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).

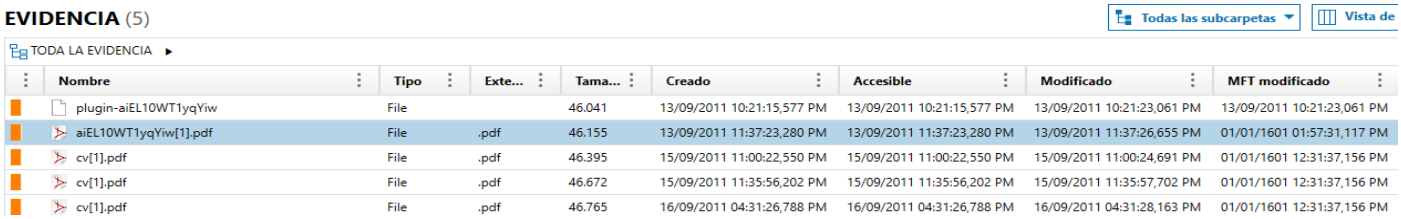
El objetivo final es sustentar técnicamente las hipótesis sobre el daño del sistema y como sufrió el ataque la víctima.

Método Analítico:

Objetivo: Entender el origen.

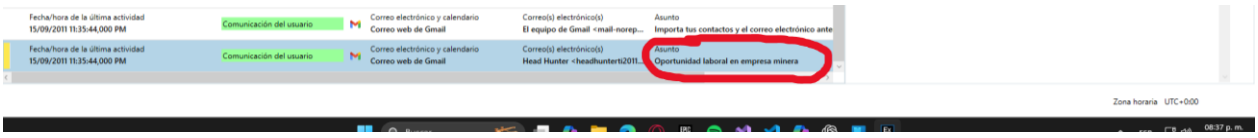
Identificar la fuente:

- Posiblemente descargada. (Un CV).

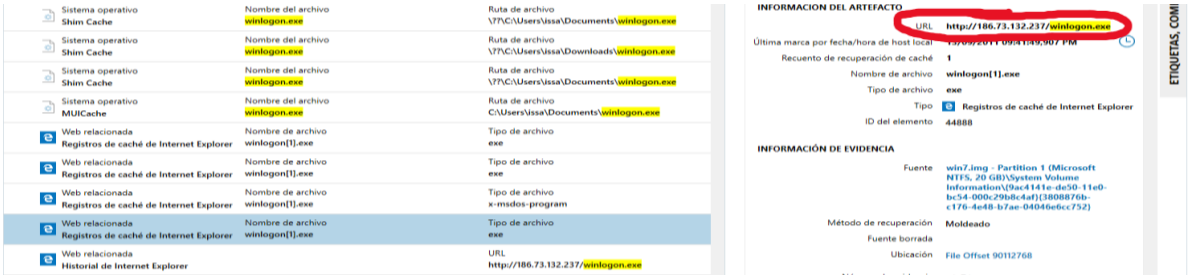


Contexto de aparición:

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



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



Conceptos clave:

1. Malware

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.

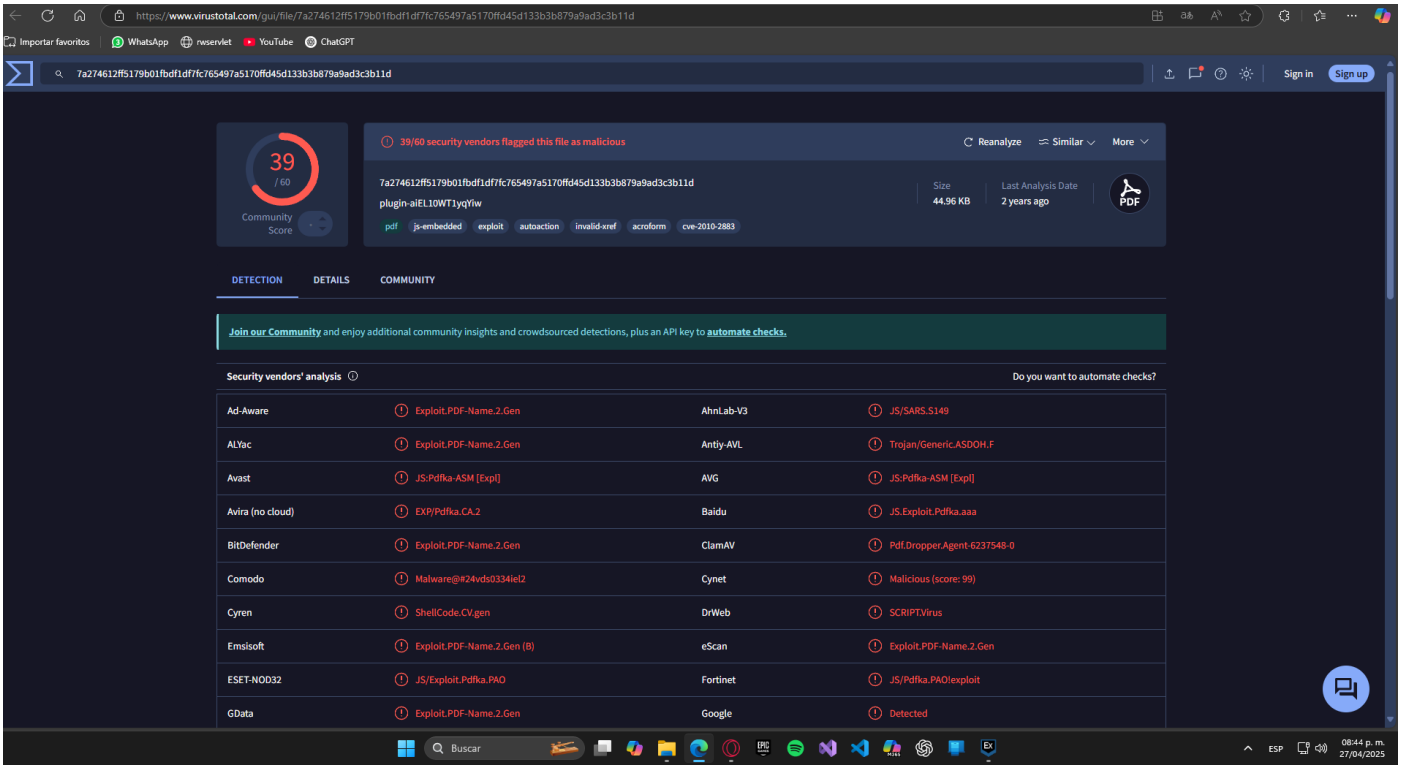
Iniciamos por validar en VirusTotal, las primeras evidencias encontradas en Examine brindadas por la misma aplicación, las cuales son las CV.

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



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:

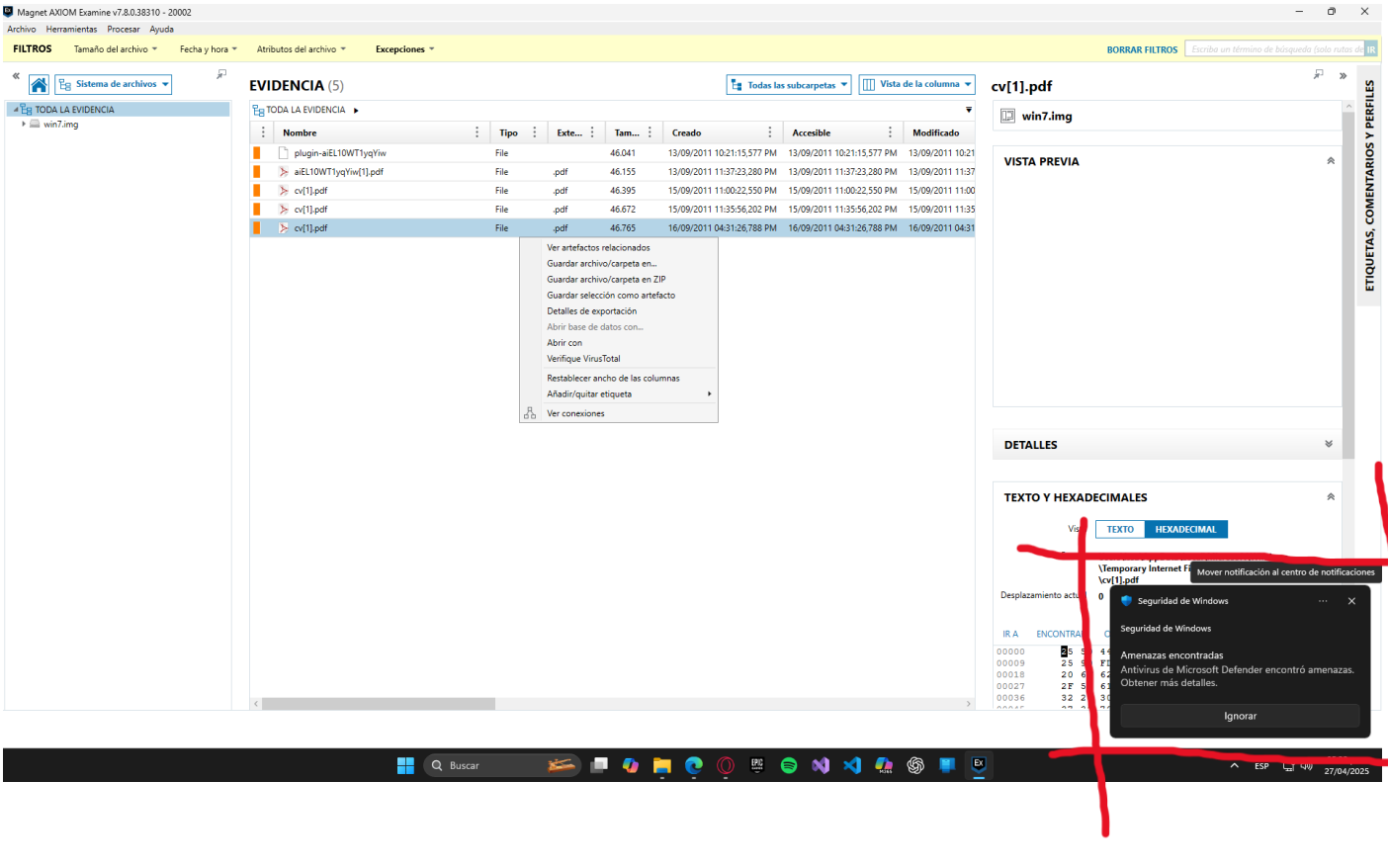
Marcas como "Claw MJ" o "Gymel" que no existen en la industria.

Análisis Técnico:

Objetivo: Buscar evidencias técnicas de manipulación o malware.

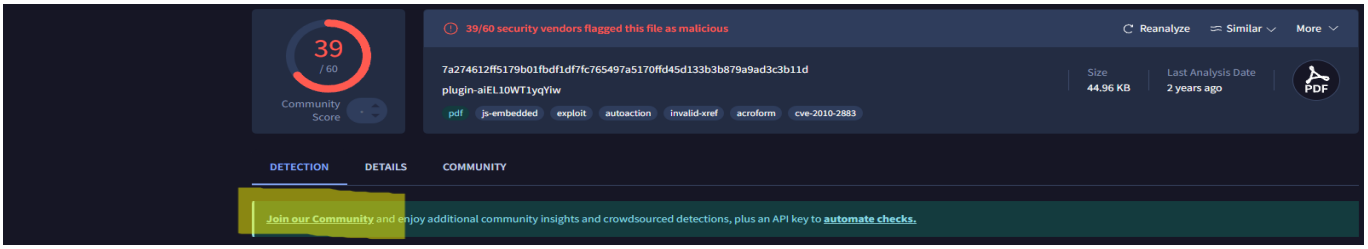
Extraer y analizar artefactos:

De las imagenes 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.



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).

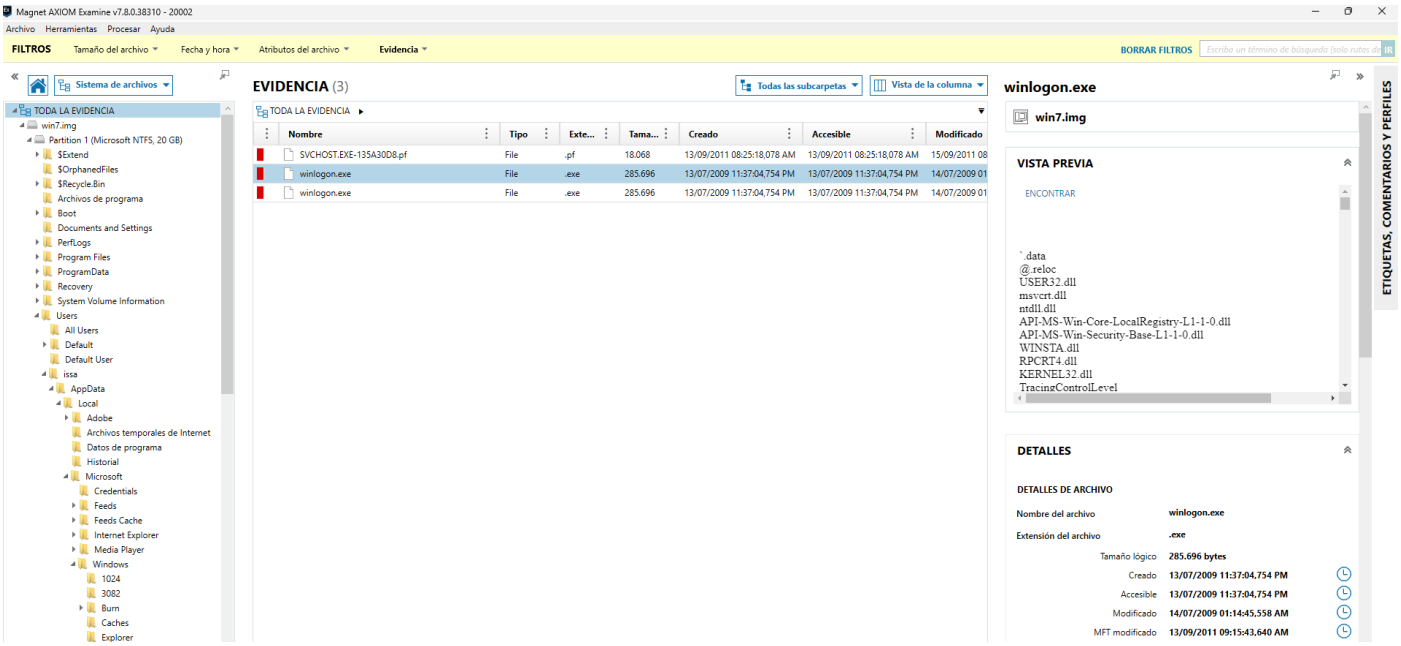


Con esto, podemos tener correlación con amenazas y determinar que el reporte está vinculado a softwares maliciosos.

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.



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 modifiacion MFT que es la modificación de la carpeta sin necesidad del contenido como tal.

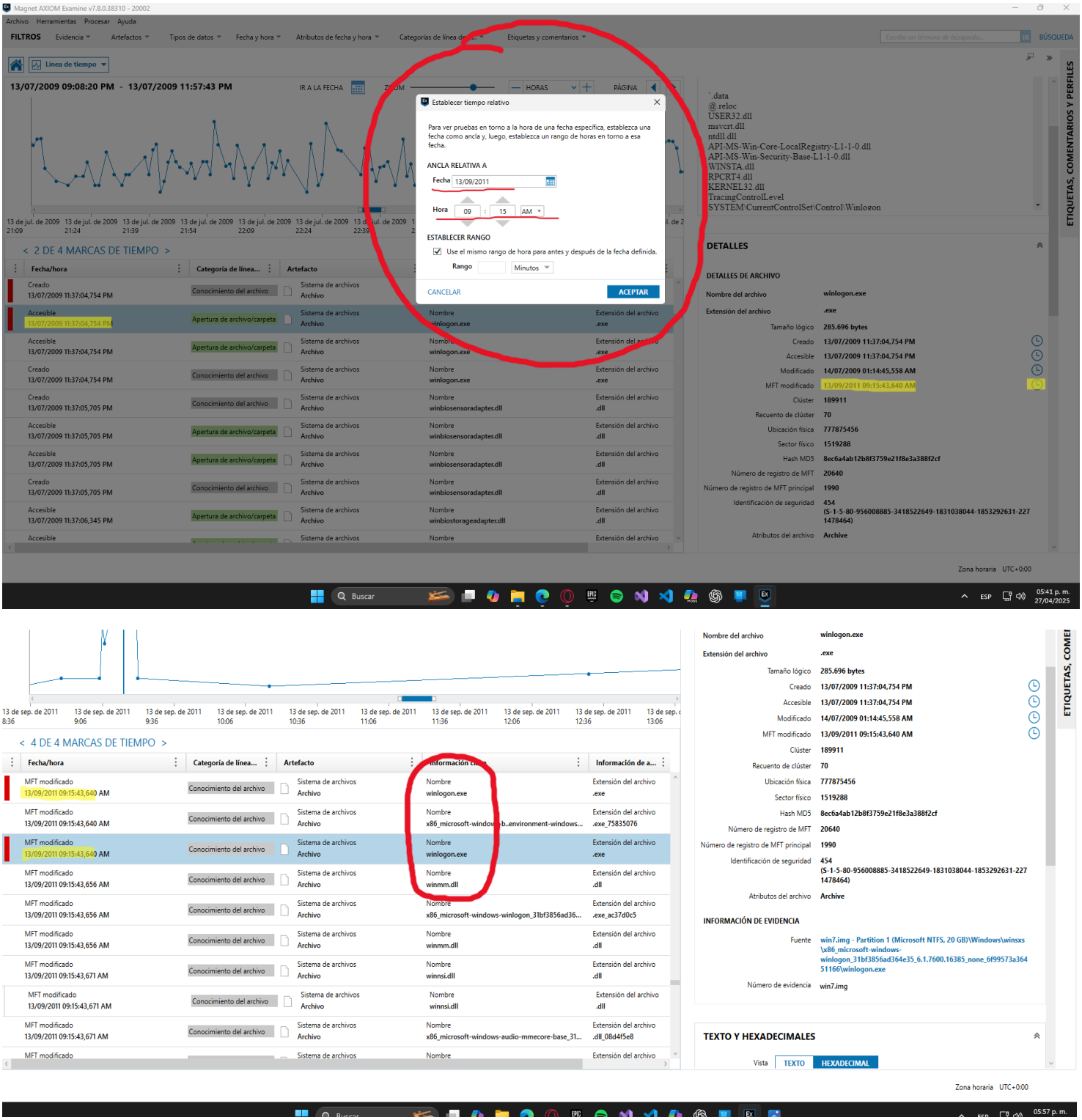
NOTA:
“La Fecha de Modificación MFT es clave en análisis forense para:

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.

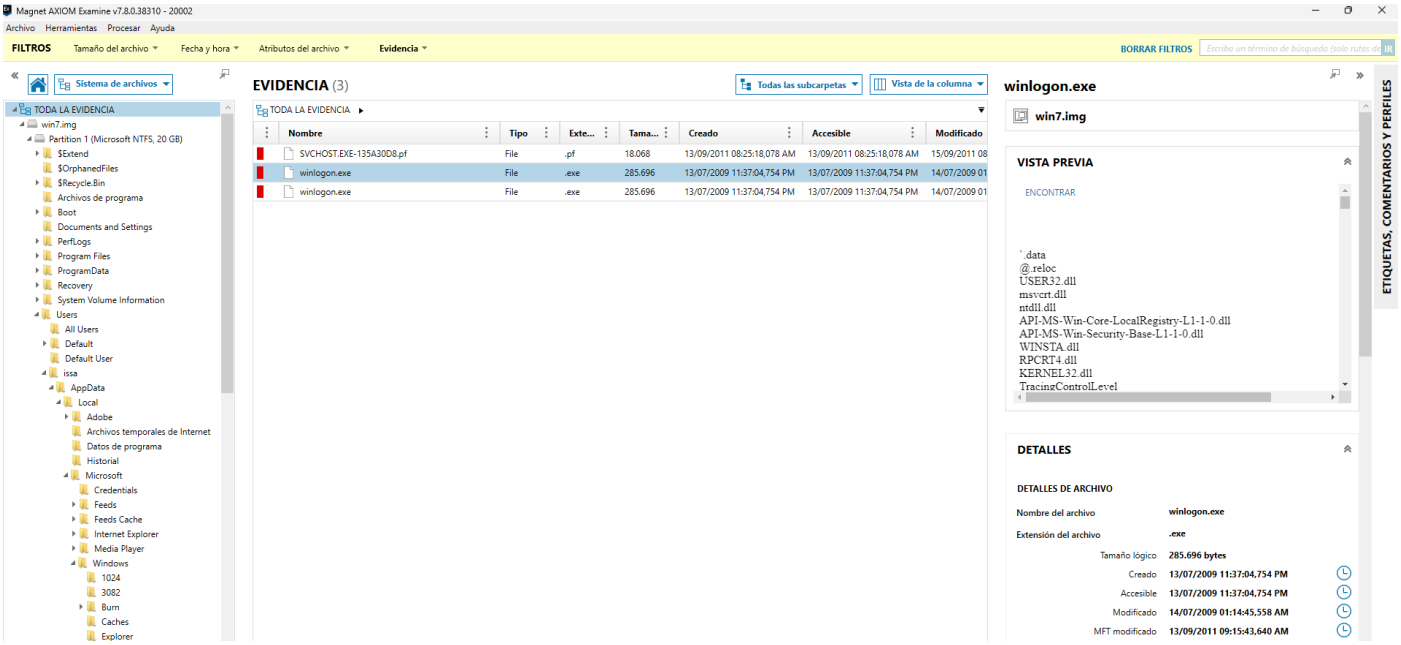
MATERIAL DE ESTUDIO

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).

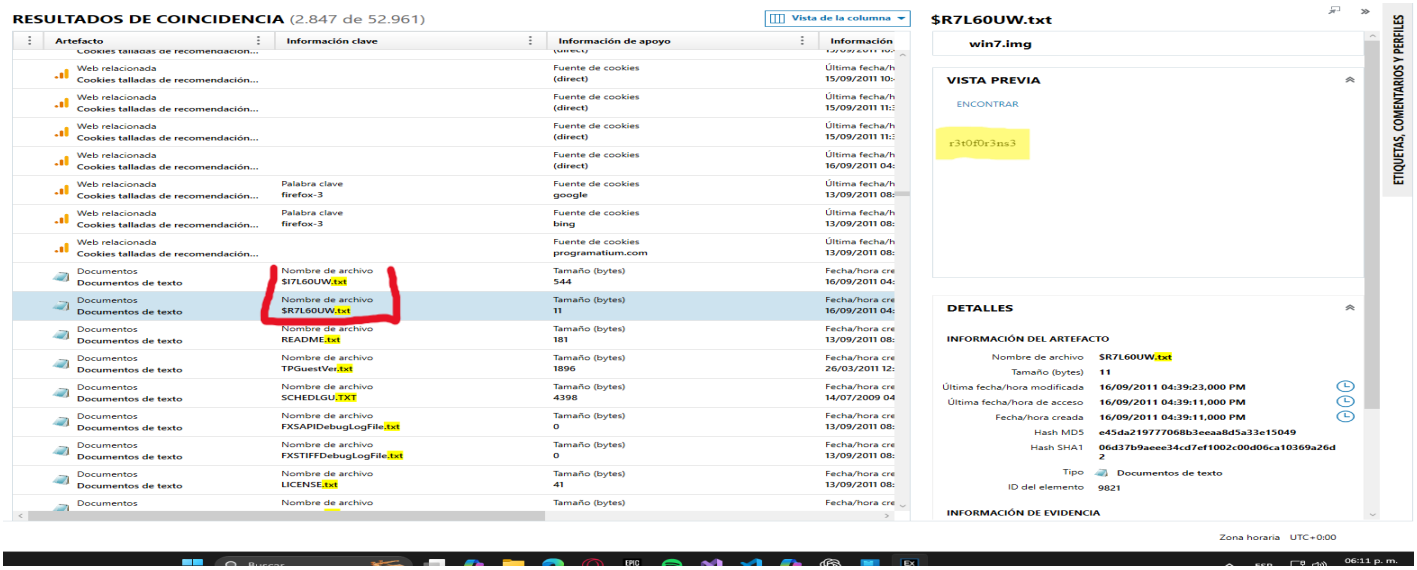
Utilizamos herramientas tales como: Axiom Process, Examine, kali linux y VirtualBox.

Evidencias:

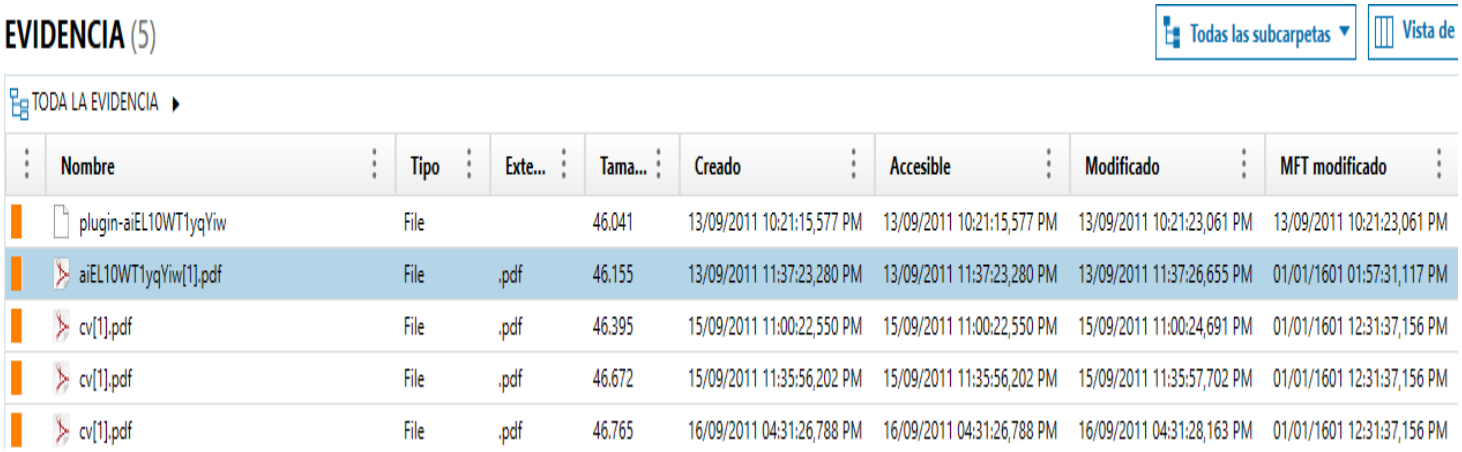
Winlogon corrupto.



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



PDFs maliciosos.



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

ANÁLISIS DEL CASO:

- La victima 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 llego 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 intento 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

Posible 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.

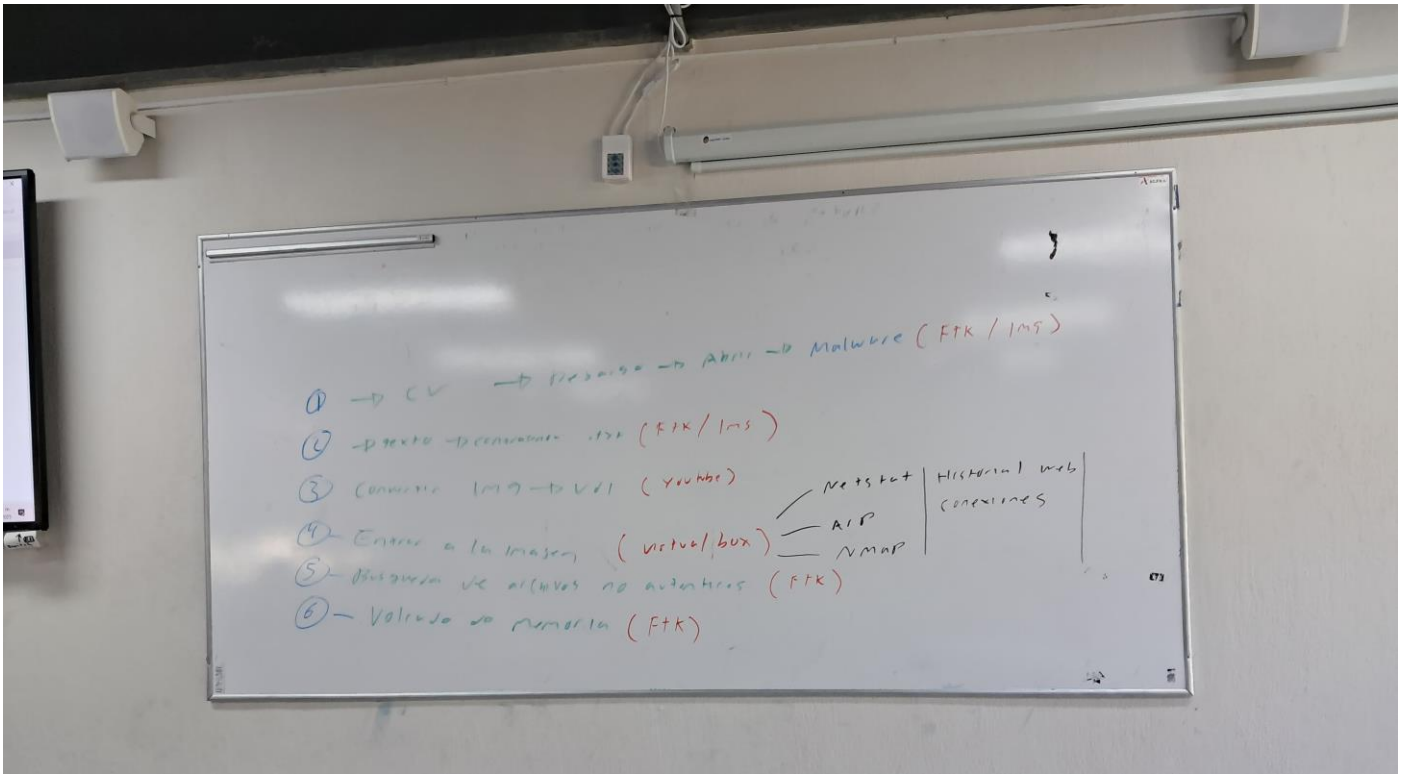
¿Quién es el responsable?

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 sabiamos desde clase:

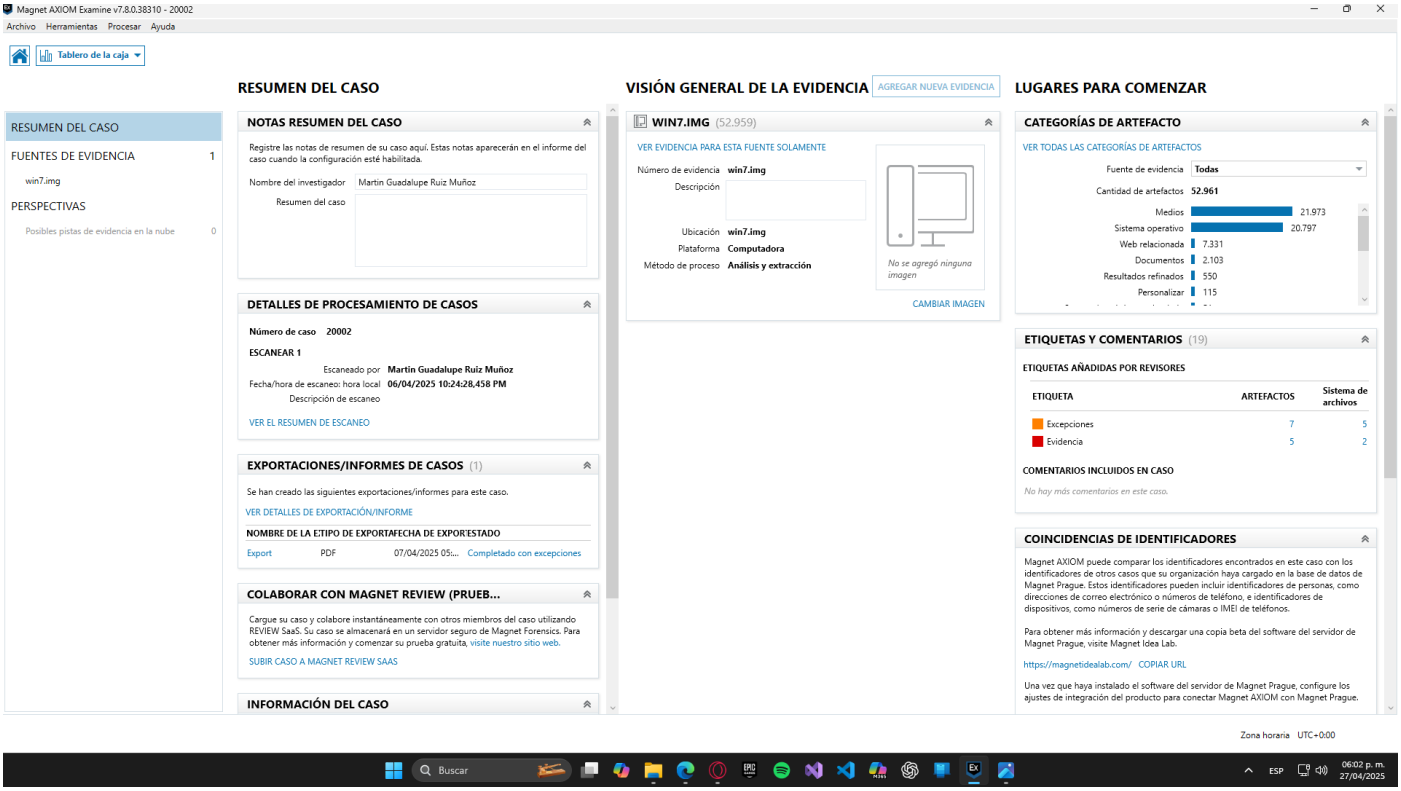


Donde contábamos con 6 puntos claves

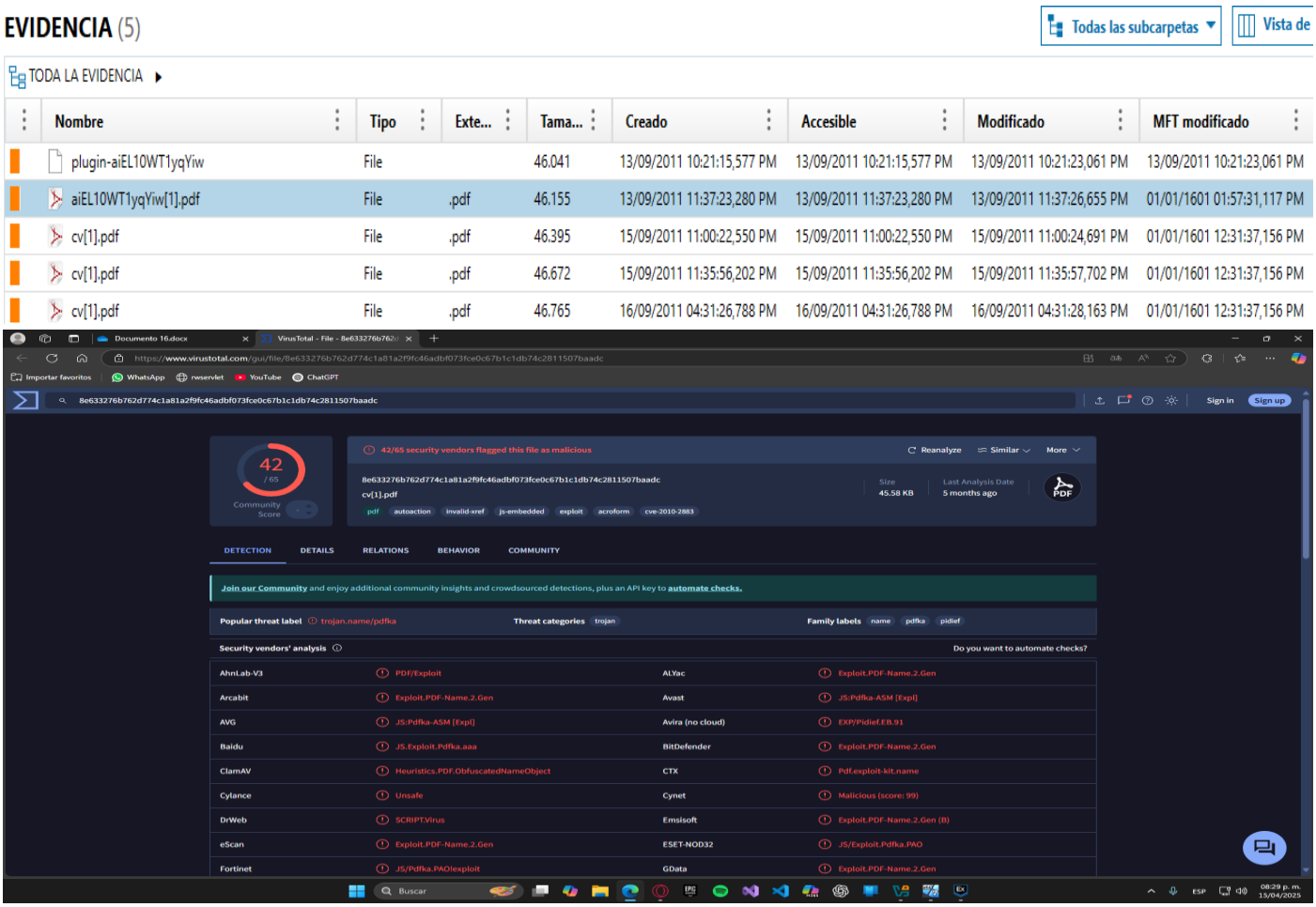
- → El CD infectado.
- → El txt de la contraseña en caso de requerirse de alguna.
- → La conversión de img a vdi para VB.
- → La extracción de la imagen en la VB.
- → La búsqueda de archivos.
- → Y el volcado de memoria.

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.

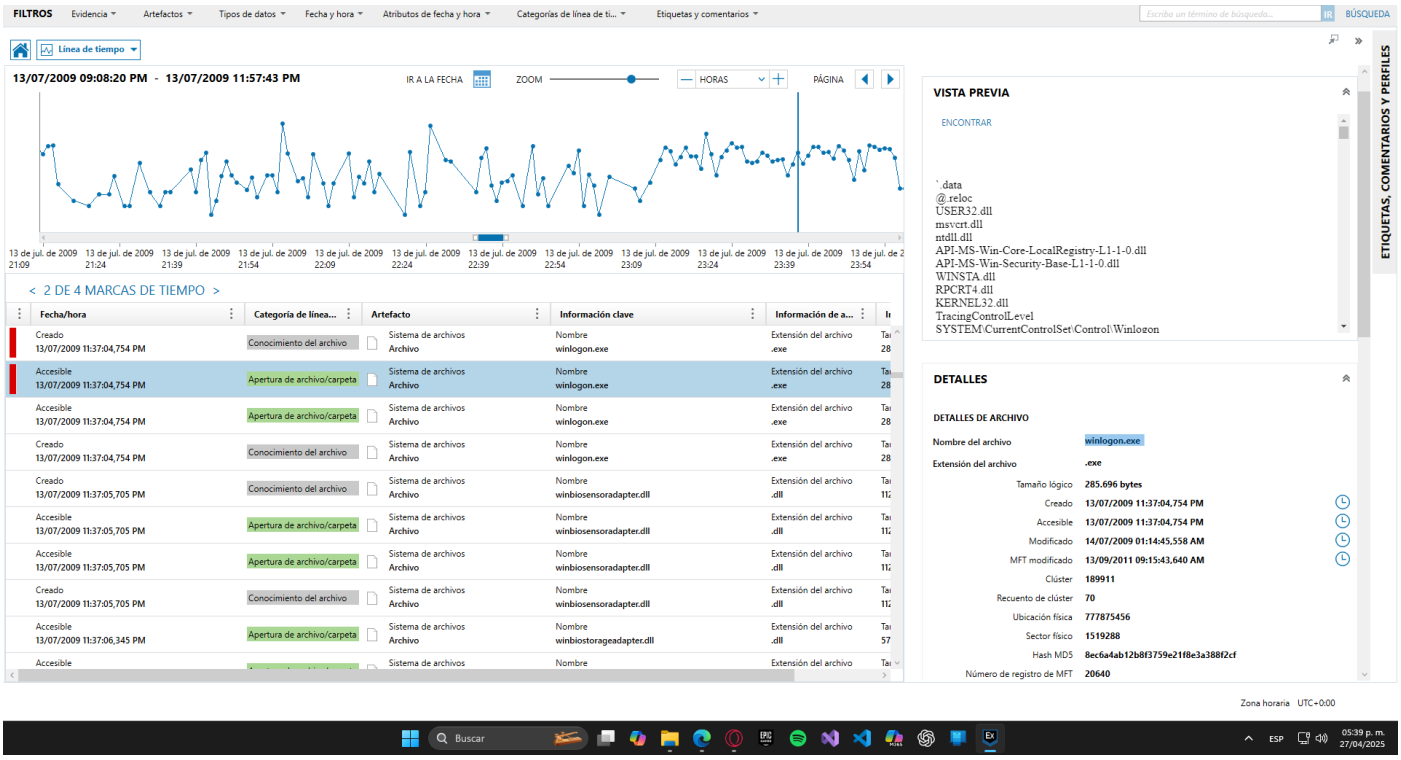


Después Analizamos la evidencia de sistema dada por la app examine (Los CVs).

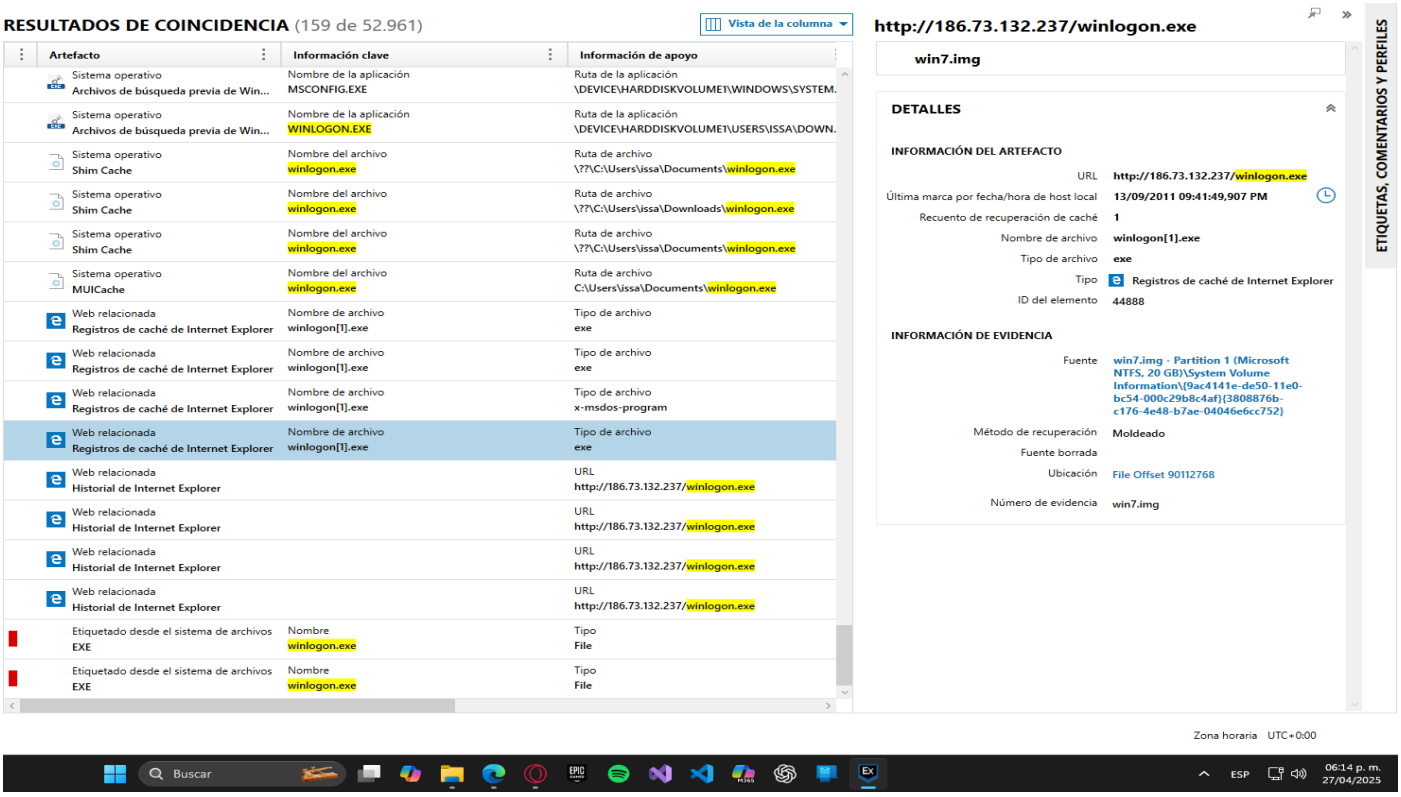


Luego, pasamos a la linea del tiempo, donde manualmente tenemos que buscar actividad sospechosa o directamente malwares.

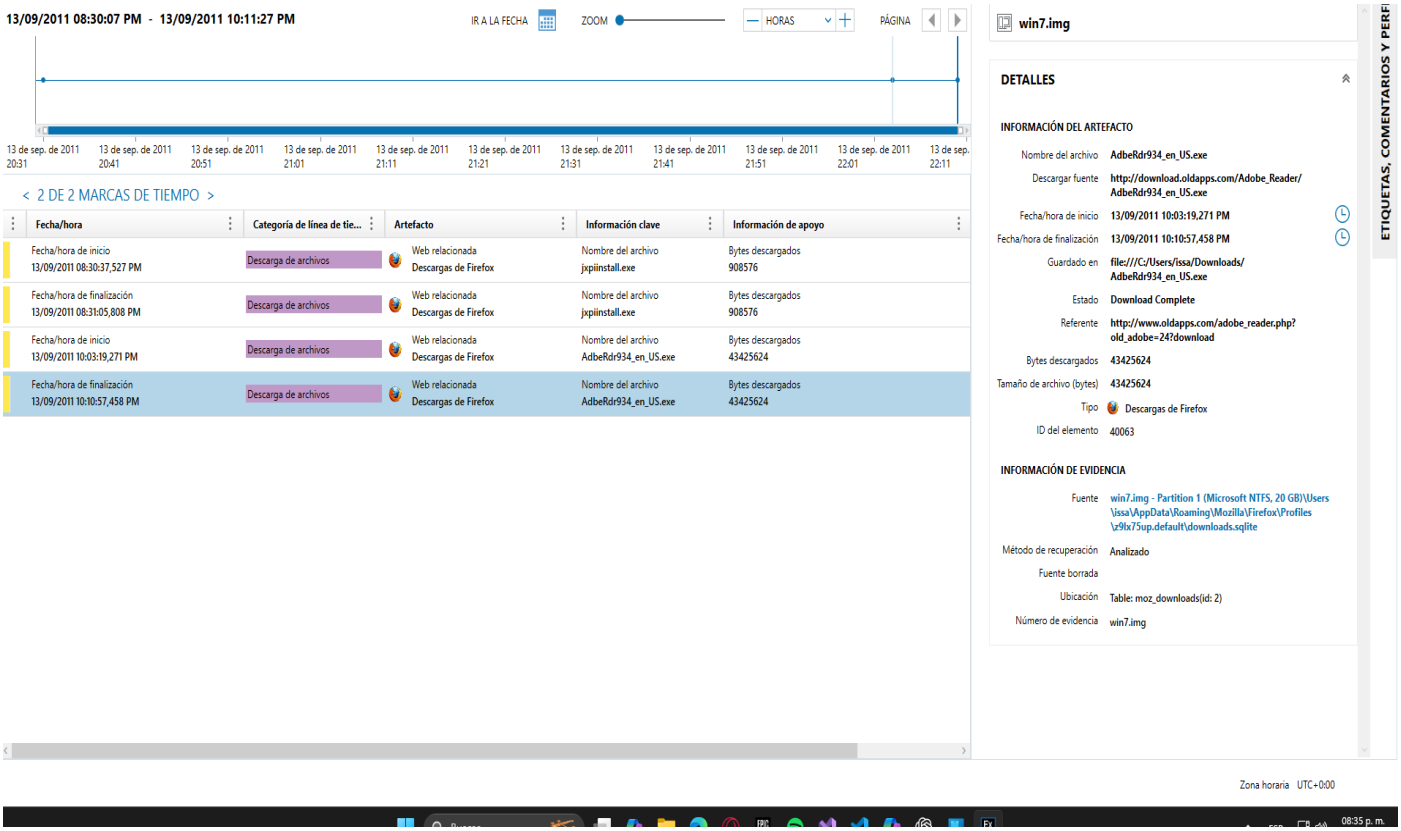
Llegados al 2009, damos con lo primero, un winlogon.exe externo y con fechas diferentes, de creación, modificación etc.



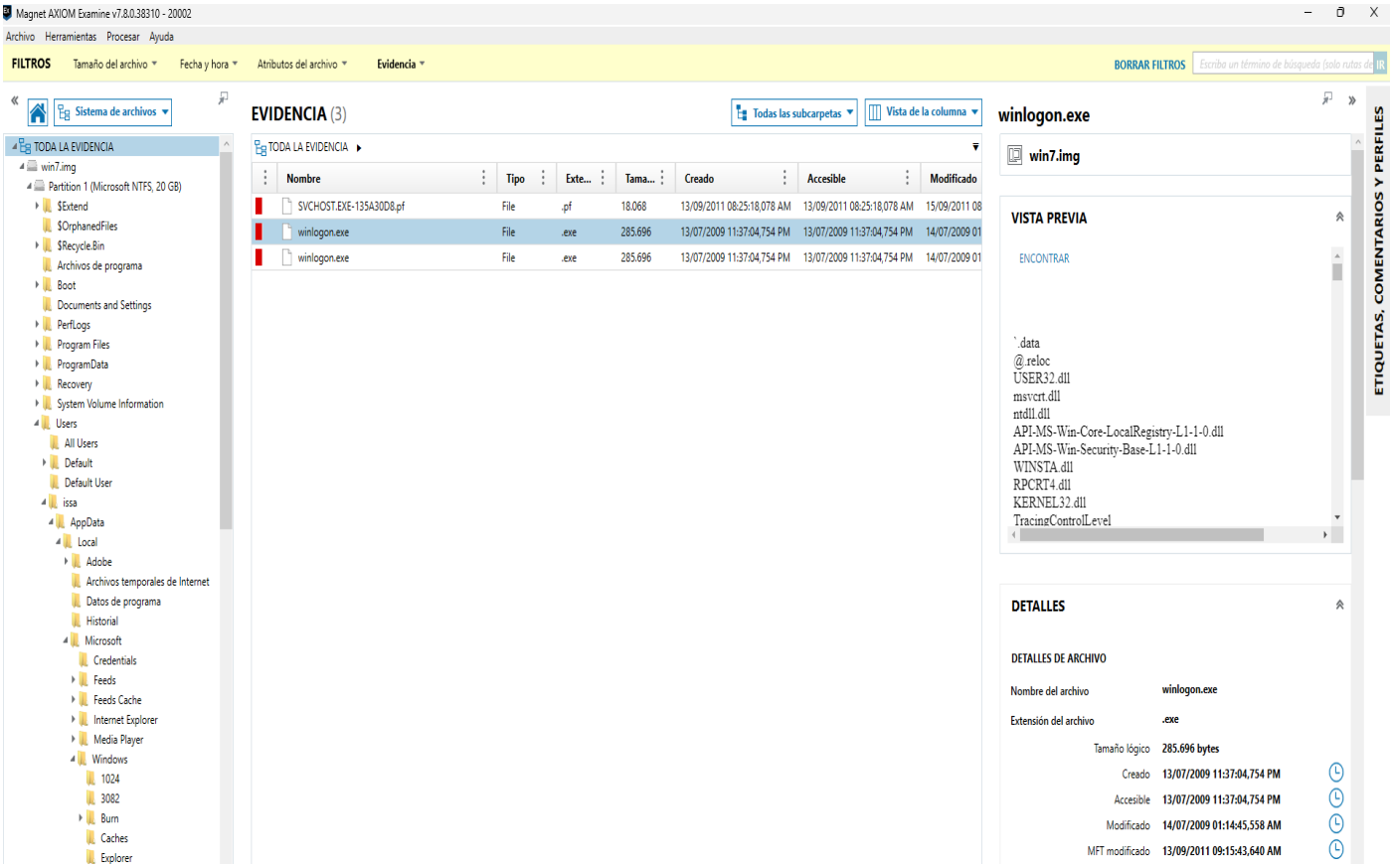
Si nos redirigimos a su fecha de modificación MFT 13 de sep de 2011 llegamos a fechas donde encontraremos mucha evidencia. (Registros web con dicho nombre “winlogon”).



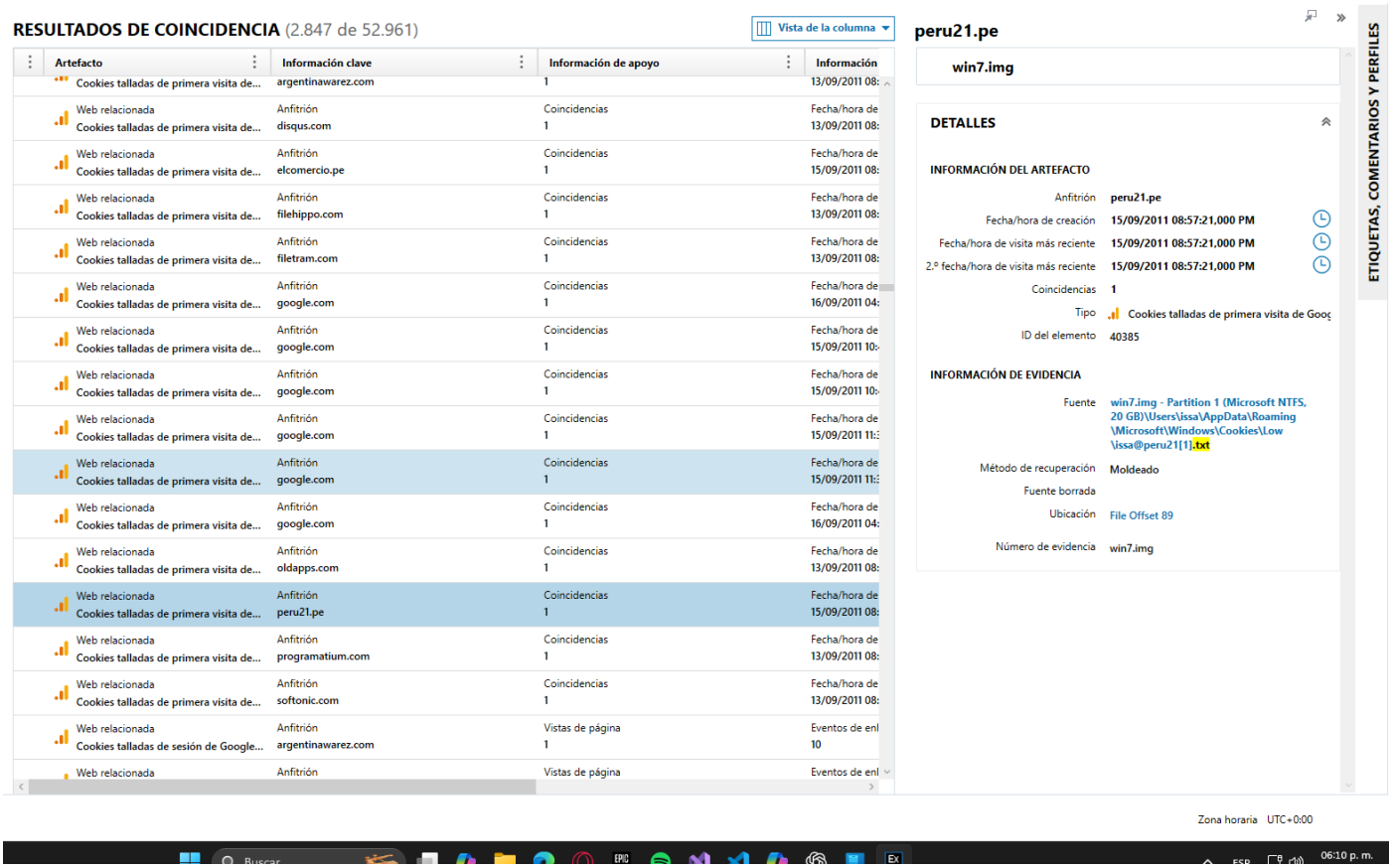
La descarga de adobe reader.



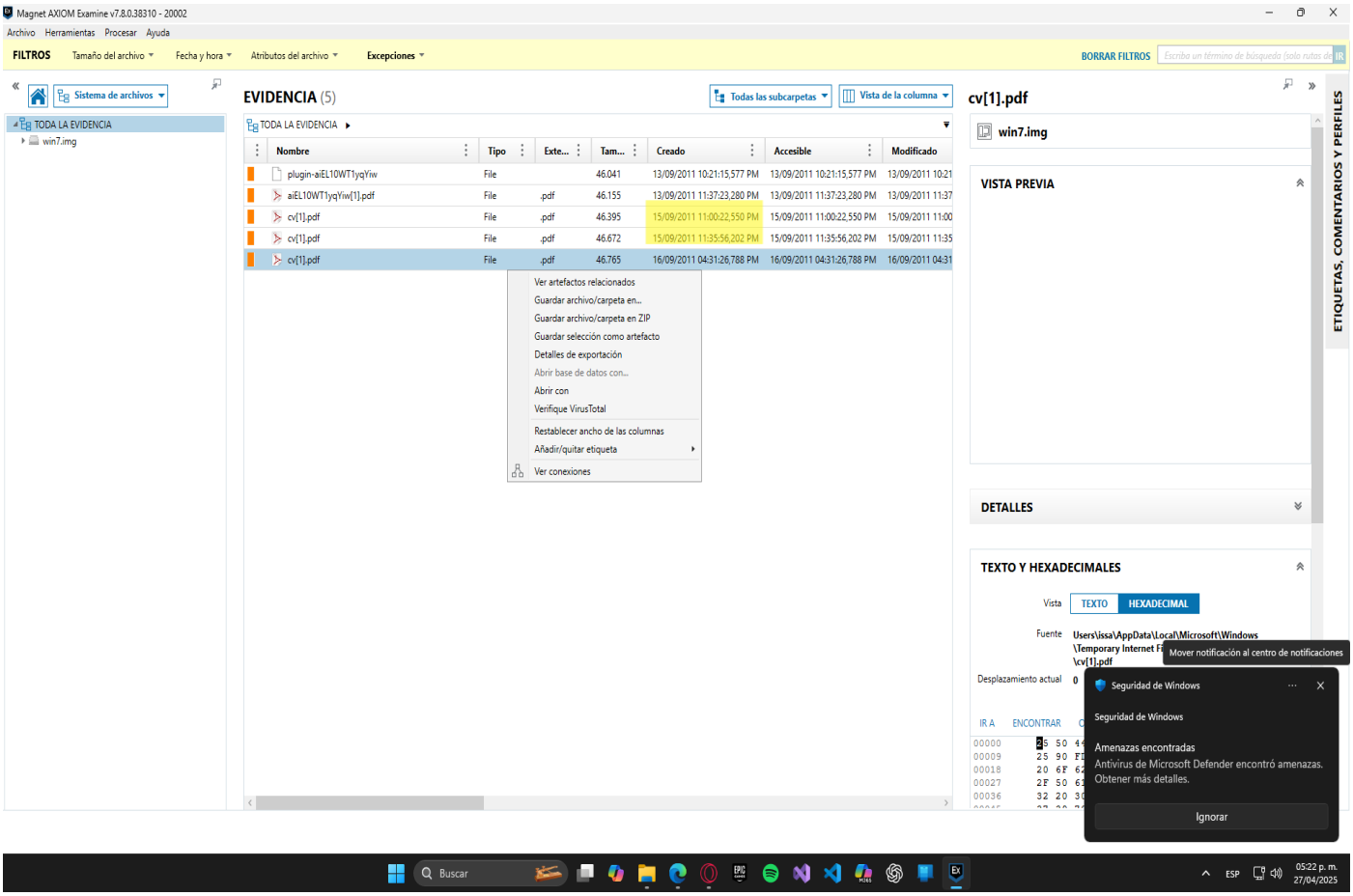
Y los ejecutables del winlogon y el host en .exe



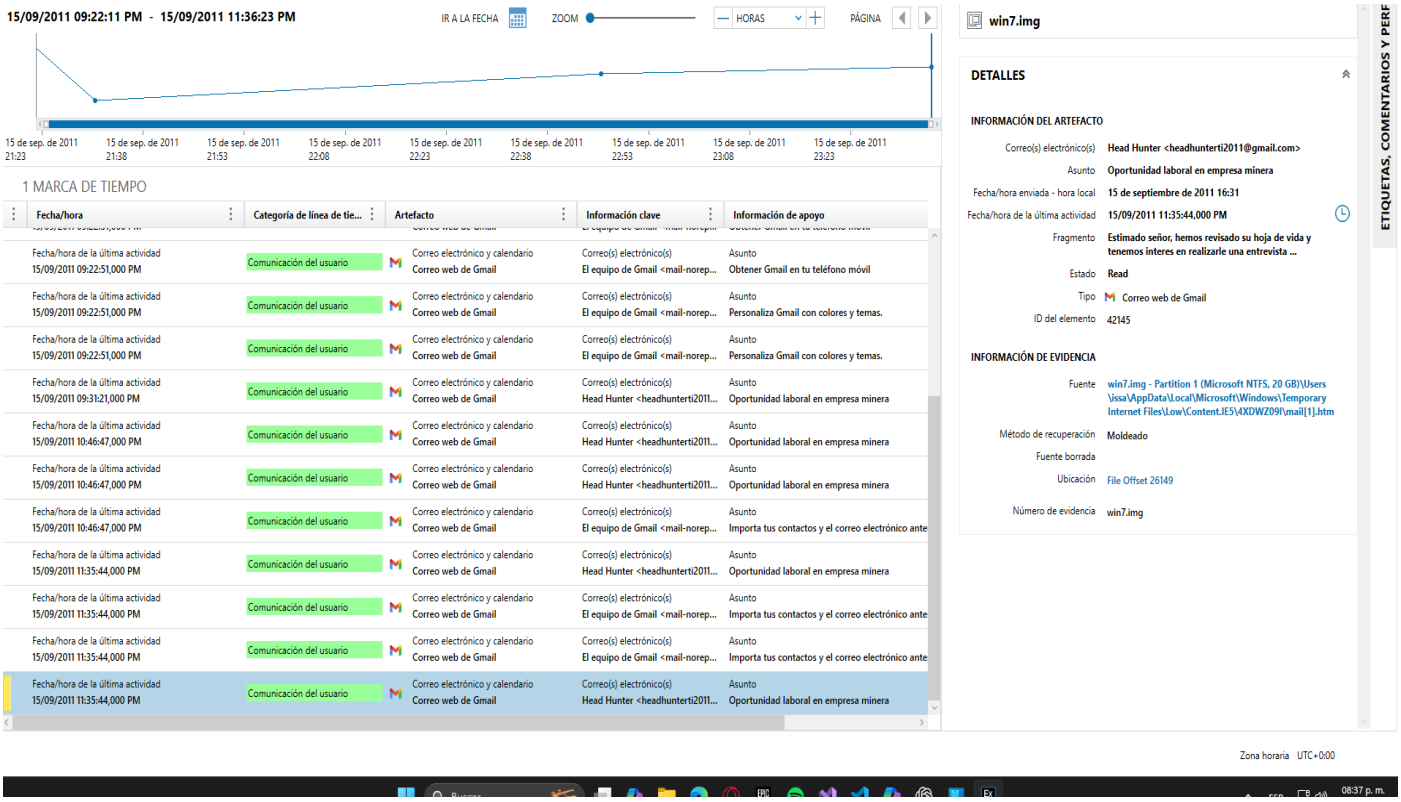
Días después, obtenemos su historial: 15 de sep de 2011



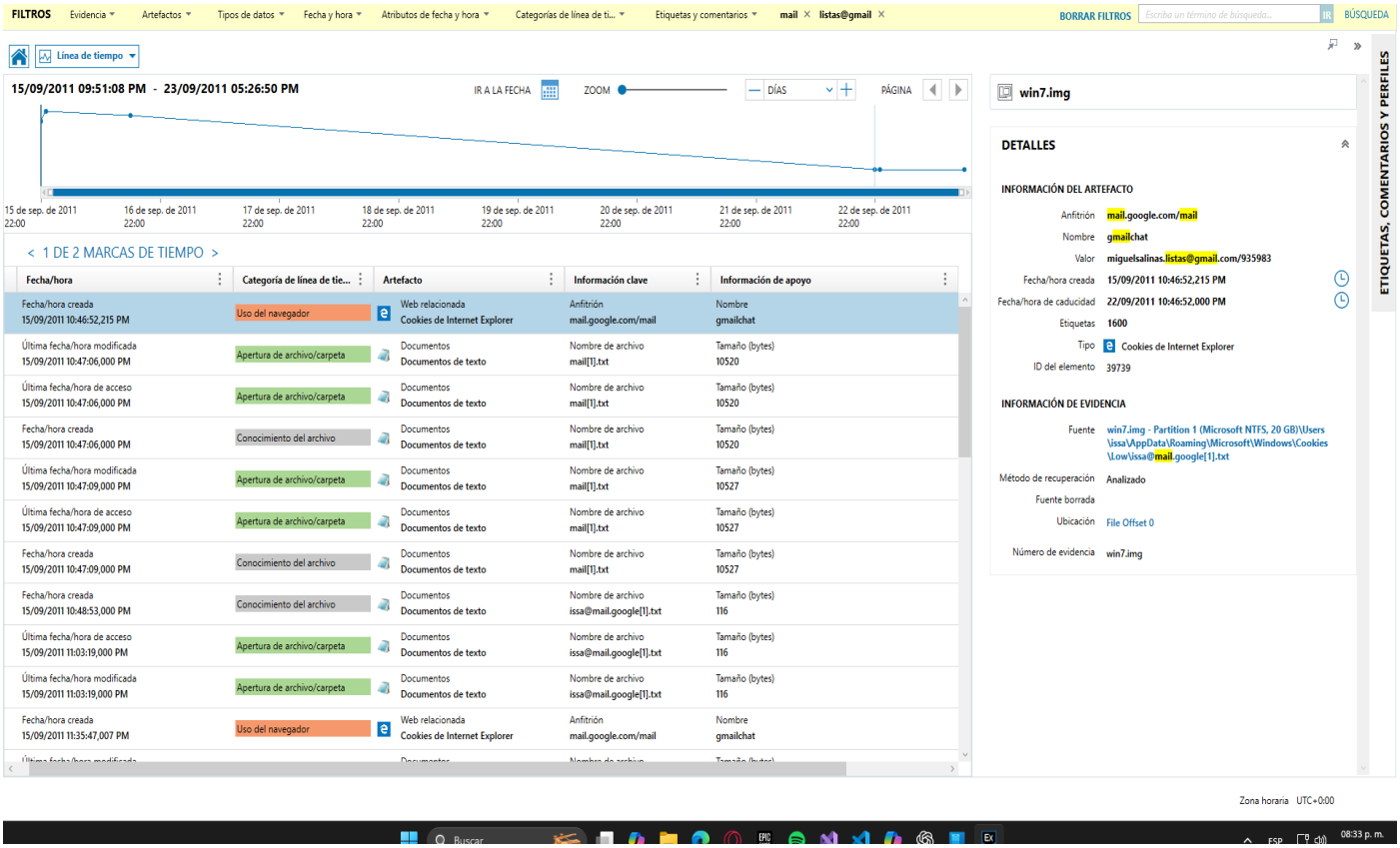
Los primeros dos intentos de ejecución del CV.

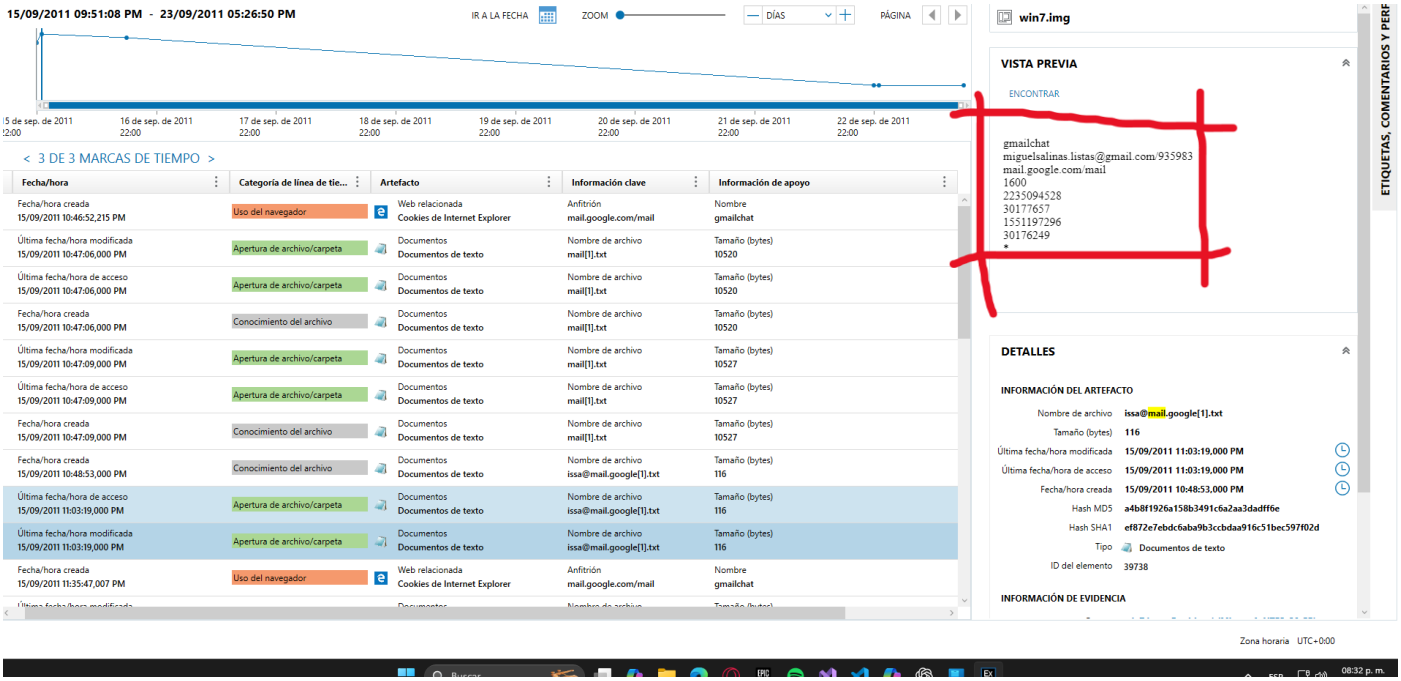


Los correos recibidos:

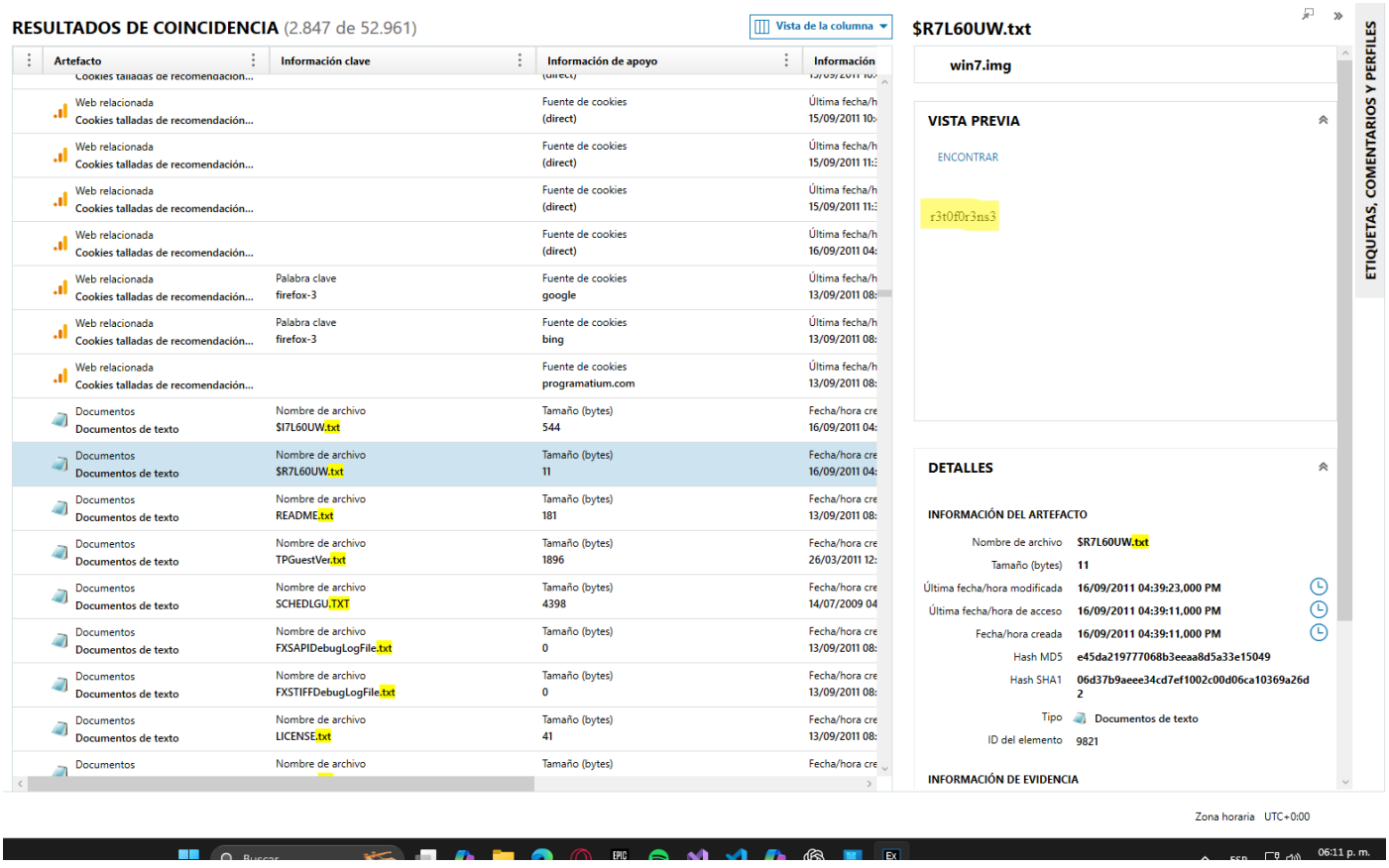


Y lo que aparentemente son ejecuciones de correo, donde se pueden obtener sus datos.

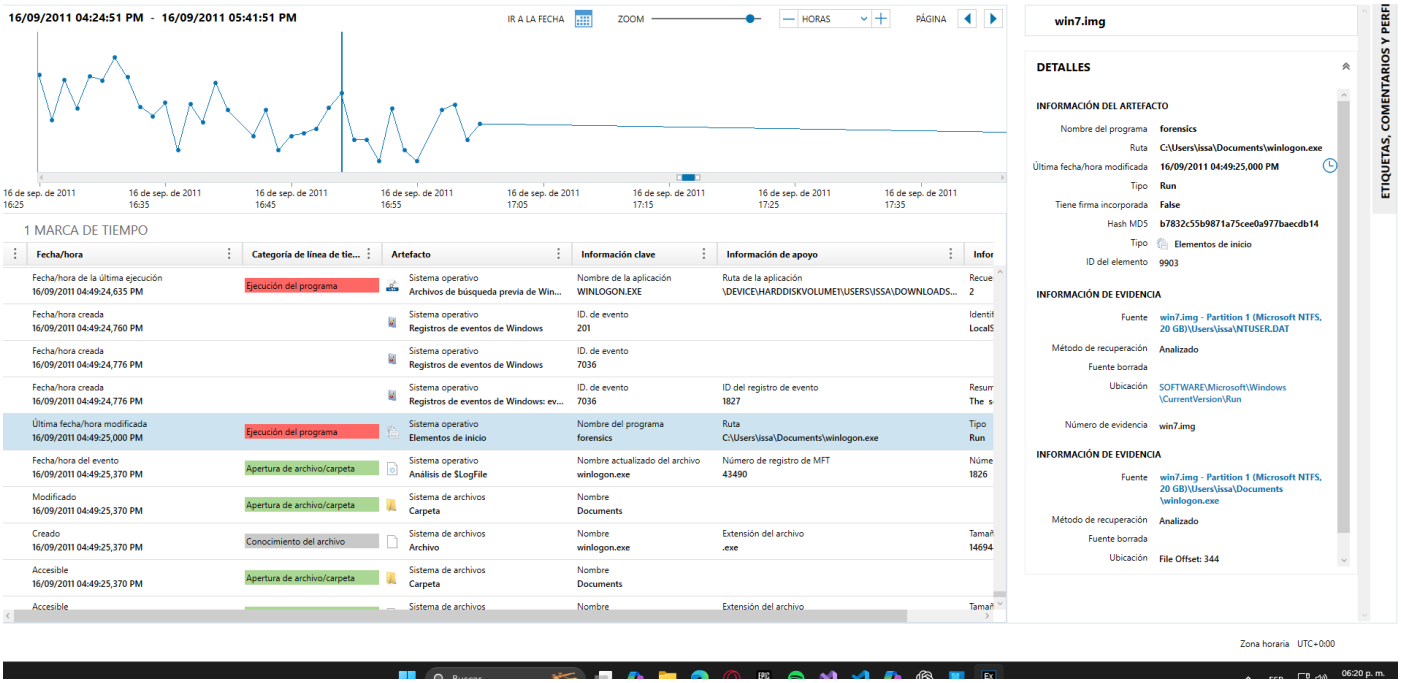




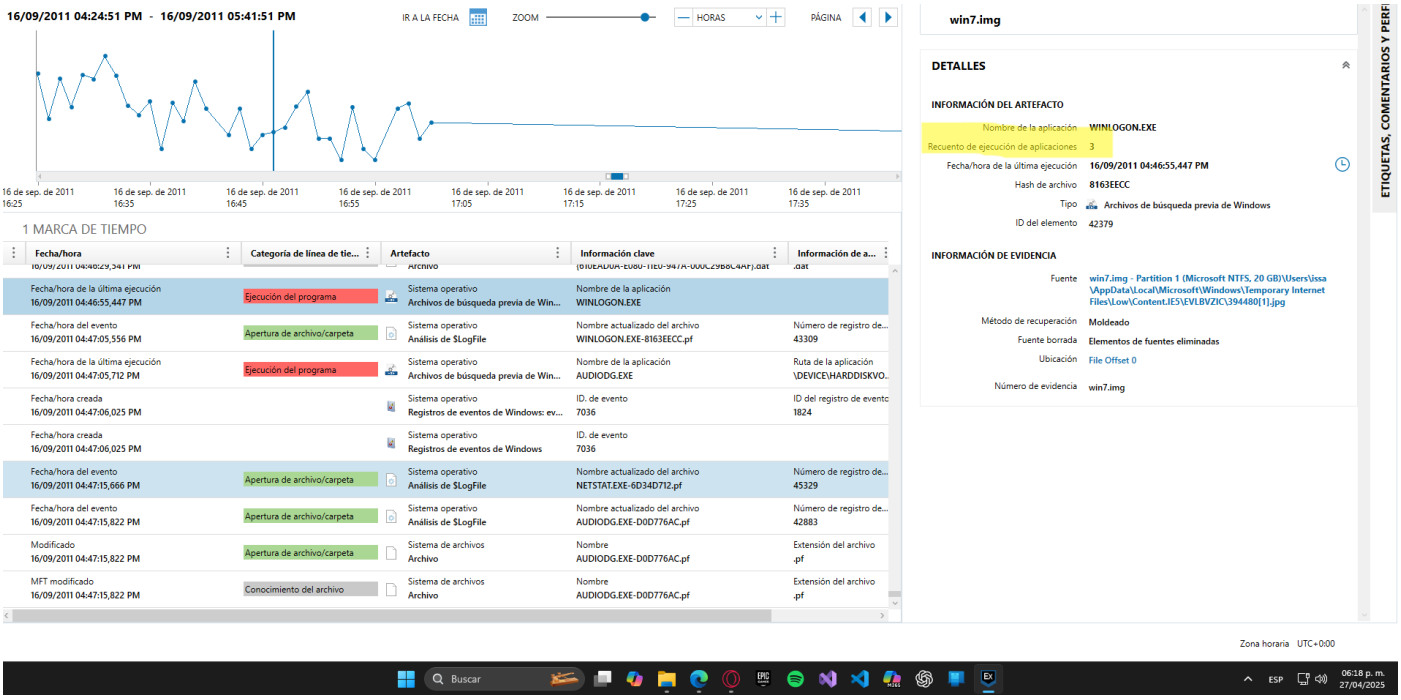
Pasando así al último día revisado el 16 de sep de 2011 obteniendo la contraseña para abrir el vdi en la máquina virtual.



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

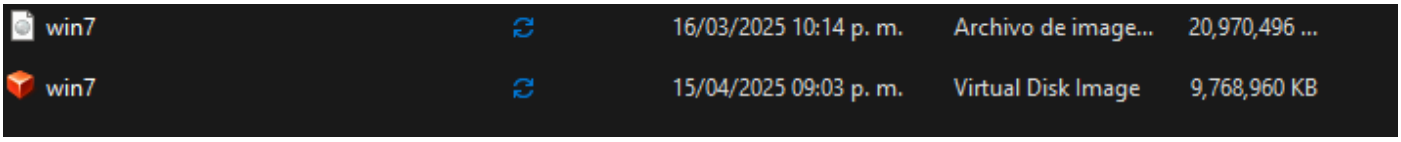


y por ultimo, un winlogon ejecutando 3 aplicaciones:

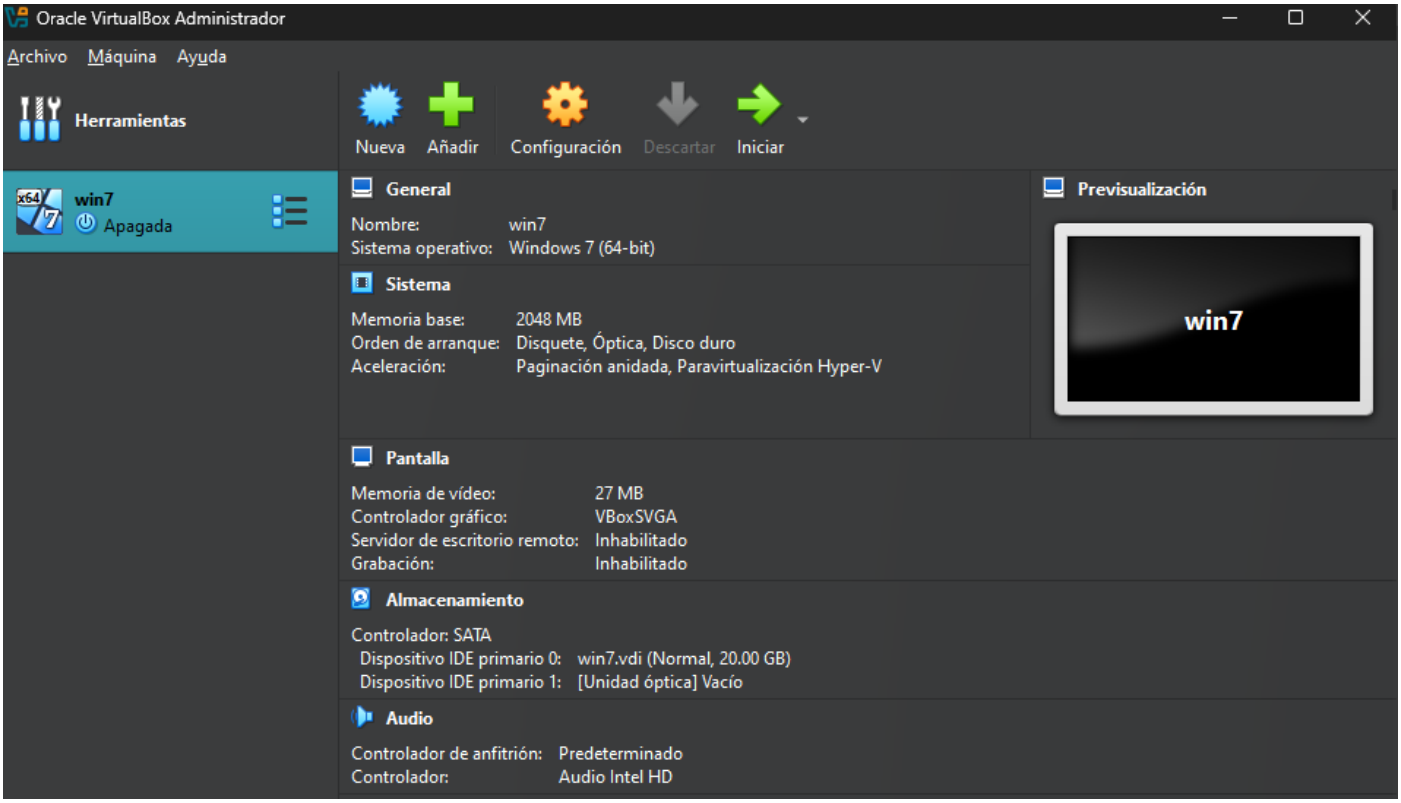


Despues de ello, pasamos a la maquina virtual, que para convertir la img a vdi necesitamos: entrar a la siguiente ruta desde CMD: C:\Program Files\Oracle\VirtualBox>vboxmanage convertdd C:\Users\CDHI9\OneDrive\Documentos\Ciberseguridad\win7.img C:\Users\CDHI9\OneDrive\Documentos\Ciberseguridad\win7.vdi

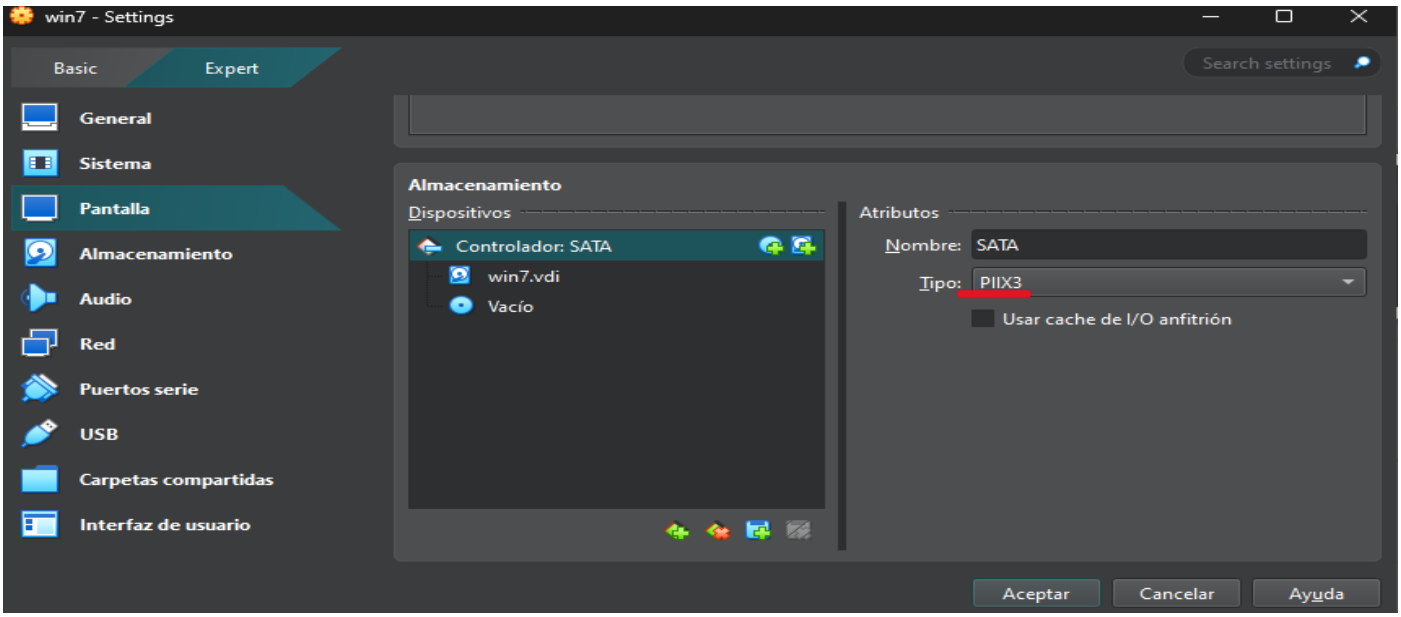
Lo que convertira a vdi:



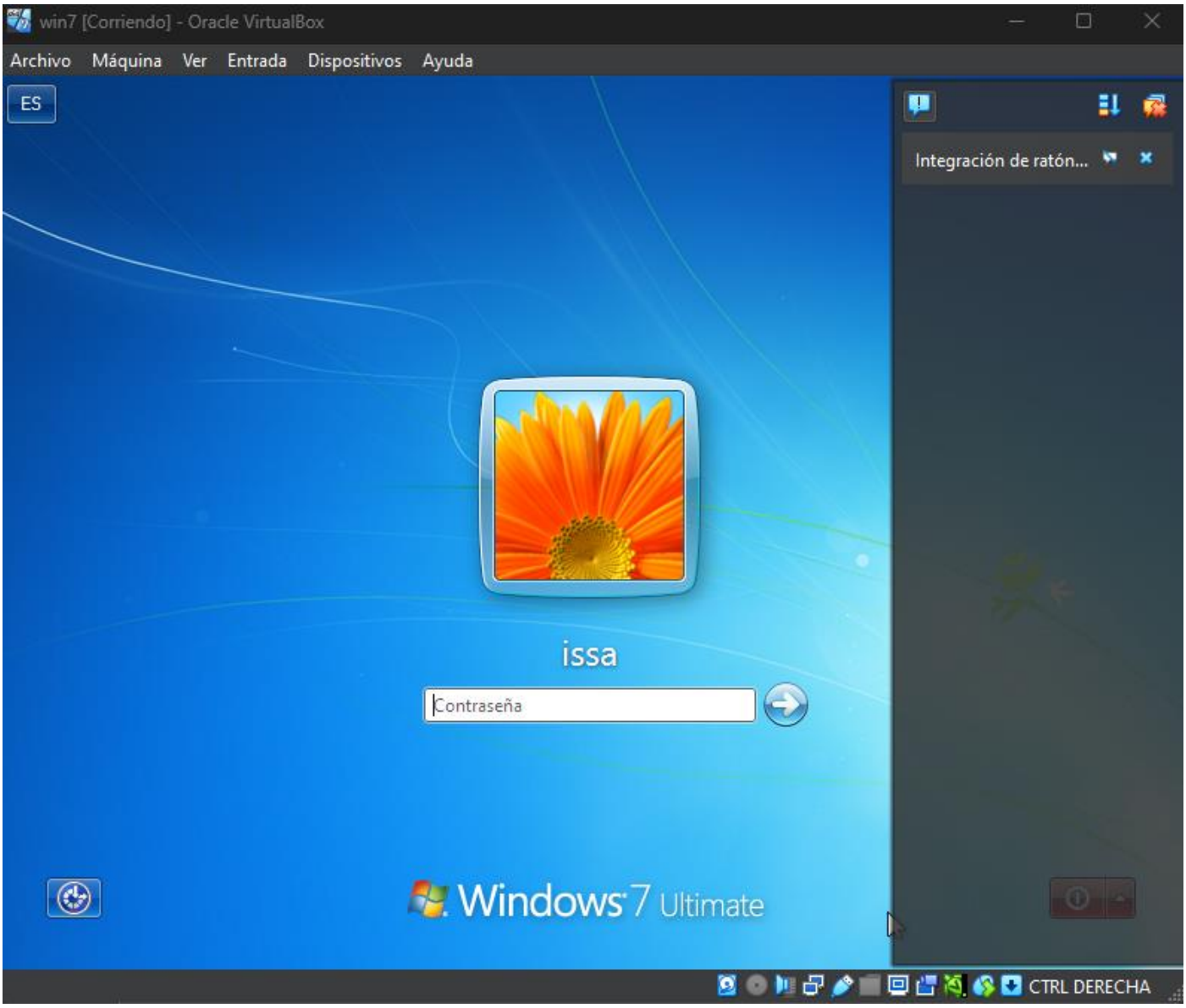
Despues, ejecutamos la VM:



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 “PllX3” y será la solución:

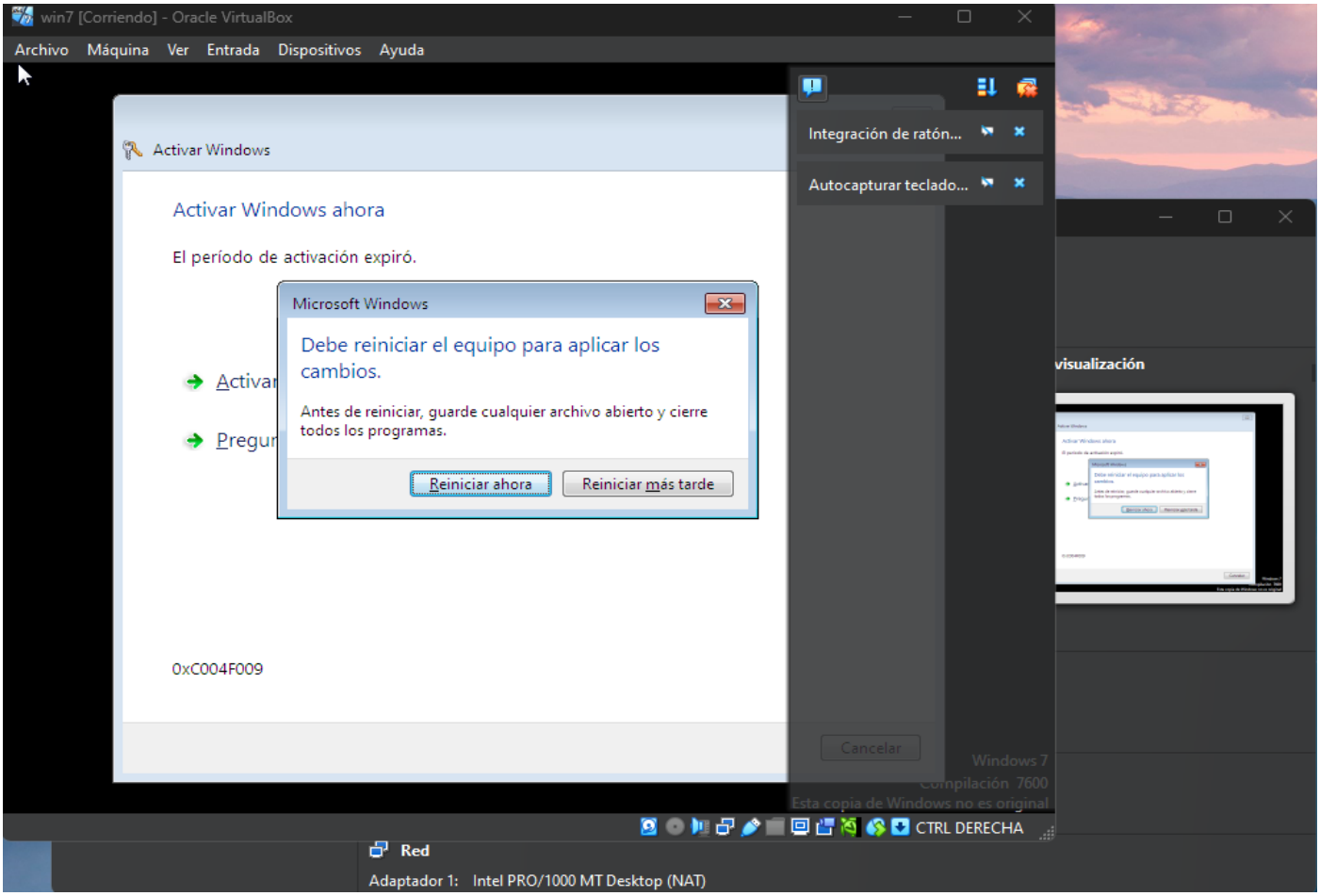


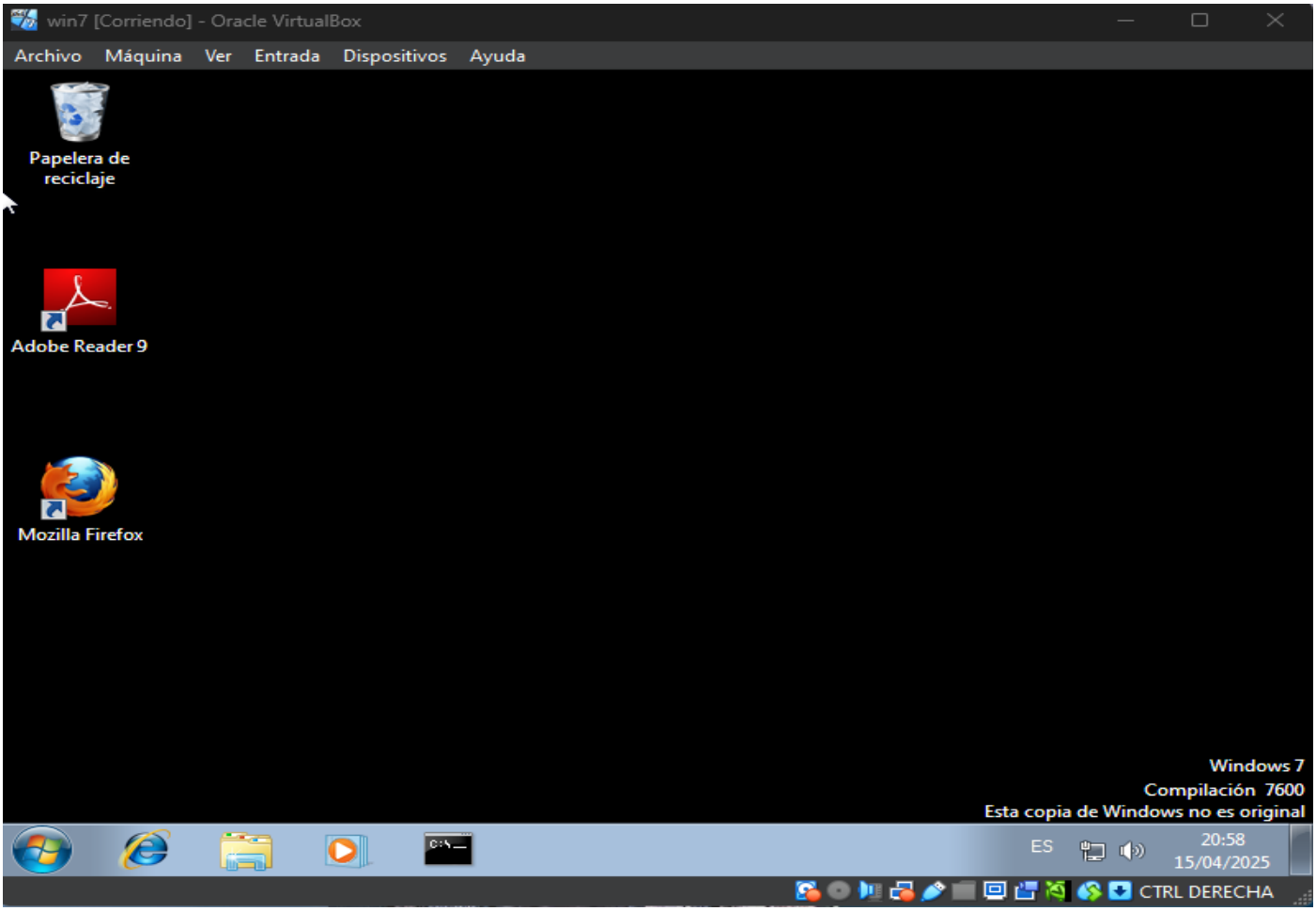
Corremos con normalidad la maquina:



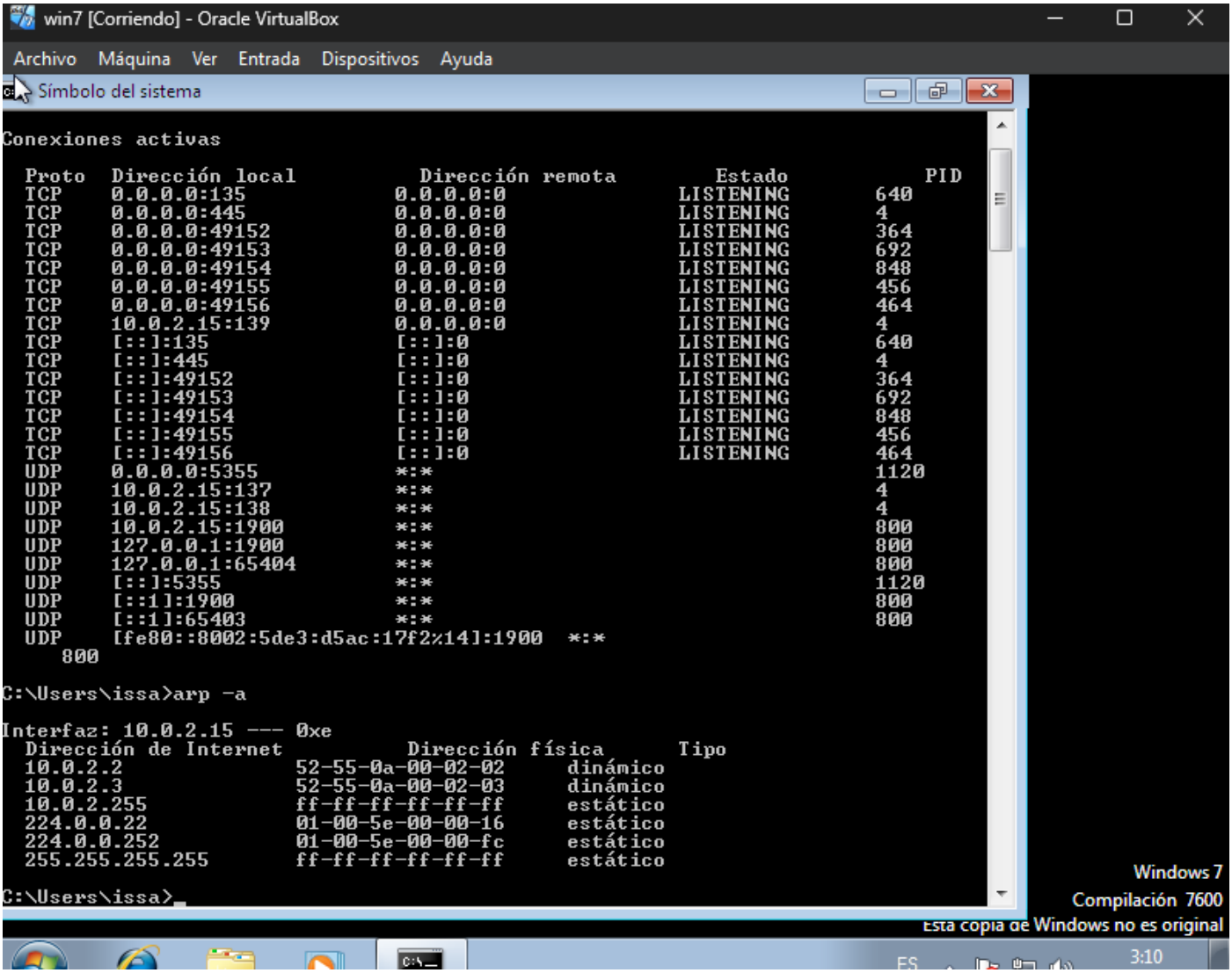
E iniciamos sesión con la contraseña obtenida:

“r3t0f0r3ns3”

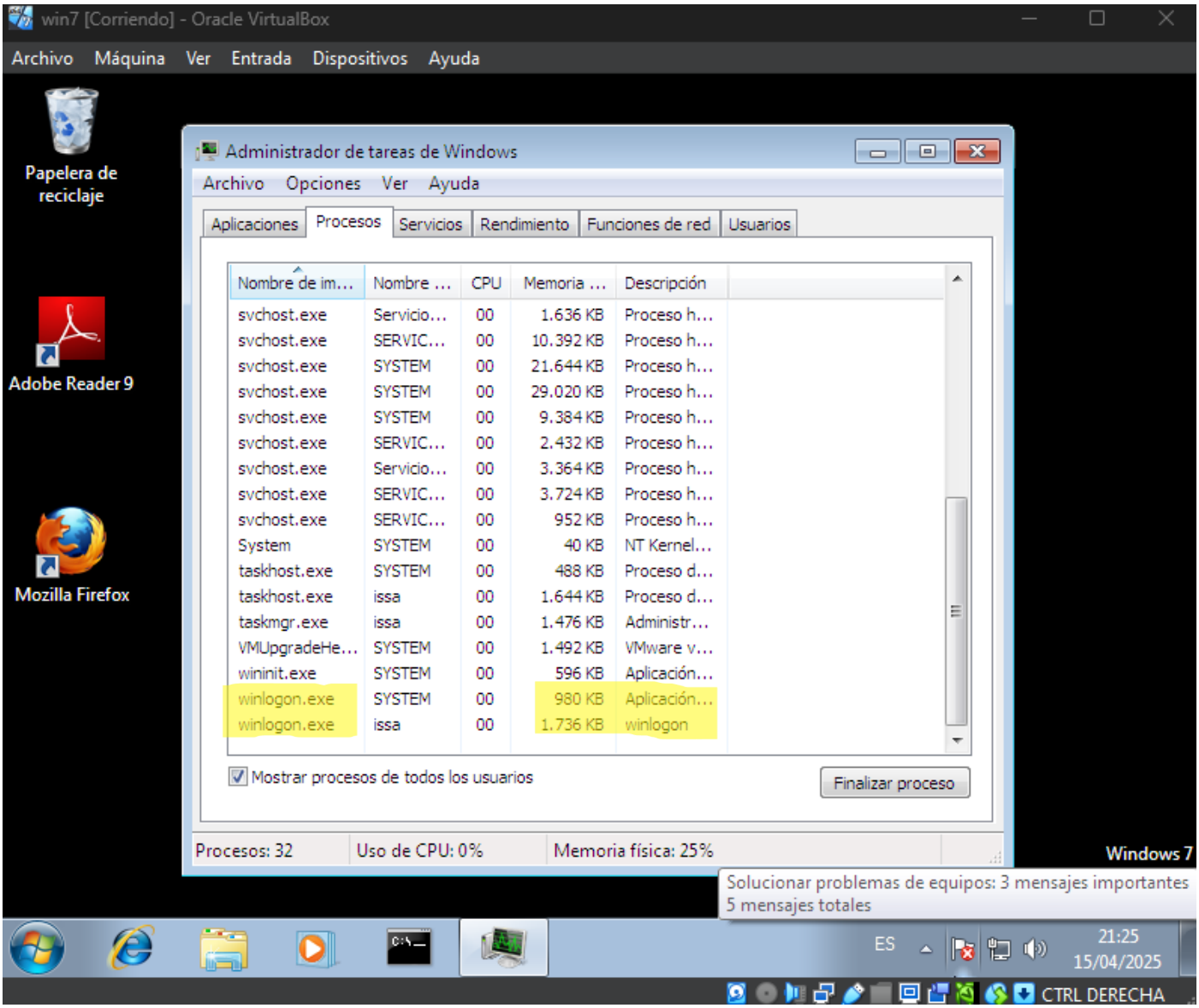




Ejecutamos algunos de los comandos recomendados en clase: netstats y arp.

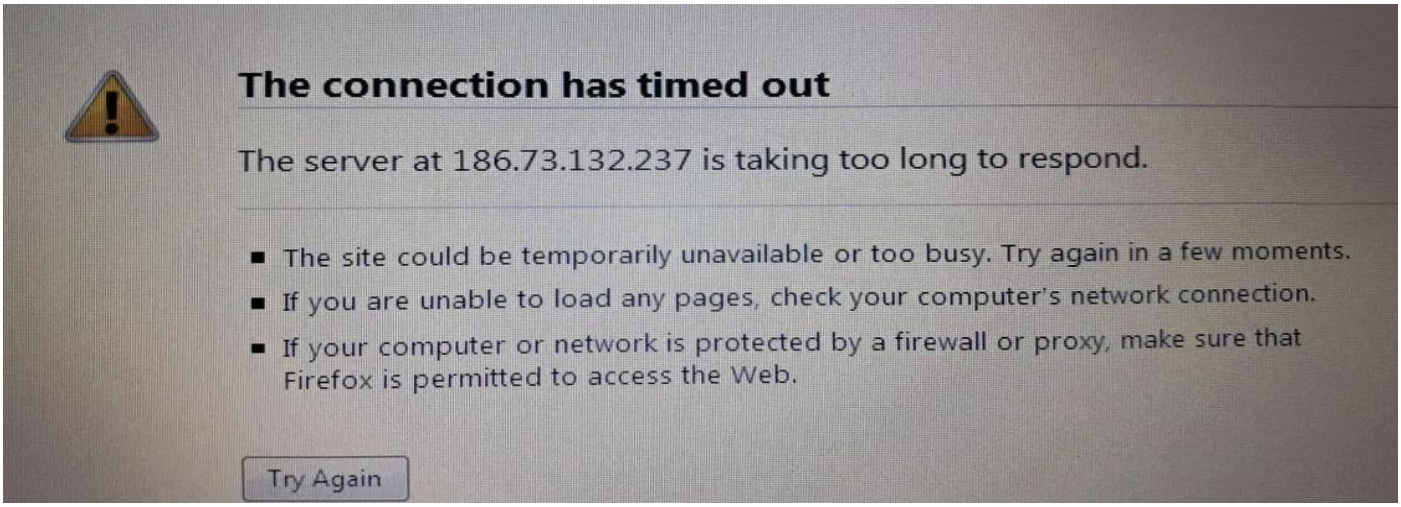

win7 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Símbolo del sistema
Conexiones activas
Proto Dirección local Dirección remota Estado PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 640
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING 364
TCP 0.0.0.0:49153 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 [::1]:1900 *:* 800
UDP [::1]: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
C:\Users\issa>
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.

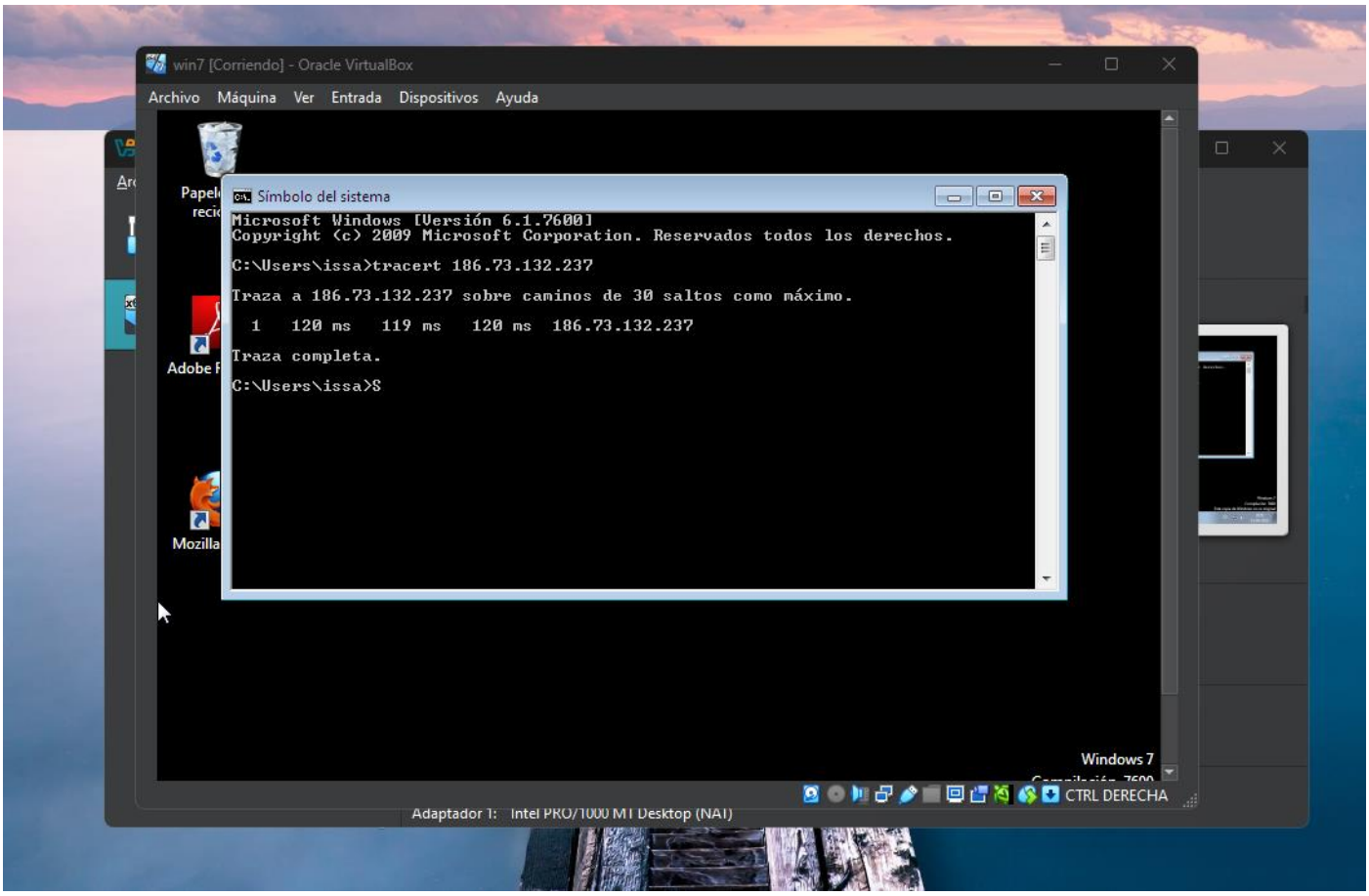
Revisamos Firefox y nos topamos con:



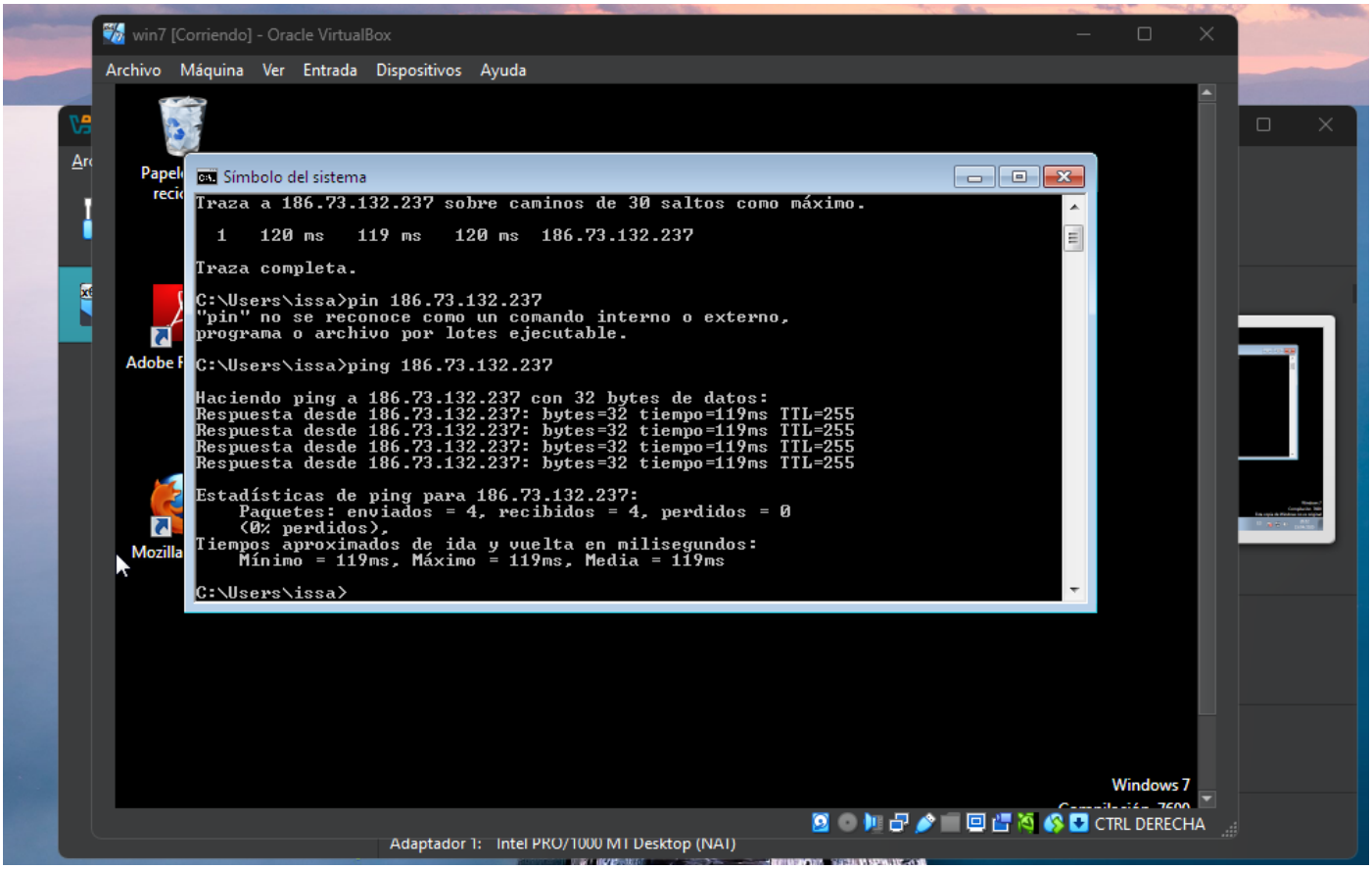
PRUEBAS DE CONEXIÓN REMOTA

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.