Estación de Trabajo SIFT

Documentación y Enlaces (Español)

Alonso Eduardo
Caballero Quezada

Correo electrónico: reydes@gmail.com
Sitio web: www.reydes.com

Versión 1.0 – Agosto del 2020

La versión más actual de este documento se ubica en: http://www.reydes.com/d/?q=documentos
La versión original en idioma inglés de este documento se ubica en: https://digital-forensics.sans.org/community/downloads

DESCARGA E INSTALACIÓN DE LA ESTACIÓN DE TRABAJO SIFT

Opción 1: Descarga del Appliance VM de SIFT:

Descarga el Appliance Virtual de la Estación de Trabajo SIFT (formato .ova)

https://digital-forensics.sans.org/community/download-sift-kit/3.0

- Login = **sansforensics**
- Contraseña = **forensics**

Opción2: Instalación Fácil de SIFT

1. Descargar el archivo ISO de Ubuntu 16.04 e instalar Ubuntu 16.04 en cualquier sistema

http://releases.ubuntu.com/16.04.6

2. Instalar SIFT-CLI utilizando las siguientes instrucciones de instalación:

https://github.com/teamdfir/sift-cli#installation

3. Ejecutar el comando "sudo sift install" para instalar la versión más reciente de SIFT-CLI

4. Felicitaciones – ahora se tiene una estación de trabajo SIFT-CLI

- Login = **sansforensics**
- Contraseña = **forensics**

¿Se ha encontrado alguna falla o problema con la instalación?. Si se está experimentando errores en SIFT, por favor enviar los errores, fallas, y actualizaciones recomendadas a:

https://github.com/teamdfir/sift/issues

Resumen de la Estación de Trabajo SIFT

¿Porque SIFT?

La estación de trabajo SIFT, es un grupo de herramientas libres de fuente abierta para respuesta de incidentes y forense digital, diseñado para realizar exámenes detalladas de forense digital, en una diversidad de configuraciones. Puede coincidir con cualquier suite actual de herramientas para respuesta de incidentes y forense digital. SIFT demuestra las capacidades avanzadas de respuesta de incidentes y técnicas profundas de forense digital para intrusiones, se puede

alcanzar utilizando herramientas de fuente abierta, las cuales están libremente disponibles y actualizadas frecuentemente.

¿Quién creó SIFT?

Rob Lee y su equipo crearon y continuamente actualizan la estación de trabajo SIFT. Es exitosamente utilizada para respuesta de incidentes y forense digital, además de estar disponible hacia la comunidad como un servicio público. Con más de 100,000 descargas, SIFT continúa siendo muy popular en el ámbito de la respuesta de incidentes y forense digital, junto con las soluciones comerciales.

Ofrecida como un proyecto libre y de fuente abierta, la estación de trabajo SIFT se enseña en algunos de los cursos de SANS

Advanced Incident Response Course (FOR508)

http://www.sans.org/course/advanced-incident-response-digital-forensics

Advanced Network Forensics course (FOR572)

http://www.sans.org/course/advanced-network-forensics-analysis

Cyber Threat Intelligence (FOR578)

https://www.sans.org/course/cyber-threat-intelligence

Memory Analysis In-depth (FOR526)

http://www.sans.org/course/memory-forensics-in-depth

“Incluso si SIFT costase decenas de dólares, seguiría siendo un producto muy competitivo”, expresa Alan Paller, director de investigación de SANS. “Sin costo, no hay razón para no se parte del portafolio en cada organización quienes tiene profesionales en respuesta de incidentes”.

“La estación de trabajo SIFT se ha convertido rápidamente en mi herramienta cuando realizo exámenes. El poder de las herramientas forenses de fuente abierta en el kit, sobre la cima de un sistema operativo Linux estable y versátil, genera un rápido acceso hacia todo lo necesario para realizar un exhaustivo análisis de un sistema de cómputo”, expresa Ken Pryor, GCFA Robinson, Departamento de Policía de IL.

Nuevas características clave de SIFT incluyen:

- Basado en Ubuntu LTS 16.04
- Sistema base de 64 bits
- Mejor utilización de memoria

- Actualización y personalizaciones de paquetes DFIR automáticos
- Las más recientes herramientas forenses y técnicas
- Un Appliance lista para enfrentar lo forense
- Compatibilidad cruzad entre Linux y Windows
- Opción para instalar sistemas autónomos mediante un instalador SIFT-CLI
- Soporte ampliado para Sistema de Archivos

Descargar el Appliance de la Estación de Trabajo SIFT

Descargar el Appliance Virtual de la Estación de Trabajo SIFT (formato .ova)

https://digital-forensics.sans.org/community/download-sift-kit/3.0

¿Se tienen problemas descargando SIFT?

Si se tienen inconvenientes descargando el kit SIFT, por favor contactarse al siguiente correo electrónico: sift-support@sans.org e incluir la URL proporcionada, su dirección IP, tipo de navegador, y si se está utilizando un proxy de algún tipo.

Usuario y Contraseña de SIFT

Después de su descarga, utilizar las siguientes credenciales para ganar acceso.

- Login = **sansforensics**
- Contraseña = **forensics**

$ sudo su -

Utilizarlo para elevar privilegios a root, para montar imágenes de disco.

Instalación Manual de SIFT

Instalación

El objetivo es hacer lo más simple posible la instalación (y actualización) de la estación de trabajo SIFT, por lo tanto se creo el proyecto en línea de comando de SIFT, el cual es un binario auto contenido, el cual puede ser descargado y ejecutado para convertir una instalación de Ubuntu en una estación de trabajo SIFT. El proyecto puede ser revisado en la siguiente página:

https://github.com/teamdfir/sift

Para instalar SIFT sobre un sistema Ubuntu 16.04:

1. Instalar Ubuntu 16.04 en un sistema

2. Descargar e instalar la Herramienta SIFT-CLI siguiendo las instrucciones de instalación, de la página: https://github.com/teamdfir/sift-cli#installation

3. Ejecutar **$ sudo sift install**

Para instalar SIFT sobre un sistema Windows 10:

1. Instalar la Edición Creadores de Windows 10 o superior sobre un sistema.

2. Abrir PowerShell como administrador y ejecutar: **Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux**

3. Ejecutar la Shell Bash de Ubuntu desde un PowerShell de Windows o línea de comando.

4. Descargar e instalar la Herramienta SIFT-CLI siguiendo las instrucciones de instalación, de la página: https://github.com/teamdfir/sift-cli#installation

5- Ejecutar **$ sudo sift install**

Capacidades de la Estación de Trabajo SIFT

Soporte de sistema de archivos

- NTFS (NTFS)
- iso9660 (ISO9660 CD)
- hfs (HFS+)

- raw (Datos en Crudo)
- swap (Espacio de Intercambio)
- memory (Datos de RAM)
- fat12 (FAT12)
- fat16 (FAT16)
- fat32 (FAT32)
- ext2 (EXT2)
- ext3 (EXT3)
- ext4 (EXT4)
- ufs1 (UFS1)
- ufs2 (UFS2)
- vmdk

Soporte de imágenes de evidencia

- raw (Archivo simple en crudo (dd))
- aff (Formato Avanzado Forense)
- afd (Archivo Múltiple AFF)
- afm (AFF con metadatos externos)
- afflib (Todos los formatos de imagen AFFLIB (Incluyendo los beta))
- ewf (Formato Testigo Experto (encase))
- split raw (Archivos en crudo divididos) mediante affuse
- affuse – monta imagen 001 / imágenes divididas para visualizar archivos únicos en crudo y metadatos

- split ewf (Archivos divididos E01) mediante ewf.py
- mount_ewf.py – monta imagen E01 / imágenes divididos para visualizar archivos únicos en crudo y metadatos
- ewfmount – Monta imagen E01 / imágenes divididos para visualizar archivos únicos en bruto y metadatos

Soporte para Respuesta de Incidentes

- Compatible con la Suite de Herramienta F-Responde
- Scripting Rápido y Análisis
- Inteligencia de Amenazas y Soporte para Indicadores de Compromiso
- Caza de Amenazas y Capacidades para Análisis de Malware

Software Incluido:

- log2timeline (Herramienta para la Generación de Cronologías)
- Rekall Framework (Análisis de Memoria)
- Volatility Framework (Análisis de Memoria)
- Plugins de 3eros de Volatility
- bulk_extractor
- autopsy
- afflib
- afflib-tools
- ClamAV
- dc3dd
- imagemounter

- libbde
- libesedb
- libevt
- libevtx
- libewf
- libewf-tools
- libewf-python
- libfvde
- libvshadow
- lightgrep
- log2timeline
- Plaso
- Qemu
- regripper y plugins
- SleuthKit
- Más de 100 herramientas. Para ver el listado de paquetes instalados revisar: http://sift.readthedocs.org/en/latest/user/packages.html

Compatibilidad de la Estación de Trabajo SIFT Y REMNux

Nota importante: La versión actual de REMnux únicamente funciona con Ubuntu 14.04, No con 16.04. Por lo tanto actualmente NO es compatible con la versión más reciente de la estación de trabajo SIFT. Por lo tanto, una vez REMnux sea actualizado para funcionar con 16.04, será compatible con SIFT.

How-Tos de la Estación de Trabajo SIFT

Cheat Sheets y Posters DFIR de SANS

http://digital-forensics.sans.org/community/cheat-sheets

Proyecto de Documentación de SIFT-CLI

http://sift.readthedocs.org/

Como Montar una Imagen de Disco en Modo Sólo Lectura

https://digital-forensics.sans.org/blog/2009/02/19/digital-forensic-sifting-how-to-perform-a-read-only-mount-of-evidence/

Como Crear un Cronología de Registro y Sistema de Archivos

https://digital-forensics.sans.org/blog/2009/02/24/digital-forensic-sifting-registry-and-filesystem-timeline-creation/

Como Crear una Super Cronología

https://digital-forensics.sans.org/blog/2011/12/07/digital-forensic-sifting-super-timeline-analysis-and-creation

Series en Youtube de la Estación de Trabajo SIFT

https://www.youtube.com/playlist?list=PL60DFAE759FCDF36A

FOR508 – Respuesta de Incidentes Avanzada

http://www.sans.org/course/advanced-incident-response-digital-forensics

Reporte de Fallas

Como con cualquier publicación, existirán fallas y peticiones; por favor reportar todos los problemas y fallas hacia el siguiente sitio web y localización.

https://github.com/sans-dfir/sift/issues