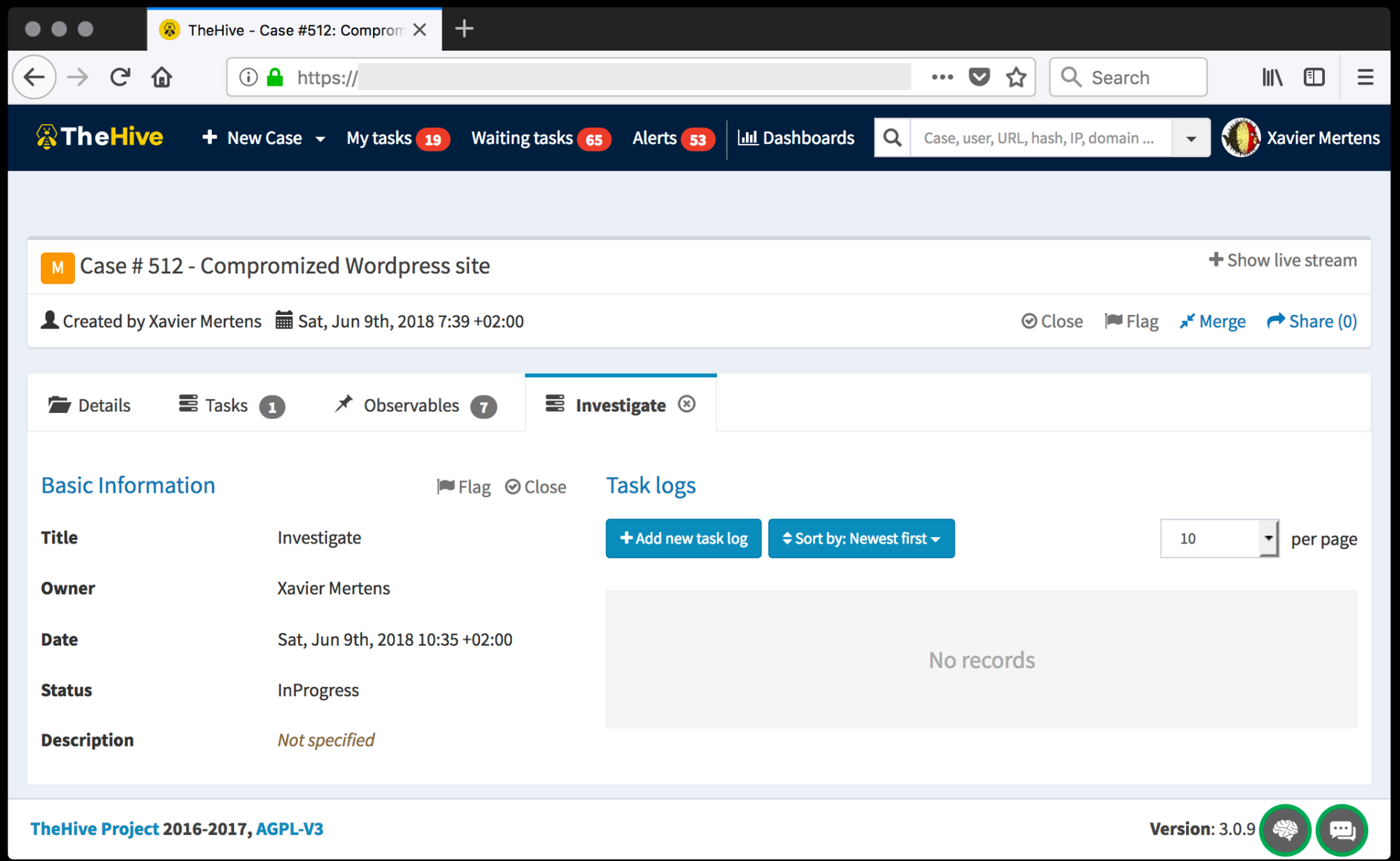
Feeding Your Bees

Imap2TheHive

TheHive in 30”

“Security Incident Response for the Masses”



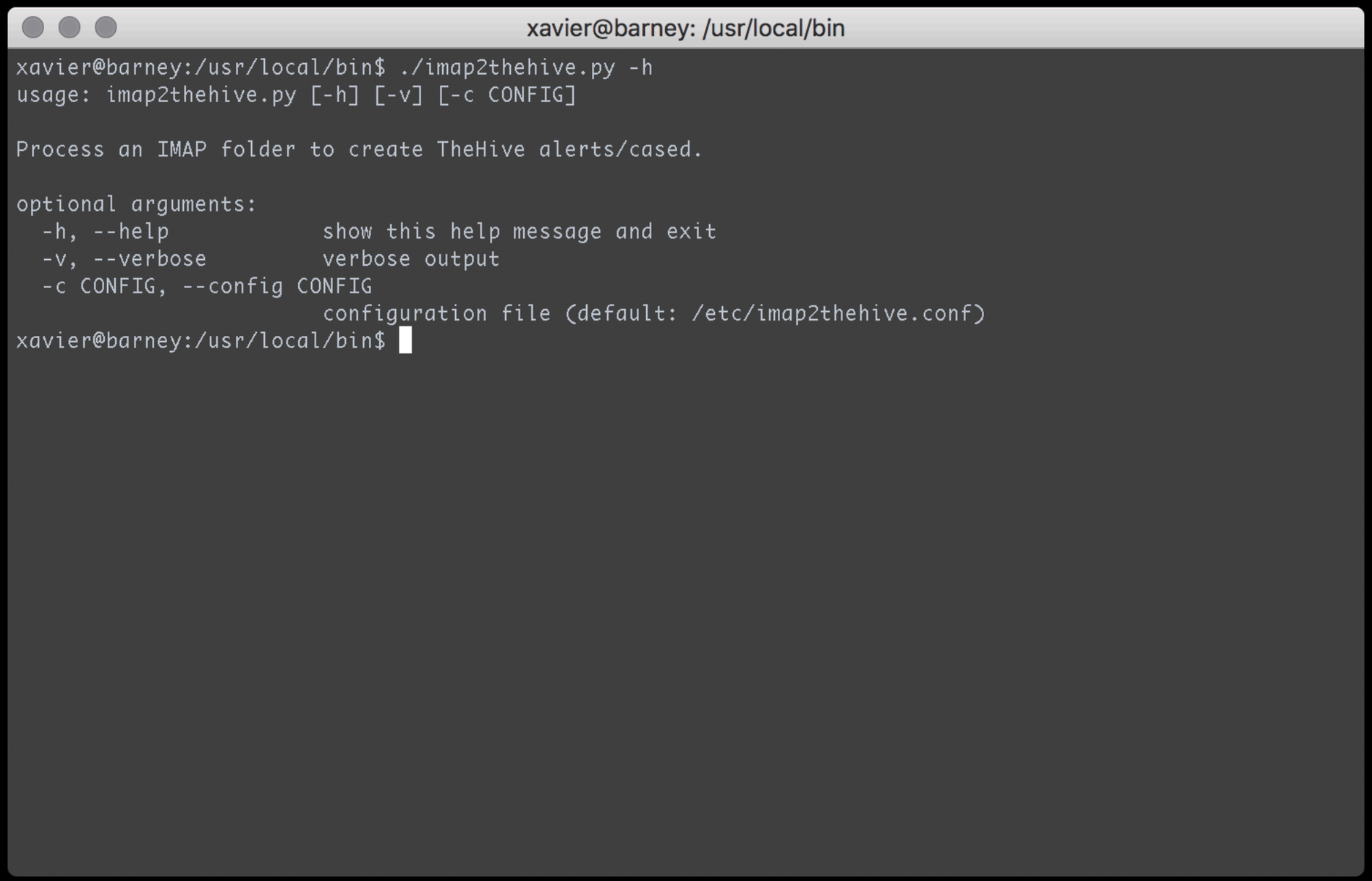
https://thehive-project.org/

Email’ll Never Die!

Email'll Never Die!

- OSSEC
- Splunk
- VTI
- Many many many home made hunting scripts

imap4thehive.py



imap4thehive.conf

xavier@barney: /usr/local/bin

```
xavier@barney:/usr/local/bin$ cat imap2thehive.conf
[imap]
host: [redacted]
port: 993
user: [redacted]
password: [redacted]
folder: incoming
expunge: false

[thehive]
url: http://127.0.0.1:9000
user: automation
password: [redacted]
observables: true
whitelists: /usr/local/bin/imap2thehive.whitelists

[alert]
tlp: 2
tags: email
keywords: \S*(ALERT|VTMIS|OSSEC)\S*

[case]
tlp: 2
tags: email
tasks: Investigation,Communication,Tracking
template: Default
#files: application/pdf
xavier@barney:/usr/local/bin$
```

Features

- Uses TheHive4Py
- Creates Cases/Alerts
- Creates Tasks or use a pre-defined profile
- Adds tags
- Extracts IOC’s and creates observables
- Supports IOC’s whitelist
- Predefined TLP level
- Adds attachment based on MIME types

What’s Next?

- Extracts custom fields via regex
  (ex: internal assets, user names, …)

- ???

https://blog.rootshell.be/2018/02/05/feeding-thehive-emails/
https://github.com/xme/dockers/tree/master/imap2thehive

@xme | xavier@rootshell.be