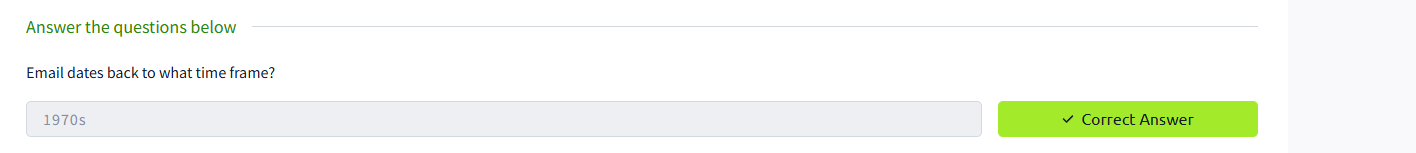
**Phishingemails1tryoe**

**Introduction**

Social Engineering Attacks by email such as spam and phishing are commonplace. Malicious emails bypass security measures and get delivered to the end-users; hence, this makes it critical for security analysts to analyse such emails, because with a single click on the malicious link or download of an attachment by an end-user, it could lead to absolute compromise of the organizational network. The analysis includes dissecting email headers and collecting intelligence to enhance security defences. One method of handling such an analysis is understanding email components and header analysis.

**The Email Address**

During the early part of the 1970s, Ray Tomlinson invented email under ARPANET. His well-known use of the "@" symbol became an icon in itself. An email address is defined as having three parts, namely: a user mailbox (username), a symbol known as @, and a domain (for example, billy@johndoe.com). This resembles how a mailing address works; the domain part is similar to a street, while the user mailbox identifies a particular house.



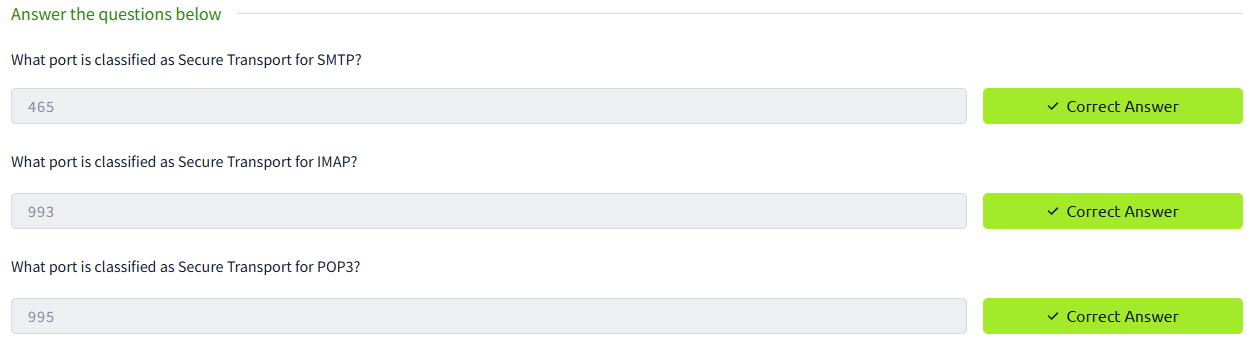
**Email Delivery**

When you send an email, there are essentially three protocols that govern the whole process:

* SMTP (Simple Mail Transfer Protocol): Delivers the email.
* POP3 (Post Office Protocol): Downloads the email onto one device, removing it from the server (unless set otherwise).
* IMAP (Internet Message Access Protocol): Syncs the email across multiple devices, leaving it on the server.

The travel of the email:

* Alexa writes her email to Billy and presses the send button.
* The SMTP server checks the DNS for all records pertaining to johndoe.com.
* The DNS server replies back with information on johndoe.com.
* The SMTP server delivers the email to the world.
* The email traverses numerous SMTP servers before arriving at the destination.
* It reaches the SMTP server assigned to Billy.
* The email is saved in a POP3/IMAP server.
* Billy's email client checks the mail server for any new emails.
* He is either downloading or synchronizing the email to read it, depending on whether it's POP3 or IMAP.



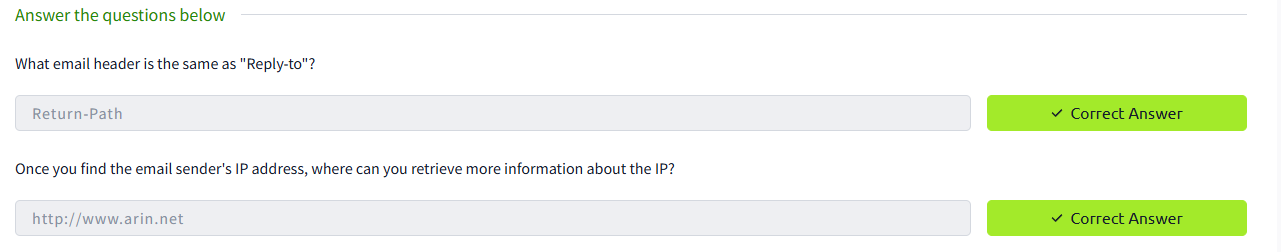
**Breaking Down the Components of Email for Analysis**

It comprises two basic sections:

* Email Header - Contains elements such as the sender and recipient and also its relay servers.
* Email Body - Contains the actual body contents of the email such as text or html.

Key Header fields in the email:

* From: the e-mail identity of the sender
* To: the e-mail identifier of the intended recipient
* Subject: Subject of the mail Headers
* Date: Date and Time when the email was sent.
* Other Header Fields of Interest:



**Email Body**

Inside An Email Body Are Contents With Real Meaning, In Either Plain Text Or HTML Format.

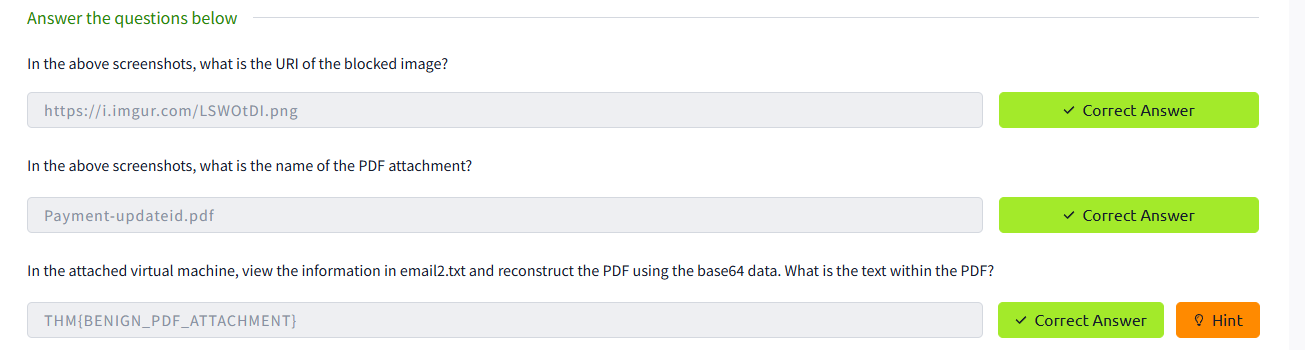
* Plain text emails are emails only formatted in text.
* HTML emails may contain images, hyperlinks, and styling.
* Most email clients permit the users to look at the raw HTML and analyze the links and other embedded entities.

**Email Attachments**

Emails can have attachments easily tracked and identified by specific headers in the email source code:

* Content-Type: The file type (e.g., application/pdf).
* Content-Disposition: Whether it is an attachment.
* Content-Transfer-Encoding: How the file is encoded (base64, for instance).

The attachments should be decoded from base64 and saved, but always analyze them carefully in order to avoid accidental execution of a malicious file.



**Types of Malicious Emails and Their Phishing Techniques:**

* Spam: Unwanted mass e-mails (MalSpam is the more dangerous form).
* Phishing: Using a facade of a trusted entity to steal sensitive data.
* Spear Phishing: Targeted phishing for individuals or organizations.
* Whaling: Phishing attacks just for certain executives, like CEOs or CFOs.
* Smishing: Phishing through SMS/text messages.
* Vishing: Phishing via voice calls.

**Common Characteristics of Phishing:**

* Spoofed sender address pretending to be a trusted entity.
* Urgent subject lines with words such as "Invoice" or "Suspended."
* Fake company brands to imitate a legitimate one (e.g., Amazon).

