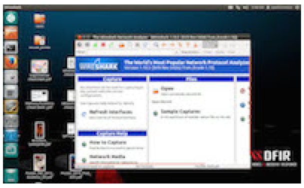
Community: Downloads

SANS Investigative Forensic Toolkit (SIFT) Workstation Version 3



[Download SIFT Workstation VMware Appliance Now - 1.5 GB]

Having trouble downloading?
If you are having trouble downloading the SIFT Kit please contact sift-support@sans.org and include the URL you were given, your IP address, browser type, and if you are using a proxy of any kind.

Having trouble with SIFT?
If you are experiencing errors in SIFT 3 itself, please submit errors, bugs, and recommended updates here: https://github.com/sans-dfir/sift/issues

How To:

1. Download Ubuntu 14.04 ISO file and install Ubuntu 14.04 on any system. -> http://www.ubuntu.com/download/desktop
2. Once installed, open a terminal and run *"wget --quiet -O - https://raw.github.com/sans-dfir/sift-bootstrap/master/bootstrap.sh | sudo bash -s -- -i -s -y"*
3. Congrats -- you now have a SIFT workstation!!

Page Links

- SIFT Workstation Overview
- Download SIFT Workstation Locations
- Manual SIFT Workstation Installation
- SIFT Workstation Capabilities
- SIFT Workstation How-Tos
- Report Bugs
- SIFT Recommendations

SIFT Workstation Overview

An international team of forensics experts, led by SANS Faculty Fellow Rob Lee, created the SANS Incident Forensic Toolkit (SIFT) Workstation for incident response and digital forensics use and made it available to the whole community as a public service. The free SIFT toolkit, that can match any modern incident response and forensic tool suite, is also featured in SANS' Advanced Incident Response course (FOR 508). It demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

Offered free of charge, the SIFT 3 Workstation is taught only in the following incident response courses at SANS:

- Advanced Incident Response course (FOR508)
- Advanced Network Forensics course (FOR572)
- Memory Analysis In-depth (FOR526)

SIFT3 demonstrates that advanced incident response capabilities and deep dive digital forensic techniques to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

"Even if SIFT were to cost tens of thousands of dollars, it would still be a very competitive product," says, Alan Paller, director of research at SANS. "At no cost, there is no reason it should not be part of the portfolio in every organization that has skilled incident responders."

Developed and continually updated by an international team of incident response and forensic experts, the SIFT is a group of free open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings. With over 100,000 downloads to date, the SIFT continues to be the most popular open-source incident-response and forensic offering next to commercial source solutions. For courses that feature the SIFT, please attend FOR508 Advanced Incident Response.

"The SIFT Workstation has quickly become my "go to" tool when conducting an exam. The powerful open source forensic tools in the kit on top of the versatile and stable Linux operating system make for quick access to most everything I need to conduct a thorough analysis of a computer system," said Ken Pryor, GCFA Robinson, IL Police Department

Key new features of SIFT 3 include:

- Ubuntu LTS 14.04 Base
- 64 bit base system
- Better memory utilization
- Auto-DFIR package update and customizations
- Latest forensic tools and techniques
- VMware Appliance ready to tackle forensics
- Cross compatibility between Linux and Windows
- Option to install stand-alone via (.iso) or use via VMware Player/Workstation
- Online Documentation Project at http://sift.readthedocs.org/
- Expanded Filesystem Support

Download SIFT Workstation 3 Locations

Download SIFT Workstation VMware Appliance - 1.5 GB

Note: The file is zipped using 7zip in the 7z format. We recommend 7zip to unzip it. Download 7zip.

Manual SIFT Installation

Installation

We tried to make the installation (and upgrade) of the SIFT workstation as simple as possible, so we create the SIFT Bootstrap project, which is a shell script that can be downloaded and executed to convert your Ubuntu installation into a SIFT workstation.

Check the project out at https://github.com/sans-dfir/sift-bootstrap

Quickstart

Using *wget* to install the latest, configure SIFT, and SIFT theme

```
wget --quiet -O - https://raw.github.com/sans-dfir/sift-bootstrap/master/bootstrap.sh | sudo bash -s -- -i -s -y
```

Using *wget* to install the latest (tools only)

```
wget --quiet -O - https://raw.github.com/sans-dfir/sift-bootstrap/master/bootstrap.sh | sudo bash -s -- -i
```

SIFT Login/Password:

After downloading the toolkit, use the credentials below to gain access.

- Login "sansforensics"
- Password "forensics"
- $ sudo su -
  - Use to elevate privileges to root while mounting disk images.

SIFT Workstation Capabilities

A key tool during incident response helping incident responders identify and contain advanced threat groups. The SIFT, provides the ability to securely examine raw disks, multiple file systems, evidence formats. Places strict guidelines on how evidence is examined (read-only) verifying that the evidence has not changed

File system support

- ntfs (NTFS)
- iso9660 (ISO9660 CD)
- hfs (HFS+)
- raw (Raw Data)
- swap (Swap Space)
- memory (RAM Data)
- fat12 (FAT12)
- fat16 (FAT16)
- fat32 (FAT32)
- ext2 (EXT2)
- ext3 (EXT3)
- ext4 (EXT4)
- ufs1 (UFS1)
- ufs2 (UFS2)
- vmdk

Evidence Image Support

- raw (Single raw file (dd))
- aff (Advanced Forensic Format)
- afd (AFF Multiple File)
- afm (AFF with external metadata)
- afflib (All AFFLIB image formats (including beta ones))
- ewf (Expert Witness format (encase))
- split raw (Split raw files) via affuse
- affuse \0x2010 mount 001 image/split images to view single raw file and metadata
- split ewf (Split E01 files) via mount_ewf.py
- mount_ewf.py \0x2010 mount E01 image/split images to view single raw file and metadata
- ewfmount - mount E01 images/split images to view single rawfile and metadata

Incident Response Support

- F-Response Tool Suite Compatible
- Rapid Scripting and Analysis
- Threat Intelligence and Indicator of Compromise Support

- Threat Hunting and Malware Analysis Capabilities

Partition Table Support

- dos (DOS Partition Table)
- mac (MAC Partition Map)
- bsd (BSD Disk Label)
- sun (Sun Volume Table of Contents (Solaris))
- gpt (GUID Partition Table (EFI))

Software Includes:

- log2timeline (Timeline Generation Tool)
- Rekall Framework (Memory Analysis)
- Volatility Framework (Memory Analysis)
- Autopsy (GUI Front-End for Sleuthkit)
- PyFLAG (GUI Log/Disk Examination)afflib
    - afflib-tools
- libbde
- libesedb
- libevt
- libevtx
- libewf
    - libewf-tools
    - libewf-python
- libfvde
- libvshadow
- log2timeline
- Plaso
- qemu
- SleuthKit
- 100s more tools -> See Detailed Package Listing

SIFT Workstation and REMNux Compatibility

Having the right tools at your fingertips can save hours and even days when performing incident response or analyzing malicious artifacts. You can now install two popular Linux distros, SIFT Workstation and REMnux, on the same system to create a powerful toolkitfor digital forensics and incident response. To quote @ma77bennett, this combo is reminiscent of "Transformers combining together to form a super robot."

You can start with SIFT and then add REMnux, or begin with REMnux and add SIFT to it. If you prefer the look and feel of SIFT Workstation, use SIFT as the starting point. If you like the look of REMnux, start with that one.

After booting into SIFT Workstation and making sure that it has Internet access, run the following command to install REMnux on it:

```
wget --quiet -O - https://remnux.org/get-remnux.sh | sudo bash
```

SIFT Workstation How-Tos

- SANS DFIR Posters and Cheat Sheets
- SIFT Documentation Project
- How To Mount a Disk Image In Read-Only Mode
- How To Create a Filesystem and Registry Timeline
- How To Create a Super Timeline
- SIFT Workstation YouTube Series
- FOR508 - Advanced Incident Response

Report Bugs

As with any release, there will be bugs and requests, please report all issues and bugs to the following website and location.

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

SIFT Recommendations

SIFT workstation is playing an important role for the Brazilian national prosecution office, especially due to Brazilian government budgetary constraints. Its incident response and forensic capabilities are bundled on a way that allows an investigation to be conducted much faster than it would take if not having the right programs grouped on such great Linux distribution. The new version, which will be bootable, will be even more helpful. I'd highly recommend SIFT for government agencies or other companies as a first alternative, for acquisition and analysis, from the pricey forensics software available on the market.

- Marcelo Caiado, M.Sc., CISSP, GCFA, EnCE

What I like the best about SIFT is that my forensic analysis is not limited because of only being ableto run an incident response or forensic tool on a specific host operating system. With the SIFT VM Appliance, I can create snapshots to avoid cross-contamination of evidence from case to case, and easily manage system and AV updates to the host OS on my forensic workstation. Not to mention, being able to mount forensic images and share them as read-only with my host OS, where I can run other forensic tools to parse data, stream-lining the forensic examination process.

- Brad Garnett www.digitalforensicsource.com

Latest Blog Posts

SANS CTI Summit & Training Twitter Contest
January 08, 2016 - 12:12 PM

DFIR Summit 2016 - Call for Papers Now Open
November 16, 2015 - 8:19 PM

SANS ThreatConnect DFIR Threat Intelligence Sharing Community Announced
October 07, 2015 - 2:08 PM

Latest Tweets @sansforensics

Tomorrow at 3pm EST @DavidJBianco presents Intelligent Intel [...]
January 11, 2016 - 8:03 PM

Two days left to save $400 at #SANSMcLean. Register here https://t.co/wtMIKBhXwD
January 11, 2016 - 7:15 PM

Blog by @MalwareJake: Former Yandex Employee Tries to sell s [...]
January 11, 2016 - 6:18 PM

Latest Papers

Investigative Forensic Workflow-based Case Study for Vectra and Cyphort
By Jennifer Mellone

On the x86 Representation of Object Oriented Programming Concepts for Reverse Engineers
By Jason Batchelor

On the x86 Representation of Object Oriented Programming Concepts for Reverse Engineers
By Jason Batchelor

"Rob has insight that few others have and that alone is worth the cost of the the course."
- Chris Spurrier, Xerox Corp

"I had taken several other forensic courses prior to this one, but none of them or their instructors made understanding forensic methodologies and techniques as clear and understandable as Rob Lee and this course has."
- Nathon Heck, Purdue

"A great course on timeline, registry, and restore point forensics. SANS is continuing to be the leader on teaching new techniques happening with forensics."
- Brad Garnett, Gibson County Sherrif's Dept.

Community | Training | Certification | Instructors | About