Digital Forensic Investigations
COS783
The Traditional Digital Forensic Investigation Process
Prof HS Venter
hventer@cs.up.ac.za

Copyright © HS Venter (2015)

Contents

• Crime scene evaluation (planning)
  – Chain of custody
  – The digital forensic examiner
• Evidence collection (acquisition)
  – Potential sources of evidence
  – Separating the wheat from the chuff
  – Flowchart for seizure of electronic evidence
Contents

- Evidence storage (preservation)
  - Disk imaging
  - Preservation of data
  - Management of evidence storage
- Evidence analysis (investigation)
  - Techniques
  - Concealment techniques
- Reporting (findings)
  - Strategy
  - Tactics

Digital Forensic Process

- Crime scene evaluation (planning, identification)
- Evidence collection (acquisition, extraction)
- Evidence storage (preservation)
- Evidence analysis (investigation, interpretation)
- Reporting (findings, communication)
Crime scene evaluation

• Crime scenes differ in two ways:
  – Crime scene in “uncontrolled” environment
  – Crime scene in controlled environment, e.g. office

• Should have the necessary police investigation background to secure crime scene

• Examine company policy statements

• Internal/corporate vs police investigations
  – Corporate investigator investigate policy violations
  – Police investigate civil/criminal crimes

• If employee committed civil crime, case must be handed to civil law enforcers (police), otherwise corporate investigator becomes liable
  – Consult legal advice if there is uncertainty

• Inform management
  – Might be concerned about commingled data

• Police search warrant should be obtained

• A subpoena or search warrant allows you to investigate without being a police officer
Crime scene evaluation – processing a crime scene

• May only obtain search warrant to investigate if probable cause exist.
• Probable cause requires meeting these criteria:
  – Specific crime was or is about to be committed
  – Evidence of specific crime exists
  – Place to be searched includes evidence of specific crime

Example search warrant wording (ccu.mdsp.org)

  “Seize and examine, by persons qualified to do so, and in a laboratory setting, any and all electronic data processing and computer storage devices, including: central processing units, internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, optical readers and scanning devices, CD Rom drives and Compact Disks and related hardware, digital cameras and digital storage media, operating logs, software and operating instructions or operating manuals, computer materials, software and programs used to communicate with other terminals via telephone or other means, and any computer modems, monitors, printers, etc., that may have been used while engaging in [specify the illegal conduct], as defined in the Annotated Code of Maryland, amended and revised.”
• Probably most important step
• Identify the nature of the case
  – Is it a corporate/internal investigation or civil/criminal case?
• Identify the type of computing system
  – Might be difficult for civil/criminal case: uncontrolled
  – Determine system type, number of systems, hard drive sizes, Oss etc.

• Determining whether you can seize a computer(s)
  – Do you have a warrant if a civil/criminal case?
  – If corporate case, you need manager’s approval
  – More convenient to seize computer and work at lab
  – If seizing would irreparably harm business, you cannot!
    • In such case, seize data from site with necessary equipment
• Obtain a detailed description of the location
  – Identify potential hazards on the scene (HAZMAT)
  – Use special HAZMAT bags
Crime scene evaluation – preparing for a search

• Determine who is in charge of crime scene
  – Corporate case allows only one person to respond
  – Civil case allows more people to collect evidence
  – At large scene, cooperate with leader

• Using additional technical expertise
  – Any additional technical expertise needed

• Determining tools you will need
  – Initial/extensive response field kit
    • Large capacity HDD, IDE ribbon cable, forensic boot disk, write blocker, flashlight, digital camera, laptop, evidence labels…

Crime scene evaluation – preparing the investigation team

• Review all available facts, plans & objectives with investigation team

• Goal to successfully gather and secure evidence

• The better prepared, the fewer problems!

• Respond as quick as possible
  – If too slow in certain environments, might risk losing important information.

• Need skilled team
Crime scene evaluation – physically securing incident or crime scene

- To preserve evidence and keep it confidential
- Use barrier tape – enforce by officers/guards
- Access restricted only to investigators
- Secure large enough area – shrinking a scene is easier than expanding it
- Digital evidence are abstract, but crime scene can also contain physical evidence e.g. DNA
- Professional curiosity can contaminate scene

Crime scene evaluation – The digital forensic examiner

- Role is discover evidence (facts)
  - Include, amongst others, gathering deleted/erased/damaged info, passwords etc
- If enough evidence gathered, all else untouched
  - However, may leave further evidence behind!
- Must decide when to “stop”
- May reveal another crime in an investigation
- Must prove every step taken
- Latent evidence (DNA)
Evidence collection

- Any items to be considered evidential value are collected
- These items include
  - Computer, Monitor, Keyboard, Mouse, Printer, Scanner, Modem, External Storage Devices (CD Drives, Zip drives, Tape Drives, External hard drives, etc), Removable Media (Floppy disks, compact disks, zip disks, etc.), Computer Manuals, Software, Digital Cameras (Including flash memory cards, Smart Media, Compact Flash, and Memory Sticks), Notebook Computers, Handwritten notes and notebooks containing names and/or e-mail addresses, website addresses, passwords, etc., PDA, palm computers etc

Evidence collection

- Requirements for evidence collection
  - Authority identification
    - Who has accessed, changed or created records
  - Authority verification
    - Verification of the authenticity of changes, access and created records
  - Authority validation
    - Ensuring that the recording processes themselves are validated and reliable
  - Availability and archiving
    - Ensuring records are available and stored in a format that is usable and accessible and can be viewed any time
Evidence collection – seizing digital evidence at the scene

- Search warrant determines what can be seized
  - Rarely authorised to seize absolutely everything
- Corporate case might require less work than a civil/criminal case
- Follow rules for civil investigations by US DoJ: www.usdoj.gov/criminal/cybercrime

Evidence collection – processing a major incident or crime scene

- Keep a journal to document ALL activities
  - Date/time arrive
  - People on scene
  - Steps taken to secure scene
  - Notes of every significant task
  - Nothing moves in scene unless it is recorded
- Be professional and courteous to spectators, but do not divulge any info – send journalists to public relations officer of your team
Evidence collection – processing a major incident or crime scene

• Remove anyone not investigating on scene
  – However, people like administrator might need to stay to help gather evidence

• Take videos and/or photographs of:
  – Overall scene
  – Back of computers (place labels on each first)
  – Label other items like wires/plugs etc
  – Area around computer, including ceiling & floor

• Sketch scene with notes on distances, positions etc of objects in relation with each other
• At scene, sketch rough. In report, computerised.
• Record whether computers are on/off
  – If off, proceed with data acquisition, else
  – Pull the plug from the wall – do NOT shut down
    • Sometimes need to recover volatile data in RAM. Decide how important that is for case. If important, do NOT pull plug
    • Acquire volatile info
  – If acquiring live info, make notes of EVERYTHING
Evidence collection – Processing data centers with an array of RAIDs

• Disk farms
• Sparse evidence recovery
  – Only data of interest is acquired
• Cloud environments

Evidence collection – Using a technical advisor at scene

• When working with advanced technologies
• Help to create search warrant, itemising what’s needed
• Responsibilities
  – Know all aspects of the system being seized
  – Direct investigators how to handle sensitive media
  – Help ensure security on scene
  – Help documenting the planning strategy
  – Conduct adhoc training for investigators
Evidence collection – Chain of custody

- Legal term that refers to the ability to guarantee the identity & integrity of evidence item from the time it is collected through the time the results of analysis are reported and disposed of.
- Assures continuous accountability
- If not properly maintained, item not admissible
- Consist of chronologic record of those individuals who have had custody (handled) the evidence from its collection until its final disposition
- Each person in chain responsible for evidence

Evidence preservation

- Preservation of seized items in a manner that is
  - Reliable: yield consistent results and dependable
  - Complete: contains all relevant info
  - Accurate: free from error
  - Verifiable: any other investigator would come to same conclusion if same procedure is followed
- Documentation of all items and the use of hash functions to ensure that data items were not altered
Evidence preservation – Disk imaging

- Disk-to-disk or disk-to-image
- Bit-by-bit exact copy of entire disk
- Create cryptographic hash of disk, used for preservation verification
- dd

Evidence preservation – Determining best acquisition method

- Many other tools (EnCase, FTK, SMART, Sleuth Kit, X-Ways)
- Storage requirements
- Lossless vs lossy compression
  - Lossless – acceptable
  - Lossy – not acceptable
- Use lossless compression for large disks
- If original drive cannot be retained, act quick
- If system cannot be taken offline long, act quick or perform sparse copy
Evidence preservation – Management of evidence storage

- Storage area should protect evidence in orderly, traceable and retrievable way while preserving integrity of the evidence
- Storage area secured from unauthorised entry
- Accurate record must be kept of evidence entering or leaving the storage area
- Routine “stock take” of evidence in storage area
- Documented disposal process must be in place
- Use ACLs for electronic evidence

- Storage area should have ambient climate control between 15 and 20 degrees, 0% humidity
- Storage area should be dust free
- Far away from large electrical circuits or magnetic fields
- Fire control should be by oxygen deprivation, not by sprinkler system
- Not be located near any source of vibration
- No direct sunlight allowed in storage area
- Additional access controls
Evidence preservation – Management of electronic evidence storage

• Increasing size requirements of evidence
• Need large storage space
• Mainly secondary storage requirements
• 30 years ago, 5mb in same size that we now put 4TB of data
  – Parallel: if a car of the 1980s used 8 liter / 100km fuel, cars of today is supposed to use same amount of fuel but be able to travel 10000km with it, not just 100.
  • (it is a pity it does not work this way with cars!)

Evidence preservation – Management of electronic evidence for analysis

• Storage that are currently being analysed
• Eventually becomes the actual record in court
• Auditing of every single action taken on the data must be enabled
• Proper access control must be maintained
Evidence preservation – Management of electronic evidence movement

- Demanding task
- Transfer rate over 1GB/s network is effectively only about 40MB/s
- From HDD to HDD still only about 60-90MB/s
- Not simply copying data around in storage area; intensive computing i.e. hashing, verification etc.
- Policies & procedures for movement of data
  - Copies of copies: Is there limit on no. working copies?
  - Who is responsible for creation of copies?
  - How are copies transported?

Evidence preservation – Management of electronic evidence movement

- Availability vs viability
  - Fast equipment more expensive – is it viable for your scenario?
  - Impacts on the productivity of analysis staff
Evidence preservation – Management of electronic archiving

- Archival storage facility
- Copy to permanent media
- Catalogue/label it well
- Digital archive can deteriorate!
- Archive management a continuous process
- Archiving media
  - Magnetic tape
  - Optical media
  - RAID/NAS

Evidence preservation – Management and maintenance of archival storage

- Archival management plan
  - What to archive
  - How stored and maintained (media)
  - When does the archive expire?
    - Differ from 5 to 75 years in different jurisdictions
    - Storage of even 5 years of archives is challenging
- Specialist skill is needed – not the DF investigator
- Moving data from old to new media before it deteriorates
- Destroying expired archives
Evidence analysis

• Address the extraction of individual elements of information (pieces of evidence) that may be significant to a particular case
• Depends on the nature of investigation and amount of data to be analysed
• May be limited to data as defined in warrant
• Scope creep – widening the scope in a bid to uncover more revealing evidence

Evidence analysis – evidence characteristics

• For useful evidence, must have characteristics:
  – Admissible
    • Acceptable for use by courts and other bodies
  – Authentic
    • Show that evidence is relevant and relates to incident
  – Complete
    • Not just material that provides evidence of guilt, but complete set
    • Also include evidence that may prove innocence
  – Reliable
    • Must have no doubt about the evidence
  – Believable
    • Must be clear to judge
Evidence analysis – refining the investigation plan

- Determine the scope of the investigation
- Estimate no. of hours to complete investigation
- Determine if only subset of evidence will be needed for investigation of large case (sparse)
- Determine if scope creep is allowed (what does search warrant say?)
- Do you have adequate resources?
- Establish deadline

Evidence analysis – general tasks to perform on electronic evidence

- Examine file/directory date/time stamps
- Locate and extract all log files
- Locate and recover any temporary print spools
- Locate and recover any encrypted/archived files
- Perform keyword search on all relevant data
- Examine
  - Shortcut/link files
  - Internet cache files
  - Recycle bin
  - Registry
Evidence analysis – general tasks to perform on electronic evidence

• Keep up with how data is stored in particular OSs
  – Can current forensic software handle this?
• Determine suspect’s motive
• Ascertain how suspect is accomplishing crime
• Play the role of a criminal profiler, or outsource
  – Determine what to look for – each case is different
  – Look for pattern in suspect’s actions
  – Only, you need to profile digitally
• Start the investigation using resources (tools)

Evidence analysis – concealment techniques

• You cannot find what you cannot investigate
• Begin with more obvious places
  – Slack space
  – Swap files
  – Drive slack
• Very difficult for investigator to stay ahead of techniques
• Investigator must remain vigilant, keep informed and continually educate themselves (courses)
Evidence analysis – concealment techniques

- Spoliation
  - Destruction of evidence or failure to preserve it
  - Can be accidental or intentional
- Cryptography (much more later in course)
  - Secret key (symmetric)
  - Public key (asymmetric)
  - Hash functions
- Secret sharing
  - k out of n people have enough info to uncover secret

Evidence analysis – concealment techniques

- IP spoofing
  - Man-in-the-middle
  - Routing redirect
  - SYN flooding
- Session hijacking
  - Similar to spoofing – encountered at log-on
- Polymorphysm
  - Viruses, trojans, zombies, backdoors
- Steganography
  - Hides contents in a covert channel
Evidence analysis – concealment techniques

• Anti-forensics
  – Covering tracks

• DoD write
  – Wipes free space by overwriting with hex data
  – Basically wipes all free space beyond recovery

Evidence analysis – concealment techniques

• Cloaking techniques
  – Swap files
  – File slack
  – Renaming files
    • File name/extension modification
    • Hiding file extensions by setting attribute properties
    • Ghosting: e.g. change colour of font from black to white
    • Compressed files
Evidence analysis – concealment techniques

• Manipulating file systems
  – FAT
  – NTFS
  – File storage hardware & disk organisation
  – Sectors & clusters
  – Slack space
  – NTFS alternate data streams
• Wiping tools
• Rootkits

Evidence analysis – concealment techniques

• Forensic eavesdropping
  – VoIP
• Direct kernel object manipulation
• Hash collisions
• Social engineering
Evidence presentation (Reporting)

- Presentation of evidence (in various forms)
- Must be accurate representation of facts
- Must be understandable to intended audience
- Supported by documentation
  - May include declarations and depositions
- Report should be clear and concise
  - Try to keep as short as possible without losing the intended meaning of evidence representation
  - Must be VERY understandable – a BIG challenge
  - Be careful for too much technical jargon
  - Judge/jury must be able to understand!

The Digital Forensics Process

1. Chain of Custody
2. Evidence collection
3. Evidence Storage
4. Analysis
5. Report

- Emails
- Trace Evidence
- Deleted data
- File metadata
- Pictures
- Access logs
- Lab information system software

Digital forensic process model
Conclusion

- The digital forensics process is vast and extensive
- MUST adhere to the process for evidence to be admissible in a court
- Each of these process phases will be unpacked in even more detail in the remainder of the course