



# Curso de Ciberseguridad

## Análisis Forense en Windows

Análisis Forense Informático



Forense de correos electrónicos.....	3
Cabecera de correo electrónico.....	3
Message ID.....	4
Mapi Headers.....	5
Content-Lenght.....	6
IMAP Internal Date .....	6
DKIM.....	8
SPF.....	10
DMARC.....	11
Authentication Results.....	13
¿Dónde Podemos encontrar mensajes de Correo Electrónico?.....	14
Microsoft Outlook PST.....	14
Microsoft Outlook OST.....	15
Recuperación de Adjuntos en Microsoft Outlook.....	16
Thunderbird MBOX.....	16
Windows 10 Mail App.....	17
Google Takeout .....	22
Modificación de mensajes de Google.....	22
Microsoft Exchange.....	23
Office365.....	25
Herramientas.....	26
Kernel EML Viewer .....	26
Mitec Mail Viewer.....	26
Yet Another Mail Analysis Tool (YAMAT).....	27
MEIOC.....	27
Forensic Email Collector.....	28
EmailRep.io.....	28

## FORENSE DE CORREOS ELECTRÓNICOS

En las investigaciones, muchas veces tendremos que analizar un correo electrónico para poder identificar si es legítimo o no, o desde qué dirección IP fue enviado.

¿Qué información podemos encontrar analizando un email o correo electrónico?

- ◆ ¿Quién envió el email? -> dirección de correo, dirección IP, pruebas de contexto
- ◆ ¿Cuándo fue enviado? -> Timestamp en la cabecera, timestamp de los servidores
- ◆ ¿Desde donde fue enviado? Dirección IP / ISP, Geolocalización, Mail server domain, Message ID
- ◆ ¿Es el contenido relevante? Message Body, Adjuntos, libreta de direcciones, Entradas de calendario

A continuación, vamos a identificar los posibles campos que podemos encontrar en un mensaje de correo electrónico y que permita poder realizar un análisis forense de los mismos.

### CABECERA DE CORREO ELECTRÓNICO

Podemos encontrar en la cabecera la fecha de cuando se envió el correo electrónico, el message ID, el destinatario, el remitente.

```
MIME-Version: 1.0
Date: Tue, 11 Sep 2018 23:04:37 +0200
Message-ID: <CANKW5xbMkzGTjQ5VanfpwQa2pgKDitj3m+9KPesrBx8+X9DUTg@mail.gmail.com>
Subject: Proof of concept
From: Gonzalo Villarejo Heras <gvillarejoh@gmail.com>
To: Gonzalo Villarejo Heras <gvillarejoh@gmail.com>
Content-Type: multipart/mixed; boundary="000000000000a772d805759ed214"
```

HEADER

```
--000000000000a772d805759ed214
Content-Type: multipart/alternative; boundary="000000000000a772d405759ed212"
```

```
--000000000000a772d405759ed212
Content-Type: text/plain; charset="UTF-8"
```

Please,

Find below the attachment.

Regards

```
--000000000000a772d405759ed212
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable
```

```
<div dir=3D"ltr">Please,=C2=A0<div><br></div><div>Find below the attachment=
.</div><div><br></div><div>Regards</div></div>
```

```
--000000000000a772d405759ed212--
```

```
--000000000000a772d805759ed214
Content-Type: image/png; name="image3.png"
Content-Disposition: attachment; filename="image3.png"
Content-Transfer-Encoding: base64
X-Attachment-Id: f_jly7ebce0
Content-ID: <f_jly7ebce0>
```

MENSAJE

ADJUNTO

Podemos encontrar sitios en internet donde le indicamos la cabecera, es decir, copiamos y pegamos la misma y automáticamente nos proporciona los campos analizados:

<https://mxtoolbox.com/EmailHeaders.aspx>

```
Delivered-To: gvillarejoh@gmail.com
Received: by 10.25.143.132 with SMTP id s4csp28084181fk;
  Fri, 24 Nov 2017 15:54:07 -0800 (PST)
X-Goog-Smtp-Source: AGs4zMBX1K0VM10Y8sdjHyd5ZKyP4hJkRoqQ0g9HqLORwofKVutPn8z1LO3L/gnWw+qHqGdg1+0d
X-Received: by 10.28.143.212 with SMTP id r203mr11223156wmd.44.1511567647489;
  Fri, 24 Nov 2017 15:54:07 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1511567647; cv=none;
  d=google.com; s=arc-20160816;
  b=c04X6KXZsCp3uMlFpR1Bbtg8NEcND0TiOVk9t4pC+w67aUQisGcu57fKxsCXGuZO0M
  /6TgdKIRHqppq5X0uS3doXhH06x+IvDTr12no81iQtJscF0r/i1xpXcQ32rHORMHJP
  yNjGfSwlKcF/tp6/YTYSYvVqeftd8KEBsvX94GPHTEBRltBe6JwXQqWgvp7AAenNpsF
  nyBCqQA9MHPMc3gYCC0B0+WPq6V/g2dTUxT5hpFTLnxEBtEMXrpdqvt0vDa6V3vZl
  hH0B0yFH3n1wXVmw0Ed7Uup+fvx9BBYH8mOfpTcX2m63/XNQTm9Fq0h6CZ4I1brkUK
  MuuQ=
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
  h=mime-version:subject:message-id:to:from:date
  :arc-authentication-results;
  bh=QzE0qZ8teQ7HYT0gn51NCRdmWQe500dQGArAxnzPo=;
  b=y1jU4ze3VIVSRgtiQwIndUDf89r8chvWQyWZDNYoVHTsUbyc9P8MC0QpLqGSD3WV
  k1X9FMCCM82vocLgzPwJ0FocTEU64QCjMfK1Np0k8PMV9rnJcNAP2fjgWshuNvkSVN
  WMAKMXHUvrcNXJMcBcM2GzGwCwLr5ITvcXsPy8M9G9a0VMhritdiFolTQ04jx4bv2ax
  iy1lpPomelvBRXBj4/OZ3RJV/LXGNEWTUtk/RQ2kc45a6arYgHeoGaZ7J2QzokPibf
  73k+ylp6NM8UartV3J504mSLGrkws1K3/KzqSokyDc4tg2beEnK1NaKDFmu45M1NtmQ
  d6yQ=
ARC-Authentication-Results: i=1; mx.google.com;
  spf=pass (google.com: domain of noresponder@idealista.com designates 62.97.67.93 as permitted sender) smtp.mailfrom=noresponder@idealista.com
Return-Path: <noresponder@idealista.com>
Received: from mx3s.idealista.com (mx3s.idealista.com. [62.97.67.93])
  by mx.google.com with ESMTPS id i80si7636220wmf.240.2017.11.24.15.54.06
  for <gvillarejoh@gmail.com>
  (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
  Fri, 24 Nov 2017 15:54:07 -0800 (PST)
Received-SPF: pass (google.com: domain of noresponder@idealista.com designates 62.97.67.93 as permitted sender) client-ip=62.97.67.93;
Authentication-Results: mx.google.com;
  spf=pass (google.com: domain of noresponder@idealista.com designates 62.97.67.93 as permitted sender) smtp.mailfrom=noresponder@idealista.com
Received:
Date: Sat, 25 Nov 2017 00:54:06 +0100 (CET)
From: idealista <noresponder@idealista.com>
To: gvillarejoh@gmail.com
Message-ID: <1222641122.387082091511567646260.JavaMail.core@comm2.pro.es.sys.idealista>
Subject: Resumen diario de nuevos anuncios
MIME-Version: 1.0
```

También podemos saber cuándo fue recibido el correo electrónico por el servidor SMTP mediante el campo: "Received"

En Gmail podemos ver la cabecera de un correo electrónico tal y como se indica aquí:

<https://support.google.com/mail/answer/29436?hl=es>

## MESSAGE ID

El message ID lo proporciona el servidor que envía el email y consiste en un único identificador añadido al nombre del servidor con la @.

Este campo puede ser utilizado para identificar mensajes relacionados gracias al tag **References** y **In-Reply-To**:

Ejemplo:

```
MIME-Version: 1.0
Date: Tue, 16 Oct 2018 12:45:49 +0200
References: <CAEzucbjNgPk+QnU4Xav-Zpg83Vm2k+1rDMw+SwBR0ahbR2FFcQ@mail.gmail.com> <CABmgGbu_5G47Ed2P-oFTBEhgJcQXRmUuJoiRX6kFFOaaQZS9w@mail.gmail.com> <CAEzucbjNgPk+QnU4Xav-Zpg83Vm2k+1rDMw+SwBR0ahbR2FFcQ@mail.gmail.com>
In-Reply-To: <CAEzucbjNgPk+QnU4Xav-Zpg83Vm2k+1rDMw+SwBR0ahbR2FFcQ@mail.gmail.com>
Message-ID: <CABmgGbt0CfcE8TEU-WMj40M04AVyCLMf42+j_zh-LCN6EBRBrw@mail.gmail.com>
Subject: Re: Mensaje 1
From: Ismael Serrano <ismiserrani2345@gmail.com>
To: juanmanuelmartinezcalala@gmail.com
Content-Type: multipart/alternative; boundary="00000000000007235c057856428a"
```

Mensajes	Message ID
Mensaje Origen	<u>CAEzucbjNgPk+QnU4Xav-Zpg83Vm2k+1rDMw+SwBR0ahbR2FFcQ@mail.gmail.com</u>
Responder al mensaje anterior	<u>CABmgGbu_5G47Ed2P-oFTBEhgJcQXRmUuJoiRX6kFFOaaQZS9w@mail.gmail.com</u>
Responder al mensaje anterior	<u>CAEzucbjNgPk+QnU4Xav-Zpg83Vm2k+1rDMw+SwBR0ahbR2FFcQ@mail.gmail.com</u>
Responder al mensaje anterior	<u>CABmgGbt0CfcE8TEU-WMj40M04AVyCLMf42+j_zh-LCN6EBRBrw@mail.gmail.com</u>

En la conversación anterior, se puede ver el histórico de Message ID que hay. Esto indica que debe haber también cuatro mensajes. Uno por cada Message ID.

## MAPI HEADERS

Si estas realizando una investigación donde hay un servidor Exchange o clientes tales como Microsoft Outlook, debes ser consciente que las propiedades MAPI (Microsoft Messaging Application Programming Interface) estarán presentes. Son unas cabeceras adicionales que nos van a permitir extraer más información de un simple correo electrónico:

- ◆ **Mapi-Client-Submit-Time:** la fecha del sistema local cuando el email fue enviado por el cliente.
- ◆ **Mapi-Conversation-Index:** indica cuantos mensajes hijos fueron parte de la cadena de emails y registra los timestamps para cada mensaje en la cadena.
- ◆ **Mapi-Entry-ID:** un identificador de mensaje dentro del almacenamiento como PST. Puede ayudar a identificar si un usuario disponía de varios ficheros PSTs.
- ◆ **Mapi-Message-Flags** y **Pr\_last\_Verb\_Executed:** proporciona información detallada de las acciones que ocurrieron en un Cliente MAPI: Leído, sin leer, respondidos, reenviados, fuera de la oficina

## CONTENT-LENGTH

El campo Content-Length campo del correo electrónico puede ser utilizado para verificar el payload del correo. Es decir, si estamos investigando una posible modificación del correo electrónico, podríamos volver a calcular el tamaño para ver si de verdad tiene el tamaño que indica.

```
Date: Tue, 26 Mar 2019 04:30:10 +0000 (UTC)~
From: <john.doe@yahoo.com>~
To: Jane Doe <jane.doe@yahoo.com>~
Message-ID: <2012827807.11465024.1553574610014@mail.yahoo.com>~
Subject: Apollo 11 Info~
MIME-Version: 1.0~
Content-Type: multipart/alternative; ~
> boundary="-----=_Part_11465023_1138928915.1553574610013"~
References: <2012827807.11465024.1553574610014.ref@mail.yahoo.com>~
Content-Length: 1981~

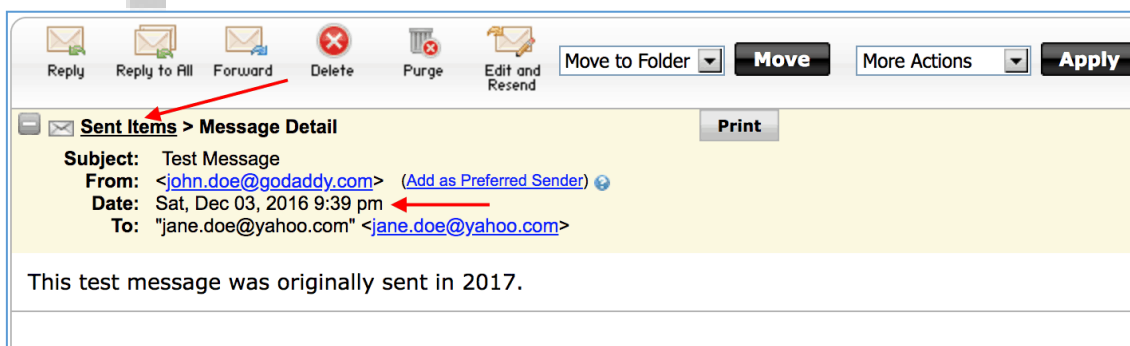
-----=_Part_11465023_1138928915.1553574610013~
Content-Type: text/plain; charset=UTF-8~
Content-Transfer-Encoding: quoted-printable~

Apollo 11 was launched by a Saturn V rocket from Kennedy Space Center on Me=
```

**1981 bytes**

## IMAP INTERNAL DATE

El campo IMAP internal date indica la fecha y hora del mensaje dentro del servidor IMAP. Este timestamp es distinto de la fecha de cuando se originó el mensaje que lo podemos encontrar en el header.



Si vemos el mensaje anterior, podemos identificar que le mensaje fue enviado el 3 de diciembre de 2016.

Si obtenemos las cabeceras del correo electrónico, podemos identificar lo siguiente:

```
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="utf-8"
User-Agent: Workspace Webmail 6.9.36
Message-Id: <20171203153135.4b5c8628937d16bc17cc44c9ad222e17.7ac1f537cc.wbe@email15.godaddy.com>
From: - <john.doe@godaddy.com>
To: "jane.doe@yahoo.com" <jane.doe@yahoo.com>
Subject: Test Message
Date: Sat, 3 Dec 2016 21:39:27 -0700
Mime-Version: 1.0
X-format: tinymce
<html><body><span style=3D"font-family:Verdana; color:#000000; font-size:10=
pt;"><div>This test message was originally sent in 2017.<br mce_bogus=3D"1"></div></span></body></html>
```

Message-Id:

[20171203153135.4b5c8628937d16bc17cc44c9ad222e17.7ac1f537cc.wbe@email15.godaddy.com](mailto:20171203153135.4b5c8628937d16bc17cc44c9ad222e17.7ac1f537cc.wbe@email15.godaddy.com)

Como hemos visto anteriormente, el Message ID es un campo único por cada correo electrónico, por lo que sería un identificador. Este caso también se puede introducir, como vemos en rojo dentro de este campo único una marca de tiempo que sería: 12/03/2017 15:31:35

No todos los Message ID contienen un timestamp, por ejemplo Yahoo no dispone de esta característica:

Message-ID: [2103767838.439800.1512250767353@mail.yahoo.com](mailto:2103767838.439800.1512250767353@mail.yahoo.com)

Entonces, ¿dónde puedo encontrar el IMAP Internal Date? Este tipo de campo podemos localizarlo en los registros o logs del servidor IMAP y podría identificarse algo tal que así:

```
INFO Imap(2)[6] Response: * 1 FETCH (UID 8 RFC822.SIZE 576 FLAGS
(\Seen) INTERNALDATE "21-Jun-2018 17:51:47 +0000" ENVELOPE ("Sat, 3 Dec 2016
21:39:27 -0700" "Test Message" ((NIL NIL "john.doe" "godaddy.com")) ((NIL NIL
"john.doe" "godaddy.com")) ((NIL NIL "john.doe" "godaddy.com"))
(("jane.doe@yahoo.com" NIL "jane.doe" "yahoo.com")) NIL NIL NIL
"<20171203153135.4b5c8628937d16bc17cc44c9ad222e17.7ac1f537cc.wbe@email15.godaddy.com
```

Tendríamos 3 fechas identificadas hasta ahora:

- Header: 3/12/2016 21:39:27 (-07:00)
- Internal Date del Servidor: 21/06/2018 17:51:47 (UTC)
- Message ID: 3/12/2017 15:31:35

Podríamos afirmar que el mensaje fue enviado 03/12/2017 y que fue añadido a su buzón IMAP el 21/06/2018.

Para poder terminar de realizar la investigación, sería necesario analizar el equipo informático desde el que se envió, para poder contextualizar las fechas localizadas y obtener una conclusión clara.

Aunque solamente hemos visto este tiempo de campos que significan marcas de tiempo, en el siguiente enlace, podemos ver que existen multitud de marcas de tiempo a lo largo de un mensaje de correo

electrónico y que debemos de tener en cuenta, para verificar si de verdad es legítimo o no, en cuanto a la fecha: <https://www.metaspike.com/timestamps-forensic-email-examination/>

## DKIM

**DomainKeys Identified Mail (DKIM)** es un estándar que permite que una entidad asuma la responsabilidad de un mensaje en tránsito, es decir, nos va a permitir identificar si el correo es legítimo o no, gracias a este campo que veremos en el header.



El mensaje de que proviene del Servidor de Correo A, viene firmado con su clave privada. El servidor de Correo A hasha el body del mensaje junto con un subconjunto de campos del header. Cuando llega al servidor de Correo B, el servidor contacta con el dominio del correo electrónico (La clave publica de la entidad que lo firma es publicado en el registro DNS como un TXT) y le solicita la clave pública. Una vez con la clave publica descifrará los campos y calculara con los campos que el ha recibido para ver si coinciden.





```
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; d=sendgrid.net;
h=content-transfer-encoding:content-type:from:mime-version:to:subject:references;
s=smtapi; bh=PaEUK52QPpczN3qipHGM0QqcYY=; b=cKzVevUu2z3xQCLhS7
JbhdLu7ApoJ1HG+8CprR+EydoQG+gJw/6Jap+t6/ZYcmIjHix/BXYoqsYNuvToG
Z+zmcS2yvYj3Ontkixi1NcgtuRGJl4y+Y2owFlwzlsblqqbFKqRAvEavM057zL
GjiEh1qyjBdalj1nITkG1bU=
Received: by filter0064p3mdw1.sendgrid.net with SMTP id filter0064p3mdw1-24524-5B9CA813-13
2018-09-15 06:34:59.812813938 +0000 UTC m=+42086.059729424
Received: from NTayNTk4MA (li86-107.members.linode.com [74.207.244.107])
by ismtpd0017p1las1.sendgrid.net (SG) with HTTP id 3rS7A7H6RcKabEBbKxr8VA
Sat, 15 Sep 2018 06:34:59.643 +0000 (UTC)
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset=UTF-8
Date: Sat, 15 Sep 2018 06:35:01 +0000 (UTC)
From: "Miralytics" <support@miralytics.com>
Mime-Version: 1.0
To: 13877929815@163.com <13877929815@163.com>
Message-ID: <3rS7A7H6RcKabEBbKxr8VA@ismtpd0017p1las1.sendgrid.net>
Subject: Ticket #118 Updated - naoshi
References: <HtSYxi45T5e99G34tpwDUw@ismtpd0003p1las1.sendgrid.net>
SentByAdroitdesk: XDFKK11
X-SG-EID: OUX5t/oyROeQbmkmVOVxRZLf9Zlp8/fSfKj8/EqzrRZ+tvDGttNaaqoXBHRQaCDIdNR47RUicuOiBz
h6lt6qVcQhFE/5v5IK8tJkxaw+WujK6cleIHlX1MlqgZ6YPGeFtjKEopX3Hhuxrz43n+JGHaEhVfP
INvZzVJnT5nLvdzUnJT/VW5ekVBpkxVjRVqYJfHzuBKnVgYcFGuesC76yvYHlnodf5Lm0aq1t8XqIJ
Q=
```

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20161025;
h=mime-version:from:date:message-id:subject:to;
bh=NuUVBkHAbInFrMSNaWdGtwpj9poc3wM2sXMhd25sPE=;
b=gGpvUwVrIr1IBFWl9ZyFDYqvIO63kM27v1T90W5YWsPeXuFHZVuKuaFBO28GkBQJsg
ogqFsLfIicvDiEs5hPQfuI3SiZmXgizbnNB85ikrNh8oekceHCzcE7Rp4fe9EBiyMOMk
VjG1b4q7h7HCqBWOh9zHIpkoT2n6JSK0VpH2nJulKy8YrnAyZAm8on5XAWWVB83OvvU7
w4f2UMWPeXZEnNdGk67Kmm09VT3NfwMX8WEhajxcuLETLPirsgxROz2GaoNJ4gqDOi/O
eZtiT+sTWDxpjkrIcTOygr3Lcgb8D8CELqZOVeR0M9ySimQsobTicF1wOERP2NvaigFP
rjVA==
```

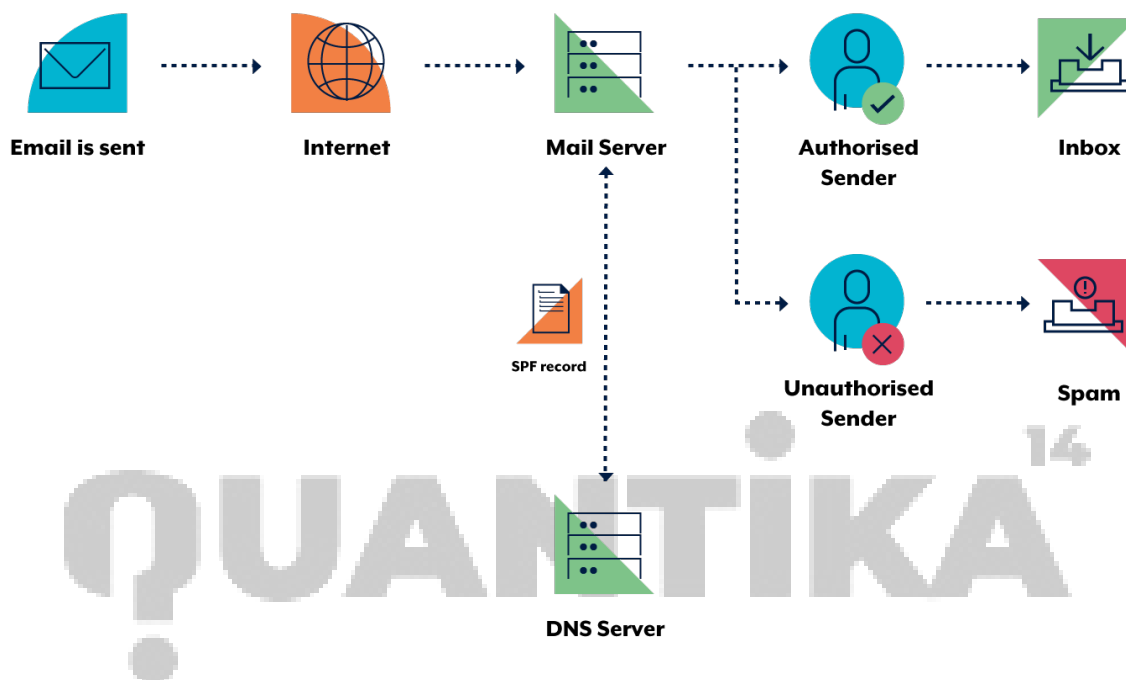
- ◆ v= indica la versión de la especificación DKIM
- ◆ a= especifica el algoritmo que fue utilizado para crear la firma. RSA-SHA256
- ◆ c=indica como el body y headers del email fueron preparados para hashear. Relaxed/Relaxed significa que aplicó a ambos. C=relaxed, solo al header y C=simple solo al body.
- ◆ d= indica el dominio al cual se debe reclamar para la responsabilidad de transmisión del mensaje
- ◆ s= indica el selector para el dominio. S=20161025 indica que podemos obtener el registro TXT así: 20161025.\_domainkey.Gmail.com para obtener la clave publica
- ◆ h=indica que campos fueron incluidos en la firma
- ◆ **bh=el hash del body del mensaje en base64**
- ◆ b= datos de la firma en base 64

Herramientas para validar los campos de DKIM:

- ◆ <https://dkimvalidator.com/>
- ◆ <https://dkimcore.org/tools/keycheck.html>
- ◆

## SPF

La protección SPF **se encarga de comprobar los servidores autorizados para enviar correos electrónicos a nombre de un dominio**. Para ello, el servidor receptor comprobará en el DNS del dominio la lista de equipos permitidos para dicho fin.



Para que pueda llevarse a cabo la comprobación SPF, se debe registrar en el DNS de tu dominio qué equipos autorizas para que envíen correos electrónicos en tu nombre.

Registro DNS, le indicamos desde que servidores se pueden enviar correos electrónicos:

```
v=spf1  
ip4:194.57.88.210 ip4:194.57.88.211 ip4:194.57.88.212 ~all
```

### Cabecera Received-SPF

```

Delivered-To: [redacted]@gmail.com
Received: by 10.76.81.100 with SMTP id z4csp597786oax;
Wed, 15 Oct 2014 07:28:55 -0700 (PDT)
X-Received: by 10.181.29.105 with SMTP id jv9mr12979657wid.25.1413383334978;
Wed, 15 Oct 2014 07:28:54 -0700 (PDT)
Return-Path: <glebowski@[redacted].net>
Received: from mail.u[redacted].net (24.Red-33-StaticIP.rima-tde.net. [80.73.140.73])
by mx.google.com with ESMTPS id qo7si25420802wjc.165.2014.10.15.07.28.53
for <[redacted]@gmail.com>
(version=TLSv1 cipher=ECDHE-RSA-AES128-SHA bits=128/128);
Wed, 15 Oct 2014 07:28:54 -0700 (PDT)
Received-SPF: pass (google.com: domain of [redacted] designates 80.73.140.73 as permitted sender) client-ip=80.73.140.73;
Authentication-Results: mx.google.com;
spf=pass (google.com: domain of glebowski@[redacted].net designates 80.73.140.73 as permitted sender) smtp.mail=glebowski@[redacted].net
Received: from ITTSRVMX03.[redacted] ([fe80::d13a:54f2:9933:a14f]) by
ITTSRVMX04.[redacted] ([fe80::2869:f02c:3d81:fc56%16]) with mapi id
14.01.0218.012; Wed, 15 Oct 2014 16:28:32 +0200
From: Gran Lebowski <glebowski@[redacted].net>
To: "[redacted]@gmail.com" <[redacted]@gmail.com>
Subject: Prueba2

```

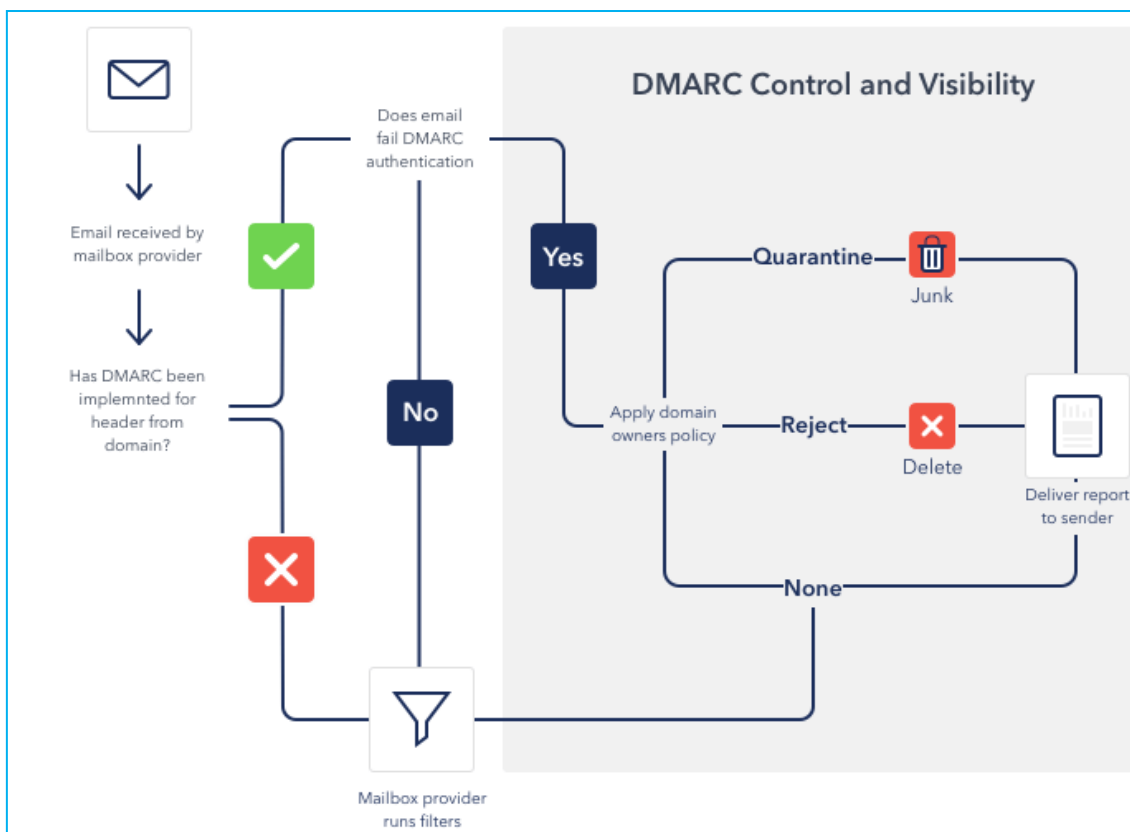
En la cabecera anterior, se indica el resultado SPF determinado por el servidor destinatario. Los posibles valores son los siguientes:

- ◆ **Pass:** Se ha verificado en el DNS que la IP consultada está autorizada para enviar correos electrónicos en nombre del dominio.
- ◆ **SoftFail / Fail:** Se ha verificado en el DNS que la IP consultada no está autorizada para enviar correos electrónicos en nombre del dominio.
- ◆ **Neutral:** No se ha podido verificar en el DNS que la IP consultada esté autorizada para enviar correos electrónicos en nombre del dominio. Puede deberse a que no se haya configurado ningún registro SPF o el DNS no esté autorizado para indicar dicha información.
- ◆ **None:** Este valor indica que no se ha configurado ningún registro SPF en el servidor DNS. Se comporta igual que Neutral.

## DMARC

La protección **DMARC** se encarga de indicar al servidor destinatario **qué hacer con el correo** si las valoraciones dadas por SPF y DKIM han determinado que el mensaje es una **suplantación de identidad**.

Por lo tanto, para que un mensaje sea validado por DMARC, debe pasar la autenticación SPF y/o la autenticación DKIM. En cambio, si ambas fallan, el mensaje será rechazado.



Con DMARC se indica al servidor que recibe el mensaje suplantado que debe hacer con él, es decir se debe configurar un registro DMARC en el DNS indicando **qué acción quiero que tome un servidor que reciba un correo suplantando mi identidad.**

```
_dmarc.onretrieval.es IN TXT "v=DMARC1; p=quarantine; sp=quarantine; rua=mailto:admin@onretrieval.es; adkim=r; aspf=r;"
```

**El parámetro clave es p.** Este define cómo quieres que el **servidor** receptor **gestione los mensajes sospechosos** que le llegan haciéndose pasar por tu dominio. Este campo puede estar compuesto por uno de los siguientes valores:

- ◆ **NONE:** Le indica al servidor que **no haga nada con el mensaje y siga sus propias políticas para determinar el destino del mismo.** Este es el valor por defecto.
- ◆ **QUARANTINE:** Le indica al servidor que marque los mensajes como spam y que los mantenga en cuarentena a la espera de seguir tratándolos. **También se enviaría notificación a la entidad suplantada.**
- ◆ **REJECT:** Le indica al servidor que rechace el correo, evitando que llegue al destinatario. **Al igual que los anteriores, se enviaría notificación a la entidad suplantada.**



## AUTHENTICATION RESULTS

Esta cabecera indica un **resumen** de las valoraciones dadas por el servidor final tras realizar las comprobaciones **SPF, DKIM Y DMARC**

Será en la misma donde nosotros, como analistas, podremos ver la valoración del protocolo DKIM.

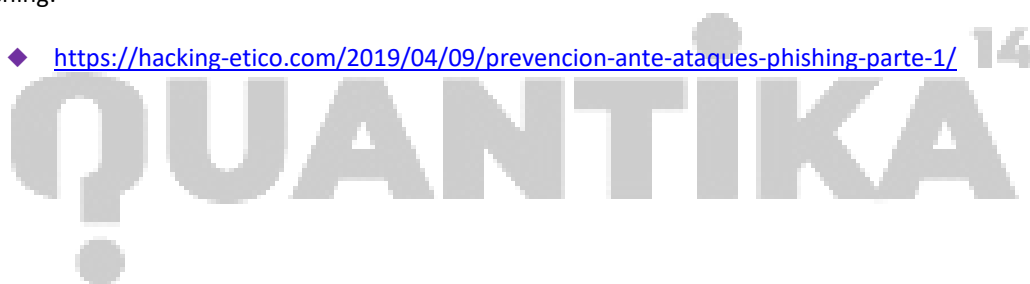
Los **valores** posibles de éste son los mismos que en el caso de SPF: **pass, neutral, fail, softfail** o **none**.

```
Authentication-Results:mx.google.com;  
spf=pass (google.com: domain of admin@onretrieval.es designates 194.57.88.211  
as permitted sender) smtp.mailfrom=admin@onretrieval.es;  
dkim=pass header.i=@onretrieval.es header.s=miclave header.b=54afea8b;  
dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=onretrieval.es
```

La cabecera **Authentication-Results** para el protocolo **DKIM** del ejemplo anterior, podemos ver que el receptor ha determinado que **el mensaje es auténtico e íntegro** debido a que el parámetro DKIM es igual a **pass**.

Una vez vistos todos estos campos, podemos poner en practica como poder detectar un caso de Phishing:

- ◆ <https://hacking-etico.com/2019/04/09/prevencion-ante-ataques-phishing-parte-1/>



## ¿DÓNDE PODEMOS ENCONTRAR MENSAJES DE CORREO ELECTRÓNICO?

Hoy en día, cuando estamos analizando un equipo informático con sistema operativo Windows podemos encontrarnos con las siguientes fuentes de información que contengan mensajes de correo electrónico.

### MICROSOFT OUTLOOK PST

El cliente de correo por excelencia de sistemas Windows, es Microsoft Outlook. Todos los mensajes enviados, recibidos, contactos y calendario se almacenan en un fichero PST.

Fichero almacenado por defecto:

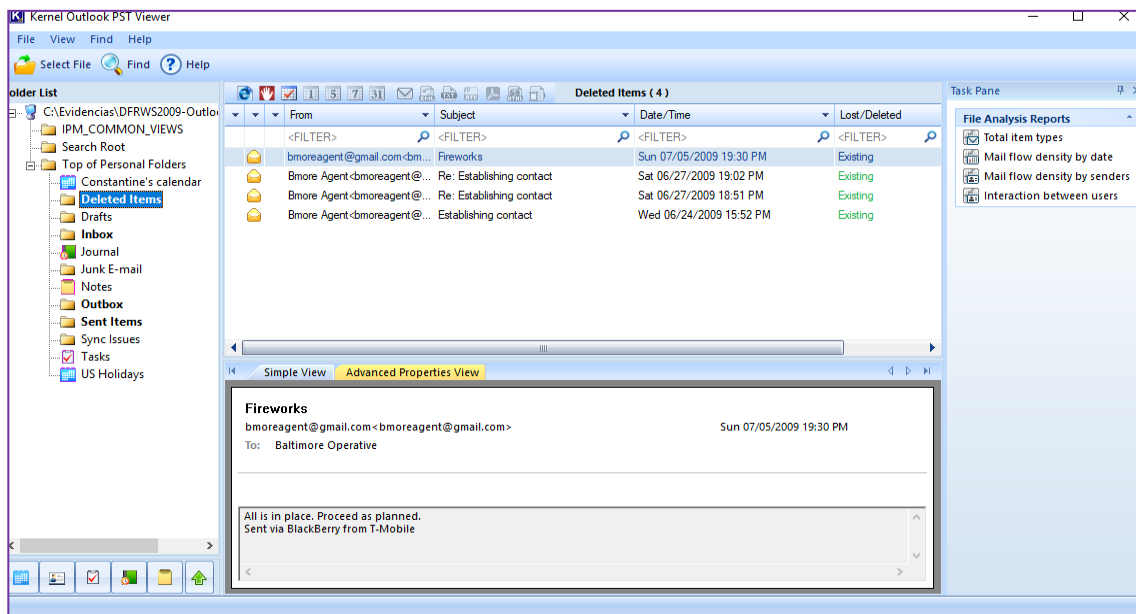
- ◆ %USERPROFILE%\Local Settings\Application Data\Microsoft\Outlook (WinXP y anteriores)
- ◆ %USERPROFILE%\AppData\Local\Microsoft\Outlook -> Win7 / Win8 y en adelante

La clave de registro nos puede indicar que archivos están siendo utilizados.

- ◆ HKEY\_CURRENT\_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook
- ◆ El Archivo tiene un tamaño máximo de 50 GB

Sino lo encontrásemos, deberíamos buscar por extensión o realizar técnica de recuperación de datos, ya que el fichero PST dispone de cabecera conocida. Se podría realizar mediante Photorec.

Herramienta para ver ficheros PST: **Kernel PST Viewer**



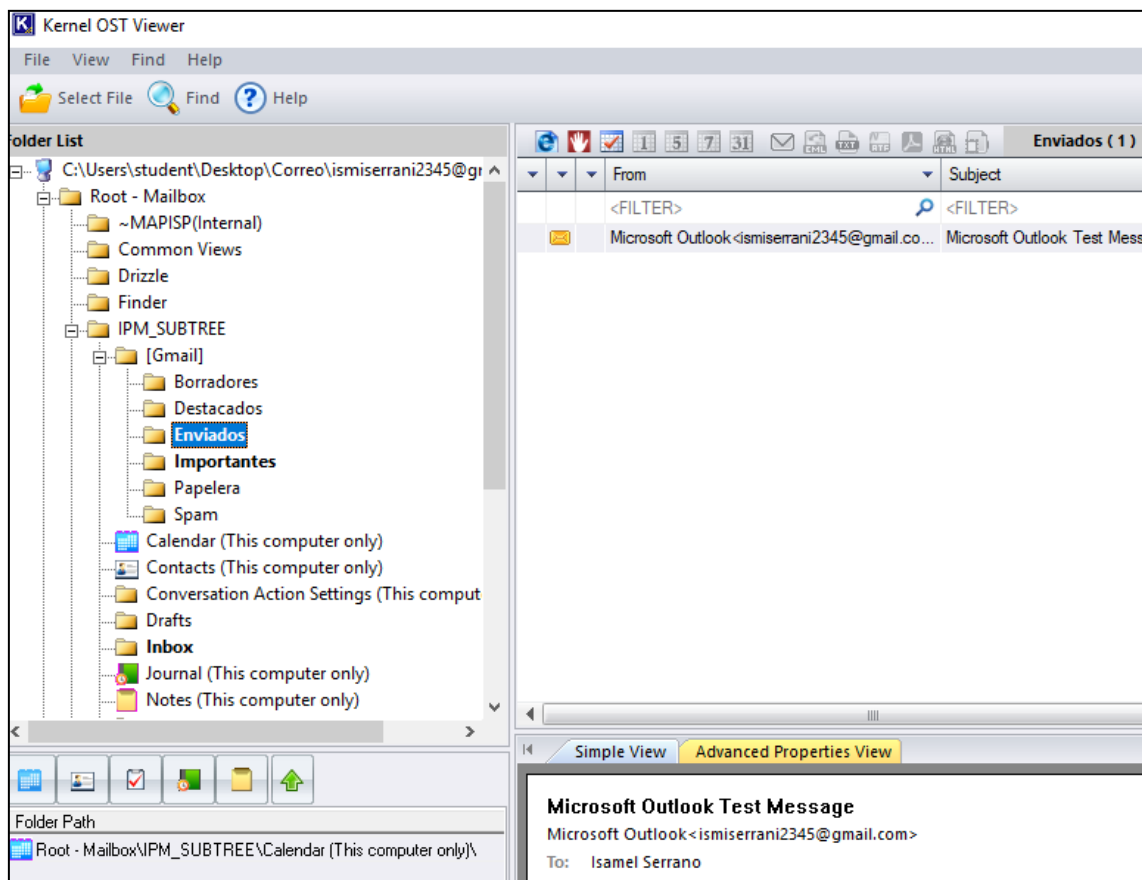
<https://www.nucleustechologies.com/download-outlook-pst-viewer.php>

## MICROSOFT OUTLOOK OST

Microsoft Outlook genera un fichero OST cuando la cuenta ha sido configurada mediante IMAP o mediante Exchange. Al igual que en PST, almacena mensajes enviados, recibidos, contactos, calendario. El buzón local (fichero OST) de mensajes es sincronizado con el servidor.

- ◆ Últimos 12 meses de email por defecto
- ◆ Fichero máximo de 50gb
- ◆ La ruta es la misma que el fichero PST
- ◆ Se puede realizar técnicas de carving para recuperarlo

### Herramienta: Kernel OST Viewer



*\*Ver video: 001 /MÓD. 5 - Kernel OST Viewer*

Hay que tener en cuenta que se puede recuperar un fichero OST/PST del sistema de archivos porque se haya borrado, o recuperar emails borrados de dentro del fichero OST/PST. En el caso de ficheros OST, existe una herramienta de pago: <https://www.kerneldatarecovery.com/ost-recovery.html>

## RECUPERACIÓN DE ADJUNTOS EN MICROSOFT OUTLOOK

Microsoft Outlook utiliza un directorio temporal seguro para abrir los adjuntos de los mensajes de correo electrónico:

- ◆ **%APPDATA%\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook -> IE10**
- ◆ **%APPDATA%\Local\Microsoft\InetCache\Content.Outlook -> IE11+**

Antes de la versión de Outlook 2007, los mensajes quedaban guardados siempre.

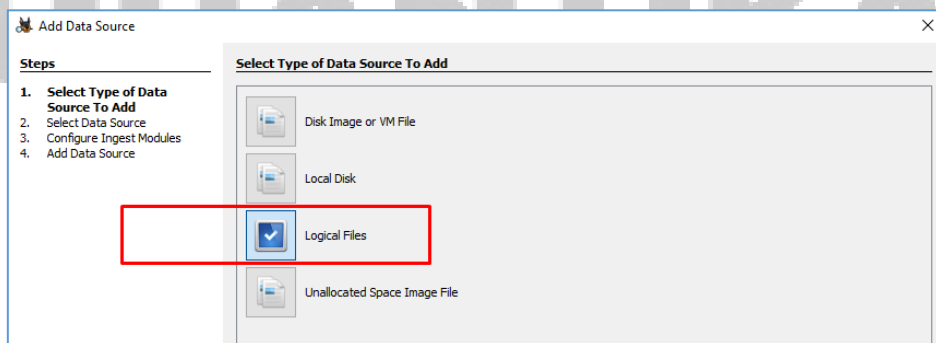
Después de la versión de Outlook 2007 en adelante, los adjuntos están, mientras que el correo electrónico este abierto o quedaría en esa carpeta si Outlook es cerrado correctamente.

## THUNDERBIRD MBOX

El cliente de correo Thunderbird almacena en la información en ficheros MBOX. Estos ficheros pueden ser encontrados en la siguiente ruta:

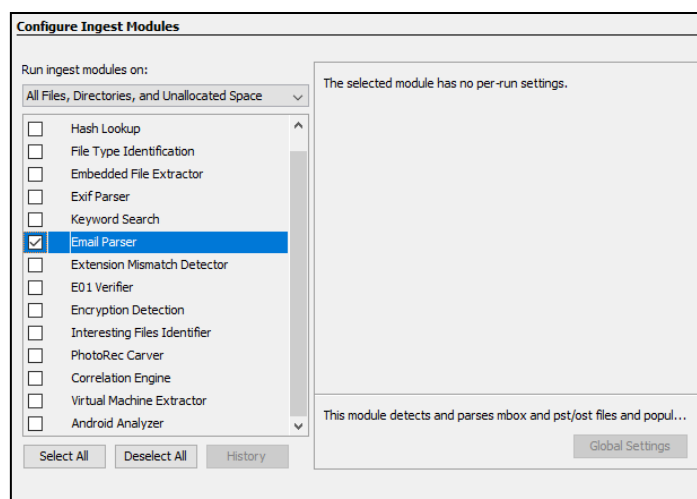
**\Users\%USERNAME%\AppData\Roaming\Thunderbird\Profiles**

Para poder leer este fichero MBOX sin la necesidad de Thunderbird podemos recurrir a Autopsy. Creamos un nuevo caso como hemos visto anteriormente, pero esta vez, en vez de añadir una imagen forense vamos a añadir un fichero, en este caso el fichero MBOX.

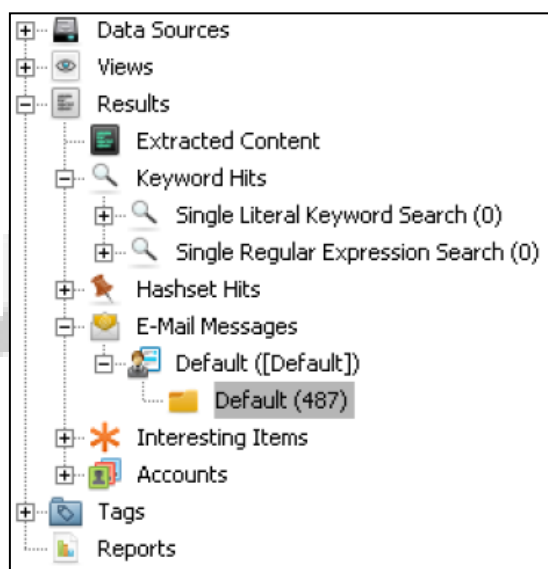


Después seleccionamos el “Email Parser” para que pueda extraer los emails contenidos en el fichero MBOX



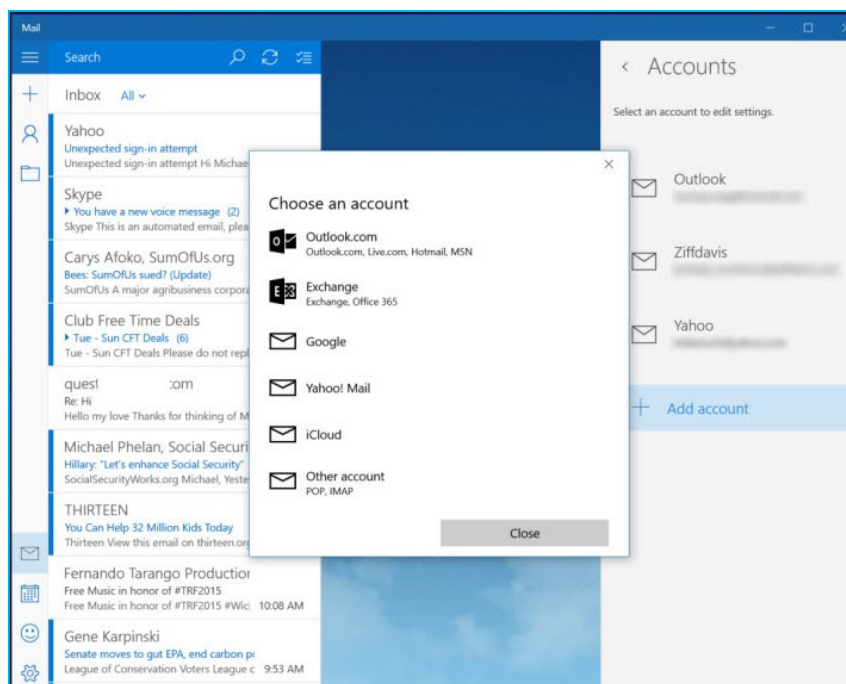


Este Modulo, es capaz también de leer ficheros PST y OST. Una vez que haya terminado de analizar el fichero MBOX podremos acceder a los correos en la siguiente sección:



## WINDOWS 10 MAIL APP

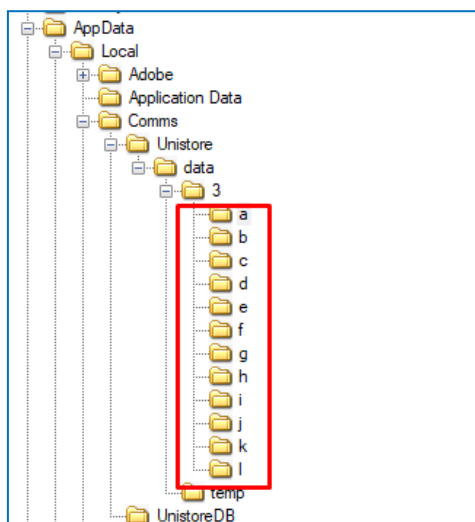
La aplicación de gestión de correo electrónico de Windows 10 que viene por defecto, también pudiese ser objeto de una investigación forense. Los mensajes de correo electrónico se almacenan en HTML o fichero de texto.



Otra característica de esta aplicación es que permite conectar múltiples cuentas de correo electrónico, como Gmail, Yahoo! y Outlook, tal y como vemos en la imagen anterior.

El cuerpo de los mensajes de correo electrónico se encuentra en la siguiente ruta:

◆ `\Users\{user_name}\AppData\Local\Comms\Unistore\data\3\`



Dentro de cada una de las subcarpetas están los correos electrónicos con extensión .dat

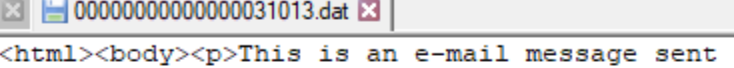
```

000 3C 00 68 00 74 00 6D 00-6C 00 3E 00 3C 00 62 00 <.h.t.m.l.>.<.b.
010 6F 00 64 00 79 00 3E 00-3C 00 70 00 3E 00 54 00 o.d.y.>.<.p>.T.
020 68 00 69 00 73 00 20 00-69 00 73 00 20 00 61 00 h.i.s. i.s. a.
030 6E 00 20 00 65 00 2D 00-6D 00 61 00 69 00 6C 00 n. e. m.a.i.l.
040 20 00 6D 00 65 00 73 00-73 00 61 00 67 00 65 00 .m.e.s.s.a.g.e.
050 20 00 73 00 65 00 6E 00-74 00 20 00 61 00 75 00 .s.e.n.t. a.u.
060 74 00 6F 00 6D 00 61 00-74 00 69 00 63 00 61 00 t.o.m.a.t.i.c.a.
070 6C 00 6C 00 79 00 20 00-62 00 79 00 20 00 4D 00 l.l.y. b.y. M.
080 69 00 63 00 72 00 6F 00-73 00 6F 00 66 00 74 00 i.c.r.o.s.o.f.t.
090 20 00 4F 00 75 00 74 00-6C 00 6F 00 6F 00 6B 00 .O.u.t.l.o.o.k.
0a0 20 00 77 00 68 00 69 00-6C 00 65 00 20 00 74 00 .w.h.i.l.e. t.
0b0 65 00 73 00 74 00 69 00-6E 00 67 00 20 00 74 00 e.s.t.i.n.g. t.
0c0 68 00 65 00 20 00 73 00-65 00 74 00 74 00 69 00 h.e. s.e.t.t.i.
0d0 6E 00 67 00 73 00 20 00-66 00 6F 00 72 00 20 00 n.g.s. f.o.r.
0e0 79 00 6F 00 75 00 72 00-20 00 61 00 63 00 63 00 y.o.u.r. a.c.c.
0f0 6F 00 75 00 6E 00 74 00-2E 00 0D 00 0A 00 3C 00 o.u.n.t.,...<.
100 2F 00 70 00 3E 00 3C 00-2F 00 62 00 6F 00 64 00 /p>.<./b.o.d.
110 79 00 3E 00 3C 00 2F 00-68 00 74 00 6D 00 6C 00 y>.<./h.t.m.l.
120 3E 00 >.

```

QUANTIKA

Podríamos exportarlos y visualizar con Notepad++:



The screenshot shows a Notepad window with two tabs. The first tab is titled 'new 1' and the second tab is titled '0000000000000000031013.dat'. The text in the Notepad window is as follows:

```

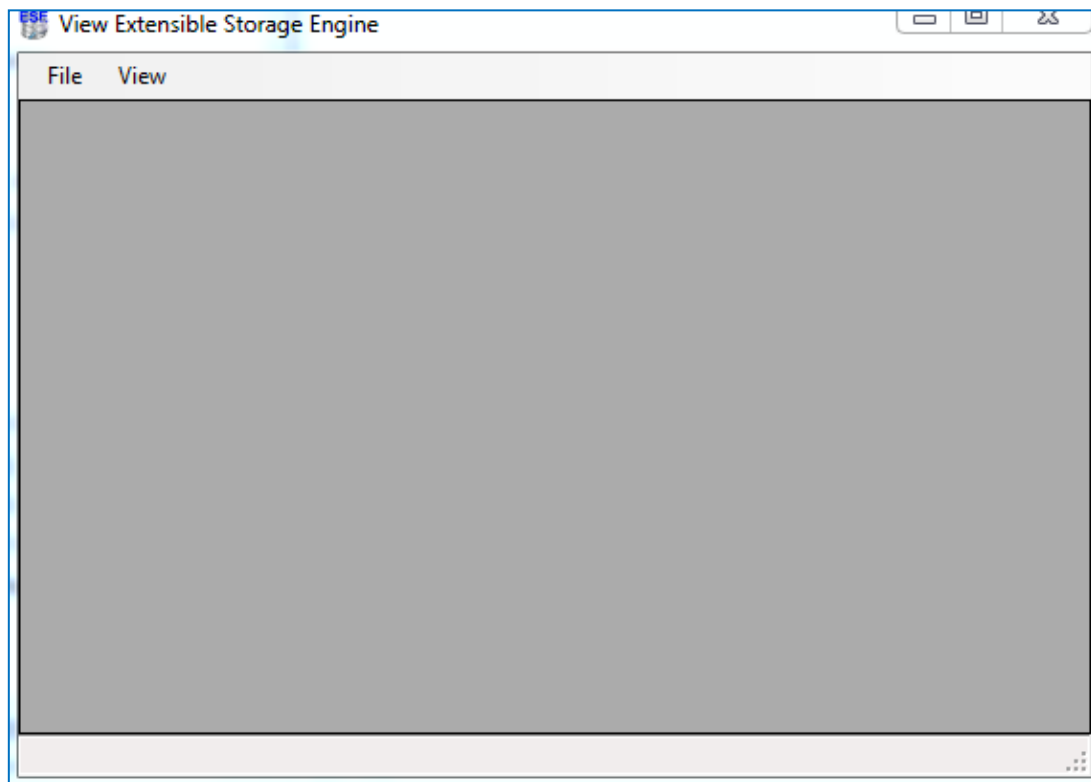
1  <html><body><p>This is an e-mail message sent
   automatically by Microsoft Outlook while testing the
   settings for your account.
2  </p></body></html>

```

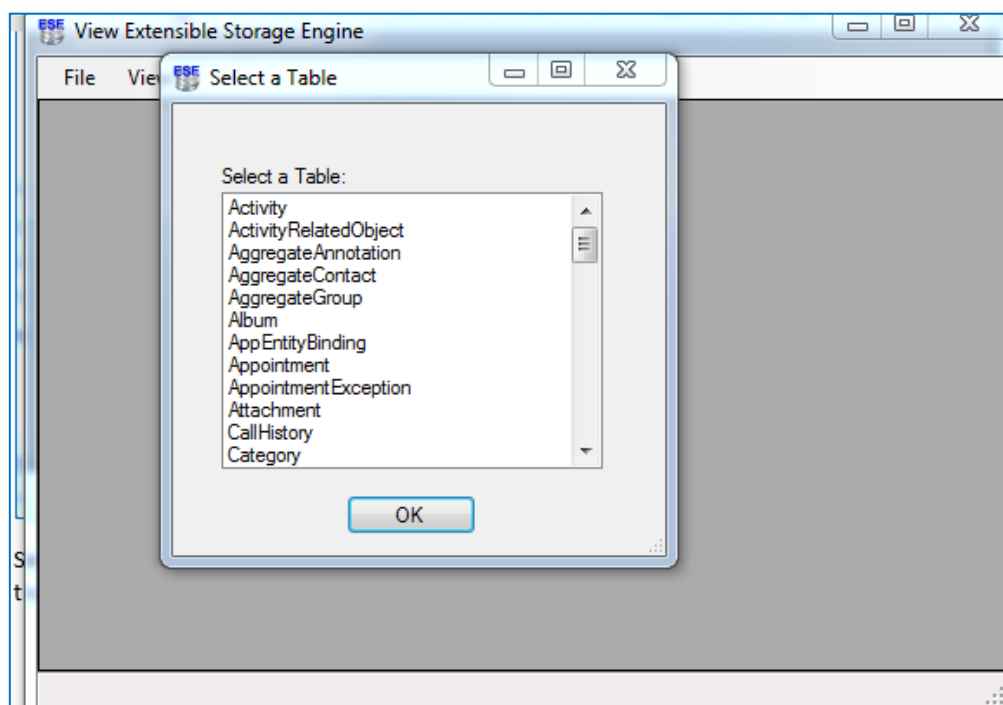
Los metadatos de los correos electrónicos, junto con los contactos se encuentra en la base de datos EDB:

- ◆ \Users\user\_name\AppData\Local\Comms\UnistoreDB\store.vol

Para poder visualizar esta base de datos, vamos a utilizar la herramienta ViewEse:



Seleccionamos la base de datos store.vol. Es necesario cambiarle la extensión a .EDB para que la aplicación pueda abrirlo. Una vez abierta nos va a pedir la tabla con la que queremos trabajar:



Seleccionamos la tabla "Message":

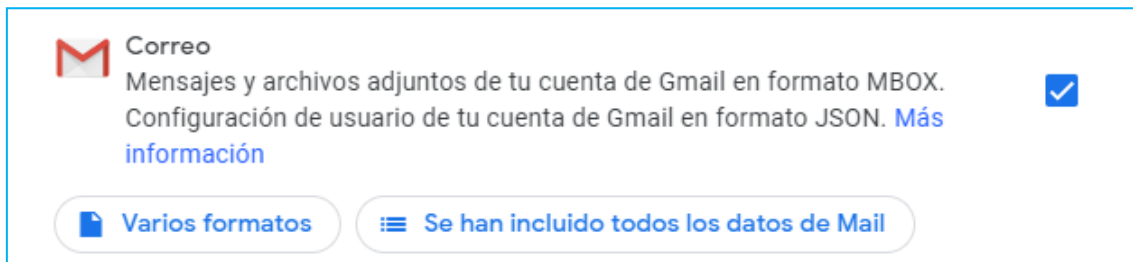
File	View		
	0c1f001f	0c1a001f	8279001f
►	"Microsoft Outlook" <ismiserrani2345@gmail.com>	Microsoft Outlook	ismiserrani2345@g
	"El equipo de la comunidad de Google" <googlecommunityteam-noreply@google.com>	El equipo de la comunidad de Google	googlecommunityte
	"Equipo de cuentas Microsoft" <account-security-noreply@accountprotection.microsoft.com>	Equipo de cuentas Microsoft	account-security-n
	"Microsoft OneDrive" <email@mail.onedrive.com>	Microsoft OneDrive	email@mail.onedri
	"Dropbox" <no-reply@dropbox.com>	Dropbox	no-reply@dropbox
	"Dropbox" <no-reply@dropbox.com>	Dropbox	no-reply@dropbox
	"Google" <no-reply@accounts.google.com>	Google	no-reply@account
	"Google" <no-reply@accounts.google.com>	Google	no-reply@account
	"Microsoft Outlook" <ismiserrani2345@gmail.com>	Microsoft Outlook	ismiserrani2345@g
	"Skype" <hello@email.skype.com>	Skype	hello@email.skype
	"Dropbox" <no-reply@dropboxmail.com>	Dropbox	no-reply@dropbox
	"Google" <no-reply@accounts.google.com>	Google	no-reply@account

Nos aparecen las cabeceras de los correos electrónicos.

## GOOGLE TAKEOUT

Google Takeout y Google Vault son comúnmente usadas para exportar la mensajería de correo electrónico para investigaciones forenses.

En el siguiente enlace podemos seleccionar que información queremos exportar de la cuenta Google:  
<https://takeout.google.com/settings/takeout?pli=1>



Como vemos, nos generará un fichero MBOX con todos los mensajes de correo electrónico sin tener opción a realizar búsquedas. De hecho, cuando Google termina la exportación del Takeout, avisa mediante un correo electrónico.

Google Vault, es la bóveda donde Google almacena toda la información de una cuenta de pago o GSUITE. En Google Vault si existe la posibilidad de exportar ciertos correos electrónicos. Google Vault viene incluido en GSUITE Business and Enterprise.

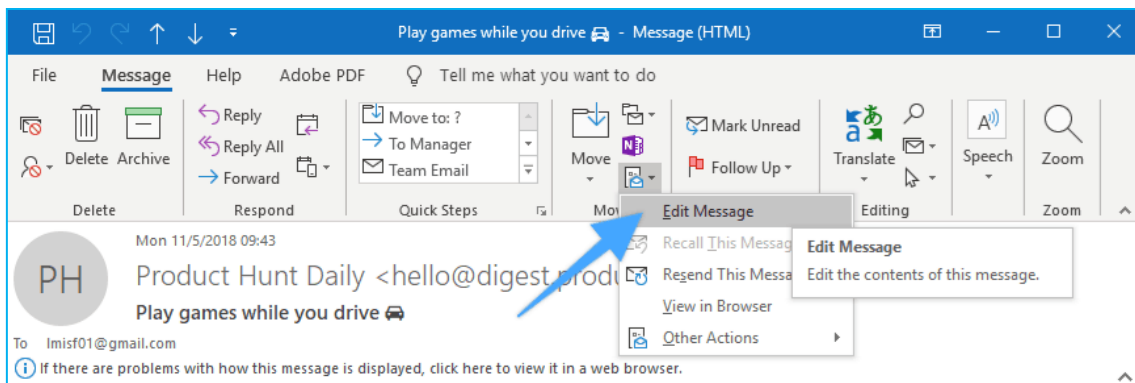
Google Vault proporciona un hash MD5 de los ficheros exportados, así como un indicar del tiempo de exportación.

Google ha introducido recientemente una característica de seguridad llamada "Confidential Mode" que impide buscar correos mediante la Api de Google pero si con Google Vault. Más información aquí:  
<https://protonmail.com/blog/gmail-confidential-mode-security-privacy/>

---

## MODIFICACIÓN DE MENSAJES DE GOOGLE

Aunque parezca mentira, se pueden modificar los mensajes de correo electrónico que hay en el propio de servidor de Gmail. Para ello el "atacante" o persona que vaya a modificar un mensaje de GMAIL, debe conectar el cliente de correo Microsoft Outlook mediante IMAP a una cuenta de correo de GMAIL.



Como vemos en la anterior imagen, una vez que tengamos sincronizado el buzón de correo de Gmail en nuestro Outlook, podremos realizar los cambios dándole a “Editar Mensaje” y después guardarlo.

### ¿Cómo podríamos identificarlo?

- ◆ Existe una cabecera llamada UID (Unique Identifier) dentro del protocolo IMAP. Si hemos descargado el buzón entero podremos ver los UID de los mensajes que sean temporalmente cercanos a dicho mensaje. Si identificamos, que el UID de ese mensaje en cuestión tiene un salto muy gradual respecto a los mensajes de correo electrónico cercanos, estamos ante una posible modificación del mensaje.
- ◆ Cuando se produce la modificación del mensaje, se cambia o añade el campo X-Mailer por el programa que ha realizado la modificación, en este Microsoft Outlook. Debiese ser comparados con varios mensajes de la misma dirección si es normal que envíe desde X-Mailer o no.
- ◆ Se añade un delimitador MIME donde aparece el momento exacto de la modificación realizada en formato FILETIME

## MICROSOFT EXCHANGE

La mayoría de los entornos corporativos utilizan servidores de correo dedicados o en cloud. Un servicio de correo electrónico dedicado es Exchange.

Exchange 2007 y superiores utilizan el formato .EDB (Extensible Storage Format), donde se almacena el correo electrónico, los adjuntos, los contactos, las notas, las tareas, el calendario e incluso la libreta de direcciones. Los ficheros .log que hay alrededor de una base de datos EDB, son mensajes que todavía no han sido escritos a la propia base de datos. La base de datos EDB

### Versión de Exchange Server 2019 and 2016

- C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database Name.edb

### Versión de Exchange Server 2013

- C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox database Name\Mailbox database Name.edb

### Versión de Exchange 2010

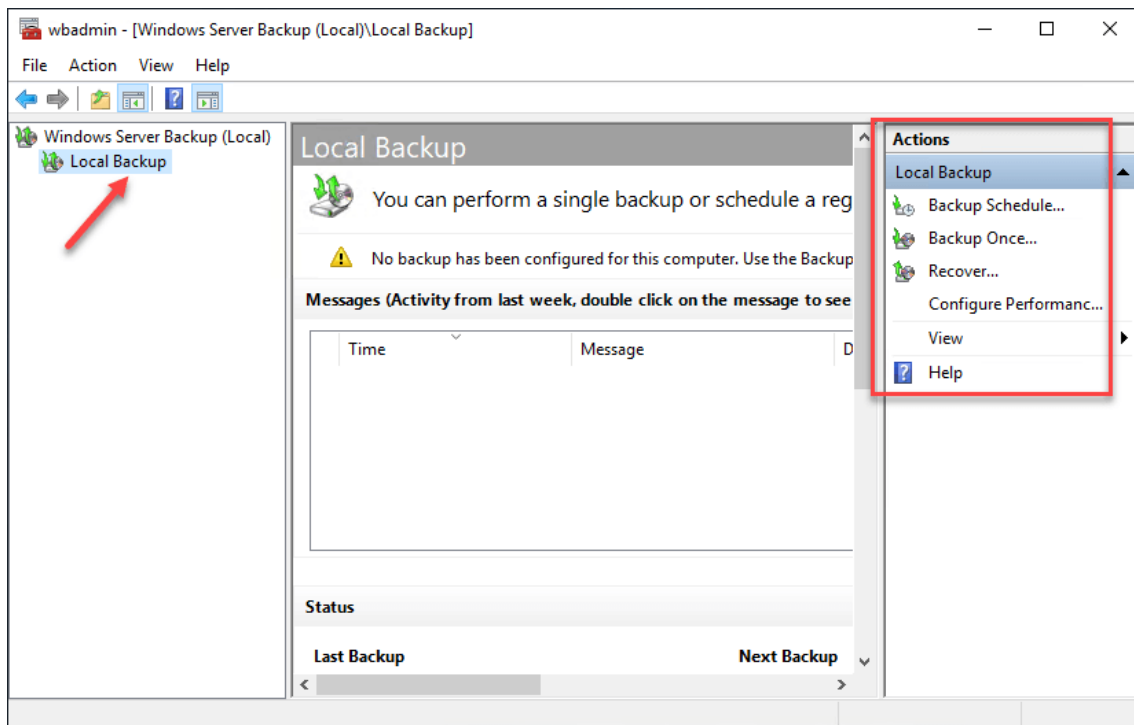
- C:\Program Files\Microsoft\Exchange Server\V14\Mailbox Database\Mailbox Database.edb

Exchange dispone una carpeta por cada usuario llamada "Recoverable Items" que tiene como objetivo proteger de borrados accidentales o maliciosos y que permita su recuperación inmediata. ¿Qué hay dentro de esta carpeta?

- Deleted item retention
- Single item recovery
- In-Place Hold
- Litigation Hold
- Mailbox audit logging
- Calendar logging

Por defecto hay 14 días desde que se produce el borrado para se pueda recuperar la información sin problemas.

Tenemos dos opciones para afrontar una investigación, hacer una imagen forense del mismo para poder obtener la base de datos EDB y sus correspondientes carpetas o podríamos utilizar una herramienta que viene por defecto a partir de Windows 2008: **Windows Server Backup (wbadmin.msc)**



Los backups generados por esta herramienta, generan contenedores VHD. Todos los pasos de como realizar esta copia de seguridad, en el siguiente enlace:

<https://www.solvetic.com/tutoriales/article/2612-windows-server-backup-copia-de-seguridad-y-restaurar/>

Otra opción sería exportar los buzones que se desean investigar a ficheros PST. El proceso paso de como realizarlo podemos encontrarlo en el siguiente enlace:

<https://docs.microsoft.com/es-es/exchange/recipients/mailbox-import-and-export/export-procedures?view=exchserver-2019>

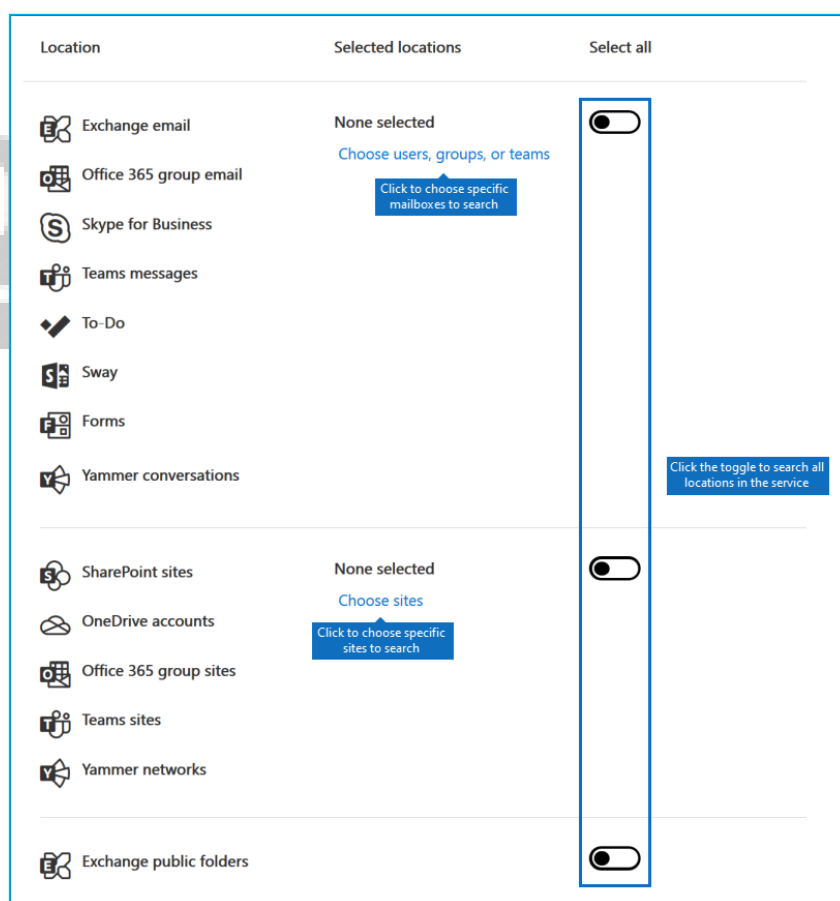


## OFFICE365

Office365 es una herramienta que nos permite crear, acceder y compartir documentos de Word, Excel, OneNote y PowerPoint. En este sentido no presenta cambios con un paquete Office normal, pero la diferencia está en que puedes acceder a todos los programas en tiempo real. Además, podemos acceder desde cualquier dispositivo que tenga acceso a Internet y OneDrive, y también dispone de la aplicación Outlook para mensajería de correo electrónico.

Office365 dispone de una herramienta de eDiscovery que permite hacer búsquedas sobre las siguientes fuentes de información:

- Buzones de Exchange Online y carpetas públicas
- Sitios de SharePoint Online y cuentas de OneDrive para la Empresa
- Conversaciones de Skype Empresarial
- Microsoft Teams
- Grupos de Microsoft 365
- Grupos de Yammer



En el siguiente enlace se explica el procedimiento a seguir para realizar este tipo de búsquedas.

<https://docs.microsoft.com/es-es/microsoft-365/compliance/content-search?view=o365-worldwide>

Office365 también dispone de la opción de exportar a ficheros PST mediante el proceso de búsqueda de “Content Search” tal y como se explica aquí:

<https://docs.microsoft.com/es-es/microsoft-365/compliance/export-search-results?view=o365-worldwide>

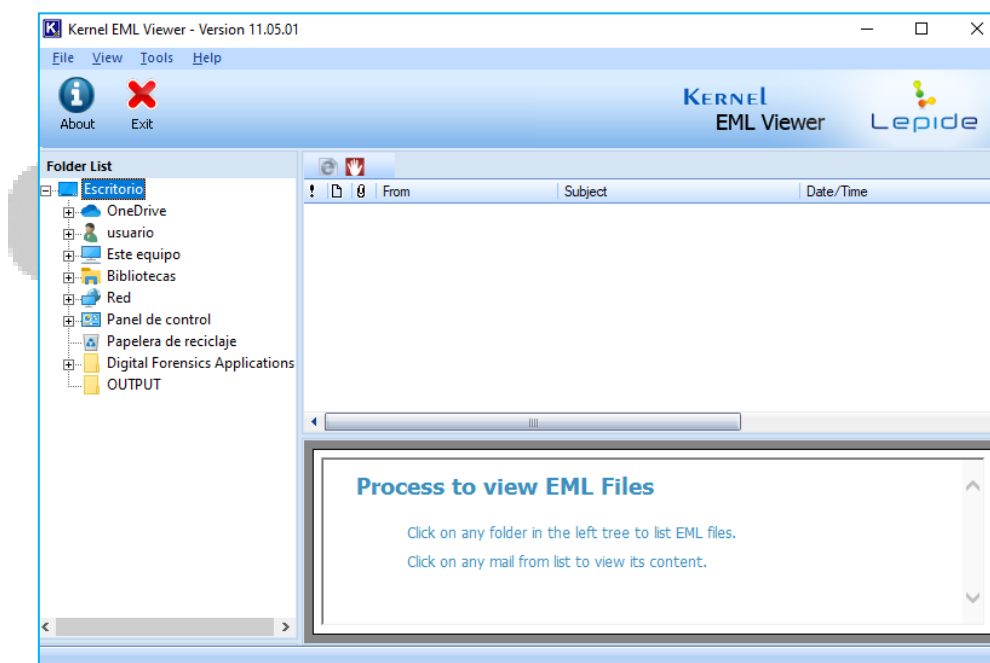
Por defecto la auditoria no esta habilitada en Office365, su periodo máximo de retención es de 90 días. Para habilitar es necesario hacerlo usuario por usuario. En el siguiente enlace se explica (en inglés) los pasos a realizar para habilitar la auditoria:

<https://support.microsoft.com/es-es/office/auditing-in-office-365-for-admins-9f6484d2-0fd2-17de-165f-c41346023906>

## HERRAMIENTAS

### KERNEL EML VIEWER

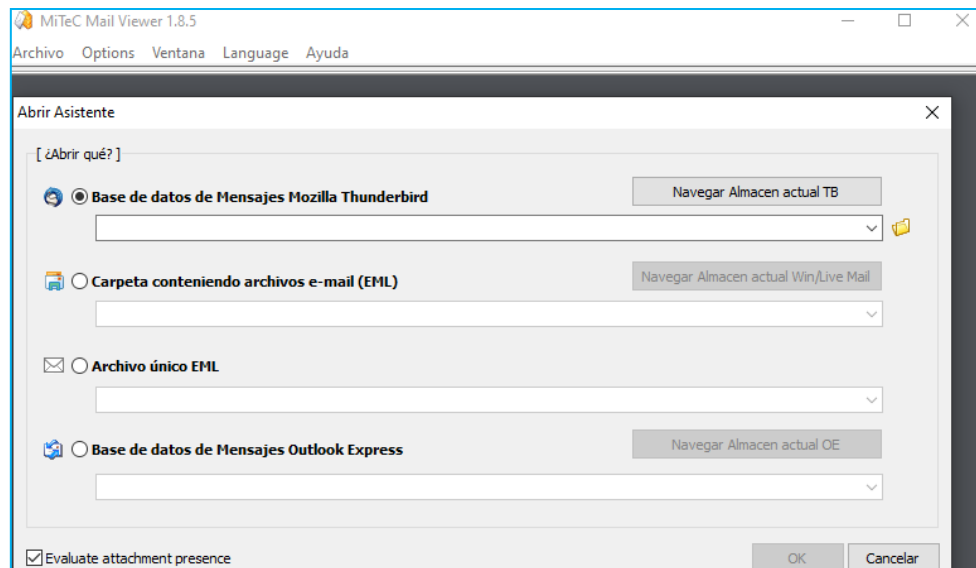
Es un visor de mensajes de correo electrónico en formato EML gratuito.



<https://www.nucleustechologies.com/eml-viewer.html>

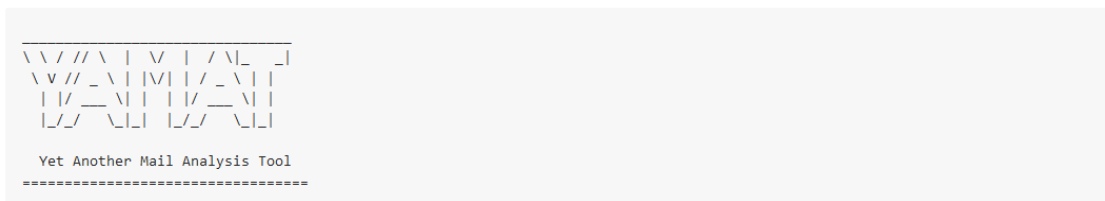
### MITEC MAIL VIEWER

Visor EML, y formato MBOX de Thunderbird



<http://www.mitec.cz/Downloads/MailView.zip>

## YET ANOTHER MAIL ANALYSIS TOOL (YAMAT)



## Yet Another Mail Analysis Tool

There several tools to analyze email headers and body, some of them analyses the headers, other does body analysis by extracting indicator of compromise. But, there is not a tool that do all in one. YAMAT pretends to be the tool that includes all that a cybersecurity analyst needs when analysing emails.

Es una herramienta escrita en GO que analizar correos de manera masiva, cuyo objetivo es obtener:

- ◆ Extraer los indicadores de compromiso
- ◆ Mostrar las cabeceras estandar y no estándar
- ◆ Mostrar información del adjutno
- ◆ Mostrar la version de texto y la versión HTML
- ◆ Realizar una comprobación en VirusTotal de la url y del adjunto
- ◆ Extraer el adjunto

<https://dev.jau.me/Xumeiquer/YAMAT/>

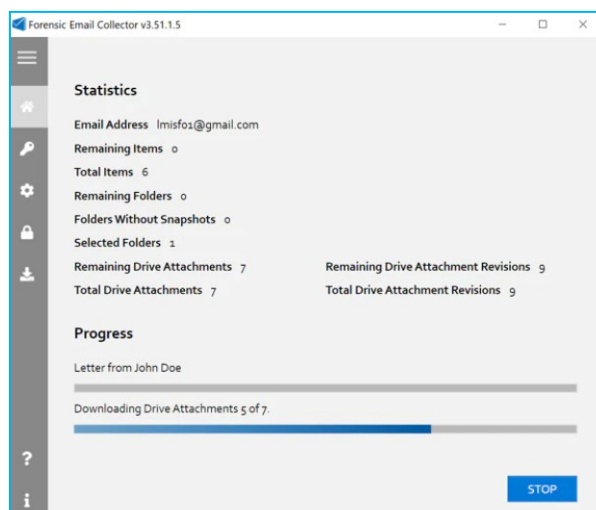
## MEIOC

Es muy parecida a YAMAT pero escrita en Python3 y hace comprobaciones de SPF

<https://github.com/drego85/meioc>

## FORENSIC EMAIL COLLECTOR

Esta herramienta es un recolector de buzones, es decir, imaginemos que no tenemos el buzón de correo dentro de nuestro sistema Windows, sino que está en los servidores de Google, Exchange, Office365 o IMAP. Gracias a esta herramienta, podremos hacer una adquisición que forensicamente hablando, mantenga las propiedades originales y que no sean convertidas.



<https://www.metaspike.com/shop/forensic-email-collector/>

## EMAILREP.IO

Esta herramienta, es gratuita y se puede utilizar de manera online accediendo a la siguiente dirección:

<https://emailrep.io/>


Una vez dentro podrás consultar la reputación de una cuenta de correo electrónico basado en el historial de la misma, es decir, que no haya estado involucrada en incidentes de seguridad, que disponga de cuentas legítimas, etc.

### Simple Email Reputation

Una vez insertado el correo electrónico se obtiene el siguiente informe:

# RISKY

Suspicious. We have not observed this email address on the internet, it is a free provider, and it has no profiles on major services like LinkedIn, Facebook, and iCloud. A lack of digital presence may simply indicate a new email address, but is typically suspicious.

SHARE 

```
curl emailrep.io/ismiserrani2345@gmail.com
{
  "email": "ismiserrani2345@gmail.com",
  "reputation": "none",
  "suspicious": true,
  "references": 0,
  "details": {
    "blacklisted": false,
    "malicious_activity": false,
    "malicious_activity_recent": false,
    "credentials_leaked": false,
    "credentials_leaked_recent": false,
    "data_breach": false,
    "first_seen": "never",
    "last_seen": "never",
    "domain_exists": true,
    "domain_reputation": "n/a",
    "new_domain": false,
    "days_since_domain_creation": 9220.
```

También podemos instalar esta herramienta dentro de nuestros servidores gracias al Código fuente en el siguiente enlace:

<https://github.com/sublime-security/emailrep.io>

