**Naomi Johnsons**

**Lab 3 Report**

**Question 1:**

The three images being examined are different copies from the same thumb drive, only that each was created differently and contains different data types. Part 1 Image is a full disk image that has a full copy of the thumb drive, including both allocated and unallocated space. On the other hand, Part 2 Image is composed only of allocated space only. It is also called a logical file. Deleted files and unallocated space are not included. Part 3 image on the other side is an unlocated space only. It does not have current active files and filesystems

**Question 2: Validating PhotoRec’s Data Carving from Unallocated Space**

To validate PhotoRec and its data carving capabilities, loaded I Part 3 image (unallocated space) to PhotoRec, but it was not readable. I solved it by renaming it to part3.dd so that PhotoRec could recognize and process it. I placed this file in the same folder as the PhotoRec application and launched gPhotoRec for ease of navigation. The tool successfully scanned the image and recovered 202 files.

I reviewed the files recovered by PhotoResc and I discovered that the tools got the same files that Autopsy. There were many files, but the following two serve as an example:

* f0000576.jpg
* f0057472.pdf

It should be considered that Autopsy recovered 269 files in total — more than PhotoRec — the overlapping files confirm that PhotoRec's carving feature is functional and accurate to a significant extent. The slight difference in the number of recovered files shows how each tool handles file system metadata, file structure recognition, and recovery algorithms. Autopsy may have used additional metadata from the file system to identify recoverable files that PhotoRec could not detect purely through carving.

**Quiz 3: Keyword Search Results (Email Addresses)**

The task inlovled searching a keyword using Autopsy to detect potential digital evidence, and it was specifically email addresses. I used the predefined GREP signatures available in Autopsy to search for strings that matched standard email address formats.

I was able to identify several files having email addresses and some of the files include:

* logfile 2012-07-02-1200.eml: This log file contained the email address joe.sum.twelve@gmail.com. The .eml extension indicates that the file is likely an email message, possibly saved from an email client.
* 047603.html: This HTML file revealed the email address Betty.Freeman@nrc.gov, which appears to be part of a web-based message or saved webpage content.

These results shows that the image contained communication records or references to email conversations. Files like .eml and .html often store data related to email activity, such as received or sent messages, headers, or cached web content.

**Question 4**

The recovered email content appeared to be routine and non-threatening, mostly involving personal and work-related communication. One email mentioned a student's absence from school for about a week, while others focused on regular updates and discussions. Some messages came from or were addressed to government domains like @nrc.gov, but none of the content appeared sensitive or confidential. Attachments such as PDFs and HTML files were also reviewed and contained no suspicious or alarming information. Overall, there was no indication of any criminal or civil offenses in the email communications analyzed.

**Question 5**

Conduct a simple keyword search for the expression "cyb3r4n6" in the dataset.  Did this keyword search identify all of the files that contain this keyword?  If not, for each file containing the keyword that did not have a search hit in Autopsy, why do you think that is?

*Yes, it identified, in fact a total of 18 files having the keyword cyb3r4n6 er found.*

**Question 6**

The file identified by Autopsy as encrypted is Word Document 2.docx. The password is 1234. Autopsy was not able to find the word cyb3r4n6 simply because the file was encrypted. Autopsy could only categorize it as encrypted.

**Question 7**

Images from ExDocs and GovDocs had a particular time frame when it was accessed and edited. The time was of two sessions. These sessions ranged from 2021-09-05 08:00 am and the other time was 2021-09-05 -2013

**Question 8**

Autopsy geolocation:

*latitude:* 33.9172222222222

*Longitude:* -78.2583333333333

***ExifTool:***

*GPS Latitude* : 33.9172222222222

*GPS Longitude* : -78.2583333333333

Autopsy and EXifTool produced the same geolocation results. This shows that the tool is accurate and can be trusted and used. I tested by searching them in Google Maps, and sure enough. It was the same

