

Experiment 06

Learning Objective To learn about Email Spoofing & Analyzing Email Headers.

Tools: Emkei Mailer for email spoofing & Mx toolbox for email header analysis.

Theory:

What IS Email Spoofing?

Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they know or trust. In spoofing attacks, the sender forges email headers so that client software displays the fraudulent sender address, which most users take at face value. Users don't realize the sender is forged unless they inspect the header more closely. If it's a name they recognize, they're more likely to trust it. So, they will click malicious links, open malware attachments, send sensitive data, and even wire corporate funds.

Email spoofing is possible due to how email systems are designed. The client application assigns a sender address to outgoing messages, so outgoing email servers cannot identify whether the sender address is legitimate or spoofed.

Recipient servers and antimalware software can help detect and filter spoofed messages. Unfortunately, not every email service has security protocols in place. Still, users can review each message's email header to determine whether the sender address is forged.

How Email Spoofing Works

Email spoofing aims to trick users into believing the email is from someone they know or trust—in most cases, a colleague, vendor, or brand. Exploiting that trust, the attacker asks the recipient to divulge information or take some other action.

A typical email client (such as Microsoft Outlook) automatically enters the sender address when a user sends a new email message. But an attacker can programmatically send messages using basic scripts in any language that configures the sender address to a chosen email address. Email API endpoints allow a sender to specify the sender address regardless of whether the address exists. And outgoing email servers can't determine whether the sender's address is legitimate.

Outgoing email is retrieved and routed using the Simple Mail Transfer Protocol (SMTP). When a user clicks "Send" in an email client, the message is first sent to the outgoing SMTP server configured in the client software. The SMTP server identifies the recipient domain and routes it to the domain's email server. The recipient's email server then routes the message to the right user inbox.

For every "hop" an email message takes as it travels across the internet from server to server, the IP address of each server is logged and included in the email headers. These headers divulge the true route and sender, but many users do not check headers before interacting with an email sender.

The three major components of an email are:

- 1.The sender address
- 2.The recipient address
- 3.The body of the email

Another component often used in phishing is the Reply-To field. The sender can configure this field and use it in a phishing attack. The Reply-To address tells the client email software where to send a reply, which can be different from the sender's address. Again, email servers and the SMTP protocol do not validate whether this email is legitimate or forged. It's up to the user to realize that the reply is going to the wrong recipient.

Spoofing vs. Phishing

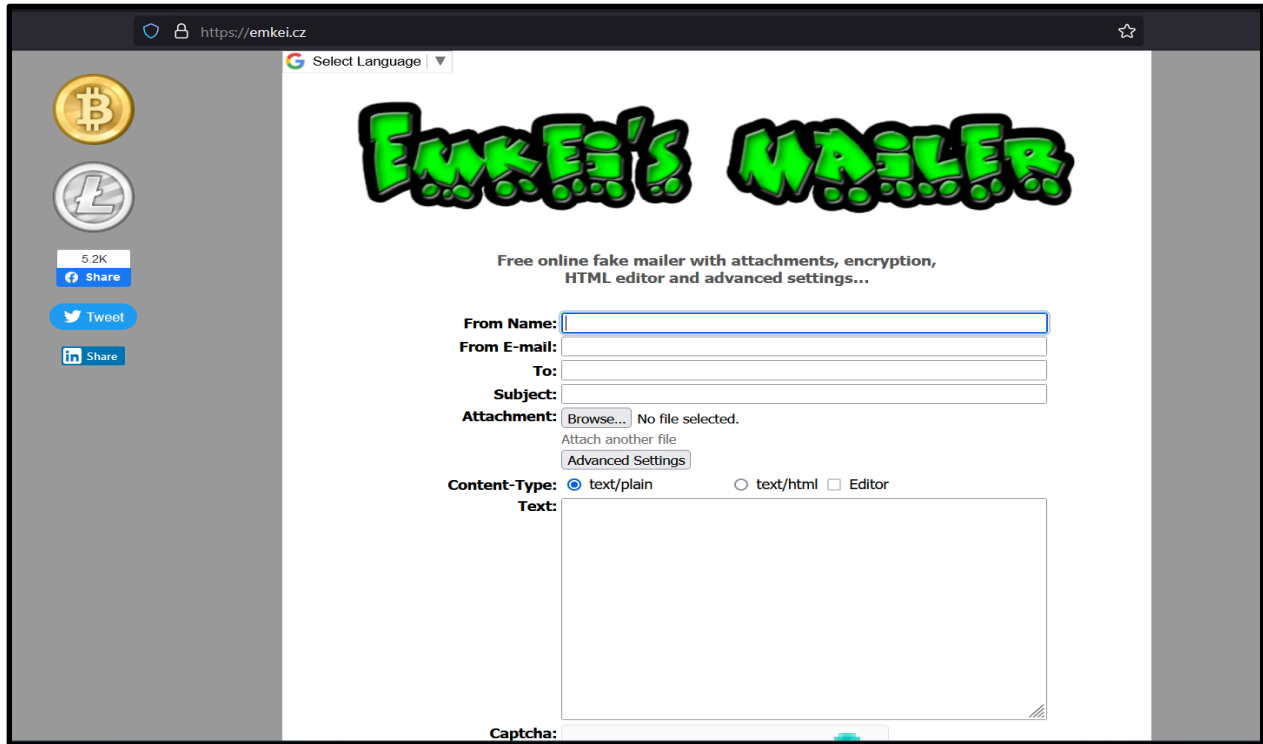
Despite sharing some similarities, spoofing and phishing are two distinct cyber threats with several fundamental differences.

- 1.The goal of spoofing is to impersonate someone's identity, while the goal of phishing attacks is to steal information.
- 2.Phishing scams are fraudulent because they involve information theft. However, spoofing is not considered fraud because the victim's email address or phone number is not stolen but rather imitated.
- 3.Phishing often involves the attacker pretending to be from a trusted organization, whereas spoofing involves changing the sender's email address or phone number to impersonate someone else.
- 4.Phishing is commonly executed with fake websites and data collection portals. Spoofing emails can be used to breach system security or steal user information.

The tool we will be using for email spoofing is **Emkei Mailer**

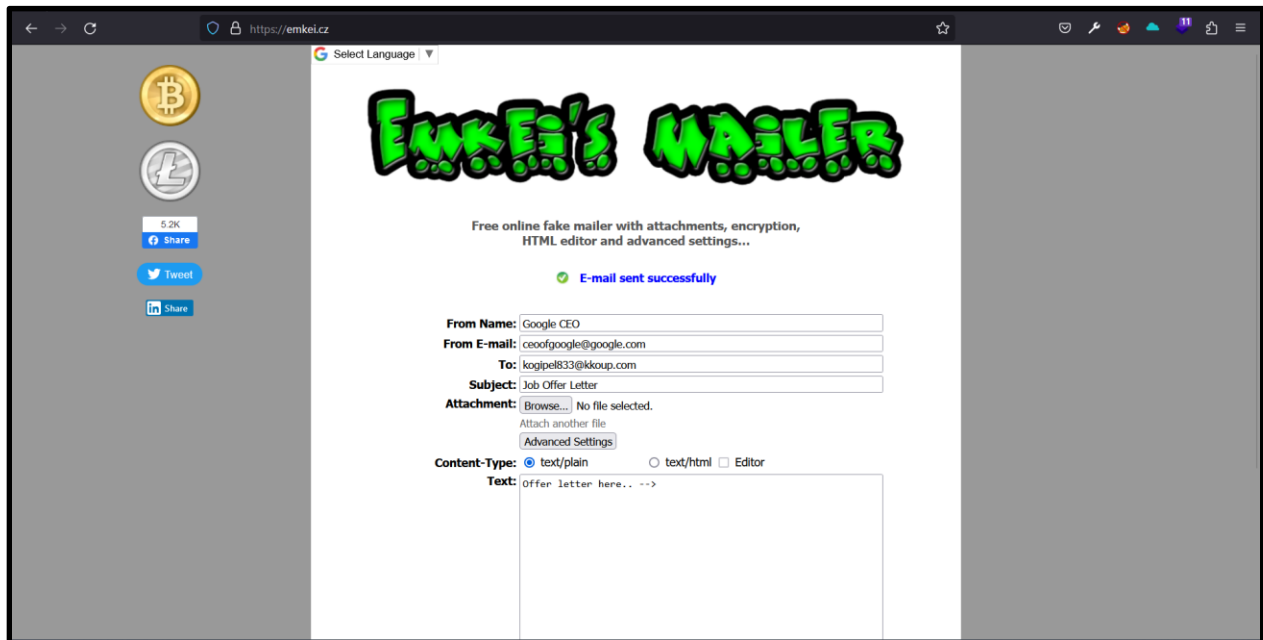
Learning Objective 01: To learn about Email Spoofing.

Step 1: Go to the website → <https://emkei.cz/>



The screenshot shows the Emkei's Mailer website interface. On the left sidebar, there are Bitcoin and Litecoin logos with a balance of 5.2K, and social media share buttons for Facebook, Twitter, and LinkedIn. The main content area features the 'EMKEI'S MAILER' logo in a green, bubbly font. Below the logo, it states 'Free online fake mailer with attachments, encryption, HTML editor and advanced settings...'. The form includes fields for 'From Name:', 'From E-mail:', 'To:', and 'Subject:'. There is an 'Attachment:' section with a 'Browse...' button and a note 'No file selected.', along with an 'Attach another file' button and an 'Advanced Settings' button. The 'Content-Type:' section has radio buttons for 'text/plain' (selected), 'text/html', and a checkbox for 'Editor'. A large text area for the email body is present, and a 'Captcha:' field is at the bottom.

Step 2: Enter all the required details.




This screenshot shows the same Emkei's Mailer website, but the form is now filled out with example data. A green checkmark and the message 'E-mail sent successfully' are displayed above the form fields. The filled-in details are: 'From Name: Google CEO', 'From E-mail: ceoofgoogle@google.com', 'To: kogipe833@kkoup.com', and 'Subject: Job Offer Letter'. The 'Attachment:' section remains the same. The 'Content-Type:' section still has 'text/plain' selected. The text area now contains the placeholder text 'Offer letter here.. -->'. The sidebar and logo remain unchanged.

Step 3: Solve the captcha and send the mail.

Step 4: Now check inbox of the mail that we have entered.

SENDER	SUBJECT	VIEW
<ul style="list-style-type: none"> Google CEO ceofgoogle@google.com 	Job Offer Letter	>
<ul style="list-style-type: none"> bob bobb@gmail.com 	Great work done on recent project	>

Step 5: Here is the result, you will see the mail that we have sent from Emkei mailer.

< BACK TO LIST	Delete	Source
<div>  <div> Google CEO ceofgoogle@google.com </div> </div>	Date: 27-07-2023 15:17:04	
Subject: Job Offer Letter		
Offer letter here.. -->		

Learning Objective 02: To learn about Email Headers.

What is an email header?

An email has two parts. It consists of the body, which is the information sent to the recipient within the message, and the header. The email header includes the **'To,' 'From,' 'Date,'** and **'Subject'** lines, but it also contains important metadata within the email. Every email you receive or send contains this code; it shows the email's route, including where it originated from.

What is Email Header Analyzing

Tracing an email address by analyzing the header provides useful data in cases of malicious messages, such as in phishing attacks. This tool works for an email header extracted from any client, including Gmail and Outlook.

What information can you find using email header analysis?

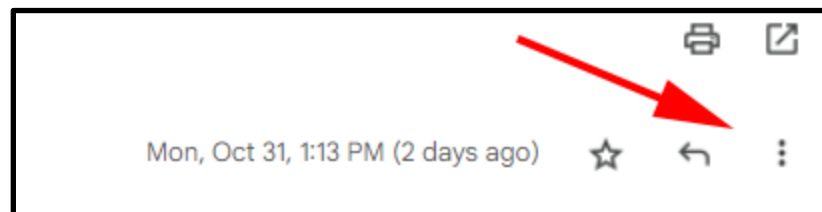
Aside from the basic sender and recipient information, analyzing an email header also reveals the content type and date of delivery. With an email header analyzer tool, users can also see the source of a message from the email headers, including a sender's IP address and location. However, it only reveals the sender's public IP, not their private IP.

How to Find the Header From an Email?

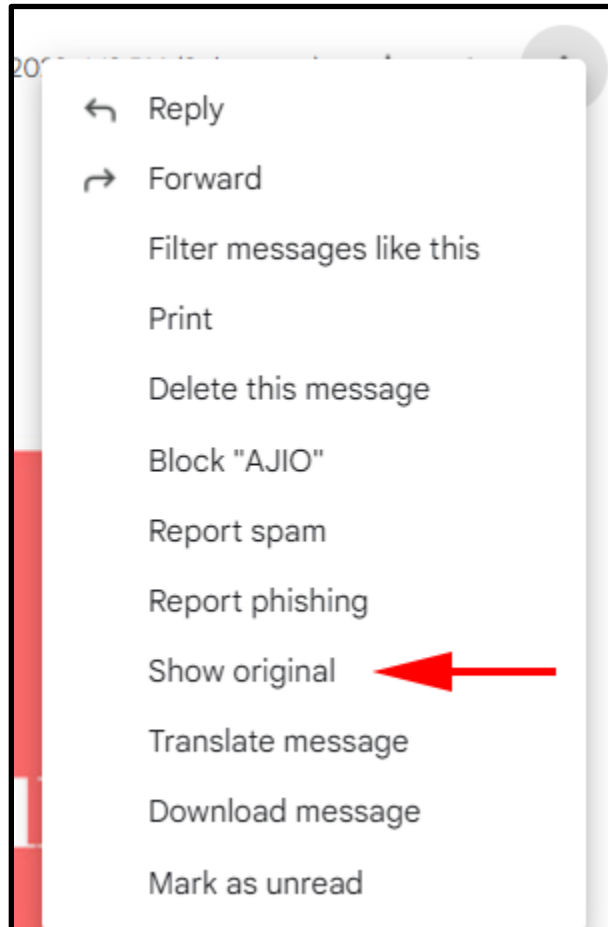
While all mail providers allow you to find the header from an email, there are different steps for each. Since many of us use Gmail, let's find out how to get the header from an email you received on your Google account.

Step 1: Log in to your Gmail account and open the particular email.

Step 2: From the right side, click on the 3 dots.



Step 3: Click on where it says “Show original”.



Step 4: The extended email header should look like this: Here you will find all the details you will need.

Original Message

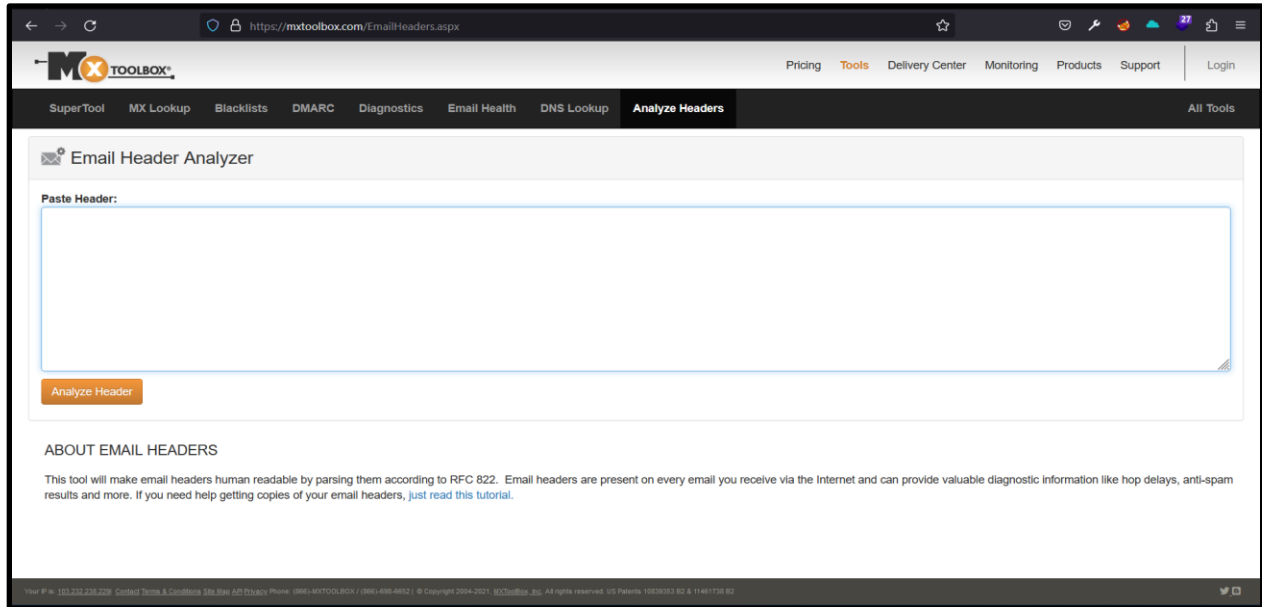
Message ID	
Created at:	Mon, Oct 31, 2022 at 12:26 PM (Delivered after 2810 seconds)
From:	AJIO <alert@...>
To:	
Subject:	Dresses for You & Your Mine me!
SPF:	PASS with IP ... Learn more
DKIM:	'PASS' with domain mailer.ajio.in Learn more

[Download Original](#)
[Copy to clipboard](#)

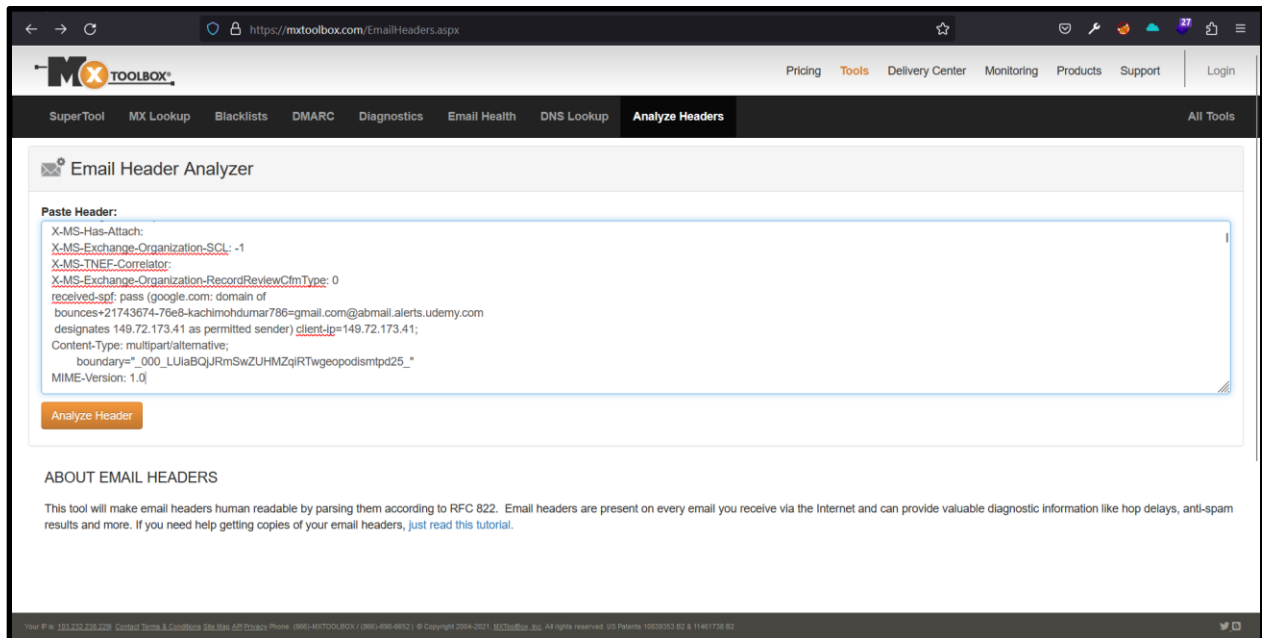
Learning Objective 03: To learn about Email Header Analysis.

Analyzing Header using Mxtoolbox

This email header analyzer by MxToolbox is a very simple and straightforward tool. After you paste the header snippet you copied from the email you received, this tool will return the information in a very readable manner, separated by columns and tables.



Step 1: Paste the header in the **Paste Header** box after that click on the **Analyze Header**.



Step 2: Here is the result of the email header.

Header Analyzed
 Email Subject: Dresses for You & Your Mine me! ◀ Analyze New Header

Delivery Information

> ✖ DMARC Compliant (No DMARC Record Found)

> ✔ SPF Alignment

> ✔ SPF Authenticated

> ✔ DKIM Alignment

> ✔ DKIM Authenticated

Relay Information

Received	0 seconds
Delay:	

Learning Outcomes: The student should have the ability to:

LO1: Understand usage of Emkei Mailer.

LO2: Understand about Email Headers.

LO3: Understand usage of Mxtoolbox for Email Header Analysis.

Course Outcomes: Upon completion of the practical students will be able to understand the concept of email spoofing and Email header analysis and will be able to use the tools for security purposes.

Conclusion: Through this experiment we learned the concept of email headers & Email spoofing and we used the MXtoolbox for analyzing the email header.

For Faculty Use:

Correction Parameters	Formative Assessment [40%]	Timely completion of Practical [40%]	Attendance / Learning Attitude [20%]	
Marks Obtained				