[AF] Análisis forense en sistemas Windows

Artefactos

Un aterfacto se refiere a cualquier objeto, dato o elemento almacenado en un sistema que pueda proporcionar información valiosa a una investigación. Hay 2 tipos:

- de aplicación
- de sistema operativo

Logs

Los archivos de registro o logs son artefactos interesantes en cualquier SO.

Registro de eventos

Sirve para obtener inicios de sesión, camibos de configuración, fechas, etc... Antiguamente se guardaban en %SystemRoot%\System32\config en formato .evt y actualmente van en %SystemRoot%\System32\winevt\Logs en formato evtx

NOTA: %WinDir% lleva al directorio de instalación de windows(legacy) y %SystemRoot% hace lo mismo, pero se usa en la actualidad, se recomienda usar el segundo.

Registros de aplicaciones

Pueden estar en varios sitios:

- Carpeta de instalación de la aplicación
- %AppData%: Ajustes de aplicación de un usuario
- %ProgramData%: Ajustes de aplicación comunes de todos los usuarios

Registros sobre la instalación

- %SystemRoot%\setupact.log: Información de las acciones de instalación
- %SystemRoot%\setuperr.log: Información sobre errores de instalación
- %SystemRoot%\WindowsUpdate.log: Registra información sobre actualización del sistema y aplicaciones
- %SystemRoot%\Debug\mrt.log: Resultados de la herramienta de eliminación de software malintencionado de windows (MSRT)