Answers **(5)**	Coding Efficiency **(5)**	Viva **(5)**	Timely Completion **(5)**	Total **(20)**	Dated Sign of Subject Teacher

Expected Date of Completion:----------

Actual Date of Completion:----------

Experiment No: Group A-1

Problem Definition:

Write a program for Tracking Emails and Investigating Email Crimes. i.e. Write a program to analyze e–mail header

1.1 Prerequisite:

Application Layer Protocols

1.2 Learning Objective:

1. To understand how Mails are transferred from Sender to Receiver.
2. To Understand Email related Parameter.

1.3 Theory:

1.3.1 Introduction

Analysis of email is especially important not just because email may be used to communicate about things that we might be interested in for an investigation, but because it is a comparatively permanent and public record of those communications. In the case of a phone call, there is only the record that a call took place; in a spoken conversation, there may be no record at all. Conventional mail can be virtually untraceable, and paper documents are easily destroyed. Email, however, is unique; when a message is sent, the entire message is stored for both the sender and the receiver, and records of the mail being sent are stored on dozens of servers that the message passes through before arriving at its destination. There are a number of ways to analyze email, including: data mining techniques, which may be applied to large or small data sets; straightforward searching of a user's email for certain content; and in-depth analysis of an individual email's lineage.

E-mail system comprises of various hardware and software components that include sender’s client and server computers and receiver’s client and server computers with required software and services installed on each. Besides these, it uses various systems and

services of the Internet. The sending and receiving servers are always connected to the Internet but the sender's and receiver's client connects to the Internet as and when required.

An e-mail communication between a sender '*Alice'* having e-mail address '*alice@a.com*' and recipient '*Bob'* having e-mail address '*bob@b.com*' is shown in figure 1.'*Alice'* composes an e-mail message on her computer called client for '*Bob'* and sends it to her sending server 'smtp.a.org' using *SMTP* protocol. Sending server performs a lookup for the mail exchange record of receiving server '*b.org*' through Domain Name System (*DNS)* protocol on *DNS* server '*dns.b.org*'. The *DNS* server responds with the highest priority mail exchange server '*mx.b.org'* for the domain 'b.org'. Sending server establishes *SMTP* connection with the receiving server and delivers the e-mail message to the mailbox of '*Bob'* on the receiving server. '*Bob'* downloads the message from his mailbox on receiving server to local mailbox on his client computer using *POP3* or *IMAP* protocols. Optionally, '*Bob'* can also read the message stored in his server mailbox without downloading it to the local mailbox by using a Webmail program.

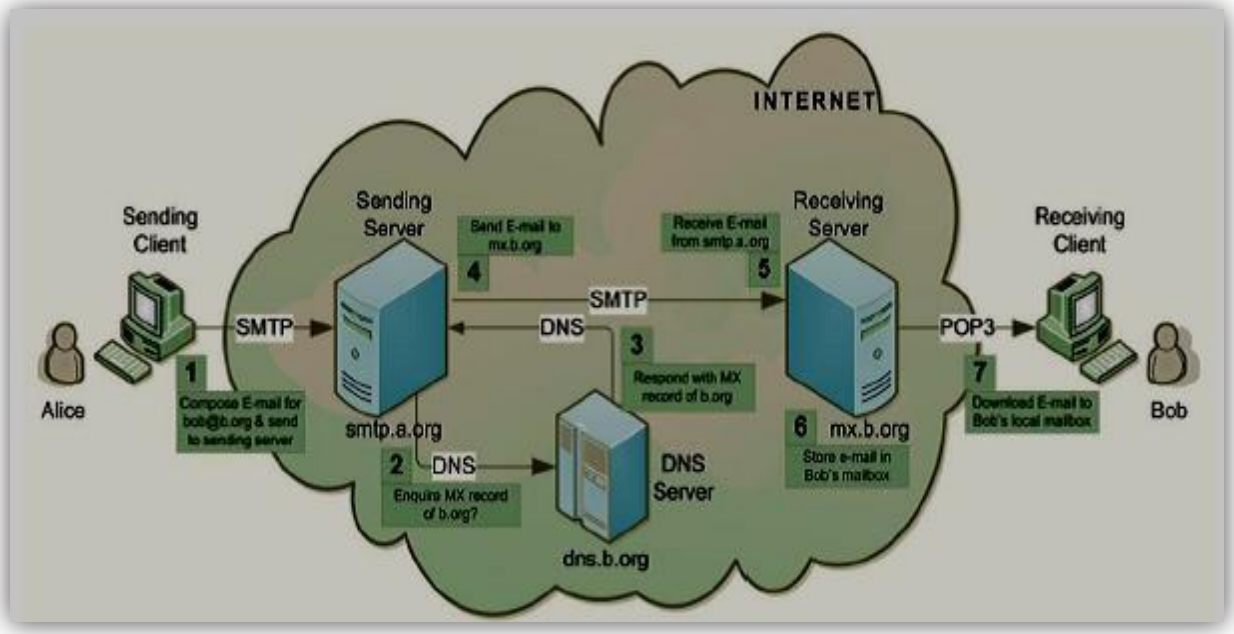

Figure 1*: E-mail communication between a sender 'Alice' and recipient 'Bob'*

1.3.2 E-MAIL ACTORS, ROLES AND RESPONSIBILITIES

E-mail is a highly distributed service involving several actors that play different roles to accomplish end-to-end mail exchange. These actors fall under "User Actors", "Message Handling Service (*MHS*) Actors" and "Administrative Management Domain (*ADMD*) Actors" groups.

User Actors are people, organizations or processes that serve as sources or sinks of messages. They can generate, modify or look at the whole message. User Actors can be of following four types (Table 1):

User Actor Type	Roles and Responsibilities
Author	▪ Responsible for creating the message, its contents, and its list of Recipient addresses. ▪ The MHS transfers the message from the Author and delivers it to the Recipients. ▪ The MHS has an Originator role that correlates with the Author role.
Recipient	▪ The Recipient is a consumer of the delivered message. ▪ The MHS has a Receiver role that correlates with the Recipient role. ▪ A Recipient can close the user-communication loop by creating and submitting a new message that replies to the Author e.g. an automated form of reply is the Message Disposition Notification (MDN)
Return Handler	▪ It is a special form of Recipient that provides notifications (failures or completions) generated by the MHS as it transfers or delivers the message. ▪ It is also called Bounce Handler.
Mediator	▪ It receives, aggregates, reformulates, and redistributes messages among Authors and Recipients. ▪ It forwards a message through a re-posting process. ▪ It shares some functionality with basic MTA relaying, but has greater flexibility in both addressing and content than is available to MTAs. It preserves the integrity and tone of the original message, including the essential aspects of its origination information. It might also add commentary. ▪ It does not create new message that forwards an existing message, Reply or annotation. ▪ Some examples of mediators are: Alias, ReSender, Mailing Lists, Gateways and Boundary Filter.

All types of Mediator user actors set HELO/EHLO, ENVID, RcptTo and Received fields. Alias actors also typically change To/CC/BCC and MailFrom fields. Identities relevant to ReSender are: From, Reply-To, Sender, To/CC/BCC, Resent-From, Resent-Sender, Resent-To/CC/BCC and MailFrom fields. Identities relevant to Mailing List processor are: List-Id, List-*, From, Reply-To, Sender, To/CC and MailFrom fields. Identities relevant to Gateways are: From, Reply-To, Sender, To/CC/BCC and MailFrom fileds.

Message Handling Service (MHS) Actors are responsible for end-to-end transfer of messages. These Actors can generate, modify or look at only transfer data in the message. *MHS* Actors can be of following four types (Table 2):

MHS Actor Type	Roles and Responsibilities
Originator	▪ It ensures that a message is valid for posting and then submits it to a Relay ▪ It is responsible for the functions of the Mail Submission Agent. ▪ It also performs any post-submission that pertain to sending error and delivery notice. ▪ The Author creates the message, but the Originator handles any transmission issues with it
Relay	▪ It performs MHS-level transfer-service routing and store-and-forward function by transmitting or retransmitting the message to its Recipients. ▪ It adds trace information but does not modify the envelope information or the semantics of message content. ▪ It can modify message content representation, such as changing the form of transfer encoding from binary to text, but only (as required) to meet the capabilities of the next hop in the MHS. ▪ When a Relay stops attempting to transfer a message, it becomes an Author because it sends an error message to the Return Address.
Gateway	▪ It connects heterogeneous mail services despite differences in their syntax and semantics. ▪ It can send a useful message to a Recipient on the other side, without requiring changes to any components in the Author's or Recipient's mail services.
Receiver	▪ It performs final delivery or sends the message to an alternate address. ▪ It can also perform filtering and other policy enforcement immediately before or after delivery.

For networks, a port means an endpoint to a logical connection. The port number identifies what type (application/service offered) of port it is. The commonly used default port numbers used in e-mail are shown in Table 3. A complete list of default port numbering assignment is given in

Port No	Protocols/Services	Description
25	SMTP SMTP e-mail server	Simple Mail Transfer Protocol - core Internet protocol used to transfer from client to server (MUA to MTA) and server to server (MTA to MTA)
110	POP3 POP e-mail server	Post Office Protocol allows clients (MUA's) to retrieve stored e-mail
143	IMAP IMAP(4) e-mail server	Internet Message Access Protocol provides a means of managing e-mail messages on a remote server and retrieve stored e-mail
465	SMTPS WSMTP (SSMTP) protocol over TLS|SSL	SMTP via SSL encrypted connection (Unofficial)
993	IMAPS SSL encrypted IMAP	IMAP via SSL encrypted connection
995	POP3S SPOP SSL encrypted POP	POP via SSL encrypted connection
587	MSA	Outgoing Mail (Submission)
80	HTTP	Webmail
443	HTTPS	Secure Webmail

1.3.3 Analyzing an Individual Email

Although webmail will feature prominently in this section, the analysis of a particular email's lineage is much broader and can be applied to any email. A simple view of the path of an email from a sender to a client is presented in Figure 2. The email originates from the sender, whether from a local email client or a webmail application. When the email is sent, it is first sent to a Simple Mail Transfer Protocol (SMTP) server. That server forwards it to other SMTP servers until it finally reaches the destination server. On reaching its destination, the email is sent to a Post Office Protocol (POP) server, or any number of similar mail-delivery servers (IMAP is another, and webmail services may use their own servers for this purpose). The receiving client then connects to that server, retrieves the message, and allows the recipient to read it.

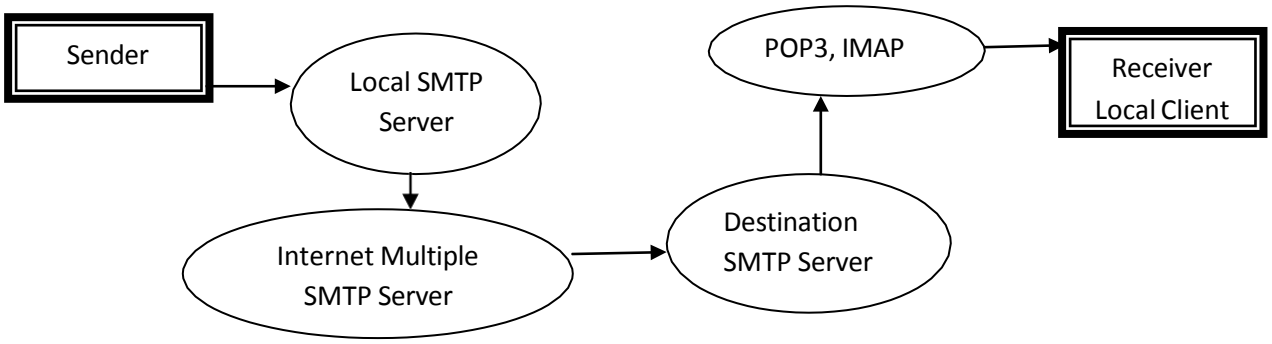

Figure 2: *Path of an email from a sender to a client*

When the email is sent and when it is received, those respective servers add their own information to the email's header, and most likely log the action. Access to those logs may be required for much analysis, but specifics are outside of the scope of this paper. Considerable information can be gleaned from the header alone.

Suppose Moses, with the address moses@nmt.edu, sends an email from his office on the New Mexico Tech campus to his similarly named friend, with the email address thenewmoses@gmail.com. The subject of this email is "Snakes," and the content "Fish."

Below is the entire theoretical email, including all headers.

From:
moses@nmt.edu
Subject: Snakes
Date: September 25, 2021 9:35:29 PM
MDT To: thenewmoses@gmail.com
X-Gmail-Received:
ca493ed685a8e9ae77165ab2ce345127e5b310b4 Delivered-
To: thenewmoses@gmail.com
Received: by 10.90.33.15 with SMTP id g15cs279684agg; Mon, 25 Sep
2021 20:35:32 0700 (PDT)
Received: by 10.35.113.12 with SMTP id q12mr526602pym; Mon, 25 Sep 2021
20:35:32 -0700 (PDT)
Received: from mailhost.nmt.edu (mailhost.NMT.EDU
[129.138.4.52]) by mx.gmail.com with ESMTP id 36si2059018nza.
2021.09.25.20.35.32; Mon, 25 Sep 2021 20:35:32 -0700 (PDT)
Received: from localhost (localhost.localdomain [127.0.0.1]) by
localhost.localdomain (Postfix) with ESMTP id 09FF4436164 for
<thenewmoses@gmail.com>; Mon, 25 Sep 2021 21:35:32 -0600
(MDT) Received: from mailhost.nmt.edu ([127.0.0.1]) by localhost
(mailhost.nmt.edu [127.0.0.1]) (amavisd-new, port 10024) with
ESMTP id 11225-05 for <thenewmoses@gmail.com>; Mon, 25 Sep 2021
21:35:30 -0600 (MDT)
Received: from [192.168.1.2] (cs-fitch017.nmt.edu [129.138.21.110])
by mailhost.nmt.edu (Postfix) with ESMTP id 6FD4B436030 for
<thenewmoses@gmail.com>; Mon, 25 Sep 2021 21:35:30 -0600
(MDT) Return-Path: <moses@nmt.edu>
Received-Spf: pass (gmail.com: best guess record for
domain of moses@nmt.edu designates 129.138.4.52 as
permitted sender) Mime-Version: 1.0 (Apple Message
framework v752.2)
Content-Transfer-Encoding: 7bit
Message-Id: <77E313EF-271F-4AD0-A8D3-81263BF7B083@nmt.edu>

Content-Type: text/plain; charset=US-ASCII;
format=flowed X-Mailer: Apple Mail (2.752.2)
X-Virus-Scanned: by amavisd-new-2.3.1 (20050509) (RHEL AS) at
nmt.edu Fish

E-MAIL IDENTITIES:

Field Name	Set By	Field Description
Layer: ***Message Header Fields (Identification Fields)***		
Message- ID:	Originator	Globally unique message identification string generated when it is sent.
In-Reply-To:	Originator	Contains the Message-ID of the original message in response to which the reply message is sent.
References:	Originator	Identifies other documents related to this message, such as other e-mail message.
Layer: ***Message Header Fields (Originator Fields)***		
From:	Author	Name and e-mail address of the author of the message
Sender:	Originator	Contains the address responsible for sending the message on behalf of Author, if not omitted or same as that specified in From field.
Reply- To:	Author	E-mail address, the author would like recipients to use for replies. If present it overrides the From field.
Layer: ***Message Header Fields (Originator Date Fields)***		
Date:	Originator	It holds date and time when the message was made available for delivery.
Layer: ***Message Header Fields (Informational Fields)***		
Subject:	Author	It describes the subject or topic of the message.
Comments:	Author	It contains summarized comments regarding the message.
Keyword:	Author	It contains list of comma separated keywords that may be useful to the recipients e.g. when searching mail.
Layer: ***Message Header Fields (Destination Address Fields)***		
TO:	Author	Specifies a list of addresses of the recipients of the message. These addresses might be different from address in RcptTo SMTP commands
CC:	Author	Generally same as To Field. Generally a To field specifies primary recipient who is expected to take some action and CC addresses

1.4 Execution Steps

- Open the Email which you want to analyze header
- Click on the right side three vertical dot(more) and select show original.
- New tab will be open then copy header information which you want to analyze.
- Open **https://www.whatismyip.com/email-header-analyzer** website.
- Copy the header information and click on analyze button.
- Then You will see the header analysis on screen.

1.5 Assignment Question:

1. Why to Analyze Email Header?
2. What Fields are analyzed during Email Analysis Header?
3. Which Readymade Tools are Available for Analyzing E-Mail Header?
4. Explain Email Architecture in Detail?
5. What is POP3, IMAP, SMTP, and MIME?

1.6 Conclusion:

E-mail is a widely used and highly distributed application involving several actors that play Different roles. These actors include hardware and software components, services and protocols which provide interoperability between its users and among the components along the path of transfer. Cybercriminals forge e-mail headers or send it anonymously for illegitimate purposes which lead to several crimes and thus make e-mail forensic investigation crucial.