**Digital Forensic Report**

**Analyst:** Naomi Johnson

**Date:**

**Case Name:** INFS6681 Exercise 1

**Tool Used:** Autopsy 4.14

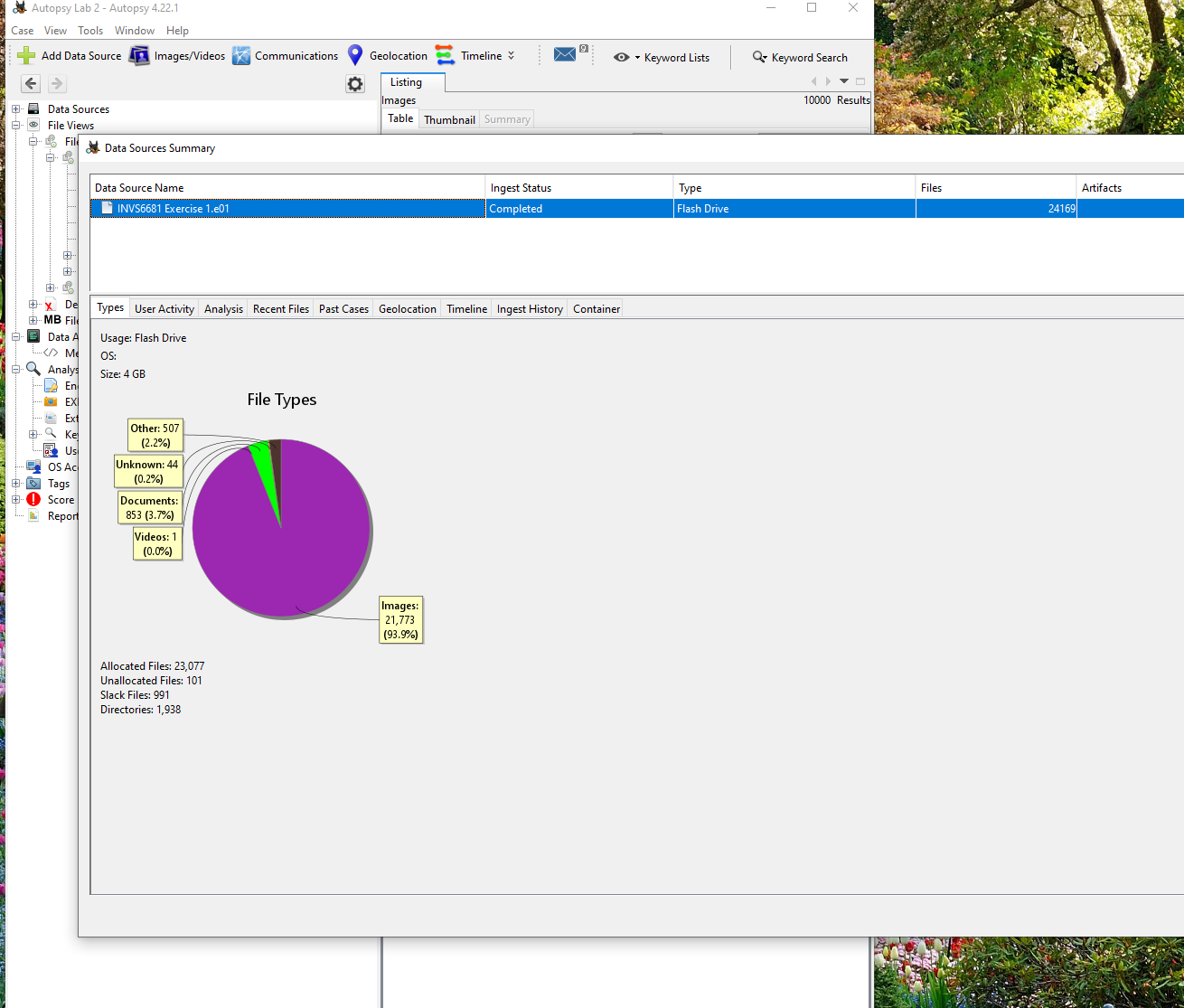
**Image File Analyzed:** INFS6681 Exercise 1.E01

### **Case Overview**

A forensic image named INFS6681 Exercise 1.E01 was provided for analysis. The image file was downloaded from the Module 2 folder and examined using Autopsy. All ingest modules were enabled to ensure a comprehensive scan.

**Findings:**

* **Images Identified:** 21773, which occupied 93.9.5% of the total storage.
* **Documents Identified:** 853 (3.7%)
* **Videos Identified:** 1
* **Directories Identified:** 1938
* **The most common cities (Geolocation)** are Little River, South Carolina, and Leland, North Carolina, United States.  
   **Interpretation:** The suspect may have taken images or used devices in these areas Maps.
* **Earliest File Activity Date:** Oct 8, 1985

****

1. What is the file system that is on the thumb drive (i.e. in the image file you are examining)?

***Win95 FAT32 (0x0c) file system***

1. What is the "Volume Label Entry" for vol2 on the thumb drive? This is the volume name you would give a thumb drive during format.

***The thumb drive image contains two partitions. The second partition, vol2, uses the Win95 FAT32 (0x0c) file system, and it is seen that it does not have a custom volume label assigned to i****t.*

1. What is the name of the file in the folder 032?

***032132.txt***

1. What does the extension .txt indicate to you?

***It is a text file, and it can be opened using Notepad.***

1. Perform a text search for the expression "groundfish." How many files contain the search expression?

***Four files***

1. Find the file "2016-08-07 10.26.26.jpg." Do a Google Maps search for the geolocation. Where do the geolocation coordinates indicate the photograph was taken? Can you corroborate that address? If you can, explain the process and provide a screenshot in your report of how you did that.

***The image file did not have any GPS coordinates in its metadata. The device used to capture the image did not have location services on***

1. What is the spelling error depicted in the photograph 2016-08-07 10.26.26.jpg

***The image has a poster indicating “Now Hiriing Drivers.” Hiriing is the mispelled word.***

1. Tag 3 files that pertain to the Department of Defense. Describe the process you used to find them. After you found them, can you think of a more expeditious means of finding them? Tag each with a comment.

***I found three files.***

1. **249193*.pdf This document is labeled Federal Register and also Department of State. It is also concerned with the Department of Defense.***
2. ***-*53568.pdf *This document title is The Army Lawyer***
3. **577954.html *is a file that talks about Decision and order.***

***| used the search keyword list and searched for Department of Defense. I then reviewed the contents to verify its relevance and then finally tagged them with some comments.  
To improve future search, it is important to have a centralized keyword list and the use of Autopsy’s Keyword list should be implemented***.

1. The report is attached to this document. It is an Excel document.