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

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

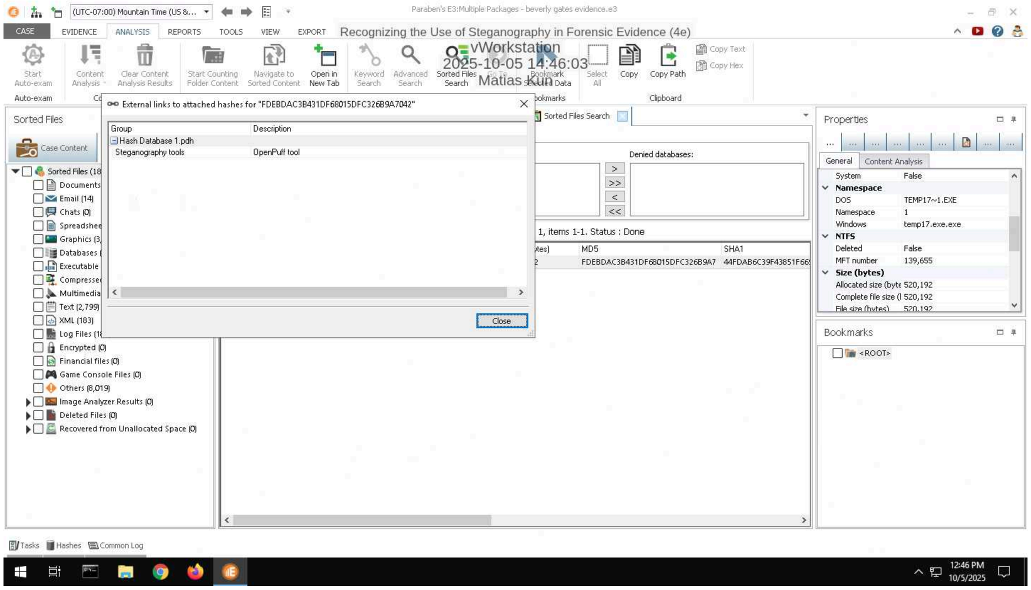
Student: Matias Kun	Email: rvh4zx@virginia.edu
Time on Task: 9 hours, 20 minutes	Progress: 100%

Report Generated: Sunday, October 5, 2025 at 4:40 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**.



External links to attached hashes for "FDEBDAC3B431DF68015DFC326B9A7042"

Group	Description
Hash Database 1.pdh	
Steganography tools	OpenPuff tool

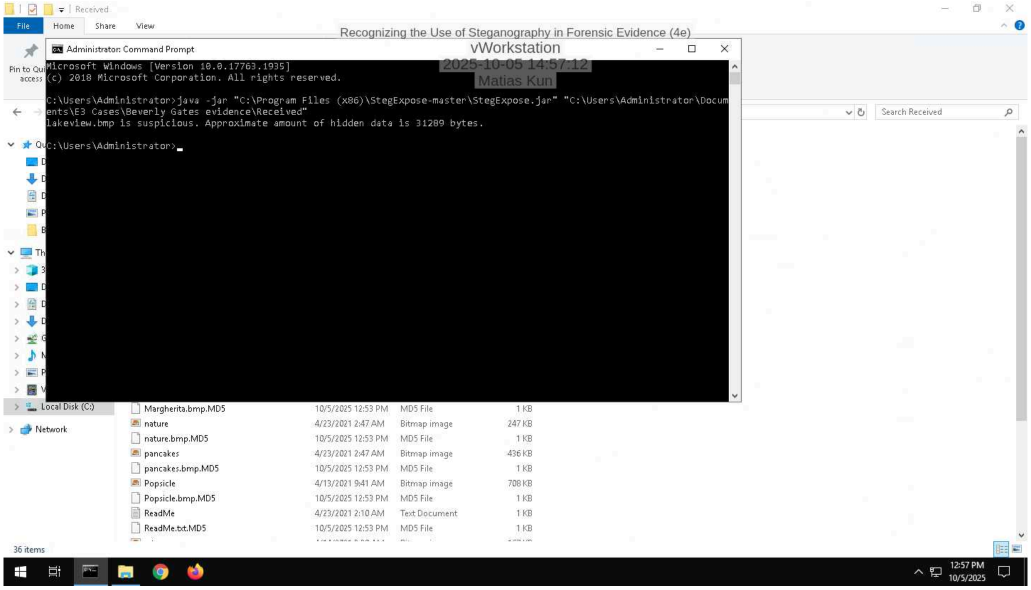
1, items 1-1. Status : Done

MD5	SHA1
FDEBDAC3B431DF68015DFC326B9A7	44FDAB6C39F43851F66

System	False
Namespace	
DOS	TEMP17~1.EXE
Namespace	1
Windows	temp17.exe.exe
NTFS	
Deleted	False
MFT number	139,655
Size (bytes)	
Allocated size (byte	520,192
Complete file size (l	520,192
File size (bytes)	520,192

Part 2: Detect Hidden Data in Image Files

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



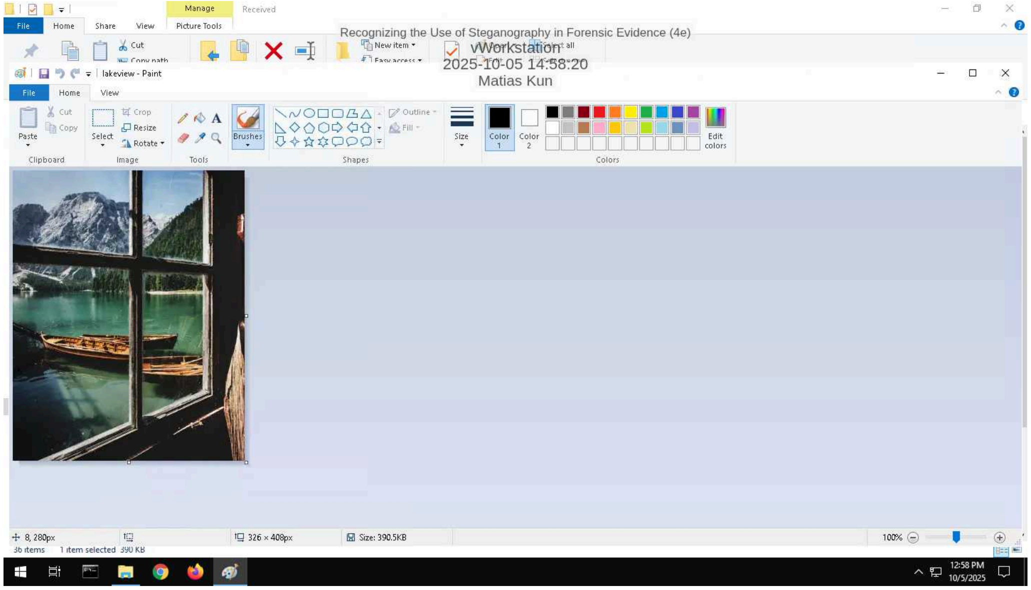
```
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

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>_
```

Margherita.bmp.MD5	10/5/2025 12:53 PM	MD5 File	1 KB
nature	4/23/2021 2:47 AM	Bitmap image	247 KB
nature.bmp.MD5	10/5/2025 12:53 PM	MD5 File	1 KB
pancakes	4/23/2021 2:47 AM	Bitmap image	436 KB
pancakes.bmp.MD5	10/5/2025 12:53 PM	MD5 File	1 KB
Popsicle	4/13/2021 9:41 AM	Bitmap image	708 KB
Popsicle.bmp.MD5	10/5/2025 12:53 PM	MD5 File	1 KB
ReadMe	4/23/2021 2:10 AM	Text Document	1 KB
ReadMe.txt.MD5	10/5/2025 12:53 PM	MD5 File	1 KB

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

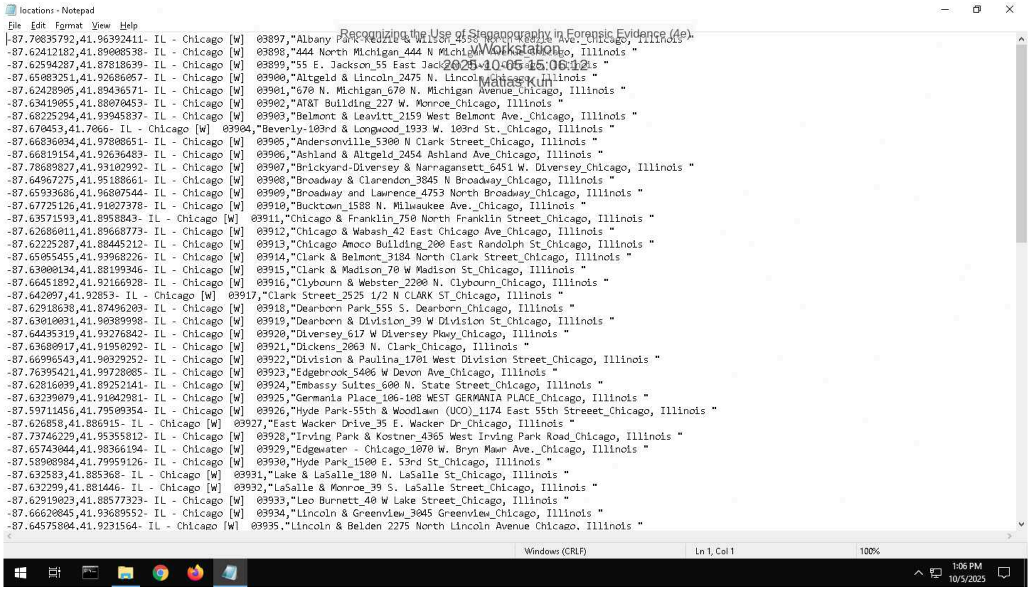


Part 3: Extract Hidden Data from Image Files

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 "
-87.73746229,41.95355812- IL - Chicago [W]  03928,"Irving Park & Kostner_4365 West Irving Park Road_Chicago, Illinois "
-87.65743044,41.98366194- IL - Chicago [W]  03929,"Edgewater - Chicago_1070 W. Bryn Mawr Ave._Chicago, Illinois "
-87.58908984,41.79959126- IL - Chicago [W]  03930,"Hyde Park_1500 E. 53rd St_Chicago, Illinois "
-87.632583,41.885368- IL - Chicago [W]  03931,"Lake & LaSalle_180 N. LaSalle St_Chicago, Illinois "
-87.632299,41.881446- IL - Chicago [W]  03932,"LaSalle & Monroe_39 S. LaSalle Street_Chicago, Illinois "
-87.62919023,41.88577323- IL - Chicago [W]  03933,"Leo Burnett_40 W Lake Street_Chicago, Illinois "
-87.66620845,41.93689552- IL - Chicago [W]  03934,"Lincoln & Greenview_3045 Greenview_Chicago, Illinois "
-87.64575804,41.9231564- IL - Chicago [W]  03935,"Lincoln & Belden_2275 North Lincoln Avenue_Chicago, Illinois "
```

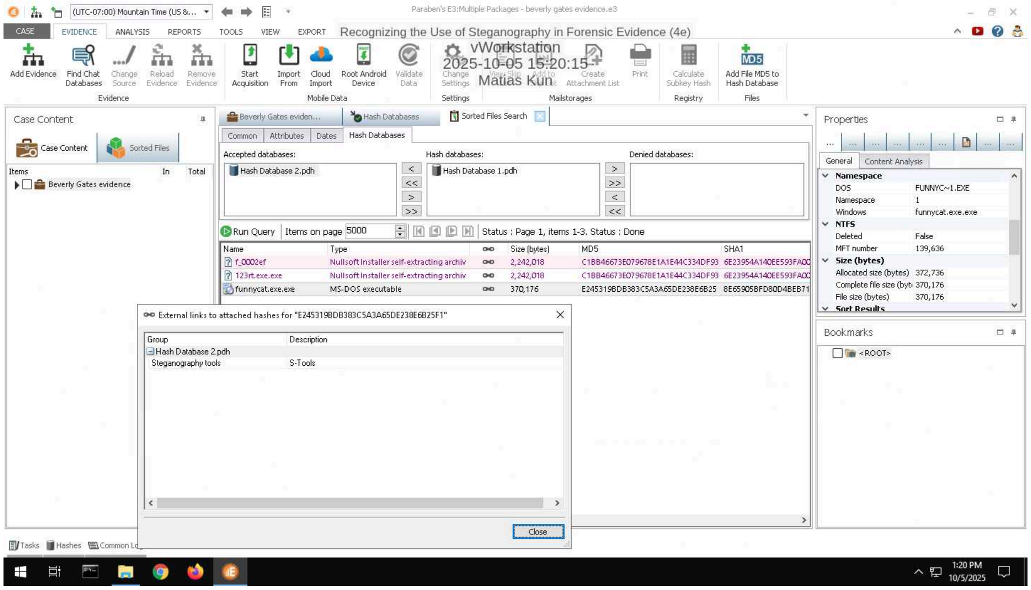
17. **Describe** the contents of the hidden file. How might it be relevant to the current investigation?

The contents of the hidden file reveal the addresses and coordinates of the locations where the suspect is traveling. This could be used as evidence against the suspect if they were to lie about their whereabouts, the time they spent there, and the exact locations mentioned in the evidence.

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**.



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

Recognizing the Use of Steganography in Forensic Evidence (4e)
vWorkstation
2025-10-05 15:20:15
Matias Kun

Sorted Files Search — Hash Databases

Accepted databases: Hash Database 2.pdh
Hash databases: Hash Database 1.pdh
Denied databases:

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

Name	Type	Size (bytes)	MD5	SHA1
f_0002ef	Nullsoft Installer self-extracting archiv	2,242,018	C1BB46673E079678E1A1E44C334DF93	6E23954A140EE593FA0C
123rt.exe.exe	Nullsoft Installer self-extracting archiv	2,242,018	C1BB46673E079678E1A1E44C334DF93	6E23954A140EE593FA0C
funnycat.exe.exe	MS-DOS executable	370,176	E245319BDB383C5A3A65DE238E6B25	8E65905BFD80D4BEB71

External links to attached hashes for "E245319BDB383C5A3A65DE238E6B25F1"

Group	Description
Hash Database 2.pdh	
Steganography tools	S-Tools

Properties — General

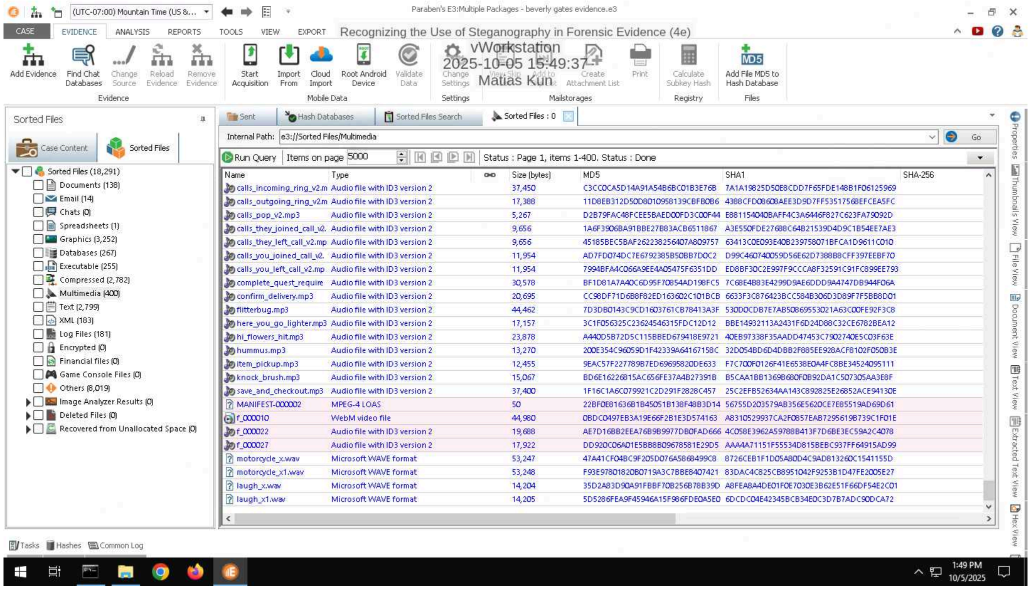
Namespace	
DOS	FUNNYC~1.EXE
Namespace	1
Windows	funnycat.exe.exe
NTFS	
Deleted	False
MFT number	139,636
Size (bytes)	
Allocated size (bytes)	372,736
Complete file size (byt	370,176
File size (bytes)	370,176
Sort Results	

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**.



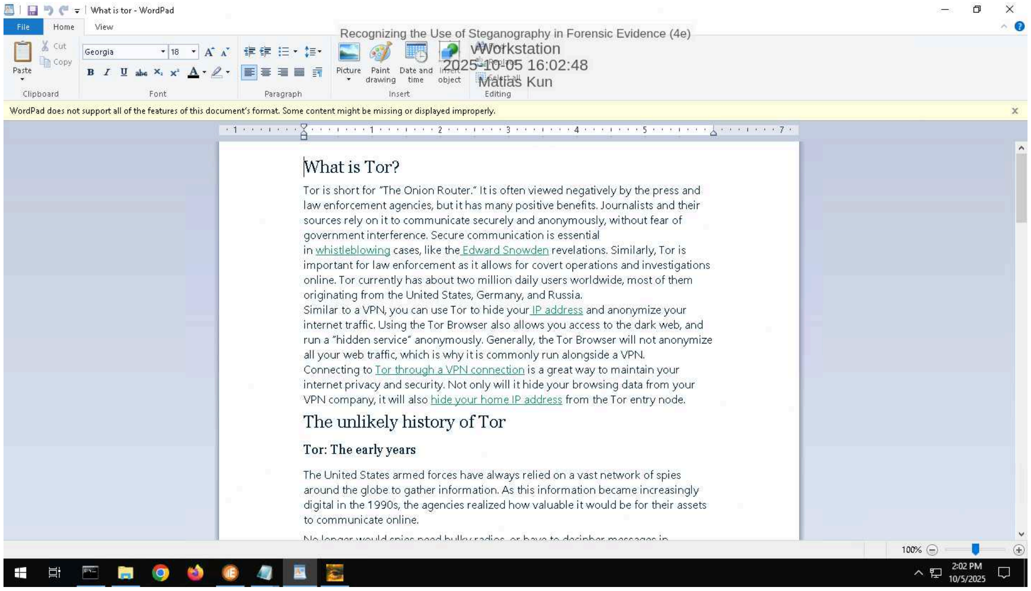
Internal Path: e3://Sorted Files/Multimedia

Status : Page 1, items 1-400. Status : Done

Name	Type		Size (bytes)	MD5	SHA1	SHA-256
calls_incoming_ring_v2.m	Audio file with ID3 version 2		37,450	C3CC0CA5D14A91A54B6BC01B3E76B	7A1A19825D50E8CDD7F65FDE148B1F06125969	
calls_outgoing_ring_v2.m	Audio file with ID3 version 2		17,388	11D8EB312D50D8010958139CBFB0B6	4388CFD08608AEE3D9D7FF53517568EFCEA5FC	
calls_pop_v2.mp3	Audio file with ID3 version 2		5,267	D2B79FAC48FCEE5BAED00FD3C00F44	E881154040BAFF4C3A6446F827C623FA79092D	
calls_they_joined_call_v2.	Audio file with ID3 version 2		9,656	1A6F3906BA91BBE27B83ACB6511867	A3E550FDE27688C64B21539D4D9C1B54EE7AE3	
calls_they_left_call_v2.mp	Audio file with ID3 version 2		9,656	45185BEC5BAF262238256407A809757	63413C0E093E40B239758071BFCA1D9611C010	
calls_you_joined_call_v2.	Audio file with ID3 version 2		11,954	AD7FD074DC7E6792385B50BB7D0C2	D99C460740059D56E62D7388B8CFF397EEBF70	
calls_you_left_call_v2.mp	Audio file with ID3 version 2		11,954	7994BFA4C066A9EE4A05475F6351DD	ED8BF30C2E997F9CCCA8F32591C91FC899EE793	
complete_quest_require	Audio file with ID3 version 2		30,578	BF1D81A7A40C6D95F70854AD198FC5	7C68E4B83E4299D9AE6DDD9A4747DB944F06A	
confirm_delivery.mp3	Audio file with ID3 version 2		20,695	CC98DF71D6B8F82ED163602C101BCB	6633F3C876423BCC584B306D3D89F7F5BB8D01	
flitterbug.mp3	Audio file with ID3 version 2		44,462	7D3DB0143C9CD1603761CB78413A3F	530D0CDB7E7AB50869553021A63C00FE92F3C8	
here_you_go_lighter.mp3	Audio file with ID3 version 2		17,157	3C1F056325C23624546315FDC12D12	BBE14932113A2431F6D24D88C32CE6782BEA12	
hi_flowers_hit.mp3	Audio file with ID3 version 2		23,878	A440D5B72D5C115BBED679418E9721	40EB97338F35AADD47453C7902740E5C03F63E	
hummus.mp3	Audio file with ID3 version 2		13,270	200E354C96059D1F42339A64167158C	32D054BD6D4DBB2F885EE928ACF8102F050B3E	
item_pickup.mp3	Audio file with ID3 version 2		12,455	9EAC57F227789B7ED69695820DE633	F7C700F0126F41E6538E0A4FC8BE34524095111	
knock_brush.mp3	Audio file with ID3 version 2		15,067	BD6E16226815AC656FE37A4B27391B	B5CAA1BB1369B680F0B92DA1C507305AA3E8F	
save_and_checkout.mp3	Audio file with ID3 version 2		37,400	1F16C1A6C079921C2D291F2828C457	25C2EFB52634AA143C892825E26852ACE94130E	
MANIFEST-000002	MPEG-4 LOAS		50	22BF0E81636B1B45051B138F48B3D14	56755D203579AB356E5620CE7E85519AD69D61	
f_000010	WebM video file		44,980	0BDC0497EB3A19E66F2B1E3D574163	A8310529937CA2F0857EAB7295619B739C1F01E	
f_000022	Audio file with ID3 version 2		19,688	AE7D16BB2EEA76B9B9977DB0FAD666	4C058E3962A59788B413F7D6BE3EC59A2C4078	
f_000027	Audio file with ID3 version 2		17,922	DD920C06A01E5BB8B09678581E29D5	AAA4A71151F55534D815BEBC937FF64915AD99	
motorcycle_x.wav	Microsoft WAVE format		53,247	47A41CF04BC9F205D076A5868499C8	8726CEB1F1D05A80D4C9AD813260C1541155D	
motorcycle_x1.wav	Microsoft WAVE format		53,248	F93E97801820B0719A3C7BBE8407421	83DAC4C825CB8951042F9253B1D47FE2005E27	
laugh_x.wav	Microsoft WAVE format		14,204	35D2A83D90A91FBBF70B256B78B39D	A8FEA8A4DE01F0E7030E3B62E51F66DF54E2C01	
laugh_x1.wav	Microsoft WAVE format		14,205	5D5286FEA9F45946A15F986FDE0A5E0	6DCDC04E42345BCB34E0C3D7B7ADC90DCA72	

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.

Similar to a VPN, you can use Tor to hide your IP address and anonymize your internet traffic. Using the Tor Browser also allows you access to the dark web, and run a "hidden service" anonymously. Generally, the Tor Browser will not anonymize all your web traffic, which is why it is commonly run alongside a VPN.

Connecting to Tor through a VPN connection is a great way to maintain your internet privacy and security. Not only will it hide your browsing data from your VPN company, it will also hide your home IP address from the Tor entry node.

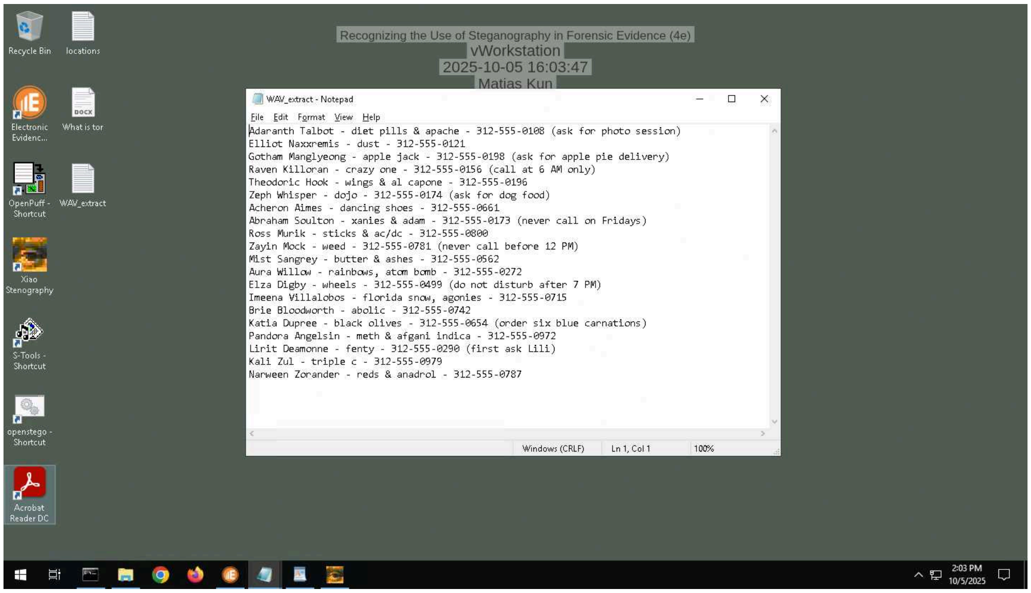
The unlikely history of Tor

Tor: The early years

The United States armed forces have always relied on a vast network of spies around the globe to gather information. As this information became increasingly digital in the 1990s, the agencies realized how valuable it would be for their assets to communicate online.

No longer would spies need bulky radios, or have to decipher messages in

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 of the hidden files reveal names, phone numbers, and references to black markets, which potentially help lead investigators to find probable cause for a crime.

Section 3: Challenge and Analysis

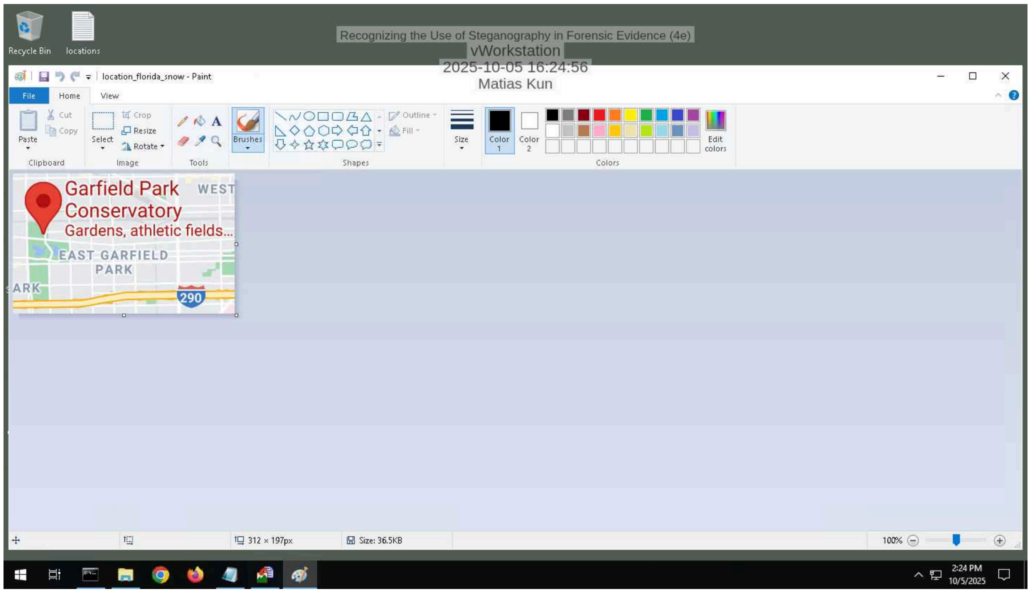
Part 1: Detect More Hidden Data

Record the names of the files that contain concealed data.

chicago.bmpchicago1.bmp

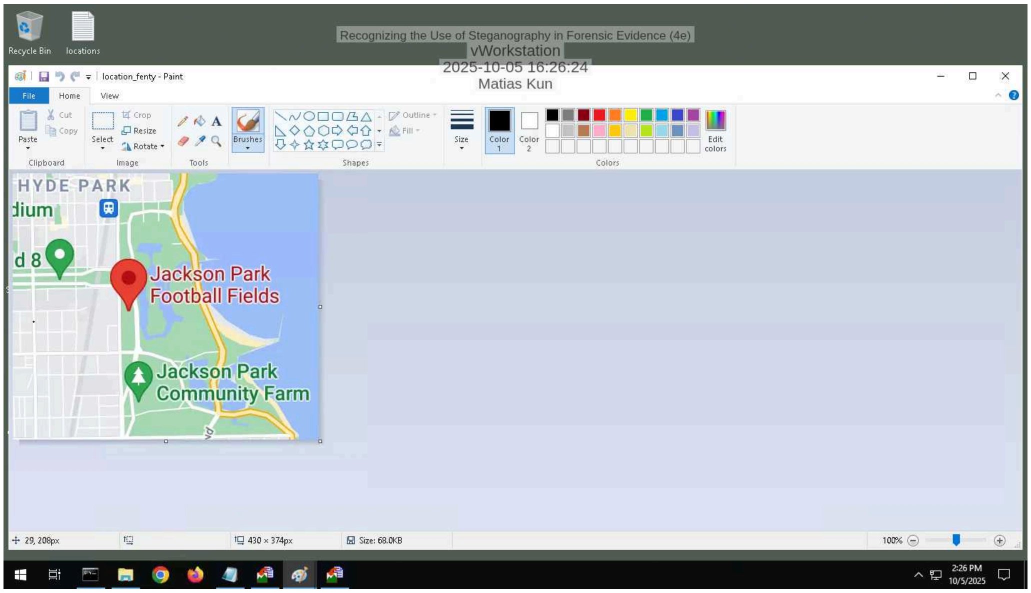
Part 2: Extract More Hidden Data

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



Recognizing the Use of Steganography in Forensic Evidence (4e)
vWorkstation
2025-10-05 16:24:56
Matias Kun

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



Recognizing the Use of Steganography in Forensic Evidence (4e)
vWorkstation
2025-10-05 16:26:24
Matias Kun

location_fenty - Paint

29, 208px
430 × 374px
Size: 68.0KB
100%

2:26 PM
10/5/2025