Final Practical Assignment

Jackson Nestler

University of Advancing Technology

Final Practical Assignment

For this assignment, our goal is to answer some critical questions about a cold case that opened recently, after nearly 30 years of being unsolvable. An interesting note is that the RP stated the device wouldn't be accessible until the year 2015. In theory, this means that the files should have last been modified on or about October 21, 1985, since the evidence hadn't been touched since. We're lucky to have made some amazing advances in digital forensics since 1985, having tools like FTK Imager and Autopsy at our fingertips should help this investigation quite a bit. The suspect allegedly partook in "nefarious activities" including drug trafficking, sexual exploitation of a minor, and murder.

I began by opening the E01 file in Autopsy, and ran all of the ingest modules except "Android Analysis," along with "Disk Encryption Detection." The ingest modules take an incredibly long time to run, but I was waiting for the "Recent Activity" module to run; this will give us an overview of evidence that's interesting to us, like web history and files such as PDFs, JPGs, etc. Upon finishing, the ingest showed that there's a lot of evidence to parse through.

Content	**Count**
Images	3,605
Videos	149
Audio	669
Archives	71
Databases	55
HTML	373
Plain Text/Rich Text	1,035/129

Office-Type	6
PDF	7

Additionally, we have some information about the device available to us.

Data Type	**Remarks**
Operating System	Windows 7 Home Basic
Number of Users	2 Users + 1 Guest + 1 Administrator
VM?	Yes, made with VMWare Product Family
Hostname	WIN-4GQCPGD6SQF

The case comes with some questions that previous detectives left behind. We'll step through those now. Autopsy was used for questions 3-14, FTK is utilized everywhere else unless noted.

1. Does the acquisition log contain a hash verification? Does the hash value verify?
    a. Yes it contains a hash verification. Yes it validates.
2. How many partitions are on the device?
    a. According to FTK Imager, there are two partitions: Partition 1 is 33138MB and is unnamed. It's formatted as NTFS. Partition 2 is 2000MB and formatted as FAT32, entitled "BUSINESS."
3. What file systems are each partition?
    a. Partition 1: NTFS.
    b. Partition 2: FAT32

4. What is the cluster size for each partition?
    a. NONAME (NTFS, Partition 1): 4,096
    b. BUSINESS (FAT32, Partition 2): 4,096
5. What is the cluster count on each partition?
    a. NONAME (Partition 1): 8,483,327
    b. BUSINESS (Partition 2): 510,976
6. What is the starting sector of each partition?
    a. NONAME (Partition 1): 2,048
    b. BUSINESS (Partition 2): 67,868,672
7. What is the sector count of each partition?
    a. NONAME: 67,866,624
    b. BUSINESS: 67,868,672
8. What are the volume labels of each partition?
    a. Partition 1: NONAME
    b. Partition 2: BUSINESS
9. What file is found at physical sector 6293504 and/or logical sector 6291456?
    a. It appears to be the Master File Table (MFT) record.
10. What user accounts are on each partition?
    a. Partition 1 (NONAME):
        i. Biff Tannen
        ii. Lorraine 1986B
        iii. Default User

   b. Partition 2 (BUSINESS): None

11. Document any notable files located in user accessible directories. Why are they notable?
    a. C:\Users\Biff Tannen\Desktop\Business.vhd - Virtual hard drive file, potentially contains information useful to the investigation.
    b. C:\Users\Biff Tannen\Desktop\uTorrent.lnk
        i. Has uTorrent installed, frequently used for piracy. This is **not** proof that a crime has been committed, but warrants further investigation.
    c. C:\Users\Biff Tannen\Desktop\My Journal Entries
        i. Contains 8 text files and their associated file slack. Seems to reference time travel ("a younger self.")
        ii. Files are dated throughout October and November 2015.
        iii. Fileslack indicates that CCleaner was used on these files.
        iv. In "15 MAR 1996.txt" there's reference to someone bringing their "younger self" to a penthouse on the 27th Floor of Pleasure Paradise. Possible inclination of sexual exploitation.
    d. C:\Users\Biff Tannen\Documents
        i. Contains a Wiki entry for a Back To The Future location.
    e. C:\Users\Biff Tannen\Downloads
        i. 7zip, Avast, CCLeaner, Gimp, and a Java binary are downloaded.

1. The FileSlack of the Java binary references the system time clock being interrupted every 10 seconds.

f. C:\Users\Biff Tannen\Google Drive

i. Offline cache of Google Drive.

ii. Contains images of, or for, promotion of the Pleasure Paradise, along with a photograph of an elder man. Possibly Biff Tannen.

g. C:\Users\Biff Tannen\Humor

i. Contains an MP4, an MP3, and a JPG image all relating to Biff Tannen.

h. C:\Users\Biff Tannen\My Programs

i. Exiftool, Hexedit, and FTK Imager Lite are notable executable files. Also TrueCrypt, Timestomp (a timestamp modification application), and uTorrent executables are present.

i. C:\Users\Biff Tannen\Pictures

i. "1955" Folder

1. Contains newspaper clippings from the Hill Valley Telegraph.

2. Photograph "my boys.jpg" seems to have a young Biff Tannen and two unidentified men.

3. Promotional poster for "Ooh La La", a music festival on Thursday, Sept 26.

ii. "1985" Folder

1. JPG of a Delorean

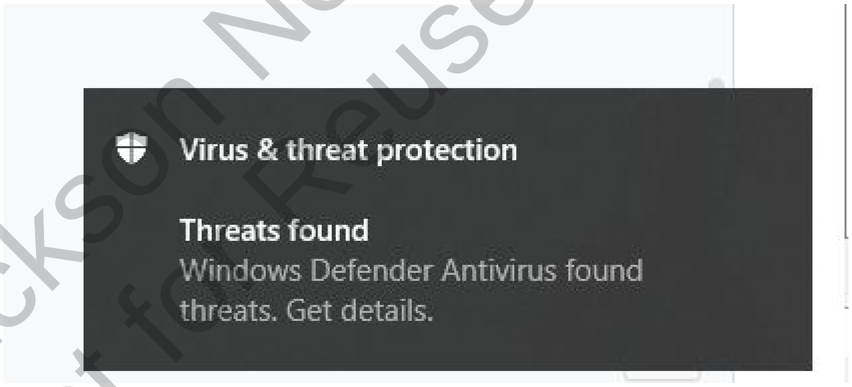
iii. “1985-B” Folder

1. Same images that were included in C:\Users\Biff Tannen\Google Drive.

iv. “2015” Folder

1. Some of the same images from C:\Users\Biff Tannen\Google Drive” are present.

j. In C:\Users\Biff Tannen\Videos, there’s a “Howard the Duck.exe” file that was erased by Windows Defender.[1]

i. 

Virus & threat protection

Threats found

Windows Defender Antivirus found threats. Get details.

k. C:\Users\Biff Tannen\Videos\Howard the Duck

i. Contains an AVI file that’s an animated video of Earth with some classical-sounding music.

l. C:\Users\Lorraine 1985B\

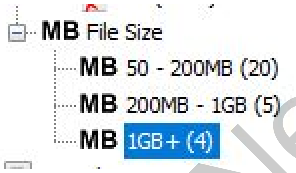
i. “Downloads” folder contains images of Lorraine from Back to the Future. File slack indicates these files were cleaned with CCleaner.

[1] I would prefer to avoid recovering this file - I added an exception in Defender for this file, but it was then immediately deleted again. For some reason it’s flagged as malware.

    ii. Favorites has links to various .gov domains. (GobineroUSA.gov, USA.gov)

12. Find any compound files (zip, docx, vhd).
    a. VHD: C:\Users\Biff Tannen\Desktop\Business.vhd
        i. Likely the VHD of the “Business” partition.
    b. $Recycle.bin
        i. Contains a deleted version of HexEdit
    c. Office files
        i. (Deleted) Compound_File.docx - Empty
        ii. (Deleted) Compound_Interest.docx - Empty
        iii. (Deleted) Compound_Interest_2.docx - Empty
        iv. Special Contract Ledger.xlsx
            1. Finances for “sales of designer RX for Biff’s Pleasure Paradise Backdoor”
        v. Compound_Interest.docx
            1. Asks to identify the top salesmen of 1985, and contains an image from what appears to be a news cast.
        vi. Compound_Interest_2.docx
            1. Asks “are there any messages from the boss?”
                a. Image has a reference to “Sector 2 has the key to my heart.”
    d. PDF

        i. Hill Valley Wiki.pdf - Previously referenced
        ii. Hill Valley Wiki.pdf - Second copy in Lorraine's user folder.
        iii. FTKImager_UserGuide.pdf - User guide that ships with FTK Imager.

13. Are there files over 1GB in size?
    a. Per Autopsy, there are 4 files that are 1GB+ in size, and 5 that are 200MB-1GB in size.
        i. 

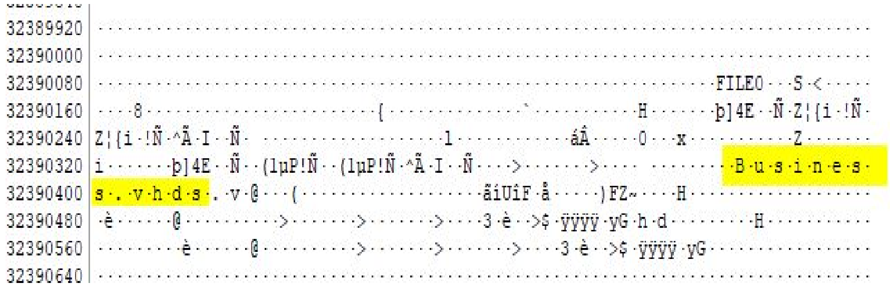
MB File Size
MB 50 - 200MB (20)
MB 200MB - 1GB (5)
MB 1GB+ (4)

    b. 1GB+ category contains pagefile.sys, Business.vhd, and $BadClus:$bad
        i. [2]$BadClus:$bad is "a sparse file which has the size equal to the size of the whole file system. A sparse file is a file of bigger size than actually allocated on the disk - it's filled with zeros and treated similarly to a compressed one. So even though it reports to have several gigs, it may have no space allocated at all."

14. How many bytes is each $MFT entry?
    a. Partition 1: 75,497,472 bytes.
    b. Partition 2: No $MFT file found.

15. What file is listed in the $MFT as record number 31,631?
    a. Business.vhd

[2] https://forum.piriform.com/topic/21594-badclusbad/

b. 

```
32389920 ································································
32390000 ································································
32390080 ··················································FILE0···S·<·····
32390160 ····8·····················{·············`··········H······þ]4E··Ñ·Z¦{i·!Ñ·
32390240 Z¦{i·!Ñ·^Ã·I··Ñ· ·················l···········áÂ····0···x·········Z·······
32390320 i·······þ]4E··Ñ··(1µP!Ñ··(1µP!Ñ·^Ã·I··Ñ···>·······>···· ········B·u·s·i·n·e·s·
32390400 s·.·v·h·d·s·.·v·@···(··················ãiÜîF·å·····)FZ~····H·················
32390480 ·è······@·········>·······>·······>····3·è··>$·ÿÿÿÿ·yG·h·d········H···········
32390560 ·········è······@·········>·······>·······>····3·è··>$·ÿÿÿÿ·yG················
32390640 ································································
```

16. What is the header signature for the Standard Information Attribute for every MFT entry?

    a. Either “FILE” or “BAAD”[3]

17. In the Standard Information Attribute, what is the hex value of the created time for MFT entry 31,631?

    a. Struggling to find this information. I looked around and found a Santa Clara University[4] entry about analyzing MFT, but wasn’t able to find relevant information.

18. In the Standard Information Attribute, what is the decoded value of the created time for MFT entry 31,631?

    a. Again struggling to find this information.

19. What is the header signature for the File Information Attribute for every MFT entry?

    a. I believe it’s “FILE 0” - **46 49 4C 45 30**

20. What is the hex value of the file name and extension for MFT entry 31,631?

    a. 42 00 75 00 73 00-69 00 6E 00 65 00 73 00 73

[3] http://www.c-jump.com/bcc/t256t/Week04NtfsReview/Week04NtfsReview.html#W01_0210_mft_entries
[4] http://www.cse.scu.edu/~tschwarz/coen252_07Fall/Lectures/NTFS.html

        i. “Business”

   b. 76 00 68 00-64 00 73

        i. “.vhd”

21. What is the ASCII value of the file name and extension at MFT entry 31,631?

    a. Business.vhd

22. How many data streams are there for MFT entry 31,631?

    a. Not sure about the answer to this. Guidance would be appreciated!

23. Is this file resident or non-resident?

    a. Resident. This is because the file’s information fits within the MFT entry. [5]

24. What is the offset of the first run list?

    a. Runlists for non-resident files is at bytes 32-33.

        i. “Then there's an offset to the runlist at bytes 32-33. The runlist is in the following format. First there's a single byte that describes the length and offset of the next run; then there's a variable number of bytes describing the length of the run, and a variable number of bytes describing the offset to the run.” (Liberatore, 2017)

    b. It looks like the offset is 0040800.

25. How many run lists are there for this entry? Is the file fragmented or contiguous?

    a. In this MFT, there are 73,727 entries.

[5] https://www.ntfs.com/ntfs-files-types.htm

b. Used an MFT analysis tool.[6]

26. List all the run lists for this entry.

    a. I've included a CSV with the

27. What is the run list header value?

    a. 0x21[7]

28. What is the hexadecimal value of the fragment size in clusters?

    a. Not entirely sure what the question is here. The hexadecimal value is easy to grab, but the fragment size in clusters is foreign to me. It's not a full file (therefore fragmented), but is the question asking what the size of the file is, or which sector it starts/ends at?

29. What is the decimal value of the fragment size in clusters?

    a. Same as above -- could convert hex to decimal once found.

30. What is the starting cluster of the run list in hexadecimal and decimal?

    a. I imagine question 28 needs to be found before this can be found.

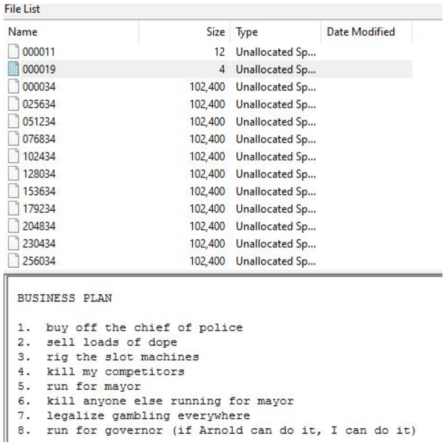
31. What is the file signature of the file starting at logical cluster 2,375,311?

    a. 4D 5A - This is a DLL file.

Interesting Evidence Points

- In the unallocated space of the drive, there's a reference at offset 00200: "MY WINDOWS PW lorraine". At 0230: "MY VHD PW kill-mcfly". At 260: "My vhd is hidden in a zip file...heheheheheh!!!"

[6] https://github.com/dkovar/analyzeMFT
[7] https://flatcap.org/linux-ntfs/ntfs/concepts/data_runs.html

- In the unallocated space of partition 2, there’s a business plan:
    - 

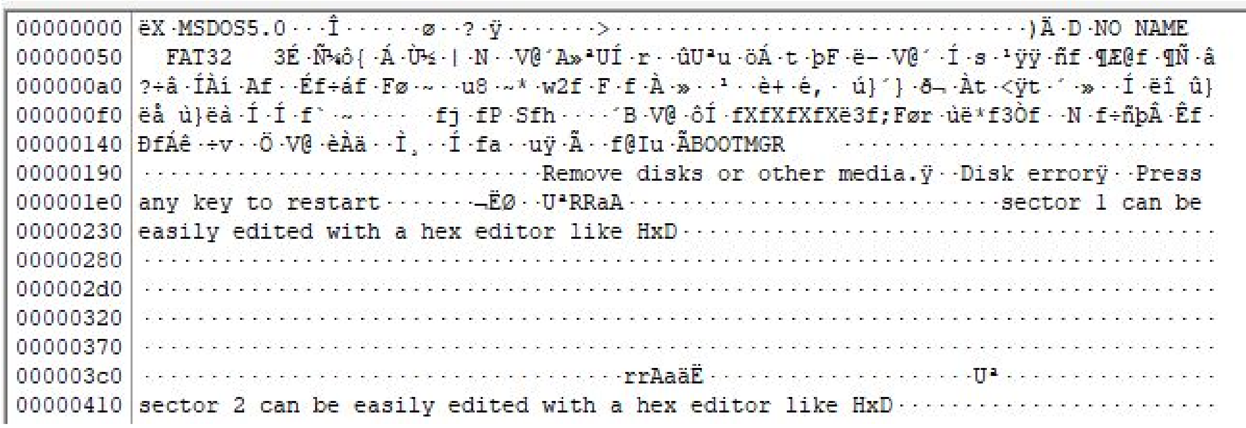
File List

Name	Size	Type	Date Modified
000011	12	Unallocated Sp...	
000019	4	Unallocated Sp...	
000034	102,400	Unallocated Sp...	
025634	102,400	Unallocated Sp...	
051234	102,400	Unallocated Sp...	
076834	102,400	Unallocated Sp...	
102434	102,400	Unallocated Sp...	
128034	102,400	Unallocated Sp...	
153634	102,400	Unallocated Sp...	
179234	102,400	Unallocated Sp...	
204834	102,400	Unallocated Sp...	
230434	102,400	Unallocated Sp...	
256034	102,400	Unallocated Sp...	

```
BUSINESS PLAN

1.  buy off the chief of police
2.  sell loads of dope
3.  rig the slot machines
4.  kill my competitors
5.  run for mayor
6.  kill anyone else running for mayor
7.  legalize gambling everywhere
8.  run for governor (if Arnold can do it, I can do it)
```

- In C:\Users\Biff Tannen\Desktop\My Journal Entries, there’s a text file called “26 MAR 1958.txt”
    - This file contains the following: “...young biff said, ‘If I see em, kill em’ That’s right, I said. That’s right.”
    - Shows intent to commit murder.
- An image said “Sector 2 contains the key to my heart.”
    - At sector 2 of partition 2 (“BUSINESS”), there’s a note that says “Sector 1 can be easily edited with a hex editor like HxD.” Further down is an entry for “sector 2 can be easily edited with a hex editor like HxD.”
    - Potentially destroying or modifying evidence.

- 

```
00000000 ëX·MSDOS5.0···Î······ø··?·ÿ·······>······························)Ä·D·NO NAME
00000050   FAT32   3É·Ñ¬¼ô{·Á·Ù¼·|·N··V@´A»ªUÍ·r··ûUªu·öÁ·t·þF·ë–·V@´·Í·s·¹ÿÿ·ñf·¶Æ@f·¶Ñ·â
000000a0 ?÷â·ÍÀí·Af··Éf÷áf·Fø·~··u8·~*·w2f·F·f·À·»··¹··è+·é,· ú}´}·ð¬·Àt·<ÿt·´·»··Í·ëî û}
000000f0 ëå ù}ëà·Í·Í·f`·~·····fj·fP·Sfh····´B·V@·ôÍ·fXfXfXfXë3f;Før·ùë*f3Òf··N·f÷ñþÂ·Êf·
00000140 ÐfÁê·÷v··Ö·V@·èÀä··Ì¸··Í·fa··uÿ·Ã··f@Iu·ÃBOOTMGR  ·····························
00000190 ·······························Remove disks or other media.ÿ··Disk errorÿ··Press
000001e0 any key to restart·······¬Ëø··UªRRaA···························sector 1 can be
00000230 easily edited with a hex editor like HxD········································
00000280 ································································································
000002d0 ································································································
00000320 ································································································
00000370 ································································································
000003c0 ·······································rrAaäË····················Uª·················
00000410 sector 2 can be easily edited with a hex editor like HxD························
```

- Many deleted files, including what could have been credentials.
  - C:\Users\Biff Tannen\Downloads\GmailPassword.docx
  - C:\Users\Biff Tannen\Desktop\my secret.txt
  - C:\Users\Biff Tannen\Desktop\Special Files.vhd
  - C:\Users\Biff Tannen\Desktop\Sector 2.txt
  - C:\Users\Biff Tannen\Pictures\1985-B\My-Secret.png
- USB drives were inserted previously. Appear to be Kingston drives.
  - File accessed: E:\Sales Team.jpg
  - File accessed: E:\The Boss.jpg
- Google Drive files were previously accessed.
  - Supporting evidence: Google Drive's sync utility attempts to mount at mountpoint G:\
  - Previously accessed: G:\Compound_Interest.docx
  - Previously accessed: G:\Compound_Interest_2.docx
  - Previously accessed: G:\Business Plan.txt

What evidence did you find to support the alleged crime of drug trafficking?

- The business plan found in the unallocated space of the disk references "sell loads of dope."
- This is nowhere near enough for a warrant, much less being charged or going to trial. It's something to consider, though.

What evidence did you find to support the alleged crime of sexual exploitation as a minor?

- As with the previous allegation, there's not much to go off of.
- On Bill's desktop is a text file containing reference to taking his "younger self" to the penthouse suite of "Pleasure Paradise" and having a talk. Lorraine called younger Bill a "sl*t," perhaps indicating something sexual has, or was going to occur.

What evidence did you find to support the alleged crime of homicide?

- Several references to killing people in the journal entries. These people include "younger Bill" and anyone that gets in his way.
- Business plan involves murdering anyone that runs for mayor.
- Perhaps enough to perform further investigation.

Conclusion

This device is certainly interesting. The timestamps don't match up with the RP stating that it wouldn't be accessible until 2015; it's highly likely that our time traveling suspect has utilized this device since it was stored in evidence. Problems of space-time continuity aside, law enforcement should follow up with Bill and his associates. It's likely that Bill committed crimes in the past, including murder and trafficking of narcotics. Bill went to great lengths to avoid digital investigators from finding data, including wiping some data with CCleaner (a file cleanup utility that can “shred” data from drives). He knew forensicators would be looking at his machine and left easter-eggs behind.

References

B, M. (2017, February 4). A Journey into NTFS: Part 6. Retrieved from https://medium.com/@bromiley/ntfs-part-6-43a50fad89f3

CCleaner Community Forum. (2009, April 22). $BadClus:$Bad. Retrieved from https://forum.piriform.com/topic/21594-badclusbad/

C-Jump. (n.d.). NTFS File System Overview. Retrieved from http://www.c-jump.com/bcc/t256t/Week04NtfsReview/Week04NtfsReview.html#W01_0210_mft_entries

Flatcap. (n.d.). $STANDARD_INFORMATION (0x10) - Attribute - NTFS Documentation. Retrieved from https://flatcap.org/linux-ntfs/ntfs/attributes/standard_information.html

Kessler, G. (2019, August 25). File Signatures. Retrieved from https://www.garykessler.net/library/file_sigs.html

Liberatore, M. (2017). 13: Introduction to NTFS | COMPSCI 365/590F | Digital Forensics (Spring 2017). Retrieved from https://people.cs.umass.edu/~liberato/courses/2017-spring-compsci365/lecture-notes/13-introduction-to-ntfs/

NTFS File Types. (n.d.). Retrieved from https://www.ntfs.com/ntfs-files-types.htm