Beratung

Top 10 mobile device acquisition challenges

25. Oktober 2023, von Gareth Wilson

Introduction

There was a brief period of time where I thought that the forensic acquisition puzzle had well-defined solutions. For any acquisition project, I knew what devices and data sources I could come across at client sites, and I was well armed with the knowledge and tools to forensically acquire data from any common combination of systems and software.

This all started to change with the standardization and inclusion of encryption technologies in consumer-grade software and hardware, but the real acceleration was kicked off by the widespread adoption of mobile devices in the workplace. These became pocketable problems that added mobile forensics as a new piece of the forensic acquisition puzzle.

If you are new to managing projects involving mobile forensics, or if you are in a senior position such as being a CISO or compliance officer and your technical knowledge is a little out of date, what do you need to keep in mind and prepare for when planning a forensic acquisition project? If technical people dealing with the challenges of mobile forensics on a

daily basis are already working hard to keep up to date, how can you improve your awareness of the challenges in order to effectively lead your project?

In this blog post I would like to share what I believe are the key challenges to be aware of in order to effectively plan and execute an acquisition project involving mobile forensics. As I take you through my list of challenges, think about whether you have already thoroughly considered them, or if these are new challenges that you might need to start accounting for on your projects.

Top 10 Challenges

1 - Bring Your Own Device "BYOD"

Allowing users to use their own devices for work purposes creates a number of challenges for the data collection process. Without a consistent set of device models and operating systems, and with varying versions and configurations of hardware, operating systems, and applications, each device becomes an independent collection project with unique challenges and considerations. Compare this to dedicated work devices, where a consistency across all of these variables means that the collection process can be planned once and repeated for every device to be collected.

Typically, user devices are also not included (or only partially included) in Mobile Device Management (MDM) policies. This results in a lack of control about where data is stored, how it is modified and shared, and features such as remote wiping or automatically deleted messages become additional considerations during acquisitions.

In summary, there is some truth to the well-known alternative of "Bring Your Own Disaster" for the "BYOD" acronym.

2 - Change is Rapid and Relentless

Is the latest iPhone the 15 or the 16, and what are its features? What is the latest version of Android? What information does an Apple Watch store? When a device is powered off, can it still be tracked via Find My Phone? What is wearable computing and what data can it store?

The answers to these questions will be different today than they will be in 6-12 months' time, and keeping on top of all of the changes and related implications on data collection and security is a challenge that has more chances of increasing in complexity and pace of change

than becoming simpler to manage in the near future.

3 - Segregation of Personal and Professional Information

In my experience, work mobile devices are rarely used solely for work purposes if the devices leave the office with the custodian. At some point a work device is likely to be used to take a personal photo or note, to Google-search a medical concern, or add a personal contact or address to the associated apps, resulting in the blending of personal and professional information on a work mobile device.

This creates both a challenge in separating personal and professional information, and resistance to data acquisitions from the custodian of the mobile device. It's natural that someone wouldn't want an investigator to go through their personal family photos when investigating a work-related matter, but it's a common issue with digital investigations.

4 - How Long Can You Be Without Your Mobile Phone?

With the huge volumes of data stored on mobile devices combined with the slow collection process, it can take many hours to collect data during an investigation. How long can the custodian be without their device and what is the impact on their work during that time? Could the device be kept over night or for a number of days?

As mobile devices have become so integral to daily work functions, it is increasingly difficult to ask custodians to be without their devices for an extended period of time. This puts pressure on the acquisition team to perform their job quickly, and adds additional stress to custodians already concerned about the investigation being performed.

5 - Internet Connectivity

Mobile devices and applications are designed to be integrated with the internet. This means that special considerations need to be made when performing acquisitions to collect data without compromising the investigation. Remote-wiping functionality, application updates, or the reception of new data can impact the repeatability of the acquisition and the integrity of the data, and requires thorough consideration.

6 - Recent Lists

How far back can you scroll in your messaging app before you reach the message that tells you to load the rest of the data from the server? This is also likely to be the limit for data stored locally on the device, and therefore accessible to investigators without pulling data from the messaging servers. Reception of new messages could push older messages out of this list and impact the collection process.

This finite number of entries issue can appear anywhere where there is a “recent” list, such as in search history, locations, recent emails, call logs, etc.

7 - Ephemeral Data

Some data on mobile devices can be lost with time, creating time pressure to acquire mobile devices before the data is lost forever.

This data can include logs (such as call logs) being limited to a set number of days, information flagged for deletion being permanently deleted after a set time period (either via the application functionality, or OS/hardware level garbage collection processes), and modern messaging apps have a temporary message feature that automatically deletes messages after a pre-defined time period.

8 - Cloud Data

As more functionality moves to cloud services and Software as a Service (SaaS), it is important to know what information is accessed via the mobile device but not stored locally, and how to acquire that data.

Acquiring cloud data could require having access to additional credentials and specialist tools, and could include requiring the custodian to approve the action via an email link which removes the possibility of a covert acquisition.

A final point of consideration for cloud data concerns the host country of the data. Does the location of the data create any legal, contractual, or other issue regarding the collection, ownership, or handling of the data?

9 - Passwords and Acquisition Limits

On modern mobile devices data acquisition is extremely limited without having access credentials to the device. Without these credentials the device must be stored until a vulnerability is found that can bypass the device’s security. This could take years to be

identified, made public, and implemented within specialist mobile acquisition tools.

Even with full access to the mobile device, hardware vendors such as Apple limit what can be extracted with non-invasive acquisition techniques, and typically the image of the mobile device needs to be combined with secondary data collections such as cloud and email server acquisitions to get the full data set.

10 - Secure Applications

With data privacy and security being a current hot topic, developers are taking matters into their own hands and adding extra levels of security to their applications beyond those implemented by the hardware and the Operating System (OS). This can include requiring additional credentials to log into the app when the device is rebooted, limiting data exfiltration options or warning the user of data exfiltration, encrypting the internal application databases, or excluding the application data from being included in the device backups that are used for typical data acquisition methods.

Conclusion

Was this list an affirmation of your mobile forensics knowledge, or do you now have a few new topics to consider the next time you need to lead a forensic acquisition project? As the mobile forensics landscape is constantly changing at such a rapid pace, the only consistent point that I can see is that the challenges are always changing and we always have to make an effort to keep our knowledge up to date.

If any of these challenges resonated with you, or if have any questions or comments about mobile forensics, join our discussion on [LinkedIn] or reach out to us via our contact page on our website to continue the conversation.

Gareth Wilson

Gareth Wilson has a passion for working in domains where technology and people intersect, resulting in him specializing in eDiscovery, Mobile Forensics, and Information Security at Swiss FTS.