

Linux: Restore permanently deleted data with Scalpel

Check GitHub for helpful DevOps tools:

Michael Robotics

Hi, I'm Michal. I'm a Robotics Engineer and DevOps enthusiast. My mission is to create skill-learning platform that combats information overload by adhering to the set of principles: simplify, prioritize, and execute.

 <https://github.com/MichaelRobotics>



Ask Personal AI Document assistant to learn interactively (FASTER)!

1


Download PDF

1

<https://github.com/MichaelRobotics/DevOpsTools/blob/main/LinuxScalpel.pdf>

2

Go to website

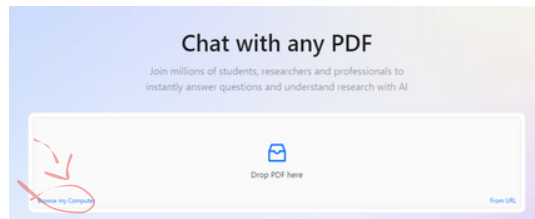
 | Click there to go to ChatPdf website

2

3

Browse file

3



4

Chat with Document

Ask questions about document!

4

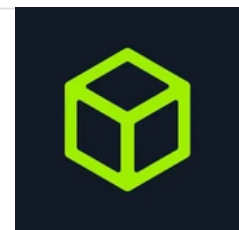
Completely new to Linux?

Essential for this PDF is a thorough knowledge of networking. I highly recommend the HTB platform's networking module, which offers extensive information to help build a comprehensive understanding.

HTB - Your Cyber Performance Center

We provide a human-first platform creating and maintaining high performing cybersecurity individuals and organizations.

 <https://www.hackthebox.com/>



What is Scalpel?

Scalpel is a powerful data recovery tool designed for Linux systems that specializes in recovering lost files from storage devices, such as hard drives. It scans the raw data on the disk to retrieve files that have been permanently deleted or lost.

How Scalpel works?

Scalpel operates by examining the file system for recognizable file signatures, allowing it to identify and extract deleted files even when they are no longer indexed in the directory. It uses a configuration file to specify which file types to search for, enhancing its efficiency in recovery.



Scalpel: Why and When

Scalpel is particularly useful when you need to recover accidentally deleted files or files lost due to corruption or formatting. It's ideal to use Scalpel immediately after realizing a file has been deleted, especially if you want to minimize the risk of data being overwritten.

For example, it can be invaluable in forensic investigations or data recovery scenarios where critical files have been lost.

System Requirements

- 8 gb ram
- 10 free gb storage
- ubuntu 22.04

If you want to install it on a different Linux distro, ask in the comments and I will write an Ansible playbook or bash script.

Scalpel: Main components & packages

- scalpel package

Scalpel: How to install

1) Installation

Scalpel is available in the default repositories for Ubuntu and Debian, so it can be installed using apt:

```
$ sudo apt update
```

```
$ sudo apt install scalpel
```

Verify Installation by checking version

```
$ scalpel -V
```

How to use Scalpel

Once installed, Scalpel requires a configuration file (usually located at **/etc/scalpel/scalpel.conf** or **/etc/scalpel.conf**) where you define which file types to carve based on their file signatures. You'll need to edit this file before running Scalpel.

When you open the configuration file, you'll see that everything is initially commented out with '#' symbols.

```
sudo nano /etc/scalpel/scalpel.conf
```

or

```
sudo nano /etc/scalpel.conf
```

Before running **Scalpel**, you have to uncomment the file formats you want to recover. However, uncommenting the entire file can be time-consuming and may lead to a lot of false results.

For example, if you only want to recover '.jpg' files, you can simply uncomment the '.jpg' file section in the Scalpel configuration file.

Now run the the following command in the terminal to search for deleted files.

```
sudo scalpel /path/to/target/directory
```

Once you run Scalpel on the directory, it will take time to recover your deleted file depending on the disk space that you are trying to scan and the speed of the machine.

Common troubleshooting

1) Scalpel Fails to Run or Command Not Found

Verify Installation: Ensure Scalpel is installed correctly by checking the version.

2) Permission Denied

Run with sudo: Scalpel requires elevated privileges to access raw devices or certain files. Use sudo to run Scalpel with administrative rights:

3) Scalpel.conf File Not Found or Misconfigured

Verify the Configuration File Location: The default location for the configuration file is `/etc/scalpel/scalpel.conf`. Ensure that this file exists and is properly configured. If not, you can copy the default config:

4) Check the man page

5) If everything is a complete mess

delete scalpel and install again

Scalpel: How to remove

1) Remove scalpel

As the first step, you need to remove scalpel:

```
$ sudo apt remove scalpel
```

2) Remove dependencies

Remove any unused dependencies: After uninstalling Scalpel, you can clean up any unused dependencies by running:

```
$ sudo apt autoremove
```

Learn more about Scalpel

Check Scalpel GitHub repo:

sleuthkit / scalpel

Scalpel is an open source data carving tool.



<https://github.com/sleuthkit/scalpel>



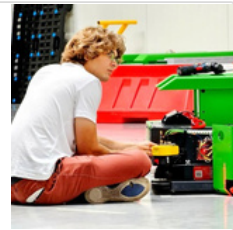
Share, comment, DM and check GitHub for scripts & playbooks created to automate process.

Check my GitHub

Michael Robotics

Hi, I'm Michal. I'm a Robotics Engineer and DevOps enthusiast. My mission is to create skill-learning platform that combats skill information overload by adhering to the set of principles: simplify, prioritize, and execute.

 <https://github.com/MichaelRobotics>



PS.

If you need a playbook or bash script to install KVM on a specific Linux distribution, feel free to ask me in the comments or send a direct message!