Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Incidentes de Ciberseguridad

UD03. Investigación de incidentes de ciberseguridad.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

1.- Descripción de la tarea.

Las Técnicas de Investigación de Incidentes

Como hemos estudiado en la Unidad 3, las técnicas de investigación de incidentes están asociadas al momento en el que se efectúa la investigación del incidente, a saber:

- ✓ **Antes de la aparición del incidente en el entorno**. Se trata de técnicas de prevención de incidentes a través del conocimiento profundo de los sistemas de la empresa. Una de las más habituales es constituir un Red Team o Equipo Rojo, con objeto de emular a los atacantes que dan lugar a los incidentes habituales. **El objeto de esta tarea será proponer una configuración de alto nivel para la plataforma de hacking ético de este Equipo Rojo.**
- ✓ **Durante la manifestación del incidente**. Técnicas de monitorización, alerta temprana y respuesta rápida.
- ✓ **Tras la finalización del incidente**. Técnicas de análisis forense.

En este caso práctico, nos vamos a centrar en la fase de análisis forense. Supondremos que se ha detectado una posible amenaza desde el SOC y acudimos al equipo que ha podido sufrir un ataque para analizarlo. Además, se procederá al análisis de un pen de datos que podría contener información confidencial de la empresa.

¿Qué te pedimos que hagas?

- ✓ **Descripción de los hechos acontecidos:**

En una mañana de trabajo del equipo de seguridad de la empresa “Unp4wn4ble Systems” saltan las alarmas en el SOC detectando una actividad sospechosa en la red interna de trabajo de la empresa.

El sistema IDS SIEM (detección de intrusos y manejo de eventos de seguridad) ha detectado una comunicación fuera de los normal entre dos equipos de la red.

El equipo Work-PC, con dirección IP: 10.0.2.4 ha establecido una comunicación hacia otro equipo de la red con dirección 10.0.2.7. Esta sería la comunicación establecida:

10.0.2.4:49358/TCP ↔ 10.0.2.7:6666/TCP

Produciéndose un tráfico de red entre estos equipos por los puertos indicados, lo cual no es usual, así que han saltado las alarmas en el SOC.

Uno de los técnicos de seguridad acude al equipo Work-PC donde encuentra al usuario del equipo que está encendiendo el equipo. El técnico de seguridad le comienza a realizar una serie de preguntas para averiguar qué ha podido suceder. Tras las preguntas realizadas obtiene la siguiente información: “El usuario al llegar por la mañana comenzó con su trabajo habitual y abrió su correo electrónico donde había encontrado un nuevo correo con una versión mejorada de la herramienta “putty.exe” que suele usar para determinadas conexiones por lo que procedió a la descarga de este software y lo ejecutó para ver qué tal funciona. Tras comprobar que no veía ninguna mejora aparente, al cabo de unos minutos cerró el programa de nuevo y prosiguió con su trabajo. Todo era normal hasta que de repente el equipo se le había apagado y al encenderlo de nuevo llegó el técnico de seguridad.”

Mientras el primer técnico acude al equipo indicado, otro da un aviso a seguridad para que observen si detectan algún sospechoso. Al poco tiempo, el empleado de seguridad comienza a revisar la identificación de todas las personas que intentan salir de la empresa. De repente, un

chico intenta salir corriendo y el empleado forcejea con él, pero finalmente se zafa y escapa, aunque se le cae un pequeño dispositivo de un bolsillo de su chaquetón, se trata de un dispositivo USB. Este dispositivo se pone a disposición del equipo de seguridad informática de la empresa.

Es el momento de que este departamento realice un análisis del equipo Work-PC y del pen drive de datos. Ha llegado el momento de la investigación…

**Nota: El análisis forense tiene una serie de fases secuenciales definidas para su correcta realización y validez. En este caso práctico vamos a reducir el análisis a la fase de recolección de evidencias del ataque sufrido, ya que la realización de todas las fases conllevaría un trabajo demasiado extenso para una realización telemática individual.*

✓ **Apartado 1: Deducción del posible ataque sufrido.**

Tras los datos y la información recabada por el SOC y de la declaración del trabajador. Realiza una reflexión sobre qué ha podido suceder respondiendo a las siguientes preguntas:

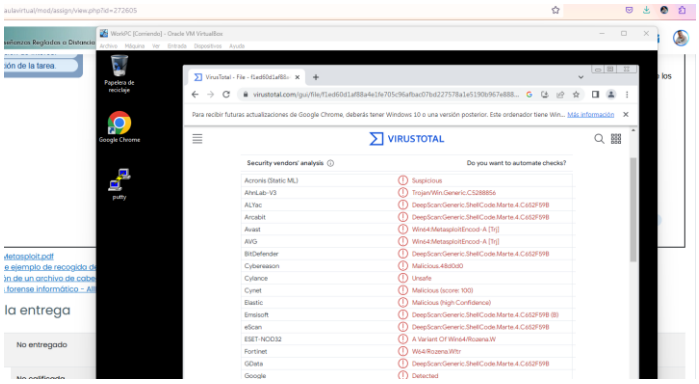
- Con respecto al correo electrónico recibido, ¿Crees que puede estar relacionado con algún tipo de incidente según la taxonomía de incidentes de ciberseguridad? Justifica la respuesta.

  Señala un posible caso de phishing, donde un correo con apariencia legítima (a juzgar por la actuación del empleado) le está instando a descargar e instalar una nueva versión de la herramienta putty.exe

- El software ejecutado por el trabajador, ¿podría tratarse de un software no legítimo o por el hecho de ejecutarlo y funcionar con normalidad podemos descartar esa teoría? ¿qué método se usa para la comprobación de la integridad de las aplicaciones descargadas?

  No. El hecho de funcionar con normalidad no descarta la teoría (aunque tampoco funcionó con normalidad total, visto que se le apagó en cuanto cerró el programa, apuntando a un software no legítimo).

  Puede comprobar desde una fuente oficial si hay una nueva versión. Verificar la integridad mediante la verificación de la firma digital a través de VirusTotal o de SignCheck. Comparar que coincide el Hash publicado por el desarrollador con el del archivo descargado, o podría haberlo pasado por el antivirus antes de la instalación e incluso, durante la misma, es positivo estar atento a posibles permisos inusuales.



Análisis con Virustotal de putty.exe

  En el ámbito empresarial es además positivo tener un área de carga y descarga o una SandBox donde comprobar de forma aislada y segura dichos archivos.

✓ **Apartado 2: Análisis de la máquina víctima.**

**Nota: Al pie de la práctica hay un tutorial práctico sobre el uso del framework "Metasploit". No es necesario realizar ninguna de las acciones que se explican en este tutorial, pero su lectura puede ser muy útil para tener más claro cómo analizar la víctima, ya que conociendo cómo se pueden atacar máquinas, se pueden analizar mejor los rastros que dejan los atacantes.*

Realiza una recolección de evidencias de que la máquina ha podido sufrir un ataque.

Para este análisis se considera que se ha realizado una clonación del sistema y te han proporcionado una copia, que sería la que se encuentra en el siguiente recurso:

WorkPC.ova

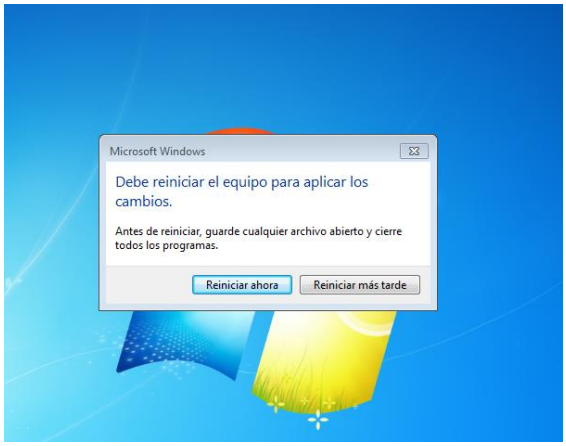
Credenciales de acceso: usuario: Worker. Clave: Unp4wn4ble

Máquina preparada para instalar en VirtualBox.

Realiza los siguientes análisis en caso de ser posible, para ello:

➢ En el caso de análisis de la memoria RAM de la máquina y de cachés, ¿se podría obtener alguna información del posible ataque realizado? ¿Por qué?

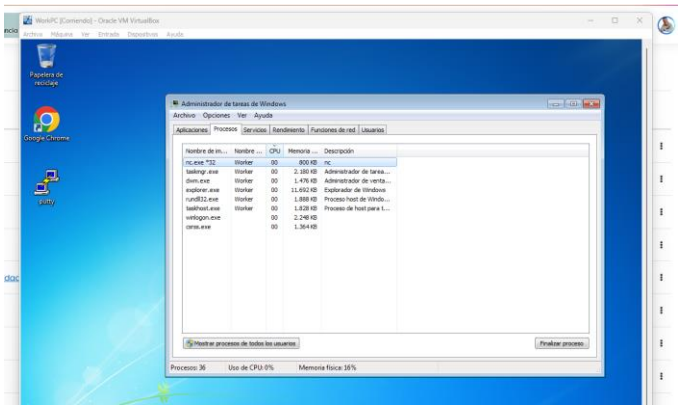
Según arranco la máquina me pide reiniciar es sistema.



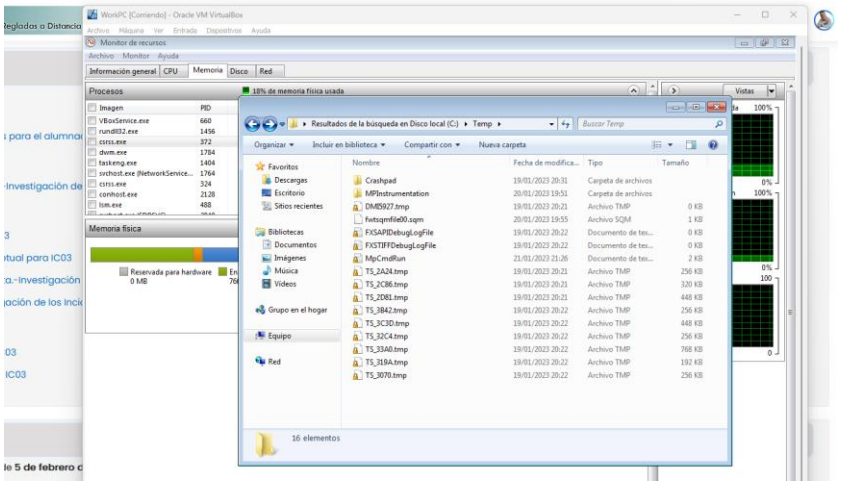
Entiendo que la copia mantiene el estado de la máquina infectada. Visto eso, podemos buscar primero elementos inusuales en el Administrador de tareas.

Observamos dos que pueden ser sospechosos:

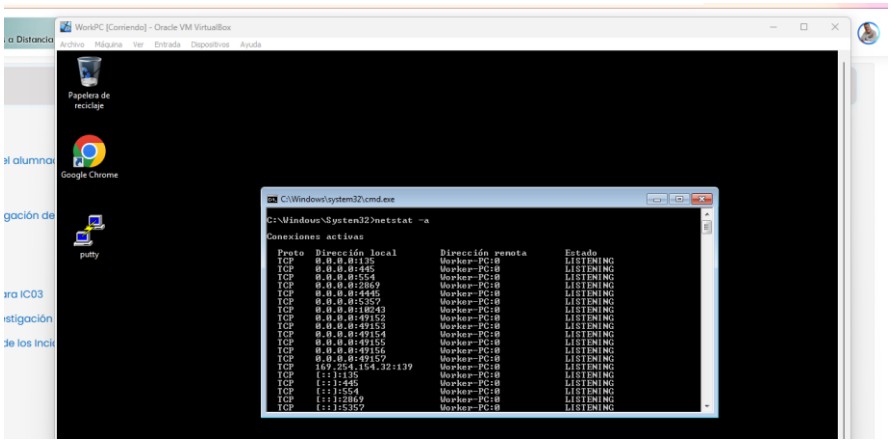
`nc.exe *32` y **`csrss.exe`** que mantienen ubicaciones inusuales



También podemos revisar posibles archivos extraños entre los temporales.



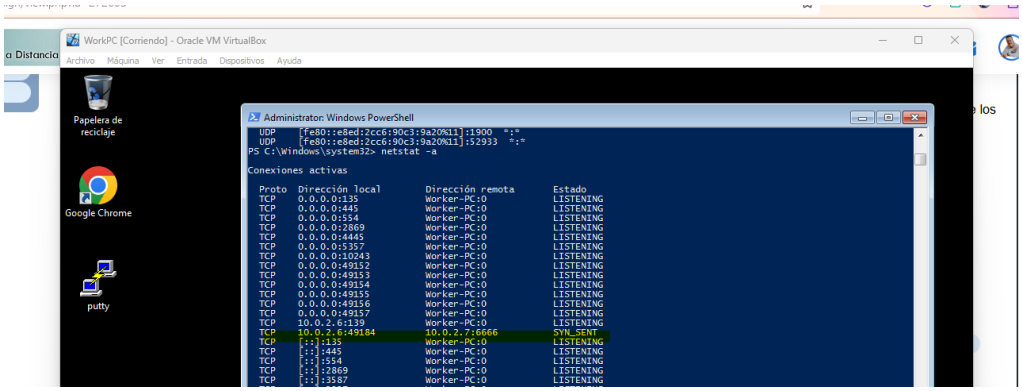
En las conexiones, de momento, no veo nada extraño.



Reinicio entonces la máquina para observar cambios y teniendo en cuenta estos datos.

- Tras analizar las conexiones de red, ¿existen datos que confirmen una conexión o intento de conexión local hacia otra máquina de la red?

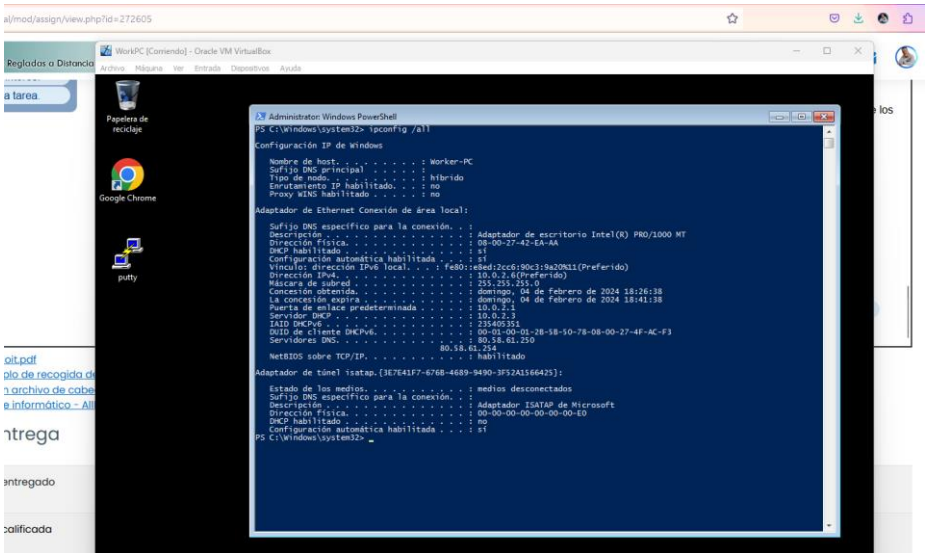
`netstat -a`



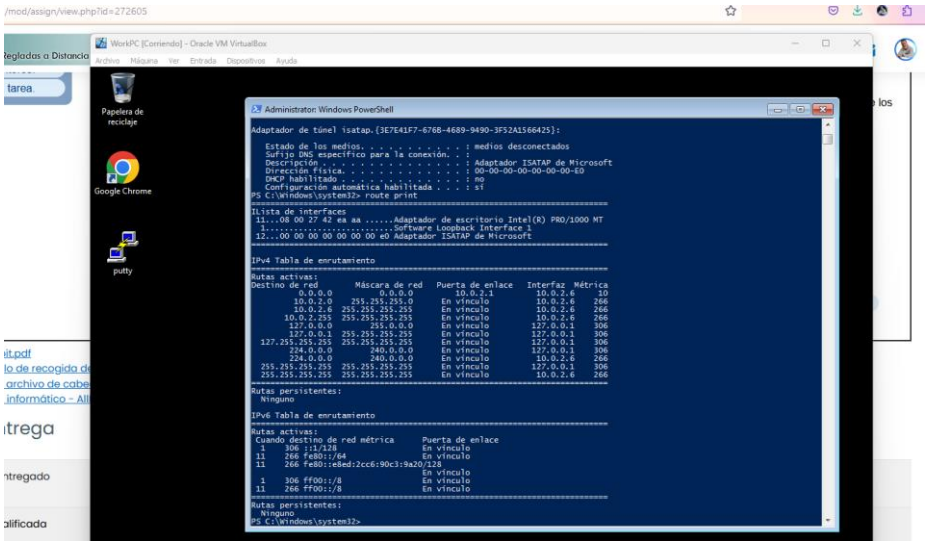
Arranco **`Putty`**. Comprobamos que, al igual que sucedía en el enunciado, hay una conexión desde la **`IP 10.0.2.7`** con estado **`SYN_SENT`** (a la espera de conexión), por lo que podemos deducir que el atacante está a la escucha, durante un corto periodo, desde el puerto **`6666`**.

Reviso la IP e imprimimos rutas para confirmar que ya aparece.

`ipconfig /all`

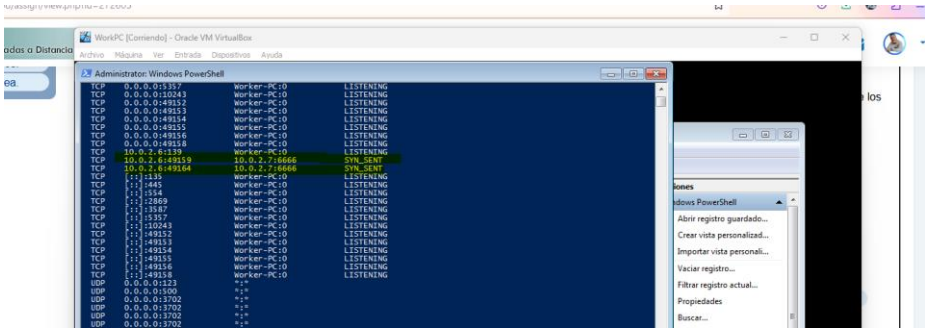


`route print`

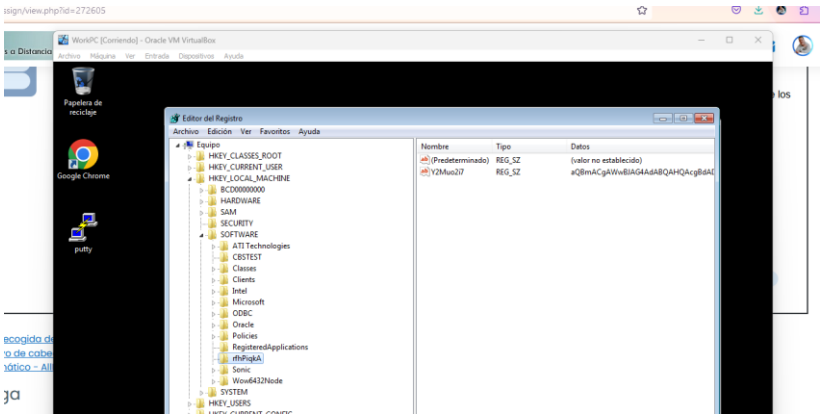


➢ Tras analizar la red, si se han descubierto intentos de conexión es muy probable que estén provocados por intentos de persistencia de un ataque perpetrado tras apagados de la máquina. Intenta localizar evidencias del intento de persistencia mediante un análisis del registro de Windows localizando el servicio que activa.

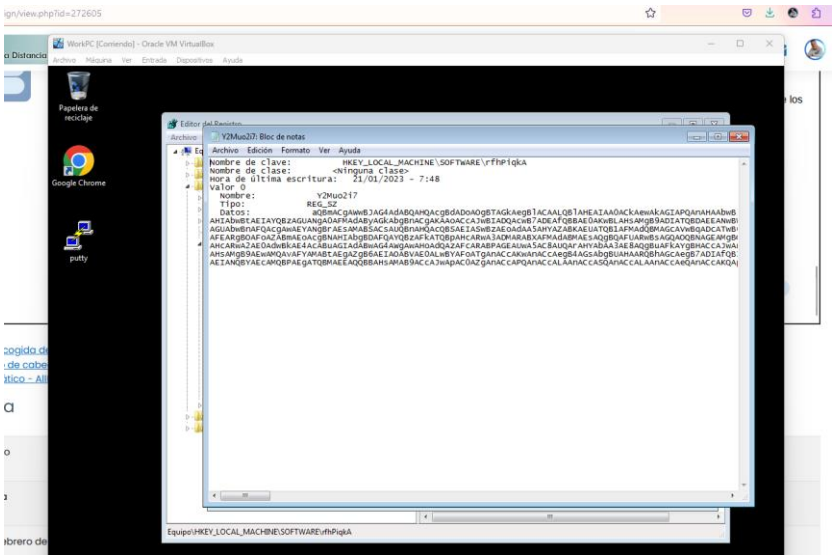
Realizo un par de apagados de la máquina y volvemos a revisar las conexiones, para unos segundos después, buscar información en el registro.



Busco directorios que puedan ser sospechosos y comienzo a ver algunos registros en formato Base64.

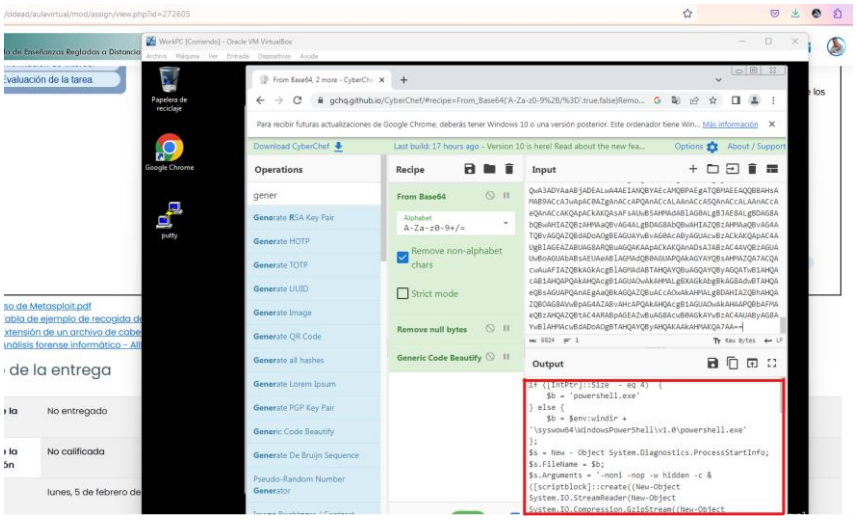


Lo exporto para poder revisarlo y viendo que es son datos en Base64, intentaremos descifrarlo.

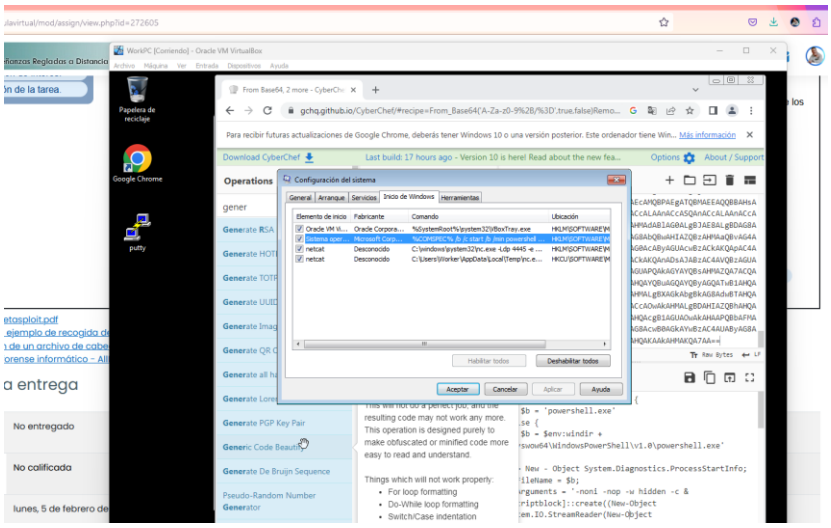


Paso el contenido del archivo por **CyberChef**.

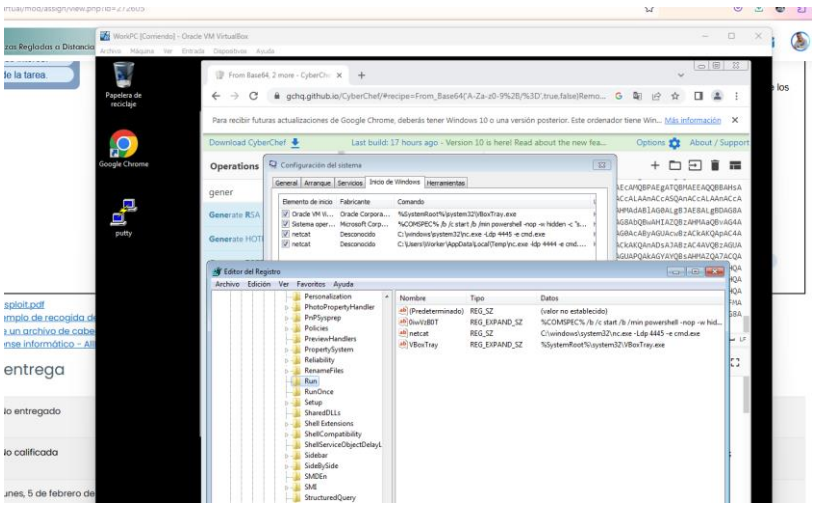
Aparenta ser un comando para ejecutarse desde powershell, lo que nos hace sospechar que se trata de malware.



Abro la configuración del sistema para confirmar que está entre las tareas de inicio.



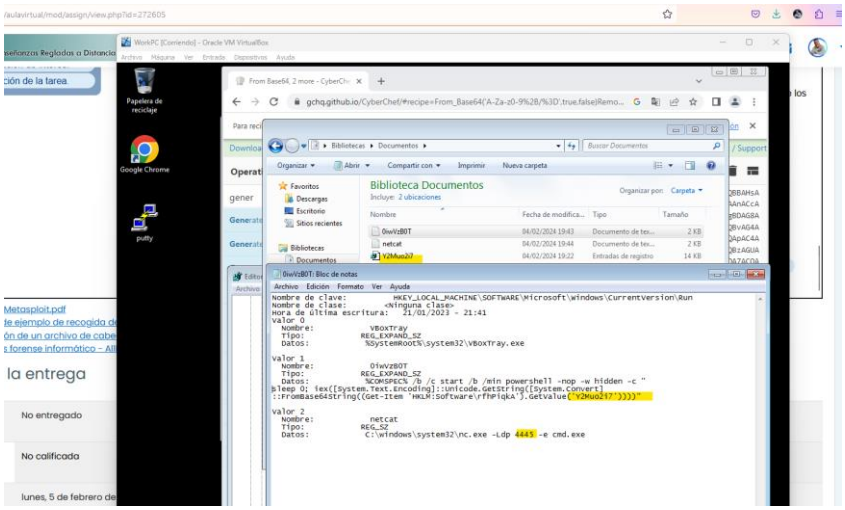
Por lo que se observa, aparece no solo el powershell, sino dos procesos **`netcat`**.



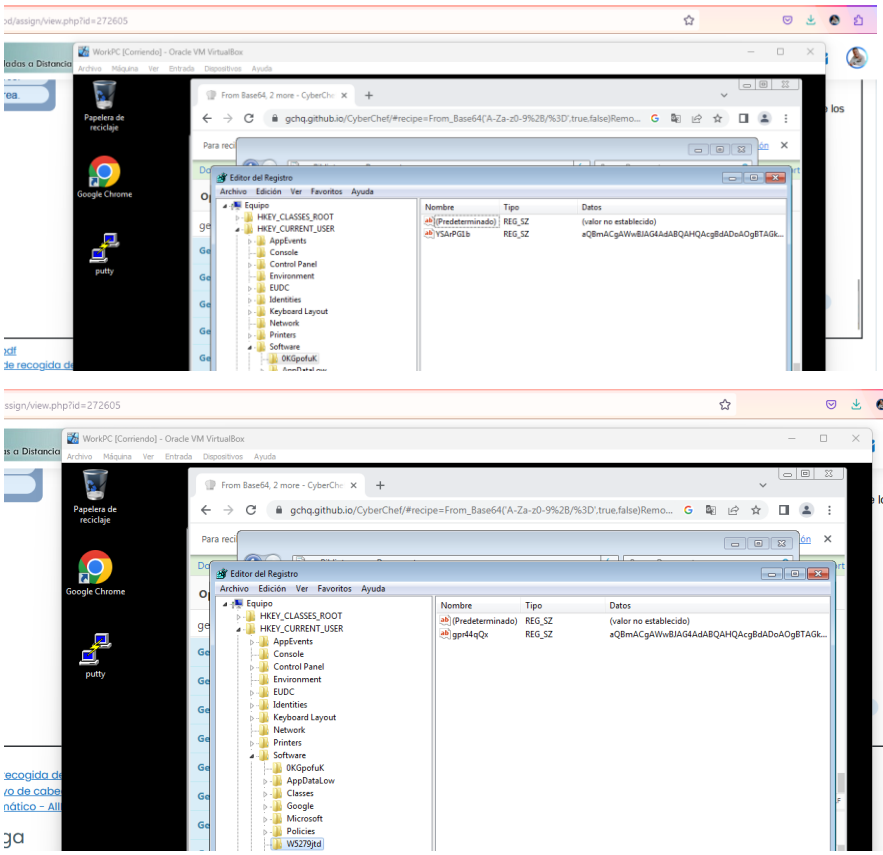
Uno de ellos queda a la escucha desde **`worker`** y el otro escucha desde **`System32`**

Volvemos al registro y en el apartado **`Run`** (arranque) vuelve a estar junto a otro más que también es sospechoso.

Al exportarlo y abrirlo, vemos la relación.



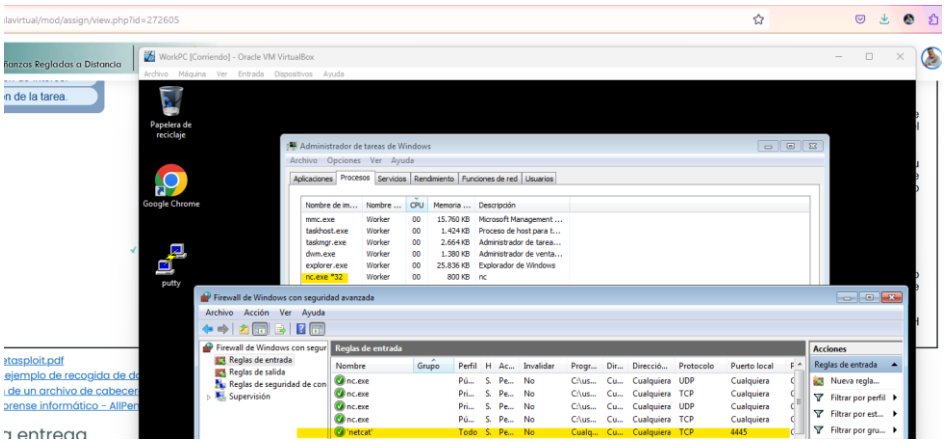
Si seguimos buscando, se pueden ver más claves para el mismo base64.



- Otra característica importante a tener en cuenta serían los procesos, ¿hay algún proceso que sea sospechoso de que se ha sufrido un ataque? Tras su localización, investiga cómo se ha podido conseguir lanzar este proceso encontrando las modificaciones del sistema que han hecho posible la creación de este proceso con el arranque de la máquina. (Análisis del registro, posibles ficheros en alguna ubicación del disco, reglas de entrada de firewall). (Extra, no solicitado en la práctica: Puedes intentar realizar una prueba de conexión hacia esta máquina para comprobar la "puerta abierta").

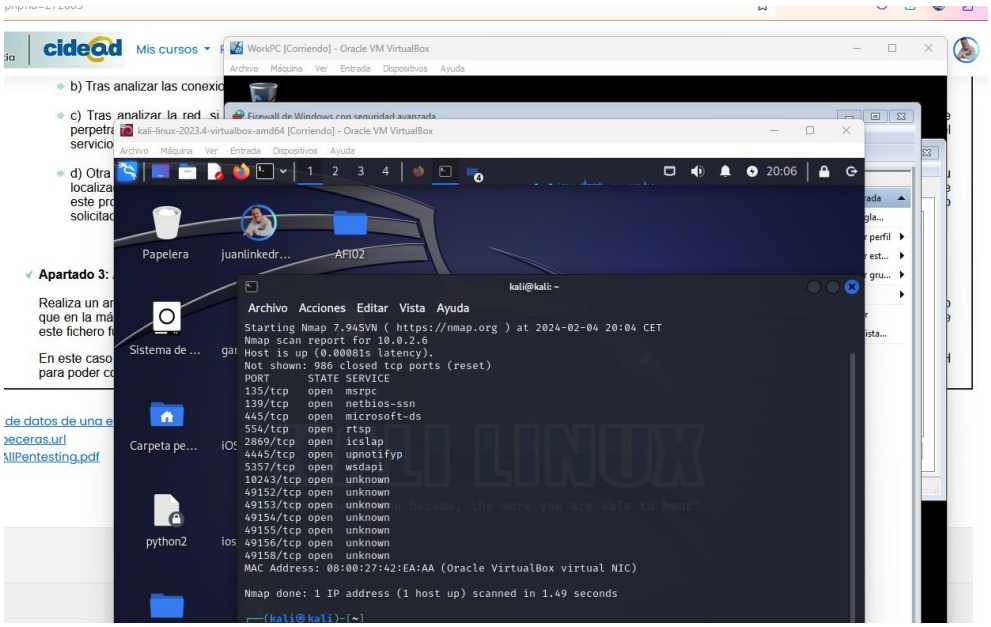
Retomo la información del punto primero donde veíamos procesos que eran sospechosos.

Abriendo las reglas del Firewall, podemos ver que hace referencia abriendo el puerto **4445** de **TCP**.



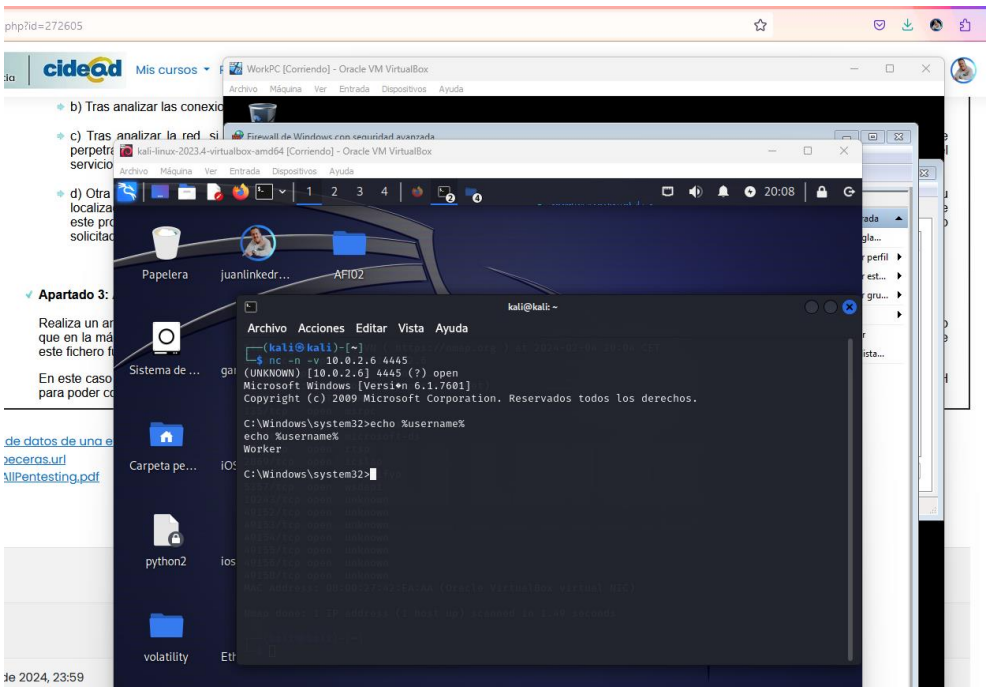
Compruebo con **nmap** si el puerto está abierto

```
sudo nmap -sS 10.0.2.6
```



Pruebo entonces la conexión contra la máquina

```
nc -n -v 10.0.2.6 4445
```



✓ **Apartado 3: Análisis del pen de datos requisado.**

Realiza un análisis de los datos encontrados en el pen drive que se le cayó a la persona atacante en el momento de su huida. Pasado un tiempo se ha detectado que en la máquina infectada falta un documento llamado "Fórmula de la felicidad.docx", por lo que el objetivo principal de este análisis es intentar demostrar que este fichero fue sustraído y se encuentra en alguna ubicación en el pen de datos, aunque puede que no sea tan evidente su localización.

En este caso se provee de una imagen del dispositivo que ha sido extraída con "GuyManager". Además de esta imagen, se incluye un fichero con su firma HASH para poder comprobar la integridad de la imagen descargada. El enlace a estos ficheros es el mismo del apartado anterior.

Imagen del pen de datos: datosPen.E01

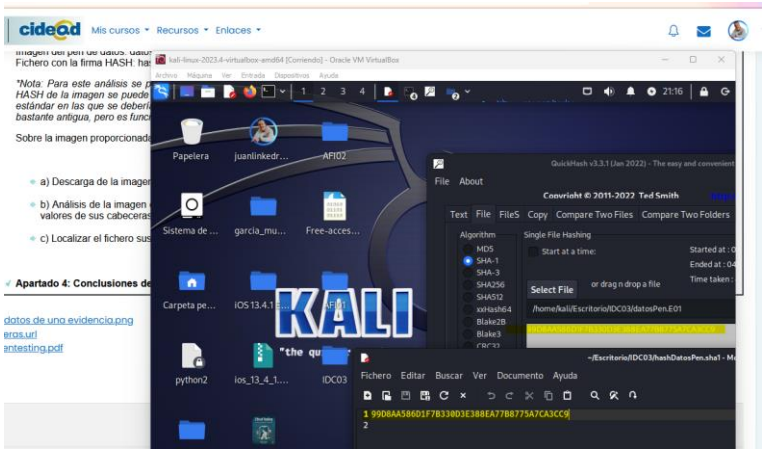
Fichero con la firma HASH: hashDatosPen.sha1

**Nota: Para este análisis se puede usar cualquier herramienta de análisis de imágenes, aunque se recomienda el uso de Autopsy. Para la comprobación del HASH de la imagen se puede usar la herramienta QuickHash. Estas herramientas se pueden instalar en Windows o se pueden usar desde distribuciones Linux estándar en las que se deberían instalar o en distribuciones Linux especializadas como Kali Linux o CAINE. La versión de Autopsy incorporada en Kali Linux es bastante antigua, pero es funcional. La elección del software a usar es libre.*

Sobre la imagen proporcionada realiza las siguientes acciones:

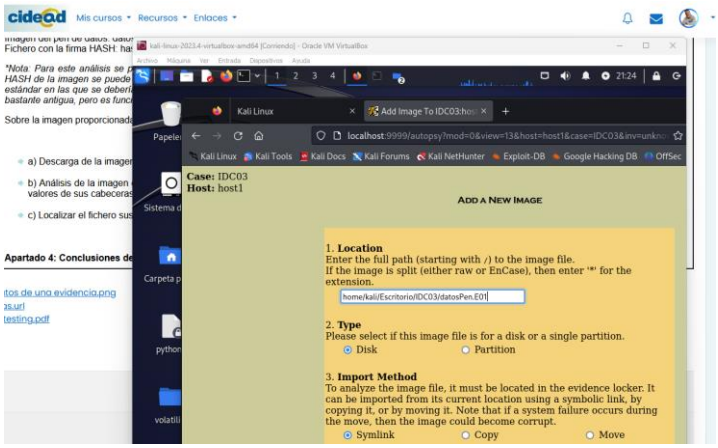
- Descarga de la imagen y comprobación de la integridad de esta imagen mediante la comprobación de su hash.

  Descargo la imagen y la firma, comprobando la integridad con **`QuickHash`**.



- Análisis de la imagen del pen de modo que compruebes si existe algún fichero que está corrompido, por lo que se ha podido modificar algún dato de los valores de sus cabeceras y ser ilegibles.

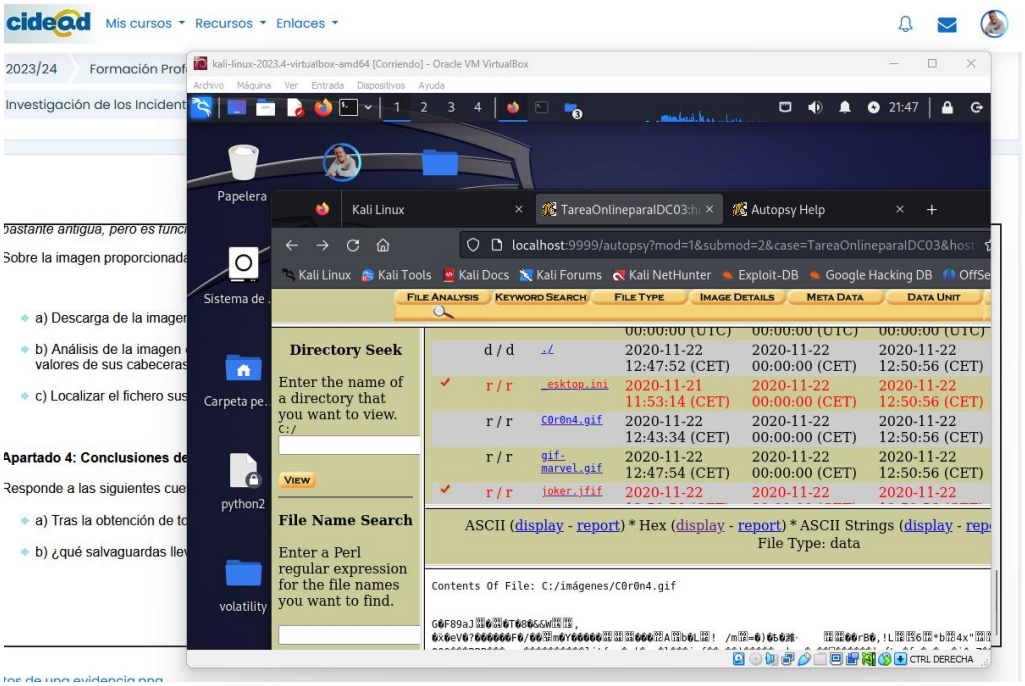
  Creo un nuevo caso en **`Autopsy`** para esta parte de la tarea.



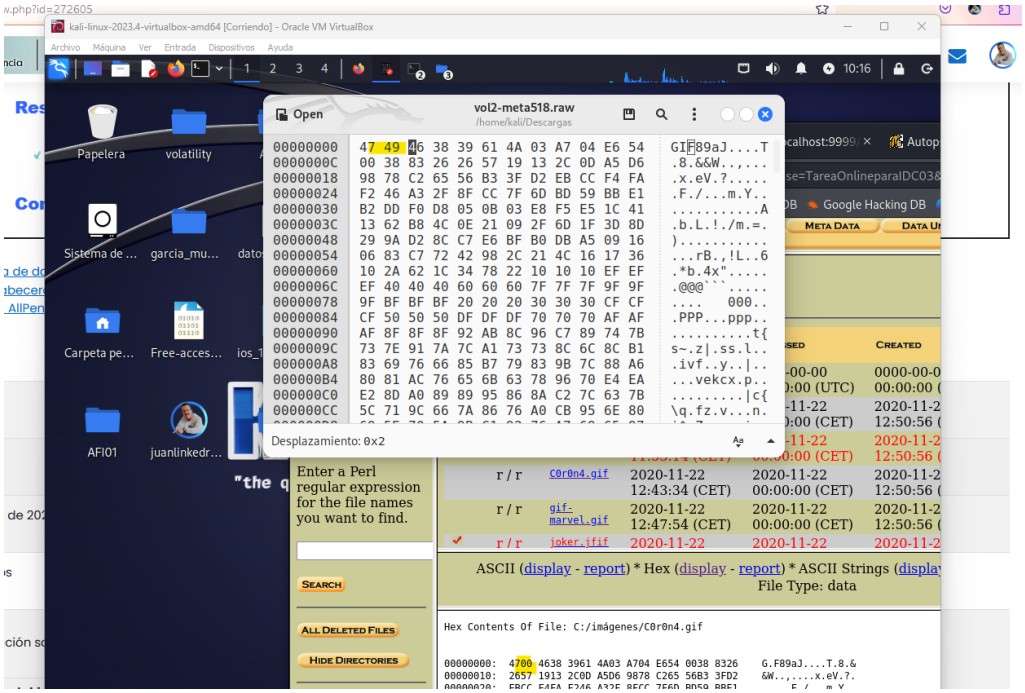
Tras cargar la imagen, procedemos a analizar los datos.

Tras la revisión podemos observar que una de las imágenes (**`C0r0n4.gif`**) no abre correctamente.

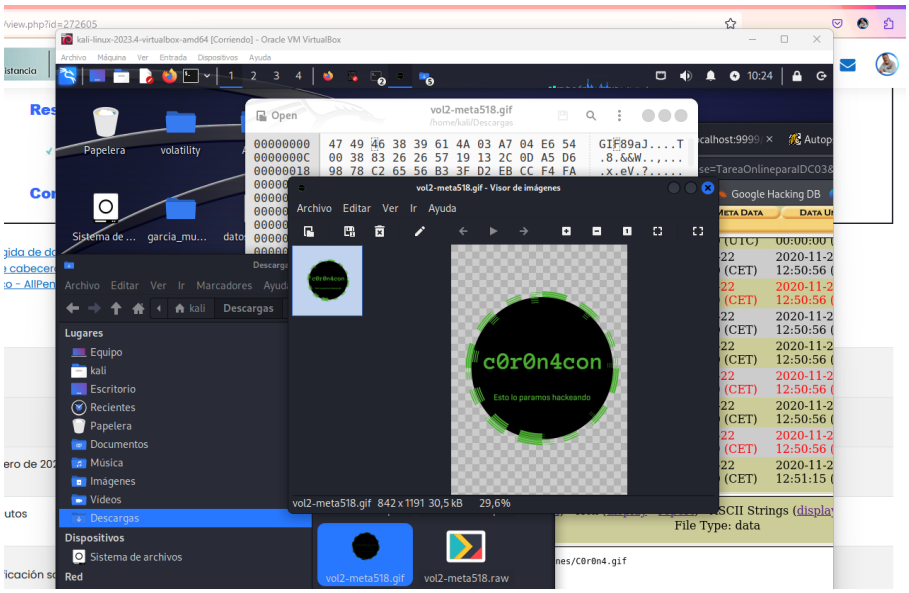
Parece ser un archivo **`gif.`**



Tras revisar los hexadecimales, vemos que la cabecera no coindice con las cabeceras gif, así que procedo a abrirlo para editarlo desde **`GHex`**.

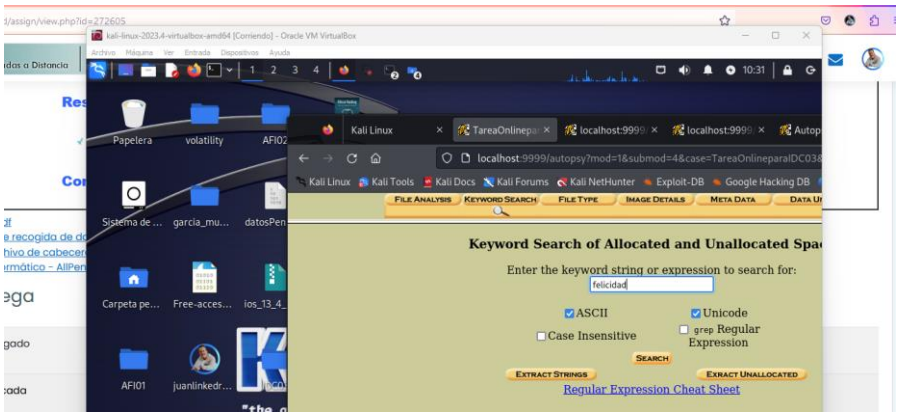


Tras modificarlo, guardamos el archivo con extensión **`.gif`** y lo abrimos.

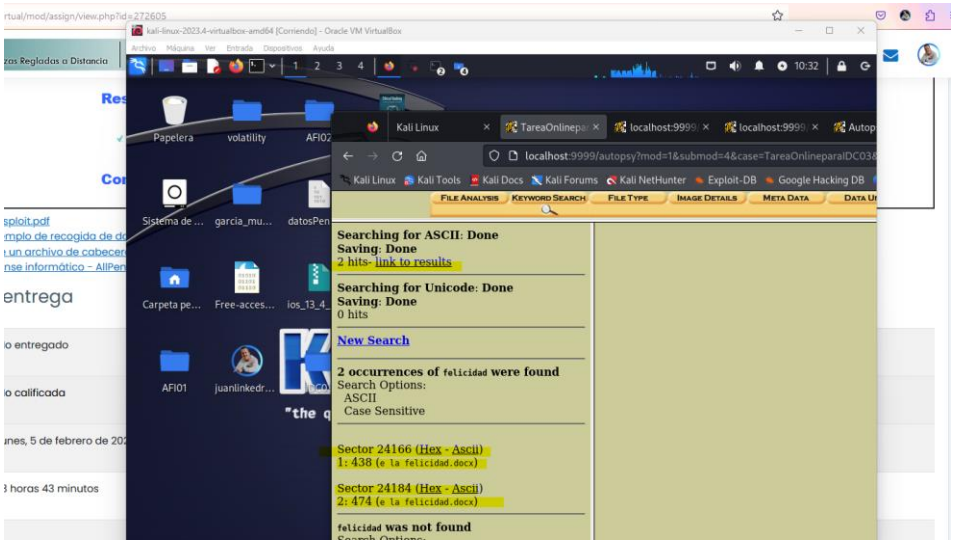


- Localizar el fichero sustraído en la información. Puede que esta información no esté a la vista, sino que esté ofuscada en otro fichero.

Proseguimos entonces desde la misma herramienta y hago una búsqueda de la palabra clave **“`felicidad`”**.

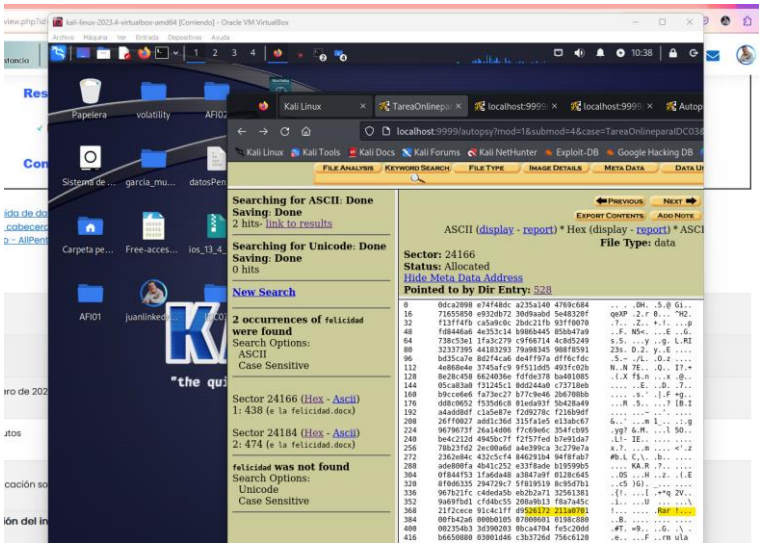


Muestra dos resultados:

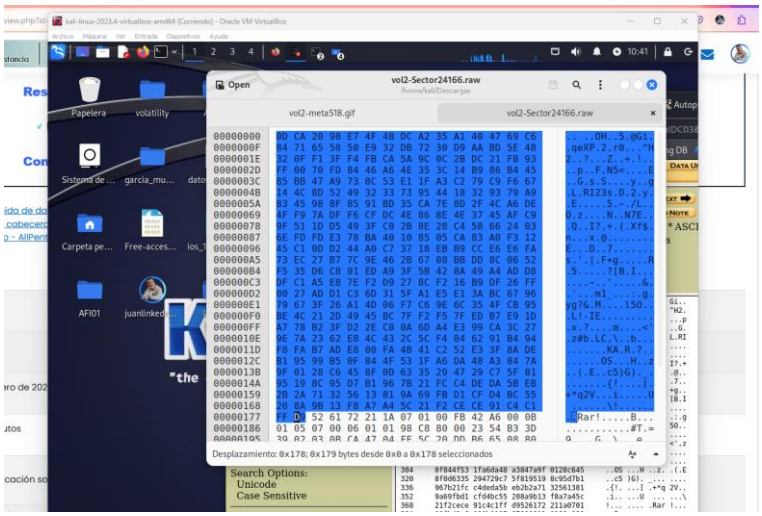


Tras revisarlos, veo que la cabecera rar está en medio del archivo.

Lo exporto para trabajar con seguridad y poder editarlo desde **GHex**.

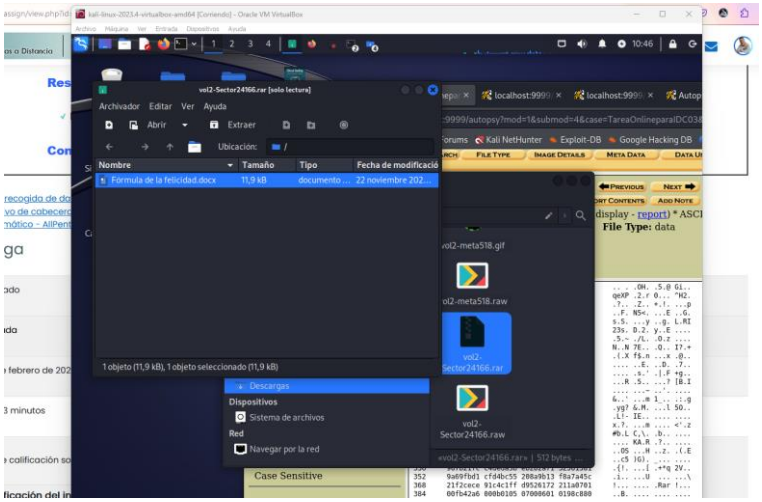


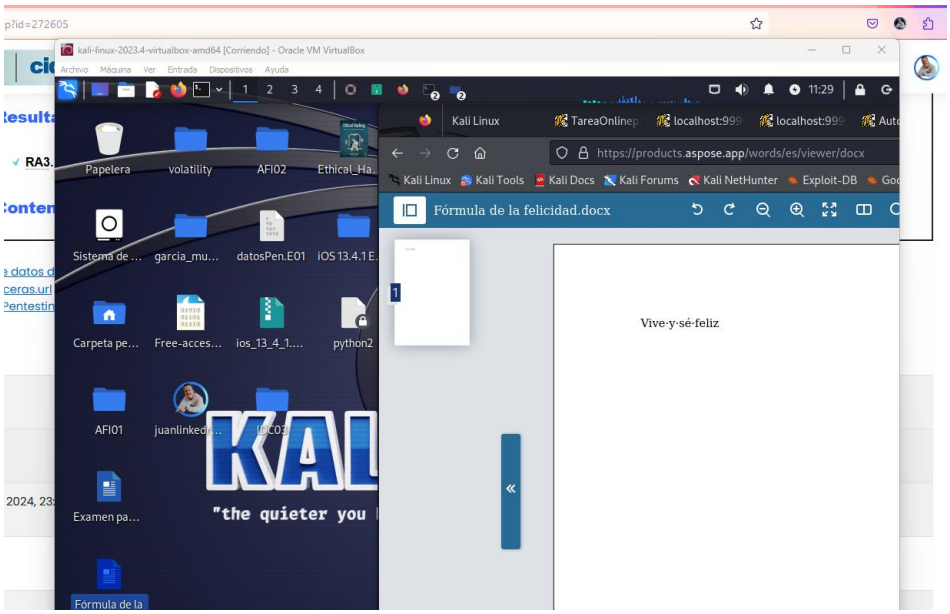
Elimino todo lo anterior a la cabecera **rar**.



Vuelvo a guardar con extensión **.rar** y abro el fichero creado.

Vemos dentro el documento de texto **"Fórmula de la felicidad.docx"**.





✓ **Apartado 4: Conclusiones del análisis realizado.**

Responde a las siguientes cuestiones:

➢ Tras la obtención de todas las evidencias, ¿dónde crees aspectos crees que falló principalmente la seguridad de la empresa? Indica dos aspectos.

- Formación y sensibilización: El empleado a descargado y ejecutado un software sin conocer los riesgos y/o por no seguir los correctos protocolos que entiendo debería tener la empresa. Como ya sabemos, es necesaria la formación en seguridad y concienciar al personal de un correcto uso de los recursos y herramientas para evitar problemas de seguridad como este.
- Protección antimalware: la acción se realizó, o por no tener un antivirus actualizado que alertara del riesgo y/o sin comprobar la autenticidad del ejecutable.

➢ ¿qué salvaguardas llevarías a cabo para reducir el riesgo de volver a sufrir un incidente similar? Indica al menos dos salvaguardas.

Siguiendo la argumentación del punto anterior:

- Formar y sensibilizar al personal en identificación de riesgos asociados a las descargas o ejecución de software sin comprobar su autenticidad.
- Implementar soluciones siempre actualizadas de antivirus y antimalware en todos los equipos de la red.

Webgrafía.

https://www.virustotal.com/gui/home/upload

https://gchq.github.io/CyberChef/

https://github.com/SVelizDonoso/forense-autopsy