CRJS475 Unit 4 Individual Project - Investigative Steps & Forensic Training

With the advent of cybercrime, tracking malicious online activity has become crucial for protecting people, businesses and national security. Tracking digital activity allows investigators to collect cyber evidence for digital storage and prosecution. Digital evidence involving cybercrimes can be delicate and highly sensitive (Cybersecurity, 2017). Understanding legal concepts, in conjunction with a good training program, will help an agency to conduct digital investigations. Law enforcement cybersecurity experts need to (Cybersecurity, 2017):

- Determine proper investigative procedures.
- Ensure the legal preservation of digital evidence.
- Establish rules governing all digital investigations by an agency.

Digital Constitutional Protections

- 1st Amendment – Freedom of speech
- 4th Amendment – Freedom from unreasonable searches & seizures.
- 5th Amendment – Freedom from self-incrimination

First Amendment

The First Amendment to the U.S. Constitution is famously known for freedom of speech. However, there are limitations to freedom of speech, particularly when it comes to public safety. For example:

- In the year 1919, U.S. Supreme Court Justice Oliver Wendell Holmes said that the First Amendment does not protect free speech if it "presents a clear and present [to public safety]" (Schenck v. United States).
- In some states, it is illegal to write a threat to kill or harm someone. You can explore a Florida State Statute example here.
- You can read more about cyber-harassment or cyberbullying, as it relates to freedom of speech, here.

Fourth & Fifth Amendments

The main purpose of the Fourth Amendment is to protect people's privacy rights. It does so by protecting people from unreasonable searches and seizures by the government – and that includes Constitutional protections for digital data from cellphones, computers, clouds, emails, hard drives, etc. The Fifth Amendment protects people from self-incrimination, which means a person does not have to surrender passwords or digital keys to the government because a person "has a right to remain silent."

Identity Theft in Digital Investigations

In the past, identity theft would happen when people went *dumpster diving*. They would rummage through discarded trash that was left at the curbside. Criminals would look for enough personal-identity information to be able to steal someone's identity. Today, identities are stolen through other online schemes, such as using phishing emails and websites – or hacking into businesses to steal customer's personal information – which can then be used to create new credit card accounts, to make fraudulent online purchases with stolen identities.

In the online world, personal information can be discretely collected by companies through:

- Voluntary disclosure agreements
- Cookies
- Website bugs
- Tracking software
- Phishing
- Malware i.e., worms, trojans and spyware

In some cases, online legal disclosures must be presented to users – and accepted by users – before their personal information can be collected through tracking software. However, criminals do not follow rules or laws – and they have access to the same technologies to subtly get the personal information from online users – without the legal authorization to do so (Atrizadeh, 2021). Online crimes also includes posting fake products on Craigslist or eBay to lure victims into sharing credit card information, which can then be used in identity theft schemes (Cybersecurity, 2017). Identity thieves can also get personal information by watching victims from a close distance, such as peering over their shoulder when they are entering their credit card or bank account information. Identity theft can cause significant damage to a person's credit and reputation (Atrizadeh, 2021).

Digital investigators need to understand how online criminals circumvent security measures against firewalls, network routers and digital devices (Atrizadeh, 2021). If a digital investigator wants to legally prove that a person committed digital identity theft, then he may have to sift through hard drives, email accounts, social networking sites and other digital archives to retrieve and assess any information that can serve as evidence in a criminal case. Before conducting an investigation, the investigator should determine the types of evidence that may be involved – and then figure out how to preserve it, in case it is needed in a future court case. Digital investigators must work in close collaboration with detectives and lawyers to ensure a thorough understanding of the nuances of a case, to include knowing what type of information is evidentiary or pertinent (Cybersecurity, 2017).

First Responders

First responder responsibilities:

- Identify and secure crime scene.
- Preserve digital evidence.
- Acquire known data from the site.
- Conduct preliminary interviews to collect useful information.
- Document preliminary findings for investigators.

Potential first responders:

- Network administrator
- Law enforcement officer
- Investigating officer

Those who are the first to respond to cybercrimes may or may not be adequately trained to conduct advanced digital investigations, but they can still preserve digital evidence that comes to their attention. If digital evidence is properly preserved, then it can be forensically examined at a future date by cyber-investigators who have specialized digital training.

Advanced Digital Investigations

A fully trained cyber-investigator will assess potential evidence in a digital crime (Cybersecurity, 2017). Understanding how a digital investigation will proceed involves (Cybersecurity, 2017):

- Reading preliminary case briefs written by patrol officers, detectives, attorneys or network administrators.
- Obtaining required permissions that might be needed, prior to pursuing the case.
- Understand how warrant-applications work.

Those who are fully trained in digital investigations must consider all of the following basic and advanced investigatory steps (Volonino & Anzaldua, n.d.):

- Obtain legal authorization to search and seize digital evidence (verbal consent or with a warrant).
- Secure the area, which may be a crime scene.
- Document the chain-of-custody of every seized item.
- Bag, tag and safely transport seized equipment and digital evidence.
    - Computers
    - Hard drives
    - Digital documents
    - Digital images
    - Cellphones
    - Flash drives
    - Emails
    - Anything else of evidentiary value
- Acquire digital evidence from equipment by using forensically sound methods and tools to create a forensic image of the evidence.
    - Keep the original material in a safe, secure location.
- Design a review strategy of the digital evidence.
    - Include lists of keywords and search terms.
- Examine and analyze forensic images of digital evidence.
    - Never examine the original.
- Interpret and draw inferences that are based on facts gathered from the digital evidence.
- Describe your analysis and findings in an easy-to-understand and clearly written report.
- Give testimony under oath in a deposition or courtroom.

Forensic Examination

Technical expertise is needed for investigators who examine evidentiary data that has been digitally archived for forensic evaluation. Examination might include (Cybersecurity, 2017):

- Using software to search large amounts of archived data for specific keywords or file types.
- Using digital investigatory techniques to retrieve files that have been deleted by a suspect.
    - Data tagged with times and dates.
    - Suspicious files or programs that have been encrypted or intentionally hidden.
- Analyzing file names to determine when and where specific data was created, downloaded or uploaded. That can help investigators connect files on storage devices to online data transfers, such as cloud-based storage, email and other types of Internet communications.

Policy Development & Forensic Training

- Policy & Procedure Terms:
- Quality Assurance = QA
- Quality Control = QC
- Standard Operating Procedures (SOP)

There are five critical steps in computer forensic investigations that every agency needs to develop, train for and follow (Cybersecurity, 2017):

1. Policy and Procedure Development.
2. Evidence Assessment
3. Evidence Acquisition.
4. Evidence Examination
5. Documenting and Reporting

For example, it is important to develop and follow strict QA and QC procedures during digital investigations. That includes providing specific forensic instructions and training for determining (Cybersecurity, 2017):

- When digital investigators are authorized to recover forensic evidence.
- How to prepare computer systems for evidence retrieval.
- Examination of hardware and software.
- Copying and transferring digital evidence to an evidentiary storage system.
- Documenting and authenticating a chain-of-custody for a court case.

Acquiring evidence must be legal and should be governed by written policies that will help to preserve it.

References

Atrizadeh, S. (2021). Understanding the importance of U.S. privacy and identity theft laws [Legal Analysis]. Information Systems Audit and Control Association. https://www.isaca.org/resources/news-and-trends/industry-news/2021/understanding-the-importance-of-us-privacy-and-identity-theft-laws

Cybersecurity. (2017). 5 Steps for conducting computer forensics investigations. Norwich University. https://online.norwich.edu/academic-programs/resources/5-steps-for-conducting-computer-forensics-investigations

Volonino, L., & Anzaldua, R. (n.d.). Steps to take in a computer forensics investigation [Digital Investigations]. https://www.dummies.com/computers/pcs/computer-security/steps-to-take-in-a-computer-forensics-investigation/