

SPPU-BE-COMP-CONTENT - KSKA Git

Q1. Why are Email Headers so important in Computer Forensics?

ANS. The Email Header is a HTML code snippet in a HTML document, that contains information about the sender, recipient, email route to get to the inbox and various Authentication details.

IMPORTANT! (In Computer Forensics)

1. To Identify the Source of Email.

- The Header of Email can help determine IP Address source, sender, it is important in tracking spam, phishing or impersonation.

2. Detecting Forgery in Email.

- If an Email gets spoofed, inconsistencies are found in the Email Headers.
- So, these Headers can help reveal fraud Emails.

3. Validating Digital Evidence.

- Headers serve as a technical proof admissible in court, it ensures that email has not been tampered.

4. Timeline Verification.

- Header contains timeline stamps from each mail server it is passed through.
- This helps to detect when was the email sent and received.

Q2. How can Email Header Analysis be used in the Legal Process?

ANS. Legal Process uses Email Headers in the Following ways:-

(A) Challenging Email Authenticity:

- Defence teams can use headers to challenge the validity of Emails used against the clients.
- Discrepancies like mis-matched IP's or Forged time

SPPU-BE-COMP-CONTENT - KSKA Git

stamps can undermine claims.

(2.) Supporting the Digital Evidence in Court.

- Often used in cases like, cybercrime, Hacking, workplace harassment or threats.
- Requires Expert testimony to Explain Header Data and validate the Forensic findings.

(3.) Authenticating Emails.

- Header can confirm whether an email passed SPF, DKIM and DMARC checks
- Supports arguments about whether an email is legitimate or falsified.

(4.) Identifying the sender of the Email.

- IP Addresses in Header can pin-point the senders location OR Network
- It helps in determining whether an email came from an Authorized Account/Network or was it Spoofed.

Q3. How the use of Email Header Information could be used by a Digital Forensic professional in an Investigation?

Ans. In Digital Forensics, Email Header serves as a RoadMap of Every step of Email takes.

All Forensic professional can extract, Analyze and correlate this meta-data to uncover sender identity, timeline and discrepancies, Routing Anomalies, etc.

(1.) Collection and Preservation:



SPPU-BE-COMP-CONTENT – KSKA Git

- Acquire complete Email including Headers.
- Verify integrity via cryptographic hashes (md5, sha-256)
- Store the Original and Working Copies separately to prevent Accidental Alteration.

(2) Parsing and Extraction:

- Load preserved email into Specialized Tools.
- Extract key Header Fields such as received, ReturnPath, MessageID, SPF, DKIM, DMARC, etc.

(3) IP Address and Geolocation Analysis:

- Identify the originating IP from the earliest "Received" line
- Perform WHOIS lookups and Geolocation Mapping
- Cross Reference Against Threats Intelligence to Flag known Malicious actors.

(4) Correlating with other Evidences

- Correlate email content or headers with chat logs, browser History, or other communication channels.

CONCLUSION:-



Thus, Implementation of Email Header program is performed Successfully.