

# SIFT workstation



## context

dit document beschrijft de installatie van SIFT workstation, een analyse werkstation voor digital forensics.

## installatie

### old school

- installeer Ubuntu 20.04
- installeer de [SIFT-CLI](#)
  - Als je wat kort door de bocht wil gaan:
    - wget <https://github.com/teamdfir/sift-cli/releases/download/v1.13.1/sift-cli-linux>
    - apt-get update && apt-get autoremove
    - mv sift-cli-linux /usr/local/bin/sift && chmod 755 /usr/local/bin/sift
- installeer ahv sift install --mode=server
- alle bestanden/scripts komen onder /usr/local/bin

### Docker

- docker pull digitalsleuth/sift-remnux (ca 6Gb)
- docker create --name sift --hostname sift -p 22:22 -p 139:139 -p 445:445 digitalsleuth/sift-remnux
- docker run sift
- hiermee heb je Sift workstation, beschikbaar op tcp/22 en mogelijkheid om case bestanden via SMB te uploaden.
- verder:
  - apt-get install nmap smbclient
  - tridupdate
  - mkdir -p /shares/cases /shares/software
  - exporteer bovenstaande directory via SMB:

```
[cases]
comment = case files
```

```
browseable = no
path = /shares/cases
guest ok = no
read only = no
create mask = 660
directory mask = 770

[software]
comment = software
browseable = no
path = /shares/software
guest ok = no
read only = no
create mask = 660
directory mask = 770
```

## update

- bestaande sift versie bijwerken: `sift update`
- nieuwe (major) versie van sift upgraden: `sift upgrade`

## problemen, problemen

### logboeken

- `/var/cache/sift/cli/v2021.9.0/saltstack.log`  
geen timestamps. Slordig...

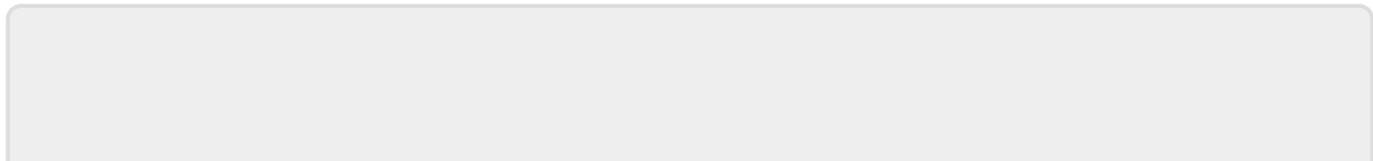
### meest geziene fouten

- problemen met installatie van packages waarbij apt system gelocked is of unhealthy.  
Doe dus steeds: `apt-get update && apt-get autoremove`

## meer info

- [brontekst](#)
- [cheatsheet](#)

[digital forensics, sift](#)



From:

<https://louslab.be/> - **Lou's lab**

Permanent link:

[https://louslab.be/doku.php?id=digital\\_forensics:sift\\_workstation](https://louslab.be/doku.php?id=digital_forensics:sift_workstation)

Last update: **2024/11/16 18:14**

