MIS 5208 - Lecture 12 – Investigation Methods – Data Acquisition

Ed Ferrara, MSIA, CISSP
eferrara@temple.edu

TEMPLE UNIVERSITY

Objectives

- List digital evidence storage formats
- Explain ways to determine the best acquisition method
- Describe contingency planning for data acquisitions
- Explain how to use acquisition tools
- Explain how to validate data acquisitions
- Describe RAID acquisition methods
- Explain how to use remote network acquisition tools
- List other forensic tools available for data acquisitions

Digital Evidence Storage Formats

- Data in a forensics acquisition tool is stored as an image file
- Three formats
  - Raw format
  - Proprietary formats
  - Advanced Forensics Format (AFF)

Raw Format

- Makes it possible to write bit-stream data to files
- Advantages
  - Fast data transfers
  - Ignores minor data read errors on source drive
  - Most computer forensics tools can read raw format
- Disadvantages
  - Requires as much storage as original disk or data
  - Tools might not collect marginal (bad) sectors

Proprietary Formats

- Most forensics tools have their own formats
- Features offered
  - Option to compress or not compress image files
  - Can split an image into smaller segmented files
  - Can integrate metadata into the image file
- Disadvantages
  - Inability to share an image between different tools
  - File size limitation for each segmented volume
- The Expert Witness format is unofficial standard

Advanced Forensics Format

- Developed by Dr. Simson L. Garfinkel as an open-source acquisition format
- Design goals
  - Provide compressed or uncompressed image files
  - No size restriction for disk-to-image files
  - Provide space in the image file or segmented files for metadata
  - Simple design with extensibility
  - Open source for multiple platforms and OSs

Advanced Forensics Format

- Design goals (cont'd)
  - Internal consistency checks for self-authentication
- File extensions include .afd for segmented image files and .afm for AFF metadata
- AFF is open source

Determining the Best Acquisition Method

- Types of acquisitions
  - **Static acquisitions** and **live acquisitions**
- Four methods of data collection
  - Creating a disk-to-image file
  - Creating a disk-to-disk
  - Creating a logical disk-to-disk or disk-to-data file
  - Creating a sparse data copy of a file or folder
- Determining the best method depends on the circumstances of the investigation

Determining the Best Acquisition Method

- Creating a disk-to-image file
  - Most common method and offers most flexibility
  - Can make more than one copy
  - Copies are bit-for-bit replications of the original drive
  - ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLookIX
- Creating a disk-to-disk
  - When disk-to-image copy is not possible
  - Tools can adjust disk's geometry configuration
  - EnCase, SafeBack, SnapCopy

Determining the Best Acquisition Method

- **Logical acquisition** or **sparse acquisition**
  - Can take several hours; use when your time is limited
  - Logical acquisition captures only specific files of interest to the case
  - Sparse acquisition collects fragments of unallocated (deleted) data
  - For large disks
  - PST or OST mail files, RAID servers

Determining the Best Acquisition Method

- When making a copy, consider:
  - Size of the source disk
    - Lossless compression might be useful
    - Use digital signatures for verification
  - When working with large drives, an alternative is using tape backup systems
  - Whether you can retain the disk

Contingency Planning for Image Acquisitions

- Create a duplicate copy of your evidence image file
- Make at least two images of digital evidence
  - Use different tools or techniques
- Copy **host protected area** of a disk drive as well
  - Consider using a hardware acquisition tool that can access the drive at the BIOS level
- Be prepared to deal with encrypted drives
  - **Whole disk encryption** feature in Windows called BitLocker makes static acquisitions more difficult
  - May require user to provide decryption key

Using Acquisition Tools

- Acquisition tools for Windows
  - Advantages
    - Make acquiring evidence from a suspect drive more convenient
      - Especially when used with hot-swappable devices
  - Disadvantages
    - Must protect acquired data with a well-tested write-blocking hardware device
    - Tools can't acquire data from a disk's host protected area
    - Some countries haven't accepted the use of write-blocking devices for data acquisitions

Mini-WinFE Boot CDs and USB Drives

- Mini-WinFE
  - Enables you to build a Windows forensic boot CD/DVD or USB drive so that connected drives are mounted as read-only
- Before booting a suspect's computer:
  - Connect your target drive, such as a USB drive
- After Mini-WinFE is booted:
  - You can list all connected drives and alter your target USB drive to read-write mode so you can run an acquisition program

Acquiring Data with a Linux Boot CD

- Linux can access a drive that isn't mounted
- Windows OSs and newer Linux automatically mount and access a drive
- Forensic Linux Live CDs don't access media automatically
  - Which eliminates the need for a write-blocker
- Using Linux Live CD Distributions
  - Forensic Linux Live CDs
    - Contain additionally utilities

Acquiring Data with a Linux Boot CD

- Using Linux Live CD Distributions (cont'd)
  - Forensic Linux Live CDs (cont'd)
    - Configured not to mount, or to mount as read-only, any connected storage media
    - Well-designed Linux Live CDs for computer forensics
      - Penguin Sleuth
      - F.I.R.E
      - CAINE
      - Deft
      - Kali Linux
      - Knoppix
      - SANS Investigative Toolkit

Acquiring Data with a Linux Boot CD

- Preparing a target drive for acquisition in Linux
  - Current Linux distributions can create Microsoft FAT and NTFS partition tables
  - **fdisk** command lists, creates, deletes, and verifies partitions in Linux
  - **mkfs.msdos** command formats a FAT file system from Linux
  - If you have a functioning Linux computer, follow steps starting on page 99 to learn how to prepare a target drive for acquisition

Acquiring Data with a Linux Boot CD

- Acquiring data with dd in Linux
  - dd ("data dump") command
    - Can read and write from media device and data file
    - Creates raw format file that most computer forensics analysis tools can read
  - Shortcomings of dd command
    - Requires more advanced skills than average user
    - Does not compress data
  - dd command combined with the split command
    - Segments output into separate volumes

Acquiring Data with a Linux Boot CD

- Acquiring data with dd in Linux (cont'd)
  - Follow the step starting on page 104 in the text to make an image of an NTFS disk on a FAT32 disk
- Acquiring data with dcfldd in Linux
  - The dd command is intended as a data management tool
    - Not designed for forensics acquisitions

Acquiring Data with a Linux Boot CD

- Acquiring data with dcfldd in Linux (cont'd)
  - dcfldd additional functions
    - Specify hex patterns or text for clearing disk space
    - Log errors to an output file for analysis and review
    - Use several hashing options
    - Refer to a status display indicating the progress of the acquisition in bytes
    - Split data acquisitions into segmented volumes with numeric extensions
    - Verify acquired data with original disk or media data

Image with AccessData FTK

- Included with AccessData Forensic Toolkit
- Designed for viewing evidence disks and disk-to-image files
- Makes disk-to-image copies of evidence drives
  - At logical partition and physical drive level
  - Can segment the image file
- Evidence drive must have a hardware write-blocking device
  - Or run from a Live CD, such as Mini-WinFE

AccessData FTK Imager Lite

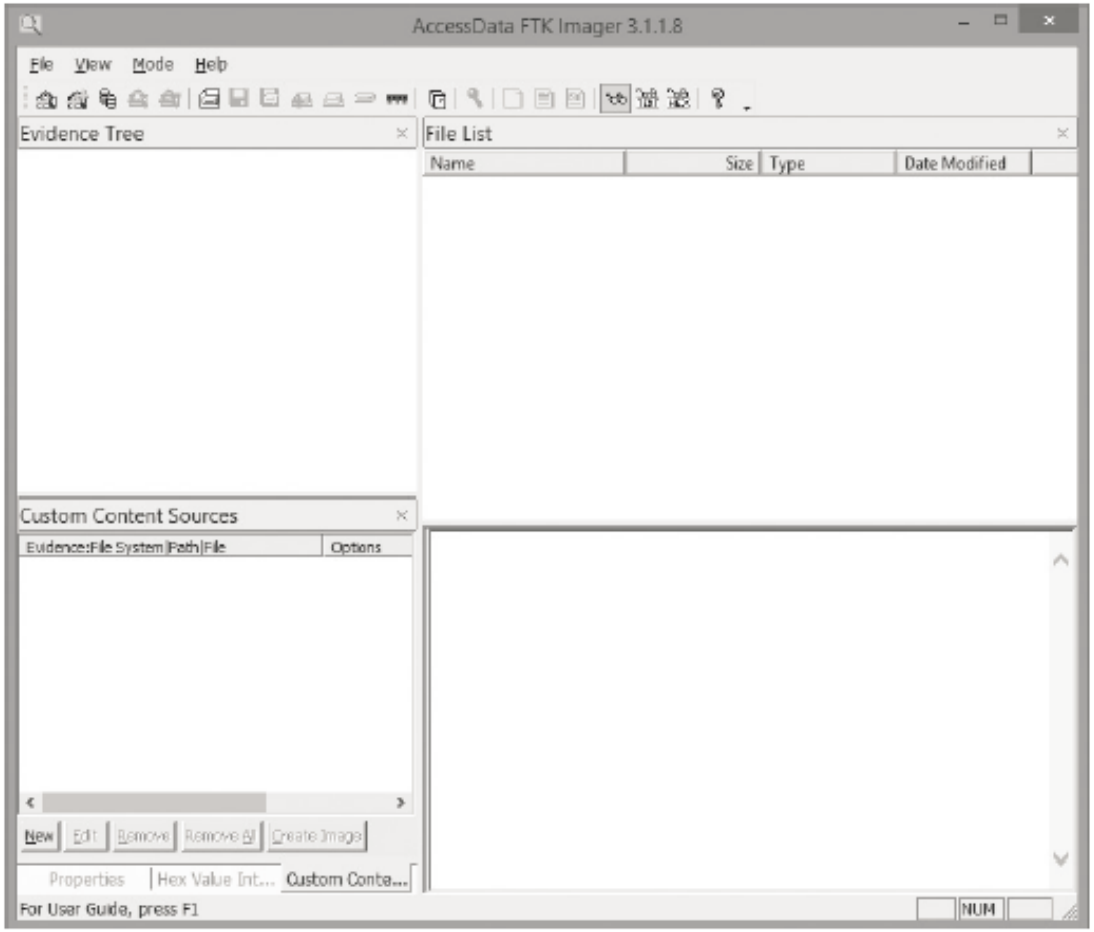

Figure 3-4 The FTK Imager main window
Courtesy of AccessData Group, Inc.

AccessData FTK Imager Lite

- FTK Imager can't acquire a drive's host protected area
- Use a write-blocking device and follow these steps
  - Boot to Windows
  - Connect evidence disk to a write-blocker
  - Connect target disk to write-blocker
  - Start FTK Imager Lite
  - Create Disk Image - use Physical Drive option
  - See Figures on the following slides for more steps

AccessData FTK Imager Lite

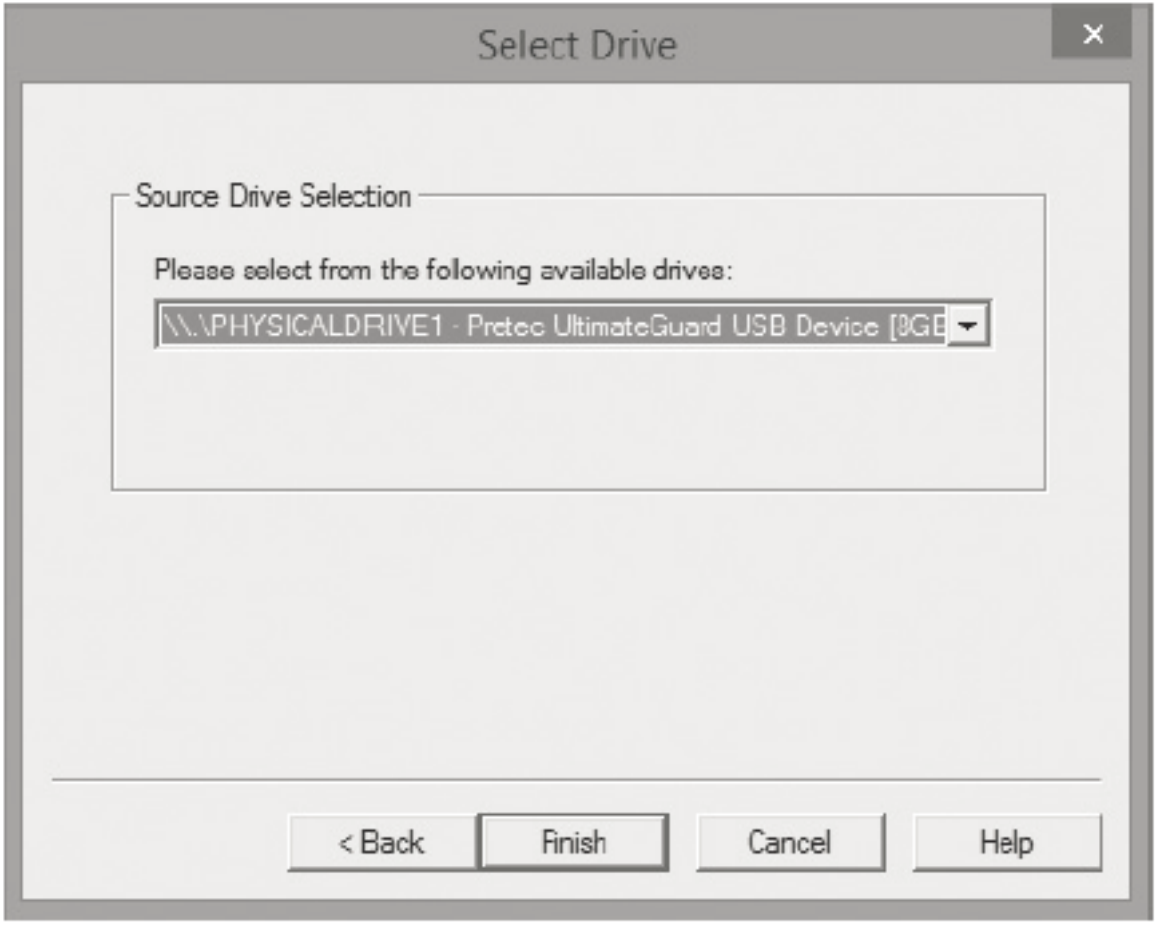

Figure 3-5 The Select Drive dialog box

AccessData FTK Imager Lite

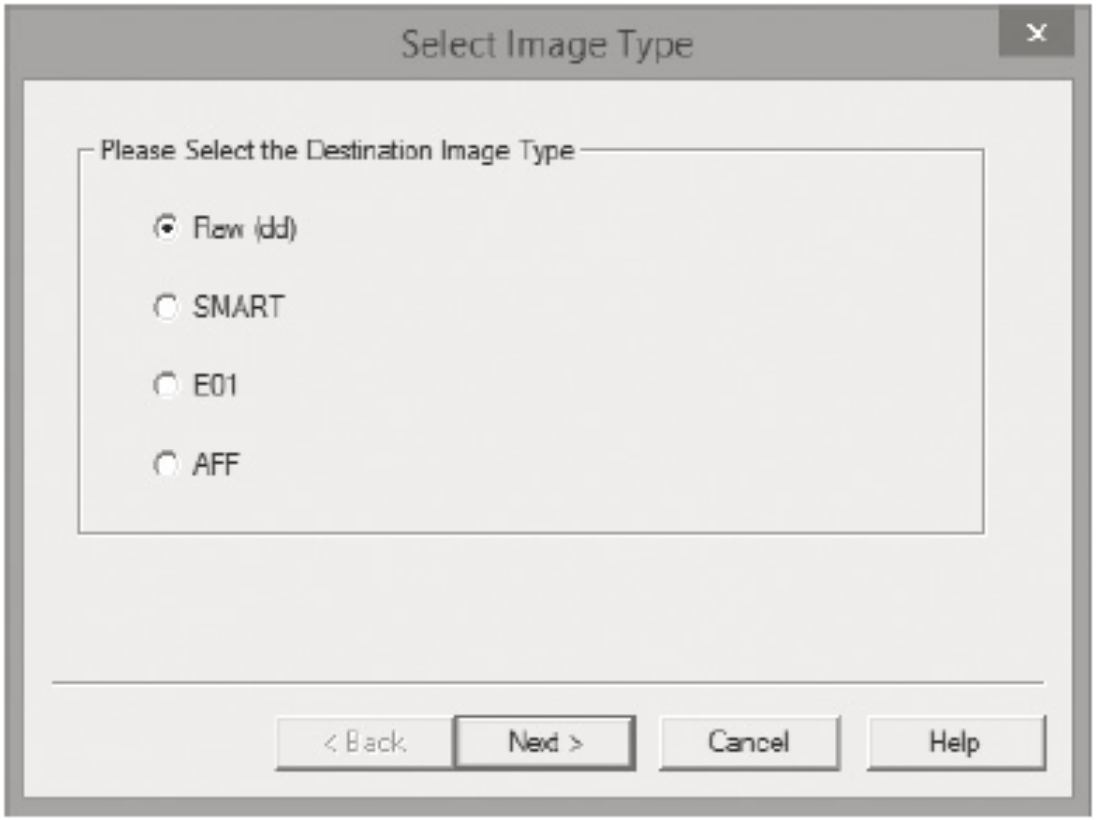

Figure 3-6 The Select Image Type dialog box
Courtesy of AccessData Group, Inc.

AccessData FTK Imager Lite

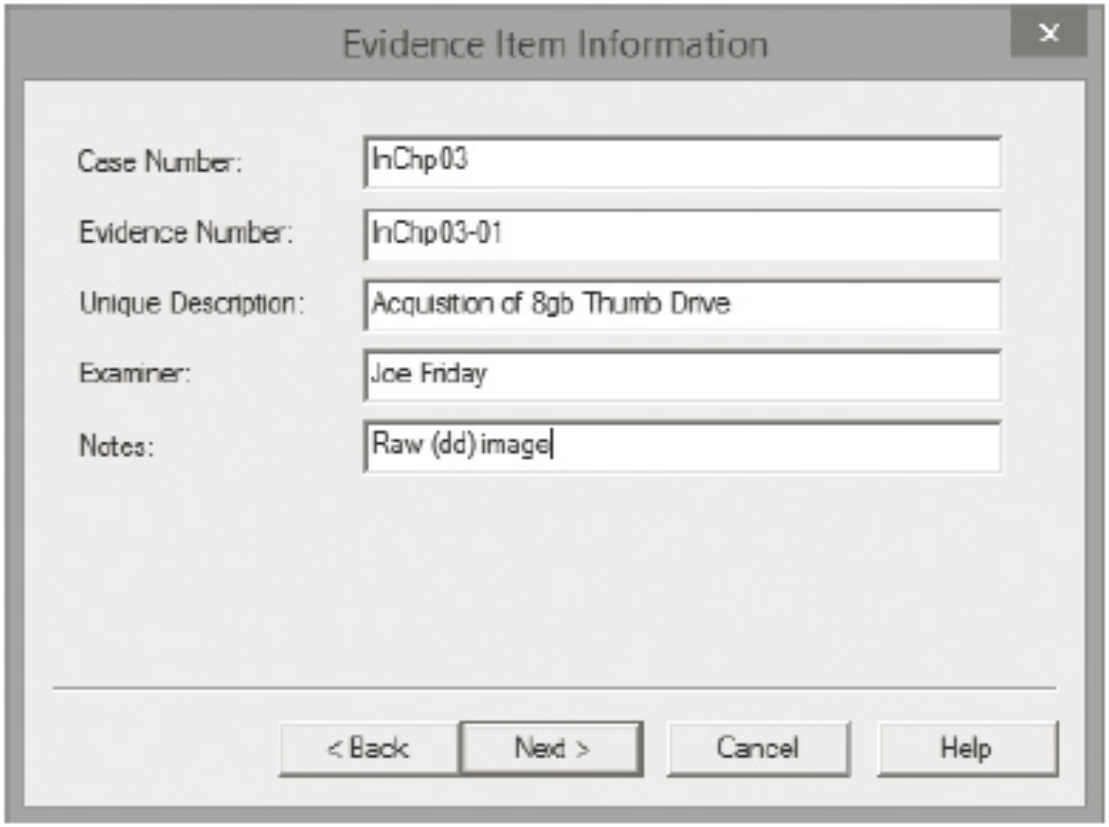

Figure 3-7 The Evidence Item Information dialog box
Courtesy of AccessData Group, Inc.

AccessData FTK Imager Lite

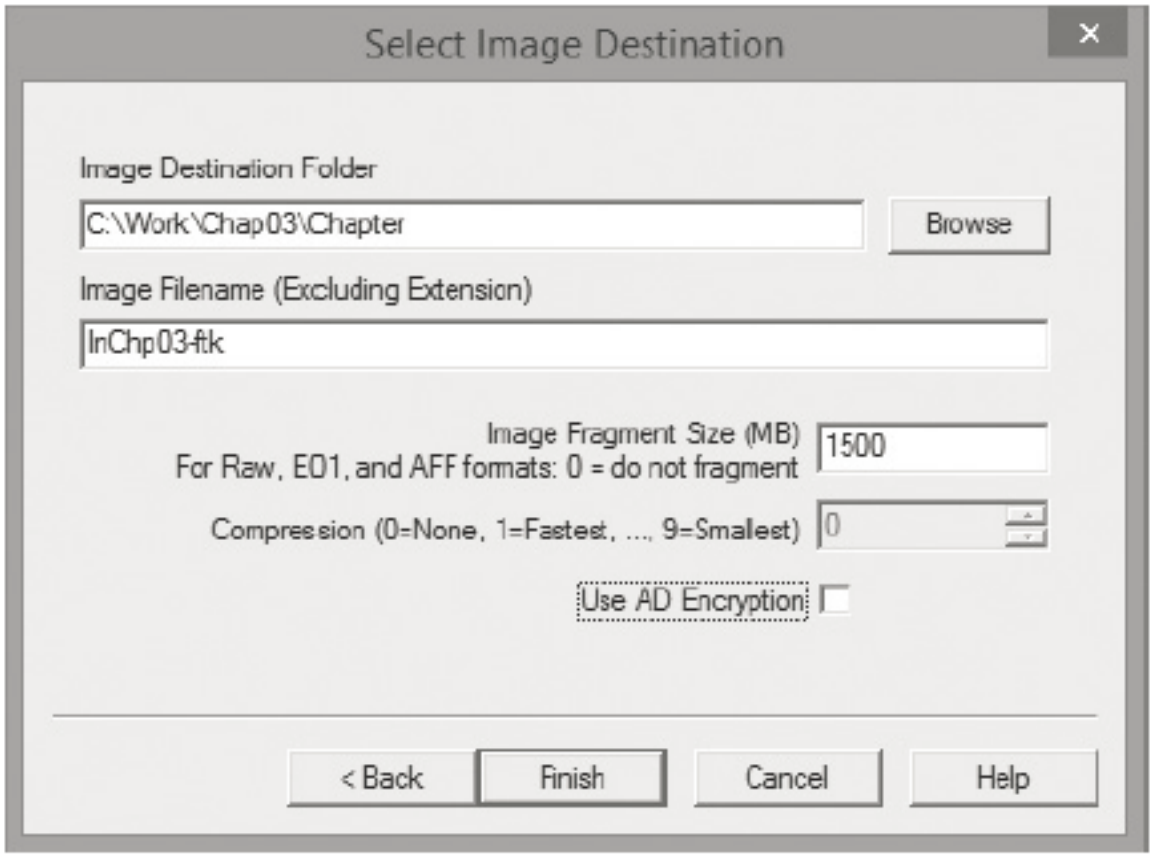

Figure 3-8 Selecting where to save the image file

Courtesy of AccessData Group, Inc.

AccessData FTK Imager Lite

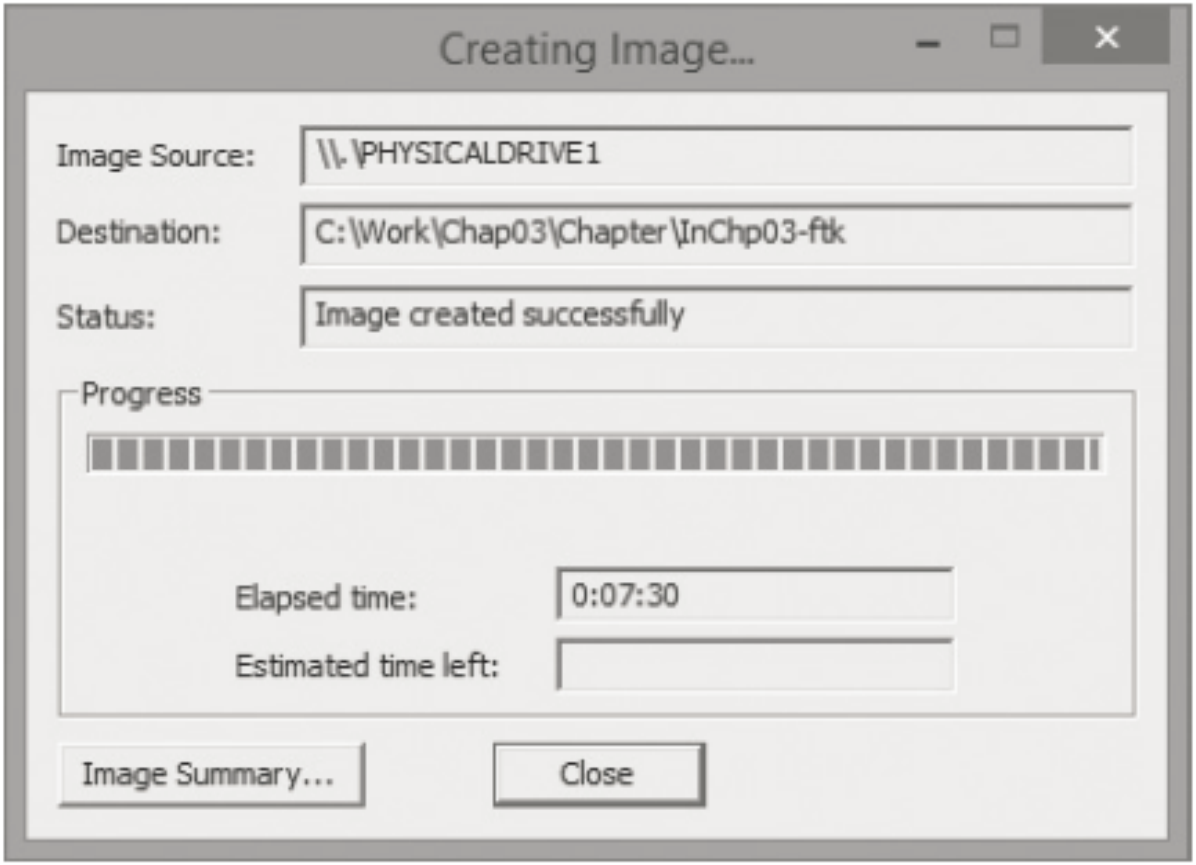

Figure 3-9 A completed image save

Courtesy of AccessData Group, Inc.

Validating Data Acquisitions

- Validating evidence may be the most critical aspect of computer forensics
- Requires using a hashing algorithm utility
- Validation techniques
  - CRC-32, MD5, and SHA-1 to SHA-512

Linux Validation Methods

- Validating dd acquired data
  - You can use md5sum or sha1sum utilities
  - md5sum or sha1sum utilities should be run on all suspect disks and volumes or segmented volumes
- Validating dcfldd acquired data
  - Use the hash option to designate a hashing algorithm of md5, sha1, sha256, sha384, or sha512
  - hashlog option outputs hash results to a text file that can be stored with the image files
  - vf (verify file) option compares the image file to the original medium

Windows Validation Methods

- Windows has no built-in hashing algorithm tools for computer forensics
  - Third-party utilities can be used
- Commercial computer forensics programs also have built-in validation features
  - Each program has its own validation technique
- Raw format image files don't contain metadata
  - Separate manual validation is recommended for all raw acquisitions

Performing RAID Data Acquisitions

- Acquisition of RAID drives can be challenging and frustrating because of how RAID systems are
  - Designed
  - Configured
  - Sized
- Size is the biggest concern
  - Many RAID systems now have terabytes of data

Understanding RAID

- **Redundant array of independent** (formerly "inexpensive") **disks (RAID)**
  - Computer configuration involving two or more disks
  - Originally developed as a data-redundancy measure
- RAID 0
  - Provides rapid access and increased storage
  - Biggest disadvantage is lack of redundancy
- RAID 1
  - Designed for data recovery
  - More expensive than RAID 0

SourceForge

- SourceForge provides several applications for security, analysis, and investigations
- For a list of current tools, see:
  - http://sourceforge.net/directory/security-utilities/storage/archiving/os:windows/freshness:recently-updated

Summary

- Forensics data acquisitions are stored in three different formats:
  - Raw, proprietary, and AFF
- Data acquisition methods
  - Disk-to-image file
  - Disk-to-disk copy
  - Logical disk-to-disk or disk-to-data file
  - Sparse data copy

Summary

- Several tools available
  - Lossless compression is acceptable
- Plan your digital evidence contingencies
  - Make a copy of each acquisition
- Write-blocking devices or utilities must be used with GUI acquisition tools
- Always validate acquisition
- A Linux Live CD, such as SIFT, Kali Linux, or Deft, provides many useful tools for digital forensics acquisitions

Summary

- Preferred Linux acquisition tool is dcfldd (not dd)
- Use a physical write-blocker device for acquisitions
- To acquire RAID disks, determine the type of RAID
  - And then which acquisition tool to use
- Remote network acquisition tools require installing a remote agent on the suspect computer

Thank you