AUGUSTA UNIVERSITY
SCHOOL OF COMPUTER AND CYBER SCIENCES

Forensic Analysis of Snapchat iOS App Containing Spectacles-synced Artifacts

Logan VanPutte and Dr. Gokila Dorai — Augusta University, Augusta, Georgia
Andrew Clark IV, Rayna Mock, and Josh Brunty — Marshall University, Huntington, West Virginia

INTRODUCTION

- Worldwide in 2020, over 347 million users were active on Snapchat each month, with India and the United States having an enormous user-base by a large margin [1], [2]. In biannual surveys from 2012 to 2020 [3], Snapchat has been ranked as the most critical social media by teens in the United States (since 2018), followed by TikTok and Instagram.
- Snapchat is a social media mobile messaging application with related desktop and web applications [4], [5] used for multimedia instant messaging and communication Developed and maintained by the United States-based company Snap Inc.
- Spectacles wearable smart glass device from Snapchat records snaps and videos for use in Snapchat. It can sync data with a paired smartphone and upload recorded contents to a user's app.
- Extracting and analyzing data from a Snapchat app is challenging due to the disappearing nature of the media. Very few commercial tools are available to obtain data from Snapchat apps. The purpose of this research was to determine what artifacts we could extract and analyze from Snapchat app and specifically, Spectacles device(s) paired with Apple iPhones. The research provides interesting insights into evidence collection from wearable devices paired with Apple iPhones.

METHODS

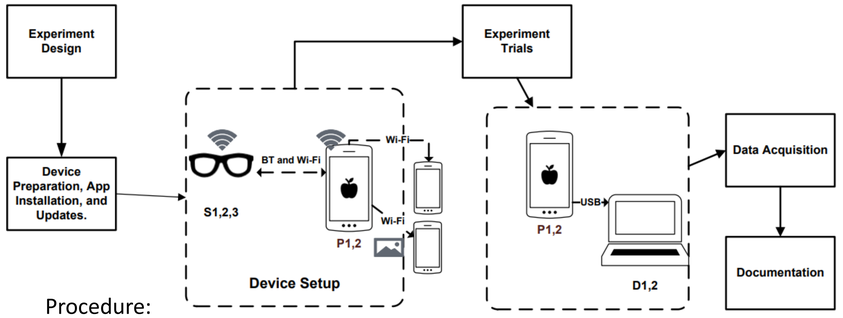
Table 1. Device details.

Device	Type	Operating System
Spectacles that Snap! (Coral) First Generation (S1)	Wearable IoT	Spectacles v1.11.5
Spectacles 2 (Original Onyx) Second Generation (S2)	Wearable IoT	Spectacles v2.15.2
Spectacles 2 (Original Onyx) Second Generation (S3)	Wearable IoT	Spectacles v2.15.2
iPhone 11 (P1)	Smartphone	iOS 14.6
iPhone 12 (P2)	Smartphone	iOS 14.6
Alienware 13 R3 (D1)	Laptop	Windows 10 Home v21H1
Computer (D2)	Computer	Windows 10 Enterprise v20H2
USB Cables	Connector	NA

Table 2. Software details.

Software	Version	Devices
Cellebrite Physical Analyzer	7.36.0.42	Computer
Cellebrite UFED	7.49.0.2	Computer
iExplorer	4.4.2	Laptop
iTunes	12.11.3.17	Laptop
Magnet AXIOM Process and Examine	5.3.0.25803	Laptop, Computer
Magnet AXIOM Process and Examine	5.5.1.26621	Laptop, Computer
Snapchat App for iOS	11.34.1.34-5	iPhone 11, iPhone 12

METHODS



Procedure:

1. Setup iPhones, install updates, and setup Snapchat accounts.
2. Setup Spectacles and update.
3. Connect iPhone to Wi-Fi and pair with Spectacles via Bluetooth.
4. Create Snaps (pictures and videos) with Spectacles & upload into Snapchat application when iPhone and Spectacles connected to the Wi-Fi.
5. Confirm appearance in Snapchat application.
6. Share Snaps in application with another account.
7. Create Snaps in Snapchat application with iPhone camera.
8. Share with another account.
9. Create forensic image using iTunes, backup, Cellebrite UFED, &/or Magnet AXIOM Process.
10. Analyze with Macroplant's iExplorer, Cellebrite Analyzer, and Magnet AXIOM Examine.

RESULTS

Table 3. Main Snapchat data locations.

Directory	Folder	Subfolder
App	com.toyopagroup.picaboo (F1)	/Documents (SF1) /Library (SF2)
App Group	group.snapchat.picaboo (F2)	/Library/Preferences (SF3) /WidgetExention (SF4)
App Plugin	com.toyopagroup.picaboo.homeWidget (F3) com.toyopagroup.picaboo.notification (F4) com.toyopagroup.picaboo.share (F5) com.toyopagroup.picaboo.today (F6)	

- Snaps taken with Spectacles and shared showed thumbnails after sharing and had rounded edges.
  - Snaps taken within the Snapchat application and shared, only displayed message confirming delivery and no thumbnail
- Corresponding .MOV, .THM, .JPG, .IMU, AND .MDA files for Snaps taken with Spectacles were stored under SF1's "laguna" folder using unique identifiers.
  - The same folder also contained a file "device-list-archive.dat" which contained information about Spectacles.
  - Playable video files were found for older videos taken with Spectacles.

RESULTS

CONCLUSIONS

- Most of the artifacts discovered are related to Spectacles and they were in SF's 'laguna' file and the PLIST and JSON files in SF2.
- The iPhones we used were not jailbroken; however, we may have been able to use encryptions keys to discover more artifacts and decrypt Snapchat Memories and Snapchat My Eyes Only [6].
  - There were several folders under SF1 with promising sounding names, which were empty, such as 'gallery,' gallery_data_object', and 'gallery_encrypted_db.'

REFERENCES

[1] Statista, Snapchat: number of global users 2018-2024, New York, New York, USA (www.statista.com/statistics/626835/number-of-monthly-active-snapchat-users), 2021.
[2] Statista, Countries with the most Snapchat users 2021, New York, New York, USA (www.statista.com/statistics/315405/snapchat-user-region-distribution), 2021.
[3] Statista, Favorite social networks of U.S. teens 2012-2020, New York, New York, USA (www.statista.com/statistics/250172/ social-network-usage-of-us-teens-and-young-adults), 2021.
[4] Snap Inc, Snap Camera FAQ, Santa Monica, California, USA (support.snapchat.com/en-US/article/snap-camera-faq).
[5] Snap Inc, About Snap Map, Santa Monica, California, USA (support.snapchat.com/en-US/article/snap-map-about).
[6] Magnet Forensics, Decrypt app data using the iOS Keychain and GrayKey, Waterloo, Canada (support.magnetforensics.com/s/article/Decrypt-app-data-using-the-iOS-Keychain-and-GrayKey), 2021.

ACKNOWLEDGEMENTS

We thank the National Science Foundation (NSF) for support through the CyberCorps SFS program and the IFIP Working Group 11.9 on Digital Forensics for publication of the peer-reviewed conference paper.