**HERRAMIENTAS ADQUISICIÓN DE EVIDENCIA**

Nathalya Cortes Diaz

Christian Fernández

Juan Galeano

Jesús Rivera

Brandon Vidal

Brayan Arenas

Docente

Juan Carlos Valencia

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Institución Universitaria Antonio José Camacho

Ingeniería Sistemas

2021

**INTRODUCCIÓN**

El presente documento busca explicar paso a paso diferentes herramientas de recopilación de pruebas para análisis forense rápido para ver cuáles eran las diferencias. Verifico la función principalmente desde el punto de vista de volcar el archivo.

Esta descripción la haremos por medio de varias experiencias de aprendizaje: una desde Brimorlabs Windows live response, dónde veremos una herramienta automatizada de respuesta en vivo, recopila datos volátiles y crea un volcado de memoria y el segundo es desde Triage IR requiere el kit de herramientas de Sysinternals para una ejecución exitosa, donde se realizarán los pasos de una forma más amigable.

**CONTENIDO**

[Herramientas Adquisición de Evidencia 4](#_Toc82302605)

[Brimorlabs Windows live response 4](#_Toc82302606)

[Descargar e Implementar 4](#_Toc82302607)

[Triage: Incident Response 7](#_Toc82302608)

[¿Por qué utilizar IRTriage? 12](#_Toc82302609)

[CyLR: herramienta de recopilación de respuestas en vivo (Live Response) 13](#_Toc82302610)

[¿De qué se trata la herramienta? 13](#_Toc82302611)

[¿Qué es Live Response? 13](#_Toc82302612)

[¿Qué se recopila? 13](#_Toc82302613)

[Principales características: 14](#_Toc82302614)

[Práctica 16](#_Toc82302615)

[Conclusiones 18](#_Toc82302616)

[WINTRIAGE 19](#_Toc82302617)

[Referencias 24](#_Toc82302618)

# Herramientas Adquisición de Evidencia

Una evidencia digital es cualquier dato almacenado o transmitido utilizando computadores que prueba o rebate una teoría de cómo un delito ocurrió o de los elementos críticos implicados del delito como coartada o intención. También puede definirse una evidencia digital como cualquier información, sujeto de intervención humana o no, que pueda extraerse de un computador.

# Brimorlabs Windows live response

Es una herramienta automatizada de respuesta en vivo, recopila datos volátiles y crea un volcado de memoria. Esta herramienta es creada por BriMor Labs.

Esta herramienta puede extraer mucha evidencia útil de Windows. También es compatible con varios sistemas operativos como OSX / mac OS y \* nix. Resulta demasiado difícil desentrañar la relación entre el nombre de la carpeta de salida y la fecha.

La respuesta en vivo es una zona que administra la recopilación de datos de una máquina en vivo para distinguir si ha ocurrido algo. Dicha información incorpora artefactos, por ejemplo, listas de procesos, información de conexión, archivos almacenados, información de registro, etc.

## Descargar e Implementar

1. Descargue "Live Response Collection" de la página de lanzamiento, Brimor Labs.

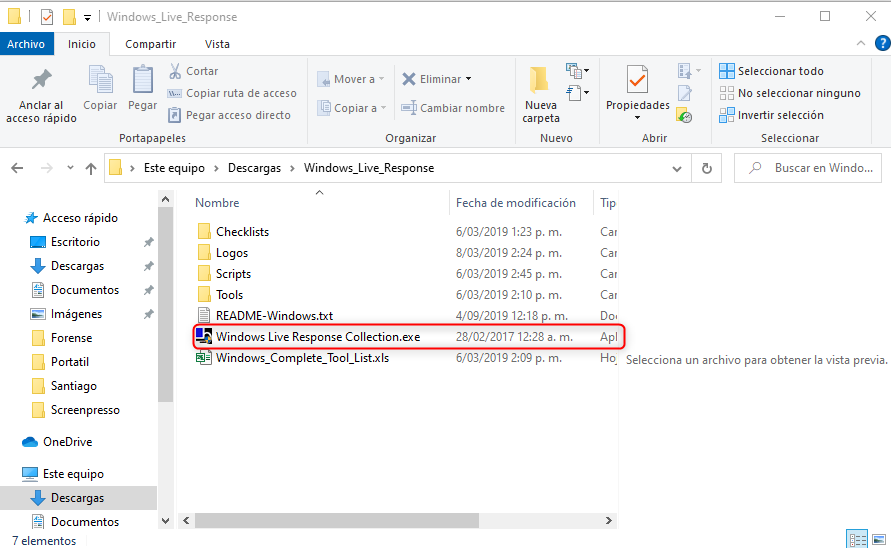
Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Ejecute " Windows\_Live\_Response \ Windows Live Response Collection.exe " en la máquina de destino.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente



1. Seleccione el script que requiera.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. Definición de las siguientes opciones para elegir scripts de recopilación de datos:

**Seguro completo:** si elige esta opción, se creará un volcado de memoria, se recopilará información volátil y también se creará una imagen de disco completa. Toda la información recopilada estará comprimida y protegida por una contraseña.

**Volcado de memoria segura:** si elige esta opción, se creará un volcado de memoria y se recopilarán datos volátiles. Toda la información recopilada estará comprimida y protegida por una contraseña.

**Triage seguro:** si elige esta opción, solo se recopilarán datos volátiles. Toda la información recopilada estará comprimida y protegida por una contraseña.

**Completo:** si elige esta opción, se creará un volcado de memoria, se recopilará información volátil y también se creará una imagen de disco completa.

**Volcado de memoria:** si elige esta opción, se creará un volcado de memoria y se recopilarán datos volátiles.

**Triaje:** si elige esta opción, solo se recopilarán datos volátiles.

1. Los resultados se envían a la carpeta " LAPTOP-7VK7OU28\_009. vi\_205116", que se crea en la misma ubicación que el ejecutable.

Tabla

Descripción generada automáticamente con confianza media

1. Tiene un registro automático de errores / procesamiento de comandos, que se almacena inteligentemente en el archivo de texto "Processing\_Details". Para facilitar la visualización de los archivos, "File\_Hashes" se almacena por separado.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

# Triage: Incident Response

La fuente flamante es del autor Michael Ahrendt, El aplicativo Triage está destinado a los equipos de respuesta a incidentes que necesitan datos de host rápidamente. La herramienta ejecutará una plétora de comandos automáticamente basados ​​en la selección. También tiene la capacidad de copiar datos a una unidad, los datos se copiarán donde se almacene el script.   
  
Es una utilidad para ayudar al personal de respuesta a incidentes a recopilar rápidamente información y artefactos del sistema de un sistema en vivo. La utilidad es altamente personalizable, satisfaciendo las necesidades de los procesos de investigación modernos.

La clasificación está diseñada para ejecutarse desde una unidad flash localmente en la máquina, a través de la ubicación de la red

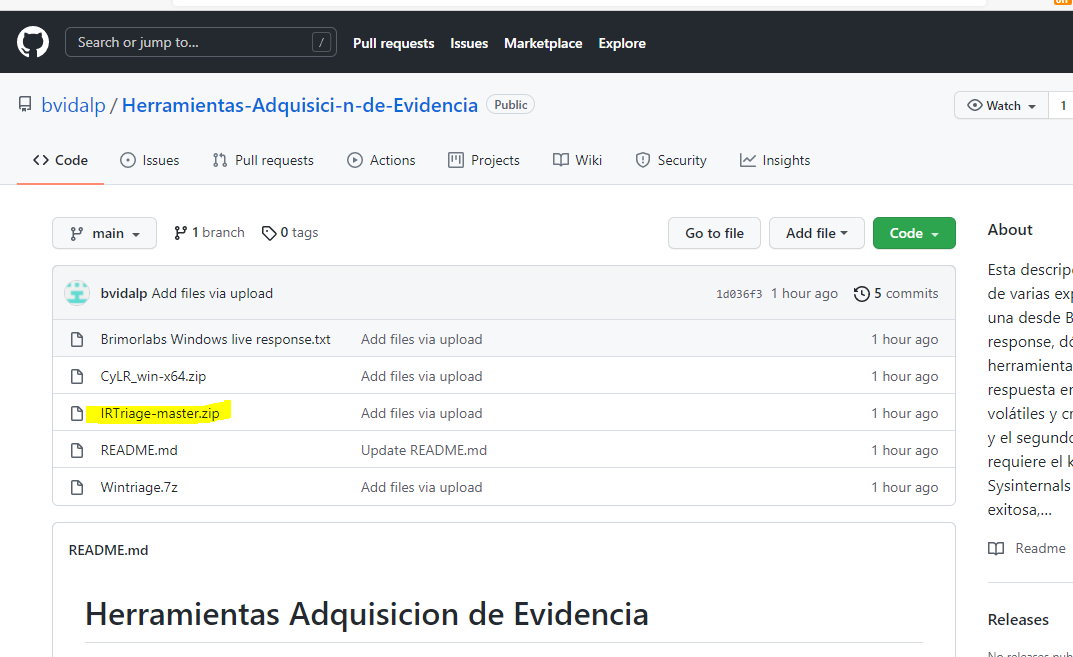
**IRTriage recopila:**- Información del sistema  
- Información de la red  
- Palos de registro  
- Información del disco duro y vertedero.

Una de las poderosas características de IRTriage es el resumen de información de Volume Shadow Copy (crear copias de seguridad o instantáneas de archivos o volúmenes de computadora) que puede estar de moda para derrotar muchas técnicas anti-forenses.

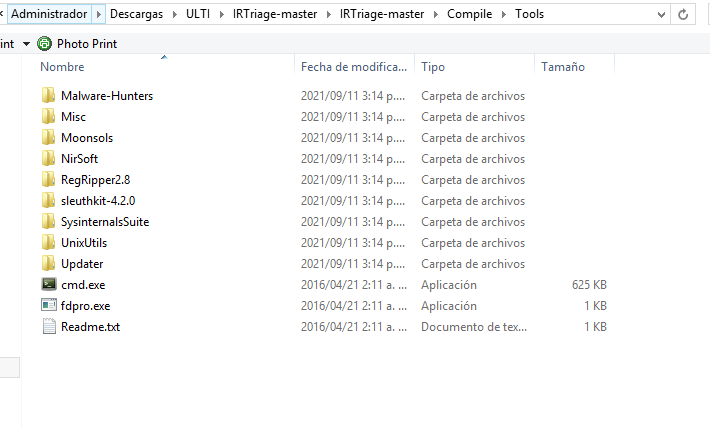
El **IRTriage** en sí es solo un script de autoit que depende de otras herramientas como:

* Win32 | 64dd (evadido de Moonsols) o FDpro \* (producto comercial de HBGary)
* Suite Sysinternals
* El kit de detective
* Regripper
* NirSoft => MFTDump y WinPrefetchView
* md5deep y sha1deep
* CSVFileView
* 7zip
* y algunos comandos integrados en Windows.

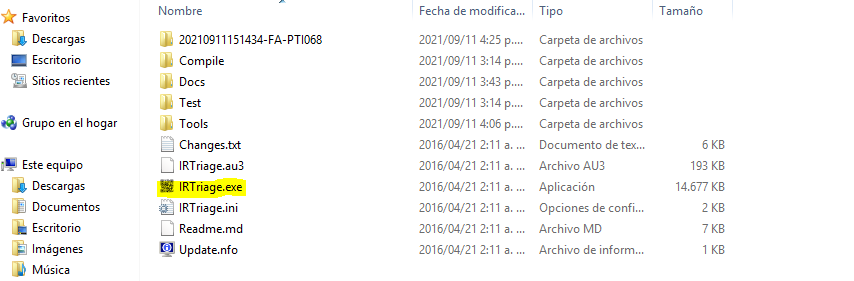
1. Para descargar el aplicativo debe ingresar a la siguiente Ruta: htttps://github.com/bvidalp/Herramientas-Adquisici-n-de-Evidencia



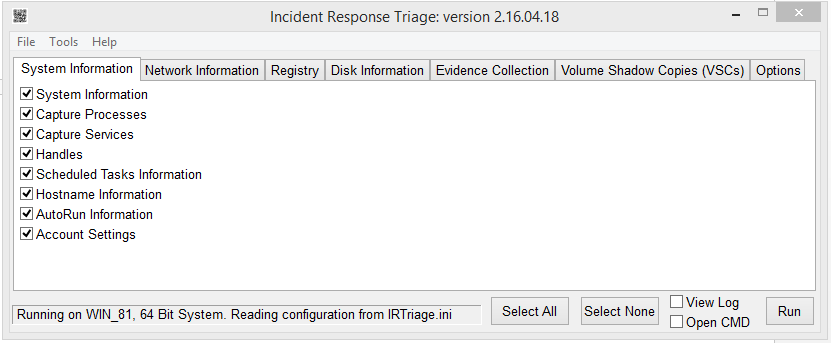
1. Al descargar el archivo desde el repositorio, revisamos que tenga las herramientas necesarias para realizar la recopilación de evidencia, los tool se encuentran en la ruta: C:\IRTriage-master\IRTriage-master\Compile\Tools



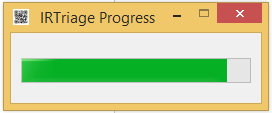
1. Luego de realizar la validación, se procede a ejecutar el aplicativo IRTriage



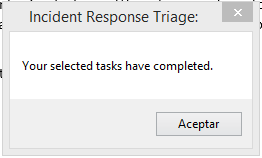
1. En la interface del aplicativo se selecciona los procesos que desea realizar dentro de la memoria donde se encuentra alojado, como se puede visualizar es muy adaptable, se tienen muchas opciones para el escaneo



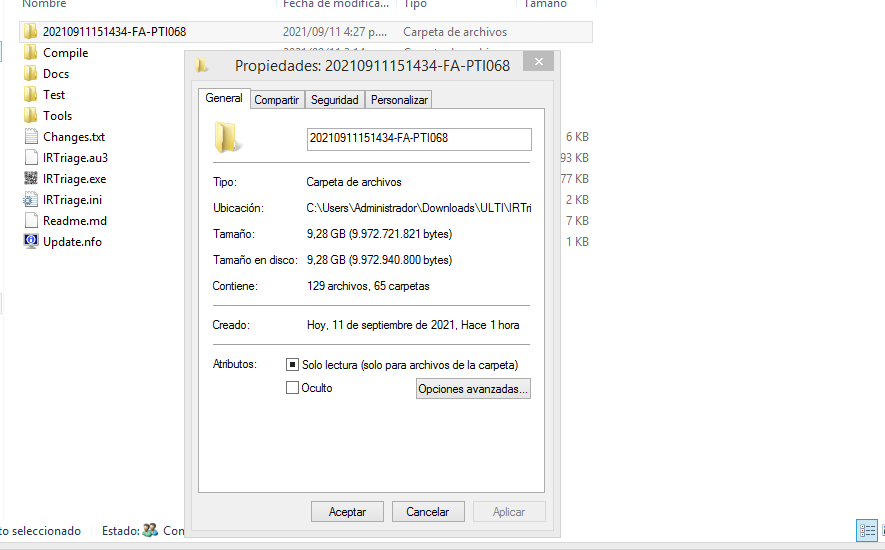
1. Después escoger lo requerido, se presiona en el botón **Run**

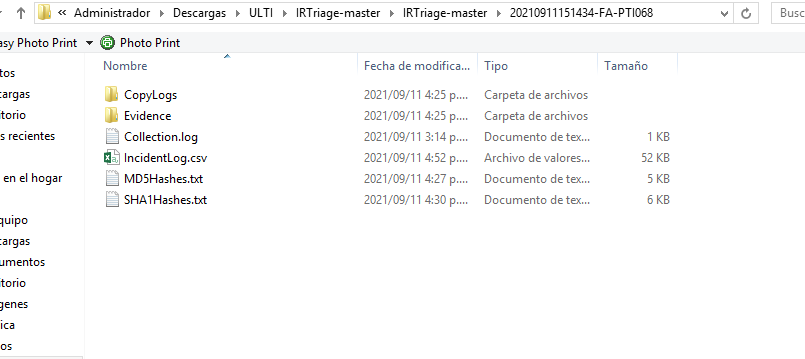


1. Proceso finalizado



1. La evidencia obtenida se encuentra en la ruta donde está alojado el aplicativo, como se puede observar en la siguiente imagen





## ¿Por qué utilizar IRTriage?

Con el tamaño de la unidad actual, el tiempo necesario para realizar imágenes de disco completo es una práctica obsoleta y debe evitarse en la medida de lo posible. Por esa razón triage-ir es una gran utilidad y se adhiere a la práctica forense moderna de rastrear los datos que se van a recopilar.

# CyLR: herramienta de recopilación de respuestas en vivo (Live Response)

El siguiente documento se encargará de describir el objetivo y funcionalidad de la herramienta CyLR, junto con una demostración de la misma.

Desarrollada y liberada al público por Alan Orlikoski y Jason Yegge el 23 de septiembre del 2016, fue una herramienta construida para el beneficio de la comunidad DFIR (*digital forensics and incident response professional*), y pensada desde un principio como una herramienta multiplataforma, abarcando los sistemas operativos de MacOS, Linux y Windows.

En un principio, el hecho de liberar esta herramienta por si sola, implicaba una serie de problemas para la comunidad en general, siendo obvia una gran curva de aprendizaje, por lo cual *Alan Orlikoski* optó por elaborar un paquete de herramientas englobado con la herramienta ***Skadi,*** dicha herramienta facilitaba el despliegue y complementaba la funcionalidad inicial de CyLR, logrando ser una “*colección de herramientas de código abierto que permite la recopilación, el procesamiento y el análisis avanzado de imágenes y artefactos forenses*”.

## ¿De qué se trata la herramienta?

La herramienta CyLR recopila artefactos forenses de hosts con sistemas de archivos NTFS de forma rápida, segura y minimiza el impacto en el host.

## ¿Qué es Live Response?

Recopilar y analizar un subconjunto de datos para determinar rápidamente la validez y gravedad de un presunto evento malicioso.

## ¿Qué se recopila?

* Historial de inicio de sesión
* Historial del navegador web
* Procesos activos
* Conexiones de red activas
* Programas instalados
* Lista de todos los usuarios

CyLR usa .NET Core y se ejecuta de forma nativa en Windows, Linux y MacOS. Las aplicaciones autónomas para lo siguiente se incluyen en las versiones de la versión 2.0 y posteriores.

**Plataformas soportadas:**

* Windows x86
* Windows x64
* Linux x64
* MacOS x64

|  |  |
| --- | --- |
| **Respuesta en vivo frente a disco frío**  **VS**  **Imagen de disco** | |
| **Respuesta en vivo:**  Pequeña colección de artefactos críticos | **Disco frío / Imagen de disco:**  Copia en bloque de la estructura completa del archivo |
| Permite una investigación rápida | Crea un retraso antes de la investigación |
| Conjunto inicial de artefactos | Recopila todos los datos en el host de destino |
| Requiere la recopilación posterior de archivos sospechosos | No requiere recogida posterior |
| No es una técnica de recolección sólida desde el punto de vista forense | Requerido para una investigación forense sólida |

## Principales características:

* Recolección rápida (es realmente rápido).
* El proceso de recopilación de archivos sin procesar no utiliza la API de Windows.
* Colección de artefactos clave de forma predeterminada.
* Posibilidad de especificar objetivos personalizados para la recopilación.
* Adquisición de archivos especiales y en uso, incluidos flujos de datos alternativos, archivos del sistema y archivos ocultos.
* Los patrones de expresión regular y global están disponibles para especificar objetivos personalizados.
* Los datos se recopilan en un archivo .zip, lo que permite al usuario modificar el nivel de compresión, establecer una contraseña de archivo y un nombre de archivo.
* Especificación de un destino SFTP para el archivo de archivos.

CyLR ahora usa .NET Core y ahora se ejecuta de forma nativa en Windows, Linux y MacOS como una aplicación .NET Core o un ejecutable autónomo a través del empaquetador warp. Como nota, el script del paquete descargará el empaquetador warp para generar un único binario con los recursos CyLR y el tiempo de ejecución CLR completo para la portabilidad. Esto significa que el binario se descomprimirá en una ubicación temporal para su ejecución. Según la documentación de warp, estas ubicaciones son:

**Ubicación de la caché de paquetes:**

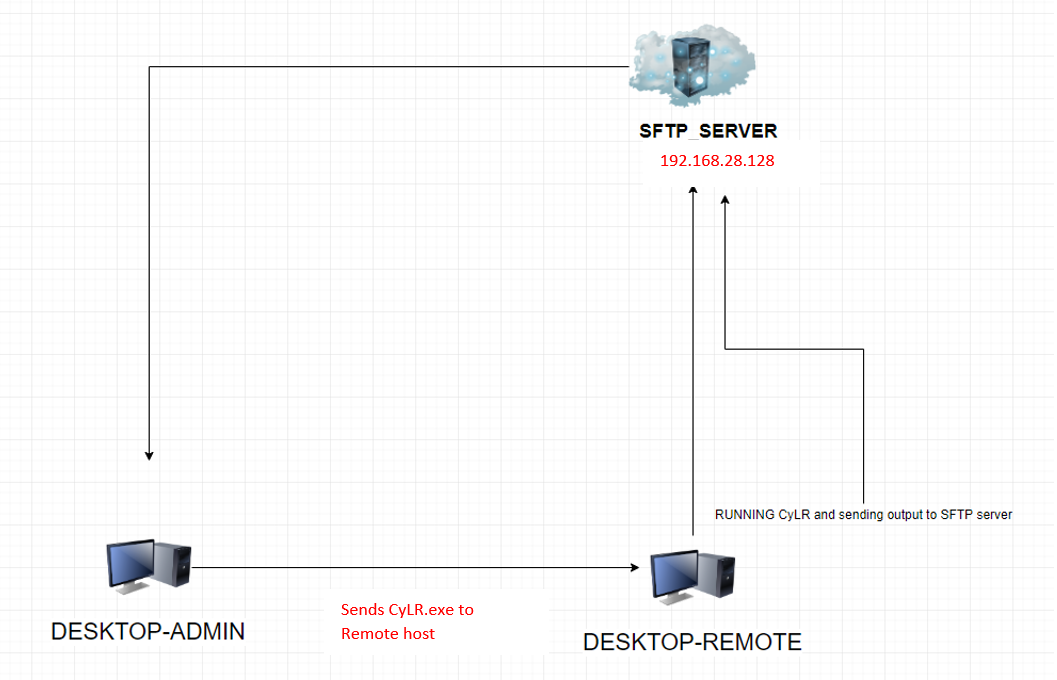
* Linux: $HOME/.local/share/warp/packages
* Mac OS: $HOME/Library/Application Support/warp/packages
* Windows: %LOCALAPPDATA%\warp\packages

**Ubicación de la caché de los corredores:**

* Linux: $HOME/.local/share/warp/runners
* Mac OS: $HOME/Library/Application Support/warp/runners
* Windows: %LOCALAPPDATA%\warp\runners

Estos cachés solo se crean en la primera ejecución o cuando se actualiza el binario empaquetado.

**Diagrama de concepto Funcional**



**Diagrama tomado de** [**https://www.datadigitally.com/2019/08/cylr-live-response-collection-tool.html**](https://www.datadigitally.com/2019/08/cylr-live-response-collection-tool.html)

El diagrama anterior simula cómo un administrador se conecta de forma remota a un escritorio, ejecuta CyLR y envía los resultados a un servidor SFTP para su recuperación.

## Práctica

A continuación, se dará un paso a paso de cómo hacer uso de esta herramienta. El ejercicio planteado es para una recolección de artefactos desde un equipo con sistema operativa Kali Linux hacia un equipo con Windows 10, para efectos de la práctica se partirá del hecho de que el equipo a escanear ya cuenta con el ejecutable de la herramienta CyLR.

**Consideraciones para el equipo Windows 10:**

Debido a que la herramienta utiliza una transferencia de archivos basada en SSH, el equipo Windows debe tener habilitado el complemento de Open SSH, para habilitarlo se deben realizar los siguientes pasos:

1. Ingresar a la opción de **Ajustes o Configuración** de Windows.
2. Seleccionar la opción **Aplicaciones**.
3. Seleccionar la opción **Aplicaciones y características**.
4. Seleccionar la opción **Características opcionales**.
5. Seleccionar la opción **Agregar una característica**.
6. Nos aparecerá un buscador, aquí digitamos “Servidor Open SSH”, y lo seleccionamos
7. Damos clic en **Instalar**.



**Consideraciones para el equipo Kali Linux:**

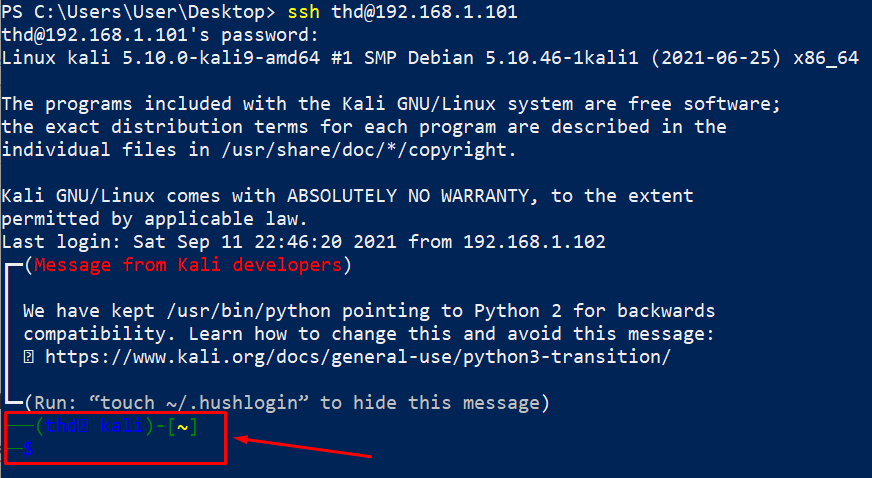
Por lo general, el servicio ssh se encuentra habilitado para Linux, pero en caso de no estarlo, seguir los siguientes pasos:

1. Instalar Open SSH:
   1. **apt-get install openssh-server**
2. Configurar inicio automático del servicio:
   1. **update-rc.d -f ssh remove**
3. Cargamos el run level por defecto de SSH:
   1. **update-rc.d -f ssh defaults**
4. Ahora cambiamos las llaves que vienen por defecto. El primer paso es hacer un respaldo de las llaves actuales:
   1. **cd /etc/ssh/**
   2. **mkdir backup\_keys**
   3. **mv ssh\_host\_\* backup\_keys/**
5. Ahora creamos las nuevas llaves:
   1. **dpkg-reconfigure openssh-server**
6. Finalmente hacemos que el servicio ssh levante al momento de bootear KALI con el siguiente comando:
   1. **sytemctl enable ssh.service**

Como primer ejercicio, vamos a validar que desde Windows nuestro servicio ssh esté disponible, para ello intentaremos conectarnos a nuestra máquina Linux con el siguiente comando:

**ssh usuario\_kali@ip\_kali**

Al ejecutar este comando nos solicitará la clave de ese usuario, la ingresamos y deberá respondernos el inicio de sesión por ssh:



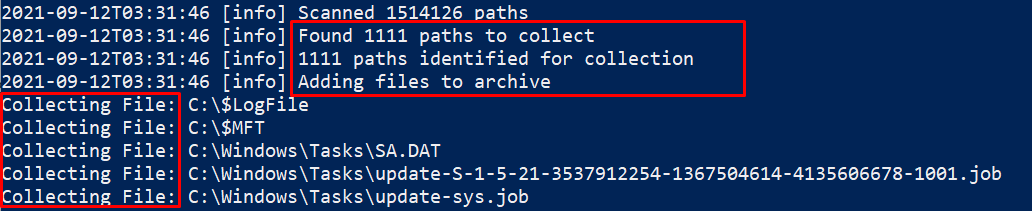
**Nota:** Tener en cuenta que por defecto OpenSSH deshabilita el inicio de sesión para el usuario root.

Luego de haber confirmado que nuestro servicio ssh se encuentra disponible, procedemos a utilizar la herramienta CyLR, para ello deberemos ubicar la ruta exacta donde se encuentra el .exe, nos ubicamos vía consola PowerShell y ejecutamos el siguiente comando:

**CyLR.exe -u usuario\_kali -p clave\_kali -s ip\_kali -of nombre\_archivo.zip**

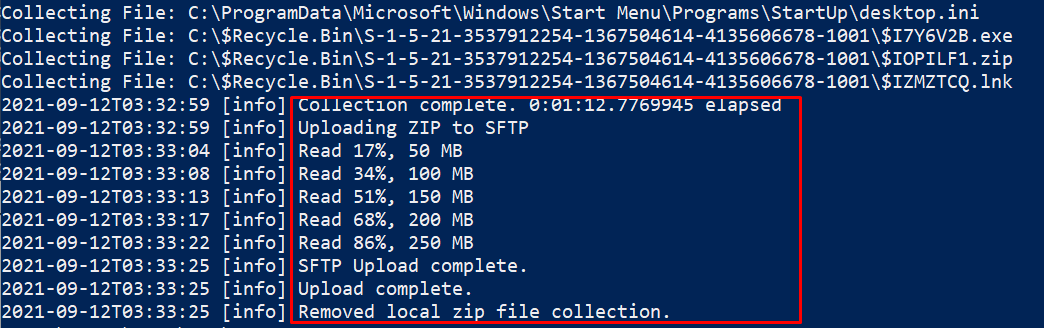
Tener en cuenta que el parámetro **nombre\_archivo.zip** es el que contendrá toda la información de los artefactos recolectados de la máquina Windows, y será colocado en el home del usuario Kali.

Procedemos a ejecutar el comando, y nos aparecerá en consola, en primera instancia un escaneo de las rutas a las cuales nuestra herramienta puede acceder, de acuerdo a este escaneo el definirá qué archivo serán comprimidos. Esto puede variar de acuerdo a los permisos del equipo Windows.



Como se puede ver en la anterior imagen la herramienta escanea y de acuerdo a las rutas que pudo acceder empieza a recolectar y comprimir la información.

Al finalizar la recolección y comprimir, la herramienta confirmará que finalizó e intentará conectarse a nuestro servidor Kali de acuerdo a las credenciales que le pasamos. Y nos confirmará que pasó el archivo y que lo eliminó del Windows local. Tener en cuenta que la herramienta genera el .zip en Windows, luego lo traslada a Linux y por último borra el .zip de Windows:



## Conclusiones

La herramienta CyLR es de gran utilidad, como una primera instancia de un análisis forense que se debe realizar en caliente y en el menor tiempo posible, la principal falencia de éste es garantizar la calidad del análisis con tan poco de tiempo sabiendo que se recopilan artefactos en vivo. A pesar de esta falencia, es de gran utilidad el canal bajo el cual se logra obtener la información, agilizando la intervención de equipos remotos.

# WINTRIAGE

**¿De qué se trata la herramienta?**

WinTriage se inspiró en el proyecto RapidTriage y utiliza partes del código original. A pesar de que RapidTriage requería solo dos indicadores de línea de comandos para ejecutarse, descubrí que todavía requería algo de educación y explicación para que nuestros analistas lo ejecutaran.

WinTriage no requiere ningún flags. Se puede ejecutar con un simple clic derecho, ejecutar como administrador. Además, en el futuro se implementará más funcionalidad específica de Windows. Llama a herramientas que extraen una imagen de memoria, ficheros de registro de Windows, eventos de sistema, Prefetch, ficheros Setupapi, información de directorio activo (si el sistema tiene el rol de controlador de dominio), así como Alternate Data Streams, listados de todos los ficheros, de aquellos que tengan el atributo de oculto, Papeleras de reciclaje, $MFT, $Logfile y $journal de todos los sistemas de ficheros NTFS existentes en la máquina, entre otros muchos artefactos. Ejecuta comandos en el sistema víctima que permiten identificar si hay algún sistema de ficheros montado actualmente, cuyo volumen se encuentre cifrado con Bitlocker, Truecrypt o Veracrypt. Esto es de gran utilidad antes de tirar del cable y hacer una imagen forense de un sistema de ficheros, cuyo análisis será un quebradero de cabeza si no se dispone de la clave de descifrado.

Además, se lleva extensa información específica de cada usuario: registro, ficheros recientes, jumplist, shellbags, soporte de hasta 6 navegadores distintos, etc… cuyo análisis permite identificar la actividad de quien sea necesario de la forma más completa posible. Todo esto lo puede extraer, tanto del estado actual del sistema, como del que este tuviera en el momento en que se llevaron a cabo cualquiera de las Shadow Copies que puedan existir en el mismo. Por defecto se lleva todo lo nombrado, pero por supuesto, Wintriage deja a elección del DFIRer, qué elementos extraer.

**¿Para qué se utiliza?**

WinTriage recopila rápidamente información crítica de áreas clave del sistema operativo para ayudar a los controladores de incidentes de seguridad de la información a determinar si ha habido o no compromiso. WinTriage automatiza la ejecución de varios comandos integrados de Windows. Es una herramienta de respuesta en vivo que extrae artefactos de Windows. Debe ejecutarse con privilegios de administrador local o de dominio y se recomienda que se realice desde una unidad externa.

**Que artefactos se pueden extraer:**

Hasta ahora, obtiene los siguientes artefactos, si se seleccionan (siguiendo las mejores prácticas forenses basadas en el orden de volatilidad):

* Volcado de memoria
* Prefetch
* Ejecución de comandos (algunos de ellos son de sistema operativo nativo y otras llamadas de herramientas externas) para obtener un montón de información en vivo, captura de red, etc.
* Información sobre volúmenes cifrados: clave de recuperación de bitlocker, advertencias truecrypt y veracrypt si se montan
* Flujos de datos alternativos en cada volumen montado
* Registro de Windows
* Eventos: EVT/EVTX y ETL
* SRUM
* Trabajos de cola de impresión fallidos
* Papelera de todos los usuarios en cada volumen lógico
* Active Directory ntds.dit (si se ejecuta en un controlador de dominio)
* Artefactos de usuarios: Registry, shellbags, navegadores (IE, Edge, Edge Chromium, Chrome, Firefox, Brave y Opera), Jumplist, Recent, Office Recent, etc...
* Instantáneas. Los mismos artefactos en cada instantánea que tiene el sistema.
* Imagen forense en vivo. Hace una imagen en vivo de C:\ Unidad lógica en formato EWF. Esto es útil en caso de que el volumen esté encriptado, por lo que la imagen física podría ser más complicada para ser procesada más adelante.

**¿Características de la herramienta?**

WinTriage se puede implementar en muchos sistemas y los resultados se analizan entre sí para ayudar al manejador de incidentes a priorizar dónde enfocar sus esfuerzos de contención. Con frecuencia, el gestor de incidentes no tiene acceso inmediato o autorización a los sistemas en cuestión y configurarlo puede llevar mucho tiempo. WinTriag se puede proporcionar rápidamente a los administradores de sistemas autorizados para recopilar la información crítica muchas veces utilizada para ayudar a identificar un compromiso. Además de la velocidad de implementación y la superación de las barreras de acceso, los otros beneficios principales de usar WinTriage incluyen:

* Capacidad para agregar/modificar comandos de colección o orígenes de eventos según sea necesario
* Resultados consistentes y formato de salida
* Simplicidad (indicador -d opcional)
* Script de colección única para mantener para todas las versiones de Windows
* Especialmente diseñado y adaptado para Windows
* Recopile información que puede necesitar para determinar si el sistema está comprometido con un solo comando

**¿Recursos del equipo para utilizar la herramienta?**

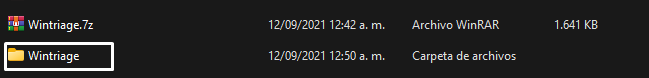
Maquina con sistemas operativo Windows

**Practica:**

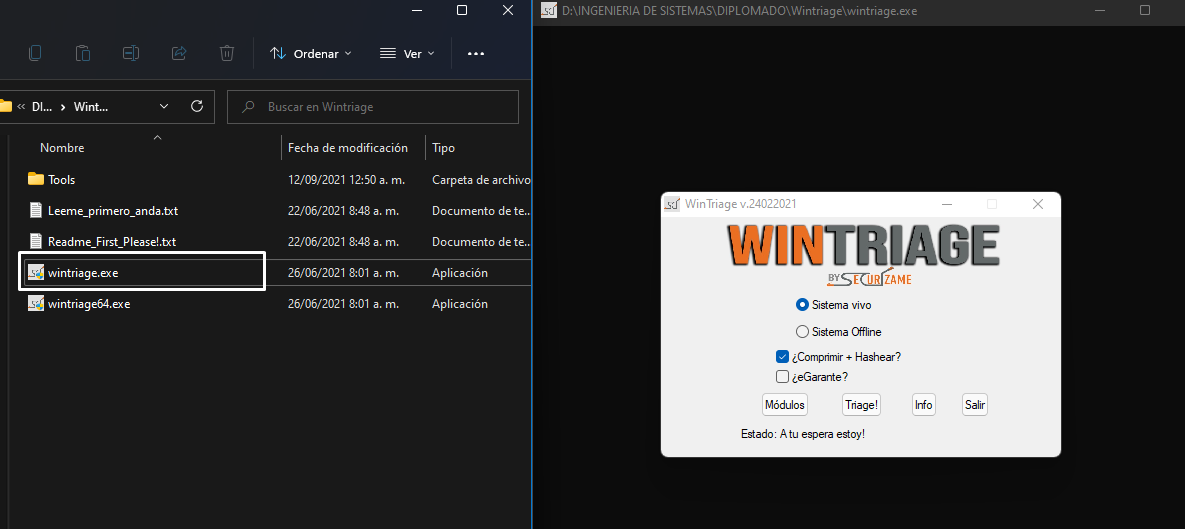
Para empezar con la implementación del software, se descargará en el siguiente enlace:

<https://cursos.securizame.com/extra/Wintriage.7z>

seguido a esto se descomprime el archivo previamente descargado.



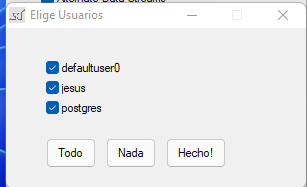
Procedemos a ejecutar la herramienta que está dentro de la carpeta descomprimida y nos carga la siguiente ventana.



Dentro de la ventana WINTRIAGE, tenemos varias opciones; en este caso ejecutaremos el análisis del sistema vivo, el cual permite extraer los siguientes módulos que se verán de la siguiente manera.



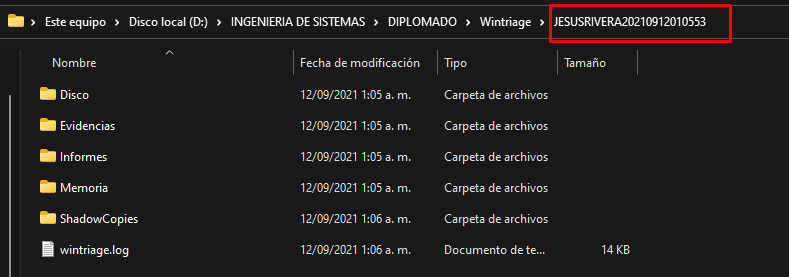
En el anterior proceso se listaron los módulos disponibles para hacer el análisis. A parte de esto está la opción de seleccionar otro usuario del sistema como se verá en la siguiente ventana.



En este caso, seleccionaremos el usuario al cual le haremos todo el análisis



Regresamos a la ventana principal y le damos en la opción de triage para que el empiece hacer el análisis. Esta herramienta también permite comprimir y sacar el hash de la información o también nos permite realizar mediante la utilización de certificados.



Ejecutando el paso anterior, el software nos genera una carpeta donde se puede observar todo lo capturado realizado mediante Wintriage.

# Referencias

* <https://github.com/orlikoski/CyLR>
* <https://docs.google.com/document/d/1L6CBvFd7d1Qf4IxSJSdkKMTdbBuWzSzUM3u_h5ZCegY/edit>
* <https://www.skadivm.com/>
* <https://docs.google.com/presentation/d/1Rl_wF9mUDOkPlbHiWAt-hOiJ-_X8WzTsRfgyYQi9t6M/htmlpresent>
* <https://securityaffairs.co/wordpress/115719/security/wintriage-triage-tool-windows-dfirers.html>
* <https://sh3llcon.org/wintriage-la-herramienta-para-el-dfirer-en-windows/>
* <https://github.com/karolpivo/wintriage>

**Repositorio para descarga de herramientas:**

https://github.com/bvidalp/Herramientas-Adquisici-n-de-Evidencia