SIFT Workstation

The SIFT Workstation is a collection of free and open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings. It can match any current incident response and forensic tool suite. SIFT demonstrates that advanced incident response capabilities and deep-dive digital forensic techniques can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

By Rob Lee

Option 1: SIFT Workstation VM Appliance

Click the 'Login to Download' button and input (or create) your SANS Portal account credentials to download the virtual machine. Once you have booted the virtual machine, use the credentials below

- Hash Values
  - MD5: 6d82c7287e15ecc0c4f90f74d629e282
  - SHA256: fb7c343e65c21d0ff5591957f7a1890b1eaf76acd20f31de619ea6c5c7e4dcf2

Having trouble downloading SIFT?

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

Option 2A: SIFT Easy Installation on Native Ubuntu System

1. Download Ubuntu 22.04 ISO file and install Ubuntu 22.04 on any system - http://www.ubuntu.com/download/desktop

2. Install the Latest Cast Binary from its release page

3. Run '**sudo cast install teamdfir/sift**' to install the latest version of SIFT

4. Congrats -- you now have a SIFT workstation!

1. Login = **sansforensics**

2. Password = **forensics**

3. $ **sudo su -**

1. Use to elevate privileges to root while mounting disk images.

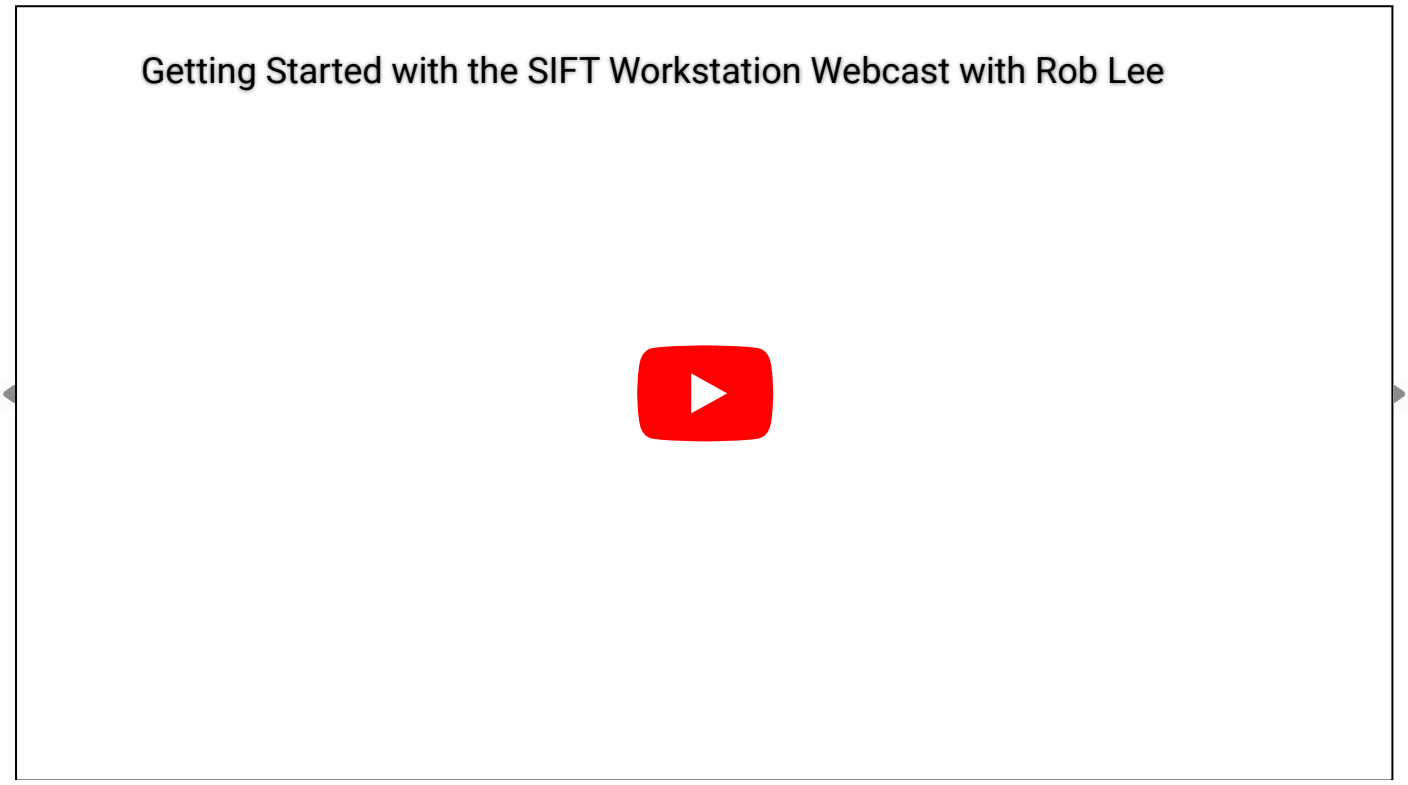
Option 2B: SIFT Easy Installation on Microsoft Windows using Windows Subsystem for Linux

1. Install Windows Subsystem for Linux (WSL) according to Microsoft's latest guidance, currently located at https://docs.microsoft.com/en-us/windows/wsl/install-win10 . The SIFT distribution can be installed on either WSL version 1 or version 2.

1. Choose Ubuntu 22.04 during the WSL installation process

4. Run '**sudo cast install --mode=server teamdfir/sift-saltstack**' to install the latest version of SIFT in WSL

5. Congrats -- you now have a SIFT Workstation in Windows!



Why SIFT?

The SIFT Workstation is a collection of free and open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings. It can match any current incident response and forensic tool suite. SIFT demonstrates that advanced incident response capabilities and deep-dive digital forensic techniques can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

Rob Lee created the original SIFT Workstation in 2007 to support forensic analysis in the SANS FOR508 class. Over the years, he and a small team have continually updated the SIFT Workstation for use in class, as well as for the wider community as a public resource. With over 125,000 downloads to date, the SIFT Workstation continues to be one of the most popular open-source incident-response and digital forensic offerings available.

Offered as an open source and free project, the SIFT Workstation is used in the following incident response courses at SANS:

- Advanced Incident Response course (FOR508)
- Advanced Network Forensics course (FOR572)
- Cyber Threat Intelligence (FOR578)
- Enterprise-Class Incident Response & Threat Hunting Course (FOR608)

"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."

"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, who has run countless cases supporting a variety of forensic and incident response priorities.

Key new SIFT Workstation features include:

- Ubuntu LTS 20.04 Base
- 64-bit base system
- Better memory utilization
- Auto-DFIR package update and customizations
- Latest forensic tools and techniques
- VM Appliance ready to tackle forensics
- Cross compatibility between Linux and Windows
- Option to install/upgrade stand-alone system via SIFT-CLI installer
- Expanded Filesystem Support

SIFT Workstation Capabilities

A key tool during incident response, helping incident responders identify and contain advanced threat groups. The SIFT provides robust capabilities for analyzing file systems, network evidence, memory images, and more.

- swap (Swap Space)
- memory (RAM Data)
- fat12 (FAT12)
- fat16 (FAT16)
- fat32 (FAT32)
- ext2 (EXT2)
- ext3 (EXT3)
- ext4 (EXT4)
- ufs1 (UFS1)
- ufs2 (UFS2)

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 - mount 001 image/split images to view single raw file and metadata
- split ewf (Split E01 files) via mount_ewf.py
- mount_ewf.py - mount E01 image/split images to view single raw file and metadata
- ewfmount - mount E01 images/split images to view single raw file and metadata
- vmdk
- vhd/vhdx
- qcow

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

Software Includes:

- Plaso/log2timeline (Timeline Generation Tool)
- Rekall Framework (Memory Analysis)
- Volatility Framework (Memory Analysis)
- 3rd Party Volatility Plugins
- bulk_extractor
- afflib
- afflib-tools
- ClamAV
- dc3dd

- libewf-python
- libfvde
- libvshadow
- lightgrep
- Qemu
- regripper and plugins
- SleuthKit
- Hundreds of additional tools

SIFT Workstation and REMnux Compatibility

REMnux® is a Linux toolkit for reverse-engineering and analyzing malicious software. REMnux provides a curated collection of free tools created by the community. Analysts can use it to investigate malware without having to find, install, and configure the tools. REMnux is used in SANS FOR610: Reverse Engineering Malware.

REMnux can be added into a SIFT Workstation installation. To install REMnux, first install the SIFT Workstation using the instructions found above. Then, follow these instructions to add the REMnux components .

SIFT Workstation How-Tos and Resources

- SANS DFIR Posters and Cheat Sheets
- 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

Reporting Issues

Please report all issues, bugs, and feature requests to the GitHub project page, located here:

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

SIFT Workstation Testimonials

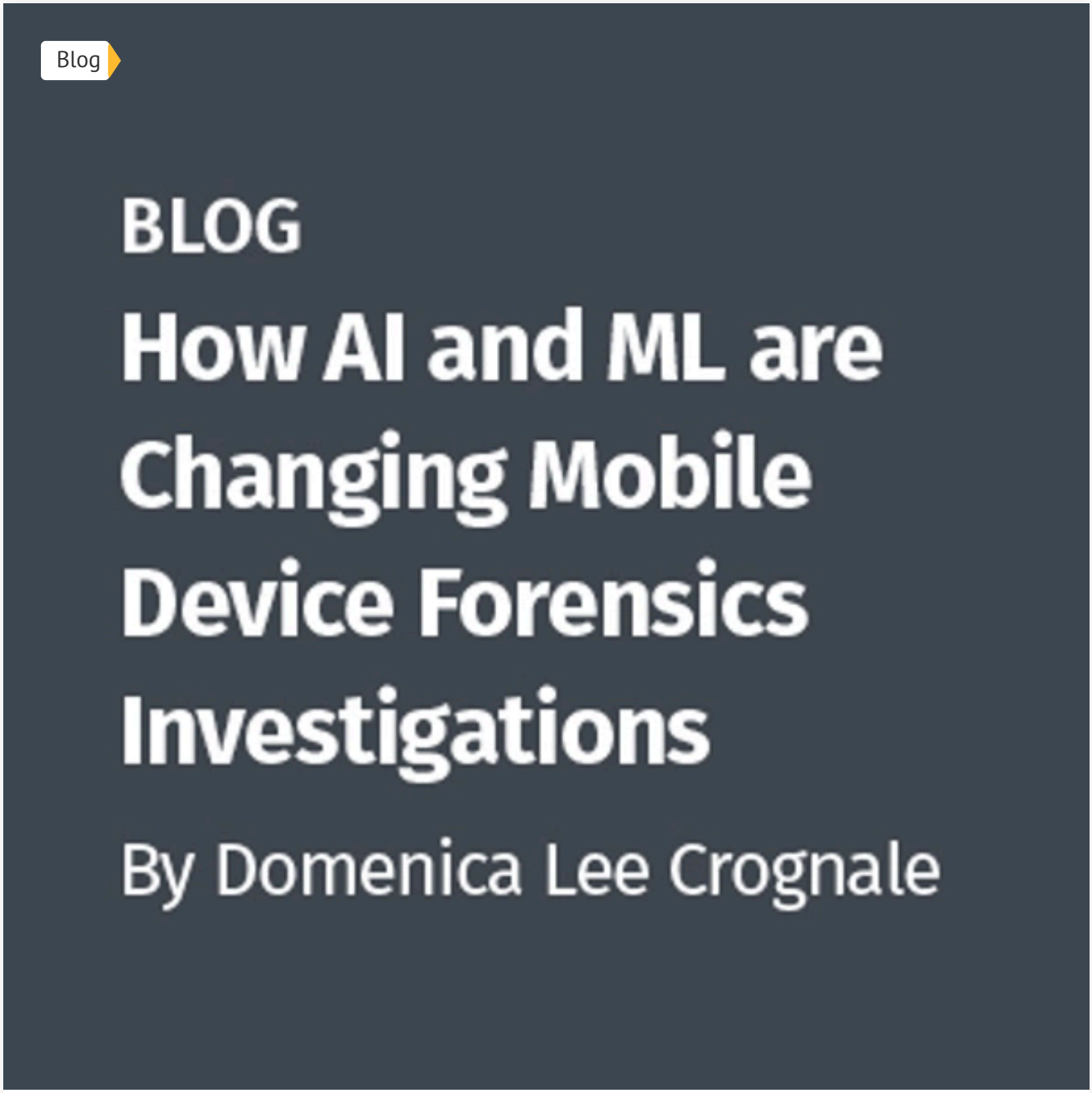
SIFT workstation is playing an essential role for the Brazilian national prosecution office, especially due to Brazilian government budgetary constraints. Its incident response and forensic capabilities

- 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 able to 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

Related Content



Digital Forensics, Incident Response & Threat Hunting May 3, 2024

How AI and ML are Changing Mobile Device Forensics Investigations

One of the biggest challenges with AI comes with determining whether the artifact in question was generated by a human behind the keyboard or by AI.

Domenica Crognale

Digital Forensics, Incident Response & Threat Hunting April 26, 2024

Spring 2024 Update: Explore the Latest Enhancements to SANS FOR585: Smartphone Forensic Analysis In-Depth

We are excited to announce the latest update to the SANS Institute's FOR585: Smartphone Forensic Analysis In-Depth!

Heather Mahalik Barnhart

Industrial Control Systems Security, Digital Forensics, Incident Response & Threat Hunting

April 9, 2024

The Quest to Summit | SANS ICS Security Summit 2024

Register for the ICS Security Summit to be able to participate in The Quest to Summit and win big prizes.

Tim Conway

Industrial Control Systems

Offensive Operations