Investigating Email Crimes

Module 12

Investigating Email Crimes

Module 12

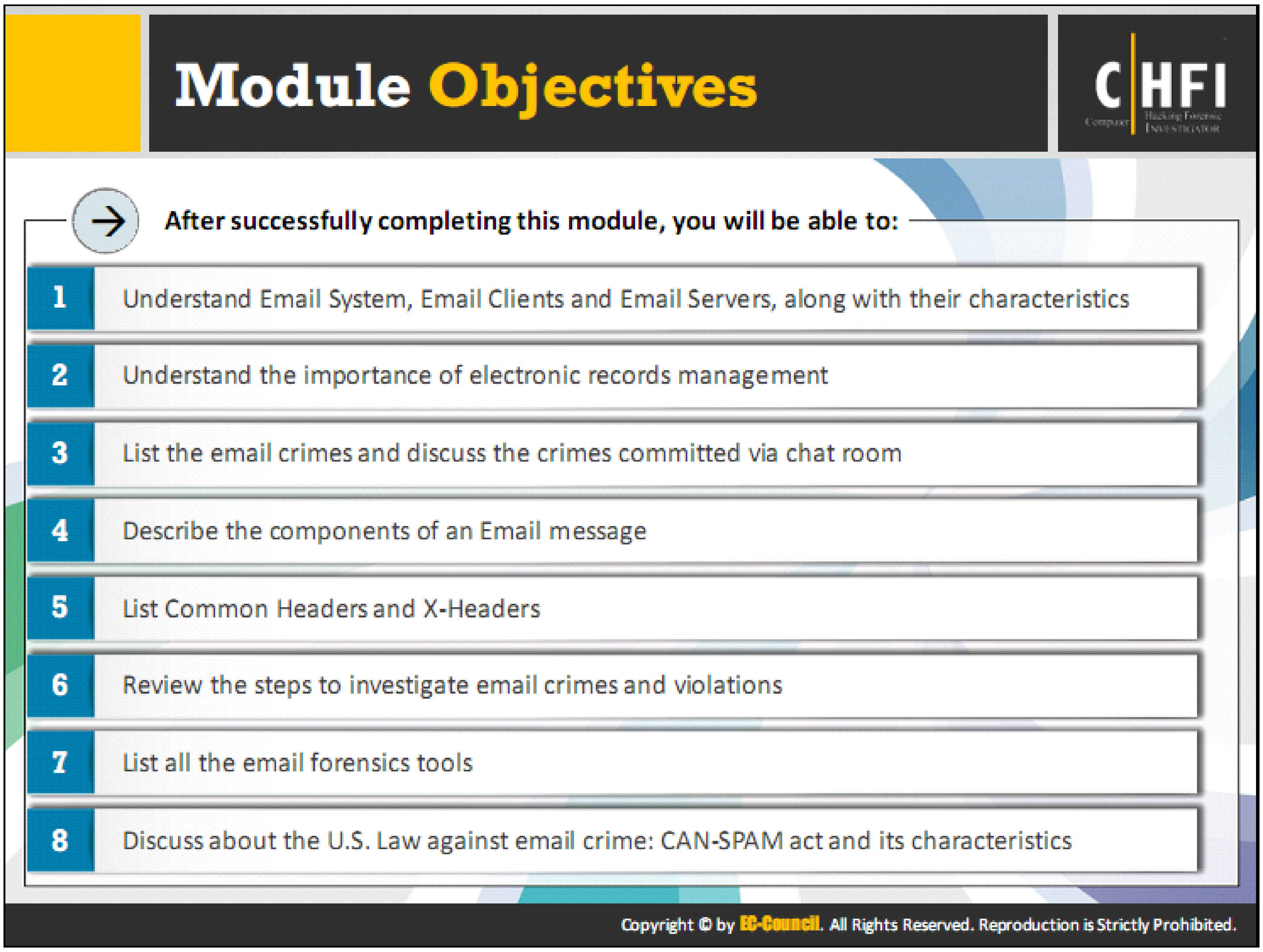
Designed by Cyber Crime Investigators. Presented by Professionals.

CHFI
Computer Hacking Forensic Investigator
1010101

Computer Hacking Forensic Investigator v9

Module 12: Investigating Email Crimes

Exam 312-49



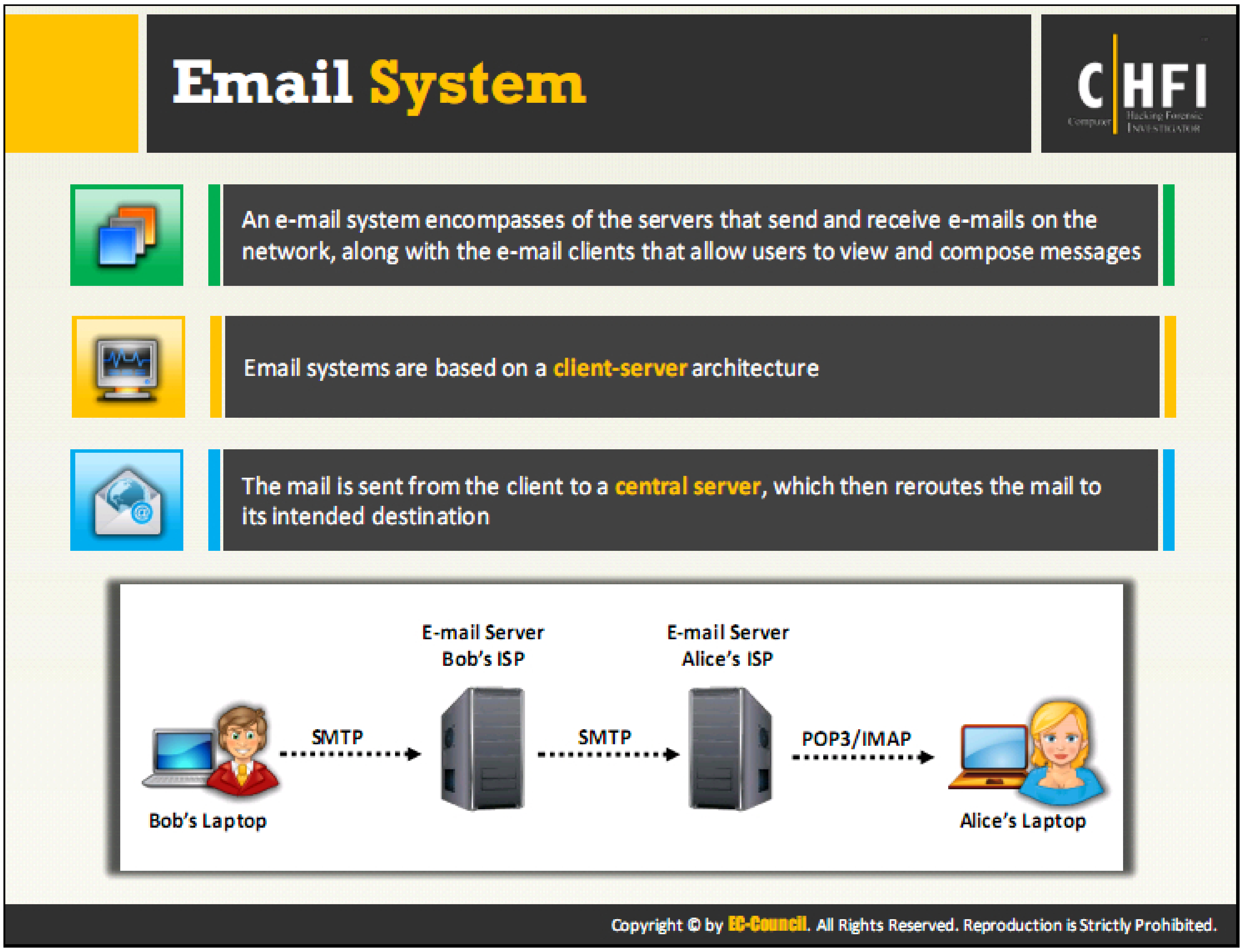
Module Objectives

CHFI

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

Electronic communication offers global connectivity, but cyber criminals can exploit this unique feature. This module intends to make you familiar with a subject that is currently a prime concern: email crime. This module focuses on how to investigate email crime.



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

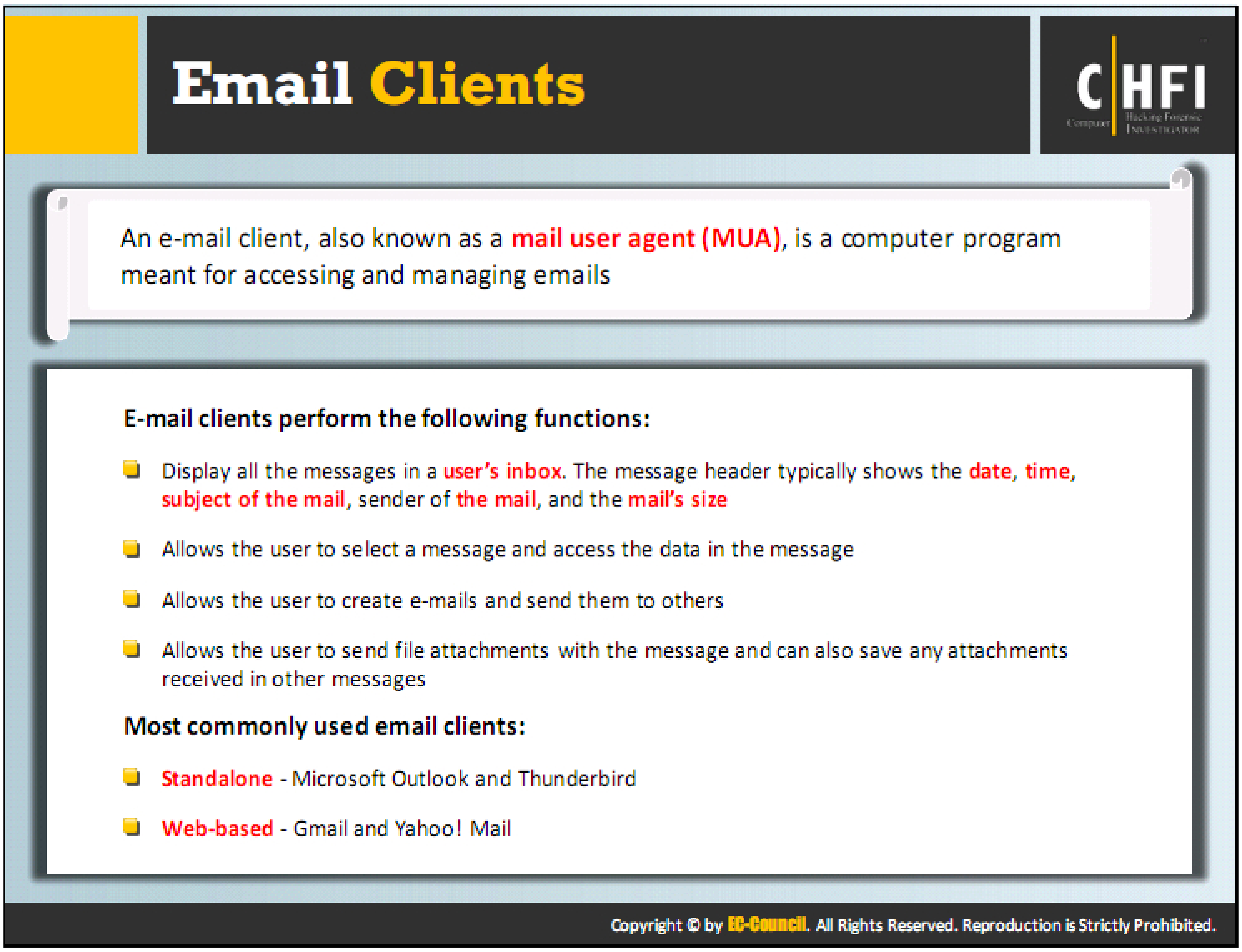
Email systems are based on a client-server architecture

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

Email is an abbreviation of "electronic mail," which is used for sending, receiving, and saving messages over an electronic communication system. An email system works on the basic Client Server architecture. When we send a message from e-mail client, it goes through an e-mail server, which handles the received messages. This e-mail server forwards the message to a POP or IMAP service if the server has to send the message to a recipient on the same subnet, or else it implements the standard process to send the message over the Internet to the recipient.

An email system consists of the mail clients to send or fetch emails and two different SMTP and POP3 or IMAP servers running on a server. An email system works as follows:

1. For example, Jane composes a message using her mail user agent (MUA), writes the email address of the person she wants to correspond with, Peter, and hits the Send button.
2. Jane's MUA formats the message in Internet email format and uses SMTP to send the message to the local mail transfer agent (MTA).
3. The MTA looks at the destination address provided in the SMTP protocol.
4. To find out whether the email exchange server accepts the messages for Peter's domain, the MTA looks at the domain name in the Domain Name System (DNS).
5. The DNS server responds with a mail exchange record of Peter's domain.
6. Jane's SMTP sends the message to the mail exchange of Peter's domain.
7. Peter checks his mail with the Get Mail button in his MUA using the POP3 server.



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:

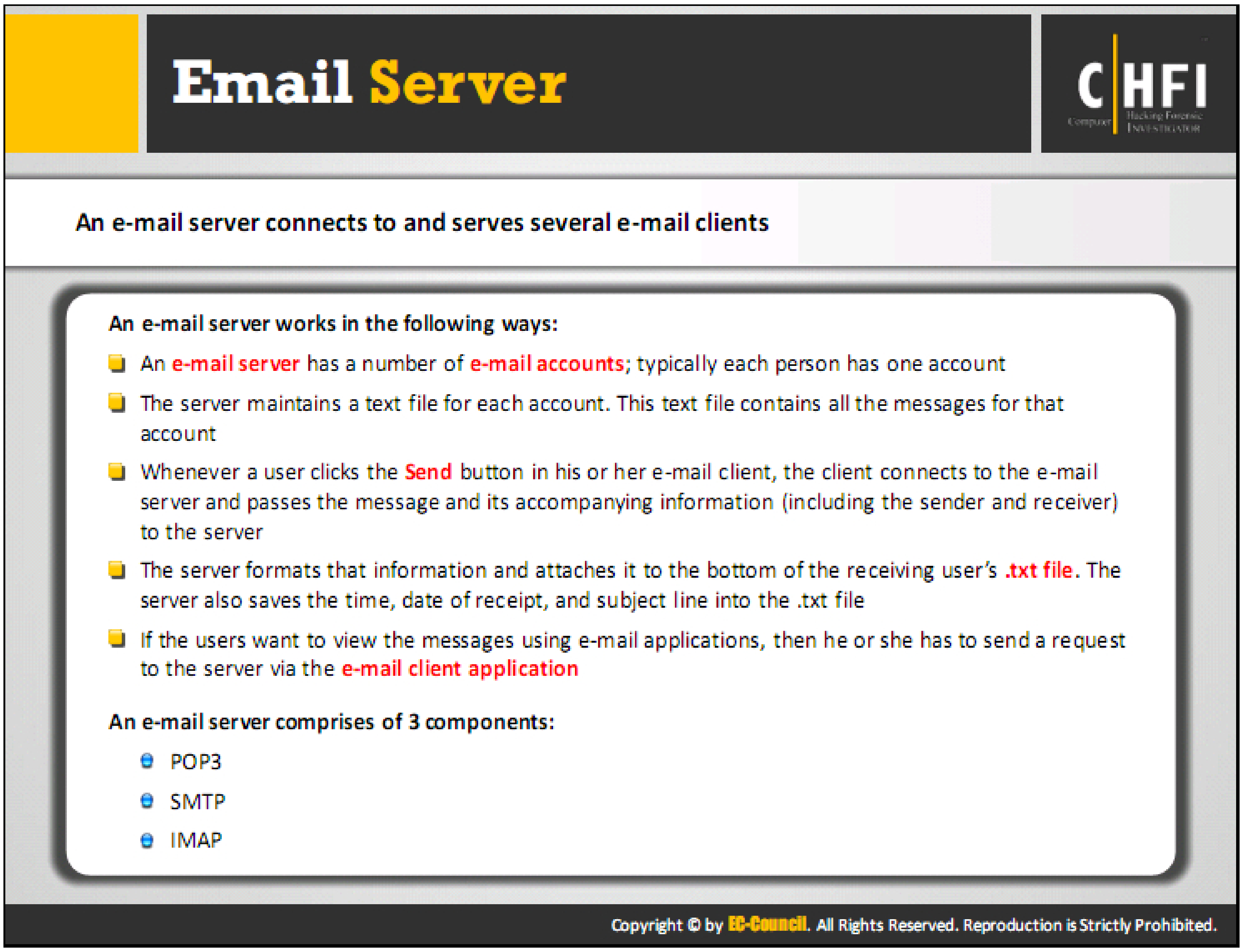
- Display all the messages in a **user's inbox**. The message header typically shows the **date**, **time**, **subject of the mail**, sender of **the mail**, and the **mail's size**
- Allows the user to select a message and access the data in the message
- Allows the user to create e-mails and send them 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

An email client, also known as mail user agent (MUA), is a desktop application for reading, sending, and organizing emails. It provides an interface for users to receive, compose, or send emails from their configured email address. A user needs to set up and configure his/her email address before using the email client. The configuration includes issuing email ID, password, POP3/IMAP and SMTP address, port number, and other related preferences. There are a number of standalone and web-based email clients such aseM Client, Claws Mail, Thunderbird, Mailbird, Zimbra Desktop, Gmail, Outlook.com, etc. The email client becomes active only when a user runs it.

An ESP (Email Service Providers) hosts and manages a mailbox that stores the users' emails. So, when a user runs the client, the ESP's Mail Transfer Agent (MTA) sends the emails stored in the users' mailbox to the users' inbox. Until then, the ESP stores all the emails in the user's mailbox. Similarly, while sending mails, the email client sends the mails to the server using a Mail Submission Agent (MSA), and from there, the mail reaches the destination email Id.



Email Server

CHFI
Computer Hacking Forensic Investigator

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:

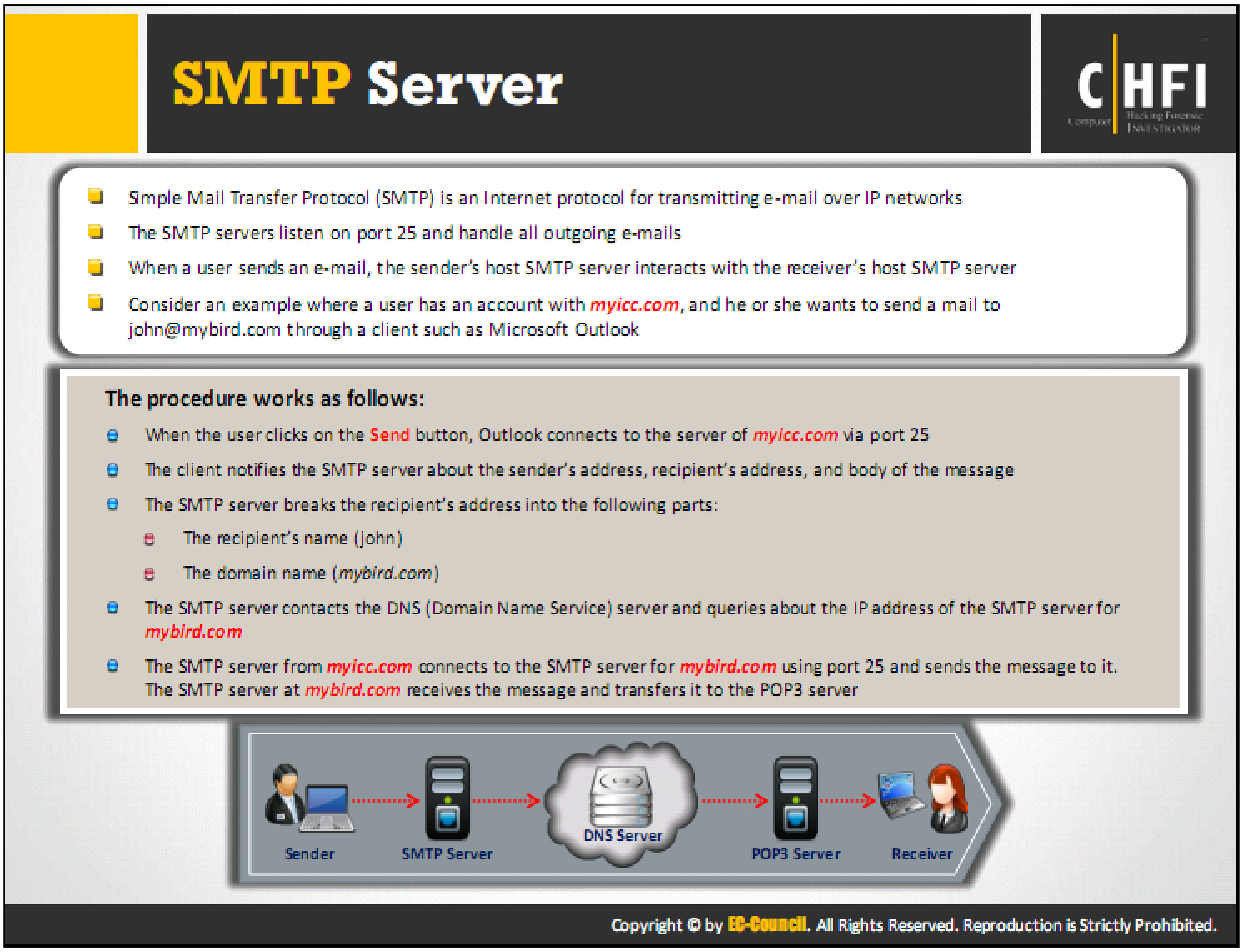
- POP3
- SMTP
- IMAP

Email or mail server is a computer within the network that works as a virtual post office. An email server connects and serves several email clients. Email servers exchange email with the SMTP server. When a user sends an email, the client application first directs it to the email server. This contacts the addressee's email server and carries out a conversation in accordance with the rules defined by SMTP over the Internet. The email server checks for the validity of the username with the other email server. If validated, it transfers the email and the receiving email server stores it until the addressee logs on and downloads it.

An email server works as follows:

- The server has a number of email accounts; each person has one account.
- It contains the text file for each account i.e., if an account name is MTony, then the text file is MTONY.TXT and if an account name is JMary, it becomes JMARY.TXT.
- Now consider that Tony is sending messages to Mary. For example, Tony writes, "Mary, how are you? Tony" using an email client.
- When Tony presses the Send button, the email client connects to the email server and passes the name of the sender (Tony) and the recipient (Mary) with the body of the message to the email server.
- The server formats that information and attaches it to the bottom of the JMARY.TXT file. The entry in the file may look like:
    - From: MTony

  - To: JMary
  - Mary, how are you?
  - Tony
- The server also saves the time, date of receipt, and subject line into the file.
- If Mary wants to see the message in the email client, then she has to send the request to the server.



SMTP Server

CHFI

- 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:

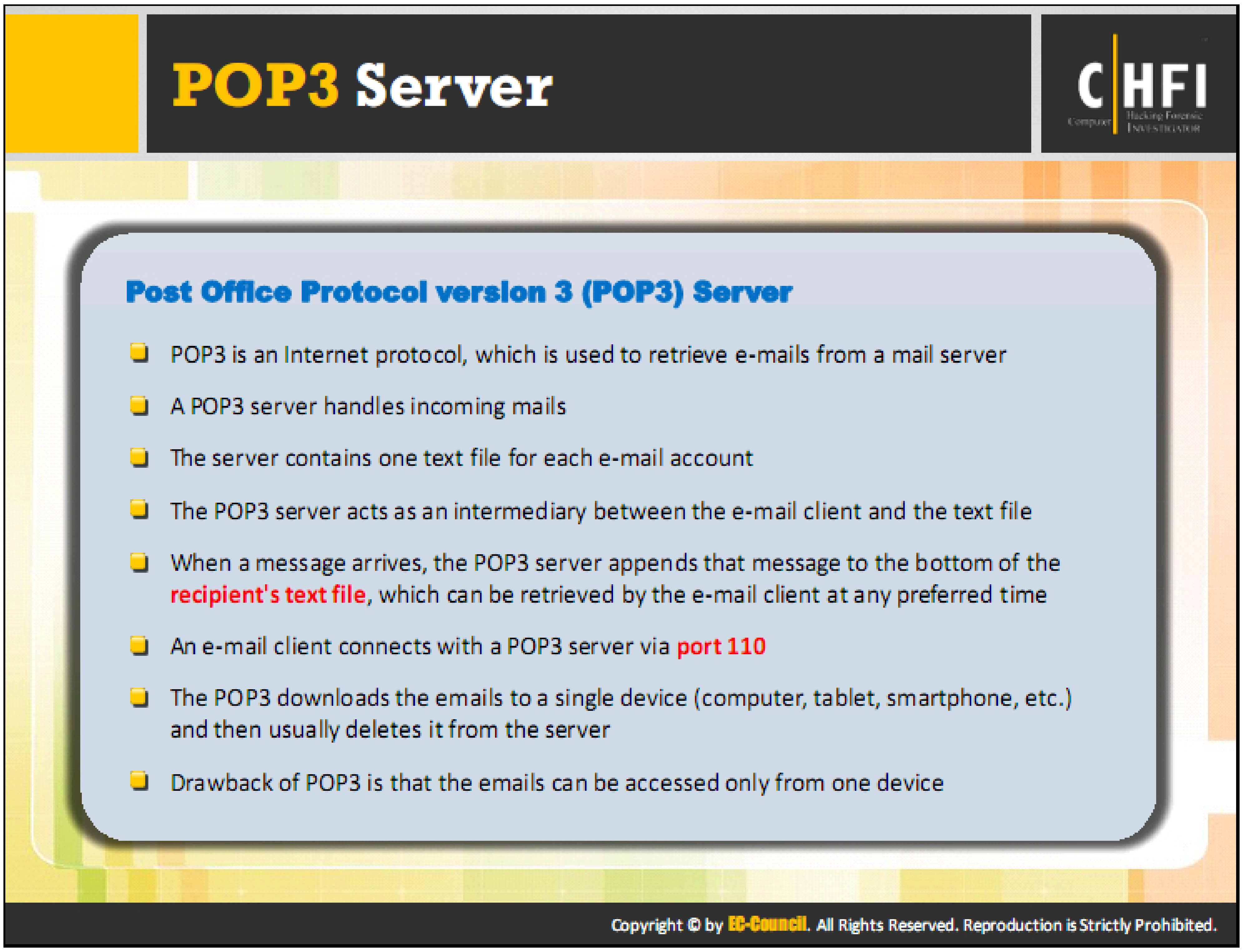
- When the user clicks on the Send button, Outlook connects to the server of *myicc.com* via port 25
- The client notifies the SMTP server about the sender's address, recipient's address, and body of the message
- The SMTP server breaks the recipient's address into the following parts:
  - The recipient's 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

SMTP (Simple Mail Transfer Protocol) is an outgoing mail server, which allows a user to send emails to a valid email address. Users cannot use SMTP server to receive emails; however, in conjunction with POP or IMAP, they can use SMTP to receive emails with proper configuration. The SMTP server is just a computer running SMTP, and it acts like a postman.

Consider you have an account with myicc.com, and you have to send an email to your friend at john@mybird.com through a client such as Outlook Express.

The process of email delivery by the SMTP server is as below:

1. When you click the Send button, the Outlook Express client connects to the server of myicc.com at port 25.
2. This client tells the sender, recipient's address, and body of the message to the SMTP server.
3. The SMTP server breaks the recipient's address into:
   - The recipient's name (john)
   - The domain name (mybird.com)
4. This SMTP server contacts the DNS and asks about the IP address of the SMTP server of mybird.com. The DNS replies to it and gives one or more IP addresses.
5. The SMTP server from myicc.com connects with the SMTP server of mybird.com using port 25 and gives the message to it. The SMTP server at mybird.com gets 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

POP3 (Post Office Protocol, version 3) is a simple protocol for retrieving emails from an email server. When the POP server receives emails, they are stored on the server until and unless the user requests it.

POP3 server does not allow the concept of folders; it considers the mailbox on the server to be its sole store. Once the user connects to the mail server to recover his or her mail using the email client, the messages automatically download from the mail server to the user's hard disk, and the mails are no longer stored on the mail server unless the user specifies to keep a copy of it.

The POP3 server can understand simple commands such as:

- **USER** - enter your user ID
- **PASS** - enter your password
- **QUIT** - quit the POP3 server
- **LIST** - list the messages and their size
- **RETR** - retrieve a message, according to a message number
- **DELETE** - delete a message, according to a message number

The type of mail server used by the mail account needs to be specified when a user configures his or her email client. Email programs such as Microsoft Outlook and Eudora can automatically support POP3. To set up their email program, users have to provide their usernames and passwords in order to receive POP3 mails. Examples of POP3 server address are “mail.testserver.com” or “pop.testserver.com.” Every POP3 mail server has its own address, which is normally allotted to the users by the web hosting company.

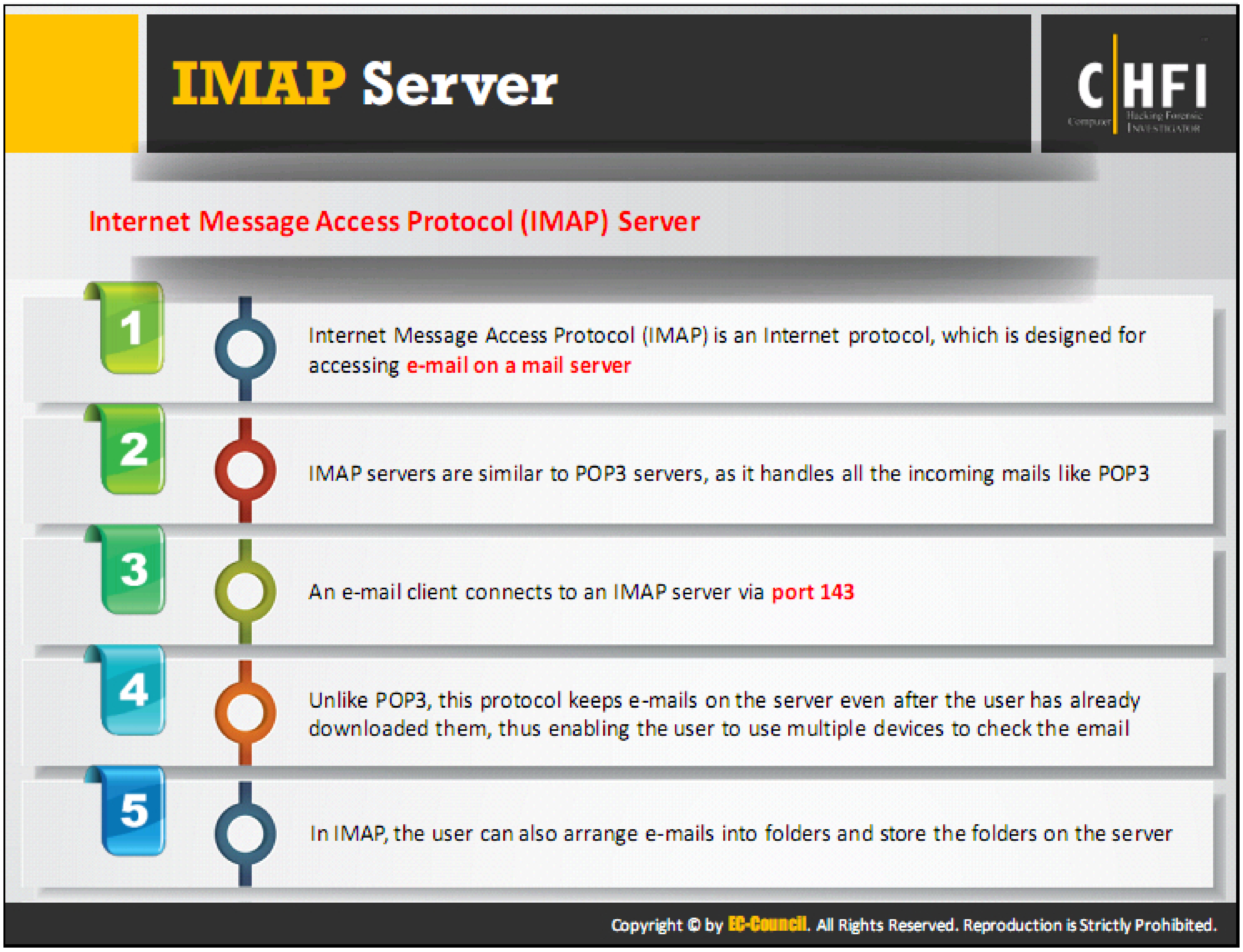
The POP protocol can collaborate virtually with any email program as long as the POP3 server is able to host the protocol.

Advantages:

- Since POP3 implemented email clients download mails onto the system, a user can read mails even when there is no internet connectivity.
- Users can create a new message and edit them even without logging onto the internet. These created messages are stored in the “hold folder.”
- Since all the mails and their attachments are stored on the hard drive of the system, you can quickly download the attachments whenever required.
- You can send and receive emails holding any amount of size, as there are no size limits.
- The size of mailbox depends on the size of the hard drive. Higher the capacity of the hard drive, higher the size of the mailbox.

Disadvantages:

- Since mails are stored on the hard drive, users cannot access these mails from remote machines.
- There is no proper email filtering mechanism, so if users download attachments containing malware, the malware may affect the entire system.
- If the folder storing the emails and attachments is corrupted or deleted, it is often cumbersome to retrieve them.
- Since emails are stored on the users’ machines, other people who have access to the users’ systems may be able to read the mails using applications that help to open the mail folders.



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

IMAP servers are similar to POP3 servers. Like POP3, IMAP handles the incoming mail. By default, the IMAP server listens on port 143, and the IMAPS (IMAP over SSL) listens on port 993.

IMAP stores emails on the mail server and allows users to view and manipulate their emails, as if the mails are stored on their local systems. This enables the users to organize all the mails depending on their requirement.

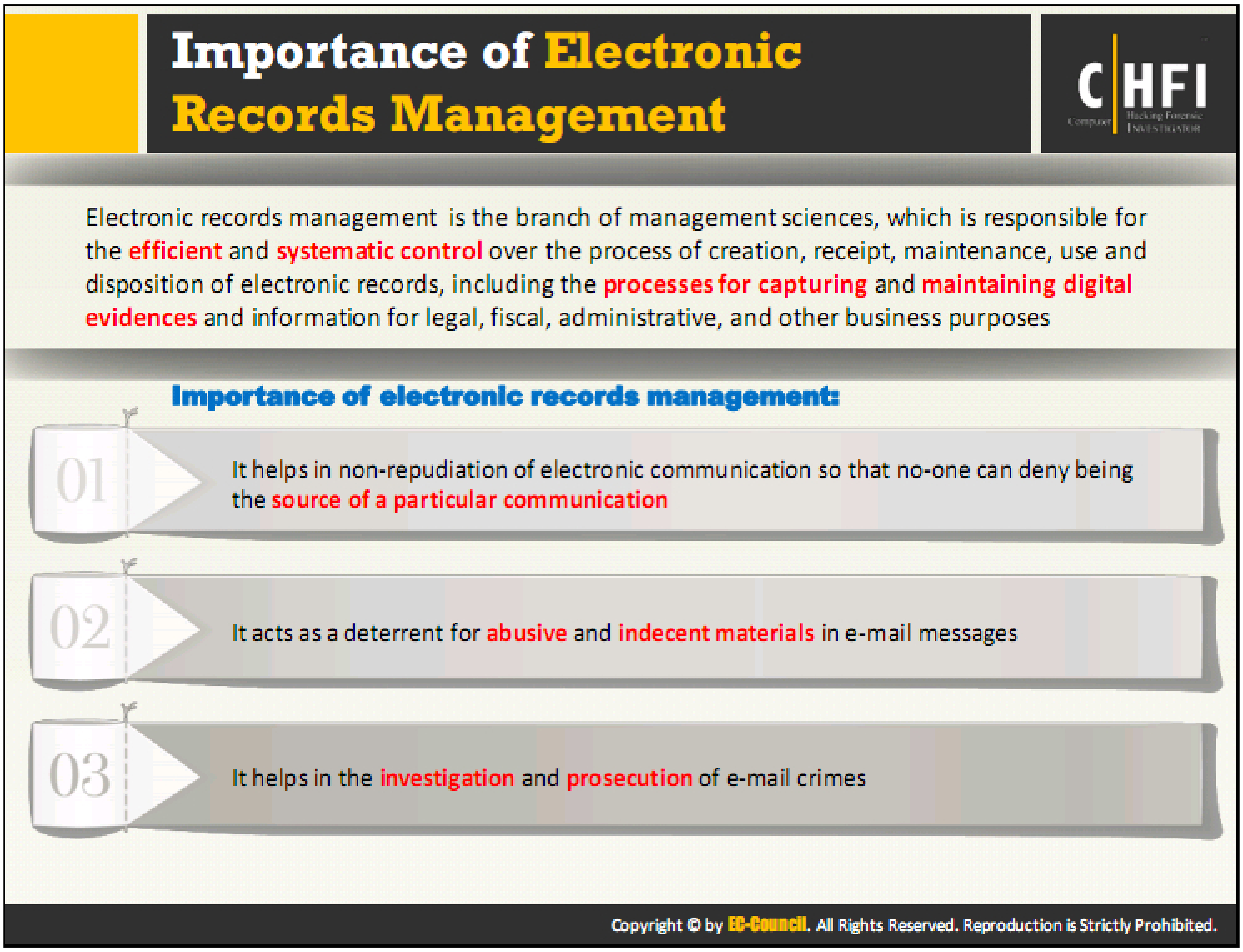
In contrast with POP3, IMAP does not move mails from the mail server to the user's mailbox. It acts as a remote server that stores all the user's mails in the mail server. IMAP allows email clients to retrieve MIME parts either in the form of an entire message or in multiple bits, allowing the clients to retrieve only the text part of the mail without downloading the attachment. This protocol stores a copy of all the emails on the server even if the user downloads them onto his/her system. You can also arrange your mails into folders and store them on the server.

Advantages:

- One can access the messages from any computer round the globe as they are stored on the server.
- It enables server-side filtering of spam messages.
- Saves time in deleting large messages in short time without having them downloaded, as users can view the header information of the message without having it downloaded

Disadvantages:

- The IMAP protocol does not allow users to access emails in offline mode.
- The mail server is sensitive to store space and requires regular archival of email messages.
- It is supported by very few ISPs as IMAP is assumed to be complex and a high-end option.
- Although IMAP implements authentication mechanism, attackers can easily bypass it since the credentials traverse through a network in plain text format.



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:

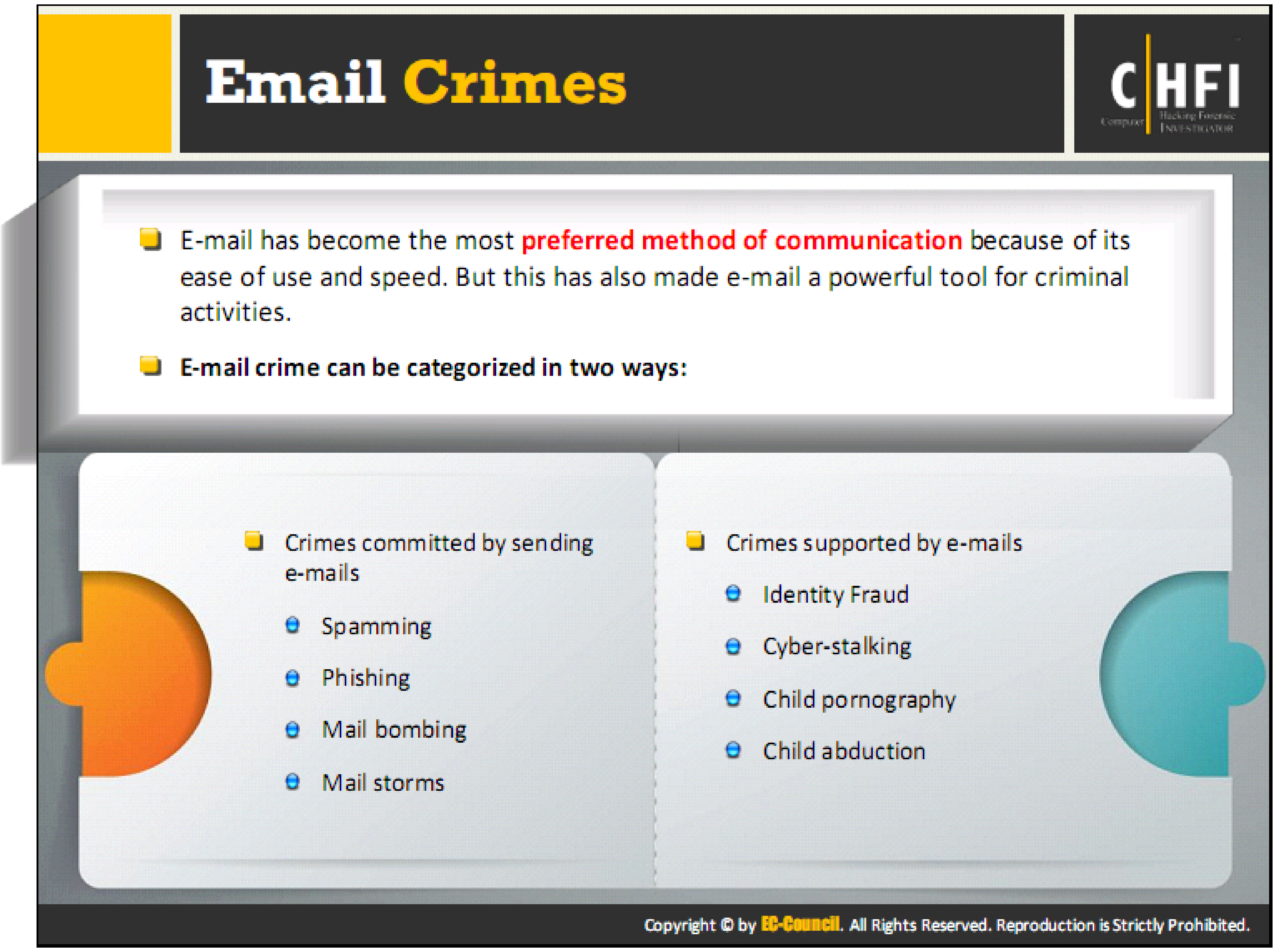
01 It helps in non-repudiation of electronic communication so that no-one can deny being the source of a particular communication

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

For an organization, any information in the form of electronic documents or records is a proprietary asset. ERM makes sure that the organization has all the documents or records it needs when they are required.

- It helps to the organizations to tackle any legal mandates pertaining to the protection of the organization.
- It protects against unauthorized access or manipulations of electronic data.
- It reduces the retrieval costs of the records that are no more required to be maintained on the system and also reduces the burden of keeping paper records.
- It helps to produce data on demand and withhold it for inspection.
- It helps in capacity management for effective usage of the IT resources such as servers and disk storages.
- Helps in preserving original form of email messages, thereby ensuring consistent mail forms.



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

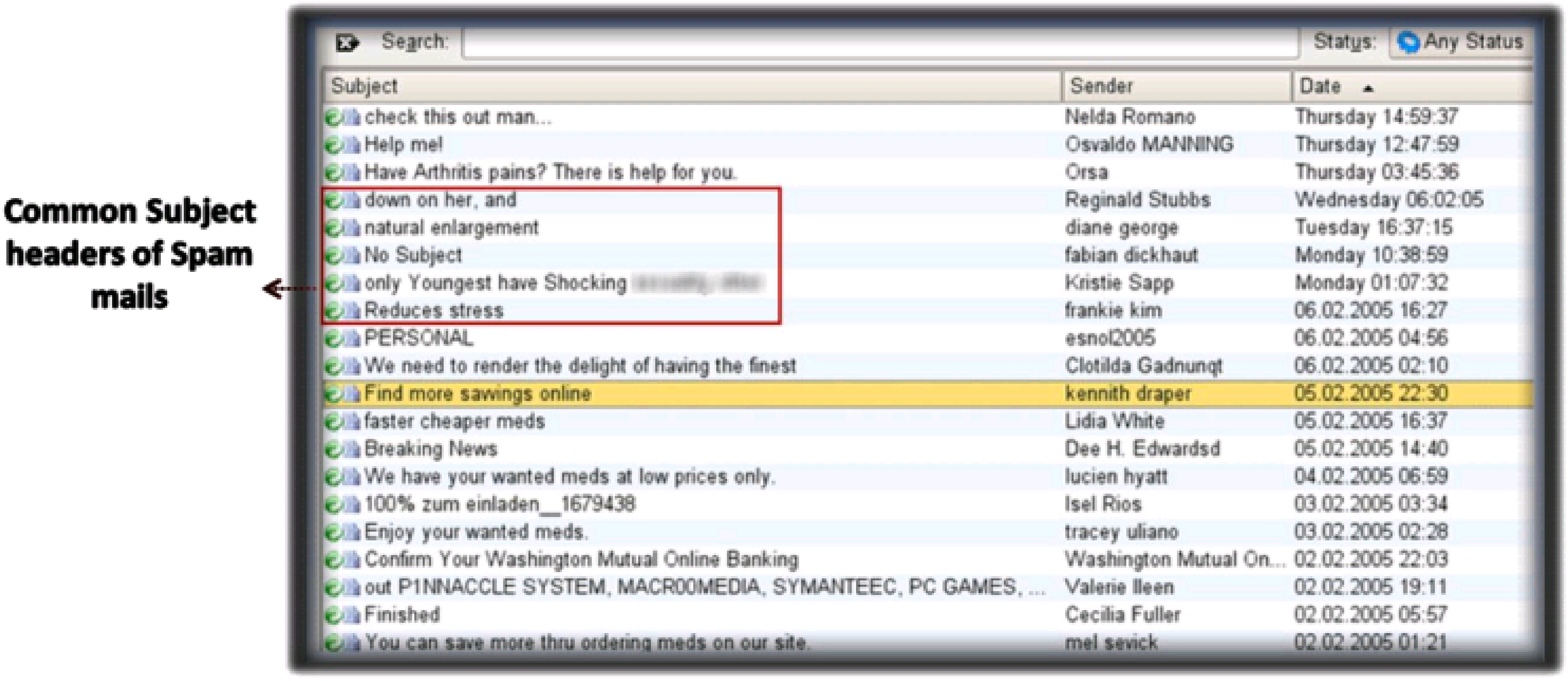
- Crimes supported by e-mails
  - Identity Fraud
  - Cyber-stalking
  - Child pornography
  - Child abduction

Before starting an email investigation, one should understand the term 'email crime.' Email crime is a serious offense. In the last few years, email has become the most preferred method of communication because of ease of use and speed. But these advantages have made email a powerful tool for criminals.

Email crimes and violations depend on the cyber laws created by the government of the place from where the email originates. For example, spamming is a crime in Washington State but not in other states. We can categorize email crime in two ways: one committed by sending emails and the other supported by emails. When criminals use emails for selling narcotics, stalking, fraud, child pornography, or child abduction, spamming, fake email, mail bombing, or mail storms then we can say that emails support cybercrime.

Email Spamming

Spam is unsolicited commercial email (UCE) or junk mail. Spam mail involves sending the same content to a huge number of addresses at the same time. Spamming or junk mail fills mailboxes and prevents users from accessing their regular emails. These regular emails start bouncing because the server exceeds its capacity limit. Spammers hide their identities by forging the email header. To avoid getting responses from annoyed receivers, spammers provide misleading information in the FROM and REPLY-TO fields and post them to a mailing list or newsgroup.



Common Subject headers of Spam mails

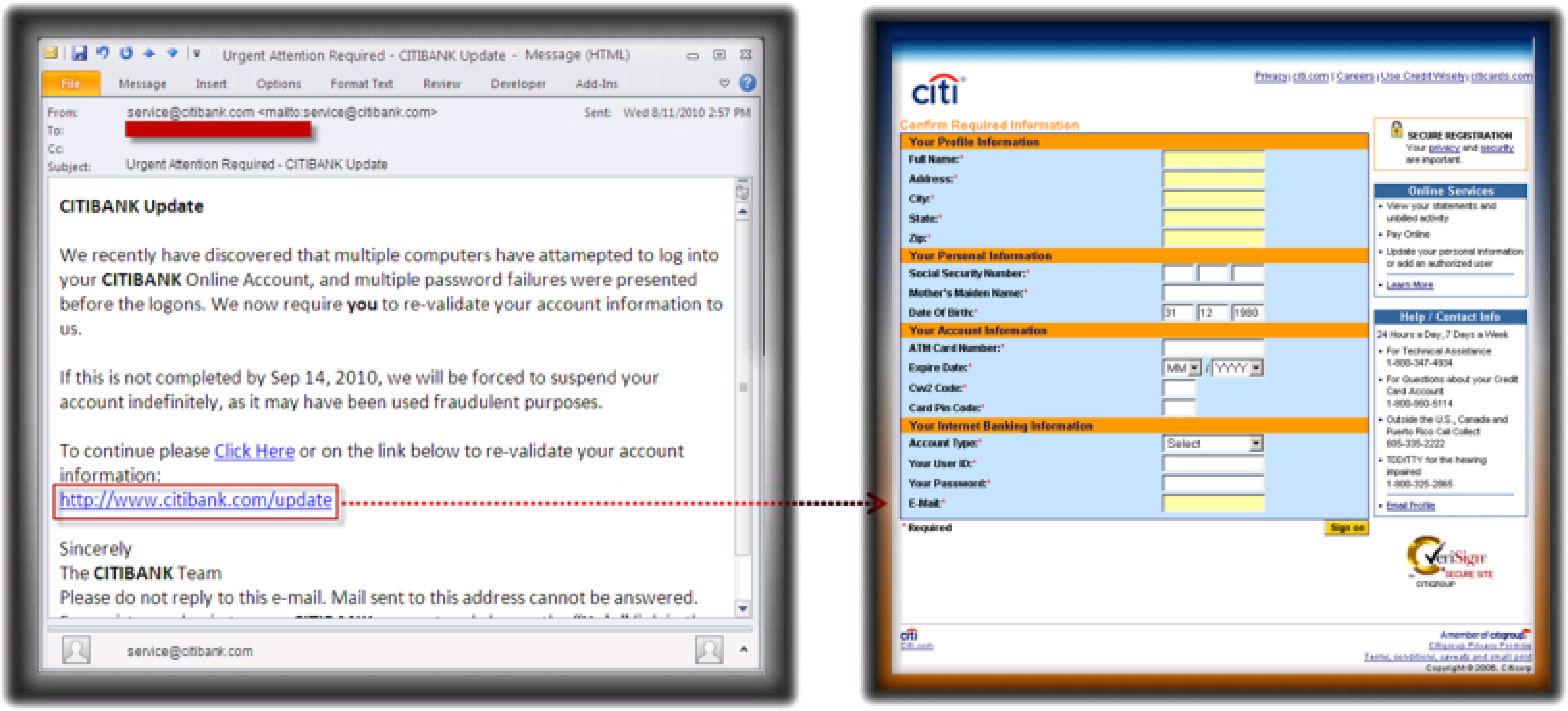
Subject	Sender	Date
check this out man...	Nelda Romano	Thursday 14:59:37
Help me!	Osvaldo MANNING	Thursday 12:47:59
Have Arthritis pains? There is help for you.	Orsa	Thursday 03:45:36
down on her, and	Reginald Stubbs	Wednesday 06:02:05
natural enlargement	diane george	Tuesday 16:37:15
No Subject	fabian dickhaut	Monday 10:38:59
only Youngest have Shocking [redacted]	Kristie Sapp	Monday 01:07:32
Reduces stress	frankie kim	06.02.2005 16:27
PERSONAL	esnol2005	06.02.2005 04:56
We need to render the delight of having the finest	Clotilda Gadnunqt	06.02.2005 02:10
Find more sawings online	kennith draper	05.02.2005 22:30
faster cheaper meds	Lidia White	05.02.2005 16:37
Breaking News	Dee H. Edwardsd	05.02.2005 14:40
We have your wanted meds at low prices only.	lucien hyatt	04.02.2005 06:59
100% zum einladen__1679438	Isel Rios	03.02.2005 03:34
Enjoy your wanted meds.	tracey uliano	03.02.2005 02:28
Confirm Your Washington Mutual Online Banking	Washington Mutual On...	02.02.2005 22:03
out P1NNACCLE SYSTEM, MACR00MEDIA, SYMANTEEC, PC GAMES, ...	Valerie Ileen	02.02.2005 19:11
Finished	Cecilia Fuller	02.02.2005 05:57
You can save more thru ordering meds on our site.	mel sevick	02.02.2005 01:21

FIGURE 12.1: Subject Headers of Spam Mails

Phishing

Phishing has emerged as an effective method used to steal personal and confidential data of users. It is an Internet scam that tricks users into divulging their personal and confidential information by making interesting statements and offers. Phishers can attack users by mass mailings to millions of email addresses across the world.

The phishing attack deceives and convinces the user with the fake technical content along with social engineering practices. The major task for phishers is to make the victims believe the phishing sites are legitimate. The sources that can be impersonated include web pages, instant messaging, emails, and Internet Relay Chat (IRC). Most phishing attacks are done through emails, where the user gets an email that tricks the user to follow the link given, navigating him or her to a phishing website. The email may contain a message stating that a particular transaction has occurred from the user's account and may have a link to check his or her balance, or the email may contain a link to perform a security check for the user's account.


Urgent Attention Required - CITIBANK Update - Message (HTML)
File
Message
Insert
Options
Format Text
Review
Developer
Add-Ins

From: service@citibank.com <mailto:service@citibank.com> Sent: Wed 8/11/2010 2:57 PM
To: [redacted]
Cc:
Subject: Urgent Attention Required - CITIBANK Update

CITIBANK Update

We recently have discovered that multiple computers have attamepted to log into your **CITIBANK** Online Account, and multiple password failures were presented before the logons. We now require **you** to re-validate your account information to us.

If this is not completed by Sep 14, 2010, we will be forced to suspend your account indefinitely, as it may have been used fraudulent purposes.

To continue please Click Here or on the link below to re-validate your account information:
http://www.citibank.com/update

Sincerely
The **CITIBANK** Team
Please do not reply to this e-mail. Mail sent to this address cannot be answered.

service@citibank.com

citi
Privacy | citi.com | Careers | Use Credit Wisely | citicards.com

Confirm Required Information

Your Profile Information
Full Name:*
Address:*
City:*
State:*
Zip:*

Your Personal Information
Social Security Number:*
Mother's Maiden Name:*
Date Of Birth:* 31 12 1980

Your Account Information
ATM Card Number:*
Expire Date:* MM / YYYY
Cvv2 Code:*
Card Pin Code:*

Your Internet Banking Information
Account Type:* Select
Your User ID:*
Your Password:*
E-Mail:*

* Required

Sign on

SECURE REGISTRATION
Your privacy and security are important.

Online Services
- View your statements and unbilled activity
- Pay Online
- Update your personal information or add an authorized user
- Learn More

Help / Contact Info
24 Hours a Day, 7 Days a Week
- For Technical Assistance 1-800-347-4934
- For Questions about your Credit Card Account 1-800-950-5114
- Outside the U.S., Canada and Puerto Rico Call Collect 605-335-2222
- TDD/TTY for the hearing impaired 1-800-325-2865
- Email Profile

A member of citigroup
Citigroup Privacy Promise
Terms, conditions, caveats and small print
Copyright © 2006, Citicorp

FIGURE 12.2: Phishing Attack

Mail Bombing

Email bombing refers to the process of repeatedly sending an email message to a particular address at a specific victim's site. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial of service impact.

Mail bombing is an intentional act of sending multiple copies of identical content to the same recipient. The primary objective behind mail bombing is to overload the email server and degrade the communication system by making it unserviceable. Usually, a mail bomber and the victim know each other. Newsgroup postings that do not agree with the recipient's opinion also result in mail bombing. The target of a mail bomber can be either a specific machine or a particular person. Mail bombing is more abusive than spamming because it not only sends mails in excessive amounts to a particular person, but it also prevents other users from accessing their email using the same server.

Mail Storms

A mail storm occurs when computers start communicating without human intervention. The flurry of junk mail sent by accident is a mail storm. Usage of mailing lists, auto-forwarding emails, automated response, and the presence of more than one email address are the various causes for a mail storm. Malicious software code is also written to create mail storms such as the "Melissa, I-Love-u" message. Mail storms hinder communication systems and also make them inoperable.

Identity Fraud

Identity fraud is the illegitimate retrieval and use of others' personal data for malicious and monetary gains. Identity theft is a crime that is quickly gaining popularity. It is the willful act of stealing someone's identity for monetary benefits. Criminals obtain personal information about a person and misuse it, causing heavy financial loss to the victim. Online shopping sites that have false representations and spam emails that contain irresistible offers are the common means used to obtain the victim's credit card numbers. Once the user has placed the order placed online, criminals can intercept the email message and used it. Criminals not only withdraw huge amounts of money from the victims' accounts but can also make the victim bankrupt.

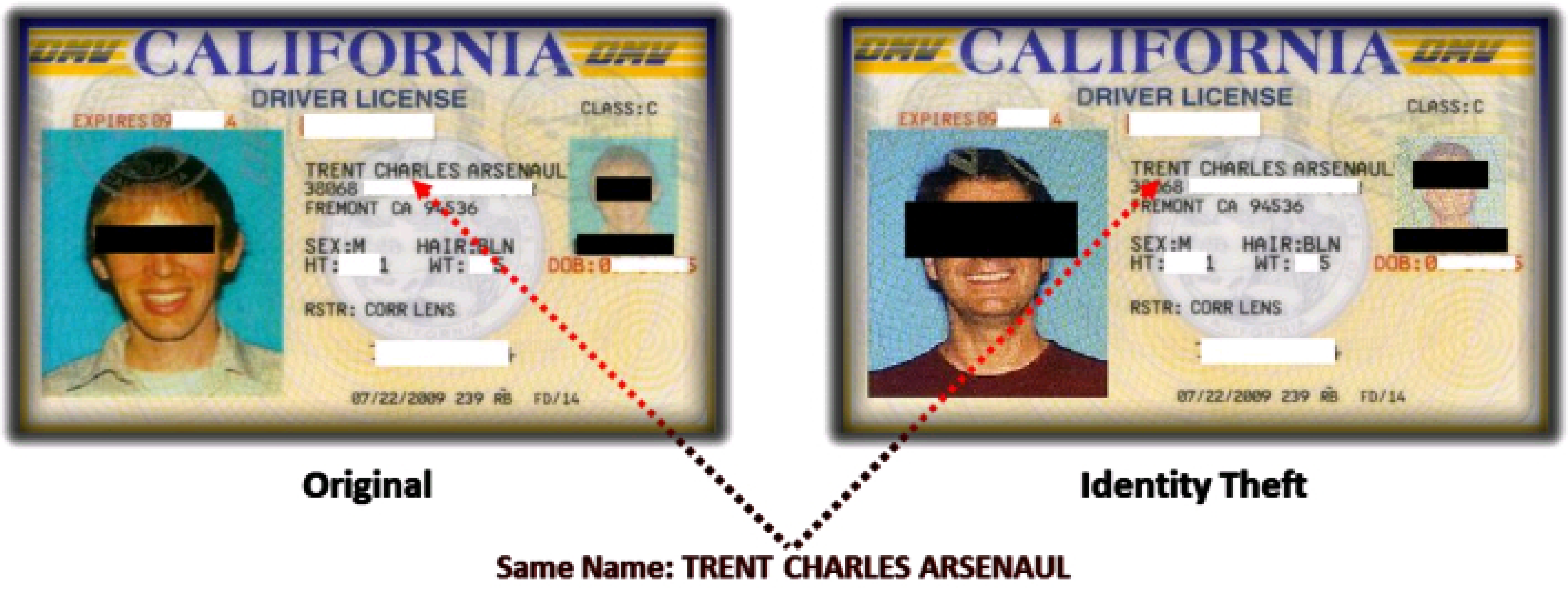


FIGURE 12.3: Identity Fraud

Cyberstalking

Cyberstalking is a crime where attackers harass an individual, a group, or an organization using emails or IMs (instant messengers). Attackers try to threaten, solicit for sex, make false accusations, defame, slander, libel, or steal the identity of the victim/victims as a part of cyberstalking. The stalker can be someone associated with the victim or a stranger.

Child Pornography

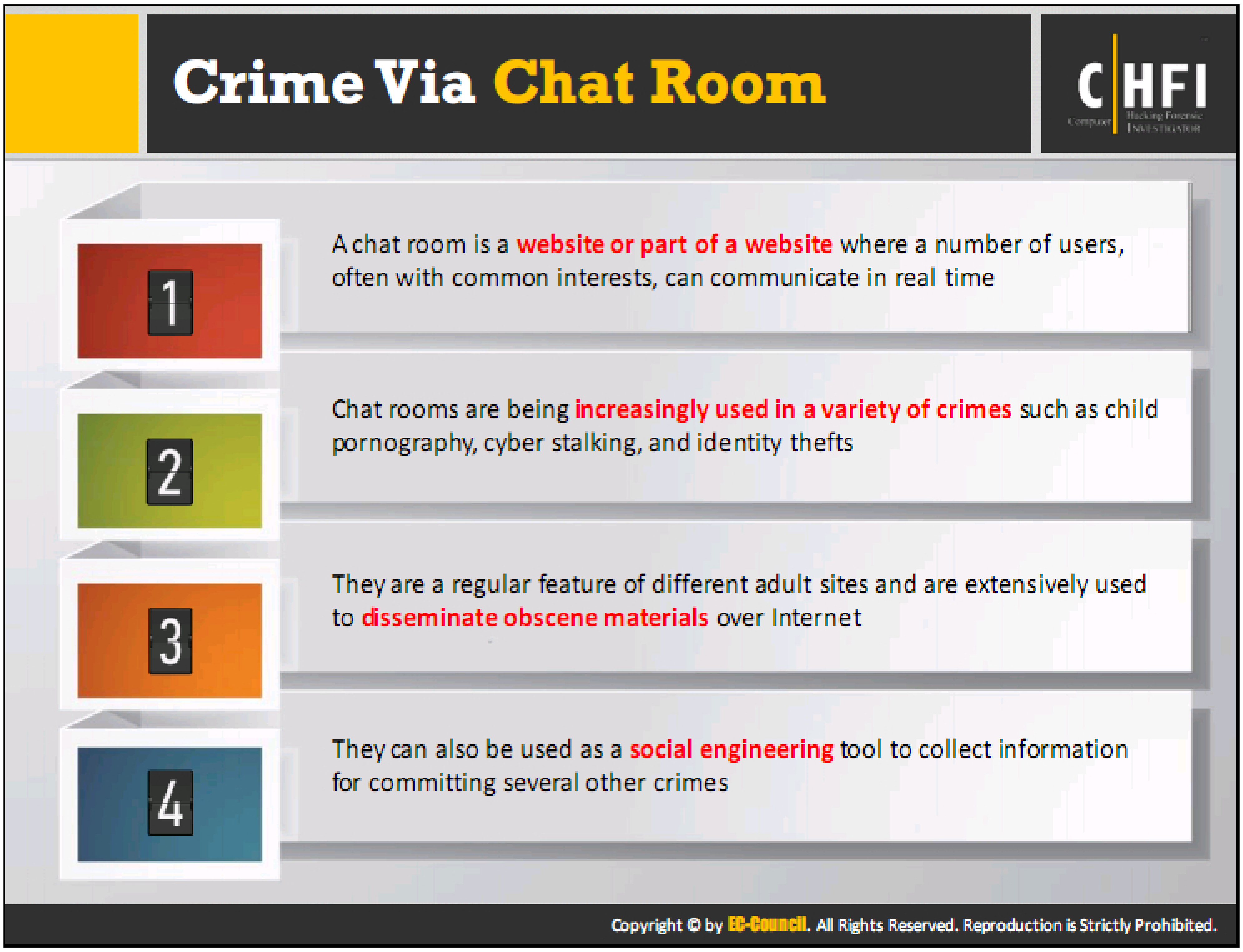
Source: *https://www.hg.org*

Child Pornography is a criminal offense where a child or a minor is depicted of engaging in a sexually explicit conduct such as photographs, film, video, pictures or computer-generated images or pictures, whether made or produced by electronic, mechanical, or other means.

Child Abduction

Source: *https://www.hg.org*

Child Abduction is the offense of wrongfully removing or wrongfully retaining, detaining or concealing a child or baby. Abduction is defined as taking away a person by persuasion, fraud, or open force or violence. There are two types of child abduction: parental child abduction and abduction by a stranger. Parental child abductions are the most common type while abduction by stranger comes under kidnap.



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

"A chat room is a website, part of a website, or part of an online service such as America Online, that provides a venue for communities of users with a common interest to communicate in real time."

On one hand, online instant messaging or chat rooms have benefited children, but on the other hand, these have become a potential source of sexual abuse. Pedophiles use chat rooms to sexually abuse children by establishing online relationships with them. They emotionally attract the child and befriend them. After establishing a steady relationship, they introduce children to pornography by providing images and videos that contain sexually explicit material. Pedophiles exploit children for cybersex, which may lead to physical abuse.

Email Message

An email message is composed of three parts:

1. Header

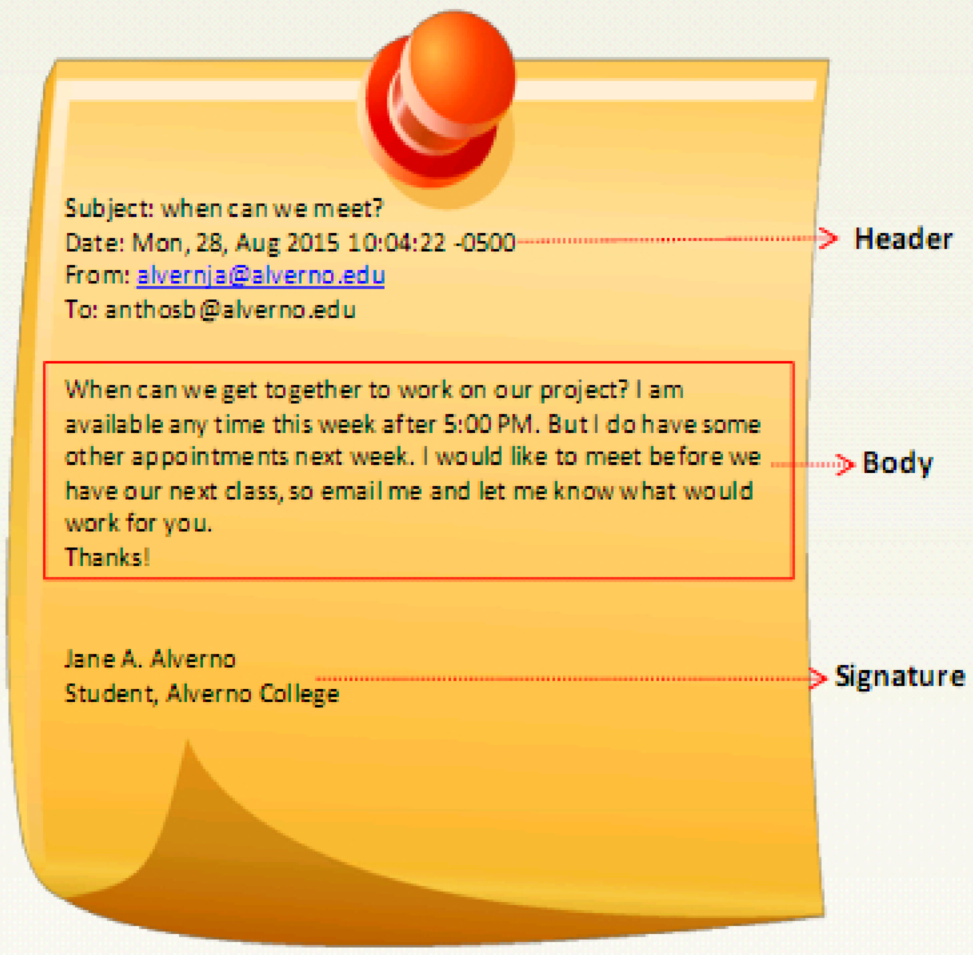
- E-mail headers contain information about the e-mail origin such as the address from where it came, the routing, time of the message, and the subject line
- Some of the header information that is usually important to a technician is kept hidden by the email software
- Examples include To, Cc, Bcc, From, 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



Subject: when can we meet?
Date: Mon, 28, Aug 2015 10:04:22 -0500
From: alvernja@alverno.edu
To: anthosb@alverno.edu

When can we get together to work on our project? I am available any time this week after 5:00 PM. But I do have some other appointments next week. I would like to meet before we have our next class, so email me and let me know what would work for you.
Thanks!

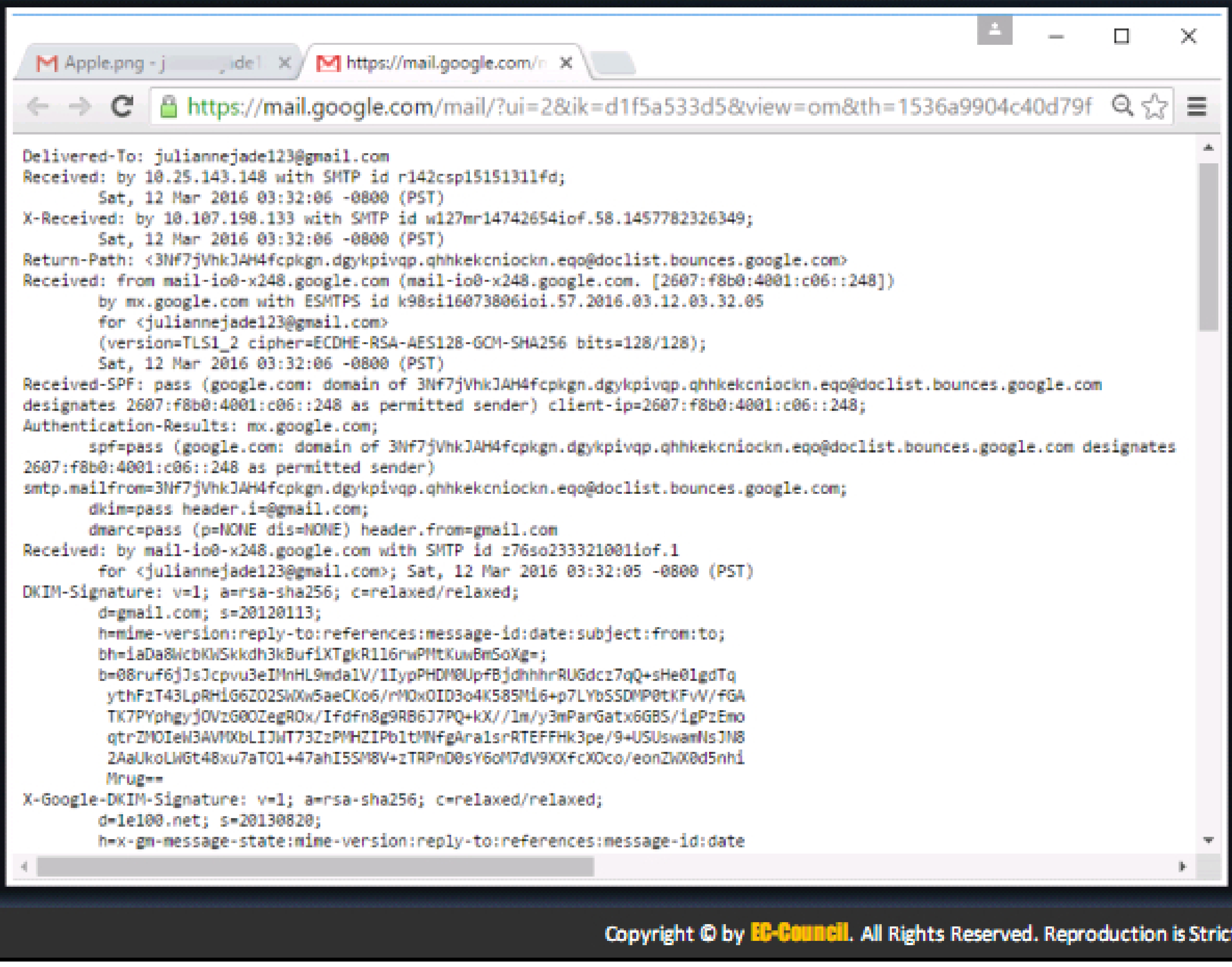
Jane A. Alverno
Student, Alverno College

Header

Body

Signature

Sample Email Header



Apple.png - j ide1
https://mail.google.com/
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=iaDa8WcbKWSkkdh3kBufiXTgkR116rwPMtKuwBmSoXg=;
        b=08ruf6jJsJcpvu3eIMnHL9mdalV/1IypPHDM0UpfBjdhhhrRUGdcz7qQ+sHe01gdTq
         ythFzT43LpRHiG6ZO2SWXw5aeCKo6/rMOxOID3o4K585Mi6+p7LYbSSDMP0tKFvV/fGA
         TK7PYphgyjOVzG0OZegROx/Ifdfn8g9RB6J7PQ+kX//1m/y3mParGatx6GBS/igPzEmo
         qtrZMOIeW3AVMXbLIJWT73ZzPMHZIPb1tMNfgAra1srRTEFFHk3pe/9+USUswamNsJN8
         2AaUkoLWGt48xu7aTO1+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
```

Email message is a brief and informal text sent or received over a network. Email messages are simple text messages, which also include attachments like image files and spreadsheets. Multiple recipients can receive email messages at a time. At present, RFC 5322 defines the Internet email message format, and RFC 2045 through RFC 2049 defines multi-media content attachments, together called Multipurpose Internet Mail Extensions or MIME.

Email messages are made of two main sections: one is the message header, and the other is the message body. The message header may include following fields:

- **To**

  This header specifies to whom the message is addressed. Note that the "To" header does not always contain the recipient's address.

- **Cc**

  This stands for "carbon copy." This header specifies additional recipients beyond those listed in the "To" header.

  The difference between "To" and "Cc" is essentially connotative; some mailers also deal with them differently in generating replies.

- **Bcc**

  This stands for "blind carbon copy." This header sends copies of e-mails to people who might not want to receive replies or appear in the headers.

  Blind carbon copies are popular with spammers since they confuse many inexperienced users who get an e-mail that does not have their address or does not appear to be for them.

- **From**

  This specifies the sender of the message.

- **Reply-To**

  This header specifies an address for sending replies. Though this header has many legitimate uses, it is also widely used by spammers to deflect criticism. Occasionally, a naive spammer will solicit responses by e-mail and use the "Reply-To" header to collect them, but more often, the address specified in junk e-mail is either invalid or that of an innocent victim.

- **Sender**

  This header is unusual in e-mail ("X-Sender" is usually used instead) but appears occasionally, especially, in copies of Usenet posts. It should identify the sender; in the case of Usenet posts, it is a more reliable identifier than the "From" line.

- **Subject**

  This is a completely free-form field specified by the sender to describe the subject of the message.

- **Apparently-To**

  Messages with many recipients sometimes have a long list of headers of the form "Apparently-to: rth@bieberdorf.edu."

  These headers are unusual in the legitimate mail; they are normally a sign of a mailing list, and in recent times, mailing lists have generally used software sophisticated enough not to generate a giant pile of headers.

- **Comments**

  This is a nonstandard, free-form header field. Some mailers add this header to identify the sender; however, spammers often add it by hand (with false information).

- **Date**

  The header specifies a date of creation and sending of the email. If the sender's computer omits this header, a mail server or some other machine might conceivably add it or even along the route.

- **Errors-To**

  This header specifies an address for mailer-generated errors, such as bounce messages, and to go to (instead of the sender's address). This is not a particularly common header, as the sender usually wants to receive any errors at the sending address, which is what most mail server software does by default.

- **Message-Id**

  This header more-or-less specifies a unique ID associated with each message that the first mail server coming across the message generally assigns to it.

  Usually, it is in the form "foo@mailserv.com," where:

  "foo" part could be absolutely anything (at times it indicates the sender's username).

  "mailserv.com" part represents the machine's name that assigned the unique ID to the message.

- **In-Reply-To**

  A Usenet header that occasionally appears in mail, the "In-Reply-To" header gives the message ID of the message to which it is replying. It is unusual for this header to appear except in e-mail directly related to Usenet; spammers use it, probably in an attempt to evade filtration programs.

- **Content-Transfer-Encoding**

  This header relates to MIME, a standard way of enclosing non-text content in e-mail. It has no direct relevance to the delivery of mail, but it affects how MIME-compliant mail programs interpret the content of the message.

- **Content-Type**

  This is another MIME header, which informs the MIME-compliant email programs regarding the type of content to expect in the message.

- **MIME-Version**

  This is another MIME header that specifies the version of the MIME protocol used by the sender.

- **Newsgroups**

  This header appears only in e-mail connected with Usenet—either e-mail copies of Usenet postings or e-mail replies to postings. In the first case, it specifies the newsgroup(s) to which the user posted the message; in the second, it specifies the newsgroup(s) in which another user had posted the reply message.

- **Organization**

  This is an entirely free-form header that holds the name of the organization through which the sender of the message has net access. The sender can generally control this header.

- **References**

  The "References" header is rare in e-mail except for copies of Usenet postings. It is used to identify the upstream posts to which a message is a response; when it appears in an e-mail, it is usually just a copy of a Usenet header. It may also appear in e-mail responses to Usenet postings, giving the message ID of the post getting responses to as well as the references from that post.

- **Priority**

  This is an essentially free-form header that assigns a priority to the mail. Most software ignores it. Spammers use it often in an attempt to get their messages read.

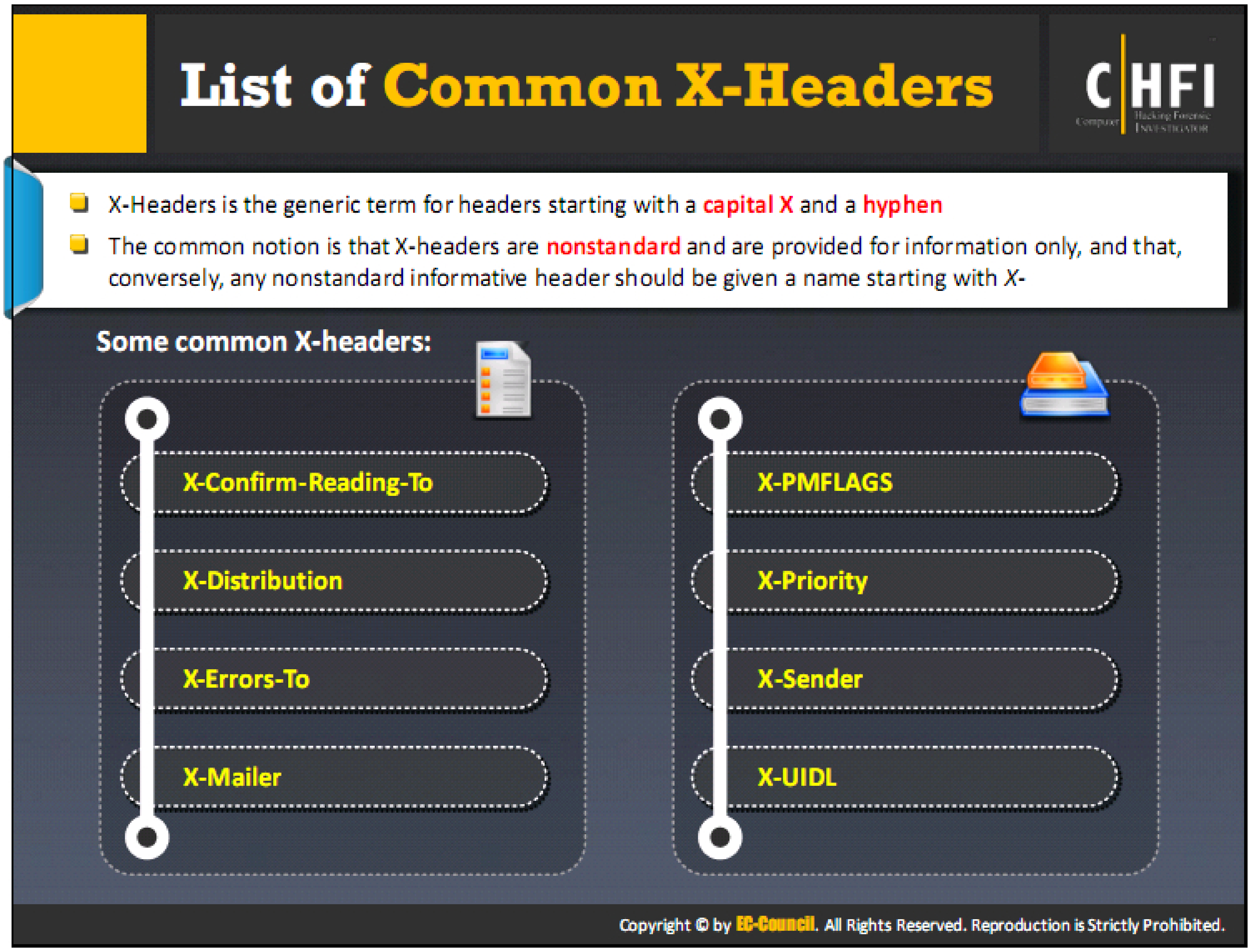
The body has the message conveyed through the mail that sometimes includes a signature block in the end. A blank line separates the header and the body. In an email, the body or text always comes after the header lines.

The email body is the main message of the email which contains text, images and other data (like attachments). The email body displays attachments separately that appear in line with the text. The size of an email's body text does not have limitations set by the internet email standard. However, mail servers have message size limits. The maximum size for email body with attachments is 10-25 MB. The minimum size allowed for both email header lines and body is 64 KB.

An email signature is a small amount of additional information attached at the end of the email message, which consists of name and contact details of the email sender. They can also contain plain text or images.

Sample Email Header

Email Headers are the metadata attached to every email which contains a lot of useful evidentiary information for a forensic investigator. Each email is included with a block of text at the top called a header. The header has the information about the message, like the sender information, the recipient information, the servers managing the message, etc. There are few compulsory headers like FROM, TO, and DATE. Other headers like SUBJECT and CC are optional. Other headers consist of the sending and receiving time stamps of all mail transfer agents that received and sent the message. It means, when a message is transferred from one person to another (i.e. sending or forwarding email), that message is date/time stamped by a mail transfer agent (MTA). An MTA is a computer program or software agent that enables email transfer from one system to another. This date/time stamp is one of the headers that precede the email body. Most of the email clients by default do not show the header information.



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

Common X-headers:

- **X-Confirm-Reading-To**

  This header helps users to receive an automated notification when the recipient receives or reads the message. The emails send these notifications as soon as the recipient performs the above-said actions.

- **X-Distribution**

  The author of Pegasus had added this header to address the issue with mass mailing or spams. This helps Pegasus to identify if the received mail had numerous recipients by adding the 'X-Distribution: bulk' tag to the header.

- **X-Errors-To**

  This enables the users to add an email address to which it can send the errors.

- **X-Mailer**

  Users can use this free-form header field when they want the recipient to know their mail software. Attackers use special software to send junk e-mail, and this field will help the filters in their task.

- **X-PMFLAGS**

  Pegasus adds this header added in any message users sends using it.

- **X-Priority**

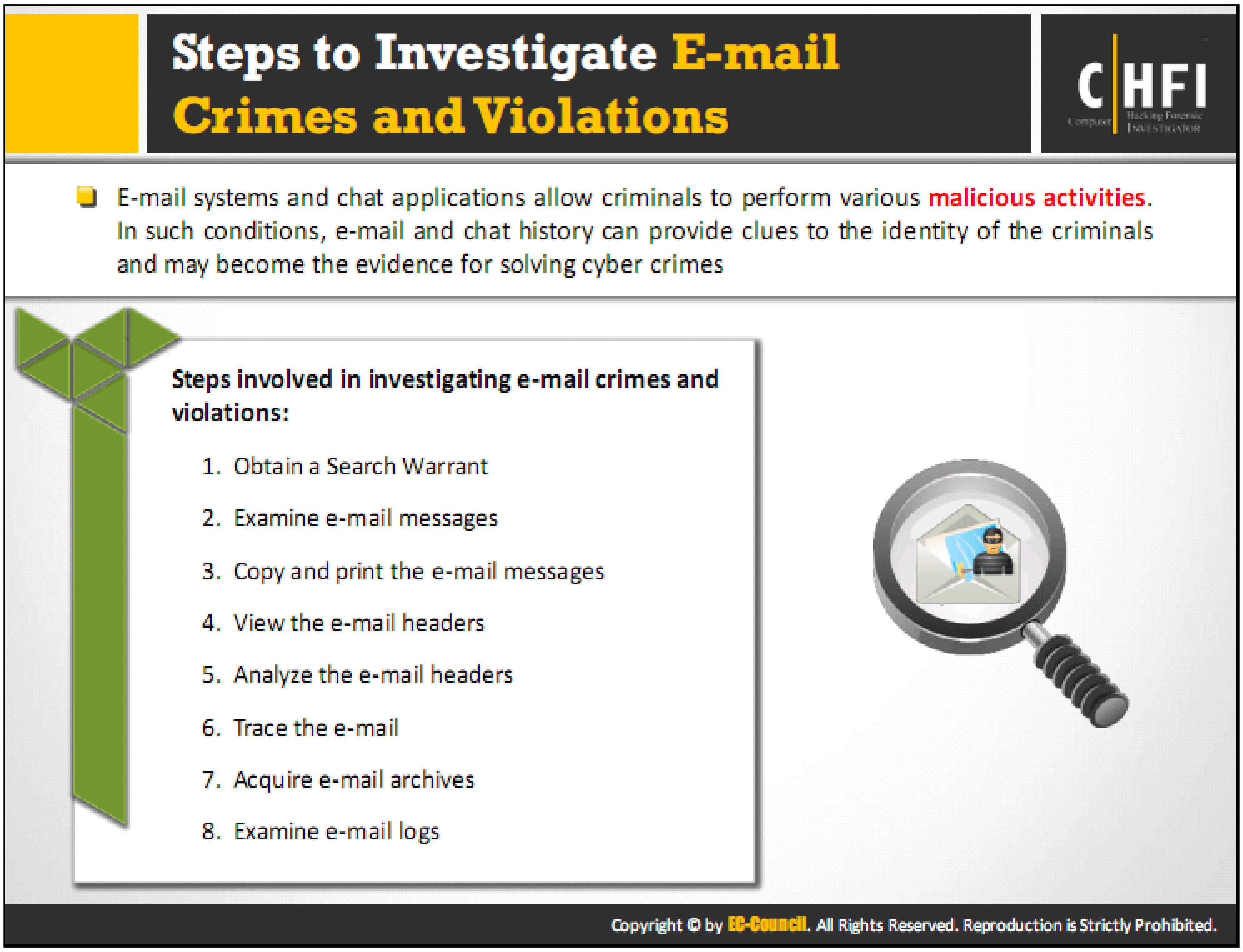
  This header helps in defining priority. Outlook uses this header to assign a priority.

- **X-Sender**

  The e-mail equivalent to the Sender in normal messages that is more consistent in defining the Sender of the email compared to the “From” header. Attackers can easily forge this header.

- **X-UIDL**

  POP uses this unique identifier for retrieving mail from a server. Attackers add this header between the recipient’s mail server and the recipient’s mail client; if mail arrives at the mail server with an “X-UIDL” header, it is probably junk.



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

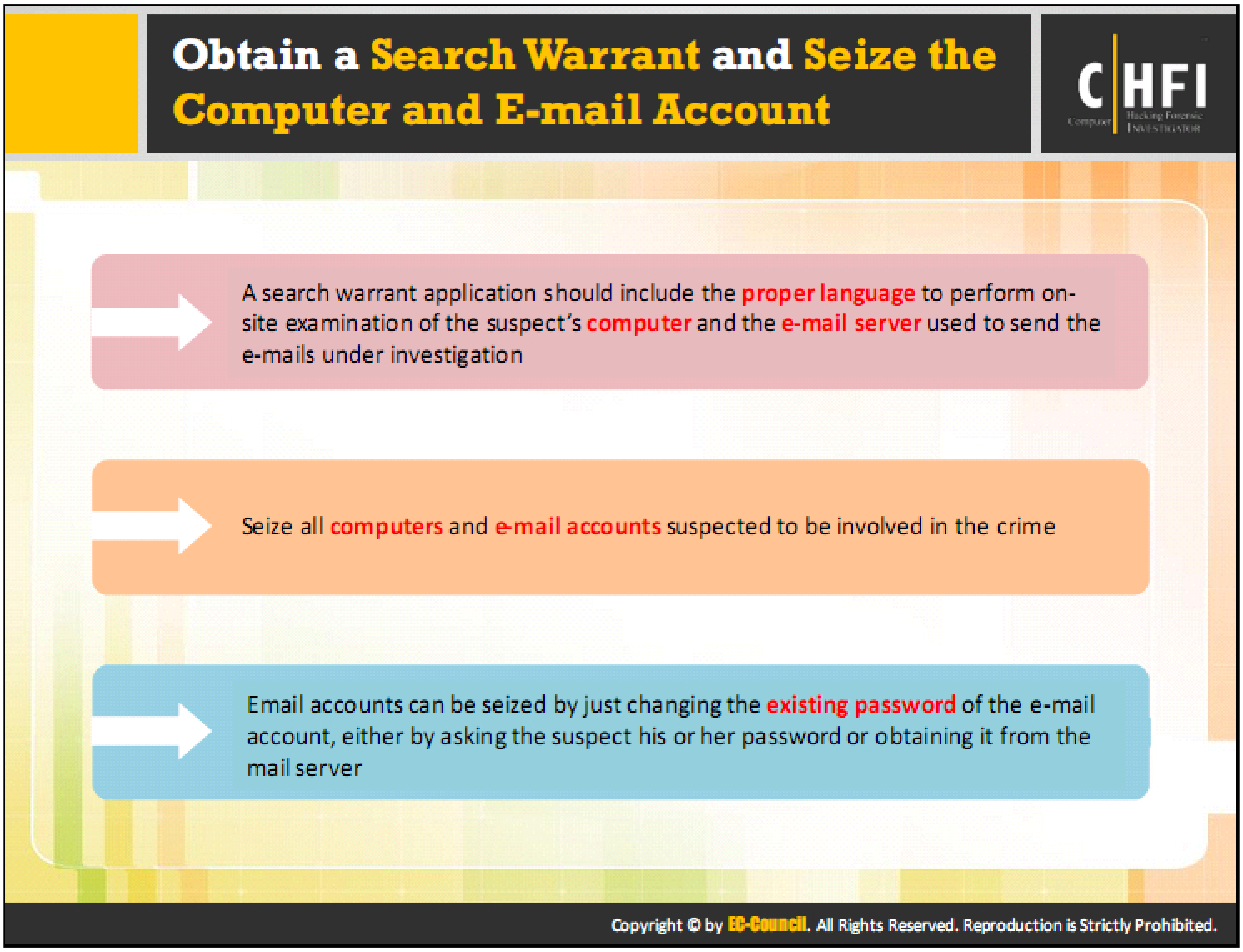
Steps involved in investigating e-mail crimes and violations:

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

The investigations of criminal activities or violation of policies related to e-mails are similar to other kinds of computer crime investigations. The primary goal is to gather evidence and report findings in order to find and prosecute the perpetrator. E-mail crimes depend on the location where the e-mails arise. Example, in Washington State, it is illegal to send unsolicited e-mails, whereas it is legal in other states.

Crimes involving e-mails are becoming common, and the investigators have linked e-mail communications to crimes. Many illegal activities such as extortion, narcotics, trafficking, stalking, sexual harassment, terrorism, fraud, child abductions, child pornography, etc., involve using e-mails for communications. Therefore, any crime or policy violation can involve e-mail, and it is an important medium to gather evidence.

In order to be able to find, extract, and analyze the e-mail related evidence, the investigators must follow a series of defined and practiced steps. This will not only ease the process of gathering the evidence but also help the investigators in maintaining compliance and integrity.

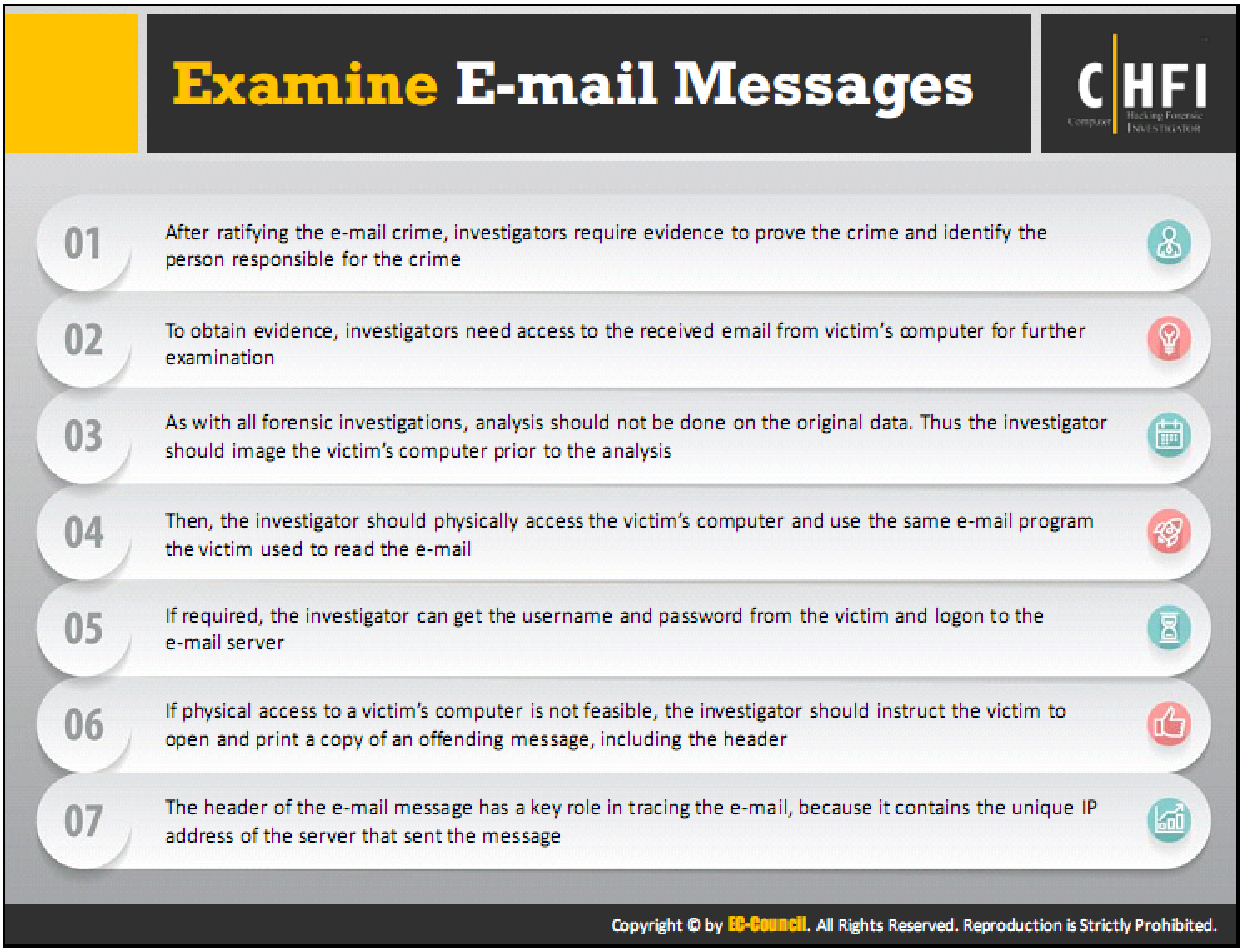


Obtain a Search Warrant and Seize the Computer and E-mail Account

- 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

To carry out the on-site examination of the computer and email server, the investigators should obtain a search warrant application in the appropriate language. Then, they should conduct a forensics test on the permitted equipment as mentioned in the warrant. All the computers and email accounts suspected to be involved in the crime should be seized. The investigators can seize the email accounts by changing the existing password of the email account, either by asking the victim his or her password or from the mail server.

After the detection of an email crime, investigators and prosecutors require evidence to prove the crime. To obtain evidence, the investigator requires access to the victim's computer, which contains the email that the victim received. The first thing to do is to image the victim's computer and then, physically access the victim's computer and use the email program used by the victim to read the email. If required, the investigators can get the username and password from the victim and can log into the email service to open protected or encrypted files. In case physical access to a victim's computer is not feasible, the investigators may instruct the victim to open and print the copy of an offending message, including the header. The header of the email message plays a key role in email tracing because it contains the unique IP address of the server that sent the message.



Examine E-mail Messages

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

After confirming the crime, the investigators need to check if the crime involves email. If the report mentions any email, the email account should be accessed from the victim's desktop and the mail along with the headers should be copied. Forensics investigation and analysis should be performed on the system to find relevant data. In case the client or email account details are not available, various email artifacts should be gathered from the system, including the email archive, email client backup, RAM data that can contain email account credentials, system and network logs, etc.

If the victim is a corporate organization, then the investigators should have permission from the concerned authorities and work in collaboration with the internal network and system administrators to understand their policies and abide by their data safety regulations.

The primary information required for starting an email investigation is the unique IP address. The investigator can retrieve this by examining the email header. The email headers also provide additional information such as the date and time of sending the message, attachments, and the unique message, which are helpful in email tracking. The message header can provide significant information if examined properly. It is important to know how to find emails headers in various command-line, Web-based, and GUI clients. For this, open the email header and copy and paste the headers to a text document.

Copy and Print the E-mail Message

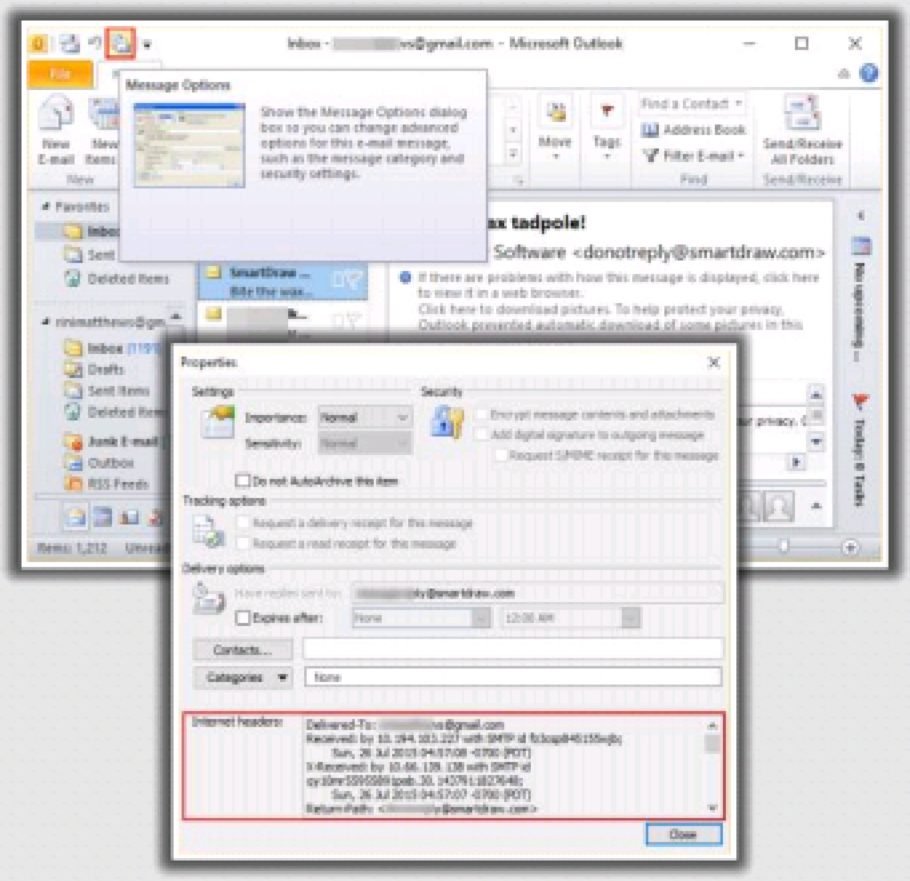
- An e-mail investigation can be started as soon as the offending e-mail message is copied and printed
- Some e-mail clients will allow an investigator to copy e-mail messages from the inbox folder to a portable device

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.


Inbox - [redacted]vs@gmail.com - Microsoft Outlook

Message Options

Show the Message Options dialog box so you can change advanced options for this e-mail message, such as the message category and security settings.

...ax tadpole!
... Software <donotreply@smartdraw.com>

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this

Properties

Settings
Importance: Normal
Sensitivity: Normal
□ Do not AutoArchive this item

Security
□ Encrypt message contents and attachments
□ Add digital signature to outgoing message
□ Request S/MIME receipt for this message

Tracking options
□ Request a delivery receipt for this message
□ Request a read receipt for this message

Delivery options
Have replies sent to: [redacted]ly@smartdraw.com
□ Expires after: None 12:00 AM

Contacts...
Categories: None

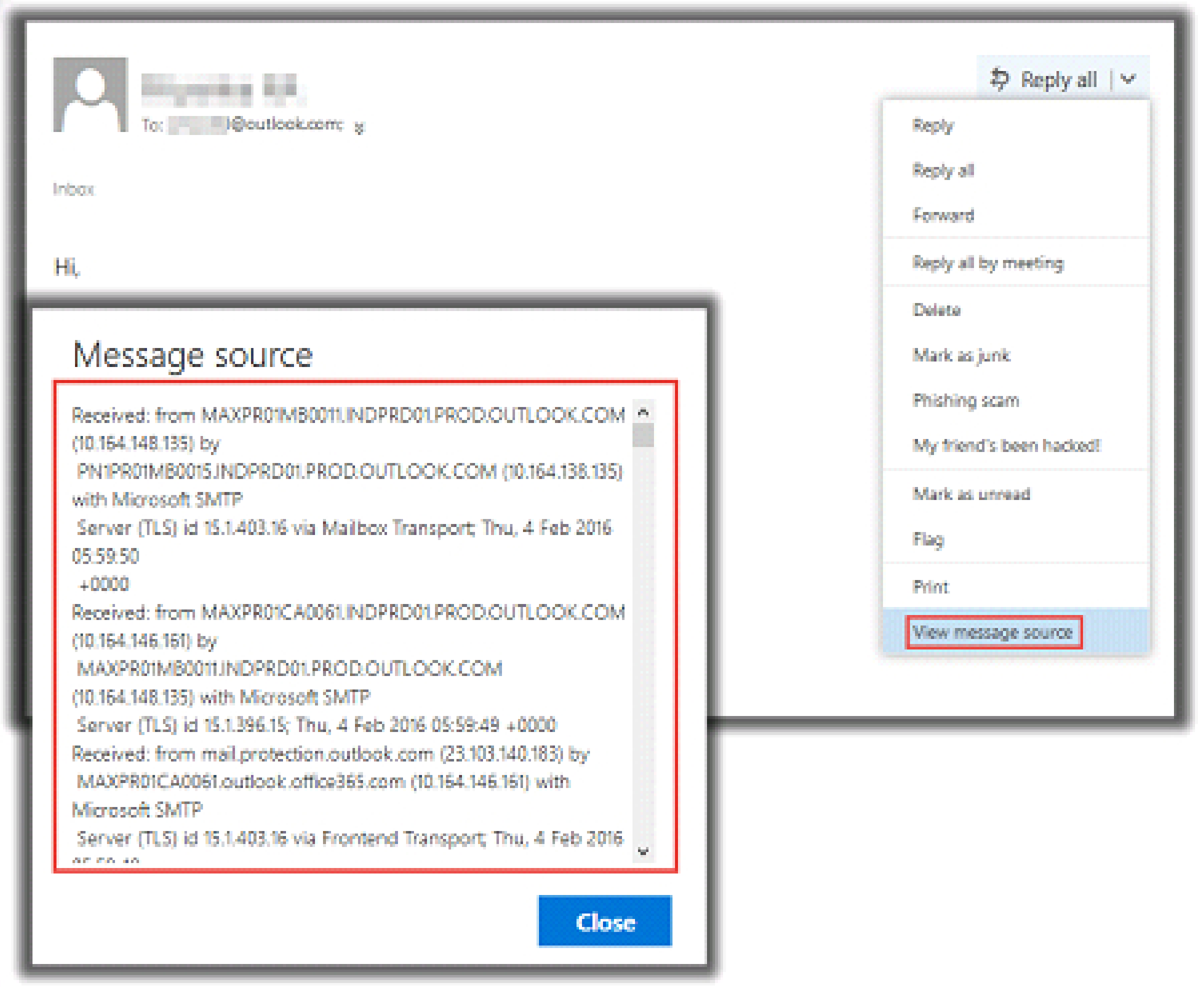
```
Internet headers:  Delivered-To: [redacted]vs@gmail.com
                   Received: by 10.194.103.227 with SMTP id fo3csp840155wjb;
                           Sun, 26 Jul 2015 04:57:08 -0700 (PDT)
                   X-Received: by 10.66.139.138 with SMTP id
                   cy10mr55950569pab.30.1437911827646;
                           Sun, 26 Jul 2015 04:57:07 -0700 (PDT)
                   Return-Path: <[redacted]ly@smartdraw.com>
```

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



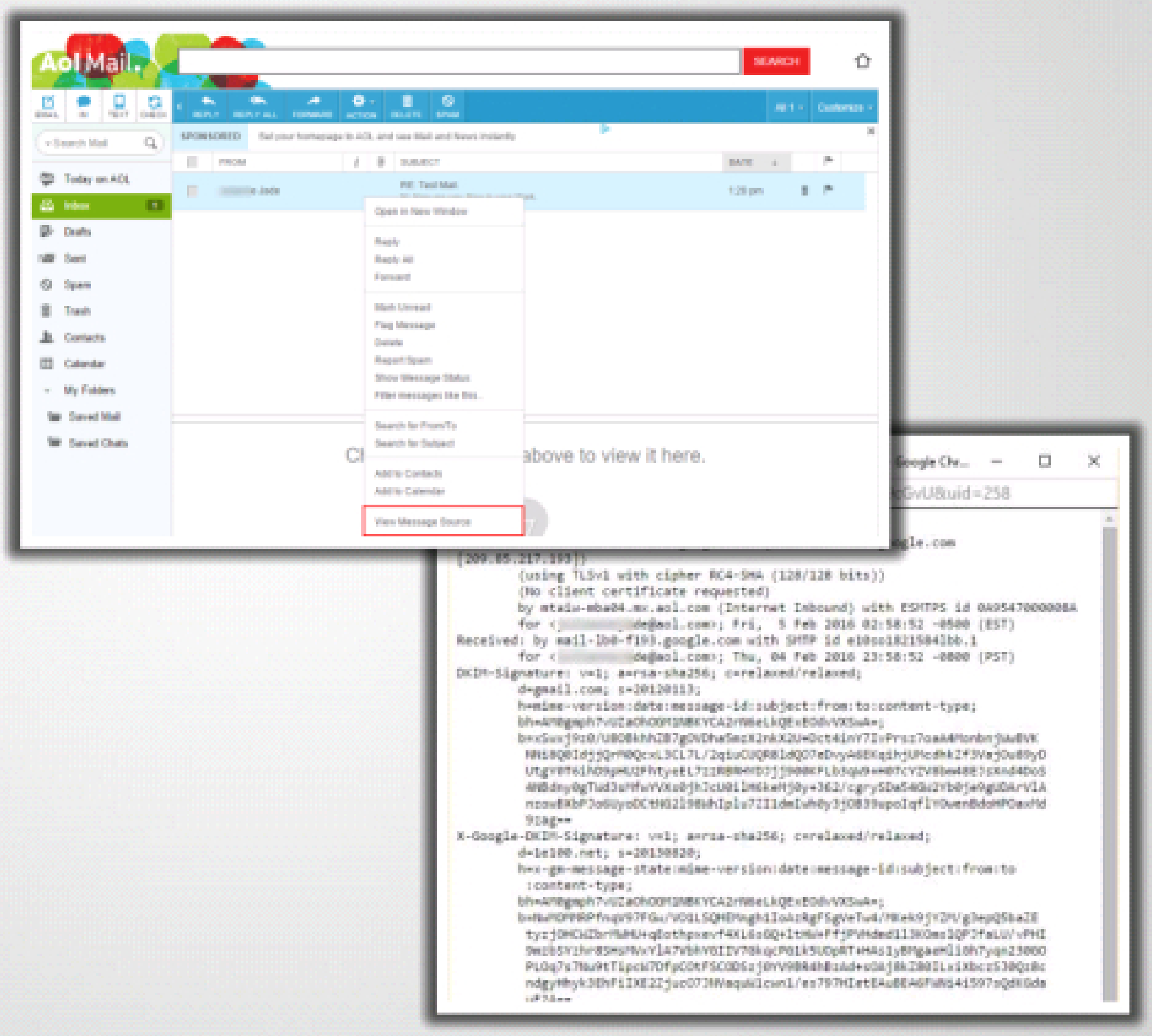
[redacted]
To: [redacted]@outlook.com

Message source

```
Received: from MAXPR01MB0011.INDPRD01.PROD.OUTLOOK.COM
(10.164.148.135) by
 PN1PR01MB0015.INDPRD01.PROD.OUTLOOK.COM (10.164.138.135)
with Microsoft SMTP
 Server (TLS) id 15.1.403.16 via Mailbox Transport; Thu, 4 Feb 2016
05:59:50
 +0000
Received: from MAXPR01CA0061.INDPRD01.PROD.OUTLOOK.COM
(10.164.146.161) by
 MAXPR01MB0011.INDPRD01.PROD.OUTLOOK.COM
(10.164.148.135) with Microsoft SMTP
 Server (TLS) id 15.1.396.15; Thu, 4 Feb 2016 05:59:49 +0000
Received: from mail.protection.outlook.com (23.103.140.183) by
 MAXPR01CA0061.outlook.office365.com (10.164.146.161) with
Microsoft SMTP
 Server (TLS) id 15.1.403.16 via Frontend Transport; Thu, 4 Feb 2016
```

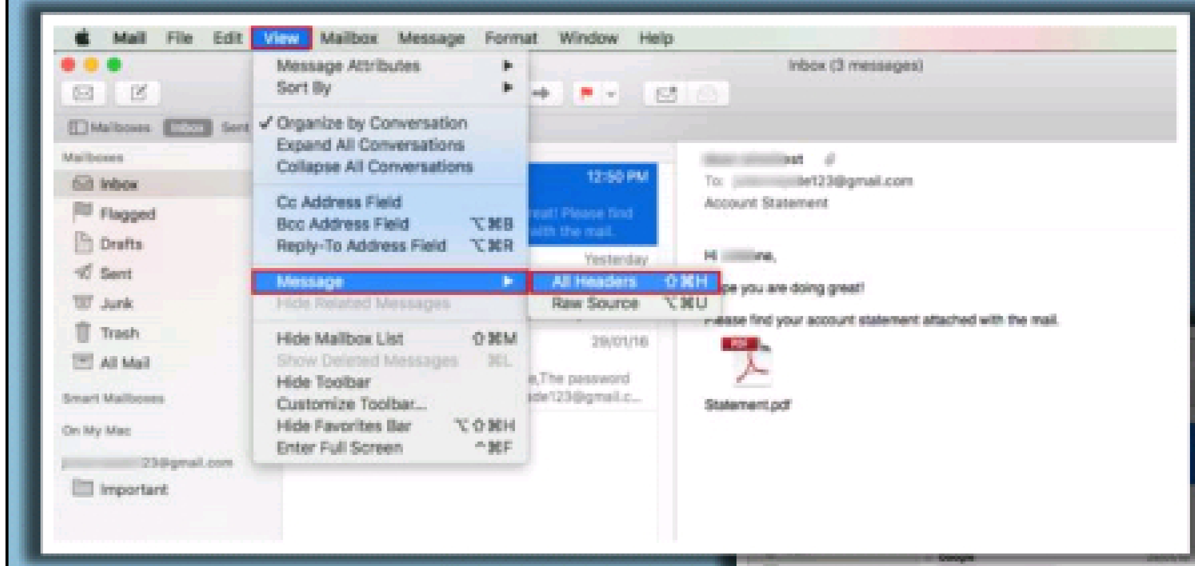
Viewing the E-mail Headers in AOL

- 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



```
[209.85.217.193])
        (using TLSv1 with cipher RC4-SHA (128/128 bits))
        (No client certificate requested)
        by mtaiw-mba04.mx.aol.com (Internet Inbound) with ESMTPS id 0A9547000008A
        for <[redacted]de@aol.com>; Fri,  5 Feb 2016 02:58:52 -0500 (EST)
Received: by mail-lb0-f193.google.com with SMTP id e10so1821584lbb.1
        for <[redacted]de@aol.com>; Thu, 04 Feb 2016 23:58:52 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20120113;
        h=mime-version:date:message-id:subject:from:to:content-type;
        bh=[illegible]
        b=[illegible]
         9iag==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20130820;
        h=x-gm-message-state:mime-version:date:message-id:subject:from:to
         :content-type;
        bh=[illegible]
        b=[illegible]
```

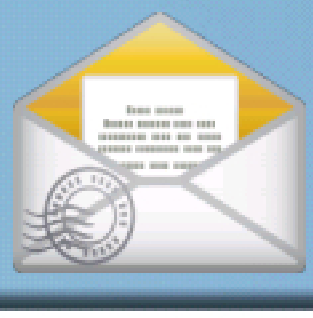
Viewing the E-mail Headers in Apple Mail

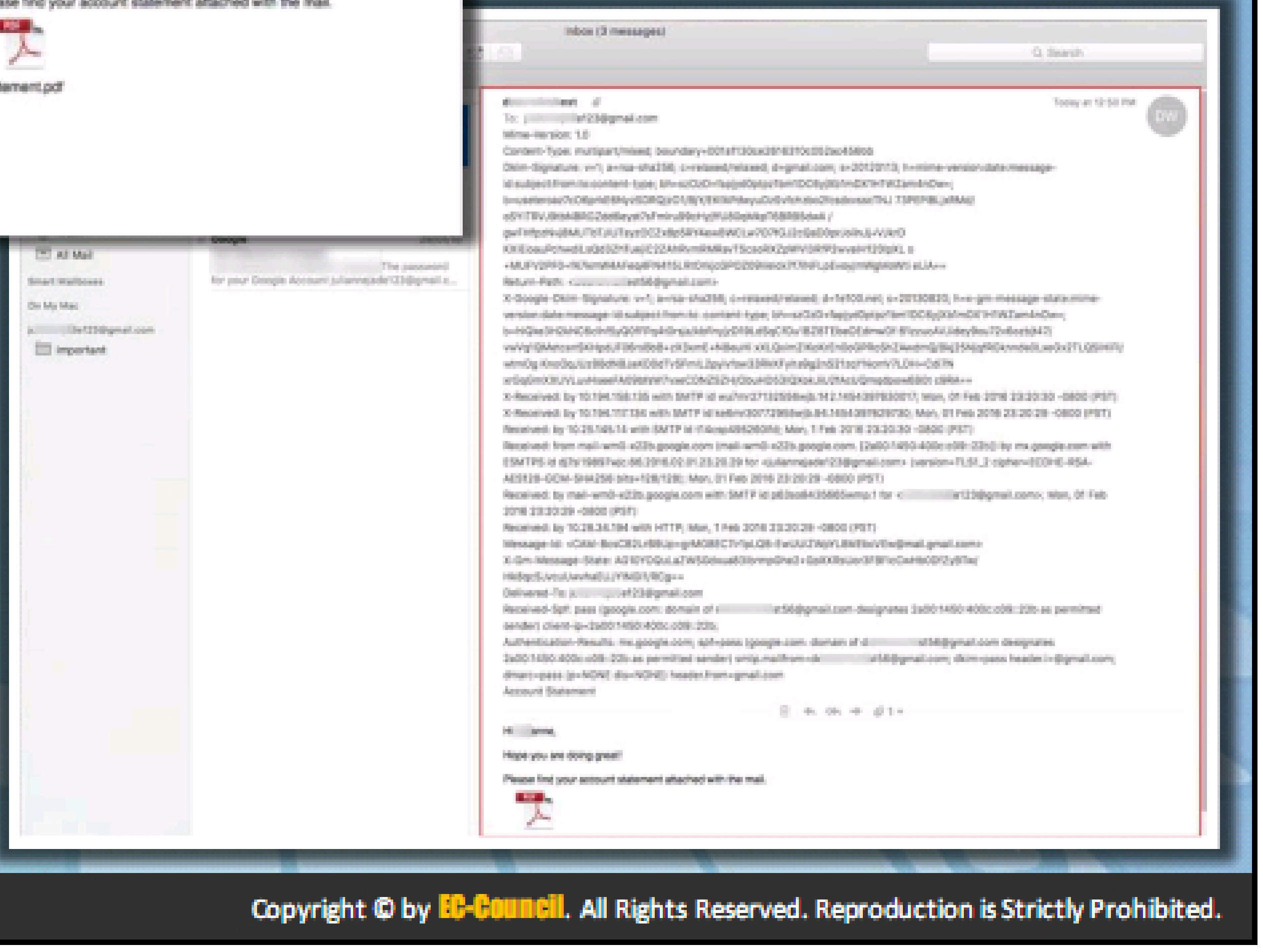


Hi [redacted]ne,

Hope you are doing great!

Please find your account statement attached with the mail.





To: [redacted]e123@gmail.com
Mime-Version: 1.0
Return-Path: <[redacted]st56@gmail.com>
Delivered-To: [redacted]e123@gmail.com
Account Statement

Hi [redacted]nne,

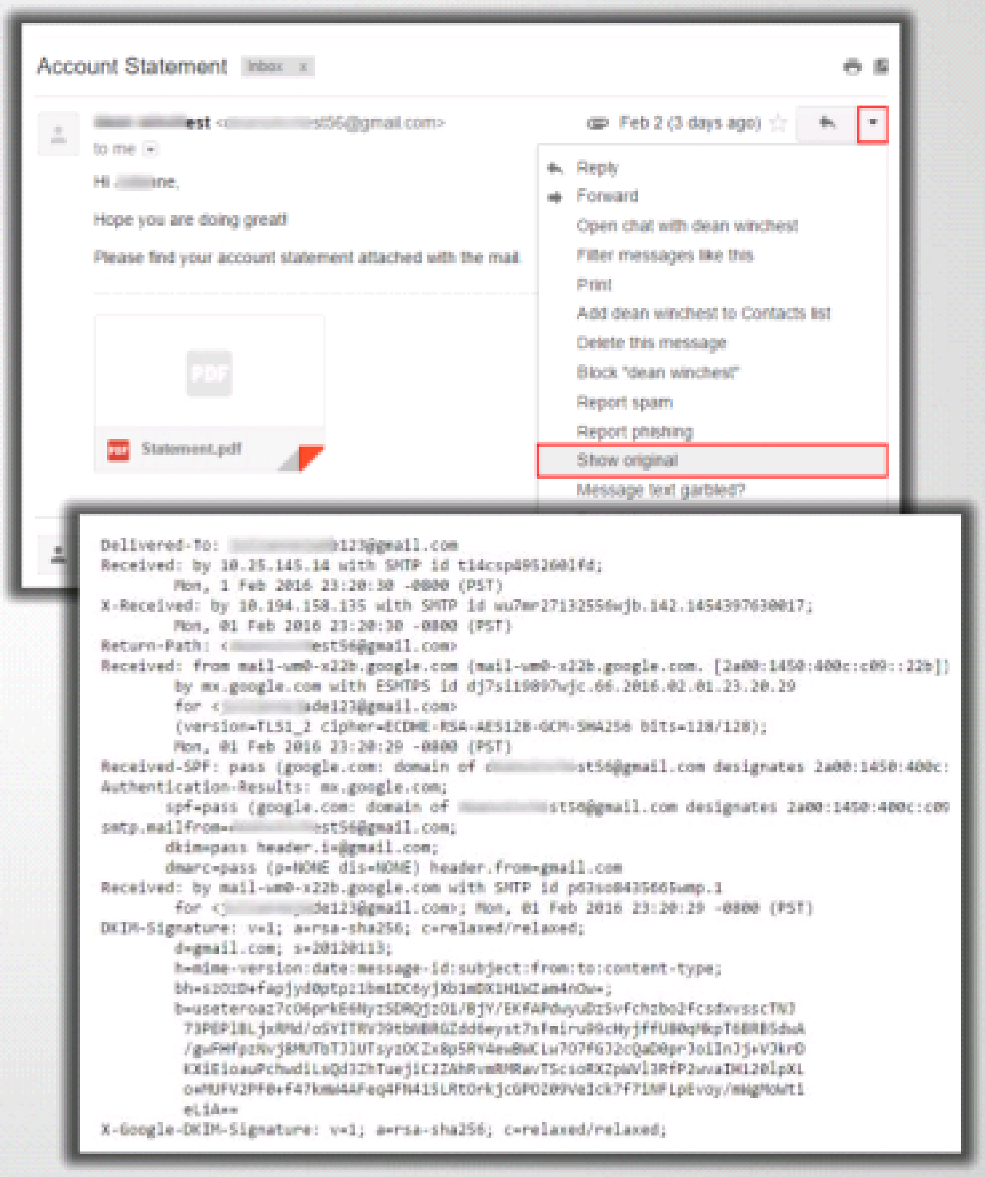
Hope you are doing great!

Please find your account statement attached with the 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



Hi [redacted]ne,

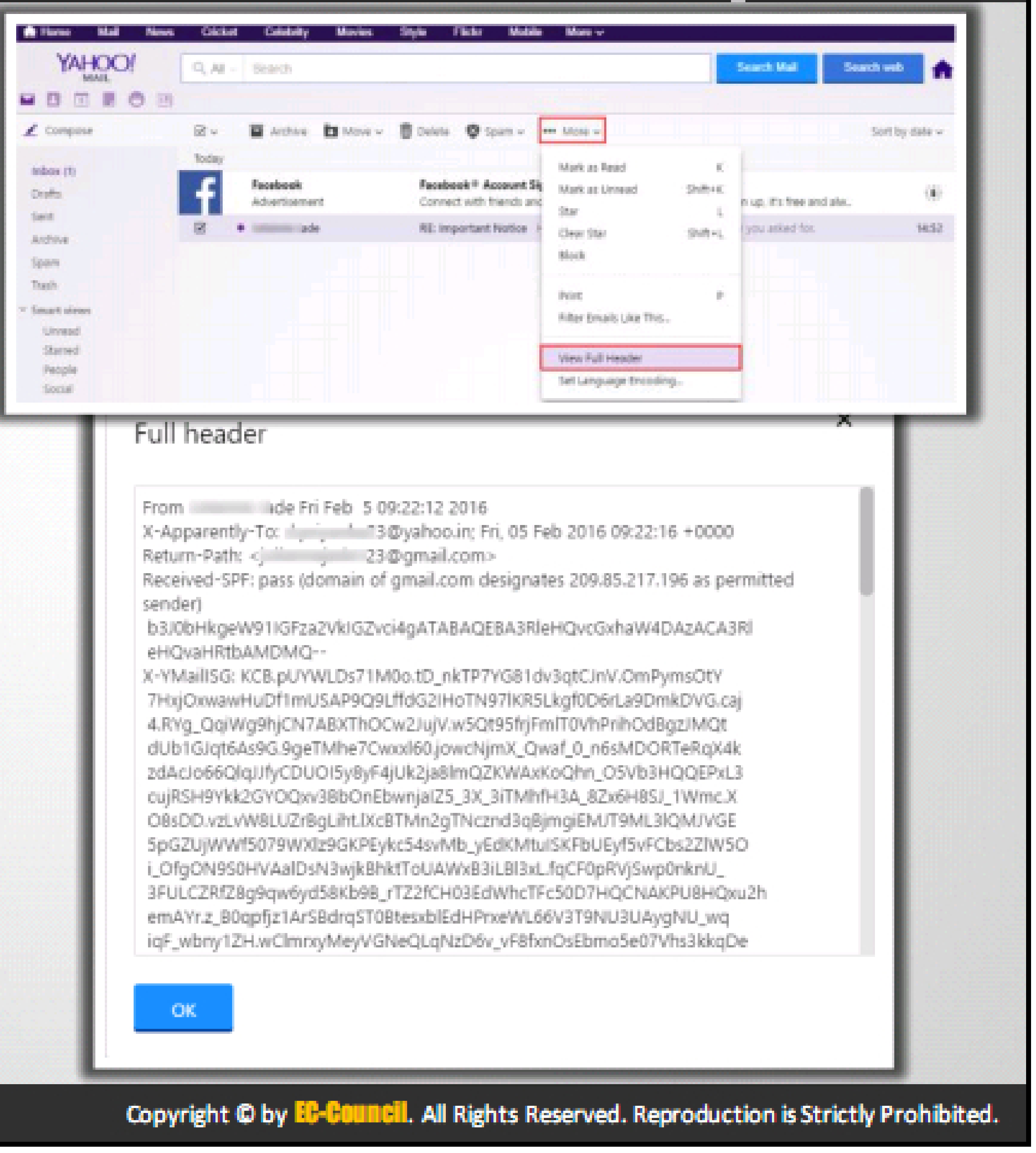
Hope you are doing great!

Please find your account statement attached with the mail.

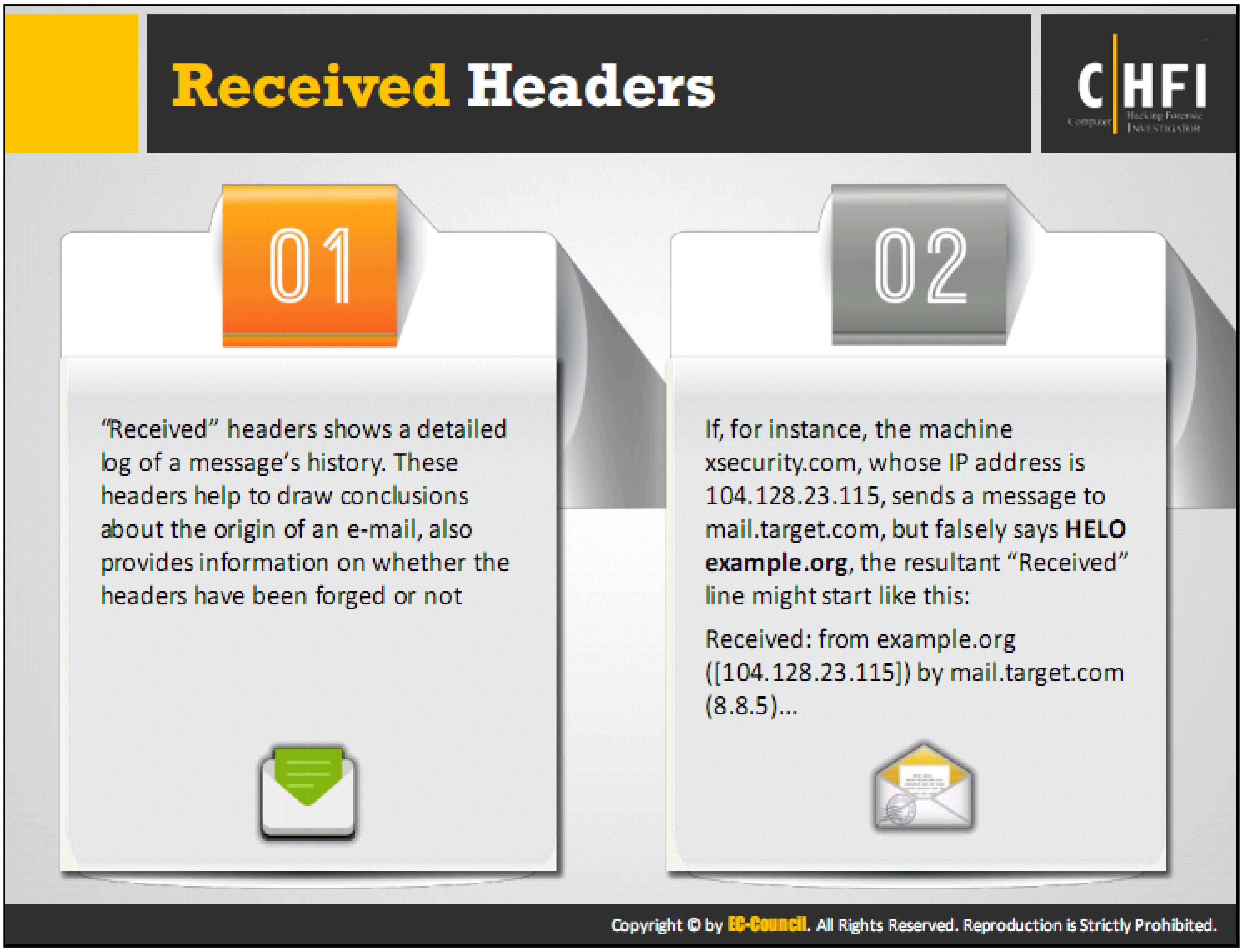
```
Delivered-To: [redacted]123@gmail.com
Received: by 10.25.145.14 with SMTP id t14csp4952601fd;
        Mon, 1 Feb 2016 23:20:30 -0800 (PST)
X-Received: by 10.194.158.135 with SMTP id wu7mr27132556wjb.142.1454397630017;
        Mon, 01 Feb 2016 23:20:30 -0800 (PST)
Return-Path: <[redacted]est56@gmail.com>
Received: from mail-wm0-x22b.google.com (mail-wm0-x22b.google.com. [2a00:1450:400c:c09::22b])
        by mx.google.com with ESMTPS id dj7si119897wjc.66.2016.02.01.23.20.29
        for <[redacted]ade123@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Mon, 01 Feb 2016 23:20:29 -0800 (PST)
Received-SPF: pass (google.com: domain of [redacted]st56@gmail.com designates 2a00:1450:400c:
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of [redacted]st56@gmail.com designates 2a00:1450:400c:c09
smtp.mailfrom=[redacted]est56@gmail.com;
       dkim=pass header.i=@gmail.com;
       dmarc=pass (p=NONE dis=NONE) header.from=gmail.com
Received: by mail-wm0-x22b.google.com with SMTP id p63so8435665wmp.1
        for <[redacted]de123@gmail.com>; Mon, 01 Feb 2016 23:20:29 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20120113;
        h=mime-version:date:message-id:subject:from:to:content-type;
        bh=s2O1D+fapjyd0ptp21bm1DC6yjXb1mDX1H1WZam4nOw=;
        b=useteroaz7cO6prkE6Nyz5DRQjz01/BjY/EKfAPdwyuDz5vfchzbo2fcsdxvsscTN3
         73PEP18LjxRMd/oSYITRV39tbNBRGZdd6eyst7sFmiru99cHyjffU80qMkpT6BRBSdwA
         /gwFHfpzNvj8MUTbTJ1UTsyzOCZx8p5RY4ewBWCLw707fGJ2cQaD0prJolInJj+VJkrD
         KXiEioauPchwdiLsQd3ZhTuejiC2ZAhRvmRMRavTScsoRXZpWVl3RfP2wvaIH120lpXL
         o+MUFV2PF0+F47kmW4AFeq4FN415LRtOrkjcGPO209VeIck7F71NFLpEvoy/mWgMoWt1
         eLiA==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
```

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



```
From [redacted]ade Fri Feb  5 09:22:12 2016
X-Apparently-To: [redacted]3@yahoo.in; Fri, 05 Feb 2016 09:22:16 +0000
Return-Path: <[redacted]23@gmail.com>
Received-SPF: pass (domain of gmail.com designates 209.85.217.196 as permitted
sender)
 b3J0bHkgeW91IGFza2VkIGZvci4gATABAQEBA3RleHQvcGxhaW4DAzACA3Rl
 eHQvaHRtbAMDMQ--
X-YMailISG: KCB.pUYWLDs71M0o.tD_nkTP7YG81dv3qtCJnV.OmPymsOtY
 7HxjOxwawHuDf1mUSAP9Q9LffdG2IHoTN97lKR5Lkgf0D6rLa9DmkDVG.caj
 4.RYg_QqiWg9hjCN7ABXThOCw2JujV.w5Qt95frjFmlT0VhPrihOdBgzJMQt
 dUb1GJqt6As9G.9geTMhe7Cwxxl60.jowcNjmX_Qwaf_0_n6sMDORTeRqX4k
 zdAcJo66QlqJJfyCDUOI5y8yF4jUk2ja8lmQZKWAxKoQhn_O5Vb3HQQEPxL3
 cujRSH9Ykk2GYOQxv38bOnEbwnjalZ5_3X_3iTMhfH3A_8Zx6H8SJ_1Wmc.X
 O8sDD.vzLvW8LUZr8gLiht.lXcBTMn2gTNcznd3q8jmgiEMJT9ML3IQMJVGE
 5pGZUjWWf5079WXlz9GKPEykc54svMb_yEdKMtulSKFbUEyf5vFCbs2ZIW5O
 i_OfgON9S0HVAalDsN3wjkBhktToUAWxB3iLBl3xL.fqCF0pRVjSwp0nknU_
 3FULCZRfZ8g9qw6yd58Kb98_rTZ2fCH03EdWhcTFc50D7HQCNAKPU8HQxu2h
 emAYr.z_B0qpfjz1ArSBdrqST0BtesxblEdHPrxeWL66V3T9NU3UAygNU_wq
 iqF_wbny1ZH.wClmnxyMeyVGNeQLqNzD6v_vF8fxnOsEbmo5e07Vhs3kkqDe
```



Received Headers

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)...

Received headers of an email message provide information about the message origin, the route it took to reach the recipient, and the cause of delivery delays. It is important to examine this part of the email header once we identify that the email is spam.

When the SMTP Server receives an email message, a received Header gets added to the email. Therefore, Received Headers are essentially in reverse order; in other words, the last Received Header added is the first one at the top. To understand the Received Headers correctly, read from the bottom (first Received Header) to the top (last Received Header).

Investigators must be aware of the forged headers, which attackers make up to deceive the users, systems, security, etc. and enter the normal traffic.

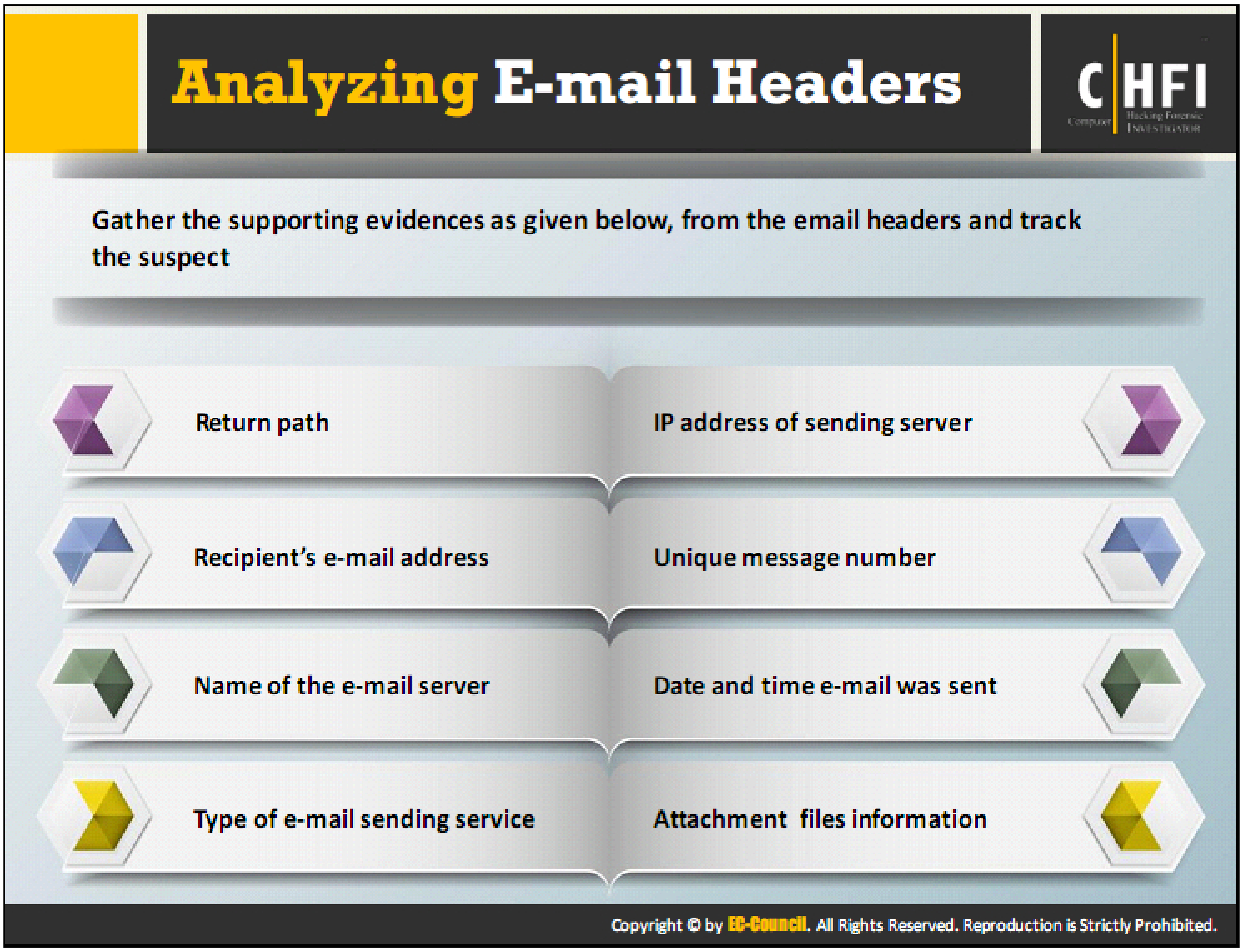
If, for instance, the machine turmeric.com, whose IP address is 104.128.23.115, sends a message to mail bieberdorf.edu but falsely says HELO galangal.org, the resultant "Received" line might start like this:

Received: from galangal.org ([104.128.23.115]) by mail.bieberdorf.edu (8.8.5)...

This means that the e-mail sent from turmeric.com might have "Received" lines that look something like this:

Received: from galangal.org ([104.128.23.115]) by mail.bieberdorf.edu (8.8.5)...

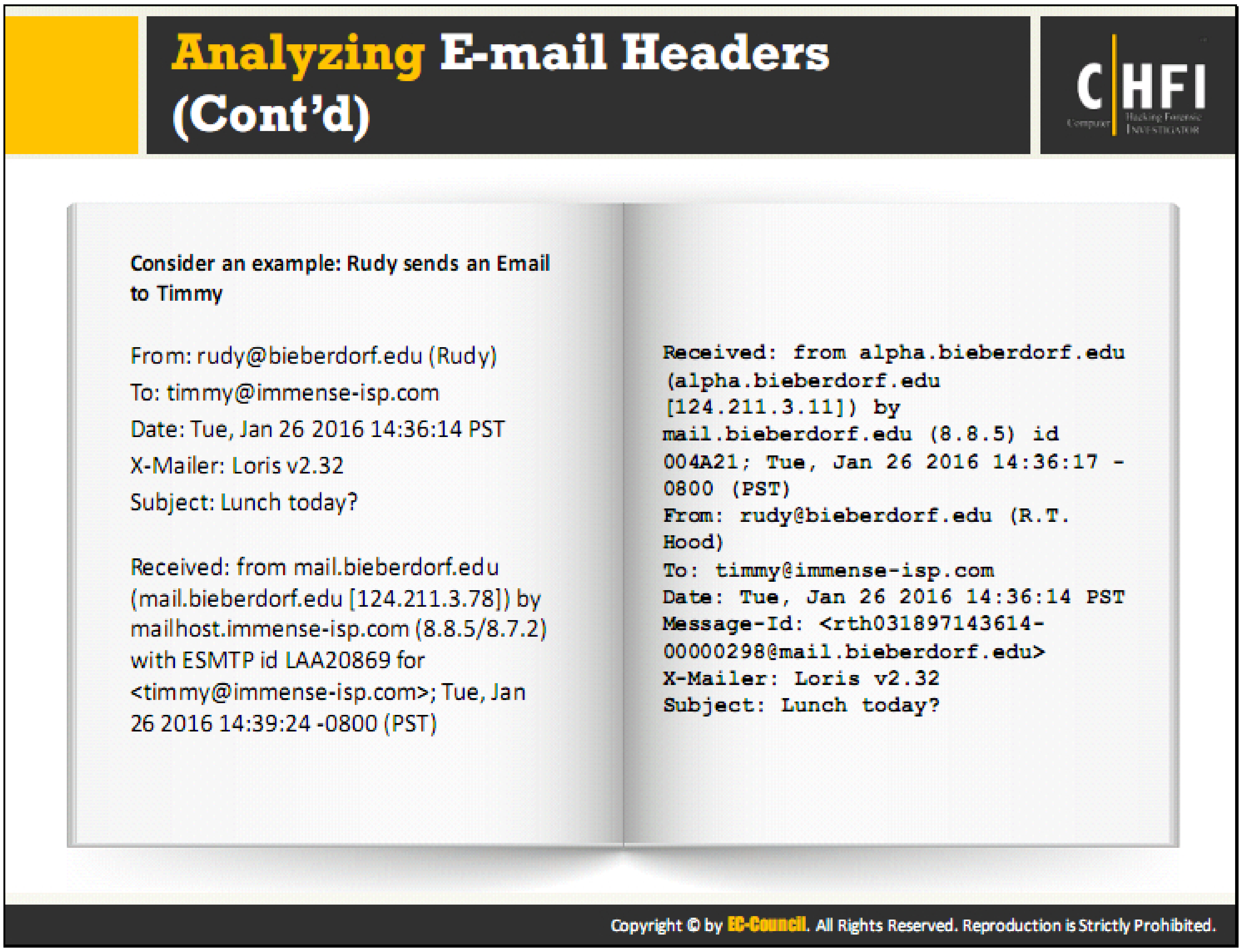
Received: from nowhere by outer space (8.8.3/8.7.2)...



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)

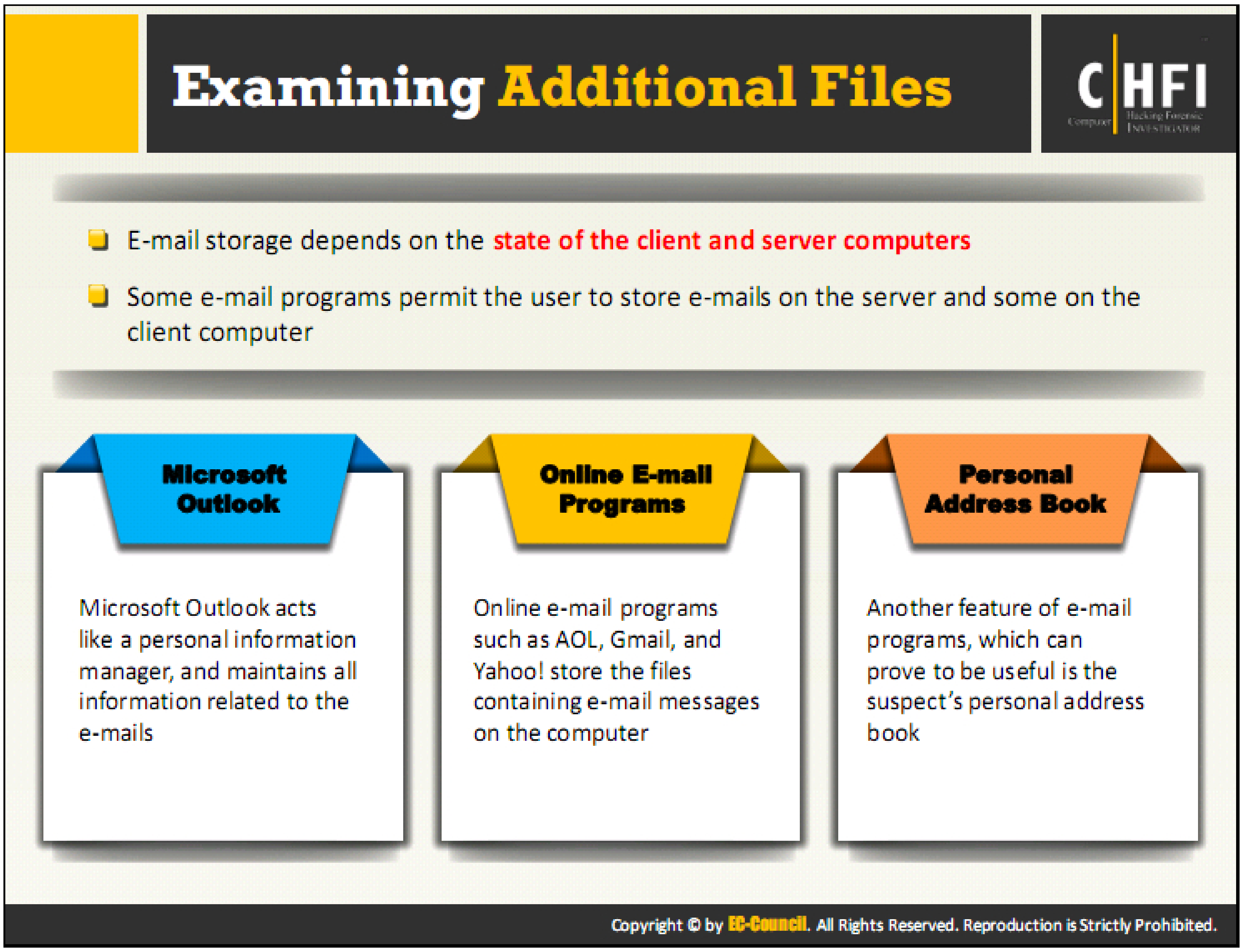
```
Received: from alpha.bieberdorf.edu
(alpha.bieberdorf.edu
[124.211.3.11]) by
mail.bieberdorf.edu (8.8.5) id
004A21; Tue, Jan 26 2016 14:36:17 -
0800 (PST)
From: rudy@bieberdorf.edu (R.T.
Hood)
To: timmy@immense-isp.com
Date: Tue, Jan 26 2016 14:36:14 PST
Message-Id: <rth031897143614-
00000298@mail.bieberdorf.edu>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

The investigator can track fraudulent e-mail's originating location by examining the e-mail header. The most valuable information for investigation is the originating e-mail's domain address or an IP address. Other supporting data is the date and time of the message sent, attachment filenames, and the unique message number.

In the above e-mail header, Received: from mail.bieberdorf.edu represents that a machine named mail.bieberdorf.edu sent the mail and bears the IP address 124.211.3.11 by using the Sendmail version 8.8.5 with assigned ID number 004A21.

The rth@bieberdorf.edu, who gives his real name as R.T. Hood, sent the mail to tmh@immense-isp.com with mail ID rth031897143614-00000298@mail.bieberdorf.edu.

This ID does not represent the SMTP and ESMTP ID numbers and is attached to this message for life. The sender used a program called Loris, version 2.32 to send the message.



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

Examining Additional Files

Email storage depends on the state of the client and server computers. Some email programs permit you to store email on a server, and some on the client computer. Various email clients, for example, Microsoft Outlook, allow the user to save all their email messages in a separate folder, which can later be accessed from anywhere without logging on to the user's email client.

Microsoft Outlook

Microsoft Outlook Mail acts like a personal information manager, maintaining the information related to email in the proper format. Microsoft Outlook gives the users the advantage of saving all their email messages in two different file locations:

- Personal email file (.pst)
- Offline email file (.ost)

The client stores these files in different folders such as History, Cookies, Temp, Cache, and the Temporary Internet folder. Investigators should use forensic tools to retrieve the folder for the respective email client and then extract the files to find supportive information. Sometimes, the data is not in readable format. In that case, the programs required to read the data should be downloaded. For example, a cookie reader can help to read the cookies.

Online E-mail Programs:

Online e-mail programs such as AOL, Gmail, and Yahoo! leave the files containing e-mail messages on the computer. They store the files in different folders such as History, Cookies, Temp, Cache, and Temporary Internet Folder. Investigators can use forensic tools to retrieve the folder for the respective e-mail client in order to find information about the suspect e-mails.

Personal Address book:

Another useful feature of the email program is the personal address book. A suspect's personal address book can become supporting evidence, which can indicate the suspect's involvement in the crime.

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

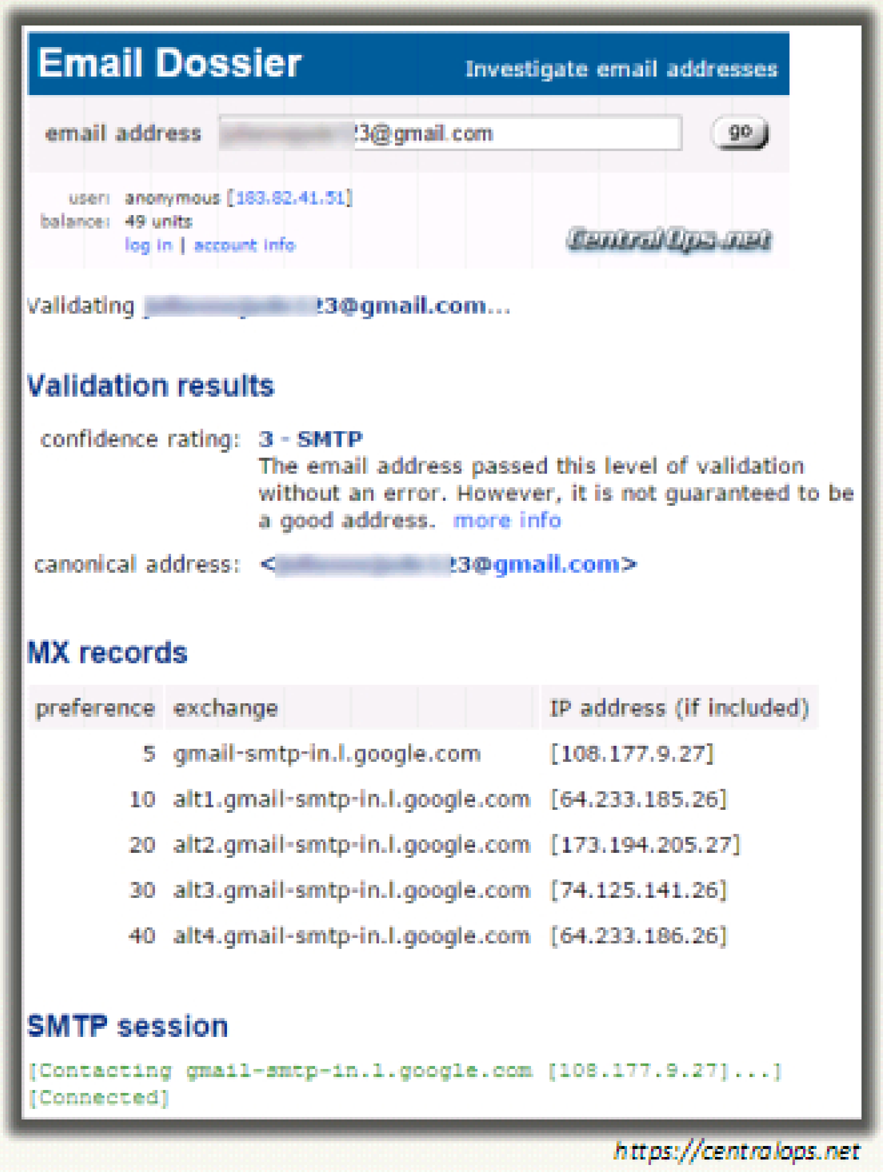
Other tools to check e-mail validity:

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

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

A valid email address is the one to which we can send or receive emails. There are particular standards and guidelines for validating email addresses.

Email Address Verifier

Source: *https://tools.verifyemailaddress.io*

This email address verification technology connects to mailboxes to check whether an email address exists or not.

Email Checker

Source: *http://email-checker.net*

Email Checker is a simple tool for verifying an email address. It's free and quite easy to use. Just enter the email address and hit check button. Then it tells you whether the email address is real or not. It extracts the MX records from the email address and connect to mail server (over SMTP and also simulates sending a message) to make sure the mailbox really exist for that user/address.

G-Lock Software Email Verifier

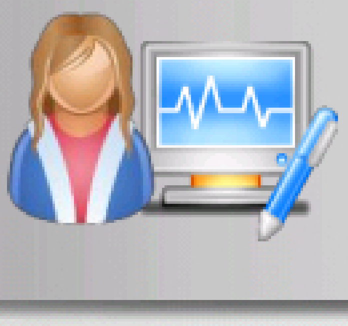
Source: *http://www.glocksoft.com*

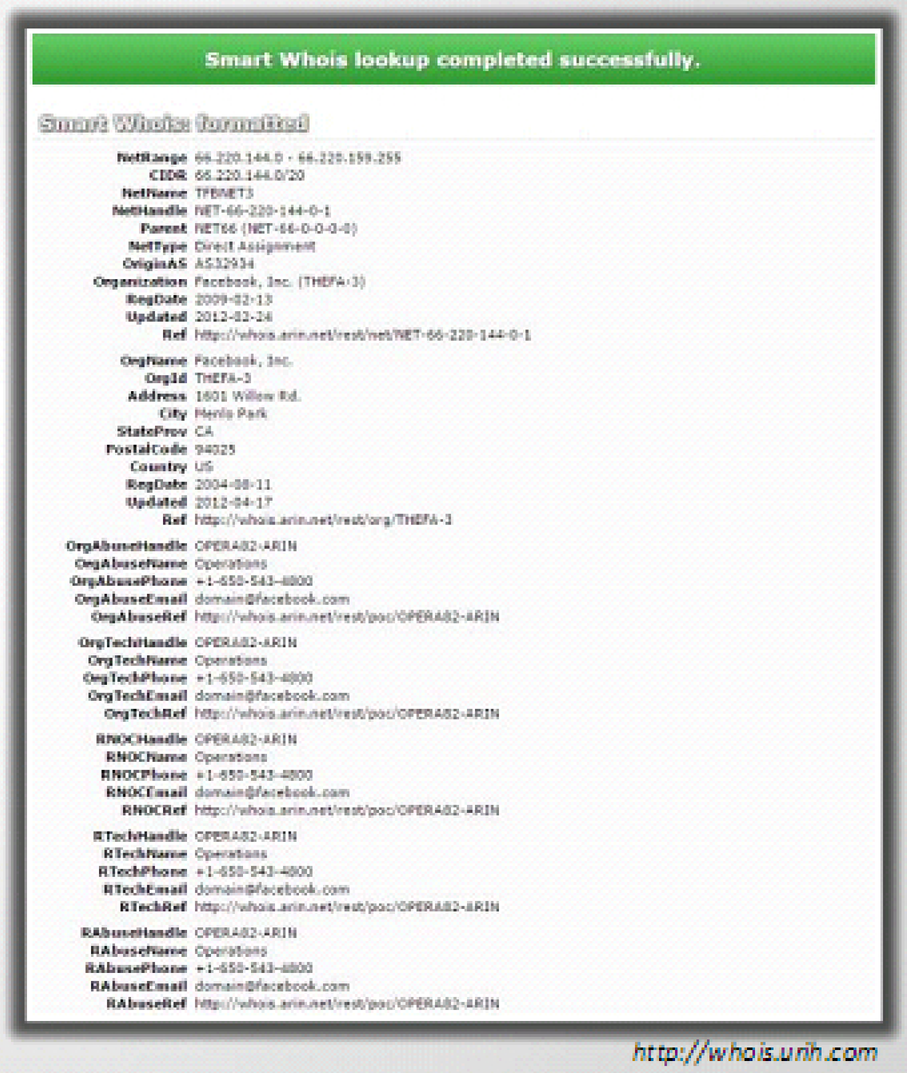
G-Lock SoftwareE-mail Verifier will check every email address from a database or a mailing list and determine if the e-mails are still valid.

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.

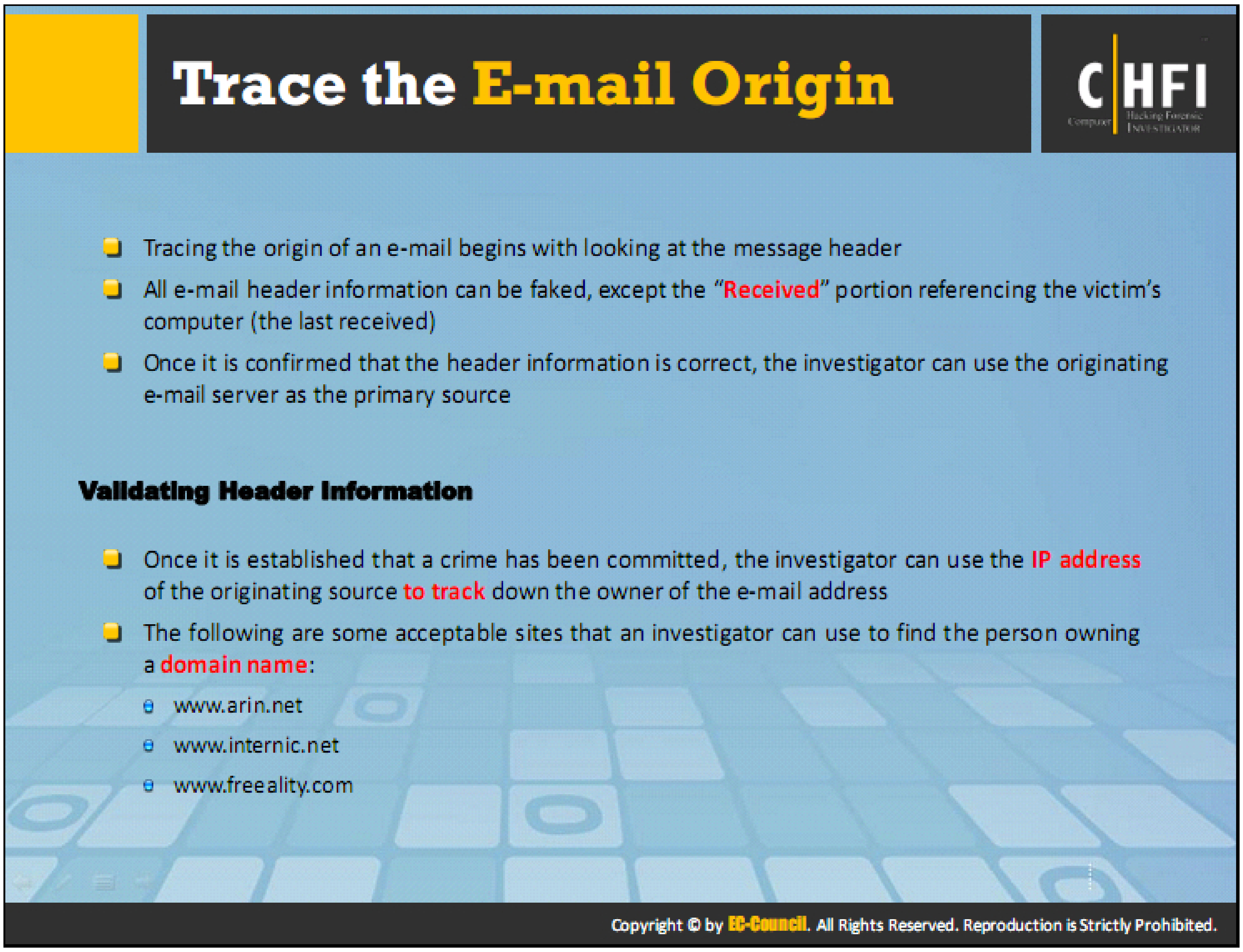
Smart Whois: formatted

```
      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.arin.com

The following steps are involved in the process of examining the originating IP address using the Trace Email Analyzer tool:

1. Open the email to trace and find its header.
2. Copy the header and paste it in the box space in the Trace Email Analyzer tool webpage.
3. Press the "Get Source" icon.
4. Scroll down below the webpage to find a box containing the Trace Email results.



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

E-mail origin refers to the details of the source used to send the email. It includes the IP address, mail server, username, domain name, etc. These details will help the investigators in tracing the perpetrator or sender of an email as well as understanding their motive behind the attack. To achieve this, the investigators need to further examine the email message header with one of the free Internet tools.

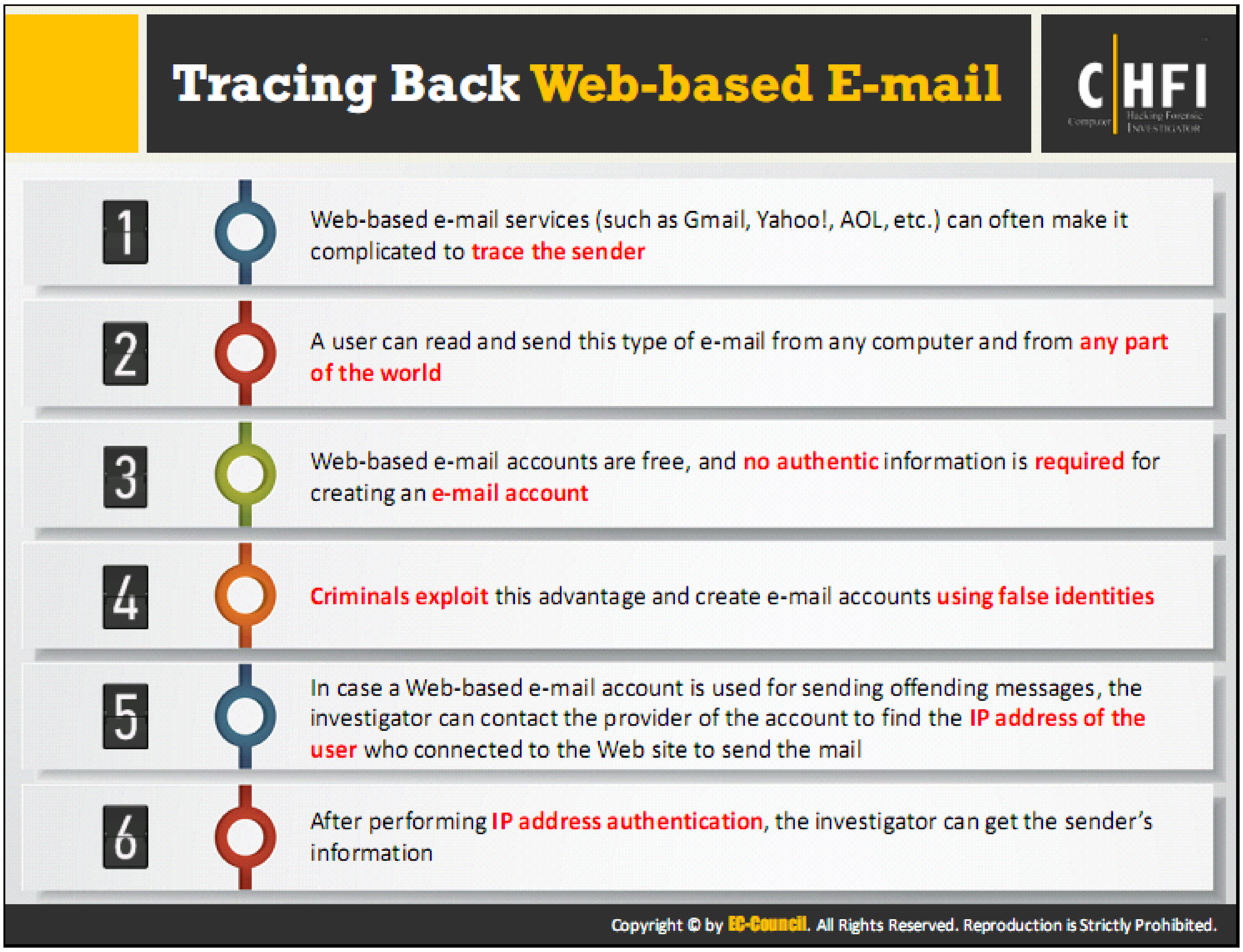
Validating Header Information

Tracing back email begins by looking at the message header information. The header has a subject, date, and the "From"/"Received" address. The "From" line contains the source of the email, and "Received" indicates every point the email passed through, along with the date and time. Attackers can fake all email header information except the "Received" portion referencing the victim's computer (the last received).

Once the investigators confirm that the header information is correct, they can use the originating email server as the primary source to trace back. The investigators can approach the court and get a court order served by law enforcement or a civil complaint filed by attorneys. The court order helps to obtain the log files from the server in order to determine the sender. After getting the contact information about the suspect, they can take punitive steps against the suspect.

The investigators may use the following registry sites to determine the Email origin:

- www.arin.net**:** It employs the American Registry for Internet Numbers (ARIN) to match the domain name for an IP address. It also provides the point of contact for the domain name.
- www.internic.com**:** It provides the identical information given by www.arin.net.
- www.freeality.com**:** This site provides the various options for searching such as email address, phone numbers, and names. One can do a reverse email search, which could reveal the subject's real name. This site can do other searches such as reverse phone number searches and address searches.



Tracing Back Web-based E-mail

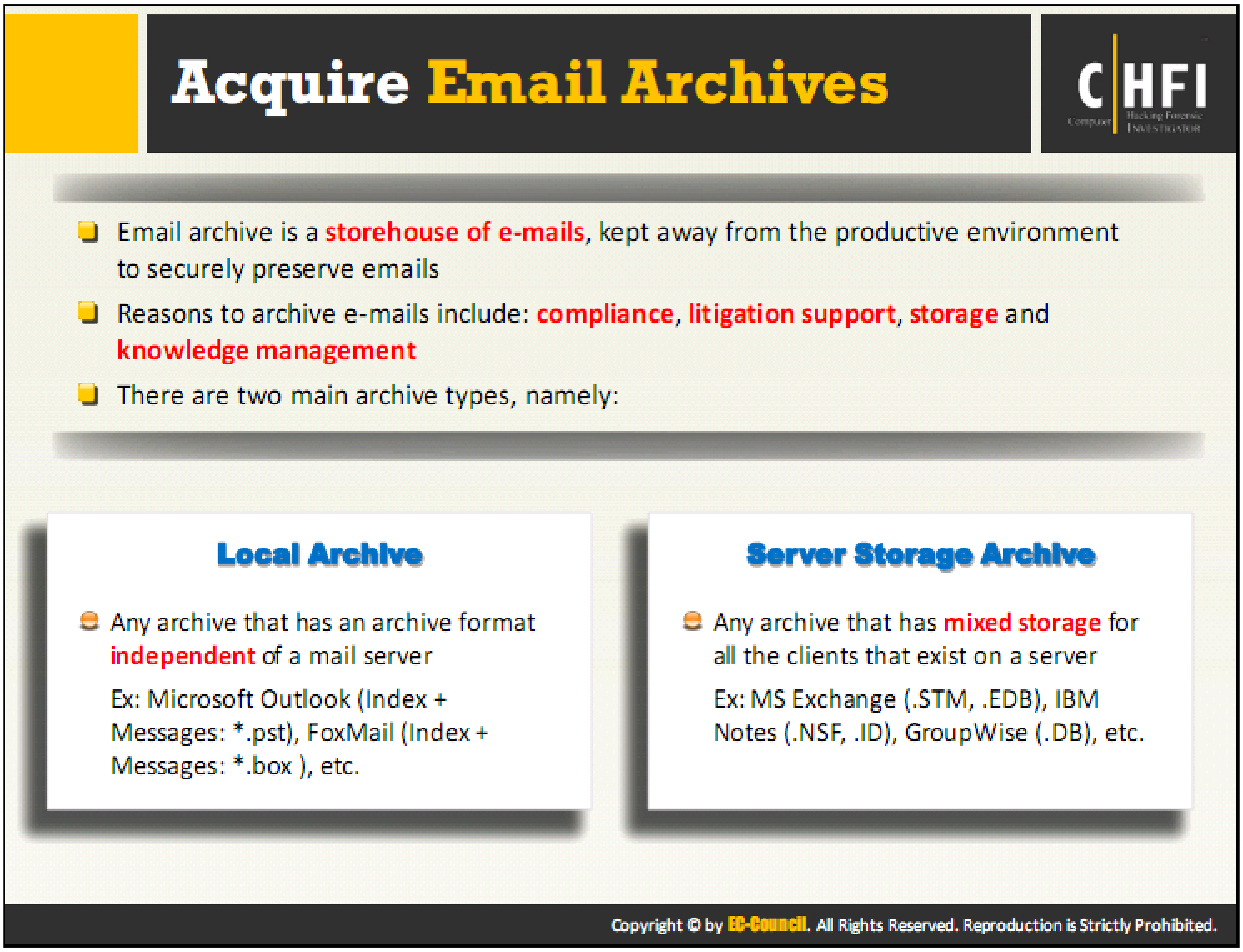
1. Web-based e-mail services (such as Gmail, Yahoo!, AOL, etc.) can often make it complicated to **trace the sender**
2. A user can read and send this type of e-mail from any computer and from **any part of the world**
3. Web-based e-mail accounts are free, and **no authentic** information is **required** 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

There are two ways to transmit an email over the Internet. One is by using the email program installed on the machine, and the other is an email service on the web.

Email programs such as Eudora and Outlook require configuration with the ISP, and if one wants to use the email program on another computer, he or she has to first install the email program on that computer. Tracing a suspect becomes far easier in this case.

On the other hand, if one is using web-based email, then it becomes difficult to trace the sender. One can read and send the email from any computer and from any part of the world. These web-based emails are free, and no authentic information is required for creating an email account. The criminals exploit this advantage and make fake email accounts with false details.

When the attacker sends offending messages through a web-based email account, the investigator can use a unique IP address to find the suspect. The online websites such as Yahoo!, Hotmail, etc. maintain the IP address of each machine accessing their email services. After IP address authentication, the examiner can contact an email provider to 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.

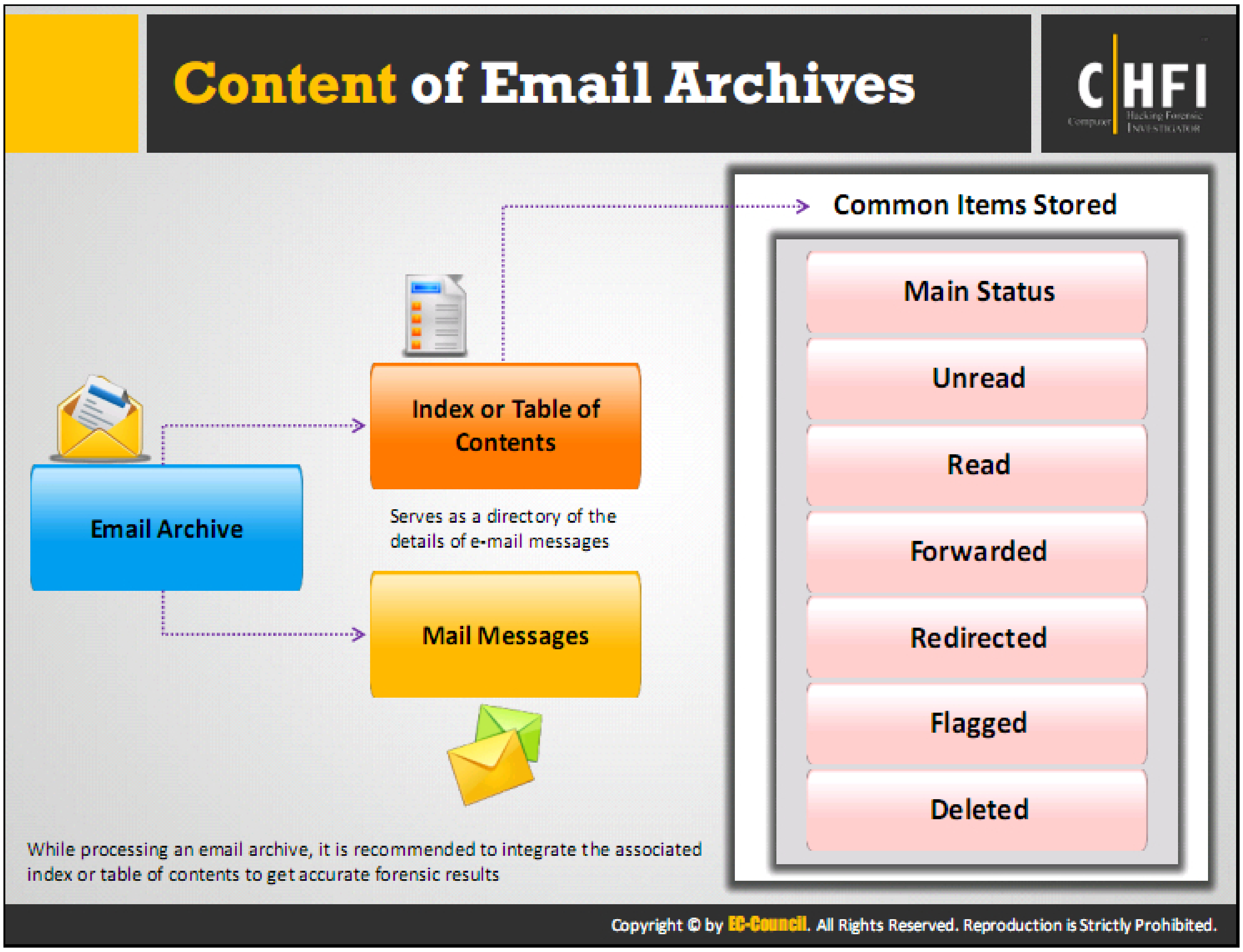
Server Storage Archive

- 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.

Email archiving is an organized method to save and protect email messages so as to be able to quickly access them at a later date. IT managers can manage large email archives using the policy-based email archiving software applications; archiving also frees up space on production servers and speeds up backup times. A lifecycle management component, which uses rules set up by the administrator, verifies all the emails coming into the company. This identifies all the email messages in the archive and moves the messages to the storage media.

Email archives store the received and sent emails, contacts, attachments, and other email client related data, and store them on the system hard drive. Investigators should check for the presence of such archives across the system and extract them. These archives should be analyzed to find the email trends and determine if it can provide any evidential artifacts.



Content of Email Archives

Email Archive

Index or Table of Contents

Serves as a directory of the details of e-mail messages

Mail Messages

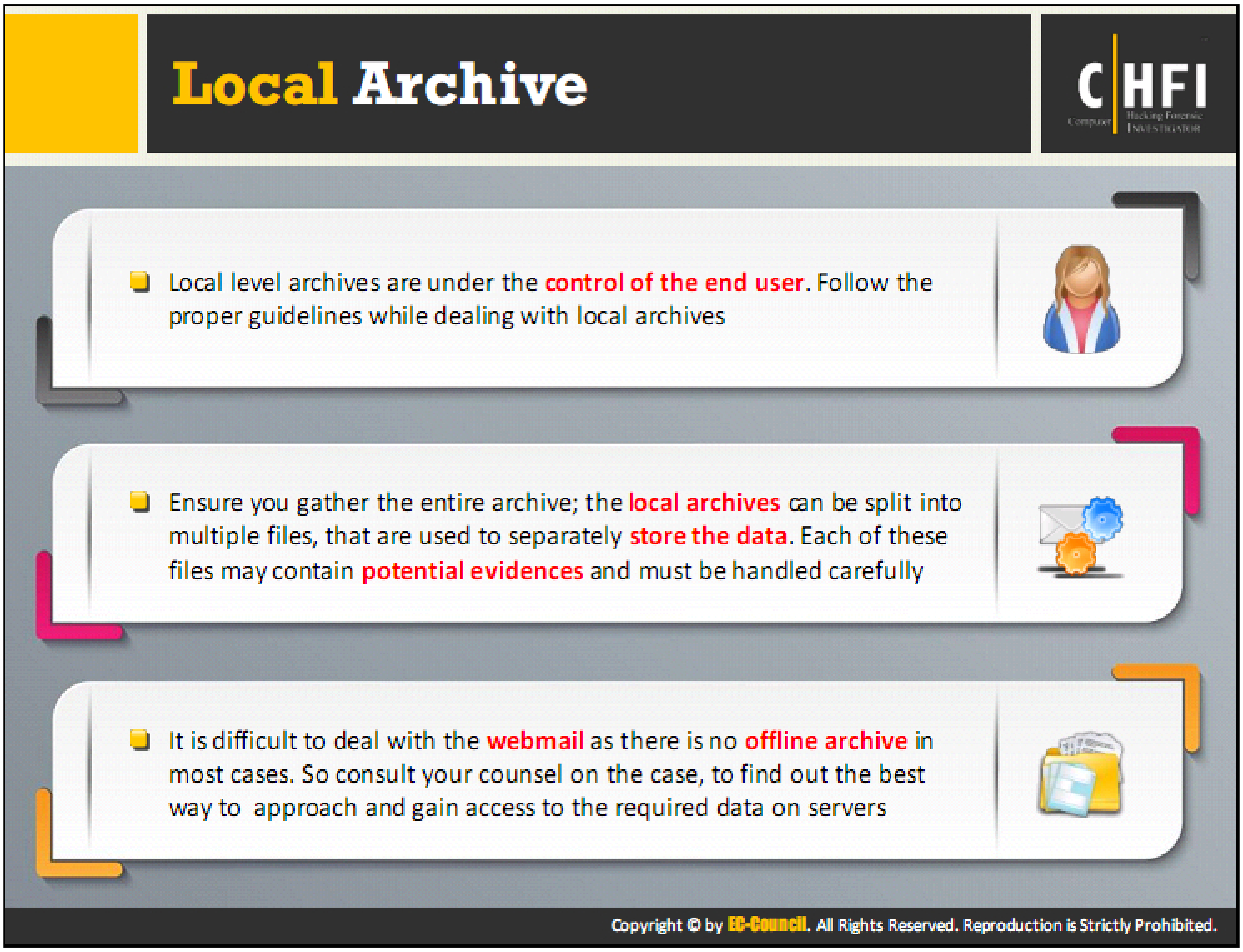
Common Items Stored

- Main Status
- Unread
- Read
- Forwarded
- Redirected
- Flagged
- Deleted

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

There are a few other files included in an email archive called the table of contents files. These files act as a directory of the details of the email message. To receive proper forensic results, it should be ensured that the email is associated with its table of contents or index file while processing an email archive. Following are the common items that are stored in the table of contents or index files:

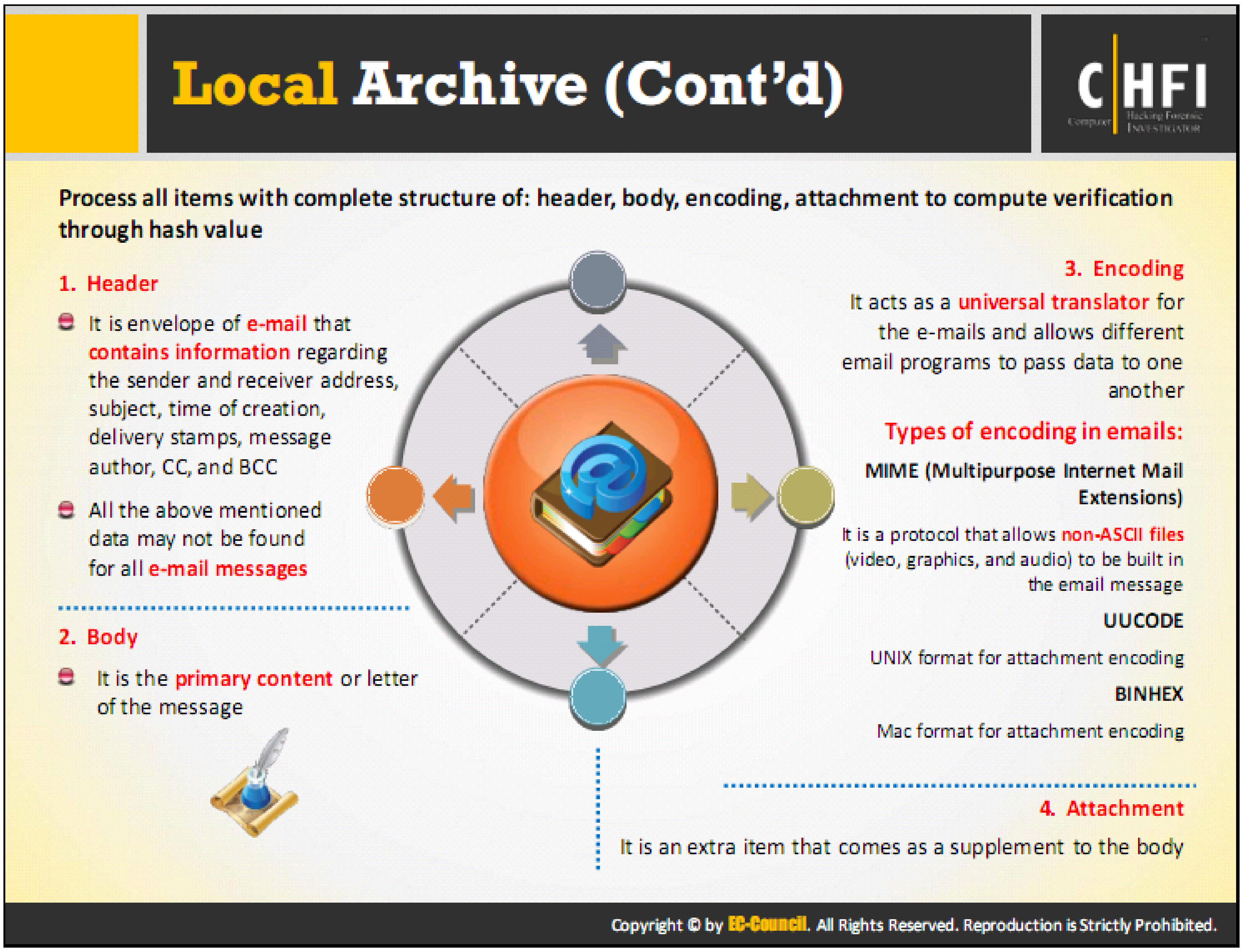
- Main status
- unread and read
- Forwarded
- Redirected
- Flagged
- Deleted



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

Unlike a server storage archive where the server end deals with the archives, the end user on the local computer deals with the local archive.



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

A proper email message always consists of a header, body, and encoding, which are placed together in a single archive. Attachments are also a part of an email archive.

Types of encoding in emails

MIME

It is an Internet standard that extends the email format for supporting the following:

- Text in non-ASCII character sets
- Attachments like application programs, images, audio, video, etc. other than text
- Multiple part message bodies
- Non-ASCII character set header information

Uuencode

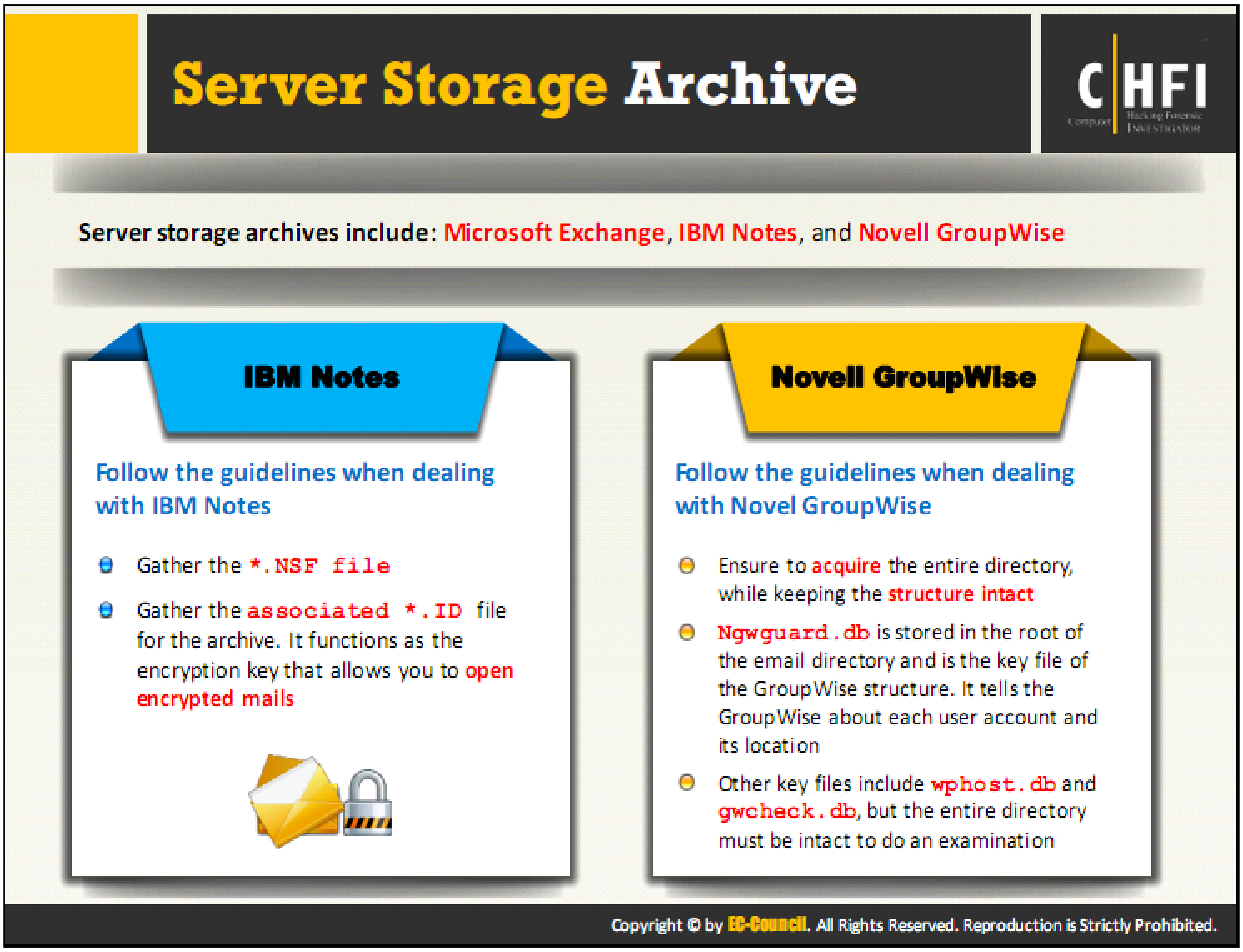
Uuencode, also known as UNIX-to-UNIX encoding or Uuencode/Uudecode, is a utility for encoding and decoding files shared between users or systems using the UNIX operating systems. It is also available for all other operating systems, and many e-mail applications offer it as an encoding alternative, especially for e-mail attachments. While sending e-mails with attachments, if the recipient(s) do not have an MIME-compliant system, the Uuencode should be used to send the attachment as an e-mail note.

BinHex

BinHex is the short form for "binary-to-hexadecimal." It is a binary-to-text encoding system used on Mac OS to send binary files via e-mails. This system is similar to Uuencode, but BinHex combines both "forks" of the Mac file system including extended file information.

Attachment

Attachments are additional items added to the email. For analysis of attachments, use separate tools that understand various file types sent as attachments.



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

IBM Notes

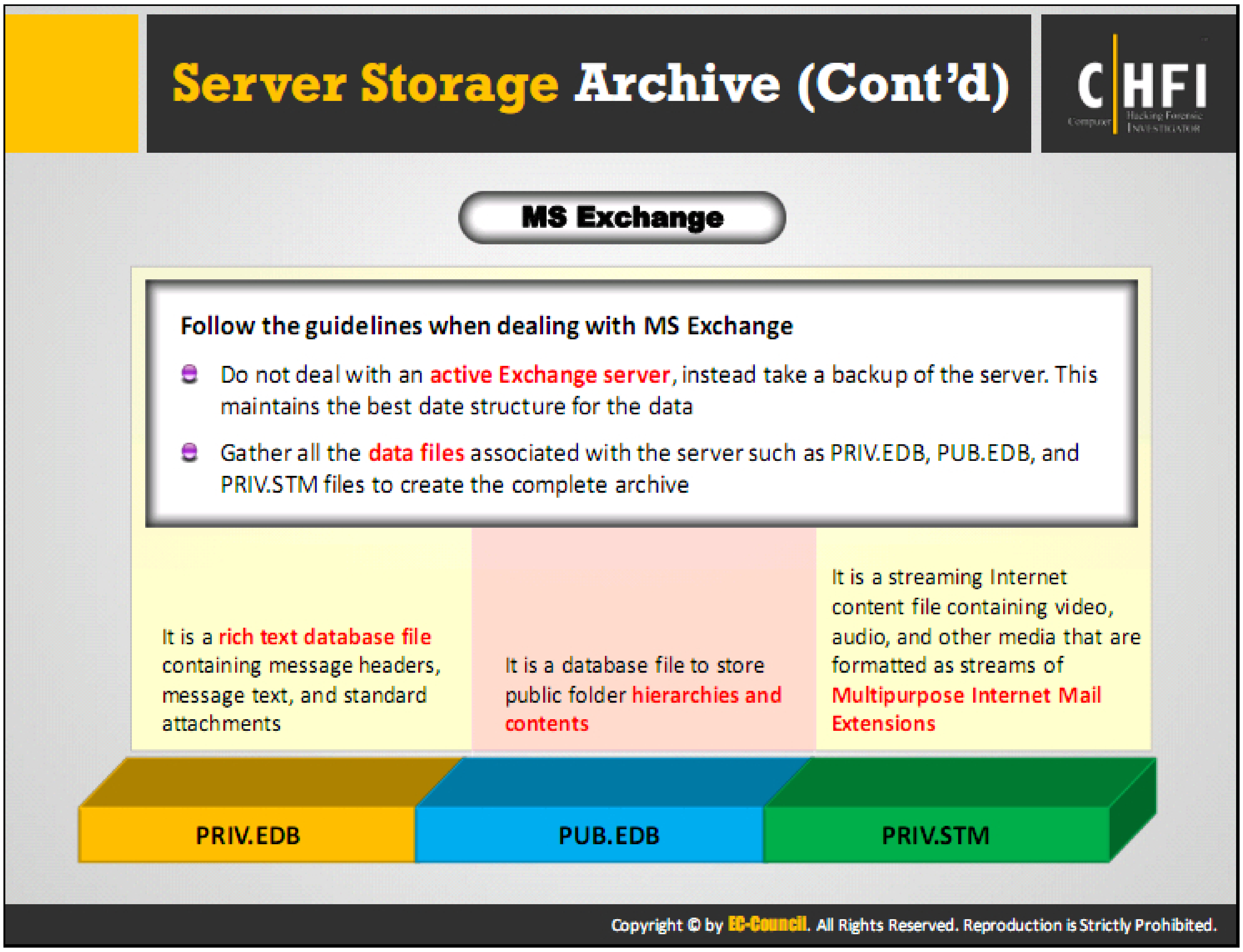
IBM Notes, formerly IBM Lotus Notes, is an enterprise email client that integrates messaging, business applications, and social collaboration. It allows the users to archive the messages sent and received, calendar, contacts, etc. in an encrypted format. The IBM Notes stores the archives with .nsf extension. Investigators need to search for the archives if they find that the client is present or uninstalled from a system in order to extract the details. As the archive is in an encrypted format, the investigators should gather the associated encryption key (also called as ID), which allows decryption of the file.

Novel GroupWise

Using the Novel GroupWise archiving process, the users and investigators can store the email contents from the main GroupWise server to a local or networked drive. The process assigns a networked drive in the AS server to each account. Archiving helps to save the disk storage space on the main GroupWise server by compressing it and also increases the server speed.

Guidelines for dealing with Novell GroupWise:

- Do not alter or modify the structure to acquire the entire directory. The structure should remain unaltered for a successful processing through the mail.
- Ngwguard.db is stored in the root of the mail directory and is the key file of the GroupWise structure. It tells GroupWise about each user account and their locations.
- Other key files include wphost.db and gwcheck.db, but the entire directory must be intact to perform 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

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

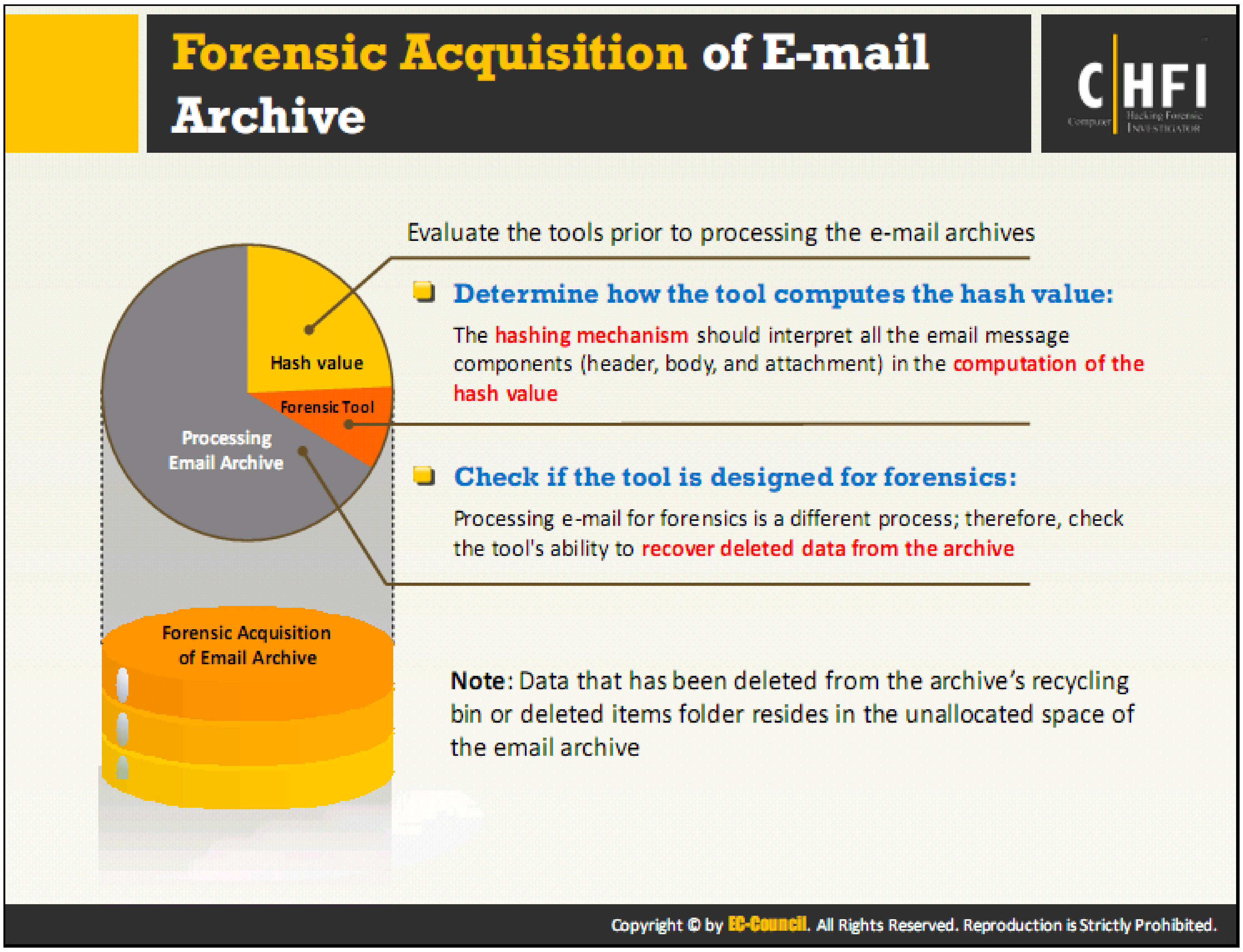
MS Exchange

Follow these guidelines when dealing with MS Exchange:

In an organization, various employees connect with each other through servers such as the Microsoft Exchange Server. Therefore, the investigators should not access an active Exchange server. The best way is to create a backup of the server, which will be available for users to connect to the Exchange server. Investigators must collect all the data files associated with the server, as there is more than one file associated with Exchange email. The archive file consists of the PRIV.EDB file, PUB.EDB file, and PRIV.STM file. The files available will vary according to the Exchange server you are dealing with.

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

Most of the backups are part of the forensic process, which is why it is important to be careful with backups and offline storage. An expert should be engaged to restore the server data in the case the investigators are not familiar with the restore process for Exchange servers.



Forensic Acquisition of E-mail Archive

Evaluate the tools prior to processing the e-mail archives

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

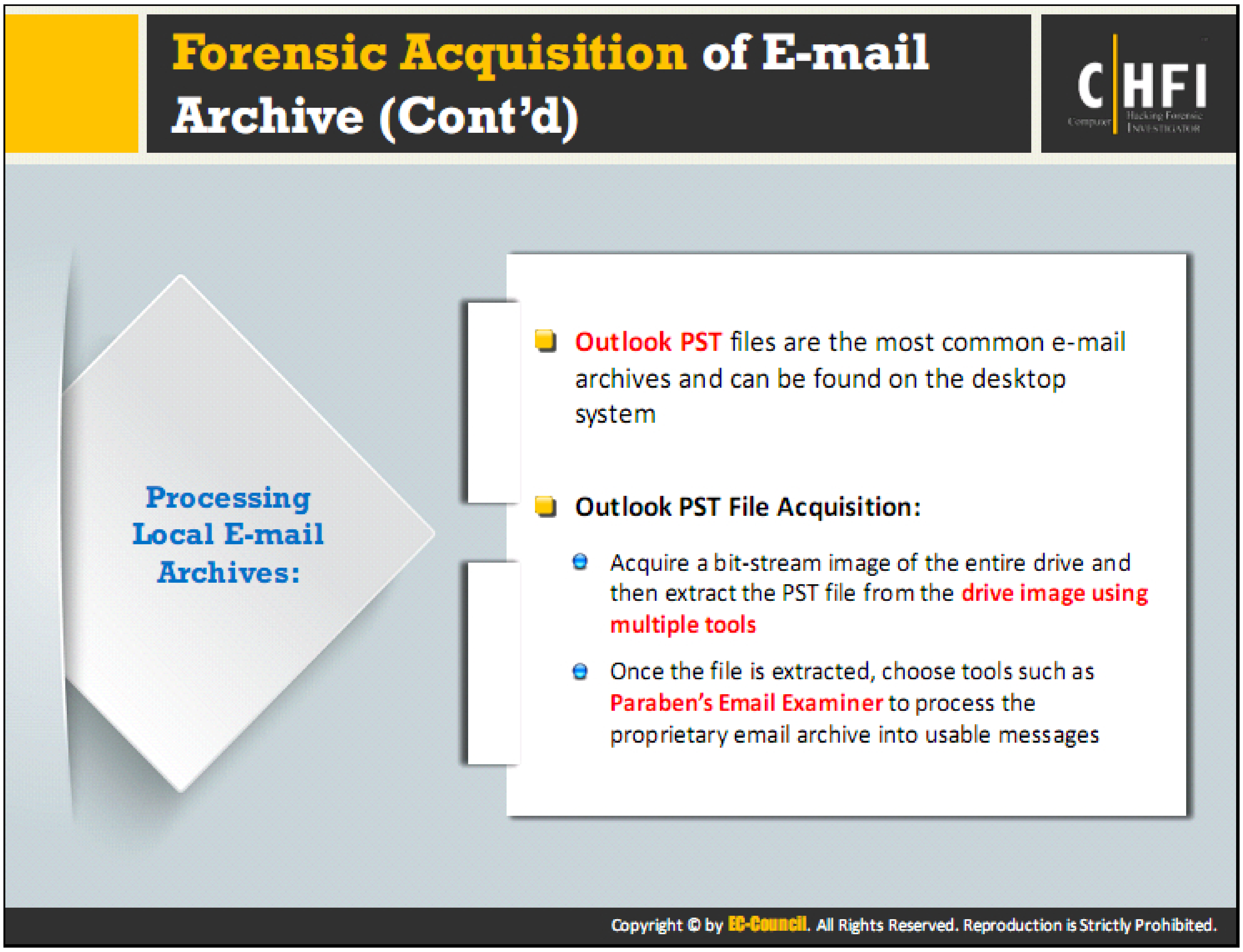
  The hashing mechanism should interpret all the email message components (header, body, and attachment) in the computation of the hash value

- **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

Hash value
Forensic Tool
Processing Email Archive
Forensic Acquisition of Email Archive
CHFI
Computer Hacking Forensic Investigator



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

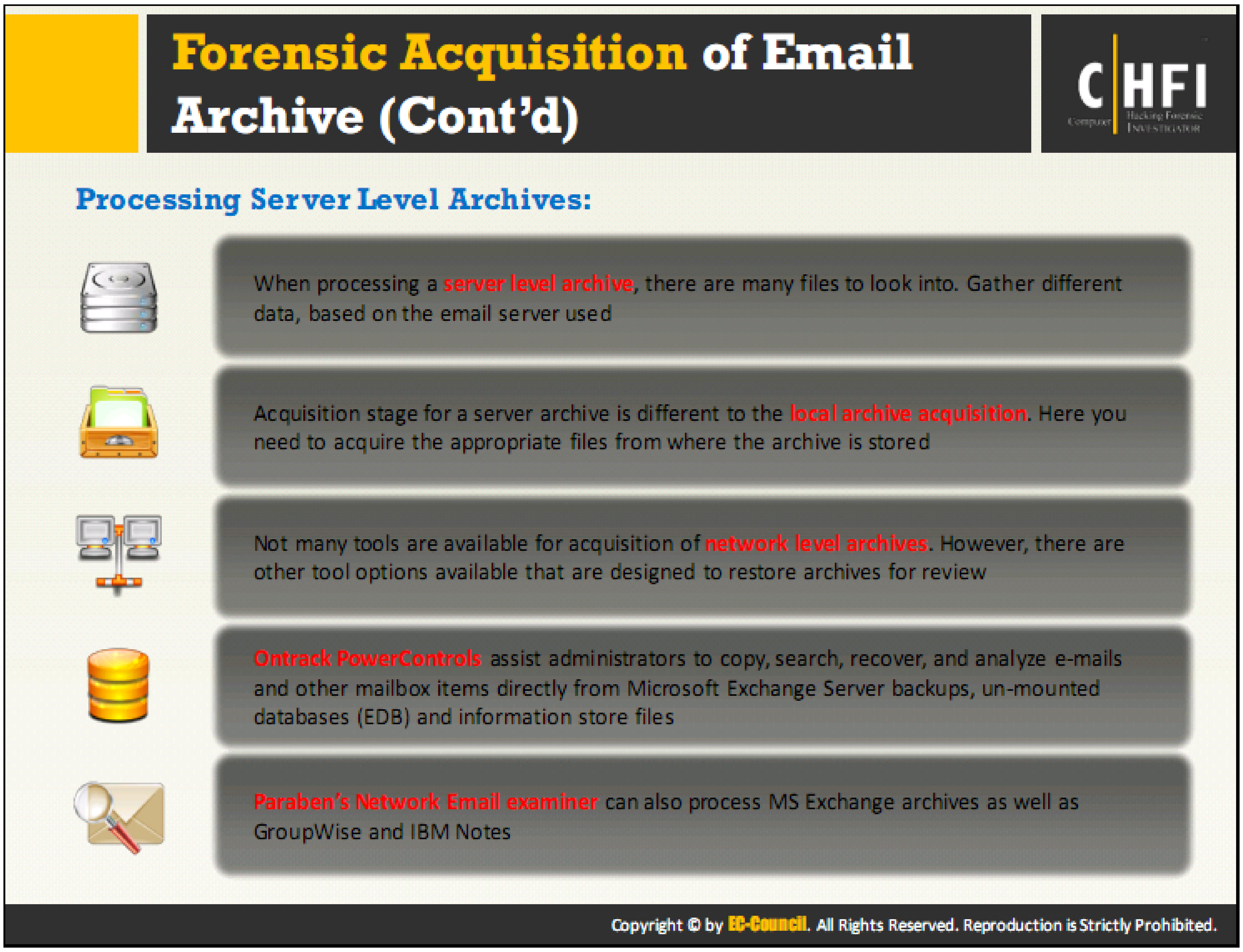
CHFI
Computer Hacking Forensic Investigator

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

Outlook PST File Acquisition

Usually, PST file extraction from the drive image takes place by bit-streaming an image of the entire drive. While extracting the PST file from the image, multiple tools should be used. Many virtual mounting programs are present that let you mount the acquired drive and then extract the copy of the data from the drive. It is one of the best methods for data extraction, as other common methods used in automated forensic suites are not always feasible to extract a usable PST file. Choose tools such as Paraben's Email Examiner to process the proprietary email archive into usable messages once the file extraction is complete.



Forensic Acquisition of Email Archive (Cont'd)

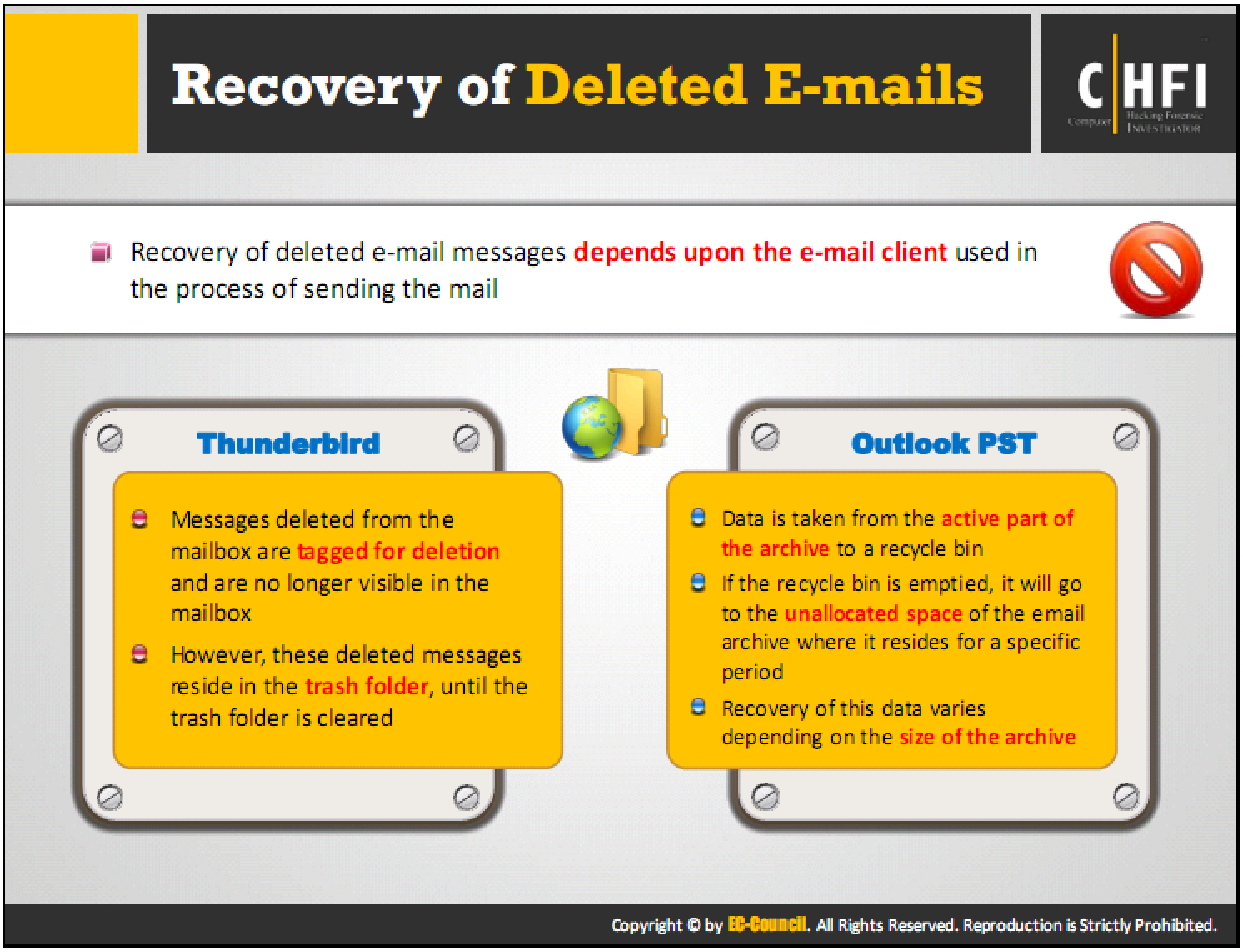
CHFI
Computer Hacking Forensic Investigator

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

Processing Server Level Archives

Unlike the local stores where the investigators do the acquisition by bit-streaming the image, the acquisition stage for a server archive is different. They do the acquisition by acquiring the appropriate files where the archive date is stored, which depends on the structure of the network archive and size.



Recovery of Deleted E-mails

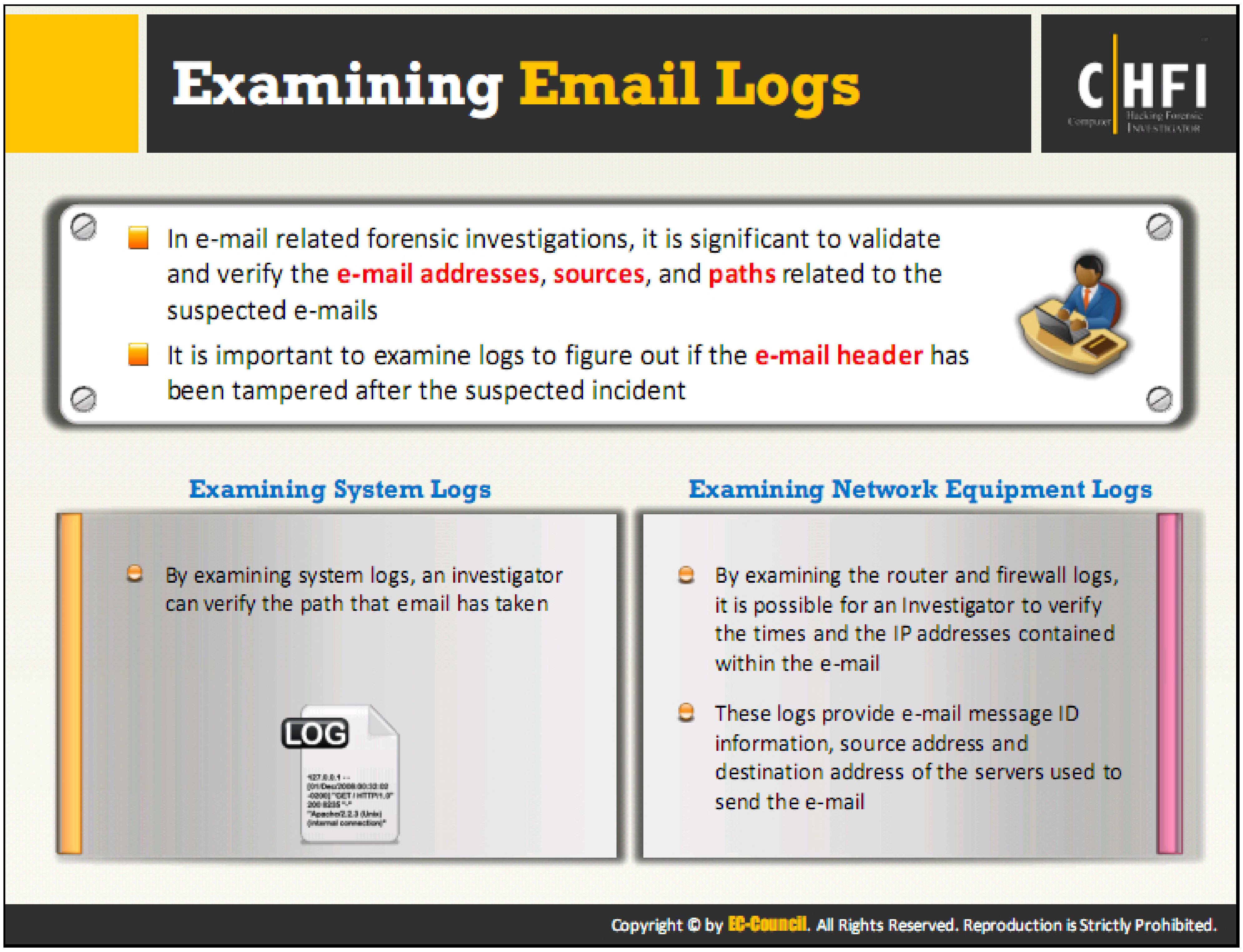
- Recovery of deleted e-mail messages **depends upon the e-mail client** used in the process of sending the mail

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

C|HFI
Computer Hacking Forensic Investigator

- 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

```
127.0.0.1 --
[01/Dec/2008:00:32:02
-0200] "GET / HTTP/1.0"
200 8235 "-"
"Apache/2.2.3 (Unix)
(internal connection)"
```

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

Email logs are very useful in forensic investigations to solve a case. Although the attackers are capable of altering the email headers, they cannot change the logs across the network, routers, firewalls, system, etc. Emails need to pass through all these devices. Investigators can use logs from various devices to check the email path and other details.

They identify email messages by:

- The received account
- IP address of the system from which they were sent
- Time and date
- IP addresses

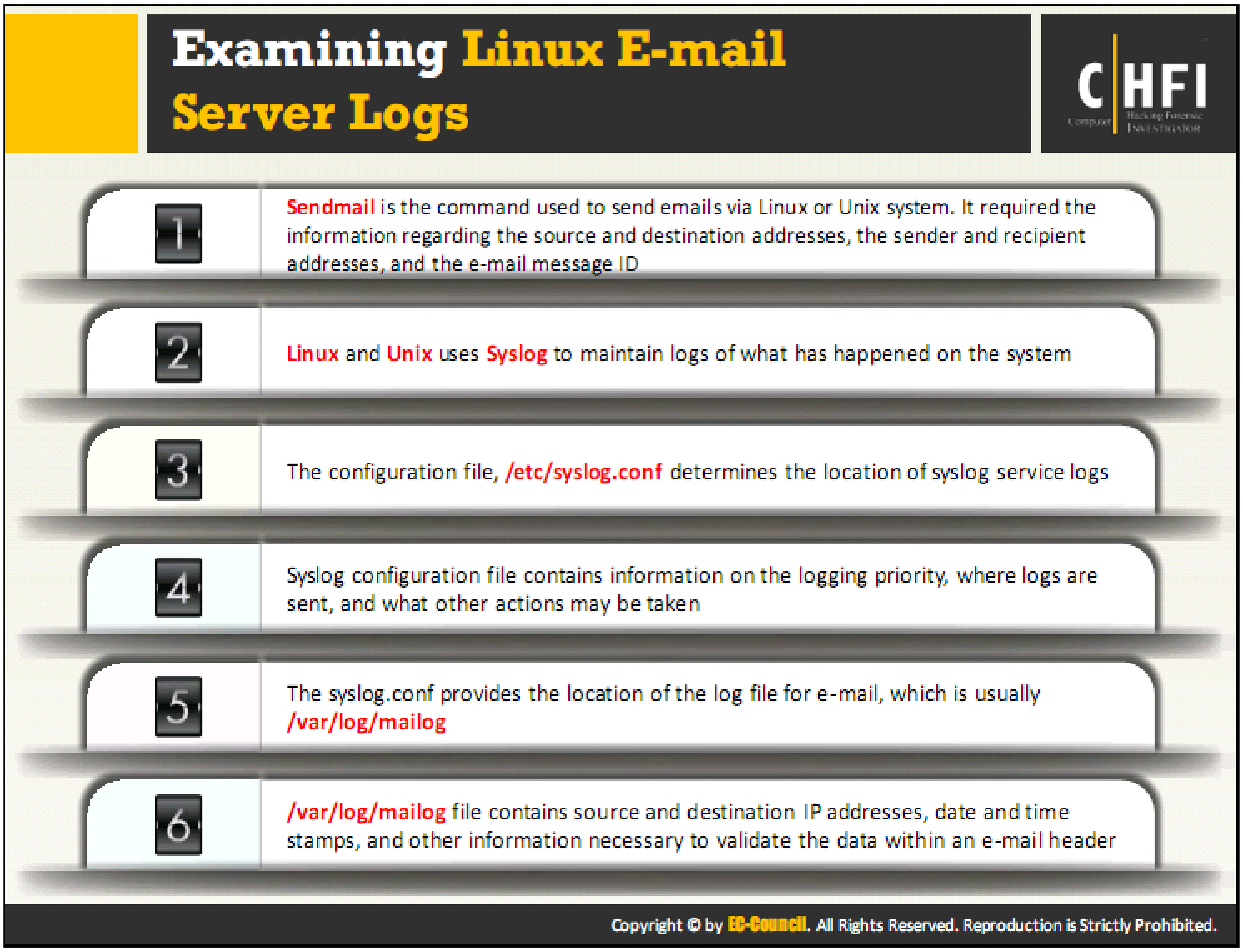
System Logs:

Systems store details of all the traffic they receive and send, along with details such as application, user, port, and protocol used to transfer the data. Therefore, these system logs can also contribute to the investigation of emails and provide detailed data about them. Investigators should know the process of finding and collecting this evidential data that can help in creating the timeline of the security event.

Network Equipment Logs:

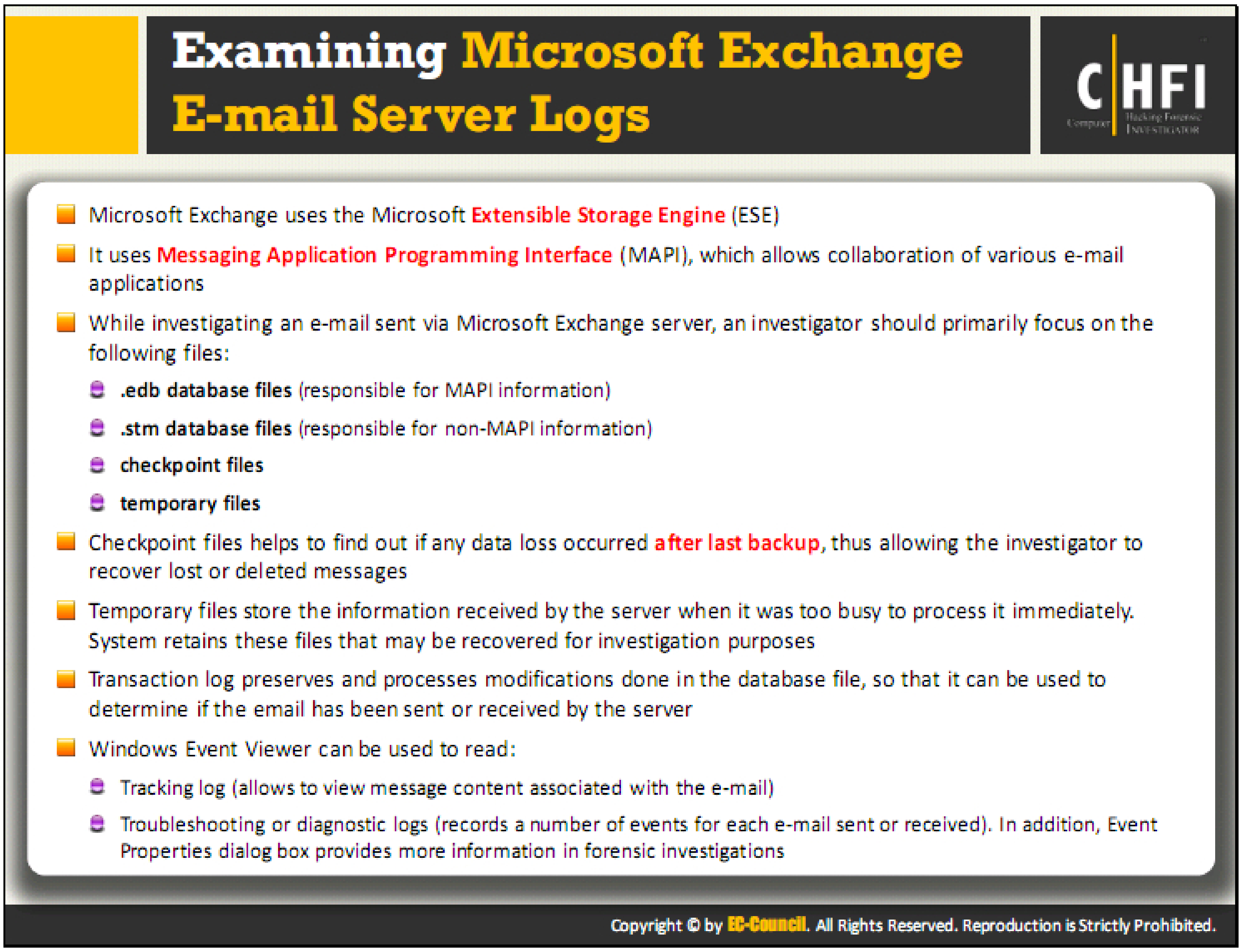
Network equipments, such as routers, switches, firewall, server, etc., store the transmission data and logs. Investigators can work in association with the administrators to gather the inbound and outbound traffic logs. The logs from the routers include details of the traffic they allow or deny, source or destination IP address, type of transmission, etc.

The network admins also maintain the firewall logs that filter Internet traffic and can contain the details of emails that have passed through the firewall. Gathering of all the details and their cross-checking can help in finding the difference between header information and the information provided by the other sources to determine any manipulation.



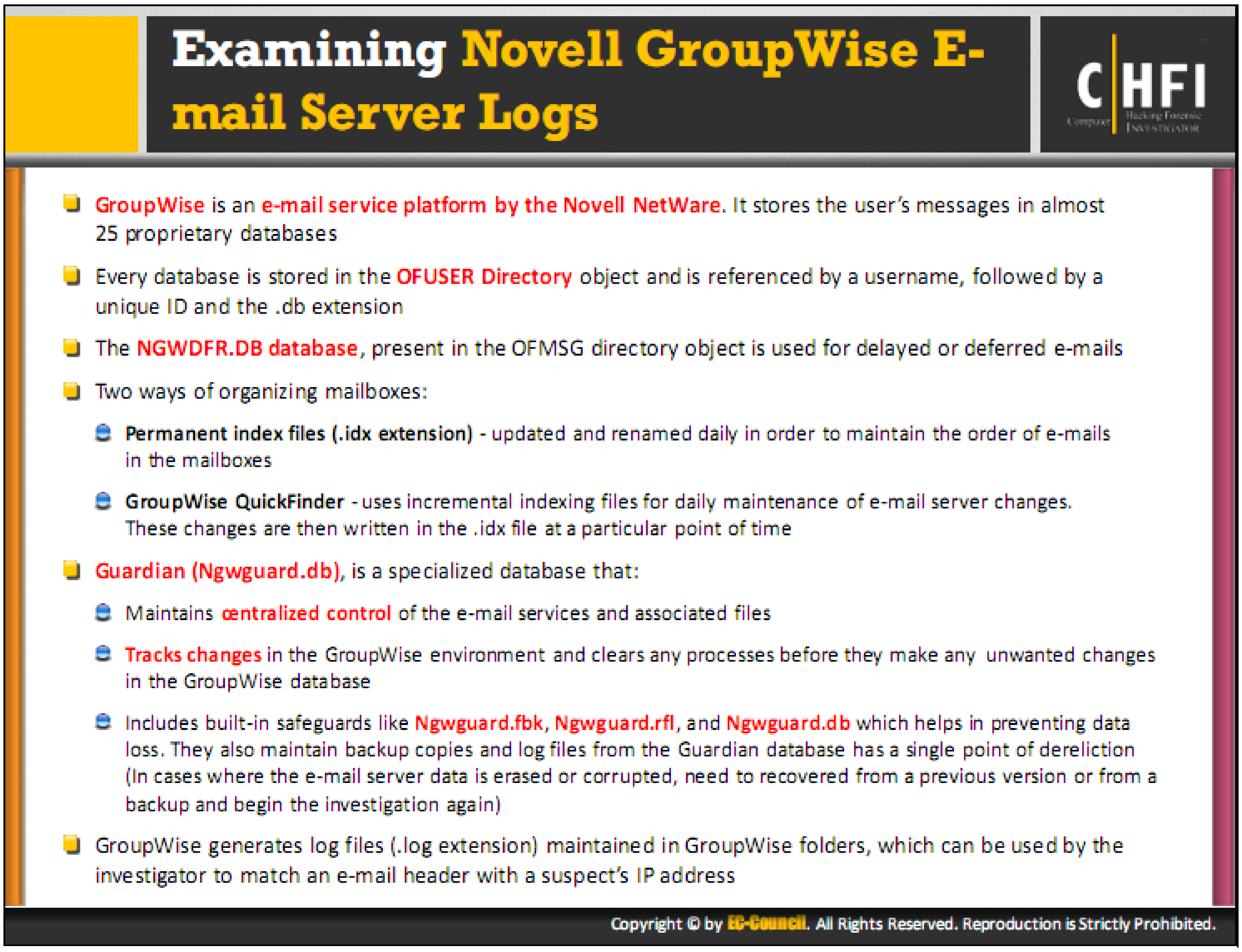
Examining Linux E-mail Server Logs

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

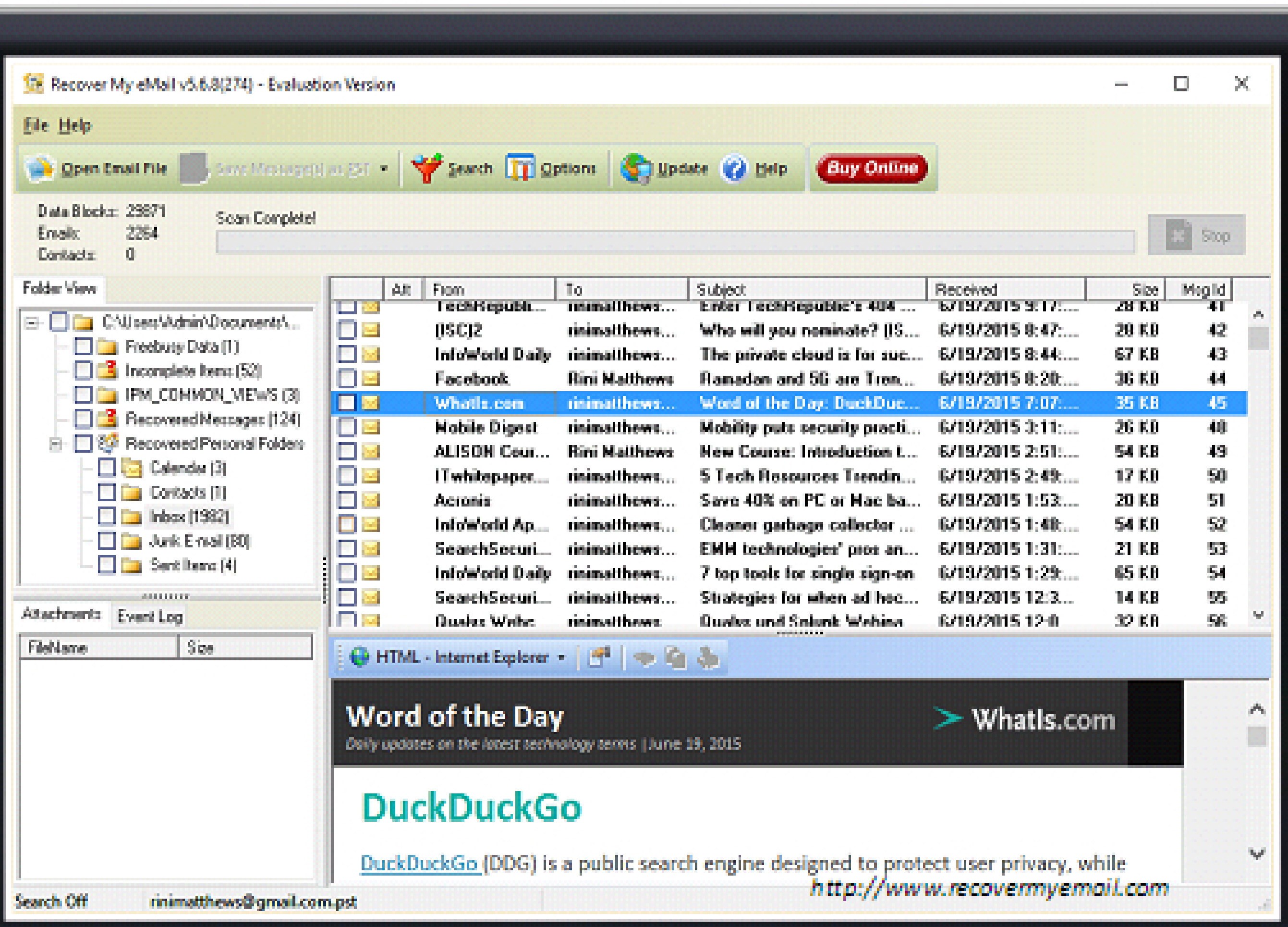


Examining Novell GroupWise E-mail Server Logs

- 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



Data Blocks: 29871
Emails: 2264
Contacts: 0

Scan Complete!

- C:\Users\Admin\Documents\...
  - Freebusy Data (1)
  - Incomplete Items (52)
  - IPM_COMMON_VIEWS (3)
  - Recovered Messages (124)
  - Recovered Personal Folders
    - Calendar (3)
    - Contacts (1)
    - Inbox (1982)
    - Junk E-mail (80)
    - Sent Items (4)

Att	From	To	Subject	Received	Size	Msg Id
	TechRepubl...	rinimatthews...	Enter TechRepublic's 404 ...	6/19/2015 9:17:...	28 KB	41
	(ISC)2	rinimatthews...	Who will you nominate? (IS...	6/19/2015 8:47:...	20 KB	42
	InfoWorld Daily	rinimatthews...	The private cloud is for suc...	6/19/2015 8:44:...	67 KB	43
	Facebook	Rini Matthews	Ramadan and 5G are Tren...	6/19/2015 8:20:...	36 KB	44
	WhatIs.com	rinimatthews...	Word of the Day: DuckDuc...	6/19/2015 7:07:...	35 KB	45
	Mobile Digest	rinimatthews...	Mobility puts security practi...	6/19/2015 3:11:...	26 KB	48
	ALISON Cour...	Rini Matthews	New Course: Introduction t...	6/19/2015 2:51:...	54 KB	49
	ITwhitepaper...	rinimatthews...	5 Tech Resources Trendin...	6/19/2015 2:49:...	17 KB	50
	Acronis	rinimatthews...	Save 40% on PC or Mac ba...	6/19/2015 1:53:...	20 KB	51
	InfoWorld Ap...	rinimatthews...	Cleaner garbage collector ...	6/19/2015 1:48:...	54 KB	52
	SearchSecuri...	rinimatthews...	EMM technologies' pros an...	6/19/2015 1:31:...	21 KB	53
	InfoWorld Daily	rinimatthews...	7 top tools for single sign-on	6/19/2015 1:29:...	65 KB	54
	SearchSecuri...	rinimatthews...	Strategies for when ad hoc...	6/19/2015 12:3...	14 KB	55
	Qualys Webc...	rinimatthews	Qualys und Splunk Webina	6/19/2015 12:0	32 KB	56

Word of the Day
Daily updates on the latest technology terms | June 19, 2015
WhatIs.com

DuckDuckGo

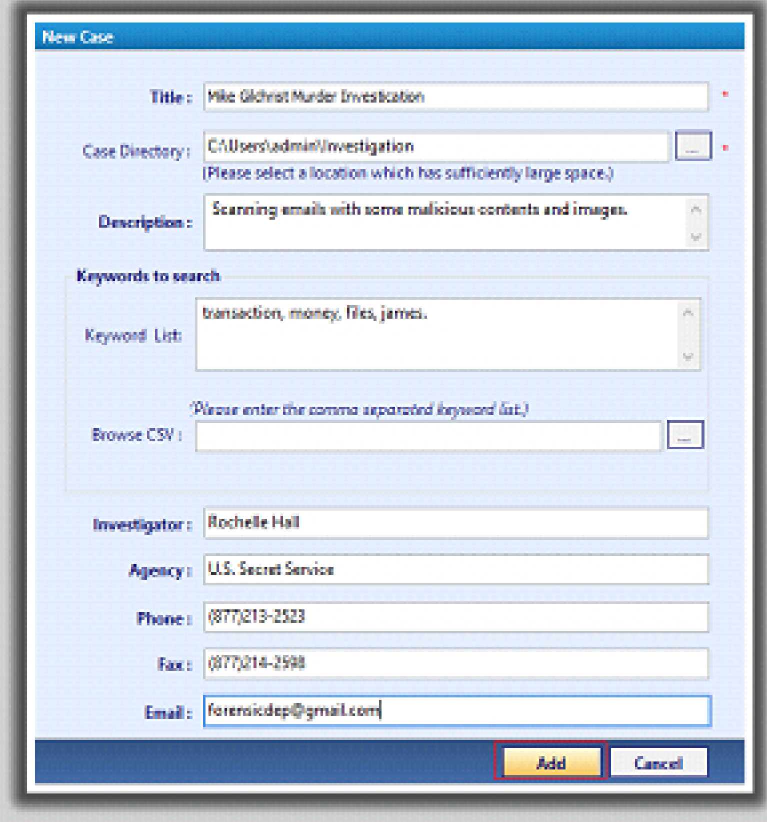
DuckDuckGo (DDG) is a public search engine designed to protect user privacy, while

Search Off   rinimatthews@gmail.com.pst

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



Title : Mike Gilchrist Murder Investigation *

Case Directory : C:\Users\admin\Investigation *
(Please select a location which has sufficiently large space.)

Description : Scanning emails with some malicious contents and images.

Keywords to search

Keyword List: transaction, money, files, james.

(Please enter the comma separated keyword list.)

Browse CSV :

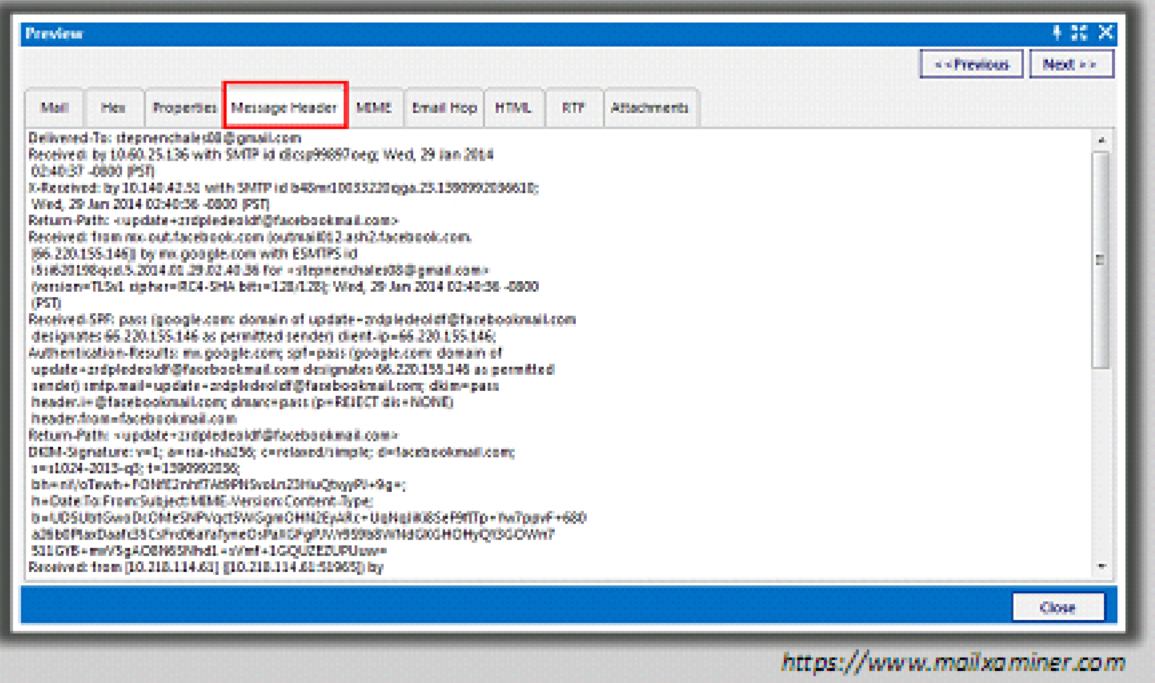
Investigator : Rochelle Hall

Agency : U.S. Secret Service

Phone : (877)213-2523

Fax : (877)214-2598

Email : forensicdep@gmail.com



```
Delivered-To: stephenchales08@gmail.com
Received: by 10.60.25.136 with SMTP id dicsp99887oeg; Wed, 29 Jan 2014
 02:40:37 -0800 (PST)
X-Received: by 10.140.42.51 with SMTP id b48mr10053220qga.25.1390992036610;
 Wed, 29 Jan 2014 02:40:36 -0800 (PST)
Return-Path: <update+zrdpledeoldf@facebookmail.com>
Received: from mx-out.facebook.com (outmail012.ash2.facebook.com.
 [66.220.155.146]) by mx.google.com with ESMTPS id
 i5si620198qcd.5.2014.01.29.02.40.36 for <stephenchales08@gmail.com>
 (version=TLSv1 cipher=RC4-SHA bits=128/128); Wed, 29 Jan 2014 02:40:36 -0800
 (PST)
Received-SPF: pass (google.com: domain of update+zrdpledeoldf@facebookmail.com
 designates 66.220.155.146 as permitted sender) client-ip=66.220.155.146;
Authentication-Results: mx.google.com; spf=pass (google.com: domain of
 update+zrdpledeoldf@facebookmail.com designates 66.220.155.146 as permitted
 sender) smtp.mail=update+zrdpledeoldf@facebookmail.com; dkim=pass
 header.i=@facebookmail.com; dmarc=pass (p=REJECT dis=NONE)
 header.from=facebookmail.com
Return-Path: <update+zrdpledeoldf@facebookmail.com>
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=facebookmail.com;
 s=s1024-2013-q3; t=1390992036;
 bh=nl/oTewh+FGNfE2nhfTA6PNSvoLn23HuQbyyPl+9g=;
 h=Date:To:From:Subject:MIME-Version:Content-Type;
 b=UDSUbtGwoDcOMeSNPVqctSWGgmOHN2EyARc+UgNqlKl8SeP9fTp+fwTpgvF+680
 a2bb0PlaxDaafc35CsFrd6afafyneOsPaRGFgPJV/95598WNdGXGHOHyQYSGOWm7
 531GYB+mVSgAO8N65Nhdl+sVmf+1GQUZEZUPUuw=
Received: from [10.218.114.61] ([10.218.114.61:51965]) by
```

https://www.mailxaminer.com

Some of the features of MailXaminer include:

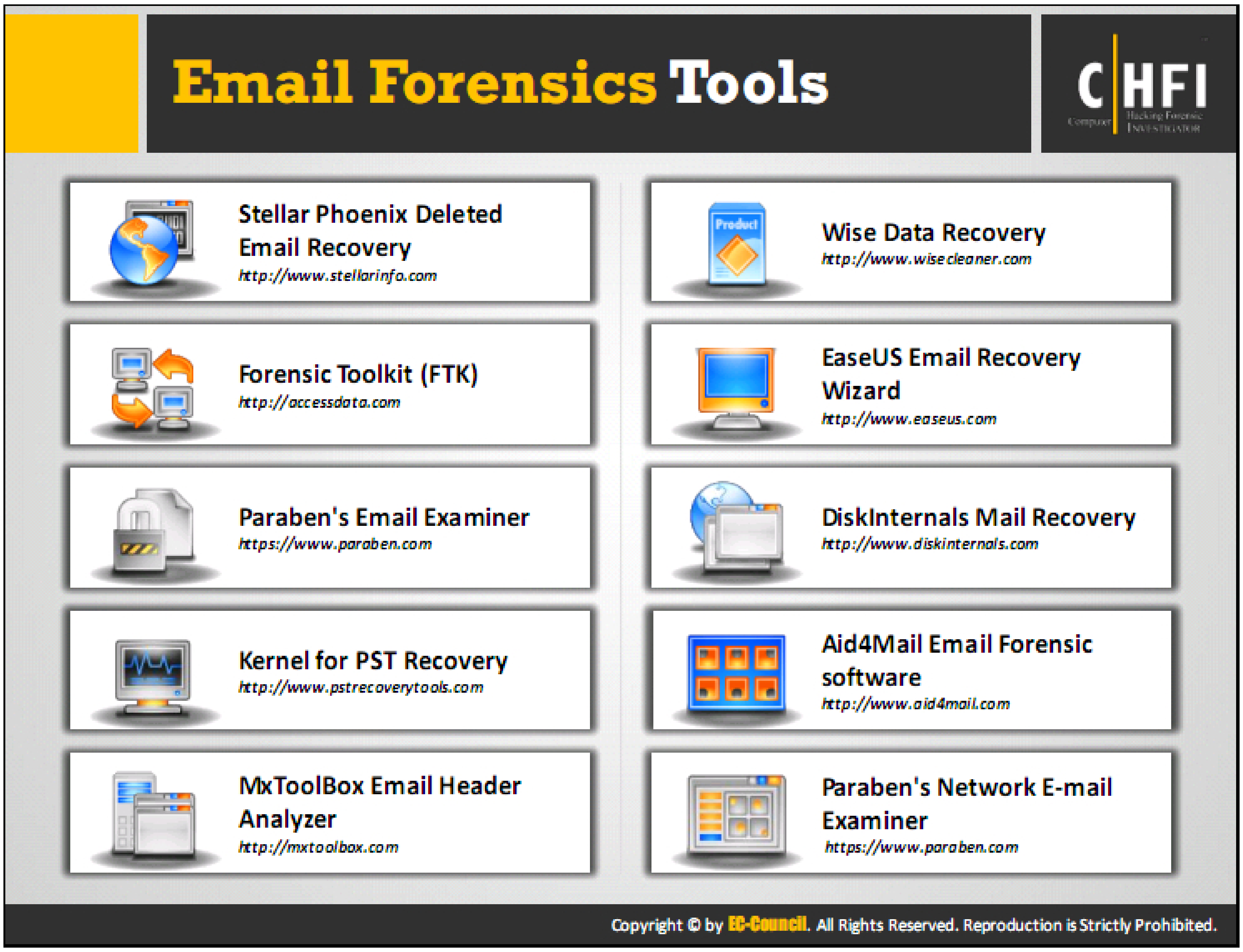
1. Case management facility like creating case repository, analyze & recover email, scan status, interactive dashboards, log files and bookmarking options make the investigation more efficient and faster.

2. The custodians can share all case related progress or evidence over web / on cloud with fellow investigators for review purpose. This can be accomplished via Shared Location, Mail Settings, or over Cloud.

3. Skin tone based analysis can be performed on media files, particularly images. The intensity of detection can be adjusted accordingly from very low, low, high, to very high respectively for accurate results.

4. Video files such as .mp4, .avi, .3gp can be investigated using the software for detection of availability of pornographic content. The parameters deciding the intensity of detection fall between the range of very low and very high.

5. KML (Keyhole Markup Language) file format is used to save and display the geographic data Google Maps and Google Earth. The available image attachments having GPS locations can be exported using "Export as KML"; and can be viewed using Google Earth.



Email Forensics Tools

CHFI

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

Stellar Phoenix Deleted Email Recovery

Source: http://www.stellarinfo.com

It is a software that safely recovers lost or deleted emails from MS Outlook data (PST) files and Outlook Express data (DBX) files.

Forensic Toolkit (FTK)

Source: http://accessdata.com

FTK is a court-cited digital investigations platform built for speed, stability and ease of use. It provides comprehensive processing and indexing up front, so that filtering and searching is fast. This means we can “zero-in” on the relevant evidence quickly, increasing the analysis speed.

Paraben's Email Examiner

Source: https://www.paraben.com

Email Examiner forensically examines email formats including Outlook (PST and OST), Thunderbird, Outlook Express, Windows mail and more. It allows to analyze message headers, bodies and attachments. It recovers email in the deleted folders, supports advanced searching, reporting and exporting to PST and other formats and supports all major email types that are stored on local computers for analysis, reporting, and exporting/conversion.

Kernel for PST Recovery

Source: *http://www.pstrecoverytools.com*

Kernel for PST Recovery is a enables to repair corrupted PST file and recover all email items from them. It successfully fixes errors resulted due to damaged or corrupted PST file, virus attacks, deleted emails, broken PST files, header corruption, disk corruption, errors due to large PST file size and others.

MxToolBox Email Header Analyzer

Source: *http://mxtoolbox.com*

This tool will make email headers human readable by parsing them according to RFC 822.

Wise Data Recovery

Source: *http://www.wisecleaner.com*

Wise Data Recovery is a data recovery program to get back deleted photos, documents, videos, emails etc. from your local or removable drives for free.

EaseUS Email Recovery Wizard

Source: *http://www.wisecleaner.com*

EaseUS Email Recovery Wizard is an email recovery software to recover deleted or lost emails, folders, calendars, appointments, meeting requests, contacts, tasks, task requests, journals, notes and attachments from corrupted .pst file. It is a safe and read-only utility which reads the lost/deleted mail items without modifying the existing content and restores the lost data into a new file.

DiskInternals Mail Recovery

Source: *http://www.diskinternals.com*

DiskInternals Mail Recovery can automatically locate, recover and fix broken Outlook Express, Vista Mail, Microsoft Outlook, **Server Storage Archive** and The Bat email databases on severely corrupted and damaged disks in one action.

Aid4Mail Email Forensic software

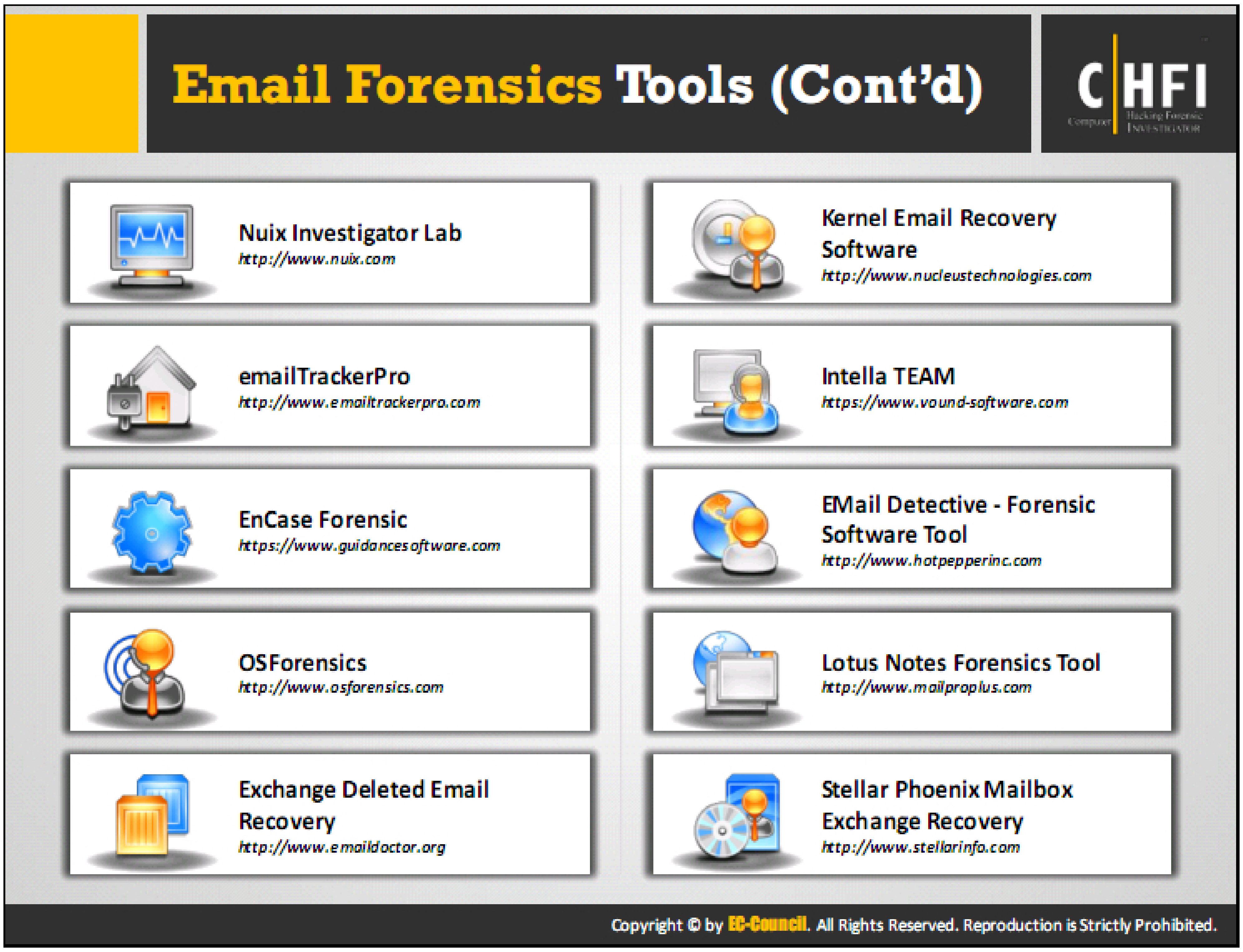
Source: *http://www.aid4mail.com*

Aid4Mail™ is used to quickly and reliably migrate email accounts, easily transfer messages between email apps and web-based services.

Paraben's Network E-mail Examiner

Source: *https://www.paraben.com*

Network E-mail Examiner makes it easy to analyze and filter messages and output the results into PST files.



Email Forensics Tools (Cont'd)

CHFI
Computer Hacking Forensic Investigator

- **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*

Nuix Investigator Lab

Source: http://www.nuix.com

Nuix Investigator Lab is for organizations looking to set up a dedicated facility that can rapidly ingest and process terabytes of digital evidence per day and make it available for timely analysis.

It enables multiple investigators and subject matter experts simultaneously to review and collaborate on an investigation with secure remote access, and produce comprehensive reports on your findings.

emailTrackerPro

Source: http://www.emailtrackerpro.com

EmailTrackerPro not only offers the ability to trace an email using the email header but it also comes with a spam filter (advanced edition), which scans each email as it arrives and warns the user if it is suspected spam. Stops spam email before it reaches its intended recipient.

EnCase Forensic

Source: https://www.guidancesoftware.com

It empowers examiners with efficiency and results in forensic investigations.

Features:

- Rapidly acquire data from the wide variety of devices
- Unearth potential evidence with disk-level forensic analysis
- Produce comprehensive reports on your findings
- Maintain the integrity of your evidence in a format the courts have come to trust

OSForensics

Source: http://www.osforensics.com

It helps discover relevant forensic data faster with high performance file searches and indexing as well as restores deleted files. It identifies suspicious files and activity with hash matching, drive signature comparisons and looks into e-mails, memory and binary data. It also manages digital investigation, organizes information and creates reports about collected forensic data.

Exchange Deleted Email Recovery

Source: http://www.emaildoctor.org

This Product features MS Exchange Server Email Data EDB File recovery from any extent of file corruption, protection and deletion thus eliminating server downtime.

Kernel Email Recovery Software

Source: http://www.nucleustechnologies.com

Kernel data recovery group presents an wide range of email recovery products, which recover the lost and deleted emails, email attachments, images, files and email properties.

This recovery software is developed to restore and repair files of MS Outlook (OST and PST), Outlook Express (DBX), IncrediMail (.IMM, .IMH, .IMB) which might get corrupt due to accidental deletion of emails, virus attacks, emails corrupted in the transit and even when the emails are emptied from the 'Deleted Items' folder of the email clients.

Intella TEAM

Source: https://www.vound-software.com

Intella TEAM enables multiple individuals to review evidence independently. It is an email investigation and eDiscovery software tool for an agency, law firm or investigative team that needs to coordinate the search and analysis of ESI and files that exceed 250 gigabytes. Investigators can quickly and easily process, search, review and analyze email and ESI as well as process and search multiple email sources, file types and metadata. It allows viewing results in a visual layout of choice and exporting the documents of interest in a wide variety of file formats.

EMail Detective - Forensic Software Tool

Source: http://www.hotpepperinc.com

This application is used to extract any MBOX or AOL email that has been cached or saved on a user's disk. Additionally, a comprehensive report is produced that contains all the emails for a user. This report can then be instantly viewed and searched for any specific words or phrases by the investigator.

Lotus Notes Forensics Tool

Source: http://www.mailproplus.com

It recovers and extracts evidence from NSF Files.

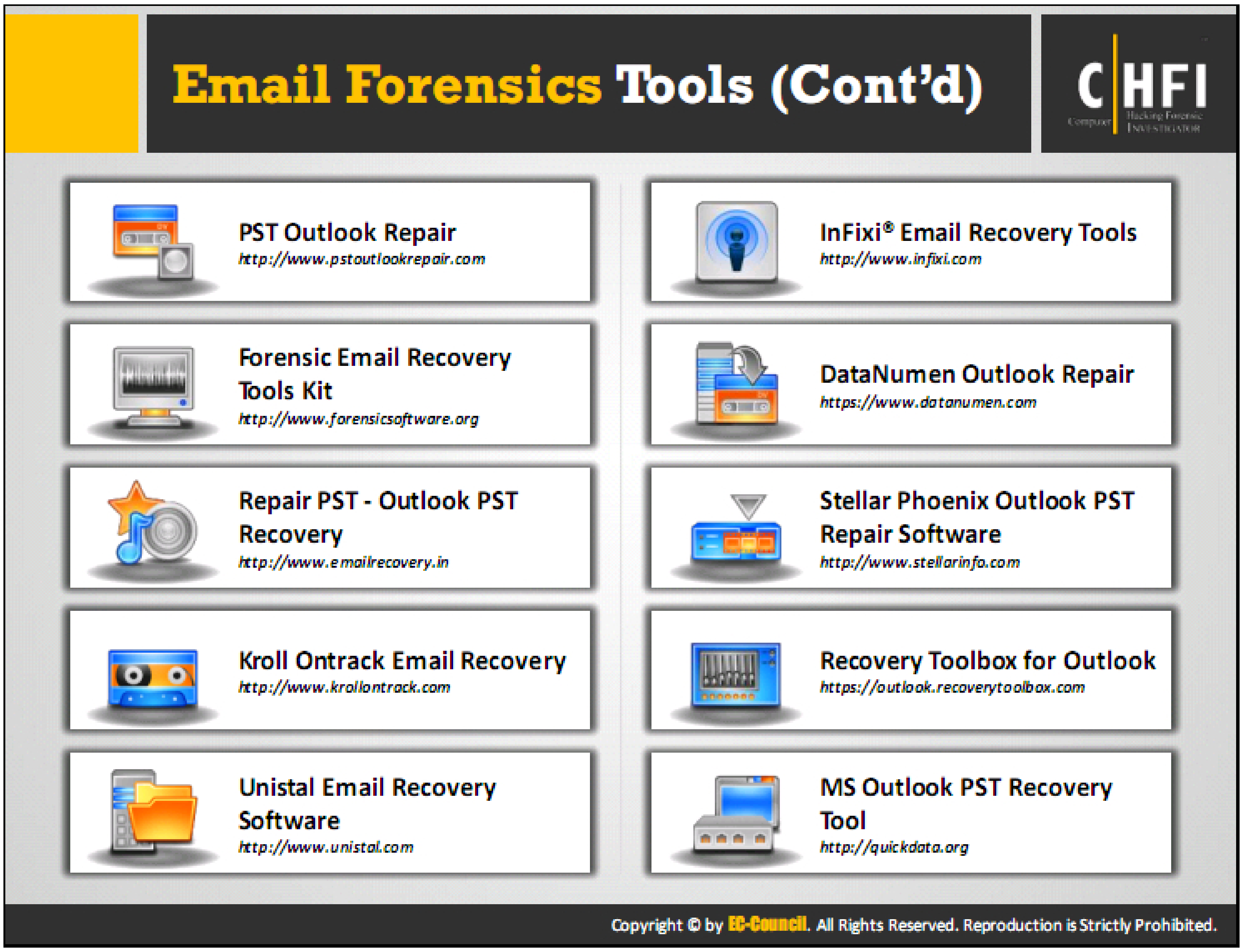
Features:

- Forensically Analyze Lotus Notes mails with several preview modes for carving out evidence
- Multiple search types like general expression available to look for available trails
- Recursive listing option enables collective email preview displaying all emails.

Stellar Phoenix Mailbox Exchange Recovery

Source: http://www.stellarinfo.com

Stellar Phoenix Mailbox Exchange Recovery repairs corrupt Exchange Database (EDB) files. It is capable of handling any level of corruption in EDB and restoring mailbox contents like emails, attachments, contacts, calendars, tasks, etc.



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

PST Outlook Repair

Source: http://www.pstoutlookrepair.com

Outlook PST stores the Outlook files and maintains the Outlook data till the space does not gets consumed or the MS Outlook itself does not encounter some technical glitches.

Forensic Email Recovery Tools Kit

Source: http://www.forensicsoftware.org

This kit looks into suspect's mailbox even if he/she played the trick to corrupt/delete the relevant emails from his/her email database of Outlook application, Exchange email system or from Mac Outlook email program.

Repair PST - Outlook PST Recovery

Source: http://www.emailrecovery.in

Repair PSTis an Outlook PST Recovery Software to recover emails from corrupt PST files of Microsoft Outlook. It successfully recovers emails from Outlook PST with tasks, contacts, calendar, journal, notes and attachments.

Kroll Ontrack Email Recovery

Source: *http://www.krollontrack.com*

It is an email management tool that helps IT administrators granularly search and restore mailboxes, messages, attachments and other Microsoft® Office Outlook items without restoring the entire database.

Unistal Email Recovery Software

Source: *http://www.unistal.com*

This software tool helps recover and restore MS Outlook Files, Lotus Notes email files, Incredimail as well as MS Exchange email files.

InFixi® Email Recovery Tools

Source: *http://www.infixi.com*

InFixi Software group offers a great range of software product for "Email Recovery", "Email Conversion", "File Repair", "File Recovery" and "Password Recovery".

DataNumen Outlook Repair

Source: *https://www.datanumen.com*

DataNumen Outlook Repairscans the corrupt Outlook personal folders (.pst) files and recovers mail messages, folders, posts, calendars, appointments, meeting requests, contacts, distribution lists, tasks, task requests, journals, notes, etc. in them, thereby minimizing the loss in file corruption.

Stellar Phoenix Outlook PST Repair Software

Source: *http://www.stellarinfo.com*

Stellar Phoenix® Outlook PST Repair is a reliable solution to repair and recover Outlook personal storage file '.PST'. After repair, the contents are restored to a new importable PST file. The application also facilitates the recovery of folders.

Recovery Toolbox for Outlook

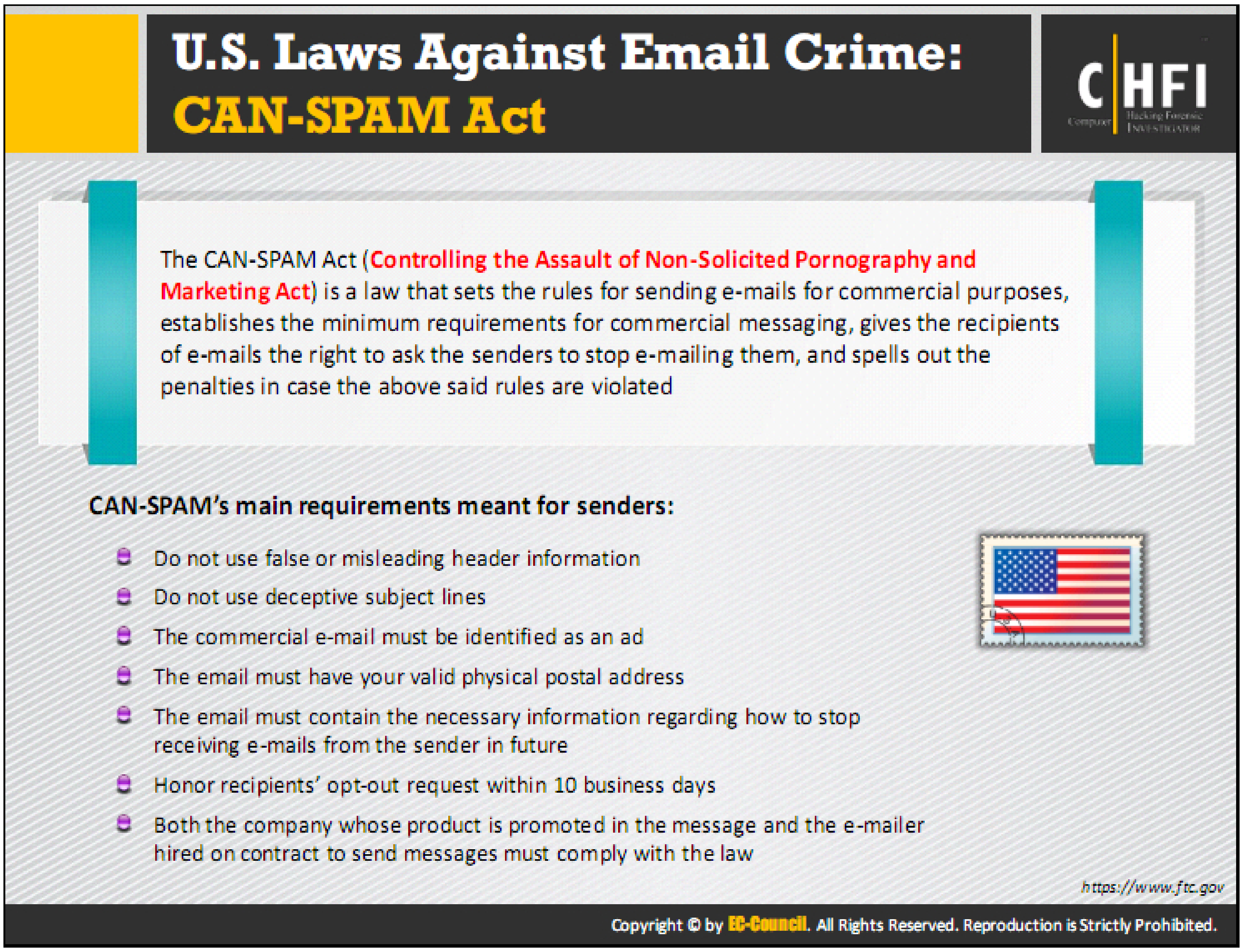
Source: *https://outlook.recoverytoolbox.com*

Recovery Toolbox for Outlook helps to restore emails, attachments, contacts and other from damaged .PST or .OST file. PST repair software helps to fix errors detected in Outlook.

MS Outlook PST Recovery Tool

Source: *http://quickdata.org*

It is a reliable solution to repair corrupted PST files, recover shift deleted emails, contacts, tasks, and save data in the different formats like; PST, MSG, or EML.



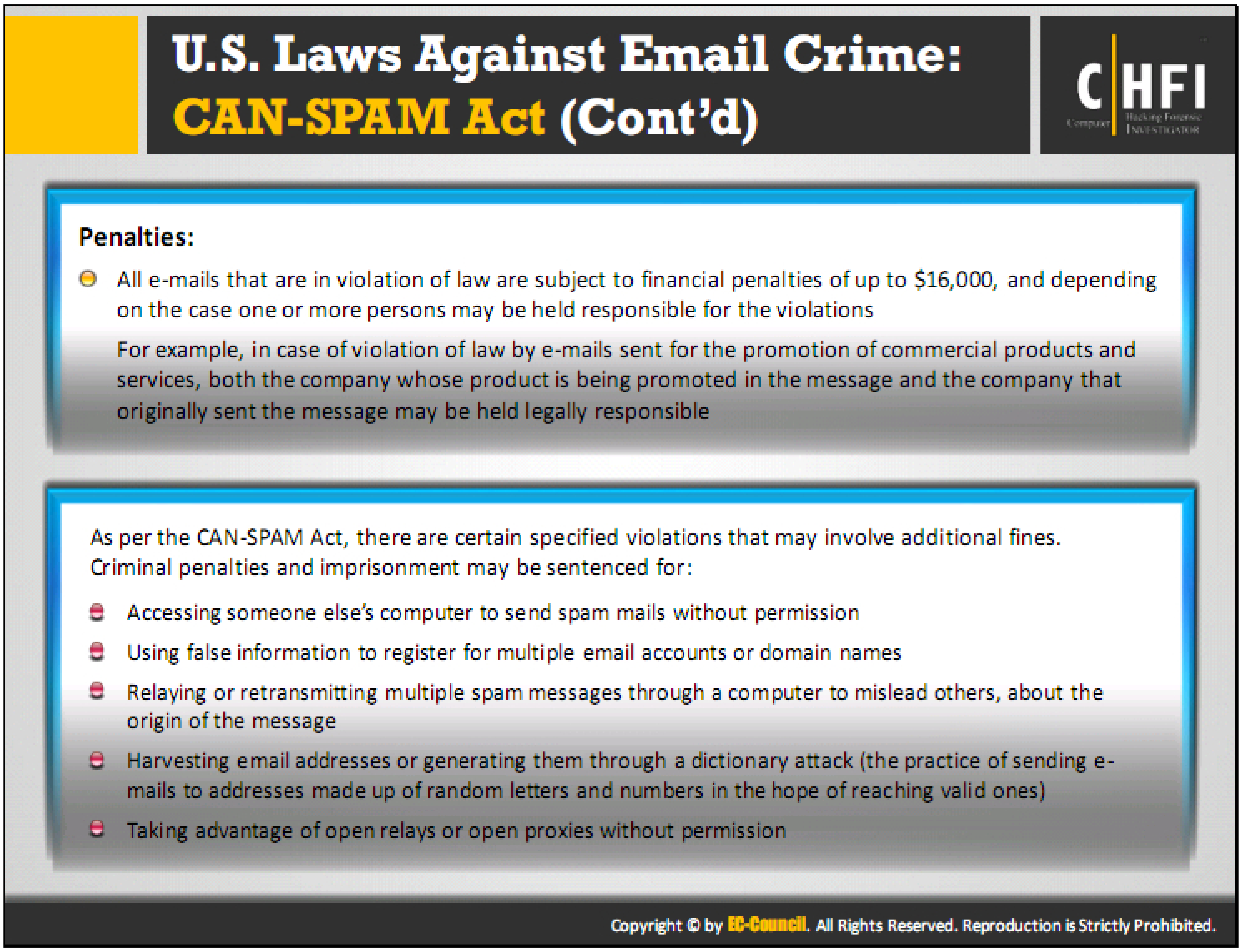
U.S. Laws Against Email Crime: CAN-SPAM Act

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)

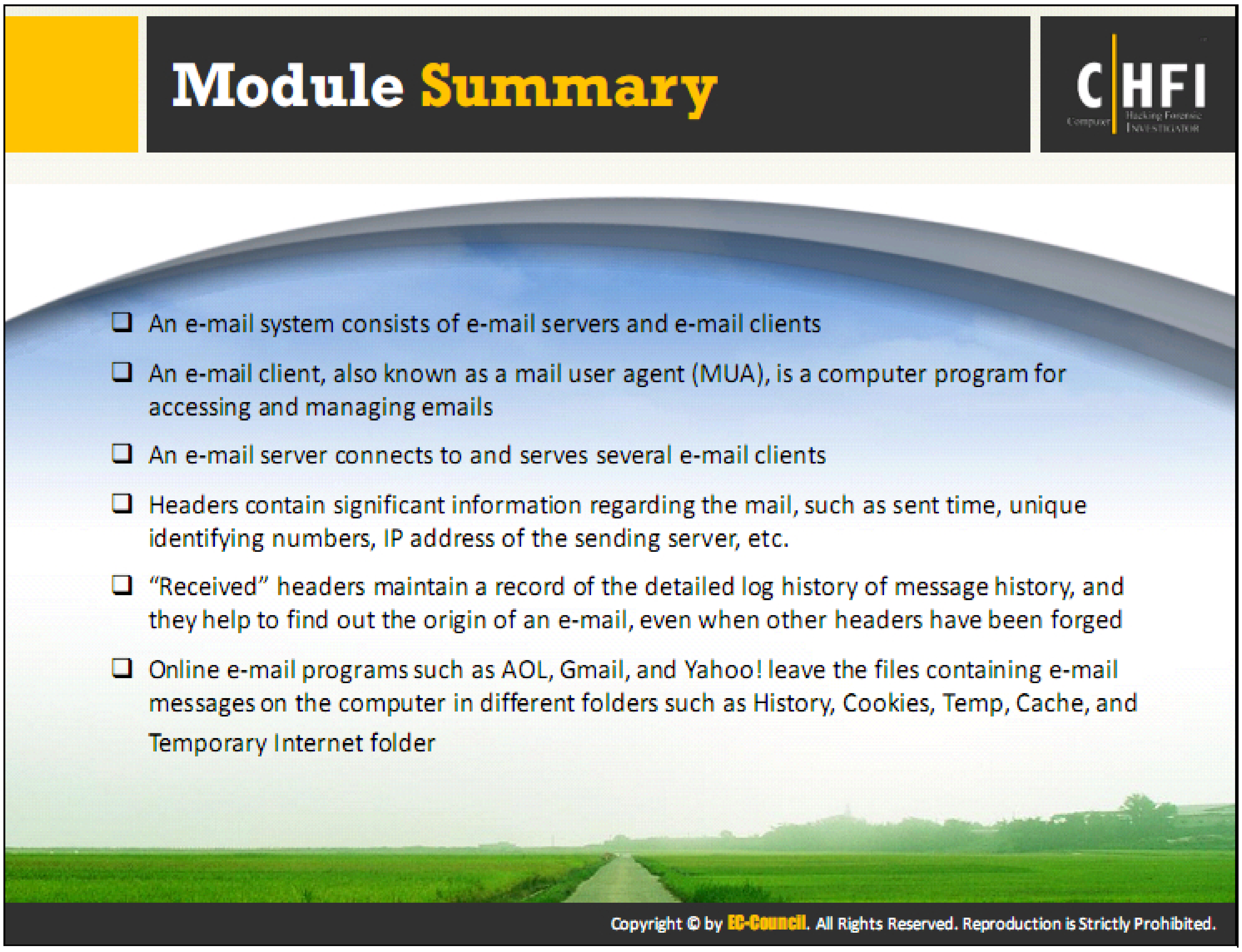
Penalties:

- 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

This module discusses email crimes and the processes attackers use to compromise security using email services, as well as the evidences that can help investigators to find and confirm the perpetrators. This module describes various methods of accessing and using email services, as well as the evidential data that the investigators can find using these methods and states the differences between them. This module helps to analyze different parts of an email, extract email data from different systems, and find the email logs and artifacts from systems and servers alike.

In the next module, we will learn about different mobile-related crimes and the methods to conduct a forensic investigation to determine evidence in such scenarios.