Computer Security: Digital Forensic Software Tools

Prof HS Venter
hventer@cs.up.ac.za
Department of Computer Science
University of Pretoria
Copyright © Venter (2015)
Agenda

- Security tools used in Digital Forensic operations
- Digital Forensic Tools Overview
- Hands-on Demonstrations of Forensic Tools
Security Tools used in Digital Forensic Operations
Core labs

- Email tracking
- Interviewing suspects and witnesses
- **Gathering physical evidence**
- **Gathering digital evidence**
- **Password cracking**
- Investigating log files
- **Imaging drives**
- **Extracting digital evidence**
- Investigating Web hacking incidents
- Restoring files
- Investigating wireless incidents
- Understanding biometric techniques…
Password Cracking – Definitions

• Hash Value – encrypted version of a password that can't be reversed
• Salt – Additional values added to the password during encryption so that two users with the same password don't generate the same hash value
• Weak Password – any password that can easily be guessed or cracked
• Strong Password – any password that is difficult to guess or crack
Password Cracking – Definitions

• Bad Password
  – Too weak for the resources it’s supposed to defend
  – Too difficult for users to use and remember

• Good Password
  – Sufficiently strong password
  – Reasonably easy to remember without having to be written down
• Password Cracking
  – The process of guessing, intelligently or non-intelligently, a plaintext password
  – Often aided by additional information
    • The encrypted password value or “hash”
    • The encryption algorithm used to encrypt the password
• Plaintext passwords are not stored
• A password is initially entered by a user and is encrypted with some one-way function $F$ to produce a “hash” value
• The hash value is stored in a password file
• When a user wants to be authenticated, they enter their password which is hashed with $F$
• The new hash is compared with the stored hash, if the hashes match access is granted
Password Cracking – Purpose

• Auditing
  – Penetration testing
  – Increase host/network security
    • If the good guys can crack a password, so can the bad guys
    • Automated password cracking increases chance the good guys will discover a bad password before bad guys get a chance
  – Enforcement of policy
Password Cracking – Purpose

- Computer and Network Forensics
  - Discover administrative passwords for later access to systems
  - Open locked files/folders on a seized system
  - Access logs of network-based hardware (IDS, Routers)
  - Passwords are often reused for other resources such as online email
Password Cracking – Forensic Scenarios

• First step: ask suspect(s) for password
• Most commonly performed on a forensic computer using commercial or free tools
• May be a trusted utility run from a forensic toolkit CD (if performed at the crime scene or on a seized computer)
• Necessary to use under special circumstances when a system or piece of hardware (e.g. router) has been seized, and the system administrators are non-cooperative
Password Cracking – Common Password Files

• Key to cracking passwords lies in obtaining the stored hash values
• Windows 9x
  – *.pwl (Password Lists)
• Windows NT/2000/XP/7/8 - SAM (Security Accounts Manager)
  – %WINDIR%\System32\config
  – %WINDIR%\System32\repair
• Linux/UNIX
  – /etc/passwd
  – /etc/shadow
Password Cracking – Methods

- Username crack
- Dictionary attack
- Hybrid attack
- Brute force
- Rainbow table attack
  - Uses a brute force approach, but is much faster
  - If encryption algorithm is known, hash values can be precomputed for all possible character combinations
  - Once the “rainbow table” is computed, cracking a password becomes at worst a linear search through the rainbow table
  - CPU time to compute rainbow table
  - Storage space typically > 50gb for a good table
Password Cracking – Tools

• Operating system-based (Windows, Linux, UNIX)
  – @stake LC5 (L0phtCrack)
  – John the Ripper
  – CAIN
  – ShowPass
  – Crack
  – Pwdump
  – Brutus
  – SamInside
  – RainbowCrack

• Application-based (MS Office, VNC, Messenger)
  – ElcomSoft
    • Office XP
    • Encrypted File System
    • Instant Messenger
  – Wide array of non-trusted applications
Password Cracking – References

http://www.symantec.com/
http://www.openwall.com/john/
http://packetstormsecurity.nl
http://www.microsoft.com/athome/security/privacy/password.mspx
http://mtechit.com/concepts/password.html
http://wikipedia.org
Phishing – what is it?

- A form of social engineering
- Attempt to fraudulently acquire sensitive information by masquerading as a trustworthy person or business
  - This is done via an apparently official electronic communication, such as an email
- The term phishing arises from the use of increasingly sophisticated lures to "fish" for users' financial information and passwords
Phishing

- Emails are sent out in mass quantities requesting personal information in the form of:
  - ID Number
  - Bank Account
  - PIN
  - Username/Passwords
### Is Phishing Spam?

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Spam</th>
<th>Phishing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery</td>
<td>Front door</td>
<td>Back door</td>
</tr>
<tr>
<td>Content</td>
<td>Unwanted</td>
<td>Wanted</td>
</tr>
<tr>
<td>Appeals to</td>
<td>Desire</td>
<td>Fear</td>
</tr>
<tr>
<td>Credibility attribute</td>
<td>Product</td>
<td>Brand</td>
</tr>
<tr>
<td>Results of action</td>
<td>Receive product</td>
<td>Loss of resources</td>
</tr>
<tr>
<td>Real purpose</td>
<td>Selling</td>
<td>Stealing</td>
</tr>
</tbody>
</table>
Phishing Methodology

• Step 1: Build credibility
  – Spoof a real company
  – Send from a spoofed company email address
  – Provide links to a real site for disclaimers, legalese, etc...

• Step 2: Create a reason to act
  – Proffer a plausible premise
  – Generate a sense of urgency
  – Require a quick response

• Step 3: Provide an avenue for action
  – Provide a good visual URL
  – Have a good hidden URL
Phishing Technology

- Phishing emails are generally delivered in HTML format
- URLs are “hidden” to fool the user into thinking they point to a legitimate site
- URL hiding is accomplished via
  - Link tricks
  - JavaScript
  - Misdirection
Phishing - URL Hiding

- **Link Tricks**
  - Credible IP string
    - Uses a credible looking text string within the URL
  - The @ sign
    - Everything to the left is forgotten, everything to the right is used
    - http://usbank.com/update.pl@12.3.4.5/usb/upd.pl
- **Long status line**
  - The URL is so long it can not be completely displayed in the status bar
  - Often combined with the @ trick
    - http://www.usbank.com/update/cust=90119323...
- **Similar names**
  - Uses a credible sounding, but fraudulent, domain name
  - http://www.ebay-secure.com/verify
Phishing – URL Disguising With @


• Display Link: http://internal/loginupdate.htm
• Status Bar: http://internal/login/update/accounts/sec...
• Reality: http://www.badstuff.com/index.html
• The simple redirect
  – Uses a “known” redirect to send the user to the phishing site
  – http://r.aol.com/cgi/redir?http://www.badstuff.com

• Wearing a mask
  – Uses a URL masking service such as cjb.net or tinyurl.com
  – http://tinyurl.com/5pzsc
Phishing – Fake Certificates

• The email has a fake “https://” address shown
• When the link is clicked the phisher pops up a “Security Alert” window
• Additional fake pop-ups appear if the “View Certificate” button is clicked
Tracing an Email

• To figure out where an email actually came from, you must view the email headers
• Different email programs have different ways of viewing the headers
• Most have an “Options” or “Settings” button to configure your personal settings
Tracing an Email

- To Display the Headers in Yahoo
  - Open the email to be viewed
  - Next click the “Full Headers” link at the bottom of the email
Yahoo Mail

Full Headers Link
Email Headers
• **X-Apparently-To:** theodoreward@sbcglobal.net via 68.142.199.140; …

• **X-Originating-IP:** [216.55.181.47]

• **Received:** from 207.115.57.54 (EHLO ylpvm23.prodigy.net) (207.115.57.54) by mta812.mail.scd.yahoo.com with SMTP; …

• **X-Originating-IP:** [216.55.181.47]

• **Received:** from mail5.zoneedit.com (mail5.zoneedit.com [216.55.181.47]) by ylpvm23.prodigy.net (8.12.10 083104/8.12.10) with ESMTP id k0PFu5R8021493 for <theodoreward@sbcglobal.net>; …

• **Received:** from EXE1.ad.okstate.edu (Exe001.ad.okstate.edu [139.78.102.207]) by mail5.zoneedit.com (Postfix) with ESMTP id 3F2DF4B3246 for <ted@astrocomma.com>; …
How to Trace an Email

• The important information is the originating IP address (139.78.102.207)
• If there are multiple IP addresses (e.g. 216.55.181.47) the further down it is the closer to the originating source it is
• The IP address at the bottom would be the source email server
• The source server is what you want to trace
How to Trace an IP Address

• Lookup the IP address using public sources
• Every IP address is assigned to an organization or individual
• These records are kept in a public database called WHOIS
• Ways to interact with this database
  – whois (unix)
  – Nslookup
  – http://www.arin.net/whois
  – http://www.dnsstuff.com
• Use nslookup to find basic information about a host
• Comes with most operating systems
Arin whois search
Whois Results

OrgName: Oklahoma State University
OrgID: OSU-7
Address: 407 Whitehurst
Address: Oklahoma State University
City: Stillwater
StateProv: OK
PostalCode: 74078
Country: US
NetRange: 139.78.0.0 - 139.78.255.255
CIDR: 139.78.0.0/16
NetName: OKSTATE
NetHandle: NET-139-78-0-0-1
Parent: NET-139-0-0-0-0
NetType: Direct Assignment
NameServer: NS.CIS.OKSTATE.EDU
NameServer: NS2.CIS.OKSTATE.EDU
Comment:

RegDate: 1990-02-12
Updated: 1998-06-05
RTechHandle: MM129-ARIN
RTechName: McCormick, Martin G.
RTechPhone: +1-405-744-6301
RTechEmail: martin@dc.cis.okstate.edu
OrgAbuseHandle: NSO-ARIN
OrgAbuseName: Network Security Officer
OrgAbusePhone: +1-405-744-6301
OrgAbuseEmail: abuse@okstate.edu
OrgTechHandle: MM129-ARIN
OrgTechName: McCormick, Martin G.
OrgTechPhone: +1-405-744-6301
OrgTechEmail: martin@dc.cis.okstate.edu
How to Trace an Email

• With this information I know OSU in Stillwater hosts this email server
• I now have the following contact information at the originating server
  – Name of a responsible individual
  – Phone number
  – Email address
How to Trace an Email

- What I wouldn’t know in the case of a spoofed email address, is who really sent the email
- The email server should have some logs that contain information connecting the email to the person that created the email
- Law enforcement would have to subpoena the information


Digital Forensic Tools Overview

• FTK
Hardware Requirements

PC Platform
- Mult-core CPU, 1TB HD, 8GB RAM, Gigabit Ethernet cards
  - Memory/card readers; wireless network cards

Hard Drives for Imaging
Forensics File Server (for project images)
  - Many Terabytes storage space
  - Memory/card reader; wireless network card
  - NICs (1 for lab, 1 for Internet)

Network switches
Wireless Access Point - 802.11g
Wireless NICs
Typical Lab Setup

COS 783

- Forensics 1
- Forensics 2
- Forensics 3
- Forensics 3
- Forensics 4

- Forensics 6
- Forensics 7
- Forensics 8
- Forensics 9
- Forensics 10

Hub

Forensics Server

Internet
Software Requirements

- NetBSD
- Windows
- Knoppix / Backtrack / KaliLinux
- EnCase
- ILook Investigator v8
- FTK: Forensics Tool Kit
- Various Public Domain/Security Tools
Forensic Toolkit (FTK)

- FTK (or UTK)
  - Access Data (www.accessdata.com)
  - Full functionality limited objects free version
  - Buy dongle for each station for full version
FTK Abilities

- Acquire from different image formats
- Powerful file filtering capabilities
- Powerful searching capabilities
- Recovery of deleted files and partitions
- Email and Internet investigation
- Identifying file signature inconsistencies
- Hash value creation
- External file viewers (over 270 file formats)
- Generates audit logs and case reports
FTK Specifications

• Runs in Windows 9x/Me/NT/2000/XP/7/8
• Accepts the following file systems:
  – NTFS
  – NTFS compressed
  – FAT 12/16/32
  – Linux ext2 & ext3
• Accepts the following image formats:
  – Encase
  – SMART
  – Snapback
  – Safeback (up to, but not including v.3)
  – Linux DD image
Hands-on Demonstrations of Forensics Tools

- Linux Forensics (DD)
- Windows Forensics (FTK)
• Three steps
  1. Acquire the evidence
     • Make a *forensically* sound image, OR
     • Preview the evidence without mounting disk or otherwise altering evidence (use a write-blocker)
  2. Authenticate the evidence
     • Verify the integrity of the copy
  3. Analyze the evidence
     • Logical analysis: From a file system viewpoint
     • Physical analysis: From a flat file viewpoint

• Linux supports both logical & physical analysis
• Demo… (Slides following are covered in demo)
'Forensically sound image' = exact physical duplicate
  - `dd` is a utility available with all Linux/UNIX distributions

• # `dd if=/dev/fd0 of=floppy.dd`
  - 'if' or 'input file' is the source of the bits
  - 'of' or 'output file' is the name of the file to be written

• How do I know the # drives? The # of partitions? The file systems involved?
  - `# fdisk -l`
  - `fdisk` is a utility used for partitioning.
    • NOT the same as `fdisk` that comes with DOS
### Linux Forensics – Acquire Evidence (DD)

```
[root@gheera root]# fdisk -l

Disk /dev/hda: 40.0 GB, 40016019456 bytes
16 heads, 63 sectors/track, 77536 cylinders
Units = cylinders of 1008 * 512 = 516096 bytes

<table>
<thead>
<tr>
<th>Device</th>
<th>Boot</th>
<th>Start</th>
<th>End</th>
<th>Blocks</th>
<th>Id</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/hda1</td>
<td>*</td>
<td>1</td>
<td>24385</td>
<td>12289693+</td>
<td>7</td>
<td>HPFS/NTFS</td>
</tr>
<tr>
<td>/dev/hda2</td>
<td></td>
<td>24385</td>
<td>40641</td>
<td>8193150</td>
<td>7</td>
<td>HPFS/NTFS</td>
</tr>
<tr>
<td>/dev/hda3</td>
<td></td>
<td>40642</td>
<td>40844</td>
<td>102312</td>
<td>83</td>
<td>Linux</td>
</tr>
<tr>
<td>/dev/hda4</td>
<td></td>
<td>40845</td>
<td>77536</td>
<td>18492768</td>
<td>f</td>
<td>Win95 Ext'd (LBA)</td>
</tr>
<tr>
<td>/dev/hda5</td>
<td></td>
<td>40845</td>
<td>75456</td>
<td>17444416+</td>
<td>83</td>
<td>Linux</td>
</tr>
<tr>
<td>/dev/hda6</td>
<td></td>
<td>75457</td>
<td>77536</td>
<td>1048288+</td>
<td>82</td>
<td>Linux swap</td>
</tr>
</tbody>
</table>

Disk /dev/hdb: 200.0 GB, 200049647616 bytes
255 heads, 63 sectors/track, 24321 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

<table>
<thead>
<tr>
<th>Device</th>
<th>Boot</th>
<th>Start</th>
<th>End</th>
<th>Blocks</th>
<th>Id</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/hdb1</td>
<td>*</td>
<td>1</td>
<td>11475</td>
<td>92172906</td>
<td>7</td>
<td>HPFS/NTFS</td>
</tr>
<tr>
<td>/dev/hdb3</td>
<td></td>
<td>11476</td>
<td>16709</td>
<td>42042105</td>
<td>c</td>
<td>Win95 FAT32 (LBA)</td>
</tr>
<tr>
<td>/dev/hdb4</td>
<td></td>
<td>16710</td>
<td>24321</td>
<td>61143390</td>
<td>f</td>
<td>Win95 Ext'd (LBA)</td>
</tr>
<tr>
<td>/dev/hdb5</td>
<td></td>
<td>16710</td>
<td>24321</td>
<td>61143358+</td>
<td>7</td>
<td>HPFS/NTFS</td>
</tr>
</tbody>
</table>
```

Linux Forensics – Complete example of Acquisition

```
[root@gheera root]# script evidence.notes
Script started, file is evidence.notes
[root@gheera root]# date
Wed Mar 3 11:32:20 CST 2004
[root@gheera root]# dd if=/dev/fd0 of=floppy.dd conv=noerror,notrunc, sync
2880+0 records in
2880+0 records out
[root@gheera root]# md5sum /dev/fd0 > evidence.md5
[root@gheera root]# md5sum floppy.dd >> evidence.md5
[root@gheera root]# cat evidence.md5
df68d978ca0872223ccfd6d6e26eb1dd  /dev/fd0
df68d978ca0872223ccfd6d6e26eb1dd  floppy.dd
[root@gheera root]# date
Wed Mar 3 11:34:48 CST 2004
[root@gheera root]# Script done, file is evidence.notes
[root@gheera root]#
```
Different types each with different advantages & disadvantages

- Direct connection
  - Connect drive directly to IDE ribbon cable
  - Fast
- External HD case
  - Fast if used with Firewire
- Network acquisition
  - Connect computer with cross-over cable
Write-block is necessary for imaging under Windows.
Direct IDE connection

No write-blocker necessary if imaging under Linux
External Firewire drive connector
Linux Forensics (2) – Authenticate the evidence

- # md5sum /dev/fd0 > evidence.md5
  - Generate a one-way hash of the (original) floppy, redirect to a file.
- # md5sum floppy.dd >> evidence.md5
  - Do the same for our bit image copy, append the value to our evidence.md5 file
- # cat evidence.md5
  - Are they the same? Good!
- # date
  - Other side of the sandwich
• File system maximum file sizes
  – FAT32 = 4 GB, NTFS = 2 Terabytes
  – EXT2/3 = 2 Terabyte, ReiserFS = 1 Exabyte

(LFS) Large Files System support must be compiled in.

• Easy to copy files to and from FAT32 drive
  • Limited to 4GB, very small?

• How to copy a very large file from Linux to an NTFS volume
  • Not well supported by Linux, but getting better
  • Supported by some 3rd party commercial drivers
• Logical
  – From a file system viewpoint
    • Folders/directories, files, etc.
  – View files, contents, capture metadata
  – Create time line: who did what and when?

• Physical
  – From a flat file viewpoint
  – There are no 'files' or 'folders'
  – Can view hidden systems areas
    • MBR, VBR, FAT, MFT, root directory, slack, unallocated, etc.
  – Can (manually) seek out and recover deleted files
Types of Analysis

- Logical View
- Physical View
Linux Forensics – References

- Free Linux distributions
  - Fedora Core (based on Redhat)
    - fedora.redhat.com
  - FIRE: Forensic Incident Response Environment
    - fire.dmzs.com
  - Knoppix (bootable CD, HD installable)
    - www.knoppix.org
FTK – Before starting the tool!

• Crime Scene Investigation
  – Students Should have Already Learned Crime Scene Acquisition Procedures
    • Evidence Preservation
    • Chain of Custody
    • Bagging and Tagging
    • Evidence Storage
    • Interviewing Procedures

• Media Preparation
  – Evidence Floppies and Hard Drives
• Creating a Case in FTK
  – Investigator Information
    • Case Number
    • Crime Scene Data
    • Bookmarks
  – Acquisition
    • Evidence Preservation
    • Chain of Custody
    • Evidence Lockers
    • Evidence Logs
Getting Started with FTK

• Creating a Case in FTK
  – Analysis
    • File Analysis
    • Searches
    • Findings
  – Reporting
    • Case Information
    • Easily Understood Format
    • Concise Reporting Procedures
Getting Started with FTK

- Demo…
- The next number of slides gives an idea of this demo
• FTK will prompt to assign a number, name, and path to the case
Continue Wizard

- Forensic Examiner Information Screen
- Fill in your information
- Will be used in report later
The investigator then selects case logging options.
The investigator selects which items will be added to the evidence and what kind of files will be indexed.
Refine Case - Defaults

In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.

Unconditionally Add
- File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
- Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
- KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
- Extract files from KFF ignorable containers

Conditionally Add
Add other items to the case only if they satisfy BOTH the file status and the file type criteria

File Status Criteria
- Deletion Status:
  - Deleted
  - Not deleted
  - Either
- Encryption Status:
  - Encrypted
  - Not encrypted
  - Either
- Email Status:
  - From email
  - Not from email
  - Either

File Type Criteria
- Documents
- Spreadsheets
- Executables
- Archives
- Databases
- Folders
- Graphics
- Other Known
- Email msgs
- Unknown

Options:
- Include All Items
- Optimal Settings
- Email Emphasis
- Text Emphasis
- Graphics Emphasis

Next >
Refine Case - Defaults

Refine Index - Default

In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude items from being indexed, make any changes to the settings below. Note: any items that don’t get indexed initially can be indexed later by clicking on “Analysis Tools” under the “Tools” menu item.

Unconditionally Index

- File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
- Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
- KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)

Conditionally Index

Index other items in the case only if they satisfy BOTH the file status and the file type criteria.

File Status Criteria

- Deletion Status:
  - Deleted
  - Not deleted
  - Either

- Encryption Status:
  - Encrypted
  - Not encrypted
  - Either

- Email Status:
  - From email
  - Not from email
  - Either

- Duplicate Files

File Type Criteria

- Documents
- Spreadsheets
- Executables
- Archives
- Databases
- Folders
- Graphics
- Other Known
- Email msgs
- Unknown

< Back  Next >  Cancel  Help
Adding Evidence

- Choices: Drive image, local drive, directory, or individual file
Add Evidence

• Select Type

• Continue

• Fill in applicable information

• ...Next...Finish
• Interface Overview
  – Investigator will Become Familiar with GUI Interface
    • Different Panes and Viewers
Overview Window

Viewer Toolbar
General Case Information
File List Toolbar
File List

COS 783
Using FTK

- Evidence Floppies
  - Investigator Learns to Add Evidence to a Case
  - Step Through Acquisition of Evidence
  - Investigators Should Use Viewers, File Filters, and Different Tabs in FTK
Using FTK

- **Imaging**
  - Floppy
    - Investigators Image Floppy Using FTK Imager
    - Hashes Used to Verify Information Integrity
  - Hard Drive
    - Investigators Image Small Hard Drive
    - Hashes Used to Verify Information Integrity

- **Viewing Evidence**
  - Investigators Take Acquired Images From Previous Example
  - Images are Viewed Using FTK Viewers
  - Files are Searched for Specific Information
Overview Window

[Image of the AccessData FTK interface]

- General Case Information
- File List Toolbar
- Viewer

Note: The diagram shows the interface of AccessData FTK, including various tools and sections for managing evidence and files.
Explore Window

Neutron Stars

Neutron stars are about 10 km in diameter and have the mass of about 1.4 times that of our Sun. This means that a neutron star is so dense that on Earth, one teaspoonful would weigh a billion tons! Because of its small size and high density, a neutron star possesses a surface gravitational field about 300,000 times that of Earth.
Graphics Window
E-Mail Window

- File List Toolbar
- File List
- Tree View
- Tree View Toolbar
- Viewer Toolbar
- Viewer
- Attachment List
Search Window

Search Tabs
Search Form
Viewer Toolbar
Viewer
File List Toolbar
File List
Search Results List
Live Search

Search Tabs
Search Form
Viewer Toolbar
Viewer
File List Toolbar
File List
Search Results List
Bookmark Window

Bookmark List
Bookmark Toolbar
Viewer Toolbar
Viewer
File List Toolbar
File List

Bookmark Information

AccessData FTK version 1.33 build 01.07.15 -- C:\Cases\Acct_Co\ 

File Name | Full Path | Recycle | File Type | Ext | Category | Subject
--- | --- | --- | --- | --- | --- | ---
fireball.jpg | messier\Part_2NNTFS-NNTFS\DriveFreeSpace11... | JPEG/JFIF File | pg | Graphic |
M20 - Trifid Nebula | messier\Part_1\FAT32\FAT32\Messier_ObjectsA... | Folder | Folder |
M31 - Andromeda Galaxy | messier\Part_1\FAT32\FAT32\Messier_ObjectsA... | Folder | Folder |
Report Wizard

- Lets you choose various file attributes to add to report
- Will add thumbnails to the report for important images
- Add special emphasis to bookmarked items.
- Report is in HTML format
Case Information

Oct 26, 2003
FTK Version: Version 1.33, build 03.07.16
KFF Version: Unknown
Case Number: 2
Case Location: F:\stewie\
Case Description: Test
Report Created: Oct 26, 2003 9:58pm
Investigator: Pedro
Agency: Find Stuff, Inc.
Address: 34345 blah blah
Tulsa, OK 74104
Phone: 918-555-1212
Fax: 
Email: nomail@findstuff.com
Comments: 

AccessData Forensic Toolkit
Example Report

COS 783

[Image of FTKReport software interface showing file paths and images]
Example Report
• Digital Forensics is a broad field
  – Includes traditional forensic steps
  – Not just tool-oriented
• Use a vast combination of tools and experience
• Follow the digital forensic investigation process for evidence to be admissible in a court of law!
Assignment 3

• Create a text document and save your name and student number in it. Zip the file and place the password zip_studentNumber_pass on the zip file.
• Do the same with an Excel document with the password sheet_studentNumber_pass on the file.
• Find the password footprints of these passwords in the RAM. You need to do several experiments such as the footprints just after putting the passwords on the file, all at once, separately, rebooting and just opening the documents with the passwords etc.
Assignment 3

• The more experiments you do, the more marks you will get (10)
• The more footprints you can show, the better (10)
• Generalise about the patterns you can find about the passwords, e.g. location, artifacts on how to identify them (e.g. always preceded/after a certain sting? Always ‘near’ a certain ‘block’ of code?) (20)
• Write up your findings in a report of no more than 10 pages including screenshots etc. (10)
• Total: 50, deadline: 30 Sept ‘15, 12:00pm
• Demo: 30 September 2015, 16:30-18:30 in class