Overview of Computer (Digital) Forensics

CIS 3003, Introduction to Information Technology

Dr. Sheau-Dong Lang (lang@cs.ucf.edu)

What is Computer Forensics?

Computer forensics is largely a response to a demand for service from the law enforcement community [Noblett, Pollitt, and Presley]. The term "Computer Forensics" was coined in 1991 in the first training session held by the International Association of Computer Investigative Specialists (IACIS, http://www.cops.org) in Portland, Oregon [Marcella and Greenfield]. Computer forensics is “the application of science and engineering to the legal problem of digital evidence” [Sammes and Jenkinson].

- Marcella, Albert J., Jr. and Greenfield, Robert S., Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition, Chapter 17, Auerbach Publishers, 2002
- Noblett, Michael G., Pollitt, Mark M., and Presley, Lawrence A., Recovering and Examining Computer Forensic Evidence, Forensic Science Communications, Volume 2, Number 4, US Department of Justice, October 2000
- Sammes, T. and Jenkinson, B., Forensic Computing, Springer-Verlag, 2000

Roles of computer (or digital device) played in digital crime investigations:

- as the instrument used in committing a crime (an intruder or a computer virus writer using computers in illegal activities)
- as the victim (a comprised system, data stolen or deleted)
- as a container or storage warehouse for a crime (a cell phone that has pictures of a stolen car, text messages with suspects)

❑ The Digital Evidence discipline became part of the American Society of Crime Laboratory Directors/Laboratory Accreditation Board's (ASCLD/LAB) accreditation program in April 2003, see articles by John J. Barbara, Mark Pollitt, and Carrie Whitcomb discussing the efforts led by the SWGDE (Scientific Working Group on Digital Evidence)

❑ Formation of the new Digital and Multimedia Sciences Section of the American Academy of Forensic Sciences, 2/20/2008

Computer Crimes and Crime Scene Investigation:

- As personal computers and access to the Internet become more prevalent the modern society is increasingly dependent on the computer and networking technologies for storing, processing, and sharing data, and for email and message communication.
- The proliferation of computers has made computer-based systems and computer networks easy targets for criminal activities.
- *"Computer crimes were originally thought of just in the terms of hackers and virus makers, mainly due to the fact that at first only a few geeks had access to computers, but now anyone can point and click and use a computer to commit just about any crime,"* Sgt. Stenger , OCSO Computer Crime Squad

Computer (or digital) forensics involves the following steps in handling of digital evidence:

- preservation (acquiring evidence without tampering, chain of custody, transport and storage, collecting data within legal constraints)
- identification (labeling each item of evidence, bagging and tagging, identifying with case number, descriptions, date/time of collection, signatures of handlers)
- extraction (authenticating evidence using hashes, using tools and established procedures for data analysis, keyword searches, hex and graphics viewer, establishing timeline of events, corroborating evidence, who-what-when-where-why-how)
- documentation (actions taken during investigation, the findings)
- interpretation (testifying and presentation in the court, as an examiner or expert, see a recent news article)

Computer (Digital) forensics tools:

Features provided to aid in forensic examination:

- Recover previously deleted files and folders
- Recognize disk partitions and common file systems (Windows FAT and NTFS, Linux ext2 and ext3, Unix UFS)
- Carve graphics and other files of known signatures from unallocated disk clusters
- Search strings using regular expressions
- Review registry files (on Microsoft Windows systems)
- Recover user passwords
- Recover emails and instant messages (IMs)
- Provide timelines of file access activities based on date/time stamps
- Identify known files based on hash sets
- Identify artifacts specific to the operating system on disk

Host-based computer forensics vs. network forensics:

- host-based forensics deals with personal or desktop devices, small enough to be taken down and imaged for analysis
- network forensics deals with servers, company databases, network devices such as routers, firewalls, intrusion detection

Three issues involved in computer forensics investigations:

- technical (the can-we issue): are there tools to extract the necessary evidence, does the investigator have the expertise
- legal (the may-we issue): is there violation of the 4th amendment of the US Constitution which guards against unreasonable search and seizure, digital wiretapping
- ethical (the should-we issue): ethical concerns relating to the use of computer forensics include proper use of prosecutorial and police discretion (see "Computer forensics: admissibility of evidence in criminal cases" by Jerry Wegman)

Email and IM investigations:

- find email artifacts in client-based email (e.g., Outlook’s PST files, Outlook Express DBX files) and web-based email (Yahoo, Hotmail)
- use FTK or open-source tools libPST (for Outlook), Eindeutig (for Outlook Express), AOL clients (for AOL email) to reconstruct emails
- apply string searches (grep) to filter relevant emails and instant messages (IMs)
- track email origins (reading email header information)

Windows Registry Files:

- identify installed applications (date/time, configurations, deleted applications)
- identify installed malicious code (compromised systems with virus, rootkit, spyware programs)
- identify “most recently used” documents to understand recent activities on a computer
- identify USB devices connected to the computer
- use FTK registry viewer (or regedit) to view registry files

Internet Web-browsing Activity:

- Internet Explorer (IE) uses history, cookies, and temporary Internet Files (i.e. Internet cache) to save web activities
- use FTK or open-source tools pasco and galleta to view browsing activities (both pasco and galleta are available at http://sourceforge.net/docman/?group_id=78332)
- use Paraben's Netanalysis (commercial tool) for Internet cache, history, cookies, even in unallocated clusters
- two articles written by Keith J. Jones and Rohyt Belani about web browser forensics (for IE and Mozilla/Firefox history and cache files) are http://www.securityfocus.com/infocus/1827 and http://www.securityfocus.com/infocus/1832

Live system forensics and incident response:

- extract information about running applications (processes), open files, network connections, data contained in RAM
- server machines that cannot be shut down or have too much data requiring filtering from live system
- real time forensic analysis on remote systems (e.g., EnCase Enterprise edition) in corporate environments
- open-source tools Helix and FIRE provide support for live system forensics
- freeware tools that monitor processes, file and disk operations, and registry activities in real time, available at http://technet.microsoft.com/en-us/sysinternals/bb545027.aspx
- two articles (1, 2) on forensic analysis of live Linux systems

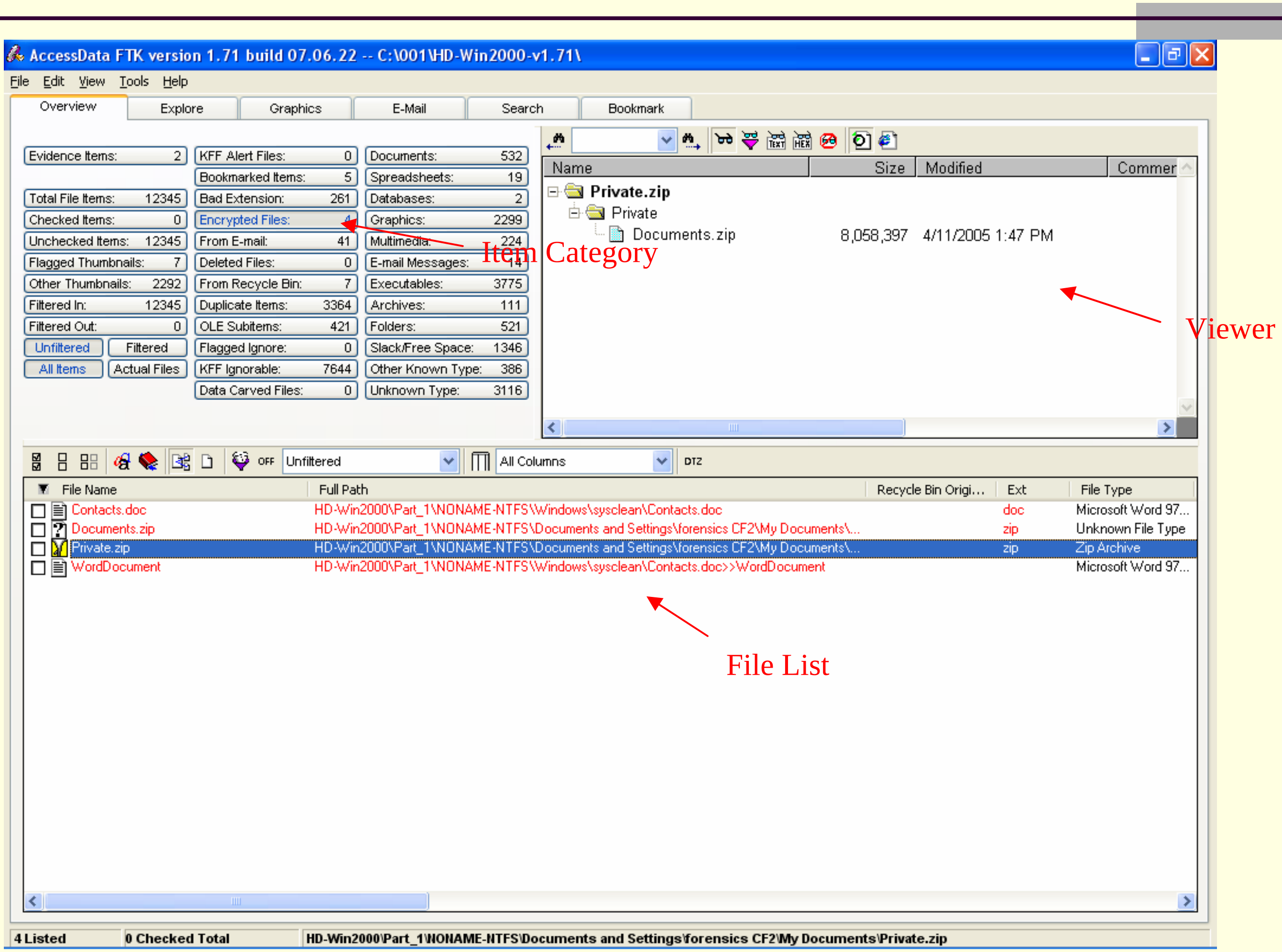
Static and dynamic analysis of unknown executables:

- malicious codes such as virus, rootkit, spyware are executable (binary) files
- string searches of executables may reveal minimum information regarding the code’s functionality
- a disassembler such as OllyDbg features an intuitive user interface, advanced code analysis capable of recognizing procedures, loops, API calls, switches, tables, constants and strings, an ability to attach to a running program, and good multi-thread support.
- a disassembler and debugger such as IDA Pro provides controlled execution and debugging of executables allowing user interactions and analysis of runtime behaviors

Data Analysis:

- Forensic examiners typically are given some background information from the investigator (case agent) – things like names, addresses, time window, types of files (spreadsheets, pictures, movies), installed applications -- that will aid the examination phase.
- Experienced examiners know where (files, folders, Windows registry) to look for relevant evidence, how to corroborate evidences, and how to get the most out of forensic tools.

AccessData's FTK:



AccessData FTK version 1.71 build 07.06.22 -- C:\001\HD-Win2000-v1.71\

Evidence Items:	2	KFF Alert Files:	0	Documents:	532
		Bookmarked Items:	5	Spreadsheets:	19
Total File Items:	12345	Bad Extension:	261	Databases:	2
Checked Items:	0	Encrypted Files:	4	Graphics:	2299
Unchecked Items:	12345	From E-mail:	41	Multimedia:	224
Flagged Thumbnails:	7	Deleted Files:	0	E-mail Messages:	14
Other Thumbnails:	2292	From Recycle Bin:	7	Executables:	3775
Filtered In:	12345	Duplicate Items:	3364	Archives:	111
Filtered Out:	0	OLE Subitems:	421	Folders:	521
		Flagged Ignore:	0	Slack/Free Space:	1346
		KFF Ignorable:	7644	Other Known Type:	386
		Data Carved Files:	0	Unknown Type:	3116

Name	Size	Modified	Commer
Private.zip			
Private			
Documents.zip	8,058,397	4/11/2005 1:47 PM	

Unfiltered

All Columns

	File Name	Full Path	Recycle Bin Origi...	Ext	File Type
□	Contacts.doc	HD-Win2000\Part_1\NONAME-NTFS\Windows\sysclean\Contacts.doc		doc	Microsoft Word 97...
□	Documents.zip	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\My Documents\...		zip	Unknown File Type
□	Private.zip	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\My Documents\...		zip	Zip Archive
□	WordDocument	HD-Win2000\Part_1\NONAME-NTFS\Windows\sysclean\Contacts.doc>>WordDocument			Microsoft Word 97...

4 Listed | 0 Checked Total | HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\My Documents\Private.zip

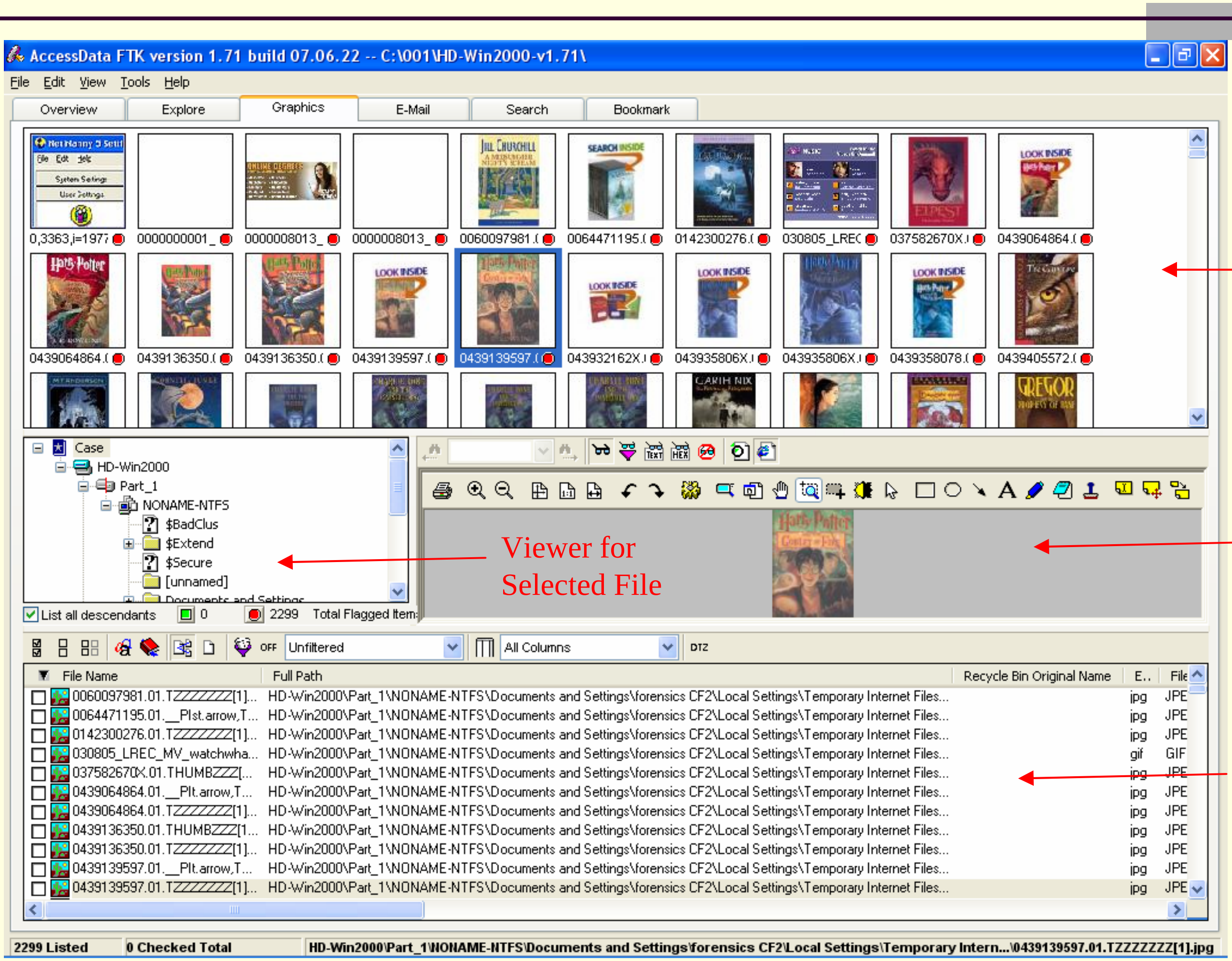
Item Category

Viewer

File List

The initial screen (Overview tab selected) for an open case in FTK

AccessData’s FTK (cont’d):



	File Name	Full Path	Recycle Bin Original Name	E..	File
☐	0060097981.01.TZZZZZZZ[1]...	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\Local Settings\Temporary Internet Files...		jpg	JPE
☐	0064471195.01.__Plst.arrow,T...	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\Local Settings\Temporary Internet Files...		jpg	JPE
☐	0142300276.01.TZZZZZZZ[1]...	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\Local Settings\Temporary Internet Files...		jpg	JPE
☐	030805_LREC_MV_watchwha...	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\Local Settings\Temporary Internet Files...		gif	GIF
☐	037582670X.01.THUMBZZZ[...	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\Local Settings\Temporary Internet Files...		jpg	JPE
☐	0439064864.01.__Plt.arrow,T...	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\Local Settings\Temporary Internet Files...		jpg	JPE
☐	0439064864.01.TZZZZZZZ[1]...	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\Local Settings\Temporary Internet Files...		jpg	JPE
☐	0439136350.01.THUMBZZZ[1...	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\Local Settings\Temporary Internet Files...		jpg	JPE
☐	0439136350.01.TZZZZZZZ[1]...	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\Local Settings\Temporary Internet Files...		jpg	JPE
☐	0439139597.01.__Plt.arrow,T...	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\Local Settings\Temporary Internet Files...		jpg	JPE
☐	0439139597.01.TZZZZZZZ[1]...	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\Local Settings\Temporary Internet Files...		jpg	JPE

2299 Listed | 0 Checked Total | HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\Local Settings\Temporary Intern...\0439139597.01.TZZZZZZZ[1].jpg

Thumbnail Viewer

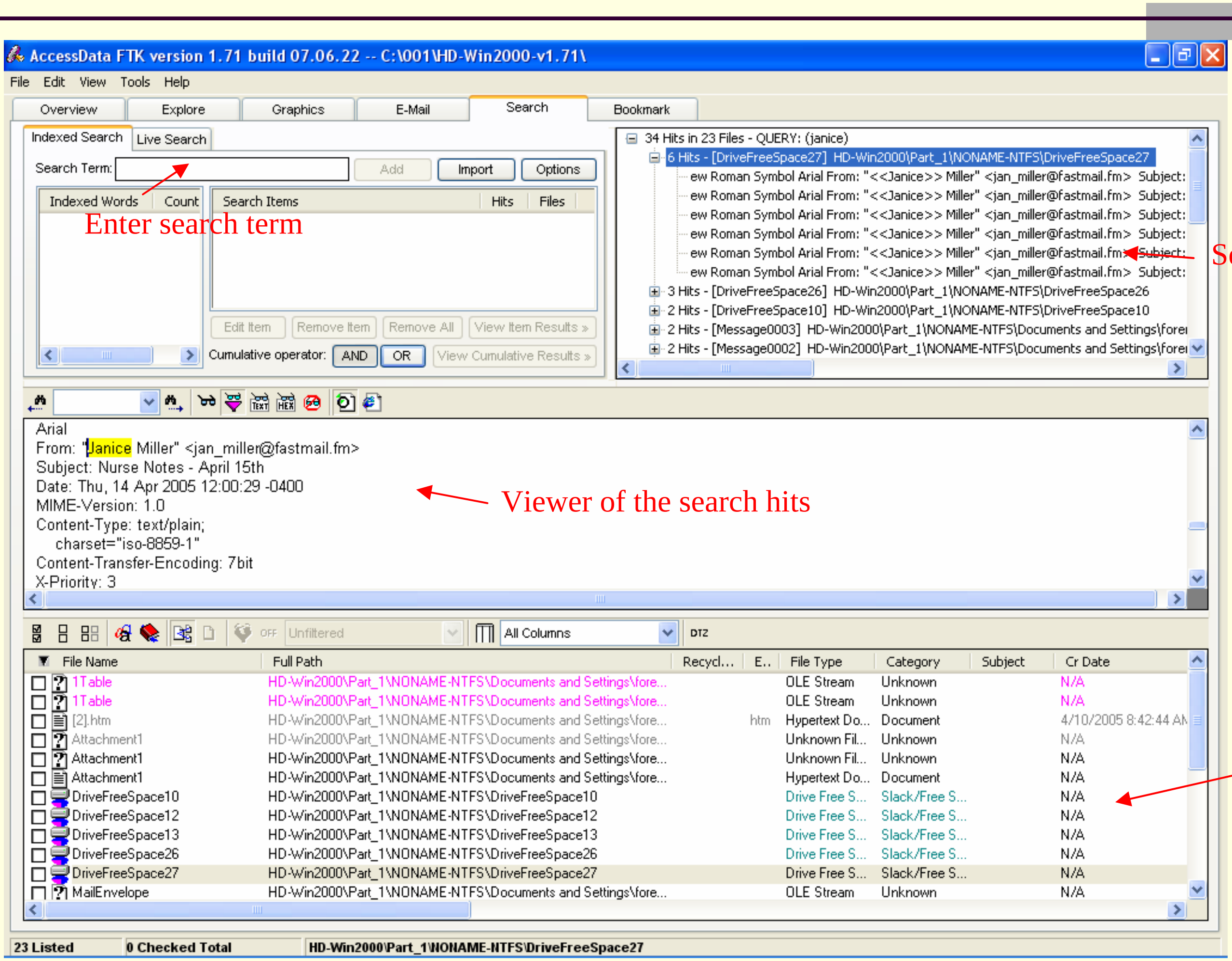
Viewer for Selected File

Viewer for Selected File

Viewer for Selected File

Graphics tab selected for an open case in FTK

AccessData's FTK (cont'd):



```
⊟ 34 Hits in 23 Files - QUERY: (janice)
  ⊟ 6 Hits - [DriveFreeSpace27] HD-Win2000\Part_1\NONAME-NTFS\DriveFreeSpace27
      ew Roman Symbol Arial From: "<<Janice>> Miller" <jan_miller@fastmail.fm> Subject:
      ew Roman Symbol Arial From: "<<Janice>> Miller" <jan_miller@fastmail.fm> Subject:
      ew Roman Symbol Arial From: "<<Janice>> Miller" <jan_miller@fastmail.fm> Subject:
      ew Roman Symbol Arial From: "<<Janice>> Miller" <jan_miller@fastmail.fm> Subject:
      ew Roman Symbol Arial From: "<<Janice>> Miller" <jan_miller@fastmail.fm> Subject:
      ew Roman Symbol Arial From: "<<Janice>> Miller" <jan_miller@fastmail.fm> Subject:
  ⊞ 3 Hits - [DriveFreeSpace26] HD-Win2000\Part_1\NONAME-NTFS\DriveFreeSpace26
  ⊞ 2 Hits - [DriveFreeSpace10] HD-Win2000\Part_1\NONAME-NTFS\DriveFreeSpace10
  ⊞ 2 Hits - [Message0003] HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forei
  ⊞ 2 Hits - [Message0002] HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\forei
```

```
Arial
From: "Janice Miller" <jan_miller@fastmail.fm>
Subject: Nurse Notes - April 15th
Date: Thu, 14 Apr 2005 12:00:29 -0400
MIME-Version: 1.0
Content-Type: text/plain;
    charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Priority: 3
```

	File Name	Full Path	Recycl...	E..	File Type	Category	Subject	Cr Date
□	1Table	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\fore...			OLE Stream	Unknown		N/A
□	1Table	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\fore...			OLE Stream	Unknown		N/A
□	[2].htm	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\fore...		htm	Hypertext Do...	Document		4/10/2005 8:42:44 AM
□	Attachment1	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\fore...			Unknown Fil...	Unknown		N/A
□	Attachment1	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\fore...			Unknown Fil...	Unknown		N/A
□	Attachment1	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\fore...			Hypertext Do...	Document		N/A
□	DriveFreeSpace10	HD-Win2000\Part_1\NONAME-NTFS\DriveFreeSpace10			Drive Free S...	Slack/Free S...		N/A
□	DriveFreeSpace12	HD-Win2000\Part_1\NONAME-NTFS\DriveFreeSpace12			Drive Free S...	Slack/Free S...		N/A
□	DriveFreeSpace13	HD-Win2000\Part_1\NONAME-NTFS\DriveFreeSpace13			Drive Free S...	Slack/Free S...		N/A
□	DriveFreeSpace26	HD-Win2000\Part_1\NONAME-NTFS\DriveFreeSpace26			Drive Free S...	Slack/Free S...		N/A
□	DriveFreeSpace27	HD-Win2000\Part_1\NONAME-NTFS\DriveFreeSpace27			Drive Free S...	Slack/Free S...		N/A
□	MailEnvelope	HD-Win2000\Part_1\NONAME-NTFS\Documents and Settings\fore...			OLE Stream	Unknown		N/A

23 Listed | 0 Checked Total | HD-Win2000\Part_1\NONAME-NTFS\DriveFreeSpace27

Enter search term

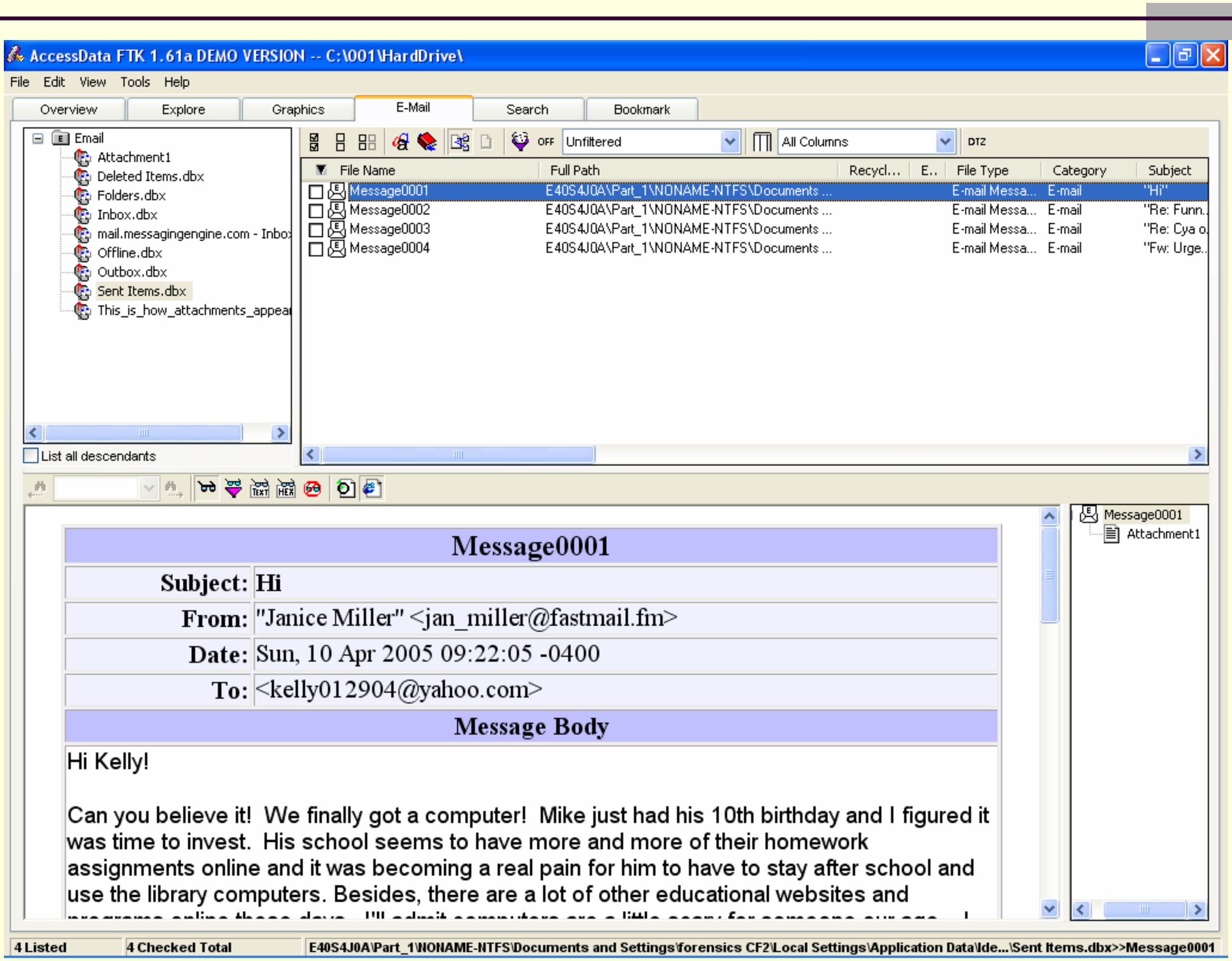
Search Results

Viewer of the search hits

File List

Search results in FTK

AccessData’s FTK (cont’d):



Email
- Attachment1
- Deleted Items.dbx
- Folders.dbx
- Inbox.dbx
- mail.messagingengine.com - Inbox
- Offline.dbx
- Outbox.dbx
- Sent Items.dbx
- This_is_how_attachments_appear

File Name	Full Path	Recycl...	E..	File Type	Category	Subject
□ Message0001	E40S4J0A\Part_1\NONAME-NTFS\Documents ...			E-mail Messa...	E-mail	"Hi"
□ Message0002	E40S4J0A\Part_1\NONAME-NTFS\Documents ...			E-mail Messa...	E-mail	"Re: Funn.
□ Message0003	E40S4J0A\Part_1\NONAME-NTFS\Documents ...			E-mail Messa...	E-mail	"Re: Cya o
□ Message0004	E40S4J0A\Part_1\NONAME-NTFS\Documents ...			E-mail Messa...	E-mail	"Fw: Urge.

Message0001	
Subject:	Hi
From:	"Janice Miller" <jan_miller@fastmail.fm>
Date:	Sun, 10 Apr 2005 09:22:05 -0400
To:	<kelly012904@yahoo.com>

Message Body

Hi Kelly!

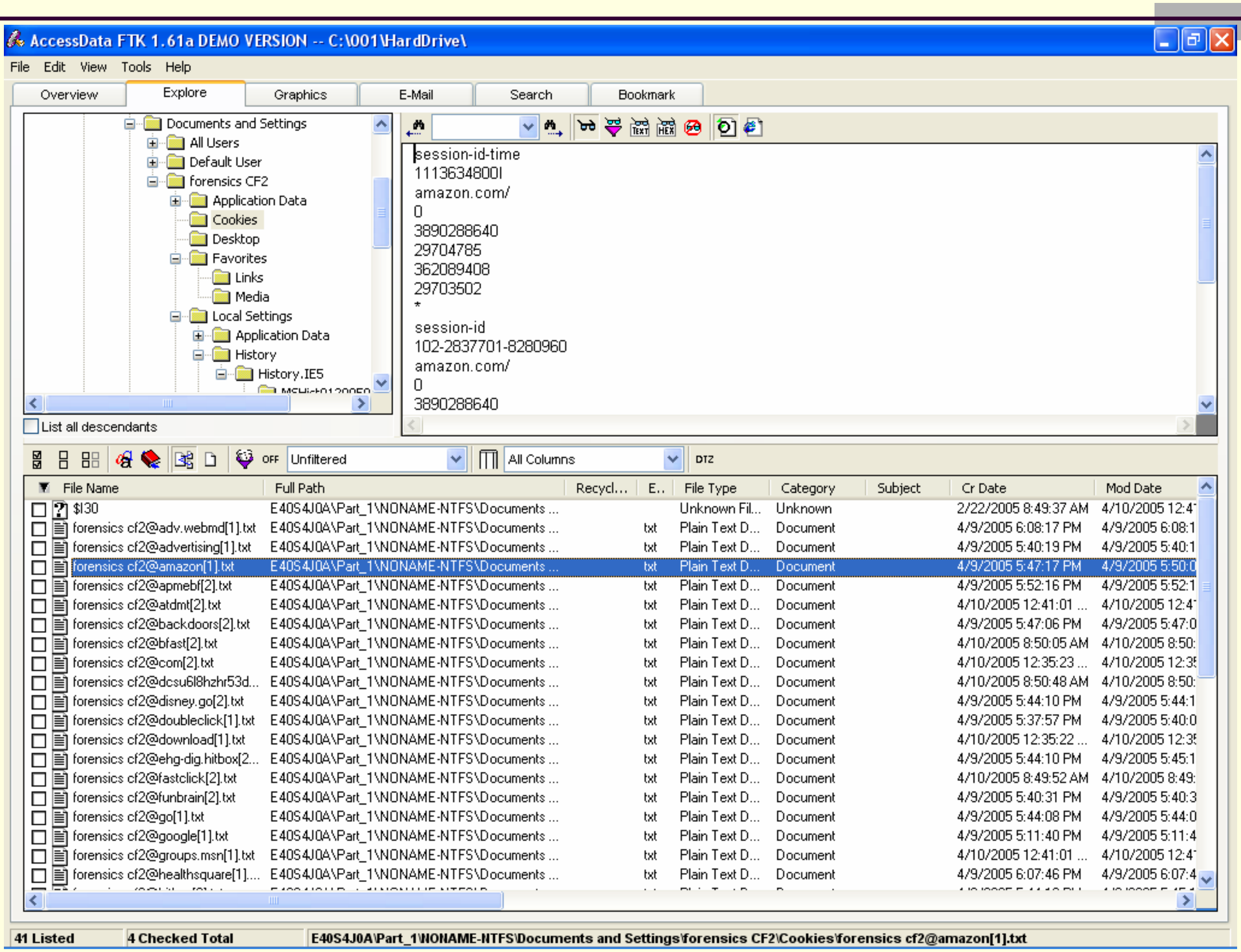
Can you believe it! We finally got a computer! Mike just had his 10th birthday and I figured it was time to invest. His school seems to have more and more of their homework assignments online and it was becoming a real pain for him to have to stay after school and use the library computers. Besides, there are a lot of other educational websites and programs online these days. I'll admit computers are a little scary for someone our age. I

Message0001
- Attachment1

4 Listed | 4 Checked Total | E40S4J0A\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\Local Settings\Application Data\Ide...\Sent Items.dbx>>Message0001

FTK Email Viewer

AccessData’s FTK (cont’d):



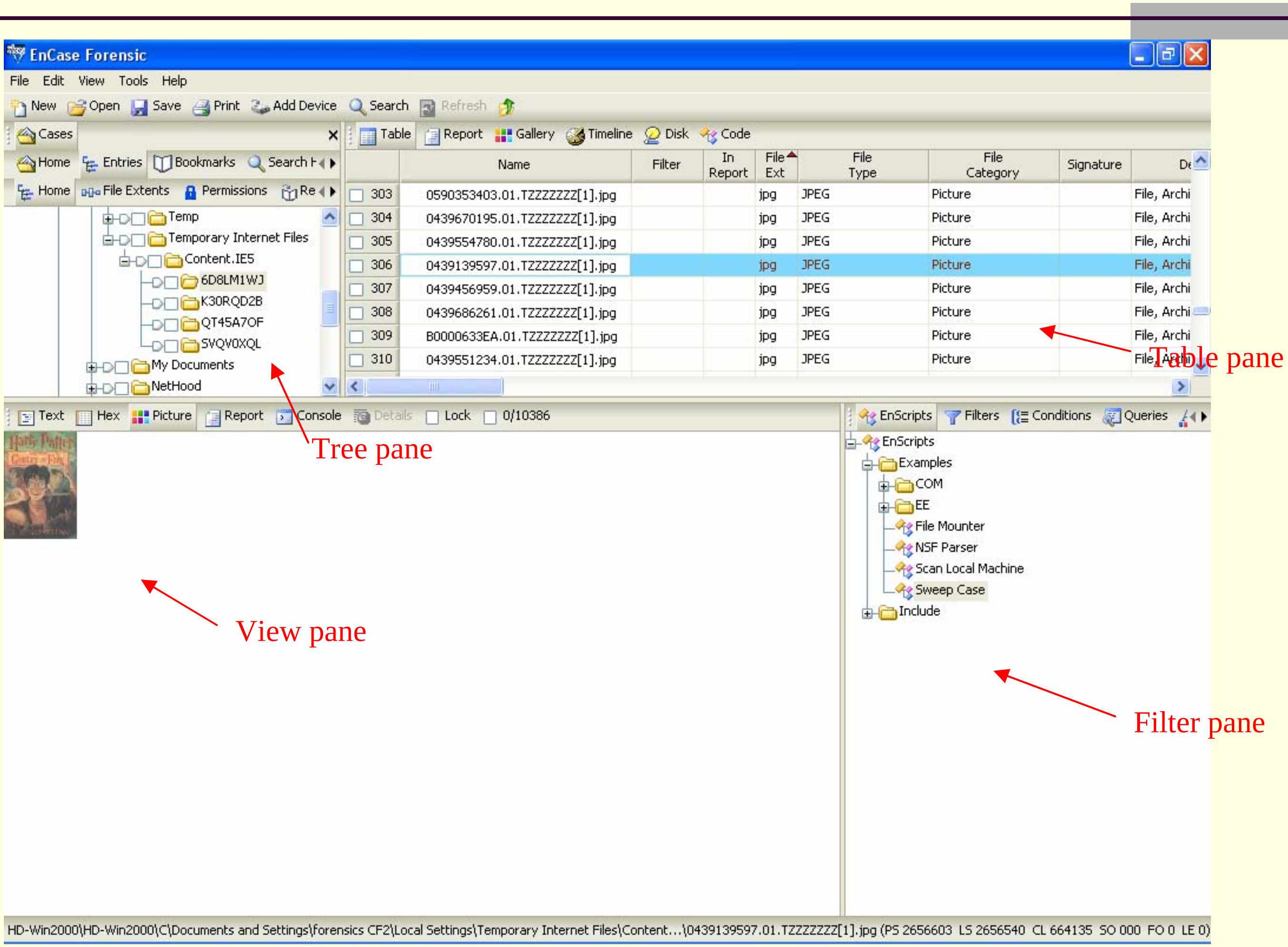
```
session-id-time
1113634800l
amazon.com/
0
3890288640
29704785
362089408
29703502
*
session-id
102-2837701-8280960
amazon.com/
0
3890288640
```

File Name	Full Path	Recycl...	E..	File Type	Category	Subject	Cr Date	Mod Date
□ $I30	E40S4J0A\Part_1\NONAME-NTFS\Documents ...			Unknown Fil...	Unknown		2/22/2005 8:49:37 AM	4/10/2005 12:41
□ forensics cf2@adv.webmd[1].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/9/2005 6:08:17 PM	4/9/2005 6:08:1
□ forensics cf2@advertising[1].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/9/2005 5:40:19 PM	4/9/2005 5:40:1
□ forensics cf2@amazon[1].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/9/2005 5:47:17 PM	4/9/2005 5:50:0
□ forensics cf2@apmebf[2].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/9/2005 5:52:16 PM	4/9/2005 5:52:1
□ forensics cf2@atdmt[2].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/10/2005 12:41:01 ...	4/10/2005 12:41
□ forensics cf2@backdoors[2].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/9/2005 5:47:06 PM	4/9/2005 5:47:0
□ forensics cf2@bfast[2].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/10/2005 8:50:05 AM	4/10/2005 8:50:
□ forensics cf2@com[2].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/10/2005 12:35:23 ...	4/10/2005 12:35
□ forensics cf2@dcsu6l8hzhr53d...	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/10/2005 8:50:48 AM	4/10/2005 8:50:
□ forensics cf2@disney.go[2].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/9/2005 5:44:10 PM	4/9/2005 5:44:1
□ forensics cf2@doubleclick[1].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/9/2005 5:37:57 PM	4/9/2005 5:40:0
□ forensics cf2@download[1].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/10/2005 12:35:22 ...	4/10/2005 12:35
□ forensics cf2@ehg-dig.hitbox[2...	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/9/2005 5:44:10 PM	4/9/2005 5:45:1
□ forensics cf2@fastclick[2].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/10/2005 8:49:52 AM	4/10/2005 8:49:
□ forensics cf2@funbrain[2].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/9/2005 5:40:31 PM	4/9/2005 5:40:3
□ forensics cf2@go[1].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/9/2005 5:44:08 PM	4/9/2005 5:44:0
□ forensics cf2@google[1].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/9/2005 5:11:40 PM	4/9/2005 5:11:4
□ forensics cf2@groups.msn[1].txt	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/10/2005 12:41:01 ...	4/10/2005 12:41
□ forensics cf2@healthsquare[1]....	E40S4J0A\Part_1\NONAME-NTFS\Documents ...		txt	Plain Text D...	Document		4/9/2005 6:07:46 PM	4/9/2005 6:07:4

41 Listed | 4 Checked Total | E40S4J0A\Part_1\NONAME-NTFS\Documents and Settings\forensics CF2\Cookies\forensics cf2@amazon[1].txt

FTK Cookie Viewer

Other Forensics Tools:


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases
Home Entries Bookmarks Search H
Home File Extents Permissions Re
Table Report Gallery Timeline Disk Code
Text Hex Picture Report Console Details Lock 0/10386
EnScripts Filters Conditions Queries
Table pane
Tree pane
View pane
Filter pane

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	De
□ 303	0590353403.01.TZZZZZZZ[1].jpg			jpg	JPEG	Picture		File, Archi
□ 304	0439670195.01.TZZZZZZZ[1].jpg			jpg	JPEG	Picture		File, Archi
□ 305	0439554780.01.TZZZZZZZ[1].jpg			jpg	JPEG	Picture		File, Archi
□ 306	0439139597.01.TZZZZZZZ[1].jpg			jpg	JPEG	Picture		File, Archi
□ 307	0439456959.01.TZZZZZZZ[1].jpg			jpg	JPEG	Picture		File, Archi
□ 308	0439686261.01.TZZZZZZZ[1].jpg			jpg	JPEG	Picture		File, Archi
□ 309	B0000633EA.01.TZZZZZZZ[1].jpg			jpg	JPEG	Picture		File, Archi
□ 310	0439551234.01.TZZZZZZZ[1].jpg			jpg	JPEG	Picture		File, Archi

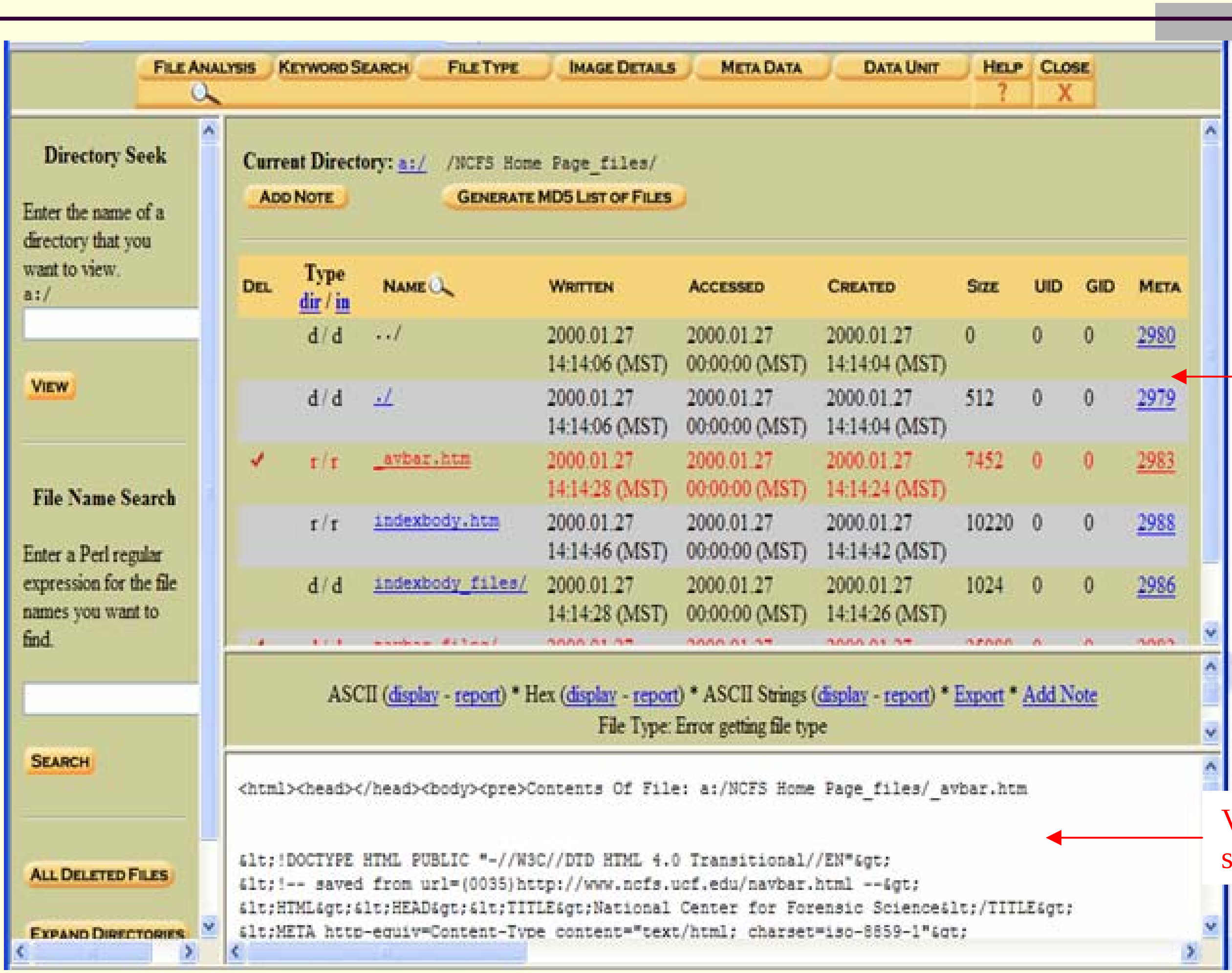
- Temp
- Temporary Internet Files
  - Content.IE5
    - 6D8LM1WJ
    - K30RQD2B
    - QT45A7OF
    - SVQV0XQL
- My Documents
- NetHood

- EnScripts
  - Examples
    - COM
    - EE
    - File Mounter
    - NSF Parser
    - Scan Local Machine
    - Sweep Case
  - Include

HD-Win2000\HD-Win2000\C\Documents and Settings\forensics CF2\Local Settings\Temporary Internet Files\Content...\0439139597.01.TZZZZZZZ[1].jpg (PS 2656603 LS 2656540 CL 664135 SO 000 FO 0 LE 0)

Guidance Software’s EnCase

Other Forensics Tools (cont’d):



Directory Seek

Enter the name of a directory that you want to view.

a:/

File Name Search

Enter a Perl regular expression for the file names you want to find.

Current Directory: a:/ /NCFS Home Page_files/

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	d / d	../	2000.01.27 14:14:06 (MST)	2000.01.27 00:00:00 (MST)	2000.01.27 14:14:04 (MST)	0	0	0	2980
	d / d	./	2000.01.27 14:14:06 (MST)	2000.01.27 00:00:00 (MST)	2000.01.27 14:14:04 (MST)	512	0	0	2979
✓	r / r	_avbar.htm	2000.01.27 14:14:28 (MST)	2000.01.27 00:00:00 (MST)	2000.01.27 14:14:24 (MST)	7452	0	0	2983
	r / r	indexbody.htm	2000.01.27 14:14:46 (MST)	2000.01.27 00:00:00 (MST)	2000.01.27 14:14:42 (MST)	10220	0	0	2988
	d / d	indexbody_files/	2000.01.27 14:14:28 (MST)	2000.01.27 00:00:00 (MST)	2000.01.27 14:14:26 (MST)	1024	0	0	2986

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note

File Type: Error getting file type

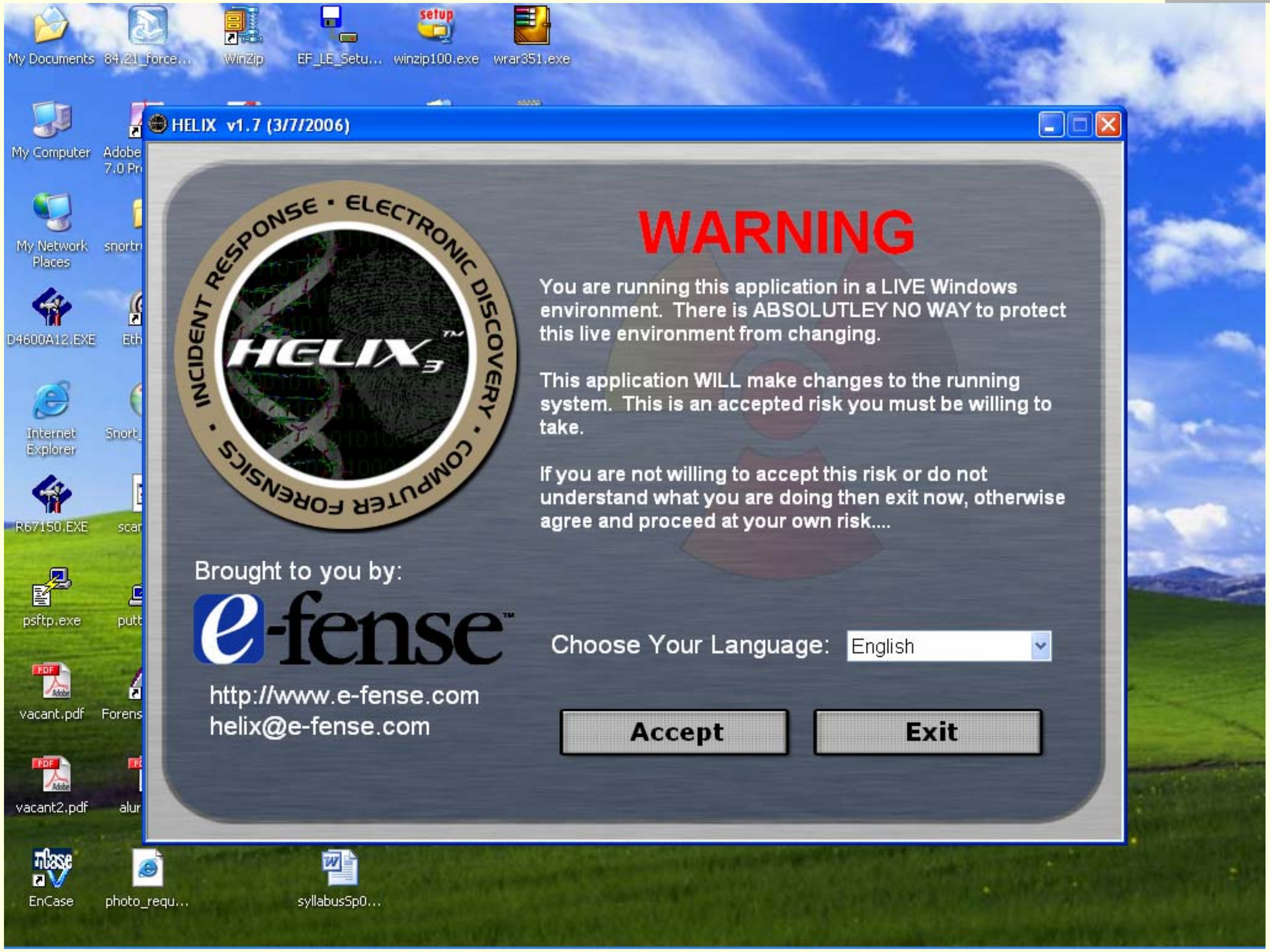
```
<html><head></head><body><pre>Contents Of File: a:/NCFS Home Page_files/_avbar.htm


&lt;!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"&gt;
&lt;!-- saved from url=(0035)http://www.ncfs.ucf.edu/navbar.html --&gt;
&lt;HTML&gt;&lt;HEAD&gt;&lt;TITLE&gt;National Center for Forensic Science&lt;/TITLE&gt;
&lt;META http-equiv=Content-Type content="text/html; charset=iso-8859-1"&gt;
```

File List

Viewer for selected file

TSK/Autopsy’s Interface for File Analysis

Helix live system analysis:



HELIX v1.7 (3/7/2006)

WARNING

You are running this application in a LIVE Windows environment. There is ABSOLUTLEY NO WAY to protect this live environment from changing.

This application WILL make changes to the running system. This is an accepted risk you must be willing to take.

If you are not willing to accept this risk or do not understand what you are doing then exit now, otherwise agree and proceed at your own risk....

Brought to you by:

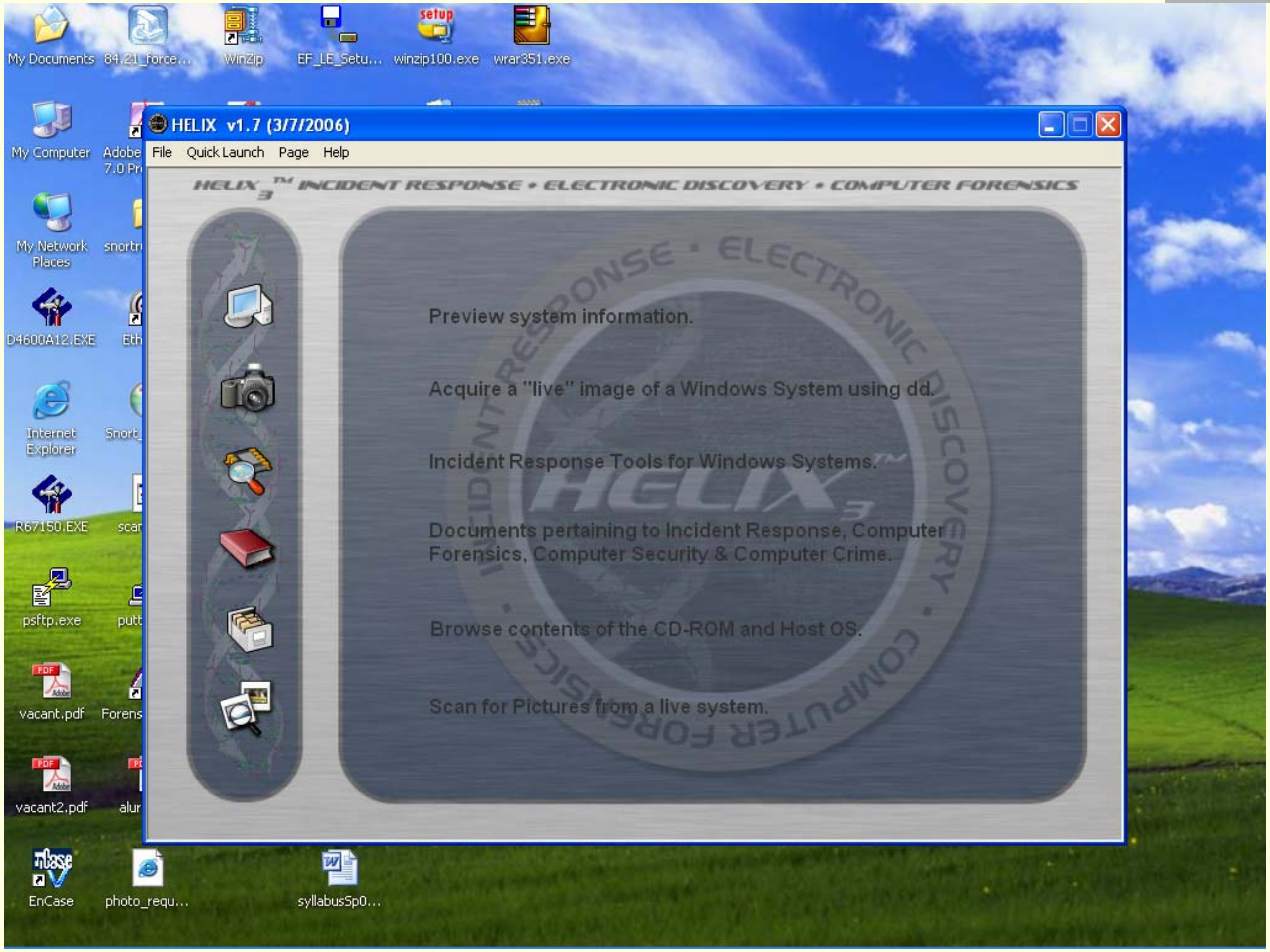
e-fense™

http://www.e-fense.com
helix@e-fense.com

Choose Your Language: English

Helix initial screen

Helix live system analysis (cont’d):



Preview system information.

Acquire a "live" image of a Windows System using dd.

Incident Response Tools for Windows Systems.

Documents pertaining to Incident Response, Computer Forensics, Computer Security & Computer Crime.

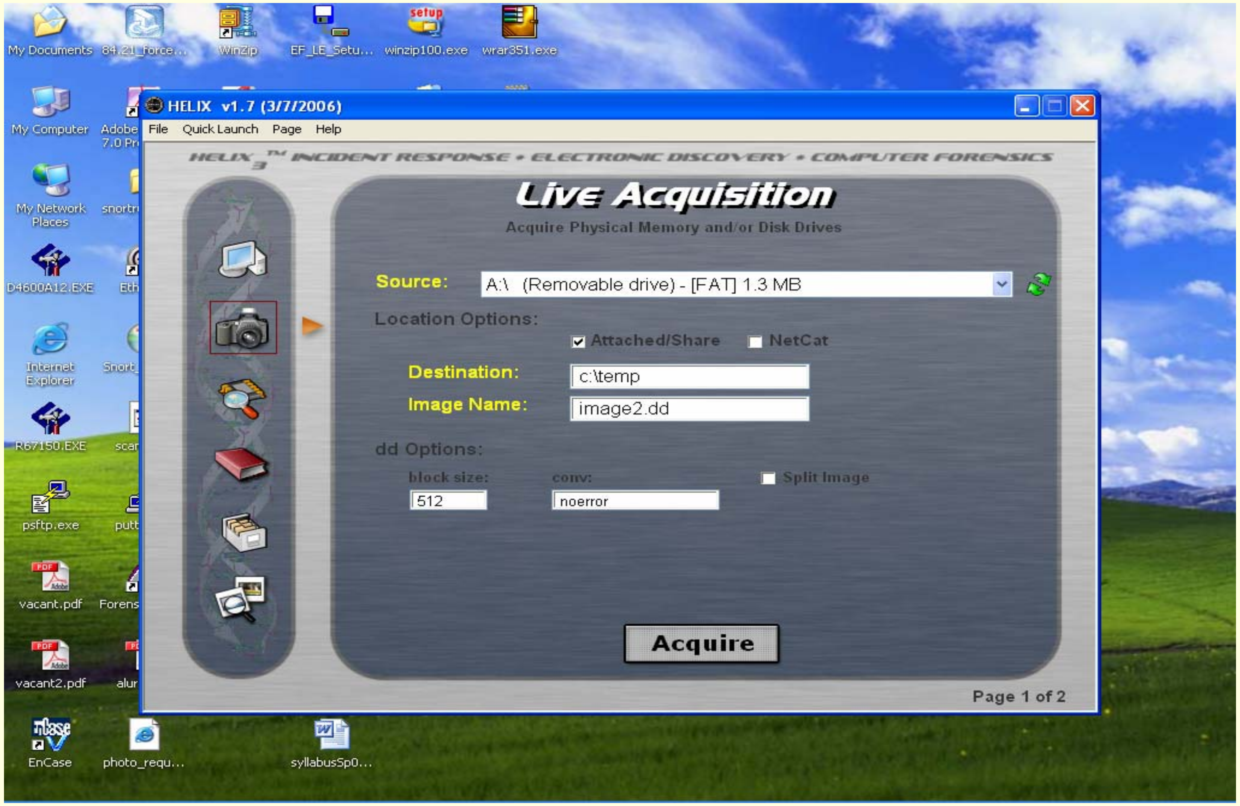
Browse contents of the CD-ROM and Host OS.

Scan for Pictures from a live system.

Built-in tools on Helix CD

Using Helix to image disk:

Helix uses dd (data dump) to duplicate disks (see explanation of the command syntax and options at http://www.softpanorama.org/Tools/dd.shtml)



Source: A:\ (Removable drive) - [FAT] 1.3 MB

Location Options: ☑ Attached/Share ☐ NetCat

Destination: c:\temp

Image Name: image2.dd

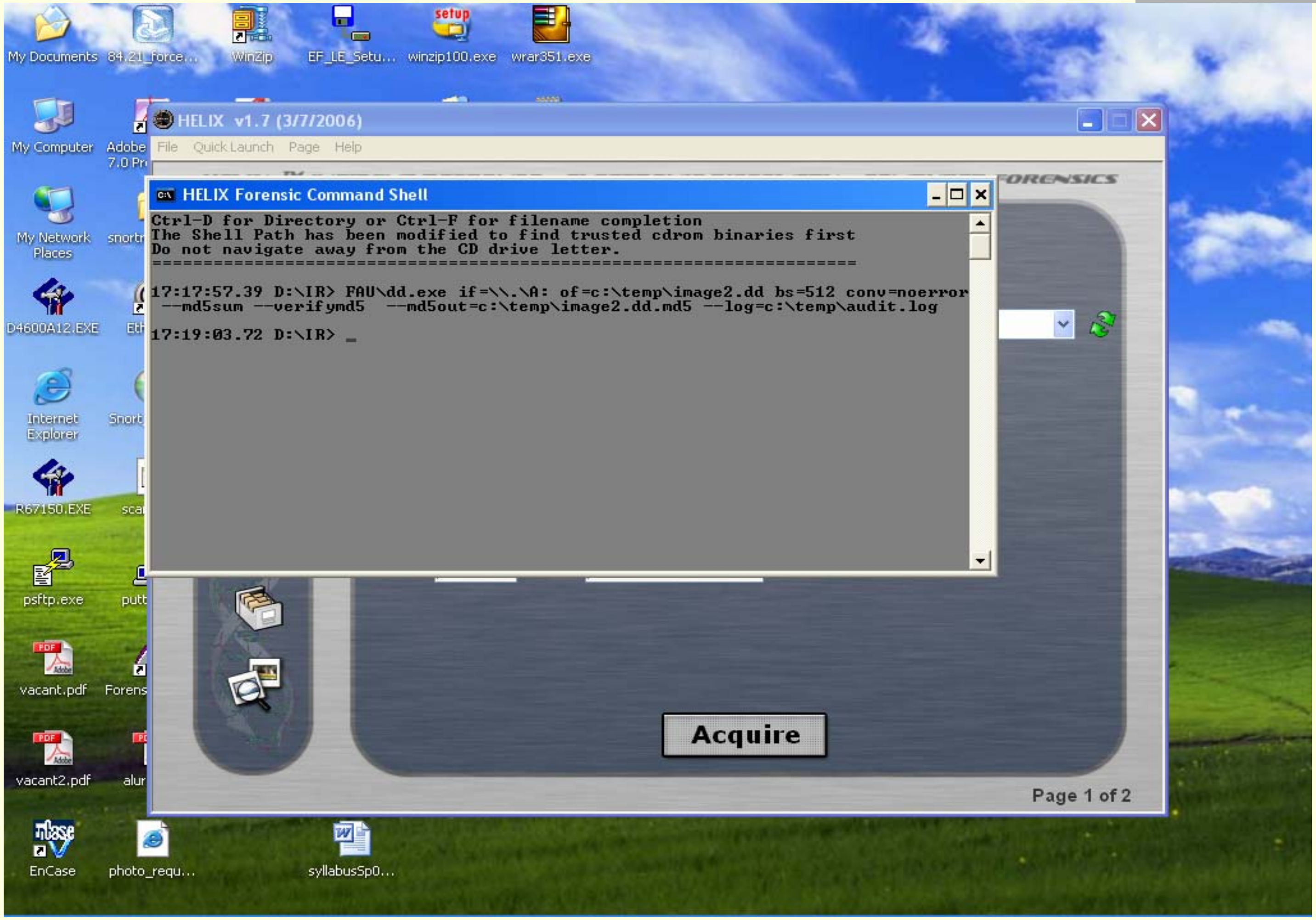
dd Options:

block size: 512

conv: noerror

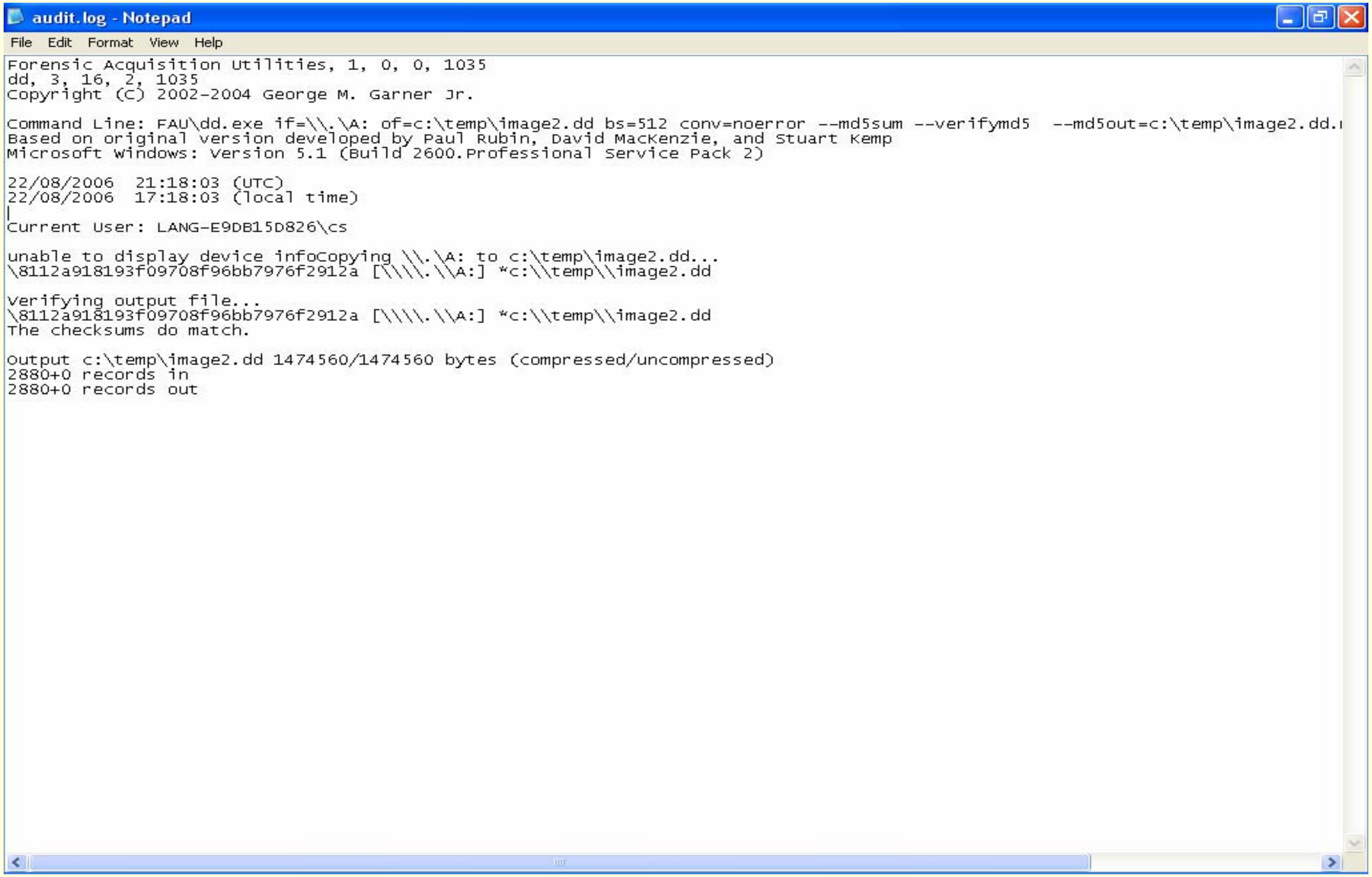
☐ Split Image

Using helix to image a floppy disk (cont’d):



```
Ctrl-D for Directory or Ctrl-F for filename completion
The Shell Path has been modified to find trusted cdrom binaries first
Do not navigate away from the CD drive letter.
======================================================================

17:17:57.39 D:\IR> FAU\dd.exe if=\\.\A: of=c:\temp\image2.dd bs=512 conv=noerror
 --md5sum --verifymd5  --md5out=c:\temp\image2.dd.md5 --log=c:\temp\audit.log

17:19:03.72 D:\IR> _
```

Audit.log file after dd is complete:



```
Forensic Acquisition Utilities, 1, 0, 0, 1035
dd, 3, 16, 2, 1035
Copyright (C) 2002-2004 George M. Garner Jr.

Command Line: FAU\dd.exe if=\\.\A: of=c:\temp\image2.dd bs=512 conv=noerror --md5sum --verifymd5  --md5out=c:\temp\image2.dd.
Based on original version developed by Paul Rubin, David MacKenzie, and Stuart Kemp
Microsoft Windows: Version 5.1 (Build 2600.Professional Service Pack 2)

22/08/2006  21:18:03 (UTC)
22/08/2006  17:18:03 (local time)

Current User: LANG-E9DB15D826\cs

unable to display device infoCopying \\.\A: to c:\temp\image2.dd...
\8112a918193f09708f96bb7976f2912a [\\\\.\\A:] *c:\\temp\\image2.dd

Verifying output file...
\8112a918193f09708f96bb7976f2912a [\\\\.\\A:] *c:\\temp\\image2.dd
The checksums do match.

Output c:\temp\image2.dd 1474560/1474560 bytes (compressed/uncompressed)
2880+0 records in
2880+0 records out
```

Forensics Software Tools:

- Guidance Software's EnCase (commercial, requires license dongle)
- Access Data Forensic Toolkit (commercial, runs in demo mode without license dongle)
- Penguin Sleuth (knock-off of Knoppix with extra forensic tools)
- Helix (another knock-off): booting from Penguin Sleuth or Helix will boot all drives Read-Only, boots into Linux in RAM (with more than 128MB of RAM)
- The Sleuth Kit consists of command-line tools and a browser-like front-end Autopsy
- Spada (Law Enforcement only, also a knock-off)
- AccessData's FTK Imager (does not require license dongle)

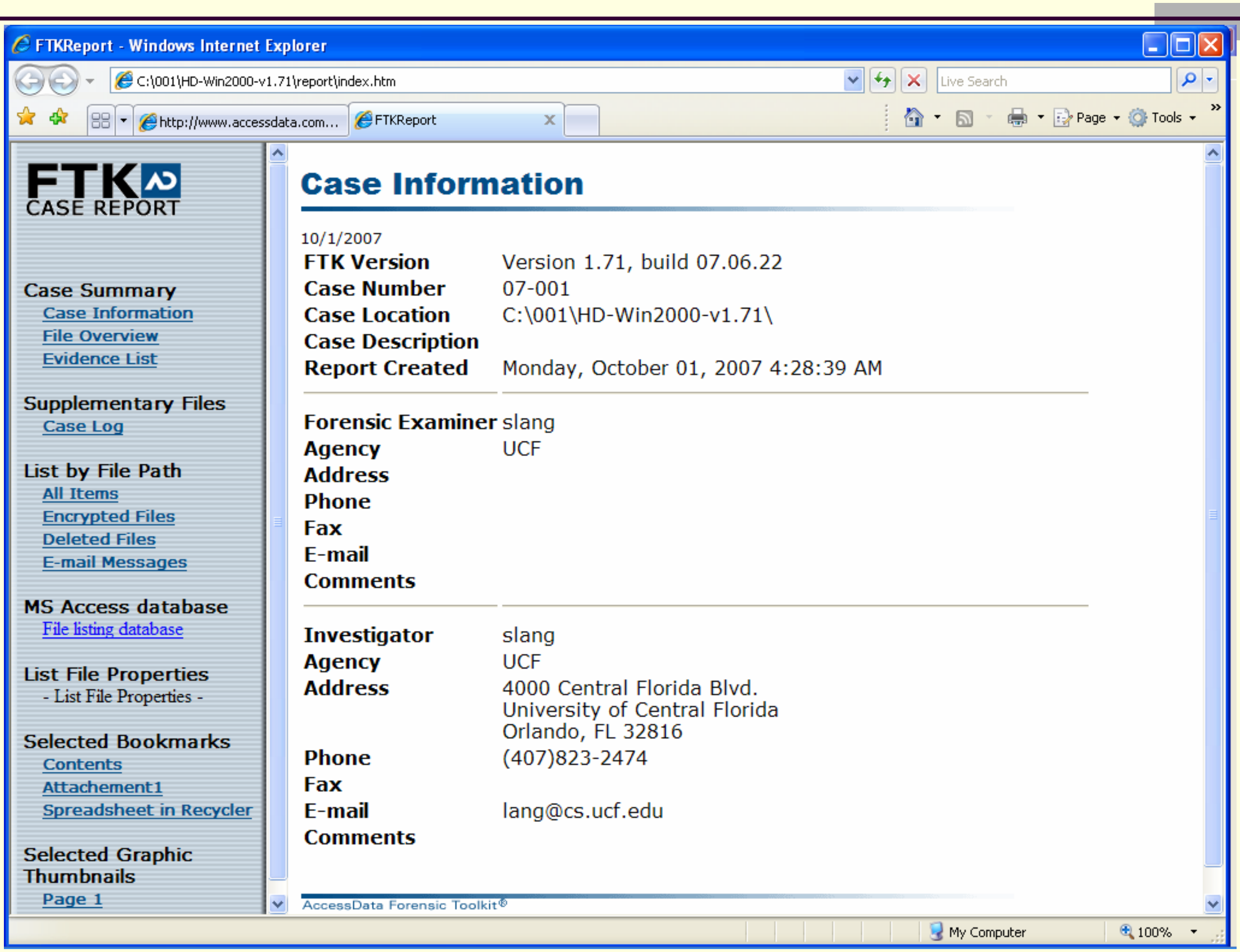
Forensics Software Tools (cont'd):

- Norton Utilities/SystemWorks (DiskEdit is the primary one)
  * Unerase - in 2003 and earlier
  * Unformat - in 2003 and earlier
  * gDisk - in 2003 and earlier
- WhatFormat, FileAlyzer: tools to analyze files
- Quick View Plus: views many different file types (read-only)
- WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor

❑ A Microsoft article on Fundamental Computer Investigation Guide For Windows, Jan. 11, 2007

❑ National Institute of Justice's Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, April 14, 2008

Forensic Report:



FTKReport - Windows Internet Explorer
C:\001\HD-Win2000-v1.71\report\index.htm
Live Search
http://www.accessdata.com...
FTKReport
Page
Tools
My Computer
100%

FTK CASE REPORT

Case Summary
- Case Information
- File Overview
- Evidence List

Supplementary Files
- Case Log

List by File Path
- All Items
- Encrypted Files
- Deleted Files
- E-mail Messages

MS Access database
- File listing database

List File Properties
- List File Properties -

Selected Bookmarks
- Contents
- Attachement1
- Spreadsheet in Recycler

Selected Graphic Thumbnails
- Page 1

Case Information

10/1/2007

FTK Version	Version 1.71, build 07.06.22
Case Number	07-001
Case Location	C:\001\HD-Win2000-v1.71\
Case Description	
Report Created	Monday, October 01, 2007 4:28:39 AM
Forensic Examiner	slang
Agency	UCF
Address	
Phone	
Fax	
E-mail	
Comments	
Investigator	slang
Agency	UCF
Address	4000 Central Florida Blvd. University of Central Florida Orlando, FL 32816
Phone	(407)823-2474
Fax	
E-mail	lang@cs.ucf.edu
Comments	

AccessData Forensic Toolkit®

FTK's Case Report

Careers in Computer Forensics:

- An article on computer forensics careers available at http://About.com under careers > tech careers > computer jobs
- Monster.com's career advices on computer forensics
- Careers in the U.S. Government, at http://www.usajobs.gov/ entering keywords "computer forensic"
- Search http://www.careerbuilder.com/ entering keywords "computer forensics"

It is a tough job to be a computer forensics expert: "In view of the above I find that the defendants have not met their burden of showing by a preponderance of the evidence that Moshlak's methodologies are reliable under Federal Rule of Evidence 702, or would otherwise assist the jury to understand the evidence or to determine a fact in issue. Therefore, it is my recommendation that plaintiff's motion to exclude Moshlak as an expert witness at trial be GRANTED." in United States District Court, D. Puerto Rico, Nilda RIVERA-CRUZ, Plaintiff, v. LATIMER, BIAGGI, RACHID & GODREAU, LLP, et al., Defendants,.**Civil No. 04-2377 (ADC).** June 16, 2008.

The Defendants' expert witness Mr. Steven Moshlak contacted me via email on 11/29/2008 and gave the following response to the ruling of the Daubert Hearing:

"After reading Chief Magistrate-Judge's R&R (Report and Recommendation), it was quite contrary to the testimony and exhibits that were presented at the Daubert Hearing. Although the US District Judge assigned to this case relied upon the Magistrate's R&R, she never saw the testimony and the attorneys for the defense should have aggressively pursued the misinformation. No mention of the alteration of the data contained on the hard drive, while in the custody of the Plaintiff's Counsel's Expert, was noted in the R&R, which can impact the credibility of the Plaintiff's case, nor was the testimony cited that the basis for the CF methodology employed is based upon US Department of Justice computer forensics methodologies.

In essence the attorney is responsible for being an advocate of the client and the interface with the court, not the CF person. Thus, the CF person was essentially left "hung-out to dry," due to the systems and circumstances beyond the control of the CF person in this case."