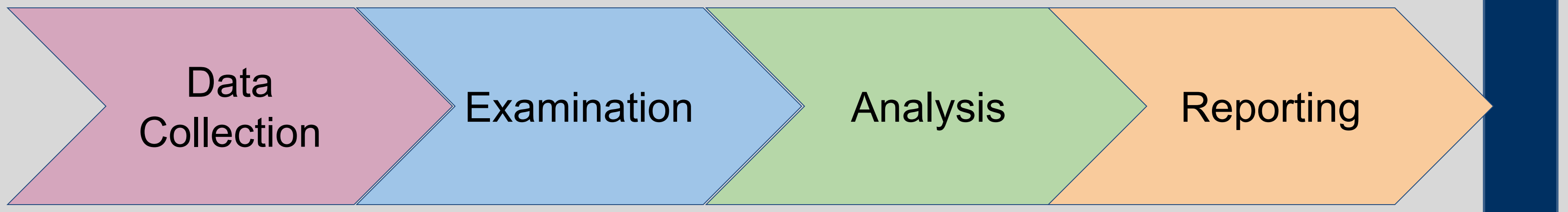
RET Site: Research Experience in Cybersecurity for Nevada Teachers (RECNT)

Morgan Satterfield
Carl Antiado and Eric Valdez
PI: Shamik Sengupta, Co-PI: David Feil-Seifer

Introduction

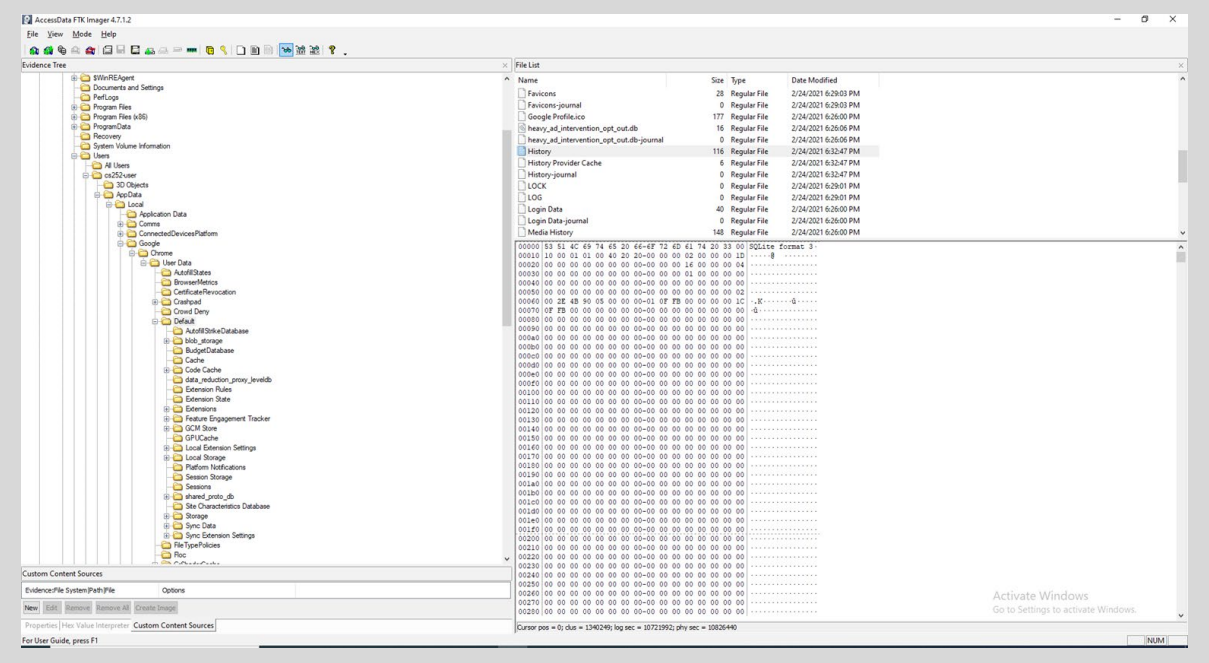
Digital forensics requires an investigator to go through 4 main steps: collecting the data, examining it, analyzing the data, and reporting the findings.



A forensic image of each forensic artifact (e.g. documents, images, emails, etc.) must be made so that the integrity of the evidence is preserved. This can be done through the use of write blockers and can be checked through the use of hash values.

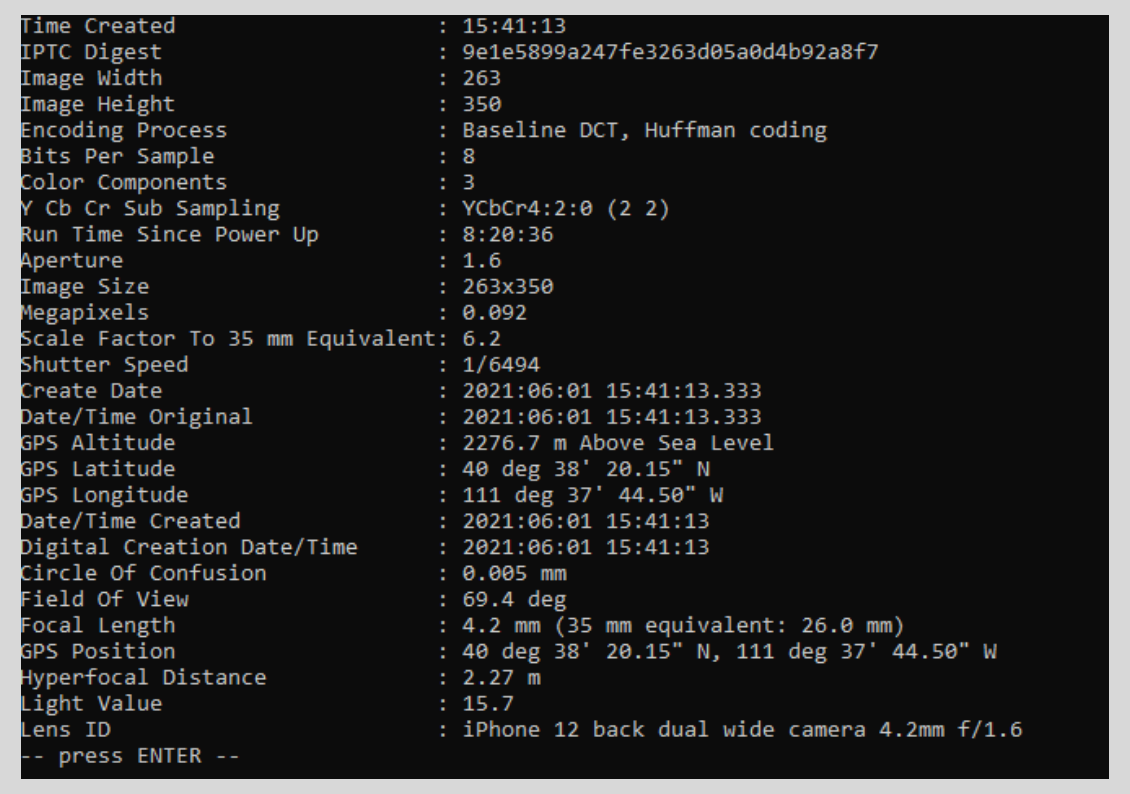
Examples of Forensics Tools

Any tool that is used must be verified in order to be used in a forensic investigation. Multiple tools and hashing can be utilized to ensure the validity of said tool.

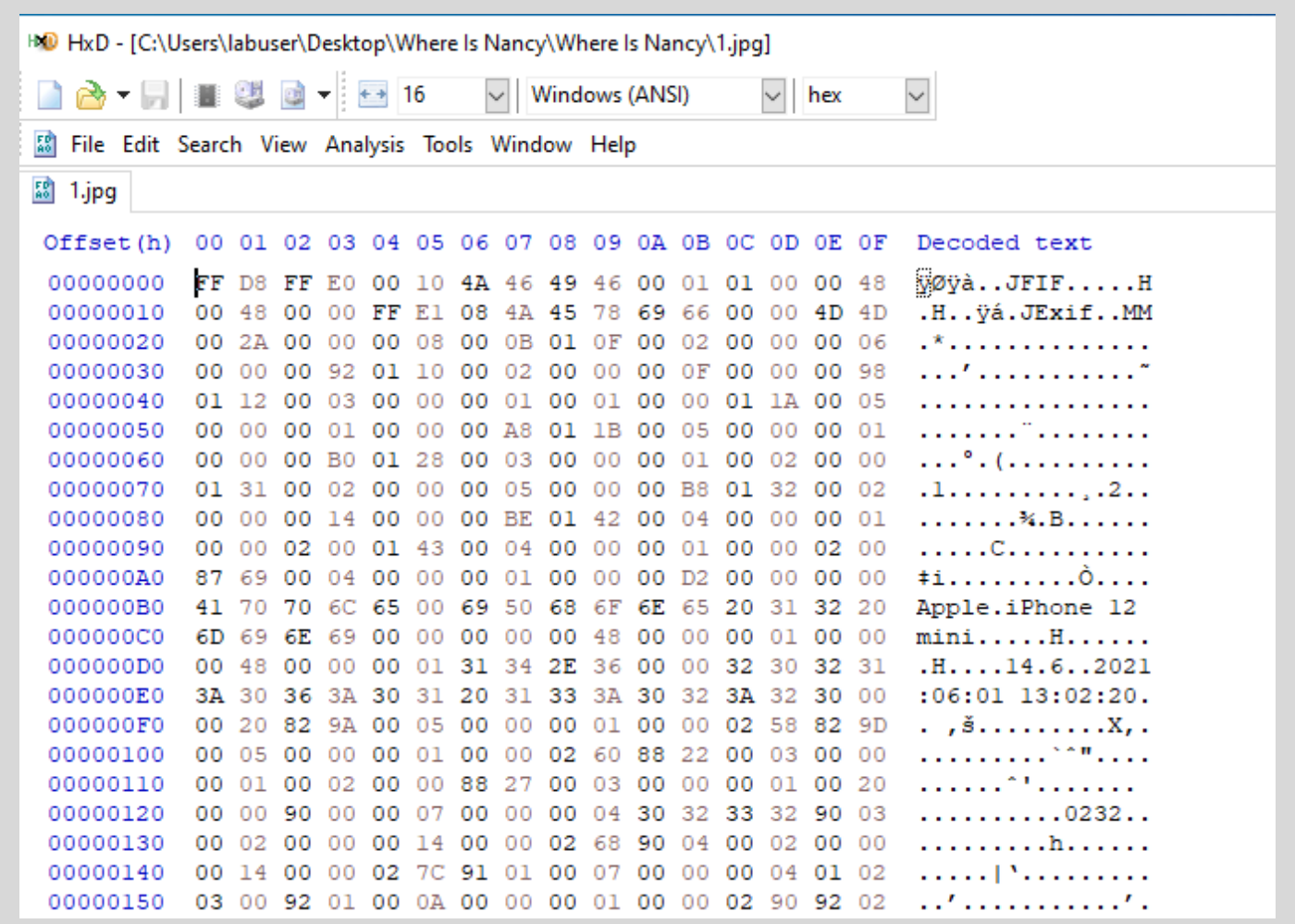


FTK Tools can be used to create a forensic image of the data so that the forensic artifacts can be accessed while maintaining its integrity.

Exiftools can be utilized to analyze and alter the metadata of an image. Such metadata can include date/timestamps, GPS coordinates, devices utilized, image descriptors, and so on.



```
Time Created                    : 15:41:13
IPTC Digest                     : 9e1e5899a247fe3263d05a0d4b92a8f7
Image Width                     : 263
Image Height                    : 350
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Run Time Since Power Up         : 8:20:36
Aperture                        : 1.6
Image Size                      : 263x350
Megapixels                      : 0.092
Scale Factor To 35 mm Equivalent: 6.2
Shutter Speed                   : 1/6494
Create Date                     : 2021:06:01 15:41:13.333
Date/Time Original              : 2021:06:01 15:41:13.333
GPS Altitude                    : 2276.7 m Above Sea Level
GPS Latitude                    : 40 deg 38' 20.15" N
GPS Longitude                   : 111 deg 37' 44.50" W
Date/Time Created               : 2021:06:01 15:41:13
Digital Creation Date/Time      : 2021:06:01 15:41:13
Circle Of Confusion             : 0.005 mm
Field Of View                   : 69.4 deg
Focal Length                    : 4.2 mm (35 mm equivalent: 26.0 mm)
GPS Position                    : 40 deg 38' 20.15" N, 111 deg 37' 44.50" W
Hyperfocal Distance             : 2.27 m
Light Value                     : 15.7
Lens ID                         : iPhone 12 back dual wide camera 4.2mm f/1.6
-- press ENTER --
```



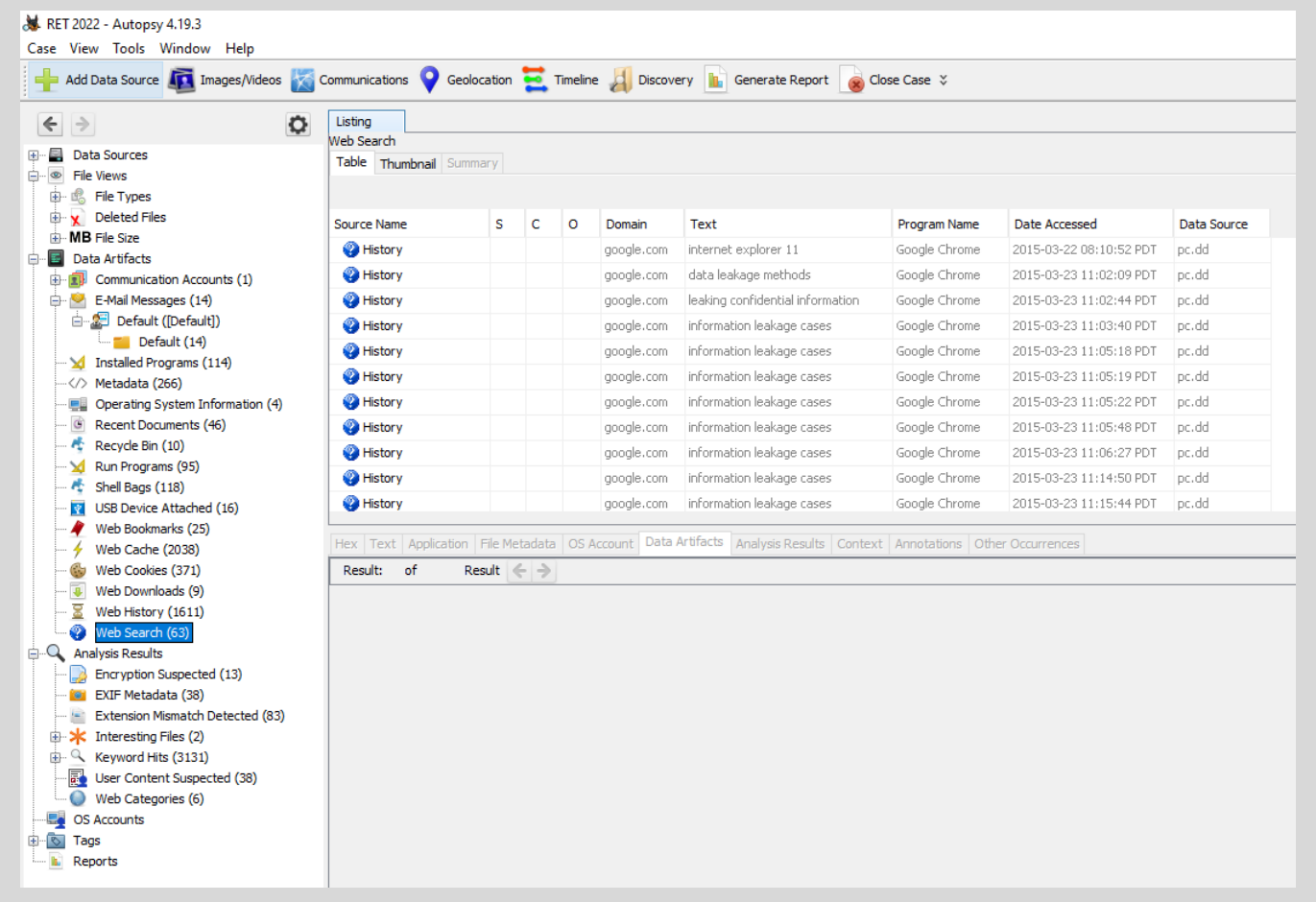
HxD - [C:\Users\labuser\Desktop\Where Is Nancy\Where Is Nancy\1.jpg]

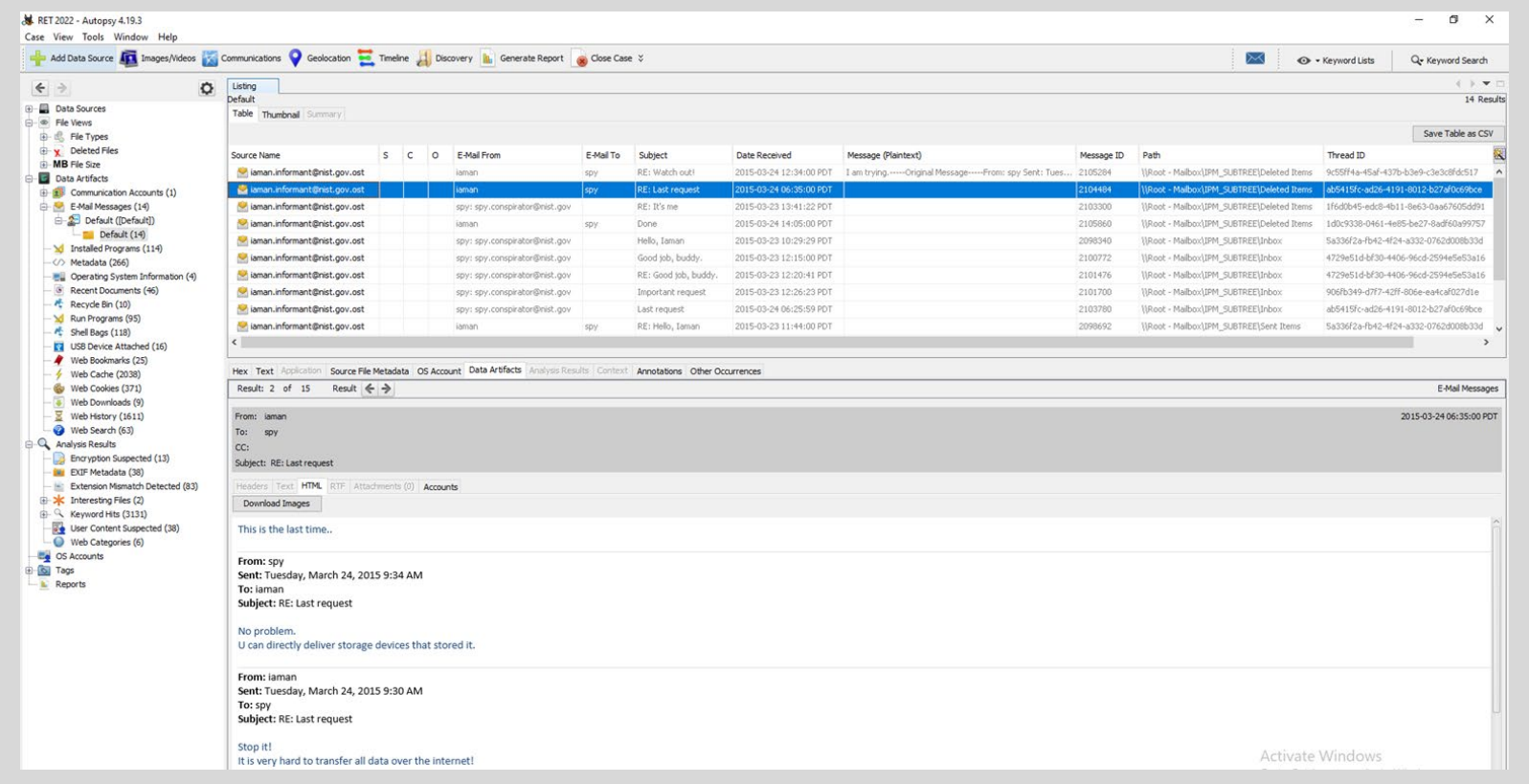
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 48  ÿØÿà..JFIF.....H
00000010  00 48 00 00 FF E1 08 4A 45 78 69 66 00 00 4D 4D  .H..ÿá.JExif..MM
00000020  00 2A 00 00 00 08 00 0B 01 0F 00 02 00 00 00 06  .*..............
00000030  00 00 00 92 01 10 00 02 00 00 00 0F 00 00 00 98  ...'...........˜
00000040  01 12 00 03 00 00 00 01 00 01 00 00 01 1A 00 05  ................
00000050  00 00 00 01 00 00 00 A8 01 1B 00 05 00 00 00 01  .......¨........
00000060  00 00 00 B0 01 28 00 03 00 00 00 01 00 02 00 00  ...°.(..........
00000070  01 31 00 02 00 00 00 05 00 00 00 B8 01 32 00 02  .1.........¸.2..
00000080  00 00 00 14 00 00 00 BE 01 42 00 04 00 00 00 01  .......¾.B......
00000090  00 00 02 00 01 43 00 04 00 00 00 01 00 00 02 00  .....C..........
000000A0  87 69 00 04 00 00 00 01 00 00 00 D2 00 00 00 00  ‡i.........Ò....
000000B0  41 70 70 6C 65 00 69 50 68 6F 6E 65 20 31 32 20  Apple.iPhone 12 
000000C0  6D 69 6E 69 00 00 00 00 00 48 00 00 00 01 00 00  mini.....H......
000000D0  00 48 00 00 00 01 31 34 2E 36 00 00 32 30 32 31  .H....14.6..2021
000000E0  3A 30 36 3A 30 31 20 31 33 3A 30 32 3A 32 30 00  :06:01 13:02:20.
000000F0  00 20 82 9A 00 05 00 00 00 01 00 00 02 58 82 9D  . ‚š.........X‚.
00000100  00 05 00 00 00 01 00 00 02 60 88 22 00 03 00 00  .........`ˆ"....
00000110  00 01 00 02 00 00 88 27 00 03 00 00 00 01 00 20  ......ˆ'....... 
00000120  00 00 90 00 00 07 00 00 00 04 30 32 33 32 90 03  ..........0232..
00000130  00 02 00 00 00 14 00 00 02 68 90 04 00 02 00 00  .........h......
00000140  00 14 00 00 02 7C 91 01 00 07 00 00 00 04 01 02  .....|'.........
00000150  03 00 92 01 00 0A 00 00 00 01 00 00 02 90 92 02  ..'..........'.
```

HxD can be used to file carve, including locating, restoring, and altering files through the hex code.

Investigation

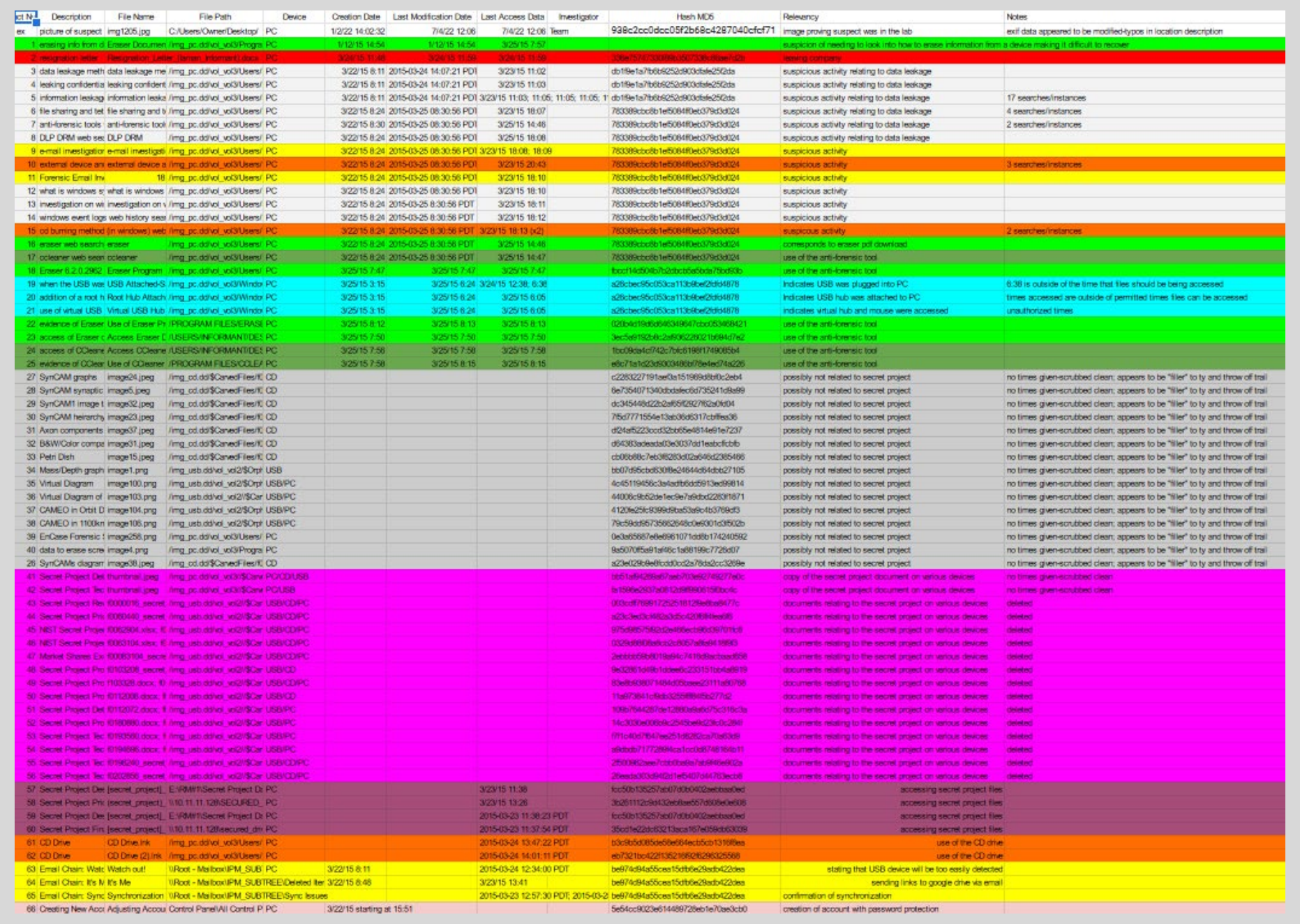
Programs such as Autopsy combine the individual tools to analyze multiple sources and artifact types at once. This program shows the artifact, metadata (including creation/access/modification dates), hash values, and specific paths. While this tool is convenient, it is still important to remember to validate the results.

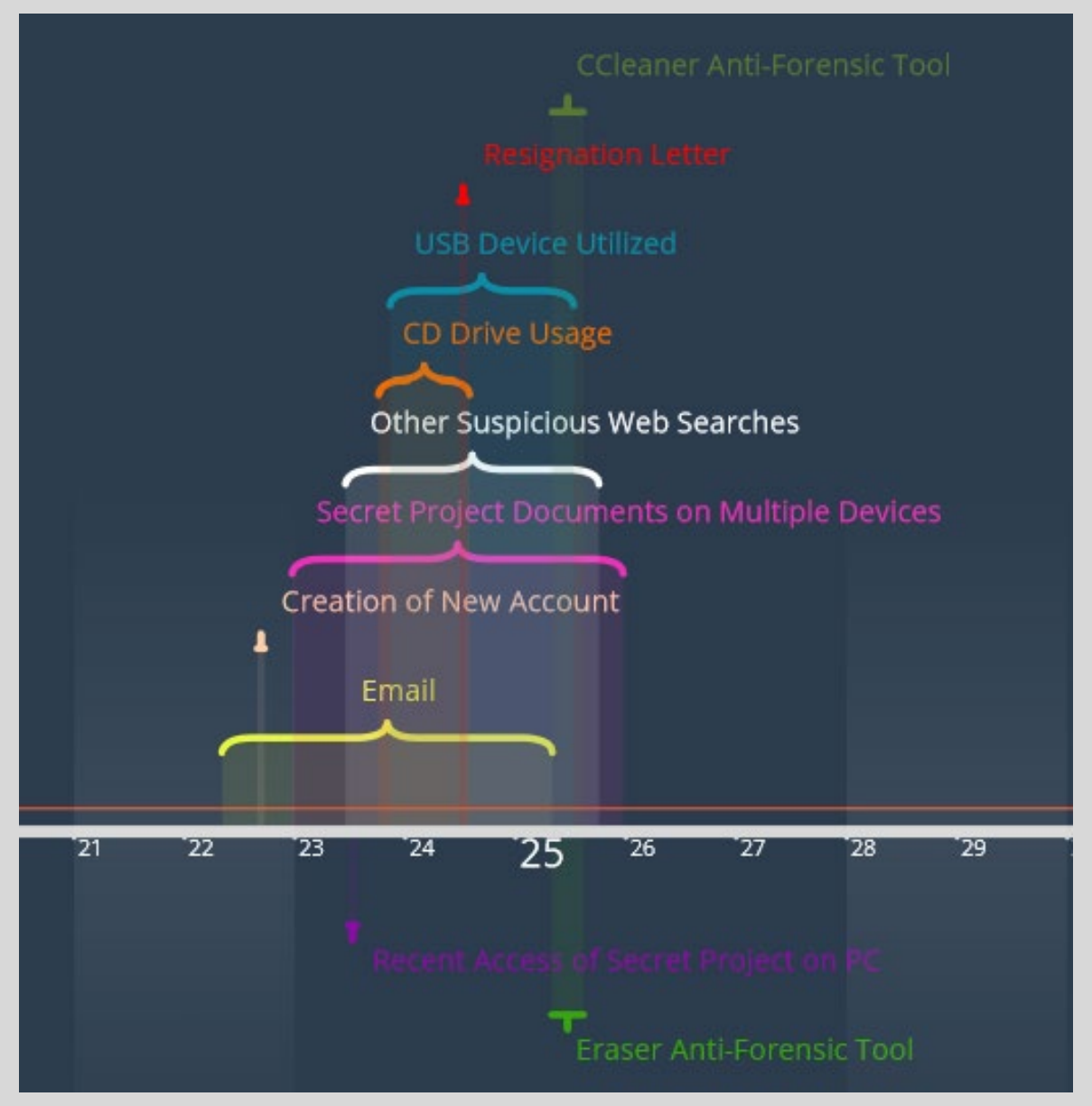




Documentation

The documentation can be done in a variety of ways. First, the investigator can keep a spreadsheet of all of the artifacts and the information that was recovered. From there, a timeline can be created illustrating when different events took place based off of the information found in the spreadsheet. A final report can be written specifically outlining the steps, programs utilized, and findings.



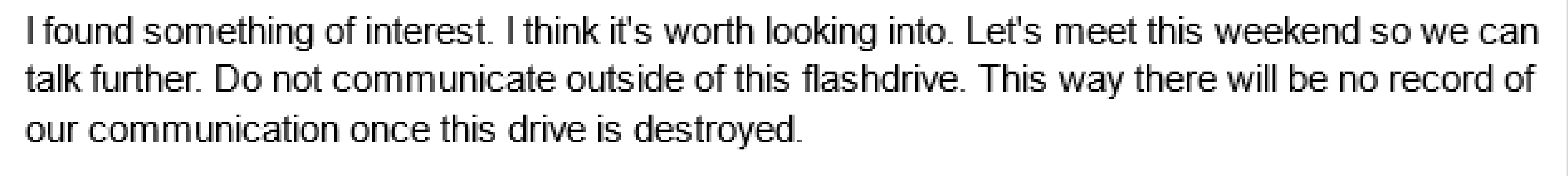

CCleaner Anti-Forensic Tool
Resignation Letter
USB Device Utilized
CD Drive Usage
Other Suspicious Web Searches
Secret Project Documents on Multiple Devices
Creation of New Account
Email
21
22
23
24
25
26
27
28
29
Recent Access of Secret Project on PC
Eraser Anti-Forensic Tool

Classroom Application

After learning about the different sources of information for a forensic investigation and the programs utilized to analyze said information, there was an opportunity to work backwards and create an investigation for students to participate in.

Context: lab equipment has been stolen from the University of Nevada, Reno

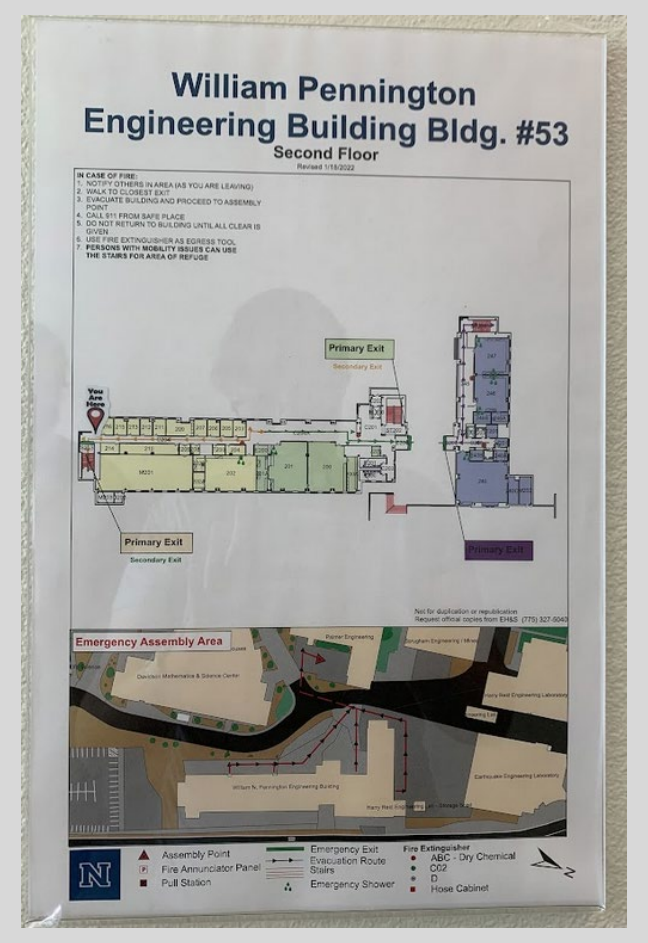
Question: put together a timeline of what happened leading up to the investigation and identify what was stolen using a USB that was found at the scene of the crime

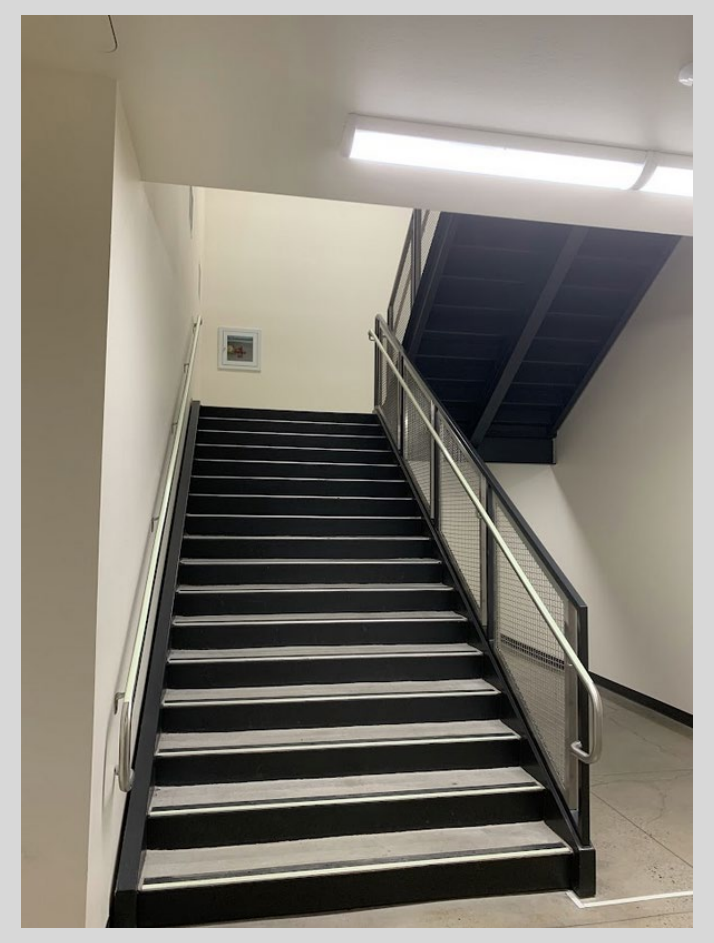


I found something of interest. I think it's worth looking into. Let's meet this weekend so we can talk further. Do not communicate outside of this flashdrive. This way there will be no record of our communication once this drive is destroyed.

Considerations that had to be made:

- Amount of artifacts that students can analyze
- Types of artifacts that will be available
- Any misleading information/artifacts
- Devices used to collect artifacts
  - How many collaborators are taking part in the "crime"?
- Creation of timeline when the "crime" took place
  - What dates/times were used for "casing" the lab where the equipment was taken from?
    - Which collaborator is responsible for which part at which time?
  - What dates/times would the "crime" actually take place?
- Collection of supporting documents/files to be included in the investigation
- Ability to scale up or scale down the investigation based on individual student/classroom needs
- Forensic tools that will be available to the studnets





This research is supported by NSF Award #1855159: RET Site: Research Experiences in Cybersecurity for Nevada Teachers (RECNT).