Mobile and Forensics (MF)
Vol. 4, No. 1, March 2022, pp. 44-52
P-ISSN: 2656-6257, E-ISSN: 2714-6685, DOI: http://dx.doi.org/10.12928/mf.v1i1.5762

A FORENSIC ANALYSIS OF VIDEO STREAMING ACTIVITIES ON ANDROID APPLICATIONS

[1*]Adil Ahmad, [2]Mehdi Hussain
[1]NUST School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad, 44000, Pakistan, +92-51- 9085 2400
[2] NUST School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad, 44000, Pakistan, +92-51- 9085 2400
*Corresponding e-mail: adilahmad95@gmail.com

Abstract

Mobile applications of video streaming platforms store a lot of information on mobile devices which can have both positive and negative impacts. Positive, in the sense that it could assist law enforcement agencies in solving crime, and the negative impact is that it could be accessed by malicious actors. In this study, we forensically investigate the Netflix, Amazon Prime Video, and iFlix android applications. The major focus is on identifying stored artifacts on the mobile devices left behind by the android video streaming applications. It will give law enforcement agencies and forensic investigators a clear direction when it comes to extracting evidence to solve a crime. On the other hand, it will notify the mobile application developers on how to further improve the security of their mobile applications.

Keywords: Mobile Forensics, Video Streaming Platforms, Autopsy, Netflix, Android

INTRODUCTION

The past decade has seen a major shift in electronic media, especially in the entertainment sector [1]. Now, more people are consuming content through digital media, which was earlier being viewed via electronic media [2]. This has given rise to online video streaming platforms which allow users to view content at the time of their convenience as opposed to electronic media where the transmission has a set schedule [3]. Initially, these platforms could only be accessed through their web-based applications, but over time, mobile applications were also developed for these video streaming platforms [4]. These applications tend to store personal information and also leave behind remnants of the activities performed even after the application has been uninstalled [5]. These remnants need to be examined to verify whether they violate the privacy of the user [6]. In the scenario where malicious actors gain access to the mobile device of a user, it can prove detrimental for the user [7]. Furthermore, they can also aid in investigations where the law-enforcing authorities need to cross-check the alibi of the suspects [8]. A very common use case for this can be a road accident where the law enforcement agencies can prove that the suspect was viewing a video on one of these platforms. In this study, we will examine the video streaming applications. For this we selected the three most popular video streaming platforms which are Netflix, Amazon Prime Video, and iFlix. Amongst the three, Netflix is the most popular and has been present for the longest time. The goal is to present the artifacts left behind the applications along with the path to their location

Received January 9, 2022; Revised February 8, 2022; Accepted March 5, 2022

in a well-documented format that will assist the forensic investigators to get a better understanding of the applications' behavior.

Literature Review

Most of the forensic work conducted on android applications has dealt with instant messaging applications [9]. Over the last decade, we have seen a huge rise in the popularity of instant messaging applications that can be credited to the ubiquity of mobile devices. People share all sorts of personal information through these messaging applications, be it in the form of text or media, and a lot of this personal information gets left behind on the mobile device through which they are accessing the applications.

M.A.K. Sudozai et al. [10] carried out a forensic research study on the IMO call and chat app on both Android and iOS-based mobile devices. They examined both the artifacts left on the mobile device as well the network traffic transmitted while the application was running. Special emphasis was laid on extensively analyzing the encrypted network traffic. Furthermore, the file structure of the IMO app was studied and it was established what information is present in the different folders and file locations. Interesting artifacts were discovered which included audio, video, text, and image messages along with the personal information of the contacts of the user. Another significant discovery was the links of the IMO server at which the content was being uploaded. The researchers were able to access the information at those links without any authentication. On the network analysis side, it was found out that even if all the IMO servers are on the firewall, the application still keeps on working by maintaining connections with google servers on port number 443.

Similarly, Asmara Afzal et al. [11] also performed forensic analysis on an instant messaging application named Signal Messenger App. In their research, they targeted how secure instant messaging applications can be used for conducting crimes. Since the communication is end-to-end encrypted, the criminals can use this fact to their advantage as forensic analysis becomes difficult for such type of communication. The researchers opted for a network forensic strategy to identify artifacts. This was done by examining the payload patterns of the encrypted traffic. Researchers were able to detect activities such as text, audio, video, and image messages as well as calls. The list of chat servers and IP addresses involved was also acquired. Emails applications were forensically analyzed by Rusydi Umar et al. [12] and digital evidence was acquired.

In another study, Hijrah Nurhairani et al. [13] worked on the android application of the social media platform Twitter. In their study, they examined the differences in the artifacts acquired from a rooted and non-rooted android mobile device after running the Twitter application on it. The motive behind this research was to determine if any criminal activity was taking place on the application such as hate speech, cyberbullying, and stalking. The forensic methodology of the National Institute of Justice was followed which includes 5 stages which are identification, collection, examination, analysis, and reporting. The results showed that more evidence was obtained from the rooted phone as compared to the non-rooted phone. Furthermore, the evidence from the rooted phone proved the existence of hate speech by the user.

Internet users today face a lot of privacy issues, which has led to a shift towards private browsers. Muhammad Raheel Arshad et al. [14] conduct a forensic analysis on one such private browser called TOR which is based on onion routing. The analysis was conducted on Windows 10 and Android 10 devices. The study negates the privacy and anonymity

claims made by the TOR Project as the researchers were able to retrieve significant artifacts that revealed details about the user's browsing activities.

Proposed Method

The proposed research methodology is shown in figure 1. We start with rooting the device, then we install the desired application either through Google Play Store or through an APK downloaded from the internet. Next, we perform the required activities on the application and take the physical image of the mobile device. Finally, we examine, analyze and report our findings. This workflow was repeated for all the 3 android applications which were a part of this research project.

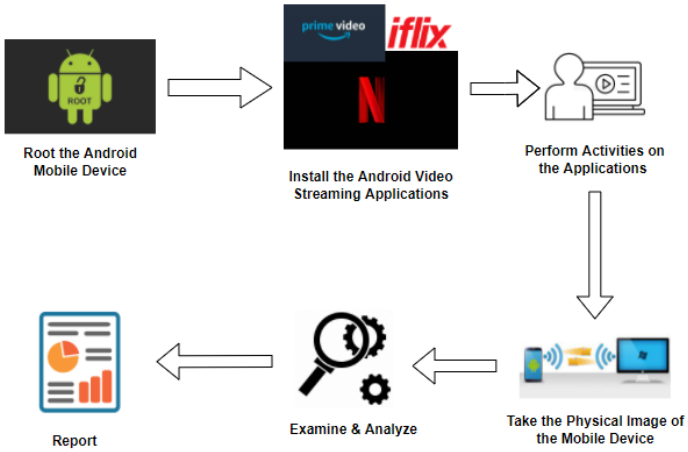

Fig. 1 Methodology of this Research

The following activities were performed individually on all the 3 applications and a physical image was taken after each activity was successfully conducted:

- Application Installation
- User Login
- Viewing a Video
- Searching for a Video
- Creating a List of Videos
- Downloading a Video
- Creating User Profiles
- Rating a Video
- Deleting a User Profile
- Uninstalling the Application

Following are the codes for the above-mentioned groups of activities:

Table 2 Description of groups of activities

Code of Groups of Activities	Description of the Group
AI	Downloading the application from Google Play Store or the internet and the subsequent Installation
UL	Logging in to the application
VW	Viewing an episode of a TV Show or watching a Movie
SV	Entering a search query in the search bar
CL	Creating a list of videos for easier access
DV	Downloading a video for later use
CP	Creating a separate profile for another user
RV	Providing feedback by upvoting or downvoting a video
DP	Deleting a user profile that was earlier created
UA	Uninstalling the application from the mobile device

RESULT AND DISCUSSIONS

1) Netflix

Netflix is the oldest and most popular online video streaming platform [15]. It can be accessed both on the web and through mobile device applications [16]. The company was formed in 1997 when it operated as a DVD rental business. It began its online streaming services in 2007 and ever since then it has seen tremendous success and growth. As of the year 2020, Netflix has over 200 million paid subscribers [17].
Netflix is also available on android mobile devices where it has over a billion downloads. In order to subscribe to the streaming platform, we need to purchase the subscription via a debit or credit card. There are multiple subscription plans available depending upon your requirements. The cheapest plan only allows you to view the content on your smartphones and tablets in 480p resolution, whereas the most expensive allows you to watch on any device with resolutions up to 4k.
The analysis of this application is based on its version 8.6.0, whose APK is available online at the following link: www.apkmirror.com. The following remnants were discovered concerning the activities performed along with the path to their location.

Table 2 Summary of Netflix Remnants with Location Path

Code	Main Directory	Folder	Filename
AI	1.1)/app	1.1.1)/com.netflix.mediaclient -1	1.1.1-a) Main Folder
	1.2)/app	1.2.1)/com.netflix.mediaclient 1.2.2) /com.android.vending/databases/ 1.2.3) /com.google.android.gms/databases	1.2.1-a) Main Folder 1.2.2-a) frosting.db 1.2.3-a) gass.db

			1.2.3-b) google_app_measurement .db
	1.3)/user_de	1.3.1) /0/com.netflix.mediaclient	1.3.1-a) Main Folder
UL	2.1)/data	2.1.1)/com.samsung.android.providers.contexy/databases	2.1.1-a) ContextLog.db
VW	3.1)/data	3.1.1) /com.netflix.mediaclient/databases 3.1.2) /com.samsung.android.providers.contexy/databases	3.1.1-a) appHistory 3.1.2-a) ContextLog.db
SV	4.1)/data	4.1.1) /com.samsung.android.providers.contexy/databases	4.1.1-a) ContextLog.db
CL	-	-	-
DV	6.1)/data	6.1.1) /com.netflix.mediaclient/databases 6.1.2) /com.netflix.mediaclient/files / img/of/videos	6.1.1-a) offlineDb 6.1.2-a) Image Files
CP	-	-	-
RV	-	-	-
DP	-	-	-
UA	4.1)/app	4.1.1) /com.netflix.mediaclient -1	4.1.1-a) Main Folder
	4.2)/data	4.2.1) /com.netflix.mediaclient 4.2.2) /com.google.android.gms/databases 4.2.3)/com.samsung.android.providers.contexy/databases	4.2.1-a) Main Folder 4.2.2-a) gass.db 4.2.3-a) ContextLog.db

2) Amazon Prime Video

Amazon Prime Video was launched in the year 2006 as an online video streaming service [18]. Later its mobile applications were also released. Currently, it has over 175 million users and its android application has over 100 million downloads. Amazon Prime Video is available in over 200 countries worldwide [19].

Upon subscription, Amazon Prime Video offers you a one-week trial period during which you can cancel the subscription and you will not be charged for it. You can subscribe through the android application by using your credit card or through the google play store payments feature [20].

The analysis of Amazon Prime Video's android application is based on its version 3.0.308.15647, which is the latest version available on the google play store as of now.

The following remnants were discovered concerning the activities performed along with the path to their location.

Table 3 Summary of Amazon Prime Video Remnants with Location Path

Code	Main Directory	Folder	Filename
AI	1.1)/app	1.1.1)/com.amazon.avod.thirdpartyclient -1	1.1.1-a) Main Folder
	1.2)/app	1.2.1)/com.amazon.avod.thirdpartyclient	1.2.1-a) Main Folder 1.2.2-a) frosting.db

		1.2.2) /com.android.vending/databases/ 1.2.3) /com.google.android.gms/databases	1.2.2-b) library.db 1.2.2-c) localappstore.db 1.2.3-a) gass.db
	1.3)/user_de	1.3.1) /0/com.amazon.avod.thirdpartyclient	1.3.1-a) Main Folder
UL	2.1)/data	2.1.1)/com.samsung.android.providers.contexy/databases	2.1.1-a) ContextLog.db
VW	3.1)/data	3.1.1) /com.samsung.android.providers.contexy/databases	3.1.1-a) ContextLog.dn
SV	4.1)data	4.1.1) /com.samsung.android.providers.contexy/databases	4.1)data
CL	5.1)data	5.1.1) /com.samsung.android.providers.contexy/databases	5.1.1-a) ContextLog.db
DV	6.1)data	6.1.1) /com.amazon.avod.thirdparty client/files/ downloads	6.1.1-a) Episode Folders
CP	-	-	-
RV	-	-	-
DP	-	-	-
UA	4.1)/app	4.1.1) /com.amazon.avod.thirdparty client-1	4.1.1-a) Main Folder
	4.2)/data	4.2.1) /com.amazon.avod.thirdparty client 4.2.2) /com.google.android.gms/databases	4.2.1-a) Main Folder 4.2.2-a) gass.db

3) iFlix

iFlix is one of the more recent entrants in the market of online video streaming platforms [21]. It was launched in the year 2014 and it primarily catered the Asian market with most of its content originating from China and Korea. As of 2020, iFlix has over 25 million active users and its android application has been downloaded over 50 million times.
Some of the features on this platform are free of cost while for others you have to subscribe to its service. You can view and download the initial episodes for free for most of the TV Shows currently hosted by iFlix, however to for later episodes you need to be a paid subscriber.
The analysis of the android application of iFlix is based on its version 4.6.6.603590720, which is the latest version available on google play store as of now.

The following remnants were discovered concerning the activities performed along with the path to their location.

Table 4 Summary of iFlix Remnants with Location Path

Code	Main Directory	Folder	Filename
AI	1.1)/app	1.1.1)/iflix.play-1	1.1.1-a) Main Folder
	1.2)/data	1.2.1)/iflix.play 1.2.2) /com.android.vending/databases/ 1.2.3) /com.google.android.gms/databases	1.2.1-a) Main Folder 1.2.2-a) frosting.db 1.2.2-b) library.db 1.2.2-c) localappstore.db 1.2.3-a) gass.db

	1.3)/user_de	1.3.1) /0/iflix.play	1.3.1-a) Main Folder
UL	2.1)/data	2.1.1)/com.samsung.android.providers.contexy/databases	2.1.1-a) ContextLog.db
VW	3.1)/data	3.1.1)/iflix.play/databases	3.1.1-a) videointernational.db
SV	4.1)/data	4.1.1) /com.samsung.android.providers.contexy/databases	4.1.1-a) ContextLog.db
CL	-	-	-
DV	6.1)/data	6.1.1) /com.samsung.android.providers.contexy/databases 6.1.2)/iflix.play/files	6.1)/data 6.1.2-a) Downloaded Episodes
CP	-	-	-
RV	-	-	-
DP	-	-	-
UA	4.1)/app	4.1.1) /iflix.play-1	4.1.1-a) Main Folder
	4.2)/data	4.2.1) /iflix.play 4.2.2) /com.google.android.gms/databases	4.2.2-a) gass.db

Conclusion

Our results included several artifacts with great forensics value. These contained the account information of the user who downloaded the application, information about the application such as its package name and version. More importantly, we could exactly state the timestamps between which a user was viewing a video. This helps in reliably formulating the timeline of activities of the suspect should he be involved in any criminal activity such as a car accident. Furthermore, artifacts related to downloading a video were also found.

The artifacts, apart from having forensic value, also pose a privacy risk. As so much information related to the user is stored on the mobile device, it can prove detrimental to the user should the mobile device be accessed by malicious actors. Mobile application developers should limit the amount of information stored on the mobile devices and try to encrypt it as much as possible.

Future Work

In our research project, we tried to as comprehensive as possible given our constraints. However, due to limitations of time and technology there still remains potential for future work in this domain. The focus of our study was on the physical image of the device storage and in the future people can work on acquiring the volatile memory when an application is running to study the artifacts present in it. Secondly, we carried our research on android based applications as this is the more popular mobile OS, however, a similar study can be conducted on iOS based video streaming applications and the artifacts can be compared with those collected from android applications to formulate a comparative study. Finally, this study was conducted on the most popular video streaming platforms globally and in the future researchers can focus on the local alternatives of these applications.

References

[1] T. Hermawan, Y. Suryanto, F. Alief, and L. Roselina, ‘Android Forensic Tools Analysis for Unsend Chat on Social Media’, in *2020 3rd International Seminar on Research of*

Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, Dec. 2020, pp. 233–238. doi: 10.1109/ISRITI51436.2020.9315364.

[2] A.-S. T. Olanrewaju, M. A. Hossain, N. Whiteside, and P. Mercieca, 'Social media and entrepreneurship research: A literature review', *International Journal of Information Management*, vol. 50, pp. 90–110, Feb. 2020, doi: 10.1016/j.ijinfomgt.2019.05.011.

[3] C. Ruiz-Mafe, E. Bigné-Alcañiz, and R. Currás-Pérez, 'The effect of emotions, eWOM quality and online review sequence on consumer intention to follow advice obtained from digital services', *JOSM*, vol. 31, no. 3, pp. 465–487, Jun. 2020, doi: 10.1108/JOSM-11-2018-0349.

[4] J. Moore, I. Baggili, and F. Breitinger, 'Find Me If You Can: Mobile GPS Mapping Applications Forensic Analysis & SNAVP the Open Source, Modular, Extensible Parser', *JDFSL*, 2017, doi: 10.15394/jdfsl.2017.1414.

[5] H. Xie, H.-C. Chu, G.-J. Hwang, and C.-C. Wang, 'Trends and development in technology-enhanced adaptive/personalized learning: A systematic review of journal publications from 2007 to 2017', *Computers & Education*, vol. 140, p. 103599, Oct. 2019, doi: 10.1016/j.compedu.2019.103599.

[6] Z. Zhang, Y. Wang, J. Jing, Q. Wang, and L. Lei, 'Once Root Always a Threat: Analyzing the Security Threats of Android Permission System', in *Information Security and Privacy*, vol. 8544, W. Susilo and Y. Mu, Eds. Cham: Springer International Publishing, 2014, pp. 354–369. doi: 10.1007/978-3-319-08344-5_23.

[7] S. Sack, K. Kröger, and R. Creutzburg, 'Location tracking forensics on mobile devices', Burlingame, California, USA, Mar. 2013, p. 866712. doi: 10.1117/12.2003952.

[8] N. Al Mutawa, J. Bryce, V. N. L. Franqueira, A. Marrington, and J. C. Read, 'Behavioural Digital Forensics Model: Embedding Behavioural Evidence Analysis into the Investigation of Digital Crimes', *Digital Investigation*, vol. 28, pp. 70–82, Mar. 2019, doi: 10.1016/j.diin.2018.12.003.

[9] C. Anglano, M. Canonico, and M. Guazzone, 'Forensic analysis of Telegram Messenger on Android smartphones', *Digital Investigation*, vol. 23, pp. 31–49, Dec. 2017, doi: 10.1016/j.diin.2017.09.002.

[10] M. A. K. Sudozai, S. Saleem, W. J. Buchanan, N. Habib, and H. Zia, 'Forensics study of IMO call and chat app', *Digital Investigation*, vol. 25, pp. 5–23, Jun. 2018, doi: 10.1016/j.diin.2018.04.006.

[11] A. Afzal, M. Hussain, S. Saleem, M. K. Shahzad, A. T. S. Ho, and K.-H. Jung, 'Encrypted Network Traffic Analysis of Secure Instant Messaging Application: A Case Study of Signal Messenger App', *Applied Sciences*, vol. 11, no. 17, p. 7789, Aug. 2021, doi: 10.3390/app11177789.

[12] R. Umar, I. Riadi, and B. F. Muthohirin, 'Live forensics of tools on android devices for email forensics', *TELKOMNIKA*, vol. 17, no. 4, p. 1803, Aug. 2019, doi: 10.12928/telkomnika.v17i4.11748.

[13] H. Nurhairani and I. Riadi, 'Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method', *IJCA*, vol. 177, no. 27, pp. 35–42, Dec. 2019, doi: 10.5120/ijca2019919749.

[14] M. R. Arshad, M. Hussain, H. Tahir, S. Qadir, F. I. Ahmed Memon, and Y. Javed, 'Forensic Analysis of Tor Browser on Windows 10 and Android 10 Operating Systems', *IEEE Access*, vol. 9, pp. 141273–141294, 2021, doi: 10.1109/ACCESS.2021.3119724.

[15] B. Burroughs, 'House of Netflix: Streaming media and digital lore', *Popular Communication*, vol. 17, no. 1, pp. 1–17, Jan. 2019, doi: 10.1080/15405702.2017.1343948.

[16] R. Lobato and A. D. Lotz, 'Imagining Global Video: The Challenge of Netflix', *JCMS*, vol. 59, no. 3, pp. 132–136, 2020, doi: 10.1353/cj.2020.0034.

[17] A. D. Lotz, 'In between the global and the local: Mapping the geographies of Netflix as a multinational service', *International Journal of Cultural Studies*, vol. 24, no. 2, pp. 195–215, Mar. 2021, doi: 10.1177/1367877920953166.

[18] A. Lad, S. Butala, and P. Bide, 'A Comparative Analysis of Over-the-Top Platforms: Amazon Prime Video and Netflix', in *Communication and Intelligent Systems*, vol. 120, J. C. Bansal, M. K. Gupta, H. Sharma, and B. Agarwal, Eds. Singapore: Springer Singapore, 2020, pp. 283–299. doi: 10.1007/978-981-15-3325-9_22.

[19] I. Tiwary, 'Amazon Prime Video: A Platform Ecosphere', in *Platform Capitalism in India*, A. Athique and V. Parthasarathi, Eds. Cham: Springer International Publishing, 2020, pp. 87–106. doi: 10.1007/978-3-030-44563-8_5.

[20] M. Song, 'A Comparative Study on Over-The-Tops, Netflix & Amazon Prime Video: Based on the Success Factors of Innovation', *International journal of advanced smart convergence*, vol. 10, no. 1, pp. 62–74, Mar. 2021, doi: 10.7236/IJASC.2021.10.1.62.

[21] E. Ferraz and G. Fernandez, 'Patrick Grove: Co-founder, iflix', in *Asian Founders at Work*, Berkeley, CA: Apress, 2020, pp. 115–123. doi: 10.1007/978-1-4842-5162-1_10.