

Análisis Forense Informático

M57-Jean



Cursos 23/24 – IES La Marisma

Trabajo Práctico Caso M57-Jean

Pedro Manuel García Álvarez

ÍNDICE

1.- Introducción	4
1.1.- Contexto del Caso M57-jean 2008.....	5
1.2.- Objetivos del Análisis Forense	6
2.- Marco Metodológico.....	7
2.1.- Adquisición.....	7
2.1.1.- Copia de Seguridad Completa del Disco Original.....	7
2.1.2.- Herramientas y Aplicaciones Destacadas	8
2.1.3.- Imagen Forense Encase (E01) del Escenario M57-Jean 2008	8
2.2.- Análisis	9
2.2.1.- Identificación, Estudio e Interpretación de Elementos de Evidencia	9
2.2.2.- Resumen de Entrevistas a las Personas Involucradas.....	9
2.2.3.- Evidencia Encontrada en la Imagen Forense Tipo Encase (E01)	10
2.3.- Presentación	11
2.3.1.- Recopilación y Transformación de Información en Informe Comprensible	11
2.3.2.- Consideraciones sobre Archivos Tallados y Tipos de Datos.....	11
3.- Línea de Tiempo	13
3.1.- Herramientas Informáticas para Obtener la Secuencia de Eventos	13
3.2.- Uso de la Línea de Tiempo en la Comprensión de Eventos	13
3.3.- Verificar si la imagen esta correcta con programa AccessData FTK Imagen 4.7.1.2	15
3.4.- Sacar el fichero system a un directorio llamado Archivos del Sistemas.....	15
3.5.- Zona horaria	16
3.6.- Programa Autopsy 4.19.3.....	17
3.7.- Fichero según se ha infiltrado m57biz.zlx.	18
3.8.- Localizamos el fichero de los correo electronico.....	18
3.9.- Extraemos el fichero outlook.pst para ver los correo electronico.....	19
3.10.- Con el programa Outlook Viewer revisamos los correos electronicos.....	19

3.10.1.- Primera evidencia mensaje de Alison a Jean con el asunto background checks 20/07/2008 1:39:57	21
3.10.2.- Segunda evidencia Alison a Jean con el asunto Please send me the information now 20/07/2008 3:22.45	21
3.10.3.- Tercera evidencia Jean enviar el correo electrónico a tuckgorge 20/07/2008 3:28:47	22
4.- Conclusiones	24
4.1.- Evidencias de Manipulación Ilegal de Información.....	24
4.2.- Importancia de las Herramientas Forenses en la Resolución de Casos.....	24
4.3.- Aspectos de Seguridad Negligentes en el Manejo de Correo Corporativo.....	25
5.- Anexos	26
5.1.- Especificaciones técnicas de la imagen forense Encase (E01)	26
5.2.- Evidencias de mensajes en la plataforma Microsoft Outlook 2000	27
5.2.1.- Imagen 1: Mensaje de Alison a Jean con el asunto "Background Checks"	27
5.2.2.- Imagen 2: Encabezado de correo electrónico "Background checks"	28
5.2.3.- Imagen 3: Mensaje de Alison a Jean con la solicitud de información	29
5.2.4.- Imagen 4: Encabezado de correo electrónico "Please send me the information now"	30
5.2.5.- Imagen 5: Envío de la hoja de cálculo al correo electrónico "tuckgorge@gmail.com".	31
6.- Cronología gráfica del escenario M57-Jean	32

1.- Introducción

El caso M57-Jean plantea un escenario en el que se ha producido la filtración de documentos corporativos desde la computadora portátil de Jean, un alto ejecutivo de la empresa M57.Biz. Pocos días después del inicio del caso, se descubrió una hoja de cálculo confidencial que detalla nombres y salarios de empleados clave. Curiosamente, esta información confidencial se publicó en la sección de "comentarios" de un competidor de la empresa. La hoja de cálculo está vinculada exclusivamente a Jean, generando dudas sobre la seguridad de la información interna de la empresa.

Jean sostiene que desconoce cómo los datos salieron de su computadora portátil y sugiere la posibilidad de un ataque informático. Se proporciona una imagen de disco de la computadora portátil de Jean en formato EnCase E01, que incluye los archivos nps-2008-jean.E01 y nps-2008-jean.E02. Tu tarea consiste en examinar estos materiales para determinar cómo se produjo la filtración de datos o si hay evidencia que sugiera que Jean no es tan inocente como afirma.

Materiales:

Disco de Jean en formato EnCase E01:

[nps-2008-jean.E01](#)

[nps-2008-jean.E02](#)

1.1.- Contexto del Caso M57-jean 2008

El escenario M57-Jean se desarrolla en el contexto de una pequeña empresa emergente denominada M57.Biz. En este caso específico, la trama se desata unas semanas después del inicio de las operaciones de la empresa. La situación involucra la filtración de documentos corporativos críticos desde la computadora portátil de un alto ejecutivo de M57.Biz, el Director Financiero Jean.

La problemática surge cuando una hoja de cálculo altamente confidencial, que detalla nombres y salarios de empleados clave de la empresa, aparece publicada en la sección de "comentarios" de un competidor. Cabe destacar que dicha hoja de cálculo era exclusiva para uno de los empleados de M57, en este caso, Jean.

Jean, el afectado directo, niega tener conocimiento sobre cómo los datos salieron de su computadora portátil y sostiene la hipótesis de que su dispositivo podría haber sido comprometido por un ataque informático. En este contexto, se proporciona al investigador forense una imagen de disco de la computadora portátil de Jean en formato EnCase E01, con los archivos nps-2008-jean.E01 y nps-2008-jean.E02.

La tarea del investigador es esclarecer el misterio detrás de la filtración de datos, determinar si Jean es realmente inocente en este incidente o si existe alguna complicidad por su parte. Para ello, se emplearán herramientas y metodologías forenses con el fin de analizar la imagen del disco y reconstruir los eventos que llevaron a la publicación no autorizada de la información confidencial de la empresa.

1.2.- Objetivos del Análisis Forense

El análisis forense en el caso M57-Jean 2008 se orienta hacia el esclarecimiento de la filtración de datos corporativos desde la computadora portátil de Jean, el Director Financiero de M57.Biz. Los objetivos específicos del análisis forense son:

- **Determinar el Método de Filtración:**

- Identificar cómo se llevaron a cabo la filtración y publicación no autorizada de la hoja de cálculo confidencial.
- Establecer si la filtración se realizó de manera interna o externa a la empresa.

- **Verificar la Aseveración de Jean:**

- Evaluar la afirmación de Jean acerca de ser ajeno a la filtración y determinar si su computadora portátil fue realmente objeto de un ataque informático.
- Analizar posibles evidencias de manipulación externa del dispositivo.

- **Reconstruir la Secuencia de Eventos:**

- Elaborar una línea de tiempo detallada de los eventos relacionados con la filtración de datos.
- Identificar los momentos clave que condujeron a la publicación de la información confidencial.

- **Examinar la Autenticidad de la Hoja de Cálculo:**

- Validar la autenticidad de la hoja de cálculo filtrada y asegurarse de que sea una reproducción fiel de los datos internos de la empresa.
- Detectar posibles alteraciones o manipulaciones en el contenido.

-

- **Determinar la Responsabilidad:**

- Establecer si Jean fue de alguna manera cómplice o negligente en la filtración de datos.
- Identificar a posibles responsables internos o externos involucrados en el incidente.

- **Proponer Medidas Correctivas:**

- Sugerir recomendaciones y medidas de seguridad adicionales para prevenir futuras filtraciones de datos.
- Asesorar sobre prácticas y políticas de seguridad informática para fortalecer la protección de la información sensible.

El conjunto de estos objetivos busca proporcionar una visión integral del incidente, permitiendo a la empresa M57.Biz tomar decisiones informadas y mitigar los riesgos de seguridad que puedan surgir a raíz de este evento.

2.- Marco Metodológico

En el desarrollo del análisis forense del caso M57-Jean 2008, se sigue un enfoque metódico que abarca diversas etapas fundamentales. El marco metodológico se desglosa de la siguiente manera:

2.1.- Adquisición

La adquisición de datos es un paso crítico para preservar la integridad de la evidencia digital. En este contexto:

2.1.1.- Copia de Seguridad Completa del Disco Original

Se realiza una copia de seguridad exhaustiva del disco original, abarcando la totalidad de la información almacenada. Este procedimiento incluye el respaldo del espacio no asignado por los sistemas de archivos y datos que pudieron existir antes del formateo del soporte.

2.1.2.- Herramientas y Aplicaciones Destacadas

El proceso de adquisición se apoya en herramientas y aplicaciones especializadas, entre las que se destacan dd, EnCase, FTK, Air, y otras, seleccionadas por su capacidad para obtener resultados detallados en la toma de información forense. Estas herramientas desempeñan un papel crucial en la obtención de datos relevantes para el análisis posterior.

2.1.3.- Imagen Forense Encase (E01) del Escenario M57-Jean 2008

Se utiliza una imagen forense del tipo Encase (E01) obtenida desde la página web del instituto. La imagen, denominada nps-2008-jean.E01, abarca toda la información del disco de almacenamiento de la computadora portátil del CFO de M57.Biz, Jean. Las especificaciones técnicas de la imagen, incluyendo el tamaño, tipo de sistema, y huellas de verificación, se detallan mediante el software libre Autopsy 4.19.3.

Este proceso de adquisición sienta las bases para el análisis subsiguiente, asegurando la preservación y documentación adecuada de la evidencia digital.

2.2.- Análisis

En esta fase del análisis forense del caso M57-Jean 2008, se lleva a cabo una evaluación detallada de la información adquirida. El análisis se estructura de la siguiente manera:

2.2.1.- Identificación, Estudio e Interpretación de Elementos de Evidencia

Conforme a las pautas establecidas, el análisis implica la identificación, estudio, y la interpretación de los elementos de evidencia presentes en el soporte de datos. Cada dato obtenido se somete a una evaluación exhaustiva para determinar su relevancia en el contexto del caso. Se busca discernir archivos sospechosos y comprender en detalle su contenido.

2.2.2.- Resumen de Entrevistas a las Personas Involucradas

Se recopila y resume la información derivada de entrevistas realizadas a las dos personas clave en el caso M57: Alison, la presidenta, y Jean, el director financiero. Las declaraciones proporcionadas por ambas partes se presentan de manera estructurada para destacar las discrepancias y similitudes en sus relatos.

- Resumen de Entrevistas:

- Alison (Presidenta):

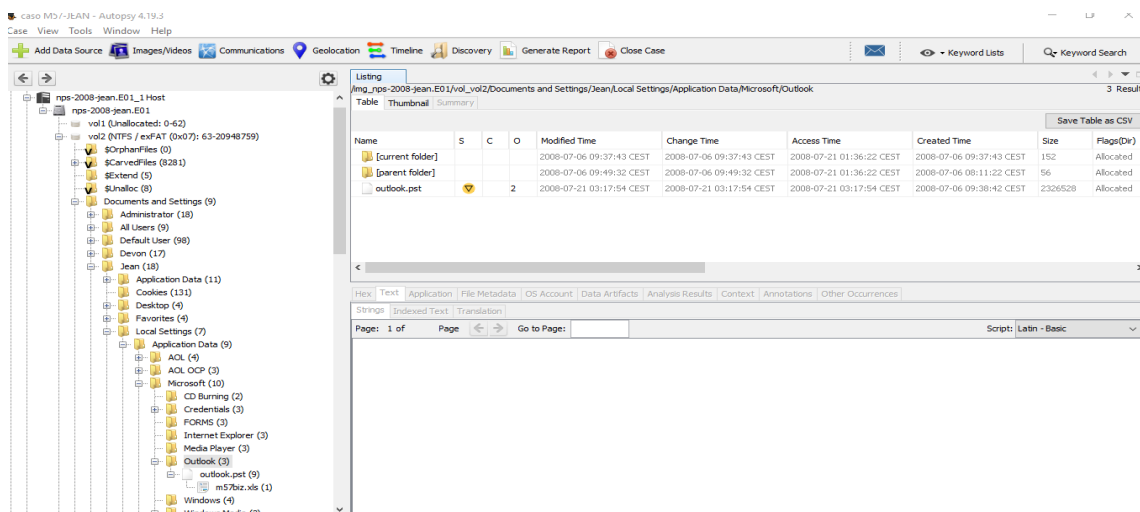
- Desconoce la situación mencionada por Jean.
 - Niega haber solicitado la hoja de cálculo.
 - Afirma no haber recibido la hoja de cálculo por correo electrónico.

- Jean (Director Financiero):
 - Asegura que Alison le pidió la hoja de cálculo como parte de una nueva ronda de financiación.
 - Afirma que Alison solicitó el envío de la hoja de cálculo por correo electrónico.
 - Limita su conocimiento sobre el caso a estas circunstancias.

2.2.3.- Evidencia Encontrada en la Imagen Forense Tipo Encase (E01)

Se examina la imagen forense Encase (E01) en busca de evidencia relevante. La ilustración del total de archivos tallados revela 8281 archivos eliminados del sistema de archivos del disco de almacenamiento de la computadora portátil de Jean. Se destaca la presencia de un archivo Outlook.pst en la ruta específica "vol2/Documentos and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst", el cual contiene conversaciones entre Jean, Alison, y otros colegas de la empresa.

Esta fase de análisis busca arrojar luz sobre los eventos ocurridos y proporcionar una base sólida para la presentación de conclusiones y hallazgos.



The screenshot shows the Autopsy 4.19.3 interface. The left pane displays a file tree for 'nps-2008-jean.E01_1.Host'. The right pane shows a listing of files in the path '/img_nps-2008-jean.E01/vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook'. The table below shows the details of the 'outlook.pst' file.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]				2008-07-06 09:37:43 CEST	2008-07-06 09:37:43 CEST	2008-07-21 01:36:22 CEST	2008-07-06 09:37:43 CEST	152	Allocated
[parent folder]				2008-07-06 09:49:32 CEST	2008-07-06 09:49:32 CEST	2008-07-21 01:36:22 CEST	2008-07-06 08:11:22 CEST	56	Allocated
outlook.pst		2		2008-07-21 03:17:54 CEST	2008-07-21 03:17:54 CEST	2008-07-21 03:17:54 CEST	2008-07-06 09:38:42 CEST	2326528	Allocated

2.3.- Presentación

En esta etapa, asumiendo el rol de investigador forense, estoy dedicado a la presentación de los hallazgos y la información recopilada en un informe claro y comprensible. Esta fase se organiza de la siguiente manera:

2.3.1.- Recopilación y Transformación de Información en Informe Comprensible

Mi tarea principal consiste en reunir todos los datos significativos descubiertos durante el análisis y transformarlos en un informe de fácil comprensión. Se están siguiendo los siguientes pasos:

- Recopilación de Información: Se recopilan todos los datos relevantes, incluidos los detalles de la imagen forense Encase (E01), entrevistas, y cualquier otra evidencia significativa.
- Estructuración del Informe: La información se presenta de manera estructurada, siguiendo una secuencia lógica que permita a cualquier lector comprender los eventos y conclusiones.

2.3.2.- Consideraciones sobre Archivos Tallados y Tipos de Datos

Se realiza una consideración especial sobre los archivos tallados encontrados en la imagen forense Encase (E01). Entre los 8281 archivos eliminados, se identifican diversos tipos de datos, como imágenes en formatos JPG, PNG, GIF, archivos de acceso directo y de aplicaciones, documentos de texto (Word, TXT), hojas de cálculo (XLS) y archivos DLL.

- Ejemplos de Archivos Tallados:
 - Imágenes (JPG, PNG, GIF)
 - Archivos de Acceso Directo y de Aplicaciones

- Documentos de Texto (Word, TXT)
- Hojas de Cálculo (XLS)
- Archivos DLL

Este enfoque destaca la diversidad de información contenida en los archivos eliminados, lo que puede ser crucial para comprender la naturaleza y el alcance de la filtración de datos.

Esta fase de presentación no solo busca informar de manera efectiva, sino también sentar las bases para las conclusiones finales del análisis forense.

3.- Línea de Tiempo

En esta sección, me enfoco en la construcción y análisis de la línea de tiempo del caso M57-Jean 2008, utilizando herramientas informáticas especializadas. La línea de tiempo se desarrolla de la siguiente manera:

3.1.- Herramientas Informáticas para Obtener la Secuencia de Eventos

Para establecer una línea de tiempo precisa, empleo herramientas informáticas diseñadas para analizar registros y eventos del sistema. Algunas de las herramientas destacadas incluyen:

- **Autopsy 4.19.3:** Esta herramienta de software libre se utiliza para el análisis forense y la generación de informes. Proporciona funciones avanzadas para examinar la imagen forense Encase (E01) y extraer información de eventos clave.
- **Herramientas de Análisis Temporal:** Se utilizan herramientas específicas para identificar y analizar registros temporales, como la marca de tiempo de archivos y eventos del sistema.

3.2.- Uso de la Línea de Tiempo en la Comprensión de Eventos

La línea de tiempo se convierte en una herramienta crucial para entender la secuencia de eventos en el escenario M57-Jean 2008. A través de esta representación gráfica, se logra:

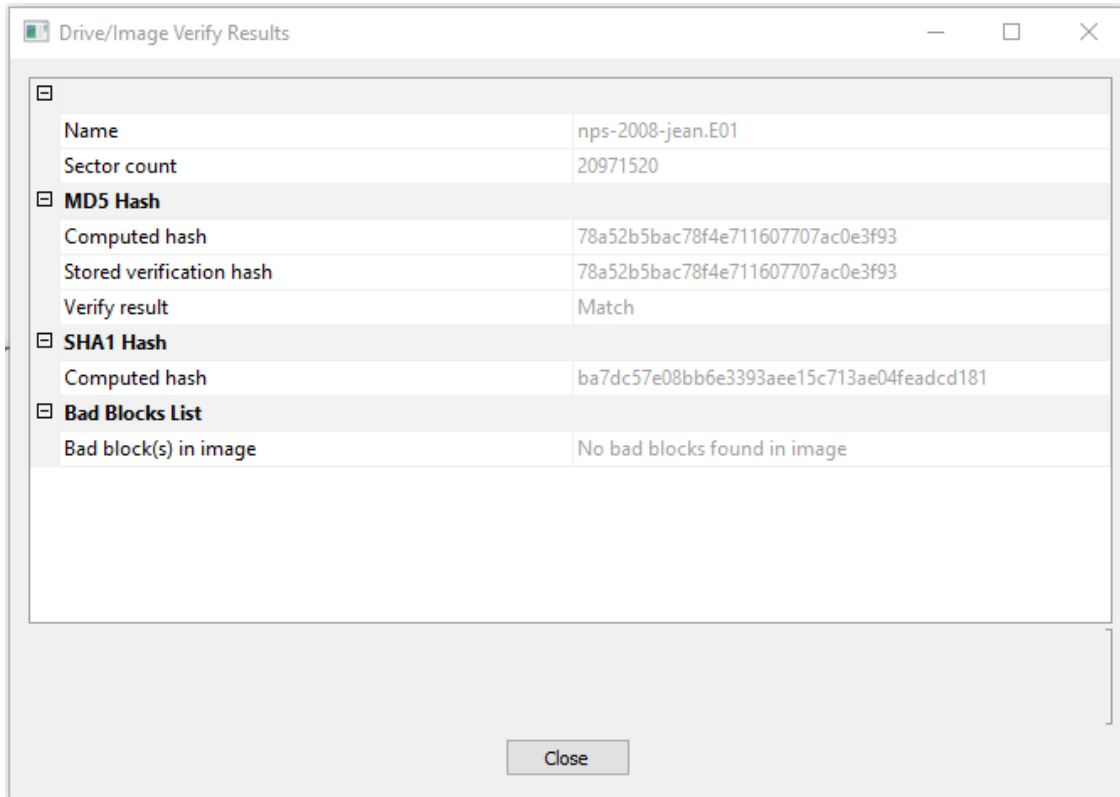
- **Identificación de Actividades Relevantes:** Se destacan las actividades y cambios significativos en el

sistema, desde la creación y modificación de archivos hasta posibles intrusiones.

- **Relación entre Eventos:** La línea de tiempo permite establecer conexiones entre eventos, ayudando a comprender las relaciones de causa y efecto. Esto puede revelar patrones y proporcionar insights sobre la filtración de datos.
- **Marco Temporal de la Filtración de Datos:** Al examinar detenidamente la línea de tiempo, se busca identificar el momento exacto en que ocurrió la filtración de la hoja de cálculo confidencial desde la computadora portátil de Jean.

Esta sección contribuye significativamente a la reconstrucción de los eventos clave y facilita la comprensión del cronograma de actividades relacionadas con la filtración de datos en el caso M57-Jean 2008.

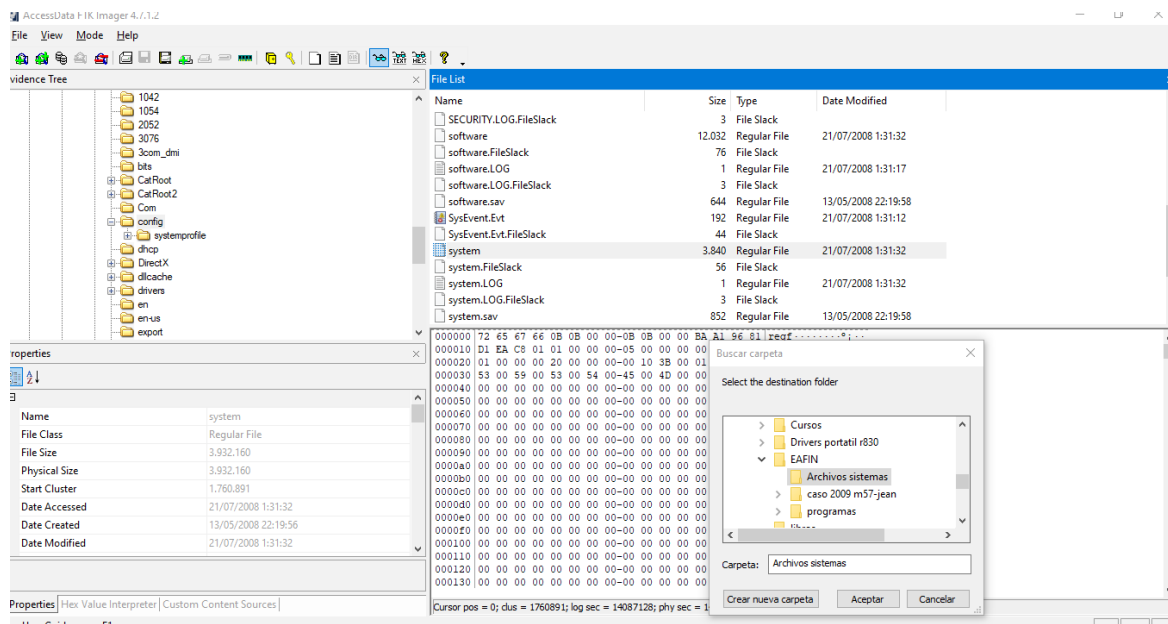
3.3.- Verificar si la imagen esta correcta con programa AccessData FTK Imagen 4.7.1.2



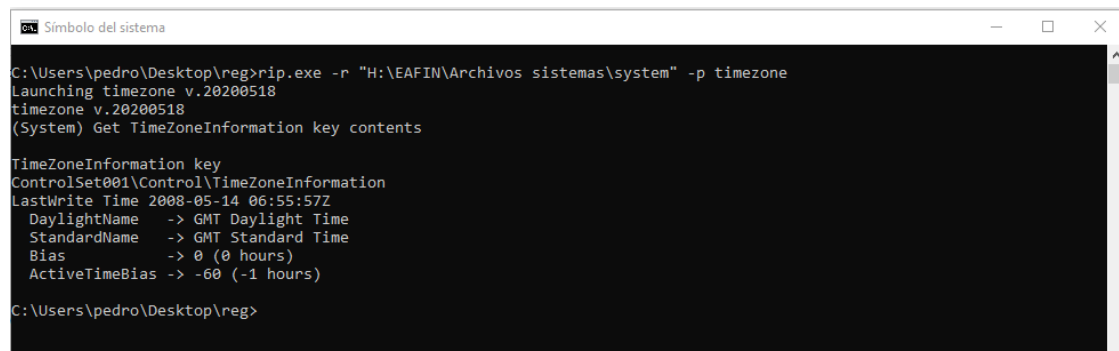
En esta pantalla se ve que todos los datos y la imagen esta correcta. Aquí podemos ver que md5 hash Computed hash y Stored verification hash esta correcto y coincide.

3.4.- Sacar el fichero system a un directorio llamado Archivos del Sistemas.

Localizo el fichero system en la imagen nps-2008-jean.E01 con el programa AccessData FTK Imager 4.7.1.2 y lo guardo a la carpeta del Archivos del Sistemas.



3.5.- Zona horaria



Con el programa RegRipper consulto la zona horaria del fichero System llegando a la conclusión que es (GMT+1:00) ETC/GMT-1.

3.6.- Programa Autopsy 4.19.3.

Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path:

☐ Ignore orphan files in FAT file systems

Time zone:

Sector size:

Hash Values (optional):

MD5:

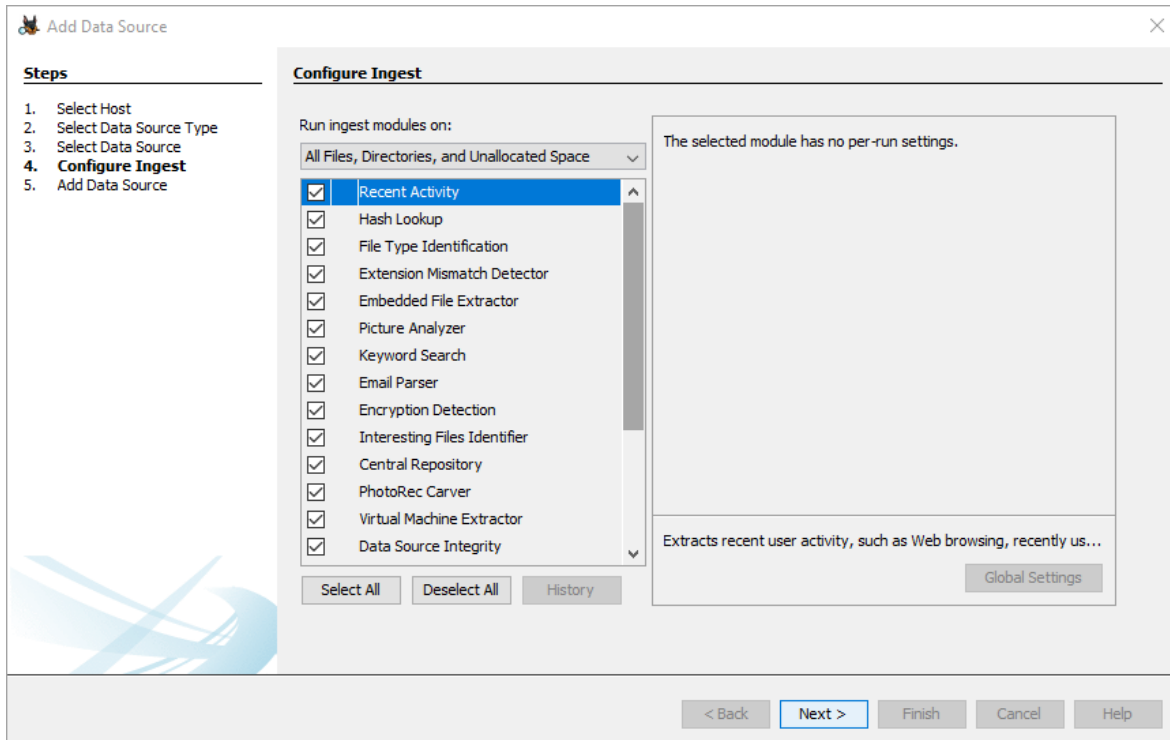
SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

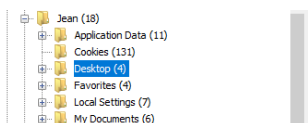
< Back **Next >** Finish Cancel Help

Seleccionar el fichero nps-2008-jean.E01 y seleccionar la zona horaria (GMT+1:00) ETC/GMT-1 y pulsa la tecla next.



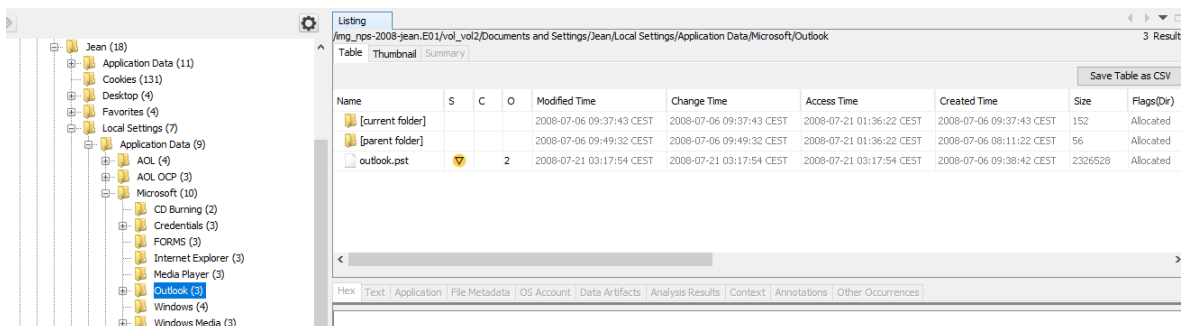
Seleccionar todas las opciones y pulsar la tecla next.

3.7.- Fichero según se ha infiltrado m57biz.zlx.



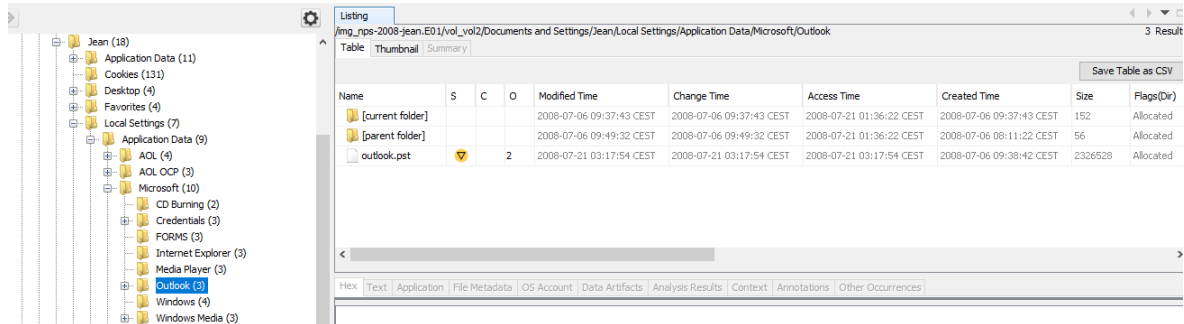
File Name	Size	Created Time	Modified Time	Access Time	Changed Time	Flags
[current folder]		2008-07-20 03:28:03 CEST	2008-07-20 03:28:03 CEST	2008-07-21 03:17:54 CEST	2008-07-21 03:17:54 CEST	Allocated
[parent folder]		2008-07-06 09:51:00 CEST	2008-07-06 09:51:00 CEST	2008-07-21 02:44:52 CEST	2008-07-06 08:11:22 CEST	56 Allocate
AIM Tunes.url	2	2008-07-18 06:30:49 CEST	2008-07-18 06:30:49 CEST	2008-07-20 03:28:02 CEST	2008-07-18 06:30:49 CEST	110 Allocate
m57biz.xls	3	2008-07-20 03:28:03 CEST	2008-07-20 03:28:04 CEST	2008-07-20 03:28:03 CEST	2008-07-20 03:28:03 CEST	291840 Allocate

3.8.- Localizamos el fichero de los correo electronico.

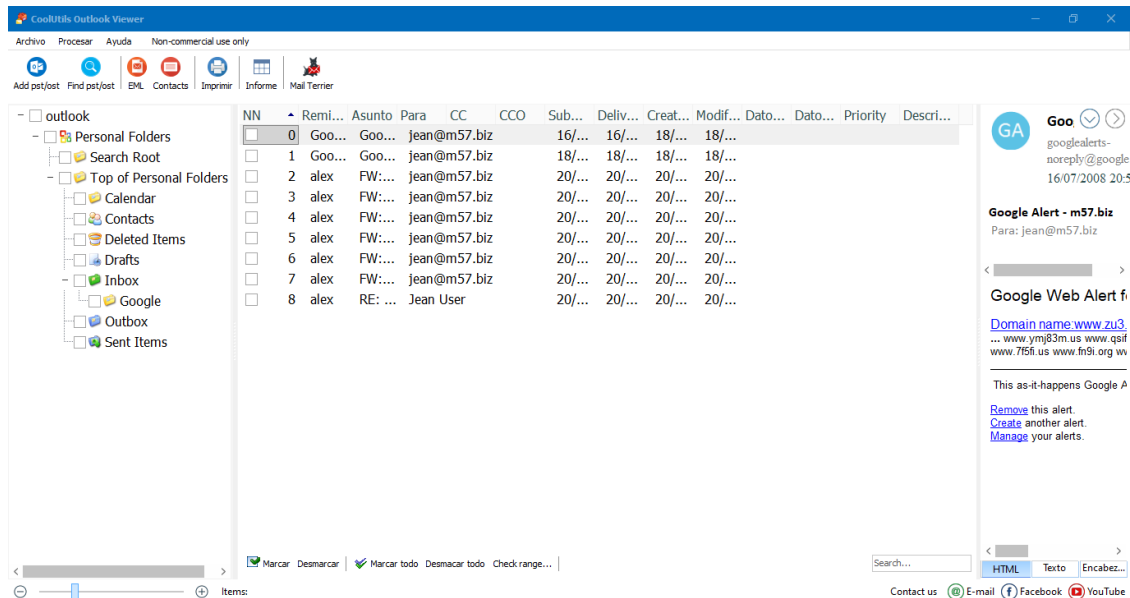


En esta imagen no encontramos con el fichero que se ha infiltrado.

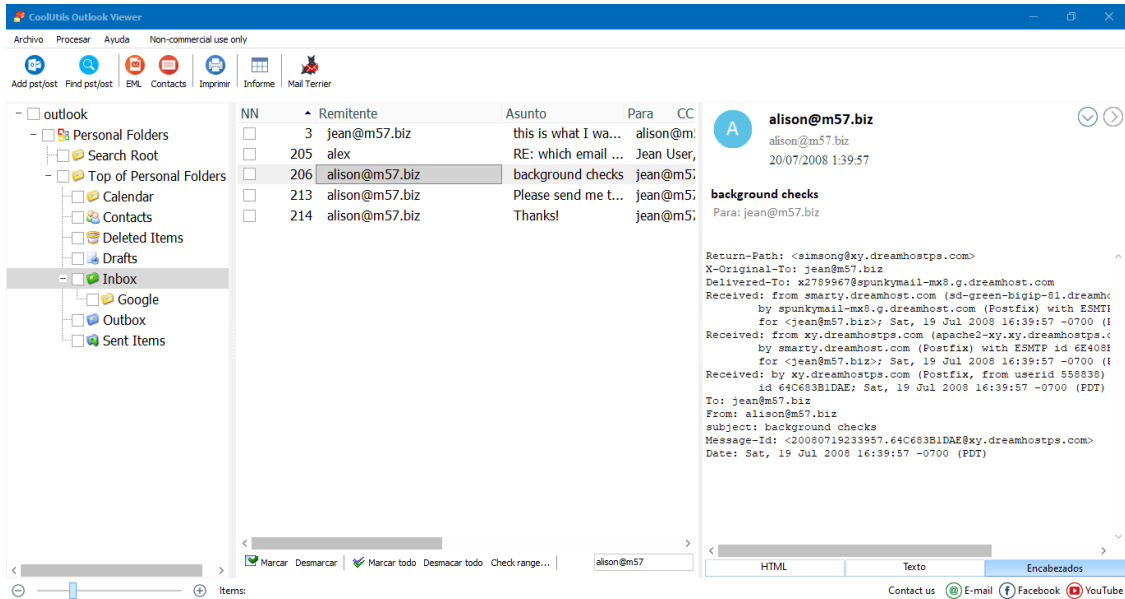
3.9.- Extraemos el fichero outlook.pst para ver los correo electronico.



3.10.- Con el programa Outlook Viewer revisamos los correos electronicos.



Una vez abierto el fichero no encontramos con la bandeja de entrada de jean. Con esta bandeja de entrada buscaremos si Alison envió algún correo electrónico a Jean para solicitar la hoja de cálculo.



3.10.1.- Primera evidencia mensaje de Alison a Jean con el asunto background checks 20/07/2008 1:39:57

alison@m57.biz

alison@m57biz

20/07/2008 1:39:57

Background checks

Para: Jean@m57.biz

Jean,

Uno de los inversores potenciales con los que he estado tratando me pidió que conociera sus antecedentes. Control de nuestros empleados actuales. Aparentemente recientemente tuvieron algunos problemas en algún otro empresa que financiaron.

¿Podría por favor elaborarme una hoja de cálculo que especifique cada uno de nuestros empleados, sus salario actual y su SSN?

Por favor, no le menciones esto a nadie.

Gracias.

3.10.2.- Segunda evidencia Alison a Jean con el asunto Please send me the information now 20/07/2008 3:22:45

alison@m57.biz

tuckgorge@gmail.com

20/07/2008 3:22:45

Por favor envíame la información ahora

Para: Jean@m57.biz

Hola jean.

Lamento molestarte, pero realmente necesito esa información ahora. Este tipo de VC está siendo muy insistente.

¿Puede responder a este correo electrónico con la información que solicité: los nombres, salarios y

¿Números de seguro social (SSN) de todos nuestros empleados actuales y contrataciones previstas?

Gracias.

En este encabezado vemos que el correo fue enviado por tuckgorge@gmail.com

No estamos dando cuenta que el correo de alison@m57.biz ha sido falsificado.

Ahora buscaremos si jean ha enviado el correo con el fichero Excel.

3.10.3.- Tercera evidencia Jean enviar el correo electrónico a tuckgorge 20/07/2008 3:28:47

Jean User

jean@m57.biz

20/07/2008 3:28:47

M57biz.xls (288,51 KB)

Adjunté la información que usted solicitó a este mensaje de correo electrónico.

-----Mensaje original-----

De: alison@m57.biz [correo a:tuckgorge@gmail.com]

Enviado: domingo 20 de julio de 2008 2:23

Para: jean@m57.biz

Asunto: Por favor envíame la información ahora

Hola jean.

Lamento molestarte, pero realmente necesito esa información ahora. Este tipo de VC está siendo muy insistente.

¿Puede responder a este correo electrónico con la información que solicité: los nombres, salarios y

¿Números de seguro social (SSN) de todos nuestros empleados actuales y contrataciones previstas?

Gracias.

alison

Estamos viendo que Jean a enviado el fichero a otro correo que no es el de alison sino tuckgorge@gmail.com.

4.- Conclusiones

En esta sección, se presentan las conclusiones derivadas del análisis forense en el caso M57-Jean 2008, enfocándome en aspectos clave relacionados con la filtración de datos desde la computadora portátil de Jean.

El caso de Jean M57 parece ser claramente un caso de suplantación de correo electrónico. La suplantación de identidad por correo electrónico, también conocida como phishing, es un intento de engañar a las personas para que revelen información personal, como contraseñas y números de tarjetas de crédito. Es importante estar atento a las señales de suplantación de identidad en los correos electrónicos, como direcciones de remitente sospechosas o solicitudes inusuales de información personal.

4.1.- Evidencias de Manipulación Ilegal de Información

Tras un exhaustivo análisis forense, se ha identificado claramente la existencia de manipulación ilegal de información en el escenario M57-Jean 2008. La presencia de archivos borrados y tallados en la imagen forense Encase (E01) revela la eliminación intencionada de datos confidenciales, incluida una hoja de cálculo con información sensible de los empleados. Este hallazgo respalda la existencia de actividades fraudulentas que comprometen la integridad de los datos corporativos.

4.2.- Importancia de las Herramientas Forenses en la Resolución de Casos

El caso M57-Jean destaca la relevancia crucial de las herramientas forenses en la resolución de casos de seguridad informática. El uso de aplicaciones especializadas como Autopsy 4.19.3 y la imagen forense

Encase (E01) ha permitido no solo la recuperación de datos eliminados, sino también la reconstrucción de eventos clave. Estas herramientas desempeñan un papel fundamental al proporcionar a los investigadores los medios necesarios para analizar, interpretar y presentar evidencia de manera eficiente.

4.3.- Aspectos de Seguridad Negligentes en el Manejo de Correo Corporativo

Una conclusión relevante es la identificación de aspectos de seguridad negligentes en el manejo del correo corporativo. El cambio del correo corporativo al personal, como evidenciado en los mensajes analizados, sugiere una falta de controles de seguridad adecuados. La vulnerabilidad de las contraseñas y la falta de medidas de seguridad contribuyen al riesgo de filtración de información confidencial. Esto destaca la necesidad urgente de mejorar las prácticas de seguridad en el entorno corporativo, incluyendo políticas de contraseñas sólidas y capacitación en seguridad para los empleados.

Estas conclusiones ofrecen una visión integral de los problemas identificados durante el análisis forense, proporcionando una base sólida para la toma de decisiones y acciones correctivas en el caso M57-Jean 2008.

5.- Anexos

Esta sección proporciona información adicional relevante que complementa el análisis forense del caso M57-Jean 2008.

5.1.- Especificaciones técnicas de la imagen forense Encase (E01)

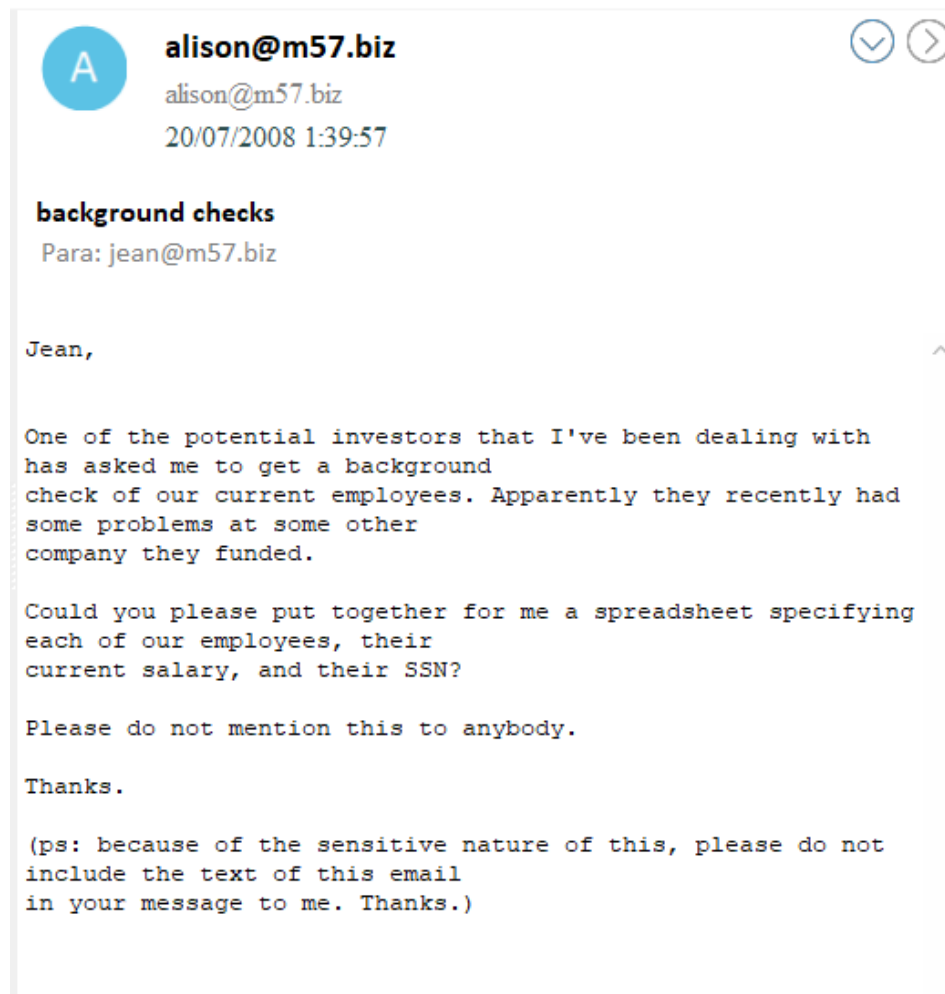
La tabla a continuación detalla las especificaciones técnicas de la imagen forense tipo Encase utilizada en el análisis del escenario M57-Jean 2008.

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Conte
Metadata							
Name:	/img_nps-2008-jean.E01						
Type:	E01						
Size:	10737418240						
MD5:	78a52b5bac78f4e711607707ac0e3f93						
SHA1:	Not calculated						
SHA-256:	Not calculated						
Sector Size:	512						
Time Zone:	Etc/GMT-1						
Acquisition Details:	Description: Jean's hard drive from the first M57 project						
:	Evidence Number: 2008-M57-Jean						
:	Examiner Name: Donny						
:	Acquired Date: Mon Jan 31 22:38:29 2011						
:	System Date: Mon Jan 31 22:38:29 2011						
:	Acquiry Operating System: Darwin						
:	Acquiry Software Version: 20101104						
Device ID:	88c361fd-f9d6-4c98-9155-686d3ed423e3						
Internal ID:	1						
Local Path:	H:\EAFIN\nps-2008-jean.E01						
:	H:\EAFIN\nps-2008-jean.E02						

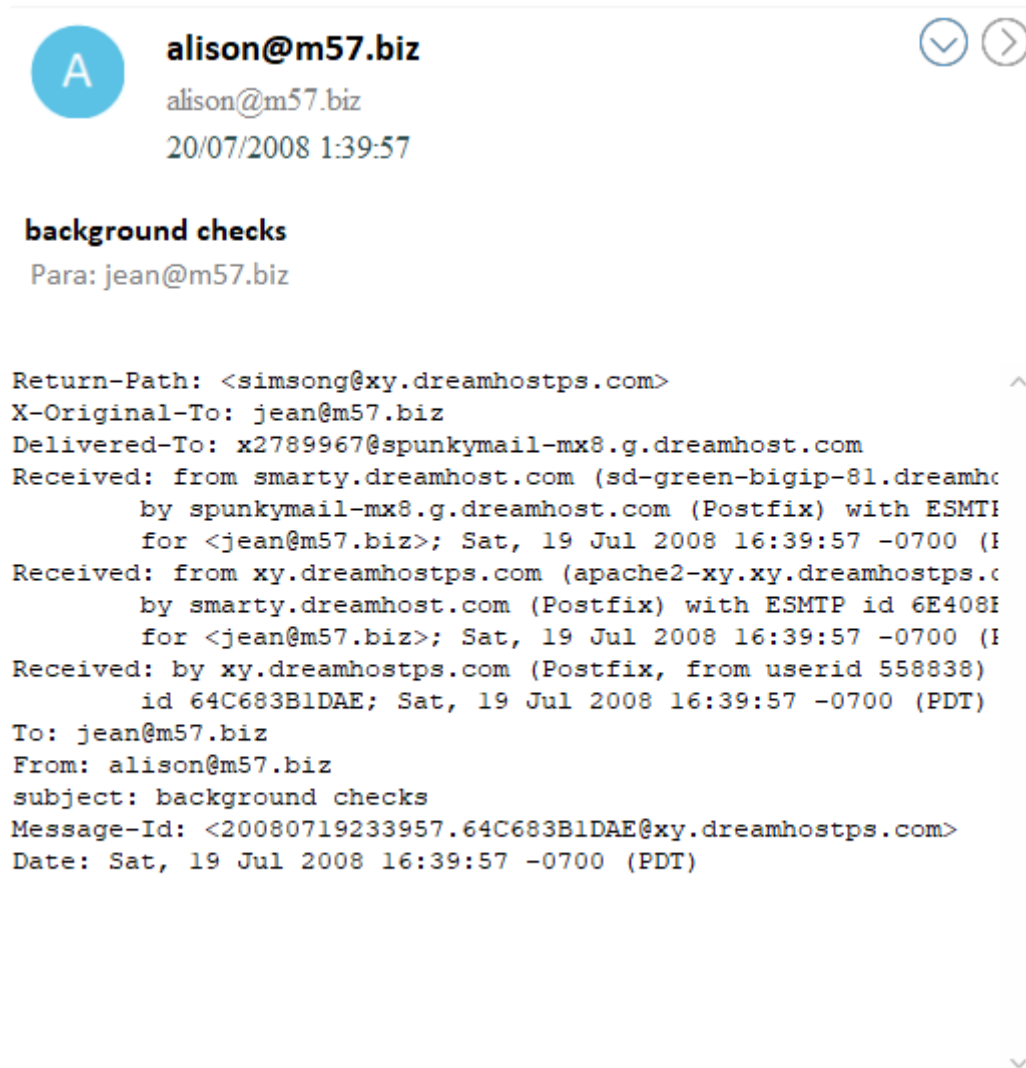
5.2.- Evidencias de mensajes en la plataforma Microsoft Outlook 2000

A continuación se presentan ejemplos de mensajes recuperados de la imagen forense Encase (E01) que involucran a los empleados de la empresa M57 dotbiz a través de la plataforma Microsoft Outlook 2000.

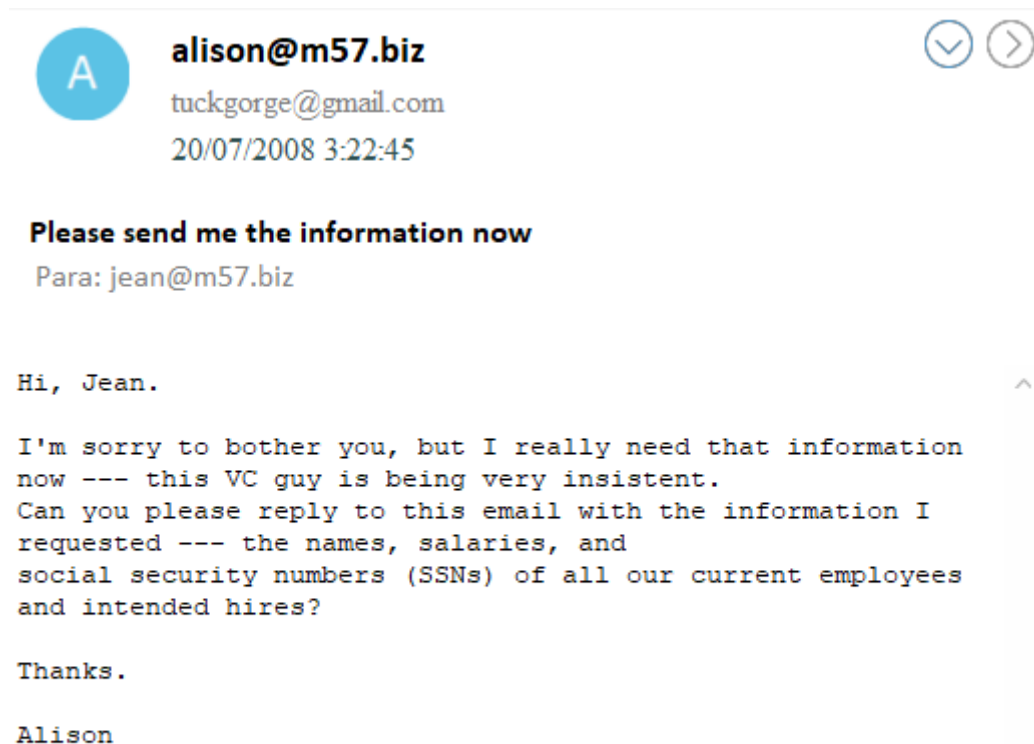
5.2.1.- Imagen 1: Mensaje de Alison a Jean con el asunto "Background Checks"



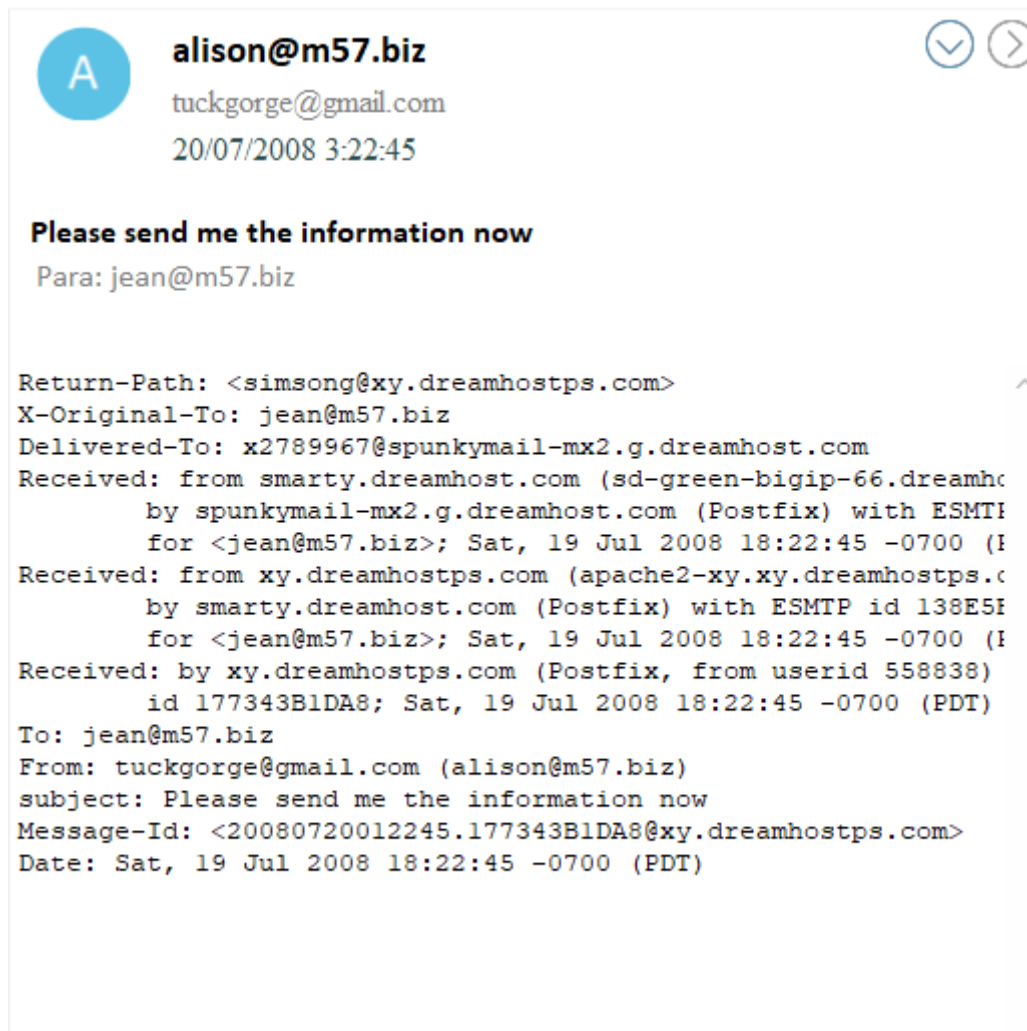
5.2.2.- Imagen 2: Encabezado de correo electrónico "Background checks"



5.2.3.- Imagen 3: Mensaje de Alison a Jean con la solicitud de información



5.2.4.- Imagen 4: Encabezado de correo electrónico "Please send me the information now"



5.2.5.- Imagen 5: Envío de la hoja de cálculo al correo electrónico "tuckgorge@gmail.com"



Jean User

jean@m57.biz

20/07/2008 3:28:47



RE: Please send me the information now

Para: alison@m57.biz

[m57biz.xls \(288,51 KB\)](#)

I've attached the information that you have requested to this email message.

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

From: alison@m57.biz [mailto:tuckgorge@gmail.com]

Sent: Sunday, July 20, 2008 2:23 AM

To: jean@m57.biz

Subject: Please send me the information now

Hi, Jean.

I'm sorry to bother you, but I really need that information now --- this VC guy is being very insistent.

Can you please reply to this email with the information I requested --- the names, salaries, and social security numbers (SSNs) of all our current employees and intended hires?

6.- Cronología gráfica del escenario M57-Jean



Presenta una representación visual de la secuencia de eventos y cambios en el escenario M57-Jean, proporcionando una línea de tiempo para ayudar en la comprensión de la evolución de los hechos.

Índice Alfabético

A

abarca	7, 8
acceso	11
AccessData	2, 15
acerca	6
Actividades	13
Adjunté	22
adquisición	7, 8
Afirma	9, 10
ajeno	6
alcance	12
Alison	3, 9, 10, 19, 21, 27, 29
almacenamiento	8, 10
ambas	9
Análisis	1, 2, 6, 13
Analizar	6
Aparentemente	21
Aplicaciones	2, 8
Archivos	2, 11, 12, 15
Asegura	10
Asesorar	7
Aseveración	6
Aspectos	3, 25
asunto	3, 21, 27
ataque	4, 5, 6
atento	24
Autenticidad	6
Autopsy	2, 8, 13, 17, 24

B

Background	3, 21, 27, 28
bandeja	19
bases	8, 12
Biz	7
busca	7, 9, 10, 12, 14

C

Cabe	5
cabo	6, 9
cálculo	3, 4, 5, 6, 9, 10, 11, 14, 21, 24, 31
cambios	13, 32
capacidad	8
capacitación	25
caso	4, 5, 6, 7, 9, 10, 13, 14, 24, 25, 26

CFO	8
clave	5, 6, 9, 14, 24
colegas	10
Completa	2, 7
cómplice	7
complicidad	5
comprensión	14, 32
Computed	15
conclusiones	10, 12, 24, 25
Conforme	9
conjunto	7
conocimiento	5, 10
Consideraciones	2, 11
construcción	13
contraseñas	24, 25
contrataciones	22, 23
Control	21
controles	25
conversaciones	10
Copia	2, 7
correo	2, 3, 9, 10, 18, 19, 22, 23, 24, 25, 28, 30, 31
correos	2, 19, 24
creación	14
críticos	5
cronograma	14
Cronología	3, 32

D

dando	22
dato	9
decisiones	7, 25
declaraciones	9
desarrollo	7
Desconoce	9
detalle	9
detalles	11
Detectar	6
Determinar	6, 7
dicha	5
direcciones	24
Director	5, 6, 10
directorio	2, 15
disco	4, 5, 8, 10
discrepancias	9
diversidad	12
diversos	11
documentación	8
documentos	4, 5, 11
domingo	22

dudas _____ 4

E

Ejemplos _____ 11
Elaborar _____ 6
electrónico _____ 3, 19, 22, 23, 28, 30, 31
Elementos _____ 2, 9
eliminación _____ 24
empleo _____ 13
empresa _____ 4, 5, 7, 21, 27
Encabezado _____ 3, 28, 30
EnCase _____ 4, 5
Encontrada _____ 2, 10
enfoque _____ 7, 12
entorno _____ 25
Entrevistas _____ 2, 9
envío _____ 10
escenario _____ 3, 4, 5, 13, 24, 26, 32
esclarecimiento _____ 6
espacio _____ 8
específica _____ 10
especificaciones _____ 8, 26
específicas _____ 13
específicos _____ 6
Establecer _____ 6, 7
Estamo _____ 23
estructura _____ 9
Estructuración _____ 11
Estudio _____ 2, 9
etapas _____ 7
evaluación _____ 9
Evaluar _____ 6
eventos _____ 5, 6, 10, 11, 13, 14, 25, 32
evidencia _____ 3, 4, 7, 8, 9, 10, 11, 21, 22, 25
evidencias _____ 6
evolución _____ 32
Examinar _____ 6
existencia _____ 24
externos _____ 7
Extraemos _____ 2, 19

F

favor _____ 21, 23
Fichero _____ 2, 18
fiel _____ 6
filtración _____ 4, 5, 6, 7, 12, 14, 24, 25
filtraciones _____ 7
Financiero _____ 5, 6
forense _____ 3, 5, 6, 7, 8, 9, 10, 11, 13, 24, 25, 26, 27

forenses _____ 5, 24
formato _____ 4, 5
formatos _____ 11
fraudulentas _____ 24
FTK _____ 2, 15
futuras _____ 7

G

generación _____ 13
gráfica _____ 3, 32

H

hallazgos _____ 11
herramientas _____ 5, 8, 13, 24
hipótesis _____ 5
hoja _____ 3, 4, 5, 6, 9, 10, 14, 19, 21, 24, 31
hojas _____ 11
horaria _____ 16, 17
huellas _____ 8

I

identidad _____ 24
identificación _____ 25
Identificar _____ 6, 7
ilustración _____ 10
imagen _____ 2, 3, 4, 5, 8, 10, 11, 13, 15, 19, 24, 26, 27
imágenes _____ 11
Imager _____ 15
Importancia _____ 3, 24
información _____ 4, 5, 6, 7, 8, 9, 11, 12, 13, 21, 22, 23, 24, 25, 26
informática _____ 7
informáticas _____ 13
informe _____ 11
inicio _____ 4, 5
integridad _____ 7, 24
internos _____ 6, 7
Interpretación _____ 2, 9
inusuales _____ 24
inversores _____ 21

J

Jean _____ 2, 3, 4, 5, 6, 7, 8, 9, 10, 13, 14, 19, 21, 22, 23, 24, 25, 26, 27, 29

L

Lamento	22, 23
lector	11
libre	8, 13
Limita	10
línea	6, 13, 14, 32
Localizamos	2, 18
Localizo	15
lógica	11

M

Manejo	3, 25
manipulación	6, 24
manipulaciones	6
marca	13
Medidas	7
medios	25
mensaje	3, 21, 22
mensajes	3, 25, 27
metódico	7
Método	6
metodologías	5
Microsoft	3, 27
misterio	5
modificación	14
momentos	6

N

necesarios	25
Negligentes	3, 25
Niega	9
nombres	4, 5
Números	22, 23

O

Objetivos	2, 6
obtención	8
opciones	18
operaciones	5
Outlook	2, 3, 19, 27

P

página	8
--------	---

pantalla	15
papel	8, 25
paso	7
patrones	14
plataforma	3, 27
Please	3, 21, 30
políticas	7, 25
posibilidad	4
prácticas	7, 25
Presenta	32
presentación	10, 11, 12
preservación	8
problemas	21, 25
problemática	5
procedimiento	8
proceso	8
programa	2, 15, 16, 19
Proponer	7
Proporciona	13
protección	7
publicación	5, 6
pudieron	8
puedan	7

R

raíz	7
recomendaciones	7
reconstrucción	14, 25
Reconstruir	6
Recopilación	2, 11
recuperación	25
registros	13
RegRipper	16
Relación	14
relevancia	9, 24
relevantes	8
representación	13, 32
reproducción	6
Resolución	3, 24
respaldo	8
Resumen	2, 9
riesgos	7
rol	11

S

Sacar	2, 15
salarios	4, 5, 22, 23
sección	4, 5, 14, 26
Secuencia	2, 6, 13

seguridad	4, 7, 8, 24, 25
seguro	22, 23
Settings/Application	10
Settings/Jean/Local	10
similitudes	9
sistemas	8
situación	5, 9
software	8, 13
solicitudes	24
soporte	9
sospechosas	24
sospechosos	9
Stored	15
suplantación	24
System	16

T

tabla	26
Tallados	2, 11
tarea	4, 5, 11
tecla	17, 18
técnicas	3, 8, 26
Temporal	14

Tipos	2, 11
toma	8, 25
totalidad	8
trama	5
Transformación	2, 11

U

Uso	2, 13
-----	-------

V

Validar	6
Verificar	2, 6, 15
Viewer	2, 19
visión	7, 25
vulnerabilidad	25

W

web	8
-----	---