Student:	Email:
Loksharan Saravanan	loksharan.soc@gmail.com

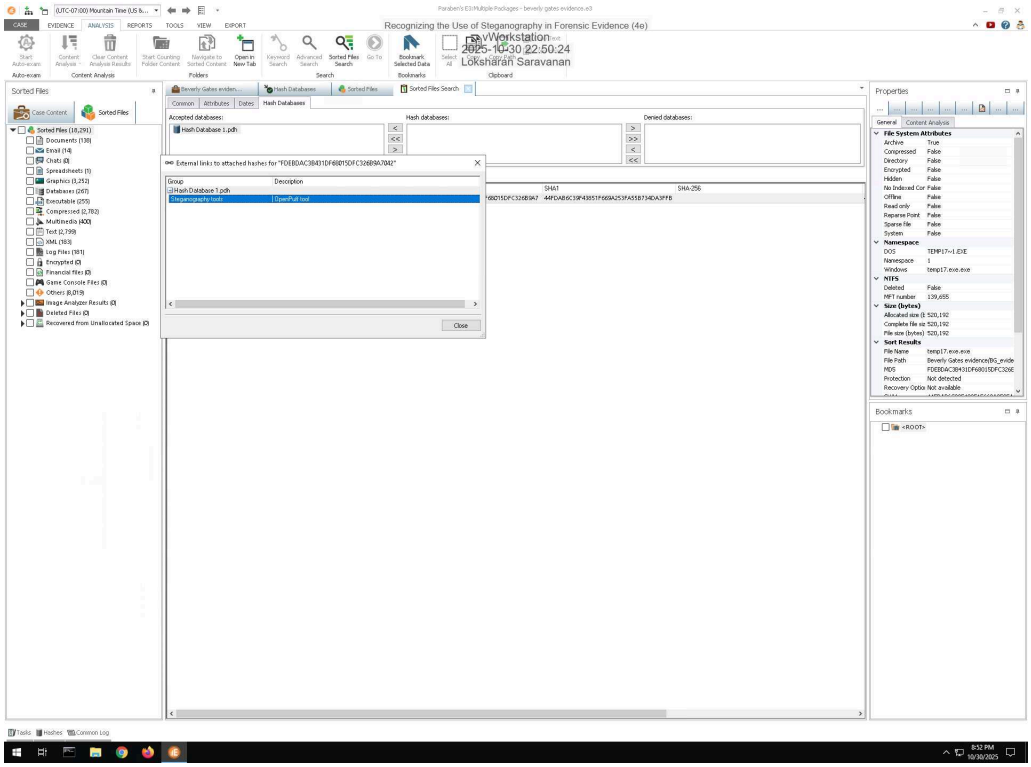
Time on Task:	Progress:
2 hours, 37 minutes	100%

Report Generated: Friday, October 31, 2025 at 1:54 AM

Section 1: Hands-On Demonstration

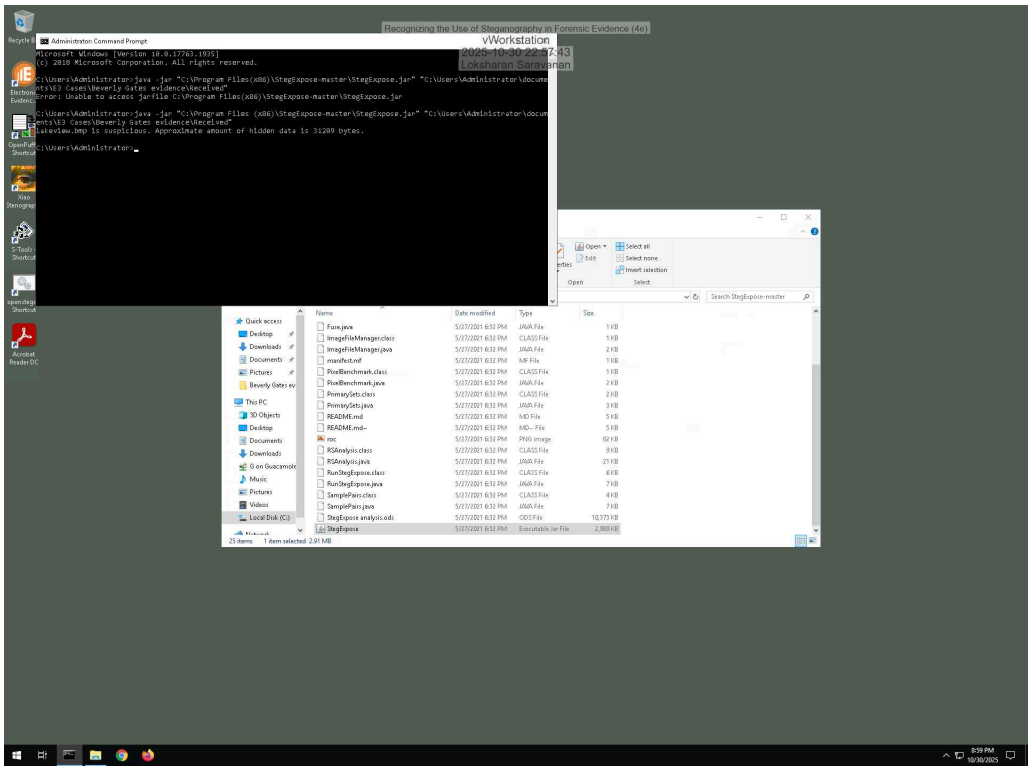
Part 1: Detect Steganography Software on a Drive Image

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

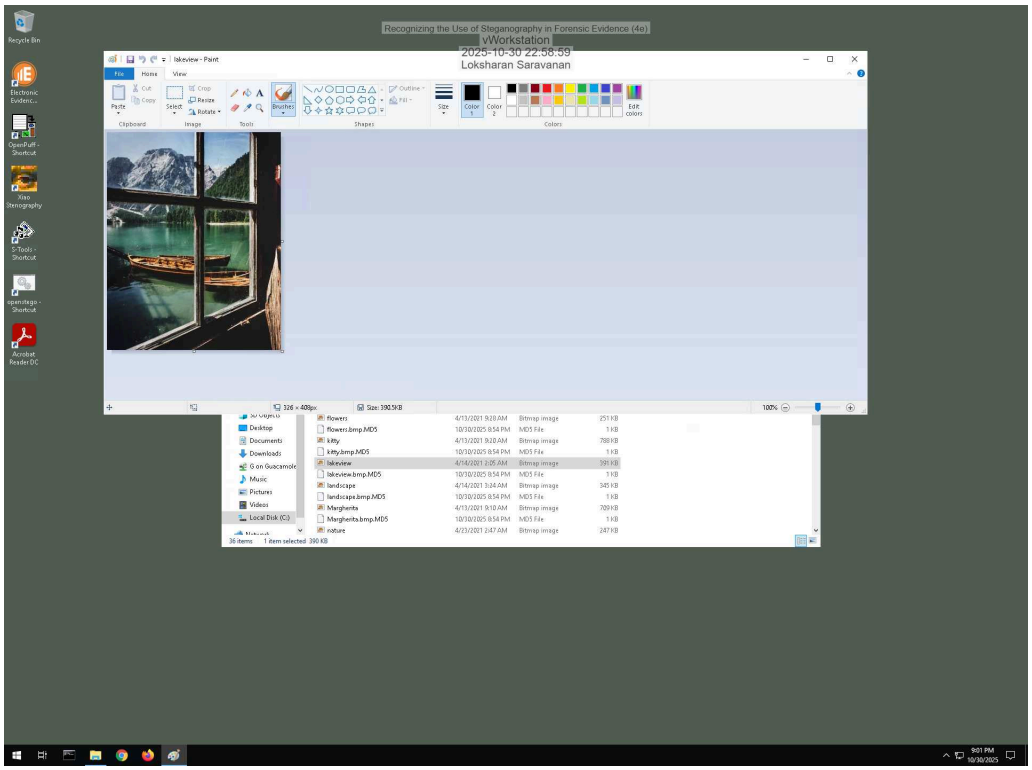


Part 2: Detect Hidden Data in Image Files

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



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

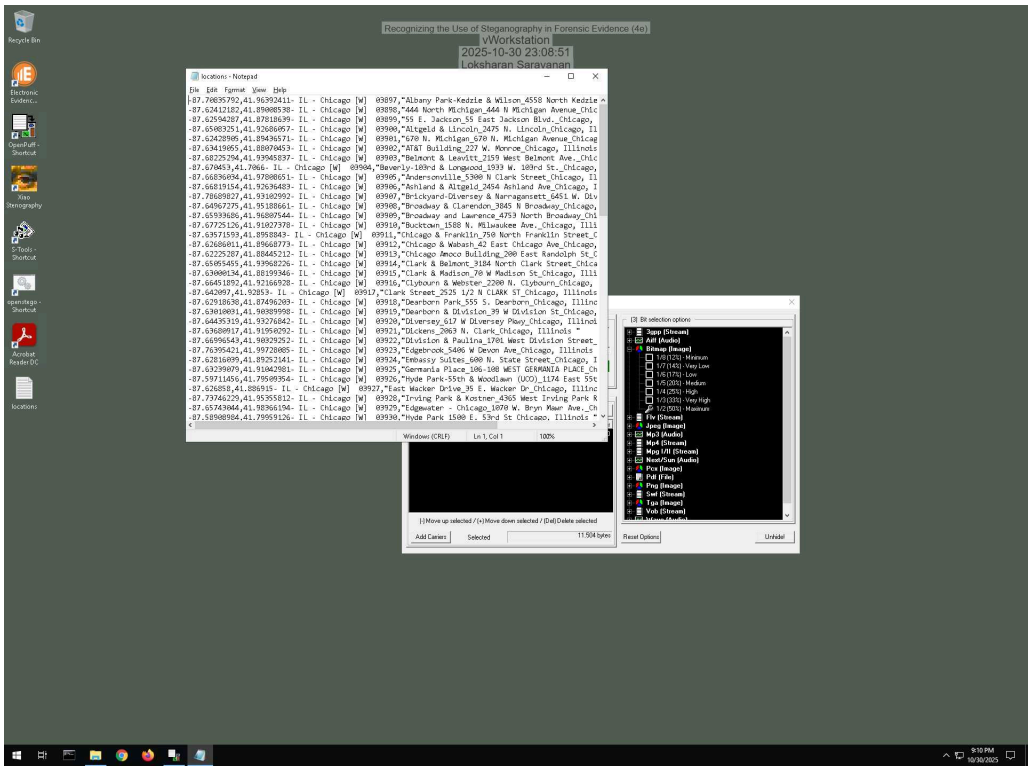


Part 3: Extract Hidden Data from Image Files

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

landmarks

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



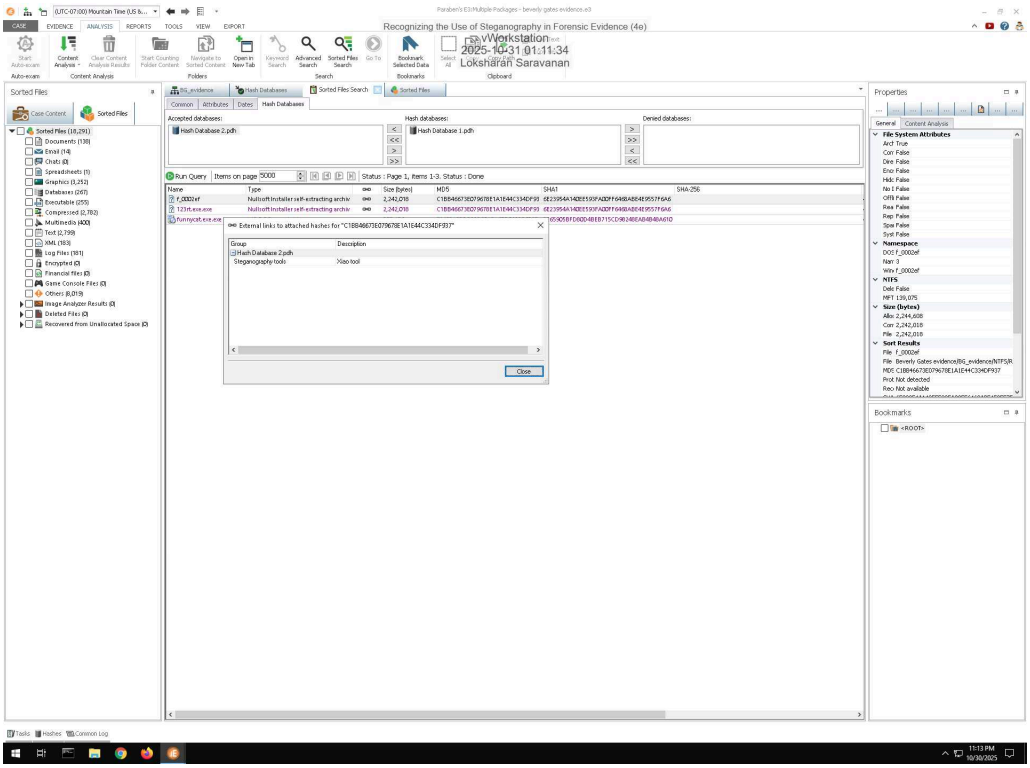
17. **Describe** the contents of the hidden file. How might it be relevant to the current investigation?

The hidden file contains GPS coordinates and a named location . This indicates the file was used to encode a physical meeting or drop site likely logistics for trafficking , meeting place, time window, or rendezvous instructions . It’s highly relevant because it: 1) ties digital evidence to a real-world location, 2) provides actionable intelligence for investigators (surveillance, warrants, witness/interview follow?up), and 3) can corroborate other evidence emails, calendar entries, travel records, CCTV, cell?site data.

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**.

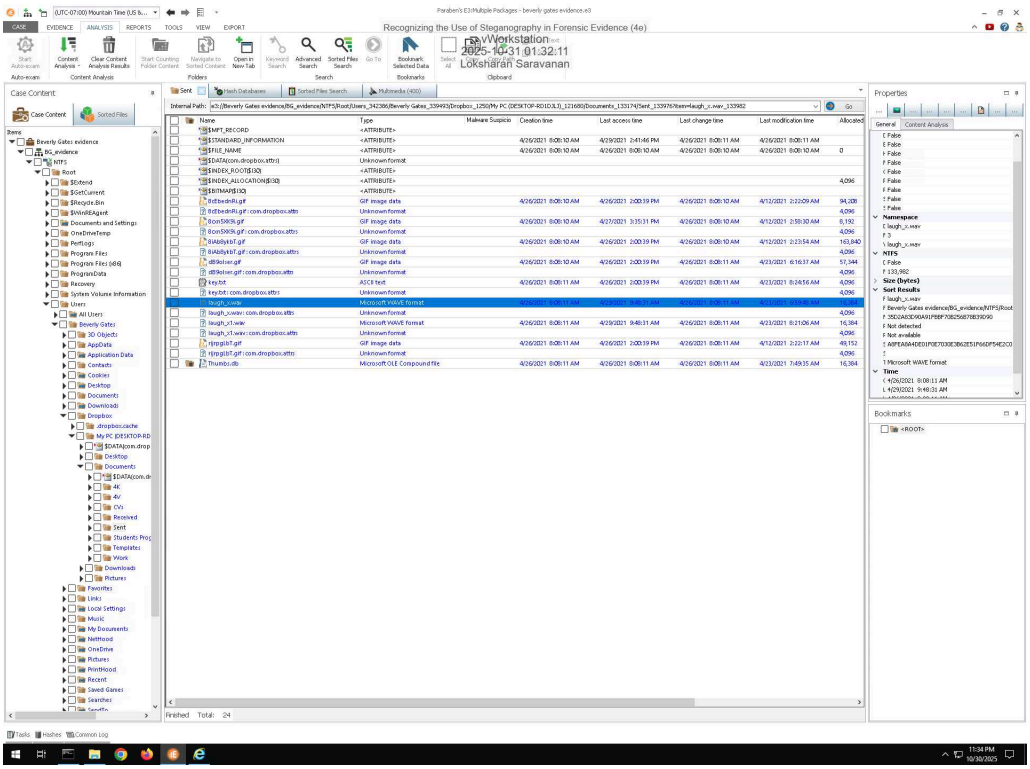


Part 2: Detect Hidden Data in Image and Audio Files

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

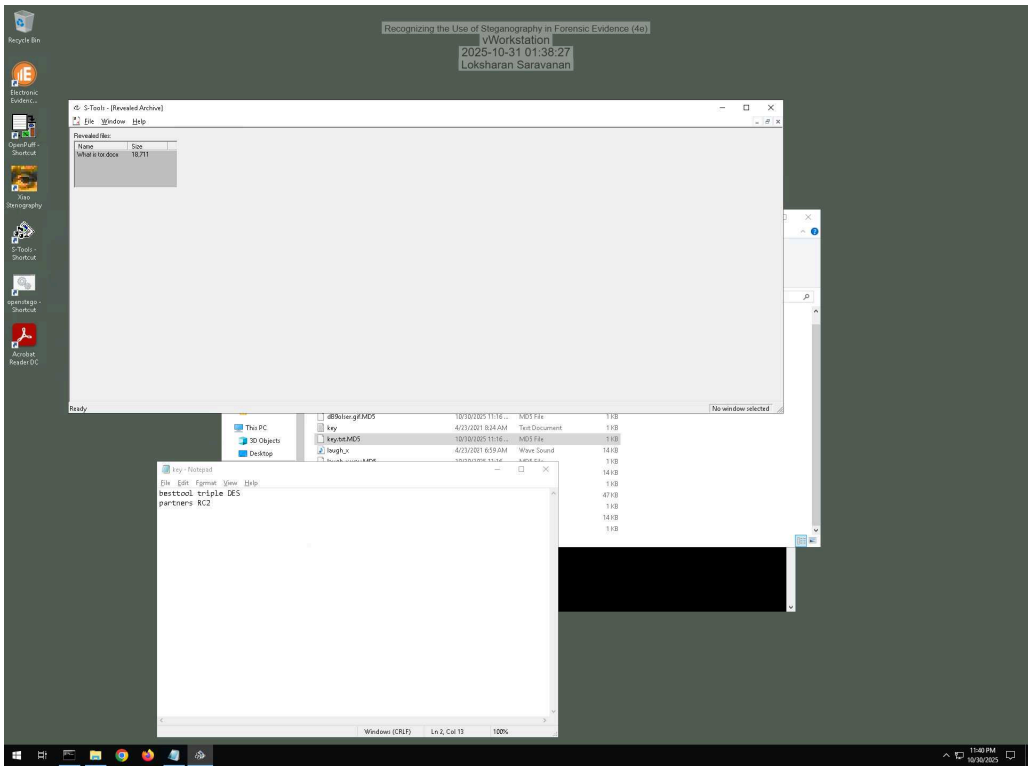
dB9olser.gif

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

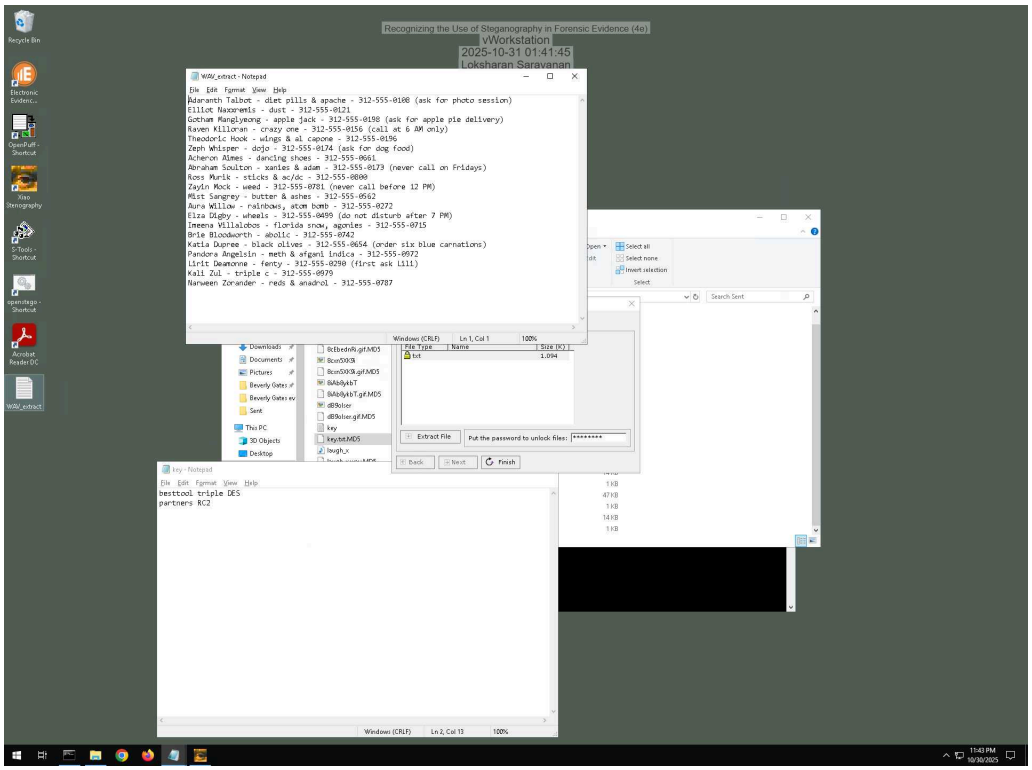


Part 3: Extract Hidden Data from Image and Audio Files

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?

The two hidden files contained text records listing individual names, drug names, contact numbers, and specific call times. This information strongly suggests coordination between Beverly Gates and external parties involved in drug distribution or trafficking operations. The presence of detailed communication instructions and controlled substance references indicates the files were used to manage or schedule illicit transactions. These findings directly support the ongoing investigation by linking Beverly to organized criminal activity and demonstrate intentional concealment of incriminating data using steganography.

Section 3: Challenge and Analysis

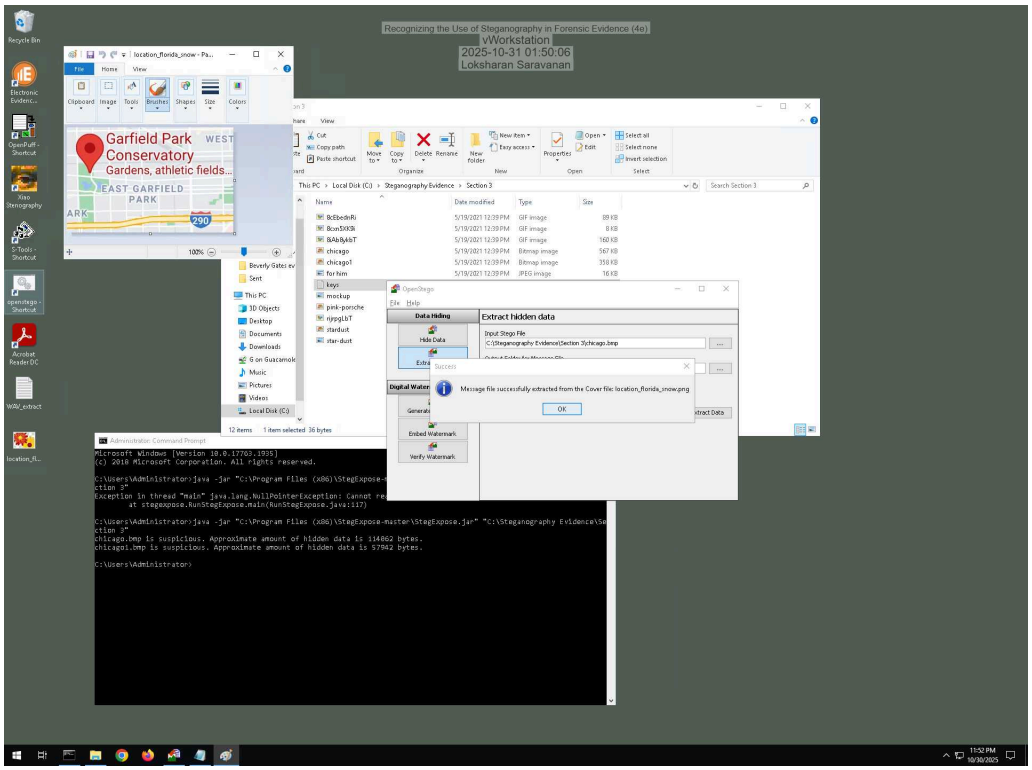
Part 1: Detect More Hidden Data

Record the names of the files that contain concealed data.

chicago.bmpchicago1.bmp are suspicious

Part 2: Extract More Hidden Data

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



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