Comparative Analysis of Data Extraction Methods: Evaluating the Effectiveness of Forensic Tools

Author: Olivia D. Renfro

Reviewed and Acknowledged: George Rodriguez

The purpose of this research is to better align mobile data extraction methods with case-specific investigative needs. With the increasing reliance on mobile devices in criminal and civil investigations, selecting the most effective extraction and analysis tools is crucial for obtaining relevant digital evidence.

Extracting data from iOS devices is a vital aspect of mobile forensics, enabling investigators to recover critical digital evidence. Different extraction methods provide varying levels of access and data integrity, each suited to specific forensic needs. iTunes backup extraction[1] creates a backup through Apple's iTunes software, Quick Image extraction[2] captures a logical image of a device, Advanced Logical extraction builds upon logical methods by accessing additional files, such as application sandboxes[3] and specific system artifacts. Full file system (FFS) extraction[4] is the most comprehensive approach, capturing all data stored on a device. Understanding these extraction techniques helps forensic analysts select the most appropriate method based on a device's security measures and the needs of the investigation.

The device under examination is an iPhone 14 running iOS 18.3.0 with 128 GB of storage, of which 107.02 GB is used. As a personal device, it is primarily utilized for daily activities, with the majority of storage consumed by applications such as Spotify, Snapchat, and Facebook. These apps suggest heavy media streaming, social interaction, and communication usage. The user maintains a high average screen time of 20 hours per day, indicating extensive engagement with the device for entertainment, messaging, and social media.

To analyze extracted data effectively, forensic professionals rely on advanced tools such as Belkasoft Evidence Center X, Axiom Cyber[5], and Cellebrite Physical Analyzer. Belkasoft Evidence Center X is a powerful digital forensics tool that enables investigators to extract, analyze, and visualize data from multiple sources, including computers, mobile devices, and cloud services.[6] Axiom Examine, developed by Magnet Forensics, is the analysis component of

[1] Creates a logical copy of user data, including messages, call logs, and app data, but it does not retrieve deleted or system files.

[2] A fast, intrusive method that captures essential user data without requiring a full backup.

[3] An application sandbox is a security mechanism that isolates applications from the underlying operating system and other apps, restricting their access to system resources and user data.

[4] Allowing forensic examiners to access all user and system data, including deleted and encrypted content, often requiring device exploitation or a jailbreak. FFS require a keychain to unlock all encrypted content.

[5] Both Axiom Process and Axiom Examine were used.

[6] It specializes in recovering deleted files, parsing application data, and identifying hidden artifacts.

Magnet Axiom, offering a user-friendly interface to investigate digital evidence from mobile devices, computers, and cloud sources.[7] Cellebrite Physical Analyzer[8] is a leading mobile forensic tool designed for in-depth examination of mobile device data. Each of these tools plays a crucial role in mobile forensics, enabling investigators to efficiently analyze and interpret digital evidence.

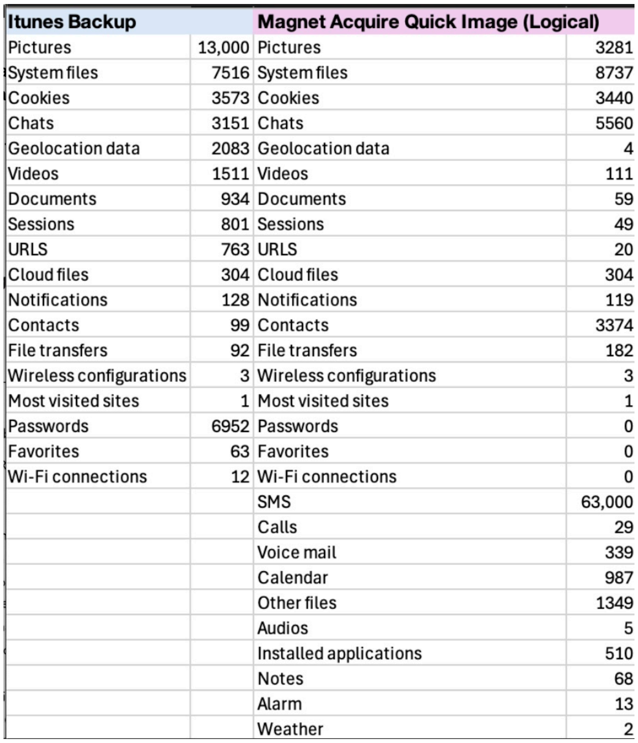
Over a series of days, the unaltered device was systematically processed using various extraction methods to ensure a comprehensive evaluation of data retrieval capabilities. Each method was conducted under controlled conditions to maintain consistency. Following extraction, the datasets were analyzed using the most current versions of forensic examination tools. This approach ensured that the analysis leveraged the latest software capabilities, providing an accurate assessment of each tool's effectiveness in parsing and interpreting the extracted data.

We will begin by conducting a comparative analysis of an iTunes backup (version 12.13.4.4) and a Magnet Acquire Quick Image (version 2.81.0.41575) to assess their effectiveness in extracting data from the device. This comparison will focus on the volume and types of data recovered, including images, system files, application data, and deleted content. By evaluating these extraction methods side by side, we aim to determine which approach provides a more comprehensive dataset for forensic analysis. Additionally, this assessment will help identify any limitations or advantages each method offers, ensuring a clearer understanding of how they perform in real-world investigative scenarios.

[7] With features like keyword searching, timeline analysis, and built-in reporting tools, it is widely used in both law enforcement and corporate investigations.

[8] Supports physical, logical, and file system extractions. It excels at decoding complex data structures, reconstructing deleted files, and providing advanced analytical capabilities such as timeline views and application artifact parsing.

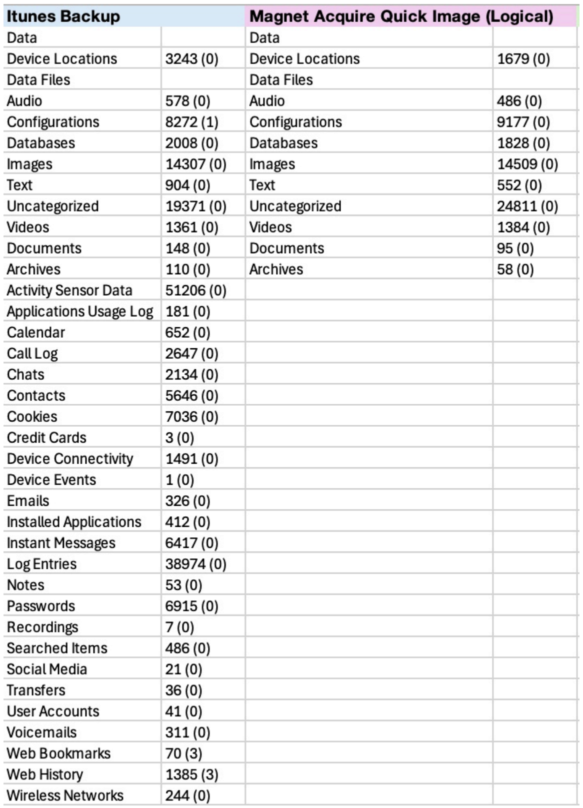
Figure 1



Itunes Backup		Magnet Acquire Quick Image (Logical)	
Pictures	13,000	Pictures	3281
System files	7516	System files	8737
Cookies	3573	Cookies	3440
Chats	3151	Chats	5560
Geolocation data	2083	Geolocation data	4
Videos	1511	Videos	111
Documents	934	Documents	59
Sessions	801	Sessions	49
URLS	763	URLS	20
Cloud files	304	Cloud files	304
Notifications	128	Notifications	119
Contacts	99	Contacts	3374
File transfers	92	File transfers	182
Wireless configurations	3	Wireless configurations	3
Most visited sites	1	Most visited sites	1
Passwords	6952	Passwords	0
Favorites	63	Favorites	0
Wi-Fi connections	12	Wi-Fi connections	0
		SMS	63,000
		Calls	29
		Voice mail	339
		Calendar	987
		Other files	1349
		Audios	5
		Installed applications	510
		Notes	68
		Alarm	13
		Weather	2

Belkasoft X (Version 2.6.18629)

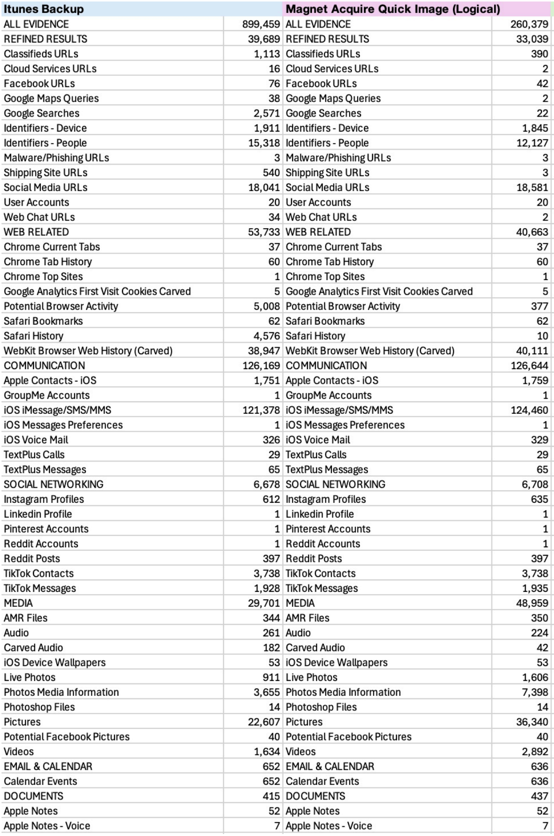
Figure 2



Itunes Backup		Magnet Acquire Quick Image (Logical)	
Data		Data	
Device Locations	3243 (0)	Device Locations	1679 (0)
Data Files		Data Files	
Audio	578 (0)	Audio	486 (0)
Configurations	8272 (1)	Configurations	9177 (0)
Databases	2008 (0)	Databases	1828 (0)
Images	14307 (0)	Images	14509 (0)
Text	904 (0)	Text	552 (0)
Uncategorized	19371 (0)	Uncategorized	24811 (0)
Videos	1361 (0)	Videos	1384 (0)
Documents	148 (0)	Documents	95 (0)
Archives	110 (0)	Archives	58 (0)
Activity Sensor Data	51206 (0)		
Applications Usage Log	181 (0)		
Calendar	652 (0)		
Call Log	2647 (0)		
Chats	2134 (0)		
Contacts	5646 (0)		
Cookies	7036 (0)		
Credit Cards	3 (0)		
Device Connectivity	1491 (0)		
Device Events	1 (0)		
Emails	326 (0)		
Installed Applications	412 (0)		
Instant Messages	6417 (0)		
Log Entries	38974 (0)		
Notes	53 (0)		
Passwords	6915 (0)		
Recordings	7 (0)		
Searched Items	486 (0)		
Social Media	21 (0)		
Transfers	36 (0)		
User Accounts	41 (0)		
Voicemails	311 (0)		
Web Bookmarks	70 (3)		
Web History	1385 (3)		
Wireless Networks	244 (0)		

Cellebrite PA (Version 7.70.0.5)

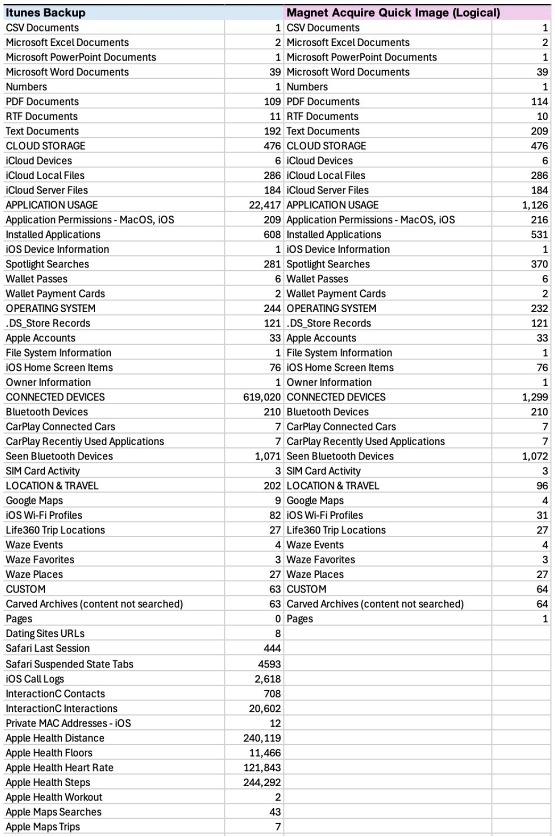
Figure 3.a



Itunes Backup		Magnet Acquire Quick Image (Logical)	
ALL EVIDENCE	899,459	ALL EVIDENCE	260,379
REFINED RESULTS	39,689	REFINED RESULTS	33,039
Classifieds URLs	1,113	Classifieds URLs	390
Cloud Services URLs	16	Cloud Services URLs	2
Facebook URLs	76	Facebook URLs	42
Google Maps Queries	38	Google Maps Queries	2
Google Searches	2,571	Google Searches	22
Identifiers - Device	1,911	Identifiers - Device	1,845
Identifiers - People	15,318	Identifiers - People	12,127
Malware/Phishing URLs	3	Malware/Phishing URLs	3
Shipping Site URLs	540	Shipping Site URLs	3
Social Media URLs	18,041	Social Media URLs	18,581
User Accounts	20	User Accounts	20
Web Chat URLs	34	Web Chat URLs	2
WEB RELATED	53,733	WEB RELATED	40,663
Chrome Current Tabs	37	Chrome Current Tabs	37
Chrome Tab History	60	Chrome Tab History	60
Chrome Top Sites	1	Chrome Top Sites	1
Google Analytics First Visit Cookies Carved	5	Google Analytics First Visit Cookies Carved	5
Potential Browser Activity	5,008	Potential Browser Activity	377
Safari Bookmarks	62	Safari Bookmarks	62
Safari History	4,576	Safari History	10
WebKit Browser Web History (Carved)	38,947	WebKit Browser Web History (Carved)	40,111
COMMUNICATION	126,169	COMMUNICATION	126,644
Apple Contacts - iOS	1,751	Apple Contacts - iOS	1,759
GroupMe Accounts	1	GroupMe Accounts	1
iOS iMessage/SMS/MMS	121,378	iOS iMessage/SMS/MMS	124,460
iOS Messages Preferences	1	iOS Messages Preferences	1
iOS Voice Mail	326	iOS Voice Mail	329
TextPlus Calls	29	TextPlus Calls	29
TextPlus Messages	65	TextPlus Messages	65
SOCIAL NETWORKING	6,678	SOCIAL NETWORKING	6,708
Instagram Profiles	612	Instagram Profiles	635
Linkedin Profile	1	Linkedin Profile	1
Pinterest Accounts	1	Pinterest Accounts	1
Reddit Accounts	1	Reddit Accounts	1
Reddit Posts	397	Reddit Posts	397
TikTok Contacts	3,738	TikTok Contacts	3,738
TikTok Messages	1,928	TikTok Messages	1,935
MEDIA	29,701	MEDIA	48,959
AMR Files	344	AMR Files	350
Audio	261	Audio	224
Carved Audio	182	Carved Audio	42
iOS Device Wallpapers	53	iOS Device Wallpapers	53
Live Photos	911	Live Photos	1,606
Photos Media Information	3,655	Photos Media Information	7,398
Photoshop Files	14	Photoshop Files	14
Pictures	22,607	Pictures	36,340
Potential Facebook Pictures	40	Potential Facebook Pictures	40
Videos	1,634	Videos	2,892
EMAIL & CALENDAR	652	EMAIL & CALENDAR	636
Calendar Events	652	Calendar Events	636
DOCUMENTS	415	DOCUMENTS	437
Apple Notes	52	Apple Notes	52
Apple Notes - Voice	7	Apple Notes - Voice	7

AXIOM Cyber (Version 8.9.0.43012)

Figure 3.b



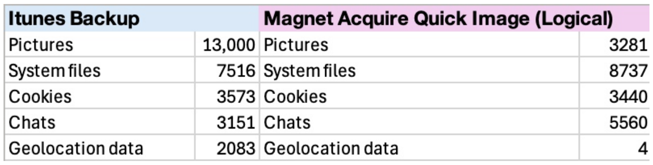
Itunes Backup		Magnet Acquire Quick Image (Logical)	
CSV Documents	1	CSV Documents	1
Microsoft Excel Documents	2	Microsoft Excel Documents	2
Microsoft PowerPoint Documents	1	Microsoft PowerPoint Documents	1
Microsoft Word Documents	39	Microsoft Word Documents	39
Numbers	1	Numbers	1
PDF Documents	109	PDF Documents	114
RTF Documents	11	RTF Documents	10
Text Documents	192	Text Documents	209
CLOUD STORAGE	476	CLOUD STORAGE	476
iCloud Devices	6	iCloud Devices	6
iCloud Local Files	286	iCloud Local Files	286
iCloud Server Files	184	iCloud Server Files	184
APPLICATION USAGE	22,417	APPLICATION USAGE	1,126
Application Permissions - MacOS, iOS	209	Application Permissions - MacOS, iOS	216
Installed Applications	608	Installed Applications	531
iOS Device Information	1	iOS Device Information	1
Spotlight Searches	281	Spotlight Searches	370
Wallet Passes	6	Wallet Passes	6
Wallet Payment Cards	2	Wallet Payment Cards	2
OPERATING SYSTEM	244	OPERATING SYSTEM	232
.DS_Store Records	121	.DS_Store Records	121
Apple Accounts	33	Apple Accounts	33
File System Information	1	File System Information	1
iOS Home Screen Items	76	iOS Home Screen Items	76
Owner Information	1	Owner Information	1
CONNECTED DEVICES	619,020	CONNECTED DEVICES	1,299
Bluetooth Devices	210	Bluetooth Devices	210
CarPlay Connected Cars	7	CarPlay Connected Cars	7
CarPlay Recentiy Used Applications	7	CarPlay Recently Used Applications	7
Seen Bluetooth Devices	1,071	Seen Bluetooth Devices	1,072
SIM Card Activity	3	SIM Card Activity	3
LOCATION & TRAVEL	202	LOCATION & TRAVEL	96
Google Maps	9	Google Maps	4
iOS Wi-Fi Profiles	82	iOS Wi-Fi Profiles	31
Life360 Trip Locations	27	Life360 Trip Locations	27
Waze Events	4	Waze Events	4
Waze Favorites	3	Waze Favorites	3
Waze Places	27	Waze Places	27
CUSTOM	63	CUSTOM	64
Carved Archives (content not searched)	63	Carved Archives (content not searched)	64
Pages	0	Pages	1
Dating Sites URLs	8		
Safari Last Session	444		
Safari Suspended State Tabs	4593		
iOS Call Logs	2,618		
InteractionC Contacts	708		
InteractionC Interactions	20,602		
Private MAC Addresses - iOS	12		
Apple Health Distance	240,119		
Apple Health Floors	11,466		
Apple Health Heart Rate	121,843		
Apple Health Steps	244,292		
Apple Health Workout	2		
Apple Maps Searches	43		
Apple Maps Trips	7		

Observations

The analysis revealed that Belkasoft X extracted more information from a Quick Image compared to an iTunes backup, highlighting its capability to recover a broader range of data from forensic images. However, when analyzing the same datasets, both Cellebrite PA and Magnet AXIOM retrieved a greater volume of data from the iTunes backup, suggesting that these tools are more effective in parsing and interpreting structured backups. This indicates that the choice of extraction and analysis method can significantly impact the amount and type of recoverable data, emphasizing the importance of selecting the most appropriate tool / using multiple tools based on investigative needs to perform a proper analysis.

Let's take a more in depth look at some of the differences in the data found regarding pictures/ images found.[9]

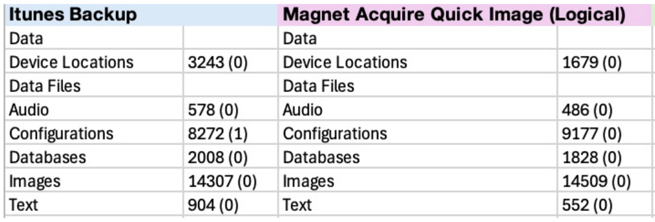
Figure 4



Itunes Backup		Magnet Acquire Quick Image (Logical)	
Pictures	13,000	Pictures	3281
System files	7516	System files	8737
Cookies	3573	Cookies	3440
Chats	3151	Chats	5560
Geolocation data	2083	Geolocation data	4

Belkasoft X

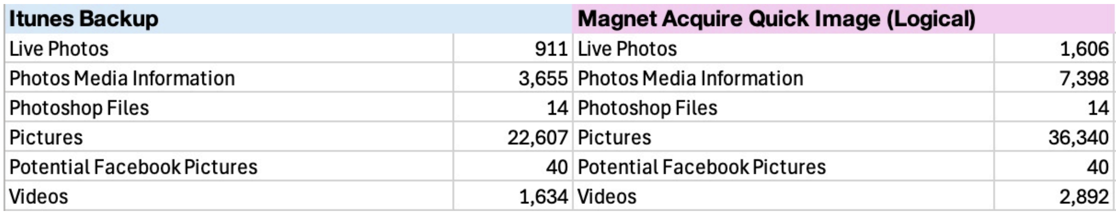
Figure 5



Itunes Backup		Magnet Acquire Quick Image (Logical)	
Data		Data	
Device Locations	3243 (0)	Device Locations	1679 (0)
Data Files		Data Files	
Audio	578 (0)	Audio	486 (0)
Configurations	8272 (1)	Configurations	9177 (0)
Databases	2008 (0)	Databases	1828 (0)
Images	14307 (0)	Images	14509 (0)
Text	904 (0)	Text	552 (0)

Cellebrite PA

Figure 6



Itunes Backup		Magnet Acquire Quick Image (Logical)	
Live Photos	911	Live Photos	1,606
Photos Media Information	3,655	Photos Media Information	7,398
Photoshop Files	14	Photoshop Files	14
Pictures	22,607	Pictures	36,340
Potential Facebook Pictures	40	Potential Facebook Pictures	40
Videos	1,634	Videos	2,892

AXIOM

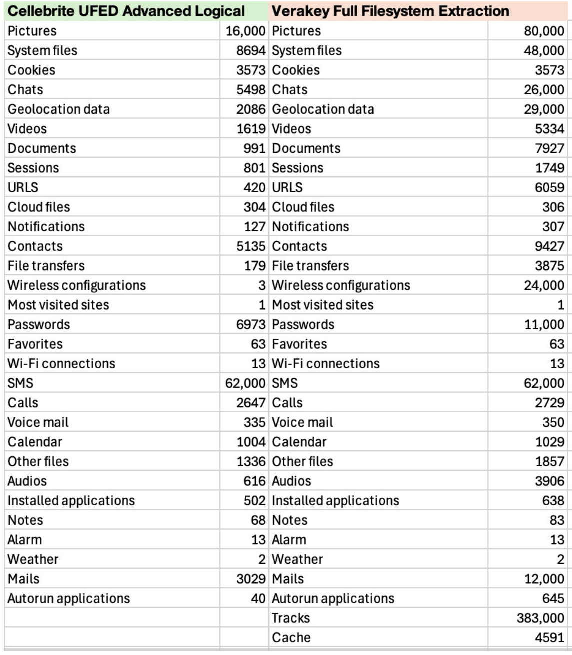
The findings suggest that while the Quick Image method may be more effective at capturing and storing images[10], as it retrieved a substantial number of pictures, the iTunes backup generally retained a greater volume of other forms of data. The iTunes backup extracted more images in some cases (Figure 4), but it also stored significantly higher amounts of additional data types, such as device locations, databases, and configuration files. This indicates that Quick Image may be preferable for investigations focused on multimedia recovery, whereas iTunes backups provide a more comprehensive dataset for broader forensic analysis. The choice of extraction method should therefore align with the specific investigative needs, balancing the depth of image recovery against the breadth of overall data retention.

[9] Note that the categorization of pictures/images is different across the three examination tools. Belkasoft X and Cellebrite PA use broader categories such as "Pictures" or "Images", while AXIOM is more specific in the type of image.

[10] See Figures 5 and 6

Next, we will conduct a detailed comparison between Cellebrite UFED Advanced Logical (version 7.71.406) and Magnet VeraKey FFS (Version 1.25.0.30192015) to examine the differences in data extraction capabilities. This analysis will focus on the volume and depth of data retrieved, including user-generated content, system artifacts, application data, and deleted files. While UFED Advanced Logical is designed to extract accessible and structured data, VeraKey's FFS method allows for deeper access, potentially uncovering hidden or deleted content that may not be retrievable through traditional logical extractions.

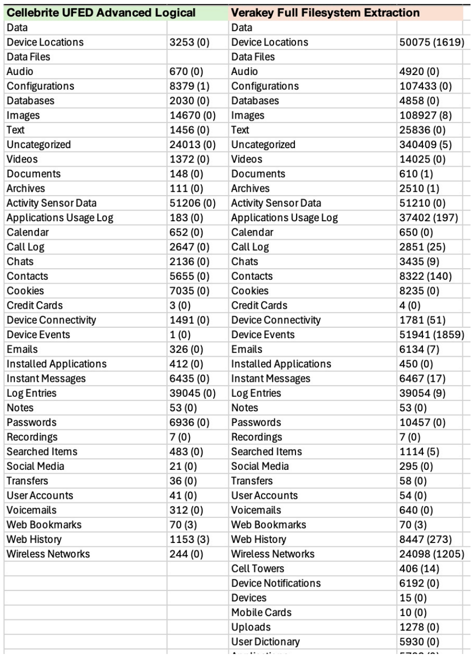
Figure 7



Cellebrite UFED Advanced Logical		Verakey Full Filesystem Extraction	
Pictures	16,000	Pictures	80,000
System files	8694	System files	48,000
Cookies	3573	Cookies	3573
Chats	5498	Chats	26,000
Geolocation data	2086	Geolocation data	29,000
Videos	1619	Videos	5334
Documents	991	Documents	7927
Sessions	801	Sessions	1749
URLS	420	URLS	6059
Cloud files	304	Cloud files	306
Notifications	127	Notifications	307
Contacts	5135	Contacts	9427
File transfers	179	File transfers	3875
Wireless configurations	3	Wireless configurations	24,000
Most visited sites	1	Most visited sites	1
Passwords	6973	Passwords	11,000
Favorites	63	Favorites	63
Wi-Fi connections	13	Wi-Fi connections	13
SMS	62,000	SMS	62,000
Calls	2647	Calls	2729
Voice mail	335	Voice mail	350
Calendar	1004	Calendar	1029
Other files	1336	Other files	1857
Audios	616	Audios	3906
Installed applications	502	Installed applications	638
Notes	68	Notes	83
Alarm	13	Alarm	13
Weather	2	Weather	2
Mails	3029	Mails	12,000
Autorun applications	40	Autorun applications	645
		Tracks	383,000
		Cache	4591

Belkasoft X

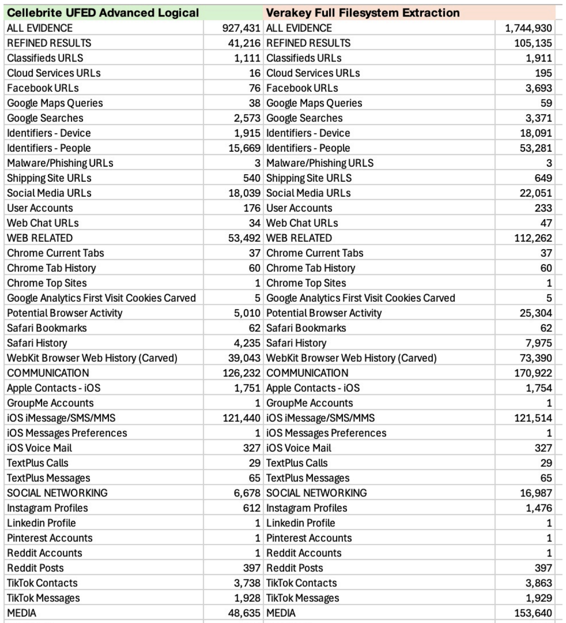
Figure 8



Cellebrite UFED Advanced Logical		Verakey Full Filesystem Extraction	
Data		Data	
Device Locations	3253 (0)	Device Locations	50075 (1619)
Data Files		Data Files	
Audio	670 (0)	Audio	4920 (0)
Configurations	8379 (1)	Configurations	107433 (0)
Databases	2030 (0)	Databases	4858 (0)
Images	14670 (0)	Images	108927 (8)
Text	1456 (0)	Text	25836 (0)
Uncategorized	24013 (0)	Uncategorized	340409 (5)
Videos	1372 (0)	Videos	14025 (0)
Documents	148 (0)	Documents	610 (1)
Archives	111 (0)	Archives	2510 (1)
Activity Sensor Data	51206 (0)	Activity Sensor Data	51210 (0)
Applications Usage Log	183 (0)	Applications Usage Log	37402 (197)
Calendar	652 (0)	Calendar	650 (0)
Call Log	2647 (0)	Call Log	2851 (25)
Chats	2136 (0)	Chats	3435 (9)
Contacts	5655 (0)	Contacts	8322 (140)
Cookies	7035 (0)	Cookies	8235 (0)
Credit Cards	3 (0)	Credit Cards	4 (0)
Device Connectivity	1491 (0)	Device Connectivity	1781 (51)
Device Events	1 (0)	Device Events	51941 (1859)
Emails	326 (0)	Emails	6134 (7)
Installed Applications	412 (0)	Installed Applications	450 (0)
Instant Messages	6435 (0)	Instant Messages	6467 (17)
Log Entries	39045 (0)	Log Entries	39054 (9)
Notes	53 (0)	Notes	53 (0)
Passwords	6936 (0)	Passwords	10457 (0)
Recordings	7 (0)	Recordings	7 (0)
Searched Items	483 (0)	Searched Items	1114 (5)
Social Media	21 (0)	Social Media	295 (0)
Transfers	36 (0)	Transfers	58 (0)
User Accounts	41 (0)	User Accounts	54 (0)
Voicemails	312 (0)	Voicemails	640 (0)
Web Bookmarks	70 (3)	Web Bookmarks	70 (3)
Web History	1153 (3)	Web History	8447 (273)
Wireless Networks	244 (0)	Wireless Networks	24098 (1205)
		Cell Towers	406 (14)
		Device Notifications	6192 (0)
		Devices	15 (0)
		Mobile Cards	10 (0)
		Uploads	1278 (0)
		User Dictionary	5930 (0)

Cellebrite PA

Figure 9



Cellebrite UFED Advanced Logical		Verakey Full Filesystem Extraction	
ALL EVIDENCE	927,431	ALL EVIDENCE	1,744,930
REFINED RESULTS	41,216	REFINED RESULTS	105,135
Classifieds URLS	1,111	Classifieds URLs	1,911
Cloud Services URLs	16	Cloud Services URLs	195
Facebook URLs	76	Facebook URLs	3,693
Google Maps Queries	38	Google Maps Queries	59
Google Searches	2,573	Google Searches	3,371
Identifiers - Device	1,915	Identifiers - Device	18,091
Identifiers - People	15,669	Identifiers - People	53,281
Malware/Phishing URLs	3	Malware/Phishing URLS	3
Shipping Site URLs	540	Shipping Site URLS	649
Social Media URLs	18,039	Social Media URLs	22,051
User Accounts	176	User Accounts	233
Web Chat URLs	34	Web Chat URLs	47
WEB RELATED	53,492	WEB RELATED	112,262
Chrome Current Tabs	37	Chrome Current Tabs	37
Chrome Tab History	60	Chrome Tab History	60
Chrome Top Sites	1	Chrome Top Sites	1
Google Analytics First Visit Cookies Carved	5	Google Analytics First Visit Cookies Carved	5
Potential Browser Activity	5,010	Potential Browser Activity	25,304
Safari Bookmarks	62	Safari Bookmarks	62
Safari History	4,235	Safari History	7,975
WebKit Browser Web History (Carved)	39,043	WebKit Browser Web History (Carved)	73,390
COMMUNICATION	126,232	COMMUNICATION	170,922
Apple Contacts - iOS	1,751	Apple Contacts - iOS	1,754
GroupMe Accounts	1	GroupMe Accounts	1
iOS iMessage/SMS/MMS	121,440	iOS iMessage/SMS/MMS	121,514
iOS Messages Preferences	1	iOS Messages Preferences	1
iOS Voice Mail	327	iOS Voice Mail	327
TextPlus Calls	29	TextPlus Calls	29
TextPlus Messages	65	TextPlus Messages	65
SOCIAL NETWORKING	6,678	SOCIAL NETWORKING	16,987
Instagram Profiles	612	Instagram Profiles	1,476
Linkedin Profile	1	Linkedin Profile	1
Pinterest Accounts	1	Pinterest Accounts	1
Reddit Accounts	1	Reddit Accounts	1
Reddit Posts	397	Reddit Posts	397
TikTok Contacts	3,738	TikTok Contacts	3,863
TikTok Messages	1,928	TikTok Messages	1,929
MEDIA	48,635	MEDIA	153,640

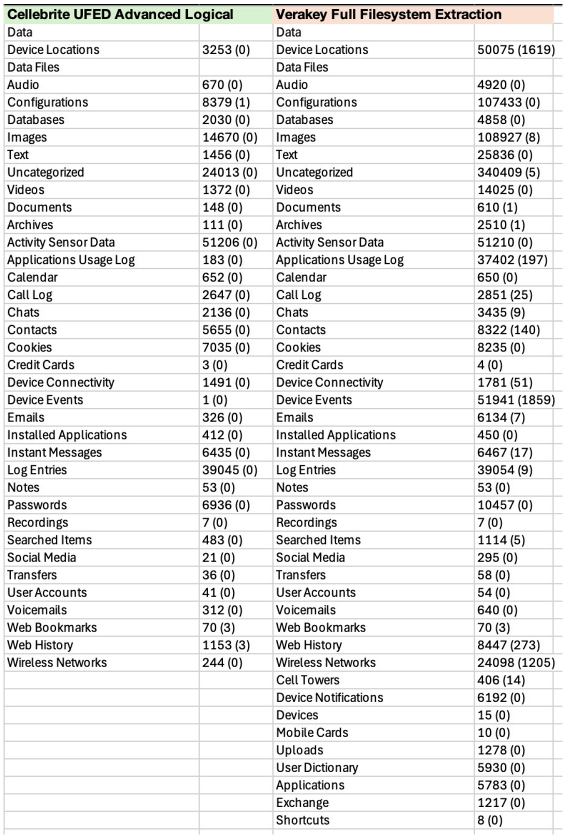
AXIOM

Observations

The analysis demonstrates that a FFS extraction consistently retrieves more data than a UFED advanced logical extraction[11]. This is primarily due to the fundamental differences in how these methods access and extract data. A FFS extraction, such as VeraKey, provides low-level access to the device's storage, allowing for the recovery of a complete file structure, including deleted and hidden files, system artifacts, application data, and encrypted content. In contrast, UFED's advanced logical extraction relies on APIs and structured data access, which limits its ability to capture certain file system components and volatile data.

Let's take a look at deleted files and data.

Figure 10



Cellebrite UFED Advanced Logical		Verakey Full Filesystem Extraction	
Data		Data	
Device Locations	3253 (0)	Device Locations	50075 (1619)
Data Files		Data Files	
Audio	670 (0)	Audio	4920 (0)
Configurations	8379 (1)	Configurations	107433 (0)
Databases	2030 (0)	Databases	4858 (0)
Images	14670 (0)	Images	108927 (8)
Text	1456 (0)	Text	25836 (0)
Uncategorized	24013 (0)	Uncategorized	340409 (5)
Videos	1372 (0)	Videos	14025 (0)
Documents	148 (0)	Documents	610 (1)
Archives	111 (0)	Archives	2510 (1)
Activity Sensor Data	51206 (0)	Activity Sensor Data	51210 (0)
Applications Usage Log	183 (0)	Applications Usage Log	37402 (197)
Calendar	652 (0)	Calendar	650 (0)
Call Log	2647 (0)	Call Log	2851 (25)
Chats	2136 (0)	Chats	3435 (9)
Contacts	5655 (0)	Contacts	8322 (140)
Cookies	7035 (0)	Cookies	8235 (0)
Credit Cards	3 (0)	Credit Cards	4 (0)
Device Connectivity	1491 (0)	Device Connectivity	1781 (51)
Device Events	1 (0)	Device Events	51941 (1859)
Emails	326 (0)	Emails	6134 (7)
Installed Applications	412 (0)	Installed Applications	450 (0)
Instant Messages	6435 (0)	Instant Messages	6467 (17)
Log Entries	39045 (0)	Log Entries	39054 (9)
Notes	53 (0)	Notes	53 (0)
Passwords	6936 (0)	Passwords	10457 (0)
Recordings	7 (0)	Recordings	7 (0)
Searched Items	483 (0)	Searched Items	1114 (5)
Social Media	21 (0)	Social Media	295 (0)
Transfers	36 (0)	Transfers	58 (0)
User Accounts	41 (0)	User Accounts	54 (0)
Voicemails	312 (0)	Voicemails	640 (0)
Web Bookmarks	70 (3)	Web Bookmarks	70 (3)
Web History	1153 (3)	Web History	8447 (273)
Wireless Networks	244 (0)	Wireless Networks	24098 (1205)
		Cell Towers	406 (14)
		Device Notifications	6192 (0)
		Devices	15 (0)
		Mobile Cards	10 (0)
		Uploads	1278 (0)
		User Dictionary	5930 (0)
		Applications	5783 (0)
		Exchange	1217 (0)
		Shortcuts	8 (0)

Cellebrite PA

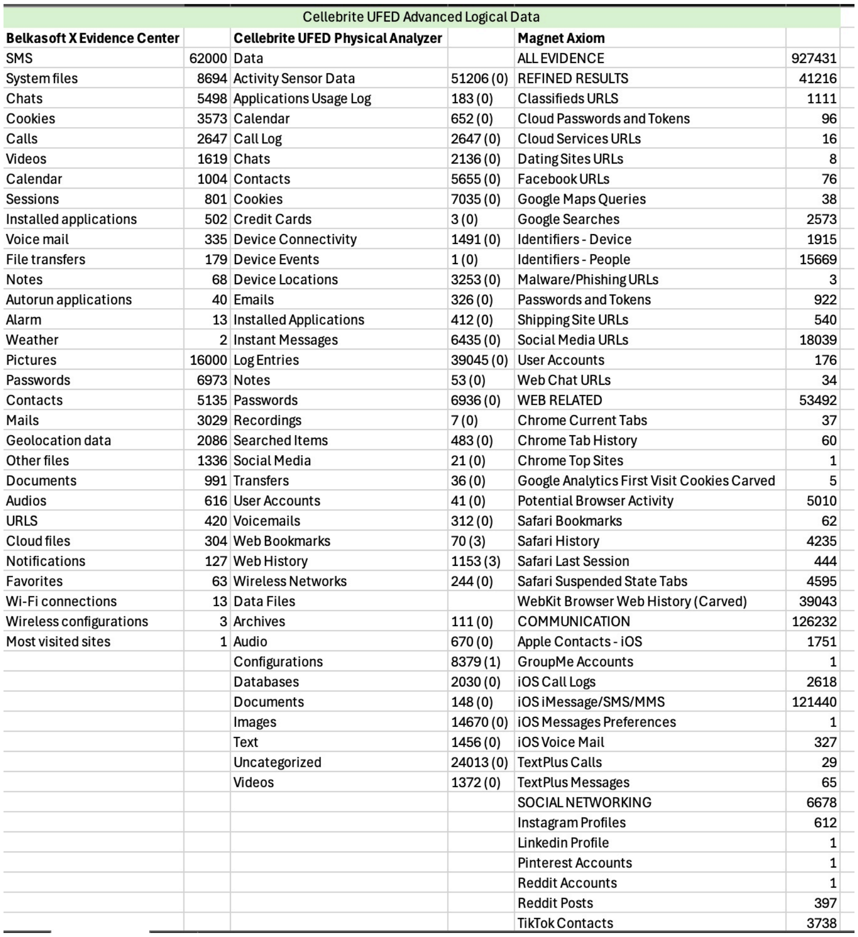
Figure 10 shows that while the UFED advanced logical extraction recovered some deleted files, the FFS extraction retrieved significantly more. This difference highlights the varying capabilities of each method, with UFED capturing a limited subset of deleted data while VeraKey provides a more extensive recovery. In cases where access to deleted messages, images,

[11] Reference Figure 9, FFS resulted in 1,744,930 artifacts while the Advanced Logical resulted in 927,431 artifacts

or documents is critical, such as criminal investigations or civil disputes, the broader data retrieval offered by a FFS can be a decisive advantage.

Now, we will take a broader look at how the various examination tools performed in extracting and analyzing data. Each tool demonstrated unique strengths and limitations, with some excelling in specific data types while others provided more comprehensive overall extraction.[12]

Figure 11



		Cellebrite UFED Advanced Logical Data			
Belkasoft X Evidence Center		**Cellebrite UFED Physical Analyzer**		**Magnet Axiom**	
SMS	62000	Data		ALL EVIDENCE	927431
System files	8694	Activity Sensor Data	51206 (0)	REFINED RESULTS	41216
Chats	5498	Applications Usage Log	183 (0)	Classifieds URLS	1111
Cookies	3573	Calendar	652 (0)	Cloud Passwords and Tokens	96
Calls	2647	Call Log	2647 (0)	Cloud Services URLs	16
Videos	1619	Chats	2136 (0)	Dating Sites URLs	8
Calendar	1004	Contacts	5655 (0)	Facebook URLs	76
Sessions	801	Cookies	7035 (0)	Google Maps Queries	38
Installed applications	502	Credit Cards	3 (0)	Google Searches	2573
Voice mail	335	Device Connectivity	1491 (0)	Identifiers - Device	1915
File transfers	179	Device Events	1 (0)	Identifiers - People	15669
Notes	68	Device Locations	3253 (0)	Malware/Phishing URLs	3
Autorun applications	40	Emails	326 (0)	Passwords and Tokens	922
Alarm	13	Installed Applications	412 (0)	Shipping Site URLs	540
Weather	2	Instant Messages	6435 (0)	Social Media URLs	18039
Pictures	16000	Log Entries	39045 (0)	User Accounts	176
Passwords	6973	Notes	53 (0)	Web Chat URLs	34
Contacts	5135	Passwords	6936 (0)	WEB RELATED	53492
Mails	3029	Recordings	7 (0)	Chrome Current Tabs	37
Geolocation data	2086	Searched Items	483 (0)	Chrome Tab History	60
Other files	1336	Social Media	21 (0)	Chrome Top Sites	1
Documents	991	Transfers	36 (0)	Google Analytics First Visit Cookies Carved	5
Audios	616	User Accounts	41 (0)	Potential Browser Activity	5010
URLS	420	Voicemails	312 (0)	Safari Bookmarks	62
Cloud files	304	Web Bookmarks	70 (3)	Safari History	4235
Notifications	127	Web History	1153 (3)	Safari Last Session	444
Favorites	63	Wireless Networks	244 (0)	Safari Suspended State Tabs	4595
Wi-Fi connections	13	Data Files		WebKit Browser Web History (Carved)	39043
Wireless configurations	3	Archives	111 (0)	COMMUNICATION	126232
Most visited sites	1	Audio	670 (0)	Apple Contacts - iOS	1751
		Configurations	8379 (1)	GroupMe Accounts	1
		Databases	2030 (0)	iOS Call Logs	2618
		Documents	148 (0)	iOS iMessage/SMS/MMS	121440
		Images	14670 (0)	iOS Messages Preferences	1
		Text	1456 (0)	iOS Voice Mail	327
		Uncategorized	24013 (0)	TextPlus Calls	29
		Videos	1372 (0)	TextPlus Messages	65
				SOCIAL NETWORKING	6678
				Instagram Profiles	612
				Linkedin Profile	1
				Pinterest Accounts	1
				Reddit Accounts	1
				Reddit Posts	397
				TikTok Contacts	3738

Consolidated data of the Cellebrite UFED Advanced Logical extraction ran through the three test examination methods.

[12] Please note that the three analysis tools use varying levels of specificity in its categorization, Axiom being more specific, while Belkasoft X and Cellebrite PA use broader terms. This is an important detail to remember as it may be vital to certain investigative needs. Further showing the importance of using multiple tools

Observations

Figure 11 shows that Belkasoft X was particularly effective at parsing data from a Quick Image, while Cellebrite PA and AXIOM extracted more information from an iTunes backup. Similarly, FFS consistently outperformed UFED advanced logical in recovering deleted files, showcasing its superiority in forensic investigations requiring deep data recovery. By comparing these tools across different extraction methods, we can better understand their effectiveness and determine the most suitable option for various forensic scenarios.

Conclusion

The testing of various extraction methods using three different forensic examination tools; Belkasoft X, Cellebrite PA, and Magnet AXIOM, revealed distinct strengths and limitations in data recovery. Quick Image proved effective in capturing a large volume of images, but iTunes backups generally retained a greater variety of data, making them more suitable for comprehensive forensic analysis. While Cellebrite UFED advanced logical extraction successfully recovered some deleted files, the VeraKey FFS extraction consistently retrieved significantly more, demonstrating its advantage in deep data recovery. Additionally, Belkasoft X was more effective in parsing data from Quick Images, whereas Cellebrite PA and Magnet AXIOM performed better with iTunes backups. These findings highlight the importance of selecting the appropriate extraction and examination tool based on the investigative needs, as different methods yield varying results depending on the type of data sought. A tailored approach, considering both the strengths and limitations of each tool, is essential for maximizing forensic data recovery in legal and investigative contexts.This research has been reviewed and improved with feedback from George Rodriguez, whose insights have strengthened the accuracy and depth of this analysis.