

Práctica 1

Análisis forense de correo electrónico

Jose Almirón López

19 de Mayo del 2024

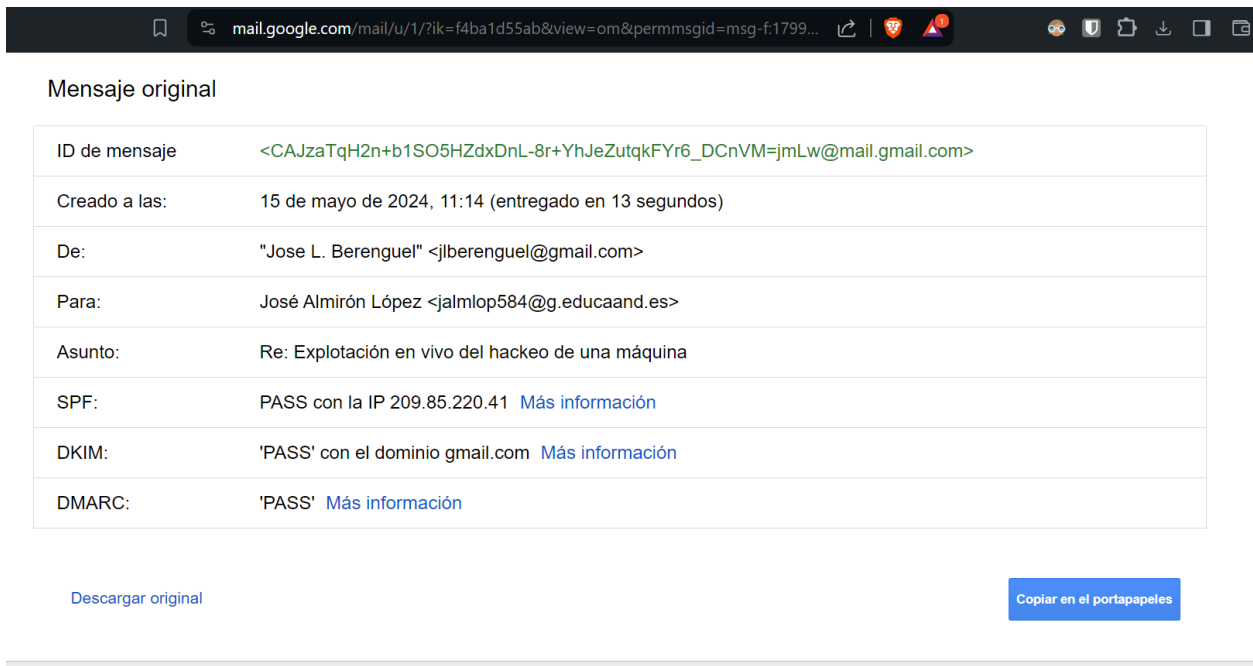


Tabla de contenidos

Familiarización con las cabeceras de los correos electrónicos.	3
Cabeceras del Correo	5
Autenticación del Correo	5
Spoofing	7
Instalar los clientes de correo electrónico más utilizados	10
Mozilla Thunderbird	10
Outlook	12
Herramientas para la Extracción de Evidencias en Thunderbird	13

Familiarización con las cabeceras de los correos electrónicos.

Para familiarizarnos con las cabeceras de los correos electrónicos, lo primero que haremos será seleccionar un correo de nuestro servicio de correo electrónico. En mi caso, seleccionaré Gmail. Una vez que tengamos el correo abierto, pulsamos sobre los tres puntos verticales (más opciones) que se encuentran en la esquina superior derecha del mensaje. Esto desplegará un menú. Si nos dirigimos a la opción "Mostrar original", podremos ver el formato completo del correo, incluyendo las cabeceras y toda la información detallada del mensaje.



The screenshot shows a web browser window displaying the 'Show original' view of an email in Gmail. The browser's address bar shows the URL: mail.google.com/mail/u/1/?ik=f4ba1d55ab&view=om&permmsgid=msg-f:1799... Below the browser window, the text 'Mensaje original' is displayed. Underneath this, a table lists the email's headers. The headers include: ID de mensaje (a long alphanumeric string), Creado a las (15 de mayo de 2024, 11:14), De (Jose L. Berenguel), Para (José Almirón López), Asunto (Re: Explotación en vivo del hackeo de una máquina), SPF (PASS), DKIM (PASS), and DMARC (PASS). At the bottom of the screenshot, there are two buttons: 'Descargar original' and 'Copiar en el portapapeles'.

Mensaje original	
ID de mensaje	<CAJzaTqH2n+b1SO5HZdxDnL-8r+YhJeZutqkFYr6_DCnVM=jmLw@mail.gmail.com>
Creado a las:	15 de mayo de 2024, 11:14 (entregado en 13 segundos)
De:	"Jose L. Berenguel" <jlberenguel@gmail.com>
Para:	José Almirón López <jalmlop584@g.educaand.es>
Asunto:	Re: Explotación en vivo del hackeo de una máquina
SPF:	PASS con la IP 209.85.220.41 Más información
DKIM:	'PASS' con el dominio gmail.com Más información
DMARC:	'PASS' Más información

[Descargar original](#) [Copiar en el portapapeles](#)

Delivered-To: jalmlop584@g.educaand.es
 Received: by 2002:ab0:3b4c:0:b0:7f1:30b3:1f11 with SMTP id o12csp3258340uaw;
 Wed, 15 May 2024 02:14:58 -0700 (PDT)
 X-Received: by 2002:a17:906:da8b:b0:a59:bdb7:73f8 with SMTP id a640c23a62f3a-a5a2d66a3b4mr1350918566b.47.1715764498578;
 Wed, 15 May 2024 02:14:58 -0700 (PDT)
 ARC-Seal: i=1; a=rsa-sha256; t=1715764498; cv=none;
 d=google.com; s=arc-20160816;
 b=yNH+Q0Msqyji8/Dq0DkMI8YPueF60NFLptWcZ71JiEiLvWvT67Lv890W89ZCWCzd9Ic
 V56Chr/wDVPion+MtF/Z0Cud5f5oF6oAAIze7QRT0EyBPpAqxGBkAIXxU8HF0Ce+yGhs
 3+qZH2GpzQNN/V7ICJ+/bv0zh/OpXcc1VLnVivj8qqsioOzo6IgIDMb16xwqEUMdt8XA
 7iyUE6CLPGnLXr/OSg5hn4v7s1htxIqcJM1Id87urJRkdyKti2i98XjQVI/4VcPy8nXr
 Ws00fy7kWL05IXMb0/uSQTSYm7/xpOM4xocMNkbDULU/6D3EKvpZNwJG2QS4Kmtu039
 3IAQ==
 ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
 h=to:subject:message-id:date:from:in-reply-to:references:mime-version
 :dkim-signature;
 bh=yp7612PnoyXXX6xWodSXumJe69DfLin0UAFW5NCPFcc=;
 fh=KgtbjyvkqHhYmiQKjKOjd8Jv5o9rawhacSVLr3RhwE0=;
 b=12zXtawa37RrCJ87X8PHx6V1pUAhGqZ+E0SZkc6hItffPUXGr+mQ3qNnIgL4Ih8lpZ
 wZmRnFovxIIEzLZheKI+vJrKTKrOyLbZ1x9/8j11mb7HkC4MjzdUb97kelngNemgaVn2
 khmCwYxkUiwuNkVsDU2hus0uKdNeAKyM+Gr8FWhL9Rzc6u+t3lDKM9taYBmyinyD4m9V
 EEzOPGMJDCL2AP9z8L0yMONUGiLZxs3ftV/hDTNXV68bdZ2DpnvJNirNVNuIi36HxP
 huY24q4LnustPsat9CQ9aLAceyxwajMZC3kpFgX9Bu9Fdf0YvT+0GB711XVXhQ6ACp0z
 Z51A==;
 dara=google.com
 ARC-Authentication-Results: i=1; mx.google.com;
 dkim=pass header.i=@gmail.com header.s=20230601 header.b=EXWlW4MV;
 spf=pass (google.com: domain of jlberenguel@gmail.com designates 209.85.220.41 as permitted sender)
 smtp.mailfrom=jlberenguel@gmail.com;
 dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
 Return-Path: <jlberenguel@gmail.com>
 Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
 by mx.google.com with SMTPS id a640c23a62f3a-a5a1796de1fsor388492966b.7.2024.05.15.02.14.58
 for <jalmlop584@g.educaand.es>
 (Google Transport Security);
 Wed, 15 May 2024 02:14:58 -0700 (PDT)
 Received-SPF: pass (google.com: domain of jlberenguel@gmail.com designates 209.85.220.41 as permitted sender) client-
 ip=209.85.220.41;
 Authentication-Results: mx.google.com;

Vamos a copiar el formato completo del correo electrónico y usar las herramientas de Google para analizar las cabeceras.

Caja de herramientas de Google Admin Messageheader

Ayuda

MessageId	CAJzaTqH2n+b1SO5HZdxDnL-8r+YhJeZutqkFYr6_DCNVM=jmLw@mail.gmail.com
Created at:	15/5/2024, 11:14:45 CEST (Delivered after 13 sec)
From:	"Jose L. Berenguel" <jlberenguel@gmail.com>
To:	"José Almirón López" <jalmlop584@g.educaand.es>
Subject:	Re: Explotación en vivo del hackeo de una máquina
SPF:	pass con la IP 209.85.220.41 Más información
DKIM:	pass con el dominio gmail.com Más información
DMARC:	pass Más información

Cabeceras del Correo

- **Message-ID:** Este es un identificador único asignado al correo electrónico por el servidor de envío. Sirve para rastrear y referenciar el correo.
- **Created at:** Fecha y hora en que el correo fue creado y enviado, en el huso horario CEST (Central European Summer Time). El correo fue entregado 13 segundos después de ser enviado.
- **From:** Dirección de correo electrónico y nombre del remitente del mensaje.
- **To:** Dirección de correo electrónico y nombre del destinatario del mensaje.
- **Subject: Re:** Asunto del correo, indicando que es una respuesta a un correo previo sobre la explotación en vivo del hackeo de una máquina.

Autenticación del Correo

- **SPF (Sender Policy Framework):** El correo pasó la verificación SPF, lo que indica que fue enviado desde una dirección IP (209.85.220.41) autorizada a enviar correos en nombre del dominio del remitente (gmail.com).
- **DKIM (DomainKeys Identified Mail):** El correo pasó la verificación DKIM, confirmando que el mensaje no fue alterado y que proviene del dominio gmail.com.
- **DMARC (Domain-based Message Authentication, Reporting & Conformance):** El correo pasó la verificación DMARC, lo que significa que tanto SPF como DKIM fueron verificados correctamente y el mensaje cumple con la política de autenticación del dominio del remitente.

Ahora veremos cómo comprobar la información DKIM de las cabeceras. Lo primero que haremos será buscar el selector. Este parámetro lo encontraremos buscando por "DKIM-Signature". En este caso, el valor que indica el selector es "**s=20230601**".

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
d=gmail.com; s=20230601; t=1715764498; x=1716369298; darn=g.educaand.es;  
h=to:subject:message-id:date:from:in-reply-to:references:mime-version  
:from:to:cc:subject:date:message-id:reply-to;  
bh=yp7612PnoyXXX6xWodSXumJe69DfLIIn0UAFW5NCPFcc=;  
b=EXWlW4MVi9arGMC2ixVKLFK/k4npLnApwDVAYdUMB/hoYfUxWAjaZrCW8ZzzHYx8Je  
l70nnpYh0fa90KdYnH0iD17cGav57f7SCuCRtphbDaeioMEa9D7DexbD32Fch/hV7wh
```

El dominio también lo encontramos en la misma captura, justo antes del selector. Comienza con "d=" y en este caso es "gmail.com".

Check a published DKIM Core Key

Selector:

Domain name:

Enter the selector and domain you have published keys for and press the button.

Check a DKIM Core Key Record

Key record:

Si ingresamos el selector y el dominio en la página dkimcore.org, nos proporcionará la clave pública correspondiente.

Spoofing

Podemos emplear herramientas como la ofrecida por emkei.cz para usurpar la identidad de alguien y enviar correos electrónicos en su nombre.



Free online fake mailer with attachments, encryption,
HTML editor and advanced settings...

From Name:

From E-mail:


To:

Subject:

Attachment: Ningún archivo seleccionado
[Attach another file](#)

Content-Type: ☒ text/plain ☐ text/html ☐ Editor

Text:

Captcha: ☒ I am human  hCaptcha
Privacy - Terms

Las herramientas para evitar correos electrónicos fraudulentos incluyen filtros de spam y sistemas de seguridad de los proveedores de correo, que usan algoritmos y listas negras. Además, se emplean medidas de autenticación como SPF, DKIM y DMARC para verificar la autenticidad del remitente y reducir la suplantación de identidad.

EMKEE'S MAILER

Free online fake mailer with attachments, encryption,
HTML editor and advanced settings...

✓ E-mail sent successfully

From Name: Bill Gates

From E-mail: billgates@microsoft.com


To: 0fUWA1Hc5Wkl89@dkimvalidator.com

Subject: asunto

Attachment: Ningún archivo seleccionado
[Attach another file](#)

Content-Type: ☒ text/plain ☐ text/html ☐ Editor

Text: Viva Apple

Captcha: ☒ I am human  hCaptcha
Privacy - Terms

Como podemos observar, intentamos nuevamente enviar un correo fraudulento, pero esta vez utilizando otro servicio. En lugar de Gmail, estamos usando dkimvalidator.com, donde efectivamente lo recibimos y podemos analizar el correo.


Email Validation Results

Address:

0fuwa1hc5wkl89@dkimvalidator.com

Original Message:

```
Received: from emkei.cz (emkei.cz [114.29.236.247])  
    by relay-7.us-west-2.relay-prod (Postfix) with ESMTPS id 014A1259C2  
    for <0fuwa1hc5wkl89@dkimvalidator.com>; Mon, 20 May 2024 07:06:21 +0000  
(UTC)  
Received: by emkei.cz (Postfix, from userid 33)  
    id 65AE6191C; Mon, 20 May 2024 09:06:19 +0200 (CEST)  
To: 0fuwa1hc5wkl89@dkimvalidator.com  
Subject: asuntito  
From: "Bill Gates" <billgates@microsoft.com>  
X-Priority: 3 (Normal)  
Importance: Normal  
Errors-To: billgates@microsoft.com  
Reply-To: billgates@microsoft.com  
Content-Type: text/plain; charset=utf-8  
Message-Id: <20240520070619.65AE6191C@emkei.cz>  
Date: Mon, 20 May 2024 09:06:19 +0200 (CEST)  
  
Viva Apple
```



He llegado a la conclusión de que las tecnologías SPF, DKIM y DMARC desempeñan un papel crucial en la prevención del spoofing de correos electrónicos.

- **SPF (Sender Policy Framework):** Permite a los dominios especificar qué servidores de correo tienen permiso para enviar correos en su nombre. Esto ayuda a evitar que remitentes no autorizados envíen correos falsificados desde ese dominio.
- **DKIM (DomainKeys Identified Mail):** Añade una firma digital a los correos electrónicos, lo que permite al receptor verificar que el correo no ha sido alterado y que proviene del dominio que afirma ser el remitente.
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance):** Utiliza los mecanismos de SPF y DKIM para proporcionar instrucciones a los servidores de correo sobre cómo manejar los correos que no superan las verificaciones de autenticidad, además de ofrecer un informe sobre la actividad de los correos electrónicos en el dominio.

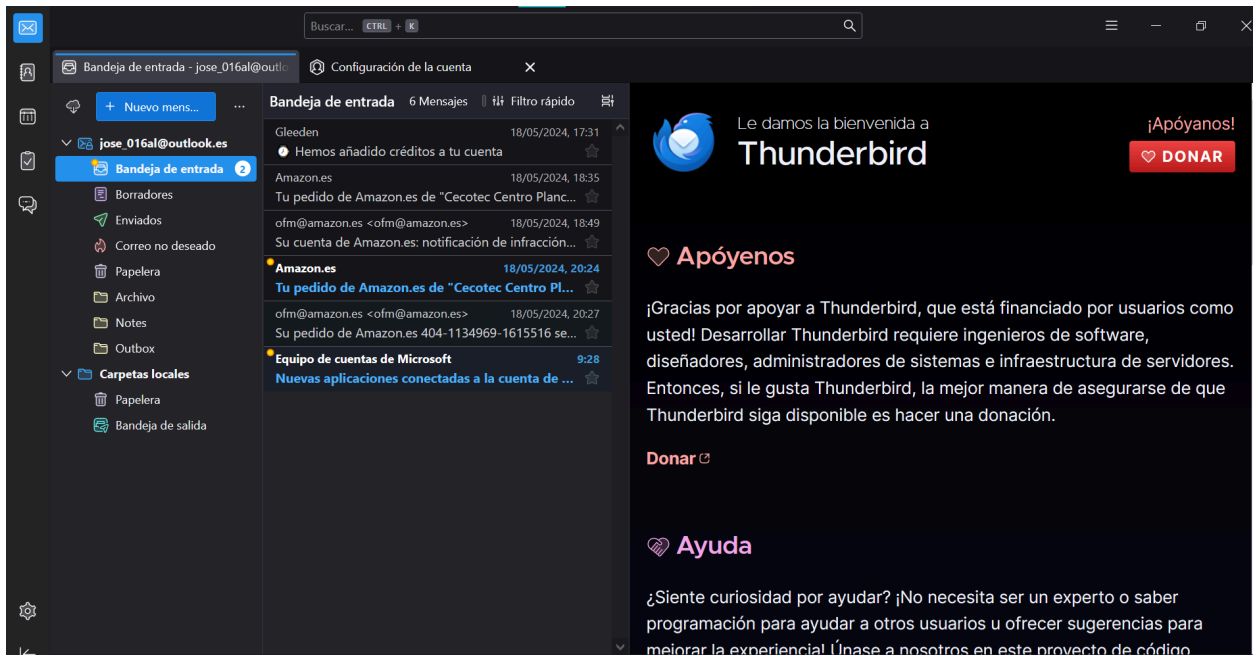
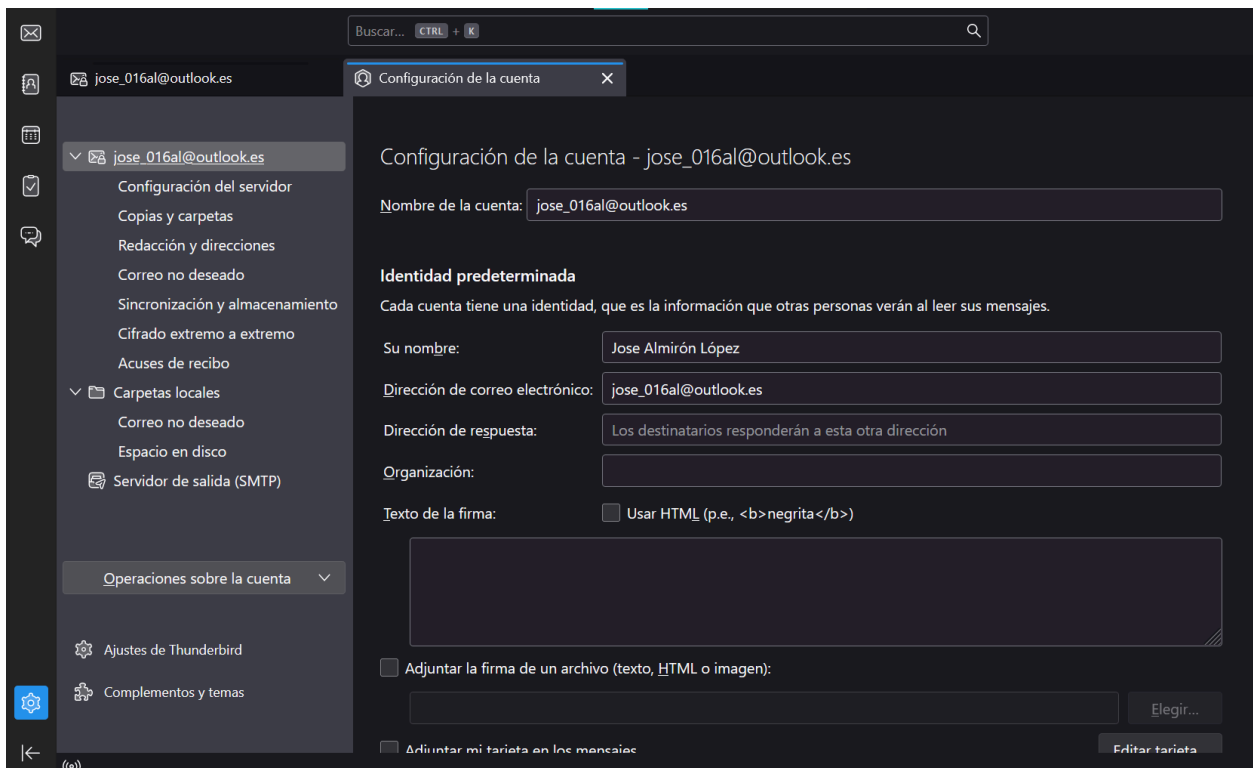
Estas tecnologías, al trabajar conjuntamente, mejoran significativamente la seguridad del correo electrónico, reduciendo el riesgo de suplantación de identidad y asegurando que los correos sean auténticos y confiables.

Instalar los clientes de correo electrónico más utilizados

Mozilla Thunderbird

Almacena los correos electrónicos en una estructura de archivos conocida como MBOX. La ubicación típica en sistemas Windows es

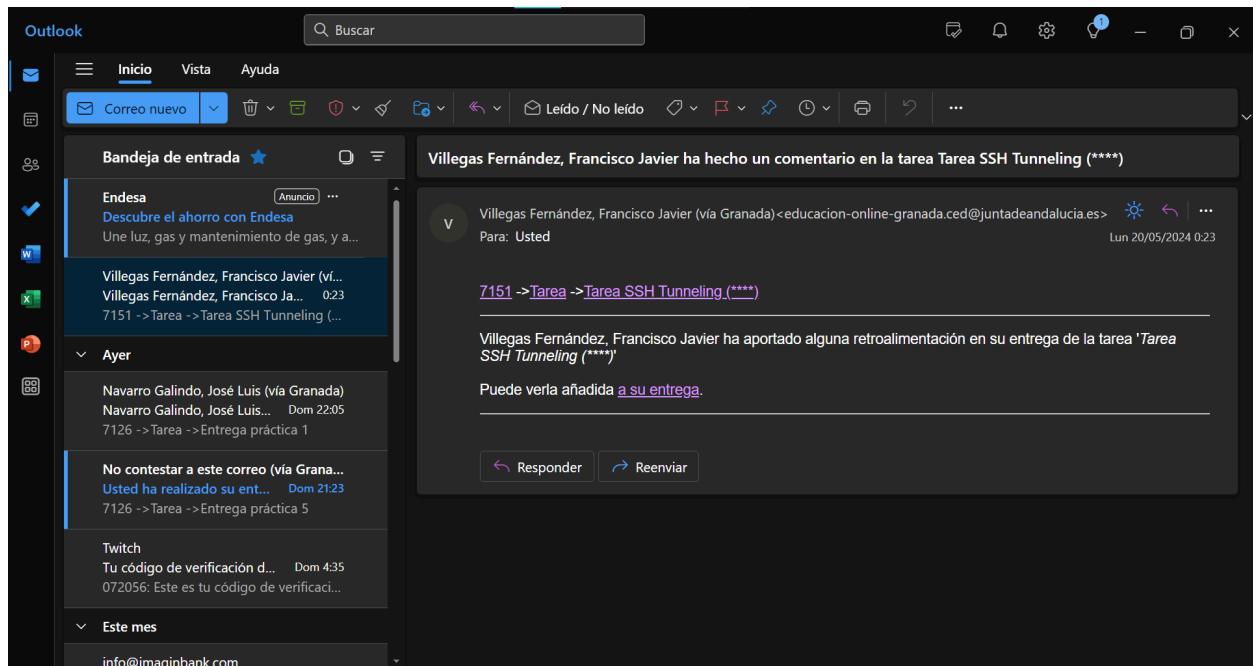
C:\Users\<tu_usuario>\AppData\Roaming\Thunderbird\Profiles\<nombre_del_perfil>\Mail\.



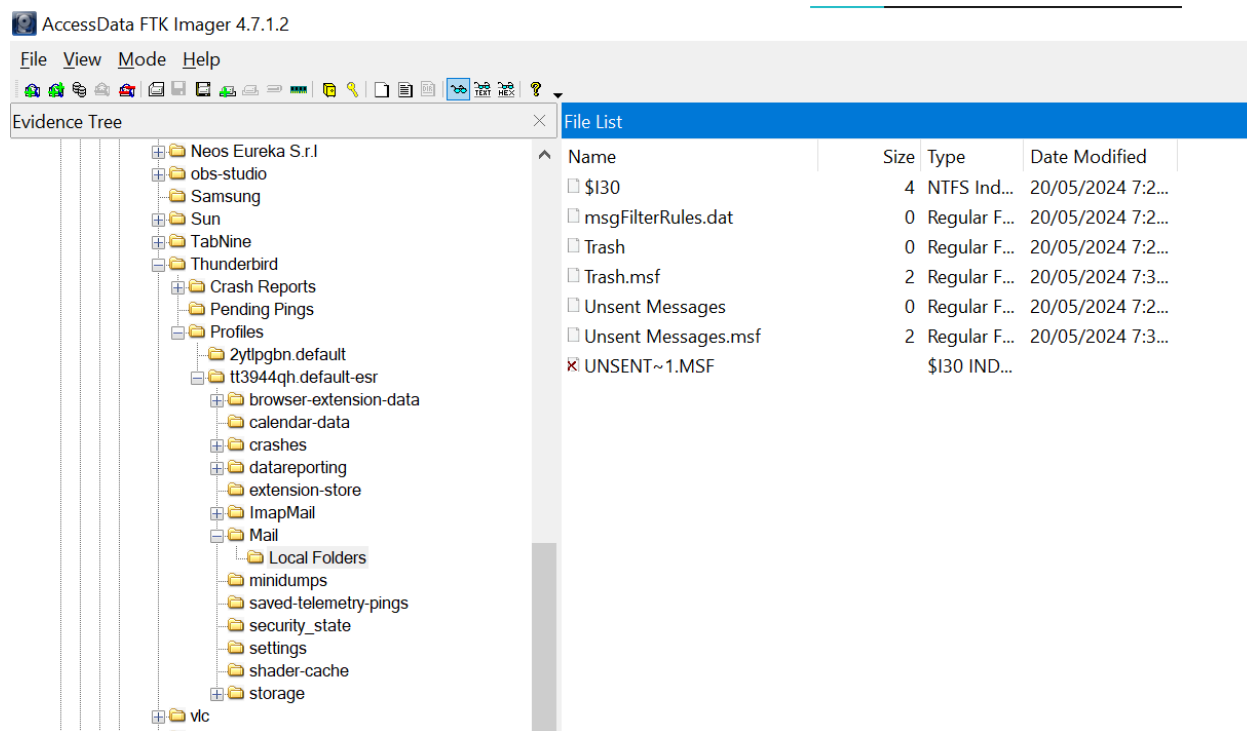
Outlook

Utiliza archivos PST (Personal Storage Table) o OST (Offline Storage Table) para almacenar los correos. La ubicación típica en sistemas Windows es

C:\Users\<tu_usuario>\AppData\Local\Microsoft\Outlook\.



Herramientas para la Extracción de Evidencias en Thunderbird



1. Mbox Viewer

- **Descripción:** Una herramienta gratuita que permite abrir y leer archivos MBOX.
- **Uso forense:** Puede abrir archivos MBOX sin necesidad de tener Thunderbird instalado, lo que facilita la visualización y extracción de correos electrónicos.
- **Ventaja:** Fácil de usar, permite exportar correos en formatos como EML, y es ideal para revisiones rápidas.

2. MailStore Home

- **Descripción:** Una solución gratuita para archivar y gestionar correos electrónicos de varias fuentes, incluidos archivos MBOX.
- **Uso forense:** Permite importar archivos MBOX y buscar, filtrar y exportar correos electrónicos de manera eficiente.
- **Ventaja:** Soporta múltiples formatos y fuentes, y proporciona una interfaz amigable para la gestión de grandes volúmenes de correos.

3. Aid4Mail

- **Descripción:** Una herramienta profesional para la conversión y exportación de correos electrónicos.

- **Uso forense:** Capaz de extraer y convertir correos electrónicos de Thunderbird (y otros formatos) a varios formatos, lo que facilita su análisis y presentación como evidencia.
 - **Ventaja:** Muy robusta y flexible, adecuada para grandes volúmenes de datos y conversiones complejas.
4. Forensic Email Collector (FEC)
- **Descripción:** Una herramienta especializada en la extracción forense de correos electrónicos.
 - **Uso forense:** Diseñada para capturar correos electrónicos de manera segura y precisa, manteniendo la integridad de los datos.
 - **Ventaja:** Ofrece características avanzadas de autenticidad y preservación de evidencias, cruciales para investigaciones legales.
5. Emailchemy
- **Descripción:** Una herramienta para la conversión de formatos de correo electrónico.
 - **Uso forense:** Puede convertir archivos MBOX a otros formatos como PST, facilitando su importación en herramientas de análisis forense.
 - **Ventaja:** Compatible con múltiples formatos de correo, es útil para investigadores que trabajan con diferentes sistemas de correo electrónico.