

Forensic Email Investigations Training

ARMAN GUNGOR
METASPIKE

MARCH 22-23, 2023
SERVICES AUSTRALIA

Background

Arman Gungor
CEO, Metaspike
@ArmanGungor
www.metaspike.com

Agenda — Day 1

- ▶ Anatomy of An Email Message
 - ▶ Message Headers
 - ▶ Message Body, Attachments, and MIME
 - ▶ Email over The Internet
- ▶ Sources of Email Evidence
- ▶ Common Hosted Email Services and Protocols
- ▶ Forensic Email Preservation
- ▶ Email Storage Formats
- ▶ Server Metadata, Logs, and History Records
- ▶ Q&A

Agenda — Day 2

- ▶ Forensic Email Authentication
 - ▶ Authenticating Messages
 - ▶ DKIM, ARC, SPF, DMARC
 - ▶ Hidden Metadata
 - ▶ Leveraging Server Metadata
- ▶ MAPI
- ▶ Q&A

What is Email Forensics?

Intersection with related disciplines

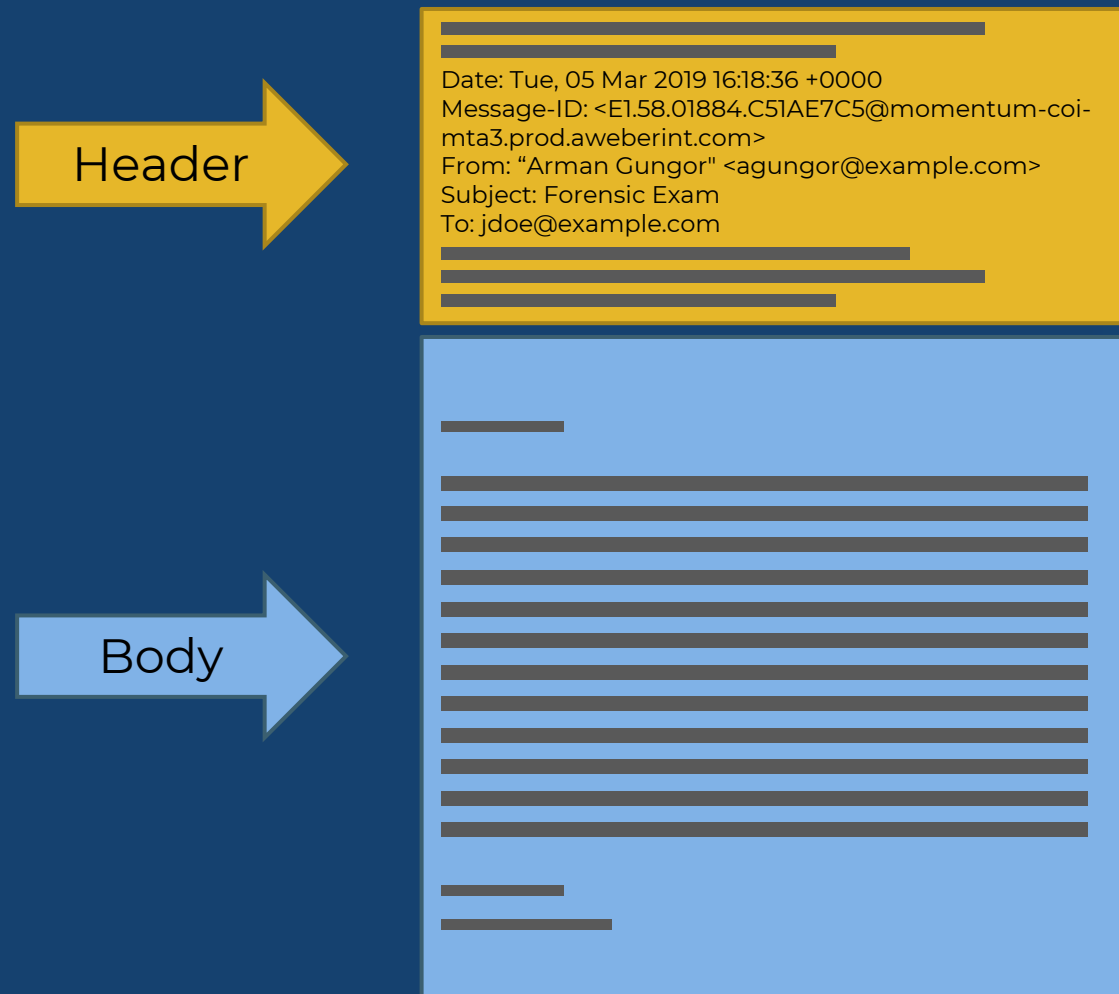
- ▶ Cloud forensics
- ▶ Network forensics
- ▶ Dead-box forensics
- ▶ Mobile forensics
- ▶ Malware analysis / reverse engineering
- ▶ Incident response
- ▶ More...

Anatomy of An Email Message

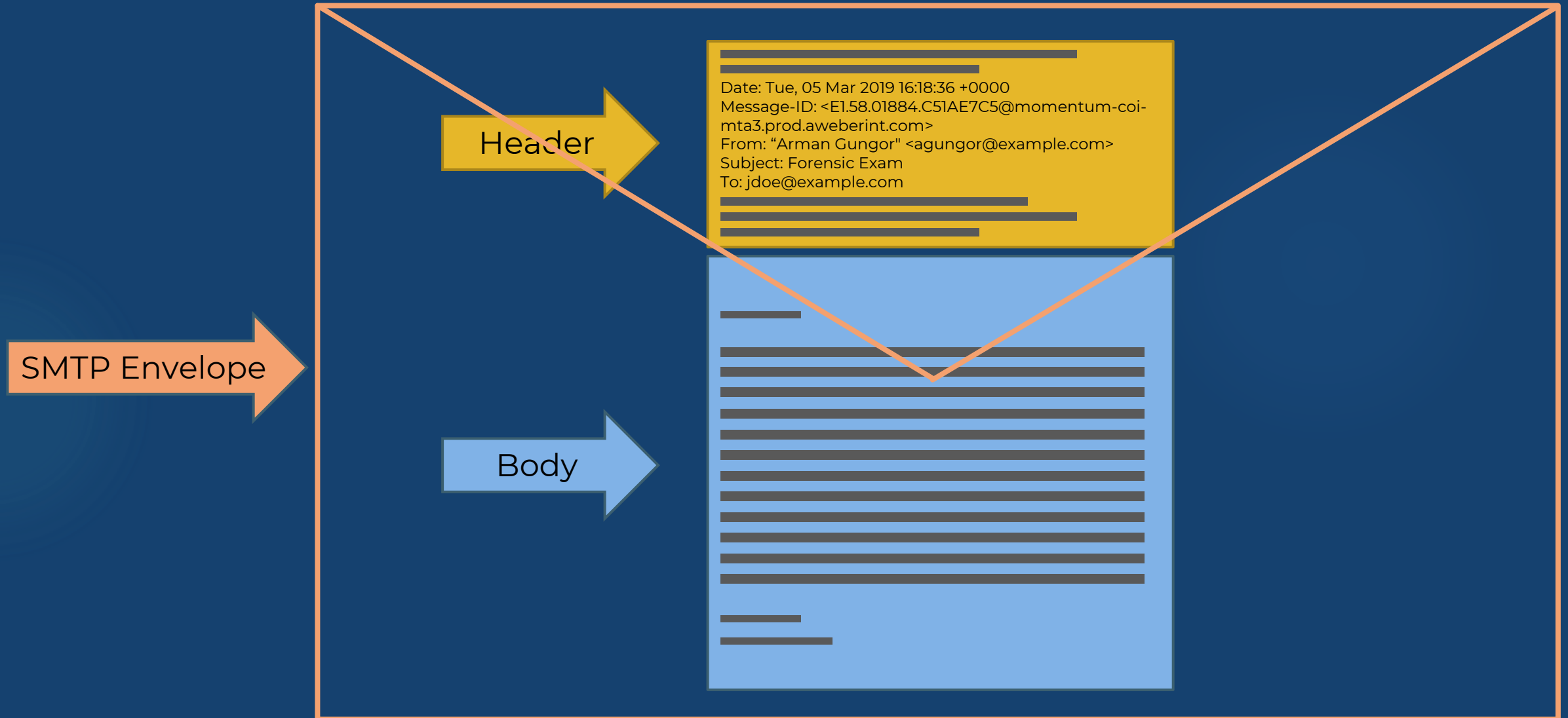
- ▶ What is Internet Message Format?
 - ▶ RFC 5322 — <https://datatracker.ietf.org/doc/html/rfc5322>
 - ▶ Contents
 - ▶ Text messages
 - ▶ US ASCII charset (1 – 127)
 - ▶ For images & other attachments, see MIME ([RFC 2045](#))
- ▶ Why is IMF needed?
- ▶ When is it used?
- ▶ Message envelope ([RFC 5321](#)) vs. contents

Ref [1](#) [2](#)

Internet Message Format



Internet Message Format



Internet Message Format

Let's start creating our own MIME message!

Message Headers

- ▶ RFC 4021 — Registration of Mail and MIME Header Fields
<https://datatracker.ietf.org/doc/html/rfc4021>
- ▶ The Origination Date Field
Specifies the date and time at which the creator of the message indicated that the message was complete and ready to enter the mail delivery system.

Date: Wed, 18 Nov 2020 15:26:08 -0800

- ▶ Message-ID:
The "Message-ID:" field provides a unique message identifier that refers to a particular version of a particular message. The uniqueness of the message identifier is guaranteed by the host that generates it.

Message-ID: <0a6f01d5c4cc\$b9145e70\$2b3d1b50\$@gmail.com>

Message Headers

- ▶ RFC 4021 — Registration of Mail and MIME Header Fields
<https://datatracker.ietf.org/doc/html/rfc4021>
- ▶ The Origination Date Field
Specifies the date and time at which the creator of the message indicated that the message was complete and ready to enter the mail delivery system.

Date: Wed, 18 Nov 2020 15:26:08 -0800

- ▶ Message-ID:
The "Message-ID:" field provides a unique message identifier that refers to a particular version of a particular message. The uniqueness of the message identifier is guaranteed by the host that generates it.

Message-ID: <0a6f01d5c4cc\$b9145e70\$2b3d1b50\$@gmail.com>

Message Headers — Message-ID

- ▶ 01d5c4cc:b9145e70 ⇒ 0x01d5c4ccb9145e70 (FILETIME)
- ▶ 2020-01-06 20:06:03.4790000 +00:00
- ▶ How are Message-ID values calculated?
- ▶ Python email library source code (see make_msgid; line 174 - 194)
<https://github.com/python/cpython/blob/main/Lib/email/utils.py>

Message-ID: <142480216486.20800.16526388040877946887@nightshade.la.mastaler.com>

Ref 1

Message Headers — Message-ID

- ▶ 01d5c4cc:b9145e70 ⇒ 0x01d5c4ccb9145e70 (FILETIME)
- ▶ 2020-01-06 20:06:03.4790000 +00:00
- ▶ How are Message-ID values calculated?
- ▶ Python email library source code (see make_msgid; line 174 - 194)
<https://github.com/python/cpython/blob/main/Lib/email/utils.py>

Message-ID: <142480216486.20800.16526388040877946887@nightshade.la.mastaler.com>

1424802164860 (Epoch time) ⇒ Tuesday, February 24, 2015 6:22:44.860 PM (GMT)

MTA Message-ID Override

- ▶ Original Message-ID:

Message-ID: <000701d94304\$3d1e0cd0\$b75a2670\$@doe@ool1eo.com>

MTA Message-ID Override

- ▶ Original Message-ID:

Message-ID: <000701d94304\$3d1e0cd0\$b75a2670\$@doe@oolleo.com>

- ▶ [Outlook 2007 Bug](#) causing malformed Message-IDs.

- ▶ Gmail MTA override:

Message-ID: <63efd26d.170a0220.527cf.ba99SMTPIN_ADDED_BROKEN@mx.google.com>

X-Google-Original-Message-ID: <000701d94304\$3d1e0cd0\$b75a2670\$@doe@oolleo.com>

Ref [1](#)

MTA Message-ID Override

- ▶ Original Message-ID:

Message-ID: <000701d94304\$3d1e0cd0\$b75a2670\$@doe@oolleo.com>

- ▶ [Outlook 2007 Bug](#) causing malformed Message-IDs.

- ▶ Gmail MTA override:

Message-ID: <63efd26d.170a0220.527cf.ba99SMTPIN_ADDED_BROKEN@mx.google.com>

X-Google-Original-Message-ID: <000701d94304\$3d1e0cd0\$b75a2670\$@doe@oolleo.com>

Message Headers — In-Reply-To

- ▶ The message identifier(s) of the original message(s) to which the current message is a reply.

In-Reply-To: <CAMvYnDOXTyeEceg_LarzmzdQ0LTvjjpRdq+r8+BrKU9qRcb_QA@mail.gmail.com>

Message Headers — References

- ▶ Contains a list of all Message-IDs of messages in the preceding email chain.

References: <CAMvYnDMmZTb+83cKfh8BzbzGZByxvPDxbF2kCikQFfn7ggLicQ@mail.gmail.com>
<1238690485.283884.1611701787702@mail.yahoo.com>

Message Headers — Reply-To

- ▶ Indicates the mailbox(es) to which the author of the message suggests that replies be sent. In the absence of the "Reply-To:" field, replies SHOULD by default be sent to the mailbox(es) specified in the "From:" field.

Reply-To: <jdoe@example.com>

Message Headers — Return-Path

- ▶ Return path for message response diagnostics. When the delivery SMTP server makes the "final delivery" of a message, it inserts a return-path line at the beginning of the mail data.

Return-Path: <jdoe@example.com>

Message Headers — Disposition-Notification-To

- ▶ Indicates that the sender wants a disposition notification when this message is received (read, processed, etc.) by its recipients.
- ▶ E.g., “Request a Read Receipt” option in Outlook.

`Disposition-Notification-To: John Doe <jdoe@example.com>`

Side Note: TNEF

- ▶ Transport Neutral Encapsulation Format
- ▶ Encapsulates MAPI message properties
- ▶ Contains:
 - ▶ Original formatted version of the message (for example, fonts, text sizes, and text colors)
 - ▶ OLE objects (for example, embedded pictures or embedded Office documents)
 - ▶ Special Outlook features (for example, custom forms, voting buttons, or meeting requests)
 - ▶ Regular message attachments that were in the original message
- ▶ Winmail.dat or Win.dat

see <https://docs.microsoft.com/en-us/Exchange/mail-flow/content-conversion/content-conversion?view=exchserver-2019#Exchange>

Message Headers — Return-Receipt-To (non-standard)

- ▶ To set the value of the PidTagOriginatorDeliveryReportRequested property ([MS-OXOMSG] section 2.2.1.20), clients MUST set the (non-standard) Return-Receipt-To header value.
- ▶ I.e., “Request a Delivery Receipt” option in Outlook.

Return-Receipt-To: <jdoe@example.com>

Message Headers — Thread-Index (non-standard)

- ▶ Carries the conversation index (i.e., PR_CONVERSATION_INDEX) value in base64-encoded form.

Thread-Index: AddpUaqWUvNBn/8KTG60i74ymh4DjQ==

Message Headers

► X-Originating-IP

X-Originating-IP: [47.19.100.11]

► X-Mailer

X-Mailer: WebService/1.1.15302 YMailNorrin Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36 Edg/80.0.361.62

Message Headers

- ▶ Content-Length

Content-Length: 2032

- ▶ DKIM-Signature
- ▶ Authentication-Results
- ▶ Received-SPF
- ▶ ARC-Authentication-Results
- ▶ ARC-Message-Signature
- ▶ ARC-Seal

MIME

- ▶ What is Multipurpose Internet Mail Extensions (MIME)?
 - ▶ RFC 2045 — <https://datatracker.ietf.org/doc/html/rfc2045>
- ▶ Why is MIME needed?
 - ▶ Non-ASCII text bodies
 - ▶ Non-text message bodies
 - ▶ Multi-part message bodies
 - ▶ Non-ASCII headers

MIME Header Fields

- ▶ MIME-Version
- ▶ Content-Type
- ▶ Content-Transfer-Encoding
- ▶ Content-Disposition
- ▶ Content-ID
- ▶ Content-Description
- ▶ Content-Base
- ▶ Content-Location
- ▶ Content-Features
- ▶ Content-Language
- ▶ Content-Alternative
- ▶ Content-MD5
- ▶ Content-Duration

MIME Headers — MIME Version

- ▶ MIME-Version: 1.0
- ▶ MIME-Version: 1.0 (produced by XYZ Corp Vx.x)
- ▶ MIME-Version: (produced by XYZ Corp Vx.x) 1.0
- ▶ MIME-Version: 1.(produced by XYZ Corp Vx.x)0

MIME Headers — MIME Version

- ▶ MIME-Version: 1.0
- ▶ MIME-Version: 1.0 (produced by XYZ Corp Vx.x)
- ▶ MIME-Version: (produced by XYZ Corp Vx.x) 1.0
- ▶ MIME-Version: 1.(produced by XYZ Corp Vx.x)0

MIME Headers — Content-Type

- ▶ Defaults to:
 - ▶ Content-type: text/plain; charset=us-ascii
- ▶ Discrete Types:
 - ▶ text
 - ▶ image
 - ▶ audio
 - ▶ video
 - ▶ application
- ▶ Composite Types
 - ▶ message
 - ▶ multipart

MIME Headers — Content-Transfer-Encoding

`Content-transfer-encoding: base64`

- ▶ Mechanism:
 - ▶ 7bit
 - ▶ 8bit
 - ▶ binary
 - ▶ quoted-printable
 - ▶ base64
 - ▶ ietf-token (defined by a standards-track RFC & registered with IANA)
 - ▶ x-token (non-standard, private extension)

Quoted-Printable Content-Transfer-Encoding

- ▶ Encoded lines must not be longer than 76 characters, not counting the trailing CRLF.
- ▶ Longer lines are folded using soft line breaks—an equal sign as the last character on an encoded line.
- ▶ CR ⇨ (ASCII 13) ⇨ =0D
- ▶ LF ⇨ (ASCII 10) ⇨ =0A
- ▶ Space ⇨ (ASCII 32) ⇨ =20
- ▶ = ⇨ (ASCII 61) ⇨ =3D
- ▶ " ⇨ (ASCII 34) ⇨ =22

Quoted-printable Example

=C2=A0 $\Rightarrow$ 0xC2 0xA0 (UTF-8) $\Rightarrow$ U+00A0 $\Rightarrow$ Non-breaking space ()

Ref 1

Base64 Content-Transfer-Encoding

```
TG9yZW0gaXBzdW0gZG9sb3Igc2l0IGFtZXQsIGNvbmlY3R1dHVyIGFkaXBpc2NpbmcgZWxpdC4g  
TWF1cm1zIGF1Z3VlIGFyY3UsIG1hdHRpcyBzZWQgZXJhdCBpbwgdGVtcG9yIHZhcm11cyB2ZWxp  
dC4gU3VzcGVuZGlzc2UgdWxsYW1jb3JwZXIgdmsIG5pYmogaWQgZWZmaWNpdHVyLiBOYW0gc29k  
YWxlcwgc2FwaWVlIHBlbHRyaWNlcYB0ZW1wdXMsIG51bGxhIGV4IHZlc3RpYnVsdW0gcXVh  
bSwgY29uc2VjdGV0dXIgdHJpc3RpcXVlIGFudGUgZXJhdCBpZCB1cm5hLiBGdXNjZSB2ZWwgbWFz  
c2EgYSB0ZWxsZXNlcY29uZ3VlIGF1Y3RvcjBlbSBhIGxlbY4gUHJhZXNlbnQgcHJldGl1bSBvZGlv  
IHNPdCBhbWV0IGZhdWNpYnVzIHZ1bHB1dGF0ZS4=
```

► Base64 v. Quoted-Printable

Message Headers

Using non-ASCII header field bodies:

=?charset?encoding?encoded-text?=

Example 1:

=?utf-8?Q?Hello=20World?=
Hello World

Example 2:

=?utf-8?q?V-Day_Debt_=26_Inflation=F0=9F=92=94?=
V-Day Debt & Inflation 💔

B ⇨ Base64
Q ⇨ Quoted Printable

Ref [1](#)

MIME Boundaries

- ▶ Theoretical simplest delimiter "--o" / "--o--" (not realistic)
- ▶ Example:

```
--my boundary
```

```
...
```

```
--my boundary--
```

- ▶ Must not appear in the body parts being encapsulated.
- ▶ Unique boundaries are typically created programmatically.
- ▶ *More on this later in forensic analysis.*

Ref [1](#)

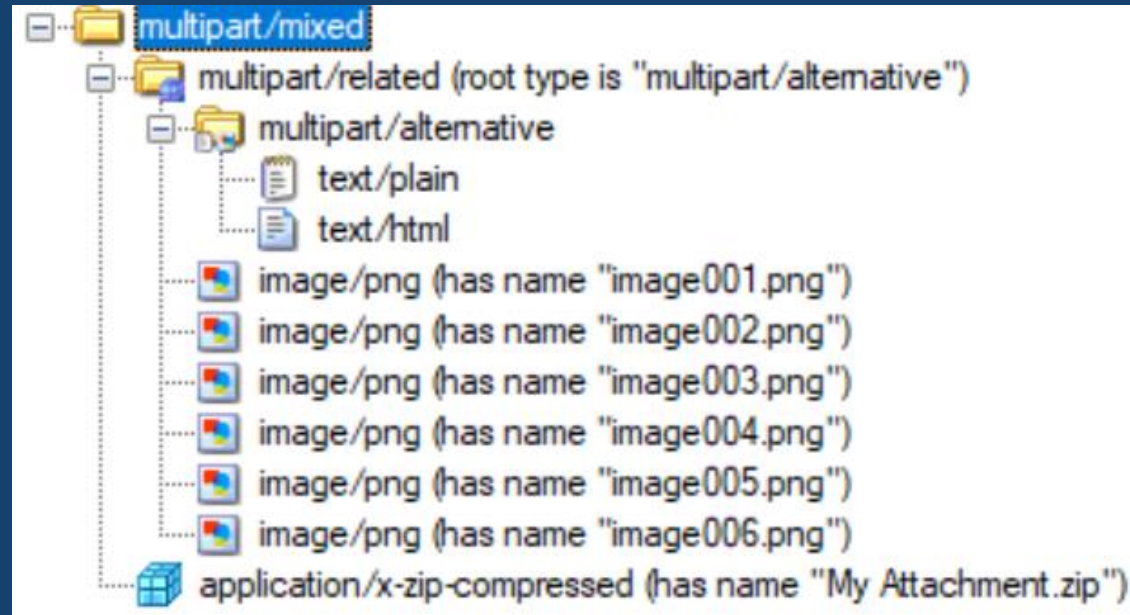
MIME Headers — Content-Disposition

- ▶ RFC 2183 — <https://datatracker.ietf.org/doc/html/rfc2183>
- ▶ Disposition type
 - ▶ Inline
 - ▶ Attachment
- ▶ Disposition Parameters
 - ▶ Filename
 - ▶ Creation date
 - ▶ Modification date
 - ▶ Read date
 - ▶ Size

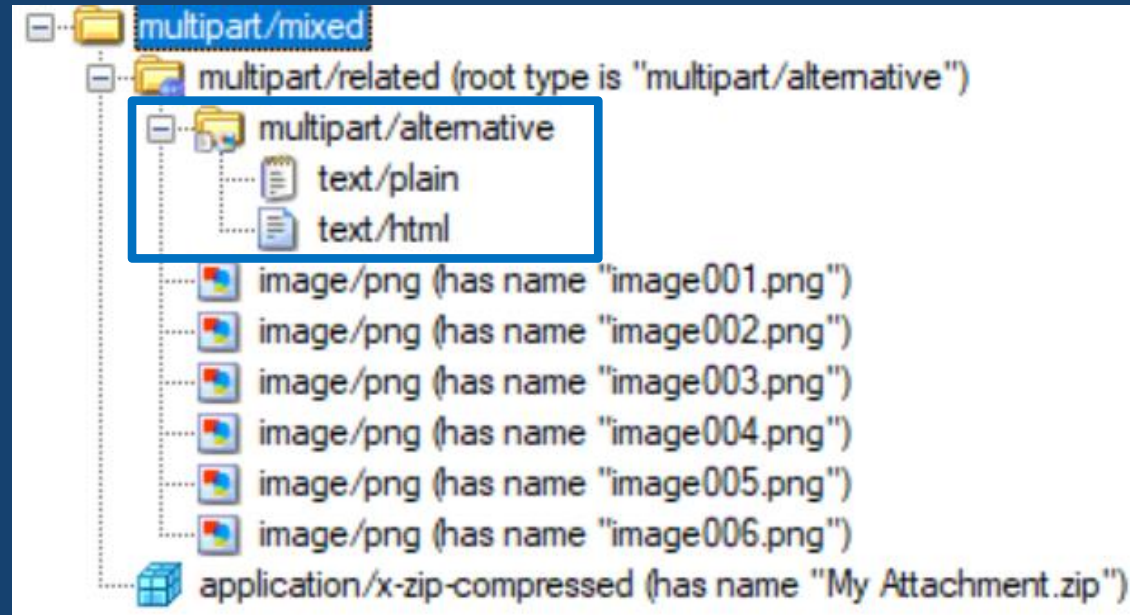
Content-Type: image/jpeg

Content-Disposition: attachment; filename=genome.jpeg;
modification-date="Wed, 12 Feb 1997 16:29:51 -0500";

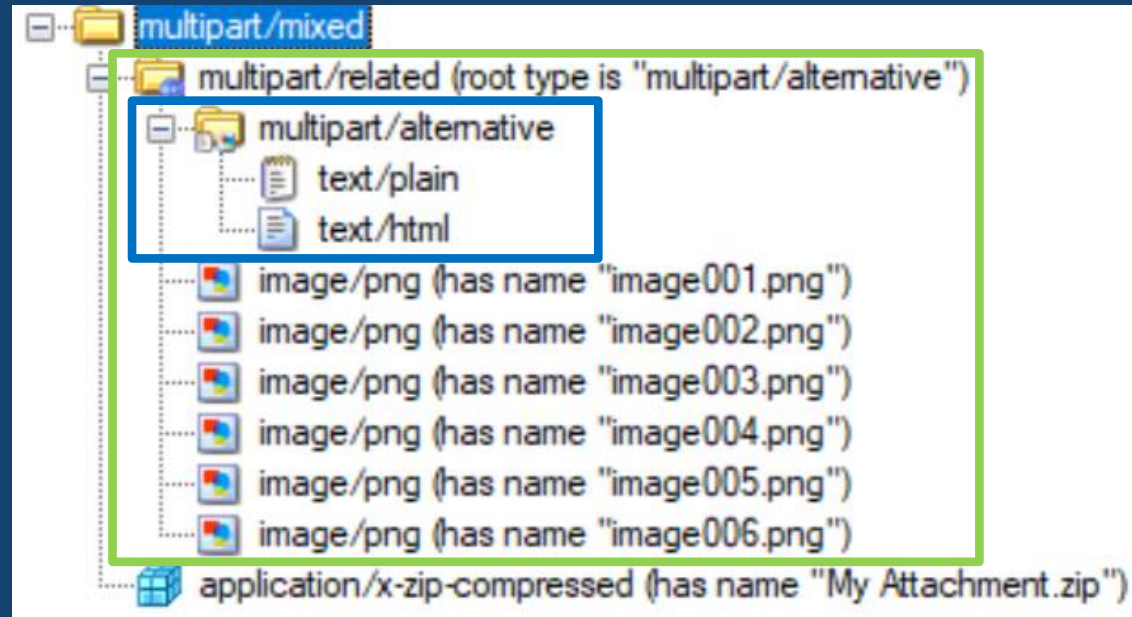
Anatomy of An Email Message



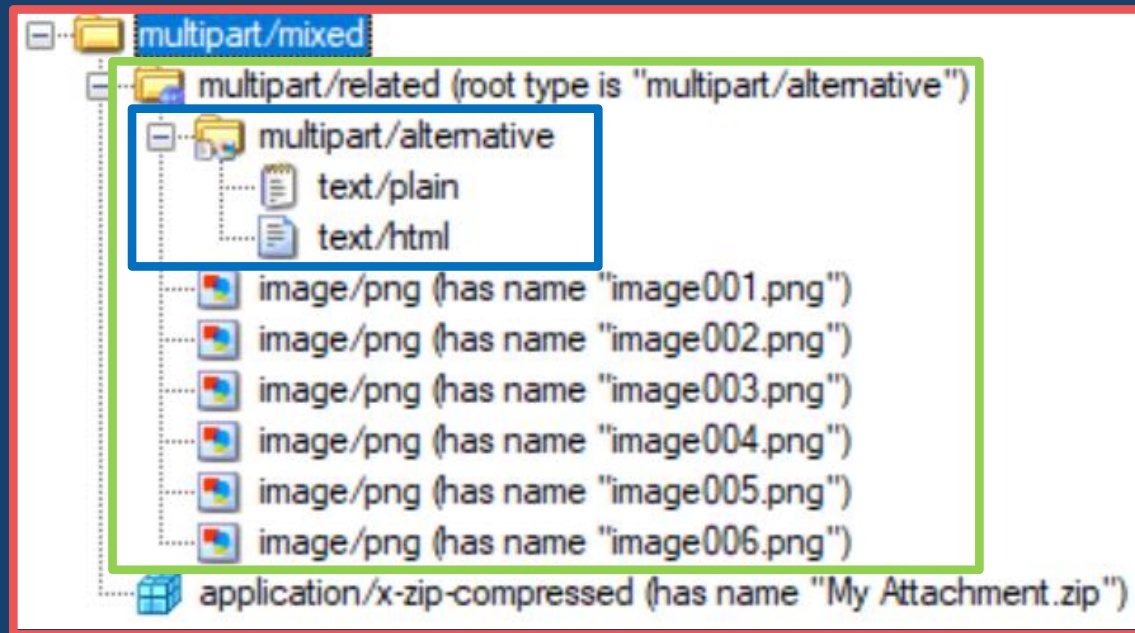
Anatomy of An Email Message



Anatomy of An Email Message



Anatomy of An Email Message



SMTP

- ▶ What is Simple Mail Transfer Protocol?
 - ▶ RFC 5321 — <https://datatracker.ietf.org/doc/html/rfc5321>
- ▶ Inbound vs. outbound
- ▶ Common ports 25, 587, 465, or 2525
- ▶ TCP, NCP, NITS, X.25

Terminology

- ▶ Mail User Agent (MUA)
- ▶ Mail Submission Agent (MSA)
- ▶ Mail Transfer Agent (MTA)
- ▶ Mail Delivery Agent (MDA)

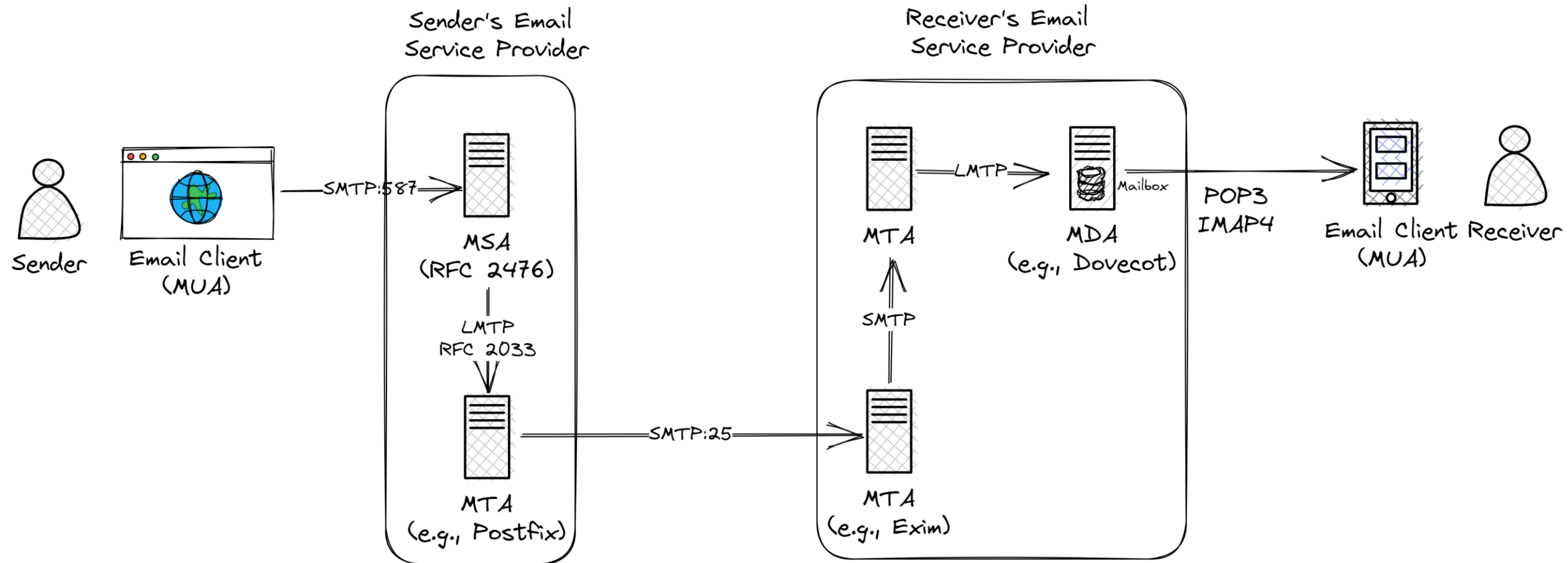
Mail Exchanger Records

- ▶ Current MX lookup
- ▶ Historical MX lookup
- ▶ Using MX history for reconnaissance

Ref [1](#) [2](#)

Simplified Email Flow

Ref [123](#)



SMTP

Let's talk to an SMTP server!

MSA Processing

- ▶ Changes to the message?
- ▶ Yahoo admits mangling e-mail
 - ▶ <http://news.bbc.co.uk/2/hi/science/nature/2138014.stm>
- ▶ Yahoo Mail puts words in your mouth
 - ▶ <https://www.cnet.com/news/yahoo-mail-puts-words-in-your-mouth/>
- ▶ Who else?

EMLX Format

- ▶ Emlx vs Partial Emlx
- ▶ DKIM & ARC verification opportunities
- ▶ Emlx Flags (<https://www.jwz.org/blog/2005/07/emlx-flags/>)

Sources of Email Evidence

- ▶ User devices
 - ▶ Mobile phones
 - ▶ Tablets
 - ▶ Workstations
 - ▶ Laptops
- ▶ On-premises Email Servers
- ▶ Hosted Email Servers
- ▶ Printouts
- ▶ Backups
 - ▶ User device backups
 - ▶ Server backups
 - ▶ Cloud vs. local backups
 - ▶ iTunes
 - ▶ iCloud
 - ▶ Google One
 - ▶ Carbonite, etc.
- ▶ Browser artifacts (webmail)
- ▶ User activity around attachments

Common Email-Related Protocols

- ▶ IMAP
- ▶ POP
- ▶ SMTP
- ▶ HTTP
 - ▶ Graph API — REST
 - ▶ Gmail API — REST
 - ▶ Exchange Web Services (EWS) — SOAP
 - ▶ ...
 - ▶ ...
- ▶ Notes Remote Procedure Calls (NRPC)
- ▶ ...

JSON Example

```
{  
  "id": "172ed79b0337c14f",  
  "threadId": "172ed79b0337c14f",  
  "labelIds": [  
    "UNREAD",  
    "IMPORTANT",  
    "INBOX"  
  ],  
  "historyId": "201239",  
  "sizeEstimate": 4135  
}
```

Outlook to Exchange

- ▶ What protocols does Outlook use to connect to Exchange?

Outlook to Exchange

- ▶ Remote Procedure Call (RPC)
- ▶ RPC over HTTP ([Outlook Anywhere](#))
 - ▶ EOL Oct 31, 2017
- ▶ MAPI over HTTP
 - ▶ Introduced May 2014 (Exchange 2013 SP1 / Outlook 2013 SP1)
- ▶ Exchange Web Services
 - ▶ Calendar sharing, Autodiscover, and access to the global address book
- ▶ Exchange ActiveSync

Ref [1](#) [2](#) [3](#) [4](#)

Common Email-Related Protocols

- ▶ IMAP
- ▶ POP
- ▶ SMTP
- ▶ HTTP
 - ▶ Graph API — REST
 - ▶ Gmail API — REST
 - ▶ Exchange Web Services (EWS) — SOAP
 - ▶ MAPI over HTTP
 - ▶ RPC over HTTP
- ▶ Notes Remote Procedure Calls (NRPC)
- ▶ RPC

Forensic Email Preservation

- ▶ Preservation from local user devices
- ▶ Preservation from servers
 - ▶ Exchange
 - ▶ Full server
 - ▶ Mailboxes
 - ▶ As a client
- ▶ API-based acquisition
- ▶ IMAP / POP

Exchange

- ▶ Recoverable Items Folder
see <https://docs.microsoft.com/en-us/exchange/security-and-compliance/recoverable-items-folder/recoverable-items-folder>
- ▶ In-place Archive
- ▶ Teams data
- ▶ Outlook Customer Manager (OCM)
 - ▶ PersonMetadata
- ▶ Throttling

On-prem Exchange — Export

- ▶ Mailbox Import Export role
- ▶ New-MailboxExportRequest

```
foreach ($Mailbox in (Get-Mailbox)) { New-MailboxExportRequest -Mailbox $Mailbox.Alias -FilePath  
"\\<server FQDN>\<shared folder name>\$($Mailbox.Alias).pst" }
```

- ▶ Event log
- ▶ -IsArchive
- ▶ -BadItemLimit
- ▶ -ExcludeDumpster
- ▶ -ContentFilter

```
New-MailboxExportRequest -Mailbox Tony -ContentFilter "(Body -like '*company*') -and (body -like  
'*profit*') -and (Received -lt '01/01/2018')" -FilePath  
"\\SERVER01\PSTFileShare\Tony_CompanyProfits.pst"
```

see <https://docs.microsoft.com/en-us/powershell/module/exchange/new-mailboxexportrequest>

On-prem Exchange — Throttling

- ▶ Set-ThrottlingPolicy
- ▶ New-ThrottlingPolicy

see <https://docs.microsoft.com/en-us/exchange/change-user-throttling-settings-for-specific-users-exchange-2013-help>

On-prem Exchange Data Store

- ▶ .edb (MAPI-based Database)
- ▶ .stm (Streaming Database)

What Should be Preserved?

- ▶ Item-level unique identifiers
- ▶ Server metadata
- ▶ MIME contents of items
- ▶ Historical backups / journal

Depending on Requirements

- ▶ Related, non-message item types
- ▶ Cloud attachments/revisions

Authentication

- ▶ Modern authentication
- ▶ Delegate access
- ▶ Impersonation
- ▶ Domain-wide delegation of authority
- ▶ Whitelisting Apps in Google Workspace
- ▶ Remote Authentication
- ▶ OAuth token reuse

Ref [1](#)

OAuth 2.0

```
"access_token": "ya29.A0AfH6SMBQAL41aiH7JD1LfnBUfWtn-9-kEqxwrNLRGPvw-  
ERlA4uF7gOL9DfOXnI4tDQQtrVaQpTS8V3SRRbEyDoUQdz7koWhuyi7fLbXUmA7PK0vXqmDEETG88t8M9fsx6QLcEHfiu1JPsmxocuU4o  
ZO91QO"    (~3600 secs)
```

```
"refresh_token": "1//04SVLXWq0TK7HCgYIARAAGAQSNwF-L9IrFaEKgxVU13Ismo9dmDJpjZrI0Uu4-  
n3Yjm1zCLO_pQZdvjgxA9dbp8yjQ6SrQ-F3mto"
```

OAuth 2.0

```
"access_token": "ya29.A0AfH6SMBQAL41aiH7JD1LfnBUfWtn-9-kEqxwrNLRGPvw-  
ERlA4uF7gOL9DfOXnI4tDQQtrVaQpTS8V3SRRbEyDoUQdz7koWhuyi7fLbXUmA7PK0vXqmDEETG88t8M9fsx6QLcEHfiu1JPsmxocuU4o  
ZO91QO"    (~3600 secs)
```

```
"refresh_token": "1//04SVLXWq0TK7HCgYIARAAGAQSNwF-L9IrFaEKgxVU13Ismo9dmDJpjZrI0Uu4-  
n3Yjm1zCLO_pQZdvjgxA9dbp8yjq6SrQ-F3mto"
```

Gmail Example:



What is an ID Token?

- ▶ Used in OpenID Connect
- ▶ Security token
- ▶ Contains Claims about the Authentication of an End-User by an Authorization Server
- ▶ JSON Web Token (JWT)
- ▶ Digitally signed
- ▶ see https://openid.net/specs/openid-connect-core-1_0.html#IDToken

Let's take a look at an example!

Google Takeout, Vault, and OCC

- ▶ When to use Google Vault
 - ▶ Confidential mode
 - ▶ `label:confidentialmode`
- ▶ When to use OCC
 - ▶ Azure RMS
 - ▶ Partially indexed/unindexed files

End-to-end Encryption

- ▶ Client-side encryption (CSE) for Gmail
- ▶ Following features are unavailable:
 - ▶ Confidential mode
 - ▶ Sending to groups as recipients
 - ▶ Searching the message body (users can still search by recipient and subject line)
 - ▶ Signatures
 - ▶ Print
 - ▶ Using Gmail mobile apps

Ref [1](#) [2](#)

Server Metadata

- ▶ Information about the messages
- ▶ Kept on the server
- ▶ Typically not acquired with the messages

IMAP Server Metadata

- ▶ Unique Identifier (UID) Message Attribute
- ▶ Flags Message Attribute
- ▶ Internal Date Message Attribute

Unique Identifier (UID) Message Attribute

- ▶ Unique 32-bit value that identifies a message within a mail folder
- ▶ Assigned in an ascending fashion
- ▶ Not necessarily contiguous
- ▶ Rarely changes
- ▶ Next UID changes when new messages are added to the folder
- ▶ Folder name + UIDVALIDITY + UID refers to a single immutable message on the server forever
- ▶ UIDVALIDITY can represent the creation date of a folder

Ref [1](#)

Internal Date Message Attribute

- ▶ Internal date/time of the message on the server
- ▶ Reflects creation within the mail folder
 - ▶ SMTP — Time of final delivery
 - ▶ IMAP COPY — Timestamp of source message (COPY *should* preserve internal date and flags; sets \Recent flag on the copy)
 - ▶ IMAP APPEND — Timestamp argument or time of APPEND

Ref [1](#)

IMAP Server Metadata

Let's talk to an IMAP server!

Server Metadata

Re: Any News?



Kenny Galloway <kgalloway8791@gmail.com>

To Ernie Daniel

Cc afrench@mdcclxxxix.com



Reply



Reply All



Forward



Tue 1/7/2020 10:32 AM

Great. I'm copying Alessandra as well.

Kenny

On Tue, Jan 7, 2020 at 11:31 AM Ernie Daniel <edaniel@example.com> wrote:

Yes! Let's mark tomorrow as the date of hire for Benny. Thanks.

-Ernie

On Tuesday, January 7, 2020, 11:25:05 AM PDT, Kenny Galloway <kgalloway8791@gmail.com> wrote:

Any news on the new hire?

Kenny

UID	Internal Date
7405	2020-01-05 15:06:37Z
7406	2020-01-06 09:28:44Z
9113	2020-01-07 18:32:32Z
7408	2020-01-08 12:29:24Z
7409	2020-01-09 13:44:57Z

Gmail Server Metadata

- ▶ threadId
- ▶ labelIds
- ▶ historyId
 - ▶ labelAdded
 - ▶ labelRemoved
 - ▶ messageAdded
 - ▶ messageDeleted
- ▶ internalDate — can reflect Date header for API-migrated mail

History Records

Let's acquire Gmail History Records!

PART 2

Forensic Email Authentication

Visual Appearance of the Email

- ▶ Email client that was used
- ▶ Quote strings
- ▶ Formatting of the printout
- ▶ Time zone issues
- ▶ Day of the week issues
- ▶ Company-wide disclaimers and email signatures
- ▶ More...

Download Resource

Download SET 1A data from
<https://sa19.metaspike.com>

Email Appearance — Quote Strings

The web interface of Google's Gmail and G Suite:

On Thu, Apr 23, 2020 at 10:35 AM John Doe <johndoe@example.com> wrote:

Apple Mail on Mac and iPhone:

On Apr 23, 2020, at 10:35 AM, John Doe <johndoe@example.com> wrote:

Yahoo Mail's web interface:

On Thursday, April 23, 2020, 10:35:00 AM PDT, John Doe <johndoe@example.com> wrote:

Plain-text message, Microsoft Outlook 16:

-----Original Message-----

From: John Doe <johndoe@example.com>

Sent: Thursday, April 23, 2020 10:35 AM

To: Jane Doe <janedoe@example.com>

Subject: Test

Suspect Message: Appearance

Five-message thread:

Matt Sheppard ⇌ Perry Mcgrath

Perry Mcgrath ⇌ Matt Sheppard

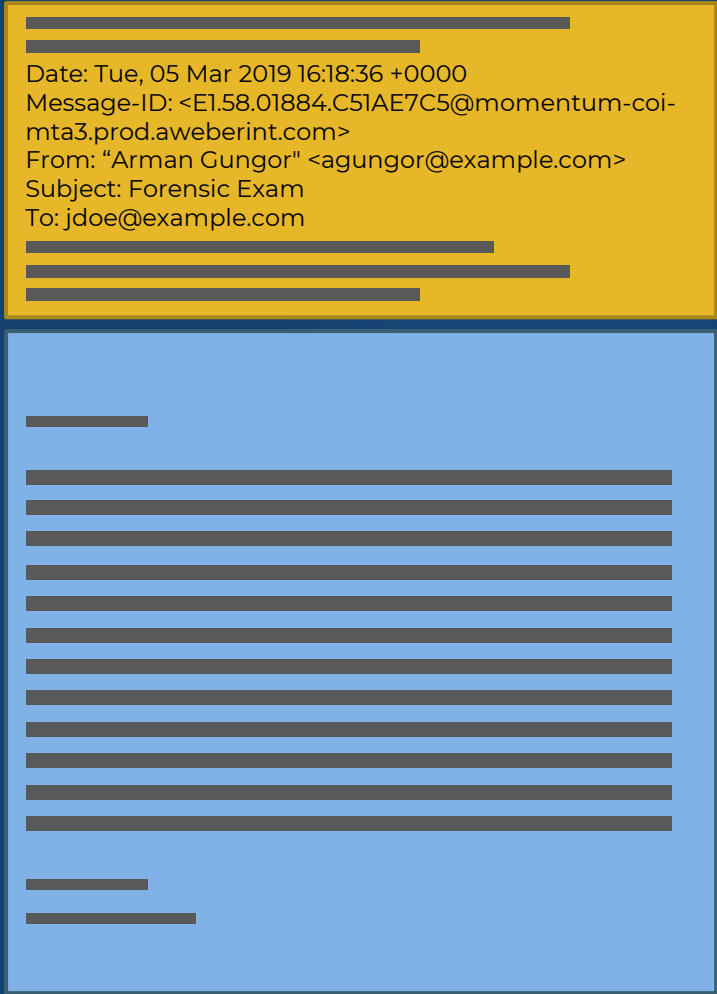
Matt Sheppard ⇌ Perry Mcgrath

Perry Mcgrath ⇌ Matt Sheppard

Matt Sheppard ⇌ Perry Mcgrath

Message Data & Metadata

- ▶ Acquired with the message
 - ▶ Message-ID
 - ▶ In-Reply-To
 - ▶ References
 - ▶ Trace Fields
 - ▶ Content-Length
 - ▶ X-Originating-IP
 - ▶ MIME boundary delimiters
 - ▶ DKIM Signatures
 - ▶ and more...



The diagram illustrates the structure of an email. It consists of two main parts: a yellow header box and a light blue body box. The yellow header box contains the email's metadata, including the date, message ID, from, subject, and to fields. The light blue body box contains the main content of the email, which is represented by several horizontal lines. The entire diagram is set against a dark blue background.

Date: Tue, 05 Mar 2019 16:18:36 +0000
Message-ID: <E1.58.01884.C51AE7C5@momentum-coi-mta3.prod.aweberint.com>
From: "Arman Gungor" <agungor@example.com>
Subject: Forensic Exam
To: jdoe@example.com

Message IDs

► Message-ID Header Field

Message-ID: 0a6f01d5c4cc\$b9145e70\$2b3d1b50\$@gmail.com
01D5C4CC:B9145E70 ⇨ 01/06/2020 08:06:03.479 PM (GMT)

Message-ID: 379739993.5402.1611615098569@mail.yahoo.com
1611615098569 ⇨ Monday, January 25, 2021 10:51:38.569 PM (UTC)

► Service Provider Message IDs

172ed79b0337c14f ⇨ Thursday, June 25, 2020 9:54:34.675 PM (UTC)

Content-IDs

```
<p class=3DMsoNormal><b><i><img width=3D190 height=3D140 =  
id=3D"Picture_x0020_1"  
src=3D"cid:image001.png@01D942C0.F9EE7A50" =  
alt=3Dsig><o:p></o:p></i></b></p>
```

```
-----=_NextPart_002_0003_01D942C0.FE1FC7F0--  
-----=_NextPart_001_0002_01D942C0.FE1FC7F0
```

```
Content-Type: image/png;  
    name="image001.png"
```

```
Content-Transfer-Encoding: base64
```

```
Content-ID: <image001.png@01D942C0.F9EE7A50>
```

```
iVBORw0KGgoAAAANSUhEUgAAAL4AAACMCAAAAADnrUznAAAABGdBTUEAALGOfpTRkwAAAAAwSF1z  
AAAOxAAADsQBlSsOGwAAABl0RVh0U29mdHdhcmUATWljcm9zb2Z0IE9mZmljZX/tNXEAAAHNSURB  
...
```

Content-IDs

```
<p class=3DMsoNormal><b><i><img width=3D190 height=3D140 =  
id=3D"Picture_x0020_1"  
src=3D"cid:image001.png@01D942C0.F9EE7A50" =  
alt=3Dsig><o:p></o:p></i></b></p>
```

```
-----=_NextPart_002_0003_01D942C0.FE1FC7F0--  
-----=_NextPart_001_0002_01D942C0.FE1FC7F0
```

```
Content-Type: image/png;  
    name="image001.png"
```

```
Content-Transfer-Encoding: base64
```

```
Content-ID: <image001.png@01D942C0.F9EE7A50>
```

```
iVBORw0KGgoAAAANSUhEUgAAAL4AAACMCAAAAADnrUznAAAABGdBTUEAALGO  
fPtRkwAAAAAwSFlz  
AAAOxAAADsQBlSsOGwAAABl0RVh0U29mdHdhcmUATWljcm9zb2Z0IE9mZmljZX  
/tNXEAAAHNSURB  
...
```

Content-IDs

```
<p class=3DMsoNormal><b><i><img width=3D190 height=3D140 =  
id=3D"Picture_x0020_1"  
src=3D"cid:image001.png@01D942C0.F9EE7A50" =  
alt=3Dsig><o:p></o:p></i></b></p>
```

```
-----=_NextPart_002_0003_01D942C0.FE1FC7F0--  
-----=_NextPart_001_0002_01D942C0.FE1FC7F0
```

```
Content-Type: image/png;  
    name="image001.png"
```

```
Content-Transfer-Encoding: base64
```

```
Content-ID: <image001.png@01D942C0.F9EE7A50>
```

```
iVBORw0KGgoAAAANSUhEUgAAAL4AAACMCAAAAADnrUznAAAABGdBTUEAALGOfpTRkwAAAAAwSF1z  
AAAOxAAADsQBlSsOGwAAABl0RVh0U29mdHdhcmUATWljcm9zb2Z0IE9mZmljZX/tNXEAAAHNSURB  
...
```

MIME Boundary Delimiters

Gmail API / webmail

00000000000000e54ae05a8c4954b

Yahoo Webmail

-----=_Part_1819530_1525945855.1592937065974

Outlook Desktop

-----=_NextPart_000_0A70_01D5C489.AAF193A0

MIME Boundary Delimiters

Gmail API / webmail

0000000000000000e54ae05a8c4954b

Yahoo Webmail

-----=_Part_1819530_1525945855.1592937065974

Outlook Desktop

-----=_NextPart_000_0A70_01D5C489.AAF193A0

MIME Boundary Delimiters

Unknown

--7A6E80CA6774BE6EE6F2CB14F513FA4750B477E9BD1ABC005DFE8B4E54F93640

MIME Boundary Delimiters

- ▶ Who creates MIME boundary delimiters?
- ▶ Can they be updated?

MIME Boundary Delimiters

Example scenarios where delimiters are updated:

- ▶ Email is modified → saved
- ▶ Email is moved between IMAP folders via Outlook 2013 or later (see [Outlook bug report](#))
- ▶ Email is forwarded as an attached MIME message

MIME Boundary Delimiters

Example scenarios where delimiters are updated:

- ▶ Email is modified → saved
- ▶ Email is moved between IMAP folders via Outlook 2013 or later (see [Outlook bug report](#))
- ▶ Email is forwarded as an attached MIME message

Are Message-IDs updated the same way?

Effects of Outlook Modifications

Let's review:

- ▶ Changes to a message edited by Outlook
- ▶ Changes to a message copied/moved by Outlook 2013+ between IMAP folders
- ▶ Changes to a forwarded message

Download Resource

Download SET 1B data from
<https://sa19.metaspike.com>

Quoted-printable Transfer Encoding Refresher

- ▶ RFC 2045 – 6.7
- ▶ Requires that encoded lines be no more than 76 characters long.
- ▶ If longer, “soft” line breaks must be used, indicated by an equal sign as the last character on an encoded line.

Ref [1](#)

What is DKIM?

- ▶ DomainKeys Identified Mail (DKIM)
- ▶ [RFC 6376](#)
- ▶ Uses public key cryptography
- ▶ Provides assurance on the identity of the sender of a message
- ▶ Relationship to Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting & Conformance (DMARC)

Sender Policy Framework

- ▶ [RFC 7208](#)
- ▶ DNS-based email authentication
- ▶ Aims to prevent sender address forgery by checking the envelope sender's IP address against the claimed sending domain
- ▶ 10-lookup limit
- ▶ Checks **HELO** identity and **MAIL FROM** identity (SMTP)
- ▶ Header sender vs. envelope sender alignment

SPF Results

- ▶ **None**: No valid domain name, or no SPF records found.
- ▶ **Neutral**: Explicit statement that whether the IP address is authorized is not asserted.
- ▶ **Pass**: Explicit statement that the client is authorized to send mail with the given identity.
- ▶ **Fail**: Explicit statement that the client is not authorized to send mail with the given identity.

```
v=spf1 ip4:47.181.19.3 -all
```

- ▶ **Softfail**: Weak statement that the client is probably not authorized. (*Mail can be allowed, but should be flagged as spam or suspicious*)

```
v=spf1 include:spf.protection.outlook.com ~all
```

- ▶ **Temperror**: SPF verifier encountered a transient (e.g., DNS) error while performing the check.
- ▶ **Permerror**: The domain's published records could not be correctly interpreted.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

- ▶ Combines SPF and DKIM into a single coherent policy
- ▶ Provides feedback to senders via reporting
 - ▶ Aggregate reports
 - ▶ Forensic reports
- ▶ Senders tell receivers what to do when a message fails authentication
- ▶ Notable contributors include PayPal, Bank of America, Fidelity Investments, JPMorganChase, LinkedIn, Facebook, and Twitter

Sender composes & sends email

Sending mail server inserts DKIM Header

Recipient's mail server receives email

Standard validation tests are run
(rate limit, reputation checks, block lists, etc.)

DKIM and SPF verified. Sender's DMARC policy
is applied

Standard Processing
Anti-spam, antivirus, etc.

Pass

Quarantine

Reject

Aggregate report to Sender updated

Failure report
sent to Sender

How DKIM Works

- ▶ Signing entity normalizes & hashes the body of the message and digitally signs it along with a subset of its header fields using its private key
- ▶ Public key of the signing entity is published as a _domainkey DNS TXT Resource Record for the signer's domain
- ▶ Recipient retrieves the signer's public key with a DNS query and attempts to verify the digital signature

Original Message

Delivered-To: lmisf01@gmail.com
Received: by 2002:a5d:6487:0:0:0:0 with SMTP id o7csp2293978wri;
Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJyWhaMfNbRsrQe35V/ZMXtub5vbdIE2jqxMYgOSdLcJJcYq2T0nY07gAYZujzkv0zH7nRF
X-Received: by 2002:a37:6c42:: with SMTP id h63mr1170343qkc.243.1634923777253;
Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1634923777; cv=none;
d=google.com; s=arc-20160816;
b=bxtn2LvysX8jAuR9slchGhca00nvsD7Wt27ADiTSV08RD141L4wOGsWn4YGTI+vNSM
KXrh8mIwyQDpHir2X9tvyiBrf0VgzghQgwaKjWcGo8MmeQcuFHVX5jon20iH4pX0s1lT
Dwn7tEKqr/vp7dQC1Id/ul0Tixi21jD1yXzR2P86QV2t2cFdd+mH1pjLY4eJIqxKo86
073Sg5RNK8KPeKGrB16xj3U6QA5f8A+z/zzq4Vs5TuKm0blASQsClvbajX7LLrB+n3f
xKvkWfJrzfpitG218QSKCXqNGx+qp2des9+oV0sCTGpWln6Z75JL+4ZrJkZwCVHC3KW
6Y7A==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=references:mime-version:subject:message-id:to:from:date
:dkim-signature;
bh=qm8gQM068LjBKcDOJlgtE6bbnQdUepEnLvq3Q8/2NrY=;
b=tVQiE9PZGt18qpRuyzys0MQBinhOyog19rFNpNqBPwnf00+FPzhc3gMLjGxHUC46W
S1BWqm6WN+GKyJlDNSJQJTAMt3z1C+532IccOT5gjeaFs7DL/GwkXGyaMQL5LxI2Ih0
KJDONU2HGWrEoQ8/fPkH2Qt5S1p/AEeX83gZpVNQYxgNgJ90p1+K4ZZVPixC5pAiOtUM
gK7BiigXNYs+9PnaBt8ja63RpKUj0cJ6LPxxVS13nR9C3YI+3M3Qk6TB1i02p9izmiKe
At5sNz8E3sdpRVfXSNqh3eAauLwyQf9mW45N/xd32wFwyg5ncz2H9IhSHUTUNH19Qzg5
Oebg==
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@yahoo.com header.s=s2048 header.b=kGDAPJSu;
spf=pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
smtp.mailfrom=fecdev@yahoo.com;
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
Return-Path: <fecdev@yahoo.com>
Received: from sonic306-21.consmr.mail.ne1.yahoo.com (sonic306-21.consmr.mail.ne1.yahoo.com.
[66.163.189.83])
by mx.google.com with ESMTPS id bp13si8762888qkb.34.2021.10.22.10.29.36
for <lmisf01@gmail.com>
(version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
Received-SPF: pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
client-ip=66.163.189.83;
Authentication-Results: mx.google.com;
dkim=pass header.i=@yahoo.com header.s=s2048 header.b=kGDAPJSu;
spf=pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
smtp.mailfrom=fecdev@yahoo.com;
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKcDOJlgtE6bbnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To;
b=kGDAPJSuIZNdM/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvwYBTRFFwBPd5BveOVxBE99yiX0gR19ZsbaeYazJP
q55yZ2GDacT7/q+g0a6EDS0bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkwg6ZhB8HEpYku+21zKbS8VsL50H/a7rKbbC2YL/VFwyN73F
7QVhpPfd/cpOTT13co0wgGcWootEFOXVrwuQtxQePpa8CKZX53JFAYv1rUYWd8BkmifbR8c1WnmOv4ho1nL5003w+gXKGwom6Qh0o
GeF8KxNM31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==
Received: from sonic.gate.mail.ne1.yahoo.com by sonic306.consmr.mail.ne1.yahoo.com with HTTP; Fri, 22
Oct 2021 17:29:35 +0000
Date: Fri, 22 Oct 2021 17:28:56 +0000 (UTC)
From: FEC Dev <fecdev@yahoo.com>
To: "lmisf01@gmail.com" <lmisf01@gmail.com>
Message-ID: <217157422.687119.1634923736910@mail.yahoo.com>
Subject: DKIM Verification Exercise
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="-----_Part_687118_578898387.1634923736909"
References: <217157422.687119.1634923736910.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.19198 YMailNorrrin
Content-Length: 688

-----_Part_687118_578898387.1634923736909
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

This is where the message body goes!

-----_Part_687118_578898387.1634923736909
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit

<html><head></head><body><div class="yahoo-style-wrap" style="font-family:Helvetica Neue, Helvetica,
Arial, sans-serif;font-size:16px;"><div dir="ltr" data-setdir="false">This is where the message body
goes!</div><div dir="ltr" data-setdir="false">
</div><div dir="ltr" data-
setdir="false">
</div><div dir="ltr" data-setdir="false">
</div></div></body></html>
-----_Part_687118_578898387.1634923736909--

Original Message

Delivered-To: lmisf01@gmail.com
Received: by 2002:a5d:6487:0:0:0:0 with SMTP id o7csp2293978wri;
Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJyWhaMfNbRsrQe35V/ZMXtub5vbDiE2jqxMYgOSdLcJJcYq2T0nY07gAYZujzkv0zH7nRF
X-Received: by 2002:a37:6c42:: with SMTP id h63mr1170343qkc.243.1634923777253;
Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1634923777; cv=none;
d=google.com; s=arc-20160816;
b=bxtn2LvysX8jAuR9slchGhca00nvsD7Wt27ADiTSV08RD141L4wOGsWn4YGTI+vNSM
KXrh8mIwyQDpHir2X9tvyiBrf0VgzghQgwaKjWcGo8MmeQcuFHVX5jon20iH4pX0s11T
Dwn7tEKqr/vp7dQC1Id/ulOTixi21jD1yXzR2P86QV2t2cFdd+mH1pjlY4eJIqxKo86
073Sg5RNK8KPeKGrB16xj3U6QA5f8A+z/zzq4Vs5TuKmOb1ASQsC1vbajX7LLrB+n3f
xKvkWfJrzfpitG218QSKCXqNGx+qp2des9+oV0sCTGpWln6Z75JL+4ZrJkZwCVHC3KW
6Y7A==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=references:mime-version:subject:message-id:to:from:date
:dkim-signature;
bh=qm8gQM068LjBKcDOJlgtE6bbnQdUepEnLvq3Q8/2NrY=;
b=tVQie9PZGt18qpRuyzys0MQBinhOyog19rFNpNqBPwnf00+FPzhc3gMLjGxHUC46W
S1BWqm6WN+GKyJ1dDNSJQJTAMt3z1C+532IccOT5gjeaFs7DL/GwkXGyaMQ15LxI2Ih0
KJDONU2HGWrEoQ8/fPkH2Qt5S1p/AEeX83gZpVNQYxgNgJ90p1+K4ZZVPixC5pAiOtUM
gK7BiigXNYs+9PnaBt8ja63RpKUj0cJ6LPxxVS13nR9C3YI+3M3Qk6TB1i02p9izmiKe
At5sNz8E3sdpRVfXSNqh3eAauLwyQf9mW45N/xd32wFwyg5ncz2H9IhSHUTUNH19Qzg5
Oebg==
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@yahoo.com header.s=s2048 header.b=kGDAPJSu;
spf=pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
smtp.mailfrom=fecdev@yahoo.com;
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
Return-Path: <fecdev@yahoo.com>
Received: from sonic306-21.consmr.mail.ne1.yahoo.com (sonic306-21.consmr.mail.ne1.yahoo.com.
[66.163.189.83])
by mx.google.com with ESMTPS id bp13si8762888qkb.34.2021.10.22.10.29.36
for <lmisf01@gmail.com>
(version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
Received-SPF: pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
client-ip=66.163.189.83;
Authentication-Results: mx.google.com;
dkim=pass header.i=@yahoo.com header.s=s2048 header.b=kGDAPJSu;
spf=pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
smtp.mailfrom=fecdev@yahoo.com;
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKcDOJlgtE6bbnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To;
b=kGDAPJSuIZNdM/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvwYBTRFFwBPd5BveOVxBE99yiX0gR19ZsbaeYazJP
q55yZ2GDacT7/q+g0a6EDS0bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkwg6ZhB8HEpYku+21zKbS8VsL50H/a7rKbbC2YL/VFwyN73F
7QVhpPfD/cpOTT13co0wgGcWootEFOXVrwuQtxQePpa8CKZX53JFAYv1rUYWd8BkmiFbR8c1WnmOv4ho1nL5003w+gXKGwom6QhOo
GeF8KxNM31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==
Received: from sonic.gate.mail.ne1.yahoo.com by sonic306.consmr.mail.ne1.yahoo.com with HTTP; Fri, 22
Oct 2021 17:29:35 +0000
Date: Fri, 22 Oct 2021 17:28:56 +0000 (UTC)
From: FEC Dev <fecdev@yahoo.com>
To: "lmisf01@gmail.com" <lmisf01@gmail.com>
Message-ID: <217157422.687119.1634923736910@mail.yahoo.com>
Subject: DKIM Verification Exercise
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="-----_Part_687118_578898387.1634923736909"
References: <217157422.687119.1634923736910.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.19198 YMailNorrrin
Content-Length: 688

-----_Part_687118_578898387.1634923736909
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

This is where the message body goes!

-----_Part_687118_578898387.1634923736909
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit

<html><head></head><body><div class="yahoo-style-wrap" style="font-family:Helvetica Neue, Helvetica,
Arial, sans-serif;font-size:16px;"><div dir="ltr" data-setdir="false">This is where the message body
goes!</div><div dir="ltr" data-setdir="false">
</div><div dir="ltr" data-
setdir="false">
</div><div dir="ltr" data-setdir="false">
</div></div></body></html>
-----_Part_687118_578898387.1634923736909--

DKIM Signature

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
d=yahoo.com; s=s2048; t=1634923775;  
bh=qm8gQM068LjBKcD0Jlgte6bbnQdUepEnLvq3Q8/2NrY=;  
h=Date:From:To:Subject:References:From:Subject:Reply-To;  
b=kGDApJSuIZNdm/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvw  
YBTRfFWbPD5Bve0VxBE99yiX0gR19ZsbaeYazJPq55yZ2GDacT7/q+g0a6EDSO  
bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkkg6ZhB8HEpYku+21zKbS8VsL50H/a7r  
KbbC2YL/VFwyN73F7QVhpPfd/cp0TT13co0wgGcWootEF0XVrwuQtxQePpa8CK  
ZX53JFAYv1rUYWd8Bkmi fbR8c1Wnm0v4ho1nL5003w+gXKgWom6Qh0oGeF8KxN  
M31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==
```

DKIM Signature

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKcD0Jlgte6bbnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To;
b=kGDApJSuIZNdm/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvw
YBTRfFWbPD5Bve0VxBE99yiX0gR19ZsbaeYazJPq55yZ2GDacT7/q+g0a6EDSO
bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkkg6ZhB8HEpYku+21zKbS8VsL50H/a7r
KbbC2YL/VFwyN73F7QVhpPfd/cp0TT13co0wgGcWootEFOXVrwuQtxQePpa8CK
ZX53JFAYv1rUYWd8Bkmi fbR8c1Wnm0v4ho1nL5003w+gXKgWom6Qh0oGeF8KxN
M31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==

DKIM Signature

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKcD0Jlgte6bbnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To;
b=kGDApJSuIZNdm/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvw
YBTRfFWbPD5Bve0VxBE99yiX0gR19ZsbaeYazJPq55yZ2GDact7/q+g0a6EDSO
bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkkg6ZhB8HEpYku+21zKbS8VsL50H/a7r
KbbC2YL/VFwyN73F7QVhpPfd/cp0TT13co0wgGcWootEF0XVrwuQtxQePpa8CK
ZX53JFAYv1rUYWd8Bkmi fbR8c1Wnm0v4ho1nL5003w+gXKgWom6Qh0oGeF8KxN
M31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==

DKIM Signature

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
d=yahoo.com; s=s2048; t=1634923775;  
bh=qm8gQM068LjBKcD0Jlgte6bbnQdUepEnLvq3Q8/2NrY=;  
h=Date:From:To:Subject:References:From:Subject:Reply-To;  
b=kGDApJSuIZNdm/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvw  
YBTRfFWbPD5Bve0VxBE99yiX0gR19ZsbaeYazJPq55yZ2GDacT7/q+g0a6EDSO  
bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkkg6ZhB8HEpYku+21zKbS8VsL50H/a7r  
KbbC2YL/VFwyN73F7QVhpPfd/cp0TT13co0wgGcWootEFOXVrwuQtxQePpa8CK  
ZX53JFAYv1rUYWd8Bkmi fbR8c1Wnm0v4ho1nL5003w+gXKgWom6Qh0oGeF8KxN  
M31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==
```

DKIM Signature

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
d=yahoo.com; s=s2048; t=1634923775;  
bh=qm8gQM068LjBKcD0Jlgte6bbnQdUepEnLvq3Q8/2NrY=;  
h=Date:From:To:Subject:References:From:Subject:Reply-To;  
b=kGDApJSuIZNdm/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvw  
YBTRfFWbPD5Bve0VxBE99yiX0gR19ZsbaeYazJPq55yZ2GDacT7/q+g0a6EDSO  
bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkkg6ZhB8HEpYku+21zKbS8VsL50H/a7r  
KbbC2YL/VFwyN73F7QVhpPfd/cp0TT13co0wgGcWootEFOXVrwuQtxQePpa8CK  
ZX53JFAYv1rUYWd8Bkmi fbR8c1Wnm0v4ho1nL5003w+gXKgWom6Qh0oGeF8KxN  
M31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==
```

DKIM Signature

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKcD0Jlgte6bbnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To;
b=kGDApJSuIZNdm/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvw
YBTRfFWbPD5Bve0VxBE99yiX0gR19ZsbaeYazJPq55yZ2GDacT7/q+g0a6EDSO
bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkkg6ZhB8HEpYku+21zKbS8VsL50H/a7r
KbbC2YL/VFwyN73F7QVhpPfd/cp0TT13co0wgGcWootEFOXVrwuQtxQePpa8CK
ZX53JFAYv1rUYWd8Bkmi fbR8c1Wnm0v4ho1nL5003w+gXKgWom6Qh0oGeF8KxN
M31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==

DKIM Signature

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKcD0Jlgte6bbnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To;
b=kGDApJSuIZNdm/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvw
YBTRfFWbPD5Bve0VxBE99yiX0gR19ZsbaeYazJPq55yZ2GDacT7/q+g0a6EDSO
bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkkg6ZhB8HEpYku+21zKbS8VsL50H/a7r
KbbC2YL/VFwyN73F7QVhpPfd/cp0TT13co0wgGcWootEFOXVrwuQtxQePpa8CK
ZX53JFAYv1rUYWd8Bkmi fbR8c1Wnm0v4ho1nL5003w+gXKgWom6Qh0oGeF8KxN
M31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==

DKIM Signature

Friday, October 22,
2021 5:29:35 PM (UTC)

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKcD0Jlgte6bbnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To;
b=kGDApJSuIZNdm/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvw
YBTRfFWbPD5Bve0VxBE99yiX0gR19ZsbaeYazJPq55yZ2GDacT7/q+g0a6EDSO
bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkkg6ZhB8HEpYku+21zKbS8VsL50H/a7r
KbbC2YL/VFwyN73F7QVhpPfd/cp0TT13co0wgGcWootEFOXVrwuQtxQePpa8CK
ZX53JFAYv1rUYWd8Bkmi fbR8c1Wnm0v4ho1nL5003w+gXKgWom6Qh0oGeF8KxN
M31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==

DKIM Signature

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKcD0Jlgte6bbnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To;
b=kGDApJSuIZNdm/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvw
YBTRfFWbPD5Bve0VxBE99yiX0gR19ZsbaeYazJPq55yZ2GDact7/q+g0a6EDSO
bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkkg6ZhB8HEpYku+21zKbS8VsL50H/a7r
KbbC2YL/VFwyN73F7QVhpPfd/cp0TT13co0wgGcWootEFOXVrwuQtxQePpa8CK
ZX53JFAYv1rUYWd8Bkmi fbR8c1Wnm0v4ho1nL5003w+gXKgWom6Qh0oGeF8KxN
M31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==

DKIM Signature

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKcD0Jlgte6bbnQdUepEnLvq3Q8/2NrY=;
h=**Date:From:To:Subject:References:From:Subject:Reply-To;**
b=kGDApJSuIZNdm/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvw
YBTRfFWbPD5Bve0VxBE99yiX0gR19ZsbaeYazJPq55yZ2GDacT7/q+g0a6EDSO
bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkkg6ZhB8HEpYku+21zKbS8VsL50H/a7r
KbbC2YL/VFwyN73F7QVhpPfd/cp0TT13co0wgGcWootEF0XVrwuQtxQePpa8CK
ZX53JFAYv1rUYWd8Bkmi fbR8c1Wnm0v4ho1nL5003w+gXKgWom6Qh0oGeF8KxN
M31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==

DKIM Signature

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
d=yahoo.com; s=s2048; t=1634923775;  
bh=qm8gQM068LjBKcD0Jlgte6bbnQdUepEnLvq3Q8/2NrY=;  
h=Date:From:To:Subject:References:From:Subject:Reply-To;  
b=kGDApJSuIZNdm/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvw  
YBTRfFWbPD5Bve0VxBE99yiX0gR19ZsbaeYazJPq55yZ2GDacT7/q+g0a6EDSO  
bpFajxDQglko9XH/yeG3ZPSYnoc5CRkWG6ZhB8HEpYku+21zKbS8VsL50H/a7r  
KbbC2YL/VFwyN73F7QVhpPfd/cp0TT13co0wgGcWootEF0XVrwuQtxQePpa8CK  
ZX53JFAYv1rUYWd8Bkmi fbR8c1Wnm0v4ho1nL5003w+gXKgWom6Qh0oGeF8KxN  
M31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==
```

DKIM Signature

Signature

```
kGDApJSuIZNdm/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvwYB
TRfFWbPD5Bve0VxBE99yiX0gR19ZsbaeYazJPq55yZ2GDacT7/q+g0a6EDS0bp
FajxDQglko9XH/yeG3ZPSYnoc5CRkWG6ZhB8HEpYku+21zKbS8VsL50H/a7rKb
bC2YL/VFwyN73F7QVhpPfd/cp0TT13co0wgGcWootEF0XVrwuQtxQePpa8CKZX
53JFAYv1rUYWd8BkmifbR8c1Wnm0v4ho1nL5003w+gXKgWom6Qh0oGeF8KxNM3
1j51JnpH3gJZxFou5nLGF8p0fX6syoKg==
```

DKIM Verification

Simple Canonicalization

Header: Presents the header fields exactly as they are without changing their case, altering whitespace, etc.

Body: Removes any extra empty lines at the end of the message body.

DKIM Verification

Relaxed Canonicalization

Header:

- ▶ Converts all header field names to lowercase (e.g., "Subject:" -> "subject:")
- ▶ Unfolds all lines
- ▶ Converts all sequences of one or more whitespace characters to a single space
- ▶ Removes all whitespace at the end of each header field value
- ▶ Removes any whitespace before and after the colon that separates the header field name from the value (e.g., "subject : test" -> "subject:test")

Body:

- ▶ Removes all whitespace at line endings
- ▶ Replaces all whitespace within a line with a single space
- ▶ Extra empty lines at the end of the message body are also removed

DKIM Verification

Step 1 — Calculate Body Hash

Original Message

Delivered-To: lmisf01@gmail.com
Received: by 2002:a5d:6487:0:0:0:0 with SMTP id o7csp2293978wri;
Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJyWhaMfNbRsrQe35V/ZMXtub5vbDiE2jqxMYgOSdLcJJcYq2T0nY07gAYZujzkv0zH7nRF
X-Received: by 2002:a37:6c42:: with SMTP id h63mr1170343qkc.243.1634923777253;
Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1634923777; cv=none;
d=google.com; s=arc-20160816;
b=bxtn2LvysX8jAuR9slchGhca00nvsD7Wt27ADiTSV08RD141L4wOGsWn4YGTI+vNSM
KXrh8mIwyQDpHir2X9tvyiBrf0VgzghQgwaKjWcGo8MmeQcuFHVX5jon20iH4pX0s1lT
Dwn7tEKqr/vp7dQC1Id/ulOTixi21jD1yXzR2P86QV2t2cFdd+mH1pjlY4eJlqxKo86
073Sg5RNK8KPeKGrB16xj3U6QA5f8A+z/zzq4Vs5TuKm0blASQsClvbajX7LLrB+n3f
xKvkWfJrzfpitG2L8QSKCXqNGx+qp2des9+oV0sCTGpWln6Z75JL+4ZrJkZwCVHC3KW
6Y7A==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=references:mime-version:subject:message-id:to:from:date
:dkim-signature;
bh=qm8gQM068LjBKcDOJlgtE6bbnQdUepEnLvq3Q8/2NrY=;
b=tVQie9PZGt18qpRuyzys0MQBInhOyog19rFNpNqBPwnf00+FPzhc3gMLjGxHUC46W
S1BWqm6WN+GKyJlDNSJQJTAMt3z1C+532IccOT5gjeaFs7DL/GwkXGyaMQL5LxI2Ih0
KJDONU2HGWrEoQ8/FPkH2Qt5S1p/AEeX83gZpVNQYxgNgJ90p1+K4ZzVPixC5pAiOtUM
gK7BiigXNYs+9PnaBt8ja63RpKUj0cJ6LPxxVS13nR9C3YI+3M3Qk6TB1i02p9izmiKe
At5sNz8E3sdpRVfXSNqh3eAauLwyQf9mW45N/xd32wFwyg5ncz2H9IhSHUTUNH19Qzg5
Oebg==
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@yahoo.com header.s=s2048 header.b=kGDAPJSu;
spf=pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
smtp.mailfrom=fecdev@yahoo.com;
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
Return-Path: <fecdev@yahoo.com>
Received: from sonic306-21.consmr.mail.ne1.yahoo.com (sonic306-21.consmr.mail.ne1.yahoo.com.
[66.163.189.83])
by mx.google.com with ESMTPS id bp13si8762888qkb.34.2021.10.22.10.29.36
for <lmisf01@gmail.com>
(version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
Received-SPF: pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
client-ip=66.163.189.83;
Authentication-Results: mx.google.com;
dkim=pass header.i=@yahoo.com header.s=s2048 header.b=kGDAPJSu;
spf=pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
smtp.mailfrom=fecdev@yahoo.com;
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKcDOJlgtE6bbnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To;
b=kGDAPJSuIZNdM/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvwYBTRFFwBPd5BveOVxBE99yiX0gR19ZsbaeYazJP
q55yZ2GDacT7/q+g0a6EDS0bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkwg6ZhB8HEpYku+21zKbS8VsL50H/a7rKbbC2YL/VFwyN73F
7QVhpPfd/cpOTT13co0wgGcWootEFOXVrwuQtxQePpa8CKZX53JFAYv1rUYWd8BkmifbR8c1WnmOv4ho1nL5003w+gXKGwom6QhOo
GeF8KxNM31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==
Received: from sonic.gate.mail.ne1.yahoo.com by sonic306.consmr.mail.ne1.yahoo.com with HTTP; Fri, 22
Oct 2021 17:29:35 +0000
Date: Fri, 22 Oct 2021 17:28:56 +0000 (UTC)
From: FEC Dev <fecdev@yahoo.com>
To: "lmisf01@gmail.com" <lmisf01@gmail.com>
Message-ID: <217157422.687119.1634923736910@mail.yahoo.com>
Subject: DKIM Verification Exercise
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="-----_Part_687118_578898387.1634923736909"
References: <217157422.687119.1634923736910.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.19198 YMailNorrrin
Content-Length: 688

-----_Part_687118_578898387.1634923736909
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

This is where the message body goes!

-----_Part_687118_578898387.1634923736909
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit

```
<html><head></head><body><div class="yahoo-style-wrap" style="font-family:Helvetica Neue, Helvetica,
Arial, sans-serif;font-size:16px;"><div dir="ltr" data-setdir="false">This is where the message body
goes!</div><div dir="ltr" data-setdir="false"><br></div><div dir="ltr" data-
setdir="false"><br></div><div dir="ltr" data-setdir="false"><br></div></div></body></html>
-----_Part_687118_578898387.1634923736909--
```


DKIM Verification

Step 1 — Calculate Body Hash

Hex: AA-6F-20-40-CD-3A-F0-B8-C1-29-C0-CE-26-58-2D-7B-A6-DB-9D-07-54-7A-91-27-2E-FA-B7-43-CF-F6-36-B6

Base64: qm8gQM068LjBKcDOJlgte6bbnQdUepEnLvq3Q8/2NrY=

DKIM Signature

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKcD0Jlgte6bbnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To;
b=kGDApJSuIZNdm/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvw
YBTRfFWbPD5Bve0VxBE99yiX0gR19ZsbaeYazJPq55yZ2GDact7/q+g0a6EDSO
bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkWG6ZhB8HEpYku+21zKbS8VsL50H/a7r
KbbC2YL/VFwyN73F7QVhpPfd/cp0TT13co0wgGcWootEF0XVrwuQtxQePpa8CK
ZX53JFAYv1rUYWd8Bkmi fbR8c1Wnm0v4ho1nL5003w+gXKgWom6Qh0oGeF8KxN
M31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==

DKIM Verification

Step 2 — Retrieve Public Key

DNS lookup for TXT record:

s2048._domainkey.yahoo.com

Result:

TTL: 5 hours 42 minutes 57 seconds

VALUE: k=rsa;

p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuoWufgbWw58MczUGbMv176RaxdZGOMkQmn800J/HGoQ6da1SMWiLaj8IMcHC1cubJx2gz,iAPQHVPtFYayyLA4ayJUSNk10/uqfByiU8qiPCE4JSFrpxflhMIKV4bt+g1uHw7wLzguCf4Y AoR6XxUKRsAoHuoF7M+v6bMZ/X1G+viWHkBl4UfgJQ608F1ckKKoZ5K,qUkJH5pDaqbgs+F3PpyiAUQfB6EEzOA1KMPRWJGpzgPtKoukDcQuKUw9GAul7kSIyEcizqrbaUKNLGAmz0elkqRnzIsVpz6jdT1/YV5Ri6YUOQ5sN5bqNzZ8TxoQ1kb,VRy6eK0jUnoSSmSAhwIDAQAB;

DKIM Verification

Step 2 — Retrieve Public Key

Public Key

```
-----BEGIN PUBLIC KEY-----
```

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuoWufgbWw58MczUGbMv176RaxdZGOMkQmn800  
J/HGoQ6daISMWiLaj8IMcHC1cubJx2gziAPQHVPtFYayyLA4ayJUSNk10/uqfByiU8qiPCE4JSFrpxflh  
MIKV4bt+g1uHw7wLzguCf4YAO6XxUKRsAoHuoF7M+v6bMZ/X1G+viWHkB14UfgJQ608F1ckKKoZ5KqUk  
JH5pDaqbgS+F3PpyiAUQfB6EEzOA1KMPRWJGpzgPtKoukDcQuKUw9GAu17kSIyEcizqrbaUKNLGAmz0e1  
kqRnzIsVpz6jdT1/YV5Ri6YUOQ5sN5bqNzZ8TxoQ1kbVRy6eK0jUnoSSTmSAhwIDAQAB
```

```
-----END PUBLIC KEY-----
```

DKIM Verification

Step 3 — Construct Signed Message

Original Message

Delivered-To: lmisf01@gmail.com
Received: by 2002:a5d:6487:0:0:0:0 with SMTP id o7csp2293978wri;
Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJyWhaMfNbRsrQe35V/ZMXtub5vbDiE2jqxMYgOSdLcJJcYq2T0nY07gAYZujzkv0zH7nRF
X-Received: by 2002:a37:6c42:: with SMTP id h63mr1170343qkc.243.1634923777253;
Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1634923777; cv=none;
d=google.com; s=arc-20160816;
b=bxtn2LvysX8jAuR9slchGhca00nvsD7Wt27ADiTSV08RD141L4wOGsWn4YGTI+vNSM
KXrh8mIwyQDpHir2X9tvyiBrf0VgzghQgwaKjWcGo8MmeQcuFHVX5jon20iH4pX0s1lT
Dwyn7tEKqr/vp7dQC1Id/ul0Tixi21jD1yXzR2P86QV2t2cFdd+mH1pjlY4eJlqxKo86
073Sg5RNK8KPeKGrB16xj3U6QA5f8A+z/zzq4Vs5TuKmOb1ASQsClvbajX7LLrB+n3f
xKvkWfJrzfpitG218QSKCXqXNGx+qp2des9+oV0sCTGpWln6Z75jL+4ZrJkZwCVhc3KW
6Y7A==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=references:mime-version:subject:message-id:to:from:date
:dkim-signature;
bh=qm8gQM068LjBKcDOJlgt6b6bnQdUepEnLvq3Q8/2NrY=;
b=tVQie9PZGt18qpRuyzys0MQBinhOyog19rFNpNnqBPwnf00+FPzhc3gMLjGxHUC46W
S1BWqm6WN+GKyJldDNSJQJTAMt3z1C+532Icc0T5gjeaFs7DL/GwkXGyaMQL5LxI2Ih0
KJDONU2HGwrEoQ8/FPkH2Qt5S1p/AEeX83gZpVNQYxgNgJ90p1+K4ZzVPixC5pAiOtUUM
gK7BiigXNYs+9PnaBt8ja63RpKUj0cJ6LPxxVS13nR9C3YI+3M3Qk6TB1i02p9izmiKe
At5sNz8E3sdpRVfXSNqh3eAauLwyQf9mW45N/xd32wFwyg5ncz2H9IhSHUTUNH19Qzg5
Oebg==
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@yahoo.com header.s=s2048 header.b=kGDAPJSu;
spf=pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
smtp.mailfrom=fecdev@yahoo.com;
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
Return-Path: <fecdev@yahoo.com>
Received: from sonic306-21.consmr.mail.ne1.yahoo.com (sonic306-21.consmr.mail.ne1.yahoo.com.
[66.163.189.83])
by mx.google.com with ESMTPS id bp13si8762888qkb.34.2021.10.22.10.29.36
for <lmisf01@gmail.com>
(version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
Received-SPF: pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
client-ip=66.163.189.83;
Authentication-Results: mx.google.com;
dkim=pass header.i=@yahoo.com header.s=s2048 header.b=kGDAPJSu;
spf=pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
smtp.mailfrom=fecdev@yahoo.com;
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKcDOJlgt6b6bnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To;
b=kGDAPJSuIZNdM/9iomv3xoejj2Eh/dH+y1XooeXGyghLxIPKSJY1ZCTeJVvwyBTR+FwBPd5BveOVx8E99y1X0gR19ZsbaeYazJP
q55yZ2GDacT7/q+g0a6EDS0bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkwg6ZhB8HEpYku+21zKbS8VsL50H/a7rKbbC2YL/VFwyN73F
7QVhpPfd/cpOTT13co0wgGcwootEFOXVrwuQtxQePpa8CKZX53JFAYv1rUYWd8BkmifbR8c1WnmOv4ho1nL5003w+gXKgWom6Qh0o
GeF8KxNM31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==
Received: from sonic.gate.mail.ne1.yahoo.com by sonic306.consmr.mail.ne1.yahoo.com with HTTP; Fri, 22
Oct 2021 17:29:35 +0000
Date: Fri, 22 Oct 2021 17:28:56 +0000 (UTC)
From: FEC Dev <fecdev@yahoo.com>
To: "lmisf01@gmail.com" <lmisf01@gmail.com>
Message-ID: <217157422.687119.1634923736910@mail.yahoo.com>
Subject: DKIM Verification Exercise
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----- Part 687118 578898387.1634923736909"
References: <217157422.687119.1634923736910.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.19198 YMailNorrrin
Content-Length: 688

-----=_Part_687118_578898387.1634923736909
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

This is where the message body goes!

-----=_Part_687118_578898387.1634923736909
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit

<html><head></head><body><div class="yahoo-style-wrap" style="font-family:Helvetica Neue, Helvetica,
Arial, sans-serif;font-size:16px;"><div dir="ltr" data-setdir="false">This is where the message body
goes!</div><div dir="ltr" data-setdir="false">
</div><div dir="ltr" data-
setdir="false">
</div><div dir="ltr" data-setdir="false">
</div></div></body></html>
-----=_Part_687118_578898387.1634923736909--

DKIM Verification

Step 4 — Verify Signature

Message

```
date:Fri, 22 Oct 2021 17:28:56 +0000 (UTC)
from:FEC Dev fecdev@yahoo.com
to:"lmisf01@gmail.com" lmisf01@gmail.com
subject:DKIM Verification Exercise
references:217157422.687119.1634923736910.ref@mail.yahoo.com
dkim-signature:v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com;
s=s2048; t=1634923775;
bh=qm8gQM068LjBKcDOJlgte6bbnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To; b=
```

DKIM Verification

Step 4 — Verify Signature

MIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAuoWu
fgbWw58MczUGbMv176RaxdZG
OMkQmn800J/HGoQ6daISMWiL
aj8IMcHC1cubJx2gziAPQHVP
tFYayyLA4ayJUSNk10/uqfBy
iU8qiPCE4JSFrpXflhMIKV4b
t+g1uHw7wLzguCf4YAoR6XxU
KRSAoHuoF7M+v6bMZ/X1G+vi
WHkBl4UfgJQ608F1ckKKoZ5K
qUkJH5pDaqbgS+F3PpyIAUQf
B6EEz0A1KMPRWJGpzgPtKouk
DcQuKUw9GAu17kSIyEcizqrb
aUKNLGAmz0elkqRnzIsVpz6j
dT1/YV5Ri6YU0Q5sN5bqNzZ8
TxoQ1kbVRY6eK0jUnoSSTmSA
hwIDAQAB

Public Key

Message

RSA Signature Verification

Signature

date:Fri, 22 Oct 2021 17:28:56 +0000 (UTC)
from:FEC Dev fecdev@yahoo.com
to:"lmsf01@gmail.com" lmsf01@gmail.com
subject:DKIM Verification Exercise
references:217157422.687119.1634923736910.ref@mail.yahoo.com
dkim-signature:v=1; a=rsa-sha256; c=relaxed/relaxed;
d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKCD0Jlgt6bbnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To; b=

VALID SIGNATURE

kGDAPjSuIZNdm/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvwYBTRfFWbPD5BveOVxBE99yiX0gR19ZsbaeYazJPq55yZ2GDacT7/q+g0a6EDS0bpFajxDQglko9XH/yeG
3ZPSYnoc5CRkgw6ZhB8HEpYku+21zKbS8VsL5OH/a7rKbbC2YL/VFwyN73F7QVhpPfd/cp0TT13co0wgGcWootEF0XVrwuQtXQePpa8CKZX53JFAYv1rUYWd8BkmiFBR8c1WnmOv4ho1n
L5003w+gXKgwom6QhOoGeF8KxNM31j51JnpH3gJZxFOu5nLGF8p0fX6syoKg==

DKIM Verification

Let's verify a DKIM signature!

Download SET 2 data from
<https://sa19.metaspike.com>

Verify RSA Signature w/OpenSSL

```
openssl dgst -sha256 -verify PublicKey.pem -signature Signature.sig  
Message.txt
```

Attacks on DKIM

- ▶ Exploitation of inconsistencies among the different components of the email system (MUA, DNS, DKIM, SPF, DMARC, MTA features, etc.)
- ▶ From Headers
- ▶ MIME comments
- ▶ NULL terminators
- ▶ Sender headers
- ▶ Duplicate fields
- ▶ Lookalike domains
- ▶ <https://www.microsoft.com/>

What is ARC?

- ▶ [RFC 8617](#)
- ▶ An Authenticated Received Chain is the record of individual authentication assessments as a message traverses through ARC-participating Administrative Management Domains (ADMD)
- ▶ Provides an authenticated "chain of custody" for a message

What is ARC?

- ▶ Three new header fields:
 - ▶ ARC-Authentication-Results (AAR)
 - ▶ ARC-Message-Signature (AMS)
 - ▶ ARC-Seal (AS)

What is ARC?

- ▶ Three new header fields:

- ▶ ARC-Authentication-Results (AAR)
- ▶ ARC-Message-Signature (AMS)
- ▶ ARC-Seal (AS)

ARC SET

Original Message

Delivered-To: lmisf01@gmail.com
Received: by 2002:a5d:6487:0:0:0:0 with SMTP id o7csp2293978wri;
Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJyWhaMfNbsirQe35V/ZMXtub5vbdIE2jqxMYGOSnRF
X-Received: by 2002:a37:6c42:: with SMTP id h63mr1170343qkc.243.163.
Fri, 22 Oct 2021 10:29:37 -0700 (PDT)

ARC-Set: i=1; a=rsa-sha256; t=1634923777; cv=none;
d=google.com; s=arc-20160816;
b=bxtn2LvysX8jAuR9slchGhca00nvsD7Wt27ADiTSV08RD141L4wOGsWn4YGTI+vNSM
KXrh8mIwyQDpHir2X9tvyiBrf0VgzghQgwaKjWcGo8MmeQcuFHVX5jon20iH4pX0s11T
Dwyn7tEKqr/vp7dQC1Id/ul0Tixi21jD1yXzR2P86QV2t2cFdd+mH1pj1Y4eJlqxKo86
073Sg5RNK8KPeKGrB16xj3U6QA5f8A+z/zzq4Vs5TuKm0blASQsClvbajX7LLrB+n3f
xKvkWfJrzfpitG218QSKCXqNGx+qp2des9+oV0sCTGpWln6Z75jL+4ZrJkZwCVHC3KW
6Y7A==

ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=references:mime-version:subject:message-id:to:from:date
:dkim-signature;
bh=qm8gQM068LjBKcDOJlgtE6bbnQdUepEnLvq3Q8/2NrY=;
b=tVQie9PZGt18qpRuyzys0MQBinhOyog19rFNpNqBPwnf00+FPzhc3gMLjGxHUC46W
S1BWqm6WN+GKyJlDNSJQJTAMt3z1C+532Icc0T5gjeaFs7DL/GwkXGyaMQL5LxI2Ih0
KJDONU2HGWrEoQ8/fPkH2Qt5S1p/AEeX83gZpVNQYxgNgJ90p1+K4ZZVPixC5pAi0tUM
gK7BiigXNYs+9PnaBt8ja63RpKUj0cJ6LPxxVS13nR9C3YI+3M3Qk6TB1i02p9izmiKe
At5sNz8E3sdpRVfXSNqh3eAauLwyQf9mW45N/xd32wFwyg5ncz2H9IhSHUTUNH19QzG5
Oebg==

ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@yahoo.com header.s=s2048 header.b=kGDAPJSu;
spf=pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
smtp.mailfrom=fecdev@yahoo.com;
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com

Return-Path: <fecdev@yahoo.com>
Received: from sonic306-21.consmr.mail.ne1.yahoo.com (sonic306-21.consmr.mail.ne1.yahoo.com.
[66.163.189.83])
by mx.google.com with ESMTPS id bp13si8762888qkb.34.2021.10.22.10.29.36
for <lmisf01@gmail.com>
(version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
Received-SPF: pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
client-ip=66.163.189.83;
Authentication-Results: mx.google.com;
dkim=pass header.i=@yahoo.com header.s=s2048 header.b=kGDAPJSu;
spf=pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
smtp.mailfrom=fecdev@yahoo.com;
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com

ARC SET

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKcDOJlgtE6bbnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To;
b=kGDAPJSuIZNdM/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvwYBTRFFwBPd5BveOVxBE99yiX0gR19ZsbaeYazJP
q55yZ2GDacT7/q+g0a6EDS0bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkwg6ZhB8HEpYku+21zKbS8VsL50H/a7rKbbC2YL/VFwyN73F
7QVhpPfd/cpOTT13co0wgGcWootEFOXVrwuQtxQePpa8CKZX53JFAYv1rUYWd8BkmifbR8c1WnmOv4ho1nL5003w+gXKGwom6Qh0o
GeF8KxNM31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==
Received: from sonic.gate.mail.ne1.yahoo.com by sonic306.consmr.mail.ne1.yahoo.com with HTTP; Fri, 22
Oct 2021 17:29:35 +0000
Date: Fri, 22 Oct 2021 17:28:56 +0000 (UTC)
From: FEC Dev <fecdev@yahoo.com>
To: "lmisf01@gmail.com" <lmisf01@gmail.com>
Message-ID: <217157422.687119.1634923736910@mail.yahoo.com>
Subject: DKIM Verification Exercise
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="-----_Part_687118_578898387.1634923736909"
References: <217157422.687119.1634923736910.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.19198 YMailNorrin
Content-Length: 688

-----_Part_687118_578898387.1634923736909
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

This is where the message body goes!

-----_Part_687118_578898387.1634923736909
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit

<html><head></head><body><div class="yahoo-style-wrap" style="font-family:Helvetica Neue, Helvetica,
Arial, sans-serif;font-size:16px;"><div dir="ltr" data-setdir="false">This is where the message body
goes!</div><div dir="ltr" data-setdir="false">
</div><div dir="ltr" data-
setdir="false">
</div><div dir="ltr" data-setdir="false">
</div></div></body></html>
-----_Part_687118_578898387.1634923736909--

ARC SET



```
<html><head></head><body><div class="yahoo-style-wrap" style="font-family:Helvetica Neue, Helvetica, Arial, sans-serif;font-size:16px;"><div dir="ltr" data-setdir="false">This is where the message body goes!</div><div dir="ltr" data-setdir="false"><br></div><div dir="ltr" data-setdir="false"><br></div><div dir="ltr" data-setdir="false"><br></div></div></body></html>
----- Part 687118 /57898387.1634923736909--
```


ARC SET



```
<html><head></head><body><div class="yahoo-style-wrap" style="font-family:Helvetica Neue, Helvetica, Arial, sans-serif;font-size:16px;"><div dir="ltr" data-setdir="false">This is where the message body goes!</div><div dir="ltr" data-setdir="false"><br></div><div dir="ltr" data-setdir="false"><br></div><div dir="ltr" data-setdir="false"><br></div></div></body></html>
----- Part 687118 578898387.1634923736909--
```


ARC SET



```
<html><head></head><body><div class="yahoo-style-wrap" style="font-family:Helvetica Neue, Helvetica, Arial, sans-serif;font-size:16px;"><div dir="ltr" data-setdir="false">This is where the message body goes!</div><div dir="ltr" data-setdir="false"><br></div><div dir="ltr" data-setdir="false"><br></div><div dir="ltr" data-setdir="false"><br></div></div></div></body></html>
----- Part 687118_578898387.1634923736909--
```

What is ARC?

- ▶ ARC-Seal:
 - ▶ Signature does not cover the body of the message (i.e., no bh=)
 - ▶ Only "relaxed" header field canonicalization
 - ▶ The DKIM "h" tag is NOT allowed and, if found, MUST result in a status of "fail"
 - ▶ Within an ARC Set, header fields are supplied to the hash function in the following order:
 - ▶ ARC-Authentication-Results
 - ▶ ARC-Message-Signature
 - ▶ ARC-Seal

How do DKIM and ARC help us in forensic email investigations?

- ▶ Message authentication
- ▶ Content rollback

Caveats: Signing Domain

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
d=yahoo.com; s=s2048; t=1634923775;  
bh=qm8gQM068LjBKcD0Jlgte6bbnQdUepEnLvq3Q8/2NrY=;  
h=Date:From:To:Subject:References:From:Subject:Reply-To;  
b=kGDApJSuIZNdm/9iomv3xoejj2Eh/dH+yiXooeXGYghLx1PkSJY1ZCTeJVvw  
YBTRfFWbPD5Bve0VxBE99yiX0gR19ZsbaeYazJPq55yZ2GDact7/q+g0a6EDSO  
bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkkg6ZhB8HEpYku+21zKbS8VsL50H/a7r  
KbbC2YL/VFwyN73F7QVhpPfd/cp0TT13co0wgGcWootEFOXVrwuQtxQePpa8CK  
ZX53JFAYv1rUYWd8Bkmi fbR8c1Wnm0v4ho1nL5003w+gXKgWom6Qh0oGeF8KxN  
M31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==
```

Caveats: Availability

- ▶ Messages without DKIM & ARC Signatures
- ▶ Older public keys may no longer be available

Caveats: Coverage

- ▶ Only certain fields are covered
- ▶ != tag may further limit coverage

Caveats: Coverage

```
Delivered-To: lmisf01@gmail.com
Received: by 2002:a5d:6487:0:0:0:0 with SMTP id o7csp2293978wri;
  Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
X-Goog-SMTP-Source: ABdhPJyWhaMfNbRsrQe35V/ZMXtub5vbDiE2jqxMYgOSdLcJJcYq2T0nY07gAYZujzkv0zH7nRF
X-Received: by 2002:a37:6c42:: with SMTP id h63mr1170343qkc.243.1634923777253;
  Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1634923777; cv=none;
  d=google.com; s=arc-20160816;
  b=bxtn2LvysX8jAuR9s1clhGhca00nvsD7Wt27ADiTSV08RD141L4wOGsWn4YGTI+vNSM
  KXrh8mIwyQDpHir2X9tvyiBrf0VgzghQgwaKjWcGo8MmeQcuFHVX5jon20iH4pX0s11T
  Dwn7tEKqr/vp7dQC1Id/ul0Tixi21jD1yXzR2P86QV2t2cFdd+mH1pj1Y4eJlqxKo86
  073Sg5RNK8KPeKGrB16xj3U6QA5f8A+z/zzq4Vs5TuKm0blASQsClvbajX7LLrB+n3f
  xKvkWfJrzfpitG218QSKCXQxNGx+qp2des9+oV0sCTGpWln6Z75jL+4ZrJkZwCVHC3KW
  6Y7A==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
  h=references:mime-version:subject:message-id:to:from:date
  :dkim-signature;
  bh=qm8gQM068LjBKcDOJlgtE6bbnQdUepEnLvq3Q8/2NrY=;
  b=tVQie9PZGt18qpRuyzys0MQBInhOyog19rFNpNqBPwnf00+FPzhc3gMLjGxHUC46W
  S1Bwqm6WN+GKyJlDNSJQJTAMt3z1C+532Icc0T5gjeaFs7DL/GwkXGyaMQL5LxI2Ih0
  KJDONU2HGwrEoQ8/FPkH2Qt5S1p/AEeX83gZpVNQYxgNgJ90p1+K4ZzVPixC5pAiOtUM
  gK7BiigXNYs+9PnaBt8ja63RpKUj0cJ6LPxxVS13nR9C3YI+3M3Qk6TB1i02p9izmiKe
  At5sNz8E3sdpRVfXSNqh3eAauLwyQf9mW45N/xd32wFwyg5ncz2H9IhSHUTUNH19Qzg5
  Oebg==
ARC-Authentication-Results: i=1; mx.google.com;
  dkim=pass header.i=@yahoo.com header.s=s2048 header.b=kGDAPJSu;
  spf=pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
  smtp.mailfrom=fecdev@yahoo.com;
  dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
Return-Path: <fecdev@yahoo.com>
Received: from sonic306-21.consmr.mail.ne1.yahoo.com (sonic306-21.consmr.mail.ne1.yahoo.com.
[66.163.189.83])
  by mx.google.com with ESMTPS id bp13si8762888qkb.34.2021.10.22.10.29.36
  for <lmisf01@gmail.com>
  (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
  Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
Received-SPF: pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
client-ip=66.163.189.83;
Authentication-Results: mx.google.com;
  dkim=pass header.i=@yahoo.com header.s=s2048 header.b=kGDAPJSu;
  spf=pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
  smtp.mailfrom=fecdev@yahoo.com;
  dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
```

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKcDOJlgtE6bbnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To;
b=kGDAPJSuIZNdM/9iomv3xoejj2Eh/dH+y1XooeXGyghLxIPKSJY1ZCTeJVvwyBTR+FwbPD5BveOVx8E99y1X0gR19ZsbaeYazJP
q55yZ2GDacT7/q+g0a6EDS0bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkwg6ZhB8HEpYku+21zKbS8VsL50H/a7rKbbC2YL/VFwyN73F
7QVhpPfd/cp0TT13co0wgGcWootEFOXVrwuQtxQePpa8CKZX53JFAYv1rUYWd8BkmifbR8c1WnmOv4ho1nL5003w+gXKgWom6Qh0o
GeF8KxNM31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==
Received: from sonic.gate.mail.ne1.yahoo.com by sonic306.consmr.mail.ne1.yahoo.com with HTTP; Fri, 22
Oct 2021 17:29:35 +0000
Date: Fri, 22 Oct 2021 17:28:56 +0000 (UTC)
From: FEC Dev <fecdev@yahoo.com>
To: "lmisf01@gmail.com" <lmisf01@gmail.com>
Message-ID: <217157422.687119.1634923736910@mail.yahoo.com>
Subject: DKIM Verification Exercise
MIME-Version: 1.0
Content-Type: multipart/alternative;
  boundary="----- Part 687118 578898387.1634923736909"
References: <217157422.687119.1634923736910.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.19198 YMailNorrrin
Content-Length: 688
```

-----=_Part_687118_578898387.1634923736909

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

Content-Transfer-Encoding: 7bit

This is where the message body goes!

-----=_Part_687118_578898387.1634923736909

Content-Type: text/html; charset=UTF-8

Content-Transfer-Encoding: 7bit

```
<html><head></head><body><div class="yahoo-style-wrap" style="font-family:Helvetica Neue, Helvetica,
Arial, sans-serif;font-size:16px;"><div dir="ltr" data-setdir="false">This is where the message body
goes!</div><div dir="ltr" data-setdir="false"><br></div><div dir="ltr" data-
setdir="false"><br></div><div dir="ltr" data-setdir="false"><br></div></div></body></html>
-----=_Part_687118_578898387.1634923736909--
```


Caveats: Coverage

- ▶ The l= tag informs the verifier of the number of octets in the body of the email after canonicalization included in the cryptographic hash, starting from 0 immediately following the CRLF preceding the body
- ▶ Intended to increase signature robustness when sending to mailing lists that both modify their content and do not sign their messages
- ▶ Major security implications

Caveats: Coverage

```
Delivered-To: lmisf01@gmail.com
Received: by 2002:a5d:6487:0:0:0:0 with SMTP id o7csp2293978wri;
  Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJyWhaMfNbRsrQe35V/ZMXtub5vbDiE2jqxMYgOSdLcJJcYq2T0nY07gAYZujzkv0zH7nRF
X-Received: by 2002:a37:6c42:: with SMTP id h63mr1170343qkc.243.1634923777253;
  Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1634923777; cv=none;
  d=google.com; s=arc-20160816;
  b=bxtn2LvysX8jAuR9slchGhca00nvsD7Wt27ADiTSV08RD141L4wOGsWn4YGTI+vNSM
  KXrh8mIwyQDpHir2X9tvyiBrf0VgzghQgwaKjWcGo8MmeQcuFHVX5jon20iH4pX0s11T
  Dwn7tEKqr/vp7dQC1Id/ul0Tixi21jD1yXzR2P86QV2t2cFdD+mH1pjlY4eJlqxKo86
  073Sg5RNK8KPeKGrB16xj3U6QA5f8A+z/zzq4Vs5TuKmOb1ASQsC1vbajX7LLrB+n3f
  xKvkWfJrzfpitG218QSKCXQxNGx+qp2des9+oV0sCTGpWln6Z75jL+4ZrJkZwCVHC3KW
  6Y7A==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
  h=references:mime-version:subject:message-id:to:from:date
  :dkim-signature;
  bh=qm8gQM068LjBKcDOJlgt6bbnQdUepEnLvq3Q8/2NrY=;
  b=tVQie9PZGt18qpRuyzys0MQBInhOyog19rFNpNnqBPwnf00+FPzhc3gMLjGxHUC46W
  S1Bwqm6WN+GKyJldDNSJQJTAMt3z1C+532Icc0T5gjeaFs7DL/GwkXGyaMQL5LxI2Ih0
  KJDONU2HGWrEoQ8/FPkH2Qt5S1p/AEeX83gZpVNQYxgNgJ90p1+K4ZzVPixC5pAiOtUM
  gK7BiigXNYs+9PnaBt8ja63RpKUj0cJ6LPxxVS13nR9C3YI+3M3Qk6TB1i02p9izmiKe
  At5sNz8E3sdpRVfXSNqh3eAauLwyQf9mW45N/xd32wFwyg5ncz2H9IhSHUTUNH19Qzg5
  Oebg==
ARC-Authentication-Results: i=1; mx.google.com;
  dkim=pass header.i=@yahoo.com header.s=s2048 header.b=kGDAPJSu;
  spf=pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
  smtp.mailfrom=fecdev@yahoo.com;
  dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
Return-Path: <fecdev@yahoo.com>
Received: from sonic306-21.consmr.mail.ne1.yahoo.com (sonic306-21.consmr.mail.ne1.yahoo.com.
[66.163.189.83])
  by mx.google.com with ESMTPS id bp13si8762888qkb.34.2021.10.22.10.29.36
  for <lmisf01@gmail.com>
  (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
  Fri, 22 Oct 2021 10:29:37 -0700 (PDT)
Received-SPF: pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
client-ip=66.163.189.83;
Authentication-Results: mx.google.com;
  dkim=pass header.i=@yahoo.com header.s=s2048 header.b=kGDAPJSu;
  spf=pass (google.com: domain of fecdev@yahoo.com designates 66.163.189.83 as permitted sender)
  smtp.mailfrom=fecdev@yahoo.com;
  dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
```

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1634923775;
bh=qm8gQM068LjBKcDOJlgt6bbnQdUepEnLvq3Q8/2NrY=;
h=Date:From:To:Subject:References:From:Subject:Reply-To;
b=kGDAPJSuIZNdM/9iomv3xoejj2Eh/dH+y1XooeXGYghLxIPKSJY1ZCTeJVvwYBTR+FwbPD5BveOVx8E99y1X0gR19ZsbaeYazJP
q55yZ2GDacT7/q+g0a6EDS0bpFajxDQg1ko9XH/yeG3ZPSYnoc5CRkwg6ZhB8HEpYku+21zKbS8VsL50H/a7rKbbC2YL/VFwyN73F
7QVhpPfd/cp0TT13co0wgGcWootEFOXVrwuQtxQePpa8CKZX53JFAYv1rUYWd8BkmifbR8c1WnmOv4ho1nL5003w+gXKgWom6QH0o
GeF8KxNM31j51JnpH3gJZxFou5nLGF8p0fX6syoKg==
Received: from sonic.gate.mail.ne1.yahoo.com by sonic306.consmr.mail.ne1.yahoo.com with HTTP; Fri, 22
Oct 2021 17:29:35 +0000
Date: Fri, 22 Oct 2021 17:28:56 +0000 (UTC)
From: FEC Dev <fecdev@yahoo.com>
To: "lmisf01@gmail.com" <lmisf01@gmail.com>
Message-ID: <217157422.687119.1634923736910@mail.yahoo.com>
Subject: DKIM Verification Exercise
MIME-Version: 1.0
Content-Type: multipart/alternative;
  boundary="----- Part 687118 578898387.1634923736909"
References: <217157422.687119.1634923736910.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.19198 YMailNorrrin
Content-Length: 688
```

```
-----=_Part_687118_578898387.1634923736909
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit
```

This is where the message body goes!

```
-----=_Part_687118_578898387.1634923736909
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit
```

```
<html><head></head><body><div class="yahoo-style-wrap" style="font-family:Helvetica Neue, Helvetica,
Arial, sans-serif;font-size:16px;"><div dir="ltr" data-setdir="false">This is where the message body
goes!</div><div dir="ltr" data-setdir="false"><br></div><div dir="ltr" data-
setdir="false"><br></div><div dir="ltr" data-setdir="false"><br></div></div></body></html>
-----=_Part_687118_578898387.1634923736909--
```

Caveats: MTA modifications

Message body sent via Gmail:

```
--000000000000f776ad05cef9f14a
Content-Type: text/plain; charset="UTF-8"
This is a *simple *message body.
--000000000000f776ad05cef9f14a
Content-Type: text/html; charset="UTF-8"
<div dir="ltr">This is a <b>simple </b>message body.</div>
--000000000000f776ad05cef9f14a--
```

Received message body after O365 processing:

```
--000000000000f776ad05cef9f14a
Content-Type: text/plain; charset="UTF-8"
This is a *simple *message body.
--000000000000f776ad05cef9f14a
Content-Type: text/html; charset="UTF-8"
<meta http-equiv="Content-Type" content="text/html;
charset=utf-8"><div dir="ltr">This is a <b>simple
</b>message body.</div>
--000000000000f776ad05cef9f14a--
```

Download Resource

Download SET 3 data from
<https://sa19.metaspike.com>

MAPI

- ▶ Messaging Application Programming Interface
- ▶ Simple MAPI (MAPI v0) — Outlook Express/Windows Mail
- ▶ Extended MAPI (MAPI v1) — Outlook / Exchange

Message EntryIDs

00000000ABDD210E5EF63044812535223E6642A90700BF759E405D816B4592B37C65319A7E66000043CA0CFB0000BF759E405D816B4592B37C65319A7E6600057058CB500000

Flags (4 bytes): 00000000

ProviderUID (16 bytes): ABDD210E5EF63044812535223E6642A9

MessageType (2 bytes): 0700 (0x0007 = Private Message) (see [Messaging Object EntryIDs Structures](#))

FolderDatabaseGuid (16 bytes): BF759E405D816B4592B37C65319A7E66

FolderGlobalCounter (6 bytes): 000043CA0CFB

Pad (2 bytes): 0000

MessageDatabaseGuid (16 bytes): BF759E405D816B4592B37C65319A7E66

MessageGlobalCounter (6 bytes): 00057058CB50

Pad (2 bytes): 0000

Two Adjacent Message EntryIDs

00000000ABDD210E5EF63044812535223E6642A90700BF759E405D816B4592B37C65319A7E6600000000010C0000BF759E405D816B4592B37C65319A7E6600057058B8310000

00000000ABDD210E5EF63044812535223E6642A90700BF759E405D816B4592B37C65319A7E6600000000010C0000BF759E405D816B4592B37C65319A7E6600057058B8320000

- ▶ Same FolderGlobalCounter
- ▶ Adjacent MessageGlobalCounter values — 23359698993 and 23359698994.

Conversation Index

01D4BCDA6FEB4D8718988E9F407DB0164AF82711A59E0000252500000006AFF0005EDE3B80

- ▶ 22-byte header
- ▶ 0 or more 5-byte child blocks

Conversation Index

01D4BCDA6FEB4D8718988E9F407DB0164AF82711A59E

0000252500

000006AFF0

005EDE3B80

Conversation Index

01D4BCDA6FEB4D8718988E9F407DB0164AF82711A59E

0000252500

000006AFF0

005EDE3B80



HEADER

01D4BCDA6FEB0000

Date (FILETIME)
02/04/2019 22:39:06.7151360 (UTC)

4D8718988E9F407DB0164AF82711A59E

GUID
4d871898-8e9f-407d-b016-4af82711a59e

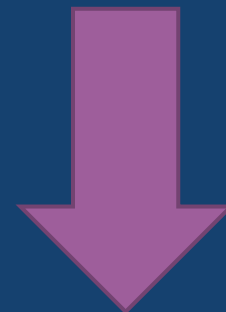
Conversation Index

01D4BCDA6FEB4D8718988E9F407DB0164AF82711A59E

0000252500

000006AFF0

005EDE3B80



CHILD 1

Time Difference: 00:04:09.2727296

02/04/2019 22:43:15.9878656 (UTC)

Conversation Index

01D4BCDA6FEB4D8718988E9F407DB0164AF82711A59E

0000252500

000006AFF0

005EDE3B80



CHILD 2

Time Difference: 00:00:44.8528384

02/04/2019 22:44:00.8407040 (UTC)

Conversation Index

01D4BCDA6FEB4D8718988E9F407DB0164AF82711A59E

0000252500

000006AFF0

005EDE3B80

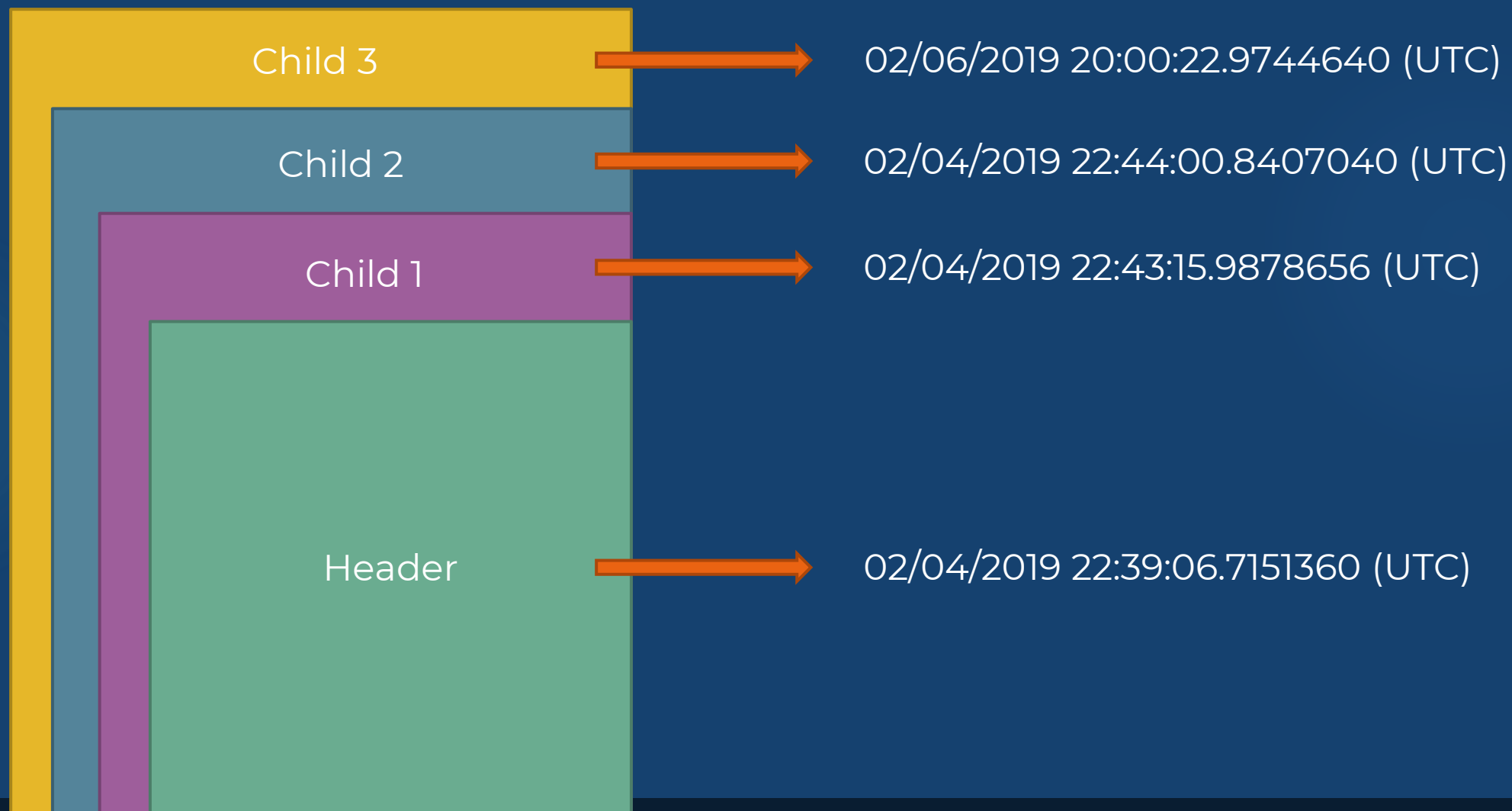


CHILD 3

Time Difference: 1.21:16:22.1337600

02/06/2019 20:00:22.9744640 (UTC)

Conversation Index



Download Resource

Download SET 4 data from
<https://sa19.metaspike.com>

M365 Developer Program

Configure your M365 E5 developer sandbox:

<https://developer.microsoft.com/en-us/microsoft-365/dev-program>

Takeaways

Takeaway Questions #1

- ▶ What can we do to minimize our BEC exposure?

Takeaway Questions #2

- ▶ Do emails contain sender's computer information?
How can we tie an email to a suspect?

Takeaway Questions #3

- ▶ Does a verified DKIM signature indicate a completely authentic email?

Takeaway Questions #4

- ▶ What information do we need to authenticate emails?

Takeaway Questions #5

- ▶ What are the common methods used to impersonate an executive in BEC scenarios?

Takeaway Questions #6

- ▶ Is it okay to whitelist domains?

“To make sure you keep getting these lovely emails, please add example.com to your address book or whitelist us.”

Q&A

Get In Touch

Arman Gungor
agungor@metaspike.com