JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Forensic Toolkit Components

CYBER INCIDENT RESPONSE

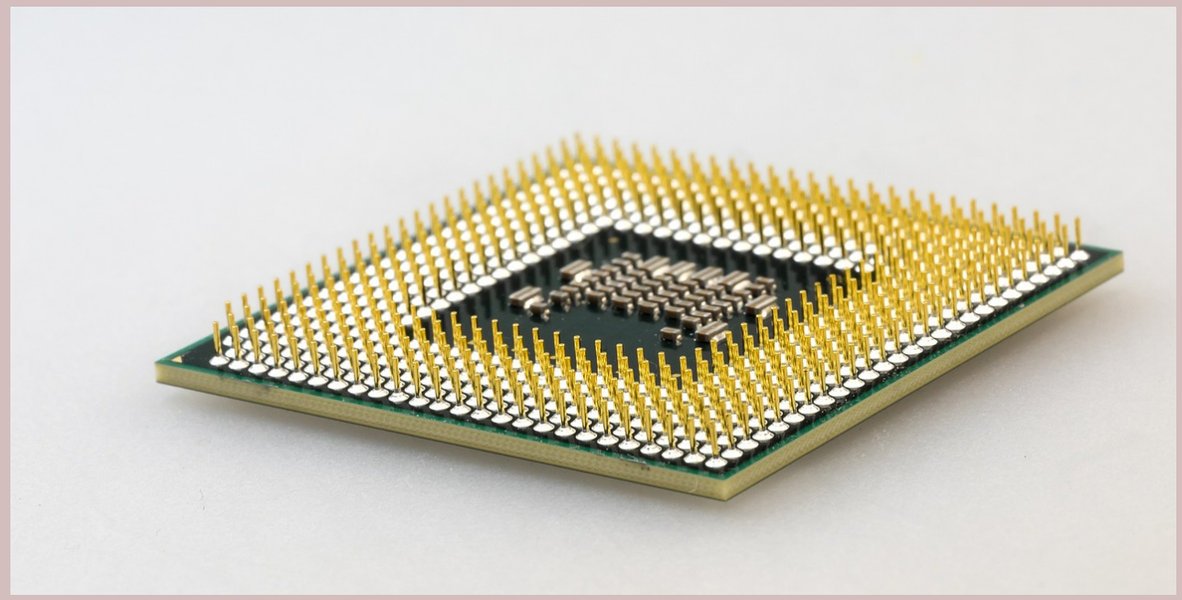
Forensic Toolkit

- Contain a wide variety of software and hardware needed to conduct collection and analysis of data in the field

- Toolkits vary widely in cost and capability

Digital Forensic Workstation

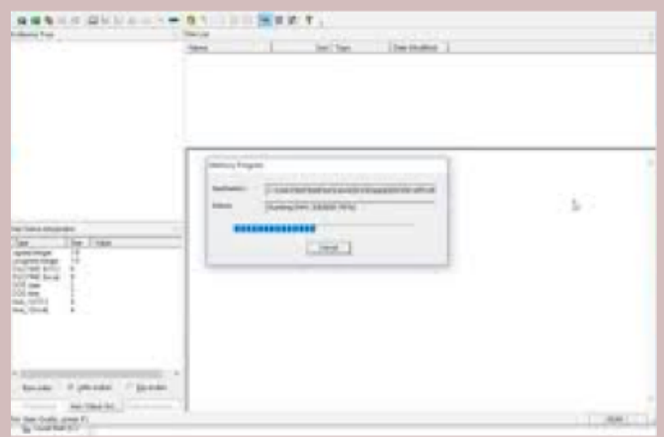
- Conducts data capture and analysis
  - Multicore CPU
  - Maximum RAM
  - Large, fast storage



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Forensic Investigation Software

- Capture and analyze forensic images
- Document and track investigations
  - Forensic Toolkit (FTK)
  - EnCase
  - SANS Investigative Forensic Kit (SIFT)
  - The Sleuth Kit (TSK)



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Write Blocker

- Ensures hard drives being imaged cannot be written to or its data changed
  - Hardware variants
  - Software variants
- Ensures integrity of the captured disk

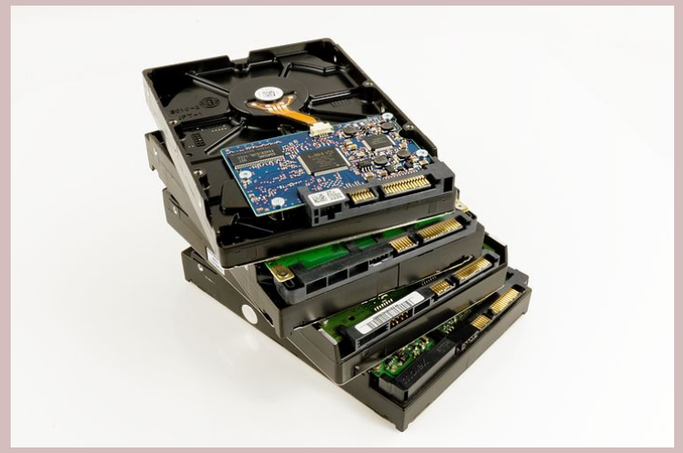
Forensic Drive Duplicator

- Designed to copy hard drives without changing the original
- Dedicated device that copies drive and hashes the disk image

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

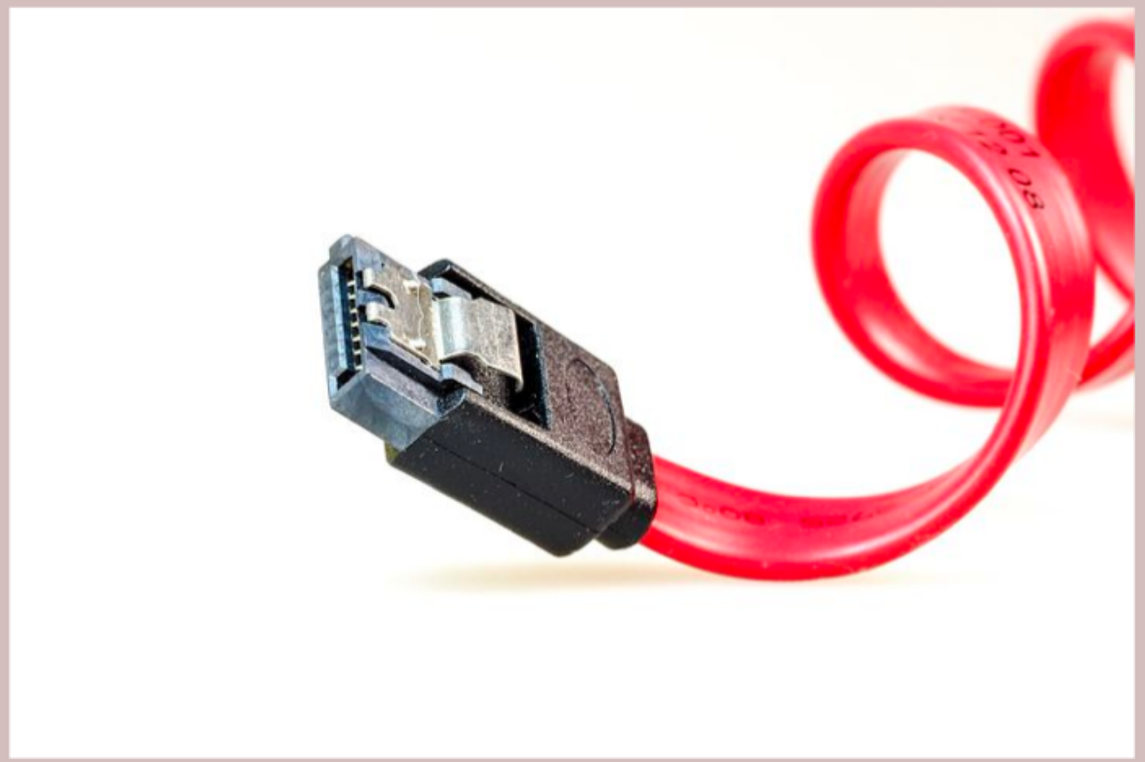
Wiped Drives and Removable Media

- Clean hard drives that are ready to receive disk images on
- Drives are prepared using a drive wipe before use in the field



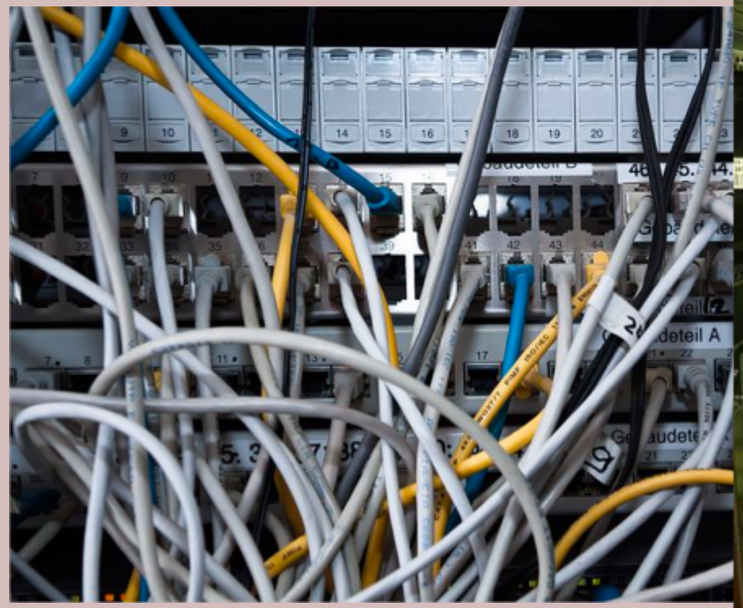
Cables and Drive Adapters

- Be ready to copy/collect any type of media you come across while in the field



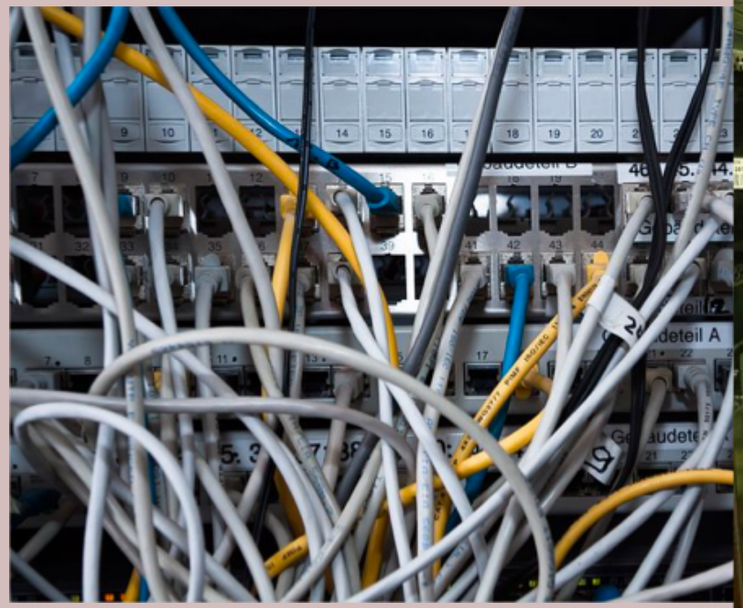
Digital Camera

- Used to photograph system layout, system configurations, drive labels, how a machine is cabled, etc.



Label Maker and Labels

- Label cables, components, and other items collected while in the field



Documentation and Checklists

- Chain of Custody forms, incident response forms and plan, and more

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE