CIBERSEGURIDAD

‘Bootcamp IX’

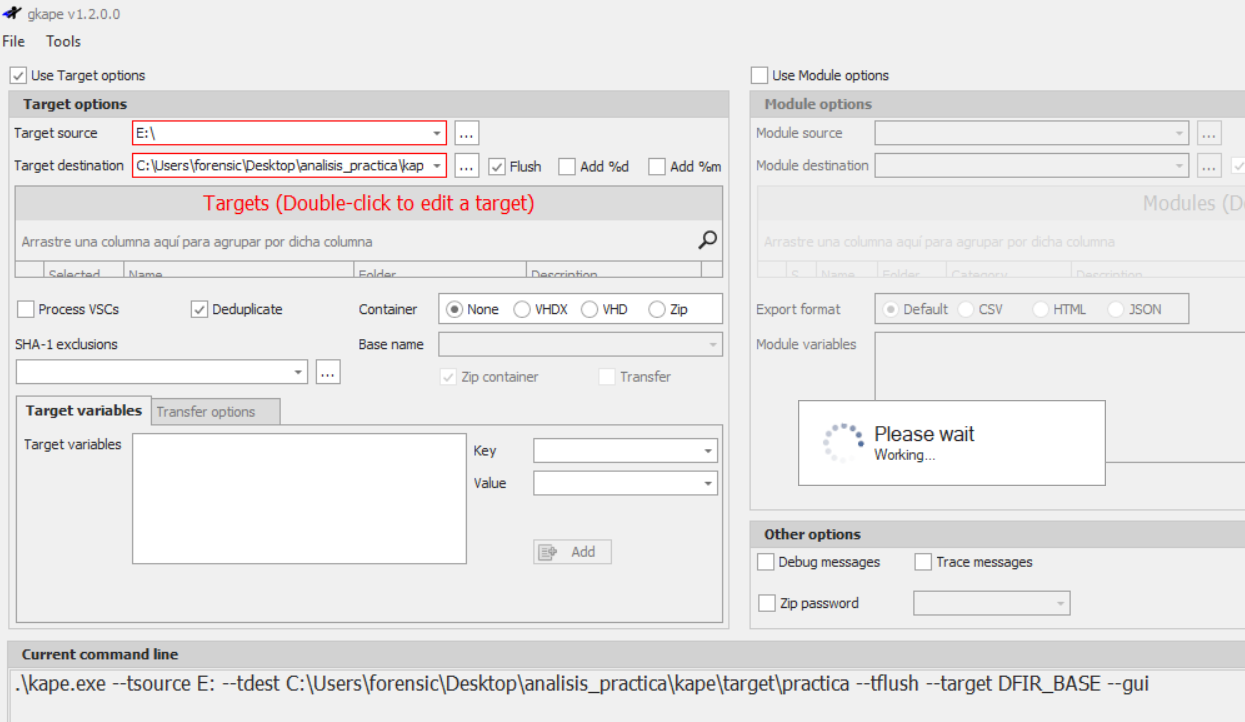
Informe Práctica Módulo DFIR.

Maximiliano Dariel Altamirano.

Academia KeepCoding.

# DESARROLLO

Para el análisis de la evidencia vamos a preprocesar los datos y ficheros sobre con la herramienta Kape, utilizando el módulo con el target predefinido “DFIR\_BASE.tkape”.

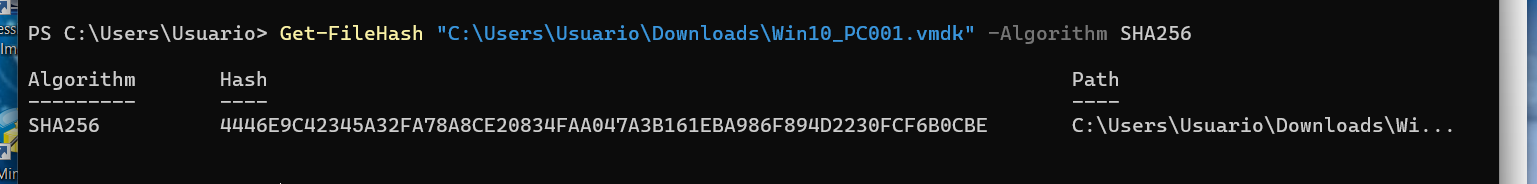


# AVANCE DESAFIOS CTF

## Forensic

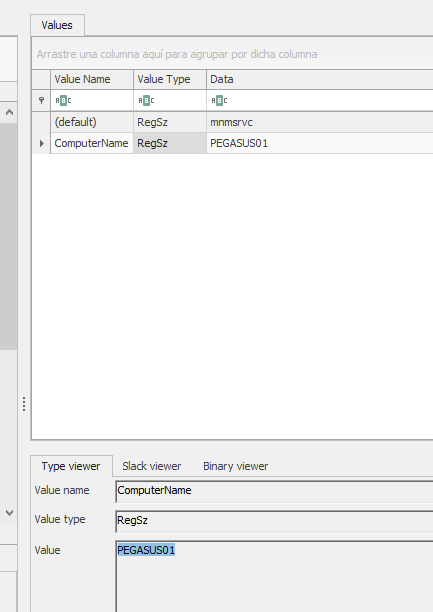
### Hash del fichero

Valimos el hash del fichero con el siguiente comando en la consola de Windows



### Nombre de la máquina

Navegaremos las opciones con la herramienta RegistryExplorer para identificar el nombre de la máquina



### Ficheros maliciosos

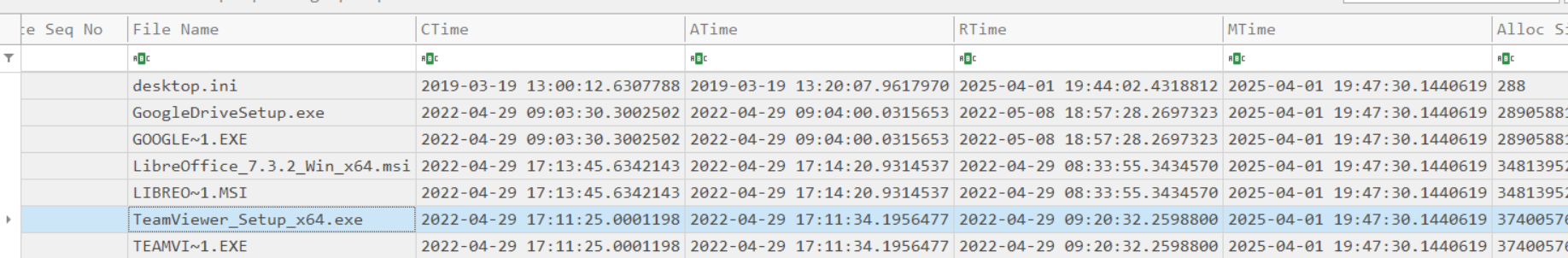
### Descarga fichero de control remoto

Con la herramienta FTK Imager identificamos el archivo .exe de control remoto que ha descargado el usuario.



### Fecha descarga software control remoto

Identificamos con la herramienta Timeline Explorer, procesando con Indx2Csv previamente el fichero $I30 del directorio Descargas del usuario, la fecha en la que hizo la descarga.

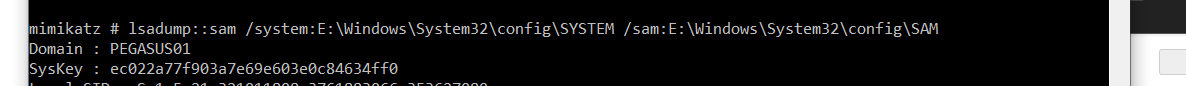


### Ficheros eliminados

Con la herramienta UsnJrnl2Csv64.exe exploramos la información del fichero $J para identificar el fichero .zip eliminado

### Contraseñas débiles

Para descubrir la contraseña, utilizamos el módulo mimikatz, lanzando el siguiente comando:



Obteniendo como resultado el siguiente HASH

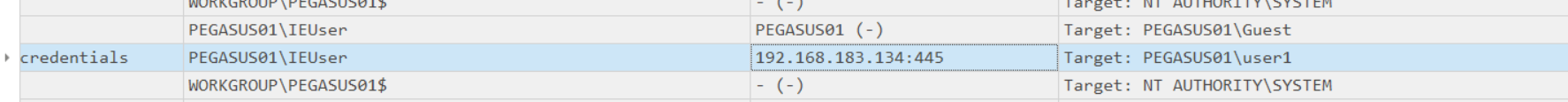


Solo resta romper el hash desde <https://crackstation.net/>



### Conexión RDP

Hemos identificado el IP de conexión por RDP con los datos obtenidos desde los eventos de seguridad de Wind (192.168.183.134:445).



# MEMORIA RAM

Trabajaremos con el fichero 20230810.mem con las siguientes características.

