Introduction to Computer Forensics
CSCI 3800
Lecture Notes
Chapter 6

Conducting Digital Investigations

- Remember, the goal of any investigation is to find the "truth."
- Every case will be investigated in a unique way based on the individual facts of that particular case.
- But there are some common techniques that are employed.
- Early on there was a drive to make a "stepwise" approach to conducting these investigations.
- It was quickly discovered that due to all of the unique characteristics of the individual cases that there wasn't "one glove" that fit all cases.
- "Process Models" are descriptions of generalizable steps that should be taken during a digital investigation.
- Why do we have process models:
    - Training
    - Research
    - Benchmarking
    - SOP
- Modern thinking is to use a process model as a guide and not a rigid set of rules.
- Most process models have these common steps:
    - Preparation: make your plan of "attack".
    - Survey/Identification: Take a survey of all of your evidence to identify all sources of relevant digital evidence.
    - Preservation: Ensure that no changes are made to the evidence (including things that you might not know is evidence at first, like logs).
    - Examination and Analysis: Searching for and interpreting evidence.
    - Presentation: writing the report and preparing to testify.
- Different Models:
    - Physical Model: treat the digital crime scene as a physical crime scene.
    - Staircase Model: (figure)
    - Evidence Flow Model: (figure)
    - Roles and Responsibilities Model: (figure)
- Not all models show every last "step", for example what about authorization and transportation?
    - Accusation or incident alert.
        - Consider the source of the accusation.
        - Automated "alarms": may signal an attempted intrusion instead of an actual intrusion.
        - Fact checking and gathering initial information before a "full blown" investigation.
    - Authorization:

        - Government agent v. non-government agent (Elec. Comm. Privacy Act).
        - If warrant is needed, seizing the computer while application is made.
    - Threshold considerations.
    - Transportation.
    - Verification: recheck the information that you received during the survey phase.
    - Case Management.
- Applying the scientific method:
    - Why? Because the process models don't always address the completeness, repeatability, and reliability that are hallmarks of the science of forensics. Also, these process models are very rigid and sometimes difficulty to apply.
    - Observation: use the initial observations to try and formulate a theory about "what is going on."
    - Hypothesis: Formulate a detailed theory of what is happening.
    - Prediction: Based on your hypothesis, predict where you think the evidence is, and what that evidence will show.
    - Experimentation/Testing: This is where you will "search" for the evidence based on your prediction.
    - Conclusion: Did your analysis support your hypothesis?
- Need to anticipate possible defenses to the case, so that your testing can rule them out.