Module 11: Investigating Email Crimes

Scenario

Emily had received an email stating that she has won a huge amount from a big company but the amount can be collected only after paying certain taxes. The email also had instructions along with the account number to send the tax amount to as a precursor to receiving the cash prize. She followed all instructions in the email and later came to know that it was a spoofed email and someone had scammed her.

To investigate email crimes as a forensic investigator, you must know how to examine the email headers within an email message, trace the origin of a malicious email message, and extract or recover deleted email messages using various email tracking and investigation tools.

Lab Objectives

The objective of this lab is to help you understand how to examine different components of an email message and other responsibilities that include:

- Extracting metadata from email headers
- Finding the origin of a spoofed email message

Overview of Investigating Email Crimes

Email crime investigation is primarily conducted to examine the content as well as the origin of any email message that is found to be offending or suspected to be spoofed. Investigators need to use different forensic tools to examine emails related to spamming, mail bombing/mail storms, spoofing, phishing attacks, and email hijacking.

Lab Tasks

Recommended labs to assist you in investigating email crimes:

- Investigating a suspicious email

Lab 1: Investigating a Suspicious Email

Lab Scenario

John Dove, a manager at a reputed hotel, received an email in the hotel's official email account that stated that the hotel's Facebook account handle had been compromised and that the password to the account needs to be reset in order to recover the account. The email contained a link and an attachment in the form of a document that supposedly contained the instructions to reset the password for the affected Facebook account.

Panicked, John clicked on the link so he could follow the instructions to reset the password for the hotel's Facebook account and recover it.

As he went through the process, John realized that something was fishy about the Facebook page he was interacting with on the screen. However, during this process, he also inadvertently parted with the hotel's confidential information. The hotel's management soon learned that its key confidential information was stolen and was being misused for malicious purposes. John reported his encounter with the fishy email he received that stated itself to be from Facebook. Upon learning of the incident, the hotel's management sought the services of a cyber-forensics agency.

Investigator Johnson now has to analyze the suspicious email and find its origin.

Lab Objectives

Investigating a suspicious e-mail message involves the analysis of its email headers to determine if it is spoofed. It also involves determining the origin of the email message and checking the validity/genuineness of the sender's email address.

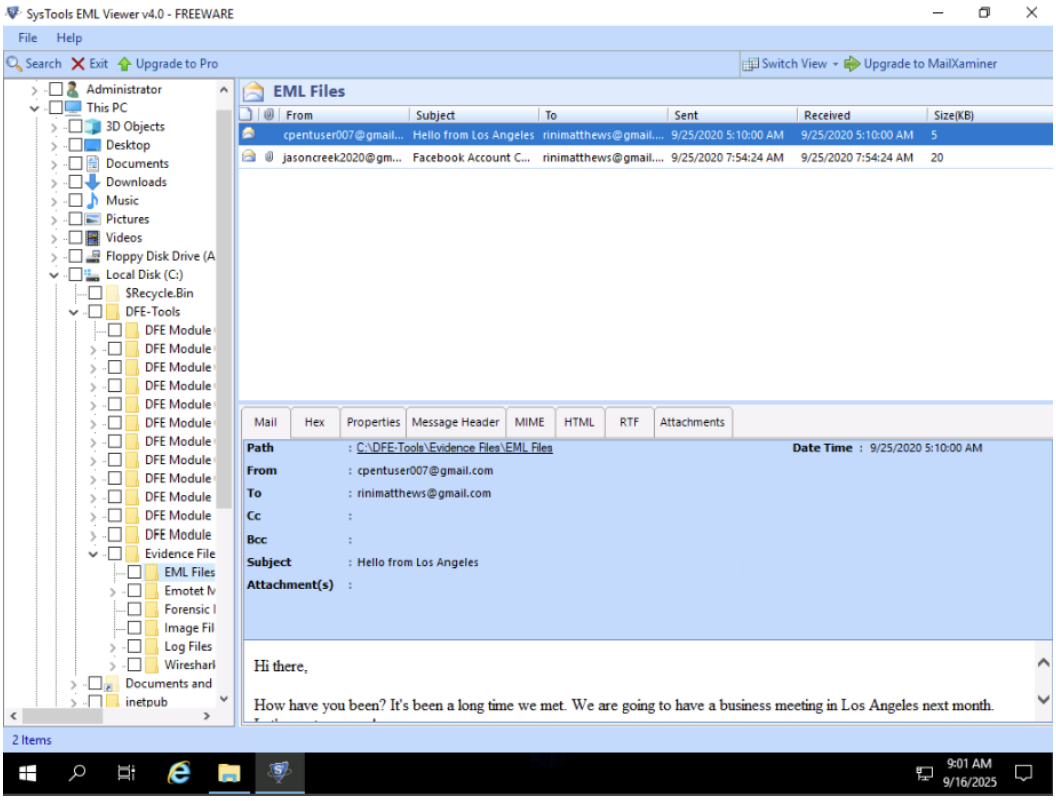
The objective of this lab is to help you understand how to perform forensic investigation on suspicious emails and how to analyze them.

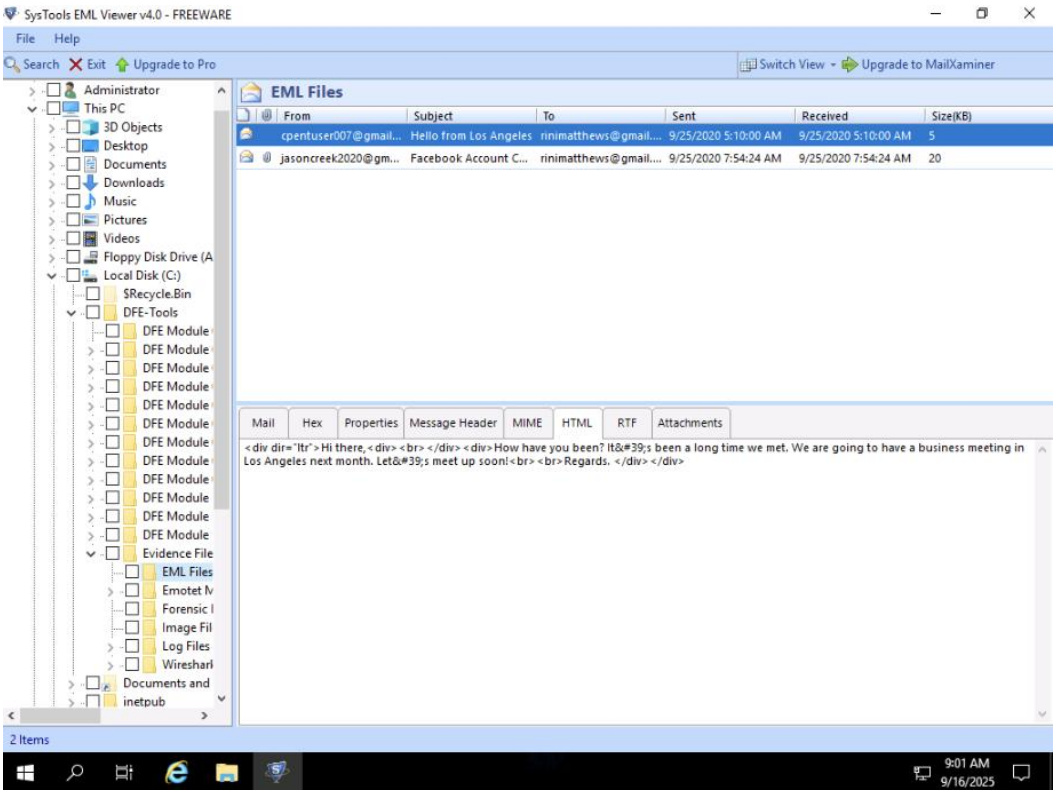
Overview of the Lab

This lab familiarizes you with the process of identifying a suspicious email and examining it in detail to determine if it is spoofed.

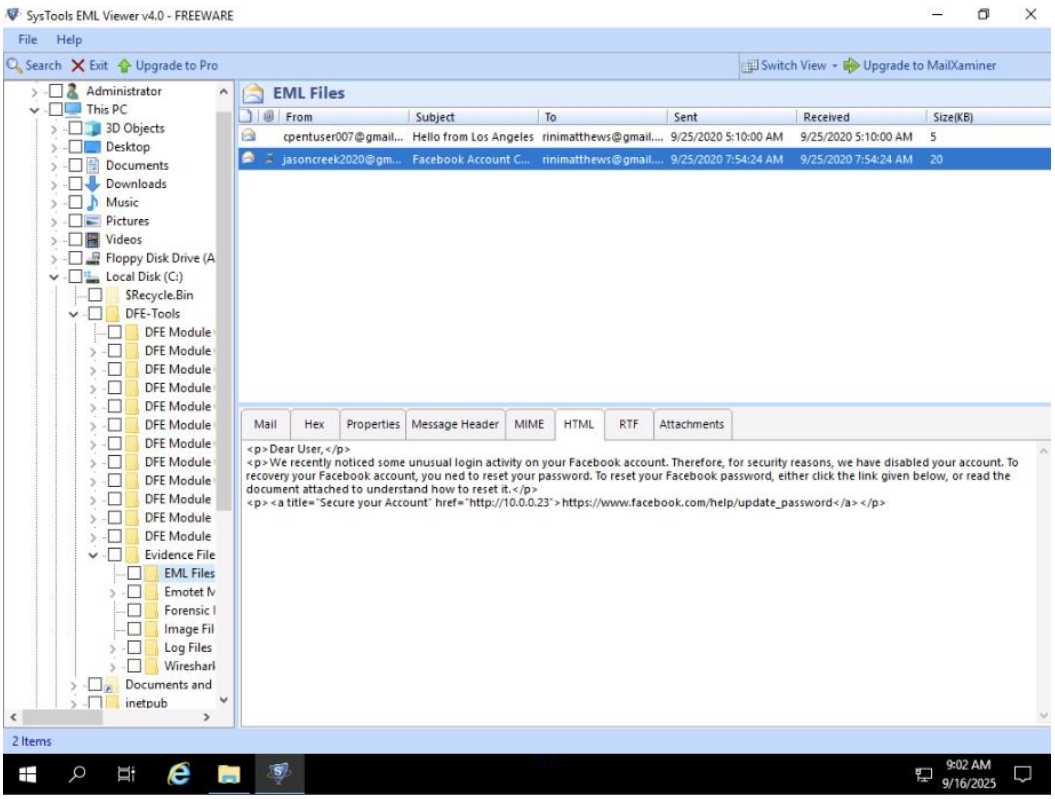
1. In this lab exercise, we will be examining and comparing two email files named **Suspicious Email Message** and **Normal Email Message**, so that you can differentiate a **spoofed email** message from a **genuine** one. We have downloaded these email messages from a Gmail account and have provided them to you in **C:\DFE-Tools\Evidence Files\EML Files**.

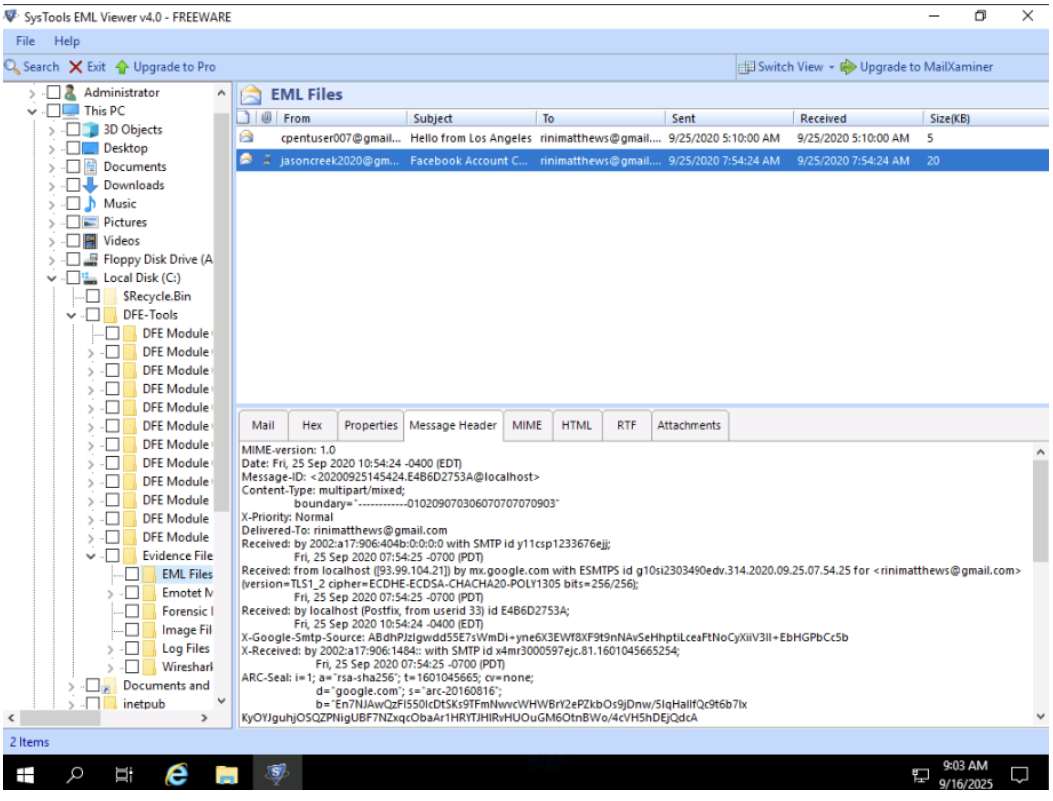
In a **real scenario**, as a forensic investigator, you will have to **identify** and **download** only the **suspicious email** message for investigation. The normal-looking email message has been used only for the demonstrative purpose of this lab, wherein we can show you how the details of a normal email message look like by comparing them with those of a suspicious email message.

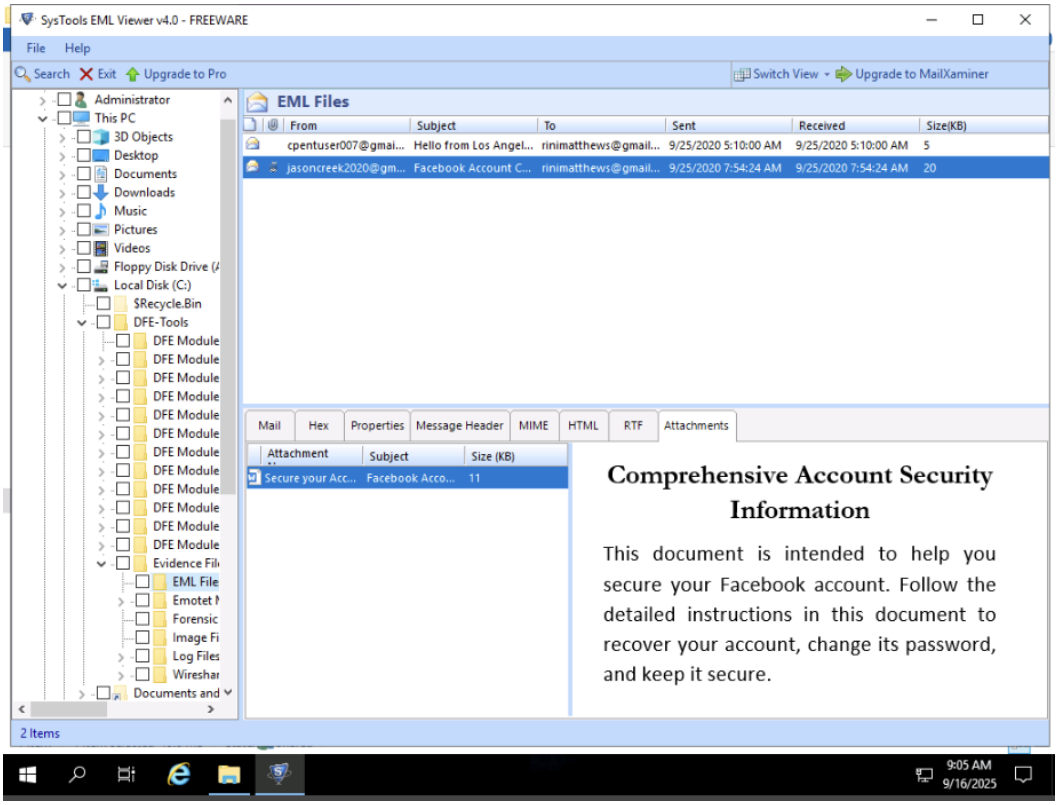

SysTools EML Viewer v4.0 - FREEWARE
File
Help
Search
Exit
Upgrade to Pro
Switch View
Upgrade to MailXaminer
Administrator
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Floppy Disk Drive (A
Local Disk (C:)
$Recycle.Bin
DFE-Tools
DFE Module
Evidence File
EML Files
Emotet M
Forensic I
Image Fil
Log Files
Wireshark
Documents and
inetpub
EML Files
From
Subject
To
Sent
Received
Size(KB)
cpentuser007@gmail...
Hello from Los Angeles
rinimatthews@gmail....
9/25/2020 5:10:00 AM
9/25/2020 5:10:00 AM
5
jasoncreek2020@gm...
Facebook Account C...
rinimatthews@gmail....
9/25/2020 7:54:24 AM
9/25/2020 7:54:24 AM
20
Mail
Hex
Properties
Message Header
MIME
HTML
RTF
Attachments
Path : C:\DFE-Tools\Evidence Files\EML Files
Date Time : 9/25/2020 5:10:00 AM
From : cpentuser007@gmail.com
To : rinimatthews@gmail.com
Cc :
Bcc :
Subject : Hello from Los Angeles
Attachment(s) :
Hi there,
How have you been? It's been a long time we met. We are going to have a business meeting in Los Angeles next month.
2 Items
9:01 AM
9/16/2025


SysTools EML Viewer v4.0 - FREEWARE
File
Help
Search
Exit
Upgrade to Pro
Switch View
Upgrade to MailXaminer
Administrator
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Floppy Disk Drive (A
Local Disk (C:)
$Recycle.Bin
DFE-Tools
DFE Module
Evidence File
EML Files
Emotet M
Forensic I
Image Fil
Log Files
Wireshark
Documents and
inetpub
EML Files
From
Subject
To
Sent
Received
Size(KB)
cpentuser007@gmail...
Hello from Los Angeles
rinimatthews@gmail....
9/25/2020 5:10:00 AM
9/25/2020 5:10:00 AM
5
jasoncreek2020@gm...
Facebook Account C...
rinimatthews@gmail....
9/25/2020 7:54:24 AM
9/25/2020 7:54:24 AM
20
Mail
Hex
Properties
Message Header
MIME
HTML
RTF
Attachments
Hi there,
 How have you been? It's been a long time we met. We are going to have a business meeting in Los Angeles next month. Let's meet up soon!

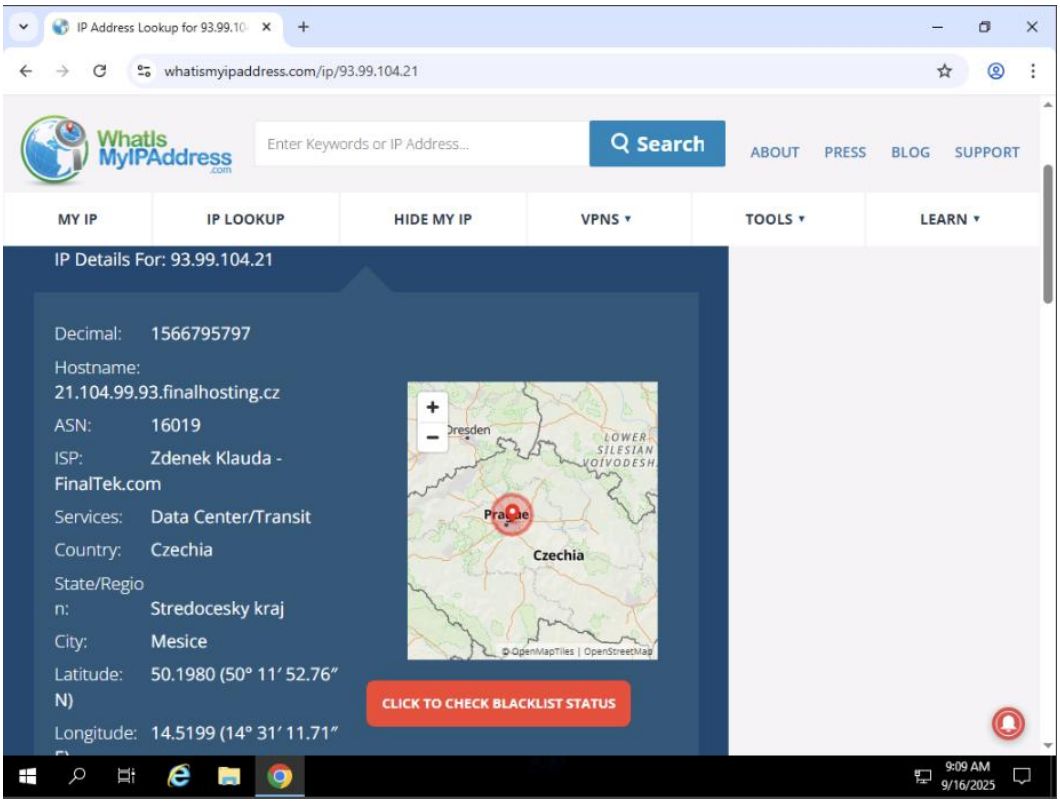
Regards.
2 Items
9:01 AM
9/16/2025

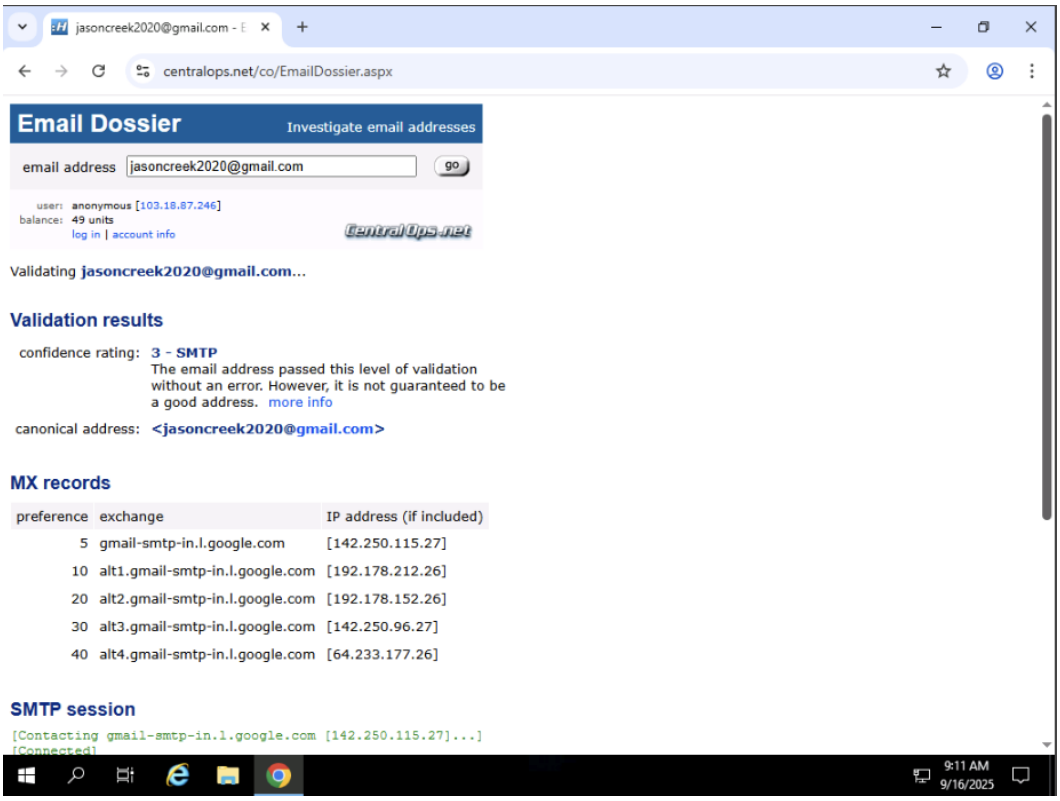

SysTools EML Viewer v4.0 - FREEWARE
File Help
Search Exit Upgrade to Pro
Switch View Upgrade to MailXaminer
EML Files
From Subject To Sent Received Size(KB)
cpentuser007@gmail... Hello from Los Angeles rinimatthews@gmail.... 9/25/2020 5:10:00 AM 9/25/2020 5:10:00 AM 5
jasoncreek2020@gm... Facebook Account C... rinimatthews@gmail.... 9/25/2020 7:54:24 AM 9/25/2020 7:54:24 AM 20
Mail Hex Properties Message Header MIME HTML RTF Attachments
Dear User,
We recently noticed some unusual login activity on your Facebook account. Therefore, for security reasons, we have disabled your account. To recovery your Facebook account, you ned to reset your password. To reset your Facebook password, either click the link given below, or read the document attached to understand how to reset it.
https://www.facebook.com/help/update_password
2 Items
9:02 AM
9/16/2025


SysTools EML Viewer v4.0 - FREEWARE
File Help
Search Exit Upgrade to Pro
Switch View Upgrade to MailXaminer
EML Files
From Subject To Sent Received Size(KB)
cpentuser007@gmail... Hello from Los Angeles rinimatthews@gmail.... 9/25/2020 5:10:00 AM 9/25/2020 5:10:00 AM 5
jasoncreek2020@gm... Facebook Account C... rinimatthews@gmail.... 9/25/2020 7:54:24 AM 9/25/2020 7:54:24 AM 20
Mail Hex Properties Message Header MIME HTML RTF Attachments
MIME-version: 1.0
Date: Fri, 25 Sep 2020 10:54:24 -0400 (EDT)
Message-ID: <20200925145424.E4B6D2753A@localhost>
Content-Type: multipart/mixed;
boundary="----------010209070306070707070903"
X-Priority: Normal
Delivered-To: rinimatthews@gmail.com
Received: by 2002:a17:906:404b:0:0:0:0 with SMTP id y11csp1233676ejj;
Fri, 25 Sep 2020 07:54:25 -0700 (PDT)
Received: from localhost ([93.99.104.21]) by mx.google.com with ESMTPS id g10si2303490edv.314.2020.09.25.07.54.25 for <rinimatthews@gmail.com>
(version=TLS1_2 cipher=ECDHE-ECDSA-CHACHA20-POLY1305 bits=256/256);
Fri, 25 Sep 2020 07:54:25 -0700 (PDT)
Received: by localhost (Postfix, from userid 33) id E4B6D2753A;
Fri, 25 Sep 2020 10:54:24 -0400 (EDT)
X-Google-Smtp-Source: ABdhPJzlgwdd55E7sWmDi+yne6X3EWf8XF9t9nNAvSeHhptiLceaFtNoCyXiiV3II+EbHGPbCc5b
X-Received: by 2002:a17:906:1484:: with SMTP id x4mr3000597ejc.81.1601045665254;
Fri, 25 Sep 2020 07:54:25 -0700 (PDT)
ARC-Seal: i=1; a="rsa-sha256"; t=1601045665; cv=none;
d="google.com"; s="arc-20160816";
b="En7NJAwQzFi550IcDtSKs9TFmNwvcWHWBrY2ePZkbOs9jDnw/5IqHaIfQc9t6b7Ix
KyOYJguhjOSQZPNigUBF7NZxqcObaAr1HRYTJHIRvHUOuGM6OtnBWo/4cVH5hDEjQdcA
2 Items
9:03 AM
9/16/2025


SysTools EML Viewer v4.0 - FREEWARE
File
Help
Search
Exit
Upgrade to Pro
Switch View
Upgrade to MailXaminer
EML Files
From
Subject
To
Sent
Received
Size(KB)
cpentuser007@gmai...
Hello from Los Angel...
rinimatthews@gmail...
9/25/2020 5:10:00 AM
9/25/2020 5:10:00 AM
5
jasoncreek2020@gm...
Facebook Account C...
rinimatthews@gmail...
9/25/2020 7:54:24 AM
9/25/2020 7:54:24 AM
20
Administrator
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Floppy Disk Drive (A
Local Disk (C:)
$Recycle.Bin
DFE-Tools
DFE Module
Evidence File
EML File
Emotet M
Forensic
Image Fi
Log Files
Wireshar
Documents and
Mail
Hex
Properties
Message Header
MIME
HTML
RTF
Attachments
Attachment
Subject
Size (KB)
Secure your Acc...
Facebook Acco...
11
Comprehensive Account Security Information
This document is intended to help you secure your Facebook account. Follow the detailed instructions in this document to recover your account, change its password, and keep it secure.
2 items
9:05 AM
9/16/2025


Instant IP Address Lookup
whatismyipaddress.com/ip-lookup
WhatIs MyIPAddress .com
Enter Keywords or IP Address...
Search
ABOUT
PRESS
PODCAST
SUPPORT
MY IP
IP LOOKUP
HIDE MY IP
VPNS
TOOLS
LEARN
Look up IP Address Location
If you can find out the IPv4 or IPv6 address of an Internet user, you can get an idea what part of the country or world they're in by using our IP Lookup tool. What to do: Enter the IP address you're curious about in the box below, then click "Get IP Details."
93.99.104.21
GET IP DETAILS
How to get someone's IP address
Once you have an IP address it is as easy as pasting and clicking above.
9:08 AM
9/16/2025


IP Address Lookup for 93.99.10
whatismyipaddress.com/ip/93.99.104.21
WhatIs MyIPAddress .com
Enter Keywords or IP Address...
Search
ABOUT
PRESS
BLOG
SUPPORT
MY IP
IP LOOKUP
HIDE MY IP
VPNS
TOOLS
LEARN
IP Details For: 93.99.104.21
Decimal: 1566795797
Hostname: 21.104.99.93.finalhosting.cz
ASN: 16019
ISP: Zdenek Klauda - FinalTek.com
Services: Data Center/Transit
Country: Czechia
State/Region: Stredocesky kraj
City: Mesice
Latitude: 50.1980 (50° 11′ 52.76″ N)
Longitude: 14.5199 (14° 31′ 11.71″
Dresden
LOWER SILESIAN VOIVODESH
Prague
Czechia
© OpenMapTiles | OpenStreetMap
CLICK TO CHECK BLACKLIST STATUS
9:09 AM
9/16/2025


jasoncreek2020@gmail.com - E
centralops.net/co/EmailDossier.aspx
Email Dossier
Investigate email addresses
email address
jasoncreek2020@gmail.com
go
user: anonymous [103.18.87.246]
balance: 49 units
log in | account info
CentralOps.net
Validating jasoncreek2020@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: <jasoncreek2020@gmail.com>
MX records
preference exchange IP address (if included)
5 gmail-smtp-in.l.google.com [142.250.115.27]
10 alt1.gmail-smtp-in.l.google.com [192.178.212.26]
20 alt2.gmail-smtp-in.l.google.com [192.178.152.26]
30 alt3.gmail-smtp-in.l.google.com [142.250.96.27]
40 alt4.gmail-smtp-in.l.google.com [64.233.177.26]
SMTP session
[Contacting gmail-smtp-in.l.google.com [142.250.115.27]...]
[Connected]
9:11 AM
9/16/2025

Module 11: Investigating Email Crimes – Summary

This lab focused on analyzing suspicious email messages to investigate potential email-based crimes, including spoofing, phishing, and fraud. Using forensic tools, investigators examined email headers, metadata, and sender details to trace the origin of a malicious email. The lab included comparing a suspicious email with a normal email to differentiate spoofed messages from genuine ones. Key objectives were to extract metadata, identify the source of the email, and evaluate its legitimacy, providing foundational skills for detecting and investigating email-related cybercrimes.