Preparing for an Investigation

“Always Be Prepared”

Scope of the Investigation

- What Evidence do you need to collect
  - Files, Static Memory, Live Memory, Network Information/Data, Images etc
  - This will determine the required tools
- What Authority do you need to collect that evidence

Criminal

Warrants

Corporate (Private Sector, Public Sector)

Permission of the Organization

No access to private property of individuals

Handling and Storage of Evidence

1. Identify the required Evidence Lockers
2. Have all Required Forms, Tags and Containers
3. Have all Required Equipment (i.e. Cameras, Network Taps, Wireless Cards, External drives etc.

Forensic Workstation

- Operating System
- Interfaces, Cables, Connections, Connectors (SATA, Firewire, SCUZZY, Bluetooth, Wireless versions, etc
- Drives (Floppy, Blueray, DVD, CD, USB version)
- Consider Building/Acquiring and Booting a Live CD specially designed for forensics.

In-Class exercise: Research Tsurugi and CAINE Linux**.** Hint, you may be building a forensic workstation using these on virtual box.

Make notes! You may be turning these in for assessment.

Forensic Tools

- FTK Forensic Tool Kit
- Prodiscover
- The Sleuth Kit & Autopsy
- dcfldd & dc3dd (Linux)
- Libewf
- EWF Tools
- Oxygen Forensics
- Magnet Forensics

In-class Exercise: Review each of these. **Briefly record notes on each** as to: 1) What does it do 1) Free or Paid, 2) OS dependency (linux or Windows). **You may be turning these notes in for assessment.**