Student:	Email:
Jake Simpson	jaksimps@iu.edu

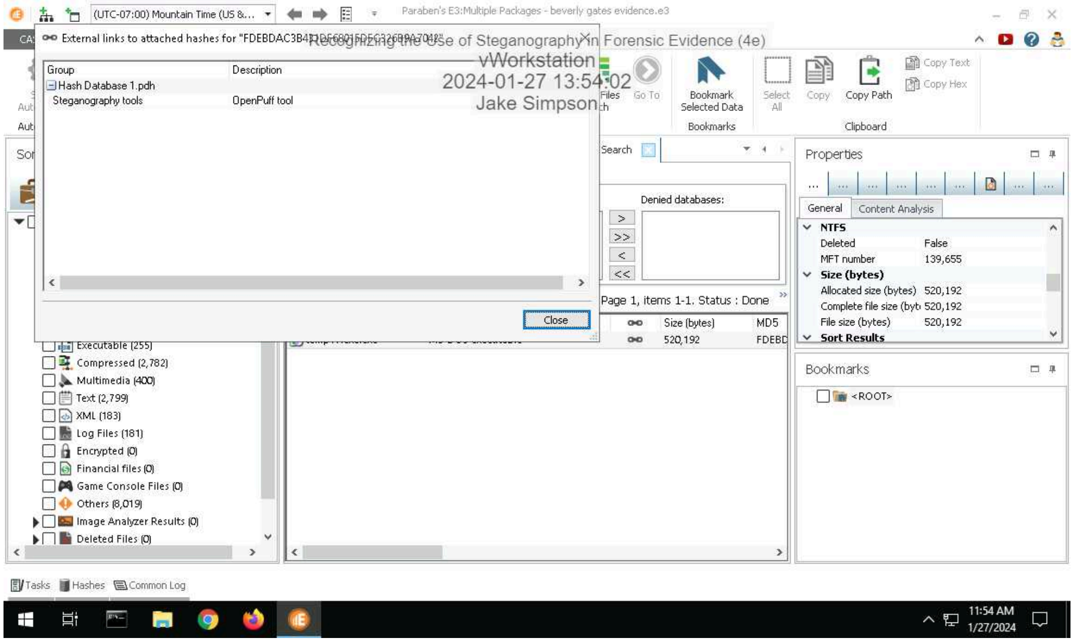
Time on Task:	Progress:
0 hours, 52 minutes	100%

Report Generated: Saturday, January 27, 2024 at 2:35 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**.



Paraben's E3:Multiple Packages - beverly gates evidence.e3

External links to attached hashes for "FDEBDAC3B4[illegible]"

Group	Description
Hash Database 1.pdh	
Steganography tools	OpenPuff tool

Recognizing the Use of Steganography in Forensic Evidence (4e)
vWorkstation
2024-01-27 13:54:02
Jake Simpson

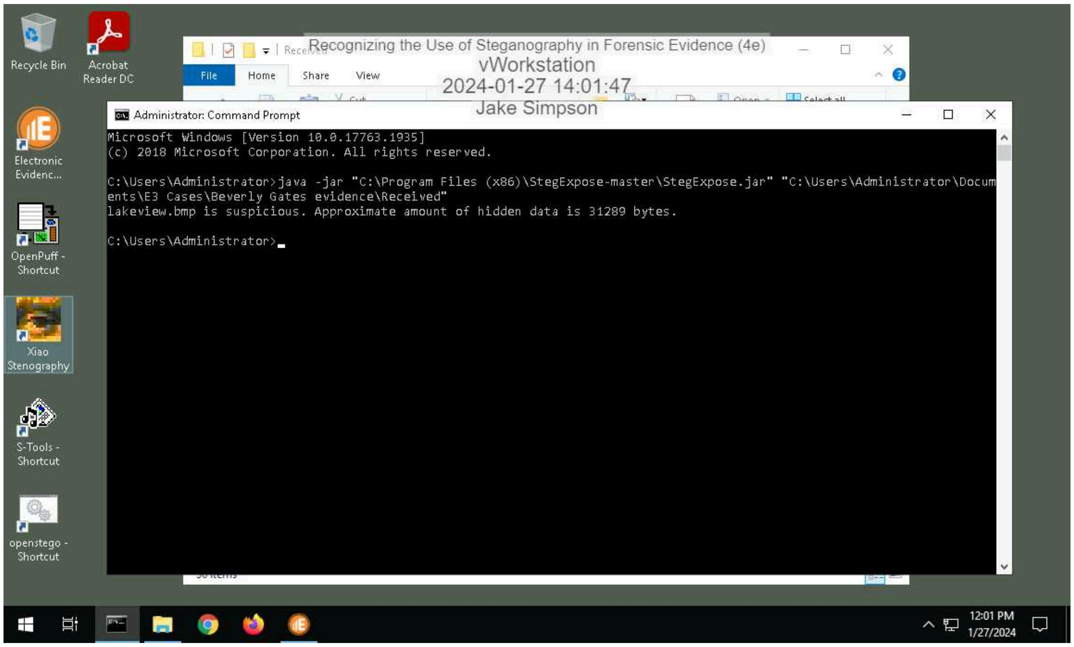
Page 1, items 1-1. Status : Done

Size (bytes)	MD5
520,192	FDEBD

Properties	
NTFS	
Deleted	False
MFT number	139,655
Size (bytes)	
Allocated size (bytes)	520,192
Complete file size (byt	520,192
File size (bytes)	520,192
Sort Results	

Part 2: Detect Hidden Data in Image Files

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

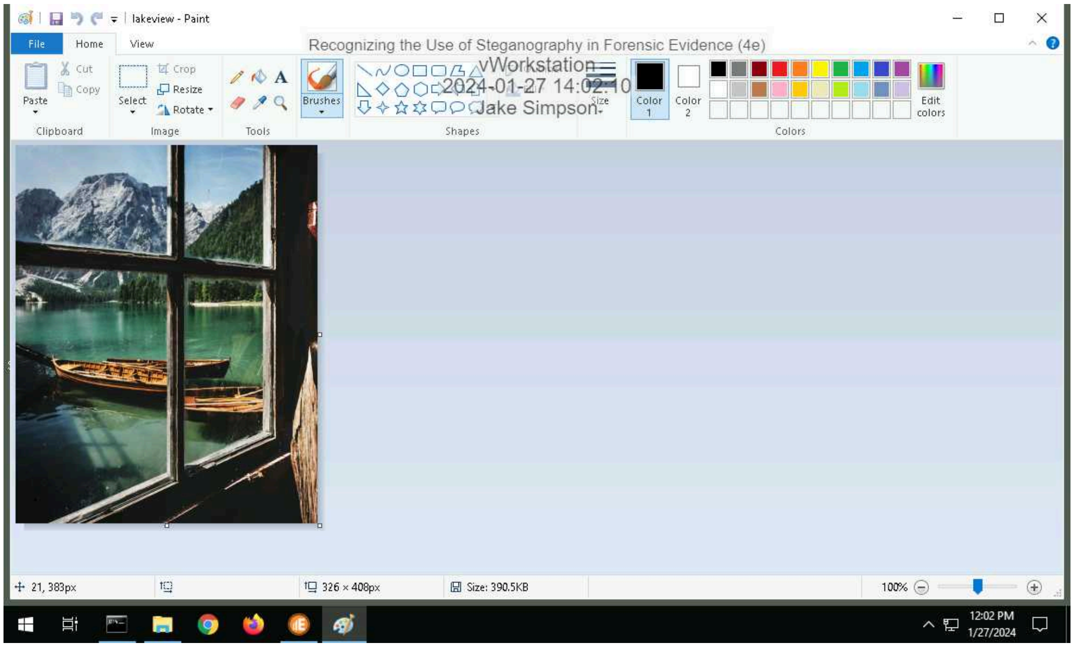


```
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>java -jar "C:\Program Files (x86)\StegExpose-master\StegExpose.jar" "C:\Users\Administrator\Docum
ents\E3 Cases\Beverly Gates evidence\Received"
lakeview.bmp is suspicious. Approximate amount of hidden data is 31289 bytes.

C:\Users\Administrator>
```

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

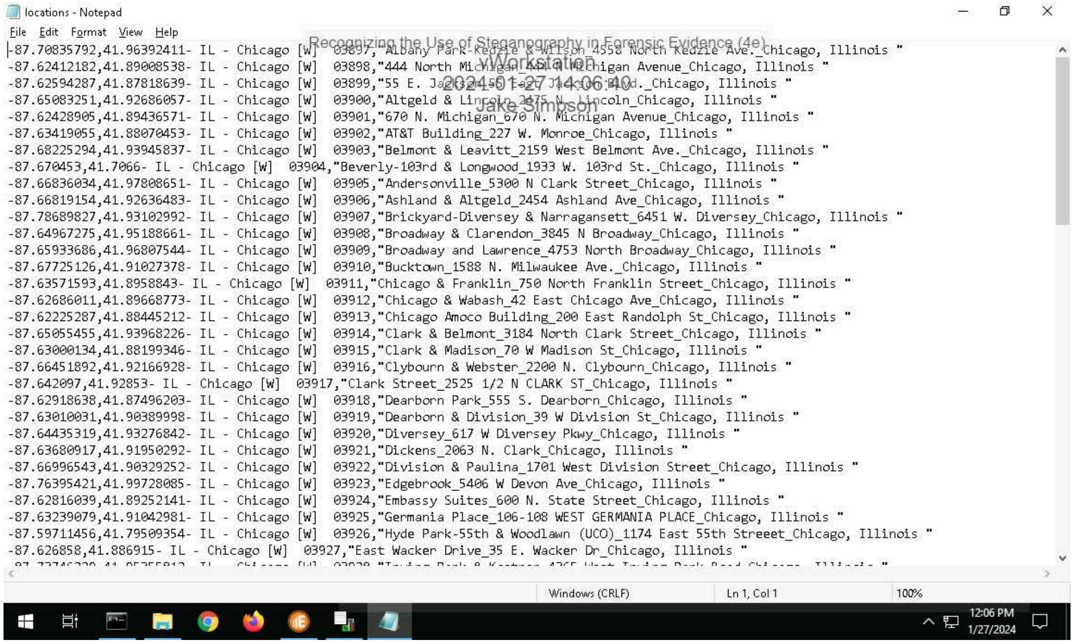


Part 3: Extract Hidden Data from Image Files

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

landmarks

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



```
-87.70835792,41.96392411- IL - Chicago [W]  03897,"Albany Park-Kedzie & Wilson_4558 North Kedzie Ave._Chicago, Illinois "
-87.62412182,41.89008538- IL - Chicago [W]  03898,"444 North Michigan_444 N Michigan Avenue_Chicago, Illinois "
-87.62594287,41.87818639- IL - Chicago [W]  03899,"55 E. Jackson_55 East Jackson Blvd._Chicago, Illinois "
-87.65083251,41.92686057- IL - Chicago [W]  03900,"Altgeld & Lincoln_2475 N. Lincoln_Chicago, Illinois "
-87.62428905,41.89436571- IL - Chicago [W]  03901,"670 N. Michigan_670 N. Michigan Avenue_Chicago, Illinois "
-87.63419055,41.88070453- IL - Chicago [W]  03902,"AT&T Building_227 W. Monroe_Chicago, Illinois "
-87.68225294,41.93945837- IL - Chicago [W]  03903,"Belmont & Leavitt_2159 West Belmont Ave._Chicago, Illinois "
-87.670453,41.7066- IL - Chicago [W]  03904,"Beverly-103rd & Longwood_1933 W. 103rd St._Chicago, Illinois "
-87.66836034,41.97808651- IL - Chicago [W]  03905,"Andersonville_5300 N Clark Street_Chicago, Illinois "
-87.66819154,41.92636483- IL - Chicago [W]  03906,"Ashland & Altgeld_2454 Ashland Ave_Chicago, Illinois "
-87.78689827,41.93102992- IL - Chicago [W]  03907,"Brickyard-Diversey & Narragansett_6451 W. Diversey_Chicago, Illinois "
-87.64967275,41.95188661- IL - Chicago [W]  03908,"Broadway & Clarendon_3845 N Broadway_Chicago, Illinois "
-87.65933686,41.96807544- IL - Chicago [W]  03909,"Broadway and Lawrence_4753 North Broadway_Chicago, Illinois "
-87.67725126,41.91027378- IL - Chicago [W]  03910,"Bucktown_1588 N. Milwaukee Ave._Chicago, Illinois "
-87.63571593,41.8958843- IL - Chicago [W]  03911,"Chicago & Franklin_750 North Franklin Street_Chicago, Illinois "
-87.62686011,41.89668773- IL - Chicago [W]  03912,"Chicago & Wabash_42 East Chicago Ave_Chicago, Illinois "
-87.62225287,41.88445212- IL - Chicago [W]  03913,"Chicago Amoco Building_200 East Randolph St_Chicago, Illinois "
-87.65055455,41.93968226- IL - Chicago [W]  03914,"Clark & Belmont_3184 North Clark Street_Chicago, Illinois "
-87.63000134,41.88199346- IL - Chicago [W]  03915,"Clark & Madison_70 W Madison St_Chicago, Illinois "
-87.66451892,41.92166928- IL - Chicago [W]  03916,"Clybourn & Webster_2200 N. Clybourn_Chicago, Illinois "
-87.642097,41.92853- IL - Chicago [W]  03917,"Clark Street_2525 1/2 N CLARK ST_Chicago, Illinois "
-87.62918638,41.87496203- IL - Chicago [W]  03918,"Dearborn Park_555 S. Dearborn_Chicago, Illinois "
-87.63010031,41.90389998- IL - Chicago [W]  03919,"Dearborn & Division_39 W Division St_Chicago, Illinois "
-87.64435319,41.93276842- IL - Chicago [W]  03920,"Diversey_617 W Diversey Pkwy_Chicago, Illinois "
-87.63680917,41.91950292- IL - Chicago [W]  03921,"Dickens_2063 N. Clark_Chicago, Illinois "
-87.66996543,41.90329252- IL - Chicago [W]  03922,"Division & Paulina_1701 West Division Street_Chicago, Illinois "
-87.76395421,41.99728085- IL - Chicago [W]  03923,"Edgebrook_5406 W Devon Ave_Chicago, Illinois "
-87.62816039,41.89252141- IL - Chicago [W]  03924,"Embassy Suites_600 N. State Street_Chicago, Illinois "
-87.63239079,41.91042981- IL - Chicago [W]  03925,"Germania Place_106-108 WEST GERMANIA PLACE_Chicago, Illinois "
-87.59711456,41.79509354- IL - Chicago [W]  03926,"Hyde Park-55th & Woodlawn (UCO)_1174 East 55th Streeet_Chicago, Illinois "
-87.626858,41.886915- IL - Chicago [W]  03927,"East Wacker Drive_35 E. Wacker Dr_Chicago, Illinois "
```

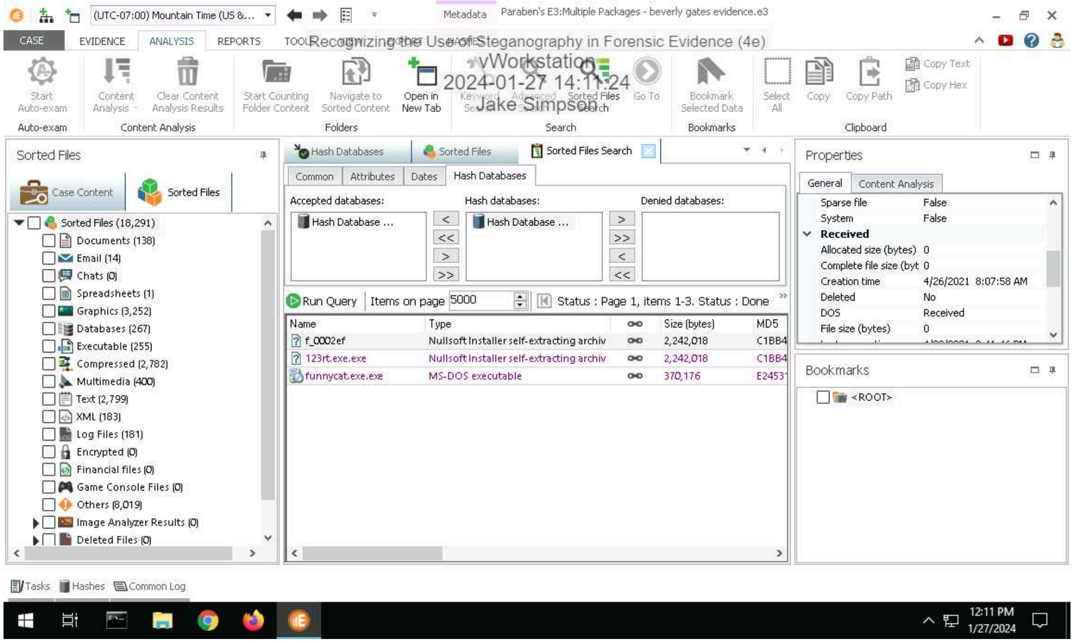
17. **Describe** the contents of the hidden file. How might it be relevant to the current investigation?

The contents appear to be specific locations. This could be important to the investigation into her illegal drug trafficking.

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**.



Items on page 5000 | Status : Page 1, items 1-3. Status : Done

Name	Type		Size (bytes)	MD5
f_0002ef	Nullsoft Installer self-extracting archiv		2,242,018	C1BB4
123rt.exe.exe	Nullsoft Installer self-extracting archiv		2,242,018	C1BB4
funnycat.exe.exe	MS-DOS executable		370,176	E2453

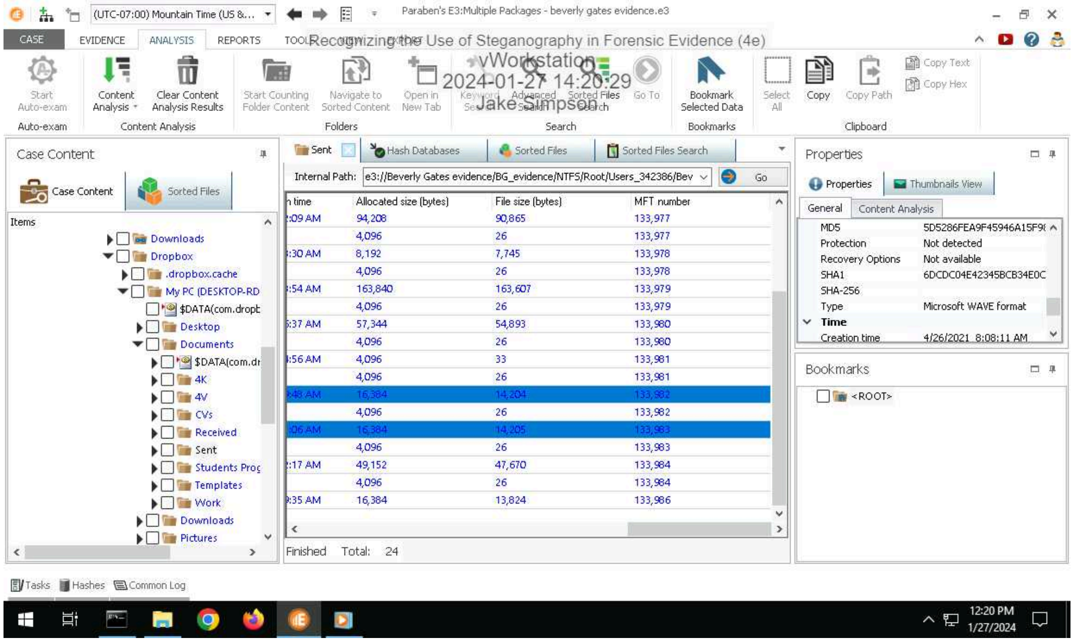
Sparse file	False
System	False
Received	
Allocated size (bytes)	0
Complete file size (byt	0
Creation time	4/26/2021 8:07:58 AM
Deleted	No
DOS	Received
File size (bytes)	0

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 suspicious

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



Internal Path: e3://Beverly Gates evidence/BG_evidence/NTFS/Root/Users_342386/Bev

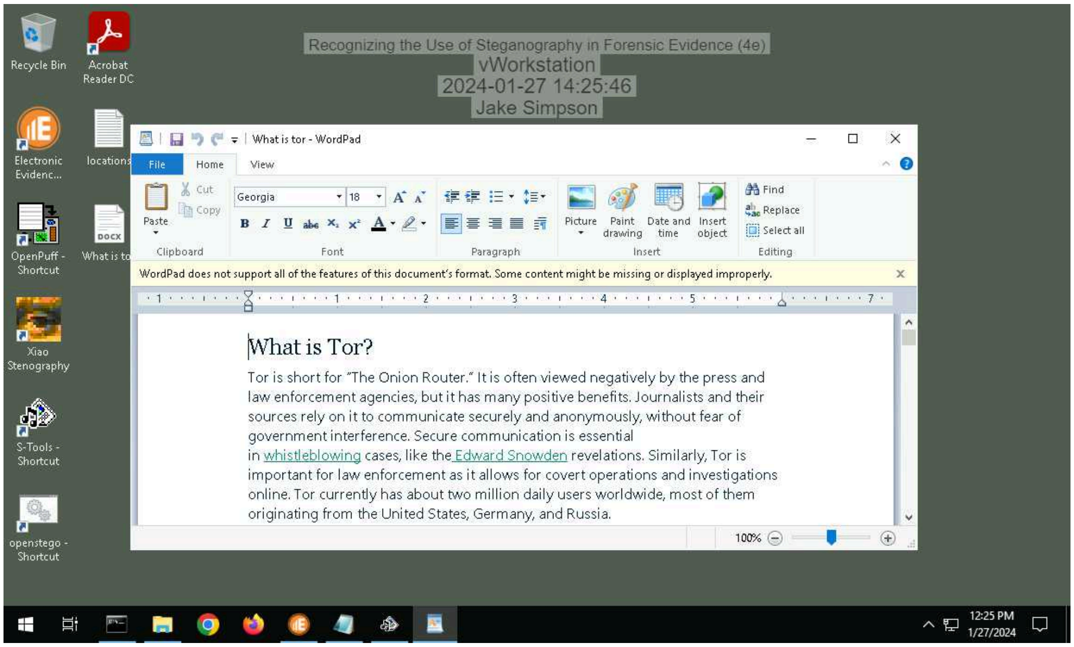
n time	Allocated size (bytes)	File size (bytes)	MFT number
:09 AM	94,208	90,865	133,977
	4,096	26	133,977
:30 AM	8,192	7,745	133,978
	4,096	26	133,978
:54 AM	163,840	163,607	133,979
	4,096	26	133,979
:37 AM	57,344	54,893	133,980
	4,096	26	133,980
:56 AM	4,096	33	133,981
	4,096	26	133,981
:48 AM	16,384	14,204	133,982
	4,096	26	133,982
:06 AM	16,384	14,205	133,983
	4,096	26	133,983
:17 AM	49,152	47,670	133,984
	4,096	26	133,984
:35 AM	16,384	13,824	133,986

Finished Total: 24

MD5	5D5286FEA9F45946A15F9(
Protection	Not detected
Recovery Options	Not available
SHA1	6DCDC04E42345BCB34E0C
SHA-256	
Type	Microsoft WAVE format
Time	
Creation time	4/26/2021 8:08:11 AM

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**.

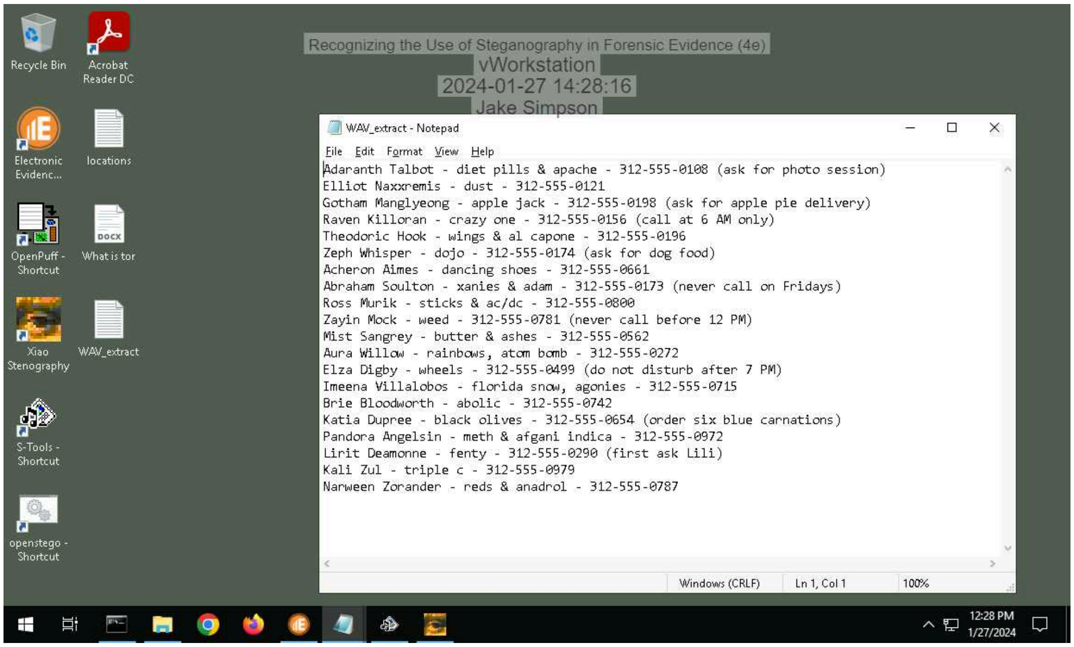


WordPad does not support all of the features of this document's format. Some content might be missing or displayed improperly.

What is Tor?

Tor is short for "The Onion Router." It is often viewed negatively by the press and law enforcement agencies, but it has many positive benefits. Journalists and their sources rely on it to communicate securely and anonymously, without fear of government interference. Secure communication is essential in whistleblowing cases, like the Edward Snowden revelations. Similarly, Tor is important for law enforcement as it allows for covert operations and investigations online. Tor currently has about two million daily users worldwide, most of them originating from the United States, Germany, and Russia.

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



```
Adaranth Talbot - diet pills & apache - 312-555-0108 (ask for photo session)
Elliot Naxxremis - dust - 312-555-0121
Gotham Manglyeong - apple jack - 312-555-0198 (ask for apple pie delivery)
Raven Killoran - crazy one - 312-555-0156 (call at 6 AM only)
Theodoric Hook - wings & al capone - 312-555-0196
Zeph Whisper - dojo - 312-555-0174 (ask for dog food)
Acheron Aimes - dancing shoes - 312-555-0661
Abraham Soulton - xanies & adam - 312-555-0173 (never call on Fridays)
Ross Murik - sticks & ac/dc - 312-555-0800
Zayin Mock - weed - 312-555-0781 (never call before 12 PM)
Mist Sangrey - butter & ashes - 312-555-0562
Aura Willow - rainbows, atom bomb - 312-555-0272
Elza Digby - wheels - 312-555-0499 (do not disturb after 7 PM)
Imeena Villalobos - florida snow, agonies - 312-555-0715
Brie Bloodworth - abolic - 312-555-0742
Katia Dupree - black olives - 312-555-0654 (order six blue carnations)
Pandora Angelsin - meth & afgani indica - 312-555-0972
Lirit Deamonne - fenty - 312-555-0290 (first ask Lili)
Kali Zul - triple c - 312-555-0979
Narween Zorander - reds & anadrol - 312-555-0787
```

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

The contents from the gif file show information about Tor which is a software used for anonymous communication. The contents from the WAV file show names and phone numbers of people and drugs corresponding to the people. This is useful for the narcotics investigation

Section 3: Challenge and Analysis

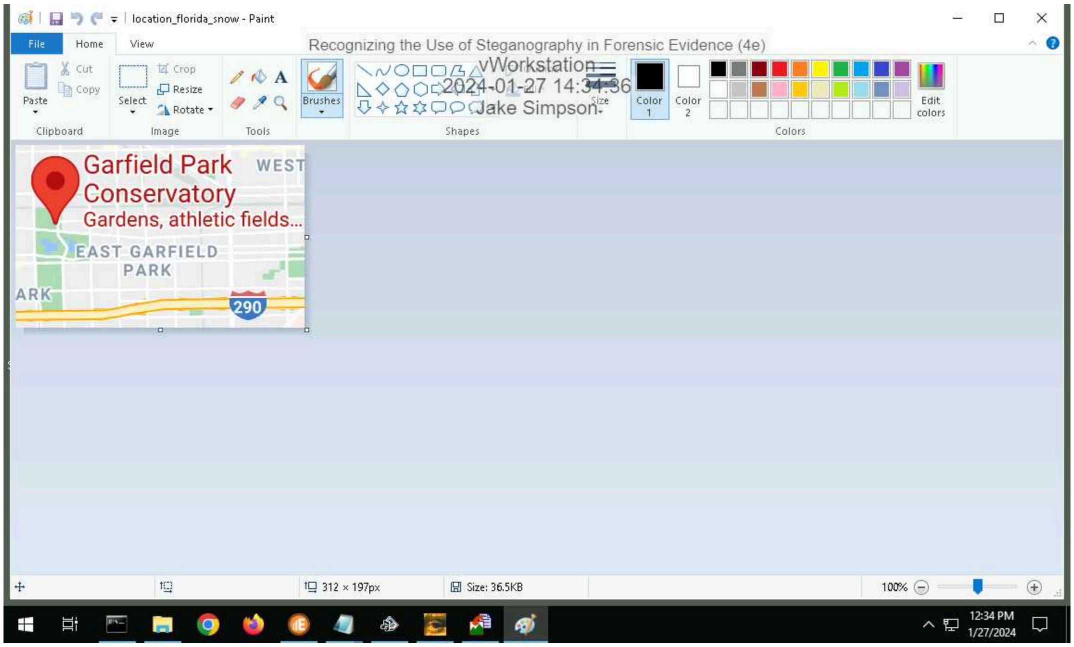
Part 1: Detect More Hidden Data

Record the names of the files that contain concealed data.

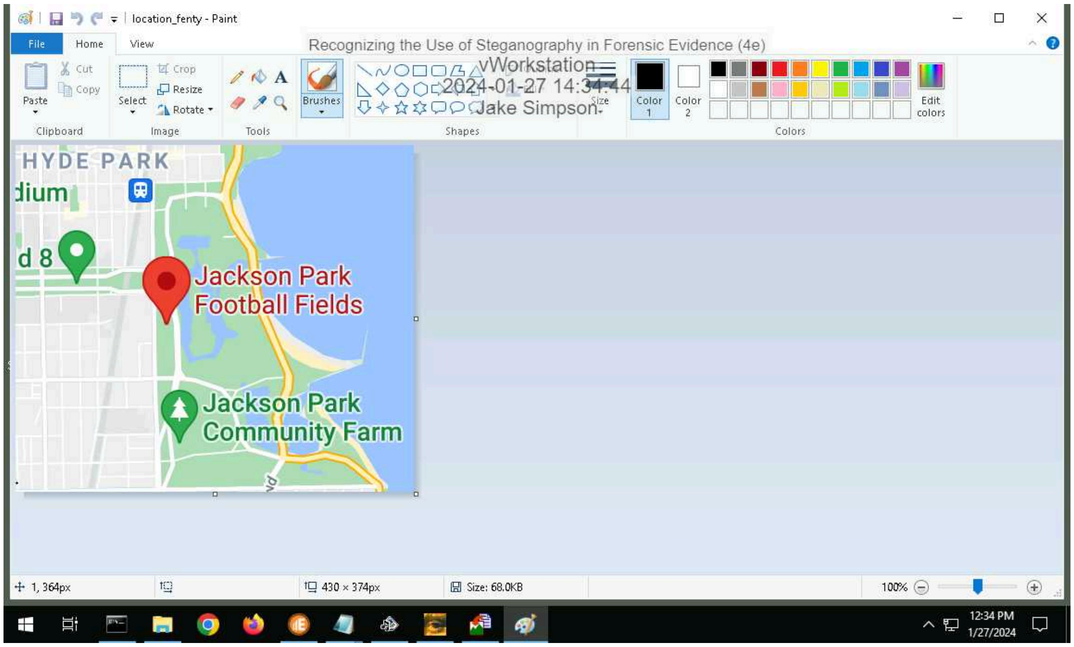
Both chichago.bmp and chichago1.bmp are suspicious.

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**.


location_fenty - Paint
File
Home
View
Recognizing the Use of Steganography in Forensic Evidence (4e)
vWorkstation
2024-01-27 14:34:44
Jake Simpson
Paste
Cut
Copy
Clipboard
Select
Crop
Resize
Rotate
Image
Tools
Brushes
Shapes
Size
Color 1
Color 2
Colors
Edit colors
HYDE PARK
dium
d 8
Jackson Park Football Fields
Jackson Park Community Farm
1, 364px
430 × 374px
Size: 68.0KB
100%
12:34 PM
1/27/2024