Email Tracing and analysis

Nikhil Kumar (22BCY10158)
VIT BHOPAL
Kothri Kalan Bhopal , MP
09th Dec 2024

Importance of Email tracing in Cybersecurity and Digital Forensics

Email Headers:

Imagine this as the letter's address and the postmarks on the envelope. It tells us who sent it and where it has been.

Cybersecurity:

This is like having guards to protect our digital world. We want to make sure the letters (emails) are safe and not dangerous.

Phishing:

Imagine someone trying to trick you with a fake letter that looks real. Email tracing helps us spot these tricks.

Spoofing:

It's like someone pretending to be a friend in their letter when they're not. We want to check if it's really from them.

Malware and Viruses:

These are like hidden germs in the letter. We need to see if the letter carries any germs that can harm our computer.

Digital Detective Work:

Think of email tracing as being a digital detective. We follow clues in the letter's address to figure out where it came from and if it's safe.

Spam:

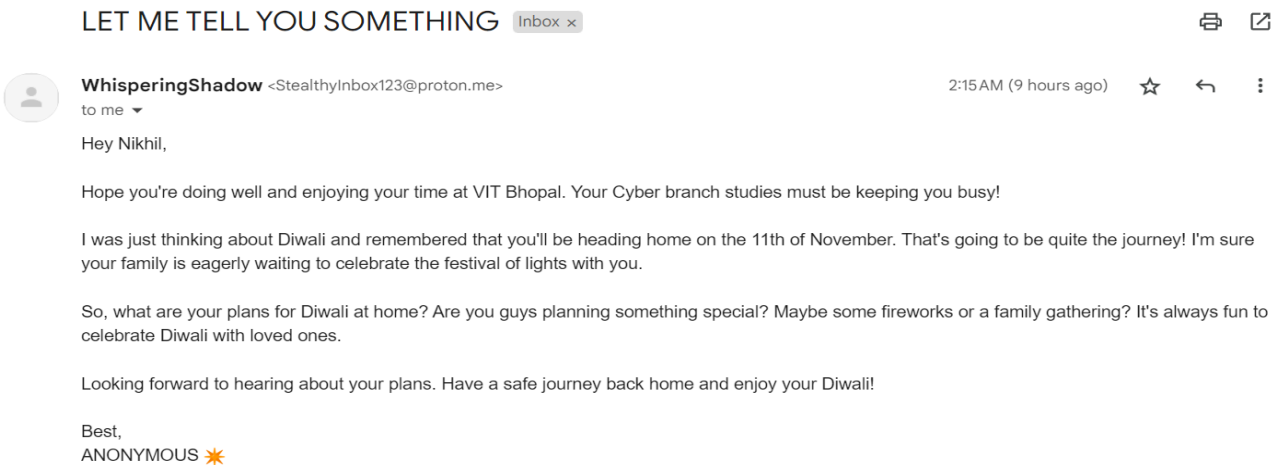
Imagine getting lots of junk mail in your mailbox. Email tracing helps us sort out the real letters from the junk.

Legal Investigations:

Sometimes we need to use email tracing in court, like showing evidence from the letters.

Step 1: Selecting a mail

I have sent mail to myself using the app proton mail.



LET ME TELL YOU SOMETHING Inbox ×

WhisperingShadow <StealthyInbox123@proton.me> 2:15 AM (9 hours ago)
to me

Hey Nikhil,

Hope you're doing well and enjoying your time at VIT Bhopal. Your Cyber branch studies must be keeping you busy!

I was just thinking about Diwali and remembered that you'll be heading home on the 11th of November. That's going to be quite the journey! I'm sure your family is eagerly waiting to celebrate the festival of lights with you.

So, what are your plans for Diwali at home? Are you guys planning something special? Maybe some fireworks or a family gathering? It's always fun to celebrate Diwali with loved ones.

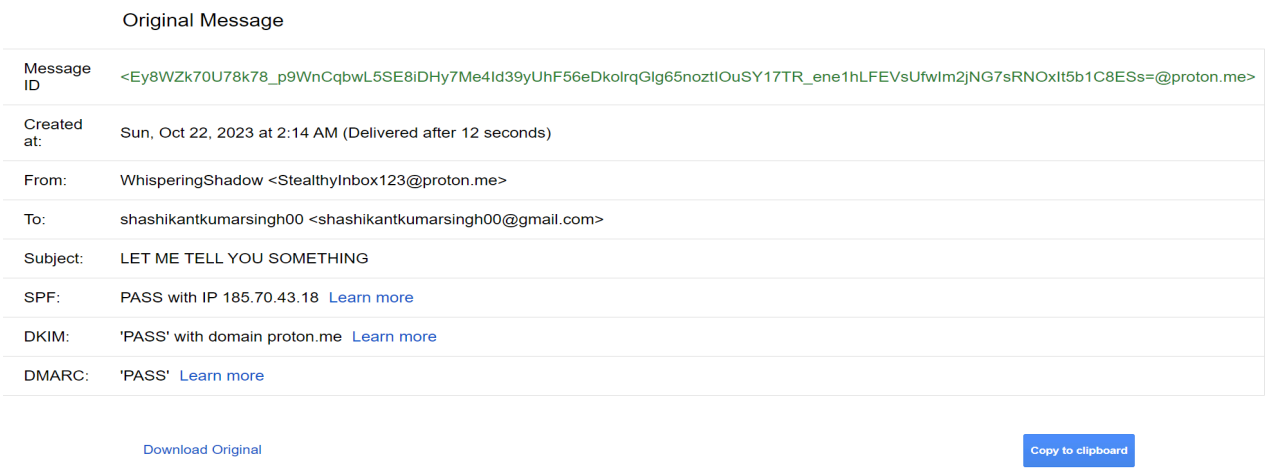
Looking forward to hearing about your plans. Have a safe journey back home and enjoy your Diwali!

Best,
ANONYMOUS

Step 2: Examine the header of mail

After selecting the mail we can access the header info of the mail by following way:

- *CLick on the 3 dots on the extreme right .*
- *There will be an option to **show original .***
- *Now after this we will get the information of the mail as follows:*



Original Message

Message ID	<Ey8WZk70U78k78_p9WnCqbwL5SE8iDHy7Me4Id39yUhF56eDkoIrqGlg65noztIOuSY17TR_ene1hLFEVsUfwIm2jNG7sRNOxIt5b1C8ESs=@proton.me>
Created at:	Sun, Oct 22, 2023 at 2:14 AM (Delivered after 12 seconds)
From:	WhisperingShadow <StealthyInbox123@proton.me>
To:	shashikantkumarsingh00 <shashikantkumarsingh00@gmail.com>
Subject:	LET ME TELL YOU SOMETHING
SPF:	PASS with IP 185.70.43.18 Learn more
DKIM:	'PASS' with domain proton.me Learn more
DMARC:	'PASS' Learn more

Download Original Copy to clipboard

So from the show original we can get the informations like **:**

- *When it was created or sent*
- *From which mail id*
- *To whom along with the subject.*
- ***Ip address 185.70.43.18***
- *Info. like* ***SPF, DKIM & DMARC*** *this will help in validation of the mail .*

Experts Flow examination

1. Email Headers Examination:

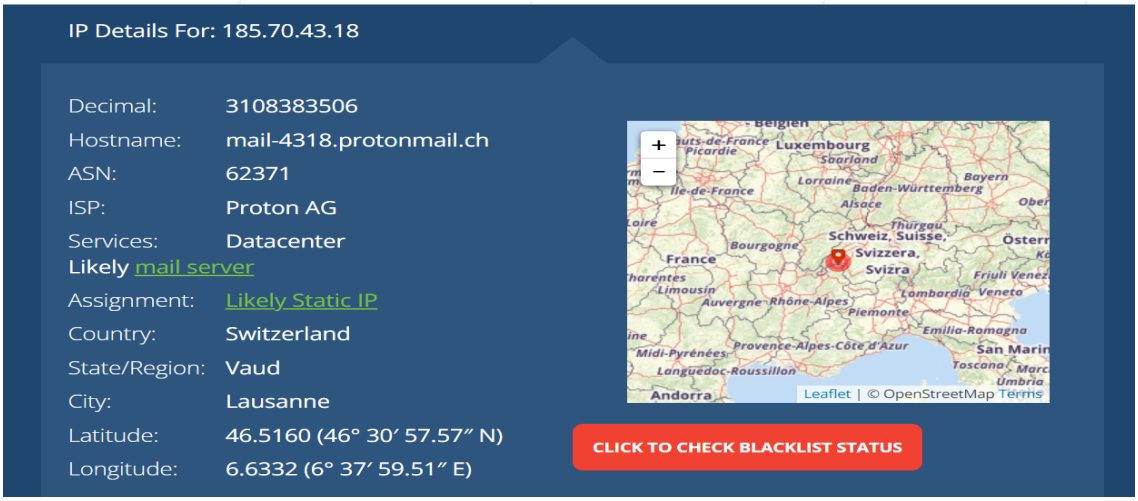
You received an email , but something doesn't seem right. You open the email and look for the "Show Original" or "View Headers" option in your email client. This shows you the email headers.

2. Online Header Analysis Tools:

You copy the email headers and paste them into an online email header analysis tool, like ***"Email Header Analyzer.****" This tool breaks down the header information, making it easier to understand.*

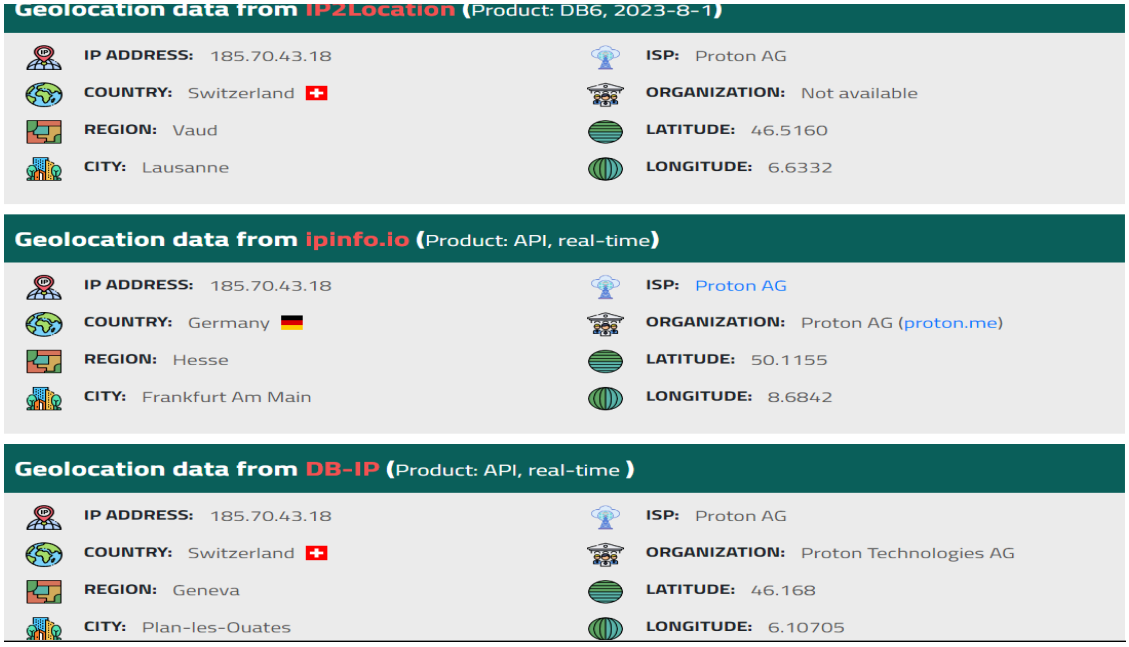
3. Tracing IP Addresses:

*In the header analysis, you notice the sender's IP address, such as "****185.70.43.18****" To trace this, you use an* ***IP lookup tool****. The tool tells you that this IP address is located .*



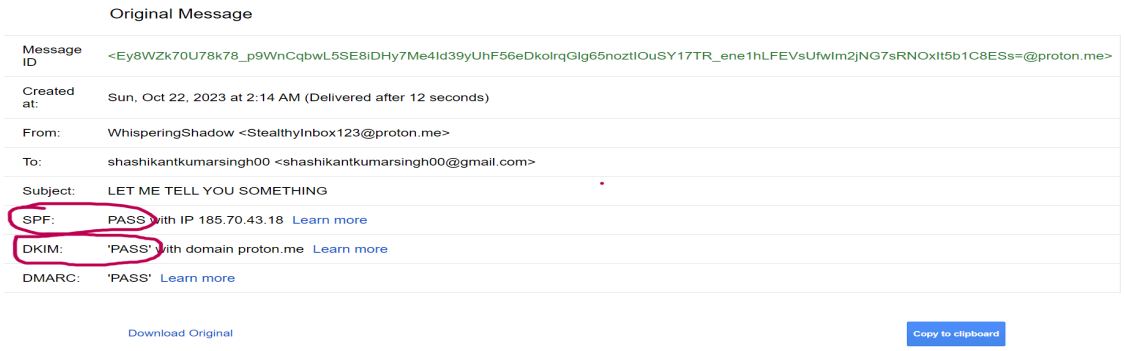
4. Geolocation Tools:

*Geolocation tools like "**IP Geolocation Lookup**" help you map the IP address. You discover that the sender's IP address points to a city in a different country .*



5. Validation of Authentication:

*You see a "**DKIM: PASS**" in the email header. This means the email's signature has been successfully verified using **DKIM.** It's like a genuine signature on a letter, confirming its authenticity.*



6. Analyzing Email Servers:

*As you examine the headers, you notice the email passed through various servers, including "**StealthyInbox123@proton.me**" and "**shashikantkumarsingh00@gmail.com**" . It's like tracking the journey of a letter as it passes through different post offices.*

7. Timestamp Analysis:

The header timestamps show the email's journey, from the sender's server to your inbox. This helps you create a timeline, like putting events in order on a calendar, to understand the email's path.

The sender's name is "WhisperingShadow," and the email address is "StealthyInbox123@proton.me."

To:

The recipient's email address is "shashikantkumarsingh00@gmail.com."

Subject:

The subject of the email is "LET ME TELL YOU SOMETHING."

SPF:

*The SPF record indicates "PASS" with the IP address **185.70.43.18**. This suggests that the email passed **Sender Policy Framework (SPF**) checks and the sender's IP address is authorized to send emails on behalf of the domain "proton.me." It aligns with the claimed domain, which is a positive sign.*

DKIM:

*The DKIM check reports "'**PASS**'" with the domain "**proton.me**." This indicates that the DKIM signature was successfully verified, ensuring the email's authenticity and that it hasn't been tampered with during transmission.*

DMARC:

The DMARC result is "'PASS.'" A DMARC policy set to "PASS" means that the email passed both SPF and DKIM checks, enhancing the email's authentication.

8. Software and Online Services:

Throughout this investigation, you use various software tools and online services that are like detective tools. They help you understand the email headers, trace IP addresses, and perform geolocation checks.

9. Forensic Techniques:

In more complex cases, like investigating cybercrimes, digital forensics experts might employ advanced forensic techniques. These can involve deep analysis of email headers and metadata to gather evidence and build a case against cybercriminals.

Report

Subject: Email Tracing and Analysis Report

Date: 09-12-24

Report Prepared by: Nikhil Kumar (22BCY10158)

Executive Summary:

This report presents the results of an email tracing and analysis exercise to investigate the origin and authenticity of an email received by [Recipient's Name]. The email in question is from the sender "WhisperingShadow" with the email address "StealthyInbox123@proton.me" and is addressed to "shashikantkumarsingh00@gmail.com." Our analysis includes a thorough examination of the email headers, geolocation information, domain investigation, and content analysis.

I. **Email Header Analysis:**

The Message ID is <Ey8WZk70U78k78_p9WnCqbwL5SE8iDHy7Me4Id39yUhF56eDkolrqGlg65noztIOuSY17TR_ene1hLFEVsUfwIm2jNG7sRNOxIt5b1C8ESs=@proton.me>, providing a unique identifier for the email.

The email was created on Monday, December 22, 2024, at 8:14 AM.

It was delivered approximately 12 seconds after creation.

II. Geolocation Information:

The email's sender IP address, ***185.70.43.18,*** *was determined to be the source of the email.*

*Geolocation tools indicate that this IP address is located at (****Switzerland/Germany)*** *which appears to align with the claimed domain.*

III. Domain Investigation:

SPF record: The email passes Sender Policy Framework (SPF) checks with IP 185.70.43.18, indicating the sender's IP is authorized to send emails on behalf of "proton.me."

DKIM result: The DKIM check reports "'PASS'" with the domain "proton.me," verifying the email's authenticity and integrity.

DMARC result: The DMARC result is "'PASS,'" indicating successful alignment with SPF and DKIM policies.

IV. Content Analysis:

The email's subject is "LET ME TELL YOU SOMETHING." Further content analysis reveals the body of the email, which should be reviewed carefully for any suspicious content or attachments.

Conclusion:

The email under investigation, with the sender "WhisperingShadow" and originating from "StealthyInbox123@proton.me," shows strong signs of authenticity and has passed essential authentication checks (SPF, DKIM, and DMARC). The geolocation information aligns with the claimed domain. However, despite these positive indicators, recipients should exercise caution and conduct a thorough review of the email's content for any potential red flags or malicious elements.