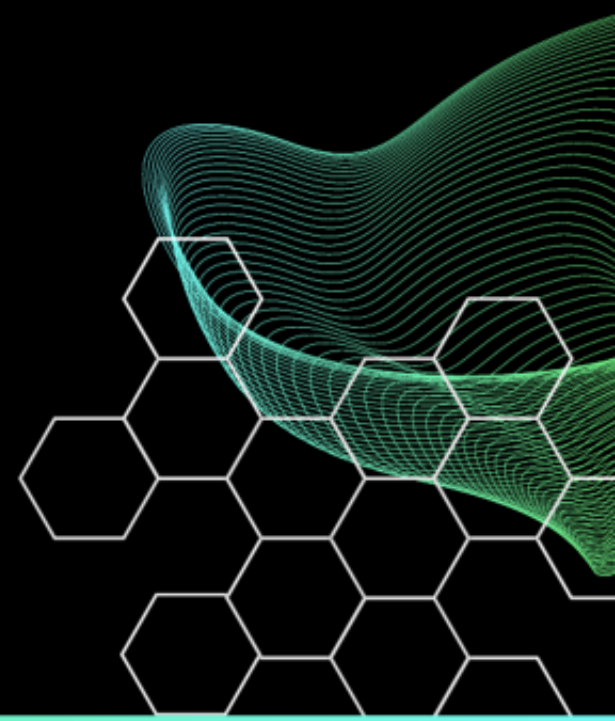


Missing Pieces:



Tips and Tricks on how to ensure your
acquisitions aren't missing critical
data

Cesar Quezada, ArcPoint
Jessica Hyde, Hexordia



MEET CESAR

RESEARCH & DEVELOPMENT ENGINEER, ARCPPOINT

- Sr. Technical Exploitation Officer, Mantech
- CDR, 133rd Cyber Security Company, Army National Guard

Previous:

- Basis Technology
- Booz Allen Hamilton
- General Dynamics Information Technology
- Army Intelligence Officer

M.S. in Computer Forensics, George Mason University
Reviewer, DFIR Review



MEET JESSICA

FOUNDER & OWNER, HEXORDIA

- **Adjunct Professor, George Mason University**

Previous:

- **Director Forensics, Magnet Forensics**
- **Basis Technology**
- **Ernst and Young**
- **American Systems**

- **M.S. in Computer Forensics, George Mason University**
- **Chair, DFIR Review**
- **Advisory Board, Cyber Sleuth Labs**
- **HTCIA IEC 2nd VP**
- **Associate Editor, Forensic Science International: Digital Investigations**



AGENDA

- Why do we care
- Examples of Data could be missing
 - Hard Drives
 - Mobile
- How to Test to determine
- Questions



HEXORDIA



Why do we care?





Don't know what you don't
know



Triage Extractions

Important!

Why waste time on a full when you can get a partial

And in some instances, it is all you need –

i.e. internal investigations, malware, etc.

Triage Extractions

Important!

Why waste time on a full when you can get a partial

And in some instances, it is all you need –

i.e. internal investigations, malware, etc.

However, this may be a problem if you need to provide all exonerable content

Scope?

Difference between examination and analysis vs collection?

- Do you limit on collection?
- Do you limit on analysis?

Computers / Hard Drives



Examples of Data You Could be missing



Don't know what you don't know

Some drives are incompatible with communicating to Linux and can only communicate with a Windows or MacOS

ex Samsung T7+ drives using Samsung's encryption

Samsung T7 Touch



Source:

https://downloadcenter.samsung.com/content/UM/202111/20211108104322367/T7_Touch_User_Manual_English_1.1.pdf



Samsung T7 Touch

When I connect the T7 Touch to devices other than a PC, they do not recognize the T7 Touch.

The T7 Touch was developed for use with **Windows OS and Mac OS** PCs and mobile devices. When connected to devices other than those, the T7 Touch may not be recognized or use of its features may be restricted depending on their level of support. Moreover, if you have enabled security mode with Password, you cannot enter your password from non-PC or non-mobile devices and thus will be unable to access data stored on the T7 Touch. Please disable the security mode before using the T7 Touch with such devices.

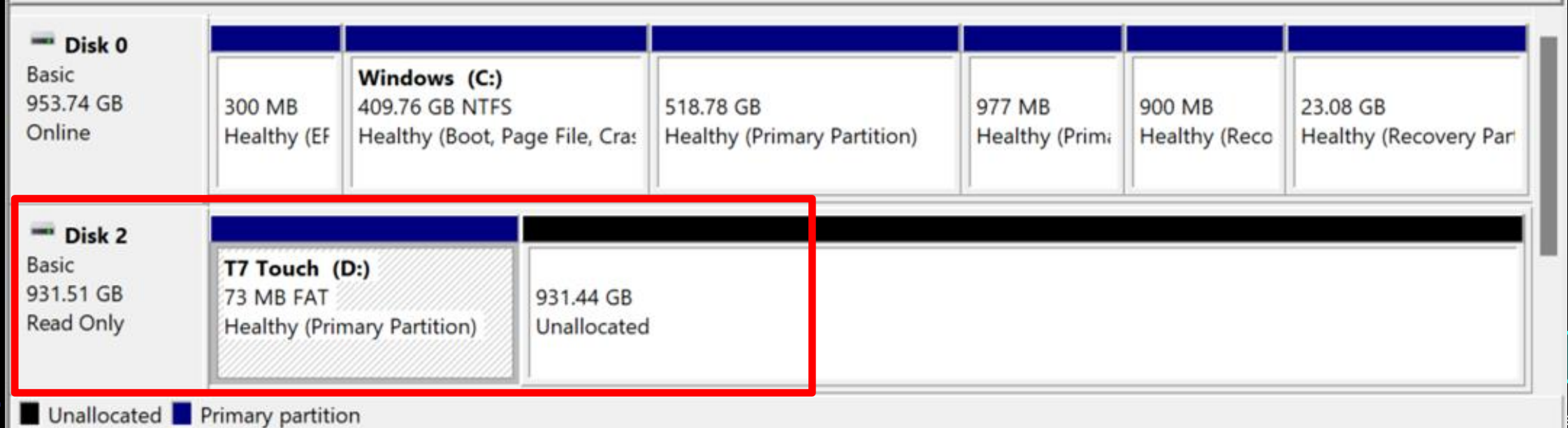
Source:

https://downloadcenter.samsung.com/content/UM/202111/20211108104322367/T7_Touch_User_Manual_English_1.1.pdf



Without fingerprint: Locked

Volume	Layout	Type	File System	Status	Capacity	Free Sp...	% Free
(Disk 0 partition 1)	Simple	Basic		Healthy (E...	300 MB	300 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (R...	900 MB	900 MB	100 %
(Disk 0 partition 5)	Simple	Basic		Healthy (R...	23.08 GB	23.08 GB	100 %
(Disk 0 partition 6)	Simple	Basic		Healthy (P...	518.78 GB	518.78 GB	100 %
(Disk 0 partition 7)	Simple	Basic		Healthy (P...	977 MB	977 MB	100 %
T7 Touch (...)	Simple	Basic	FAT	Healthy (P...	73 MB	1 MB	1 %
Windows (C:)	Simple	Basic	NTFS	Healthy (B...	409.76 GB	183.72 GB	45 %



With fingerprint: Unlocked

Volume	Layout	Type	File System	Status	Capacity	Free Sp...	% Free
(Disk 0 partition 1)	Simple	Basic		Healthy (E...	300 MB	300 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (R...	900 MB	900 MB	100 %
(Disk 0 partition 5)	Simple	Basic		Healthy (R...	23.08 GB	23.08 GB	100 %
(Disk 0 partition 6)	Simple	Basic		Healthy (P...	518.78 GB	518.78 GB	100 %
(Disk 0 partition 7)	Simple	Basic		Healthy (P...	977 MB	977 MB	100 %
(Disk 2 partition 1)	Simple	Basic		Healthy (E...	200 MB	200 MB	100 %
Hidden	Simple	Basic	exFAT	Healthy (B...	4.65 GB	4.65 GB	100 %
T7 (E:)	Simple	Basic	exFAT	Healthy (B...	926.63 GB	926.62 GB	100 %
Windows (C:)	Simple	Basic	NTFS	Healthy (B...	409.76 GB	149.22 GB	36 %

Disk 0 Basic 953.74 GB Online	300 MB Healthy (Windows (C:) 409.76 GB NTFS Healthy (Boot, Page File,	518.78 GB Healthy (Primary Partitio	977 MB Healthy (Pri	900 MB Healthy (Re	23.08 GB Healthy (Recovery
Disk 2 Basic 931.51 GB Online	200 MB Healthy (EFI System	T7 (E:) 926.66 GB exFAT Healthy (Basic Data Partition)	Hidden 4.66 GB exFAT Healthy (Basic Data Partition)			

■ Unallocated ■ Primary partition



Samsung T7 Touch – Fingerprint Locked

The screenshot shows a Windows File Explorer window. On the left sidebar, the drive 'T7 Touch (D:)' is selected and highlighted with a red box. Below it, the folder 'SamsungPortableSSD_1.0.app' is also highlighted with a red box. The main pane displays the contents of this folder, which are also highlighted with a red box. The contents include:

Name	Date modified	Type
SamsungPortableSSD_1.0	8/5/2021 11:06 PM	App
This is Read Only partition	8/5/2021 11:06 PM	Text
Samsung Portable SSD SW for Android	8/5/2021 11:06 PM	Text
SamsungPortableSSD_1.0.app	8/5/2021 11:06 PM	File



Samsung T7 Touch – Fingerprint unlocked

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- Music
- Videos

OneDrive - Personal CESAR

This PC

- T7 Touch (D:)**
 - .fseventsd
 - .Spotlight-V100
 - .TemporaryItems

Name	Date modified	Type
._Testing	5/20/2022 1:49 PM	Text
Testing	5/20/2022 1:49 PM	Text
SoftwareLicense_NewComputer_2022-05-27_20-03-10.C2V	5/27/2022 8:06 PM	C2V
SamsungPortableSSD_Setup_Win_1.0	4/5/2020 10:59 PM	App
SamsungPortableSSD_Setup_Mac_1.0.pkg	4/5/2020 10:59 PM	PKG
Samsung portable SSD SW for Android	1/20/2016 1:41 AM	Text
.TemporaryItems	5/20/2022 1:50 PM	File
.fseventsd	5/20/2022 12:46 PM	File
.Spotlight-V100	5/15/2022 6:49 PM	File



Without fingerprint: Locked

The screenshot displays a forensic analysis tool interface. On the left, a file system tree shows a partition containing several folders, including 'SamsungPortableSSD_1.0.app' and 'UniversalApp'. Below the tree, the 'Properties' window is open, showing the following information:

Evidence Source Path	\\PHYSICALDRIVE2
Evidence Type	Physical Disk
Disk	
Drive Geometry	
Cylinders	121,601
Tracks per Cylinder	255
Sectors per Track	63
Bytes per Sector	512
Sector Count	1,953,525,168
Physical Drive Information	
Drive Model	Samsung PSSD T7 Touch SCSI Disk De

On the right, a hex dump window shows the raw data of the disk. A red box highlights a section of the dump from offset 000000000 to 0000000d0. The data is mostly zeros, with some non-zero values at the end of the highlighted section, including 'FD 7F 84' and 'fy'. The cursor position is 0; phy sec = 0.



With fingerprint: Unlocked

AccessData FTK Imager 4.5.0.3

File View Mod Help

Evidence Tree

- PHYSICALDRIVE2
 - Partition 1 [953867MB]
 - T7 Touch [exFAT]
 - [root]
 - \$RECYCLE.BIN
 - .fsevents
 - .Spotlight-V100
 - .TemporaryItems
 - System Volume Information
 - [unallocated space]
 - Unpartitioned Space [basic disk]
 - [unallocated space]

File List

Name	Size	Type	Date Modified
\$RECYCLE.BIN	128	Directory	6/8/2022 3:30:30 PM
.fsevents	128	Directory	6/20/2022 4:46:29 ...
.Spotlight-V100	128	Directory	6/15/2022 10:49:04...
.TemporaryItems	128	Directory	6/20/2022 5:50:00 ...
System Volume Information	128	Directory	6/8/2022 3:29:51 PM
._Testing.txt	4	Regular File	6/20/2022 5:49:42 ...
._Testing.txt.FileSlack	124	File Slack	
<input checked="" type="checkbox"/> ._Testing.txt.sb-c9771a4f-vENL6H	4	Regular File	6/20/2022 5:49:31 ...
Samsung portable SSD SW for A...	1	Regular File	1/20/2016 6:41:24 ...
Samsung portable SSD SW for A...	128	File Slack	
SamsungPortableSSD_Setup_Ma...	10,171	Regular File	4/6/2020 2:59:26 AM
SamsungPortableSSD_Setup_Ma...	70	File Slack	
<input checked="" type="checkbox"/> SamsungPortableSSD_Setup_Wi...	7,686	Regular File	4/6/2020 2:59:38 AM
SamsungPortableSSD_Setup_Wi...	123	File Slack	
SoftwareLicense_NewComputer_...	1	Regular File	5/28/2022 12:06:12...
SoftwareLicense_NewComputer_...	128	File Slack	
Testing.txt	1	Regular File	6/20/2022 5:49:41 ...
Testing.txt.FileSlack	128	File Slack	
<input checked="" type="checkbox"/> Testing.txt.sb-c9771a4f-vENL6H	0	Regular File	6/8/2022 3:34:30 PM

Properties

Name [root]
File Class Regular File
File Size 0
Physical Size 0
Start Cluster 0
Date Accessed N/A
Date Created N/A
Date Modified N/A
Actual File True

Hex Value Interpreter Custom Content Sources

For User Guide, press F1

```
0000 83 08 54 00 37 00 20 00-54 00 6F 00 75 00 63 00  --T-7- -T-o-u-c-
0010 68 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  h.....
0020 81 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
0030 00 00 00 00 02 00 00 00-ED 8D 0E 00 00 00 00 00  .....i
0040 82 00 00 00 0D D3 19 E6-00 00 00 00 00 00 00 00  ....ó-e.....
0050 00 00 00 00 0A 00 00 00-CC 16 00 00 00 00 00 00 00  .....i.....
0060 85 04 C2 66 20 00 00 00-FD 12 BB 50 2C 35 34 48  --Äf --ý-wP,54H
0070 2D 16 D0 54 91 00 80 80-90 00 00 00 00 00 00 00 00  --DT.....
0080 C0 03 00 27 CD EA 00 00-76 00 00 00 00 00 00 00 00  Ä-·íe-v.....
0090 00 00 00 00 0C 00 00 00-76 00 00 00 00 00 00 00 00  .....v.....
00a0 C1 00 53 00 61 00 6D 00-73 00 75 00 6E 00 67 00  Ä-S-a-m-s-u-n-g-
00b0 20 00 70 00 6F 00 72 00-74 00 61 00 62 00 6C 00  p-o-r-t-a-b-l-
00c0 C1 00 65 00 20 00 53 00-53 00 44 00 20 00 53 00  Ä-e-S-S-D-S-
00d0 57 00 20 00 66 00 6F 00-72 00 20 00 41 00 6E 00  W-f-o-r-A-n-
00e0 C1 00 64 00 72 00 6F 00-69 00 64 00 2E 00 74 00  Ä-d-r-o-i-d-.t-
00f0 78 00 74 00 00 00 00 00-00 00 00 00 00 00 00 00 00  x-t.....
0100 85 04 83 AE 20 00 00 00-FD 5A BB 50 6D 5F 86 50  --ö --ýZePm_P
0110 22 16 D0 54 94 00 A4 A4-90 00 00 00 00 00 00 00 00  "DI-ññ.....
0120 C0 03 00 24 C7 63 00 00-DD E9 9E 00 00 00 00 00 00  Ä-çc-ÿe.....
0130 00 00 00 00 0D 00 00 00-DD E9 9E 00 00 00 00 00 00  .....ÿe.....
0140 C1 00 53 00 61 00 6D 00-73 00 75 00 6E 00 67 00  Ä-S-a-m-s-u-n-g-
0150 50 00 6F 00 72 00 74 00-61 00 62 00 6C 00 65 00  P-o-r-t-a-b-l-e-
```



With fingerprint: Unlocked

```
00000 83 08 54 00 37 00 20 00-54 00 6F 00 75 00 63 00  .-T-7- -T-o-u-c-
00010 68 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  h.....
00020 81 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
00030 00 00 00 00 02 00 00 00-ED 8D 0E 00 00 00 00 00  .....i.....
00040 82 00 00 00 0D D3 19 E6-00 00 00 00 00 00 00 00  ....óæ.....
00050 00 00 00 00 0A 00 00 00-CC 16 00 00 00 00 00 00 00  .....Ī.....
00060 85 04 C2 66 20 00 00 00-FD 12 BB 50 2C 35 34 48  -Äf ...ÿ»P,54H
00070 2D 16 D0 54 91 00 80 80-90 00 00 00 00 00 00 00 00  -DT.....
00080 C0 03 00 27 CD EA 00 00-76 00 00 00 00 00 00 00  Ä..'íé..v.....
00090 00 00 00 00 0C 00 00 00-76 00 00 00 00 00 00 00  .....v.....
000a0 C1 00 53 00 61 00 6D 00-73 00 75 00 6E 00 67 00  Ä-S-a-m-s-u-n-g-
000b0 20 00 70 00 6F 00 72 00-74 00 61 00 62 00 6C 00  .p-o-r-t-a-b-l-
000c0 C1 00 65 00 20 00 53 00-53 00 44 00 20 00 53 00  Ä-e- -S-S-D- -S-
000d0 57 00 20 00 66 00 6F 00-72 00 20 00 41 00 6E 00  W- f-o-r- A-n-
000e0 C1 00 64 00 72 00 6F 00-69 00 64 00 2E 00 74 00  Ä-d-r-o-i-d-.t-
000f0 78 00 74 00 00 00 00 00-00 00 00 00 00 00 00 00  x-t.....
00100 85 04 83 AE 20 00 00 00-FD 5A BB 50 6D 5F 86 50  ...» ...ÿZ»Pm_ -P
00110 22 16 D0 54 94 00 A4 A4-90 00 00 00 00 00 00 00 00  " -DT..nn.....
00120 C0 03 00 24 C7 63 00 00-DD E9 9E 00 00 00 00 00 00  Ä-çc-ÿé.....
00130 00 00 00 00 0D 00 00 00-DD E9 9E 00 00 00 00 00 00  .....ÿé.....
00140 C1 00 53 00 61 00 6D 00-73 00 75 00 6E 00 67 00  Ä-S-a-m-s-u-n-g-
00150 50 00 6F 00 72 00 74 00-61 00 62 00 6C 00 65 00  P-o-r-t-a-b-l-e-
```

Cursor pos = 0; clus = 11; log sec = 65792; phy sec = 67840



Updated Specs for Old Devices

USB 3.2 Gen 2 = 10 Gbps

USB 3.2 Gen 2x2 = 20 Gbps

- Still USB - what could go wrong?
- Be leery of adopting immediately adopting brand new technology
- Test new devices before field use




```
(root@arc004)-[~/home/arc004]
```

```
# fdisk -l /dev/sdb
```

```
Disk /dev/sdb: 931.51 GiB, 1000204886016 bytes, 1953525168 sectors
```

```
Disk model: 2135
```

```
Units: sectors of 1 * 512 = 512 bytes
```

```
Sector size (logical/physical): 512 bytes / 4096 bytes
```

```
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
```

```
Disklabel type: gpt
```

```
Disk identifier: F9988288-A4B8-4504-8900-13C02A1D48E7
```

Device	Start	End	Sectors	Size	Type
/dev/sdb1	2048	739327	737280	360M	EFI System
/dev/sdb2	739328	1001471	262144	128M	Microsoft reserved
/dev/sdb3	1001472	941918207	940916736	448.7G	Microsoft basic data
/dev/sdb4	941918208	943925247	2007040	980M	Windows recovery environment
/dev/sdb5	943925248	972568575	28643328	13.7G	Microsoft basic data
/dev/sdb6	972568576	976762879	4194304	2G	Microsoft basic data




```
(root@arc004) - [ /home/arc004 ]
```

```
# fdisk -l /dev/sdb
```

```
The backup GPT table is corrupt, but the primary appears OK, so that will be used.
```

```
Disk /dev/sdb: 931.51 GiB, 1000204885504 bytes, 1953525167 sectors
```

```
Disk model: BACKUP+
```

```
Units: sectors of 1 * 512 = 512 bytes
```

```
Sector size (logical/physical): 512 bytes / 4096 bytes
```

```
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
```

```
Disklabel type: gpt
```

```
Disk identifier: F9988288-A4B8-4504-8900-13C02A1D48E7
```

Device	Start	End	Sectors	Size	Type
/dev/sdb1	2048	739327	737280	360M	EFI System
/dev/sdb2	739328	1001471	262144	128M	Microsoft reserved
/dev/sdb3	1001472	941918207	940916736	448.7G	Microsoft basic data
/dev/sdb4	941918208	943925247	2007040	980M	Windows recovery environment
/dev/sdb5	943925248	972568575	28643328	13.7G	Microsoft basic data
/dev/sdb6	972568576	976762879	4194304	2G	Microsoft basic data





Evidence Tree

- StarTechAdapter.E01

File List

Name	Size	Type	Date Modified
e8e0db5da0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5db0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5dc0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5dd0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5de0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5df0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5e00	45 46 49 20 50 41 52 54 00 00 01 00 5c 00 00 00	EFI PART	
e8e0db5e10	48 c2 75 ab 00 00 00 00 00 af 6d 70 74 00 00 00 00	HÄu<<.....mpt	
e8e0db5e20	01 00 00 00 00 00 00 00 00 00 22 00 00 00 00 00 00"	
e8e0db5e30	8e 6d 70 74 00 00 00 00 00 88 82 98 f9 b8 a4 04 45	mpt.....ù, M-E	
e8e0db5e40	89 00 13 c0 2a 1d 48 e7 8f 6d 70 74 00 00 00 00	..À* Hç mpt	
e8e0db5e50	80 00 00 00 80 00 00 00 00 89 e7 7a f6 00 00 00 00çzö	
e8e0db5e60	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5e80	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5e90	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5ea0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5eb0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5ec0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5ed0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5ee0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5ef0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5f00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5f10	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5f20	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5f30	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5f40	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5f50	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5f60	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5f70	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5f80	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5f90	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5fa0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5fb0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5fc0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5fd0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5fe0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
e8e0db5ff0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

Custom Content Sources

- Evidence:File System|Path|File
- Options

Properties | Hex Value In... Custom Con...

Cursor pos = 1000204885504; phy sec = 1953525167

Adds all evidence from attached disks

NUM



e8e0db5da0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
e8e0db5db0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
e8e0db5dc0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
e8e0db5dd0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
e8e0db5de0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
e8e0db5df0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
e8e0db5e00	45 46 49 20 50 41 52 54-00 00 01 00 5C 00 00 00	EFI PART \ ...
e8e0db5e10	48 C2 75 AB 00 00 00 00-AF 6D 70 74 00 00 00 00	HÃu« mpt
e8e0db5e20	01 00 00 00 00 00 00 00-22 00 00 00 00 00 00 00".....
e8e0db5e30	8E 6D 70 74 00 00 00 00-88 82 98 F9 B8 A4 04 45	.mpt ù, H ·E
e8e0db5e40	89 00 13 C0 2A 1D 48 E7-8F 6D 70 74 00 00 00 00	...À* ·Hç ·mpt
e8e0db5e50	80 00 00 00 80 00 00 00-89 E7 7A F6 00 00 00 00çzö.....
e8e0db5e60	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00



AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree: Old_Adapter.E01

File List

Name	Size	Type	Date Modified
e8e0db5ba0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5bb0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5bc0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5bd0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5be0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5bf0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5c00	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5c10	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5c20	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5c30	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5c40	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5c50	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5c60	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5c70	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5c80	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5c90	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5ca0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5cb0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5cc0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5cd0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5ce0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5cf0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5d00	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5d10	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5d20	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5d30	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5d40	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5d50	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5d60	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5d70	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5d80	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5d90	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5da0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5db0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5dc0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5dd0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5de0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00
e8e0db5df0	00 00 00 00 00 00 00 00-00	00 00 00 00 00 00 00

Custom Content Sources

system|Path|File Options

New Edit Remove Remove All Create Image

Properties Hex Value In... Custom Con...

Cursor pos = 1000204884992; phy sec = 1953525166

NUM



Disk Size lies

- Courtney Webb presentation at 2017 SANS DFIR
 - Implications of Firmware Trickery Hard Drives
- TLDR – Drive is labeled and appears to be one size, but is actually larger!
 - Tools like HDDHackr allow folks to alter drivesize with firmware manipulation
 - Can fool into thinking a drive is a different size



Microsoft Surface

Problem

- Only 1x USB port

Acquisition Requirements

- Powered USB Hub
- External drive
- Mouse
- Keyboard



Chromebooks

Custom Recovery method for decrypted logical when you have a password based off Daniel Dickerman Method

<https://dfir.pubpub.org>

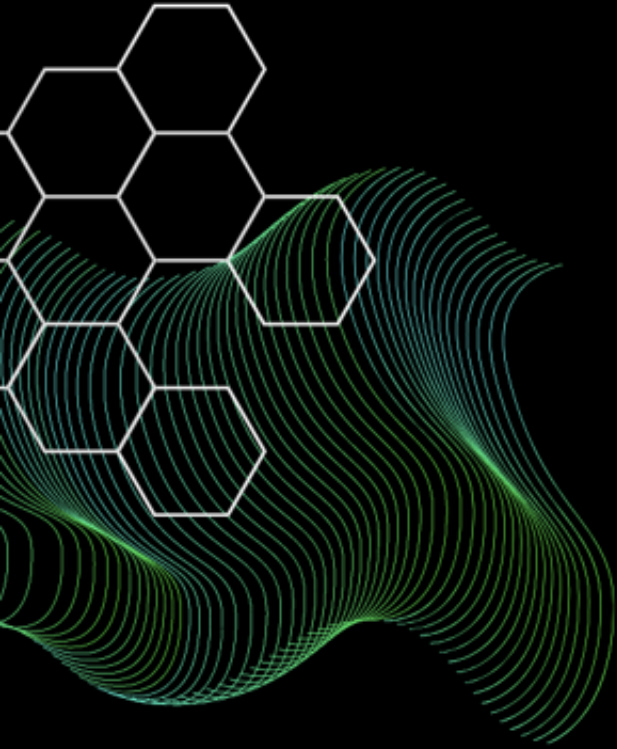


Chromebooks Daniel Dickerman Method

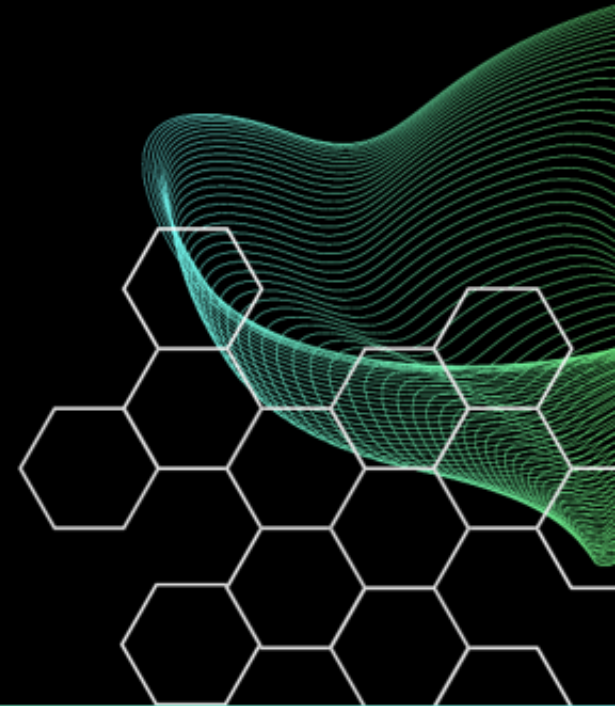
First writes to available space before writing out

So... if you have 64GB drive and 50GB are used - you will only get 14 GB image





Mobile Devices



Mobile Image Types

- Physical Mobile Forensic Image
- Logical Mobile Forensic Image
- Filesystem Mobile Forensic Image



Physical Mobile Forensic Image

**Data pulled directly from a connection
to the device storage area**



Logical Mobile Forensic Image

**Collection of requested data as
interpreted by the operating system**



Filesystem Mobile Forensic Image

Collection of the active files and folders from the file system which may contain remnants of data and non-user data



Android Example

Physical image only includes data from 1 chip; Not all

Make sure you are looking at specs for what device can hold





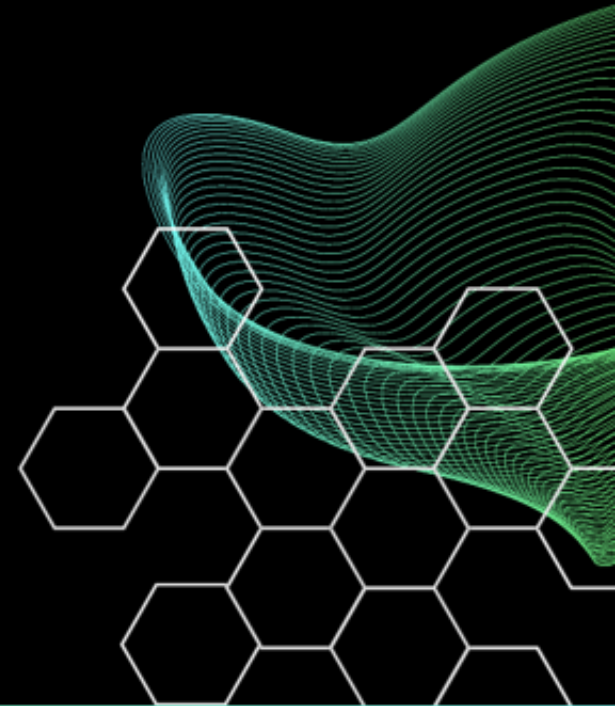
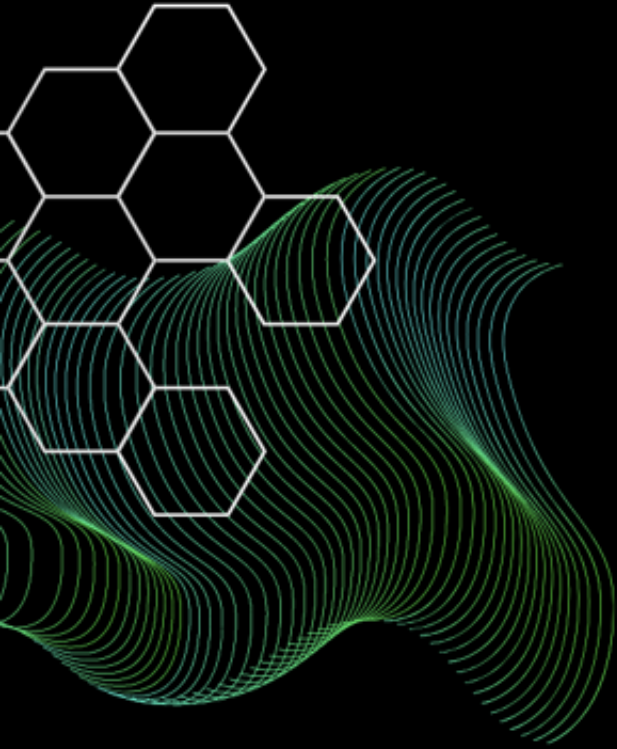
Triage Extractions

There is total value to these, but there could be issues as well...





Android



Android Comparative – Equipment User Data

Test Data	Logical	FFS
IMEI/MEID/ESN	Present	Present
MSISDN	Present	Present



Source: Jay Varda of Gray Shift



HEXORDIA

Android Comparative – PIM Data

Test Data	Logical	FFS
Contacts	Present	Present
Calendar	Present	Present
Memos / Notes	Not Present	Present



Source: Jay Varda of Gray Shift



HEXORDIA

Android Comparative – Call Logs

Test Data	Logical	FFS
Incoming	Present	Present
Outgoing	Present	Present
Missed	Present	Present



Source: Jay Varda of Gray Shift



HEXORDIA

Android Comparative – SMS Messages

Test Data	Logical	FFS
Incoming	Present	Present
Outgoing	Present	Present



Source: Jay Varda of Gray Shift



HEXORDIA

Android Comparative – MMS Messages

Test Data	Logical	FFS
Graphic	Present	Present
Audio	Present	Present
Video	Present	Present



Source: Jay Varda of Gray Shift



HEXORDIA

Android Comparative – Stand Alone Files

Test Data	Logical	FFS
Graphic	Partial	Present
Audio	Partial	Present
Video	Partial	Present



Source: Jay Varda of Gray Shift



HEXORDIA

Android Comparative – Application Data

Test Data	Logical	FFS
Documents (txt, pdf files)	Partial	Present



Source: Jay Varda of Gray Shift



HEXORDIA

Android Comparative – Social Media Data

Test Data	Logical	FFS
Facebook	Not Present	Present
Snapchat	Not Present	Present



Source: Jay Varda of Gray Shift



HEXORDIA

Android Comparative – Communication App Data

Test Data	Logical	FFS
Signal	Not Present	Present
Facebook Messenger	Not Present	Present
WhatsApp	Not Present	Present



Source: Jay Varda of Gray Shift



HEXORDIA

Android Comparative – Internet Data

Test Data	Logical	FFS
Chrome Bookmarks	Not Present	Present
Chrome History	Not Present	Present



Source: Jay Varda of Gray Shift



HEXORDIA

Android Comparative - Email

Test Data	Logical	FFS
Gmail	Not Present	Present



Source: Jay Varda of Gray Shift



HEXORDIA

Android Comparative – OS / App Activity

Test Data	Logical	FFS
Usage History	Partial	Present
Application Permissions	Not Present	Present
Google Play	Not Present	Present
App Power Usage	Present	Present

Source: Jay Varda of Gray Shift



HEXORDIA

Android Comparative – Deleted

Test Data	Logical	FFS
Artifacts	Not Present	Possible



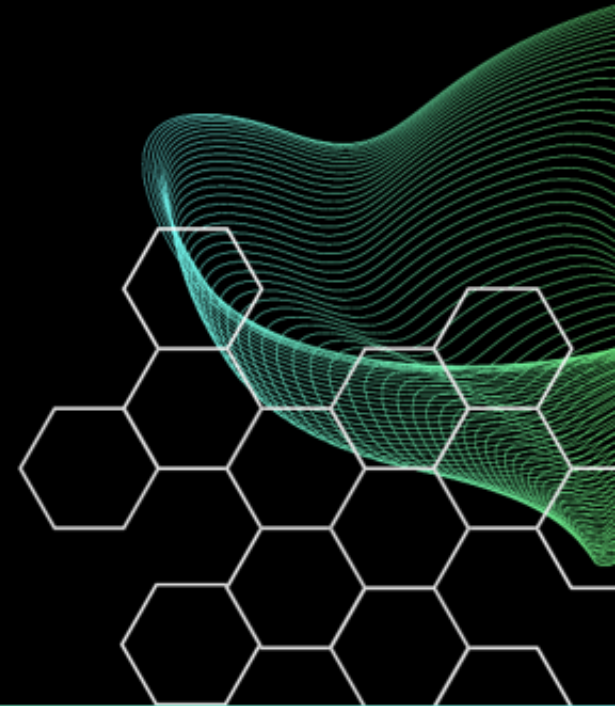
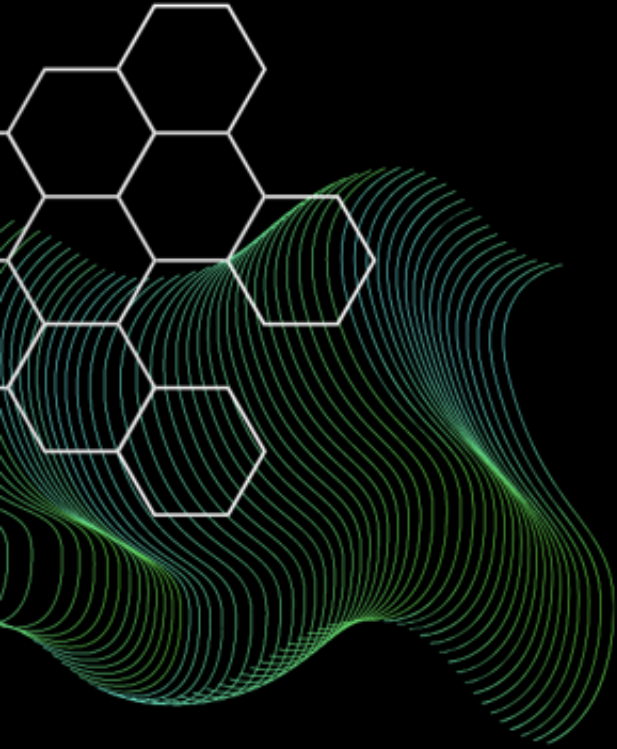
Source: Jay Varda of Gray Shift



HEXORDIA



iOS



HEXORDIA

AFU vs BFU

After First
Unlock

Before First
Unlock



iOS Comparative – Equipment User Data

Test Data	BFU	Logical	AFU	FFS
IMEI/MEID /ESN	Present	Present	Present	Present
MSISDN	Present	Present	Present	Present



Source: Jay Varda of Gray Shift



HEXORDIA

iOS Comparative – PIM Data

Test Data	BFU	Logical	AFU	FFS
Contacts	Not Present	Present	Present	Present
Calendar	Not Present	Present	Present	Present
Memos / Notes	Not Present	Present	Present	Present



iOS Comparative – Call Logs

Test Data	BFU	Logical	AFU	FFS
Incoming	Partial	Present	Present	Present
Outgoing	Partial	Present	Present	Present
Missed	Partial	Present	Present	Present



iOS Comparative – SMS Messages

Test Data	BFU	Logical	AFU	FFS
Incoming	Not Present	Present	Present	Present
Outgoing	Not Present	Present	Present	Present

Source: Jay Varda of Gray Shift



iOS Comparative – MMS Messages

Test Data	BFU	Logical	AFU	FFS
Graphic	Not Present	Present	Present	Present
Audio	Not Present	Present	Present	Present
Video	Not Present	Present	Present	Present



iOS Comparative – Stand Alone Files

Test Data	BFU	Logical	AFU	FFS
Graphic	Partial	Partial	Present	Present
Audio	Partial	Partial	Present	Present
Video	Partial	Partial	Present	Present



Source: Jay Varda of Gray Shift



HEXORDIA

iOS Comparative – Application Data

Test Data	BFU	Logical	AFU	FFS
Documents (txt, pdf files)	Partial	Partial	Present	Present
Apple Health	Not Present	Present	Not Present	Present

Source: Jay Varda of Gray Shift



HEXORDIA

iOS Comparative – Social Media Data

Test Data	BFU	Logical	AFU	FFS
Facebook	Not Present	Not Present	Present	Present
Snapchat	Present	Not Present	Present	Present

Source: Jay Varda of Gray Shift



HEXORDIA

iOS Comparative – Communication App Data

Test Data	BFU	Logical	AFU	FFS
Signal	Not Present	Not Present	Present	Present
Facebook Messenger	Not Present	Not Present	Present	Present
WhatsApp	Not Present	Present	Present	Present



iOS Comparative – Internet Data

Test Data	BFU	Logical	AFU	FFS
Safari Bookmarks	Not Present	Present	Present	Present
Safari History	Partial	Present	Present	Present



Source: Jay Varda of Gray Shift



HEXORDIA

iOS Comparative - Email

Test Data	BFU	Logical	AFU	FFS
Apple Mail	Not Present	Not Present	Not Present	Present



Source: Jay Varda of Gray Shift



HEXORDIA

iOS Comparative – GPS Data

Test Data	BFU	Logical	AFU	FFS
Coordinates / Geo-tagged	Not Present	Partial	Present	Present
Significant Locations	Not Present	Not Present	Not Present	Present
Cached Locations	Not Present	Not Present	Not Present	Present

Source: Jay Varda of Gray Shift



iOS Comparative – OS / App Activity

Test Data	BFU	Logical	AFU	FFS
KnowledgeC	Not Present	Not Present	Present	Present
Airdrop	Not Present	Not Present	Present	Present
User Word Dictionary	Not Present	Not Present	Present	Present
PowerLog	Not Present	Not Present	Present	Present



Source: Jay Varda of Gray Shift



XORDIA

iOS Comparative – Deleted

Test Data	BFU	Logical	AFU	FFS
Artifacts	Not Present	Not Present	Possible	Possible



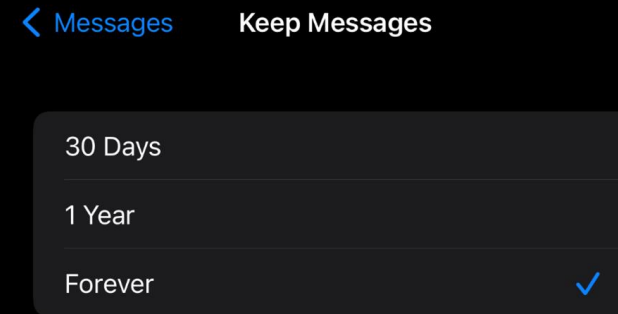
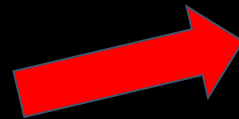
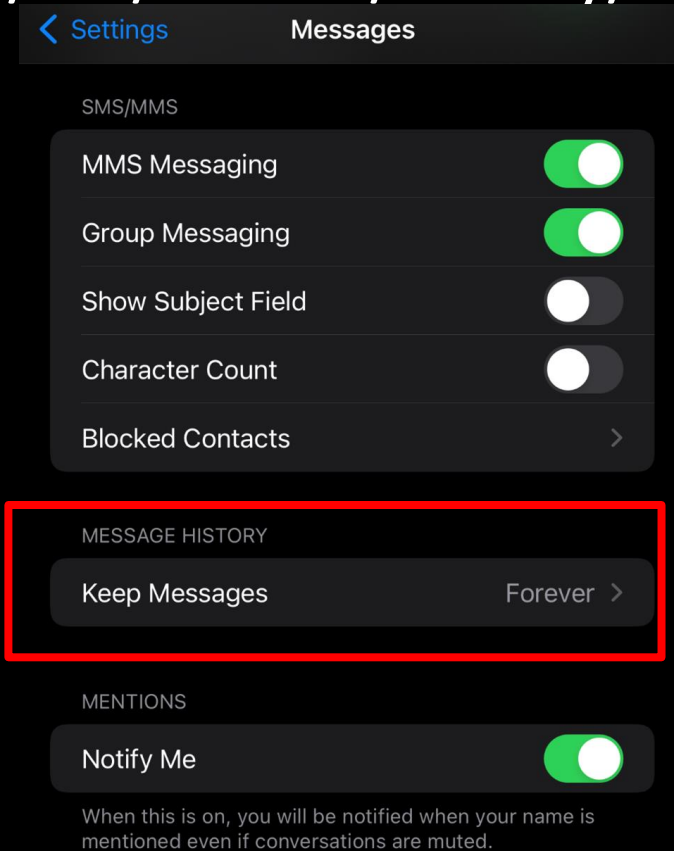
Source: Jay Varda of Gray Shift



HEXORDIA

iOS Message Retention

/private/var/mobile/Library/Preferences/com.apple.MobileSMS.plist



iOS Message Retention

`/private/var/mobile/Library/Preferences/com.apple.MobileSMS.plist`

ACTION

1. Imaged iOS device and left it on Forever.
2. Changed option to 1 year and re-imaged iOS device.

RESULT

1. The KeepMessageForDays key did not appear.
2. The KeepMessageForDays key appears with a value of 365.



iOS Message Retention

`/private/var/mobile/Library/Preferences/com.apple.MobileSMS.plist`

ACTION

3. Changed option to 30 days and re-imaged iOS device.
4. Changed option back to Forever and re-imaged iOS device.

RESULT

3. The KeepMessageForDays key appears with a value of 30.
4. The KeepMessageForDays key appears with a value of 0.



iOS – Retention not

Are you losing data because of iOS default retention rates?

- Safari History – 30 days
- Deleted Photos – 30 days
- Knowledge C – differs by artifact all under 30 days
- Cached locations – 7 days
- Call Logs – can vary by carrier





How to Determine



How do you know

- Listen to the community –
 - #DFIR on Twitter for findings
 - Thisweekin4n6 for blogs from community
 - Digital Forensics Discord Server – conversation about issued
- Ask questions when you don't see what you expect
- Test, Test, Test!



Testing, Testing, Testing



HOW TO USE
EXEMPLARS



HOW TO POPULATE



Validate assumptions



Summary

- Triage images are valuable, they won't have all the data
- Once you have the image, you may not have another opportunity, so ensure it is complete
- Tools may not be self-aware that a collection is incomplete
- The examiner's knowledge is critical
- State of the device at time of acquisition is important
- Time from seizure to acquisition is important



Questions



Jessica Hyde
@B1N2H3X

Cesar Quezada
@CQ_DFIR

