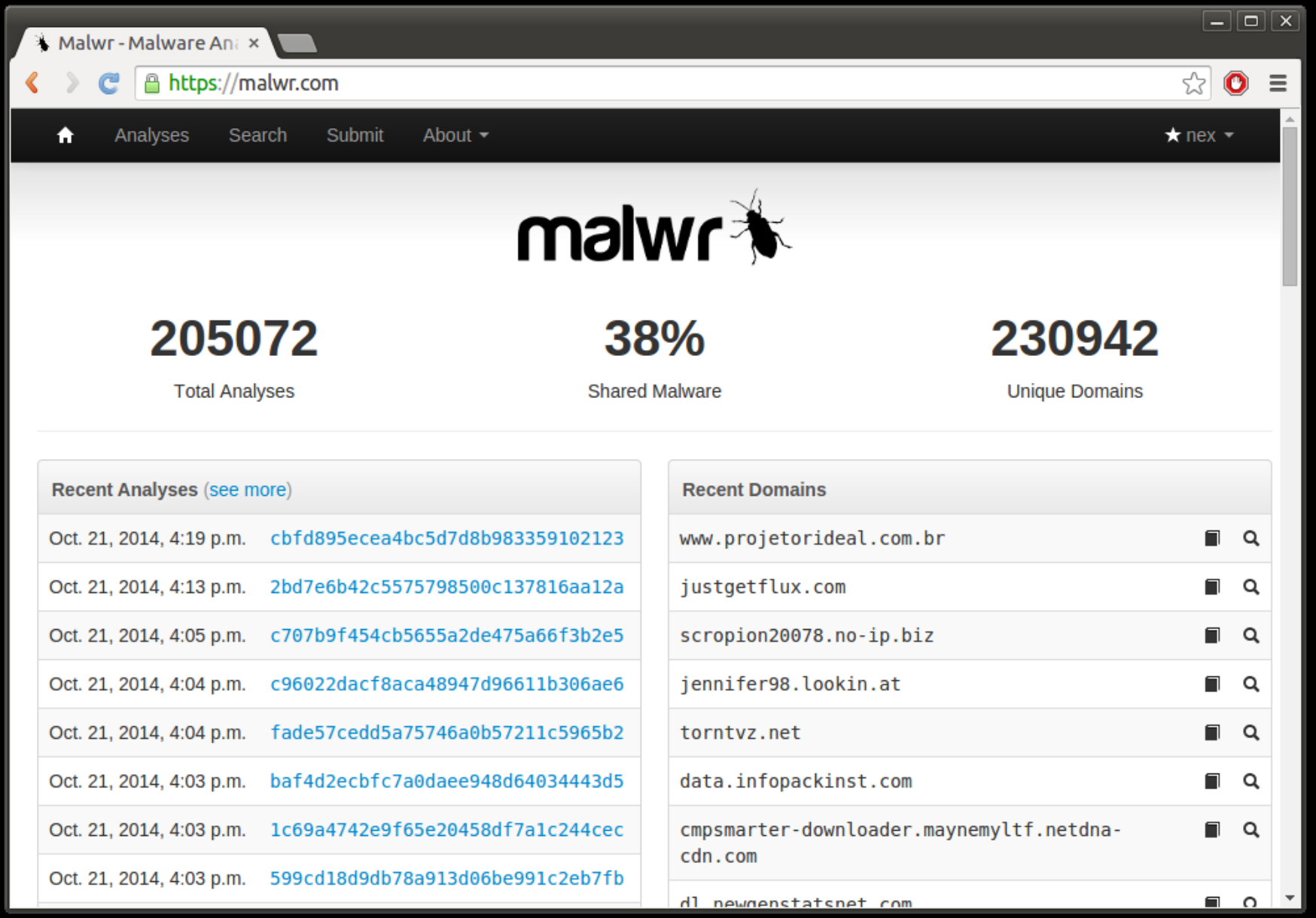
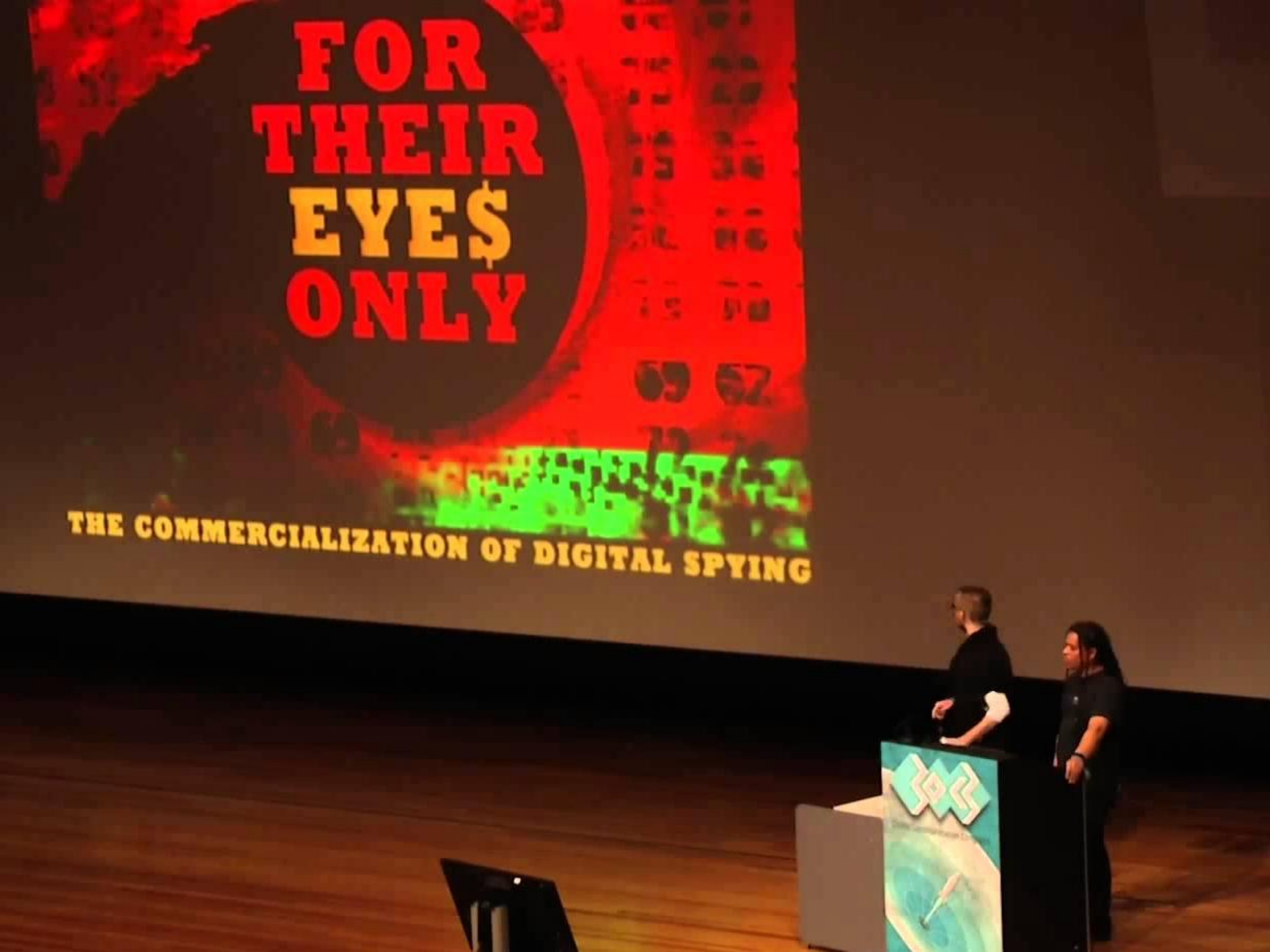
This is a kitten-free presentation, because snakes.

@botherder


I'M A
CUCKOO
DEVELOPER


Malwr - Malware An
https://malwr.com
Analyses
Search
Submit
About
nex
malwr
205072
Total Analyses
38%
Shared Malware
230942
Unique Domains
Recent Analyses (see more)
Oct. 21, 2014, 4:19 p.m. cbfd895ecea4bc5d7d8b983359102123
Oct. 21, 2014, 4:13 p.m. 2bd7e6b42c5575798500c137816aa12a
Oct. 21, 2014, 4:05 p.m. c707b9f454cb5655a2de475a66f3b2e5
Oct. 21, 2014, 4:04 p.m. c96022dacf8aca48947d96611b306ae6
Oct. 21, 2014, 4:04 p.m. fade57cedd5a75746a0b57211c5965b2
Oct. 21, 2014, 4:03 p.m. baf4d2ecbfc7a0daee948d64034443d5
Oct. 21, 2014, 4:03 p.m. 1c69a4742e9f65e20458df7a1c244cec
Oct. 21, 2014, 4:03 p.m. 599cd18d9db78a913d06be991c2eb7fb
Recent Domains
www.projetorideal.com.br
justgetflux.com
scropion20078.no-ip.biz
jennifer98.lookin.at
torntvz.net
data.infopackinst.com
cmpsmarter-downloader.maynemyltf.netdna-cdn.com


FOR
THEIR
EYE$
ONLY
THE COMMERCIALIZATION OF DIGITAL SPYING

Those exploit guys

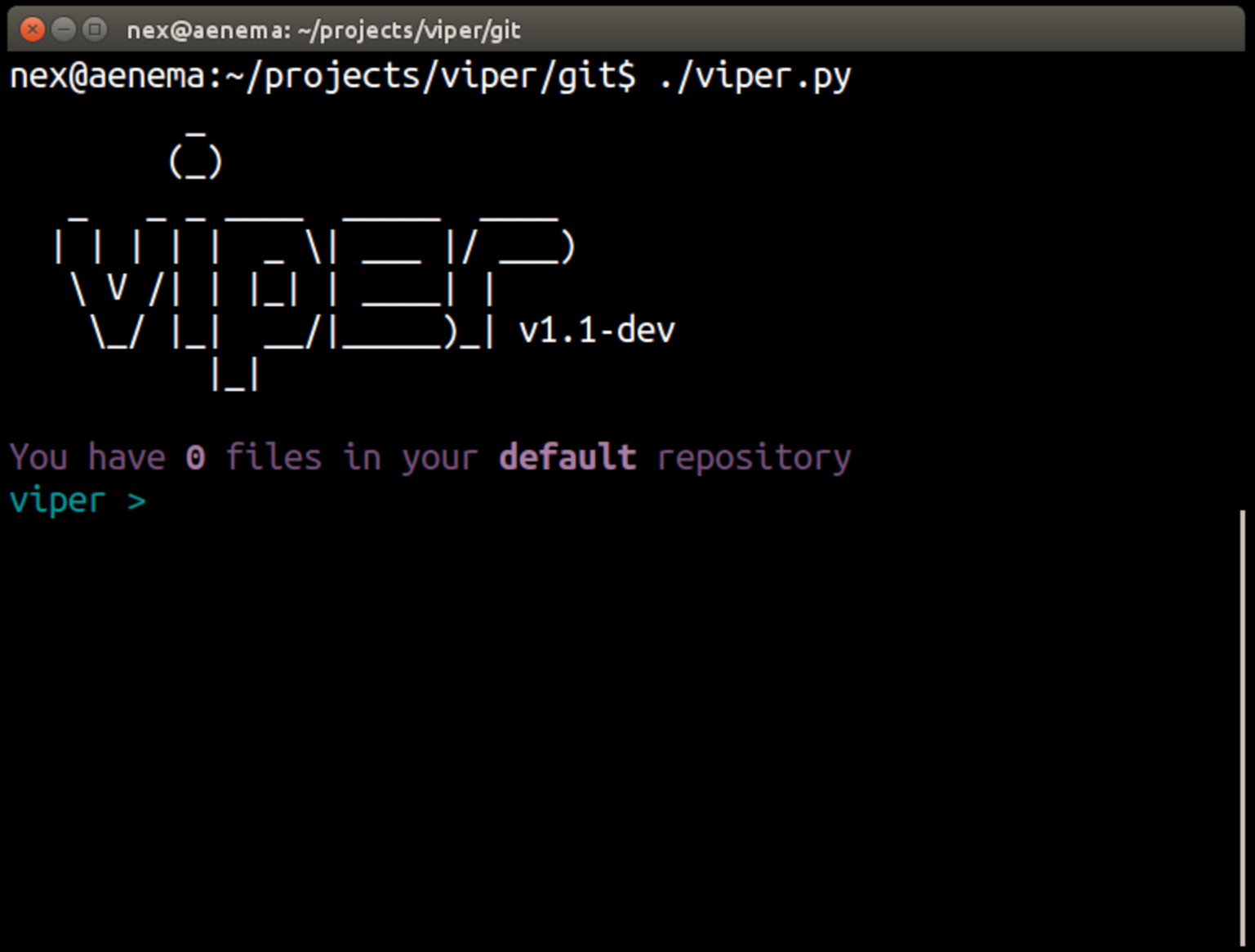
- Exploits started accumulating
- Written in many different languages
- Everyone kind of hacked their own framework
- Some commercial ones popped up early 2000s
- HD Moore figured it out and started Metasploit

10 years later

- Malware samples all over the place
  - Forgetting what they are
- Analysis scripts all over the place
  - Hard to maintain coherently
  - Hard to integrate them
  - Lots of redundancy and re-engineering
  - Many just suck ass

VxCage

- First attempt at making sense of my filesystem
- Quickly realized its shortcomings
- Was never a finished project
- I never made a pretty logo for it
  - FAILED


nex@aenema: ~/projects/viper/git
nex@aenema:~/projects/viper/git$ ./viper.py
v1.1-dev
You have 0 files in your default repository
viper >

Why did I start Viper?

- Cause I was tired of being the Cuckoo Guy
- Cause I was tired of being the FinFisher Guy
- Cause “the Viper Guy” sounds a lot cooler
- And in the end marginally cause I think it could be useful to some

What's that

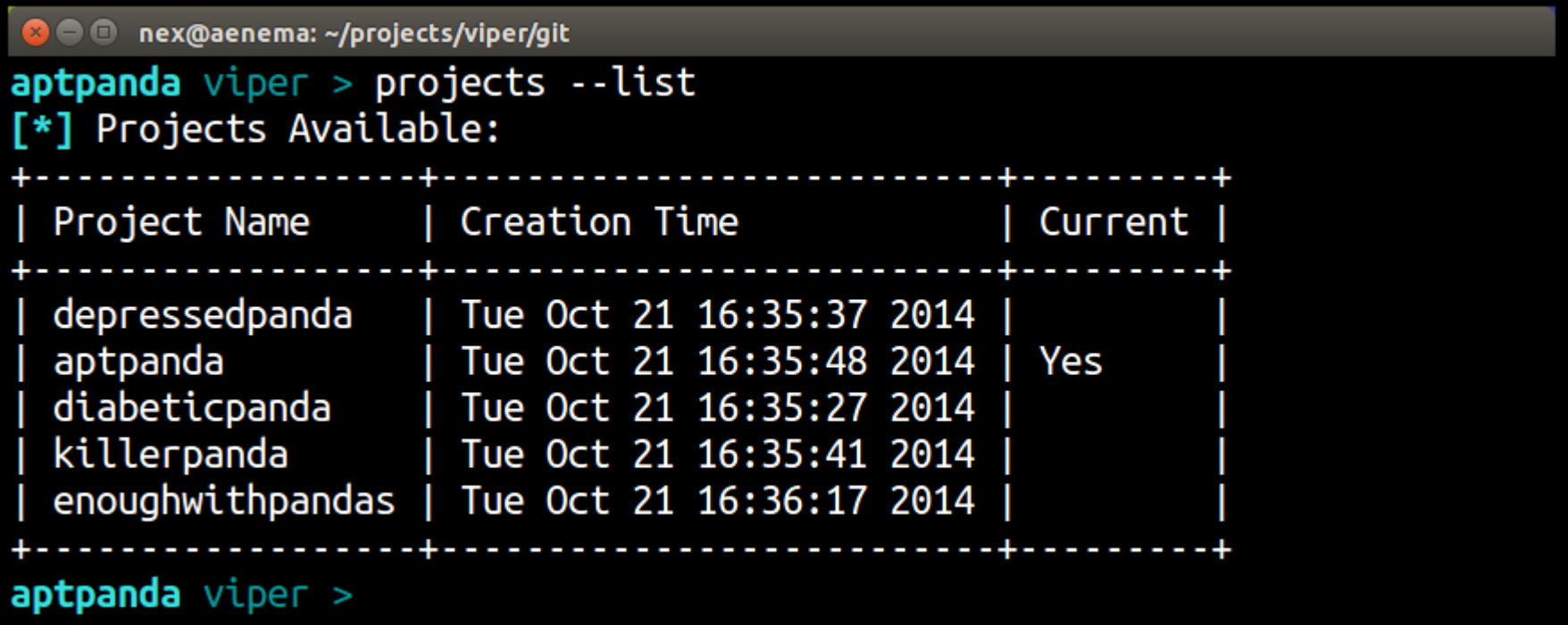
- It's a framework, release as BSD 3-Clause
- You can store and organize your samples
- It provides analysis modules to inspect your samples
- It provides an easy interface to create new modules
- Right now just a shell, other UIs are possible
  - Ok well, there's REST API

Structure

- File repository
- Database
  - Metadata on samples
  - Notes, Tags, etc.
- Shell history file
- Core commands
- Modules
  - About 30 now

Projects

- Separate repository
- Separate SQLite database
- Separate command history file

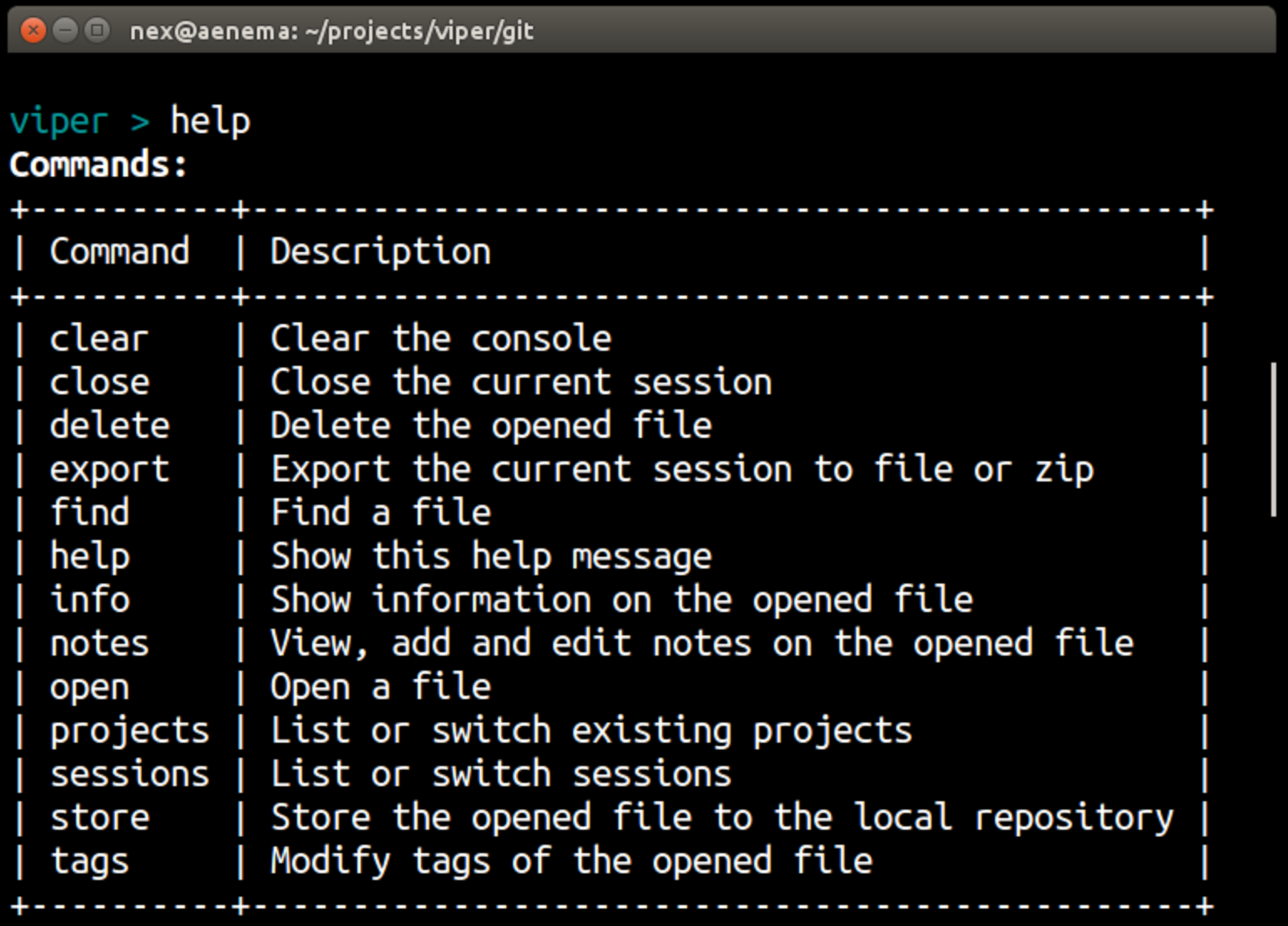


Sessions

- Currently opened file
- Previously opened files
- Modules can interact with them

nex@aenema: ~/projects/viper/git

```
hackingteam viper rcs_saudi.exe > sessions -l
[*] Opened Sessions:
+---+--------------------+----------------------------------+---------------------+---------+
| # | Name               | MD5                              | Created At          | Current |
+---+--------------------+----------------------------------+---------------------+---------+
| 1 | rcs_lebanon.exe    | 018cffa519af0ad1b5126b85e88071ac | 2014-10-21 16:44:18 |         |
| 2 | rcs_italy.exe      | cb8259668b17059f1078227995aad4c2 | 2014-10-21 16:44:19 |         |
| 3 | rcs_uzbekistan.exe | c18ec79c933d8dec08c92de1139d9972 | 2014-10-21 16:44:20 |         |
| 4 | rcs_kazakhstan.exe | 9c223cdebbd6870115a530869491a7a9 | 2014-10-21 16:44:27 |         |
| 5 | rcs_saudi.exe      | 1e71cbf364fd05168a9ccaf435eb66e8 | 2014-10-21 16:44:32 | Yes     |
+---+--------------------+----------------------------------+---------------------+---------+
hackingteam viper rcs_saudi.exe >
```


nex@aenema: ~/projects/viper/git
viper > help
Commands:
Command	Description
clear	Clear the console
close	Close the current session
delete	Delete the opened file
export	Export the current session to file or zip
find	Find a file
help	Show this help message
info	Show information on the opened file
notes	View, add and edit notes on the opened file
open	Open a file
projects	List or switch existing projects
sessions	List or switch sessions
store	Store the opened file to the local repository
tags	Modify tags of the opened file

Sort all the samples

- Divide samples across thematic projects
- You can tag samples and search for them
- You can add notes to samples and search for them
- You can add Yara signatures and make Viper automatically classify and tag samples

Modules

- They’re what makes Viper powerful
- Python modules
- They are loaded dynamically from *modules/*
- They can do pretty much anything
  - Interact and alter the database
  - Interact and alter sessions
- Generally perform parsing and analysis of specific file formats

Current modules

- apk
- clamav
- cuckoo
- debup
- editdistance
- elf
- email
- exif
- fuzzy
- html
- ida
- idx
- image
- jar
- office
- pdf
- pe
- r2
- rat
- reports
- shellcode
- strings
- swf
- virustotal
- xor
- yara

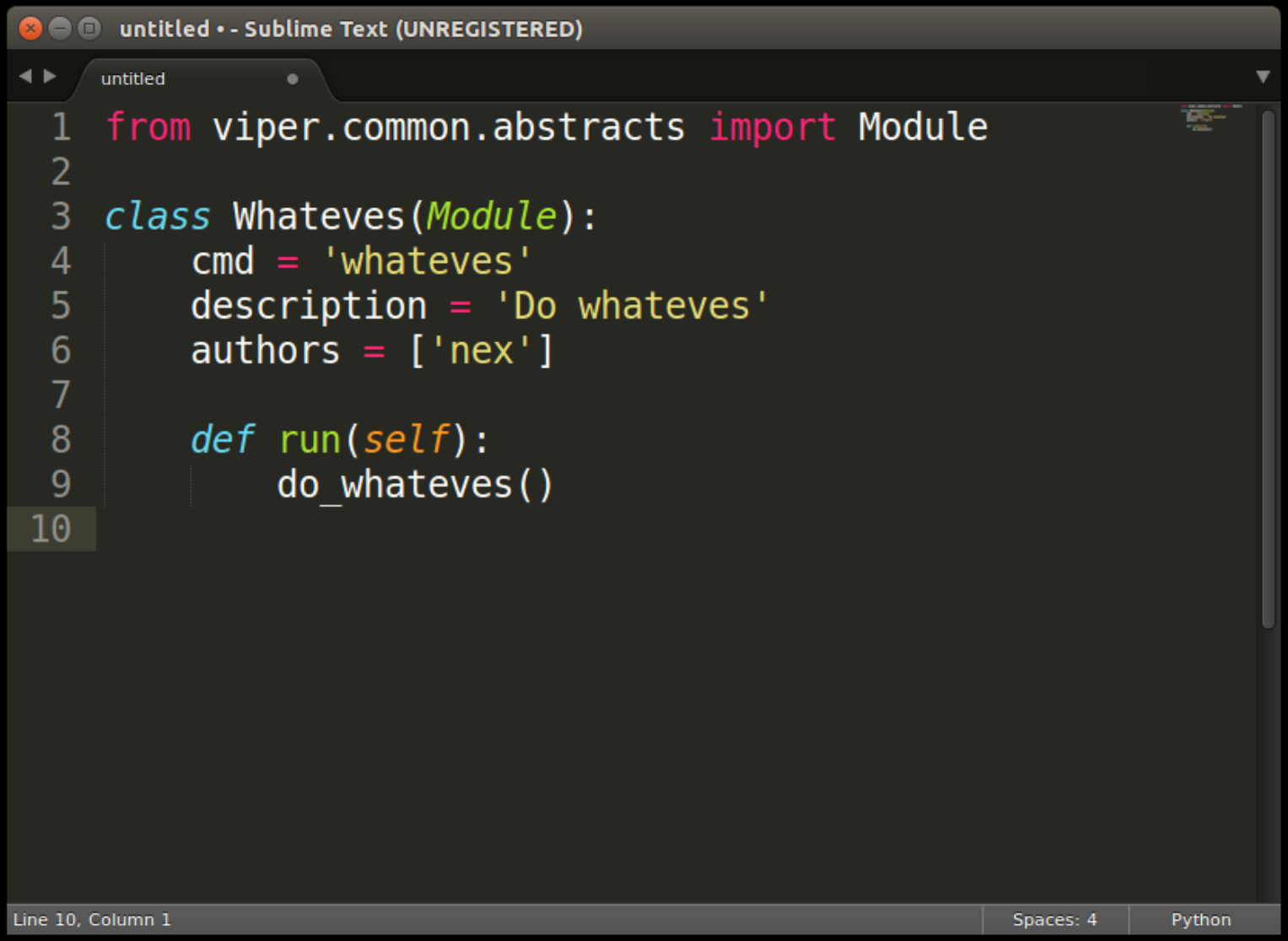
Current modules

- apk
- clamav
- cuckoo
- debup
- editdistance
- elf
- **email**
- exif
- fuzzy
- html
- ida
- idx
- image
- jar
- **office**
- **pdf**
- **pe**
- r2
- **rat**
- reports
- shellcode
- strings
- swf
- virustotal
- xor
- **yara**

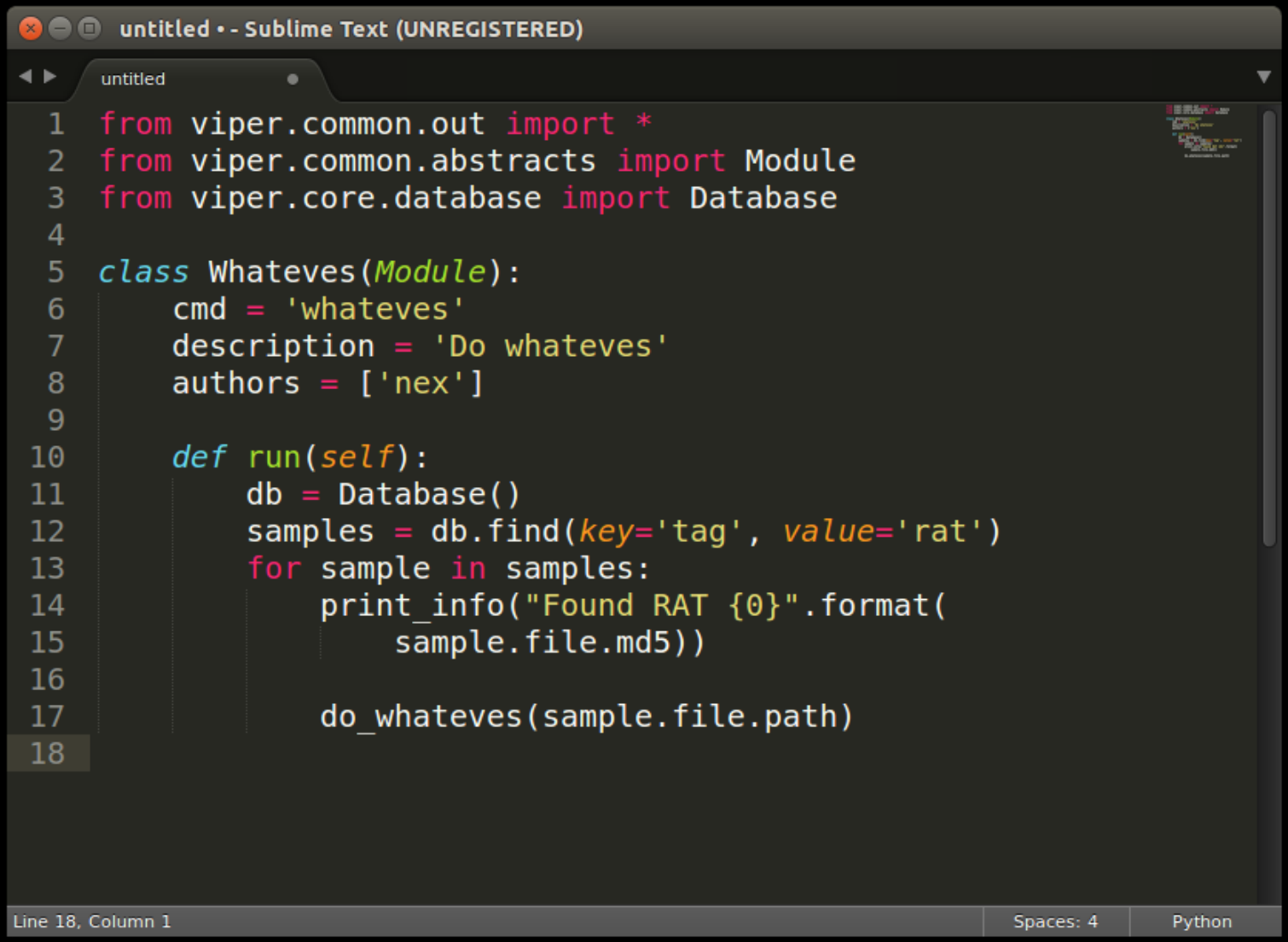
Philosophy

- Analyze file formats
- Cluster your collection files
- Find files with similar properties to the one you're analyzing
- Interact with other tools and security systems

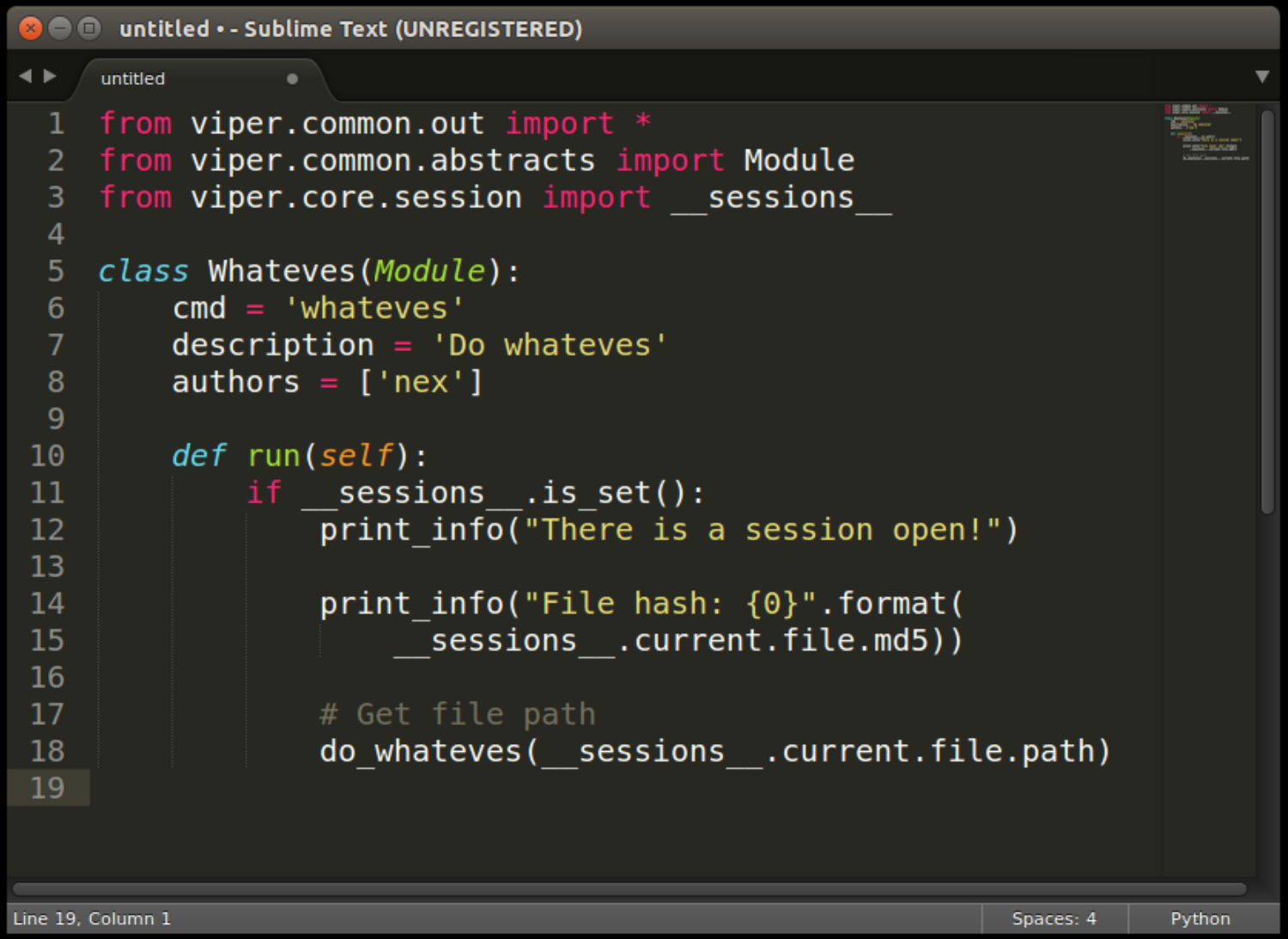
Module Skeleton



Interact with Database



Interact with Sessions



Shall we create a module right now?

What’s to be done?

- Some modules are incomplete
- There’s plenty of missing analysis features
- Yara support is great, but needs ordering
- Scripting and automating?
- Store command results in a database

Contribute

- This is not MY project, it's a community project
  - Without contributions it will never be successful
  - I come up with decent ideas I leave up to others to make actually work
- Join *###viper* on FreeNode
- Send Pull Requests and pester me on IRC
- Looking for developers!

Thanks to

- Kevin Breen
- Mariano Graziano
- Alessandro Tanasi
- Mark Schloesser
- Jurriaan Bremer
- Morgan Marquis-Boire
- Felix Leder
- Tillmann Werner
- Citizen Lab
- Everybody contributing to the project


Questions?
nex@nex.sx
0521 6F3B 8684 8A30 3C2F E37D D166 F166 7359 D880
SOME SHIT IS ABOUT TO GO DOWN