VIT-AP UNIVERSITY

# CSE4026: CYBER SECURITY

# A PROJECT REPORT ON

## E-MAIL FORENSICS USING EMAILTRACKERPRO AND SMARTWHOIS

**NAME:** DASARI SRIKANTH

**REG.NO:** 20BCE7076

School of Computer Science and Engineering

**LAB SLOT:** L29+L30

**DATE:** 25 – 12 – 2022

**SUBMITTED TO:**
Prof. Dr. Kumar Debasis

## ABSTRACT:

Over the last decades, email has been the major carrier for transporting spam and malicious contents over the network. Email is also the primary source of numerous criminal activities on the Internet. Computer Forensics is a systematic process to retain and analyse saved emails for the purpose of legal proceedings and other civil matters. Email analysis is challenging due to not only various fields that can be forged by hackers or malicious users, but also the flexibility of composing, editing, deleting of emails using offline or online email applications.

Towards this direction, a number of opensource forensics tools have been widely used by the practitioners. However, these tools have been developed in an isolated manner rather than a collaborative approach. Given that email forensic tool users need to understand to what extent a tool would be useful for his/her circumstances and conducting forensic analysis accordingly.

Email forensics refers to studying the source and content of electronic mail as evidence, identifying the actual sender and recipient of a message, date it was sent and etc. Emails frequently contain malicious viruses, threats and scams that can result in the loss of data, confidential information and even identity theft.

The tools namely emailtrackerpro and SmartwhoIs provide an easy-to-use browser format, automated reporting and easy tool bar access features. These tools help to identify the point of origin of the message, trace the path traversed by the message and also to identify the phishing emails that try to obtain confidential information from the receiver.

## INDEX

1. Introduction… ................................................................. 4
2. Problem Definiton… ......................................................... 5
   a. Malware......................................................................6
   b. Spam and Phishing........................................................6
   c. Social Engineering .........................................................7
   d. Entities with malicious intent.......................................7
   e. Unintentional acts by authorized users ....................... 7
3. Objectives ..........................................................................8
4. Methodology....................................................................... 9
5. Results and discussion
   a. Emailtrackerpro .......................................................11
   b. Samrtwhois ............................................................... 16
6. Conclusion and future scope ............................................ 20
7. References ........................................................................ 21

# INTRODUCTION:

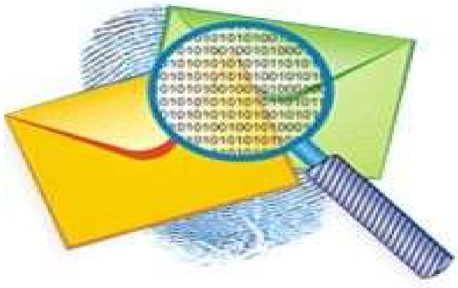
Email forensics is exactly what it sounds like. The analysis of emails and the content within to determine the legitimacy, source, date, time, the actual sender, and recipients in a forensically sound manner. The aim of this is to provide admissible digital evidence for use in civil or criminal courts.

Email is one of the most common ways people communicate, ranging from internal meeting requests, to distribution of documents and general conversation. Emails are now being used for all sorts of communication including providing confidentiality, authentication, non-repudiation and data integrity. As email usage increases, attackers and hackers began to use emails for malicious activities.

Spam emails are a major source of concern within the Internet community. Emails are more vulnerable to be intercepted and might be used by hackers to learn of secret communication.

Most organisations have specific internal and external email policies in place to help safeguard their data, intellectual property, finances, and reputation. However, this does not always stop individuals from violating these policies to the detriment of their employer. These violations can present themselves in the form of forbidden file transfers, data breaches, indecent imagery, and incriminating email threads.

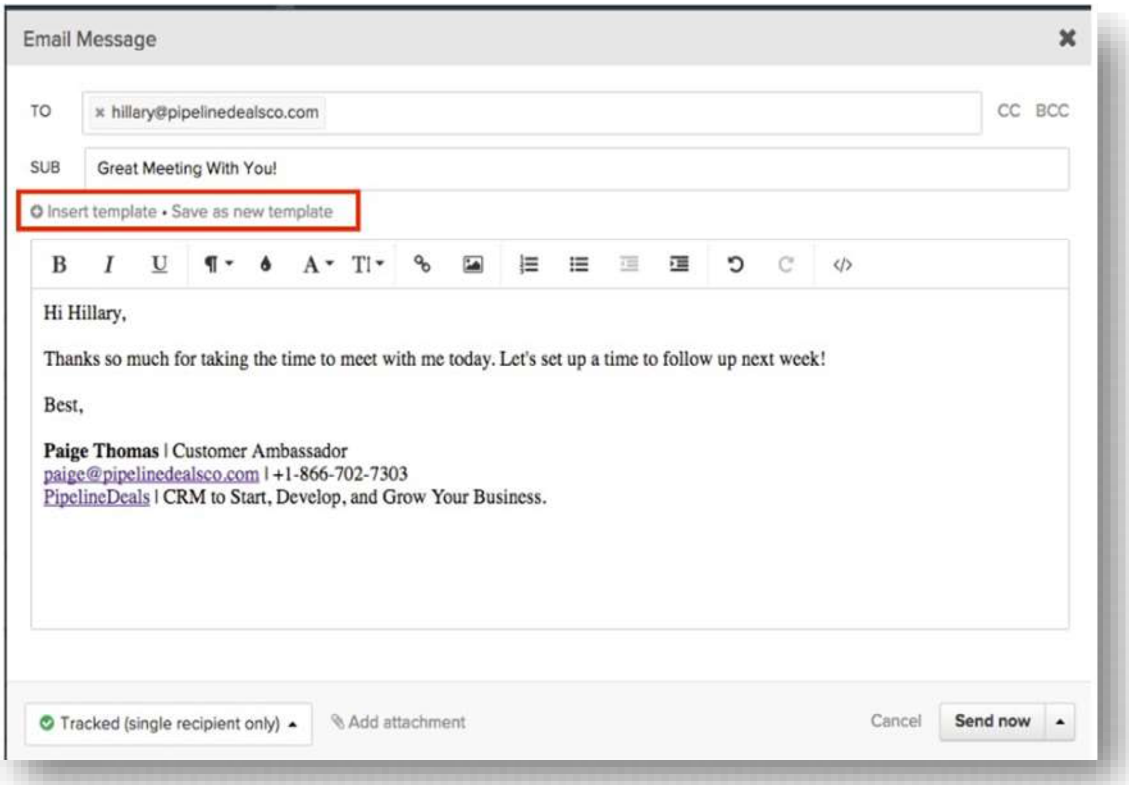
These tools not only offers the ability to trace an e-mail using the e-mail header but it also comes with a spam filter, which scans each e-mail as it arrives and warns the user if it's suspected spam. Essentially stopping spam e-mail before it reaches its intended recipient.



## PROBLEM DEFINITION:

Today, email has become the backbone of many professionals daily activity. Email is one communication technology that can be used to exchange information, data, and etc. Emails are most frequently used in our everyday life, we rely on email's confidentiality and integrity to exchange data and communication. The development of email technology not only can be opened using a computer but can be opened using a smartphone.

As the Internet has become open, public and widely used as a source of data transmission and exchanging messages between criminals, terrorists and those who have illegal motivations. Moreover, it can be used for exchanging important data between various military and financial institutions, or even ordinary citizens.



Email Message
TO
CC BCC
SUB
Insert template • Save as new template
Tracked (single recipient only)
Add attachment
Cancel
Send now

TO: hillary@pipelinedealsco.com

SUB: Great Meeting With You!

Hi Hillary,

Thanks so much for taking the time to meet with me today. Let's set up a time to follow up next week!

Best,

**Paige Thomas** | Customer Ambassador
paige@pipelinedealsco.com | +1-866-702-7303
PipelineDeals | CRM to Start, Develop, and Grow Your Business.

**E-mail format**

Because e-mail is widely deployed, well understood, and used to communicate with untrusted, external organizations, it is frequently the target of attacks. Attackers can exploit e-mail to gain control over an organization, access confidential information, or disrupt IT access to resources. Common threats to e-mail systems include the following:

## 1.MALWARE:

Increasingly, attackers are taking advantage of e-mail to deliver a variety of attacks to organizations through the use of malware, or “malicious software,” that include viruses, worms, Trojan horses, and spyware. These attacks, if successful, may give the malicious entity control over workstations and servers, which can then be exploited to change privileges, gain access to sensitive information, monitor users’ activities, and perform other malicious actions.

## 2.SPAM AND PHISHING:

Unsolicited commercial e-mail, commonly referred to as spam, is the sending of unwanted bulk commercial e-mail messages. Such messages can disrupt user productivity, utilize IT resources excessively, and be used as a distribution mechanism for malware. Related to spam is phishing, which refers to the use of deceptive computer-based means to trick individuals into responding to the e-mail and disclosing sensitive information. Compromised e-mail systems are often used to deliver spam messages and conduct phishing attacks using an otherwise trusted e-mail address.

## 3. SOCIAL ENGINEERING:

Rather than hack into a system, an attacker can use e-mail to gather sensitive information from an organization’s users or get users to perform actions that further an attack. A common social engineering attack is e-mail spoofing, in which one person or program successfully masquerades as another by falsifying the sender information shown in e-mails to hide the true origin.

## 4. ENTITIES WITH MALICIOUS INTENT:

Malicious entities may gain unauthorized access to resources elsewhere in the organization’s network via a successful attack on a mail server. For example, once the mail server is compromised, an attacker could retrieve users’ passwords, which may grant the attacker access to other hosts on the organization’s network.

## 5. UNINTENTIONAL ACTS BY AUTHORIZED USERS:

Not all security threats are intentional. Authorized users may inadvertently send proprietary or other sensitive information via e-mail, exposing the organization to embarrassment or legal action.

Towards this direction, a number of open source forensics tools have been widely used by the practitioners like smartwhois and emailtrackerpro. However, these tools have been developed in an isolated manner rather than a collaborative approach.

## OBJECTIVES:

EmailForensic science is a critical element of the criminal justice system. Scientists examine and analyze evidence from crime scenes and elsewhere to develop objective findings that can assist in the investigation and prosecution of perpetrators of crime or absolve an innocent person from suspicion.

Email forensic readiness plan will have the following goals: To gather admissible evidence legally without interfering with business processes. To gather evidence targeting potential crimes and disputes that could have adverse impact on an organization.

Within a row, the development technology of higher cybercrime such as email fraud catching cybercrime offenders need evidence to be submitted to a court, for obtain evidence can use tools like emailtrackerpro and smartwhois to analyze network traffic on live networks. Over the last decades, email has been the major carrier for transporting spam and malicious contents over the network. Email is also the primary source of numerous criminal activities on the Internet. E-mail security relies on principles of good planning and management that provide for the security of both the e-mail system and the IT infrastructure. With proper planning, system management, and continuous monitoring, organizations can implement and maintain effective security.

## METHODOLOGY:

One of the important means of exchanging information widely used on the Internet medium is the e-mail. Email messages are digital evidence that has been become one of the important means to adopt by courts in many countries and societies as evidence relied upon in condemnation, that prompts the researchers to work continuously to develop email analysis tool using the latest technologies to find digital evidence from email messages to assist the forensic expertise into to analyse email groups.

Here we use two main tools namely Emailtrackerpro and Smartwhois as to analyse the spam and to check any threat levels to the email that we are getting daily through help of header

## 1. EMAIL TRACKER PRO:

EMailTrackerPro is a Windows application that analyzes header information contained in every e-mail as a way to trace the route taken by the mail after it was sent. E-mail header information details the path e-mail takes from its source to its destination. The application also tracks the IP (Internet Protocol) address it was sent from and the geographical location where the mail originated. The program also attempts to recognize and cut through the misdirection and forged headers that are often the hallmark of spammers by looking for logical paths for e-mail to be sent on, she added.

EMailTrackerPro can also determine what continent a particular IP address is located on. When combined with VisualRoute, Visualware's trace route application, eMailTrackerPro can pinpoint IP addresses within countries and cities.

Though the tracking of header information and the like can already be done manually, expect that eMailTrackerPro will appeal to people who want analysis done automatically or a graphical user interface through which to do such analysis. The software may also appeal to users who are attempting to do basic verification of claims made in e-mail or to protect themselves from online auction fraud.The software can be used with any e-mail program, but is integrated with Microsoft Corp.'s Outlook. EMailTrackerPro is immediately available worldwide and can be purchased through Visualware's Web site also.

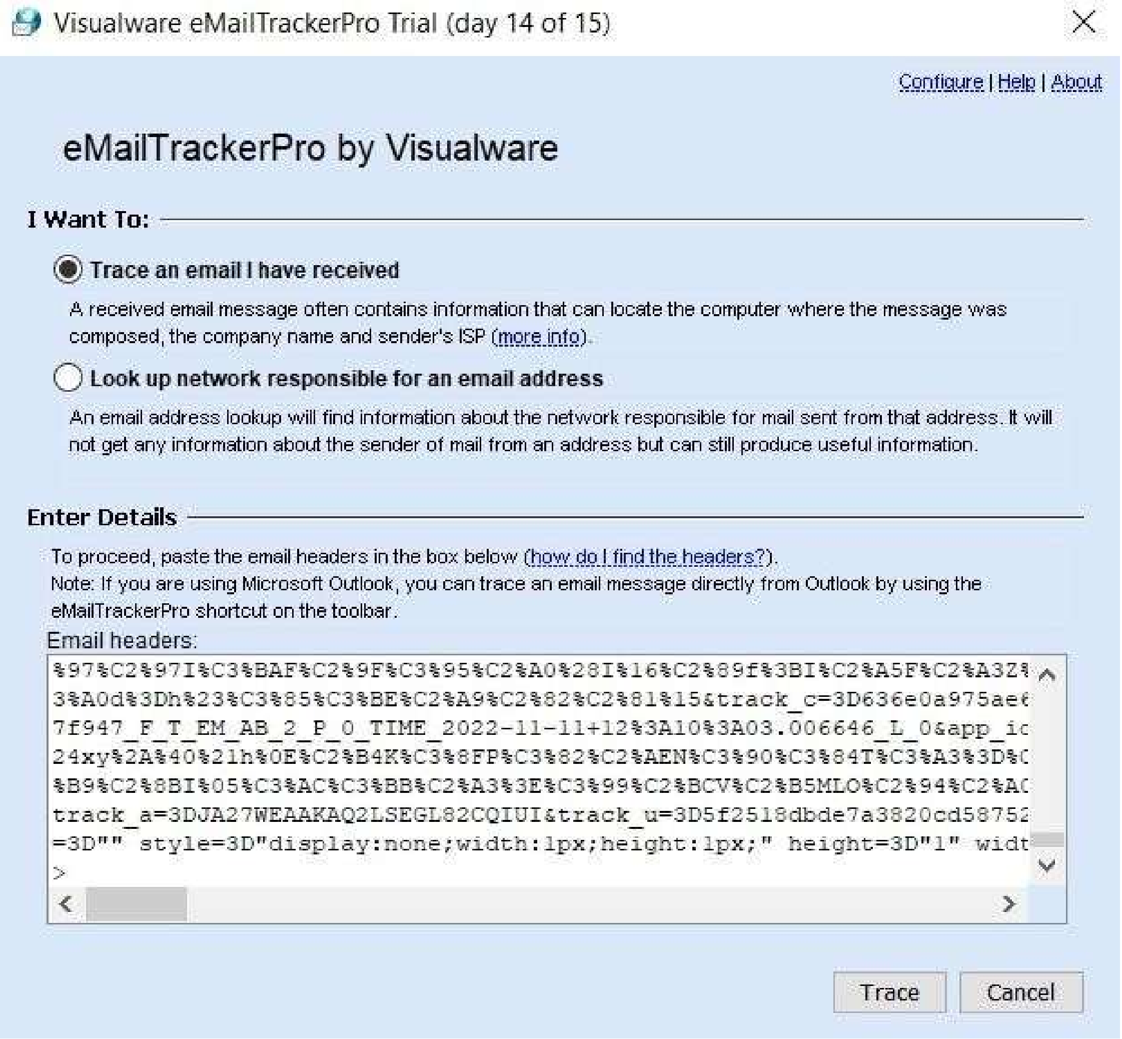
For a deeper search, the software will show you also the IP address of the source and how many hops are from the source to the destination. You just need to obtain the email headers. This is an operation that can be done very easy by entering in the Outlook Express and copy the properties of the email.

The program has also an inbuilt email client in order to help you quickly track emails. If you consider that you found a spam or a virus email, you can report it through a quick reporting system.

eMailTrackerPro helps identify the true source of emails to help track suspects, verify the sender of a message, trace and report email abusers. The trace analysis reports the sender's IP address, estimated location, network and domain information. eMailTrackerPro also helps uncover misdirection a technique often used to disguise the sender to expose the true origins of the email.

To track an email message, we have copy and paste the header of the email in eMailTrackerPro to start the tool. A basic trace will be shown on the main Graphical User Interface and a summary report can be obtained. The summary report provides an option to report the abuse of the particular email address to the administrators of the sender and/or victim networks and also contains some critical information that can be useful for forensic analysis and investigation. The report includes the location of the IP address from which the email was sent, and if this cannot be found, the report at least includes the location of the target’s ISP. The report also includes the domain contact information of the network owner or the ISP, depending on the sender email address.

## 1.1 RESULTS AND DISCUSSION:



Visualware eMailTrackerPro Trial (day 14 of 15)

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.

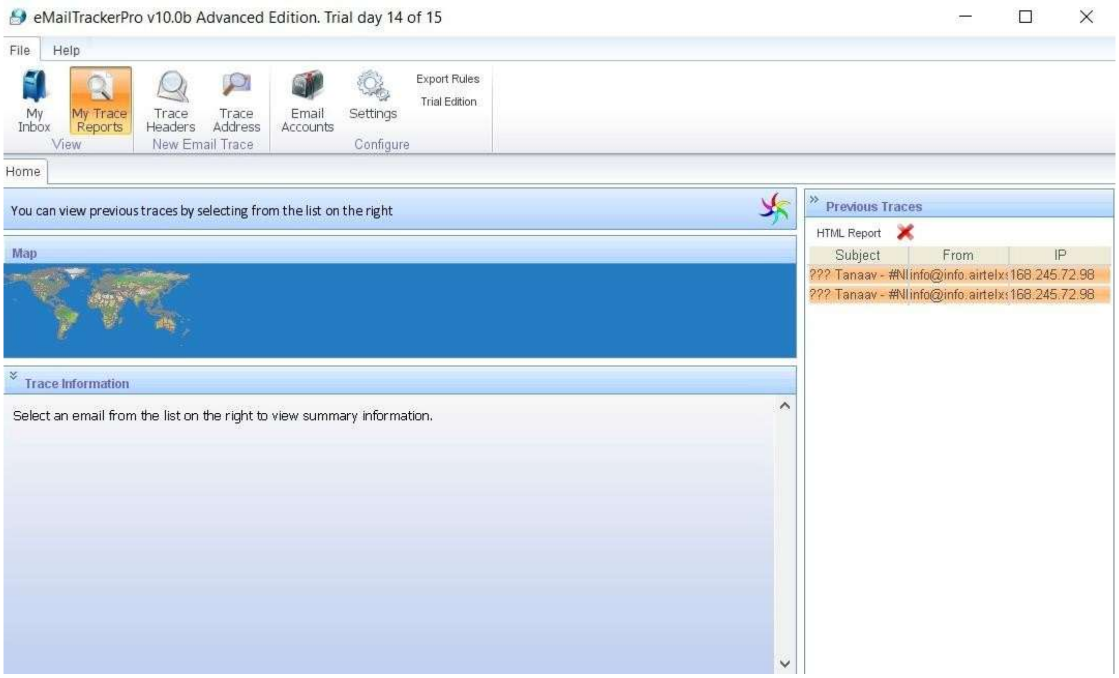
Enter Details

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:

```
%97%C2%97I%C3%BAF%C2%9F%C3%95%C2%A0%28I%16%C2%89f%3BI%C2%A5F%C2%A3Z%
3%A0d%3Dh%23%C3%85%C3%BE%C2%A9%C2%82%C2%81%15&track_c=3D636e0a975ae
7f947_F_T_EM_AB_2_P_0_TIME_2022-11-11+12%3A10%3A03.006646_L_0&app_i
24xy%2A%40%21h%0E%C2%B4K%C3%8FP%C3%82%C2%AEN%C3%90%C3%84T%C3%A3%3D%
%B9%C2%8BI%05%C3%AC%C3%BB%C2%A3%3E%C3%99%C2%BCV%C2%B5MLO%C2%94%C2%A
track_a=3DJA27WEAAKAQ2LSEGL82CQIUI&track_u=3D5f2518dbde7a3820cd58752
=3D"" style=3D"display:none;width:1px;height:1px;" height=3D"1" widt
>
```

eMailTrackerPro analyzes the header of an email to detect the IP address of the machine that sent the message so that the sender can be tracked down. All email messages contain a header, located at the top of the email. The header contains the source of an email in the “From” line, while in the “Received” lines, the header lists every point the email passed through on its journey, along with the date and time. The message header provides an audit trail of every machine the email has passed through.

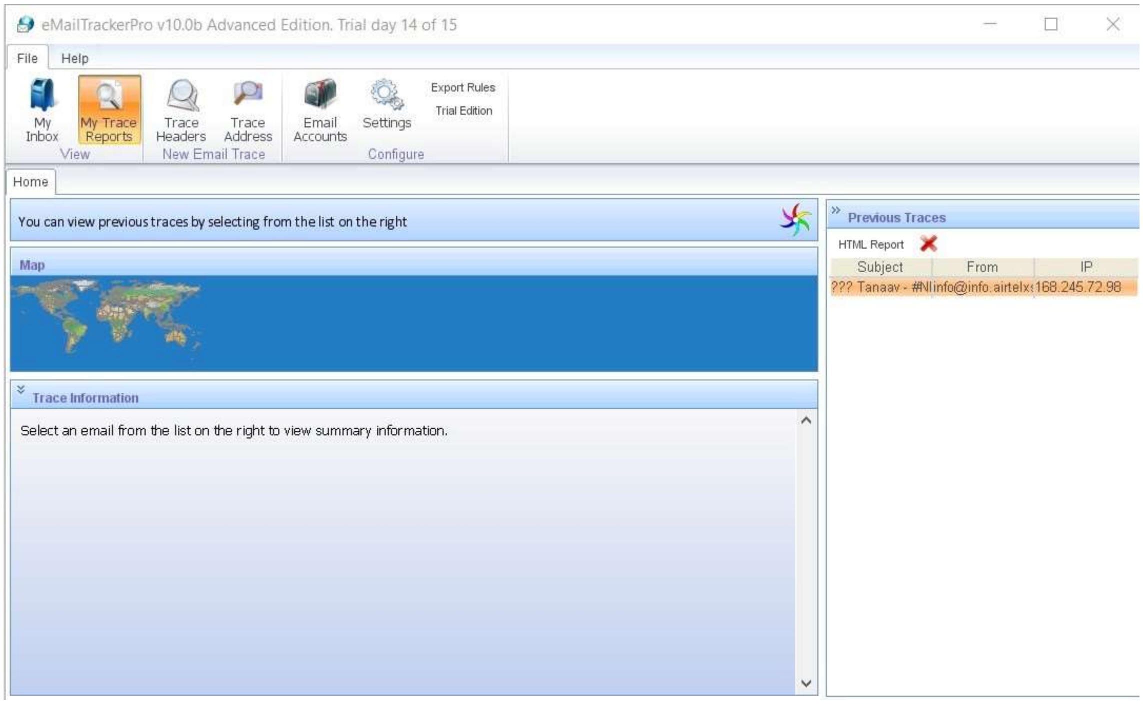


You can view previous traces by selecting from the list on the right

Select an email from the list on the right to view summary information.

| Subject | From | IP |
|---|---|---|
| ??? Tanaav - #Nl | info@info.airtelx | 168.245.72.98 |
| ??? Tanaav - #Nl | info@info.airtelx | 168.245.72.98 |

This application is very useful when it comes to tracking and reporting email abusers. Depending on what we choose we can obtain the address from which the sender sent the email, the location of the server, the email address of the contact person of the server, a contact telephone number and eventually

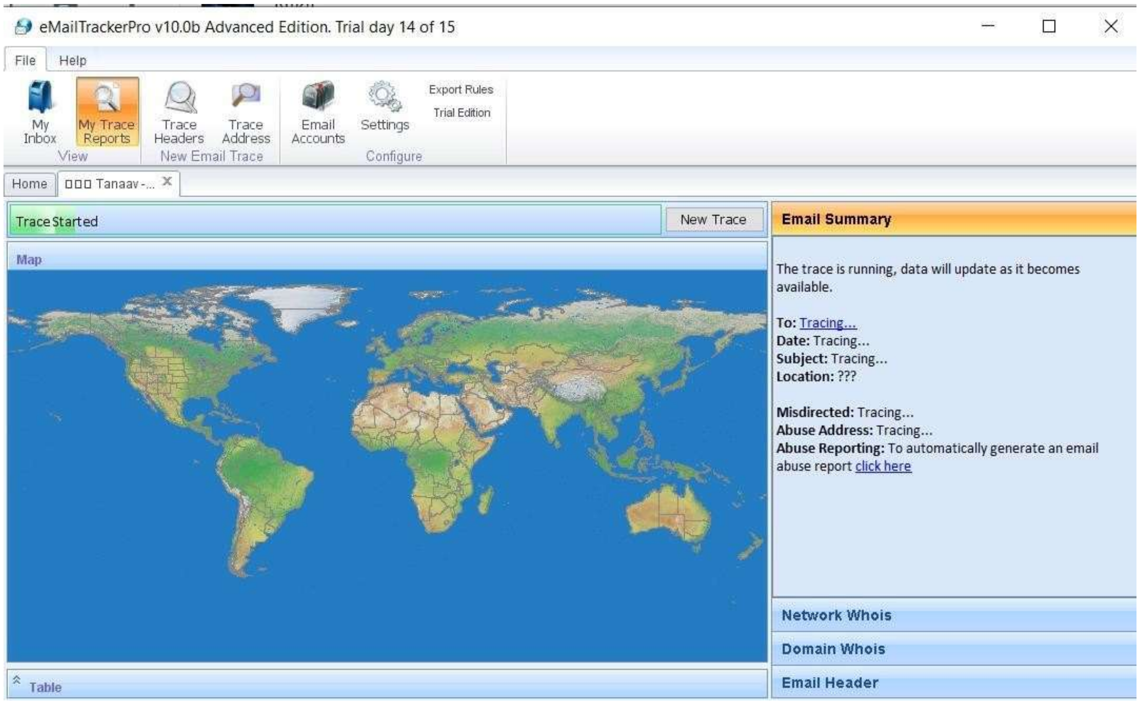


You can view previous traces by selecting from the list on the right

Select an email from the list on the right to view summary information.

| Subject | From | IP |
|---|---|---|
| ??? Tanaav - #Nl | info@info.airtelx | 168.245.72.98 |

The domain registration details provide information such as who has registered the website address, from what time and how many emails have been sent from that address, and etc.



Trace Started

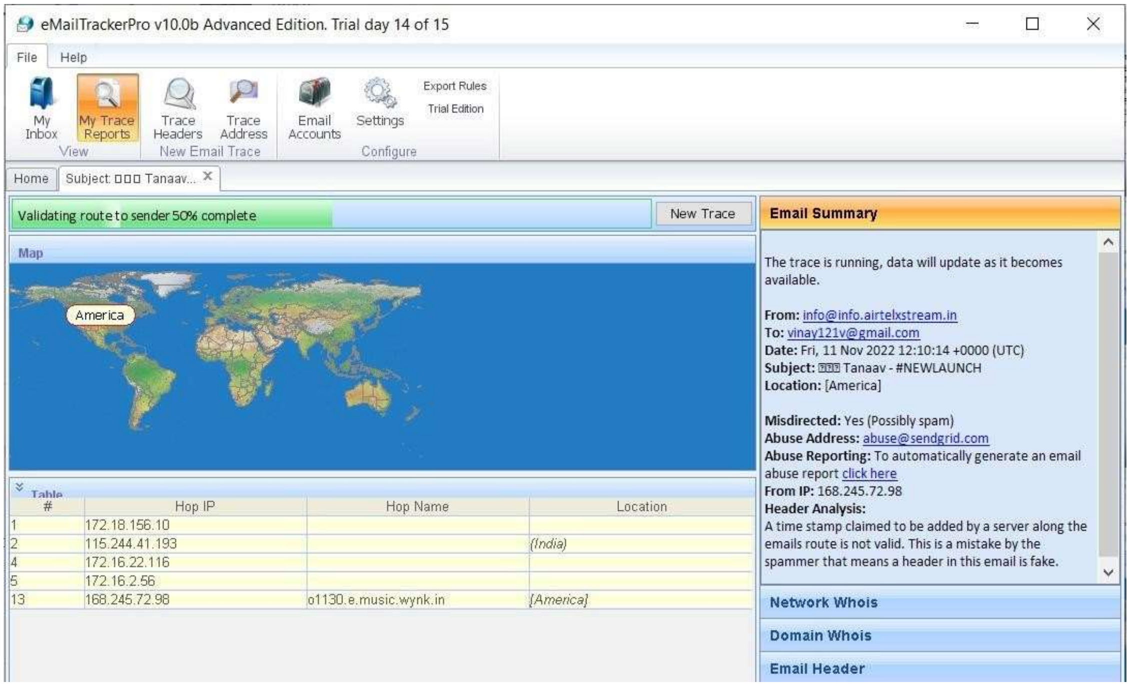
**Email Summary**

The trace is running, data will update as it becomes available.

**To:** Tracing...
**Date:** Tracing...
**Subject:** Tracing...
**Location:** ???

**Misdirected:** Tracing...
**Abuse Address:** Tracing...
**Abuse Reporting:** To automatically generate an email abuse report click here

The built-in location database in eMailTrackerPro helps to track emails to a country or region of the world, showing information on a global map.



Validating route to sender 50% complete

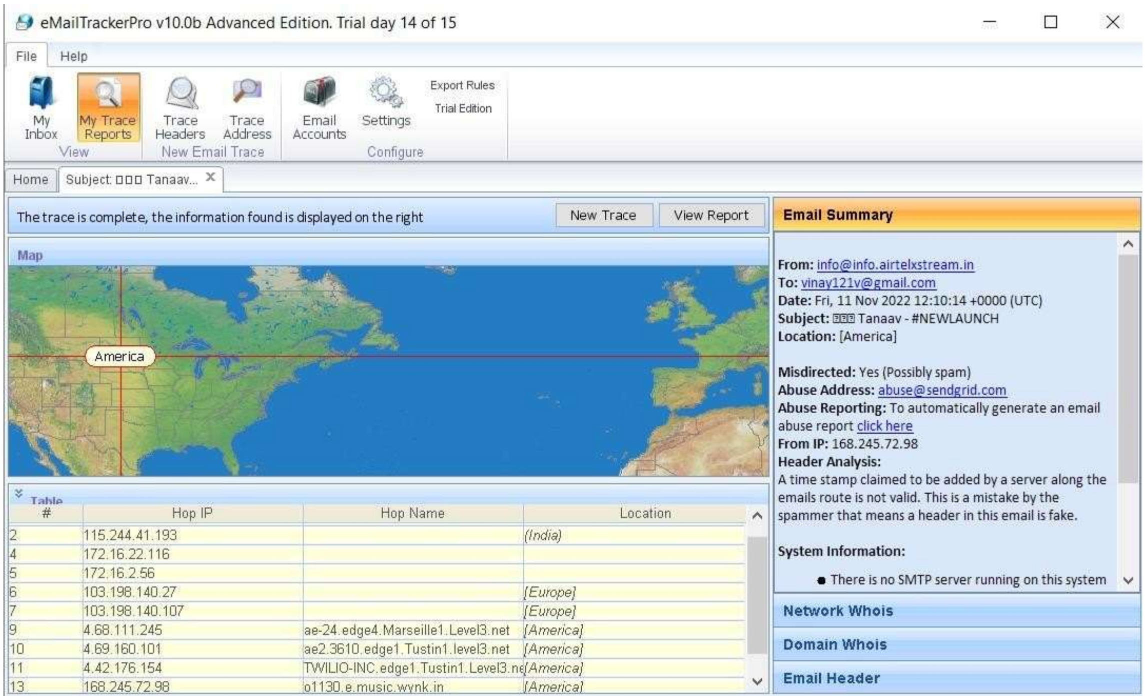
| # | Hop IP | Hop Name | Location |
|---|---|---|---|
| 1 | 172.18.156.10 | | |
| 2 | 115.244.41.193 | | *(India)* |
| 4 | 172.16.22.116 | | |
| 5 | 172.16.2.56 | | |
| 13 | 168.245.72.98 | o1130.e.music.wynk.in | *[America]* |

**Email Summary**

The trace is running, data will update as it becomes available.

**From:** info@info.airtelxstream.in
**To:** vinay121v@gmail.com
**Date:** Fri, 11 Nov 2022 12:10:14 +0000 (UTC)
**Subject:** □□□ Tanaav - #NEWLAUNCH
**Location:** [America]

**Misdirected:** Yes (Possibly spam)
**Abuse Address:** abuse@sendgrid.com
**Abuse Reporting:** To automatically generate an email abuse report click here
**From IP:** 168.245.72.98
**Header Analysis:**
A time stamp claimed to be added by a server along the emails route is not valid. This is a mistake by the spammer that means a header in this email is fake.



The trace is complete, the information found is displayed on the right

| # | Hop IP | Hop Name | Location |
|---|---|---|---|
| 2 | 115.244.41.193 | | (India) |
| 4 | 172.16.22.116 | | |
| 5 | 172.16.2.56 | | |
| 6 | 103.198.140.27 | | [Europe] |
| 7 | 103.198.140.107 | | [Europe] |
| 9 | 4.68.111.245 | ae-24.edge4.Marseille1.Level3.net | [America] |
| 10 | 4.69.160.101 | ae2.3610.edge1.Tustin1.level3.net | [America] |
| 11 | 4.42.176.154 | TWILIO-INC.edge1.Tustin1.Level3.ne | [America] |
| 13 | 168.245.72.98 | o1130.e.music.wynk.in | [America] |

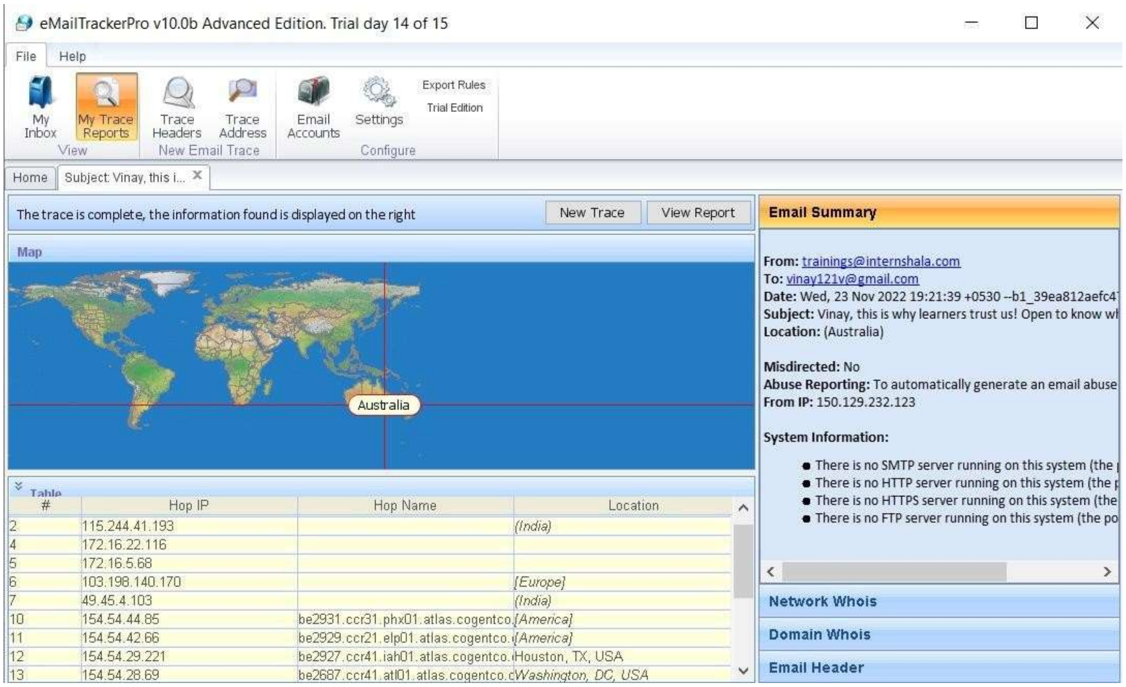
**Email Summary**

**From:** info@info.airtelxstream.in
**To:** vinay121v@gmail.com
**Date:** Fri, 11 Nov 2022 12:10:14 +0000 (UTC)
**Subject:** □□□ Tanaav - #NEWLAUNCH
**Location:** [America]

**Misdirected:** Yes (Possibly spam)
**Abuse Address:** abuse@sendgrid.com
**Abuse Reporting:** To automatically generate an email abuse report click here
**From IP:** 168.245.72.98
**Header Analysis:**
A time stamp claimed to be added by a server along the emails route is not valid. This is a mistake by the spammer that means a header in this email is fake.

**System Information:**

- There is no SMTP server running on this system



The trace is complete, the information found is displayed on the right

| # | Hop IP | Hop Name | Location |
|---|---|---|---|
| 2 | 115.244.41.193 | | (India) |
| 4 | 172.16.22.116 | | |
| 5 | 172.16.5.68 | | |
| 6 | 103.198.140.170 | | [Europe] |
| 7 | 49.45.4.103 | | (India) |
| 10 | 154.54.44.85 | be2931.ccr31.phx01.atlas.cogentco. | [America] |
| 11 | 154.54.42.66 | be2929.ccr21.elp01.atlas.cogentco. | [America] |
| 12 | 154.54.29.221 | be2927.ccr41.iah01.atlas.cogentco. | Houston, TX, USA |
| 13 | 154.54.28.69 | be2687.ccr41.atl01.atlas.cogentco.c | Washington, DC, USA |

**Email Summary**

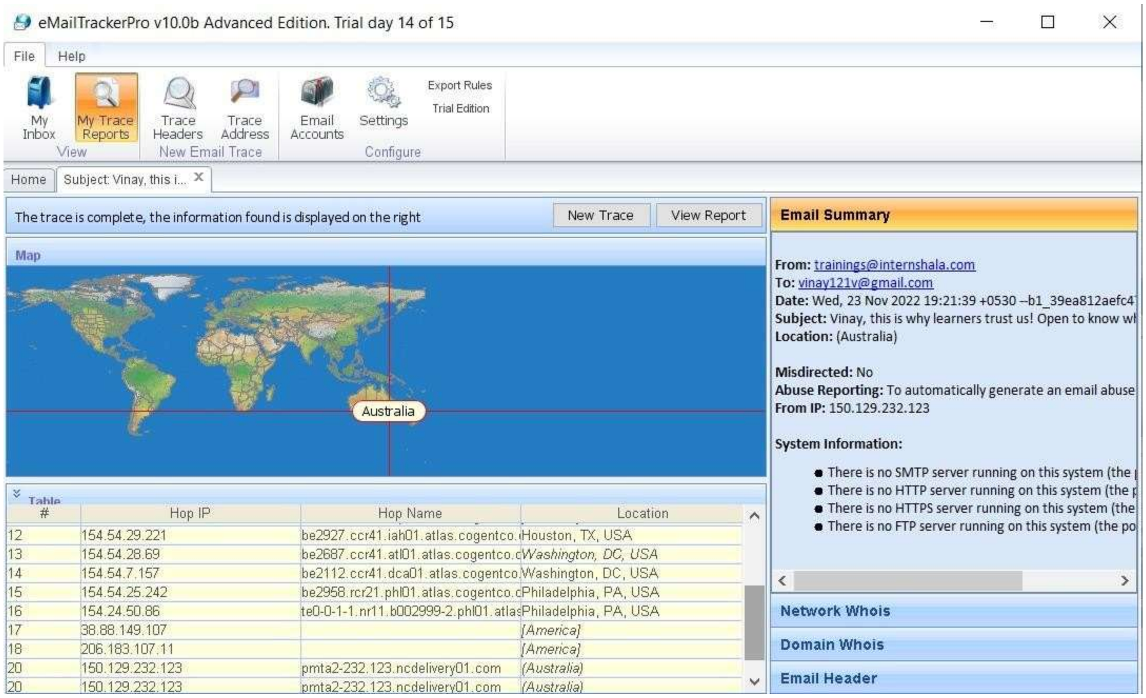
**From:** trainings@internshala.com
**To:** vinay121v@gmail.com
**Date:** Wed, 23 Nov 2022 19:21:39 +0530 --b1_39ea812aefc4
**Subject:** Vinay, this is why learners trust us! Open to know wh
**Location:** (Australia)

**Misdirected:** No
**Abuse Reporting:** To automatically generate an email abuse
**From IP:** 150.129.232.123

**System Information:**

- There is no SMTP server running on this system (the
- There is no HTTP server running on this system (the
- There is no HTTPS server running on this system (the
- There is no FTP server running on this system (the po

**Example of emailtrackerpro**



The trace is complete, the information found is displayed on the right

| # | Hop IP | Hop Name | Location |
|---|---|---|---|
| 12 | 154.54.29.221 | be2927.ccr41.iah01.atlas.cogentco.c | Houston, TX, USA |
| 13 | 154.54.28.69 | be2687.ccr41.atl01.atlas.cogentco.c | *Washington, DC, USA* |
| 14 | 154.54.7.157 | be2112.ccr41.dca01.atlas.cogentco. | Washington, DC, USA |
| 15 | 154.54.25.242 | be2958.rcr21.phl01.atlas.cogentco.c | Philadelphia, PA, USA |
| 16 | 154.24.50.86 | te0-0-1-1.nr11.b002999-2.phl01.atlas | Philadelphia, PA, USA |
| 17 | 38.88.149.107 | | *[America]* |
| 18 | 206.183.107.11 | | *[America]* |
| 20 | 150.129.232.123 | pmta2-232.123.ncdelivery01.com | *(Australia)* |
| 20 | 150.129.232.123 | pmta2-232.123.ncdelivery01.com | *(Australia)* |

**Email Summary**

**From:** trainings@internshala.com
**To:** vinay121v@gmail.com
**Date:** Wed, 23 Nov 2022 19:21:39 +0530 --b1_39ea812aefc4
**Subject:** Vinay, this is why learners trust us! Open to know wh
**Location:** (Australia)

**Misdirected:** No
**Abuse Reporting:** To automatically generate an email abuse
**From IP:** 150.129.232.123

**System Information:**

- There is no SMTP server running on this system (the
- There is no HTTP server running on this system (the p
- There is no HTTPS server running on this system (the
- There is no FTP server running on this system (the po

## 2. SMARTWHOIS:

It's interesting to look at the situation from the standpoint of the user whose IP address is being queried or otherwise analyzed. Is it safe to reveal it? Do we need to hide it? The answer is not an easy one, and it's outside the scope of this tutorial. In brief, if we are looking for anonymity, we should consider implementing some measures to hide it. If you're not particularly concerned about anonymity or privacy, there are still situations where hiding the IP address might be advisable. Consider a news group posting that you made today using an alias, and another one that you made a month ago, under your real name. If you have a static IP address, searching news groups for  IP address will show all your postings, no matter what name you used.

SmartWhois is a great starting point for an online investigation. When we know the IP address or domain name that we want to learn more about. SmartWhoIs is a freeware network utility to look up all the available information about an IP address, hostname or domain, including country, state or province, city, name of the network provider, administrator and technical support contact information. Using SmartWhoIs, we can also query about multiple IP addresses, hostnames or domains at a time.

SmartWhois is a useful network information utility that allows you to find out all available information about an IP address, host name, or domain, including country, state or province, city, name of the network provider, administrator, technical support, and abuse contact information. It is an Internet program that allows users to query a database of domains and IP addresses to retrieve information about the owners, administrators, geographic location, etc. As the name suggests, SmartWhois is a smart, feature-rich Whois utility capable of performing such queries.

People who hate spam or want to identify the origin of suspicious e-mail messages can check the message header and locate the real sender we can also send e-mail to the network administrator with a mouse click.

People who want to identify the origin of suspicious e-mail messages by studying the headers can find out with the help of smartwhois tool.

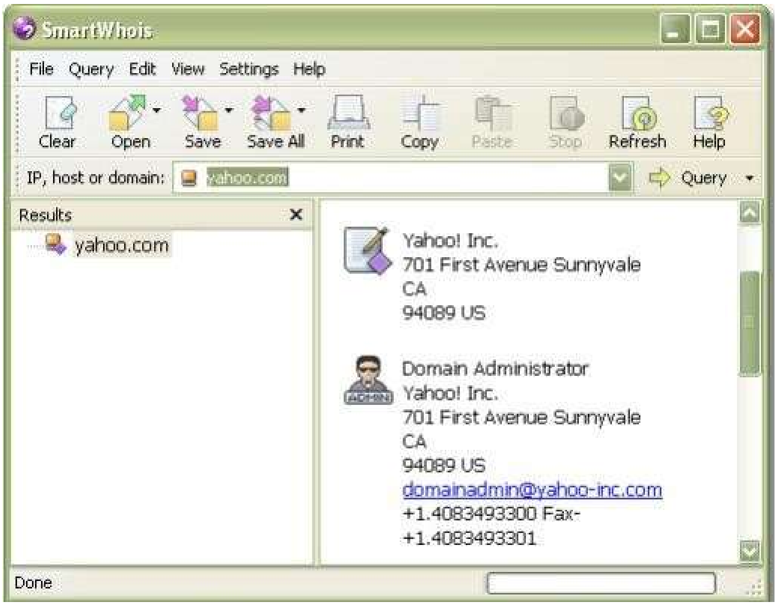
## 2.1 RESULTS AND DISCUSSION:

### Domain vs ip address

Understanding the difference between domain and IP address / host name queries is the key to successful usage of SmartWhois. When trying to find information on a particular web site, users are frequently confused about what kind of query they should perform and what they should type in the input field

Suppose that you want to check who owns yahoo.com, a popular site on weather. To find the owner of a web site, you should find out who owns the domain. In this example, the domain name is "yahoo.com." So you should type "yahoo.com" in the input field, click on the Query button, and select As Domain:

A domain is a logical region of the Internet. Domain names consist of one or several parts separated by periods, for example: "yahoo.com." You can refer to all of the computers that share the right-most portion of a name as being in the same domain, for example: "weather.yahoo.com" and "finance.yahoo.com" are both in the "yahoo.com" domain.



IP, host or domain: yahoo.com

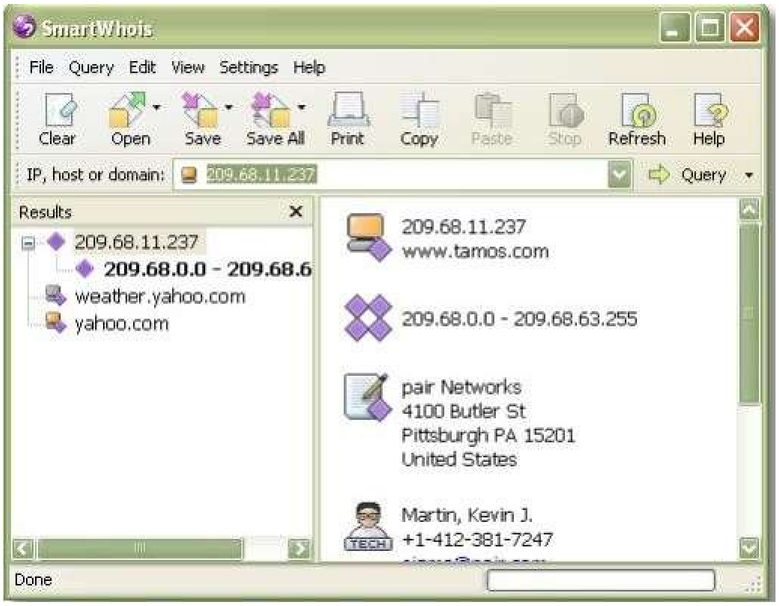
yahoo.com

Yahoo! Inc.
701 First Avenue Sunnyvale
CA
94089 US

Domain Administrator
Yahoo! Inc.
701 First Avenue Sunnyvale
CA
94089 US
domainadmin@yahoo-inc.com
+1.4083493300 Fax-
+1.4083493301

In just a few seconds, you see that "yahoo.com" belongs to Yahoo!, a California-based company. we enter "yahoo.com" rather than "weather.yahoo.com", because "weather.yahoo.com" is not a second-level domain In most of the cases we should query only second-level domain names, such as "yahoo.com" rather than third-level domain names, such as "weather.yahoo.com."

Every computer connected to the Internet is assigned a unique number known as an Internet Protocol (IP) address. This number identifies each sender or receiver of information that is sent in packets across the Internet. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 4.90.50.60 or 208.1.0.15 could be valid IP addresses.



IP, host or domain: 209.68.11.237

- 209.68.11.237
  - 209.68.0.0 - 209.68.6
- weather.yahoo.com
- yahoo.com

209.68.11.237
www.tamos.com

209.68.0.0 - 209.68.63.255

pair Networks
4100 Butler St
Pittsburgh PA 15201
United States

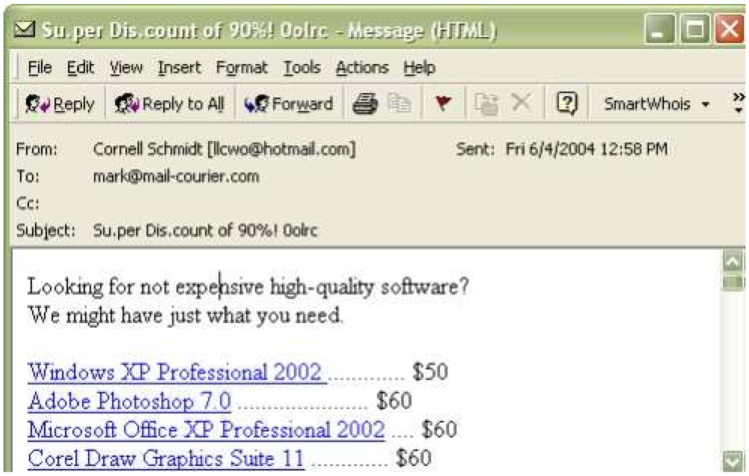
Martin, Kevin J.
+1-412-381-7247

That's right; "tamos.com" belongs to TamoSoft, a New Zealand-based company. This leads us to an important observation that Domain and IP address / host name queries usually give you different results, and this is quite understandable. Query a domain to find out who owns it. Query a host name or IP address to find out where the computer with the given host name is located and who owns the corresponding range of IP addresses. "Tamos.com" is owned by a company based in New Zealand, but the company's web server, "www.tamos.com" at the time of writing, this corresponds to 209.68.11.237 is located in the USA in the data center that belongs to Pair Networks.

**how to avoid spam:**

Every e-mail message that we receive includes so called "headers," that messy block of text that precedes the actual message body. Headers are included in every message, but they aren't normally displayed to the user. However, every e-mail client can be configured to show this information, and the SmartWhois add-in can help you quickly display it. Headers contain information about the path the message took before reaching our e-mail box. Each computer that handled the message en route added something to the header, and it is this additional info we can use to help trace the message back to its source. Reading and understanding e-mail headers is not a black art, but it requires some knowledge and practice. Here, we can simply show case you how we can use SmartWhois to get information on the IP addresses that you can find in the headers.

**Here is a typical spam message:**

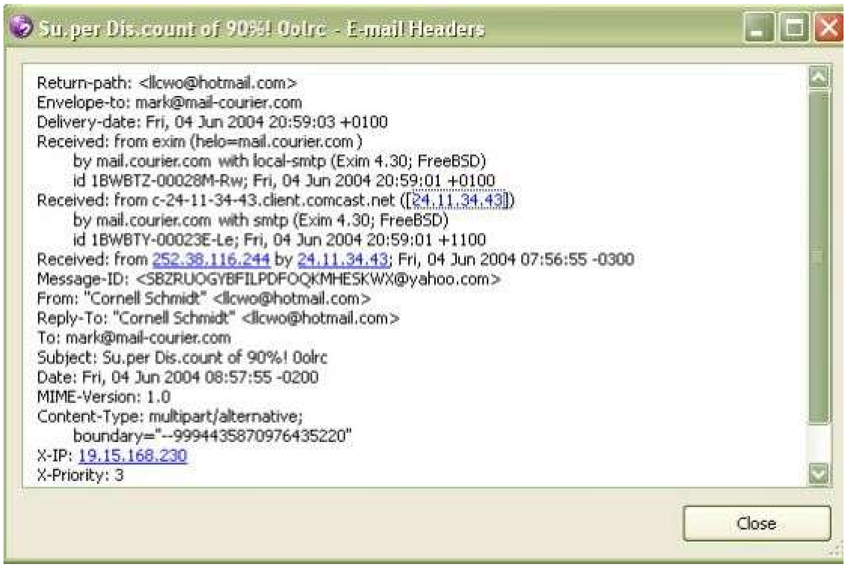

Su.per Dis.count of 90%! 0olrc - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward
SmartWhois

From: Cornell Schmidt [llcwo@hotmail.com] Sent: Fri 6/4/2004 12:58 PM
To: mark@mail-courier.com
Cc:
Subject: Su.per Dis.count of 90%! 0olrc

Looking for not expensive high-quality software?
We might have just what you need.

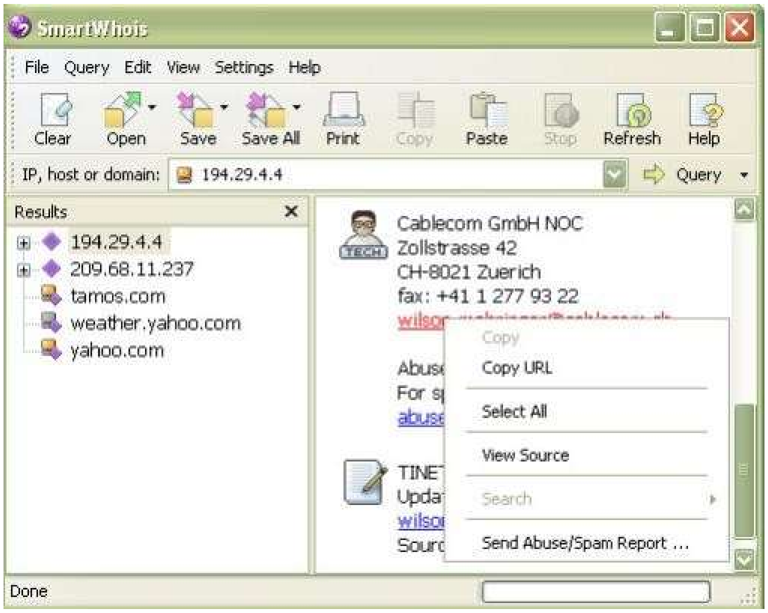
| | |
|---|---|
| Windows XP Professional 2002 | $50 |
| Adobe Photoshop 7.0 | $60 |
| Microsoft Office XP Professional 2002 | $60 |
| Corel Draw Graphics Suite 11 | $60 |

after sending it to smartwhois:



```
Return-path: <llcwo@hotmail.com>
Envelope-to: mark@mail-courier.com
Delivery-date: Fri, 04 Jun 2004 20:59:03 +0100
Received: from exim (helo=mail.courier.com )
      by mail.courier.com  with local-smtp (Exim 4.30; FreeBSD)
      id 1BWBTZ-00028M-Rw; Fri, 04 Jun 2004 20:59:01 +0100
Received: from c-24-11-34-43.client.comcast.net ([24.11.34.43])
      by mail.courier.com  with smtp (Exim 4.30; FreeBSD)
      id 1BWBTY-00023E-Le; Fri, 04 Jun 2004 20:59:01 +1100
Received: from 252.38.116.244 by 24.11.34.43; Fri, 04 Jun 2004 07:56:55 -0300
Message-ID: <SBZRUOGYBFILPDFOQKMHESKWX@yahoo.com>
From: "Cornell Schmidt" <llcwo@hotmail.com>
Reply-To: "Cornell Schmidt" <llcwo@hotmail.com>
To: mark@mail-courier.com
Subject: Su.per Dis.count of 90%! 0olrc
Date: Fri, 04 Jun 2004 08:57:55 -0200
MIME-Version: 1.0
Content-Type: multipart/alternative;
      boundary="--9994435870976435220"
X-IP: 19.15.168.230
X-Priority: 3
```

The IP address found in the headers are highlighted, just like hyperlinks on a web page. Clicking on any of the hyperlinks will make SmartWhois retrieve information about the selected IP address. We can also select any part of the text and query the selection as a host name or domain. We  want to find the originating IP address of a message. We want to find the physical location of your correspondent someone who claims to be staying in France might be in Italy. We want to find to which organization the IP address in question is registered for instance if we get a message from customerservice@citibank.com but the message came from Nigeria, it's a good reason to think twice before submitting a web form with your account password Or we want to complain about spam. Regardless of the purpose of the query, it's important to understand the limitations of the technology.



IP, host or domain: 194.29.4.4

Results
- 194.29.4.4
- 209.68.11.237
- tamos.com
- weather.yahoo.com
- yahoo.com

Cablecom GmbH NOC
Zollstrasse 42
CH-8021 Zuerich
fax: +41 1 277 93 22
wilsor

Abus
For s
abus

TINE
Upda
wilso
Sourc

Carefully analyze the e-mail headers, find the spammer's IP address the spammer could be using an open mail relay server or a "zombie" computer to send e-mail, but it's still good to let the ISP know, perform a SmartWhois query, locate the administrative or abuse contact, rightclick on the e-mail address, and select Send Abuse/Spam Report. There we go, a new e-mail message will be opened in your e-mail client and pre-filled with the template. Be sure to edit the text and add the details. You can send the report in a matter of minutes.

## CONCLUSION AND FUTURE SCOPE:

E-mail is a widely used and highly distributed application involving several actors that play different roles. These actors include hardware and software components, services and protocols which provide interoperability between its users and among the components along the path of transfer. Cybercriminals forge e-mail headers or send it anonymously for illegitimate purposes which lead to several crimes and thus make e-mail forensic investigation crucial. These tools portrays e-mail actors, roles and their responsibilities. It illustrated logical e-mail architecture and underlining various core components, modules and protocols used in the system. It presents the meta-data contained in e-mail message and various techniques used for e-mail forensics. The tools also introduce several software e-mail forensic tools such as smartwhois and emailtrackerpro that have functionalities to automatically analyse e-mail and produce reports providing diverse information about it.

Finally, we can conclude that due to immense technology we procure we can easily access this software program to monitor all the emails, it will currently give an idea as what can be alternate solution to the problem of security in the email forensics that can be implemented if one is affected with the spam and any cyber related issues.

## REFERENCES:

https://www.salvationdata.com/knowledge/email-forensics-definition-and-guideline/

https://sintelix.com/email-forensic-tools/

https://www.systoolsgroup.com/email-forensics.html

https://www.tamos.com/products/smartwhois/

https://smartwhois.en.softonic.com/

https://filehippo.com/download_emailtrackerpro/

https://archive.org/details/tucows_244156_eMailTrackerPro

https://emailtrackerpro.soft112.com/

**SUBMITTED BY:**

**DASARI SRIKANTH-20BCE7076**

*****************THANK YOU*********************