OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN

Digital Forensics

Week 11 – e-mail Analysis

Date: Friday 28th November 2025

Course Code: TU856 TU857 TU858 (Full-Time)

TU Dublin – Grangegorman Campus

School of Computer Science

Seoladh Cláraithe / Registered Address
OT Baile Átha Cliath - Teach na Páirce Ghráinseach Ghormáin
191 An Cuarbhóthar Thuaidh, D07 EWV4, Éire

TU Dublin - Park House Grangegorman
191 North Circular Road, D07 EWV4, Ireland

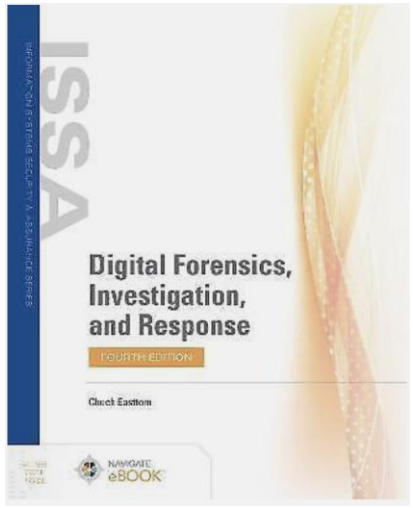
OT Baile Átha Cliath
Gráinseach Ghormáin
D07 H6K8, Éire

TU Dublin
Grangegorman
D07 H6K8, Ireland

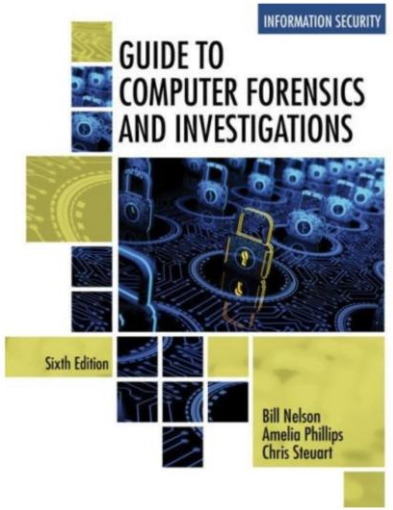
~ +353 1 220500
~ tudublin.ie

Overview

- Intro to main e-mail components
- E-mail Headers
- Walkthrough Example
- Key identifiers for an e-mail investigation



Book reference: Chapter 11



Book reference: Chapter 11

Why is Email Forensics Important

- Email evidence is an important part of any computer investigation
- Investigator must know how e-mail is processed to examine and interpret the unique content of e-mail messages.
- Focused on the recovery, analysis, and investigation of emails and their associated data to gather evidence for legal, organizational, or cybersecurity purposes.
- Looking at examining email messages, headers, metadata, attachments, and the email system to gather relevant evidence for the investigation.

Case Study Example

“The Court's expert concluded, in a 147-page detailed report, that the August 3, 2000 e-mail produced by Munshani "is clearly not authentic." In short, the expert's conclusion establishes that Munshani took the header from another e-mail sent to him by Mr. Trivedi, altered the substance of that e-mail to provide supporting evidence that would avoid a statute of frauds defense, and then provided the altered e-mail in response to documentary production and urged its authenticity in sworn affidavits in the Federal Court and in this Court.”

Munshani v. Signal Lake, No, No. 005529BLS, (Mass. Cmmw. Oct. 9, 2001) : https://casetext.com/case/munshani-v-signal-lake

The Extended/Enhanced Simple Mail Transfer Protocol number in the message header didn’t match. A text editor was used to alter an existing email received from the CTO.

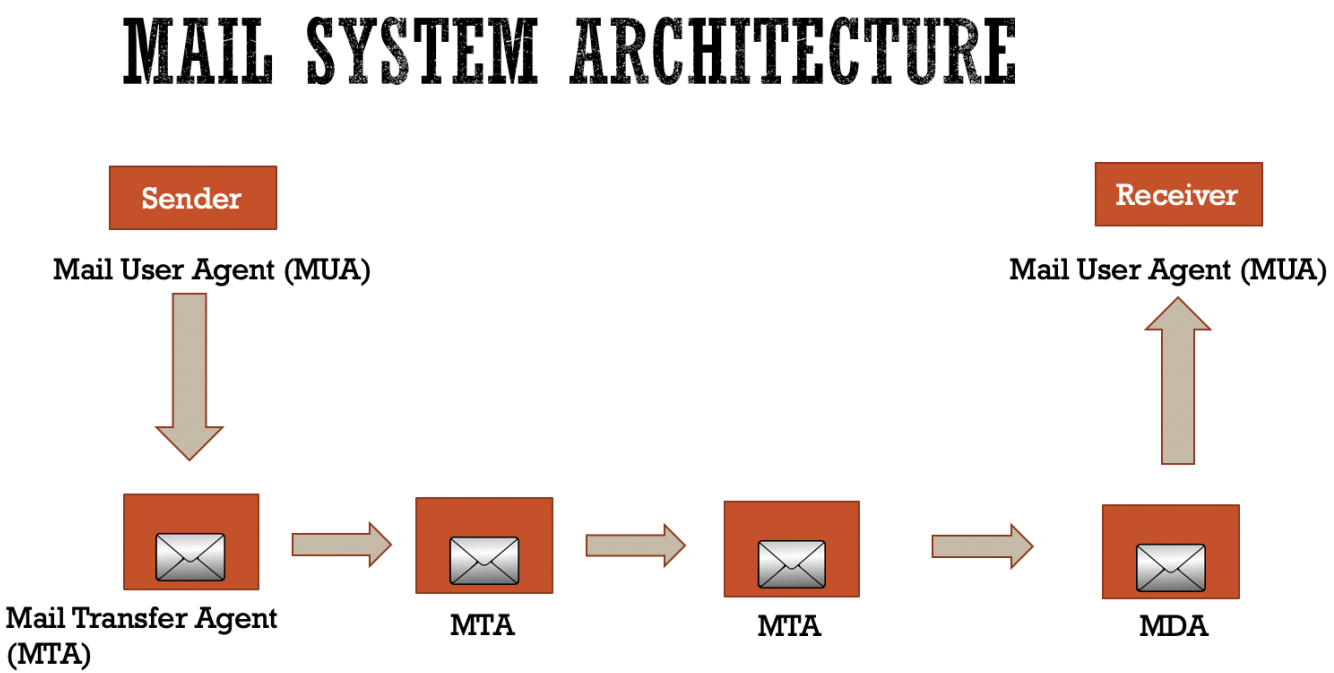
Investigating e-mail crimes

- Investigating e-mail may be criminal or policy violations.
- Goal is to prove or disprove the alleged offence.
- As per a standard investigation, we need to collect evidence, conduct the investigation and present the findings.
- It is important to know the appropriate privacy laws for a given jurisdiction.

Legal Considerations

- General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- Criminal Justice (Offences Relating to Information Systems) Act 2017: Protects against unauthorized access, interception, or alteration of emails.

Basic operation of e-mail



Where:

- MUA – Mail User Agent
  - Client application ti send and receive mail
- MTA – Mail Transfer Agent
  - Accepts messages and routes them towards their intended destination
- SPF – Sender Policy Framework
  - Specify what servers are allowed to send email on the domains behalf. SPF is used as a check to see if an email was send from a listed server (anti spam check)
- DKIM – Domain Keys Identified Mail
  - Cryptographic check to see if a message originated from the sending domain (anti spam an forged mail checks).
- MDA – Mail Delivery Agent
  - Deliver mail to client inbox

Mail Protocols

- SMTP (Simple Mail Transfer Protocol)
  - sending emails from a client to a server or between servers.
- POP3 – Post Office Protocol 3
  - Allow a MUA communicate with the MTA
- IMAP – Internet Message Access Protocol
  - Allow a MUA communicate with the MTA, benefits is emails remain on server, can sync multiple devices etc…
- POP3 has been mainly replaced by IMAP

Email Header

- An email header is a section of an email message that contains metadata about the email, providing detailed technical information about its origins, routing, and handling. It is not typically visible in the main body of the email that users see but can be viewed through advanced settings in email clients.
- Depending on the system, there are different mechanisms to view the full email header for a given email.

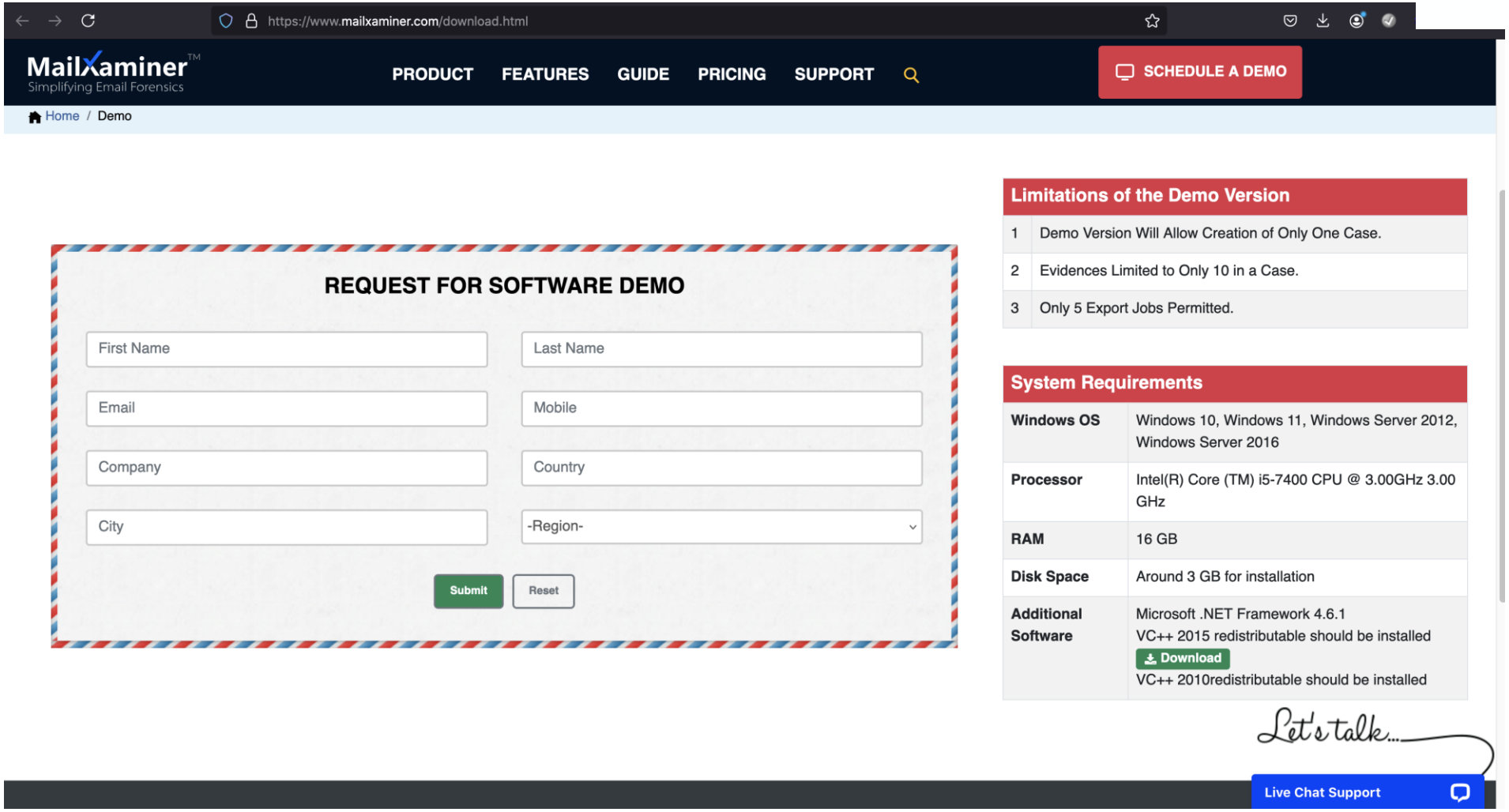
The method for viewing headers depends on the email client:
Gmail: Open the email → Click the three-dot menu (top-right) → Select *Show Original*.
Outlook: Open the email → Right-click → Select *View Source* or *Message Options* (look for the *Internet headers* section).
Apple Mail: Open the email → Select *View* → *Message* → *All Headers*.
Thunderbird: Open the email → Select *View* → *Message Source*.

Tool Demo

- **Email Examiner Software**
  - https://www.freeviewer.org/email-forensics/

"Being one of the most trusted Email Examiner Software in the industry, this application permits users to load and ingest data from multiple platforms. A user can load email data files from 25+ desktop based email clients, all IMAP based cloud-based platforms. Moreover, users can also disk image files and Skype to scan its chats and calls."

Tool Demo….


https://www.mailxaminer.com/download.html
MailXaminer
Simplifying Email Forensics
PRODUCT
FEATURES
GUIDE
PRICING
SUPPORT
SCHEDULE A DEMO
Home / Demo
REQUEST FOR SOFTWARE DEMO
First Name
Last Name
Email
Mobile
Company
Country
City
-Region-
Submit
Reset
Limitations of the Demo Version
1 Demo Version Will Allow Creation of Only One Case.
2 Evidences Limited to Only 10 in a Case.
3 Only 5 Export Jobs Permitted.
System Requirements
Windows OS
Windows 10, Windows 11, Windows Server 2012, Windows Server 2016
Processor
Intel(R) Core (TM) i5-7400 CPU @ 3.00GHz 3.00 GHz
RAM
16 GB
Disk Space
Around 3 GB for installation
Additional Software
Microsoft .NET Framework 4.6.1
VC++ 2015 redistributable should be installed
Download
VC++ 2010redistributable should be installed
Let's talk...
Live Chat Support

Examining e-mail Headers

- Once we have an e-mail header we can begin our investigation.
- To start we will need to have a good understanding of the key header fields in the e-mail header

- Example:
- Gmail to Gmail demo

Received (key header fields)

- Lists the mail servers the email passed through, from the sender to the recipient.
- Look at the first "Received" line (closest to the bottom of the header) to identify the sender's originating IP address.
- Check the timestamps in each "Received" line to trace the email's journey and detect delays or abnormalities.

```
Received-SPF: pass (google.com: domain of jonmcire2016@gmail.com designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20230601 header.b=Bw1LrZwj;
       spf=pass (google.com: domain of jonmcire2016@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=jonmcire2016@gmail
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com;
       dara=pass header.i=@gmail.com
```

First Received entry in our example

From (key header fields)

- Shows the sender's email address.
- Cross-check against the Return-Path and SPF/DKIM results to detect spoofing.

```
MIME-Version: 1.0
From: Jon McCarthy <jonmcire2016@gmail.com>
Date: Sat, 23 Nov 2024 13:28:45 +0000
Message-ID: <CAM-CHUZYP0tSGmkN_Siwpf7x61E22isLk_Xv6YKxKxSNX0Y45w@mail.gmail.com>
Subject: Test Email
To: jonathan.mccarthy.ire@gmail.com
Content-Type: multipart/alternative; boundary="0000000000007f5e280627947bbe"
```

To (key header fields)

- Indicates the recipient's email address. Ensure it matches the intended target.

```
MIME-Version: 1.0
From: Jon McCarthy <jonmcire2016@gmail.com>
Date: Sat, 23 Nov 2024 13:28:45 +0000
Message-ID: <CAM-CHUZYP0tSGmkN_Siwpf7x61E22isLk_Xv6YKxKxSNX0Y45w@mail.gmail.com>
Subject: Test Email
To: jonathan.mccarthy.ire@gmail.com
Content-Type: multipart/alternative; boundary="0000000000007f5e280627947bbe"
```

Subject (key header fields)

- Look for suspicious or deceptive subject lines (e.g., "URGENT" or "Congratulations").

```
MIME-Version: 1.0
From: Jon McCarthy <jonmcire2016@gmail.com>
Date: Sat, 23 Nov 2024 13:28:45 +0000
Message-ID: <CAM-CHUZYP0tSGmkN_Siwpf7x61E22isLk_Xv6YKxKxSNX0Y45w@mail.gmail.com>
Subject: Test Email
To: jonathan.mccarthy.ire@gmail.com
Content-Type: multipart/alternative; boundary="0000000000007f5e280627947bbe"
```

Date (key header fields)

- Confirms when the email was sent. Compare this with other timestamps in the header to detect manipulation.

```
MIME-Version: 1.0
From: Jon McCarthy <jonmcire2016@gmail.com>
Date: Sat, 23 Nov 2024 13:28:45 +0000
Message-ID: <CAM-CHUZYP0tSGmkN_Siwpf7x61E22isLk_Xv6YKxKxSNX0Y45w@mail.gmail.com>
Subject: Test Email
To: jonathan.mccarthy.ire@gmail.com
Content-Type: multipart/alternative; boundary="0000000000007f5e280627947bbe"
```

Return-Path (key header fields)

- indicates where undelivered emails would be sent back. If this doesn't match the "From" address, it may be a red flag.

```
Return-Path: <jonmcire2016@gmail.com>
```

Message-ID (key header fields)

- A unique identifier for the email, generated by the originating mail server.
- If this is missing or unusual (e.g., random strings), it could indicate a forged email.

```
Message-ID: <CAM-CHUZYP0tSGmkN_Siwpf7x61E22isLk_Xv6YKxKxSNX0Y45w@mail.gmail.com>
```

Authentication Results (key header fields)

- Includes SPF, DKIM, and DMARC results:SPF (Sender Policy Framework): Verifies if the sender's server is authorized to send on behalf of the domain.
- DKIM (DomainKeys Identified Mail): Checks if the email was digitally signed by the sender.
- DMARC (Domain-based Message Authentication, Reporting, and Conformance): Ensures alignment between SPF/DKIM and the "From" address.
- Look for "pass" or "fail" in these checks to validate sender authenticity.

Content-Type (key header fields)

- Specifies the format of the email (e.g., plain text, HTML, or multipart). HTML emails with embedded scripts or links may indicate phishing.

```
Content-Type: text/plain; charset="UTF-8"
```

X-Headers (key header fields)

- Custom headers added by email systems (e.g., spam scores or internal tracking). Look for unusual tags like *X-Spam*, *X-Originating-IP*, or *X-Mailer*.

```
X-Gm-Message-State: AOJu0YxBA4/0P5Kb2a53JyKXjBisL+d0tJ8ssKno7aY/+Q+kEB0Z1QR5 KDsyLOTrclWrPlV35TiAVvYvjqtbzb9vLZDZwZWIfT6DOe2WNpfWTz7YPwiFnVj
X-Gm-Gg: ASbGncuu1LEn5sS6dKtEzIF1waKiqxQfEbbTztbiRtaEx2wFgUEHBe0AjF/+21qVlqr wp4UzWpZSi4QzTZOghVc5/jY5/01XrYQ=
X-Google-Smtp-Source: AGHT+IHjUz7AZNI444l0YibM8iOqC7ld0NXV23zMbojJFYtKt9hUZ6b1EPJLCVwen3o3CZle2URI1oEeQFZYTcLfXIY=
X-Received: by 2002:a05:600c:4e08:b0:42f:7c9e:1f96 with SMTP id 5b1f17b1804b1-433ce420a5cmr49401555e9.1.1732368540849; Sat, 23 Nov 2024 05:2
MIME-Version: 1.0
```

Identify Key Forensic Information

- **IP Address**:
  - Extract the originating IP address from the last "Received" entry.
  - Use an IP lookup tool to determine the sender's geographical location or organization.
  - Beware of private IPs (e.g., 192.168.x.x) as they may indicate an internal server.
- **Timestamps**:
  - Verify if timestamps match the expected sending time.
  - Look for discrepancies that may indicate time zone manipulation.

MxToolbox Results

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
TECHNOLOGICAL UNIVERSITY DUBLIN

Headers Found

Header Name	Header Value
Delivered-To	jonathan.mccarthy.ire@gmail.com
X-Received	by 2002:a05:600c:3b9b:b0:431:4c14:abf4 with SMTP id 5b1f17b1804b1-433ce427c60mr57476665e9.14.1732368541609; Sat, 23 Nov 2024 05:29:01 -0800 (PST)
ARC-Seal	i=1; a=rsa-sha256; t=1732368541; cv=none; d=google.com; s=arc-20240605; b=Q7SS9AKGAqcfNe8Q6zlOJ7oy3v8p/Le4KAf+35t085BWydm0UYCxluc3A9wqkt/twK VPxkFtTVx8egthfL1+JeVD1kGrUcBaDczz/Rxpw7d3WtVeRl8v/NctXueDD5Zs7wsQo9 RDrp8ydZWRqrTpUvVdk6o5mvTghvXC8IlrCpFHVFY9CMHeL14kM0KLowfivXQ4cxSGHh nmAYibl6EKpD0wPdZC2H4mLYHfRuBBAPidMcwh1ZwBfKNU/MWvS4G4dh8zuWs018B1hp gweCVJysxSjEFAqGMBCsCChkkFkj/G4al/zA/B85Y+6spmVimc4u/HcS50P8OtTEAgeV /53A==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605; h=to:subject:message-id:date:from:mime-version:dkim-signature; bh=urK7ZJpsV4QJyHdisBT89yTghGWRYQlZJtgstnaWUk0=; fh=MKa3ZjYdS0b/248TAQP/7yOaUaxbH5l2jk2mDJfkl0g=; b=RhHXwad2a5KTwoKT5UvZP7uL4Uev2PifKX7wLWUPTE5Lf27P0NmTk5w5JWDq+7wC7D R7NkitlbmVBPiaS4PE1UxbsgqBEVjTN3ice/G2kHc5GHB+CW5YPCBX0l3Ywp1twkr7pr gfnH0z4QZ+xB0HjFZK1EGi+syPXe5rGzbnAKbdt7gkm7vD9FwNJS6xnYRyn5+JrnBz7y NlWMgDDsNxDw2lwD5O57wFYXPQKG5EsYGA5eJRTYZG8u4E2Z2i10p0pw2C1ztS00UhFD 6OMR0n+1AgLN/b1IYYtMuuDzUqYrZPKtKdq1a0xCqEZ9f5R3HpD2hos/w0+RyGaQTDwa EpQQ==; dara=google.com
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@gmail.com header.s=20230601 header.b=Bw1LrZwj; spf=pass (google.com: domain of jonmcire2016@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=jonmcire2016@gmail.com; dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com; dara=pass header.i=@gmail.com
Return-Path	<jonmcire2016@gmail.com>
Received-SPF	pass (google.com: domain of jonmcire2016@gmail.com designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results	mx.google.com; dkim=pass header.i=@gmail.com header.s=20230601 header.b=Bw1LrZwj; spf=pass (google.com: domain of jonmcire2016@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=jonmcire2016@gmail.com; dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com; dara=pass header.i=@gmail.com
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=20230601; t=1732368541; x=1732973341; dara=google.com; h=to:subject:message-id:date:from:mime-version:from:to:cc:subject :date:message-id:reply-to; bh=urK7ZJpsV4QJyHdisBT89yTghGWRYQlZJtgstnaWUk0=; b=Bw1LrZwjIuL7KvFxH8QPPHEtLl2a+nhnJEcFK+WOFaHng6JVbb98GFMXPrlZEh8qdm +V0E7daDC/ayrl6mMDZ9zuVzANY2jHKiUo8cQIL/7euxHsW+diFYngc9OrQ5yk4G4Iwe 9y2dhCiba7KY7h1gTSmkzAK2Wr31nRQmmc2za1rALDF6ik1wZRnr3CU/XJTA3X+AQX0q0pusw8kROsMVRkX3gMSRG2KQkZ66+1wwy6NOSiFXYyTttYQ7olkrEPzx0T5v6x/ZTNz7 wrCx+qyysFWMj3BlkYYRc7YHB309bET8KfZoNK9CrPRxLkDTZwk1WCtKkV4l3bGrAnpM E31g==
X-Google-DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20230601; t=1732368541; x=1732973341; h=to:subject:message-id:date:from:mime-version:x-gm-message-state :from:to:cc:subject:date:message-id:reply-to; bh=urK7ZJpsV4QJyHdisBT89yTghGWRYQlZJtgstnaWUk0=; b=LqBEvqEBmWaRXNCqhQq/571EmH8kLVivIRl7nQjm4YZkF+gRtrh9kv8oGukarGls7T 78FfxhgM8MXTNlaSqgAbj8D1axYcs9bhdNzbfbnpn360JX7w7HrH4rnAJwnBhNhDPjb2 gz+4QGWh6DIoY0w7k8zWz6EurOa6xru6xqZiqrpWk+cNEASxWJA7hot+xS/uARa5DOoY h7QKBJ4NJfDafwoeiR1nv39zO57Ga790/g4rHGe04HKVaEPSFOntfxiFVog+yjK0b/x2 err9AAAHhdhdTkPxc/U2g3O3xqrZrl9ud3FaufdhURURUxVyL4nXNbq5YQTp+aPro1s4 Yzvg==
X-Gm-Message-State	AOJu0YxBA4/0P5Kb2a53JyKXjBisL+d0tJ8ssKno7aY/+Q+kEB0Z1QR5 KDsyLOTrclWrPlV35TiAVvYvjqtbzb9vLZDZwZWlfT6DOe2WNpfWTz7YPwiFnVjqJ1otuJ3rqS4 7CJ5/ArianITs2IFRLjj23W6fHluinQ==
X-Gm-Gg	ASbGncuu1LEn5sS6dKtEzIF1waKiqxQfEbbTztbiRtaEx2wFgUEHBe0AjF/+21qVlqr wp4UzWpZSi4QzTZOghVc5/jY5/01XrYQ=
X-Google-Smtp-Source	AGHT+IHjUz7AZNI444l0YibM8iOqC7Id0NXV23zMbojJFYtKt9hUZ6b1EPJLCVwen3o3CZle2URI1oEeQFZYTcLfXlY=
MIME-Version	1.0
From	Jon McCarthy <jonmcire2016@gmail.com>
Date	Sat, 23 Nov 2024 13:28:45 +0000
Message-ID	<CAM-CHUZYP0tSGmkN_Siwpf7x61E22isLk_Xv6YKxKxSNX0Y45w@mail.gmail.com>
Subject	Test Email
To	jonathan.mccarthy.ire@gmail.com
Content-Type	multipart/alternative; boundary="0000000000007f5e280627947bbe"

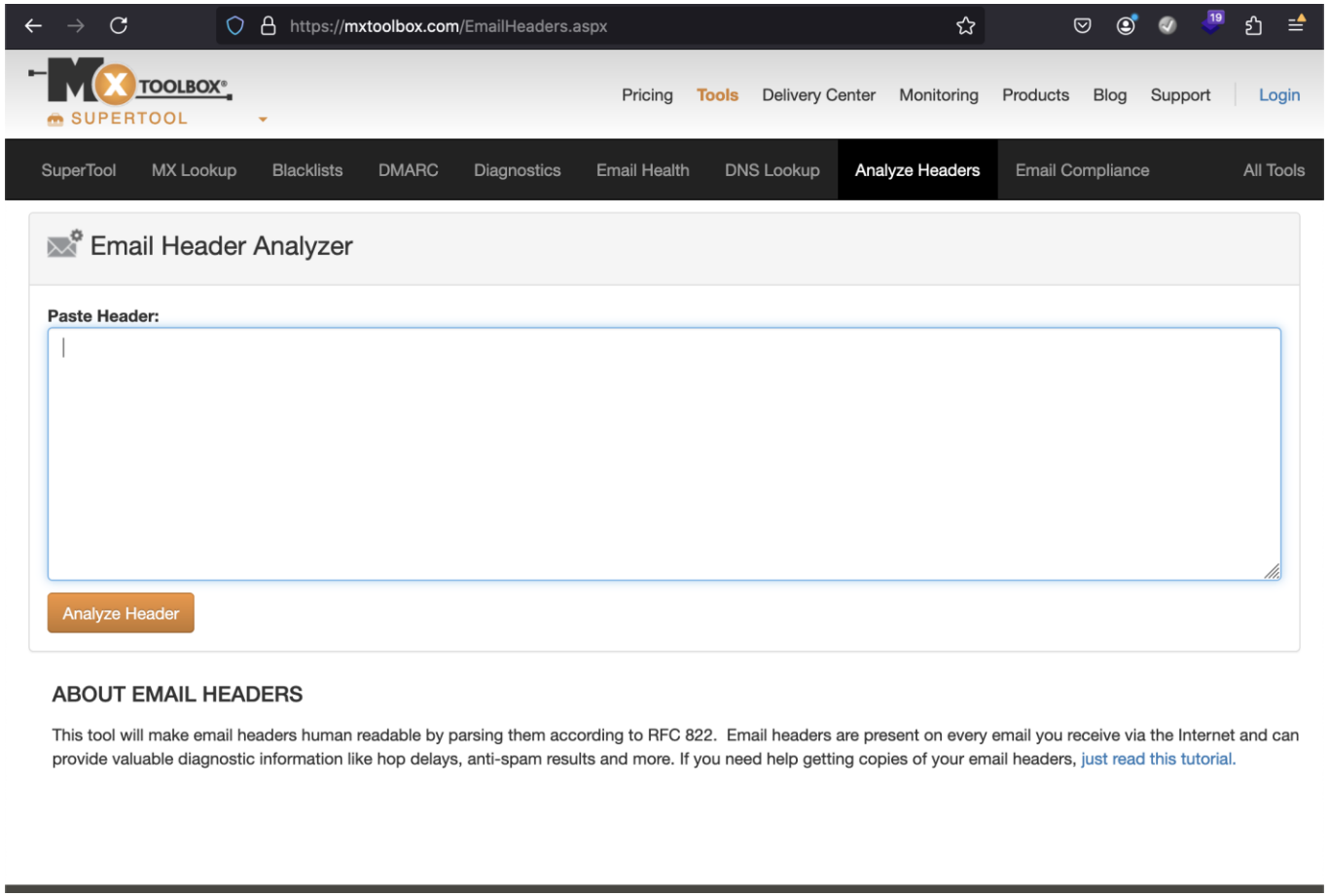
Identify Key Forensic Information

- **Email Spoofing**:
  - Check if the "From" address matches the authenticated domain (SPF/DKIM).
  - Use online tools to validate DKIM signatures and SPF alignment.
- **Relay Analysis**:
  - Trace the path of the email across servers. If unexpected servers appear, it could indicate redirection or tampering.

Forensic Tools

- Specialized tools can simplify header analysis and provide detailed reports:
- **MxToolbox Email Header Analyzer**: Extracts and interprets email header information.
- **MailXaminer**: A forensic email analysis tool for detailed investigation.
- **Header Analyzer Pro**: Parses headers for quick detection of anomalies.

MxToolbox Email Header Analyzer

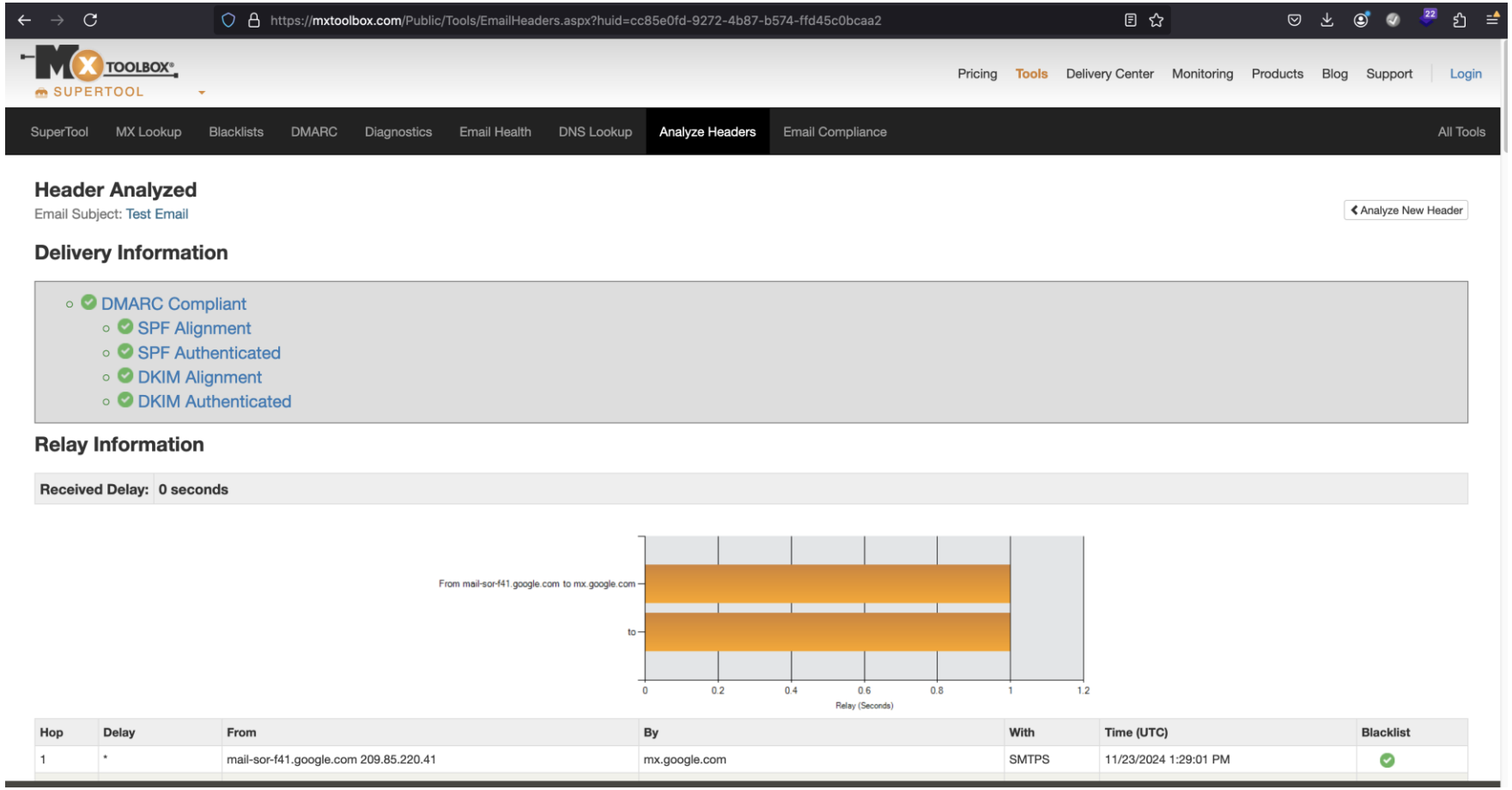


ABOUT EMAIL HEADERS

"This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provide valuable diagnostic information like hop delays, anti-spam results and more. If you need help getting copies of your email headers, just read this tutorial. "

https://mxtoolbox.com/EmailHeaders.aspx

Results


https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=cc85e0fd-9272-4b87-b574-ffd45c0bcaa2
MX TOOLBOX SUPERTOOL
Pricing Tools Delivery Center Monitoring Products Blog Support Login
SuperTool MX Lookup Blacklists DMARC Diagnostics Email Health DNS Lookup Analyze Headers Email Compliance All Tools
Header Analyzed
Email Subject: Test Email
Analyze New Header
Delivery Information
DMARC Compliant
SPF Alignment
SPF Authenticated
DKIM Alignment
DKIM Authenticated
Relay Information
Received Delay: 0 seconds
From mail-sor-f41.google.com to mx.google.com
to
0 0.2 0.4 0.6 0.8 1 1.2
Relay (Seconds)
Hop Delay From By With Time (UTC) Blacklist
1 * mail-sor-f41.google.com 209.85.220.41 mx.google.com SMTPS 11/23/2024 1:29:01 PM

Interpret Findings

- **Phishing or Spoofing**:
  - Failing SPF/DKIM/DMARC checks.
  - "From" address not aligning with return-path or originating server.
- **Spam Indicators**:
  - High spam scores in X-headers.
  - Suspicious subject lines, multiple recipients, or malformed message IDs.
- **Malware**:
  - Check attachments or links in the email body for malicious content.
  - Investigate the "Content-Type" field for hidden scripts.

Examining an Email

- Email headers contain information about the path that email traversed

- The first thing to look at is the following:
- **From:** jonathan.mccarthy@tudublin.ie
- **Return path:** jonathan.mccarthy@tudublin.ie
  - If these don't match we may have a spoofed email.
- It is easy to spoof the **from:**, the return path can be spoofed too.
- The **Return-Path:** field is verified by the Sender Policy Framework (SPF)
- **SPF / DKIM / DMARC / ARC** data (where available)

Examining an Email

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
TU DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN

Received Headers

- The received header is the most important part of the email header and is usually the most reliable.
- They offer a list of all the servers the message visited as it was routed from source to destination.
- The top-most received header is closest to the destination, the bottom-most received header is closest to the source.
- The means the last Received: is where the mail originated.
- **This IP can be checked (with dig) to see if this matches the domain name in the senders email address. We can check this by comparing value from the final bottom-most Received: header against the value of DNS entry of the domain**

Examining an Email

- SPF
  - SPF can pass for a spoofed email address if the Return Path has not been spoofed
  - SPF uses the Return Path email address in its check process.
  - If the return path is spoofed SPF will catch this (dig).

- The result of the verification is detailed in the Authentication-Results: spf=pass

Important Fields

- Delivered To:
- From:
- Return-Path:
- Message-ID:
- Sender Mailer Fingerprints (X-Headers:)
  - headers that are added to messages along with standard headers, can be custom to the mail provider
- Received:

Suspicious Events

- Detect spoofed emails
- Determine source of origin for email
- Detect modifications
- Identify the actual sender, recipient, data and time when it was sent, etc.
- Email found on client can be linked to the originating server via unique ID

Questions