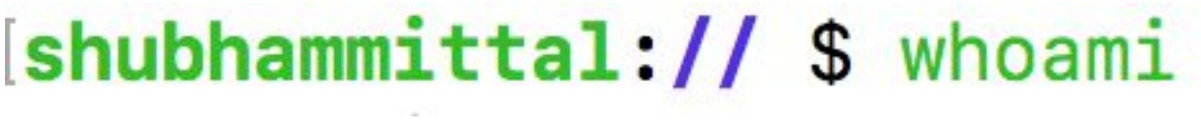
DataSploit

Open Source Assistant for #OSINT

https://github.com/datasploit/datasploit

http://datasploit.info | @datasploit



```
[shubhammittal:// $ whoami
```

- Just another Pen-tester.
- Security Consultant @ NotSoSecure
- 5+ Years of Experience

- Twitter - @upgoingstar
- Email - upgoingstaar@gmail.com

What’s DataSploit?

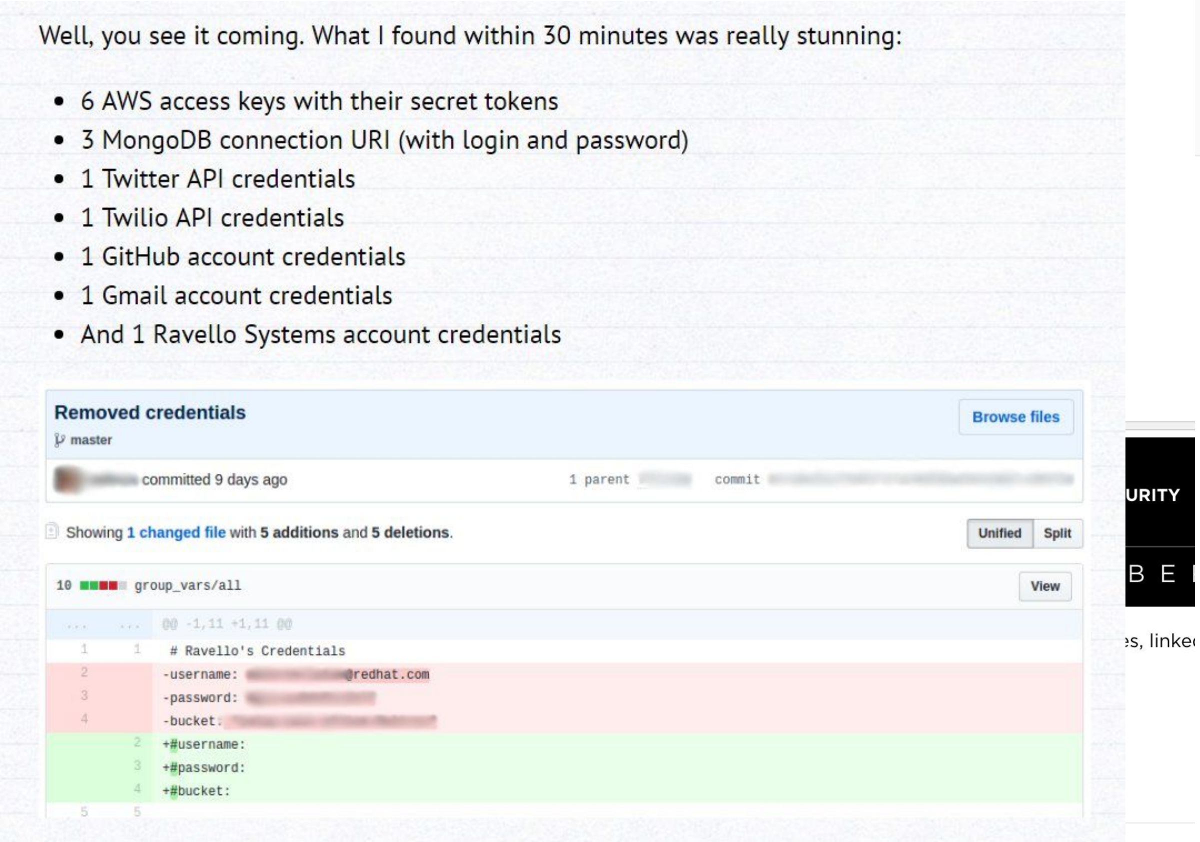
- Automated OSINT Tool for Domain / Email / Username / IP Addresses
- Fetches information from multiple HIDDEN sources.
- Works in passive mode.
- Written in Python.
- Multiple report formats available.

- Customized for Pen-testers / Product Security Guys / Cyber Investigators.

Why DataSploit?

- So much data.
  - Server’s Username / Passwords
  - Address
  - Email Id
  - Phone Number
  - Credentials
  - Interests
  - Friends
  - Preferences
  - Legacy Machines
  - Unnecessary Ports Information
  - Technologies in use, and blah blah..

Lets talk real time? History?



Well, you see it coming. What I found within 30 minutes was really stunning:

- 6 AWS access keys with their secret tokens
- 3 MongoDB connection URI (with login and password)
- 1 Twitter API credentials
- 1 Twilio API credentials
- 1 GitHub account credentials
- 1 Gmail account credentials
- And 1 Ravello Systems account credentials

Removed credentials

[redacted] committed 9 days ago   1 parent [redacted]   commit [redacted]

Showing 1 changed file with 5 additions and 5 deletions.

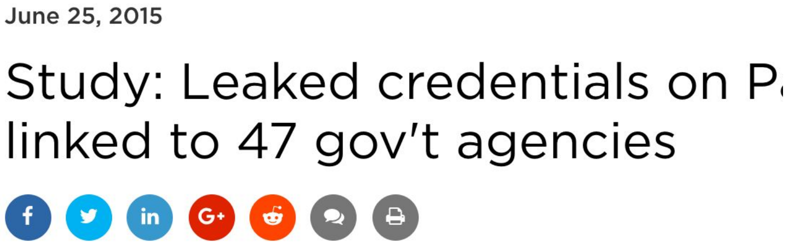
10 group_vars/all

```
@@ -1,11 +1,11 @@
 # Ravello's Credentials
-username: [redacted]@redhat.com
-password: [redacted]
-bucket: [redacted]
+#username:
+#password:
+#bucket:
```

URITY

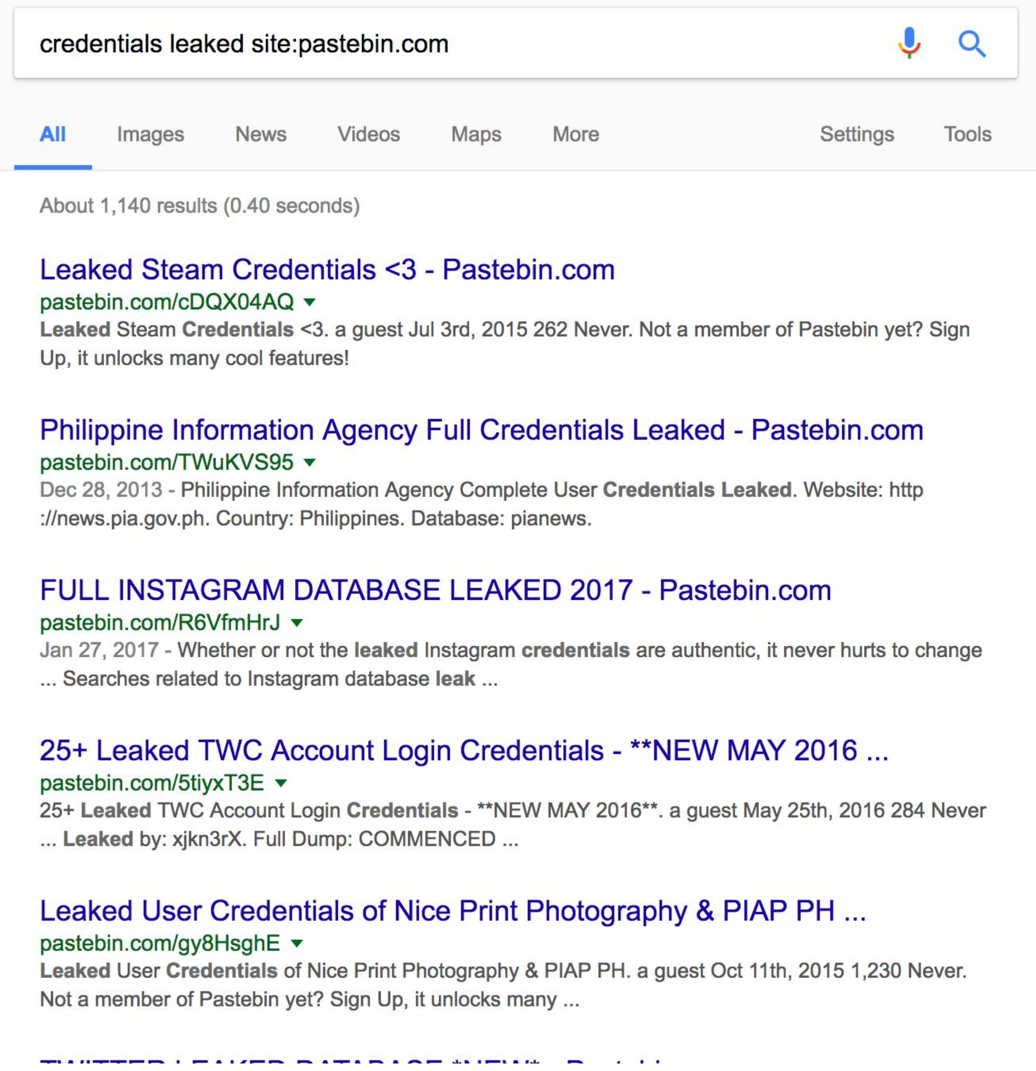
B E

es, linked



June 25, 2015

Study: Leaked credentials on P
linked to 47 gov't agencies



credentials leaked site:pastebin.com

About 1,140 results (0.40 seconds)

Leaked Steam Credentials <3 - Pastebin.com
pastebin.com/cDQX04AQ ▾
Leaked Steam **Credentials** <3. a guest Jul 3rd, 2015 262 Never. Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

Philippine Information Agency Full Credentials Leaked - Pastebin.com
pastebin.com/TWuKVS95 ▾
Dec 28, 2013 - Philippine Information Agency Complete User **Credentials Leaked**. Website: http ://news.pia.gov.ph. Country: Philippines. Database: pianews.

FULL INSTAGRAM DATABASE LEAKED 2017 - Pastebin.com
pastebin.com/R6VfmHrJ ▾
Jan 27, 2017 - Whether or not the **leaked** Instagram **credentials** are authentic, it never hurts to change ... Searches related to Instagram database **leak** ...

25+ Leaked TWC Account Login Credentials - **NEW MAY 2016 ...
pastebin.com/5tiyxT3E ▾
25+ **Leaked** TWC Account Login **Credentials** - **NEW MAY 2016**. a guest May 25th, 2016 284 Never ... **Leaked** by: xjkn3rX. Full Dump: COMMENCED ...

Leaked User Credentials of Nice Print Photography & PIAP PH ...
pastebin.com/gy8HsghE ▾
Leaked User **Credentials** of Nice Print Photography & PIAP PH. a guest Oct 11th, 2015 1,230 Never. Not a member of Pastebin yet? Sign Up, it unlocks many ...

Components

- Domain Osint
- Email Osint
- IP Osint
- Username Osint

- WIP
  - Company Scoping
  - Phone Number OSINT
  - Active Modules

Sources and Flow

Domain:

WhoIS
DNS Records
PunkSpider
Wappalyzer
Github
Email Harvestor □□
Domain IP History
Paste(s) Search
Pagelinks
Wikileaks
Links from Forums
Passive SSL Scan
ZoomEye
Shodan
Censys
Subdomains □□

Email:

Basic Email Checks
Work History
Social profiles
Enumerated Usernames □□
Location Information
Slides
Scribd Documents
Related Websites
HaveIBeenPwned

Username:

Git Details
Check username on various sites.
Profile Pics –Output saved in
$username directory
Frequent Hashtags
Interaction on Twitter.

Active Modules

Setting it up..

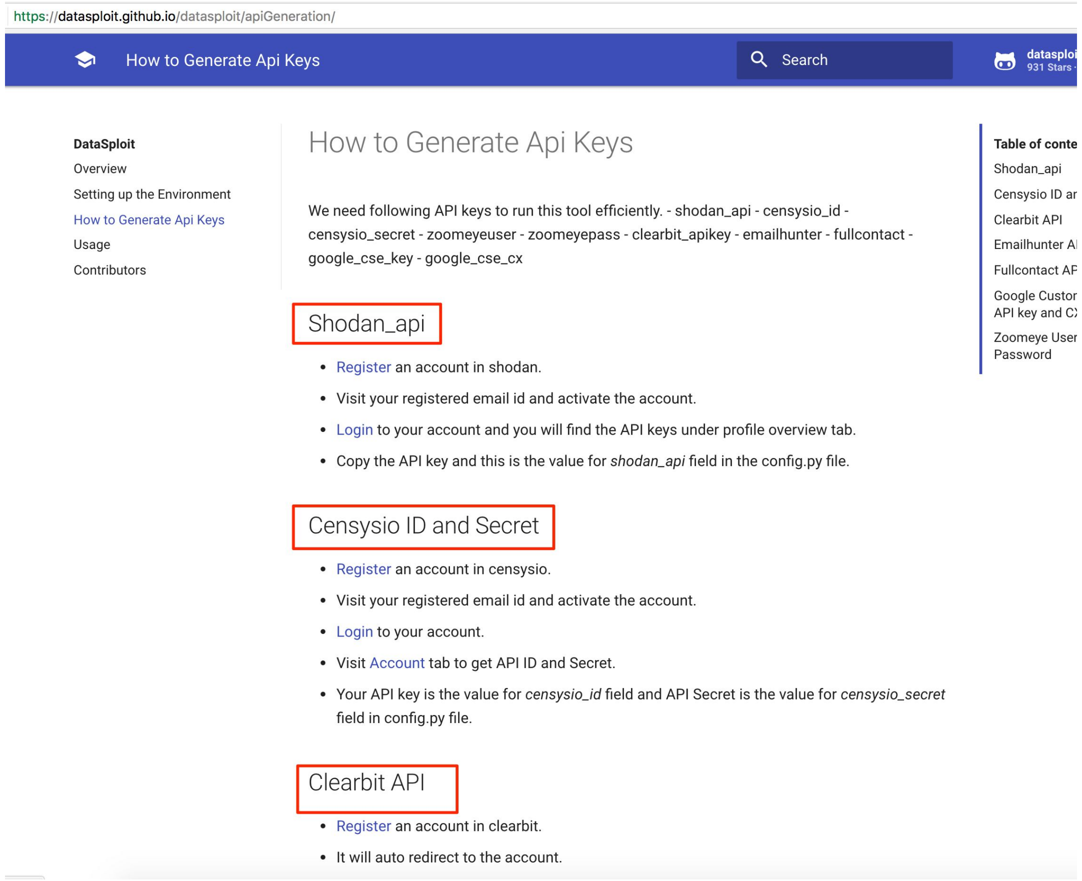
- Manual
  - Download from git (git clone or download)

    git clone https://github.com/DataSploit/datasploit.git
  - pip install –r requirements.txt
  - config.py holds API keys
  - **domain_xyz.py** – running stand alone scripts.
  - **domainOsint / emailOsint / ipOsint** – automated OSINT
  - active_scan.py

- Automated
  - https://hub.docker.com/r/appsecco/datasploit/
  - https://hub.docker.com/r/ftorn/datasploit/

Documentation.

https://datasploit.github.io/datasploit/



DataSploit
Overview
Setting up the Environment
How to Generate Api Keys
Usage
Contributors

How to Generate Api Keys

We need following API keys to run this tool efficiently. - shodan_api - censysio_id - censysio_secret - zoomeyeuser - zoomeyepass - clearbit_apikey - emailhunter - fullcontact - google_cse_key - google_cse_cx

Shodan_api

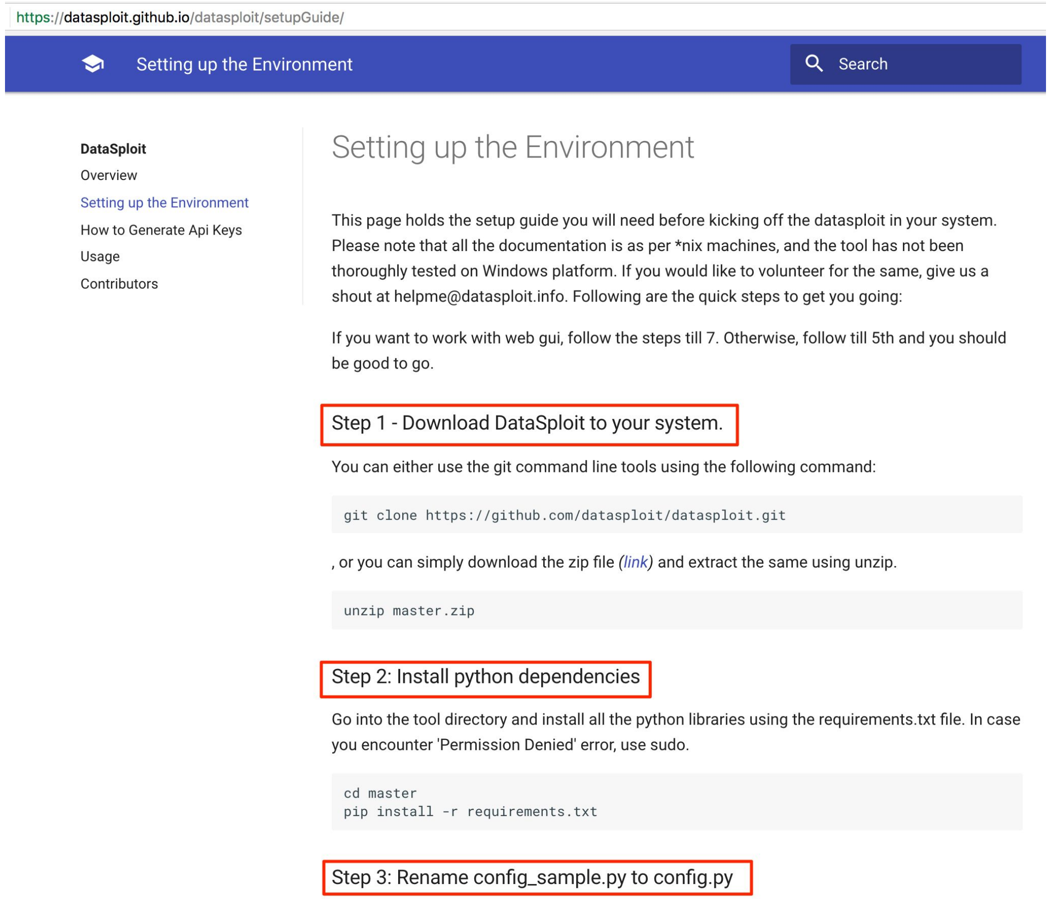
- Register an account in shodan.
- Visit your registered email id and activate the account.
- Login to your account and you will find the API keys under profile overview tab.
- Copy the API key and this is the value for *shodan_api* field in the config.py file.

Censysio ID and Secret

- Register an account in censysio.
- Visit your registered email id and activate the account.
- Login to your account.
- Visit Account tab to get API ID and Secret.
- Your API key is the value for *censysio_id* field and API Secret is the value for *censysio_secret* field in config.py file.

Clearbit API

- Register an account in clearbit.
- It will auto redirect to the account.


https://datasploit.github.io/datasploit/setupGuide/
Setting up the Environment
Search

DataSploit
Overview
Setting up the Environment
How to Generate Api Keys
Usage
Contributors

Setting up the Environment

This page holds the setup guide you will need before kicking off the datasploit in your system. Please note that all the documentation is as per *nix machines, and the tool has not been thoroughly tested on Windows platform. If you would like to volunteer for the same, give us a shout at helpme@datasploit.info. Following are the quick steps to get you going:

If you want to work with web gui, follow the steps till 7. Otherwise, follow till 5th and you should be good to go.

Step 1 - Download DataSploit to your system.

You can either use the git command line tools using the following command:

```
git clone https://github.com/datasploit/datasploit.git
```

, or you can simply download the zip file (*link*) and extract the same using unzip.

```
unzip master.zip
```

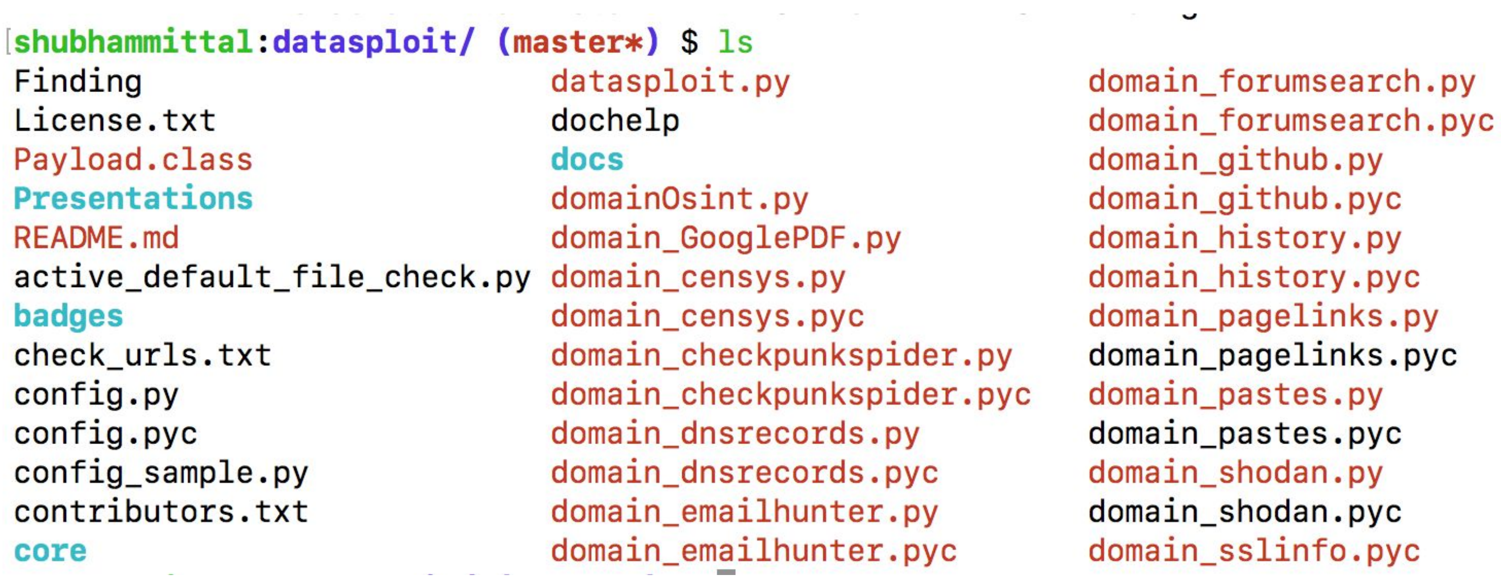
Step 2: Install python dependencies

Go into the tool directory and install all the python libraries using the requirements.txt file. In case you encounter 'Permission Denied' error, use sudo.

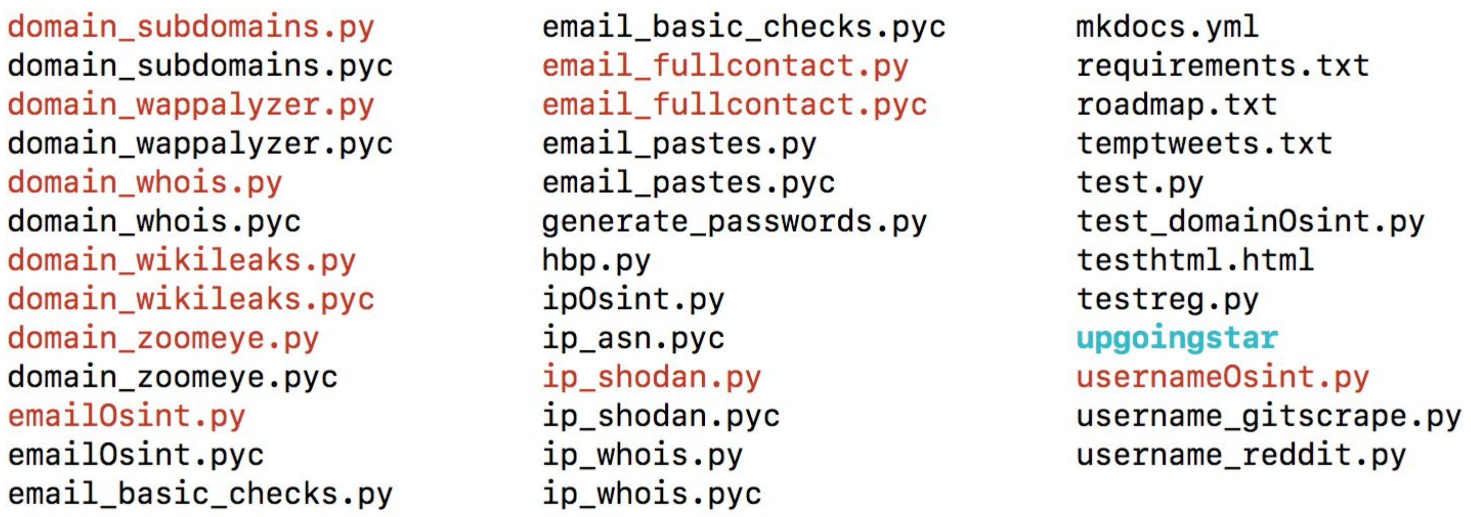
```
cd master
pip install -r requirements.txt
```

Step 3: Rename config_sample.py to config.py

What’s in there?



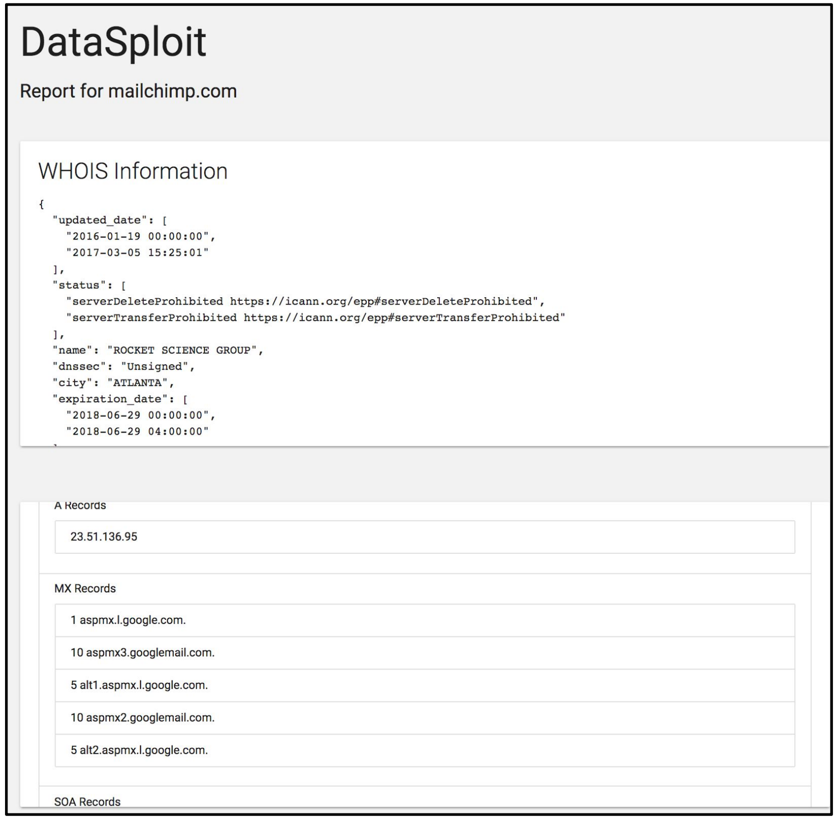
```
shubhammittal:datasploit/ (master*) $ ls
Finding                      datasploit.py                domain_forumsearch.py
License.txt                  dochelp                      domain_forumsearch.pyc
Payload.class                docs                         domain_github.py
Presentations                domainOsint.py               domain_github.pyc
README.md                    domain_GooglePDF.py          domain_history.py
active_default_file_check.py domain_censys.py             domain_history.pyc
badges                       domain_censys.pyc            domain_pagelinks.py
check_urls.txt               domain_checkpunkspider.py    domain_pagelinks.pyc
config.py                    domain_checkpunkspider.pyc   domain_pastes.py
config.pyc                   domain_dnsrecords.py         domain_pastes.pyc
config_sample.py             domain_dnsrecords.pyc        domain_shodan.py
contributors.txt             domain_emailhunter.py        domain_shodan.pyc
core                         domain_emailhunter.pyc       domain_sslinfo.pyc
```



```
domain_subdomains.py         email_basic_checks.pyc       mkdocs.yml
domain_subdomains.pyc        email_fullcontact.py         requirements.txt
domain_wappalyzer.py         email_fullcontact.pyc        roadmap.txt
domain_wappalyzer.pyc        email_pastes.py              temptweets.txt
domain_whois.py              email_pastes.pyc             test.py
domain_whois.pyc             generate_passwords.py        test_domainOsint.py
domain_wikileaks.py          hbp.py                       testhtml.html
domain_wikileaks.pyc         ipOsint.py                   testreg.py
domain_zoomeye.py            ip_asn.pyc                   upgoingstar
domain_zoomeye.pyc           ip_shodan.py                 usernameOsint.py
emailOsint.py                ip_shodan.pyc                username_gitscrape.py
emailOsint.pyc               ip_whois.py                  username_reddit.py
email_basic_checks.py        ip_whois.pyc
```

Output Formats

- HTML
- JSON
- Emails List (txt file)
- Subdomains List (txt file)



DataSploit

Report for mailchimp.com

WHOIS Information

```
{
  "updated_date": [
    "2016-01-19 00:00:00",
    "2017-03-05 15:25:01"
  ],
  "status": [
    "serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited",
    "serverTransferProhibited https://icann.org/epp#serverTransferProhibited"
  ],
  "name": "ROCKET SCIENCE GROUP",
  "dnssec": "Unsigned",
  "city": "ATLANTA",
  "expiration_date": [
    "2018-06-29 00:00:00",
    "2018-06-29 04:00:00"
```

A Records

23.51.136.95

MX Records

1 aspmx.l.google.com.

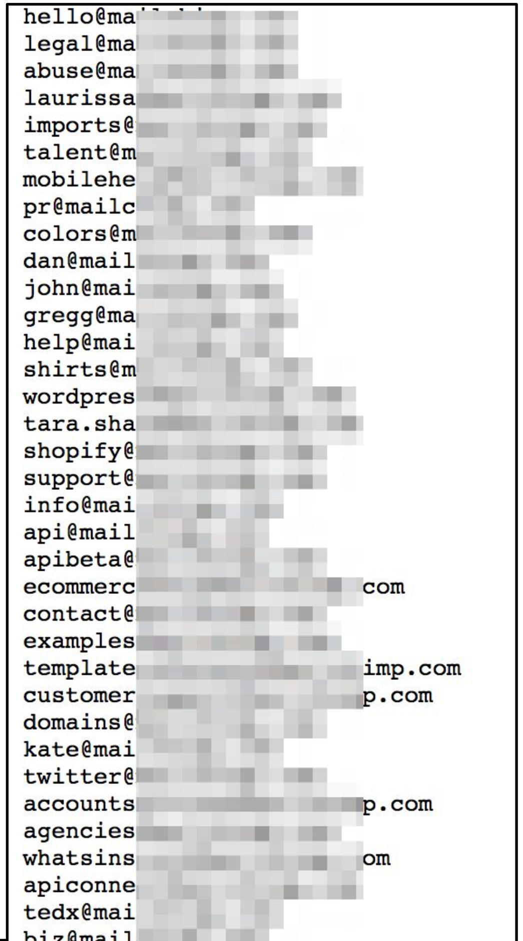
10 aspmx3.googlemail.com.

5 alt1.aspmx.l.google.com.

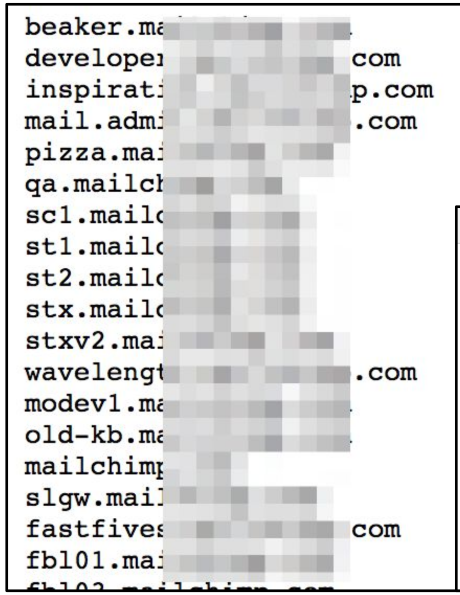
10 aspmx2.googlemail.com.

5 alt2.aspmx.l.google.com.

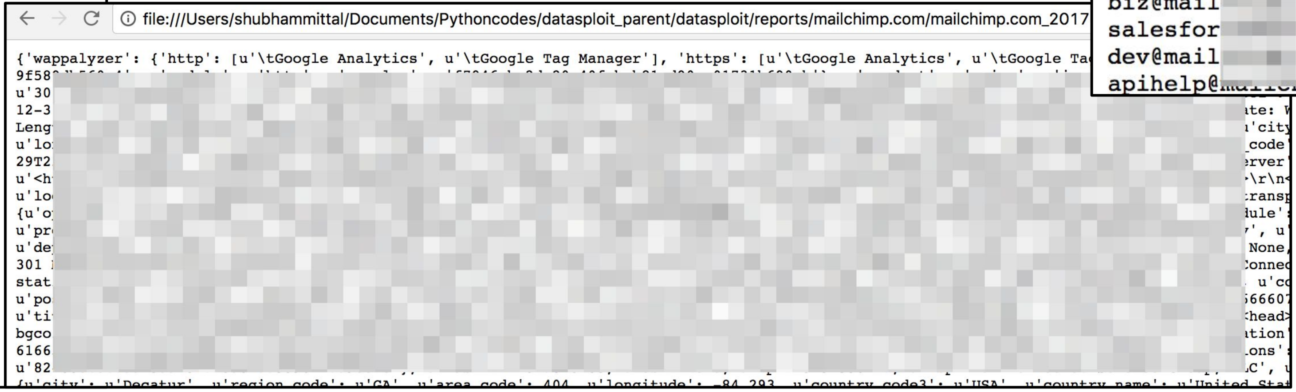
SOA Records



```
hello@ma[redacted]
legal@ma[redacted]
abuse@ma[redacted]
laurissa[redacted]
imports@[redacted]
talent@m[redacted]
mobilehe[redacted]
pr@mailc[redacted]
colors@m[redacted]
dan@mail[redacted]
john@mai[redacted]
gregg@ma[redacted]
help@mai[redacted]
shirts@m[redacted]
wordpres[redacted]
tara.sha[redacted]
shopify@[redacted]
support@[redacted]
info@mai[redacted]
api@mail[redacted]
apibeta@[redacted]
ecommerc[redacted]com
contact@[redacted]
examples[redacted]
template[redacted]imp.com
customer[redacted]p.com
domains@[redacted]
kate@mai[redacted]
twitter@[redacted]
accounts[redacted]p.com
agencies[redacted]
whatsins[redacted]om
apiconne[redacted]
tedx@mai[redacted]
biz@mail[redacted]
salesfor[redacted]
dev@mail[redacted]
apihelp@[redacted]
```



```
beaker.ma[redacted].
developer[redacted]com
inspirati[redacted]p.com
mail.admi[redacted].com
pizza.mai[redacted]
qa.mailch[redacted]
sc1.mailc[redacted]
st1.mailc[redacted]
st2.mailc[redacted]
stx.mailc[redacted]
stxv2.mai[redacted]
wavelengt[redacted].com
modev1.ma[redacted].
old-kb.ma[redacted].
mailchimp[redacted]
slgw.mail[redacted]
fastfives[redacted]com
fbl01.mai[redacted]
fbl02.ma[redacted]
```



file:///Users/shubhammittal/Documents/Pythoncodes/datasploit_parent/datasploit/reports/mailchimp.com/mailchimp.com_2017

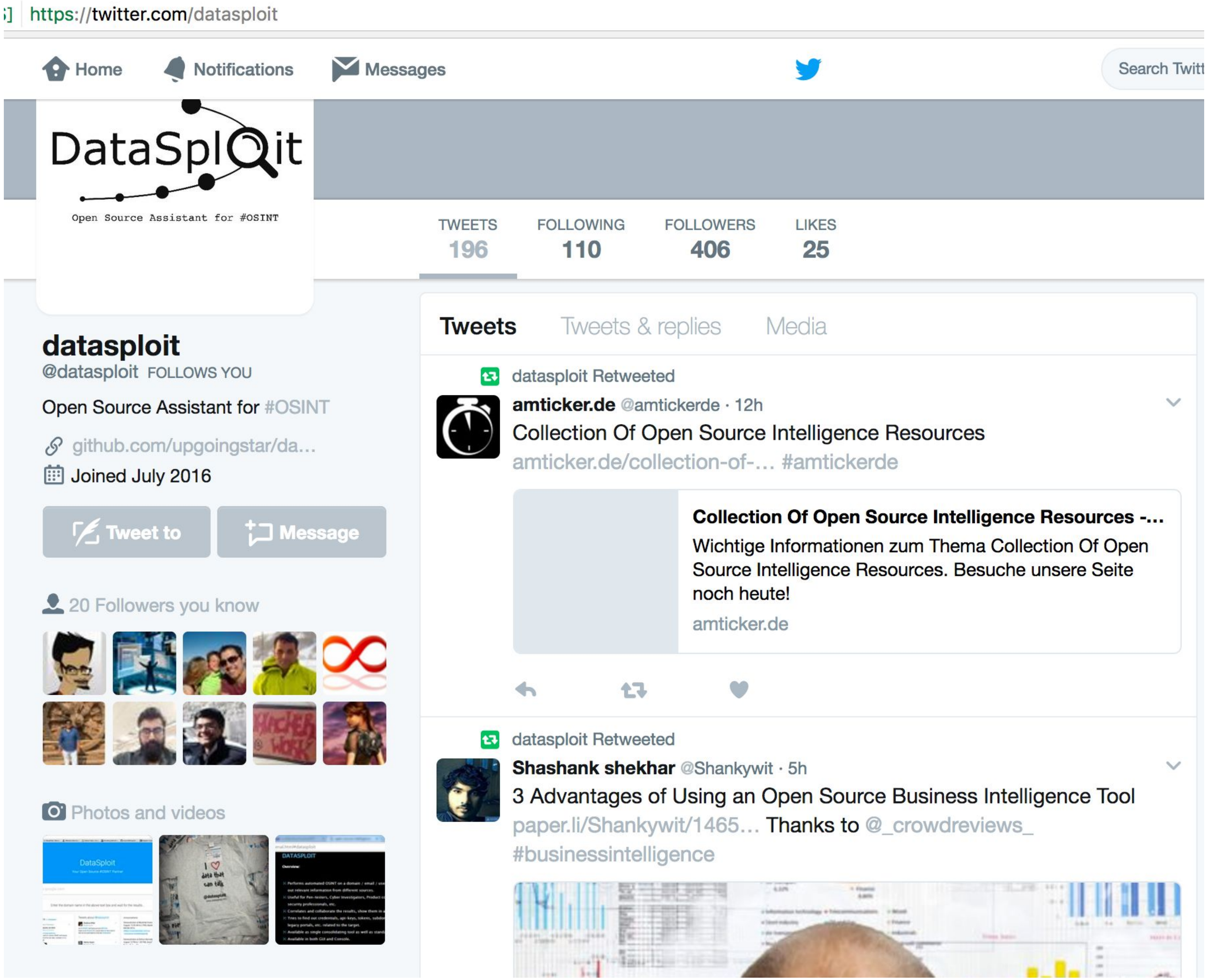
```
{'wappalyzer': {'http': [u'\tGoogle Analytics', u'\tGoogle Tag Manager'], 'https': [u'\tGoogle Analytics', u'\tGoogle Ta
[redacted]
{u'city': u'Decatur', u'region_code': u'GA', u'area_code': 404, u'longitude': -84.293, u'country_code3': u'USA', u'country_name': u'United Stat
```

DEMO TIME
LET'S HOPE THE DEMO-GODS ARE SMILING!
memegenerator.net

Twitter:

@datasploit

https://twitter.com/datasploit



datasploit
@datasploit FOLLOWS YOU

Open Source Assistant for #OSINT

github.com/upgoingstar/da...

Joined July 2016

datasploit Retweeted

amticker.de @amtickerde · 12h

Collection Of Open Source Intelligence Resources amticker.de/collection-of-... #amtickerde

Collection Of Open Source Intelligence Resources -...
Wichtige Informationen zum Thema Collection Of Open Source Intelligence Resources. Besuche unsere Seite noch heute!
amticker.de

datasploit Retweeted

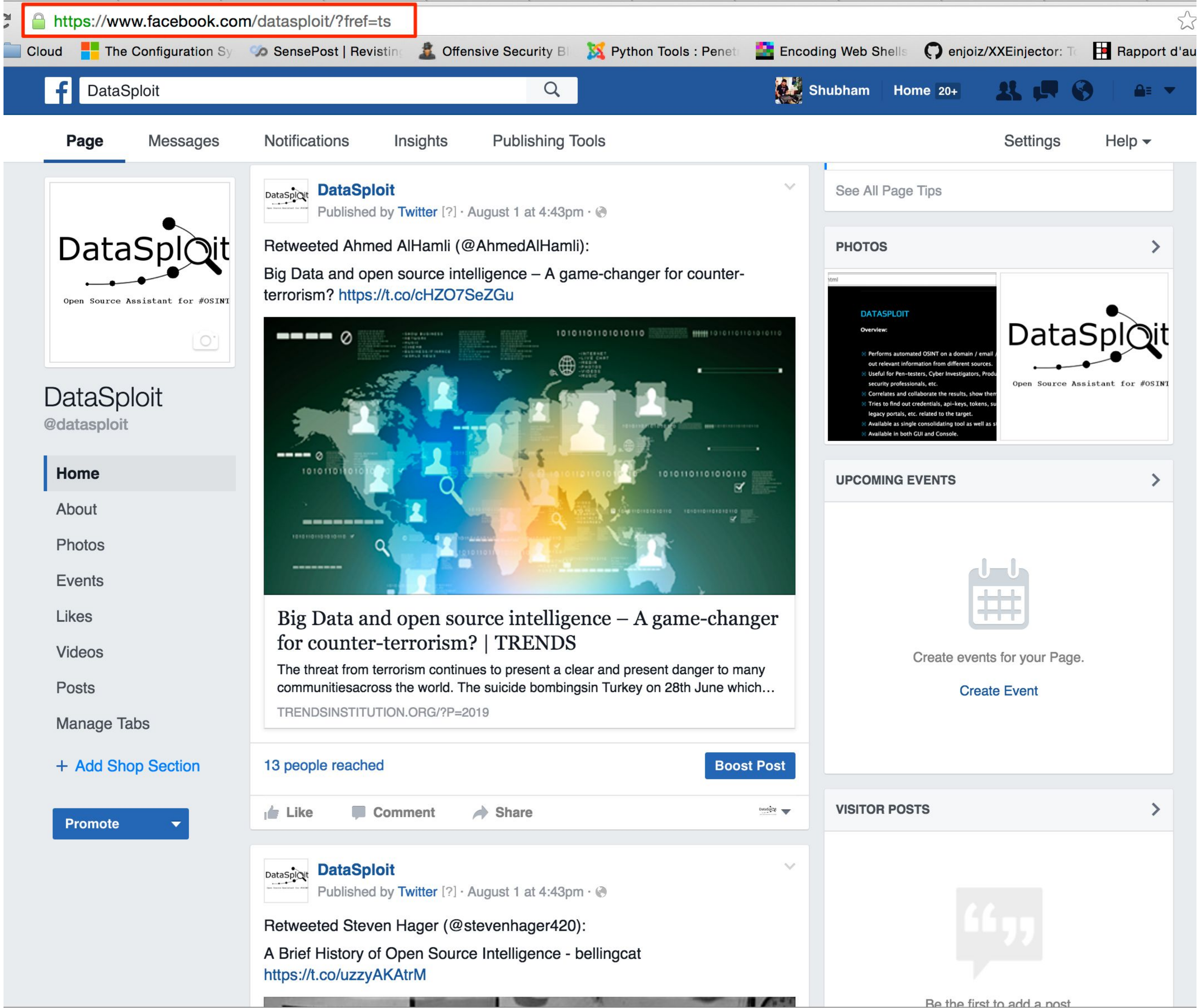
Shashank shekhar @Shankywit · 5h

3 Advantages of Using an Open Source Business Intelligence Tool paper.li/Shankywit/1465... Thanks to @_crowdreviews_ #businessintelligence

Facebook:

/datasploit

https://www.facebook.com/datasploit/



DataSploit
Published by Twitter [?] · August 1 at 4:43pm ·

Retweeted Ahmed AlHamli (@AhmedAlHamli):

Big Data and open source intelligence – A game-changer for counter-terrorism? https://t.co/cHZO7SeZGu

Big Data and open source intelligence – A game-changer for counter-terrorism? | TRENDS

The threat from terrorism continues to present a clear and present danger to many communitiesacross the world. The suicide bombingsin Turkey on 28th June which…

TRENDSINSTITUTION.ORG/?P=2019

DataSploit
Published by Twitter [?] · August 1 at 4:43pm ·

Retweeted Steven Hager (@stevenhager420):

A Brief History of Open Source Intelligence - bellingcat
https://t.co/uzzyAKAtrM

Roadmap

- Allows to set up periodic scans and alerting for product security companies.
- Intelligence on co-relation and identity verification.
- Reports in CSV.
- Reverse Image Search and profile validation.
- Works closely with various social network APIs.
- Refine Pastebin and Github Searches.
- IP Threat Intelligence.
- Organization Scoping.
- Integration with SE other tools.
- Cloud related OSINT and active modules.
- pip install datasploit (to be installed as both library as well as script)

Coverage

2016
TOP 10 BEST SECURITY TOOLS
toolswatch
HACKERS ARSENAL

KIWICON X

CON VERGE

DEF 24 CON
DEMO LABS

BSIDES CHARM 2017

HACK TV NAKED
http://securityweekly.com

SECURITY LIST NETWORK™
"TO KEEP EVERYTHING TESTED AND SECURE"

info security
STRATEGY | INSIGHT | TECHNOLOGY

SC MEDIA

Blackarch linux

The Register®
Biting the hand that feeds IT

CircleCityCon 4.0

OSINT Framework

black hat® USA 2016

black hat® EUROPE 2016

black hat® ASIA 2017

How to Contribute

- Help us in testing the tool
- Expand : Write/Suggest modules
- Give Feedback: raise issues, tweet, drop an email.
- Use / Promote / Write about the tool.
- Write OSINT blogs / tool walkthrough(s) / etc.

- Report issues at https://github.com/datasploit/datasploit/issues

Core Contributors.

- Shubham Mittal (@upgoingstar)
- Nutan Kumar Panda (@nutankumarpanda)
- Sudhanshu (@sudhanshu_c)
- Kunal (@KunalAggarwal92)

- Kudos to
  - @anantshri for mentoring.
  - @ bnchandrapal for feedbacks, suggestions and other help around issues.

Thanks. g0t questions?

https://github.com/DataSploit/datasploit

Follow @datasploit for OSINT news and latest updates.

Tweet / DM to ***@datasploit***

upgoingstaar@gmail.com