Report

Seminar 1

Author: Anas KWEFATI
Email: ak223wd@student.lnu.se
Semester: Spring 2021
Area: Digital Forensics
Course code: 2DV704

Contents

1 Question 1

As said in the book [1] chapter 2, a system internal clock should always be noted, and during the investigation the recording of correct timestamps is helpful to identify correlations between multiple data objects. However, what if all data objects have been modified using anti-forensics tools, which would make them all to have different, not coherent timestamps? How does such things is taken into consideration and solved?

2 Question 2

In the chapter 2 of the book [1], they say that a cybercriminal can use Steganography to hide data, which might be useful over encryption method, because it does not attract attention. For instance, steganography could be used to hide data in another file, message, image, audio, or even video. However, what if a cybercriminal is using steganography with, also, encryption. Wouldn't it be more difficult to find any hidden data. As firstly, the investigator would need to search in each file, to see if there is any hidden data, which is time-consuming. But then, if the cybercriminal has also used encryption method, it may not even be visible to the investigator. So the question is, what the investigator will do in such scenario, where no evidence can be found due to the cybercriminal using such advanced techniques to hide information that could be at the same time not readable because of encryption and not even visible thanks to steganography?

3 Question 3

Regarding Digital Forensics, what if a hacker managed to get access into a network, and take a lot of cryptocurrencies worth millions of dollar. This cybercriminal, can also launder all that money through some tools that are accessible in the underground realm. After getting all the money in his bank accounts, this person decides to destroy all his electrical devices, change his location (e.g. go to another country that is quite poor, and where digital forensics is not developed), but also would disappear from the underground forums. If all evidence are destroyed and the person has probably even changed his name in another country, thus, how does an investigator will go from here to collect enough evidence and find the criminal?

References

[1] A. Årnes, *Digital Forensics*, 1st ed. John Wiley & Sons Ltd, 2018.