JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Digital Forensics

CYBER INCIDENT RESPONSE

Digital Forensics

- Forensics are used to determine any changes, activities, or actions that have occurred on a host or server
- Allows incident responders to determine what occurred by putting together various pieces of information
- Similar techniques are used by incident response teams and law enforcement

Documentation in Digital Forensics

- Documentation is one of the most important steps in digital forensics
- Everything you do needs to be repeatable by a third-party investigator
- Chain of Custody is imperative for use in law enforcement

Forensics Toolkits

- Consist of specialized software and hardware to conduct imaging of hard disks and follow-on analysis

- Mobile devices require additional specialized tool kits