Jade Hedrick

#25934306

Homework #2

1. Pros: Imaging techniques allow us to get an exact replica of the evidence to play with, whereas physical evidence is much harder to investigate without accidental tampering. Digital evidence is also more easily retrievable after it has been deleted. Assuming the unallocated space in memory hasn’t been overwritten, the deleted file and related metadata can still be retrieved. This contrasts with an important paper document that cannot be recovered after it is destroyed.

Cons: Incriminating digital evidence, such as timestamps, can be easily altered by the user compared to, for example, DNA evidence. Even if the evidence were not modified by the user, virtually all of it is indirect and circumstantial; one can easily claim they were hacked at the time a suspicious email was sent out, but a video of them sending that email cannot be so easily disputed.

1. Let’s say someone is sending me threatening anonymous emails. In retaliation, I invest in a packet sniffer and have it running at the time I receive one of these **emails** (class). The email headers show me the **source IP address of the email** (class). I filter out the packets in the packet sniffer program to show only packets with that source. From there I can obtain the **MAC address** (individual) of the machine. The beginning of the IP address is 72.19.x.x, which means the person sending the emails is connecting on the UMass network. Every device connecting to the network is associated with an IT account **netID** (individual) via the device’s MAC address. The netID belongs to a former professor that I’d had a grading dispute with the semester before, and it is coming from their single-user office desktop computer. There are **logs** (class) on the professor’s local SMTP server matching the destination and timestamp of the malicious anonymous emails sent to me.
2. Ws
3. Dfdh
4. Advantages: With the device in your hands and not the suspect’s, you know that the suspect cannot attempt to remove further evidence. It is also much faster than waiting for a specialist to perform digital forensics on it.

Disadvantages: There is no proof that you are not tampering with the data or planting data in yourself. You are changing the access and last modified times of some files. You also cannot retrieve deleted but not-yet overwritten data, and you may miss important data.