Website Forensic Analysis on Application X for Online Prostitution Cases using National Institute of Justice Method

Jingga Musfita Maharani Rustam
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

The increasing use of social media has made communication easier but also opened opportunities for misuse, such as online prostitution. The web-based X application is one of the platforms exploited by perpetrators to operate covertly. This study aims to obtain digital evidence to support investigations by uncovering traces of the perpetrator's activities through forensic analysis. The method applied follows the National Institute of Justice (NIJ) model, which consists of five stages: preparation, collection, examination, analysis, and reporting. Data collection was carried out through the acquisition of digital data from the perpetrator's device, followed by the examination of metadata, cache, and hidden files. The analysis focused on conversations, uploaded images, and activity history on the X application. The results show that FTK Imager successfully revealed the perpetrator's username and four promotional text posts. Browser History Examiner extracted access history to X, two deleted images, and one transfer proof image. HxD recovered 19 deleted conversations, including price negotiations and bank account details. These findings confirm that digital forensic approaches are effective in supporting the investigation and substantiation of web-based social media crimes.

Keywords

Digital Evidence, Online Prostitution, X, National Institute of Justice (NIJ)

1. INTRODUCTION

The rapid advancement of information technology has significantly increased the use of social media as a means of communication and online interaction. These platforms allow users to share information, communicate, and express themselves through text, images, audio, and video formats [1][2]. According to the 2023 report by We Are Social, the number of active social media users in Indonesia reached 13 million, representing approximately 49.9% of the national population. The most widely used platforms include WhatsApp, Instagram, Facebook, TikTok, Telegram, and X (formerly Twitter) [3].

X has emerged as one of the most popular social media platforms in Indonesia, with 27.05 million users recorded as of October 2023, ranking fourth globally [3],[4]. Its core feature, which enables users to share short public status updates, makes it an effective tool for rapid information dissemination. However, this ease of use also facilitates misuse, including covert online prostitution activities carried out through private messages or symbolic posts and coded secret deceptive language [5],[6].

Online prostitution refers to the exchange of sexual services via digital media, where social media platforms serve as promotional tools for pimps, commercial sex workers (CSWs), and clients. A notable case occurred in May 2024, involving the exploitation of minors through X and Telegram, which were used as the primary channels for communication and service promotion [7]. Other studies have found that prostitution conducted through X often yields higher income compared to other platforms [8]. The impact of online prostitution extends beyond the perpetrators and clients, posing threats to social structures and contributing to increased criminal activity.

Previous studies have demonstrated that digital forensic investigations can effectively uncover hidden conversations and data related to such illegal activities. For instance, Wira Tama et al. applied the NIJ method along with Mobile Forensic Express to extract evidence of prostitution-related conversations from the Twitter application [9]. Similarly, Yudharta et al. and Fanani et al. reported the effectiveness of various forensic tools in retrieving evidence from social media platforms such as X and MiChat [10],[11],[12].

Online prostitution is a form of cybercrime supported by digital technology and the internet. It is one of the negative effects of the Internet of Things, where interactions no longer require physical presence [13]. This study examines the communication between perpetrators and clients on the X platform and explores how hidden information is shared. The research uses the NIJ method, which consists of five structured stages: Preparation, Collection, Examination, Analysis, and Reporting [14].

2. LITERATURE STUDY

2.1 Digital Forensics

Digital forensics is a branch of forensic science that focuses on the investigation and analysis of data on electronic devices, particularly in relation to computer crime. Originally, the term was synonymous with computer forensics, but it now encompasses the examination of a wide range of devices that store digital data. Digital forensics is important because data on devices is often locked, deleted or hidden, requiring specialised techniques for recovery and analysis. In general, digital forensics involves the recovery, collection and examination of material found on digital devices, computers, networks and applications [15].

The digital forensics process includes the stages of seizure, acquisition, analysis of digital media, and preparation of reports based on the evidence found. From a legal perspective, the obtained electronic documents must fulfil the requirements in order to be used as valid evidence, not only in criminal trials, but also in investigations and other judicial proceedings. Without the application of digital forensic methods, the validity of electronic evidence cannot be guaranteed [16].

2.2 Digital Evidence

Digital forensics and digital evidence are two interrelated concepts, but have different definitions. Digital evidence refers to data collected from various digital storage media that can be analysed using computer forensic methods. Thus, any information in the form of digital data can be the object of investigation and serve as evidence as long as it fulfils the requirements of authenticity and integrity [17].

Digital evidence includes data transmitted or stored via computer or mobile devices, which can be used to support or refute involvement in a crime, as well as provide clues to the offence. However, this evidence is fragile and susceptible to damage or loss if not handled properly [18].

2.3 X

X is a social networking and microblogging service that allows users to send and read short messages (tweets) with a limit of up to 280 characters. It was founded in 2006 in San Francisco by Jack Dorsey, Noah Glass, Biz Stone, and Evan Williams. Originally, X was designed for sharing statuses via SMS, but has now evolved into one of the most popular social media platforms with many additional features. As a form of online microblogging, X allows users to share information in text, image, video, and audio formats. Users can share their thoughts, current news, or daily activities through tweets that are easy to access and consume [5].

In addition to publishing tweets, X provides interaction features, such as the "like" button (heart icon), "retweet" (circular arrow icon) to reshare tweets, and the quote tweet option to add comments to retweets. These features support dynamic interaction between users and accelerate the dissemination of information on social networks. Fauzi, Siti, and Maud's research shows that X facilitates the dissemination of information very quickly, thus triggering discussions and the formation of broad public opinion [19].

2.4 Online Prostitution

Online prostitution is a form of prostitution that utilises the internet or social media as a means of transaction. This phenomenon has been an unresolved social problem for a long time. In Indonesia, prostitution is seen as an act that violates the law, social norms, and human rights [20],[21]. In practice, commercial sex workers (CSWs) use social media to promote themselves and communicate with potential customers freely. Research shows that online prostitution on platform X tends to offer higher prices and income than other forms of prostitution [8].

2.5 Digital Forensic Tools

In digital forensic investigations, various software (tools) are used that have different functions according to the type of analysis being carried out. Some commonly used tools include:

2.5.1 Browser History Examiner (BHE)

Browser History Examiner is forensic software designed to capture and analyse the history of browsing activity on web browsers. BHE supports the acquisition, extraction, and visualisation of history data from popular browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge. The information collected includes visited URLs, access times, page titles, and keywords typed by users. Efficient search and filtering features allow investigators to accurately track user activity, which is helpful in browsing activity-based investigations [22].

2.5.2 FTK Imager

FTK Imager is one of the forensic tools that supports various file formats and operating systems, and is able to extract deleted or hidden data. This tool can examine directory structures, view file headers, and restore deleted files. FTK Imager is used to ensure the integrity and validity of electronic evidence through the process of acquiring data from hard disks and network drives quickly and systematically [23],[24].

2.5.3 HxD

HxD is a hexadecimal editor used to read and modify raw data, either from storage media or main memory (RAM). In the context of digital forensics, HxD is useful for accessing temporary data, including conversations (chats) that are not directly visible on the operating system. Important features of HxD include hexadecimal data search, checksum calculation, statistical analysis, and file splitting. With these capabilities, HxD enables researchers to find and extract digital evidence such as conversations related to illegal activities temporarily stored in RAM [25].

2.6 National Instate of Justice (NIJ)

The National Institute of Justice (NIJ) method is a systematic approach to digital forensic investigation that consists of five stages: Preparation, the identification of digital evidence and strategic planning; Collection, the retrieval of data from media while maintaining integrity; Examination, the process of extracting and organising data; Analysis, in-depth analysis to find evidence related to the case; and Reporting, the preparation of a report containing legally accountable procedures, tools, and findings.

3. RESEARCH METHOD

This research implements the static forensic method based on the National Institute of Justice (NIJ) stages, namely Preparation, Collection, Examination, Analysis, and Reporting Figure 1.

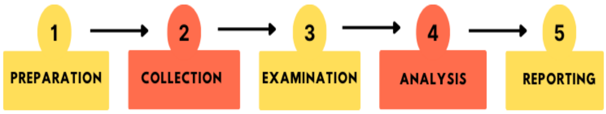


Figure 1 : Research Stages

As shown in Figure 1, the research stages from preparation to reporting. In the Preparation stage, the objectives and scope of the investigation were determined, focusing on uncovering digital evidence from the social media platform X. The case scenario involved the use of a laptop device as the primary medium, and three forensic tools were selected: FTK Imager for data acquisition and memory capture, Browser History Examiner (BHE) for browser artefact extraction, and HxD Hex

Editor for low-level memory analysis. In the Collection stage, forensic images were acquired from the target device, including a 34 GB RAM dump and browser history cache, while maintaining integrity using hash verification (MD5/SHA1). The Examination stage involved categorizing and verifying the collected artefacts, including login data, browser cache, deleted conversations, and promotional posts. The process was supported by FTK Imager to inspect volatile data, BHE to trace browsing history and cached images, and HxD to recover deleted conversations from process dumps. In the Analysis stage, evidence was interpreted by correlating communication records, browsing patterns, and metadata to reconstruct the offender's activities. This included identifying usernames, deleted promotional content, transfer proof, and negotiation details. Finally, the Reporting stage documented the entire investigation process in a structured format, including the tools, procedures, and findings, with screenshots, extracted logs, and tables to ensure that the results are comprehensive, objective, and legally accountable.

4. RESULTS AND DISCUSSION

The initial flow of online prostitution practices through web-based social media (X). The case started when a pimp accessed the Mozilla Firefox browser on a laptop, created an X account, and uploaded photos of women with veiled captions to offer prostitution services. This content attracts the attention of customers who then contact the pimp. Communication occurs via DM to negotiate services. After an agreement, a physical meeting occurs, and the pimp deletes posts and conversations to eliminate traces.

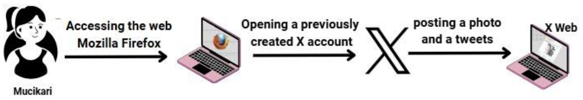

Mucikari
Accessing the web Mozilla Firefox
Opening a previously created X account
posting a photo and a tweets
X Web

Figure 2 : Pre Incident Prostitution Cases

As shown in Figure 2, the initial stage starting with the pimp accessing X through Mozilla Firefox, creating an anonymous account to disguise identity, then posting photos of women accompanied by captions with certain codes. This post aims to lure customers to contact the pimp.

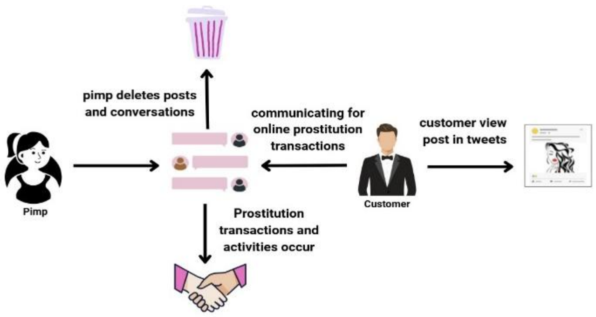

pimp deletes posts and conversations
communicating for online prostitution transactions
customer view post in tweets
Pimp
Customer
Prostitution transactions and activities occur

Figure 3 : Incident Prostitution Cases

As shown in Figure 3, after the post is viewed, the customer contacts the pimp via DM. They negotiate the rate, location, and time. After the agreement, the prostitution takes place physically. The pimp then deletes the digital footprint (post and conversation), but the metadata and cache can still be recovered using digital forensics.

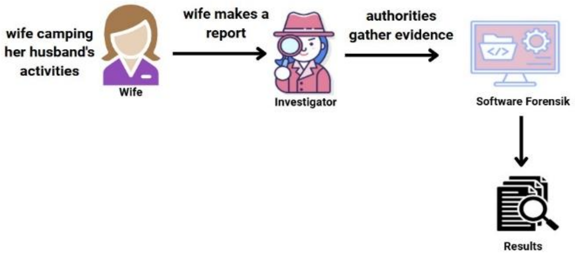

wife camping her husband's activities
Wife
wife makes a report
Investigator
authorities gather evidence
Software Forensik
Results

Figure 4 : Post Incident Prostitution Cases

As shown in Figure 4, the final stage involves a report from the customer's wife to the authorities. Investigators collected digital evidence using tools such as FTK Imager, Browser History Examiner, and HxD to recover conversations, browser history, and metadata files.

4.1 Investigation Preparation

The preparation stage in this research involves the use of several forensic software to support the process of identifying digital evidence in online prostitution cases through the X application accessed using the Mozilla Firefox browser. This process is carried out systematically to ensure that the evidence obtained has high integrity and validity.

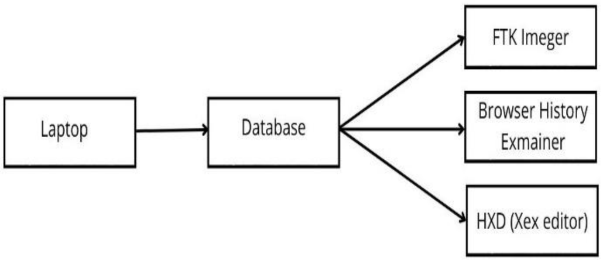


Figure 5 : Flow of Preparation Stage

As shown in Figure 5, the flow of digital forensic data collection and analysis in online prostitution cases. The data was collected through laptop hardware, then processed using FTK Imager, Browser History Examiner (BHE), and HxD Editor software.

4.2 Collection

The collection stage is carried out to secure physical evidence and digital data related to online prostitution cases through social media X. The physical evidence secured was a glossy white Asus Zenbook 14 UX3405MA laptop with a backlight keyboard, and a 65W TYPE-C charger. The device was found powered on, so to maintain the integrity of the evidence, a live forensic approach was taken before the device was switched off. This process aims to secure volatile data, such as memory (RAM), running processes, and active login sessions that could be lost if the device is switched off.

Data acquisition started with FTK Imager, which was used to perform memory capture (RAM dump). The capture file with the extension .mem with a size of 34 GB is stored in a secure directory and contains temporary data, such as login session, chat logs, browser activity artefacts, and the cache of X application. This data is crucial for finding traces of the perpetrator's illegal communications and activities. Afterwards, the Browser History Examiner (BHE) was used to extract the web browsing history, including history, cache and cookies from the Mozilla Firefox browser used by the perpetrator to access the X platform. This extraction reveals related browsing activity, including indications of access to login pages, content posting, and communication interactions with potential customers.

Table 1 : Specification of Evidence

Evidence	Brand	Processor	RAM	Storage
Laptop	Asus Zenbook UX3405M A	Intel® Core™ Ultra 7 155H	32GB	1TB M.2 NVMe™ PCIe® 4.0 SSD

As shown in Table 1, the evidence specification consists of an Asus Zenbook 14 UX3402 laptop with 32 GB of RAM and a 1 TB NVMe PCIe SSD, which supports large and fast data acquisition. The RAM capacity enables the retrieval of volatile data through memory forensics, while the SSD stores important digital artefacts.

The acquisition process was performed with FTK Imager through the following steps: memory capture, directory selection (memdump.mem file, size 34 GB), and storage in E:\Orange. This file contains activity data of the X app used for online prostitution, including logins, history, and conversations.

In addition, Browser History Examiner was used to extract the browsing history and cache from the browser (e.g. Mozilla Firefox). The steps include browser selection and data type, 2-3 minutes loading process, then the results are saved in the E:\Jingga\Capture directory. The analysis results showed a profiles folder structure with core data in the form of history, cache, and thumbnails that revealed case-related browsing activities.

4.3 Examination

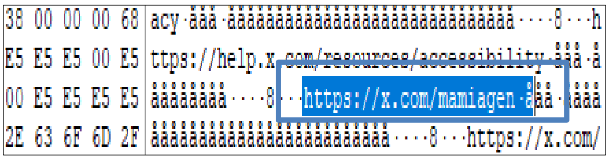
The examination stage was conducted on the digital data obtained through the acquisition process, especially the RAM capture, web browsing history, and browser application dump files. The analysis was conducted using three main software tools, namely FTK Imager, Browser History Examiner (BHE), and HxD Hex Editor.

All digital evidence was stored in the E:\Jingga directory as the main repository, which contains raw evidence and extraction results.

4.3.1 RAM Data Discovery with FTK Imager

The first step of the examination is to open the .mem memory capture file using FTK Imager. The process begins by selecting the Add Evidence Item menu, which allows the investigator to add digital evidence sources for analysis. The evidence type selected was Image File, as per the format of the RAM dump file obtained earlier. At this stage, the investigator browsed through the E:\Jingga directory to select the memory capture file, then loaded it into the FTK Imager interface.

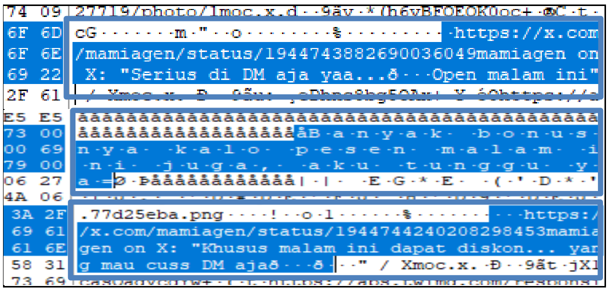
Once the file was successfully loaded, FTK Imager displayed a representation of the memory structure in hexadecimal and ASCII form, enabling a detailed search of the stored data chunks. An important feature used is Find, which supports keyword-based searches in both text and hexadecimal formats, and can be customised to specific encodings (ANSI, Unicode).



```
38 00 00 00 68 acy·ååå·åååååååååååååååååååååååååååå····8···h
E5 E5 E5 00 E5 ttps://help.x.com/resources/accessibility·ååå·å
00 E5 E5 E5 E5 åååååååå····8···https://x.com/mamiagen·ååå·åååå
2E 63 6F 6D 2F ååååååååååååååååååååååååååå····8···https://x.com/
```

Figure 6 : FTK Imager Search Results

As shown in Figure 6, the search result with the keyword "mamiagen" reveals traces of activity related to the X account used by the perpetrator. This finding includes a URL leading to the X site and the perpetrator's username, "mamiagen," which serves as the main digital identity.



```
74 09 27719/photo/1moc.x.d··9ãv·*(h6vBFOEOK0oc+·@C·t·
6F 6D cG·······m·"··o········%·········-https://x.com
6F 6E /mamiagen/status/1944743882690036049mamiagen on
69 22  X: "Serius di DM aja yaa...ð···Open malam ini"
2F 61
E5 E5 åååååååååååååååååååååååååååååååååååååååå
73 00 ååååååååååååååååååååB·a·n·y·a·k· ·b·o·n·u·s·
00 69 n·y·a· ·k·a·l·o· ·p·e·s·e·n· ·m·a·l·a·m· ·i
79 00 ·n·i· ·j·u·g·a·,· ·a·k·u· ·t·u·n·g·g·u· ·y·
06 27 a·=Ø·Þåååååååååååååå|·|· ·E·G·*·E· ·(·'·D·*·'
4A 06
3A 2F .77d25eba.png····!··o·1······%·······-··https:/
69 61 /x.com/mamiagen/status/1944744240208298453mamia
61 6E gen on X: "Khusus malam ini dapat diskon... yan
58 31 g mau cuss DM ajað···ð·|··" / Xmoc.x.·Ð··9ãt·jX1
73 69
```

Figure 7 : FTK Imager Discovery Evidence

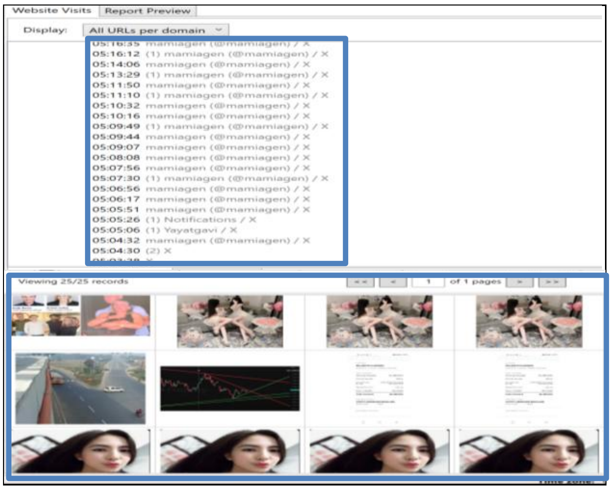
As shown in Figure 7, the evidence obtained through in-depth analysis reveals text uploads that had been deleted by the perpetrator but were still stored in memory data (cache). Some examples of successfully recovered uploads include:

- "Khusus malam ini dapat diskon… yang mau cuss DM aja."
- "Serius di DM aja yaa, open malam ini."
- "Aku kasih bonus deh buat yang book malam ini, cuss…"
- "Banyak bonusnya kalo pesen malam ini juga, aku tunggu yaa…"

These findings provide evidence that the perpetrators were actively promoting prostitution services through account X, despite trying to erase traces of the uploads. In-memory cache analysis proves that digital information is persistent, even after content is deleted at the application level.

4.3.2 Browser History Findings with Browser History Examiner

In addition to RAM data, web browsing history was also examined using Browser History Examiner (BHE). This tool is used to collect, extract and analyse digital artefacts from the Mozilla Firefox browser used by the perpetrator. The process starts with the Load History feature, then the investigator selects the history capture folder previously saved in E:\Jingga\Capture.



```
05:16:12 (1) mamiagen (@mamiagen) / X
05:14:06 mamiagen (@mamiagen) / X
05:13:29 (1) mamiagen (@mamiagen) / X
05:11:50 mamiagen (@mamiagen) / X
05:11:10 (1) mamiagen (@mamiagen) / X
05:10:32 mamiagen (@mamiagen) / X
05:10:16 mamiagen (@mamiagen) / X
05:09:49 (1) mamiagen (@mamiagen) / X
05:09:44 mamiagen (@mamiagen) / X
05:09:07 mamiagen (@mamiagen) / X
05:08:08 mamiagen (@mamiagen) / X
05:07:56 mamiagen (@mamiagen) / X
05:07:30 (1) mamiagen (@mamiagen) / X
05:06:56 mamiagen (@mamiagen) / X
05:06:17 mamiagen (@mamiagen) / X
05:05:51 mamiagen (@mamiagen) / X
05:05:26 (1) Notifications / X
05:05:06 (1) Yayatgavi / X
05:04:32 mamiagen (@mamiagen) / X
05:04:30 (2) X
```

Figure 8 : BHE Evidence Findings

As shown in Figure 8, the evidence indicates that BHE successfully extracted various important artefacts, including:

- Site visit history (URL visited) completes with timestamps.
- Search terms and the search engine used.
- Cached web pages and cached images.
- Login data, cookies, and form history.
- The analysis results show patterns of browsing activity relevant to the case, including:
- Access to website X on 19/07/2025 at 05:05:06 via Mozilla Firefox.
- Search for the keyword "X login" at 05:02:20.

Cache files containing X website pages, including images identical to the offender's account postings and proof of transfers sent via conversation. In addition, BHE provides a Detailed View that shows complete data such as URL, page title, number of visits, and browser information. An activity graph is also visualised to illustrate the intensity of site usage. The findings confirm that the offender used a browser to access site X, log in, and interact with customers, leading to online prostitution transactions.

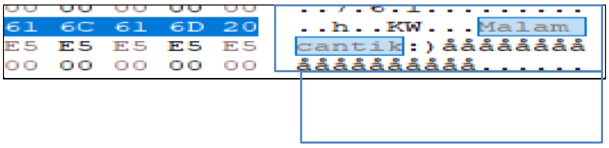
4.3.3 Firefox Dump File Findings with HxD

To strengthen the evidence, investigators created a dump file of the Firefox application process via Task Manager. This was done by selecting the Firefox process, then right-clicking and selecting the Create Dump File option, resulting in the firefox.DMP file stored in the temporary directory C:\Users\Zenbook\AppData\Local\Temp\firefox.DMP. This dump file has a size of ±751 MB, indicating that the copy of browser memory data is large enough to analyse.

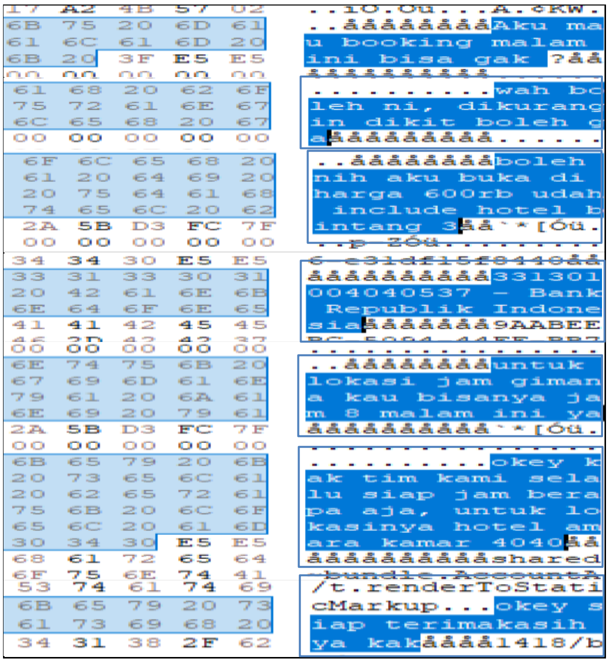
The firefox.DMP file was then analysed using the HxD Hex Editor, which displays the contents of the file in hexadecimal format. From the analysis results, digital artefacts such as:

- URLs pointing to X site.
- Snippets of text-based conversations.
- Cached data and residual browsing activity.

This analysis shows that even if data is deleted from the application, information can still be recovered from the application's process memory.



```
61 6C 61 6D 20    ..h..KW...Malam
E5 E5 E5 E5 E5    cantik:)åååååååå
00 00 00 00 00    ååååååååååå......
```



```
6B 75 20 6D 61    ..ååååååååååAku ma
61 6C 61 6D 20    u booking malam
6B 20 3F E5 E5    ini bisa gak ?åå
61 68 20 62 6F    ............wah bo
75 72 61 6E 67    leh ni, dikurang
6C 65 68 20 67    in dikit boleh g
00 00 00 00 00    aåååååååååå......
6F 6C 65 68 20    ..ååååååååååboleh
61 20 64 69 20    nih aku buka di
20 75 64 61 68    harga 600rb udah
74 65 6C 20 62     include hotel b
2A 5B D3 FC 7F    intang 3åå`*[Óü.
00 00 00 00 00    ..p Zóü..........
34 34 30 E5 E5    6 e31df15f8440åå
33 31 33 30 31    ååååååååååå331301
20 42 61 6E 6B    004040537 - Bank
6E 64 6F 6E 65     Republik Indone
41 41 42 45 45    siaååååååå9AABEE
00 00 00 00 00    ................
6E 74 75 6B 20    ..ååååååååååuntuk
67 69 6D 61 6E    lokasi jam giman
79 61 20 6A 61    a kau bisanya ja
6E 69 20 79 61    m 8 malam ini ya
2A 5B D3 FC 7F    ååååååååååå`*[Óü.
00 00 00 00 00    ...............
6B 65 79 20 6B    ............okey k
20 73 65 6C 61    ak tim kami sela
20 62 65 72 61    lu siap jam bera
75 6B 20 6C 6F    pa aja, untuk lo
65 6C 20 61 6D    kasinya hotel am
30 34 30 E5 E5    ara kamar 4040åå
68 61 72 65 64    ååååååååååååshared
6F 75 6E 74 41    bundle.AccountA
53 74 61 74 69    /t.renderToStati
6B 65 79 20 73    cMarkup...okey s
61 73 69 68 20    iap terimakasih
34 31 38 2F 62    ya kakåååå1418/b
```

Figure 9 : HxD Proof of Findings

As shown in Figure 9, the evidence from Hex Editor's HxD reveals a series of conversations between the perpetrator (the "mamiagen" account) and a customer, containing negotiations related to online prostitution transactions, including:

1) Initial conversation: The customer greets and makes a request, e.g. " malam cantik ", " bisa nggak book malam ini?".
2) Rate offer: The offender offers a price of IDR 600,000 including a 3-star hotel, indicating a service agreement.
3) Transaction approval: The customer requests an account number, the performer provides bank details, and the customer confirms the payment, including the remainder being paid in cash on site.
4) Meeting details: The offender sends the meeting time, which is 8pm at the address of Hotel Amara room 404, followed by a conversation about privacy and filling in the booking format.
5) Final confirmation: The customer provides the account name and date, the offender closes the conversation with " okeey siap terimakasih ya kakaa ".

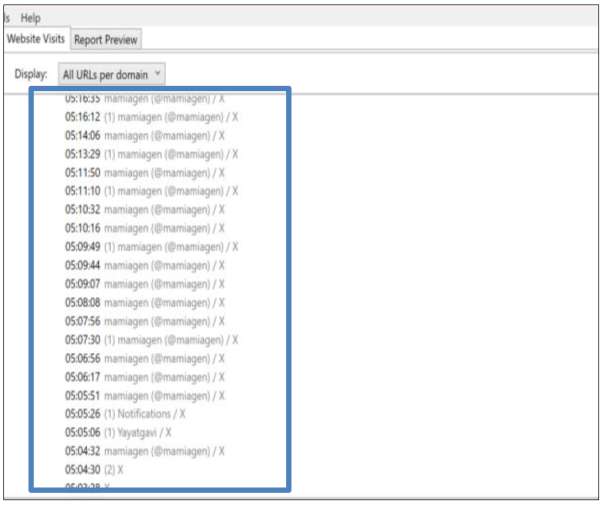
This conversation strengthens the evidence of the perpetrator's involvement in online prostitution through social media, as it includes all elements of the transaction: promotion, price negotiation, payment, and location.

4.4 Analysis

The analysis stage is an advanced process after examination, aiming to examine in depth the digital findings obtained previously. Analysis is carried out by utilising several forensic tools, namely FTK Imager, Browser History Examiner (BHE), and HxD, to identify important information that can corroborate allegations of perpetrator activity related to online prostitution.

4.4.1 Browser History Examiner Analysis

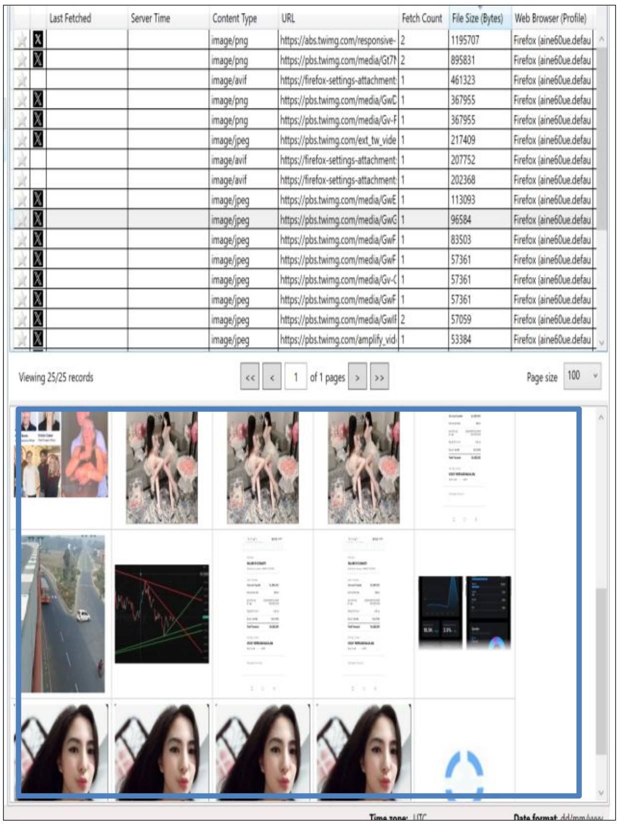
Browser History Examiner (BHE) successfully found a visit to the site on 19/07/2025 at around 05:00. From this data, the perpetrator accessed the X account with the username "@mameagen" repeatedly through the Mozilla Firefox browser. The time and date of access correspond with the conversation evidence that also occurred during the same timeframe, thereby strengthening the suspicion that the browsing activity is directly related to the communication conducted by the perpetrator. The activity log can be observed in Figure 10.



```
05:16:35 mamiagen (@mamiagen) / X
05:16:12 (1) mamiagen (@mamiagen) / X
05:14:06 mamiagen (@mamiagen) / X
05:13:29 (1) mamiagen (@mamiagen) / X
05:11:50 mamiagen (@mamiagen) / X
05:11:10 (1) mamiagen (@mamiagen) / X
05:10:32 mamiagen (@mamiagen) / X
05:10:16 mamiagen (@mamiagen) / X
05:09:49 (1) mamiagen (@mamiagen) / X
05:09:44 mamiagen (@mamiagen) / X
05:09:07 mamiagen (@mamiagen) / X
05:08:08 mamiagen (@mamiagen) / X
05:07:56 mamiagen (@mamiagen) / X
05:07:30 (1) mamiagen (@mamiagen) / X
05:06:56 mamiagen (@mamiagen) / X
05:06:17 mamiagen (@mamiagen) / X
05:05:51 mamiagen (@mamiagen) / X
05:05:26 (1) Notifications / X
05:05:06 (1) Yayatgavi / X
05:04:32 mamiagen (@mamiagen) / X
05:04:30 (2) X
```

Figure 10 : Activity Log and Cached Image Evidence

Analysis of cached images revealed images deleted by the perpetrator, including promotional posts uploaded via his X account and images of transfer receipts made during online prostitution. These images were stored in the browser cache, indicating that the perpetrator was actively uploading or viewing promotional content for the service. The cached images can be seen in Figure 11.



		Last Fetched	Server Time	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser (Profile)
☆	X			image/png	https://abs.twimg.com/responsive-	2	1195707	Firefox (aine60ue.defau
☆	X			image/png	https://pbs.twimg.com/media/Gt7N	2	895831	Firefox (aine60ue.defau
☆				image/avif	https://firefox-settings-attachment:	1	461323	Firefox (aine60ue.defau
☆	X			image/png	https://pbs.twimg.com/media/GwD	1	367955	Firefox (aine60ue.defau
☆	X			image/png	https://pbs.twimg.com/media/Gv-F	1	367955	Firefox (aine60ue.defau
☆	X			image/jpeg	https://pbs.twimg.com/ext_tw_vide	1	217409	Firefox (aine60ue.defau
☆				image/avif	https://firefox-settings-attachment:	1	207752	Firefox (aine60ue.defau
☆				image/avif	https://firefox-settings-attachment:	1	202368	Firefox (aine60ue.defau
☆	X			image/jpeg	https://pbs.twimg.com/media/GwE	1	113093	Firefox (aine60ue.defau
☆	X			image/jpeg	https://pbs.twimg.com/media/GwG	1	96584	Firefox (aine60ue.defau
☆	X			image/jpeg	https://pbs.twimg.com/media/GwF	1	83503	Firefox (aine60ue.defau
☆	X			image/jpeg	https://pbs.twimg.com/media/GwF	1	57361	Firefox (aine60ue.defau
☆	X			image/jpeg	https://pbs.twimg.com/media/Gv-(	1	57361	Firefox (aine60ue.defau
☆	X			image/jpeg	https://pbs.twimg.com/media/GwF	1	57361	Firefox (aine60ue.defau
☆	X			image/jpeg	https://pbs.twimg.com/media/GwlF	2	57059	Firefox (aine60ue.defau
☆	X			image/jpeg	https://pbs.twimg.com/amplify_vid	1	53384	Firefox (aine60ue.defau

Figure 11 : Cache Image

4.4.2 FTK Imager Analysis

FTK Imager was used to analyse the RAM capture memory file. A search with the keyword "mamiagen" successfully identified the username of the perpetrator's X account. In addition, four promotional text posts were found that had been deleted, but were still stored in memory.

Table 2 : FTK Imager Analysis Results

Information	Result	Description
Username/Account name	mamiagen	Found
Text upload 1	Aku kasih bonus deh buat kamu yang book aku sekarang	Found
Upload text 2	Banyak bonusnya kalo pesan malam ini juga, aku tunggu ya	Found
Upload text 3	Khusus malam ini dapat diskon...yang mau cuss DM aja	Found
Upload text 4	Serius di DM aja ya...Open malam ini	Found

As shown in Table 2, the findings from FTK Imager confirm the identity of the perpetrator's account and prostitution promotion activities conducted through social media X.

4.4.3 HxD Analysis

HxD was used to analyse the firefox.DMP file, which is a memory dump of the Firefox process. The analysis revealed direct conversations between the perpetrator and customers, including price negotiations, requests for account numbers, and confirmation of meeting locations.

Table 3 : Conversation Analysis Results (HxD)

Information	Conversation Content	Description
Conversation 1	Malam cantik	Found
Conversation 2	Malammm :)	Found
Conversation 3	Aku mau book malam ini bisa nggak?	Found
Conversation 4	Aku bisa dapat harga berapa buat malam ini?	Found
Conversation 5	Boleh nih aku buka di harga 600 rb udah include hotel bintang 3	Found
Conversation 6	Wah boleh nih, dikurangin dikit boleh nggak?	Found
Conversation 7	Kan dipostingan banyak bonusnya	Found
Conversation 8	Boleh deh buat kamu, cust pertamaku buat malam ini	Found
Conversation 9	Aku kasih 500 aja	Found
Conversation 10	Mantap banget nih, oke bisa kirim norek nya ya langsung aku tf	Found
Conversation 11	331301004040537 - Bank Republik Indonesia	Found
Conversation 12	sisanya aku kasih cash in room ya	Found
Conversation 13	Wahhh terimakasih kak	Found
Conversation 14	Untuk lokasi jam gimana aku bisanya jam 8 malam ini ya	Found
Conversation 15	Okey kak tim kami selalu siap jam berapa aja, untuk lokasi hotel Amara 404	Found
Conversation 16	Mantap banget privacy aman yah	Found
Conversation 17	Wkwkw pastinya, oh iya tolong isi format pemesanan nama dan tanggal order ya	Found
Conversation 18	Nama akun X yayatgavi, tanggal pesan 19 juli 2026 jam 8 malam	Found
Conversation 19	Okey siap terimakasih kak	Found

As shown in Table 3, a summary of the successfully recovered conversations is presented. This analysis strengthens the evidence that the conversations included rate negotiations (IDR 600,000), facility details (a 3-star hotel), the perpetrator's account number, and location information (Amara Hotel, room 404). These data provide strong evidence of the perpetrator's involvement in online prostitution activities.

4.5 Reporting

This reporting phase presents the results of the identification of digital evidence found in the online prostitution case through platform X. The investigation process was conducted using three forensic tools, namely FTK Imager, Browser History Examiner (BHE), and HxD Hex Editor, which were applied according to the National Institute of Justice (NIJ) method. The examination was conducted on one unit of Asus ZenBook laptop with the following technical specifications: Intel® Core™ Ultra 7 Processor 155H (1.4 GHz), 32GB LPDDR5X RAM, 1TB M.2 NVMe™ PCIe® 4.0 SSD Storage, and Windows 11 Pro Operating System.

The results of the digital investigation show a direct link between the perpetrator's activities and the practice of online prostitution. A summary of the findings of the digital evidence is shown in the Table 4.

Table 4 : Classification and Identification of Research Results

Identification Result	FTK Imager	BHE	HxD	Total
Username	✓	-	-	2
Browsing History (Date & Time)	-	✓	-	3
Deleted conversations (chats)	-	-	✓	19
Deleted posts (images)	-	✓	-	2
Deleted posts (text)	✓	-	-	4
Proof of Transfer (Mobile Banking)	-	✓	-	2

The results of the investigation demonstrate that the NIJ framework combined with FTK Imager, BHE, and HxD is effective in uncovering hidden artefacts related to online prostitution activities on platform X. FTK Imager successfully identified the offender's username "@mamiagen" and recovered four deleted promotional text posts stored in memory cache. BHE revealed browsing history and cached images, including promotional content and transfer proof, confirming the offender's online activity. HxD provided deeper analysis of process memory, recovering 19 deleted conversations containing details of negotiations, account numbers, and meeting locations.

To strengthen these findings, a classification of evidence was created in Table 4, showing the contribution of each tool to different artefact types. The results indicate that combining multiple tools ensures completeness of evidence, where FTK Imager excels in memory artefact recovery, BHE in browsing activity reconstruction, and HxD in deleted conversation retrieval.

For a more extensive evaluation, this approach can be compared with similar research on other platforms such as Telegram or MiChat. While this study focused on one dataset (account "@mamiagen" via Mozilla Firefox), applying the same methodology to different datasets or communication channels could provide further validation of its reliability. This comparative evaluation would also highlight potential limitations, such as encrypted data or cloud-based storage, which require additional forensic approaches.

5. CONCLUSIONS

The digital forensic process of web-based online prostitution cases can be carried out systematically using the National Institute of Justice (NIJ) method which includes five stages, namely preparation, data collection, examination, analysis, and reporting. This research utilises a combination of three forensic tools, namely FTK Imager, Browser History Examiner, and HxD, each of which contributes significantly to the disclosure of digital evidence. FTK Imager successfully recovered the perpetrator's username as well as some deleted promotional text posts, Browser History Examiner revealed the site's browsing history and promotional image cache, while HxD enabled the recovery of conversations containing price negotiations, meeting locations, and payment account details. These results show that the application of the NIJ method is effective in ensuring the integrity of digital evidence, even though most of the data has been deleted by the perpetrator, so that it can support the process of evidence and law enforcement. In the future, this research can be expanded by applying the NIJ method to other social media or messaging platforms, integrating more advanced forensic tools capable of detecting encrypted or cloud-based data, and testing the approach on larger datasets and diverse case scenarios to improve accuracy, reliability, and applicability in real-world digital crime investigations.

6. REFERENCES

[1] H. Septya Mikayla, A. Kusyanti, P. H. Trisnawan3, dan P. Korespondensi, "Analisis Forensik Digital Untuk Investigasi Kasus Cyberbulyying Pada Media Sosial TikTok", doi: 10.25126/jtiik.2023108017.

[2] C. Ridwan Caesar, Y. Servanda, dan Y. Dwi Atma, "Analisis Forensik Digital Pada Aplikasi Media Sosial Facebook Menggunakan Metode Statik Forensik." [Daring]. Tersedia pada: https://journal.universitasmulia.ac.id/index.php/forbis

[3] Cindy mutia annur, "Ada 27 Juta Pengguna Twitter di Indonesia, Terbanyak ke-4 Global," Databoks. Diakses: 15 April 2024. [Daring]. Tersedia pada: https://databoks.katadata.co.id/datapublish/2023/11/28/ada-27-juta-pengguna-twitter-di-indonesia-terbanyak-ke-4-global

[4] Cindy mutia annur, "Ini Media Sosial Paling Banyak Digunakan di Indonesia Awal 2024," Databoks. Diakses: 15 April 2024. [Daring]. Tersedia pada: https://databoks.katadata.co.id/datapublish/2024/03/01/ini-media-sosial-paling-banyak-digunakan-di-indonesia-awal-2024

[5] J. Kajian dkk., "Civilia: Analisa Kepada Para Oknum Yang Tidak Bijak Dalam Menggunakan Media Sosial Cyberspace." Diakses: 16 Juli 2024. [Daring]. Tersedia pada: https://doi.org/10.572349/civilia.v3i1.1664

[6] "Cara Login Twitter Web dengan Mudah via Browser, Ngetwit Seru dari PC!," https://jalantikus.com/. Diakses: 21 Mei 2025. [Daring]. Tersedia pada: https://jalantikus.com/tips/cara-login-twitter-web-untuk-meningkatkan-penghasilan-bisnis-anda/

[7] "Polisi Bongkar Sindikat Open BO Anak di X dan Telegram," metrotvnews. Diakses: 21 Mei 2025. [Daring]. Tersedia pada: https://www.metrotvnews.com/play/NrWC5BQV-polisi-bongkar-sindikat-openbo-anak-di-x-dan-telegram

[8] G. F. Ardianto dan U. Sumarwan, "Prostitusi Online di Jejaring Media Sosial Twitter Ditinjau dari Alasan Pelaku Berdasarkan Teori Pilihan Rasional," 2021.

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

[10] Y. Arif, E. I. Alwi, dan M. A. Asis, "Analisis Bukti Digital Direct Message Pada Twitter Menggunakan Metode National Institute Of Justice (NIJ)," 2023.

[11] A. Hidayah dan F. Fachri, "Analisis Bukti Digital Terhadap Kasus Prostitusi Online Pada Aplikasi Michat Menggunakan Metode ACPO," 2025.

[12] G. Fanani, I. Riadi, dan A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," Jurnal Media Informatika Budidarma, vol. 6, no. 2, hlm. 1263, Apr 2022, doi: 10.30865/mib.v6i2.3946.

[13] I. Riadi, R. Umar, dan D. Bernadisman, "Analisis Forensik Database Menggunakan Metode Forensik Statis," Jurnal Sistem Informasi Bisnis, vol. 9, no. 1, hlm. 9, Mei 2019, doi: 10.21456/vol9iss1pp9-17.

[14] A. Primukti, P. K. Sari, D. Suhartono, dan K. N. Isnaini, "Analisis Memori Forensik Pada TikTok Berbasis Web Menggunakan Metode National Institute Of Justic(NIJ)," Jurnal Informatika dan Teknik Elektro Terapan, vol. 13, no. 2, Apr 2025, doi: 10.23960/jitet.v13i2.6108.

[15] A. Nofiyan, "Analisis Forensik pada Web Phishing Menggunakan Metode National Institute of Standards and Technology," CYBERNETICS, vol. 4, no. 02, hlm. 79–92, 2020, [Daring]. Tersedia pada: https://centralops.net

[16] I. Faniyah, "Penggunaan Alat Bukti Digital Dalam Komputer Forensik Pada Penyidikan Tindak Pidana Mayantara Di Direktorat Kriminal Khusus Polda Sumbar," vol. 2, no. 4, 2019.

[17] Ronal Watrianthos, Forensik Digital. Yayasan Kita Meinuilis, 2021.

[18] R. Umar,Metode NIST Untuk Analisis Forensik Bukti Digital Pada Perangkat Andorid.

[19] F. Solihin, S. Awaliyah, A. Muid, dan A. Shofa, "Pemanfaatan Twitter Sebagai Media Penyebaran Informasi Oleh Dinas Komunikasi dan Informatika," Jurnal Pendidikan Ilmu Pengetahuan Sosial (JPIPS), vol. 1, no. 13, hlm. 52–58, 2021, [Daring]. Tersedia pada: http://e-journal.upr.ac.id/index.php/JP-IPS

[20] Faturohman, "Prostitusi Online Dalam Prespektif Hukum Pidana Di Indonesia", doi: 10.46306/rj.v2i2.

[21] R. S. Setiawan, B. Budiyono, dan R. Hendriana, "Sebab-Sebab Terjadinya Prostitusi Online Dan Upaya Penanggulangan Dari Prespektif Kriminologi (Studi di Wilayah Hukum Polresta Banyumas)," Soedirman Law Review, vol. 5, no. 1, Feb 2023, doi: 10.20884/1.slr.2023.5.1.3488.

[22] "Browser History Examiner." Diakses: 9 Juli 2025. [Daring]. Tersedia pada: https://www.foxtonforensics.com/browser-history-examiner/

[23] Mega Rosita, "Analisis Komparatif Performa FTK IMAGER dan AUTOPSY dalam Forensik Digital pada Flashdisk," Info Kripto, vol. 17, no. 3, Des 2023, doi: 10.56706/ik.v17i3.83.

[24] "FTK Imager," Exterro. Diakses: 22 Juni 2024. [Daring]. Tersedia pada: Exterro.

[25] "HxD - Freeware Hex Editor and Disk Editor." Diakses: 9 Juli 2025. [Daring]. Tersedia pada: https://mh-nexus.de/en/hxd/