

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

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

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

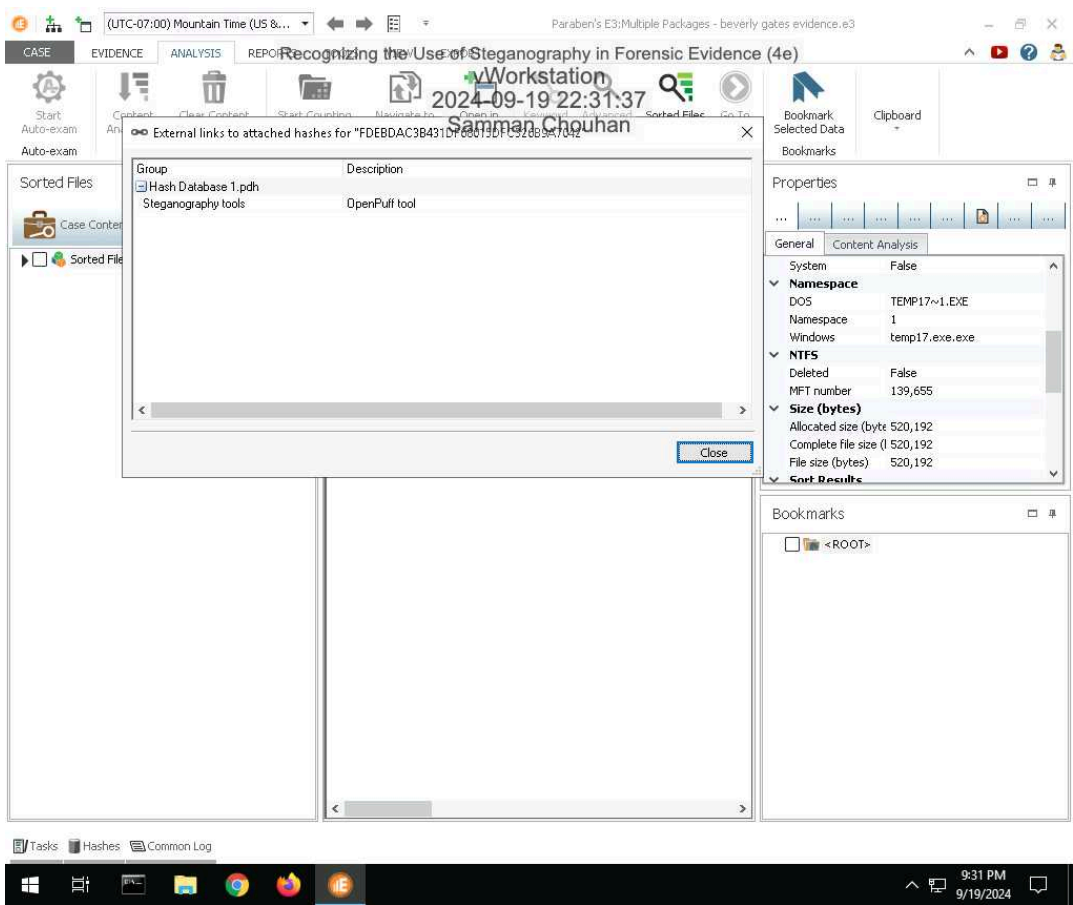
Time on Task:	Progress:
3 hours, 50 minutes	100%

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.

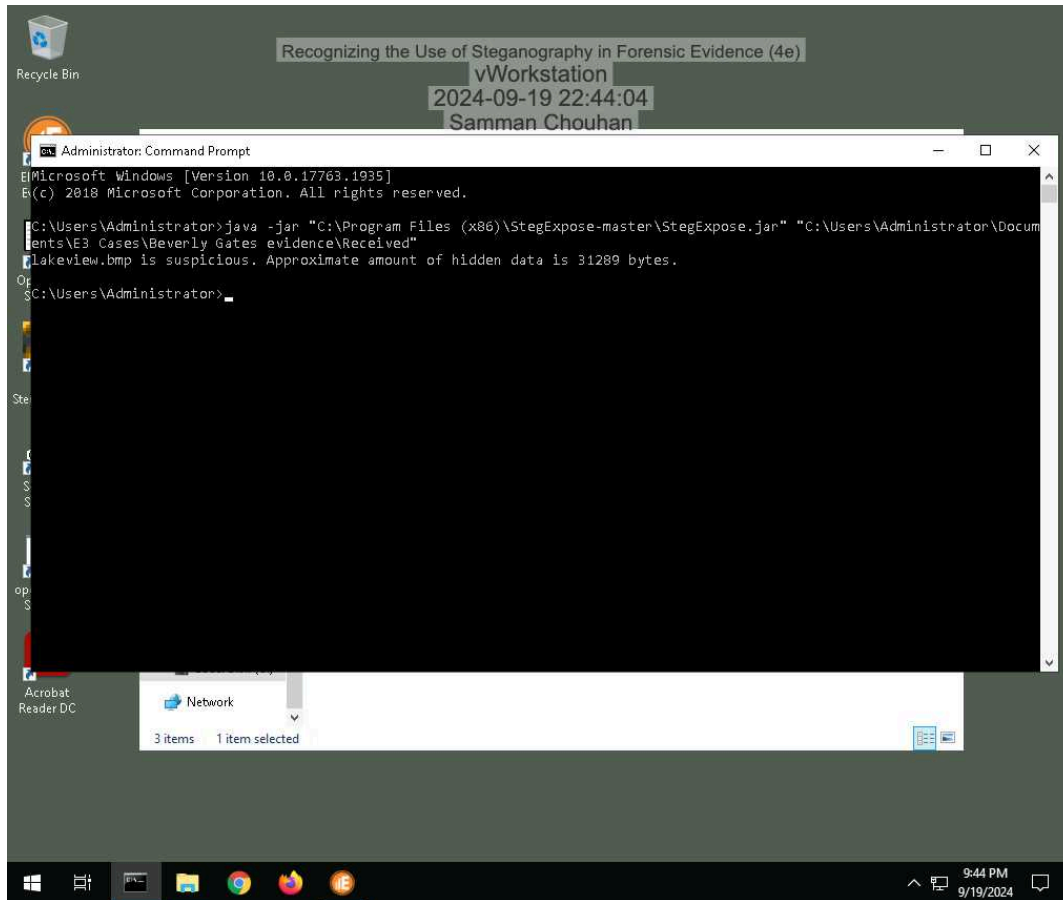


Part 2: Detect Hidden Data in Image Files

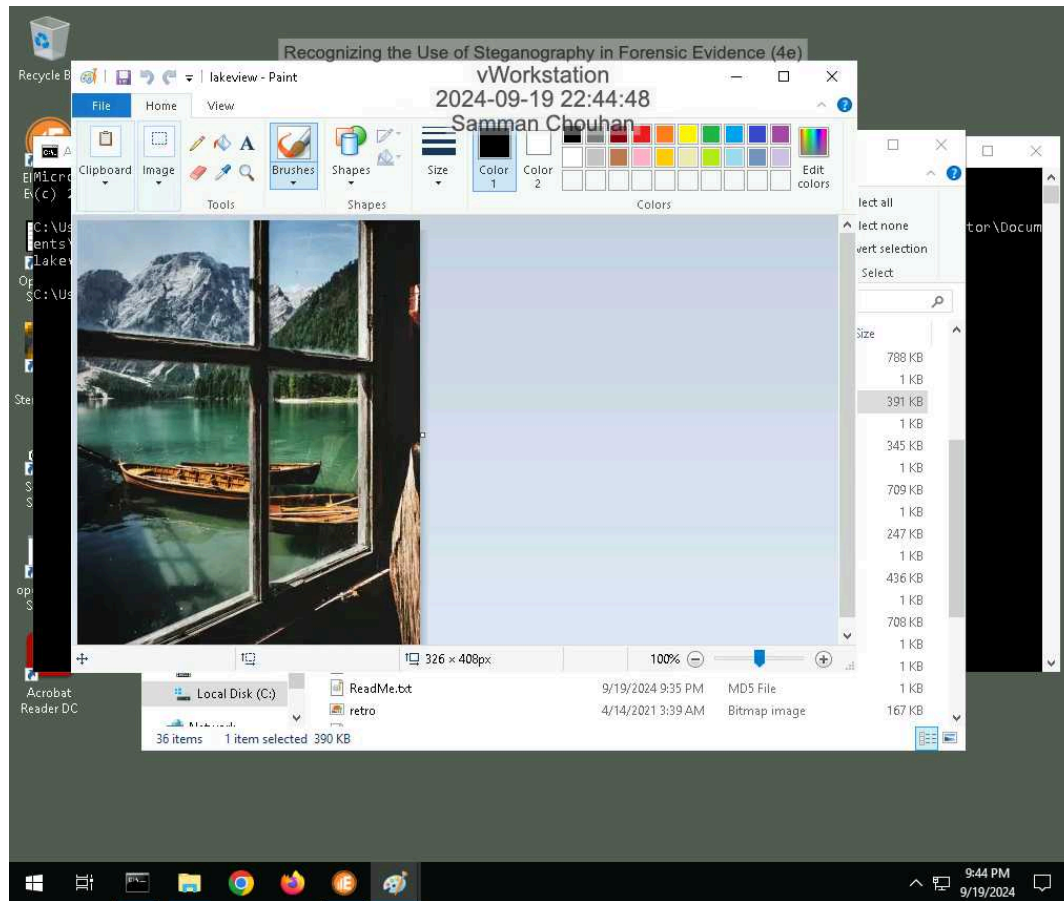
Recognizing the Use of Steganography in Forensic Evidence (4e)

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

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



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

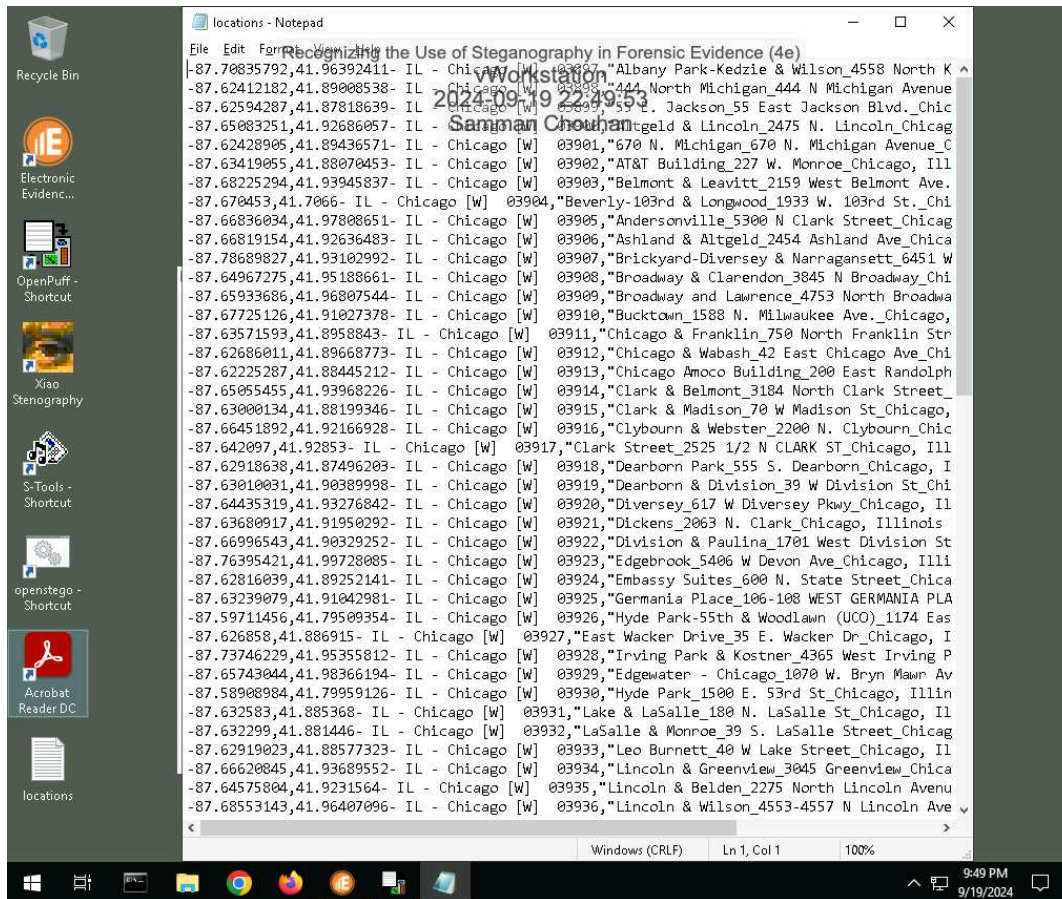


Part 3: Extract Hidden Data from Image Files

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.



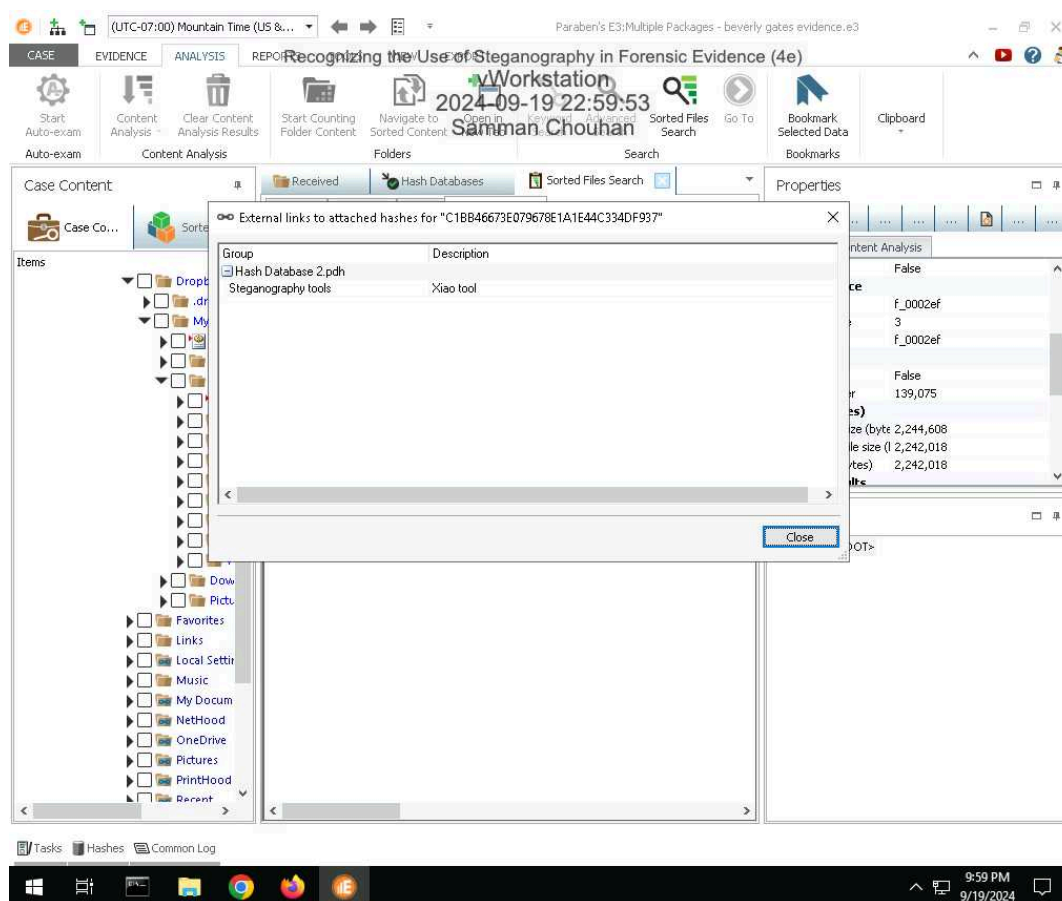
17. Describe the contents of the hidden file. How might it be relevant to the current investigation?

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 investigation

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

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

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

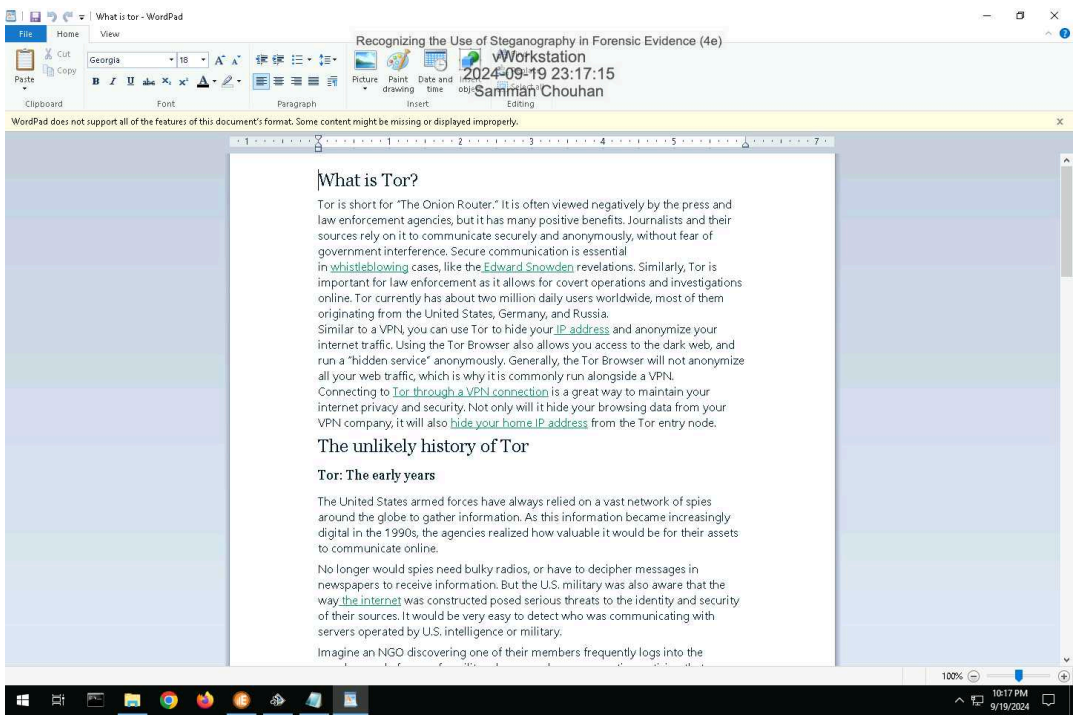
7. Make a screen capture showing the WAV file sizes and hash values in E3.

The screenshot displays the Paraben's E3 Multiple Packages interface. The main window shows a list of files under the 'Multimedia (400)' category. The list includes various audio files (e.g., b1.mp3, b2.mp3, b3.mp3) and video files (e.g., b1.avi, b2.avi, b3.avi). The columns shown are Name, Type, Size (Bytes), MD5, and SHA1. The status bar at the bottom indicates 'Page 1, Items 1-400, Status: Done'.

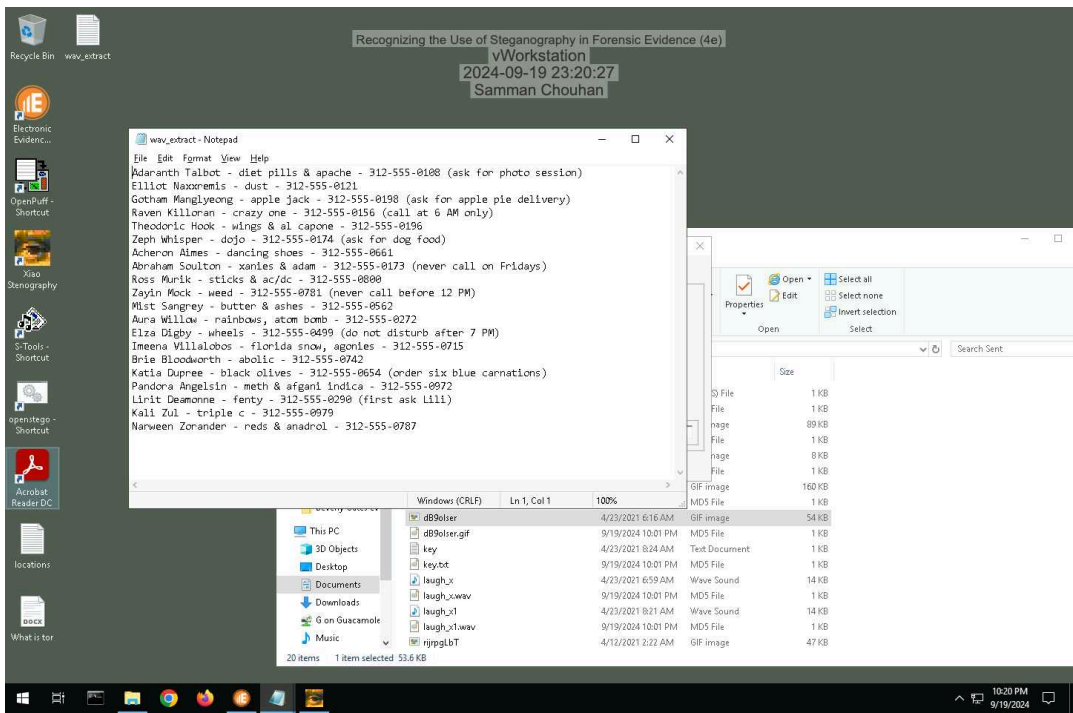
Name	Type	Size (Bytes)	MD5	SHA1
b1.mp3	Audio file with ID3 version 2	13,693	74D2956CE9D36E74A0F0D69049576C	26E91DE390CA839B966700063215E3BE12F91
b2.mp3	Audio file with ID3 version 2	36,937	93ABF8C9F57580273AFEB00000380	57FD58A074292ED024664AF2F4E3220646230
b3.mp3	Audio file with ID3 version 2	16,093	D8184AC32F54226AEECE5A86C0B52	97C0B844D0AD4C10A96957354812192A0AD13C
b4.mp3	Audio file with ID3 version 2	9,656	5C2E5A717374AEFF178D9CA8BEE8F	CEFD24FBC4183C8E2BCF3C3E567A0267524BA
b5.mp3	Audio file with ID3 version 2	8,611	DE3AAAE8B82071F1A0F0D07FCA4A8	1D267FCE7E0E3768A452C0A5442C39C0C39
b6.mp3	Audio file with ID3 version 2	37,450	C3C0CA5D14A05A4848C0B3E1E0B	7A3A180255C0B8C0D7F669F0E4B01F001258D
b7.mp3	Audio file with ID3 version 2	17,388	11D8E8312D50D0709913KCFB0B6	4389CF00B2BAFEE3D9D7F5351558EFCFA5FC
b8.mp3	Audio file with ID3 version 2	5,267	D2B79FAC48CE5E8AED00F3C0DF44	681154042BAFAC3A64469237C623F7A020D
b9.mp3	Audio file with ID3 version 2	9,656	1A8F306BA91B8E27883ACB51186F	A3E550FDE27886C6B21539D0C1B54EE7AE3
b10.mp3	Audio file with ID3 version 2	9,656	45185BEC5BAF26238256407A0D9757	63413C0E93E40B2397580718FCA1D9611C01D
b11.mp3	Audio file with ID3 version 2	11,954	AD7F007AD7CE6792385850B87D0C2	D99C4607400540056E62D7388B8CF397EE8F7D
b12.mp3	Audio file with ID3 version 2	11,954	7994BFA4C066A9E4A05475F6351D0	ED08F30C2E997F9CC0A873591C91F099E793
b13.mp3	Audio file with ID3 version 2	30,578	BF1D81A7A40C6D957705A4D198F5C	7C6B48B3E429909A6E0DD9A4747D6944706A
b14.mp3	Audio file with ID3 version 2	20,695	C8B0F71D40B8F8E161640C12D18C8	603F3C7A4238C4C98403D03A9F1F5B80021
b15.mp3	Audio file with ID3 version 2	44,463	7D3D80143C9CD16D2767C878A13AF3	53D0DC0B7E8A5086953021A63C0DFE9073C8
b16.mp3	Audio file with ID3 version 2	17,157	3C1F056325C2362454615FDC12D12	88E1493213A2431F6D40B8C32CE67828EA12
b17.mp3	Audio file with ID3 version 2	23,878	A440D5B72D5C1158B8D679418E9721	40E897338F35A4D047453C70027A0E5C03F63E
b18.mp3	Audio file with ID3 version 2	13,270	200E354C96D59D1F42339A64167159C	32D0548D6D40BB2F885E928ACF8102F050E3E
b19.mp3	Audio file with ID3 version 2	12,455	9EAC57F22778987ED69895820C633	F7C700F0126F41E6538E04F4C8E3452A095111
b20.mp3	Audio file with ID3 version 2	15,067	BD6E16228815AC65F637A4B27391B	85CAA1B81369B80F0B92DA1C507305A3B8F
b21.mp3	Audio file with ID3 version 2	37,400	1F16C1A6C079921C2D29F3828C857	25CE6F82634AA143C86825E26832AC94130E
b22.mp3	Audio file with ID3 version 2	50	228F8B1638B184051B136F4881D14	5675D3A2D37A8359E85C27B85194D0B61
b23.mp3	Audio file with ID3 version 2	44,980	0B0C0807E3A17866F381E3D57A163	4E310529037CA785B1A87056198739C140E
b24.mp3	Audio file with ID3 version 2	19,080	AETD16BB2EAE7469899770B0FAD666	4C05E1362A59788B413F7D0B83E5943CA70
b25.mp3	Audio file with ID3 version 2	17,922	D0920C0A0E5E8B80D967851E2305	AA4A7115F5534D81B8EBC79F744915AD99
b26.mp3	Audio file with ID3 version 2	53,247	47A71CF04BC9F3D5D076A5840499C8	8726CEB1F1D05A00C4C9AD813260C1541155D
b27.mp3	Audio file with ID3 version 2	53,240	F91E978D1820E719A3C78B8E4024741	83D4C4C825C8B951042F9253181D47FE200E27
b28.mp3	Audio file with ID3 version 2	14,204	35D1A81010A91F8BF705B10B10930	A0FEA8A4D01F0E1D3E3B6E51F66D54E2C01
b29.mp3	Audio file with ID3 version 2	14,205	5D52B6E6A0F45146A15F869FDE0A5E0	8DCC0B42345B1C34E0C3D787AD7C00CA72

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.



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

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

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

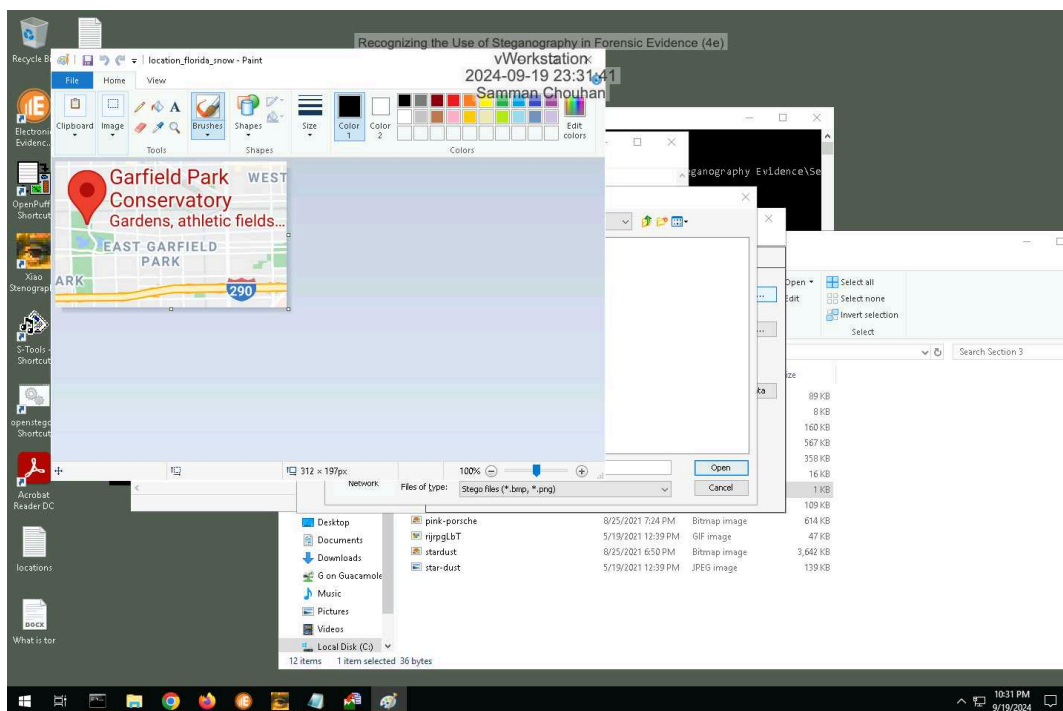
Part 1: Detect More Hidden Data

Record the names of the files that contain concealed data.

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

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.

