Electronic Crime Scene Investigation

CJ341 – Cyberlaw & Cybercrime
Lecture #19

M. E. Kabay, PhD, CISSP-ISSMP
D. J. Blythe, JD
School of Business & Management

1

Topics

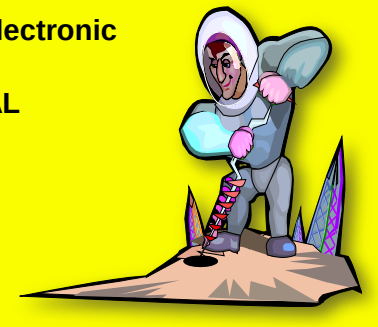
- Introduction
- Nature of Electronic Evidence
- Handling Electronic Evidence at the Crime Scene
- Electronic Devices
- Securing and Evaluating the Scene
- Documenting the Scene

ECSIGFR = *Electronic Crime Scene Investigation: A Guide for First Responders (NIJ)*

Another useful reference: Volonino, L., R. Anzaldua, J. Godwin (2007). *Computer Forensics: Principles and Practices.* Pearson Prentice Hall (ISBN 0-13-154727-5). xviii + 534. Index.

Introduction

- Law Enforcement Response to Electronic Evidence
- Latent Nature of Electronic Evidence
- RULE 1 OF DIGITAL FORENSICS
- Forensic Process



3

Law Enforcement Response to Electronic Evidence

- Computers involved in crime may be
  - Tools
  - Repositories of evidence
  - Targets
- Personnel of many types may be involved in responding to crime involving computers
  - LEOs
  - Investigators (private, corporate)
  - Forensic examiners
  - Managers (case, corporate, political)
- First responder can be anyone in LE
  - Must safeguard EE against loss or tampering

4

Latent Nature of Electronic Evidence [EE]

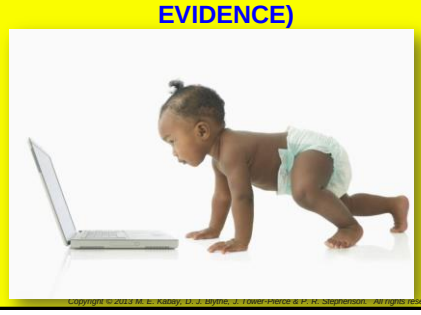
- "Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device." [ECSIGFR p. 17]
- EE thus *latent* (like fingerprints, DNA evidence) because not immediately visible
  - Requires technical equipment & expertise
  - May need expert testimony in court to explain analysis
- EE fragile
  - Easily destroyed or altered
  - Chain of custody & technical safeguards essential for successful prosecution

5

RULE 1 OF DIGITAL FORENSICS

HARM NOTHING!

(E.G., DON'T LET AMATEURS COLLECT DIGITAL EVIDENCE)



6

Forensic Process

Key phases:

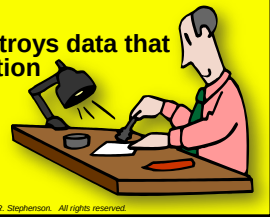
- Collection: search / recognition / collection / documentation of evidence
- Examination (technical perspective)
  - Document content / state of evidence
  - Reveal hidden data
  - Identify relevant data
- Analysis (legal perspective)
- Reporting
  - Process notes for expert testimony
  - Results
  - Reliability

7

Nature of Electronic Evidence

Quoting directly from ECSIGFR p. 20

- Is often latent in the same sense as fingerprints or DNA evidence.
- Can transcend borders with ease and speed.
- Is fragile and can be easily altered, damaged, or destroyed.
- Is sometimes time-sensitive
- Therefore only those with expertise should handle digital evidence
  - E.g., rebooting alters or destroys data that could be useful in investigation
  - Forensic data-capture tools often require training



8

Handling Electronic Evidence at the Crime Scene

- Preparations
  - Secure and document crime scene (photographs, sketches, notes)
  - Use protective equipment to avoid contaminating crime scene (e.g., gloves)
- Recognize and identify evidence
- Document electronic equipment at crime scene
- Collect and preserve EE
- Package and transport EE
- Maintain chain of custody

9

The Digital Forensics Tool Kit (1)

Volonino *et al.* p 126 ff
ECSIGFR p 23 ff

- Cellular phone
- Basic hardware toolkit: screwdrivers, pliers, duct tape etc.
- Watertight & static-resistant plastic evidence bags
- Labels and indelible markers
- Bootable media: DOS startup, bootable CDs, bootable USB drives w/ forensic software
- Cables: USB, FireWire, CAT5 crossover & straight-through, power cables
- Laptop computer for tools and notes
- PDA with integrated camera & link to PC

10

The Digital Forensics Tool Kit (2)

- High-resolution camera(s) w/ date-time stamps
- Hardware-write blocker (e.g., FastBloc, DriveLock) to prevent damage to removed drive
- Luggage cart
- Flashlight
- Power strip
- Log book
- Gloves
- External USB hard drive
- Forensic examiner platform (e.g., specialized tools) for data acquisition

11

Specialized Forensics Tools

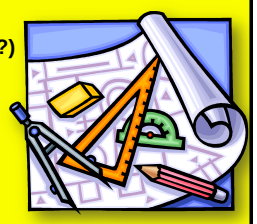
- E.g., *Logicube*® < http://www.logicube.com/ >
- Popular hard-drive cloning systems
- Used by
  - Law enforcement
  - Military
  - Internal IT departments
- Products support various drive interfaces and connectors
  - IDE
  - SATA
  - SAS
  - SCSI
  - USB

12

Establish Your Search Parameters

Volonino *et al.* p 129

- What types of evidence are you looking for?
  - Photographs? Document? DBs? E-mail?
- What is the user's/suspect's skill level?
- What kind of hardware is involved?
  - Computers (Mac? Windows? Linux?)
  - PDAs? Cell phones? Watches?
- What kind of software is involved?
- Do I need to preserve other types of evidence?
  - Fingerprints? DNA?
- What is the computer environment?
  - Network? (Protocols, topology…) ISP?
  - Security? UserIDs? Passwords? Encryption?
  - Real bombs inside the cases *[thanks to Chris Tanguay]*

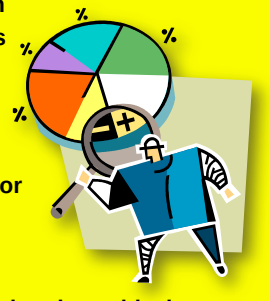


13

Managing the Onsite Investigation

Volonino *et al.* p 130 ff

- Maintain integrity of data collection process
- Estimate time required for onsite examination
- Limit costs to target organization
  - Legal liability for interruptions of business
  - May outweigh importance of crime
  - May stop investigation
- Evaluate necessary equipment for onsite work
- Evaluate personnel costs
  - Who should be onsite?
  - Would their involvement impede other critical investigations?

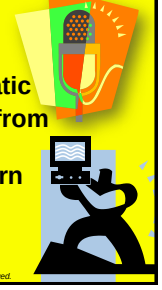


14

Remove Suspect from Computer

Moore Ch 9

- Potential for instant data deletion by suspect
  - Can prepare programs to delete key evidence
  - Activate at touch of keyboard (macros, "hot keys")
  - Or through voice-command interface
    - ✓E.g., Dragon Dictation, Windows voice-recognition
- *No-knock* search warrants still problematic
- Therefore instantly move suspect away from computer
  - Shake hands with LEO & prevent return
  - Physical force only if necessary
  - Allow no return to computer



15

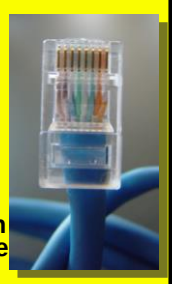
Secure the Scene

- Photograph scene
  - Agencies are currently using digital cameras
  - But recall discussion of falsifiability of digital images
  - Use video camera to document process
  - May see cases hinging on credibility of such evidence
    - ✓Defense sometimes challenges timestamps
    - ✓But claims of fraud / error must include likelihood (proffer of proof)
- Photograph computer screen(s)
  - Especially evidence of system time
- Photograph *everything* that may be evidence
  - Cost is not a factor w/ digital cameras

16

Disconnect Outside Control

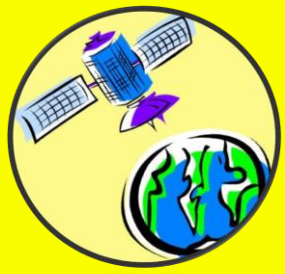
- Remove network connectivity
  - Phone line / DSL
  - Cable / satellite modem
  - Suspect may be storing evidence on remote systems
- Wireless connectivity may be more difficult to handle*
  - Wireless I/F may be integrated within computer case – not obvious outside
  - Especially true in laptop computers
- Look for evidence of home network
  - May have data storage in other locations



*For more details see "The Need for a Technical Approach to Digital Forensic Evidence Collection for Wireless Technologies" by B. Turnbull & J. Slay (2006) < http://www.itoc.usma.edu/Workshop/2006/ Program/Presentations/IAW2006-07-1.pdf >

Handling Downloads

- What if system shows signs that user was downloading file(s)?
  - Could be evidence
- *Photograph* download window
  - Reduces chance that suspect can successfully deny involvement in download
  - May allow download to complete
- Videotape entire process



18

Powering Down Computer

ECSIGFR p 30 ff

Want to avoid damaging data

- Determine Operating System
- Save Data from Running Programs?
- Save Data in RAM?
- Handling Specific OSs
- Laptop Computers

19

Determine OS for Mobile Devices

- GOAL: make bit-images of RAM and of DISK before going any further
- OS does *not* much influence which tools for bit-image capture on
  - Mac versions
  - Windows versions
  - Unix flavors
- OS *does* influence which tools to use for bit-image capture from *mobile devices*
  - Hardware-specific OSs (cell phones, PDAs)
  - Must have right tools and procedures
  - Avoid imprecise copy
  - Subject of more advanced courses

20

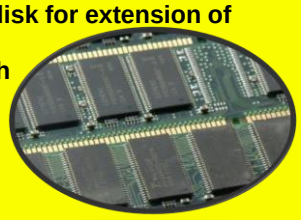
Save Data from Running Programs?

- May be able to see that programs are running (e.g., on program bar)
- Disagreement among experts
  - Pull the plug: data in temporary regions on disk anyway; or
  - Save the temporary data explicitly in case they have not yet been written to disk
- Technical knowledge essential
  - E.g., many OS use extensive *write-behind buffering*
  - Encrypted volumes may be corrupted by instant power-down

21

Save Data in RAM?

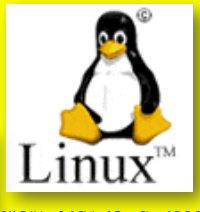
- Most OSs use Virtual Memory (VM)
  - Reserve space on hard disk for extension of main memory (RAM)
  - Swap data back and forth between VM and RAM
  - Thus VM swap file a treasure-trove of potentially valuable data about what was in RAM
  - However, some users disable VM because of large RAM (e.g., 12 GB)
- Specialized utilities for saving data directly from RAM depending on OS & hardware
- Particularly important for cell phones and PDAs which may depend on battery power for maintenance of volatile memory



22

Handling Specific OSs at the Scene

- Not suitable topic for this course
- For brief overview of instructions involved, see Moore p 175 ff
  - Microsoft OSs
    - ✓Windows 3.11 through XP
  - Macintosh
  - Unix/Linux
- Special tools for PDAs (e.g., Palm, Windows CE)



palm

23

Laptop Computers

- Problem: unplugging laptop instantly switches to battery power
- Need to remove battery from laptop
  - Usually easy
  - Simple latch or an easy screw or two
- Keep battery with laptop for bagging & shipment

* TRS Model 100 from 1983
Computer Desktop Encyclopedia
Used with permission.
Prof Kabay's very first portable…

24

Disassembling Computer

- Critically important that each computer can be reassembled exactly as it was
- Identify each computer with unique identifier
- Label absolutely every component with its computer's identifier
  - Particularly the ports
  - Mask and mark ports not in use
  - Masking tape or colored labels are fine
  - Colors can be assigned to specific computers
- Show directions of connectors (which end to which computer and port)

25

Securing Additional Evidence (1)

- How much peripheral equipment should you seize?
  - Terms of warrant
  - Peculiarities of system (e.g., old)
- Peripherals may have evidence
  - Cameras, games (XBox, PSPs)
  - Scanners (check the scanner bed)
  - Sound recorders, iPods (can even carry computer data or operating environments)*
  - Calculators (large memory)
- Other evidence
  - Paper notes and documents
  - Digital storage media (magnetic & optical disks – but remember old tape systems)
  - Label evidence bags in detail (where, who…)

*Thanks to Ryan Davis & Stanley François

26

Securing Additional Evidence (2)

- Already mentioned obvious devices
  - PDAs, cell phones, data-watches
- USB flash drives may not be obvious
  - Small
  - May look like pens
  - May look like … *wait for it* … sushi!

27

Preparing for Transport

- Complete asset-seizure log
  - Provide copy to suspect
  - Get suspect to sign log sheet
  - Note refusal & have OIC sign sheet
- Bags or boxes depending on agency
  - Do not use Styrofoam – static electricity
  - Disk drives that take mobile media (floppies, CDs) should have blanks inserted to prevent damage in transit
- DO NOT PUT IN TRUNK OF CAR
  - Heat & electronic gear can harm evidence
  - Place on floor or on storage surface

28

Chain of Custody

- Standard concerns about maintaining credible *protection of evidence* in custody
- NEVER allow evidence to be unsecured at any time
- Digital evidence can be altered at any time
- Unique identification to ensure credibility in court
- Detailed records of *who accessed the evidence* at *what time* and for *how long*
- Provide detailed records of *why individuals needed access to evidence*
- Ideally, original data must never be released – keep for *comparison* with digital bitwise copies if anyone challenges authenticity

Now go and study

30