Unit 7 Critical Thinking Questions

1. **Why is it so important to document the process by which evidence passes through investigative units and adhere to standard operating procedures and/or national standards? Is this equally important for those who are innocent as well as those who are guilty? How? Explain.**

It is important because this helps to ensure that the investigation operates smoothly. If these things don't go through, the investigation won't go through correctly. This can result in either someone incorrectly being declared guilty, or someone incorrectly being declared innocent.

2. **What is the main difference between the CIRT model for dealing with incidents and the NIST/SANS model? Compare and contrast how these models deal with incidents. What do you think is the reason for this difference? Explain.**

CIRT Model – Preparation, Identification, Containment, Eradication, Recovery, and finally Lessons Learned.

NIST/SANS Model – Verification, track the journey of the data, evidence is closely scrutinized to create a timeline analysis, investigators then focus on media and artifact analysis, and finally communicating all the findings to the organization who suffered the attack.

The NIST/SANS model tends to be far more extensive and focuses not just on recovery and learning but on establishing the exact method and identity of the perpetrator (from Notes). It is more of something you see out of Dateline, just in the cybersecurity field.

3. **What threshold, if any, do you think a criminal investigator must establish before they should be allowed to search through a person's smartphone or computer for evidence of a crime? Similarly, how far into the public sphere should law enforcement be allowed to search for evidence—and how should that be balanced against the privacy of other users not under investigation?**

If they come to the part in which they need to do this, they have a reason for it. If they need to search someone's computer, they have established that they believe the owner most likely had a major role in the crime. They should only be allowed to search for what is needed and what it's under, not everything (as people have privacy rights). For example, they shouldn't be searching through family photos unless they have a part of the investigation.

4. **What are the various incident categories and correlating incident responses in digital forensics? Explain the general timeline for these incidents and incident responses. Evaluate how important developing an incident response plan is.**

An incident response plan is very important. Knowing what to do when something is going to/has happened, having that already developed plan will go a long way in making things easier and quicker. Without the plan, things can go really bad.

- Intellectual property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Inappropriate use of internet and email in the workplace

All of these incidents have responses within digital forensics. By following the steps that were listed in Question 2, these incidents can be handled.

5. **Why should cybercrime investigators always work with problematic data on a non-infected system and use an approved forensic toolkit? How do these things relate to volatile memory? Describe a specific tool that can be helpful when dealing with volatile data and/or memory and explain why this tool is helpful.**

A forensic toolkit is actually really useful. It scans the hard drive looking for all sorts of things. It can actually find deleted emails and scan for strings that can be used to crack encryption. Volatile memory is important in digital forensics because it can provide evidence of system/internet activity. A useful program that deals with this stuff is BlackLight. The program analyses computer volumes and organizes different memory locations to find the traces of activities done on the system.