Muhammad Izham Bin Norhamadi
B032020039

Class Activity

General steps of email forensics

- Analyse the email headers. Some of the important email header fields are Delivered-To, Received, X-Received, Return-Path, Received from, Received-SPF and DRIM-Signature
- Check the X headers as X-originating-IP header can be used to find original sender
- Investigate the source of the email from related ISP, and also server logs to identify the address of the computer which the email originated.
- Use Hexadecimal Editor analyse email and carve messages

Difference between Spam email and Spear Phishing

Spam email is unwanted junk email sent out in bulk to an indiscriminate recipient. Spam can be sent in massive volume by botnets, networks of infected computers. Spear phishing on the other hand is an email or electronic communications scam targeted towards a specific individual or organization. Phishing often intended to steal data for malicious purposes or install malware to target's computer.

Email header Analysis

Email header Analysis is the process of analysing the path of a message of where it has traversed before reaching its final destination. The information that can be extracted are recipient's and sender's names, time of sending and receiving email, email client, ISP, and IP address. This can help determining the legitimacy of email and malicious email.