International Journal of Artificial Intelligence Research
Vol 6, No 2, December 2022 ISSN: 2579-7298

Mobile Forensic Investigation of Fake News Cases on Instagram Applications with Digital Forensics Research Workshop Framework

Imam Riadi[a,1], Herman[b,2], Irhash Ainur Rafiq[b,3,*]

[a] *Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
[b] *Department of Informatic, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
[1]*imam.riadi@is.uad.ac.id;* [2] *hermankaha@mti.uad.ac.id;* [3] *irhash67@gmail.com*
* *corresponding author*

ARTICLE INFO

Article history:
Received 15 April 2022
Revised 05 May 2022
Accepted 30 June 2022

Keywords:
Instagram
Cybercrime
Fake News
Mobile Forensic
DFRWS

ABSTRACT

The number of digital crimes or cybercrimes today continues to increase every year, and lately a lot of it happens on social media like Instagram. The social behavior of today's people who communicate more through social media encourages the perpetrators of these digital crimes. Instagram is a social media that is often found content that contains elements of pornography, hoax news, hate speech, etc. This research is aimed at processing digital evidence of cases of the spread of hoax news on the Instagram application. This research follows the framework of the Digital Forensics Research Workshop (DFRWS) with six stages, namely identification, preservation, collection, examination, analysis and presentation. The process of obtaining digital evidence is assisted by the application of Axiom Magnet and Cellebrite UFED. Digital evidence sought from the smartphone device of the suspected hoax news disseminator seized following the case scenario consists of 8 variables in the form of accounts, emails, images, videos, urls, times, ip address and location. The results of this research with the help of the application of Magnet Axiom digital proof obtained by 87.5% and the Cellebrite UFED application of 68.75%. The results of this study show that Magnet Axiom have better performance than MOBILedit Forensics.

I. Introduction

Man is a creature that cannot live by depending on himself, according to his nature of always needing others therefore called a social being [1][2]–[3]. Social media is currently very popular among the public because of its rapid and varied development [4]. The development of social media has changed people's behavior patterns in socializing, such as the Instagram application that changes the pattern of entrepreneurs in promoting their business.

The development of social media also has a negative impact because many use it as a digital crime medium. Currently, human social behavior has begun to change due to the development of technology and the emergence of several social media applications such as Instagram which make it easier for humans to communicate remotely and more varied, not just exchanging messages but also being able to exchange pictures, videos, documents and voice calls and even group voice calls. The changes that occur can be seen in the patterns of socializing in society, usually if a person wants to communicate with others must be in a state of relationship or meeting, whereas now everyone can communicate from anywhere and anytime [5].

The influence of Instagram is not only on social behavior, but also business or trading behavior due to the global nature of Instagram so that what we upload to introduce our business can be seen by anyone and from anywhere [6]. With all the benefits obtained from Instagram there are some people who abuse it, leading to negative things and even criminals because it is easy to get the desired

information [7]. Digital crime or cybercrime is a criminal act whose practice utilizes cyberspace or digital, so that the evidence needed later in digital form is also [8].

Cybercrime is a crime that occurs in cyberspace or digitally [9]. Cybercrime actors in carrying out their actions use digital devices such as smartphones, laptops or PCs [10]. Cybercrime can happen anywhere and anytime, and can attack anyone [11]. In its legal handling cybercrime cases require digital evidence. The handling of cybercrime is not much different from other crimes, it's just that judges must be more careful in observing the evidence presented [12]. Mobile Forensic is a science used by investigators to obtain digital evidence [13][14]–[15]. Digital evidence is evidence obtained from cyber or digital, digital evidence can be in the form of images, videos, texts, voice messages and call records [3][12], [16]. Digital evidence must be in its original state in order to be used in legal proceedings, so as to obtain digital evidence using a special application. This study used Cellebrite UFED and Magnet Axiom. Mobile forensic is a branch of science of digital forensic that is suitable for returning digital evidence on mobile devices [17].

Mobile forensic can be used to search for digital evidence such as images, videos, text, deleted voice [18][19]–[21], mobile forensic is an illegitimate branch of digital forensic that focuses more on mobile devices or smartphones [22]. The digital evidence that can be obtained from this mobile forensic action can be in the form of images, videos, text, voice messages and other communication records [23]. Previous research on Digital Evidence Identification on Mobile Device Acquisition from instant messaging app "WhatsApp" using NIST framework. The study used the XRY application and also encase mobile forensic to acquire digital evidence on android and iOS smartphones from the whatsapp application. From the results of this study, it is said that when using forensic applications on smartphones, it must be in a state that has been rooted first [24]. This research will acquire digital evidence using two forensic applications, namely Magnet Axiom and Cellebrite UFED to obtain digital evidence from the Instagram application. This research was conducted based on the DFRWS framework. In the scenario, mobile forensics is carried out in cases of spreading hoax news using the Instagram application. The perpetrator deletes the data that has been spread on Instagram on his smartphone to remove traces. The evidence that this study is in the form of images, videos, emails, accounts, times, and locations.

II. Methods

This research follows the DFRWS framework for obtaining digital evidence and data exchange records collected by a centralized mechanism [25]. In its use the DFRWS framework consists of six stages [26] as in Figure 1.

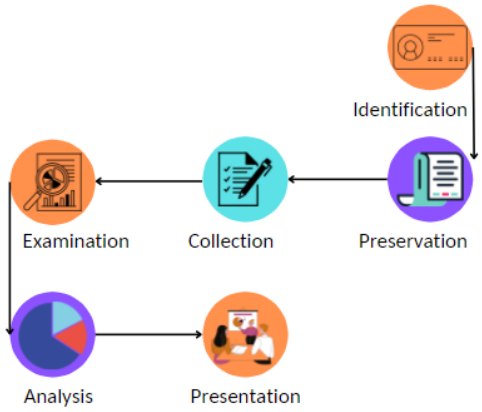

Fig. 1. Stages of the DFRWS Framework

The stages in figure 1 are outlined as follows:

- Identification: The initial stage to identify evidence and determine what is needed in the investigation process.
- Preservation: The stage of maintaining evidence in order to maintain authenticity and also changes and damage to the data contained in the evidence.

- Collection: The stage of collecting and identifying the required data from the data source on the evidence.
- Examination: The stage of separating or filtering on a part of the data source, in order to maintain the authenticity of other data, because it is to maintain the validity of digital evidence.
- Analysis: An analysis of the evidence obtained is carried out to find where, by whom and how the evidence data was obtained.
- Presentation: This stage displays all the information obtained from the previous analysis, then reports what actions should be taken next.

This research used some hardware and software in the forensic process in order to obtain the digital evidence sought, some of the devices used as in Table 1.

Table 1. Research Tools

No	Research Tools	Description
1	PC	G4560 - 8 GB RAM
2	Smartphone	Samsung Galaxy Tab A8
3	USB Cable	Connecting tool a smartphone with a PC
4	Instagram	Social Media Apps (Digital Crime Media)
5	Cellebrite UFED	Windows-based Forensic Application to find digital evidence on Smartphones
6	Magnet Axiom	Windows-based Forensic Application to find digital evidence on Smartphones
7	Power ISO	Supporting application to open the extraction results from the Cellebrite UFED application

A. Case Scenarios

Research raises cases of spreading fake news or hoaxes. To help this research, a simulation of how the process when a crime occurs is indicated by the spread of hoax news, scenario will be carried out as shown in Figure 2.

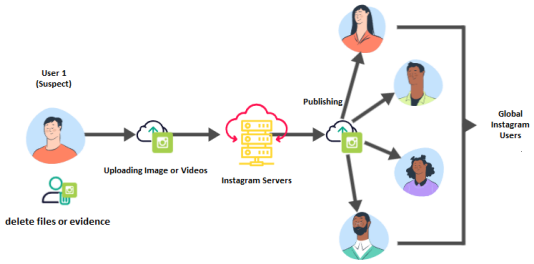

Fig. 2. Case Simulation

From Figure 2, it is explained that a user 1 or suspect uploaded several videos and pictures containing fake news on his Instagram account, after the suspect managed to upload videos and photos on his smartphone, it was immediately deleted as well as those on his Instagram account after the video was spread and seen by many other users. The suspect in his actions was using a Samsung Galaxy A8 tablet. After the video and images were viewed and forwarded by several other users, it caused an uproar among the public.

The authorities found this news and also some reports from the public directly investigating the truth and source of the hoax. After the suspect was successfully secured by the authorities, a mobile forensic process was carried out on the smartphone used by the suspect to obtain the digital evidence

needed for the legal process. The investigation process focuses on the search for digital evidence with several variables defined as in Table 2.

Table 2. Origin Data

No		Data		Amount
		Data Digital	**Meta Data**	
1	Text	Sender	50345927492/inyong2269	1
		Receiver	irhashainur	
		Message Date/ Time	06/12/2021 01:16:21	
2	Picture	MIME Type	image/jpeg	5
		Created Date	26/04/2022 02:15:33	
		Last Modified Date	26/04/2022 02:15:33	
		Size (Bytes)	50055	
		Resolution	1080x1920	
		MIME Type	image/jpeg	
		Created Date	26/04/2022 02:15:28	
		Last Modified Date	26/04/2022 02:15:28	
		Size (Bytes)	52904	
		Resolution	1080x1920	
		MIME Type	image/jpeg	
		Created Date	26/04/2022 02:15:33	
		Last Modified Date	26/04/2022 02:15:33	
		Size (Bytes)	40638	
		Resolution	1080x1920	
		MIME Type	image/jpeg	
		Created Date	26/04/2022 02:15:27	
		Last Modified Date	26/04/2022 02:15:27	
		Size (Bytes)	49707	
		Resolution	1080x1920	
		MIME Type	image/jpeg	
		Created Date	26/04/2022 02:14:02	
		Last Modified Date	26/04/2022 02:14:02	
		Size (Bytes)	66302	
		Resolution	640X640	
3	Video	File Extension	.mp4	5
		Created Date	27/04/2022 04:32:57	
		Modified Date	27/04/2022 04:33:01	
		File Size (Bytes)	837263	
		Duration (Sec)	2.73	
		Resolution	1088X1088	
		File Extension	.mp4	
		Created Date	27/04/2022 04:33:17	
		Modified Date	27/04/2022 04:33:20	
		File Size (Bytes)	806767	
		Duration (Sec)	2.54	
		Resolution	1088X1088	
		File Extension	.mp4	
		Created Date	27/04/2022 04:33:31	
		Modified Date	27/04/2022 04:33:34	
		File Size (Bytes)	582704	
		Duration (Sec)	1.91	
		Resolution	1088X1088	
		File Extension	.mp4	
		Created Date	27/04/2022 04:33:44	
		Modified Date	27/04/2022 04:33:46	
		File Size (Bytes)	294854	
		Duration (Sec)	1.11	

	Resolution	1088X1088	
	File Extension	.mp4	
	Created Date	27/04/2022 04:33:57	
	Modified Date	27/04/2022 04:33:59	
	File Size (Bytes)	299424	
	Duration (Sec)	1.11	
	Resolution	1088X1088	
Suplementary Data			
4	Account	inyong2269	1
5	IP address		1
6	Location		2
7	Url	https://www.instagram.com/	1

This origin data Table 2 will also function as a measure of the ability of forensic applications used in obtaining digital evidence.

III. Results and Discussion

This research follows the DFRWS framework in the forensic process in order to obtain digital evidence in a structured manner.

A. Identification

Identification is the first stage that is carried out as a reference for searching for digital evidence based on the case that occurred. The evidence of this research is a unit of smartphone / tablet with the Samsung brand in Table 3.

Table 3. Research Device Specifications

Thumbnail	Specifications	
	Manufacturer	Samsung
	Product	SM-P355
	Platform	Android
	Serial Number	RR2G600K09A
	IMEI	359896060296033
	Rooted	Yes

Table 3 shows the results of the identification of the mobile device used as a digital crime medium, namely a Samsung android smartphone with serial number SM-P355 and already in a rooted state.

B. Preervation Stage

Preservation is the stage of treatment and safety of original evidence. At this stage the smartphone is given special treatment to maintain the original state of the evidence. The special treatment carried out is to isolate the smartphone from the flow in and out of communication. The technique that is carried out when isolating the smartphone is to turn off data access and change the status of the smartphone device into airplane mode. An isolation process is put in place to prevent possible changes in data on the smartphone. Changes in data can be caused by the entry and exit of new data from the internet, which can damage the authenticity value of evidence in the law.

C. Collection Stage

Collection is a stage of collecting digital data from smartphones with a high-risk value, because if something goes wrong in the process, it can result in damage to digital evidence, so that the evidence on the smartphone cannot be opened or even permanently lost. The data collection process is carried out by connecting the smartphone to the pc / workstation used. The smartphone must be rooted so that

the data retrieval process using Cellebrite UFED and Axiom Magnet does not go wrong. The data obtained in the collection process will be stored into the PC / Workstation storage in the form of folders.

D. Examination Stage

The data obtained will be tested with Cellebrite UFED and Axiom Magnet by sorting from the data obtained as needed, the data that is suspected to be digital evidence will be opened whether there can be errors so that they can be used as legal evidence. If digital data is found that is suspected of being digital evidence but cannot be accessed, a re-data acquisition process will be carried out so that all digital evidence presented in the legal process is of legal value and can be used.

E. Analysis Stage

The results of the analysis of the data found and accessible using Cellebrite UFED and Axiom Magnet are presented as in Table 4.

Table 4. Data Analysis Results

No	Data	Informations
1	Instagram Version	299.0.0.11.111
2	Instagram Account	@inyong2269
3	Direct Message	13 Messages
4	Picture	267 Pictures
5	Video	1229 Videos
6	Ip Address	-
7	Location	-
8	URLs	100

Table 4 is the result of digital data analysis obtained using Cellebrite UFED and Magnet Axiom there is an Instagram account with a username @inyong22689 from the Instagram account there are 13 direct messages consisting of text messages, pictures and videos. From the Instagram application database, there are also 267 digital data images and 1229 videos and 100 URLs were found that had been accessed through the Instagram account @inyong22689.

F. Presentation

The final stage of the DFRWS framework is presentation, this stage is carried out to display a summary of the previous stage of the process after processing the evidence needed for the legal process. The digital evidence obtained must be presented in a table so that it makes it easier to present when asked to show digital evidence that is in accordance with the digital crime case being heard. All information obtained from the entire mobile forensic process is only selected based on the data needed and in accordance with the original data in Table 2 and obtained results as in Table 5.

Table 5. Artifacts Found

No	Variable	Amount	Cellebrite UFED	Magnet Axiom
Data Digital				
1	Text	1	0	1
2	Picture	5	5	5
3	Video	5	5	5
Suplementary Data				
4	Account	1	1	1
5	IP Address	1	0	1
6	Location	2	0	0
7	URL	1	0	1
Total		16	11	14

The entire data in the table above comes from testing using applications and scenarios according to the DFRWS framework intended to look for these variables. The value of accuracy in the ability to detect digital evidence of each application can use the following equation [27].

$$Par = \frac{\sum ar0}{\sum arT} \times 100\% \quad (1)$$

Par is the value of the accuracy of forensic applications
ar0 is the number of variables detected
arT is the number of variables used

By following equation (1) the level of accuracy and performance of Cellebrite UFED and Magnet Axiom in obtaining digital data as follows.

Cellebrite UFED

$$Par = \frac{11}{16} \times 100\% = 68.75\%$$

Magnet Axiom

$$Par = \frac{14}{16} \times 100\% = 87.5\%$$

Based on the above values, the digital evidence that can be obtained from each forensic application according to all the variables determined is Cellebrite UFED 68.75% and Magnet Axiom 87.5%.

IV. Conclusion

From all the steps taken to obtain digital evidence by following the DFRWS framework with evidence in the form of a Samsung Galaxy TAB A8 smartphone model number SM-P355, digital evidence was found with the value of each forensic application Cellebrite UFED 68.75% and Magnet Axiom 87.5% of the total 16 variables determined. Further research that will use the Cellebrite UFED application is expected to use the compatible Cellebrite Analyzer or Physical Image Analys application to obtain more detailed information from the extraction results on the Cellebrite UFED application.

References

[1] D. Hantono and D. Pramitasari, "Aspek Perilaku Manusia Sebagai Makhluk Individu Dan Sosial Pada Ruang Terbuka Publik," *Nat. Natl. Acad. J. Archit.*, vol. 5, no. 2, p. 85, 2018, doi: 10.24252/nature.v5i2a1.

[2] M. T. D. R, "A Review on Activity Extraction from Mobile Devices And Analyzing User Behavior," vol. 8, no. 7, pp. 568–575, 2021.

[3] 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, no. January, 2020, doi: 10.1016/j.cose.2019.101650.

[4] I. Riadi, A. Yudhana, and M. C. F. Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)," *J. Tek. Inform. dan Sist. Inf.*, vol. 4, no. 2, pp. 219–227, 2018.

[5] N. Istiani and A. Islamy, "Fikih Media Sosial Di Indonesia," *Asy Syar'Iyyah J. Ilmu Syari'Ah Dan Perbank. Islam*, vol. 5, no. 2, pp. 202–225, 2020, doi: 10.32923/asy.v5i2.1586.

[6] M. H. Purwidiantoro, D. F. Kristanto, and W. Hadi, "Pengaruh Penggunaan Media Sosial Terhadap Usaha Kecil Menengah (UKM)," *AMIK Cipta Darma Surakarta*, vol. 1, no. 1, pp. 30–39, 2016, [Online]. Available: http://journal.amikomsolo.ac.id/index.php/ekacida/article/view/19/11.

[7] A. Antoni, "Kejahatan Dunia Maya (Cyber Crime) Dalam Simak Online," *Nurani J. Kaji. Syari'ah dan Masy.*, vol. 17, no. 2, pp. 261–274, 2018, doi: 10.19109/nurani.v17i2.1192.

[8] G. B. Satrya *et al.*, "Analisis Forensik Android : Artefak Pada Aplikasi Penyimpanan Awan Box Android Forensics Analysis : Artifacts of Box Cloud Storage," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 3, pp. 521–530, 2020, doi: 10.25126/jtiik.202072220.

[9] I. Riadi, A. Yudhana, and I. Anshori, "Analisis Forensik Aplikasi Instant Messenger pada Smartphone Berbasis Android," *J. Insa. Comtech*, vol. 2, no. 2, pp. 25–32, 2017.

[10] E. S. Wijaya and R. Mukidah, "Analisis Forensik Perbandingan Tingkat Kerentanan Serangan Malware pada Smartphone Berbasis IOS dan Android menggunakan Metode NIST," no. November, pp. 67–76, 2019.

[11] N. Anwar and I. Riadi, "Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, p. 1, 2017, doi: 10.26555/jiteki.v3i1.6643.

[12] V. F. Dr. Vladimir, "**済無**No Title No Title No Title," *Gastron. ecuatoriana y Tur. local.*, vol. 1, no. 69, pp. 5–24, 1967.

[13] T. Rochmadi, "Deteksi Bukti Digital Pada Adrive Cloud Storage Menggunakan Live Forensik," *Cyber Secur. dan Forensik Digit.*, vol. 2, no. 2, pp. 65–68, 2019, doi: 10.14421/csecurity.2019.2.2.1455.

[14] I. Riadi and R. Umar, "Identification Of Digital Evidence On Android ' s," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 5, pp. 3–8, 2017.

[15] B. Dangar, "Forensic Analysis on WhatsApp / Linkedin," vol. 8, no. 5, pp. 528–531, 2021.

[16] N. Chakraborty, "Framework for Data Extraction and Analysis of Damaged Android Mobile Device," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 7, no. 5, pp. 306–311, 2019, doi: 10.22214/ijraset.2019.5050.

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

[18] S. R. Ardiningtias, S. Sunardi, and H. Herman, "Forensik Digital Kasus Penyebaran Pornografi pada Aplikasi Facebook Messenger Berbasis Android Menggunakan Kerangka Kerja National Institute of Justice," *J. Edukasi dan Penelit. Inform.*, vol. 7, no. 3, p. 322, 2021, doi: 10.26418/jp.v7i3.48805.

[19] K. D. O. Mahendra and I. K. Ari Mogi, "Digital Forensic Analysis Of Michat Application On Android As Digital Proof In Handling Online Prostitution Cases," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 9, no. 3, p. 381, 2021, doi: 10.24843/jlk.2021.v09.i03.p09.

[20] L. H. Singh, "A Forensic approach to Perform Android Mobile Forensic Analysis and Locating Artifacts from Digital Evidence," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 8, no. 4, pp. 1770–1791, 2020, doi: 10.22214/ijraset.2020.4291.

[21] M. Asim, M. F. Amjad, W. Iqbal, H. Afzal, H. Abbas, and Y. Zhang, "AndroKit: A toolkit for forensics analysis of web browsers on android platform," *Futur. Gener. Comput. Syst.*, vol. 94, pp. 781–794, 2019, doi: 10.1016/j.future.2018.08.020.

[22] M. S. Chang and C. P. Yen, "Forensic Analysis of Social Networks Based on Instagram," *Int. J. Netw. Secur.*, vol. 21, no. 5, pp. 850–860, 2019, doi: 10.6633/IJNS.201909.

[23] R. Rahmansyah, "Perbandingan Hasil Investigasi Barang Bukti Digital Pada Aplikasi Facebook Dan Instagram Dengan Metode Nist," *Cyber Secur. dan Forensik Digit.*, vol. 4,

no. 1, pp. 49–57, 2021, doi: 10.14421/csecurity.2021.4.1.2421.

[24] A. Wirara, B. Hardiawan, and M. Salman, "Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan 'WhatsApp,'" *Teknoin*, vol. 26, no. 1, pp. 66–74, 2020, doi: 10.20885/teknoin.vol26.iss1.art7.

[25] A. L. Suryana, R. El Akbar, and N. Widiyasono, "Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS)," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 2, pp. 111–117, 2016, doi: 10.26418/jp.v2i2.16821.

[26] I. Zuhriyanto, Anton Yudhana, and Imam Riadi, "Comparative analysis of Forensic Tools on Twitter applications using the DFRWS method," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 5, pp. 829–836, 2020, doi: 10.29207/resti.v4i5.2152.

[27] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic tools performance analysis on android-based blackberry messenger using NIST measurements," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 3991–4003, 2018, doi: 10.11591/ijece.v8i5.pp3991-4003.