1. While a physical crime scene has certain steps to prevent contamination of the crime scene, it involves steps such as don't allow unnecessary persons to cross into the crime scene, don't let things enter into or exit from the scene (expands from Locard's exchange principle), preserve evidence, etc. Identify 10 steps necessary to preserve the digital crime scene, where did you get your listing - the Department of Justice, local law enforcement checklists, the FBI? Provide a link to where you found your references. What provides credibility to the list that you provided? Explain.
   Answer: After going through the reference, I think the following 10 steps are necessary to preserve the digital crime scene
   1. **Immediate Isolation of the System**: Prevent further access to the system to avoid data alteration or deletion, ensuring the original data remains intact.
   2. **Documentation of the scene**: Document all actions taken and observations made during the investigation, maintaining a clear record.
   3. **Capture Volatile Data**: Quickly and carefully collect volatile data (data that might be lost upon system shutdown) including system processes, network connections, and login sessions
   4. **Forensic Imaging**: Create forensic images of the storage devices to preserve the data in its current state for analysis.
   5. **Preserve Log Files**: Secure and preserve log files which might contain crucial information regarding the events leading up to the incident.
   6. **Chain of Custody**: Establish and maintain a chain of custody to document who handled the evidence and when, ensuring the integrity of the evidence.
   7. **Secure Physical Environment**: If necessary, secure the physical environment where the digital devices are located to prevent unauthorized access or tampering
   8. **Malware Analysis**: Conduct malware analysis if any malicious software is suspected to be involved in the crime scene.
   9. **Legal Considerations**: Be aware of and comply with legal considerations including search warrants and consent for the search to maintain the admissibility of evidence in court.
   10. **Expert Consultation**: Consult with digital forensic experts for technical guidance and to ensure the proper handling and analysis of digital evidence.

The steps may not be followed in the exact same way as mentioned depending on the type of Digital crime the Investigator is dealing with.

Reference:
Palter, J. (2023, February 15). Preserving Digital Evidence the Right Way: Your 10-Step Guide. RealTimeNetworks. https://www.realtimenetworks.com/blog/preserving-digital-evidence-the-right-way-your-10-step-guide
Justice, U. S. D. O. (2014, pp. 19–20). Electronic Crime Scene investigation: A Guide for First Responders, Second Edition (2nd ed.). CreateSpace.
Collecting and preserving digital evidence. (2002). In Elsevier eBooks (pp. 545–606). https://doi.org/10.1016/b978-193183665-4/50015-x

2. 18 US Code § 1028 - 1031 defines many of the major types of crimes associated with hacking or computer crimes (below is a list of these subsections), pick one and identify how computer usage ties into the violations described.

a. § 1028. Fraud and related activity in connection with identification documents, authentication features, and information
b. § 1028A. Aggravated identity theft
c. § 1029. Fraud and related activity in connection with access devices
d. § 1030. Fraud and related activity in connection with computers
e. § 1031. Major fraud against the United States

Answer:

Under the subsection "18 US Code § 1028" which pertains to 'Fraud and related activity in connection with identification documents, authentication features, and information', computer usage ties significantly into the violations described in it. Especially in the digital age. Here are the some ways the computer usage tied to violating the Code § 1028:

Unauthorized Access and Data Theft: Criminals use computers to illegally access databases and steal personal information. This data can then be used to create false identities, open bank accounts, digital presence and commit fraud without the knowledge of the person.

Phishing and Social Engineering: Computers are used to conduct phishing attacks where criminals impersonate legitimate organizations to trick individuals into providing their personal information. This information can then be used to create fake IDs or conduct financial fraud.

Reference:

18 U.S. Code § 1028 - Fraud and related activity in connection with identification documents, authentication features, and information. (n.d.). LII / Legal Information Institute. https://www.law.cornell.edu/uscode/text/18/1028

GovInfo. (n.d.). https://www.govinfo.gov/app/details/USCODE-2021-title18/USCODE-2021-title18-partI-chap47-sec1028

3. In Computer Crime Categories: How Techno-Criminals Operate Located at (

https://www.ojp.gov/ncjrs/virtual-library/abstracts/computer-crime-categories-how-techno-criminals-operate)Links to an external site. Computers are listed as the target of a criminal activity, as the instrument used to commit a crime, as incidental to other crimes, or with a prevalence of computers. Unfortunately, not all countries see the same criteria - identify a country in which one of the four criteria are not present in their laws. Which component? Explain how you were able to discern that the component was missing from the law of the target country.

Answer:

Laws related to India doesn't include "Computer As the target" directly as one of the criteria but has using it has a tool to do a crime. The article I have provided in the reference tells different types of criteria which are related to computers.

Reference:

Global Legal Group. (n.d.). Cybersecurity Laws and Regulations Report 2023 India. International Comparative Legal Guides International Business Reports. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india

Cyber Laws of India - ISEA. (n.d.). ISEA. https://infosecawareness.in/cyber-laws-of-india