Cyber Evidence Software as the Digital Forensics Tools in the Investigation of Cybercrime[⋆]

Vladyslav Bilous[1,†], Dmytro Bodnenko[1,†], Oleksandra Lokaziuk[1,2,†], Pavlo Skladannyi[1,*,†] and Vadym Abramov[1,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine*

[2] *Institute of Mathematics of NAS of Ukraine, 3 Tereshchenkivska str., 01024 Kyiv, Ukraine*

Abstract

Digital forensics is the key element in the detection, preservation, and analysis of digital evidence, and helps in the investigation of complex cybercrimes such as identity theft and corporate espionage. The study emphasizes the importance of methods for analyzing physical data storage devices and arrays in crime investigations, in particular for identifying key individuals in criminal networks, which can lead to critical information. The paper also discusses the main difficulties of implementing digital forensic tools, including legal restrictions, technical problems, human factors, high cost, and complexity of integration. The comparative analysis of digital tools for investigating cybercrime, including data collection, data analysis, and data structure management tools, is made. Particular attention is paid to the author's software "Cyber Evidence", which offers a wide range of functions for analyzing electronic evidence and integrating with full data sources. This software allows cyber units and forensic experts to work efficiently with data, check for malware, and obtain digital evidence of cybercrime, making it one of the tools in the field of digital forensics.

Keywords

cybercrime, cyber forensic, digital forensic tool, data analytics, data analysis, software cyber evidence

1. Introduction

In the digital era of growing cybercrime, the problem of the evolution of investigative techniques arises, with digital forensics becoming a crucial component in the fight against online crime. Digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analyzing, and reporting electronically stored data [1].

Digital forensics tools [2, 3] play an important role in identifying, preserving, and analyzing digital evidence, helping law enforcement agencies and organizations solve complex cybercrimes ranging from identity theft to corporate espionage. The effectiveness of these tools can be measured by a variety of metrics, including their ability to recover deleted files, track digital traces, and provide actionable intelligence that leads to successful prosecutions. However, the implementation of digital forensics is not without its challenges; technical difficulties, such as the rapid development of technology outpacing forensic capabilities, along with legal and ethical concerns regarding privacy and admissibility of evidence, complicate the investigative environment. In addition, limitations inherent in current digital forensics technologies, such as the inability to effectively analyze encrypted data, underscore the ongoing need for innovation and adaptation in this area. Establishing best practices for digital forensics investigations, including systematic protocols for processing evidence and ensuring the reliability of digital evidence, is crucial to maximizing the effectiveness of these tools. With the multitude of digital forensics tools available, a comparative analysis of their characteristics and capabilities is essential for

[⋆] *CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2025, Kyiv, Ukraine*

[*] Corresponding author.

[†] These authors contributed equally.

v.bilous@kubg.edu.ua (V. Bilous); d.bodnenko@kubg.edu.ua (D. Bodnenko); o.lokaziuk@kubg.edu.ua (O. Lokaziuk); p.skladannyi@kubg.edu.ua (P. Skladannyi), v.abramov@kubg.edu.ua (V. Abramov)

0000-0001-6915-433X (V. Bilous); 0000-0001-9303-6587 (D. Bodnenko); 0000-0001-9663-251X (O. Lokaziuk); 0000-0002-7775-6039 (P. Skladannyi); 0000-0002-8026-1475 (V. Abramov)

investigators to select the best solutions. Solutions should be tailored to specific cases, including a thorough evaluation of both open-source and commercial options. As technology evolves, future trends such as the integration of artificial intelligence into digital forensics [4, 5] promise to improve investigative techniques, but also present new challenges that may redefine the parameters of digital crime investigations.

The objectives of this study are:

- Analyze the problems that arise when implementing digital forensics tools.
- Compare the use of tools in the investigation of cybercrime.
- Describe the author's software Cyber Evidence.

2. Research methodology

The following methods were used in the study: analysis of scientific literature on digital forensics tools; analysis of social networks; analysis of resources and methods for collecting digital evidence; software development; testing of the author's software to predict its further development; visualization of the data obtained to present the results of the study.

3. Results and discussion

3.1. Problems arising from the implementation of digital forensics tools

Digital forensics tools are indispensable in the modern fight against cybercrime, as they offer important capabilities for both detecting and prosecuting cybercriminals. These tools are specially designed to track information related to system or network breaches, and the information obtained can be important for identifying criminals and further prosecuting them in a forensic investigation [6]. The development of cybercrime requires the improvement of digital forensics tools. At the same time, there are obstacles to interagency cooperation that hinder the fight against cybercrime.

When evaluating the effectiveness of digital forensics tools, social network analysis (SNA) methods should be used [7]. One of the main functions of SNA is to identify key individuals to understand the dynamics of criminal networks and increase the effectiveness of investigations. SNA methods provide insight into the density of communications in the network, which can indicate the level of interaction and potential collusion between people, revealing the operational structure of the network. At the same time, analyzing the strength of ties between individuals or nodes makes it easier for investigators to optimize the investigation (relationships, priorities). The integration of SNA methods into digital forensics contributes to the efficiency and validity of investigations.

The introduction of digital forensics tools, such as the US Integrated Automated Fingerprint Identification System (IAFIS) and the UK National DNA Database (NDNAD), demonstrates their key role in modern crime-solving and intelligence gathering [7]. These systems are an example of how the use of advanced databases contributes to criminal investigations. SNA helps in mapping relationships and influence in networks, IAFIS and NDNAD provide the infrastructure for identifying individuals using biometric data, helping to narrow down the range of suspects and verify identities [7]. The UK's National Fingerprint Database (IDENT1) complements these systems by providing additional layers of verification and cross-referencing that together optimize the investigation process and increase the accuracy of criminal identification [7]. Databases are being improved and modernized. Ongoing cooperation between law enforcement agencies and technology developers is crucial to ensure that tools are effective and adapt to new challenges in solving crimes.

The analysis of sources [3, 4, 6] and the experience of developing and implementing OSINT-oriented software [8] gives grounds to highlight the most important problems that may arise when implementing digital forensics tools.

Legal restrictions

One of the main problems is the gap between the technological capabilities of digital forensics and the current legal framework. In many countries, legislation does not keep pace with rapid changes in technology.

International context. Collecting digital evidence often involves accessing data located outside the jurisdiction of the country of investigation. For example, criminals may store their files on servers located in countries with strict privacy laws or no international legal assistance agreements. In 2020, the European Union faced a problem when data obtained through violation of international cooperation procedures could not be used in court [9].

Maintaining confidentiality. Investigations often involve the extraction of data that contains the personal information of third parties. For example, analyzing a suspect's phone may reveal messages, photos, or other information belonging to third parties who are not parties to the case. This creates a conflict between the needs of the investigation and personal data protection legislation, such as the GDPR in the European Union [10].

Technical challenges

Adaptation to new technologies. The development of technology makes the work of digital forensic scientists more complex. For example, cloud-based technologies such as Amazon Web Services or Google Cloud allow criminals to quickly transfer data without having to physically seize the storage media. Another example is encryption, which is becoming a standard in many apps and services, such as Signal or WhatsApp. In such cases, access to data is often only possible through sophisticated technical solutions or cooperation with developers.

Data sets. The sheer volume of digital data is another challenge. For example, investigating a cybercrime may involve analyzing terabytes of information from a company's servers or cloud storage. This requires high-performance systems and algorithms that can quickly process such data. However, even with modern technology, such investigations can take days or weeks.

Human factor

Insufficient qualifications. The biggest challenge is staff training. For instance, the use of sophisticated tools such as FTK [11] or EnCase [12] requires specialized knowledge. Inexperienced professionals may make mistakes, for example, failing to record the chain of custody of evidence, which will lead to its discredit in court [13].

Errors in the process. Even minor mistakes during data extraction or analysis can have serious consequences. For instance, if an investigator accidentally changes the metadata of a file, it can be seen as tampering and cast doubt on the reliability of the evidence.

High cost

The cost of licenses and equipment. Many modern digital forensics tools are commercial and cost tens of thousands of dollars. For instance, a license for EnCase [12] can cost from 20,000 dollars, and specialized devices for analyzing mobile phones, such as Cellebrite UFED, have a similar price. This becomes a serious barrier to the implementation of such tools in countries with limited budgets.

Additional costs. In addition to purchasing licenses, you need to consider the costs of staff training, technical support, software, and infrastructure upgrades. This creates a significant financial burden even for large organizations.

Complexity of integration

Inconsistencies in data formats. Digital forensics tools often use different data formats, which makes it difficult to use them in an integrated manner. For example, one tool may generate reports in XML format, while another only supports CSV. To combine such data, additional software or manual work is required.

Time spent on integration. It can take months to integrate a new tool into an existing system, especially if the organization is using legacy systems. For example, institutions running on older operating systems often have problems with compatibility with modern tools.

The speed of development of cyber threats

Increasing complexity of threats. Hackers are constantly improving their methods. For example, ransomware has become more sophisticated, using double encryption and multi-level attacks. In the case of the WannaCry attack in 2017 [14], thousands of organizations suffered losses due to a lack of preparedness for such threats.

Use of anonymization. Anonymization via Tor or VPN makes it much more difficult for criminals to identify the perpetrators. Even after the device is removed, all activities can be hidden through encryption systems, anonymous accounts, and dynamic IP addresses [15–17].

3.2. Examples of the use of OSINT to document war crimes in Ukraine

A successful digital forensics investigation depends on several key steps to ensure both thoroughness and accuracy. First and foremost, organizations must establish robust training requirements for personnel involved in digital forensics investigations to ensure that they have the necessary skills and knowledge to handle complex cases. This training should cover the identification, handling, and storage of evidence, as these components are critical to maintaining the integrity of evidence throughout the investigation process. In addition, assessing and improving IT governance structures play a key role in supporting an effective digital forensics strategy. They provide the necessary structure and policies to manage digital evidence and align investigative practices with organizational goals. To increase preparedness, an organization should adopt a proactive approach to digital forensics (ProDF) by implementing measures that strengthen readiness for potential investigations or compliance tests. This includes defining clear goals, steps, and deliverables for ProDF to ensure a structured and efficient investigation process [18]. Comprehensive training facilitates successful investigations and enables organizations to respond effectively to potential digital threats or incidents. The comprehensive approach includes the implementation of standardized procedures for collecting, preserving, storing, and presenting digital evidence, which is critical to maintaining its integrity throughout the investigation process [19].

When working with digital forensics tools, it is crucial to follow recommended protocols to ensure the integrity and reliability of digital evidence. One of the main aspects of these protocols is to follow best practices in forensic data processing [20]. It is important to use:

Standardized methods for collecting, storing, and analyzing digital evidence. For example, when collecting data from a mobile device, software tools such as Cellebrite or XRY should be used to minimize the risk of data modification. In the case of analyzing a computer's hard disk, methods of creating copies of the disk using write-blocker devices are used to ensure the preservation of original information.

Integrity and chain of custody of digital evidence. For instance, when storing files from the suspect's servers, it is necessary to use hash functions such as MD5 or SHA-256 to record the file's checksum. This allows you to confirm that the data has not been altered during the investigation. Each step of evidence processing, including the transfer of evidence between experts, should be documented in the form of a "storage log."

A clear and documented data processing trail. For example, when removing email from a server, all actions should be documented, including the tools used, their versions, and the timestamps of each operation. The report should indicate which method was used, for example, exporting mail via IMAP or taking a snapshot of the server.

By implementing these practices, forensic investigators can effectively support court proceedings and ensure justice.

Comparison of digital forensics tools. Through a comparison of digital forensics tools [21–36], we emphasize the distinctive features and capabilities that distinguish open-source solutions from their commercial counterparts. We have analyzed the functionality and capabilities of digital forensics tools in specialized areas (Table 1).

Table 1
Functionality and capabilities of digital forensics tools in specialized areas

Tool Name	Features	Advantages	Disadvantages	License Type	Supported Platforms
			Data Acquisition Tools		
FTK Imager	Capture physical/logical data, export files, verify integrity	Free, simple, multi-file system support	Lacks full disk analysis	Free	Windows
Cellebrite UFED	Data extraction, decode deleted data, analyze calls/messages	Wide device range, regular updates	Expensive, requires training	Commercial	Windows
			Data Analysis Tools		
EnCase	File recovery, damaged media analysis, report generation	Handles big data, integrates with tools	Expensive, complex for beginners	Commercial	Windows
X-Ways Forensics	Metadata analysis, file recovery	High speed, low resource consumption	Complex interface	Commercial	Windows
			Data Recovery Tools		
Recuva	File recovery from drives, USBs	Free, intuitive interface	Limited free version	Free/Pro	Windows
R-Studio	Recover data from formatted/damaged drives, RAID support	High efficiency	Expensive	Commercial	Windows, macOS, Linux
			Network Traffic Analysis Tools		
Wireshark	Capture and analyze network traffic	Supports many protocols	Complex for beginners	GPL	Windows, macOS, Linux
Network Miner	Packet monitoring	Simple usage	Fewer features	Proprietary	Windows
			Mobile Device Analysis Tools		
Oxygen Forensic Suite	Data extraction from phones, IoT devices	Supports many models, regular updates	Expensive license, high system re	Commercial	Windows

Magnet AXIOM	Data extraction, cloud integration, social media analysis	Supports many data sources, quick processing	Expensive, resource-heavy	Commercial	Windows
Memory Analysis Tools					
Volatility	Memory dumps analysis, process/network/password discovery	Free, wide plugin support	Command-line complexity, limit	Open Source	Windows, Linux, macOS
Belkasoft RAM Capturer	Real-time memory capture	Simple interface, small size	Only captures, no analysis tools	Free	Windows
Email Analysis Tools					
MailXaminer	Email format support, metadata/IP analysis	Wide format support, multilingual analysis	Expensive license	Commercial	Windows
Aid4Mail	Email conversion, attachment analysis	Fast processing	The limited free version lacks forensic	Commercial	Windows
Case Management Tools					
CaseMap	Case database creation, evidence linkage	Intuitive interface, easy case management	Limited integration	Commercial	Windows
Nuix	Data/text/ email/ document analysis	Accurate, fast, complex file support	Expensive, complex for new users	Commercial	Windows, macOS, Linux

Open-source tools can corroborate evidence found with other products, which underscores their value in the verification process [8]. Although open-source tools are a cost-effective option, they require additional time and expertise, which requires targeted training interventions and capacity building in digital forensic investigations.

It is important to consider the tool's search and indexing capabilities; cross-platform capabilities; and the tool's ability to quickly process large volumes of digital forensic data. These criteria ensure that the selected tool meets the specific requirements of the investigation.

In the field of digital forensics, the choice between open-source and commercial tools involves weighing various factors such as cost, functionality, and support.

3.3. The author’s software “Cyber Evidence”

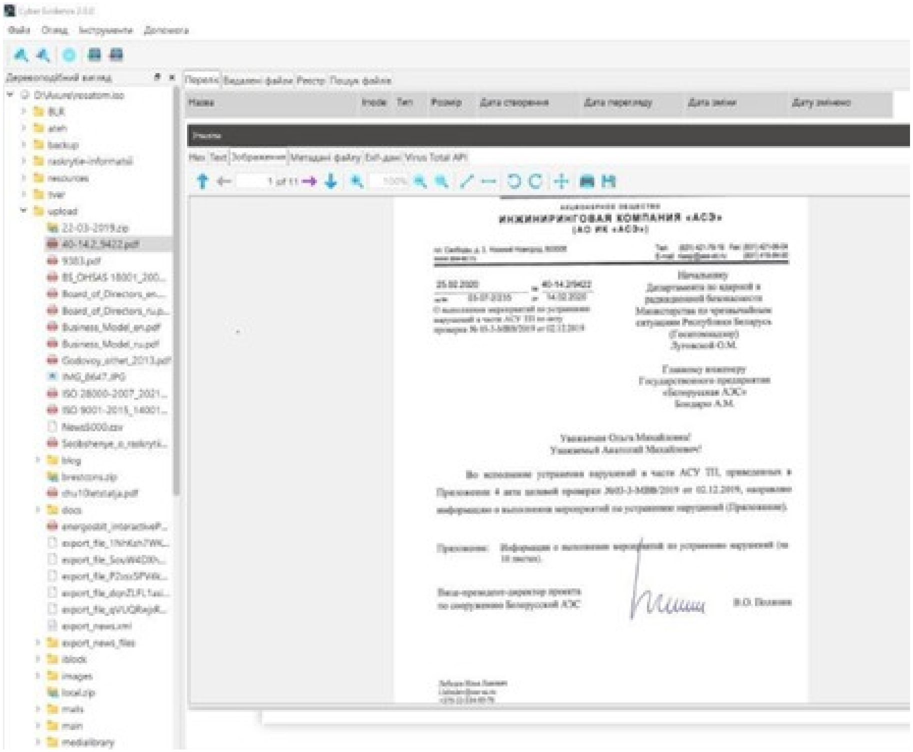
In the context of cybercrime investigations, we have created proprietary software that provides the following functions: Tools for data capture; Tools for analyzing digital evidence (RAID, RAW, etc.); Tools for data array recovery (Arsenal Image Mounter software is connected); Tools for analyzing mobile device operating systems (sleuthkit-4.12.0 framework is connected); Tools for analyzing registries (sleuthkit-4.12.0 framework is connected); Tools for analyzing various types of email (analogous to PSTViewer Pro). It is worth noting that part of the software functionality includes the OpenAI key API, which is used to obtain data on Verizon, Verifone API (mobile number databases), and digital embedded analytics of multimedia files. Artificial intelligence capabilities are built into Cyber Evidence and are used to analyze and provide analytics of multimedia files.

The name of the author’s software is Cyber Evidence. This is a digital forensic tool that provides an intuitive interface for analyzing images of mounted disks of various formats (*.iso, *.dd, *.E01, etc.) and includes some functionalities that help forensic experts extract and view the contents of various file and multimedia formats.

Features of the software product:

- Mounting images: Mounts forensic disk images (Windows only).
- Tree viewer: Navigate through the disk image structure, including partitions and files.
- Detailed file analysis: View file contents in various formats such as HEX, text, and application-specific formats.
- Extract EXIF data: Extract and display EXIF metadata from photos.
- View registry: View and explore Windows registry files.
- Basic file recovery: Recover deleted files from disk images.
- Integration with Virus Total API: Scan files for malware using the Virus Total API.
- Integration with Verizone API: Search for phone numbers in an international database for identification purposes.
- Scanning and recovery: Thanks to the built-in AI of the Dan model package, it is possible to recover deleted and damaged files [33].
- E01 Image Verification: Verifies the integrity of E01 disk images.
- Convert E01 to raw: Converts E01 disk images to a raw format.
- Message decoding: Decode messages from base64, binary, and other encodings. When testing the application, the following was done.
- Tested formats: The tool has been tested primarily with dd and E01 files. Although these formats are well supported, additional testing with other formats such as Ex01, Lx01, s01, and others is needed.
- File systems are tested: Currently, the tool is tested only on the NTFS file system. To ensure wider compatibility, testing with other file systems such as FAT32, exFAT, HFS+, APFS, EXT4, and others is required.

Here are fragments of the program’s operation. The program allows you to open various types of files inside it without harming your PC. An example of opening a mounted rosatom.iso image containing files from the servers of this structure (Fig. 1). The system automatically scans for vulnerabilities in the image, but manual scanning is also available and then allows you to view the file structure and open various types of files without harming your PC. In the example above, you can view a pdf file.



АКЦИОНЕРНОЕ ОБЩЕСТВО
ИНЖИНИРИНГОВАЯ КОМПАНИЯ «АСЭ»
(АО ИК «АСЭ»)

[illegible]

25.02.2020 № 40-14.2/9422
на № 03-07/2335 от 14.02.2020
О выполнении мероприятий по устранению нарушений в части АСУ ТП по акту проверки № 03-3-МВВ/2019 от 02.12.2019

Начальнику
Департамента по ядерной и радиационной безопасности
Министерства по чрезвычайным ситуациям Республики Беларусь
(Госатомнадзор)
Луговской О.М.

Главному инженеру
Государственного предприятия
«Белорусская АЭС»
Бондарю А.М.

Уважаемая Ольга Михайловна!
Уважаемый Анатолий Михайлович!

Во исполнение устранения нарушений в части АСУ ТП, приведенных в Приложении 4 акта целевой проверки №03-3-МВВ/2019 от 02.12.2019, направляю информацию о выполнении мероприятий по устранению нарушений (Приложение).

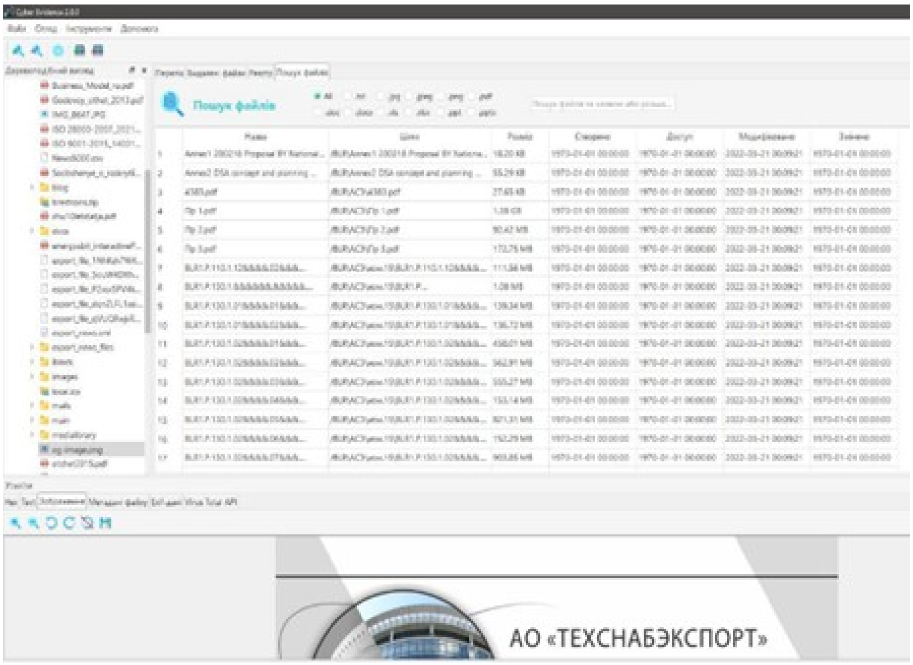
Приложение: Информация о выполнении мероприятий по устранению нарушений (на 10 листах).

Вице-президент-директор проекта
по сооружению Белорусской АЭС В.О. Поляков

[illegible]

Figure 1: Home screen interface of the application

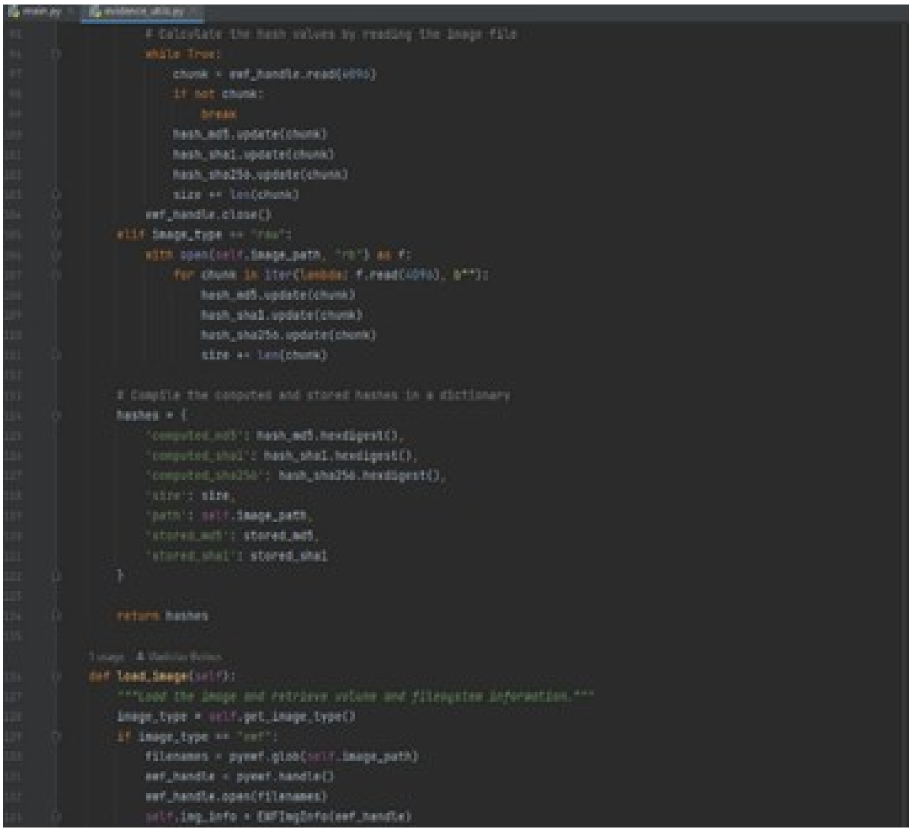
Here is an example of a general overview of all files on the mounted image (Fig. 2). You can determine the actual dates of creation and modification of files.


Cyber Evidence 2.0.0
Файл Огляд Інструменти Допомога
Деревоподібний вигляд
Перегляд Видалені файли Реєстр Пошук файлів
Пошук файлів
All
txt
jpg
jpeg
png
pdf
doc
docx
xls
xlsx
ppt
pptx
Пошук файлів за назвою або розшир...
Hex Text Зображення Метадані файлу Exif-дані Virus Total API
АО «ТЕХСНАБЭКСПОРТ»

	Назва	Шлях	Розмір	Створено	Доступ	Модифіковано	Змінено
1	Annex1 200218 Proposal BY National...	/BLR/Annex1 200218 Proposal BY Nationa...	18.20 KB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
2	Annex2 DSA concept and planning ...	/BLR/Annex2 DSA concept and planning ...	55.29 KB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
3	4383.pdf	/BLR/ACh/4383.pdf	27.63 KB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
4	Пр 1.pdf	/BLR/ACh/Пр 1.pdf	1.38 GB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
5	Пр 2.pdf	/BLR/ACh/Пр 2.pdf	90.42 MB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
6	Пр 3.pdf	/BLR/ACh/Пр 3.pdf	172.75 MB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
7	BLR1.P.110.1.12&&&&&02&&&...	/BLR/ACh/[illegible]/BLR1.P.110.1.12&&&&...	111.58 MB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
8	BLR1.P.130.1.&&&&&&&&&&&&...	/BLR/ACh/[illegible]/BLR1.P...	1.08 MB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
9	BLR1.P.130.1.01&&&&&01&&&...	/BLR/ACh/[illegible]/BLR1.P.130.1.01&&&&...	139.34 MB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
10	BLR1.P.130.1.01&&&&&02&&&...	/BLR/ACh/[illegible]/BLR1.P.130.1.01&&&&...	136.72 MB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
11	BLR1.P.130.1.02&&&&&01&&&...	/BLR/ACh/[illegible]/BLR1.P.130.1.02&&&&...	458.01 MB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
12	BLR1.P.130.1.02&&&&&02&&&...	/BLR/ACh/[illegible]/BLR1.P.130.1.02&&&&...	342.91 MB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
13	BLR1.P.130.1.02&&&&&03&&&...	/BLR/ACh/[illegible]/BLR1.P.130.1.02&&&&...	555.27 MB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
14	BLR1.P.130.1.02&&&&&04&&&...	/BLR/ACh/[illegible]/BLR1.P.130.1.02&&&&...	153.14 MB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
15	BLR1.P.130.1.02&&&&&05&&&...	/BLR/ACh/[illegible]/BLR1.P.130.1.02&&&&...	821.31 MB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
16	BLR1.P.130.1.02&&&&&06&&&...	/BLR/ACh/[illegible]/BLR1.P.130.1.02&&&&...	152.29 MB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00
17	BLR1.P.130.1.02&&&&&07&&&...	/BLR/ACh/[illegible]/BLR1.P.130.1.02&&&&...	903.85 MB	1970-01-01 00:00:00	1970-01-01 00:00:00	2022-03-21 20:09:21	1970-01-01 00:00:00

Figure 2: Screenshot of files on the mounted image

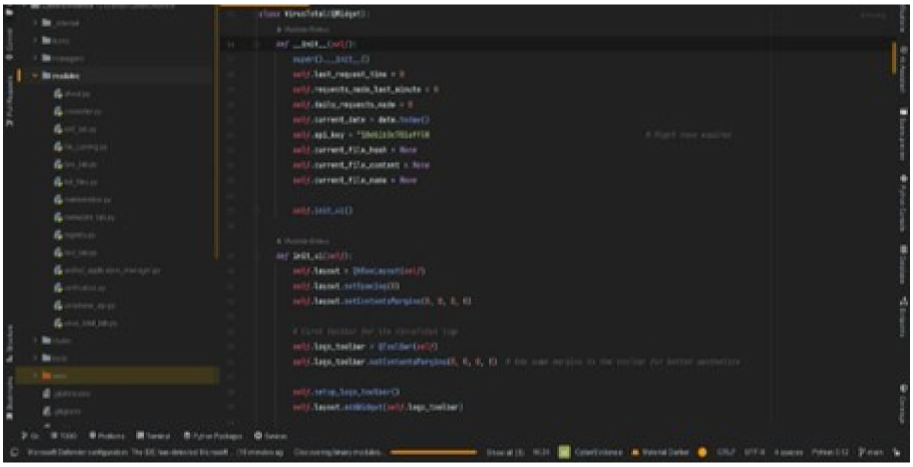
An example of encryption and decryption code for collecting checksums is in Fig. 3.



```
        # Calculate the hash values by reading the image file
        while True:
            chunk = ewf_handle.read(4096)
            if not chunk:
                break
            hash_md5.update(chunk)
            hash_sha1.update(chunk)
            hash_sha256.update(chunk)
            size += len(chunk)
        ewf_handle.close()
    elif image_type == "raw":
        with open(self.image_path, "rb") as f:
            for chunk in iter(lambda: f.read(4096), b""):
                hash_md5.update(chunk)
                hash_sha1.update(chunk)
                hash_sha256.update(chunk)
                size += len(chunk)

    # Compile the computed and stored hashes in a dictionary
    hashes = {
        'computed_md5': hash_md5.hexdigest(),
        'computed_sha1': hash_sha1.hexdigest(),
        'computed_sha256': hash_sha256.hexdigest(),
        'size': size,
        'path': self.image_path,
        'stored_md5': stored_md5,
        'stored_sha1': stored_sha1
    }

    return hashes

def load_image(self):
    """Load the image and retrieve volume and filesystem information."""
    image_type = self.get_image_type()
    if image_type == "ewf":
        filenames = pyewf.glob(self.image_path)
        ewf_handle = pyewf.handle()
        ewf_handle.open(filenames)
        self.img_info = EWFImgInfo(ewf_handle)
```

Figure 3: A code snippet for encrypting and decrypting files

The following program snippet shows the connection of the artificial intelligence API to find vulnerabilities using VirusTotal, a cloud-based scanner for rootkits, randomizers, trojans, etc. This example shows the connection of both manual and automatic scanning in Fig. 4.



```
class VirusTotal(QWidget):
    def __init__(self):
        super().__init__()
        self.last_request_time = 0
        self.requests_made_last_minute = 0
        self.daily_requests_made = 0
        self.current_date = date.today()
        self.api_key = '[illegible]'                    # [illegible]
        self.current_file_hash = None
        self.current_file_content = None
        self.current_file_name = None

        self.init_ui()

    def init_ui(self):
        self.layout = QVBoxLayout(self)
        self.layout.setSpacing(0)
        self.layout.setContentsMargins(0, 0, 0, 0)

        # [illegible]
        self.logo_toolbar = QToolBar(self)
        self.logo_toolbar.setContentsMargins(0, 0, 0, 0)  # [illegible]

        self.setup_logo_toolbar()
        self.layout.addWidget(self.logo_toolbar)
```

Figure 4: The connection of the artificial intelligence API

Prospects for further research are seen in improving the software (and creating instructions for using the software) to expand the following functionality:

- Live video/audio playback: Currently, the video and audio player temporarily store files before playing them, which can cause delays. The goal is to enable direct playback to speed up the experience.

- Integrated file search and browsing: The file search function is not yet connected to the View tab, which displays HEX, text, application-specific views, metadata, and other details. This integration needs to be implemented.
- Cross-platform image mounting: Image mounting currently only works on Windows using the Arsenal Image Mounter executable. The goal is to make this feature work on all platforms without relying on external executables.
- File cutting and integration with viewers: The file-cutting functionality is not yet connected to the "Viewer Tab" where users can view HEX, text, application-specific views, and metadata. In addition, the current file cut process does not distinguish between deleted and uninstalled files; it "cuts" all files of the selected file type from the disk image.

Problems with color in dark mode: The program is currently experiencing some color display issues on Linux and macOS systems when using dark mode. Certain interface elements may be fuzzy or display incorrectly.

Conclusions

The results of this study highlight the important role of methods of digital data analytics in improving investigative outcomes by identifying key influencers in criminal networks, which can lead to the disclosure of critical information that might otherwise remain hidden.

Based on the analysis of using of digital forensics tools, the authors identify the main difficulties that may arise in their implementation, including legal restrictions (international context and confidentiality), technical challenges (adaptation to new technologies and data sets), human factor (lack of qualifications and errors in the process), high cost (cost of licenses and equipment, additional costs), complexity of integration (inconsistencies in data formats and time spent on integration), speed of cyber threats (increasing complexity of threats and the use of anonymization).

A comparative analysis and systematization of digital tools that can be used in the investigation of cybercrime is carried out. A list of titles of digital forensics tools is provided by key functionality, which includes Features, Advantages, Disadvantages, License Type, and Supported Platforms. Each of the proposed tools was recommended for use among software products: Data Acquisition Tools, Data Analysis Tools, Data Recovery Tools, Network Traffic Analysis Tools Mobile, Device Analysis Tools, Memory Analysis Tools, Email Analysis Tools, and Case Management Tools.

This study proposes the author's software "Cyber Evidence," which is a digital forensics tool that provides a wide range of functions for analyzing and processing data in the context of cybercrime. The software includes tools for capturing data, analyzing electronic evidence, recovering information from disks, and integrating with APIs to retrieve data from various sources. The system allows users (e.g., cyber specialists and/or forensic experts) to work with disk images of various formats, view file contents, obtain digital evidence of cybercrime, and check for malware [37]. The work contains screenshots of fragments of software and software code snippets [38, 39].

Acknowledgments

The research was carried out within the framework of: the complex scientific theme of the Faculty of Information Technologies and Mathematics "Mathematical methods and digital technologies in education, science, technology," DR No. 0121U111924; the scientific theme of the Department of Information and Cyber Security named after Professor Volodymyr Buryachok of Borys Grinchenko Kyiv Metropolitan University "Methods and models of ensuring cyber security of information processing systems and functional security of software and technical complexes of critical infrastructure management," DR No. 0122U200483, and the research by a grant from the Simons Foundation (1290607, O. L.).

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] Interpol.int, Digital forensics, 2024. URL: https://www.interpol.int/How-we-work/Innovation/Digital-forensics

[2] K. Sindhu, B. Meshram, Digital forensics and cyber crime datamining, J. Inf. Secur. 03(03) (2012) 196–201. doi:10.4236/jis.2012.33024.

[3] K. Kaushik, M. Ouaissa, A. Chaudhary, Advanced techniques and applications of cybersecurity and forensics, Chapman and Hall, 2024. URL: https://f.eruditor.link/file/4195730/

[4] M. Omar, Digital forensics in the age of AI, IGI Global, 2025. doi:10.4018/979-8-3373-0857-9.

[5] H. Zangana, M. Omar, Introduction to digital forensics and artificial intelligence, Advances in Digital Crime, Forensics, and Cyber Terrorism (2025) 1–30. doi:10.4018/979-8-3373-0857-9.ch001

[6] Enisa Europa, Report on the State of cybersecurity in the union—condensed version, Publication, 2024. URL: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

[7] A. Irons, H. Lallie, Digital forensics to intelligent forensics, Future Internet, 6 (2014) 584–596. doi:10.3390/fi6030584

[8] V. Bilous, et al., Open source intelligence for war crime documentation, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654, 2024, 368–375.

[9] Hudoc Echr Coe, HUDOC, European court of human rights, 2024. URL: https://hudoc.echr.coe.int/ukr#{%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22,%22DECGRANDCHAMBER%22]}

[10] Eur-Lex Europa, Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016. URL: http://data.europa.eu/eli/reg/2016/679/2016-05-04

[11] Exterro.Com, FTK forensic toolkit, 2025. URL: https://www.exterro.com/digital-forensics-software/forensic-toolkit/

[12] Cybermarket.Com, EnCase forensic, 2022. URL: https://cybermarket.com.ua/product/encase-forensic/

[13] Z. B. Hu, V. Buriachok, V. Sokolov, Implementation of social engineering attack at institution of higher education, in: 1st International Workshop on Cyber Hygiene & Conflict Management in Global Information Networks (CybHyg), vol. 2654 (2020) pp. 155–164.

[14] S. Mohurle, M. Patil, A brief study of wannacry threat: Ransomware attack 2017, Int. J. Adv. Res. Comput. Sci. 8 (2017) 1938–1940.

[15] O. Mykhaylova, et al., Mobile application as a critical infrastructure cyberattack surface, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II, vol. 3550 (2023) 29–43.

[16] M. TajDini, V. Sokolov, P. Skladannyi, Performing sniffing and spoofing attack against ADS-B and Mode S using Software Define Radio, in: IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (2021) 7–11. doi:10.1109/UkrMiCo52950.2021.9716665

[17] M. TajDini, V. Sokolov, V. Buriachok, Men-in-the-middle attack simulation on low energy wireless devices using software define radio, in: 8th International Conference on "Mathematics.

Information Technologies. Education:” Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 287–296.

[18] C. Grobler, C. Louwrens, S. von Solms, A framework to guide the implementation of proactive digital forensics in organisations, in: 2010 International Conference on Availability, Reliability and Security, 2010, 677–682. doi:10.1109/ARES.2010.62

[19] J. Sachowski, Implementing digital forensic readiness: From reactive to proactive process, Boca Raton: CRC Press, 2021.

[20] A. Malik, et al., Cloud digital forensics: Beyond tools, techniques, and challenges, Sensors 24 (2024). doi:10.3390/s24020433

[21] Exterro, FTK imager 4.7.3.81, 2025. URL: https://www.exterro.com/ftk-product-downloads/ftk-imager-4-7-3-81

[22] Cellebrite, Cellebrite UFED, The industry standard for lawfully accessing and collecting digital data, 2025. URL: https://cellebrite.com/en/ufed/

[23] Guidancesoftware, OpenText Forensic (EnCase), 2025. URL: https://www.guidancesoftware.com/encase-forensic

[24] X-Ways, X-Ways forensics: Integrated computer forensics software, 2025. URL: https://x-ways.net/forensics/

[25] Ccleaner, Recuva, recover your deleted files quickly and easily, 2025. URL: https://www.ccleaner.com/recuva

[26] R-Studio, Disk recovery software and hard drive recovery tool, 2025. URL: https://www.r-studio.com/

[27] Wireshark.org, The world’s most popular network protocol analyzer, 2025. URL: https://www.wireshark.org/

[28] Network Miner, 2025. URL: https://www.netresec.com/?page=NetworkMiner

[29] Oxygenforensics.Com, Oxygen Forensic Suite, 2025. URL: https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective

[30] Magnetforensics.Com, Magnet AXIOM, 2025. URL: https://www.magnetforensics.com/products/magnet-axiom/

[31] Volatilityfoundation, Volatility, 2025. URL: https://www.volatilityfoundation.org/

[32] Belkasoft, Belkasoft RAM Capturer, 2025. URL: https://belkasoft.com/ram-capturer

[33] Mail Xaminer, Know MailXaminer’s Range & Areas of Investigation, 2025. URL: https://www.mailxaminer.com/

[34] Aid4Mail, Software for email forensics, eDiscovery & Conversion, 2025. URL: https://www.aid4mail.com/

[35] Cloudnine, Discovery document review software for law firms and enterprises, 2025. URL: https://cloudnine.com/ediscovery-software/cloudnine-review/

[36] Nuix.Com, Helping to protect, govern and leverage enterprise data, 2025. URL: https://www.nuix.com/

[37] R. Marusenko, V. Sokolov, P. Skladannyi, Social engineering penetration testing in higher education institutions, Advances in Computer Science for Engineering and Education VI, vol. 181 (2023) 1132–1147.

[38] M. Astafieva, et al., Formation of high school students’ resistance to destructive information influences, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 87-96.

[39] V. Buriachok, et al., Implementation of active cybersecurity education in Ukrainian higher school, Information Technology for Education, Science, and Technics, vol. 178 (2023) 533–551. doi:10.1007/978-3-031-35467-0_32