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>

1. 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.
   1. § 1028. Fraud and related activity in connection with identification documents, authentication features, and information
   2. § 1028A. Aggravated identity theft
   3. § 1029. Fraud and related activity in connection with access devices
   4. § 1030. Fraud and related activity in connection with computers
   5. § 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>

1. 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>

Computer As the Target

Computer As the Instrumentality of the Crime

Computer Is Incidental to Other Crime

Crimes Associated With the Prevalence of Computers

To prevent digital crimes we need to follow and be precautioned at few times. I have browsed and referred two different websites for steps necessary to prevent digital forensic crimes. The websites I have used are real time networks and geeks for geeks. My list consists of :

Have a clear chain of custody : A chain custody can be recorded on paper, and authentication of digital record is often more reliable. (Palter, 2023)The gaps which are present that will prevent the evidence from being admitted.

Get a forensic expert involved : It’s always important to have an experts concern and point of view in Digital crime. It’s also important to know when to stop using with evidences and hand over to an expert. (Palter, 2023)

Monitor evidence transaction : It’s hard for most of the organisations who are nit staffed as full-time evidence managers. Considering automated evidence lockers can simplify transaction monitoring. (Palter, 2023)

Periodically audit your evidence management program : The new Gen-devices are constantly hitting the market. (Palter, 2023)Regularly reviewing your personal evidence management practices to ensure all new types of devices.

Secure the device : Make sure that proper chain of custody of both hardware and data with strong physical security. Never store the device in an open access area. Poor chain custody can make a lot of loss.

Do not plug any external storage media in the device : Media cards, USB devices etc these should not be plugged into the device.

Do not copy anything from devices : The trace of copying data can be stooges and that can be stolen and also slack space of the memory.

Take a picture of the piece of the evidence : Make sure taking a screenshot or picture will help in observing and have a clear analysis. (GeeksforGeeks, 2020)This is one of the safe way to have an evidence.

Don’t change the current state of the device : If the device is ON then must be kept ON always to track, if the device is OFF then it must be kept OFF all the time. We shouldn’t change the state at any cost .(GeeksforGeeks, 2020)

Do not trust anyone with forensic training : Only properly certified forensic And authorised devices are safe to share data. Its risk to share to unknown and not certified forensic which will lead to scams and loose data.(GeeksforGeeks, 2020)

After reviewing all steps necessary to preserve or prevent digital crime, being careful and never sharing any personal details and not trusting 3rd parties and also uncertified forensic .Collect all the evidences without missing is also important.

CITATION 1 : GeeksforGeeks. (2020). Digital evidence preservation digital forensics. GeeksforGeeks. https://www.geeksforgeeks.org/digital-evidence-preservation-digital-forensics/

CITATION 2 : Palter, J. (2023) Preserving digital evidence the right way: Your 10-step guide, Real Time Networks. Available at: https://www.realtimenetworks.com/blog/preserving-digital-evidence-the-right-way-your-10-step-guide (Accessed: 06 September 2023).

18 US Code § 1031, titled "Major fraud against the United States," is a federal statute that addresses fraudulent schemes and also activities that involved defrauding the United States government . This statute is designed to combat major fraud and corruption involving federal programs, contracts, grants, and other government-related matters.This code 1031 is highly followed in united states and the rules are strictly followed.There are few key points to be followed in code 1031. This “Major fraud against the united states” comes under like crossing the banking rules and violating rules, robbery, things which effect the government and the country will be under 18 US code 1031.

There are key points and elements of 18 US Code § 1031:

Scope : The statute is applied for every person who is knowingly involved in a fraud activity, that will affect within the jurisdiction of any department in united states.

Fraudulent schemes : False statements, false claims, stealing information, defraud government all these are part of fraudulent scheme.

Intent : Doing fraud intentionally and accepting it. That person who is doing the fraud activities have an intention to do it on purpose.

Matters within jurisdiction : The highly confidential fraud activities should be not leaked and not allow it to spread to common people. The government contacts, army details, health care programs, disaster relief programs etc, many more all these should be highly confidential.

Penalties : The people who committed the fraud activities hold be under gone punishment and penalties. The penalties depends upon the condition of the fraud activity.

Civil remedies: The addon to the criminal penalties, the statute that all the civil remedies. Those which caused more damage and more loss.

China is a country which experienced with computer crime as target. China is in the top of all countries with the highest ratae of cybercrime. In 2021 china had total 5,000 cases of online gambling cybercrime through online sites(Kass, 2023). In the same year there are total 65,000 cases related to cyber crime in chain(Kass, 2023). There’s no proper security system for computers line and also there are many scams which got more loss of money to people. Through links share and online platforms crimes occurred. Mobiles, iPads, computers all these are connected to servers and those servers are hacked and under controlled by unknown people where they can track and get all updates even personal information. Websites should be certified and alters should be warned to people so that they don’t get lot of loss.

In your text, you've outlined a comprehensive plan on how to prevent digital forensic crimes, drawing from expert advice found on two websites, Real Time Networks and GeeksforGeeks.

You highlighted the importance of maintaining a clear chain of custody for digital records, which seems to be a more reliable method compared to paper records. This step, cited from a 2023 article by Palter, helps in ensuring that the evidence remains admissible in court.

You also emphasized the need to involve forensic experts early in the process, to monitor evidence transactions closely, and to regularly audit evidence management programs, especially considering the constant influx of new generation devices in the market. These steps, as suggested by Palter, aim to streamline the process and ensure the reliability of the evidence collected.

Furthermore, you noted several precautionary measures, such as securing the device in question, avoiding the use of external storage media, and not altering the current state of the device. These steps were advised by GeeksforGeeks in a 2020 article, and they seem to be aimed at preserving the integrity of the evidence.

Interestingly, you mentioned the importance of not trusting individuals without proper forensic training, emphasizing the risks associated with sharing data with uncertified individuals. This seems to be a crucial step in preventing scams and data loss.

In the latter part of your text, you discussed the provisions of 18 US Code § 1031, which addresses major frauds against the US government. You've detailed the scope, the nature of fraudulent schemes covered, the intent behind the crimes, jurisdictional matters, penalties, and civil remedies associated with this statute. This section gives an overview of the legal framework that governs major fraud cases in the US.

Lastly, you touched upon the high incidence of cybercrimes in China, citing a high number of cases in 2021. You suggested that the high rate of cybercrime could be due to the lack of a proper security system, and called for certified websites and warning alerts to prevent substantial losses to individuals.

Overall, your text provides a detailed and well-cited guideline on preventing digital forensic crimes, alongside insights into the legal repercussions of major frauds in the US and the current state of cybercrimes in China.

---

I hope this review serves the purpose! Let me know if there's anything else you'd like to add or modify.