Estación de Trabajo SIFT

(Traducción al Español)

Alonso Eduardo
Caballero Quezada

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

Versión 2.0 - Febrero del 2022

La versión más actual de este documento se ubica en: https://www.reydes.com/d/?q=documentos
La versión original en idioma inglés de este documento se ubica en: **https://www.sans.org/tools/sift-workstation/**

Estación de Trabajo 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 detallados en forense digital, para una diversidad de configuraciones. Puede coincidir con cualquier suite actual de herramientas para respuesta de incidentes y forense digital. SIFT demuestra las capacidades avanzadas en 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 son actualizadas frecuentemente.

DESCARGA E INSTALACIÓN DE LA ESTACIÓN DE TRABAJO SIFT

Opción 1: Descarga del Appliance VM de SIFT:

Hacer clic en el botón “Login to Download” o “Login para Descargar”, e ingrese (o cree) sus credenciales de su cuenta para el Portal de SANS, y así descargar la máquina virtual. Una vez iniciada la máquina virtual, utilizar las credenciales a continuación detalladas para obtener acceso.

https://idp.sans.org/simplesaml/module.php/core/loginuserpass.php

- Login = **sansforensics**
- Contraseña = **forensics**
- **$ sudo su -**

  Utilizado para elevar privilegios hacia root mientras monta las imágenes del disco

- Valores Hash

  MD5: b838d44bd56ad0e8f4f6a5a6b00b7c8d SIFT-Workstation.ova
  SHA256: 27fac07e95498db5eaaa2c6c0b85ef9ca96090fb0964e552a7792a441ebe4d74 SIFT-Workstation.ova

¿Tiene problemas descargando SIFT?

Si tiene inconvenientes descargando la Máquina Virtual de la Estación de trabajo SIFT, por favor contacte con sift-support@sans.org, e incluya la URL obtenida, su dirección IP pública, tipo de navegador, y si está utilizando o no algún tipo de proxy.

Opción 2A: Instalación Fácil sobre un Sistema Ubuntu Nativo

1. Descargar el archivo ISO de Ubuntu 20.04 e instalar Ubuntu 20.04 en cualquier sistema

http://www.ubuntu.com/download/desktop

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

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

- Login = **sansforensics**
- Contraseña = **forensics**
- **$ sudo su -**
  Usado para elevar privilegios hacia root mientras monta imágenes de disco

Opción 2B: Instalación Fácil sobre Microsoft Windows utilizando el Subsistema Windows para Linux

1. Instalar el Subsistema Windows para Linux (WSL) de acuerdo a la más reciente directriz de Microsoft, actualmente ubicado en:

https://docs.microsoft.com/en-us/windows/wsl/install-win10

La distribución SIFT puede ser instalado ya sea en WSL versión 1 o versión 2.

Seleccionar Ubuntu 20.04 durante el proceso de instalación de WSL.

2. Lanzar la Shell Bash de Ubuntu y elevar hacia root (**sudo su**) para evitar inconvenientes de permisos durante el proceso de instalación.

3. Prepararse para instalar SIFT-CLI utilizando estas instrucciones de instalación.

https://github.com/sans-dfir/sift-cli#installation

4. Ejecutar "**sift install --mode=server**" para instalar la versión más reciente de SIFT en WSL

5. Felicitaciones - ahora se tiene una estación de trabajo SIFT

¿Quién creó SIFT?

Rob Lee y su equipo crearon la Estación de trabajo original SIFT en el año 2007, con el propósito de apoyar el análisis forense en las clases de SANS FOR508. A través de los años, él y un pequeño equipo han actualizado continuamente la Estación de trabajo SIFT para su uso en clase, como también ser un recurso público para la comunidad. Con más de 125,000 descargas hasta la fecha, la Estación de trabajo SIFT continua siendo una de las ofertas disponibles más populares de fuente abierta para la respuesta de incidentes y análisis forense digital.

Ofrecida como un proyecto libre y de fuente abierta, la estación de trabajo SIFT se utiliza en los siguientes cursos sobre respuesta de incidentes en SANS

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

https://www.sans.org/cyber-security-courses/advanced-incident-response-threat-hunting-training/

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

https://www.sans.org/cyber-security-courses/advanced-network-forensics-threat-hunting-incident-response/

FOR578: Cyber Threat Intelligence

https://www.sans.org/cyber-security-courses/cyber-threat-intelligence/

FOR608: Enterprise-Class Incident Response & Threat Hunting

https://www.sans.org/cyber-security-courses/enterprise-incident-response-threat-hunting/

“Incluso si SIFT costase decenas de miles de dólares, seguiría siendo un producto muy competitivo”, expresa Alan Paller, director de investigación de SANS. “Sin costo alguno, no hay razón para no sea parte del portafolio de cada organización con 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, quien ha realizado incontables casos relacionados con forense y respuesta de incidentes.

Nuevas Características Clave de la Estación de trabajo SIFT

- Basado en Ubuntu LTS 20.04
- 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 de Máquina Virtual lista para enfrentar lo forense
- Compatibilidad cruzada entre Linux y Windows
- Opción para instalar sistemas autónomos mediante un instalador SIFT-CLI
- Soporte ampliado para Sistema de Archivos

Capacidades de la Estación de Trabajo SIFT

Una herramienta clave durante una respuesta de incidentes, la cual ayuda a los profesionales en respuesta de incidentes a identificar y contener grupos de amenazas avanzadas. SIFT proporciona

capacidades robustas para analizar sistemas de archivos, evidencia de red, imágenes de memoria, y más.

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)

Soporte de imágenes de evidencia

- raw (Archivo sencillo 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
- vmdk
- vhd/vhdx
- qcow

Soporte para Respuesta de Incidentes

- Compatible con la Suite de Herramienta F-Response https://www.f-response.com/
- Scripting Rápido y Análisis
- Inteligencia de Amenazas y Soporte para Indicadores de Compromiso
- Caza de Amenazas y Capacidades para Análisis de Malware

Software Incluido:

- Plaso/log2timeline (Herramienta para la Generación de Cronologías)
- Rekall Framework (Análisis de Memoria)
- Volatility Framework (Análisis de Memoria)
- Plugins de 3eros de Volatility
- bulk_extractor
- afflib
- afflib-tools

- ClamAV
- dc3dd
- imagemounter
- libbde
- libesedb
- libevt
- libevtx
- libewf
- libewf-tools
- libewf-python
- libfvde
- libvshadow
- lightgrep
- Qemu
- regripper y plugins
- SleuthKit
- Cientos de herramientas adicionales

Compatibilidad de la Estación de Trabajo SIFT Y REMnux

REMnux es un conjunto de herramientas Linux para ingeniería reversa y análisis de software malicioso. REMnux proporciona una colección curada de herramientas libres creadas por la comunidad. Los analistas pueden utilizarlas para investigar malware sin tener que encontrar, instalar, y configurar herramientas. REMnux es utilizado en SANS FOR610: Reverse Engineering Malware.

https://www.sans.org/cyber-security-courses/reverse-engineering-malware-malware-analysis-tools-techniques/

REMnux puede añadirse dentro de una instalación de la Estación de trabajo SIFT. Para instalar REMnux primero instalar la Estación de trabajo SIFT, utilizando las instrucciones antes detalladas, Luego seguir las instrucciones para añadir los componentes de REMnux.

https://docs.remnux.org/install-distro/add-to-existing-system

How-Tos y Recursos sobre la Estación de Trabajo SIFT

Posters & Cheat Sheets

https://www.sans.org/posters/?focus-area=digital-forensics

Digital Forensic SIFTing: How to perform a read-only mount of filesystem evidence

https://www.sans.org/blog/digital-forensic-sifting-how-to-perform-a-read-only-mount-of-filesystem-evidence/

Digital Forensic SIFTing: Registry and Filesystem Timeline Creation

https://www.sans.org/blog/digital-forensic-sifting-registry-and-filesystem-timeline-creation

Digital Forensic SIFTing: SUPER Timeline Creation using log2timeline

https://www.sans.org/blog/digital-forensic-sifting-super-timeline-creation-using-log2timeline

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

https://www.sans.org/cyber-security-courses/advanced-incident-response-threat-hunting-training

Reportar Fallas

Por favor reporte todos los inconvenientes, fallas, y peticiones de funcionalidades hacia la página del proyecto en GitHub, ubicada en:

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

Mis Cursos Sobre Forense Digital

Curso de Informática Forense

https://www.reydes.com/d/?q=Curso_de_Informatica_Forense

Curso Forense de Redes

https://www.reydes.com/d/?q=Curso_Forense_de_Redes

Curso Forense de Autopsy

https://www.reydes.com/d/?q=Curso_Forense_de_Autopsy

Curso Fundamentos de Forense Digital

https://www.reydes.com/d/?q=Curso_Fundamentos_de_Forense_Digital

Todos mis cursos virtuales

https://www.reydes.com/d/?q=cursos