

Week in OSINT #2019–29

This week a tool, some tips, a podcast and an extremely interesting article!



Sector035 [Follow](#)

Jul 22 · 4 min read

Welcome to yet another episode of Week in OSINT. A little bit of everything this week, as you expect from me, starting with a nifty little tool to search for some sensitive information in GitHub and ending with a little smile.

- [truffleHog](#)
- [Searchbook in Chrome](#)
- [Dislikes Instagram](#)
- [dark.fail](#)
- [Bellingcat Podcast](#)

- Lampyre for Basic Phone and Email
- Behind a Website

. . .

Tool: truffleHog

The new OSINT team chatroom was hardly online, or former and new accounts already found their way inside, asking for help. One question peaked my interest, since it was a question about finding possible ‘secrets’ being exposed in GitHub repositories. And Twitter user and my awesome partner during the TraceLabs CTF Salaheldinaz had the perfect tool for that: truffleHog! A simple script that can check repos and their commits for juicy information and has some nice options, like using custom RegEx to search for private keys, possible passwords, IP addresses and whatever you might be looking for.

```
sector035@Discovery:~$ trufflehog --regex --entropy=False https://github.com/xyhStruggler/COMS319_Lab05.git
Reason: RSA private key
Date: 2016-10-28 05:37:11
Hash: f73ce249bd11a680285b5aeaaec4e6382a679af
Filepath: lab5/phpseclib/Crypt/RSA.php
Branch: origin/master
Commit: PublicPosts_PHP
```

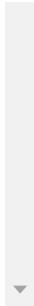
```
-----BEGIN RSA PRIVATE KEY-----  
Reason: RSA private key  
Date: 2016-10-28 05:37:11  
Hash: f73ce249bd11a680285b5aeaaeec4e6382a679af  
Filepath: lab5/user.txt  
Branch: origin/master  
Commit: PublicPosts_PHP  
  
-----BEGIN RSA PRIVATE KEY-----
```

A little test run on a repo that I knew it had something interesting

Link: <https://github.com/dxa4481/truffleHog>

• • •

Tip: Searchbook in Chrome



The Searchbook extension of sowdust that gives you the ability to query the graph search engine of Facebook, was only available for Firefox. But thanks to [Justin Seitz](#) you can now enjoy the same extension inside Chrome if you need it. Especially handy for users of [Hunchly](#)!

Thread: https://twitter.com/jms_dot_py/status/1152277562531430401

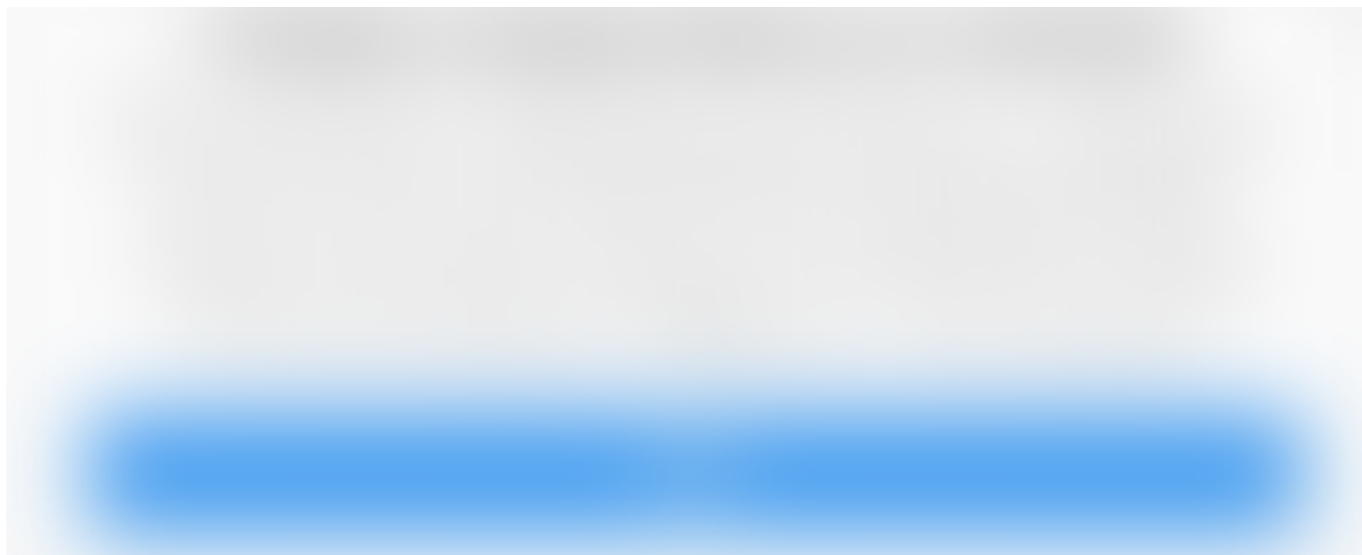
. . .

Tip: Dislikes Instagram

It seems that not just Facebook is tightening up the privacy of the users on their own site, but they now start removing a very handy feature within Instagram: The visibility of likes. I personally doubt that Facebook is

REALLY concerned with protecting your privacy, especially when you read in this PDF (HT: @random_walker) but here we are.

The first thing that people will see is a small message, explaining that this is the case:



After this, you will not be able to see any likes within a post. The difference is clearly visible. Here is the difference between a browser session where nobody is not logged in on the left, with a 'censored' Instagram account on the right.





As shown, it is still possible to see the likes when you are not logged in. It can be that for now only the mobile apps are affected for some people, but at least querying the API still works. I do want to send a special shout-out to

Tokyo_v2 who provided me with some information and who manually tested the API query for this. So, for the moment all the information is still there, so get your Python ready and get going with Instagram scraper while it still works!

Facebook Article: <https://mislove.org/publications/PII-PETS.pdf>

GitHub: <https://github.com/realsirjoe/instagram-scraper>

. . .

Tip: dark.fail

A simple tweet, a simple mention in Week in OSINT. [OSINT Techniques](#) shared a link to a very basic looking website, that lists the most popular online markets, forums and sites on the dark web with their online status.

Link: <https://dark.fail/>

. . .

Media: Bellingcat Podcast

Last week Bellingcat went live with a Podcast. The very first episode is called ‘The People Who Fell From The Sky’ and deals with the downing of MH17. The event itself is well known and the role of Bellingcat in the investigation has been vital for uncovering the truth. So if you have about half an hour to spare, do open your favourite app and grab another coffee.

Listeners discretion is advised, because the details that are shared, for instance by the first journalists on site, are fairly graphic.

Link: <https://overcast.fm/+TGXEzn7Ro> or in your favourite Podcast app

• • •

Article: Lampyre for Basic Phone and Email

This weekend [wondersmith_rae](#) shared an article on Medium describing some basics of Lampyre and how to perform some easy searches. This is a really nice explanation, detailing some easy to follow steps. Great to see write-ups like this, sharing knowledge and helping others to get familiar with tools. I give this a 5/7!



Image taken from the article by Rae Baker

Link: <https://medium.com/@raebaker/using-lampyre-for-basic-email-and-phone-number-osint-e0e36c710880>

. . .

Article: Behind a website

I am working in IT security, and have a long history with computers, websites and the internet itself. But not everybody has had a career that went technically as deep. Some things or actions that are a second nature for me when doing research online, might be complete magic to others. But last week [Serge Courier](#) shared a link with a lot of good hints, tips and explanations. So if you feel the need to brush off your knowledge, or you are completely new at this, do save this page and spend an afternoon going over all the information inside. This is definitely one to keep!





A small excerpt of the article, covering reverse Whois searches

Link: <https://kit.exposingtheinvisible.org/how/web.html>

. . .

FUNINT: Snapchat Map

...

Have good week and have a good search!

Osint

Open Source Intelligence

Open Source Investigation



18 claps



WRITTEN BY

Sector035

Follow

Just a shadowy nerd... Busy with InfoSec, geolocation and OSINT



Week in OSINT

Follow

Your weekly dose of OSINT websites, tools and aimed at anyone working in the field of analysts, researchers and pentesters.

Write the first response

More From Medium

Related reads

DCShadow: detecting a rogue domain controller replicating malicious changes to your Active...





Maarten Goet

Dec 18, 2018 · 6 min read



59



Related reads

A Phishing Guide: Lessons Learned on the Journey to Detecting Phishing Domains



Jonathan Ticknor in security...

Jan 24 · 8 min read



148



Related reads

Putting Sysmon v9.0 AND/OR Grouping Logic to the Test

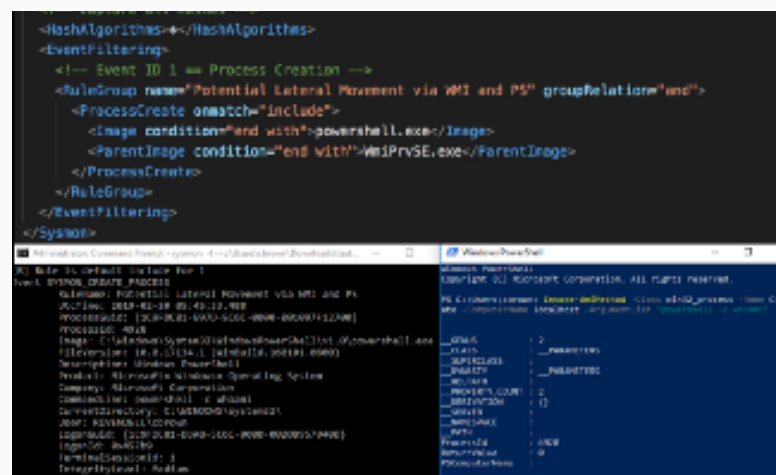
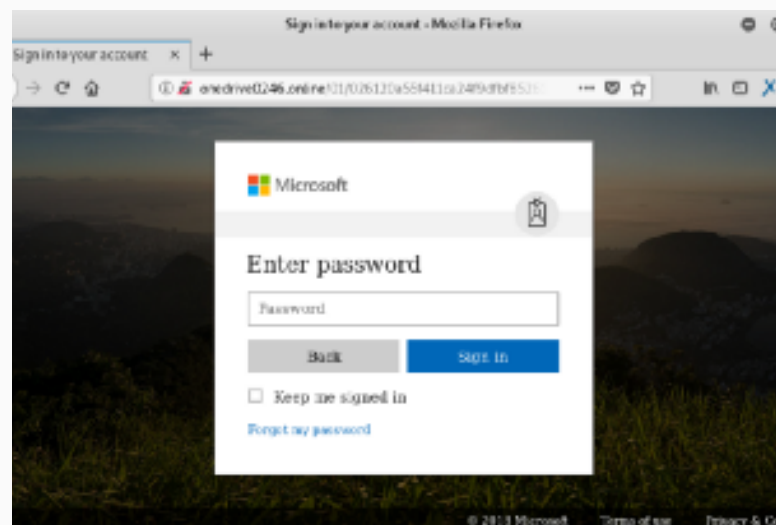
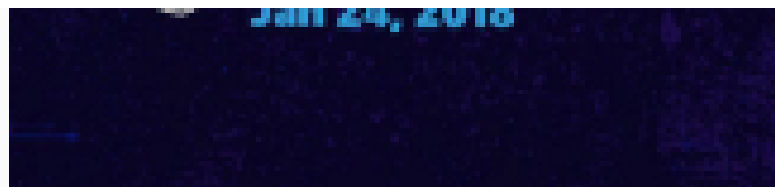


Roberto Rodriguez in Posts By...

Feb 20 · 12 min read



47



[illegible]