Challege REvil Corp

- *Andres Valdivieso Pinilla - Líder de Ciberseguridad (Consultor)*
- *www.linkedin.com/in/andres-valdivieso-pinilla*

Como parte del apoyo en el uso de la herramienta Redline realice el desafío de REvil Corp en esta maquina podemos encontrar un ejercicio de respuesta a incidentes donde necesitamos analizar un host infectado mediante Redline.

Investigación del punto final comprometido

El Escenario Que Nos Presentan en el Desafío

Nos indica que Uno de los empleados de Lockman Group llamó al departamento de TI; el usuario estaba frustrado y mencionó que todos sus archivos habían cambiado de nombre a una extensión de archivo extraña que nunca había visto antes.

Después de observar la estación de trabajo del usuario, el técnico de TI ya sabía lo que estaba sucediendo y transfirió el caso al equipo de respuesta a incidentes para que investigaran más a fondo.

y que nosotros somos los encargados de responder a los incidentes.

Contextualización

**Antes de entrar a la resolución de este desafío me gustaría contextualizar un poco sobre la herramienta:

- Donde tenemos que Redline®, es una de las principales herramientas gratuita de seguridad de endpoints de FireEye, ofrece a los usuarios capacidades de investigación de host para encontrar señales de actividad maliciosa mediante el análisis de archivos y memoria y el desarrollo de un perfil de evaluación de amenazas. Utilice Redline para recopilar, analizar y filtrar datos de endpoints y realizar análisis de IOC y revisión de aciertos. Además, los usuarios de Endpoint Security (HX) de FireEye pueden abrir recopilaciones de triaje directamente en Redline para realizar un análisis en profundidad, lo que permite al usuario establecer la cronología y el alcance de un incidente.
  - Esto es lo que podemos hacer usando Redline:
  - Recopilar datos de registro (solo hosts de Windows)
  - Recopilar procesos en ejecución
  - Recopilar imágenes de memoria (antes de Windows 10)
  - Recopilar el historial del navegador
  - Busque cadenas sospechosas
  - Y Mucho mas.
- También podemos apoyarnos en otra de las herramientas de FireEye como el IOC Editor. El editor de indicadores de compromiso (IOC) de FireEye es una herramienta gratuita que proporciona una interfaz para gestionar datos y manipular las estructuras lógicas de los IOC. Los IOC son documentos XML que ayudan a los responsables de responder a incidentes a capturar información diversa sobre amenazas, incluidos los atributos de archivos maliciosos, las características de los cambios de registro y los artefactos en la memoria. El editor de IOC incluye:
  - Manipulación de las estructuras lógicas que definen el IOC
  - Aplicación de metainformación a los IOC, incluidas descripciones detalladas o

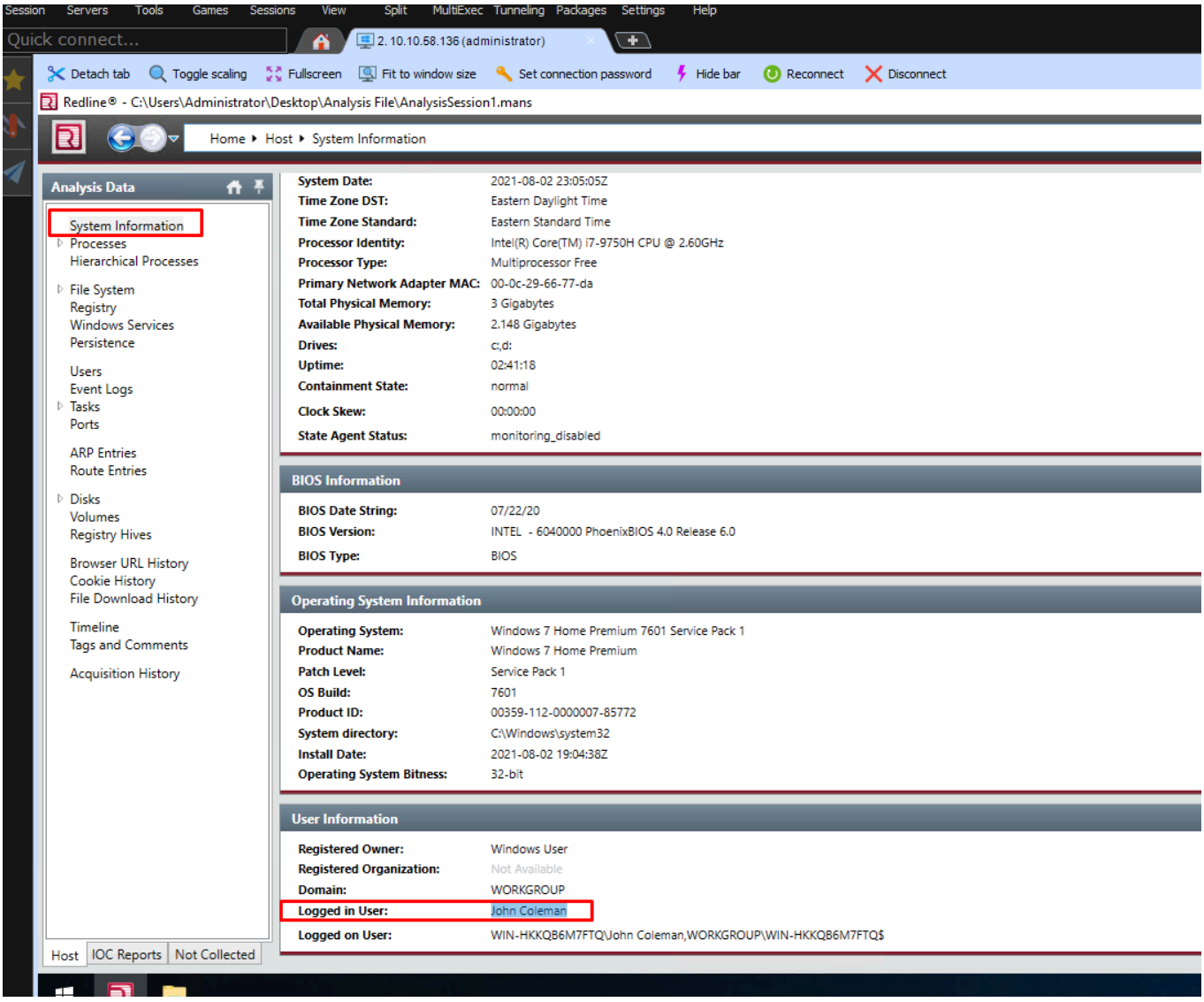
etiquetas arbitrarias
- Conversión de IOC en filtros XPath
- Gestión de listas de “términos” utilizados en los IOC

Ya con esta contextualización comenzamos a realizar la Cacería!.

Responda las preguntas a continuación

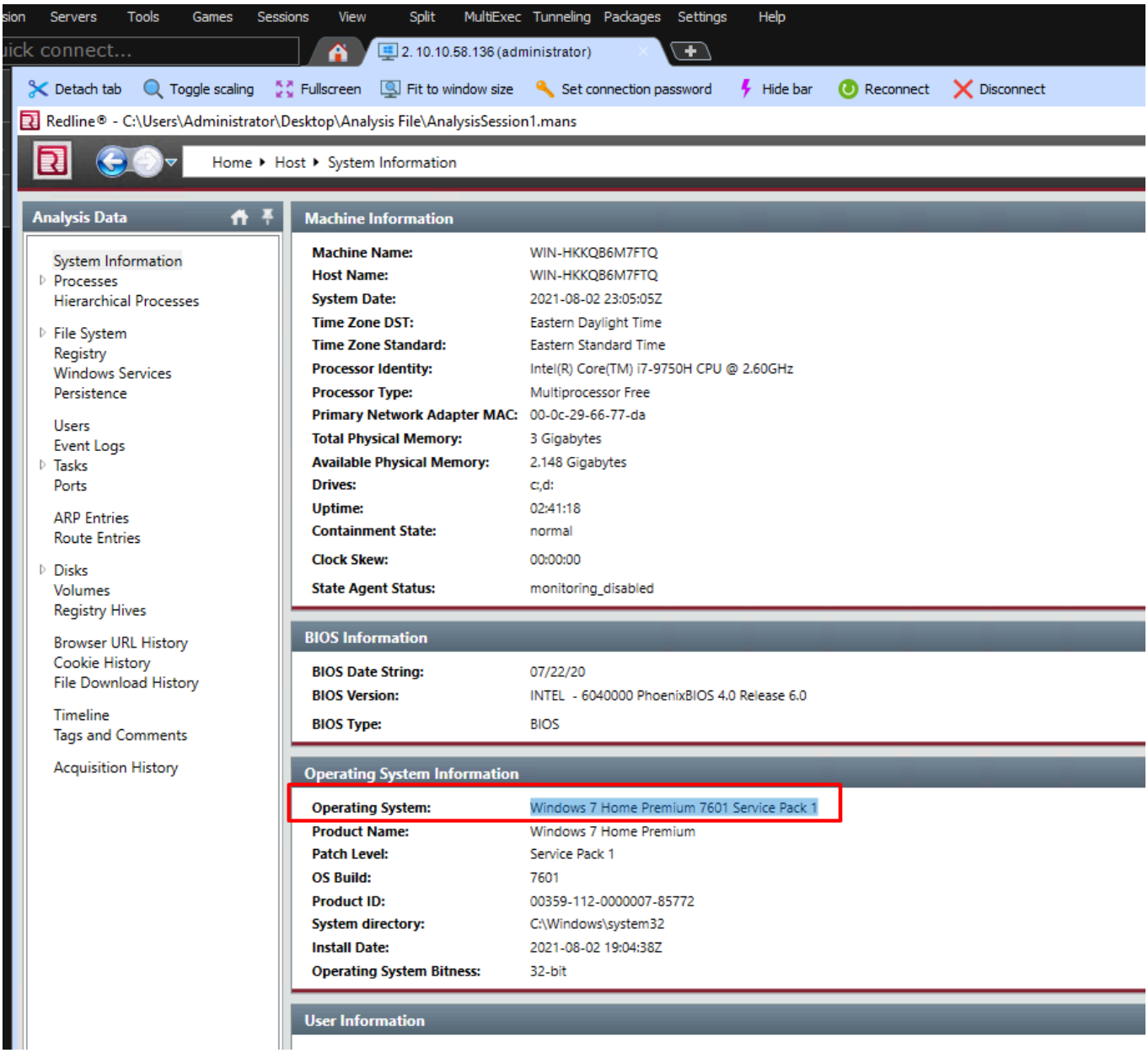
¿Cuál es el nombre completo del empleado comprometido?

De acuerdo con lo indicado en el escenario el archivo que contiene la información del evento esta en el escritorio, al abrirlo tenemos dos menús uno que nos muestra los datos analizados y un panel mas grande del costado derecho como estamos buscando el nombre del usuario, se debe buscar en el **System Information** acá tenemos información del equipo en general:



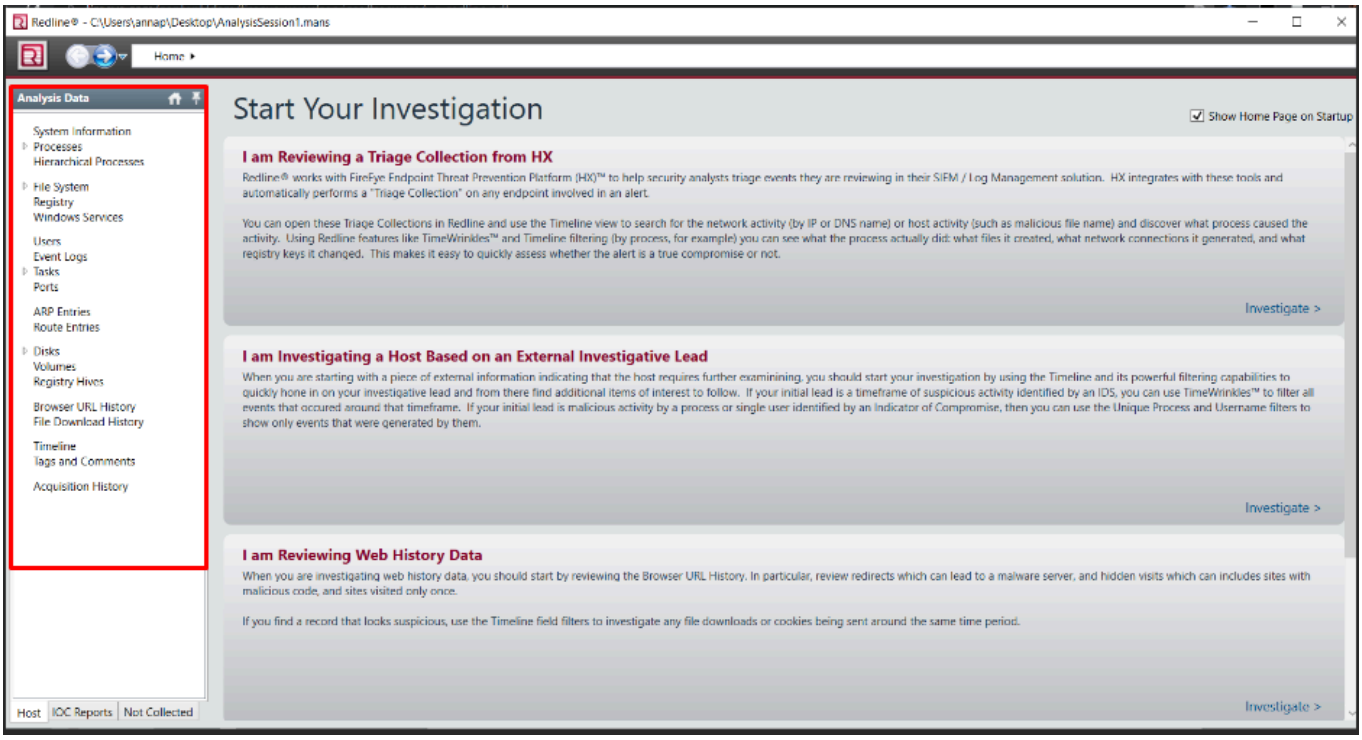
¿Cuál es el sistema operativo del host comprometido?

Ahora solicitan que proporcionemos el S.O. este esta en el mismo lugar:

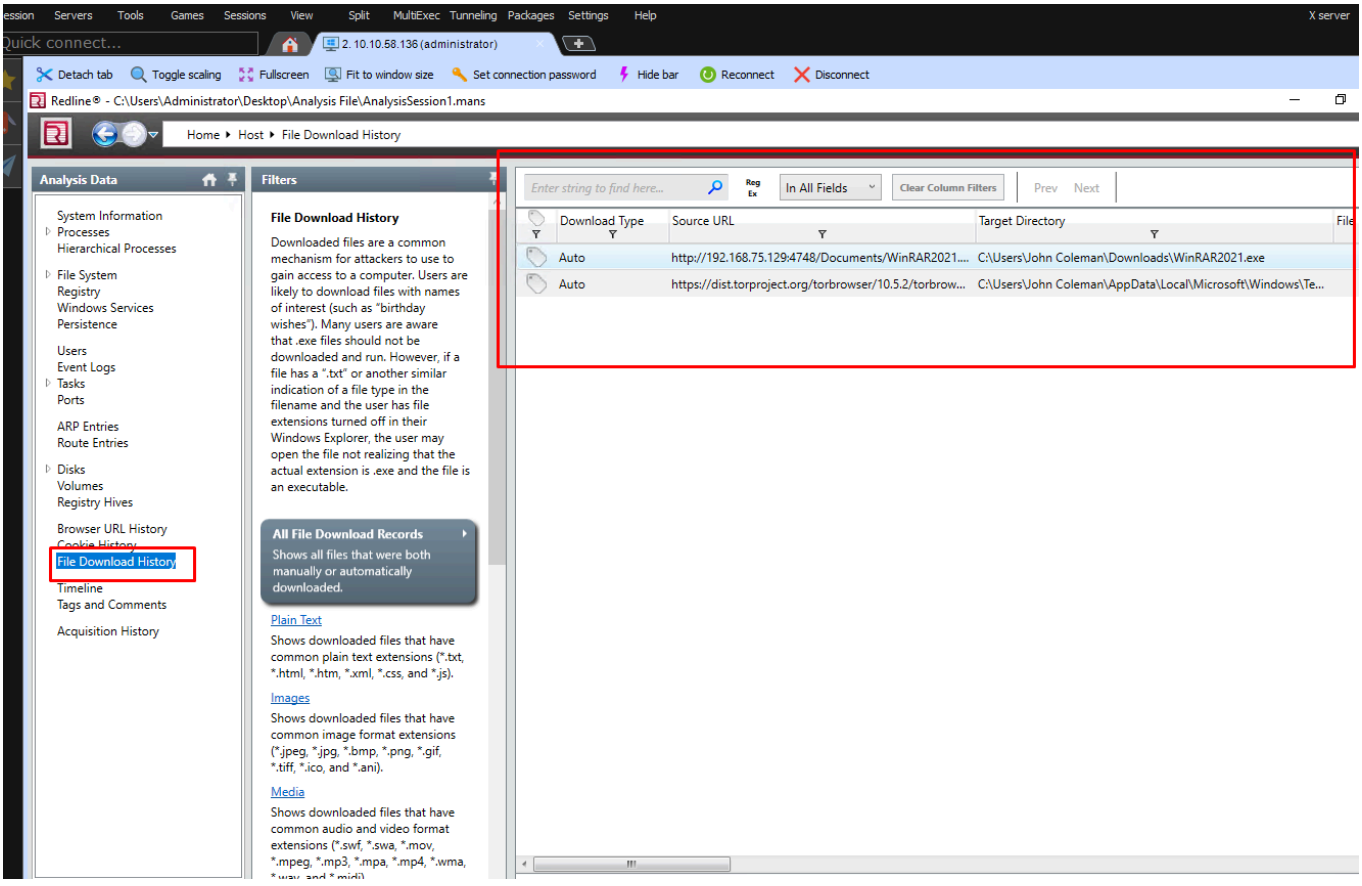


¿Cuál es el nombre del ejecutable malicioso que abrió el usuario?

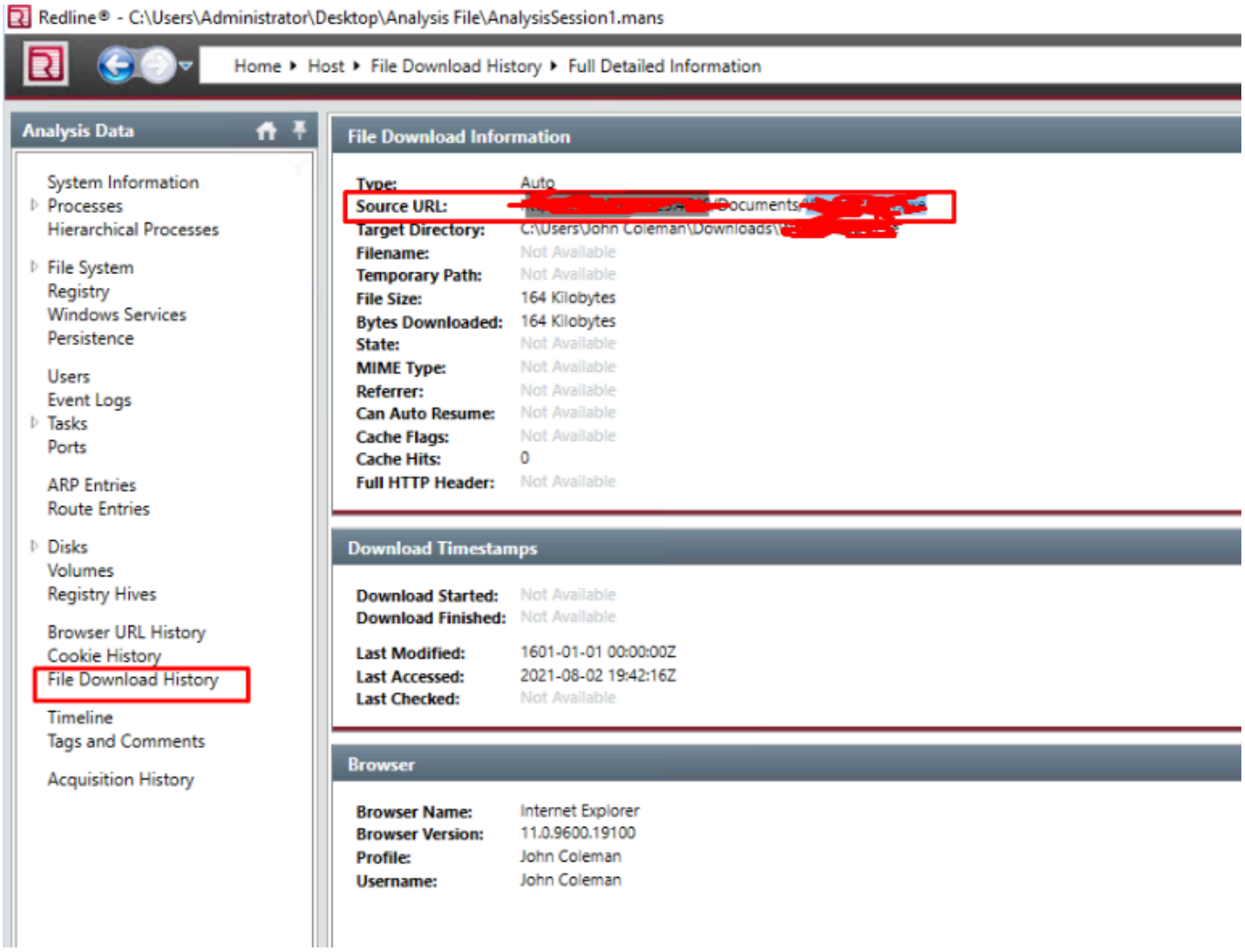
Posteriormente ya entramos a buscar la información que esta asociada con el ejecutable malicioso para esto podemos ver el panel izquierdo en este encontramos los datos que se recolectaron, dentro de ellos podemos ver que tenemosuna gran cantidad de opciones que se analizaron demos determinar que opción escoger (Es bueno antes de analizar darse un paseo por todos los Ítems analizados para ver que datos nos muestran):



Después de validar los menús vemos que lo que buscamos esta en la ruta de los archivos descargados, acá podemos ver que fue lo que descargo el usuario y encontramos dos recursos :

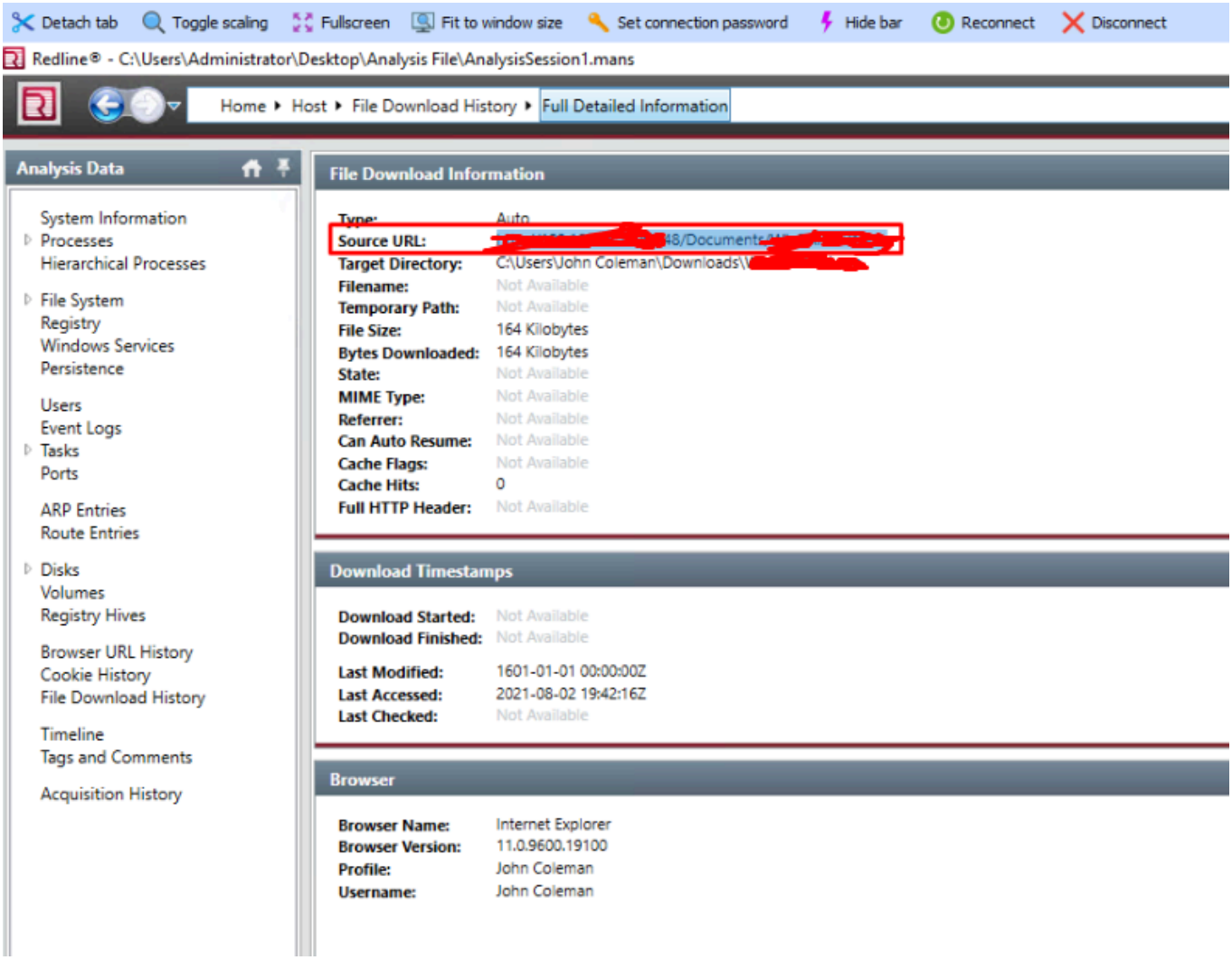


Ingresamos a los recursos dando doble clic y validamos que información contienen y determinamos que la descarga maliciosa se ve después de descargar el siguiente archivo Desde esta parte no mostrare la respuesta con e fin de que lo repliquen en la plataforma debido a que es la mejor forma de aprender a usar la herramienta quedaran algunas indicaciones de cual puede ser la respuesta si ingresan y validan los eventos verán las mismas horas tamaños de archivo y podrán deducir cual es este:



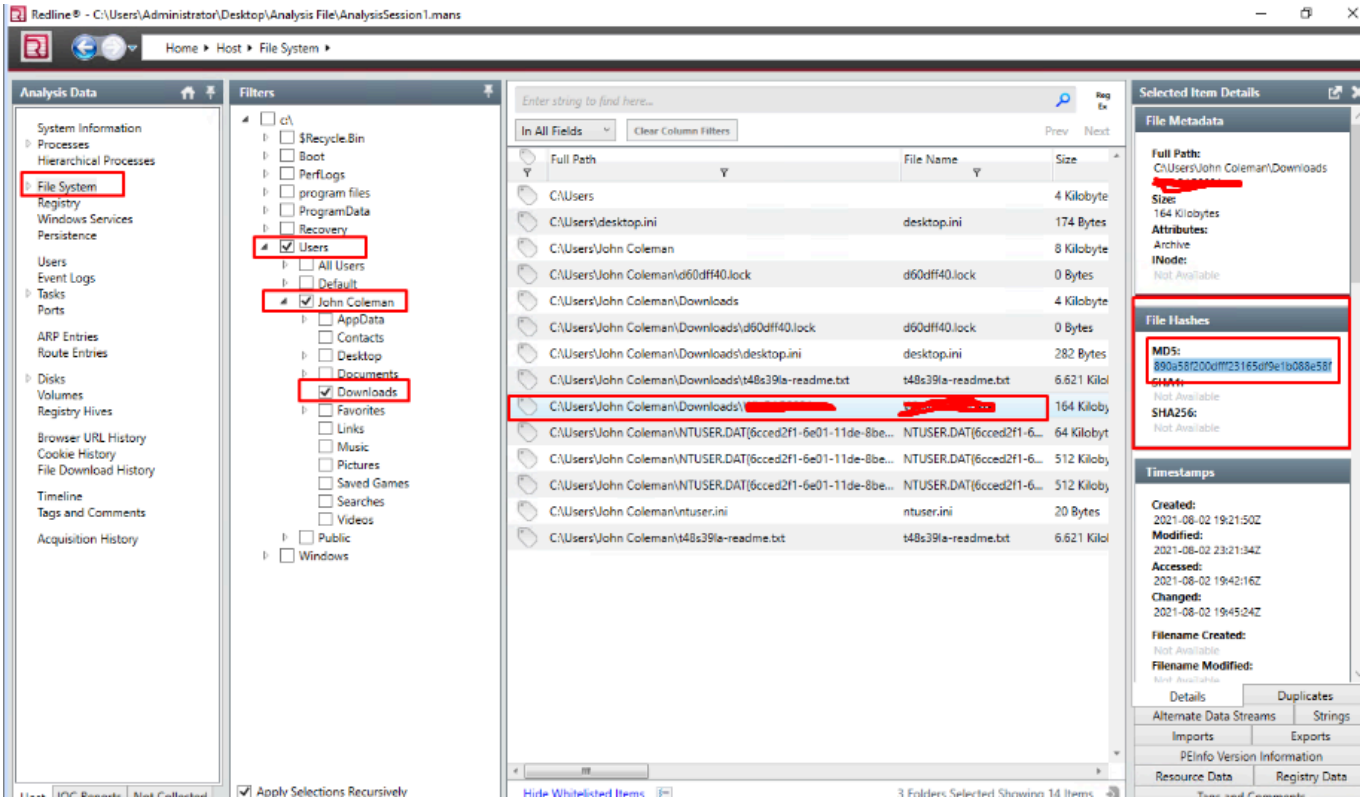
¿Cuál es la URL completa que visitó el usuario para descargar el binario malicioso? (incluya también el binario)

Ya que logramos determinar el archivo también podemos responder cual era la URL completa de la descarga que la encontramos en el mismo menú:



¿Cuál es el hash MD5 del binario?

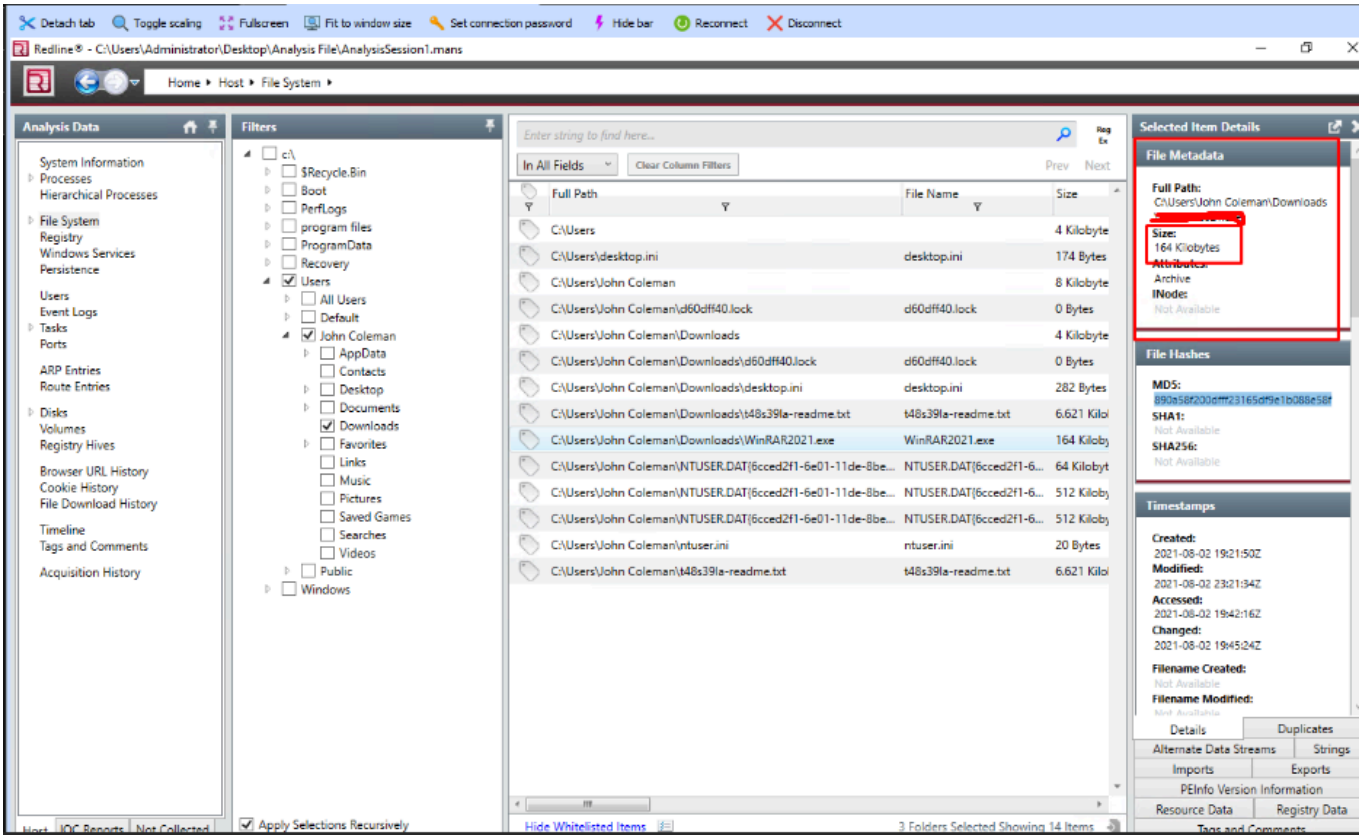
Ahora nos piden validar el MD5 esto o podremos encontrar en el File System en la carpeta de descargas del usuario:



Como apoyo deje a la vista el MD5 del artefacto.

¿Cuál es el tamaño del binario en kilobytes?

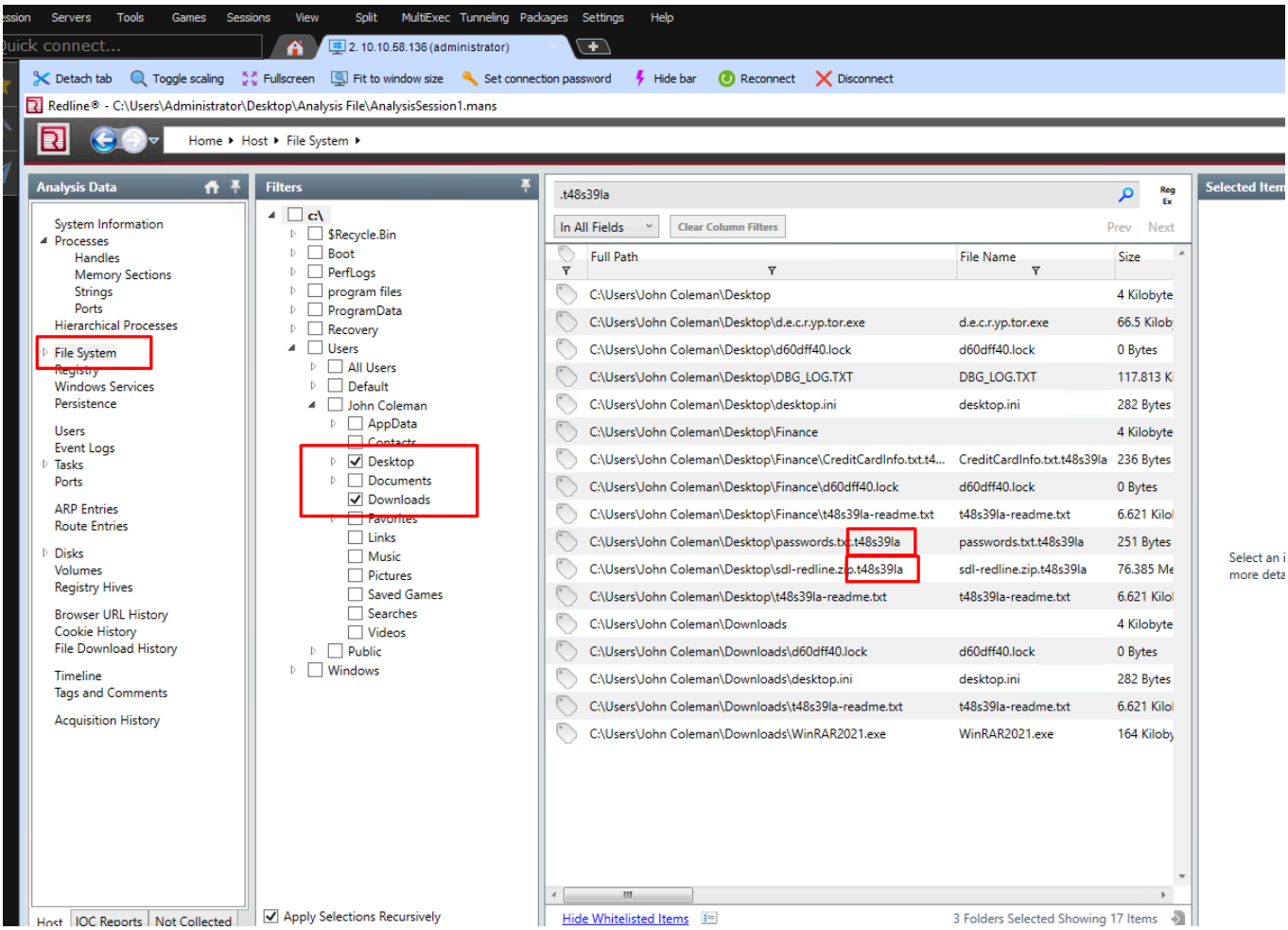
Validando el mismo evento podemos ver que el tamaño se encuentra en el menú de detalles en el File Path:



Ya hemos logrado identifcar hasta este punto cual fue el archivo que se uso para el ataque de manera inicial pero nos indican que este archivo genero una modificacion en las extensiones de los archivos del usuario y que debemos determinar ¿Cuál es la extensión a la que se renombraron los archivos del usuario?

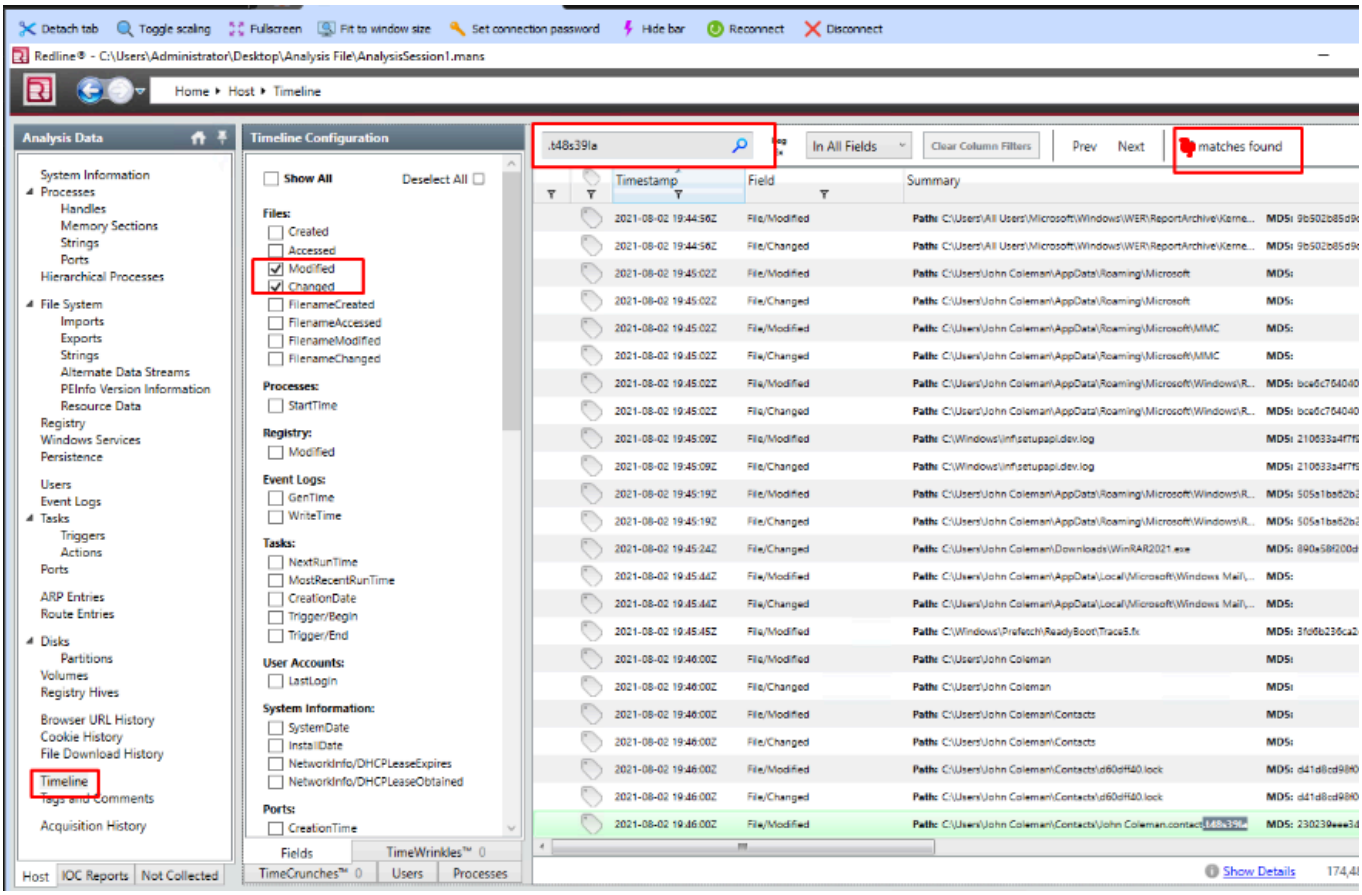
Para ello tenemos que pensar donde podríamos encontrar esta información y lo primero que se me ocurrió fue validar los archivos desde el escritorio y desde las descargas para ver si podía ver algo, por lo que volvi a usar la informacion del File System:

Encontré dos opciones una de ella esta a simple vista que es la .lock pero habían otros archivos que tenían una extensión diferente por lo que validando determine que la extensión era:



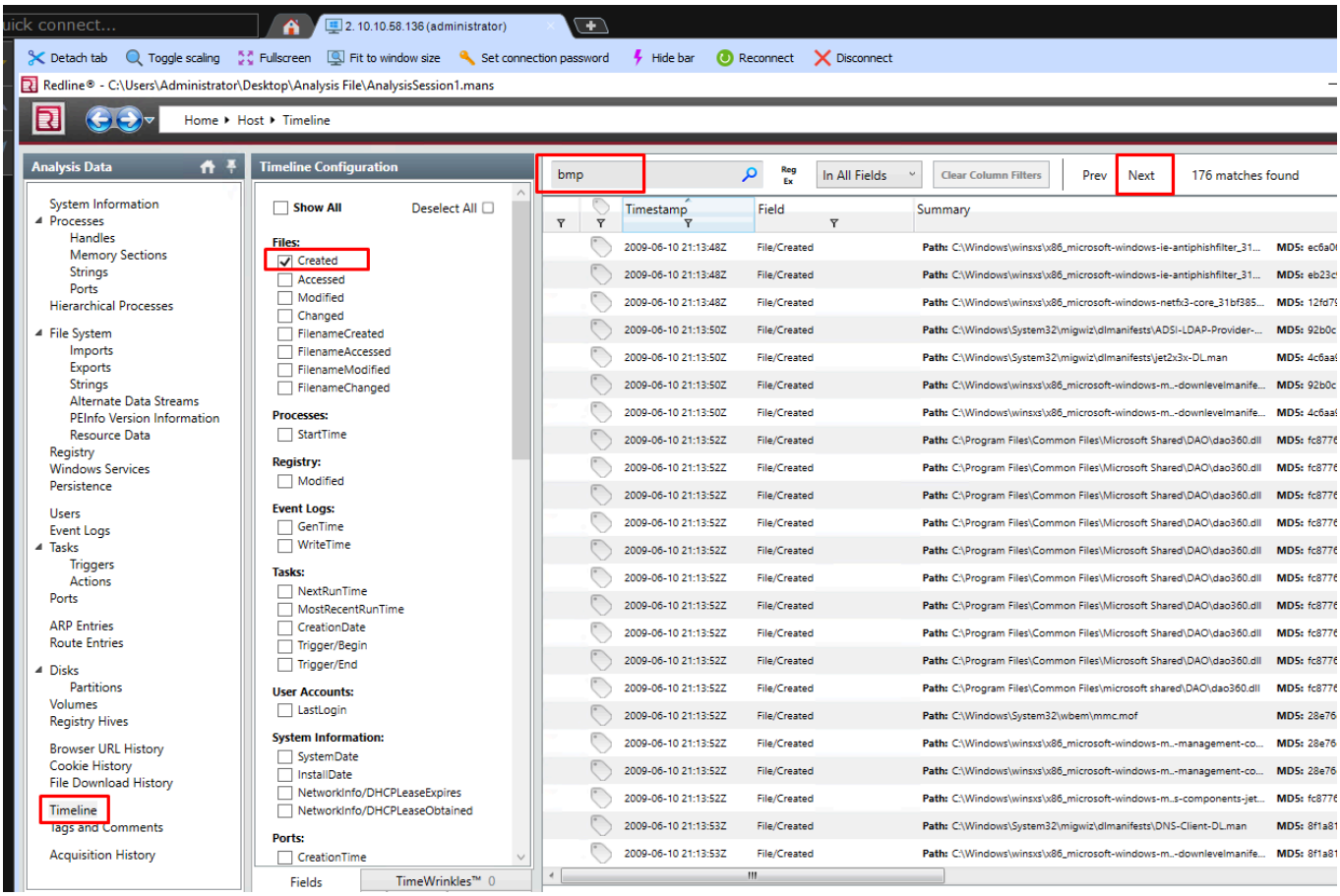
Ya que se logro determinar cual es el tipo de extension ahora nos piden detrminar cuantos archivos fueron renombrados. ¿Cuál es el número de archivos que fueron renombrados y cambiados a esa extensión?

Para esto podemos usar el timeline en este podemos ver a nivel de archivo procesos eventos de log y demás, por lo que usaremos las opciones de file y veremos los que fueron modificados y cambiados, esto nos dará una respuesta de los maches que se encontraron bajo este parámetro:

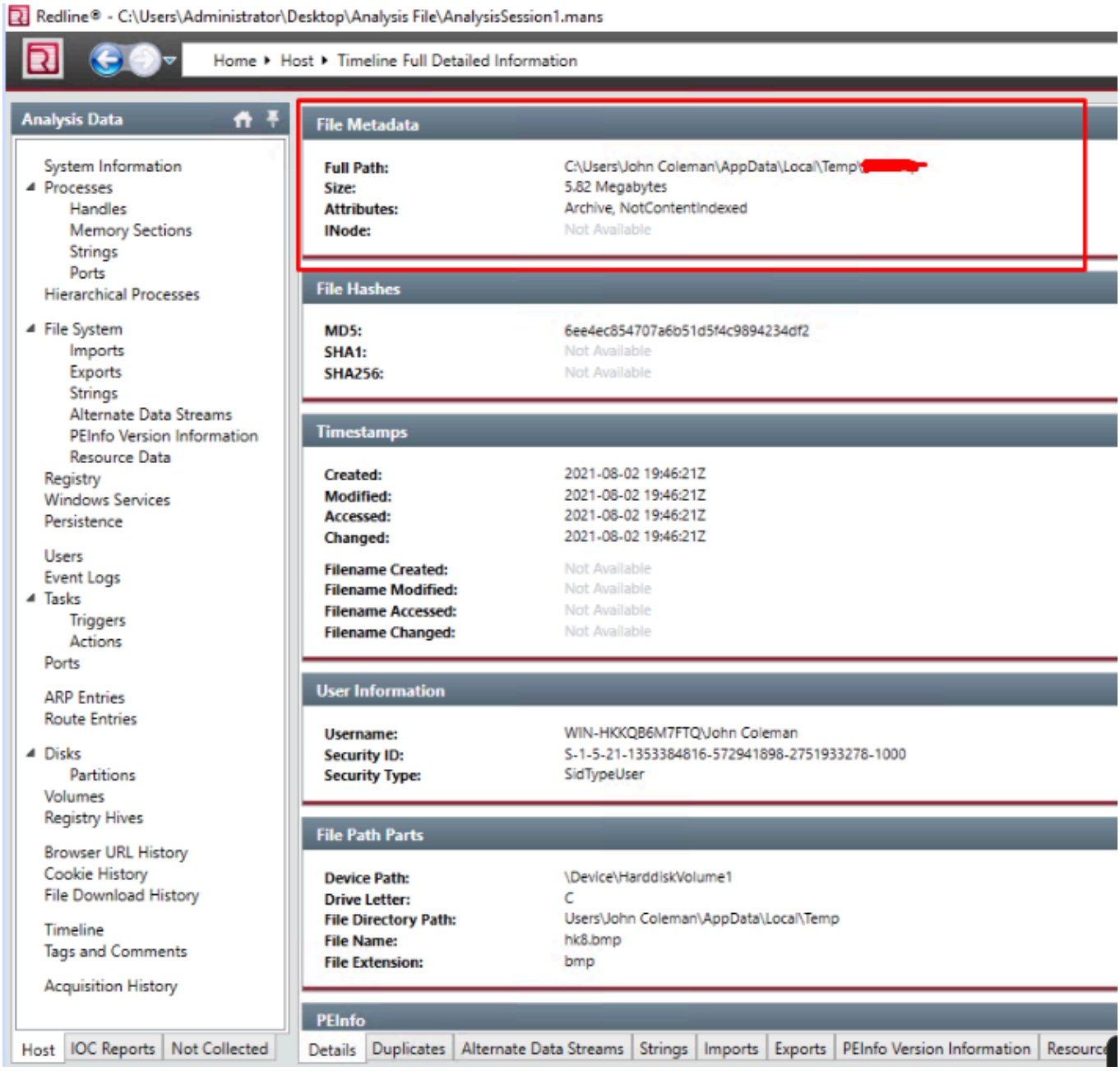


Ya sabemos donde encontrar cambios y modificaciones y creaciones en la maquina por lo que ahora solicitan saber ¿Cuál es la ruta completa al fondo de pantalla que fue cambiado por un atacante, incluido el nombre de la imagen?

Usamos la misma opción pero esta vez vamos a buscar por creación, en esta opción sabemos que se cambia la imagen de fondo de pantalla y que esta es de extensión .BMP por lo que al filtrar nos encontraremos con la siguiente vista:



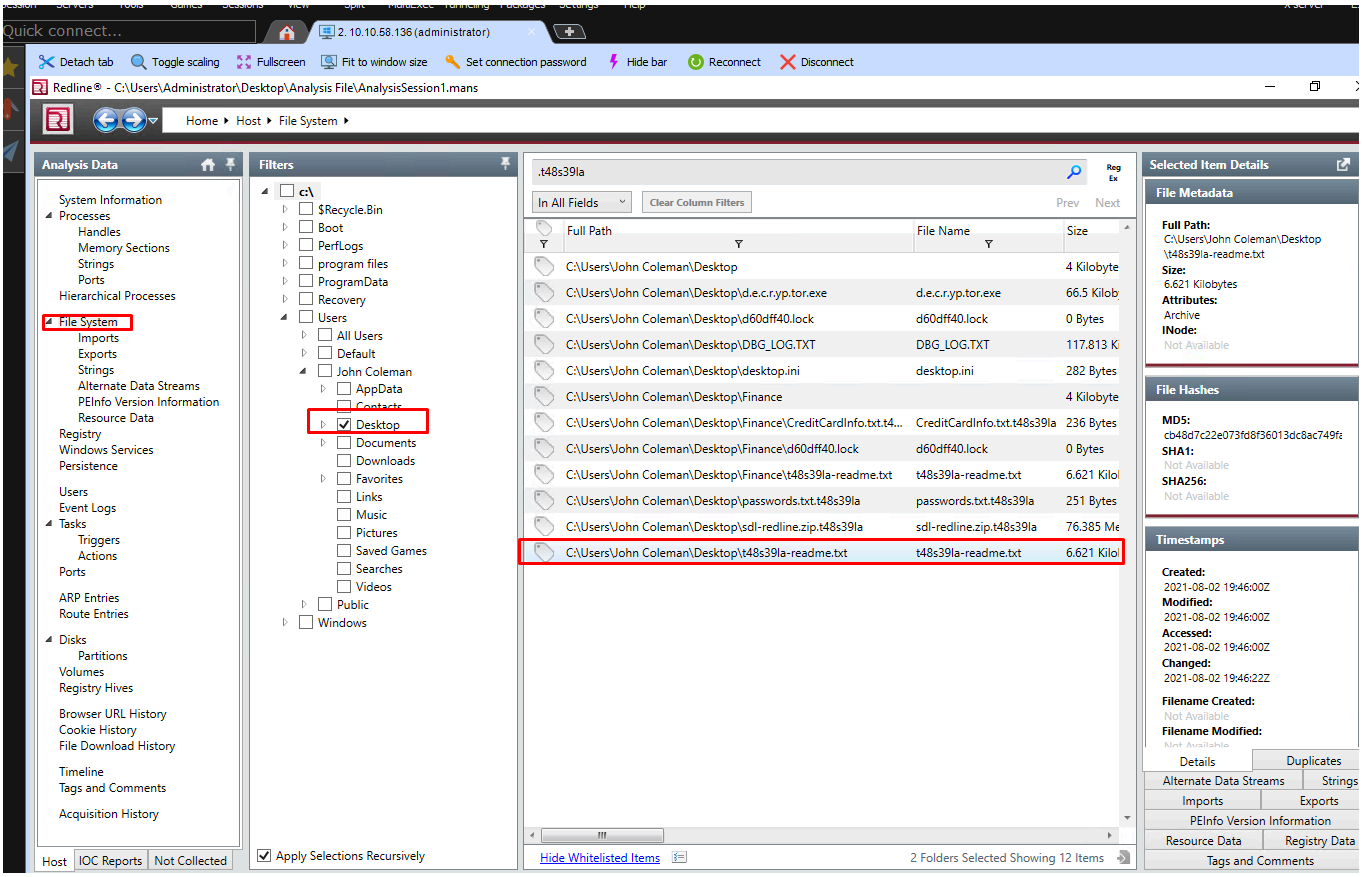
Esta me resulto algo tediosa de encontrar debido a la gran cantidad de archivos intente determinar la búsqueda con la ruta por defecto usando C:\Windows\Resources\Theme y C:\Windows\Web\Wallpaper pero no encontré nada por lo que me di un paseo por las opciones encontradas solo por la extensión y encontré una ruta en el Temp que tenia un nombre extraño:

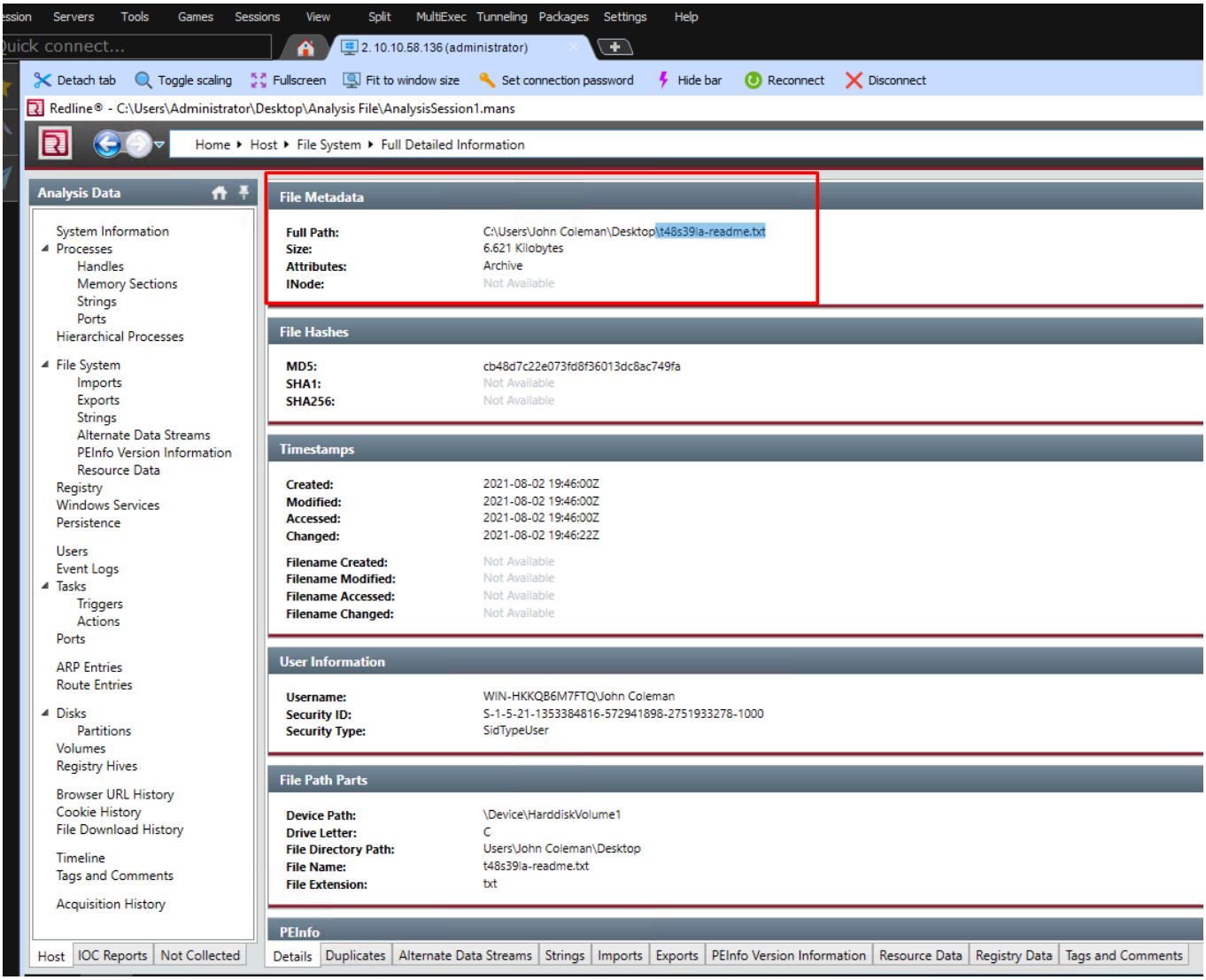


Después me di cuenta que podía haber usado os filtros solo para la fecha en la que se vio el incidente con el find e segmentar mejor los datos esto también ayudaría a encontrar la respuesta.

Ya que tenemos mas información sobre el artefacto nos solicitan validar la nota que dejo el atacante para el usuario en el escritorio; y que proporcionemos el nombre de la nota con la extensión.

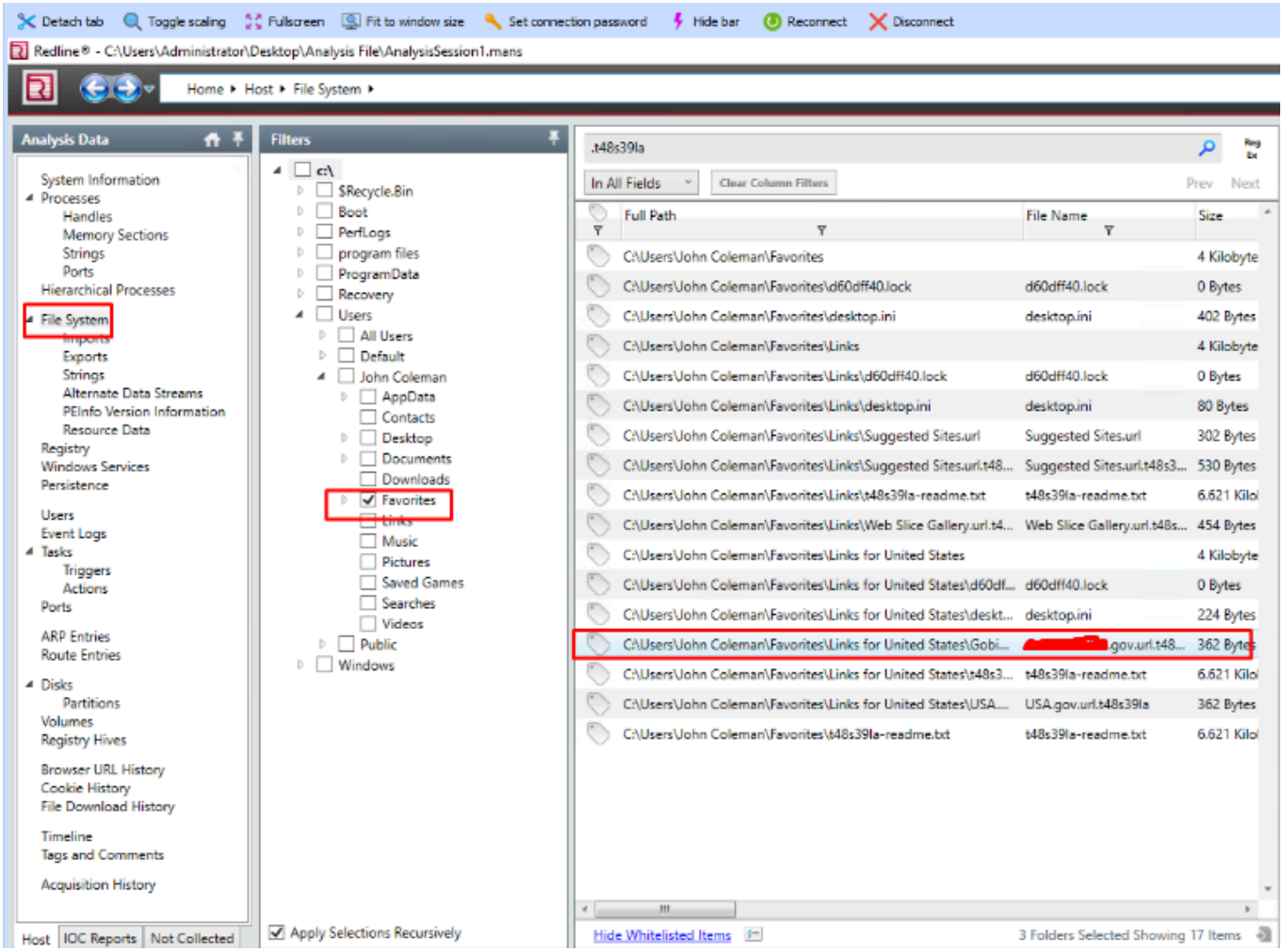
Acá volvemos a tener que buscar la información en el File System en la misma pregunta nos piden validar en el Escritorio asi que vamos a la ruta y vemos que existen 12 elementos de los cuales podemos ver una que se llama:


Quick connect...
2. 10.10.58.136 (administrator)
Detach tab
Toggle scaling
Fullscreen
Fit to window size
Set connection password
Hide bar
Reconnect
Disconnect
Redline® - C:\Users\Administrator\Desktop\Analysis File\AnalysisSession1.mans
Home ▸ Host ▸ File System ▸
Analysis Data
System Information
Processes
Handles
Memory Sections
Strings
Ports
Hierarchical Processes
File System
Imports
Exports
Strings
Alternate Data Streams
PEInfo Version Information
Resource Data
Registry
Windows Services
Persistence
Users
Event Logs
Tasks
Triggers
Actions
Ports
ARP Entries
Route Entries
Disks
Partitions
Volumes
Registry Hives
Browser URL History
Cookie History
File Download History
Timeline
Tags and Comments
Acquisition History
Host
IOC Reports
Not Collected
Filters
c:\
$Recycle.Bin
Boot
PerfLogs
program files
ProgramData
Recovery
Users
All Users
Default
John Coleman
AppData
Contacts
Desktop
Documents
Downloads
Favorites
Links
Music
Pictures
Saved Games
Searches
Videos
Public
Windows
Apply Selections Recursively
.t48s39la
Reg Ex
In All Fields
Clear Column Filters
Prev
Next
Full Path
File Name
Size
C:\Users\John Coleman\Desktop
4 Kilobyte
C:\Users\John Coleman\Desktop\d.e.c.r.yp.tor.exe
d.e.c.r.yp.tor.exe
66.5 Kilob
C:\Users\John Coleman\Desktop\d60dff40.lock
d60dff40.lock
0 Bytes
C:\Users\John Coleman\Desktop\DBG_LOG.TXT
DBG_LOG.TXT
117.813 K
C:\Users\John Coleman\Desktop\desktop.ini
desktop.ini
282 Bytes
C:\Users\John Coleman\Desktop\Finance
4 Kilobyte
C:\Users\John Coleman\Desktop\Finance\CreditCardInfo.txt.t4...
CreditCardInfo.txt.t48s39la
236 Bytes
C:\Users\John Coleman\Desktop\Finance\d60dff40.lock
d60dff40.lock
0 Bytes
C:\Users\John Coleman\Desktop\Finance\t48s39la-readme.txt
t48s39la-readme.txt
6.621 Kilo
C:\Users\John Coleman\Desktop\passwords.txt.t48s39la
passwords.txt.t48s39la
251 Bytes
C:\Users\John Coleman\Desktop\sdl-redline.zip.t48s39la
sdl-redline.zip.t48s39la
76.385 Me
C:\Users\John Coleman\Desktop\t48s39la-readme.txt
t48s39la-readme.txt
6.621 Kilo
Hide Whitelisted Items
2 Folders Selected Showing 12 Items
Selected Item Details
File Metadata
Full Path:
C:\Users\John Coleman\Desktop\t48s39la-readme.txt
Size:
6.621 Kilobytes
Attributes:
Archive
INode:
Not Available
File Hashes
MD5:
cb48d7c22e073fd8f36013dc8ac749fa
SHA1:
Not Available
SHA256:
Not Available
Timestamps
Created:
2021-08-02 19:46:00Z
Modified:
2021-08-02 19:46:00Z
Accessed:
2021-08-02 19:46:00Z
Changed:
2021-08-02 19:46:22Z
Filename Created:
Not Available
Filename Modified:
Details
Duplicates
Alternate Data Streams
Strings
Imports
Exports
PEInfo Version Information
Resource Data
Registry Data
Tags and Comments

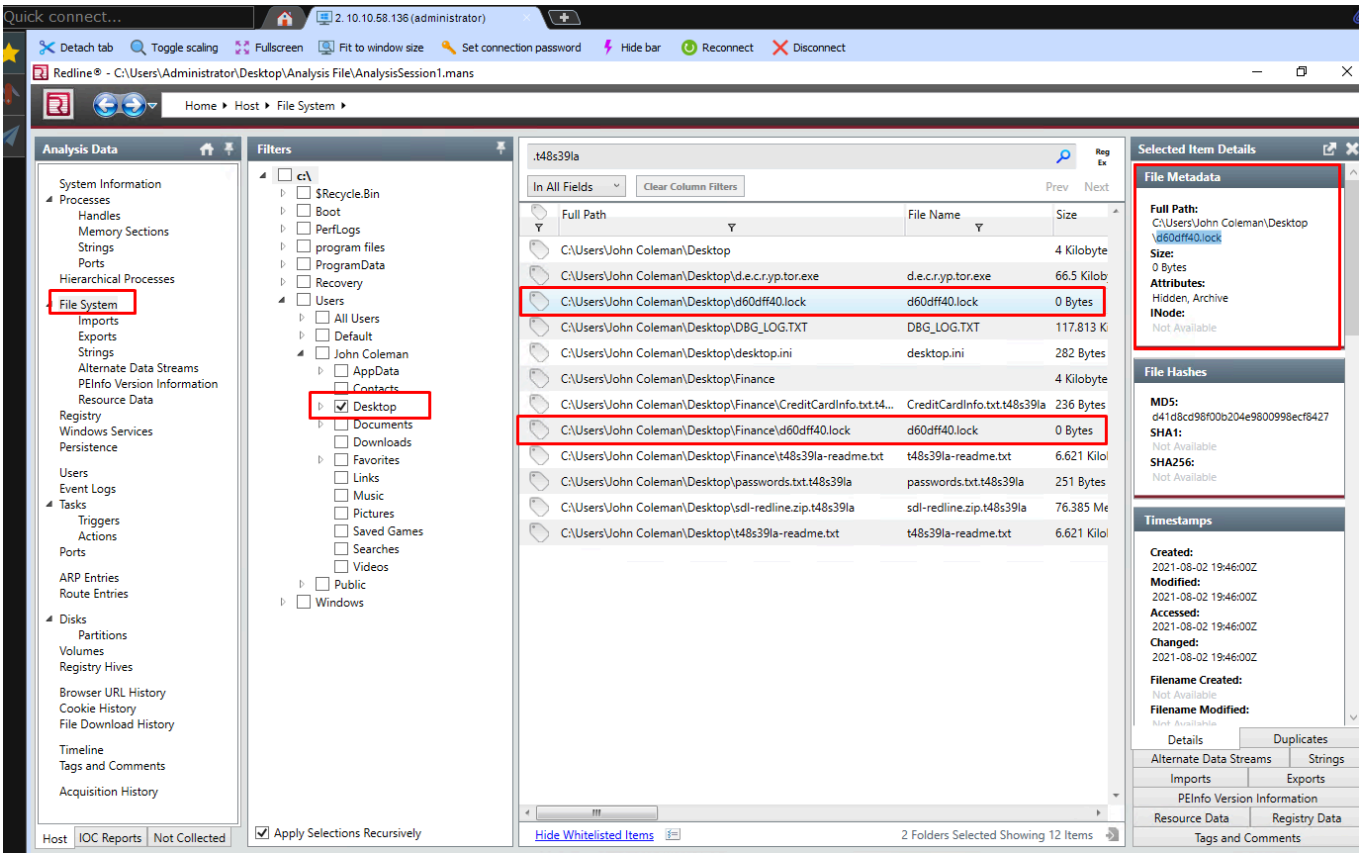


También nos indican que el atacante creó una carpeta llamada "Enlaces para Estados Unidos" en C:\Users\John Coleman\Favorites\ y dejó un archivo allí. Y que debemos proporcionar el nombre del archivo.

Usando la misma dinámica buscamos en la ruta de favoritos y en esta encontramos varios archivos, como pista nos indican que la respuesta esta asociada a un archivo que en el nombre contiene palabras en español:

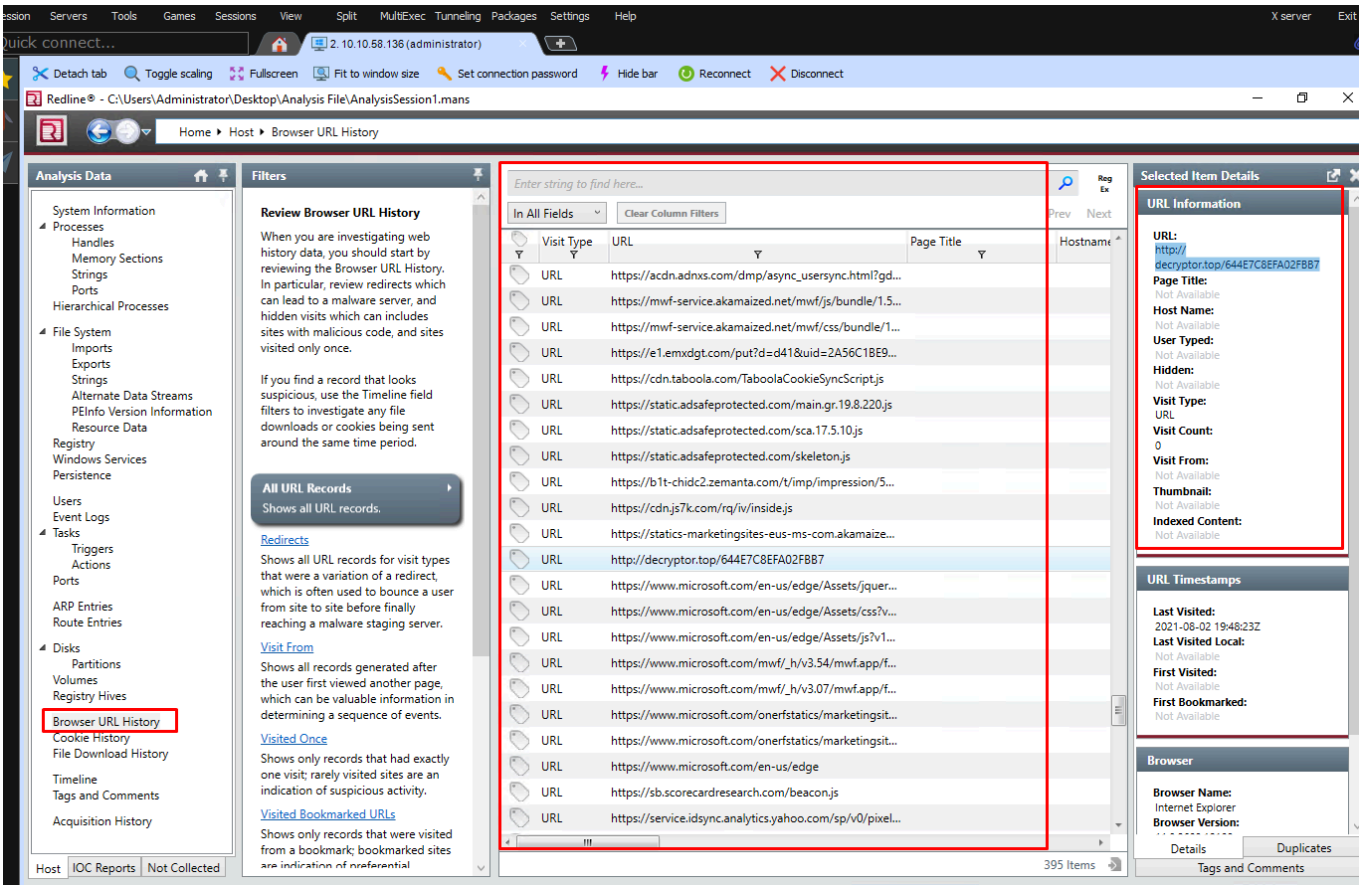


También nos piden buscar un archivo oculto que se creó en el escritorio del usuario y que tiene 0 bytes. proporcionando el nombre del archivo oculto.

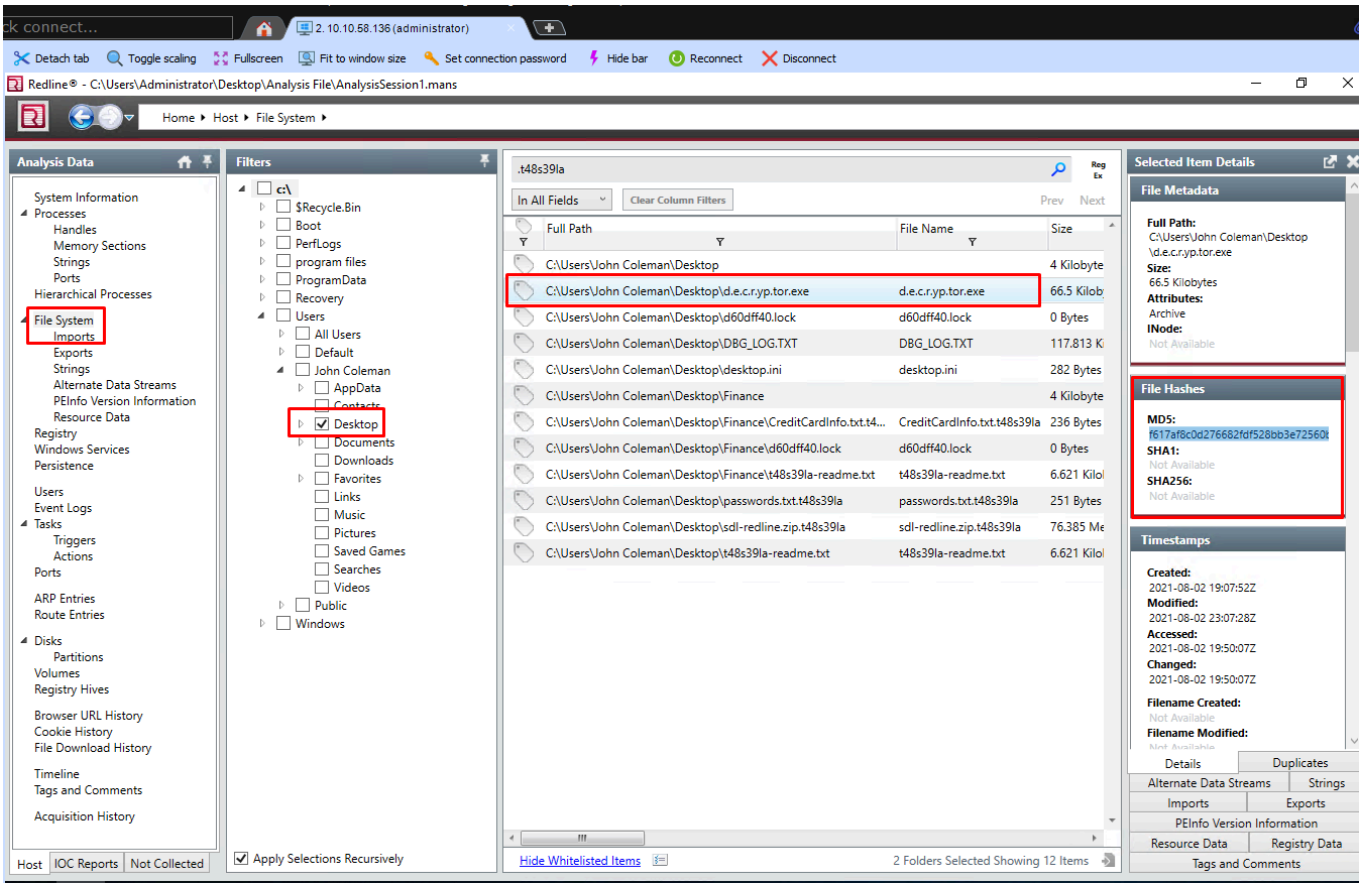


Después de haber analizado esta información nos indican que el usuario descargó un descifrador con la esperanza de descifrar todos los archivos, pero no lo logró. Que proporcionemos el hash MD5 del archivo descifrador.

Ya que sabemos que lo que buscaos es un desencriptador buscamos en los archivos analice en el Historial web debido lo que se indicaba en la pregunta y se puede ver que el usuario busco información asociada a los eventos ingreso a descargar el navegador de tor y también encontré el evento asociado a el desencriptador:

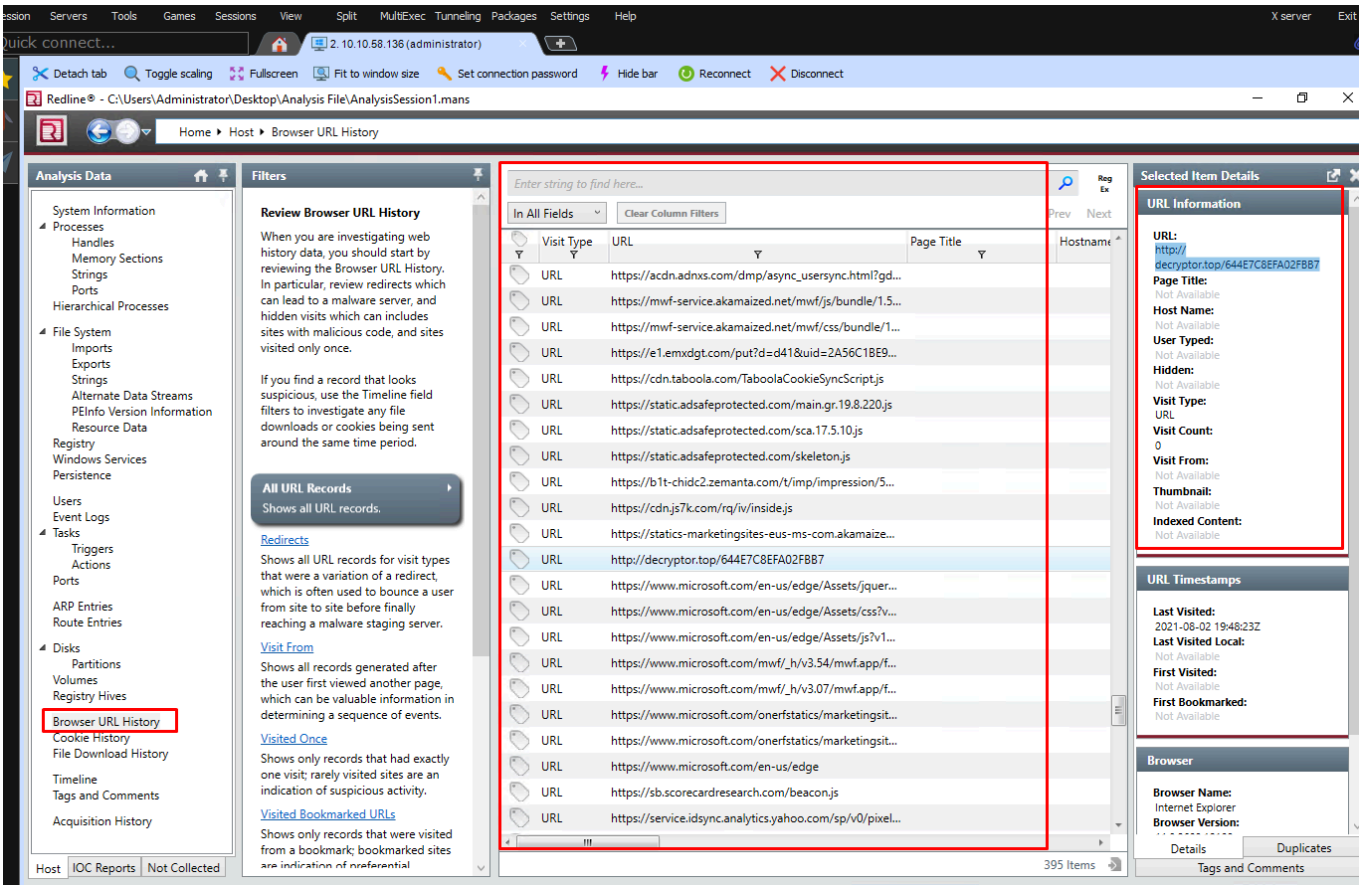


Con esto asumí que se vería el archivo en las descargas pero no lo encontré por lo que valide las demás rutas que ya había validado y en el escritorio logre encontrar un archivo con el nombre de:



También nos solicitaron encontrar la ruta completa de la URL que proporciono el atacante en la nota del ransomware, desde la que se puede acceder a través del navegador normal para descifrar uno de los archivos cifrados de forma gratuita. El usuario intentó acceder a ella. Proporcione la ruta URL completa.

Debido a lo que había realizado en la pregunta anterior ya contaba con esta URL solo valide los detalles para sacar a ruta completa:

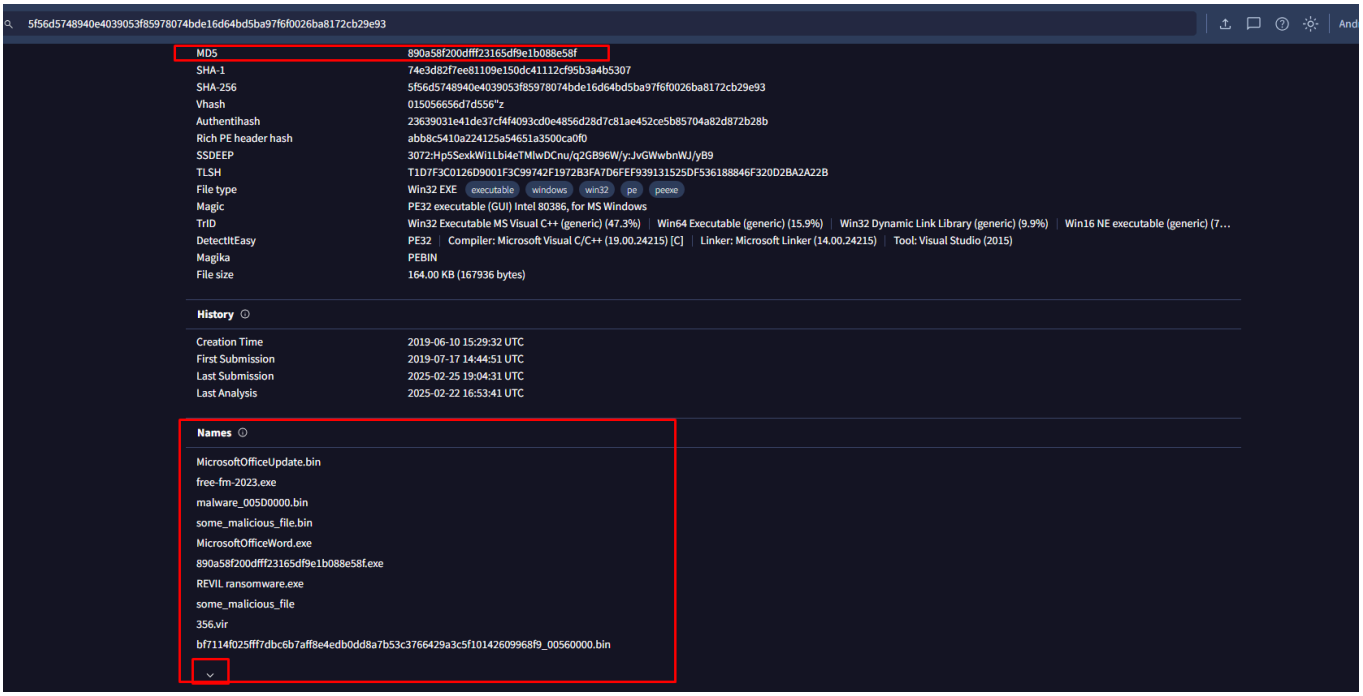


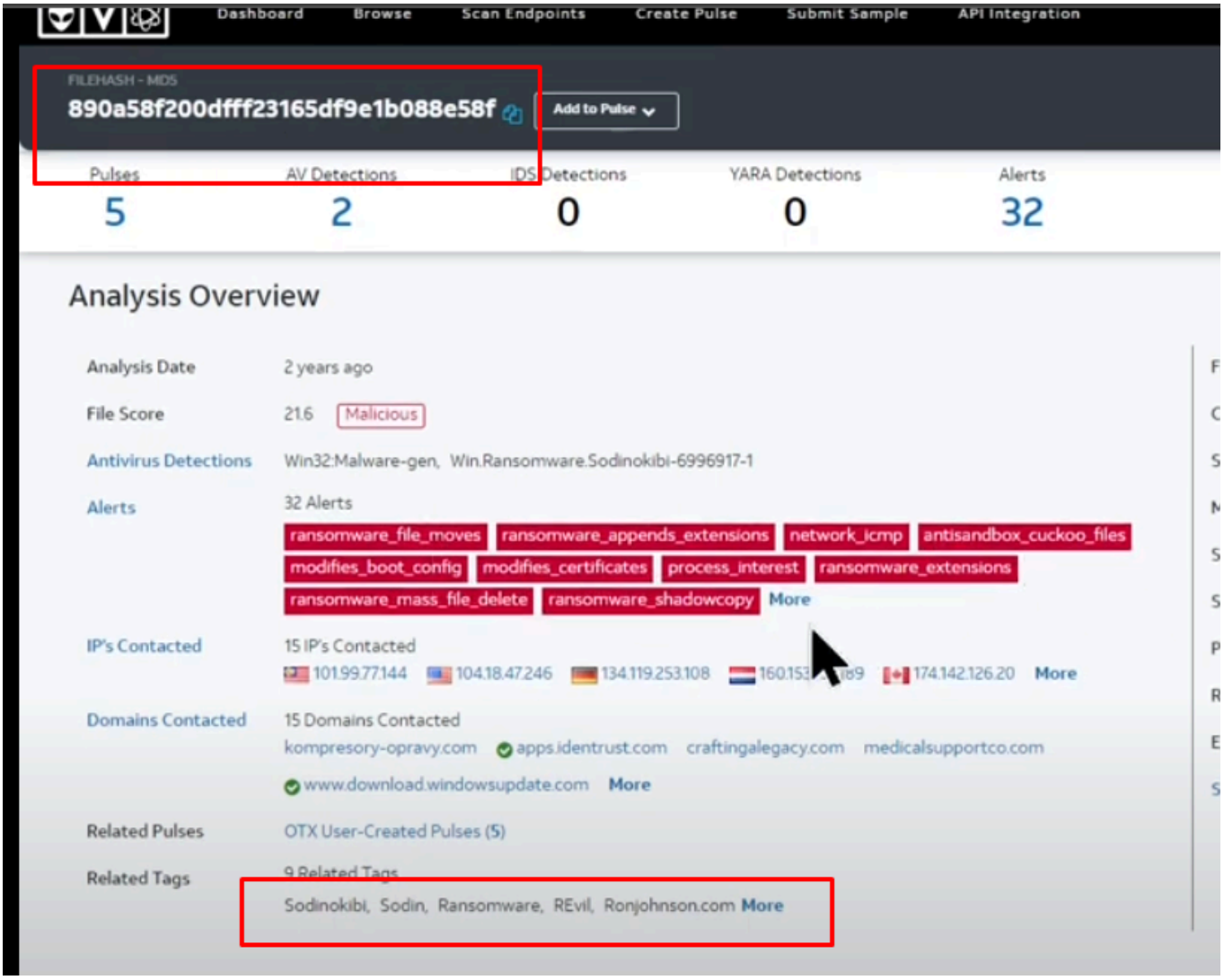
Con toda esta información ya podemos encontrar información asociada a el evento y al artefacto mediante fuentes de inteligencia por lo que podemos usar los siguientes links para ver mas información del evento:

- https://www.virustotal.com/gui/file/5f56d5748940e4039053f85978074bde16d64bd5ba97f6f0026ba8172cb29e93/detection
- https://tria.ge/240203-xwllrsafcn
- https://www.hybrid-analysis.com/sample/5f56d5748940e4039053f85978074bde16d64bd5ba97f6f0026ba8172cb29e93
- https://malshare.com/sample.php?action=detail&hash=5f56d5748940e4039053f85978074bde16d64bd5ba97f6f0026ba8172cb29e93
- https://otx.alienvault.com/indicator/file/5f56d5748940e4039053f85978074bde16d64bd5ba97f6f0026ba8172cb29e93

Apoyándose en estos links se puede realizar la ultima pregunta en la que se pueden encontrar mas datos del Ransomware com o ¿Cuáles son los tres nombres

asociados con el malware que infectó este host? (ingrese los nombres en orden alfabético)





Gracias..!