

The Curious Case of Alice and Bob:

What You Can (And Cannot!) Do as Digital Investigators



Agenda

- Introduction
- Understanding the investigative process
- Scoping
- Data gathering
- Data analysis
- Data correlation
- Timeline analysis
- Post incident

Introduction

@investigatorchi



Dr. Catherine J. Ullman

- Principle Technology Architect, Security - University at Buffalo
- Staff: BSidesROC, UB GenCyberCamp, PHV/DEFCON, BSidesLV
- Volunteer: CPTC, Skytalks, CCDC, BlueTeamCon
- Speaker: PHV/DEFCON, BTV, GrrCON, Diana Initiative, BlueTeamCon, Cyphercon, BSides Buffalo
- Loves sloths (see photo of adopted sloth, Flash, above)

Understanding the Investigative Process

What is forensic science?

- Application of science to criminal and civil laws



Edmund Locard (1877 – 1966)

- French criminologist
- Considered a pioneer of forensic science and criminology
- Contributed substantial research to dactylography (the study of fingerprints)



Locard’s Exchange Principle

"It is impossible for a criminal to act, especially considering the intensity of a crime, without leaving traces of this presence.“

- Every contact leaves a trace.
- Trace, for digital forensics, often involves logs.



What is Digital Forensics?

- A branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.



- *The goal is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.”*

Digital Forensics Process

- Acquire the evidence without altering or damaging the original
  - Chain of custody required
  - Write blockers often used
- Authenticate the image (copy)
- Analyze the data without modifying it



Print Form

PROPERTY / EVIDENCE CHAIN OF CUSTODY FORM

APLCS, LLC (http://www.aplcs.com)

Case Name:		**Reason Obtained:**	
Case Number:			
Item Number:	**Evidence Type / Manufacturer:**	**Model Number:**	**Serial Number:**
Content Owner / Title:	**Content Description:**		
Content Owner Contact Information:			
Forensic Agent:	**Creation Method:**	**HASH Value:**	**Creation Date/Time:**
Forensic Agent Contact Information:			

CHAIN OF CUSTODY

Tracking Number	Date / Time	Released By	Received By	Reason for Change
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	

Item Number: _____ **Page: 1 of** _____

Traditional vs. Digital Forensics

Traditional

- Evidence can be changed/destroyed for testing

Digital

- Evidence can not be changed/destroyed during testing

Investigative Process

- Incident scope
- Data gathering
- Data analysis
- Data correlation
- Timeline analysis
- Post incident/Reporting



A Meeting of the Minds

The Scoping Call



Scoping Goals

- Summary of the incident
- Details about the affected individuals
- Timestamps of key events
- Details around the incident
- Objectives (what is requested?)



Bob is dead!



- The police were called to 456 Central Ave, home of Bob Byte where Bob is found deceased at 12:01am on February 13, 2022. His time of death is estimated to be about three hours earlier.
- Initial reports suggest he was stabbed. Bob is known to have a pre-existing relationship with someone named Alice Ascii who lives at 123 Main St.
- The police believe that Alice went to Bob's house and killed him.
- You have been asked to work with the team to investigate the relevant digital equipment to prove Alice's involvement.



Objectives

The police have asked you to perform an analysis on the relevant digital evidence. As part of this analysis, they would like answers to the following:

1. What evidence exists that proves Alice killed Bob?
2. Why did Alice kill Bob?

Scoping Challenges

- Open-ended questions
- Questions not meant for digital forensics
- Incorrect assumptions
- Unrealistic time frames
- Recovery limitations
- Evidence scope too large
- Incomplete requests

Revised Objectives

1. Any activity around time of death?
2. Any evidence to indicate person(s) involvement?
3. Retrieve all relevant digital communications between Alice and Bob.



Data Gathering

Data Gathering Goals

- Gather all relevant data to meet objectives in scoping call
  - Note: Data may not always be digital
- Data examples
  - Forensic image(s)
  - Security consoles
  - Log files
  - Virtual file systems
  - Triage script output
  - Password(s)

Tools for Data Gathering

- Forensic tools
  - FTK Imager, EnCase, X-ways, Magnet AXIOM, Magnet GREYKEY, Cellebrite Collector, Paladin, Autopsy, write blocking hardware/software
- Triage scripts
  - Velociraptor, KAPE, Trident
- Photographs/Video (without sound)
- Old fashioned paper/pen



Name: iPhone
Software Version: 11.2.5 15D60
Model: iPhone10,3 D22AP
UDID: 32a57641ee0cbe4fd12361ec2273cfa81825fcfd
Unique Chip ID: 687929281651770
Lock status: Before-first-unlock
Found passcode: 987987

Results

Type	Size	SHA256
iTunes Backup	107M	eac6cd344974982c50351033c8a1da489943e4eb49474b6163052600e5d43410
Full Filesystem	3.18G	ae83f4031c519029c52c23b0bb707a4daac9f2975c6c7bcd93338908e5d05480

AccessData FTK Imager 4.5.0.3

File View Mode Help

Evidence Tree

\\.\PHYSICALDRIVE0
- EFI system partition (1) [500MB]
- Microsoft reserved partition (2) [128MB]
- Basic data partition (3) [966367MB]
  - Unrecognized file system [Data]
- Basic data partition (4) [9763MB]
- Unpartitioned Space [GPT]

File List

Name	Size	Type	Date Modified
unallocated space	989,559,808	Unallocated Sp...	

```
0000000000 EB 58 90 2D 46 56 45 2D-46 53 2D 00 02 08 00 00 ëX·-FVE-FS-·····
0000000010 00 00 00 00 00 F8 00 00-3F 00 FF 00 00 A8 13 00 ·····ø··?·ÿ··¨··
0000000020 00 00 00 00 E0 1F 00 00-00 00 00 00 00 00 00 00 ····à···········
0000000030 01 00 06 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000040 80 00 29 00 00 00 00 00-4E 4F 20 4E 41 4D 45 20 20 ··)····NO NAME
0000000050 20 20 46 41 54 33 32 20-20 20 33 C9 8E D1 BC F4   FAT32   3É·Ñ¼ô
0000000060 7B 8E C1 8E D9 BD 00 7C-A0 FB 7D B4 7D 8B F0 AC {·Á·Ù½·| û}´}·ð¬
0000000070 98 40 74 0C 48 74 0E B4-0E BB 07 00 CD 10 EB EF ·@t·Ht·´·»··Í·ëï
0000000080 A0 FD 7D EB E6 CD 16 CD-19 00 00 00 00 00 00 00  ý}ëæÍ·Í······
0000000090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000000a0 3B D6 67 49 29 2E D8 4A-83 99 F6 A3 39 E3 D0 01 ;ÖgI).ØJ··ö£9ãÐ·
00000000b0 00 90 8E 40 01 00 00 00-00 90 8F 40 01 00 00 00 ···@·····@····
00000000c0 00 90 90 40 01 00 00 00-00 00 00 00 00 00 00 00 ···@············
00000000d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000000e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000000f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000100 0D 0A 52 65 6D 6F 76 65-20 64 69 73 6B 73 20 6F ··Remove disks o
0000000110 72 20 6F 74 68 65 72 20-6D 65 64 69 61 2E FF 0D r other media.ÿ·
0000000120 0A 44 69 73 6B 20 65 72-72 6F 72 FF 0D 0A 50 72 ·Disk errorÿ··Pr
0000000130 65 73 73 20 61 6E 79 20-6B 65 79 20 74 6F 20 72 ess any key to r
0000000140 65 73 74 61 72 74 0D 0A-00 00 00 00 00 00 00 00 estart·········
0000000150 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000160 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000170 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000180 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000190 00 00 00 00 00 00 00 00-78 78 78 78 78 78 78 78 ········xxxxxxxx
00000001a0 78 78 78 78 78 78 78 78-78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxx
00000001b0 78 78 78 78 78 78 78 78-78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxx
00000001c0 78 78 78 78 78 78 78 78-78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxx
00000001d0 78 78 78 78 78 78 78 78-78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxx
00000001e0 78 78 78 78 78 78 78 78-FF FF FF FF FF FF FF FF xxxxxxxxÿÿÿÿÿÿÿÿ
00000001f0 FF FF FF FF FF FF FF FF-FF FF FF 00 1F 2C 55 AA ÿÿÿÿÿÿÿÿÿÿÿ··,U²
0000000200 48 14 1D 29 18 B6 4F EE-75 C7 F2 82 23 BE 44 BC H··)·¶OîuÇò·#¾D¼
0000000210 87 6A 76 5C 8E 18 5D 83-3B 0D 8B A5 F4 DF A8 FE ·jv\··]·;··¥ôß¨þ
0000000220 F1 03 C2 AA 7F 98 C7 7D-1D 43 35 45 33 E4 68 97 ñ·Âª··Ç}·C5E3äh·
0000000230 45 93 F8 1C 44 AD 8C EF-2D 4B 3A 9F 2C 68 77 92 E·ø·D-·ï-K:·,hw·
0000000240 21 A9 33 C1 FC FB D8 E7-8B C4 93 83 4D C0 B6 60 !©3ÁüûØç·Ä·ÀM¶`
0000000250 4F 25 41 96 7D 85 FF F7-7D 85 45 A6 30 93 C5 B9 O%A·}·ÿ÷}·E¦0·Å¹
0000000260 A1 36 61 EC 0C 18 9F E0-BC 2D 00 D1 2D D7 14 06 ¡6aì···à¼-·Ñ-×··
0000000270 F4 CC C5 2E B3 01 7B 0A-6E 23 9E 39 F6 08 C8 1F ôÌÅ.³·{·n#·9ö·È·
0000000280 7B A7 39 6B 1B 86 2B B1-06 FE 1C 07 0B 40 35 5E {§9k··+±·þ···@5^
0000000290 70 FF E9 3D 70 70 3A 29-26 2F 9F 58 EC 75 CC 9A pÿé=pp:)&/·XìuÌ·
```

Custom Content Sources

Evidence:File System|Path|File	Options

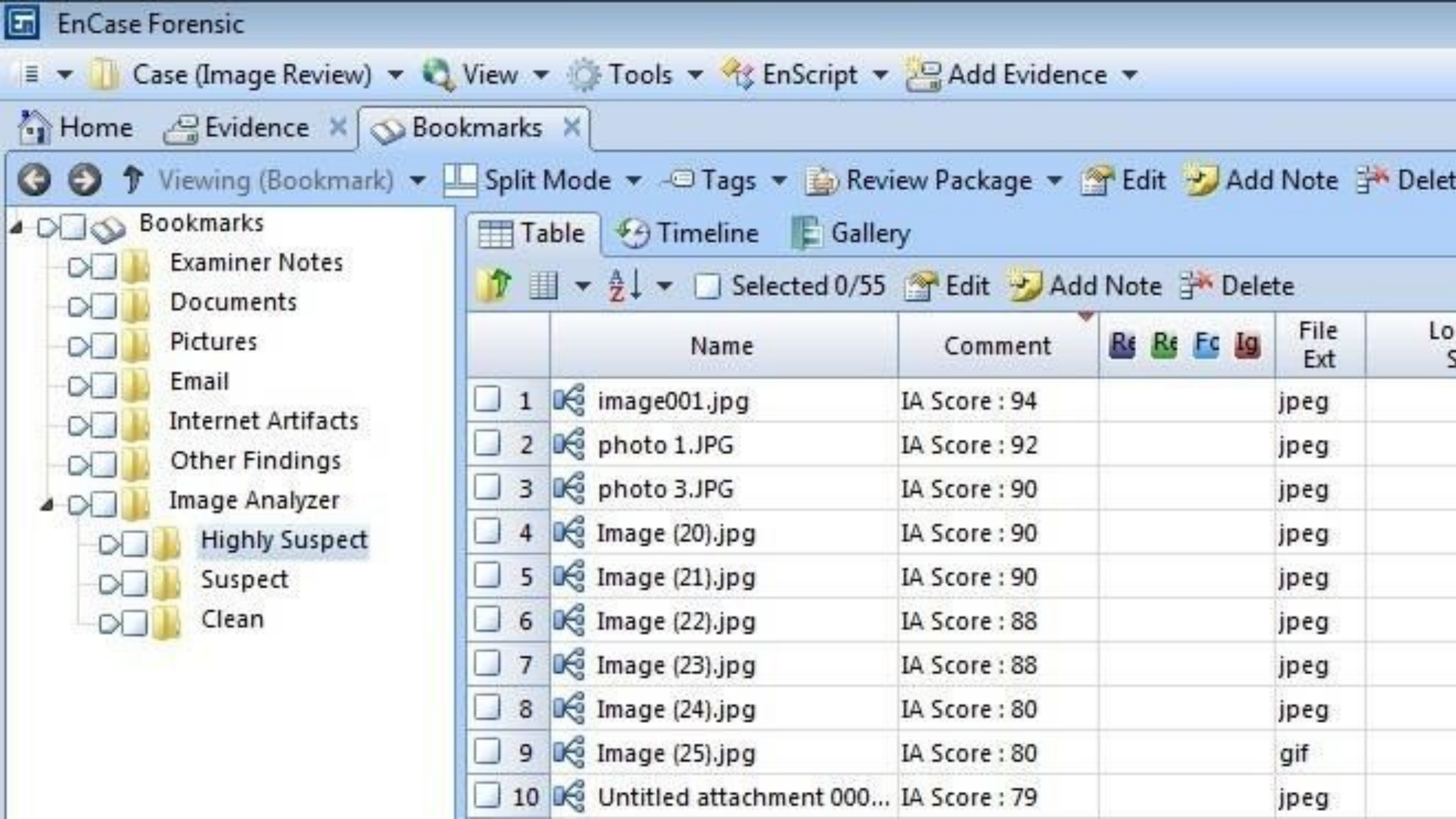
New Edit Remove Remove All Create Image

Properties | Hex Value Inter... | Custom Conte...

Cursor pos = 0; log sec = 0; phy sec = 1288192

Listed: 1 Selected: 0 \\.\PHYSICALDRIVE0/Basic data partition (3) [966367MB]/Unrecognized file system [Data]

NUM


EnCase Forensic
Case (Image Review)
View
Tools
EnScript
Add Evidence
Home
Evidence
Bookmarks
Viewing (Bookmark)
Split Mode
Tags
Review Package
Edit
Add Note
Bookmarks
Examiner Notes
Documents
Pictures
Email
Internet Artifacts
Other Findings
Image Analyzer
Highly Suspect
Suspect
Clean
Table
Timeline
Gallery
Selected 0/55
Edit
Add Note
Delete
Name
Comment
File Ext
1 image001.jpg IA Score : 94 jpeg
2 photo 1.JPG IA Score : 92 jpeg
3 photo 3.JPG IA Score : 90 jpeg
4 Image (20).jpg IA Score : 90 jpeg
5 Image (21).jpg IA Score : 90 jpeg
6 Image (22).jpg IA Score : 88 jpeg
7 Image (23).jpg IA Score : 88 jpeg
8 Image (24).jpg IA Score : 80 jpeg
9 Image (25).jpg IA Score : 80 gif
10 Untitled attachment 000... IA Score : 79 jpeg

Hacking_Case - Autopsy 4.17.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Discovery | Generate Report | Close Case | Keyword Lists

Data Sources
- 4Dell Latitude CPi.E01
  - vol1 (Unallocated: 0-62)
  - vol2 (NTFS / exFAT (0x07): 63-9510479)
    - $OrphanFiles (0)
    - $CarvedFiles (1006)
    - $Extend (5)
    - $Unalloc (4)
    - Documents and Settings (7)
    - My Documents (11)
    - Program Files (36)
    - RECYCLER (3)
    - System Volume Information (3)
    - Temp (2)
    - WIN98 (103)
    - WINDOWS (109)
  - vol3 (Unallocated: 9510480-9514259)

Views
- File Types
- Deleted Files
- File Size

Results
- Extracted Content
  - Encryption Suspected (2)
  - Extension Mismatch Detected (9)
  - Installed Programs (32)
  - Metadata (10)
  - Operating System Information (2)

Listing

/img_4Dell Latitude CPi.E01/vol_vol2

Table | Thumbnail | Summary

Save Table

Name	S	C	Modified Time	Change Time	Access Time	Created Time
$OrphanFiles			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
$CarvedFiles			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
$Extend			2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43
$Unalloc			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
[current folder]			2004-08-26 21:16:18 IST	2004-08-27 20:38:18 IST	2004-08-27 20:38:05 IST	2004-08-19 22:27:43
Documents and Settings			2004-08-20 04:34:05 IST	2004-08-20 04:34:05 IST	2004-08-27 20:38:05 IST	2004-08-19 22:29:01
My Documents			2004-08-20 20:51:05 IST	2004-08-20 20:51:05 IST	2004-08-20 20:51:09 IST	2004-08-18 22:25:24
Program Files			2004-08-27 20:58:49 IST	2004-08-27 20:58:49 IST	2004-08-27 20:59:18 IST	2004-08-18 22:01:52
RECYCLER			2004-08-25 21:48:25 IST	2004-08-25 21:48:25 IST	2004-08-27 20:42:30 IST	2004-08-25 21:48:25
System Volume Information			2004-08-20 04:23:09 IST	2004-08-20 04:23:09 IST	2004-08-27 20:38:06 IST	2004-08-20 04:23:08

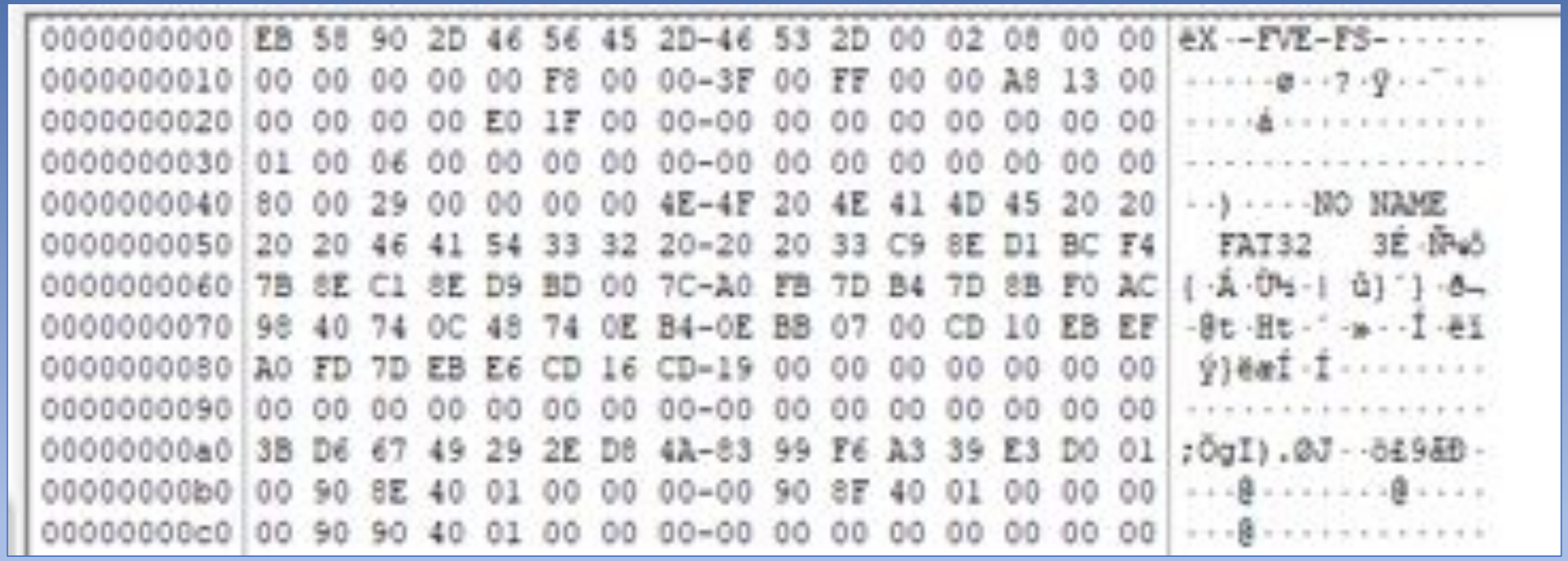
Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences

Related Questions

- Should we prioritize any data source over any other (e.g. instant messaging vs. email, web searches vs. documents)
- Was anything interesting observed on-scene (e.g. passwords on paper or verbally stated)
- Any restrictions on time for initial analysis?

Data Gathering Challenges

- Acquiring unnecessary data
- Necessary data unavailable
- Necessary data inaccessible
- Inability to obtain data in a forensically sound manner
- Unrealistic time frames to gather data
- ISO or other regulations
- Incompatible collection method/undersized media
- Inappropriate file systems for collection purposes



```
0000000000 EB 58 90 2D 46 56 45 2D-46 53 2D 00 02 08 00 00 ëX·-FVE-FS-·····
0000000010 00 00 00 00 00 F8 00 00-3F 00 FF 00 00 A8 13 00 ·····ø··?·ÿ··¨··
0000000020 00 00 00 00 E0 1F 00 00-00 00 00 00 00 00 00 00 ····à···········
0000000030 01 00 06 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000040 80 00 29 00 00 00 00 4E-4F 20 4E 41 4D 45 20 20 ··)····NO NAME  
0000000050 20 20 46 41 54 33 32 20-20 20 33 C9 8E D1 BC F4   FAT32   3É·Ñ¼ô
0000000060 7B 8E C1 8E D9 BD 00 7C-A0 FB 7D B4 7D 8B F0 AC {·Á·Ù½·| û}´}·ð¬
0000000070 98 40 74 0C 48 74 0E B4-0E BB 07 00 CD 10 EB EF ·@t·Ht·´·»··Í·ëï
0000000080 A0 FD 7D EB E6 CD 16 CD-19 00 00 00 00 00 00 00  ý}ëæÍ·Í·······
0000000090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000000a0 3B D6 67 49 29 2E D8 4A-83 99 F6 A3 39 E3 D0 01 ;ÖgI).ØJ·ö£9ãÐ·
00000000b0 00 90 8E 40 01 00 00 00-00 90 8F 40 01 00 00 00 ···@·····@····
00000000c0 00 90 90 40 01 00 00 00-00 00 00 00 00 00 00 00 ···@············
```



Data Analysis

Data Analysis Goals

- Looking for scoped indicators – e.g. Hostnames, IP address/domains, user accounts
- Leads – a piece of data that may guide you to answer the objective (e.g. keywords, names, etc.)
- Pivots – a piece of data that moves you to another source
- Document findings – Timestamp (UTC), Event Description, Evidence Source (Including query or procedure), Context (Who, what, where, when, why), Code (Filepath, registry entry, command)
- Document lack of findings – Lack of evidence is itself evidence

Tools for Data Analysis

- Magnet AXIOM, GRAYKEY
- Autopsy
- Eric Zimmerman’s collection (Timeline Explorer, EvtxECmd, Registry Explorer, etc.)
- Obsidian Forensics Hindsight
- EnCase, Xways, FTK, Nuix
- Cellebrite Inspector
- Volatility

Cellebrite Physical Analyzer 7.68.0.25

File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks

Commander Search Advanced

Home | Transfer | Analyzed Data | File Systems | Insights | Tags | Reports | Cloud

[redacted] | Welcome | Extraction Summary (2)

All Content | File System | Physical

Extraction Summary

+ Add extraction | Add external file | Project settings | Generate report | Open Virtual Analyzer

Extractions: 2

File System
samsung SM-J330F
File System [Android ADB]
Extraction start date/time [redacted]
Extraction end date/time [redacted]

Image Hashes
Hash data is available for this extraction.
Verify image hash

Physical
samsung SM-J330F
Physical [Android ADB]
Extraction start date/time [redacted]
Extraction end date/time [redacted]

Image Hashes
Hash data is available for this extraction.
Verify image hash

Insights from Installed Apps

- Chat applications (11 apps)
- Clean mobile (6 apps)
- Hide files or pictures (4 apps)
- Browser (4 apps)
- Games (468 apps)
- Entertainment (62 apps)
- Developer tools (51 apps)
- Utilities (43 apps)

View all

Case Information

Examiner	2
Exhibit Description	2
Exhibit Seized By	2
Exhibit Seized Time	2
OIC / Division	2
Notes	Cellebrite processing [redacted]
Victim / Witness	No
Exhibit Seized Location	2
Exhibit Seized Date	2
Operation / Reference	2
FURN	2

Device Info

Generate preliminary device report

Physical

Advertising ID #1	[redacted]	adid_settings.xml : 0x5B
Android fingerprint	[redacted]	build.prop : 0x5C1
Bluetooth MAC Address	[redacted]	bt_addr : 0x0
Chipset	[redacted]	Taken from UFD extraction file
Android ID	[redacted]	settings_secure.xml : 0x9AC4
Bluetooth device address	[redacted]	settings_secure.xml : 0x7720
Bluetooth device name	Galaxy J3	settings_secure.xml : 0x4C88
Carrier Name	[redacted]	telephony.db : 0x3FB8
Carrier Name	[redacted]	telephony.db : 0x3E75
Current SIM Country ISO	[redacted]	SimCard.dat : 0x9F
Current SIM Operator	[redacted]	SimCard.dat : 0x85
Current SIM Operator Name	[redacted]	SimCard.dat : 0xD2
Current SIM Phone Number	[redacted]	SimCard.dat : 0x11C
Detected Phone Model	SM-J330F	build.prop : 0x31A
Detected Phone Vendor	samsung	build.prop : 0x324
Location Services Enabled	True	googlesettings.db : 0x3F10
Mock locations allowed	False	
OS Version	9	build.prop : 0x144
SIM Change Operation	3	SimCard.dat : 0x159
Device model	SM-J330F	Taken from UFD extraction file
Factory number	[redacted]	serial_no : 0x0
ICCID	[redacted]	SimCard.dat : 0x12
ICCID	[redacted]	telephony.db : 0x9 C2
ICCID	[redacted]	telephony.db : 0x3F9A
ICCID	[redacted]	telephony.db : 0x3E5A
IMEI	[redacted]	2400257.cfg : 0x100
IMEI1	[redacted]	Taken from UFD extraction file
IMEI2	[redacted]	Taken from UFD extraction file
IMSI	[redacted]	simprof.preferences_name.xml : 0x146
Mac Address	[redacted]	mac.info : 0x0
Model	SM-J330F	Taken from UFD extraction file
OS	Android 9	Taken from UFD extraction file
Recovery Mode Event	[redacted]	tmp_recovery.log : 0x3B
Security Patch Level	[redacted]	Taken from UFD extraction file
SIM Change Time	[redacted]	SimCard.dat : 0x138
Vendor	samsung	Taken from UFD extraction file

Content

Data

Autofill 2926	Calendar 4	Call Log 1974 (296)	Cell Towers 1252	Chats 258 (46)
Contacts 651 (68)	Cookies 1051 (8)	Device Connectivity 4	Device Events 10 (1)	Device Locations 7970
Device Notifications 184	Device Users 2	Devices 4	Downloads 50	Emails 502
Installed Applicati... 3848	Instant Messages 1009 (29)	Network Usages 7122	Notes 2	Passwords 3600 (2)
Searched Items 724 (144)	Social Media 810	User Accounts 74	Web Bookmarks 14	Web History 5592
Wireless Networks 15971				

Data Files

Applications 4444 (802)	Archives 404 (60)	Audio 3620 (290)	Configurations 75 (2)	Databases 1929 (17)
Documents 4	Images 116628 (2421)	Shortcuts 20	Text 18756 (7139)	Uncategori... 129418 (24600)
Videos 199 (35)				

Magnet AXIOM Examine v7.0.0.35443 [redacted]

File Tools Process Help

Case dashboard

CASE OVERVIEW

EVIDENCE SOURCES 2

L:\

[redacted]files_full.zip

INSIGHTS

Potential Cloud Evidence Leads 45

CASE OVERVIEW

CASE SUMMARY NOTES

Record your case summary notes here. These notes will appear in the case report when the setting is enabled.

Examiner name

Case summary

CASE PROCESSING DETAILS

CASE NUMBER 1782021181_48

SCAN 1

Scanned by

Scan date/time - local time [redacted]

Scan description

CASE INFORMATION

The Case Information.txt file contains information about how the case was processed. For example, the file includes the settings that were applied to the search, search type, number of artifacts discovered, and more.

OPEN CASE INFORMATION FILE

The AXIOMExamine.log file contains information about any errors encountered, jobs that were run, and general debugging information.

OPEN LOG FILE

EVIDENCE OVERVIEW

ADD NEW EVIDENCE

L:\ (4,051)

VIEW EVIDENCE FOR THIS SOURCE ONLY

Evidence number L:\

Description

Location [redacted]keychain.plist

Platform Mobile

Process method Parsing and carving

No picture added

CHANGE PICTURE

[redacted] FILES_FULL.ZIP (2,914,082)

VIEW EVIDENCE FOR THIS SOURCE ONLY

Evidence number [redacted]files_full.zip

Description

Location [redacted]files_full.zip

Platform Mobile

Process method Parsing and carving

No picture added

CHANGE PICTURE

PLACES TO START

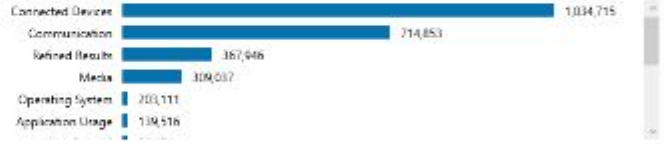
Loading...

ARTIFACT CATEGORIES

VIEW ALL ARTIFACT CATEGORIES

Evidence source All

Number of artifacts 2,918,133



TAGS AND COMMENTS (131)

TAGS ADDED BY REVIEWERS

TAG	ARTIFACTS
Evidence	101
Of Interest	25

COMMENTS INCLUDED IN CASE

There are no comments in this case.

CPS DATA MATCHES

IDENTIFIER MATCHES

Magnet AXIOM can compare identifiers found in this case with identifiers from other cases that your organization has uploaded to the Magnet Proquo database. These identifiers can include people identifiers, such as email addresses or phone numbers, and device identifiers, such as camera serial numbers or phone IMEIs.

For more information and to download a beta copy of the Magnet Proquo server software, visit Magnet Idea Lab.

https://magnetideelab.com/ COPY URL

Once you have installed the Magnet Proquo server software, configure product integration settings to connect Magnet AXIOM to Magnet Proquo.

CONFIGURE PRODUCT INTEGRATIONS

MAGNET.AI CATEGORIZATION

KEYWORD MATCHES

POTENTIAL CLOUD EVIDENCE LEADS (45)

Magnet AXIOM discovered the following cloud accounts in the evidence. With AXIOM Cloud, you can attempt to access accounts using available credentials to acquire cloud evidence. Alternatively, you can try other methods such as public data acquisition, processing user downloaded packages, or warrant returns.

VIEW ALL POTENTIAL CLOUD EVIDENCE LEADS

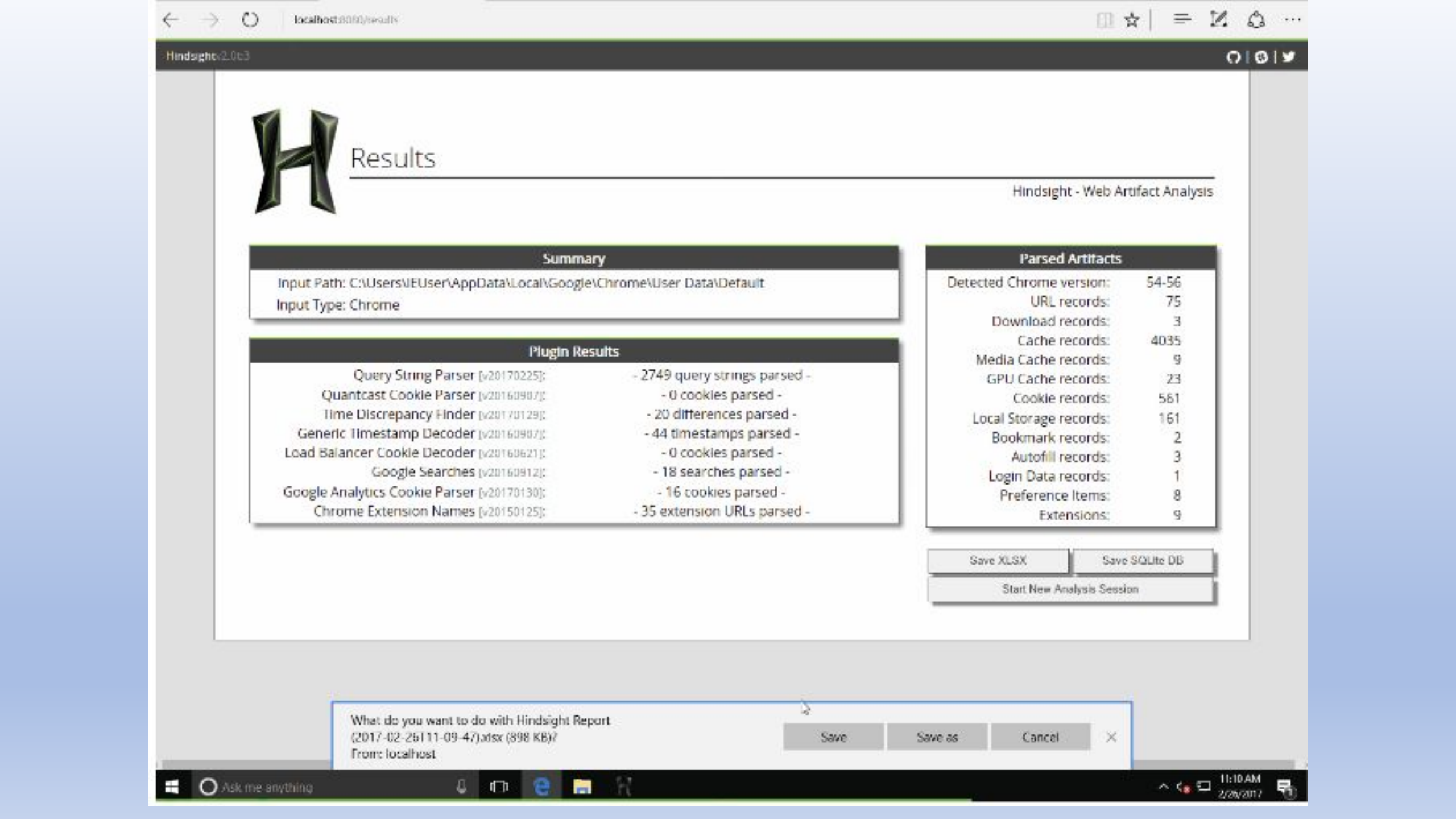
USER NAME	CLOUD SERVICE
[No username found]	Apple

Time zone UTC+0:00

Social Media URLs	7,277
Tax Site URLs	32
Tor URLs	43
Torrent URLs	2
User Accounts	161
Web Chat URLs	710
WEB RELATED	**81,174**
COMMUNICATION	**714,853**
Apple Contacts - iOS	363
Discord Messages	966
Facebook Messenger Groups	3

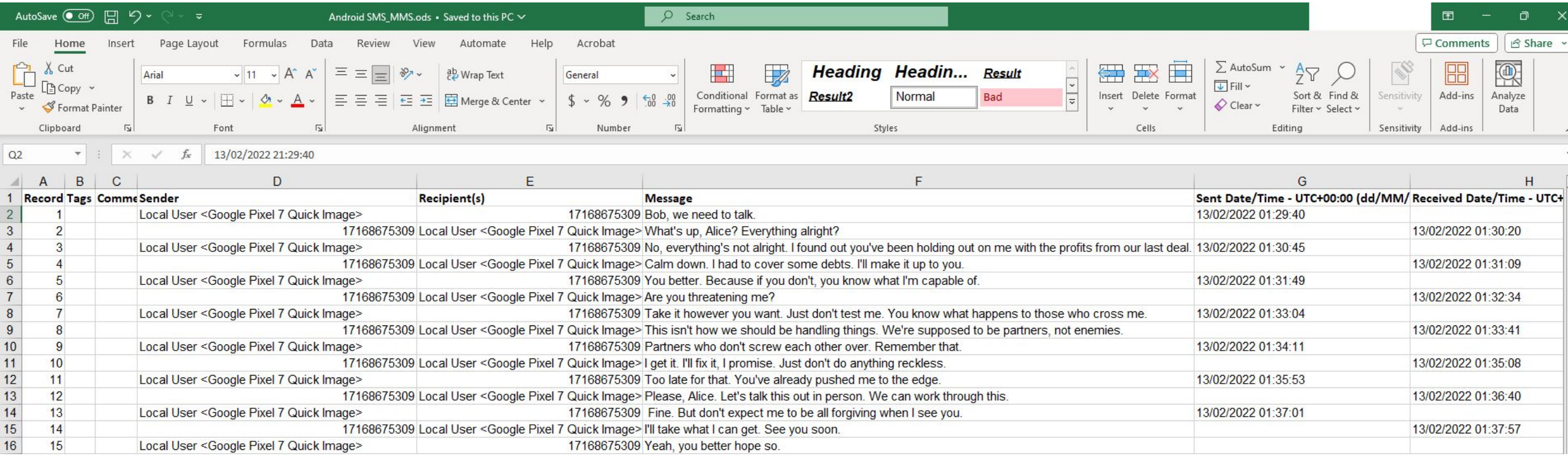
Communication
iOS Call Logs

Communication
iOS Call Logs
Communication
iOS Call Logs
Communication
iOS Call Logs
Communication
iOS Call Logs
Communication
iOS Call Logs
Communication
iOS Call Logs
Communication
iOS Call Logs


Hindsight
Results
Hindsight - Web Artifact Analysis
Summary
Input Path: C:\Users\IEUser\AppData\Local\Google\Chrome\User Data\Default
Input Type: Chrome
Plugin Results
Query String Parser [v20170225]: - 2749 query strings parsed -
Quantcast Cookie Parser [v20160907]: - 0 cookies parsed -
Time Discrepancy Finder [v20170129]: - 20 differences parsed -
Generic Timestamp Decoder [v20160907]: - 44 timestamps parsed -
Load Balancer Cookie Decoder [v20160621]: - 0 cookies parsed -
Google Searches [v20160912]: - 18 searches parsed -
Google Analytics Cookie Parser [v20170130]: - 16 cookies parsed -
Chrome Extension Names [v20150125]: - 35 extension URLs parsed -
Parsed Artifacts
Detected Chrome version: 54-56
URL records: 75
Download records: 3
Cache records: 4035
Media Cache records: 9
GPU Cache records: 23
Cookie records: 561
Local Storage records: 161
Bookmark records: 2
Autofill records: 3
Login Data records: 1
Preference Items: 8
Extensions: 9
Save XLSX
Save SQLite DB
Start New Analysis Session
What do you want to do with Hindsight Report (2017-02-26 11-09-47).xlsx (898 KB)?
From: localhost
Save
Save as
Cancel
Ask me anything
11:10 AM
2/26/2017

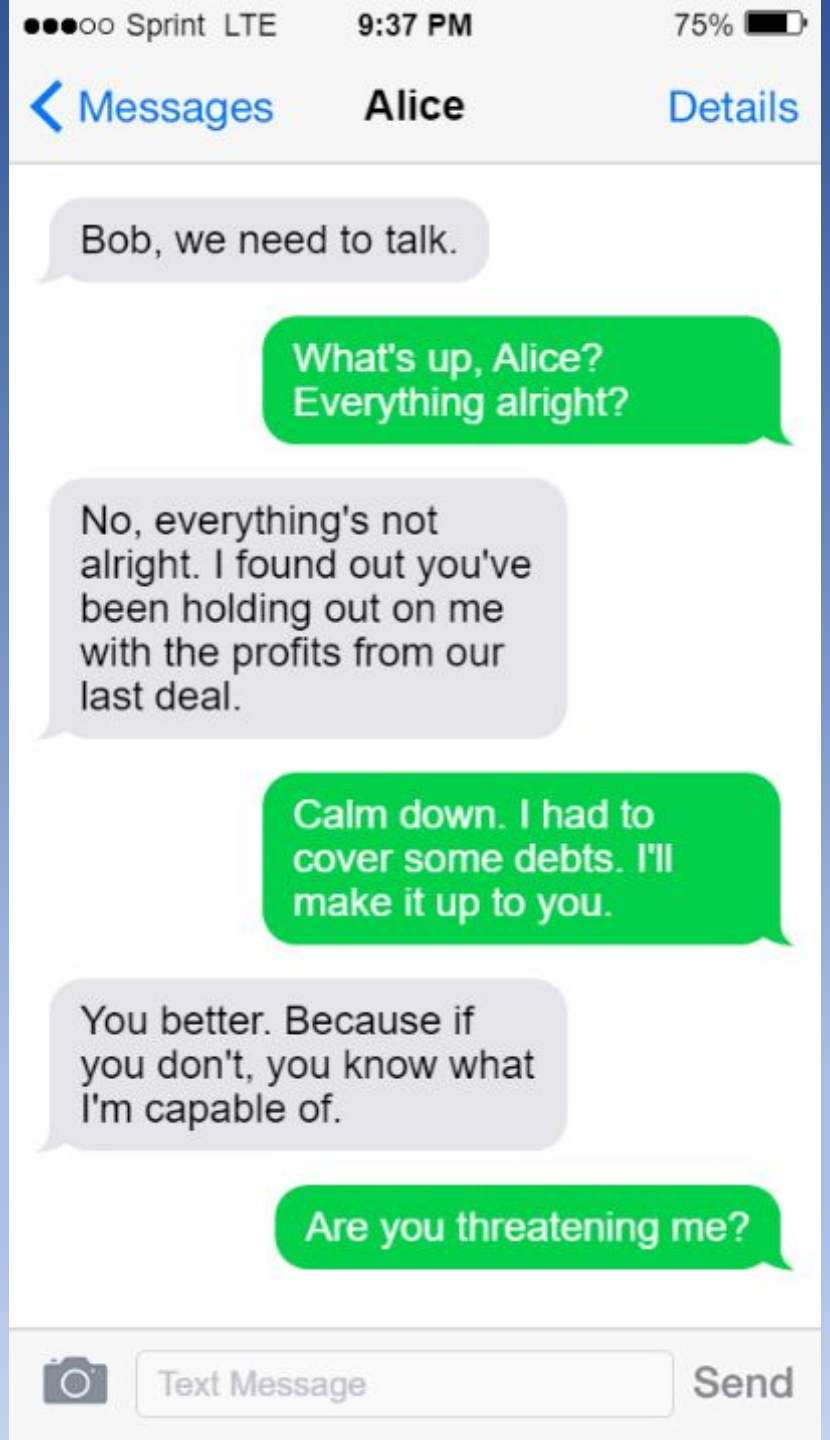
Data Analysis Challenges

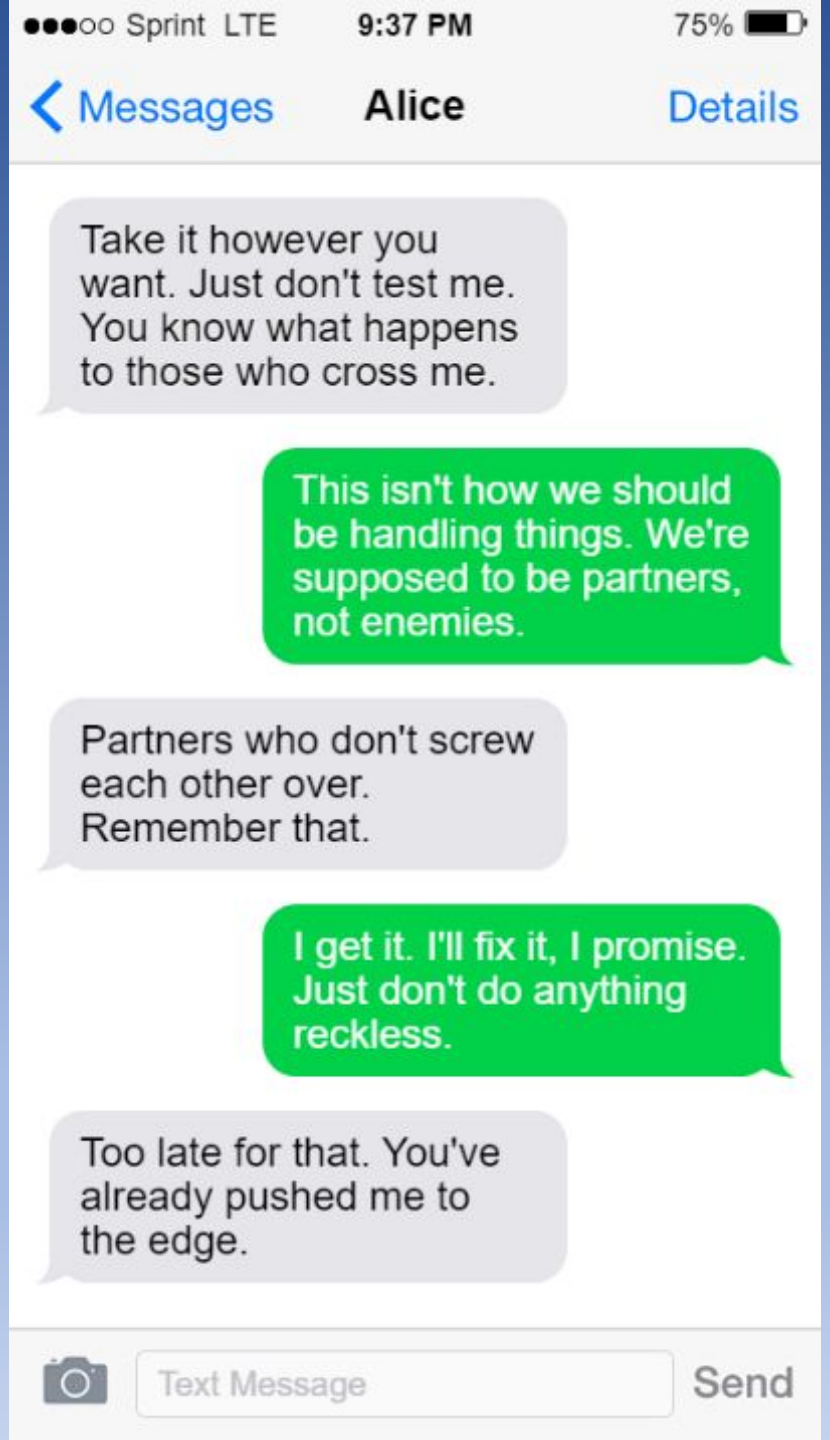
- Needing permission to review data (behind a login)
- Ignoring relevant evidence (e.g. believing something is a random text file, when it actually contains an important code.)
- Evidence unable to be processed by existing tools
- Analyzing data not relevant to the goals of the case (e.g. exploring malware when the issue is a deceased person)
- Tunnel vision
- Lack of following through

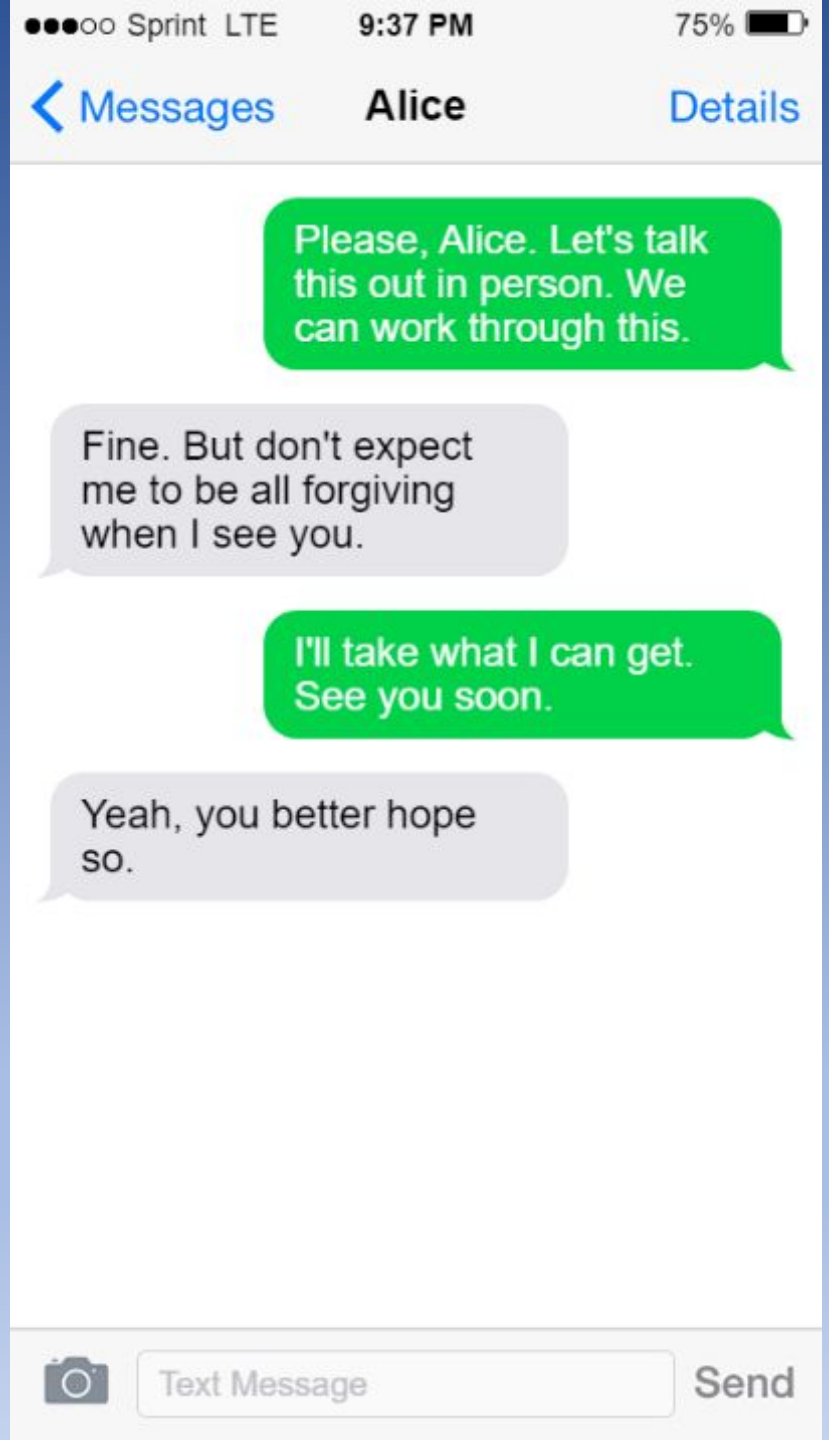


	A	B	C	D	E	F	G	H
1	Record	Tags	Comme	Sender	Recipient(s)	Message	Sent Date/Time - UTC+00:00 (dd/MM/	Received Date/Time - UTC+
2	1			Local User <Google Pixel 7 Quick Image>	17168675309	Bob, we need to talk.	13/02/2022 01:29:40	
3	2			17168675309	Local User <Google Pixel 7 Quick Image>	What's up, Alice? Everything alright?		13/02/2022 01:30:20
4	3			Local User <Google Pixel 7 Quick Image>	17168675309	No, everything's not alright. I found out you've been holding out on me with the profits from our last deal.	13/02/2022 01:30:45	
5	4			17168675309	Local User <Google Pixel 7 Quick Image>	Calm down. I had to cover some debts. I'll make it up to you.		13/02/2022 01:31:09
6	5			Local User <Google Pixel 7 Quick Image>	17168675309	You better. Because if you don't, you know what I'm capable of.	13/02/2022 01:31:49	
7	6			17168675309	Local User <Google Pixel 7 Quick Image>	Are you threatening me?		13/02/2022 01:32:34
8	7			Local User <Google Pixel 7 Quick Image>	17168675309	Take it however you want. Just don't test me. You know what happens to those who cross me.	13/02/2022 01:33:04	
9	8			17168675309	Local User <Google Pixel 7 Quick Image>	This isn't how we should be handling things. We're supposed to be partners, not enemies.		13/02/2022 01:33:41
10	9			Local User <Google Pixel 7 Quick Image>	17168675309	Partners who don't screw each other over. Remember that.	13/02/2022 01:34:11	
11	10			17168675309	Local User <Google Pixel 7 Quick Image>	I get it. I'll fix it, I promise. Just don't do anything reckless.		13/02/2022 01:35:08
12	11			Local User <Google Pixel 7 Quick Image>	17168675309	Too late for that. You've already pushed me to the edge.	13/02/2022 01:35:53	
13	12			17168675309	Local User <Google Pixel 7 Quick Image>	Please, Alice. Let's talk this out in person. We can work through this.		13/02/2022 01:36:40
14	13			Local User <Google Pixel 7 Quick Image>	17168675309	Fine. But don't expect me to be all forgiving when I see you.	13/02/2022 01:37:01	
15	14			17168675309	Local User <Google Pixel 7 Quick Image>	I'll take what I can get. See you soon.		13/02/2022 01:37:57
16	15			Local User <Google Pixel 7 Quick Image>	17168675309	Yeah, you better hope so.		

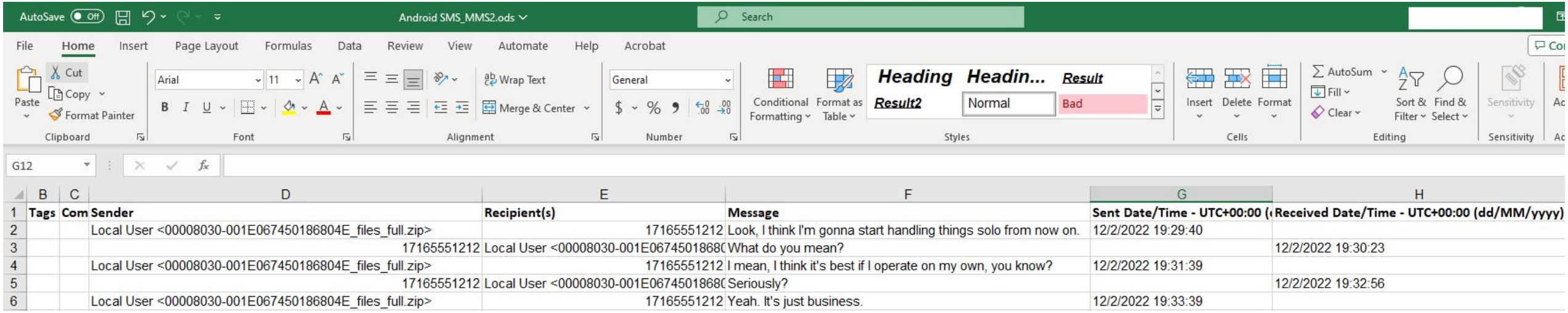
SMS conversation between Alice and Bob


●●●○○ Sprint LTE
9:37 PM
75%
Messages
Alice
Details
Bob, we need to talk.
What's up, Alice? Everything alright?
No, everything's not alright. I found out you've been holding out on me with the profits from our last deal.
Calm down. I had to cover some debts. I'll make it up to you.
You better. Because if you don't, you know what I'm capable of.
Are you threatening me?
Text Message
Send


●●●○○ Sprint LTE
9:37 PM
75%
Messages
Alice
Details
Take it however you want. Just don't test me. You know what happens to those who cross me.
This isn't how we should be handling things. We're supposed to be partners, not enemies.
Partners who don't screw each other over. Remember that.
I get it. I'll fix it, I promise. Just don't do anything reckless.
Too late for that. You've already pushed me to the edge.
Text Message
Send


●●●○○ Sprint LTE
9:37 PM
75%
Messages
Alice
Details
Please, Alice. Let's talk this out in person. We can work through this.
Fine. But don't expect me to be all forgiving when I see you.
I'll take what I can get. See you soon.
Yeah, you better hope so.
Text Message
Send

PD reports that Alice’s fingerprint were identified all over the victim’s home including on a kitchen knife that has a profile that appears to be similar to that of the murder weapon



	B	C	D	E	F	G	H
1	**Tags**	**Com**	**Sender**	**Recipient(s)**	**Message**	**Sent Date/Time - UTC+00:00 (**	**Received Date/Time - UTC+00:00 (dd/MM/yyyy)**
2			Local User <00008030-001E067450186804E_files_full.zip>	17165551212	Look, I think I'm gonna start handling things solo from now on.	12/2/2022 19:29:40	
3			17165551212	Local User <00008030-001E0674501868(	What do you mean?		12/2/2022 19:30:23
4			Local User <00008030-001E067450186804E_files_full.zip>	17165551212	I mean, I think it's best if I operate on my own, you know?	12/2/2022 19:31:39	
5			17165551212	Local User <00008030-001E0674501868(	Seriously?		12/2/2022 19:32:56
6			Local User <00008030-001E067450186804E_files_full.zip>	17165551212	Yeah. It's just business.	12/2/2022 19:33:39	

SMS conversation between Bob B. and a mystery person.


●●●○○ Sprint LTE
3:33 PM
75%
Messages
Bob
Details
Look, I think I'm gonna start handling things solo from now on.
What do you mean?
I mean, I think it's best if I operate on my own, you know?
Seriously?
Yeah. It's just business.
Text Message
Send

PD reports that interviews from witnesses and neighbors indicate several people were really concerned about Bob because of Alice’s reported severe temper. They also indicated that Bob seemed to have visitors at all hours of the day and night. There was a question as to whether drugs might somehow be involved.

CASE | EVIDENCE | ANALYSIS | REPORTS | TOOLS | VIEW | EXPORT

Add Evidence | Find Chat Databases | Change Source | Reload Evidence | Remove Evidence — Evidence
Start Acquisition | Import From | Cloud Import | Root Android Device | Validate Data — Mobile Data
Change Settings — Settings
View Skip List | Add to Skip List | Create Attachment List | Print — Mailstorages
Calculate Subkey Hash — Registry
Add File MD5 to Hash Database — Files

Case Content

Case Content | Sorted Files

Items | In | Total

- aascii
  - 9F3F6C90-0000000B
    - Eml file
      - Read Message
        - Email Folder

Email Folder

Internal Path: e3://aascii/9F3F6C90-0000000B/Eml file/mbx:#0000000000000000/mbx:#0000000000000000:fld:#0000000000000000?item=fld:#0000000000000000:msg:#0000000000000000

Go

Subject	From	To	Created	Sent	Received	Last Modified
Your ride with Mohammad on Feb 12	Lyft Receipts <no-reply@ly	aascii@gmail.com	2/12/2022 10:26:51 PM		3/3/2022 9:27:01 AM	

Finished Total: 1

E-mail Data

Your ride with Mohammad on Feb 12

"Lyft Receipts" <no-reply@lyftmail.com>

To: aascii@gmail.com

Thanks for riding with Mohammad!

Feb 12, 2022 AT 10:13 PM

Thanks for riding with Mohammad!

100% of tips go to drivers. Add a tip

Lyft fare (1.40mi, 7m 18s)	$8.58
DC City Fee	$0.41
Tip	$3.00
Lyft Credits	-$1.79
Visa *1234	**$10.20**

You've already paid for this ride.

This total may not match the charge on your account statement. The payment for this ride might be combined with any other rides you took on Feb 12, 2022. Keep in mind that the cost of this ride and the total charge may not reflect refunds, credits, or other changes.

Pickup 10:13 PM
123 Main St., Anytown, NY

Drop-off 10:20 PM
456 Central Ave, Anytown, NY

Make expensing business rides easy

Enable business profile on Lyft to make expensing rides quick and easy.
GET BUSINESS PROFILE

Tip driver

RFC Header | Text | RTF | HTML | Raw HTML | Attachments

Properties

General | Content Analysis

Additional Info	
Internet Message ID	<20220303142651.ecd0f9
Message Class	IPM.Note
Message Size (bytes)	86,952
Dates	
Creation Date	2/12/2022 10:26:51 PM
Received Date	3/3/2022 9:27:01 AM
Message Flags	
Deleted	Undefined
Encrypted	Undefined
Has Attachments	Undefined
Importance	Normal
Priority	Normal
Read	Yes
Recipients	
To	aascii@gmail.com
Sender	
From	Lyft Receipts <no-reply@ly
Sender Address Type	
Sender E-mail	no-reply@lyftmail.com
Sender Name	Lyft Receipts

Bookmarks

<ROOT>

Tasks | Hashes | Common Log

Your ride with Mohammad on Feb 12

"Lyft Receipts" <no-reply@lyftmail.com>

To: aascii@gmail.com

Thanks for riding with Mohammad!

Feb 12, 2022 AT 10:13 PM

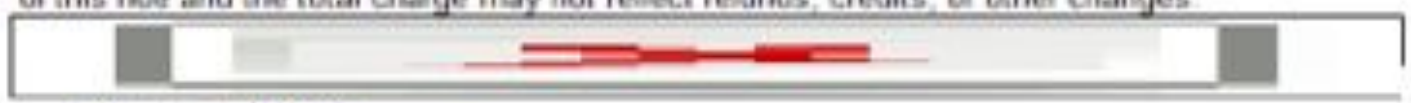
Thanks for riding with Mohammad!

100% of tips go to drivers. Add a tip

Lyft fare (1.40mi, 7m 18s)	$8.58
DC City Fee	$0.41
Tip	$3.00
Lyft Credits	-$1.79
Visa *1234	**$10.20**

You've already paid for this ride.

This total may not match the charge on your account statement. The payment for this ride might be combined with any other rides you took on Feb 12, 2022. Keep in mind that the cost of this ride and the total charge may not reflect refunds, credits, or other changes.



Pickup 10:13 PM

123 Main St., Anytown, NY

Drop-off 10:20 PM

456 Central Ave, Anytown, NY



Data Correlation

Data Correlation Goals

- Bring together data from all sources
- Normalize findings
- Match timestamps
- Finding patterns
- Building a picture of events

Tools for Data Correlation

- Mind mapping software
  - Maltego
  - i2 Analyst's Notebook
- Pen/paper
- Spreadsheets

Data to Correlate

- SMS Messages
  - Bob’s phone
  - Alice’s phone
- Email showing Alice’s trip via Lyft
- Reports from PD
  - Information about Alice’s fingerprints
  - Concern about Alice’s temper

Data Correlation Challenges

- Not enough context provided
- Incorrectly dismissing info as irrelevant
- Unrealistic time frames
- Not taking the time to correlate



Timeline Analysis

Timeline Analysis Goals

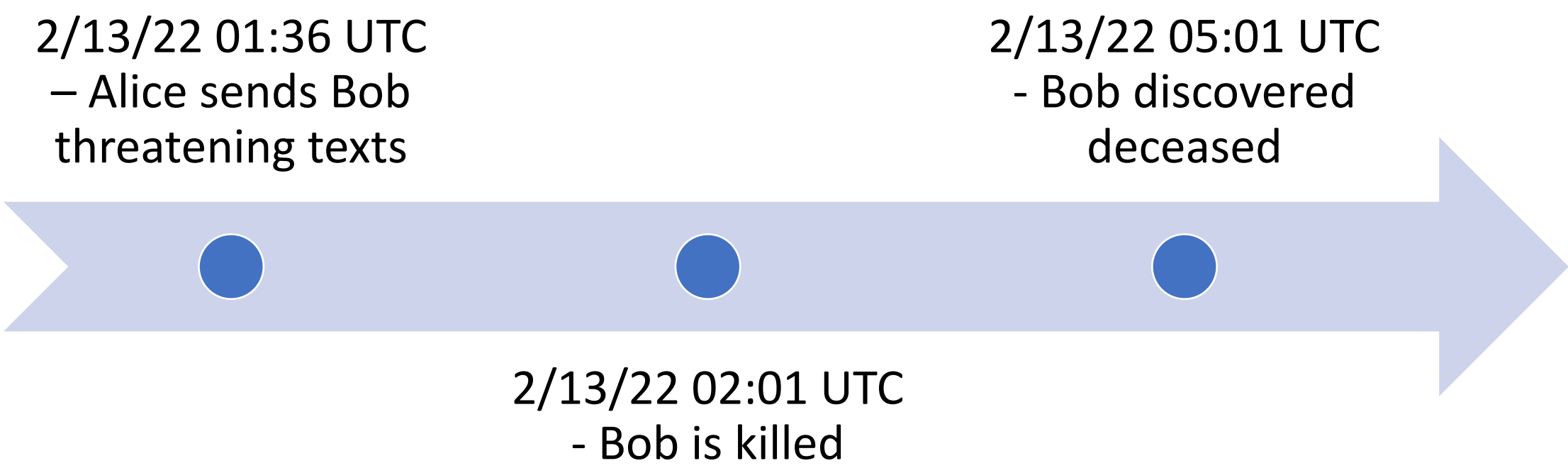
- Check for timestamps with all evidence
- Be aware of time zones (UTC is your friend)
- Know the attributes (e.g. Timestamp, Host, User, Source, location of information, Event Type, Description, etc.)
- Create timeline of all digital forensic findings

Timeline Analysis Tools

- Axiom
- log 2 timeline
- Excel
- Timeline Explorer

Timeline Analysis Challenges

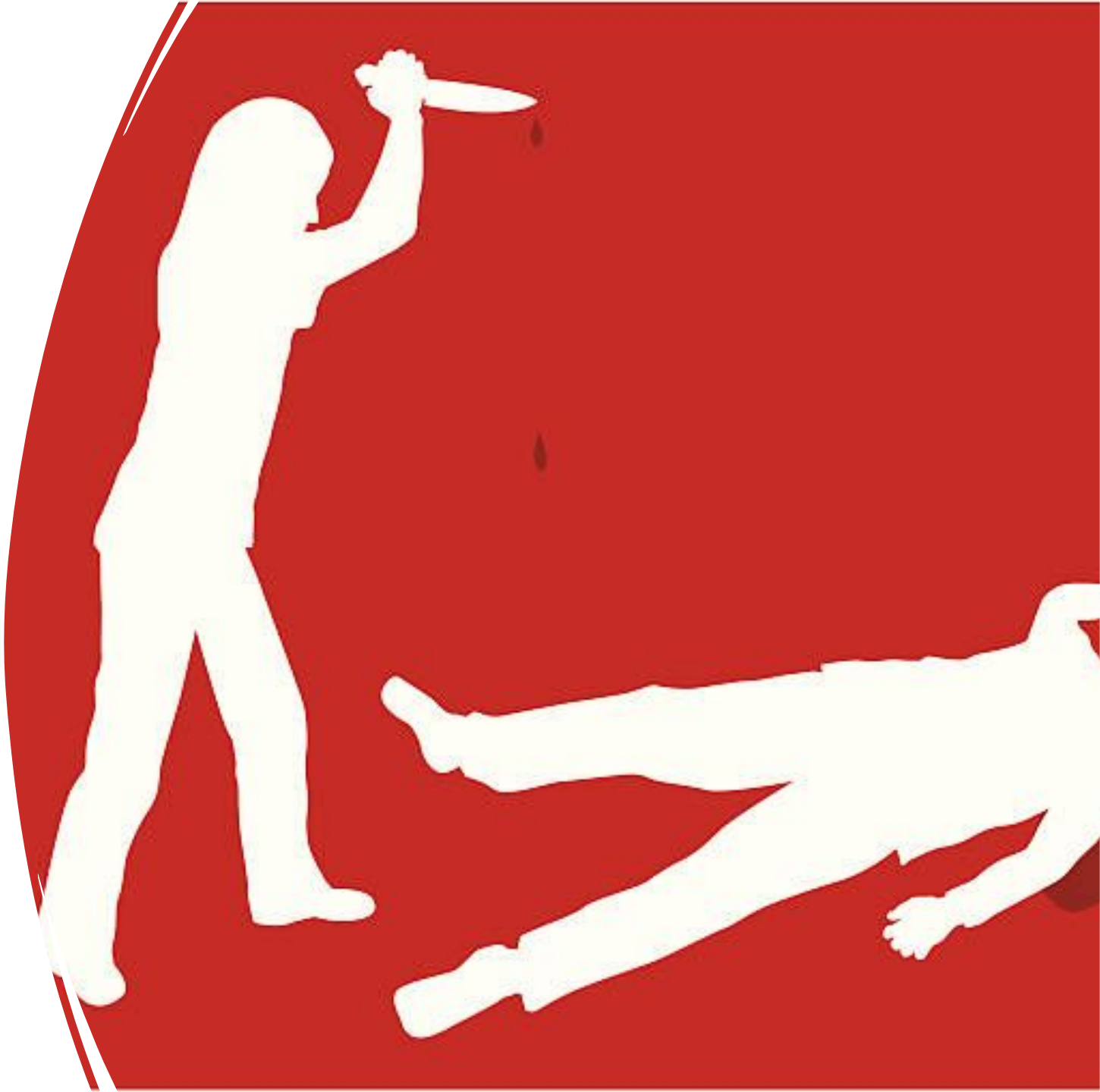
- Missing time stamps
- Different time zones not recognized
- Not paying attention to time stamps



Timeline of Bob Byte homicide

Initial hypothesis?

Alice killed Bob!

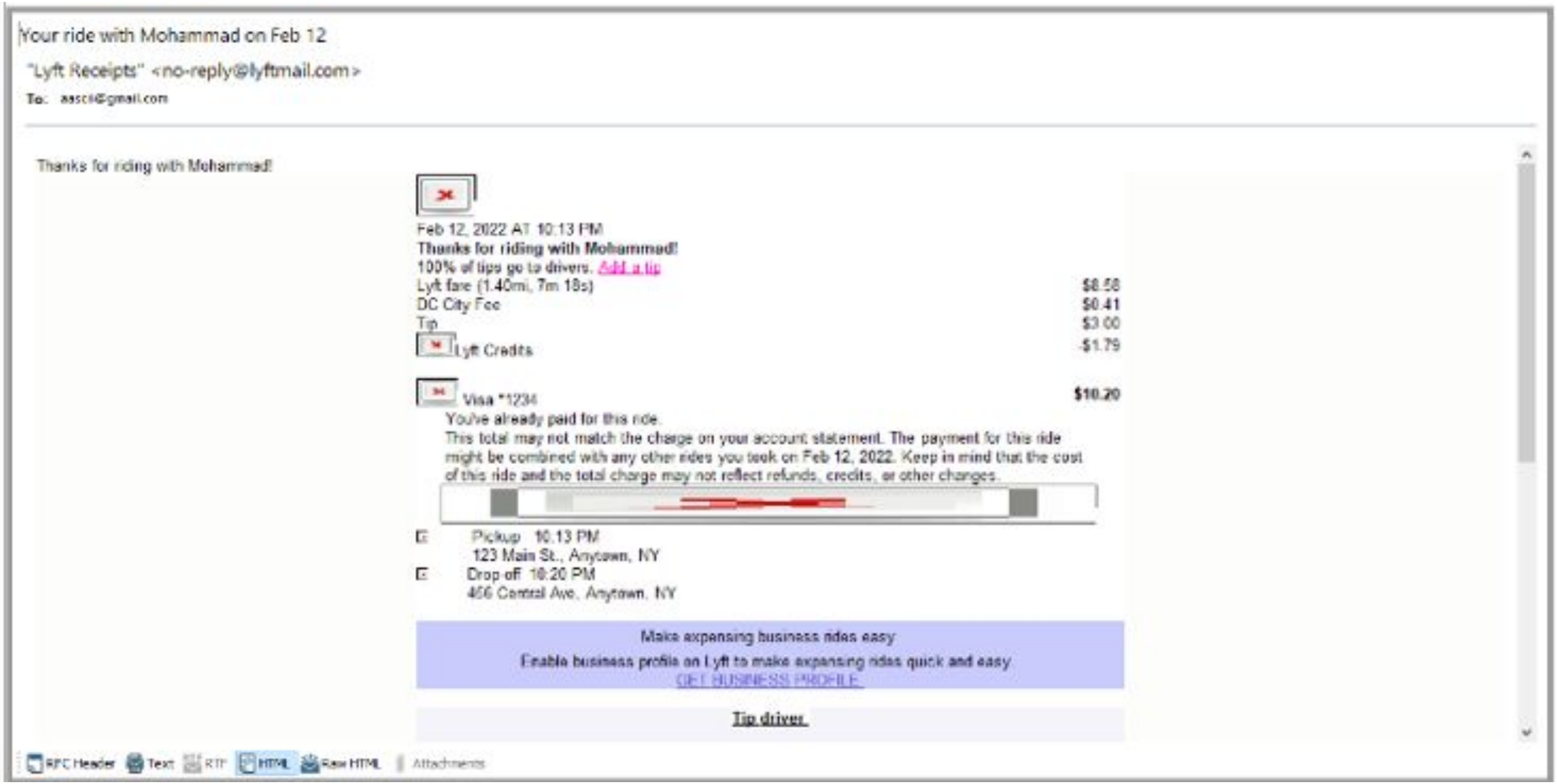



That's how it
could have happened.


But how about
this?



Data Analysis (again)



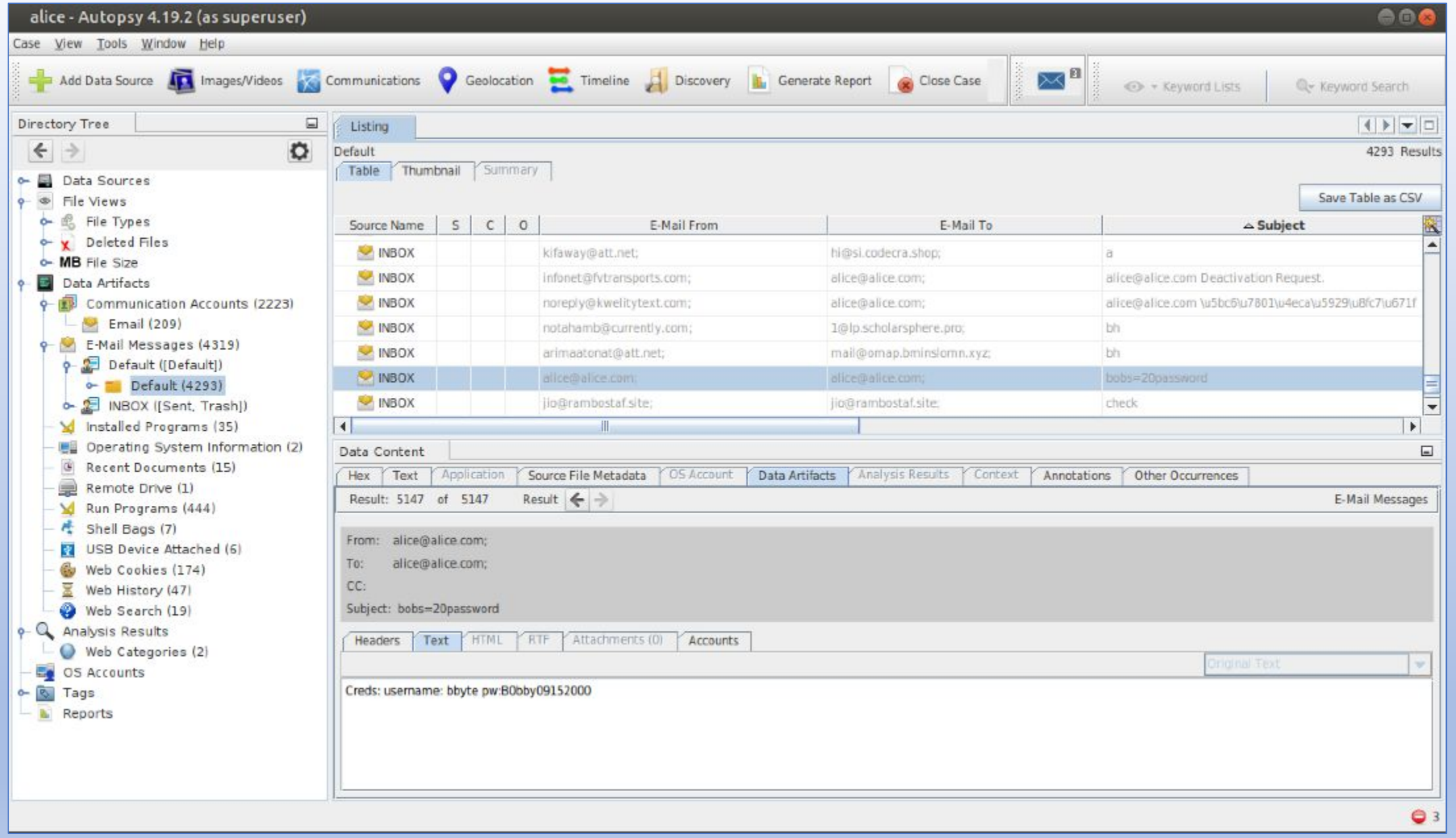
NOTE: TIME STAMP ONE HOUR PAST ToD!

	A	B	C	D	F	G	H	I
1	Hindsight Internet History Forensics (v2021.12)							
2	Ty	Timestamp (UTC)	URL	Title / Name / Status	Interpretation	Profile	Source	Duration
67	url	2022-02-13 03:33:42.000	https://www.google.com/?gws_rd=ssl	Google	gws_rd: ssl [Query String Parser]	Z:\maya\uplo	Local	None
71	url	2022-02-13 03:33:55.000	https://www.google.com/search?q=holiday+travel&	holiday travel - Google Search	Searched for "holiday travel"	Z:\maya\uplo	Local	None
72	url	2022-02-13 03:33:53.000	https://www.google.com/search?q=holiday+travel&	holiday travel - Google Search	Searched for "holiday travel"	Z:\maya\uplo	Local	None
74	url	2022-02-13 03:34:01.000	https://www.google.com/url?sa=t&rct=j&q=&esrc=s	Travel Destinations | Holiday Vacati	sa: t | rct: j | esrc: s | source: web | ved: 2ahUKEwiEi6qf-Y-FAxXKMDC	Z:\maya\uplo	Local	None
76	url	2022-02-13 03:34:03.000	https://www.holidayvacations.com/destinations/	Travel Destinations | Holiday Vacations		Z:\maya\uplo	Local	0:00:08.318175
85	url	2022-02-13 03:34:03.000	https://www.google.com/search?q=holiday+travel+f	holiday travel for couples - Google S	Searched for "holiday travel for couples"	Z:\maya\uplo	Local	None
86	url	2022-02-13 03:34:20.000	https://www.google.com/search?q=holiday+travel+f	holiday travel for couples - Google S	Searched for "holiday travel for couples"	Z:\maya\uplo	Local	None
88	url	2022-02-13 03:34:30.000	https://www.google.com/url?sa=t&rct=j&q=&esrc=s	25 Best Vacation Spots for Couples	sa: t | rct: j | esrc: s | source: web | ved: 2ahUKEwiM5o6r-Y-FAxWnAD	Z:\maya\uplo	Local	None
93	url	2022-02-13 03:34:50.000	https://www.travelandleisure.com/trip-ideas/romar	25 Best Vacation Spots for Couples		Z:\maya\uplo	Local	0:00:46.920613
221	url	2022-02-13 03:35:58.000	https://www.google.com/url?sa=t&rct=j&q=&esrc=s	The 34 Best Couples Vacations	sa: t | rct: j | esrc: s | source: web | ved: 2ahUKEwiM5o6r-Y-FAxWnAD	Z:\maya\uplo	Local	None
226	url	2022-02-13 03:36:01.000	https://travel.usnews.com/gallery/top-couples-vaca	The 34 Best Couples Vacations		Z:\maya\uplo	Local	0:00:09.091970
230	url	2022-02-13 03:36:18.000	https://www.google.com/search?q=couples+counse	couples counseling - Google Search	Searched for "couples counseling"	Z:\maya\uplo	Local	None
231	url	2022-02-13 03:36:20.000	https://www.google.com/search?q=couples+counse	couples counseling - Google Search	Searched for "couples counseling"	Z:\maya\uplo	Local	None
233	url	2022-02-13 03:36:30.000	https://www.googleadservices.com/pagead/aclk?sa	Best Online Couples Counseling of 2	sa: L | ai: DChcSEwiboObj-Y-FAxW_0cIEHWD7Dg0YABABGgJwdg | ae:	Z:\maya\uplo	Local	None
234	url	2022-02-13 03:36:30.000	https://www.forbes.com/health/l/best-online-coup	Best Online Couples Counseling of 2	utm_content: 154362444869 | utm_term: kwd-24923020 | utm_campa	Z:\maya\uplo	Local	0:00:22.003992
263	url	2022-02-13 03:36:46.000	https://www.google.com/search?q=couples+counse	couples counseling - Google Search	Searched for "couples counseling"	Z:\maya\uplo	Local	None
283	url	2022-02-13 03:36:58.000	https://www.googleadservices.com/pagead/aclk?sa	Landing Page SNB - Grow Therapy	sa: L | ai: DChcSEwiboObj-Y-FAxW_0cIEHWD7Dg0YABAAGgJwdg | ae:	Z:\maya\uplo	Local	None
284	url	2022-02-13 03:36:58.000	https://growtherapy.com/wp/find-therapist-nb/?g_a	Landing Page SNB - Grow Therapy	g_acctid: 735-200-2909 | g_adgroupid: 154594176602 | g_adid: 672121	Z:\maya\uplo	Local	0:00:15.640767
307	url	2022-02-13 03:33:08.000	https://growtherapy.com/filters?utm_device=c&utm	Grow Therapy - Therapy Made Acce	utm_device: c | utm_source: google | utm_medium: cpc | utm_camp	Z:\maya\uplo	Local	None
312	url	2022-02-13 03:33:14.000	https://growtherapy.com/filters?utm_device=c&utm	Grow Therapy - Therapy Made Acce	utm_device: c | utm_source: google | utm_medium: cpc | utm_camp	Z:\maya\uplo	Local	0:00:47.355979
321	url	2022-02-13 03:38:01.000	https://growtherapy.com/about-us?utm_campaign=	About Grow Therapy: Mental health	utm_campaign: 154594176602 | utm_medium: cpc | utm_source: goo	Z:\maya\uplo	Local	None
322	url	2022-02-13 03:38:01.000	https://growtherapy.com/about-us/?utm_campaign=	About Grow Therapy: Mental health	utm_campaign: 154594176602 | utm_medium: cpc | utm_source: goo	Z:\maya\uplo	Local	0:00:33.755729
360	url	2022-02-13 03:38:42.000	https://www.google.com/search?q=couples+counse	couples counseling marriage - Goog	Searched for "couples counseling marriage"	Z:\maya\uplo	Local	None
361	url	2022-02-13 03:38:45.000	https://www.google.com/search?q=couples+counse	couples counseling marriage - Goog	Searched for "couples counseling marriage"	Z:\maya\uplo	Local	None
363	url	2022-02-13 03:38:52.000	https://www.googleadservices.com/pagead/aclk?sa	Best Online Therapy Services	sa: L | ai: DChcSEwjUwdKo-o-FAxUJHa0GHTJRAGYYABAEGgJwdg | ae:	Z:\maya\uplo	Local	None
364	url	2022-02-13 03:38:52.000	https://bestonlinetherapyservices.com/couples?utm	Best Online Therapy Services	utm_source: google | utm_term: couple counselling | externalcreati	Z:\maya\uplo	Local	None
365	url	2022-02-13 03:38:55.000	https://bestonlinetherapyservices.com/couples?utm	Best Online Therapy Services	utm_source: google | utm_term: couple counselling | externalcreati	Z:\maya\uplo	Local	0:00:11.743436
372	url	2022-02-13 03:39:00.000	https://www.google.com/search?q=couples+counse	couples counseling marriage - Goog	Searched for "couples counseling marriage"	Z:\maya\uplo	Local	None
376	url	2022-02-13 03:39:04.000	https://www.google.com/search?sca_esv=dd5fb20fe	Free Relationship Counseling Houst	Searched for "Free Relationship Counseling Houston" [Browser scre	Z:\maya\uplo	Local	None
377	url	2022-02-13 03:39:06.000	https://www.google.com/search?sca_esv=dd5fb20fe	Free Relationship Counseling Houst	Searched for "Free Relationship Counseling Houston" [Browser scre	Z:\maya\uplo	Local	None
380	url	2022-02-13 03:39:17.000	https://www.google.com/search?q=fishing&sca_esv	fishing - Google Search	Searched for "fishing" [Browser screen 1295x791]	Z:\maya\uplo	Local	None
381	url	2022-02-13 03:39:18.000	https://www.google.com/search?q=fishing&sca_esv	fishing - Google Search	Searched for "fishing" [Browser screen 1295x791]	Z:\maya\uplo	Local	None
384	url	2022-02-13 03:39:31.000	https://www.google.com/search?q=fishing+techniq	fishing techniques - Google Search	Searched for "fishing techniques" [Browser screen 1295x791]	Z:\maya\uplo	Local	None
385	url	2022-02-13 03:39:32.000	https://www.google.com/search?q=fishing+techniq	fishing techniques - Google Search	Searched for "fishing techniques" [Browser screen 1295x791]	Z:\maya\uplo	Local	None
386	url	2022-02-13 03:39:37.000	https://www.google.com/url?sa=t&rct=j&q=&esrc=s	Fishing - Angling, Trolling, Casting |	sa: t | rct: j | esrc: s | source: web | ved: 2ahUKEwjxm9C_-o-FAxUNN	Z:\maya\uplo	Local	None
388	url	2022-02-13 03:39:40.000	https://www.britannica.com/topic/fishing-recreatio	Fishing - Angling, Trolling, Casting |	Britannica	Z:\maya\uplo	Local	0:00:10.511204
390	url	2022-02-13 03:39:41.000	https://www.google.com/url?sa=t&rct=j&q=&esrc=s	Types of Fishing - Take Me Fishing	sa: t | rct: j | esrc: s | source: web | ved: 2ahUKEwjxm9C_-o-FAxUNN	Z:\maya\uplo	Local	None

Web activity on Bob's machine

2022-02-13 03:39:00.000	https://www.google.com/search?q=couples+counse	couples counseling marriage - Goog	Searched for "couples counseling marriage"
2022-02-13 03:39:04.000	https://www.google.com/search?sca_esv=dd5fb20fe	Free Relationship Counseling Houst	Searched for "Free Relationship Counseling Houston" [Browser scree
2022-02-13 03:39:06.000	https://www.google.com/search?sca_esv=dd5fb20fe	Free Relationship Counseling Houst	Searched for "Free Relationship Counseling Houston" [Browser scree
2022-02-13 03:39:17.000	https://www.google.com/search?q=fishing&sca_esv	fishing - Google Search	Searched for "fishing" [Browser screen 1295x791]
2022-02-13 03:39:18.000	https://www.google.com/search?q=fishing&sca_esv	fishing - Google Search	Searched for "fishing" [Browser screen 1295x791]
2022-02-13 03:39:31.000	https://www.google.com/search?q=fishing+techniq	fishing techniques - Google Search	Searched for "fishing techniques" [Browser screen 1295x791]
2022-02-13 03:39:32.000	https://www.google.com/search?q=fishing+techniq	fishing techniques - Google Search	Searched for "fishing techniques" [Browser screen 1295x791]

Marriage counseling, fishing…



Bob's credentials stored as a draft in Alice's email

From: alice@alice.com;

To: alice@alice.com;

CC:

Subject: bobs=20password

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Creds: username: bbyte pw:B0bby09152000

PD reports that during an interview with Alice Ascii they learned that upon arriving at Bob's house she found him deceased and, because she was terrified of being implicated, she logged into Bob's computer with his credentials. She admitted to using Bob's computer as Bob to make it look like he was still alive.



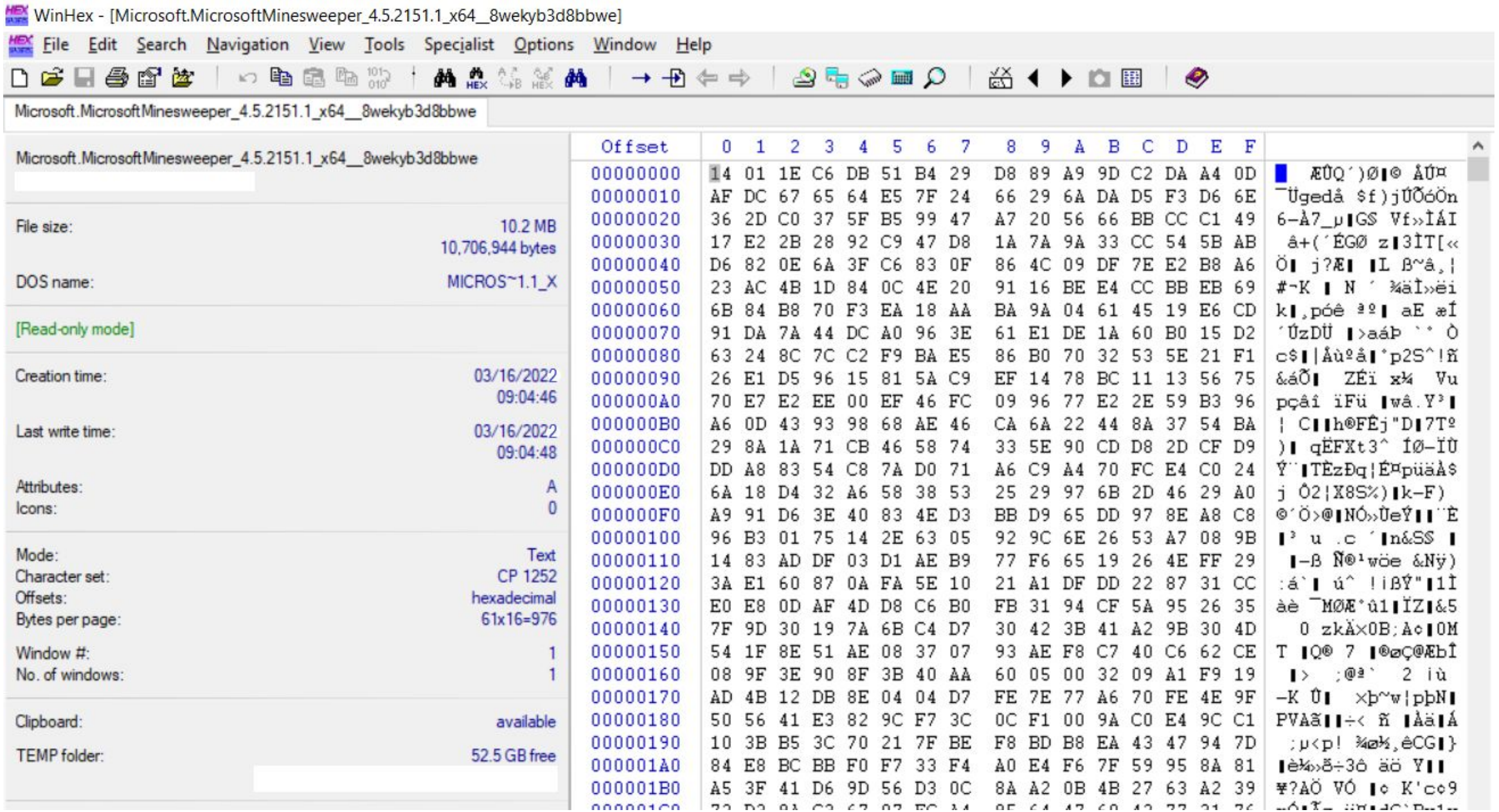
Wait…it’s not Alice?


But here's what
really happened.

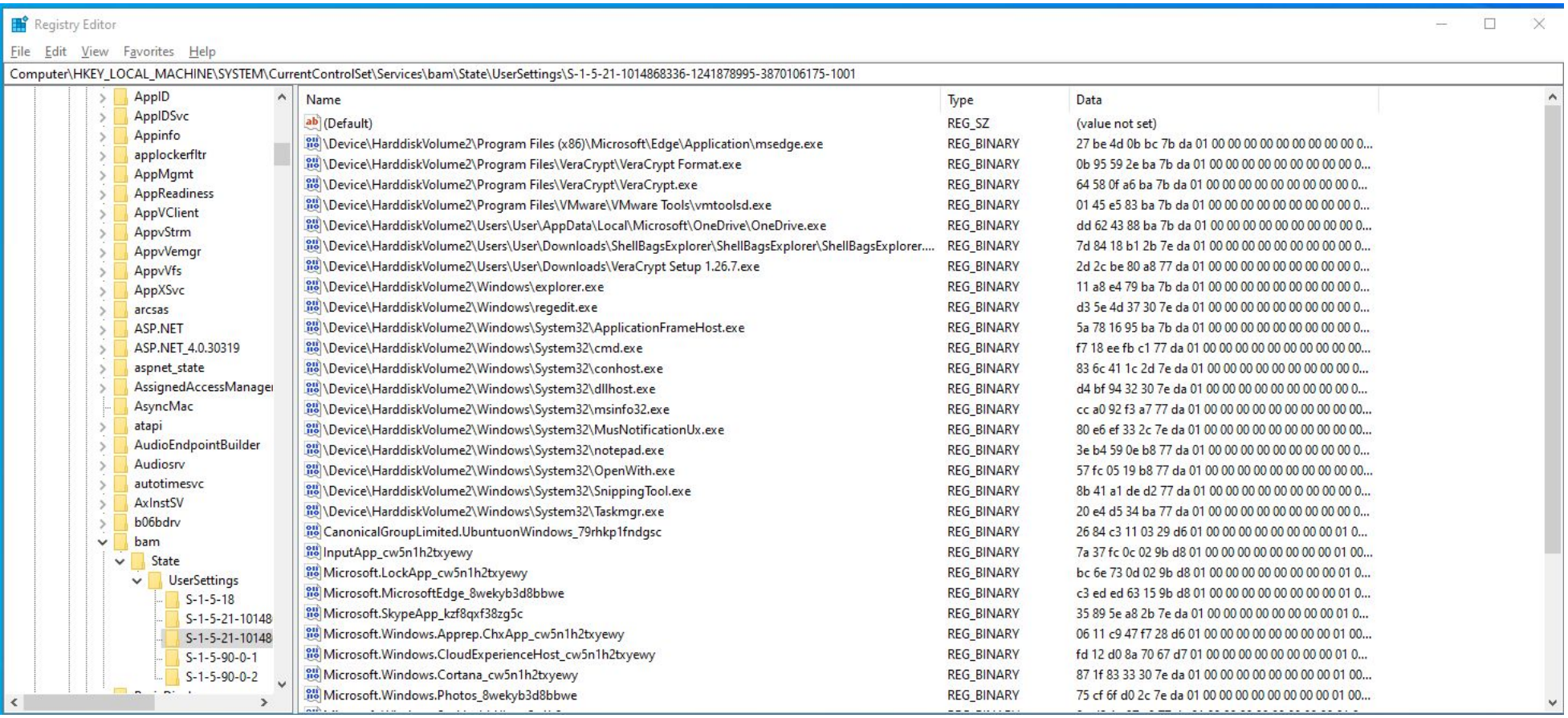
PD reports that the phone number found in the text message from Bob to someone else was that of someone named Charlie C.



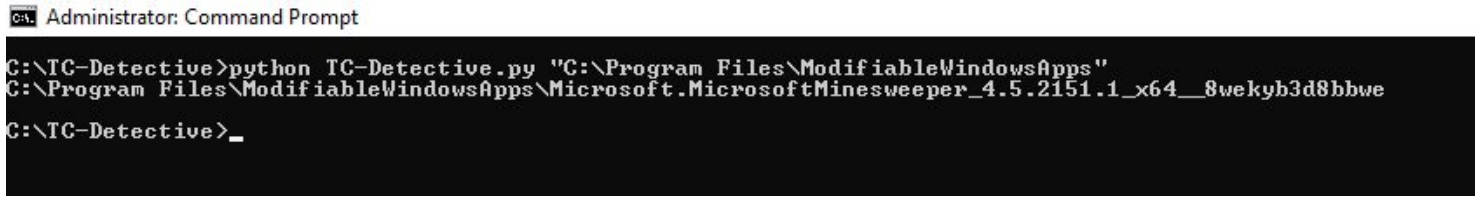
Data Analysis (again)



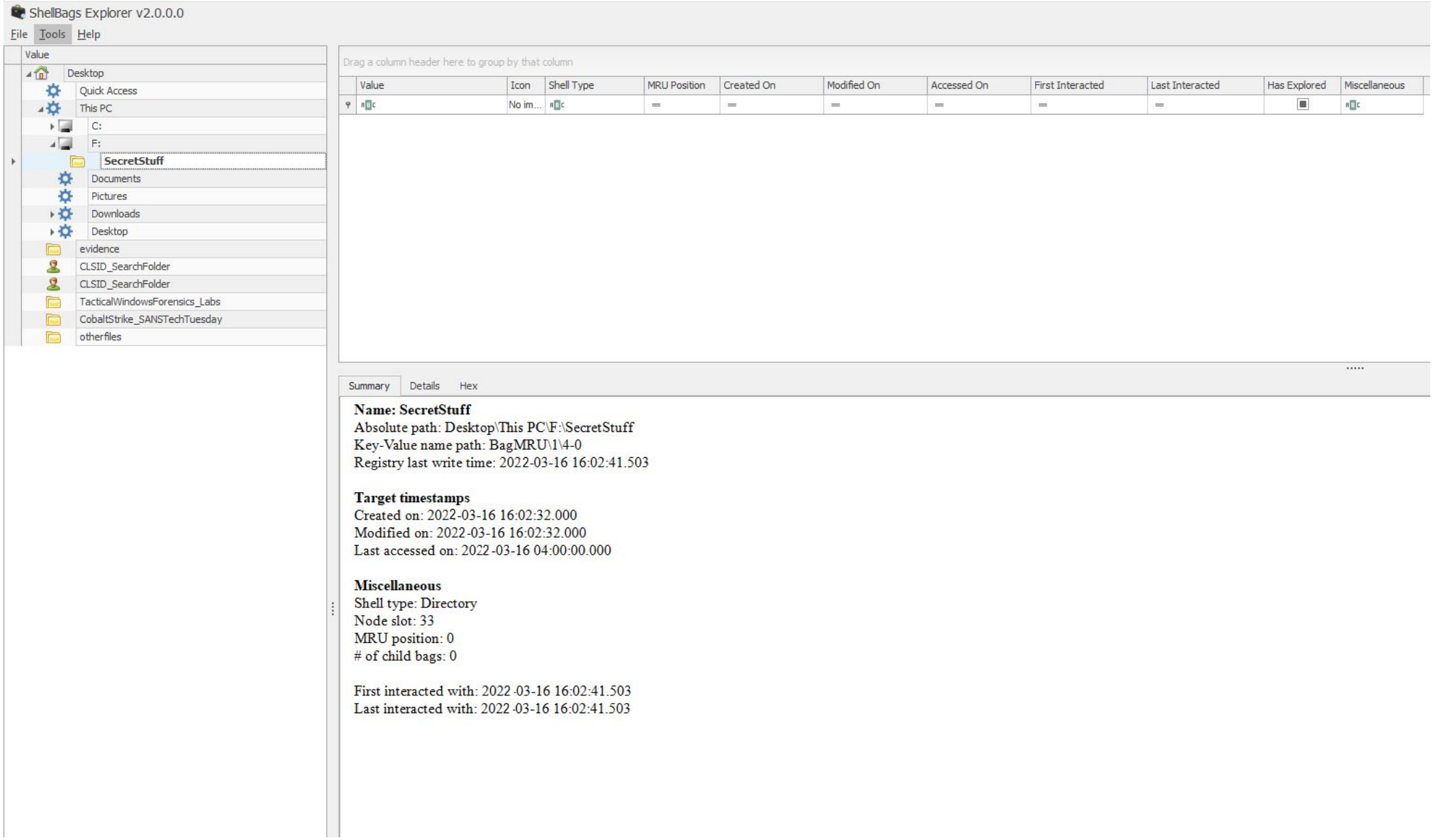
Weird file with random characters



Veracrypt installed on Bob's laptop



TC Detective confirms Veracrypt file



Shellbags Explorer showing mountpoint

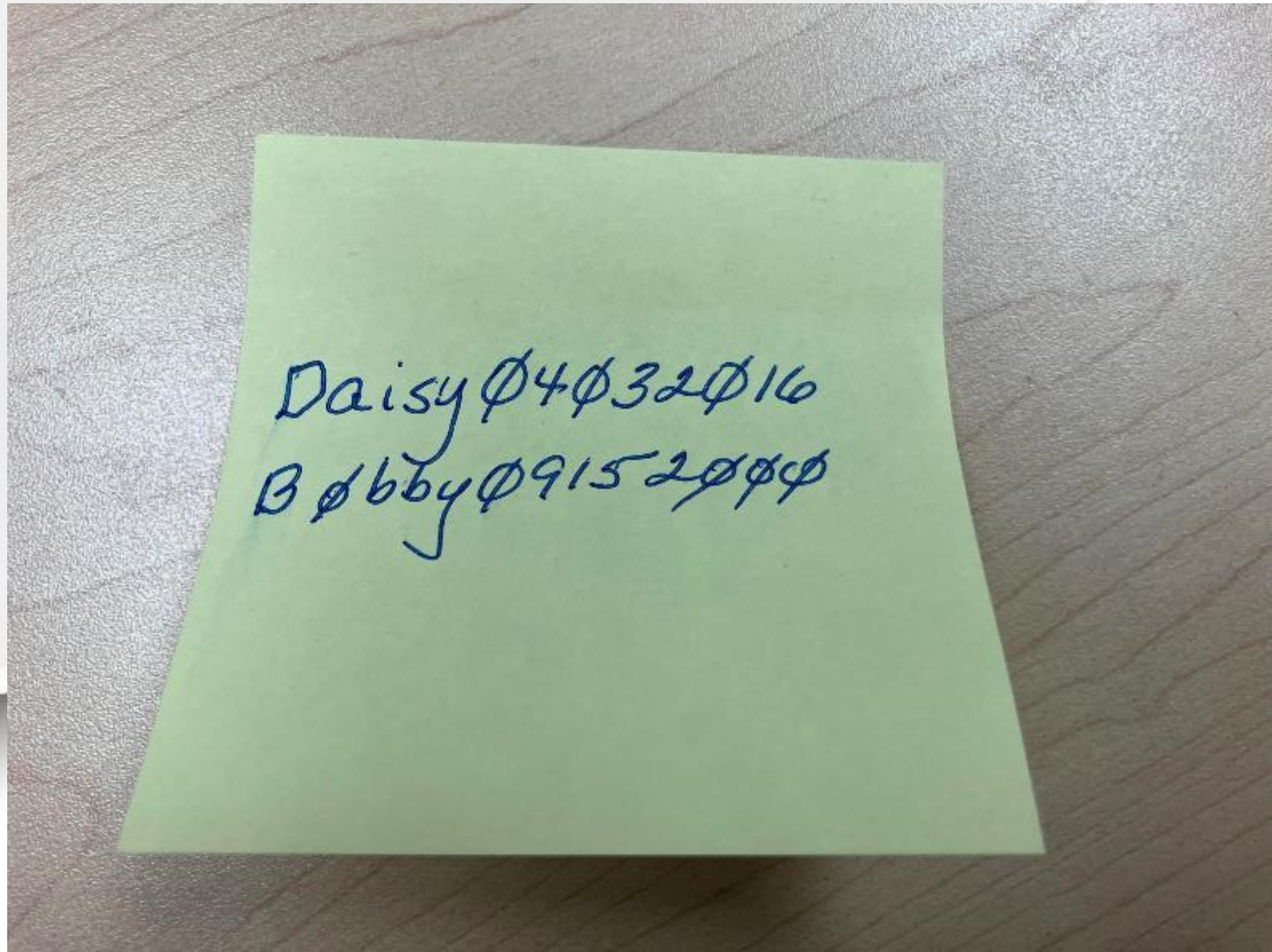
Name: SecretStuff
Absolute path: Desktop\This PC\F:\SecretStuff
Key-Value name path: BagMRU\1\4-0
Registry last write time: 2022-03-16 16:02:41.503

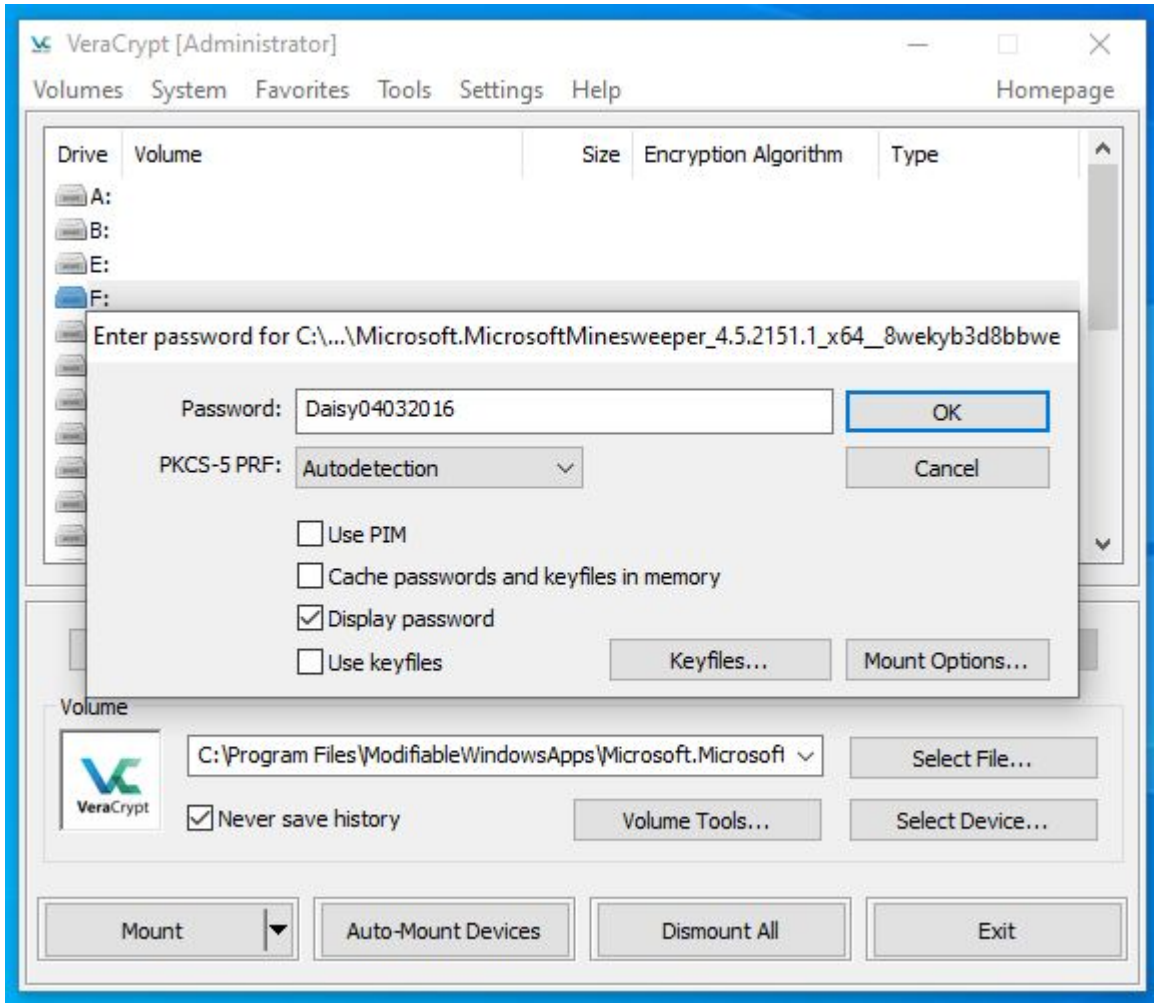
Target timestamps
Created on: 2022-03-16 16:02:32.000
Modified on: 2022-03-16 16:02:32.000
Last accessed on: 2022-03-16 04:00:00.000

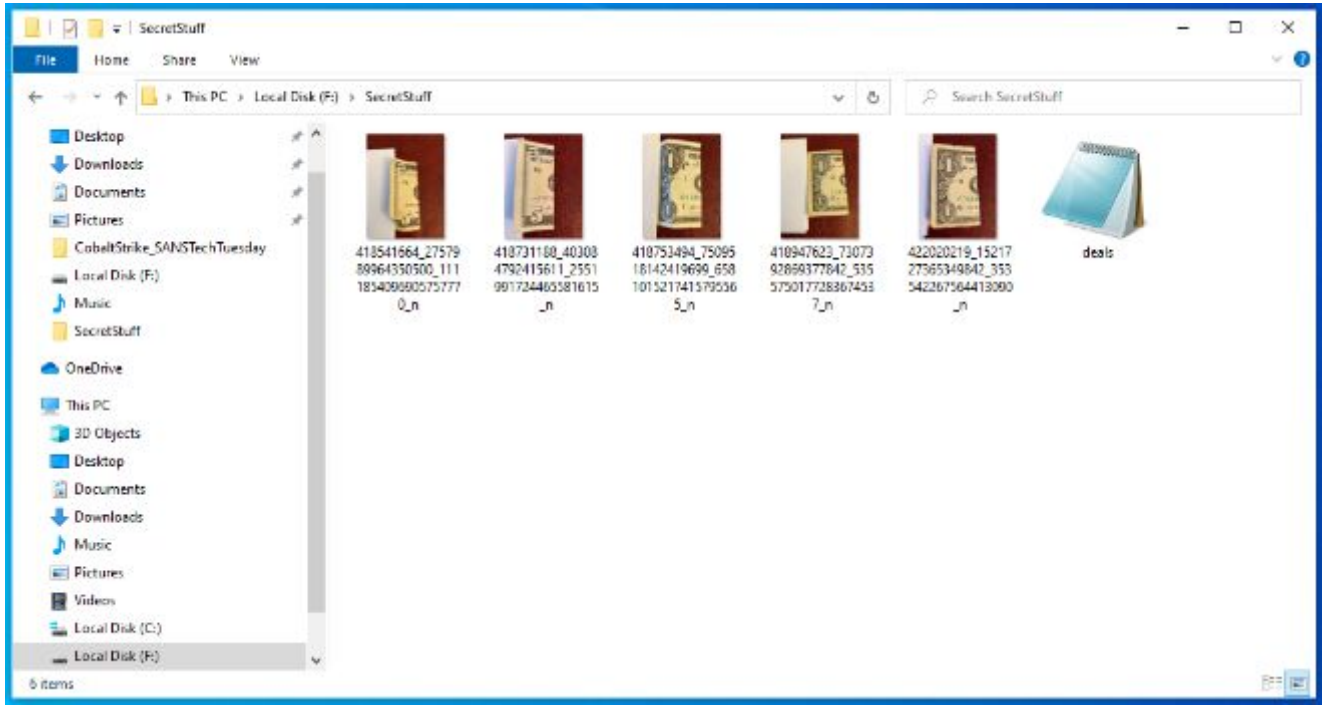
Miscellaneous
Shell type: Directory
Node slot: 33
MRU position: 0
# of child bags: 0

First interacted with: 2022-03-16 16:02:41.503
Last interacted with: 2022-03-16 16:02:41.503

PD reports that they found a post-it note with what appear to be passwords on it







Testing of passwords from post-it is successful and reveals six hidden files.











In discussion with Detective Hart, you learn that there is a Charlie C who is known for dealings in the drug world. His full name is Charlie Cyber.

F17

	A	B	C	D	E
1	For Alice A	100000	outstanding		
2	For Charlie C	200000	outstanding		
3	=	300000	+359000	for Charlie C + Alice A	
4	=	659000	-99500	27/3	IF3134
5	=	559500	-1000000	31/3	F7233
6	=	459500	+404000	for Charlie C	
7	=	863500	+ 292000	for Bob B + Charlie C	
8	=	1155500	-109000	4/4	A4184
9	=	1055500	-100000	6/4	KK3240
10	=	955500	+4500	he gave me	
11	=	960000	-50000	7/4	MF0267
12	=	910000	-100000	CD7488	
13	=	810000	-100000	18/4	L5583
14	=	679000	-100000	26/4	L1272
15	=	579000	-20000		
16	=	559000	-100000	28/4	
17					
18					
19					
20					
21					
22					

PD reports that further inquiries reveal a neighbor has a Ring camera with a direct view towards the victim’s back door.

Camera footage obtained from it shows Charlie Cyber entering Bob’s house via the back door moments before Bob’s death and exiting shortly thereafter.



Data Correlation (again)

Data to Correlate

- SMS Messages
  - Bob's phone
  - Alice's phone
- Email showing Alice's trip via Lyft (updated)
- Encrypted space with hidden files
  - Ledger

- Reports from PD
  - Information about Alice's fingerprints
  - Concern about Alice's temper

After reviewing evidence revealed in the encrypted file, PD explains to you and the rest of the forensic team that the portion of the serial numbers found in photos of currency are often used by drug dealers to match sellers to buyers

Final Conclusion

Charlie killed Bob.





Post Incident

Post Incident Goals

- Review of what was good/bad
- Was enough information provided?
- Outcomes achieved (both positive/negative)
- Any further work could be completed?
- Feedback from each team
- Any technical challenges identified for future reference
- Full documentation of what was achieved/not achieved

Post Incident Tools

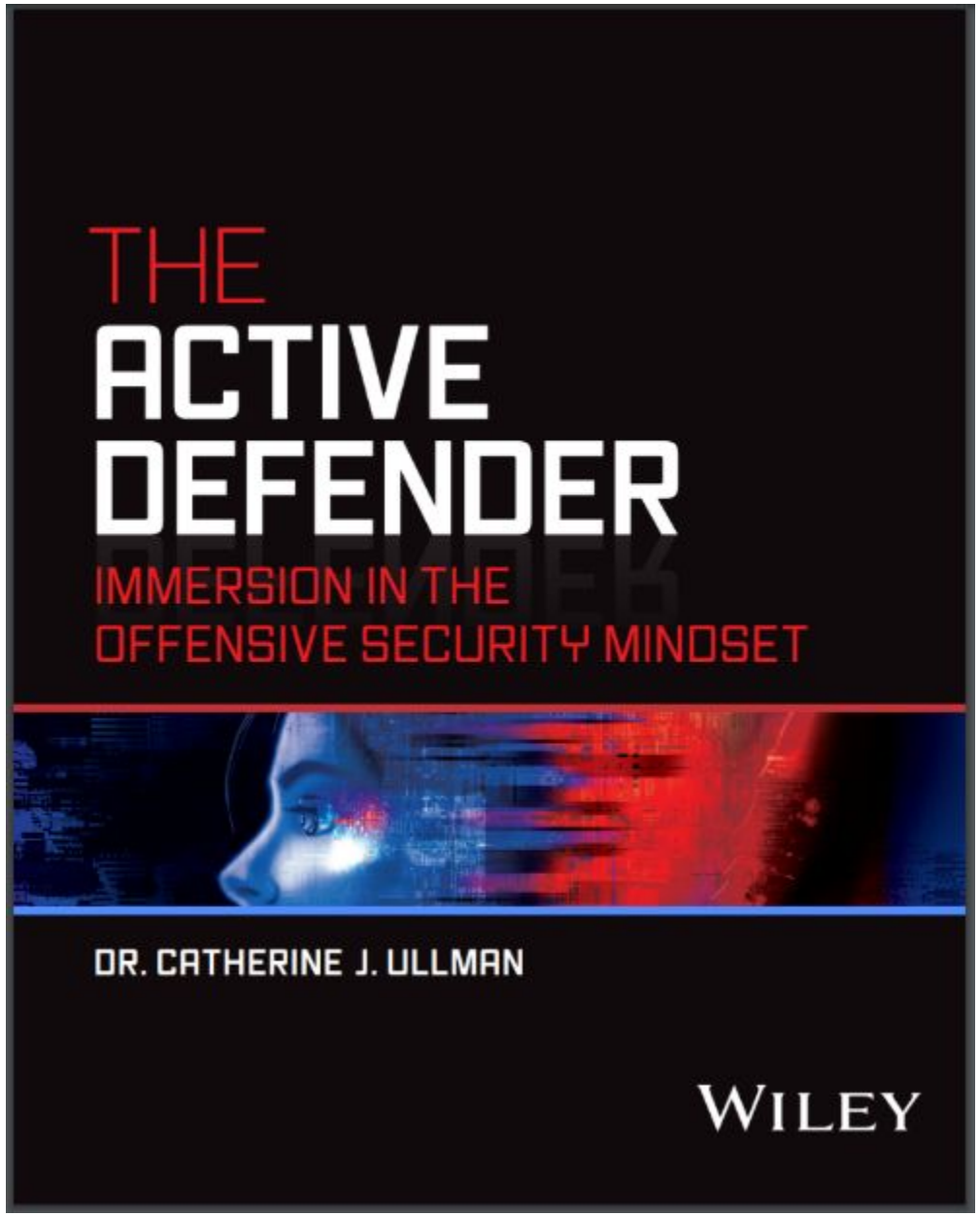
- Communication e.g. document ALL THE THINGS
- Paper/pen/computer/etc.

Post Incident Challenges

- Not documenting at all (e.g. too hurried to write up a report)
- Forgetting to document activities (e.g. documenting imaging a phone, but not a desktop)
- Forgetting to provide context to documentation (e.g. machine is located in a public space)
- Documenting something that did not occur. (e.g. inferences made by the investigator)
- Full story not told through documentation. (e.g. requiring reader to make assumptions)
- After action meeting not held or documented



"I may not have gone where I intended to go, but I think that I have ended up where I needed to be." ~Douglas Adams



Shameless Self-Promotion

Available in both hardcopy and e-book from booksellers everywhere!