Web Forensics on Instagram Services using National Institute of Justice Method

Lina Julianti
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
The rapid development of technology has made people increasingly exchange information and make transactions through social media. One of the social media sites that can be used is Instagram. The use of the Instagram application can have a positive or negative impact. The number of Instagram users makes this application vulnerable to abuse, such as online scams among Instagram users. This research aims to obtain digital evidence of online shop fraud cases on Instagram that run on the Mozilla Firefox web browser and apply web forensics to Instagram services. The research object that will be discussed in this research is the Instagram application, which runs on the Mozilla Firefox web browser platform. This research implements the investigation process using the National Institute of Justice method. The National Institute of Justice method has five stages of research: preparation, collection, examination, analysis, and reporting. The tools used in this research are FTK Imager, Browser History Examiner, and HXD. The results of this research obtained results in the form of one username and one password used by the perpetrator to log into his Instagram account, the date and time of accessing Instagram, the web browser used, the cache image in the form of two images or posts that have been deleted by the perpetrator, 21 conversations, and one upload that has been deleted by the perpetrator.

Keywords
Digital Evidence, Instagram, Mozilla Firefox, National Institute of Justice (NIJ)

1. INTRODUCTION
The number of social media users in the world, especially in Indonesia, is increasing. Quoted from databoks.co.id Instagram is one of the most popular social media platforms in Indonesia, especially among young people. As of the first quarter of 2021, the number of active Instagram users worldwide reached 1.07 billion, of which 354 million were aged 25 to 34 years. The number of Instagram users in Indonesia until July 2021 was 91.77 million. The largest users are in the age group of 18–24 years, accounting for 36.4%. Instagram is the third-most-used social media platform after YouTube and WhatsApp [1]. Instagram is a social media platform that is used to send pictures and can be used to have conversations or chat, making it easier to communicate between fellow Instagram social media users [2]. Quoted from KOMPAS.com Instagram has a feature that allows users to upload photo and video content via a web browser on Mac and PC computers [3]. A web browser is a computer program that provides facilities for users to access the internet and store information in the form of URL history, search keywords, timestamps, and passwords [4]. One of the web browsers that can be used is Mozilla Firefox. Proper use of web browsers can make it easier to find any information on the internet, but along with the times the use of web browsers is now widely misused to commit crimes via the internet or known as cybercrime [5].

cybercrime is a result of the misuse of advances in information technology that utilise computers and internet networks [6]. One form of cybercrime is fraud through social media. Quoted from Liputan6.com throughout 2019, the Directorate of Cyber Crime of Bareskrim recorded 1,617 cases of online fraud, including 534 cases of online shop fraud through Instagram. The cases that are often encountered are fraud modes that use fake accounts by taking product photos from active Instagram online shops and committing fraud [7].

To prevent and overcome the occurrence of cybercrime cases, digital forensic analysis and methods are needed [8]. Digital forensics is one form of treatment carried out to reveal cybercrime problems [9]. According to Cahyadri (2021), digital forensics can assist investigators in conducting investigations to collect digital evidence and analyze the digital evidence [10]. The process of retrieving digital evidence can be done using several methods, namely the Integrated Digital Forensics Indentification Framework (IDFIF), the National Institute of Standards and Technology (NIST), the National Institute of Justice (NIJ), and the Digital Forensics Research Workshop (DFRWS). The four methods have different processes and work steps for obtaining digital evidence [11]. Based on the above problems, this research aims to obtain digital evidence of online shop fraud cases on social media platforms like Instagram, which runs on the Mozilla Firefox web browser, and implement web forensics on Instagram services using the National Institute of Justice (NIJ) method.

2. LITERATURE STUDY
2.1 Digital Forensics
Digital forensics is the application of computer science and technology for the benefit of legal evidence, in this case, to prove high-tech crimes or computer crimes scientifically to get digital evidence that can use to trap criminals [12]. Digital forensics is a forensic science that covers the recovery and investigation of materials found on digital devices, computers (hosts and servers), networks, and applications [13]

2.2 Digital Evidence
Digital evidence is information in the form of data sent or data stored using mobile devices or computers that can support or refute a particular crime and provide clues that lead to clues related to an offense [14]. Digital evidence relates to digital crimes, such as crimes using social media to commit crimes, so digital evidence can be used to assist in prosecuting all types of digital crimes [15].

2.3 Instagram
The term instagram comes from the word insta," which comes from the word instant," and the word "gram" comes from the

wordtelegram, with the workings of sending information quickly [16]. Instagram is an application that allows users to share photos, record videos, use digital filters, and share them on various social media services, including Instagram itself. Instagram is used to carry out activities such as sending images or photos, having conversations, or chatting that can facilitate communication between fellow Instagram social media users [2].

2.4 Cybercrime

Cybercrime is a crime related to technology, computers, and the internet [17]. Cybercrime refers to using computer networks in various ways to commit criminal acts by abusing the convenience of digital technology [18]. Cybercrime has several types, such as unauthorized access, illegal content, hacking and cracking, data forging, and bullying, intimidating or threatening others [13]. One form of cybercrime that is often found in society is online fraud cases through social media. This fraud can be carried out through social media such as Facebook, WhatsApp, Twitter, TikTok, and especially Instagram [19].

2.5 Web Browser

A web browser is a computer program that provides users with the facilities to read web pages of a computer [20]. Web browsers can store user browsing activities through visited URL information, downloaded files and images, cookies, caches, and other information [21]. Web browsers are also used to display and interact with files provided by web servers to obtain information provided by web servers [22] .

2.6 FTK Imager

FTK Imager FTK Imager is a review and imaging tool used to examine files and folders on challenging disk locations, CD/DVD, and network drives to find digital evidence quickly; FTK Imager can view and recover files that have been deleted from the recycle bin but have not been overwritten on the drive [23].

2.7 Browser History Examiner

Browser History Examiner is forensic software that captures web browser browsing history and reads and views data from the main desktop web browser. Browser History Examiner can capture, analyze, and report web browser browsing history. Browsers that support this software are Google Chrome, Microsoft Edge, Mozilla Firefox, and Internet Explorer [24]

2.8 HXD

HxD is a hex editor software or tool used to edit raw disks and modify RAM (Random Access Memory) and can handle files of various sizes. HDX has features such as search, replace, checksum, export, insert byte patterns, statistics, and file splitting [25].

3. RESEARCH METHODS

This research uses the National Institute of Justice (NIJ) method to implement the investigation process. The National Institute of Justice (NIJ) method consists of 5 stages: preparation, collection, examination, analysis, and reporting. The National Institute of Justice (NIJ) stages are described in Figure 1.

Figure 1 : National Institute Of Justice method.

Figure 1 shows the stages of the National Institute of Justice (NIJ) method. The preparation stage is preparing all the equipment used in conducting the investigation. The collection stage involves collecting evidence in files, documents, data, and physical evidence. The examination stage is the stage of examining the data obtained from the previous location. The analysis stage is the stage of analyzing the examination results. The reporting stage is the reporting of the results of the analysis that has been carried out.

4. RESULTS AND DISCUSSION

This research discusses the simulation of a crime or cybercrime case, namely the case of online shop fraud on the Instagram web. Case simulation is carried out in three stages. The first stage is pre-incident, the second is incident, and the third is post-incident. The pre-incident stage can be seen in Figure 2.

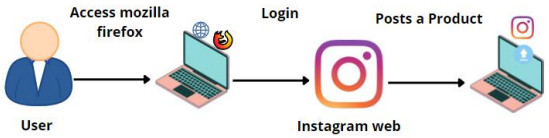

Figure 2 : Pre-Incident of Online Shop Fraud Case

Figure 2, the perpetrator uses a laptop and accesses the Mozilla Firefox web browser connected to the internet. The perpetrator logs into his Instagram account by entering the username or email and password used to log into his Instagram account. The perpetrator posts a product through his Instagram account, offering low prices and free shipping.

The second stage in the case simulation is the inside stage. The incident stage can be seen in Figure 3.

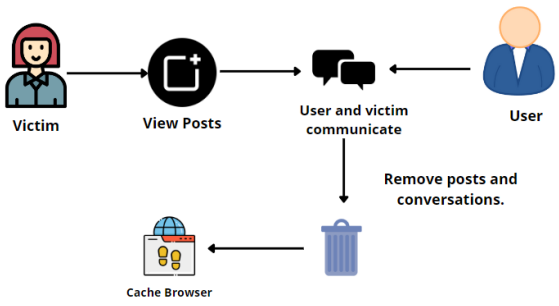

Figure 3 : Incident of Online Shop Fraud Case

Figure 3, the victim saw the post and felt interested and tempted by the price offered by the perpetrator, so the victim and the perpetrator communicated with each other by sending chats and pictures via Instagram. The perpetrator and the victim carried out product-buying and selling activities. After the successful

transaction, the perpetrator did not send the promised goods or products, and the perpetrator also deleted his posts and conversations with the victim.

The third stage in the case simulation is the post-incident stage. The post-incident stage can be seen in Figure 4.

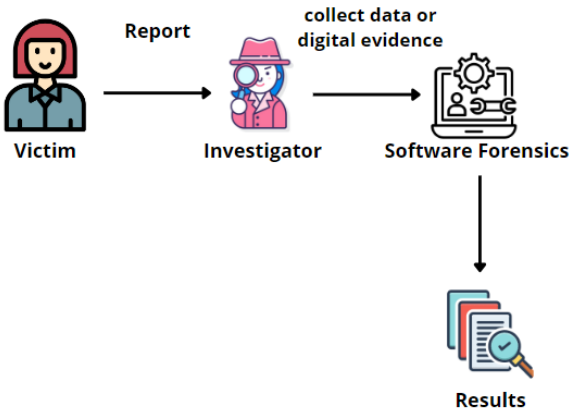

Figure 4 : Post-Incident Online Shop Fraud Case

Figure 4, victims who feel aggrieved report cases of online shop fraud by showing evidence of the perpetrator's account, posts, and proof of transfers that have been made by the victim as shown below, the victim explains the chronology of events that have been experienced, so that an exam.

4.1 Preparation

Preparation is done by preparing equipment or tools that will be used to obtain evidence. The tools that will be used can be seen in Table 1.

Table 1. Tools and Materials

No	Alat dan Bahan	Keterangan
1	Laptop	Prosesor 11th Gen Intel (R) Core (TM) i3-1115G4 @ 3.00GHz (4 CPUs), 3.00GHz, RAM 8.0 GB , SSD 512 GB
2	Instagram	Applications that are the object of research
3	FTK Imager	Applications used to lift digital evidence on laptops
4	HXD	Applications used to lift digital evidence on laptops
5	Browser History Examiner	Applications used to lift digital evidence on laptops laptop

Table 1 is the tools and materials used in this research. The tools and materials to be used are hardware and software. The hardware used is a laptop, and the software used is Instagram, FTK Imager, HXD, and Browser History Examiner.

4.1 Collection

This stage is carried out by collecting and securing physical evidence and collecting data. Physical evidence found is one laptop found in a lit state. Physical evidence can be seen in Figure 5.

Figure 5 : Physical Evidence

Figure 5 is evidence of one Asus laptop belonging to the perpetrator found in a lit state. The evidence found was carried out by a forensic process by capturing a memory or taking data from the laptop's RAM used by the perpetrator. FTK Imager and Browser History Examiner tools are used to capture the memory.

The RAM capture process stage uses the FTK Imager tool. FTK Imager performs memory capture or retrieves data and information. The memory capture feature can be seen in Figure 6.

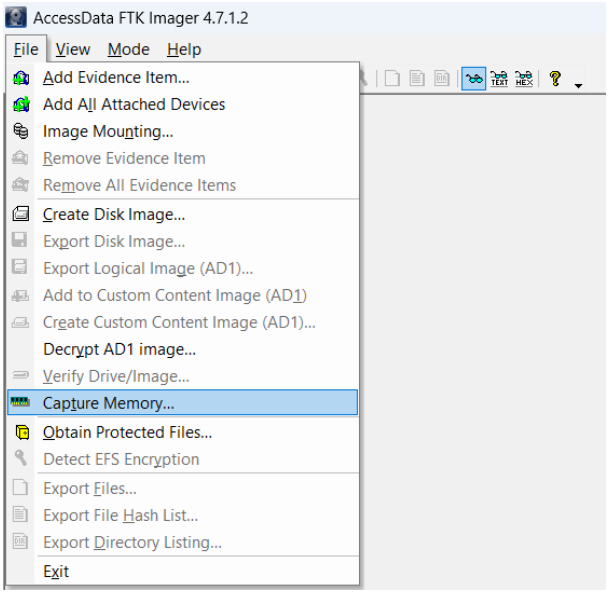

Figure 6 : FTK Imager Capture Memory feature

Figure 6 is the memory capture feature on FTK Imager. FTK Imager will retrieve data and information from all applications, including Instagram usernames and passwords on the device used. The results of the RAM capture process using the FTK Imager tool are files with the extension .mem. The capture file can be seen in Figure 7.

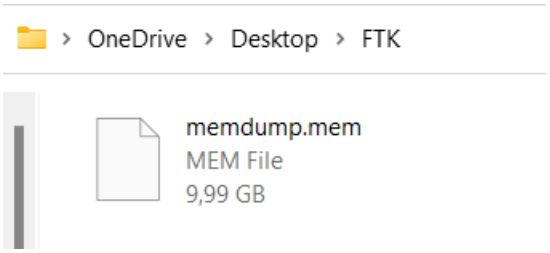

Figure 7 : FTK Imager Capture File

Figure 7 is the result of the RAM capture. The capture result file is 9.99 GB with the file name mem dump. Mem.

The stages of the search history capture process use the Browser History Examiner tool. This tool will take data from the Mozilla Firefox web browser. The Browser Examiner history capture process can be seen in Figure 8.

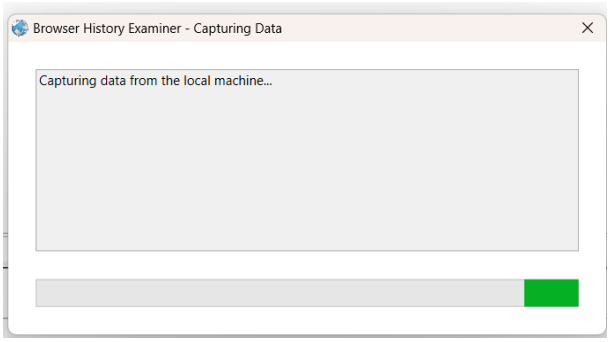

Figure 8 : Browser Examiner Capture History Process

Figure 8 is the Capture Browser History Examiner process. Browser History Examiner captures the browsing history of the Mozilla Firefox web browser. Browser History Examiner can capture, analyze, and report web browser browsing history. The capture results can be seen in Figure 9.

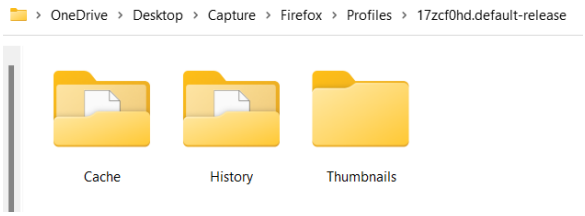

Figure 9 : Browser History Examiner Capture Result

Figure 9 shows the contents of the default-release folder, which contains the Cache, History, and Thumbnails folders. These three folders are the result of the capture process of the Mozilla Firefox web browser.

4.2 Examination

This stage is carried out in the process of checking the data that has been obtained previously. The examination is carried out on the data from the captured memory. Forensic tools are used to read the data that has been received, namely FTK Imager, Browser History Examiner, and HXD tools.

FTK Imager reads the data from the RAM capture results using the FTK Imager tool. FTK Imager will read the previous RAM capture data in the ".mem" format. The data found is the Instagram username and password of the perpetrator. The username perpetrator can be seen in Figure 10.

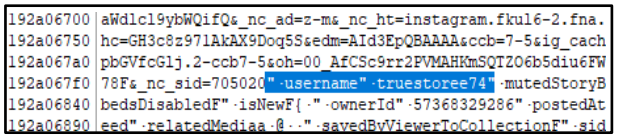

Figure 10 : Perpetrator's Instagram Username

Figure 10 shows the results of searching for the perpetrator's username using the FTK Imager tool. From the "username" keyword search results, the username the perpetrator used to log into his Instagram account is "truestroree74".

From the "password" keyword search results, the password used by the perpetrator to log into his Instagram account is obtained. The perpetrator's Instagram password can be seen in Figure 11.

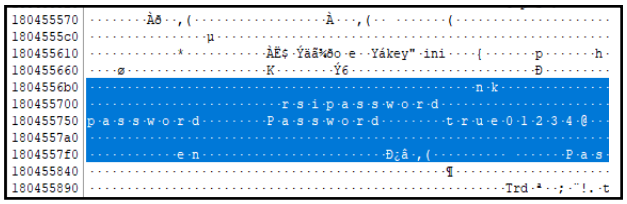

Figure 11 : Perpetrator's Instagram Password

Figure 11 shows the results of searching for the perpetrator's password. It can be seen that the password used by the perpetrator to log into his Instagram account is "true01234@".

Browser History Examiner will open the capture of browsing history on the Mozilla Firefox web browser. Browser History Examiner will display a graph of browsing activities performed by users. Browser History Examiner will show details of the data retrieved from the browser, such as date and time of access, URL, email, browser used from browsing history, loaded images, and pages that have been loaded.

Browser History Examiner displays the activities performed by the perpetrator. The action of the perpetrator can be seen in Figure 12.

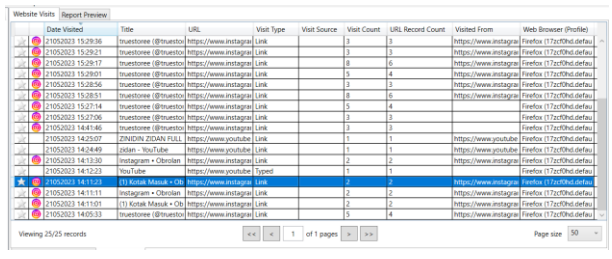

Figure 12 : Activity on Instagram Web

Figure 12 shows the activities carried out by the perpetrator on the Instagram web using the Mozilla Firefox web browser; the action was carried out on 21/05/2023, which led to chatting or chatting between the perpetrator and the victim. Browser History Examiner also displays the web page cache, which can be seen in Figure 13.

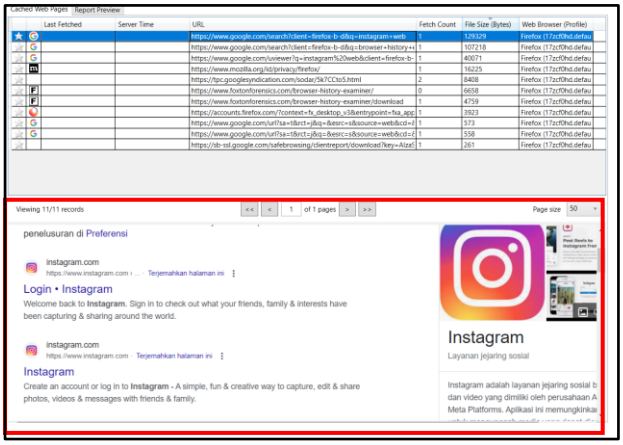

Figure 13 : Cache Web Page

Figure 13 is a Cache Web Page that displays evidence of searching the Instagram web using the Mozilla Firefox web browser. Evidence of searching Instagram web pages has been stored in the cache accessed by the perpetrator. Proof of the perpetrator's post can be seen in the cached image. The cached image can be seen in Figure 14.

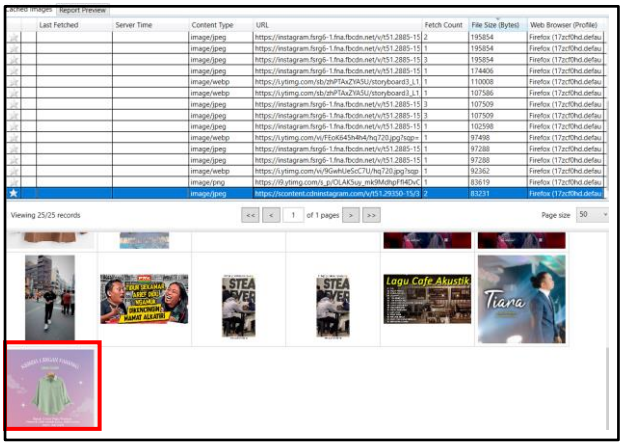

Figure 14 : Evidence of Offender Postings

Figure 14 shows an image loaded when the perpetrator accessed his Instagram. The *cached image* contains information in content type, URL, file size, and *web browser* used. In the *cached image*, two shots of shirts were found that had been posted by the perpetrator on his Instagram account. The picture seen is the same as the image ordered by the victim, namely a long-sleeved shirt. The other two ideas cannot be found by this tool.

The examination stage uses Forensic tools, namely HXD. HXD Tools will read the dump data from the Mozilla Firefox device used by the perpetrator. The dumping result file can be seen in Figure 15.

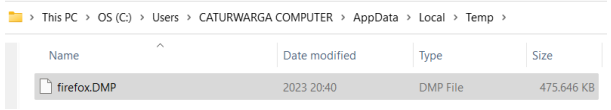

Figure 15 : Dumping Result File

Figure 15 is the dumped file, with the file name Firefox.DMP, with a file size of 475,646 KB. This file will be opened using Forensic tools, namely HXD, to find information in the form of conversation text between the perpetrator and the victim and look for the perpetrator's upload in the form of deleted text. Evidence of the perpetrator's upload can be seen in Figure 16.

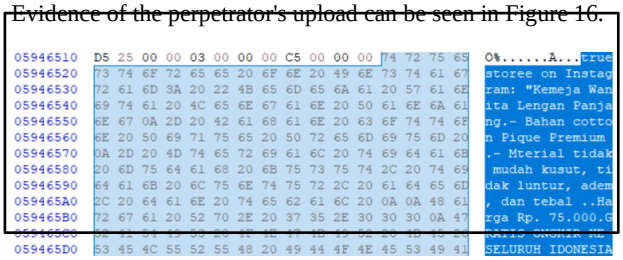

Figure 16 : Evidence of Offender Uploads

Figure 16 shows the discovery of evidence of the perpetrator's upload on his Instagram account, which wrote, "Long Sleeve Women's Shirt, Premium Cotton Pique Material, Material is not easily wrinkled, does not fade, cool and thick, Price Rp.75,000, Free Shipping Throughout Indonesia".

Other evidence found by HXD tools is evidence in the form of a conversation between the perpetrator and the victim that the perpetrator has deleted. Evidence of the conversation can be seen in Figure 17.

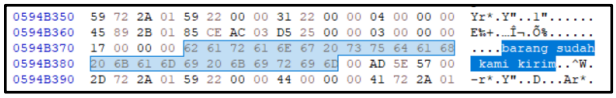

Figure 17 : Evidence of the Perpetrator's Conversation

Figure 17 is one of the evidence of conversations that have been deleted by the perpetrator on his Instagram, found using HXD too.

4.3 Analysis

4.4.1 FTK Imager Analysis

Based on the examination results that have been carried out using the FTK Imager tool, evidence is found in usernames and passwords used by the perpetrator to log into his Instagram account. The username and password can be seen in Table 2.

Table 2. FTK Imager Tools Results

Information	Results	Description
Username	Truestoree74	Found
Password	True01234@	Found

Table 2 is evidence obtained using the FTK Imager tool. FTK Imager tools receive a proof in the form of the perpetrator's Instagram username and password. The username found is Truestoree74, and the password is True01234@.

4.4.2 Browser History Examiner Analysis

Based on the results of the examination that has been carried out, the Browser History Examiner tool can find evidence in the form of website visit history, such as the date and time of accessing Instagram, namely on 05/25/2023, the victim and the perpetrator chat via Instagram, the web browser used by the perpetrator is mozilla firefox. Browser History Examiner also shows the results of the cached image in the form of two pictures of shirts that have been posted by the perpetrator on his Instagram account. The image found is the same as the image of the sweater ordered by the victim, but this tool cannot

capture the other two posts and proof of transfer in the form of ideas.

4.4.3 HXD Analysis

Based on the examination results that have been carried out using the HXD tools, evidence is found in the conversation between the victim and the perpetrator and proof of the perpetrator's uploads on his Instagram account. The contents of the conversation can be seen in Table 3.

Table 3. Content of Conversations and Posts

Information	Content of conversation	Description
Conversation	Is the shirt ready?	Found
Conversation	ready	Found
Conversation	What colour options are there?	Found
Conversation	for this one, all the colours are ready	Found
Conversation	okay, please fill in the order format yes	Found
Conversation	Order Format: Name : Size: Color: Quantity: Address No.Hp: Goods Cannot be Canceled 1	Found
Conversation	Order Format: Name : Kikio Size: L Color : black, white, blue Quantity : 3 Address: Umbulharjo IV, warungboto village, RT 31 RW 008, 870h. Gang Mukmin No.Hp: Goods Cannot be Canceled 1	Found
Conversation	total payment 225 yes ka, please make payment through account 477301014725530	Found
Conversation	has it been sent or not	Found
Conversation	Already	Found
Conversation	ka barang yes, how come it hasn't arrived yet	Found
Conversation	has it been shipped or not	Found
Conversation	Already	Found
Conversation	ka barang yes, how come it hasn't arrived yet	Found
Conversation	we have sent the goods	Found
Conversation	Hasn't the item arrived yet?	Found
Conversation	You?	Found
Upload	Long Sleeve Women's Shirt, Premium Cotton Pique Material, Material is not easy to wrinkle, does not fade, cool and thick, price Rp.75,000. Free Shipping Throughout Indonesia	Found

Table 3 shows the evidence that has been obtained using the HXD tool. HXD tools can find proof through conversations and uploads that the perpetrator has deleted. There are 20 conversations and one upload of the perpetrator.

4.4 Reporting

This report contains the results or digital evidence in the case of online shop fraud on the Instagram web found using forensic tools, namely FTK Imager, Browser History Examiner, and HXD. The physical evidence found in this study is one laptop unit with the following details:

Device Name : Laptop ASUS VivoBook

Processor : Intel ®Core ™ i3-1115g4 @3.00GHz (4 CPUs)

RAM :8.0 GB

SSD : 512 GB

Information obtained on physical evidence found, namely laptops that have been examined and analyzed, brought digital evidence, which can be seen in Table 4. The results found using the FTK Imager, Browser History Examiner, and HXD tools, using the National Institute Of Justice method, can be seen in Table 4.

Table 4. Outcome Identification

Identification Result	FTK Imager	Browser History Examiner	HXD	Total
Username	✓	-	-	1
Password	✓	-	-	1
Web Visit History (Date and time of event, web browser used)	-	✓	-	1
Deleted conversations between the perpetrator and the victim	-	-	✓	21
Deleted image post	-	✓	-	2
Deleted post (text)	-		✓	1
Account number of the perpetrator			✓	1
Proof of Transfer	-	-	-	-

Table 4 is digital evidence found from online shop fraud cases on the Instagram web using three forensic tools. FTK Imager tools can find digital proof through the usernames and passwords the perpetrator uses to enter his Instagram account. Browser History Examiner tools find digital evidence in the record of web visit history (date and time of the incident and the web browser used, as well as posts in the form of images deleted by the perpetrator, but these tools cannot identify or find evidence in the form of proof of transfer images sent by the victim. HXD tools find digital evidence in the record of evidence in the form of conversations or chats between the perpetrator and the victim, and these tools also find digital proof in the form of the perpetrator's uploads in the form of text promoting the products he offers, as well as the perpetrator's account number.

5. CONCLUSIONS

Based on the results of research entitled "Web Forensics on Instagram Services Using the National Institute of Justice Method," it can be concluded that the National Institute of Justice method can be used in the Instagram web forensics process to obtain digital evidence of online shop fraud cases through five stages, namely preparation, collection, examination, analysis, and reporting. The results obtained in this study are the username and password used by the perpetrator can be known or identified using the FTK Imager tools. Digital evidence that has been deleted can be found again using the Browser History Examiner tool in the form of a history of web visits (date and time of the incident and the web browser used, as well as posts in the form of images deleted by the perpetrator, but this tool cannot identify or find evidence in the form of proof images of transfers sent by the victim. The HXD tool obtains evidence through conversations or chats deleted by the perpetrator, the perpetrator's uploads in the form of text promoting the products he offers, and the perpetrator's account number.

6. REFERENCES

[1] "Inilah Negara Pengguna Instagram Terbanyak, Indonesia Urutan Berapa?," Aug. 03, 2021.

[2] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "1490-Article Text-2859-1-10-20190413," Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ), vol. 4, pp. 219–227, 2018.

[3] "Resmi, Pengguna Instagram Bisa 'Posting' Foto serta Video dari PC dan Mac ," Oct. 20, 2021.

[4] H. Y. Sarjimin, "Perbandingan Tool Forensik pada Mozilla Firefox Private Mode Menggunakan Metode NIST," 2021. [Online]. Available: http://jurnal.itg.ac.id/

[5] Vatqiah Nurul, "Forensik Digital Web Browser Berbasis Desktop pada Kasus Penipuan Online Shop Melalui Facebook Menggunakan Metode Live Forensik".

[6] D. Haryadi, Kebijakan integral penangulangan cyberporn di Indonesia. Semarang : Lima, 2012.

[7] "Berita Terkini, Kabar Terbaru Hari Ini Indonesia dan Dunia - Liputan6.com." https://www.liputan6.com/ (accessed Jun. 03, 2023).

[8] J. Elektronik et al., "Analisis Forensik Digital pada Aplikasi Twitter di Android sebagai Bukti Digital dalam Penanganan Kasus Prostitusi Online".

[9] N. Iman, A. Susanto, and R. Inggi, "Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review)," Jurnal Telekomunikasi dan Komputer, vol. 9, no. 3, p. 186, Jan. 2020, doi: 10.22441/incomtech.v9i3.7210.

[10] R. Cahyadri, Apa yang Harus Ditanyakan kepada Ahli Digital Forensics. Yogyakarta: CV Budi Utama, 2021.

[11] S. Sunardi, I. Riadi, and J. Triyanto, "Forensics Mobile Layanan WhatsApp pada Smartwatch Menggunakan Metode National Institute of Justice," JOINTECS (Journal of Information Technology and Computer Science), vol. 6, no. 2, p. 63, 2021, doi: 10.31328/jointecs.v6i2.2315.

[12] N. A. Muhammad, Digital forensik : Panduan praktis investigasi komputer. Jakarta : Salemba Infotek, 2012.

[13] A. Nofiyan and Mushlihudin, "Analisis Forensik pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST)," 2020.

[14] R. Umar and Sahiruddin, "Metode Nist Untuk Analisis Forensik Bukti Digital Pada Perangkat Android," Prosiding SENDU_U_2019, pp. 978–979, 2019.

[15] I. Riadi and A. Firdonsyah, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," 2017. [Online]. Available: https://www.researchgate.net/publication/317620078

[16] "About The Instagram Company." 2020.

[17] W. G. Kruse and J. G. Heiser, Computer forensics : incident response essentials. Addison-Wesley, 2001.

[18] M. Alfian, "Penguatan Hukum Cyber Crime di Indonesia dalam Perspektif Peraturan Perundang-Undangan," Kosmik Hukum, 2017.

[19] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," Elinvo (Electronics, Informatics, and Vocational Education), vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.

[20] I. Journal of , T. Rochmadi, and J. Brawijaya No, "'Tri Rochmadi' LIVE FORENSIK UNTUK ANALISA ANTI FORENSIK PADA WEB BROWSER STUDI KASUS BROWZAR," 2018. [Online]. Available: https://ejournal.almaata.ac.id/index.php/IJUBI

[21] H. HARIANI, "Eksplorasi Web Browser Dalam Pencarian Bukti Digital Menggunakan Sqlite," Jurnal INSTEK (Informatika Sains dan Teknologi), vol. 6, no. 1, p. 66, 2021, doi: 10.24252/instek.v6i1.18638.

[22] Hastanti Rulia Puji, Purnama Bambang Eka, and Wardati Indah Uly, "Sistem Penjualan Berbasis Web (E-Commerce) Pada Tata Distro Kabupaten Pacitan," Indian Journal of Pure and Applied Mathematics, vol. 3, no. 2, pp. 549–557, 2015, doi: 10.1007/s13226-018-0284-5.

[23] "FTKImager - Exterro." https://www.exterro.com/ftk-imager (accessed Jun. 07, 2023).

[24] "Browser History Examiner - Analyse & report on web browser activity." https://www.foxtonforensics.com/browser-history-examiner/ (accessed Jun. 05, 2023).

[25] "HxD - Freeware Hex Editor and Disk Editor | mh-nexus." https://mh-nexus.de/en/hxd/ (accessed Jun. 07, 2023).