Data Search for Pornographic Content on Twitter Services using National Institute of Standard and Technology (NIST) Method

Vioni Retno Gita Leri
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT

The development of mobile device technology, especially on social media to interact with two or more people, has become a necessity that cannot be separated from daily life. Twitter is an online social networking and microblogging service that allows its users to send and read text-based messages,Twitter is currently experiencing rapid growth and is popular throughout the world, due to its high popularity, Twitter is often used for various purposes at this time Twitter is the social media with the highest pornographic content contributor. This study will scenario the crime case using the Twitter application that runs on application mobile using the NIST stages related to the topic of cyberporn distribution. The stages of theforensics National Institute of Standards and Technology (NIST)are collection, examination, analysis, and reporting. This study uses a smartphone with a rooted condition and the Twitter application is installed. The crime case scenario in cyberporn this research is the distribution of pornographic content on Twitter based on examples of existing cases. The process of collecting digital evidence through the Twitter API and using two forensic tools, namely MOBILedit forensic express and SQLite. This study produces digital evidence in the form of account information, posts or tweets that have been deleted including text, images and videos from smartphone a rooted.The results of the evidence obtained will be given to the court if needed, to assist in the law enforcement process to uncover digital crime cases.

Keywords

Forensics, Cellular, Twitter, Cyberporn, NIST

1. INTRODUCTION

The development of information technology, especially social media which is used to interact with two or more people, done online has become a necessity that cannot be separated from everyday life.One of the social media that is often used by the public is Twitter [1]. In cyberspace, it is not possible to regulate someone to post or publish content, but content that is harmful or contains something that can trigger public unrest can be reported, people who are restless and feel aggrieved by posts that are spread, report to the authorities. Many examples of cases that are often reported such as pornography, cyberbullying, defamation, fraud and many more cases of crime in cyberspace. Computer crime is a crime whose traces of criminal activity need to be analyzed to become evidence [2]. Such crimes can be uncovered with the help of digital forensics. One of the steps to assist investigators in conducting digital forensics is the NIST stage. The NIST stage is used to obtain information from digital evidence [3]. There are several stages in the NIST method, namely collection, examination, analysis, and reporting [4].

1.1 Study Literature

1.1.1 Previous Study

Rusydi and Sahiruddin (2019) has conducted a digital forensic research entitled "NIST Method for Forensic Analysis of Digital Evidence on Android Devices".In this study, it describes the forensic process that is running to get back digital evidence in the form of deleted data on ansmartphone androidusing the Wondershare dr. Fone for Android, Oxygen Forensic Suite 2014 to prove crimes at trial. It can be concluded: to find digital evidence in the form of contact data, logs call, and messages that have been deleted on thesmartphone, Samsung Galaxy J1 Aceit can be concluded that recovery with the Wondershare tool only reaches 30%, while the results of recovery with Oxygen forensics reach 73% of deleted data. can be returned. Therefore, the data recovered from digital evidence with thetool is Oxygenhighly recommended as evidence in proving criminal cases in court. [5].

Ermadi Satriya Wijaya and Teguh Subagyo (2017) have conducted a digital forensic research entitled "Analysis of Digital Evidence on Random Access Memory AndroidUsingMethods in Live Forensic Child Abduction Cases", it can be concluded: this study scenarios the process of disclosing digital evidence in child abduction cases. , in the process of proving this research managed to find digital evidence in the form of pictures sent by the perpetrator, previously deleted text messages and log files of incoming calls on the victim's smartphone and log file of outgoing calls on thesmartphone perpetrator's, but there were some data that could not be found such as time and voice calls [6].

Fadillah, Noor, Umar, and Yudhana (2018) have conducted a digital forensic research entitled "The Design of the NIST Method for Forensic Mobile Payment Android-BasedApplications". This research can be concluded that the process of removing digital evidence from a smartphone that has aapplication installed mobile payment requires rooting for ansmartphone Android, and there are many tools that can be used in the process of removing digital evidence that runs on the Windows platform. [7].

Prasongko, Yudhana, and Fadil (2018) have conducted a digital forensic research entitled"Forensic Analysis of Kakaotalk Applications Using the NIST Method". In this study, conclusions can be drawn: This study uses the NIST Mobile Forensic method and research tools to perform forensic analysis on the KakaoTalk application. During the process of removing digital evidence from KakaoTalk, rooting for Android smartphones is required. Digital evidence is expected from the appointment process and forensic analysis can help the process of investigating a digital crime [8].

Imam and Nurhairani (2019) have conducted digital forensic research entitled “Analysis of Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method. This study discusses the Twitter application for handling cybercrime containing hate speech in direct messengers or secret chats, the conclusions obtained are: the results of forensic evidence research obtained using the stages of the method NIJ, identification, collection, examination, analysis, reports using smartphone rooted with DB Browser for SQLite, SQLite Manager, Root Explorer, evidence that can be found 2 user participants, 3messages chat and 1 picture, location, and profile of the perpetrator while a smartphone with condition non-root only gets 1 file APK[9].

1.1.2 Digital Forensics

Digital forensics is the science of identifying evidence from digital sources and provides forensic experts with powerful tools and techniques to solve complex digital-related crimes [10]. Digital Forensics is also a science computertechnology, for proving a crime - a high-tech [11].Forensic methods are an important factor that supports a more effective and efficient crime investigation in handling a case [12]. The purpose of forensics is to obtain the value of evidence. Digital or electronic evidence consists of information and value data stored or transmitted by digital devices [13].

1.1.3 Mobile Application

application mobile comes from two words, and applications. mobile terms, an application is a ready-made program that is made to carry out a function for another user or application, while mobile is a movement from one place to another [14]. applications Mobile are software that runs on devices mobile such as smartphones or Tablet PCs.applications are Mobile also known as applications that can be downloaded and have certain functions that add to the functionality of the device mobile itself, to get mobile application the desired, users can download it through certain sites according to their operating systems such as Google Play and iTunes.

1.1.4 Digital Evidence

evidence is generally related to digital crimes such as crimes that use social media as a place to commit crimes, so digital evidence is used to assist in prosecuting all types of digital crimes [15]. Digital evidence is included in Law no. 11 of 2008 concerning Information and Electronic Transactions. Digital evidence is so susceptible to alteration that it can affect its authenticity if not handled properly. Any kind of alteration that contains digital evidence will lead to wrong conclusions, or the evidence will be useless [16]. Digital evidence requires a standardized and formalized process so that digital evidence can be accepted during the trial process [17].Digital evidence is divided into 15 types, namely logical files, encrypted audio files,deleted files, video files, emails,images files, user id / password, etc [18].

1.1.5 Twitter

Twitter is a social networking service as well as microblog online, Twitter is a medium of communication, information, news, motivation, business, media for driving and influencing the masses, entertainment media in spare time, and honing writing skills. On Twitter users can also upload other media besides text such as images and videos called tweet pic [19]. Tweets themselves can consist of messages, text, and photos. Apart from that, tocompose messages based on topic users can also use the # sign (hashtag) [20].The Twitter service also provides a Twitter API which is used to get information. API stands for Application Programming Interface, API allows users to manage Twitter information that users have previously been allowed to do.

1.1.6 Cybercrime

Cybercrime is a crime that uses information technology as a crime target, and digital forensics is basically, answering the questions: when, what, who, where, how, and why related to digital crime. The misuse of social media and instant messaging in mobile services allows cybercriminals to take advantage of these services for malicious purposes [21]. There are many types of cybercrime: one example is cyber pornography, the term refers to the use of information technology to create, display, distribute, publish pornography and obscene material in the form of text, photos, and videos.

1.1.7 National Institute of Standard Technology

This is a forensic stage that has policy work guidelines and standards to ensure each examiner follows the same workflow so that work is documented and the results can be repeated and can be maintained, this stage will assist investigators in conducting digital forensics. The stages in NIST are collection, examination, analysis, and reporting [22]. The stages can be seen in Figure 1.

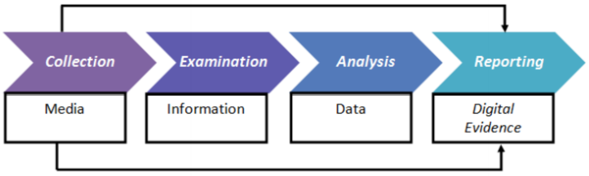


Figure 1. The stages of NIST

1. Collection
   Collection is labeling, identification, recording, and retrieval of data from relevant data sources with the following procedures to maintain data integrity.
2. Examination
   Examination is a process to protect evidence from damage and alteration by parties who are not responsible for the process collection in collecting electronic evidence and analyzing electronic data by forensic experts.
3. Analysis
   Analysis is the analysis of the results of the examination using technically justified methods and the law.
4. Reporting
   Reporting is reporting the results of the analysis which includes the description of the actions taken.

1.1.8 Pornography

Pornography is all forms of audio, visual, and audio-visual material that is in a sexual context in the form of writing, pictures, video shows that focus on the genitals and sexual behavior for sexual gratification and pleasure. One factor in the development of the spread of pornographic content is the increasingly advanced technology, especially the internet [23]. Based on the Law of theIndonesia number 44 of 2008 concerning pornography, it is stated in article 1 paragraph 1 that pornography is pictures, sketches, illustrations, photos, writings, sounds, sounds, moving images, animations, cartoons, conversations, gestures, or other forms of messages. through various forms of communication media or public performances, which contain obscenity or sexual exploitation that violates the norms of decency in the society.

2. METHODOLOGY

2.1 Research Scenario

This scenario is created to explain how the stages of the mobile application forensic process will be carried out. The case scenario in this research is the spread of pornographic content on Twitter using a smartphone, so that on Twitter, many quick views, comments, and even re-post the tweet retweeting or commonly known as. The video is being seen and distributed more and more, people who feel restless or feel aggrieved by this report to the authorities, after the user or account owner finds out that the video is viral, the user intentionally deletes his post on Twitter to eliminate evidence.

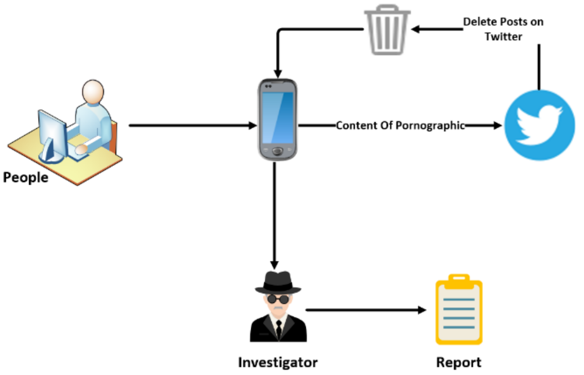


Figure 2. Simulation of the Research Scenario

Figure 2 explains after the suspect is caught, evidence will be confiscated in the form of a smartphone suspected of spreading pornographic content to Twitter, then it will be handed over to the Investigator team to investigate the case by investigating the perpetrator's smartphone.

The investigator process will collect digital evidence through the Twitter API and carry out a forensic process using forensic tools that have been prepared previously to obtain digital evidence. The results of the evidence obtained will be given to the court if needed.

2.2 Research Stages

The NIST forensic stage is a forensic stage that has policy work guidelines and standards to ensure each investigator follows the same workflow so that work is documented and the results obtained can be repeated and can be maintained. At this stage, the investigator team conducts an investigation process to obtain information. The stages or methods used to obtain digital evidence include collection, examination, analysis, and reporting.

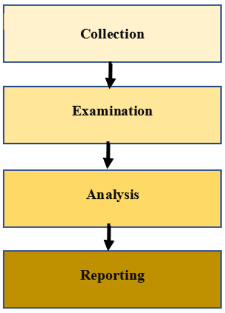


Figure 3. Stages of Research Implementation

In Figure 3 are the stages of NIST implementation. This investigative model is used to find digital evidence to find evidence facts cyberporn that occurs on the Twitter application. The steps that will be taken by the investigator team in finding and collecting digital evidence are explained as follows:

2.2.1 Collection

Collecting evidence from the Twitter API and through the R Studio application managed to get Twitter data in CSV format. Other evidence that was successfully obtained was a smartphone, as can be seen in Table 1.

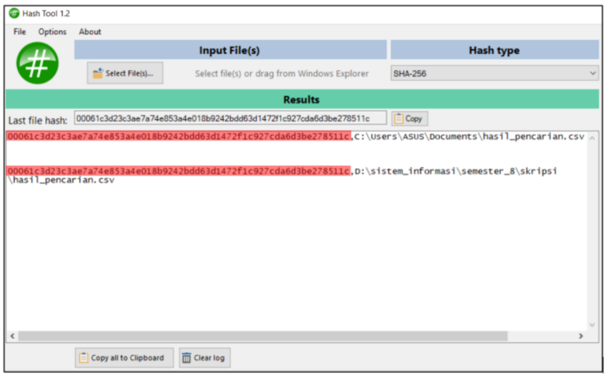
Table 1. Physical Evidence Found

No.	Name	Image	Description
1	The smartphone perpetrator's , front view of the		Samsung Galaxy Grand Prime brand, is on, connected to the network, and in a root state
2	Smartphone behind-the-scenes		

The evidence collected will be subject to an acquisition process to view and search for digital evidence on data smartphone stored in the database smartphone.

2.2.2 Examination

At this stage the process of transferring or retrieving information obtained from the smartphone perpetrators and maintaining the authenticity and integrity of the data. The way to protect digital evidence is by hashing electronic data that has been successfully backed up. The initial hashing results and the final hashing results will be matched to determine the authenticity of the data from the digital evidence obtained. The process of hashing the file CSV from the Twitter API, software MOBILedit, and SQlite using the software tool, the first process step is to copy the original folder from the backup data.



Hash type: SHA-256

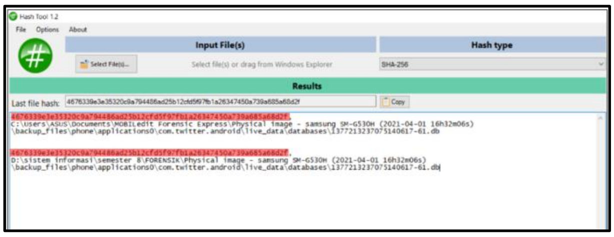
Last file hash: 00061c3d23c3ae7a74e853a4e018b9242bdd63d1472f1c927cda6d3be278511c

```
00061c3d23c3ae7a74e853a4e018b9242bdd63d1472f1c927cda6d3be278511c,C:\Users\ASUS\Documents\hasil_pencarian.csv

00061c3d23c3ae7a74e853a4e018b9242bdd63d1472f1c927cda6d3be278511c,D:\sistem_informasi\semester_8\skripsi
\hasil_pencarian.csv
```

Figure 4. Twitter API File Hashing Results

Figure 4 is the display of hashing results on the Twitter API file, the red color shows the encryption code file Twitter API, from the row of words the encryption code remains the same, which means that no data changes have occurred.



Last file hash: 4676339e3e35320c9a794486ad25b12cfd5f97fb1a26347450a739a685a68d2f

```
4676339e3e35320c9a794486ad25b12cfd5f97fb1a26347450a739a685a68d2f,
C:\Users\ASUS\Documents\MOBILedit Forensic Express\Physical image - samsung SM-G530H (2021-04-01 16h32m06s)
\backup_files\phone\applications0\com.twitter.android\live_data\databases\1377213237075140617-61.db

4676339e3e35320c9a794486ad25b12cfd5f97fb1a26347450a739a685a68d2f,
D:\sistem informasi\semester 8\FORENSIK\Physical image - samsung SM-G530H (2021-04-01 16h32m06s)
\backup_files\phone\applications0\com.twitter.android\live_data\databases\1377213237075140617-61.db
```

Figure 5. Results of HashingData Backup Files Smartphone

Figure 5 shows the results of hashing the backup data from MOBILedit, the red color shows the file encryption code, from the row of words the encryption code remains the same meaning no data changes have occurred.

2.2.3 *Analysis*

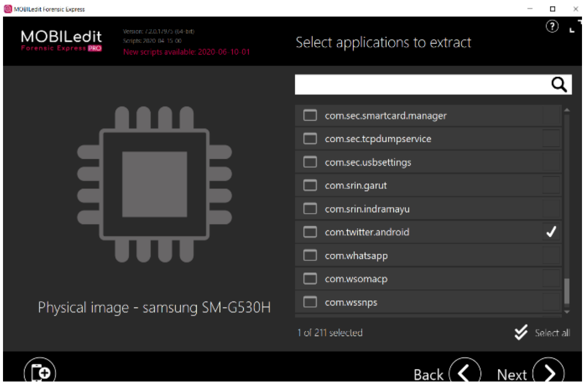
The analysis, the stage is the process of searching for information in the form of digital evidence from data extracted from the Twitter API and acquisitions smartphone previous. The information sought is account information, tweets that have been deleted in the form of text, images, and videos. Analysis of the results of the examination using the Twitter API and forensic tools MOBILedit forensic express, and SysTools SQLite Viewer.

2.2.3.1 Twitter API

Limitations of using the Twitter API if the investigation team collects data for more than one week from the user posting tweets then the evidence data cannot be found due to limited access and if the user has deleted the tweets on his Twitter account then the investigation team cannot find digital evidence in Twitter API, because the simulation case in this study tells about a user intentionally uploading or distributing pornographic content to Twitter and intentionally deleting the content because the content has gone viral and was reported by the public, therefore collecting evidence from the Twitter API is not prioritized.

2.2.3.2 MOBILedit Forensic

The data acquisition process begins by analyzing the previously created image. Twitter application options will appear, as in the existing application options.

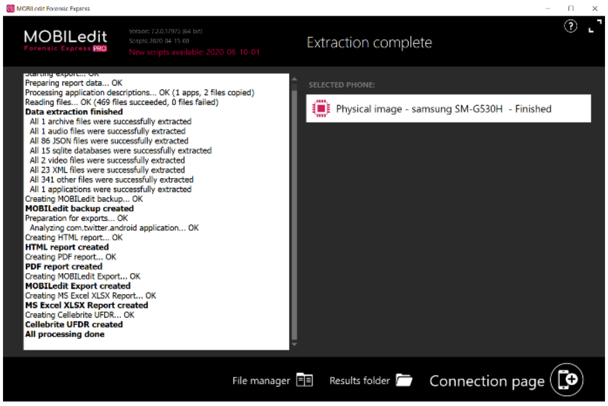

MOBILedit Forensic Express
MOBILedit
Forensic Express PRO
Version: 7.2.0.17975 (64 bit)
Scripts: 2020 04 15 00
New scripts available: 2020 06 10 01
Select applications to extract
Physical image - samsung SM-G530H
Back
Next
Select all

□ com.sec.smartcard.manager
□ com.sec.tcpdumpservice
□ com.sec.usbsettings
□ com.srin.garut
□ com.srin.indramayu
□ com.twitter.android ✓
□ com.whatsapp
□ com.wsomacp
□ com.wssnps

1 of 211 selected

Figure 6. Application List Display on File Image

Figure 6 is a list of applications from which the then investigator selects the Twitter application to extract data, the Twitter application is stored in the com.twitter.android directory and performs data extraction.


MOBILedit Forensic Express
MOBILedit
Forensic Express PRO
Version: 7.2.0.17975 (64 bit)
Scripts: 2020 04 15 00
New scripts available: 2020 06 10 01
Extraction complete
SELECTED PHONE:
Physical image - samsung SM-G530H - Finished
File manager
Results folder
Connection page

```
Starting export... OK
Preparing report data... OK
Processing application descriptions... OK (1 apps, 2 files copied)
Reading files... OK (469 files succeeded, 0 files failed)
Data extraction finished
  All 1 archive files were successfully extracted
  All 1 audio files were successfully extracted
  All 86 JSON files were successfully extracted
  All 15 sqlite databases were successfully extracted
  All 2 video files were successfully extracted
  All 23 XML files were successfully extracted
  All 341 other files were successfully extracted
  All 1 applications were successfully extracted
Creating MOBILedit backup... OK
MOBILedit backup created
Preparation for exports... OK
  Analyzing com.twitter.android application... OK
Creating HTML report... OK
HTML report created
Creating PDF report... OK
PDF report created
Creating MOBILedit Export... OK
MOBILedit Export created
Creating MS Excel XLSX Report... OK
MS Excel XLSX Report created
Creating Cellebrite UFDR... OK
Cellebrite UFDR created
All processing done
```

Figure 7. Display of the Data Extraction Process

Figure 7 the display of the data extraction process for the Twitter application installed on the smartphone. The results of data extraction on the smartphone will be stored automatically in the form of reporting or reports.

2.2.3.3 SysTools SQLite Viewer

Stages of the analysis process to find and obtain digital evidence stored in the smartphone database perpetrators using the SysTools SQLite Viewer tool. In the initial screen select the open database, open the database with the name 1377213237075140617-61.db then open the browse data menu, in the table column select the users table which includes id, user_id, username, name, image_url, user flags, friendship, friendship_time, header_url, description, location, url_entities, web_url, link_, fast_followers, friends, statuses, favorites, media_, updated, and others whose more complete details can be seen in the image below.

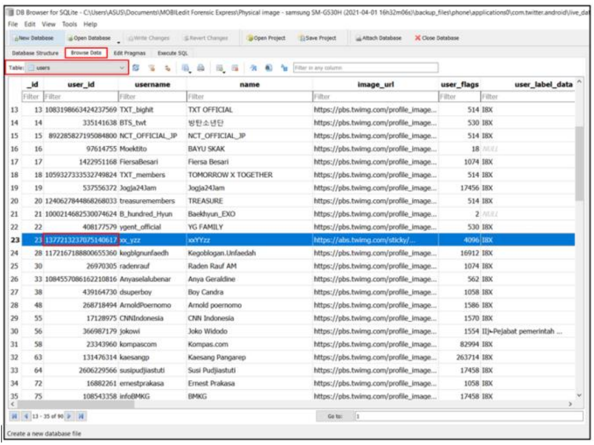

DB Browser for SQLite - C:\Users\ASUS\Documents\MOBILedit Forensic Express\Physical image - samsung SM-G530H (2021-04-01 16h32m06s)\backup_files\phone\applications0\com.twitter.android\live_da
File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Open Project
Save Project
Attach Database
Close Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Filter in any column
Go to:
Create a new database file

Table: users

	_id	user_id	username	name	image_url	user_flags	user_label_data
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
13	13	1083198663424237569	TXT_bighit	TXT OFFICIAL	https://pbs.twimg.com/profile_image...	514	I8X
14	14	335141638	BTS_twt	방탄소년단	https://pbs.twimg.com/profile_image...	530	I8X
15	15	892285827195084800	NCT_OFFICIAL_JP	NCT_OFFICIAL_JP	https://pbs.twimg.com/profile_image...	514	I8X
16	16	97614755	Moektito	BAYU SKAK	https://pbs.twimg.com/profile_image...	18	NULL
17	17	1422951168	FiersaBesari	Fiersa Besari	https://pbs.twimg.com/profile_image...	1074	I8X
18	18	1059327333532749824	TXT_members	TOMORROW X TOGETHER	https://pbs.twimg.com/profile_image...	514	I8X
19	19	537556372	Jogja24Jam	Jogja24Jam	https://pbs.twimg.com/profile_image...	17456	I8X
20	20	1240627844868268033	treasuremembers	TREASURE	https://pbs.twimg.com/profile_image...	514	I8X
21	21	1000214682530074624	B_hundred_Hyun	Baekhyun_EXO	https://pbs.twimg.com/profile_image...	2	NULL
22	22	408177579	ygent_official	YG FAMILY	https://pbs.twimg.com/profile_image...	530	I8X
23	23	1377213237075140617	xx_yzz	xxYYzz	https://abs.twimg.com/sticky/...	4096	I8X
24	28	1172167188800655360	kegblgnunfaedh	Kegoblogan.Unfaedah	https://pbs.twimg.com/profile_image...	16912	I8X
25	30	26970305	radenrauf	Raden Rauf AM	https://pbs.twimg.com/profile_image...	1074	I8X
26	33	1084557086162210816	Anyaselalubenar	Anya Geraldine	https://pbs.twimg.com/profile_image...	562	I8X
27	38	439164730	dsuperboy	Boy Candra	https://pbs.twimg.com/profile_image...	1058	I8X
28	48	268718494	ArnoldPoernomo	Arnold poernomo	https://pbs.twimg.com/profile_image...	1586	I8X
29	55	17128975	CNNIndonesia	CNN Indonesia	https://pbs.twimg.com/profile_image...	1570	I8X
30	56	366987179	jokowi	Joko Widodo	https://pbs.twimg.com/profile_image...	1554	I lj•Pejabat pemerintah ...
31	58	23343960	kompascom	Kompas.com	https://pbs.twimg.com/profile_image...	82994	I8X
32	63	131476314	kaesangp	Kaesang Pangarep	https://pbs.twimg.com/profile_image...	263714	I8X
33	64	2606229566	susipudjiastuti	Susi Pudjiastuti	https://pbs.twimg.com/profile_image...	17458	I8X
34	72	16882261	ernestprakasa	Ernest Prakasa	https://pbs.twimg.com/profile_image...	1058	I8X
35	75	108543358	infoBMKG	BMKG	https://pbs.twimg.com/profile_image...	17458	I8X

13 - 35 of 90

Go to: 1

Figure 8. Display of User Results Table

Figure 8 is the results of Table users, there are names of Twitter users stored in the database, one of which is a Twitter account that posts pornographic content to Twitter.

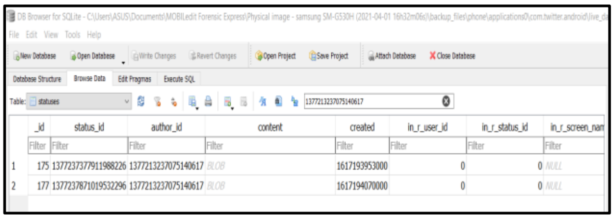

DB Browser for SQLite - C:\Users\ASUS\Documents\MOBILedit Forensic Express\Physical image - samsung SM-G530H (2021-04-01 16h32m06s)\backup_files\phone\applications0\com.twitter.android\live_da
File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Open Project
Save Project
Attach Database
Close Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL

Table: statuses

1377213237075140617

	_id	status_id	author_id	content	created	in_r_user_id	in_r_status_id	in_r_screen_nam
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	175	1377237377911988226	1377213237075140617	BLOB	1617193953000	0	0	NULL
2	177	1377237871019532296	1377213237075140617	BLOB	1617194070000	0	0	NULL

Figure 9. Display of Statuses Table Results

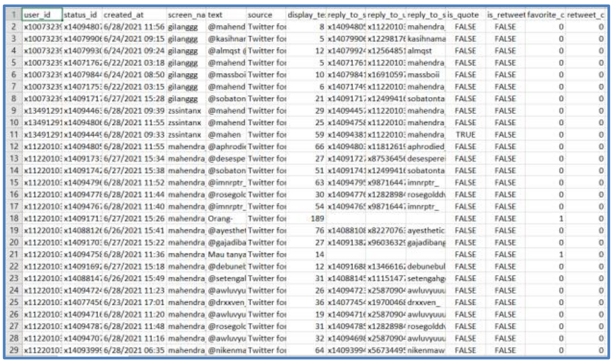
In Figure 9 are the results of TableStatuses, Statuses is the name of the table in the databases and there is evidence of posts from Twitter users who post pornographic content.

2.2.4 *Reporting*

Reporting is the final stage that aims to present the data from the analysis that has been found by the investigator. Reporting the results of searching for evidence from the software R Studio and collecting digital evidence from the tool MOBILedit forensic express and SysTools SQLite Viewer

2.2.4.1 Twitter API

Reporting results from the Twitter API directly occurs feature extraction (Tokenizing, Filtering, Stemming, Tagging) through R Studio software which produces CSV files which can be seen in Figure 10.



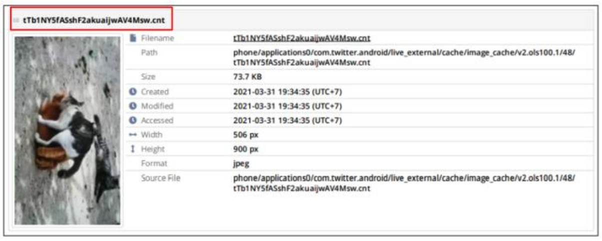
1	user_id	status_id	created_at	screen_na	text	source	display_te	reply_to_s	reply_to_u	reply_to_s	is_quote	is_retweet	favorite_c	retweet_c
2	x10073239	x14094807	6/28/2021 11:56	gilanggg	@mahend	Twitter fo	8	x14094805	x11220103	mahendra_	FALSE	FALSE	0	0
3	x10073239	x14079906	6/24/2021 09:15	gilanggg	@kasihnar	Twitter fo	5	x14079906	x12298176	kasihnama	FALSE	FALSE	0	0
4	x10073239	x14079930	6/24/2021 09:24	gilanggg	@almqst (	Twitter fo	12	x14079924	x12564851	almqst	FALSE	FALSE	0	0
5	x10073239	x14071762	6/22/2021 03:18	gilanggg	@mahend	Twitter fo	5	x14071761	x11220103	mahendra_	FALSE	FALSE	0	0
6	x10073239	x14079844	6/24/2021 08:50	gilanggg	@massboi	Twitter fo	10	x14079841	x16910597	massboii	FALSE	FALSE	0	0
7	x10073239	x14071753	6/22/2021 03:15	gilanggg	@mahend	Twitter fo	6	x14071749	x11220103	mahendra_	FALSE	FALSE	0	0
8	x10073239	x14091717	6/27/2021 15:28	gilanggg	@sobaton	Twitter fo	21	x14091717	x12499416	sobatonta	FALSE	FALSE	0	0
9	x13491291	x14094463	6/28/2021 09:39	zssintanx	@mahend	Twitter fo	29	x14094457	x11220103	mahendra_	FALSE	FALSE	0	0
10	x13491291	x14094806	6/28/2021 11:55	zssintanx	@mahend	Twitter fo	25	x14094758	x11220103	mahendra_	FALSE	FALSE	0	0
11	x13491291	x14094445	6/28/2021 09:33	zssintanx	@mahen	Twitter fo	59	x14094381	x11220103	mahendra_	TRUE	FALSE	0	0
12	x11220103	x14094805	6/28/2021 11:55	mahendra_	@aphrodi	Twitter fo	66	x14094803	x11812615	aphrodied_	FALSE	FALSE	0	0
13	x11220103	x14091733	6/27/2021 15:34	mahendra_	@desespe	Twitter fo	27	x14091727	x87536456	desesperei	FALSE	FALSE	0	0
14	x11220103	x14091742	6/27/2021 15:38	mahendra_	@sobaton	Twitter fo	51	x14091741	x12499416	sobatonta	FALSE	FALSE	0	0
15	x11220103	x14094796	6/28/2021 11:52	mahendra_	@imnrptr_	Twitter fo	63	x14094795	x98716447	imnrptr_	FALSE	FALSE	0	0
16	x11220103	x14094778	6/28/2021 11:44	mahendra_	@rosegolc	Twitter fo	30	x14094776	x12828984	rosegolddy	FALSE	FALSE	0	0
17	x11220103	x14094767	6/28/2021 11:40	mahendra_	@imnrptr_	Twitter fo	54	x14094765	x98716447	imnrptr_	FALSE	FALSE	0	0
18	x11220103	x14091711	6/27/2021 15:26	mahendra_	Orang-	Twitter fo	189				FALSE	FALSE	1	0
19	x11220103	x14088126	6/26/2021 15:41	mahendra_	@ayesthet	Twitter fo	76	x14088108	x82270763	ayesthetic	FALSE	FALSE	0	0
20	x11220103	x14091703	6/27/2021 15:22	mahendra_	@gajadiba	Twitter fo	27	x14091382	x96036329	gajadibang	FALSE	FALSE	0	0
21	x11220103	x14094758	6/28/2021 11:36	mahendra_	Mau tanya	Twitter fo	14				FALSE	FALSE	1	0
22	x11220103	x14091692	6/27/2021 15:18	mahendra_	@debunet	Twitter fo	12	x14091688	x13466162	debunebul	FALSE	FALSE	0	0
23	x11220103	x14088147	6/26/2021 15:49	mahendra_	@setengal	Twitter fo	31	x14088145	x11151477	setengahg	FALSE	FALSE	0	0
24	x11220103	x14094724	6/28/2021 11:23	mahendra_	@awluvyu	Twitter fo	26	x14094723	x25870904	awluvyuuu	FALSE	FALSE	0	0
25	x11220103	x14077456	6/23/2021 17:01	mahendra_	@drxxven_	Twitter fo	36	x14077454	x19700468	drxxven_	FALSE	FALSE	0	0
26	x11220103	x14094716	6/28/2021 11:20	mahendra_	@awluvyu	Twitter fo	19	x14094716	x25870904	awluvyuuu	FALSE	FALSE	0	0
27	x11220103	x14094787	6/28/2021 11:48	mahendra_	@rosegolc	Twitter fo	31	x14094785	x12828984	rosegolddy	FALSE	FALSE	0	0
28	x11220103	x14094707	6/28/2021 11:16	mahendra_	@awluvyu	Twitter fo	32	x14094698	x25870904	awluvyuuu	FALSE	FALSE	0	0
29	x11220103	x14093999	6/28/2021 06:35	mahendra_	@nikenma	Twitter fo	64	x14093994	x56734495	nikenmaw	FALSE	FALSE	0	0

Figure 10. Results of extraction features through R Studio

It was explained in the case simulation that the perpetrator had deleted the post on his personal Twitter account, due to limitations using the Twitter API, so the investigation team did not find digital traces and even digital evidence in this data.

2.2.4.2 MOBILedit Forensic

The file report will be issued after the data extraction process is complete. The contents of the file reporting PDF form show information on device specifications smartphone account information user, and tweets that were deleted by the perpetrator and successfully recovered by the tool MOBILedit.

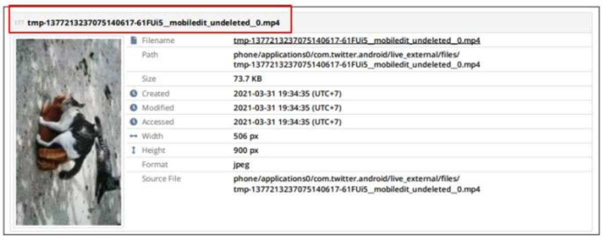


tTb1NY5fASshF2akuaijwAV4Msw.cnt

Filename	tTb1NY5fASshF2akuaijwAV4Msw.cnt
Path	phone/applications0/com.twitter.android/live_external/cache/image_cache/v2.ols100.1/48/ tTb1NY5fASshF2akuaijwAV4Msw.cnt
Size	73.7 KB
Created	2021-03-31 19:34:35 (UTC+7)
Modified	2021-03-31 19:34:35 (UTC+7)
Accessed	2021-03-31 19:34:35 (UTC+7)
Width	506 px
Height	900 px
Format	jpeg
Source File	phone/applications0/com.twitter.android/live_external/cache/image_cache/v2.ols100.1/48/ tTb1NY5fASshF2akuaijwAV4Msw.cnt

Figure 11. Deleted Image Files on Smartphone

Figure 11 is a deleted file image, there is some information such as filename, format, size, created, modified, accessed, width, height, and source files.



tmp-1377213237075140617-61FUi5_mobiledit_undeleted_0.mp4

Filename	tmp-1377213237075140617-61FUi5_mobiledit_undeleted_0.mp4
Path	phone/applications0/com.twitter.android/live_external/files/ tmp-1377213237075140617-61FUi5_mobiledit_undeleted_0.mp4
Size	73.7 KB
Created	2021-03-31 19:34:35 (UTC+7)
Modified	2021-03-31 19:34:35 (UTC+7)
Accessed	2021-03-31 19:34:35 (UTC+7)
Width	506 px
Height	900 px
Format	jpeg
Source File	phone/applications0/com.twitter.android/live_external/files/ tmp-1377213237075140617-61FUi5_mobiledit_undeleted_0.mp4

Figure 12. Deleted Video Files on Smartphone

Figure 12 is a deleted file video, there is some information such as filename, path, size, created, modified, accessed, width, height, and source file. There is a difference in the format file in the image above namely, file image with CNT format which means a file to help save different topics for help documents for Windows applications, because for case analysis this research uses a laptop with a Windows operating system, while the video format uses a Windows operating system. MP4 formats.

2.2.4.3 SysTools SQLite Viewer

The process for obtaining evidence by performing analysis stored in the database local smartphones. Figure 9 shows the results of the search the statuses table, when the column is contentclicked, the results will appear.

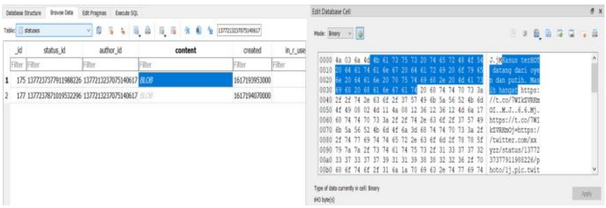


Table: statuses | 1377213237075140617

Mode: Binary

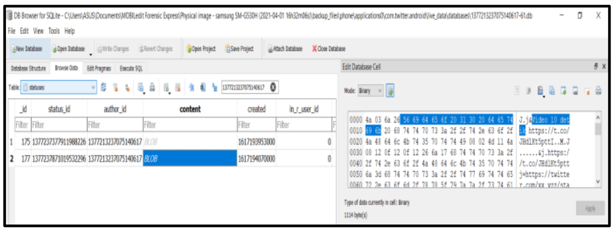
	_id	status_id	author_id	content	created	in_r_use
	Filter	Filter	Filter	Filter	Filter	Filter
1	175	1377237377911988226	1377213237075140617	BLOB	1617193953000	
2	177	1377237871019532296	1377213237075140617	BLOB	1617194070000	

```
0000 4a 03 6a 4d 4b 61 73 75 73 20 74 65 72 48 4f 54  J.jMKasus terHOT
0010 20 64 61 74 61 6e 67 20 64 61 72 69 20 6f 79 65   datang dari oye
0020 6e 20 64 61 6e 20 70 75 74 69 68 2e 20 4d 61 73  n dan putih. Mas
0030 69 68 20 68 61 6e 67 61 74 20 68 74 74 70 73 3a  ih hangat https:
0040 2f 2f 74 2e 63 6f 2f 37 57 49 6b 5a 56 52 4b 6d  //t.co/7WIkZVRKm
0050 4f 49 08 02 4d 11 4a 08 12 36 12 36 12 4d 6a 17  OI..M.J..6.6.Mj.
0060 68 74 74 70 73 3a 2f 2f 74 2e 63 6f 2f 37 57 49  https://t.co/7WI
0070 6b 5a 56 52 4b 6d 4f 6a 3d 68 74 74 70 73 3a 2f  kZVRKmOj=https:/
0080 2f 74 77 69 74 74 65 72 2e 63 6f 6d 2f 78 78 5f  /twitter.com/xx_
0090 79 7a 7a 2f 73 74 61 74 75 73 2f 31 33 37 37 32  yzz/status/13772
00a0 33 37 33 37 37 39 31 31 39 38 38 32 32 36 2f 70  37377911988226/p
00b0 68 6f 74 6f 2f 31 6a 1a 70 69 63 2e 74 77 69 74  hoto/1j.pic.twit
```

Type of data currently in cell: Binary
643 byte(s)

Figure 13. Results of Deleted Photo Tweets

Figure 13 shows the results of posting tweets deleted photo, data has been recovered in the form of proof of account information, profile photos, and image & video URLs along with the location of the folder that stores the data.



DB Browser for SQLite - C:\Users\ASUS\Documents\MOBILedit Forensic Express\Physical image - samsung SM-G530H (2021-04-01 16h32m06s)\backup_files\phone\applications0\com.twitter.android\live_data\databases\1377213237075140617-61.db

Table: statuses | 1377213237075140617

Mode: Binary

	_id	status_id	author_id	content	created	in_r_user_id
	Filter	Filter	Filter	Filter	Filter	Filter
1	175	1377237377911988226	1377213237075140617	BLOB	1617193953000	0
2	177	1377237871019532296	1377213237075140617	BLOB	1617194070000	0

```
0000 4a 03 6a 26 56 69 64 65 6f 20 31 30 20 64 65 74  J.j&Video 10 det
0010 69 6b 20 68 74 74 70 73 3a 2f 2f 74 2e 63 6f 2f  ik https://t.co/
0020 4a 48 64 6c 4b 74 35 70 74 74 49 08 02 4d 11 4a  JHdlKt5pttI..M.J
0030 08 12 0f 12 0f 12 26 6a 17 68 74 74 70 73 3a 2f  ......&j.https:/
0040 2f 74 2e 63 6f 2f 4a 48 64 6c 4b 74 35 70 74 74  /t.co/JHdlKt5ptt
0050 6a 3d 68 74 74 70 73 3a 2f 2f 74 77 69 74 74 65  j=https://twitte
0060 72 2e 63 6f 6d 2f 78 78 5f 79 7a 7a 2f 73 74 61  r.com/xx_yzz/sta
```

Type of data currently in cell: Binary
1134 byte(s)

Figure 14. Results of Deleted Video Tweets Posts

Figure 14 shows the results of posting tweets video that has been deleted, data has been recovered in the form of proof of account information, profile photos, and image & video URLs along with the location of the folder that stores the data. In the picture above is a data extraction process using binary data, and to make it easier to read the data is also provided in hexadecimal form.

2.2.5 *Results*

Tools are tools used to help obtain digital evidence. The evidence obtained from tools forensics can be seen from the comparison table below in Table 2.

Table 2. Comparison of Results obtained from Several Tools

Information	Data/Software/tools		
	Api Twitter / R Studio	*MOBILEdit forensic express*	*SysTools SQLite Viewer*
Recover deleted tweet data	×	✓	✓
Limited data taken	✓	×	×
Limited time for data collection	✓	×	×
Get account information after content is deleted	×	✓	✓

Based on the results of the comparison table above, it produces information to recover deleted tweets data by using 2 tools, namely MOBILedit and SQLite. Data retrieval is not possible from the Twitter API due to the limitations of the data taken and the limited time of data retrieval, to get account information after the content is deleted, you can use 2 forensic tools, namely MOBILedit and SQLite, while Twitter API cannot get information that has been deleted.

Table 3. The original evidence obtained

Name	The results found from the imaging data process				
	User Information	Text	Picture/ Photo	Videos	Profile Picture
Digital evidence obtained	✓	✓	✓	✓	✓

In table 3 is a record of digital evidence that was found, in the form of account information, text, photos, videos in tweets, and user profile photos.

3. CONCLUSION

Digital evidence can be found through the Twitter API to help collect digital evidence, but due to limited access, investigations through the Twitter API are not the main focus of searching and collecting evidence in this study. The collection of evidence is focused on the perpetrator's smartphone. Postings that have been deleted on the Twitter app can be restored after a process root on smartphones actors and process imaging smartphone using tools MOBILedit express forensic and seek evidence digital smartphone database using SysTools SQLite Viewer tool. The results of digital evidence found in the form of account information, posts, or tweets that have been deleted include text, images, and videos.

4. REFERENCES

[1] T. E. Damayanti, "Utilization of Twitter as Media Information Sharing in Libraries (Case Study About Utilization of Social Media Twitter as Media Information Sharing in Libraries of City 2Surabaya)."

[2] I. Riadi, S. Sunardi, and A. A. Kadim, "Monitoring of Mobile Native Application Logs Using the Grr Rapid Response Framework," *J. Buana Inform.*, vol. 10, no. 1, p. 1, 2019, doi:10.24002/jbi.v10i1.1909.

[3] D. Hariyadi, U. Jenderal, and A. Yani, "Identification of Conversation Evidence on the Dual Apps Whatsapp Application," no. November, 2018, doi:10.13140/RG.2.2.20253.56805.

[4] I. Riadi, R. Umar, and I. M. Nasrulloh, "Digital Forensic Analysis on Frozen Solid State Drives Using the National Institute of Justice (NIJ)," *MethodElinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.

[5] R. Umar and Sahiruddin, "Nist Method For Forensic Analysis of Digital Evidence On Android Devices," *Pros. SENDU_U_2019*, p. 978–979, 2019.

[6] E. S. Wijaya, "Analysis of Digital Evidence on Android Random Access Memory Using the Live Forensic Method of Child Abduction Cases," *Media Pratama Journal*, pp. 1–11, 2017.

[7] M. N. Fadillah, R. Umar, and A. Yudhana, "Design of the Nist Method for Forensic Android-Based Mobile Payment Applications," *Semin. Nas. Inform. 2018 (semnasIF 2018)*, vol. 2018, no. November, pp. 115–119, 2018, [Online] Available at: http://jurnal.upnyk.ac.id/index.php/semnasif/article/view/2626.

[8] R. Y. Prasongko, A. Yudhana, and A. Fadil, "Forensic analysis of the KakaoTalk application using national institute s method standard technology," *Semin. Nas. information. 2018 (semnasIF 2018) UPN "Veteran" Yogyakarta, 24 Novemb. 2018 ISSN 1979-2328*, vol. 2018, no. November, p. 129–133, 2018.

[9] H. Nurhairani and I. Riadi, "Analysis of Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method," *Int. J. Comput. app.*, vol. 177, no. 27, p. 35–42, 2019, doi:10.5120/ijca2019919749.

[10] B. Carrier, "Open {Source} {Digital} {Forensics} {Tools}: {The} {Legal} {Argument}," no. October, 2002.

[11] S. Pambayun dan I. Riadi, "Investigation on Instagram Android-based using Digital Forensics Research Workshop Framework," *Int. J. Comput. Appl.*, vol. 175, no. 35, hal. 15–21, 2020, doi: 10.5120/ijca2020920904.

[12] R. Umar, A. Yudhana, and M. Nur Faiz, "Performance Analysis of Live Forensics Methods for Random Access Memory Investigations in Proprietary Systems," *Pros. conf. Nas. The 4 Asos. program. Postgraduate. teacher. Muhammadiyah High*, no. June 2016, p. 207–211, 2016.

[13] R. Montasari, "Review and Assessment of the Existing Digital Forensic Investigation Process Models," Int. J. Comput. Appl., vol. 147, no. 7, pp. 1–9, 2016.

[14] Buyens, Jim. 2001. Web Database Development. Elex Media Komputindo. Jakarta

[15] I. Riadi, R. Umar, and A. Firdonsyah, "Identification of Digital Evidence on Android's Blackberry Messenger Using NIST Mobile Forensic Method," *Int. J. Comput. science. inf. Secur.*, vol. 15, no. 5, p. 3–8, 2017.

[16] I. Publication, "International Journal of Computer Science and Information Security (IJCSIS)," *Int. J. Comput. science. inf. Secur. IJCSIS*, vol. 9, no. 6, p. 355, 2011, [Online]. Available at: http://sites.google.com/site/ijcsis/.

[17] M. S. Ahmad, I. Riadi, and Y. Prayudi, "A Live Forensic Investigation from the User's Side to Analyze Man in the Middle Attack Attacks Based on Evil Twins," *Ilk. J. Ilm.*, vol. 9, no. 1, p. 1–8, 2017, doi:10.33096/ilkom.v9i1.103.1-8.

[18] T. Pandela and I. Riadi, "Browser Forensics on Webbased Tiktok Applications," 2020.

[19] P. W. Setyaningsih, Y. Prayudi, and B. Sugiantoro, "Management of Digital Evidence from the Acquisition of Dfxml," *J. Tek. information.*, vol. 11, no. 1, p. 47–54, 2018, doi:10.15408/jti.v11i1.6680.

[20] R. Saputra dan I. Riadi, "Forensic Browser of Twitter based on Web Services," *Int. J. Comput. Appl.*, vol. 175, no. 29, hal. 34–39, 2020, doi: 10.5120/ijca2020920832.

[21] M. N. Faiz, R. Umar, and A. Yudhana, "Analysis of Live Forensics for Comparison of Email Security on Proprietary Operating Systems," *Ilk. J. Ilm.*, vol. 8, no. 3, p. 242–247, 2016, doi:10.33096/ilkom.v8i3.79.242-247.

[22] A. Yudhana, I. Riadi, and I. Anshori, "Analysis of Digital Evidence for Facebook Messenger Using the Nist Method," *It J. Res. Dev.*, vol. 3, no. 1, p. 13–21, 2018, doi:10.25299/itjrd.2018.vol3(1).1658.

[23] Raka, Z. D, "4523/Kom-D/Sd-S1/2021 Analysis of P3Sps Violations on Bigo Live Application Shows," 2021.