

## Access

User: ds4n6  
Password: forensics

## Anaconda Plugins

Ipywidgets, pandas-bokeh, pyarrow

## Forensic Tools

ds4n6\_lib, Sleuth Kit Tools (fls, mactime, mac-robber, etc), plaso, Volatility, RegRipper

## JupyterLab

Browser Access Port: 8888  
Token: Run Desktop Script

## TimeSketch

Browser Access Port: 80  
User: timesketch  
Password: timesketch  
Logs: /data/timesketch/logs/  
Add new user:  
\$ cd /opt/timesketch  
\$ sudo docker-compose exec timesketch-web tsctl add\_user --username <USERNAME>  
Services control:  
\$ sudo systemctl (status|start|stop) docker-compose-timesketch  
\$ sudo docker ps

## Installed Packages

ds4n6\_lib, Picatrix, TimeSketch, Jupyter, Anaconda3

## Jupyter Plugins

TOC, Collapsible Headings, jupyterlab-manager, ipynb, jupyterlab-favorites, osscar, /output\_auto\_scroll, gdown

## Demo Forensics Evidence (Optional)

Precooked data for Szechuan Sauce case, Magnet CTF 2019 and Ali Hadi User Policy Violation Case

## Picatrix

Browser Access Port: 8888  
Logs: /var/log/picatrix\_server/picatrix\_server.(out|err)  
Services Control:  
\$ sudo supervisorctl (status|start|stop) picatrix\_server  
TS Credentials: /home/ds4n6/.timesketchrc .timesketch.token

## Python Plugins

Timesketch-api-client, dill, untangle, qgrid, ipyaggrid, eland

## Other

Cheatsheets  
Preloaded notebooks for ds4n6\_lib

