# Investigating Social Media User Activity on Android Smartphone

Muhammad Romi Nasution
Islamic University of Indonesia
Yogyakarta

Yudi Prayudi
Islamic University of Indonesia
Yogyakarta

Ahmad Luthfi
Islamic University of Indonesia
Yogyakarta

## ABSTRACT
Considering the trend of social interaction and relationships on the internet, online social media has greatly affected people's daily lives. Everyone can now easily connect in their social circle via smartphone, making it an easier choice by users. Social media applications definitely leave their mark on smartphones. The attractive trait of smartphones for forensic examiners is due to user activity on smartphones. Forensic investigators can extract evidence by selecting appropriate extraction techniques and forensic tools. The main contribution of this research is to emphasize digital forensics on android smartphones on the well-known social media application TikTok, because it is one of the social media that is currently on the rise, judging by the advantages of TikTok in presenting short video content so creative and interesting. some users create content to get more attention and recognition thereby increasing their sociality. The purpose of the study was to identify the characteristics of activity on smartphones when using more than one TikTok account.

## General Terms
Activity Artifact, Investigation Smartphone, XML Files, Information User Application, Database SQL

## Keywords
Smartphone, Android, Activity, Digital Forensics, Social Media

## 1. INTRODUCTION
Smartphones are not only used in interpersonal communication. However, most play a key role in all activities such as eating, sleeping, exercising, driving, and interacting with other people, etc. All are associated with the applications installed on our mobile devices. Installed apps generate and store large data sets on the device. Later, it can be used to reconstruct the activities performed by the user on the device [1]. Including android operating system smartphones whose partition contains the user's personal information stored by each application. Android applies Sandboxer to each application, providing the ID and package name of access only to the file system path that was previously declared in the APK file to prevent the application from accessing different areas for security reasons. Android also allows each app to store attributes such as app permissions and file system information in the system log [2]. Social media allows users to interact online, contribute concepts, ideas, and experiences from the same interests such as status updates, pictures, videos, and share files and other information as well as work together on various activities and events besides being able to communicate with friends and relatives online via instant messaging and electronic mail. The abundance of these facilities attracts a large number of social media users around the world, the population of continued addition to short video applications comes from those who experience more social interaction anxiety, thus seeking more entertainment through the use of the application [3]. One such application is TikTok. As the application was originally an application called musica.ly later acquired by the bite dance company, the video creation and sharing application has attracted the attention of young viewers around the world. Featuring audio and visual controls for creating 15-second videos, it includes in-camera speed controls, image-tracking composites, collaborative split-screens, and a shortened video timeline. The next feature is to forward video content to their friends on TikTok. They can also forward videos to other social media. Thus making TikTok the most downloaded video application by teenagers aged 13-18 and active. Half of 500 million monthly users [4]. Shown in the figure, 1 active TikTok users in August 2020 reached 22.2 million in Indonesia.

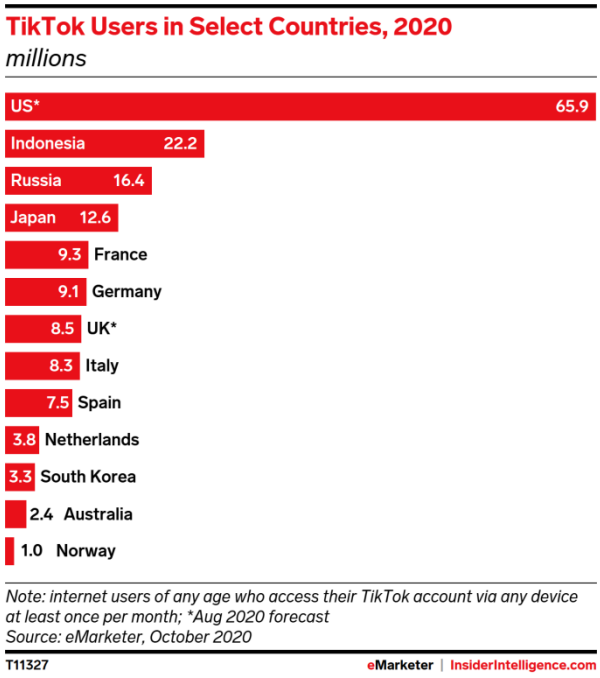


**Figure 1: Active TikTok users in August 2020**

The United States is the largest market for TikTok in 2020 with 65.9 million monthly users after excluding commercial, duplicate, fake and non-human accounts. Indonesia has also become an important market with more than 22 million monthly users. Of the countries in Europe, Russia, France and Germany will be the largest user bases. Analyzing user interest through algorithm technology, one of which is strong and accurate hashtags so that recommending short video content is how the TikTok application works, users often see short video content from the same label and feel the

homogenization of content [5].

More TikTok users, the more the dark side. As the subject of unsettling reports about its content, which is reportedly filled with images of naked children, child predators, sneaky algorithms, lack of privacy, and teenagers intimidating and harassing each other and even allowing the flow of illegal drugs, messages of murder and animal cruelty, security and weak controls have made it possible to become a magnet for pedophiles, profanity, crime, violence, and extremism [6].

TikTok features can cause serious problems when the user is a child or teenager who does not yet fully understand the threat of the social network. TikTok allows users to make these short singing and dancing videos a useful tool for criminals to approach and sexually harass [7].

The TikTok application apparently leaves traces of xml files and databases on smartphones that contain important information about all application user activities. Field of xml files and databases there are several fundamental functions, such as insertion, deletion, modification, data modeling, storage and manipulation [8].

Various types of additional offensive actions that can be carried out on social media sites such as masquerading, humiliating or shocking, publishing prohibited material, stalking, immoral information for money or threatening to share personal, etc. Importance of digital forensic analysis of social media applications in smartphone devices is due to the increasing number of illegal activities that can be carried out in this field. The purpose of this research is to find out user activities, such as whether the activities carried out using the TikTok application are more than one account which can later be used for digital forensics.

## 2. LITERATURE REVIEW

Identification of digital artifacts on Facebook, Twitter and LinkedIn applications on Android, iOS, Windows and BlackBerry operating systems. The method used is disk image extraction and then performs analysis on the database file. All applications tested have different characteristics for each operating system, the challenge is that more and more social media will need to be analyzed every day [3]. Research [9] activity is divided into 5 types: web browsing history, cookies, images, downloads and instant messengers. As for browsing history, 11 web pages were found. As for cookies there are 8 activities, then 4 recoverable images. PDF file found in download activity and audio message on WhatsApp app. XML files are used in many ways as research [10] found several systems adopting XML (eXtensible Markup Language) to represent semi-structured data. XML documents as a standard for storing, representing, and exchanging data are adopted by several industries and the scientific community. As a result, a large number of XML documents are created every day. Examples include applications, health care departments and others. The research method [11] is to analyze artifacts left on Android smartphones. As a result, answering general questions including: how to obtain TikTok user data and how to disclose its contents. such as friends and followers, with whom users communicate. The drawback of this research is the time in XML file analysis, from 103 XML files it would be better if a feature was made to make it easier to determine the files related to needs.

## 3. METHODS

This study focuses on determining whether activity data from 2 social media application accounts on smartphones can be found and retrieved from the device's internal memory. The research methodology adopted forensically analyzes and investigates the activities carried out on the TikTok application version 16.6.4 using the android OS. Checking smartphone to extract digital evidence has its own significance as is verification and validation of evidence from different sources. All tests were performed following general guidelines and procedures for digital forensics recommendations National Institute of Standards and Technology (NIST) method. This method recommends the basic steps of the forensic process, namely collection, examination, analysis, declaration [12]. Forensic techniques are applied to ensure the reliability and security of evidence in order to avoid rejection in court by applying the hash value of each file so that the integrity and authenticity of the results are maintained [13].

### 3.1 Investigation Framework

Using indiscriminate processes and tools to extract digital evidence can compromise the integrity and credibility of evidence, the NIST steps used in forensic investigations have four stages: identification, preservation, analysis and presentation of digital evidence [9]. Research papers adapt the framework to guide smartphone investigations. The investigative framework consists of the following.

1. Identification and collection. Evidence is collected from the smartphone's internal storage. The context of this research, Xiaomi Redmi 5A running Android version Oreo 10.0 and 16 GB internal storage. Image by Image Android device internal memory is obtained using ADB debugging by following the following command line: adb pull -p <path on Android> <path to save data>.
2. Preservation. The MD5 hash value of each retrieved file is calculated. Furthermore, it is verified so that can detect any modification. Research investigation, comparison of MD5 level hash values and timestamp metadata of extracted files from the TikTok application revealed that the originality of the files from the start and end of the study had the same values, as shown in Table 1. Android file system hash values.

Each file must have a difference called the hash value, the first level of the value is MD5, time created is the time when the file was created [14]. File path is the name of the file following the extension it has, the file is obtained from several different directories such as the shared_prefs directory, databases and filters. the base of all artifact directory of TikTok app in android smartphone is com.ss.android.ugc.trill.

**Table 1. Information XML File**

| File Path | MD5 | Time Created |
|---|---|---|
| description.info.xml | 6E99229D2B1FFAD81964E650034A6A08 | Monday, February 22, 2021, 7:02:23 PM |
| aweme_local_video.xml | 0E5792E5196AA9F3A3822D254DC62E38 | Monday, February 22, 2021, 7:05:35 PM |
| aweme_user.xml | E3C3B987AF1A67F7F667D9ED5350BCA7 | Monday, February 22, 2021, 7:05:35 PM |
| Login Share | 07796660350D8BD1423D3A1 | Monday, February 22, 2021, 7:05:34 |

| | | |
|---|---|---|
| Preferences.xml | 4D15D29CA | PM |
| version.xml | 802354F9BAE ABEFFD4ED5 E4294D9C155 | Monday, February 22, 2021, 7:05:40 PM |
| 6930551655360 414721_im.db | 2021BFE5B3E8 358AE529430E A327FA53 | Monday, February 22, 2021, 7:03:21 PM |

3. Examination and analysis. Important process in the validation of xml documents to ensure the correct data structure then arises The DFXML (Digital Forensis XML) language is formalized by implementing an XML schema, and validation can be performed using the xml utility [15].The data collected from the device's internal memory is checked to determine the possible residual data usage of the TikTok application, TikTok version 16.6.4 has more than 100 XML files containing important information.

4. Presentation. A summary of the findings and their forensic value is presented at this stage

## 3.2 System Preparation

System Preparation consists of two things, namely hardware and software. The investigator has a hardware (***Table 2***) as a tool for extracting and analyzing evidence and use and use android backup to pull data from smartphone.

**Table 2. System Preparation**

| Hardware | Software |
|---|---|
| Redmi 5A (unlocked) specs 2 GB RAM, 1.40 GHz Quad-Core CPU with 16 GB Storage | Android Operating System Oreo version 10.0 |
| Dell latitude e7240 laptop with Windows 10 Pro 64-bit specifications, an Intel Core i5-4310U with a frequency speed of up to 2.6 GHz, 8 GB RAM and a 250 GB SSD as a tool for extracting and analyzing evidence | TikTok version 16.6.4 for Android (2 accounts) |
| | Android backup |
| | AccessData FTK Imager |
| | Hash Tool 1.2.1 |

AccessData FTK Imager to compile the file tree that has been extracted from the smartphone and Hash Tool 1.2.1 to create a has value (keyword) that maintains the originality of the file.

## 3.3 Scenario

The case scenario is logging in using the perpetrator's original account with the username @karambiaaa0 and doing nothing, the account only serves as a marker in the case scenario. The next account that enters is the username @kell_1.3 simulating activities on the TikTok application such as using the feature of making SARA videos with content that vilifies a religion and uploading it. Next, send messages to @muhammadromi_0.1 with verbal harassment, then on the device used by the perpetrator the message is deleted with the intention of eliminating traces.

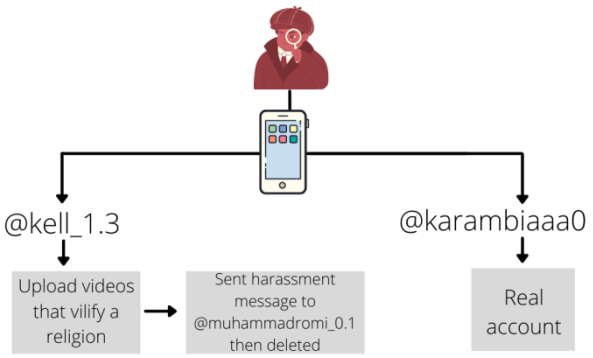


**Figure 2: Case simulation**

# 4. RESULT AND DISCUSSION

In this stage, the results and discussion of activities in the form of XML metadata on the TikTok application are generally stored in the com.ss.android.ugc.trill directory.

## 4.1 File XML Description Applications TikTok

Information that can be pulled from Figure 3 such as source value (start directory), source value name (application name), application size, first installation and application update.

```
<?xml version="1.0" encoding="UTF-8"
standalone="yes"?> <Appinfo type="Android">
<Name
sourceValue="nonLocalizedLabel">TikTok</Name>
<Package
sourceValue="packageName">com.ss.android.ugc.trill</
Package> <Version \
sourceValue="versionName">16.6.4</Version>
<AndroidValue
sourceValue="versionCode">160604</AndroidValue>
<AndroidValue
sourceValue="installLocation">/data/app/com.ss.android.u
gc.trill-
XIvUQzj2XjZaB6g4SibbXg==/base.apk</AndroidValue>
<AndroidValue
sourceValue="flags">953695812</AndroidValue>
<AndroidValue
sourceValue="packageSize">95208458</AndroidValue>
<AppSize sourceValue="codeSize">0</AppSize>
<DataSize sourceValue="dataSize">0</DataSize>
<CacheSize sourceValue="cacheSize">0</CacheSize>
<AndroidValue
sourceValue="derivedApplicationType">Regular
Application</AndroidValue>
<AndroidValue
sourceValue="firstInstallTime">20210219T073605Z</An
droidValue>
<AndroidValue
sourceValue="lastUpdateTime">20210219T073605Z</An
droidValue>
<AppDataPath>/data/data/com.ss.android.ugc.trill</AppDa
taPath>
<AndroidValue
sourceValue="installerPackageName">com.google.android
.packageinstaller</AndroidValue>

</Appinfo>
```

**Figure 3 Component XML structure about the TikTok App**

Components about the TikTok application can be found in the com.ss.android.ugc.trill directory, where the file name "description.info" is usually 4 KB in size and is second to last, the file type is "XML Document". Some information that can be obtained such as Application Size 95.8 MB, APK Verification Successful Yes, APK Verifications Schema 2, First Installed 2021-02-19 14:36:05 (UTC+7) and Last Update 2021-02-19 14:36: 05 (UTC+7).

The metadata element documents additional information about the app profile i.e. The app name using the code "Appinfo" can only be installed on Android with TikTok.

**Table 3. Display Application Description**

| Name | Information |
|---|---|
| Label Application | TikTok |
| Application Size | 95.8 MB |
| APK Verification Succesful | Yes |
| APK Verifications Schema | 2 |
| *First Installed* | 2021-02-19 14:36:05 (UTC+7) |
| *Last Update* | 2021-02-19 14:36:05 (UTC+7) |

## 4.2 File XML Description Video TikTok

Uploaded Video activity is logged and can be viewed in the aweme_local_video.xml

<?xml version="1.0" encoding="UTF-8" standalone="true"?>-<map> <string name="extra_data">{"6930877942188788994":{"local_path":"/data/user/0/com.ss.android.ugc.trill/files/synthetise_2021-02-19-144205227-concat v","author_id":"6930551655360414721","create_time":185068285,"duration":8006.0,"is_h265":false,"m_vr":false,"ratio_uri":"v07025e80000c0nmpcbrgkfme10fb8o0_h264_540p_3922628","source_id":"6930877942188788994","height":960,"data_size":0,"uri":"v07025e80000c0nmpcbrgkfme10fb8o0_h264_540p_3922628","width":544},"6930882230294220033}</string></map>

**Figure 4. Video activity XML structure**

XML file, the information provided is very significant. Starting from the saved video location "com.ss.android.ugc.trill/files/", video name "synthetise_2021-02-19-144205227-concat v", creation time "185068285".

The video uploaded by the @kell_1.3 account is recorded with the ID "6930551655360414721" and the video has a duration of "8006.0" or about 8 seconds.

**Table 4. Video information display.**

| Name | Information |
|---|---|
| Video Location | com.ss.android.ugc.trill/files/ |
| Video Name | synthetise_2021-02-19-144205227-concat v |
| Created Time | 185068285 |
| Account | @Kell_1.3 |
| ID | 6930551655360414721 |

## 4.3 File XML Description User

Account @karambiaaa0 that has been used and stored in aweme_user.xml with the description name "6896333489403724802", short name "karambia aa", unique id "karambiaaa0, avatar URL https://p16-sign-sg.tiktokcdn.com/aweme/100x100 /tiktok-obj/1683676134080514.webp.

<string name="6896333489403724802_significant_user_info">{"uid":"6896333489403724802","short_id":"0","unique_id":"karambiaaa0","nickname":"karambia aa","avatar_url":"https://p16-sign-sg.tiktokcdn.com/aweme/100x100/tiktok-obj/1683676134080514.webp?x-expires\u003d1613808000\u0026x-signature\u003dF%2FGeSW6ybEsY4xWFfRpPO%2FpTrDA%3D"}</string>

</string><string name="6930551655360414721_significant_user_info">{"uid":"6930551655360414721","short_id":"0","unique_id":"kell_1.3","nickname":"Kell_1.3","avatar_url":"https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_100x100.webp?x-expires\u003d1613808000\u0026x-signature\u003dXopf2O0xFqJDb3RLUwvmOywUBWo%3D"}</string><string name="6930551655360414721_aweme_user_info">{"accept_private_policy":false,"account_region":"","account_type":0,"allowStatus":0,"authority_status":0,"avatar_larger":{"height":0,"data_size":0,"uri":"musically-maliva-obj/1594805258216454","url_list":["https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_1080x1080.webp?x-expires\u003d1613808000\u0026x-signature\u003dre3HHNF98wm%2FUaZHqr9hxiZmlIQ%3D","https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_1080x1080.jpeg?x-expires\u003d1613808000\u0026x-signature\u003dN6F6L4RMeVUudzGgMVt5Ggst54U%3D"],"width":0},"avatar_medium":{"height":0,"data_size":0,"uri":"musically-maliva-obj/1594805258216454","url_list":["https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_720x720.webp?x-expires\u003d1613808000\u0026x-signature\u003djxf5GmoA8E25TbYGHNrbb2MI5pA%3D",https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_720x720.jpeg?x-expires\u003d1613808000\u0026x-signature\u003dKX0OLuMzf5w6qu6GspVWDTvI27M%3D}}</string>

**Figure 5. @Kell_1.3 account XML structure**

The @kell_1.3 account is the one who uploaded the SARA video. The information that can be retrieved from the aweme_user.xml file is quite complete in the account description section, such as UID "6930551655360414721", short_id "0", unique_id "kell_1.3", short name "Kell_1.3",

avatar_url "https://p16-sign-sg.tiktokcdn.com/aweme/100x100/tiktok-obj/1683676134080514.webp". Login activity was seen eight times on the app for all accounts while it was operating on account @kell_1.3, recorded with login number 1594805258216454 then re-entered at the same avatar address https://p16-sign-sg.tiktokcdn.com/musically-maliva -obj/1594805258216454~c5_1080x1080.jpeg?x-expires\u003d1613808000\u0026x-signature\u003dN6F6L4RMeVUudzGgMVt5Ggst54U%3D.

**Table 5. Display of user information.**

| Name | Information |
|---|---|
| ID | 6930551655360414721<br>6896333489403724802 |
| unique_id | kell_1.3 dan karambiaaa0 |
| Nick Name | Kell_1.3 dan karambia aa |
| avatar_url | https://p16-sign-sg.tiktokcdn.com/aweme/100x100/tiktok-obj/1683676134080514.webp |
| Sign Number | 1594805258216454 |

## 4.4 File XML Description Login

Additional login information is located in LoginSharePreferences.xml.

<?xml version="1.0" encoding="UTF-8" standalone="true"?> -<map> <string name="latest_login_info">[{"name":"kell0000011@gmail.com","commonUserInfo":{"avatarUrl":"https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_100x100.webp?x-expires\u003d1613808000\u0026x-signature\u003dXopf2O0xFqJDb3RLUwvmOywUBWo%3D","secUid":"MS4wLjABAAAAKrnEpz3gQIsda93DwsYtMpaltqZCVfpmom8z-PaLswRt2nwHNtlYQgCvQ_6g3Ve3","userName":"Kell_1.3"},"expires":"Mar 21, 2021 2:38:47 PM","lastActiveTime":-1,"loginMethodName":"EMAIL_PASS","loginTime":1613720327000,"uid":"6930551655360414721"}]</string></map>

**Figure 6. XML structure at login**

Account @kell_1.3 login using "EMAIL_PASS" method with email name "kell0000011@gmail.com", loginTime: "1613720327000" and ending on March 21, 2021 2:38:47 PM will be automatically logged out of the device.

**Table 6. Display of user login information**

| Name | Information |
|---|---|
| Account | @kell_1.3 |
| Login Method | EMAIL_PASS |
| Time Login | 1613720327000 |
| Automatic Out | Maret 21, 2021 2:38:47 |

## 4.5 File XML Description Version APP

**The TikTok application used has version 16.6.4.**

<?xml version="1.0" encoding="UTF-8" standalone="true"?>

-<map>

<string name="app_version">16.6.4</string>

</map>

**Figure 7. The XML structure of the TikTok app version.**

The version of the application used can be found in the XML version.xml file. located in the string name line followed by the version.

The easy way can be seen in table 7 which shows the version of the application used is 16.6.4 "

**Table 7. Display of Application Version Information**

| Name | Information |
|---|---|
| Application Version | 16.6.4 |

## 4.6 File Convert XML Message

Like other social media, TikTok can also exchange messages with the condition that the accounts are already following each other so that the status from "Following" to "Friends".

{"type":0,"isDefault":false,"text":"jelek Lo mirip banget aa monyet \ntolol bodoh eek kontol lo","is_card":false,"mSendStartTime":1613722263921,"msgHint":"","aweType":700}

**Figure 8. Visual XML message content**

Location of the message DB is in the live_data directory, usually each message DB will start with the sender's UID followed by _im reading with .db extension. In this case the UID of kell_1.3 is "6930551655360414721", so the file name is "6930551655360414721_im.db".

It should be noted, messages stored on smartphones in DB form are in JSON format and can be converted to XML visuals. The unique code "\n" indicates the next message in a newline state "enter" at the time of writing is then sent to the target.

**Table 8. Messages sent**

| Name | Information |
|---|---|
| 6930551655360414721 | Pesan "jelek Lo mirip banget aa monyet tolol bodoh eek kontol lo" |

## 4.7 ANALYSIS

There are more than 200 XML files but the directory location of the xml files which contain a lot of information of user activity is at applications0\com.ss.android.ugc.trill\live_data \shared_prefs. There are more than 100 xml files in

shared_prefs, the file that contains the most information is aweme_user.


**Figure 9. Directory User**

How it works is a collection of all accounts that are joined in one device, no new files will be created because each account will be recorded in the aweme_user file. per account is recorded based on the level of entry, the time displayed will be accumulated according to the line of code in Figure 5.

the total database that can be extracted is 69 items. but not all databases can provide information to investigators such as localHashTag.db, meta_log.db, psdkmon_v2.db, npth_log.db and others. Researchers have reviewed all files related to the .db extension. the most informative file for the message section is at 6930551655360414721_im.db


**Figure 10. Message Database**

The sent message will persist even if it is deleted in the application, the artifact can be found in the .db file. the functional part of the message in the application will not be visible the content sent. In conclusion, every message created will be directly recorded in the db file with the condition that when it has been sent.

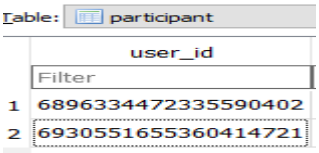


**Figure 11. UID who exchanged messages**

The UID "6930551655360414721" belongs to the kell_1.3 account and the message target has the UID "6896334472335590402" with the account name muhammadromi_0.1.

## 5. CONCLUSION

The results of this study found that each logged in account activity will be recorded in one file "aweme_user.xml", regardless of the number of accounts will be combined with the order of the entry code of each ID, application user information can be traced, requires extracting information from a total of 3260 files, the number of files is specific to the package on the TikTok application with the directory name :com.ss.android.ugc.trill". Information about the application being used is in two files "description.info and version". For XML files, there are 111 items. The files don't all have activity logs, filtering is needed to determine the relevant files, one static way is to read each line of code in the XML file. The location of the video directory can be found in the aweme_local_video.xml file, the video is saved simultaneously when uploading, the saved format does not include an extension in the file details, but judging by the 6D 70 34 signatures it is MP4, video artifacts can be played via media player software such as MPC -H or VLC.

## 6. REFERENCES

[1] C. Anglano, M. Canonico, and M. Guazzone, "The Android Forensics Automator (AnForA): A tool for the Automated Forensic Analysis of Android Applications," *Comput. Secur.*, vol. 88, 2020, doi: 10.1016/j.cose.2019.101650.

[2] D. Kim and S. Lee, "Study of identifying and managing the potential evidence for effective Android forensics," *Forensic Sci. Int. Digit. Investig.*, vol. 33, 2020, doi: 10.1016/j.fsidi.2019.200897.

[3] A. Ali and Fazeel, "Forensic examination of social networking applications on smartphones," *Proc. - 2015 Conf. Inf. Assur. Cyber Secur. CIACS 2015*, pp. 36–43, 2016, doi: 10.1109/CIACS.2015.7395564.

[4] E. Bresnick, "Intensified Play: Cinematic study of TikTok mobile app," *Univ. South. Calif.*, vol. 4, no. 4, pp. 1–12, 2019, [Online]. Available: https://www.researchgate.net/publication/335570557_Intensified_Play_Cinematic_study_of_TikTok_mobile_app.

[5] L. Xu, X. Yan, and Z. Zhang, "Research on the Causes of the 'Tik Tok' App Becoming Popular and the Existing Problems," *J. Adv. Manag. Sci.*, vol. 7, no. 2, pp. 59–63, 2019, doi: 10.18178/joams.7.2.59-63.

[6] G. Weimann and N. Masri, "Research Note: Spreading Hate on TikTok," *Stud. Confl. Terror.*, vol. 0, no. 0, pp. 1–14, 2020, doi: 10.1080/1057610X.2020.1780027.

[7] Y. Wang, "Humor and camera view on mobile short-form video apps influence user experience and technology-adoption intent, an example of TikTok (DouYin)," *Comput. Human Behav.*, vol. 110, no. November 2019, p. 106373, 2020, doi: 10.1016/j.chb.2020.106373.

[8] Z. Brahmia, H. Hamrouni, and R. Bouaziz, "XML data manipulation in conventional and temporal XML databases: A survey," *Comput. Sci. Rev.*, vol. 36, p. 100231, 2020, doi: 10.1016/j.cosrev.2020.100231.

[9] P. Cedillo, J. Camacho, K. Campos, and A. Bermeo, "A forensics activity logger to extract user activity from mobile devices," *2019 6th Int. Conf. eDemocracy eGovernment, ICEDEG 2019*, pp. 286–290, 2019, doi: 10.1109/ICEDEG.2019.8734298.

[10] A. Oliveira, T. Kohwalter, M. Kalinowski, L. Murta, and V. Braganholo, "XChange: A semantic diff approach for XML documents," *Inf. Syst.*, vol. 94, no. August, 2020, doi: 10.1016/j.is.2020.101610.

[11] N. Hoang Khoa, P. The Duy, H. Do Hoang, D. Thi Thu Hien, and V. H. Pham, "Forensic analysis of TikTok application to seek digital artifacts on Android smartphone," *Proc. - 2020 RIVF Int. Conf. Comput. Commun. Technol. RIVF 2020*, 2020, doi: 10.1109/RIVF48685.2020.9140739.

[12] I. Riadi, A. Yudhana, and M. C. F. Putra, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," *Sci. J. Informatics*, vol. 5, no. 2, pp. 235–247, 2018, doi: 10.15294/sji.v5i2.16545.

[13] R. Ayers, W. Jansen, and S. Brothers, "Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1)," *NIST Spec. Publ.*, vol. 1, no. 1, p. 85, 2014, [Online]. Available:

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf.

[14] F. Norouzizadeh Dezfouli, A. Dehghantanha, B. Eterovic-Soric, and K. K. R. Choo, "Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms," *Aust. J. Forensic Sci.*, vol. 48, no. 4, pp. 469–488, 2016, doi: 10.1080/00450618.2015.1066854.

[15] T. Laurenson, S. MacDonell, and H. Wolfe, "Towards a standardised strategy to collect and distribute application software artifacts," *Aust. Digit. Forensics Conf. ADF 2015*, vol. 2015, pp. 54–61, 2015, doi: 10.4225/75/57b3f5cffb889.