ITIS 4250 / 5250

Alex Onghena

Lab # 3

10/9/2019

**Overview:**

Officer Jimmy Johns of the University of North Carolina Charlotte Police Department has tasked me to help him catch the criminal involved with the thief of an Apple Computer, Apple Tv’s, iPad and iPhone from Woodward hall on Feburary 23rd 2016. I have obtained a forensic image of a thumb drive owned by the potential suspect, this has been obtained by officer john during a traffic stop and I have received proper legal permissions to analyze the information found within the thumb drive for evidence.

**Forensic Acquisition & Exam Preparation**

This section should include details like:

- all the steps you went through to prepare the image for examination

- the verified hash of the image **(must include screenshot of hash)**

- what software you used for this lab (FTK, FTK Imager… etc)

**Findings and Report (Forensic Analysis)**

This is the most important section of your report. **In this section you should include the answers to all the questions, the explanation for the answers and screen shots to prove that you found the answers.**

Note: \* you must include the original question before your answer. \*

This is an example of what I mean:

* 1. **What was the MD5 hash value for nps-2008-jean.e01?**

- Include a screen shot which shows the MD5 hash

- explain how you found the hash

* 1. **What file systems are present within nps-2008-jean.e01? (FAT32, NTFS, EXT3, Reiser, ZFS, UDF, etc)**

- write down which files systems you found and include a screen shot to support your answer

* 1. **What is the total file size for nps-2008-jean.e01 + nps-2008-jean.e02, an what was the size of the original device (hard drive) that nps-2008-jean.e01 is imaged from?**

- write down your answers

- include screen shots showing where you got your answers

- explain your answers

Be very clear which answers go with which question since there are two questions in question c.

**Conclusion:**

In this section you should recap what you did and the evidence you found in this lab. Only state the facts. Don’t talk about how easy or how hard the lab was. Focus on summing up the evidence that you discover, but NO opinion.

**DO NOT:**

- include opinion in any section of your lab report

- say that the suspect is guilty

- say that the investigating officer should have done a better job

- refer to your evidence as “the smoking gun”

- speculate regarding evidence

- copy another student’s screen shots

- forget to include your name in the lab report

- write the answers in your lab report without including the original questions (I need to know which question you are trying to answer.)

**DO:**

- highlight or **bold** you answer to each question.

- only make statements that are true “beyond reasonable doubt”.

- you may only talk about a suspect’s guilt **only** **if** the lab question specifically asks you to do so!

- If the lab says that you are supposed to find a certain pictures and you can’t find it, email me. Don’t just say that you couldn’t find it in the lab report.

- If you have any questions about your lab grade, email me.