

Hecho por:

Ruiz Muñoz Martin Guadalupe.



Estudios de casos de ciberseguridad.

Mtro. Enrique Hoyos Peña

Fecha: 28/04/2025

Introducción:

el análisis de evidencias en sistemas operativos obsoletos —como Windows 7— representa un desafío técnico y metodológico. Este reporte documenta el proceso de investigación realizado sobre la imagen forense win7.img, asociada a la computadora de un usuario, utilizando eventos potencialmente maliciosos.

La investigación se centró en tres hallazgos clave obtenidos mediante Axiom Examine:

Un archivo winlogon.exe corrupto, sugerente de manipulación por malware (ej. inyección de código o rootkits).

La recuperación de la contraseña de la máquina virtual, permitiendo el acceso al sistema.

Un archivo cv {1}.pdf malicioso, vinculado a posibles exploits de la época.

Además, se realizaron pruebas de conexión remota para determinar si el sistema fue comprometido mediante protocolos como RDP (Remote Desktop Protocol).

El objetivo final es sustentar técnicamente las hipótesis sobre el daño del sistema y como sufrió el ataque la víctima.

Método Analítico:

Objetivo: Entender el origen.

Identificar la fuente:

- Posiblemente descargada. (Un CV).

EVIDENCIA (5)											Todas las subcarpetas	Vista de
	Nombre	Tipo	Exte...	Tama...	Creado	Accesible	Modificado	MFT modificado				
1	plugin-aiEL10WT1yqYiw	File		46.041	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:23,061 PM	13/09/2011 10:21:23,061 PM				
2	aiEL10WT1yqYiw[1].pdf	File	.pdf	46.155	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:26,655 PM	01/01/1601 01:57:31,117 PM				
3	cv[1].pdf	File	.pdf	46.395	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:24,691 PM	01/01/1601 12:31:37,156 PM				
4	cv[1].pdf	File	.pdf	46.672	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:57,702 PM	01/01/1601 12:31:37,156 PM				
5	cv[1].pdf	File	.pdf	46.765	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:28,163 PM	01/01/1601 12:31:37,156 PM				

Contexto de aparición:

- Enviada por terceros, en los correos que tenía, se menciona una entrevista de trabajo, por una posible “Empresa minera” quizás le mandaron un (CV) como ejemplo de lo que gustan los currículos a la empresa y ahí inicio.

- Direcciones del posible intruso. (Dominio externo "186.73.132.237").

Sistema operativo	Nombre del archivo	Ruta de archivo	INFORMACIÓN DEL ARTEFACTO
Shim Cache	winlogon.exe	V:\NC\Users\Vissa\Documents\winlogon.exe	URL http://186.73.132.237/winlogon.exe
Shim Cache	winlogon.exe	V:\NC\Users\Vissa\Downloads\winlogon.exe	
Shim Cache	winlogon.exe	V:\NC\Users\Vissa\Documents\winlogon.exe	
MUICache	winlogon.exe	C:\Users\Vissa\Documents\winlogon.exe	
Web relacionada	winlogon[1].exe		
Registros de caché de Internet Explorer	winlogon[1].exe		
Web relacionada	winlogon[1].exe		
Registros de caché de Internet Explorer	winlogon[1].exe		
Web relacionada	winlogon[1].exe		
Registros de caché de Internet Explorer	winlogon[1].exe		
Historial de Internet Explorer		URL http://186.73.132.237/winlogon.exe	

Conceptos

1. Malware

clave:

Definición: Término general para cualquier software malicioso.

Ejemplos: Virus, gusanos, troyanos, ransomware, spyware, etc.

2. Malware por inyección

Definición: Técnica donde el malware se introduce en un sistema explotando vulnerabilidades, como inyección de código (ej. SQL, DLL, JavaScript).

Cómo funciona: Inyección SQL: Inserta comandos SQL maliciosos en entradas de bases de datos.

Inyección de DLL: Carga bibliotecas maliciosas en procesos legítimos.

Objetivo: Robar datos, tomar control o corromper sistemas.

3. Indicadores de phishing

Frases como "Join our Community" o "plan an API key" son señales de engaño.

4. Troyano (Trojan)

Definición: Malware que se disfraza de software legítimo para engañar a los usuarios y ejecutar acciones maliciosas.

5. Exploit

Definición: Código o técnica que aprovecha vulnerabilidades en software/hardware para causar comportamientos no deseados.

6. Backdoors

Definición: Punto de acceso secreto que evade los controles de seguridad para permitir acceso remoto no autorizado.

7. Rootkits

Definición: Conjunto de herramientas que ocultan procesos, archivos o privilegios de malware para mantener acceso administrativo (root) en un sistema.

Análisis estructural:

Objetivo: Detectar incoherencias.

Iniciamos por validar en VirusTotal, las primeras evidencias encontradas en Examine brindadas por la misma aplicación, las cuales son las CV.

EVIDENCIA (5)

Todas las subcarpetas Vista de

TODA LA EVIDENCIA ▶

Nombre	Tipo	Exte...	Tama...	Creado	Accesible	Modificado	MFT modificado
plugin-aiEL10WT1yqYiw	File		46.041	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:23,061 PM	13/09/2011 10:21:23,061 PM
aIEL10WT1yqYiw[1].pdf	File	.pdf	46.155	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:26,655 PM	01/01/1601 01:57:31,117 PM
cv[1].pdf	File	.pdf	46.395	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:24,691 PM	01/01/1601 12:31:37,156 PM
cv[1].pdf	File	.pdf	46.672	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:57,702 PM	01/01/1601 12:31:37,156 PM
cv[1].pdf	File	.pdf	46.765	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:28,163 PM	01/01/1601 12:31:37,156 PM

The screenshot shows the VirusTotal analysis interface. At the top, it displays a 'Community Score' of 39/60. Below this, the file name is shown as 7a274612ff5179b01fbfd1df7fc765497a5170ffd45d133b3b879a9ad3c3b11d. The file type is identified as plugin-aiEL10WT1yqYiw.pdf. The analysis summary indicates 39/60 security vendors flagged the file as malicious. The file size is 44.96 KB, and the last analysis date is 2 years ago. A PDF icon is present. Below the summary, there are tabs for DETECTION, DETAILS, and COMMUNITY. The DETAILS tab is selected, showing a table of security vendors' analysis results. The table includes columns for vendor, detection name, and status. Some entries show detections like 'Exploit.PDF-Name.2.Gen' or 'Malware@!24vds0334le2'. The COMMUNITY tab is visible below the details. The bottom of the screen shows the Windows taskbar with various pinned icons.

En esa imagen podemos encontrar un ejemplo legítimo de lo que viene siendo un malware que es:

Trojan: Win32/Emotet.D!MTB (Microsoft) vs. inventado: English/MP4-slama.Gen.

Falsificación de herramientas:

Marcas como "Claw MJ" o "Gymel" que no existen en la industria.

Análisis Técnico:

Objetivo: Buscar evidencias técnicas de manipulación o malware.

Extraer y analizar artefactos:

De las imágenes del punto anterior, podemos observar cómo nuestra evidencia parte de 5 archivos, de los cuales 4 son pdf e inclusive 3 cuentan con el mismo nombre, al usar Axiom Examine y VirusTotal, podemos obtener que cualquiera de los 5 archivos son maliciosos. Incluso al ejecutar cualquiera de estos 5, se recomienda abrir el Windows defender apenas hacer clic.

EVIDENCIA (5)

Nombre	Tipo	Extensión	Tam...	Creado	Accesible	Modificado
plugin-al10WT1yqYw	File	.pdf	46.041	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:15,577 PM	13/09/2011 10:21
cv[1].pdf	File	.pdf	46.155	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:23,280 PM	13/09/2011 11:37
cv[1].pdf	File	.pdf	46.395	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:22,550 PM	15/09/2011 11:00
cv[1].pdf	File	.pdf	46.672	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:56,202 PM	15/09/2011 11:35
cv[1].pdf	File	.pdf	46.765	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:26,788 PM	16/09/2011 04:31

VISTA PREVIA

DETALLES

TEXTO Y HEXADECIMALES

Al iniciar con la linea del tiempo, detectamos rutas que son el host de la maquina y rutas o direcciones externas, indicadores de phishing:

Frases como "Join our Community" o "plan an API key" son señales de engaño. (Referencia de VirusTotal).

39/60 security vendors flagged this file as malicious

7a274612ff5179b01fbdf1df7fc765497a5170ffd45d133b3b879a9ad3c3b11d
plugin-al10WT1yqYw

pdf js-embedded exploit autoaction invalid-xref acroform cve-2010-2883

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Con esto, podemos tener correlación con amenazas y determinar que el reporte está vinculado a softwares maliciosos.

Malware activo: Archivo asociado a software malicioso.

Método Sintético:

Al iniciar con el escenario de ataque y continuando con la investigación por la línea del tiempo, obtenemos 3 archivos importantes, el primero un winlogon.exe posiblemente externo, ya que es detectado como aplicación, otro con el mismo nombre, pero de 2 años después y un host, también ejecutable y también como aplicación.

Nombre	Tipo	Extensión	Tamaño	Creado	Accesible	Modificado
SVCHOST.EXE-135A30D8.pf	File	.pf	18.068	13/09/2011 08:25:18,078 AM	13/09/2011 08:25:18,078 AM	15/09/2011 08
winlogon.exe	File	.exe	285.696	13/07/2009 11:37:04,754 PM	13/07/2009 11:37:04,754 PM	14/07/2009 01
winlogon.exe	File	.exe	285.696	13/07/2009 11:37:04,754 PM	13/07/2009 11:37:04,754 PM	14/07/2009 01

Como se muestra en la imagen en la parte inferior derecha, podemos ver que el archivo “Winlogon” cuenta con 4 fechas, de creación, de acceso, de modificación y de modificación MFT que es la modificación de la carpeta sin necesidad del contenido como tal.

NOTA:

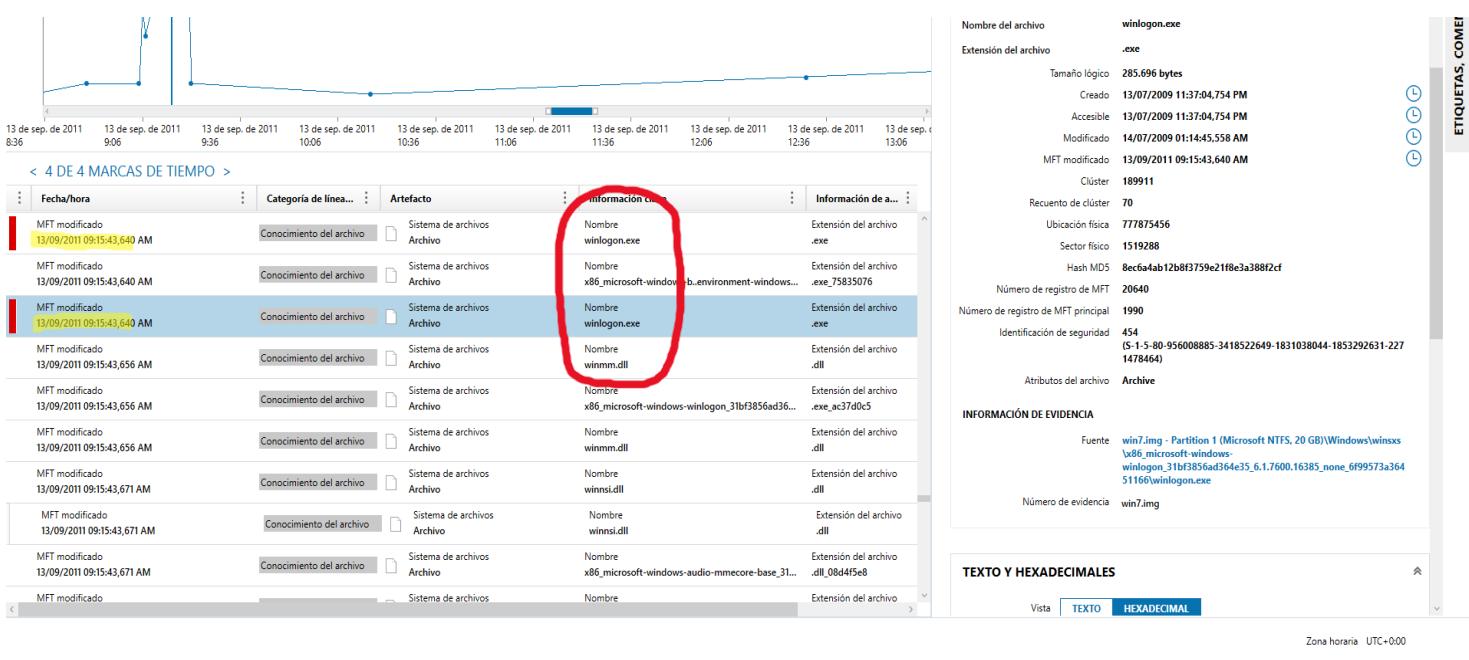
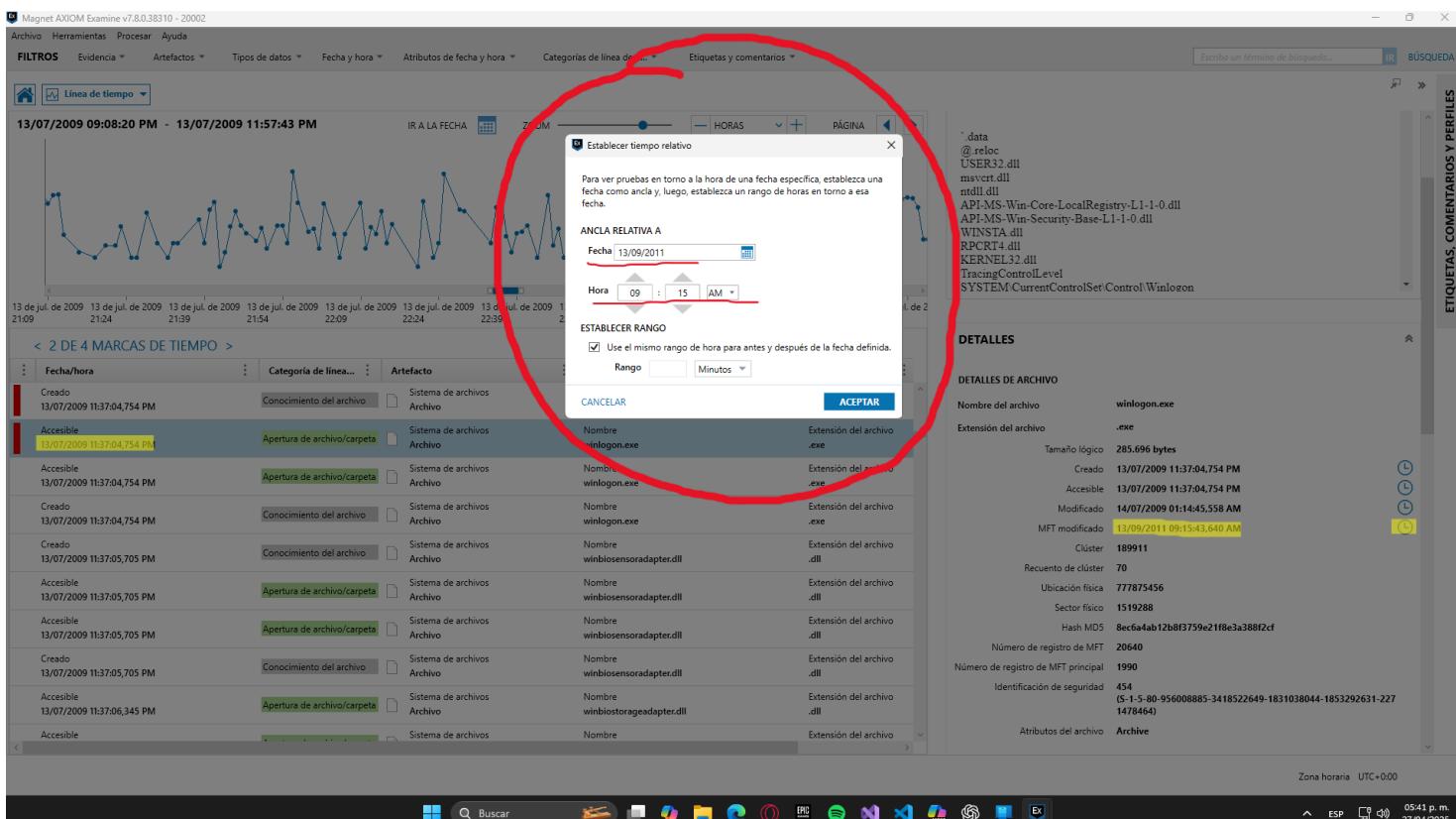
“La Fecha de Modificación MFT es clave en análisis forense para:

Identificar cambios en metadatos (no solo en contenido).

Detectar manipulación maliciosa de archivos.

Reconstruir eventos en investigaciones de seguridad.” Obtenido de: [DeepSeek - Into the Unknown](#).

Lo interesante de esto, es que si vamos a la ultima fecha, nos redirecciona a el 13 de septiembre de 2011, donde encontramos otros archivos winlogon y algunos otros sospechosos, sin ruta perteneciente al host principal, además de más evidencia que puede servirnos para más adelante. Como contraseñas, información personal, correo, descargas e historial de navegación.



Esto puede significar o relacionar el winlogon.exe corrupto con posibles inyecciones de malware como un troyano o incluso un rootkit completo.

MATERIAL DE ESTUDIO

Contamos con diversos materiales, iniciando por la imagen forense: win7.img natural para la extracción de información en Axiom process y los datos de examine y esta misma en una máquina virtual (convertida a VDI).

Utilizamos herramientas tales como: Axiom Process, Examine, kali linux y VirtualBox.

Evidencias:

Winlogon corrupto.

The screenshot shows the Magnet AXIOM Examine interface. On the left, the 'Sistema de archivos' (File System) tree view shows a mounted image named 'win7.img'. The main pane, titled 'EVIDENCIA (3)', displays a table of files found in the root directory of the image. One file, 'winlogon.exe', is highlighted in red and has its details expanded. The right side of the interface includes a preview window showing the file's contents and a 'DETALLES' (Details) panel with specific file metadata.

Nombre	Tipo	Extensión	Tamaño	Creado	Accesible	Modificado
SVCHOST.EXE-135A30D8.pf	File	.pf	18.068	13/09/2011 08:25:18,078 AM	13/09/2011 08:25:18,078 AM	15/09/2011 08:25:18,078 AM
winlogon.exe	File	.exe	285.696	13/07/2009 11:37:04,754 PM	13/07/2009 11:37:04,754 PM	14/07/2009 01:14:45,558 AM
winlogon.exe	File	.exe	285.696	13/07/2009 11:37:04,754 PM	13/07/2009 11:37:04,754 PM	14/07/2009 01:14:45,558 AM

Contraseña ¿de la VM?... (r3t0f0r3ns3)

The screenshot shows the Examine interface with the search term 'r3t0f0r3ns3' entered in the search bar. The results table on the left lists various artifacts found in the image, with several files highlighted in yellow. The right side of the interface shows detailed information for one of the highlighted files, '\$R7L60UW.txt', including its content ('r3t0f0r3ns3') and various metadata fields like name, size, and creation date.

Artefacto	Información clave	Información de apoyo	Información
Cookies talladas de recomendación...		Fuente de cookies (direct)	Última fecha/hora: 15/09/2011 10:13:13
Web relacionada		Fuente de cookies (direct)	Última fecha/hora: 15/09/2011 11:13:13
Web relacionada		Fuente de cookies (direct)	Última fecha/hora: 15/09/2011 11:13:13
Web relacionada		Fuente de cookies (direct)	Última fecha/hora: 15/09/2011 11:13:13
Web relacionada		Fuente de cookies (direct)	Última fecha/hora: 15/09/2011 11:13:13
Web relacionada		Fuente de cookies (direct)	Última fecha/hora: 15/09/2011 11:13:13
Web relacionada		Fuente de cookies (direct)	Última fecha/hora: 15/09/2011 11:13:13
Web relacionada		Fuente de cookies (direct)	Última fecha/hora: 15/09/2011 11:13:13
Web relacionada		Fuente de cookies (direct)	Última fecha/hora: 15/09/2011 11:13:13
Web relacionada		Fuente de cookies (direct)	Última fecha/hora: 15/09/2011 11:13:13
Palabra clave	firefox-3	Fuente de cookies google	Última fecha/hora: 13/09/2011 08:16:44
Palabra clave	firefox-3	Fuente de cookies bing	Última fecha/hora: 13/09/2011 08:16:44
Palabra clave	firefox-3	Fuente de cookies programatum.com	Última fecha/hora: 13/09/2011 08:16:44
Nombre de archivo	\$R7L60UW.txt	Tamaño (bytes)	544
Nombre de archivo	\$R7L60UW.txt	Tamaño (bytes)	11
Nombre de archivo	README.txt	Tamaño (bytes)	181
Nombre de archivo	TPGuestVer.txt	Tamaño (bytes)	1896
Nombre de archivo	SCHEDLGU.TXT	Tamaño (bytes)	4398
Nombre de archivo	FXSAPIDebugLogFile.txt	Tamaño (bytes)	0
Nombre de archivo	FXSTIFFDebugLogFile.txt	Tamaño (bytes)	0
Nombre de archivo	LICENSE.txt	Tamaño (bytes)	41
Nombre de archivo		Tamaño (bytes)	

PDFs maliciosos.

TODA LA EVIDENCIA ▶								
	Nombre	Tipo	Exte...	Tama...	Creado	Accesible	Modificado	MFT modificado
1	plugin-aiEL10WT1yqYiw	File		46.041	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:23,061 PM	13/09/2011 10:21:23,061 PM
2	aiEL10WT1yqYiw[1].pdf	File	.pdf	46.155	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:26,655 PM	01/01/1601 01:57:31,117 PM
3	cv[1].pdf	File	.pdf	46.395	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:24,691 PM	01/01/1601 12:31:37,156 PM
4	cv[1].pdf	File	.pdf	46.672	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:57,702 PM	01/01/1601 12:31:37,156 PM
5	cv[1].pdf	File	.pdf	46.765	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:28,163 PM	01/01/1601 12:31:37,156 PM

ANÁLISIS DEL CASO:

- La víctima descargo archivos “pdf” dañados, aparentemente lo que es un CV y uno más que podría ser parte de lo mismo del CV u otro intento con algún nombre random sin conocer como llegó a descargarse.
- Se ejecuta con dicho código malicioso.
- El archivo abre espacio a la ejecución de un Troyano que cuenta con un winlogon externo perteneciente a un dominio 186.73.132.237.
- El atacante obtiene acceso al pc de la víctima.
- Cambia la configuración de sistema y ejecuta el malware apenas se inicie el sistema.

no olvidemos que, en 2011, malware como Duqu o ZeroAccess secuestraba winlogon.exe para persistencia.

Evidencia

PDF malicioso:

Exploits en PDF reader (Que curiosamente el icono del CV es de adobe acrobat a pesar de ser PDF.).

Datos

Hasta el momento, podemos observar y obtener los siguientes datos y son, que el exploit se intentó mas de una sola vez, pues tenemos el mismo malware en el pdf en distintas fechas y algún otro pdf también con código malicioso, tenemos que a través de ellos se obtuvieron unos datos personales como lo son su correo y lo que conlleva a que sea seguramente su nombre.

Correo: miguelsalinas.listas@gmail.com

Possible nombre de la víctima: Miguel Salinas

MARCO TEÓRICO / Análisis del caso

Hasta el momento, hemos recabado información suficiente para hacer una posible hipótesis de lo sucedido.

Tenemos que examinando a win7.img nos topamos con una imagen de un disco virtual infectado con malware, trabajando con el llegamos a la sospecha de que se realizó la descarga del malware a través de un presunto CV y con ello se le dio acceso al atacante con el posible troyano, si lo desarrollamos en el mismo formato que en estudios del caso, podemos obtener lo siguiente:

Hipótesis:

Nuestra víctima de posible nombre Miguel, descargo un CV interesado en algún trabajo, sin darse cuenta de que estaba siendo víctima de malware y dando entrada a los atacantes a su máquina.

El CV se puede relacionar a la oferta de trabajo que tenía en su correo y a su vez a la descarga de Adobe Acrobat Reader para poder descargar el CV o cualquier otro PDF infectado sin que él lo supiera.

Lo que a mí me hace pensar e hilar que se le ofreció un trabajo, se le pidió que descargara un PDF dañado y para descargarlo o poderlo ejecutar, se le pidió que se instalara “Adobe Acrobat Reader”.

Elementos del hecho:

Esta persona en base a sus correos recibidos, historial de navegación y hechos observados en Axiom, descargo Adobe Acrobat Reader, tiene o tuvo en su máquina PDF infectados y también tiene ofertas de trabajo en una empresa minera, ejecuto el malware pensando que era un CV y daño su máquina.

Datos de prueba:
Su historial y descargas.
Los PDFs como evidencia en Axiom Examine por el mismo software
El winlogon de host y el de aplicación.

¿Qué necesito?

Detalles de la ejecución del malware.

Recopilación de los datos personales robados y para que.

Evidencia valida y dar con el posible atacante para llevarlo a un proceso legal.

¿Por qué paso?

Porque Miguel descargo “PDFs” infectados.

¿Quién es el responsable?

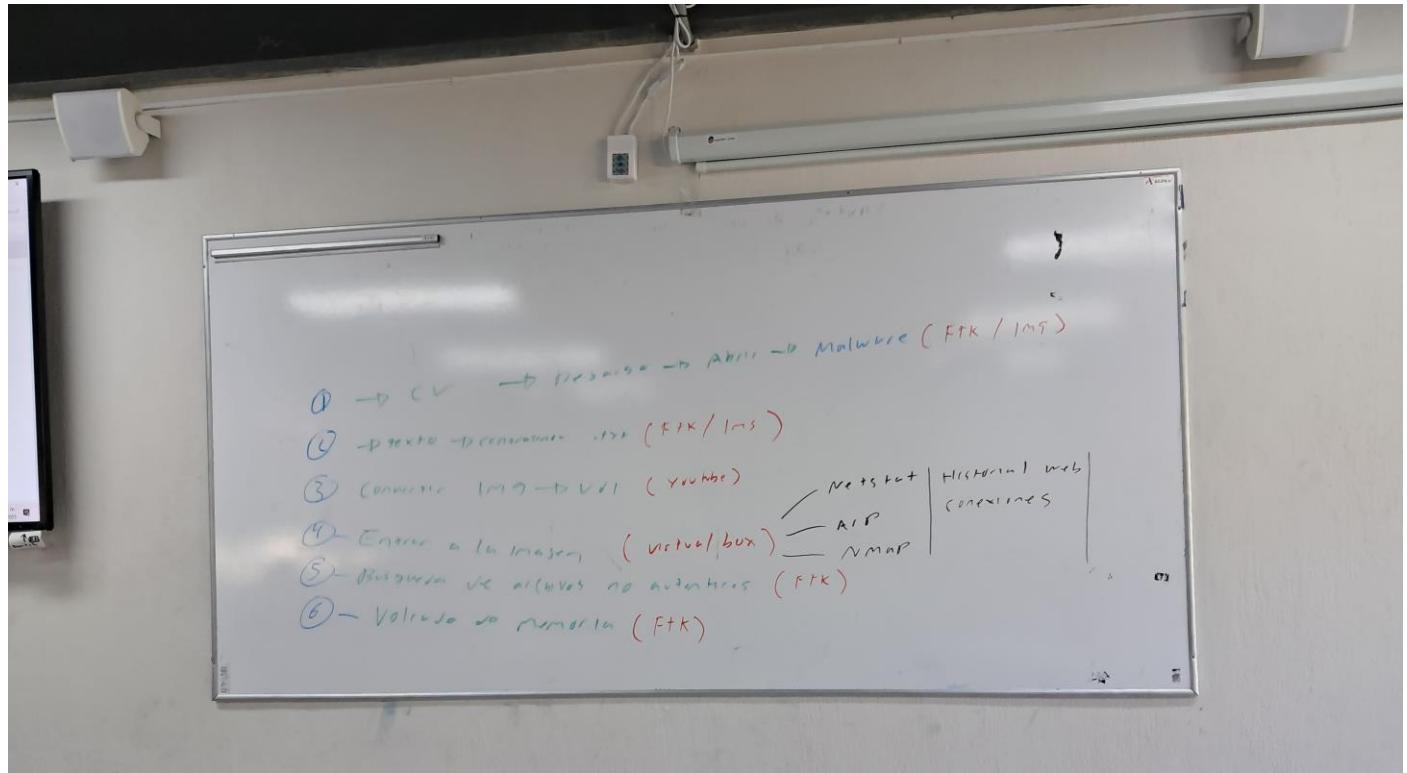
El atacante y Miguel.

¿Comó se puede prevenir?

Ahora basta con tener tu sistema actualizado y con un antivirus, en ese año desconozco cuales eran los protocolos o las medidas de seguridad, pero supongo verificar que fuese un PDF, aunque quizá para el año y si no saben del tema, mas personas como Miguel podrían caer.

Procedimiento con capturas: (Paso a Paso).

Primero, iniciamos con lo que sabíamos desde clase:



Donde contábamos con 6 puntos claves

- El CD infectado.
- El txt de la contraseña en caso de requerirse de alguna.
- La conversión de img a vdi para VB.
- La extracción de la imagen en la VB.
- La búsqueda de archivos.
- Y el volcado de memoria.

Una vez sabiendo esto, realizaríamos la mayoría de los puntos con el Axiom y con la ayuda del virtual box, los restantes.

Iniciamos cargando el caso y el img al Axiom, después, seleccionando la img y realizando el proceso de examinación hasta llegar al Examine.

The screenshot shows the Magnet AXIOM Examine v7.8.0.38310 - 2002 interface. The main window is divided into several panels:

- RESUMEN DEL CASO**: Shows Fuentes de evidencia (1) win7.img and Perspectivas (0) Posibles pistas de evidencia en la nube.
- NOTAS RESUMEN DEL CASO**: Notes about the case.
- VISIÓN GENERAL DE LA EVIDENCIA**: Displays evidence item WIN7.IMG (52.959). Details include Número de evidencia: win7.img, Descripción: , Ubicación: win7.img, Plataforma: Computadora, Método de procesamiento: Análisis y extracción. Status: No se agregó ninguna imagen.
- LUGARES PARA COMENZAR**: Categorías de artefacto: Fuente de evidencia Todas (52.961), Medios 21.973, Sistemas operativos 20.797, etc.
- ETIQUETAS Y COMENTARIOS (19)**: Includes ETIQUETAS AÑADIDAS POR REVISORES (Excepciones 7, Evidencia 5) and COMENTARIOS INCLUIDOS EN CASO (No hay más comentarios en este caso).
- COINCIDENCIAS DE IDENTIFICADORES**: Information on identifying features.

At the bottom, the taskbar shows various application icons and the system clock indicates 06:02 p.m. on 27/04/2025.

Después Analizamos la evidencia de sistema dada por la app examine (Los CVs).

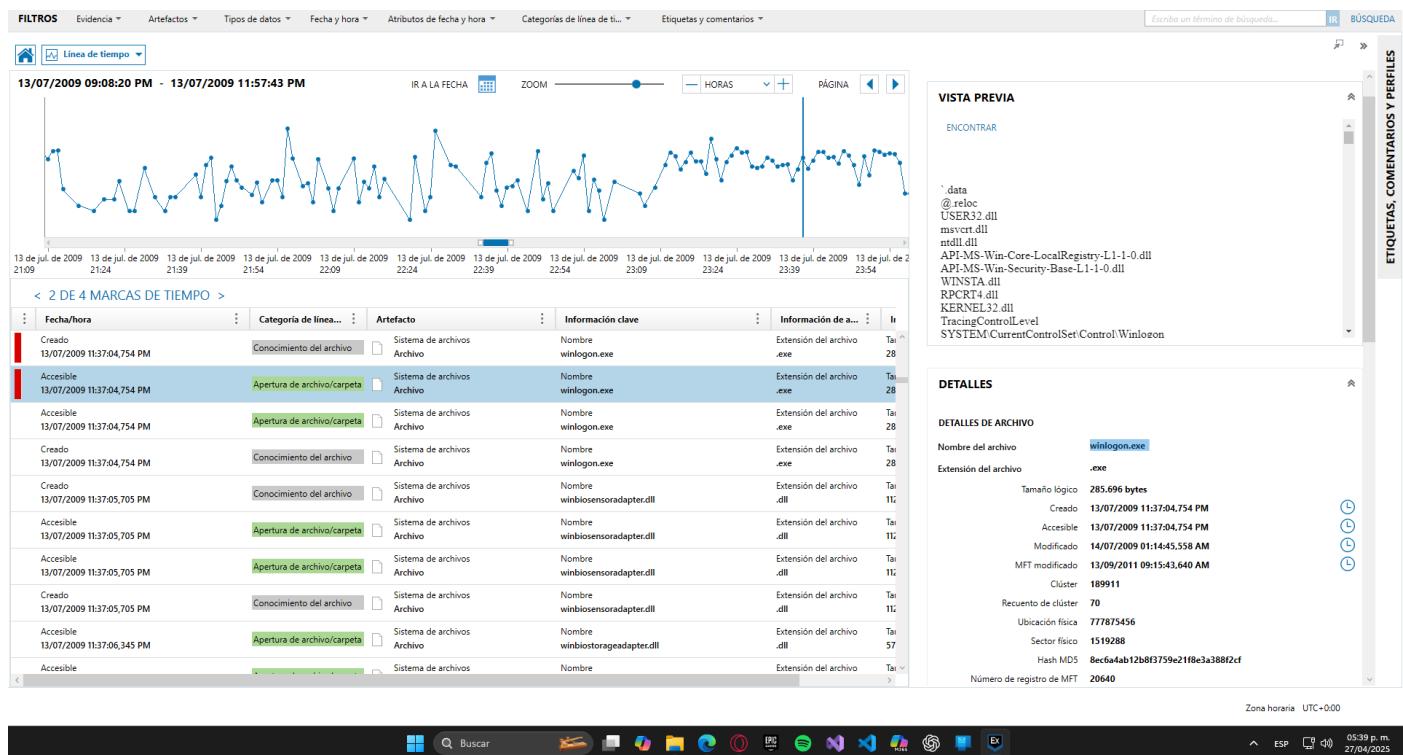
The screenshot shows the Magnet AXIOM Examine interface with the Evidence section open, displaying a list of files:

Nombre	Tipo	Exte...	Tama...	Creado	Accesible	Modificado	MFT modificado
plugin-aiEL10WT1yqYiw	File		46.041	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:23,061 PM	13/09/2011 10:21:23,061 PM
aiEL10WT1yqYiw[1].pdf	File	.pdf	46.155	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:26,655 PM	01/01/1601 01:57:31,117 PM
cv[1].pdf	File	.pdf	46.395	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:24,691 PM	01/01/1601 12:31:37,156 PM
cv[1].pdf	File	.pdf	46.672	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:57,702 PM	01/01/1601 12:31:37,156 PM
cv[1].pdf	File	.pdf	46.765	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:28,163 PM	01/01/1601 12:31:37,156 PM

Below this, a screenshot of a browser showing a VirusTotal analysis for the file 8e633276b762d774c1a81a2f9fc46adb0f3fce0c67b1c1db74c2811507baadc. The report indicates 42/65 security vendors flagged it as malicious. It provides details like file size (45.58 KB), last analysis date (5 months ago), and a PDF download link.

Luego, pasamos a la linea del tiempo, donde manualmente tenemos que buscar actividad sospechosa o directamente malwares.

Llegados al 2009, damos con lo primero, un winlogon.exe externo y con fechas diferentes, de creación, modificación etc.



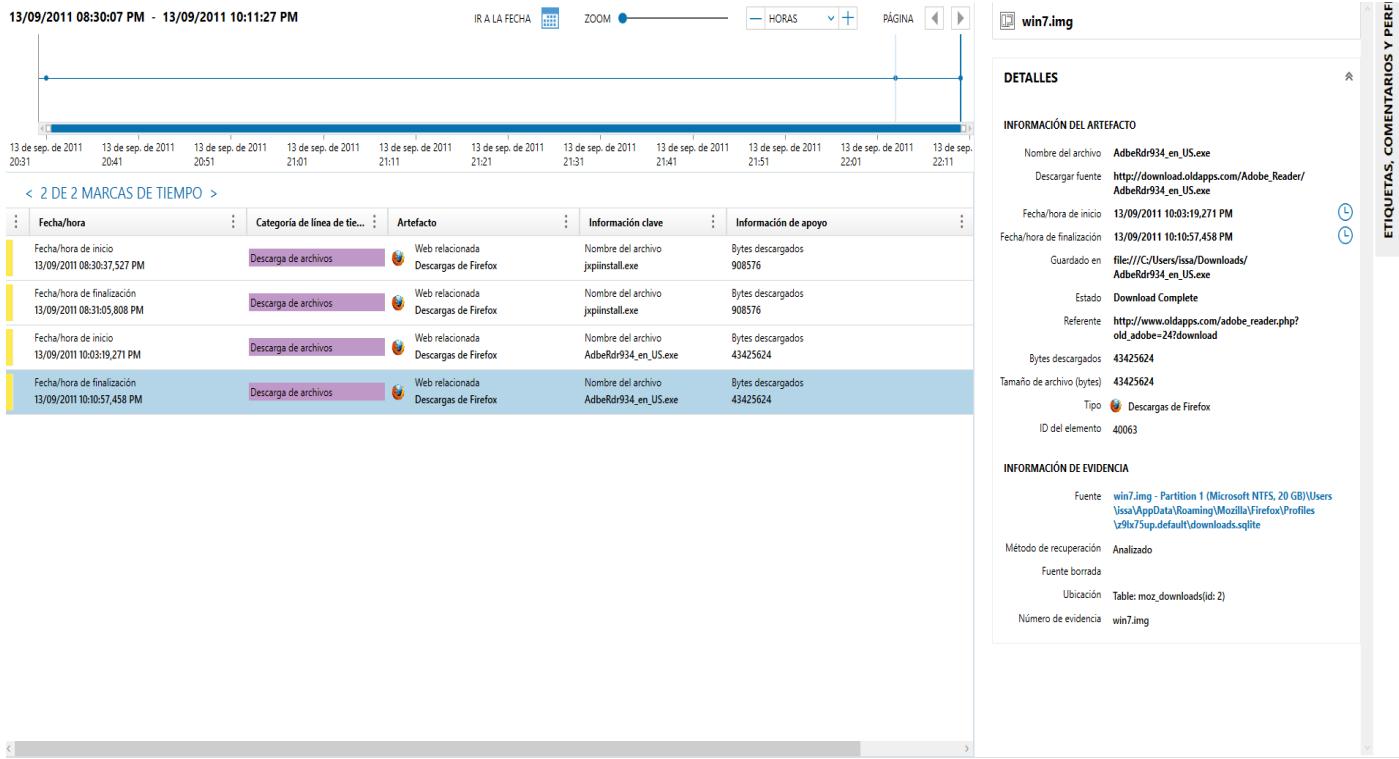
Si nos redirigimos a su fecha de modificación MFT 13 de sep de 2011 llegamos a fechas donde encontraremos mucha evidencia. (Registros web con dicho nombre “winlogon”).

The screenshot shows the EnCase Forensic interface with a search results table titled 'RESULTADOS DE COINCIDENCIA (159 de 52.961)'. The table has columns for 'Artefacto', 'Información clave', and 'Información de apoyo'.

Artefacto	Información clave	Información de apoyo
Sistema operativo Archivos de búsqueda previa de Win...	Nombre de la aplicación MSCONFIG.EXE	Ruta de la aplicación \\DEVICE\\HARDISKVOLUME1\\WINDOWS\\SYSTEM.
Sistema operativo Archivos de búsqueda previa de Win...	Nombre de la aplicación WINLOGON.EXE	Ruta de la aplicación \\DEVICE\\HARDISKVOLUME1\\USERS\\ISSA\\DOWN...
Sistema operativo Shim Cache	Nombre del archivo winlogon.exe	Ruta de archivo ???\Users\issa\Documents\winlogon.exe
Sistema operativo Shim Cache	Nombre del archivo winlogon.exe	Ruta de archivo ???\Users\issa\Downloads\winlogon.exe
Sistema operativo Shim Cache	Nombre del archivo winlogon.exe	Ruta de archivo ???\Users\issa\Documents\winlogon.exe
Sistema operativo MUICache	Nombre del archivo winlogon.exe	Ruta de archivo C:\Users\issa\Documents\winlogon.exe
e Web relacionada Registros de caché de Internet Explorer	Nombre de archivo winlogon[1].exe	Tipo de archivo exe
e Web relacionada Registros de caché de Internet Explorer	Nombre de archivo winlogon[1].exe	Tipo de archivo exe
e Web relacionada Registros de caché de Internet Explorer	Nombre de archivo winlogon[1].exe	Tipo de archivo x-msdos-program
e Web relacionada Registros de caché de Internet Explorer	Nombre de archivo winlogon[1].exe	Tipo de archivo exe
e Web relacionada Historial de Internet Explorer		URL http://186.73.132.237/winlogon.exe
e Web relacionada Historial de Internet Explorer		URL http://186.73.132.237/winlogon.exe
e Web relacionada Historial de Internet Explorer		URL http://186.73.132.237/winlogon.exe
e Web relacionada Historial de Internet Explorer		URL http://186.73.132.237/winlogon.exe
Etiquetado desde el sistema de archivos EXE	Nombre winlogon.exe	Tipo File
Etiquetado desde el sistema de archivos EXE	Nombre winlogon.exe	Tipo File

To the right of the table is a detailed view for 'http://186.73.132.237/winlogon.exe' with sections for 'DETALLES', 'INFORMACIÓN DEL ARTEFACTO', and 'INFORMACIÓN DE EVIDENCIA'.

La descarga de adobe reader.



Y los ejecutables del winlogon y el host en .exe

Magnet AXIOM Examine v7.8.0.38310 - 20002

Archivo Herramientas Procesar Ayuda

FILTROS Tamaño del archivo Fecha y hora Atributos del archivo Evidencia BORRAR FILTROS

EVIDENCIA (3)

TODA LA EVIDENCIA

Nombre	Tipo	Extensión	Tamaño	Creado	Accesible	Modificado
SVCHOST.EXE-135A30D8.pf	File	.pf	18.068	13/09/2011 08:25:18,078 AM	13/09/2011 08:25:18,078 AM	15/09/2011 08:25:18,078 AM
winlogon.exe	File	.exe	285.696	13/07/2009 11:37:04,754 PM	13/07/2009 11:37:04,754 PM	14/07/2009 01:14:45,558 AM
winlogon.exe	File	.exe	285.696	13/07/2009 11:37:04,754 PM	13/07/2009 11:37:04,754 PM	14/07/2009 01:14:45,558 AM

winlogon.exe

win7.img

VISTA PREVIA

ENCONTRAR

data
@ reloc
USER32.dll
msvcr.dll
ntdll.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
API-MS-Win-Security-Base-L1-1-0.dll
WINSTA.dll
RPCRT4.dll
KERNEL32.dll
TracingControlLevel

DETALLES

DETALLES DE ARCHIVO

Nombre del archivo: winlogon.exe
Extensión del archivo: .exe
Tamaño lógico: 285.696 bytes
Creado: 13/07/2009 11:37:04,754 PM
Accesible: 13/07/2009 11:37:04,754 PM
Modificado: 14/07/2009 01:14:45,558 AM
MFT modificado: 13/09/2011 09:15:43,640 AM

ETIQUETAS, COMENTARIOS Y PERFILES

Días después, obtenemos su historial: 15 de sep de 2011

RESULTADOS DE COINCIDENCIA (2.847 de 52.961)

Artefacto	Información clave	Información de apoyo	Información
Cookies talladas de primera visita de... argentinawarez.com	Anfitrío disqus.com	Coincidencias 1	Fecha/hora de 13/09/2011 08:
Web relacionada Cookies talladas de primera visita de... elcomercio.pe	Anfitrío elcomercio.pe	Coincidencias 1	Fecha/hora de 13/09/2011 08:
Web relacionada Cookies talladas de primera visita de... filehippo.com	Anfitrío filehippo.com	Coincidencias 1	Fecha/hora de 13/09/2011 08:
Web relacionada Cookies talladas de primera visita de... filetram.com	Anfitrío filetram.com	Coincidencias 1	Fecha/hora de 13/09/2011 08:
Web relacionada Cookies talladas de primera visita de... google.com	Anfitrío google.com	Coincidencias 1	Fecha/hora de 16/09/2011 04:
Web relacionada Cookies talladas de primera visita de... google.com	Anfitrío google.com	Coincidencias 1	Fecha/hora de 15/09/2011 10:
Web relacionada Cookies talladas de primera visita de... google.com	Anfitrío google.com	Coincidencias 1	Fecha/hora de 15/09/2011 10:
Web relacionada Cookies talladas de primera visita de... google.com	Anfitrío google.com	Coincidencias 1	Fecha/hora de 15/09/2011 11:
Web relacionada Cookies talladas de primera visita de... google.com	Anfitrío google.com	Coincidencias 1	Fecha/hora de 15/09/2011 11:
Web relacionada Cookies talladas de primera visita de... google.com	Anfitrío google.com	Coincidencias 1	Fecha/hora de 16/09/2011 04:
Web relacionada Cookies talladas de primera visita de... oldapps.com	Anfitrío oldapps.com	Coincidencias 1	Fecha/hora de 13/09/2011 08:
Web relacionada Cookies talladas de primera visita de... peru21.pe	Anfitrío peru21.pe	Coincidencias 1	Fecha/hora de 15/09/2011 08:
Web relacionada Cookies talladas de primera visita de... programatium.com	Anfitrío programatium.com	Coincidencias 1	Fecha/hora de 13/09/2011 08:
Web relacionada Cookies talladas de primera visita de... softonic.com	Anfitrío softonic.com	Coincidencias 1	Fecha/hora de 13/09/2011 08:
Web relacionada Cookies talladas de sesión de Google... argentinawarez.com	Anfitrío argentinawarez.com	Vistas de página 1	Eventos de enl... 10
Web relacionada	Anfitrío	Vistas de página	Eventos de enl... >

peru21.pe

win7.img

DETALLES

INFORMACIÓN DEL ARTEFACTO

Anfitrío	peru21.pe
Fecha/hora de creación	15/09/2011 08:57:21,000 PM
Fecha/hora de visita más reciente	15/09/2011 08:57:21,000 PM
2.º fecha/hora de visita más reciente	15/09/2011 08:57:21,000 PM
Coincidencias	1
Tipo	Cookies talladas de primera visita de Goog...
ID del elemento	40385

INFORMACIÓN DE EVIDENCIA

Fuente	win7.img - Partition 1 (Microsoft NTFS, 20 GB)\Users\issa\AppData\Roaming\Microsoft\Windows\Cookies\LowVissa@peru21[1].txt
Método de recuperación	Moldeado
Fuente borrada	
Ubicación	File Offset 89
Número de evidencia	win7.img

Zona horaria UTC+00

Los primeros dos intentos de ejecución del CV.

Magnet AXIOM Examine v7.8.0.38310 - 20002

Archivo Herramientas Procesar Ayuda

FILTROS

Tamaño del archivo

Fecha y hora

Atributos del archivo

Excepciones

BORRAR FILTROS

Escribe un término de búsqueda (solo rutas de

Sistema de archivos

TODA LA EVIDENCIA win7.img

EVIDENCIA (5)

TODA LA EVIDENCIA > win7.img

Nombre	Tipo	Extensión	Tam...	Creado	Accesible	Modificado
plugin-a1E10Wt1yqYiw	File	.pdf	46.041	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:15,577 PM	13/09/2011 10:21
a1E10Wt1yqYiw[1].pdf	File	.pdf	46.155	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:23,280 PM	13/09/2011 11:37
cv[1].pdf	File	.pdf	46.395	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:22,550 PM	15/09/2011 11:00
cv[1].pdf	File	.pdf	46.672	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:56,202 PM	15/09/2011 11:35
cv[1].pdf	File	.pdf	46.765	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:26,788 PM	16/09/2011 04:31

- Ver artefactos relacionados
- Guardar archivo/carpeta en...
- Guardar archivo/carpeta en ZIP
- Guardar selección como artefacto
- Detalles de exportación
- Abrir base de datos con...
- Abrir con
- Verifique VirusTotal
- Restablecer ancho de las columnas
- Añadir/quitar etiqueta
- Ver conexiones

cv[1].pdf

win7.img

VISTA PREVIA

DETALLES

TEXTO Y HEXADECIMALES

Vista **TEXTO** HEXADECIMAL

Fuente Users\issa\AppData\Local\Microsoft\Windows\Temporary Internet Files\cv[1].pdf Mover notificación al centro de notificaciones

Desplazamiento actual 0 Seguridad de Windows

IR A ENCONTRAR C Seguridad de Windows

00000 5 50 44 Amenazas encontradas

00009 25 90 F1 Antivirus de Microsoft Defender encontró amenazas.

00018 20 6F 62 Obtener más detalles.

00027 2F 50 61

00036 32 20 3C

...

Ignorar

Buscar

ETIQUETAS, COMENTARIOS Y PERFILES

ETIQUETAS, COMENTARIOS Y PERFILES

ETIQUETAS, COMENTARIOS Y PERFILES

LOS

correos

15/09/2011 09:22:11 PM - 15/09/2011 11:36:23 PM

IR A LA FECHA ZOOM PÁGINA

1 MARCA DE TIEMPO

Fecha/hora	Categoría de línea de tie...	Artefacto	Información clave	Información de apoyo
Fecha/hora de la última actividad	Comunicación del usuario	Correo electrónico y calendario	Correo(s) electrónico(s)	Asunto
15/09/2011 09:22:51,000 PM	Comunicación del usuario	Correo web de Gmail	El equipo de Gmail <mail-norep...	Obtener Gmail en tu teléfono móvil
Fecha/hora de la última actividad	Comunicación del usuario	Correo electrónico y calendario	Correo(s) electrónico(s)	Asunto
15/09/2011 09:23:51,000 PM	Comunicación del usuario	Correo web de Gmail	El equipo de Gmail <mail-norep...	Personaliza Gmail con colores y temas.
Fecha/hora de la última actividad	Comunicación del usuario	Correo electrónico y calendario	Correo(s) electrónico(s)	Asunto
15/09/2011 09:22:51,000 PM	Comunicación del usuario	Correo web de Gmail	El equipo de Gmail <mail-norep...	Personaliza Gmail con colores y temas.
Fecha/hora de la última actividad	Comunicación del usuario	Correo electrónico y calendario	Correo(s) electrónico(s)	Asunto
15/09/2011 09:31:21,000 PM	Comunicación del usuario	Correo web de Gmail	Head Hunter <headhunterti2011...	Oportunidad laboral en empresa minera
Fecha/hora de la última actividad	Comunicación del usuario	Correo electrónico y calendario	Correo(s) electrónico(s)	Asunto
15/09/2011 10:46:47,000 PM	Comunicación del usuario	Correo web de Gmail	Head Hunter <headhunterti2011...	Oportunidad laboral en empresa minera
Fecha/hora de la última actividad	Comunicación del usuario	Correo electrónico y calendario	Correo(s) electrónico(s)	Asunto
15/09/2011 10:46:47,000 PM	Comunicación del usuario	Correo web de Gmail	Head Hunter <headhunterti2011...	Oportunidad laboral en empresa minera
Fecha/hora de la última actividad	Comunicación del usuario	Correo electrónico y calendario	Correo(s) electrónico(s)	Asunto
15/09/2011 10:46:47,000 PM	Comunicación del usuario	Correo web de Gmail	El equipo de Gmail <mail-norep...	Importa tus contactos y el correo electrónico ante
Fecha/hora de la última actividad	Comunicación del usuario	Correo electrónico y calendario	Correo(s) electrónico(s)	Asunto
15/09/2011 11:35:44,000 PM	Comunicación del usuario	Correo web de Gmail	El equipo de Gmail <mail-norep...	Importa tus contactos y el correo electrónico ante
Fecha/hora de la última actividad	Comunicación del usuario	Correo electrónico y calendario	Correo(s) electrónico(s)	Asunto
15/09/2011 11:35:44,000 PM	Comunicación del usuario	Correo web de Gmail	Head Hunter <headhunterti2011...	Oportunidad laboral en empresa minera

win7.img

DETALLES

INFORMACIÓN DEL ARTEFACTO

Correo(s) electrónico(s)	Head Hunter <headhunterti2011@gmail.com>
Asunto	Oportunidad laboral en empresa minera
Fecha/hora enviada - hora local	15 de septiembre de 2011 16:31
Fecha/hora de la última actividad	15/09/2011 11:35:44,000 PM
Fragmento	Estimado señor, hemos revisado su hoja de vida y tenemos interés en realizarle una entrevista ...
Estado	Read
Tipo	Correo web de Gmail
ID del elemento	42145

INFORMACIÓN DE EVIDENCIA

Fuente	win7.img - Partition 1 (Microsoft NTFS, 20 GB)\Users\Visa\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content\IE3\4XDW209\mail[1].htm
Método de recuperación	Moldeado
Fuente borrada	
Ubicación	File Offset 26149
Número de evidencia	win7.img

Zona horaria UTC+0:00

Y lo que aparentemente son ejecuciones de correo, donde se pueden obtener sus datos.

FILTROS Evidencia ▾ Artefactos ▾ Tipos de datos ▾ Fecha y hora ▾ Atributos de fecha y hora ▾ Categorías de línea de tie... ▾ Etiquetas y comentarios ▾ mail x listas@gmail x BORRAR FILTROS Escribe un término de búsqueda... IN BÚSQUEDA

Línea de tiempo ▾

15/09/2011 09:51:08 PM - 23/09/2011 05:26:50 PM

IR A LA FECHA ZOOM PÁGINA

< 1 DE 2 MARCAS DE TIEMPO >

Fecha/hora	Categoría de línea de tie...	Artefacto	Información clave	Información de apoyo
Fecha/hora creada	Uso del navegador	Web relacionada	Anfitrón mail.google.com/mail	Nombre gmailchat
15/09/2011 10:46:52,215 PM	Uso del navegador	Cookies de Internet Explorer	mail.google.com/mail	
Última fecha/hora modificada	Apertura de archivo/carpeta	Documentos	Nombre de archivo mail[1].txt	Tamaño (bytes) 10520
15/09/2011 10:47:06,000 PM	Apertura de archivo/carpeta	Documentos	Nombre de archivo mail[1].txt	Tamaño (bytes) 10520
Última fecha/hora de acceso	Apertura de archivo/carpeta	Documentos	Nombre de archivo mail[1].txt	Tamaño (bytes) 10520
15/09/2011 10:47:06,000 PM	Apertura de archivo/carpeta	Documentos	Nombre de archivo mail[1].txt	Tamaño (bytes) 10520
Fecha/hora creada	Conocimiento del archivo	Documentos	Nombre de archivo mail[1].txt	Tamaño (bytes) 10520
15/09/2011 10:47:06,000 PM	Conocimiento del archivo	Documentos	Nombre de archivo mail[1].txt	Tamaño (bytes) 10520
Última fecha/hora modificada	Apertura de archivo/carpeta	Documentos	Nombre de archivo mail[1].txt	Tamaño (bytes) 10527
15/09/2011 10:47:09,000 PM	Apertura de archivo/carpeta	Documentos	Nombre de archivo mail[1].txt	Tamaño (bytes) 10527
Última fecha/hora de acceso	Apertura de archivo/carpeta	Documentos	Nombre de archivo mail[1].txt	Tamaño (bytes) 10527
15/09/2011 10:47:09,000 PM	Apertura de archivo/carpeta	Documentos	Nombre de archivo mail[1].txt	Tamaño (bytes) 10527
Fecha/hora creada	Conocimiento del archivo	Documentos	Nombre de archivo mail[1].txt	Tamaño (bytes) 10527
15/09/2011 10:48:53,000 PM	Conocimiento del archivo	Documentos	Nombre de archivo issa@mail.google[1].txt	Tamaño (bytes) 116
Última fecha/hora de acceso	Apertura de archivo/carpeta	Documentos	Nombre de archivo issa@mail.google[1].txt	Tamaño (bytes) 116
15/09/2011 11:03:19,000 PM	Apertura de archivo/carpeta	Documentos	Nombre de archivo issa@mail.google[1].txt	Tamaño (bytes) 116
Última fecha/hora modificada	Apertura de archivo/carpeta	Documentos	Nombre de archivo issa@mail.google[1].txt	Tamaño (bytes) 116
15/09/2011 11:03:19,000 PM	Apertura de archivo/carpeta	Documentos	Nombre de archivo issa@mail.google[1].txt	Tamaño (bytes) 116
Fecha/hora creada	Uso del navegador	Web relacionada	Anfitrón mail.google.com/mail	Nombre gmailchat
15/09/2011 11:35:47,007 PM	Uso del navegador	Cookies de Internet Explorer	mail.google.com/mail	

win7.img

DETALLES

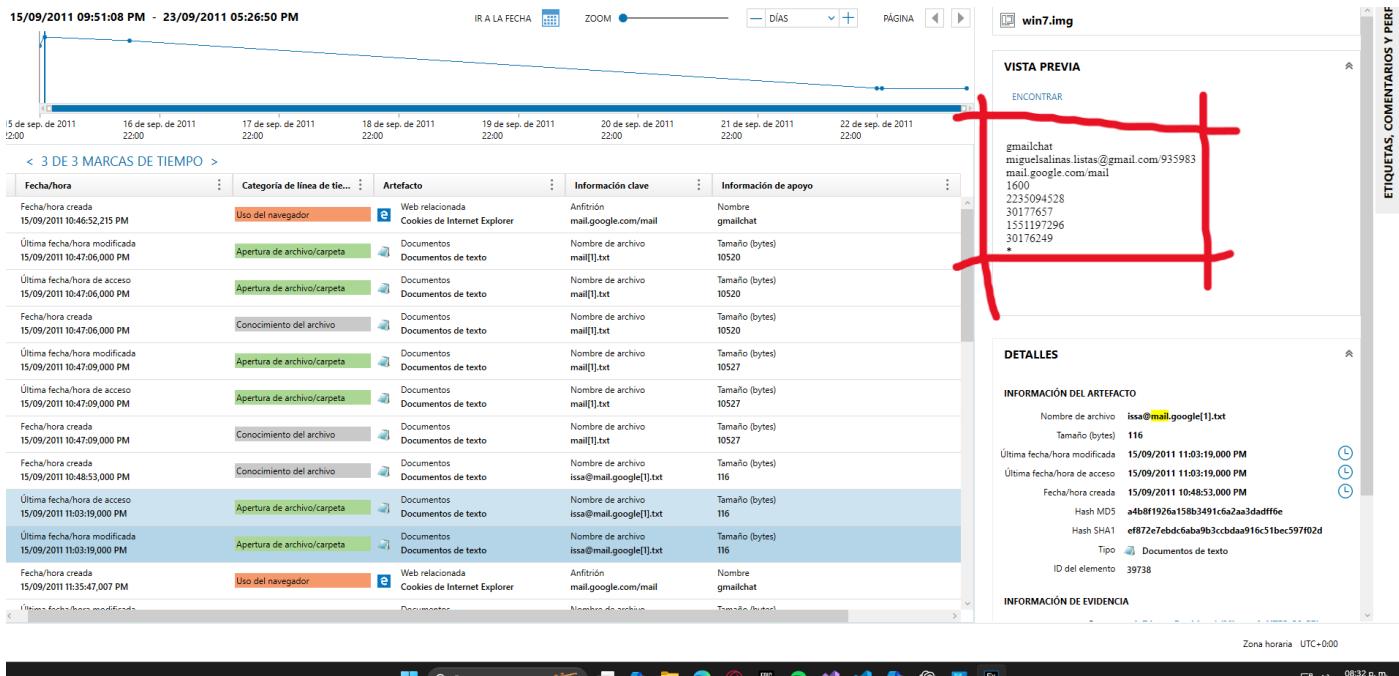
INFORMACIÓN DEL ARTEFACTO

Artefacto	mail.google.com/mail
Nombre	gmailchat
Valor	miguelasalinas.listas@gmail.com/935983
Fecha/hora creada	15/09/2011 10:46:52,215 PM
Fecha/hora de caducidad	22/09/2011 10:46:52,000 PM
Etiquetas	1600
Tipo	Cookies de Internet Explorer
ID del elemento	39739

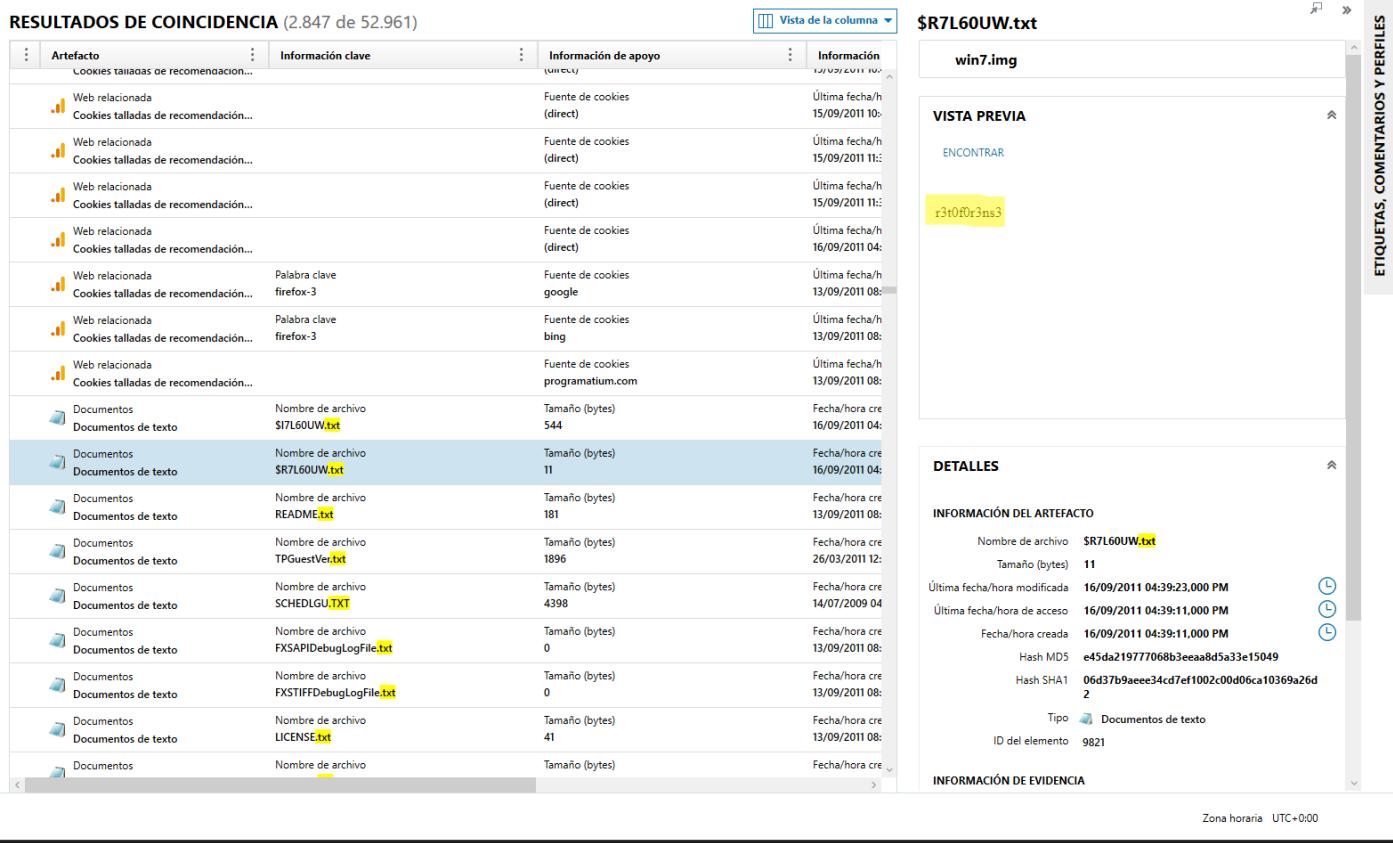
INFORMACIÓN DE EVIDENCIA

Fuente	win7.img - Partition 1 (Microsoft NTFS, 20 GB)\Users\Visa\AppData\Roaming\Microsoft\Windows\Cookies\LowVisa@mail.google[1].txt
Método de recuperación	Analizado
Fuente borrada	
Ubicación	File Offset 0
Número de evidencia	win7.img

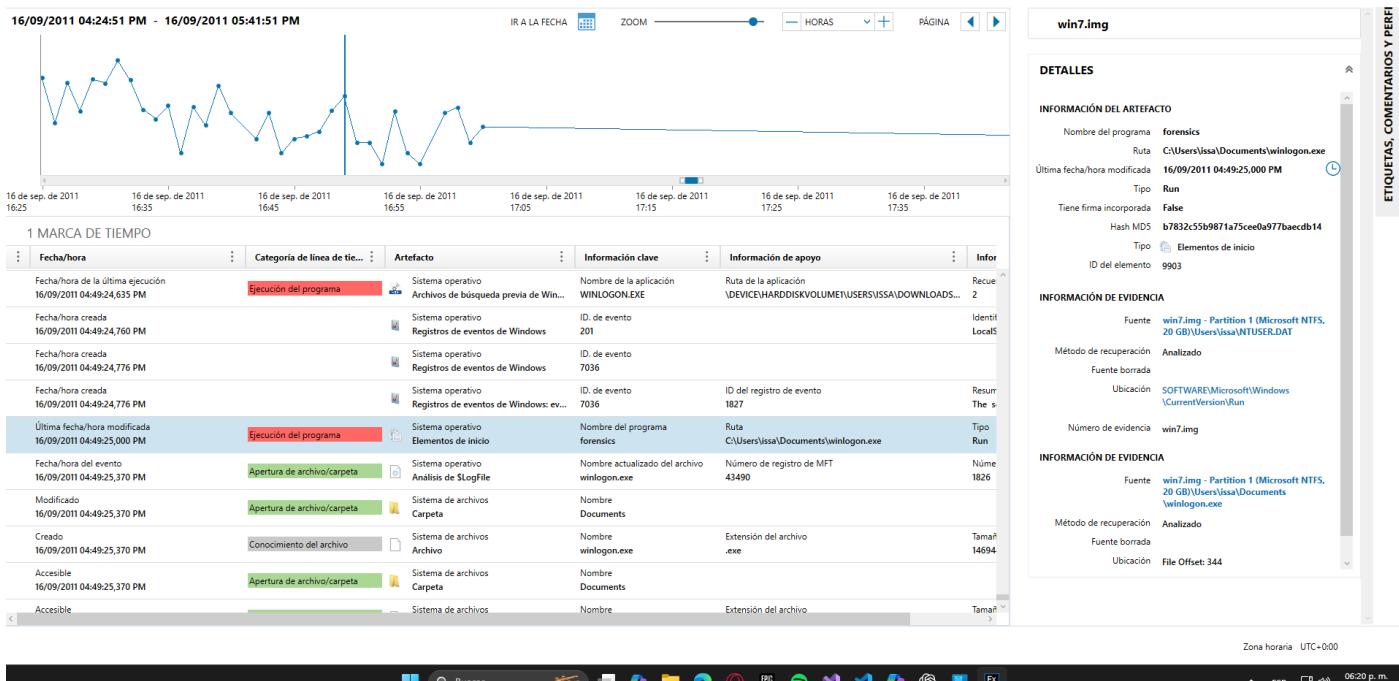
Zona horaria UTC+0:00



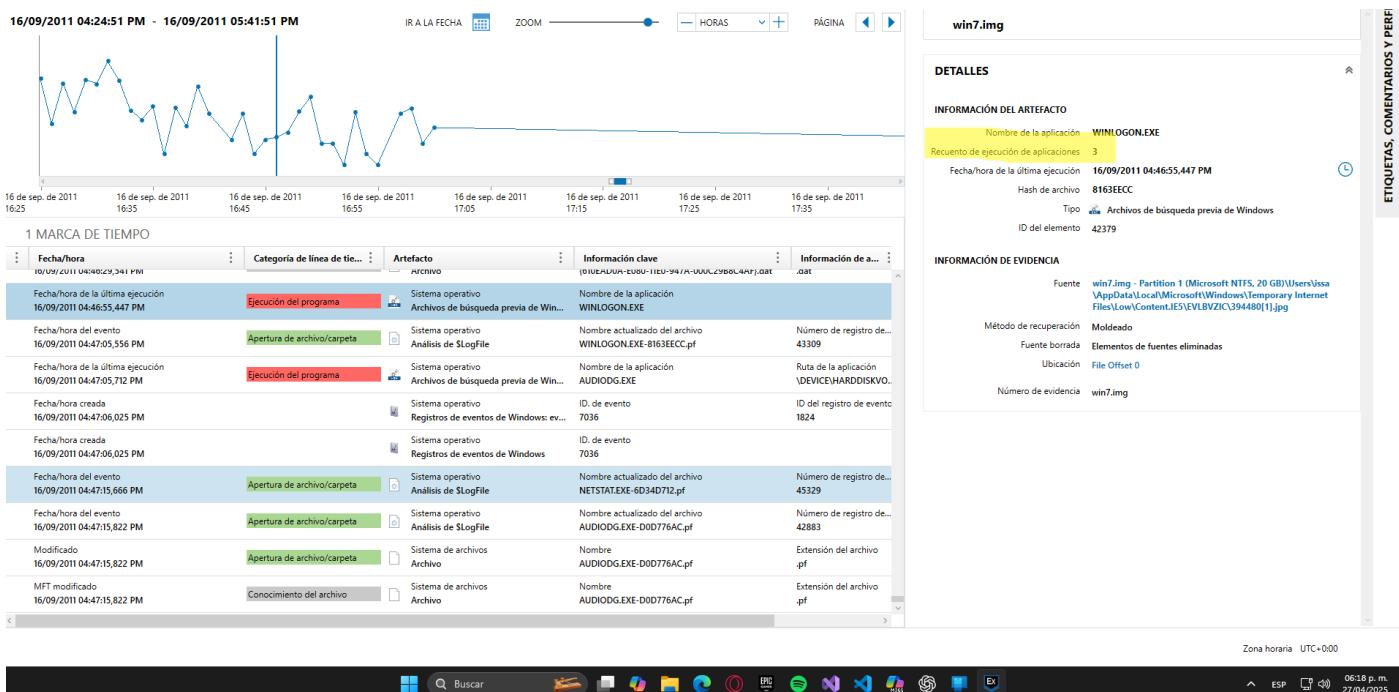
Pasando así al último día revisado el 16 de sep de 2011 obteniendo la contraseña para abrir el vdi en la máquina virtual.



Encontrando un programa llamado forensics que viene desde la ruta del winlogon ejecutable.



y por ultimo, un winlogon ejecutando 3 aplicaciones:

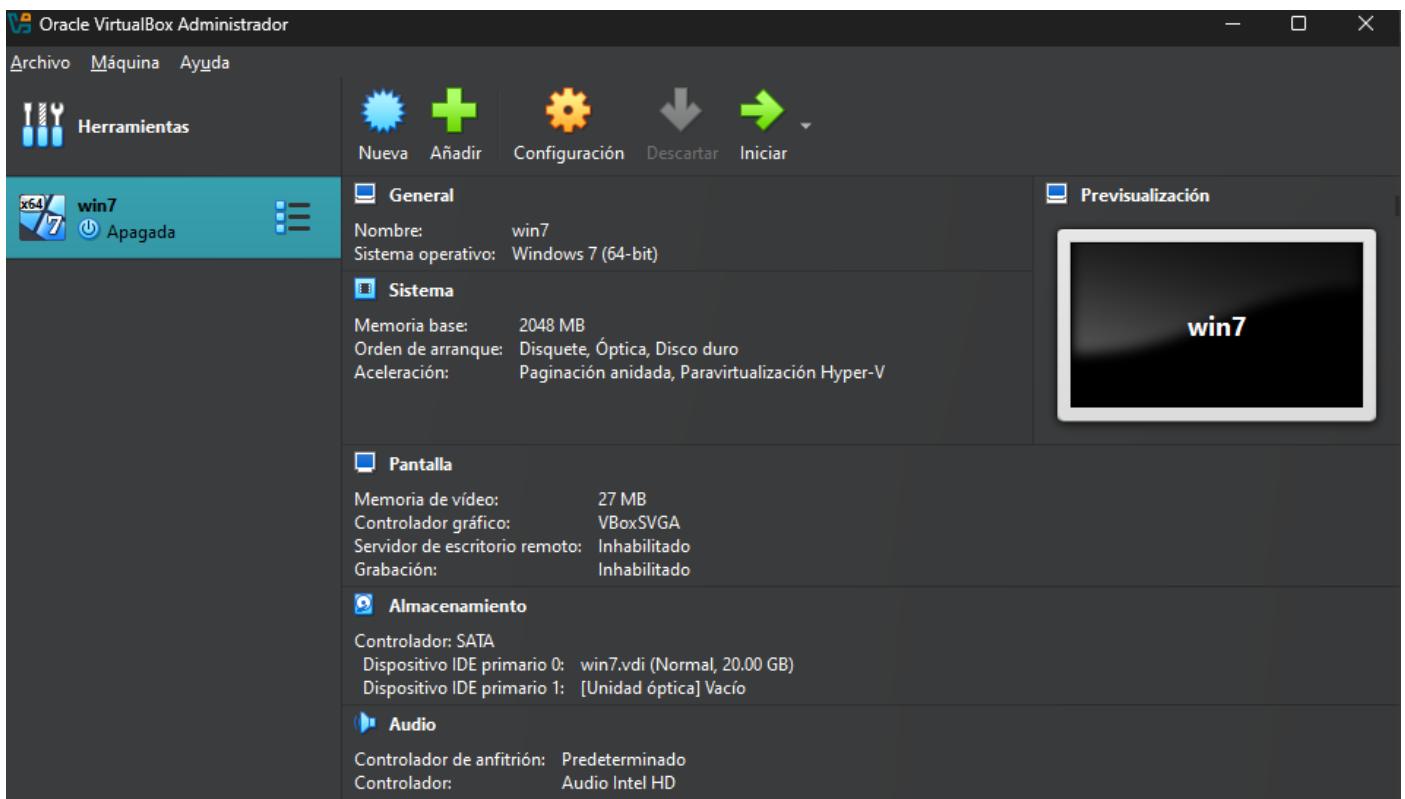


Despues de ello, pasamos a la maquina virtual, que para convertir la img a vdi necesitamos:
entrar a la siguiente ruta desde CMD:
C:\Program Files\Oracle\VirtualBox>vboxmanage
C:\Users\CDHI9\OneDrive\Documentos\Ciberseguridad\win7.img
C:\Users\CDHI9\OneDrive\Documentos\Ciberseguridad\win7.vdi

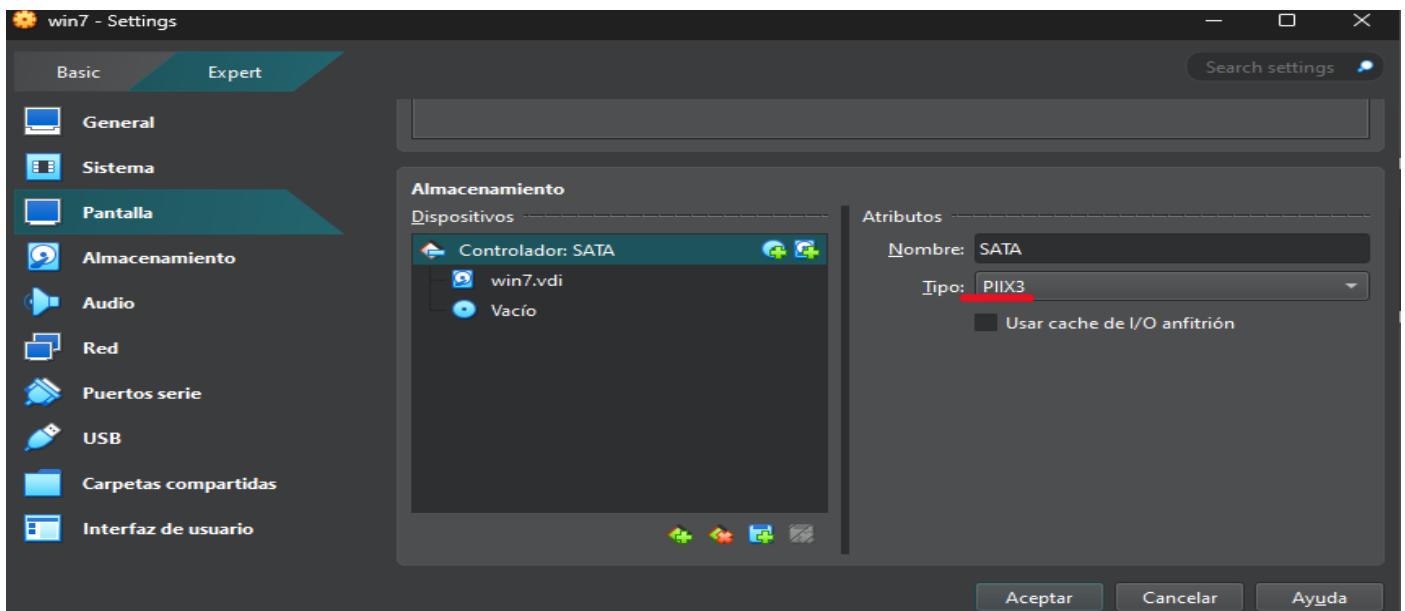
Lo que convertira a vdi:

win7		16/03/2025 10:14 p. m.	Archivo de image...	20,970,496 ...
win7		15/04/2025 09:03 p. m.	Virtual Disk Image	9,768,960 KB

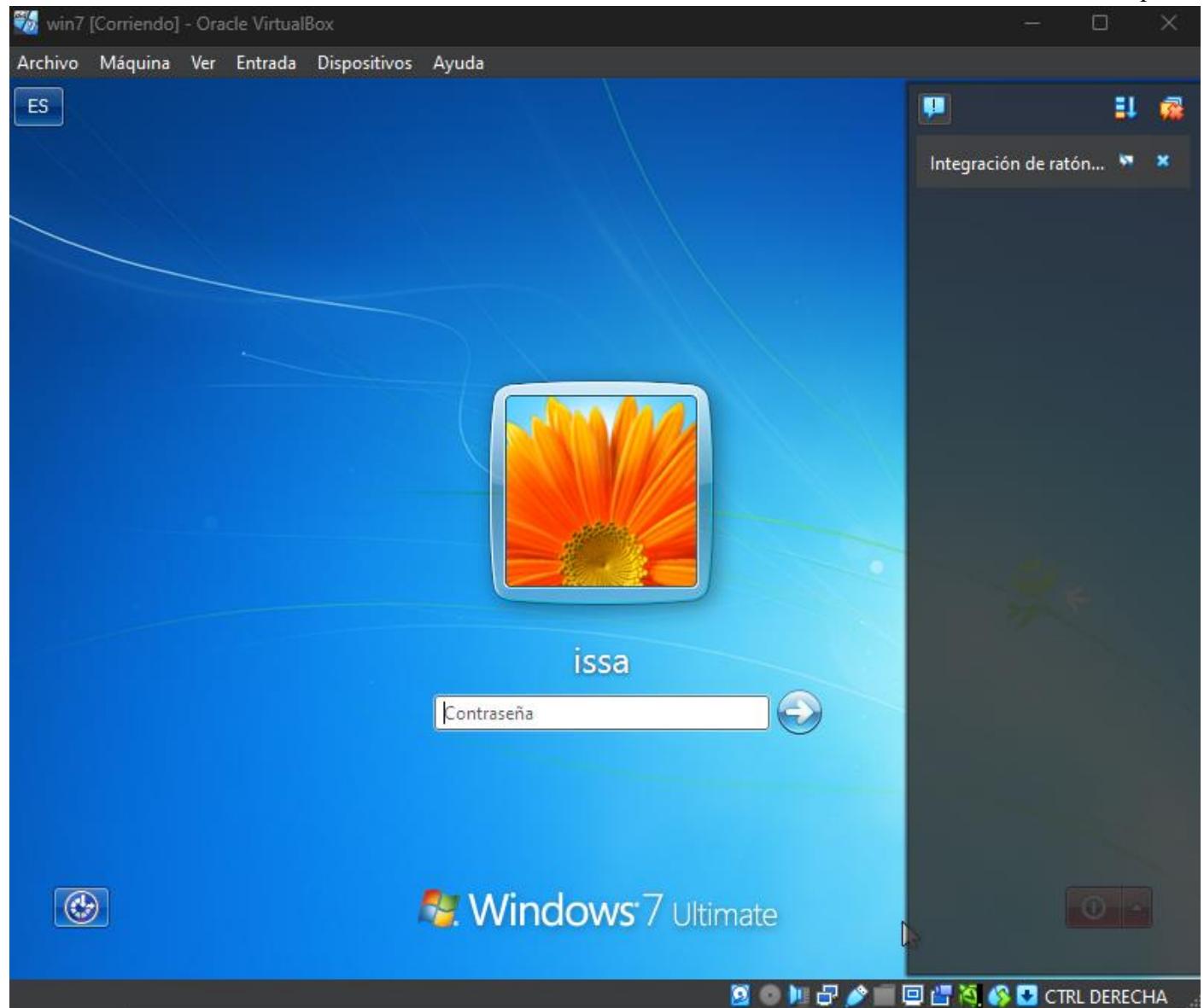
Despues, ejecutamos la VM:



Nota: si intentamos correrla sin más, nos dará un problema, ya que es un reconvertido de img a vdi, pero solo necesitamos entrar a configuración, pantalla, y cambiar el tipo a "PIIX3" y será la solución:

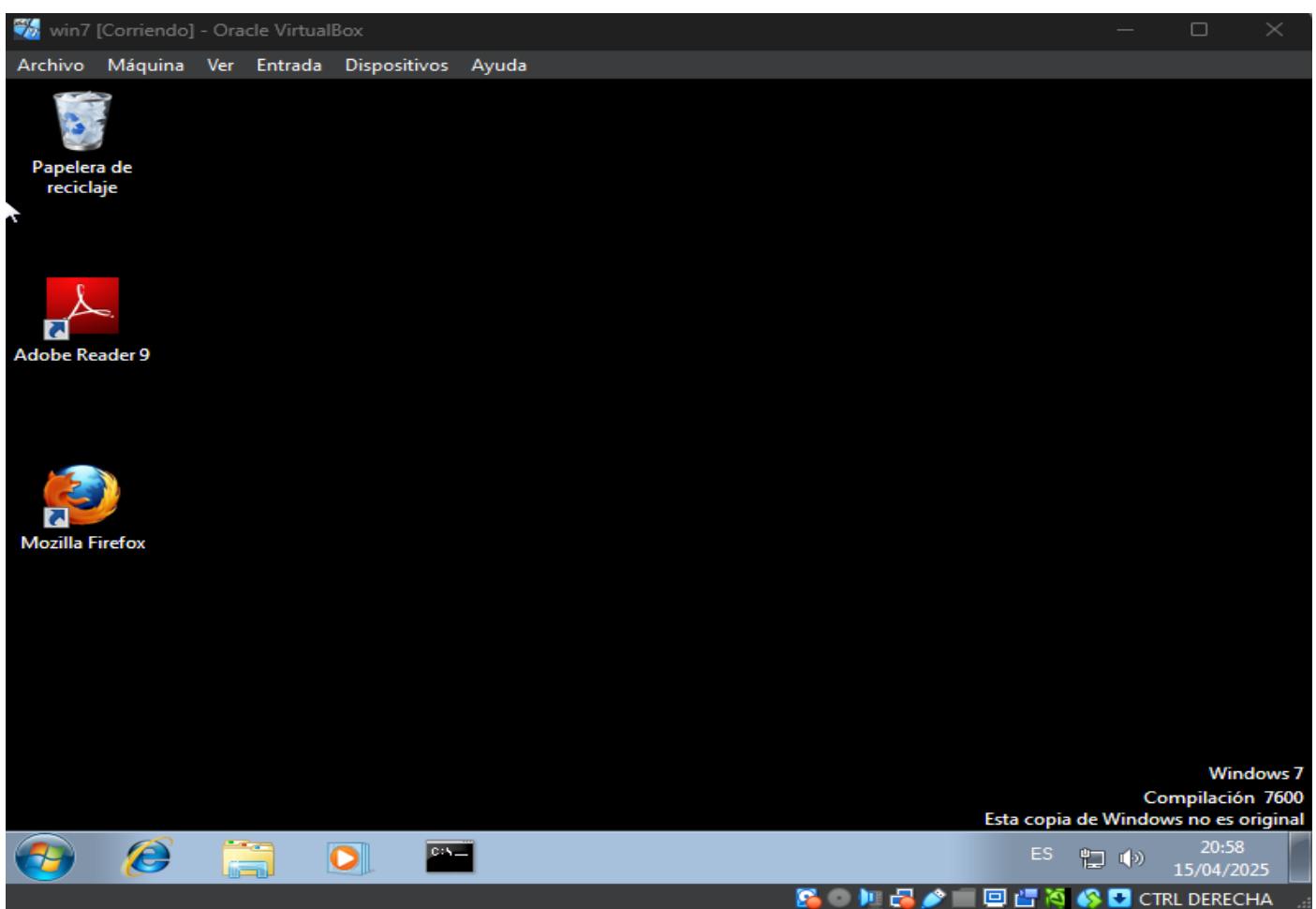
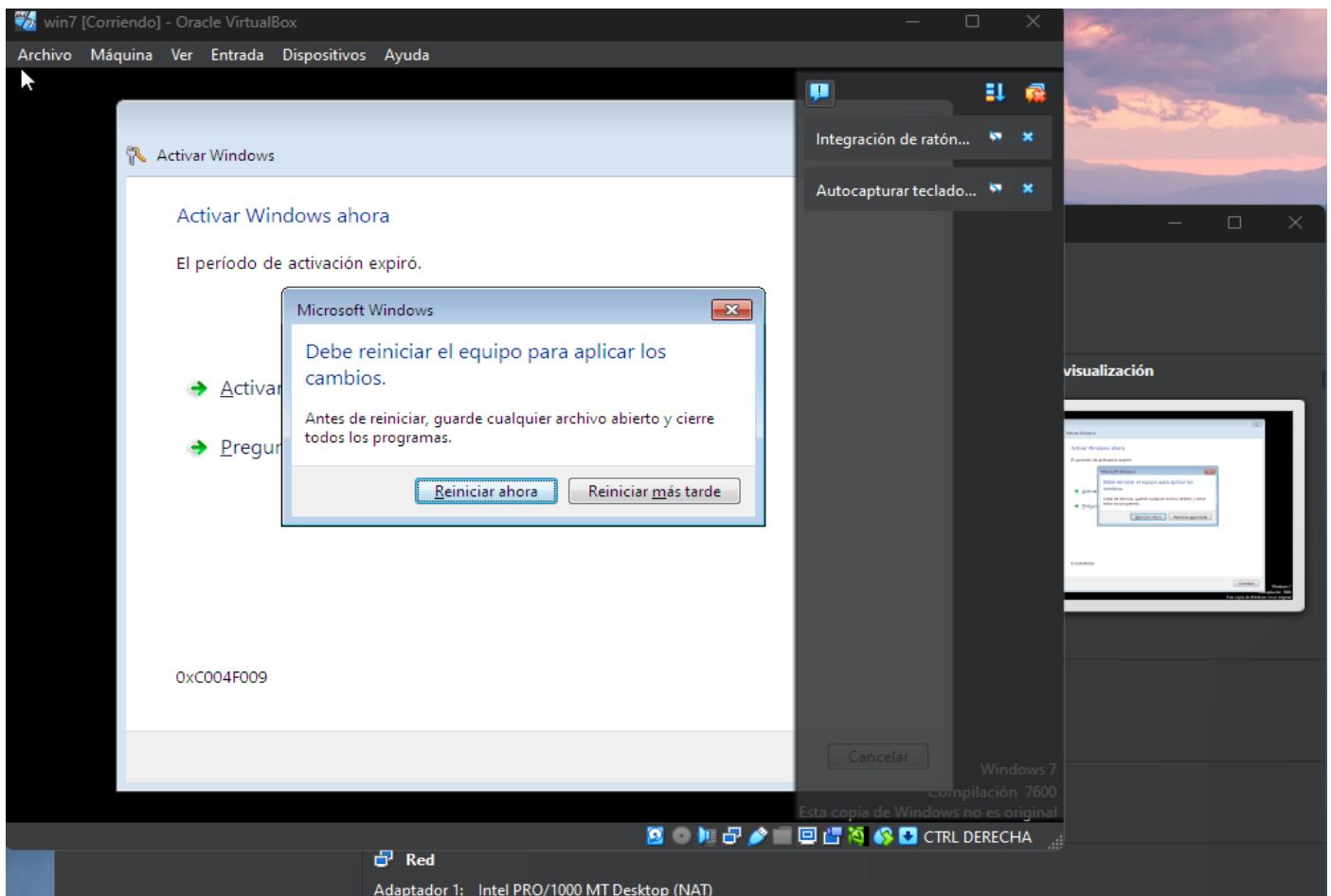


Corremos con normalidad la maquina:



E iniciamos sesión con la contraseña obtenida:

“r3t0f0r3ns3”



Ejecutamos algunos de los comandos recomendados en clase: netstats y arp.

win7 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Símbolo del sistema

Conexiones activas

Proto	Dirección local	Dirección remota	Estado	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	640
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	364
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	692
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	848
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	456
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING	464
TCP	10.0.2.15:139	0.0.0.0:0	LISTENING	4
TCP	[::]:135	[::]:0	LISTENING	640
TCP	[::]:445	[::]:0	LISTENING	4
TCP	[::]:49152	[::]:0	LISTENING	364
TCP	[::]:49153	[::]:0	LISTENING	692
TCP	[::]:49154	[::]:0	LISTENING	848
TCP	[::]:49155	[::]:0	LISTENING	456
TCP	[::]:49156	[::]:0	LISTENING	464
UDP	0.0.0.0:5355	***		1120
UDP	10.0.2.15:137	***		4
UDP	10.0.2.15:138	***		4
UDP	10.0.2.15:1900	***		800
UDP	127.0.0.1:1900	***		800
UDP	127.0.0.1:65404	***		800
UDP	[::]:5355	***		1120
UDP	[::]:1900	***		800
UDP	[::]:65403	***		800
UDP	[fe80::8002:5de3:d5ac:17f2%14]:1900	***		800

C:\Users\issa>arp -a

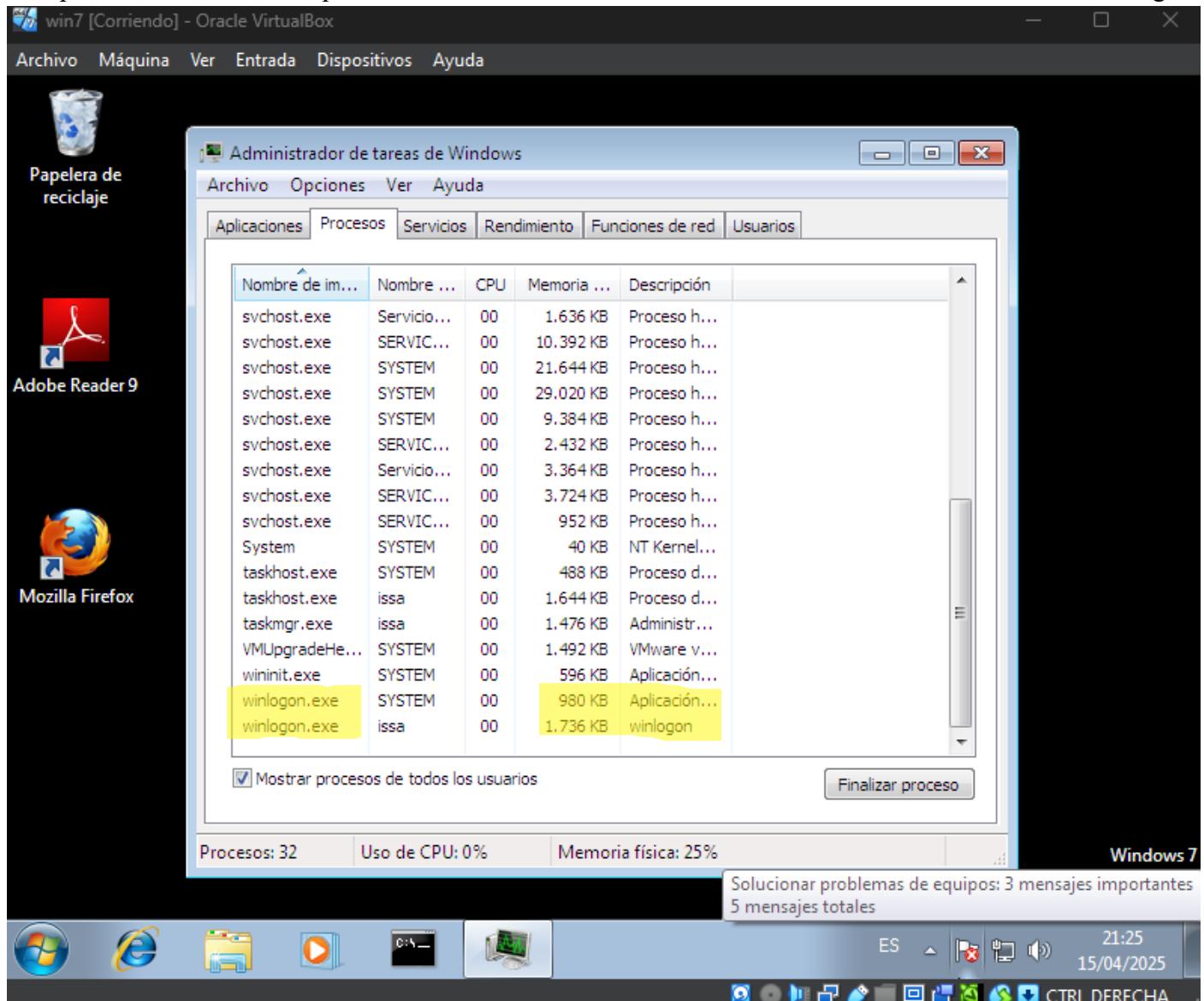
Interfaz: 10.0.2.15 --- 0xe

Dirección de Internet	Dirección física	Tipo
10.0.2.2	52-55-0a-00-02-02	dinámico
10.0.2.3	52-55-0a-00-02-03	dinámico
10.0.2.255	ff-ff-ff-ff-ff-ff	estático
224.0.0.22	01-00-5e-00-00-16	estático
224.0.0.252	01-00-5e-00-00-fc	estático
255.255.255.255	ff-ff-ff-ff-ff-ff	estático

Windows 7
Compilación 7600
Esta copia de Windows no es original

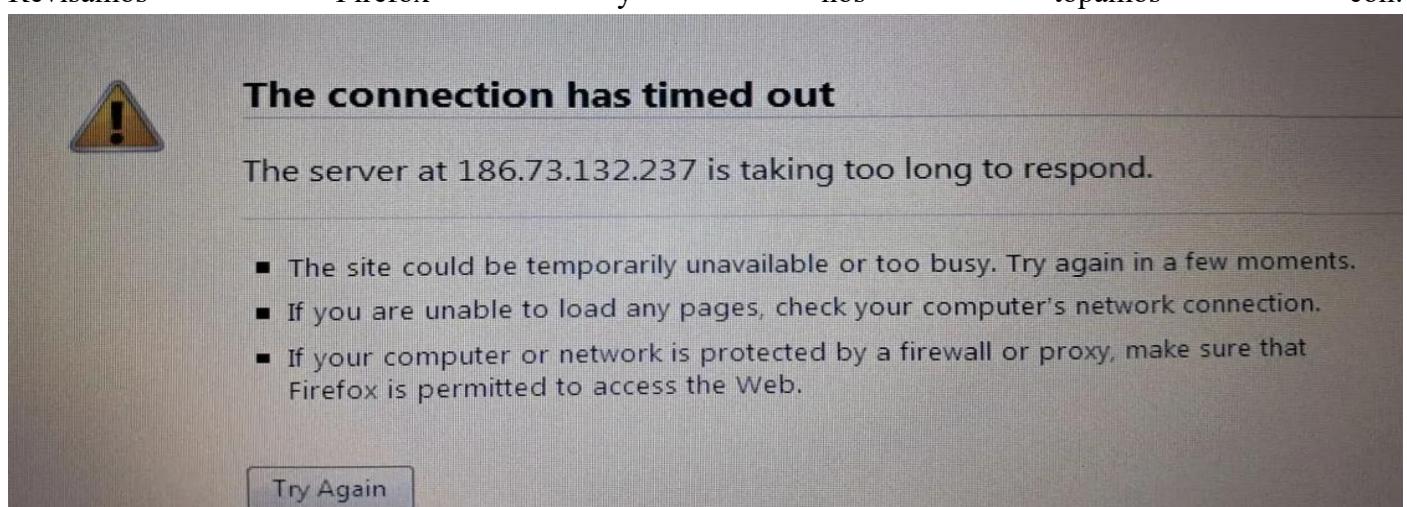
ES 3:10

Comprobamos que existen los dos winlogon:



Intentamos otros comandos para verificar la conexión con el atacante, pues los puertos de arp y netstats no coinciden con el puerto del malware.

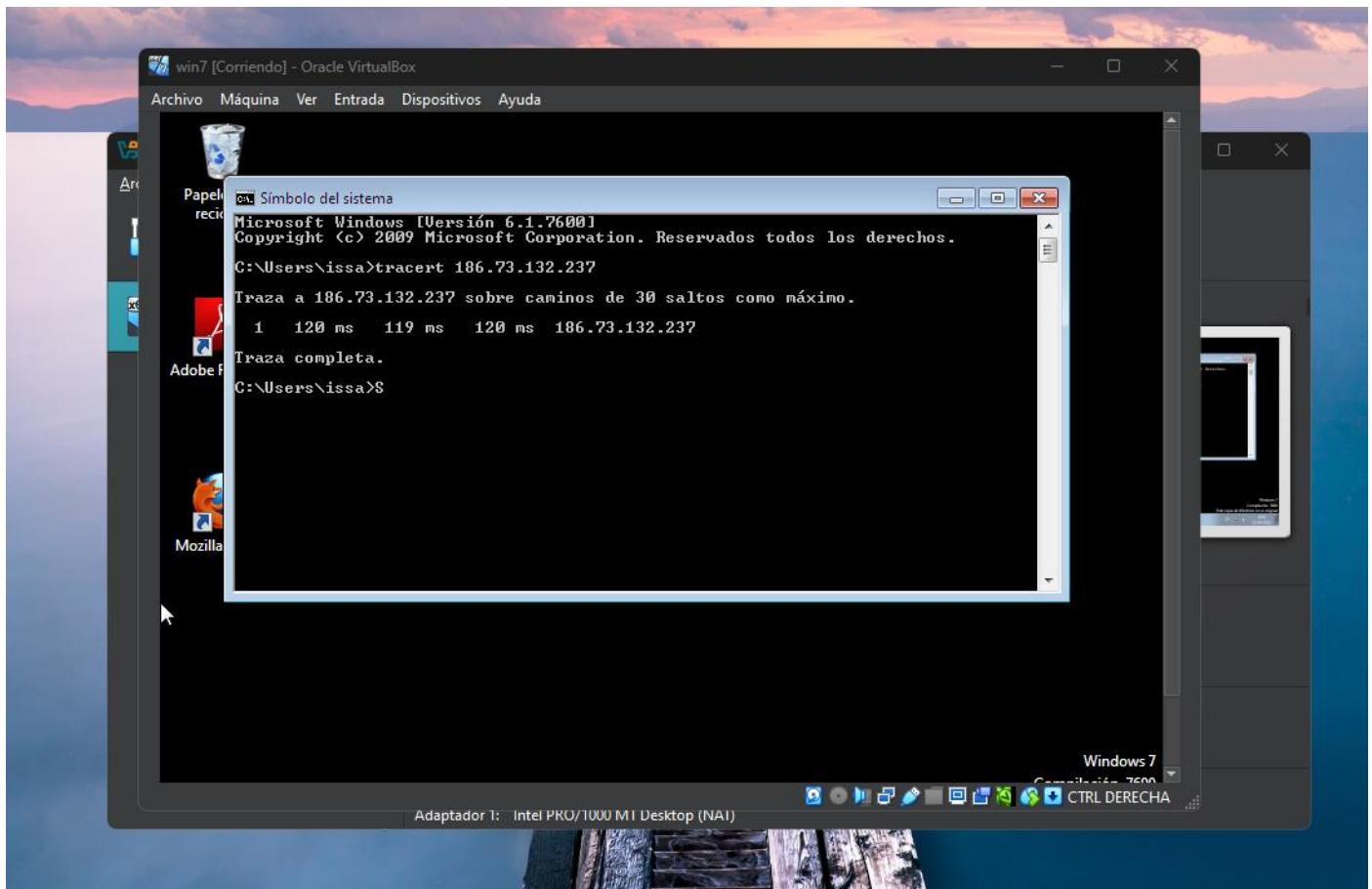
Revisamos Firefox y nos topamos con:



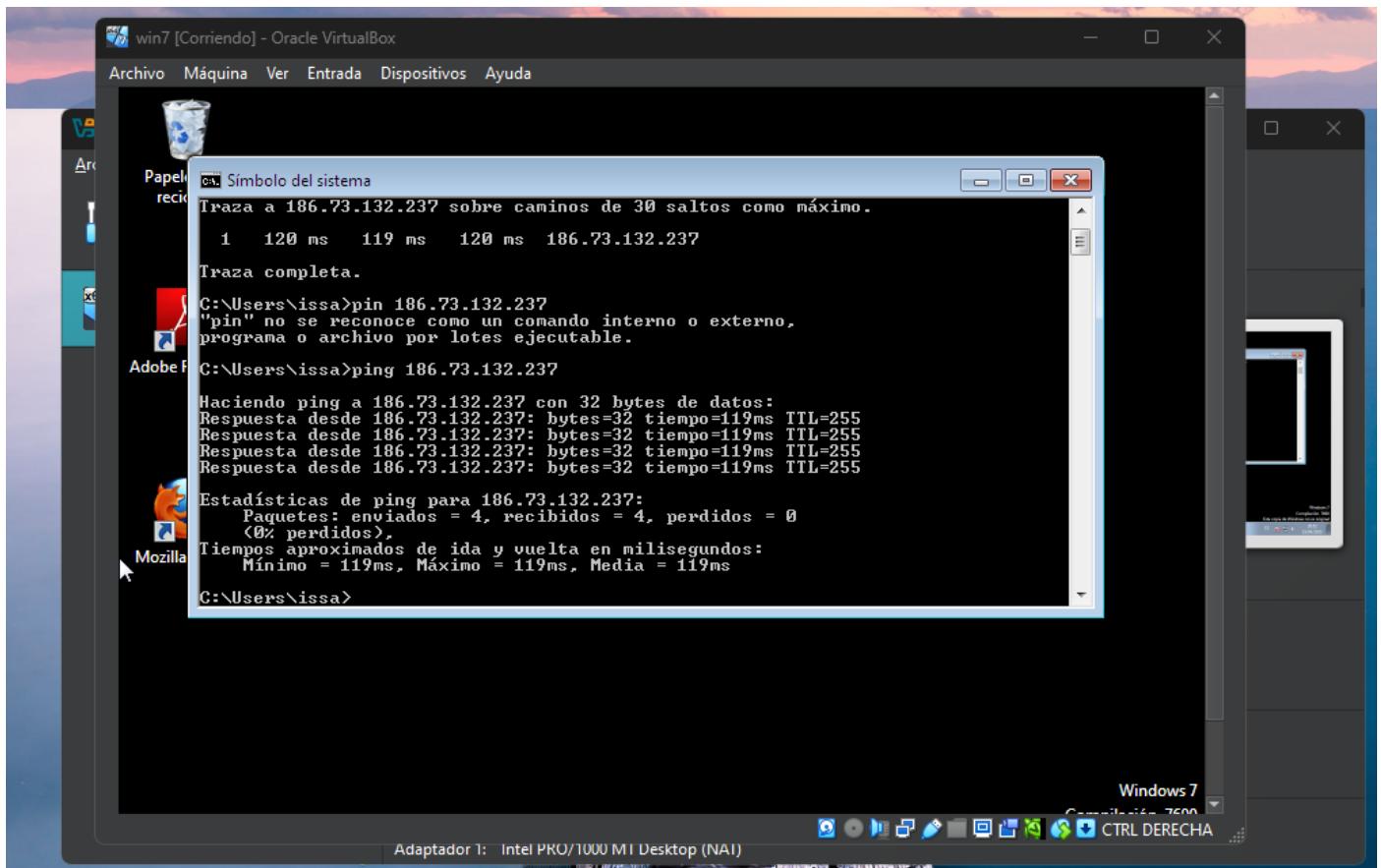
PRUEBAS DE CONEXIÓN REMOTA

Objetivo: Demostrar si hubo acceso remoto al sistema.

Como podemos ver en la máquina virtual y su navegador, existen los dos winlogon y si existe una conexión a otro servidor, a otro host, entonces podemos intentar nuevas maneras de ver si hay conexión con este, probando a trazo directo a dicho server y ver si hay caminos hacia el, con el comando tracert y seguido del dominio.



Y, por último, realizaremos un ping con dicho server, para ver si no se pierden los paquetes.



Como podemos observar, los paquetes son enviados y recibidos, obteniendo respuesta, por lo que podemos comprobar las conexiones remotas.

EVIDENCIAS PARA SUSTENTAR

- ✓ Winlogon corrupto y doble winlogon en la máquina virtual.
- ✓ Capturas de Axiom Examine mostrando archivos maliciosos.
- ✓ PDF malicioso:
- ✓ Reporte de Examine.
- ✓ Registro de logs.
- ✓ Captura de la Virtual corriendo la VDI.
- ✓ Conexiones remotas.

Conclusiones:

En conclusión, sostengo lo que dije en mi hipótesis creyendo que la víctima fue engañada con una posible oportunidad de empleo, dando ejecución a un software con malware dañando su sistema y llevando consigo todo lo demás.