

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

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

Student:

Jose Cruz

Email:

jose.cruz2@udc.edu

Time on Task:

18 hours, 8 minutes

Progress:

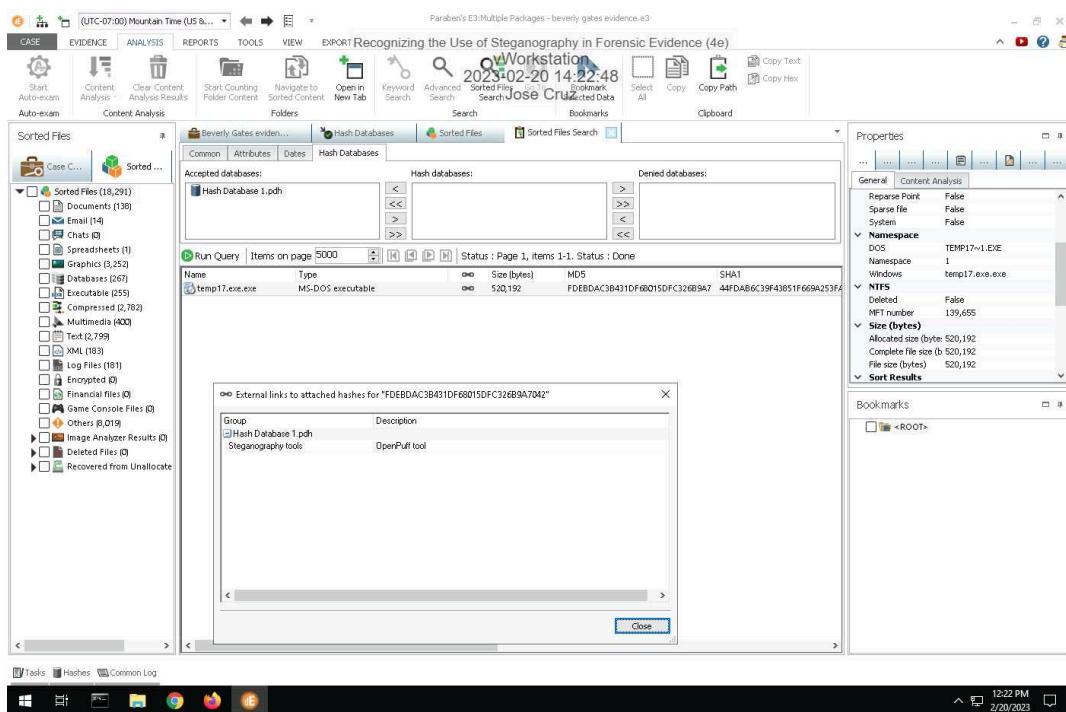
100%

Report Generated: Saturday, February 25, 2023 at 8:37 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.

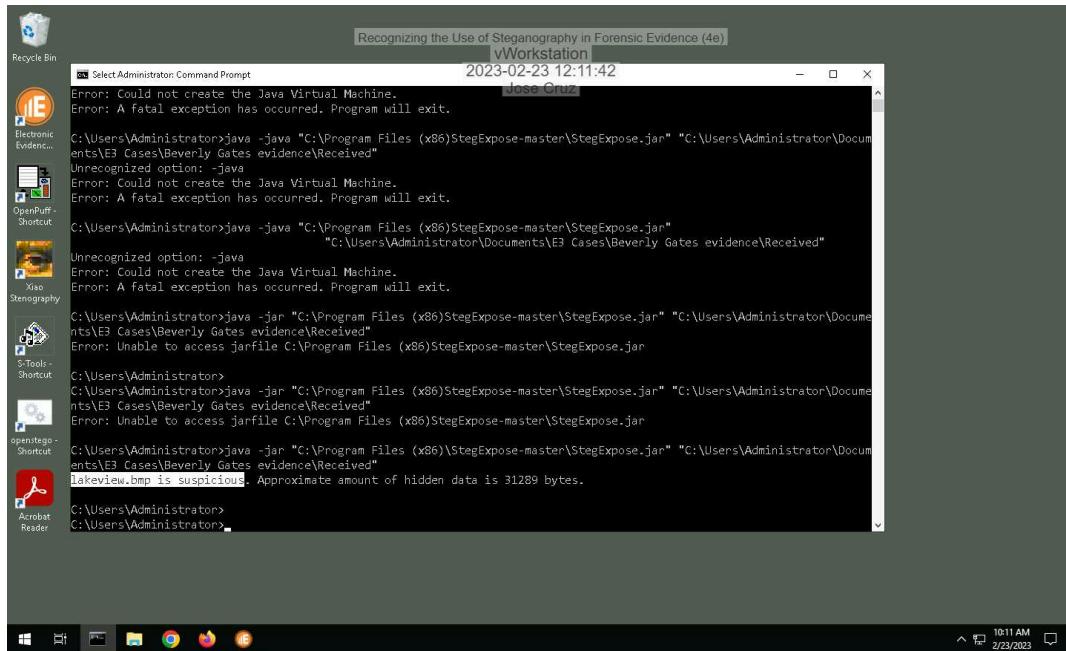


Part 2: Detect Hidden Data in Image Files

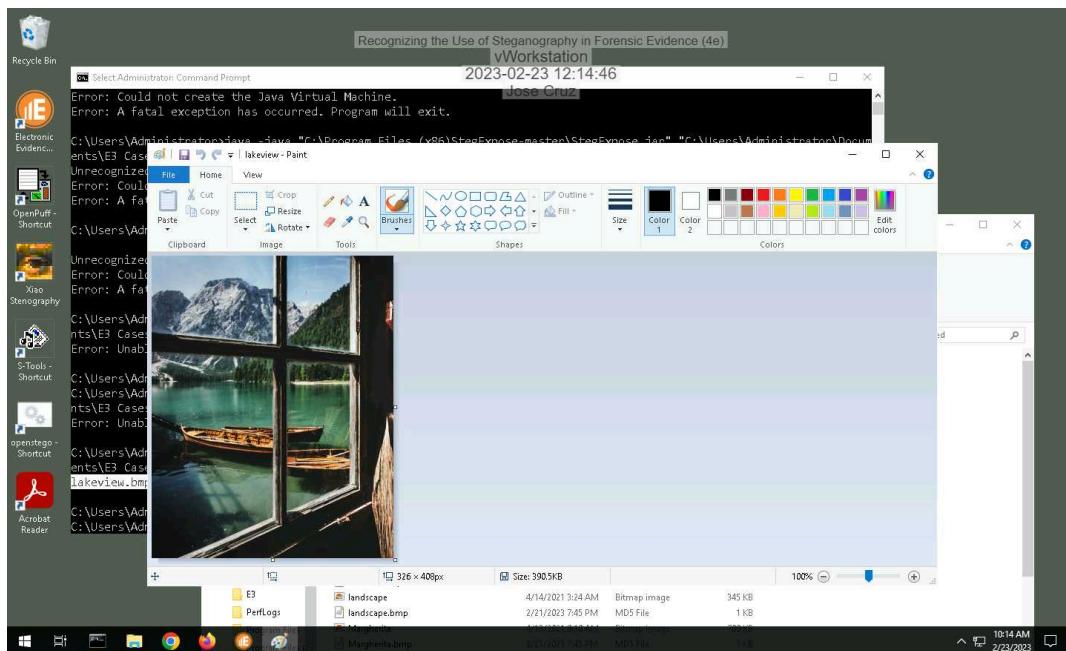
Recognizing the Use of Steganography in Forensic Evidence (4e)

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.



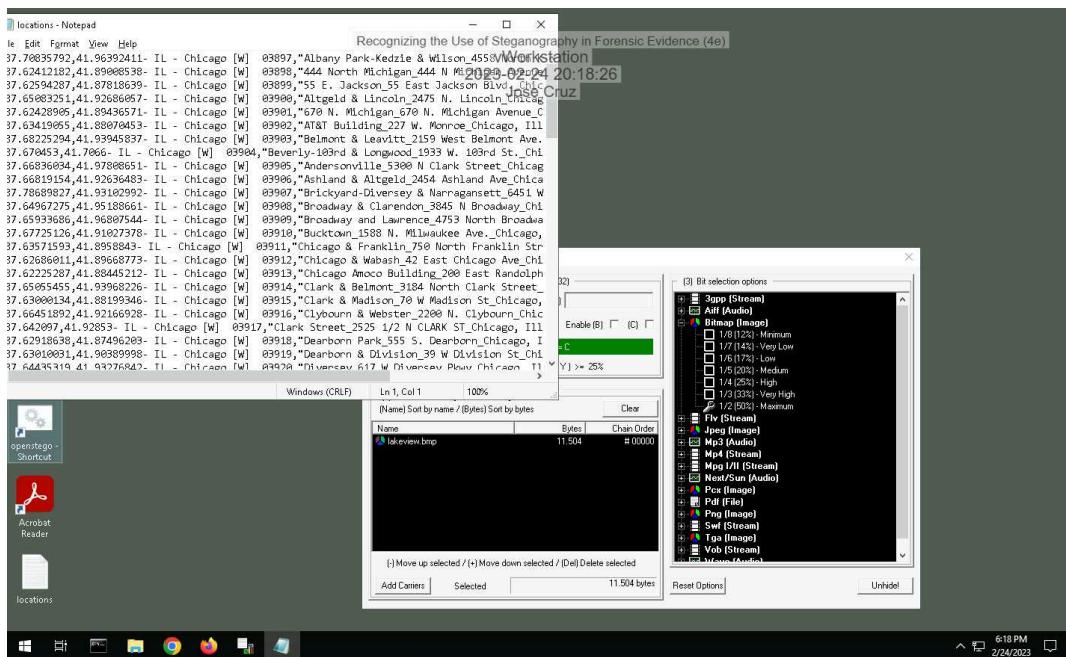
Part 3: Extract Hidden Data from Image Files

2. Record the passphrase saved in the ReadMe file.

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

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

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



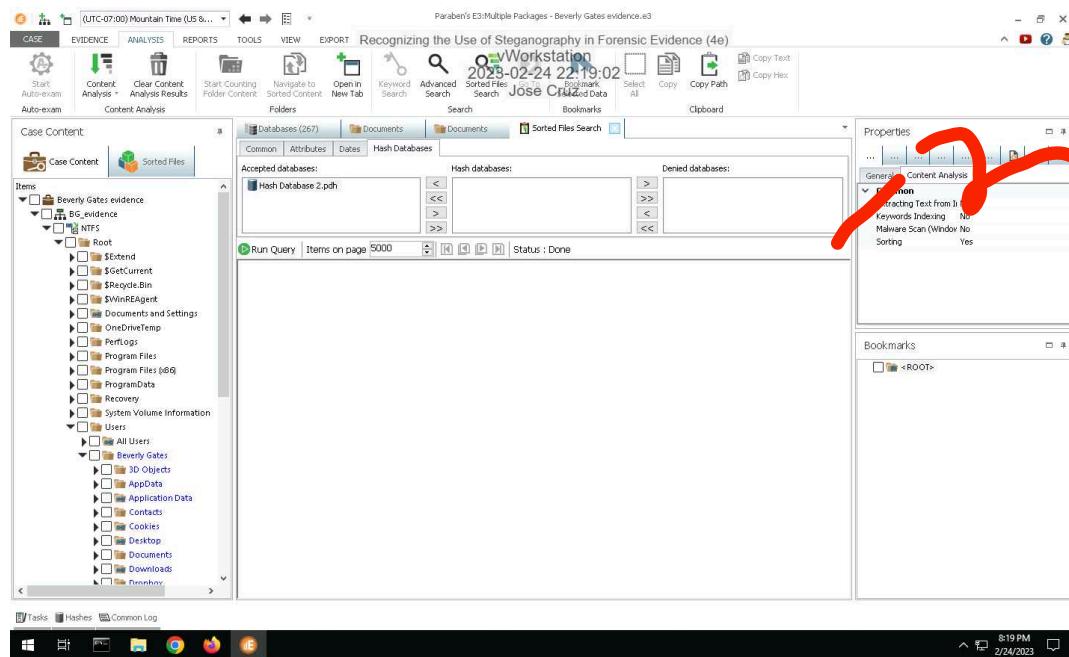
17. Describe the contents of the hidden file. How might it be relevant to the current investigation?

In the text file there is many addresses and random numbers, it can be addresses to Beverly corrupted friends. This information can be relevant to the contacts on her emails. We can try to connect them to see if they match.

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.

The image file displayed in the command prompt is "dB9olser.gif"

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 shows the Paraben's E3:Multiple Packages software interface. The main window displays a list of multimedia files under the 'Multimedia (400)' tab. The columns include Name, Type, Size (bytes), and MD5. The list includes various audio files like 'been_tree.mp3', 'calls_alert_v2.mp3', and 'motorcycle_low.wav'. The 'Properties' panel on the right shows common file details such as extracting text from file (No), keywords indexing (No), malware scan (Windows No), and sorting (Yes). The status bar at the bottom indicates the date and time as 2/24/2023 8:59 PM.

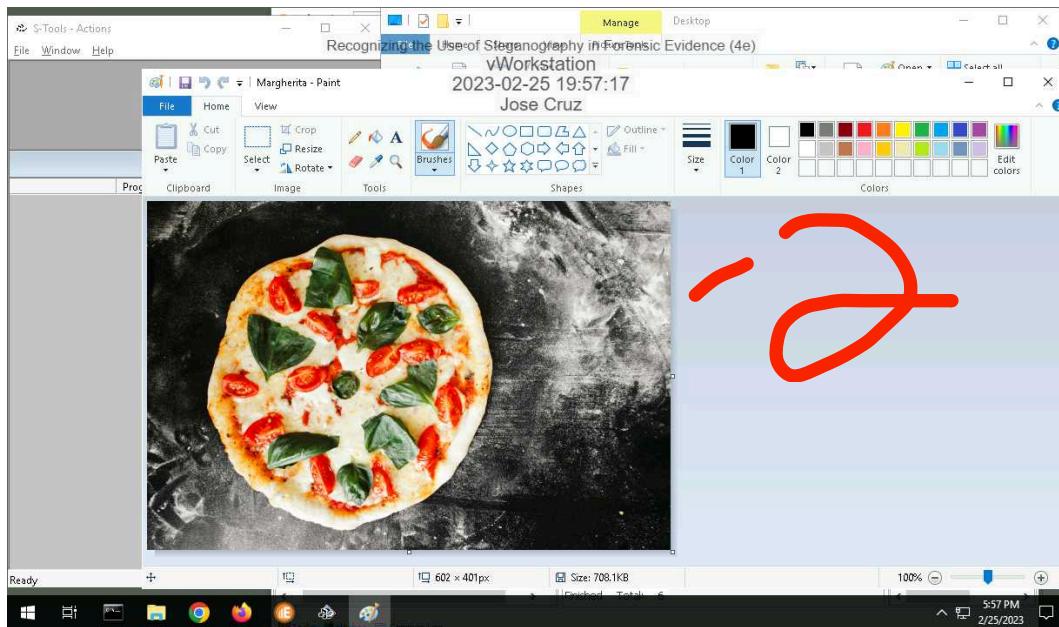
Name	Type	Size (bytes)	MD5
been_tree.mp3	Audio file with ID3 version 2	16,093	DB184AC372F54226AECCE5AB6C3
calls_alert_v2.mp3	Audio file with ID3 version 2	9,656	S2E5A57173C74AEF178D9C9A8BE
calls_confirmation_v2.mp3	Audio file with ID3 version 2	8,611	DE3AAE8B20B71F1A2D9F04DF7C
calls_incoming_ring_v2.m	Audio file with ID3 version 2	37,450	C3CC0CA5D1A4A91A54B6B01B3E
calls_outgoing_ring_v2.m	Audio file with ID3 version 2	17,388	11D8EB312D508070958139CBFE
calls_pop_v2.mp3	Audio file with ID3 version 2	5,267	D2B79FA1C4BFCEEEBAED0D9F3CD
calls_they_joined_call.v0	Audio file with ID3 version 2	9,656	1A6F310GBA91BEE27B83AC6511
calls_they_left_call_v2.mp3	Audio file with ID3 version 2	9,656	45185BEC5BAF26228525407A80
calls_you_joined_call.v0	Audio file with ID3 version 2	11,954	AD7FD074DC7E6792365B50B7D
calls_you_left_call_v2.mp3	Audio file with ID3 version 2	11,954	7994BF4AC066A9E4A05475F65
complete_quest_require	Audio file with ID3 version 2	30,578	BF1D91A7AA0C6D595F10854D11K
confirm_delivery.mp3	Audio file with ID3 version 2	20,695	CC960F71D688P82ED163602C10
filterbug.mp3	Audio file with ID3 version 2	44,462	7D3D80143C9CD1603761CB7841
here_you_go_lighter.mp3	Audio file with ID3 version 2	17,157	3C1F06325C2362456315FC121
hi_flowers_hi.mp3	Audio file with ID3 version 2	23,818	A440D5B72D5C115BBED679418E
humusus.mp3	Audio file with ID3 version 2	13,270	20E35AC9605D0142339A64167
item_pickup.mp3	Audio file with ID3 version 2	12,455	9EAC5TF22789B7E6D69695020E
knock_brush.mp3	Audio file with ID3 version 2	15,067	BDE616226815AC656F37A4B273
save_and_checkout.mp3	Audio file with ID3 version 2	37,400	1F16C1AC079921C2D291F2038C
MANIFEST-000001	MPEG-4 LSAS	50	22BFD6B1636B1B45D1B130F46B
f_000010	WebM video file	44,960	0BDCC0497EB3A19E66F2B1E3D574
f_000022	Audio file with ID3 version 2	19,688	AETD16B2E2EA76B9B9977D0BFA
f_000027	Audio file with ID3 version 2	17,922	DD920CC60A01E5B88B09678581E2
motorcycle_low.wav	Microsoft WAVE format	53,247	474A1CF04B-C9F2D5D076A5989A5
motorcycle_x1.wav	Microsoft WAVE format	53,246	F91E97801820B0179A3CTBBE840
laugh_x.wav	Microsoft WAVE format	14,204	35D2481D0A9A1FBFB70B256B781
laugh_x1.wav	Microsoft WAVE format	14,205	5D5286FEA9F45946A15F96FDEQ

Part 3: Extract Hidden Data from Image and Audio Files

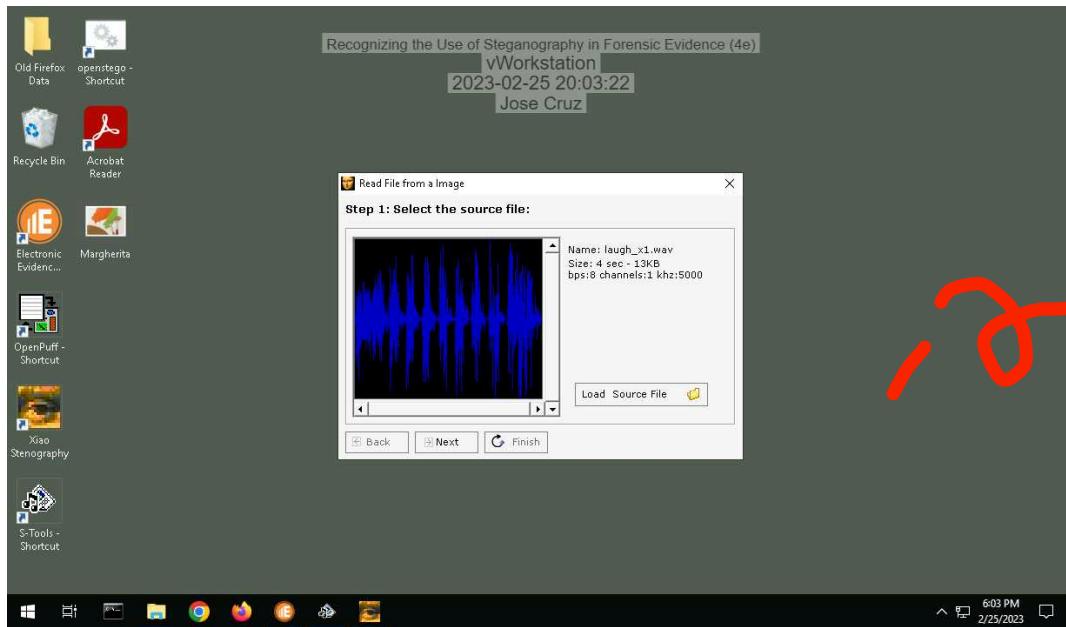
Recognizing the Use of Steganography in Forensic Evidence (4e)

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

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?

Showing so much hidden information using multiple software's, details displaying bit by bit to give more suspicious actions by Beverly.

Section 3: Challenge and Analysis

Part 1: Detect More Hidden Data

Record the names of the files that contain concealed data.

8cEbednRi

8cxn5XK9i

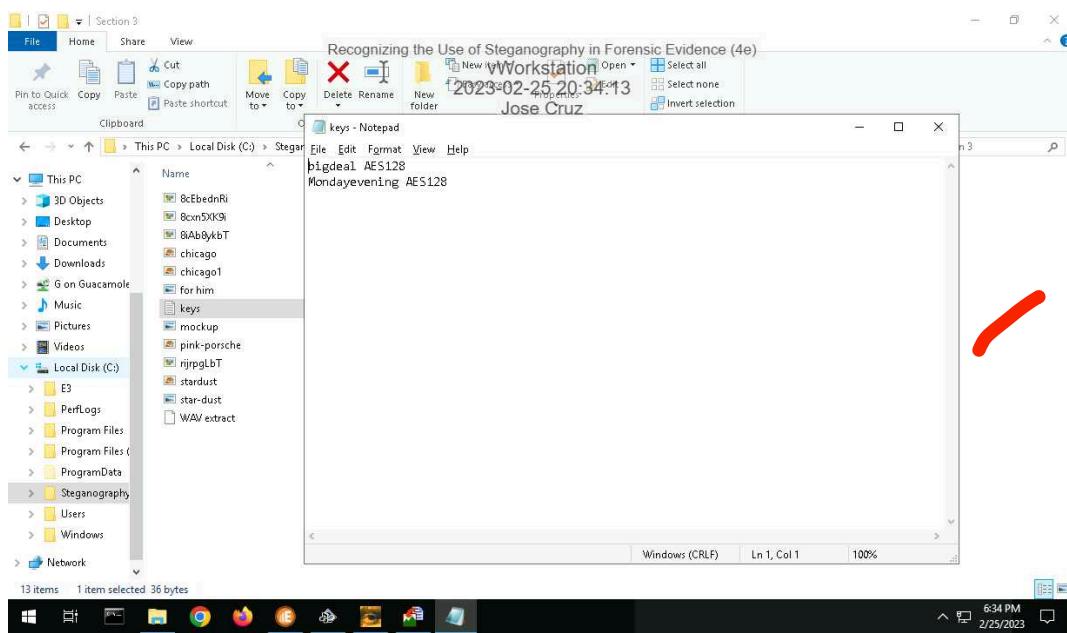
-2

8iAb8ykbT

rijrpgLbT

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.

