ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

2025 (24) 4

қазан- желтоқсан

ISSN 2708–2032 (print)
ISSN 2708–2040 (online)

Халықаралық ақпараттық және коммуникациялық технологиялар журналы
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Меншік иесі: АҚ «Халықаралық ақпараттық технологиялар университеті» (Алматы қ.).
Қазақстан Республикасы Ақпарат және қоғамдық даму министрлігіне мерзімді баспасөз басылымын есепке қою туралы куәлік № KZ82VPY00020475, 20.02.2020 ж. берілген
Тақырып бағыты: ақпараттық технологиялар, ақпараттық қауіпсіздік және коммуникациялық технологиялар, әлеуметтік-экономикалық жүйелерді дамытудағы цифрлық технология.
Мерзімділігі: жылына 4 рет.
Тираж: 100 дана.
Редакция мекенжайы: 050040 Алматы қ., Манас к., 34/1, каб. 709, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz
Журнал сайты: https://journal.iitu.edu.kz

Международный журнал информационных и коммуникационных технологий
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (г. Алматы).
Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан **№ KZ82VPY00020475,** выданное от **20.02.2020 г.**
Тематическая направленность: информационные технологии, информационная безопасность и коммуникационные технологии, цифровые технологии в развитии социо-экономических систем**.**
Периодичность: 4 раза в год.
Тираж: 100 экземпляров.
Адрес редакции: 050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz Сайт журнала: https://journal.iitu.edu.kz

«International Journal of Information and Communication Technologies»
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Owner: International Information Technology University JSC (Almaty).
The certificate of registration of a periodical printed publication in the Ministry of Information and Social Development of the Republic of Kazakhstan, Information Committee No. KZ82VPY00020475, issued on 20.02.2020.
Thematic focus: information technology, digital technologies in the development of socio-economic systems, information security and communication technologies
Periodicity: 4 times a year.
Circulation: 100 copies.
Editorial address: 050040. Manas st. 34/1, Almaty. +7 (727) 244-51-09. E-mail: ijict@iitu.edu.kz
Journal website: https://journal.iitu.edu.kz

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 6. Is. 4. Number 24 (2025). Pp. 153–173
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2025.24.4.009
UDC 004.021

MATHEMATICAL FILTERING IN CALL HISTORY FORENSICS MODULE

T. Grigoryev[1], P. Tazhibayeva[1*], A. Imanberdi[2], R. Lisnevskyi[1]
[1,]Astana IT University, Astana, Kazakhstan;
[2]TSARKA GROUP, Astana, Kazakhstan.
E-mail: 242924@astanait.edu.kz

Abulkair Imanberdi — Master of Science, head of the team of "TSARKA" GROUP, Astana, Kazakhstan
https://orcid.org/0009-0005-6144-2392;
Timur Grigoriev — Master's student, BSc, researcher, Astana IT University, Astana, Kazakhstan
https://orcid.org/0009-0002-1082-5295;
Tazhibayeva Perizat — Master's student, BSc, researcher, Astana IT University, Astana, Kazakhstan
https://orcid.org/0009-0009-1566-636X;
Lisnevskyi Rostyslav — PhD, associate professor, Cybersecurity School, Astana IT University, Astana, Kazakhstan
https://orcid.org/ 0000-0002-9006-6366.

Abstract. The growing sophistication of technology-enabled crime demands that forensic practitioners move beyond data extraction toward analytical interpretation. This study evaluates four major suites - Cellebrite UFED, Oxygen Forensic Detective, Elcomsoft iOS Forensic Toolkit, and MOBILedit Pro - focusing on their ability to parse call logs from modern Android and iOS devices. While reliable in acquisition, these tools show recurring limitations: incomplete reconstruction of fragmented SQLite tables, weak temporal visualization, and poor cross-device correlation. To address these issues, we propose a lightweight Call History Analysis Module that integrates into existing workflows. It unifies heterogeneous call databases into a chronological ledger, applies mathematical filters to detect patterns or anomalies, and visualizes communication trends via heatmaps, duration ridgelines, and ego-network graphs. A built-in similarity search engine identifies shared contacts and parallel timelines. Pilot testing confirms improved accuracy, reduced triage time, and enhanced contextual insight, extending digital forensic capabilities at minimal operational cost.

Keywords: forensics, mobile, calls, analysis, filtering, visualization, evidence

For citation: T. Grigoryev, P. Tazhibayeva, A. Imanberdi, R. Lisnevskyi. Mathematical Filtering in Call History Forensics Module//International journal of information and communication technologies. 2025. Vol. 6. No. 24. Pp. 153–173.

(In Eng.). https://doi.org/10.54309/IJICT.2025.24.4.009.

Conflict of interest: The authors declare that there is no conflict of interest.

ҚОҢЫРАУЛАР ТАРИХЫНДАҒЫ СОТ САРАПТАМАСЫ МОДУЛІНДЕГІ МАТЕМАТИКАЛЫҚ СҮЗУ

Т. Григорьев[1], П. Тажибаева[1], А. Иманберді[2], Р. Лисневский[1]
[1]Astana IT University, Астана, Қазақстан;
[2]TSARKA GROUP, Астана, Қазақстан.
E-mail: 242924@astanait.edu.kz

Иманберді Әбілқайыр — Ғылым Магистрі, «ЦАРКА» ТОБЫ ұжымының жетекшісі
https://orcid.org/0009-0005-6144-2392;
Григорьев Тимур — магистрант, бакалавр, Астана IT Университетінің ғылыми қызметкері
https://orcid.org/0009-0002-1082-5295;
Перизат Тажибаева — магистрант, бакалавр, Astana IT Университетінің ғылыми қызметкері
https://orcid.org/0009-0009-1566-636x;
Лисневский Ростислав — PhD, Астана IT университетінің киберқауіпсіздік мектебінің доценті
https://orcid.org/ 0000-0002-9006-6366.

Аннотация. Технологияны қолдана отырып жасалған қылмыстардың өсіп келе жатқан күрделілігі сот-медициналық сарапшылардан деректерді жинау шеңберінен шығып, аналитикалық интерпретацияға көшуді талап етеді. Бұл зерттеу төрт негізгі жиынтықты бағалайды - Cellebrite UFED, Oxygen Forensic Detective, Elcomsoft Ios Forensic Toolkit және MOBILedit Pro - олардың заманауи Android және iOS құрылғыларындағы қоңыраулар журналдарын талдау қабілетіне бағытталған. Сатып алу кезінде сенімді болғанымен, бұл құралдар қайталанатын шектеулерді көрсетеді: Фрагменттелген SQLite кестелерінің толық емес қайта құрылуы, әлсіз уақытша визуализация және құрылғылар арасындағы нашар корреляция. Осы мәселелерді шешу үшін біз Бар Жұмыс процестеріне біріктірілген Қоңыраулар Тарихын Талдаудың жеңіл Модулін ұсынамыз. Ол қоңыраулардың гетерогенді дерекқорларын хронологиялық кітапқа біріктіреді, заңдылықтарды немесе ауытқуларды анықтау үшін математикалық сүзгілерді қолданады және жылу карталары, ұзақтық сызықтары және эго-желілік графиктер арқылы байланыс тенденцияларын визуализациялайды. Кірістірілген ұқсастық іздеу жүйесі ортақ контактілерді және параллель уақыт кестелерін анықтайды. Пилоттық тестілеу дәлдіктің жақсарғанын, сұрыптау уақытының қысқарғанын және контекстік түсініктің жақсарғанын растайды, бұл цифрлық сот сараптамасының мүмкіндіктерін ең аз

операциялық шығындармен кеңейтеді.

Түйін сөздер: Криминалистика, Ұялы Байланыс, Қоңыраулар, Талдау, Сүзу, Визуализация, Дәлелдемелер

Дәйексөздер үшін: Ә. Иманберді, Т. Григорьев, П. Тажибаева, Р. Лисневский. Қоңыраулар Тарихындағы Сот Сараптамасы Модуліндегі Математикалық Сүзу // Халықаралық ақпараттық және коммуникациялық технологиялар журналы. 2025. Том. 6. № 24. 153–173 бет. (Ағыл). https:// doi. org/10.54309/IJICT.2025.24.4.009.

Мүдделер қақтығысы: Авторлар осы мақалада мүдделер қақтығысы жоқ деп мәлімдейді.

МАТЕМАТИЧЕСКАЯ ФИЛЬТРАЦИЯ В МОДУЛЕ СУДЕБНОЙ ЭКСПЕРТИЗЫ ИСТОРИИ ЗВОНКОВ

Т. Григорьев[1], П. Тажибаева[1], А. Иманберди[2], Р. Лисневский[1]

[1]Астана ИТ университет, Астана, Казахстан;
[2]TSARKA GROUP, Астана, Казахстан.
Email: 242924@astanait.edu.kz

Иманберди Абулкаир — магистр наук, руководитель команды группы компаний «ЦАРКА»
https://orcid.org/0009-0005-6144-2392;
Тимур Григорьев — магистрант, бакалавр, исследователь, Астана ИТ университет, Астана, Казахстан
https://orcid.org/0009-0002-1082-5295;
Тажибаева Перизат — магистрант, бакалавр, исследователь, Астана ИТ университет, Астана, Казахстан
https://orcid.org/0009-0009-1566-636x;
Ростислав Лисневский — кандидат технических наук, доцент, Школа кибербезопасности, Астана ИТ университет, Астана, Казахстанhttps://orcid.org/ 0000-0002-9006-6366.

Аннотация. Растущая сложность преступлений, совершаемых с использованием современных технологий, требует от судебно-медицинских экспертов перехода от извлечения данных к аналитической интерпретации. В этом исследовании оцениваются четыре основных пакета - Cellebrite UFED, Oxygen Forensic Detective, Elcomsoft iOS Forensic Toolkit и MOBILedit Pro - с акцентом на их способность анализировать журналы вызовов с современных устройств Android и iOS. Несмотря на надежность сбора данных, эти инструменты имеют ряд недостатков: неполное восстановление фрагментированных таблиц SQLite, слабая временная визуализация и плохая корреляция между устройствами. Для решения этих проблем мы предлагаем легкий модуль анализа истории звонков, который интегрируется в существующие рабочие процессы. Он объединяет

разнородные базы данных о звонках в хронологический реестр, применяет математические фильтры для выявления закономерностей или аномалий и визуализирует тенденции обмена сообщениями с помощью тепловых карт, временных линий и графиков эго-сети. Встроенная система поиска сходства идентифицирует общие контакты и параллельные временные линии. Пилотное тестирование подтверждает повышение точности, сокращение времени сортировки и улучшение понимания контекста, расширяя возможности цифровой криминалистики при минимальных эксплуатационных затратах.

Ключевые слова: криминалистика, телефон, звонки, анализ, фильтрация, визуализация, доказательства

Для цитирования: Т. Григорьев, П. Тажибаева, А. Иманберди, Р. Лисневский. Математическая фильтрация в модуле судебной экспертизы истории звонков//Международный журнал информационных и коммуникационных технологий. 2025. Т. 6. No. 23. Стр. 153–173. (На анг.). https://doi.org/10.54309/IJICT.2025.24.4.009.

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Introduction

Due to the exponential rise in cybercrime, digital forensics plays a critical role in supporting legal investigations and ensuring evidentiary integrity (Batra: 2020: 42–46). This involves analyzing various devices, including computers, tablets, SIM cards, and, most importantly, mobile phones, which have become integral to daily life due to their widespread use and large storage capacities (Alatawi: 2020: 1–6). Digital forensics plays a critical role in modern law enforcement, cybersecurity, and legal investigations and offers the technical framework to ensure the integrity and reliability of digital evidence (Mahmoud: 2023: 1–6).

Data extraction and analysis are the two primary stages of digital forensic investigations, and global trends in these areas should be reviewed (Shimmi: 2020: 1–7). It is important to take into consideration that the second stage was developed only after the development of modern technologies for accounting and registration of new digital information about a person and his environment, which are generated in automatic, semi-automatic and manual mode and in unlimited quantities. As a result, nowadays the stage of forensic analysis is equally important with the extraction stage (Khalaf: 2019: 1–5).

For example, artificial intelligence enhances data analysis, blockchain ensures evidence authenticity, and cloud solutions facilitate the storage and processing of large amounts of information (Tyagi: 2022: 1–6).

Data analysis technologies, particularly those leveraging artificial intelligence, are increasingly critical and widely adopted (Rizvi: 2022: 110362–110384). For instance: AI helps automate routine tasks such as extracting and classifying data from various sources, can perform semantic analysis, especially analyzing text messages and emails to identify potential malicious content or threat (Waluyo: 2022: 95–100). In addition, machine learning models can be used to predict likely locations and types of crimes based on historical data (Punjabi: 2022: 1–5).

There are a number of important fields that is needed to be taken into consideration for digital forensics analysis:

1. Artificial Intelligence (AI) and Machine Learning (ML)
2. Cloud technologies
3. Internet of Things (IoT)
4. Blockchain

Artificial Intelligence (AI) and Machine Learning (ML) are revolutionizing digital forensics by automating complex tasks and increasing the accuracy of investigations (Rizvi: 2022: 110362–110384).

Cloud technologies are also important, because more and more organizations move their data and application to the cloud, cloud forensics is becoming an important area of attention. It presents unique challenges for criminologists, such as data variability, multi-user architecture and jurisdiction issues (Fernandes: 2020: 422–427).

Internet of Things forensics involves extracting and analyzing data from interconnected devices such as smart home systems, wearable technologies, and industrial control systems. These devices generate huge amounts of data, and forensic investigators must develop specialized methods to process the variety and volume of information (Fernandes: 2020: 422–427).

Blockchain Technology is known for its secure and immutable registry and gaining momentum in digital forensics. It is relevant for investigation of crimes related to cryptocurrency, such as fraud, money laundering, corruption and attacks using ransomware. Furthermore, blockchain is used to ensure the integrity and authenticity of digital evidence (Hou: 2020: 1–15).

New technologies, such as tamper-proof storage and advanced hashing algorithms, are being developed to enhance the security and integrity of digital evidence. These include tamper- proof data storage solutions, blockchain-based proof chains, and advanced hashing algorithms to verify data integrity (Alatawi: 2020: 1–6).

Basic call, text message, and contact data are stored on mobile devices, but smart phones retain considerably more valuable data, including chat logs, email, personal information, and browser history.

The article (Mallidi: 2016: 1–12) highlights the need for forensic tools tailored to smartphones for data examination and recovery. Analyzing call history is crucial in mobile forensics, as call logs reveal communication patterns, connections, and time- lines. Overlooking key insights in call history analysis can impact the entire forensic process.

Methods and materials

Modern software products for mobile forensics allow experts to receive and analyze data from mobile devices, which plays a key role in digital investigations. Among the many solutions, several popular tools stand out, which have their own characteristics and fields of application (Cristian: 2020: 1–7).

A. Cellebrite UFED

Cellebrite has developed a series of products called the Universal Forensic Extraction Device (UFED), which are used for mobile forensic examinations (Tara: 2021: 97–104).

Key Features:

• Physical abstraction and decrypting while bypassing the pattern lock

• Set of analysis characteristics

• Advanced searching and filtering to quickly locate critical data (keywords, dates, specific data types)

• Timeline Analysis, powerful reporting capabilities

• Supports more than 30,000 device models

• Ability to work with deleted data and backups

B. Oxygen Forensic Tool

Oxygen Forensic Tool provides deep data analysis, that includes application data and records (Oxygen Forensics: 2024).

Key Features:

• Extract data from over 31.000 devices

• Data extraction from drones, IoT Devices, Smartwatches, Fitness Apps

• Finds, extracts and decrypts passwords, credentials, system files, and user data from Windows, macOS, or Linux

• Optical Character Recognition (OCR)

• Statistic widgets, Social Graph interface

• Timeline analytics

• Identification of frequently visited places, specify time periods, common locations and animate travels

• Face categorization and analytics (gender, race, age)

C. Elcomsoft IOS Forensic Toolkit

Elcomsoft IOS Forensic Toolkit is a program for extracting data from iOS devices, including physical extraction from locked phones, as well as working with iTunes and iCloud backups (Lahaie: 2015: 1–50).

Key Features:

• Passcode unlock: Brute-forces 4-digit and 6-digit screen lock passcodes via DFU exploit.

• Full file system extraction and keychain decryption for many devices running iOS 12 through 16.5.

• Media extraction, shared files, and advanced logical acquisition for iOS devices running versions that the extraction agent does not support.

• Has the ability to extract saved files and crash/diagnostics logs from many apps. Extract documents locally stored in Adobe Reader and Microsoft Office, access the Mini-KeePass password database, and much more.

D. MOBILedit Pro

MOBILedit Pro is a forensic tool that is designed for phone and cloud extraction, data analyzing and report generating, uses both physical and logical data acquisition methods (Hermawan: 2020: 233–238).

Key Features:

• Security bypassing – acquires physical image even when phone is protected by a password or pattern

• Physical data acquisition (extract physical images and have exact binary clones) and analysis (open image files created by this process)

• Advanced application analysis (adaptive and in-depth methods to ensure retrieving the most data available).

Focus on timeline as a note, a photo, video or a flow of messages

• Walkthrough for applications, photos, accounts, contacts, messages, emails,

calls and organizers

- Malware detection
- Scientific image analysis
- Has photo recognizer and photo matcher

A comparative analysis reveals that, although all four forensic tools excel in specific areas, they also exhibit notable weaknesses. Some of them are great in data extraction others in data analyzing. They all have shortcomings where other tools perform better. One main common problem is a wide range of devices under study, that happens because of constant changes and updates of devices (Delija: 2021: 1231–1235).

Additionally, challenges vary depending on the task, including gaining access to or unlocking devices, searching and filtering data, analyzing specific elements, and generating reports. Furthermore, none of them provide a comprehensive solution for the deep call history analysis.

Each tool has their own strength, but when it comes to detailed examination of call logs they all fail. Even though, they all support general call extraction, none of the tools specifically focus on those points:

1. Comprehensive analysis of call metadata, that includes: frequency of calls between specific users and call duration patterns

2. Identifying call trends through visualization and reporting on call interactions

3. Advanced filtering call related data that includes missed or rejected calls(-can be helpful during forensic investigations)

Recent research emphasizes the necessity of specialized modules for analyzing call history, focusing on mathematical filtering, semantic search, and statistical visualization, which traditional forensic tools still lack (Rzayeva: 2025: 66–74).

According to everything that is written above, it follows that there are no universal methods for solving these problems in the market within the framework of the tasks being solved.

To thoroughly analyze a mobile device, relying on two to three (or even five) programs is often insufficient. The organization that provided some of these tools and test data asked to combine all the useful functions of analyzing and tracking phone calls in one module.

Below is a table of functions and a list of tested applications. Unfortunately, the data used in the tests is personal data that is used in the investigation. According to the law of the Republic of Kazakhstan, these data cannot be published.

Table 1. «Comparison of forensic analysis tools»

Feature	UFED 4PC	MOBILedit Pro	Oxygen forensic
Average call duration	+	-	+
Call types (incoming, outgoing)	+	+	+
Call apps used	+	-	+
Top 10 contacts	+	-	+
Activity periods	-	-	-
Total calls periods	+	+	+

International calls location detection	-	-	-
Kazakhstan city calls detection	-	-	-

Results

The proposed Call History Analysis Module enables investigators to efficiently filter and analyze large datasets of call records using phone number and timestamp conditions. Key features such as phone number filtering, duration statistics and app usage analysis helps to give a comprehensive picture of communication patterns. Furthermore, the module provides insights into important contacts, call durations, and active communication periods, which are visualized through charts. This method not only makes call history analysis easier, but it also improves investigators' capacity to swiftly pinpoint important contacts and communication patterns. In the future, functions will be developed to determine the locations of international calls and cities in Kazakhstan. All tested tools do not have this feature.

A. Call history analyzer

The following functions are demonstrated on dataset $D = \{d_1, d_2, \ldots d_n\}$, where each element d_i has the following attributes:

- $d_{i.number}$: The phone number involved in the call..
- $d_{i.timestamp}$:The timestamp of the call in ISO format.
- $d_{i.type}$:, which can be either "incoming" or "outgoing".
- $d_{i.duration}$: The duration of the call (in seconds).
- $d_{i.app}$: The application used for the call.

Let:

- N be the given phone number filter (optional).
- t_s be the given start time (optional).
- t_e be the given end time (optional).
- $ISO(t)$ be a function that converts a timestamp string t to an ISO datetime object for comparison.

The filtered dataset F can be expressed as:

$$F = \{d_i \epsilon D \mid (N = \emptyset \vee d_i.number = N) \wedge (t_s = \emptyset \vee t_e = \emptyset \vee t_s \leq ISO(d_i.timestamp) \leq t_e)\} \quad (1)$$

Where:

- $N = \emptyset$ means no phone number filter is applied
- $t_s = \emptyset$ or $t_e = \emptyset$ means no time boundary is set.

Explanation

1) Phone Number Filtering:
   - If N is provided, only records where $d_i.number = N$ are included.
   - If N is not provided, all records are included.
2) Time Range Filtering:
   - If both t_s and t_e are provided, the records must satisfy:

- $t_s \leq ISO(d_i.timestamp) \leq t_e$
- If only one boundary is given (either t_s or t_e), the records are filtered accordingly.

1) Total Call Counts: The number of incoming and outgoing calls. The total number of incoming and outgoing calls in the filtered dataset is calculated. To do this, iterate over each call record and increase the increment responsible for each type of call:

Incoming calls: Calls whose type has been marked as ”incoming”.
Outgoing calls: Calls whose type has been marked as ”outgoing”.
Mathematical Representation of get_incoming_outgoing_calls
Let:

- C_{in}represents the total number of incoming calls.
- C_{out} represents the total number of outgoing calls.

The function calculates:

$$C_{in} = \sum_{d_i \in D} 1(d_i.type = "incoming") \quad (2)$$

Formula (2) calculates C_{in} by adding 1 for every call record whose type is “incoming,” giving the total count of inbound calls.

$$C_{out} = \sum_{d_i \in D} 1(d_i.type = "outgoing") \quad (3)$$

Formula (3) determines C_{out} by adding 1 for each record labeled “outgoing,” producing the total number of outbound calls.

where:

$$1(P) = \begin{cases} 1 \ if \ P \ is \ true \\ 0 \ if \ P \ is \ false \end{cases} \quad (4)$$

Formula (4) defines the indicator function $1(P)$, which returns 1 when condition P is true and 0 when it is false.

Explanation:

1) Incoming Calls:

$$C_{in} = \sum_{d_i \in D} 1(d_i.type = \text{incoming}) \quad (5)$$

counts all records where the call type is “incoming”.

Formula (5) sums the indicator $1(d_i.type$ =incoming) over every record $d_i \in D$, yielding the total number of incoming calls C_{in}.

2) Outgoing Calls:

$$C_{out} = \sum_{d_i \in D} 1(d_i.type = "outgoing") \quad (6)$$

counts all records where the call type is "outgoing".

Formula (6) sums the indicator $1(d_i.type$="outgoing") over every record $d_i \in D$, yielding the total number of outgoing calls C_{out}.

The function returns the tuple (C_{in}, C_{out}), representing the total counts of incoming and outgoing calls, respectively.

2) *Call Duration:* Detailed statistics on the duration of calls have been calculated to assess the duration and patterns of communication. The statistics included:

Total number of calls: the total number of analyzed calls.

Average duration: The average duration of calls calculated by summing all call durations and dividing by the total number of calls.

Maximum and minimum durations: The longest and shortest of the observed call durations.

Calculations are performed for all calls in aggregate and separately for incoming and outgoing calls.

Mathematical Representation of "get_call_duration_statistics"

Let:

- C_{in} is the total number of incoming calls.
- C_{out} is the total number of outgoing calls.
- $n = |D|$ is the total number of calls.

The function computes the following statistics:

a) Total Calls Statistics:

Total Amount = n

$$Average\ Duration = \frac{1}{n}\sum_{i=1}^{n} d_i.duration \quad (7)$$

Formula (7) finds the overall average call length by dividing the sum of all call durations by the total number of calls n.

$$Max\ Duration = max\{d_i.duration | d_i \in D\} \quad (8)$$

Formula (8) returns the single longest call duration present in the entire data set D.

$$Min\ Duration = min\{d_i.duration | d_i \in D\} \quad (9)$$

Formula (9) returns the single shortest call duration present in D.

b) Incoming Calls Statistics:

$$Incoming\ Amount = C_{in} \tag{10}$$

Formula (10) simply states that the total number of incoming calls equals C_{in}

$$Average\ Incoming\ Duration = \frac{1}{C_{in}} \sum_{\substack{i=1 \\ d_i.type="incoming"}}^{n} d_i.duration \tag{11}$$

Formula (11) computes the mean duration of incoming calls by averaging only those records whose type is "*incoming*."

$$Max\ Incoming\ Duration = max\{d_i.duration | d_i.type = "incoming"\} \tag{12}$$

Formula (12) selects the maximum duration among all incoming calls.

$$Min\ Incoming\ Duration = min\{d_i.duration | d_i.type = "incoming"\} \tag{13}$$

Formula (13) selects the minimum duration among all incoming calls.

c) Outgoing Calls Statistics:

$$Average\ Outgoing\ Duration = \frac{1}{C_{outgoing}} \sum_{\substack{i=1 \\ d_i.type="outgoing"}}^{n} d_i.duration \tag{14}$$

Formula (14) computes the mean duration of outgoing calls by averaging only those records whose type is "outgoing."

$$Max\ Outgoing\ Duration = max\{d_i.duration | d_i.type = "outgoing"\} \tag{15}$$

Formula (15) selects the maximum duration among all outgoing calls.

$$Min\ Outgoing\ Duration = min\{d_i.duration | d_i.type = "outgoing"\} \tag{16}$$

Formula (16) selects the minimum duration among all outgoing calls.

d) Handling Special Cases:

- If $D = \emptyset$, all statistics are set to 0.
- If $min\{d_i.duration \mid d_i \in D\} = \infty$, it is reset to 0.

3) Application Usage: In some systems, the applications (Telegram, WhatsApp, etc.) used for the call may be present in the call history. In this case, for each application registered in the call data, the number of incoming and outgoing calls made using this application is calculated.

Mathematical Representation of get_call_apps

Let:

- $A = \{a_1, a_2, \ldots, a_m\}$ be the set of unique apps in the dataset.
- calls(a_j ,t) be the number of calls for app $a_j \in$ A and
- type $t \in$ {“incoming”, “outgoing”}.

The function computes the following:

$$calls(a_j, t) = \sum_{\substack{i=1 \\ d_i.app = a_j \\ d_i.type = t}}^{n} 1 \quad (17)$$

Formula (17) counts how many calls of type tt are handled by application a_j

Where:

$$t \in \{"incoming", "outgoing"\} \quad (18)$$

Formula (18) specifies that tt can be either “incoming” or “outgoing.”

The result is a dictionary:

app calls = (19)

$$\left\{ a_j \mapsto \begin{pmatrix} \text{incoming: } calls(a_j, \text{incoming}) \\ \text{outgoing: } calls(a_j, \text{outgoing}) \end{pmatrix} | a_j \in A \right\}$$

Formula (19) builds a dictionary that maps every app a_j to its total incoming and outgoing

call counts.

4) Key Contact Identification: Determining the most frequent contacts using the longest duration:

Number of calls on contacts: The total number of calls associated with each phone number.

Ranking of contacts: Sort contacts in descending order based on the duration of calls.

Mathematical Representation of “get_key_contacts”

Let:

- $C(p)$ be the number of calls for a given phone number p.

The function calculates:

$$C(p) = \sum_{\substack{i=1 \\ d_i.number=p}}^{n} 1 \quad (20)$$

Formula (20) counts how many call records reference the phone number pp by adding

1 for every entry where $d_i.number = p$.

The result is a dictionary:

$$contact\ calls = \{p \mapsto C(p) \mid p \in P\} \quad (21)$$

where P is the set of all unique phone numbers in the dataset D.
The contacts are then sorted by the number of calls in descending order:
sorted contacts = sort(contact calls, key = C(p), reverse = True)

5) Active Periods: A function "get_most_active_periods" analyzes call data by categorizing it into predefined time periods (morning afternoon, evening, and night). It processes timestamps from the input data, counts the number of calls for each period on a given day, and returns the results sorted by total daily activity in descending order.

Mathematical Representation of "get_most_active_periods"
Define the time periods as:

morning calls :	(6, 12)	(6 AM to 12 PM)
afternoon calls :	(12, 18)	(12 PM to 6 PM)
evening calls :	(18, 24)	(6 PM to 12 AM)
night calls :	(0, 6)	(12 AM to 6 AM)

The function calculates the activity counts for each day and period.

a) Activity Count for Each Period: For each call d_i, determine the call hour:

$$hour(d_i) = hour(ISO(d_i.timestamp)) \quad (22)$$

Formula (22) extracts the hour component (0 – 23) from the ISO-formatted timestamp of each call d_i.

and assign it to a period P where:

$$P = \{(s,e) \mid s \leq hour(d_i) < e\}\ or\ (s = 0 \wedge hour(d_i) < e) \quad (23)$$

Formula (23) assigns a call to the time interval $P=(s,e)$ whenever its hour value lies within $[s,e)$.

The number of calls for a specific period P on day t is:

$$C_t(P) = \sum_{\substack{i=1 \\ day(d_i)=t \\ hour(d_i)\in P}} 1 \quad (24)$$

Formula (24) counts the calls that fall into period PP on day tt by summing one indicator per qualifying record.

b) Daily Total Calls:: The total number of calls for a given day *t* is:

$$total\ calls(t) = \sum_{p} C_t(P) \quad (25)$$

Formula (25) obtains the total call volume for day *t* by summing the counts $C_t(P)$ over all periods *P*.

c*) Sorted Activity:* The result is a dictionary of days sorted by the total number of calls:

$$sorted\ activity = sort(\{t \longmapsto total\ calls(t) \mid t \in T\}, rev \quad (26)$$
$$True)$$

where *T* is the set of all days in the dataset.

Discussion

After collecting all the statistics, a json is created, which is sent to the data visualization block, where the collected statistics are shown in various charts.

Incoming vs Outgoing Calls: A bar chart (Figure 1) compares incoming and outgoing calls, showing a slight dominance of outgoing calls. This distinction helps determine an individual's role in a communication network-more outgoing calls suggest planning or coordination, while more incoming calls indicate receiving instructions. Understanding this is crucial for identifying roles in a criminal group.

1) Call Duration: The system visualizes the average duration of incoming and outgoing calls (Figure 2). Call duration provides insights into the significance of communications, enabling investigators to prioritize key interactions. Short calls suggest quick exchanges, while long calls may signal important discussions or negotiations, aiding investigators in focusing on critical communications.

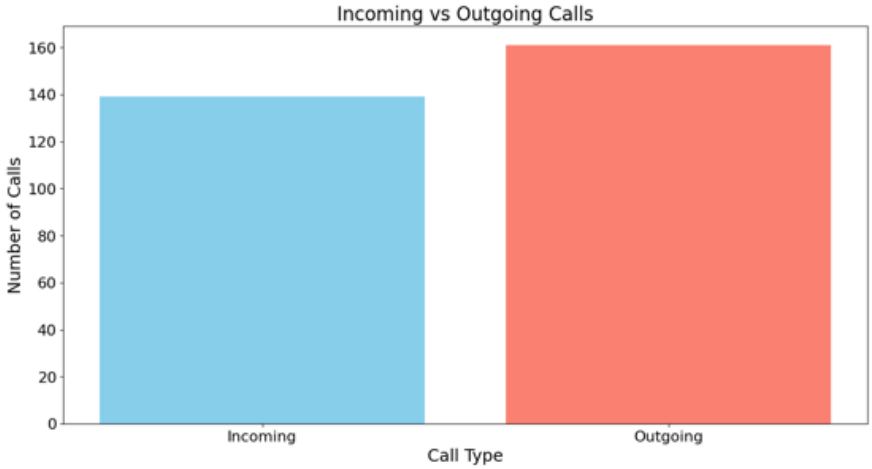

Fig.1. «Incoming vs Outgoing Calls »

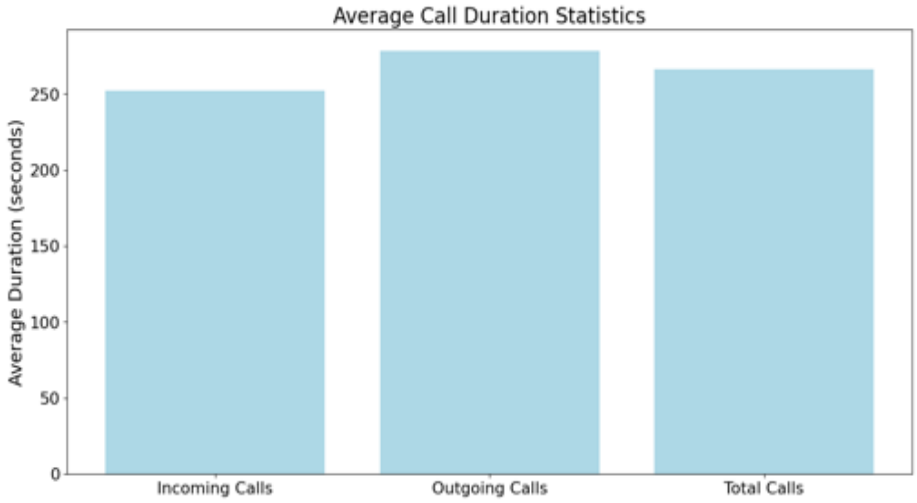

Fig.2. «Call Duration»

2) Call App Usage: A chart (Figure 3) displays call activity by app, distinguishing incoming and outgoing calls. Different apps offer varying privacy levels, making usage analysis crucial in digital forensics. Encrypted apps like WhatsApp and Telegram may indicate an attempt to conceal communication. This insight guides investigators in data extraction and prioritizing metadata, message content, and logs for deeper analysis.

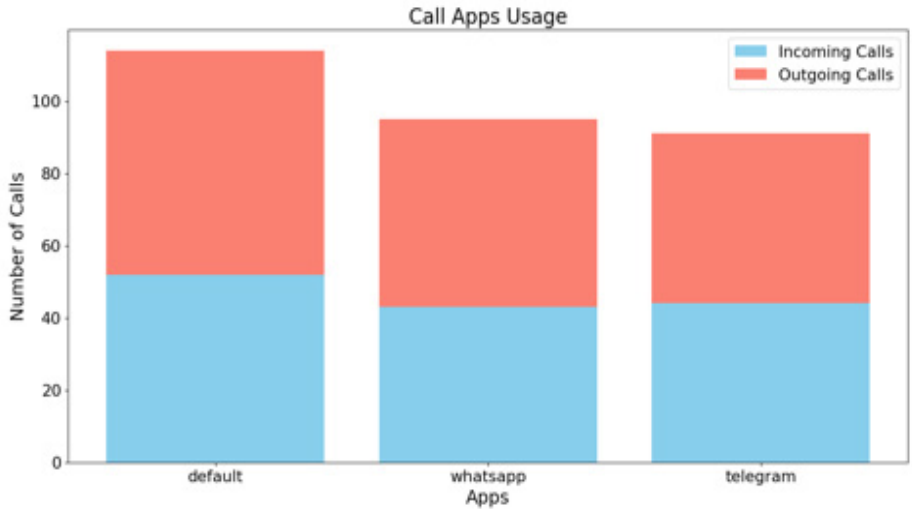

*Fig.3. «*Call App Usage*»*

3) Top 10 Key Contacts: The top 10 contacts, based on the frequency and duration of calls, are highlighted in a bar chart. (Figure 4) Identifying key contacts is crucial in forensic investigations. This chart highlights the suspect's most frequent contacts, potentially revealing important figures in a criminal network. Prioritizing these communications helps investigators establish patterns, build timelines, and uncover links between individuals.

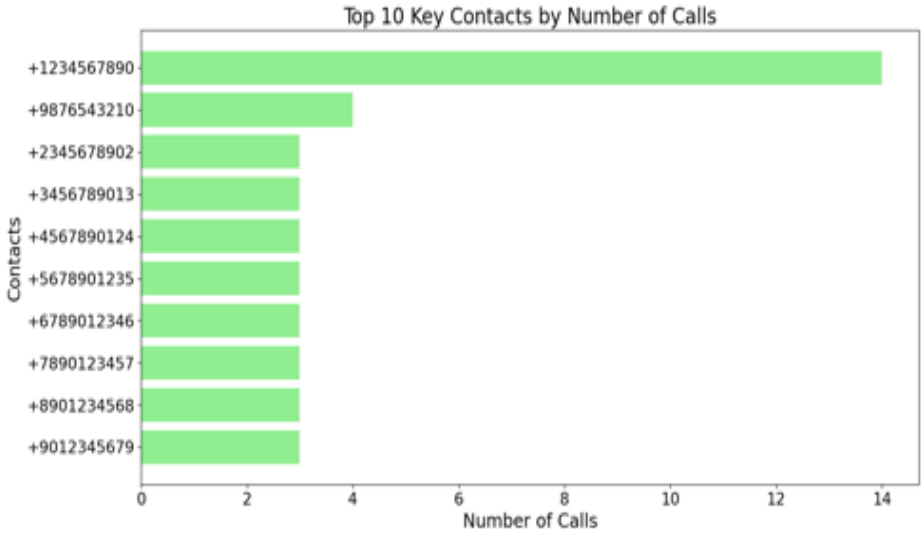

*Fig.4. «*Top 10 Key Contacts*»*

4) Call Activity Heatmap: A heatmap (Figure 5) visualizes call activity by time and date, aiding timeline reconstruction. Peaks in call volume may correlate with key events like crime planning or emergencies. Investigators can align these pat-

terns with other data (e.g., transactions, GPS) to build a cohesive narrative, narrowing down critical communication moments for deeper analysis.

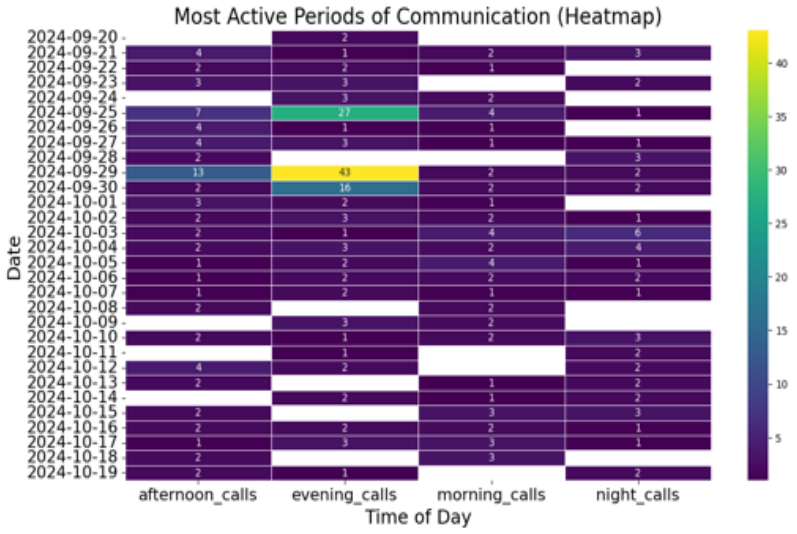

Fig.5. «Call Activity Heatmap»

5) Total Calls per Day: A line chart (Figure 6) tracks daily call volume, highlighting trends over time. It helps identify key dates of increased or decreased activity, potentially correlating with critical events. Spikes may indicate crime planning, while drops could suggest efforts to avoid detection or disruptions in communication patterns.

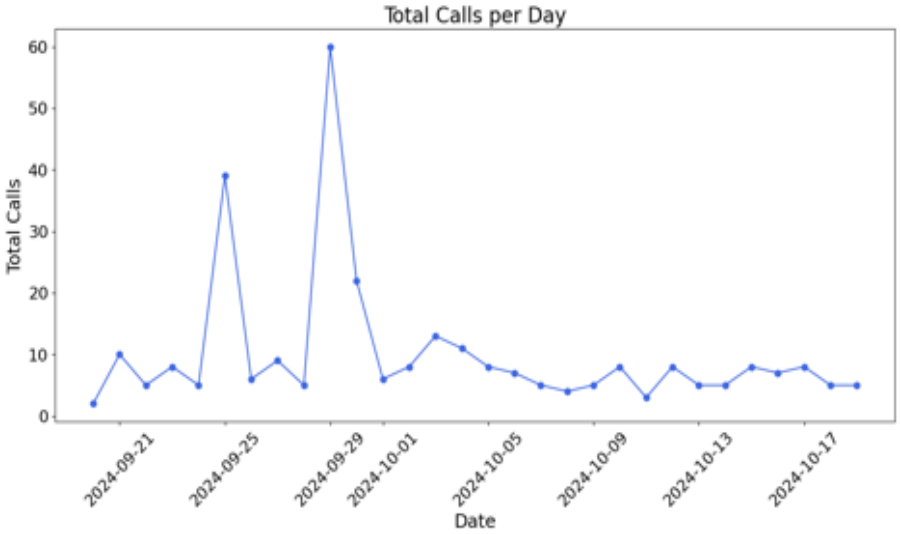

Fig.6. «Total Calls per Day»

C. Search for connections in multiple devices

The ability to process data from multiple sources simultaneously can also be useful in digital forensics. This section describes methods and algorithms that allow to track possible coincidences in the history of phone calls recorded from multiple devices simultaneously.

Let $\mathcal{C}$ be the set of call objects, where each call $c \in \mathcal{C}$ is a mapping from keys to values. Define the set of keys to ignore as

$$S = \{"field_1","field_2","field_N"\}. \quad (27)$$

For each key f (with $f \notin S$) and for each value v such that there exists a call $c \in \mathcal{C}$ with $c(f) = v$, define the group

$$G(f,v) = \{ c \in \mathcal{C} \mid c(f) = v \} \quad (28)$$

Next, define the set of sources for the group $G(f,v)$ as

$$\Sigma(f,v) = \{ c("source") \mid c \in G(f,v) \} \quad (29)$$

The function returns the groups for which the key-value pair is shared by calls from at least two different sources. Formally, the output is

$$\text{Result} = \{ (f,v,G(f,v)) \mid f \notin S \text{ and } |\Sigma(f,v)| > 1 \} \quad (30)$$

After generating the result, the received objects can be filtered by a special field or value.

Conclusion

After a thorough review of existing digital forensic tools and their capabilities, it becomes evident that most commercial and open-source platforms remain limited when dealing with complex patterns embedded in call history data. Suites such as Cellebrite UFED, Oxygen Forensic Detective, and MOBILedit Pro provide dependable extraction and parsing of call logs, yet they tend to focus on static record reconstruction rather than analytical interpretation. In contemporary investigations, where communication is increasingly fragmented across multiple applications and devices, this limitation can obscure vital links between suspects, witnesses, and events. To overcome these challenges, the development of the Call History Analysis Module represents a decisive step toward a more intelligent and interpretive approach to mobile forensics.

The proposed module introduces a unified workflow that normalizes heterogeneous call-record databases into a consistent analytical format. By using mathematical filtering, the system can isolate key behavioral indicators such as repeated contact frequencies, sudden communication gaps, or abnormal call durations. These features allow investigators to move from simple data retrieval to contextual understanding. Moreover, the embedded statistical engine correlates multiple parameters - such as timestamp intervals, geolocation markers, and contact density - to create a holistic picture of user behavior over time. This analytical depth is rarely achieved with traditional tools that rely on manual sorting or keyword searches.

Another major contribution lies in the module's advanced visualization capabilities. Instead of presenting lengthy tabular outputs, the system employs dynamic heat-mapped calendars, duration ridgelines, and ego-network diagrams to represent the flow of interactions between users. Such visual analytics enable examiners to detect hidden clusters of communication, recurrent call cycles, or significant deviations in activity timelines. For instance, the color-coded temporal plots can highlight bursts of contact before or after a crime event, while ego-networks reveal the centrality and influence of specific individuals in a suspect's communication sphere. This visual clarity translates raw call logs into an intuitive narrative that supports both technical and legal decision-making.

Equally important, the Call History Analysis Module strengthens data provenance and integrity, ensuring that every transformation or visualization remains traceable to its original dataset. The inclusion of an embedded similarity-search engine allows forensic analysts to compare call sequences across multiple devices, exposing parallel routines and shared interlocutors that often elude conventional examination. This cross-device correlation mitigates common issues such as timezone drift, duplicated contacts, and inconsistent labeling between Android and iOS platforms. As a result, the accuracy of extracted intelligence improves while the overall triage time is significantly reduced.

From an operational standpoint, the module does not attempt to replace established forensic ecosystems but rather complements them. It can be seamlessly integrated into laboratory workflows as a lightweight analytical layer. Investigators gain an additional interpretive stage between extraction and reporting, enabling faster identification of relevant communication threads. The module's modular architecture also ensures compatibility with future extensions, including plug-ins for chat-log parsing, SMS analysis, and app-specific metadata correlation. This flexibility is crucial for maintaining relevance as digital communication evolves toward more decentralized and encrypted platforms.

The implications of this advancement extend beyond immediate casework. By augmenting investigators' analytical capabilities, such tools contribute to the transparency and reliability of digital evidence presented in court. Enhanced visualization and mathematical reasoning help reduce human bias, offering objective representations of communication behavior. Moreover, the automation of pattern recognition supports scalability in high-volume forensic environments where thousands of records must be processed within limited time frames. Consequently, the Call History Analysis Module not only streamlines technical processes but also elevates the evidential quality of mobile data analytics.

Looking ahead, future research will focus on expanding the module's intel-

ligence through integration with machine learning and artificial intelligence techniques. Predictive analytics could, for instance, forecast communication behaviors or detect anomalies suggesting collusion or identity spoofing. Another prospective direction involves extending coverage to additional data channels such as encrypted messaging applications, multimedia exchanges, and social media call logs. Combining these diverse communication layers within a single analytical framework would provide investigators with unprecedented situational awareness.

As the landscape of digital communication continues to evolve, forensic science must adapt accordingly. The Call History Analysis Module exemplifies how targeted innovation - grounded in mathematical filtering, visualization, and behavioral analysis - can fill existing gaps in forensic practice. It transforms call history from a static archive into a dynamic source of actionable intelligence. As digital forensic tools evolve, modules like this will remain vital for strengthening investigative capacities, ensuring evidential integrity, and ultimately guaranteeing justice in the digital era.

Acknowledgment. This research was conducted with financial support from the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan under Contract No. 388/PCF-24-26 dated October 1, 2024, as part of the scientific project BR24993232, "Development of Innovative Technologies for Digital Forensic Investigations Using Intelligent Software and Hardware Complexes."

REFERENCES

Alatawi H., Alenazi K., Alshehri S., Alshamakhi S., Mustafa M., Aljaedi A. (2020). Mobile forensics: A review // *2020 International Conference on Computing and Information Technology (ICCIT-1441)*. — Pp. 1–6. URL: https://www.researchgate.net/publication/357822812_A_Comprehensive_Survey_on_Computer_Forensics_State-of-the-Art_Tools_Techniques_Challenges_and_Future_Directions

Batra S., Gupta M., Singh J., Srivastava D., Aggarwal I. (2020). An empirical study of cybercrime and its preventions // *2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC)*. — Pp. 42–46. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9315785&isnumber=9315319

Cristian P.-C., Hernan T.-C., Rene G.-Q., Francisco A.-P., Cristian N.-G. (2020). Methodologies and forensic analysis tools on android mobile devices: A systematic literature review // *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*. — P. 1–7. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9140852&isnumber=9140439

Delija D., Mohenski I., Sirovatka G. (2021). Comparative analysis of network forensic tools on different operating systems // *44th International Convention on Information, Communication and Electronic Technology (MIPRO)*. — Pp. 1231–1235. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9596833&isnumber=9596611

Fernandes R., Colaco R. M., Shetty S., Moorthy H. R. (2020). A new era of digital forensics in the form of cloud forensics: A review // *Second International Conference on Inventive Research in Computing Applications (ICIRCA)*. — Pp. 422–427. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9182938&isnumber=9182787

Hermawan T., Suryanto Y., Alief F., Roselina L. (2020). Android forensic tools analysis for unsend chat on social media // *3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*. — Pp. 233–238. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9315364&isnumber=9315328

Hou J., Li Y., Yu J., Shi W. (2020). A survey on digital forensics in internet of things // *IEEE Internet of Things Journal*. — Vol. 7, No. 1. — Pp. 1–15. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8831387&isnumber=8955685

Jacob J., Kumar S. (2022). A framework for digital forensics using blockchain to secure digital data // *IEEE World Conference on Applied Intelligence and Computing (AIC)*. — P. 899–904. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9848860&isnumber=9848805

Khalaf R. S., Varol A. (2019). Digital forensics: Focusing on image forensics // *7th International Symposium on Digital Forensics and Security (ISDFS)*. — Pp. 1–5. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?t-

p=&arnumber=8757557&isnumber=8757466

Lahaie C. (2015). Elcomsoft iOS Forensic Toolkit Guide // *LCDI, Champlain College*. URL: http://www.lcdi.champlain.edu

Mahmoud A. A. S., Mandela N., Agrawal A. K., Mistry N. R. (2023). Online crime reporting system for digital forensics // *International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS)*. — Pp. 1–6. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10391347&isnumber=10391098

Mallidi S.K.R., Palli P. (2016). A comprehensive analysis of smartphone forensics data acquisitions. URL: https://www.researchgate.net/publication/326826849_A_Comprehensive_Analysis_of_Smartphone_Forensics_Data_Acquisitions

Mehta J., Bhadania Y., Shah P., Prajapati P. (2024). Comparative study of mobile forensics tools: Autopsy, Belkasoft X and Magnet Axiom // *5th International Conference on Electronics and Sustainable Communication Systems (ICESC)*. — Pp. 1257–1263. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10689971&isnumber=10689723

Oxygen Forensics Inc. (2024). Oxygen Forensic Detective Brochure. URL: https://oxygenforensics.com

Punjabi S. K., Chaure S. (2022). Forensic intelligence — combining artificial intelligence with digital forensics // *2nd International Conference on Intelligent Technologies (CONIT)*. — Pp. 1–5. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9848406&isnumber=9847665

Rizvi S., Scanlon M., Mcgibney J., Sheppard J. (2022). Application of artificial intelligence to network forensics: Survey, challenges and future directions // *IEEE Access*. — Vol. 10. — Pp. 110362–110384. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9919162&isnumber=9668973

Rzayeva L., Pogolovkin D., Shayea I. (2025). Development of a correspondence analysis service using artificial intelligence technology and a vector database for digital forensics // *International Journal of Information and Communication Technologies*. — Vol. 6. — No. 1. — Pp. 66–74. DOI: 10.54309/IJICT.2025.21.1.014

Shimmi S. S., Dorai G., Karabiyik U., Aggarwal S. (2020). Analysis of iOS SQLite schema evolution for updating forensic data extraction tools // *8th International Symposium on Digital Forensics and Security (ISDFS)*. — Pp. 1–7. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9116208&isnumber=9116190

Tara H., Mishra A. (2021). A comparative study of digital forensic tools for data extraction from electronic devices // *Journal of Punjab Academy of Forensic Medicine Toxicology*. — Vol. 21. — Pp. 97–104. URL: https://www.researchgate.net/publication/355065035_A_Comparative_Study_of_Digital_Forensic_Tools_for_Data_Extraction_From_Electronic_Devices

Tyagi R., Sharma S., Mohan S. (2022). Blockchain enabled intelligent digital forensics system for autonomous connected vehicles // *International Conference on Communication, Computing and Internet of Things (IC3IoT)*. — Pp. 1–6. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9767987&isnumber=9767723

Waluyo A., Cahyono M. T. S., Mahfud A. Z. (2022). Digital forensic analysis on caller ID spoofing attack // *7th International Workshop on Big Data and Information Security (IWBIS)*. — Pp. 95–100. DOI: 10.1109/IWBIS56557.2022.9924733. URL: https://ieeexplore.ieee.org/document/9924733

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Правила оформления статьи для публикации в журнале на сайте:
https://journal.iitu.edu.kz
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (Казахстан, Алматы)

Подписано в печать 15.12.2025.
Формат 60x881/8. Бумага офсетная. Печать - ризограф. 9,0 п.л. Тираж 100
050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09).

Издание Международного университета информационных технологий
Издательский центр КБТУ, Алматы, ул. Толе би, 59