

Digital Forensics at a University

Calvin Weeks

Director, Oklahoma Digital Forensics Lab
University of Oklahoma

Calvin Weeks

- Director, Oklahoma Digital Forensics Lab
- Former Director of IT Security
- Certified EnCASE Examiner (EnCE)
- VP of the local chapter of HTCIA
- Co-Chair of the EDUCAUSE Security Task Force E&A WG

Oklahoma Digital Forensics Lab

University of Oklahoma

Oklahoma Digital Forensics Lab

Information Technology

- Fully functional forensics lab
- Operational incident response team
- Security Operations Center
- Certified Professional Development
- Work with local, state, and federal law enforcement
- <https://odfl.ou.edu>

Overview

- What is Digital Forensics?
- Why you want Digital Forensics capability?
- Who should perform Digital Forensics Exams?
- How to manage Digital Forensics?

What is Digital Forensics?

- Exact scientific analysis
 - Post mortem data
 - Real or perceived
 - Report with validated findings
- Art
 - Knowledge of technology communications
 - How programs and O.S.'s function
 - Identifying trace evidence patterns left behind

Why?

- Regulatory compliance
 - GLBA, SOX, HIPAA, FERPA, etc.
- Compliance requirements
 - COBITT, ITIL, ISO17799, other Information Assurance practices.
- Grant compliance
 - NSF, DOJ, most other funding sources
- Properly respond to security incidents
 - Internal problem analysis, contractual negotiating/breach, civil or criminal proceedings, policy violations

Get a complete picture

- It will show which files were accessed or written to the host
- Might show why the host was compromised
 - File store
 - Launching point for further attacks
 - Accessing sensitive information stored on the host
- Knowledge level of the attacker

Who performs Digital Forensics Exams?

- Experienced and Trained personnel whom:
 - Understand applicable legal requirements and policies
 - Are willing to testify in court
 - Received professional training
 - Have a firm grasp of security threats and vulnerabilities

What is needed?

- Dedicated “beefy” Workstation
- Write-blocking hardware
- Laptop for on-site forensics
- Several spare hard drives
- Write once media
 - CDR’s
 - DVDR’s
- Forensics Software

How to manage Digital Forensics?

- Team Safety
- Recognizing Potential Evidence
- Preparing for the Search and/or Seizure
 - Consent Search vs. Search Warrant
 - Search Warrants
- Conducting the Search and/or Seizure
- Forensics Exam

Secure the Area

- Team Safety
- Preserve potential fingerprints
- Restrict physical and logical access to devices
- Remove all unauthorized persons

Secure the Device

DO NOT BROWSE OR LOOK
THROUGH THE DEVICE AS
THIS WILL DESTROY
EVIDENCE.

DOCUMENT ALL ACTIONS.

Recognizing Potential Evidence

- Is the device contraband (suspect)
- Is the device a tool (Victim or innocent party)
- Is the device incidental
 - Combo with contraband
 - Combo with tool
- What is your probable cause (cause for action)
 - Hardware?
 - Software?
 - Data?

Basic Investigation Skills

- Interview techniques
 - Passwords
 - Names
 - ScreenNames
 - Email addresses
 - Encryption used and what type
- Handwritten notes
- Media
- Trash

Preparing or Requirements

- Probable cause (Cause for action)
 - What is your scope
- Collection Techniques
- Trained and/or Certified personnel only
- Where will the search be conducted

Consent vs. Warrant

- Warrant
 - Predefined search, seizure, and examination of electronic evidence (signed by judge)
 - Two primary sources
 - Electronic Storage Device
 - Service Provider
- Consent
 - Law Enforcement is normally in writing, signed by the individual giving consent, and can be revoked by the individual at any time.
 - Private Organizations must be predefined in policy, law, or must follow similar restrictions as law enforcement.

Secure the Device

- OFF – **Do not turn on**
- On
 - Stand-alone or NON-Networked device
 - Consult with trained professionals
 - Process appropriately
 - Networked device
 - Consult with trained professionals
 - Process appropriately

Processing Protocol

Device that is “ON”

- Photograph the screen
- Photograph the search area

NON-Networked device

- Unplug power cord from the device
- For laptop or other devices that does not turn off by pulling the power you must remove the battery
 - Do NOT place battery back in device
 - Seize all power cables for laptops or unique devices

Processing Protocol

Networked Devices

- DO NOT TOUCH
- Seek persons trained to handle networked computers
- Have computer shut down properly
 - Pulling the plug could damage the system, disrupt legitimate business, or create officer or department liability.

Processing Protocol

EXCEPTIONS

- Activity ongoing
- No trained professional available
- Damage risk if not removed immediately

Processing Protocol

All Devices

- Place tape over each drive slot or removable media compartment
- Diagram and label device and components with existing connections
- Label all connector/cable ends
- Photograph all connections for reassembly

Processing Protocol

- Disconnect connections and cables
- Pack components for transport
- Keep away from magnets, radio transmitters, liquids, etc.
- Collect all peripheral devices, cables, keyboards, and monitors
- Collect manuals, documentations, and notes
- Look for potential passwords or keywords to search data.

Other Devices

- Wireless, Mobile, Cordless Phones
- Answering, Caller ID Machines
- Electronic Pagers
- Scanners, Printers, Copiers, Fax Machines
- Smart Cards, Magnetic Stripe Cards, ID Cards, Card Printers
- CD Duplicators/Labelers
- Digital Cameras/Video/Audio

...More

- Electronic Games, Home Electronic Devices
- GPS Devices
- PDA's/Palm Pilots/Blackberry/Hand held computer
- Security Systems, Vehicle Computer Devices
- Storage Media
- Skimmers or credit card readers

Forensics Exam

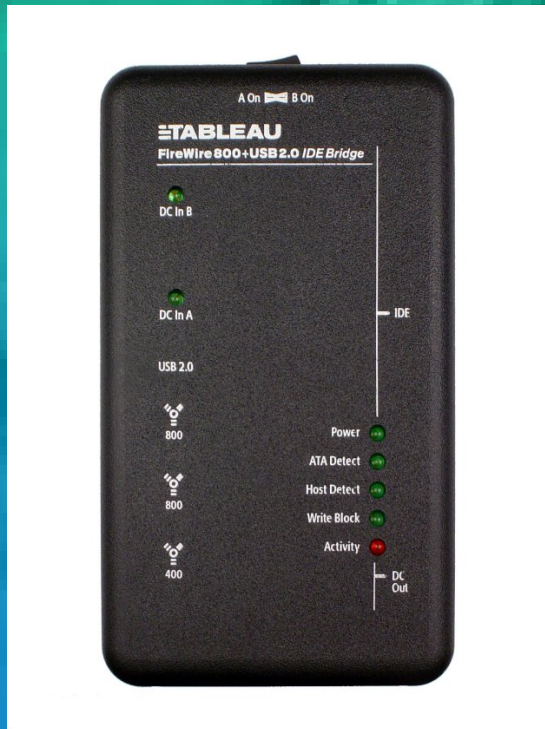
- Follow and maintain chain of custody documentation
- Write protect all devices
- Create a forensics (bit-for-bit) copy of the device
- Working with the copy conduct forensics exam using validated forensics software.

Chain of Custody

- **EVIDENCE CUSTODY FORM**
 - CASE# / Incident#
 - Item# / Description
 - Make / Model / Serial
 - Other Identifying #
 - Date / Time
 - Name / Organization / Signature
 - Reason for transaction

Write Protect

- Hardware/Software
 - IDE / SATA, SCSI, USB, Firewire



Conduct Exam using a Copy

- Must use a bit-for-bit validated forensics copy of the media
- Forensics Software
 - EnCase - <http://www.encase.com/>
 - AccessData FTK - <http://www.accessdata.com/>
 - Helix - <http://e-fense.com/helix/>
 - Coroners Toolkit - <http://www.porcupine.org/forensics/tct.html>
 - Sleuth Kit / Autopsy - <http://www.sleuthkit.org/index.php>

Resources

- DoE
 - www.linuxsecurity.com/resource_files/documentation/firstres.pdf
- DOJ
 - www.usdoj.gov/criminal/cybercrime/searching.html
- NIJ
 - <http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm>
 - <http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm>
- Secret Service
 - www.secretservice.gov/electronic_evidence.shtml

Resources

- Searching and Seizing Computers
 - www.cybercrime.gov/s&smanual2002.htm
- Computer Security Incident Handling Guide
 - csrc.nist.gov/publications/nistpubs/index.html
- EnCase
 - www.encase.com
- Professional Organizations
 - HTCIA – www.htcia.org

A blue-tinted photograph of a computer keyboard. The word "Questions?" is written in white, sans-serif font, centered over the keyboard. The background is a solid blue color.

Questions?

Calvin Weeks, EnCE, CISSP, CISM
Director, Oklahoma Digital Forensics Lab
University of Oklahoma
Information Technology

Email: cweeks@ou.edu

Phone: 405-325-5902

Website: <https://odfl.ou.edu>