

Student:	Email:
Jordan Calvert	jordanryancalvert@gmail.com

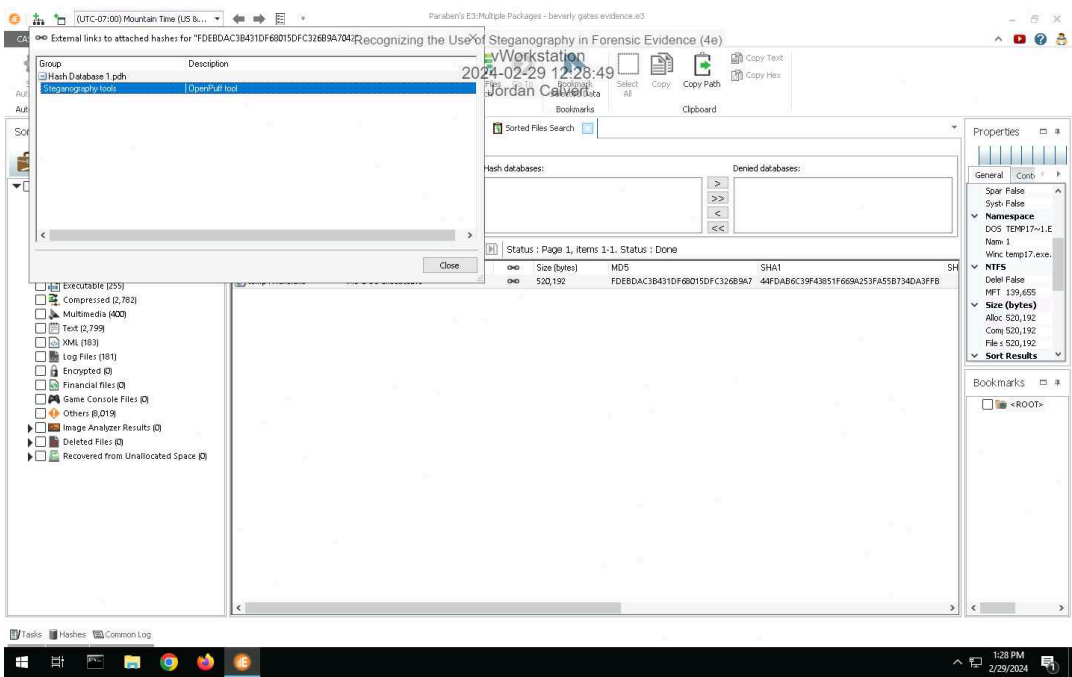
Time on Task:	Progress:
5 hours, 13 minutes	100%

Report Generated: Thursday, June 6, 2024 at 1:53 PM

Section 1: Hands-On Demonstration

Part 1: Detect Steganography Software on a Drive Image

14. Make a screen capture showing the search result and its description.

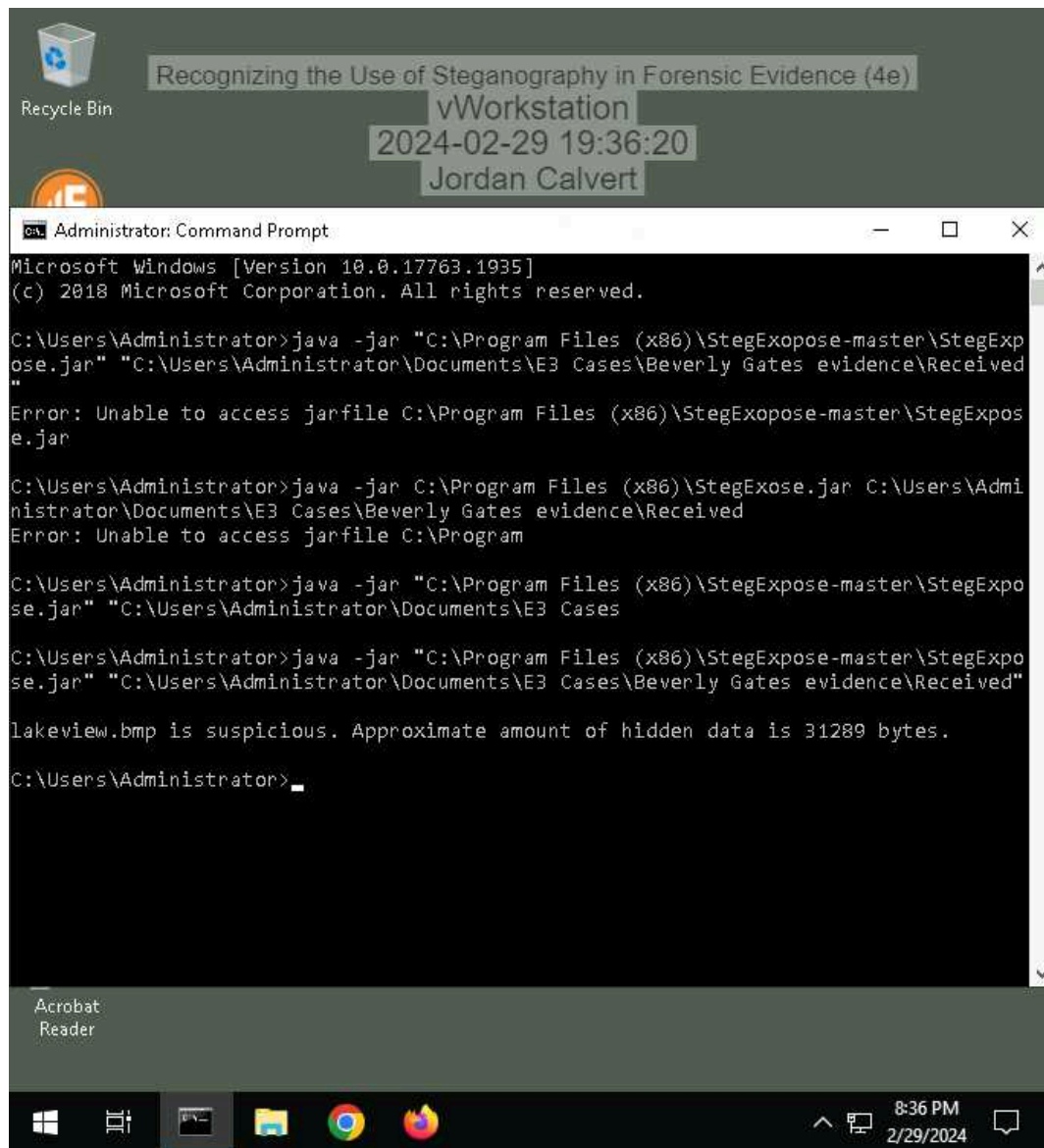


Part 2: Detect Hidden Data in Image Files

## Recognizing the Use of Steganography in Forensic Evidence (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 02

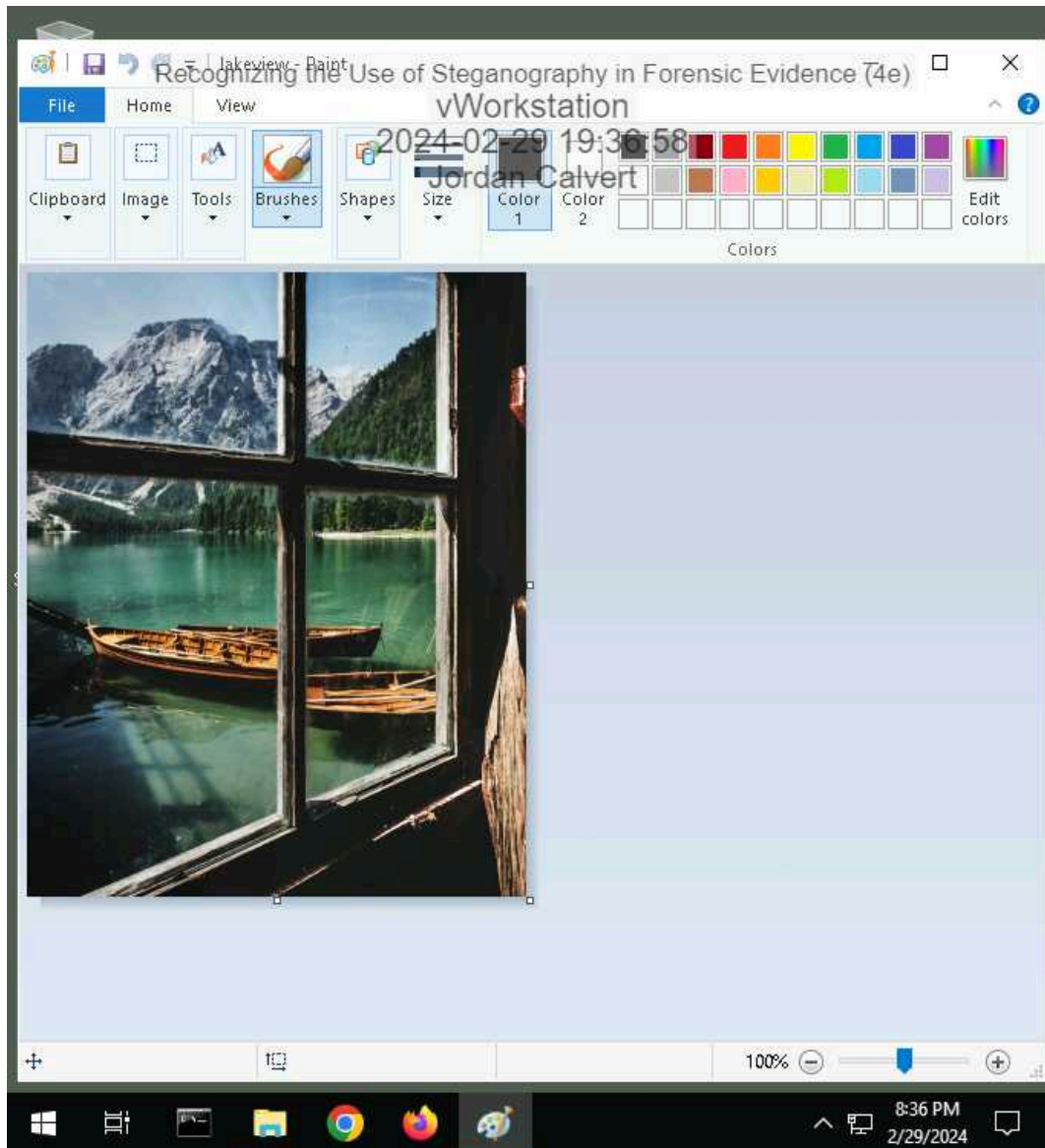
10. Make a screen capture showing the **StegExpose** results.



## Recognizing the Use of Steganography in Forensic Evidence (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 02

13. **Make a screen capture** showing the **suspicious file** in **Microsoft Paint**.



### Part 3: Extract Hidden Data from Image Files

2. **Record** the passphrase saved in the ReadMe file.

passphrase saved in the ReadMe file is **landmarks**

### 16. Make a screen capture showing the contents of the file extracted by OpenPuff.



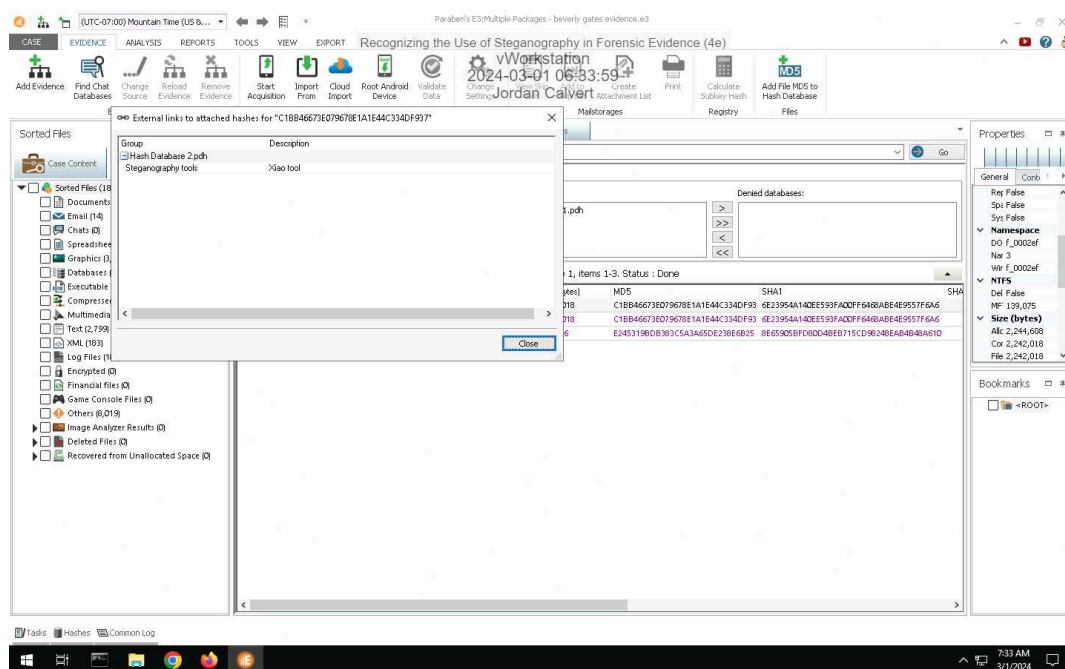
### 17. Describe the contents of the hidden file. How might it be relevant to the current investigation?

The contents of the hidden file include what looks like coordinates and addresses.

### Section 2: Applied Learning

#### Part 1: Detect Steganography Software on a Drive Image

5. Make a screen capture showing the search result and its description.



#### Part 2: Detect Hidden Data in Image and Audio Files

4. Identify the image file with concealed data according to the StegExpose steganalysis tool.

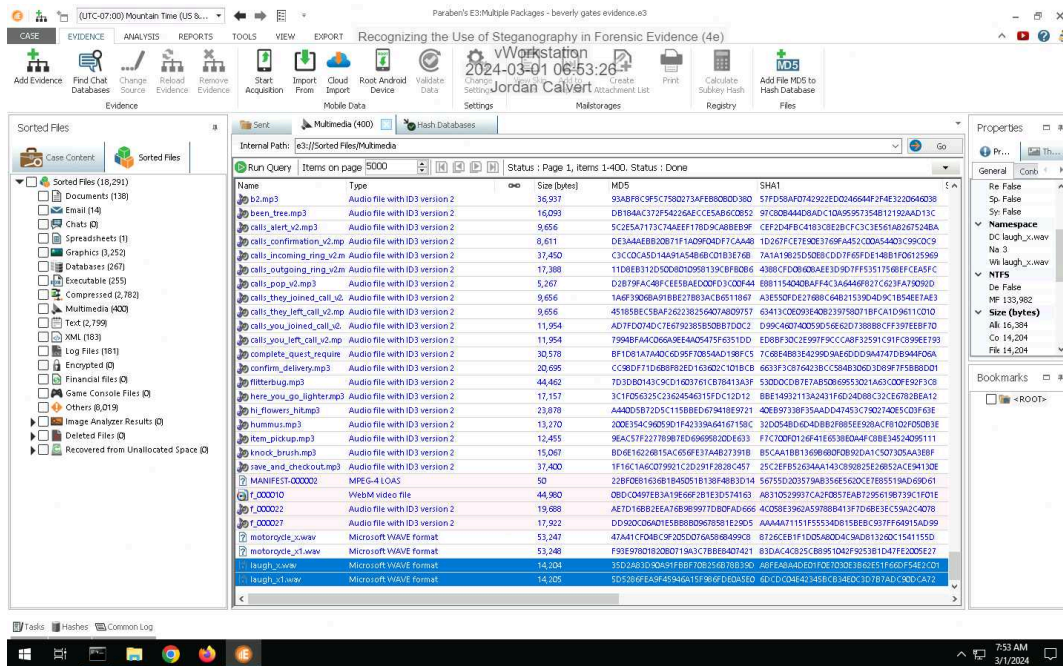
the image file with concealed data according to the StegExpose steganalysis tool is **dB9olser.gif**



# Recognizing the Use of Steganography in Forensic Evidence (4e)

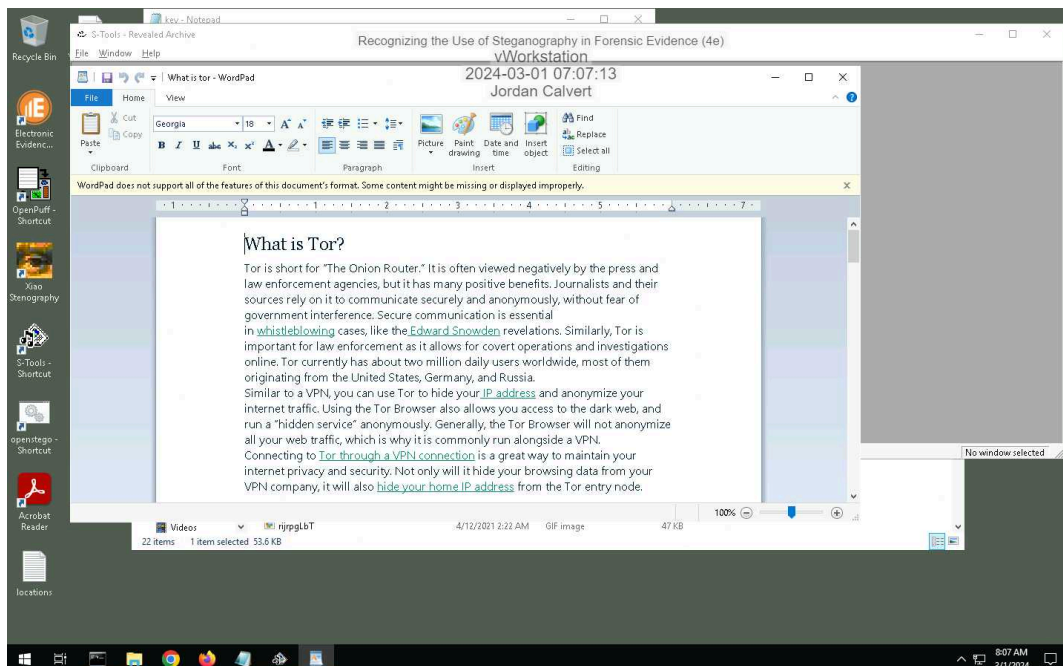
## Digital Forensics, Investigation, and Response, Fourth Edition - Lab 02

### 7. Make a screen capture showing the WAV file sizes and hash values in E3.

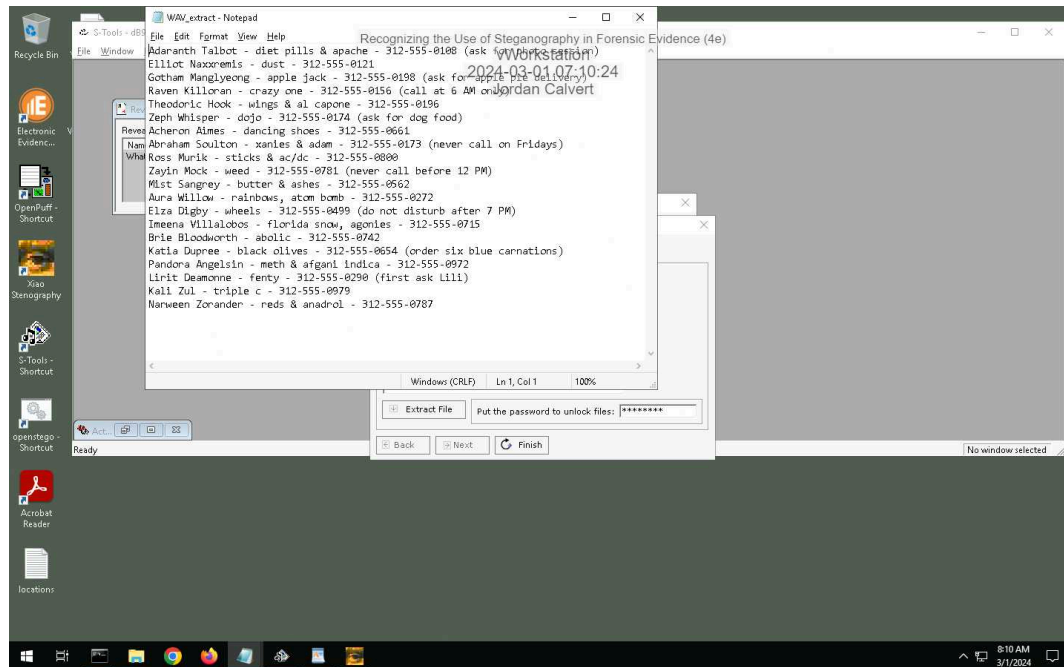


## Part 3: Extract Hidden Data from Image and Audio Files

### 9. Make a screen capture showing the contents of the hidden file extracted by S-Tools.



15. **Make a screen capture** showing the **contents of the hidden file** extracted by Xiao.



16. **Describe** the contents of the two hidden files. How might they be relevant to the current investigation?

It looks like these are clients and their orders, along with their phone numbers. This is relevant to the current investigation because it might lead to identifying who exactly is involved.

## Section 3: Challenge and Analysis

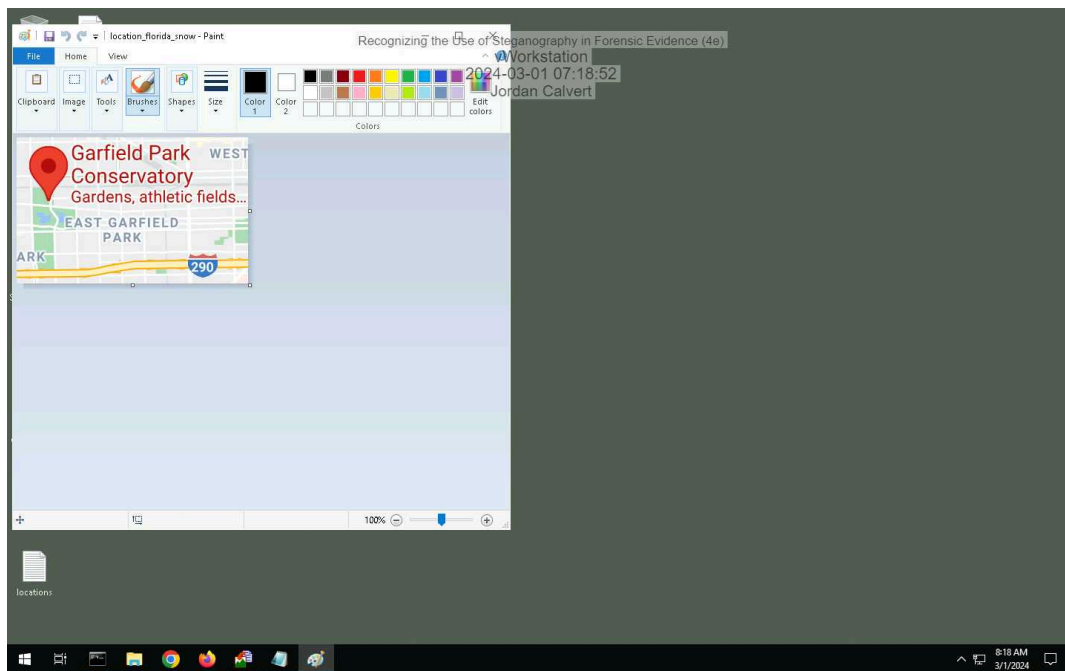
### Part 1: Detect More Hidden Data

**Record** the names of the files that contain concealed data.

The names of the files that contain concealed data are **chicago.bmp** and **chicago1.bmp**

### Part 2: Extract More Hidden Data

**Make a screen capture** showing the **first file extracted by OpenStego**.





# Recognizing the Use of Steganography in Forensic Evidence (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 02

---

**Make a screen capture showing the second file extracted by OpenStego.**

