**SY486J: Cyber Crime Investigation: Lab Two**

**Assigned: January 23rd, 2019**

**Due date: January 30th, 2019**

**Background to the case:**

You have been asked to investigate George Montgomery. Steve Billings had the IT Department confiscated George’s storage media that might contain information about his whereabouts. After talking to George’s co-workers, Steve learned that George has been conducting a personal business on the side using company computers. Therefore, the focus of the case is possible employee abuse of company resources. You are not the first responder to this case – someone has already seized the equipment and acquired the media.

**Deliverable:**

Please submit a forensic investigation report, which follows the format presented in class last Friday (01/18/2019), which is in the Appendix of this assignment.

**Case Assessment as presented by first responder:**

You can begin assessing this case as follows:

1. **Situation**—Employee abuse of resources.
2. **Nature of the case**—Side business conducted on the company computer.
3. **Specifics of the case**—The employee is reportedly conducting a side business on his company computer that involves registering domain names for clients and setting up their Web sites at local ISPs. Co-workers have complained that he’s been spending too much time on his own business and not performing his assigned work duties. Company policy states that all company-owned digital assets are subject to inspection by company management at any time. Employees have no expectation of privacy when operating company computer systems.
4. **Type of evidence**—Small-capacity USB drive connected to a company computer.
5. **Known disk format**—NTFS.
6. **Location of evidence**—One USB drive recovered from the employee’s assigned computer.

**Planning your investigation**

You know the requirements, now you can plan your investigation. Now you need to perform the following steps:

1. Acquire the USB drive from the IT Department, which bagged and tagged the evidence.
2. Complete an evidence form and establish a chain of custody.
3. Transport the evidence to your digital forensics lab.
4. Place the evidence in an approved secure container.
5. Prepare your forensic workstation.
6. Retrieve the evidence from the secure container.
7. Make a forensic copy of the evidence drive (in this case, the USB drive).
8. Return the evidence drive to the secure container.
9. Process the copied evidence drive with your digital forensics tools.

**Analyzing the digital evidence using Windows Autopsy**

1. Create a folder called Working\_folder on your Desktop.
2. Download montgomery.dd from the network folder.
3. .Start Autopsy for Windows.
4. In Autopsy’s main window, click the Create New Case button.
5. In the New Case Information window, enter George\_Case in the Case Name text box and click Browse next to the Base Directory text box. Navigate to and click your work folder. Make sure the Single-user option button is selected for Case Type, and then click Next
6. In the Optional Information window, type 0001 in the Case Number text box and your name in the Examiner text box, and then click Finish to start the Add Data Source Wizard.
7. In the Select Data Source window, click the Select data source type list arrow, and click Disk Image or VM file and click next.
8. Click the Browse button next to the “Browse for an image file” text box, navigate to and click your work folder and theMontgomery.dd file, and then click Next.
9. Keep the default settings in the Configure Ingest Modules window. Click Next and then Finish.

Next, let’s follow the next steps to display the contents of the acquired data.

1. In the Tree Viewer pane on the left, click to expand Views, File Types, By Extension, and Documents.
2. Under Documents, click Office. In the Result Viewer (upper-right pane), click the first file, Billing Letter.doc, to display its contents in the Content Viewer (lower-right pane).
3. Right-click Billing Letter.doc, point to Add Tag File, and click Tag and Comment.
4. Click on New Tag, and in the New Tag section, type Recovered Office Documents in the Tag Name text box, click OK, and then click OK again.
5. In the Result Viewer pane, highlight and select the files Billing Letter.doc, Income.xls, Regrets.doc, f0000000.doc, and f0000049.doc . Right-click the files Add Tag Files , and then click Recovered Office Documents.
6. Under Documents in the Tree Viewer pane, click Plain Text to display more recovered files.
7. In the Result Viewer pane, select the files listed in Step 5 again, right-click the selection, point to Add File Tags then click Follow Up.
8. Leave Autopsy running for the next activity.

The next step is analyzing the data and searching for information related to the complaint. Data analysis can be the most time-consuming task, even when you know exactly what to look for in the evidence. The method for locating evidentiary artifacts is to search for specific known data values. Data values can be unique words or nonprintable characters, such as hexadecimal codes. With Autopsy, you can search for keywords of interest in the case. For this case, you need to find any files associated with George Montgomery. Follow these steps to search for any reference to the name “George”:

1. Click the Keyword Search button at the far upper right, type George in the text box, and then click Search.
2. In the Result Viewer pane, a new tab named Keyword search 1 opens.
3. Click each file to view its contents in the Content Viewer. Look for files containing the name “George.”
4. Click the Keyword Lists button at the far upper right, click the Email Addresses check box, and then click Search.
5. In the Result Viewer pane, a new tab named Keyword search 2 opens. Click each file to view its contents in the Content Viewer pane and examine all e-mail addresses found in the search.
6. Try to search using IP addresses
7. To view the Excel files, click the file and Open in External Viewer.

**Completing the case**

Autopsy’s Report Generator Autopsy has several styles of reports, including a plain text file, an HTML Web page with links to artifacts, and an Excel spreadsheet. To generate a report, you can follow this general procedure:

1. If you exited Autopsy, start it again, and click Open Recent Case. Click InChap01 and then click Open in the Recent Case window. In Autopsy’s main window, click the Generate Report button at the top.
2. In the Generate Report window, select the report format you want in the Report Modules section. The Results - HTML option, for example, produces a linkable Web page with tagged artifacts, and the Files - Text option creates a plain text output file. When you’re finished, click Next.
3. If you select Results - HTML, the Configure Artifacts Report window opens, where you can select what data to add to the report. After you make your selections, click Finish to generate the report.
4. After the report is generated, Autopsy displays the Report Generation Progress window. Click the link to open the report, and then click Close after you’ve reviewed it.

Now that you have retrieved and analyzed the evidence, you need to find the answers to the following questions to write the final report:

1. How did George’s manager acquire the disk?
2. Did George perform the work on a laptop, which is his own property?
3. If so, did he conduct business transactions on his break or during his lunch hour?
4. At what times of the day was George using the non-work-related files?
5. How did you retrieve this information?
6. Which company policies apply?
7. Are there any other items that need to be considered?

Now you need to produce a report similar to the example presented in class

The report you generated with Autopsy outlines the steps you took. Please include it as as an appendix to your report.

**In any digital investigation, you should be able to repeat the steps you took and produce the same results. This capability is referred to as repeatable findings; without it, your work product has no value as evidence.**

**Critiquing the case**

After you close the case and make your final report, you need to meet with your department or a group of fellow investigators and critique the case in an effort to improve your work. Ask yourself assessment questions such as the following:

1. How could you improve your performance in the case?
2. Did you expect the results you found?
3. Did the case develop in ways you did not expect?
4. Was the documentation as thorough as it could have been?
5. What feedback has been received from the requesting source?
6. Did you discover any new problems? If so, what are they?
7. Did you use new techniques during the case or during research?

Make notes to yourself in your journal about techniques or processes that might need to be changed or addressed in future investigations. Then store your journal in a secure place.

When you write your report, state what you did and what you found. The report you generate with a forensics tool gives an account of the steps you took. As part of your final report, In any digital investigation, you should be able to repeat the steps you took and produce the same results. This capability is referred to as repeatable findings; without it, your work product has no value as evidence. In addition to writing a report, keep a written journal of everything you depending on guidance from management or legal counsel, include this report file to document your work.

**APPENDIX**

**Digital Forensic Report**

**Total points – 70**

**Case Summary(10 points)**

This should be a quick summary versus containing details about the case. You need to explain the relevant information regarding why you are involved and what digital evidence is being investigated. This section should not include the results from the investigation or any details about the case. Think of this section as explaining what is being looked at and why you were selected. That’s it.

Example:

*John Columbus contacted me on 8/17/2017 to investigate a laptop potentially containing stolen company trade secrets recovered from an employee who recently left the organization. Mr. Columbus requested that my team examine the laptop and identify if company trade secrets exist on the system as well as if there is evidence that data was misused. Mr. Columbus has requested a forensic report and support if criminal charges and civil litigation are enforced due to the results of what is found.*

**Acquisition and Exam Preparation (10 points) –** *the incident responder has provided you the evidence, however you need to assume that he/she explained some processes used to acquire and preserve the evidence)*

1. Provide details regarding how you interacted with the digital evidence, including steps taken to acquire and preserve the data - everything from when you started the chain of custody for the artifact you are investigating to how you secured the artifact when you were not working on it to ensure contamination wasn’t introduced.
2. Details such as the hash values of each copy of an artifact, tools used to make the copies, how write protection was enforced, and so on
3. Include pictures and notes taken during the investigation process

Example

* ***7/13/2017****: Laptop (Make, Model, and Serial address) was delivered by Irene Muniz to our lab located at 7345 Carrie Wood Dr., Valrico, FL 33591. Article 1 represents a photograph of the current state of the device upon delivery to our lab for investigation. The system was not powered on at the time of delivery. Articles found at Appendix 9523.*
* ***7/14/2017****: Analyst Steve Stasiukiewicz prepared to create three (3) forensic copies of the system of interest using the Digital Forensic Framework (DFF) installed on investigation system (Name and Serial). Articles found at Appendix 9524.*
* ***7/16/2017****: Analyst Steve Stasiukiewicz enabled write blocking and connected to the laptop using a USB 2.0 cable to the examination machine. Once the hard drive from the laptop of interest was recognized, analyst Steve Stasiukiewicz proceeded with developing three forensic copies of the laptop of interest. The hash values of the copies are listed and stored on an isolated investigation system previously mentioned. Articles found at Appendix 9524.*

**Findings (20 points):**

The Findings section is the part of the report where you include details about what you did and what was found during the investigation. It is typically the longest part of the report based on the level of details you should include. YOU WILL NEED TO INCLUDE SOME SCREENSHOTS here. You should highlight each artifact found and what steps you used to find it.

This is where the opposing counsel who want to challenge look for gaps in your process.

Example:

*Analyst Lynne Doherty used the following tools to proceed with investigating the copy of the laptop via hash (hash value). Tools include WinHex, Guidance Encase 7.12, Kali Linux 2.1. Registry data was abstracted using DFF shown as appendix item 23491. In this figure, we highlight the folder containing web browser history. This led us to believe the following websites were accessed that could potentially have received communication from this laptop containing sensitive data.*

**Conclusions (20 points)**

This is where you outline the logical conclusions derived from the facts. Do not include any assumptions you cannot back up. You need to link all details of your findings to what you propose occurred or didn’t happen. Provide your opinion by referencing evidence that is presented as an unbiased resource—for example, “XYZ, which was found using these methods, help me believe this happened. Remember that many legal systems view evidence as hearsay, so you are always trying to make your evidence seen extremely absolute and nonvolatile to increase its weight to prove your point.

Example:

*Our team has identified the following artifacts to exist on the laptop provided for this investigation. (List artifacts.) Artifacts have been validated by Moses Hernandez as authentic and sensitive according to company policy. Artifact one demonstrates the websites accessed by this system. Within that are email and cloud storage sources highlighted in image 2315. Artifact two represents a recovered email sent on 4/16/2017 to the email address example@company.com. Based on the header information demonstrated in image 2532, the owner of the email account example@company.com sent an email containing the attachment collected from investigating Outlook records represented in image 8342. The results of the email header indicate intent by the owner of the email account to send the attachment to the following cloud email accounts.*

**List of authors (5 points):**

*Example*

*Lead investigator: Joseph Muniz, joeymuniz@thesecurityblogger.com. 1.800.123.4567*

*First Responder: Aamir Lakhani, aamirlakhani@drchaos.com. 1.800.321.7654*

**Certification (5 points):**

I hereby certify that the work presented above was personally performed by me and the opinions and conclusions stated are my own and based upon the work that I performed.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature