Forensics Best Practices and Creating Procedures

Joshua Lopez

California Lutheran University

IT-540 Digital Forensics

Wayne Snyder

January 15, 2025

Forensics Best Practices and Creating Procedures

1. **Procedure for capturing video of a crime scene** (Best Practices for the Retrieval of Digital Video, 2013, section 24)
   1. Arriving at the scene
      1. Capture detailed notes of steps/methods taken
      2. Find out if the system user manual is available
   2. Confirm that the applicable video has been captured by reviewing footage
      1. Someone knowledgeable about the device operating during the review
         1. This will help if any authorized authentication is required
         2. Insure a progressive maneuvering to the video in question
   3. Determine the earliest recorded date/time.
      1. Helps to gauge how much time is left before the system overwrites footage
         1. Example, it was 7 days ago. You have that amount of time to review.
      2. It is best if the owner or security staff performs the retrieval
         1. This will be helpful for authorization needed to extract the data
      3. Also, if the system installer company or experienced operator is available to assist
         1. It would be wise to have the vendor present in case of technical difficulty not experienced before
   4. Document the following system details
      1. System and camera(s) make, model, serial number
      2. Is the system a standalone or PC Based
      3. Number of recording units installed
      4. Is the system networked
         1. Confirm you have admin rights on the computer downloading to
         2. Firewalls are disabled
         3. Confirm network speed is adequate
            1. Avoid data loss/crashes
      5. Recording Capacity
         1. If replacing the hard drive
            1. Properly shut down the system even if hot-swappable
      6. Number of camera(s) and the active camera number
      7. Any camera(s) infrared sensitive?
      8. Is audio being captured?
         1. If yes, the number of channels and if retrievable.
      9. System configuration settings.
         1. Image quality, frames per sec, etc.
      10. Request a copy of the maintenance log
      11. Scene contact information
          1. Address, hours, POC, etc.
      12. Photograph of the system. Front and Back.
      13. Native file format system uses
2. **Assess The Recording System**
   1. How much and type of data to be retrieved
      1. Study the output options to determine the best and most practical method for retrieval
         1. Most systems will have an export function
            1. Allow you to copy proprietary viewer while burning video
   2. Some systems have flash media as an option.
      1. This is not suggested as flash is not intended as permanent storage
         1. Verify that media copy can playback
            1. USB/DVD/CD for retrieving smaller amounts of data

Use Write Once – CDs

* + - * 1. The best practice for large data amounts is an external hard drive
        2. Determine how much data needs to be retrieved

Create a **forensic** clone to a more permanent media(Master Evidence – with write blocker)

Work on a copy, not the original copy from the scene

Maintain integrity of data

1. **Type of Evidence to Screenshot** (Advanced Digital Forensic Solutions [ADF], 2023)
   1. Digital Evidence(Screenshots)
      1. Text Messages
      2. Social Media Posts
      3. Contacts
      4. Installed applications
   2. Must be authentic
   3. Follow the Chain of Custody
   4. Relevant to the case
   5. Expert Testimony may be required to explain said relevance
      1. Helps create a timeline of events
   6. Recommended Software(Best Practice Tools)
      1. ADFs Mobile Device Investigator(MDI)
         1. Extract, analyze, and present digital evidence
         2. Take notes of findings during the acquisition phase
2. **Recording Computers Time Offset** (Raincock Consultancy & Raincock, 2011)
   1. Device time setting
      1. Device may self-regulate
      2. Assumption device sync with GPS Signal
   2. Examining devices
      1. Their date and time settings are recorded
         1. Compared to current time
            1. Difference between them

The Offset

* + 1. Significance
       1. Applied to all timed evidence on the device
       2. Alone cannot establish the accuracy of events
       3. Establishes the accuracy of examination date and time
       4. Determine if time sync is with a server
       5. Determine if time has been tampered with manually
       6. Perform checks to confirm time settings are consistent
          1. Example – cross-reference email

Replied to prior to being received

Examining user access to websites

Timeline of events

Note time may be local time

1. **Collecting Evidence from Memory and Hard Drive** (Easttom, 2021, p. 70)
   * 1. **Consider the life span of information**
        1. Volatility
           1. More volatility = shorter the lifespan
           2. Subject to organizations' practice

Email retention policy

Log files for months or years

Unless regulated

Act Accordingly

* + - 1. Critical in the planning of evidence collection
    1. **Collect Information Quickly**
       1. Changes
          1. Not practical to determine whom or when
       2. The target of the investigation may try to conceal
       3. Unauthorized changes
          1. User does not have to be local
    2. **Collect Bit-Level Information**
       1. Bit-Level Forensic Image
          1. Most accurate view of information stored
          2. File system copy may not retrieve

Slack space

Hidden Partitions

* + - 1. Text, Pictures, Screen Displays, Videos, Audio
         1. All derived from BITS

1s and 0s stored in memory

* + - 1. Evaluate Bit-Level Information
         1. Forensic Tools

Reconstruct fragmented data

Have unrelated bits been inserted

1. **e-discovery** (Easttom, 2021, p. 74)
   1. Three high-level requirements
      1. Find Evidence
         1. Initial Seizure
      2. Preserve Evidence
         1. Avoid changing equipment
            1. Photograph
            2. Label
      3. Prepare Evidence
         1. When was it created
            1. Create Timeline
         2. Bit-Level Search Device
         3. Are there encrypted or steganized files?
         4. Present Evidence
            1. Logical, Compelling, Persuasive

Jury must understand

Solid against rebuttal

* + - * 1. Prepare charts, graphs, and exhibits

Explain how and what was done

Must withstand scrutiny

* + - * 1. Testimony

Simple and Clear

Know your audience

No technical jargon

1. **Interviewing Witnesses(Best Practices)** (Cyber Secure, n.d., Communication Techniques During Interviews section)
   1. Effective Communication
      1. Active Listening
         1. Focus entirely on what is said
         2. Confirm Understanding
            1. Paraphrasing
            2. Ask clarifying questions
      2. Use of Non-Verbal Signals
         1. Eye Contact
         2. Nodding
         3. Facial Expressions
            1. Convey Engagement
      3. Avoid Leading Questions
         1. Not suggesting a desired response
         2. Can undermine the credibility of witness statement
         3. Use open-ended questions
            1. Allows witnesses to speak freely
   2. Cognitive Interviewing Techniques
      1. Sensory Retrieval
         1. Share memories
            1. Using sight, sound, smell, and feelings
            2. Allows for a more textured count of events
2. **Expert Witness(Best Practices)** (Easttom, 2021, pp. 7–10)
   1. No Jargon or Technobabble
      1. Clear
         1. Language
         2. Graphics
         3. Demonstrations
   2. Back-Up Conclusions
      1. Two to Three
         1. Reputable References
         2. Recognized Authoritative Works
            1. Agree or Support
         3. Do not volunteer information
   3. Do not Perjure Yourself
      1. Obfuscate Evidence
         1. Felony
         2. Irrevocable Loss of Reputation
   4. Do not understand question
      1. Ask for clarification
      2. Do not guess
      3. Do not be evasive
   5. Be Prepared
      1. The forensic process is done correctly
      2. Well-documented
         1. Charts
         2. Diagrams
         3. Graphics
      3. Review report and Notes
         1. Objectively
         2. Are there any alternative ways to interpret evidence
         3. Why were they rejected
   6. Skill
      1. \*Avoid exceeding your knowledge
         1. Best Practices
            1. Defer to someone with specialized knowledge

Lack of knowledge in a particular area will become apparent in trial or depo

Resulting in the damaging loss of reputation

* + - 1. Consider Adopting a Standard
         1. Never testify or write a report

Certain of expertise

Relevant technologies

Confident in your conclusions

\*This issue is problematic. The textbook suggests a truth in the IT Industry. It has been my experience that experience and specialized knowledge in a specific area are sufficient to resolve many technical issues that occur at the Enterprise Level. This is not the case. Additionally, I think it is quite dangerous in a production environment. This sometimes leads to individuals adapting the Wild Wild West mentality/approach to resolving issues. With that said, yes, there are applicable analytic, methodical, and troubleshooting skills that are possessed. However, when it comes to specific Operating Systems, Networks, Hardware, and software, it is best to involve Subject Matter Experts(SMEs) in the triage of or conclusions of the general practitioner. I see it often in the field where a general practitioner will google an issue/error in another specialized area and proceed with the resolution. In my experience, this approach has, unfortunately, brought production systems/applications down during business hours. If the practitioner had true knowledge/expertise in the area, he/she would not have needed to “google” information on it. The layperson does that when curious about a topic (Easttom, 2021, p. 69). It is a best practice not to exceed your knowledge. Don’t be a cowboy...

References

Advanced Digital Forensic Solutions. (2023, June 25). 4 Key Considerations for Using Screenshots in Forensic Investigations. ADF. Retrieved January 10, 2025, from <https://www.adfsolutions.com/adf-blog/4-key-considerations-for-using-screenshots-in-digital-forensic-investigations>

Best Practices for the Retrieval of Digital Video. (2013, September 27). Science Working Group On Digital Evidence. Retrieved January 8, 2025, from <https://www.swgde.org/swgit_24/>

Cyber Secure. (n.d.). Techniques for Interviewing Witnesses in Cyber Forensics (S. Karush, Ed.). Retrieved January 11, 2025, from <https://cybersecure.monster/techniques-for-interviewing-witnesses-in-cyber-forensics/>

Easttom, C. (2021). Digital forensics, investigation, and response (4th ed.). Jones & Bartlett Learning.

Raincock Consultancy & Raincock, S. (2011, July 19). Sometimes it's all about timing. Forensic Focus. Retrieved January 10, 2025, from <https://www.forensicfocus.com/articles/sometimes-its-all-about-timing/>