Introduction to Iphone Forensics

Saaduddin Ahmed

Cyber Forensics: ITMS-538-02

Abstract

Forensic investigators should use the resources around to thoroughly investigate the device they are handed. However, for this report the major topics covered will be: iPhone's Configuration files, Pre Installed/Third Party Applications. The focus on configuration files is because they provide a way for checking on deleted notifications, pairing certificates, password, and even the system logs. Preinstalled and third party applications also help provide greater detail to investigators, such as text messages and numbers on WhatsApp, Social Media data such as last login and website visits, cache of downloads in cloud storage applications, and much more. The abundance of information found in these locations can help the investigator comb through the device and figure out what to put into the report.

Introduction

The reveal of the iPhone in 2007 brought about a change to the mobile industry as we went from flip phones to touch screens. Along with it becoming user friendly, the iPhone introduced the basic springboard app design through its iPhone OS, which to this day is widely used throughout the mobile industry. The introduction of the app store and popularity of the iPhone is what makes it important for forensic investigators to be knowledgeable with this device. While there are many places that are important to a forensic investigator, only Configuration files, Preinstalled Apps, and Third party Applications will be covered. In addition, the general information about the iPhone, IOS, and its history will be covered.

IOS and iPhone Information

The iPhone operating system, which was renamed from iPhone OS to IOS starting from IOS 4, is the main Operating system running on iPhone. It was released alongside the iPhone in 2007 as OS X, as it shared a similar unix core to a computer. This was later renamed to iPhone OS when released to the public. On initial release you could only use the preinstalled apps, but with the release of iPhone OS 2, in 2008, you were able to use Apple's app store for third party apps. With IOS 4's announcement Apple took another leap in making video phone calls a reality, and the trend continued, as IOS 5 introduced Notification center, iMessage, Siri and so forth, until we have arrived at our current IOS 16. Throughout this time Apple has tried to stay atop security practices with its Operating system as well, pushing security updates out to devices that are six to seven years old. This has helped keep people within the Apple ecosystem. Thanks to such practices, the iPhone in the US shares a 57.06% market share in the mobile vendor as of

February 2023 (StatCounter GlobalStats). The popularity of the iPhone should give forensic investigators a reason to be versed in how to tackle the investigation of such devices.

iPhone Configuration files

The iPhone configuration files is one of the first places an investigator should look, as it can help get general info about the iPhone as well the settings and configurations. The types of files you will find within the configuration are Plist and SQLite databases. The Plist stores commonly used data, such as preferences and settings, whereas the SQLite databases store the data of application, both third party and native. While the information extracted will vary on a case by case basis, some of the crucial areas to look at are the account and device information, as that will give you information about the device along with the account holder. The Installed application list is also important, as it contains every application that is installed along with its path, so marking a globally unique identifier for each application will be simpler. To know which computers the iPhone has paired with, we can look in the lockdown certificate information, which contains the pairing records. We can also do something similar with the network information and wifi networks, as the cache for the ip, router, network address, and server used along with timestamps is stored within the network information and wifi configuration file. Last but not least, sim card information such as the ICCID and IMSI of the sim can also be found in these files as well as system logs. Depending on the version of IOS you are using, you can also find stored passwords and login information within the keychain configuration files, allowing for a forensic investigator to know when the login was saved, last used, and on what website. While the Configuration file also holds a lot more information such as cleared notifications, last searched apps on the App Store, springboard information, these can all be useful to the

investigator to understand what was going on through the iPhone and how it was used. It can also help timestamp as well as check what other devices might have been used and shared with.

Preinstalled/Third Party Applications

Investigators should be familiar with various popular applications that users download. Whether the applications are pre-installed or downloaded after purchase, forensic investigators should be aware of popular applications and how they are used. Since the focus of our research has been on iPhone forensics, let us discuss various popular applications that are installed on iPhones. First, we will begin this discussion by defining the difference between pre-installed software versus third party software and how this difference relates to applications. Second, we will provide a few examples of pre-installed and third party applications. Lastly, we will discuss how to find artifacts for the applications discussed.

Pre-installed software is defined as any software that is installed into a PC prior to being purchased, and before the PC reaches the customer's hands (Law Insider n.d.). Compared to third-party software, which is software that was created by an entity that is not a part of the product's manufacturer or not the product's creator (Cambridge Dictionary n.d.). Due to the fact an application is a type of software, we can apply these definitions of software to applications as well. Since we live in an age where phones have been transfigured into mobile computers, it can be assumed the term, pre-installed software, applies to phones as well. With this difference being established, let us discuss various examples of iPhone applications that are considered either pre-installed or third party.

Two examples of pre-installed iPhone applications are Calendar and Safari. Calendar is a pre-installed application that allows the user to log various events on a digital calendar. On top of

that, Calendar provides the user with the ability to connect their calendar to other applications (Shaikh 2021). This way, the user is able to keep track of their events even when they are not within the Calendar application. Safari is the default internet browser that is pre-installed on every iPhone device (Shaikh 2021). For a forensic investigator, this can be a good place to look, as safari not only holds onto the history of what you have browsed but also saves the passwords and usernames used to login as well, only locked behind the iPhone's password. This can allow a forensics investigator to broaden their scope to see what other applications and resources might have been used. Alongside that, the forensic investigator can use the calendar app to see what other accounts might be connected to the device, with dates that might be important to the investigation. Besides these two pre-installed applications, iPhones contain many more pre-installed applications. For forensic investigators who look to specialize in iPhones, it is recommended to continue researching and understanding all other pre-installed applications that come with the iPhone. The amount of third party applications are increasing daily, but as of 2023 when it was last reported by Apple, there are already 1.76 million Iphone apps on the app store, so getting a better understanding of them is crucial (Curry 2023). Whatsapp and Pokemon GO are great examples of popular third-party applications. WhatsApp is a messaging application that can be installed from the Apple's Application store. Within WhatsApp, you can create private messages and group messages (Shaikh 2021). For forensic investigators this is important because whatsapp messages are stored on both the phone and iCloud, Apple's Cloud Service.These messages can be critical to figuring out leads as it can help understand what a person might be doing at a certain time. In my personal experience, WhatsApp is popular because it is free to use and it simulates typical instant messaging services that phones provide. Unlike the built in Apple Imessage, which is only free to use between iphones, WhatsApp allows you to message people

as if you have a phone, without having to pay for messaging rates. Pokemon GO is a free third party application that uses augmented reality and location tracking as a way to let you enjoy the game of catching pokemon (Lopez, 2016). It combines the real world and phone to make you feel as though you are within the world of pokemon. For forensic investigators, games like these are extremely important, as they are always tracking and saving the location of the phone. This can help give the investigators a general sense of where the phone had been traveling and around what time as well. Without even digging into a forensics application, you can view your own location history through going into location services, choosing system services and selecting frequent or significant locations. These third party apps while games and or helpful for weather can also be used in a way that is advantageous to the forensic investigator to gather times, date, and location of where the phone has traveled.

Conclusion

The field of forensics for an iPhone is broad and ever changing, as the major releases of IOS overhaul the systems used by Apple. Keeping up and understanding what has changed will make the life of a forensics investigator much simpler, as it will allow them to be ready for the investigation rather than relying only on previous knowledge. The information stored on an Iphone is vast as it can allow you to not only access the user's accounts, location, numbers, but also other individuals they interacted or made contact with. In addition, even deleted information is stored within a cache and can be retired to further help with the investigation. In some cases, the data might be uploaded to the ICloud, so having access to the Iphone and its data can help retrieve whatever might have been tried to be hidden. Not only does this help with third party applications, but even preinstalled applications use this type of configuration to store the

information, so being able to access it has many advantages for the investigator. Though forensic investigators will need to go through due diligence while investigating, the results will be helpful in any case they are building, resulting in information that could reveal what had been taking place.

References:

A brief history of Ios. Gizmodo. (2016, June 7). from https://gizmodo.com/a-brief-history-of-ios-1780790760

App Store Data (2023). Business of Apps. (2023, February 23). from https://www.businessofapps.com/data/app-stores/

Lopez, G. (2016, July 11). *Pokémon go, explained*. Vox. from https://www.vox.com/2016/7/11/12129162/pokemon-go-android-ios-game

Mobile Vendor Market Share United States of america. StatCounter GlobalStats. (n.d.). from https://gs.statcounter.com/vendor-market-share/mobile/united-states-of-america

Pre-installed software definition. Law Insider. (n.d.). from https://www.lawinsider.com/dictionary/pre-installed-software

Shaikh, H. (2021, September 7). Ios Forensics. Infosec Resources. from https://resources.infosecinstitute.com/topic/ios-forensics/

Third-party software. THIRD-PARTY SOFTWARE definition | Cambridge English Dictionary. (n.d.). from https://dictionary.cambridge.org/us/dictionary/english/third-party-software