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: 3/24/2022
OFFENSE: MISC.

EVIDENCE SUBMITTED:

One unpackaged evidence item (Item 1), relative to the above case, was received into the Laboratory from Sergeant xxxx by Sheriff's Technician xxxx on [date]. The item was found as follows:

Item #1:
.VDI image ch-case-e1t1-win10 (snake assault v0.2).vdi - 13.3GB
Case Study Instruction: Contraband Snake Assault Case(handout for students) v0.2 [public]

Forensic System/Software/Tools – Acquisition (VDI):
System: ASUS VivoBook 15, No errors on boot
Acquisition software used: Oracle VM Virtual Box, VBoxManage.exe (convert to raw)

Forensic System/Software/Tools – Analysis (IMG): snakecase.img 21.4GB
System: ASUS VivoBook 15, No errors on boot

EXAMINATION

EXAMINER'S NAME: Mike Dilbeck 3/24/22

_____
EXAMINER'S SIGNATURE DATE
TITLE: Intern Extraordinaire

_____
TECHNICAL REVIEWER'S SIGNATURE DATE

FILE NAME: xxxxxxx

_____
ADMINISTRATIVE REVIEWER'S SIGNATURE DATE

CASE #: xx-xxxx
CRIME: xxxxxx
VICTIM OR SUSPECT: UNKNOWN

Analysis software used: Autopsy 4.19.3

REQUEST:

On 3/22/22, Sergeant xxxx of the San Francisco PD submitted a request for the forensic examination of a VDI image obtained from a suspect's laptop. Sergeant xxxx requested an examination of the virtual drive for any images, videos, emails, chat logs, active/deleted/altered files, or any other files that would assist with her investigation.

Sergeant xxxx prepared a search warrant that was signed by a judge of the Alameda County Superior Courts authorizing the examination of the digital media. The search warrant was reviewed prior to processing this case.

On 3/22/22 I examined the submitted virtual drive. It appeared to be in working condition. I documented the findings with screenshots. To examine the drive it would need to be converted to a format that is recognized by the examination software (Autopsy). To do this I used VBoxManage to convert the program to .img format.

I conducted a keyword search using the following terms (not case-sensitive)

- Abuse
- Kicked
- Meeting
- Payback
- Pet
- Snake
- steg

Major Evidence Found

Device Overview

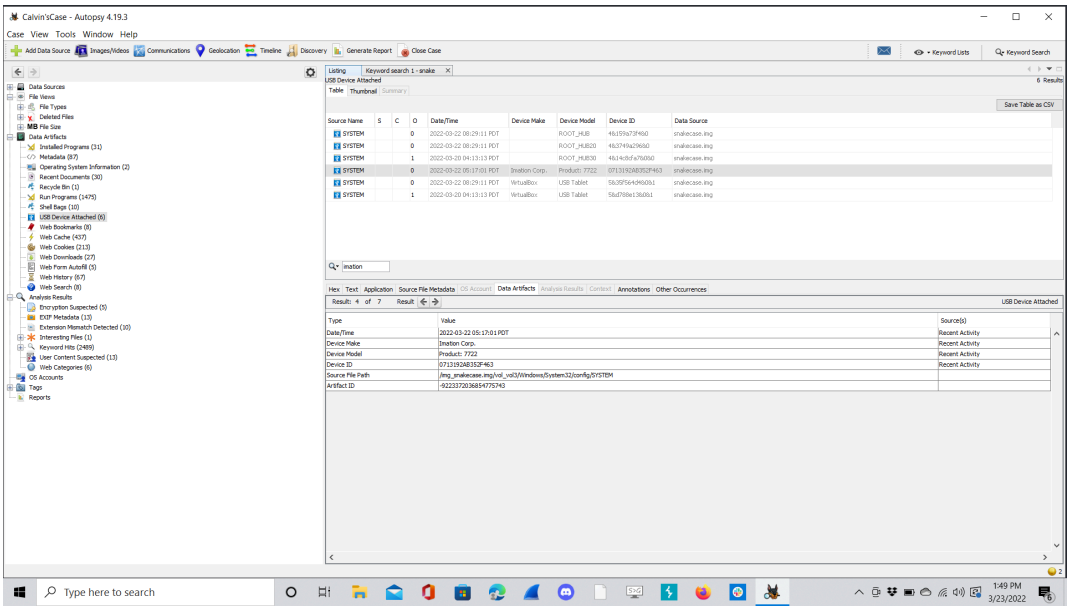
1. Device Information

CASE #: xx-xxxx
CRIME: xxxxxx
VICTIM OR SUSPECT: UNKNOWN

a. Device Owner: Suspect
b. OS: Windows 10 Home
    i. Installation Date: 03/20/2022
    ii. Language: English

2. Partitions
    a. # of Visible Partitions: 7
        i. Vol 1: Unallocated
        ii. Vol 2: NTFS
        iii. Vol 3: NTFS - Main drive (C:/)
        iv. Vol 4: Unallocated
        v. Vol 7: NTFS -possible hidden partition(E:/)
        vi. Vol 8: Unknown
        vii. Vol 9: Unallocated
    b. # of Hidden Partitions: 2?
        i. Vol 7: seems to contain a file that may be an attempt at hiding it (E:/)
        ii. Vol 8: Unknown may indicate attempted hiding but nothing of interest on partition
3. Accounts
    a. Suspect
    b. Admin
    c. Guest
4. Devices Attached
    a. USB 1: Root Hub
    b. USB 2: Root Hub 2.0
    c. USB 3: Root Hub 3.0
    d. USB 4: Imation corp. Product 7722 (Flash drive)
    e. USB 5: VirtualBox USB tablet
    f. USB 6: VirtualBox USB tablet

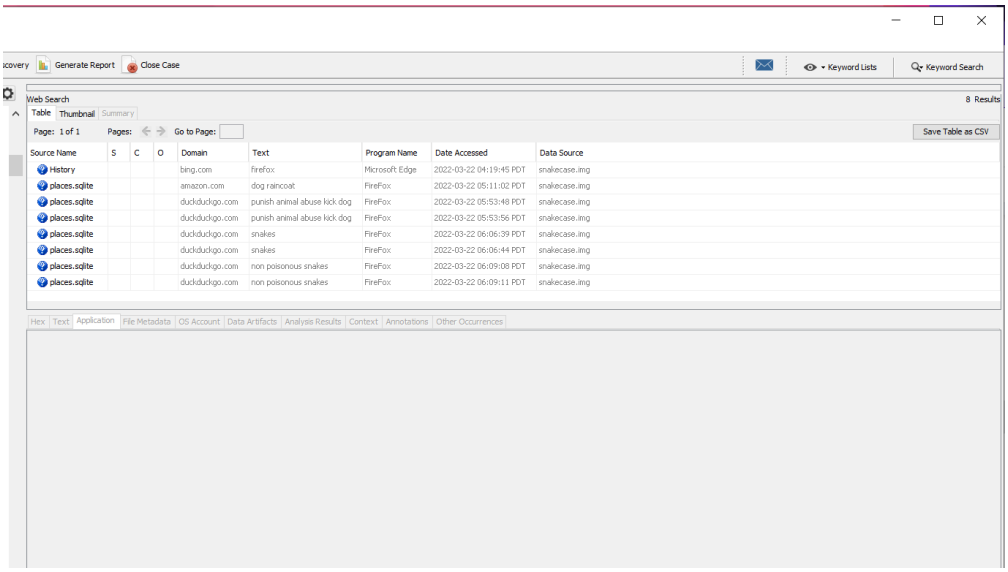
CASE #: xx-xxxx
CRIME: xxxxxx
VICTIM OR SUSPECT: UNKNOWN



Internet-Related

5. Internet Activities
    a. Web Search Terms
        i. Firefox
        ii. Dog raincoat
        iii. Punish animal abuse kick - dog
        iv. Snakes
        v. Non poisonous snakes

CASE #: xx-xxxx
CRIME: xxxxxx
VICTIM OR SUSPECT: UNKNOWN



b. Web Site Visited
   i. duckduckgo.com
   ii. tutanota.com
   iii. Amazon.com
   iv. Animalpetitions.org
   v. Kb.rspca.org.au
   vi. Nationalgeographic.com
   vii. Travel.earth
   viii. Nps.gov
   ix. A-z-animals.com
   x. En.wikipedia.org
   xi. Sourceforge.net
   xii. nordpass.com

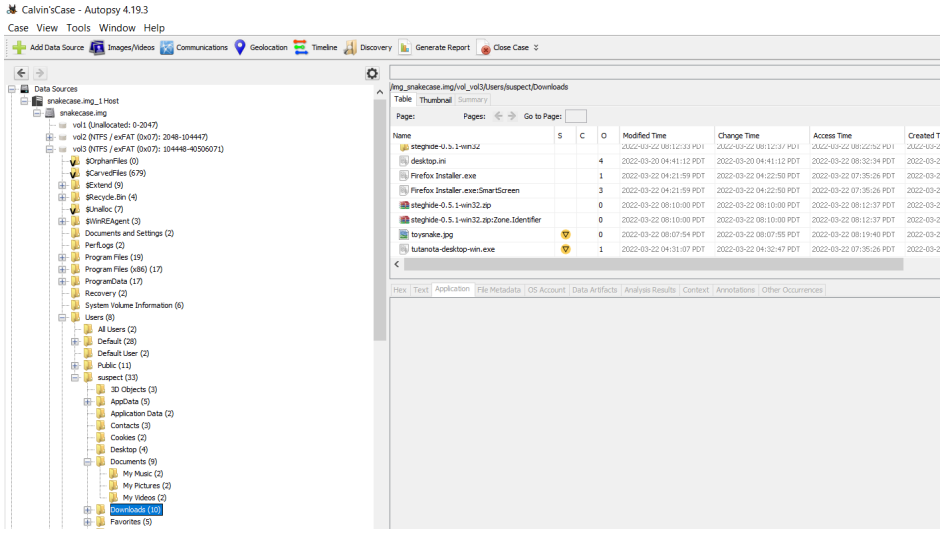
c. Web Sites Bookmarked
   i. https://www.wikihow.com/Take-Care-of-an-Injured-Dog
   ii. https://animalpetitions.org/748436/punish-mother-who-allegedly-encouraged/animal-abuse/
   iii. 6 more that are apparently not linked to case

d. Online Accounts
   i. mystery-mc@account@tutanota.com

e. Online Map Locations and Directions

None

f. Downloaded Files



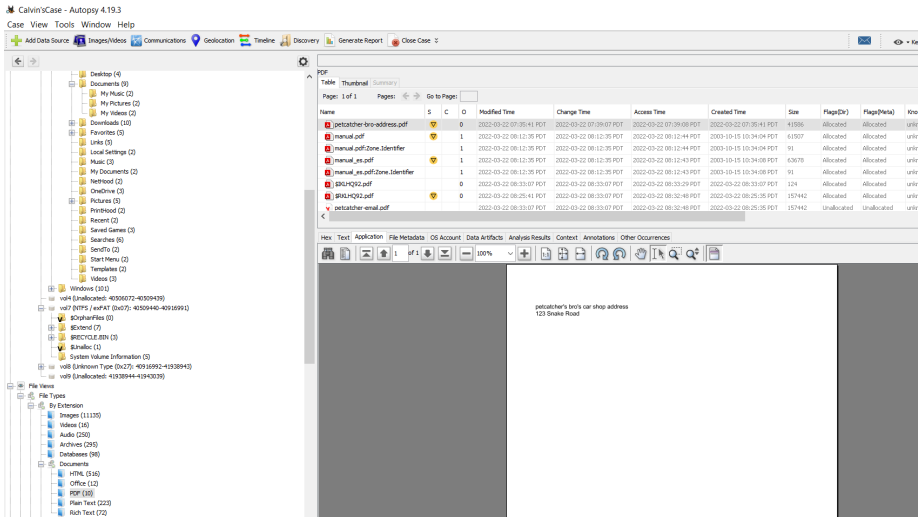
i. toy-snake.jpg
ii. steghide.zip

g. Downloaded Programs
i. Firefox Installer
ii. Tutanota Desktop
iii. Steghide

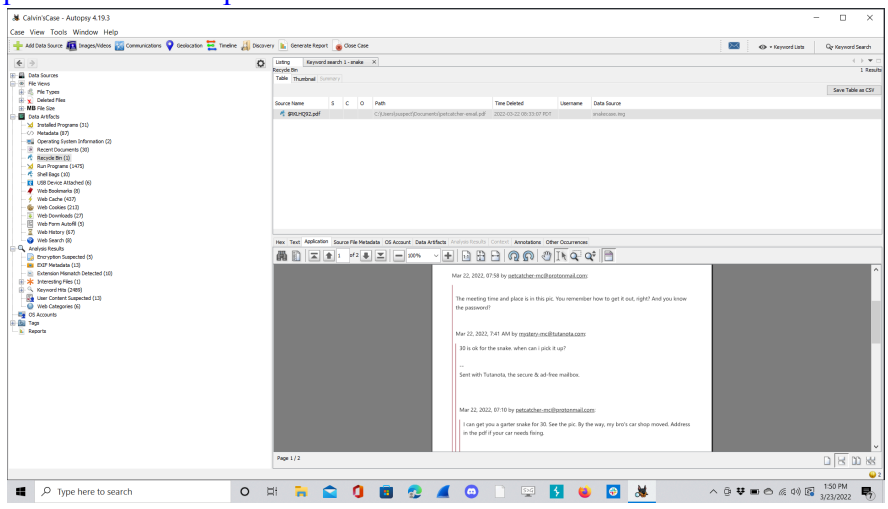
6. Emails
a. Email Accounts
None(evidence suggests suspect used online email-Tutanota)
b. Suspicious Email Addresses
i. mystery-mc@tutanota.com
ii. petcatcher-mc@protonmail.com
c. Email Subject Lines or Messages Found
i. Pet-catcher-email.pdf (copy of an email string)
d. Email Attachment Downloads
None
e. Local Email Clients
None
f. Email Backups
None

Data Files and Programs

7. Files
    a. Plain Text Files
        i. Suspect_email_list.txt (on hidden partition?)
        ii. Meetingtimeplace.txt (hidden within image)
    b. Documents of other formats
        i. petcatcher-bro-address.pdf

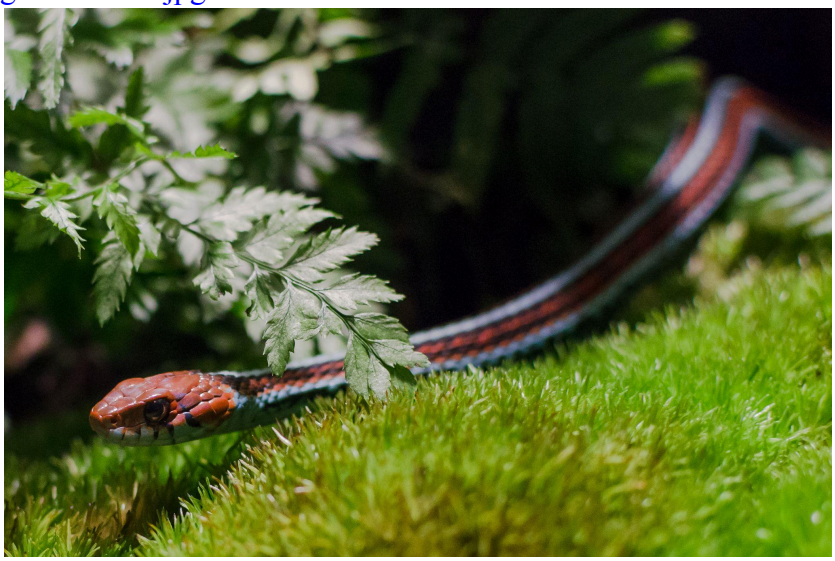


        ii. petcatcher-email.pdf



c. Images

i. garter-snake.jpg



ii. toysnake.jpg

d. Videos / Audios / etc.

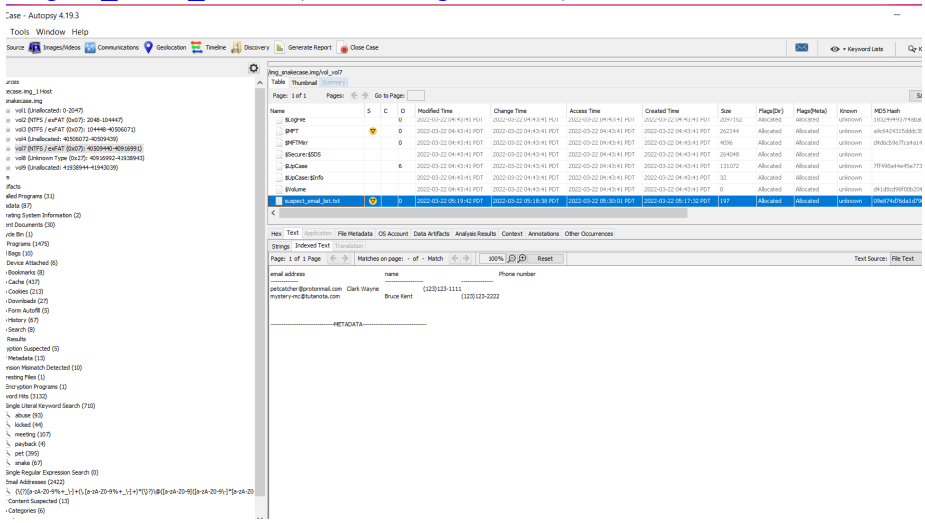
None

e. Opened Files

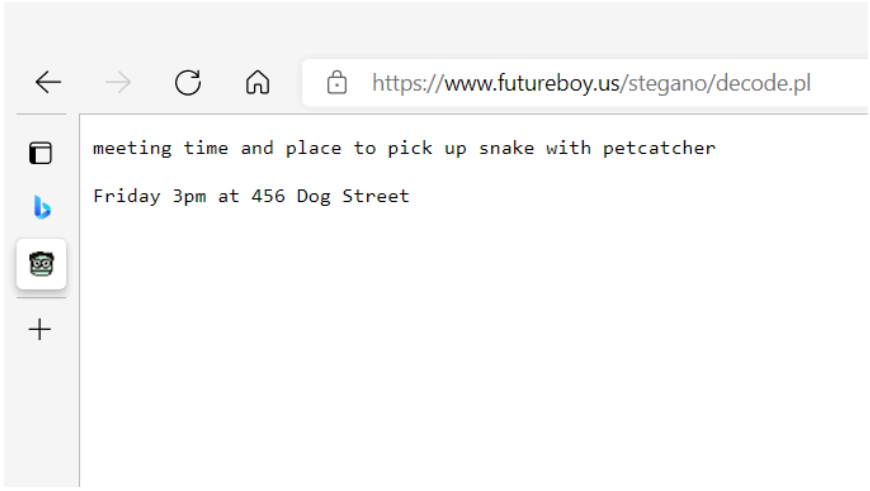
CASE #: xx-xxxx
CRIME: xxxxxx
VICTIM OR SUSPECT: UNKNOWN

i. garter-snake.jpg
ii. toysnake.jpg
iii. Mettingtimeplace.txt
iv. Suspect_email_list.txt
v. Petcatcher-bro-address.pdf
vi. Petcatcher-email.pdf
vii. steghide-0.5.1-win32.zip

f. Hidden Files (in visible folders, or in hidden partitions)
   i. Suspect_email_list.txt (on hidden partition?)

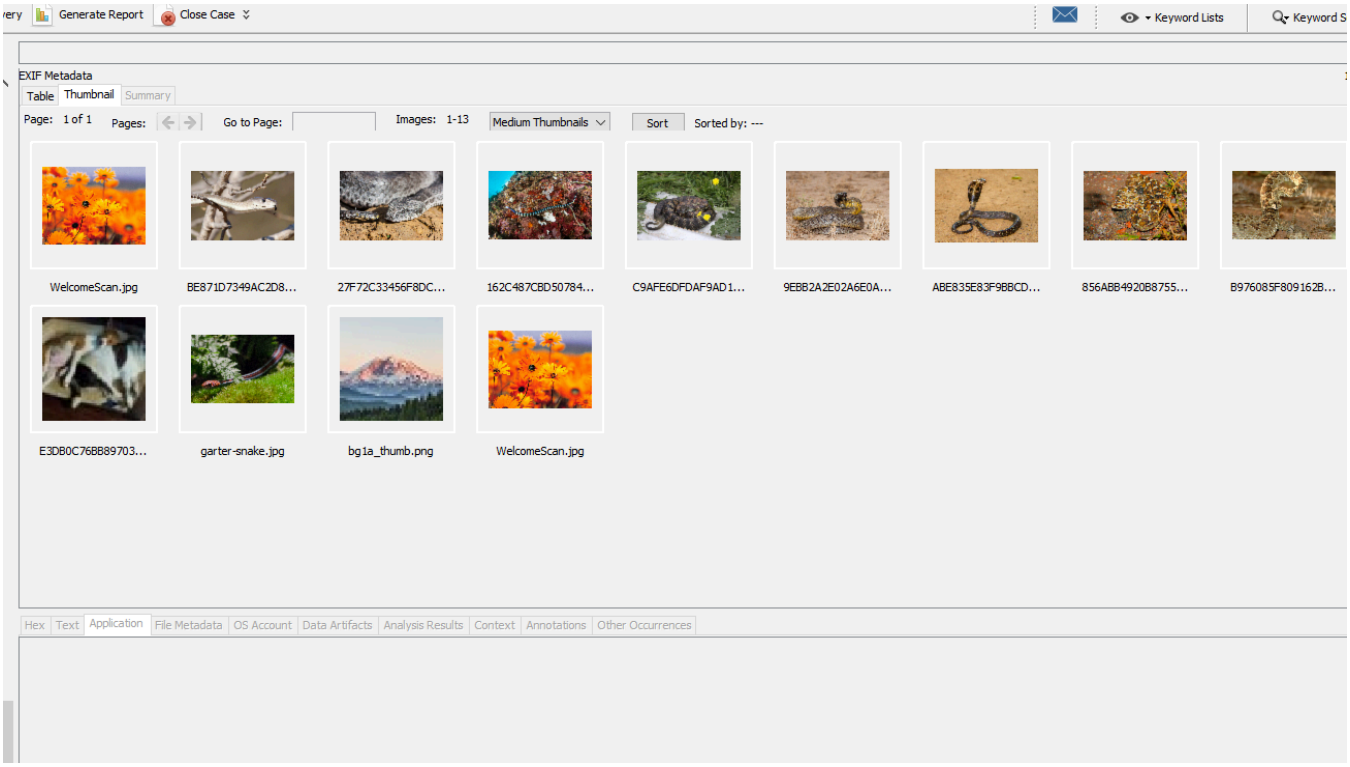


   ii. Meetingtimeplace.txt (hidden within image)

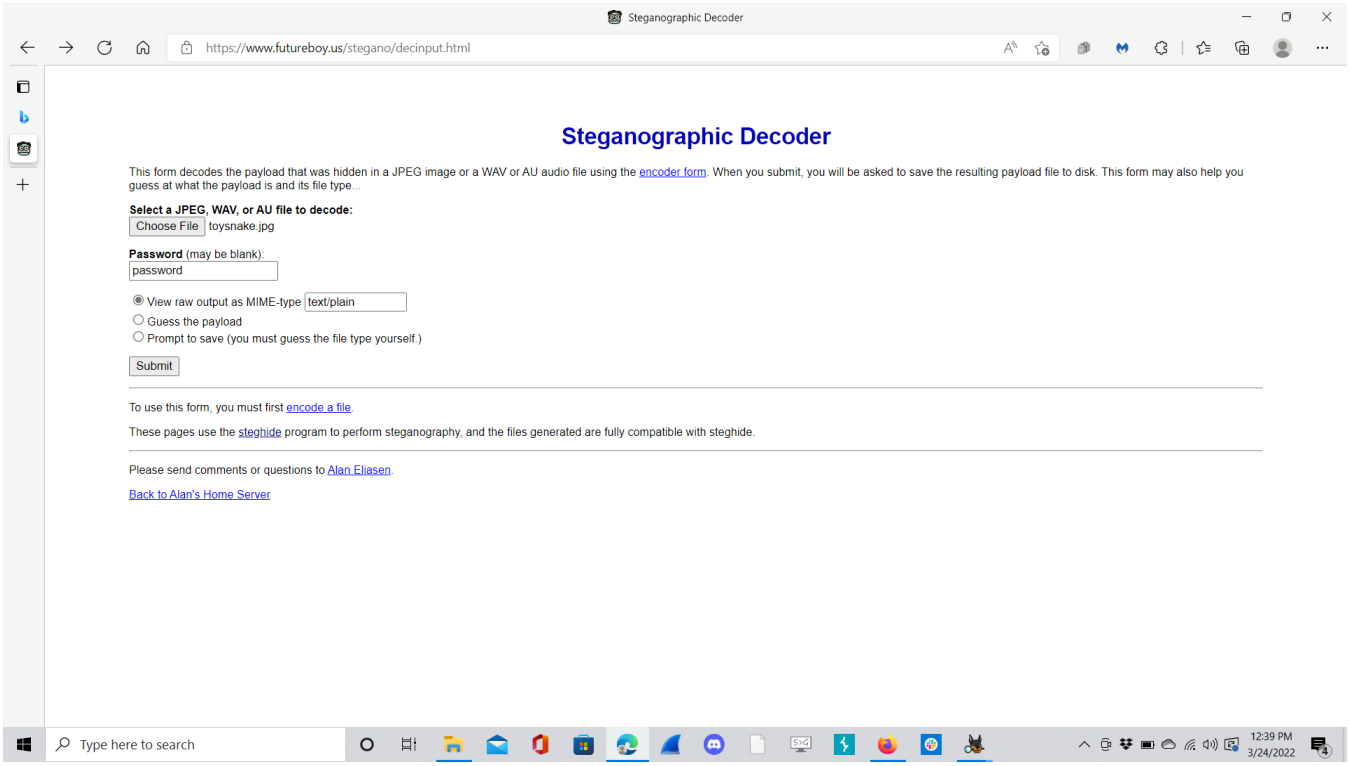


g. Files with mismatched extension
   None
h. Encrypted Files
   None
i. Deleted Files
   i. petcatcher-email.pdf (Recycle Bin)

j. Recovered / Carved files
   i. 8 images of Snakes (EXIF Metadata)
   ii. Image of a dog and cat (EXIF Metadata)



8. Password
   a. Password found
      None
   b. Password guessed
      i. password (to unlock meetingplacetime.txt from toysnake.jpg)



c. Password cracked
   None
d. Password files
   None

9. Programs
   a. Installed Programs
      i. Firefox

   b. Executed Programs
      i. Firefox
      ii. Tutanota Desktop
      iii. Steghide
   c. Log files
      None

   d. Uninstalled Programs
      i. Tutanota (not installed but run)
      ii. Steghide (not installed but run)

CASE #: xx-xxxx
CRIME: xxxxxx
VICTIM OR SUSPECT: UNKNOWN

Peripherals and Networks

10. Phone backup data
    None
11. Network Traffic Files (PCAP):
    None

Reconstructed Timeline of Major Events

36 events

Date/Time	Event Type	Description	Tagged	Hash Hit
2022-03-22 04:21:45	Web Downloads	https://download.mozilla.org/?product=firefox-stub&os=win&lang=en-US		
2022-03-22 04:29:56	Web Form Autofill Accessed	searchbar-history:tutanota Access count: 1 : :		
2022-03-22 04:29:56	Web Form Autofill Created	searchbar-history:tutanota : :		
2022-03-22 04:30:32	Web History Accessed	https://tutanota.com/#download		
2022-03-22 04:30:41	Web Downloads	https://mail.tutanota.com/desktop/tutanota-desktop-win.exe		
2022-03-22 05:10:38	Web History Accessed	https://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&field-keywords=dog+raincoat		
2022-03-22 05:11:53	Web History Accessed	https://www.amazon.com/HDE-Raincoat-Slicker-X-Large-Puppies/d ... J4D965/ref=sr_1_5?keywords=dog+raincoat&qid=1647951039&sr=8-5		
2022-03-22 05:17:01	Devices Attached	Imation Corp. : Product: 7722 : 0713192AB352F463		
2022-03-22 05:51:15	Web Form Autofill Accessed	searchbar-history:how to treat injured dog Access count: 1 : :		
2022-03-22 05:51:15	Web Form Autofill Created	searchbar-history:how to treat injured dog : :		
2022-03-22 05:52:19	Web History Accessed	https://www.handicappedpets.com/blog/injured-dog-care/		
2022-03-22 05:53:48	Web History Accessed	https://duckduckgo.com/?q=punish+animal+abuse+kick+dog&t=ffab		
2022-03-22 06:03:35	Web History Accessed	https://kb.rspca.org.au/knowledge-base/what-are-the-penalties-for-animal-cruelty-offences/		
2022-03-22 06:06:08	Web Bookmarks	https://www.wikihow.com/Take-Care-of-an-Injured-Dog		
2022-03-22 06:06:19	Web Bookmarks	https://animalpetitions.org/748436/punish-mother-who-allegedly-encouraged-animal-abuse/		
2022-03-22 06:06:53	Web History Accessed	https://www.nationalgeographic.com/animals/reptiles/facts/snakes-1		
2022-03-22 06:07:36	Web History Accessed	https://travel.earth/dangerous-snakes-in-the-world/		
2022-03-22 06:09:37	Web History Accessed	https://a-z-animals.com/blog/9-non-poisonous-snakes-in-the-world/		
2022-03-22 07:37:27	Web History Accessed	file:///C:/Users/suspect/Downloads/petcatcher-bro-address.pdf		
2022-03-22 07:39:40	Web Form Autofill Created	searchbar-history:garter snake : :		
2022-03-22 07:39:40	Web Form Autofill Accessed	searchbar-history:garter snake Access count: 1 : :		
2022-03-22 07:39:53	Web History Accessed	https://en.wikipedia.org/wiki/Garter_snake		
2022-03-22 08:07:54	_BM	/Users/suspect/Downloads/toysnake.jpg		
2022-03-22 08:07:55	_C_	/Users/suspect/Downloads/toysnake.jpg		
2022-03-22 08:09:07	Web Form Autofill Created	searchbar-history:steghide windows : :		

Time / Date	Event	Artifact Created	Artifact Location	Evidence Category

_____

Forensic Examiner's initials _____
Technical Reviewer's Initials_____
Administrative Reviewer's Initials_____

CASE #: xx-xxxx
CRIME: xxxxxx
VICTIM OR SUSPECT: UNKNOWN

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.

_____

Forensic Examiner's initials _____
Technical Reviewer's Initials_____
Administrative Reviewer's Initials_____

CASE #: xx-xxxx
CRIME: xxxxxx
VICTIM OR SUSPECT: UNKNOWN

DISC CONTENTS (as applicable):

N/A