Executive Summary

Tiktok is a social media application that has soared in popularity in recent years due to its usage among the adolescent (10 to 14 years old) and teenage (15 to 19) demographic. It consists of 15 seconds to 10 minute video uploads with a library of music or user created sounds to accompany it (D'Souza, 2024). Cases of crimes committed through social media such as cyberbullying, distribution of child sexual abuse material and cyberstalking on the platform have been recorded with minors being victims. One such case of cyberstalking is the story of how Ava Majury rose to fame during the lockdown phase of the COVID-19 pandemic in 2020, attracting a diverse following of her peers and adults alike on the application. One of her older male followers, Eric Justin began stalking Ava to the point of harassing her school mates and friends for personal details of her life such as her home address in exchange for money. Eric showed up to Ava's house with a gun but was unsuccessful in harming anyone there and was shot and killed by Ava's father instead. Two phones with thousands of pictures of Ava were found on him. (Williamson, 2022). The Information Commissioners Office's Directorate of Economic Analysis, (2023) reported there were between 1.1 million and 1.4 million children under the age of 13 with a TikTok account. TikTok was also handed EUR 345 million in administrative fines following an investigation that concluded in 2023 on how the organization was verifying the age of registered users and handling privacy settings for accounts of minors on the platform (Irish Data Protection Commission, 2023).

This investigation seeks to identify artifacts related to operations performed by the user within TikTok's Android application through forensic analysis performed according to the National Institute of Standards and Technology (NIST) 800-101 R1 guidelines on mobile forensics. The NIST 800-101 R1 guidelines are part of the industry standards for conduction of mobile forensic investigations. (Ayers, Brothers and Jansen, 2014).

The major findings of the investigation are information on registered user accounts signed into the application as well as information on the device the application is installed on.

Methodology

This report seeks to critically analyze the app, interrogate it for how it is structured and potential sources of evidence, identify artifacts and suggest ways information/artifacts could be utilized for investigations into real life incidents. This was done mainly through literature review of existing works related to TikTok Android forensics. Peer reviewed papers from industry journals not preceding January 2020 were preferred for review in this report. Investigations by Hoang Khoa *et al.*, (2020) and Domingues *et al.*, (2021) were reviewed and their analysis was replicated using some of the tools and methods used to verify the validity of the artifacts obtained under similar conditions. The four phases of mobile device forensics namely Identification, Acquisition, Analysis and Reporting according to the NIST 800-101 guidelines

were followed in this investigation to ensure best practices are followed and the investigation is done to industry standards. ((Ayers, Brothers and Jansen, 2014)

Preservation: This phase of the process involves identification of the artifacts on the Android emulator. Hoang Khoa *et al.*, (2020) identified the /data/`data/com.zhiliaoapp.musically` directory as the location of artifacts found on a rooted Nox player emulator in TikTok version 8.9.4. This directory structure was also confirmed by (Domingues *et al.*, 2021) in their paper on version 18.1.3 of the TikTok android app.

Acquisition: The emulator is put in airplane mode and connected to Android Debug Bridge (ADB). The `adb shell` command is then run to access the emulator's file system where a tape archive (tar) of the `/data` directory in the root filesystem and zipped for ease of export to a Windows PC for analysis. The zipped file is then exported to the Downloads directory for analysis. A copy of the original extracted tape archive zip file was preserved on an external thumb drive as a precaution taken to ensure the evidence is not lost in the event of loss or damage of the PC used for analysis. A Level 2 acquisition was performed to logically acquire artifacts according to the NIST 800-101 R1 guidelines (Ayers, Brothers and Jansen, 2014).

A diagram of the folder structure of the acquired artifacts is shown below:

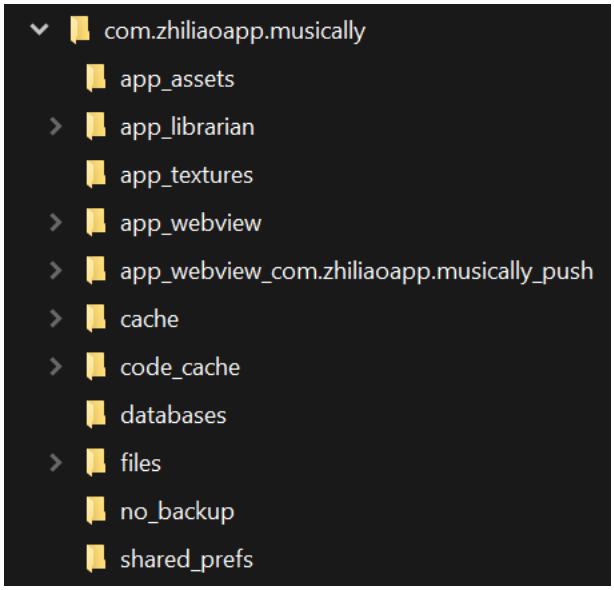

Fig. 1 Directory structure of the logically acquired artifacts.

The Analysis and Reporting phases will be covered by the following sections of the report:

Environment setup

To analyze the Android application the following tools were used:

- **NoxPlayer**: Version 33.4.3 of the TikTok Android application was installed on a rooted version 7.0.5.9 Noxplayer emulator running the Android 9 operating system (Pie) on a Windows 10 PC (build num, update). (Nox, no date). This tool was preferred for use in this investigation due to the ease of rooting the emulator.
- **Android Debug Bridge (ADB):** Version 34.0.5 Android Debug Bridge (ADB) tools were used to interact with the emulator via a command line interface. (Android Developers, 2023). The command line utilities utilized in the acquisition and extraction of evidence from the emulator are detailed in Appendix A-1. This tool was preferred for use in this investigation because it originated from Google who are the creators of the Android operating system.
- **SQLite DB Browser:** Version 3.12.2 of the DB Browser for SQLite was used to view the SQLite databases discovered within the databases directory. (SQLite Browser, no date). This tool was preferred for use in this investigation due to its usage of open-source technologies and a lack of competent free alternatives.
- **Visual Studio Code:** Version 1.87 of the Visual Studio Code (VS Code) was used to view the Xtensive Markup Language (XML) files discovered within the `shared_prefs` folder. (Microsoft, no date). VS Code was preferred to other text editors and Integrated Development Environments (IDE) due to its ease of use and lively marketplace of extensions such as the XML Support extension to make inspection of XML code much easier. (Redhat, no date)
- **7zip:** Version 24.01 of the 7zip tool was used to unzip the tape archive of the logical acquisition. (Igor, no date). A logical acquisition of artifacts was preferred for this investigation due to the rooted status of the Noxplayer emulator. See Appendix A-1 for screenshots of the command line interactions in the logical acquisition process.

App Investigation and Findings

Behavior of the app

TikTok is a video creation and sharing platform where videos can be any length from 15 seconds to 10 minutes. Live video sessions may also be shared by users provided they have 1000 or more followers. Users may also send messages to other registered users of the platform. Upon opening the app, the first screen presented to a user is a personalized stream of videos suggested by the TikTok algorithm and plays on a loop until the user scrolls vertically. (D'Souza, 2024). Each video can be viewed, liked, bookmarked, or commented on by the user.

Sources of artifacts

Upon investigation of the acquired evidence, `the databases` and `shared_prefs` directories stood out as containing the most information on the user and the device the application is installed on.

`databases` directory

Of the 71 files contained in this directory, 14 stood out as forensically relevant because they all contain a `user_id` field within one or more tables in the databases denoting the User ID number of the user(s) logged into the app on the device. One of the most forensically relevant tables in this directory is the `msg` table contained in the `<userID>_im` database which contains the content of messages exchanged between users as well as the timestamp of messages and an indication of whether the message was deleted or not. This was consistent with results obtained by (Domingues *et al.*, 2021) after inspection. See Appendix * for screenshots of the SQLite database inspection within the SQLite DB Browser.

`shared_prefs` directory

This directory contains XML files relating to user and device configurations. One interesting file within this directory is `aweme_user.xml` file. This file contains data on user information including information that is not immediately visible within the app such as age, gender and bits of the email and phone number registered to the user. (Domingues *et al.*, 2021) reported the `applog_stats.xml` file previously held device network data for user tracking in previous versions of the application, but this was criticized and removed due to the privacy concerns it caused.

Recommendations

The tools used have pointed to a few sources of forensic artifacts that can be obtained from the device. These artifacts can be used to reconstruct elements of events that occurred in cases of harassment via messages in the event an accused individual denies allegations. Investigators can use the artifacts highlighted in this report to also establish provenance of these events in cases where the facts are disputed.

Conclusion

From the story of Ava Majury at the beginning of this report, it is logical to posit, the evidence contained in the phones found on him along with publicly known information and witness testimony may have been useful prosecuting a case against him in the event her assailant had been caught, taken into custody alive and charges brought against him. This may have given the prosecutor enough evidence to link the information found on the phones as well as the phones to the assailant. This demonstrates the importance of digital forensic investigation techniques, tools and results based on the behavior of the application for obtaining evidence to utilize in all types of cases.

References

Android Developers (2023) *Android Debug Bridge (adb) | Android Studio | Android Developers*. Available at: https://developer.android.com/tools/adb (Accessed: 1 March 2024).

Ayers, R., Brothers, S. and Jansen, W. (2014) *Guidelines on mobile device forensics*. NIST SP 800-101r1. National Institute of Standards and Technology, p. NIST SP 800-101r1. Available at: https://doi.org/10.6028/NIST.SP.800-101r1.

Domingues, P. *et al.* (2021) 'Analyzing TikTok from a Digital Forensics Perspective', *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 12(3), pp. 87–115. Available at: https://doi.org/10.22667/JOWUA.2021.09.30.087.

D'Souza, D. (2024) *TikTok: What It Is, How It Works, and Why It's Popular*. Available at: https://www.investopedia.com/what-is-tiktok-4588933 (Accessed: 1 March 2024).

Hoang Khoa, N. *et al.* (2020) 'Forensic analysis of TikTok application to seek digital artifacts on Android smartphone', in *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)*. *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)*, Ho Chi Minh, Vietnam: IEEE, pp. 1–5. Available at: https://doi.org/10.1109/RIVF48685.2020.9140739.

Igor, P. (no date) *7-Zip*. Available at: https://www.7-zip.org/ (Accessed: 1 March 2024).

Information Commissioners Office's Directorate of Economic Analysis (2023) *Annex 2: Estimated TikTok users in the UK, under the age of 13*.

Irish Data Protection Commission (2023) *Irish Data Protection Commission announces €345 million fine of TikTok | 15/09/2023 | Data Protection Commission*. Available at: https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok (Accessed: 17 February 2024).

Microsoft (no date) *Visual Studio Code February 2024*. Available at: https://code.visualstudio.com/updates/v1_87#vscode (Accessed: 1 March 2024).

Nox (no date) *Noxplayer – Fastest and Smoothest Android Emulator for PC & Mac – Free and Safe*. Available at: https://www.bignox.com/ (Accessed: 1 March 2024).

Redhat (no date) *XML - Visual Studio Marketplace*. Available at: https://marketplace.visualstudio.com/items?itemName=redhat.vscode-xml (Accessed: 1 March 2024).

SQLite Browser (no date) *About - DB Browser for SQLite*. Available at: https://sqlitebrowser.org/about/ (Accessed: 1 March 2024).

Williamson, E. (2022) 'TikTok star Ava Majury discovers the dark side of fame', 17 February. Available at: https://www.nytimes.com/2022/02/17/us/politics/tiktok-ava-majury.html (Accessed: 28 February 2024).

Appendix A

1

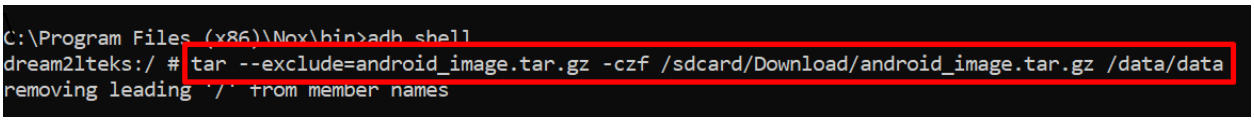

Fig 2. Command input to create tape archive zip file within root shell prompt of Android emulator.

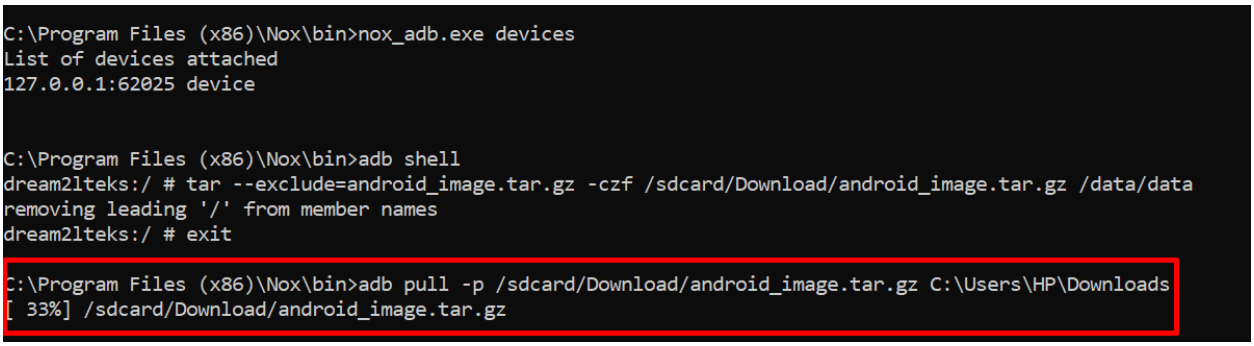

Fig 3. Command input to pull extract tape archive from emulator storage to Downloads directory.

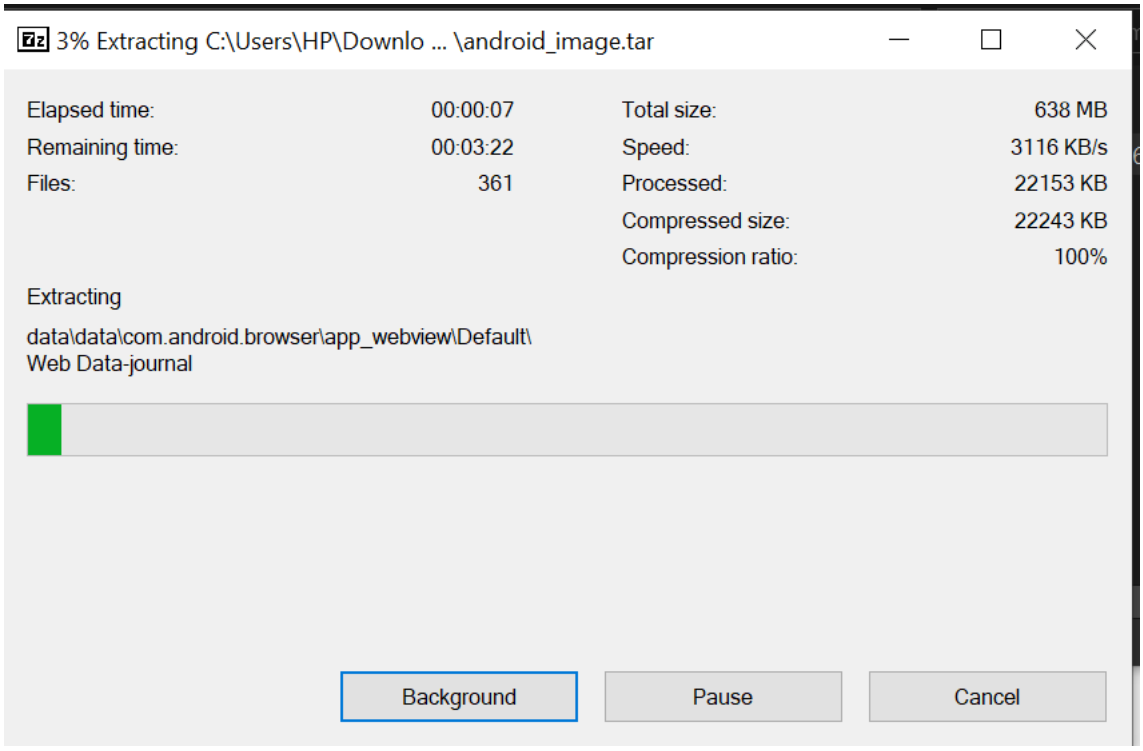

Fig 4. Extracting the data with 7zip

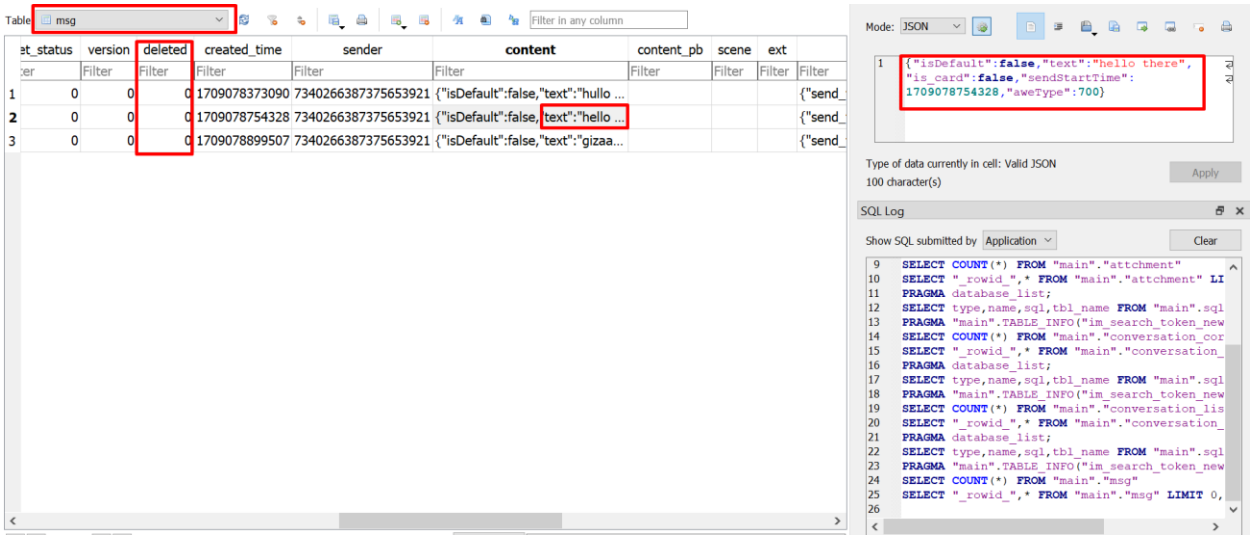

Fig 5. Messaging data contained within the msg table

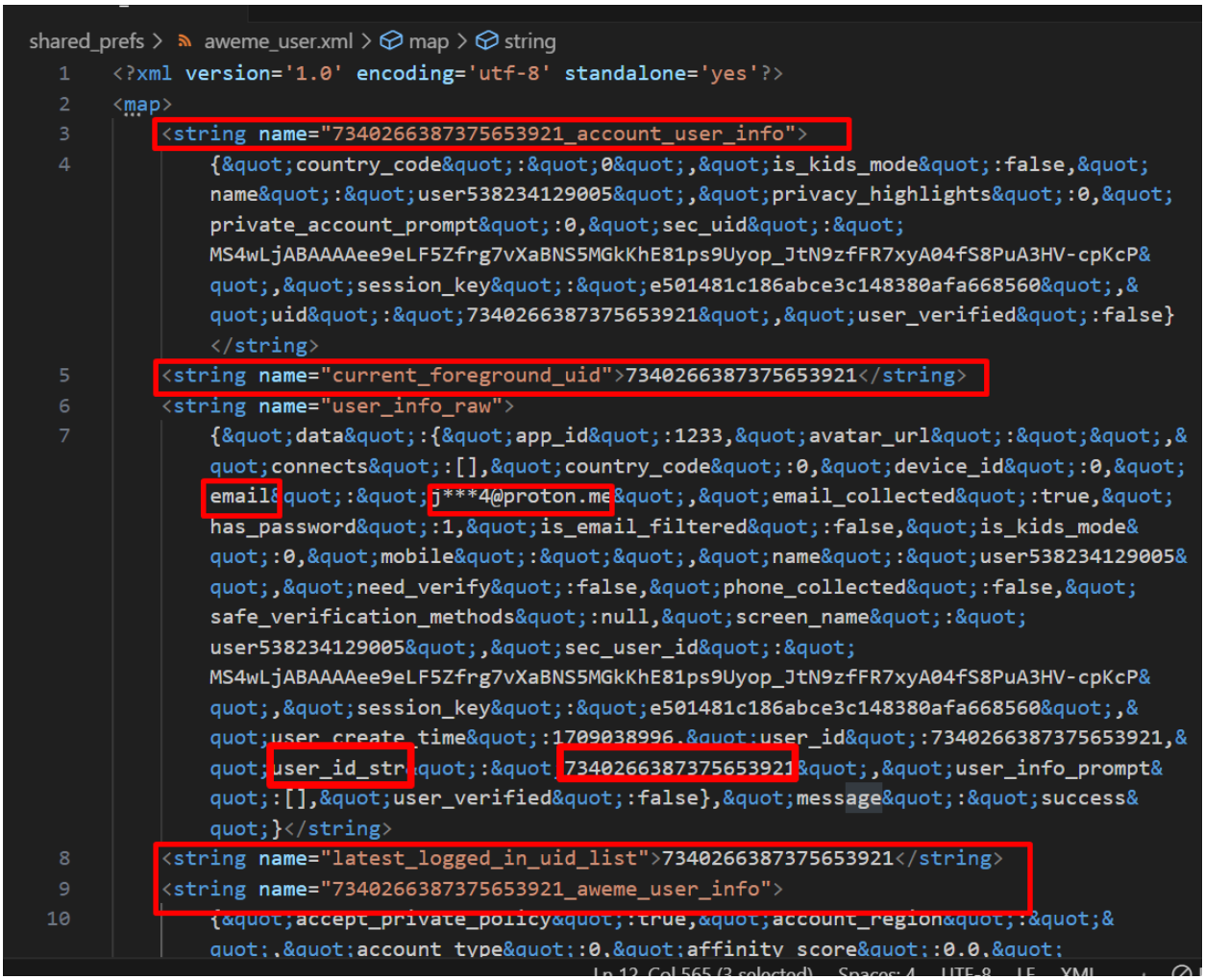

Fig. 6 User data contained within the aweme_user.xml file