FINAL PROJECT - Investigative Conclusion and Testimony

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

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

\*\*\*Read the parts of each section of this project carefully as you are being asked to answer questions assuming different roles for different questions.

SECTION I

In the course of this investigation you, as the Information Security Analyst for Provincial Worldwide, have or will need to interview (or perhaps "interrogate") several people to provide context for the evidence you have collected as well as the rational for your searches. Ms. McPherson and Provincial Worldwide management are asking for everything to be documented and would like you to provide them responses to the following pieces of information:

Provide a list of people you believe should be interviewed for this investigation and how they relate to the investigation. What information could they possibly supply?

Provide a narrative description of the interview setting and the intended process, before, during, and following the interview (remember that depending on the type of interview, the setting may be different).

Explain to the management why these stages are important to a successful interview and investigation.

SECTION II

For the purpose of the first part of this Section, you are still the Information Security Analyst for the company. Consider this project a continuation of the work you performed in Projects #1 and #2.

After seeing you search Mr. Belcamp’s work area and take several pieces of evidence, Ms. Victoria Evans who works in the office across the hall, comes forward with an odd story. Ms. Evans states that she is Mr. Belcamp’s girlfriend, but lately things in their relationship had begun to sour. She produces a thumb drive she says Mr. Belcamp gave her earlier that day. She tells you Mr. Belcamp told her to “keep it safe” and asked her to take it home with her at the end of the day. Ms. Evans tells you she really likes her job at Provincial Worldwide and has no interest in being wrapped up in whatever Mr. Belcamp has done to invite negative attention.

1. The laboratory has asked you to write a short summary of what information you want them to look for on the submitted thumb drive. Identify, for the lab, what digital or non-digital evidence you would like them to look for and explain why that evidence would be important to the case.

2. Because you are the most familiar with the investigation, Ms. McPherson is asking you to brain storm all the locations outside of Mr. Belcamp's immediate work space where pertinent digital evidence might be found to help with your case. Identify all of these locations, including places where police would have to be involved to search. Identify what places are legal for the company to search, and which ones would require police involvement. Support your inclusion of each location with a short description of what type of evidence might be found there.

Now, please assume a different character for the purpose of this next segment of the assessment… You are a forensic examiner at the above mentioned Provincial Worldwide lab. Mr. Stephen Bishop, a newly promoted Regional Security Operations Manager, sent an email to Ms. McPherson who has forwarded it to respond.

3. Write a response to the following email that you have received:

To: You, Provincial Worldwide, Digital Forensics Examiner

From: Ms. Carol McPherson

This case has made Provincial Worldwide upper management recognize the importance of forensic readiness. They have asked that you nominate three (3) forensic examination/analysis (software) tools for them to keep in their budget for the following year. They also state that they want to make sure that the tools nominated are ones that would meet criminal justice-level standards and evidentiary requirements under the Daubert Standard. Please construct a table (chart) that identifies the tool name and their manufacturer, and the capabilities of the tools. Since these tools must meet the Daubert standard, please provide an explanation of how the three tools meet the standards of Daubert. (Management specifically wants tools that can examine/analyze the digital data inside the devices and is not interested in your input on additional tools that write protect or image devices at this time.)

After receiving the package from the Data Security Analyst in the field, you sign the chain of custody form and get set to begin your examination.

4. After taking the thumb drive out of storage, you, as the digital forensics analyst, sit down to examine the data. (Presume all personal protective equipment discussed in the course readings is already in place.) Prior to looking through the data contained on the device, you have to make a forensic image. Document what step you take prior to making the image and why this step is important to your overall case. Explain your actions and reasoning thoroughly.

Fortunately, the Information Security Analyst was on his/her game, and ALSO sent you copies of several files, reported to be the source code of “Product X”.

5. You, as the digital forensics examiner, used hash values to help locate the source code on the thumb drive. Using verbiage that would be appropriate to communicate to a judge and jury that may not understand computer technology at all, detail and explain the following:

• What is a hash value, and how did you use it to identify the source code was present?

• Explain an additional use of hash values in the context of digital forensics.

You complete your laboratory examination and return the evidence, with your report, back to the Information Security Analyst at the field office.

Now, reverting back to your role as the Information Security Analyst back at the field office (a.k.a., you), you receive the report from the Lab which shows that the complete “Product X” source code was found on Mr. Belcamp’s thumb drive. In addition, while the evidence was at the lab for examination, you determined it is also likely that Mr. Belcamp emailed copies of the source code to his personal email address.

6. Do you recommend reporting the crime to law enforcement? Why or why not? Are private companies required to report crimes to law enforcement?

7. Explain what additional steps you could take to prove that the source code had been sent to his personal email address.

The decision is ultimately made to report the theft to law enforcement and, using primarily the evidence that you developed during your investigation, Mr. Belcamp is brought to trial for the crime. You (now as the forensic examiner from the Lab) are qualified as an expert witness at the trial and called to testify.

8. What is the significance of you being qualified as an expert witness? How is it different from being a simple fact witness? Explain thoroughly.

9. Mr. Belcamp’s attorney in this case calls you to the stand and brings up the fact that you write a personal blog about digital forensics in your off-time, from which it appears you are a staunch supporter of law enforcement. She believes you are biased in support of law enforcement and that you only had your company’s bottom line in mind. The company’s attorney however, prepared you for these types of questions and had you prepare for trial by practicing answering the following questions - respond to Mr. Belcamp’s attorney by typing up a transcript for your response (You may use first-person grammar, I, me, my, etc., in your response for this question).

“How do we know you are not biased in this case, choosing to report only what would help law enforcement and your company's bottom-line? How can we know from your work that your analysis should be accepted by the court?”

Project Requirements:

• Each question should be answered thoroughly looking at all the issues presented, so do your research, be specific, be detailed, and demonstrate your knowledge; submitting your project through the appropriate assignment folder.

• This project 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 (which means - I, me, myself, etc.); except for question nine (9).

• 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).