ANSWER KEY

Q1.

A. LIST AND BRIEFLY DESCRIBE THE DIFFERENT COMPONENTS OF AN EMAIL MESSAGE. EXPLAIN HOW EACH COMPONENT IS USEFUL IN AN EMAIL FORENSIC ANALYSIS.

 Header:

- Description: Contains metadata like the sender's and recipient's email addresses, subject, date, and routing information.
- Usefulness in Forensics: Helps identify the origin and destination of the email, as well as the servers it passed through, which is essential for tracing the email's path and detecting potential spoofing or forging attempts.

 From Field:

- Description: Specifies the sender's email address.
- Usefulness in Forensics: Provides the primary identification of the sender, which can be cross-referenced with other evidence to confirm or deny the sender's identity.

 To Field:

- Description: Contains the recipient's email address.
- Usefulness in Forensics: Useful to verify the intended recipient of the email, assisting in linking the email to the person under investigation.

 Subject Field:

- Description: Brief description or title of the email's content.
- Usefulness in Forensics: Helps in identifying the context of the email. It can provide crucial clues regarding the email's purpose or the nature of the communication.

 Date and Time Stamp:

- Description: Indicates when the email was sent.
- Usefulness in Forensics: Essential for establishing a timeline of events and verifying the authenticity of the email in relation to other communications or events.

 Message Body:

- Description: The main content of the email.
- Usefulness in Forensics: Contains the core information of the email, which can be examined for intent, language patterns, or evidence of illegal activity, such as threats or confidential data sharing.

 Attachments:

- Description: Files that are sent along with the email (e.g., documents, images, or videos).
- Usefulness in Forensics: Attachments can contain evidence such as malware, documents with sensitive information, or other artifacts critical for investigation.

 Reply-To Field:

- Description: Specifies the address to which replies should be sent, if different from the sender's address.
- Usefulness in Forensics: Identifies the communication path in case the reply differs from the sender's email address, which may help uncover hidden communications or fraud.

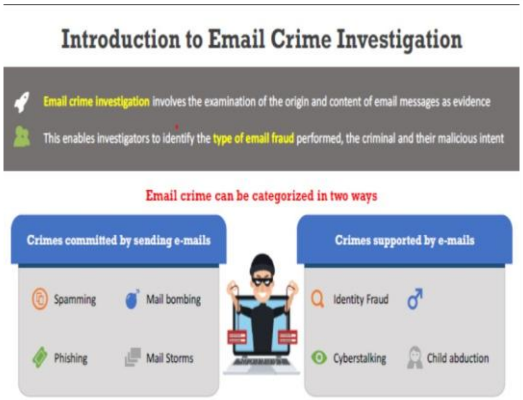
 Received Field:

- Description: Shows the email's route, including the servers it passed through before reaching the recipient.
- Usefulness in Forensics: Crucial for tracing the email’s path and verifying if it came from a legitimate source or was manipulated (e.g., spoofing, interception).

 IP Address (in headers):

- Description: The originating IP address of the email.
- Usefulness in Forensics: Provides a way to trace the physical location of the sender, which can be useful in confirming or challenging the sender’s identity.

B. DEVELOP A SUITABLE METHODOLOGY FOR CARRYING OUT EMAIL FORENSICS.



Introduction to Email Crime Investigation

Email crime investigation involves the examination of the origin and content of email messages as evidence

This enables investigators to identify the type of email fraud performed, the criminal and their malicious intent

Email crime can be categorized in two ways

Crimes committed by sending e-mails

Spamming

Mail bombing

Phishing

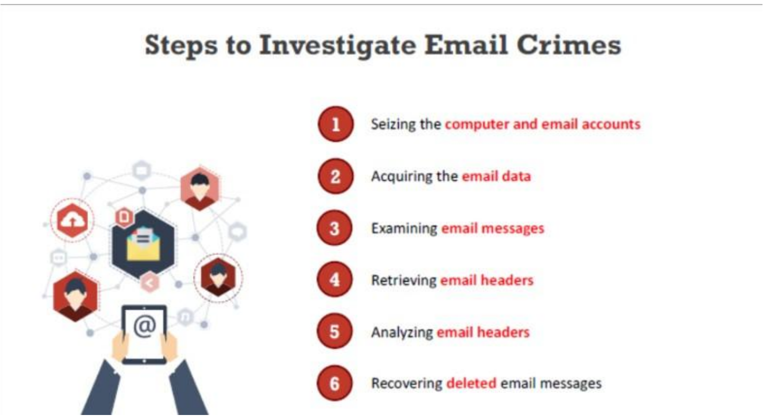
Mail Storms

Crimes supported by e-mails

Identity Fraud

Cyberstalking

Child abduction



Steps to Investigate Email Crimes

1 Seizing the computer and email accounts

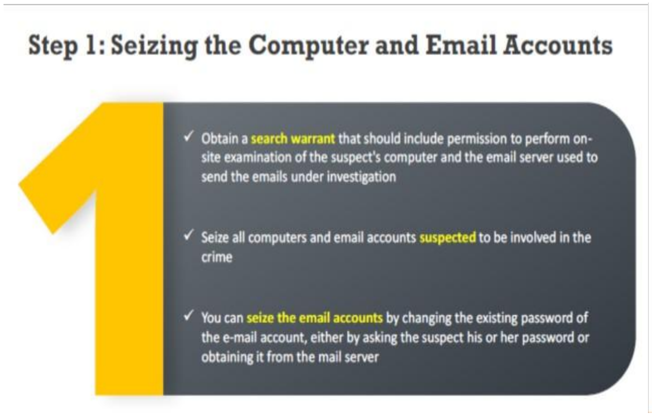
2 Acquiring the email data

3 Examining email messages

4 Retrieving email headers

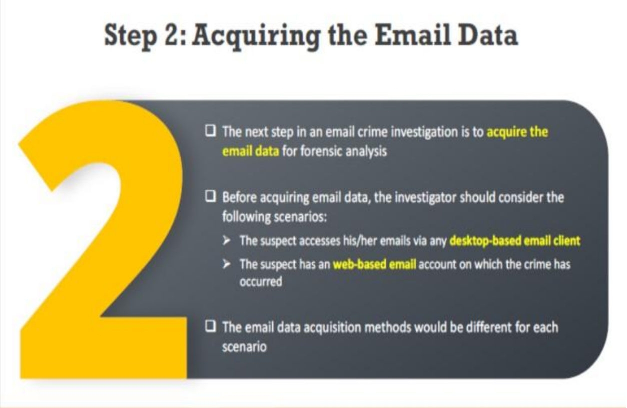
5 Analyzing email headers

6 Recovering deleted email messages



Step 1: Seizing the Computer and Email Accounts

- ✓ Obtain a search warrant that should include permission to perform on-site examination of the suspect's computer and the email server used to send the emails under investigation
- ✓ Seize all computers and email accounts suspected to be involved in the crime
- ✓ You can seize the email accounts by changing the existing password of the e-mail account, either by asking the suspect his or her password or obtaining it from the mail server

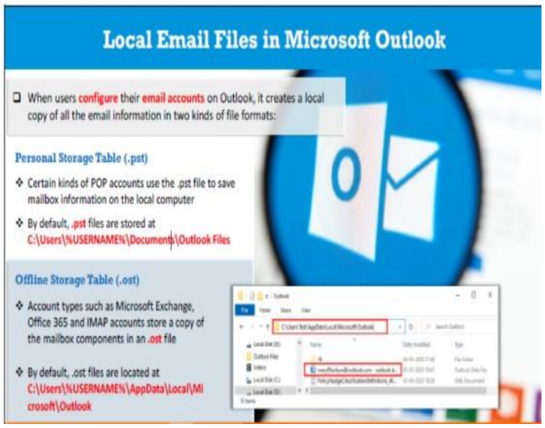


Step 2: Acquiring the Email Data

- ❑ The next step in an email crime investigation is to acquire the email data for forensic analysis
- ❑ Before acquiring email data, the investigator should consider the following scenarios:
  - ➢ The suspect accesses his/her emails via any desktop-based email client
  - ➢ The suspect has an web-based email account on which the crime has occurred
- ❑ The email data acquisition methods would be different for each scenario

Acquiring Email Data from Desktop-based Email Clients

local folders and archived files



Local Email Files in Microsoft Outlook

❑ When users configure their email accounts on Outlook, it creates a local copy of all the email information in two kinds of file formats:

Personal Storage Table (.pst)

- ❖ Certain kinds of POP accounts use the .pst file to save mailbox information on the local computer
- ❖ By default, .pst files are stored at C:\Users\%USERNAME%\Documents\Outlook Files

Offline Storage Table (.ost)

- ❖ Account types such as Microsoft Exchange, Office 365 and IMAP accounts store a copy of the mailbox components in an .ost file
- ❖ By default, .ost files are located at C:\Users\%USERNAME%\AppData\Local\Microsoft\Outlook

Acquiring Thunderbird Local Email Files via SysTools MailPro+

Source: *https://www.systoolsgroup.com*

Features

- ▪ Supports more than 12 email file formats
- ▪ Read the mailbox of any email file type
- ▪ Search emails within source email files in just a few clicks
- ▪ Create and save collections for easy mailbox management
- ▪ Search and extract emails from hard drive or external storage
- ▪ Add files in three modes to the software's dashboard
- ▪ Export emails into .pst, .pdf, .msg, .html, .eml, .tiff, and .csv file types
- ▪ Preview attachment types such as JPG, GIF, PNG, DOC, and PDF

Previewing Emails

This tool provides a preview of emails in various modes such as given below:

▪ **Normal Hex View**

It shows emails along with attributes such as To, CC, BCC, Subject, Date, and Time

Hex View

It shows emails in hex code in a bit-by-bit manner

▪ **Properties View**

It displays properties associated with emails such as message flags, recipients, and sender

▪ **Message Header View**

It provides viewing details such as X-Priority, Message ID, Thread-Index, Content-Type, and other information

MIME View

It shows emails in MIME format with various details

▪ **HTML View**

It displays emails in HTML with all the tags and body

▪ **RTF View**

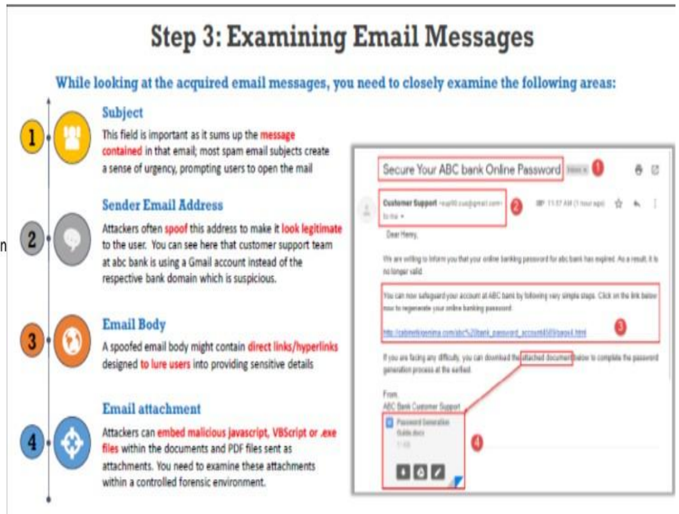
▪ This provides a preview of emails in plain text format

▪ **Attachments View**

This allows users to view the attachments in emails

▪ **Hierarchical View**

This shows the hierarchical view of the folder containing the source file



Step 3: Examining Email Messages

While looking at the acquired email messages, you need to closely examine the following areas:

1. **Subject**
   This field is important as it sums up the message contained in that email; most spam email subjects create a sense of urgency, prompting users to open the mail
2. **Sender Email Address**
   Attackers often spoof this address to make it look legitimate to the user. You can see here that customer support team at abc bank is using a Gmail account instead of the respective bank domain which is suspicious.
3. **Email Body**
   A spoofed email body might contain direct links/hyperlinks designed to lure users into providing sensitive details
4. **Email attachment**
   Attackers can embed malicious javascript, VBScript or .exe files within the documents and PDF files sent as attachments. You need to examine these attachments within a controlled forensic environment.

Secure Your ABC bank Online Password

Customer Support <[illegible]@gmail.com>
to me

11:57 AM (1 hour ago)

Dear Henry,

We are writing to inform you that your online banking password for abc bank has expired. As a result, it is no longer valid.

You can now safeguard your account at ABC bank by following very simple steps. Click on the link below now to regenerate your online banking password.

http://cabinetrigonima.com/abc%20bank_password_account45[illegible]page4.html

If you are facing any difficulty, you can download the attached document below to complete the password generation process at the earliest.

From,
ABC Bank Customer Support

Password Generation Guide.docx

Step 4: Retrieving Email Headers

If an offending email has been **identified or is suspected to be spoofed**, investigators must examine its header information

The email header plays a vital role in forensic investigation as it holds detailed **information on the email's origin**, which can help investigators gather supporting evidence and identify the culprit behind the crime

Email header information can be **retrieved** after acquiring the email messages

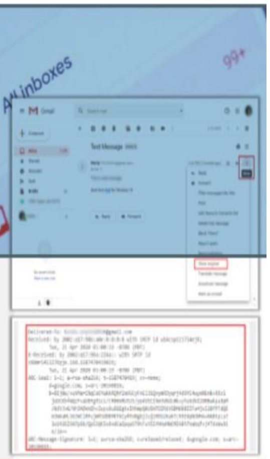
If the investigator is physically accessing the suspect's computer, they can **view the email header** using the same email program as the one used by the suspect. This process is different for different email programs.

Retrieving Email Headers in Gmail

Log on to **Gmail** and select the received mail for which you would like to see headers

Click on the **more** drop-down button and navigate to the **Show original** option

Select the message headers text, copy and paste the text in any **text editor**, and save the file



```
Delivered-To: [illegible]@gmail.com
Received: by 2002:[illegible] with SMTP id [illegible];
        Tue, 21 Apr 2020 [illegible] -0700 (PDT)
X-Received: by 2002:[illegible] with SMTP id
[illegible];
        Tue, 21 Apr 2020 [illegible] -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=[illegible]; cv=none;
        d=google.com; s=arc-[illegible];
        b=[illegible]
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-
[illegible]
```

Step 5: Analyzing Email Headers

01 **Timestamp:** Shows the **date and time** when the mail was sent

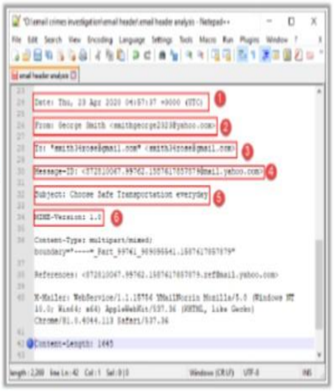
02 **From:** Shows the **email ID of the sender** as it is visible to the recipient; this can be forged in case of spam emails

03 **To:** Shows the **email ID of the recipient**

04 **Message ID:** As per **RFC 2822**, a specific email message should have a globally unique message identifier
The first part of the message ID before '@' contains the timestamp of the email (1587617857 in Unix epoch format converts to Thursday April 23, 2020 04:57:37 am in UTC)
The part of message ID after '@' contains the Fully Qualified Domain Name (here, the domain name is mail.yahoo.com)

05 **Subject:** Shows the subject as given by the **sender**

06 **MIME-Version:** Multi-purpose Internet Mail Extensions are used to **support non-text attachments** such as video, images, and audio and the default version is 1.0

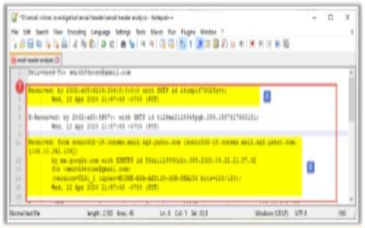

*D:\email crimes investigation\email header\email header analysis - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
email header analysis
1
2
3
4
5
6
length : 2,288 lines : 42 Ln : 42 Col : 1 Sel : 0 | 0 Windows (CR LF) UTF-8 INS

```
Date: Thu, 23 Apr 2020 04:57:37 +0000 (UTC)

From: George Smith <smithgeorge2323@yahoo.com>

To: "smith34rose@gmail.com" <smith34rose@gmail.com>

Message-ID: <872810047.99762.1587617857879@mail.yahoo.com>

Subject: Choose Safe Transportation everyday

MIME-Version: 1.0

Content-Type: multipart/mixed;
boundary="----=_Part_99761_989898541.1587617857879"

References: <872810047.99762.1587617857879.ref@mail.yahoo.com>

X-Mailer: WebService/1.1.15756 YMailNorrin Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/81.0.4044.113 Safari/537.36

Content-Length: 1445
```

Analyzing Email Headers (Cont'd)

07 **Received Header**

- The entries in the received headers are of significant forensic value as these **cannot be forged** unlike other email header elements
- The number of received headers found in an email message **depends on the mail servers** that processed the message as it travelled from source to destination
- Investigators should start with the bottommost received header **(B)**, as it is closest to the source and then move towards the top headers **(A)**
- Here, the **B header** is showing the domain name from which the email message originated (sonic302-19.consmr.mail.sg3.yahoo.com), the associated IP address (106.10.242.139), and the date and time in PDT


*D:\email crimes investigation\email header\email header analysis - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
email header analysis
7
A
B
Normal text file length : 2,183 lines : 41 Ln : 8 Col : 1 Sel : 0 | 0 Windows (CR LF) UTF-8 INS

```
Delivered-To: smith34rose@gmail.com
Received: by 2002:a05:6214:[illegible] with SMTP id [illegible];
        Wed, 22 Apr 2020 21:57:43 -0700 (PDT)

X-Received: by 2002:a05:[illegible] with SMTP id [illegible];
        Wed, 22 Apr 2020 21:57:43 -0700 (PDT)

Received: from sonic302-19.consmr.mail.sg3.yahoo.com (sonic302-19.consmr.mail.sg3.yahoo.com.
[106.10.242.139])
        by mx.google.com with ESMTPS id [illegible]
        for <smith34rose@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Wed, 22 Apr 2020 21:57:43 -0700 (PDT)
```

Analyzing Email Headers (Cont'd)

08 **Return-Path**

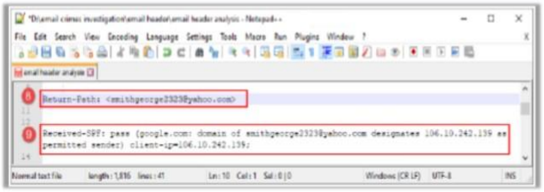
✓ It is the **bounce address for emails** that are sent but not delivered to the recipient

✓ If the sender's email address and the return-path address are different, it generally **indicates email spoofing**

09 **Received-SPF**

✓ Sender Policy Framework or SPF refers to the process that enables organizations to **mention servers** that can send emails on behalf of their domains

✓ An email header showing a failed SPF check can help **detect spam messages**


*D:\email crimes investigation\email header\email header analysis - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
email header analysis
8
9
Normal text file length : 1,816 lines : 41 Ln : 10 Col : 1 Sel : 0 | 0 Windows (CR LF) UTF-8 INS

```
Return-Path: <smithgeorge2323@yahoo.com>

Received-SPF: pass (google.com: domain of smithgeorge2323@yahoo.com designates 106.10.242.139 as
permitted sender) client-ip=106.10.242.139;
```

Analyzing Email Headers (Cont'd)

10 **DomainKeys Identified Mail (DKIM) Signature**

□ It offers a **cryptographic way** of verifying whether a received email has actually originated from the sending domain

Different elements of the DKIM signature

"v=" field stands for the DKIM signature version which should always be set to 1

"a=" field shows the algorithm (sha256) used to generate the signature

"c=" field denotes the canonicalization algorithm used. It shows if there is any modification in the email in terms of whitespace or line-wrapping; the first value before "/" is for the header and the rest is for the body

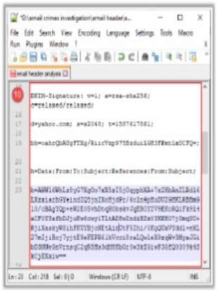
"d=" field refers to the domain of the sender

"s=" field refers to the selector to identify the DNS public key

"t=" field denotes the timestamp of the signature in Unix epoch time and should always match or be close to the time reflected in the Received header and Message ID fields

"bh=" field is the hash for the body as per the hashing algorithm in use and then encoded in Base64

"b=" field includes the DKIM signature that should be calculated as per the header field mentioned in the "h=" field


*D:\email crimes investigation\email header\a...
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
email header analysis
10
Ln : 23 Col : 218 Sel : 0 | 0 Windows (CR LF) UTF-8 INS

```
DKIM-Signature: v=1; a=rsa-sha256;
c=relaxed/relaxed;

d=yahoo.com; s=s2048; t=1587617861;

bh=[illegible];

h=Date:From:To:Subject:References:From:Subject;

b=[illegible]
```

Analyzing Email Headers: Checking Email Authenticity

□ Once the sender's email address has been identified, investigators should check **whether it is valid**

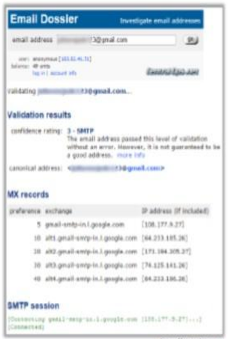
□ Use Email Dossier, a **scanning tool** included in the CentralOps.net suite of online network utilities

□ This tool provides **information** about e-mail address, including the mail exchange records

□ It **initiates SMTP sessions** to check address acceptance, but it never actually sends e-mail

Other tools to check email validity:

- ○ **Email Address Verifier**
  https://tools.verifyemailaddress.io
- ○ **Email Checker**
  https://email-checker.net
- ○ **G-Lock Software Email Verifier**
  https://www.glocksoft.com



email address [redacted]3@gmail.com

user: anonymous [[illegible]]
balance: 49 units

validating [redacted]3@gmail.com...

Validation results

confidence rating: 3 - SMTP
The email address passed this level of validation without an error. However, it is not guaranteed to be a good address. more info

canonical address: <[redacted]3@gmail.com>

MX records

preference	exchange	IP address (if included)
5	gmail-smtp-in.l.google.com	[108.177.9.27]
10	alt1.gmail-smtp-in.l.google.com	[64.233.185.26]
20	alt2.gmail-smtp-in.l.google.com	[173.194.205.27]
30	alt3.gmail-smtp-in.l.google.com	[74.125.141.26]
40	alt4.gmail-smtp-in.l.google.com	[64.233.186.26]

SMTP session

```
[Connecting gmail-smtp-in.l.google.com [108.177.9.27]...]
[Connected]
```

https://centralops.net

Q2.

a. **CRITICALLY EVALUATE THE ROLE OF EMAIL HEADERS IN FORENSIC INVESTIGATIONS. HOW RELIABLE ARE THEY IN TRACING AN EMAIL'S ORIGIN, AND WHAT LIMITATIONS SHOULD INVESTIGATORS CONSIDER?**

- Introduction **to Email Headers in Forensics**

  - **Description:** Email headers contain metadata such as the sender’s and recipient’s addresses, subject line, timestamps, and routing information. These elements are crucial in tracing the email’s origin and evaluating its authenticity.

- Role **of Email Headers in Tracing Email Origin**

  - **Key Points:**
    - **Received Fields:** The “Received” fields in the header show the route an email has taken, from the sender’s server to the recipient's server. Each server the email passes through adds a new “Received” line, allowing investigators to trace the email’s journey.
    - **Sender and Recipient Information:** The "From" and "To" fields reveal the sender's and recipient's email addresses, which are essential for identifying involved parties.
    - **IP Address:** The IP address associated with the email can indicate the physical location of the sender, helping to verify or dispute the sender’s claims about their whereabouts.
  - **Why Important:** These details provide a direct path for tracing the email to its origin and identifying potential tampering or spoofing.

- Reliability **of Email Headers in Tracing Origin**

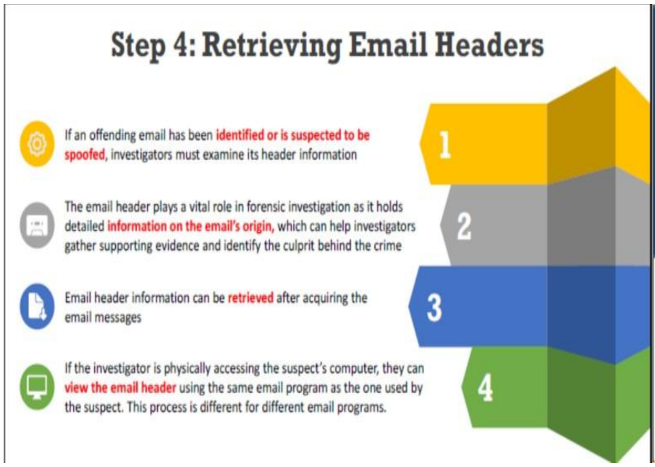
  - **Strengths:**
    - **Direct Evidence:** Headers provide tangible, verifiable information that can be used to trace the email's journey from the sender to the recipient.
    - **Tampering Detection:** Headers allow forensic experts to identify whether an email has been altered or forged, which is key in cases of email spoofing or phishing.
  - **Limitations:**
    - **Spoofing or Forging:** The sender's address and other fields in the header can be easily spoofed, meaning that investigators cannot always trust the "From" address without further verification.
    - **Misleading Routing Information:** Attackers can manipulate the "Received" fields to hide the true origin of the email or obscure its path, especially in cases where the attacker uses compromised servers.
    - **Limited Context:** While headers provide routing information, they do not reveal the content of the email or its intent, which is necessary for a comprehensive analysis.

- Limitations **of Email Header Evidence in Forensics**

- **Lack of Full Context:** Email headers only provide technical data but do not give any insight into the content or the reason behind the email, which is essential for understanding the email's intent.
- **Vulnerability to Manipulation:** The information in email headers can be easily altered by attackers, making it unreliable in some cases. Techniques such as "header spoofing" allow a malicious actor to forge an email header to appear legitimate.
- **Confusion from Multiple Servers:** When emails pass through multiple servers (e.g., in cases of email forwarding or using intermediary services), the headers may become cluttered or misleading, making it harder to trace the true source.

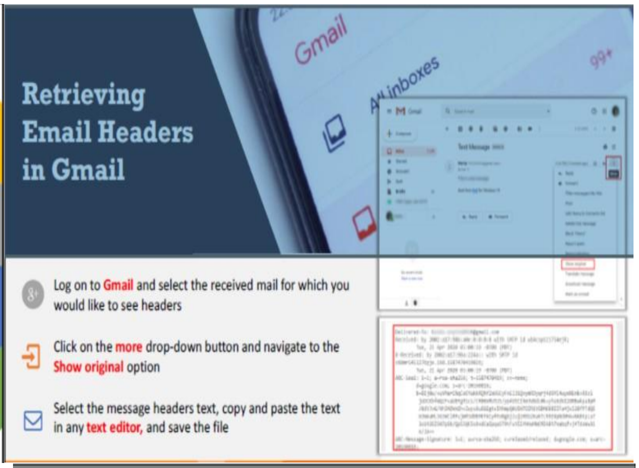
- Conclusion

  - **Overall Assessment:** Email headers are an essential component in forensic investigations, particularly in tracing the origin and route of an email. However, they should be used in conjunction with other evidence, such as IP logs, content analysis, and cross-referencing with other data sources, to ensure accuracy and reliability. Investigators must be cautious of the limitations and potential for manipulation when relying solely on email headers to trace an email's origin.



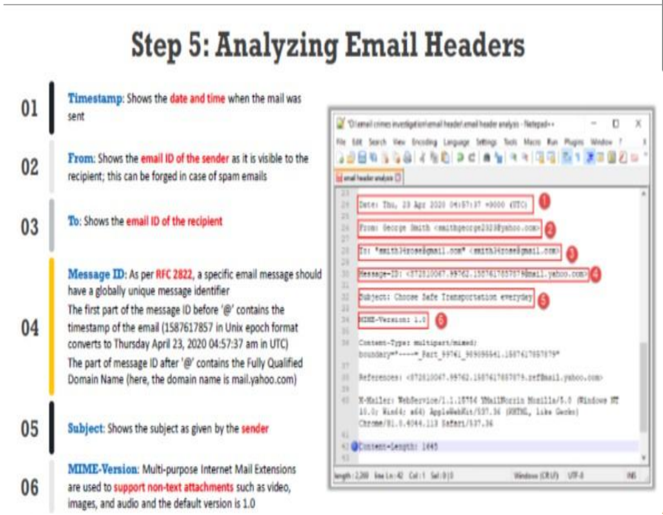
Step 4: Retrieving Email Headers

1. If an offending email has been **identified or is suspected to be spoofed**, investigators must examine its header information
2. The email header plays a vital role in forensic investigation as it holds detailed **information on the email's origin,** which can help investigators gather supporting evidence and identify the culprit behind the crime
3. Email header information can be **retrieved** after acquiring the email messages
4. If the investigator is physically accessing the suspect's computer, they can **view the email header** using the same email program as the one used by the suspect. This process is different for different email programs.



Retrieving Email Headers in Gmail

- Log on to **Gmail** and select the received mail for which you would like to see headers
- Click on the **more** drop-down button and navigate to the **Show original** option
- Select the message headers text, copy and paste the text in any **text editor,** and save the file



Step 5: Analyzing Email Headers

01 **Timestamp:** Shows the **date and time** when the mail was sent

02 **From:** Shows the **email ID of the sender** as it is visible to the recipient; this can be forged in case of spam emails

03 **To:** Shows the **email ID of the recipient**

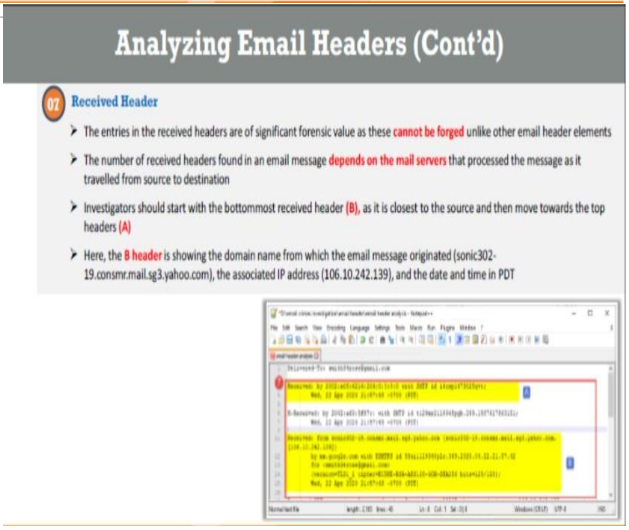
04 **Message ID:** As per **RFC 2822**, a specific email message should have a globally unique message identifier
The first part of the message ID before '@' contains the timestamp of the email (1587617857 in Unix epoch format converts to Thursday April 23, 2020 04:57:37 am in UTC)
The part of message ID after '@' contains the Fully Qualified Domain Name (here, the domain name is mail.yahoo.com)

05 **Subject:** Shows the subject as given by the **sender**

06 **MIME-Version:** Multi-purpose Internet Mail Extensions are used to **support non-text attachments** such as video, images, and audio and the default version is 1.0

```
Date: Thu, 23 Apr 2020 04:57:37 +0000 (UTC)  1
From: George Smith <smithgeorge2323@yahoo.com>  2
To: "smith34rose@gmail.com" <smith34rose@gmail.com>  3
Message-ID: <572810047.99762.1587617857879@mail.yahoo.com>  4
Subject: Choose Safe Transportation everyday  5
MIME-Version: 1.0  6

Content-Type: multipart/mixed;
boundary="----=_Part_99761_969096641.1587617857879"

References: <572810047.99762.1587617857879.ref@mail.yahoo.com>

X-Mailer: WebService/1.1.15756 YMailNorrin Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/81.0.4044.113 Safari/537.36

Content-Length: 1445
```

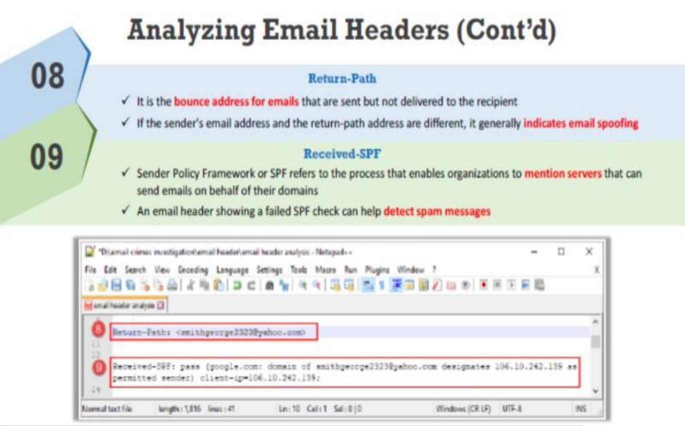
email header analysis - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?



Analyzing Email Headers (Cont'd)

07 **Received Header**

- The entries in the received headers are of significant forensic value as these **cannot be forged** unlike other email header elements
- The number of received headers found in an email message **depends on the mail servers** that processed the message as it travelled from source to destination
- Investigators should start with the bottommost received header **(B),** as it is closest to the source and then move towards the top headers **(A)**
- Here, the **B header** is showing the domain name from which the email message originated (sonic302-19.consmr.mail.sg3.yahoo.com), the associated IP address (106.10.242.139), and the date and time in PDT



Analyzing Email Headers (Cont'd)

Return-Path

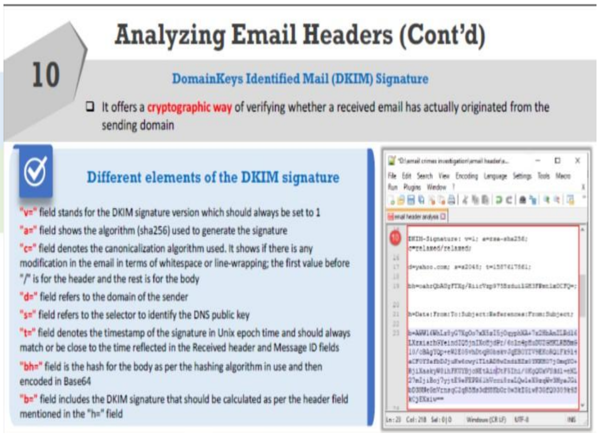
- ✓ It is the bounce address for emails that are sent but not delivered to the recipient
- ✓ If the sender's email address and the return-path address are different, it generally indicates email spoofing

Received-SPF

- ✓ Sender Policy Framework or SPF refers to the process that enables organizations to mention servers that can send emails on behalf of their domains
- ✓ An email header showing a failed SPF check can help detect spam messages

*D:\email crimes investigation\email header\email header analysis - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
email header analysis
8
9
Normal text file length : 1,816 lines : 41 Ln : 10 Col : 1 Sel : 0 | 0 Windows (CR LF) UTF-8 INS

```
Return-Path: <smithgeorge2323@yahoo.com>

Received-SPF: pass (google.com: domain of smithgeorge2323@yahoo.com designates 106.10.242.139 as
permitted sender) client-ip=106.10.242.139;
```



Analyzing Email Headers (Cont'd)

DomainKeys Identified Mail (DKIM) Signature

- □ It offers a cryptographic way of verifying whether a received email has actually originated from the sending domain

Different elements of the DKIM signature

"v=" field stands for the DKIM signature version which should always be set to 1

"a=" field shows the algorithm (sha256) used to generate the signature

"c=" field denotes the canonicalization algorithm used. It shows if there is any modification in the email in terms of whitespace or line-wrapping; the first value before "/" is for the header and the rest is for the body

"d=" field refers to the domain of the sender

"s=" field refers to the selector to identify the DNS public key

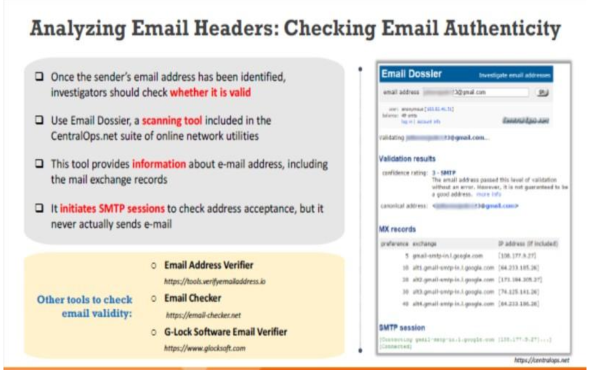
"t=" field denotes the timestamp of the signature in Unix epoch time and should always match or be close to the time reflected in the Received header and Message ID fields

"bh=" field is the hash for the body as per the hashing algorithm in use and then encoded in Base64

"b=" field includes the DKIM signature that should be calculated as per the header field mentioned in the "h=" field

*D:\email crimes investigation\email header\a...
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
email header analysis
10
Ln : 23 Col : 218 Sel : 0 | 0 Windows (CR LF) UTF-8 INS

```
DKIM-Signature: v=1; a=rsa-sha256;
c=relaxed/relaxed;

d=yahoo.com; s=s2048; t=1587617561;

bh=oahrQbA0gFTXq/[illegible]

h=Date:From:To:Subject:References:From:Subject;

b=[illegible]
```



Analyzing Email Headers: Checking Email Authenticity

- □ Once the sender's email address has been identified, investigators should check whether it is valid
- □ Use Email Dossier, a scanning tool included in the CentralOps.net suite of online network utilities
- □ This tool provides information about e-mail address, including the mail exchange records
- □ It initiates SMTP sessions to check address acceptance, but it never actually sends e-mail

Other tools to check email validity:

- ○ Email Address Verifier
  https://tools.verifyemailaddress.io
- ○ Email Checker
  https://email-checker.net
- ○ G-Lock Software Email Verifier
  https://www.glocksoft.com

validating [redacted]3@gmail.com...

Validation results

confidence rating: 3 - SMTP
The email address passed this level of validation without an error. However, it is not guaranteed to be a good address. more info

canonical address: <[redacted]3@gmail.com>

MX records

```
preference  exchange                           IP address (if included)
5           gmail-smtp-in.l.google.com         [108.177.9.27]
10          alt1.gmail-smtp-in.l.google.com    [64.233.185.26]
20          alt2.gmail-smtp-in.l.google.com    [173.194.205.27]
30          alt3.gmail-smtp-in.l.google.com    [74.125.141.26]
40          alt4.gmail-smtp-in.l.google.com    [64.233.186.26]
```

SMTP session

```
[Connecting gmail-smtp-in.l.google.com [108.177.9.27]...]
[Connected]
```

https://centralops.net

B. EXAMINE MICROSOFT EMAIL SERVER LOGS.

ANS: Examining Microsoft Email Server Logs

1. **Locate or Access Logs**:
   - For Exchange Server: Found under `C:\Program Files\Microsoft\Exchange Server\V15\Logging`.
   - For Microsoft 365: Access via Security & Compliance Centre or PowerShell.
2. **Open Logs**:
   - Use a text editor (Notepad/Notepad++) or PowerShell for analysis.
3. **Key Events**:
   - **Authentication Issues**: Failed/unusual logins.
   - **Message Delivery Failures**: Errors like "550 5.1.1".
   - **Server Errors**: Resource issues or crashes.
4. **Analyse Timestamps**:
   - Check for recurring patterns or unusual activity indicating issues or breaches.
5. **Event Codes**:
   - **1000**: General errors (e.g., crashes).
   - **1033**: Mail routing issues.
   - **12014**: SSL certificate problems.
6. **Correlate Logs**:
   - Cross-reference with system, firewall, or antivirus logs for a comprehensive analysis.

Q3.

A. DISCUSS THE FUNCTIONALITIES OF VARIOUS TYPES OF EMAIL SERVERS AND EMAIL CLIENTS.

Email Servers:

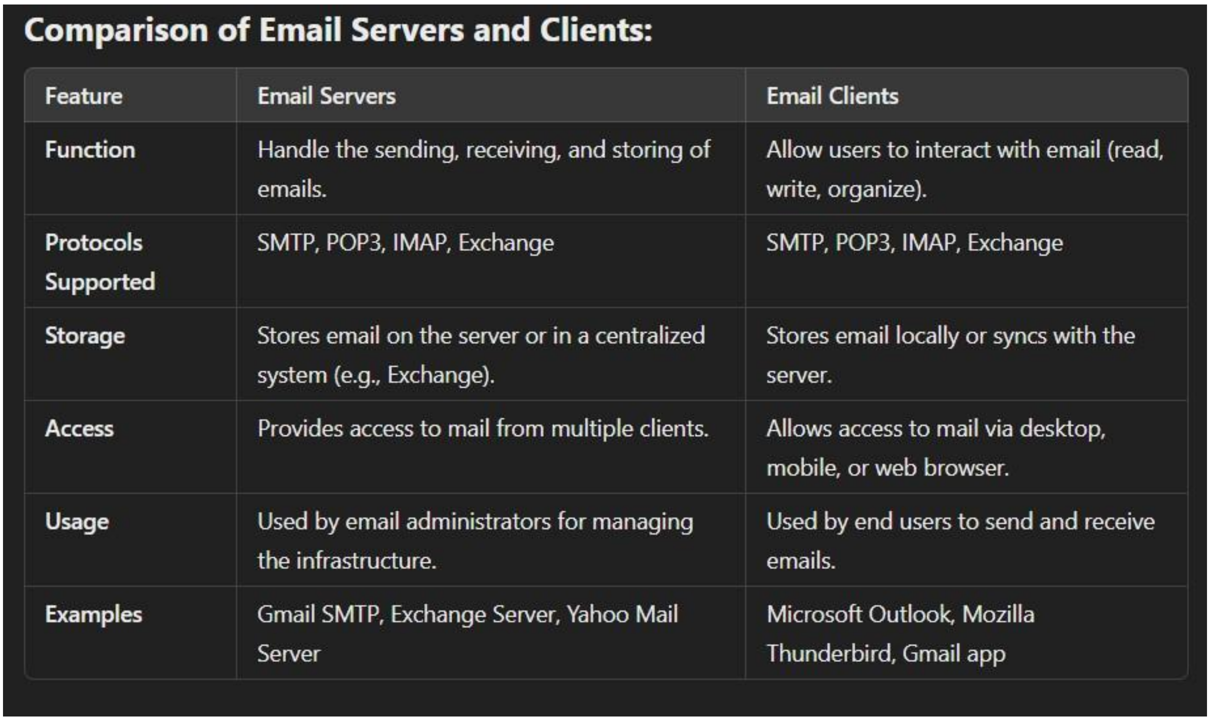
1. **SMTP Server (Simple Mail Transfer Protocol)**:
   - **Function**: Sends and routes outgoing emails to other servers or clients.
   - **Role**: Handles only outgoing mail.
   - **Example**: `smtp.gmail.com` for Gmail.
2. **POP3 Server (Post Office Protocol v3)**:
   - **Function**: Downloads emails from the server to the user's device and removes them from the server.
   - **Role**: Ideal for offline access; emails are stored locally.
   - **Example**: `pop.gmail.com` for Gmail.
3. **IMAP Server (Internet Message Access Protocol)**:
   - **Function**: Enables viewing and managing emails directly on the server without downloading them.
   - **Role**: Supports synchronization across devices, reflecting actions (read, delete, move) everywhere.
   - **Example**: `imap.gmail.com` for Gmail.
4. **Exchange Server**:
   - **Function**: Manages emails, calendars, contacts, and tasks, primarily for enterprise use.
   - **Role**: Provides advanced collaboration features like shared mailboxes and calendar integration with Microsoft services.
   - **Example**: Microsoft Exchange.
5. **Webmail Server**:
   - **Function**: Allows email access through web browsers.
   - **Role**: Platform-independent, requiring no dedicated client installation.
   - **Example**: Gmail, Yahoo Mail, Outlook.com.

Email Clients:

1. **Desktop Clients**:
   - **Function**: Installed on PCs to manage emails.
   - **Example**: Microsoft Outlook, Mozilla Thunderbird.
2. **Mobile Clients**:
   - **Function**: Apps on smartphones/tablets for email access on the go.
   - **Example**: Gmail app, Apple Mail.
3. **Webmail Clients**:
   - **Function**: Browser-based email access from any internet-connected device.
   - **Example**: Gmail.com, Outlook.com.
4. **Unified Messaging Clients**:
   - **Function**: Integrate email, voice, and SMS in one platform.
   - **Example**: Microsoft Outlook with Exchange Server.

Conclusion:

Email servers manage routing, delivery, and storage (SMTP for sending, POP3/IMAP for retrieval and storage, Exchange for enterprise features, and webmail for browser access). Email clients (desktop, mobile, web-based, or unified) facilitate user interaction across devices, ensuring seamless communication and management.



Comparison of Email Servers and Clients:

Feature	Email Servers	Email Clients
Function	Handle the sending, receiving, and storing of emails.	Allow users to interact with email (read, write, organize).
Protocols Supported	SMTP, POP3, IMAP, Exchange	SMTP, POP3, IMAP, Exchange
Storage	Stores email on the server or in a centralized system (e.g., Exchange).	Stores email locally or syncs with the server.
Access	Provides access to mail from multiple clients.	Allows access to mail via desktop, mobile, or web browser.
Usage	Used by email administrators for managing the infrastructure.	Used by end users to send and receive emails.
Examples	Gmail SMTP, Exchange Server, Yahoo Mail Server	Microsoft Outlook, Mozilla Thunderbird, Gmail app

---

B. DESCRIBE THE SMTP PROTOCOL AND ITS IMPORTANCE IN EMAIL COMMUNICATION. HOW DOES SMTP FACILITATE THE SENDING AND RECEIVING OF EMAILS ACROSS DIFFERENT DOMAINS?

SMTP Protocol Overview:

SMTP (Simple Mail Transfer Protocol) is a standard communication protocol for sending, relaying, and transferring emails between servers. It converts email messages into a standard ASCII format and routes them to the recipient's mail server.

Importance in Email Communication:

1. **Reliable Delivery**: SMTP ensures emails are transmitted accurately and efficiently between servers across networks.

2. **Standardization**: It provides a standardized approach to email delivery, ensuring compatibility across platforms.
3. **Error Feedback**: Sends delivery failure notifications (e.g., invalid recipient or server issues), enabling troubleshooting.
4. **Core Email Backbone**: Without SMTP, email transmission across domains would not be possible.

How SMTP Facilitates Email Communication Across Domains:

1. **SMTP Server Setup**:
   - Clients (e.g., Outlook, Gmail) use a specific SMTP server (e.g., `smtp.gmail.com`) for outgoing emails.
   - This setup directs emails to the appropriate mail server.
2. **Email Transmission**:
   - When a user sends an email, the client forwards it to the SMTP server.
   - The SMTP server identifies the recipient's domain (e.g., `@yahoo.com`) and routes the email accordingly.
3. **Relaying Across Servers**:
   - Emails sent across domains pass through multiple SMTP servers.
   - These servers use DNS "MX" (Mail Exchange) records to locate the recipient’s mail server.
4. **Handling Failures**:
   - If delivery fails, the server generates a bounce-back message with details (e.g., invalid address or server issues), helping the sender resolve the problem.

SMTP Headers and Their Importance:

1. **Purpose of Headers**:
   - Contain metadata such as sender and recipient addresses, IP addresses, timestamps, and routing details.
   - Vital for email management and tracing its journey.
2. **Email Forging**:
   - Attackers manipulate headers to disguise the sender’s identity, often for phishing or spam.
   - Forged emails exploit open SMTP relays, which don’t require authentication.
3. **Open Relays**:
   - Servers that allow unrestricted email sending.
   - Often abused by spammers to send mass unsolicited emails with forged headers.

SMTP's Role in Email Security:

1. **Header Analysis**:
   - Helps trace email origins and verify authenticity.
   - Crucial for detecting anomalies like forged emails or phishing attempts.
2. **Spoofing Detection**:
   - Examines the "From" field and other header details to uncover manipulated sender addresses.
   - Mitigates phishing attacks by identifying deceitful messages.
3. **Spam Filtering**:

    - Tools like Spam Assassin analyse headers to flag spam based on IP, domain, and content.
    - Ensures cleaner inboxes by filtering out unwanted messages.
4. **Delay Tracking**:
    - Timestamps in headers identify transmission delays between servers.
    - Assists in troubleshooting delivery issues.

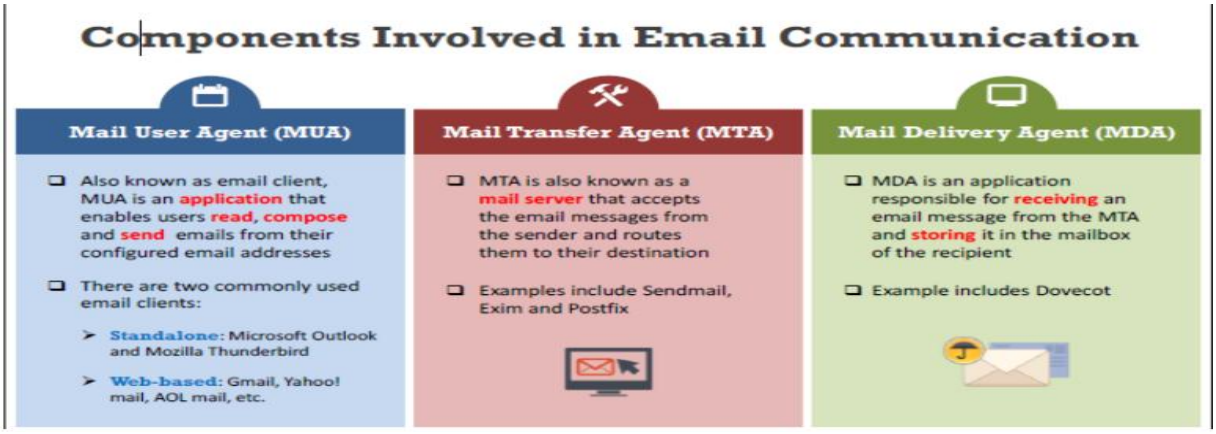
Conclusion:

SMTP is the backbone of email communication, facilitating reliable message transmission across domains. It standardizes email delivery, provides failure notifications, and enhances security by enabling header analysis to detect forging, spoofing, and spam.

Q4.

A. DISCUSS THE IMPORTANCE OF THE THREE COMPONENTS INVOLVED IN EMAIL COMMUNICATION.

1. **Mail User Agent (MUA):**
    - **Role:** MUA is the email client (e.g., Outlook, Gmail) used by the sender and receiver to compose, send, and access emails.
    - **Importance:** Facilitates user interaction with the email system, ensuring that emails can be created, sent, and retrieved easily.
2. **Mail Transfer Agent (MTA):**
    - **Role:** The MTA is responsible for routing and delivering emails from the sender's server to the recipient's server using protocols like SMTP.
    - **Importance:** Acts as the backbone for email transmission, handling routing, queuing, and error reporting during the delivery process.
3. **Mail Delivery Agent (MDA):**
    - **Role:** The MDA receives emails from the MTA and delivers them to the recipient's mailbox.
    - **Importance:** Ensures that emails are stored correctly in the recipient's mail account, enabling retrieval by the MUA.



Components Involved in Email Communication

Mail User Agent (MUA)

❑ Also known as email client, MUA is an application that enables users read, compose and send emails from their configured email addresses

❑ There are two commonly used email clients:

➤ Standalone: Microsoft Outlook and Mozilla Thunderbird

➤ Web-based: Gmail, Yahoo! mail, AOL mail, etc.

Mail Transfer Agent (MTA)

❑ MTA is also known as a mail server that accepts the email messages from the sender and routes them to their destination

❑ Examples include Sendmail, Exim and Postfix

Mail Delivery Agent (MDA)

❑ MDA is an application responsible for receiving an email message from the MTA and storing it in the mailbox of the recipient

❑ Example includes Dovecot

B. CREATE A STEP-BY-STEP METHODOLOGY FOR ANALYSING A SUSPICIOUS EMAIL, FROM EXAMINING HEADERS TO VERIFYING THE SENDER'S IDENTITY USING SPF, DMARC, AND DKIM.

- Examine **the Email Header:**

  - View the header to trace the email's origin, check the sender's IP address, and review timestamps for anomalies.

- Analyse **the "From" and "Reply-To" Fields:**

  - Verify if the sender's email address matches the domain and looks legitimate.

- Check **for Suspicious Links and Attachments:**

  - Hover over links without clicking to inspect the actual URL. Avoid opening unknown attachments.

- Verify **Sender Identity Using SPF, DKIM, and DMARC:**

  - **SPF (Sender Policy Framework):** Confirms that the email comes from an authorized server for the sender's domain.
  - **DKIM (DomainKeys Identified Mail):** Validates that the email has not been altered during transit using a cryptographic signature.
  - **DMARC (Domain-based Message Authentication, Reporting, and Conformance):** Provides domain-level protection by ensuring alignment between "From" and authenticated domains.

- Scan **for Malware:**

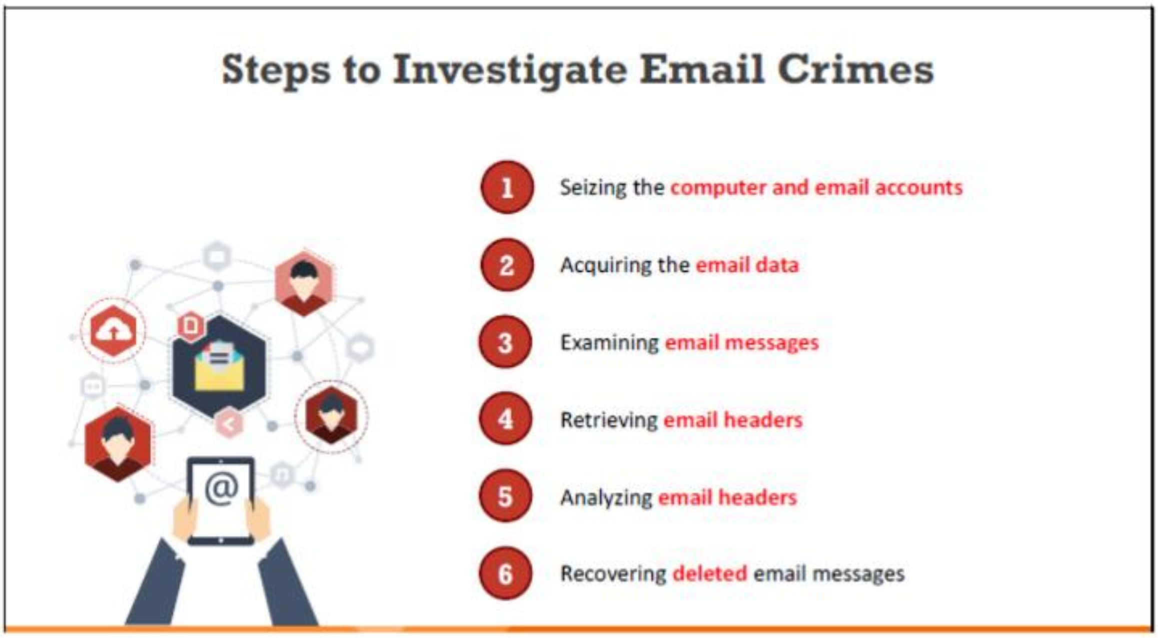
  - Use antivirus tools to scan attachments and links for potential malware.

- Analyse **Language and Content:**

  - Look for poor grammar, urgent language, or requests for sensitive information.

- Cross-**Check with the Sender:**

  - If in doubt, contact the sender through an alternate, verified channel to confirm authenticity.



Steps to Investigate Email Crimes

1 Seizing the computer and email accounts

2 Acquiring the email data

3 Examining email messages

4 Retrieving email headers

5 Analyzing email headers

6 Recovering deleted email messages

Q5.

A. REPORT THE VARIOUS SECURITY THREATS ASSOCIATED WITH THE INFRASTRUCTURE OF AN EMAIL.

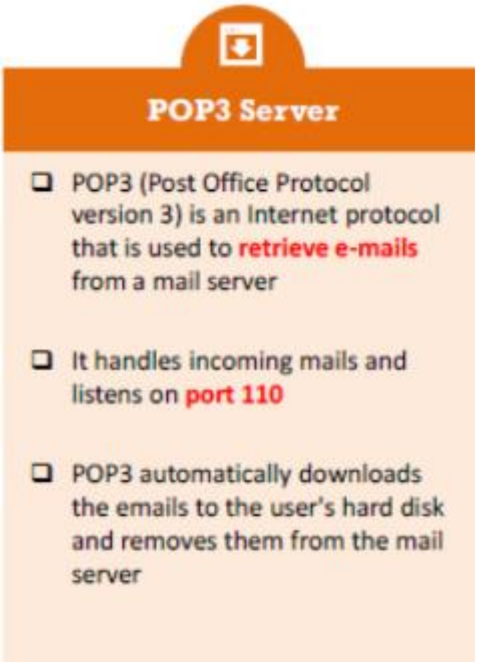
Security Threats Associated with Email Infrastructure

1. **Phishing Attacks:**
   - Cybercriminals use deceptive emails to trick users into revealing sensitive information like passwords or financial details.
2. **Malware and Ransomware:**
   - Emails with malicious attachments or links can deliver malware or ransomware to compromise systems.
3. **Spoofing and Identity Theft:**
   - Attackers forge sender addresses to impersonate trusted entities, often to commit fraud.
4. **Spam:**
   - Unsolicited emails can clog inboxes, consume resources, and potentially carry malicious content.
5. **Man-in-the-Middle Attacks:**
   - Interception of email traffic can expose sensitive data or allow attackers to inject malicious content.
6. **Open Relays Exploitation:**
   - Misconfigured servers can be exploited to send spam or forged emails.
7. **Insufficient Authentication:**
   - Lack of proper SPF, DKIM, or DMARC policies increases vulnerability to spoofing and unauthorized access.

B. ILLUSTRATE THE WORKING OF POP3 IN ESTABLISHING COMMUNICATION BETWEEN MAIL SERVER AND MAIL CLIENT.

1. **Client Connection:**
   - The email client establishes a connection to the POP3 server using credentials.
2. **Authentication:**
   - The user logs into the server with a username and password to access their mailbox.
3. **Retrieval of Emails:**
   - Emails are downloaded from the server to the client's local device. By default, emails are removed from the server after download.
4. **Disconnection:**
   - The client closes the connection to the POP3 server after retrieving emails.
5. **Local Storage and Access:**
   - Emails are stored locally, enabling offline access and management.

Note: POP3 is suited for single-device access, as downloaded emails are no longer available on the server unless specifically configured otherwise.



POP3 Server

❑ POP3 (Post Office Protocol version 3) is an Internet protocol that is used to **retrieve e-mails** from a mail server

❑ It handles incoming mails and listens on **port 110**

❑ POP3 automatically downloads the emails to the user's hard disk and removes them from the mail server

---

Q6.

A. DESCRIBE THE WORKING PRINCIPLE OF CLUTTER FILTERING.

Clutter Filtering

Clutter filtering helps discover and remove unusable or random files. It needs to be explicitly enabled under the **"Deleted data only"** settings, as it is turned off by default when the program is first installed. This setup filters out all duplicate or incomplete records.

How It Works:

- Each processed table in the database is defined as a set of columns.
- Each recovered record is compared (based on the defined set of columns) with:
    1. All valid records.
    2. All previously recovered records.
- Records identified as duplicates are discarded.

B. SUMMARIZE THE ACQUISITION AND ANALYSIS PHASES OF ANDROID DEVICE FORENSICS.

Introduction: Android forensics follows a structured process of acquiring, extracting, and analysing data from Android devices. The process is influenced by the device's access level (rooted or non-rooted), with rooted devices offering complete data access and non-rooted devices providing limited access. Root access allows more detailed extraction, including system-level data, while non-rooted access typically focuses on logical data.

1. Acquisition Phase:
a. Device Security and Android Version:

- **Pattern Locks, Password Locks, and Fingerprints:**
    - Bypassed with root access and USB debugging enabled.
    - Passwords are stored securely, requiring root access for full retrieval.
    - Fingerprint or Bluetooth unlocks still require a backup password in some cases.
- **Android Version Impact:**
    - Newer Android versions often have enhanced security, making forensic acquisition more challenging and limiting access to data.

b. Device Accessibility:

- **Non-rooted Devices:**
    - Only logical data such as contacts, messages, and photos are accessible.
    - System partitions and deleted data cannot be extracted without rooting.
- **Rooted Devices:**
    - Provides full administrative access, including system partitions and deleted data recovery.
    - Enables complete acquisition and more extensive analysis of the device.

c. Connection Medium:

- **USB Debugging:**
    - Essential for connecting the device to a forensic workstation.
- **USB Cable:**
    - The most secure and reliable method for data extraction.
- **Wireless Methods (Bluetooth/Wi-Fi):**
    - Less secure, more prone to interference, and require both devices to be on the same network.

d. Device Acquisition Techniques:

- **USB Connectivity:**
    - The safest and most reliable method for data acquisition.
- **Forensic Tools:**

    - Tools like Cellebrite, Oxygen Forensics, and Magnet AXIOM help in acquiring data from both rooted and non-rooted devices.
    - **Rooted Devices:** Full device image and system partition recovery.
    - **Non-rooted Devices:** Only logical data can be extracted.

2. Analysis Phase:
a. Data Preservation and Extraction:

- **Imaging:**
    - A bit-for-bit copy of the device's data is made to ensure evidence integrity.
- **Write Blockers:**
    - Used to prevent data modification during transfer, ensuring original evidence is preserved.
- **Forensic Utilities:**
    - Automated tools assist in the extraction and preservation process, especially for rooted devices.

b. Data Examination and Review:

- **Communication Data:**
    - Call logs, messages, and contacts are essential for analysis.
- **App Data:**
    - App data, including social media messages and app-specific files, is reviewed for evidence.
- **System Files:**
    - Root access allows in-depth analysis of system files, hidden files, and ROM data.
- **Deleted Data Recovery:**
    - Rooted devices enable data carving techniques to recover deleted files, providing critical evidence.

c. Evidence Identification:

- **Geolocation Data:**
    - GPS data and other app data can provide valuable location information.
- **Communication Logs:**
    - SMS, call history, and social media messages are key to investigation.
- **Photos, Files, and Documents:**
    - Multimedia files provide crucial case evidence.
- **Carving Deleted Files:**
    - Data carving techniques can recover deleted files, which may contain important evidence that was intentionally erased.

Conclusion:
The success of Android device forensics depends on the access level—rooted devices offer extensive data recovery, while non-rooted devices limit access to logical data. Forensic investigators use specialized tools, write blockers, and thorough protocols to ensure data integrity and accurate evidence recovery. Both acquisition and analysis are critical phases that allow investigators to gather reliable evidence for legal proceedings.
4o mini

Q7.

A. EMPLOY CFTT AND JTAG IN COMPUTER FORENSICS WITH A CLEAR EXPLANATION.

JTAG (Joint Test Action Group)

What is JTAG?

- JTAG is a standard method used to test and access circuits on printed circuit boards (PCBs).
- It allows direct communication with internal components like processors and memory chips.

How JTAG Works in Forensics:

- **Non-Destructive:** JTAG allows data extraction without damaging the device.
- **Bypasses Security:** It can access data even when the device is locked or USB debugging is disabled.
- **Data Extraction:** JTAG retrieves raw memory data, though encrypted data will remain encrypted.
- **Mobile Devices:** It is useful for extracting data from locked Android devices or devices with disabled USB ports.
- **Invasive:** It often requires disassembling the device to access the JTAG ports on the PCB.

JTAG Advantages:

- **Byte-for-Byte Data:** Extracts all data from memory without altering it.
- **No Special Cables:** JTAG works without needing specific cables for each device type.
- **Recovers PINs/Passcodes:** JTAG can recover passwords, PIN codes, or swipe patterns.
- **Useful for Damaged Devices:** It works on devices damaged by liquid, heat, or structural issues.

JTAG Process:

1. Disassemble the device to access the JTAG ports.
2. Connect the device to a JTAG hardware interface.
3. Power on the device and establish a connection.
4. Extract memory and create a binary image.
5. Import the image into an analysis tool for further review.

CFTT (Computer Forensic Tool Testing)

What is CFTT?

- CFTT is a program by NIST that validates forensic tools used in investigations.
- It ensures that forensic tools provide accurate and reliable results.

CFTT Benefits:

- **Validates Tools:** Ensures that forensic tools used in investigations give correct results.
- **Helps Investigators Choose Tools:** Provides reliable information to help investigators select the best tools.
- **Improves Tools:** Provides feedback to developers for tool improvement.
- **Quality Control:** Ensures that forensic tools meet industry standards and are of high quality.

Challenges in Mobile Device Forensics:

- **Multiple Interfaces:** Different devices may require different connection methods.
- **Device Security:** Newer devices often have better security, making data access harder.
- **Physical Damage:** Devices damaged by liquid, heat, or physical impact can complicate data extraction.

Data Extraction Levels:

- **Level 1:** Manual Extraction (simple data retrieval).
- **Level 2-3:** Logical and Physical Extraction (advanced extraction methods).
- **Level 4-5:** JTAG and Chip-Off (used for extracting data from damaged or locked devices).

Conclusion:

- **JTAG** is a powerful tool for accessing data from locked or damaged devices, allowing forensic experts to extract data without causing damage.
- **CFTT** ensures the reliability and accuracy of forensic tools, helping investigators choose the best tools and maintain high-quality standards.

B. PREPARE A SUITABLE REPORT ON THE VARIOUS PARAMETERS INVOLVED IN NON-TRADITIONAL AND OLDER DEVICE ACQUISITION.

In digital forensics, non-traditional and older device acquisition methods are employed when standard techniques fail, especially when devices are locked, damaged, or outdated. These methods offer alternatives to access data from devices that conventional forensic techniques cannot reach. This report outlines various methods and parameters involved in acquiring data from such devices.

Non-Traditional Device Acquisition Methods:
1. JTAG (Joint Test Action Group)

- **Purpose:** JTAG provides direct access to device components through Test Access Ports (TAPs), enabling data acquisition from devices that traditional methods cannot access.
- **Key Points:**
  - **Non-Destructive:** JTAG allows byte-for-byte memory extraction without damaging the device.
  - **Bypass Locked Ports:** It can bypass locked USB ports and extract data from locked or physically damaged devices.
  - **Device Disassembly:** The device must be disassembled to access the JTAG TAPs, requiring technical expertise.
  - **Application:** JTAG is particularly useful when the device's operating system is unresponsive or when the device is too damaged for normal access.

2. Chip-Off Acquisition

- **Purpose:** This method involves physically removing the memory chip from the device to extract data directly from the chip.
- **Key Points:**
  - **Destructive:** The process is invasive and requires significant technical skill to ensure proper extraction.
  - **Severely Damaged Devices:** Used primarily for devices that are physically damaged (e.g., burned or broken smartphones) or non-functional.
  - **Data Extraction:** Even if the device is non-functional, data stored on the memory chip can still be retrieved.
  - **Expertise Required:** Specialized equipment is needed to solder and read the memory chip, requiring an experienced technician.

Older Device Acquisition Methods:

1. Logical Extraction

- **Purpose:** Logical extraction retrieves accessible data from devices without needing physical access to the device's storage hardware.
- **Key Points:**
  - **Suitable for Older Devices:** Logical extraction is effective with older devices that do not have complex encryption or security features.
  - **Data Access:** Retrieves accessible files like contacts, text messages, photos, and documents.
  - **Limitations:** Cannot recover deleted, hidden, or encrypted data; restricted to the files the system can expose via standard access methods.

2. Physical Extraction

- **Purpose:** Physical extraction involves copying the entire memory content of the device, including deleted data and hidden files.
- **Key Points:**
  - **Data Dump:** Provides a complete data dump, including data not normally accessible through logical extraction.
  - **Effective for Older Devices:** Most effective on older devices that lack encryption or complex file systems.
  - **Data Recovery:** Allows recovery of deleted files and system files that may contain valuable forensic evidence.

3. Manual Extraction

- **Purpose:** Manual extraction involves directly accessing the device and copying data manually.
- **Key Points:**

    - **Basic File Transfers:** Limited to simple file transfers such as copying pictures, contacts, and documents from older, non-smart devices.
    - **No Data Recovery:** Does not recover deleted or hidden files, making it less effective for in-depth forensic investigations.

Challenges:
1. Technical Expertise
Non-traditional methods, such as JTAG and Chip-Off, require specialized knowledge and skills to execute properly, including the ability to disassemble devices, solder chips, and use specialized equipment.
2. Device Damage
Invasive methods like Chip-Off may cause physical damage to the device, complicating data recovery or rendering it impossible. It is crucial to minimize the risk of damage to hardware during extraction.
3. Data Integrity
Ensuring data integrity during extraction is essential in forensic investigations. The device must be handled carefully, and write-blockers or other tools should be used to prevent any modification of the original data.
4. Legal Considerations
Non-traditional methods must follow strict legal protocols to ensure the admissibility of the data in court. Proper documentation of the extraction process, chain of custody, and forensic procedures is crucial to maintaining the legal validity of the evidence.

Q8.

A. IDENTIFY THE NECESSITY OF SECURITY IN MOBILE APPLICATIONS.

Necessity of Security in Mobile Applications:

- Mobile app security focuses on the software security of apps on platforms like Android, iOS, and Windows Phone.
- Covers apps on both mobile phones and tablets.
- Involves assessing apps for security issues based on:
    - The platform they run on.
    - The frameworks used for development.
    - The anticipated users (e.g., employees or general users).
- Mobile apps are crucial for business online presence, helping businesses connect with global users.
- Many businesses depend entirely on mobile apps for user interaction.

What is Mobile Application Security?

- More users are relying on mobile apps for digital tasks instead of desktop applications.
- Popular mobile platforms offer security controls for developers, but it’s up to developers to choose and implement them properly.
- If security features aren’t properly implemented, attackers may easily bypass them.
- Common issues in mobile apps include:

    - Storing or leaking sensitive data accessible by other apps on the phone.
    - Weak authentication and authorization check that can be bypassed.
    - Use of weak encryption methods that can be easily broken.
    - Sending sensitive data over the Internet without encryption.
- These issues can be exploited by malicious apps or attackers on the same Wi-Fi network.

What is Mobile Application Security Testing?

- Security testing involves evaluating the app's security by simulating attacks from a malicious user.
- Effective testing starts with understanding the app's business purpose and the data it handles.
- The testing process involves:
    - Interacting with the app to understand how it stores, receives, and transmits data.
    - Decrypting encrypted parts of the app.
    - Decompiling the app's code for analysis.
    - Using static analysis to identify security weaknesses in the decompiled code.
    - Using reverse engineering and static analysis to drive dynamic analysis and penetration testing.
    - Evaluating the effectiveness of security controls (like authentication and authorization).

Mobile Application Security Testing Tools:

- Various free and commercial security tools are available for testing mobile apps.
- Some tools use static or dynamic testing methods but no single tool covers all vulnerabilities.
- A combination of static and dynamic testing, along with manual review, provides the best assessment.
- Security testing serves as a pre-production check to ensure security controls work properly.
- It helps identify edge cases that could lead to security issues not anticipated by the development team.

B. SUMMARIZE THE WORKING PRINCIPLE OF VARIOUS OPEN-SOURCE MOBILE FORENSICS TOOLS.

□ **Santoku (current version 0.5):**

- Free and open-source bootable Linux distro based on Lubuntu.
- Preinstalled apps for mobile forensics, mobile malware analysis, and mobile app security assessment.

□ Kali **Linux:**

- Free solution for advanced penetration testing.
- Based on Debian Linux.
- Hosts several toolkits, scripts, and frameworks for security penetration testing and digital forensics.

 The **SANS Investigative Forensic Toolkit (SIFT) (current version 3.0):**

- Comprehensive workstation for digital forensics investigation using open-source tools.
- Based on Ubuntu LTS 16.04, can be installed on Windows 10.
- Not specifically designed for mobile forensics, but can be used for general digital forensics and in education/training.

 The **Digital Evidence & Forensics Toolkit (DEFT):**

- Live GNU Linux distribution for Digital Forensics and Incident Response (DFIR).
- Includes tools for mobile forensics, malware analysis, devices imaging, network forensics, OSINT, artefacts extraction, data recovery, passwords extraction, and more.

 The **Computer Aided Investigative Environment (CAIN):**

- Live GNU Linux distribution for digital forensics investigations.
- Includes tools for memory, network, mobile, and disk forensics, as well as malware analysis.
- Includes Live Windows forensics tools like Nirsoft tools and FTK Imager.

 The **Sleuth Kit (TSK):**

- Framework for digital forensics, with several command-line tools and libraries.
- Works on Linux-based and Windows systems.
- Android device physical images can be analysed using the Android Analyzer module.

 Autopsy**:**

- GUI interface for The Sleuth Kit (TSK).
- Supports both Linux-based and Windows systems.

 Linux **Memory Extractor (LiME):**

- Free and open-source Loadable Kernel Module (LKM) to capture full RAM images from Linux-based systems (e.g., Android devices).
- Captured memory images can be saved directly to the device or over the network.

Q9.

A. REVIEW THE VARIOUS COMPONENTS OF THE GSM CELLULAR NETWORK WITH A SUITABLE ARCHITECTURE DIAGRAM.

ANS:

Cellular Network Architecture

Cellular networks provide mobile communication services over large areas, ensuring connectivity and scalability through various subsystems.

1. Mobile Station (MS)

Represents the user side, enabling access to network services.

- **Components**:
  - **Mobile Equipment (ME)**: Devices like phones and tablets.
  - **SIM/UICC/USIM**: Stores subscriber info, enhances security, and supports multi-apps.

- **Role**: Connects to the network for communication, sending/receiving calls, SMS, and internet.

2. Access Network (AN)

Links the Mobile Station to the Core Network over the air interface.

- **Components**:
  - **BTS**: Antennas and transceivers managing individual cells.
  - **BSC**: Manages BTS, allocates resources, and handles handovers.
- **Role**: Ensures seamless connectivity as users move between cells.

3. Core Network (CN)

The backbone for subscriber management, call routing, and external connectivity.

- **Subsystems**:
  - **NSS**: Includes MSC (call routing), HLR/VLR (subscriber data), AuC (authentication), and EIR (device tracking).
  - **SMSC**: Handles SMS delivery.
- **Role**: Provides voice, data, roaming, SMS, and secure authentication.

4. External Network

Facilitates global connectivity by interfacing with external systems.

- **Components**: PSTN (landlines) and the Internet.
- **Role**: Connects cellular and external communication systems.

Unique Identifiers

- **MSISDN**: User’s phone number.
- **IMSI**: Unique subscriber ID.
- **IMEI**: Device identifier, tracks status (e.g., stolen).
- **ICCID**: SIM card identifier.

Cellular Network Technologies

1. **1G (Analogue, 1970s-1980s)**: Basic voice calls, bulky devices, no data.
2. **2G (Digital, 1990s)**: Enabled GSM (voice, SMS) and CDMA (efficient spectrum use). Introduced SMS, MMS, caller ID, and basic internet.
3. **3G (High-Speed Internet)**: UMTS-based, faster internet for browsing, streaming, and apps.
4. **4G (LTE)**: Faster speeds, HD streaming, online gaming, VoIP, IoT devices.
5. **5G (Next-Gen)**: Ultra-low latency, speeds up to 20 Gbps, IoT-ready, D2D communication.

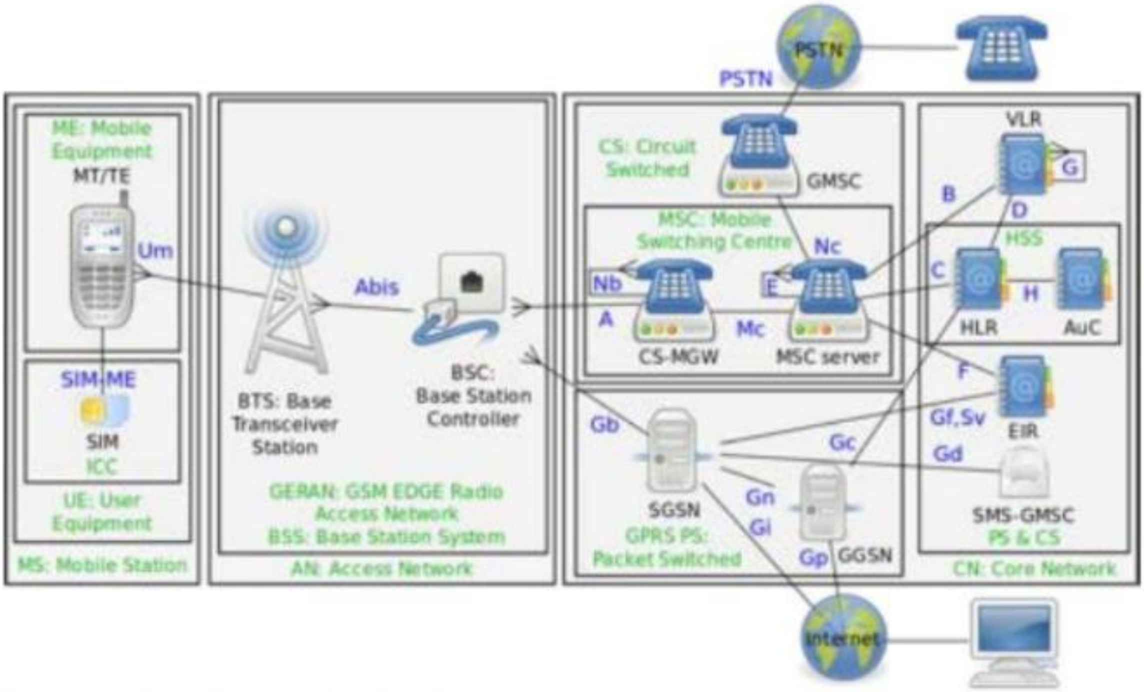


Figure 3. Architecture of the GSM Cellular Network.