Lab Assignment 1B – Analyzing Digital Evidence

Background

Students will use Autopsy[1] to analyze a case and gain experience with a common forensic tool that will be used in future assignments. This walkthrough is intended to give the student experience with the interface while answering basic investigation questions during a company policy violation.

Manager Steve Billings has been receiving complaints from customers about the job performance of one of his sales representatives, George Montgomery. George has worked as a representative for several years. He's been absent from work for two days but hasn't called in sick or told anyone why he wouldn't be at work. Another employee, Martha, is also missing and hasn't informed anyone of the reason for her absence. Steve asks the IT Department to confiscate George's hard drive and all storage media in his work area. He wants to know whether any information on George's computer and storage media might offer a clue to his whereabouts and job performance concerns. To help determine George's and Martha's whereabouts, you must take a systematic approach to examining and analyzing the data found on George's desk.

In the company-policy violation case, you have been asked to investigate George Montgomery. Steve Billings had the IT Department confiscate 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 has shifted to include possible employee abuse of company resources. You can begin assessing this case as follows:

- *Situation*—Employee abuse of resources.
- *Nature of the case*—Side business conducted on the company computer.
- *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 Internet Service Providers (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.
- *Type of evidence*—Small-capacity USB drive connected to a company computer.
- *Known disk format*—NTFS.
- *Location of evidence*—One USB drive recovered from the employee's assigned computer.

Based on these details, you can determine the case requirements. You now know that the nature of the case involves employee abuse of company resources, and you're looking for evidence that an employee was conducting a side business using his employer's computers. On the USB drive retrieved from George's computer, you're looking for any information related to Web sites, ISPs, or domain names. You know that the USB drive uses the NTFS file system. To duplicate the USB drive and find deleted and hidden files, you need a

[1] For detailed information on using Autopsy, see http://sleuthkit.org/autopsy/docs/user-docs/4.3/. For an explanation of the user interface, see http://sleuthkit.org/autopsy/docs/user-docs/4.3/uilayout_page.html.

reliable digital forensic tool. Because the USB drive has already been retrieved, you don't need to seize the drive yourself. Your task is to gather data from the storage media seized to confirm or deny the allegation that George is conducting a side business on company time and computers. Remember that he's suspected only of resource abuse, and the evidence you obtain might be exculpatory—meaning it could prove his innocence. You must always maintain an unbiased perspective and be objective in your fact-findings. If you are systematic and thorough, you're more likely to produce consistently reliable results.

Objectives

- Conduct a company policy violation investigation
- Analyze an imaged USB device by reviewing files and associated metadata
- Become familiar with Autopsy's tagging, bookmarking, and reporting functions

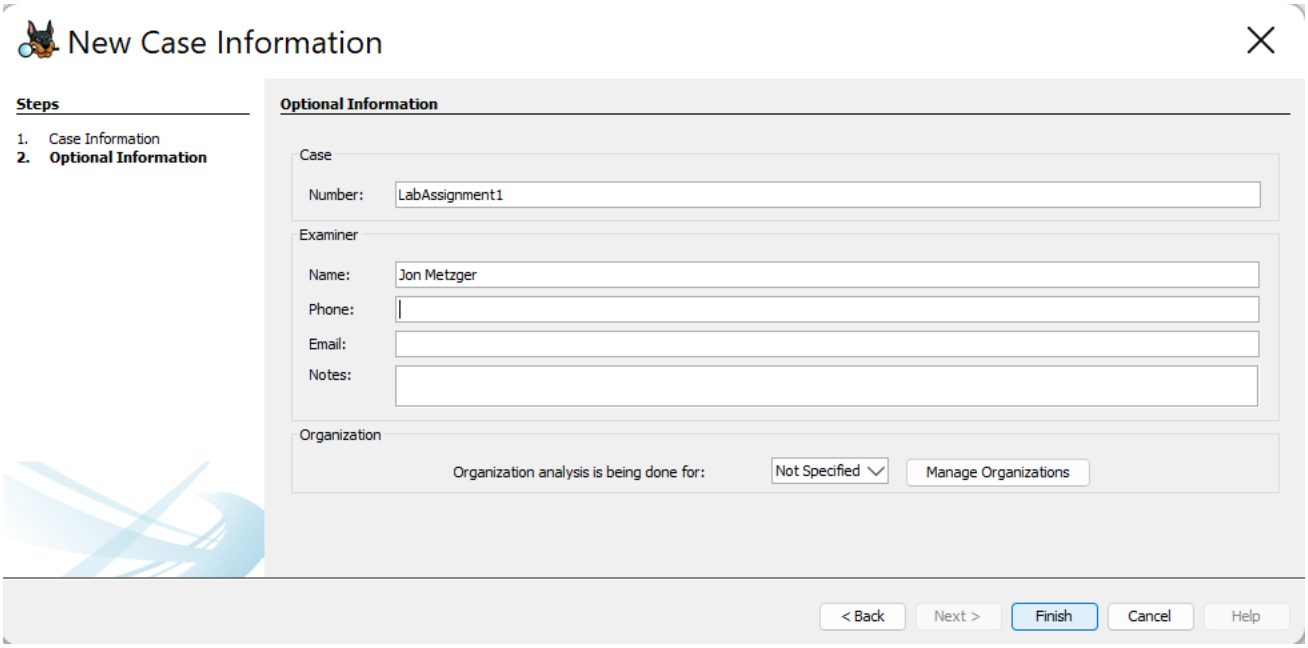
Exercise Preparation

When you analyze digital evidence, your job is to recover the data. If users have deleted or overwritten files on a disk, the disk contains deleted files and file fragments in addition to existing files. Remember that as files are deleted, the space they occupied becomes free space—meaning it can be used for new files that are saved or files that expand as data is added to them. The files that were deleted are still on the disk until a new file is saved to the same physical location, overwriting the original file. In the meantime, those files can still be retrieved. Forensics tools such as FTK Imager and Autopsy can retrieve deleted files for use as evidence.

In the following steps, you analyze George Montgomery's USB drive. The first task is to configure Autopsy for a new case and analyze the image file of George Montgomery's USB drive. To perform the analysis, follow these steps:

1. Download Assignment 1B evidence (LabAssignment1B.dd). Start Autopsy 4.16[2] for Windows (Can also be run on Linux or macOS).
2. In Autopsy's main window, click the **New Case** button. In the New Case Information window, enter **LabAssignment1** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to the appropriate lab folder. Make sure the **Single-user** option button is selected for Case Type, and then click **Next**.
3. In the Optional Information window, type **LabAssignment1** in the Case Number text box and your name in the Examiner text box (**ENTER SCREENSHOT BELOW**), and then click Finish to start the Add Data Source Wizard.

[2] Version 4.16 can be downloaded here https://www.autopsy.com/download/, which includes The Sleuth Kit (TSK) 4.10.0.



4. In the Add Data Source window, in the **Select Type of Data Source To Add** list, select **Disk Image or VM File** and click **Next**. Click the **Browse** button next to the "Path" text box, navigate to and click your lab folder and the **LabAssignment1B.dd** file, and then click **Next**.
5. Keep the default settings in the Configure Ingest Modules window. Click **Next** and then **Finish**.

DONE

Follow these 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 File Tag**, and click **Tag and Comment**.
4. In the Create Tag dialog box, click the **New Tag** button. In the New Tag section, type **Recovered Office Documents** in the Tag Name text box, click **OK**, and then click **OK** again (Select Recovered Office Documents if this tag already exists).
5. In the Result Viewer pane, Ctrl+click **Billing Letter.doc**, **Income.xls**, **Regrets.doc**, **f0000000.doc**, and **f0000049.doc** to select these files, and then release the Ctrl key. Right-click the highlighted five files, point to **Add File Tag** 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, once again under Office documents (File Types\Documents\Office), select the five files noted above again, right-click the selection, point to **Add File Tag** and then click **Follow Up**. Leave Autopsy running for the next activity.

DONE

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. There are also printable character codes that can't be generated from a keyboard, such as the copyright (©) or registered trademark (™) symbols. Many digital forensics programs can search for character strings (letters and numbers) and hexadecimal values, such as 0xA9 for the copyright symbol or 0xAE for the registered trademark symbol. All these searchable data values are referred to as "keywords."

With Autopsy, you can search for keywords of interest in the case[3]. 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. Click each file to view its contents in the Content Viewer. Look for files containing the name "George."
3. Click the **Keyword Lists** button at the far upper right, click the **Email Addresses** check box, and then click **Search**.
4. 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. Leave Autopsy running so that you can learn about more of its features in the next section.

DONE

Exercise – Questions

After analyzing the disk, you can retrieve deleted files, e-mail, and items that have been purposefully hidden, which we'll do later in the course. The files on George's USB drive indicate that he was conducting a side business on his company computer. Now that you have retrieved and analyzed the evidence, you need to find the answers to the following questions to write the final report (these are examples and are not deliverables for this assignment):

- How did George's manager acquire the disk?

  George's manager Steve Billings had the IT Department confiscate George's storage media that might contain information about his whereabouts.

- Did George perform the work on a laptop, which is his own property? If so, did he conduct business transactions on his break or during his lunch hour?

  Answered with the next question

- At what times of the day was George using the non-work-related files? How did you retrieve this information?

[3] This keyword searching process will be used many times throughout the course and is one of the most commonly used techniques in digital forensics. This example is much simpler than advanced techniques that include GREP expressions or complex keywords.

It was done at 2:50 which is noy during his lunch break and on company time. George performed on his laptop, but with work private information on the "Client Info.mdb" From there he was able to contact each member for his own private side business.

- Which company policies apply?

  All company-owned digital assets are subject to inspection by company management at any time. Since George was using company information on his work laptop, they can at any time investigate his system.

- Are there any other items that need to be considered?

  The two letters from October 13th 2003 and November 2nd 2003 where George uses company confidential information for his side job to threaten Laura Roper and Randall Watson.

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, depending on guidance from management or legal counsel, include this report file to document your work. 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.

Basic report writing involves answering the six Ws: who, what, when, where, why, and how. In addition to these basic facts, you must also explain computer and network processes. Typically, your reader is a manager, a lawyer, or occasionally a judge who might have little computer knowledge. Identify your reader and write the report for that person. Provide explanations for processes and how systems and their components work.

Your organization might have templates to use when writing reports. Depending on your organization's needs and requirements, your report must describe the findings from your analysis. The reports generated by forensics tools generally list your examination and data recovery findings. Some digital forensics tools also generate a log file of all actions taken during your examination and analysis. Integrating a log file from these other tools can enhance your final report. When describing the findings, consider writing your narrative first and then placing the log file at the end of the report, with references to it in the main narrative. This course will cover report writing in more detail in a later lesson.

In the LabAssignment1B case, you want to show what evidence exists proving that George had his own business registering domain names. You should include a list of his clients' names, his income from this business, and any correspondence he wrote to clients about their accounts. The time and date stamps on the files are during work hours, so you should include this information, too. Eventually, you hand the evidence file to your supervisor or to Steve, George's manager, who then decides on a course of action.

The file Client Info.mdb has client names, addresses and domains with their IP addresses, date registered and renewal date. From this information, George can use for his own use to profit off of his work through the company.

client info.mdb

Client Id	First Name	Last Name	Street Address	City	State	Zip
1	Randall	Watson	89 Darnell Street	Des Moines	WA	98000
2	Laura	Roper	48 Mockingbird Lane	Seattle	WA	98119
3	Earnest	Bell	12891 Dexter Ave	Bellevue	WA	98769
4	Frank	Haron	5679 Washington Streetq	Ballard	WA	98107
5	Thomas	George	567 Port Ave Seattle	WA	98118	
6	Claude	Finsk	1789 Through Drive	Seattle	WA	98791

Client ID	Domain Name	ISP or NSP	IP Address	Registered Through	Date Registered	Next Renewal
1	www.lauras_stuff.com	Groups.com	123.13.78.231	INterNIC	9/13/03	9/13/05
2	www.nature.com	others.com	89.34.98.123	InterNIC	10/2/03	10/2/05

For the month of January, in income.xls George made $3945 from his side job using company confidential information.

income.xls January

January Cash Flow

Income	Setup	Contact	Confirmation	Total	
Laura Roper	$ 450.00	$ 75.00	$ 150.00	$ 675.00	
Earnest Bell	$ 450.00	$ 250.00	$ 150.00	$ 850.00	
Frank Haron	$ 575.00	$ 75.00	$ 150.00	$ 800.00	
Thomas George		$ 450.00	$ 120.00	$ 150.00	$ 720.00
Randall Watson		$ 575.00	$ 175.00	$ 150.00	$ 900.00
			Grand Total	$ 3,945.00	

Files with timestamps below

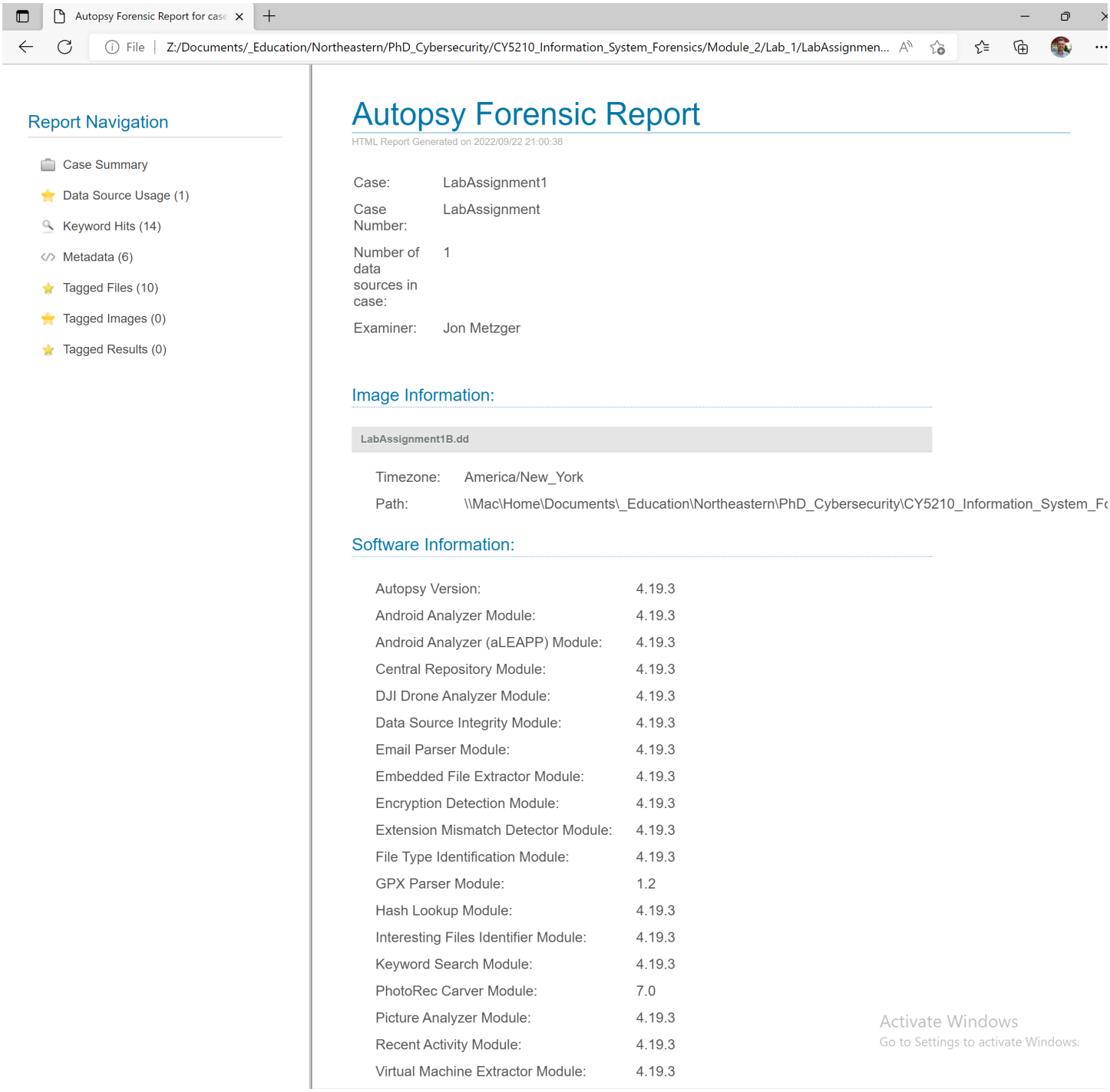
Billing Letter.doc	address listed below.«George« Montgomery3467 Main	/img_LabAssignment1B.dd/Billing Letter.doc	2005-12-09 06:50:28 EST
Regrets.doc	nowhere.comRegards,«George« Montgomery-------	/img_LabAssignment1B.dd/Regrets.doc	2005-12-09 06:50:52 EST
letter1.txt	Please contact me ASAP.«George«----------	/img_LabAssignment1B.dd/letter1.txt	2005-12-09 06:51:50 EST
Income.xls	00 $ 800.00 Thomas «George« $ 450.00 ...	/img_LabAssignment1B.dd/Income.xls	2005-12-09 06:52:18 EST
confirmation.txt	you for your business«George«----------	/img_LabAssignment1B.dd/confirmation.txt	2005-12-09 06:52:58 EST
Client Info.mdb	Ballard WA 98107 5 Thomas «George...	/img_LabAssignment1B.dd/Client Info.mdb	2005-12-09 06:53:58 EST

Generating Reports

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 **LabAssignment1B** 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 HTML Report 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. In the Select which data source(s) to include window, select the evidence sources to be included in the report, click **Next**.
4. Configure Report to include **All Results** and select **Finish** to generate the report.

5. 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.
6. **Include the report content, or a snapshot in this submission.**



DONE

Exercise—Key Takeaways

- Forensic professionals must always remain objective when initiating investigations
- Autopsy is one of many tools that can help identify deleted, hidden, or otherwise obscured files
- Tags and bookmarks can be used to highlight useful evidence in a report for reporting or presentation purposes
- Any analysis or answers to forensic questions should be documented in a report in all cases

***Please submit the final assignment as a single .PDF and any applicable reports as a .ZIP file.**
**Screenshots may also be added to this document when appropriate.