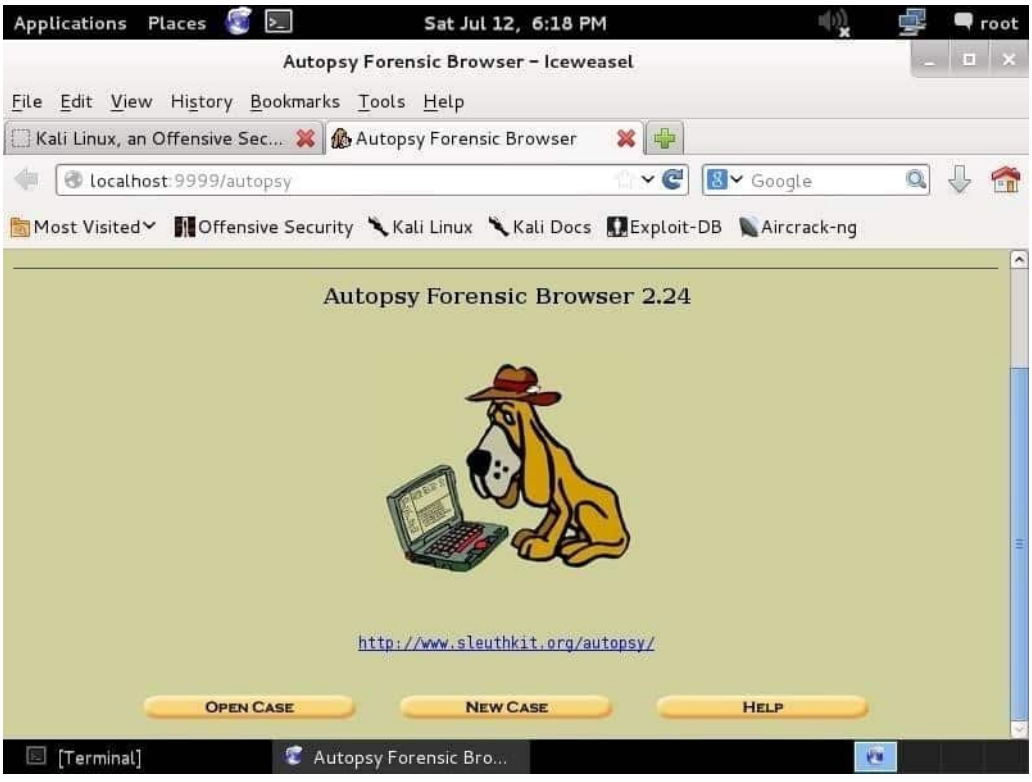
Sans Investigative Forensics Toolkit (SIFT)

By *Roy Schestowitz*
Created *30/06/2020 - 9:36pm*
Submitted by Roy Schestowitz on Tuesday 30th of June 2020 09:36:15 PM Filed under GNU [1] Linux [2]



SIFT is a computer forensics distribution created by the SANS Forensics team for performing digital forensics. This distro includes most tools required for digital forensics analysis and incident response examinations. SIFT is open-source and publicly available for free on the internet. In today?s digital world, where crimes are committed every day using digital technology, attackers are becoming more and more stealthy and sophisticated. This can cause companies to lose important data, with millions of users exposed. Protecting your organization from these attacks requires strong forensic techniques and knowledge in your defense strategy. SIFT provides forensic tools for file systems, memory and network investigations to perform in-depth forensic investigations.

In 2007, SIFT was available for download and was hard coded, so whenever an update arrived, users had to download the newer version. With further innovation in 2014, SIFT became available as a robust package on Ubuntu, and can now be downloaded as a workstation. Later, in 2017, a version of SIFT came to market allowing greater functionality and providing users the ability to leverage data from other sources. This newer version contains more than 200 tools from third parties, and contains a package manager requiring users to type only one command to install a package. This version is more stable, more efficient, and provides better functionality in terms of memory analysis. SIFT is scriptable, meaning that users can combine certain commands to make it work according to their needs.

SIFT can run on any system running on Ubuntu or Windows OS. SIFT supports various evidence formats, including AFF, E01, and raw format (DD). Memory forensics images are also compatible with SIFT. For file systems, SIFT supports ext2, ext3 for linux, HFS for Mac and FAT, V-FAT, MS-DOS, and NTFS for Windows.

[3]

GNU Linux

Links:
[1] http://www.tuxmachines.org/taxonomy/term/144
[2] http://www.tuxmachines.org/taxonomy/term/63
[3] https://linuxhint.com/sans_investigative_forensics_toolkit/