Digital Forensics

Tools & Identification

Objectives:

- Understand that methodology and technical knowledge is what makes up Forensics
- Introduce a few Commercial / Open Source Forensics Tools such as EnCase, FTK, and Helix.

What is Digital Forensics?:

- A collection of specialized techniques, processes, and procedures used to preserve, extract, analyze, and present electronic evidence.
- A methodology for computer investigation and analysis techniques in the interest of determining potential legal evidence.

- It isn’t like CSI – it takes time and attention to detail.

Forensics:

Important Questions:

- Does the analyst have the technical background to support the results of their investigation?
- Have they properly authenticated their results?
- Was a sound investigation performed from start to finish?

Forensic Techniques:

Was the evidence gathered and verified in a sound manner?

One of the tenets of digital forensics is to assure that the original media is not altered, and that the methods used to create forensic quality copies of media and data assure that the integrity of the original is maintained. [1]

Forensic Techniques:

Was a chain of custody maintained?

- All media, documents, and evidence related to a case or situation should be kept in your custody and closely controlled.
- Only those that have a right to see the information should see it and have access to it.

Forensic Techniques:

Is the ownership and licensing appropriate for the tools used?

- Whatever software is used for the technical processing needs to be registered and properly licensed to protect the integrity of your investigation.

Forensic Techniques:

Can the results of the technical analysis be duplicated using other tools?

- Once evidence has been extracted and will be used in some type of proceeding, it needs to be authenticated using other tools.
- Can other software tools obtain the same results?
- Builds your creditability and adds support to your case.

Forensic Techniques:

Do other professionals use the same techniques and methodology?

- If you are doing digital forensics related work and truly know what you are doing, you are using techniques that other professionals use.
- Think about having to explain to a jury how your homegrown tool works...

Forensic Techniques:

Is the Analyst technically capable of defending/supporting their interpretation of the evidence?

- Methodology and technical knowledge is important. Only depending on one tool could lead to failure
- Experience forensic practitioners will use additional tools to authenticate the results of the primary tool

Tools:

Does the Tools Really Matter?

Dr. Peter Stephenson -

“Essentially, incident management is a forensic problem. That challenge demands a serious toolkit of computer forensic, network-enabled forensic, network forensic and analytical tools.” [1]

Different Views:

Steve Hailey -

> "If the tools being used are the mechanism to find evidence on a computing device, and several different tools can replicate the process, then it doesn't matter what tools were used." [2]

Tools:

Most have the same underlying principles:

- Creating forensic quality or sector-by-sector images of media
- Locating deleted/old partitions
- Ascertaining date/time stamp information
- Obtaining data from slack space
- Recovering or "un-deleting" files and directories "Carving" or recovering data based on file headers/file footers
- Performing keyword searches
- Recovering Internet History information

Tools:

Commercial:

- Pros: Great Quality Software
  - Provides many forms of support “Security Blanket”
- Cons: Expensive / Additional features Cost

Open Source:

- Pros: Free – Offers Advanced Features
  - Enhancements are faster
- Cons: No Direct Support
  - Everything is Message Boards or Email.

Tools:

Encase (Commercial)

By: Guidance Software

- Recognized as a court-validated standard in computer forensics software
- Encase is the most commonly use forensics software by the forensics community
- Guidance consulting service
- Encase training seminars and certifications

Encase:

Products:

- Encase Enterprise - Enterprise-wide investigations. Requires a servlet on the client system
- Field Intelligence Model - network-based investigations. Pushes out a servlet on the client system
- Encase Forensic - local investigations

Encase:

Image acquisition:

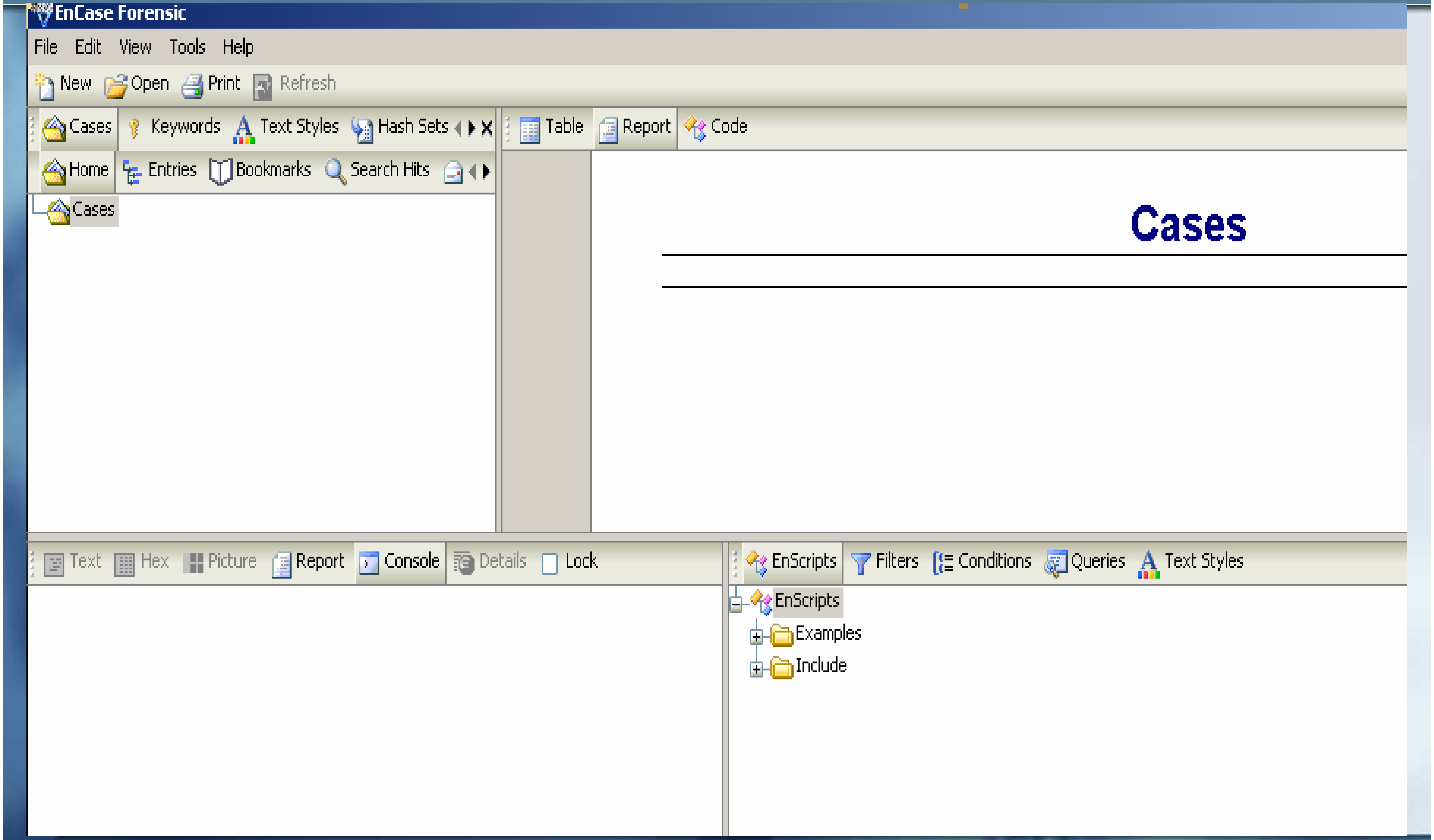
- Bit-by-bit image acquisition (Fastblock) and evidence preservation
- Imaging and analysis of RAID arrays
- Acquire by Boot CD / Disk
- Cross-Over cable to PC
- VMWARE, DD, Safeback v2 Images
- Analyze / Acquire some encrypted volumes

Encase:

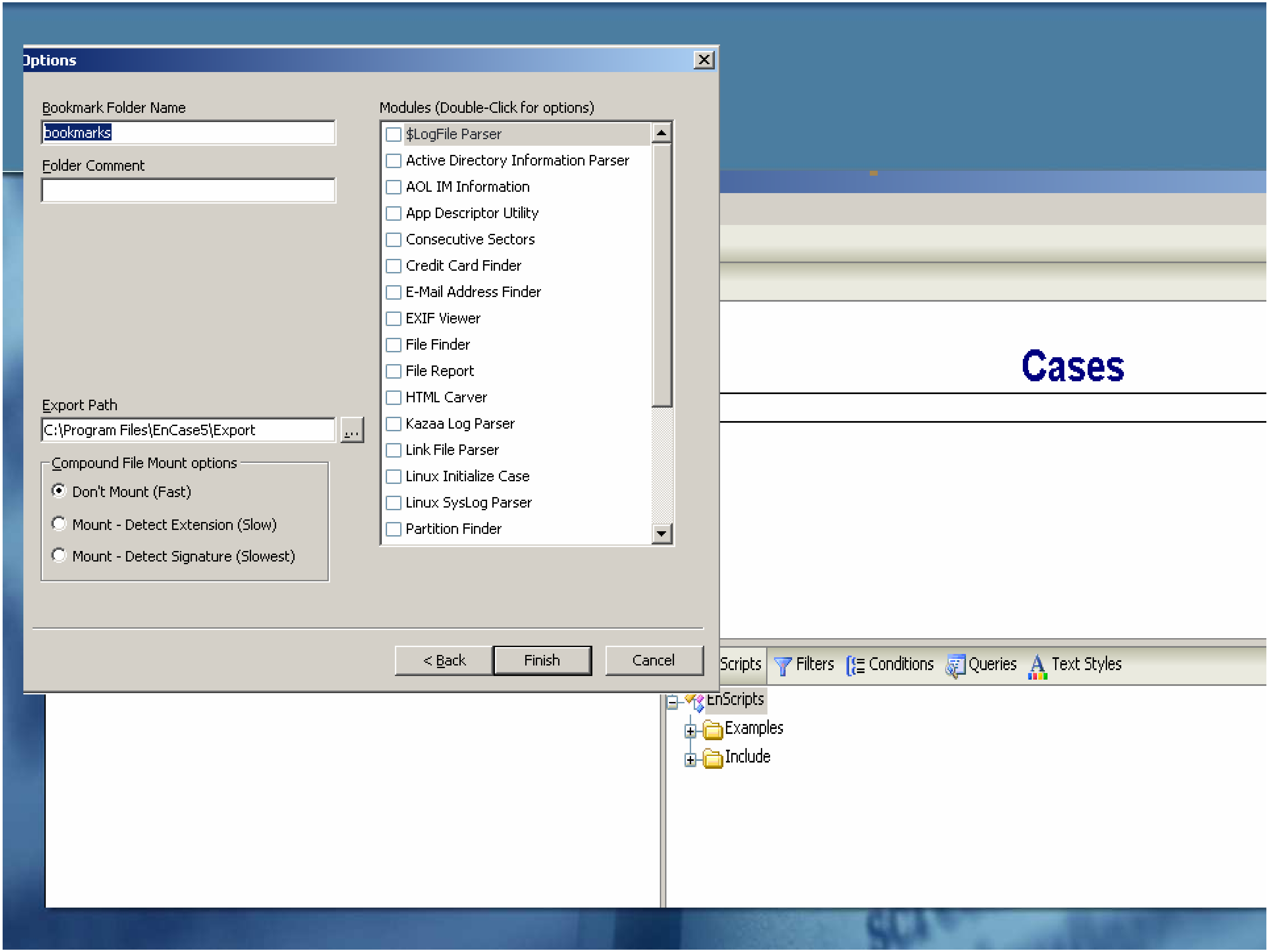
What can it do?

- File signature analysis
- Filter conditions and queries
- View deleted files and file fragments in unallocated or slack space
- Folder recovery
- Log file and event log analysis
- File type search
- Registry viewer, external file viewer

Encase:



EnCase Forensic
File Edit View Tools Help
New Open Print Refresh
Cases Keywords Text Styles Hash Sets
Home Entries Bookmarks Search Hits
Cases
Table Report Code
Cases
Text Hex Picture Report Console Details Lock
EnScripts Filters Conditions Queries Text Styles
EnScripts
Examples
Include



Options

Bookmark Folder Name: bookmarks

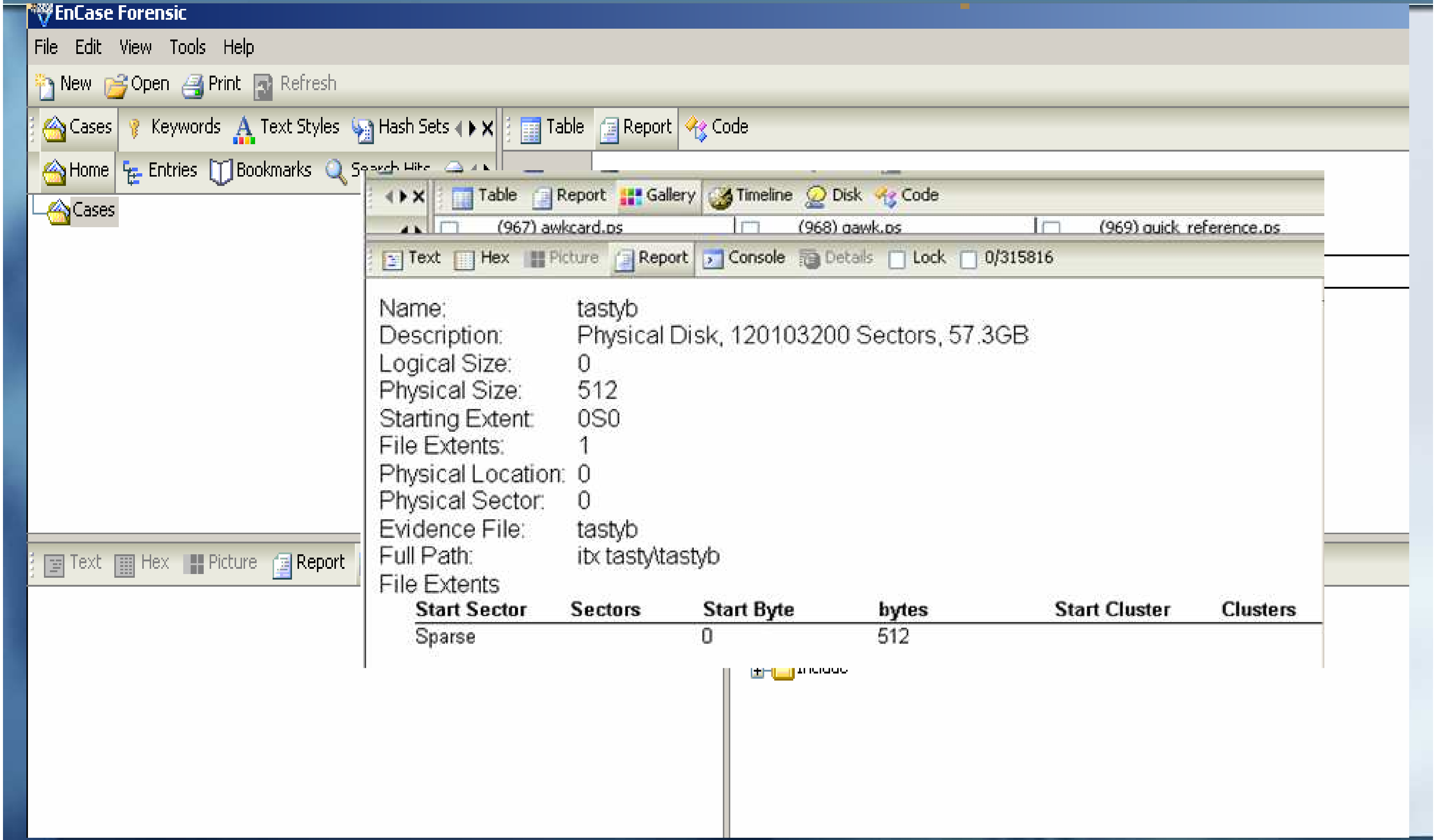
Folder Comment:

Export Path: C:\Program Files\EnCase5\Export

Compound File Mount options
- ● Don't Mount (Fast)
- ○ Mount - Detect Extension (Slow)
- ○ Mount - Detect Signature (Slowest)

Modules (Double-Click for options)
- □ $LogFile Parser
- □ Active Directory Information Parser
- □ AOL IM Information
- □ App Descriptor Utility
- □ Consecutive Sectors
- □ Credit Card Finder
- □ E-Mail Address Finder
- □ EXIF Viewer
- □ File Finder
- □ File Report
- □ HTML Carver
- □ Kazaa Log Parser
- □ Link File Parser
- □ Linux Initialize Case
- □ Linux SysLog Parser
- □ Partition Finder

Encase:


EnCase Forensic
File Edit View Tools Help
New Open Print Refresh
Cases Keywords Text Styles Hash Sets
Table Report Code
Home Entries Bookmarks Search Hits
Cases
Table Report Gallery Timeline Disk Code
(967) awkcard.ps
(968) gawk.ps
(969) quick_reference.ps
Text Hex Picture Report Console Details □ Lock □ 0/315816
Text Hex Picture Report

Name: tastyb
Description: Physical Disk, 120103200 Sectors, 57.3GB
Logical Size: 0
Physical Size: 512
Starting Extent: 0S0
File Extents: 1
Physical Location: 0
Physical Sector: 0
Evidence File: tastyb
Full Path: itx tasty\tastyb

File Extents

Start Sector	Sectors	Start Byte	bytes	Start Cluster	Clusters
Sparse		0	512		

Tools:

- FTK IMAGER:
  - Less than 7 MB / Stored on USB Key/Drive
  - Acquire locked system files (SAM / SYSTEM / NTUSER)
  - MD5 and SHA1 Hashing for verification
  - Preview media (thumbnail views, keyword searches, properties)

Site:
http://www.accessdata.com/products/imager/

Tools:

Helix 1.8:

- Ultimate Open Source Forensic Tool
- Two Great Features:
  - Windows Side (Menu Driven)
  - Linux Side (Live CD)

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

Tools:

LiveView: (Open Source)

- Java-based Windows forensics tool that creates a VMware virtual machine out of a raw (dd-style) disk image or physical disk.
- Its still in **beta** but has many possibilities.
- Site: http://liveview.sourceforge.net/

Great Reference:

- Forensic Focus www.forensicfocus.com
- A web site dedicated to forensic investigation and incident response. The message boards are filled with great information and the members range from professionals to those new to the field of computer forensics.

Learn:

- Ask yourself the very few questions about forensic methodologies and techniques. This will help you as a Forensics Examiner

- Try not to get too dependent on one tool. Use a combination of them to become familiar what they have to offer

Questions:

Contact:

Jesse Crim, MSIA
Information Security Analyst
Virginia Commonwealth University
Email: jcrim@vcu.edu
Office: #804-827-1074