

Cyber Threat Intelligence

Tracking Emails Like a Cyber Spy!

Learn Email Footprinting & DNS Interrogation

Task 01: Data Collection through Email Foot-Printing

Email Footprinting:

- **Email Footprinting** is the process of gathering information about a target by analyzing emails sent by or received from them.
- This technique is commonly used to collect valuable details about a target's **email server, IP addresses, mail headers, metadata,** and security configurations.

Method of Email Footprinting by Analyzing Email Headers

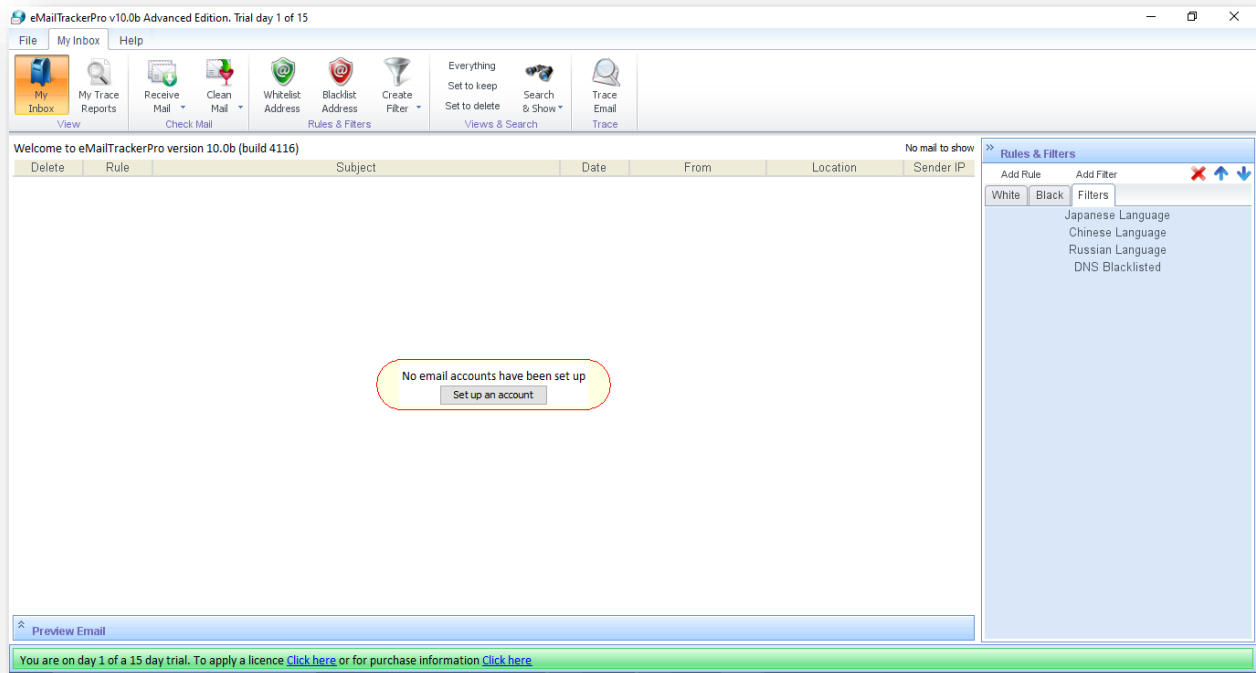
Every email contains a header that provides details about the sender, recipient, and route. In this, we will collect data by using **EmailTrackerPro** tool.

EmailTrackerPro:

EmailTrackerPro is an email tracking tool that helps users analyze email headers, track sent emails, and identify recipient interactions. It is commonly used for:

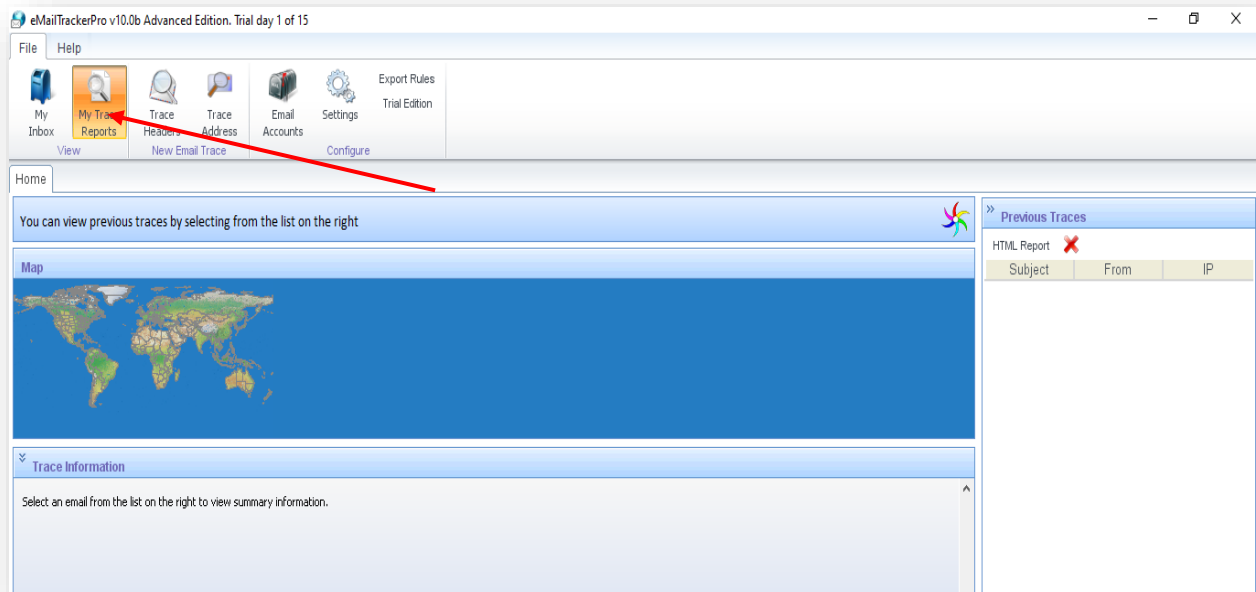
- **Tracking email delivery status** (sent, opened, or clicked).
- **Extracting sender IP addresses** from email headers.
- **Analyzing email paths and servers** involved in transmission.
- **Detecting email spoofing attempts** and phishing threats.

Main Window of EmailTrackerPro:



Let's trace Email by **Email Header**. For this, we click on

MyTraceReports Icon:



Target:

“WsCube Cyber Security” an **Indian platform** that offer courses related to cyber security. I have used their email header information and paste it in this tool.

Visualware eMailTrackerPro Trial (day 1 of 15) ×

[Configure](#) | [Help](#) | [About](#)

eMailTrackerPro by Visualware

I Want To: _____

☒ **Trace an email I have received**

A received email message often contains information that can locate the computer where the message was composed, the company name and sender's ISP ([more info](#)).

☐ **Look up network responsible for an email address**

An email address lookup will find information about the network responsible for mail sent from that address. It will not get any information about the sender of mail from an address but can still produce useful information.

Enter Details _____

To proceed, paste the email headers in the box below ([how do I find the headers?](#)).

Note: If you are using Microsoft Outlook, you can trace an email message directly from Outlook by using the eMailTrackerPro shortcut on the toolbar.

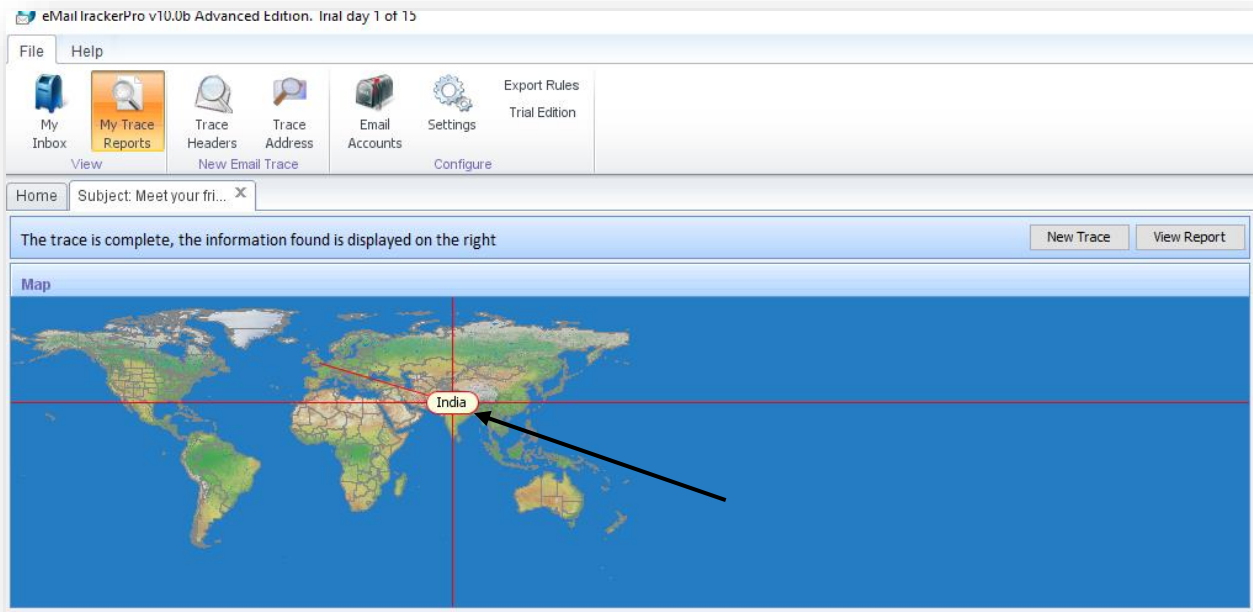
Email headers:

```
campaign=3D6648b4c01770203b94d144a8&utm_medium=3DEMAIL/t/api/campaig
c/emailView?campaignReportLogId=3D6648b4c01770203b94d144a8" alt=3D"P
tyle=3D"width: 1px; height: 1px; opacity: 0; border: none;">
</body>

</html>
--_-----=_171630010326207171--|
< _____ >
```

By tracing email through emailheader, it gives us **location and complete route of email**:

Location:



Route of Email:

Table #	Hop IP	Hop Name	Location
1	192.168.183.207		
2	192.168.100.1		
3	202.163.72.253		(Pakistan)
4	192.168.63.250		
5	192.168.100.133		
6	192.168.4.29		
8	213.202.7.208		(United Arab Emirates)
11	213.202.6.194		(United Arab Emirates)
12	134.0.220.105		(Australia)
13	195.66.224.76	ae15.mpr1.lhr15.uk.above.net	London, UK
16	64.125.30.59	ae6.mpr3.phl2.us.zip.zayo.com	(America)
17	64.125.21.74	ae4.mpr4.phl2.us.zip.zayo.com	(America)
18	64.124.191.83	64.124.191.83.IPYX-136392-008-ZYO.zip.zayo.com	(America)
19	206.183.107.11		(America)
End	175.158.66.157	mta6-66.157.pttransmail.com	(India)

Email Summary:

Email Summary

From: notifications@mg1.graphy.com

To: [REDACTED]

Date: Tue, 21 May 2024 19:31:43 +0530

Subject: Meet your friends on WsCube Tech's online platform

Location: (India)

Misdirected: No

Abuse Address: abuse@mumbai.ravience.in

Abuse Reporting: To automatically generate an email abuse report [click here](#)

From IP: 175.158.66.157

System Information:

- There is no SMTP server running on this system (the port is closed).
 - There is no HTTP server running on this system (the port is closed).
 - There is no HTTPS server running on this system (the port is closed).
 - There is no FTP server running on this system (the port is closed).
-

Task 02: Data Collection through DNS Interrogation

- DNS (Domain Name System) Interrogation is a technique used to gather publicly available information about a target domain by querying DNS server.
- It is used to **find the IP address of given domain names**.
- The information it gives include DNS domain names, computer name, IP addresses and information about particular network.

Methods of DNS Interrogation

1. WHOIS Lookup

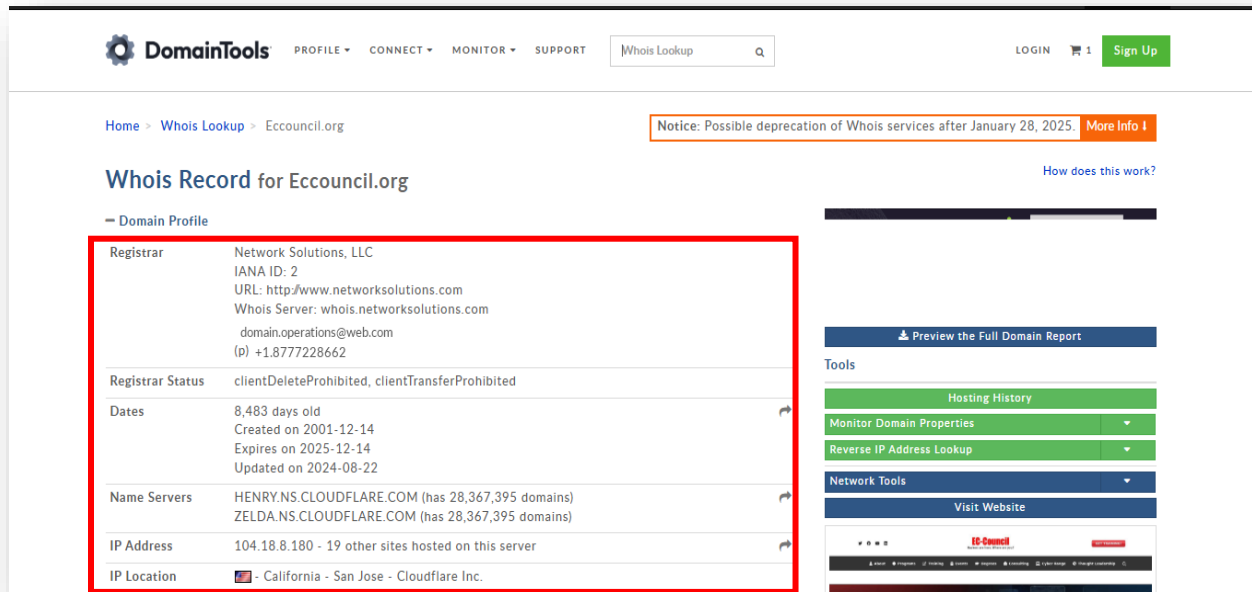
- It provides **domain registration details**, including: domain owner name, registrar information, contact details (unless protected by privacy services), domain creation & expiry dates

Main Window of Whois LookUp:



Now, we enter the domain name of **EC-council** organization to collect its data.

The publicly available data:



The screenshot shows the DomainTools Whois Lookup interface for the domain Eccouncil.org. The page includes a navigation bar with links like PROFILE, CONNECT, MONITOR, and SUPPORT, along with a search bar and a LOGIN button. A notice at the top right states: "Notice: Possible deprecation of Whois services after January 28, 2025. More Info". The main heading is "Whois Record for Eccouncil.org". Below this, a "Domain Profile" section is highlighted with a red box, containing the following data:

Registrar	Network Solutions, LLC IANA ID: 2 URL: http://www.networksolutions.com Whois Server: whois.networksolutions.com domain.operations@web.com (p) +1.8777228662
Registrar Status	clientDeleteProhibited, clientTransferProhibited
Dates	8,483 days old Created on 2001-12-14 Expires on 2025-12-14 Updated on 2024-08-22
Name Servers	HENRY.NS.CLOUDFLARE.COM (has 28,367,395 domains) ZELDA.NS.CLOUDFLARE.COM (has 28,367,395 domains)
IP Address	104.18.8.180 - 19 other sites hosted on this server
IP Location	🇺🇸 - California - San Jose - Cloudflare Inc.

To the right of the domain profile, there are several tool buttons: "Preview the Full Domain Report", "Tools", "Hosting History", "Monitor Domain Properties", "Reverse IP Address Lookup", "Network Tools", and "Visit Website". At the bottom, there is a small preview of the Eccouncil website.

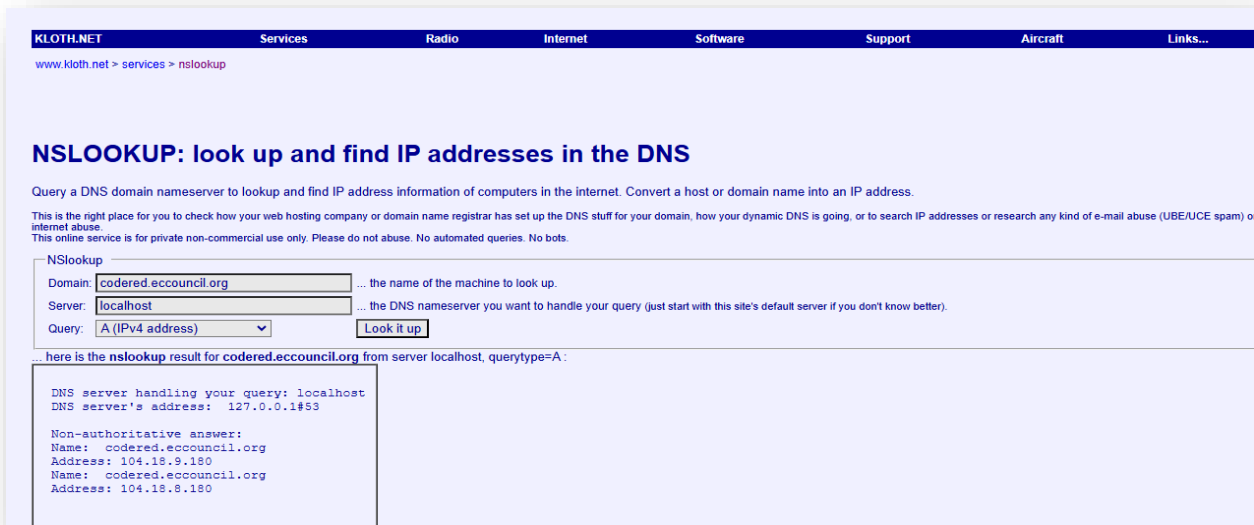
2- NSLookUp Tool:

Now we perform Data collection through DNS interrogation using **NSlookup** website.



The screenshot shows the NSLOOKUP website interface. At the top is a navigation bar with links: KLOTH.NET, Services, Radio, Internet, Software, Support, and Aircraft. Below the navigation bar is a breadcrumb trail: www.kloth.net > services > nslookup. The main heading is "NSLOOKUP: look up and find IP addresses in the DNS". Below the heading is a paragraph explaining the tool's purpose: "Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name into an IP address." This is followed by a disclaimer: "This is the right place for you to check how your web hosting company or domain name registrar has set up the DNS stuff for your domain, how your dynamic DNS is going, or to search IP addresses or research any kind of internet abuse. This online service is for private non-commercial use only. Please do not abuse. No automated queries. No bots." The search form is titled "NSlookup" and contains three input fields: "Domain:" with a text box containing "localhost", "Server:" with a text box containing "localhost", and "Query:" with a dropdown menu showing "A (IPv4 address)". A "Look it up" button is to the right of the query field. Below the form is a detailed explanation of the NSLOOKUP utility, its purpose, and how to use it. It mentions that the utility is a Unix tool and provides a link to the nslookup manual. It also explains that the website's online service can query a specific DNS server, but in most cases, it's sufficient to use the KLOTH.NET default nameserver "localhost/127.0.0.1". It notes that the service can perform PTR queries (reverse lookup) but only if the IP address owner has inserted a PTR record. It also mentions that other records like LOC, RP, and TXT are not mandatory and that the service can't trust the LOC to locate a host.

- Checking DNS information of **EC-council** website:



The screenshot shows the NSLOOKUP website interface with the search results for "codered.eccouncil.org". The navigation bar and breadcrumb trail are the same as in the previous screenshot. The main heading is "NSLOOKUP: look up and find IP addresses in the DNS". Below the heading is a paragraph explaining the tool's purpose: "Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name into an IP address." This is followed by a disclaimer: "This is the right place for you to check how your web hosting company or domain name registrar has set up the DNS stuff for your domain, how your dynamic DNS is going, or to search IP addresses or research any kind of e-mail abuse (UBE/UCE spam) or internet abuse. This online service is for private non-commercial use only. Please do not abuse. No automated queries. No bots." The search form is titled "NSlookup" and contains three input fields: "Domain:" with a text box containing "codered.eccouncil.org", "Server:" with a text box containing "localhost", and "Query:" with a dropdown menu showing "A (IPv4 address)". A "Look it up" button is to the right of the query field. Below the form is a detailed explanation of the NSLOOKUP utility, its purpose, and how to use it. It mentions that the utility is a Unix tool and provides a link to the nslookup manual. It also explains that the website's online service can query a specific DNS server, but in most cases, it's sufficient to use the KLOTH.NET default nameserver "localhost/127.0.0.1". It notes that the service can perform PTR queries (reverse lookup) but only if the IP address owner has inserted a PTR record. It also mentions that other records like LOC, RP, and TXT are not mandatory and that the service can't trust the LOC to locate a host. The search results are displayed in a box with the following text: "here is the nslookup result for codered.eccouncil.org from server localhost, querytype=A: DNS server handling your query: localhost DNS server's address: 127.0.0.1#53 Non-authoritative answer: Name: codered.eccouncil.org Address: 104.18.9.180 Name: codered.eccouncil.org Address: 104.18.8.180".