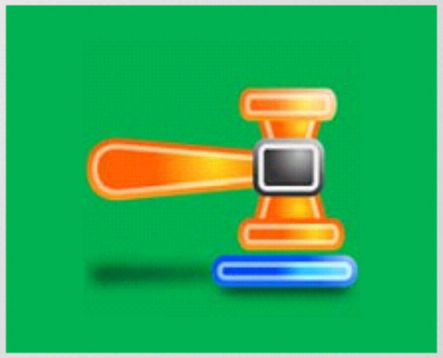
Investigating Email Crimes

Module 12

Designed by Cyber Crime Investigators. Presented by Professionals.



Module Objectives

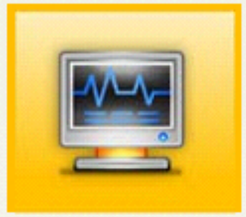
CHFI Computer Hacking Forensic Investigator

After successfully completing this module, you will be able to:

1. Understand Email System, Email Clients and Email Servers, along with their characteristics
2. Understand the importance of electronic records management
3. List the email crimes and discuss the crimes committed via chat room
4. Describe the components of an Email message
5. List Common Headers and X-Headers
6. Review the steps to investigate email crimes and violations
7. List all the email forensics tools
8. Discuss about the U.S. Law against email crime: CAN-SPAM act and its characteristics

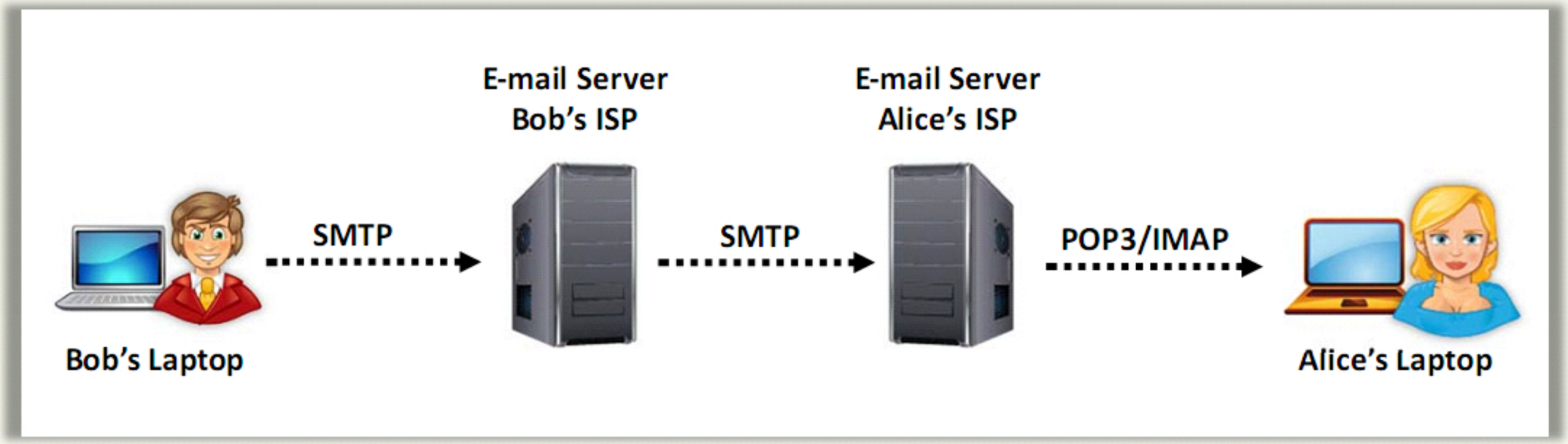
Email System

An e-mail system encompasses of the servers that send and receive e-mails on the network, along with the e-mail clients that allow users to view and compose messages



Email systems are based on a **client-server** architecture

The mail is sent from the client to a **central server**, which then reroutes the mail to its intended destination



Email Clients

An e-mail client, also known as a **mail user agent (MUA)**, is a computer program meant for accessing and managing emails

E-mail clients perform the following functions:

- Display all the messages in a **user's inbox**. The message header typically shows the **date**, **time**, **subject of the mail**, sender of **the mail**, and the **mail's size**
- Allows the user to select a message and access the data in the message
- Allows the user to create e-mails and send them to others
- Allows the user to send file attachments with the message and can also save any attachments received in other messages

Most commonly used email clients:

- **Standalone** - Microsoft Outlook and Thunderbird
- **Web-based** - Gmail and Yahoo! Mail

Email Server

An e-mail server connects to and serves several e-mail clients

An e-mail server works in the following ways:

- An **e-mail server** has a number of **e-mail accounts**; typically each person has one account
- The server maintains a text file for each account. This text file contains all the messages for that account
- Whenever a user clicks the **Send** button in his or her e-mail client, the client connects to the e-mail server and passes the message and its accompanying information (including the sender and receiver) to the server
- The server formats that information and attaches it to the bottom of the receiving user's **.txt file**. The server also saves the time, date of receipt, and subject line into the .txt file
- If the users want to view the messages using e-mail applications, then he or she has to send a request to the server via the **e-mail client application**

An e-mail server comprises of 3 components:

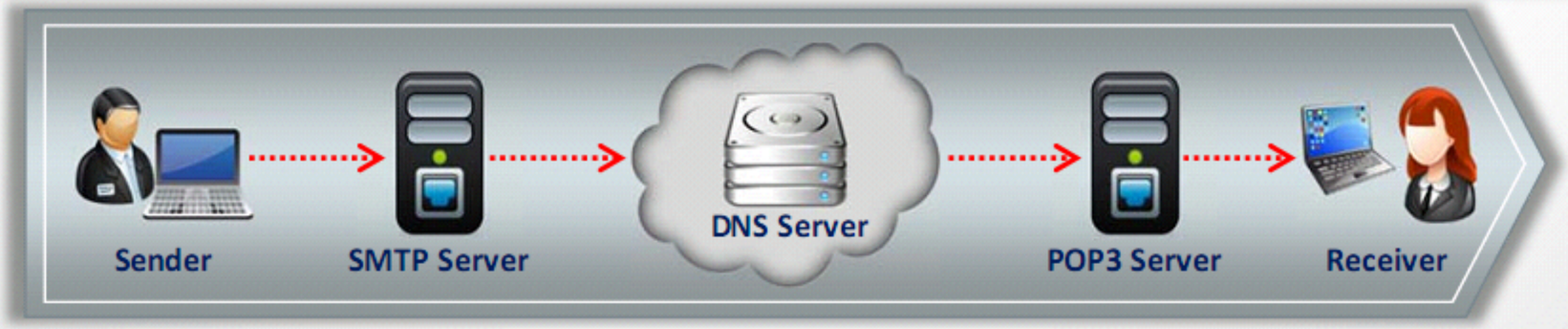
- POP3
- SMTP
- IMAP

SMTP Server

- Simple Mail Transfer Protocol (SMTP) is an Internet protocol for transmitting e-mail over IP networks
- The SMTP servers listen on port 25 and handle all outgoing e-mails
- When a user sends an e-mail, the sender's host SMTP server interacts with the receiver's host SMTP server
- Consider an example where a user has an account with ***myicc.com***, and he or she wants to send a mail to john@mybird.com through a client such as Microsoft Outlook

The procedure works as follows:

- When the user clicks on the **Send** button, Outlook connects to the server of ***myicc.com*** via port 25
- The client notifies the SMTP server about the sender's address, recipient's address, and body of the message
- The SMTP server breaks the recipient's address into the following parts:
  - The recipient's name (john)
  - The domain name (*mybird.com*)
- The SMTP server contacts the DNS (Domain Name Service) server and queries about the IP address of the SMTP server for ***mybird.com***
- The SMTP server from ***myicc.com*** connects to the SMTP server for ***mybird.com*** using port 25 and sends the message to it. The SMTP server at ***mybird.com*** receives the message and transfers it to the POP3 server



POP3 Server

Post Office Protocol version 3 (POP3) Server

- POP3 is an Internet protocol, which is used to retrieve e-mails from a mail server
- A POP3 server handles incoming mails
- The server contains one text file for each e-mail account
- The POP3 server acts as an intermediary between the e-mail client and the text file
- When a message arrives, the POP3 server appends that message to the bottom of the **recipient's text file**, which can be retrieved by the e-mail client at any preferred time
- An e-mail client connects with a POP3 server via **port 110**
- The POP3 downloads the emails to a single device (computer, tablet, smartphone, etc.) and then usually deletes it from the server
- Drawback of POP3 is that the emails can be accessed only from one device

IMAP Server

Internet Message Access Protocol (IMAP) Server

1. Internet Message Access Protocol (IMAP) is an Internet protocol, *which is designed for* accessing **e-mail on a mail server**
2. IMAP servers are similar to POP3 servers, as it handles all the incoming mails like POP3
3. An e-mail client connects to an IMAP server via **port 143**
4. Unlike POP3, this protocol keeps e-mails on the server even after the user has already downloaded them, thus enabling the user to use multiple devices to check the email
5. In IMAP, the user can also arrange e-mails into folders and store the folders on the server

Importance of Electronic Records Management

Electronic records management is the branch of management sciences, which is responsible for the **efficient** and **systematic control** over the process of creation, receipt, maintenance, use and disposition of electronic records, including the **processes for capturing** and **maintaining digital evidences** and information for legal, fiscal, administrative, and other business purposes

Importance of electronic records management:

01 It helps in non-repudiation of electronic communication so that no-one can deny being the **source of a particular communication**

02 It acts as a deterrent for **abusive** and **indecent materials** in e-mail messages

03 It helps in the **investigation** and **prosecution** of e-mail crimes

Email Crimes

- E-mail has become the most **preferred method of communication** because of its ease of use and speed. But this has also made e-mail a powerful tool for criminal activities.
- **E-mail crime can be categorized in two ways:**

- Crimes committed by sending e-mails
  - Spamming
  - Phishing
  - Mail bombing
  - Mail storms

- Crimes supported by e-mails
  - Identity Fraud
  - Cyber-stalking
  - Child pornography
  - Child abduction

Crime Via Chat Room

1. A chat room is a **website or part of a website** where a number of users, often with common interests, can communicate in real time
2. Chat rooms are being **increasingly used in a variety of crimes** such as child pornography, cyber stalking, and identity thefts
3. They are a regular feature of different adult sites and are extensively used to **disseminate obscene materials** over Internet
4. They can also be used as a **social engineering** tool to collect information for committing several other crimes

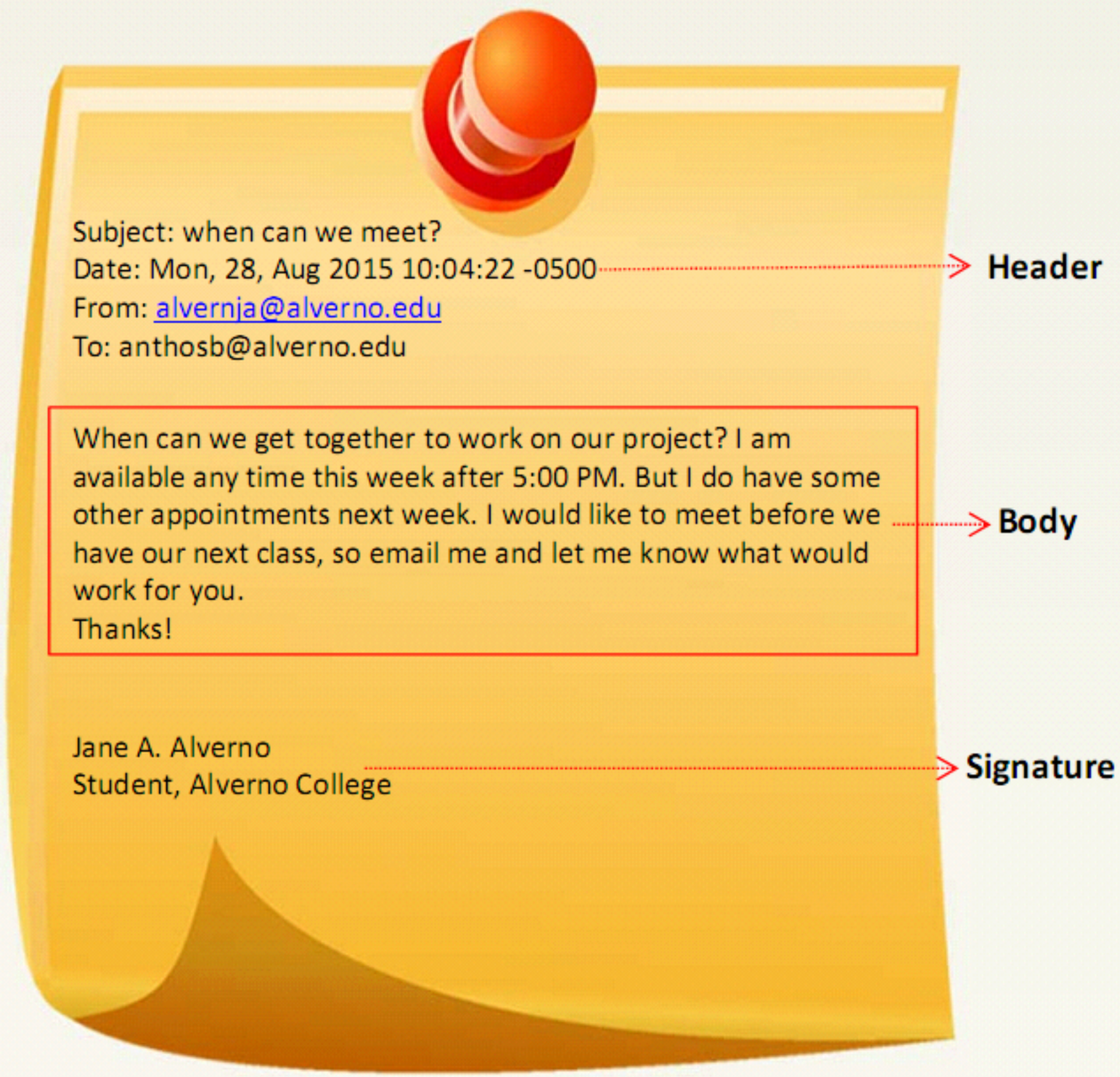
Email Message

An email message is composed of three parts:

1. **Header**
   - E-mail headers contain **information about the e-mail origin** such as the address from where it came, the routing, time of the message, and the subject line
   - Some of the **header information** that is usually important to a technician is kept **hidden** by the email software
   - Examples include To, Cc, Bcc, From, Message-Id, Reply-To, Sender, Subject, MIME-Version, Priority, etc.
2. **Body**

   Body contains the actual message
3. **Signature**

   Provides information to the **recipients** about the identity or designation of the senders. Email programs can be set to enter this **line automatically** on all the emails sent



Sample Email Header

Apple.png - j ... de1 | https://mail.google.com/n

https://mail.google.com/mail/?ui=2&ik=d1f5a533d5&view=om&th=1536a9904c40d79f

```
Delivered-To: juliannejade123@gmail.com
Received: by 10.25.143.148 with SMTP id r142csp1515131lfd;
        Sat, 12 Mar 2016 03:32:06 -0800 (PST)
X-Received: by 10.107.198.133 with SMTP id w127mr14742654iof.58.1457782326349;
        Sat, 12 Mar 2016 03:32:06 -0800 (PST)
Return-Path: <3Nf7jVhkJAH4fcpkgn.dgykpivqp.qhhkekcniockn.eqo@doclist.bounces.google.com>
Received: from mail-io0-x248.google.com (mail-io0-x248.google.com. [2607:f8b0:4001:c06::248])
        by mx.google.com with ESMTPS id k98si16073806ioi.57.2016.03.12.03.32.05
        for <juliannejade123@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Sat, 12 Mar 2016 03:32:06 -0800 (PST)
Received-SPF: pass (google.com: domain of 3Nf7jVhkJAH4fcpkgn.dgykpivqp.qhhkekcniockn.eqo@doclist.bounces.google.com
designates 2607:f8b0:4001:c06::248 as permitted sender) client-ip=2607:f8b0:4001:c06::248;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of 3Nf7jVhkJAH4fcpkgn.dgykpivqp.qhhkekcniockn.eqo@doclist.bounces.google.com designates
2607:f8b0:4001:c06::248 as permitted sender)
smtp.mailfrom=3Nf7jVhkJAH4fcpkgn.dgykpivqp.qhhkekcniockn.eqo@doclist.bounces.google.com;
       dkim=pass header.i=@gmail.com;
       dmarc=pass (p=NONE dis=NONE) header.from=gmail.com
Received: by mail-io0-x248.google.com with SMTP id z76so233321001iof.1
        for <juliannejade123@gmail.com>; Sat, 12 Mar 2016 03:32:05 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20120113;
        h=mime-version:reply-to:references:message-id:date:subject:from:to;
        bh=iaDa8WcbKWSkkdh3kBufiXTgkR1l6rwPMtKuwBmSoXg=;
        b=08ruf6jJsJcpvu3eIMnHL9mdalV/1IypPHDM0UpfBjdhhhrRUGdcz7qQ+sHe0lgdTq
         ythFzT43LpRHiG6ZO2SWXw5aeCKo6/rMOxOID3o4K585Mi6+p7LYbSSDMP0tKFvV/fGA
         TK7PYphgyjOVzG0OZegROx/Ifdfn8g9RB6J7PQ+kX//lm/y3mParGatx6GBS/igPzEmo
         qtrZMOIeW3AVMXbLIJWT73ZzPMHZIPbltMNfgAra1srRTEFFHk3pe/9+USUswamNsJN8
         2AaUkoLWGt48xu7aTOl+47ahI5SM8V+zTRPnD0sY6oM7dV9XXfcXOco/eonZWX0d5nhi
         Mrug==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20130820;
        h=x-gm-message-state:mime-version:reply-to:references:message-id:date
```

List of Common X-Headers

- X-Headers is the generic term for headers starting with a **capital X** and a **hyphen**
- The common notion is that X-headers are **nonstandard** and are provided for information only, and that, conversely, any nonstandard informative header should be given a name starting with *X-*

Some common X-headers:

- X-Confirm-Reading-To
- X-Distribution
- X-Errors-To
- X-Mailer
- X-PMFLAGS
- X-Priority
- X-Sender
- X-UIDL

Steps to Investigate E-mail Crimes and Violations

- E-mail systems and chat applications allow criminals to perform various **malicious activities**. In such conditions, e-mail and chat history can provide clues to the identity of the criminals and may become the evidence for solving cyber crimes

Steps involved in investigating e-mail crimes and violations:

1. Obtain a Search Warrant
2. Examine e-mail messages
3. Copy and print the e-mail messages
4. View the e-mail headers
5. Analyze the e-mail headers
6. Trace the e-mail
7. Acquire e-mail archives
8. Examine e-mail logs

Obtain a Search Warrant and Seize the Computer and E-mail Account

A search warrant application should include the **proper language** to perform on-site examination of the suspect's **computer** and the **e-mail server** used to send the e-mails under investigation

Seize all **computers** and **e-mail accounts** suspected to be involved in the crime

Email accounts can be seized by just changing the **existing password** of the e-mail account, either by asking the suspect his or her password or obtaining it from the mail server

Examine E-mail Messages

C|HFI Computer Hacking Forensic Investigator

01 After ratifying the e-mail crime, investigators require evidence to prove the crime and identify the person responsible for the crime

02 To obtain evidence, investigators need access to the received email from victim's computer for further examination

03 As with all forensic investigations, analysis should not be done on the original data. Thus the investigator should image the victim's computer prior to the analysis

04 Then, the investigator should physically access the victim's computer and use the same e-mail program the victim used to read the e-mail

05 If required, the investigator can get the username and password from the victim and logon to the e-mail server

06 If physical access to a victim's computer is not feasible, the investigator should instruct the victim to open and print a copy of an offending message, including the header

07 The header of the e-mail message has a key role in tracing the e-mail, because it contains the unique IP address of the server that sent the message

Copy and Print the E-mail Message

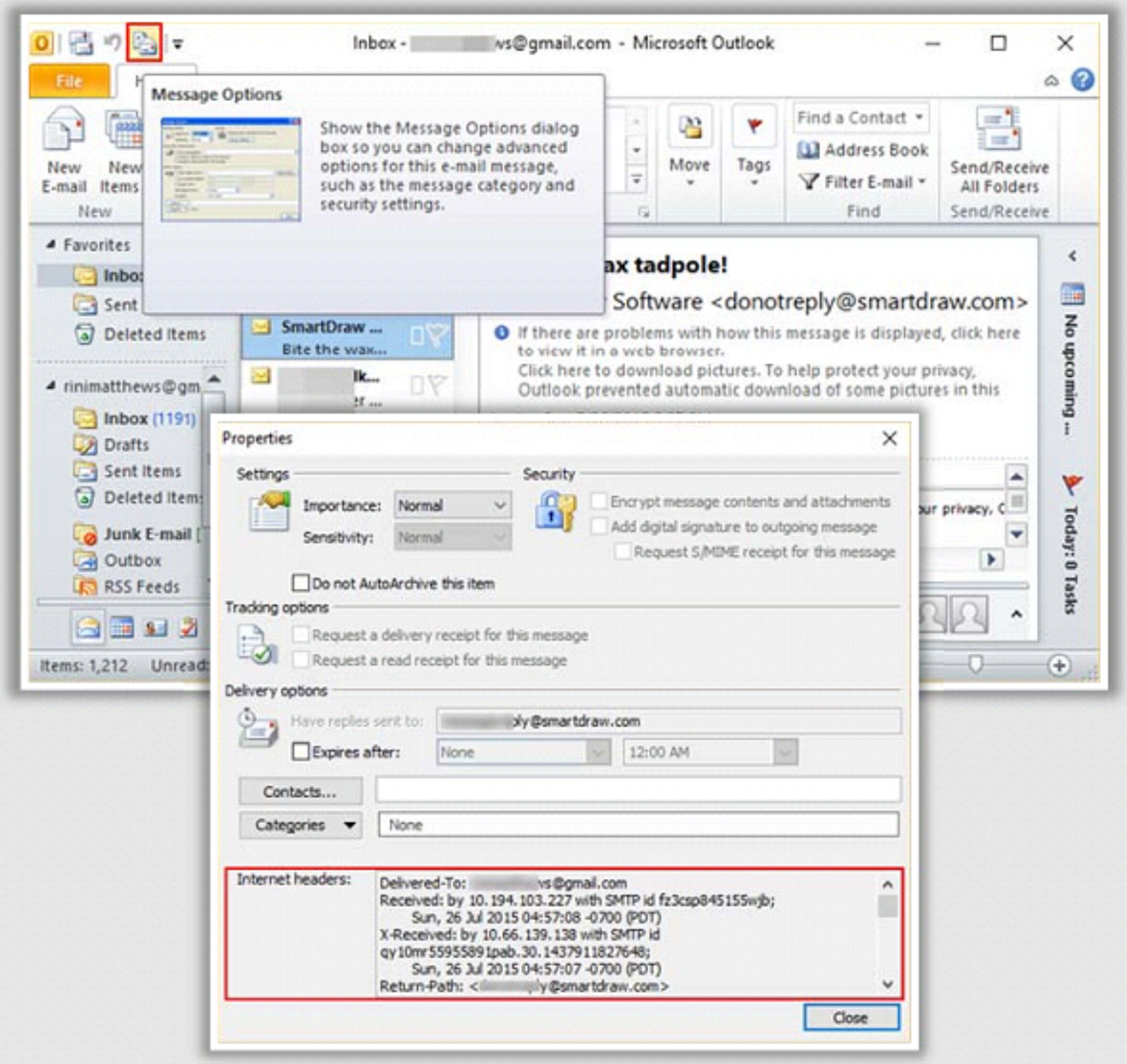
- An **e-mail investigation** can be started as soon as the offending e-mail message is copied and printed
- Some e-mail clients will allow an investigator to **copy e-mail messages** from the inbox folder to a **portable device**

Steps to copy an e-mail message using Microsoft Outlook:

1. Insert a formatted USB key into the machine's USB port
2. Navigate to **My Computer** or **Windows Explorer** to access the USB key
3. Open **Microsoft Outlook**
4. Click the folder that contains the offending message, while keeping the folders list open.
5. A list of messages in the selected folder will be displayed in the mid-section of the panel. Click the message you want to copy
6. Resize the Outlook window to see both the message to be copied and the USB drive icon
7. Drag the message from the Outlook window to the USB drive icon
8. The next step after copying the e-mail message is to print it. Go to **File** menu → click **Print** → click **Print Options**. Select the settings for printing in the Print dialog box and then click the **Print** button
9. You can include the printed e-mail copy in your final report

Viewing the E-mail Headers in Microsoft Outlook

- The e-mail header plays a vital role in forensic investigations as it holds detailed information on the e-mail's origin. Therefore, an investigator should successfully capture the e-mail header.
- After copying the e-mail message, the e-mail header can be retrieved. This process is different for each e-mail program.

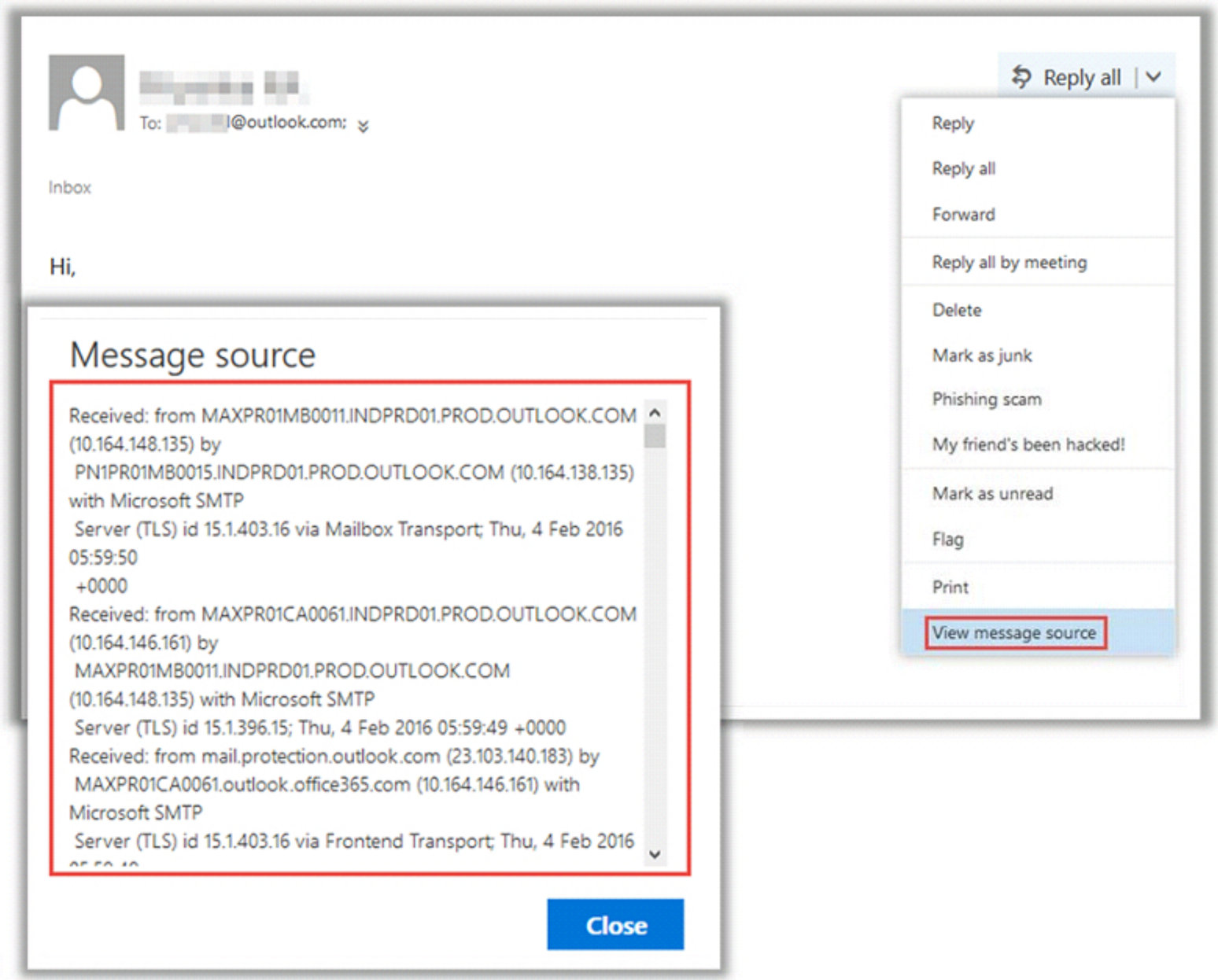


Steps below are in reference to Microsoft Outlook 2010 desktop application:

- Launch **Microsoft Outlook** and open the copied e-mail message
- Click **Message Options** icon located on the top-left of the screen
- This opens a **Properties** window. Select the message header text from the **Internet headers:** box, then copy and paste the text in any text editor and save the file

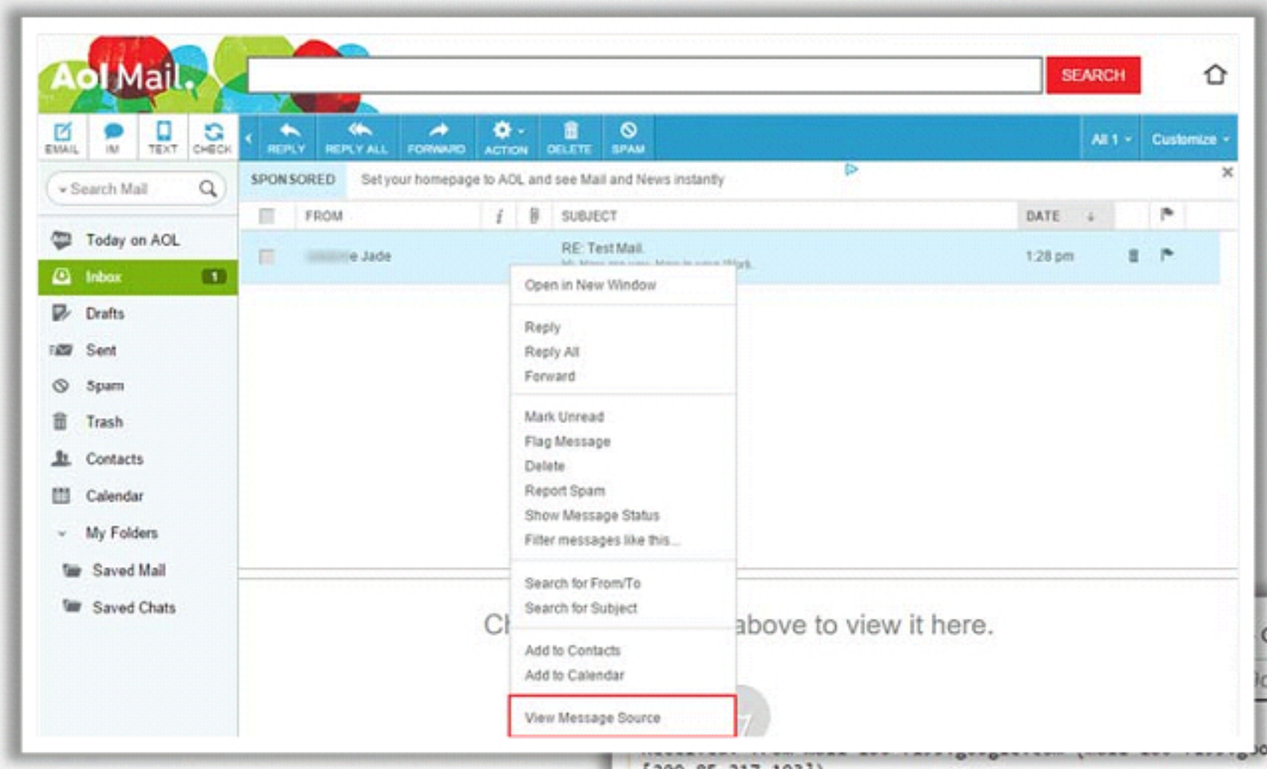
Viewing the E-mail Headers in Microsoft Outlook.com

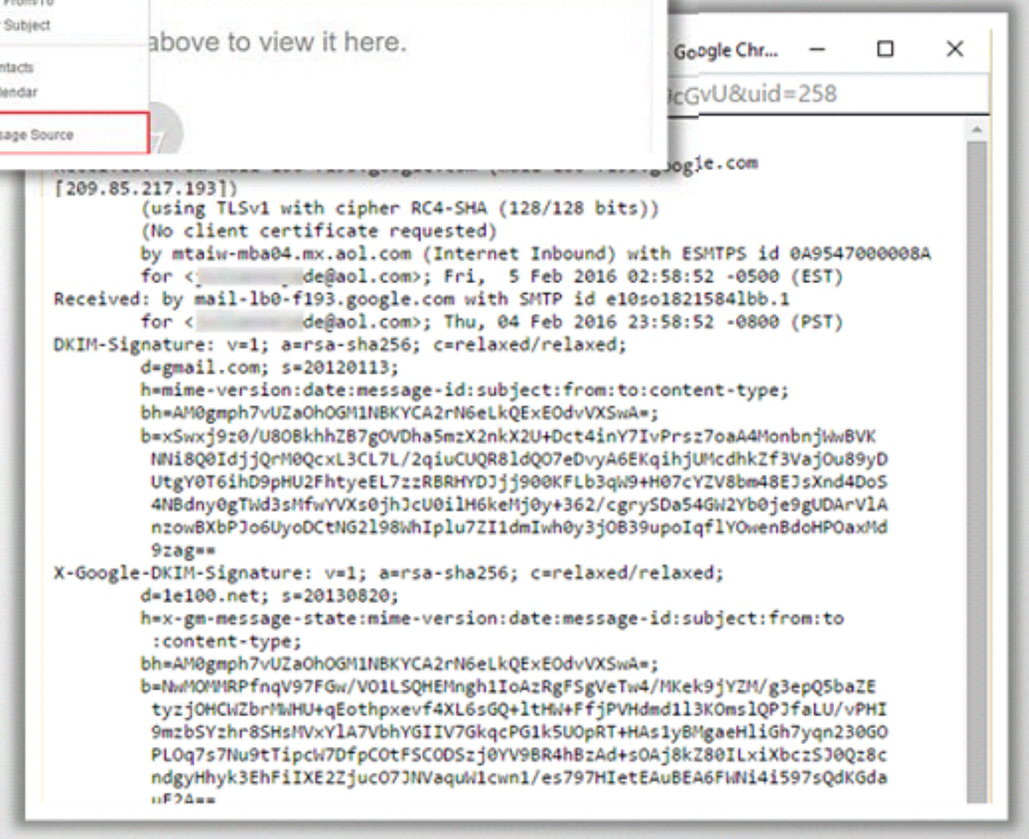
- Log on to **Microsoft Outlook.com**. Click the received mail for which you would like to see headers
- Click on **Reply all** drop-down button and navigate to the **View message source** option
- Select message headers text from the **Message source** box, copy and paste the text in any text editor and save the file



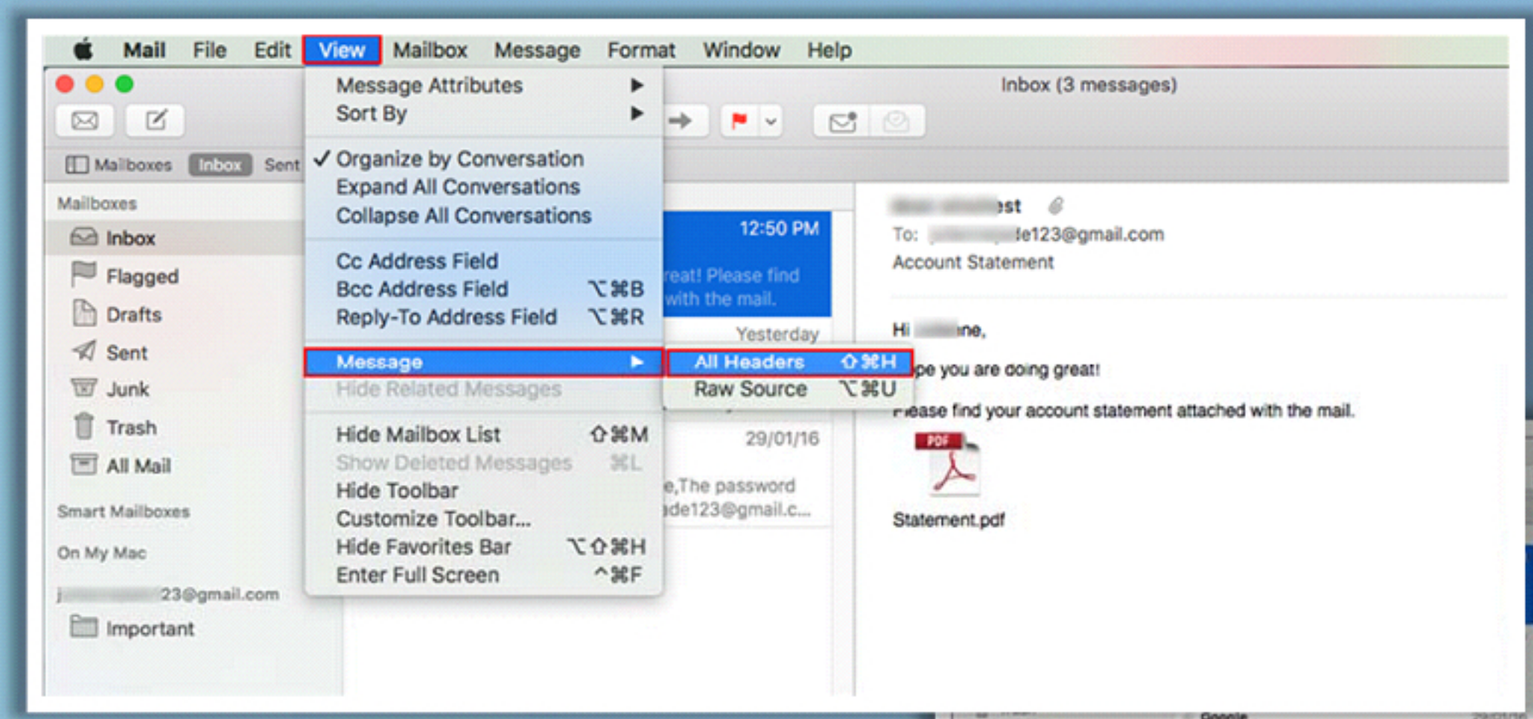
Viewing the E-mail Headers in AOL

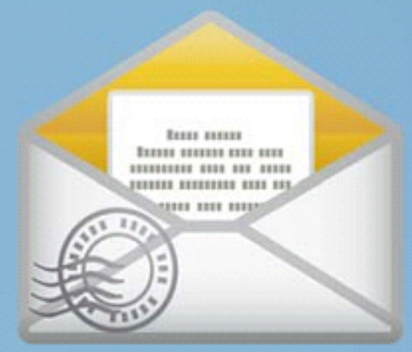
- Log on to **AOL mail**. Right-click the received mail for which you would like to see headers
- Navigate to the **View Message Source** option
- Select the message header text, copy and paste the text in any text editor and save the file

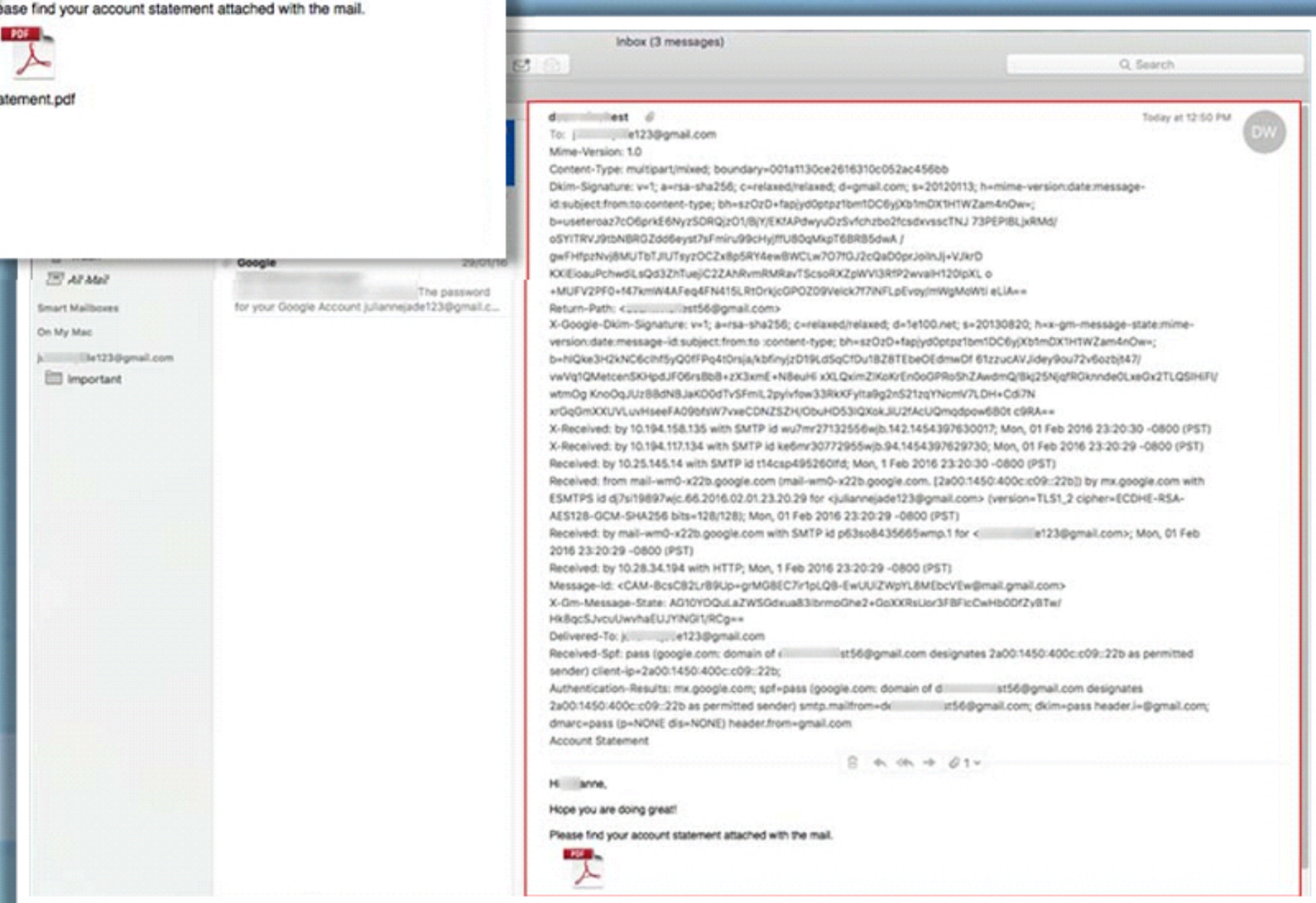




Viewing the E-mail Headers in Apple Mail



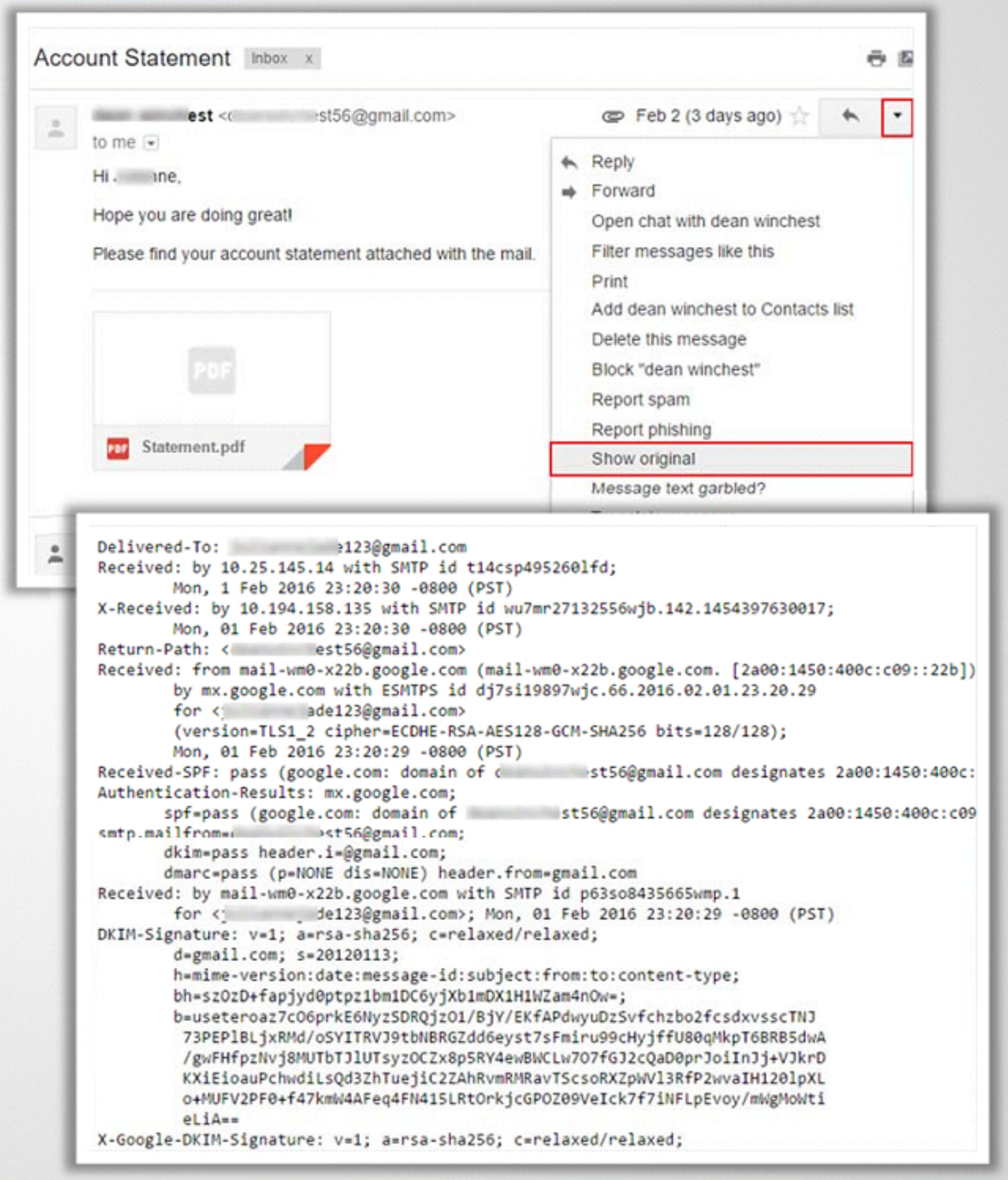




- Launch **Apple Mail** and click the received mail for which you would like to see headers
- Go to **View** → **Message** → **All Headers**
- Select message headers text, copy and paste the text in any text editor and save the file

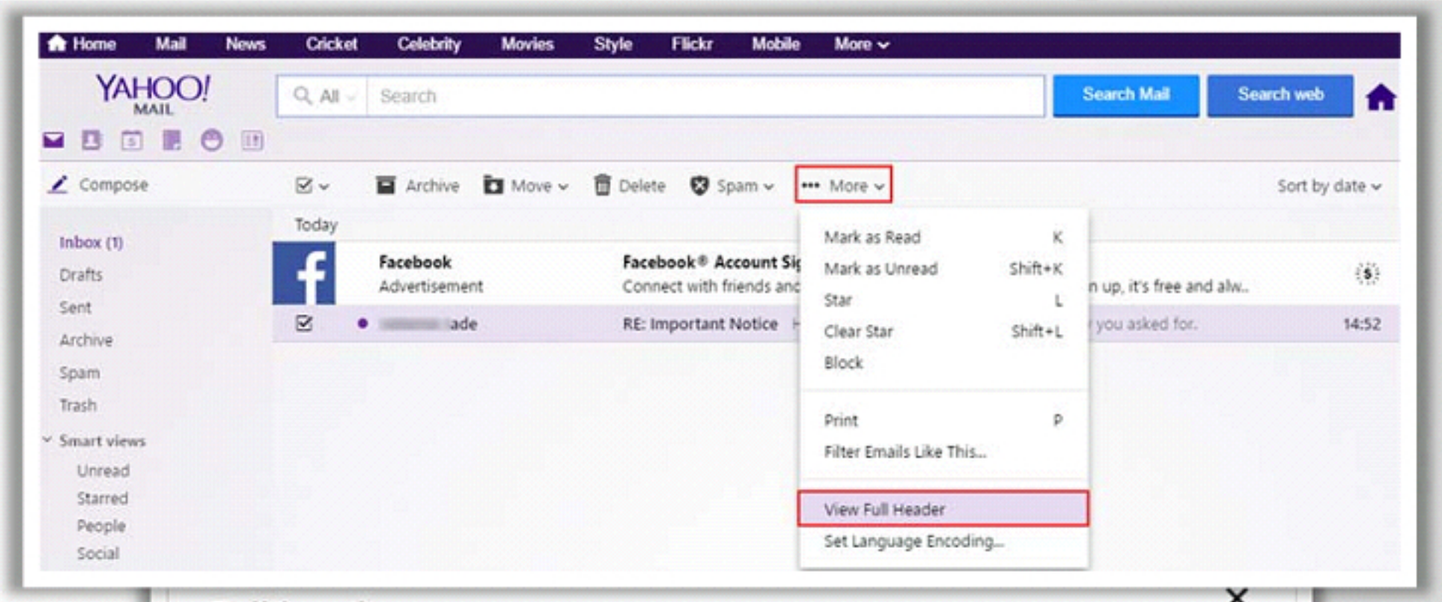
Viewing the E-mail Headers in Gmail

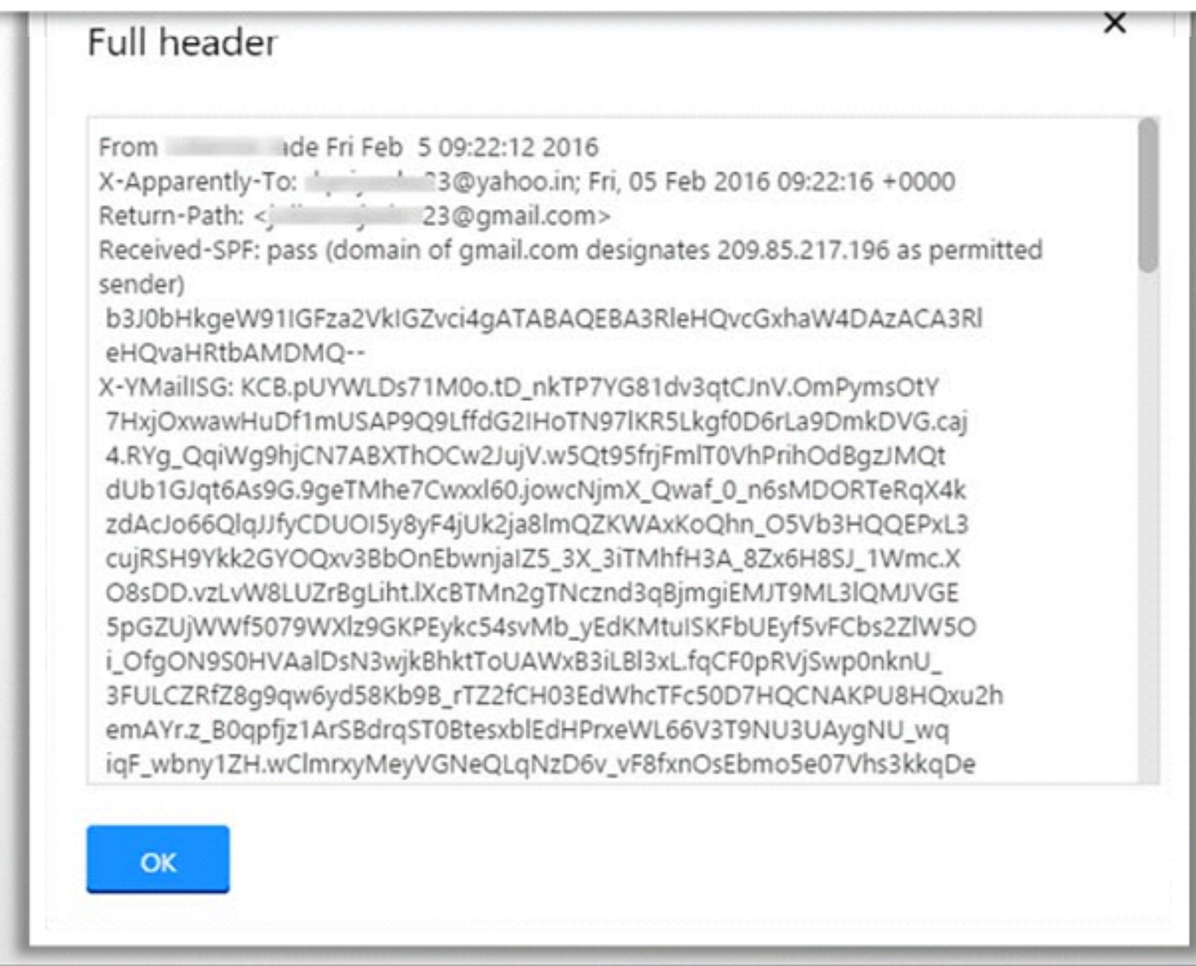
- Log on to **Gmail**. Click on the received mail for which you would like to see headers
- Click on the **Reply** drop-down button and navigate to the **Show original** option
- Select message headers text, copy and paste the text in any **text editor** and save the file



Viewing the E-mail Headers in Yahoo Mail

- Log on to **Yahoo Mail**. Select the received email for which you would like to see headers
- Click on the **...More** drop-down button and navigate to the **View Full Header** option
- Select message headers text, copy and paste the text in any text editor and save the file





Received Headers

CHFI Computer Hacking Forensic Investigator

01

"Received" headers shows a detailed log of a message's history. These headers help to draw conclusions about the origin of an e-mail, also provides information on whether the headers have been forged or not

02

If, for instance, the machine xsecurity.com, whose IP address is 104.128.23.115, sends a message to mail.target.com, but falsely says **HELO example.org**, the resultant "Received" line might start like this:

Received: from example.org ([104.128.23.115]) by mail.target.com (8.8.5)...

Analyzing E-mail Headers

Gather the supporting evidences as given below, from the email headers and track the suspect

- Return path
- IP address of sending server
- Recipient's e-mail address
- Unique message number
- Name of the e-mail server
- Date and time e-mail was sent
- Type of e-mail sending service
- Attachment files information

Analyzing E-mail Headers (Cont'd)

Consider an example: Rudy sends an Email to Timmy

From: rudy@bieberdorf.edu (Rudy)

To: timmy@immense-isp.com

Date: Tue, Jan 26 2016 14:36:14 PST

X-Mailer: Loris v2.32

Subject: Lunch today?

Received: from mail.bieberdorf.edu (mail.bieberdorf.edu [124.211.3.78]) by mailhost.immense-isp.com (8.8.5/8.7.2) with ESMTP id LAA20869 for <timmy@immense-isp.com>; Tue, Jan 26 2016 14:39:24 -0800 (PST)

```
Received: from alpha.bieberdorf.edu
(alpha.bieberdorf.edu
[124.211.3.11]) by
mail.bieberdorf.edu (8.8.5) id
004A21; Tue, Jan 26 2016 14:36:17 -
0800 (PST)
From: rudy@bieberdorf.edu (R.T.
Hood)
To: timmy@immense-isp.com
Date: Tue, Jan 26 2016 14:36:14 PST
Message-Id: <rth031897143614-
00000298@mail.bieberdorf.edu>
X-Mailer: Loris v2.32
Subject: Lunch today?
```

Examining Additional Files

- E-mail storage depends on the **state of the client and server computers**
- Some e-mail programs permit the user to store e-mails on the server and some on the client computer

Microsoft Outlook

Microsoft Outlook acts like a personal information manager, and maintains all information related to the e-mails

Online E-mail Programs

Online e-mail programs such as AOL, Gmail, and Yahoo! store the files containing e-mail messages on the computer

Personal Address Book

Another feature of e-mail programs, which can prove to be useful is the suspect's personal address book

Checking the E-mail Validity

- Email Dossier is a part of the CentralOps.net suite of online network utilities
- It is a scanning tool that the investigator can use to check the validity of an e-mail address
- It provides information about e-mail address, including the mail exchange records
- This tool initiates SMTP sessions to check address acceptance, but it never actually sends e-mail

Other tools to check e-mail validity:

Email Address Verifier - https://tools.verifyemailaddress.io

e-Mail Validator Tool - http://e-mailvalidator.com

Email Checker - http://email-checker.net

G-Lock Software Email Verifier - http://www.glocksoft.com

Email Dossier Investigate email addresses

email address [redacted]3@gmail.com go

user: anonymous [183.82.41.51]
balance: 49 units
log in | account info

CentralOps.net

Validating [redacted]3@gmail.com...

Validation results

confidence rating: **3 - SMTP**
The email address passed this level of validation without an error. However, it is not guaranteed to be a good address. more info

canonical address: <[redacted]3@gmail.com>

MX records

preference	exchange	IP address (if included)
5	gmail-smtp-in.l.google.com	[108.177.9.27]
10	alt1.gmail-smtp-in.l.google.com	[64.233.185.26]
20	alt2.gmail-smtp-in.l.google.com	[173.194.205.27]
30	alt3.gmail-smtp-in.l.google.com	[74.125.141.26]
40	alt4.gmail-smtp-in.l.google.com	[64.233.186.26]

SMTP session

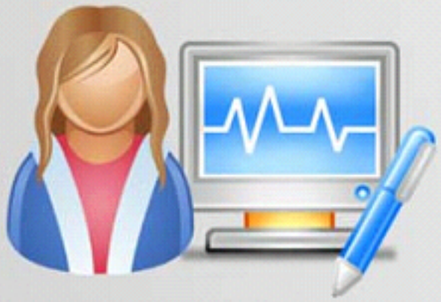
```
[Contacting gmail-smtp-in.l.google.com [108.177.9.27]...]
[Connected]
```

https://centralops.net

Examine the Originating IP Address

The following steps are involved in examining the originating IP address of an e-mail:

- Collect the IP address of the sender from the header of the received mail
- Search for the IP in the WHOIS database
- Look for the geographic address of the sender in the WHOIS database



Smart Whois lookup completed successfully.

Smart Whois: formatted

NetRange	66.220.144.0 - 66.220.159.255
CIDR	66.220.144.0/20
NetName	TFBNET3
NetHandle	NET-66-220-144-0-1
Parent	NET66 (NET-66-0-0-0-0)
NetType	Direct Assignment
OriginAS	AS32934
Organization	Facebook, Inc. (THEFA-3)
RegDate	2009-02-13
Updated	2012-02-24
Ref	http://whois.arin.net/rest/net/NET-66-220-144-0-1
OrgName	Facebook, Inc.
OrgId	THEFA-3
Address	1601 Willow Rd.
City	Menlo Park
StateProv	CA
PostalCode	94025
Country	US
RegDate	2004-08-11
Updated	2012-04-17
Ref	http://whois.arin.net/rest/org/THEFA-3
OrgAbuseHandle	OPERA82-ARIN
OrgAbuseName	Operations
OrgAbusePhone	+1-650-543-4800
OrgAbuseEmail	domain@facebook.com
OrgAbuseRef	http://whois.arin.net/rest/poc/OPERA82-ARIN
OrgTechHandle	OPERA82-ARIN
OrgTechName	Operations
OrgTechPhone	+1-650-543-4800
OrgTechEmail	domain@facebook.com
OrgTechRef	http://whois.arin.net/rest/poc/OPERA82-ARIN
RNOCHandle	OPERA82-ARIN
RNOCName	Operations
RNOCPhone	+1-650-543-4800
RNOCEmail	domain@facebook.com
RNOCRef	http://whois.arin.net/rest/poc/OPERA82-ARIN
RTechHandle	OPERA82-ARIN
RTechName	Operations
RTechPhone	+1-650-543-4800
RTechEmail	domain@facebook.com
RTechRef	http://whois.arin.net/rest/poc/OPERA82-ARIN
RAbuseHandle	OPERA82-ARIN
RAbuseName	Operations
RAbusePhone	+1-650-543-4800
RAbuseEmail	domain@facebook.com
RAbuseRef	http://whois.arin.net/rest/poc/OPERA82-ARIN

http://whois.urih.com

Trace the E-mail Origin

- Tracing the origin of an e-mail begins with looking at the message header
- All e-mail header information can be faked, except the "**Received**" portion referencing the victim's computer (the last received)
- Once it is confirmed that the header information is correct, the investigator can use the originating e-mail server as the primary source

Validating Header Information

- Once it is established that a crime has been committed, the investigator can use the **IP address** of the originating source **to track** down the owner of the e-mail address
- The following are some acceptable sites that an investigator can use to find the person owning a **domain name**:
  - www.arin.net
  - www.internic.net
  - www.freeality.com

Tracing Back Web-based E-mail

1. Web-based e-mail services (such as Gmail, Yahoo!, AOL, etc.) can often make it complicated to **trace the sender**
2. A user can read and send this type of e-mail from any computer and from **any part of the world**
3. Web-based e-mail accounts are free, and **no authentic** information is **required** for creating an **e-mail account**
4. **Criminals exploit** this advantage and create e-mail accounts **using false identities**
5. In case a Web-based e-mail account is used for sending offending messages, the investigator can contact the provider of the account to find the **IP address of the user** who connected to the Web site to send the mail
6. After performing **IP address authentication**, the investigator can get the sender's information

Acquire Email Archives

- Email archive is a **storehouse of e-mails**, kept away from the productive environment to securely preserve emails
- Reasons to archive e-mails include: **compliance**, **litigation support**, **storage** and **knowledge management**
- There are two main archive types, namely:

Local Archive

- Any archive that has an archive format **independent** of a mail server

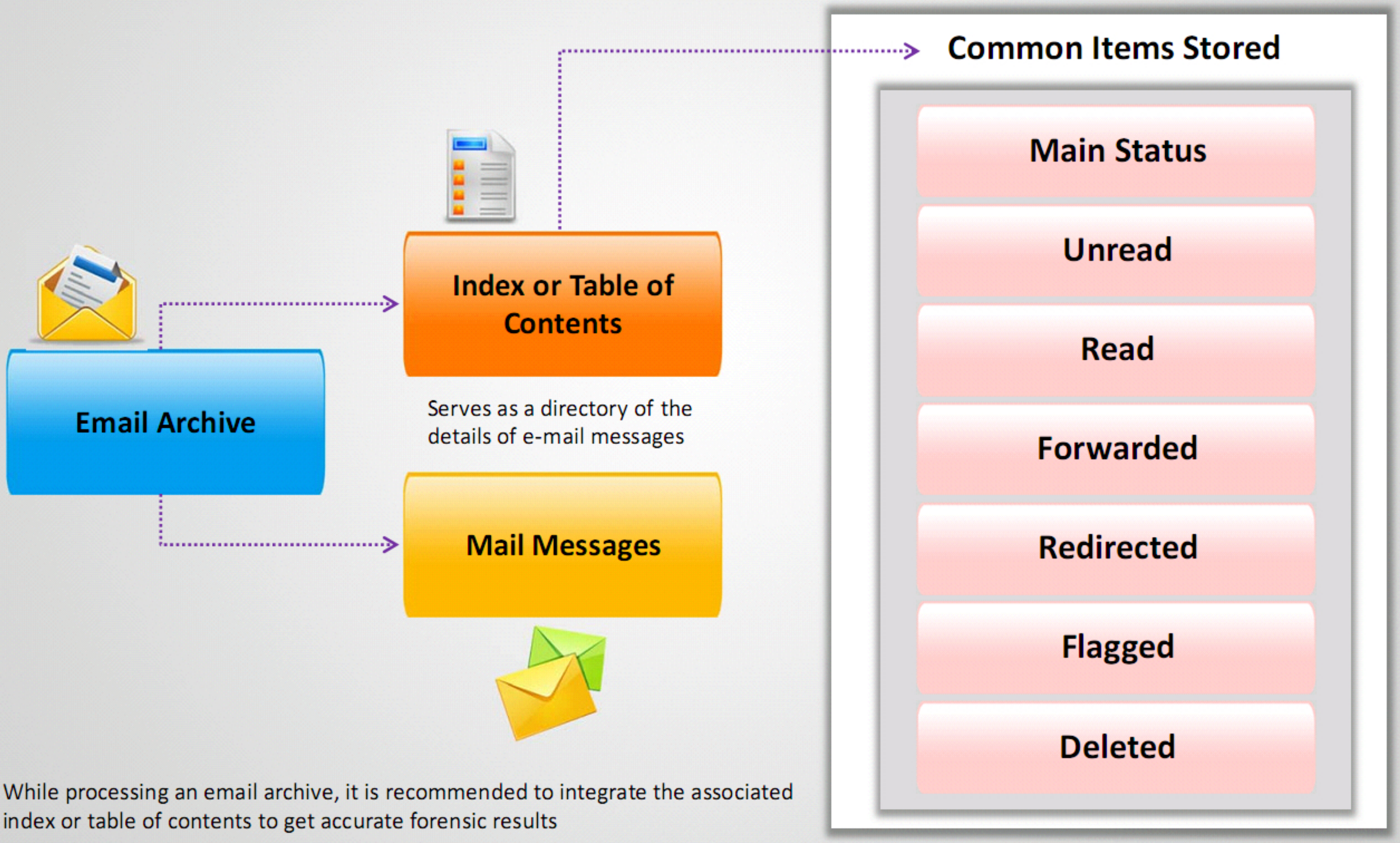
  Ex: Microsoft Outlook (Index + Messages: *.pst), FoxMail (Index + Messages: *.box), etc.

Server Storage Archive

- Any archive that has **mixed storage** for all the clients that exist on a server

  Ex: MS Exchange (.STM, .EDB), IBM Notes (.NSF, .ID), GroupWise (.DB), etc.

Content of Email Archives



While processing an email archive, it is recommended to integrate the associated index or table of contents to get accurate forensic results

Local Archive

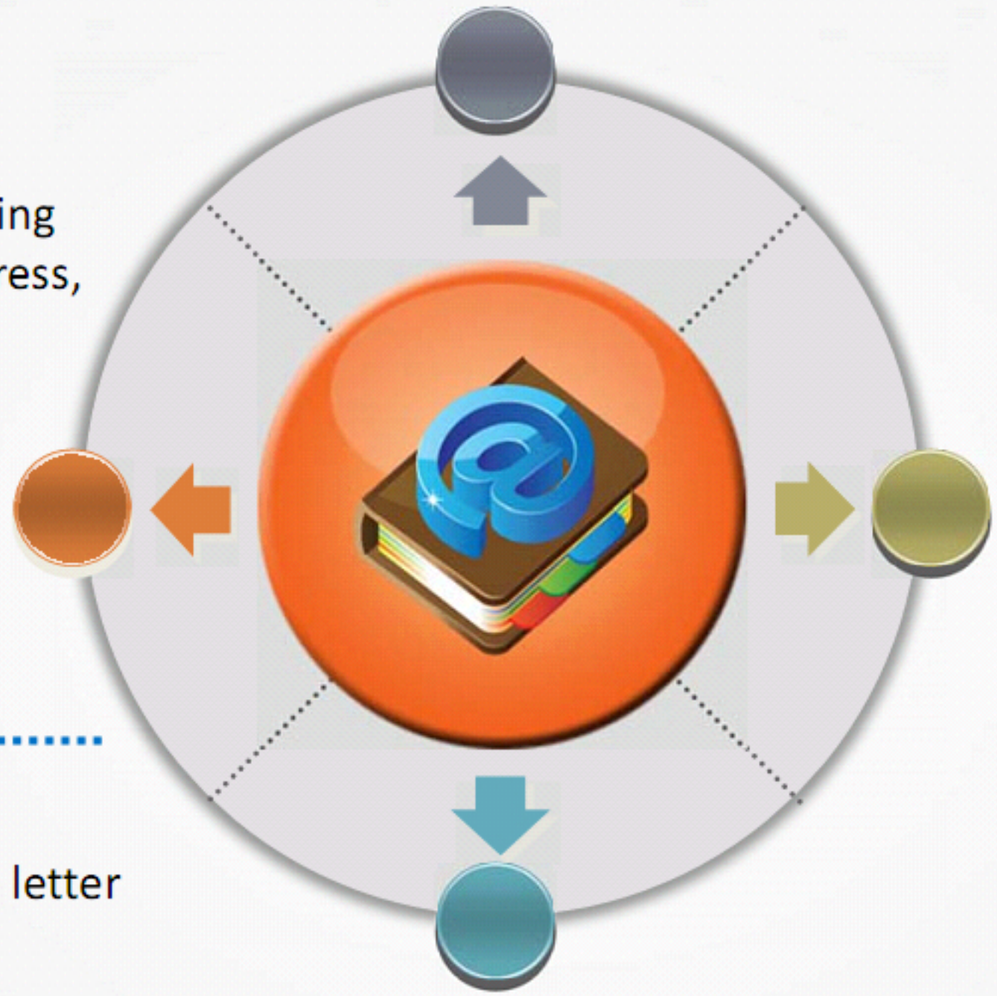
- Local level archives are under the **control of the end user**. Follow the proper guidelines while dealing with local archives

- Ensure you gather the entire archive; the **local archives** can be split into multiple files, that are used to separately **store the data**. Each of these files may contain **potential evidences** and must be handled carefully

- It is difficult to deal with the **webmail** as there is no **offline archive** in most cases. So consult your counsel on the case, to find out the best way to approach and gain access to the required data on servers

Local Archive (Cont'd)

Process all items with complete structure of: header, body, encoding, attachment to compute verification through hash value



1. Header

- It is envelope of **e-mail** that **contains information** regarding the sender and receiver address, subject, time of creation, delivery stamps, message author, CC, and BCC
- All the above mentioned data may not be found for all **e-mail messages**

2. Body

- It is the **primary content** or letter of the message

3. Encoding

It acts as a **universal translator** for the e-mails and allows different email programs to pass data to one another

Types of encoding in emails:

MIME (Multipurpose Internet Mail Extensions)

It is a protocol that allows **non-ASCII files** (video, graphics, and audio) to be built in the email message

UUCODE

UNIX format for attachment encoding

BINHEX

Mac format for attachment encoding

4. Attachment

It is an extra item that comes as a supplement to the body

Server Storage Archive

Server storage archives include: Microsoft Exchange, IBM Notes, and Novell GroupWise

IBM Notes

Follow the guidelines when dealing with IBM Notes

- Gather the `*.NSF file`
- Gather the `associated *.ID` file for the archive. It functions as the encryption key that allows you to **open encrypted mails**

Novell GroupWise

Follow the guidelines when dealing with Novel GroupWise

- Ensure to **acquire** the entire directory, while keeping the **structure intact**
- `Ngwguard.db` is stored in the root of the email directory and is the key file of the GroupWise structure. It tells the GroupWise about each user account and its location
- Other key files include `wphost.db` and `gwcheck.db`, but the entire directory must be intact to do an examination

Server Storage Archive (Cont'd)

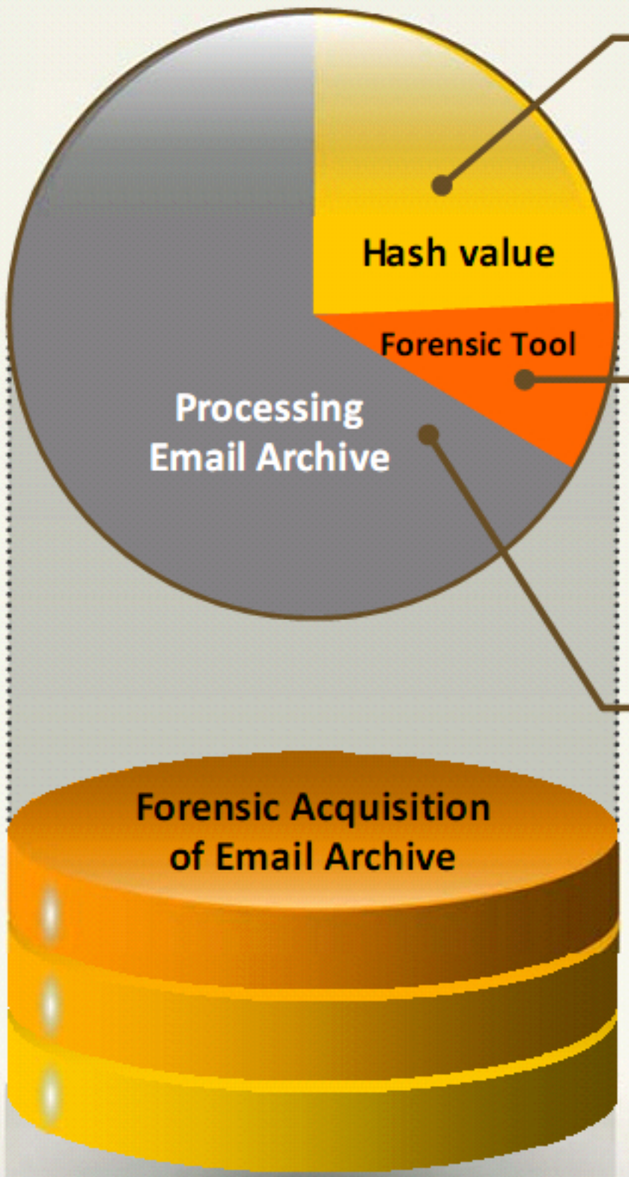
MS Exchange

Follow the guidelines when dealing with MS Exchange

- Do not deal with an **active Exchange server**, instead take a backup of the server. This maintains the best date structure for the data
- Gather all the **data files** associated with the server such as PRIV.EDB, PUB.EDB, and PRIV.STM files to create the complete archive

PRIV.EDB	PUB.EDB	PRIV.STM
It is a **rich text database file** containing message headers, message text, and standard attachments	It is a database file to store public folder **hierarchies and contents**	It is a streaming Internet content file containing video, audio, and other media that are formatted as streams of **Multipurpose Internet Mail Extensions**

Forensic Acquisition of E-mail Archive



Evaluate the tools prior to processing the e-mail archives

- **Determine how the tool computes the hash value:**

  The **hashing mechanism** should interpret all the email message components (header, body, and attachment) in the **computation of the hash value**

- **Check if the tool is designed for forensics:**

  Processing e-mail for forensics is a different process; therefore, check the tool's ability to **recover deleted data from the archive**

Note: Data that has been deleted from the archive's recycling bin or deleted items folder resides in the unallocated space of the email archive

Forensic Acquisition of E-mail Archive (Cont'd)

CHFI Computer Hacking Forensic Investigator

Processing Local E-mail Archives:

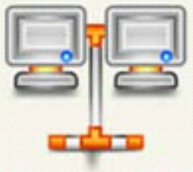
- **Outlook PST** files are the most common e-mail archives and can be found on the desktop system
- **Outlook PST File Acquisition:**
  - Acquire a bit-stream image of the entire drive and then extract the PST file from the **drive image using multiple tools**
  - Once the file is extracted, choose tools such as **Paraben's Email Examiner** to process the proprietary email archive into usable messages

Forensic Acquisition of Email Archive (Cont'd)

Processing Server Level Archives:

When processing a **server level archive**, there are many files to look into. Gather different data, based on the email server used

Acquisition stage for a server archive is different to the **local archive acquisition**. Here you need to acquire the appropriate files from where the archive is stored



Not many tools are available for acquisition of **network level archives**. However, there are other tool options available that are designed to restore archives for review

Ontrack PowerControls assist administrators to copy, search, recover, and analyze e-mails and other mailbox items directly from Microsoft Exchange Server backups, un-mounted databases (EDB) and information store files

Paraben's Network Email examiner can also process MS Exchange archives as well as GroupWise and IBM Notes

Recovery of Deleted E-mails

- Recovery of deleted e-mail messages **depends upon the e-mail client** used in the process of sending the mail

Thunderbird

- Messages deleted from the mailbox are **tagged for deletion** and are no longer visible in the mailbox
- However, these deleted messages reside in the **trash folder**, until the trash folder is cleared

Outlook PST

- Data is taken from the **active part of the archive** to a recycle bin
- If the recycle bin is emptied, it will go to the **unallocated space** of the email archive where it resides for a specific period
- Recovery of this data varies depending on the **size of the archive**

Examining Email Logs

- In e-mail related forensic investigations, it is significant to validate and verify the **e-mail addresses**, **sources**, and **paths** related to the suspected e-mails
- It is important to examine logs to figure out if the **e-mail header** has been tampered after the suspected incident

Examining System Logs

- By examining system logs, an investigator can verify the path that email has taken

Examining Network Equipment Logs

- By examining the router and firewall logs, it is possible for an Investigator to verify the times and the IP addresses contained within the e-mail
- These logs provide e-mail message ID information, source address and destination address of the servers used to send the e-mail

Examining Linux E-mail Server Logs

1. **Sendmail** is the command used to send emails via Linux or Unix system. It required the information regarding the source and destination addresses, the sender and recipient addresses, and the e-mail message ID
2. **Linux** and **Unix** uses **Syslog** to maintain logs of what has happened on the system
3. The configuration file, **/etc/syslog.conf** determines the location of syslog service logs
4. Syslog configuration file contains information on the logging priority, where logs are sent, and what other actions may be taken
5. The syslog.conf provides the location of the log file for e-mail, which is usually **/var/log/mailog**
6. **/var/log/mailog** file contains source and destination IP addresses, date and time stamps, and other information necessary to validate the data within an e-mail header

Examining Microsoft Exchange E-mail Server Logs

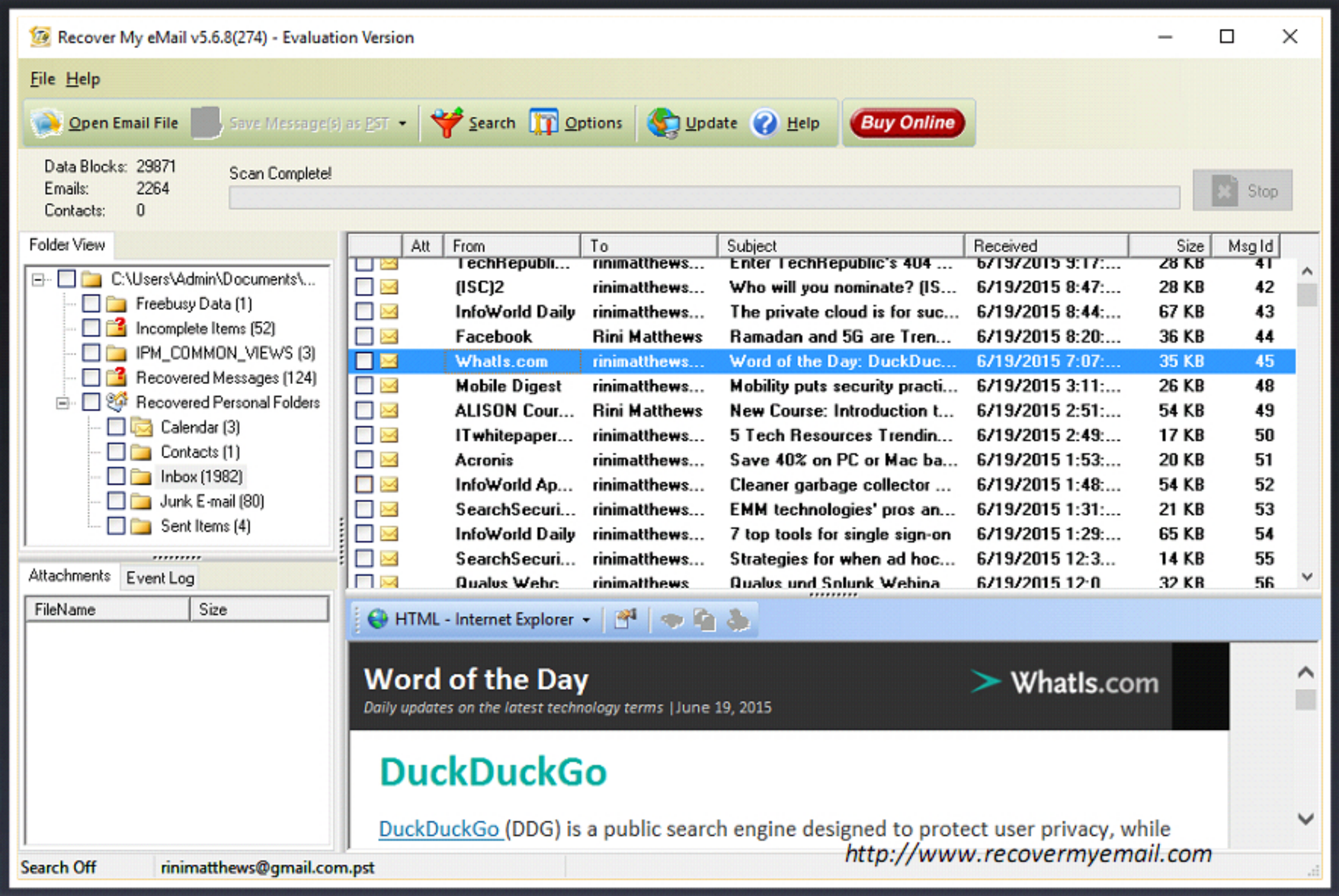
- Microsoft Exchange uses the Microsoft **Extensible Storage Engine** (ESE)
- It uses **Messaging Application Programming Interface** (MAPI), which allows collaboration of various e-mail applications
- While investigating an e-mail sent via Microsoft Exchange server, an investigator should primarily focus on the following files:
  - **.edb database files** (responsible for MAPI information)
  - **.stm database files** (responsible for non-MAPI information)
  - **checkpoint files**
  - **temporary files**
- Checkpoint files helps to find out if any data loss occurred **after last backup**, thus allowing the investigator to recover lost or deleted messages
- Temporary files store the information received by the server when it was too busy to process it immediately. System retains these files that may be recovered for investigation purposes
- Transaction log preserves and processes modifications done in the database file, so that it can be used to determine if the email has been sent or received by the server
- Windows Event Viewer can be used to read:
  - Tracking log (allows to view message content associated with the e-mail)
  - Troubleshooting or diagnostic logs (records a number of events for each e-mail sent or received). In addition, Event Properties dialog box provides more information in forensic investigations

Examining Novell GroupWise E-mail Server Logs

- **GroupWise** is an **e-mail service platform by the Novell NetWare**. It stores the user's messages in almost 25 proprietary databases
- Every database is stored in the **OFUSER Directory** object and is referenced by a username, followed by a unique ID and the .db extension
- The **NGWDFR.DB database**, present in the OFMSG directory object is used for delayed or deferred e-mails
- Two ways of organizing mailboxes:
  - **Permanent index files (.idx extension)** - updated and renamed daily in order to maintain the order of e-mails in the mailboxes
  - **GroupWise QuickFinder** - uses incremental indexing files for daily maintenance of e-mail server changes. These changes are then written in the .idx file at a particular point of time
- **Guardian (Ngwguard.db)**, is a specialized database that:
  - Maintains **centralized control** of the e-mail services and associated files
  - **Tracks changes** in the GroupWise environment and clears any processes before they make any unwanted changes in the GroupWise database
  - Includes built-in safeguards like **Ngwguard.fbk**, **Ngwguard.rfl**, and **Ngwguard.db** which helps in preventing data loss. They also maintain backup copies and log files from the Guardian database has a single point of dereliction (In cases where the e-mail server data is erased or corrupted, need to recovered from a previous version or from a backup and begin the investigation again)
- GroupWise generates log files (.log extension) maintained in GroupWise folders, which can be used by the investigator to match an e-mail header with a suspect's IP address

Email Forensics Tools: Recover My Email

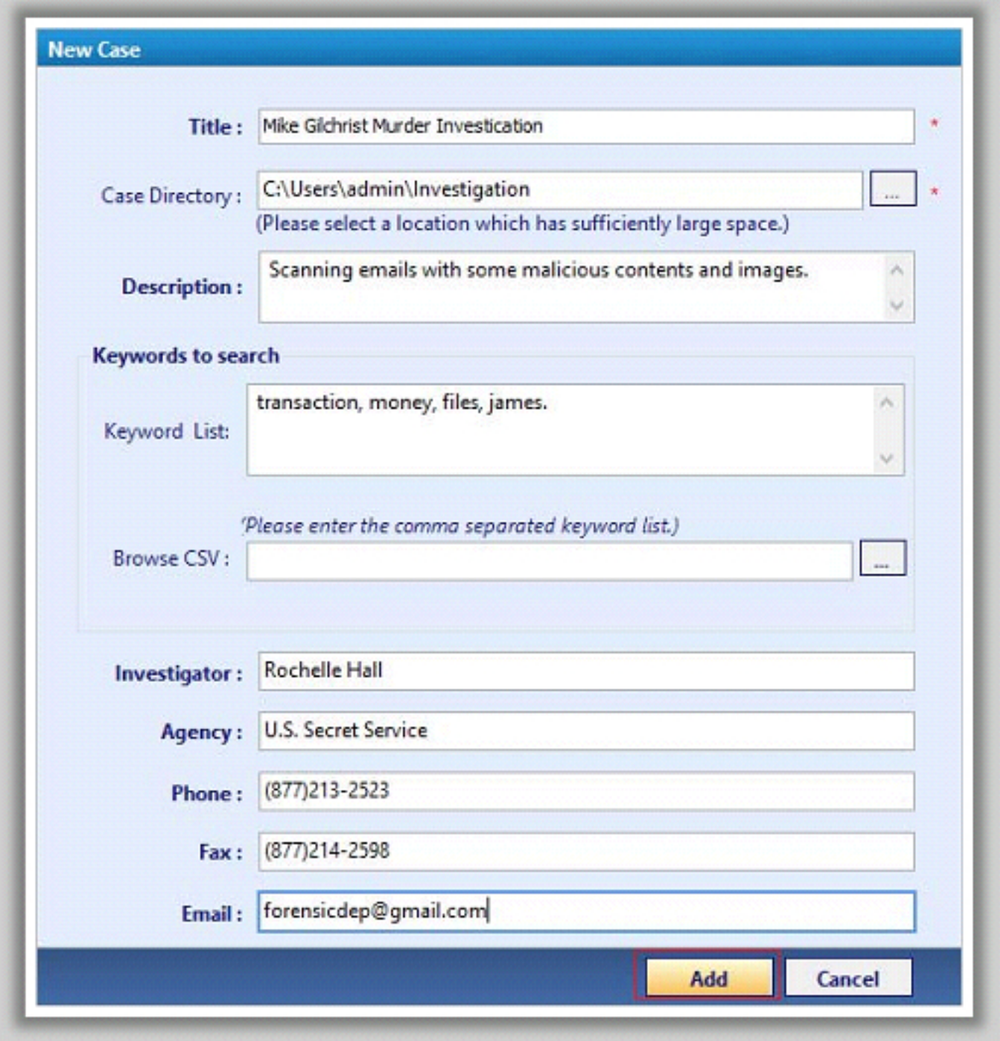
Recover My Email is mail recovery software that can recover deleted email messages from either **Microsoft Outlook PST files** or **Microsoft Outlook Express DBX files**

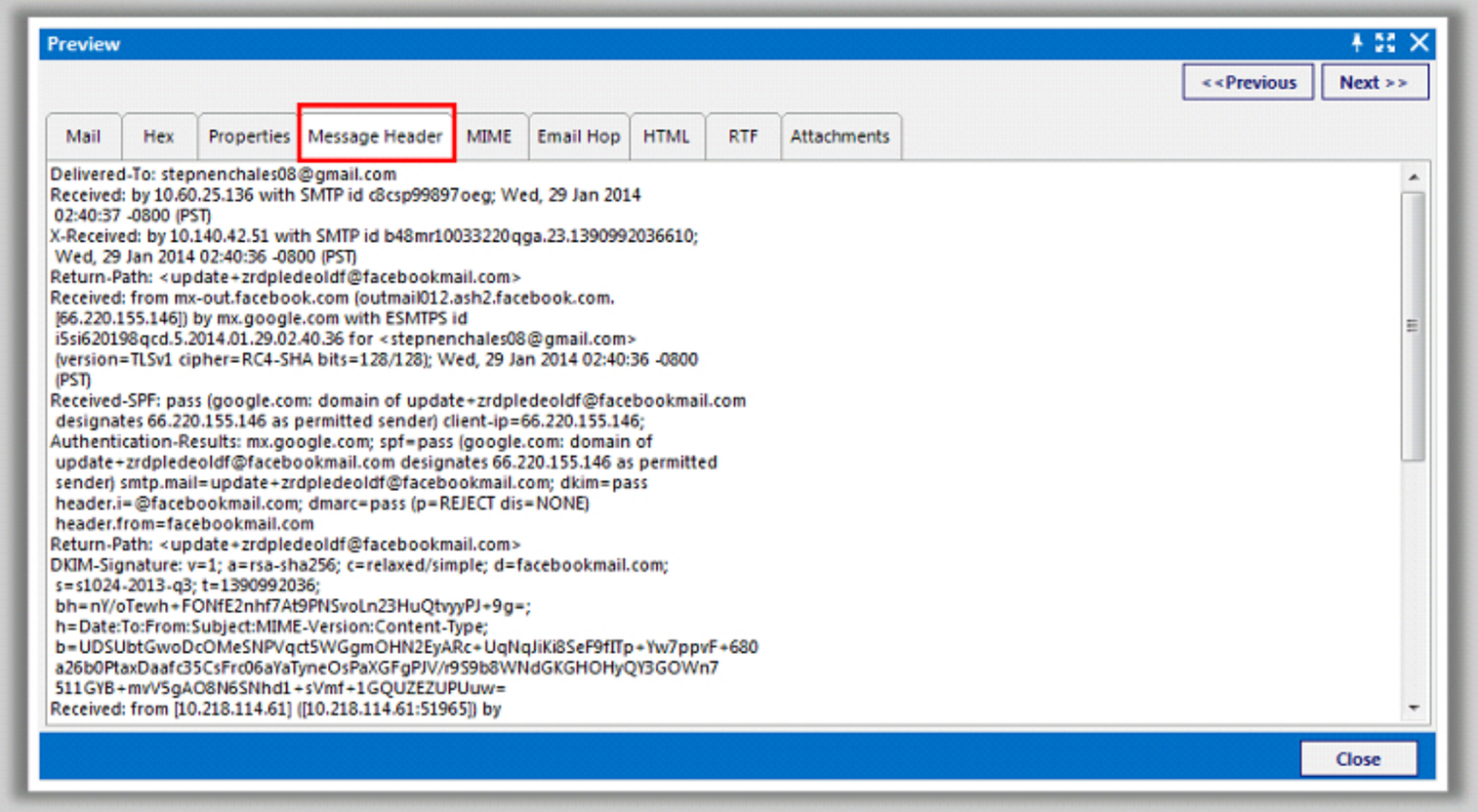


http://www.recovermyemail.com

Email Forensics Tools: MailXaminer

MailXaminer is an **e-mail searching**, **reporting**, and **exporting tool** that enables the law enforcement agencies to execute investigations and detailed analyses of the suspected e-mails





https://www.mailxaminer.com

Email Forensics Tools

Stellar Phoenix Deleted Email Recovery
http://www.stellarinfo.com

Forensic Toolkit (FTK)
http://accessdata.com

Paraben's Email Examiner
https://www.paraben.com

Kernel for PST Recovery
http://www.pstrecoverytools.com

MxToolBox Email Header Analyzer
http://mxtoolbox.com

Wise Data Recovery
http://www.wisecleaner.com

EaseUS Email Recovery Wizard
http://www.easeus.com

DiskInternals Mail Recovery
http://www.diskinternals.com

Aid4Mail Email Forensic software
http://www.aid4mail.com

Paraben's Network E-mail Examiner
https://www.paraben.com

Email Forensics Tools (Cont'd)

Nuix Investigator Lab
http://www.nuix.com

emailTrackerPro
http://www.emailtrackerpro.com

EnCase Forensic
https://www.guidancesoftware.com

OSForensics
http://www.osforensics.com

Exchange Deleted Email Recovery
http://www.emaildoctor.org

Kernel Email Recovery Software
http://www.nucleustechnologies.com

Intella TEAM
https://www.vound-software.com

EMail Detective - Forensic Software Tool
http://www.hotpepperinc.com

Lotus Notes Forensics Tool
http://www.mailproplus.com

Stellar Phoenix Mailbox Exchange Recovery
http://www.stellarinfo.com

Email Forensics Tools (Cont'd)

PST Outlook Repair
http://www.pstoutlookrepair.com

Forensic Email Recovery Tools Kit
http://www.forensicsoftware.org

Repair PST - Outlook PST Recovery
http://www.emailrecovery.in

Kroll Ontrack Email Recovery
http://www.krollontrack.com

Unistal Email Recovery Software
http://www.unistal.com

InFixi® Email Recovery Tools
http://www.infixi.com

DataNumen Outlook Repair
https://www.datanumen.com

Stellar Phoenix Outlook PST Repair Software
http://www.stellarinfo.com

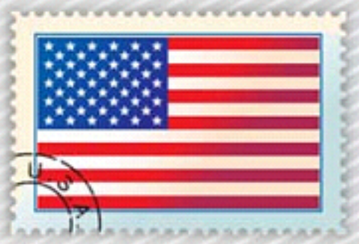
Recovery Toolbox for Outlook
https://outlook.recoverytoolbox.com

MS Outlook PST Recovery Tool
http://quickdata.org

U.S. Laws Against Email Crime: CAN-SPAM Act

The CAN-SPAM Act (**Controlling the Assault of Non-Solicited Pornography and Marketing Act**) is a law that sets the rules for sending e-mails for commercial purposes, establishes the minimum requirements for commercial messaging, gives the recipients of e-mails the right to ask the senders to stop e-mailing them, and spells out the penalties in case the above said rules are violated

CAN-SPAM's main requirements meant for senders:



- Do not use false or misleading header information
- Do not use deceptive subject lines
- The commercial e-mail must be identified as an ad
- The email must have your valid physical postal address
- The email must contain the necessary information regarding how to stop receiving e-mails from the sender in future
- Honor recipients' opt-out request within 10 business days
- Both the company whose product is promoted in the message and the e-mailer hired on contract to send messages must comply with the law

https://www.ftc.gov

U.S. Laws Against Email Crime: CAN-SPAM Act (Cont'd)

Penalties:

- All e-mails that are in violation of law are subject to financial penalties of up to $16,000, and depending on the case one or more persons may be held responsible for the violations

  For example, in case of violation of law by e-mails sent for the promotion of commercial products and services, both the company whose product is being promoted in the message and the company that originally sent the message may be held legally responsible

As per the CAN-SPAM Act, there are certain specified violations that may involve additional fines. Criminal penalties and imprisonment may be sentenced for:

- Accessing someone else's computer to send spam mails without permission
- Using false information to register for multiple email accounts or domain names
- Relaying or retransmitting multiple spam messages through a computer to mislead others, about the origin of the message
- Harvesting email addresses or generating them through a dictionary attack (the practice of sending e-mails to addresses made up of random letters and numbers in the hope of reaching valid ones)
- Taking advantage of open relays or open proxies without permission

Module Summary

- An e-mail system consists of e-mail servers and e-mail clients
- An e-mail client, also known as a mail user agent (MUA), is a computer program for accessing and managing emails
- An e-mail server connects to and serves several e-mail clients
- Headers contain significant information regarding the mail, such as sent time, unique identifying numbers, IP address of the sending server, etc.
- "Received" headers maintain a record of the detailed log history of message history, and they help to find out the origin of an e-mail, even when other headers have been forged
- Online e-mail programs such as AOL, Gmail, and Yahoo! leave the files containing e-mail messages on the computer in different folders such as History, Cookies, Temp, Cache, and Temporary Internet folder