ADVANCED COMPUTER FORENSICS

EnCE EnCase Forensics: The Official EnCase Certified Examiner Study Guide

CHAPTER 4

Acquiring Digital Evidence

EnCase Forensic Boot Disks

- Creating with EnCase 7
  - Download the image of a boot floppy from Guidance Software’s support portal
    - Downloads Tab
      - Boot Disk
  - Tools Create Boot Disk
- Booting Using the EnCase Boot Disk
  - When to utilize your boot disk
    - Geometry mismatches between the suspect machine and your machine
    - Suspect HD “married” to the motherboard for security reasons
    - HD part of HD RAID
    - HPA / DCO

Seeing Invisible HPA and DCO Data

- Host Protected Area (HPA)
  - ATA-4 – creates a place for vendors to store information
    - Recovery, security, registration etc.
  - Invisible to BIOS thus protected from users
- Device Configuration Overlay (DCO)
  - ATA-6 – limiting the apparent capacity of a drive
  - End of the drive and is also invisible to BIOS
- Accessing this “invisible” data
  - Direct ATA (legacy method of access)
    - EnCase for DOS on a forensic boot disk
    - EnCase communicates directly with the controller
  - LinEN-EnCase under Linux and FastBloc SE

HPA or DCO?

- Check Manufacturer’s website for drive specifications
- If EnCase reports less sectors than the manufacturer specs then suspect HPA or DCO

Steps for DOS Boot

- Prepare for the unexpected and have a hand on the power
  - Follow your own policies
  - Disconnect power and inspect the connections
  - Disconnect power and data (label each drive
  - Insert forensic boot disk or CD
  - Reconnect the power and start the computer
    - Enter the setup mode immediately
  - Change boot settings/boot order (record the current settings)
  - Save settings
  - TEST THIS ENVIRONMENT
  - Test with the image storage device attached
  - Reconnect target drive - start up

Drive-to-Drive DOS Acquisition - 1

- Takes place in DOS
  - Target (suspect) drive and Image storage drive attached to same motherboard
    - Only need and EnCase boot disk
    - Speed limited is the slowest component on the ATA system
- Acquisition Steps
  - Test system for safe boot
  - Install drives to one motherboard (master to master is fastest)
    - Format storage drive as FAT – Required for EnCaes DOS acquisition
    - Label the drive
    - Create the path for the image to be located – after formatting and before attaching to the system for acquisition

Drive-to-Drive DOS Acquisition - 2

- Acquisition Steps (continued)
  - Start the computer
    - Monitor the boot ready to pull the plug
  - At the A prompt type **en** and then Enter
    - Physical devices on the left and logical devices on the right (only FAT on right)
  - If you used DOS boot because of HPA or DCO now you should change to Direct ATA
    - If you are using DOS boot for another reason verify sector numbers and proceed
  - Unlock your storage device as EnCase locks all drives by default (be sure you have chosen the correct drive to unlock
  - Choose A to acquire and enter the path for the storage drive (it must already exist – you created it prior to plugging it in)
  - Enter information as prompted
  - Compression, MD5, password protected, segment size (640MB recommended), # of sectors to acquire – usually all of them, granularity
  - Acquisition

Drive-to-Drive DOS Acquisition -3

- Tableau bridges can be utilized for a hardware block in a drive-to-drive DOS acquisition
- Acquiring Mac or other drives not recognized by DOS
  - Acquire it physically and then bring it in to EnCase
  - Mac computers can be imaged utilizing FireWire
    - Hold down the T key as you boot up a Mac 0 when you see the FireWire icon
    - Connect it to you machine with a FireWire cable
    - Acquire the physical drive and mount the file system
  - Utilize a Tableau if the Mac is Dual booted using Boot Camp – Windows will mount any Windows partition on the machine

Drive-to-Drive DOS Acquisition - 4

- SCSI Acquisition
  - Image it in the host computer in a drive-to-drive DOS Acquisition
  - You must load the SCSI drivers into the EnCase boot disk
- Once acquired
  - Power down
  - Return to storage area
  - Document, label, antistatic bags etc.
- Verify image

Network Acquisitions

- Utilizing a network (crossover) cable
  - Boot the target (suspect) computer with an EnCase for DOS or LinEn option
  - Boot a second machine running EnCase
    - Advantages of DOS boot (Direct ATA) and the functionality of EnCase
    - *Considered legacy*
- Why you might utilize this acquisition type
  - HPA/DCO
  - Laptop acquisition (difficulty accessing drive)
  - Quick data acquisition
  - Previewing data

Understanding Network Cables

- Crossover cables
  - “cross” so that on one end (computer) the wires are send/receive and the other end is receive/send so that they can communicate with one another
  - Crossover adapters are also available
- Make sure the computer has a NIC
- You have an EnCase boot CD for network support
- Drivers for the NIC

Preparing an EnCase Network Boot Disk

- EnCase Network Boot Disk (not after version 5 of EnCase)
  - ENBD.EXE is a self-extracting floppy disk image
  - ENBD supports 29 drivers and 190 device variations
- EnCase Network Boot CD are both available to create boot disks with NIC drivers (not after version 5 of EnCase)
  - ENBDCD is continually updated and available from encase
  - Identical to the ENBD, but a CD has more space and thus more driver availability
  - You must match your versions of the ENBCD with your EN.EXE
- LinEn – EnCase Linux version can also be utilized for network acquisitions

Steps for Network Acquisitions - 1

- Booting up
  - Have Windows machine on, but not with EnCase open
  - Control and test the boot process
  - Reconnect target device
    - Choices
      - Network support
      - USB – no letter assigned
      - USB – letter assigned
      - Clean boot

Steps for Network Acquisitions - 2

- Setting Up Acquisition
  - Choose #1 Network support
    - SCISI drivers should be loaded first if SCSI exists (autodetect)
    - Load NIC drivers (autodetect)
    - ENBD launches EnCase for DOS (default mode is BIOS)
  - If you need HPA/DCO you must temporarily shut down the “server” mode to change to Direct ATA
  - Parallel or network (network)
- Windows Machine w/EnCase
  - Verify all connectivity and communication will be allowed (firewalls etc.)

Steps for Network Acquisitions - 3

- Windows Machine w/EnCase
  - If the EnCase machine will not connect Change the Network Settings
    - Static IP 10.0.0.50 and subnet of 255.255.255.0
    - Remove DNS
- Launch EnCase
  - Start New Case
  - Add Device
  - Network Crossover
  - Next – Select the device – Next
  - Finish
- You can preview in “real time” there might be lag
- Acquire by clicking Acquire and directing the image to be stored

Specifying Data Acquisition Options

- Capture, verification and storage of data
  - Right click device and Acquire
  - Where to store the image
    - Usually you want to replace source drive
  - Notes, file segments, compression, sectors, passwords, block size, granularity, hash, etc.
- Finish and acquisition is ready to start

FastBloc - 1

- Current Day Techniques
- FastBloc
  - Was Guidance Software’s hardware write blocker – they have since bought out Tableau and that is what is currently being utilized and updated
  - Models
    - Classic – SCSI interface (no longer available)
    - LE (Lab Edition) – IDE connection with host
    - FE (Field Edition) – USB-2 or 1394a (FireWire) connectivity
    - IDE interface to suspect drive – a SATA bridge can be added to allow for SATA acquisitions

FastBloc - 2

- FastBloc 2 – Ended in 2010 after Guidance bought Tableau
  - FastBloc2-LE (Lab Edition)
  - FastBloc2-FE (Field Edition)
    - Utilized WiebeTech Firmware
    - Forensic software recognition – EnCase recognizes the write-blocker
    - Daisy Chain
    - ATA-5 & 6, 2.5inch, SATA (adapter kits for 1.8inch drives, microdrives, PCMCIA cards and extra cables)
    - Tough aluminum enclosure
    - Plug and Play for FireWire
    - USB 2/USB support
    - Pelican Carrying case

Tableau Acquisitions

- Field and lab mounted write blockers
  - You should try to purchase adapters or the types of devices/cases you see the most
  - Models
    - T35es – IDE and SATA
    - T8-R2 – USB and external drives
    - T9 – FireWire bridge (used for Macs in Target Disk Mode TDM)
    - SCSI and SAS drives
  - Adapters
    - 2.5 IDE adapter, 1.8 IDE adapter, ZIF adapter, Adapter kit all together and SATA adapter
  - Latest models at Guidance Software

FastBloc/Tableau Acquisitions - 1

- Connect to the host which can be on or off
- Set target as Master if it’s a PATA
- Connect power cable then IDE cable
- Connect power supply to the device and turn it on
  - Write Blocker should be recognized via plug and play
- Windows will mount partitions it can recognize and you can preview them as if they are an attached external device
  - EnCase will see partitions Windows can’t
- Run EnCase – Start a new case and Add Evidence
- Add Local Device leave defaults unless using Legacy FastBloc (pre Tableau)
  - Blue triangle in corner of icon denotes a live device
  - FastBloc has it’s own icon and is easily identifiable (device symbol with a blue or green box around it)
  - Select the physical device or the logical volume you would like to image
  - Verify drive space from manufacturer matches what EnCase indicates
  - If DCO is indicated go back and check remove DCO

FastBloc/Tableau Acquisitions - 2

  - Click Finish
  - Evidence will appear
  - Preview he drive by blue checking and clicking Load Selected Device OR Double Click
  - This is a preview
- To Acquire this Evidence
  - Select device then choose Acquire from the drop down or Select the device and right click the device in the table pane Acquire
  - Search / bookmark, print reports, export and save them as well
  - Bookmarking before acquiring can be maintained if you choose the Replace Source Drive Option when acquiring the device

FastBloc SE Acquisitions

- EnCase Software write blocker
  - Can control reads/writes to attached media
    - USB, FireWire and SCSI channels
    - If the host controller is ATA-6 compliant then HPA/DCO acquisitions are also supported
      - You should document this as EnCase
        - Removes and returns HPA and DCO if only one is present
        - If both are present they are removed and permanently removed
- Acquisition Steps
  - Launch EnCase – Tools -> FastBloc SE
  - Write Blocked – wait for EnCase detection
  - Attach your device – verify it is blocked
  - Create a new Case – Add Evicence – etc.
  - Remove device
  - Stop write blocking

LinEn Acquisitions - 1

- EnCase for Linux (EnCase 5 and up)
  - Mounting a File System as Read-Only
    - Need to remove automounting of file systems in Linux
    - You will need your own version of Linux
      - Live CDs such as Helix, Knoppix and SPADA may already boot with mounting off (TEST YOUR BOOT DEVICE)
    - Good practice to keep your boot CD as is and clean
      - Maintain your LinEn on a USB

LinEn Acquisitions - 2

- Updating your Linux Boot CD with Latest Version of LinEn
  - Encase -> Tools -> Create Boot Disk
  - ISO then OK
  - Alter Boot Table check box -> Browse to your path with the ISO then browse to the modified ISO ->Next
  - Add files to the ISO – Right-click -> New browse to LinEn in the root of the folder Program Files\EnCase7 -> Finish and EnCase will update the ISO
  - Burn the updated ISO to a CD

LinEn Acquisitions - 3

- Running LinEn
  - Must be Root with full control
  - Best to run in Console mode
    - Automount off
    - Boot into console
    - Attach target
    - Attach storage device
    - LinEn on the ISO or device

LinEn Acquisitions - 4

- Acquisition Steps
  - Boot to console and logon as Root
  - Verify mounted device – type **mount**
  - Check available devices – type **fdisk -l**
  - Mount your storage drive and create a directory
    - **Mkdir /mnt/fat32**
  - Mount the newly created directory
    - **Mount /dev/hdal /mnt/fat32**
  - Verify mount
    - **Mount**
  - Create the storage area where the evidence file will be held
    - **Cd /mnt/fat32** in the root of your storage volume
    - **Mkdir /some accurate storage directory**
  - Navigate to LinEn and then **ls -al** to get a list – linen
  - Launch LinEn **./LinEn** if you get an error for permissions **chmod 777 LinEn**
  - LinEn launches and follow the interface
    - Device, MD5, A to acquire, path for evidence, granularity, etc.

Enterprise and FIM Acquisitions

- Acquiring Over a Network - *Crossover Cable*
  - EnCase Enterprise (EE)
  - EnCase Field Intelligence Model (FIM-EnCase 6)
    - Thousands of miles or feet
    - Target system is LIVE and running it's native OS
      - Can be evaluated with or without the user's knowledge
      - RAM can be captured and evaluated as well
        - Accessed by the feature *snapshot* which is an EnScript
    - EE on your machine – servlet on the target machine and SAFE licensing
      - Target communicates with SAFE and your machine
        - Servlet listens on 4445
    - FIM – SAFE existed on the machine as it was directly connected to only one computer

EnCase Portable

- Have it installed and ready to use
  - Prepare your storage device
    - Attach to the EnCase machine
    - Start EnCase -> EnScript Run Portable Management -> Choose your device
    - Exit and remove the drive
  - Boot suspect computer with EnCase Portable USB or CD (need codemeter)
    - A Windows Splash screen will appear “BARTPE” for Windows is being used to boot from the USB
    - Connect your media to receive the evidence
    - Follow choices on screen
    - OK to start
    - Shutdown once status has changed to completed
    - Remove codemeter USB and storage device

DOL Disclaimer and CCBY

This workforce product was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The product was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.