
UNIT 2 E-MAIL CRIME & INVESTIGATION

Structure

- 2.0 Introduction
- 2.1 Objectives
- 2.2 What Is Electronic Mail?
- 2.3 How E-Mail Works?
 - 2.3.1 Operations
 - 2.3.2 Sending E-Mail
- 2.4 Structure of E-Mail
- 2.5 E-Mail Crimes
- 2.6 E-Mail Header Analysis
- 2.7 Received E-Mail Tracing Tools
 - 2.7.1 E-Mail Track Pro
- 2.8 E-Mail Location Tracking Tool
 - 2.8.1 Read Notify
- 2.9 How to Trace IP Address
 - 2.9.1 Caller IP
 - 2.9.2 SmartWhois
 - 2.9.3 VisualRoute
 - 2.9.4 McAfee NeoTrace Professional
- 2.10 Securing E-Mail Accounts
 - 2.10.1 Creating Strong Passwords
 - 2.10.2 E-Mail Protector
 - 2.10.3 SuperSecret
- 2.11 Let Us Sum Up
- 2.12 Check Your Progress: The Key

2.0 INTRODUCTION

In today's electronic world, E-Mail is critical to any business being competitive. In most cases it now forms the backbone of most organisations' day-to-day activities, and its use will continue to grow. E-Mails have enabled an efficient means of communication, without the limitations of time zones, speed or cost, usually associated with many of the other forms of communication. Though it has lot of advantages, however; E-Mails can easily be used for the negative purposes as well, making SPAM and virus E-Mails a problem especially by the hackers. In this Unit, we'll understand the key elements that comprise a successful E-Mail Crime & its Investigation and eventually work out on securing the E-Mails.

E-Mail is now considered to be most important in the area of information technology. Hackers come with various sophisticated tools and techniques to invade computers and stealing personal details of users from their E-Mail accounts. There are various traditional security measures available, but in most of the cases it is useless to fight against the latest attacks. So, to protect E-Mails every user/ company should adopt the right security software on computer. The Internet has opened up new doors of opportunities for both private individuals and companies. However,



Email Crime Investigation

there are different types of viruses, malware and other harmful items that may cause your computer.

Now-a-days, most of the companies implement online transactions and not only the companies but an individual also reap the benefits of the internet. They shop online and also carry out other financial transactions online and somehow keep their personal, financial, and credit card information, Bank Statements etc. in their E-Mail. So, the risk of hacking has also gone up significantly. Due to this reason sufficient assurance for a network, software, and PC are no longer enough. In order to protect the information and data, it has become the need of the hour to adopt new methods, techniques and various tools to implement the optimum level of security. This unit will provide all of measures to be taken for the E-Mail investigation and how to trace the fake E-Mails.

2.1 OBJECTIVES

After going through this Unit, you should be able to understand:

- What is E-Mail;
- How E-Mail Works?;
- Structure of E-Mail;
- E-Mail Crimes;
- E-Mail Header Analysis;
- E-Mail Investigation;
- Tracking an E-Mail;
- Tracing IP Address; and
- Securing E-Mail Account.

2.2 WHAT IS ELECTRONIC MAIL?

Electronic mail, which is commonly known as E-Mail is a method of exchanging digital messages across the Internet or other computer networks. E-Mail systems are based on a store-and-forward model in which E-Mail server computer systems accept, forward, deliver and store messages on behalf of users, who only need to connect to the E-Mail infrastructure. Typically an E-Mail server, with a network-enabled device for the duration of message submission or retrieval. Originally, E-Mail was transmitted directly from one user's device to another user's computer, which required both computers to be connected online at the same time.

An electronic mail message consists of two components, the message header, and the message body, which is the E-Mail's content. The message header contains control information, including, minimally, an originator's E-Mail address and one or more recipient addresses. Usually additional information is added, such as a subject header field.

Originally a text-only communications medium, E-Mail was extended to carry multi-media content attachments, which was standardized in RFC 2045 through RFC 2049, collectively called, Multipurpose Internet Mail Extensions (MIME).

The foundation for today's global Internet E-Mail services reaches back to the early ARPANET and standards for encoding of messages were proposed as early as 1973 (RFC 561). An E-Mail sent in the early 1970s looked very similar to one sent on the Internet today. Conversion from the ARPANET to the Internet in the early 1980s produced the core of the current services.

Network-based E-Mail was initially exchanged on the ARPANET in extensions to the File Transfer Protocol (FTP), but is today carried by the Simple Mail Transfer Protocol (SMTP), first published as Internet standard 10 (RFC 821) in 1982. In the process of transporting E-Mail messages between systems, SMTP communicates delivery parameters using a message envelope separately from the message (header and body) itself.

2.3 HOW E-MAIL WORKS?

2.3.1 Operations

E-Mail is based around the use of electronic mailboxes. When an E-Mail is sent, the message is routed from server to server, all the way to the recipient's E-Mail server. More precisely, the message is sent to the mail server tasked with transporting E-Mails (called the MTA, for *Mail Transport Agent*) to the recipient's MTA. On the Internet, MTAs communicate with one another using the protocol SMTP, and so are logically called **SMTP** servers (or sometimes outgoing mail servers).

The recipient's MTA then delivers the E-Mail to the incoming mail server (called the MDA, for *Mail Delivery Agent*), which stores the E-Mail as it waits for the user to accept it. There are two main protocols used for retrieving E-Mail on an MDA:

- **POP3** (*Post Office Protocol*), the older of the two, which is used for retrieving E-Mail and, in certain cases, leaving a copy of it on the server.
- **IMAP** (*Internet Message Access Protocol*), which is used for coordinating the status of E-Mails (read, deleted, moved) across multiple E-Mail clients. With IMAP, a copy of every message is saved on the server, so that this synchronization task can be completed.

For this reason, incoming mail servers are called POP servers or IMAP servers, depending on which protocol is used.

To use a real-world analogy, MTA act as the post office (the sorting area and mail carrier, which handle message transportation), while MDA act as mail boxes, which store messages (as much as their volume will allow) until the recipients check the box. This means that it is not necessary for recipients to be connected in order, for them to be sent E-Mail.

To keep everyone from checking other users' E-Mails, MDA is protected by a user name called a login and by a password.

Retrieving mail is done using a software program called an **MUA** (*Mail User Agent*). When it is a web interface used for interacting with the incoming mail server, it is called **webmail**.

The MUA is the application, which an originating sender uses to compose, and read E-Mail, such as Outlook, Thunderbird, Eudora etc.

The sender's MUA transfers the E-Mail to a Mail Delivery Agent (MDA). Frequently, the sender's MUA also handles the responsibilities of an MDA. Several of the most common MTA's do this, including sendmail, postfix, exim, qmail etc. The MDA/MTA accepts the E-Mail, then routes it to local mailboxes or forwards it if it isn't locally addressed.

An E-Mail can encounter a network cloud within a large company or ISP, or the largest network cloud in existence: the Internet. The network cloud may encompass a mass of mail servers, DNS servers, routers, and other devices and services too numerous to mention. These are likely to be slow when processing an unusually

Information Gathering

In figure 1.0, MDA forwards the email to an MTA and it enters the first of a series of "network clouds,"

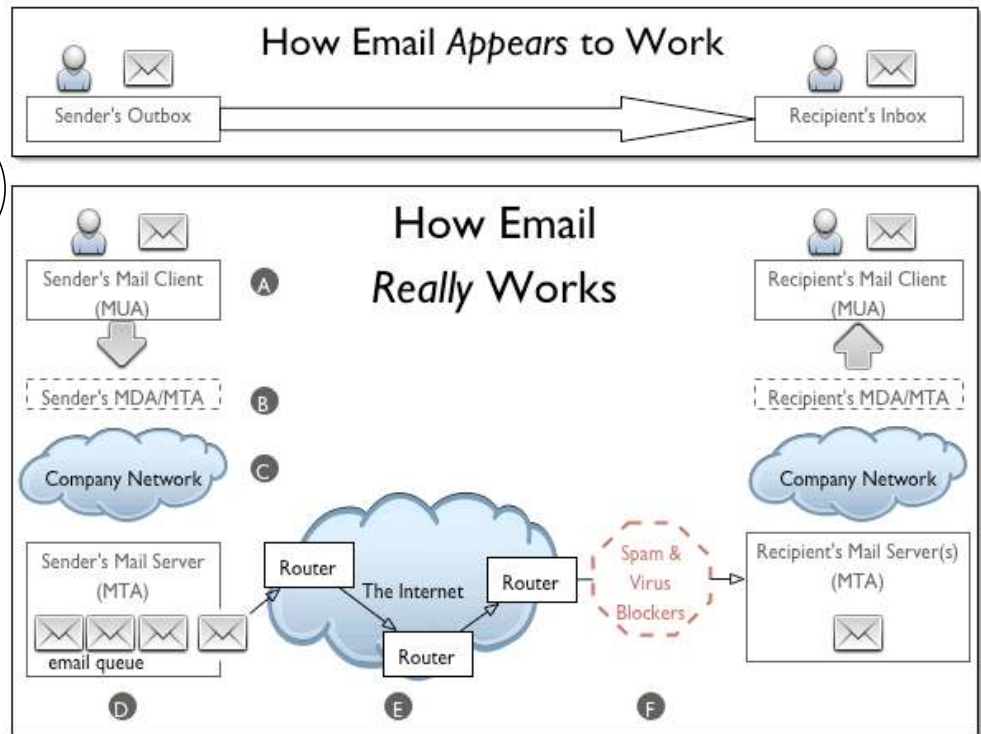


Fig. 1

heavy load, temporarily unable to receive an E-Mail when taken down for maintenance, and sometimes may not have identified themselves properly to the Internet through the Domain Name System (DNS) so that other MTAs in the network cloud are unable to deliver mail as addressed. These devices may be protected by firewalls, spam filters and malware detection software that may bounce or even delete an E-Mail. When an E-Mail is deleted by this kind of software, it tends to fail silently, so the sender is given no information about where or when the delivery failure has occurred.

The E-Mail in the figure 1 is addressed to someone at another company, so it enters an E-Mail queue with other outgoing E-Mail messages. If there is a high volume of mail in the queue, either because there are many messages or the messages are unusually large, or both then the message will be delayed in the queue until the MTA processes the messages ahead of it.

When transferring an E-Mail, the sending MTA handles all aspects of mail delivery until the message has been either accepted or rejected by the receiving MTA. As the E-Mail clears the queue, it enters the Internet network cloud, where it is routed along with a host-to-host chain of servers. Each MTA in the Internet network cloud needs to "stop and ask directions" from the Domain Name System (DNS) in order to identify the next MTA in the delivery chain. The exact route depends partly on server availability and mostly on which MTA can be found to accept E-Mail for the domain specified in the address. Most E-Mail takes a path that is dependent on server availability, so a pair of messages originating from the same host and addressed to the same receiving host could take different paths. These days, it's mostly spammers that specify any part of the path, deliberately routing their message through a series of relay servers in an attempt to obscure the true origin of the message.

To find the recipient's IP address and mailbox, the MTA must drill down through the Domain Name System (DNS), which consists of a set of servers distributed across the Internet. Beginning with the root name servers at the top-level domain (.tld), then domain name servers that handle requests for domains within that .tld, and eventually to name servers that know about the local domain. The MTA

contacts the MX servers on the MX record in order of priority until it finds the designated host for that address domain. The sending MTA asks if the host accepts messages for the recipient's username at that domain (i.e., username@domain.tld) and transfers the message.

An E-Mail may be transferred to more than one MTA within a network cloud and is likely to be passed to at least one firewall before it reaches its destination. An E-Mail encountering a firewall may be tested by spam and virus filters before it is allowed to pass inside the firewall. These filters test to see if the message qualifies as spam or malware. If the message contains malware, the file is usually quarantined and the sender is notified. If the message is identified as spam, it will probably be deleted without notifying the sender.

Spam is difficult to detect because it can assume so many different forms, so spam filters test on a broad set of criteria and tend to misclassify a significant number of messages as spam, particularly messages from mailing lists. When an E-Mail from a list or other automated source seems to have vanished somewhere in the network cloud, the culprit is usually a spam filter at the receiver's ISP or company.

In the figure, the E-Mail makes it past the hazards of the spam trap...er...filter, and is accepted for delivery by the receiver's MTA. The MTA calls a local MDA to deliver the mail to the correct mailbox, where it will sit until it is retrieved by the recipient's MUA.

2.3.2 Sending E-Mail

Create an E-Mail message

Applies to: Microsoft Outlook 2010



Fig. 2

- 1) On the Home tab, in the new group, click New E-Mail.

Keyboard shortcut to create an E-Mail message; press CTRL+SHIFT+M.

- 2) In the Subject box, type the subject of the message.
- 3) Enter the recipients' E-Mail addresses or names in the To, Cc, or Bcc box (To, Cc, and Bcc boxes: A message is sent to the recipients in the To box. Recipients in the Cc (carbon copy) and Bcc (blind carbon copy) boxes also get the message; however, the names of the recipients in the Bcc box aren't visible to other recipients.). Separate multiple recipients with a semicolon.

To select recipients' names from a list in the Address Book, click To, Cc, or Bcc and then click the names you want.

Show I don't see the Bcc box. How do I turn it on?

To display the Bcc box for this and all future messages, on the Options tab, in the Show Fields group, click Bcc.

- 4) After you have composed the message, click Send.

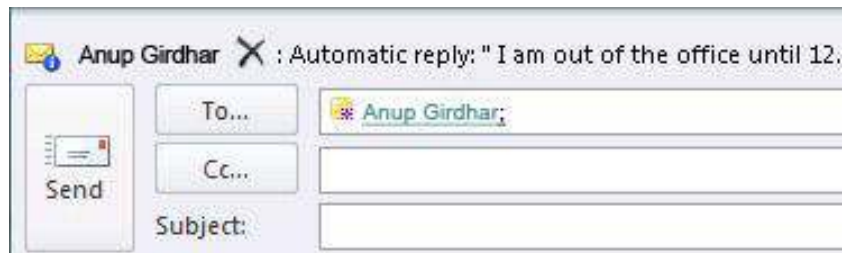


Fig. 3

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

What are the components of E-Mail? What is the use of Mail transfer agent?

.....

.....

.....

.....

.....

.....

.....

.....

2.4 STRUCTURE OF E-MAIL

A mail message consists of a header, which contains information about who the message was sent from, the recipient(s) and the route. Many of the header fields are not shown by default, but most programs used to read E-Mail will allow full headers to be displayed. This is then followed by the body of the message which contains whatever the sender wishes.

The message header should include at least the following fields:

- **From:** The E-Mail address, and optionally the name of the author(s). In many E-Mail clients not changeable except through changing account settings.
- **To:** The E-Mail address/addresses and optionally name(s) of the message's recipient(s). Indicates primary recipients (multiple allowed).
- **Cc:** Carbon copy; many E-Mail clients will mark E-Mail in your inbox differently depending on whether you are in the To: or Cc: list.
- **Bcc:** Blind Carbon Copy; addresses added to the SMTP delivery list but not (usually) listed in the message data, remaining invisible to other recipients.
- **Subject:** A brief summary of the topic of the message. Certain abbreviations are commonly used in the subject, including "RE:" and "FW!!".
- **Message-ID:** Also an automatically generated field; used to prevent multiple delivery and for reference in In-Reply-To

If the mail message is a formal one, it is customary although not obligatory to finish with your name, return address and other useful information as a signature. For example:

```

From owner-is-all-compcont@sedulitygroups.com Fri Aug 18 15:10:01 2010
Received: from sedulitygroups.com by anup@ sedulitygroups.com (8.8.8/
1.1.8.2/14Aug95-0452PM)
idPAA0000016479; Fri, 18 Aug 2000 15:10:00 +0100 (IST)
Received: from contact by sedulitygroups.com with local (Exim 3.16 #3)
id 13PmpO-0000XU-00
for IS-ALL-COMPCONT-outgoing@ sedulitygroups.com; Fri, 18 Aug 2010
15:08:58 +0530
Received: from contact by sedulitygroups.com with local (Exim 3.16 #3)
id 13PmpN-0000XK-00
for all-compcont-outgoing@ sedulitygroups.com; Fri, 18 Aug 2010 15:08:57
+0530
Received: from contact.sedulitygroups.com ([122.160.175.70] helo=clientid.
sedulitygroups.com)
by sedulitygroups.com with esmtp (Exim 3.16 #3)
id 13PmpM-0000XA-00; Fri, 18 Aug 2000 15:08:56 +0100
Received: by clientid.sedulitygroups.com (8.8.8/1.1.8.2/14Aug2010-0452PM)
idPAA0000009231; Fri, 18 Aug 2010 15:09:56 +0530 (IST)
Message-Id: <200008181409.PAA0000009231@clientid.sedulitygroups.com >
Subject: Netscape vulnerability fix
To: all-compcont@sedulitygroups.com
Date: Fri, 18 Aug 2010 15:09:56 +0530 (IST)
From: Team Sedulity <contact@ sedulitygroups.com >
Reply-To: contact@sedulitygroups.com
X-Mailer: ELM [version 2.4 PL25]
MIME-Version: 1.0
Content-Type: text/plain; charset=US-ASCII
Content-Transfer-Encoding: 7bit
Sender: owner-is-all-compcont@sedulitygroups.com
Precedence: bulk
Status: RO

Congratulations.

Sedulity Solutions & Technologies has recently launched its 64 bit operating
system.

Team Sedulity
Sedulity Solutions & Technologies

```

The header consists of lines beginning with a keyword followed by a colon (:), followed by information on each line. A brief explanation of each field of the header is given below. This header contains most of the common fields.

- **Received:** These lines indicate the route that the E-Mail has taken and which systems have handled it and the times that it was handled.
- **Date:** The date and time at which the message was sent including time zone.
- **From:** The sender. The part in angle brackets is a real electronic mail address. This field may be user settable, so may not reflect the true sender. In this case, it shows the original sender of the message.
- **Sender:** The sender. This is inserted by some systems if the actual sender is different from the text in the From: field. This makes E-Mail more difficult to forge, although this too can be set by the sender. There are other uses for a sender field. In the example above, the sender is set to the list owner by the mailing list system. This allows error messages to be returned to the list owner rather than the original sender of the message.
- **To:** Who the mail is sent to. This may be a list or an individual. However it may bear no relation to the person that the E-Mail is delivered to. Mail systems used a different mechanism for determining the recipient of a message.
- **Cc:** Addresses of recipients who will also receive copies.
- **Subject:** Subject of the message as specified by the sender.
- **Message-id:** A unique system generated id. This can sometimes be useful in fault tracing if multiple copies of a message have been received.
- **Reply-to:** Where any reply should be sent to (in preference to any electronic mail address in the From: field if present). This may be inserted by the sender, usually when they want replies to go to a central address rather than the address of the system they are using. It is also inserted automatically by some systems.
- **X-Mailer:** Any field beginning with X can be inserted by a mail system for any purpose.

When using a reply facility it is important to check where the reply is going by looking at the header of the outgoing message displayed on your screen. If the message has been forwarded to you, the reply will often go to the original sender and not the person who sent it to you.

2.5 E-MAIL CRIMES

Some of the major E-Mail related crimes are:

- 1) E-Mail spoofing
- 2) Sending malicious codes through E-Mail
- 3) E-Mail bombing
- 4) Sending threatening E-Mails
- 5) Defamatory E-Mails
- 6) E-Mail frauds

E-Mail spoofing

A spoofed E-Mail is the one that appears to originate from one source however, has emerged from another source in reality. In other words, E-Mail spoofing is the forgery of an E-Mail header so that the message appears to have originated from someone or somewhere other than the actual source. To send spoofed E-Mail,

senders insert commands in headers that will alter message information. It is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say. Thus, someone could send spoofed E-Mail that appears to be from you with a message that you didn't write.

Although most spoofed E-Mail falls into the "nuisance" category and requires little action other than deletion, the more malicious varieties can cause serious problems and security risks. For example, spoofed E-Mail may import to be from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information — any of which can be used for a variety of criminal purposes. One type of E-Mail spoofing, self-sending spam, involves messages that appear to be both to and from the recipient. E-Mail spoofing is surely possible because, Simple Mail Transfer Protocol (SMTP), is the main protocol used in sending E-Mail, does not include an authentication mechanism.

In order to send a spoofed E-Mail, the sender has to enter the following information mentioned below:

- E-Mail address of the receiver of the E-Mail
- E-Mail address(es) of the person(s) who will receive a copy of the E-Mail (referred to as CC for carbon copy)
- E-Mail address(es) of the person(s) who will receive a copy of the E-Mail (referred to as CC for carbon copy, but whose identities will not be known to the other recipients of the E-Mail (known as BCC for blind carbon copy)
- Subject of the message (a short title / description of the message)
- Message

There are certain web-based E-Mail services like, www.SendFakeMail.com, www.anonymailer.net which offers a facility, wherein in addition to the above, a sender can also enter the E-Mail address of the supposed sender of the E-Mail.

For example, Mr. XYZ whose E-Mail address is xyz@hotmail.com. His friend ABC's E-Mail address is abc@yahoo.com. Using anonymailer.net, XYZ can send E-Mails which are supposed to be sent from ABC's E-Mail account. All he has to do is enter abc@yahoo.com in the space provided for sender's E-Mail address. ABC's friends would trust such E-Mails, as they would assume that they have come from ABC (whom they trust). XYZ can use this misplaced trust to send viruses, Trojans, worms etc. to ABC's friends, who would unwittingly download them.

Spreading Trojans, viruses and worms

E-Mails are often the fastest and easiest ways to propagate malicious code over the Internet. The Love Bug virus, for instance, reached millions of computers within 36 hours of its release from the Philippines thanks to E-Mail. Hackers often bind Trojans, viruses, worms and other computer contaminants with E-greeting cards and then E-Mail them to unsuspecting persons. Such contaminants can also be bound with software that appears to be an anti-virus patch. E.g. a person receives an E-Mail from Compose From To CC BCC Subject

Message

information@mcafee.com (this is a spoofed E-Mail but the victim does not know this). The E-Mail informs him that the attachment contained with the E-Mail is a security patch that must be downloaded to detect a certain new virus. Most unsuspecting users would submit to such an E-Mail (if they are using a registered copy of the McAfee anti-virus software) and would download the attachment, which could be a Trojan or a virus itself!

E-Mail bombing

E-Mail bombing refers to sending a large amount of E-Mails to the victim resulting in the victim's E-Mail account (in case of an individual) or servers (in case of a company or an E-Mail service provider) crashing. A simple way of achieving this would be to subscribe the victim's E-Mail address to a large number of mailing lists. Mailing lists are special interest groups that share and exchange information on a common topic of interest with one another via E-Mail. Mailing lists are very popular and can generate a lot of daily E-Mail traffic – depending upon the mailing list. Some generate only a few messages per day others generate hundreds. If a person has been unknowingly subscribed to hundreds of mailing lists, his incoming E-Mail traffic will be too large and his service provider will probably delete his account. The simplest E-Mail bomb is an ordinary E-Mail account. All that one has to do is compose a message, enter the E-Mail address of the victim multiple times in the “To” field, and press the “Send” button many times.

Writing the E-Mail address 25 times and pressing the “Send” button just 50 times (it will take less than a minute) will send 1250 E-Mail messages to the victim! If a group of 10 people do this for an hour, the result would be 750,000 E-Mails!

There are several hacking tools available to automate the process of E-Mail bombing. These tools send multiple E-Mails from many different E-Mail servers, which make it very difficult, for the victim to protect himself.

Threatening E-Mails

This is another type of E-Mail crime, where an E-Mail is sent to a person for the purpose of threatening. It is a useful tool for technology savvy criminals as it becomes fairly easy for anyone with even a basic knowledge of computers to become a blackmailer by threatening someone via E-Mail.

Defamatory E-Mails

Defamation is defined as communication to third parties of false statements about a person that injure the reputation of or deter others from associating with that person. Defamation can take one of two forms: slander or libel. Slander covers oral defamatory statements while libel addresses the written version. Defamation is an abusive attack on a person's character or good name. If a person is harmed in any way by any statement(s), a person sending defamatory E-Mail can be held accountable in a court of law.

Check Your Progress 2

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

Explain the structure of an E-Mail. What are the major E-Mail related crimes?

.....

.....

.....

.....

2.6 E-MAIL HEADER ANALYSIS

Here is the starting part of the header of a junk E-Mail (spam), which includes information about the transfer of the E-Mail between the sender and the receiver:

```
Return-Path: <ydcddlhanqz@yahoo.com>
Received: from mail.fx.ro (mail4.fx.ro [193.231.208.4])
    by fx.ro (8.12.7/8.12.7) with ESMTP id i2OAVxGs024789;
    Wed, 24 Mar 2004 12:31:59 +0200 (EET)
Received: from mailv.fx.ro (localhost.localdomain [127.0.0.1])
    by mail.fx.ro (8.12.11/8.12.3) with ESMTP id i2OAVxaA004610;
    Wed, 24 Mar 2004 12:31:59 +0200
Received: (from root@localhost)
    by mailv.fx.ro (8.12.11/8.12.3/Submit) id i2OAVxh1004609;
    Wed, 24 Mar 2004 12:31:59 +0200
Received: from 206.85.220.156 by 217.225.143.240;
```

- **Return-path:** the header tells that if you reply to this E-Mail message, the reply will be sent to ydcddl...@yahoo.com. Would you use such an E-Mail address for real?
- **Received tags:** As on web blogs, read them from the bottom to top. The header says the E-Mail was originally sent from 206.85... and it was sent to 217.225... (which is the name/IP of the first mail server that got involved into transporting this message). Then suddenly, the next Received tag says the message was received from root@localhost, by mailv.fx.ro. You can also notice that so far, the Received tags do not contain any information about how the E-Mail was transmitted (the "with" tag is missing: this tag tells the protocol used to send the E-Mail).

In reality, this is the common case of a spammer pretending to be the root user of mailv.fx.ro and sending the E-Mail from 206.85..., through 217.225... and telling 217.225... to act as the root user of mailv.fx.ro, in order to use the SMTP server of mailv.fx.ro to send the E-Mail. Since more and more mail servers are not allowing open-relay connections, the spammer can only use the mail server of the receiver, in order to send the message. If the spammer will try to send the E-Mail to support@E-Mailaddressmanager.com, through exactly the same route as above, it wouldn't work, because support@E-Mailaddressmanager.com is not a network user of mailv.fx.ro. This is the reason why you may have received spam E-Mails appearing to be sent through an E-Mail address of your own ISP.

Going deeper with the analysis, you can use an IP tracing tool, like Visual Route, in order to see to whom the IP belongs to. As in most of the spamming cases, the starting IP (206.85...) is unreachable, which means that the spammer could have routed the real IP or he could have used a dynamic IP (a normal case for dial-up users). However, by tracing 217.225..., you will get to the ISP used by the spammer, a German provider. The ISP has nothing to do with the spam itself, but it was simply used by the spammer to connect to the Internet.

Let's look further into the E-Mail header:

```
Message-ID: <VHUCXEYVIXPEUNUKOJEW@hotmail.com>
From: "Julianne Lloyd" <ydcddlhanqz@yahoo.com>
Reply-To: "Julianne Lloyd" <ydcddlhanqz@yahoo.com>
To: boby_con@fx.ro
Cc: bodistvan@fx.ro, bogdan.micu@fx.ro, bogdan@fx.ro, bogdans@fx.ro
Subject: Get viagra over night - no prescription needed
Date: Wed, 24 Mar 2004 08:31:16 -0200
X-Mailer: AOL 9.0 for Windows US sub 740
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="--05917340466547820851"
X-Priority: 3
X-MSMail-Priority: Normal
X-IP: 162.238.92.104
X-RAV-Bulk: RAV AntiVirus classifies this e-mail as spam (accuracy medium)
X-RAV-Signature: 250F0FB03547C3C93609D82815AB3746
X-RAVMilter-Version: 8.4.3(snapshot 20030212) (mail)
X-UIDL: 1+/"!1-H"!JK!!^V!"
```

Information Gathering

- The Message-ID field is a unique identifier of each E-Mail message. It is like the tracing ID of an express postal mail. The rule says the ID is composed by the name of the server that assigned the ID and a unique string (for example, QESADJHO@E-Mailaddressmanager.com). Hm, this is strange, because on our case, the ID belongs to hotmail.com, while the sender appears to belong to yahoo.com. In fact, this difference mainly shows that the sender is forged (fake address or someone pretending to own that E-Mail address).
- The X-IP tag (also named X-Originating-IP) is probably the most important one and it should give precise information about the sender (from where the E-Mail was actually sent). Unfortunately, this tag is optional for E-Mail protocols, so some spam messages will not include it. As you can see, the originating IP is not even close to the sender's IP, from the Received tags.
- The X-UIDL tag is another unique ID, but this one is used by the POP3 protocol when your E-Mail client is receiving the E-Mail. This is an optional E-Mail tag, but the rule of thumb says spammers love to include it.

Spam E-Mail Header vs Regular E-Mail Header.

SPAM HEADER	REGULAR EMAIL
Return-Path: <ydcddlhangz@yahoo.com> Received: from mail.fx.ro (mail4.fx.ro [193.231.208.4]) by fx.ro (8.12.7/8.12.7) with ESMTP id i2OAVxGs024789; Wed, 24 Mar 2004 12:31:59 +0200 (EET) Received: from mailv.fx.ro (localhost.localdomain [127.0.0.1]) by mail.fx.ro (8.12.11/8.12.3) with ESMTP id i2OAVxaA004610; Wed, 24 Mar 2004 12:31:59 +0200 Received: (from root@localhost) by mailv.fx.ro (8.12.11/8.12.3/Submit) id i2OAVxhl004609; Wed, 24 Mar 2004 12:31:59 +0200 Received: from 206.85.220.156 by 217.225.143.240; Message-ID: <VHUCXEYVIXPEUNUKOJEJW@hotmail.com> From: "Julianne Lloyd" <ydcddlhangz@yahoo.com> Reply-To: "Julianne Lloyd" <ydcddlhangz@yahoo.com> To: boby_con@fx.ro Cc: bodistvan@fx.ro, bogdan.micu@fx.ro, bogdan@fx.ro, bogdans@fx.ro Subject: Get viagra over night - no prescription needed Date: Wed, 24 Mar 2004 08:31:16 -0200 X-Mailer: AOL 9.0 for Windows US sub 740 MIME-Version: 1.0 Content-Type: multipart/alternative; boundary="--05917340466547820851" X-Priority: 3 X-MSMail-Priority: Normal X-IP: 162.238.92.104 X-RAV-Bulk: RAV AntiVirus classifies this e-mail as spam (accuracy medium) X-RAV-Signature: 250F0FB03547C3C93609D82815AB3746 X-RAVMilter-Version: 8.4.3(snapshot 20030212) (mail) X-UIDL: 1+/"!-H"[JK!!^V" Status: RO	Return-Path: <bogdan@fx.ro> Received: from srv01.advenzia.com (root@localhost) by emailaddressmanager.com (8.11.6/8.11.6) with ESMTP id i2OApwQ14083 for <support@emailaddressmanager.com> X-ClientAddr: 193.231.208.29 Received: from corporate.fx.ro (corporate.fx.ro [193.231.208.29]) by srv01.advenzia.com (8.11.6/8.11.6) with ESMTP id i2OApws14078 for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 10:51:57 GMT Received: from mail.fx.ro (mail3.fx.ro [193.231.208.3]) by corporate.fx.ro (8.12.11/8.12.7) with ESMTP id i2OAtxBt025924 for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 12:55:59 +0200 Received: from localhost.localdomain (corporate2.fx.ro [193.231.208.28]) by mail.fx.ro (8.12.11/8.12.3) with ESMTP id i2OAtQe006624 for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 12:55:50 +0200 Date: Wed, 24 Mar 2004 12:55:50 +0200 Message-Id: <200403241055.i2OAtQe006624@mail.fx.ro> Content-Disposition: inline Content-Transfer-Encoding: binary MIME-Version: 1.0 To: support@emailaddressmanager.com Subject: How to read email headers From: bogdan@fx.ro Reply-To: bogdan@fx.ro Content-Type: text/plain; charset=us-ascii X-Originating-IP: [80.97.5.101] X-Mailer: FX Webmail web mail.fx.ro X-RAVMilter-Version: 8.4.3(snapshot 20030212) (mail) Status:

The look and feel for both the mail header is almost same but, the major difference is the IP address from the mail which was originated, In the above case, Regular mail was received from their Private IP i.e. 193.231... (localhost.localdomain) of the Company where the Spam mail was received from the Anonymous IP address i.e. 206.85.220.156 which belongs to some other country. And there are many validations now a days placed in the new release of the good MTA's which detects the SPAM mails like the DNS of the mail originator, Time frame, Key words placed in the mail, Attachments, Blacklisted IP's etc. So these are the ways by which we can scan whether the mail is the original or the Spam one.

Check Your Progress 3

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

Explain the function of received tags? What is message ID?

.....

.....

.....

.....

.....

2.7 RECEIVED E-MAIL TRACING TOOLS

2.7.1 E-Mail Track Pro


E-MailTrackerPro will automatically analyse an E-Mail and its headers and provide a report similar as shown below:


Identification Report for 'Cheap Pharmacy el'


Host **211.125.211.2** has been found. It is probably located in or around **Japan** as this is where the organization or individual who manages the system is located.

This system is a web and secure web server (click [here](#) for details).

Network Contact Information: The following details refer to the network that the system is on.

 hostmaster@nic.ad.jp

 +81-3-5297-2312

 Kokusai-Kougyou-Kanda Bldg 6F, 2-3-4 Uchi-Kanda Chiyoda-ku, Tokyo 101-0047, Japan

Report a hacker, spammer or other type of Internet abuser.

☒ [Click here to hide the in-depth information on this email](#) (*more info*)

- This email is sent from the computer identified on the Internet by **211.125.211.2** (or hccd37dd302.bai.ne.jp).
- The sender claims to be **garyie@verizon.net**, but this is very easily forged and as such not necessarily reliable.
- At the time of sending, one email server (identified on the Internet by **211.125.211.2**) to which this email was apparently passed claimed to be known as **verizon.net**, but it does not currently have that name. Its name could have changed, but this is a common method used by hackers and spammers to misdirect users to their true location.

Tracing an E-Mail address: If you do not have an actual E-Mail message, but only have an E-Mail address, you can trace the address through its E-Mail server. However, it should be noted that E-Mail addresses can be easily forged, the results from tracing an E-Mail address may not be related to the true sender.

In most cases, using an E-Mail tracking tool like E-MailTrackerPro to trace an E-Mail message you have received is your best option. To trace an E-Mail message received by someone else, have them forward the message to you as an attachment (just forwarding the message itself will show them as the sender). You can then open the attached message and copy the E-Mail header, start E-MailTrackerPro and paste the header for analysis.

E-Mail Internet Headers

Every received E-Mail has Internet Headers. Using Microsoft Outlook as an example (other mail programs are very similar), just follow these steps to view the headers:

- 1) Right-click on the mail message that is still in your Outlook Inbox
- 2) Select 'Options...' from the resulting popup menu
- 3) Examine the 'Internet Headers' in the resulting 'Message Options' dialog

Information Gathering

Right-click in the 'Internet Headers' field and click on 'Select All' in the popup menu (or type ctrl-A). Then right-click again and click on 'Copy' in the popup menu (or type ctrl-C). Finally, paste all the Internet Headers into your favourite text editor for full examination (such as 'Notepad', included with Windows).

Example: What you see will be very similar to the following (with 'line numbers' added for clarity and discussion in following sections):

```
1: Received: from tesla623.OnE-Mail.com.sg ([203.127.89.129]) by
   visualroute.com (8.11.6) id f9CIVSk24480; Tue, 12 Oct 2004 12:31:29 -0600
   (MDT)

2: Message-Id: <200110121831.f9CIVSk24480@s2.domain.com>

3: Received: from drb.com (IIM1608 [203.127.89.138]) by tesla623.OnE-
   Mail.com.sg with SMTP (Microsoft Exchange Internet Mail Service Version
   5.5.2448.0)

4: id 4XNK9AIR; Wed, 13 Oct 2004 01:19:10 +0800

5: From: paylesslongdistance@somedomain.com

6: To: <

7: Subject: Long Distance - 4.9 cents per min - NO FEES!

8: Date: Tue, 12 Oct 2004 13:24:26 -0400

9: X-Sender: paylesslongdistance@yahoo.com

10: X-Mailer: QUALCOMM Windows Eudora Pro Version 4.1

11: Content-Type: text/plain; charset="us-ascii"

12: X-Priority: 3

13: X-MSMail-Priority: Normal

14: X-UIDL: 8`Y!!0GR!!"?H"!k:O!!

15: Status: U
```

Header Line Syntax: The Internet Header Fields are just a series of text lines, where each line looks like:

Header-Name: Header-Value

And if a line starts with a tab or spaces, like line 4 above, that line is a continuation of the previous Header-Value line. So, the Header-Name Received in line 3 has a Header-Value that spans lines 3 and 4.

'Received' Headers

The most important header field for tracking purposes is the Received header field, which usually has syntax similar to:

Received: from ? by ? via ? with ? id ? for ? ; date-time

Where from, by, via, with, id, and for are all tokens with values within a single Header-Value, which may span multiple lines. Note: Some mail servers may not include all of these tokens — or additional tokens/values may be added to this field, but now you are prepared to break it apart and understand it.

Every time an E-Mail moves through a new mail server, a new Received header line (and possibly other header lines, like line 2 above) is added to the beginning

of the headers list. This is similar to FedEx package tracking, when your package enters a new sorting facility and is 'swiped' through a tracking machine.

This means that as you read the Received headers from top to bottom, that you are gradually moving closer to the computer/person that sent you the E-Mail.

But please note that as you read through the Received header fields and get closer to the computer/person that sent you the E-Mail, you need to consider the possibility that the sender added one or more false Received header lines to the list (at the time, the senders beginning of the list) in an attempt to redirect you to another location and prevent you from finding the true sender. But, now that you know false header lines are possible, just stay alert.

You will probably find it very useful to break a single Received line into multiple lines, with one token per line. Namely, the header line:

Received: from tesla623.OnE-Mail.com.sg ([203.127.89.129]) by visualroute.com (8.11.6) id f9CIVSk24480; Tue, 12 Oct 2004 12:31:29 -0600 (MDT)

is much easier to read and understand when formatted so that each token is on a new line, as in:

```
Received:
from tesla623.OnE-Mail.com.sg ([203.127.89.129])
by visualroute.com (8.11.6)
id f9CIVSk24480
; Tue, 12 Oct 2004 12:31:29 -0600 (MDT)
```

The Sender's IP Address

For tracking purposes, we are most interested in the from and by tokens in the Received header field. In general, you are looking for a pattern similar to:

```
Received: from BBB (dns-name [ip-address]) by A A A ...
Received: from CCC (dns-name [ip-address]) by BBB ...
Received: from DDD (dns-name [ip-address]) by CCC ...
```

In other words, mail server A A A received the E-Mail from BBB and provides as much information about BBB, including the IP Address BBB used to connect to AAA. This patterns repeats itself on each Received line. The syntax of the from token most times looks like:

```
name (dns-name [ip-address])
```

Where: name is the name the computer has named itself. Most of the time we never look at this name because it can be intentionally misnamed in an attempt to foil your tracking (but it may leak the windows computer name). dns-name is the reverse dns lookup on the ip-address. ip-address is the ip-address of the computer used to connect to the mail server that generated this Received header line. So, the ip-address is gold to us for tracking purposes.

The by token syntax just provides us with the name that the mail server gives itself. But since the last mail server could be under the control of a spammer, we should not trust this name.

So, what is crucial for tracking, is to pay attention to the trail of ip-address in the from tokens and not necessarily the host name provided to us in the by tokens. Hopefully an example will make the reason why very clear:

Information Gathering

- 1: Received: from **tesla623.OnE-Mail.com.sg** ([203.127.89.129]) by visualroute.com (8.11.6) id f9CIVSk24480; Tue, 12 Oct 2004 12:31:29 -0600 (MDT)
- 3 Received: from drb.com (IIM1608 [203.127.89.138]) by **tesla623.OnE-Mail.com.sg** with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2448.0)

If you ignore line 1, you would conclude from line 3 that mail server tesla623.OnE-Mail.com.sg sent you an E-Mail, but this would be wrong. When you trace to the host name tesla623.OnE-Mail.com.sg, you are actually tracing to the IP Address lookup on that host name, which is 192.9.200.230. But as you can see from line 1, the IP Address used was really 203.127.89.129. Do not be fooled by this attempted misdirection by spammers and fraudsters.

Determine the IP Address of the Sender: Using the example E-Mail headers above and analyzing the Received header lines we can conclude:

- A Visualware employee received an E-Mail
- which came from visualroute.com (line 1)
- which came from tesla623.OnE-Mail.com.sg (line 1; line 3 confirms)
- but whose ip-address used was 203.127.89.129 (line 1)
- which came from drb.com/IIM1608 (line 3)
- but whose ip-address used was 203.127.89.138 (line 3)

So, we have just tracked this E-Mail to the source — IP Address **203.127.89.138**.

Leaked Sender Information

The Internet Headers for an E-Mail message may contain some really interesting information about the sender.

A) **Windows Computer Name:** It appears that the Windows computer name is sometimes leaked. Consider the following partial header information from an actual E-Mail:

Received: from **hanksdell** (11-22-33-44.xyz.net [11.22.33.44]) by visualroute.com (8.8.5) id SAA26331; Mon, 11 Oct 2004 18:46:53 -0600 (MDT)

Where we can clearly see the IP Address of the sender, but we can also see the computer name of hanksdell. While the computer name can be named anything, in this case, I might assume that the person is named Hank and uses a Dell computer.

This computer name may be intentionally misleadingly named or not be meaningful but it can become very useful confirming information if law enforcement can confirm that the name of the suspect's computer matches the name in the E-Mail header.

B) **Timezone Information:** Consider lines 3 and 4 from the Internet Header discussion above:

- 3 Received: from drb.com (IIM1608 [203.127.89.138]) by tesla623.OnE-Mail.com.sg with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2448.0)
- 4 id 4XNK9AIR; Wed, 13 Oct 2004 01:19:10 +0800

Notice that in the Internet Headers, when a time is displayed, many times it is followed with a plus/minus and four digits, which represent HHMM (hour and

minutes) from GMT (Greenwich Mean Time), or London, UK time. Plus means east of GMT. Minus means west of GMT.

So, according to +0800, the server is 8 hours east of GMT. TIP: Go into the Windows Control panel and enter into the Date/Time dialog, where there is a Time Zone list. This time zone appears to be in Singapore. Then, the .sg in tesla623.OnE-Mail.com.sg means Singapore, which is one more confirmation of this information. A final confirmation comes from performing a VisualRoute trace 203.127.89.129 (the IP Address for tesla623.OnE-Mail.com.sg). TIP: Trace to the IP Address, not the host name.

C) **X-Mailer:** This will usually tell you the mailer software used by the sender of the E-Mail. Consider:

10: X-Mailer: QUALCOMM Windows Eudora Pro Version 4.1

This may or may not be immediately useful, but it can be very useful if there is a follow-up investigation by authorities.

D) **X-Originating-IP:** If you are attempting to track down an E-Mail received from a Hotmail E-Mail account, look for the X-Originating-IP header field, which will tell you the IP Address of the computer that sent the E-Mail. Consider:

- 1: Received: from hotmail.com (f105.pavl.hotmail.com [64.4.31.105]) by s2.xyz.com (8.11.6) id f9BIvve34655; Mon, 11 Oct 2004 12:58:00 -0600 (MDT)
- 2: Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;
- 3: Mon, 11 Oct 2001 11:57:51 -0700
- 4: Received: from **202.156.2.147** by pvlfd.pavl.hotmail.msn.com with HTTP;
- 5: Mon, 11 Oct 2004 18:57:51 GMT
- 6: **X-Originating-IP: [202.156.2.147]**

However, notice that we could have obtained the same IP Address information by examining the Received header fields. But it is nice to have this extra confirmation.

2.8 E-MAIL LOCATION TRACKING TOOL

2.8.1 ReadNotify



ReadNotify is the most powerful and reliable E-Mail tracking service that exists today. In short – ReadNotify tells you "when" the E-Mail you sent gets read / re-opened / forwarded and so much more. The Salient features are: Certified email with delivery Receipts, Silent Tracking, Proof of Opening History, Security and Timestamps etc.

How do you send a tracked E-Mail?

There are two ways you can send tracked E-Mails:

Information Gathering

- 1) Simply add: `.readnotify.com` to the end of your recipients E-Mail address (they won't see this)

OR

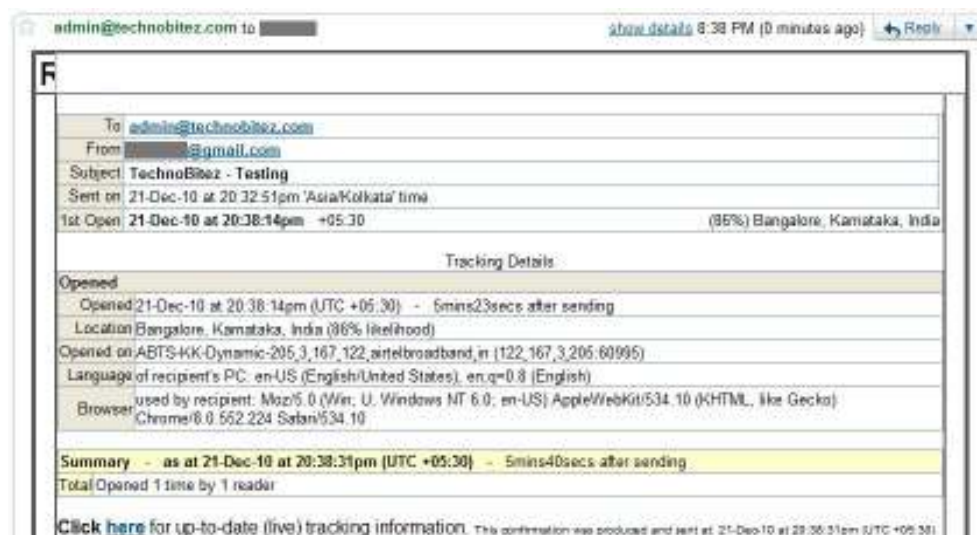
- 2) Install our ActiveTracker plugin to add the tracking for you.

Testing? If you send tracked E-Mails to yourself, your anti-spam filters may block them (people don't usually write to themselves) - so we recommend you test by sending to other people.

What will you tell me about the tracked E-Mails I send?

ReadNotify will endeavour to provide the following in your tracking reports:

- Date and time opened
- Location of recipient (per their ISP city /town)
- Map of location (available on paid subscriptions)
- Recipients IP address
- Apparent E-Mail address of opening (if available)
- Referrer details (i.e.; if accessed via web mail etc)
- URL clicks
- How long the E-Mail was read for
- How many times your E-Mail was opened
- If your E-Mail was forwarded, or opened on a different computer



All messages sent via ReadNotify benefit from our SPF compliant and Sender-ID compliant mail servers. This confirms safe transmission of your messages, and also enables us to report delivery status to you (including: bounce-backs, delays and success notifications). Delivery information is listed in your Personal Tracking Page.

Try hovering your mouse over the sections in our Live Sample Receipt for more information.

Note: ReadNotify.com does not use or contain any Spyware, Malware, nor viruses, it is not illegal to use, and does not breach any privacy regulations in any countries.

What else does ReadNotify do?

There are lots of great features available to you - these include the following sending options:

- Certified E-Mail
- Ensured-Receipts and retractable E-Mails
- Invisible tracking
- Self-Destructing E-Mails
- Block printing
- Adobe Acrobat PDF Document Tracking
- Track MS Word or Excel documents

You can also choose how to receive your receipts:

- In your Personal Tracking Page (when you log in)
- E-Mail ReadNotifications
- Legal Proof-of-Opening receipts
- Delivery Service Notifications (DSN's)
- SMS alert on your cell-phone or pager
- Instant Messenger

These options are available to you from "My Account" in Member Utilities.

Check Your Progress 4

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

How ip address is gold for the tracking purposes?

.....

.....

.....

.....

.....

.....

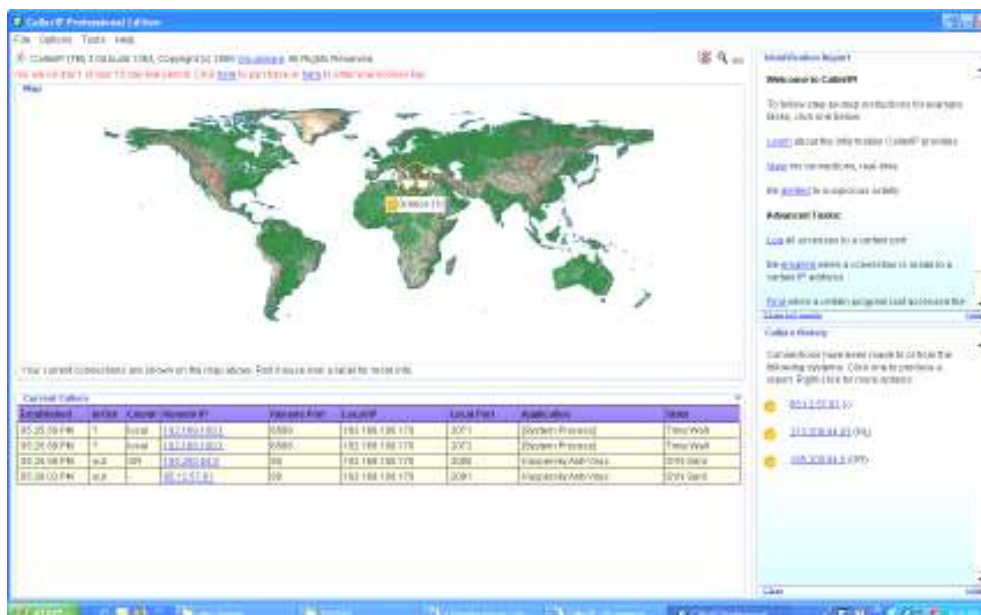
.....

2.9 HOW TO TRACE IP ADDRESS

2.9.1 CallerIP

CallerIP Standard Edition allows real time monitoring of any machine that it is installed on. This allows you to detect suspicious activity such as spyware and see where in the world they are connecting from. Worldwide whois reports and network provider reports are also available for any connection!

Advanced CallerIP Advanced Edition (inc. all Standard features) allows you to run it as a server! This allows you to monitor the connections made to and from your machines from a remote location! Automated Alerts are also available to you are notified the moment something suspicious attempts a connection to your server(s).



- **Plot all connections**

This feature enables you to have CallerIP plot all the connections on the world map. This in turn allows for easy and quick analysis of where connections made to/from your machine reside.

- **New look table**

The new look table includes gradient fills. This means the colour of the row in the table depends on the threat of the connection. If the connection being made to your machine is harmless then the gradient will be green. It is another quick and easy way to identify the threat of a connection.

- **Condensed CallerIP**

CallerIP now allows you to minimize it to a very small and detailed dialog box. The small window gives you everything you need to know but stays in the background.

- **Real-time monitoring instantly identifies suspect activity and spyware**

CallerIP monitors all connections to and from your system and actively scans ports for possible back doors that allow unauthorized access.

- **Identifies the country of origin for all connections**

A connection to/from a high-risk country is a key indicator of suspect activity and could likely be someone looking to steal your confidential information or compromise your system. CallerIP shows you the country location of connections so you can identify suspect activity and protect your information.

- **Network Provider reporting with abuse reporting information**

See the contact and abuse reporting information for the company providing internet access for an IP address or website, so you can easily report hackers or Internet abuse.

- Worldwide Whois reports

Caller IP Pro queries worldwide databases to report the up-to-date registration information for the 'owner' of an IP address or domain. Information includes name, address, phone and E-Mail contact information.

- Detailed log of connection history with search options

Each connection or attempted connection is automatically logged, with search capabilities for quick lookups of past connection activity.

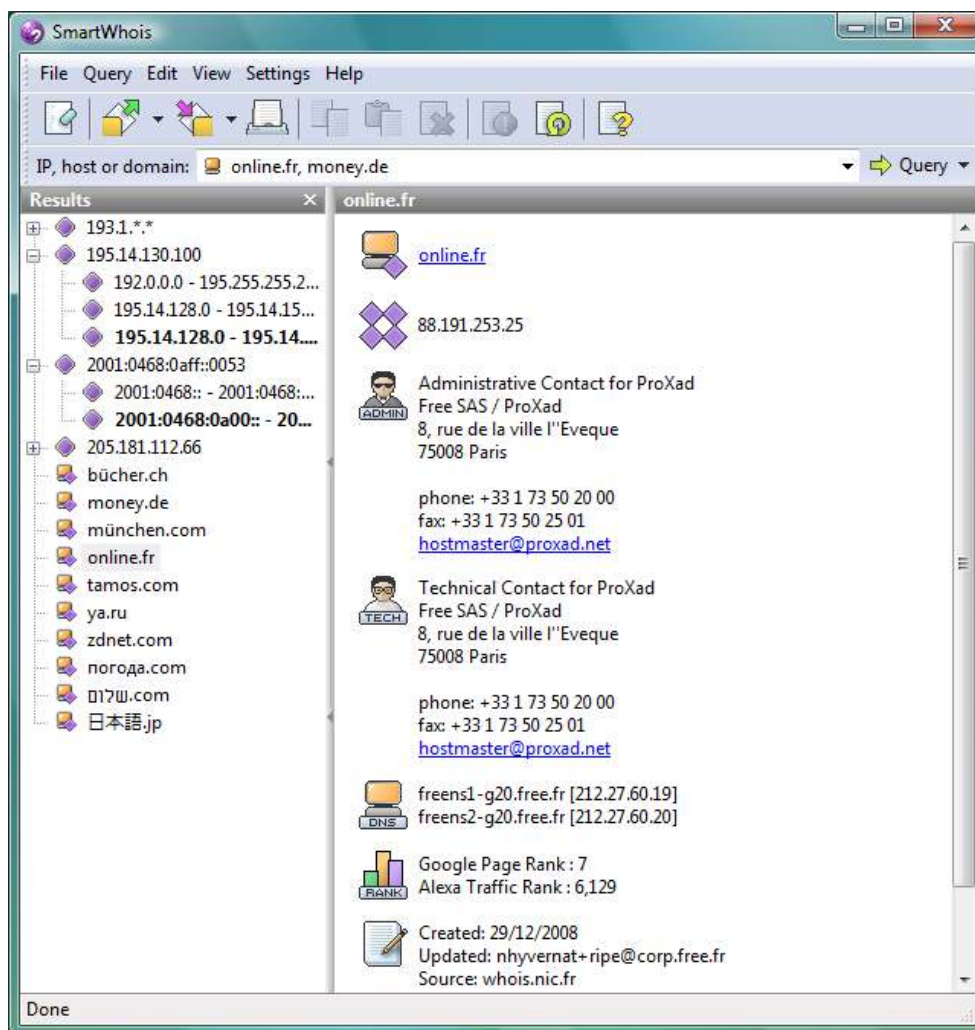
2.9.2 SmartWhois

SmartWhois is a useful network information utility that allows you 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. It helps you find answers to these important questions:

Who is the owner of the domain?

When was the domain registered and what is the owner's contact information?

Who is the owner of the IP address block?



With SmartWhois you can focus on your work; the program will unmistakably choose the right database from over 100 whois databases all over the world and fetch the most complete results within a few seconds. SmartWhois supports Internationalized Domain Names (IDNs), so you can query domain names that use

Information Gathering

non-English characters, like German umlauts, French accent grave, or fully consist of the letters from Chinese, Hebrew, Russian, and other alphabets. It also fully supports IPv6 addresses.

Features:

- Smart operation: The program always looks up whois data in the right database; you don't have to waste your time trying them all.
- Integration with Microsoft Internet Explorer and Microsoft Outlook. Look up domain owners and IP addresses in E-Mail headers instantly!
- Saving results into an archive: you can build your own database that can be viewed of flire.
- Batch processing of IP addresses or domain lists.
- Caching of obtained results.
- Hostname resolution and DNS caching.
- Integration with CommView Network Monitor: Can be accessed from CommView for quick, easy lookup.
- Calling SmartWhois directly from your application. See SmartWhois FAQ.
- Wildcard queries.
- Whois console for custom queries.
- Country code reference.
- Customizable interface.
- SOCKS5 firewall support.

Who needs SmartWhois

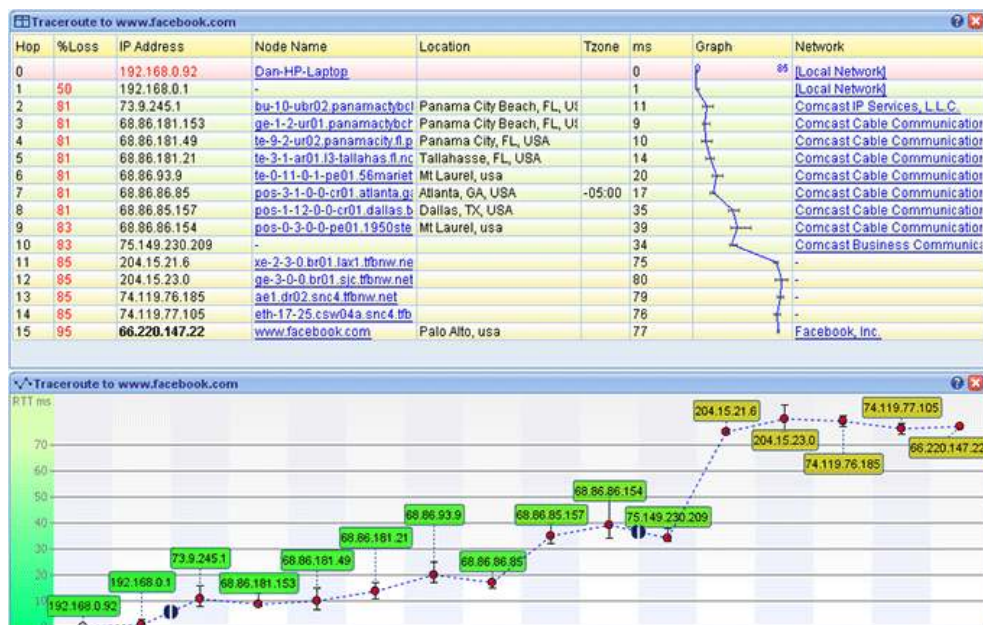
- Everyone who uses standard Whois utilities: SmartWhois saves a lot of time and does things standard Whois utilities can't do.
- People who hate spam or want to identify the origin of suspicious E-Mail messages: check the message header and locate the real sender! You can also send E-Mail to the network administrator with a mouse click.
- Webmasters who want to study the logs more carefully and are unable to identify many IP addresses.
- Online vendors who want to learn exactly where an order comes from.
- People who want to identify the origin of suspicious E-Mail messages by studying the headers.

2.9.3 VisualRoute

VisualRoute Features and Benefits

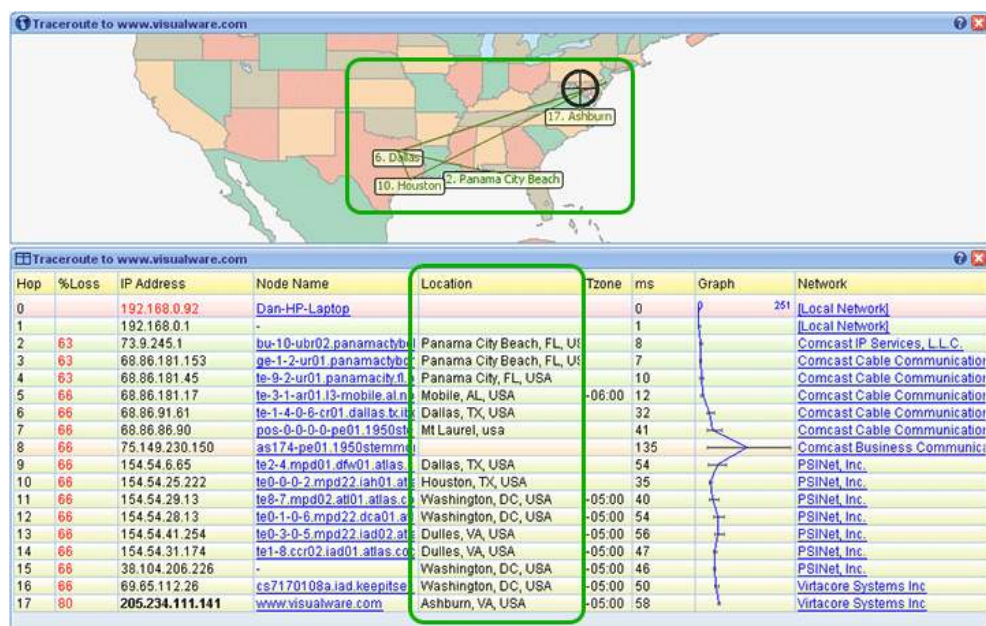
Graphical View of Traceroute provides key data in an easily digestible way.

Results from several essential network diagnostic tools are integrated into an overall connectivity report, providing a graphical view of connection performance report including packet loss and latency for each network hop. Drill-down detail is easily visible with a mouse over any network hop.



IP Location Reporting

The physical geographical locations of network servers and routers is key information for understanding routing problems, viewing the actual route path on global map provides an instant of picture of routing efficiency and distances. Try an IP trace online.



Whois Lookups, Network Provider Reporting

Get instant lookups of domain information from worldwide databases, so you can see the registered 'owner' of an IP address or domain. See the contact information for the company providing Internet access for each hop of a network route, so you can easily report network problems.

OmniPath™ Multiple Path Discovery

Get real-time views of all possible routes to a destination and easily compare the performance of different routes. The common use of load-balancers creates multiple paths that data packets may travel between the source and destination. OmniPath discovers the various paths, enables you to easily see which routes are the fastest/slowest, have the highest/lowest packet loss, or have the highest probability. More info.

NetVu™ Multiple Route Topology Graph

See a high-level view of all network routes for open trace reports, enabling easily identification of network nodes that are common to multiple routes, and network routes that have multiple path options due to load balancers or router configurations.

NetVu enables you to consistently monitor all possible paths between the source and destination for multiple routes in a single diagram, view the common nodes, and locate single points of failure. The diagram updates when even a new trace is performed, when used with the continuous trace option you can easily check the health of your network by viewing changes in the diagram.

Application Port Testing, Port Probing, DNS Performance Testing

Trace specific application ports to test if your critical applications are up and responding as expected. VisualRoute measures and reports on DNS (domain name service) response time, which can have a significant effect on connectivity performance.

Traceroute Tests from Visualware Servers

Test from Visualware servers in Washington and London to test connectivity to your servers or network devices. This capability provides additional testing points to help identify network routes and network providers causing poor performance. Try a traceroute test now.

Continuous Connection Testing with Report History

Continuous network testing from the VisualRoute desktop to another network location supports automated cycling of connectivity tests to monitor performance degradation that may occur over long periods of time.

Reverse Traces from Remote Desktops Help Resolve Customer Connectivity Problems

The SupportPro Edition enables support staff to test connectivity in both directions: to/from the VisualRoute desktop and to/from remote systems. This capability provides visibility to connectivity problems that occur in one direction only, such as from the customer location to your server — problems that are otherwise very difficult to pinpoint without imposing on the customer or traveling to the remote location. The SupportPro Edition utilizes remote agents to make reverse tracing a quick and easy process.

IPv6 Compatibility

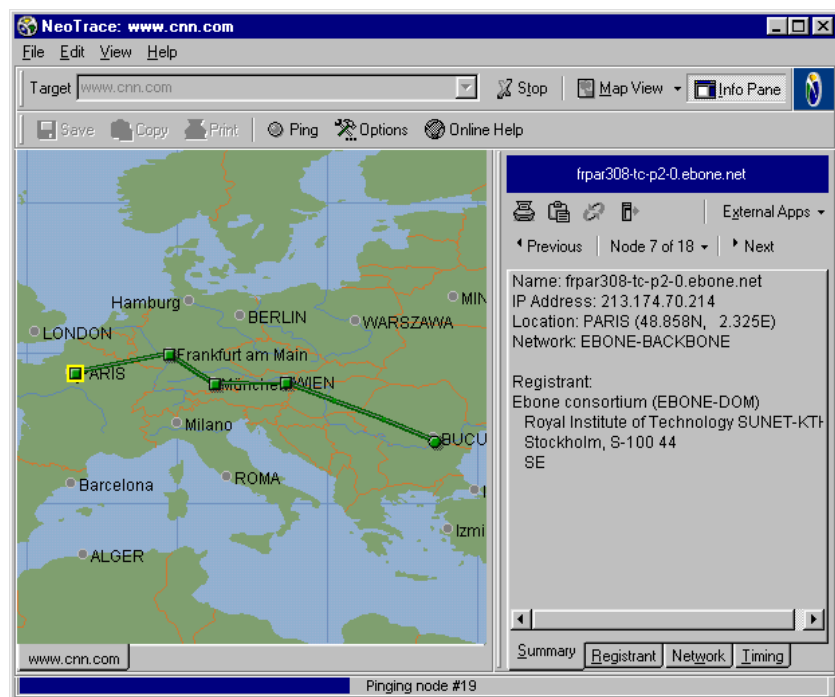
IPv6 is the next generation of the Internet Protocol, the system by which data is transferred across the Internet. VisualRoute 2009 enables traces to IPv6 addresses, including IPv6 domain and network provider lookups.

2.9.4 McAfee NeoTrace Professional

McAfee NeoTrace Pro delivers a powerful tool for checking information on internet locations.

You can trace any computer on the internet simply by entering an E-Mail, IP address or URL. The display shows you the route between you and the remote site including all intermediate nodes and their registrant information.

McAfee NeoTrace is the world's most popular Internet tracer, used by law enforcement, ISPs, and network professionals, yet easy enough for the home user. Explore the powerful new features designed to make our most popular product even easier to use!



Features:

- Internet Explorer Integration Website tracing is just a click away with our IE browser integrated Trace Button.
- Variety of Graphical Information The Node View complements improvements in our existing Map and List Views, offering users a wide range of graphical data for precision tracing.
- Detailed Map View Map View shows most detailed available map for current view using expanded regional information.
- Streamlined List View Node data is simple to understand with an integrated graph and an array of user-configurable data columns.
- Expanded Geographical Data Improves accuracy of node placement with increased server based lookups for all traces.
- HackerWatch.org Event Reporting when using McAfee NeoTrace in conjunction with a firewall it is simple to submit event reports to HackerWatch right from McAfee NeoTrace.
- Mail Server Tracing E-Mail address entry allows McAfee NeoTrace to locate the mail server for that address.
- Many Save Formats Allows trace data, maps or both to be saved in formats such as JPG, PNG, BMP, HTML, RTF, and plain text

2.10 SECURING E-MAIL ACCOUNTS

To secure the E-Mail Account from the Crackers/ Hackers is one of the major challenges for all of us now a days. However, we can still try our level best to making it secure by using the following ways mentioned below:

2.10.1 Creating Strong Passwords

Creating strong Passwords for all your online accounts is not a thing you should do. It is one of the most important thing you must do. In case you are still thinking that your Password is strong and safe, maybe it's time to wake up.

What makes a strong Password?

I shall not elaborate on this, since many sites have already discussed this in great detail. In a nutshell, a strong Password must constitute the following:

- It needs to contain special characters such as @#\$\$%^&
- It must be at least 8 characters long.
- It must not have any common words such as "123", "Password", your birth date, your login name and any words that can be found in the dictionary.
- A variation of capitalization and small letters.

Even if your Password consists of the above, it is still not secure enough. Your Password needs to be totally unique and different for each and every one of your online accounts. This is to make sure that in the event that one account is hacked into, your other accounts will not get affected.

You must be wondering that how you are going to remember so many Passwords when you have a problem remembering your existing one. Here are some steps that could be used as they are very powerful. Here it is;

- 1) First, think of a thing, date, phrase, event, place or anything that is unique only to you. It must be of at least 8 characters long. For demonstration purpose, a name "Damien Oh" will be used as the term throughout this topic. Note that the capital letters and the space in between the name are part of this term. For your own account, please select a term that is difficult for others to guess.
- 2) Use the following rules to replace the regular characters with special characters. You could even form your own rules.
 - Replace all the 'a' with @
 - Replace all the 's' with \$
 - Replace any space with %
 - Replace any 'o' with 0
 - Replace any 'i' with !
 - In this case, the simple term Damien Oh becomes D@m!e%Oh.
- 3) Now go to Password Meter (see "MakeUseOf" review here) and test the strength of your term. This is the result of the above term. If your term is not strong enough, you will see a list of items that you can improve on.

The Password Meter

Home | Feed

Test Your Password		Minimum Requirements			
Password:	●●●●●●●●	<ul style="list-style-type: none"> Minimum 8 characters in length Contains 3/4 of the following items: <ul style="list-style-type: none"> Uppercase Letters Lowercase Letters Numbers Symbols 			
Hide:	<input checked="" type="checkbox"/>				
Score:	90%				
Complexity:	Very Strong				
Additions		Type	Rate	Count	Bonus
+	Number of Characters	Flat	$+(n*4)$	9	+ 36
+	Uppercase Letters	Cond/Incr	$+(11e-n)*2$	2	+ 14
+	Lowercase Letters	Cond/Incr	$+(11e-n)*2$	4	+ 10
×	Numbers	Cond	$+(n*4)$	0	0
+	Symbols	Flat	$+(n*6)$	3	+ 18
+	Middle Numbers or Symbols	Flat	$+(n*2)$	3	+ 6
✓	Requirements	Flat	$+(n*2)$	4	+ 8

- 4) Once you are happy with your term and are sure that only you can decipher it, go to any of your online accounts now. To set a Password for that account, append the name of the site, or the URL of the site to the end of your term.

For example, for a MakeUseOf account, you may use D@m!en%0hM@keU\$e0f as your Password and use D@m!en%0hG00g!em@!l for Gmail account. If you do this for each and every one of your sites, you will be surprised to find that you have just created tens, hundreds, or even thousands of different Passwords that you can be remembered easily. Instead of the site name or the URL, you can also put a variation of the site names or any other names that are related to the site.

Is that enough?

That is just the beginning. To really make it secure and hard for others to guess, you must change your Passwords on frequent basis. Some of you may find it an assignment to come up with new Passwords every month. Here is what you can do:

Instead of appending the site name to the end, you can now append it to the front, in the middle or even split the site name out into few parts. For example:

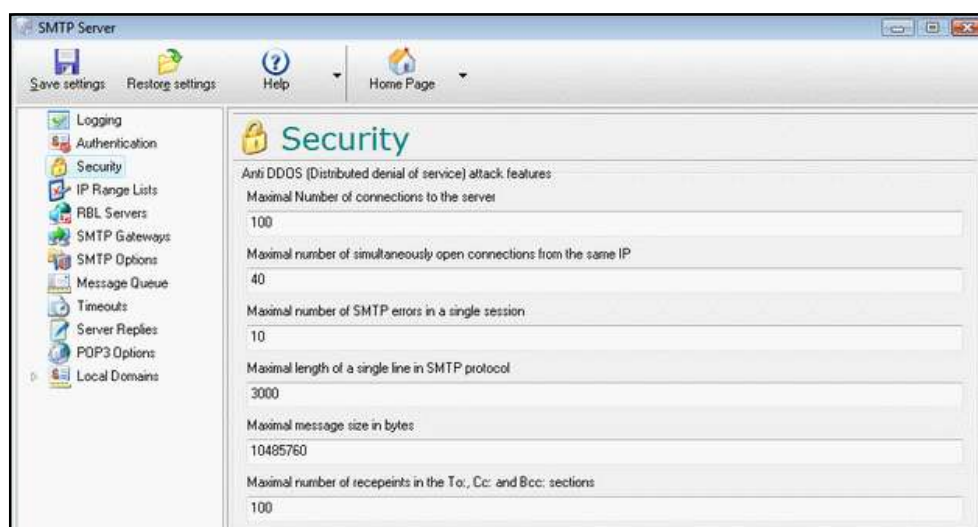
- M@keD@m!enU\$e0h0f
- M@keU\$eD@m!en%0h

You can also change the replacement characters such as @ for ~ and whatsoever. You can also do a complete changeover of your term to come up with a totally different Password.

Some important points to be noted

- Always check the strength of the Password provided to you on Password strength meter.
- At the time of creating a new mail account provide verification question so that it can be used to recover the forgotten Password for that particular E-Mail id.
- Always try to provide the secondary E-Mail id so that new Password could be mailed or Password change instructions could be mailed to you on that particular mail id.
- Never click on "Keep me sign in" check box, if you have selected this option and if Attacker gains access of your computer then he can sign in your account as well as he can recover your Password.

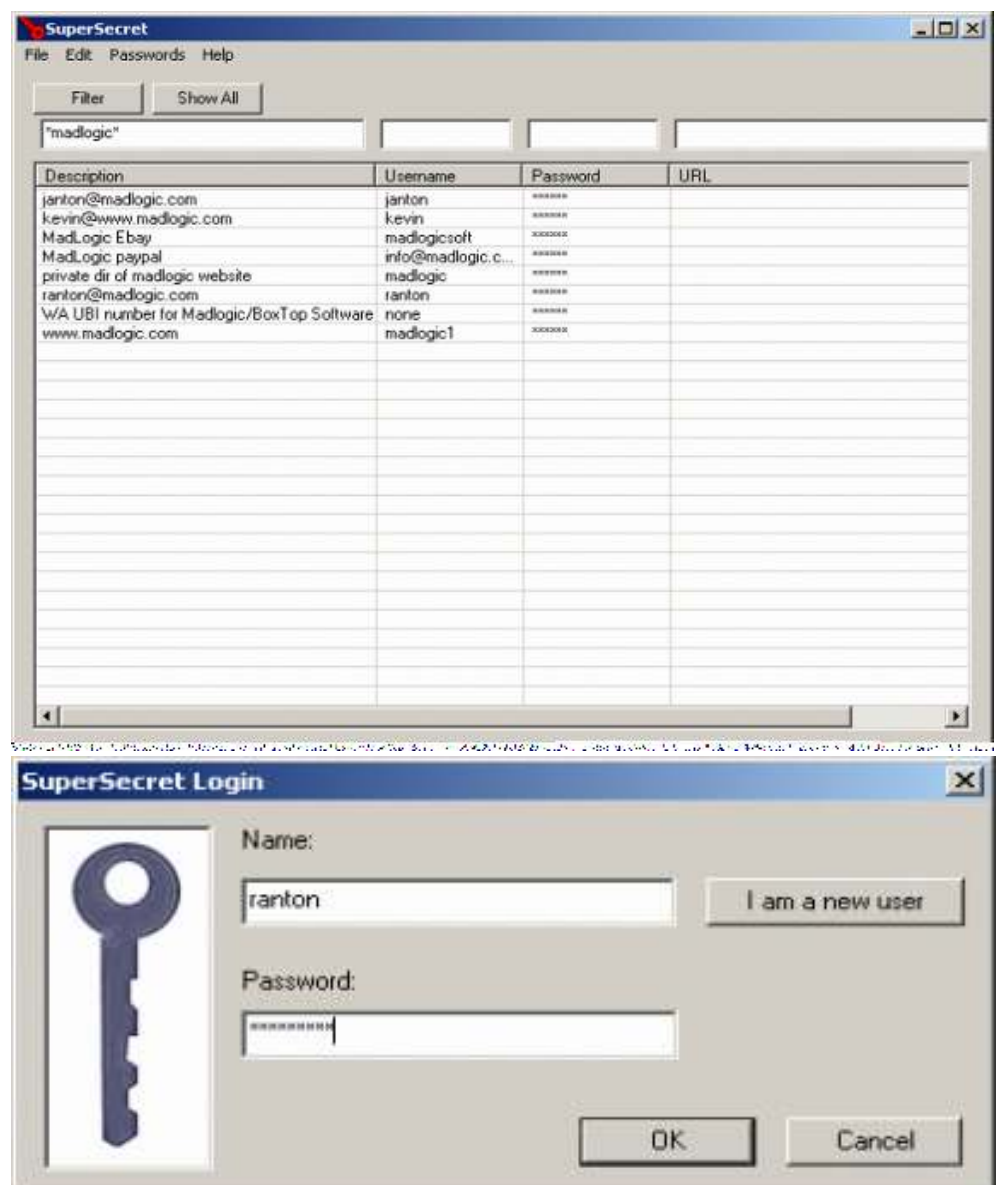
2.10.2 E-Mail Protector



Information Gathering

Do you know that when you send your E-Mail messages, they do not go directly to recipient mailboxes? Do you know that your Internet Service Provider (ISP) stores copies of all your E-Mail messages on its mail servers before it tries to deliver them? Do you know that someday all the information kept on the servers can be easily used against you? E-Mail Security is a system-tray local SMTP server program for Windows that lets you send E-Mail messages directly from your PC to recipient mailboxes ensuring your E-Mail security and privacy by means of bypassing your ISP's mail servers where your relevant information can be stored and viewed. Do you also know that when you send an E-Mail message to a list of E-Mail addresses, the respondents can see each other in the E-Mail message header? You think it is secure? While sending, E-Mail Security always breaks E-Mail messages addressed to a group of people to individual messages to ensure your security and security of your respondents. Also, E-Mail Security does not leave any traces on your PC because it just gets your E-Mail messages from your E-Mail client and puts them in the recipient mailboxes at the same time without making any temporary files on your PC. E-Mail Security supports all E-Mail programs like Outlook Express, Outlook, Eudora, etc. The E-Mail program you already use for sending and receiving messages can be connected to E-Mail Security in a very easy way – just by using the word “localhost” instead of your current SMTP host. Having done so, you can send messages in a usual manner. Install E-Mail Security on your PC before it is too late!

2.10.3 SuperSecret



SuperSecret provides secure storage for all of your logins and Passwords so that you only have one Password to remember from now on. SuperSecret supports multiple users on the same computer using different SuperSecret login names so that you can keep your Passwords private, even if you share a computer with others at work or home. Now with version 2 SuperSecret supports filtering Passwords by the login name, Password, or the entry description so that you can quickly find the Password you need. You can also store a URL for each entry so you never forget where you need to go to access your online accounts. SuperSecret can generate secure, random Passwords for you.

Only one Password is required to use SuperSecret. All of your other account and Password information is stored securely in an encrypted format on your computer and can be accessed only with your one and only Password. SuperSecret allows each family member or co-worker to have his/her own storage area for Passwords. Your confidential information is safe even if prying intruders are sitting at your computer, because SuperSecret's data can only be accessed by your one secret Password.

Use SuperSecret to remember all of your Passwords. Remember your Password to your personal E-Mail address, business E-Mail address, online banking login and Password. Store any kind of secret with SuperSecret. Keep track of the PIN number to that ATM/debit card you never use. Others will not be able to access your private information. And SuperSecret is quick and easy to use. Simply double click on an empty entry to add a new login and Password or double click on an existing entry to edit it.

Select the entry you need the Password for and the Password will be displayed; deselect the entry and the Password will be hidden again to protect you from anyone who may look over your shoulder.

You can keep SuperSecret open to save time by minimizing it to the taskbar for easy access. SuperSecret runs on W indows 95, W indows 98, W indows ME, W indows NT, W indows 2000, and W indows XP.

Check Your Progress 5

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

What are the different ways of tracing ip address? Expalin any one. Highlights the points of securing E-Mail accounts?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2.11 LET US SUM UP

This unit throws light on “E-MAIL CRIME AND INVESTIGATION”. E-Mail, as simple as it is to use, relies on a more complicated set of operating procedures than that of the Web. For most users, its operation is transparent, which means that it is not necessary to understand how email works in order to be able to use it.

This unit help users to understand its basic principles, give them an idea of how to best configure their email clients and inform them about the underlying mechanisms of spam. This unit also provides useful background information on E-Mail security issues. It will help you to examine the security threats facing by your corporate E-Mail system and determine what kind of E-Mail security solution your company needs. A variety of different elements weaken your corporate email system and while some are widely known – such as email viruses – others tend to be ignored. Emails carrying of fensive messages or confidential corporate information can create immense inconvenience and expense for a company that has not equipped its mail server with the appropriate tools. The same goes for spammers who use the email system at work to send thousands of unsolicited email messages.

2.12 CHECK YOUR PROGRESS: THE KEY

- 1) An electronic mail message consists of two components, the message header, and the message body, which is the E-Mail's content. etwork routes and network providrol information, including, minimally, an originator's E-Mail address and one or more recipient addresses. Usually additional information is added, such as a subject header field.

Originally a text-only communications medium, E-Mail was extended to carry multi-media content attachments, which was standardized in RFC 2045 through RFC 2049, collectively called, Multipurpose Internet Mail Extensions (MIME).

The user Mail User Agent formats the message in E-Mail format and uses the Simple Mail Transfer Protocol (SMTP) to send the message to the local mail transfer agent (MTA), in this case smtp.a.org, run by user's internet service provider (ISP).

The MTA looks at the destination address provided in the SMTP protocol (not from the message header), in this case bob@b.org. An Internet E-Mail address is a string of the form localpart@exampledomain. The part before the @ sign is the local part of the address, often the username of the recipient, and the part after the @ sign is a domain name or a fully qualified domain name. The MTA resolves a domain name to determine the fully qualified domain name of the mail exchange server in the Domain Name System (DNS).

- 2) A mail message consists of a header, which contains information about who the message was sent from, the recipient(s) and the route. Many of the header fields are not shown by default, but most programs used to read E-Mail will allow full headers to be displayed. This is then followed by the body of the message which contains whatever the sender wishes.

The message header should include at least the following fields:

- **From:** The E-Mail address, and optionally the name of the author(s). In many E-Mail clients not changeable except through changing account settings.
- **To:** The E-Mail address/addresses and optionally name(s) of the message's recipient(s). Indicates primary recipients (multiple allowed).

- **Cc:** Carbon copy; many E-Mail clients will mark E-Mail in your inbox differently depending on whether you are in the To: or Cc: list.
- **Bcc:** Blind Carbon Copy; addresses added to the SMTP delivery list but not (usually) listed in the message data, remaining invisible to other recipients.
- **Subject:** A brief summary of the topic of the message. Certain abbreviations are commonly used in the subject, including "RE:" and "FW:".
- **Message-ID:** Also an automatically generated field; used to prevent multiple delivery and for reference in In-Reply-To

The header consists of lines beginning with a keyword followed by a colon (:), followed by information on each line. A brief explanation of each field of the header is given below. This header contains most of the common fields.

- **Received:** These lines indicate the route that the E-Mail has taken and which systems have handled it and the times that it was handled.
- **Date:** The date and time at which the message was sent including time zone.
- **From:** The sender. The part in angle brackets is a real electronic mail address. This field may be user settable, so may not reflect the true sender. In this case, it shows the original sender of the message.
- **Sender:** The sender. This is inserted by some systems if the actual sender is different from the text in the From: field. This makes E-Mail more difficult to forge, although this too can be set by the sender. There are other uses for a sender field. In the example above, the sender is set to the list owner by the mailing list system. This allows error messages to be returned to the list owner rather than the original sender of the message.
- **To:** Who the mail is sent to. This may be a list or an individual. However it may bear no relation to the person that the E-Mail is delivered to. Mail systems used a different mechanism for determining the recipient of a message.
- **Cc:** Addresses of recipients who will also receive copies.
- **Subject:** Subject of the message as specified by the sender.
- **Message-id:** A unique system generated id. This can sometimes be useful in fault tracing if multiple copies of a message have been received.
- **Reply-to:** Where any reply should be sent to (in preference to any electronic mail address in the From: field if present). This may be inserted by the sender, usually when they want replies to go to a central address rather than the address of the system they are using. It is also inserted automatically by some systems
- **X-Mailer:** Any field beginning with X can be inserted by a mail system for any purpose.

The major E-Mail related crimes are:

- i) E-Mail spoofing
- i) Sending malicious codes through E-Mail
- iii) E-Mail bombing

Information Gathering

- iv) Sending threatening E-Mails
 - v) Defamatory E-Mails
 - vi) E-Mail frauds
- 3) **Received tags:** as on web blogs, reading from the bottom to top. The header says the E-Mail was originally sent from 206.85... and it was sent to 217.225... (which is the name/IP of the first mail server that got involved into transporting this message). Then suddenly, the next Received tag says the message was received from root@localhost, by mailv.fx.ro. One can also notice that so far, the Received tags do not contain any information about how the E-Mail was transmitted (the "with" tag is missing: this tag tells the protocol used to send the E-Mail).

The Message-ID field is a unique identifier of each E-Mail message. It is like the tracing ID of an express postal mail. The rule says the ID is composed by the name of the server that assigned the ID and a unique string (for example, QESADJHO@E-Mailaddressmanager.com).

- 4) For tracking purposes, the user is most interested in the from and by tokens in the Received header field. The pattern similar to:

Received: from BBB (dns-name [ip-address]) by AAA ...

Received: from CCC (dns-name [ip-address]) by BBB ...

Received: from DDD (dns-name [ip-address]) by CCC ...

In other words, mail server AAA received the E-Mail from BBB and provides as much information about BBB, including the IP Address BBB used to connect to AAA. This pattern repeats itself on each Received line. The syntax of the from token most times looks like: name (dns-name [ip-address])

Where: name is the name the computer has named itself. Most of the time user never look at this name because it can be intentionally misnamed in an attempt to foil your tracking (but it may leak the windows computer name). dns-name is the reverse dns lookup on the ip-address. ip-address is the ip-address of the computer used to connect to the mail server that generated this Received header line. So, the ip-address is gold to us for tracking purposes.

The by token syntax just provides us with the name that the mail server gives itself. But since the last mail server could be under the control of a spammer, one should not trust this name.

So, what is crucial for tracking, is to pay attention to the trail of ip-address in the from tokens and not necessarily the host name provided to us in the by tokens. For Example;

1: Received: from **tesla623.OnE-Mail.com.sg** ([203.127.89.129]) by visualroute.com (8.11.6) id f9CIVSk24480; Tue, 12 Oct 2004 12:31:29 -0600 (MDT)

3: Received: from drb.com (IIM1608 [203.127.89.138]) by **tesla623.OnE-Mail.com.sg** with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2448.0)

If one ignores line 1, one would conclude from line 3 that mail server tesla623.OnE-Mail.com.sg sent you an E-Mail, but this would be wrong. When one trace to the host name tesla623.OnE-Mail.com.sg, you are actually tracing to the IP Address lookup on that host name, which is 192.9.200.230. But as one can see from line 1, the IP Address used was really 203.127.89.129. Do not be fooled by this attempted misdirection by spammers and fraudsters.

Determine the IP Address of the Sender: Using the example E-Mail headers above and analyzing the Received header lines we can conclude:

- A Visualware employee received an E-Mail
- which came from visualroute.com (line 1)
- which came from tesla623.OnE-Mail.com.sg (line 1; line 3 confirms)
- but whose ip-address used was 203.127.89.129 (line 1)
- which came from drb.com/IIM1608 (line 3)
- but whose ip-address used was 203.127.89.138 (line 3)

So, we have just tracked this E-Mail to the source – IP Address **203.127.89.138**.

5) The different ways of tracing IP addresses are:

- i) CallerIP
- i) SmartWhois
- iii) VisualRoute
- iv) McAfee NeoTrace Professional

CallerIP Standard Edition allows real time monitoring of any machine that it is installed on. This allows you to detect suspicious activity such as spyware and see where in the world they are connecting from. Worldwide whois reports and network provider reports are also available for any connection!

Advanced CallerIP Advanced Edition (inc. all Standard features) allows you to run it as a server! This allows you to monitor the connections made to and from your machines from a remote location! Automated Alerts are also available to you are notified the moment something suspicious attempts a connection to your server(s).

- **Plot all connections**

This feature enables you to have CallerIP plot all the connections on the world map. This in turn allows for easy and quick analysis of where connections made to/from your machine reside.

- **New look table**

The new look table includes gradient fills. This means the colour of the row in the table depends on the threat of the connection. If the connection being made to your machine is harmless then the gradient will be green. Another quick and easy way to identify the threat of a connection.

- **Condensed CallerIP**

CallerIP now allows you to minimize it to a very small and detailed dialog box. The small window gives you everything you need to know but stays in the background.

- **Real-time monitoring instantly identifies suspect activity and spyware**

CallerIP monitors all connections to and from your system and actively scans ports for possible back doors that allow unauthorized access.

- **Identifies the country of origin for all connections**

A connection to/from a high-risk country is a key indicator of suspect activity and could likely be someone looking to steal your confidential information or compromise your system. CallerIP shows you the country location of connections so you can identify suspect activity and protect your information.

- **Network Provider reporting with abuse reporting information**

See the contact and abuse reporting information for the company providing internet access for an IP address or website, so you can easily report hackers or Internet abuse.

- **Worldwide Whois reports**

Caller IP Pro queries worldwide databases to report the up-to-date registration information for the 'owner' of an IP address or domain. Information includes name, address, phone and E-Mail contact information.

- **Detailed log of connection history with search options**

Each connection or attempted connection is automatically logged, with search capabilities for quick lookups of past connection activity.

For securing E-Mail accounts:

- a) The user should Create Strong Passwords
- b) E-Mail Protector
- c) SuperSecret