Mohmmad Ali Aghrazi Dormani

19205451

Lecture 4 : Digital Forensics and Cybercrime Investigation File

We learned that in present's connected world, everyone gains from innovative cybe-rdefense programs. At the individual level, the cybersecurity attack will lead in everything from identity theft, to extortion attacks, to the amount of valuable data like family pictures. Everyone relies on important infrastructure like power plants, hospitals, and business assistance corporations. Securing these and other organisations is crucial to maintaining our society's development.

I learned a lot of things from cybersecurity's lecture. One thing that I knew was the fact that data will not be completely deleted when it is deleted on the GUI of the computer. But what didn't know was that it could be replaced with other files to completely destroy the evidence. Which can be very dangerous for any hacker.

We also talked a little bit about the rules that are in place for cyber security. One thing that was very interesting to me was the fact that all computer and phones are encrypted these days. Another thing that was striking to me was the fact that police or the persons of authority can force you to open your phone and you can refuse by saying that you have "forgotten" your password and you can get away with major crimes. I think the Irish authorities have to force giant corporations to decrypt the evidence in case of a major crime. This would significantly decrease cybercrimes.

The lecturer also told us an amusing story about a bullet-proof hosting service. I was really impressed with the way that the host of this service got away with all the charges facing him. What he did was that he placed some magnetic fields in the door frame and when the police took the servers as evidence all of the data disappeared.

Another eye-opening thing that we learned was that the police gets a copy of the hard drive and carries investigations on that cope(image). I think it was very intriguing that the police will wipe out the forensic image's hard drive 7 times after they are done with it. Another compelling thing was that they take a Forensic Imaging rather than taking a backup, because backups do not necessarily take all the files and from the drive like files that are corrupted or partially overwritten.

We also learned about chain of custody. There are four ACPO principles involved in computer-based electronic evidence. These principles must be followed when a person conducts the Computer Forensic Investigation. The summary of those principles are as follows :

ACPO Principle 1: That no action take is taken that should change data held on a digital device including a computer or mobile phone that may subsequently be relied upon as evidence in court.

ACPO Principle 2: Where a person finds it necessary to access original data held on a digital device that the person must be competent to do so and able to explain their actions and the implications of those actions on the digital evidence to a Court.

ACPO Principle 3: That a trail or record of all actions taken that have been applied to the digital evidence should be created and preserved. An independent third party forensic expert should be able to examine those processes and reach the same conclusion.

ACPO Principle 4: That the individual in charge of the investigation has overall responsibility to ensure that these principles are followed.[1]

In conclusion I think that there are many ways to protect your data but if we act naively and blindly, we will lose our privacy. I believe that we should always keep our personal information safe using encryption or other methods of protection. in addition i think anyone that wants to pursue a carrier in computer science needs to know about cybersecurity and ACPO guideline. Modern is a very powerful tool that can be used to help or destroy lives.

[1] (The ACPO Principles of Digital Based Evidence ,athenaforensics.co.uk ,2018)