Android Analysis

Rogelio Perez-Montero

CTIS 371 Computer Forensics

Isaac Magaña

4/7/2023

Abstract

Mobile devices have increasingly become more critical to our personal lives. In recent years, it has been claimed by the Supreme Court that they contain more private data than our personal homes. Smartphones are always collecting data and are now crucial to forensic investigations. They contain information such as GPS location, phone calls, messages, and all actions performed. The objectives of the project were to extract all data from an unrooted phone, but also recover any deleted files that were purposely removed. To analyze the LG Android smartphone, software Andriller, Photorec, and Scalpel were used. The program Andriller is used to extract all the data from the phone and display it as an HTML file. To recover deleted files programs Photrec and Scalpel were used. Although limited by the root status of the smartphone, deleted files were recovered and a complete analysis of the phone was made.

Introduction to problem

Extracting deleted files was one of the main objectives of this project. People can purposely delete incriminating information and we cannot recover them from inside the phone. In order to recover deleted files, a complete physical analysis of the phone needs to be done. However, there can still be some files recovered with a logical image. The original goal was completing a physical image, but this can only be done with a rooted phone or Superuser rights. A physical image of the phone would’ve contained messages, calls, location, accounts, all files, and app data. Logical images are limited to the data the phone believes it has. Deleted files are crucial to a mobile investigation because anything incriminating will be deleted or people can try to delete information through cloud functions.

Solution

To analyze and recover deleted data, certain tools and software can be used. In police investigations, they have access to tools such as Cellebrite UFED that can easily bypass screen locks and get root privileges. The primary step is to have access to the phone or have software that can enable debugging. Depending on the type of image desired, it is important to know the root status of a device. An unrooted phone can still be analyzed but it will not show the extended amount of data as a rooted phone. Physical and digital tools can be used to obtain the image of a phone and recover lost data. For the purpose of this investigation, Andriller was used to create a logical image of the phone. Digital software Photorec and Scalpel were the solution to recovering deleted files from the phone image.

Implementation

The most important step to recover deleted data is to extract all digital information from the phone by imaging it. Andriller is a dedicated software that can extract all data by simply connecting the device to the pc. For Andriller to function properly, Python3 needs to be installed and a stable connection needs to be established but root privileges are not necessary. From the device, debugging and developer options need to be enabled. Another requirement is that the user needs access to the device or uses other software to crack the password. Without access to the phone, a logical extraction cannot be made, but it can differ from a physical image. Using Andriller, the phone's storage was extracted and it created a webpage report of all its findings(figure 1). For the image copy, it was also important Andriller is a Read-Only tool that wouldn't affect the components or hash of the phone.

To recover deleted files from the image, Photorec was first used. Photorec is a data recovery software that ignores the file system and goes for underlying data. Being able to ignore

the system made the extraction simpler. For most software, a system has to be determined and special options have to be selected. Photorec was able to recover 11 deleted files (Figure 2). However, most were .txt files which weren't helpful to the investigation. Only one JPG file was recovered and it was able to function properly. To ensure the file wasn't in the extracted files from Andriller, a comparison of images was made.

To completely achieve the objective of recovering deleted files. Scalpel was used as a tool for file recovery. Different from Photorec, it uses the file system to recover each file. It has to recognize the file system or use raw device files. As a result, multiple files were recovered, but there were mostly corrupted (figure 3). It would appear that Photorec was able to recover working files but corrupted files from Scalpel would've still been helpful.

Obstacles

Challenges facing the Android root status and Andriller were the main issues. To securely investigate the mobile device, the goal was to use all tools on the virtual machine Kali Linux. Unfortunately executing files and downloading software such as Python3 and Andriller was a challenge in itself. After failing many times, there was a way to install the needed components on a normal Windows OS. After successfully getting Andriller to function, the Android smartphone needed to be rooted. Further investigation revealed that the device could not be rooted because its Bootloader needed to be unlocked by the manufacturer LG. Unfortunately, LG, terminated their mobile services to unlock phones in 2021, making the phone unrootable. Without root status, viewing deleted information and important data such as calls and messages wasn't possible. Therefore, other software had to be used instead of doing a simple analysis on a rooted phone.

Conclusion

Mobile devices, particularly smartphones, have become an integral part of our lives and contain a vast amount of private data. This data is not only valuable for personal use but also crucial for forensic investigations. The project aimed to extract all data from an unrooted LG Android smartphone and recover any deleted files that were intentionally removed. In the process, I learned to use software for the analysis including Andriller, Photorec, and Scalpel. Although the smartphone was limited by its root status, the analysis successfully extracted all data and recovered the deleted files. This project highlights the importance of mobile device data in forensic investigations and the significance of utilizing appropriate software tools to extract and analyze it.

Total: 292

Index	Directory	Filename	Size	Modified
1	shared/0/.backups/com.activision.callofduty.shooter/helpshift/databases	__hs__backup_dao_storage	276	2019-10-02 02:24:17 UTC
2	shared/0	.profig.os	36	2020-05-14 06:09:14 UTC
3	shared/0/mtklog/gpsdbglog	file_tree.txt	30	2019-07-21 15:09:11 UTC
4	shared/0/AudioRecorder/my_sounds	20191028_162023_Normal.m4a	410.7KB	2019-10-28 20:20:28 UTC
5	shared/0/AudioRecorder/my_sounds	20190811_174943_Normal.m4a	617.0KB	2019-08-11 21:50:06 UTC
6	shared/0/AudioRecorder/my_sounds	20200528_014654_Normal.m4a	561.6KB	2020-05-28 05:48:58 UTC
7	shared/0/AudioRecorder/my_sounds	20190811_220415_Normal.m4a	536.5KB	2019-08-12 02:04:30 UTC
8	shared/0/DCIM/.thumbnails	1514766047978.jpg	23.3KB	2018-01-01 00:20:48 UTC
9	shared/0/DCIM/.thumbnails	1595879632063.jpg	36.6KB	2018-01-01 00:21:16 UTC
10	shared/0/DCIM/.thumbnails	1597575343214.jpg	17.8KB	2020-08-16 10:55:43 UTC
11	shared/0/DCIM/.thumbnails	1585086830019.jpg	22.7KB	2018-01-01 00:21:09 UTC
12	shared/0/DCIM/.thumbnails	1514766050075.jpg	15.8KB	2018-01-01 00:20:50 UTC
13	shared/0/DCIM/.thumbnails	1597575342749.jpg	5.4KB	2020-08-16 10:55:42 UTC
14	shared/0/DCIM/.thumbnails	1577852497054.jpg	7.1KB	2018-01-01 00:21:04 UTC
15	shared/0/DCIM/.thumbnails	1514766039173.jpg	9.6KB	2018-01-01 00:20:39 UTC
16	shared/0/DCIM/.thumbnails	1576200529622.jpg	44.4KB	2018-01-01 00:21:15 UTC
17	shared/0/DCIM/.thumbnails	1597710933138.jpg	10.5KB	2020-08-18 00:35:33 UTC
18	shared/0/DCIM/.thumbnails	1595519426765.jpg	30.2KB	2018-01-01 00:25:06 UTC
19	shared/0/DCIM/.thumbnails	1578889014601.jpg	20.0KB	2018-01-01 00:21:09 UTC
20	shared/0/DCIM/.thumbnails	1588684543714.jpg	10.6KB	2018-01-01 00:21:19 UTC
21	shared/0/DCIM/.thumbnails	1596786935649.jpg	9.0KB	2018-01-01 00:20:54 UTC
22	shared/0/DCIM/.thumbnails	1514766038241.jpg	10.5KB	2018-01-01 00:20:38 UTC
23	shared/0/DCIM/.thumbnails	1596387474619.jpg	5.1KB	2018-01-01 00:20:56 UTC
24	shared/0/DCIM/.thumbnails	1514766051481.jpg	19.6KB	2018-01-01 00:20:51 UTC

Figure 1: Andriler extractions

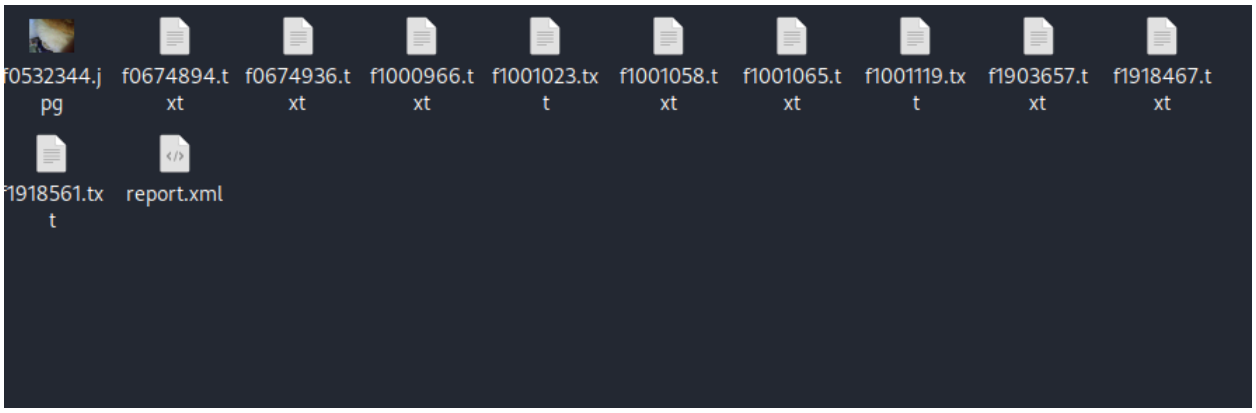

Figure 2: Photorec extractions

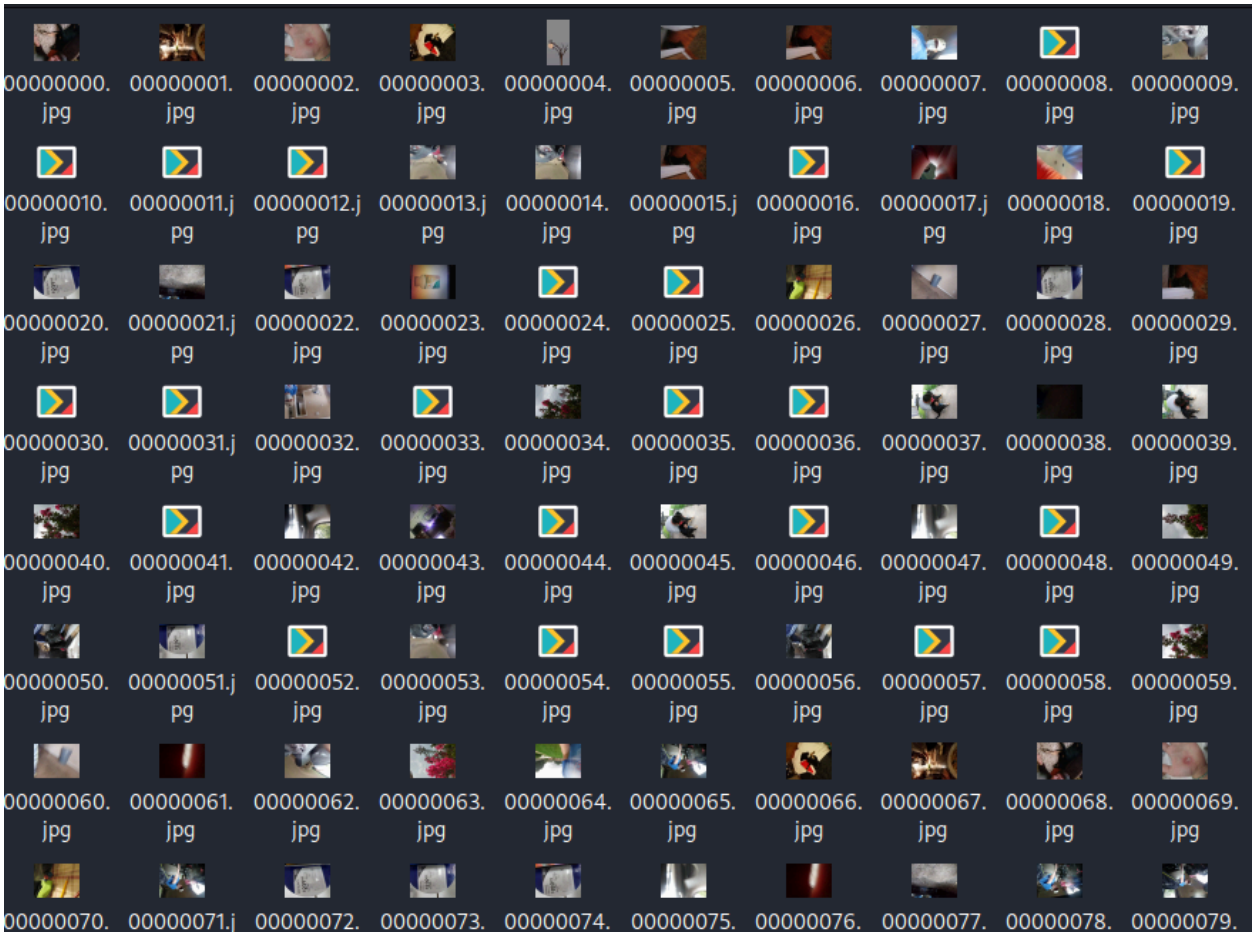

Figure 3: Scalpel Extraction

References

New York Appellate Attorney, The Law Office of Stephen N. Preziosi Law Firm New York USA. (n.d.). Retrieved April 7, 2023, from https://www.newyorkappellatelawyer.com/blog/how-private-is-your-cell-phone-u-s-supreme-court-says-its-more-private-than-your-house/

Snyder, J. (2022, July 28). What are the security risks of rooting your smartphone? Samsung Business Insights. Retrieved April 7, 2023, from https://insights.samsung.com/2022/07/28/what-are-the-security-risks-of-rooting-your-smartphone-4/#:~:text=In%20the%20Android%20ecosystem%2C%20since,custom%20image%20to%20the%20device.