No directly quoted material may be used in this project paper.

Resources should be summarized or paraphrased with appropriate in-text and Resource page

Project #2 - Investigative Collection of Evidence

For the purpose of this second Project, you are still the Data Security Analyst for Allied Technology Systems. Consider this project a continuation of the work you performed in Project #1. In this portion of the investigation, you are **ONLY** collecting the physical evidence, documenting and reporting. You will NOT be handling the digital data during this stage of the investigation. (This step will be discussed in the Final Project.) You should limit your “care and handling” of each piece of evidence to the physical handling of the digital item/container.

With the scenario in mind, you are to write a report to your supervisor, thoroughly providing a response to the following questions (in paragraph format, properly citing outside research, where appropriate) to both Part I and Part II of the project:

Part I: Overview/Case Summary

1. Write a short summary of the incident that has occurred and establish what permissions/authorities you have before you search Mr. Jackson’s former Company work area.

Part II: Physical Evidence Acquisition:

2. Look at the photo of Mr. Jackson’s work area. (See file attachment Work_Area.jpg) Identify three (3) potential items of **digital** evidence you see in the photo.

- For **EACH** item of digital evidence you identified, describe the steps that would be taken to collect the items (with emphasis on the care and handling of each item consistent with digital forensic best practices described in the module content/weekly readings) at the scene. You should document these steps in a detailed way that will mitigate questions, concerns, or a basic lack of information that will call your processes into question in court.

- Also for **EACH** item you identified, explain what potential use the item would be within the investigation (e.g., what type of data that item might hold, and what kind of evidence represents for prosecution.)

3. Look at the photo of Mr. Jackson’s work area. (See file attachment Work_Area.jpg) Identify three (3) potential items of **non-digital** evidence you see in the photo.

- For **EACH** item of non-digital evidence you identified, describe the steps that would be taken to collect the items (with emphasis on the care and handling of each item consistent with digital forensic best practices described in the module content/weekly readings) at the scene. You should document these steps in a detailed way that will mitigate questions, concerns, or a basic lack of information that will call your processes into question in court.

- Also for **EACH** item you identified, explain what potential use the item would be within the investigation (e.g., what type of data that item might hold, and what kind of evidence represents for prosecution.)

4. Detail in your report how your seized evidence from Questions two (2) and three (3) are secured and stored after removing it from the original scene (the work area) and prior to sending it for analysis. Describe the security procedures in place as well as any environmental protections (specific to computer/digital devices) that are in place within the storage area.

5. Look at the Evidence Custody Document (See file attachment Evidence Custody Document.doc) and item photographs (Items-seized (pics).pptx). Read the Evidence Custody Document prepared by one of your co-workers in which they are attempting to document the seizure of the three (3) items pictured in the accompanying photos. Did your co-worker adequately describe each item? What could be added to the descriptions, and for which items (based on what you see in the photos) to make them more complete and serve as an example to your co-worker of what they SHOULD look like (how they should be described)?

Project Requirements:

• Paper should be submitted as a basic report memo HOWEVER, an APA-formatted cover page, in-text citations, and reference page is required. (See the following link for memo writing guidelines: http://www.umuc.edu/writingcenter/writingresources/effective_memos.cfm

• Each question should be answered with a **minimum** of 1-2 paragraphs, so do your research, be specific, be detailed, and demonstrate your knowledge; submitting your project through the appropriate assignment folder.

• Answers to the above questions should be submitted in a single Microsoft Word document (.DOC/.DOCX), with answers separated and/or numbered in respect to the question, so as to make it clear which question is being answered. It may be in a question and answer format, or as described with answers to the associated question numbers;

• The paper should be written in third-person grammar, not first person (I, me, myself, etc.);

• The submission is to have a cover page that includes course number, course title, title of paper, student's name, and the date of submission per APA writing format;

• Format: 12-point font, double-space, one-inch margins;

• It is mandatory that you do some research, and utilize outside resources! You must have a reference page at the end of your project that is consistent with APA citation style and format (see https://owl.english.purdue.edu/owl/resource/560/01/ for help).