

HASIL CEK_60020397_Point-C16-IRD-850GB-Nov 2020-Forensic Browser of Twitter based on Web Services

by Imam Riadi 60020397

Submission date: 11-Dec-2020 09:48AM (UTC+0700)

Submission ID: 1471639846

File name: B-Nov_2020-Forensic_Browser_of_Twitter_based_on_Web_Services.pdf (1.03M)

Word count: 3512

Character count: 18451

Forensic Browser of Twitter based on Web Services

Revani Saputra

Department of Information Systems
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi

Department of Information Systems
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT

Twitter is a social media that can be accessed through smartphones and desktops. The large number of users makes Twitter inseparable from crimes including pornography, online gambling and hate speech. In this study, the steps used are collection, examination and analysis. This study uses a laptop as an object that is scenario in a state of opening Twitter via the Google Chrome browser with two modes, namely public mode and private mode. The research used the help of forensic tools, namely ftk imager, dumpIT, belkasoft ram capturer, XhD, browser history viewer, browser history capturer, and cached video viewer. This research produces digital evidence with google chrome browser in public mode and google chrome browser in private mode. In the condition of using the browser in public mode with indicators in the form of text posts, link posts, images, and videos, the research succeeded in getting all the evidence that was sought. Meanwhile, in the private mode google chrome browser managed to get evidence with a success of 50%, namely in the form of text posts and link posts. While the remaining 50% is not found for private mode browsers, namely in image posts and video posts.

Keywords

Forensics, Web, Browsers, Pornography, Twitter

1. INTRODUCTION

Social media has become a necessity for communication tools most often used by society today, social media can penetrate distance, space and time. In 2019, the number of social media users in Indonesia has reached 150 million users, equivalent to a penetration rate of 56% [1]. One of the social media that is often used by the community is Twitter [2]. Twitter is a microblogging social media that can be accessed through desktop, web, Android and iOS platforms [3]. The large number of users makes social media usable for criminal activities. Cybercrime can occur due to advances in computer technology and information technology, especially internet media [4]. Some examples of crimes involving social media are cyberbullying, defamation, and the distribution of pornographic content. Pornography is any form of audio, visual, and audio-visual material that focuses on genitals and sexual behavior for sexual pleasure and pleasure [5]. These crimes can be uncovered with the help of digital forensics. In general, digital forensics can be divided into 4 stages, namely collection, maintenance, analysis and presentation [6].

1.1 Literature Review

1.1.1 Previous Studies

Rusydi Umar and Anton Yudhana (2018) have conducted digital forensic research entitled "Comparative Design of Live Forensics on Social Media Security of Instagram, Facebook and Twitter in Windows 10". The research design involved three social media to carry out safety comparisons, namely Facebook, Instagram and Twitter. All social media accounts

involved in the research design are newly created accounts or special accounts for research use [7].

Muhammad Nur Faiz, Rusydi Umar, Anton Yudhana (2017) conducted a digital forensic research entitled "Implementation of Live Forensics for Comparison of Browsers in Email Security". The results show that in public mode only Google Chrome does not get the password, while in private mode the three browsers display the same results for the password, which is not visible [8].

Anton Yudhana, Imam Riadi, and Ikhsan Zuhriyanto (2019) have completed a research entitled "Analysis of Live Forensics for Social Media Applications in Browsers Using the Digital Forensics Research Workshop (DFRWS) method". This research has succeeded in obtaining evidence in the form of deleted images on twitter posts. To ensure that the images found are the results of posts from the account in question, the research was conducted to match the user id [9].

Tayomi Dwi Larasati and Bektı Cahyo Hidayanto (2017) have conducted a study in the field of digital forensics with the title "Live Forensics Analysis for Comparison of Instant Messenger Applications on the Windows 10 Operating System". Through this research, it was found that Facebook and Line Messenger were successfully foensicized, while the Telegram Messenger application was an application that had its own challenges for the forensic world because existing data had a level of confidentiality that was more secure than Facebook and Line Messenger [10].

Ermadi Satriya Wijaya and Teguh Subagyo (2018) have successfully conducted a study entitled "Analysis of Digital Evidence on Android Random Access Memory Using the Live Forensic Method of Child Abduction Cases". This research succeeded in finding digital evidence in the form of images sent by the perpetrator, previously deleted text messages and log files of incoming calls on the victim's smartphone and log files of outgoing calls on the perpetrator's smartphone. However, there are some data that cannot be found, such as time and voice calls [11].

1.1.2 Web Browser

A web browser is a program that can be used to retrieve HTML documents from web server applications that can be used to search and find various information, send and receive e-mails, communicate with instant messengers or social networks, make buying and selling transactions through e-websites. commerce [12]. Popular web browsers include Mozilla Firefox, Internet Explorer, Google Chrome, and Opera [13].

1.1.3 Social media

Social media is a form of rapid technological development. Based on the results of a survey conducted by We Are Social and Hootsuite in 2019 as can be seen in Figure 1.



Figure 1. Social Media Users in Indonesia

Figure 1 states that active social media users have increased by 7% from the previous year or 56% of the total population of Indonesia. This is directly proportional to the increasing number of internet users in Indonesia [14].

1.1.4 Twitter

Twitter is a website that offers social networking services in the form of microblogs to users, allowing users to send and read a post to the public called a tweet. On Twitter, users can also upload media other than text, such as images and videos, called tweetpics [15]. The amount of public interest in this service has made many parties use it for certain interests. Apart from that, users can also use the # sign (hashtag) to compose messages based on topic.

1.1.5 Digital Forensics

Digital forensics means a search activity that goes through the process of identification, filtering and documentation which has the power to support evidence of facts [16]. The purpose of digital forensics is to prove the existence of an instruction that has occurred by investigating the crime scene (crime scene) so that it can prove from evidence such as computer systems, storage media, electronic documents, or data packets moving through computer networks. [17].

1.1.6 Digital Evidence

Digital evidence is all data and information obtained in digital form such as images, sounds, text, symbols, numbers, etc. One of the main steps in investigating a crime is collecting digital evidence [18]. Digital evidence is so susceptible to change that it can be affected if it is handled incorrectly. If the evidence has changed, it will lead to false results or the evidence will be useless. Digital evidence is very necessary for a standardized process and formalized so that digital evidence can be accepted during the trial process [19].

1.1.7 Pornography

Pornography is images, sketches, illustrations, photographs, writings, voices, sounds, moving pictures, animation, cartoons, conversations, gestures, or other forms of messages through various forms of communication media and / or public performances, which contain obscenity or exploitation. sex that violates the norms of decency in society [20]. Pornography can be traded, for example, downloading videos on the internet and then trading in the surrounding community. One of the factors in the development of the spread of pornographic content is the increasingly advanced technology, especially the internet [21].

2. METHODOLOGY

2.1 Research Scenario

The case used in this study is the distribution of pornographic content through Twitter social media. The pornography in

question can be in the form of regular posts or posts that lead to transactions. Twitter account owners post several posts that show pornographic content activity and even account owners are trading the content. Then the post was deleted from Twitter to eliminate digital traces as can be seen in Figure 2.

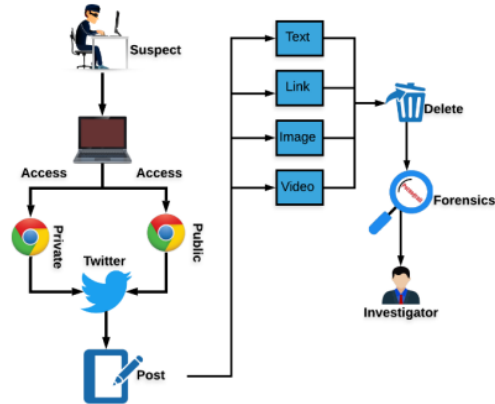


Figure 2. Research Scenarios

Figure 2 explains that the scenario uses two browser usage models, namely a private browser and a public browser. The twitter account used in this study is a special account created for research purposes with the username @forensiksatu.

2.2 Research Stages

In this implementation stage, the investigator carries out a series of activities to obtain information in accordance with procedures. The stages or methods used in finding evidence are collection, examination and analysis. These stages can be seen in Figure 3.



Figure 3. Stages of the Method

The steps to be taken by the investigator in seeking information as evidence are described as follows.

2.2.1 Collection

The evidence that was successfully obtained was a laptop that was scenarioed as evidence of a crime. As can be seen in table 1.

Table 1. Physical Evidence

No	Name	Picture	Information
1	Laptop		Lenovo G40-45 found at the scene of the crime scene with the power on and connected to the network
2	Charging Cable		The actor's Lenovo G40-45 charger cable with input 100-240 V ~ 1.8 A and outputs 20 V and 3.25 A

Evidence that has been collected is then carried out data acquisition, especially for temporary data first.

2.2.2 Examination

At this stage, the process of taking over the information contained in the perpetrator's laptop will be carried out. Prioritized data is data that is temporary, such as RAM activity. The acquisition process is carried out in two stages, namely the public mode browser and the incognito mode browser.

2.2.3 Analysis

The analysis in question is the process of searching for information that is from the previous data acquisition. The information you are looking for is text posts, link posts, image posts, and video posts.

3. RESULT AND DISCUSSION

The scenario of the case of spreading pornographic content on social media, Twitter, tries to be uncovered by doing forensics on physical evidence, namely the alleged perpetrator's laptop. The tools and materials needed, among others, can be seen in table 2.

Table 2. Tools and Materials

No.	Tools and Materials	Information
1	Laptop 1	The investigator's laptop Intel (R) Core (TM) i5-7500HQ CPU @ 2.50GHz (4 CPUs), ~ 2.5GHz
2	Laptop 2	The alleged perpetrator's laptop, namely Lenovo Ram 4GB, AMD A8-6410, Model G40-45, Windows 10 Home x64
3	FTK Imager	To read the capture result from the ram capturer and use it to check the hash value of the ram acquisition result
4	Belkasoft Ram Capturer	To carry out the acquisition of ram
5	DumpIT	To carry out the acquisition of ram
6	XhD	To read the results of the ram acquisition from the DumpIT tool
7	Browser History Viewer	To read the capture result from the Browser History Capturer tool
8	Browser History Capturer	To retrieve history from the browser including cached images and the web
9	Cached Video Viewer	To get evidence that is in video form.
10	Media Player Classical Home Cinema	To open the acquisition results from the Cached Video Viewer tool

3.1 Acquisition

This stage of the acquisition is carried out using four different tools. Temporary data is acquired using the DumpIT and Ram Capturer tools, while data that can still be accessed when the laptop is dead is acquired using the help of forensic tools, the video cache viewer and browser history capturer. The acquisition process is carried out for two models, namely the use of the public mode browser and the incognito mode browser.

3.1.1 Belkasoft Ram Capturer

Belkasoft ram capturer is used to acquire ongoing ram activities. The acquisition process can be seen in Figure 4.

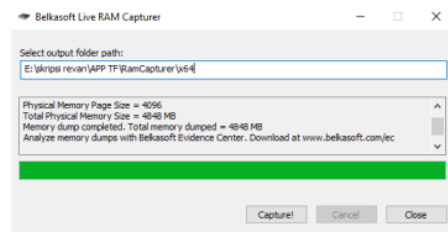


Figure 4. Acquisition with ram capturer

Figure 4 shows the acquisition process by the ram capturer and then produces data with the .mem extension.

3.1.2 DumpIT

The acquisition using the DumpIT tool can be seen as shown in Figure 5.

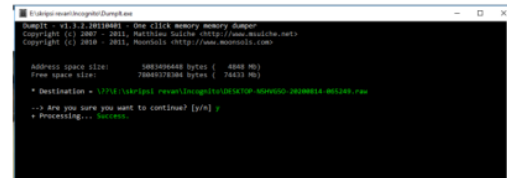


Figure 5. Acquisition with DumpIT

The resulting file has a .mem extension and a name that is automatically given by the tool according to the date and the laptop user.

3.1.3 Browser History Capturer

The acquisition process can be seen in Figure 6.

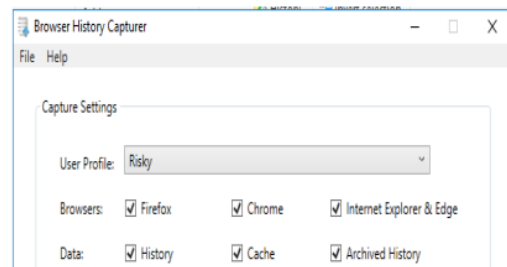


Figure 6. Acquisition with Browser History Capturer

Acquisition can choose three browsers at once, namely Firefox, Chrome, Internet Explorer & Edge or can choose one of them.

3.1.4 Video Cache Viewer

The video cache viewer will automatically capture the video cache from the browser when the tool is run. The acquisition process with a video cache viewer can be seen as shown in Figure 7.

Figure 7. Video Cache Viewer Acquisition

Figure 9. XhD results in public browsers

37

The evidence obtained from Figure 12 is in the form of the text "sell porn videos WA 08xxxxxxx80" along with several hashtags used including #openvcs, #latestporn, and teenporn which comes from the @forensiksatu account.

3.2.2.2 DumpIT

Evidence that was found with the help of the XhD tool can be seen in Figure 13.

```

717147D060    10 AE 5E 31 FF 7F 00 00 00 00 00 00 00 00 00 00 00 00 .....
717147D070    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
717147D080    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
717147D090    00 00 00 00 04 00 04 01 00 00 00 00 00 00 00 00 .....
717147D0A0    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
717147D0B0    00 00 00 00 33 AD 4F 3B D7 72 3E 10 DD 00 00 00 00 .....
717147D0C0    66 EF 72 65 6E 73 69 6B 73 61 74 75 67 6E 20 67 E2 20 [corenlkatsun
717147D0D0    54 77 69 74 74 65 72 3A 20 22 53 65 6C 6C 20 70 20 Twitter: "Shell p
717147D0E0    6F 72 6E 70 76 69 64 65 6F 73 20 57 61 20 30 38 30 gen videos WA
717147D0F0    78 65 78 78 78 78 38 30 20 23 6F 70 65 74 6E 78 88 XXXXXXXX $openm
717147D100    78 65 65 6E 70 67 72 6F 20 68 74 70 70 73 3A 2F 78 65 65 6E 70 67 72 6F 20 68 74 70 70 73 3A 2F 78 65 65 6E 70 67 72 6F 20 68 74 70 70 73 3A 2F https://
717147D120    2F 74 2E 63 6F 2F 6D 6F 57 39 6F 57 57 50 56 72 74 /e.co/mWgMwPzr/
717147D130    22 20 2F 57 67 74 74 65 72 3A 20 74 65 72 74 65 72 00 / Twitter, tte
717147D140    00 00 00 00 00 00 00 00 00 F9 D7 6D 3E 00 1E 00 00 .....
717147D150    00 B0 95 31 FF 7F 00 00 00 00 00 00 00 00 00 00 00 P'mily...

```

Figure 13. DumpIT results in incognito browser

Figure 13 shows that the text “sell porn videos WA 08xxxxxxx80 #openvcs # latestporn #teenporn” was found which came from the @forensiksatu twitter account. Evidence in the form of text has been successfully obtained using the help of the DumpIt and XhD tools. The use of the video cache viewer and browser history capturer tool did not succeed in finding the evidence that was sought, either in the form of photos or videos.

3.2.3 Result

The indicators used in the analysis include text posts, link posts, image posts, and video posts. A summary of the analysis results can be seen in table 3.

Table 3. List of Findings

Information	Public Mode Browser	Private Mode Browser
Text Posts	✓	✓
Link Posts	✓	✓
Image Posts	✓	-
Video Posts	✓	-

Based on table 5, the public mode browser managed to get all the evidence, such as text posts, link posts, images, and video posts. Meanwhile, the incognito mode browser only managed to get 50% of the data, namely for text posts and links. The remaining 50% cannot be found, namely in image posts and video posts.

4. CONCLUSION

Based on the results of research that have been carried out with the help of forensic tools and using two browser models, namely in public mode and incognito mode, it has succeeded in obtaining the evidence that is sought. The public mode browser was successful in getting all the evidence that was sought. The incognito mode browser managed to find 50% evidence, namely for text posts and link posts, while the remaining 50% were not found, namely for image and video posts. The evidence found can then be used to report and assist in the trial process.

5. REFERENCES

- The evidence obtained from Figure 12 is in the form of the text "sell porn videos WA 08xxxxxxx80" along with several hashtags used including #openvcs, #latestporn, and teenporn which comes from the @forensiksatu account.

3.2.2.2 DumpIT

Evidence that was found with the help of the XhD tool can be seen in Figure 13.

Figure 13 shows that the text "sell porn videos WA 08xxxxxxx80 #openvcs # latestporn #teenporn" was found which came from the @forensiksatu twitter account. Evidence in the form of text has been successfully obtained using the help of the DumpIT and XhD tools. The use of the video cache viewer and browser history capturer tool did not succeed in finding the evidence that was sought, either in the form of photos or videos.

3.2.3 Result

The indicators used in the analysis include text posts, link posts, image posts, and video posts. A summary of the analysis results can be seen in table 3.

Information	Public Mode Browser	Private Mode Browser
Text Posts	✓	✓
Link Posts	✓	✓
Image Posts	✓	-
Video Posts	✓	-

Based on table 3, the public mode browser managed to get all the evidence, such as text posts, link posts, images, and video posts. Meanwhile, the incognito mode browser only managed to get 50% of the data, namely for text posts and links. The remaining 50% cannot be found, namely in image posts and video posts.

4. CONCLUSION

Based on the results of research that have been carried out with the help of forensic tools and using two browser models, namely in public mode and incognito mode, it has succeeded in obtaining the evidence that is sought. The public mode browser was successful in getting all the evidence that was sought. The incognito mode browser managed to find 50% evidence, namely for text posts and link posts, while the remaining 50% were not found, namely for image and video posts. The evidence found can then be used to report and assist in the trial process.

5. REFERENCES

 - [1] WeAreSocial, & Hootsuite. Digital Report in 2019. Identified 22 October 2019, from <https://wearesocial.com/blog/2019/01/global-digital-report-2019>
 - [2] Nurhairani, H., & Riadi, I. (2019). Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method. International Journal of Computer Applications, 177 (27), 35-42. <https://doi.org/10.5120/ijca2019919749>
 - [3] Nurhairani, H., & Riadi, I. (2019). Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method. International Journal of Computer Applications, 177 (27), 35-42. <https://doi.org/10.5120/ijca2019919749>
 - [4] Ketaren, E. 2016. Cybercrime, Cyber Space, and Cyber Law. Times, 5 (2), 35-42. Retrieved from <http://stmik-time.ac.id/ejournal/index.php/jurnalTIMES/article/viewFile/556/126>
 - [5] Raka, ZD 2019. Spread of Illegal Content on Social Media (Case Study: Pornography on Bigo Live Application). 4 (1), 75-84. <https://doi.org/10.1037/0033-2909.126.1.78>
 - [6] Ahmad, MS 2017. Live Forensic Investigation from User's Side to Analyze Evil Twin-Based Man In The Middle Attack. Cell, 136 (4), 615-628. <https://doi.org/10.1016/j.cell.2009.01.043>
 - [7] Bintang, RAKN, Umar, R., & Yudhana, U. 2018. Designing a live forensics comparison on social media security Instagram, Facebook and Twitter on Windows 10. Proceedings of the 9th SNST 2018, Faculty of Engineering, Wahid Hasyim University, 125-128.
 - [8] Faiz, MN, Umar, R., & Yudhana, A. 2017. Implementation of Live Forensics for Browser Comparison on Email Security. JISKA (Journal of Informatics Sunan Kalijaga), 1 (3), 108. <https://doi.org/10.14421/jiska.2017.13-02>
 - [9] Yudhana, A., Riadi, I., & Zuhriyanto, I. 2019. Live Forensics Analysis of Social Media Applications in Browsers Using the Digital Forensics Research Workshop (DFRWS) Method. 20 (2), 125-130
 - [10] Larasati, TD 2017. Live Forensics Analysis For Comparison of Instant Messenger Applications (Line, Facebook, and Telegram) on Windows 10 Operating System.
 - [11] Wijaya, ES, & Subagyo, T. (2018). Analysis of Digital Evidence on Android Random Access Memory Using Live Forensic Method.
 - [12] Muhammad said Hasibuan. (2010). Design and Implementation of E-Journals as Improving Journal Services in Regional Koptoris 2. National Seminar on Information Technology Applications, 2010 (Snati), 46-50.
 - [13] Setiawan, D., Setiawan, R., Karunia, R., & Wicaksana, IWS (2007). Comparing Web Browser Performance. Gunadarma University, 1 (1), 1-6.
 - [14] WeAreSocial, & Hootsuite. Digital Report in 2019. Identified 22 October 2019, from <https://wearesocial.com/blog/2019/01/global-digital-report-2019>
 - [15] Saifulloh, M., & Ernanda, A. 2018. Communication Privacy Management for Adolescent Alter Ego Account Users on Twitter. WACANA, Scientific Journal of Communication Sciences, 17 (2), 235. <https://doi.org/10.32509/wacana.v17i2.652>
 - [16] Ahmad, MS 2017. Live Forensic Investigation from

- User's Side to Analyze Evil Twin-Based Man In The Middle Attack. *Cell*, 136 (4), 615–628. <https://doi.org/10.1016/j.cell.2009.01.043>
- [17] Marini, S. 2018. Digital Forensic Study in Regulation in Indonesia. National Seminar on Energy & Technology, 103–106.
- [18] Wahanggara, V., & Prayudi, Y. (2015). System Call Based Malicious Software Detection System for Classification of Digital Evidence Using Support Vector Machine Method. *SENTRA (National Seminar on Technology and Engineering)*, 1–8.
- [19] Faiz, MN, Prabowo, WA, & Sidiq, MF (2018). Digital Forensic Investigation Comparative Study on Crime. *Journal of Informatics, Information Systems, Software Engineering and Applications (INISTA)*, 1 (1), 54–62. <https://doi.org/10.20895/INISTA.V1I1>
- [20] Law of the Republic of Indonesia Number 44 of 2008 concerning Pornography. (2008). 3 (2), 54–67. Retrieved from <http://repositorio.unan.edu.ni/2986/1/5624.pdf>
- [21] Raka, ZD (2019). Distribution Of Illegal Content In Social Media (Case Study: Pornography On Bigo Live Application). 4 (1), 75–84. <https://doi.org/10.37703/ijcaonline.org.1037//0033-2909.I26.1.78>

HASIL CEK_60020397_Point-C16-IRD-850GB-Nov 2020- Forensic Browser of Twitter based on Web Services

ORIGINALITY REPORT

4%

SIMILARITY INDEX

4%

INTERNET SOURCES

3%

PUBLICATIONS

3%

STUDENT PAPERS

PRIMARY SOURCES

1

www.ijcaonline.org

Internet Source

2%

2

Reza Chandra, M. Agung Sucipta Iskandar, Lintang Yuniar Banowosari, Adang Suhendra, Prihandoko Prihandoko. "Building Corpus in Bahasa Indonesia for Pornographic Indicated Website Content", 2019 5th International Conference on Computing Engineering and Design (ICCED), 2019

Publication

2%

Exclude quotes On

Exclude matches < 1%

Exclude bibliography On