

Computer Forensics and First Response

Doug White, PhD CISSP CCE

Roger Williams University

Recommendations

- Electronic Crime Scene Investigation: A guide for first responders
- U.S. Department of Justice
- www.ojp.usdoj.gov/nij

Latent Evidence

- Like some forms of physical evidence (e.g. fingerprints), electronic evidence is both fragile and often not “Evident”.

4 Key Traits of Electronic Evidence

- Latent (not obvious)
- Can easily move beyond the borders of the scene
- Is fragile and can be easily altered, damaged, or destroyed
- May be time sensitive

Profiling Black Hat Hackers

- What would indicate a Überhacker
 - Multiple computers in evidence (especially in one workspace)
 - Partially assembled computers and computer components in evidence
 - Books or computer showing LINUX, UNIX, C++, or other operating systems besides Microsoft Windows
 - Unusual Networking Setups
 - Cable Modem with a separate computer behind it
 - Racked equipment
 - Use Level – High
 - Ability Level – Expert
 - Risk Level -- High

Why Profile Black Hats?

- Be Aware:
 - Hackers love to mess with people
 - Bombs (of the logic variety) and traps for the unwary
 - Self Destruct approaches

Important Pieces of Electronic Evidence

- You need to have a search warrant specific to the devices and appropriate to the situation
- CPU
- Storage Media
 - Floppy Disks, CDs, DVDs
 - Thumb Drives, Flash Memory
 - USB Devices – Hard Drives, etc.
 - Be advised, storage may be remote
 - Wireless Devices
- Cell Phones, Cameras, Video Recorders
- Loose Computer Equipment
 - Hard Drives (important)
 - Most other parts do not contain information
- On commercial computers, there is likely a service tag number that can be used to identify who purchased the machine via a website (like dell.com)
- Networking Equipment often has logs

More Technical Devices

- PDA's, Palms, MP3 Players
- Answering Machines (tapes and digital)
- Caller ID boxes
- Fax Machines/Copy Machines (multifunction printers)
- Digital Watches
- Cable Modems, DSL Modems
- Dongles, Flash Cards
- Phone Cloning Equipment and Cables
- Magnetic Stripe readers
- ID Cards with Stripes
- FastPass Equipment
- Tapes and Backup Media
- GPS Devices

Electronic Devices

- Be sure and confiscate power cords and adaptors (DC convertors, etc.) and keep with the devices.
- Be advised, it is usually NOT a good idea to turn off, shut down, or remove power from any running media.
- If you must unplug or move any equipment, photos are very helpful, particularly of the connections and devices.

Some General Suggestions

- Don't unplug anything unless it is a safety matter or you have to chose between destruction of the device and its removal.
- Protect storage devices and equipment from water, static, and electrical discharge
- Be careful about equipment that is plugged into other outlets or strips
- Monitors contain no useful information or other system materials
- Printers might contain evidence in their logs or unprinted documents in memory (so don't power down)
- Fax machines often store documents in memory until they are requested.
- If you feel there is a threat to the system from an external source, you might consider "airgapping" it but this would be only if you really feel there is a threat.

Static and Magnets

- Static electricity may damage or destroy smart cards, memory sticks, and other unprotected media.
- Magnetic sources can destroy media (like floppy disks and memory sticks) and can be generated by fluorescent lights and electrical generators (not to mention magnets)

Things you might have

- Plastic Sheets to protect from water
- Cable Tags
- Labels and Markers
- Toolkit
- Antistatic Bags/Evidence Tags

Thanks

- Doug White
- Doug.white@whitehatresearch.com
- www.whitehatresearch.com

Steps at the Scene

- Ensure the Safety of all persons at the scene
- Protect ALL evidence, physical and virtual
 - Visually identify all virtual evidence and ensure it is secured
 - Document and photograph all virtual evidence
 - If you see any passwords, document carefully
- If it is on, leave it on, if it is off, leave it off.
- Be sure and document any cables
- Airgap equipment by disconnecting from the wall any telephone lines (small connectors) and if you feel it is necessary any networking cables (large connectors)
- Don't forget to take documentation and search work areas for passwords and information

Other Scene Information

- Take note of anything on monitor screens (you should photograph them if possible)
- Note which machines were on and which were off.
- You may also note machines that were recently turned off by how warm they are.
- Fan noise may be a tip that the machine is running if there is no other indication.
- Small green and yellow lights on the back of the computer are usually the network and do not indicate the computer is actually on.

Photos

- Photograph front and back of computers.
- Either document or photograph (if readable) serial numbers and service tag numbers.
- Photograph the workspace. (e.g. left handed mouse).
- Photograph the screen. You may turn on the monitor using the on switch on the monitor.

Other scene issues

- Fingerprinting procedures may damage equipment (chemicals) so electronic evidence should be recovered prior to processing however this can be damaging to fingerprints so take precautions.
- Be sure any papers or notes around the work area are checked for passwords and account information before being taken for evidence (particularly if different groups handle the different evidence).
- If you have to do anything, be sure and document it carefully.
- If you have to “wake” a monitor, do this by moving the mouse, **DO NOT CLICK OR HIT THE KEYBOARD.**