

Email Analysis & Forensics

Thomas Benos

MSc UniWA, Cisco CyberOps
GR CSIRT Incident Responder
thomasbenos1291@gmail.com

Agenda

- Email Fundamentals and Delivery Process
- Email Structure and Analysis
- Email Forensic Artifacts
- Labs

Email Fundamentals and Delivery Process

E-mail Analysis Introduction

- Common Social Engineering Attacks
 - Spam
 - Phishing
- Email Address
 - User Mailbox (or Username)
 - @
 - Domain
 - Example: user1234@goodmail.com

E-mail Analysis Introduction

Types of malicious emails:

- **Spam** - unsolicited junk emails sent out in bulk to a large number of recipients.
- **Phishing** - emails sent to a target(s) claiming to be from a trusted entity to lure individuals into providing sensitive information.
 - **Spear phishing** – phishing targeting a specific individual(s) or organization.
 - **Whaling** - targeting specifically high-position individuals.
- **Smishing** - targets mobile devices with specially crafted text messages.
- **Vishing** - attacks are based on voice calls.

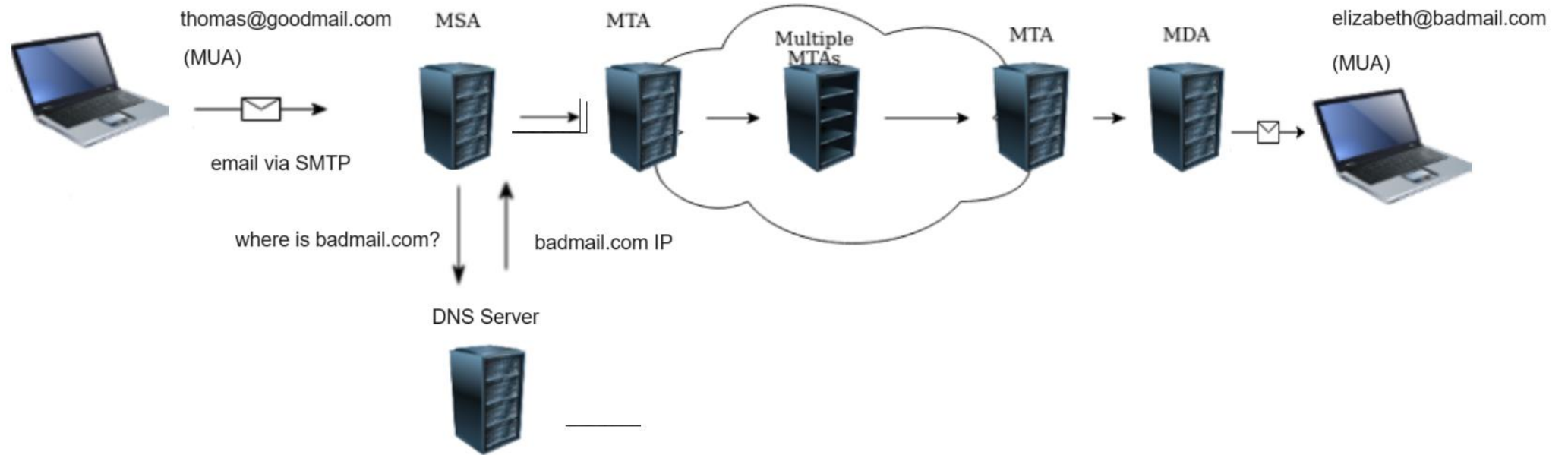
E-mail Analysis Introduction

- Email spoofing
- Sense of urgency
- Trusting entity
- Poorly formatted or written HTML code
- Generic content (Dear Sir/Madam)
- Hyperlinks
- Attachment posing as a legitimate document

E-mail Delivery

- E-mail delivery protocols:
 - **SMTP** – Handles sending
 - **POP3** – Handles transfer
 - E-mails stored on single device and can only be accessed by that device
 - When downloaded -> deleted from email server, unless "Keep email on server" is enabled
 - **IMAP** – Handles transfer
 - E-mails stored on server – can be synced - downloaded to many devices

E-mail Delivery



Email Structure and Analysis

E-mail Analysis – Things to Consider

- What a user can see, is different from what the actual mail contains
- SMTP uses simple text format, but some clients store them in binary format
- Working with languages other than english, means that special attention should be given to the Unicode characters.
- Large quantities mean that there is a need for de-duplication and filtering.
- Attachments are the biggest part of the data, need special analysis and are the main infection reason (with second to follow the malicious links).
- Attachments are the files in ASCII base-64 encoding
- Much of the Headers can be spoofed. Complete reliable headers are only from the MTAs that we trust.

E-mail Analysis - Email Example

```
Return-Path: <postmaster@multwell.net>
Delivered-To: *****@*****
Received: by mailer.***** (Postfix, from userid 506)
  id E6082BEA45; Mon, 11 Oct 2021 13:24:28 +0300 (EEST)
X-Spam-Checker-Version: SpamAssassin 3.3.2 (2011-06-06) on mailer.*****
X-Spam-Level:
X-Spam-Status: No, score=-2.0 required=6.0 tests=HTML_MESSAGE,RCVD_IN_DNSWL_HI,
  SPF_HELO_NONE,URIBL_BLOCKED,URI_FIREBASEAPP autolearn=ham version=3.3.2
Received: from ml.***** (mail.***** [192.168.250.47])
  (using TLSv1 with cipher AECDH-AES256-SHA (256/256 bits))
  (No client certificate requested)
  by mailer.***** (Postfix) with ESMTPS id 8A9B4BEA42
  for <*****@*****>; Mon, 11 Oct 2021 13:24:27 +0300 (EEST)
Received: by ml.***** (Postfix, from userid 506)
  id 1E46F12A1D6; Mon, 11 Oct 2021 13:24:26 +0300 (EEST)
X-Greylist: from auto-whitelisted by SQLgrey-
Received: from srv3.multwell.net (srv3.multwell.net [107.175.239.113])
  (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
  (No client certificate requested)
  by ml.***** (Postfix) with ESMTPS id D9D4812A1CB
  for <*****@*****>; Mon, 11 Oct 2021 13:24:21 +0300 (EEST)
From: Support@ml.*****, Team@ml.*****
To: *****@*****
Subject: Attention: You have over 16 pending messages hanging on the server !!!
Date: 11 Oct 2021 03:24:18 -0700
Message-ID: <20211011030105.BA198E6C82CF2594@multwell.net>
MIME-Version: 1.0
List-Unsubscribe: <mailto:postmaster@multwell.net>
Content-Type: multipart/alternative;
  boundary="-----_NextPart_000_0012_8F29238E.B52D7161"
```

Headers

```
-----_NextPart_000_0012_8F29238E.B52D7161
Content-Type: text/plain;
  charset="utf-8"
Content-Transfer-Encoding: quoted-printable

Dear=C2=A0*****@***** ,=C2=A0

You receive this email because your mailbox (*****@*****)=20
has multiple e-mail messages hanging on the server due to limited=20
memory space

Your mailbox may not receive e-mail because of insufficient=20
storage space.

Click on the link below to increase your storage capacity.=C2=A0

=C2=A0

CLICK HERE TO INCREASE YOUR EMAIL STORAGE CAPACITY=20
(=C2=A0https://webst2e7a952a60b98d51bc9.web.app/#*****@*****=C2=A0)

=C2=A0
```

Body

E-mail Analysis – Email Example

Action recommended: Ensure your resources that interact with Azure services are using TLS 1.2 by 31 October 2024 Inbox x



Microsoft Azure <azure-noreply@microsoft.com>
to me ▾

Nov 13, 2023, 1:01AM (4 days ago)



If you have resources that interact with Azure services and still use TLS 1.1 or earlier, transition them to TLS 1.2 or later by 31 October 2024

You're receiving this email because you're an Azure customer.

To enhance security and provide best-in-class encryption for your data, **we'll require interactions with Azure services to be secured using Transport Layer Security (TLS) 1.2 or later beginning 31 October 2024**, when support for TLS 1.0 and 1.1 will end.

The Microsoft implementation of older TLS versions is not known to be vulnerable, however, TLS 1.2 and later offer improved security with features such as perfect forward secrecy and stronger cipher suites.

Recommended action

- ↩ Reply
- ➔ Forward
- ≡ Filter messages like this
- 🖨 Print
- 🗑 Delete this message
- 🚫 Block "Microsoft Azure"
- ⚠ Report spam
- 👉 Report phishing
- <> Show original
- 🗣 Translate message
- ⬇ Download message
- 📧 Mark as unread

E-mail Analysis – Email Body

Dear *****@*****,

You receive this email because your mailbox (amsc@*****) has multiple e-mail messages hanging on the server due to limited memory space

Your mailbox may not receive e-mail because of insufficient storage space.

Click on the link below to increase your storage capacity.

[CLICK HERE TO INCREASE YOUR EMAIL STORAGE CAPACITY](#)

Dear=C2=A0*****@***** ,=C2=A0

You receive this email because your mailbox (*****@*****)=20
has multiple e-mail messages hanging on the server due to limited=20
memory space

Your mailbox may not receive e-mail because of insufficient=20
storage space.

Click on the link below to increase your storage capacity.=C2=A0

=C2=A0

CLICK HERE TO INCREASE YOUR EMAIL STORAGE CAPACITY=20
(=C2=A0https://webst2e7a952a60b98d51bc9.web.app/#*****@*****=C2=A0)

=C2=A0

E-mail Analysis – Email Headers

- FROM, TO, CC, BCC, Subject, Date

```
From: Support@ml.*****, Team@ml.*****  
To: *****@*****  
Subject: Attention: You have over 16 pending messages hanging on the server !!!  
Date: 11 Oct 2021 03:24:18 -0700
```

- Received
 - Each MTA adds a “Received” which includes the IP of the server, Server Name, date, time, timezone.
 - The order that the e-mail was sent, is from Bottom to Top
 - Spammers could insert fake “Received”

```
Received: from st14p23im-asntp004.me.com (st14p23im-asntp004.me.com. [17.164.101.35])  
by mx.google.com with ESMTPS id y23ei4998397qkj.210.2018.03.15.04.12.37  
for <prateep.gedupudi@gmail.com>  
(version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);  
Thu, 15 Mar 2018 04:12:37 -0700 (PDT)
```


E-mail Analysis – Email Headers

- **Message ID:** Provided by the originating mail server and is a Unique Identifier followed by @ and the server name.
- **X-Originating-IP:** Optional. Used to track the IP of the computer that sent the message.
- **X-Mailer:** Email client used to create the email message. (Web or Locally)
- **Reply-To:** The email address a reply email will be sent to
- **Return-Path:** where bounce-back information will be sent to, for unsuccessful delivery of the email

E-mail Analysis - Email Headers

```
Return-Path: <postmaster@multwell.net>
Delivered-To: *****@*****
Received: by mailer.***** (Postfix, from userid 506)
        id E6082BEA45; Mon, 11 Oct 2021 13:24:28 +0300 (EEST)
X-Spam-Checker-Version: SpamAssassin 3.3.2 (2011-06-06) on mailer.*****
X-Spam-Level:
X-Spam-Status: No, score=-2.0 required=6.0 tests=HTML_MESSAGE,RCVD_IN_DNSWL_HI,
        SPF_HELO_NONE,URIBL_BLOCKED,URI_FIREBASEAPP autolearn=ham version=3.3.2
Received: from ml.***** (mail.***** [192.168.250.47])
        (using TLSv1 with cipher AECDH-AES256-SHA (256/256 bits))
        (No client certificate requested)
        by mailer.***** (Postfix) with ESMTPS id 8A9B4BEA42
        for <*****@*****>; Mon, 11 Oct 2021 13:24:27 +0300 (EEST)
Received: by ml.***** (Postfix, from userid 506)
        id 1E46F12A1D6; Mon, 11 Oct 2021 13:24:26 +0300 (EEST)
X-Greylist: from auto-whitelisted by SQLgrey-
Received: from srv3.multwell.net (srv3.multwell.net [107.175.239.113])
        (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
        (No client certificate requested)
        by ml.***** (Postfix) with ESMTPS id D9D4812A1CB
        for <*****@*****>; Mon, 11 Oct 2021 13:24:21 +0300 (EEST)
From: Support@ml.*****, Team@ml.*****
To: *****@*****
Subject: Attention: You have over 16 pending messages hanging on the server !!!
Date: 11 Oct 2021 03:24:18 -0700
Message-ID: <20211011030105.BA19BE6C82CF2594@multwell.net>
MIME-Version: 1.0
List-Unsubscribe: <mailto:postmaster@multwell.net>
```


E-mail Analysis – SPF

- **Server Authenticity – Sender Policy Framework (SPF)**
 - **Prevention of Email Spoofing** – Detects forged sending addresses
 - **Verification of Sending IP Addresses** - Validates the sending IP address to the originating domain
 - **Identification of Authorized Mail Servers** - Allows organizations to identify which mail servers are allowed to send mails from their domain
 - Received-SPF: “Pass”, “Fail”, “SoftFail”, “Neutral”, “None”
 - We should pay special concern to **Received-SPF: Fail**

```
Received-SPF: pass (google.com: domain of 0100018bd2bb3f9e-6c71474e-48f7-4264-b72f-136ce236fb6e-000000@amazonses.com designates 54.240.48.184 as permitted sender) client-ip=54.240.48.184;
```


E-mail Analysis – DKIM

- DomainKeys Identified Mail (DKIM)
 - **DKIM-Signature** – Added to the header - Validates the message content has not been changed
 - **Verification of Message Integrity** - A valid DKIM check authenticates the sending domain and ensures elements of the message were not altered
 - **Public Key Cryptography** - Private key is held by the sending domain - recipients verify the signature using the public key in sender's DNS records
 - SPF and DKIM pass increase our trust in the other headers

```
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; s=224i4yxa5dv7c2xz3womw6peuasteono; d=amazonses.com; t=1700047568;
h=Date:To:From:Reply-to:Subject:Message-ID:Sender:MIME-Version:Content-Transfer-Encoding:Content-Type:Feedback-ID;
bh=5fYvNPXDWJaibiBFCYHb54SiInEWcBDLHbmK3JDUcuE=; b=Vtma7zJVXFR0YzoMANANq8lln6gFUU590YJhuDkm8/BEBhiMJBrmJ9dikKYrmP9h
Bh7PUgPUYQOMUUsNil5b0Aa72CcJQqlXjHz79jMV4SzcVrZxmd1c5X0xwLHp2yMSeKI gCtLoeNyEeZV8GjCS1Ddy5b1dWjbGk4vshepnwHM=
```


E-mail Analysis – DMARC

- Domain-based Message Authentication, Reporting, and Conformance (DMARC)
 - **Email Authentication and Alignment** – ensures alignment between sender's domain and domain in "From"
 - **Policy Enforcement** – domain owners define policies of what should be done if SPF and DKIM checks fail
 - none (just monitor)
 - quarantine (deliver to spam/quarantine folder)
 - reject (block the email)
 - DMARC pass increase overall trust

```
Authentication-Results: mx.google.com;  
dkim=pass header.i=@netacad.com header.s=p74v6vscrr5r4ayt74lg7qugkee6oujj header.b=Cs7oCuIC;  
dkim=pass header.i=@amazonses.com header.s=224i4yxa5dv7c2xz3womw6peuasteono header.b=Vtma7zJV;  
spf=pass (google.com: domain of 0100018bd2bb3f9e-6c71474e-48f7-4264-b72f-136ce236fb6e-000000@amazonses.com designates 54.240.48.184  
as permitted sender) smtp.mailfrom=0100018bd2bb3f9e-6c71474e-48f7-4264-b72f-136ce236fb6e-000000@amazonses.com;  
dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=netacad.com
```


E-mail Analysis – DMARC

Authentication-Results: mx.google.com;
dkim=pass header.i=@netacad.com
header.s=p74v6vscrr5r4ayt74lg7qugkee6oujj header.b=Cs7oCuIC;
dkim=pass header.i=@amazonses.com
header.s=224i4yxa5dv7c2xz3womw6peuasteono header.b=Vtma7zJV;
spf=pass (google.com: domain of 0100018bd2bb3f9e-6c71474e-48f7-4264-b72f-136ce236fb6e-000000@amazonses.com designates
54.240.48.184 as permitted sender) smtp.mailfrom=0100018bd2bb3f9e-6c71474e-48f7-4264-b72f-136ce236fb6e-000000@amazonses.com;
dmARC=pass (p=NONE sp=NONE dis=NONE) header.from=netacad.com

E-mail Analysis - Attachments

R: Τραπεζική μεταφορά_ 2021-03-26_ Swift αντίγραφο



Εθνική Τράπεζα της Ελλάδος S.A. <info@nbgr.xyz>

To stya@*****



NBG.S.A, TT.Swift_260321_scan.zip
167 KB

Καλό απόγευμα,

Ο πελάτης μας μας ζήτησε να στείλουμε ένα αντίγραφο της συνημμένης μεταφοράς πληρωμής στη

διεύθυνση e-mail σας.

Διεύθυνση ηλεκτρονικού ταχυδρομείου: stya@*****

Επιβεβαιώστε την παραλαβή των χρημάτων και απαντήστε ανάλογα.

Τις καλύτερες ευχές,

Αδωνης Ευαγόρου.

(Τμήμα Εξυπηρέτησης Πελατών)



NATIONAL BANK
OF GREECE

National Bank of Greece S.A.

Content-Type: application/zip; name="NBG.S.A, TT.Swift_260321_scan.zip"

Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename="NBG.S.A, TT.Swift_260321_scan.zip"

```
UESDBBQAAAAIAKZ7ZEnrbLQMgZoCAADoBQAhAAAATkJHLlMuQSwgVFQuU3dpZnRfMjYwMzIxX3NjYW4uaXNv7N3BShtBGADgf62HoAcvpRRrJC30UJB0N7bSHo1NxYtKE0hvIlbBSwQVbB+u7+QLSDubaKXasO2lSvy+ycwyM/8mh4T8MASzAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABEtvYhz4ss+oeD5VZjvM32erPbXF1q9HrN7tnhwelOayVfbhU7J3u7gzR/9X7fLy+Vn5teZY1aLWZGQzOPr6eflM2LWBh20qWW2tSczk7P1Wu1qav7G9yp7aOz/eON71bjYWjlxUpR5G+Kt633+bs8r90ayG+IWwNZANwLU5f5P/pxGINYjly0/lg2ox3r0Yxuqqx1EZ6qZT9s3Tnwc38//J155/z/9Pr6flR/q+PevVx+T8ayp2W7ThK3/9+HMDg+ivsVcbfRakM+Osg+R+YID+G+d+fEgA8JNtb/c6ncgU3AICHIiufsVuUBAAAgImWlc2CBQAAAACYZFnUPf8HAACACZeVTd0CAAAAAAAAEyyMXvsz/7aY7c6ImvH4ihi8eJ8OmL6/OLbo/m5Z69S+DDi+W+HB/Q3PvauDg/orqluNjufOwEA/EfXe+yPye7VEdmXivzfrjw84DR20sEDK5EPDyAoUu8k9mI3Bilmp76mCgA/2bv++CiKkz57P5JNcuEukGiQBA8SKG0Ao5dgYghcYg7RGrxw5A4hgK2QnleqCLuILYFLL21zLGdpS1vb2tY0tKwt/Uhba2mLIQFMQkVFUYoVCyLixEONkoYAMdvvm70D++vT/tE/G9nd+fFm5s2bmffevHlz/v/vf/dXu2QbM+NrwaPrjOlmxp+b/ee/w3jGXPv7MeyJtGcn7ZZuf3bSouA965xr1t73mbWf+pwT/2PAe+9TnJ9e5Vyr3uu8515nzR0+5+fuW7lqZmZmeiEz/t58zSK37wktTT7XPVG6tEOEP7v0JnwnP3Hj0134/vUHS5b+HN/G369e+ii+C++500jw7B/+vB7GbpsLGfJo7eyxN9JZpcypBTGlicYwSI6+0wxY8yBZ43orRE2URb9XfmysNWIGNlGIfy78qXPlb8d6xh7guGvY8Ru+6WJ/c/+gOdWE/u3fzOVVRsUfJ9bnEB0SbITV/6cJN01c+3KTymfYmxbVqLvy/EsZ3/358a/mQYY2/C4BOBEXwv+Ca5r5r0JwDAL/GsEwwS3dt3auxkjmCG51d41H+o77+bdv//+x/+1WtnI2cbIk02u1KE9zzNk61mRubnOrTMTjnlVLDrf4tVvH67adFXWc+avdbP+aokxn18r3Yb8mGdHwCuybkdwZNUgi3psMc9pI82LNK1pILJqGn5NWTQlmaJ/cl5C+1P+v32x+u59nxRLbc/3m3eF611fPu87npxywDy65Bkf3JBvf3xWm7u1v6IHJRYRCW29Chfa3/c4zDvQ3L367L9ya6Mvphn0ButHQaKa4CHZ8AS9WR7CRFCPwCRENHvBp1IxMMt5U3cvvUBXdcjmxbryp9fQmwr6nWlpRR6rUmW0gK9Hp00yrq9XAZH3QFAPr6xQHUTubUpZUuRiCgHzU6HHQCzhvSg+Fz1QxQi0WLNuSLdkEngyQNSF+x3NW19OA+B9NuL7S07wQZtRd897yYa2HMH9AWmeShfSbljtj9kkuvKH0M
```


E-mail Analysis - Attachments

The screenshot shows a web-based email analysis tool. A modal dialog box titled "gchq.github.io says" is open, prompting the user to "Please enter a filename:". The input field contains "download.zip". The dialog has "OK" and "Cancel" buttons.

The background interface includes a "Recipe" section with a "From Base64" option. Below this, there are checkboxes for "Remove non-alphabet chars" (checked) and "Strict mode" (unchecked). The main area displays a large block of Base64-encoded text. At the bottom, there is an "Output" section showing a preview of the decoded content, which appears to be a corrupted or garbled document header.

Additional UI elements include a top navigation bar with "Options" and "About / Support" links, and a bottom toolbar with icons for saving, copying, and zooming. A tooltip "Save output to file" is visible over the save icon.

E-mail Analysis - Attachments

Base64* [copy](#) [clear](#) [de](#)

```
UESDBBQAAAAIAKZ7ZErbLQMgZoCAADoBQAhAAAAATkJHL1MuQSwgVFQuU3dpZnRfMjYwMzIxX3NjYw4uaXNv7N3BShTBGADgf62HoAcvpRRrJC30UJB0N7bSho1NxYtKE0hvI1bBSwQVbB+u7+QLSDubaKXas021Svy+ycwyM/8mh4T8MAszAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABEtYhz4ss+oeD5VZjvM32erPbXF1q9HrN7tnhwe1OayVfbhU7J3u7gzR/9X7fLy+Vn5teZY1aLWZGQz0Pr6ef1M2LWbh20qW2tSczk7P1Wu1qav7G9yp7a0z/e0N71bjYwjl1xUpR
```

[Decode Base64 to File](#)

Preview
Your browser cannot display the file as "application/zip".

File Info

- MIME type: application/zip
- Extension: zip
- Size: 166.82 KB
- Download: [application.zip](#)

Hex Dump

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	
00000000	50	4b	03	04	14	00	00	00	08	00	a6	7b	64	49	eb	6c	b4	0c	81	9a	02	00	00	e8	PK.....{dI.L.....
00000018	05	00	21	00	00	00	4e	42	47	2e	53	2e	41	2c	20	54	54	2e	53	77	69	66	74	5f	...!....NBG.S.A, TT.Swift_
00000030	32	36	30	33	32	31	5f	73	63	61	6e	2e	69	73	6f	ec	dd	c1	4a	1b	41	18	00	e0	260321_scan.iso...J.A...
00000048	7f	ad	87	a0	07	2f	a5	14	6b	24	2d	f4	50	90	74	37	b6	d2	1e	8d	4d	c5	8b	4a	.../.k\$.P.t7...M.J
00000060	13	48	6f	22	56	c1	4b	04	15	6c	1f	ae	ef	e4	0b	48	3b	9b	68	a5	da	b0	ed	a5	.Ho"V.K..L....H;h.....
00000078	4a	fc	be	c9	cc	32	33	ff	26	87	84	fc	30	0b	33	01	00	00	00	00	00	00	00	00	J...23.&...0.3.....
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	44D
000000A8	b6	f6	21	cf	8b	2c	fa	87	83	e5	56	63	bc	cd	f6	7a	b3	db	5c	5d	6a	f4	7a	cd	...!....Vc...z...}j.z.
000000C0	ee	d9	e1	c1	e9	4e	6b	25	5f	6e	15	3b	27	7b	bb	83	34	7f	f5	7e	df	2f	2f	95	...Nk%_n; '{.4...~.//.
000000D8	9f	9b	5e	65	8d	5a	2d	66	46	43	33	8f	af	a7	9f	94	cd	8b	58	18	76	d2	a5	96	...^e.Z-fFC3.....X.v...
000000F0	da	d4	9c	ce	4e	cf	d5	6b	b5	a9	ab	fb	1b	dc	a9	ed	a3	b3	fd	e3	8d	ee	56	e3	...N..k.....V.
00000108	61	68	e5	c5	4a	51	e4	6f	8a	b7	ad	f7	f9	bb	3c	af	dd	1a	c8	6f	88	5b	03	59	ah...JQ.o.....<...o.[.Y
00000120	00	dc	0b	53	97	f9	3f	fa	71	18	83	58	8e	56	34	fe	58	36	a3	1d	eb	d1	8c	6e	...S...?.q..X.V4.X6.....n

<https://base64.guru/converter/decode/file>

E-mail Analysis – Tools

Header analysis:

- Message Header Analyzer: <https://mha.azurewebsites.net/>
- MxToolbox: <https://mxtoolbox.com/EmailHeaders.aspx>

Sender IP address reputation:

- VirusTotal: <https://www.virustotal.com/gui/>
- AbuseIPDB: <https://www.abuseipdb.com/>

E-mail Analysis – Tools

Email body analysis:

- URL Extractor: <https://www.convertcsv.com/url-extractor.htm>
- CyberChef: <https://gchq.github.io/CyberChef/>
- PhishTool: <https://www.phishtool.com/>

Attachment (malware) analysis:

- Any.Run: <https://app.any.run/>
- Analysis: <https://www.hybrid-analysis.com/>
- Joe Sandbox: <https://www.joesecurity.org/>

Email Forensic Artifacts

E-mail Forensic Artifacts - Host

- Email stored on Local Machine
- Identify storage locations
 - Find via filetype searches
 - Review email client configuration info
 - Search for index and message files
- Search for deleted archives
- A password may be needed

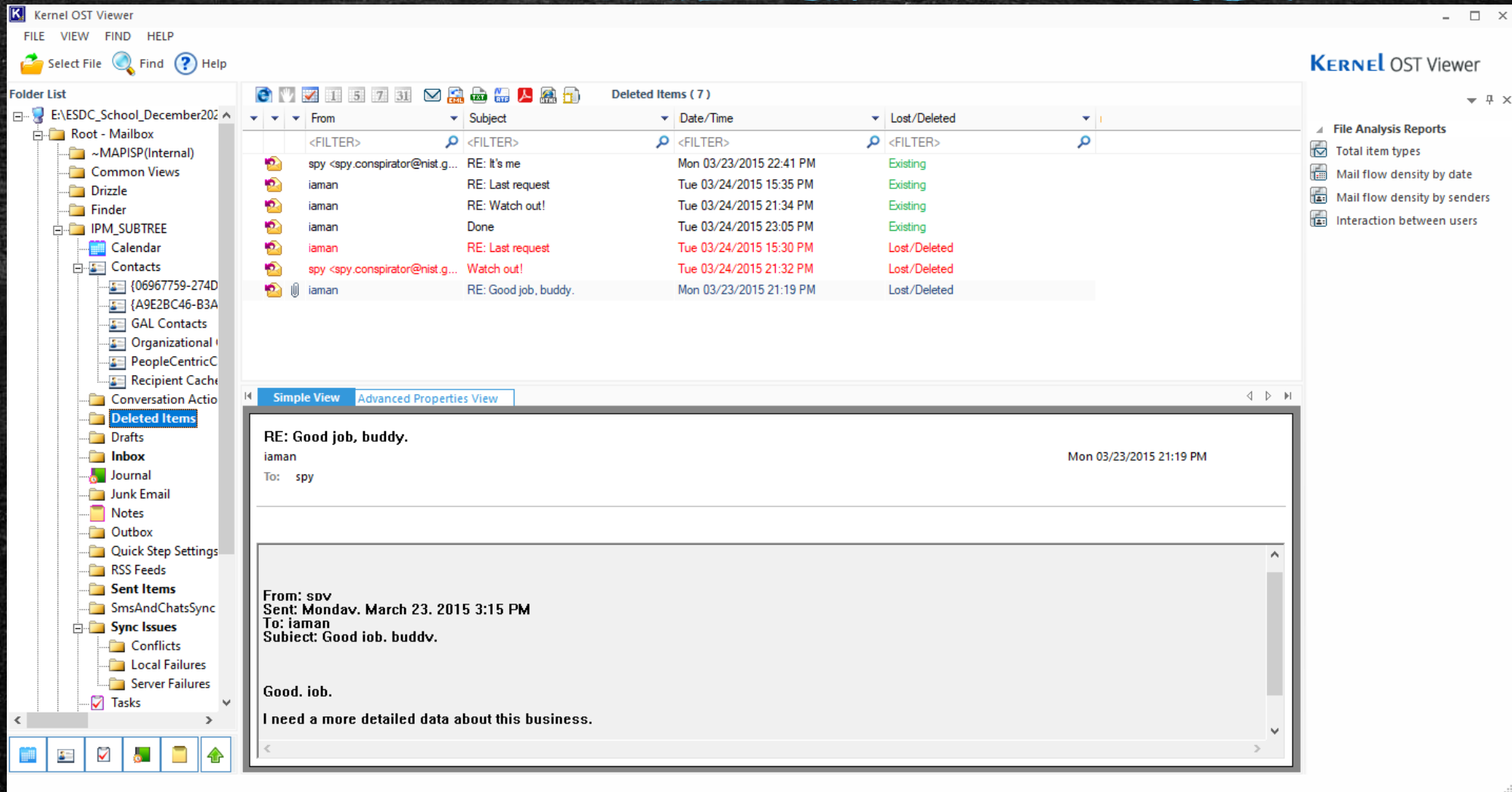
E-mail Forensic Artifacts – Outlook (POP3)

- File extension: PST
 - %AppData%\Local\Microsoft\Outlook (Outlook 2010-)
 - %UserProfile%\Documents\Outlook (Outlook 2013+)
- Registry: What archives are being used
 - HKEY_Current_User\Software\Microsoft\WindowsNT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook
- Encryption\Obfuscation
 - By default: Simple and Weak cipher
 - Options: Strong Password Encryption or No Encryption
- Tools:
 - Password Recovery: PstPassword (Nirsoft)
 - Kernel Outlook PST Viewer
 - Also pffexport in Linux

E-mail Forensic Artifacts – Outlook (IMAP)

- Exchange allows offline mail access (Cached Exchange Mode)
- Local files: **.OST** - most of them remain on the exchange server
- Path: %USERPROFILE%\AppData\Local\Microsoft\Outlook
 - Contains last 12 months of user Exchange data – up to 50 GB
- Orphan files are quite common
- Tools:
 - Kernel OST Viewer (nucleustechnologies)
 - Convert .OST to .PST: ost2pst.exe
 - Repair: scanost.exe (Native from outlook)
 - Also pffexport in Linux (Included in SIFT)

E-mail Forensic Artifacts – Outlook (Offline)



Kernel OST Viewer

FILE VIEW FIND HELP

Select File Find Help

Folder List

- E:\ESDC_School_December20...
- Root - Mailbox
 - ~MAPISP(Internal)
 - Common Views
 - Drizzle
 - Finder
 - IPM_SUBTREE
 - Calendar
 - Contacts
 - {06967759-274D}
 - {A9E2BC46-B3A}
 - GAL Contacts
 - Organizational I
 - PeopleCentricC
 - Recipient Cache
 - Conversation Actio
 - Deleted Items**
 - Drafts
 - Inbox
 - Journal
 - Junk Email
 - Notes
 - Outbox
 - Quick Step Settings
 - RSS Feeds
 - Sent Items
 - SmsAndChatsSync
 - Sync Issues
 - Conflicts
 - Local Failures
 - Server Failures
 - Tasks

Deleted Items (7)

From	Subject	Date/Time	Lost/Deleted
<FILTER>	<FILTER>	<FILTER>	<FILTER>
spy <spy.conspirator@nist.g...>	RE: It's me	Mon 03/23/2015 22:41 PM	Existing
iaman	RE: Last request	Tue 03/24/2015 15:35 PM	Existing
iaman	RE: Watch out!	Tue 03/24/2015 21:34 PM	Existing
iaman	Done	Tue 03/24/2015 23:05 PM	Existing
iaman	RE: Last request	Tue 03/24/2015 15:30 PM	Lost/Deleted
spy <spy.conspirator@nist.g...>	Watch out!	Tue 03/24/2015 21:32 PM	Lost/Deleted
iaman	RE: Good job, buddy.	Mon 03/23/2015 21:19 PM	Lost/Deleted

Simple View Advanced Properties View

RE: Good job, buddy.
iaman
To: spy
Mon 03/23/2015 21:19 PM

From: sbv
Sent: Mondav, March 23, 2015 3:15 PM
To: iaman
Subject: Good iob, buddv.

Good. iob.
I need a more detailed data about this business.

File Analysis Reports

- Total item types
- Mail flow density by date
- Mail flow density by senders
- Interaction between users

E-mail Forensic Artifacts – Outlook (Attachments)

- Secure Temp Folder:
 - %AppData%\Local\Microsoft\Windows\INetCache\Content.Outlook\
<random name subfolder> (IE11+)
 - %APPDATA%\Local\Microsoft\Windows\Temporary Internet
Files\Content.Outlook\
<random name subfolder>
 - HKCU\Software\Microsoft\Office\
<version>\Outlook\Security\
OutlookSecureTempFolder
- Attachments persisted until Outlook 2007
- Attachments after Outlook 2007, are present only after closing the program before closing the attachment or on a crash
- Timestamp of the file is attached to the time of the email
- MFT \$Filename – determine time attachment was opened

E-mail Forensic Artifacts – Server

- Most corporate environments employ dedicated mail servers
 - Can also be hosted offsite or in the cloud
- Business considerations make getting forensic copies difficult
 - Expect massive amounts of data
 - Specialized tools may be required
- Deleted mail exist, but only for a short time

E-mail Forensic Artifacts – Server (Exchange)

- Exchange database is the container for user mailboxes
- Exchange 2007 and above use .EDB format
 - Extensible Storage Engine (ESE) format
 - Previously, .EDB and .STM files composed database
- .EDB files store mail, attachments, contacts, journal, notes, tasks, calendar, and address book entries
- .log files contain messages not yet written to .EDB
- Exchange might be broken up into multiple storage groups, each with multiple .EDB databases
- Mailboxes can be exported in .PST file format

E-mail Forensic Artifacts – Server (Exchange)

- 2007
 - C:\Program Files\Microsoft\Exchange Server\Mailbox\First Storage Group\Mailbox Database.edb
 - C:\Program\Files\Microsoft\Exchange Server\Mailbox\First Storage Group\Public Folder Database.edb
- 2010+
 - C:\Program Files\Microsoft\Exchange Server\V<version>\Mailbox Database\Mailbox Database.edb
 - C:\Program Files\Microsoft\Exchange Server\V<version>\Public Folder Database\Public Folder Database.edb
- In any case through: `Get-MailboxDatabase -Status | select "edbfilepath"`
- Remember if an ESE DB is "dirty" clean it with `eseutil`
 - `esentutl /mh "C:\Path\To\Database.edb"`
 - `esentutl /r "C:\Path\To\Database.edb" /d`

E-mail Forensic Artifacts – Server (Exchange Recoverable Items)

- **Deletions:** SHIFT+DEL, remains in Deletion Folder for 14 days.
- **Purges:** After the 14 days, mails remain in the “Purges” for some time, depending on the server, where is permanently deleted.
- **Discovery Hold:** For after the 14 days period, check if “**Hold**” action was applied to the mailbox
- **Logs:** can show a lot about mailboxes, but are not enabled by default
- **Message tracing:** Message-ID, sender-receipient, dates, subject, size, delivery status, originating IP.
 - On by default, for 90 days.

E-mail Forensic Artifacts – Server (Exchange Recoverable Items)

- Export mail:
 - `New-MailboxExportRequest -Mailbox <MailboxName> -Filepath <path\to\file>.pst (MS Exchange 2010)`
 - `Export-Mailbox -Identity <MailboxName> -PSTFolderPath "<path\to\file>.pst (MS Exchange 2007)`
- Filter output:
 - `New-MailboxExportRequest -Mailbox <name> -Filepath <path\to\file>.pst -ContentFilter {(body -like "*whatever*")} -and (Received -lt "01/11/21")}`
- Also use the `New-ComplianceSearch` in Powershell
 - `New-ComplianceSearch -Name "SearchName" -ExchangeLocation All -ContentMatchQuery "Subject:'Keyword' AND Received<=01/01/2023" -Export -FilePath "\\Server\SharedFolder\MailboxExport.pst"`

E-mail Forensic Artifacts – Server (WebMail)

- Email typically stored on ISP servers
 - Possible exception for POP or IMAP
- User IP address and subscriber info may be available from ISP (correlation with Webmail addresses)
- Cached copies can be recovered
- Tool: Google Takeout
 - <https://takeout.google.com/settings/takeout>
 - Requires credentials

Thank you for your patience!
