CYBER502x
Computer Forensics

Unit 4: Windows Forensic Acquisition

II: Windows Device Acquisition

R·I·T

Basic imaging steps

- Obtain volatile data (including RAM) if possible
- Image drives and removable media

Fast forensic imaging device

- Tableau TD series Forensics Imager
  - By Guidance Software
- Fast Disk Acquisition System (FDAS)
  - By CyanLine
  - Forensic Falcon by Logicube
  - achieves 30GB/min imaging speed
- SuperImager by MediaClone
  - 29-31 GB/Min

Tableau TD2u

Image: forensicstore.com

Software-based forensic imaging

- dd and FTK imager
- EnCase Forensic Imager
- EnCase Forensic from Guidance software
- Forensic Toolkit (FTK)

EnCase Forensic Imager

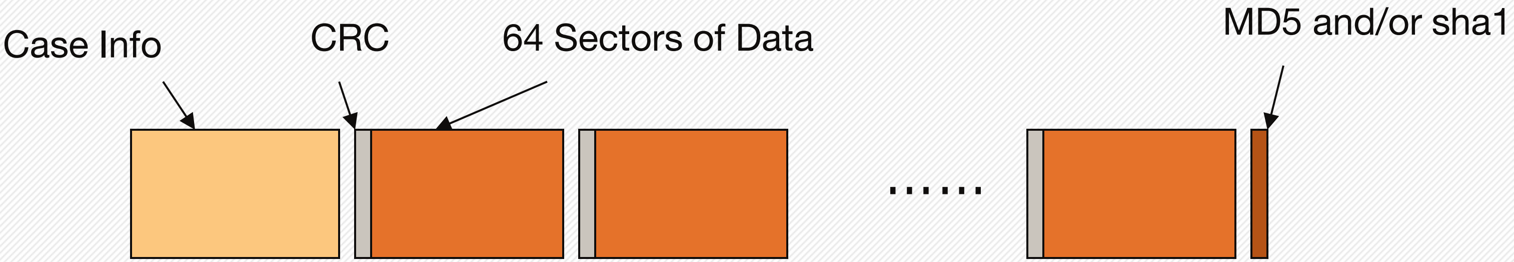
- Free to download and use
  - https://www.encase.com/products/Pages/Product-Forms/Forensic-Imager-download.aspx
- Provides easy viewing and browsing of potential evidence files
  - including folder structures and file metadata
- Note
  - When using the Imager to create a forensic image of a hard drive, make sure your are using a write-blocking mechanism.

EnCase Forensic

- By Guidance Software in 1998
- Support drive image acquisition and forensic analysis
- Reference books:
  - *EnCase Computer Forensics -- The Official EnCE: EnCase Certified Examiner Study Guide* by Steve Bunting, 2012
  - *Computer Forensics and Digital Investigation with EnCase Forensic v7* by Suzanne Widup, 2014

EnCase (Cont'd)

- Evidence File
  - The file header
  - The checksums
  - Data block



EnCase Evidence file

- .E01, .E02,…., from EnCase before v7
- .Ex01, .Ex02, …., since EnCase v7
  - Support for encryption of the data
  - Improve efficiency and performance
- Lx01 – Logical Evidence File Format

Write Blocker

- Software Write Blocker
  - EnCase FastBloc SE (Software Edition)
  - SAFE Block Win8 from ForensicSoft Inc. (~$500)
    - http://www.forensicsoft.com/help/SBlock/SBWin8-10_User_Guide.pdf
- Hardware write-blocker
  - fastBloc, Ultrablock
  - ~$400 for IDE/SATA, ~80 for flash media devices
  - Guidance Software Forensic Bridge
    - T8u, T35u, T6es, T9

FastBloc SE

- A collection of tools that control reads and writes to a drive attached to a computer through USB, FireWire, and SCSI connections.
- To write block a USB, FireWire, or SCSI device
  - (see EnCase_Examiner_v7.08_Users_Guide, page 589)
  - Make sure that the subject device is not attached
  - Click Tools > FastBloc SE
  - Select the Plug and Play tab (write blocked)
  - Insert a USB, FireWire, or SCSI device
  - Click Close

Preview vs Acquire

- View and search files without acquiring an image
- Immediately determine whether relevant evidence exists on a computer
- Alert: Have to use a write blocker to ensure no changes to the original drive.