Unit 9: The Investigative Context and Investigative Pitfalls

Welcome to Week 9.
This week's learning further explores issues concerning the digital investigate process. You will consider obstacles in the investigative process and prevention. Here you will address issues concerning reporting, investigative agencies, and knowledge management. These will be addressed in national, international and transnational contexts. You will also reflect on issues concerning the admissibility of evidence digital evidence in court.

On completion of this unit you will be able to:

- Explore issues concerning the investigative context.
- Assess the admissibility of digital evidence in court.
- Practice research skills.
- Apply evaluation skills.

Reflection:

Methodologies Employed in Digital Forensics
The process of digital forensics is quite complex. The investigators begin by scanning various electronic devices for evidence and then transferring the data to a safe disc. Then, they analyze the information and document their findings. As soon as it is ready, the digital evidence is either delivered to the police to help them solve a crime or presented in court to help convict a culprit. When investigating using digital evidence, digital forensic experts often adhere to a nine-step standard approach (The Phases of Digital Forensics, 2021).

1. **The Initial Response:**
   As soon as a security breach is discovered and reported to the proper authorities, a digital forensics team sets to work.
2. **Search and Seizure:**
   In pursuit of proof and data, the team analyses the electronic devices utilized in the commission of the crime. The devices are seized by the investigators, rendering the perpetrators incapable of further criminal conduct.
3. **The Acquisition of Evidence:**
   Following the confiscation of the devices, forensic methods will be used to capture the data so that the evidence can be processed.
4. **Safeguarding the Available Evidence**
   While in the custody of the investigators, evidence is safeguarded. Within the protected environment, the data's reliability may be verified, and its accessibility and accuracy can be shown.
5. **Data Acquisition**
   The forensic team will retrieve any electronically stored information (ESI) from the devices. To safeguard the integrity of the evidence and prevent tampering

with the data, professionals must adhere to defined procedures and use utmost caution.

6. **Data Analysis:**
   The members of the team organize, review, and transform the validated electronic evidence to identify court-worthy evidence.
7. **Evidence Assessment**
   After recognizing electronically stored information (ESI) as evidence, investigators assess it considering the security breach. During this phase, you will establish direct links between the obtained facts and the case.
8. **Event Reporting and Documentation**
   As soon as the initial criminal investigation is concluded, the second phase will commence. The team members compile and document the data and evidence in accordance with the standards of the legal system.
9. **Testimony from Experts in the Field**
   A specialist who works in a relevant field is qualified to provide expert witness testimony. The expert witness testifies in court that the data are admissible as evidence and then provides the data.

Challenges Faced by Digital Forensics

Digital forensics, according to one definition, is "the application of scientifically derived and validated methods to the identification, collection, preservation, validation, analysis, interpretation, and presentation of digital evidence derived from digital sources in order to facilitate the reconstruction of criminally motivated events" (SeventhQueen, 2020). In contrast, when these digital forensics research approaches are used, they encounter several severe hurdles. According to Fahdi, Clark, and Furnell (2013) (Focus, 2017), there are three key categories of challenges related with digital forensics:

- Technical challenges
- Legal challenges
- Resource Challenges

1. **Technical challenges**
   New technologies are met with new criminal methods. Professionals in the field of digital forensics use forensic techniques to collect evidence against offenders, but those very offenders use the same skills to cover up, modify, or delete all traces of their illicit activity. In digital forensics, this method is known as an anti-forensics technique and is seen as a major roadblock.
   The following are further technological roadblocks:
   - Organizational process administration on the cloud
   - It's archival time
   - Deficiency in skills
   - Steganography

2. **Legal Challenges**
   Since the legal framework frequently adopts a lax posture and does not recognize every aspect of cyber forensics, the presentation of digital evidence is more difficult than its collection. Jagdeo Singh v. The State is one such case in which the Honorable High Court of Delhi ruled that "while dealing with the admissibility of an intercepted telephone call in a CD and CDR which was without a certificate under Section 65B of the Indian Evidence Act, 1872 the cyber police are unable to prevent this outcome in court because they lack the requisite qualifications and the competence to identify a likely source of evidence and prove its authenticity." Furthermore, electronic evidence is usually challenged in court due to concerns over its reliability. Gathering and acquiring electronic evidence is inherently unlawful because there are no sufficient rules and explanations for doing so.
   Legal Procedures Present New Obstacles
   - Worries Regarding Personal Information
   - Accessibility for the Courts
   - Electronic evidence preservation Possibility of accumulating digital proof
   - Exploring with a Real-Time Computer
   -
3. **Resource Challenges**
   While the pressure on digital forensics experts to analyse ever-increasing data volumes grows because of the more sensitivity and volatility of digital evidence compared to physical evidence, the latter is also becoming increasingly difficult to preserve. Therefore, it is more likely that digital evidence will be lost than actual physical evidence. However, there are certain challenges involved in using these tools. To speed up and improve the accuracy of investigations, forensic experts employ a variety of technological tools for verifying the veracity of data.

   Possible resource problems include the following:
   1. **Incorporating technological improvements:**
      Because of how quickly things like operating systems, application software, and hardware can change, it can be tricky to make sense of digital evidence. This is because software companies have not provided backward compatibility, despite the legal repercussions of not doing so, and because newer versions of software do not provide support for older ones.
   2. **Volume and replication:**
      Electronic documents are vulnerable to attacks on their availability, integrity, and privacy. When WANs and the Internet work together, data may be transmitted across greater distances and to more destinations. The volume of data has increased as a result of the ease of communication and the availability of electronic documents, which has made it more challenging to identify original and relevant material.

Is Digital Evidence Admissible or Sufficient in Court?

- The significance of having a factual memory that is accurate, trustworthy, exhaustive, durable, and reproducible.
- The requirement that we must be able to trust the story being offered to us.
- If we are totally convinced that we have all of the facts, then we will be able to render a legal judgment.
- Therefore, it is vital to have evidence that can be relied upon and objectively establishes the truth of the matter.
- Insufficient evidence can lead to a variety of unfavorable results, such as uncertainty over the situation's facts, unfair treatment of persons involved, and even wrongdoing.

What types of evidence do we normally investigate?

- Witnesses (testimony as well as confession)
- Documentary (photographs, writings, objects, etc.)
- The recommendations of experts, the outcomes of site inspections, and technical improvements (forensic activity).
- The process by which we commit activity-specific details to long-term memory.

Five Digital Evidence Pieces: Is It Court-Acceptable? Is It Sufficient?

- The information must be exhaustive and accurate.
- It is essential to be authentic; it must be adequate.
- It must be acquired and then delivered legitimately.

Digital Evidence:

- Most nations accept it as proof, although its persuasiveness as evidence depends heavily on the precision of the technology.
- How can we prove that a piece of technology is trustworthy? Is the evidence enduring? (The creation of innovative technology)
- Can They Be Admitted in Court?

Recommendations:

- Understand the inner workings of your information technology as well as its capabilities and limitations
- How well information can be stored, transmitted, received, and reproduced without third-party interference.
- Determine what can be done to demonstrate the dependability of your IT.

References:

Digital Evidence – Is it Admissible or Good Enough in Court? - ppt download. (n.d.). Slideplayer.com. Retrieved October 6, 2022, from https://slideplayer.com/slide/13940883/

Focus, F. (2017, June 29). An Introduction To Challenges In Digital Forensics. Forensic Focus. https://forensicfocus.com/articles/an-introduction-to-challenges-in-digital-forensics/

SeventhQueen. (2020, May 4). Challenges faced by Digital Forensics. Legal Desire. https://legaldesire.com/challenges-faced-by-digital-forensics/

The Phases of Digital Forensics. (2021, October 1). University of Nevada, Reno. https://onlinedegrees.unr.edu/blog/digital-forensics/#:~:text=The%20digital%20forensic%20process%20is%20intensive.