Student:	Email:
Samman Chouhan	schouhan1@hawk.iit.edu

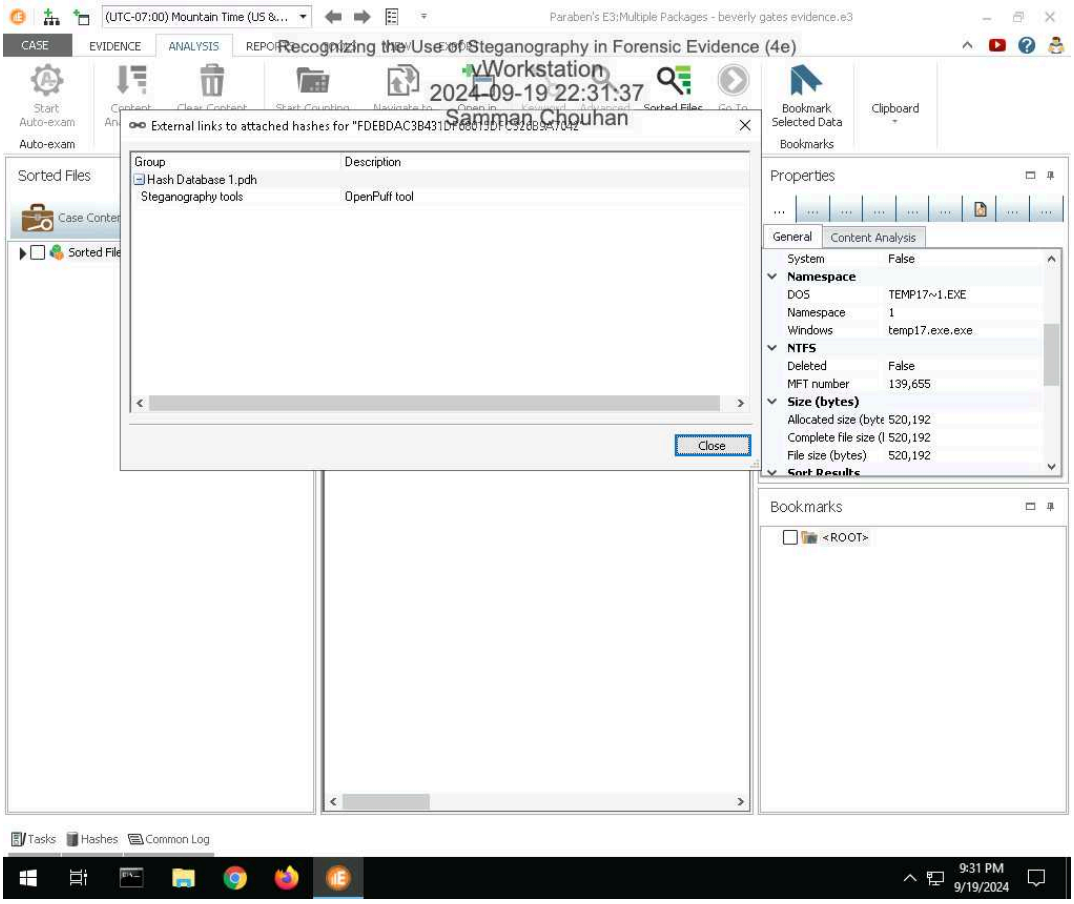
Time on Task:	Progress:
3 hours, 50 minutes	100%

Report Generated: Friday, September 20, 2024 at 12:36 AM

Section 1: Hands-On Demonstration

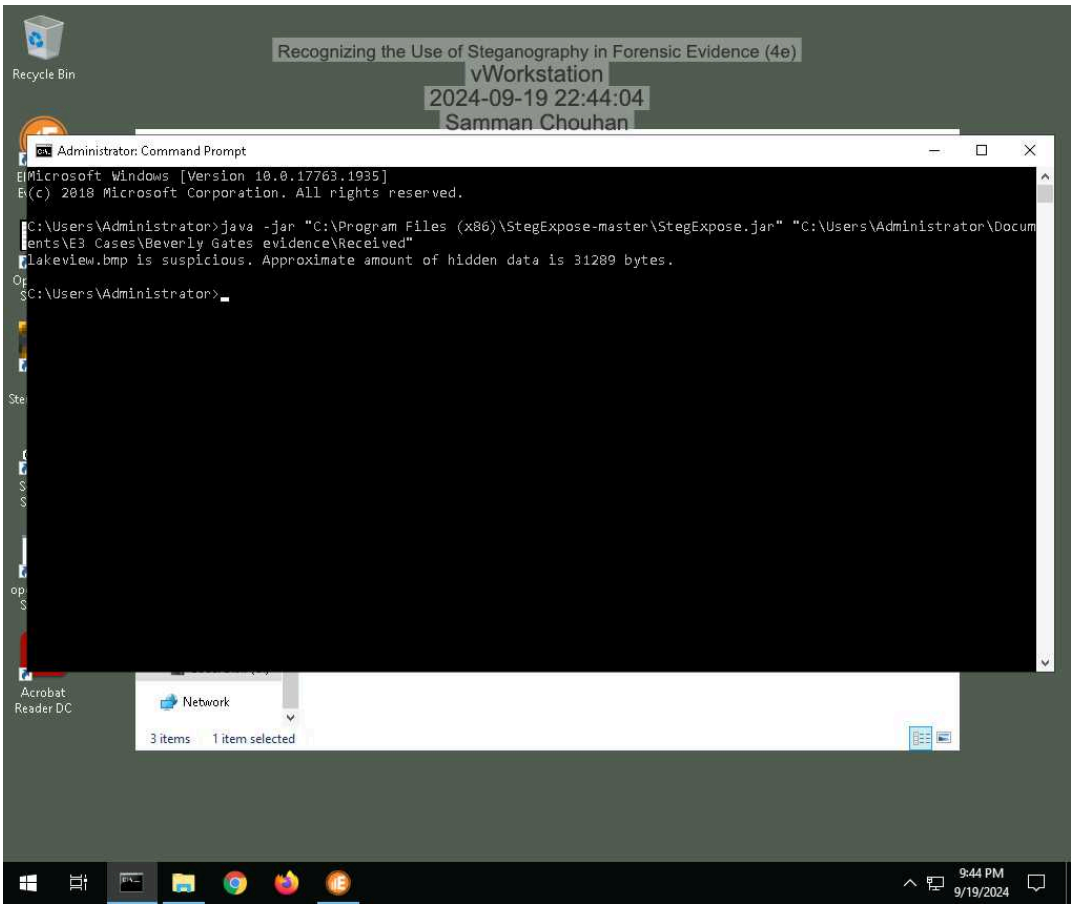
Part 1: Detect Steganography Software on a Drive Image

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

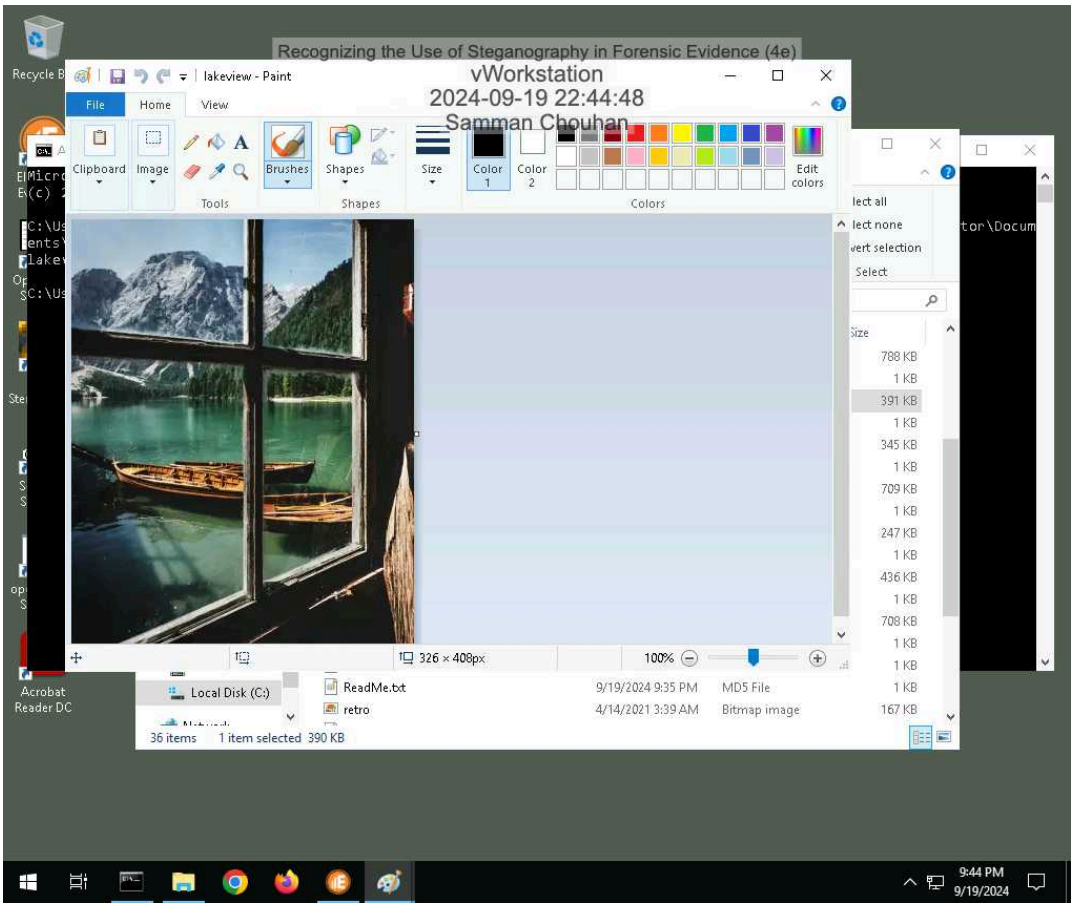


Part 2: Detect Hidden Data in Image Files

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



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

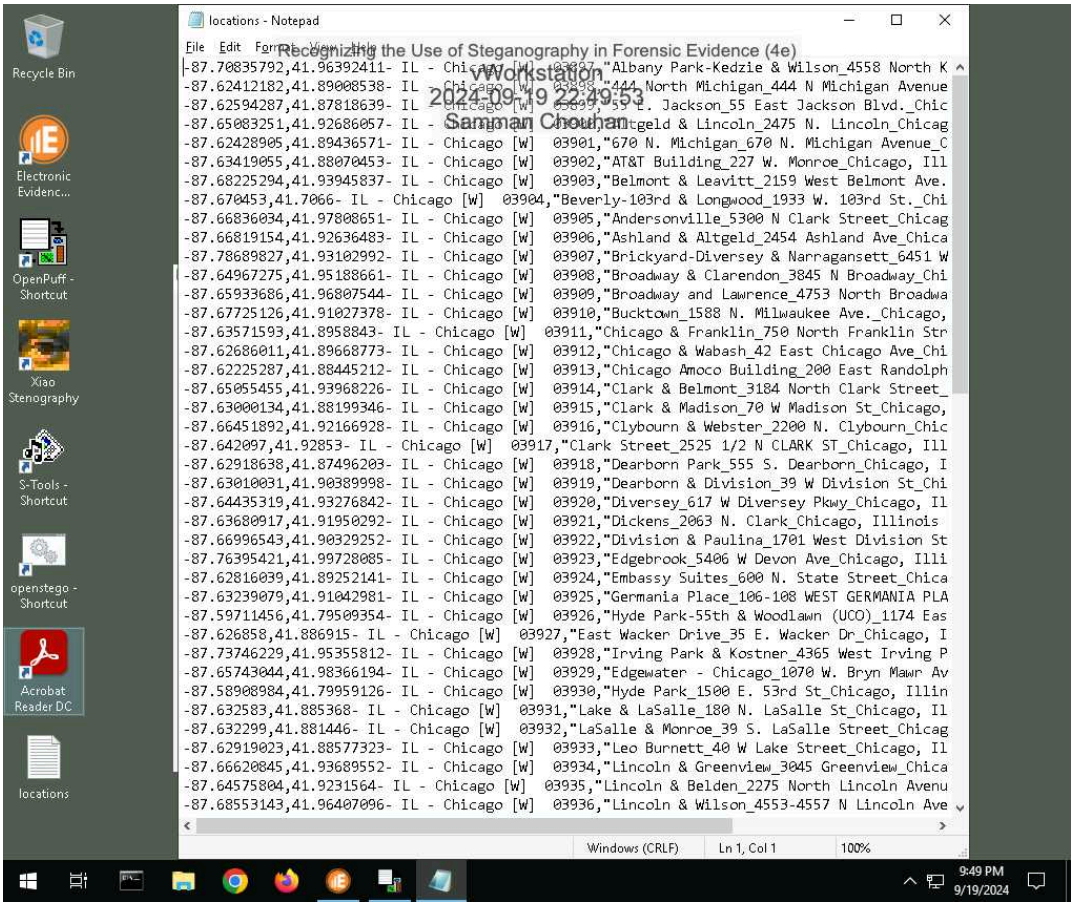


Part 3: Extract Hidden Data from Image Files

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

"landmarks" is the passphrase obtained from the readme file

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



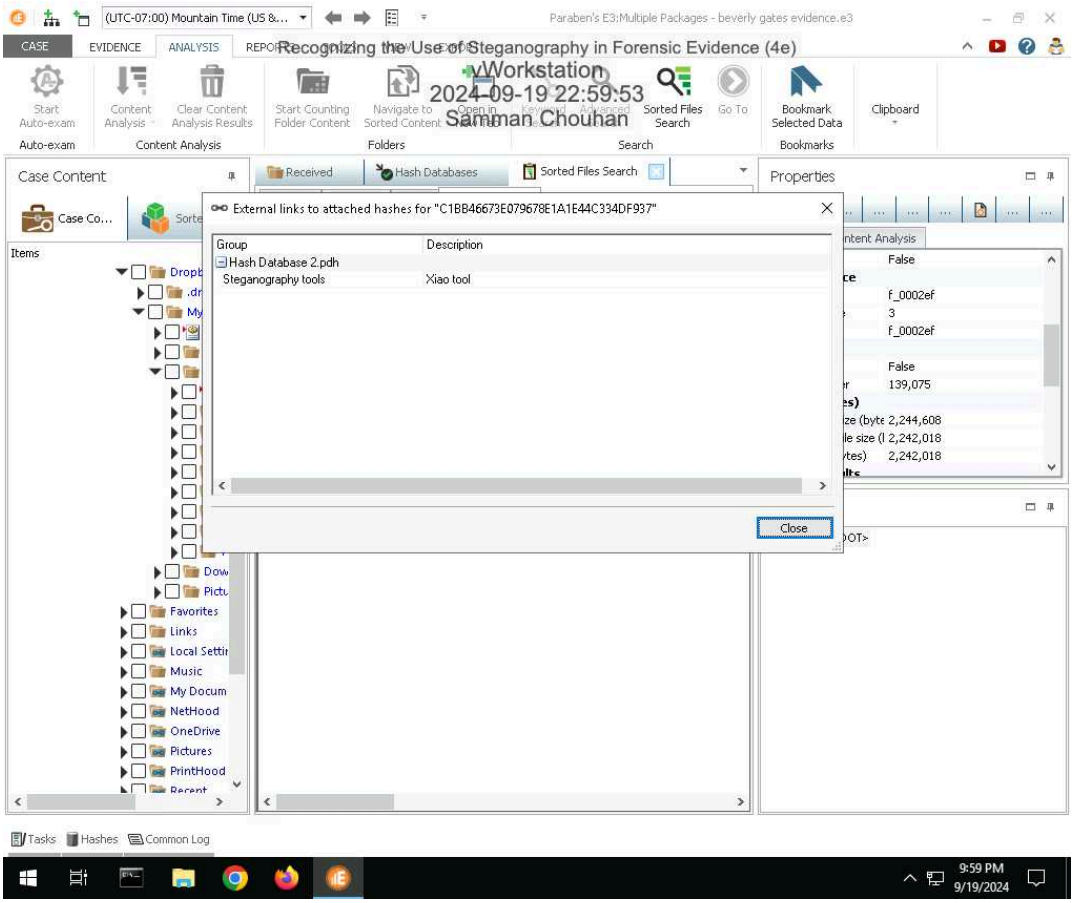
17. **Describe** the contents of the hidden file. How might it be relevant to the current investigation?

the contents of the file is relevant because the creator thought this will not be found , also the content is question contains various location which might be a the part of the current impending inevstigation

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**.

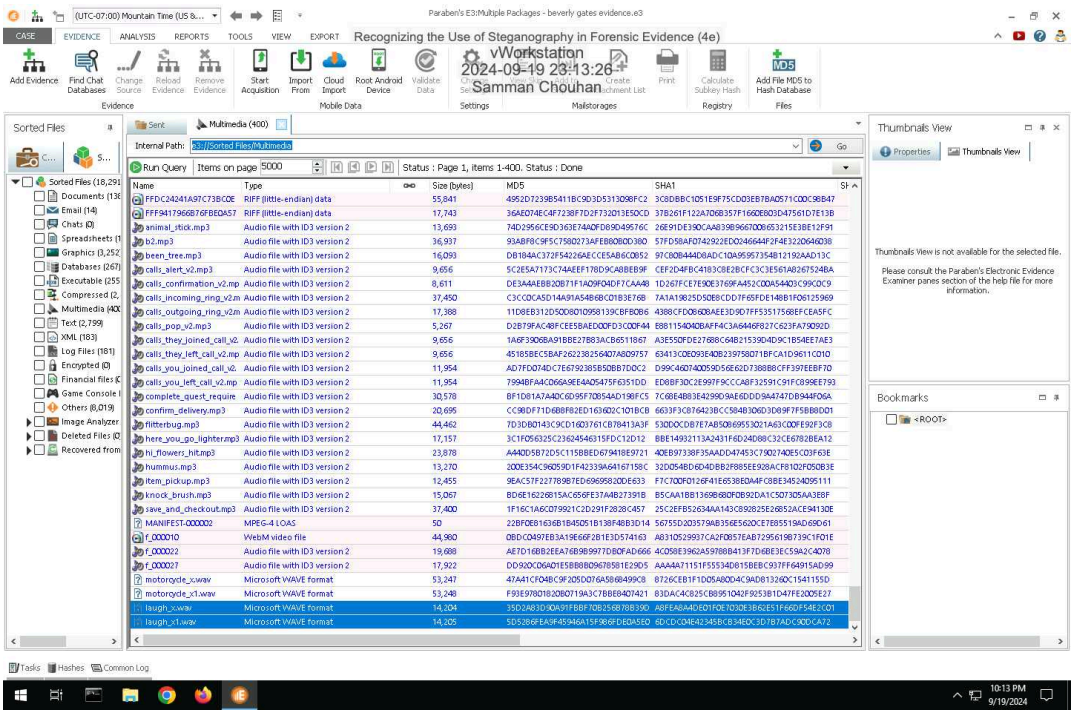


Part 2: Detect Hidden Data in Image and Audio Files

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

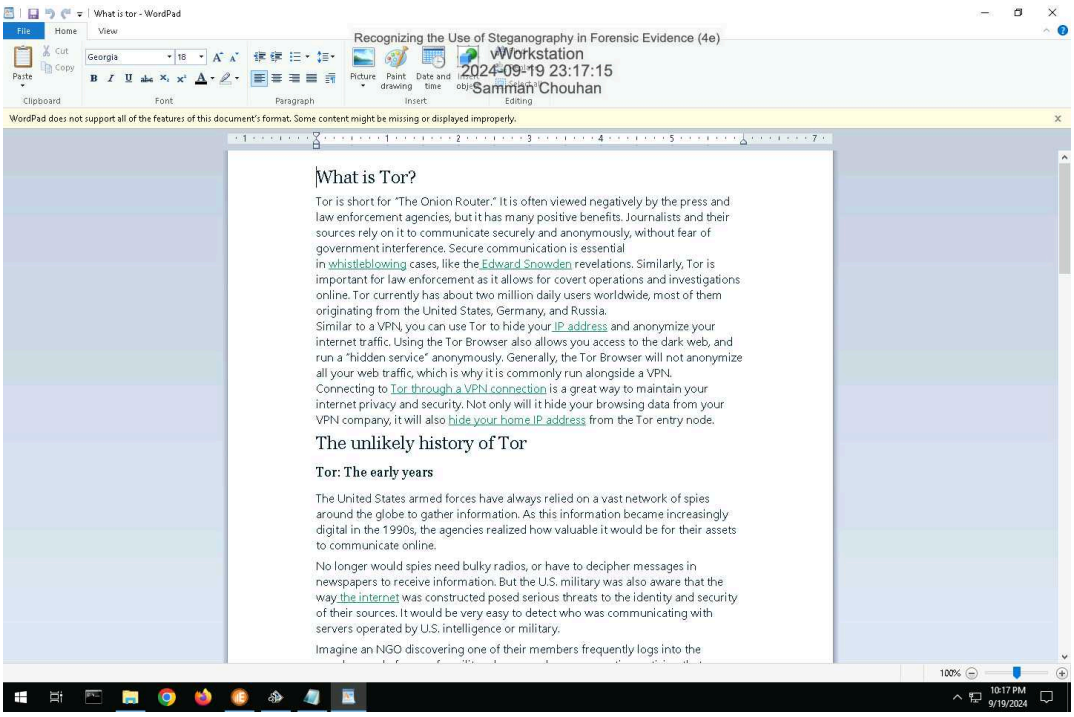
"db9olser.gif" is the suspicious file

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

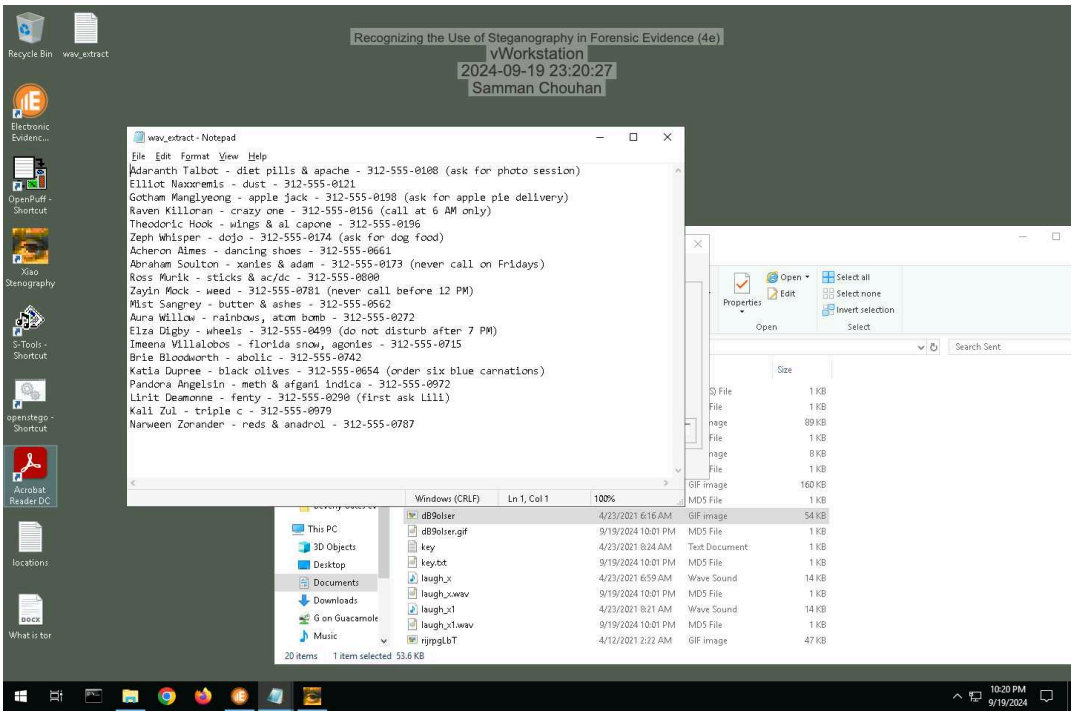


Part 3: Extract Hidden Data from Image and Audio Files

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?

one file contains information about tor , which allows the person to access the dark web and making it easier for them to hide behind the onion layer , the another files gives out names for persons with their cell ,making them potential customers or clients in the ring

Section 3: Challenge and Analysis

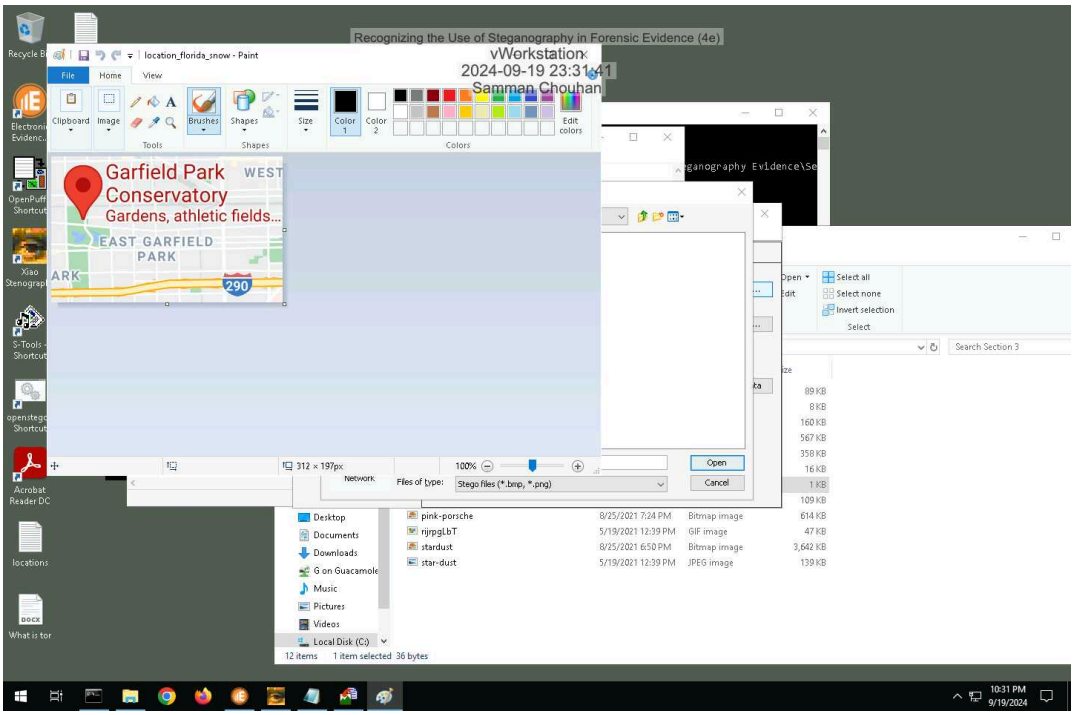
Part 1: Detect More Hidden Data

Record the names of the files that contain concealed data.

chicago.bmp and chicago1.bmp are the two suspicious files its seems from the stegexpose tool

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**.