@·············
00000170 17 00 00 00 00 00 00 00-40 00 00 00 00 00 00 00 ········@·······
00000180 00 80 01 00 00 00 00 00-08 70 01 00 00 00 00 00 ·········p······
00000190 08 70 01 00 00 00 00 00-31 01 FF FF 0B 31 17 19 ·p······1·ÿÿ·1··
000001a0 CD 01 00 00 00 80 56 90-FF FF FF FF 00 00 00 00 Í·····V·ÿÿÿÿ····
000001b0 FF FF FF FF 00 00 00 00-FF FF FF FF 00 00 00 00 ÿÿÿÿ····ÿÿÿÿ····
000001c0 FF FF FF FF 00 00 00 00-FF FF FF FF 00 00 00 00 ÿÿÿÿ····ÿÿÿÿ····
000001d0 FF FF FF FF 00 00 00 00-FF FF FF FF 00 00 00 00 ÿÿÿÿ····ÿÿÿÿ····
000001e0 FF FF FF FF 00 00 00 00-FF FF FF FF 00 00 00 00 ÿÿÿÿ····ÿÿÿÿ····
```

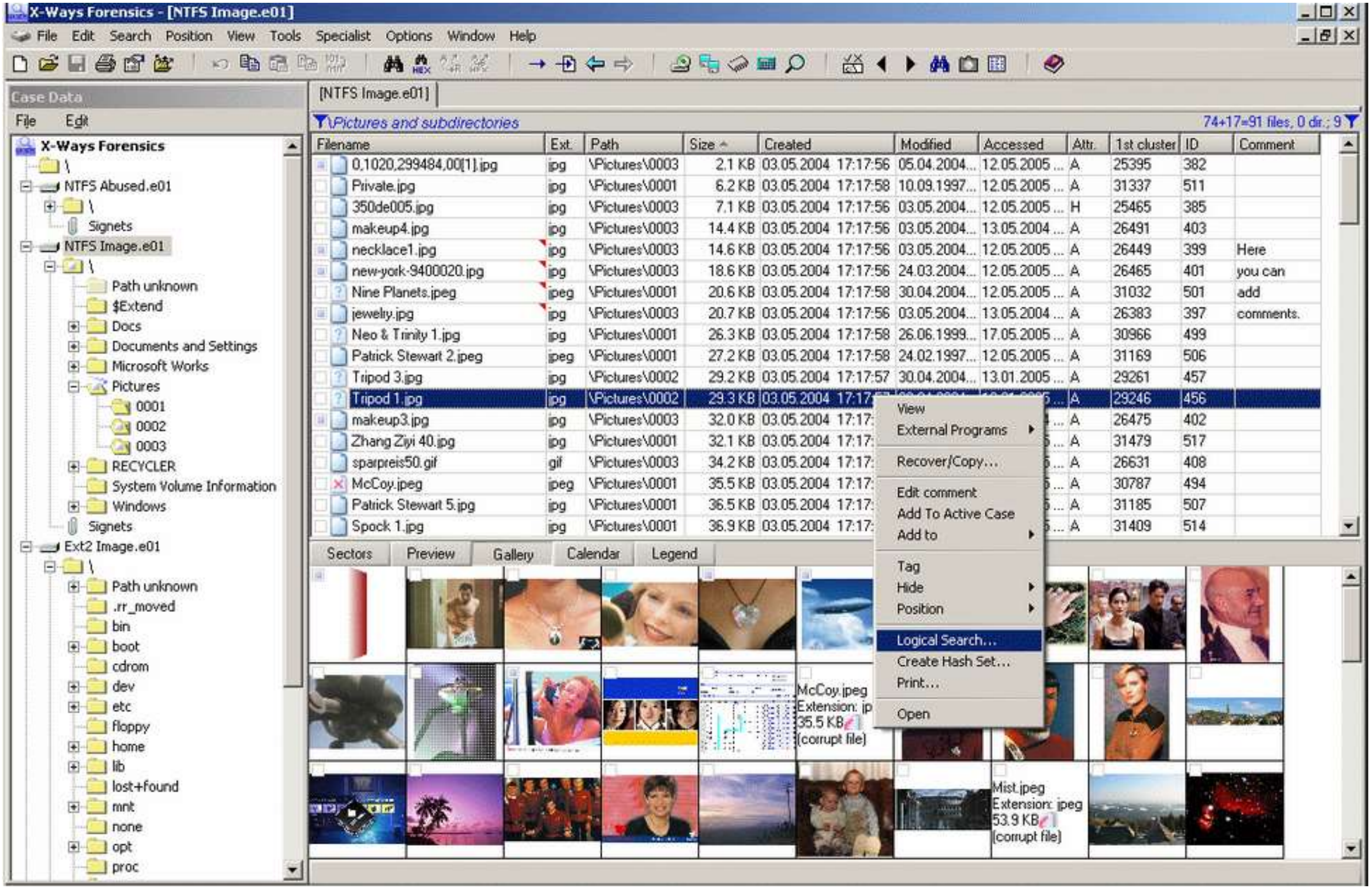
Cursor pos = 0; clus = 786432; log sec = 6291456; phy sec = 1031829504

Hex Value Interpreter

Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (UTC)	8	
FILETIME (local)	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

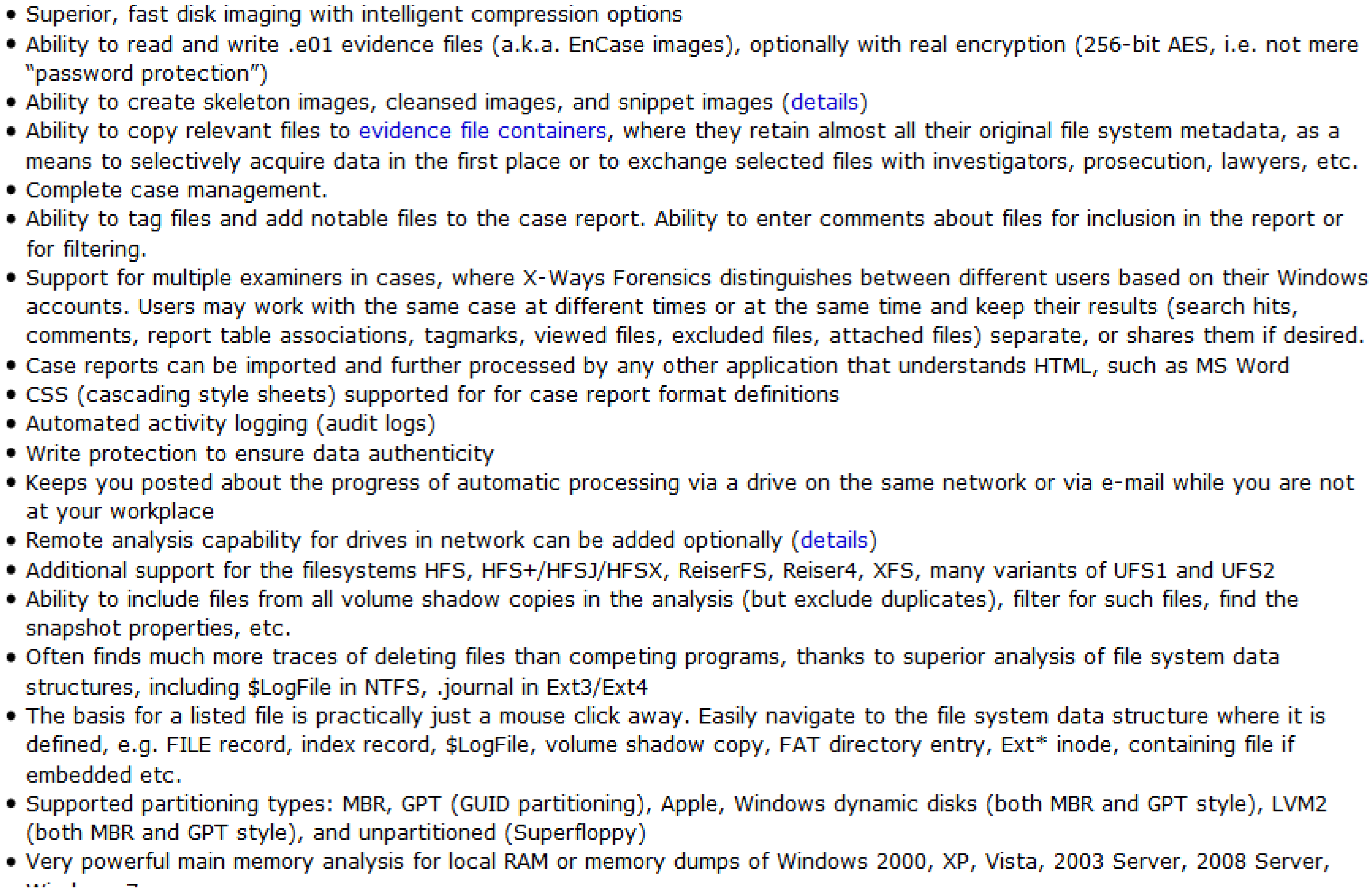
Byte order: ● Little endian ○ Big endian

X-ways forensics



Filename	Ext.	Path	Size	Created	Modified	Accessed	Attr.	1st cluster	ID	Comment
0,1020,299484,00[1].jpg	jpg	\Pictures\0003	2.1 KB	03.05.2004 17:17:56	05.04.2004...	12.05.2005 ...	A	25395	382	
Private.jpg	jpg	\Pictures\0001	6.2 KB	03.05.2004 17:17:58	10.09.1997...	12.05.2005 ...	A	31337	511	
350de005.jpg	jpg	\Pictures\0003	7.1 KB	03.05.2004 17:17:56	03.05.2004...	12.05.2005 ...	H	25465	385	
makeup4.jpg	jpg	\Pictures\0003	14.4 KB	03.05.2004 17:17:56	03.05.2004...	13.05.2004 ...	A	26491	403	
necklace1.jpg	jpg	\Pictures\0003	14.6 KB	03.05.2004 17:17:56	03.05.2004...	12.05.2005 ...	A	26449	399	Here
new-york-9400020.jpg	jpg	\Pictures\0003	18.6 KB	03.05.2004 17:17:56	24.03.2004...	12.05.2005 ...	A	26465	401	you can
Nine Planets.jpeg	jpeg	\Pictures\0001	20.6 KB	03.05.2004 17:17:58	30.04.2004...	12.05.2005 ...	A	31032	501	add
jewelry.jpg	jpg	\Pictures\0003	20.7 KB	03.05.2004 17:17:56	03.05.2004...	13.05.2004 ...	A	26383	397	comments.
Neo & Trinity 1.jpg	jpg	\Pictures\0001	26.3 KB	03.05.2004 17:17:58	26.06.1999...	17.05.2005 ...	A	30966	499	
Patrick Stewart 2.jpeg	jpeg	\Pictures\0001	27.2 KB	03.05.2004 17:17:58	24.02.1997...	12.05.2005 ...	A	31169	506	
Tripod 3.jpg	jpg	\Pictures\0002	29.2 KB	03.05.2004 17:17:57	30.04.2004...	13.01.2005 ...	A	29261	457	
Tripod 1.jpg	jpg	\Pictures\0002	29.3 KB	03.05.2004 17:17:		5 ...	A	29246	456	
makeup3.jpg	jpg	\Pictures\0003	32.0 KB	03.05.2004 17:17:		4 ...	A	26475	402	
Zhang Ziyi 40.jpg	jpg	\Pictures\0001	32.1 KB	03.05.2004 17:17:		5 ...	A	31479	517	
sparpreis50.gif	gif	\Pictures\0003	34.2 KB	03.05.2004 17:17:		5 ...	A	26631	408	
McCoy.jpeg	jpeg	\Pictures\0001	35.5 KB	03.05.2004 17:17:		5 ...	A	30787	494	
Patrick Stewart 5.jpg	jpg	\Pictures\0001	36.5 KB	03.05.2004 17:17:		5 ...	A	31185	507	
Spock 1.jpg	jpg	\Pictures\0001	36.9 KB	03.05.2004 17:17:		5 ...	A	31409	514	

X-ways forensics



- Superior, fast disk imaging with intelligent compression options
- Ability to read and write .e01 evidence files (a.k.a. EnCase images), optionally with real encryption (256-bit AES, i.e. not mere "password protection")
- Ability to create skeleton images, cleansed images, and snippet images (details)
- Ability to copy relevant files to evidence file containers, where they retain almost all their original file system metadata, as a means to selectively acquire data in the first place or to exchange selected files with investigators, prosecution, lawyers, etc.
- Complete case management.
- Ability to tag files and add notable files to the case report. Ability to enter comments about files for inclusion in the report or for filtering.
- Support for multiple examiners in cases, where X-Ways Forensics distinguishes between different users based on their Windows accounts. Users may work with the same case at different times or at the same time and keep their results (search hits, comments, report table associations, tagmarks, viewed files, excluded files, attached files) separate, or shares them if desired.
- Case reports can be imported and further processed by any other application that understands HTML, such as MS Word
- CSS (cascading style sheets) supported for for case report format definitions
- Automated activity logging (audit logs)
- Write protection to ensure data authenticity
- Keeps you posted about the progress of automatic processing via a drive on the same network or via e-mail while you are not at your workplace
- Remote analysis capability for drives in network can be added optionally (details)
- Additional support for the filesystems HFS, HFS+/HFSJ/HFSX, ReiserFS, Reiser4, XFS, many variants of UFS1 and UFS2
- Ability to include files from all volume shadow copies in the analysis (but exclude duplicates), filter for such files, find the snapshot properties, etc.
- Often finds much more traces of deleting files than competing programs, thanks to superior analysis of file system data structures, including $LogFile in NTFS, .journal in Ext3/Ext4
- The basis for a listed file is practically just a mouse click away. Easily navigate to the file system data structure where it is defined, e.g. FILE record, index record, $LogFile, volume shadow copy, FAT directory entry, Ext* inode, containing file if embedded etc.
- Supported partitioning types: MBR, GPT (GUID partitioning), Apple, Windows dynamic disks (both MBR and GPT style), LVM2 (both MBR and GPT style), and unpartitioned (Superfloppy)
- Very powerful main memory analysis for local RAM or memory dumps of Windows 2000, XP, Vista, 2003 Server, 2008 Server, Windows 7

Reporting

- To complete a forensics disk analysis and examination, you need to create a report.
- Before Windows forensics tools were available, this process required copying data from a suspect drive and extracting the digital evidence manually.
- The investigator then copied the evidence to a separate program, such as a word processor, to create a report.

- Newer Windows forensics tools can produce electronic reports in a variety of formats, such as word processing documents, HTML Web pages, or Acrobat PDF files.

These are the sub functions of the reporting function:

- Log reports
- Report generator

……..

- Many forensics tools, such as FTK, ILook, and X-Ways Forensics, can produce a log report that records activities the investigator performed.
- Then a built-in report generator is used to create a report in a variety of formats.
- The following tools are some that offer report generators displaying bookmarked evidence:
- EnCase
- FTK
- ILook
- X-Ways Forensics
- ProDiscover

- The log report can be added to your final report as additional documentation of the steps you took during the examination, which can be useful if repeating the examination is necessary.

Computer Forensics Software Tools

- Whether you use a suite of tools or a task-specific tool, you have the option of selecting one that enables you to analyze digital evidence through the command line or in a GUI.
- The following sections explore some options for command-line and GUI tools in both Windows and UNIX/Linux.

Command-Line Forensics Tools

- The first tools that analyzed and extracted data from floppy disks and hard disks were MS-DOS tools for IBM PC file systems.
- One of the first MS-DOS tools used for computer investigations was Norton Disk Edit.
- This tool used manual processes that required investigators to spend considerable time on a typical 500 MB drive.

………

- Eventually, programs designed for computer forensics were developed for DOS, Windows, Apple, NetWare, and UNIX systems.
- Some of these early programs could extract data from slack and free disk space; others were capable only of retrieving deleted files.
- Current programs are more robust and can search for specific words or characters, import a keyword list to search, calculate hash values, recover deleted items, conduct physical and logical analyses, and more.

…..

- Some command-line forensics tools are created specifically for DOS/Windows platforms;
- others are created for Macintosh and UNIX/Linux. Because there are many different versions of UNIX and Linux, these OSs are often referred to as *nix platforms.

UNIX/Linux Forensics Tools

- The *nix platforms have long been the primary command-line OSs, but typical end users haven’t used them widely.
- However, with GUIs now available with *nix platforms, these OSs are becoming more popular with home and corporate end users.
- There are several *nix tools for forensics analysis, such as SMART, BackTrack, Autopsy with Sleuth Kit, and Knoppix-STD.

…….

- SMART SMART is designed to be installed on numerous Linux versions, including Gentoo, Fedora, SUSE, Debian, Knoppix, Ubuntu, Slackware, and more.
- You can analyze a variety of file systems with SMART;
- SMART includes several plug-in utilities. This modular approach makes it possible to upgrade SMART components easily and quickly.
- SMART can also take advantage of multithreading capabilities in OSs and hardware.

….

- Another useful option in SMART is the hex viewer. Hex values are color-coded to make it easier to see where a file begins and ends.
- SMART also offers a reporting feature. Everything you do during your investigation with SMART is logged, so you can select what you want to include in a report, such as bookmarks.

……..

- Helix One of the easiest suites to use is Helix because of its user interface. What’s unique about Helix is that you can load it on a live Windows system, Its Windows component is used for live acquisitions
- During corporate investigations, often you need to retrieve RAM and other data, such as the suspect’s user profile, from a workstation or server that can’t be seized or turned off.
- This data is extracted while the system is running and captured in its state at the time of extraction.

…….

- To do a live acquisition, insert the Helix CD into the suspect’s machine. After clicking I ACCEPT in the licensing window, you see the Helix menu.

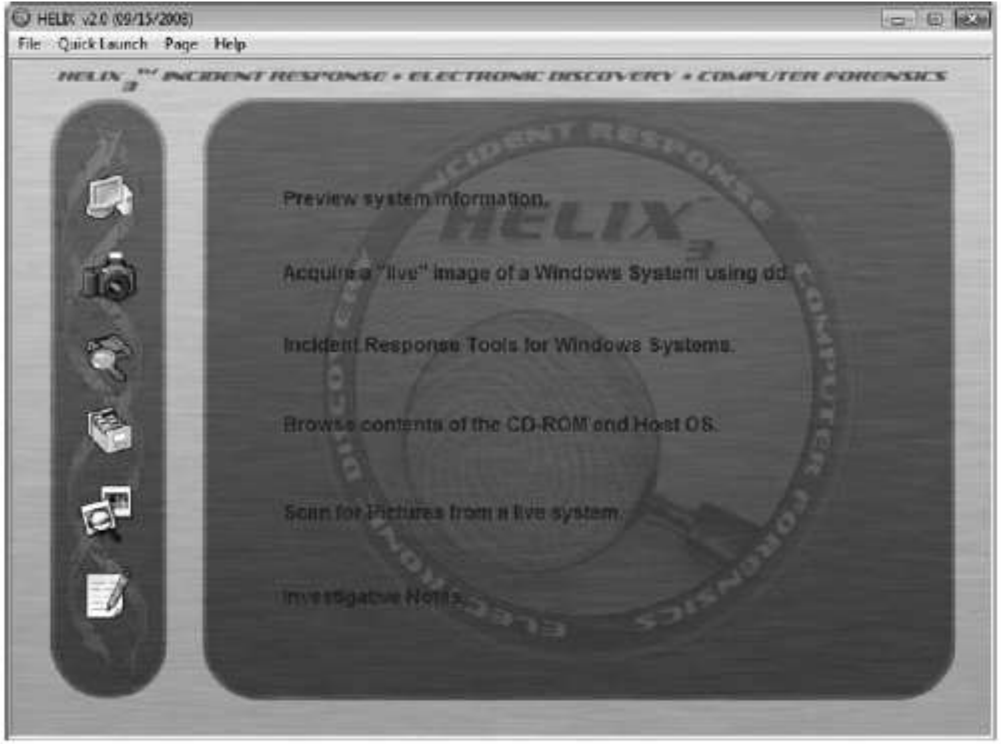

HELIX v2.0 (09/15/2008)
File Quick Launch Page Help
HELIX3 TM INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Preview system information.
Acquire a "live" image of a Windows System using dd.
Incident Response Tools for Windows Systems.
Browse contents of the CD-ROM and Host OS.
Scan for Pictures from a live system.
Investigative Notes.
HELIX3
INCIDENT RESPONSE
COMPUTER FORENSICS
ELECTRONIC DISCOVERY

Figure 7-8 The Helix menu

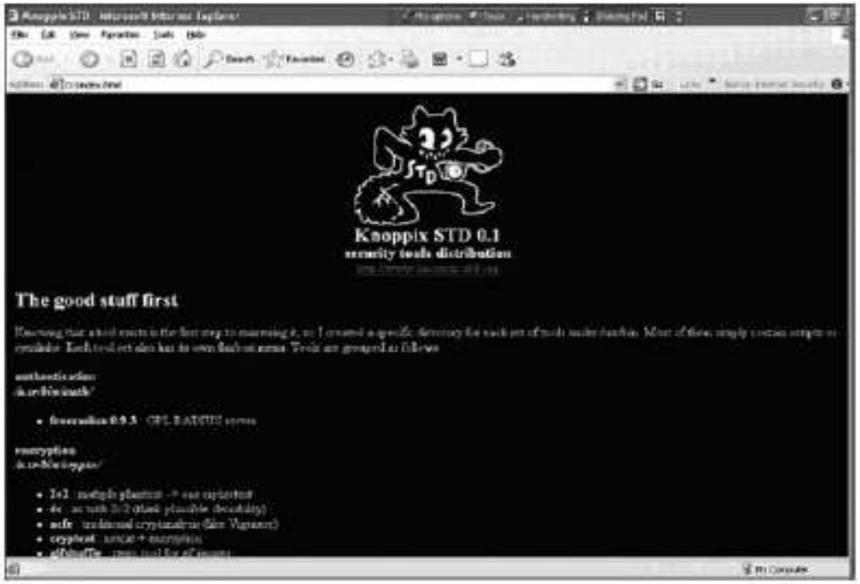
- BackTrack BackTrack is another Linux Live CD used by many security professionals and forensics investigators. It includes a variety of tools and has an easy-to-use KDE interface.
- Autopsy and Sleuth Kit Sleuth Kit is a Linux forensics tool, and Autopsy is the GUI browser interface for accessing Sleuth Kit’s tools.

…….

- Knoppix-STD Knoppix Security Tools Distribution (STD) is a collection of tools for configuring security measures, including computer and network forensics.
- Note that Knoppix- STD is forensically sound, so it doesn’t allow you to alter or damage the system you’re analyzing.
- If you boot this CD into Windows, Knoppix lists available tools. Although many of the tools have GUI interfaces, some are still command line only.

……..

- Figure 7-9 shows what you see if you load the Knoppix-STD CD in Windows.
- You can scroll through this window and see some of the available tools



KnoppixSTD - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address D:\index.html
Go Links
My Computer

Knoppix STD 0.1
security tools distribution
http://www.knoppix-std.org

The good stuff first

Knowing that a tool exists is the first step to mastering it, so I created a specific directory for each set of tools under /usr/bin. Most of these simply contain scripts or symlinks. Each tool set also has its own fluxbox menu. Tools are grouped as follows:

authentication
/usr/bin/auth/

- freeradius 0.9.3 - GPL RADIUS server

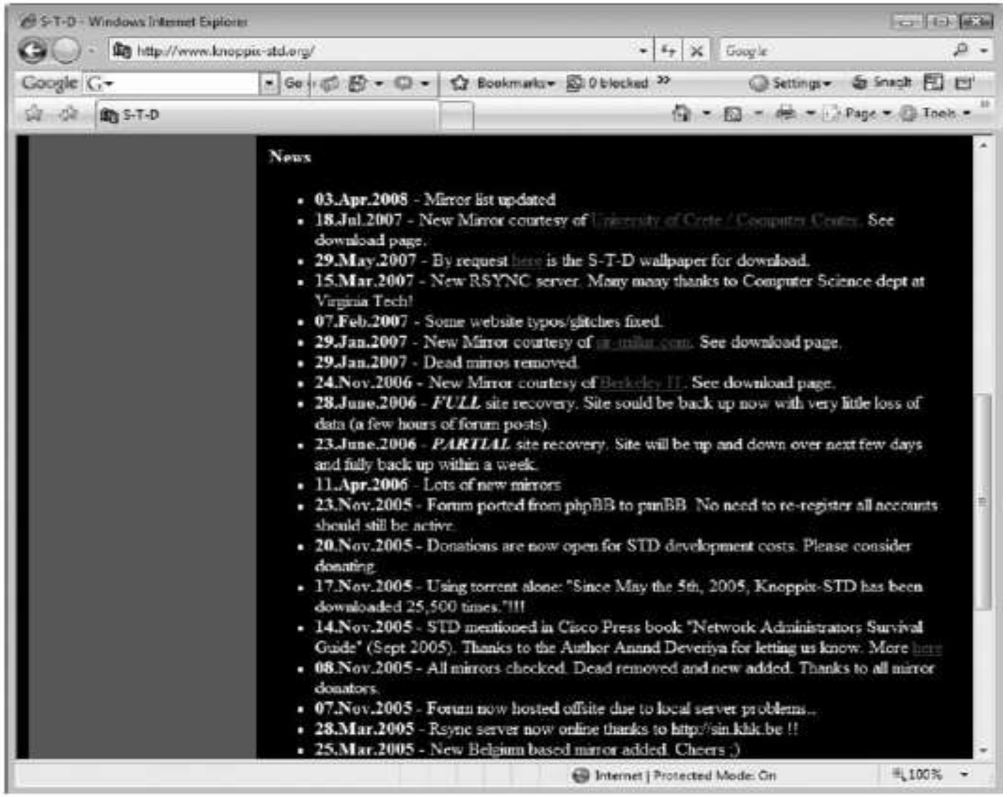
encryption
/usr/bin/crypto/

- 2c2 - multiple plaintext -> one ciphertext
- 4c - as with 2c2 (dual plausible deniability)
- acfe - traditional cryptanalysis (like Vigenere)
- cryptcat - netcat + encryption
- gifshuffle - stego tool for gif images

Figure 7-9 The Knoppix-STD information window in Windows

…

- Like Helix, Knoppix-STD is a Linux bootable CD. If you shut down Windows and reboot with the Knoppix-STD disc in the CD/DVD drive, your system boots into Linux.


S-T-D - Windows Internet Explorer
http://www.knoppix-std.org/
Google
Google G
Go
Bookmarks
0 blocked
Settings
SnagIt
S-T-D
Page
Tools
Internet | Protected Mode: On
100%

News

- **03.Apr.2008** - Mirror list updated
- **18.Jul.2007** - New Mirror courtesy of University of Crete / Computer Centre. See download page.
- **29.May.2007** - By request here is the S-T-D wallpaper for download.
- **15.Mar.2007** - New RSYNC server. Many many thanks to Computer Science dept at Virginia Tech!
- **07.Feb.2007** - Some website typos/glitches fixed.
- **29.Jan.2007** - New Mirror courtesy of [illegible]. See download page.
- **29.Jan.2007** - Dead mirros removed.
- **24.Nov.2006** - New Mirror courtesy of Berkeley II. See download page.
- **28.June.2006** - ***FULL*** site recovery. Site sould be back up now with very little loss of data (a few hours of forum posts).
- **23.June.2006** - ***PARTIAL*** site recovery. Site will be up and down over next few days and fully back up within a week.
- **11.Apr.2006** - Lots of new mirrors
- **23.Nov.2005** - Forum ported from phpBB to punBB. No need to re-register all accounts should still be active.
- **20.Nov.2005** - Donations are now open for STD development costs. Please consider donating.
- **17.Nov.2005** - Using torrent alone: "Since May the 5th, 2005, Knoppix-STD has been downloaded 25,500 times."!!!
- **14.Nov.2005** - STD mentioned in Cisco Press book "Network Administrators Survival Guide" (Sept 2005). Thanks to the Author Anand Deveriya for letting us know. More here
- **08.Nov.2005** - All mirrors checked. Dead removed and new added. Thanks to all mirror donators.
- **07.Nov.2005** - Forum now hosted offsite due to local server problems..
- **28.Mar.2005** - Rsync server now online thanks to http://sin.khk.be !!
- **25.Mar.2005** - New Belgium based mirror added. Cheers ;)

Figure 7-10 A list of forensics tools available in Knoppix-STD

Other GUI Forensics Tools

- Several software vendors have introduced forensics tools that work in Windows.
- Because GUI forensics tools don’t require the same understanding of MS-DOS and file systems as command-line tools, they can simplify computer forensics investigations.
- These GUI tools have also simplified training for beginning examiners; however, you should continue to learn about and use command-line tools because some GUI tools might miss critical evidence.

……..

- GUI tools have several advantages, such as ease of use, the capability to perform multiple tasks, and no requirement to learn older OSs.
- Their disadvantages range from excessive resource requirements (needing large amounts of RAM, for example) and producing inconsistent results because of the type of OS used, such as Windows Vista 32-bit or 64-bit systems

Computer Forensics Hardware Tools

- Hardware is hardware; whether it’s a rack-mounted server or a forensic workstation, eventually it fails.
- For this reason, you should schedule equipment replacements periodically—ideally, every 18 months if you use the hardware fulltime.
- Most computer forensics operations use a workstation 24 hours a day for a week or longer between complete shutdowns.

…………..

- You should plan your hardware needs carefully, especially if you have budget limitations.
- The longer you expect the forensic workstation to be running, the more you need to anticipate physical equipment failure and the expense of replacement equipment.

Forensic Workstations

- Many computer vendors offer a wide range of forensic workstations that you can tailor to meet your investigation needs.
- Forensic workstations can be divided into the following categories:
- Stationary workstation—A tower with several bays and many peripheral devices
- Portable workstation—A laptop computer with a built-in LCD monitor and almost as many bays and peripherals as a stationary workstation
- Lightweight workstation—Usually a laptop computer built into a carrying case with a small selection of peripheral options.

Building Your Own Workstation

- If you have the time and skill to build your own forensic workstation, you can customize it to your needs and save money, although you might have trouble finding support for problems that develop.
- For example, peripheral devices might conflict with one another, or components might fail. If you build your own forensic workstation, you should be able to support the hardware.

……

- If you decide that building a forensic workstation is beyond your skills, several vendors offer workstations designed for computer forensics, such as the F.R.E.D. unit from Digital Intelligence or the Dual Xeon Workstation from Forensic PC.
- Having a vendor-supplied workstation has its advantages.

Using a Write-Blocker

- The first item you should consider for a forensic workstation is a write-blocker.
- Write blockers protect evidence disks by preventing data from being written to them. Software and hardware write-blockers perform the same function but in a different fashion.
- Software write-blockers, such as PDBlock from Digital Intelligence, typically run in a shell mode (for example, DOS).

……..

- If you attempt to write data to the blocked drive, an alarm sounds, advising that no writes have occurred.
- With hardware write-blockers, you can connect the evidence drive to your workstation and start the OS as usual.
- Hardware write-blockers are ideal for GUI forensics tools. They prevent Windows or Linux from writing data to the blocked drive.
- Hardware write-blockers act as a bridge between the suspect drive and the forensic workstation

……

- Many vendors have developed write-blocking devices that connect to a computer through FireWire, USB 2.0, SATA, and SCSI controllers.
- Most of these write-blockers enable you to remove and reconnect drives without having to shut down your workstation, which saves time in processing the evidence drive.

Validating and Testing Forensics Software

- Using National Institute of Standards and Technology (NIST) Tools :NIST has created criteria for testing computer forensics tools, which are included in the articlen“General Test Methodology for Computer Forensic Tools”.

Testing Standards:

- Establish categories for computer forensics tools
- Identify computer forensics category requirements
- Develop test assertions
- Identify test cases
- Establish a test method
- Report test result

Using Validation Protocols

- After retrieving and examining evidence data with one tool, you should verify your results by performing the same tasks with other similar forensics tools.
- For example, after you use one forensics tool to retrieve disk data, you use another to see whether you retrieve the same information.
- Although this step might seem unnecessary, you might be asked on the witness stand “How did you verify your results?” To satisfy the need for verification, you need at least two tools to validate software or hardware upgrades.
- The tool you use to validate the results should be well tested and documented.

Computer Forensics Examination Protocol

1. First, conduct your investigation of the digital evidence with one GUI tool.
2. Then perform the same investigation with a disk editor to verify that the GUI tool is seeing the same digital evidence in the same places on the test or suspect drive’s image.
3. If a file is recovered, obtain the hash value with the GUI tool and the disk editor, and then compare the results to verify whether the file has the same value in both tools.

Computer Forensics Tool Upgrade Protocol

- In addition to verifying your results by using two disk-analysis tools, you should test all new releases and OS patches and upgrades to make sure they’re reliable and don’t corrupt evidence data.
- New releases and OS upgrades and patches can affect the way your forensics tools perform.