JOIN (Jurnal Online Informatika)
p-ISSN: 2528-1682, e-ISSN: 2527-9165
Volume 10 Number 2 | December 2025: 323-339
DOI: 10.15575/join.v10i2.1603

Forensic Analysis of Web Scraping Documents on Carding Forums and Shops using Latent Dirichlet Allocation

Fikri Irfan Adristi[1], Yudi Prayudi[2]
[1,2]Master Program in Informatics, Universitas Islam Indonesia, Indonesia

Article Info

Article history:

Received March 29, 2025
Revised June 14, 2025
Accepted July 13, 2025
Published August 17, 2025

Keywords:

Carding Forum
Carding Shop
Cybercrime
Natural Language Processing
Web Scraping

ABSTRACT

This research is based on the massive cybercrime activity in carding forums and carding shops. Based on the many victims and losses from these activities a cybercrime investigation action is needed by a digital forensic investigator. The purpose of this study is to develop a forensic carding investigation framework based on document analysis of web scraping results on carding forums and carding shops, which applies forensic profiling analysis methods and natural language processing based on the latent dirichlet allocation (LDA) algorithm. The tools used for web scraping in this study are WebHarvy Version 7.3.0.222. The tools used for data processing in this study are Microsoft Excel and Orange Data Mining. The conclusion of this study shows that the application of web scraping investigation techniques on carding forums and carding shops based on an carding investigation framework has been effective in collecting relevant data and analyzing the activities of cybercriminal appropriately. Overall, this study has succeeded in developing a more organized and data-driven approach to dealing with crimes in carding forums and carding shops, which can be a reference for further research and application in the field of digital forensic investigation.

Corresponding Author:

Yudi Prayudi
Master Program in Informatics, Universitas Islam Indonesia
Jl. Kaliurang KM. 14,5 Sleman Yogyakarta 55584

Email: prayudi@uii.ac.id

1. INTRODUCTION

Cybercrime is becoming a growing concern in today's digital age, with individuals and organizations falling victim to various types of cyber attacks [1], [2], [3], [4]. It is now thought that cybercrime is becoming more organized, larger in scale, diversified with increasing division of labor, and is expected to develop closer ties with offline organized crime [2], [5], [6], [7], [8]. Furthermore, cybercriminals are also constantly evolving their techniques and strategies, using technological advances for illegal purposes, particularly for financial gain. This emerging area of criminal behavior, known as carding, involves the use of computers and the internet to commit crimes, particularly targeting financial information such as credit card numbers, bank account details, and personal identification information [8], [9].

The impact of carding cybercrime is very significant, affecting credit card companies, merchants, and consumers [10], [11], [12]. Carding poses a significant threat to the security and integrity of financial systems and other personal information of individuals. It is a well-known fact that credit card fraud is a growing problem. Skimming, counterfeiting, and phishing schemes occur each year, causing billions of dollars in losses to companies and victims. Although credit card companies and merchants have put various measures into practice to help prevent credit card fraud, it is still a concern [13].

p-ISSN: 2528-1682
e-ISSN: 2527-9165

This concern is certainly supported by identity theft report data from the first quarter of 2019 to the first quarter of 2025, released by the Federal Trade Commission [14] and presented in Table 1.

Table 1. Comparison of Types of Identity Theft Reports from Q1 2019 to Q1 2025

Types of Stolen Identities	Total Report
Credit Card	2,512,995
Other Identity Thefts	2,013,941
Government Documents or Benefits	1,070,103
Loan or Lease	1,044,290
Bank Account	711,724
Employment or Tax-Related	581,293
Phone or Utilities	534,332

Source: Federal Trade Commission [14]

The report data in Table 1 shows that the highest total number of identity theft reports was in the credit card type, with a total of 2,512,995 reports [14]. The selection of this period is based on the most recent and complete dataset currently available from the FTC, which has been updated to include data through Q1 2025. Therefore, using the 2019–2025 period ensures that the analysis reflects the latest trends in identity theft reporting. Furthermore, the following figure 1 predicted global losses from credit card fraud [15]:

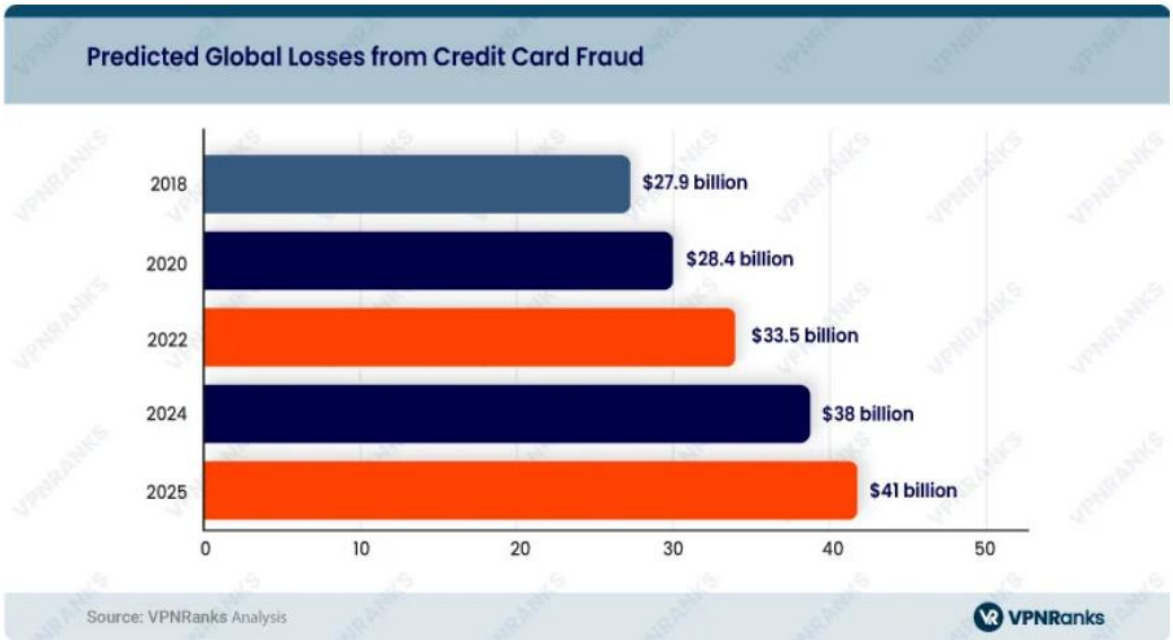

Figure 1. Predicted Global Losses from Credit Card Fraud
Source: Ashraf and Tilawat [15]

Based on Figure 1, if viewed from 2018 to 2025, the predicted global loss trend due to credit card fraud is always increasing. In 2024 Estimate Losses are expected to reach approximately $38 billion. (Based on trends and the continuation of fraud techniques). In 2025 Prediction It is projected that losses could exceed $41 billion [15]. The large number of identity theft reports and the predicted global losses from credit card fraud are certainly the result of cybercrime activities carried out by cybercriminals in carding forums and carding shops. Based on this, it certainly needs to be the attention of digital forensic investigators to conduct forensic investigations and analysis on carding forums and carding shops [14], [15].

Based on previous research, there are several solutions that can be implemented to investigate cybercrime. Among them are footprinting [16], [17], [18], reconnaissance [19], [20], [21], undercover operations [22], [23], [24], [25], and cooperation with hosting service providers [26], [27], [28], [29] to obtain information about users and activities that occur in carding forums and carding shops. Investigative techniques such as footprinting, reconnaissance, undercover operations, and cooperation with hosting providers have drawbacks, including risk of detection, slow processes, loss of identity, limited cooperation, and jurisdictional differences. While various investigative techniques are useful, web scraping is often more effective in cybercrime investigations because it allows real-time access to carding information, cybercriminal identification, and digital footprints. Web scraping differs from web crawling in both purpose and method: web scraping converts unstructured web data into structured data that can be stored and analyzed in a central database or spreadsheet for analysis [30], while web crawling uses bots to crawl and index websites for search engines such as Google or Bing [31].

The distinction between "web scraping" and "web crawling" often overlaps, as many authors use them interchangeably. In general, web crawling refers to automated navigation without a specific purpose, as search engines like Google do to index web pages [32]. Furthermore, there are also several previous studies that apply web scraping as a technique in forensic investigations, such as in studies [33], [34]. In the study by Maybir and Chapman [33], the results showed that open source investigation using web scraping techniques on online ecstasy report data proved to be the most effective in obtaining appropriate general summary data compared to other more expensive and burdensome population approaches, such as wastewater analyses and population surveys.

In the research of Muehlethaler and Albert [34], it has been emphasized that a fiber population survey is an important part of the field of forensic fiber examination. The research shows that web scraping techniques have the potential to provide near-real-time population studies that can provide great benefits for forensic practitioners. Although research [33], [34] has applied web scraping as a technique in forensic investigations, the research has weaknesses in the aspect of data analysis techniques, which are still simple in the form of descriptive profiling analysis in its presentation. This study applies a combination of web scraping-based forensic investigation and topic modeling-based data analysis, as in previous studies [35], [36]. Sonmez and Codal [35] study explores dark web criminal activities, identifying terrorism-related topics using LDA topic modeling. Meanwhile, Jin, Kim, and Jeong [36] research addresses the challenges of tracking criminals on the dark web, using advanced crawlers and machine learning to overcome them.

This research contributes to forensic profile analysis to identify carding crime patterns, the application of LDA to filter relevant information, and the development of a structured and court-justified forensic investigation framework. In addition to conventional investigation techniques such as footprinting and undercover operations, web scraping, forensic analysis, and natural language processing (NLP)-based approaches offer advantages in speed, accuracy, and scalability. For example, in researchers [35], [37], [38], [39] have used natural language processing approaches on document text from the dark web and dark forums to identify communication patterns, illegal activities, and seller profiles, which support cybercrime forensic investigations in the context of drug trafficking, terrorism, and credit card fraud.

This study utilizes the natural language processing (NLP) approach and web scraping-based data retrieval techniques to analyze activities on carding forums and carding shops that generally contain unstructured text and hidden illegal content. This approach refers to the findings of Wiratmoko et al. [40], which show the effectiveness of NLP models in automatically extracting information from large data sets, and is reinforced by the digital security perspective of Alam and Gupta [41], which emphasizes the importance of integrating technologies such as blockchain and automation in detecting and verifying online content. Thus, this study contributes to the development of intelligent solutions in the field of cybersecurity, especially in the realm of data science and natural language processing in the context of applied informatics. This study proposes a forensic carding investigation framework based on web scraping from carding forums and carding shops. By applying descriptive forensic profile analysis and natural language processing using latent Dirichlet allocation, the framework helps identify patterns of cybercrime and cybercriminal behavior. This approach improves the effectiveness of investigations, supports law enforcement, and provides strategic insights for more proactive cybersecurity policies.

p-ISSN: 2528-1682
e-ISSN: 2527-9165

1.1. Theoretical Foundation

1.1.1. Alexiou Principle

Alexiou Principle (named after its creator Mike Alexiou of IT infrastructure services provider Terremark Worldwide, Inc.) [42] provides fundamental questions, which can be used by digital forensic investigators as a guide and direction in conducting searches and managing investigations. These questions are: (1) What question are you trying to answer?; (2) What data do you need to answer that question?; (3) How do you extract that data?; and What does the data tell you? [43]

Each element of the four questions plays an important role in developing an investigation plan, which includes outlining the purpose of the investigation. This purpose is very important, because without knowing the clear purpose, it is impossible for the investigator to determine what to look for in the investigation process. This plan also describes the definition of investigative success and ensures that there is an understanding between the digital forensic investigator and the client (the organization that is the victim of a security breach) [42].

1.1.2. Previous Research

In the study of Sonmez and Codal [35] using an LDA-based topic modeling approach, it was found that discussions of recruitment and terrorism propaganda dominated the dark web, even without evidence of direct collaboration. Rao, Reddy, and Vishnu [44] developed a web scraping and text analysis framework, revealing 80% of positive reviews on searches related to Dell XPS. Research by Agarwal, Rishiwal, Tanwar, and Yadav [10] based on the random forest algorithm with 97.5% accuracy, provides a significant solution to threats in the decentralized crypto ecosystem. Research by Gong et al. [45] explores employment fraud in hybrid spaces, highlights the low geographic consistency of fake posts, and integrates AI to mitigate cyber victimization.

2. METHOD

2.1. Research Steps

In order to conduct quality research, planned steps are needed so that the research is more structured and on target. In this section, the researcher describes the stages in conducting this research. In general, the steps in this research are explained in Figure 2.

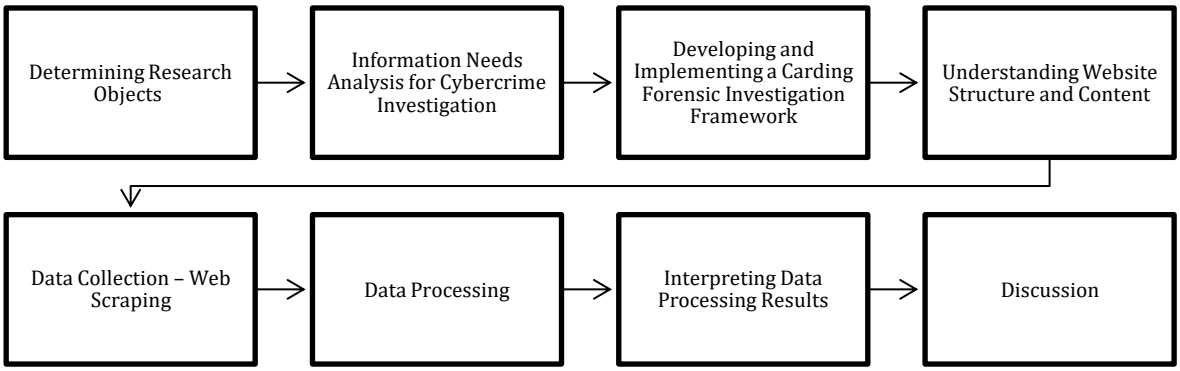

Figure 2. Research Steps

2.2. Determining Research Objects

At this stage, the researcher determines the object of the research. The object of this research is the carding forum, the carding shop, and the trend of cybercrime activities in it. In this study, the carding forum and carding shop websites that are used as research objects are:

1) Altenen Forums-Images & Videos & Porn Accounts 🔞 Section (https://altenens.is/forums/images-videos-porn-accounts🔞.469197/) [46]
2) carding.store-Cracking Tutorials Section (https://carding.store/forum/20-cracking-tutorials/) [47]
3) Astradumps Shop (https://astradumps.com/shop/) [48]
4) Money-Heist.org Shop (https://money-heist.org/shop/) [49]

The reason the researcher chose Altenen Forums-Images & Videos & Porn Accounts 🔞 Section and carding. The store-Cracking Tutorials Section as research objects is because both carding forums have a high total number of visits, bounce rate, pages per visit, and average visit duration, indicating the potential to collect rich and relevant data [46], [47], [50]. The following table 2 presents the indicators for the two carding forums:

Table 2. Carding Forum Indicators

No	Carding Forum	Total Visits	Bounce Rate	Pages per Visit	Avg Visit Duration
1	Altenen Forums	355,1K	35,66%	17,46	00:11:38
2	carding.store	9K	18%	1,47	00:01:35

Source: Similarweb LTD [50]

The high user activity indicates the significance of both forums in the carding community, so that web scraping on both forums can provide valuable insights into the growing trends and activities of cybercrime. The reason researchers chose Astradumps Shop and Money-Heist.org Shop as research objects is that both carding shops have a wide variety of illegal goods and services sold, well-identifiable web structures, and content [48], [49].

The wide variety of illegal goods and services sold, and clear web structures and content, help produce rich and structured web scraping data. This allows for in-depth forensic profiling analysis to identify trends, patterns, and cybercrime handling strategies. The four research objects will be investigated using web scraping techniques.

2.3. Information Needs Analysis for Cybercrime Investigation

At this step, the researcher conducted an analysis of information needs for cybercrime investigations on carding forums and carding shops based on 5W1H and the Alexiou Principle [43], [51], which are presented in Tables 3 and 4.

Table 3. Analysis of Information Needs for Cybercrime Investigation on Carding Forums and Carding Shops Based on 5W1H

5W1H Elements	Question	Information Needs
What	What types of cybercrime activities occur?	Information about various illegal activities such as carding, hacking & cracking, selling illegal content, and others.
Who	Who are the perpetrators involved in these cybercrime activities?	Profiling of users, active actors, and criminal networks involved in forum carding, hacking, or illegal content.
When	When did the cybercrime activity take place?	Time and frequency of illegal activity based on logs and digital footprints taken from forums or shops.
Where	Where do these cybercrime activities take place?	Location of carding forum servers or domains, carding shops, and places where illegal content and transactions are stored.
Why	Why are these cybercrime activities carried out?	The motivation behind the activity, such as financial gain, learning hacking, or distributing illicit content.
How	How are these cybercrime activities carried out?	Carding techniques, hacking, distribution of illegal content, payment methods, and ways of disguising the perpetrator's identity.

Table 3 presents an analysis of information needs for cybercrime investigations on carding forums and carding shops using the 5W1H framework (What, Who, When, Where, Why, and How). Each element provides a structured dimension to guide investigators in understanding and mapping criminal behavior in cyberspace.

The "What" aspect focuses on identifying the types of illegal activities occurring in these online spaces. This includes not only carding—the trafficking of stolen credit card information—but also broader cybercrime activities such as hacking, cracking, and trading illicit digital content. Understanding the scope of these activities is essential for categorizing threats and prioritizing responses. The "Who" element addresses the identification and profiling of actors involved. This includes both individual

perpetrators and organized cybercrime groups. Profiling is crucial for linking usernames, communication styles, transaction patterns, and behavioral markers to real-world identities or network affiliations.

The "When" element examines the timeline of criminal activity. By analyzing timestamps in logs, posts, or transaction histories, investigators can detect patterns of activity, such as peak operational hours, seasonal spikes, or coordinated campaigns. The "Where" dimension looks at the geographical and technical location of criminal operations. While many cybercriminals use anonymizing tools, investigating server IP addresses, domain registrations, and storage points can help localize their infrastructure or infer jurisdictional relevance.

The "Why" refers to the motivations behind these activities. Financial gain remains the dominant driver, but other motives such as experimentation, learning, ideology, or revenge also play a role. Understanding motivation helps in anticipating the evolution of threats and designing preventive strategies. Finally, the "How" component delves into the technical methods used to carry out cybercrime. This includes specific carding or hacking techniques, the use of dark web platforms, cryptocurrency for payments, and obfuscation methods like VPNs or spoofed identities. Mapping these methods is vital for developing effective detection and mitigation tools. Thus, Table 3 serves not just as a summary of cybercrime dimensions, but as a comprehensive guide for framing forensic investigation strategies within carding-related environments.

Table 4. Analysis of Information Needs for Cybercrime Investigation on Carding Forums and Carding Shops Based on the Alexiou Principle

Alexiou Principle	Information Needs
What question are you trying to answer?	Identify major illegal activities in carding forums and carding shops (carding, hacking, selling illegal content, etc.).
What data do you need to answer that question?	User activity logs, transactions, forum messages, identity data, and digital transaction links or traces.
How do you extract that data?	The use of web scraping techniques to collect data from carding forums and carding shops, as well as digital footprint analysis.
What does that data tell you?	Revealing cybercrime patterns, trends, and networks, and providing insights for prevention and law enforcement.

Table 4 outlines the analysis of information needs for cybercrime investigations on carding forums and carding shops based on the Alexiou Principle, a framework commonly used to guide investigative data processes through a sequence of focused questions. This principle is particularly useful in digital forensics, as it connects investigative goals with specific data sources and analytic techniques.

The first question—"What question are you trying to answer?"—anchors the investigation by clarifying the main objective, which in this context is to identify the major forms of illegal activity occurring on underground platforms. These include not only carding (the buying and selling of stolen credit card data), but also hacking-related services, identity theft, and distribution of illicit content. Clearly defining this investigative question helps narrow the focus and scope of data collection efforts.

The second part—"What data do you need to answer that question?"—highlights the specific types of data that are critical for understanding the criminal ecosystem. This includes user activity logs, transaction histories, forum posts, and metadata that can link different accounts or activities to a common actor. Identity-related data such as usernames, IP addresses, and wallet addresses are also essential for linking behavior patterns across platforms.

The third question—"How do you extract that data?"—addresses the technical methods used for data acquisition. Web scraping is emphasized here as a primary approach to systematically collect unstructured data from carding forums and carding shops. This is complemented by digital footprint analysis techniques, such as tracking timestamps, link associations, and behavioral signatures. These tools enable investigators to gather large volumes of real-time or historical data without direct system access.

Finally, the last component—"What does that data tell you?"—explains the analytical outcome of the collected data. By processing and analyzing the scraped content, investigators can uncover hidden

patterns, frequent transaction types, repeat offenders, and even coordinated criminal networks. These findings not only aid in cybercrime prevention but also provide actionable intelligence for law enforcement and policy-making. The Alexiou Principle helps translate a general investigative need into a structured, data-driven workflow that is well-suited to the complex and covert nature of carding-related cybercrime.

2.4. Developing and Implementing a Carding Forensic Investigation Framework

The development of a forensic carding investigation framework involves formulating the structure of the investigation stages, defining evidence collection procedures, and establishing important indicators. This step ensures that the framework can be used systematically to deal with carding crimes effectively. All of these stages are developed into a forensic carding investigation framework designed to provide systematic guidance in strengthening legal action against cybercrime activities in carding forums and carding shops.

2.5. Understanding Website Structure and Content

At this stage, researchers understand the structure and content of the website before starting web scraping. This stage involves analyzing web page elements, such as layout, pagination, click elements, HTML tags, and URL patterns, and identifying data to be extracted to ensure efficiency and success of data collection.

2.6. Data Collection – Web Scraping

At this step, the researcher collected data using web scraping software to retrieve data from the carding forum and carding shop web pages, select relevant elements, extract data, and save them in Microsoft Excel format (.xlsx), which can be analyzed further. The data collected comes from the websites described in Part 3.2. Determining Research Objects. Data collection using web scraping was only carried out for one day on December 5, 2024, so that changes in website content after web scraping were not included in subsequent analysis. This was done to avoid bias due to content fluctuations, ensuring that data reflects a stable snapshot. While effective in capturing carding activity at that time, this approach has limitations in representing long-term temporal dynamics. This study used WebHarvy 7.3.0.222 [52], a high-speed GUI tool that extracts data precisely without programming. WebHarvy 7.3.0.222 supports a variety of output formats, including CSV, Excel, XML, and SQL, and is capable of handling JavaScript-based dynamic pages with scheduled automated scraping. WebHarvy 7.3.0.222 can handle dynamic pages, as well as bypass CAPTCHA and IP blocking, although it is less flexible with AI-based anti-scraping.

2.7. Data Processing

After the data is obtained from the web scraping stage, the next step is data processing. Data processing in this study focuses on descriptive analysis of forensic profiling and topic modeling: the latent Dirichlet allocation algorithm.

1) Descriptive Forensic Profiling Analysis: Descriptive forensic profiling analysis is a technique for identifying important patterns and characteristics of forensic data through the use of keyword-based and detailed data visualization in criminal or digital security investigations [33], [34]. The tools used to process data in the descriptive analysis of forensic profiling in this study are Microsoft Excel [53].
2) Topic Modelling - Latent Dirichlet Allocation Algorithm: The data analysis stages are described based on the Orange Data Mining [54] Workflow in Figure 3.

p-ISSN: 2528-1682
e-ISSN: 2527-9165

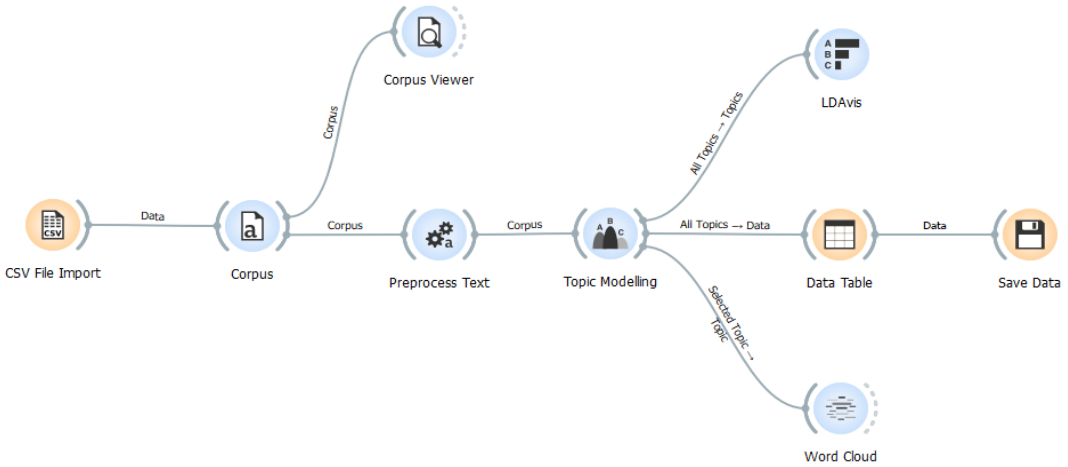

Figure 3. Orange Data Mining Workflow

This study used Orange Data Mining software to analyze text data from forensic web scraping investigations on forums and carding shops [54]. Data in CSV format was imported using semicolon separators, then collected in the "corpus" module and verified through the "corpus viewer." Text preprocessing was performed with the "preprocess text" module, including text normalization, removal of irrelevant elements, and application of Porter Stemmer. Topic modeling used latent Dirichlet allocation (LDA) to identify the distribution of latent topics in documents [55], [56], [57], with visualization through the "wordcloud" to understand cybercrime trends. Findings were organized into a "data table" summarizing the distribution of topics and keywords, then stored using the "save data" module for further analysis, ensuring a systematic and efficient workflow.

2.8. Interpreting Data Processing Results

Interpreting data processing results is the process of analyzing and understanding information generated from processed data. This interpretation process involves interpreting statistical results, identifying patterns, and conveying insights based on the results obtained.

2.9. Discussion

The most important aspect of research is the discussion, because at this stage, the research results are not only presented, but also interpreted based on theoretical foundations and previous research. In the context of forensic carding, the discussion serves to connect the results of the analysis with insights that can enrich the understanding of the modus operandi, crime patterns, and prevention strategies.

3. RESULT AND DISCUSSION

3.1. Development and Implementation of Carding Forensic Investigation Framework

In this section, the researcher has formulated a forensic carding investigation framework that was designed and implemented in this study in Table 5.

Table 5. Carding Forensic Investigation Framework

Stages	Sub-Stages	Definition
Digital Forensic Examination Request Letter	Receipt of Application Letter	Received a request letter from the police to conduct a digital forensic examination related to carding forums and carding shops.
Data Collection	Web Scraping	Collecting data from carding forums and carding shops in accordance with the permission granted in the application letter, to obtain relevant documents and transactions.

Stages	Sub-Stages	Definition
Data processing	Forensic Profiling	Analyze the collected data to identify patterns and characteristics of carding perpetrators.
	Natural Language Processing (NLP)	Using latent dirichlet allocation (LDA) technique to explore key topics in discussions in carding forums and carding shops.
Law enforcement	Preparation of Reports	Prepare findings reports based on data analysis to support legal processes.
	Coordination with Law Enforcement	Coordinate with police and legal authorities to report findings and support next steps.
Alignment with Alexiou's Principles	Questions to be Answered	What are the patterns and modus operandi of carding perpetrators?
	Required Data	Data from carding forums, carding shops and related transactions.
	Data Extraction Methods	How do I collect data via web scraping according to the permission of the application letter, and analyze it using NLP?
	Meaning of Data	What insights can be gained regarding the behavior of carding perpetrators and the main topics in their discussions?
Decision-making	Recommended Actions	Provide recommendations for next steps of investigation based on findings.
	Evaluation of Framework Performance	Assessing the effectiveness of the framework in supporting investigations and law enforcement.

The creation of the Carding Forensic Investigation Framework is an implementation of Part 3.4. Developing and Implementing a Carding Forensic Investigation Framework, aims to develop and implement a structured approach to carding case investigation by integrating established digital forensic methodologies. This framework includes collecting valid evidence through web scraping, analyzing data using NLP techniques to understand content, and applying Alexiou's systematic investigation principles to ensure legal effectiveness and sustainability of the investigation. By referring to best practices and digital forensic methodologies in the literature [35], [36], [43], [58], [59], this framework is designed to ensure a comprehensive investigation process, from data collection to coordination with law enforcement.

3.2. Web Scraping

Before conducting the web scraping process, researchers need to understand the structure and content of the carding forum and the carding shop website that are the objects of the research. After the researcher understands the structure and content of the carding forum and the carding shop website that are the objects of the research, the researcher collects data from the carding forum and carding shop according to the permission given in the investigation request letter, in order to obtain relevant documents and transactions. The web scraping data can be accessed through the researcher's Github account (https://github.com/451Fikrie/Tesis-Magister-Informatika-Fikri) [60].

3.3. Data Processing Results

3.3.1. Forensic Profiling Analysis

In this section, the author will describe the results of the forensic profiling analysis obtained from the infographic analysis in the form of charts in Microsoft Excel. Here is a further explanation of the results:

p-ISSN: 2528-1682
e-ISSN: 2527-9165

Figure 4. Top 10 Highest Prices for Items Sold on Astradump Shop
Source: Processed Data – Adristi [60]

The top 10 items for sale on Astradump Shop [48] at figure 4, show illegal transactions at varying prices. The most expensive item is a $500,000 bank transfer for $45,700. Other items, such as cloned ATM cards and transfers through platforms like CashApp, PayPal, and Venmo, are selling for between $5,900 and $10,000.

Based on the top 10 items for sale on Astradump Shop [48] at figure 4, the implications of the digital forensic investigation strategy include in-depth analysis of illegal transactions on platforms such as PayPal, Venmo, and CashApp, focusing on suspicious transfer patterns and large amounts, such as $45,700 for a $500,000 transfer. Digital artifacts such as server logs, browser history, and the perpetrator's hardware need to be analyzed to uncover the criminal network. Tracing these transaction traces requires cooperation between the victim company and investigators, as in Xiaoyu's [61] research to help understand the perpetrator's modus operandi and identify entry points for further investigation.

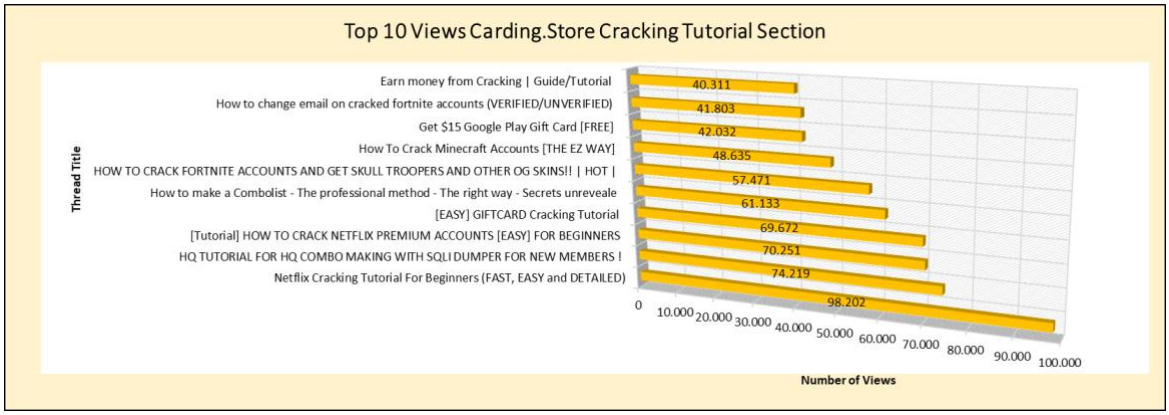

Figure 5. Top 10 Views Carding.Store Cracking Tutorial Thread Section
Source: Processed Data – Adristi [60]

Top 10 views on Carding.Store Cracking Tutorial Thread Section [47] at figure 5. above, shows cracking tutorials with popular themes such as Netflix Cracking Tutorial For Beginners (FAST, EASY and DETAILED) (98,202 views) and HQ TUTORIAL FOR HQ COMBO MAKING WITH SQLI DUMPER FOR NEW MEMBERS ! (74,219 views). The main focus is cracking premium accounts, gift cards, and combolist making guides, with views ranging from 40,311–98,202.

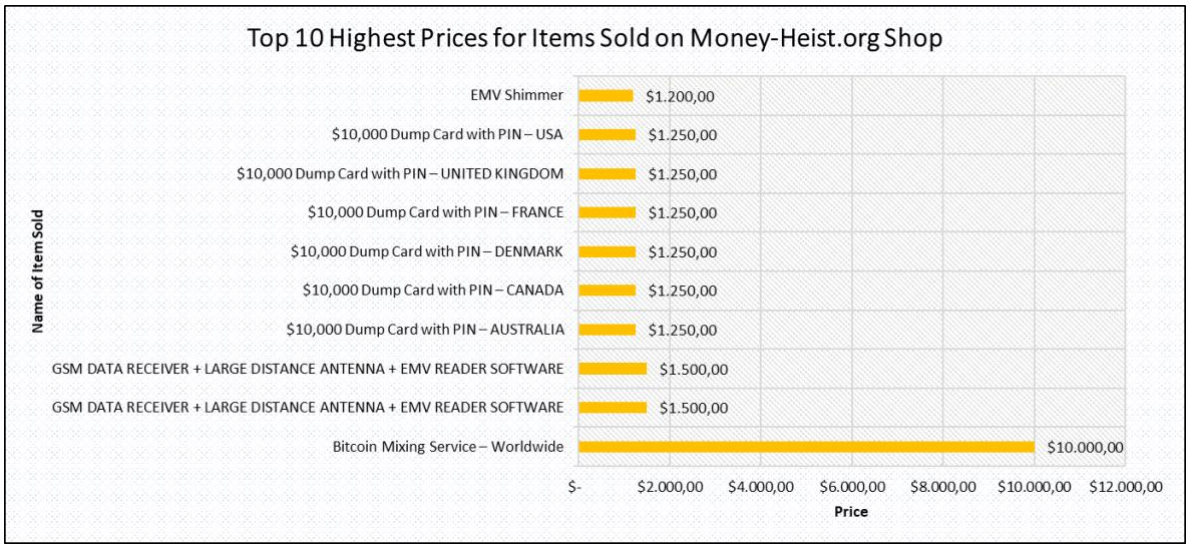

Figure 6. Top 10 Highest Prices for Items Sold on Money-Heist.org Shop
Source: Processed Data – Adristi [60]

The top 10 highest prices on Money-Heist.org Shop [49] at figure 6 are dominated by Bitcoin Mixing Service - Worldwide for $10,000. Other products include a GSM receiver ($1,500) and $10,000 Dump Card with PIN for various countries ($1,250). Additional items such as EMV Shimmer ($1,200) complete the list of high-tech cybercrime products.

Digital forensic investigation strategies should focus on tracking transactions related to high-tech cybercrime products on the Money-Heist.org Shop, such as Bitcoin Mixing ($10,000) and Dump Card with PIN for various countries ($1,250) services. Metadata investigation and analysis of payment transactions can reveal the perpetrators' network patterns, as in the [62], [63], [64] study. The modus operandi involves selling illegal goods, such as GSM receivers and EMV Shimmers, to support cybercrime activities, with the use of crypto payment instruments to obscure the traces of cybercrime.

3.3.2. Natural Language Processing - Latent Dirichlet Allocation

This section presents the results of the Orange Data Mining analysis - natural language processing with the Latent Dirichlet Allocation (LDA) approach to systematically identify and distribute topics based on available data.

Table 6. Topic Modeling: Latent Dirichlet Allocation - Altenen Porn Section

Topic Modelling: Latent Dirichlet Allocation Altenen Porn Section Number of topics: 5	
Topics	**Marginal Topic Probability**
1: leak, teen, mega, nude, girl, snapchat, hot, ☆, pack, video	0.323916
2: mega, premium, collect, ❤, nz, porn, leak, pack, gb, exclus	0.182307
3: video, nude, porn, girl, 🔞, 💦, big, n, photo, sex	0.153554
4: sexi, mega, account, hot, super, onli, ⚠, ❤, 【, ❄, 】 ✨	0.186736
5: leak, onlyfan, girl, new, 🔞, pack, collect, amateur, free, video	0.153399

Source: Processed Data – Adristi [60]

Topic modeling analysis using latent Dirichlet allocation (LDA) in table 6 identified five main themes in the distribution of explicit content on the Altenen Porn Section carding forum [48], reflecting

p-ISSN: 2528-1682
e-ISSN: 2527-9165

privacy violations, digital rights, and abuse of file-sharing platforms. The dominant topic (32.39%) related to the leak of adolescents' private content on social media such as Snapchat, followed by the illegal distribution of premium content in Mega.nz (18.23%), the distribution of pornographic material in various formats (15.36%), the promotion of exclusive services (18.67%), and the leak of OnlyFans content (15.34%). The dominance of private content leaks indicates the urgency of digital forensic investigations into social media platforms, while metadata and transaction tracking are needed to address illegal distribution. Investigation of copyright and privacy violations, especially on OnlyFans, is also a priority in mitigating legal risks, in line with previous studies [65], [66], [67], [68].

Figure 7. Altenen Porn Section Word Cloud
Source: Processed Data - Adristi [60]

Figure 7. The Altenen Porn Section word cloud reveals a primary focus on the distribution of explicit content, with “video” (5%) as the most dominant word, reflecting the primary format of content shared. Words such as “nude” (3%), “porn” (2%), and “girl” (2%) highlight explicit themes, while the symbols “🔞” and “🔥” are used as illegal marketing strategies to attract new users. In addition, the words “photo” and “se” show the variety of types of content being distributed. This word distribution reflects the modus operandi of cybercrime that exploits digital media to distribute adult material as an illegal commodity, which violates Law of the Republic of Indonesia Number 44 of 2008 concerning Pornography [69], as well as giving rise to privacy violations, copyright, and digital exploitation as part of the core activities of cybercriminals.

Table 7. Topic Modeling: Latent Dirichlet Allocation – Carding Shop & Cracking Tutorial Threads

Topic Modelling: Latent Dirichlet Allocation Carding Shop & Cracking Tutorial Threads Number of topics: 5	
Topics	**Marginal Topic Probability**
1: crack, account, hq, tutori, fortnit, spotifi, guid, make, premium, checker	0.185420
2: free, get, crack, account, method, proxi, rdp, work, tutori, hq	0.341975
3: crack, method, netflix, work, get, free, tutori, make, card, new	0.173992
4: dork, sqli, use, get, tutori, dumper, databas, hq, crack, best	0.122227
5: hq, make, dork, privat, keyword, combo, use, sqli, get, method	0.176387

Source: Processed Data - Adristi [60]

The LDA analysis in Table 7 identified five main topics in cybercrime activities. The dominant topic, Topic 2 (34.20%), discussed free account hacking methods using proxies and RDP, while Topic 1 (18.54%) focused on tools and tutorials for hacking services such as Fortnite and Spotify. Topic 3

(17.40%) dealt with unauthorized access to streaming services such as Netflix, while Topic 4 (12.22%) highlighted system exploitation using SQLi and dorks. Topic 5 (17.64%) covered a combination of SQLi keywords and techniques for data breaches. These results indicate a systematic distribution of hacking guides and tools, emphasizing the need for digital forensic investigations into the spread of illegal tools and technical methods used in unauthorized access [70], [71], [72].

Figure 8. Carding Shop & Cracking Tutorial Threads Word Cloud

Source: Processed Data – Adristi [60]

Figure 8. Carding Shop & Cracking Tutorial Threads word cloud shows that cybercriminal activity focuses on paid account cracking, with the words “crack” (8%) and “account” (6%) as the most dominant. Words such as “hq,” “tutori,” and “guid” indicate the provision of high-quality guides to facilitate hacking, while “fortnit,” “spotifi,” and “premium” indicate popular services that are often targeted. This word distribution reveals the perpetrators’ strategies in exploiting digital platform security gaps and is in line with previous studies [73], [74].

3.4. Discussions

This study develops a forensic carding investigation framework that integrates legal, technical, and analytical methodologies to support law enforcement. Digital forensic (DF) reports are compiled based on official requests, encompassing technical, investigative, and evaluative analyses to document cybercriminal activities such as carding and cracking. Coordination with law enforcement includes submitting expert testimony (BAPSA), ensuring legal compliance and confidentiality [75], [76], [77]. Data extraction via web scraping from illicit platforms follows legal protocols, with NLP and LDA applied to analyze cybercriminal behavior, despite challenges in slang interpretation [46], [47], [48], [49], [52].

The findings inform decision-making, recommending targeted actions like IP tracking, digital evidence collection, and regulatory reinforcement through international cooperation [26], [27], [78], [79], [80], [81], [82], [83], [84]. Strengthened digital security and public education are crucial in mitigating cyber threats [85], [86], [87]. Performance evaluation demonstrates the framework's effectiveness in expediting cybercrime investigations, supporting regulators in identifying fraudulent activities [88]. Aligning with AI-driven forensic advancements [89], [90], this study uniquely integrates law enforcement aspects, distinguishing it from purely technical approaches [35], [44], [91], [92], [93], [94], offering a comprehensive model for combating cybercrime.

4. CONCLUSION

This study shows that web scraping is effective in forensic carding investigations by collecting and analyzing data from carding forums and shops, while LDA-based NLP analysis identifies discussion topics that reflect illegal activities. The integration of these methods creates a structured investigation framework, improves analysis efficiency, and strengthens coordination with law enforcement. Further research is recommended to expand the scope to forums on the dark web, apply advanced analysis

techniques such as deep learning, and evaluate the effectiveness of the framework in real cases through collaboration with relevant authorities.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest, either among the authors or with the subject of this research.

ACKNOWLEDGMENT

This publication is part of a research project funded by the Directorate of Research, Technology, and Community Service – Directorate General of Higher Education, Research, and Technology (Diktiristek), Ministry of Education, Culture, Research, and Technology of the Republic of Indonesia, through the Thesis Research Grant scheme for Fiscal Year 2025, under Contract Number: 0498.01/LL5-INT/AL.04/2025. The authors gratefully acknowledge the financial support provided, which played a significant role in the successful implementation of this research.

REFERENCES

[1] D. Buil-Gil, N. Lord, dan E. Barrett, "The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention," *Vict. Offender.*, vol. 16, no. 3, hal. 286–315, Apr 2021, doi: 10.1080/15564886.2020.1814468.

[2] B.-J. Koops, "The Internet and its Opportunities for Cybercrime," Nijmegen, 09/2011, 2011. doi: 10.2139/ssrn.1738223.

[3] M. S. Malik dan U. Islam, "Cybercrime: an emerging threat to the banking sector of Pakistan," *J. Financ. Crime*, vol. 26, no. 1, hal. 50–60, Jan 2019, doi: 10.1108/JFC-11-2017-0118.

[4] N. Teodoro, L. Gonçalves, dan C. Serrão, "NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive Requirements," in *2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki: IEEE, 2015, hal. 418–425. doi: 10.1109/Trustcom.2015.402.

[5] W. Ahmad, "Is Credit Card Fraud a Real Crime? Does it Really Cripple the E-Commerce Sector of E-Business?," in *2008 International Conference on Management of e-Commerce and e-Government*, Nanchang: IEEE, 2008, hal. 364–370. doi: 10.1109/ICMECG.2008.99.

[6] P. Grabosky, "The evolution of cybercrime, 2004-2014," Canberra, 2014/58, 2014. doi: 10.2139/ssrn.2535605.

[7] V. Jirovský, A. Pastorek, M. Mühlhäuser, dan A. Tundis, "Cybercrime and Organized Crime," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, in ARES '18. New York, NY, USA: Association for Computing Machinery, 2018, hal. 1–5. doi: 10.1145/3230833.3233288.

[8] M. Yip, C. Webber, dan N. Shadbolt, "Trust among cybercriminals? Carding forums, uncertainty and implications for policing," *Polic. Soc.*, vol. 23, no. 4, hal. 516–539, Des 2013, doi: 10.1080/10439463.2013.780227.

[9] N. Kshetri, "The simple economics of cybercrimes," *IEEE Secur. Priv.*, vol. 4, no. 1, hal. 33–39, 2006, doi: 10.1109/MSP.2006.27.

[10] U. Agarwal, V. Rishiwal, S. Tanwar, dan M. Yadav, "Blockchain and crypto forensics: Investigating crypto frauds," *Int. J. Netw. Manag.*, vol. 34, no. 2, hal. e2255, Mar 2024, doi: 10.1002/nem.2255.

[11] M. Azhan dan S. Meraj, "Credit Card Fraud Detection using Machine Learning and Deep Learning Techniques," in *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, Thoothukudi: IEEE, 2020, hal. 514–518. doi: 10.1109/ICISS49785.2020.9316002.

[12] B. Al Smadi dan M. Min, "A Critical review of Credit Card Fraud Detection Techniques," in *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York: IEEE, 2020, hal. 732–736. doi: 10.1109/UEMCON51285.2020.9298075.

[13] K. J. Barker, J. D'Amato, dan P. Sheridon, "Credit card fraud: awareness and prevention," *J. Financ. Crime*, vol. 15, no. 4, hal. 398–410, Jan 2008, doi: 10.1108/13590790810907236.

[14] Federal Trade Commission, "Identity Theft Reports," Public Tableau. Diakses: 7 April 2024. [Daring]. Tersedia pada: https://public.tableau.com/app/profile/federal.trade.commission/viz/IdentityTheftReports/TheftTypesOverTime

[15] S. J. Ashraf dan M. Tilawat, Ed., "Credit Card Fraud Statistics: Losses to Explode $41 Billion by 2025!," VPNRanks.com. Diakses: 13 Juni 2025. [Daring]. Tersedia pada: https://www.vpnranks.com/resources/credit-card-fraud-statistics/

[16] H. Agrawal, S. P. Singh, S. Dixit, P. Nagdev, V. P., dan S. Thaseen, "A Digital Forensic Analysis of Profiling and Avoidance of Websites Disseminating Disinformation," in *2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)*, Vellore: IEEE, 2024, hal. 1–9. doi: 10.1109/ic-ETITE58242.2024.10493661.

[17] Y. Levy dan R. Gafni, "Introducing the concept of cybersecurity footprint," *Inf. Comput. Secur.*, vol. 29, no. 5, hal. 724–736, Jan 2021, doi: 10.1108/ICS-04-2020-0054.

[18] S. Sharmila dan C. Aparna, "Tracing footprints of anti-forensics and assuring secured data transmission in the cloud using an effective ECCDH and Kalman Filter," *J. Netw. Comput. Appl.*, vol. 221, hal. 103762, 2024, doi: 10.1016/j.jnca.2023.103762.

[19] V. B. Bollikonda dan K. Kiran, "Reconnaissance on Dark Web Trades and Traders Activities for Investigation," in *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi: IEEE, 2024, hal. 1649–1653. doi: 10.23919/INDIACom61295.2024.10498813.

[20] W. Mazurczyk dan L. Caviglione, "Cyber reconnaissance techniques," *Communications of the ACM*, vol. 64, no. 3, Association for Computing Machinery, New York, NY, USA, hal. 86–95, Februari 2021. doi: 10.1145/3418293.
[21] J. K. Pringle *et al.*, "Forensic geoscience non-invasive detection and characterisation of underground clandestine complexes, bunkers, tunnels and firing ranges," *Forensic Sci. Int.*, vol. 359, hal. 112033, 2024, doi: 10.1016/j.forsciint.2024.112033.
[22] O. J. Ndubuisi, G. Adene, B. T. Sunday, C. E. Mbonu, dan A. U. Gift-Adene, "Digitally improving UK police surveillance and incidence response using real-time crowd reporting app: Digipolice," *Glob. J. Eng. Technol. Adv.*, vol. 18, no. 3, hal. 124–138, 2024, doi: 10.30574/gjeta.2024.18.3.0048.
[23] K. F. Steinmetz, B. P. Schaefer, C. G. Brewer, dan D. L. Kurtz, "The Role of Computer Technologies in Structuring Evidence Gathering in Cybercrime Investigations: A Qualitative Analysis," *Crim. Justice Rev.*, hal. 07340168231161091, Mar 2023, doi: 10.1177/07340168231161091.
[24] A. Valiño Ces, "The Importance of the Computer Undercover Agent as an Investigative Measure Against Cybercrime: A Special Reference to Child Pornography Crimes," in *Legal Developments on Cybersecurity and Related Fields*, 1 ed., F. A. C. P. de Andrade, P. M. F. Freitas, dan J. R. de S. C. de Abreu, Ed., Cham: Springer International Publishing, 2024, hal. 145–165. doi: 10.1007/978-3-031-41820-4_9.
[25] Y. Vasoya, T. Modi, O. Patel, D. Kotak, K. Shah, dan K. Sabale, "A Comprehensive Exploration to Cybercrimes Investigation Techniques," in *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi: IEEE, 2024, hal. 1046–1053. doi: 10.23919/INDIACom61295.2024.10498752.
[26] Y. Benhamou, "Website Blocking Injunctions Under Swiss Law: From Civil and Administrative Injunctions to Criminal Seizure or Forfeiture," *Expert Focus*, no. 11, hal. 885–893, 2017, [Daring]. Tersedia pada: http://archive-ouverte.unige.ch/unige:98862
[27] E. A. Hidayat, "Kewenangan Penyadapan Badan Narkotika Nasional dalam Perspektif Undang-Undang Narkotika dan Undang-Undang Informasi dan Transaksi Elektronik," *Tadulako Master Law J.*, vol. 4, no. 2, hal. 129–145, 2020, [Daring]. Tersedia pada: http://103.245.72.41/index.php/TMLJ/article/view/197
[28] M. Kalacska dan M. Bouchard, "Using police seizure data and hyperspectral imagery to estimate the size of an outdoor cannabis industry," *Police Pract. Res.*, vol. 12, no. 5, hal. 424–434, Okt 2011, doi: 10.1080/15614263.2010.536722.
[29] K. Kopel, "Operation Seizing Our Sites: How the Federal Government is Taking Domain Names Without Prior Notice," *Berkeley Technol. Law J.*, vol. 28, no. 4, hal. 859–900, 2013, doi: 10.15779/Z384Q3M.
[30] S. de S. Sirisuriya, "A Comparative Study on Web Scraping," in *Proceedings of 8th International Research Conference, KDU*, Colombo: General Sir John Kotelawala Defence University, 2015, hal. 135–140. [Daring]. Tersedia pada: http://ir.kdu.ac.lk/handle/345/1051
[31] ScrapeOps, "Differences of Web Scraping Vs Web Crawling Explained," ScrapeOps. Diakses: 17 September 2024. [Daring]. Tersedia pada: https://scrapeops.io/web-scraping-playbook/web-scraping-vs-web-crawling/
[32] S. vanden Broucke dan B. Baesens, "From Web Scraping to Web Crawling," in *Practical Web Scraping for Data Science: Best Practices and Examples with Python*, S. vanden Broucke dan B. Baesens, Ed., Berkeley, CA: Apress, 2018, hal. 155–172. doi: 10.1007/978-1-4842-3582-9_6.
[33] J. Maybir dan B. Chapman, "Web scraping of ecstasy user reports as a novel tool for detecting drug market trends," *Forensic Sci. Int. Digit. Investig.*, vol. 37, hal. 301172, 2021, doi: 10.1016/j.fsidi.2021.301172.
[34] C. Muehlethaler dan R. Albert, "Collecting data on textiles from the internet using web crawling and web scraping tools," *Forensic Sci. Int.*, vol. 322, hal. 110753, 2021, doi: 10.1016/j.forsciint.2021.110753.
[35] E. Sonmez dan K. S. Codal, "Analyzing a Dark Web forum page in the context of terrorism: a topic modeling approach," *Secur. J.*, 2024, doi: 10.1057/s41284-024-00421-9.
[36] P. Jin, N. Kim, S. Lee, dan D. Jeong, "Forensic investigation of the dark web on the Tor network: pathway toward the surface web," *Int. J. Inf. Secur.*, vol. 23, no. 1, hal. 331–346, 2024, doi: 10.1007/s10207-023-00745-4.
[37] R. Basheer dan B. Alkhatib, "Conceptualizing Discussions on the Dark Web: An Empirical Topic Modeling Approach," *Complexity*, vol. 2024, no. 1, hal. 2775236, Jan 2024, doi: https://doi.org/10.1155/2024/2775236.
[38] W. Li, H. Chen, dan J. F. Nunamaker Jr., "Identifying and Profiling Key Sellers in Cyber Carding Community: AZSecure Text Mining System," *J. Manag. Inf. Syst.*, vol. 33, no. 4, hal. 1059–1086, Okt 2016, doi: 10.1080/07421222.2016.1267528.
[39] Á. Szigeti, R. Frank, dan T. Kiss, "Contribution to the harm assessment of darknet markets: topic modelling drug reviews on Dark0de Reborn," *Crime Sci.*, vol. 13, no. 1, hal. 13, 2024, doi: 10.1186/s40163-024-00211-z.
[40] G. Wiratmoko, H. Thamrin, dan E. W. Pamungkas, "Performance of Machine Learning Algorithms on Automatic Summarization of Indonesian Language Texts," *JOIN (Jurnal Online Inform.*, vol. 10, no. 1, hal. 196–204, 2025, doi: 10.15575/join.v10i1.1506.
[41] T. Alam dan R. Gupta, "Reviewing the Framework of Blockchain in Fake News Detection," *JOIN (Jurnal Online Inform.*, vol. 9, no. 2, hal. 286–296, 2024, doi: 10.15575/join.v9i2.1349.
[42] L. Greiner, "Sniper Forensics," *NetWorker*, vol. 13, no. 4, Association for Computing Machinery, New York, hal. 8–10, 2009. doi: 10.1145/1655737.1655740.
[43] C. Pogue, "Sniper Forensics 'One Shot, One Kill,'" *DEFCON 18*. DEF CON Communications, Inc., Las Vegas, hal. 1–33, 2010. [Daring]. Tersedia pada: https://archives.sector.ca/presentations09/Sector_SniperForensics92909_final%282%29.pdf
[44] G. M. Rao, B. R. Reddy, dan P. Vishnu, "Smart Web Investigation Framework," in *Innovations in Cyber Physical Systems*, J. Singh, S. Kumar, dan U. Choudhury, Ed., Singapore: Springer Singapore, 2021, hal. 305–314. doi: 10.1007/978-981-16-4149-7_27.
[45] W. Gong *et al.*, "Cyber victimization in hybrid space: an analysis of employment scams using natural language processing and machine learning models," *J. Crime Justice*, hal. 1–22, 2025, doi: 10.1080/0735648X.2024.2448804.
[46] Altenen, "Altenen Forums - Images & Videos & Porn Accounts?," Altenen. Diakses: 21 Maret 2024. [Daring]. Tersedia pada: https://altenens.is/forums/images-videos-porn-accounts.469197/
[47] Invision Community, "carding.store - Cracking Tutorials," carding.store. Diakses: 8 Juli 2024. [Daring]. Tersedia pada: https://carding.store/forum/20-cracking-tutorials/
[48] Astradumps, "Astra Dumps Shop," Astra Dumps. Diakses: 21 Maret 2024. [Daring]. Tersedia pada: https://astradumps.com/shop/
[49] @cashout vendors, "Money-Heist.org Shop," Money-Heist.org. Diakses: 8 Juli 2024. [Daring]. Tersedia pada:

https://money-heist.org/shop/
[50] Similarweb LTD, "Top 10 altenens.is Competitors," Similarweb LTD. Diakses: 26 Maret 2024. [Daring]. Tersedia pada: https://www.similarweb.com/website/altenens.is/competitors/
[51] J. Han, J. Kim, dan S. Lee, "5W1H-based Expression for the Effective Sharing of Information in Digital Forensic Investigations," New York, 2020. doi: 10.48550/arXiv.2010.15711.
[52] SysNucleus, "WebHarvy." SysNucleus, Kochi, 2024. [Daring]. Tersedia pada: https://www.webharvy.com/download.html
[53] Microsoft, "Microsoft Excel." Microsoft, Redmond, 2024. [Daring]. Tersedia pada: https://www.microsoft.com/en-in/microsoft-365/excel
[54] J. Demšar *et al.*, "Orange: Data Mining Toolbox in Python," *J. Mach. Learn. Res.*, vol. 14, no. 71, hal. 2349–2353, 2013, [Daring]. Tersedia pada: https://www.jmlr.org/papers/v14/demsar13a.html
[55] Zulhanif, "Pemodelan Topik dengan Latent Dirichlet Allocation," in *Seminar Nasional Pendidikan Matematika 2016*, Surakarta: Universitas Muhammadiyah Surakarta, 2016, hal. 1–8. [Daring]. Tersedia pada: https://publikasiilmiah.ums.ac.id/handle/11617/7633
[56] D. M. Blei, A. Y. Ng, dan M. I. Jordan, "Latent Dirichlet Allocation," *J. Mach. Learn. Res.*, vol. 3, hal. 993–1022, 2003, [Daring]. Tersedia pada: https://jmlr.csail.mit.edu/papers/v3/blei03a.html
[57] D. M. Blei, "Probabilistic topic models," *Communications of the ACM*, vol. 55, no. 4, Association for Computing Machinery, New York, NY, USA, hal. 77–84, April 2012. doi: 10.1145/2133806.2133826.
[58] F. B. Rodrigues, W. F. Giozza, R. de O. Albuquerque, dan L. J. G. Villalba, "Natural Language Processing Applied to Forensics Information Extraction With Transformers and Graph Visualization," *IEEE Trans. Comput. Soc. Syst.*, vol. 11, no. 4, hal. 4727–4743, 2024, doi: 10.1109/TCSS.2022.3159677.
[59] F. Amato, G. Cozzolino, V. Moscato, dan F. Moscato, "Analyse digital forensic evidences through a semantic-based methodology and NLP techniques," *Futur. Gener. Comput. Syst.*, vol. 98, hal. 297–307, 2019, doi: https://doi.org/10.1016/j.future.2019.02.040.
[60] F. I. Adristi, "Tesis Magister Informatika Fikri," Github. Diakses: 14 Desember 2024. [Daring]. Tersedia pada: https://github.com/451Fikrie/Tesis-Magister-Informatika-Fikri
[61] J. Xiaoyu, "Legal and Regulatory Research on the Involvement of Third Parties in Criminal Electronic Data Forensics," *Sci. Law J.*, vol. 3, no. 1, hal. 20–24, 2024, doi: 10.23977/law.2024.030104.
[62] A. bin Jamil, R. J. Johari, A. Zarefar, dan M. M. Yudi, "An analysis of suspicious transaction reporting decisions in Malaysia's money services business," *Edelweiss Appl. Sci. Technol.*, vol. 8, no. 1, hal. 24–32, 2024, doi: 10.55214/25768484.v8i1.413.
[63] K. Koo, M. Park, dan B. Yoon, "A Suspicious Financial Transaction Detection Model Using Autoencoder and Risk-Based Approach," *IEEE Access*, vol. 12, hal. 68926–68939, 2024, doi: 10.1109/ACCESS.2024.3399824.
[64] A. A. N. O. Y. Darmadi dan N. S. Dananjaya, "Authority of the Financial Transaction Analysis Reporting Center in Tracing Hidden Trading Crimes," *Sociol. Jurisprud. J.*, vol. 7, no. 1, hal. 8–14, 2024, doi: 10.22225/scj.7.1.2024.8-14.
[65] S. M. R. Noval *et al.*, "The Fusion of Blockchain, Pornography and Human Trafficking in A Global Digital Dragnet That Forms The Online Child Sex Trafficking," *Russ. Law J.*, vol. 11, no. 5s, hal. 1–19, 2023, [Daring]. Tersedia pada: https://cyberleninka.ru/article/n/the-fusion-of-blockchain-pornography-and-human-trafficking-in-a-global-digital-dragnet-that-forms-the-online-child-sex-trafficking
[66] T. Griné dan C. Teixeira Lopes, "A Social Media Tool for Domain-Specific Information Retrieval - A Case Study in Human Trafficking," in *Machine Learning and Principles and Practice of Knowledge Discovery in Databases. ECML PKDD 2022. Communications in Computer and Information Science, vol 1752*, I. Koprinska, P. Mignone, R. Guidotti, S. Jaroszewicz, H. Fröning, F. Gullo, P. M. Ferreira, D. Roqueiro, G. Ceddia, S. Nowaczyk, J. Gama, R. Ribeiro, R. Gavaldà, E. Masciari, Z. Ras, E. Ritacco, F. Naretto, A. Theissler, P. Biecek, W. Verbeke, G. Schiele, F. Pernkopf, M. Blott, I. Bordino, I. L. Danesi, G. Ponti, L. Severini, A. Appice, G. Andresini, I. Medeiros, G. Graça, L. Cooper, N. Ghazaleh, J. Richiardi, D. Saldana, K. Sechidis, A. Canakoglu, S. Pido, P. Pinoli, A. Bifet, dan S. Pashami, Ed., Cham: Springer Nature Switzerland, 2023, hal. 23–38.
[67] T. Alyahya dan F. Kausar, "Snapchat Analysis to Discover Digital Forensic Artifacts on Android Smartphone," *Procedia Comput. Sci.*, vol. 109, hal. 1035–1040, 2017, doi: 10.1016/j.procs.2017.05.421.
[68] K. Huie, M. Butler, dan A. Percy, "Identifying trends and patterns in offending and victimization on Snapchat: a rapid review," *Secur. J.*, vol. 37, no. 3, hal. 903–920, 2024, doi: 10.1057/s41284-023-00400-6.
[69] S. B. Yudhoyono dan A. Mattalatta, *Undang-undang (UU) No. 44 Tahun 2008 Tentang Pornografi*. Indonesia: JDIH BPK RI Database Peraturan, 2008, hal. 23. [Daring]. Tersedia pada: https://peraturan.bpk.go.id/Details/39740
[70] R.-T. Lo, W.-J. Hwang, dan T.-M. Tai, "SQL Injection Detection Based on Lightweight Multi-Head Self-Attention," *Applied Sciences*, vol. 15, no. 2. hal. 571, 2025. doi: 10.3390/app15020571.
[71] K. Takyi, R.-M. O. M. Gyening, M. Kobinnah, M. A. Boateng, dan S. Boadu-Acheampong, "Enhancing SQL Injection Detection with Long Short-Term Memory Networks in Deep Learning," *Int. J. Open Inf. Technol.*, vol. 13, no. 1, hal. 7–13, 2025, [Daring]. Tersedia pada: http://www.injoit.org/index.php/j1/article/view/1978
[72] A. Mechri, M. A. Ferrag, dan M. Debbah, "SecureQwen: Leveraging LLMs for vulnerability detection in python codebases," *Comput. Secur.*, vol. 148, hal. 104151, 2025, doi: 10.1016/j.cose.2024.104151.
[73] S. Flowers, "Harnessing the hackers: The emergence and exploitation of Outlaw Innovation," *Res. Policy*, vol. 37, no. 2, hal. 177–193, 2008, doi: 10.1016/j.respol.2007.10.006.
[74] J. Chen, S. He, dan X. Yang, "Platform Loophole Exploitation, Recovery Measures, and User Engagement: A Quasi-Natural Experiment in Online Gaming," *Inf. Syst. Res.*, vol. 35, no. 4, hal. 1609–1633, Nov 2023, doi: 10.1287/isre.2020.0416.
[75] A. Luthfi, "Documentation and Reporting ISO 27042:2015." Universitas Islam Indonesia, Yogyakarta, hal. 29, 2024.
[76] R. Soesilo, *Membuat Berita Acara dan Laporan Polisi Menurut KUHAP*. Bogor: Politeia, 1985.
[77] I. Arifisnti, E. Kustriyono, dan A. Pramitasari, "Pola Interogasi Penyidik terhadap Tersangka pada Berita Acara Pemeriksaan Kasus Delik Aduan Tinjauan Linguistik Forensik," *Parafrasa J. Bahasa, Sastra, dan Pengajaran*, vol. 6, no. 1, hal. 1–10, 2024, [Daring]. Tersedia pada: https://jurnal.unikal.ac.id/index.php/parafrasa/article/view/4668

[78] C. Baraniuk, "AlphaBay and Hansa dark web markets shut down," BBC. Diakses: 14 Desember 2024. [Daring]. Tersedia pada: https://www.bbc.com/news/technology-40670010
[79] Office of Public Affairs U.S. Department of Justice, "AlphaBay, the Largest Online 'Dark Market,' Shut Down," Office of Public Affairs U.S. Department of Justice. Diakses: 7 Maret 2024. [Daring]. Tersedia pada: https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down
[80] S.-T. Cheng, G.-J. Horng, C.-W. Hsu, dan Z.-Y. Su, "Per-user network access control kernel module with secure multifactor authentication," *J. Supercomput.*, vol. 80, no. 1, hal. 970–1008, 2024, doi: 10.1007/s11227-023-05480-0.
[81] A. Coscia, V. Dentamaro, S. Galantucci, A. Maci, dan G. Pirlo, "PROGESI: A PROxy Grammar to Enhance Web Application Firewall for SQL Injection Prevention," *IEEE Access*, vol. 12, hal. 107689–107703, 2024, doi: 10.1109/ACCESS.2024.3438092.
[82] R. Ruiz, R. Winter, F. de F. Rosa, P. Shukla, dan H. Kazemian, "Brazil Method of Anti-Malware Evaluation and Cyber Defense Impacts," *J. Appl. Secur. Res.*, vol. 18, no. 4, hal. 925–941, Okt 2023, doi: 10.1080/19361610.2022.2104104.
[83] Council of Europe, *Convention on Cybercrime*. European Union: European Treaty Series - No. 185, 2001. [Daring]. Tersedia pada: https://rm.coe.int/1680081561
[84] A. M. Aminu, "International Criminal Police Organisation and the Challenges in the Fight against Cybercrime in Nigeria," *Kashere J. Polit. Int. Relations*, vol. 2, no. 1, hal. 48–56, 2024, [Daring]. Tersedia pada: https://journals.fukashere.edu.ng/index.php/kjpir/article/view/178
[85] M. A. Ayanwale, I. T. Sanusi, R. R. Molefi, dan A. O. Otunla, "A Structural Equation Approach and Modelling of Pre-service Teachers' Perspectives of Cybersecurity Education," *Educ. Inf. Technol.*, 2023, doi: 10.1007/s10639-023-11973-5.
[86] ARTICLE 19, *Buku Panduan Moderasi Konten dan Kebebasan Berekspresi*. Uni Eropa & UNESCO, 2023. [Daring]. Tersedia pada: https://www.article19.org/wp-content/uploads/2024/03/BAHASA-Final-SM4P-Content-moderation-handbook-7-Aug-ID-translated-revised-022924_YHM.pdf
[87] S. Bhagat dan D. P. Pravin, "Cybersecurity Awareness and Adaptive Behavior: Does Prior Exposure Lead to Adaptive Behavior?," in *AMCIS 2023 Proceedings*, Panama City: AIS Electronic Library (AISel), 2023, hal. 23.
[88] Lanzarote, "Police Warn of 'Carding' Scam in The Canary Islands Costing Victims Thousands," Canarian Weekly. Diakses: 14 Januari 2025. [Daring]. Tersedia pada: https://www.canarianweekly.com/posts/Police-warn-of-carding-scam-in-the-Canary-Islands-costing-victims-thousands
[89] D. Dunsin, M. C. Ghanem, K. Ouazzane, dan V. Vassilev, "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response," *Forensic Sci. Int. Digit. Investig.*, vol. 48, hal. 301675, 2024, doi: 10.1016/j.fsidi.2023.301675.
[90] V. Gazeau, K. Gupta, dan M. K. An, "Enhancing Social Media Data Collection for Digital Forensic Investigations: A Web Parser Approach," in *2024 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Girona: IEEE, 2024, hal. 1–7. doi: 10.1109/CITS61189.2024.10607983.
[91] Z. Shahbazi dan Y.-C. Byun, "NLP-Based Digital Forensic Analysis for Online Social Network Based on System Security," *Int. J. Environ. Res. Public Health*, vol. 19, no. 12, hal. 7027, 2022, doi: 10.3390/ijerph19127027.
[92] A. Muhariya, I. Riadi, Y. Prayudi, dan I. A. Saputro, "Utilizing K-means Clustering for the Detection of Cyberbullying Within Instagram Comments," *Ing. des Syst. d'Information*, vol. 28, no. 4, hal. 939–949, 2023, doi: 10.18280/isi.280414.
[93] A. Muhariya, I. Riadi, dan Y. Prayudi, "Cyberbullying Analysis on Instagram Using K-Means Clustering," *JUITA J. Inform.*, vol. 10, no. 2, hal. 261–272, 2022, doi: 10.30595/juita.v10i2.14490.
[94] M. Zulfadhilah, Y. Prayudi, dan I. Riadi, "Cyber Profiling Using Log Analysis And K-Means Clustering," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 7, hal. 430–435, 2016, doi: 10.14569/IJACSA.2016.070759.