

SIYASAT LINUX

presented by: [reconvillageph](#)



WHOAMI

```
$ man reconvillageph
```

```
RECONVILLAGEPH(1)      Manual pager utils      SIYASAT(1)
```

NAME

reconvillageph

SYNOPSIS

```
-O, --OSINT
-c, --CTI
-S, --SOCMINT
-s, --Social Engineering
-R, --Reconnaissance
-o, --OPSEC
```



WHAT IS

SIYASAT LINUX?



Siyasat Linux is a specialized distribution designed for Open Source Intelligence (OSINT) investigations, catering to the needs of threat intelligence analysts and other intelligence professionals. Built on the foundations of Debian 12, this provides a comprehensive suite of tools and customized environment to streamline your investigation workflows.



BUT WHY???



SIMILAR LINUX DISTRO

- tsurugi
- buscador
- csi linux
- tracelabs' osint vm



Our GOAL is to have something more customizable

- Open source
- use configuration management (SaltStack)



SALTSTACK??



- configuration management & orchestration tool
- used in DevOps, similar to Ansible



BUT WHY SALTSTACK?



- idempotency
- personal preference, while learning devops stuff
- inspired by REMNUX
- more structured and easier to maintain/troubleshoot



SHOW ME THE SOURCES!!!



Download VM:
<https://archive.org/details/reconvillageph-siyasat-linux>



TO DO:

- QubesOS integration
- Regular tools maintainance
- More install options.
 - user
 - customizations
 - Documentation
 - Workflows
- Trainings



DEMO TIME!

