Evidence Acquisition

- Goal:
  - Acquire the original digital evidence in a manner that protects and preserves the evidence

General Evidence Acquisition Procedure

- Preparation
- On Site Assessment
- Disconnect devices
- Controlled Boots
- Capture BIOS / EFI information
- Verify system functionality
- Load examiner controlled operating system with devices attached
- Acquire digital evidence

Exceptions and Issues

Preparation

- Create and validate forensically sound controlled boot disk
  - Modified operation system
    - No auto-mount of devices or file systems
    - Ability to mount devices as read-only
    - Write-blocking device drivers
  - Personally validate using NIST Software Write-blocker Test Suite
  - Install and validate forensic software for use in copying and analyzing evidence

- Virus check all disks that contain software, especially the forensic boot disk
- Thoroughly wipe any disk to be used for storing a copy of digital evidence
- Document examiner’s system
  - System hardware
  - Operating system software
  - Applications
  - Hardware write-blockers

On Site Assessment

- Disassemble case of the computer to be examined
  - ensure equipment is protected from static electricity and magnetic fields
- Identify storage devices that need to be acquired
  - can be internal, external, or both
- Document internal storage devices and hardware configuration
  - Drive condition
    - make, model, geometry, size, jumper settings, location, drive interface
  - Internal components
    - sound card; video card; network card, PC Cards, media access control (MAC) address

Retrieve System Info

- Disconnect storage devices
  - using the power connector or data cable
  - prevent the destruction, damage, or alteration of data
  - check CD/DVD drive and floppy drive

- Perform first controlled boot
  - Enter BIOS and document
    - System date and time
    - Power-on passwords
    - Current boot sequence
  - Change boot sequence so it checks device with forensic boot disk first
  - Even if devices are not attached, BIOS can recognize the controllers and list
  - If using a USB drive for your forensics boot disk you may need to use the “one time” boot menu

- Check that floppy or CD/DVD drive is functional
- Power down system
  - Check to see that forensic boot disk is still in floppy or CD/DVD drive

Test Boot Device

- Connect Floppy or CD/DVD drive
  - Check both power and data cables
  - Insert forensics boot disk into the drive

- Perform second controlled boot
  - Ensure that the computer system
  - boots from the forensic boot disk
  - supports the operating system and version on the forensic boot disk
  - Check that floppy or CD/DVD drive is functional

- Power down system
  - Check to see that forensic boot disk is still in floppy or CD/DVD drive
Evidence Acquisition Procedures
- Protect the integrity of the original digital evidence.
- Authentic: any evidence originating from a digital source.
- End result is when asked to testify:
  - Utilizing my special training and available tools, I took every precaution to secure and protect the original evidence.

Controlled Boot Process
- Three Controlled Boots
- Capture BIOS / EFI information
- Verify system functionality
- Load examiner controlled operating system with devices attached
- Boot from your own:
  - Floppy
  - CD or DVD
  - USB Flash Drive
  - Portable Hard Disk
  - USB / FireWire
- Always validate Controlled Boot Disk personally

Forensic Safety Net

ACQUIRE EVIDENCE

Prior to acquiring evidence
- Generate a unique hash value
  - Drive does not need to be mounted to perform this activity
- Used to authenticate original digital evidence has not been changed

Create physical copy of subject evidence device
- Bit-for-bit copying of physical geometry (sectors) on evidence media disk
- Do not make a logical copy using operating system file manager
  - Only copies file system, directories, folders, and files on a partition
- Verify copy is exact duplicate using has value
- Power down and disconnect evidence media

ACQUIRING EVIDENCE WITH EXTERNAL MEDIA

ACQUIRING EVIDENCE WITH INTERNAL MEDIA