

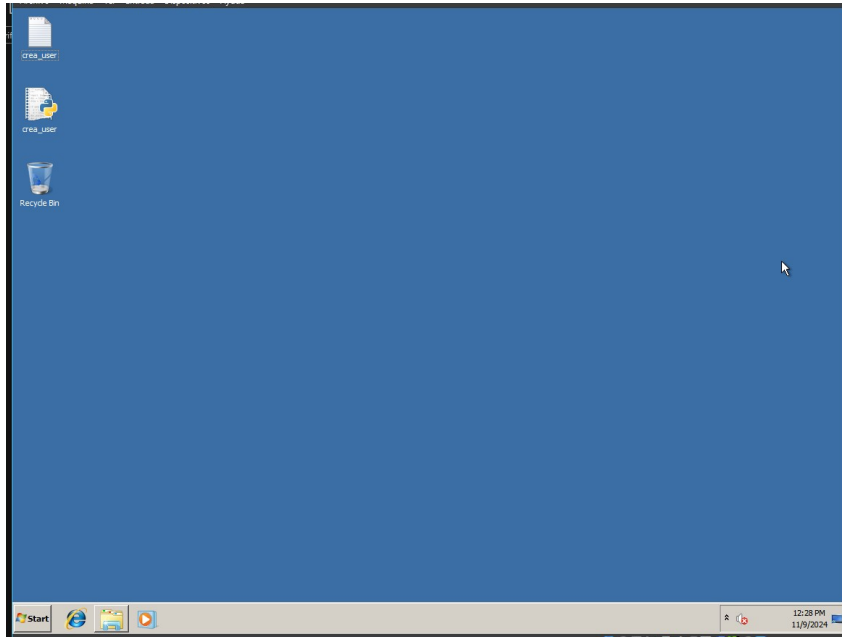
Informe técnico de adquisición de datos

Nicolás Ruiz Ruiz

Asunto: Como miembro del CSIRT de mi empresa, he sido llamado para la investigación de un incidente ocurrido en una ordenador.

09-11-24

Empiezo el análisis a las 12:28, el estado inicial de la máquina es encendido y se ve así:



(En este punto, deberíamos hacer más fotos de la escena, ordenador/torre, monitor, periféricos, etc. sin embargo al hacerlo en mi ordenador personal, prefiero mantener mi privacidad)

Una vez visto el estado inicial de la máquina, debemos acordonar la zona y bloquear la entrada, dejando solo pasar al personal autorizado: resto del equipo CSIRT, supervisores, jefes, etc.

En este caso, no es necesario el uso de equipo anti-contaminación, ya que la adquisición la voy a realizar en el puesto del propio trabajador, lo que si sería necesario es el uso de bolsas anti estáticas para el transporte final de los discos duros donde guardemos la adquisición.

La máquina consta de un Windows Vista, un monitor PHILIPS periféricos como cascos, ratón y teclado, y una torre con un adaptador conectado a la red de la empresa. No tiene dispositivos de almacenamiento conectados ni en los alrededores.

Informe técnico de adquisición de datos

Nicolás Ruiz Ruiz

Continuo con la adquisición de datos a las 13:30 y lo haré según el orden de volatilidad descrito en nuestra metodología, además, haré uso de diversas herramientas que nombraré cuando las utilice.

(La forma correcta de hacer la adquisición es usando un Pen drive donde estén nuestras herramientas, sin embargo, al poner el Pen drive en la máquina, no me lo detecta, así que lo estoy haciendo mediante carpetas compartidas por red[no desde la aplicación de VirtualBox], y arrastrando las herramientas al escritorio. Igualmente, para no romper el ambiente, lo llamaré Pen drive)

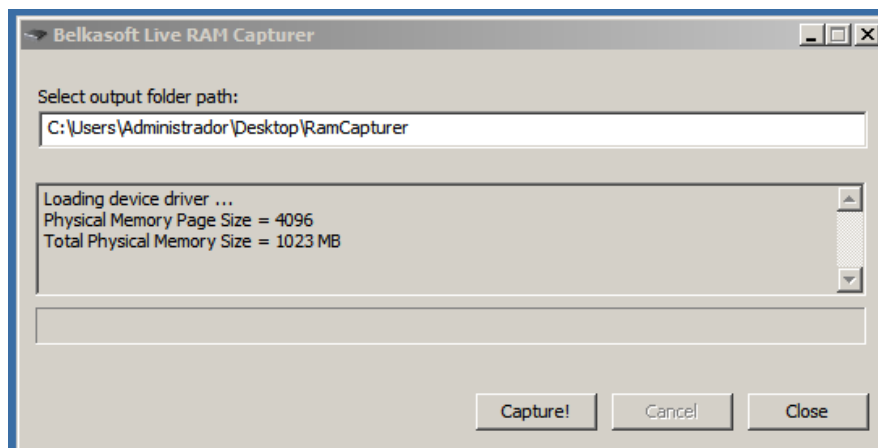
1. Contenido de la memoria RAM.

Hora de Inicio: 13:35

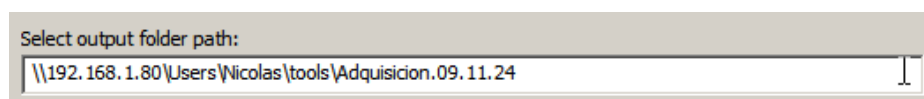
Programa utilizado: RamCapture

Modo de adquisición:

Ejecutamos la aplicación desde el Pen, en este caso, elegimos la versión de 64 bits y nos aparecerá la siguiente ventana:



Podemos ver la memoria total del ordenador(4Gb), la memoria usada(1Gb) y la ruta donde vamos a guardar el archivo resultado. Este último lo vamos a cambiar y lo vamos a guardar en nuestro Pen drive:



Una vez capturada la memoria RAM, calculamos su HASH y lo registramos:

Nombre del archivo	Fecha de adquisición	Hash
20241109.mem	09-11-24 13:57	875E36D7D85A30B6311425A2A14632FD
		35A0781E0FCFDA06132A8A5197E0D454750A62F7

Informe técnico de adquisición de datos

Nicolás Ruiz Ruiz

2. Tablas de enrutamiento y caché ARP.

Hora de inicio: 14:06

Programa utilizado: Comando “route print” y “arp -a”

Modo de adquisición:

Para capturar la tabla de enrutamiento y y caché ARP, debemos hacer uso de la consola de comandos y poner los siguientes comandos:

```
C:\Users\Administrador>route print > \\192.168.1.80\Users\Nicolas\tools\Adquisicion.09.11.24\enrutamiento.txt  
C:\Users\Administrador>arp -a > \\192.168.1.80\Users\Nicolas\tools\Adquisicion.09.11.24\arp.txt
```

1º route print > \ruta\del\pen\enrutamiento.txt

2º arp -a > \ruta\del\pen\arp.txt

Nombre del archivo	Fecha de adquisición	Hash
enrutamiento.txt	09-11-24 14:14	C721C3C0847F8CF902DD453899AC4CFE
		1D294D48930AEADDD8BD5D8F1E58A3FC6D737DE6
arp.txt	09-11-24 14:14	F15B89D5E0990F36C1BDA18CCF4BB740
		C3B60EDB9C4309E986E5CA7C93E442F51C7966DD

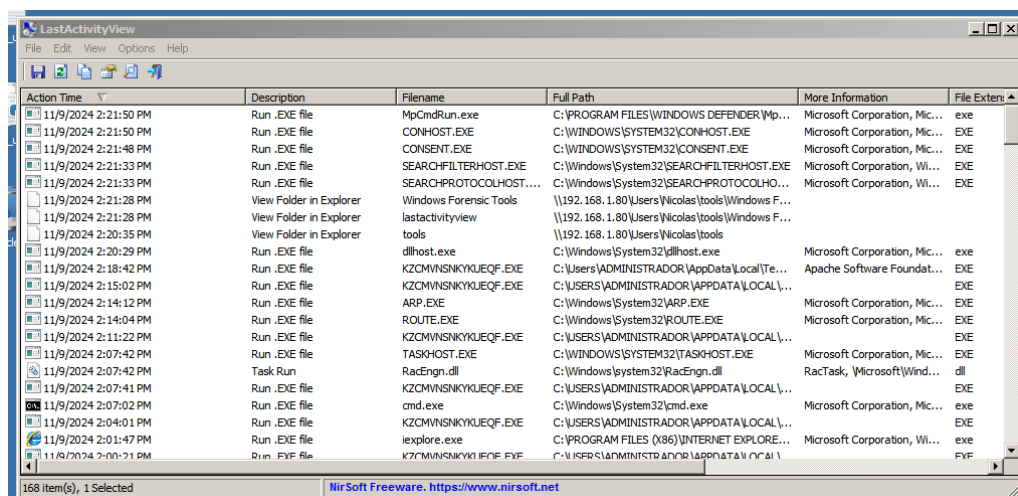
3. Tabla de procesos en ejecución.

Hora de inicio: 14:19

Programa utilizado: LastActivityView

Modo de adquisición:

Ejecutamos el programa desde el Pen drive y nos aparecerá la siguiente ventana:



Action Time	Description	Filename	Full Path	More Information	File Extens
11/9/2024 2:21:50 PM	Run .EXE file	MpCmdRun.exe	C:\PROGRAM FILES\WINDOWS DEFENDER\Mp...	Microsoft Corporation, Mic...	exe
11/9/2024 2:21:50 PM	Run .EXE file	CONHOST.EXE	C:\WINDOWS\SYSTEM32\CONHOST.EXE	Microsoft Corporation, Mic...	EXE
11/9/2024 2:21:48 PM	Run .EXE file	CONSENT.EXE	C:\WINDOWS\SYSTEM32\CONSENT.EXE	Microsoft Corporation, Mic...	EXE
11/9/2024 2:21:33 PM	Run .EXE file	SEARCHFILTERHOST.EXE	C:\WINDOWS\System32\SEARCHFILTERHOST.EXE	Microsoft Corporation, Wi...	EXE
11/9/2024 2:21:33 PM	Run .EXE file	SEARCHPROTOCOLHOST....	C:\WINDOWS\System32\SEARCHPROTOCOLHO...	Microsoft Corporation, Wi...	EXE
11/9/2024 2:21:28 PM	View Folder in Explorer	Windows Forensic Tools	\\192.168.1.80\Users\Nicolas\tools\Windows F...		
11/9/2024 2:21:28 PM	View Folder in Explorer	lastactivityview	\\192.168.1.80\Users\Nicolas\tools\Windows F...		
11/9/2024 2:20:35 PM	View Folder in Explorer	tools	\\192.168.1.80\Users\Nicolas\tools		
11/9/2024 2:20:29 PM	Run .EXE file	dllhost.exe	C:\WINDOWS\System32\dllhost.exe	Microsoft Corporation, Mic...	exe
11/9/2024 2:18:42 PM	Run .EXE file	KZCMVNSNKYUEQF.EXE	C:\Users\ADMINISTRADOR\AppData\Local\Te...	Apache Software Foundat...	EXE
11/9/2024 2:15:02 PM	Run .EXE file	KZCMVNSNKYUEQF.EXE	C:\Users\ADMINISTRADOR\AppData\Local\Te...		EXE
11/9/2024 2:14:12 PM	Run .EXE file	ARP.EXE	C:\WINDOWS\System32\ARP.EXE	Microsoft Corporation, Mic...	EXE
11/9/2024 2:14:04 PM	Run .EXE file	ROUTE.EXE	C:\WINDOWS\System32\ROUTE.EXE	Microsoft Corporation, Mic...	EXE
11/9/2024 2:11:22 PM	Run .EXE file	KZCMVNSNKYUEQF.EXE	C:\Users\ADMINISTRADOR\AppData\Local\Te...		EXE
11/9/2024 2:10:42 PM	Run .EXE file	TASKHOST.EXE	C:\WINDOWS\SYSTEM32\TASKHOST.EXE	Microsoft Corporation, Mic...	EXE
11/9/2024 2:07:42 PM	Task Run	RacEngn.dll	C:\WINDOWS\system32\RacEngn.dll	RacTask, \Microsoft\Wind...	dll
11/9/2024 2:07:41 PM	Run .EXE file	KZCMVNSNKYUEQF.EXE	C:\Users\ADMINISTRADOR\AppData\Local\Te...		EXE
11/9/2024 2:07:02 PM	Run .EXE file	cmd.exe	C:\WINDOWS\System32\cmd.exe	Microsoft Corporation, Mic...	exe
11/9/2024 2:04:01 PM	Run .EXE file	KZCMVNSNKYUEQF.EXE	C:\Users\ADMINISTRADOR\AppData\Local\Te...		EXE
11/9/2024 2:01:47 PM	Run .EXE file	ieexplore.exe	C:\PROGRAM FILES (x86)\INTERNET EXPLOR...	Microsoft Corporation, Wi...	exe
11/9/2024 2:00:21 PM	Run .EXE file	KZCMVNSNKYUEQF.EXE	C:\Users\ADMINISTRADOR\AppData\Local\Te...		EXE

Aquí podemos ver los últimos procesos ejecutados en el sistema. Para hacer un reporte de este resultado, le damos a “View” y a “HTML REPORT – ALL ITEMS”

Informe técnico de adquisición de datos

Nicolás Ruiz Ruiz

Nombre del archivo	Fecha de adquisición	Hash
report.html	09-11-24 14:28	002EE4D380E9BE711B012FE955612D74
		47C20CEDA2960712E3640D30668B80F76AB97E1C

4. Archivos temporales del sistema.

Hora de inicio: 15:00

Programa utilizado: FTK Imager

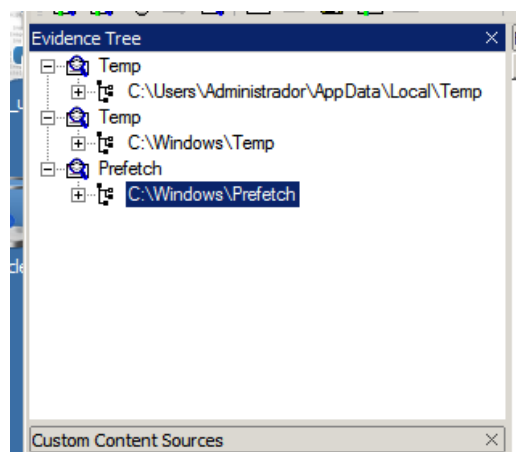
Modo de adquisición:

Para la adquisición de archivos temporales, abriremos FTK Imager y añadiremos las 3 siguientes carpetas:

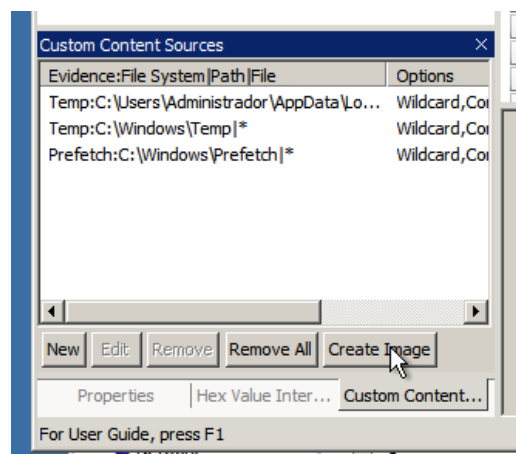
C:\Users\Administrador\AppData\Local\Temp

C:\Windows\Temp

C:\Windows\Prefetch



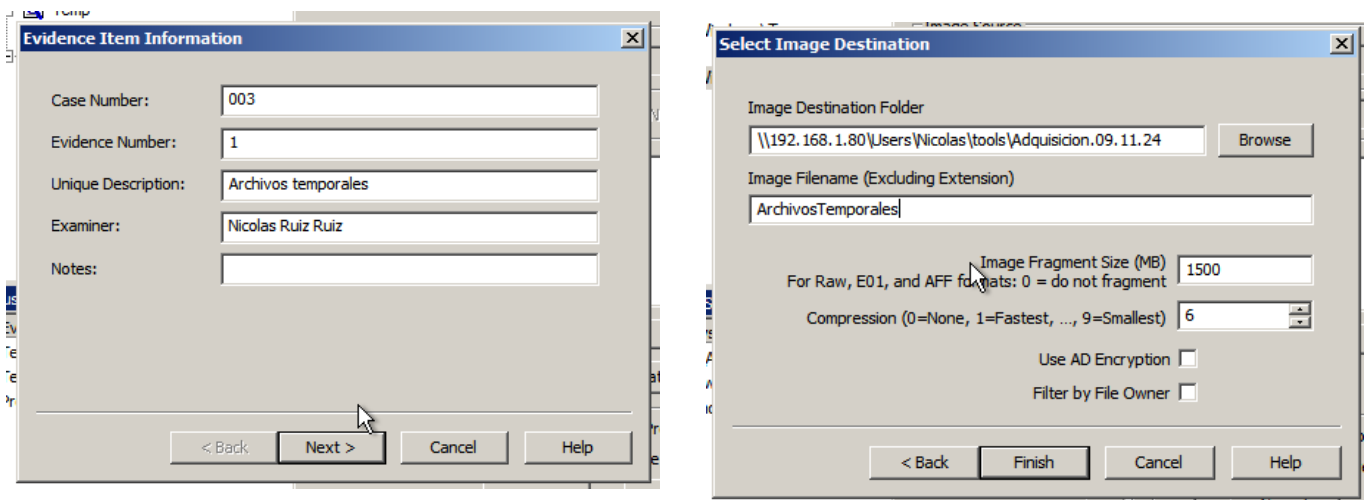
Le damos clic derecho a las rutas(no a los nombre) y las añadimos al contenido de imagen personalizada:



Informe técnico de adquisición de datos

Nicolás Ruiz Ruiz

Una vez ahí, le damos a crear imagen y la guardamos en el Pen drive.



Le damos a Finish y terminamos con la adquisición de archivos temporales.

Nombre del archivo	Fecha de adquisición	Hash
ArchivosTemporales.ad1	09-11-24 15:30	43E2E703EC3E049BA7763973AE5870A7
		4C4DCE33486243694B7577C0F933DAC75C873265

Informe técnico de adquisición de datos

Nicolás Ruiz Ruiz

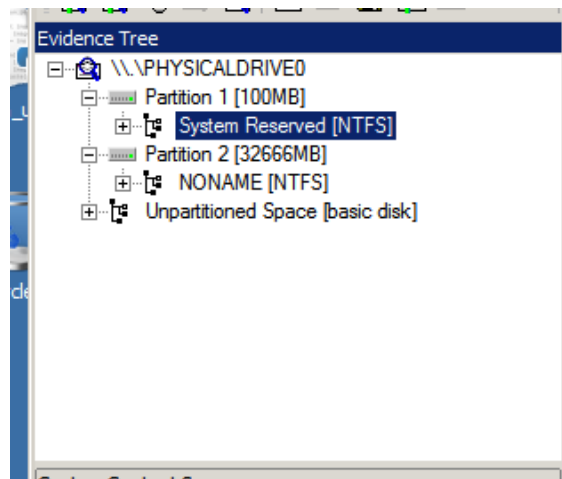
5. Contenido del disco duro.

Hora de inicio: 15:36

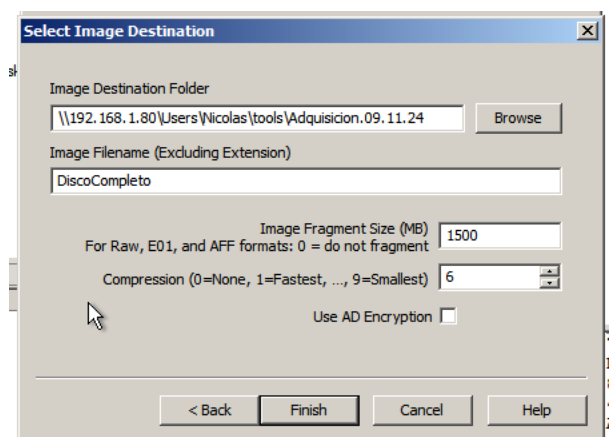
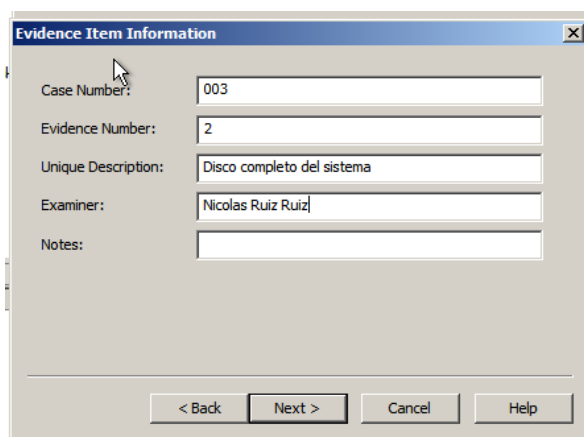
Programa utilizado: FTK Imager

Modo de adquisición:

Para la adquisición del disco, voy a utilizar el mismo programa que antes. Ejecutamos el programa, le doy a unidad física y añado el disco:



Hacemos clic derecho en el nombre del disco(no en las particiones) y le damos a exportar imagen del disco. Elegimos la extensión E01, ya que es la más compatible, en el resto de opciones pondré lo siguiente:



Informe técnico de adquisición de datos

Nicolás Ruiz Ruiz

Una vez terminado, registramos la hora y el hash:

Nombre del archivo	Fecha de adquisición	Hash
DiscoCompleto.E01	09-11-24 16:17	8483EDF792247BBD235F527C6D7714FF
		AACD22E4A14AFD67CA0CE07B69F8F4501C004844
DiscoCompleto.E02	09-11-24 16:17	5CC1FC4955102FA552CEBDE380A7B720
		1D9C665F7BB1BDB075FA5840167CCAD9488DAB43
DiscoCompleto.E03	09-11-24 16:17	895680D27627E985AF0261CF12868605
		E9270057913F6EEA8D9EDFDB314D0481557EDCF3
DiscoCompleto.E04	09-11-24 16:17	1D7CF3BA9A347A7AD728D8F14222451B
		FACDD70BA7E314BF21C7CC75CEBA794CA8B30F1B

6. Medios de almacenamiento externo.

Por último tenemos los dispositivos de almacenamiento externos que, en este caso, no vemos ninguno en la escena.

Una vez acabado el proceso de adquisición de datos, vamos a hacer apta de la cadena de custodia:

Fecha y hora	Persona que entrega	Persona que recibe	Descripción del dispositivo	Hash (MD5/SHA1)	Firma del Entregador	Firma del receptor
09-11-24	Nicolás Ruiz Ruiz	Manuel Jesús Rivas Sánchez	Pen drive USB 64 GB, marca Kingston (archivo.zip)	64F9B3A0E482AB7011660616826ECD1F 9AFEDC4BA66F3207A20D27EB691B8FF5E6EC3AEA	Nicolás Ruiz Ruiz	

Para recoger el Pen drive, hacer clic [aquí](#).