

Tracing the Invisible Threads: A Deep Dive into Email Security & Forensics

Bandu B. Meshram¹, Vikash Mendhe², Manish Kumar Singh³

¹NIMS, School of Law, NIMS University Rajasthan, Jaipur, India

²Launch IT Corp. 4430 NW, Urbandale Dr., Urbandale IA 50322, USA

³NIMS, School of Law, NIMS University Rajasthan, Jaipur, India

ABSTRACT

This paper suggests a detailed and in-depth examination of the intricacies and complexities involved in the practice of email communication systems. Email protocols like SMTP (Simple Mail Transfer Protocol), POP (Post Office Protocol), IMAP (Internet Message Access Protocol), and MIME (Multipurpose Internet Mail Extensions) are studied, alongside methods to authenticate emails and validate their integrity, such as SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance), which are crucial components of email communication systems. The standard email infrastructure, mail delivery process, digital signing and encrypting of an e-mail message at sender site and decrypting an e-mail message and verifying a digital signature at receiver site are also discussed, as understanding these aspects is essential for comprehending the email header. The researcher explores the proposed email forensic investigation process model for four methods for email forensic namely server, network, firewall logs, and port-level information, experimentation using email forensic tools, algorithms to find the forensic artefacts and use of RAM image to capture the currently running browser processes. The paper explores the email forensic investigation process, examining various forensic objects such as email server investigation concerning HTTP logs, SMTP logs, investigation of network devices like IP routing logs, firewall logs, and port-level information, which aids in tracing the source of an email message. Furthermore, the experimentation using email forensic tools like Google Message Header Analyzer, is performed to investigate the email sender's home address and how to recover the deleted email is also illustrated with suitable case study. The researcher also proposes an email forensic investigation procedure—the unique combination of experimentation and algorithms to identify the header information objects to discern intermediary ISPs and the IP address of the email sender, accompanied by an illustrative case study for email forensic analysis, it also explores the algorithmic steps for how to do email forensic based on memory & browser processes and lastly the researcher identifies the punishments for email attacks using ITA 2000 and IPC.

Keywords: Email Protocols, Cryptography, Digital Signature, Forensic Logs, Email Header

INTRODUCTION

Email forensics refers to the systematic process of collecting, analyzing, and examining electronic messages and associated metadata to uncover digital evidence, validate authenticity, reconstruct timelines, and ascertain the integrity of email communication. Emails often serve as crucial evidence in various legal, corporate, and investigative scenarios.

Email forensics assists in the systematic collection and preservation of the digital evidence, ensuring it remains admissible in legal proceedings. By examining email headers, metadata, and content, email forensics enables investigators to trace communication trails, identify involved parties, reconstruct timelines, and understand the flow of information between individuals or entities. It helps in authenticating the origin and content of emails, confirming whether messages have been altered, tampered with, or forged. This process involves analysing digital signatures, timestamps, and encryption methods to verify the integrity of the communication. In cases involving cybercrimes like phishing, hacking, identity theft, and cyber bullying, email forensics is indispensable for tracing perpetrators, understanding attack vectors, and gathering evidence for legal action. Within corporate environments, email forensics aids in maintaining data security, investigating internal incidents like data breaches or employee misconduct, ensuring compliance with industry regulations, and safeguarding sensitive information. It assists in detecting fraudulent activities, such as financial fraud or intellectual property theft, by analyzing email communications that may contain evidence or indicators of such illegal activities. Thus email forensics is a pivotal component of digital investigations, serving as a critical tool for extracting evidence, verifying authenticity, reconstructing timelines, and aiding in the resolution of legal disputes, corporate incidents, and criminal activities in the digital realm.

Email forensics holds significant importance in various contexts, including legal, corporate, and investigative realms, due to its capabilities in uncovering digital evidence, ensuring data integrity, and resolving disputes. Email forensics plays a crucial role in collecting, preserving, and presenting electronic evidence in legal proceedings. Emails often serve as critical evidence in civil, criminal, or corporate litigation. Authenticating emails and their contents is essential for their admissibility in court. Email forensics helps validate the integrity of digital evidence, ensuring it meets legal standards for admissibility. Email forensics assists legal professionals and law enforcement agencies in investigating cybercrimes, fraud, intellectual property theft, harassment, and other offenses involving electronic communication. Organizations rely on email forensics to maintain data security, investigate security breaches, and ensure compliance with industry regulations. It helps in monitoring employee communications for policy adherence and identifying potential security threats. Email forensics aids in safeguarding intellectual property by tracking unauthorized sharing or leakage of proprietary information through emails. Companies utilize email forensics to investigate allegations of employee misconduct, such as harassment, data theft, or inappropriate usage of company resources.

Email forensics is integral in examining cybercrimes, including phishing, identity theft, malware distribution, and cyberattacks involving email communication. Investigators use email forensics to trace digital footprints, reconstruct communication chains, and identify suspects or connections in criminal investigations, detecting and analysing fraudulent activities, such as financial scams or deceptive practices, often involve scrutinizing email evidence to establish motives and connections.

In essence, email forensics serves as a pivotal tool in the discovery, analysis, and presentation of digital evidence across legal, corporate, and investigative domains. Its role extends to ensuring data integrity, aiding compliance, resolving disputes, and combating cyber threats, making it indispensable in today's digital landscape.

The paper is organised as below. The second section discusses the literature survey required to do this research work, The third section presents Email Forensic Investigation Process and Tools The fourth section discusses Proposed Experimentation For Email Forensic. The fifth section explore the Use of Memory and Browser Forensic Process For Email Forensic and lastly section six Concludes the results.

LITERATURE SURVEY

The literature survey deals with an overview of email systems, protocols, and their functioning, digital certificate and digital signature, Email Communication with encryption and decryption.

A. Email Communication Systems

Email systems form the backbone of electronic communication, allowing individuals and organizations to exchange messages and information across the internet.

Email Systems: Email systems consist of various components working together to transmit messages. These components include:

Mail Servers: Mail servers are computers or systems responsible for sending, receiving, storing, and managing emails. They use protocols like SMTP (Simple Mail Transfer Protocol) for outgoing messages and POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) for incoming mail retrieval.

Email Clients: Email clients are software applications (e.g., Outlook, Thunderbird, Gmail) used by users to compose, send, receive, and manage emails. They communicate with mail servers using protocols such as POP, IMAP, or Exchange ActiveSync.

B. Email Protocols

Email protocols are standardized sets of rules governing the transmission and handling of emails across networks. Key email protocols include[2]:

(i)SMTP (Simple Mail Transfer Protocol): SMTP [RFC 821]is used for sending outgoing emails. It defines how messages are sent and relayed between mail servers. When you hit 'Send' on your email client, SMTP is used to transmit the message to the recipient's mail server.

(ii)POP (Post Office Protocol):POP, (defined in RFC 1939) define allows email clients to retrieve messages from a mail server to a local device (like a computer or smartphone). POP typically downloads emails to the device, removing them from the server (although configurations can be adjusted to leave copies on the server).

(iii) **IMAP (Internet Message Access Protocol):** IMAP [RFC1939] is another protocol for retrieving emails from a server to an email client. Unlike POP, IMAP retains emails on the server and synchronizes the client's mailbox with the server, allowing access to emails from multiple devices.

(iv) **MIME (Multipurpose Internet Mail Extensions).** MIME [RFC 2045] It is not a mail transfer protocol. Instead, it defines the content of what is transferred: the format of the messages, attachments, and so on. Refer RFC 822, RFC 2046, and RFC 2047.

C. Functioning of Email Systems

Sending Emails: When a user composes and sends an email, their email client uses SMTP to connect to their outgoing mail server. The outgoing mail server then routes the message using DNS (Domain Name System) to find the recipient's mail server [3].

Receiving Emails: When an email is sent to a user's address, the sender's mail server connects to the recipient's mail server using SMTP. The recipient's mail server stores the incoming message until the user's email client retrieves it using POP or IMAP.

Storage and Access: Emails are stored on mail servers until they are retrieved by email clients. IMAP keeps emails synchronized between the server and the client, allowing access to the same emails from multiple devices.

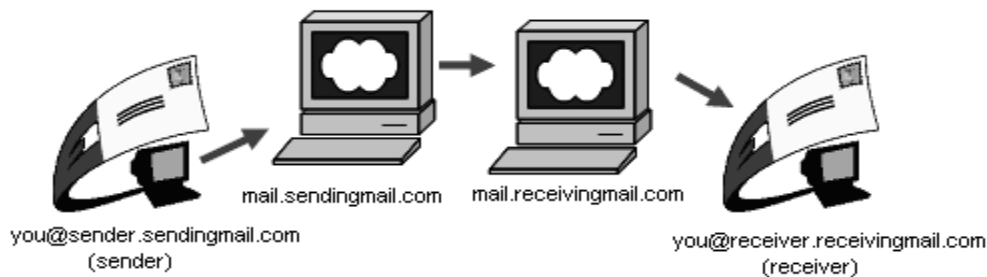


Figure 1 Standard Mail Delivery Process [11]

All e-mail headers contain the server and client information that controls the process of mail delivery. Many people who use e-mail clients have probably heard of SMTP servers and POP3 servers. Within the typical setup for e-mail, two ports are typically used: port 25, and port 110. Port 25 is the Simple Mail Transfer Protocol (SMTP), and its job is to transmit and receive mail—basically what is called a Mail Transfer Agent, or MTA. An MTA is comparable to the mail carrier who picks up the mail and sends it off to where it needs to go. Just as the mail carrier drops off and picks up mail, so does the MTA. Port 110 is the Post Office Protocol, version 3 (POP3), and it is essentially the mailbox from which users pick up their mail up. The mail server infrastructure works in such an efficient fashion that we did not use only four servers but, at minimum, eight servers to deliver our e-mail. In the process of sending e-mail, we query multiple DNS servers to obtain information about where the mail servers are on the Internet. Here is an example of the complete process for sending an e-mail.

Standard Email Process

- Create the e-mail, specifying the From, To, Subject, and content.
- After you click **Send**, the mail client will access the DNS server of your ISP to locate your local mail server.

The local mail server (mail.sendmail.com in our example) receives your e-mail and uses the local DNS to determine who sent it by doing a reverse IP lookup of Sender.

- After verification, the local mail server adds the headers and relays the mail to the mail.receiveingmail.com mail server. To do this, mail.sendmail.com has to look up what is called a mail exchange, or MX, record within DNS. This MX says, "Hello mail.sendmail.com, mail.receiveingmail.com is handling mail for receiveingmail.com." Once that has been identified by our mail server, it can relay to the proper mail server.
- Once mail.receiveingmail.com receives the e-mail, it applies more header information, including routing data and receiving time; checks the DNS server for a reverse lookup regarding mail.sendmail.com; and looks up the user you for the domain it is handling mail for.

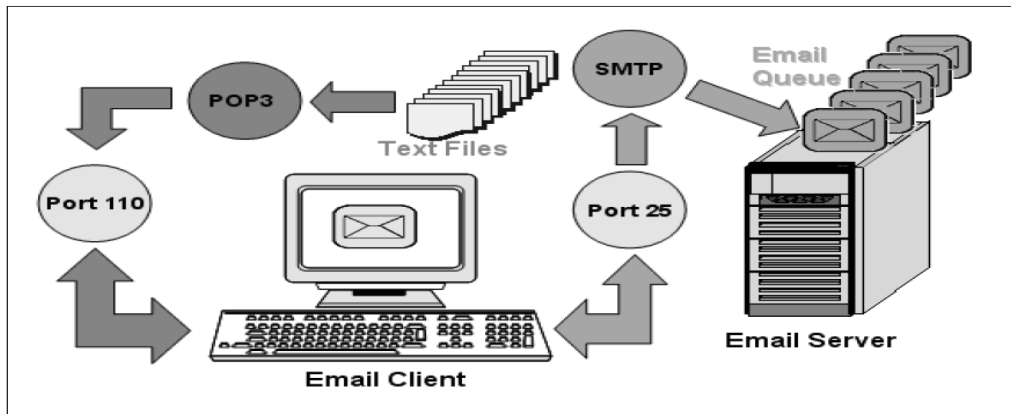


Figure 2 Standard Email Infrastructures

Client e-mail user Receiver contacts mail.receivingemail.com (again, local DNS is used), makes a request to the POP3 port (110), and asks to retrieve its e-mail. The e-mail is delivered to the e-mail client, and Receiver happily reads the e-mail. They use protocols

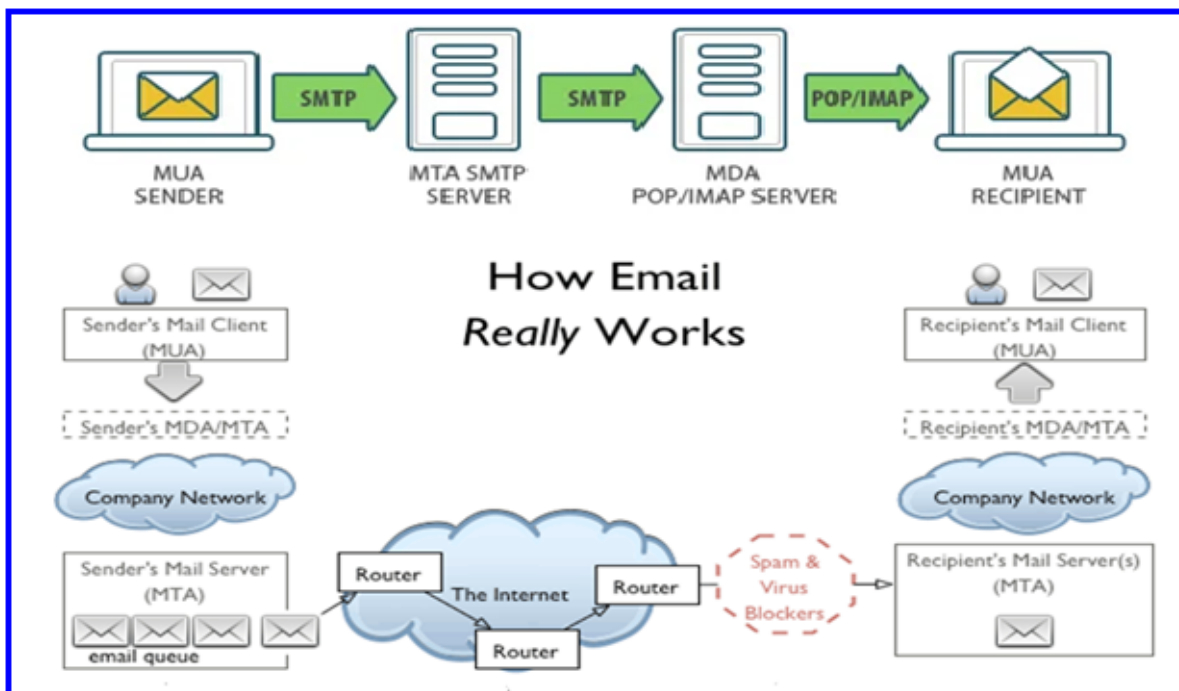


Figure3 email from the sender's (MUA) to the recipient's inbox (MUA Recipient)[1]

- **Mail user agent (MUA):** email clients. Be it a software or desktop interface, MUA stores emails, allows users to read and reply to messages, delete them, or flag as spam.
- **Mail transfer agent:** . MTA empowers the exchange of emails between the device of a recipient and that of a sender.
- **Message delivery agent:** accepts an email from the transfer agent and stores it in a reader's environment (the inbox).

Email Security Services

This section explore the S/MIME, cryptography and digital signature to provide secure email communications, but loop holes are used for the various attacks on Email Systems.

D.S/MIME (Secure/Multipurpose Internet Mail Extensions)

S/MIME[rfc5751]: provides two security services: Digital signatures and Message encryption. The best way to add security to e-mail is to use S/MIME (Secure MIME). S/MIME is a way of adding encryption, non-repudiation, authentication and data integrity to e-mail messages. S/MIME can provide a strong authentication of the sender of an e-

mail message and cryptographically strong assurances that the content (or body) of an e-mail has not been modified. When using S/MIME, the sender of a message "digitally signs" their message before sending it. When the recipient opens a digitally signed S/MIME message, their e-mail client verifies the signature, ensuring that the message content was not tampered with, and checks that the digital signature matches the return address on the mail, thus authenticating the sender. S/MIME is as important a standard as SMTP because it brings SMTP to the next level: allowing widespread e-mail connectivity without compromising security.

E. Digital Signature

A **digital signature** [3] is basically a way to ensure that an electronic document is authentic. Digital signatures is automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later. Digital signatures rely on certain types of encryption to ensure authentication. The components that a digital signature[3] comprise of Your public key, Your name and e-mail address, Expiration date of the public key, Name of the company, Serial number of the Digital ID, Digital signature of the CA (certification Authority). As with a legal signature, digital signatures provide the security capabilities such as authentication by signature, nonrepudiation enforced by **authentication and data integrity by** digitally signed e-mail.

In cryptography, Digital Certificates **Authority(DCA)** is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate.

F. Digital Signature and Verification Operations on an E-Mail Message

Although digital signatures provide data integrity, they do not provide confidentiality. Messages with only a digital signature are sent in clear text, similar to SMTP messages, and can be read by others. Authentication, nonrepudiation, and data integrity[3] are the core functions of digital signatures. Together, they ensure recipients that the message came from the sender, and that the message received is the message that was sent. At its simplest, a digital signature works by performing a signing operation on the text of the e-mail message when the message is sent, and a verifying operation when the message is read, as shown in the figure 4

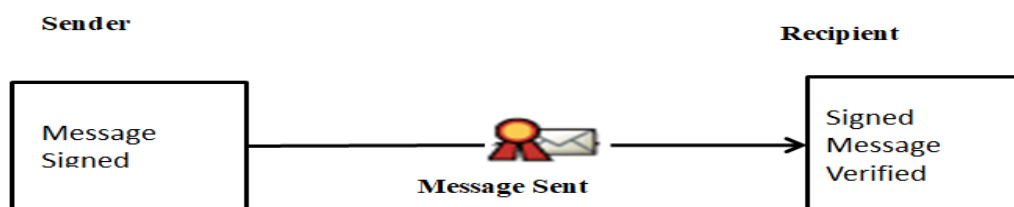


Figure 4 Digital Signature and Verification Operations on an E-Mail Message

The signing operation that is performed when the message is sent requires information that can only be supplied by the sender. This information is used in a signing operation by capturing the e-mail message and performing a signing operation on the message. This operation produces the actual digital signature. This signature is then appended to the e-mail message and included with the message when it is sent. The figure 5 shows the sequence of signing a message.

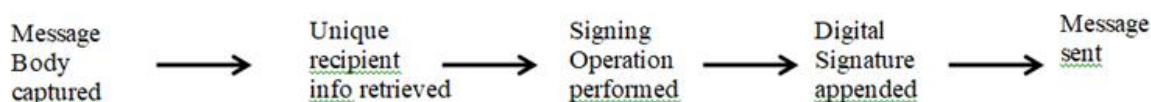


Figure 5 Digital signing of an e-mail message

Steps for Digital Signing of an E-mail Message are as follows

(i) Message is captured from the sender (ii) Information uniquely identifying the sender is retrieved. (iii) Signing operation by key is performed on the message using the sender's unique information to produce a digital signature. (iv) Digital signature is appended to the message. (v) Message is sent to the receiver. It is possible for unauthorized users to obtain the unique information that is used for digital signatures and attempt to impersonate a sender. However, the S/MIME standard can handle these situations so that unauthorized signatures are shown to be invalid. When the recipient opens a digitally signed e-mail message, a verification procedure is performed on the digital signature. The digital signature that is included with the message is retrieved from the message. The original message is

also retrieved, and a signing operation is then performed, which produces another digital signature. The digital signature included with the message is compared to the digital signature produced by the recipient

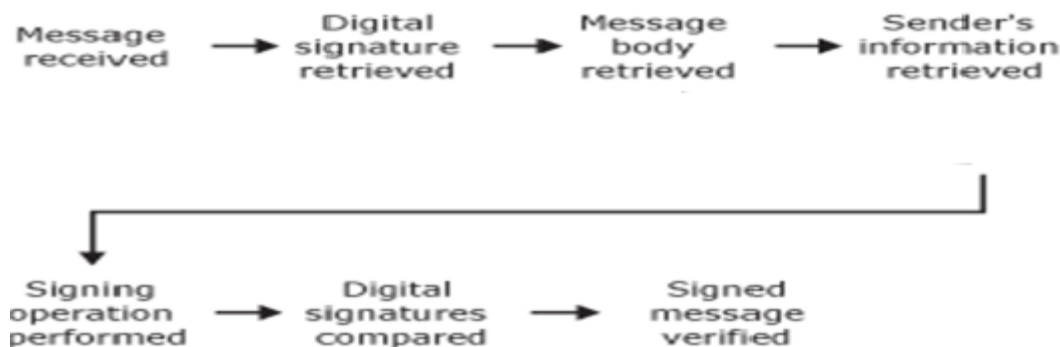


Figure 6 Steps for Verifying a Digital Signature of an E-mail Message[4]

If the signatures match, the message is verified as having come from the sender as claimed. If the signatures do not match, the message is marked as invalid. The figure 6 shows the Steps for Verifying a Digital Signature of an E-mail Message.

Taken together, the process of digital signing and verification of the digital signature authenticates the sender of an e-mail message and determines the integrity of the data within the signed message. Digital signatures are a solution to impersonation and data tampering, which are possible with standard SMTP-based Internet e-mail.

G. Message Encryption and Decryption Operations on an E-mail Message

An SMTP Internet e-mail message can be read by anyone who sees it as it travels or views it where it is stored because SMTP-based Internet e-mail does not provide encryption to secure messages. These problems are addressed by S/MIME through the use of encryption. Message encryption provides two specific security services namely (i)Confidentiality due to an e-mail message encryption provides confidentiality while the message is in transit and in storage.(ii) Data Integrity due message encryption. However message encryption does not authenticate the message sender and does not provide nonrepudiation, Hence to prove the identity of the sender, the email message must use a digital signature. Message encryption makes the text of a message unreadable by performing an encryption operation on it when it is sent. When the message is received, the text is made readable again by performing a decryption operation when the message is read, as shown in the figure 7



Figure 7 Message encryption and decryption operations on an e-mail message

The encrypted message replaces the original message, and then the message is sent to the recipient. The figure 8 shows the sequence of encrypting an e-mail message.

Encryption of an E-mail Message

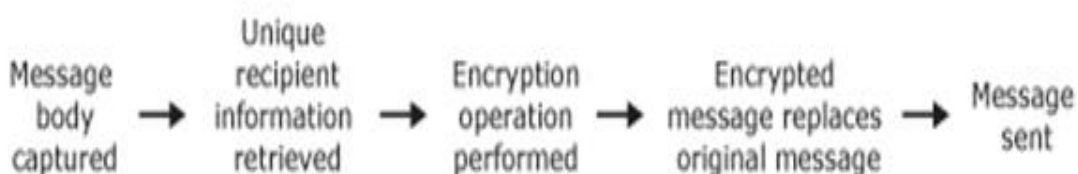


Figure 8 Encryption of an e-mail message details

When the recipient opens an encrypted message, a decryption operation is performed on the encrypted message. The encrypted message and the recipient's unique information are both retrieved. The recipient's unique information is then

used in a decryption operation performed against the encrypted message. This operation returns the unencrypted message, which is then shown to the recipient. If the message has been altered in transit, the decryption operation will fail. The figure 9 shows the sequence of decrypting an e-mail message.

Decrypting an E-mail Message



Figure 9 Decryption of an e-mail message details

The process of encryption and decryption of messages provides for the confidentiality of e-mail messages. This process addresses a serious weakness in Internet e-mail: the fact that anyone can read any message.

H.How Digital Signatures and Message Encryption Work Together

Digital signatures address security issues related to senders, and encryption addresses security issues primarily related to recipients.

Digital signatures address authentication and repudiation issues, and message encryption addresses confidentiality issues. Because each addresses different issues, a message security strategy requires both, often at the same time. To show how digital signatures and message encryption are handled together, the figure 10 shows the sequence of signing and encrypting an e-mail message.

Digital Signing and Encrypting of an E-mail Message at sender site: To ensure secure communication via email, the process of digitally signing and encrypting a message involves several steps. Initially, the message content is captured for transmission.

Subsequently, distinct information that uniquely identifies the sender is obtained from the sender's credentials or digital certificate. Simultaneously, information uniquely identifying the intended recipient is retrieved from their digital certificate or specific contact information. The sender's unique information is then utilized to execute a signing operation on the message, generating a digital signature that verifies the sender's authenticity and integrity of the message content.

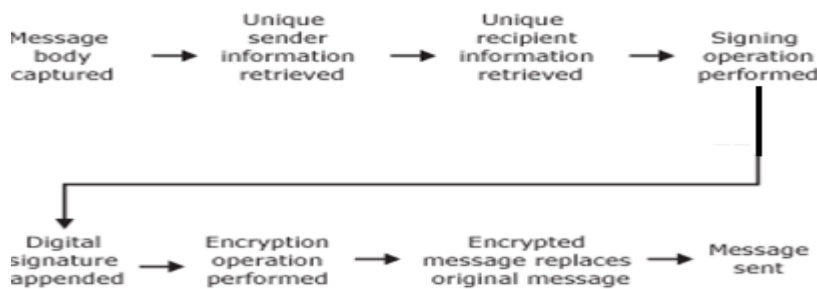


Figure 10 Digital signing and encrypting of an e-mail message together

This digital signature is appended to the message to create a signed message. Following this, an encryption operation is performed on the entire message, including the appended digital signature, utilizing the recipient's unique information.

This encryption process renders the message unreadable to anyone except the intended recipient, ensuring confidentiality during transmission.

The original message is replaced by this encrypted version, creating an encrypted message that includes both the original content and the digital signature. Finally, this encrypted message is sent securely to the recipient, safeguarding the confidentiality and integrity of the communication.

The figure 11 shows the sequence of decrypting and verifying the digital signature.

Decrypting an E-mail Message and Verifying a Digital Signature at receiver site:

Upon receiving an email, the encrypted message is retrieved along with information uniquely identifying the intended recipient, obtained typically from the recipient's credentials or digital certificates. Subsequently, a decryption operation is executed on the encrypted message, utilizing the recipient's unique information.

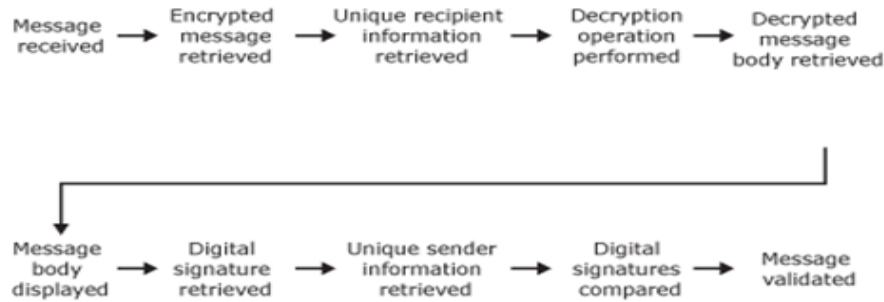


Figure 11 Decrypting an e-mail message and verifying a digital signature

This process results in the production of an unencrypted message, revealing the original content. The unencrypted message is then returned to the recipient, ensuring accessibility to the intended information. Concurrently, the digital signature associated with the message is retrieved from this unencrypted content. Additionally, information identifying the sender is obtained from the message itself. Using the sender's information, a signing operation is performed on the unencrypted message to generate a digital signature. The digital signature produced during the message reception is then compared against the digital signature created using the sender's information. If these two digital signatures match, it confirms the integrity and authenticity of the message, validating its contents as unchanged since the sender's signature was applied. This verification process ensures the validity and trustworthiness of the received message.

I. Main Email Security Protocols

The three main email security protocols DMARC, DKIM, and SPF complement one another, so implementing them all provides the best protection. The three will authenticate your mail server and prove to ISPs, mail services, and other receiving mail servers that senders are truly authorized to send an email. When properly set up, all three prove that the sender is legitimate, that their identity has not been compromised, and that they're not sending email on behalf of someone else.

(i)SPF (Sender Policy Framework): and SPF [RFC 7208] is another excellent email authentication mechanism for email delivery and security. It secures the DNS servers and limits who can send emails on your behalf. Domain spoofing can be avoided with SPF. Internet Service Providers can use an SPF record to verify that a mail server is permitted to send email for a certain domain. An SPF record is a DNS TXT record that lists the IP addresses that are permitted to send email on behalf of your domain. SPF consists of three primary components: a policy framework, an authentication technique, and particular headers in the email itself that convey this information. Receiving mail servers use SPF to verify that incoming email from a domain was sent from a host approved by the domain's administration. [<https://datatracker.ietf.org/doc/html/rfc7208>]

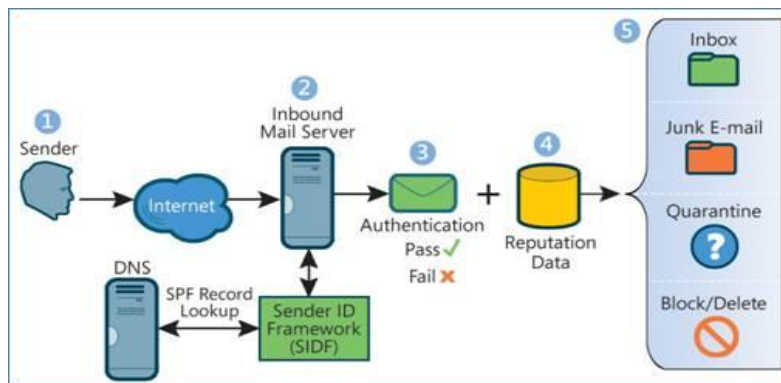


Figure 12 : SPF Working [8]

The following steps outline how SPF works:

The SPF record is published in the DNS. The record is a list of all the IP addresses that are allowed to send email on behalf of the domain and it is listed as part of the domain's overall DNS records.

The SPF mechanism uses the domain in the return-path address to identify the SPF record. The inbound server then compares the IP address of the mail sender with the authorized IP addresses defined in the SPF record.

The receiving mail server then uses the rules specified in the sending domain's SPF record to decide whether to accept, reject, or otherwise flag the email message. If you have a good sending reputation, a spammer may try to send email from your domain in order to benefit from your ISP's good sender reputation. However, properly set up SPF authentication will show the receiving ISP that even though the domain may be yours, the sending server has not been authorized to send mail for your domain.

(ii)DKIM (Domain Keys Identified Mail): DKIM [RFC 6376]is an email authentication method. This approach detects spoofed or fake sender email addresses. It is also another way to link an email back to a domain.When using DKIM, a sender can attach DKIM signatures to an email (header that is added to the message and is secured with encryption), and once the recipient receives the email, they can verify that it is actually you who sent it.Like SPF, DKIM is also used in DMARC alignment. The DNS has a DKIM record, although it's a little more difficult than SPF. DKIM has the advantage of being able to withstand forwarding, making it preferable to SPF and a solid basis for email security.

Working of DKIM: How DKIM Detects Suspect Emails?

When an inbound mail server receives a message, it will detect the DKIM signature and look up the sender's public DKIM key in DNS.

- Special DKIM signatures are attached to the emails that email servers transmit. These signatures travel with the emails and are confirmed as they make their way to their final destination by the email servers.
- These signatures operate as a watermark for email, allowing recipients to verify that the email came from the domain it claims to come from and that it hasn't been tampered with.
- The variable or DKIM selector provided in the DKIM signature is used to determine where to look for this key. If the key is found, it can be used to decrypt the DKIM signature. This is then compared to the values retrieved from the received mail. If they match, the DKIM is valid.

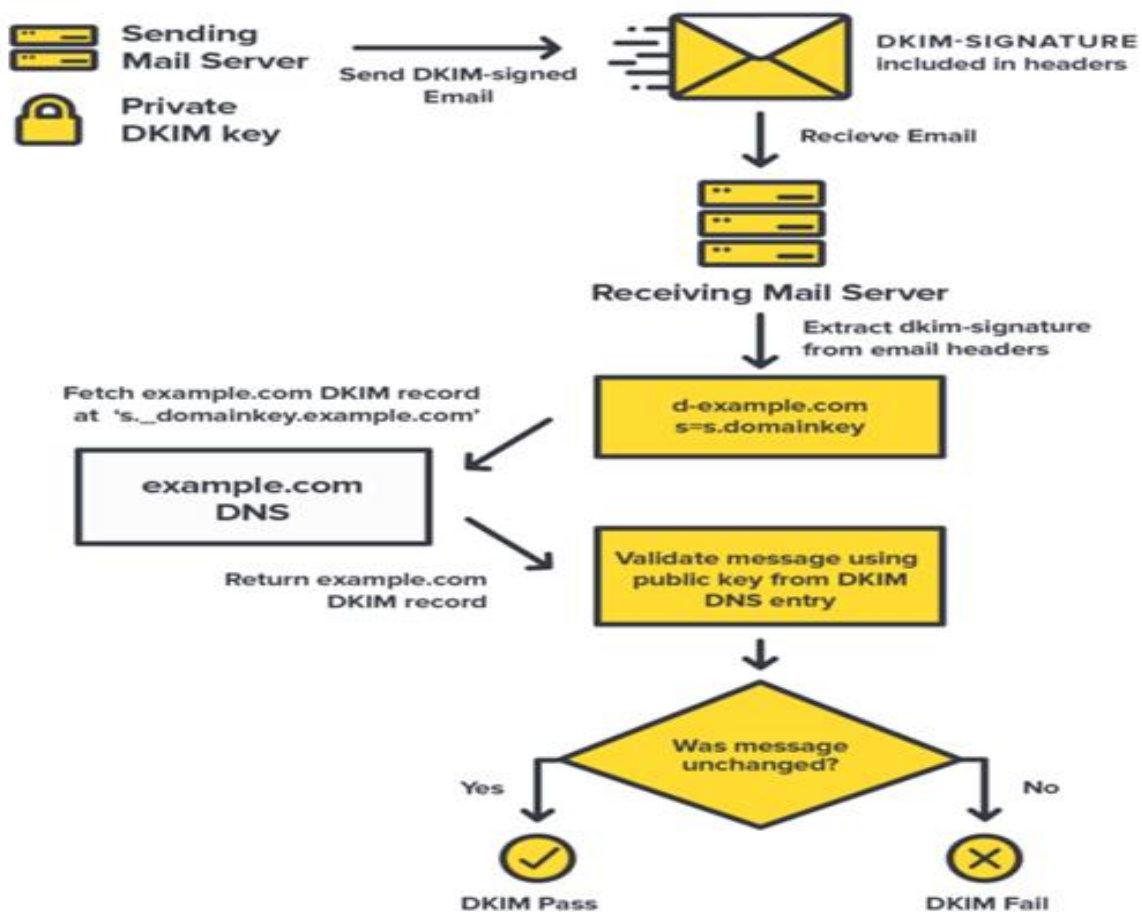


Figure 13 Working of DKIM [9]

(iii) How DMARC will suspect a malicious email?

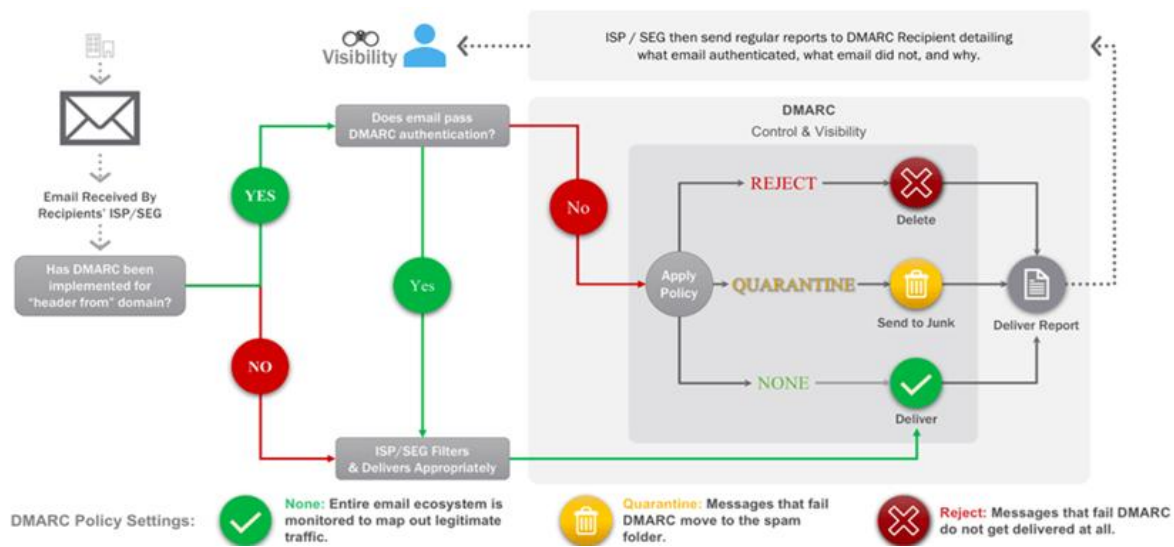


Figure14 How DMARC Works [10].

DMARC[11], an acronym for Domain-based Message Authentication, Reporting, and Conformance, relies upon established email authentication standards such as SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail). This authentication method leverages the widely-used Domain Name System (DNS) infrastructure. The process of DMARC validation begins with a domain administrator defining and publishing the email authentication practices for their domain, articulating how receiving mail servers should handle emails that contravene this policy. This DMARC policy is an integral part of the domain's overall DNS records.

When an inbound mail server receives an incoming email, it initiates a DNS lookup to retrieve the DMARC policy associated with the domain mentioned in the message's "From" header as per RFC 5322. Subsequently, the receiving server evaluates the message against three crucial criteria. Firstly, it verifies the validity of the DKIM signature appended to the message. Secondly, it confirms if the message originated from IP addresses authorized by the sending domain's SPF records. Lastly, it assesses the headers in the message to ensure proper "domain alignment."

Equipped with this information, the server proceeds to apply the DMARC policy linked to the sending domain, determining whether to accept, reject, or flag the email message for further action. Once the server applies the DMARC policy and reaches a decision regarding the appropriate handling of the message, it then reports the outcome to the owner of the sending domain. This reporting loop ensures that domain administrators stay informed about the disposition of emails sent using their domain, enhancing security and facilitating a more reliable email ecosystem.

EMAIL FORENSIC INVESTIGATION PROCESS

Conducting an email forensic investigation involves a systematic approach to collect, analyze, and interpret email-related evidence while ensuring the preservation of digital information.

J. Email Forensic Investigation

The email forensic investigation process steps involved in conducting an email forensic investigation are (i) Identification Collection, examination and preservation of digital evidence from emails. (ii) Role of metadata and header analysis in email forensics[13].

Step 1 (i) Identification and Preservation of Evidence: Identify the scope of the investigation, including specific email accounts, time frames, or subjects of interest and Immediately preserve the integrity of potential evidence by securing access to relevant email accounts or servers. Avoid accessing or altering potential evidence directly to maintain its integrity.

(a) Collection of Email Data: Gather email-related data from multiple sources, including email servers, individual devices (computers, smartphones), cloud storage, backup systems, or third-party email service providers. Ensure proper documentation of the collection process, including timestamps, sources, and chain of custody details to maintain evidentiary integrity.

(b)Metadata Extraction and Analysis: Extract metadata from email messages, including sender and recipient information, timestamps, IP addresses, and routing details. Secondly Analyze metadata to reconstruct the timeline of email communications, identify potential manipulation, or establish the authenticity of messages.

(c)Email Content Examination: Analyze the content of emails, including text, attachments, embedded files, and hyperlinks, to identify relevant information or potential threats. you can also utilize specialized tools to recover deleted or hidden data within email messages, attachments, or headers.

(d)Verification of Email Authenticity: Validate the authenticity of emails by examining digital signatures, message headers, DKIM (Domain Keys Identified Mail), SPF (Sender Policy Framework), or other cryptographic mechanisms. You can also check for signs of tampering, alterations, or spoofing in the email content or headers.

Step 2 Tracing IP Addresses and Tracking Sources: Trace the origin of emails using IP addresses, email headers, server logs, and forensic techniques to identify the source or location of email transmissions and determine the routing paths and intermediate servers used in email delivery.

(a)Tracing and Tracking Email Sources: Tracing sender and recipient details using IP addresses and header information and Analyzing email routing paths and timestamps to reconstruct the email journey. To trace IP Addresses, Forensic Investigator can use IP geolocation services or online tools to trace and map the IP addresses obtained from the email header. Enter the IP addresses into IP lookup tools or geolocation websites to determine their geographic location of senders and Internet Service Provider (ISP) and approximate physical location.

(b)Tracing sender and recipient details using IP addresses and header information. Performing an experiment to trace sender and recipient details using IP addresses and header information involves analyzing email headers and extracting IP addresses to determine the origin and destination of emails. To Verify IP Information, Forensic investigator can compare the geolocation data with known locations or the expected location of the sender or recipient. Note any inconsistencies or unexpected locations.

Step 3 Interpret Findings: Based on the traced IP addresses and their geolocation information, draw conclusions about the sender's or recipient's potential location or ISP. Consider the possibility of IP masking, VPN usage, or proxy servers that might obscure the true origin or destination.

(a)Documentation and Reporting: Document findings, observations, methodologies, and analysis in a detailed report adhering to forensic standards and Present the information gathered in a clear and organized manner, providing explanations for forensic techniques used and the significance of findings.

(b)Legal Compliance and Admissibility: Ensure that the investigation process complies with legal regulations, standards, and chain of custody requirements and Prepare the collected evidence and forensic report for presentation in legal proceedings, maintaining admissibility and reliability.

(c)Conclusion and Recommendations: Summarize key findings, conclusions, and implications arising from the email forensic investigation.

K. Research Experimentation for Email Forensic

This section discusses the research experimentation with respect to the methodologies to Access to email headers based on email clients and email header parameters to know the email senders address.

Accessing an Email Header: To Access to email headers, Open the email for which you want to trace sender and recipient details. The process to access the email header information might vary based on the email client as below[14][15][16]:

- Gmail: Open the email, click the three-dot menu, and select "Show original."
- Outlook: Open the email, go to "File," select "Properties," and find the header information.
- Other clients: Search online for instructions on viewing email headers specific to your email service.
- Identify Sender and Recipient IP Addresses:
- Locate the sender's and recipient's IP addresses within the email header.
- Look for "Received" fields or "X-Originating-IP" (sender's IP) and "Received" fields related to the recipient (if available). These fields often contain IP addresses.

L. Analyze Email Header Parameters

Analyze the email header to understand the sequence of servers the email passed through before reaching your inbox. Email headers contain essential information, including the name of the sender and receiver, the path (servers and other devices) through which the message has traversed, etc. Some of the critical email header fields are highlighted : see

email header used in Email Forensic Tool Section. Some of the vital details in email headers help investigators and forensics experts in the email investigation are discussed below [17] [18] [19].

(i) **The Delivered-To** field contains the recipient's email address, ie Indicates the email address to which the email was delivered.

And the **Received-By** field contains: (a) The last visited SMTP server's IP address. (b)It's SMTP ID. (c) The date and time at which the email is received.

(ii) **The Received: from:** Similarly, the Received: from field provides necessary details like the sender's IP address and hostname. Again, such information can be instrumental in identifying the culprit and collecting evidence.

(iii) **MIME-Version:** Indicates the MIME (Multipurpose Internet Mail Extensions) version used in the email.

(iv) **Content-Type:** Specifies the type and structure of the email content. In this case, it's a multipart/alternative message with a defined boundary.

(v) **Bounces-to:** Indicates the email address to which bounce notifications and errors should be sent. Similar to Return-Path.

(vi) **Feedback-ID:** Provides a unique identifier associated with feedback or tracking for the email.

These headers offer information about the email delivery, authentication, content structure, and handling of bounce notifications. They play a crucial role in ensuring the integrity and traceability of email communication.

These headers offer information about the email delivery, authentication, content structure, and handling of bounce notifications. They play a crucial role in ensuring the integrity and traceability of email communication.

(v) **ARC-Authentication-Results:** This header provides information about the authentication results of the email. ARC (Authenticated Received Chain) is a protocol designed to authenticate the email's forwarding history. The header contains multiple authentication results separated by semicolons (;). Each result indicates the outcome of different authentication methods such as DKIM, SPF, and DMARC. In the provided header, the email has passed DKIM, SPF, and DMARC checks [9] [10].

(vi) **ARC-Seal:** Part of the ARC (Authenticated Received Chain) protocol, this header provides a cryptographic seal for the email. The header includes information about the signature, algorithm, timestamp, and other parameters.

(vii) **ARC-Message-Signature:** Another part of the ARC protocol, this header contains the cryptographic signature for the entire email message. It includes information about the signature algorithm, message parameters, and the actual signature.

(viii) **Return-Path:** Specifies the email address to which bounce notifications and errors should be sent.

(ix) **Received-SPF:** Indicates the result of the Sender Policy Framework (SPF) check for the email. SPF helps prevent email spoofing by verifying that the sending mail server is authorized to send mail on behalf of the domain. The header specifies whether SPF validation passed or failed. In the provided header, SPF is marked as "pass," indicating that the email passed SPF validation.

(x) **Authentication-Results:** Provides a summary of the authentication results for the email. It includes information on DKIM, SPF, and DMARC. Similar to ARC-Authentication-Results, this header contains multiple authentication results. It specifies the outcome of DKIM, SPF, and DMARC checks [5] [6] [7] [8] [9] [10].

(xi) **DKIM-Signature:** Contains the DKIM signature for the email. DKIM (Domain Keys Identified Mail) is a method to digitally sign emails, allowing the recipient to verify that it was legitimately sent by the claimed domain.

The header includes information about the DKIM signature, such as the cryptographic algorithm used, the signing domain, and the signature itself. These headers collectively help ensure the authenticity and integrity of the email by verifying its origin and whether it has undergone proper authentication checks.

The "pass" results indicate that the email has successfully passed these checks [9].

Let's break down the explanation of each "X-" header in the provided email header [7]:

(xii) X-Google-Smtp-Source: Provides information about the source of the email as it passed through Google's SMTP servers. The header contains a unique identifier and details about the SMTP source, including server information.

(xiii) X-Received: Indicates the receipt of the email by a receiving server. It provides details about the server, timestamp, and other information. This header contains information such as the server's IP address, SMTP ID, timestamp, and timezone.

(xiv) X-Amazon-Mail-Relay-Type: Specifies the type of Amazon mail relay used for the email. In this case, the header indicates that the email is a "notification."

(xv) X-Amazon-Metadata: Contains metadata associated with the Amazon email relay. The header may include various metadata parameters. In the provided header, CA and CU are specified.

(xvi) X-Original-Message ID: Contains the original Message-ID of the email. It provides a unique identifier for the message. The header includes the original Message-ID enclosed in angle brackets.

(xvii) X-SES-Outgoing: Provides information about the outgoing SES (Simple Email Service) message, including the date and the IP address of the sending server. The header includes the date and the IP address of the server that sent the email.

These "X-" headers are used to convey additional information about the email's journey, origin, and characteristics, often specific to the email service providers involved in processing the message.

In email header analysis, time delay is calculated by examining the "Received" headers in the email. These headers provide a chronological record of the email's journey through various mail servers. Each "Received" header typically includes a timestamp indicating when the server received the email. The time delay between two consecutive "Received" headers is calculated by taking the timestamp of the later header and subtracting the timestamp of the earlier one. This time difference represents the delay introduced at that particular stage of the email's delivery.

J. Email Server Investigation

Email servers are investigated to locate the source of an email. For example, if an email is deleted from a client application, sender's, or receiver's, then related ISP or Proxy servers are scanned as they usually save copies of emails after delivery. Servers also maintain logs that can be analysed to identify the computer's address from which the email originated. It is worth noting that Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) logs are archived frequently by large Internet Service Providers (ISPs). If a log is archived, tracing relevant emails can take a lot of time and effort, requiring decompressing and extraction techniques. Therefore, it is best to examine the logs as soon as possible. Log paths on ISP or Proxy Servers for Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) logs for Email Communication are as below[3][4]:

(i) HTTP Logs

Proxy Servers: If the ISP uses proxy servers, HTTP logs might be stored on these servers. The path could be something like: /var/log/proxy/http.log or /var/log/squid/access.log.

Web Server Logs: If the ISP provides web hosting services or manages web servers, HTTP logs could be stored locally on those servers. Common paths include: /var/log/apache2/access.log for Apache web servers or /var/log/nginx/access.log for Nginx.

(i) SMTP Logs

Mail Server: For SMTP logs[3][4], they are often stored on the mail server itself. The location can vary based on the mail server software being used. For example:

Postfix: /var/log/mail.log or /var/log/maillog

Exim: /var/log/exim/mainlog

Sendmail: /var/log/maillog

Postfix and Exim (Experimental Internet Mailer), Sendmail are Mail Transfer Agents (MTAs), which are software programs responsible for sending, receiving, and routing email messages within a network. They are crucial components of email systems, facilitating the exchange of emails between servers and handling the delivery process.

(iii) ISP-specific Storage: Some ISPs[32] might centralize logs in specific directories for easier management. The paths might vary based on the ISP's internal configuration. The specific paths for ISP-specific storage of logs can vary significantly based on the ISP's infrastructure, server configuration, and chosen software. However, here are some general approximations of where logs might be stored within an ISP's environment. The specific paths for ISP-specific storage of logs can vary significantly based on the ISP's internal setup, server configurations, and logging mechanisms.

As such, providing exact or approximate paths for ISP-specific log storage isn't possible without direct knowledge of the ISP's infrastructure. However, in some cases, ISPs may centralize logs in directories named according to their functions or services. Here are some generic examples that might resemble the structure used by ISPs for log storage:

/var/log/isp_name/

Some ISPs might have a dedicated directory with their name (or an abbreviation) within the /var/log/ directory. For instance, /var/log/provider_name/ or /var/log/isp_initials/.

/var/log/services/

ISPs might categorize logs by services. For example:

/var/log/mail/ for email-related logs

/var/log/http/ or /var/log/web/ for HTTP-related logs

/var/log/proxy/ for proxy-related logs

/var/log/network/ for general network-related logs

/var/log/application/

Some ISPs might organize logs based on specific applications or software:

/var/log/postfix/ for Postfix MTA logs

/var/log/exim/ for Exim MTA logs

/var/log/apache2/ for Apache HTTP server logs

/var/log/nginx/ for Nginx web server logs

ISPs may centralize logs for easier management and monitoring. Common paths for centralized logs might include directories like /var/log/isp/, /var/log/network/, or custom directories designed by the ISP's system administrators.

Please note that these paths are approximate and may not match the actual directory structure of a specific ISP. Accessing these logs would typically require administrative privileges or authorized access granted by the ISP.

K. Investigation of Network Devices

In some cases, logs of servers are not available. This can happen for many reasons, such as when servers are not configured to maintain logs or when an ISP refuses to share the log files. In such an event, investigators can refer to the logs maintained by network devices such as switches, firewalls, and routers to trace the source of an email message[3][4].

Routers: Routers maintain logs of IP traffic passing through them. These logs may include information like source and destination IP addresses, ports, and timestamps. By examining router logs, investigators can potentially trace the path of email traffic as it moves through different network segments.

IP Routing Logs: Routers might store logs in locations such as:

(i)/var/log/router.log (ii)/var/log/messages (iii)/var/log/syslog

Firewalls: Firewalls record information about permitted and denied network traffic. They might log details such as source IP addresses, destination IP addresses, port numbers, protocols, and actions taken (allowed or blocked). Analyzing firewall logs can help in determining if email traffic was allowed through or blocked at specific points in the network.

Firewall Logs: Firewall logs could be located in:

(i)/var/log/firewall.log (ii)/var/log/iptables.log (iii)/var/log/security/fw.log

Switches: Switches maintain logs related to MAC addresses and port activity. While these logs might not contain email content specifics, they can provide information about the physical location of devices communicating on the network. This information could be useful in determining which devices were involved in the transmission of email messages.

Port-Level Information: Switches might store logs in places like:

(i)/var/log/switch.log (ii)/var/log/port_activity.log

Within the switch's operating system, typically accessible through command-line interfaces (CLI) rather than stored as conventional log files.

Network Flow Data: Network flow data might not be stored directly as log files but collected and managed by specialized tools or software that can store this information in databases or specific directories. If using NetFlow or sFlow, data might be stored in a dedicated directory or database managed by the monitoring tool[24].

Sender Mailer Fingerprints-headers are email headers that are added to messages along with standard headers, like Subject and To. These are often added for spam filter information, authentication results, etc., and can be used to identify the software handling the email at the client, such as Outlook or Opera Mail. In addition, the x-originating-IP header can be used to find the original sender, i.e., the IP address of the sender's computer.

Message-IDs: Message-ID is a unique identifier that helps forensic examination of emails across the globe. Message IDs are generated by client programs that send emails, such as Mail User Agents (MUA) or Mail Transfer Agents (MTA). There are two parts of a Message-ID. One part is before @, and another part is after @. The first part of the message-ID contains information, such as the message's timestamp. This information is the data regarding the time when the message was sent. The second part of the Message-ID contains information related to the Fully Qualified Domain Name (FQDN).

Embedded Software Identifiers: Sometimes, the email software used by a sender can include additional information about the message and attached files in the email. For example, it can be found in Multipurpose Internet Mail Extensions (MIME) content as a Transport Neutral Encapsulation Format (TNEF) or custom header. An in-depth analysis of these sections can reveal vital details related to the sender, like the MAC address, Windows login username of the sender, PST file name, and much more.

Bait Tactics:The bait tactic is an email investigation technique used when the location of a suspect or cybercriminal is unknown. In this, the investigators send the suspect an email containing an http: tag. The image source is on a computer that the investigators monitor. When the suspect opens the email, the computer's IP address is registered in a log entry on the HTTP server that hosts the image. The investigators can use the IP address to track the suspect. Sometimes, suspects take preventive measures like using a proxy server to protect their identity. In that case, the IP address of the proxy server is recorded. However, the log on the proxy server can be analyzed to track the suspect.

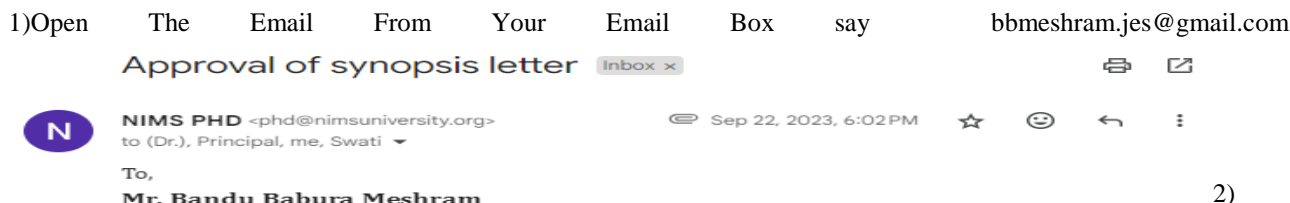
EMAIL FORENSICS TOOLS: RESEARCH EXPERIMENTATION

Email header investigation is a common technique used in email forensics to gather useful information about an email, including sender and receiver information and the path the message took to reach its destination. Google Message Header Analyser tool[20],Mail Xaminer[21],MX Toolbox[22],Email TrackerPro[23],Paraben (Network) E-mail Examiner[24],Aid4Mail Forensic[25], Digital Forensic Framework (DFF)[26] are some of the forensic tools used to obtain digital evidence from emails.

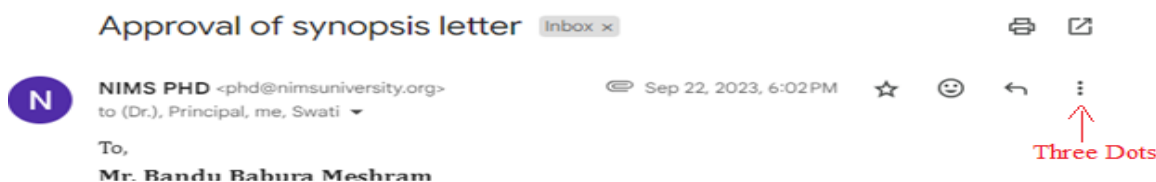
L. Research Experimentation using Google Message Header Analyser

Google Message Header Analyser is a tool provided by Google Workspace (formerly known as G Suite) that allows users to view and analyze the headers of an email message. The tool can be useful for identifying potential spam or phishing emails, as well as for troubleshooting email delivery issues. It can also provide insights into the source and path of an email message, which can be helpful for investigating suspicious or fraudulent activity[20][27][28][30].

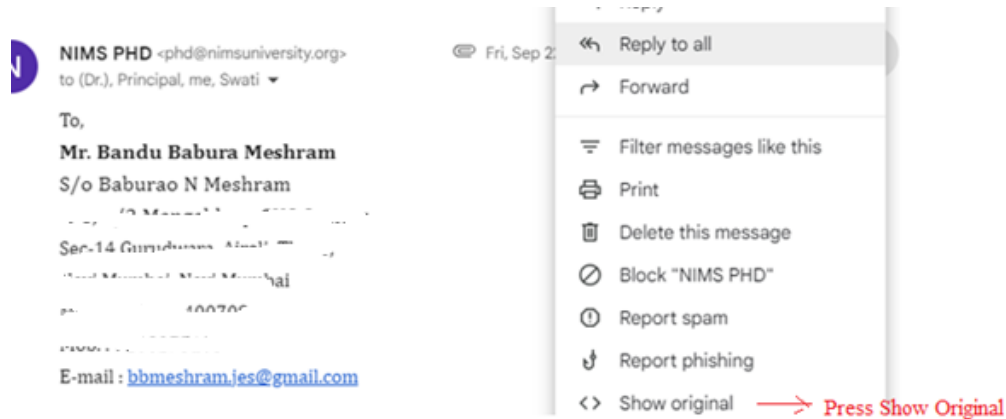
To Access the tool use the link - <https://toolbox.googleapps.com/apps/messageheader/>



Press to three dots for the above mail at Left hand side as shown below and click show original and obtain the header of email.



3) After pressing three dots you will get the following:



4) Press show original, you will get the following

mail.google.com/mail/u/0/?ik=8b4bbc5e34&view=om&permmsgid=msg-f:1777741006784180068

Original Message

Message ID	<CANVJ6uV_9SbF0Yqgg=UghN9VetobXM=usfT5actHXVTgmkVzWg@mail.gmail.com>
Created at:	Fri, Sep 22, 2023 at 6:02 PM (Delivered after 10 seconds)
From:	NIMS PHD <phd@nimsuniversity.org>
To:	"Prof. (Dr.) Manju Koolwal" <drmanjukoolwal@gmail.com>, Principal Law <principallaw@nimsuniversity.org>
Subject:	Approval of synopsis letter
SPF:	NEUTRAL with IP 209.85.220.41 Learn more
DKIM:	'PASS' with domain nimsuniversity-org.20230601.gappssmtp.com Learn more
DMARC:	'FAIL' Learn more

5) The partial header information is shown as below

Download Original Copy to clipboard

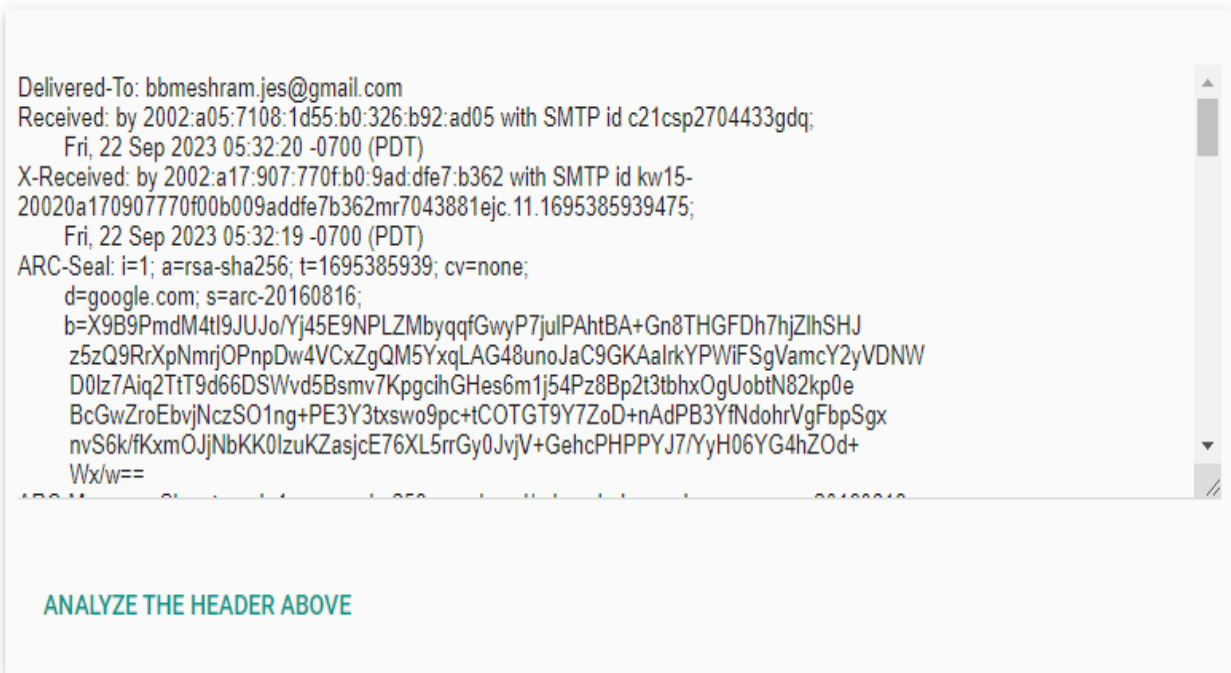
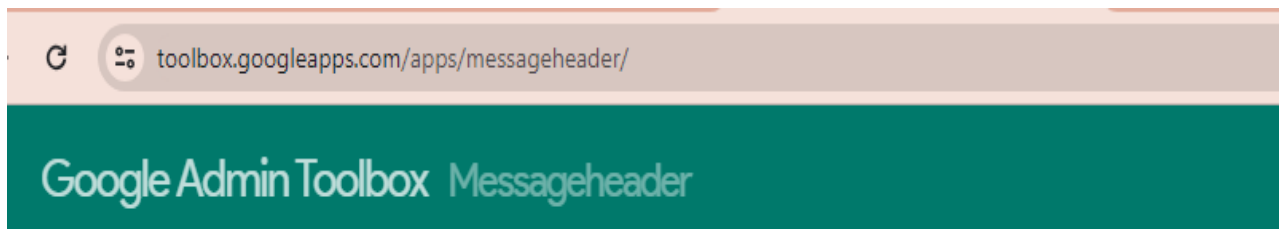
```

Delivered-To: bbmeshram.jes@gmail.com
Received: by 2002:a05:7108:1d55:b0:326:b92:ad05 with SMTP id c21csp2704433gdq;
  Fri, 22 Sep 2023 05:32:20 -0700 (PDT)
X-Received: by 2002:a17:907:770f:b0:9ad:df7:b362 with SMTP id kw15-
20020a170907770f00b009addfe7b362mr7043881ejc.11.1695385939475;
  Fri, 22 Sep 2023 05:32:19 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1695385939; cv=none;
  WX/W==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
  h=cc:to:subject:message-id:date:from:mime-version:dkim-signature;
  bh=2/VmPAQF50553SVyB2PewemE8L7dqtX9AiMmtSmy/ZA=;

```

```
ARC-Authentication-Results: i=1; mx.google.com;
    dkim=pass header.i=@nimsuniversity-org.20230601.gappssmtp.com header.s=20230601
    header.b="gkVnAA/n";
    spf=neutral (google.com: 209.85.220.41 is neither permitted nor denied by domain of
    phd@nimsuniversity.org) smtp.mailfrom=phd@nimsuniversity.org;
    dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=nimsuniversity.org
Return-Path: <phd@nimsuniversity.org>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
X-Google-Smtp-Source:
AGHT+IFQBmXpvcnePomzjWl6YG34VQSN/B7VKkq1V7irf46133UkX7DkC3rDyX0iaWeat7pxrjvpsBGHRCIrFK7Hnqw=
X-Received: by 2002:a17:906:41:b0:9ad:e66a:4141 with SMTP id 1-
20020a170906004100b009ade66a4141mr7752240ejg.28.1695385937669; Fri, 22 Sep 2023 05:32:17 -0700
(PDT)
MIME-Version: 1.0
From: NIMS PHD <phd@nimsuniversity.org>
Date: Fri, 22 Sep 2023 18:02:09 +0530
Message-ID: <CANVJ6uV_9SbF0Yqqg=UghN9VetobXM=usfT5actHXVTgmkVzWg@mail.gmail.com>
Subject: Approval of synopsis letter
To: "Prof. (Dr.) Manju Koolwal" <drmanjukoolwal@gmail.com>, Principal Law
<principallaw@nimsuniversity.org>
Cc: Bandu Meshram <bbmeshram.jes@gmail.com>, "Dr. Swati Sharma" <principalnis@nimsuniversity.org>
Content-Type: multipart/mixed; boundary="0000000000009366760605f1ccd4"
```

6) Paste the header of email in google admin tool box as below



7) Press Analyse The Header Above, you will get the following screen

toolbox.googleapps.com/apps/messageheader/analyzeheader

Google Admin Toolbox Messageheader

MessageId: CANVJ6uV_9SbF0Yqqg=UghN9VetobXM=usFT5actHXVTgmKvZwg@mail.gmail.com

Created at: 9/22/2023, 6:02:09 PM GMT+5:30 (Delivered after 11 sec)

From: NIMS PHD <phd@nimsuniversity.org>

To: "Prof. (Dr.) Manju Koolwal" <drmanjukoolwal@gmail.com>, Principal Law <principallaw@nimsuniversity.org>

Subject: Approval of synopsis letter

SPF: **neutral** with IP Unknown!
[Learn more](#)

DKIM: **pass** with domain nimsuniversity-org.20230601.gappssmtp.com
[Learn more](#)

DMARC: **fail**
[Learn more](#)

8) You will also get the intermediate server for the flow of information From to To as shown in the following screen

#	Delay	From *	To *	Protocol	Time received
0	8 sec		2002:a17:906:41:b0:9ad:e66a:4141	SMTP	9/22/2023, 6:02:17 PM GMT+5:30
1	2 sec	mail-sor-f41.google.com.	[Google] mx.google.com		9/22/2023, 6:02:19 PM GMT+5:30 <i>Originated at Gmail</i>
2			[Google] 2002:a17:907:770f:b0:9ad:df7:b362	SMTP	9/22/2023, 6:02:19 PM GMT+5:30
3	1 sec		[Google] 2002:a05:7108:1d55:b0:326:b92:ad05	SMTP	9/22/2023, 6:02:20 PM GMT+5:30

[ANALYZE ANOTHER HEADER](#)

[SHOW RAW HEADER](#)

Return-Path: <phd@nimsuniversity.org>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])

Activate Windows
Go to Settings to activate Windows

The mail is received from mail server having IPAddress:209.85.220.41, You can obtain IP address of the sender using section 4.1 //program to get an IP address of given Domain Name: <https://www.nimsuniversity.org/>, as the mail is received from phd@nimsuniversity.org .

The IP addresss of the sender is found to be: 14.139.244.19(<https://www.nimsuniversity.org>)

Note: use Geolocation Tool to find the address of sender or receiver as experimented in section 4.4 IP Geolocation Tools

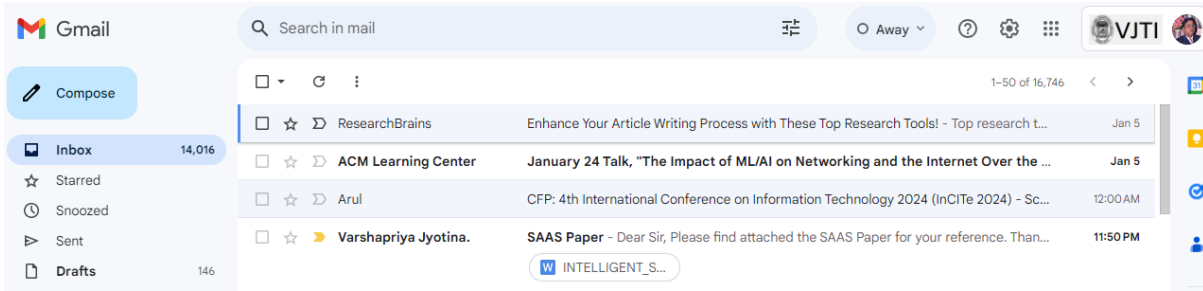
The Destination Mail Server is:gmail.com.You can use program to get an IP address of given mail server.**Received-By** field contains the last visited SMTP server's IP address. And **X-Received:** Indicates the receipt of the email by a receiving server's IP address as shown below,

Delivered-To: bbmeshram.jes@gmail.com
Received: by 2002:a05:7108:1d55:b0:326:b92:ad05 with SMTP id c21csp2704433gdq;
Fri, 22 Sep 2023 05:32:20 -0700 (PDT)
X-Received: by 2002:a17:907:770f:b0:9ad:df7:b362 with SMTP id kw15-20020a170907770f00b009addfe7b362mr7043881ejc.11.1695385939475;

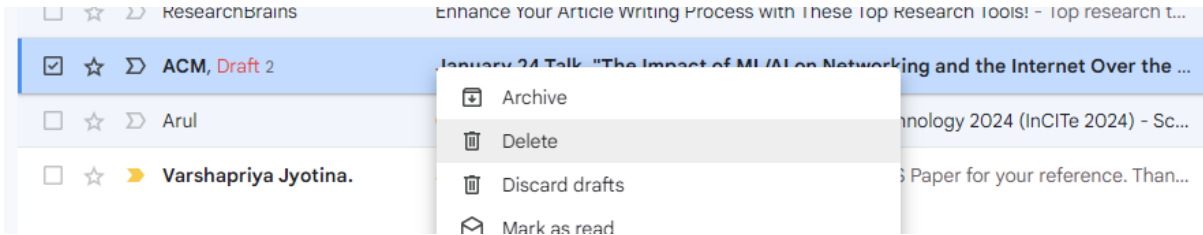
We have traced all the intermediate mail servers.

J.Deleted Email Recovery

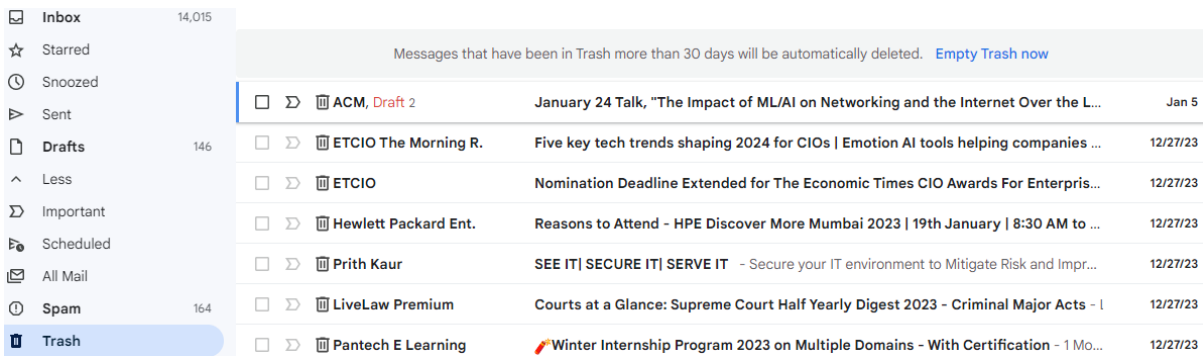
Log in to your Gmail account.bbmeshram@vjti.ac.in



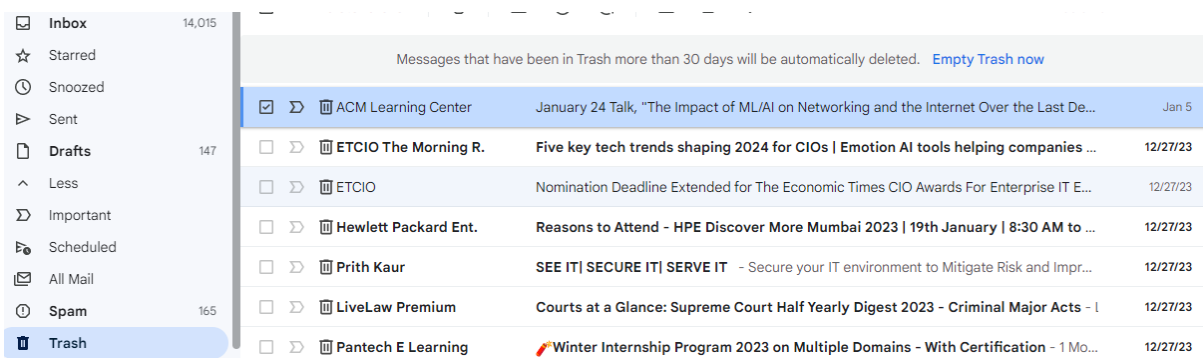
2) So, we will delete a mail from inbox



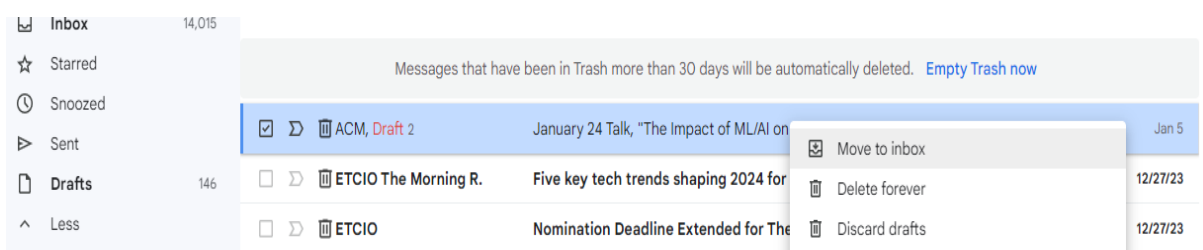
3) To the left of the screen, there is a list of folders. Choose the Trash option from this menu.



4) Once you've opened the folder, you can start to recover deleted emails. Select the messages you wish to recover by clicking on the box to the far left of the email row. ACM Learning Centre.



5) Now, click on the Move button. You can select where to put the deleted email from the drop-down menu. You can simply select the Inbox option if you don't want to organize the email into another folder.



6) Check your Inbox to see if the email has been restored.



We can see that the email that was deleted is recovered

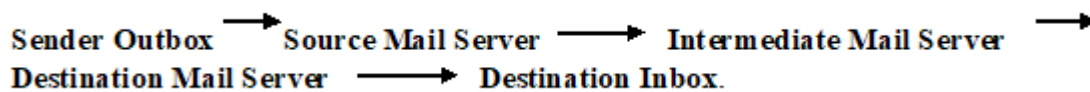


Proposed Experimentation for Email Forensic

All email communications on the internet is governed by rules and regulations laid down by two different protocols ((i)Simple Mail Transfer Protocol(SMTP port 25) (ii)Post Office Protocol(POP port 110). Each e-mail on the internet originates at the sender's post office server with the help of SMTP commands. It is routed via number of intermediate mail servers and then finally reaches to the destination post office where the receiver use POP commands to download it to local system. E-mail headers are automatically generated and embedded into an e-mail message both during composition and transfer between systems[31][32][33][34].

K. Email Travel Path

The Email Travel Path represents the exact path taken by it, which can be represented as



One can identify the source of the email by Reverse Engineering the path traveled by it. Each time an email is sent on the Internet, it not only carries the message body , but also transmits relevant information on the path travel by it. This information is known as Email Header of the email.

Algorithm for Email Tracking

```

1. Open the Email header.
// The SMTP protocol is used to send emails while the POP protocol is used to receive them.
2. Identify the source and destination of email by tracing the path
   Sender Outbox ----> Source Mail Server----> Intermediate Mail Servers ---->Destination Mail
   Server ---> Destination Inbox.
3. Identify the IP Address of the computer that was used to send the email with the help of Unique Message ID
reference stored on the log file on a Mail Server.
OR
Step 3 can be performed as below
// Use Reverse DNS look up ie convert the suspected IP Address into the corresponding hostname.
Use utility named nslookup.
$>nslookup IP Address of the sender
$>nslookup 203.94.243.71
203.94.243.71 has valid reverse DNS of mail2.mtnl.net.in
OR
Step 3 : Write a program to convert the Given IP Address to hostname or vice versa using JAVA coding IPAddress API
//Program to get domain name of IP Address
import java.net.*;
public class IPByAddress {
    public static void main (String[] args) {
        try {
            InetAddress address = InetAddress.getByName("64.135.83.93:25");
            System.out.println(address);
        }
        catch (UnknownHostException ex) {
  
```

```
System.out.println("Could not find 64.135.83.93:25");
}
}
}
```

//program to get all IP addresses of given Domain Name

```
import java.net.InetAddress;

public class GetAllIP {
    public static void main(String[] args) throws Exception {
        InetAddress[] addr = InetAddress.getAllByName("www.google.com");
        for (int i = 0; i < addr.length; i++)
            System.out.println(addr[i]);
    }
}
```

Output of the program

```
www.google.com/64.233.181.103
www.google.com/64.233.181.105
www.google.com/64.233.181.106
www.google.com/64.233.181.104
www.google.com/64.233.181.147
```

//program to get an IP address of given Domain Name

```
import java.net.InetAddress;
import java.net.UnknownHostException;

public class GetIP {
    public static void main(String[] args) {
        InetAddress address = null;
        try {
            address = InetAddress.getByName("www.vjti.ac.in");
        } catch (UnknownHostException e) {
            System.exit(2);
        }
        System.out.println(address.getHostName() + "="
            + address.getHostAddress());
        System.exit(0);
    }
}
```

```
www.vjti.ac.in=72.35.74.72
```

L. Illustrative example of Forensic Analyzing E-mail Header

To open full email header, use section 3.2.1 Accessing an Email Header as per your client browser. You can then copy and paste the entire header into the email forensic tools to view a detailed analysis of the headers [32][33][34][35]. The emailheader is given below and divided into Part1 and part 2.

Part i ;ReturnPath:Jeman.m@ce.vjti.ac.in


Path: jeman.m@ce.vjti.com
 Return Received: from Jeman.m@ce.vjti.com by (64.135.83.93:25) via ctpmail2.vjti.com
 (203.77.177.39:4627) with [InBox.Com SMTP Server] id 1007270051209.WH93 for komal@inbox.com.
 ESMTP id 2010072714324098-56908 ; Tue, 27 Jul 2010 14:32:40 +0530
 Received: from inbox.com; Tue, 27 Jul 2010 01:05:31 -0800
 Received: from ABFSSVREXHS02.BSLI.COM ([10.158.1.241]) by ctpmail1.vjti.com (Lotus Domino Release
 7.0.3) with EXMBXCLU.BSLI.COM ([10.158.1.236]) by ABFSSVREXHS02.BSLI.COM ([10.158.1.241])
 with mapi; Tue, 27 Jul 2010 14:38:39 +0530

Part I of the Email
header

Part ii: From Jeman Meshram<Jeman.m@ce.vjti.com

Content-Type: multipart/alternative;
boundary=" _000_CD6383A18C901F45A39D744A7B4F925B1AF919247EEXMBXCLUBSLIC_"
Content-Language: en-US X-Spam-Ratio: 1.95

Part II of the Email Header



From: Jeman Meshram <Jeman.m@ce.vjti.com>
To: "Komal@inbox.com" <Komal@inbox.com>
Date: Mon, 25 Sept 2023 14:38:38 +0530
Subject: Email IP Traceback
Thread-Topic: Email IP Traceback
Thread-Index: AQHLLWrMR6gRxEOHUuc+UOXI0cO9JLEe64w
Message-ID: <20100727143839.30156.@EXMBXCLU.BSLI.COM>
Accept-Language: en-US X-MS-Has-Attach: X-MS-TNEF-Correlator: acceptlanguage: en-US
MIME-Version: 1.0
X-MIME Track: Itemize by SMTP Server on CTPMAIL1/Insc(Release 7.0.3| October 14, 2023) at 09/25/2023 02:32:40 PM, Serialize by Router on Ctpmail2/Insc(Release 7.0.3| October 14, 2023) at 09/25/2023 02:36:37 PM, Serialize complete at 09/25/2023 02:36:37 PM
Content-Type: multipart/alternative;boundary=" _000_CD6383A18C901F45A39D744A7B4F925B1AF919247EEXMBXCLUBSLIC

Part 1 of the Email Header

Return Path: Jeman.m@ce.vjti.ac.in

This email address tells us that e-mail was sent by **Jeman.m@ce.vjti.ac.in**

The Source Mail Server: via ctomail2.vjti.com([203.77.177.39])

The Destination Mail Server is : inbox.com

Part II Of the Email Header analysis

Return-Path: Jeman.m@adityabirla.com

(i) This e-mail address is the sender's e-mail address.

(ii) **Message Id:** field of the e-mail header can be broken down in the following manner-

Id-20100727143839.30156: The e-mail was sent in the year 2023, month Sept, day 25th and at the time 14 hours, 38 minutes and 39 seconds. 30156: Each e-mail send by the Mail Server has unique message Id reference number associated with it. The log file contain all the message Id's. Cyber crime Investigators often use the reference number to carry out investigations.

(ii) The Source Mail Server: ABFSSVREXHS02.BSLI.COM ([10.158.1.241])

(iii) The Destination Mail Server : inbox.com

(iv) The Intermediate Mail Server: EXMBXCLU.BSLI.COM ([10.158.1.236])

(v) The receiver connects to this destination mail server and download the e-mail using simple POP command.

Thus the complete path travelled by e-mail can be depicted in the following manner :

(Source) 64.135.83.93:25----- → (Source Mail Server) ABFSSVREXHS02.BSLI.COM
([10.158.1.241]) -- → (Intermediate Mail Server) EXMBXCLU.BSLI.COM ([10.158.1.236]) --- →
(Destination Mail Server) inbox.com --- → TARGET SYSTEM(Destination).

You can use program to get an IP address of given Domain Name inbox.com or Geolocation Tool.

M. Use of Memory and Browser Forensic For Email Forensic

The researcher formulate the second procedural method for email forensic which involves memory and browser processes analysis, string searching, and parsing within the memory space of the email client process.

The steps are as bellows[36][37][38][39][40]:

Step 1.Capture Browser Processes from Live Memory

- Access the live memory (RAM) to capture the currently running browser processes.
- Identify the email-related process and extract necessary information.

For instance when analysing a process such as Google Chrome for email-related information, including email headers or other relevant data, the steps involve:

- Obtaining a memory dump of the running Google Chrome process (acquired either through live analysis or from a memory image).
- Analysing this memory dump using specialized tools like Volatility or Rekall.

Step 2 .Search for Email Header in Memory For browser Processes:

- Use specific techniques to search for the email header within the extracted browser processes in memory.
- Searching within the memory space of the browser say Chrome process for strings, patterns, or structures that may contain email-related information, including headers or sender IP addresses.
- Employ methods like STRINGS64 to scan and extract ASCII and UNICODE strings related to the email header.

Step 3. Filter and Extract Email Header

- Filter out and isolate the extracted email header information.
- Store the extracted email header in a separate file for further examination.
- Extract IP Address from Email Header:
- Identify and extract fields within the email header that contain sender-related information.
- Look for fields like "Received-By:"**X-Received** or "X-Originating-IP:" or other headers that might contain the sender's IP address.

Step 4.Examine Header Fields for Sender's IP

- Parse and examine the extracted header fields to locate the sender's IP address.
- Use regular expressions or string manipulation techniques to isolate and extract the IP address information.

Step 5 Validate and Confirm the IP Address

- Perform any necessary validation to confirm that the extracted IP address is indeed the sender's IP.
- Cross-reference with other information or external sources if available for validation.

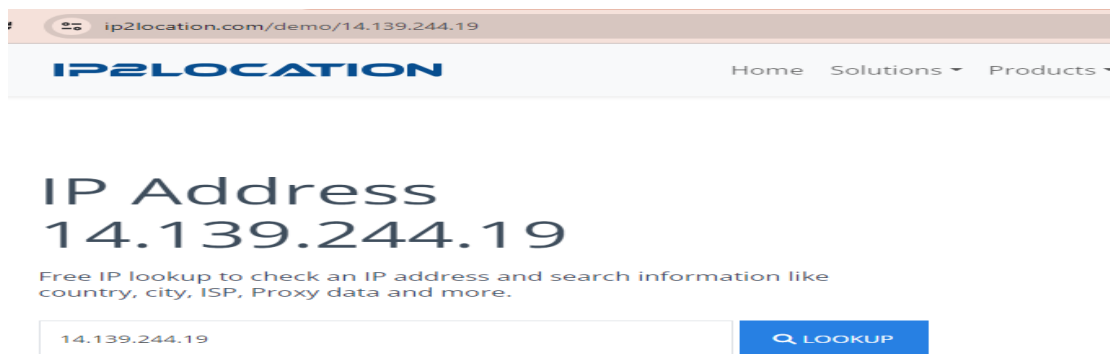
N.IP Geolocation Tools

How can you find the Geolocation of the attacker?

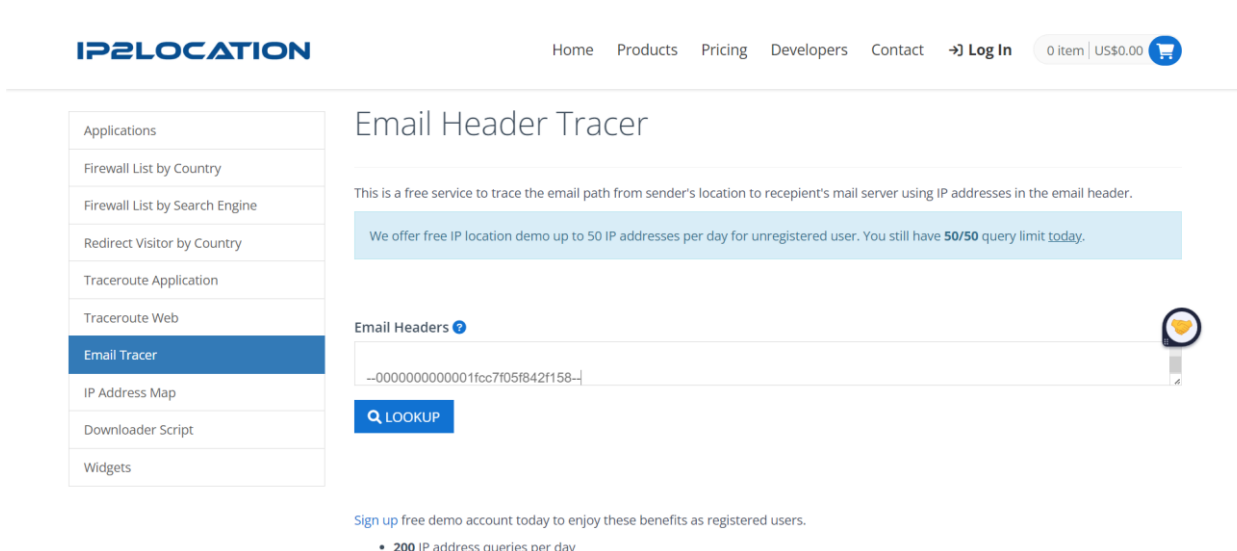
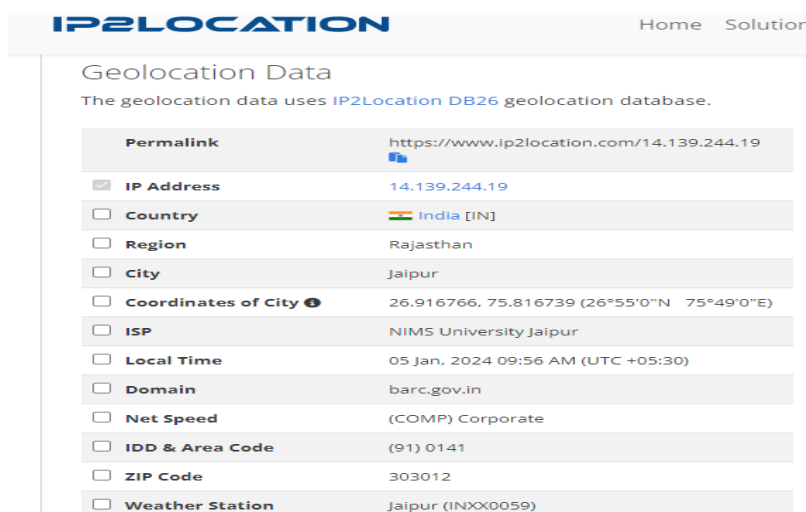
Given the IP Address , one can find the address of attacker using geolocation Tools like WhatisMyIPAddress:<https://whatismyipaddress.com/>,VirusTotal is an Alphabet product that analyzes suspicious files, URLs, domains and IP addresses to detect malware and other types of threats, and automatically shares them with the security community. To view VirusTotal reports, you'll be submitting file attachment hashes, IP addresses, or domains to VirusTotal

Now in order to get more meaningful information from the email header we copy paste the entire header in IP2 location tool to get the following results.

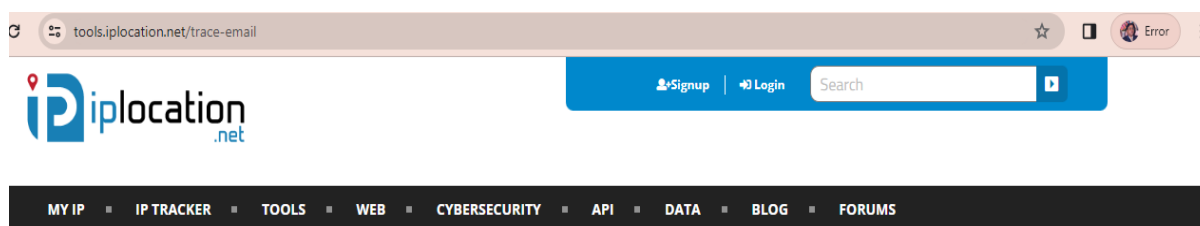
The IP address: 14.139.244.19 of case instance under section 3.2.1 Research Experimentation using Google Message Header Analyser is entered into the IP2 location tool[42] as below:



By entering the IP address 14.139.244.19, press QLOOKUP, We get the geolocationaddress of IP: 14.139.244.19 as below:



2) Now we copy paste the entire header in our second tool i.e. IP location tool to get forensic results



LAW USED FOR EMAIL HACKING AND FORGING

This section discusses the email attacks and cyber laws its sections for the punishment of email cybercrimes.

O. Email Attacks

This technical brief provides an overview of some of the most common email attacks, including hacking, spoofing, phishing, email bombing, whaling, and spamming [46][47].

- Hacking: Email hacking[5] involves unauthorized access to an individual's email account or system. An attacker may gain access to an email account by guessing a weak password, using social engineering tactics to trick the user into revealing their password, or exploiting vulnerabilities in the email server or software[45].
- Spoofing: Email spoofing is the act of forging the sender's email address to make it appear as if the message came from a different source. Spoofed emails[40] are often used in phishing attacks to trick the recipient into revealing sensitive information or downloading malicious software.
- Phishing: Phishing is a type of social engineering attack that uses fraudulent emails or messages to trick recipients into revealing sensitive information or downloading malware. Phishing emails often appear to come from a trusted source, such as a bank or financial institution, and typically ask the recipient to click on a link or download an attachment[34].
- Vishing: Vishing is a type of phishing that uses voice communication technologies. Using voice-over-IP technologies, criminals can impersonate calls from authorised sources. Victims may also hear a recorded message that appears to be authorised. Many credit card related and financial frauds happen through vishing. Vishing takes advantage of the fact that people have faith in the telephone network.
- Email Bombing: Email bombing is a type of denial-of-service attack that involves sending many emails to a target email account, causing the recipient's email server to become overloaded and crash. Email bombing attacks can be carried out manually or using automated tools[46].
- Smishing: While a text may seem perfectly normal, it could be from someone with malicious intent—someone who wants to steal your identity, your bank account number, or other sensitive information. Smishing is a phishing cybersecurity attack carried out over mobile text messaging, also known as SMS phishing[47]
- Whaling: Whaling is a type of phishing attack that targets high-level executives and other high-value targets within an organization. These attacks are often personalized and designed to trick the target into revealing sensitive information or transferring funds to an attacker-controlled account[52].
- Spamming: Email spamming involves sending large volumes of unsolicited emails to a large number of recipients. Spam messages are often used to advertise products or services, distribute malware, or carry out phishing attacks. Spam messages can be filtered and blocked using anti-spam software and other email security measures[51][54].

Email attacks are a significant threat to individuals and businesses, and attackers are constantly evolving their tactics to evade detection and gain access to sensitive information. To protect against email attacks, individuals and organizations should use strong passwords, enable two-factor authentication, regularly update their email software and security measures, and educate themselves and their employees about the risks of email attacks. Email filtering is the process of detecting and blocking unwanted or malicious messages from reaching a recipient's inbox. There are several email filtering techniques used by email service providers and organizations to prevent spam[51] [54]., phishing[52] [53] and other email-based attacks[49] [50]

P. Cyber Law For Combating Email Crimes

This section explore the sections of cyber laws and punishment for the email attacks [45][46][47]. Primarily, in terms of seeking restitution for victims of e-mail attack, concerning compensation, the options available to victims vary based on the magnitude of the financial harm & impact they have suffered as discussed below:.

Email Phishing falls under the purview of various legal sections, notably Section 66-D of the IT Amendment Act, 2008[45], along with Sections 379 and 420 of the Indian Penal Code (IPC). These legal provisions encompass different consequences and recourse for individuals engaged in such illicit activities. For instance, individuals may seek compensation up to Rs. 10 lakh through the Banking Ombudsman. Alternatively, they can pursue compensation up to 5 crore by engaging with the Adjudicating Officer. If the compensation exceeds 5 crore, recourse through the Civil Court becomes viable. Furthermore, victims also retain the option of pursuing arbitration. Secondly, in terms of penalties imposed on perpetrators, imprisonment for a maximum of 3 years and a fine of up to one lakh can be levied. These punitive measures serve as a deterrent against engaging in phishing activities. Lastly, the legal classification of the Email Phishing offense under Section 77-B entails its nature and treatment within the legal system. This offense is categorized as cognizable and bailable, aligning with Section 268 of the IPC. However, it is deemed non-cognizable, bailable, and uncompoundable with the court's permission, reflecting the legal complexities and procedures involved in addressing such offenses[52].

E-mail Bombing falls under the legal purview outlined in Section 43 (e) of the I.T. Amendment Act, 2008, along with Section 66 of the I.T. Act, and Section 287 of the Indian Penal Code (IPC). A complainant has the right to claim compensation up to 5 crore by approaching the Adjudicating Officer. If the claimed compensation surpasses 5 crore,

recourse through the Civil Court is an available avenue. Additionally, arbitration stands as an alternative mechanism for complainants seeking redressal. Secondly, regarding penalties imposed on offenders, the provisions within the I.T. Act stipulate that the punishable act may result in imprisonment for a maximum of 3 years, a fine of up to five lakh, or both. These punitive measures aim to serve as a deterrent against individuals involved in perpetrating e-mail bombing activities. Lastly, understanding the legal classification of the offense is essential for comprehending its treatment within the legal system. Under Section 77-B of the I.T. Act[46], the offense is classified as cognizable and bailable. Conversely, under Section 287 of the IPC [56], it is categorized as non-cognizable, bailable, and non-compoundable, necessitating permission from the Magistrate for resolution.

Identity theft of email credentials is a significant breach of privacy and security. Identity theft of email credentials [45] [56] constitutes a serious offense, covered under Section 66-C of I.T. Act, along with Section 449 of the Indian Penal Code (IPC). These statutory provisions define the legal framework and implications for individuals involved in such illicit activities. Firstly, in terms of the legal treatment of this offense, it is classified as cognizable and bailable[46]. This classification denotes that authorities have the power to make an arrest without a warrant and the accused can seek bail during the proceedings. Furthermore, under Section 449 of the IPC, , it is considered cognizable, bailable, and compoundable with the permission of the Court. This means that with the consent of the Court, the victim and the accused can mutually resolve the matter by reaching a settlement, subject to legal authorization.

E-mail fraud falls under the ambit of several legal statutes, notably Section 66-C and Section 66-D of I.T. Act, as well as Section 415 and Section 420 of the Indian Penal Code (IPC). Under Section 77 of the I.T. Act[45], the offense is classified as cognizable and bailable[57]. This classification signifies that authorities have the power to arrest without a warrant, and the accused can seek bail during the legal proceedings. Furthermore, the application of Section 415 of the IPC alters the legal classification, rendering the offense non-cognizable, bailable, and compoundable[47] with the permission of the Magistrate. Conversely, if the offense is charged under Section 420 of the IPC, it is characterized as cognizable, non-bailable, and compoundable with the permission of the Court.

E-mail spoofing: particularly falls in instances involving Section 66-D and additional sections such as 417, 419, and Section 465 of the IPC[56]. Primarily, under Section 66-D, the legal implications are substantial, governing the actions related to cheating by impersonation using computer resources. Additionally, Sections 417, 419, and Section 465 of the IPC supplement this framework[56], further defining the legal boundaries and consequences associated with fraudulent activities. Furthermore, the legal classification of the offense under Section 77-B denotes it as cognizable and bailable.

This classification implies that authorities have the power to arrest without a warrant and that the accused can seek bail during the legal proceedings[57].When Section 417 of the IPC is applied to the offense, it becomes non-cognizable, bailable, and compoundable with the permission of the Magistrate. In contrast, if the offense is charged under Section 419 of the IPC, it is classified as cognizable, bailable, and compoundable with the permission of the Court[56]. This particular distinction implies that while the offense may be considered grave enough to be cognizable, the accused may be granted bail more readily, and any potential resolution would require permission from the Court.

CONCLUSION

This paper suggests a detailed and in-depth examination of the intricacies and complexities involved in the practice of email communication Systems. Email protocols like SMTP (Simple Mail Transfer Protocol), POP (Post Office Protocol), IMAP (Internet Message Access Protocol), MIME(Multipurpose Internet Mail Extensions) and Methods to authenticate emails and validate their integrity like SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail), DMARC(Domain-based Message Authentication, Reporting, and Conformance) are studied which are useful for email communication systems. Standard Email Infrastructure and Mail Delivery Process, Digital signing and encrypting of an e-mail message together, Decrypting an e-mail message and verifying a digital signature is also discussed which is crucial to understand the email header.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real. Overall, email systems rely on a combination of protocols Mail servers, ISP and clients to facilitate the exchange and management of electronic messages, ensuring reliable communication across the internet. Secure email communication involves steps like capture message, obtain unique sender & recipient information from credentials or digital certificates, sign message using sender's information for authenticity, append digital signature to create a signed message. Then, encrypt the entire message, including the signature, using recipient's info for confidentiality. Replace the original message with this encrypted version, ensuring both message and signatures are encrypted. Lastly, send the encrypted message, securing confidentiality and integrity. Upon receiving the email, decrypt the message using recipient's information, producing an unencrypted message. Retrieve sender's information, create a digital signature on the message, and extract the digital signature from the unencrypted content. Compare both signatures; if they match, the message is valid, ensuring integrity and authenticity.

The headers of an email contain information such as the sender's email address, recipient's email address, date and time of the message, and routing information. The header contains metadata or control information that can be crucial evidence in criminal investigations. The authenticity of the information is also checked during header analysis to ensure its validity. Server and network device investigation can also be done to gather information related to emails. Logs maintained by servers and network devices can be helpful in tracing the source of emails. Firstly the paper explore the email forensic investigation process and examine the various forensic objects such as Email Server Investigation with respect to HTTP Logs, SMTP Logs, Investigation of Network Devices such as IP Routing Logs, Firewall logs, and Port-Level Information is also examined to trace the source of an email message. Email Log Locations can vary widely based on the monitoring or analysis software used to capture and manage network flow data. Please note that these paths are approximate and generalized. The actual log locations can differ significantly based on the device configuration, firmware, and the preferences of the network administrator. Access to these logs may require appropriate permissions and access rights. Always adhere to legal and organizational policies when accessing or analysing logs on network devices.

Secondly the experimentation using email forensic tools such as Google Message Header Analyser, is performed, for investigating the email senders home address using geolocation IP2Location tool.

Thirdly the researcher provided the algorithmic steps for opening the Email Header, analysis of Email Header, converting IP Address to domain name and vice versa to know about intermediators ISP and IP address of the Email sender with illustrative case study for email forensic.

Thirdly the researcher proposed the Email Forensic Investigation algorithm using memory image and browser processes- the combination of experiment and programs to identify the header information objects.

The researcher has also identified Email attacks- E-mail bombing, phishing, identity theft of Email credentials, E-mail fraud (breach of trust and integrity), E-mail spoofing and compensation and punishment under I.T. Act, 2008 and IPC. E-mail attack activities are subject to a spectrum of legal ramifications, encompassing options for compensation, penalties for perpetrators, and specific legal classifications of email crimes within the Indian legal framework, as outlined by the pertinent provisions of the I.T. Act and the IPC.

Future Directions: Email forensics can also be used in organized crime investigations based on social network analysis to find relationships between communications corresponding to criminal organizations.

REFERENCES

- [1]. Kavi Mailing List Manager Help,,Chapter 7. How Email Really Works, https://www.oasis-open.org/khelp/kmlm/user_help/html/how_email_works.html
- [2]. A TCP/IP Stack rfc :<https://www.rfc-editor.org/rfc>
- [3]. B. B. Meshram, Ms. K.A. Shirsath, TCP/IP and Network Security, Shroff Publishers 7 Distributors Pvt, Ltd. Mumbai Feb 2018, ISBN Number 978-93-5213-355-0
- [4]. William Stallings, Cryptography and Network Security: Principles and Practice, **8th Edition - Pearson** Paperback – 9 June 2023
- [5]. Ankit Fadia, E-Mail Hacking, 1/e, Vikas Publishing
- [6]. Internet assigned Numbers Authority (iana) (Message Headers Rfcs Information: 2023-09- :<https://www.iana.org/assignments/message-headers/message-headers.xhtml>
- [7]. IAB, IANA, IETF, IRTF, ISE, ISOC, IETF Trust: Reports <http://www.rfc-editor.org/info/rfc7208> Matt Harrison, What is Sender Policy Framework (SPF)?
- [8]. (June 18, 2014):<https://www.hallme.com/blog/sender-policy-framework-spf/> What is DKIM? DomainKeys Identified Mail Explained: [<https://www.duocircle.com/resources/what-is-dkim>]
- [9]. What is DEMARK: <https://www.proofpoint.com/au/threat-reference/dmarc>
- [10]. P. Loshin, Essential Email Standards: RFCs and Protocols Made Practical, Wiley, 2000.
- [11]. Dilpreet Singh Bajwa et al, Review of E-mail System, Security Protocols and Email Forensics International Journal of Computer Science & Communication Networks, Vol 5(3), 201-211, 07 December 2015.
- [12]. Medical Forensics Principles And Cyber Crime Forensic Investigation Model
- [13]. Journal of Web Applications and Cyber Security, :<https://qtanalytics.in/JoWACSQTanalytics> Delhi, India (accepted for publication)
- [14]. Email Header: Get to know how to view and analyse an email header in different Email Clients:https://sendpulse.com/support/glossary/email-header#How_to_find_an_email_header
- [15]. How to view an email header:<http://www.arin.net/>

- [16]. Ross Thomas is The SSL Store's IT Manager, How to read an Email Header (March 26, 2019):<https://www.thesslstore.com/blog/how-to-read-an-email-header/>
- [17]. Understanding An Email Header(**March 9, 2020**):<https://mediatemple.zendesk.com/hc/en-us/articles/204643950-understanding-an-email-header>:
- [18]. Learn more about headers at http://www.cs.utk.edu/~vose/other/mail_headers.html
- [19]. Email Header Analysis and Forensic Analysis :<https://www.thesslstore.com/blog/how-to-read-an-email-header/>
- [20]. Google Message Header Analyzer: <https://toolbox.googleapps.com/apps/messageheader/>
- [21]. MailXaminerfrom<https://www.mailxaminer.com/download.html>
- [22]. MX Toolbox:Visit<https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx>
- [23]. Email TrackerPro. <http://www.emailtrackerpro.com/>
- [24]. Paraben (Network) E-mail Examiner. <http://www.paraben.com/email-examiner.html>
- [25]. Aid4Mail Forensic. <http://www.aid4mail.com/>
- [26]. Digital forensic framework: <https://github.com/arxsys/dff>
- [27]. Vamshee Krishna Devendran, Hossain Shahriar, Victor Clincy, A Comparative Study of Email Forensic Tools,Journal of Information Security, 2015, 6, Published Online April 2015 in SciRes. <http://www.scirp.org/journal/jis> doi
- [28]. MitkoBogdanoski, LjubomirLazić , E-Mail Forensics: Techniques And Tools For Forensic Investigation ,The 10th International Conference on Business Information Security (BISEC-2018), 20th October 2018, Belgrade, Serbia.p
- [29]. Digital Forensics Framework. <http://www.digital-forensic.org/>
- [30]. Vamshee Krishna Devendran, "A Comparative Study of Email Forensic Tools", https://www.researchgate.net/publication/275027885_A_Comparative_Study_of_Email_Forensic_Tools , Journal of information security 2015
- [31]. MitkoBogdansoksi, "Email forensics: techniques and tools for forensic investigation", https://www.researchgate.net/publication/344906935_E-Mail_Forensics_Techniques_And_Tools_For_Forensic_Investigation , 10th International Conference on BISEC, 2018
- [32]. BarryRaveendram Greene , Philip Smith ,Cisco ISP Essentials, A Compressive Guide To The Best Common Practices For Internet Service Providers, Cisco press.com
- [33]. Email Header Analysis and Forensic Investigation:<https://www.youtube.com/watch?v=nK5QpGSBR8c>
- [34]. ShamalFirake, Dr.B.B.Meshrametal., Phishing E-mail Analysis
- [35]. International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 21 Volume 2, Issue 1, February 2011
- [36]. Hong Guo, Bo Jin, Wei Qian , Analysis of Email Header for Forensics Purpose 2013 International Conference on Communication Systems and Network Technologies, 2013 IEEE DOI 10.1109/CSNT.2013.78
- [37]. Hong Guo; Bo Jin; Wei Qian, "Analysis of Email Header for Forensics Purpose ", <https://ieeexplore.ieee.org/document/6524415> , International Conference on Communication Systems and Network Technologies (CSNT) [5] GautamShrivastav,Zunera Ali , "Email Classification and Forensics Analysis using Machine Learning B. B. Meshram , Manish Kumar Singh ,Cyber Crime Detection Methodology & Tools: An Experimentation Research, ICASEM-HYDERABAD
- [38]. M. R. Jadhav, B. B. Meshram, —Web Browser Forensics for Detecting User Activities" International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 07 | July 2018. [Online]. Available on: www.irjet.net
- [39]. Hassan Adamu , AbdullahiAdamu Ahmad , Adamu Hassan , Web Browser Forensic Tools: Autopsy, BHE and NetAnalysis International Journal of Research and Scientific Innovation (IJRSI) |Volume VIII, Issue V, May 2021|ISSN 2321-2705 www.rsisinternational.org .
- [40]. Sanjeev Shukla, Manoj Misra, Identification of Spoofed Emails by applying Email Forensics and Memory Forensics ,, ICCNS 2020, November 27–29, 2020, Tokyo, Japan © 2020 Association for Computing Machinery. ACM ISBN 978-1-4503-8903-7/20/11
- [41]. WhatisMyIPAddress :<https://whatismyipaddress.com/>
- [42]. IP2 location tool: <https://www.ip2location.com/demo/14.139.244.19>
- [43]. IPtrackeronlinetool :<https://www.iptrackeronline.com>
- [44]. Bandu B. Meshram , Manish Kumar Singh, " **Unveiling The Hackers' Methodology: Exploring Cyber Crimes, Cyber Laws And Punishment**", IJRARTH00102 International Journal of Research and Analytical Reviews (IJRAR) 953, 2023 IJAR July 2023, Volume 10, Issue 3 www.ijrar.org (E-ISSN 2348-1269, P- ISSN 235138): Available : <https://www.ijrar.org/papers/IJRARTH00102.pdf>
- [45]. The Information Technology Act of 2000,
- [46]. Dr. Gupta and Agrwal , Cyber Laws, Premier Publishing Company, 2023
- [47]. Dr. Santosh Kumar, Cyber Laws and Crimes, Whites Mann, Publishing Company, Sept 2020
- [48]. Iqbal, Khalid, and Muhammad Shehrayar Khan. "Email classification analysis using machine learning techniques." Applied Computing and Informatics ahead-of-print (2022).
- [49]. Shrivas, Akhilesh Kumar, Amit Kumar Dewangan, and Samrendra Mohan Ghosh. "Robust Text Classifier for Classification of Spam E-Mail Documents with Feature Selection Technique." Ingénierie des Systèmesd'Information 26, no. 5 (2021).

- [50]. Magdy, Safaa, Yasmine Abouelseoud, and Mervat Mikhail. "Efficient spam and phishing emails filtering based on deep learning." *Computer Networks* 206 (2022): 108826.
- [51]. Samarthrao, Kadam Vikas, and Vandana M. Rohokale. "Enhancement of email spam detection using improved deep learning algorithms for cyber security." *Journal of Computer Security* 30, no. 2 (2022): 231-264.
- [52]. R. Suriyal , K. Saravanan² and ArunkumarThangavelu An Integrated Approach to Detect Phishing Mail Attacks A Case Study, 3, SIN'09, October 6–10, 2009, North Cyprus, Turkey. Copyright 2009 ACM 978-1-60558-412-6/09/10
- [53]. Huajun Huang, ShaohongZhong, Junshan Tan, Browserside Countermeasures for Deceptive Phishing Attack, Fifth International Conference on Information Assurance and Security, 2009.
- [54]. Prosun, PriyoRanjanKundu, Kazi Saeed Alam, and ShovanBhowmik. "Improved Spam Email Filtering Architecture Using Several Feature Extraction Techniques." In *Proceedings of the International Conference on Big Data, IoT, and Machine Learning: BIM 2021*, pp. 665-675. Springer Singapore, 2022.
- [55]. IPC bare Act 1860
- [56]. K D Gaur, Textbook on Indian Penal Code, Universal Law Publishing, 2009
- [57]. Apar Gupta, Commentary on Information Technology Act, With Rules, Regulations, Orders, Guidelines, and Reports, Lexis Nexis Butterworths Wadhwa Nagpur, 2011