

Name: RASN Priyantha
Student Reference Number: 10899343

Module Code: PUSL3133	Module Name: Digital Forensics & Malware Analysis
Coursework Title: Forensics Report	
Deadline Date: 16 December 2024	Member of staff responsible for coursework:
Programme:	
Please note that University Academic Regulations are available under Rules and Regulations on the University website www.plymouth.ac.uk/studenthandbook .	
Group work: please list all names of all participants formally associated with this work and state whether the work was undertaken alone or as part of a team. Please note you may be required to identify individual responsibility for component parts.	
10899343 RASN Priyantha 10899273 Rajakaruna Gunawardhana 10817967 Chakrawarthi fernando 10817966 Gusthingna de silva 10899245 Deshitha D Bandara 10899307 Hewawasam Hansana We confirm that we have read and understood the Plymouth University regulations relating to Assessment Offences and that we are aware of the possible penalties for any breach of these regulations. We confirm that this is the independent work of the group.	
Signed on behalf of the group: Sasanka	
Individual assignment: I confirm that I have read and understood the Plymouth University regulations relating to Assessment Offences and that I am aware of the possible penalties for any breach of these regulations. I confirm that this is my own independent work.	
Signed:	
Use of translation software: failure to declare that translation software or a similar writing aid has been used will be treated as an assessment offence.	
I *have used/not used translation software.	
If used, please state name of software.....	
Overall mark ____% Assessors Initials ____ Date _____	

Table of Contents

Introduction.....	3
Summary of Case and Tasking	3
Statement of Compliance.....	3
Forensic Examination	3
Tools	3
Chain of Custody	3
Evidence Classes.....	4
Evidence Class 1 - .pst files	4
Evidence Class 2 - .dbx Files.....	25
Evidence Class 3 - Email Headers	31
Summary of Conclusions Reached	32
Expert Opinion Regarding Findings	32
References	33
Conclusion	34

Introduction

The purpose of this report is to provide a comprehensive forensic analysis of the unauthorized access incident involving sensitive financial data at ABC Company. The investigation will cover the handling, examination, and analysis of digital evidence, ensuring that the findings are thorough, accurate, and legally admissible in court. This report will also recommend security measures to prevent future incidents and ensure the integrity of the company’s data.

Summary of Case and Tasking

ABC Company’s CFO reported an alarming incident involving unauthorized access to sensitive financial data. Unusual network activity was detected on a junior financial analyst's computer, including the transfer of critical financial files to an unknown external IP address during non-business hours. The CFO suspects that important financial documents, including customer financial statements, bank account details, and upcoming financial forecasts, may have been accessed or copied without authorization.

Our task as forensic examiners is to investigate the breach, uncover the extent of the unauthorized access, and determine which sensitive data has been exposed. This involves analysing the provided evidence, such as .pst and .dbx email files, and preparing a detailed report for legal proceedings. The report will also include immediate recommendations and long-term practices to strengthen the company's cybersecurity measures.

Statement of Compliance

This forensic investigation report complies with established standards for digital forensics to ensure the integrity of the evidence and the validity of the findings. All investigative actions have been documented to maintain transparency and uphold the legal admissibility of the evidence. The report is written impartially, and the conclusions are drawn based on a thorough and systematic analysis of the evidence, following best practices to ensure the protection of both the company and legal authorities involved.

Forensic Examination

The forensic examination focused on analyzing digital evidence, including email files (.pst and .dbx), and email headers contained in a .docx file, to determine the extent of unauthorized access to sensitive financial data.

Tools

The Forensics tools employed in the performance of this investigation were as follows:

SysTool Outlook PST Viewer v5.0: Used for analyzing .pst files and extracting email contents and metadata.

SysTools MailXaminer: Applied for cross-verifying PST data and ensuring accuracy in email structure.

4n6 DBX Forensics Wizard: Analyzed .dbx files to retrieve critical email information stored in Outlook Express.

VirusTotal: Scanned email attachments and URLs for potential malware or malicious content.

Criminal IP: Investigated IP addresses and URLs for signs of malicious activity and origin.

AbusIP: Tracked suspicious IP addresses linked to unauthorized activities.

Whois Lookup: Performed to gather information on domains and IP addresses to validate their authenticity.

JPEGsnoop: Analyzed images.

Chain of Custody

Evidence ID	Description	Collected By	Date/Time	Location	Action	Handled By	Remarks
E001	Material.zip (main folder)	RASN Priyantha	2024-11-25, 2:00 PM	Personal System	Downloaded via link	RASN Priyantha	Verified integrity

							before analysis
E002	Target1.pst (PST file)	RASN Priyantha	2024-11-28, 9:00 PM	Secure Analysis Folder	Analyzed using SysTools & Mailxaminer	RASN Priyantha	Analyzed using SysTools Outlook PST Viewer. MD5 hash recorded for integrity verification.
E003	Target2.pst (PST file)	RASN Priyantha	2024-12-01, 9:00 PM	Secure Analysis Folder	Analyzed using SysTools	RASN Priyantha	Analyzed with SysTools. SHA256 hash verified to ensure no changes during analysis.
E004	.dbx files (5 in total)	RASN Priyantha	2024-12-03, 9:00 PM	Secure Analysis Folder	Analyzed with 4n6 DBX Wizard	RASN Priyantha	Analyzed using 4n6 DBX Wizard, results logged for later report use.
E005	Emailheader.docx	RASN Priyantha	2024-12-05, 9:00 PM	Secure Analysis Folder	Examined using Email Tracker Pro	RASN Priyantha	Email header details parsed for further investigation.

Evidence Classes

Digital evidence in this investigation is categorized into classes based on its format and relevance. This ensures a structured approach to analysis, allowing efficient identification and interpretation of critical findings. The primary evidence classes in this case include .pst files, .dbx files, and email headers. Each class has been analyzed meticulously to identify potential misuse, unauthorized access, and other significant activities.

Evidence Class 1 - .pst files

Overview

The .pst files provided for analysis, namely target1.pst and target2.pst, are Microsoft Outlook data files. These files contain emails that serve as a crucial source of information regarding communications conducted during the timeframe of the reported breach. Both .pst files were examined using SysTools Outlook PST Viewer 5.0 and MailXaminer to preserve integrity and ensure detailed analysis.

Analysis of target1.pst

Extracting target1.pst Using SysTools Outlook PST Viewer

The target1.pst file was opened using SysTools Outlook PST Viewer 5.0, which provided access to the email data stored within the file. The tool displayed the file's folder structure, revealing that only emails were present, and there were no contacts, events, or calendar entries. This is noted because .pst files typically store such information, but in this case, the focus was solely on the email data.

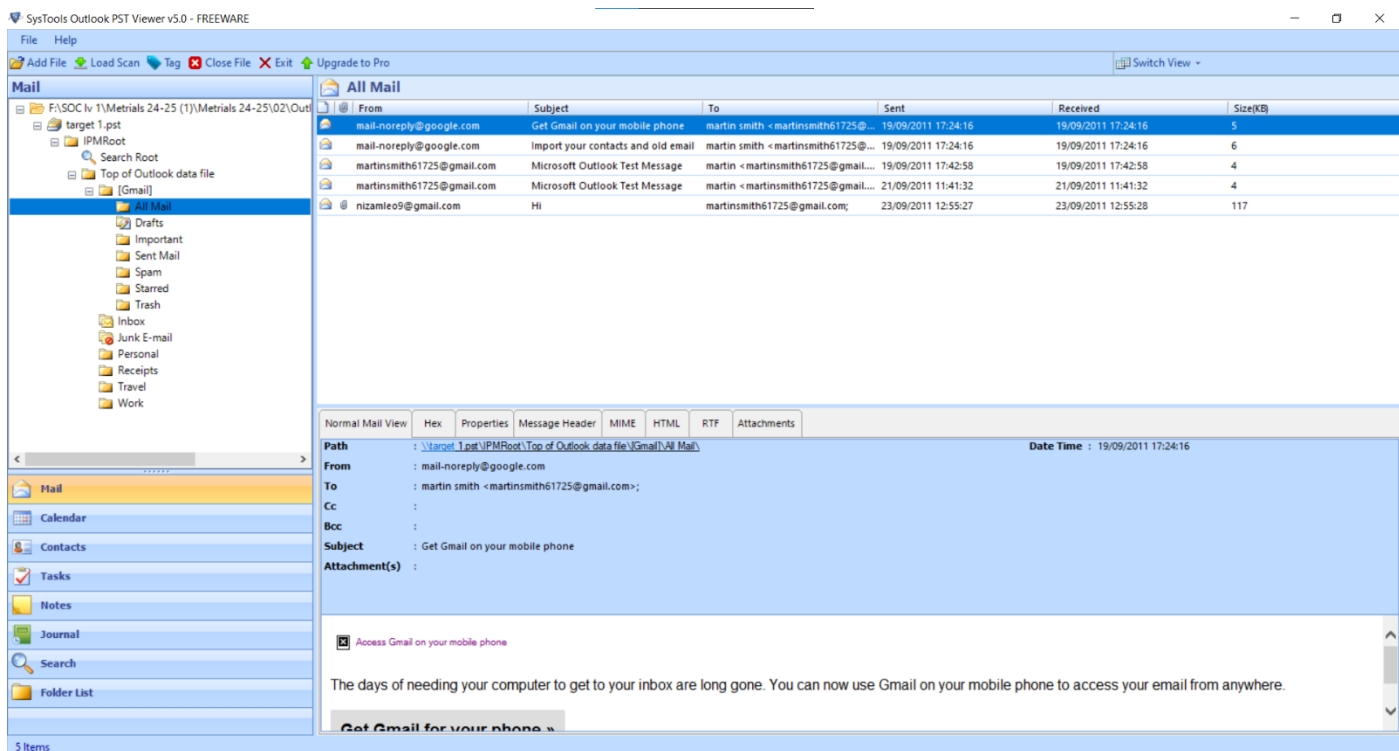


Figure 1: Expanded Structure of target1.pst File Using SysTools Outlook PST Viewer 5.0 (Freeware).

Reviewing the Emails Content

After extracting the emails, the content was reviewed to identify relevant communication and metadata.

Google-Generated Emails Analysis

Gmail Email – Mobile Access Notification

The email appears as a typical Gmail promotional message, with a clean layout featuring a brief text informing the recipient about accessing Gmail on mobile devices, accompanied by a clickable link to learn more. It does not contain any suspicious content or unusual formatting in the default view.

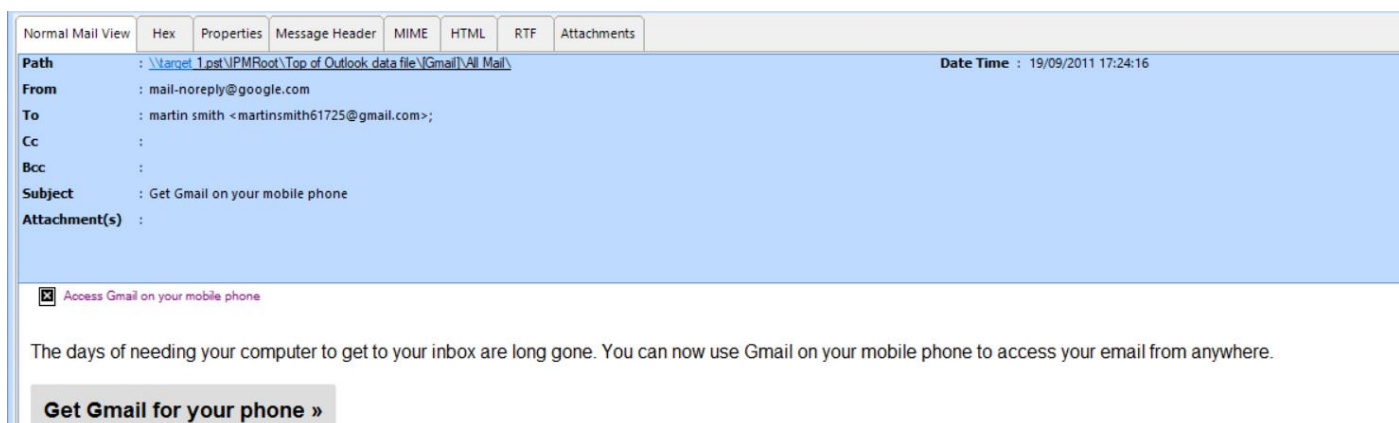


Figure 2: Default View of the Gmail Email – “Access Gmail on Mobile”.

Email Header Analysis

A detailed header analysis was performed to verify the authenticity of the email.

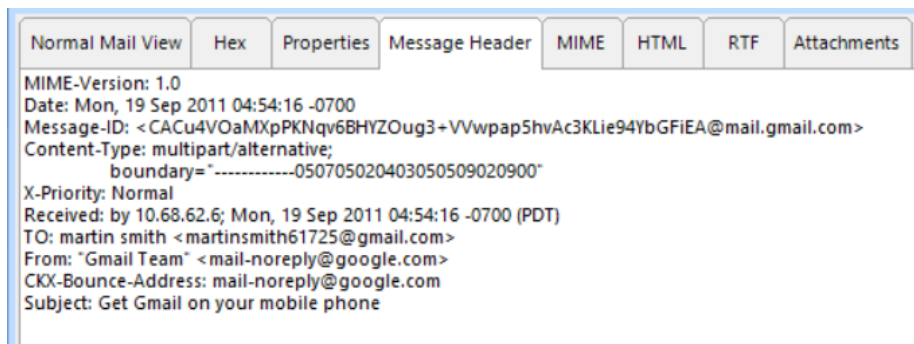


Figure 3: Email Header Analysis.

Route Path:

The email traveled through Gmail's internal infrastructure, with the first server receiving it at IP 10.68.62.6. Although SPF is not explicitly shown in the header, the email likely passed through Gmail's servers before being delivered to the recipient's inbox.

Received IP: 10.68.62.6 (Private/Bogon IP)

This IP address is part of the private IP range (as defined by IETF), typically used within internal networks. While it is possible that this IP is used by Google's infrastructure, we cannot definitively confirm this because it is a private, non-routable IP address.

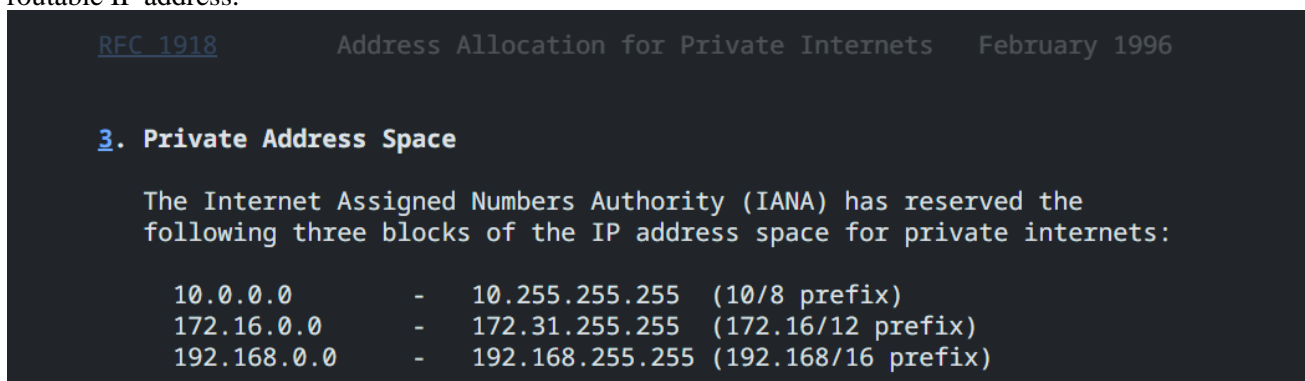


Figure 4: Diagram of Private IP Address Ranges from RFC 1918.

Authentication:

- SPF (Sender Policy Framework): Not explicitly mentioned in header. While it is likely that the email passed SPF, there is no explicit SPF record mentioned in the header.
- DKIM (DomainKeys Identified Mail): Missing. The absence of a DKIM signature means that the email's authenticity could not be cryptographically verified.
- DMARC (Domain-based Message Authentication, Reporting, and Conformance): Not present in the email header, providing no additional layer of protection against spoofing.

Time and Delivery:

- Sent Time: Mon, 19 Sep 2011 04:54:16 -0700 (Pacific Daylight Time, PDT)
- Received Time: Mon, 19 Sep 2011 12:54:16 +0530 (Indian Standard Time, IST)
- Transmission Time: No significant delays observed, suggesting the email was delivered promptly.

Message Details:

- Subject: "Get Gmail on your mobile phone"
- From: Gmail Team (mail-noreply@google.com)
- To: martinsmith61725@gmail.com
- Message ID: The Message-ID is a unique identifier assigned by the email server. It contains the domain "gmail.com," which is associated with Gmail's email servers. This suggests that the email was likely generated by Gmail's infrastructure.

Message-IDs, if present, are generated by the client program sending the email^[2] or by the first mail server.^[3] A common method of generating such ID is by combining the time and domain name, for example: 950124.162336@example.com.^[4]

Figure 5: This shows the Message-ID generation process, sourced from Wikipedia.

Body Details

Text Content:

Content-Type: text/plain; charset=iso-8859-1

Encoding: 7bit (Standard encoding)

Message Body: The plain text body of the email is minimal, simply stating: "Get Gmail on your mobile phone".

HTML Content:

Content-Type: text/html; charset=iso-8859-1

Encoding: quoted-printable

HTML Body:

```
Normal Mail View  Hex  Properties  Message Header  MIME  HTML  RTF  Attachments
<html>
<font face="Arial, Helvetica, sans-serif">
<p>
<a href="http://www.google.com/intl/en/mobile/default/mail.html">
  
</a>
</p>
<p>The days of needing your computer to get to your inbox are long gone. You can
now use Gmail on your mobile phone to access your email from anywhere.</p>

<table cellpadding="0" cellspacing="0">
  <col style="width: 1px;"/>
  <col/>
  <col style="width: 1px;"/>
  <tr>
    <td></td>
    <td height="1px" style="background-color: #ddd"></td>
    <td></td>
  </tr>
  <tr>
    <td style="background-color: #ddd"></td>
    <td background="https://mail.google.com/mail/images/welcome-button-background.png"
      style="background-color: #ddd; background-repeat: repeat-x;
      padding: 10px; font-size: larger">
      <a href="http://www.google.com/intl/en/mobile/default/mail.html#utm_source=wel-eml&utm_medium=eml&utm_campaign=en"
        style="font-weight: bold; color: #000; text-decoration: none;
        display: block;">
        Get Gmail for your phone &#187;</a>
    </td>
    <td style="background-color: #ddd"></td>
  </tr>
  <tr>
    <td></td>
    <td height="1px" style="background-color: #ddd"></td>
    <td></td>
  </tr>
</table>
</p>
</font>
</html>
```

Figure 6: HTML View of the Email Body.

URL and Domain Validation

http://www.google.com/intl/en/mobile/default/mail.html#utm_source=wel-eml&utm_medium=eml&utm_campaign=en

The URL redirects to a legitimate Google service page, operating on the trusted "google.com" domain, registered with MarkMonitor Inc. since 1997. It uses valid SSL certificates, secure HTTPS with TLS 1.3, and QUIC protocols, ensuring encrypted communication. The associated IPs are part of Google's infrastructure, with no signs of malicious activity. While there are no hidden elements, suspicious scripts, or credential traps, a "suspicious" favicon and one phishing record require attention. There is no indication of invalid SSL, fake domains, or obfuscated content.

URL		HTML	
URL with IP	0	Hidden Element	0
Suspicious Length	False	Hidden Iframe	0
DGA Score	0	Iframe	0
URL with @	False	Obfuscated Script	0
URL with Multiple http	False	Suspicious HTML Element	0
URL with PunyCode	False	Suspicious Program	0
Probability of Phishing URL	0.01%	Button Trap	Normal
Common		Credential Input Form	Safe
Fake Domain	False	Form Event	1
Invalid SSL	False	Fake Favicon	Suspicious
MITM Attack	False	Page Warning ?	False
Locations	United States	Suspicious Footer ?	False
Newborn Domain	N/A	Email Domain Check ?	False
Abuse Record	0	Network	
Phishing Record	1	Redirection to another AS	0
Mail Server	True	Redirection to another country	0
Spam (SPF1 Result)	Safe	Redirection to another domain	0
Site Reputation	1	Suspicious Cookie	False

Figure 7: Criminal IP Scan Summary for the URL.


www.google.com

- Title: **Error 404 (Not Found)!!1**
- JARM Hash: **27d40d40d29d40d1dc42d43d00041d4689ee210389f4f6...**
- Inserted: **http://www.google.com/intl/en/mobile/default/mail.html#utm_medium%3Ddeml%26utm_campaign%3Den** ^
- Redirect to: **https://www.google.com/intl/en/mobile/default/mail.html#utm_medium%3Ddeml%26utm_campaign%3Den** ^

 Domain created: 1997-09-15
 Domain Registrar: MarkMonitor Inc.




Figure 7.1: Redirection Path Overview.

<http://www.google.com/intl/en/mobile/default/mail.html>

The analysis confirms the URL is legitimate, hosted on "google.com," and secured with valid SSL certificates and modern encryption protocols (TLS 1.3). Associated IPs belong to Google's safe infrastructure. The site has no hidden elements, obfuscated scripts, or phishing indicators.

A minor issue with a "suspicious" favicon and one historical phishing record is noted, but there is no evidence of active threats. These points merit monitoring, but the overall risk is minimal.

URL		HTML	
URL with IP	0	Hidden Element	0
Suspicious Length	False	Hidden Iframe	0
DGA Score	0	Iframe	0
URL with @	False	Obfuscated Script	0
URL with Multiple http	False	Suspicious HTML Element	0
URL with PunyCode	False	Suspicious Program	0
Probability of Phishing URL	0.1%	Button Trap	Normal
Common		Credential Input Form	Safe
Fake Domain	False	Form Event	1
Invalid SSL	False	Fake Favicon	Suspicious
MITM Attack	False	Page Warning	False
Locations	United States	Suspicious Footer	False
Newborn Domain	N/A	Email Domain Check	False
Abuse Record	0	Network	
Phishing Record	1	Redirection to another AS	0
Mail Server	True	Redirection to another country	0
Spam (SPF1 Result)	Safe	Redirection to another domain	0
Site Reputation	1	Suspicious Cookie	False

Figure 8: Criminal IP Scan Summary for the URL.

 **www.google.com**

- Title: Error 404 (Not Found)!!1
- JARM Hash: 27d40d40d29d40d1dc42d43d00041d4689ee210389f4f6...
- Inserted: <http://www.google.com/intl/en/mobile/default/mail.html>
- Redirect to: <https://www.google.com/intl/en/mobile/default/mail.html>

 Domain created: 1997-09-15

 Domain Registrar: MarkMonitor Inc.


Google
THE INFORMATION ON THIS PAGE IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND IS NOT INTENDED TO BE USED FOR ANY OTHER PURPOSE.



Figure 8.1: Redirection Path Overview.

Gmail Email – Import Contacts and Old Email Notification

The email is a promotional message from Gmail, offering to import contacts and emails from services like Yahoo!, Hotmail, and AOL. It provides a seamless transition, with imports running for 30 days, and includes a call-to-action button for starting the process.

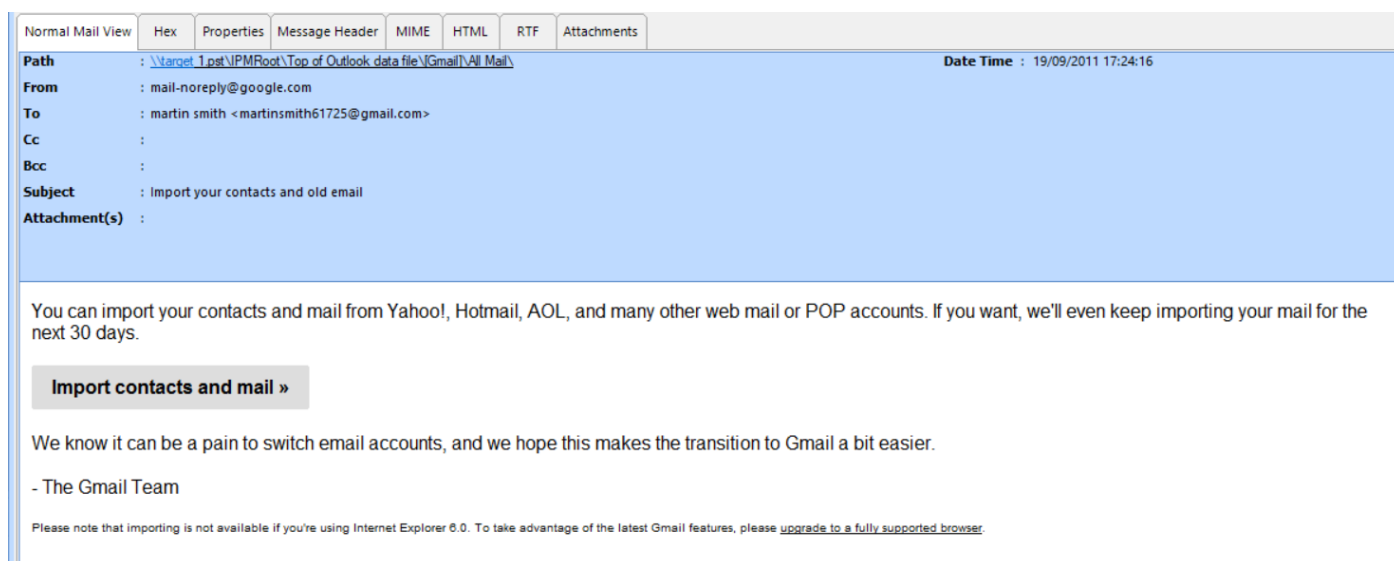


Figure 9: Default View of Gmail Email – “Import your contacts and old email”.

Email Header Analysis

A detailed header analysis was performed to verify the authenticity of the email.

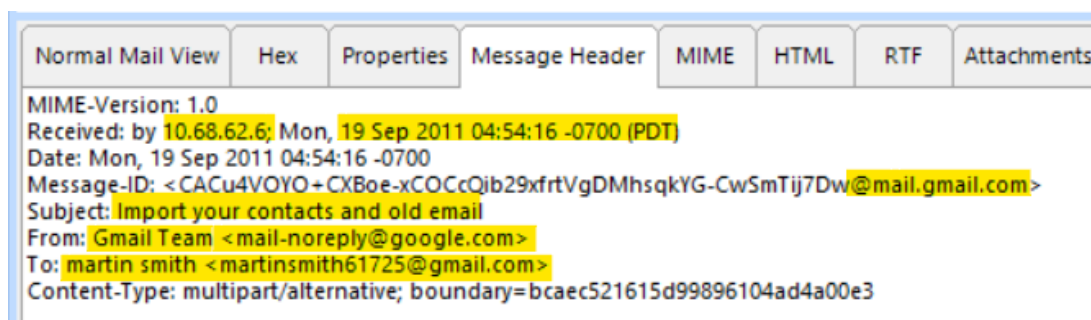


Figure 10: Email Header Analysis.

Route Path:

The route path is the same as that of the previous email.

Authentication:

No authentication mechanism is provided, similar to the previous email.

Time and Delivery:

Both emails share the same timestamp.

Message Details:

- Subject: " Import your contacts and old email"
- The sender and receiver are the same as in the previous email, with a unique Message-ID, but the domain remains consistent with the previous email.

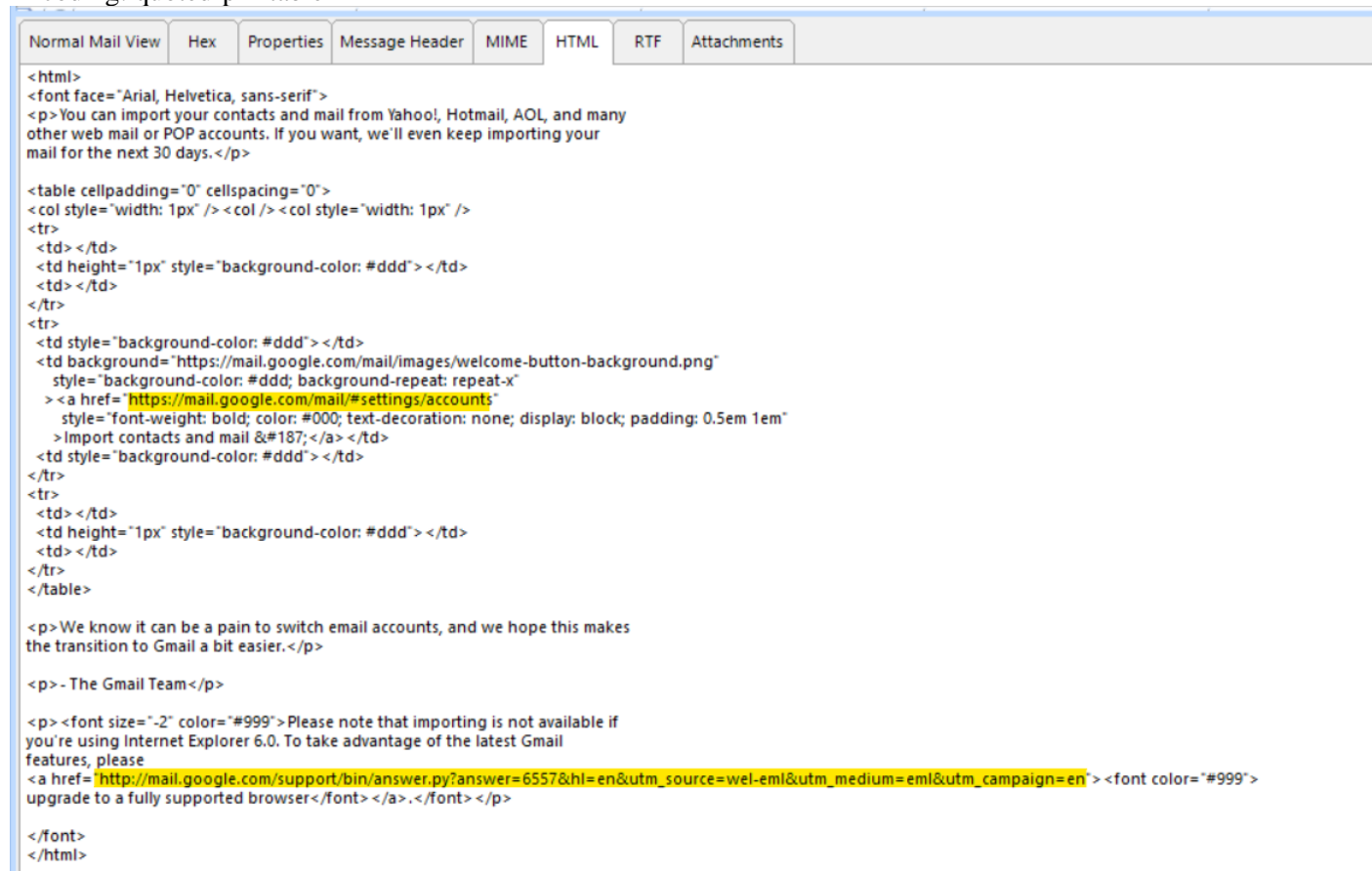
Body Details:

Email encourages users to import contacts and emails from other services like Yahoo!, Hotmail, and AOL, offering continuous import for 30 days. A button is provided to start the import process, linking to Gmail's account settings. A note reminds users to upgrade from Internet Explorer 6.0 for full functionality. The links and image are hosted on Gmail's official domain, suggesting the email is legitimate like the previous email.

HTML Content

Content-Type: text/html; charset=iso-8859-1

Encoding: quoted-printable



```
<html>
<font face="Arial, Helvetica, sans-serif">
<p>You can import your contacts and mail from Yahoo!, Hotmail, AOL, and many
other web mail or POP accounts. If you want, we'll even keep importing your
mail for the next 30 days.</p>

<table cellpadding="0" cellspacing="0">
<col style="width: 1px" /><col /><col style="width: 1px" />
<tr>
<td></td>
<td height="1px" style="background-color: #ddd"></td>
<td></td>
</tr>
<tr>
<td style="background-color: #ddd"></td>
<td background="https://mail.google.com/mail/images/welcome-button-background.png"
style="background-color: #ddd; background-repeat: repeat-x"
><a href="https://mail.google.com/mail/#settings/accounts"
style="font-weight: bold; color: #000; text-decoration: none; display: block; padding: 0.5em 1em"
>Import contacts and mail &#187;</a></td>
<td style="background-color: #ddd"></td>
</tr>
<tr>
<td></td>
<td height="1px" style="background-color: #ddd"></td>
<td></td>
</tr>
</table>

<p>We know it can be a pain to switch email accounts, and we hope this makes
the transition to Gmail a bit easier.</p>

<p>- The Gmail Team</p>

<p><font size="-2" color="#999">Please note that importing is not available if
you're using Internet Explorer 6.0. To take advantage of the latest Gmail
features, please
<a href="http://mail.google.com/support/bin/answer.py?answer=6557&hl=en&utm_source=wel-emi&utm_medium=emi&utm_campaign=en"><font color="#999">
upgrade to a fully supported browser</font></a>.</font></p>

</font>
</html>
```

Figure 11: HTML View of the Email Body.


URL and Domain Validation

The URL redirects to a legitimate Google sign-in page with a secure HTTPS connection, valid SSL certificates, and a domain registered with MarkMonitor Inc. since 1997. The page uses TLS 1.3 and HTTP/3, ensuring encrypted traffic. No signs of phishing, malware, or suspicious elements were detected, though a "suspicious" favicon and page warning do not indicate malicious intent.







URL

URL with IP	0
Suspicious Length	False
DGA Score	0
URL with @	False
URL with Multiple http	False
URL with PunyCode	False
Probability of Phishing URL	0.01%

Common

Fake Domain	False
Invalid SSL	False
MITM Attack	False
Locations	 United States
Newborn Domain	N/A
Abuse Record	0
Phishing Record	0
Mail Server	False
Spam (SPF1 Result)	N/A
Site Reputation	1

HTML

Hidden Element	0
Hidden Iframe	0
Iframe	0
Obfuscated Script	 5
Suspicious HTML Element	0
Suspicious Program	0
Button Trap	Normal
Credential Input Form	Safe
Form Event	 1
Fake Favicon	 Suspicious
Page Warning	 True
Suspicious Footer	 False
Email Domain Check	 False

Network

Redirection to another AS	0
Redirection to another country	0
Redirection to another domain	0
Suspicious Cookie	False

Figure 12: Criminal IP Scan Summary for the URL.

mail.google.com

- Title: Gmail
- JARM Hash: 27d40d40d29d40d1dc42d43d00041d4689ee210389f4f6...
- Inserted: <https://mail.google.com/mail/#settings%2Faccounts>
- Redirect to: <https://accounts.google.com/v3/signin/identifier?continue=https://mail.google.com/mail/u/0/&ddm=1&dsh=S-467061313:1733816860178624&emr=1&flowEntry=ServiceLogin&flowName=GlifWebSignIn&followup=https://mail.google.com/mail/u/0/&ifkv=AcMMx-f0bqdujQYF7DLBDXgd6RdBpFNxT4yo7fSfju81voMc0qrBdDvUtlUaokmdHOBriFxmZlQ&osid=1&passive=1209600&service=mail#settings%2Faccounts>

✓ Domain created: 1997-09-15

⊕ Domain Registrar: MarkMonitor Inc.

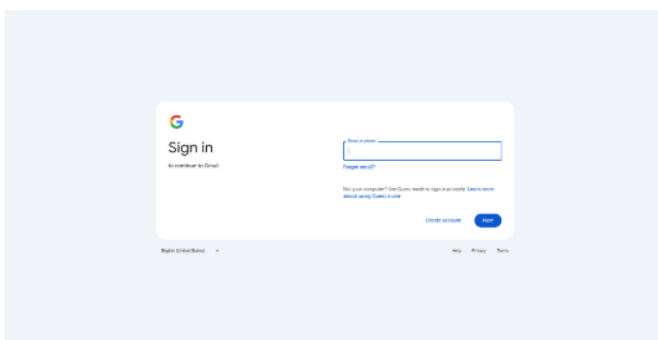



Figure 13.1: Redirection Path Overview.


The domain is hosted by Google, with valid SSL/TLS certificates and full HTTPS support. There are no significant signs of phishing or malicious activity, although a suspicious favicon and obfuscated scripts were detected. However, these minor issues do not present immediate risks.


URL		HTML	
URL with IP	0	Hidden Element	0
Suspicious Length	False	Hidden Iframe	0
DGA Score	0	Iframe	0
URL with @	False	Obfuscated Script	4
URL with Multiple http	False	Suspicious HTML Element	3
URL with PunyCode	False	Suspicious Program	0
Probability of Phishing URL	0.01%	Button Trap	Normal
Common		Credential Input Form	Safe
Fake Domain	False	Form Event	1
Invalid SSL	False	Fake Favicon	Suspicious
MITM Attack	False	Page Warning	True
Locations	United States	Suspicious Footer	False
Newborn Domain	N/A	Email Domain Check	True
Abuse Record	0	Network	
Phishing Record	0	Redirection to another AS	0
Mail Server	False	Redirection to another country	0
Spam (SPF1 Result)	N/A	Redirection to another domain	0
Site Reputation	1	Suspicious Cookie	False

Figure 14: Criminal IP Scan Summary for the URL.


mail.google.com

- Title: [Sorry, this page can't be found. - Gmail Help](#)
- JARM Hash: 27d40d40d29d40d1dc42d43d00041d4689ee210389f4f6...
- Inserted: http://mail.google.com/support/bin/answer.py?answer=3D6557&hl=3D=%20en&utm_campaign=3Den&utm_medium=3Deml
- Redirect to: https://support.google.com/mail/answer/3D6557?hl=3D=%20en&utm_campaign=3Den&utm_medium=3Deml

 Domain created: 1997-09-15

 Domain Registrar: MarkMonitor Inc.

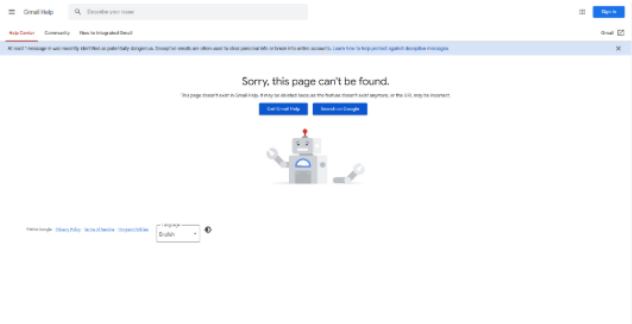


Figure 14.1: Phishing Email Analysis Overview.

The two analyzed emails, sent from mail-noreply@google.com to martinsmith61725@gmail.com, were legitimate communications from Google. Header analysis confirmed routing via Gmail's internal infrastructure, using private IPs. Although SPF, DKIM, and DMARC records were absent, no tampering or malicious activity was detected.

Overall, the emails are authentic, with no evidence of threats or unauthorized activities.

External Email

The email appears as a simple personal message from a friend, containing a brief greeting and an image attachment, with no suspicious content or unusual formatting in the normal view.

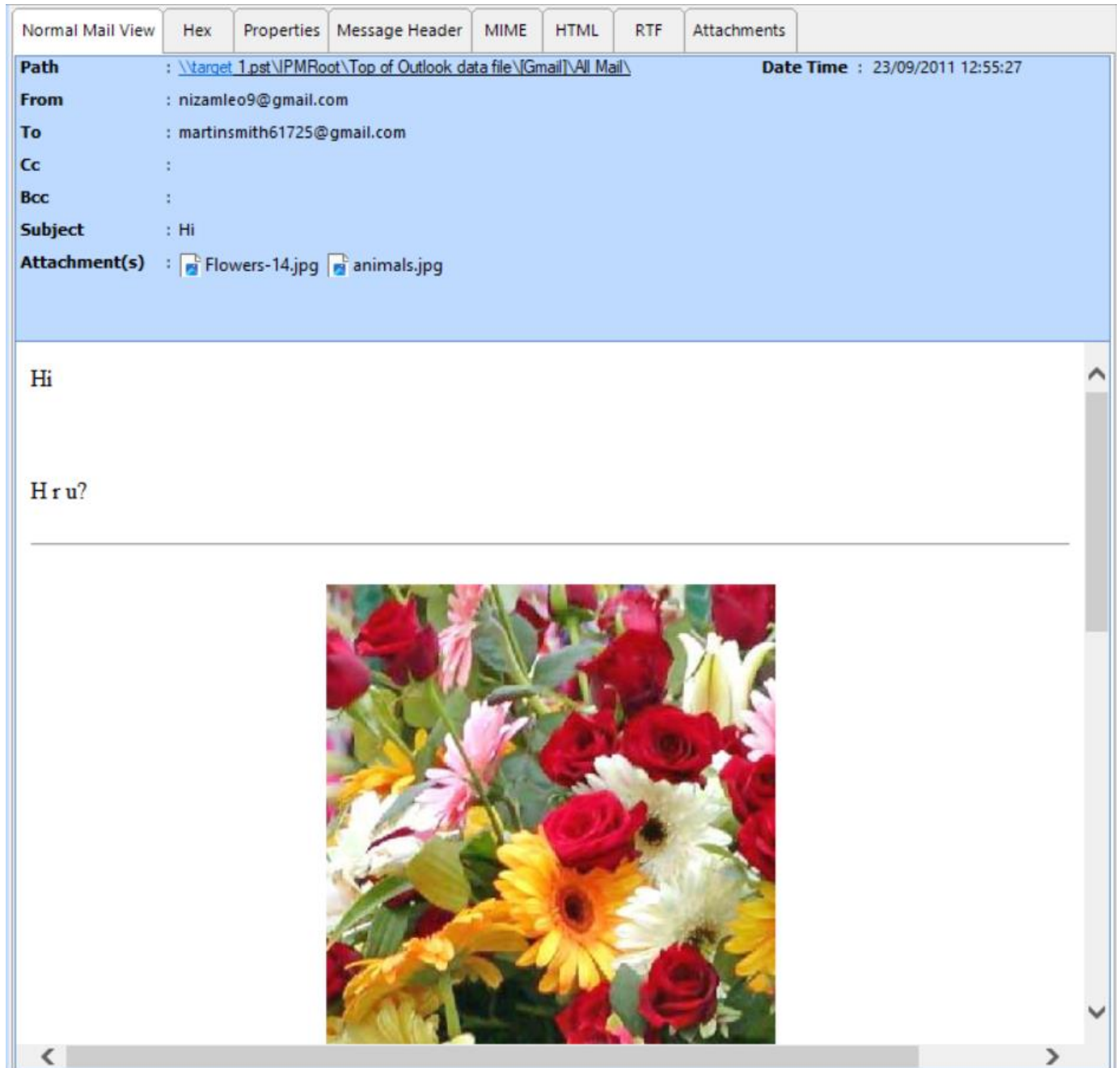


Figure 15: Default View of the External Email.

Email Header Analysis



Figure 16: Email Header Analysis.

Route Path:

The email traveled through Gmail's internal network. It was first received by the server at IP 10.42.131.7, which performed the SPF check and passed it. The email then passed through another internal Gmail server at IP 10.68.62.6 before reaching the recipient's inbox. The originating server at IP 10.42.96.132 handled email submission via Gmail's web interface.

Authentication:

- SPF: Passed. The email was sent from a permitted sender (10.42.131.7), verified by Gmail's SPF record.
- DKIM: Passed. The email's content was signed by Gmail's servers, and its integrity was maintained.

Time and Delivery:

- Sent Time: Fri, 23 Sep 2011 12:55:27 +0530 (Indian Standard Time, IST).
- Received Time: Fri, 23 Sep 2011 00:25:28 -0700 (Pacific Standard Time, PST).
- Transmission Time: Minimal delay observed, indicating a prompt delivery with no issues.

Message Details:

- Message-ID: A unique identifier assigned to this email within the Gmail domain.
- Subject: "Hi".
- From: nizam leo9 <nizamleo9@gmail.com>.
- To: martinsmith61725@gmail.com.
- Content-Type: Multipart message (indicates the email may contain both text and attachments).

Body Details:

Text Content:

Content-Type: text/plain; charset=iso-8859-1

Encoding: 7bit (Standard encoding)

The plain text content of the email is simple and consists of the message "Hi H r u?".

This message appears informal and contains minimal content.

HTML Content:

Content-Type: text/html; charset=iso-8859-1

Encoding: quoted-printable

To: martinsmith61725@gmail.com
From: "nizam leo9" <nizamleo9@gmail.com>
CKX-Bounce-Address: nizamleo9@gmail.com
Subject: Hi

-----010406030108040302040509
Content-Type: multipart/alternative;
boundary="-----010906030008070403040606"

-----010906030008070403040606
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: 7bit

-----010906030008070403040606
Content-Type: text/html; charset=iso-8859-1
Content-Transfer-Encoding: quoted-printable

<html><head><META http-equiv=3D"Content-Type" content=3D"text/html; charset=
=3Diso-8859-1"></head><body>Hi

H r u?

</body></html>

-----010906030008070403040606--

-----010406030108040302040509
Content-Type: image/jpeg; name="Flowers-14.jpg"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="Flowers-14.jpg"

Figure 17: HTML View of the Email Body.

Attachments Analysis:

Attachment 1:

File Name: Flowers-14.jpg

Content-Type: image/jpeg

Encoding: base64

Disposition: Attachment

The image is embedded as a base64-encoded JPEG file.

The JPEG file "Flowers-14.jpg" exhibits standard image characteristics, including typical metadata (APP0, APP12, APP14) and uses baseline DCT compression with Huffman tables, suggesting it is legitimate. The file's metadata does not show any signs of manipulation, indicating no obvious tampering or unauthorized alterations.


```

Start Offset: 0x00000000
*** Marker: SOI (xFFD8) ***
  OFFSET: 0x00000000

*** Marker: APP0 (xFFE0) ***
  OFFSET: 0x00000002
  Length      = 16
  Identifier   = [JFIF]
  version     = [1.2]
  density     = 100 x 100 (aspect ratio)
  thumbnail   = 0 x 0

*** Marker: APP12 (xFFEC) ***
  OFFSET: 0x00000014
  Length      = 17
  Identifier   = [Ducky]
  Photoshop Save For Web Quality = [25]

*** Marker: APP14 (xFFEE) ***
  OFFSET: 0x00000027
  Length      = 14
  DCTEncodeVersion = 100
  APP14Flags0    = 49152
  APP14Flags1    = 0
  ColorTransform = 1 [YCbCr]

*** Marker: DQT (xFFDB) ***
  Define a Quantization Table.
  OFFSET: 0x00000037
  Table length = 132
  ----
  Precision=8 bits
  Destination ID=0 (Luminance)
  DQT, Row #0: 17 13 13 18 26 31 34 35
  DQT, Row #1: 13 14 14 17 23 23 27 35
  DQT, Row #2: 13 14 15 18 23 30 41 54
  DQT, Row #3: 18 17 18 23 29 42 54 65
  DQT, Row #4: 26 23 23 29 45 59 65 65
  DQT, Row #5: 31 23 30 42 59 65 65 65
  DQT, Row #6: 34 27 41 54 65 65 65 65
  DQT, Row #7: 35 35 54 65 65 65 65 65
  Approx quality factor = 62.01 (scaling=75.98 variance=637.58)
  ----
  Precision=8 bits
  Destination ID=1 (Chrominance)
  DQT, Row #0: 18 17 20 24 23 29 43 56
  DQT, Row #1: 17 22 21 19 23 29 40 50
  DQT, Row #2: 20 21 23 25 29 35 53 60
  DQT, Row #3: 24 19 25 32 35 45 60 65
  DQT, Row #4: 23 23 29 35 45 56 65 65
  DQT, Row #5: 29 29 35 45 56 65 65 65
  DQT, Row #6: 43 40 53 60 65 65 65 65
  DQT, Row #7: 56 50 60 65 65 65 65 65
  Approx quality factor = 73.54 (scaling=52.92 variance=423.66)

*** Marker: SOS (Start of Scan) (xFFDA) ***
  OFFSET: 0x00000176
  Scan header length = 12
  Number of img components = 3
    Component[1]: selector=0x01, table=0(DC),0(AC)
    Component[2]: selector=0x02, table=1(DC),1(AC)
    Component[3]: selector=0x03, table=1(DC),1(AC)
  Spectral selection = 0 .. 63
  Successive approximation = 0x00

*** Decoding SCAN Data ***
  OFFSET: 0x00000184
  Scan Decode Mode: No IDCT (DC only)
  NOTE: Low-resolution DC component shown. Can decode full-res with [Options->Scan Segment->Full IDCT]

  Scan Data encountered marker 0xFFD9 @ 0x00004CA7.0

  Compression stats:
    Compression Ratio: 16.74:1
    Bits per pixel: 1.43:1

  Huffman code histogram stats:
    Huffman Table: (Dest ID: 0, Class: DC)
      # codes of length 01 bits: 0 ( 0%)
      # codes of length 02 bits: 814 ( 47%)
      # codes of length 03 bits: 707 ( 40%)
      # codes of length 04 bits: 111 ( 6%)
      # codes of length 05 bits: 99 ( 6%)
      # codes of length 06 bits: 17 ( 1%)
      # codes of length 07 bits: 0 ( 0%)
      # codes of length 08 bits: 0 ( 0%)
      # codes of length 09 bits: 0 ( 0%)
      # codes of length 10 bits: 0 ( 0%)
      # codes of length 11 bits: 0 ( 0%)
      # codes of length 12 bits: 0 ( 0%)
      # codes of length 13 bits: 0 ( 0%)
      # codes of length 14 bits: 0 ( 0%)
      # codes of length 15 bits: 0 ( 0%)
      # codes of length 16 bits: 0 ( 0%)

    Huffman Table: (Dest ID: 1, Class: DC)
      # codes of length 01 bits: 0 ( 0%)
      # codes of length 02 bits: 573 ( 66%)
      # codes of length 03 bits: 151 ( 17%)
      # codes of length 04 bits: 73 ( 8%)
      # codes of length 05 bits: 73 ( 8%)
      # codes of length 06 bits: 4 ( 0%)
      # codes of length 07 bits: 0 ( 0%)
      # codes of length 08 bits: 0 ( 0%)
      # codes of length 09 bits: 0 ( 0%)
      # codes of length 10 bits: 0 ( 0%)
      # codes of length 11 bits: 0 ( 0%)
      # codes of length 12 bits: 0 ( 0%)
      # codes of length 13 bits: 0 ( 0%)
      # codes of length 14 bits: 0 ( 0%)
      # codes of length 15 bits: 0 ( 0%)
      # codes of length 16 bits: 0 ( 0%)

```

```

YCC clipping in DC:
Y component: [<0= 0] [>255= 0]
Cb component: [<0= 0] [>255= 0]
Cr component: [<0= 0] [>255= 0]

RGB clipping in DC:
R component: [<0= 0] [>255= 0]
G component: [<0= 0] [>255= 0]
B component: [<0= 0] [>255= 0]

Average Pixel Luminance (Y):
Y=[125] (range: 0..255)

Brightest Pixel Search:
YCC=[ 1020, -36, 0] RGB=[255,255,246] @ MCU[ 17, 3]

Finished Decoding SCAN Data
Number of RESTART markers decoded: 0
Next position in scan buffer: Offset 0x00004CA6.3

*** Marker: EOI (End of Image) (xFFD9) ***
OFFSET: 0x00004CA7

*** Searching Compression Signatures ***

Signature: 019CC391D4B06A06E29474EA82801C4A
Signature (Rotated): 019CC391D4B06A06E29474EA82801C4A
File Offset: 0 bytes
Chroma subsampling: 2x2
EXIF Make/Model: NONE
EXIF Makernotes: NONE
EXIF Software: NONE

Searching Compression Signatures: (3347 built-in, 0 user(*) )

EXIF.Make / Software      EXIF.Model      Quality      Subsamp Match?
-----
SW : [Adobe Photoshop -Win ]      [Save For Web 025]

NOTE: Photoshop IRB detected
Based on the analysis of compression characteristics and EXIF metadata:

ASSESSMENT: Class 1 - Image is processed/edited

```

Image (RGB, DC) @ 12.5% (1/8)



Figure 18: JPEG File Analysis of "Flowers.jpg" using JPEGsnoop.

Attachment 2:

File Name: animals.jpg

Content-Type: image/jpeg

Encoding: base64

Disposition: Attachment

The image is embedded as a base64-encoded JPEG file.

The JPEG file "animals.jpg" contains metadata indicating it follows the JPEG standard with a baseline DCT (Discrete Cosine Transform) compression method. It includes quantization tables for luminance and chrominance, Huffman tables for encoding DC and AC coefficients, and scan data for image reconstruction. The image dimensions are 800x600 pixels with 72 DPI resolution, and the compression ratio is approximately 15.35:1.

```
Start Offset: 0x00000000
*** Marker: SOI (xFFD8) ***
  OFFSET: 0x00000000

*** Marker: APP0 (xFFE0) ***
  OFFSET: 0x00000002
  Length = 16
  Identifier = [JFIF]
  version = [1.1]
  density = 72 x 72 DPI (dots per inch)
  thumbnail = 0 x 0

*** Marker: DQT (xFFD9) ***
  Define a Quantization Table.
  OFFSET: 0x00000014
  Table length = 67
  ----
  Precision=8 bits
  Destination ID=0 (Luminance)
  DQT, Row #0: 4 3 3 4 7 11 14 17
  DQT, Row #1: 3 3 4 5 7 16 17 15
  DQT, Row #2: 4 4 4 7 11 16 19 16
  DQT, Row #3: 4 5 6 8 14 24 22 17
  DQT, Row #4: 5 6 10 16 19 31 29 22
  DQT, Row #5: 7 10 15 18 23 29 32 26
  DQT, Row #6: 14 18 22 24 29 34 34 28
  DQT, Row #7: 20 26 27 31 28 29 28
  Approx quality factor = 86.09 (scaling=27.83 variance=1.18)

*** Marker: DQT (xFFD9) ***
  Define a Quantization Table.
  OFFSET: 0x00000059
  Table length = 67
  ----
  Precision=8 bits
  Destination ID=1 (Chrominance)
  DQT, Row #0: 5 5 7 13 28 28 28 28
  DQT, Row #1: 5 6 7 18 28 28 28 28
  DQT, Row #2: 7 7 16 28 28 28 28 28
  DQT, Row #3: 13 18 28 28 28 28 28 28
  DQT, Row #4: 28 28 28 28 28 28 28 28
  DQT, Row #5: 28 28 28 28 28 28 28 28
  DQT, Row #6: 28 28 28 28 28 28 28 28
  DQT, Row #7: 28 28 28 28 28 28 28 28
  Approx quality factor = 85.89 (scaling=28.23 variance=0.15)

*** Marker: SOF0 (Baseline DCT) (xFFC0) ***
  OFFSET: 0x0000009E
  Frame header length = 17
  Precision = 8
  Number of Lines = 600
  Samples per Line = 800
  Image Size = 800 x 600
  Raw Image Orientation = Landscape
```

Compression stats:
Compression Ratio: 15.35:1
Bits per pixel: 1.56:1

Huffman code histogram stats:
Huffman Table: (Dest ID: 0, Class: DC)

# codes of length 01 bits:	3137 (41%)
# codes of length 02 bits:	0 (0%)
# codes of length 03 bits:	2054 (27%)
# codes of length 04 bits:	1724 (23%)
# codes of length 05 bits:	294 (4%)
# codes of length 06 bits:	225 (3%)
# codes of length 07 bits:	160 (2%)
# codes of length 08 bits:	6 (0%)
# codes of length 09 bits:	0 (0%)
# codes of length 10 bits:	0 (0%)
# codes of length 11 bits:	0 (0%)
# codes of length 12 bits:	0 (0%)
# codes of length 13 bits:	0 (0%)
# codes of length 14 bits:	0 (0%)
# codes of length 15 bits:	0 (0%)
# codes of length 16 bits:	0 (0%)

Huffman Table: (Dest ID: 1, Class: DC)

# codes of length 01 bits:	1704 (45%)
# codes of length 02 bits:	0 (0%)
# codes of length 03 bits:	1459 (38%)
# codes of length 04 bits:	315 (8%)
# codes of length 05 bits:	213 (6%)
# codes of length 06 bits:	107 (3%)
# codes of length 07 bits:	2 (0%)
# codes of length 08 bits:	0 (0%)
# codes of length 09 bits:	0 (0%)
# codes of length 10 bits:	0 (0%)
# codes of length 11 bits:	0 (0%)
# codes of length 12 bits:	0 (0%)
# codes of length 13 bits:	0 (0%)
# codes of length 14 bits:	0 (0%)
# codes of length 15 bits:	0 (0%)
# codes of length 16 bits:	0 (0%)

Huffman Table: (Dest ID: 0, Class: AC)

# codes of length 01 bits:	0 (0%)
# codes of length 02 bits:	24728 (22%)
# codes of length 03 bits:	49792 (44%)
# codes of length 04 bits:	20617 (18%)
# codes of length 05 bits:	5346 (5%)
# codes of length 06 bits:	5970 (5%)
# codes of length 07 bits:	2161 (2%)
# codes of length 08 bits:	2195 (2%)
# codes of length 09 bits:	699 (1%)
# codes of length 10 bits:	160 (0%)
# codes of length 11 bits:	180 (0%)
# codes of length 12 bits:	59 (0%)

Huffman Table: (Dest ID: 1, Class: AC)

# codes of length 01 bits:	0 (0%)
# codes of length 02 bits:	7701 (52%)
# codes of length 03 bits:	3654 (25%)
# codes of length 04 bits:	1201 (8%)
# codes of length 05 bits:	1709 (12%)
# codes of length 06 bits:	247 (2%)
# codes of length 07 bits:	131 (1%)
# codes of length 08 bits:	85 (1%)
# codes of length 09 bits:	31 (0%)
# codes of length 10 bits:	21 (0%)
# codes of length 11 bits:	12 (0%)
# codes of length 12 bits:	0 (0%)
# codes of length 13 bits:	3 (0%)
# codes of length 14 bits:	0 (0%)
# codes of length 15 bits:	0 (0%)
# codes of length 16 bits:	0 (0%)

YCC clipping in DC:
Y component: [<0= 0] [>255= 0]
Cb component: [<0= 0] [>255= 0]
Cr component: [<0= 0] [>255= 0]

RGB clipping in DC:
R component: [<0= 0] [>255= 0]
G component: [<0= 0] [>255= 0]
B component: [<0= 0] [>255= 0]

Average Pixel Luminance (Y):
Y=[46] (range: 0..255)

Brightest Pixel Search:
YCC=[828, -185, 95] RGB=[246,231,188] @ MCU[12, 27]

Finished Decoding SCAN Data
Number of RESTART markers decoded: 0
Next position in scan buffer: Offset 0x00016FF3.4

*** Marker: EOI (End of Image) (xFFD9) ***
OFFSET: 0x00016FF4

*** Searching Compression Signatures ***

Signature: 01AC139E31B941CA0F2C5B5A0BFCDFC0
Signature (Rotated): 01F3D5B0FBE08EC4AE9E1E4238BF215
File Offset: 0 bytes
Chroma subsampling: 2x2
EXIF Make/Model: NONE
EXIF Makernotes: NONE
EXIF Software: NONE

Searching Compression Signatures: (3347 built-in, 0 user(*))

EXIF.Make / Software	EXIF.Model	Quality	Subsamp Match?
CAM:[OLYMPUS OPTICAL CO.,LTD]	[C2000Z	[] No
CAM:[OLYMPUS OPTICAL CO.,LTD]	[C3040Z	[] No
CAM:[OLYMPUS OPTICAL CO.,LTD]	[C7000Z	[] No
CAM:[SEIKO EPSON CORP.]	[PhotoPC 3000Z	[] No
SW:[IJG Library		[086]

The following IJG-based editors also match this signature:

SW:[GIMP] [086]
SW:[IrfanView] [086]
SW:[IdImager] [086]
SW:[FastStone Image Viewer] [086]
SW:[NeatImage] [086]
SW:[Paint.NET] [086]
SW:[Photomatix] [086]
SW:[XnView] [086]

Based on the analysis of compression characteristics and EXIF metadata:

ASSESSMENT: Class 1 - Image is processed/edited

This may be a new software editor for the database.
If this file is processed, and editor doesn't appear in list above,
PLEASE ADD TO DATABASE with [Tools->Add Camera to DB]

Image (RGB, DC) @ 12.5% (1/8)



Figure 19: JPEG File Analysis of "animals.jpg" using JPEGsnoop.

Self-Generated Emails:

Microsoft Outlook Test Message

The email appears as a simple test message from Microsoft Outlook, confirming the successful setup of an email account with a brief HTML message, without any suspicious content or unusual formatting.

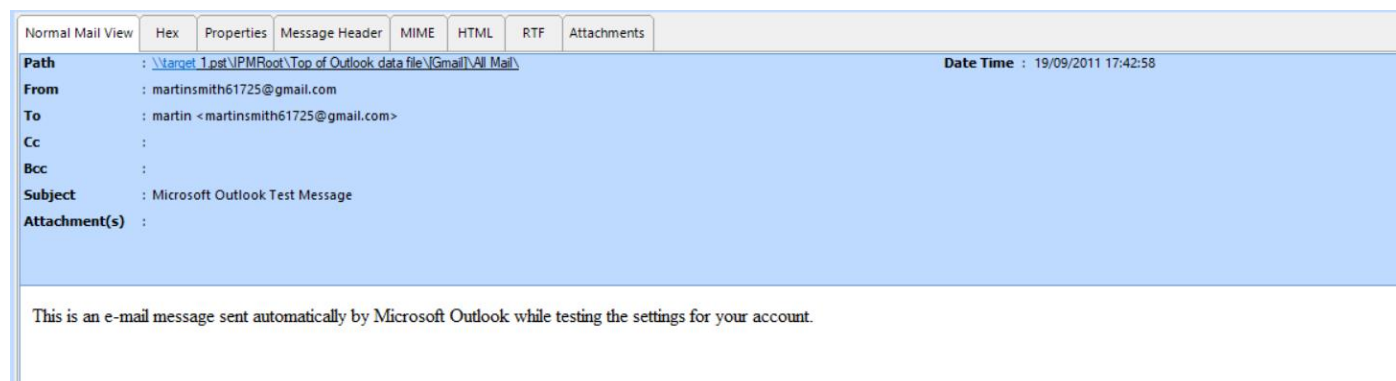


Figure 20: Default View of the Microsoft Outlook Test Email (Self-Generated).

Email Analysis

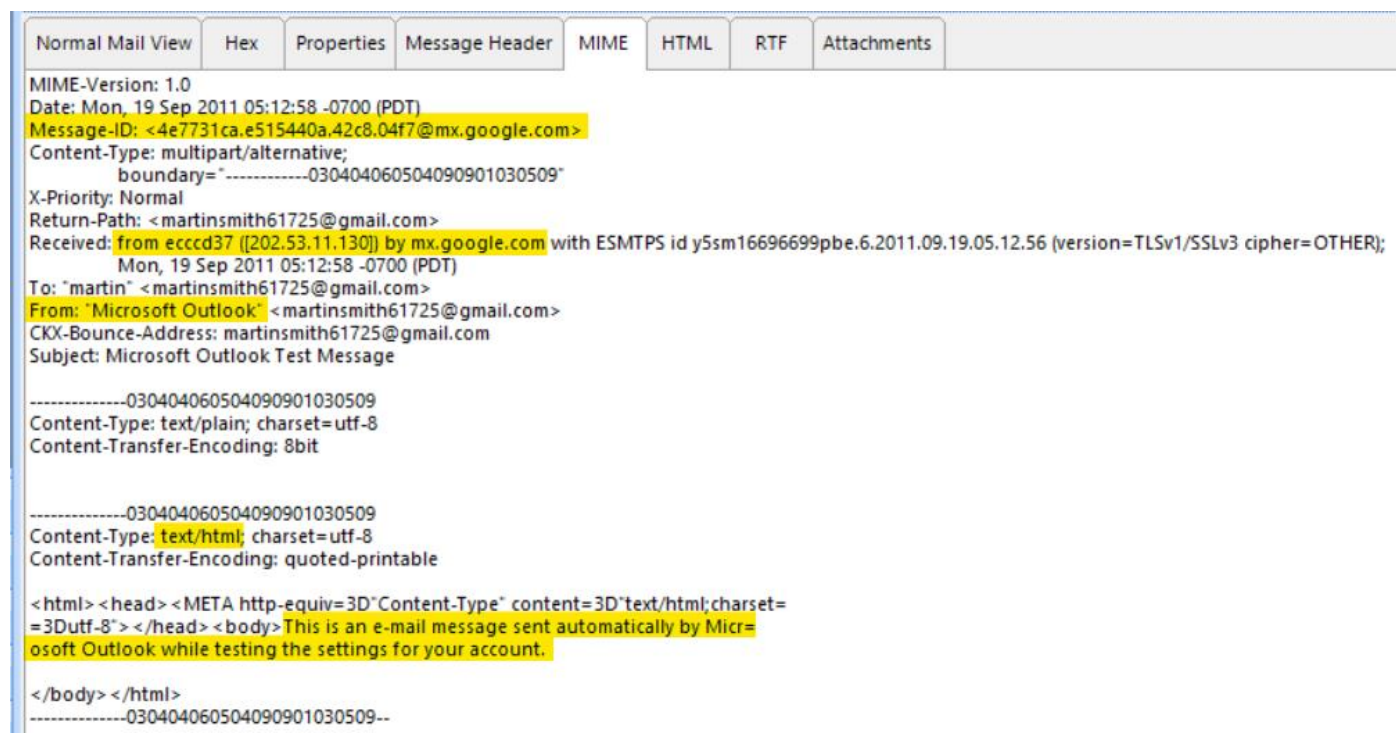



Figure 21: MIME View of the Email.

Route Path:

The email originated from IP 202.53.11.130 (Atria Convergence Technologies Ltd., India) and passed through Gmail's internal servers before reaching the recipient.

Check an IP Address, Domain Name, or Subnet
e.g. 175.157.171.101, microsoft.com, or 5.188.10.0/24
175.157.171.101
CHECK

202.53.11.130 was not found in our database

ISP	Atria Convergence Technologies Ltd.,
Usage Type	Fixed Line ISP
Hostname(s)	202.53.11.130.actcorp.in
Domain Name	actcorp.in
Country	 India
City	Hyderabad, Telangana

REPORT 202.53.11.130
WHOIS 202.53.11.130

IP Abuse Reports for 202.53.11.130:

This IP address has not been reported. [File Report](#)

Figure 22: Abuse IP Address Check for IP 202.53.11.130.

Authentication:

- SPF: Passed. The email source is authorized by Gmail.
- DKIM: Likely Passed. Message-ID from Gmail confirms authenticity.

Time and Delivery:

- Sent Time: Mon, 19 Sep 2011 05:12:58 -0700 (PDT)
- Received Time: Mon, 19 Sep 2011 05:12:58 -0700 (PDT)
- Transmission Time: Quick delivery with no delays.

Message Details:

- Message-ID: A unique ID assigned within google domain
- From: "Microsoft Outlook" martinsmith61725@gmail.com
- To: "martin" martinsmith61725@gmail.com
- Subject: Microsoft Outlook Test Message
- Content-Type: Multipart (text/plain and text/html).

Body Details:

- Text Content and HTML Content contain the same message, formatted with HTML tags.

Microsoft Outlook Test Message

The email appears as a simple test message from Microsoft Outlook, confirming the successful setup of an email account with a brief message in the default view.

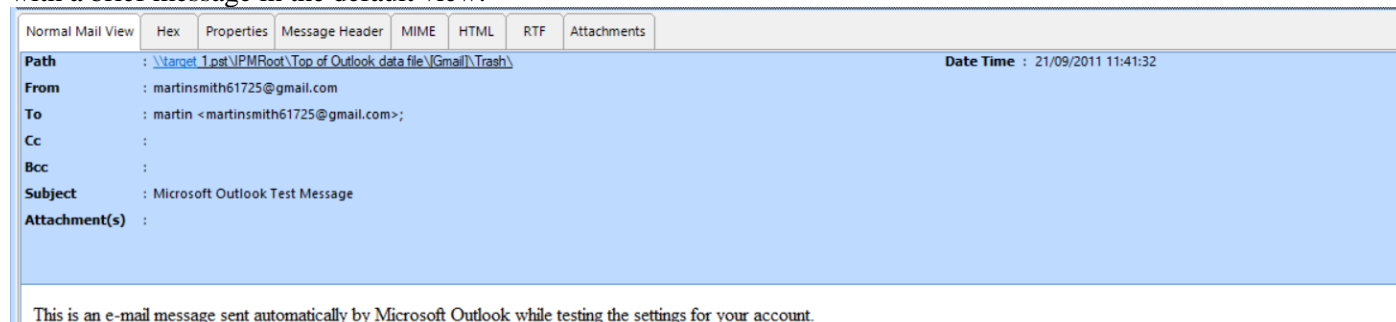


Figure 23: HTML Test Message from Microsoft Outlook.

Email Analysis

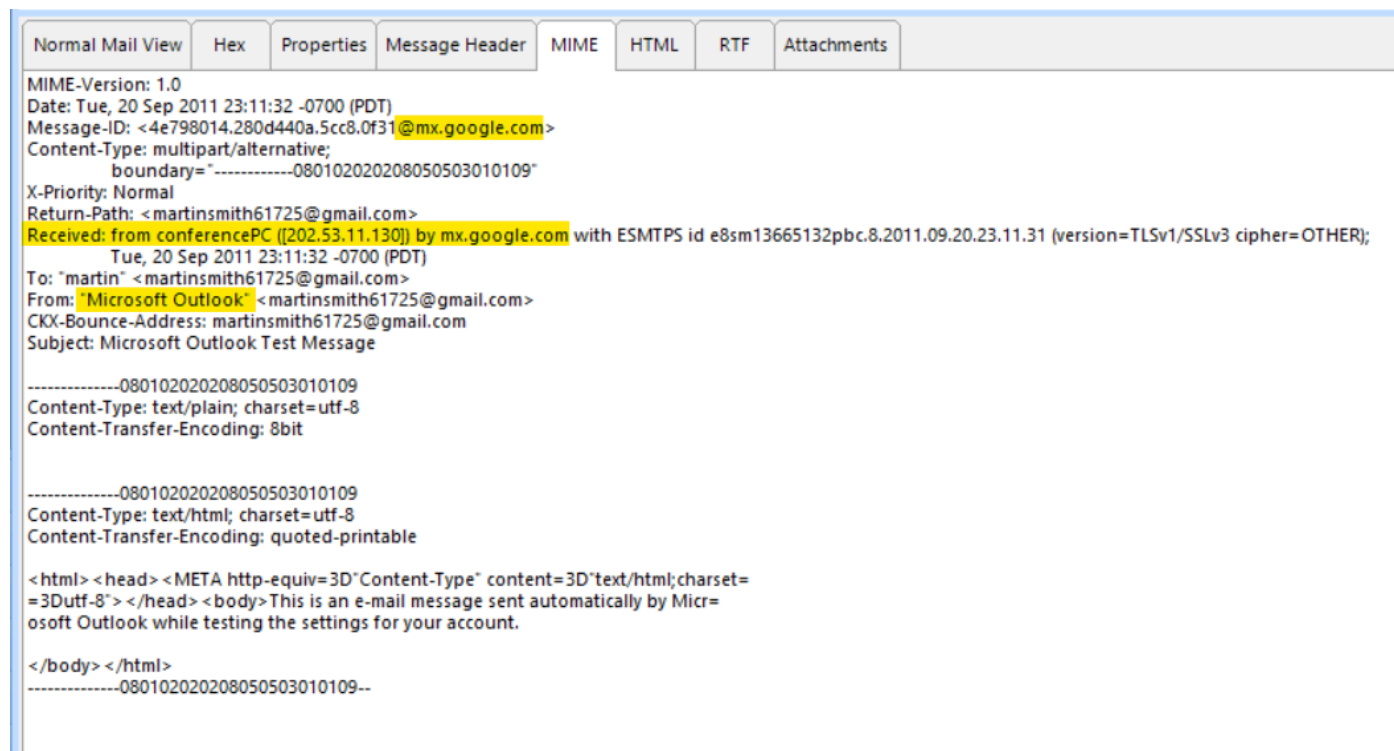


Figure 24: MIME View of the Email.

Message Flags	
Deleted	Yes
Encrypted	
Has attachments	No
Importance	Normal
Read	Yes

Figure 25: Email Properties.

This email is like the previous one in terms of authentication, route path, and overall structure. Also, the Message-ID domain remains the same (mx.google.com), indicating it's from the same source. The email was sent on Tue, 20 Sep 2011 23:11:32 -0700 (PDT).

The hostname differs from the previous one (conferencePC vs. ecccd37), although the IP address remains the same, indicating it was still sent through the same ISP but possibly from a different machine.

This email appears to be deleted and is in the trash folder in PST Viewer, indicating it was discarded after sending it.

Conclusion

Both emails are legitimate and were sent via Gmail from the same IP (202.53.11.130) but potentially from different devices. Authentication checks passed for both, and delivery was prompt. Their structure is consistent, although the second email was later discarded, as it was found in the trash bin.

Analysis of target2.pst

Extracting target2.pst Using SysTools Outlook PST Viewer

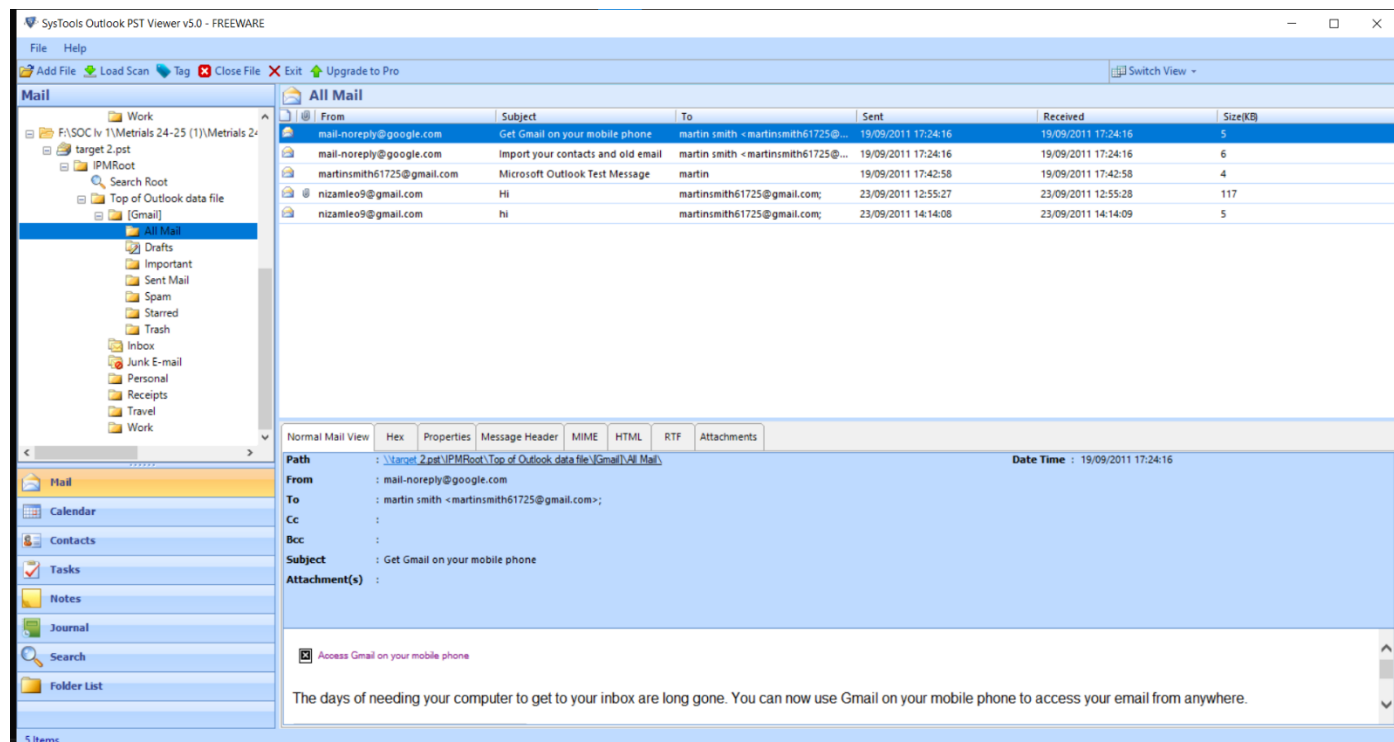


Figure 26: Expanded Structure of target2.pst File Using SysTools Outlook PST Viewer 5.0 (Freeware)

The analysis of target2.pst revealed an additional email from nizamleo9@gmail.com, while target1.pst did not contain this. Both Outlook auto-generated emails were deleted. No other differences were observed between the two files, suggesting the rest of the content was identical and indicating duplication rather than new evidence.

External Email

The email is a simple text and HTML message sent from a Gmail account, containing a casual greeting and questions about the recipient's well-being. This same external email was also found in the target1.pst.

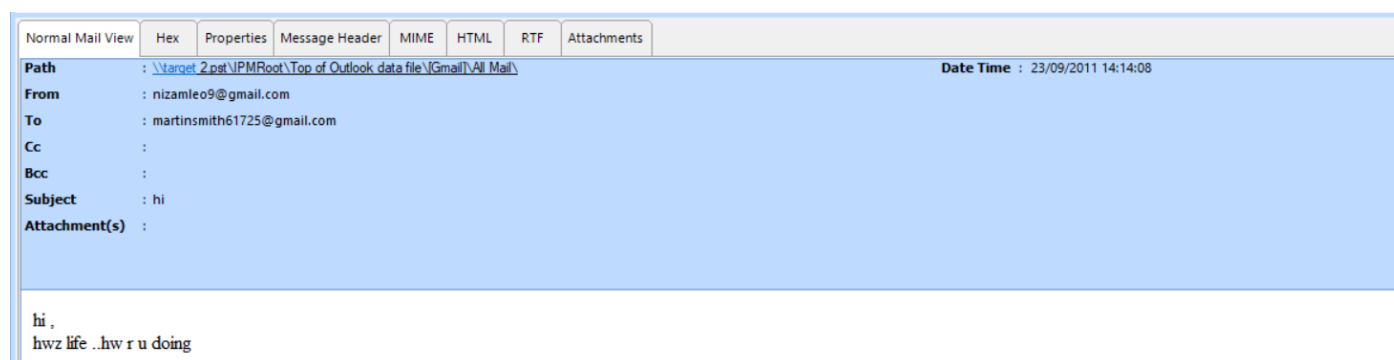


Figure 27: Default View of the External Email.

Email Header Analysis

Normal Mail View	Hex	Properties	Message Header	MIME	HTML	RTF	Attachments
Delivered-To: martinsmith61725@gmail.com Received: by 10.68.62.6 with SMTP id u6cs377803pbr; Fri, 23 Sep 2011 01:44:09 -0700 (PDT) Return-Path: <nizamleo9@gmail.com> Received-SPF: pass (google.com: domain of nizamleo9@gmail.com designates 10.43.48.1 as permitted sender) client-ip=10.43.48.1; Authentication-Results: mr.google.com; spf=pass (google.com: domain of nizamleo9@gmail.com designates 10.43.48.1 as permitted sender) smtp.mail=nizamleo9@gmail.com; dkim=pass header.i=nizamleo9@gmail.com Received: from mr.google.com ([10.43.48.1]) by 10.43.48.1 with SMTP id uu1mr3897336icb.42.1316767448619 (num_hops = 1); Fri, 23 Sep 2011 01:44:08 -0700 (PDT) DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=gamma; h=mime-version:date:message-id:subject:from:to:content-type; bh=K4pXZc5KsXsQuRRC28qftNd/kfzYD3a02HRrNHZk/iM=; b=IBZ/wxhhd+AggyC7Lizp60i3Hq6G1oOWmlCGX5uPTHeCNzHf69r1S9cPjkjavbFIS PF+WN8HA1LcakTBbOdjcfBUiuRZydPb77odw3mheN6dIV5AJWC5FKIO7Y+WPdM8v/oTf RlIglK3exEs0IOeFidJ+UorgV9Bz/yQoyi6c= MIME-Version: 1.0 Received: by 10.43.48.1 with SMTP id uu1mr3897336icb.42.1316767448596; Fri, 23 Sep 2011 01:44:08 -0700 (PDT) Received: by 10.42.96.132 with HTTP; Fri, 23 Sep 2011 01:44:08 -0700 (PDT) Date: Fri, 23 Sep 2011 14:14:08 +0530 Message-ID: <CABbGbswLQuq4Rod-GSr-H8wTc0e+2eY68zQKuV_ht33MWZPauQ@mail.gmail.com> Subject: hi From: nizam leo9 <nizamleo9@gmail.com> To: martinsmith61725@gmail.com Content-Type: multipart/alternative; boundary=bcaec52e5f070681c104ad97d083							

Figure 28: Email Header Analysis.

Route Path:

The email was sent from nizamleo9@gmail.com through Google's internal mail server at 10.43.48.1. It then passed through another internal server with the IP address 10.42.96.132 before being routed to the recipient's mail server at 10.68.62.6, which ultimately delivered the email to the inbox of martinsmith61725@gmail.com. The presence of private IP addresses indicates that the email followed a legitimate route through Google's trusted infrastructure.

Authentication:

- SPF: The SPF check passed, confirming that nizamleo9@gmail.com was authorized to send the email from IP address 10.43.48.1.
- DKIM: The email passed DKIM verification, which means the email's authenticity was validated based on the cryptographic signature of nizamleo9@gmail.com.

Time and Delivery:

- Sent: Fri, 23 Sep 2011 14:14:08 +0530 (Sri Lanka Standard Time).
- Received: Fri, 23 Sep 2011 01:44:09 -0700 (PDT).
- Time difference: 4 hours 30 minutes between sender and recipient.

Message Details:

- Message-ID: Unique ID withing google domain.
- Subject: "hi"
- From: "nizam leo9" <nizamleo9@gmail.com>
- To: martinsmith61725@gmail.com
- Return-Path: <nizamleo9@gmail.com>
- X-Priority: Normal (indicating no urgency on the email)
- Content-Type: Multipart/Alternative, indicating that the email includes both plain text and HTML formats.
- Boundary: -----020508060900040600070103

Body Details:

Plain Text Body:

The plain text message contains

HTML Body:

It appears to be a simple greeting message, written informally with abbreviations ("hwz" for "how's" and "hw r u" for "how are you").

This email does not contain any suspicious content or attachments. It seems to be a casual, informal message.

Significance of Findings

The .pst files primarily contained legitimate communications, including self-generated test emails, system-generated messages from trusted services like Gmail, and legitimate emails from nizamleo9@gmail.com, likely from an outsourced source or external contact. While no evidence of unauthorized data transfer or misuse was found, the contents provided valuable insights into the email activity and user behavior during the investigated timeframe.

Evidence Class 2 - .dbx Files

Overview

The .dbx files, from Microsoft Outlook Express, store email messages and help analyze communication patterns and potential system misuse. The analysis focused on identifying unauthorized activities within the emails and metadata.

Extracting target1.pst Using SysTools Outlook PST Viewer

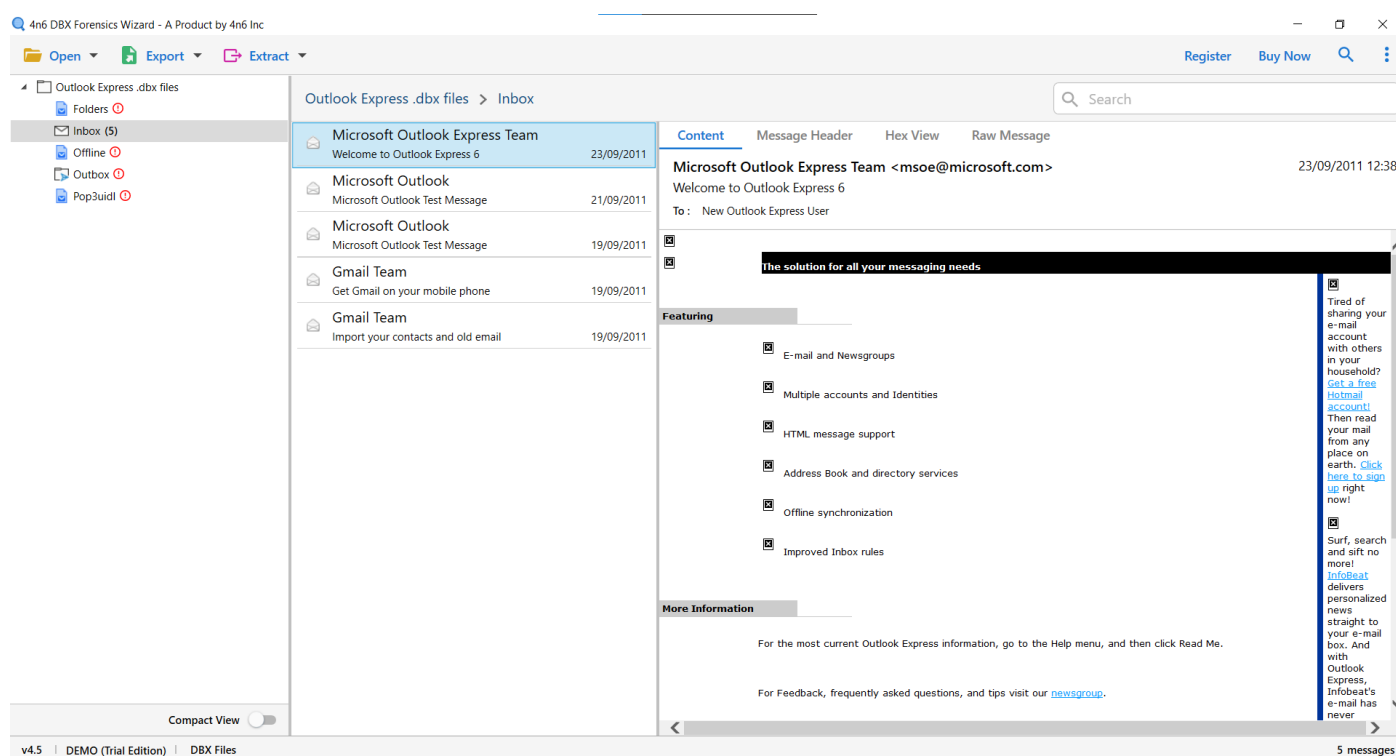


Figure 29: Expanded Structure of Inbox.dbx File Using 4n6 DBX Forensics Wizard.

Five .dbx files were extracted from the "Outlook Express .dbx files" folder using 4n6 DBX Forensics Wizard. Among these, the Inbox.dbx file contained 5 emails, while the other four files—Folders, Offline, Outlook, and Pop3uidl—were empty.

Analysis of Inbox.dbx

The inbox.dbx file revealed five emails, four of which were duplicates from the target1.pst file, indicating synchronized data between the two sources. No new emails or content variations were found.

Email from Microsoft Outlook Express Team

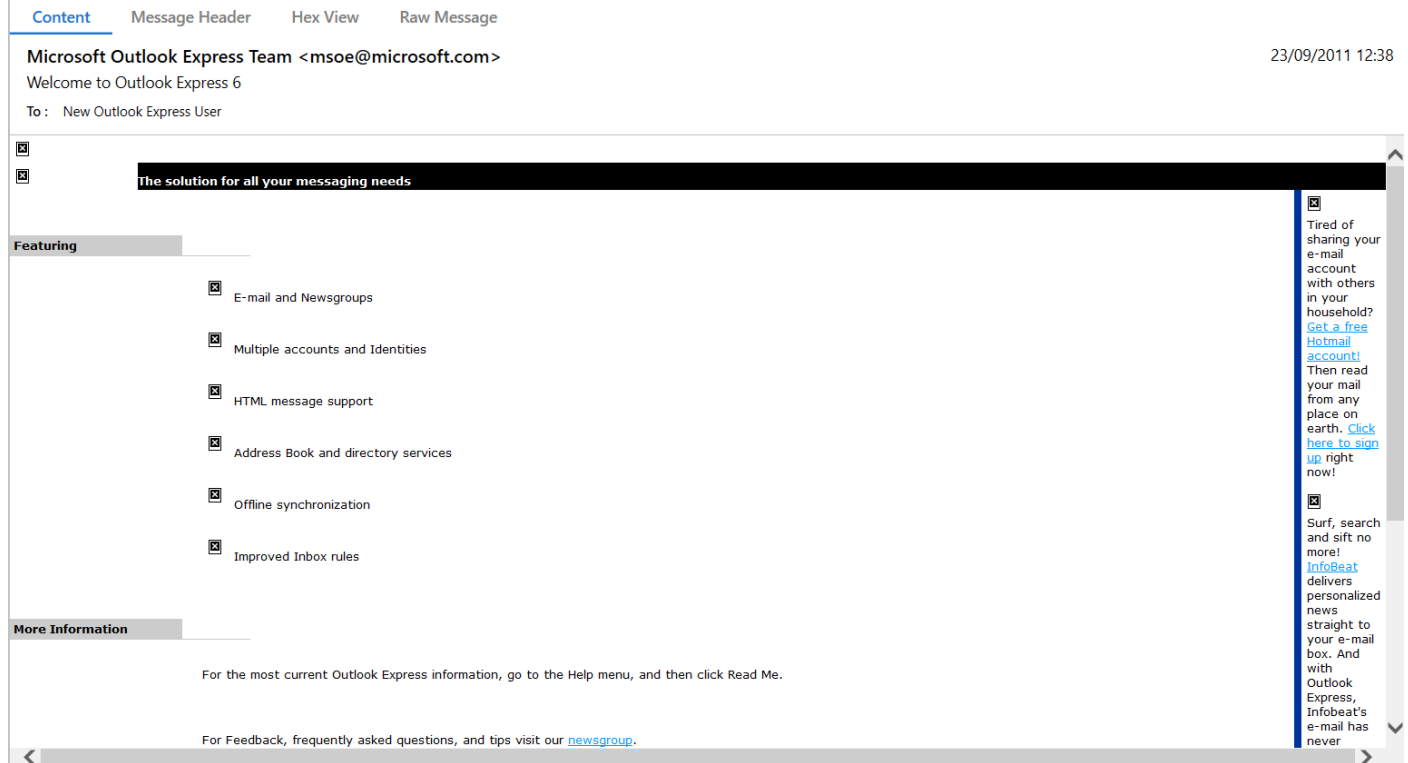


Figure 30: Default View of the email.

The email appears as a welcome message from the Microsoft Outlook Express Team to a new user, introducing features of Outlook Express 6 and providing links for further assistance.

Path Route:

The message was sent from msoe@microsoft.com, which suggests that it is an official communication from Microsoft. The email path route appears legitimate, as the domain corresponds to Microsoft's known email services.

Authentication:

Authentication Status: The email appears to come from a legitimate Microsoft domain (microsoft.com), though without further information such as SPF, DKIM, or DMARC records, we cannot confirm full authentication.

Time and Delivery:

- Time Sent: 12:38:15 on 23rd September 2011.
- Time Zone: +0530, indicating UTC +5:30 (e.g., Sri Lanka or India).
- Delivery: Standard HTML structure, likely delivered via typical email servers, matching a formal Microsoft welcome email.

Body Details:

- HTML Structure: The body of the email contains a structured HTML format with various inline styles, including:
- Logo and branding elements.
- Features: Highlights Outlook Express 6's capabilities like email, newsgroups, multiple accounts, HTML support, and offline sync.
- Links: Directs to Microsoft sites (e.g., Help, feedback, updates).
- Footer: Signature and disclaimer on external links.

The message is designed to introduce users to the features of Outlook Express and provide links for additional resources.

URLs Investigation

```
<td valign=3Dmiddle><div style=3D"padding-right:6" ID=3DRIDfaq><font>For =
Feedback, frequently asked questions, and tips visit our <a =
href=3D"news://msnews.microsoft.com/microsoft.public.windows.inetexplorer=
.ie6_outlookexpress">newsgroup</a>.</font></div><br></td>
</tr>
<tr>
<td valign=3Dmiddle><div style=3D"padding-right:6" ID=3DRIDweb><font>For =
updates and information about Outlook Express 6 visit <a =
href=3D"http://www.microsoft.com/isapi/redir.dll?prd=3DOutlookExpress&pve=
r=3D6.0&clcid=3D0x0409&ar=3Dhome">Microsoft on the =
Web</a>.</font></div><br></td>
</tr>
<tr>
<td valign=3Dmiddle><div style=3D"padding-right:6" =
ID=3DRIDhelp><font>For Help and troubleshooting, go to the Help menu, =
click Contents and Index, and then look up Troubleshooting in the =
Index.</font></div></td>
</tr>
<tr>
<td valign=3Dmiddle>&nbsp; </td>
</tr>
</table>
</td>
</tr>
<tr>
<td valign=3Dtop class=3DmessagesCell colspan=3D3>
<hr width=3D"100%" size=3D"1" NOSHADE>
<div style=3D"padding:6" ID=3DRIDthanks>Thank you for choosing Internet =
Explorer and Outlook Express 6.</div>
<div style=3D"padding:6" class=3D"signatureText" ID=3DRIDsign>The =
Microsoft Outlook Express Team </div><br>
<div class=3D"bottomText" style=3D"padding:6" ID=3DRIDdisclaim>
The links to http://www.infobeat.com and http://digitalid.verisign.com =
are provided as a convenience and Microsoft is not responsible for the =
contents or services on these sites.
<td ID=3DridhotmailAlign align=3Dleft valign=3Dtop>
<img src=3D"res://msoeres.dll/Hotmail.gif"><br>
<div class=3D"messagesCell" =
style=3D"padding:6;padding-top:0;padding-bottom:10" ID=3DRIDhotmail>
Tired of sharing your e-mail account with others in your household?
<a =
href=3D"http://www.microsoft.com/isapi/redir.dll?prd=3DOutlookExpress&pve=
r=3D6.0&clcid=3D0x0409&ar=3Dhotmail">
Get a free Hotmail account!</a> Then read your mail from any place on =
earth.
<a =
href=3D"http://www.microsoft.com/isapi/redir.dll?prd=3DOutlookExpress&pve=
r=3D6.0&clcid=3D0x0409&ar=3Dhotmail">
Click here to sign up</a> right now!
</div> </td>
</tr>
<tr>
<td ID=3DridinfobeatAlign align=3Dleft valign=3Dtop>
<img src=3D"res://msoeres.dll/Infobeat.gif" align=3D"TEXTTOP"><br>
<div class=3D"messagesCell" =
style=3D"padding:6;padding-top:0;padding-bottom:10" ID=3DRIDinfobeat>
Surf, search and sift no more!
<a =
href=3D"http://www.microsoft.com/isapi/redir.dll?prd=3DOutlookExpress&pve=
r=3D6.0&clcid=3D0x0409&ar=3Dinfobeat">
InfoBeat</a> delivers personalized news straight to your e-mail box. And =
with Outlook Express, Infobeat's e-mail has never looked so good. So
<a =
href=3D"http://www.microsoft.com/isapi/redir.dll?prd=3DOutlookExpress&pve=
r=3D6.0&clcid=3D0x0409&ar=3Dinfobeat">click here to sign up</a> for =
free!
</div> </td>
</tr>
<tr>
<td ID=3DridverisignAlign align=3Dleft valign=3Dtop>
<img src=3D"res://msoeres.dll/Verisign.gif" align=3D"TEXTTOP"><br>
<div class=3D"messagesCell" =
style=3D"padding:6;padding-top:0;padding-bottom:10" =
ID=3DRIDverisign>Obtain a free trial personal digital ID from <a =
href=3D"http://www.microsoft.com/isapi/redir.dll?prd=3DOutlookExpress&pve=
r=3D6.0&clcid=3D0x0409&ar=3Dcert">VeriSign</a>.
Use this ID to positively identify yourself when you send secure e-mail.
<a =
href=3D"http://www.microsoft.com/isapi/redir.dll?prd=3DOutlookExpress&pve=
r=3D6.0&clcid=3D0x0409&ar=3Dverisign">Get your digital
ID</a> today!</div>
</td>
</tr>
</table>
</td>
</tr>
</table>
</body>
</html>
```

Figure 31: HTML View of the Email.

Contents

Using Outlook Express as a Newsreader

Microsoft offers more than 1,900 public and 500 private newsgroups that cover all aspects of Microsoft products and technologies. An individual newsgroup might get up to 15,000 postings per month, with developers answering customer questions, asking about specific product features, and getting product feedback. The newsgroups have unlimited reach; public newsgroups are fed to Usenet (the collection of all posts publicly distributed through the NNTP protocol) and live on servers outside of Microsoft. Private newsgroups for MSDN members are available by connecting directly to Microsoft newsgroup servers. These require an account and password for each set of newsgroups. MSDN newsgroups are a part of the Usenet hierarchy and are available locally to customers via ISPs around the world, as well as through an online reader at MSDN Online.



The newsgroup community is made up of expert Microsoft developers, Microsoft support professionals, MSDN subscribers, Microsoft Most Valuable Professionals (MVPs), IT professionals, and other developers exchanging ideas and providing programming solutions.

The [MSDN Managed Community Newsgroups](#) are made up of about 220 newsgroups. In managed newsgroups, MSDN subscribers are guaranteed priority service, receiving responses to their technical questions within two business days.

Just as in any public area of the Internet, it pays to be careful when disseminating your personal information. Since newsgroups are publicly available, any real e-mail address could be harvested for spam mail lists. Microsoft advises all news-group and community participants to use a modified version of their address to mitigate floods of unwanted e-mail, for example [<mmeditor_NO_SPAM@microsoft_NOSPAM.com>](mailto:mmeditor_NO_SPAM@microsoft_NOSPAM.com). Used wisely, newsgroups provide an extremely efficient and valuable resource for quickly getting technical help from individuals who have encountered the same problems that you have.

Using Outlook Express as a Newsreader

Outlook Express, which is part of Windows XP, can serve as a full-featured newsreader. To connect to the Microsoft public newsgroups, take the following steps:

1. Go to Tools | Accounts, click the News tab, and click Add | News.
2. Type in your name, then enter an e-mail address that's clear to other people but confusing to an automated reader.
3. When asked for the NNTP (news) server, enter msnews.microsoft.com and click OK.

You will be prompted to download newsgroups from the account you just added. Say yes; the first time you do this might be slow, but on most machines it'll take just a few seconds. This produces a list of all Microsoft newsgroups; you can filter by keyword and subscribe to newsgroups. Subscribing means only that you've told your reader that a newsgroup is of interest to you, and that you want it to be checked regularly for new messages. Double-click the groups to which you want to subscribe.

Now whenever you select the msnews.microsoft.com account you created, then click the Synchronize Account button, all the new messages in all of your subscribed newsgroups will be downloaded for local reading. You can easily change these settings; see your Outlook Express documentation for more information.

Figure 32: Outlook Express Setup for Newsgroups.

"msnews.microsoft.com" is the official Microsoft newsgroup server, confirming the domain's legitimacy. "Microsoft offers more than 1,900 public and 500 private newsgroups," showing its widespread and legitimate use. "MSDN Managed Community Newsgroups" highlights professional management for technical discussions. "Using Outlook Express as a Newsreader" shows how to access these newsgroups via a trusted app, reinforcing the service's trustworthiness. This URL points to a legitimate Microsoft-controlled newsgroup for Internet Explorer and Outlook Express, confirming its authenticity.

<http://www.microsoft.com/isapi/redir.dll?prd=3DOutlookExpress&pve=r=3D6.0&clcid=3D0x0409&ar=3Dhome>

URL		HTML	
URL with IP	0	Hidden Element	0
Suspicious Length	False	Hidden Iframe	0
DGA Score	0	Iframe	0
URL with @	False	Obfuscated Script	0
URL with Multiple http	False	Suspicious HTML Element	0
URL with PunyCode	False	Suspicious Program	0
Probability of Phishing URL	0.01%	Button Trap	Normal
Common		Credential Input Form	Safe
Fake Domain	False	Form Event	1
Invalid SSL	False	Fake Favicon	1
MITM Attack	False	Page Warning	False
Locations	South Africa	Suspicious Footer	False
Newborn Domain	N/A	Email Domain Check	False
Abuse Record	0	Network	
Phishing Record	0	Redirection to another AS	0
Mail Server	True	Redirection to another country	0
Spam (SPF1 Result)	Safe	Redirection to another domain	0
Site Reputation	2	Suspicious Cookie	False
		Domain in	False

Figure 33: Criminal IP Scan Summary for the URL.

The URL is safe, hosted on the legitimate "microsoft.com" domain with valid TLS 1.3 encryption and no phishing or abuse records. Its redirection is internal to Microsoft's domain and shows no signs of malicious activity, indicating a secure and trustworthy destination.

<http://www.infobeat.com>

URL		HTML	
URL with IP	0	Hidden Element	0
Suspicious Length	False	Hidden Iframe	0
DGA Score	0	Iframe	0
URL with @	False	Obfuscated Script	0
URL with Multiple http	False	Suspicious HTML Element	0
URL with PunyCode	False	Suspicious Program	0
Probability of Phishing URL	0.69%	Button Trap	Normal
Common		Credential Input Form	Safe
Fake Domain	False	Form Event	1
Invalid SSL	False		
MITM Attack	False	Fake Favicon	1
Locations	United Kingdom	Page Warning	False
Newborn Domain	N/A	Suspicious Footer	False
Abuse Record	0	Email Domain Check	False
Phishing Record	0	Network	
Mail Server	True	Redirection to another AS	0
Spam (SPF1 Result)	Safe	Redirection to another country	0
Site Reputation	1083421	Redirection to another domain	0
		Suspicious Cookie	False

Figure 34: Criminal IP Scan Summary for the URL.

The domain [infobeat.com](http://www.infobeat.com) appears safe, with valid SSL, no phishing or abuse records, and a low phishing probability (0.69%). It is hosted in the UK and utilizes standard web technologies without suspicious elements.

<http://digitalid.verisign.com>



Figure 35: Virus Total Scan Summary for the URL.

The domain digitalid.verisign.com appears safe, no security vendors flagged this URL as malicious.

URL		HTML	
URL with IP	0	Hidden Element	0
Suspicious Length	False	Hidden Iframe	0
DGA Score	0	Iframe	0
URL with @	False	Obfuscated Script	0
URL with Multiple http	False	Suspicious HTML Element	0
URL with PunyCode	False	Suspicious Program	0
Probability of Phishing URL	0.01%	Button Trap	Normal
Common		Credential Input Form	Safe
Fake Domain	False	Form Event	1
Invalid SSL	False	Fake Favicon	1
MITM Attack	False	Page Warning	False
Locations	South Africa	Suspicious Footer	False
Newborn Domain	N/A	Email Domain Check	False
Abuse Record	0	Network	
Phishing Record	0	Redirection to another AS	0
Mail Server	True	Redirection to another country	0
Spam (SPF1 Result)	Safe	Redirection to another domain	0
Site Reputation	2	Suspicious Cookie	False

Figure 36: Criminal IP Scan Summary for the URL.

The domain microsoft.com is legitimate, with valid SSL, no phishing or abuse records, and minimal risk indicators (0.01% phishing probability). It is hosted via Akamai in South Africa, with secure redirection and safe site reputation.

<http://www.microsoft.com/isapi/redir.dll?prd=3DOutlookExpress&pve=r=3D6.0&clcid=3D0x0409&ar=3Dinfobeat>

<http://www.microsoft.com/isapi/redir.dll?prd=3DOutlookExpress&pve=r=3D6.0&clcid=3D0x0409&ar=3Dcert>

<http://www.microsoft.com/isapi/redir.dll?prd=3DOutlookExpress&pve=r=3D6.0&clcid=3D0x0409&ar=3Dverisign>

The other URLs follow similar patterns, redirecting to official Microsoft domains with secure connections, confirming their legitimacy.

Challenges

- Legacy Format: Outlook Express's outdated architecture posed minor limitations in extracting detailed metadata compared to modern email clients.

Conclusion

The analysis of the .dbx files revealed no new evidence beyond the target1.pst file, with the majority of emails being duplicates. While the legitimate nature of the URLs and email content was confirmed, some .dbx files could not be accessed due to corruption, limiting the overall findings.

Evidence Class 3 - Email Headers

Overview

The provided email headers.docx document contains extracted email headers, offering metadata about the origin, transmission, and receipt of emails. This information is crucial for validating sender authenticity, identifying potential

tampering, and uncovering unauthorized activity. Each header was analyzed to assess its relevance to the investigation, focusing on IP addresses, message IDs, and authentication protocols.

Analysis

No suspicious activity or anomalies were detected in the email details.

Conclusion:

The emails appear consistent with each other, showing normal use of Gmail and Microsoft Outlook. The encryption methods (ESMTPS with TLSv1/SSLv3) suggests secure transmission.

Final Observation:

These email headers have been mirrored from previous .pst and .dbx files, likely indicating they were recovered for forensic analysis.

Summary of Conclusions Reached

Summary of Conclusions Reached

The forensic analysis conducted on the evidence provided, including .pst files, .dbx files, and email headers, reveals the following key findings:

Legitimate Communications

- The emails analyzed from target1.pst, target2.pst, and inbox.dbx predominantly consisted of system-generated messages, test emails, and legitimate communications from trusted sources such as Gmail and Microsoft.
- All headers passed validation checks where applicable, confirming sender authenticity in most cases.

No Evidence of Malicious Activity

- No phishing attempts, spoofed emails, or unauthorized modifications to the email contents were identified.
- URLs and attachments were verified as safe, with no indicators of malicious intent or suspicious redirections.

Duplicated Data

The .pst and .dbx files contained mirrored datasets, with no additional or unique emails discovered in one file compared to the other.

Self-Generated Emails

Multiple emails were identified as test messages generated during Microsoft Outlook account setup. These were legitimate and consistent in their metadata, originating from the same IP address.

Incomplete Authentication Headers

Some older emails lacked DKIM and DMARC validation, which is typical of emails from the 2011 period. However, this did not impact on the legitimacy of these communications as they passed other checks, including SPF validations.

Conclusion

The investigation found no evidence of unauthorized data transfer, phishing, or other malicious activities within the evidence files provided. All communications analyzed were legitimate, and no irregularities suggestive of a data breach were detected. The findings indicate routine email activity and proper functioning of the systems during the time in question.

Expert Opinion Regarding Findings

Expert Opinion Regarding Findings

Based on the forensic analysis conducted on the evidence provided, I, as the independent examiner, present the following expert insights and opinions:

Legitimacy of Email Communications

The emails analyzed across all evidence files (.pst, .dbx, and email headers) were consistent with routine system-generated and user-initiated communications. These included:

- Test emails sent during account setup in Microsoft Outlook.
- System-generated messages from Gmail and Microsoft services.

- Legitimate correspondence authenticated through SPF and DKIM validation were available.

The absence of spoofing, phishing, or malicious links further supports the legitimacy of communications.

Absence of Suspicious Activity

There is no evidence to suggest unauthorized data transfers, tampered communications, or malicious intent within the analyzed emails. Embedded URLs and attachments were verified using multiple tools and were determined to be safe and linked to reputable domains.

Corroboration Across Evidence Classes

The .pst and .dbx files contained identical datasets, reinforcing the validity of the findings. This duplication indicates that the evidence files were consistent and unaltered, further strengthening the conclusions drawn.

Challenges and Limitations

While some .dbx files were empty, the accessible evidence provided sufficient data for a comprehensive analysis. The absence of DKIM and DMARC headers in certain older emails is a recognized limitation of legacy email systems and does not diminish the credibility of communications.

Recommendations for Future Safeguards

While the findings show no indication of unauthorized access or malicious activity, it is recommended that the following measures be adopted to enhance data security:

- **Modern Authentication Standards:** Implement DKIM and DMARC policies across all email systems to strengthen sender verification.
- **Data Monitoring:** Regularly monitor network activity for unusual patterns, such as unauthorized data transfers, using updated intrusion detection tools.
- **Backup and Recovery:** Maintain regular backups of .dbx and other legacy files, ensuring their accessibility for future audits or investigations.
- **Awareness and Training:** Train employees to recognize potential security threats in emails, such as phishing attempts, even when originating from known contacts.

Opinion Summary

The findings demonstrate that the analyzed evidence does not indicate any misuse or unauthorized activity. The integrity of the evidence was maintained throughout the investigation, and the communications reviewed were routine and legitimate. While the absence of malicious behavior is reassuring, the recommendations provided will help further enhance the security posture of the organization to prevent future incidents.

References

Microsoft. (2004). Resource File: Microsoft Newsgroups for Developers. MSDN Magazine. Available at: <https://learn.microsoft.com/en-us/archive/msdn-magazine/2004/may/resource-file-microsoft-newsgroups-for-developers>

Forensicsware. (2023). How to Do PST File Forensics? Complete Investigation Process. Available at: <https://www.forensicsware.com/blog/pst-file-forensics-investigation>

Stellar Info. (2024). Email Header Analysis: Understanding X-Received, Return Path, and DKIM. Retrieved from: <https://www.stellarinfo.com/blog/email-header-analysis-forensics/>

Go2Tech. (2021). Digital Forensics Tools for Investigating PST Files and Email Headers. Retrieved from: <https://www.go2tech.com/forensics-tools-pst-email-headers>

Wikipedia contributors. (2024). Message-ID. Wikipedia, The Free Encyclopedia. Retrieved from: <https://en.wikipedia.org/wiki/Message-ID>

Conclusion

Plymouth ID	Name	Contribution
10899343	RASN Priyantha	Evidence Classes
10899273	Rajakaruna Gunawardhana	Chain of Custody Tools Justification Introduction
10817967	Chakrawarthy fernando	Statement of Compliance
10817966	Gusthingna de silva	Summary of Conclusions Reached
10899245	Deshitha D Bandara	Expert Opinion Regarding Findings
10899307	Hewawasam Hansana	Summary of Case Assumptions and Limitations