Linux Incident Response - Making TSK work on XFS

Taz Wake | Halkyn Consulting Ltd | Originally published 2023-11-22

Aug 2024 Edit notes

The steps here work on versions of Ubuntu up to, and including 22.04. This distro is supported until April 2027 but it is not the most recent version. On Ubuntu 24.04 and newer, there will be issues with the libraries required and it is generally not a good idea to install older (possibly vulnerable) libraries to get a tool working. For newer distros it is recommended that you build a docker container to run Ubuntu 22.04. This is a good stop-gap solution until a more permanent solution is available.

Introduction to The Sleuth Kit (TSK)

The Sleuth Kit (TSK) is a library and collection of utilities for forensic analysis of computer systems. Originally developed by Brian Carrier based on The Coroner's Toolkit, it has become the official successor platform. TSK is designed for Unix- and Windows-based systems, facilitating the extraction of data from disk drives and other storage media. This open-source collection, protected by GPL, CPL, and IPL, serves as the foundation for Autopsy, a graphical interface that enhances the usability of TSK's command-line utilities.

TSK allows you to parse various file systems like NTFS, FAT/ExFAT, UFS, Ext2/3/4, HFS, ISO 9660, and YAFFS2. It can analyse these file systems within disk images stored in formats like raw (dd), Expert Witness, or AFF. TSK can be used to examine systems running Microsoft Windows, Apple Macintosh OSX, many Linux distributions, and some UNIX computers. It offers command line tools or can be embedded as a library in other digital forensic tools such as Autopsy or log2timeline/plaso.

One challenge is that TSK does **not** natively support the XFS filesystem.

Installing TSK with XFS Support on Ubuntu

To install a version of TSK that supports XFS file systems on an Ubuntu system, follow these steps:

1. **Clone the Fork with XFS Support**:

A fork of TSK supporting XFS has been developed, based on Silicon Graphics's XFS Filesystem Disk Structures 3rd Edition (June 2017). This version is compatible with Ubuntu 18.04 and has been tested with xfsprogs (v4.9.0). It currently supports fsstat and the allocated file extract function of tsk_recover. With some tweaking you can install this on more modern Ubuntu distros.

First, install dependencies and clone the repository to your system: (run as root or prefix commands with sudo)

2. **Compile and Install the Fork**:

Once cloned, compile and install the fork:

Now you should have a working version of The Sleuth Kit that can parse XFS filesystem evidence.

```
root@siftworkstation:/mnt/ewf# /opt/sleuthkit-xfs/tools/fstools/fsstat -f xfs -o 514048 ./ewf1
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: XFS
Volume Name:
Volume ID: 6f6fbcb-f4a5-4f1d-83fa-7ae8938b9ad
Version: V4,NLINK,ALIGN,DIRV2,LOGV2,EXTFLG,MOREBITS,ATTR2,LAZYSBCOUNT,PROJID32BIT
Features Compat: 0
Features Read-Only Compat: 0
Features Incompat: 0
CRC: 0

METADATA INFORMATION
--------------------------------------------
Allocated inode count : 0
Root Directory: 18446744073709551615
Free Inodes: 0
```

Running the forked version of TSK against an XFS image

Linking TSK Commands for Easy Use

To ensure seamless use of TSK commands from any directory, link the TSK binaries to **/usr/bin**. Assuming the binaries are installed in **/opt/sleuthkit-xfs/tools/fstools/**, you can quickly create symbolic links into **/usr/bin** with this command:

This allows you to execute TSK commands from any location, as long as /usr/bin is part of the user's path.

Staying Updated with Community Changes

Given that TSK and its forks are under active development, it is essential to stay updated with community changes:

- **Check GitHub Regularly**: Visit the Sleuth Kit's GitHub repository frequently to stay informed about new updates or pull requests related to XFS support.
- **Contribute to Testing and Debugging**: Engage in testing new versions and report any bugs or issues. Community collaboration is vital for the continuous improvement of the tool.

Summary

The Sleuth Kit, with its extended support for the XFS file system through community contributions, is a robust tool for forensic analysis. The process of installing and configuring the fork that supports XFS on Ubuntu systems enhances TSK's capabilities. By staying engaged with the community and contributing to the development process, users can ensure they are utilising a tool that is both comprehensive and current in its forensic capabilities.

Please note, however, that the version of TSK you have here (for XFS) will **not** provide the same functionality as the full, native, version.

About Halkyn Consulting

Halkyn Consulting Ltd is a UK-based security and risk management consultancy providing 24/7 incident response, digital forensics, threat hunting, virtual security leadership (vCISO) and security compliance support to organisations worldwide. We deliver clear, practical, vendor-independent advice based on real-world threats — no hype, no upsell.

More free security resources are available at www.halkynconsulting.co.uk/security-resources.

Web: www.halkynconsulting.co.uk | **Email:** info@halkynconsulting.co.uk | **Tel:** +44 1244 940858