Journal of Digital Security and Forensics
January-June 2026 3(1)
www.digitalsecurityforensics.org

Original Article

VOICE OVER INTERNET PROTOCOL (VOIP) NETWORK FORENSICS AND SECURITY: A COMPREHENSIVE SYNTHESIS OF DIGITAL INVESTIGATION TECHNIQUES, TRAFFIC ANALYSIS, AND EMERGING CHALLENGES

Vaishnavi Raut [1], Kapil Shukla [2*], Dr. Krishna Modi [3]
[1] B.Sc.–M.Sc. Integrated Course in Forensic Science with Specialization in Cyber Forensics, the National Forensic Sciences University, Gandhinagar, India
[2] Assistant Professor, School of Forensic Science, National Forensic Sciences University, Gandhinagar, Gujarat, India
[3] National Forensic Sciences University, India

ABSTRACT

Voice over Internet Protocol (VOIP) has changed the way people communicate all over the world because it provides people with flexible and inexpensive alternatives to the traditional telephony. But this change presents complicated security and forensic issues that require expert investigation techniques. This review sees a significant shift in the open-standard protocol analysis towards the application-specific study of encrypted proprietary platforms including Zoom, Discord and Microsoft Teams. Memory forensics is now capable of retrieving volatile evidence found in RAM and machine learning has improved the detection of encrypted traffic to more than 95 percent. There are still persistent problems with real-time evidence collection, cross-platform compatibility and compatibility against developing encryption standards. The upcoming studies aim at automation, privacy preserving methods of investigation, and quantum resistant security models that would address the new forensic requirements.

Keywords: Memory Forensics, Digital Forensics, Network Forensics, Traffic Analysis, Behavioral Detection, Mobile Application Forensics, VOIP Security, Artifact Recovery

INTRODUCTION

VOIP brings a fundamental change in the communication system by substituting the traditional circuit-switched networks with the versatile packet-switched one. The consequent benefit has resulted in mass cost-saving, increased flexibility, and easy integration with digital platforms, which have changed how organizations and individuals plan and communicate Federal Communications Commission (2019). This change also comes with novel challenges in fields of digital forensic, cyber-crime and network analysis. Although traditional telephony is based on specialized telco infrastructure, VoIP is built on the open Internet Nets, which introduce additional vulnerabilities and investigation issues that need special approaches Alo and Firday (2013). VoIP forensics and security are worth knowing more than just academically. Since VoIP technologies can serve as a significant means of ensuring critical infrastructure, commercial activities, and personal associations, they are appealing to cyber thieves, fraudsters, and criminals. VoIP communications are volatile, and coupled with robust encryption algorithms and proprietary protocols that make them difficult to recover evidence and to detect threats, this makes it harder on investigators and defenders. The present review provides 25-year (2000-2025) coverage of the topic and summarizes 41 peer-reviewed papers, covering the field in both a systematic and a critical

*Corresponding Author:
Email address: Vaishnavi Raut (vaishnaviirraut@gmail.com), Kapil Shukla (kapil.shukla@nfsu.ac.in), Dr. Krishna Modi (krishna.modi@nfsu.ac.in)
Received: 19 February 2026; **Accepted:** 23 March 2026; **Published** 14 April 2026
DOI: 10.29121/DigiSecForensics.v3.i1.2026.81
Page Number: 59-70
Journal Title: Journal of Digital Security and Forensics
Journal Abbreviation: J. Digi. Sec. Forensics
Online ISSN: 3048-894X
Publisher: Granthaalayah Publications and Printers, India
Conflict of Interests: The authors declare that they have no competing interests.
Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Authors' Contributions: Each author made an equal contribution to the conception and design of the study. All authors have reviewed and approved the final version of the manuscript for publication.
Transparency: The authors affirm that this manuscript presents an honest, accurate, and transparent account of the study. All essential aspects have been included, and any deviations from the original study plan have been clearly explained. The writing process strictly adhered to established ethical standards.

manner. It recognizes significant changes in techniques and priorities with the most prominent being the transition of open protocols to sophisticated means of proprietary, encryption-based applications that demand alternative investigative and defensive strategies.

EVOLUTION OF VOIP RESEARCH

VoIP forensics and security have developed in various distinguishable stages all of which were classified under different technical challenges and approaches. Initial research between 2000-2010 concentrated around the major core protocols e.g. SIP and RTP, basic quality of service parameters and early security issues in fairly simple, non-encrypted settings.

The maturation phase (2011-2015) witnessed the development of more sophisticated forensic tools, i.e. memory-based analysis tools that reflect the nature of VoIP communications being transient. The core methodology of this stage was then a form of volatile memory analysis that revealed the feasibility of retrieving rich communication artifacts through system RAM Irwin et al. (2011).

The contemporary phase (2016-2025) has been marked by the adoption of new machine learning methods, the difficulty of decryption of encrypted communications, and the transition to application-specific analysis as proprietary platforms have taken over the communication market. This development is indicative of the larger digitization of society and the growing complexity of technical means of communication and threat actors. Figure 1 demonstrates the history of VoIP research phases development.

Figure 1

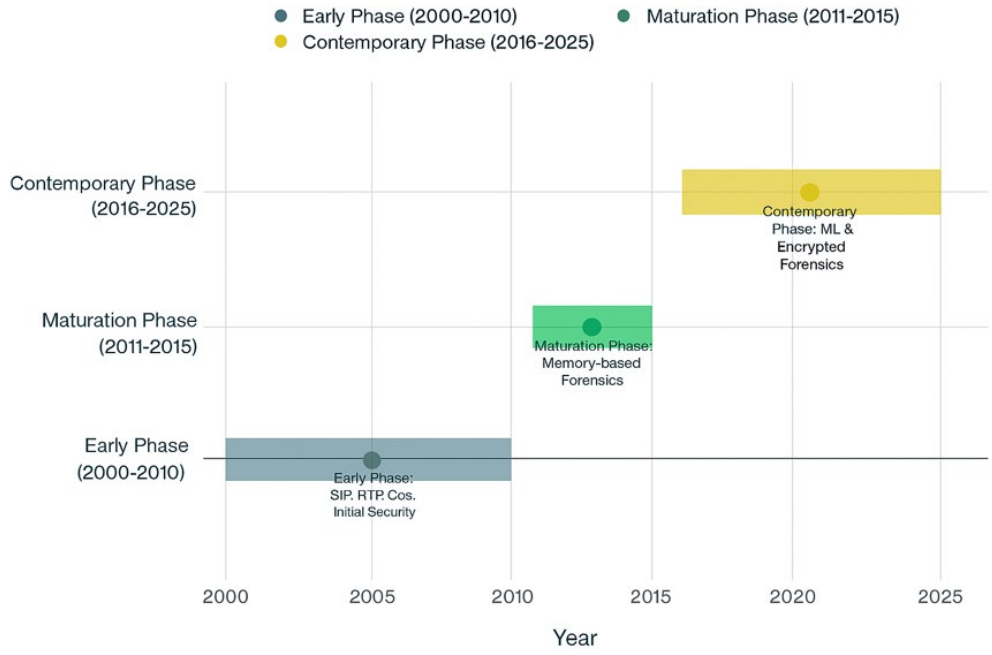

Figure 1 Evolution Timeline of VOIP Research Phases

RESEARCH OBJECTIVES AND CONTRIBUTIONS

The objective of this review is to provide a consistent synthesis that would answer three major questions: (1) methodical coverage of research developments in various fields, (2) critical analysis of significant paradigm shifts and recurring challenges, and (3) identification of future research opportunities that can inform both academic and practical research.

The analysis covers six main research areas that are distinguished by the systematized sorting of 41 studies, offering a quantitative understanding of the trends in research, but keeping a critical view of the methodological development and the existing limitations. The integration of the broad coverage and advanced synthesis makes this review a reference material to practitioners and a conceptual base to future research directions.

VOIP TECHNOLOGY OVERVIEW

A good VoIP forensic investigator should know how VoIP systems are constructed in order to do effective VoIP forensics. VoIP networks do not operate in the same manner as the traditional telephone networks. This advantage offers possibilities to collect the evidence and also poses difficulties to security.

BASIC VOIP INFRASTRUCTURE AND PROTOCOLS

VoIP systems are constructed in two layers; one is the call setup (signaling) and the other is the audio (media). As an illustration, the call is established by SIP messages and the voice is transmitted in form of RTP packets.

The primary standard that is currently used to configure and manage VoIP calls is Session Initiation Protocol (SIP). SIP messages are important during a call setup as they include information like caller ID, timestamps and session parameters. It is quite helpful information to investigate: e.g., the From and To fields in a SIP header makes you know instantly who is calling whom (Alo and Firday, 2013).

Real-time Transport Protocol (RTP) transmits the actual voice data in a VoIP call. It puts sequence numbers and timestamps on each audio packet so that the receiver can play them in order. From a forensic standpoint, RTP packets also contain clues like the type of audio codec in use or timestamps that show call duration. However, because RTP is optimized for real-time delivery, packets can get lost or arrive late on the network. Comparison of VoIP protocols and their forensic significance is given in Table 1.

Table 1

Table 1 Comparison of VoIP Protocols for Forensic Analysis

Protocol	Type	Encryption Support	Forensic Accessibility	Analysis Complexity
SIP	Signaling	Optional	High	Low
RTP	Media Transport	No (plain)	High	Low
H.323	Signaling/Media	Optional	Medium	Medium
SRTP	Secure Media	Built-in	Low	High
WebRTC	Web-based	Mandatory	Low	Very High

VoIP employs several audio encoders that compress voice information. For example, the G.711 codec provides excellent quality of audio at the cost of additional bandwidth, whereas the G.729 uses more severe compression to save on bandwidth at the price of a small amount of clarity. The data about the codec used provides the investigators a clue regarding the quality of the call and the possible artifacts in the data.

FROM OPEN STANDARDS TO PROPRIETARY APPLICATIONS

The history of the voice over internet protocol (VoIP) has clearly shown the transition of not only the open and standardized protocols but also the closed-source and proprietary applications that have introduced the custom-made communication channels. This shift of paradigm has made the investigators approach to new models of methodology and has raised the fundamental issues of concern in the field of forensic and security evaluation.

The modern platforms, such as Zoom, Discord, or Microsoft Teams, use proprietary protocols based on encrypted messages, which are regularly updated. As a result, literature has become platform-specific, and the approach adapted to one platform is not always transferable to other platforms, thus requiring continuous adaptation and platform-specific reverse engineering Gupta et al. (2024), Yu et al. (2025).

MEASURING QUALITY AND PERFORMANCE IN VOIP

Voice over Internet Protocol (VoIP) services quality is measured through the combination of the main metrics that directly influence user experience and forensic analysis. These measures are critical towards the enhancement of the quality of service and the creation of powerful analytical tools.

Jitter, as the difference in time delay between arrival of packets, has a great impact on the voice quality of VoIP communication. Unmanaged jitter might also lead to voice distortion, delay or packet loss, and the jitter patterns chosen deliberately can be used to mask malicious traffic and avoid detection mechanisms. Thus, proper jitter control becomes crucial in ensuring the quality of service (QoS) as well as the integrity and security of VoIP networks Khan and Suryawanshi (2019).

Packet loss i.e. the ratio of packets sent and which do not reach the intended destination. High loss rates mean that there is congestion in the network, which might be security breach or system failure; in addition, loss pattern can be used in explaining network topology, route behavior and other anomalies related to forensics.

The Mean Opinion Score (MOS) is a subjective measure of voice quality, which has a correlation with objective network measures. The knowledge of the technical constraints of the MOS scoring will enable the researchers to develop more effective instruments of quality control and to approximate the effect of low performance on the admissibility of forensic evidence.

METHODS OF ANALYSIS

VoIP communication requires special approaches unlike the conventional digital forensics and network security. These strategies need to overcome the unstable voice communication, scatter routes and increasing encryption systems.

Packet capture-based network analysis is needed but struggles with rising encryption. Deep packet inspection fails with encrypted data and relies on metadata and behavior approaches to infer communication without content access.

Host-based analysis is crucial with network approaches because VoIP programs leave traces in memory, databases, and configuration files. Memory forensics on the VoIP program enables examiners to restore artifacts in cases where network evidence doesn't prevail or when encrypted.

Machine learning and artificial intelligence identify patterns in encrypted traffic, profile behavior of communication, and identify anomalies. It is a synthesis of rule- and probabilistic analysis to a deeper understanding but has difficulties in model learning, verification and interpretation. Figure 2 illustrates the general workflow of forensic investigation

Figure 2

Figure 2 VoIP Forensic Investigation Workflow

THEMATIC ANALYSIS AND RESEARCH CLASSIFICATION

Analysis of 25 years of studies reveals apparent themes that are associated with technology and security transformations. This section shows scopes of research and analyses methodology changes. Quantitative research indicates that forensic examination and computer evidence recovery prevail with 40% of articles, capturing the sensitivity of investigative capabilities in the development of VoIP networks. The security and privacy research includes 34.5% and is concerned with the unending threats in VoIP networks. Figure 3 shows the allocation of research areas on the chosen studies.

Figure 3

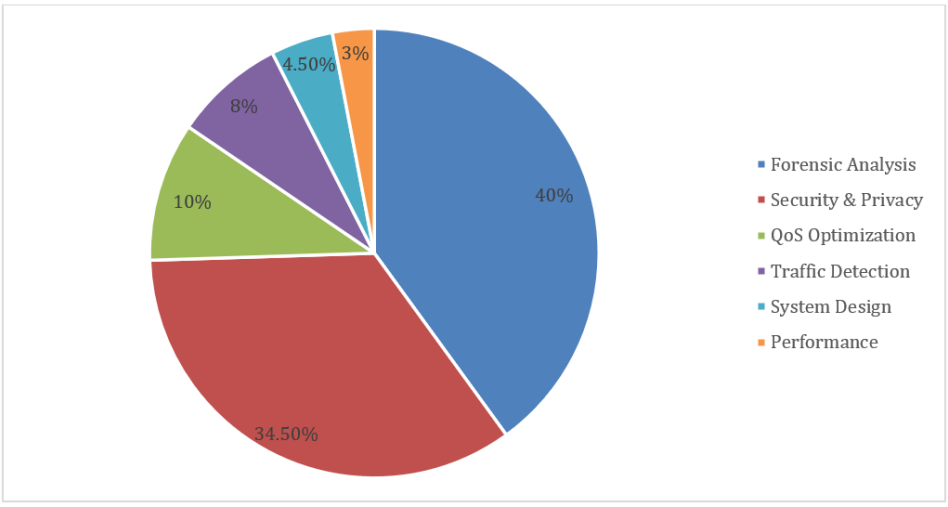

Figure 3 Distribution of VoIP Research Domains (2000-2025)

DEVELOPMENT AND EVOLUTION OF DIGITAL FORENSIC METHODOLOGIES

The field of forensic analysis has evolved considerably, as simple packet analysis has evolved into sophisticated multi-layer systems that can extract evidence by analyzing extremely sophisticated and encrypted data infrastructure. This development was possible to a large extent due to the increasing complexity of the infrastructure that is being utilized by the communication under consideration. The comparative effectiveness of different forensic approaches is summarized in Figure 4.

Figure 4

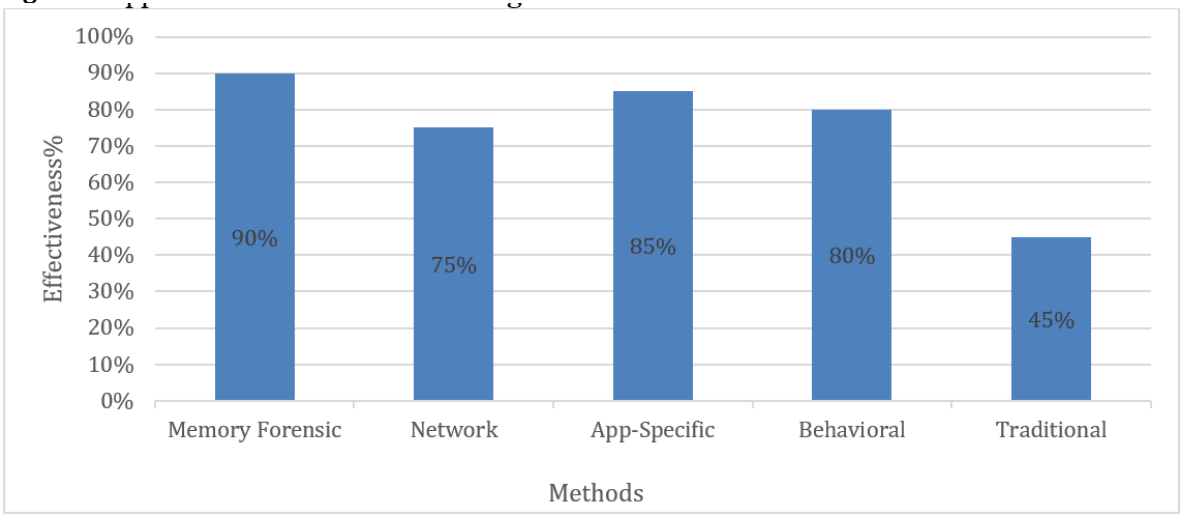

Figure 4 Comparative Effectiveness of VOIP Forensic Approaches

RISE OF MEMORY-BASED FORENSICS

Memory forensics is now the key method used to extract evidence from VoIP communications. Researchers have shown that VoIP applications leave rich artifacts in volatile RAM, even when no data is written to disk.

Irwin and Slay (2011) demonstrated that VoIP packet artifacts and SIP headers can be recovered from RAM using known hexadecimal patterns. They focused on the Ethernet/IP/UDP/RTP stack and were able to reconstruct Skype and X-Lite calls with high accuracy. Their work showed that memory analysis is a powerful complement to traditional network forensics, especially when live packet captures are unavailable. Javed et al. (2022) also emphasize the role of volatile memory and network forensics in the recent investigations, detailing the tools, challenges, and developments to maintain the effectiveness of forensics in reaction to emerging cyber threats.

Sophisticated analysis of the memory has followed the shifts in applications. Irwin et al. (2012) took memory forensic techniques a step forward into audio reconstruction, restoring digital speech portions from RAM after the call. This goes a long way beyond metadata recovery, and offers access to the actual content of the communication in selective instances.

More recently, forensic investigation of web and cloud-based communication has been revived. A thorough forensic analysis of Google Meet by Iqbal et al. (2022) allowed retrieving chat transcripts, meeting links, information about participants, and metadata of sessions in both memory dumps and browser artifacts in different operating systems. Based on memory-based forensics, their study reveals that volatile memory and browser data is abundant in user activity and meeting-related data and holds a useful value in a cloud conferencing context. The customers of GoToMeeting were also studied by Tiwari (2025), which recovers the meeting metadata and the AES keys and user interactions relying on the memory and browser artifacts.

Memory forensic tools evolved as the methodologies upgraded. Al-Saadawi and Varol (2017) contrasted tools such as Magnet IEF, Belkasoft, X-Ways, and Forensic Explorer, pointing out their capabilities and limitations during VoIP artifacts identification. From their results, they stressed the importance of the proper tool selection based on various investigations.

NETWORK FORENSICS AND TRAFFIC RECONSTRUCTION

Network-level forensic is invaluable to successful VoIP investigations, most notably to analyze or observe distributed communications in real time. It has also maintained technologically ahead of the VoIP protocol complexity, as rising encryption.

Recent studies by Sarhan et al. (2023) introduced packet inspection-based methods of analyzing VoIP instant messaging calls. Their analysis found significant metadata such as source and target IP addresses, times, and the protocols that are used on various platforms such as Facebook Messenger, Skype, and WhatsApp. The study shows that analyzing network-based forensic evidence can still be useful to recover the communication metadata in the case of encrypted content, so it can be used to support investigations where the content is inaccessible using traditional methods.

Holistic forensic systems significantly enhanced the analysis of networks. Mohemmed Sha et al. (2016) presented a forensic VoIP analyzer based on SIP filtering, call identification, port tracking, and RTP packet rescheduling to support voice reconstruction. Their Java-based implementation successfully restored voice conversations from traffic, providing investigators with powerful analysis tools for communication.

Chetry and Sharma (2024) researched on the issue of whether law enforcement can determine VoIP calls by examining the IP address data in network traces like IPDR and PCAP files. They focused on the interpretation of metadata such as IP locations, time stamps, and patterns of connection to identify the users of anonymous calls. It was also observed that encryption and anonymization were also a challenge and it is necessary to thoroughly analyze network data, as it is still critical to find evidence that will be used in court.

Network forensics is limited by encryption and protocol obfuscation. End-to-end encryption is the standard of many platforms, preventing the traditional way of packet inspection and thus necessitating new approaches that focus on metadata inspection and traffic pattern recognition instead of content inspection.

APPLICATION-SPECIFIC AND MOBILE PLATFORM FORENSICS

New proprietary messaging apps have necessitated specific forensic methods of each application depending on the specific artifacts. This change implies that the analysts are not doing protocol-level analysis anymore, but analyzing data and behavior of each application.

Multi-platform research provides some guidance on forensic technique applications for the analysis of communication. Sgaras et al. (2016) compared WhatsApp, Viber, Skype, and Tango on Androids and iOS devices, outlined the taxonomies of artifacts, and indicated the disparities in the accessibility of the data across platforms.

It was found that Android provides stronger access to forensic analysis than iOS, varying between applications on the same platform. Skype produced the greatest amount of artifact generation, and WhatsApp had restricted recoverable data, highlighting the importance of app-specific awareness during the course of an investigation.

Mobile forensic analysis presents special difficulties in persistence of artifacts as well as data recovery. It was indicated by Al-Saleh and Forihat (2013) that Skype artifacts are recovered on Android devices even after the deletion of history or user logout, indicating persistence of mobile VoIP applications.

More recent work has expanded to cloud and collaboration platforms. For example, Gupta et al. (2024) analyzed the Discord application and were able to recover chat messages, user authentication tokens, server details, and other metadata from memory.

Video conferencing forensics has become extremely important as remote meetings become more common. The recent studies have proven the ability to decrypt Zoom Team Chat databases and disclose user interactions and activity despite the difficulty in encryption Tresnadi (2025). Moreover, new forms of forensic analysis using artificial intelligence and machine learning were used to scan through social media, including video conferencing devices, and it highlights ethical, legal, and scalability issues in decryption of encrypted communications Arshad et al. (2025). In the meantime, the forensics of Tencent Meeting memory has allowed retrieving valuable metadata and user interaction artifacts within volatile memory Yu et al. (2025).

SECURITY AND PRIVACY: DETECTION TO BEHAVIORAL ANALYSIS

With the VoIP systems, security researches have extended beyond discovering the gaps that can be exploited by the protocols, to the application of advanced systems that comprehend the malicious activities even with encrypted information. This advancement emphasizes the fact that the methodology of attack is also becoming complex and the defensive ability is being enhanced respectively.

MACHINE LEARNING IN TRAFFIC DETECTION AND CLASSIFICATION

VoIP identification has advanced to a higher level of behavioral analysis that is able to determine the patterns of the communication even though the traffic is encrypted. One such example is that, earlier techniques employed header fields and a port number, however, Wu et al. (2008) suggested behavioral approaches of identifying VoIP traffic through the application of Hidden Markov Models on speech bursts and silence. With their approach, they were able to achieve 95% and 97% accuracy in 4 and 11 seconds respectively, so they were not just effective against encryption but also against alternate codes that had already proven useful in challenging traditional techniques of detection.

A good alternative to protocol-specific methods is statistical anomaly detection. Freire et al. (2008) developed means of determining the VoIP call hidden in the HTTP traffic according to the result of chi-square and Kolmogorov-Smirnoff tests to achieve the detection rate of 90-100% with a false-positive rate of 2-5%. Their findings demonstrate that it makes sense to detect hidden VoIP traffic in other traffic channels.

Machine learning has been the key factor that has changed the fundamentals of traffic classification. Saqib et al. (2017) proposed sophisticated statistical techniques, which are grounded on signature detection, packet registration, packet-size analysis, and transmission-rate analysis. It attained offline true positive rates up to 93.6% and live analysis precision up to 95%, indicating the capabilities of machine learning for the classification of encrypted traffic.

The leading method for VoIP traffic detection is Deep learning. Kapoor et al. (2023) presented MAPLE and DATE models that convert packet payloads into images and point clouds for CNN and MLP classification. MAPLE attained over 99% accuracy in RTP stream detection, while DATE demonstrated good results at various network conditions. These methods denote the transition to representation learning that spots subtle patterns missed by traditional methods.

The Advanced steganography detection applies machine learning algorithms. Yang et al. (2019) developed fast neural network algorithms to locate steganography in VoIP traffic according to the semantic mapping of the quantized LSF codewords. It enhanced the speed to 20x with high accuracy of up to 89%, indicating the possibility of real time security analysis.

FRAUD DETECTION AND SERVICE ABUSE PREVENTION

Detecting frauds and usage of services are vital and research on VoIP security has turned out to be essential. The shift from rule-based systems to advanced behavior analysis shows the evolution of fraud methods and improvements in defense technologies.

In addition, it enabled better identification of illegal traffic by utilizing new techniques. Anwar et al. (2014) built algorithms for scanning packet captures for extracting Call Detail Records (CDRs) for monitoring illegal VoIP traffic by utilizing IP address blacklists. The method proved useful for identification of illegal communication by removing false positives.

The recent developments offer the rapid response to developing threats in real time fraud detection technologies. The SCAMSTOP project Rebahi et al. (2011), Rebahi et al. (2013) further refined the area by generating the Spam over IP Telephony (SPIT)-specific adaptive signatures and by enforcing the anomaly-detection algorithms in the working service-provider systems, hence proving the practicability of automated fraud-detection as it is conducted nowadays.

Behavioral profiling is a sophisticated fraud-detection model that is dynamically changing to the changing attack techniques. The technologies that were analyzed by Rebahi et al. (2011) include neural networks and behavioral analysis, where it is important to note that threat intelligence should be shared on a mutually cooperative basis by jurisdictions and service providers.

The performance of fraud detection has been significantly enhanced by the use of sophisticated machine-learning methods. The SPIT detection systems proposed by Azad et al. (2018) incorporate several processes like collaborative filtering, which leads to greater accuracy rates and reduced false-positive rates.

UNDERSTANDING PRIVACY AND ENCRYPTED PERFORMANCE

The emergence of privacy-sensitive technologies presents new obstacles to security analytical research and encourage the creation of new analytical paradigms in the encryption field; therefore, the field is extremely dynamic in terms of research.

The analysis of encrypted traffic no longer focused on the analysis of content, but rather the analysis of metadata and behavioral features. Sarhan et al. (2023) created frameworks of the forensic examination of encrypted traffic network showing that both timing analysis and statistical profiling can be performed without decryption of the content. Their approach was effective to predict events in the encrypted Telegram and WhatsApp traffic.

Traffic analysis is used to identify the language of encrypted communications. Wright et al. (2007) demonstrated that language identification (66%) and binary classification (86%) could be achieved by encrypting VoIP traffic, even though the sizes of packets vary due to variable-bitrate encoding. The current paper sheds light on the continued information leakage in encrypted settings.

Secure communication systems have been attacked by privacy-attack techniques. Zhu and Fu (2010) carried out traffic -analysis attacks on encrypted Skype by using Hidden Markov Models to identify speaker related features and link communication sessions. They have found that encryption cannot be used alone to protect against sophisticated methods of traffic-analysis. The development of privacy-sensitive analytical processes aims at achieving the balance between security and privacy.

QUALITY OF SERVICE AND PERFORMANCE OPTIMIZATION

Quality of Service (QoS) studies have developed primitive measures of performance, to more advanced optimization models that include machine learning and adaptive algorithms as a consequence of the increased complexity of networked settings and the increased need of high-quality real-time communications.

ENHANCING AND ANALYZING NETWORK PERFORMANCE

VoIP quality literature has defined the determinants that are critical in any network infrastructure. In their experimental studies, Olateju et al. (2019) demonstrate that wireless Local Area Networks (LANs) have poor performance compared to wired LANs in three metrics: jitter, indicators of voice quality, and loss of packets.

The acquired data have some information about the system performance with heavy implications on the system design and forensic investigation. Particularly, wired networks exhibit slight and predictable jitter behavior, thereby providing a superior user

experience and generating predictable traffic behavior that can be utilized in reconstructing forensic investigations and in investigating malware.

There has been an enormous expansion in VoIP traffic mathematical modeling. To define jitter and packet loss, Toral-Cruz et al. (2011) suggested multifractal and Markov chain models that give unambiguous dependencies between the parameters of the network and the measures of service quality that enable working with proactive control of performance and the detection of anomalies.

Heavy signal-processing to enhance the quality of VoIP in harsh environments has been adopted. Indicatively, Singh (2024) used 4G and 5G networks to perform wavelet transform on VoIP networks and, therefore, minimized latency and maximized throughput using Daubechies wavelet algorithm to compress and optimize audio transmission.

ADAPTIVE QUALITY MANAGEMENT SYSTEMS

Dynamically changing services to volatile network conditions and user requests with adaptive QoS management systems using optimization and machine-learning approaches represents a significant advancement over the traditional practice of using static configuration.

VoIP-HDK2 model proposed by Chakraborty et al. (2020) had an overall mean opinion score higher than 4.0 and thus minimized the call drops and packet losses in diverse network conditions. This model makes use of the k-nearest neighbor, hidden Markov modeling and k-means clustering to control performance under changing conditions demonstrating the adaptive nature of intelligent systems in the changing network conditions.

The wireless environment optimization is used to solve the problem of mobility, bandwidth as well as interference. Eriksson et al. (2000) have come up with the ROCCO (Robust Checksum -Based Header Compression) protocol of VoIP over wireless networks, with a 90% capacity efficiency against a 50% capacity efficiency with uncompressed headers. This paper highlights the importance of optimizing protocols on resource-limited environments.

Modern studies integrate artificial intelligence in the predictive quality management. In Chaudhari et al. (2023), AI-based voice intelligent identification of VoIP-based calling was proposed, which uses speech recognition and natural language processing to improve the quality of calls and call routing in order to improve the effectiveness of customer service.

MODERN METHODS FOR TRAFFIC DETECTION AND CLASSIFICATION

Network traffic has been highly developed in terms of its detection and classification. The study area transitioned to the complex behavioral approach, rather than the simple protocol-based approach, which is effective even when the traffic is encrypted or obfuscated. Behavioral and statistical models form the basis to this advancement and identify repeated patterns of communication and derive useful features where the contents of packets are inaccessible. This results into highly accurate detection and at the same time, lower rates of false positives.

Machine and deep learning have changed the ability to classify traffic. The techniques enable systems to analyze intricate patterns that are not possible to the human eye and react to the real-time needs. Through neural network models and transforming raw network data to form that can be easily understood by a pattern recognition algorithm, are can effectively handle encrypted VoIP traffic and have a high accuracy despite different high-speed networks.

SYSTEM DESIGN AND IMPLEMENTATION

The study is based on the design of architectures that incorporate security, high-performance, and forensic features at the design stages instead of at the post-design implementation stage.

INTEGRATED SECURITY ARCHITECTURES

The design of security architecture is to protect against numerous threat vectors. A study by Tuleun (2024), demonstrated the way an Asterisk-based VoIP network could be rendered safe by adding VPN-encryption, safeguarded by firewalls, and capable of intrusion detection, thereby mitigating common attack vectors.

Blockchain provide new solutions to safeguarding VoIP. Sreenivasulu and Ravikumar (2025), for example, proposed creating Fractal Net keys authenticated by blockchain, and their solution provided improved verification speed and security compared to current methods.

INTELLIGENT SYSTEM INTEGRATION

Inclusion of AI in VoIP systems has created self-adjusting platforms that can enhance performance and security in real time. These reflect a major step forward in the development of the static configuration methods, since it enables constant adjustment to the evolving conditions. Having cuckoo search optimization in their work allowed Kumar and Roy (2022) to optimize up to 98% throughput regarding machine learning classifiers and enhance security because of the introduction of intelligent threat detection and response schemes. To summarize the main areas and representative studies of the research, Table 2 has been created.

Table 2

Table 2 Summary of Key VOIP Forensics Research Areas, Studies, and Insights

Category	Key Studies	Insights
Memory Forensics	Irwin and Slay (2011), Irwin et al. (2012), Al-Saadawi and Varol (2017), Iqbal et al. (2022), Tiwari (2025), Yu et al. (2025)	RAM and volatile memory yield crucial call/session artifacts
Traffic Analysis	Freire et al. (2008), Wu et al. (2008), Saqib et al. (2017), Kapoor et al. (2023)	Traffic features and ML models distinguish VoIP flows
Encrypted VoIP Forensics	Zhu and Fu (2010), Wright et al. (2007), Sarhan et al. (2022)	Even encrypted calls leak metadata and language cues
QoS & Performance	Toral-Cruz et al. (2011), Olateju et al. (2019), Singh (2024), Chaudhari et al. (2023), Eriksson et al. (2000)	QoS metrics affect forensic signatures of calls
Security & AI Integration	Tuleun (2024), Kumar and Roy (2022), Sreenivasulu and Ravikumar (2025)	Blockchain & AI enhance VoIP trust and resilience

CRITICAL ANALYSIS: PARADIGMS, CHALLENGES, AND PERSISTENT LIMITATIONS

As VoIP has matured, protocol inspection methods have been generalized into AI-systems. Among the changes that can be observed include implementation of encryption that transforms what the expert is doing. Behavior inference is then the most significant thing that is under investigation by the investigators as they are examining general patterns of telecommunication and not examining information stored within the message.

This shift means the reconsideration of the equilibrium between the methods of analysis and privacy issues. Ordinary VoIP encryption has made the old-fashioned forensic techniques involving the use of header, packet content, obsolete Sarhan et al. (2023). Specialists have advanced the methods of behavioral study and examine the metadata trends, time relations, and statistical deviations to distinguish communication properties without viewing direct information Saqib et al. (2017), Kapoor et al. (2023). The encryption that protects the privacy of the user also complicates the detection of bad conduct and poses an ethical and legal issue to balance the prerequisites of security and the rights to privacy. Major VoIP security challenges and corresponding solutions are outlined in Table 3.

Table 3

Table 3 VOIP Security Challenges and Solutions Assessment

Challenge	Impact Level	Current Solutions	Maturity Level	Future Outlook
Encryption	Very High	Behavioral Analysis	Developing	Promising
Real-time Analysis	High	ML Algorithms	Developing	Good
Cross-platform Compatibility	High	Universal Frameworks	Early Stage	Challenging
Scalability	Medium	Cloud Computing	Mature	Excellent
Evidence Integrity	High	Chain of Custody	Mature	Stable

FROM PROTOCOLS TO APPS: A SHIFT IN ANALYSIS

Digital forensic techniques have slowly developed as general protocol-based procedures to application specific investigations. The shift can be explained by the variety of communication platforms, in which the techniques that are effective with one application, such as Skype or Discord, would not be effective with other applications, such as Zoom. Consequently, the forensic practitioners face a fragmented landscape of special equipment and understanding which makes the process of evidence collection more complex and requires life-long learning. These challenges are highlighted by Gupta et al. (2024) and Yu et al. (2025), and Soni (2025) also points out that the ever-evolving and diverse communication technologies require flexible forensic approaches to overcome them.

The VoIP technologies also experience fast evolutions, which worsen such issues. The proprietary applications constantly modify their data processing methods and data archival methods. Unlike standard protocols, these app-specific changes demand researchers to continuously change their approaches, as published methods can become outdated quickly. This case demonstrates the requirement for forensic systems that are flexible enough to support effective investigation despite regular updates.

PROGRESS AND LIMITATIONS IN ANALYSIS

Over the past decade, manual tasks involving packet inspection, memory dump analysis Irwin and Slay (2011), is now replaced with automated solutions based on machine learning, and artificial neural networks. Existing methods use algorithms for classifying features within encrypted traffic, automating analysis of artifacts, and processing of large dataset beyond human capabilities Kapoor et al. (2023), Yang et al. (2019). Such approaches enhance analytical capacity, thus allowing real-time recognition of patterns, probabilistic decision, and reducing time, and proficiency required for VoIP investigation.

There are high-level challenges involved in applying new methods to real-world forensics. Most prominent among them is scalability: methods successful on small sets struggle with the volume of real network traffic. Also, calculations that are doable on experiments of a small laboratory scale are sometimes too slow to support queries with time constraints. Such inconsistency between the verification at the laboratory level and large-scale application in both method verification and deployment discourage large-scale application of the modern VoIP forensic techniques, which is why it is urgently required that studies be conducted to identify limitations of the deployment setting of operational forensics.

THE RESEARCH-PRACTICE GAP

Regardless of the level of development in VoIP forensic science, a gap exists between laboratory output and field application. The majority of studies are performed using simulated data in laboratory, but testing the complexity of the real world is not done. This raises questions about the effectiveness of these methods in working environment with stricter constraints. Furthermore, non-uniform tools and standards make integration difficult and slow down deployment. Without common data formats and standardized methods, end-users struggle with abrupt learning curves and quality assurance. Concluding this gap involves verification against real datasets, improved integration of tools, and enhanced standardization to deliver deployable VoIP forensic results.

CONCLUSION

VoIP forensics has transformed radically to include basic protocol analysis to complex behavioral profiling and machine learning-based investigations. Memory forensics has proven to be the most common methodology, recovering useful artifacts out of volatile system memory where the traditional network techniques fail. Artificial intelligence integration has transformed the traffic-detection capacity of an investigator to detect VoIP communications with an impressive precision in the presence of end-to-end encryption and protocol obfuscation. Nevertheless, there are still serious problems that require innovation. The disintegration of communication tools means that investigators must be sufficiently skilled in various proprietary apps all with their own forensic signatures. The computational limits of real-time analysis and the volumes of network traffic still limit the capabilities to perform real-time analysis, whereas the research-practice gap still prevents the implementation of laboratory-tested methods in real-world settings. The fast development of communication protocols gives a continuous arms race between investigative technology and privacy protection technology. VoIP forensics future is in creating automated cross-platform analysis systems capable of keeping up with new technologies without violating privacy rights. The current gaps in research should be filled with lightweight machine learning methods which can be deployed in real-time, methods of forensic research that ensure privacy, and quantum-resistant forensic models. The VoIP forensics future depends on cooperation that combines development with values, allowing for effective capabilities with respect for privacy.

ACKNOWLEDGMENTS

None.

REFERENCES

Al-Saadawi, H., and Varol, A. (2017). Voice Over IP Forensic Approaches: A Review. IEEE Xplore, 1–6. https://doi.org/10.1109/ISDFS.2017.7916507

Al-Saleh, M., and Forihat, Y. A. (2013). Skype Forensics in Android Devices. International Journal of Computer Applications, 78(7), 38–44. https://doi.org/10.5120/13504-1253

Alo, U. R., and Firday, N. H. (2013). Voice Over Internet Protocol (VoIP): Overview, Direction and Challenges. International Journal of Science and Technology, 2(3), 199–205.

Anwar, U., Shabbir, G., and Ali, M. A. (2014). Data Analysis and Summarization to Detect Illegal VOIP Traffic with Call Detail Records. International Journal of Computer Applications, 89(8), 1–7. https://doi.org/10.5120/15519-2724

Arshad, M., Ahmad, A., Onn, C. W., and Sam, E. A. (2025). Investigating Methods for Forensic Analysis of Social Media Data to Support Criminal Investigations. Frontiers in Computer Science, 7, Article 1566513. https://doi.org/10.3389/fcomp.2025.1566513

Azad, M. A., Morla, R., and Salah, K. (2018). Systems and Methods for SPIT Detection in VOIP: Survey and Future Directions. Computers and Security, 77, 1–20. https://doi.org/10.1016/j.cose.2018.03.005

Chakraborty, T., Ghosh, S., Barik, S., Kar, S., and Chatterjee, S. (2020). VoIP-HDK: A Novel Channel Allocation Technique for QOS-Aware VOIP Communication Over Heterogeneous Networks. Procedia Computer Science, 171, 62–71. https://doi.org/10.1016/j.procs.2020.04.007

Chaudhari, G., Korde, P., Patil, S., and Bhongal, R. (2023). VOIP-Based Intelligence Calling System. International Journal of Advanced Research in Science, Communication and Technology, 3(7), 1–6.

Chetry, A., and Sharma, U. (2024). Investigating VOIP Calls: Law Enforcement Perspective. INFOCOMP Journal of Computer Science, 23(2).

Eriksson, G. A. P., Olin, B., Svanbro, K., and Turina, D. (2000). The Challenges of Voice-Over-IP-Over-Wireless. Ericsson Review, 1, 20–31.

Federal Communications Commission. (2019). Voice Over Internet Protocol (VOIP).

Freire, E., Ziviani, A., and Salles, R. (2008). Detecting VOIP Calls Hidden in Web Traffic. IEEE Transactions on Network and Service Management, 5(4), 204–214. https://doi.org/10.1109/TNSM.2009.041102

Gupta, K., Lanka, P., and Varol, C. (2024). A Holistic Digital Forensic Analysis of Discord: Storage, Memory, and Network Perspectives. Journal of Forensic Sciences, 69(4), 1320–1333. https://doi.org/10.1111/1556-4029.15548

Iqbal, F., Khalid, Z., Marrington, A., Shah, B., and Hung, P. C. (2022). Forensic Investigation of Google Meet for Memory and Browser Artifacts. Forensic Science International: Digital Investigation, 43, 301448. https://doi.org/10.1016/j.fsidi.2022.301448

Irwin, D., Dadej, A., and Slay, J. (2012). Extraction of Electronic Evidence from VoIP: Identification and Analysis of Digital Speech. Journal of Digital Forensics, Security and Law, 7(1). https://doi.org/10.15394/jdfsl.2012.1128

Irwin, D., Slay, J., Dadej, A., and Shore, M. (2011). Extraction of Electronic Evidence from VOIP: Forensic Analysis of a Virtual Hard Disk vs RAM. Journal of Digital Forensics, Security and Law, 6(3). https://doi.org/10.15394/jdfsl.2011.1086

Irwin, D., and Slay, J. (2011). Extracting Evidence Related to VOIP Calls. In IFIP Advances in Information and Communication Technology (221–228). https://doi.org/10.1007/978-3-642-24212-0_17

Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., and Gadekallu, T. R. (2022). A Comprehensive Survey on Computer Forensics: State of the Art, Tools, Techniques, Challenges, and Future Directions. IEEE Access, 10, 11065–11089. https://doi.org/10.1109/ACCESS.2022.3142508

Kapoor, M., Napolitano, M., Quance, J., Moyer, T., and Krishnan, S. (2023). Detecting VOIP Data Streams: Approaches Using Hidden Representation Learning. Proceedings of the AAAI Conference on Artificial Intelligence, 37(13), 15519–15527. https://doi.org/10.1609/aaai.v37i13.26840

Khan, A., and Suryawanshi, R. (2019). Performance analysis of VOIP Codecs Under Variable Jitter and Delay Conditions. International Journal of Computer Applications, 178(43), 1–6. https://doi.org/10.5120/ijca2019918704

Kumar, V., and Roy, O. P. (2022). Enhanced Network Security for Improved Trustworthiness of VOIP Applications Via Cuckoo Search and Machine Learning. Indian Journal of Science and Technology, 15(15), 677–688. https://doi.org/10.17485/ijst/v15i15.1379

Mohemmed Sha, M., Manesh, T., and Abd El-atty, S. M. (2016). VOIP Forensic Analyzer. International Journal of Advanced Computer Science and Applications, 7(1). https://doi.org/10.14569/IJACSA.2016.070116

Olateju, A. I., Adenekan, O. A., and Abatan, T. T. (2019). Performance Evaluation of Voice Over Internet Protocol (VoIP) on Wired and Wireless Networks. Journal of Digital Innovations and Contemporary Research in Science, Engineering and Technology, 7(2), 87–100. https://doi.org/10.22624/AIMS/DIGITAL/V7N4P9

Rebahi, Y., Nassar, M., Magedanz, T., and Festor, O. (2011). A Survey on Fraud and Service Misuse in Voice Over IP (VOIP) Networks. Information Security Technical Report, 16(1), 12–19. https://doi.org/10.1016/j.istr.2010.10.012

Rebahi, Y., Ruppelt, R., Nassar, M., and Festor, O. (2013). SCAMSTOP: A Platform for Mitigating Fraud in VOIP Environments. In Proceedings of the International Conference on Network and Service Management. https://doi.org/10.4018/978-1-4666-1888-6.ch012

Saqib, N. A., Shakeel, Y., Khan, M. A., Mahmood, H., and Zia, M. (2017). An Effective Empirical Approach to VOIP Traffic Classification. Turkish Journal of Electrical Engineering and Computer Sciences, 25, 888–900. https://doi.org/10.3906/elk-1501-126

Sarhan, S. A. E., Youness, H. A., Bahaa-Eldin, A. M., and Taha, A. E. (2024). VoIP Network Forensics of Instant Messaging Calls. IEEE Access, 12, 9012–9024. https://doi.org/10.1109/ACCESS.2024.3352897

Sarhan, S. A. E., Youness, H. A., and Bahaa-Eldin, A. M. (2022). A Framework for Digital Forensics of Encrypted Real-Time Network Traffic, Instant Messaging, and VOIP Application Case Study. Ain Shams Engineering Journal, 14(9), 102069. https://doi.org/10.1016/j.asej.2022.102069

Sgaras, C., Kechadi, M., and Le-Khac, N. (2016). Forensics Acquisition and Analysis of Instant Messaging and VOIP applications. arXiv. https://doi.org/10.48550/arxiv.1612.00204

Singh, S. (2024). Performance Improvement for VOIP-Based Systems. Wireless Personal Communications, 139(1), 145–166. https://doi.org/10.1007/s11277-024-11594-2

Soni, N. (2025). Digital forensics: Confronting Modern Cybercrimes, Technological Advancements, and Future Challenges. Forensic Legal and Investigative Sciences, 11(1). https://doi.org/10.24966/flis-733x/100105

Sreenivasulu, V., and Ravikumar, C. (2025). Fractal Net-Based Key Generation for Authentication in Voice Over IP Using Blockchain. Ain Shams Engineering Journal, 16(3), 103286. https://doi.org/10.1016/j.asej.2025.103286

Tiwari, N. S. K. (2025). Forensic Analysis of Browser-Based Go To Meeting Clients: Uncovering Memory and Browser Artefacts. Journal of Information Systems Engineering and Management, 10(20s), 483–495. https://doi.org/10.52783/jisem.v10i20s.3172

Toral-Cruz, H., Pathan, A. K., and Pacheco, J. C. R. (2011). Accurate Modeling of VOIP Traffic QoS Parameters in Current and Future Networks with Multifractal and Markov Models. Mathematical and Computer Modelling, 57(11–12), 2832–2845. https://doi.org/10.1016/j.mcm.2011.12.007

Tresnadi, A. (2025, March 17). Decrypting Zoom Team Chat: Forensic Analysis of Encrypted Chat Databases. InfoSec Write-ups. April 14, 2025.

Tuleun, N. W. (2024). Design of an Asterisk-Based VOIP System and the Implementation of Security Solution Across the VOIP Network. World Journal of Advanced Research and Reviews, 23(1), 875–906. https://doi.org/10.30574/wjarr.2024.23.1.2048

Wright, C. V., Ballard, L., Monrose, F., and Masson, G. M. (2007). Language Identification of Encrypted VOIP Traffic: Alejandra Y Roberto or Alice and Bob? In Proceedings of the USENIX Security Symposium.

Wu, C., Chen, K., Chang, Y., and Lei, C. (2008). Detecting VOIP Traffic Based on Human Conversation Patterns. In Lecture Notes in Computer Science (280–295). https://doi.org/10.1007/978-3-540-89054-6_14

Yang, H., Yang, Z., Bao, Y., Liu, S., and Huang, Y. (2019). Fast Steganalysis Method for VoIP Streams. IEEE Signal Processing Letters, 27, 286–290. https://doi.org/10.1109/LSP.2019.2961610

Yu, S., Li, B., Zhu, L., Zhang, H., Yang, S., Li, Z., and Feng, W. (2025). Tencent Meeting Forensics Based on Memory Reverse Analysis. PeerJ Computer Science, 11, e2963. https://doi.org/10.7717/peerj-cs.2963

Zhu, Y., and Fu, H. (2010). Traffic Analysis Attacks on Skype VOIP Calls. Computer Communications, 34(10), 1202–1212. https://doi.org/10.1016/j.comcom.2010.12.007