

# Computer (or Digital) forensics

- Application of science and engineering to the legal problem of digital evidence
- Computer forensics is largely a response to a demand for service from the law enforcement community
- 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
- Software and hardware forensic tools are being used by forensic examiners employed by law enforcement (local, state, federal levels), IT security departments in businesses or government agencies, legal firms specializing in forensic discovery, etc.

Computer forensics involves the following steps regarding the handling of computer data ([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](#))

## Roles of a computer involved in digital crime investigations:

- as the instrument in committing a crime (an intruder or a computer virus writer that uses computers for performing illegal activities)
- as the victim (a system being comprised, data stolen or deleted)
- as a container or storage warehouse for a crime (a PDA that has spreadsheets of drug dealers and buyers information)

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)

## 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 with multiple user data, company databases, network devices such as routers, firewalls

## 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 [4<sup>th</sup> 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)

## Typical Digital Evidence in Forensic Examination:

- Recover “deleted” files and folders, remnants in swap space (pagefile) or allocated clusters
- Email 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
  - ❑ track email origins (reading email header information)

- Windows Registry Files:

- ❑ identify user accounts on a single computer

- ❑ recover user ids and passwords

- ❑ 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

- ❑ 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](http://sourceforge.net/docman/?group_id=78332))

- 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://www.sysinternals.com/FileAndDiskUtilities.html>
  - ❑ 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

# Overview of Computer Crimes

- No longer are crimes committed on computers limited to skinny guys with pimples, tape on their glasses and squeaky voices.
- Now anyone can point and click and use a computer to commit just about any crime.

# Overview of Computer Crimes

- What type of crimes are being committed with computers?
- What information is generated to corroborate the facts and circumstances of the investigation?
- We as examiners must be able to articulate how the data examined and presented is evidentiary!

# Burglary and Safe Cutters

## The Investigation

- An organized group of burglars have been breaking into restaurants, stealing the safes, or cutting them open.
- Suspects reportedly use computers in some fashion to facilitate their crimes.
- Detectives eventually seized the suspects computer.

# Burglary and Safe Cutters

## The Problem

- How exactly do you use a computer to commit burglaries and open safes?
- What in the world am I looking for?

# Burglary and Safe Cutters

## The Results

- The suspects had partners who did not know where the restaurant to be broken in to was located.
- This is how the bad guys overcame this obstacle using computers.

Comment:

Map graphic.

File Name:

mqmapgend[1].gif

File Created:

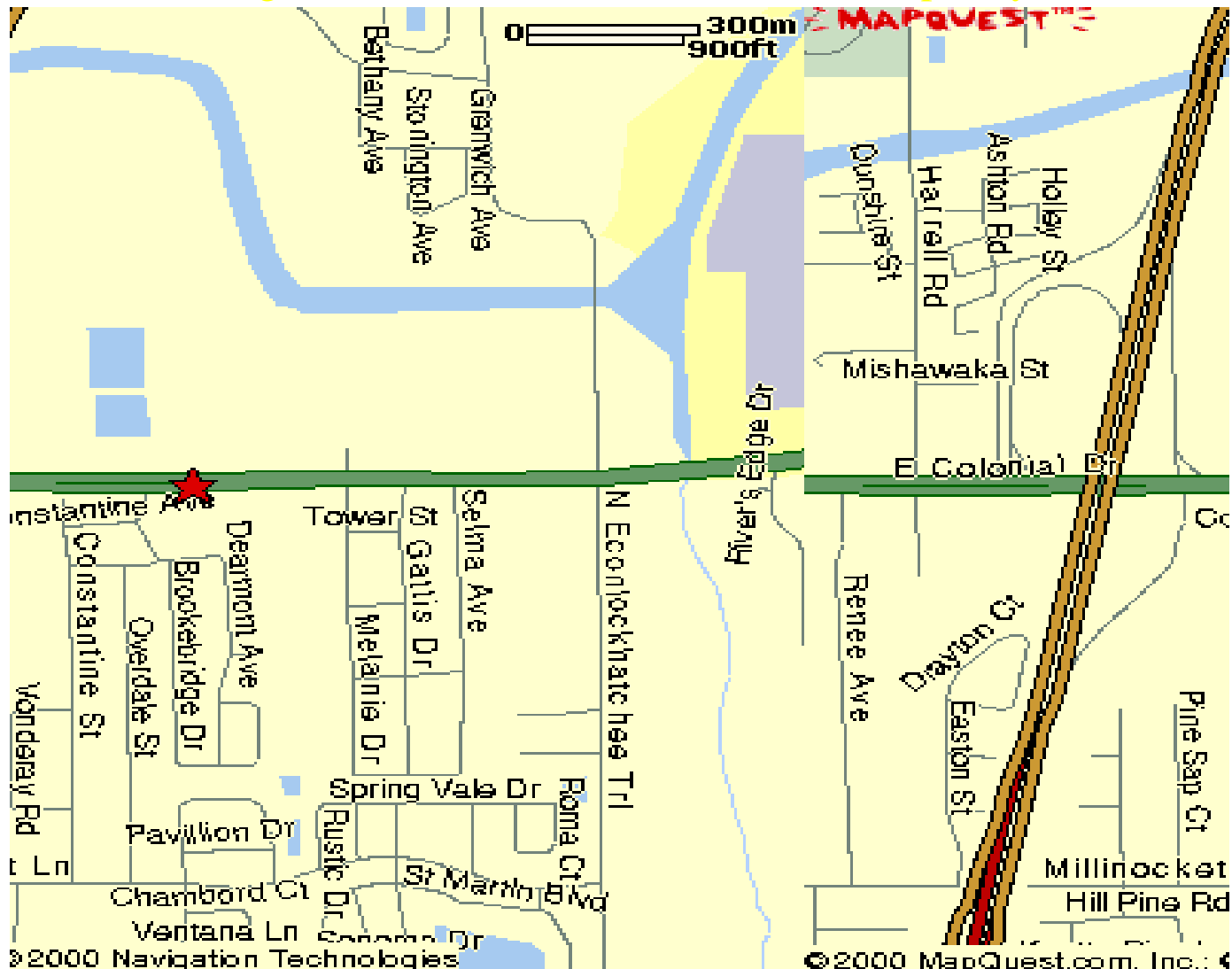
01/06/02 04:13:48AM

Last Accessed:

01/06/02

Full Path:

Seagate 7EH0AHXM\C\WINDOWS\Temporary Internet

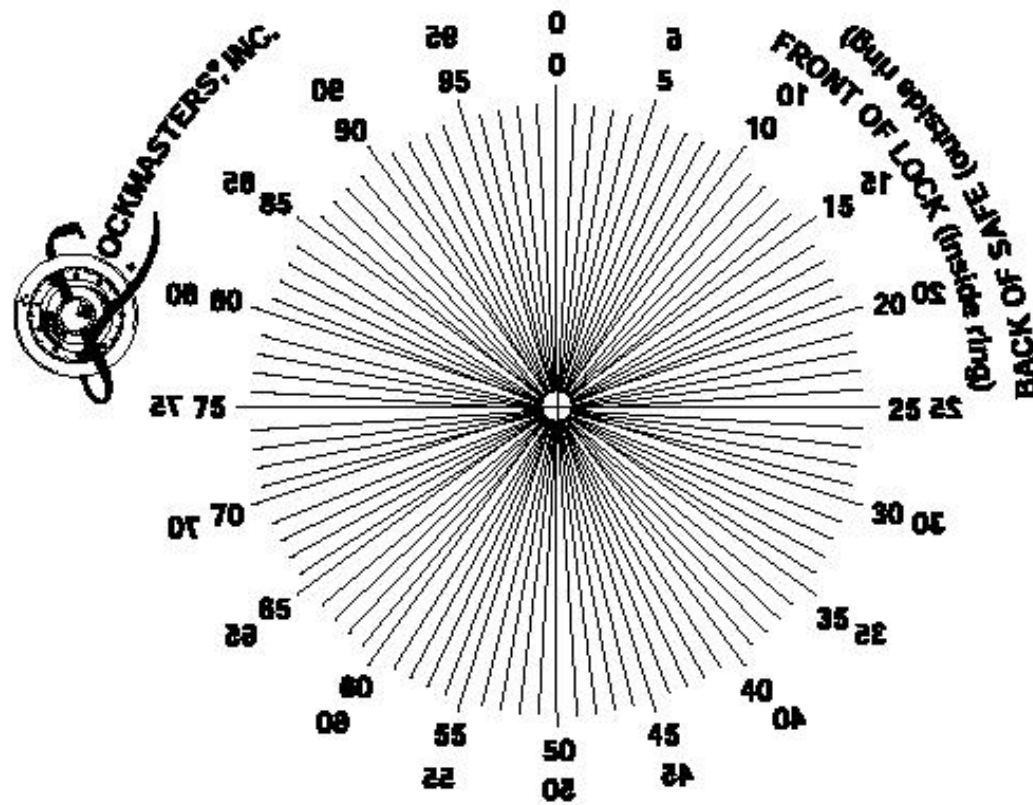


# Burglary and Safe Cutters

- Okay, our bad guys know how to get there but, will they be able to break into the safe?
- How about a template for drilling out a safe courtesy of the safe manufactures web site.



# Where to drill



# Burglary and Safe Cutters

- Better yet, lets look up the safe in advance so we know if were wasting our time.

**Comment:** Graphic of safe.  
**File Name:** F3020[1].jpg  
**File Created:** 01/06/02 06:04:08PM  
**Last Accessed:** 01/06/02  
**Full Path:** Seagate 7EH0AHXM\C\WINDOWS\Temporary Internet Files\Content.IE5\0HENSODYZ\F3020[1].jpg



# Burglary and Safe Cutters

- Since burglary is not a steady job lets subscribe to the online version of the Neilsens rating service.
- Their software keeps a database of everywhere we go on the Internet for marketing references.
- We get a few bucks a month to allow them to monitor our Internet use.

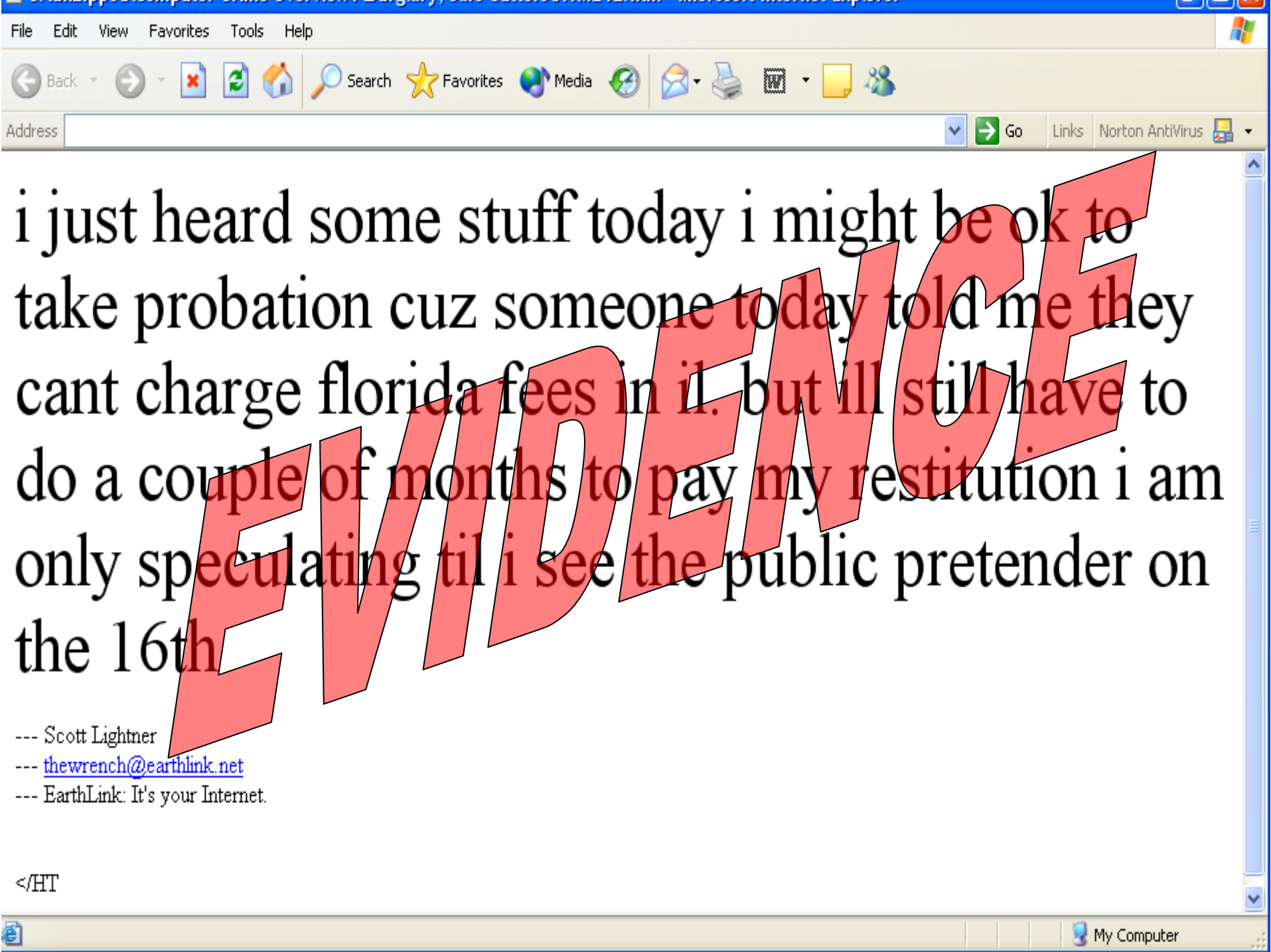
**Comment:** Web site references in Nielsen Netratings program database.  
**File Name:** pagecache.db  
**Full Path:** Seagate 7EH0AHXM\C\Program  
Files\NielsenNetratings\bin\pagecache.db  
**Physical Location:** PS:1218211, SO:0

---

```
http://www.lockmasters.com/store/display.asp?prod_type=hp
http://www.lockmasters.com/store/display.asp?prod_type=hp !
http://www.lockmasters.com/tools/   ëB| a È   text/html /U
http://www.lockmasters.com/store/prod_detail.asp?id=1
http://www.lockmasters.com/images/newproducts/Mercedestmb.jpg
http://www.lockmasters.com/store/prod_detail.asp?id=2
http://www.lockmasters.com/images/newproducts/!sktread.jpg  ÿÿÿÿ
http://www.lockmasters.com/store/prod_detail.asp?id=3
http://www.lockmasters.com/images/newproducts/!hi-secf.jpg  ÿÿÿÿ
http://www.lockmasters.com/store/prod_detail.asp?id=4
http://www.lockmasters.com/images/newproducts/PS100tmb.jpg  ÿÿÿÿ
http://www.lockmasters.com/store/prod_detail.asp?id=5
http://www.lockmasters.com/images/newproducts/ClutchLongtmb.jpg
http://www.lockmasters.com/store/prod_detail.asp?id=6
http://www.lockmasters.com/images/newproducts/CarClutchtmb.jpg
http://www.lockmasters.com/store/prod_detail.asp?id=7
```

# Burglary and Safe Cutters

- Lets give the cops a hand and make sure that they can link me to this computer.



i just heard some stuff today i might be ok to  
take probation cuz someone today told me they  
cant charge florida fees in il. but ill still have to  
do a couple of months to pay my restitution i am  
only speculating til i see the public pretender on  
the 16th

**EVIDENCE**

--- Scott Lightner  
--- [thewrench@earthlink.net](mailto:thewrench@earthlink.net)  
--- EarthLink: It's your Internet.

</HT

# Burglary and Safe Cutters

- The graphics, HTML pages, Internet History, EMF files and fragments of the same in this case added up to over 500 pages in the report.



# Identity Theft Investigation

- Law Student from University of Miami meets a female in internet chat room and communicates with this subject for over two years
- The female purported herself to be a European Model. She sent him pictures of herself via the internet.
- The female eventually tells him she wants to fly him to Europe to meet her in person.
- He provides her with all of his biographical information that was needed for the “Airline ticket”.

*Some of the information in this section was changed from the actual case facts.*

# Identity Theft Investigation

- Once the female suspect has the information, she obtains several lines of credit in the victims name.
- She purchases various items on the internet to include an HP computer and beauty products.
- A few months later, the victims attempts to obtain extension on his student loans and is denied.
- He checks his credit history only to find the various accounts he did not open.
- The suspect was not a model (by any means) and lived in Orlando, FL (not Europe).

*Some of the information in this section was changed from the actual case facts.*

# Identity Theft Investigation

- Covert operations were conducted at the suspects residence where law enforcement posed as Fedex Employee's delivering a package.
- She eventually accepted the package at which time she was caught.
- The computer was seized
- The examination provided a lot of evidence to corroborate her scheme.
- She has since fled the United States.

# Identity Theft Investigation

## Examination Results

- Several HTML files recovered which show the online applications for credit and purchases
- Chat logs recovered corroborating victim statement
- Suspects “modeling” picture recovered
- Suspect charged with ID Theft and several other credit card related offenses.

**This is the photo of the model that the suspect purported to be. The graphic was recovered from the suspects hard drive**

*C:\Program Files\Netscape\Users\default\Cache\MV4D5241.JPG*



[sign in](#) | [register](#)

LIMITED

[hp.com home](#) | [products and services](#) | [support and drivers](#) | [solutions](#) | [how to buy](#)

[contact us](#) 1-888-999-4747 (to order by phone)

search:

[search all of hp US](#)

hpshopping home

- site quick browse -

hpshopping.com

## cart details

chat

QS-  quick shop

[find out how to get free shipping](#)

### purchase info

- [order status](#)
- [shipping info](#)
- [financing options](#)
- [rebates](#)
- [find a retailer](#)

### more info

- [help](#)
- [support & troubleshooting](#)
- [drivers & downloads](#)
- [creative projects](#)
- [learning library](#)
- [digital living](#)
- [about hpshopping](#)

product #	description	price	qty.	remove	total
P9852A#ABA	hp pavilion 753n desktop pc	\$1,049.00	1	<input type="checkbox"/>	\$1,049.00
<b>subtotal:</b>					<b>\$1,049.00</b>

as low as **\$32/month** +   
[pay \\$0 for 12 months](#)

[calculate tax & shipping](#)

*For U.S. Customers Only*

\* Taxes will be added for shipments to AL, CA, TN, UT, WI

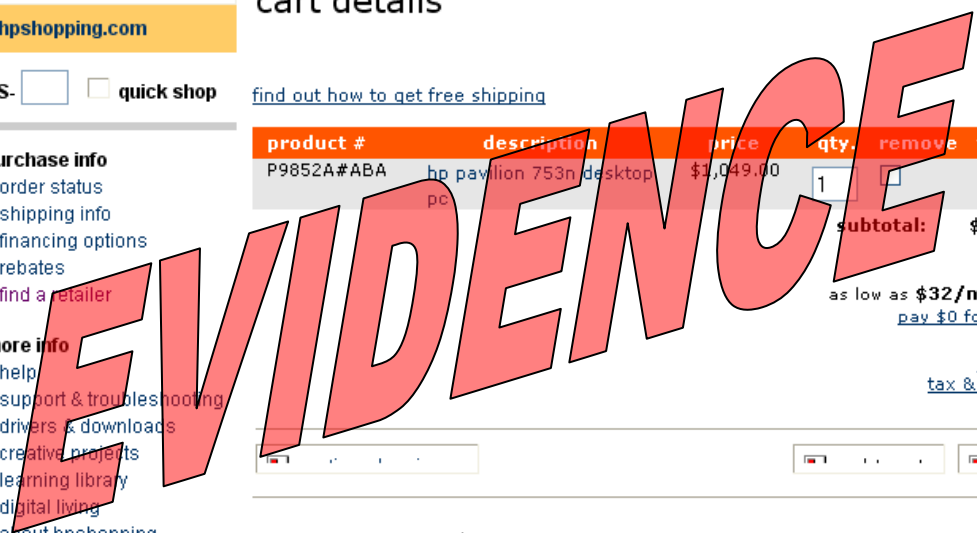
**Items will remain in your Cart for 30 days.**

The list of items above does not reflect an actual order. They are items that have been added to your Cart. Until an order is submitted and an order number is assigned, prices and availability are subject to change.

### When to Expect your Order

Orders received before 10:00pm Eastern Time Monday through Friday ship the same day. All other orders ship the next business day (except for custom-built PCs).

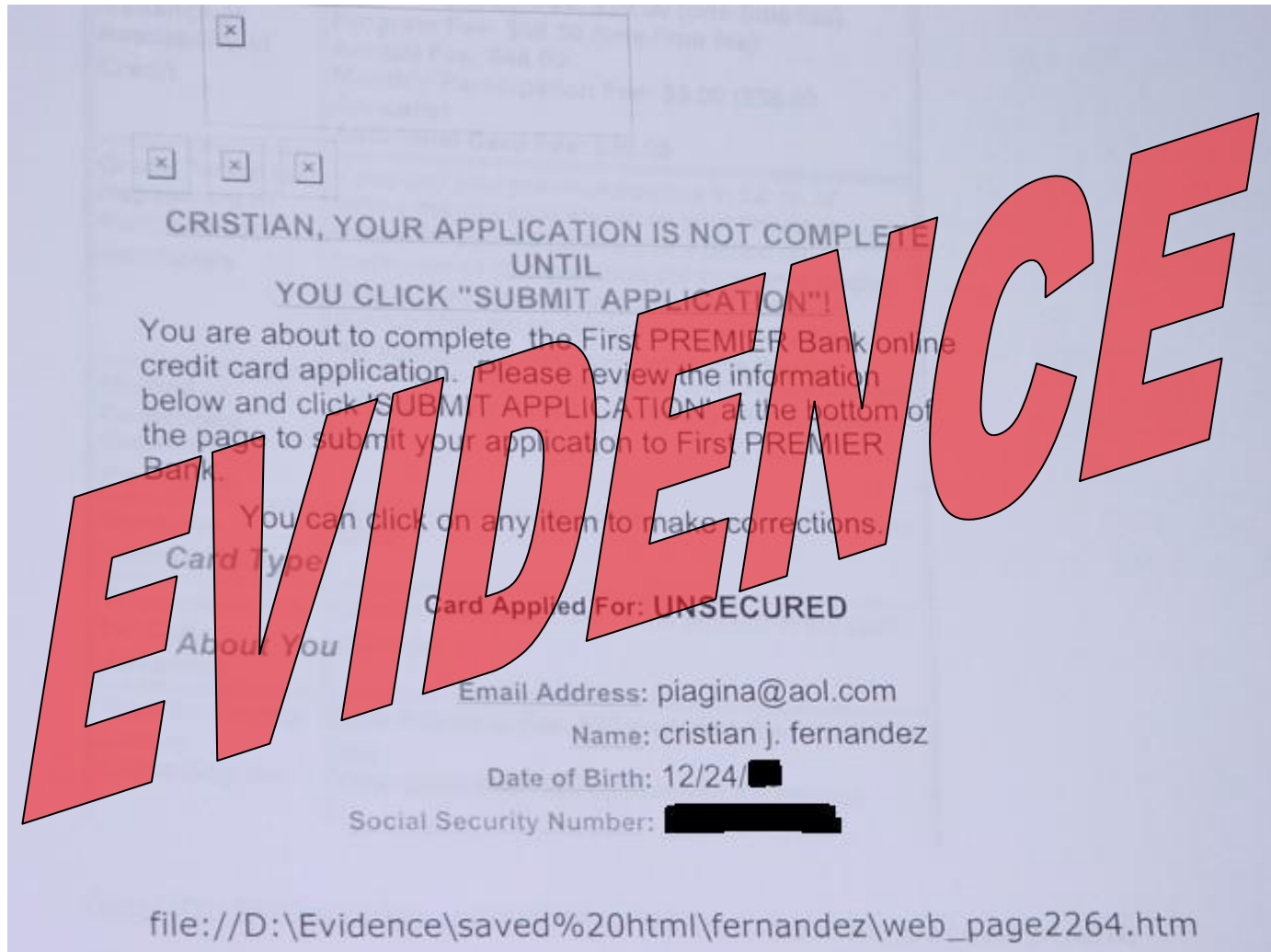
Deliveries occur Monday through Friday. Saturday delivery is available (except custom-built PCs) at an additional charge for orders placed before 9:00pm Eastern Time Thursday and Friday.



[sign up for newsletter](#)

[enter sweepstakes](#)

# HTML data from unallocated space Of online credit application



## Forensics Software Tools:

- Guidance Software's [EnCase](#) (commercial)
- Access Data [Forensic Toolkit](#) (commercial, runs in crippled mode without 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 frontend [Autopsy](#)
- Spada (Law Enforcement only, also a knock-off)
- AccessData's [FTK Imager](#) (does not require dongle)

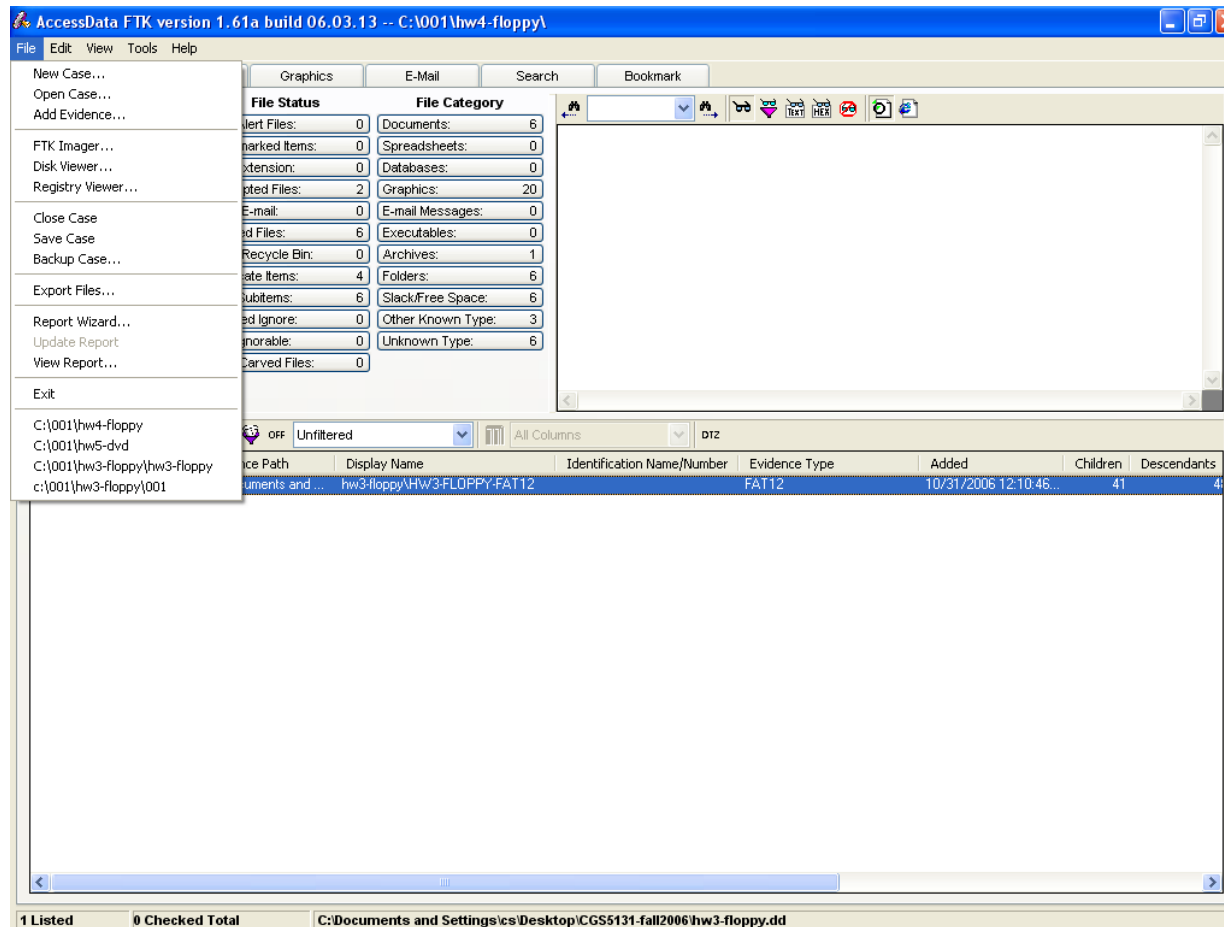


## Forensics Software Tools (cont'd):

- [Norton Utilities/SystemWorks](#) (DiskEdit is the primary one)
  - \* Unerase - in 2003 and earlier
  - \* Unformat - in 2003 and earlier
  - \* gDisk - in 2003 and earlier
- [WhatFormat](#): reads the header and tells the user what the file type is.
- [Quick View Plus](#): views many different file types (read-only)
- [FileAlyzer](#): a tool to analyze files
- [OmniXray](#), a disk editor utility that is a good replacement for DiskEdit for NTFS volumes
- [WinHex](#) and its [X-Ways Forensics](#) toolkit

# AccessData Forensic ToolKit (FTK) ([www.accessdata.com](http://www.accessdata.com)):

- a screenshot of FTK running with the security dongle attached:

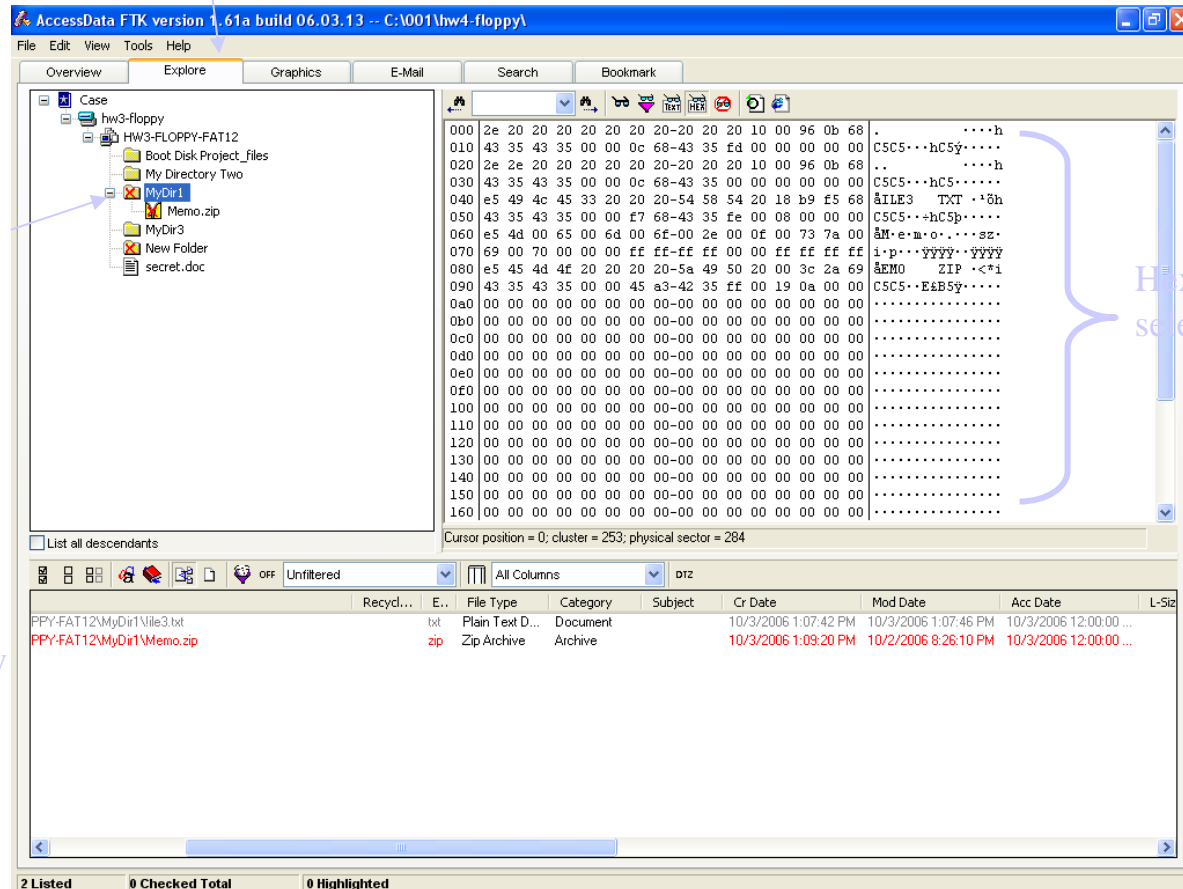


- Under the **Explore** tab, you can view the directory hierarchy, deleted files and folders, file contents (hex view), and file metadata (date/time stamps, types, disk addresses, sizes, hashes)

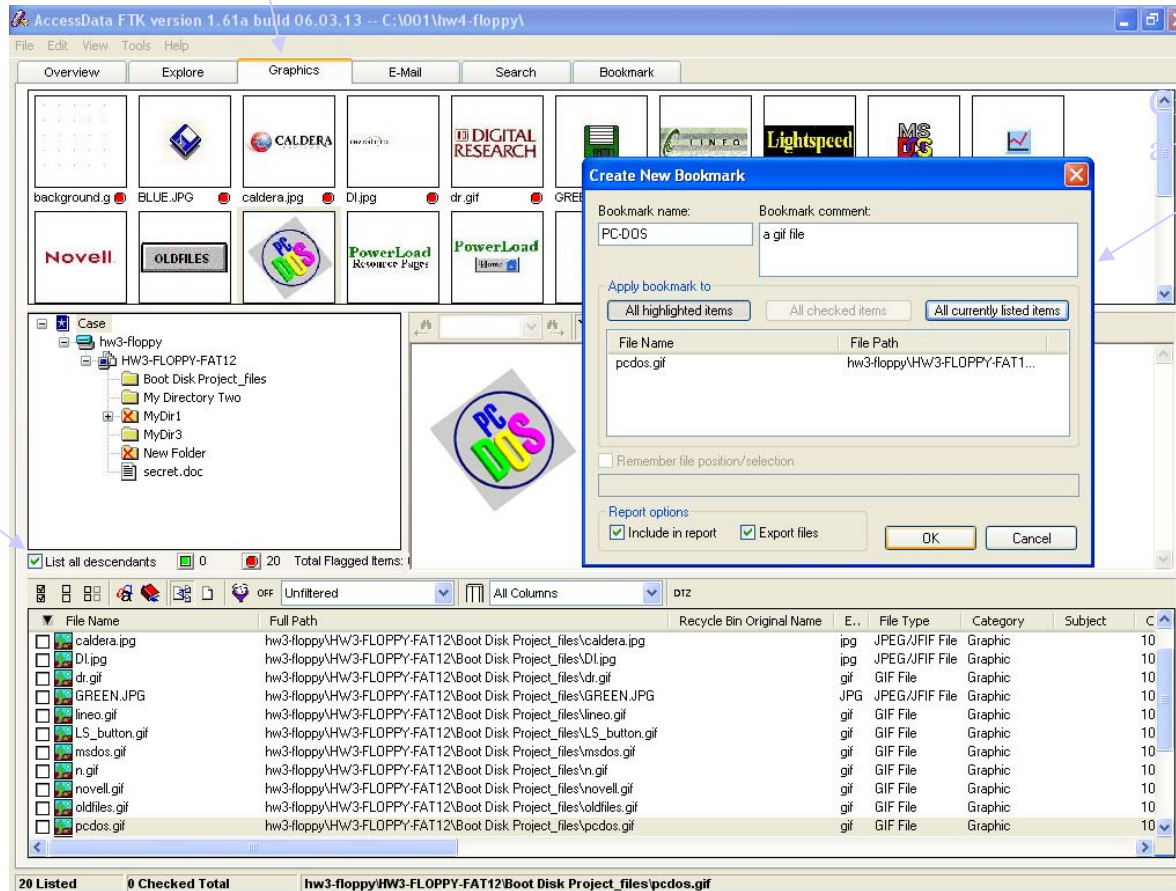
A selected folder

Hex view of the selected folder

Files under the selected directory



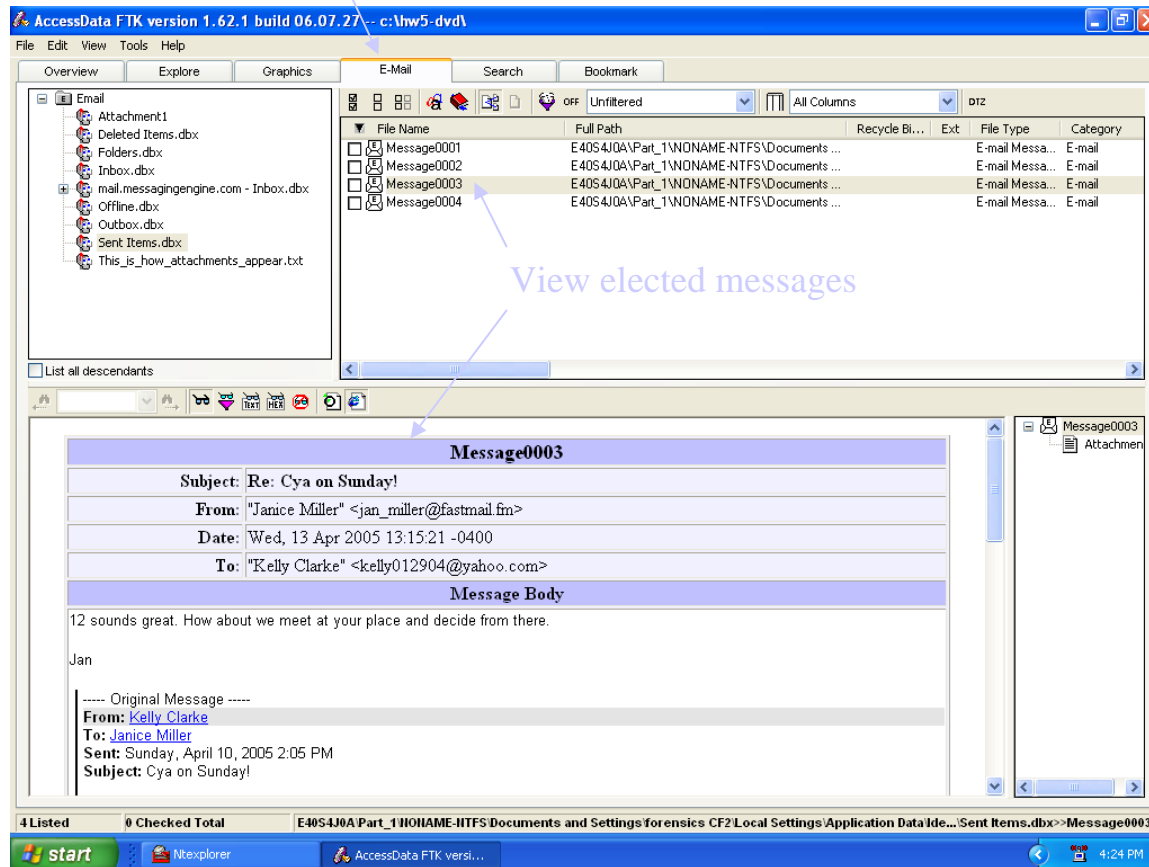
- Under the **Graphics** tab, you can preview pictures in a folder or on a drive when all file descendants are included; pictures may be bookmarked and included in the report



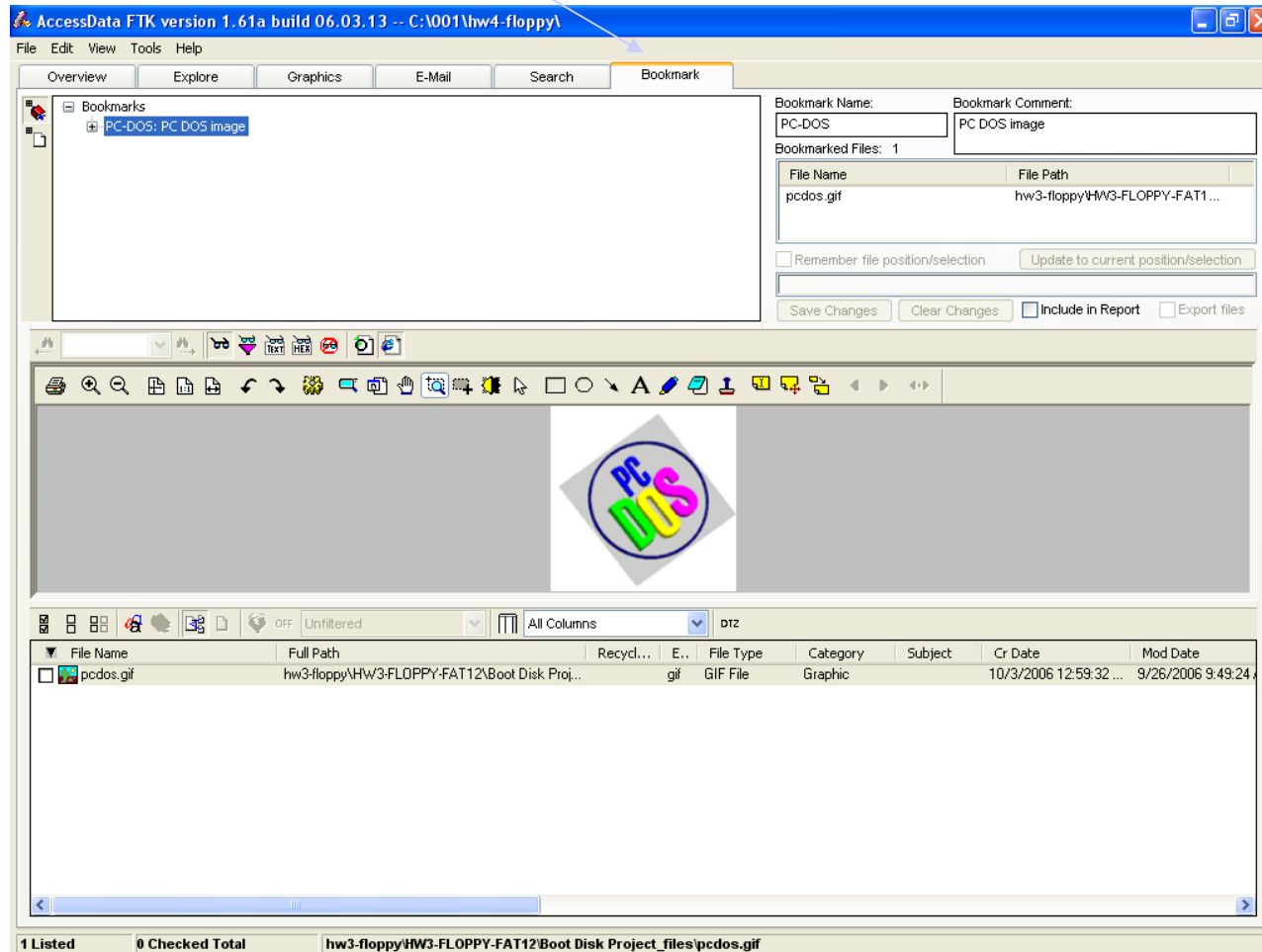
Check all descendants

Create bookmarks and add to the report

- Under the **E-Mail** tab, the left-hand box will list all of the e-mail boxes, the messages within a box, and the contents of each message (along with attachments).

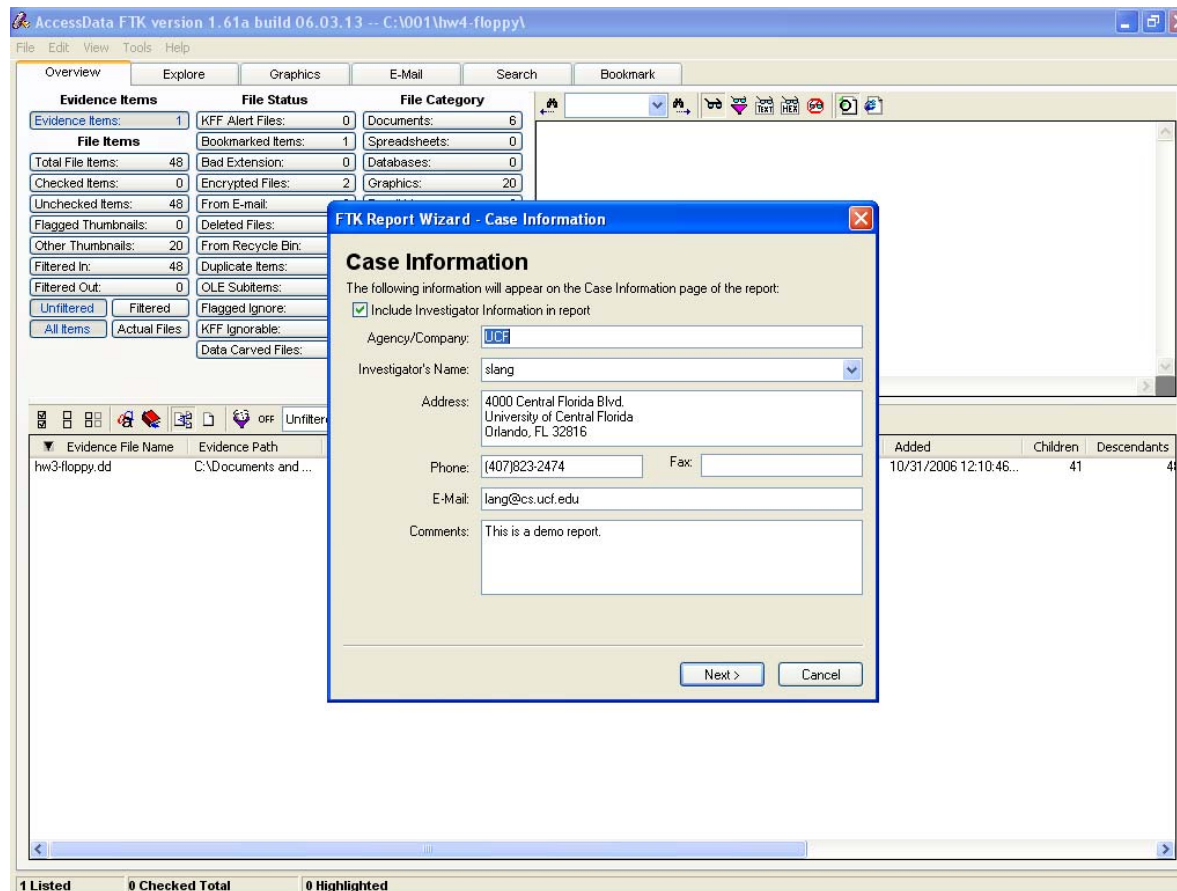


- Under the **Bookmark** tab, you can view the list of all files you have bookmarked including the descriptions.



Bookmark descriptions

- You can generate a report using the Report Wizard under the File option of the menu bar, from items that have been bookmarked with thumbnails, file paths, etc.



- The report is a HTML document that can be burned to CD as an auto-start CD that can be sent to an investigator or prosecutor. The recipient must have the correct software to run files included on the disk (e.g., they need Microsoft Word to view .doc files).

**FTK**  
CASE REPORT

Case Summary  
[Case Information](#)  
[File Overview](#)  
[Evidence List](#)

Supplementary Files  
[Case Log](#)

List by File Path  
- None -

MS Access database  
- None -

List File Properties  
[All Items](#)

Selected Bookmarks  
[Contents](#)  
[PC-DOS](#)

Selected Graphic  
Thumbnails  
- None -

### Case Information

10/31/2006  
**FTK Version** Version 1.61a, build 06.03.13  
**Case Number** 2006-Oct-31  
**Case Location** C:\001\hw4-floppy\  
**Case Description**  
**Report Created** Tuesday, October 31, 2006 4:50:38 PM

---

**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** This is a demo report.

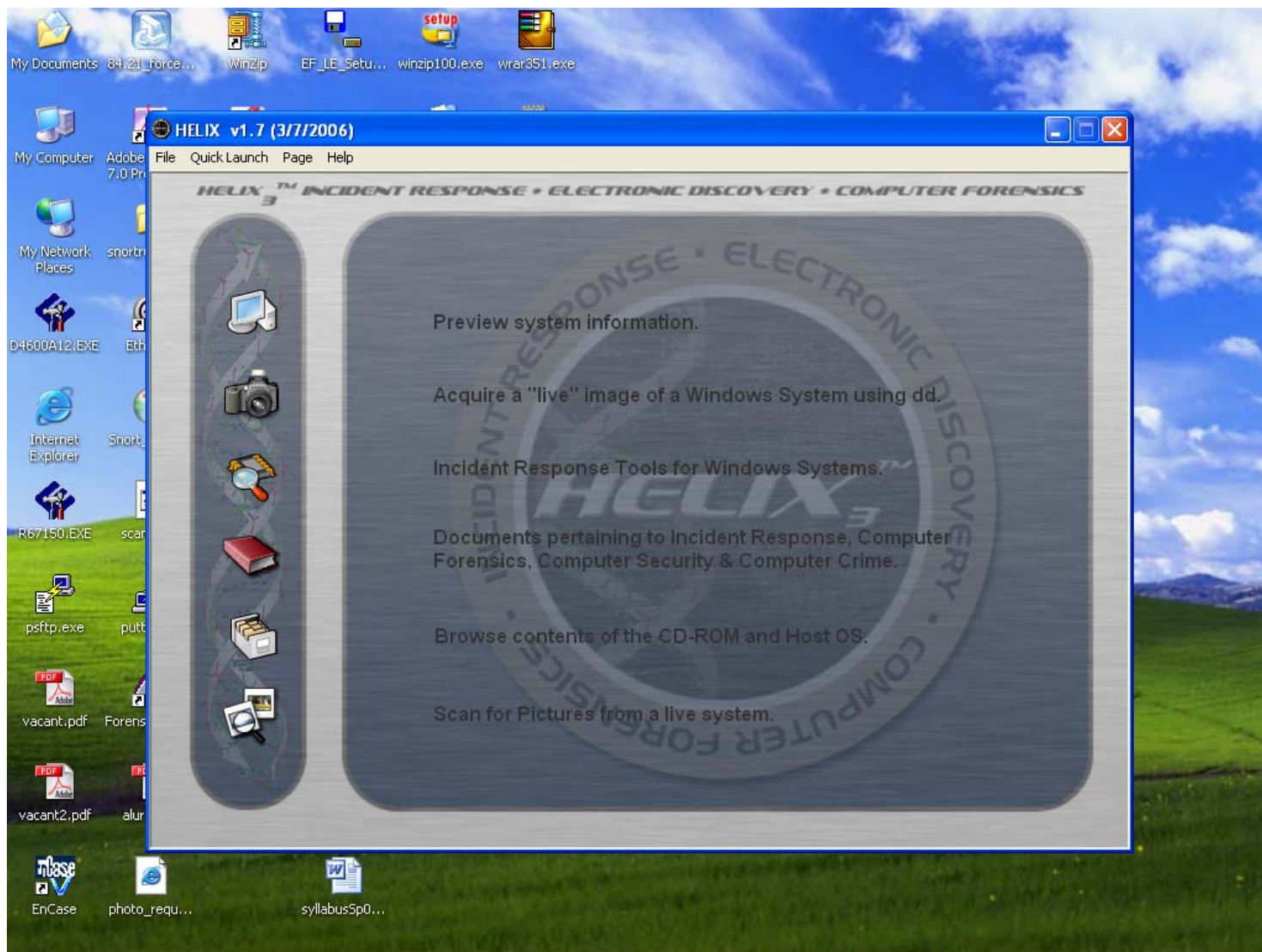
AccessData Forensic Toolkit



# Helix live system analysis (initial screen):



# Helix live system analysis (cont'd):

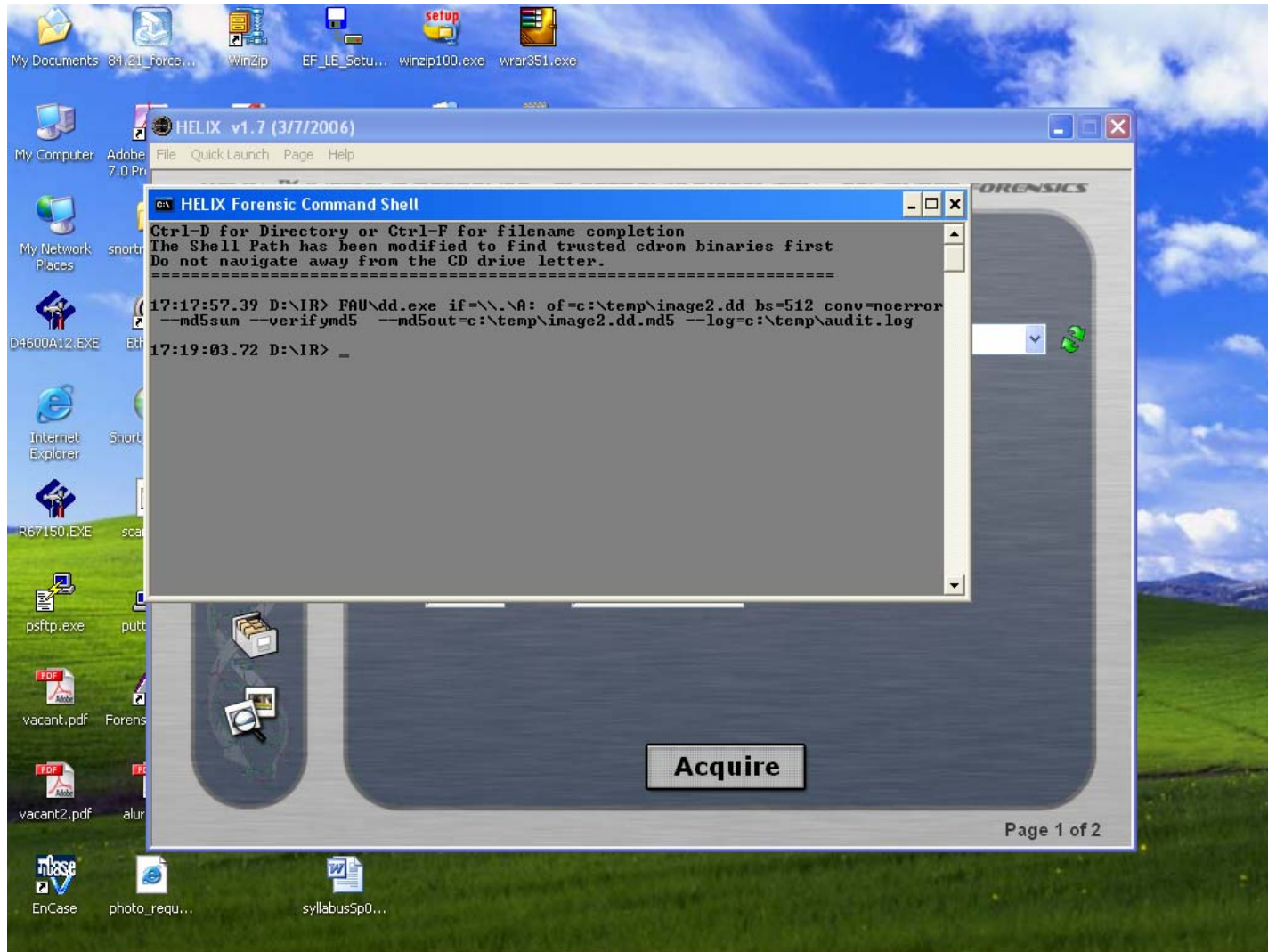


## Use Helix to image disk:

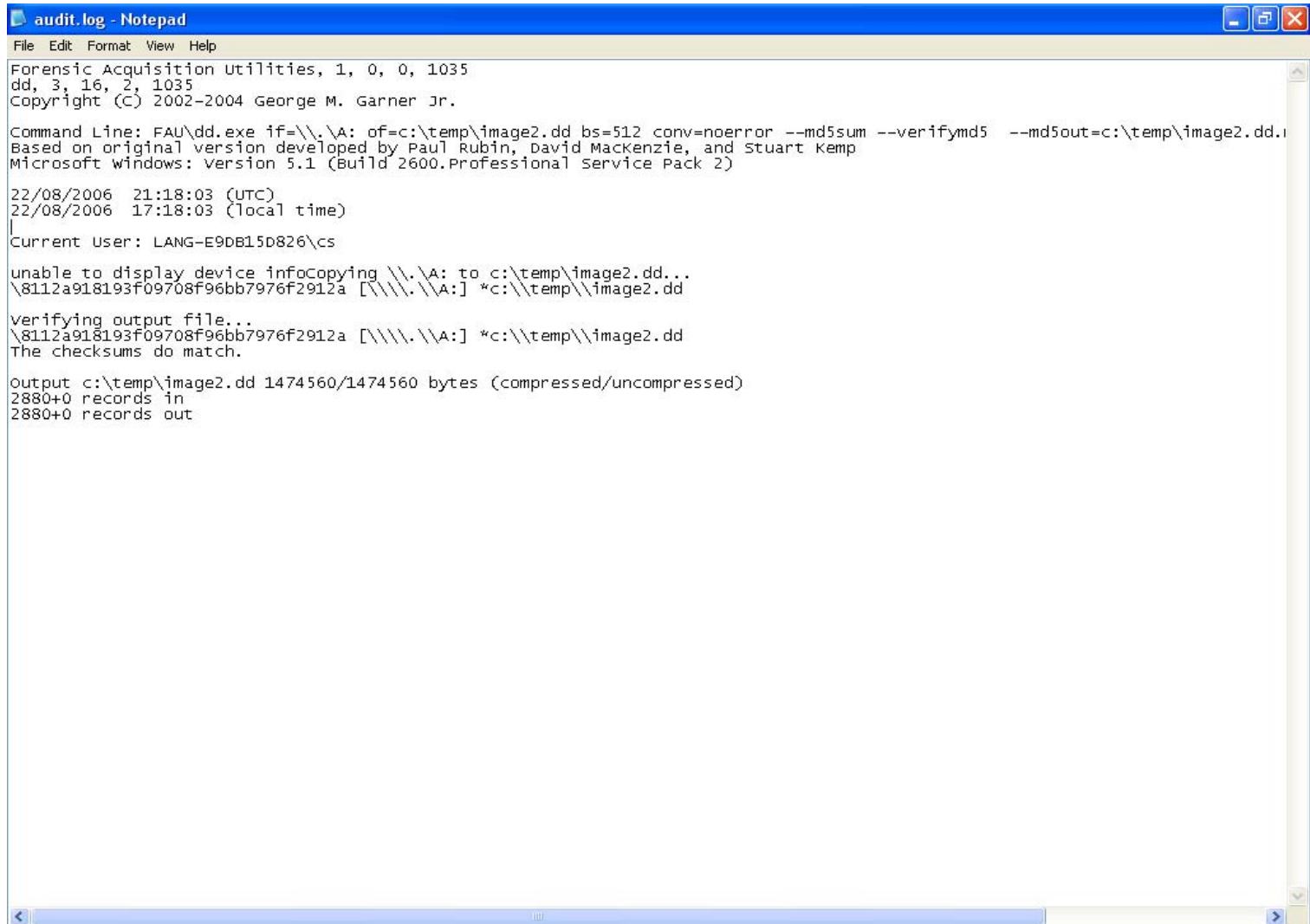
- dd (data dump) is used by helix to duplicate disks (see <http://www.softpanorama.org/Tools/dd.shtml> for explanation of the command syntax and options)



# Use helix to image a floppy disk:



# Audit.log file after dd is complete:



```
audit.log - Notepad
File Edit Format View Help
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 info copying \\.\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
```

## Relevance of Digital Forensics to Computer Science

- knowledge of computer hardware, networking, software, OS and file systems, and software tool development
- advanced topics in parallel processing (to handle large volumes of data), malware analysis (using reverse engineering, debugger and disassembler), security and cryptography (password cracking, wireless devices)

UCF's graduate programs in digital forensics:

- [GCCF](#) (Graduate Certificate in Computer Forensics) since fall 2001: 5 courses, 15 credit hours
- [MSDF](#) (Master of Science in Digital Forensics) since spring 2008: 10 courses, 30 credit hours