Review Questions: Forensic Investigations (01/22/19)

1. What term do you think best describes this field? Computer forensics, digital forensics or forensic computing and why?
2. When criminals use technology, list three advantages this has from an investigative standpoint?
3. Describe a case reported in the media that demonstrates how digital evidence can be useful in an investigation of cybercrime.
4. Provide three reasons why it is important to process digital evidence properly while conducting an investigation?
5. Provide four challenges of investigating technology related crime.
6. What is Lockard’s Exchange principle? Give an example of how this principle applies to digital forensics.
7. Research one court case (besides one presented in class) in which evidence was challenged as fruits of an illegal search, where investigators claimed protection under the plain view doctrine. Was the evidence allowed or not? Explain the reasoning behind the decision.
8. Given that you are a first responder, what questions can you ask to understand the goal of the investigation?
9. How does a responder affect the rest of the investigation process?
10. What are the things that you would need to capture to document the environment being investigated?
11. State two laws which affect the digital forensic process and how?
12. Your team may become the first responder or be called in to take over the investigation, so you will need to engage with the first responder. What tools do you need as a responder?
13. Why is it important not to change the power state of the system?
14. How do you critique a case?
15. (i) Summarize the digital investigation process we covered in class, clearly highlighting the importance of each step.

(ii) Compare the FBI model of investigation and the Casey model for similarities and differences.

1. If you are investigating a homicide case, and, while executing a search warrant you find a computer in the suspect’s home that appears to contain child pornography, what you you do?
2. Other than verifying the integrity of a file, how can the MD5 value or SHA1 value of a file be useful?
3. A lot of emphasis is placed on the necessity of using a write protection device when capturing images of media. What does a write –protection device do, and why is its function so important?
4. Why is it important what order you follow in collecting evidentiary material? Discuss the order of volatility and why this is critical.
5. What are some important pieces of evidence that can be collected from a live memory capture? What are some of the tools you can use to capture live memory?
6. Name three formats for digital forensics data acquisition. What are the two advantages and disadvantages of the raw format?
7. What does logical acquisition collect for an investigation?
8. What does physical acquisition collect for an investigation?
9. What is the difference between the dd command and the dcfldd command?
10. In the Linux dcfldd command, which three options are used for validating data?
11. You need to acquire an image of a disk on a computer that can’t be removed from the scene, and you discover that it’s a Linux computer.
12. What are your options for acquiring the image? Write a brief paper specifying the hardware and software you would use.
13. You are asked to describe to a no technical jury how data is stored on a hard disk drive, how would you go about describing this and what visual aids and/or analogies would you use?