DIGITAL & MULTIMEDIA EVIDENCE EXAMINATION REPORT

SUBMITTING AGENCY: San Francisco Police Department
LABORATORY NUMBER: xxxxxx
EXAMINATION REQUESTED BY: Sergeant xxxx
VICTIM OR SUSPECT: UNKNOWN
CASE NUMBER: xx-xxxx
LABORATORY CLASSIFICATION: Digital & Multimedia Evidence
DATE OF REPORT: [date]
OFFENSE: MISC.

EVIDENCE SUBMITTED:

Eyewitnesses saw a young man tossing a San Francisco garter snake (an endangered species) at a young boy. A bag containing a laptop computer was dropped by the attacker when he escaped from the scene of the assault. Law enforcement officers confiscated the laptop and checked it into the Crime Lab Evidence Room.

Item #1:
.VDI file
Forensic System/Software/Tools – Autopsy 4.18
System: Windows 10 home edition
Image converter software used: Virtual box/virtual media manager

REQUEST:

On [date], Sergeant xxxx of the San Francisco PD submitted a request for the forensic examination of a hard drive reportedly removed from a suspect's computer. Sergeant xxxx requested an examination of the hard drive for any images, videos, emails, chat logs, active/deleted/altered files, or any other files that would assist with her investigation.

I downloaded VDI file(11GB) from link and using virtual media manager software to convert VHD file and run through Autopsy 4.18 to analyze.

Windows 10 home was found to be installed on image file. The install date was recorded as "03/01/2022 22:22:16 AM PST" and user account name was suspect.

No logon times or logon counts had been recorded for the administrator or guest account. The guest account had been disabled.
I performed a search using the following keywords (not case sensitive):

- Snake
- mystery-mc@protonmail.com
- petcatcher-mc@protonmail.com

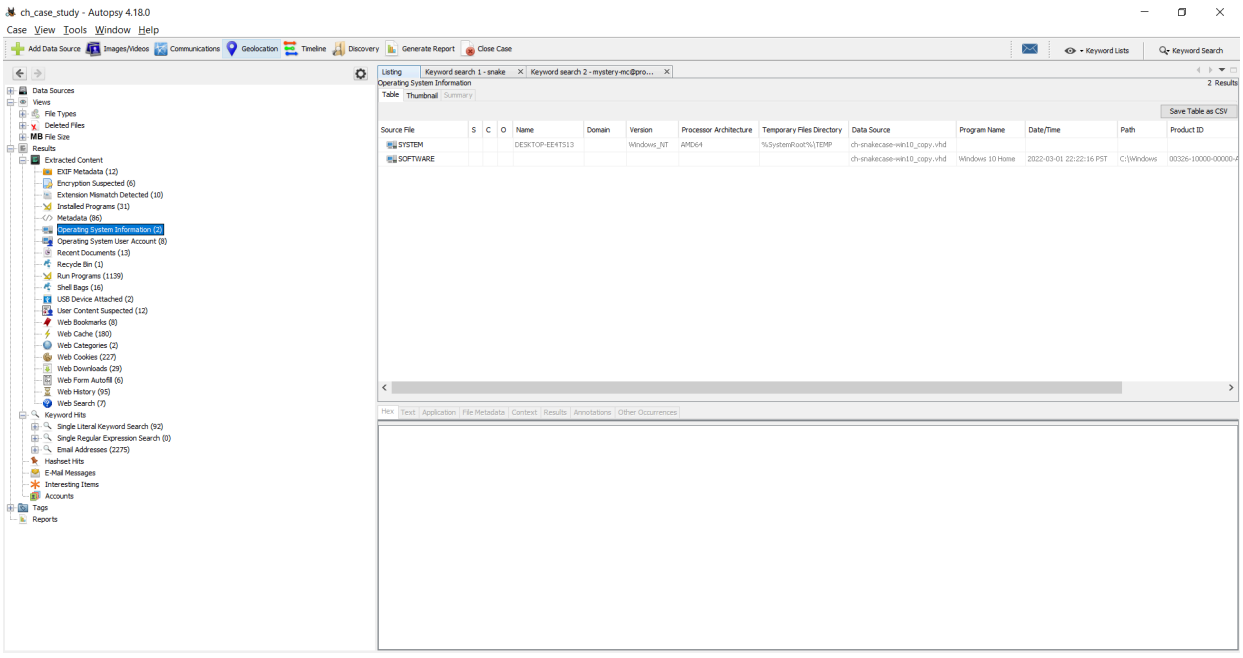
The various document and file category tabs, as well as the results of the above word searches, were reviewed to fulfill the service request. The following items of interest were located during the course of this examination:

- Exif meta data/12
- Recent document/13
- Recycle bin/1
- Web bookmarks/8
- Web downloads/29
- Web history/95

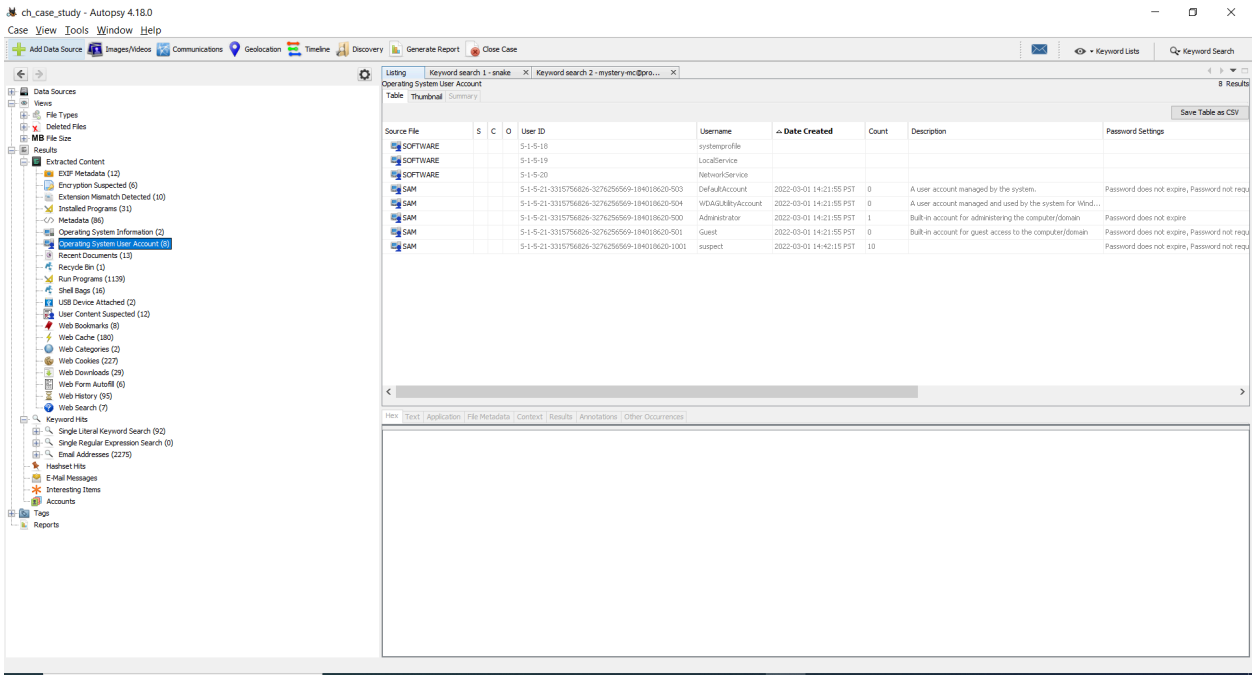
Contraband snake assault - Calvin case forensic examines

https://docs.google.com/document/d/16IS1aocfI46KQjSlBbyKiAv38O4oLY6rwkvc2zUUHQs/edit?usp=sharing

1. Custom user account name is suspect, and Windows 10 Home installed
   Operating system information

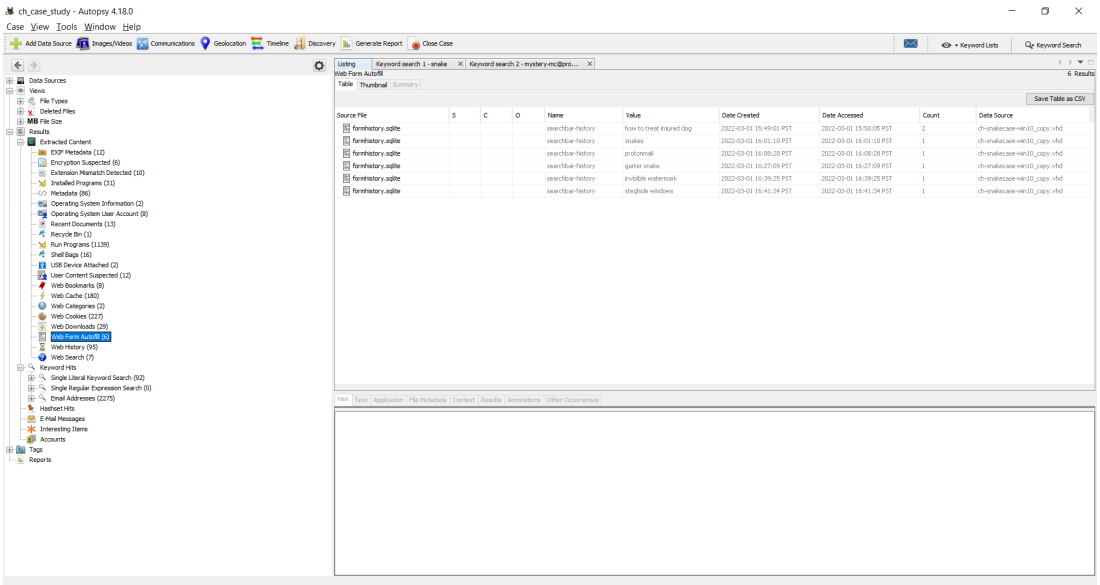


Operating system user account

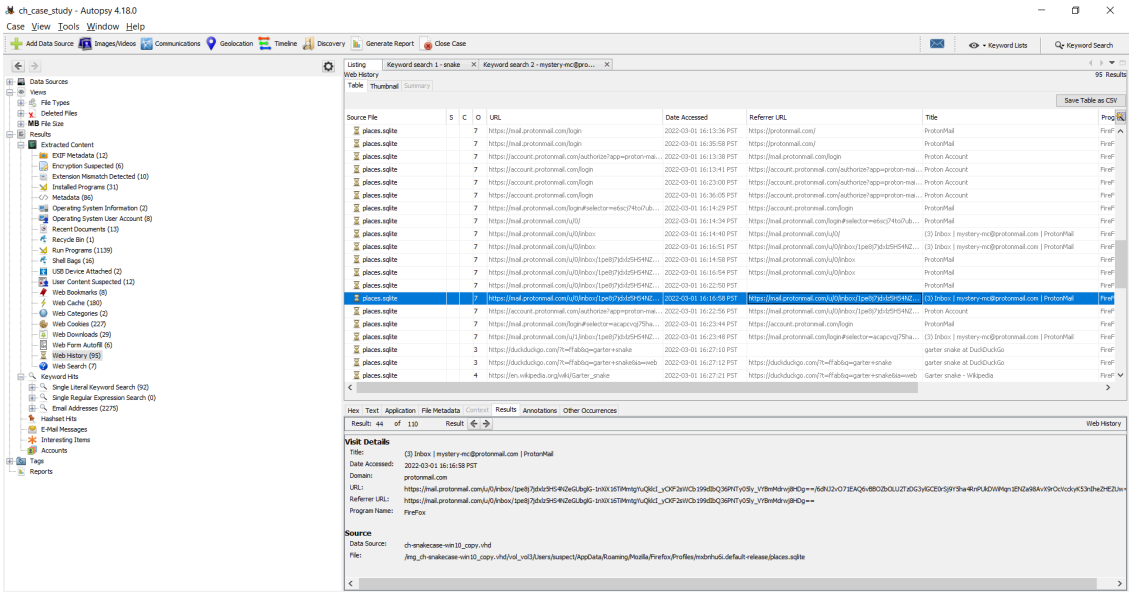


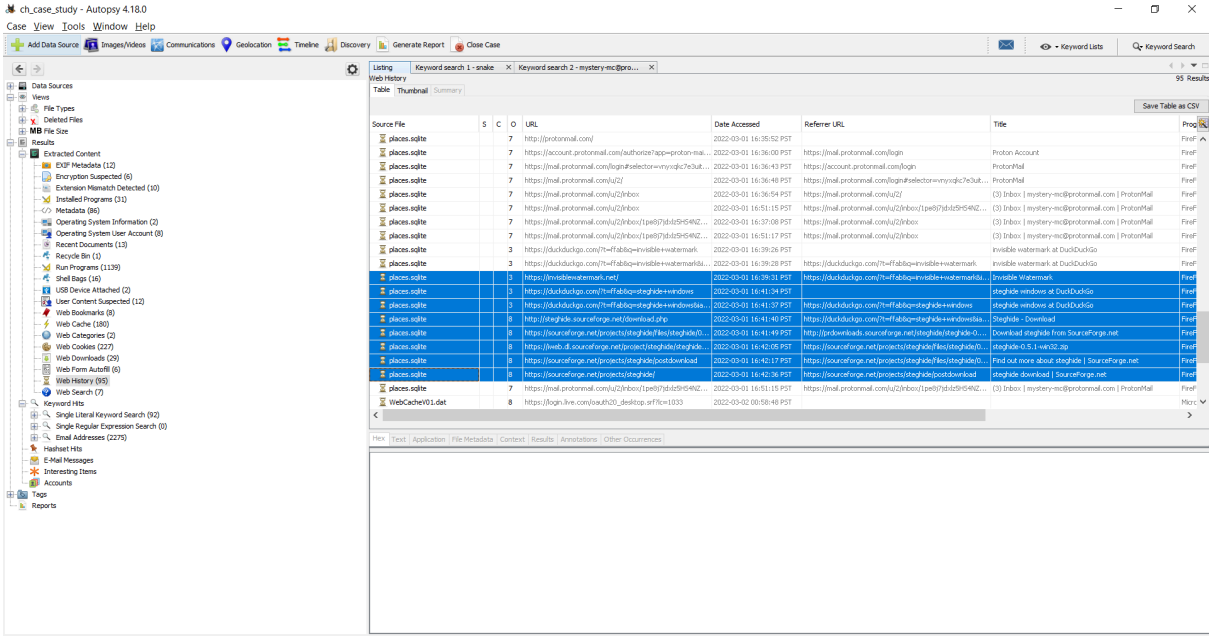
2. Web forum auto fill

- How to treat injured dog
- Snakes
- Protonmail
- Garter snake
- Invisible watermark
- Steghide windows

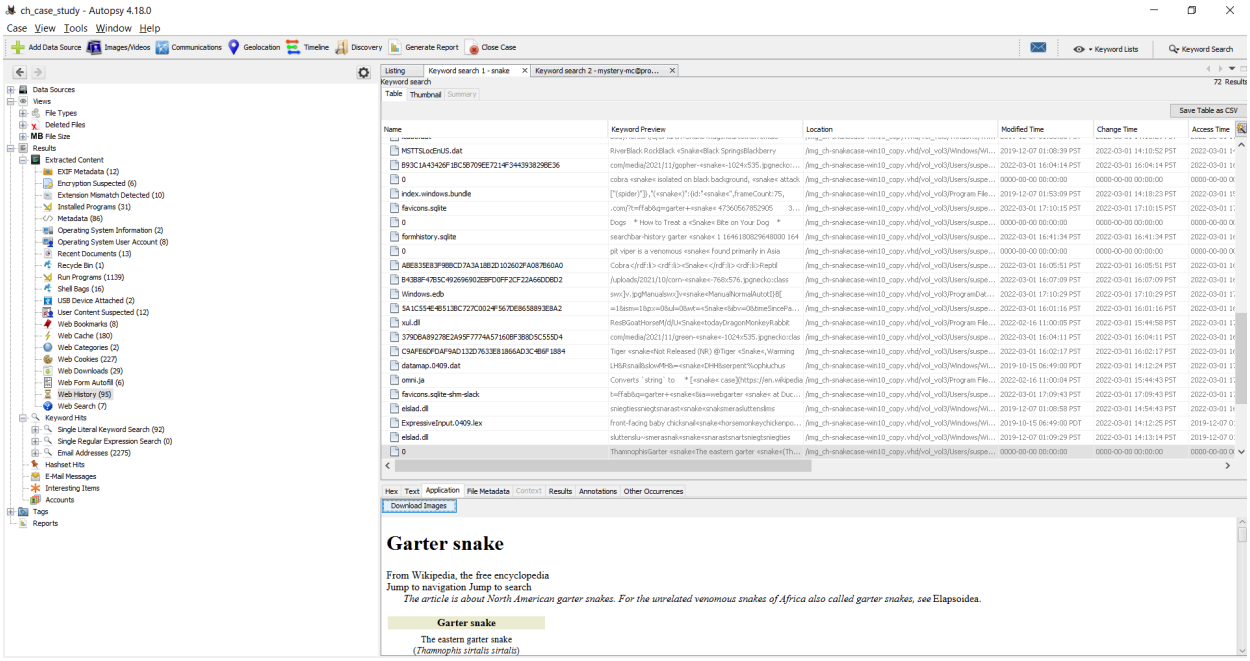


3. Web history/Proton mail inbox
   Mystery-mc@protonmail.com





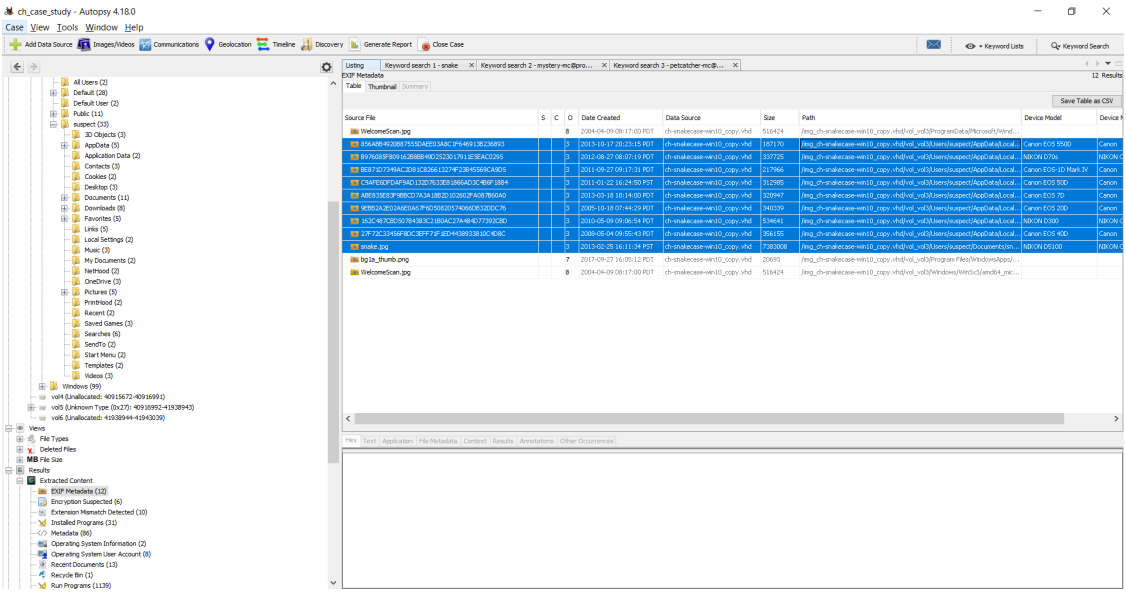
Looked gartel snake information



Searched from internet

- 10 most venomous snakes in the world
- 11 nonvenomous snakes
- 17 nonvenomous snakes
- If you are first time snake owner
- How to treat snake bites on your dog

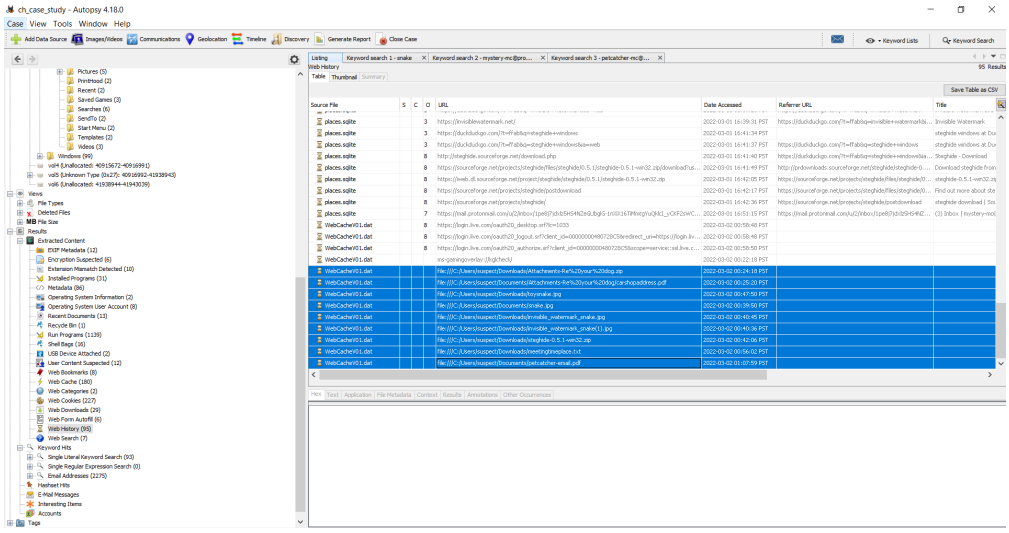
4. Exif meta data



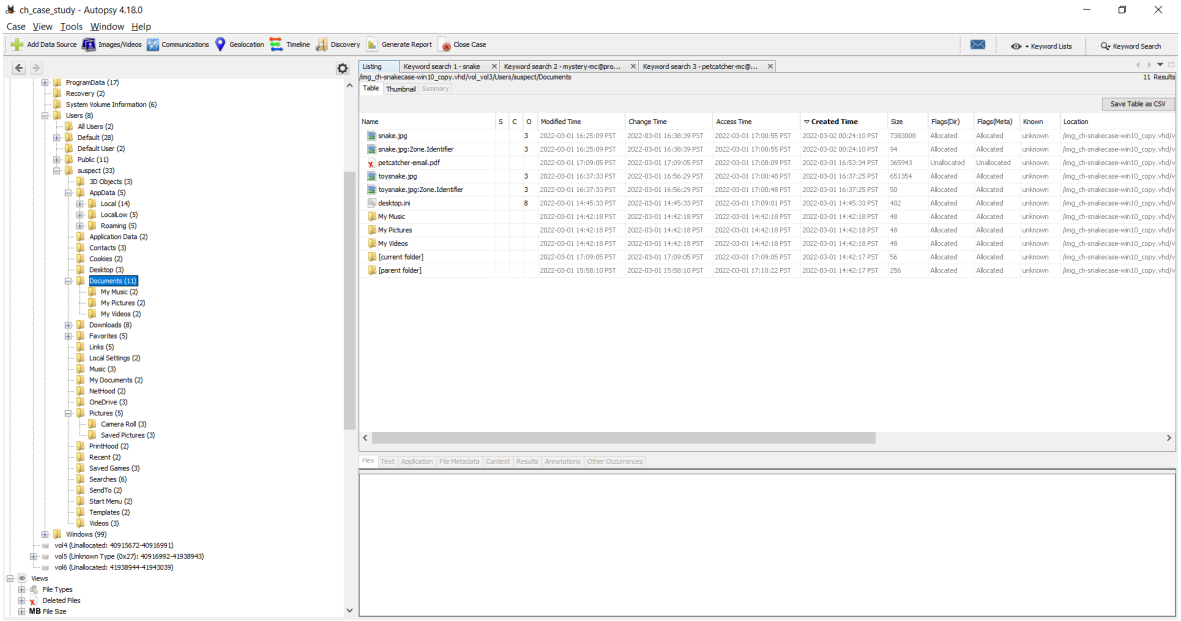
- Racer snake pic

- Hognose snake pic
- Aquatic sea snake pic
- Gopher snake pic
- Australian elapid snake pic
- Elapid snake pic
- Venomous snake pic
- Cobra snake pic
- Corn snake pic

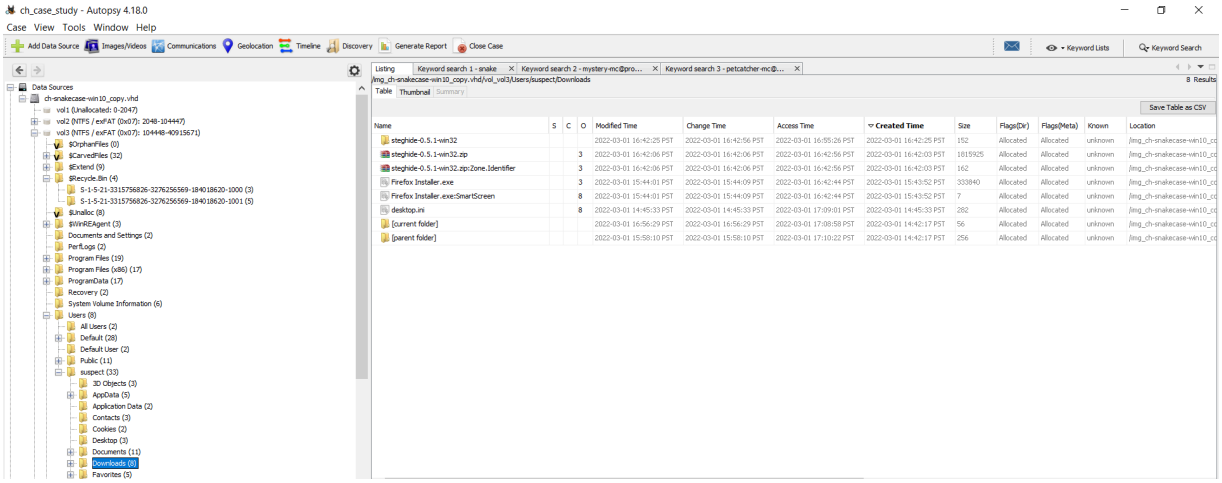
5. Web history



- Users/suspect/Documents/snake.jpg
- Users/suspect/Documents/petcatcher-email.pdf
- Users/suspect/Documents/ Attachments-Re%20your%20dog/carshopaddress.pdf
- Users/suspect/Downloads/Attachments-Re%20your%20dog.zip
- Users/suspect/Downloads/snake.jpg
- Users/suspect/Downloads/toysnake.jpg
- Users/suspect/Downloads/invisible_watermark_snake.jpg
- Users/suspect/Downloads/invisible_watermark_snake(1).jpg
- Users/suspect/Downloads/steghide-0.5.1-wini.zip
- Users/suspect/Downloads/meetingtimeplace.txt

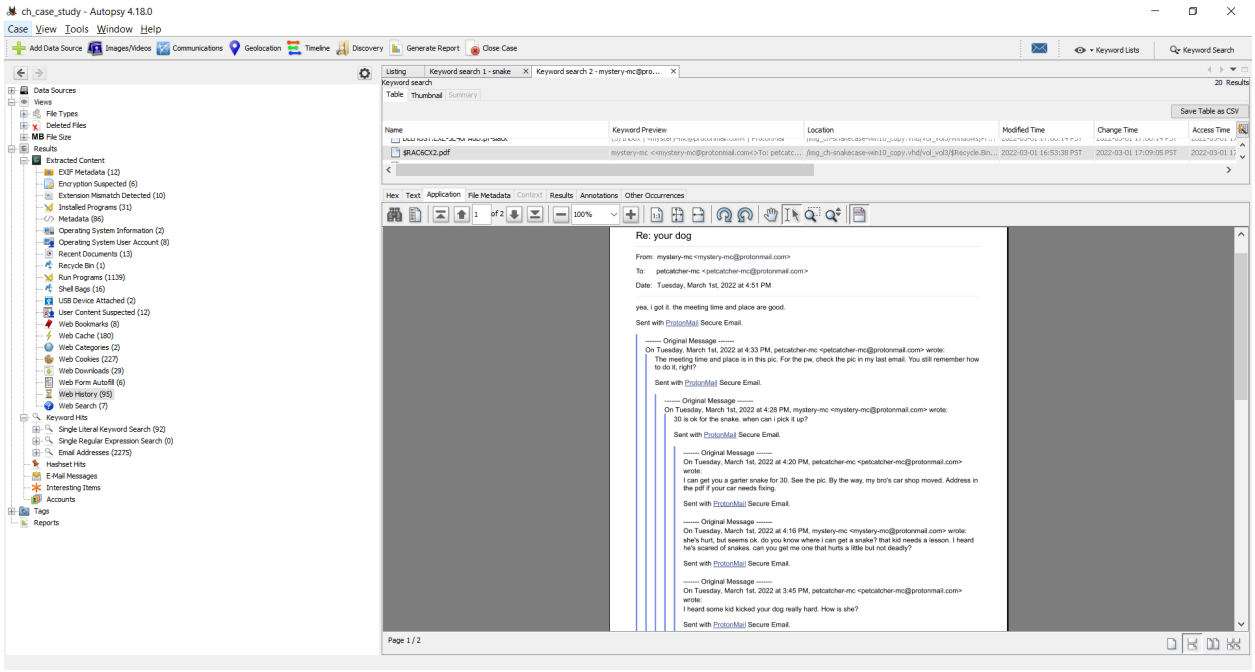


- Missing Users/suspect/Documents/ Attachments-Re%20your%20dog/carshopaddress.pdf

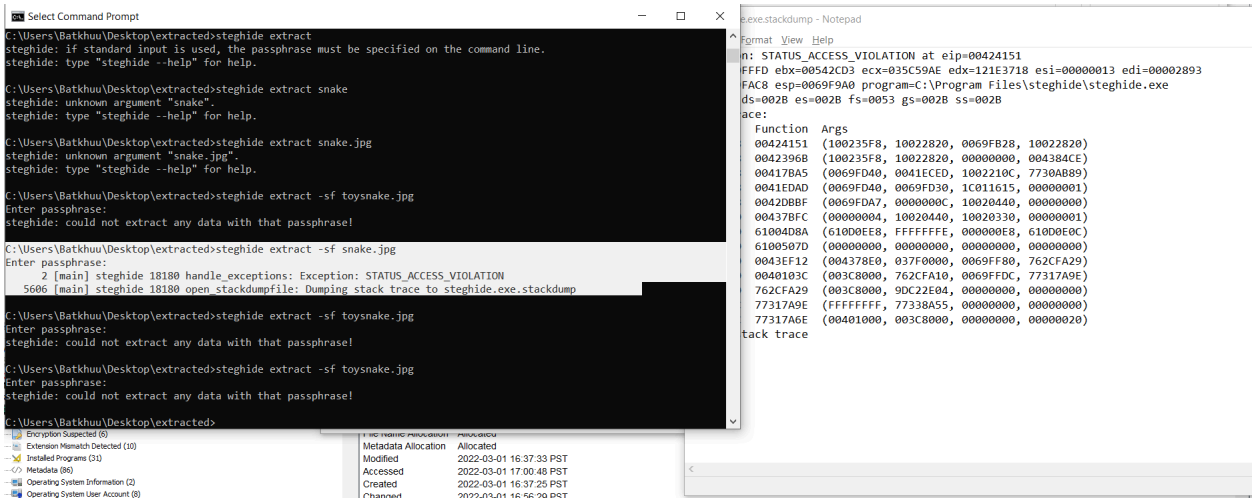


- Users/suspect/Downloads/Attachments-Re%20your%20dog.zip
- Users/suspect/Downloads/snake.jpg
- Users/suspect/Downloads/toysnake.jpg
- Users/suspect/Downloads/invisible_watermark_snake.jpg
- Users/suspect/Downloads/invisible_watermark_snake(1).jpg
- Users/suspect/Downloads/meetingtimeplace.txt

6. Main evidence



Extracted data from snake.jpg / password was snakes



Evidence points to suspect is buying a garter snake from supplier and information about car shop address with pdf information but could not find it from device, and meeting place is hidden one of the pictures using steghide application, Unfortunately, I did not recover completely. Suspect trying to get revenge of his dog and did not try to kill the victim because of looked and asks nonvenomous snake.

A report was generated for both the FTK and IEF processing. These reports were burned to a CD-R for investigative review (Item 2).

AUTHENTICATION:

During the acquisition process, the forensic software creates a hash value of the media being imaged. These hash values were compared to those generated after imaging and processing of

the image file. I verified that the hash values were the same. This indicated that the image file is identical to the original and was not altered during processing.

EVIDENCE DISPOSITION:

Upon completion of the data extraction, the original evidence (Item 1) and the report CD-R (Item 2) prepared for release to the submitting agency.

DISC CONTENTS (as applicable):

The discs contain reports in HTML and PDF format with exported files and bookmarks as described above.