Introduction to Computer Forensics
CSCI 3800
Lecture Notes
Chapter 7

Handling a Digital Crime Scene

- Processing a crime scene is more than collecting evidence, it is the start of the investigation and can steer your hunt for the truth.
- Electronic devices should be considered a part of the crime scene, even when at first glance the crime doesn't seem to involve computers.
- Must make effort to preserve the digital crime scene using forensic principals.
- When you come across a physical crime scene that contains digital evidence, ensure that you still follow your crime scene protocol, don't deviate simply because it is digital evidence. For example, if you normally photograph the crime scene, ensure that you still do that. See figure 7.1
- Keep in mind that your procedures most likely layout what an ideal processing should look like, you should strive to achieve that, but know that you may not be able to.
- DOJ and USSS have put out guidelines for handling a crime scene. These are good "guides" for what an investigator should do.
- Problems with untrained individuals working with the computers (such as line officers).
- Turning on computers at crime scenes: BAD IDEA!!!
- Take notes (or photographs) of where all of the evidence is located in relation to the crime scene (computer on the desk, iPad on the coffee table), then collect the evidence.
- Don't forget power cables!!!
- Basic aim is to preserve the evidential value of the crime scene and maximize the usefulness of the evidence.
- ACPO Guide's four fundamental principals for handling digital crime scenes:
    1. Do not do anything that will change the data on a digital device that may be relied upon in court.
    2. If the original data needs to be accessed, the person accessing it should be trained to do so and be able to explain why they needed to access the original data, and what consequences could arise from them accessing it.
    3. Documentation should be kept that creates an audit trail of what was done to the digital evidence and why (list all processes performed and the reason why).
    4. The person in charge of the investigation must have overall responsibility for ensuring that all laws are followed and that these four principals are followed.
- Safety of the investigator is paramount. Use of PPE and proper tools is a must.
- Know that working particular cases can cause a lot of stress; support systems must be provided to the investigator to ensure their mental well being.

- Before starting your work on a digital crime scene and its evidence the investigator needs to ensure that they have the proper authorization (both for private and public agents).
- Expectation of privacy and need for authorization.
- Err on the side of caution and get a warrant if ever in doubt.
- If you are the investigator and are given a case, ensure that warrant on its face is valid (good-faith exception to flawed warrant). Must particularly describe the property to be seized and searched and the probably cause for such search.
- Ensure that you don't exceed the scope of your authorization when conducting your search. Example in book: drug search, found CP.
- What about multi-user systems? See page 236 book.
- Before "tackling" a crime scene, a game plan should be made up. Every crime scene is different, so it is near impossible to make one plan for all crime scenes, and some crimes scene are too dynamic to make a detailed plan.
- Try to match the offender's skill level with that of the investigator (i.e. a very technical offender might need a more knowledgeable investigator, or might need a different response at the crime scene).
- When searching the crime scene, try to document passwords (ask suspects, see if there are any clues to passwords located on scene).
- Gather special hardware that may be needed during your examination (like backup equipment).
- Look for documentation or manuals that might be needed.
- Isolate any seized communication devices from the network.
- If the systems are password protected, but you have access to them, turn off the password protection before shutting down if possible.