CyberSecurity and Digital Forensics e-ISSN: 2615-8442
Vol. 5, No. 2, November 2022, p.51-59

FORENSIC ANALYSIS OF CYBERBULLYING CASES ON INSTAGRAM AND WHATSAPP USING THE NATIONAL INSTITUTE OF JUSTICE (NIJ) METHOD

Dina Yuliana[1], Trihastuti Yuniati[2], Bita Parga Zen[3]

[1,2,3]Program Studi Informatika, Institut Teknologi Telkom Purwokerto

Email: [1]yulianadina557@gmail.com, [2] trihastuti@ittelkom-pwt.ac.id, [3]bita@ittelkom-pwt.ac.id
corresponding author : bita@ittelkom-pwt.ac.id

Abstract

The negative impact of advances in information and communication technology which is increasing this year is the emergence of the Cyberbullying phenomenon. Anti-bullying charity, Ditch The Label in its survey "The Annual Bullying Survey 2017", noted that more young people experience cyberbullying on Instagram than on other platforms at 42 percent, with Facebook following behind with 37 percent. Snapchat ranked third with 31 percent, while WhatsApp (12 percent), Youtube (10 percent), Twitter (9 percent), and Tumblr (2 percent) reported cyberbullying. The criminal behavior committed by cyberbullying perpetrators will certainly leave evidence in the form of digital evidence of conversations about crimes committed by perpetrators and victims. therefore, it is necessary to have digital forensic techniques to search for valid digital evidence. In this study, researchers created scenarios of cyberbullying cases on Instagram and Whatsapp applications via cell phones. This study aims to find out how to carry out forensic analysis using the NIJ method and find out the results of analysis from the forensic applications MOBILedit, Autopsy, and FTK Imager in searching for digital evidence of cyberbullying on the Instagram and Whatsapp applications. The results showed that digital evidence was found in almost all of the data according to the scenario using the Autopsy and FTK Imager applications, using a physical image obtained from the MOBILedit extract in a rooted cellphone. However, the FTK imager must know the location first so that it is easier to find data.

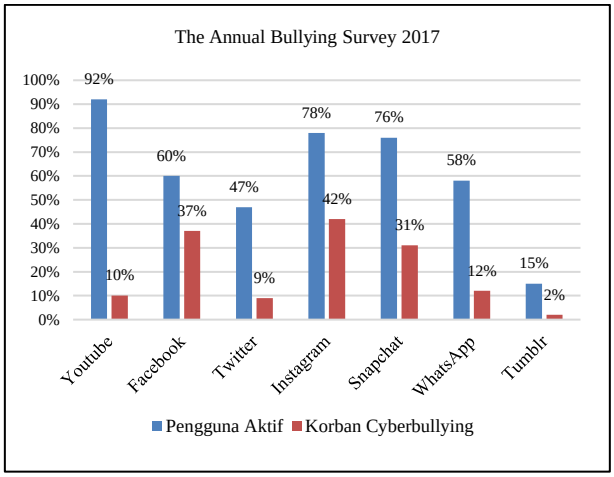
Keywords:*cyberbullying, instagram, whatsapp, NIJ, digital forensics.*

1. INTRODUCTION

The rapid development and advancement of information and communication technology has created various positive and negative impacts. One of the positive impacts that can be drawn from the development of information and communication technology is that it is easier for people to access and use information, and it is easier to communicate with other people in any part of the world.(Yudhana et al., 2019). But on the other hand this information technology can cause harm in the form of negative things, one of the negative impacts arising is the emergence of the phenomenon of cyberbullying among children and adults. Cyberbullying is a new form of bullying that is commonly experienced in the real world but with the same characteristics and effects. Cyberbullying includes relational malicious behavior techniques directed at individuals, groups using information and communication technologies(New, 2019). Cyberbullying can be through intermediaries such as messages that contain negative words, words that can lead to acts of bullying(Widiandana et al., 2020). Cyberbullying has forms including flaming (messages with anger), harassment (disturbance), denigration (defamation), impersonation (impersonation), outing (spreading), trickery (deception), exclusion (exclusion) and cyberstalking (stalking).(Syah & Hermawati, 2018).

Social media is included in one of the means of information and communication technology that is very popular with people in the world. Hootsuite (We Are Social) in its latest research states that as of February 2022, the number of active social media users in the world has reached 4.62 billion people (58.4 percent of the world's population), while the number of active social media users in Indonesia it has reached 191.4 million people, this number has increased by 12.6 percent from 2021 which amounted to 170 million people. Compared to the total population in Indonesia in 2022 which is 277.7 million people, the number of active social media users is at 68.9 percent of the total population.(Hootsuite (We are Social), 2022). The large number of active social media users that exceed 50 percent of the total population is likely to cause several cases of cyberbullying in the world or in Indonesia.

In a survey conducted by the anti-bullying donation agency, Ditch The Label entitled "The Annual Bullying Survey 2017", Instagram was named the social media most frequently used by users for online bullying or cyberbullying. The survey was conducted on 10,020 people from England with an age range of 12 to 20 years, 42 percent of whom said they had been victims of cyberbullying on Instagram. Followed by Facebook with 37 percent, Snapchat is in third place with 31 percent, while WhatsApp (12 percent), Youtube (10 percent), Twitter (9 percent), and Tumblr (2 percent) of reported cyberbullying cases(Ditch the Label, 2017).



Source: The Annual Bullying Survey 2017, Ditch the Label.

Figure 1. Cyberbullying statistics on social media

Figure 1 provides information that the black bar graph represents the percentage of all young people using the platform. Meanwhile, the moss green bar graph depicts the percentage of young people who have been bullied in cyberspace and experienced it on the platform. The pink bar graph represents the percentage of all platform users who have experienced cyberbullying on the platform(Ditch the Label, 2017).

Cyberbullying cases that have occurred in Indonesia have resulted in victims committing suicide, including experienced by Yoga, who was desperate to crash himself into a passing train on May 26 2013. Yoga was determined to commit suicide due to pressure and blasphemy due to the failure of a music event where he was chairman. the event organizer. Some time before the incident, he had tweeted on his account, "Thank you for all the swearing at @locstockfest2, these are movements towards God, greetings."(Merdeka.com, 2013).

Another case of digital bullying (Cyberbullying) came from Canada, namely the tragic story of the case of Amanda Michelle Todd. Starting from a conversation with a new friend on social media in 2010, Amanda was persuaded to show sensitive parts of her body to the perpetrator via webcam. Unexpectedly, the perpetrator had recorded it to threaten Amanda to want to "do" further. The perpetrator threatened to spread the photos he recorded to Amanda's friends if they were not willing to comply with the perpetrator's request. Amanda refused and finally the photo really spread even very widely on the internet. The digital footprint continues to follow Amanda wherever she moves. The bullying got so serious that Amanda became depressed and attempted suicide several times. Surviving the suicide attempt, netizens are even more "fierce" bullying Amanda. peak, (IGA Ayu Dewi Satyawati & Sagung Putri M. E Purwani, nd).

Researcher of The Institute for Digital Law and Society (Tordillas), namely Bunga Meisa Siagian at a seminar on Discussing Cyber Crime organized by The Institute for Digital Law and Society (Tordillas) and the Ministry of Communication and Informatics in Jakarta at the end of April 2019, mentioned the case of Amanda Todd as an important lesson for Indonesia to prevent and

regulate digital bullying (Cyberbullying) on social media. Thus, the case of Amanda Todd can be used as a valuable lesson and comparison in preventing cybercrime in Indonesia. It is also included as material to add to the rules regarding cyber bullying in the revision of the Electronic Information and Transaction Law (UU ITE).(Hukumonline.com, 2019).

The number of cyberbullying phenomena in society can have negative impacts both legally and psychologically. Legally the perpetrator can be charged according to the applicable Electronic Information and Transaction Law (UU ITE), while psychologically the victim can result in depression, difficulty concentrating, feeling isolated, treated inhumanely, decreased self-confidence and a loss of hope as well as feelings of loneliness which can lead to suicide victim(Daily, 2017). Crimes committed by cyberbullying perpetrators will certainly leave evidence in the form of digital evidence of conversations about crimes committed by perpetrators and victims. So that law enforcers can prove the crime of suspects in court by carrying out digital forensic processes (Umar & Sahiruddin, 2019). Digital forensic science can be used to practice dissecting digital devices in finding facts about crimes that have occurred for legal purposes(Star et al., 2020).

This research will apply three digital forensic applications, including the MOBILedit Forensic Express application version 7.4, Autopsy version 4.19.3 and Access Data FTK Imager version 4.7.1, these applications are used in conducting digital investigations to obtain digital evidence data obtained from the Instagram application and WhatsApp as a research object. The method used is the National Institute of Justice (NIJ), this method can simplify the investigation process starting from the collection of evidence to the stage of reporting evidence with stages*Identification*(identification), Collection (Collection), Examination (Examination), Analysis (Analysis), and Reporting (Reporting).

From the existing problems, a study was conducted entitled "Forensic Analysis of Cyberbullying Cases on Instagram and Whatsapp Using the National Institute of Justice (NIJ) Method". In this study, researchers created scenarios of cases of Cyberbullying on Instagram and Whatsapp via cell phones. The purpose of this study is to analyze the digital forensic process for Cyberbullying cases using the National Institute of Justice (NIJ) method which applies three digital forensic applications, including the MOBILedit Forensic Express application version 7.4, Autopsy version 4.19.3 and Access Data FTK Imager version 4.7.1 with the advent of digital evidence from Instagram and WhatsApp. This research is expected to contribute knowledge to academics,

2. LITERATURE REVIEW

2.A. Digital Forensics

Digital forensic science can be used to practice dissecting digital devices in finding facts about crimes that have occurred for legal purposes(Star et al., 2020).Digital forensics is an investigative technique to identify, collect, examine and store evidence/information that is stored/encoded on digital storage media as evidence in uncovering criminal cases that can be legally justified.(Saputra & Widiyasono, 2017).

2.B. *Cyberbullying*

*Cyberbullying*is a new form of bullying that is commonly experienced in the real world but with the same characteristics and effects. Cyberbullying includes relational malicious behavior techniques directed at individuals, groups using information and communication technologies(New, 2019).

2.C. Instagram

Instagram is a photo sharing service application that allows users to take photos, apply digital filters and share them on various social networking services. The social system on Instagram is to follow other user accounts, or have Instagram followers. Thus communication between fellow Instagram users can be established by giving likes and commenting on photos that have been uploaded by other users. Instagram can also display videos of quite a long duration and are filled with other complementary features(Kinasih et al., 2020).

2.D. WhatsApp

WhatsApp is a cross-platform instant messaging service application for mobile phones that rely on the internet for messaging. Based on a low-cost subscription model, WhatsApp is an inexpensive alternative to sending text messages via SMS, especially for international or group messages. Mobile messaging applications allow users to share text, picture and video messages. The WhatsApp Messenger application uses a mobile data connection and WiFi to carry out data communication, using WhatsApp, one can chat online, share files, exchange photos and other features that interest its users. (Anwar & Riadi, 2017).

2.E. National Institute of Justice

National Institute of Justice(NIJ) is a research, development, and evaluation agency of the US Department of Justice. The Institute provides objective, independent, evidence-based knowledge and tools to improve the administration of justice and public security(National Institute of Justice, 2004b).

In this study using methods from the National Institute of Justice (NIJ) with a report entitled "Forensic Examination of Digital Evidence: A Guide for Law Enforcement" published in April 2004. This guide is intended for use by law enforcement officials and the law enforcement community who are responsible for Responsible for checking digital evidence. This guide deals with common situations encountered during the examination of digital evidence. This is a guide that companies can use to assist them in developing their own policies and procedures. When dealing with digital evidence, general forensic and procedural principles must be applied. Actions taken to secure and collect digital evidence should not affect the integrity of that evidence(National Institute of Justice, 2004a).

The stages of the NIJ method are: Assessment, Acquisition, Examination, and Documenting & reporting(National Institute of Justice, 2004a).

2.F. MOBILeditForensic

MOBILedit Forensic is a mobile extractor, data analyzer and report generator all in one solution. A powerful 64-bit application using both physical and logical data acquisition methods. By connecting the phone via a USB cable, Wi-Fi or Bluetooth, it can perform individual checks on most mobile devices and generate deep reportsvarious formats(PDF, HTML, Excel, etc.) for various needs (MOBILedit, 2021).

2.G. Autopsy

Autopsy is an application that can find hidden information from a file, starting from when the file was created, modified, accessed, deleted. The application provides an intuitive workflow for users in law enforcement, military, intelligence agencies, cyber security and corporate investigators. This application only requires the disk image of the device to be analyzed(Riski Ardiningtias, 2021).

2.H. Access Data FTK Imager

Access Data Forensic Tool Kit Imager or commonly called "AD FTK Imager" is an application used in the world of digital forensics to perform a data acquisition system developed by Access Data company. The acquisition system itself is a system that functions to retrieve, collect and prepare data, to process it to produce the desired data(Kinasih et al., 2020).

3. METHODOLOGY

The research method used in carrying out this research is the National Institute of Justice (NIJ) method, published in April 2004 with a report entitled "Forensic Examination of Digital Evidence: A Guide for Law Enforcement". There are four stages, namely Assessment, Acquisition, Examination, and Documenting & reporting.(National Institute of Justice, 2004a).

Assessment stage, the forensic examiner must thoroughly assess digital evidence in relation to the scope of the Cyberbullying case to determine the actions to be taken(National Institute of Justice, 2004a).

In the Acquisition (Data Acquisition) stage, digital evidence is inherently fragile and can be altered, corrupted, or destroyed by improper inspection. So that the examiner secures and preserves the original evidence. That way the original evidence of cyberbullying cases on Instagram and WhatsApp can be maintained and the integrity of the evidence is maintained(National Institute of Justice, 2004a).

Examination stage, at this stage the examiner extracts and analyzes digital evidence. Extraction refers to recovering Cyberbullying data from Instagram and WhatsApp. Whereas Analysis refers to the interpretation of recovered and recovered data and placing it in a logical and useful format(National Institute of Justice, 2004a).

The last stage is the Documenting & reporting Stage (documentation & reporting), actions and observations must be documented during the processing of forensic evidence. In addition, it will also end with the preparation of written reports obtained in the investigation of cyberbullying cases on Instagram and WhatsApp(National Institute of Justice, 2004a).

The subjects in this study are researchers. Meanwhile, the object of this study is the case of cyberbullying on two social media applications Instagram and WhatsApp.

3.A. Research Flowchart

In this study, a research flowchart was designed to facilitate researchers in the process of conducting research. Figure 2 is a research flowchart which aims to focus and direct research steps so that they go according to plan and scope. The following flowchart, starting from Problem Identification of research conducted, Literature Study for reference, Case Scenarios created for research data, Forensic Analysis as a forensic process using the NIJ 2004 method, Report Compilation as a result of research and the final steps in this study.

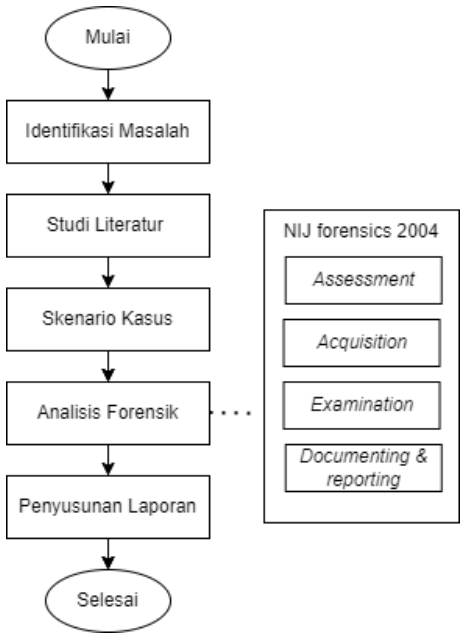


Figure 2. Research Flowchart

Researchers used the National Institute of Justice (NIJ) method, published in April 2004 with a report entitled "Forensic Examination of Digital Evidence: A Guide for Law Enforcement", which serves to find out digital evidence of cyberbullying from Instagram and WhatsApp applications.

3.B. Scenario creation

This study uses a case scenario created by the researcher. On Instagram, researchers will use 4 (four) Instagram accounts namely, 3 (three) accounts as perpetrators of cyberbullying cases and 1 account as victims of cyberbullying. In this case scenario, it begins with the researcher who plays the role of the victim and

enters the Instagram social media account via cellphone. Furthermore, researchers as victims will make posts in the form of pictures and videos of victims, which will be commented on by the perpetrators with comments containing bullying. One of the perpetrators will continue by sending private text messages to the victim's Instagram account, intending to discuss the victim's posts which contain many bullying comments. Ended up being insulted too.

Whereas on WhatsApp, the researcher as the perpetrator will enter the WhatsApp account. The researcher will create a WhatsApp group with 3 (three) members, namely 2 (two) perpetrators and 1 (one) victim of a cyberbullying case. The researcher as the perpetrator will send screenshots of posts and comments on the victim's Instagram to the group that the researcher created before. Other perpetrators will participate in making text messages so that the victim feels cornered in the group. In addition to text messages and pictures, researchers will send videos that victims post on Instagram to be used as insults.

After carrying out the Cyberbullying scenario on the Instagram and WhatsApp applications, the researcher, as an examiner or investigator, will acquire data from the perpetrator's account using MOBILedit Forensic Express 7.4 to retrieve data on the account for security and data preservation. The next stage is that the researcher will conduct an examination by extracting and analyzing digital evidence from the results of the data acquisition that has been carried out.

4. DISCUSSION

4.A. Assessment

*Assessment*or assessment, the researcher conducted a thorough assessment by reviewing cases of cyberbullying that occurred on Instagram and WhatsApp, ensuring that there were no other related cases. Identify and document the types of software, social media (Instagram and WhatsApp) used by victims and perpetrators of Cyberbullying. Make sure the device is not connected to the network to avoid changing the original.

After the assessment is carried out and it is confirmed that it is safe, the researcher will carry out the next stage, namely the Acquisition stage. Prior to the acquisition stage, there was information from mobile devices used by researchers as cyberbullying perpetrators and victims which can be seen in Table 1.

Table 1. Information for the Oppo A37f cellphone

Cell Phone Information	
Name of the owner	Dina Juliana
Phone Name	Oppo A37f
Model Number	A37f
Operating system	Android 10
IMEI	86563703*******
IMSI	51010255*******
Password or Pattern	*Yes*
Rooted	*Yes*
External Memory	*Yes*
SIM card	*Yes*

4.B. Acquisition

*Acquisition*or data acquisition on devices or evidence used by cyberbullying perpetrators and victims. Researchers use the Oppo A37f cellphone to create case scenarios as perpetrators and victims. The specifications of the cellphone are Android 10 Version ColorOS V3.0.01, 2GB RAM, 16GB Internal Memory, CPU Quad-core 1.2 GHz Cortex-A53, and Screen Size 5.0 inches.

The acquisition was carried out with the aim of securing and preserving the original evidence of Cyberbullying cases on Instagram and WhatsApp of perpetrators and victims, in anticipation of digital evidence being altered, damaged, or destroyed. The following is the acquisition process carried out by researchers on cellphones in non-root and root conditions.

1. Non-Root

Figure 3. Data Acquisition Process

It can be seen in Figure 3 that the data acquisition process in the MOBILedit experiment can read 940 files which will be extracted in the form of Microsoft Excel, HTML and PDF. The following are the results of the data obtained in this experiment with the cellphone in Non-Root conditions.

2.Roots

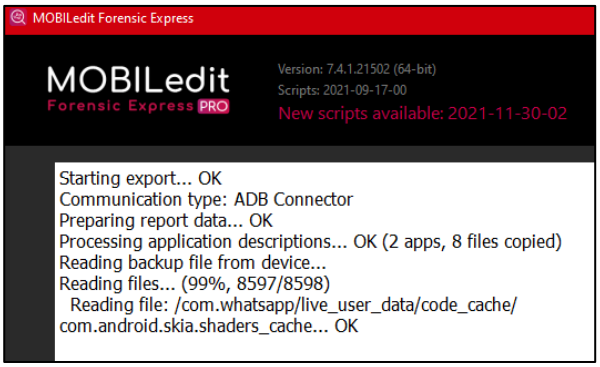


Figure 4. Data Acquisition Process

It can be seen in Figure 4 that the data acquisition process in this experiment can read 8598 files which will be extracted in the form of Microsoft Excel, HTML and

PDF. The following are the results of the data obtained in this experiment with the cellphone in Non-Root conditions.

4.C. examination

1. Non-Root

Table 2. MOBILEdit data results

No.	Results	Instagram	WhatsApp
1	Messages/Text	Not found	Not found
2	Images/Images	Not found	Found
3	Videos	Not found	Found

Based on Table 2, the results of examining data using MOBILedit on non-rooted phones found very little and could even be said to be empty because nothing was found on Instagram and on WhatsApp only the data store.

So the researchers decided to try another method, namely by cloning data from a non-rooted cellphone to a flash disk, then a disk image file would be created using the FTK Imager forensic application, and the disk image file would be analyzed using the Autopsy forensic application. Here are the results obtained.

Table 3. Autopsy data results

No.	Results	Instagram	WhatsApp
1	Messages/Text	Found	Not found
2	Images/Images	Not found	Found
3	Videos	Not found	Found

Based on Table 3, the results of the data from the Autopsy application were successful in finding text on Instagram. While on WhatsApp get the same results as before. Furthermore, these results will be analyzed with the scenarios that have been made in order to get conclusions.

2.Roots

Table 4. MOBILedit data results

No.	Results	Instagram	WhatsApp
1	Messages/Text	Found	Not found
2	Images/Images	Found	Found
3	Videos	Found	Found

Based on Table 4, the results of examining data on a rooted cellphone get better results than the previous non-root experiment using MOBILedit, it's just that WhatsApp for Messages/Texts is still not found. This can be due to the high level of security from WhatsApp messages or other factors. Based on these results, researchers will try other forensic applications so that Messages/Texts on WhatsApp are found and get maximum results. The forensic applications are Autopsy, and FTK Imager.

The Autopsy application uses a physical image in this experiment. To create a physical image, you can use the MOBILedit application using a rooted cellphone so that the "Create physical image" button appears. Meanwhile, the FTK Imager application also uses a physical image. The following are the results obtained from the Autopsy and FTK Imager applications.

Table 5. Autopsy data results

No.	Results	Instagram	WhatsApp
1	Messages/Text	Found	Found
2	Images/Images	Found	Found
3	Videos	Found	Found

Table 6. FTK Imager data results

No.	Results	Instagram	WhatsApp
1	Messages/Text	Found	Found
2	Images/Images	Found	Found
3	Videos	Found	Found

Based on Tables 5 and 6, the results of data acquisition in the Autopsy and FTK Imager applications get the same results. It's just that on Instagram, videos are found but cannot be played, because the video file is in the .exo format which means that the file is damaged or cut into several parts.

4.D. Documenting & reporting

The final stage of digital forensic analysis based on the NIJ method published in April 2004 with a report entitled "Forensic Examination of Digital Evidence: A Guide for Law Enforcement" is the Documenting & reporting stage. After carrying out several stages of forensic analysis previously, it can be documented and reported that in searching for digital evidence of cyberbullying, both on cellphones in non-rooted or rooted conditions, researchers managed to find digital evidence according to the scope required, namely messages/text, images/pictures and videos. on the Instagram and WhatsApp applications.

The number of scenarios made, namely Instagram has 43 texts, 5 pictures, 5 videos and WhatsApp has 26 texts, 4 pictures, 3 videos. The following Table 7 results of the data according to the scenario.

Table 7. Instagram data results according to the scenario from Pomsel Non Root

No.	Results	Instagram (43 Text, 5 Images, 5 Videos)	
		MOBILedit	Autopsy
1	Messages /Text	Not found	Found 2 texts
2	Images	Not found	Not found
3	Videos	Not found	Not found

Table 8. WhatsApp data results according to the scenario from non-root phone

No.	Results	WhatsApp (26 Text, 3 Images, 3 Videos)	
		MOBILedit	Autopsy
1	Messages /Text	Not found	Not found
2	Images	Found 2 Fig	Found 2 Fig
3	Videos	Found 2 Videos	Found 2 Videos

Table 9. Instagram data results according to the scenario from root phone

No.	Results	Instagram (43 Text, 5 Images, 5 Videos)		
		MOBILedit	Autopsy	FTK Imager
1	Messages/Text	Found 20 Text	Found 43 Text	Found 39 Text
2	Images	Found 5 Fig	Found 5 Fig	Found 5 Fig
3	Videos	Not found	Not found	Not found

Table 10. WhatsApp data results according to the scenario from root phone

No.	Results	WhatsApp (26 Text, 3 Images, 3 Videos)		
		MOBILedit	Autopsy	FTK Imager
1	Messages/Text	Not found	Found 23 Text	Found 23 Text
2	Images	Found 2 Fig	Found 2 Fig	Found 2 Fig
3	Videos	Found 2 Videos	Found 2 Videos	Found 2 Videos

5. CONCLUSIONS AND RECOMMENDATIONS

Based on the results of the research that has been done, it can be concluded that the NIJ Method published in April 2004 with a report entitled "Forensic Examination of Digital Evidence: A Guide for Law Enforcement" was successfully applied to the forensic analysis process with the results of uncovering cases of Cyberbullying crimes on Instagram and WhatsApp. In accordance with the reporting according to the number of scenarios that were made, namely Instagram there were 43 texts, 5 images, 5 videos and WhatsApp there were 26 texts, 4 images, 3 videos that the results on the cellphone were in non-root conditions, in the MOBILedit application according to the scope of the problem, namely Instagram was not found anything and WhatsApp only found storage files, namely 2 Images, 2 Videos. While experiments on the Autopsy forensic application, got the result that Instagram found 2 texts, 0 pictures, 0 Videos and WhatsApp found 0 Text, 2 Images, 2 Videos. So that researchers can conclude that results from cellphones in non-rooted conditions are not recommended in searching for digital evidence because they get very few results.

Furthermore, the results on a rooted cellphone, the MOBILedit application matches the scope of the problem, namely Instagram managed to find 20 texts, 5 images, 0 videos. The text messages are in the form of messages and post captions that have not been deleted, while comments and files that have been deleted cannot be found in this study. On WhatsApp, only obtaining storage files in the form of 2 images, 2 videos, for text messages is still not found in this study. Then the results of the Autopsy forensic application, which found almost all data according to the scenario created, namely on Instagram found 43 Texts, 5 Images, 0 Videos and on WhatsApp found 23 Texts, 2 Images, 2 Videos. Whereas for the forensic application FTK Imager, the results of the analysis are not much different from Autopsy, namely on Instagram found 39 texts, 5 images, 0 Videos and on WhatsApp found 23 Texts, 2 Images, 2 Videos. In addition, FTK Imager is difficult to read files, you have to use other forensic applications to find out the location of the file first so that it is easier to search for data.

After the researchers concluded that the forensic application in this study obtained almost all of the data, deleted data and was easy to read, namely Autopsy with a note that the cellphone was in a rooted condition.

Based on the research results and conclusions, here are suggestions from the author for further research, namely trying other forensic applications to try Instagram and WhatsApp applications in the search for digital evidence, trying other research objects besides Instagram and WhatsApp to find out the results of the differences and the last suggestion is to use the same research method. different so that you can find out the different paths of this research.

BIBLIOGRAPHY

ANWAR, N., & RIADI, I. (2017). Analisis Investigasi Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbasis Web. *Jurnal Ilmu Teknik Elektro Komputer Dan Informatika (JITEKI)*, *3*(1), 1–10.

BARUS, R. K. I. (2019). Korban Cyberbullying, Siapakah? *JURNAL SIMBOLIKA: Research and Learning in Communication Study*, *5*(1), 35. https://doi.org/10.31289/simbollika.v5i1.2301

BINTANG, R. A. K. N., UMAR, R., & YUDHANA, A. (2020). *Analisis Media Sosial Facebook Lite dengan tools Forensik menggunakan Metode NIST*. *21*(2), 125–130. http://jurnalnasional.ump.ac.id/index.php/Techno

Ditch the Label. (2017). *THE ANNUAL BULLYING SURVEY 2017*. https://www.ditchthelabel.org/research-papers/the-annual-bullying-survey-2017/

HARIANI. (2017). Analisis Bukti Digital Cyberbullying Pada Jejaring Sosial Menggunakan Naive Bayes Classifier (NBC). In *Yogyakarta, Maret, 2017*. Universitas Islam Indonesia.

HOOTSUITE (We are Social). (2022). Indonesian Digital Report February 2022. In *Datareportal.Com*.

https://datareportal.com/reports/digital-2021-indonesia

HUKUMONLINE.COM. (2019, May 9). *Cyberbullying, Pelajaran dari Kasus Amanda Todd*. https://www.hukumonline.com/berita/a/icyberbullying-i--pelajaran-dari-kasus-amanda-todd-lt5cd3dc51893bd

I G A AYU DEWI SATYAWATI, & SAGUNG PUTRI M. E PURWANI. (n.d.). *PENGATURAN CYBER BULLYING DALAM UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK*.

KINASIH, R. A., WIRAWAN MUHAMMAD, A., ADI PRABOWO, W., PANJAITAN NO, J. DI, KIDUL, P., PURWOKERTO SELATAN, K., & BANYUMAS, K. (2020). Analisis Keamanan Browser Menggunakan Metode National Institute of Justice (Studi Kasus: Facebook dan Instagram). *Jurnal Teknologi Informasi & Komunikasi*, *11*(x), 174–184. https://doi.org/10.31849/digitalzone.v11i2.4678ICCS

MERDEKA.COM. (2013, June 14). *Social media, tingkatkan risiko bunuh diri*. https://www.merdeka.com/teknologi/social-media-tingkatkan-resiko-bunuh-diri-part-2-sisi-hitam-jejaring-sosial.html

MOBILEDIT. (2021). *MOBILedit Forensic User Guide-MOBILedit Forensic Express 7.4*.

NATIONAL INSTITUTE OF JUSTICE. (2004a). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. In *Japanese Journal of Forensic Science and Technology* (Vol. 7, Issue 2). https://doi.org/10.3408/jafst.7.95

NATIONAL INSTITUTE OF JUSTICE. (2004b). *National Institute of Justice Annual Report 2004*. http://proxy.lib.sfu.ca/login?url=https://www.proquest.com/other-sources/national-institute-justice-annual-report-2004/docview/9791899/se-2?accountid=13800%0Ahttps://sfu-primo.hosted.exlibrisgroup.com/openurl/01SFUL/SFUL?url_ver=Z39.88-2004&rft_val_fmt=in

RISKI ARDININGTIAS, S. (2021). INVESTIGASI DIGITAL PADA FACEBOOK MESSENGER MENGGUNAKAN NATIONAL INSTITUTE OF JUSTICE. *JIP (Jurnal Informatika Polinema)* , *Volume 7*, *Edisi 4*(ISSN: 2614-6371 E-ISSN: 2407-070X), 19–26.

SAPUTRA, A. P., & WIDIYASONO, N. (2017). Analisis Digital Forensik pada File Steganography (Studi kasus : Peredaran Narkoba). *Jurnal Teknik Informatika Dan Sistem Informasi*, *3*(1), 179–190. https://doi.org/10.28932/jutisi.v3i1.594

SYAH, R., & HERMAWATI, I. (2018). The Prevention Efforts on Cyberbullying Case for Indonesian Adolescent Social Media Users. *Jurnal PKS*, *17*(2), 131–146. https://doi.org/10.31105/jpks.v17i2

UMAR, R., & SAHIRUDDIN. (2019). METODE NIST UNTUK ANALISIS FORENSIK BUKTI DIGITAL PADA PERANGKAT ANDROID. *Prosiding SENDI_U 2019*, *ISBN: 978-979-3649-99-3*, 124–130.

WIDIANDANA, P., IMAM RIADI, & SUNARDI. (2020). Implementasi Metode Jaccard pada Analisis Investigasi Cyberbullying WhatsApp Messenger Menggunakan Kerangka Kerja National Institute of Standards and Technology. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(6), 1046–1051. https://doi.org/10.29207/resti.v4i6.2635

YUDHANA, A., RIADI, I., ZUHRIYANTO, I., & DAHLAN, A. (2019). *Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS)*. *20*(2), 125–130. http://jurnalnasional.ump.ac.id/index.php/Techno