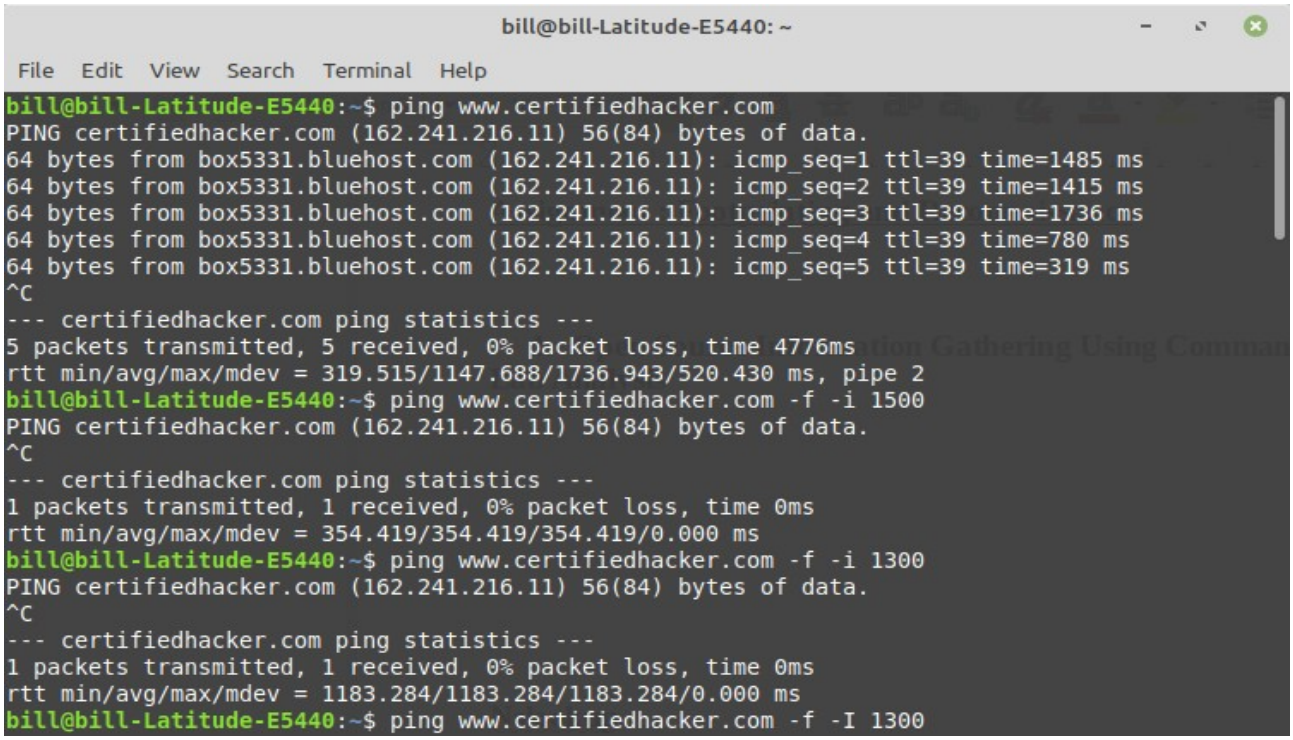
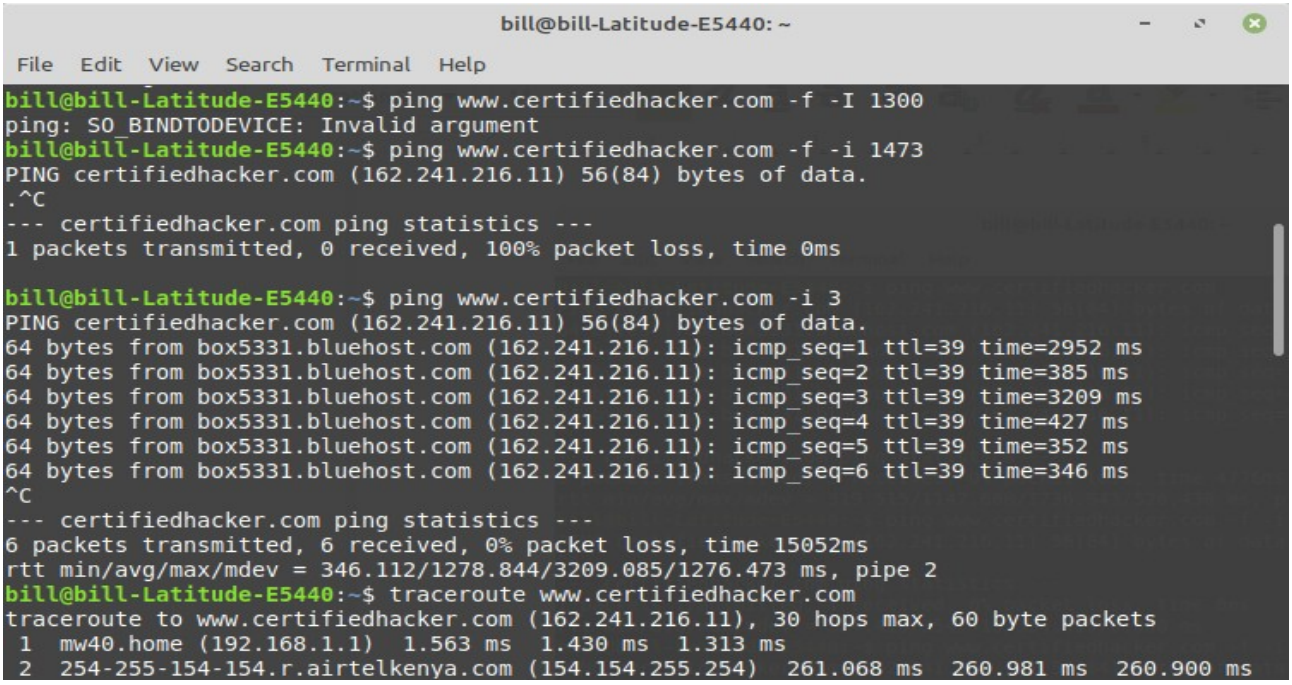
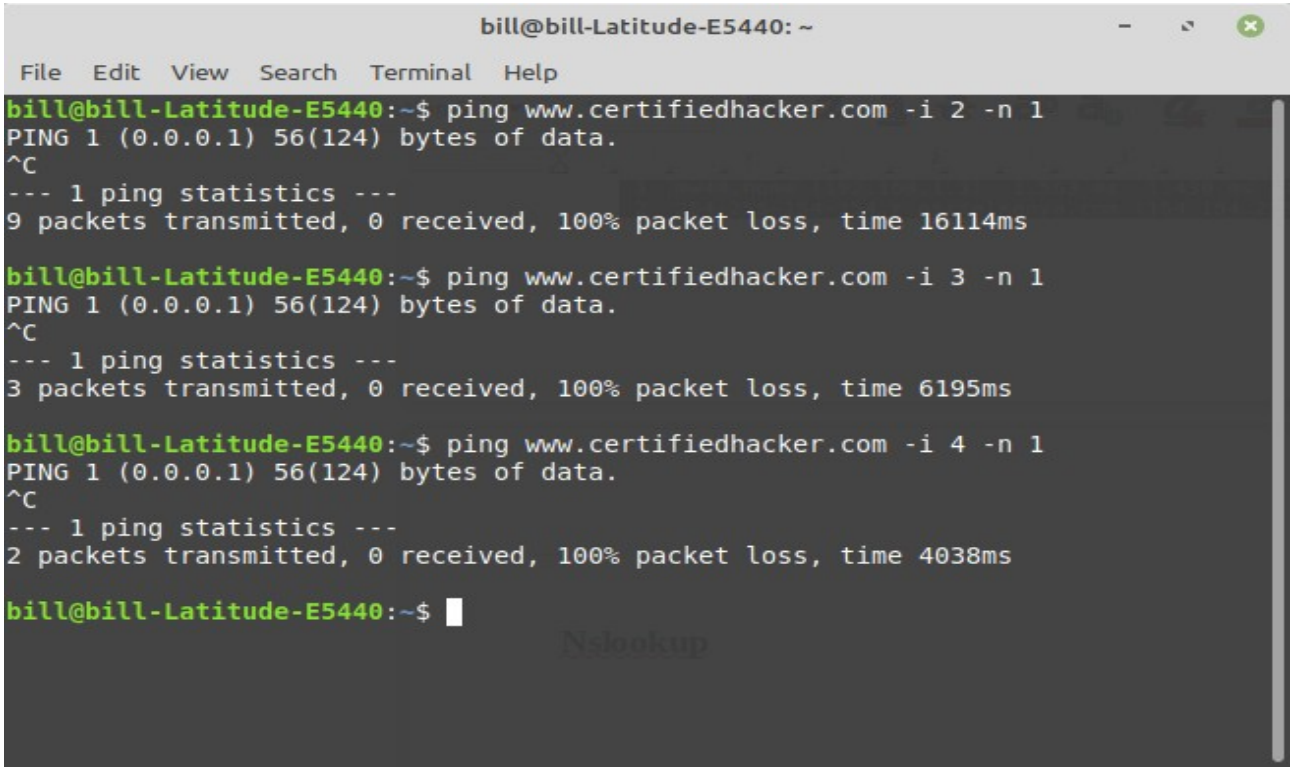
Footprinting and Reconnaissance

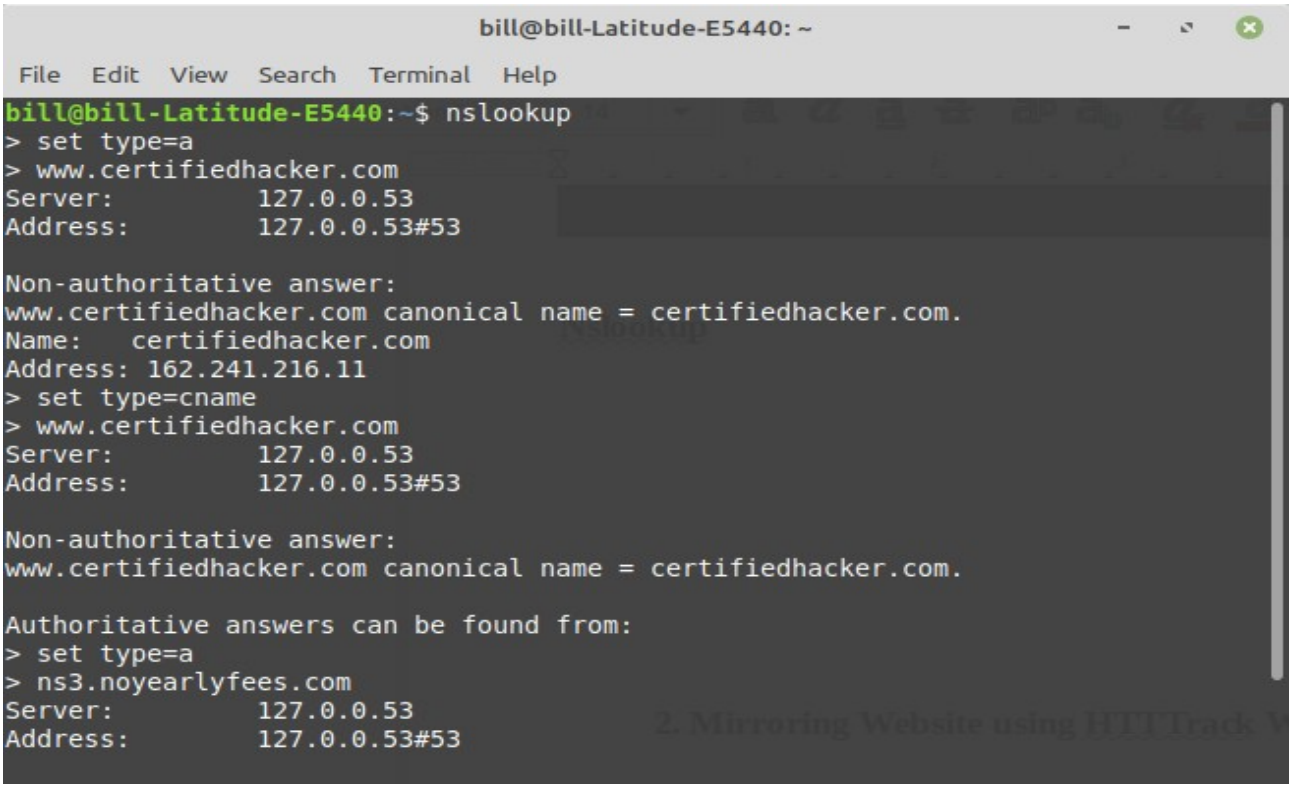
1. Open Source Information Gathering Using Command Line Utilities.





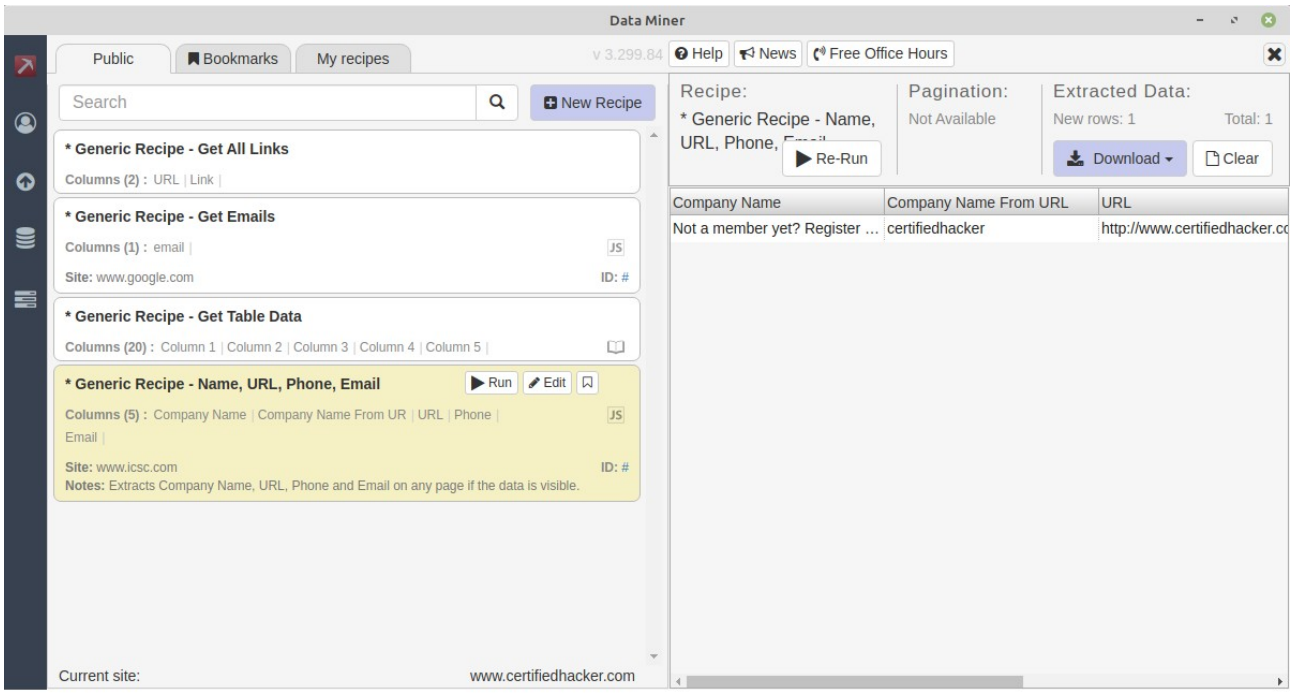

bill@bill-Latitude-E5440: ~
File Edit View Search Terminal Help
bill@bill-Latitude-E5440:~$ ping www.certifiedhacker.com -i 2 -n 1
PING 1 (0.0.0.1) 56(124) bytes of data.
^C
--- 1 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 16114ms
bill@bill-Latitude-E5440:~$ ping www.certifiedhacker.com -i 3 -n 1
PING 1 (0.0.0.1) 56(124) bytes of data.
^C
--- 1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 6195ms
bill@bill-Latitude-E5440:~$ ping www.certifiedhacker.com -i 4 -n 1
PING 1 (0.0.0.1) 56(124) bytes of data.
^C
--- 1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 4038ms
bill@bill-Latitude-E5440:~$

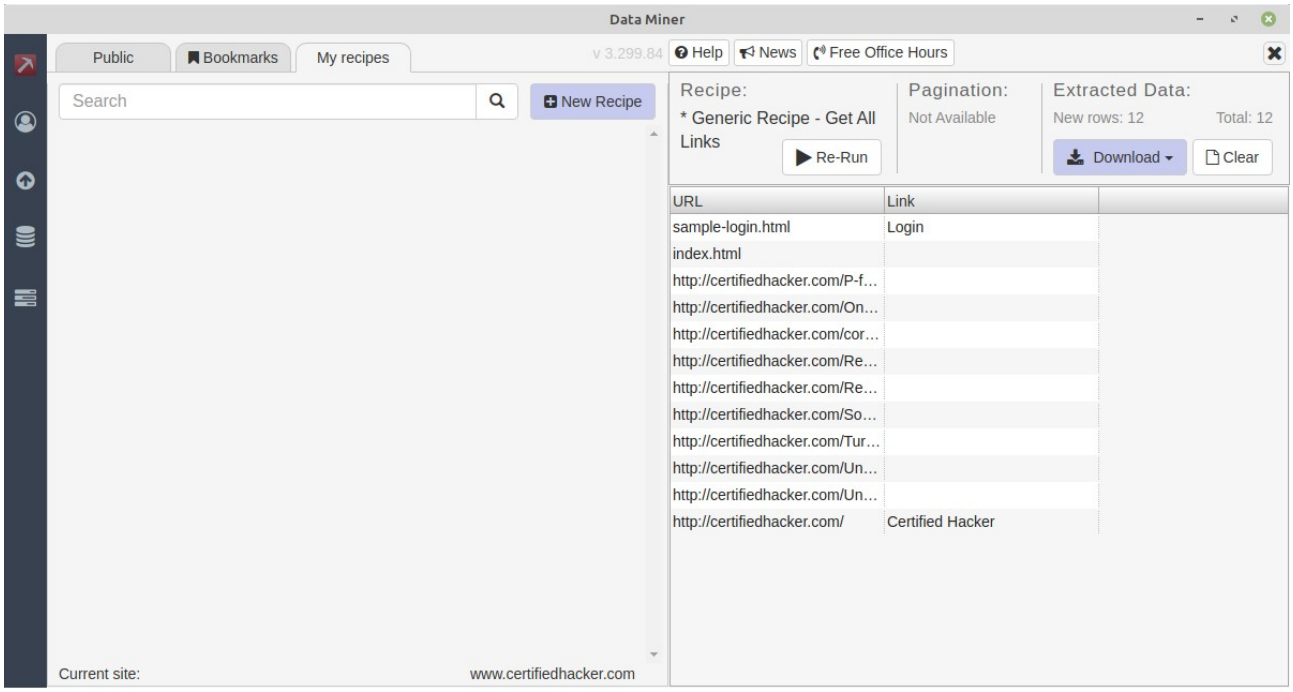
Nslookup


bill@bill-Latitude-E5440: ~
File Edit View Search Terminal Help
bill@bill-Latitude-E5440:~$ nslookup
> set type=a
> www.certifiedhacker.com
Server: 127.0.0.53
Address: 127.0.0.53#53
Non-authoritative answer:
www.certifiedhacker.com canonical name = certifiedhacker.com.
Name: certifiedhacker.com
Address: 162.241.216.11
> set type=cname
> www.certifiedhacker.com
Server: 127.0.0.53
Address: 127.0.0.53#53
Non-authoritative answer:
www.certifiedhacker.com canonical name = certifiedhacker.com.
Authoritative answers can be found from:
> set type=a
> ns3.noyearlyfees.com
Server: 127.0.0.53
Address: 127.0.0.53#53

```
> set type=a
> ns3.noyearlyfees.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ns3.noyearlyfees.com
Address: 108.174.147.235
```

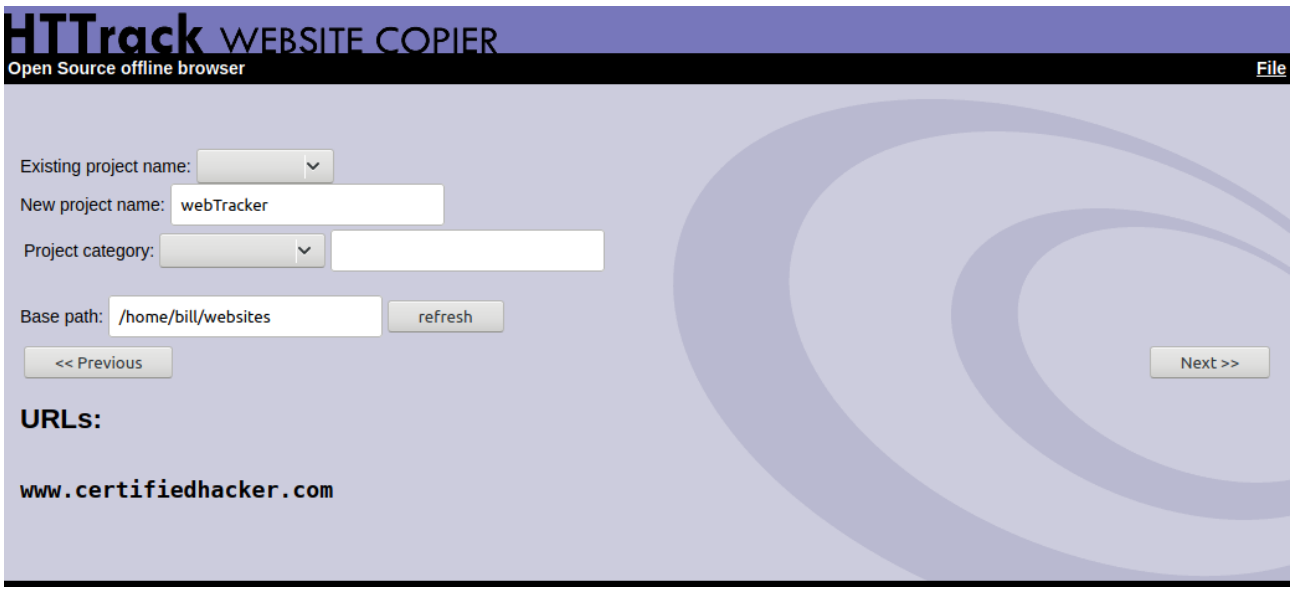
Extracting a Company’s Data Using Web Data Extractor (Data scraper)

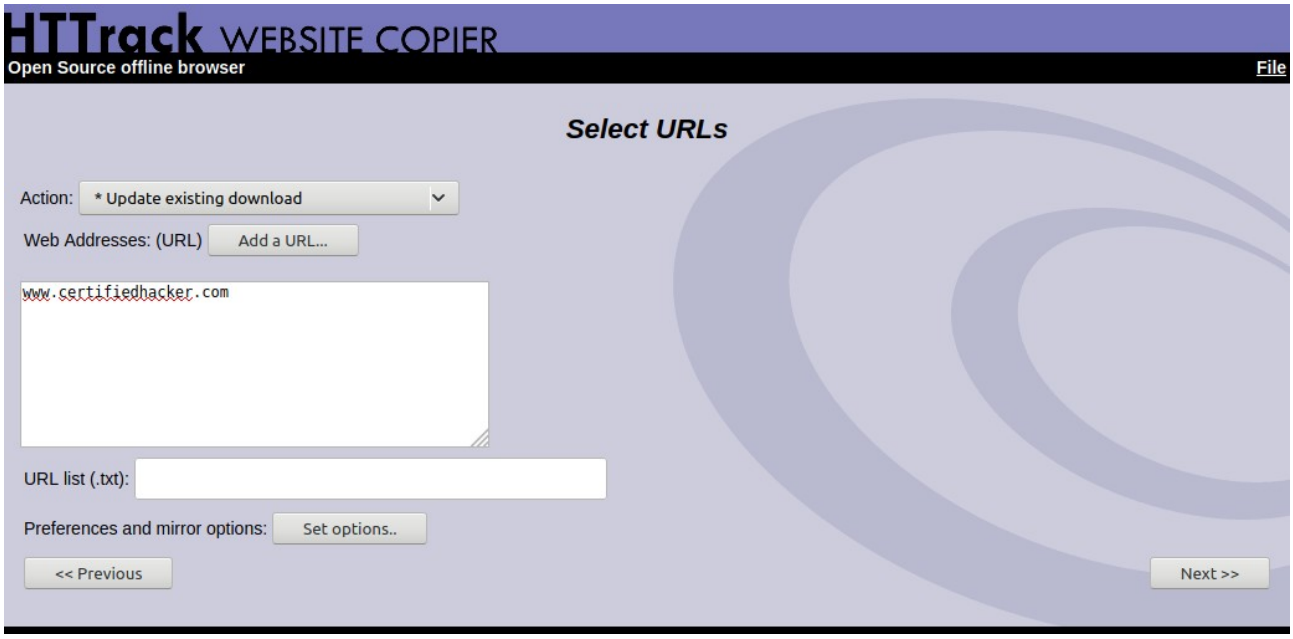




2. Mirroring Website using HTTTrack Web site Copier

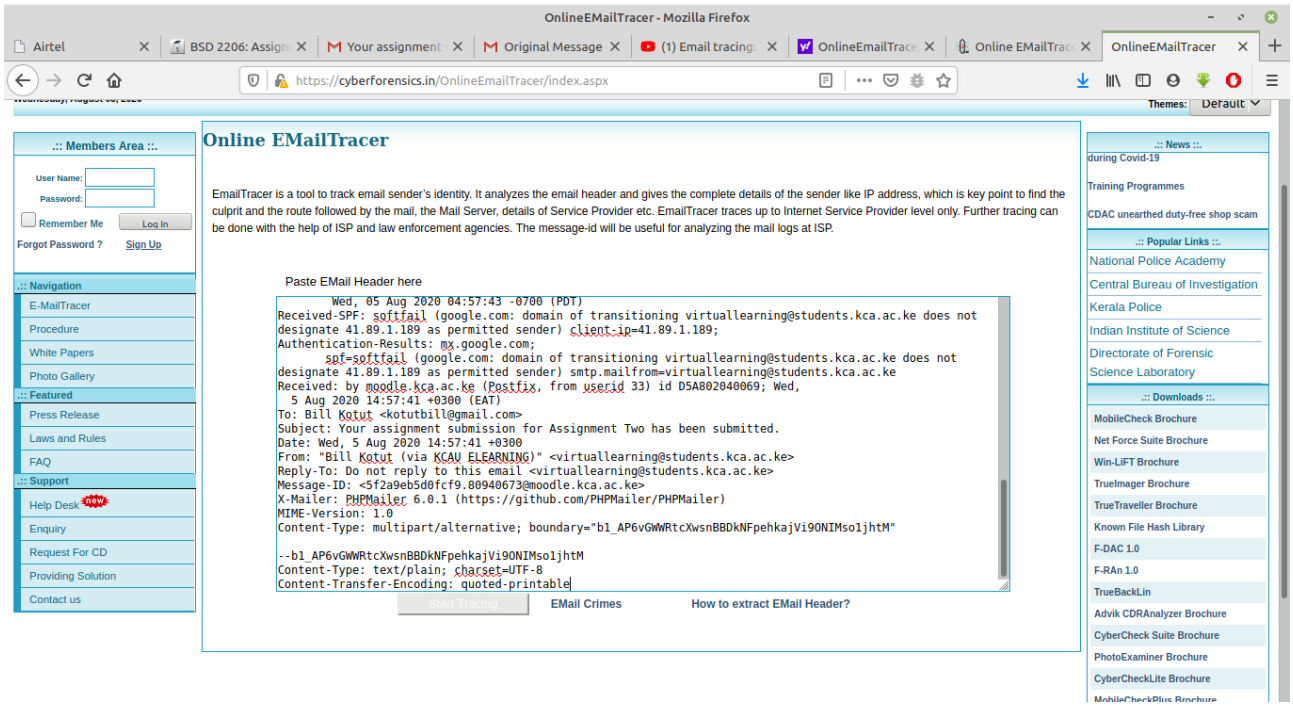
Lab analysis





Collecting Information About a Target by Tracing Emails

```
Delivered-To: kotutbill@gmail.com
Received: by 2002:a50:7887:0:0:0:0:0 with SMTP id l7csp313556ecl;
        Wed, 5 Aug 2020 04:57:43 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJxdgtqfNnxGjJGKpd43+60Hztc2jzCLLFdTOO2Hkr0cmvPqiTPr7yiE2EV8xjHAUsgIdpWu
X-Received: by 2002:adf:ef92:: with SMTP id d18mr2689768wro.71.1596628663521;
        Wed, 05 Aug 2020 04:57:43 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1596628663; cv=none;
        d=google.com; s=arc-20160816;
        b=z1pSLNTwr/v3OnR5qYDnh2aQvz3JpViv/Tp8A43Qrc05Tj5CJD9LNBqO/BjAZrICHL
         cGUzF6XMM5ZJmHB80OLXBg/lECjlL3ynJKRSfCAUm+wldqEfgq1uVo5QOdqLPmDC7qxE
         j/TjjC6OrAzr2bj4rYFV2KTDdroBejskBWwRFV1sMqORzK5Y1R/uSH32L3OLORGl2arS
         F0hp5AUbaasLPu9PCDSHE9gUVsmfqmt+dEiTwUI2PqS0mM/tVN/43eBEMG18IhqQkCTZ
         XGkB3EtqEPdnJEeVUHZfbNBAr3Ksmuq21NduchLHWJU7nxOi6QV1sRdqsSlEwHkJIbOZ
         WMhQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=mime-version:message-id:reply-to:from:date:subject:to;
        bh=ge1bI+DfGOp+gR3tGGF4zCbsTQCeYpdHXr4jm2/tTPM=;
        b=UW8LJGjFd7NnJhYQ2cP19T1Am3q3kG/8CiZdCbQWRaLpeHXEs3g2iZHoxHCI1SYl4A
         8bJE59zvg5H20E4Dw5tTZ4vl6Xr1TCHeZGUVkNDbeOb8IHeFYc2d1see4oZugj+GQ+iu
         fqhBgT1+zHfWLJpx70trHbvtLAvOA+bo+ZnfSrkekNmUoNfkMNwil19pVW8f+/uBXcxH
         L+oBUZCjbpCZlg9VhSOd2yljIeL23a+bJaD2PilockkDQwr4yQuUdTl69b+Pmb1CyOMH
         KH0R68z2hDuUtH6rPIK1sXz5/zSgUYDs4A7WFREwc7X/ccFNtNpKmBfOWf+N15uk6lxw
         sdUA==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=softfail (google.com: domain of transitioning virtuallearning@students.kca.ac.ke does not designate
41.89.1.189 as permitted sender) smtp.mailfrom=virtuallearning@students.kca.ac.ke
Return-Path: <virtuallearning@students.kca.ac.ke>
Received: from moodle.kca.ac.ke (moodle.kca.ac.ke. [41.89.1.189])
        by mx.google.com with ESMTPS id p16si1531150wrx.439.2020.08.05.04.57.43
        for <kotutbill@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Wed, 05 Aug 2020 04:57:43 -0700 (PDT)
Received-SPF: softfail (google.com: domain of transitioning virtuallearning@students.kca.ac.ke does not designate
41.89.1.189 as permitted sender) client-ip=41.89.1.189;
Authentication-Results: mx.google.com;
       spf=softfail (google.com: domain of transitioning virtuallearning@students.kca.ac.ke does not designate
```

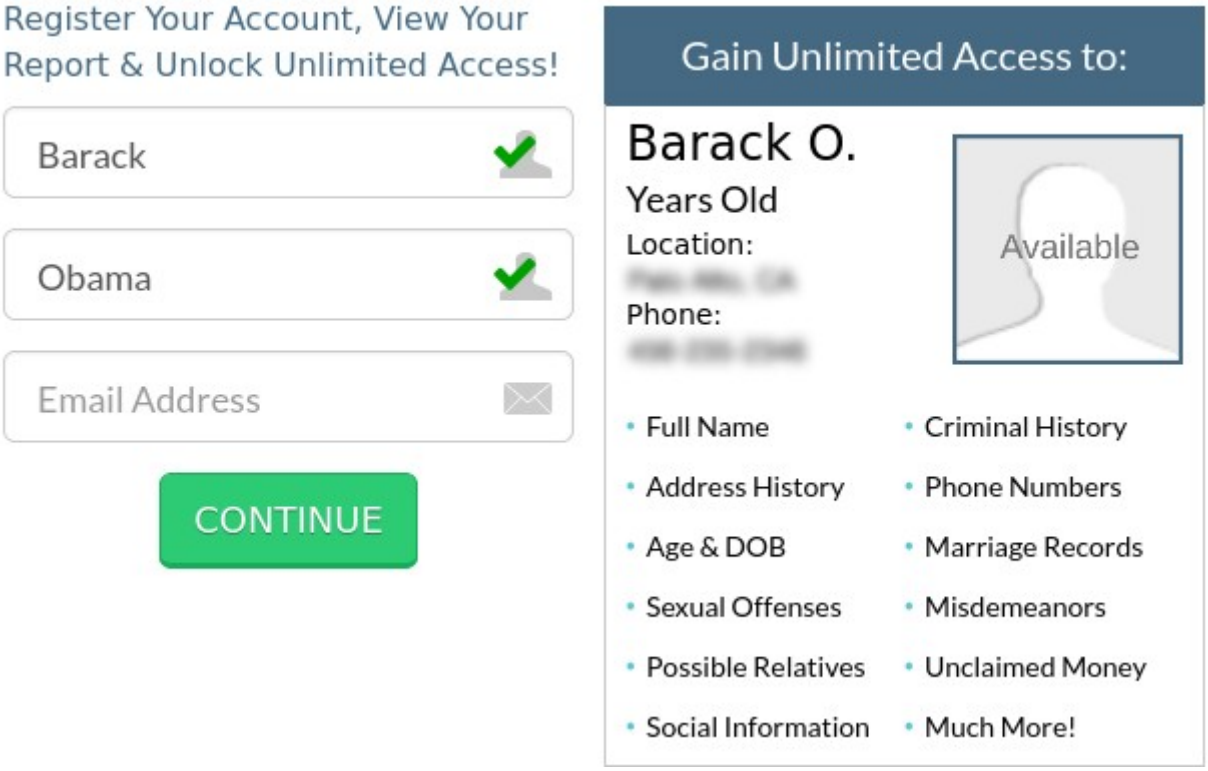


Sender

IP Address	41.89.1.189
Country	Kenya
Region & City	Nairobi City, Nairobi
Coordinates	-1.283330, 36.816670 (1°16'60"S 36°49'0"E)
ISP	Kenet Core Equipment
Local Time	05 Aug, 2020 06:40 PM (UTC +03:00)
Domain	kenet.or.ke
Net Speed	(DSL) Broadband/Cable/Fiber/Mobile
IDD & Area Code	(254) 020
ZIP Code	-
Weather Station	Nairobi (KEXX0009)
Mobile Carrier	-
Mobile Country Code (MCC)	-

Map for -1.283330, 36.816670

Gathering Personal Information Using Online People Search Services



Collecting Information About a Target Website Using Fire bug

MOVIE SCOPE
www.moviescope.xyz

What are you looking for?

HOME | MOVIES | GENRE | QUALITY | YEAR | WEB-SERIES

Deadpool (2016) [Hindi-English] 480p [300mb] | 720p Movie Download

Download Toy Story (1995) [Hindi-English] 480p [300MB] || 720p [800MB]

Download Toy Story 2 (1999) [Hindi-English] 480p [300MB] || 720p [800MB]

Download Toy Story 3 (2010) [Hindi-English] 480p [300MB] || 720p [800MB]

Download Toy Story 4 (2019) Dual Audio [Hindi-English] Bluray 480p [400MB] || 720p [850MB] || 1080p [2GB]

Download Captain America: Civil War (2016) Dual Audio 480p [460MB] || 720p [1GB] || 1080p [1.5GB] [Hindi-English]

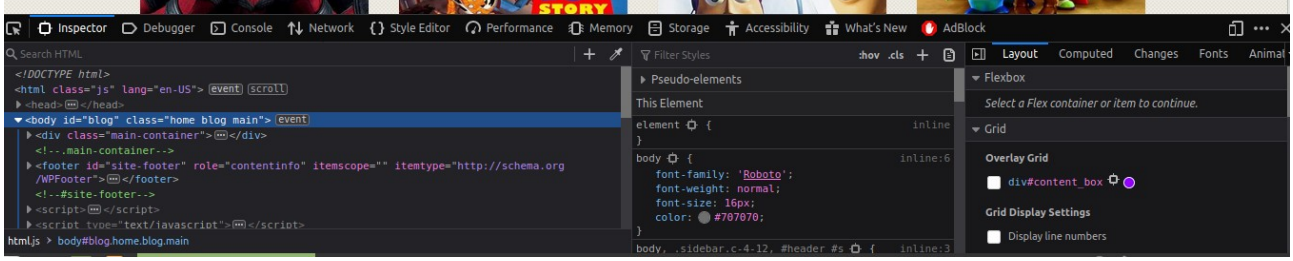
Download Batman: The Dark Knight Rises (2012) Dual Audio [Hindi-English] 480p [300MB Movie] || 720p [1.4GB] || 1080p [3.5GB]

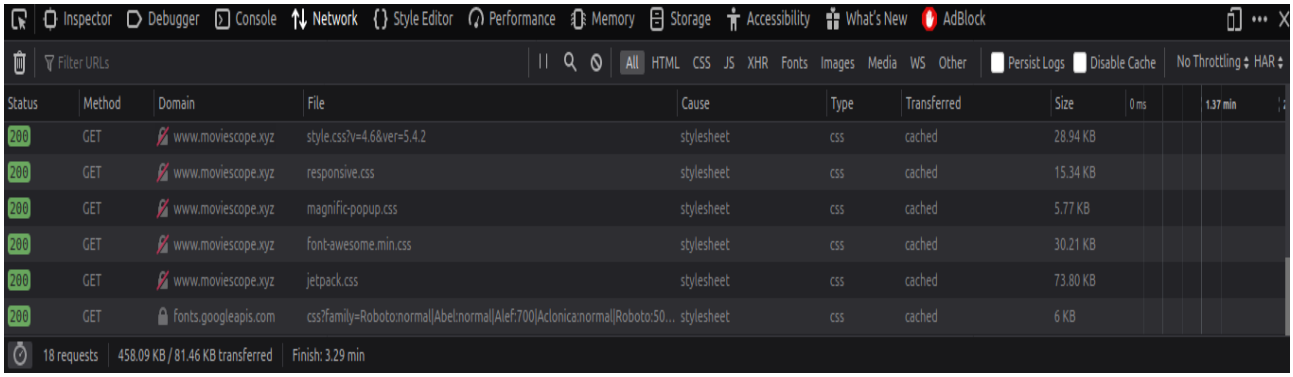
Download 30 Minutes Or Less (2011) Dual Audio Bluray 480p [450MB] || 720p [1.2GB]

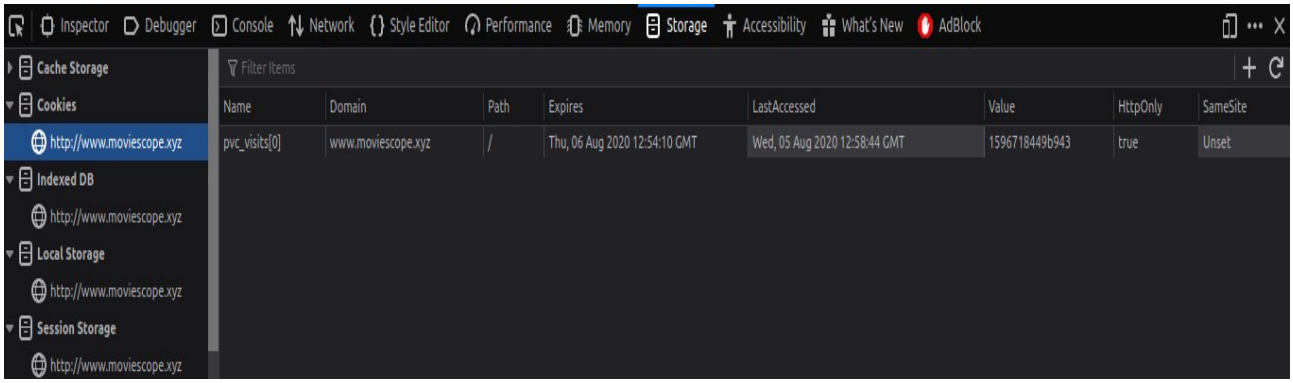
MOVIE SCOPE
www.moviescope.xyz

What are you looking for?

HOME | MOVIES | GENRE | QUALITY | YEAR | WEB-SERIES







2. Gathering IP and Domain Name Information using Whois Lookup lab analysis

Domain Information

Domain:	google.com
Registrar:	MarkMonitor Inc.
Registered On:	1997-09-15
Expires On:	2028-09-13
Updated On:	2019-09-09
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1.google.com ns2.google.com ns3.google.com ns4.google.com

Registrant Contact

Organization:	Google LLC
State:	CA
Country:	US
Email:	Select Request Email Form at https://domains.markmonitor.com /whois/google.com

Administrative Contact

Organization:	Google LLC
State:	CA
Country:	US
Email:	Select Request Email Form at https://domains.markmonitor.com /whois/google.com

Technical Contact

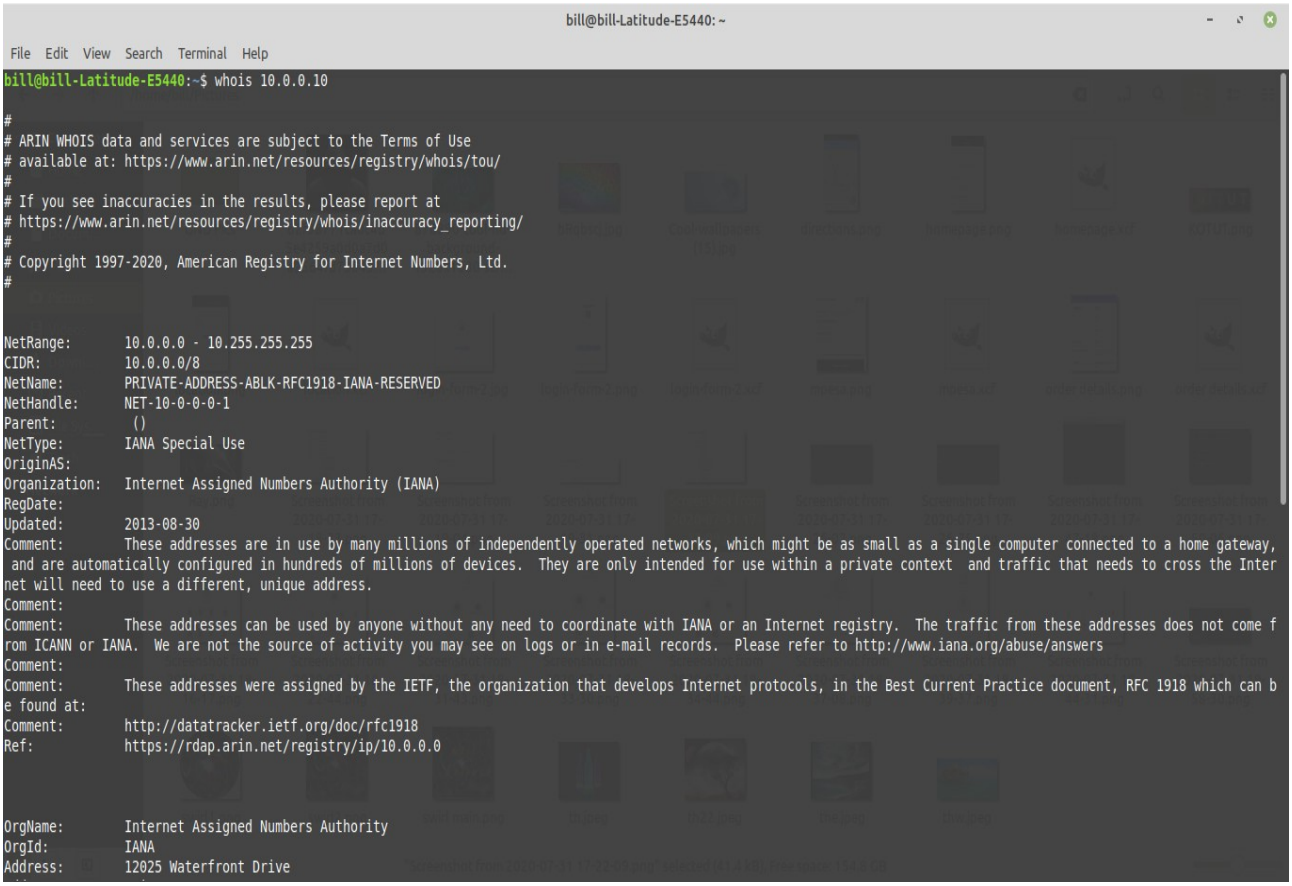
Organization:	Google LLC
State:	CA
Country:	US
Email:	Select Request Email Form at https://domains.markmonitor.com /whois/google.com

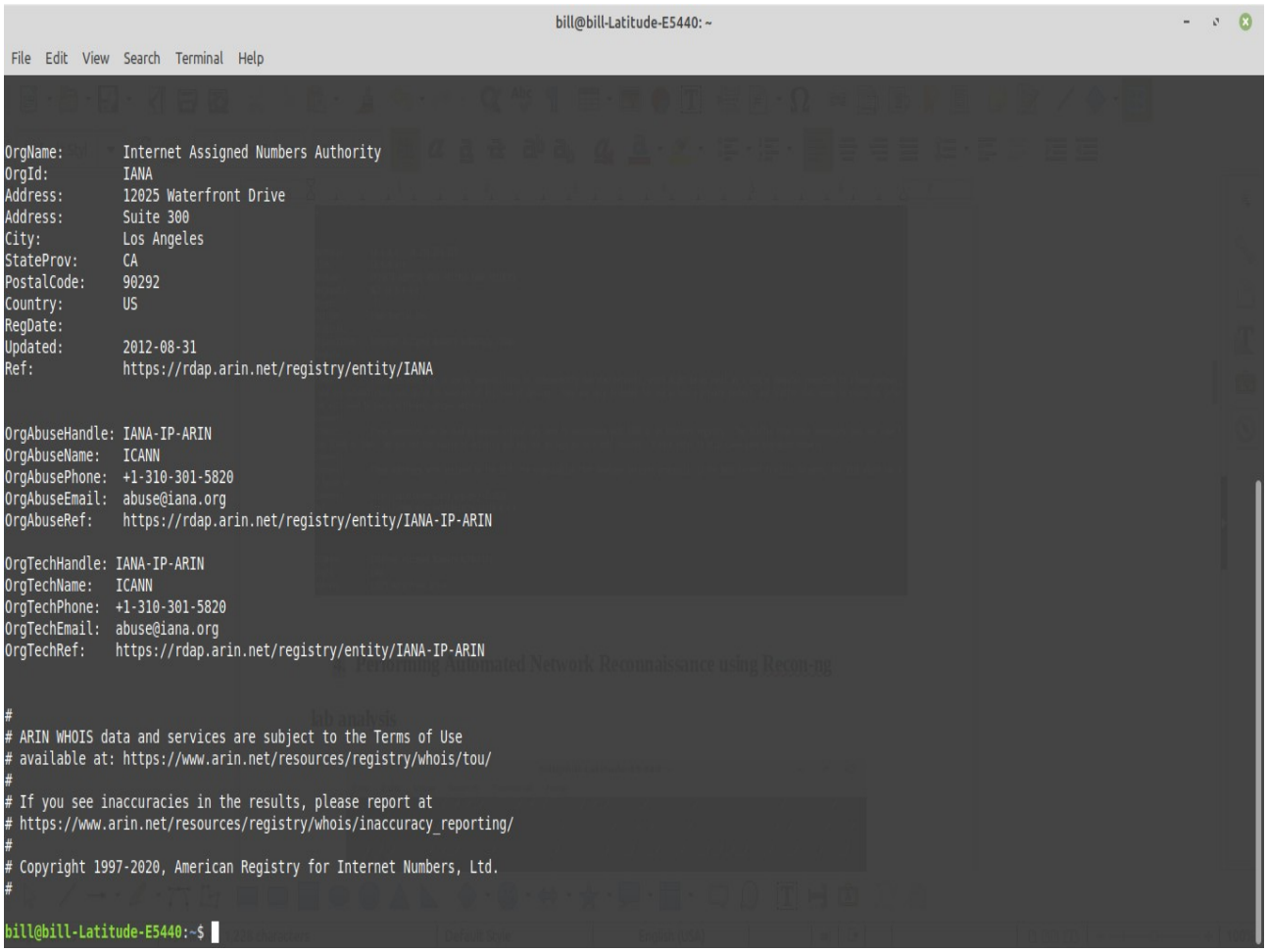
facebook.com

Domain Information

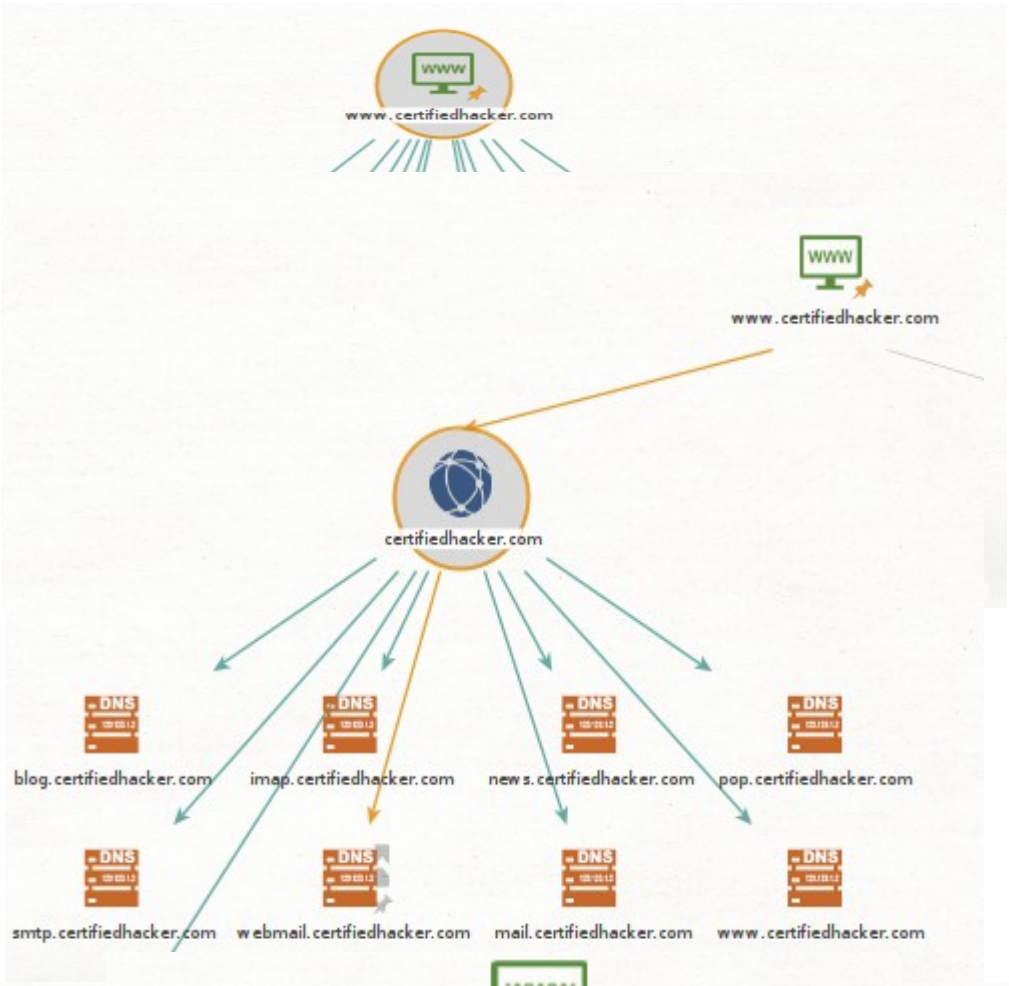
Domain:	facebook.com
Registrar:	RegistrarSafe, LLC
Registered On:	1997-03-29
Expires On:	2028-03-30
Updated On:	2020-03-10
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	a.ns.facebook.com b.ns.facebook.com c.ns.facebook.com d.ns.facebook.com

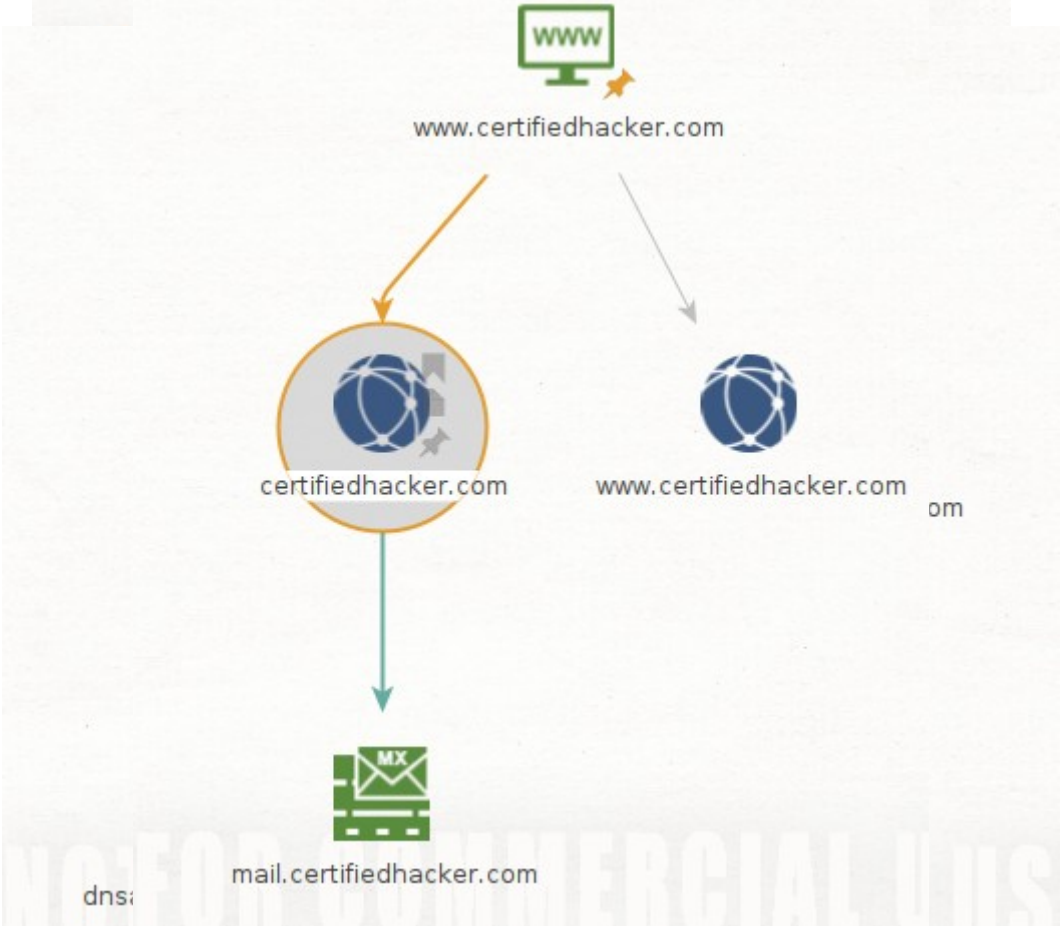
IP 10.0.0.10

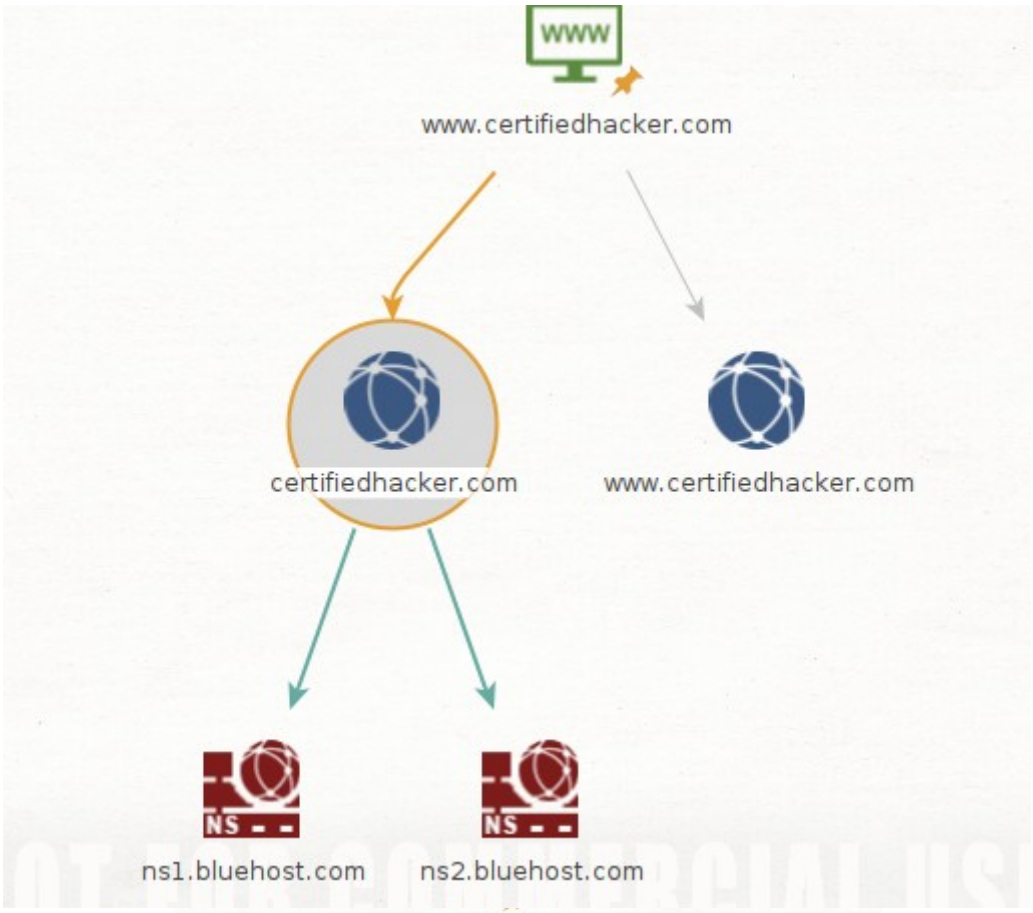

bill@bill-Latitude-E5440: ~
File Edit View Search Terminal Help
bill@bill-Latitude-E5440:~$ whois 10.0.0.10
#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/
#
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
Copyright 1997-2020, American Registry for Internet Numbers, Ltd.
#
NetRange: 10.0.0.0 - 10.255.255.255
CIDR: 10.0.0.0/8
NetName: PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED
NetHandle: NET-10-0-0-0-1
Parent: ()
NetType: IANA Special Use
OriginAS:
Organization: Internet Assigned Numbers Authority (IANA)
RegDate:
Updated: 2013-08-30
Comment: These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway,
and are automatically configured in hundreds of millions of devices. They are only intended for use within a private context and traffic that needs to cross the Inter
net will need to use a different, unique address.
Comment:
Comment: These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these addresses does not come f
rom ICANN or IANA. We are not the source of activity you may see on logs or in e-mail records. Please refer to http://www.iana.org/abuse/answers
Comment:
Comment: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC 1918 which can b
e found at:
Comment: http://datatracker.ietf.org/doc/rfc1918
Ref: https://rdap.arin.net/registry/ip/10.0.0.0
OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive


bill@bill-Latitude-E5440: ~
File Edit View Search Terminal Help
OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
StateProv: CA
PostalCode: 90292
Country: US
RegDate:
Updated: 2012-08-31
Ref: https://rdap.arin.net/registry/entity/IANA
OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName: ICANN
OrgAbusePhone: +1-310-301-5820
OrgAbuseEmail: abuse@iana.org
OrgAbuseRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN
OrgTechHandle: IANA-IP-ARIN
OrgTechName: ICANN
OrgTechPhone: +1-310-301-5820
OrgTechEmail: abuse@iana.org
OrgTechRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN
#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/
#
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
Copyright 1997-2020, American Registry for Internet Numbers, Ltd.
#
bill@bill-Latitude-E5440:~$

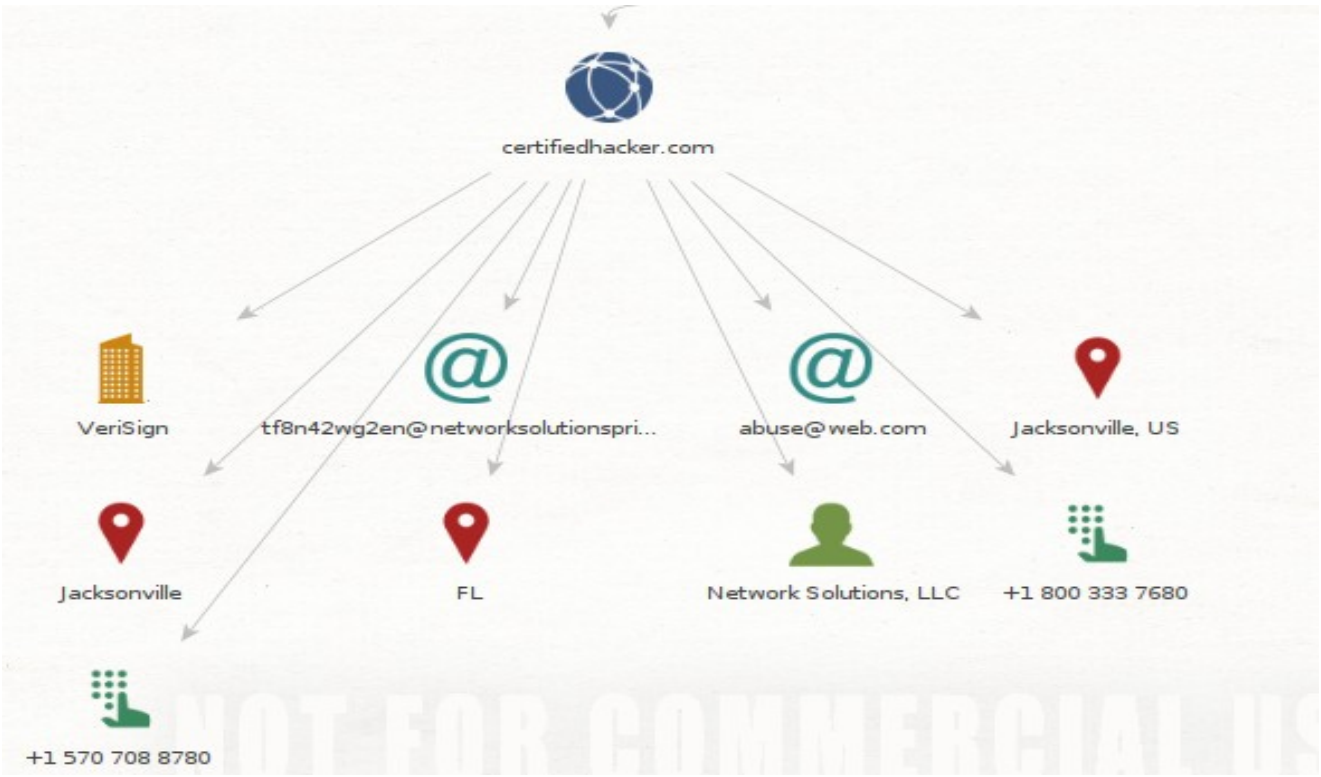
Footprinting a target using ,Maltego





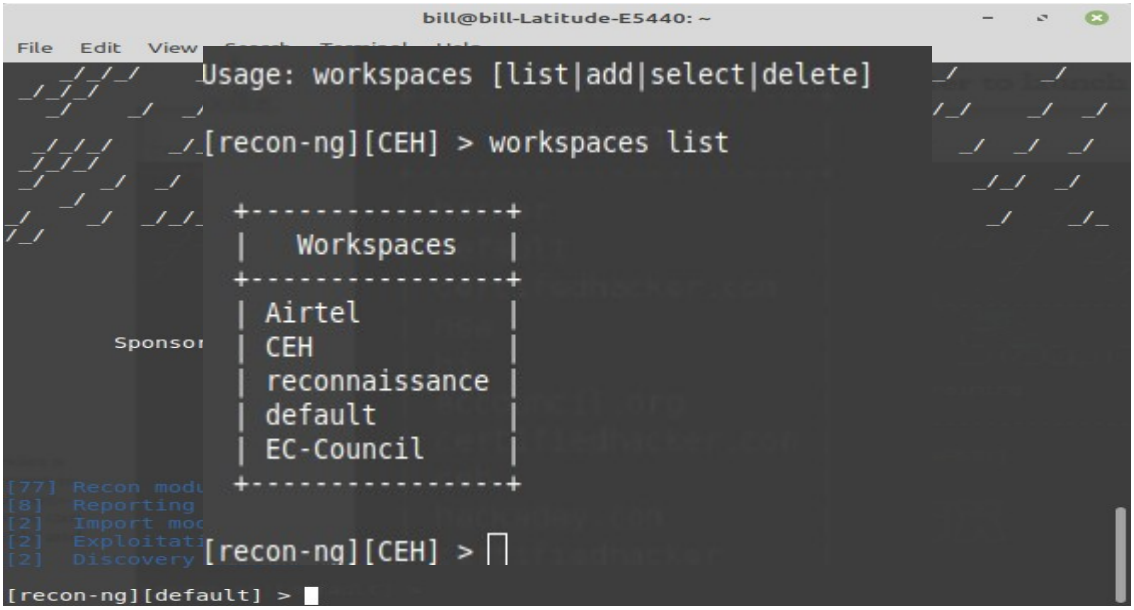

www
www.certifiedhacker.com
certifiedhacker.com
www.certifiedhacker.com
NS
NS
ns1.bluehost.com
ns2.bluehost.com


www.certifiedhacker.com
162.241.216.11
. (United States)



3. **Performing Automated Network Reconnaissance using Recon-ng**

lab analysis




```
[recon-ng][CEH] > show domains

  +-----------------------------------+
  | rowid |     domain    |   module   |
  +-----------------------------------+
  | 1     | microsoft.com | user_defined |
  +-----------------------------------+

[*] 1 rows returned
[recon-ng][CEH] > search netcraft
[*] Searching for 'netcraft'...

  Recon
  -----
    recon/domains-hosts/netcraft

[recon-ng][CEH] > load recon/domains-hosts/netcraft
[recon-ng][CEH][netcraft] > run

------------
MICROSOFT.COM
------------
[*] URL: http://searchdns.netcraft.com/?{'restriction': 'site+ends+with', 'host': 'microsoft.com'}
[*] Next page available! Requesting again...
[*] Sleeping to Avoid Lock-out...
[*] URL: http://searchdns.netcraft.com/?{'restriction': 'site+ends+with', 'host': 'microsoft.com', 'last': 'businessstore.microsoft.com', 'from': '21
[*] Next page available! Requesting again...
[*] Sleeping to Avoid Lock-out...
[*] URL: http://searchdns.netcraft.com/?{'restriction': 'site+ends+with', 'host': 'microsoft.com', 'last': 'rdweb.wvd.microsoft.com', 'from': '41'}
[*] Next page available! Requesting again...
[*] Sleeping to Avoid Lock-out...
^C
```

```
[recon-ng][CEH][netcraft] > load bing
[*] Multiple modules match 'bing'.

  Recon
  -----
    recon/companies-contacts/bing_linkedin_cache
    recon/domains-hosts/bing_domain_api
    recon/domains-hosts/bing_domain_web
    recon/hosts-hosts/bing_ip

[recon-ng][CEH][netcraft] > load recon/domains-hosts/bing_domain_web
[recon-ng][CEH][bing_domain_web] > run

-------------
MICROSOFT.COM
-------------
[*] URL: https://www.bing.com/search?first=0&q=domain%3Amicrosoft.com
[*] [host] www.microsoft.com (<blank>)
[*] [host] msdn.microsoft.com (<blank>)
[*] [host] mbs2.microsoft.com (<blank>)
[*] [host] myorder.microsoft.com (<blank>)
[*] [host] expertzone.microsoft.com (<blank>)
[*] [host] docs.microsoft.com (<blank>)
[*] [host] update.microsoft.com (<blank>)
[*] [host] answers.microsoft.com (<blank>)
[*] [host] www.msdn.microsoft.com (<blank>)
[*] [host] testconnectivity.microsoft.com (<blank>)
[*] [host] academic.microsoft.com (<blank>)
[*] [host] blogs.technet.microsoft.com (<blank>)
[*] [host] admin.powerplatform.microsoft.com (<blank>)
[*] [host] azure.microsoft.com (<blank>)
[*] [host] powerbi.microsoft.com (<blank>)
[*] [host] www.catalog.update.microsoft.com (<blank>)
```

```
-------
SUMMARY
-------
[*] 33 total (16 new) hosts found.
[recon-ng][CEH][bing_domain_web] > load brute
[*] Multiple modules match 'brute'.

  Exploitation
  ------------
    exploitation/injection/xpath_bruter

  Recon
  -----
    recon/domains-domains/brute_suffix
    recon/domains-hosts/brute_hosts

[recon-ng][CEH][bing_domain_web] > load recon/domains-hosts/brute_hosts
[recon-ng][CEH][brute_hosts] > run

-------------
MICROSOFT.COM
-------------
[*] No Wildcard DNS entry found.
[*] 1.microsoft.com => No record found.
[*] 0.microsoft.com => No record found.
[*] 01.microsoft.com => No record found.
[*] 03.microsoft.com => No record found.
[*] 02.microsoft.com => No record found.
[*] 10.microsoft.com => No record found.
[*] 13.microsoft.com => No record found.
[*] 11.microsoft.com => No record found.
[*] 12.microsoft.com => No record found.
[*] 14.microsoft.com => No record found.
[*] 15.microsoft.com => No record found.
[*] 16.microsoft.com => No record found.
[*] 17.microsoft.com => No record found.
[*] 18.microsoft.com => No record found.
```

```
-------
SUMMARY
-------
[*] 85 total (24 new) hosts found.
[recon-ng][CEH][brute_hosts] > load reverse resolve
[!] Invalid module name.
[recon-ng][CEH][brute_hosts] > load reverse_resolve
[*] Multiple modules match 'reverse_resolve'.

  Recon
  -----
    recon/hosts-hosts/reverse_resolve
    recon/netblocks-hosts/reverse_resolve

[recon-ng][CEH][brute_hosts] > load recon/hosts-hosts/reverse_resolve
[recon-ng][CEH][reverse_resolve] > run
[*] [host] a104-127-120-229.deploy.static.akamaitechnologies.com (104.127.120.229)
[*] 13.107.6.156 => No record found.
[*] 23.100.75.192 => No record found.
[*] [host] conformite-logiciels.com (134.170.185.46)
[*] [host] conformite-logiciels.com (134.170.188.221)
[*] 40.112.72.205 => No record found.
[*] 40.76.4.15 => No record found.
[*] 104.215.148.63 => No record found.
[*] 40.113.200.201 => No record found.
[*] 13.77.161.179 => No record found.
[*] 152.199.19.160 => No record found.
[*] 40.126.9.98 => No record found.
[*] 20.190.137.64 => No record found.
[*] 20.190.137.78 => No record found.
[*] 20.190.137.1 => No record found.
[*] [host] a104-121-246-117.deploy.static.akamaitechnologies.com (104.121.246.117)
[*] 13.107.42.21 => No record found.
[*] [host] a23-8-183-228.deploy.static.akamaitechnologies.com (23.8.183.228)
^C
```

```
-------
SUMMARY
-------
[*] 5 total (1 new) hosts found.
[recon-ng][CEH][reverse_resolve] > back
[recon-ng][CEH] > load reporting
[*] Multiple modules match 'reporting'.

  Reporting
  ---------
    reporting/csv
    reporting/html
    reporting/json
    reporting/list
    reporting/proxifier
    reporting/pushpin
    reporting/xlsx
    reporting/xml

[recon-ng][CEH] > load reporting/html
[recon-ng][CEH][html] > show options

  Name      Current Value                       Required  Description
  --------  ------------                        --------  -----------
  CREATOR   Bill                                yes       creator name for the report footer
  CUSTOMER  Microsoft Networks                  yes       customer name for the report header
  FILENAME  /home/bill/Desktop/CEH_results.html yes       path and filename for report output
  SANITIZE  True                                yes       mask sensitive data in the report

[recon-ng][CEH][html] > set FILENAME /home/bill/Desktop/CEH_results.html
FILENAME => /home/bill/Desktop/CEH_results.html
[recon-ng][CEH][html] > set CREATOR Bill
CREATOR => Bill
[recon-ng][CEH][html] >
[recon-ng][CEH][html] > set CUSTOMER Microsoft Networks
CUSTOMER => Microsoft Networks
[recon-ng][CEH][html] > run
[*] Report generated at '/home/bill/Desktop/CEH_results.html'.
[recon-ng][CEH][html] >
```

Microsoft Networks

www.recon-ng.com

Recon-ng Reconnaissance Report

[-] Summary

table	count
domains	1
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	133
contacts	0
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[+] Domains

[+] Hosts

Created by: Bill
Fri, Jul 31 2020 18:10:55

Using Open Source Reconnaissance Tool Recon-ng to Gather Personal Information

```
[recon-ng][reconnaissance] > workspaces list

  +----------------+
  |   Workspaces   |
  +----------------+
  | Airtel         |
  | CEH            |
  | reconnaissance |
  | default        |
  | EC-Council     |
  +----------------+

[recon-ng][reconnaissance] > load recon/domains-contacts/whois_pocs
[recon-ng][reconnaissance][whois_pocs] > show info

      Name: Whois POC Harvester
      Path: modules/recon/domains-contacts/whois_pocs.py
    Author: Tim Tomes (@LaNMaSteR53)

Description:
  Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the
  'contacts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  facebook.com   yes       source of input (see 'show info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][reconnaissance][whois_pocs] > set SOURCE facebook.com
SOURCE => facebook.com
```

```
[recon-ng][reconnaissance][whois_pocs] > run

------------
FACEBOOK.COM
------------
[*] URL: http://whois.arin.net/rest/pocs;domain=facebook.com
[*] URL: http://whois.arin.net/rest/poc/NOL17-ARIN
[*] [contact] Lea Neteork ops (leigha311@facebook.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/OPERA82-ARIN
[*] [contact] <blank> Operations (domain@facebook.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/BST184-ARIN
[*] [contact] Brandon Stout (bstout@facebook.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/DJW23-ARIN
[*] [contact] Darrell Wayne (tiffany.cameron.507@facebook.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/MZU-ARIN
[*] [contact] Mark Zuckerberg (zuck@thefacebook.com) - Whois contact

-------
SUMMARY
-------
[*] 5 total (0 new) contacts found.
[recon-ng][reconnaissance][whois_pocs] > back
[recon-ng][reconnaissance] > load recon/profiles-profiles/namechk
[recon-ng][reconnaissance][namechk] > set SOURCE MarkZuckerberg
SOURCE => MarkZuckerberg
[recon-ng][reconnaissance][namechk] > run
[*] Retrieving site data...

--------------
MARKZUCKERBERG
```

```
[recon-ng][reconnaissance][profiler] > run
[*] Retrieving https://raw.githubusercontent.com/WebBreacher/WhatsMyName/master/web_accounts_list.json...

 Looking Up Data For: Markzuckerberg
 ----------------------------------
[*] Checking: 7cup
[*] Checking: asciinema
[*] Checking: Audiojungle
[*] Checking: BiggerPockets
[*] Checking: Bookcrossing
[*] Checking: buymeacoffee
[*] Checking: championat
[*] Checking: Cloudflare
[*] Checking: cnet
[*] Checking: coroflot
[*] Checking: Codewars
[*] Checking: Coderwall
[*] Checking: crevado
[*] Checking: Dating.ru
[*] Checking: Designspriation
[*] Checking: dev.to
[*] Checking: Ello.co
[*] Checking: Eyeem
```

```
[*] [profile] MarkZuckerberg - Etsy (https://www.etsy.com/people/MarkZuckerberg)


-------
SUMMARY
-------
[*] 20 total (9 new) profiles found.
[recon-ng][reconnaissance][profiler] > back
[recon-ng][reconnaissance] > load reporting/html
[recon-ng][reconnaissance][html] > show info

     Name: HTML Report Generator
     Path: modules/reporting/html.py
   Author: Tim Tomes (@LaNMaSteR53)

Description:
  Creates a HTML report.

Options:
  Name      Current Value                          Required  Description
  --------  -------------                          --------  -----------
  CREATOR   Bill Kotut                             yes       creator name for the report footer
  CUSTOMER  Mark Zuckerberg                        yes       customer name for the report header
  FILENAME  /home/bill/Desktop/Reconnaissance.html yes       path and filename for report output
  SANITIZE  True                                   yes       mask sensitive data in the report
```

```
[recon-ng][reconnaissance][html] > set FILENAME /home/bill/Desktop/Reconnaissance.html
FILENAME => /home/bill/Desktop/Reconnaissance.html
[recon-ng][reconnaissance][html] > set CREATOR Bill Kotut
CREATOR => Bill Kotut
[recon-ng][reconnaissance][html] > set CUSTOMER Mark Zuckerberg
CUSTOMER => Mark Zuckerberg
[recon-ng][reconnaissance][html] > run
[*] Report generated at '/home/bill/Desktop/Reconnaissance.html'.
[recon-ng][reconnaissance][html] >
```

Mark Zuckerberg

www.recon-ng.com

Recon-ng Reconnaissance Report

[-] Summary

table	count
domains	0
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	0
contacts	5
credentials	0
leaks	0
pushpins	0
profiles	21
repositories	0

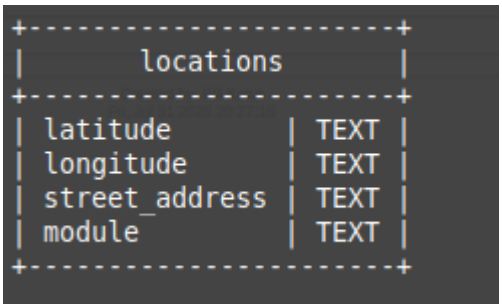
[+] Contacts

[+] Profiles

Created by: Bill Kotut
Fri, Jul 31 2020 20:27:15

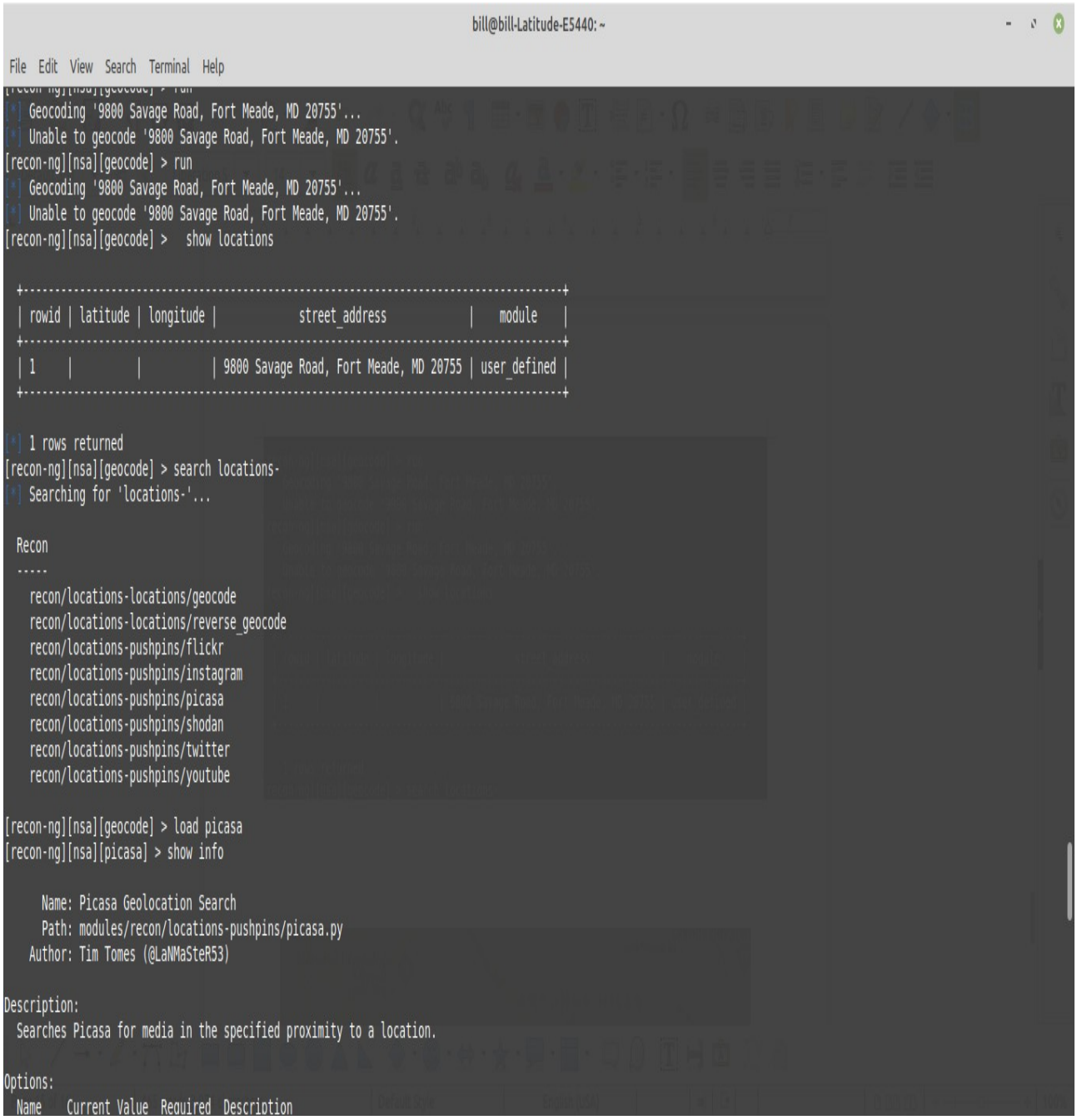
4. **Collecting Information from social Networking Sites using Recon-ng Pushpin**

lab analysis

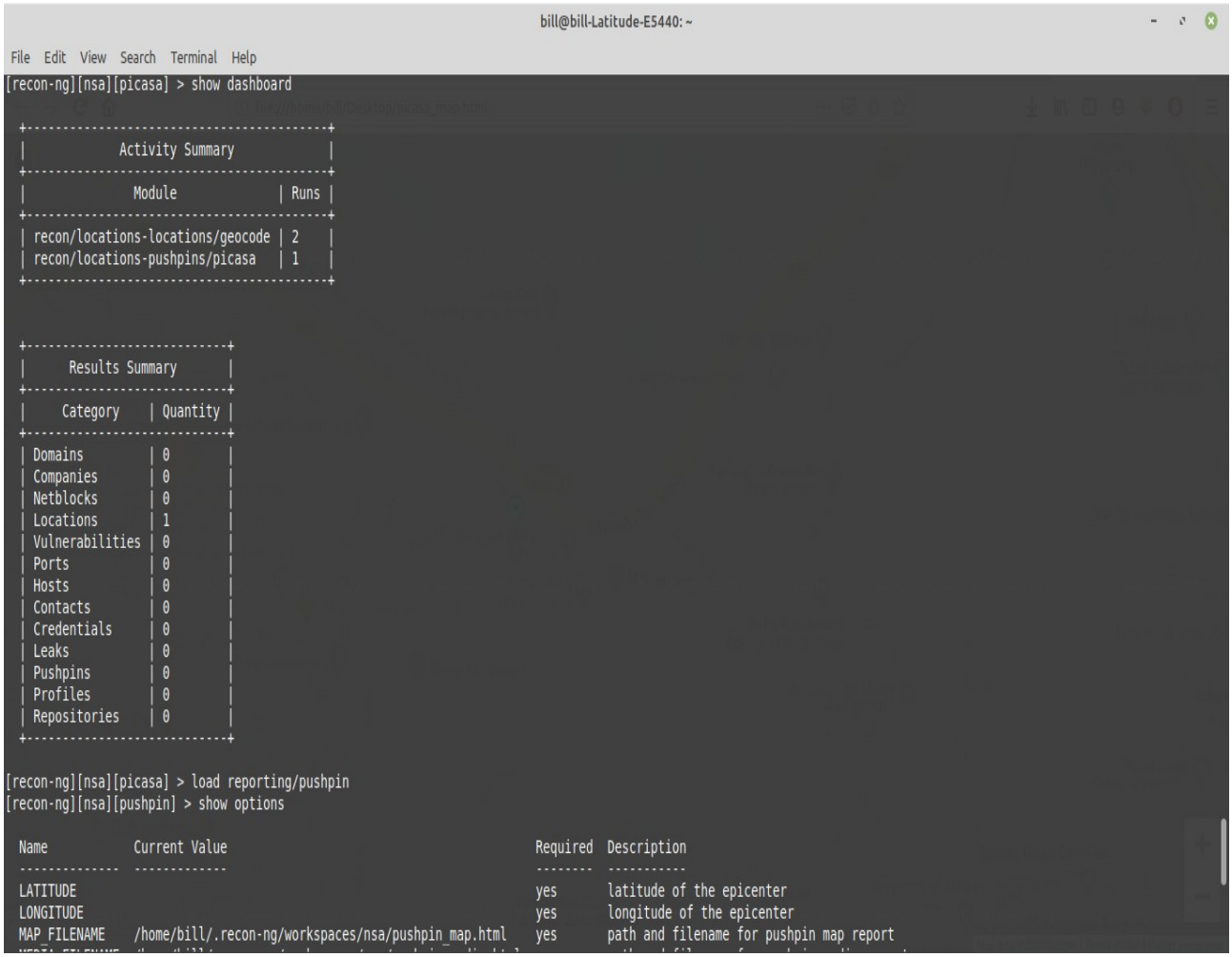


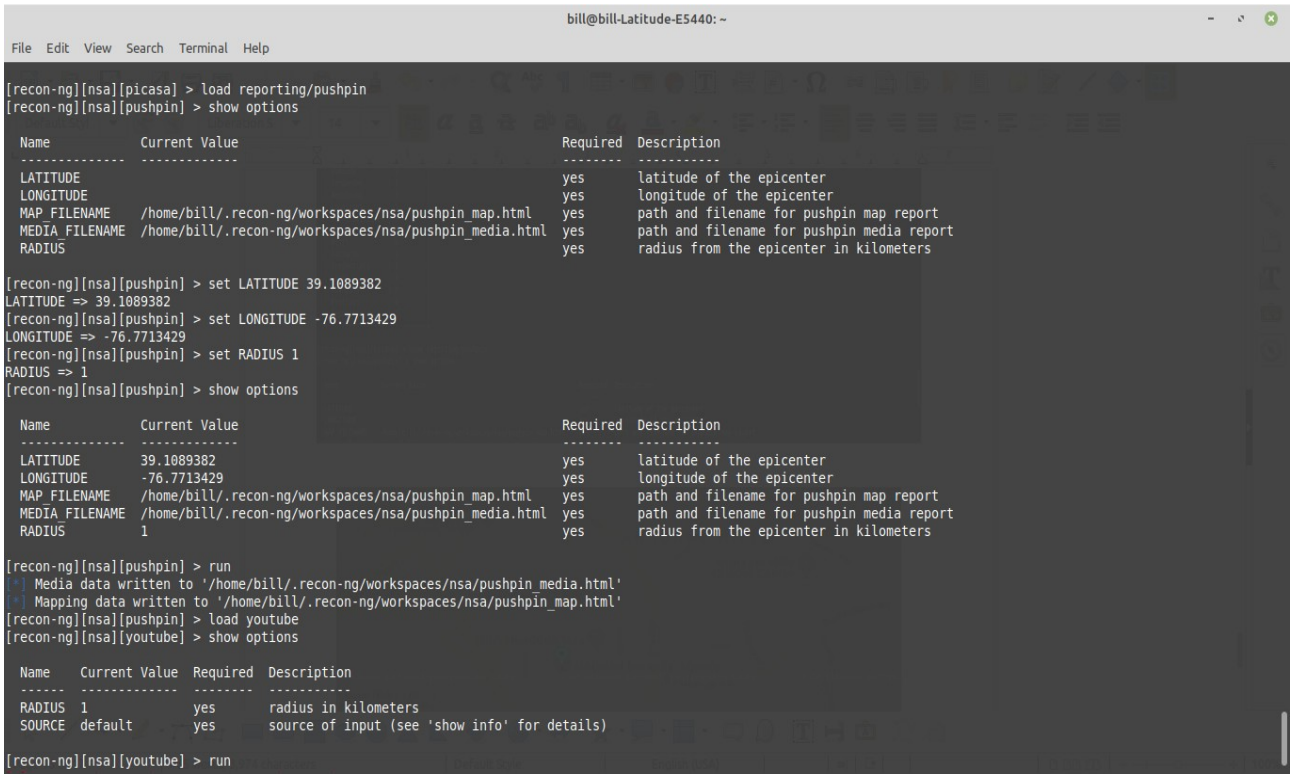
```
+----------------------+
|       locations      |
+----------------------+
| latitude       | TEXT |
| longitude      | TEXT |
| street_address | TEXT |
| module         | TEXT |
+----------------------+
```

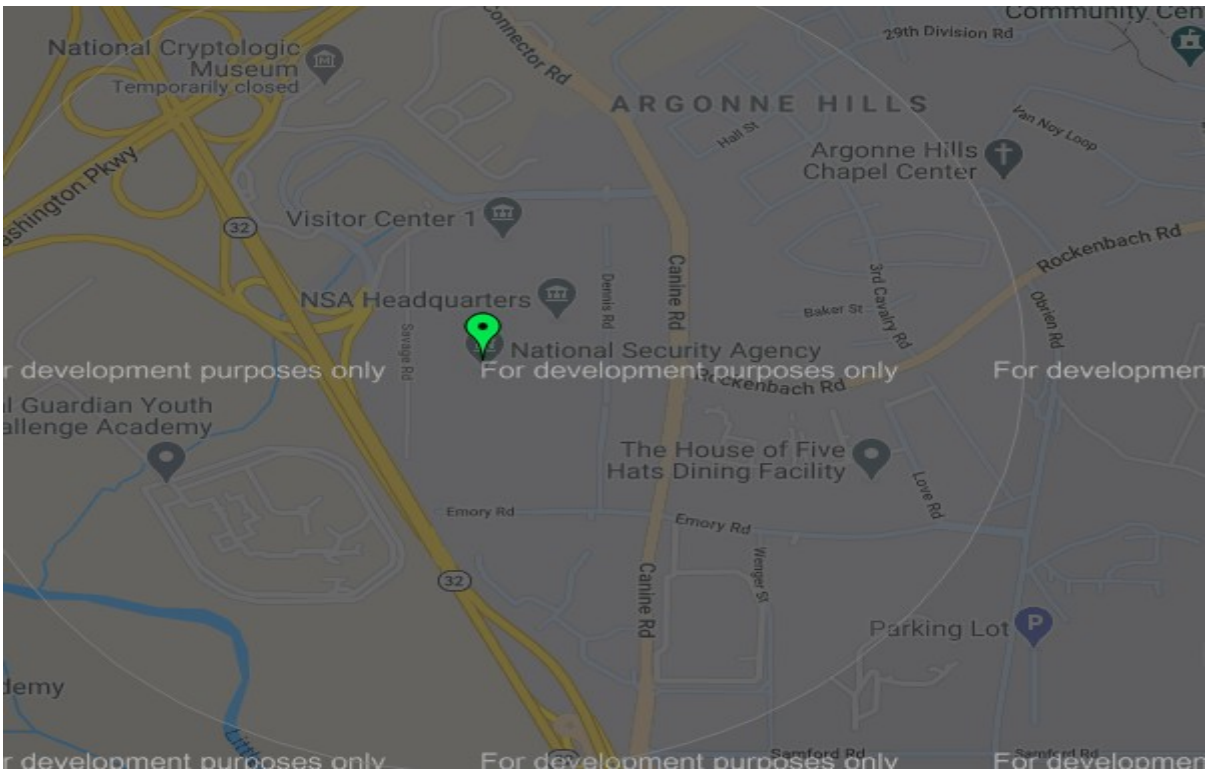
```
[recon-ng][nsa] > add locations
latitude (TEXT):
longitude (TEXT):
street_address (TEXT): 9800 Savage Road, Fort Meade, MD 20755
[recon-ng][nsa] > show locations

  +-------------------------------------------------------------------------------------+
  | rowid | latitude | longitude |            street_address            |    module    |
  +-------------------------------------------------------------------------------------+
  | 1     |          |           | 9800 Savage Road, Fort Meade, MD 20755 | user_defined |
  +-------------------------------------------------------------------------------------+

[*] 1 rows returned
[recon-ng][nsa] > load geocode
[*] Multiple modules match 'geocode'.
```

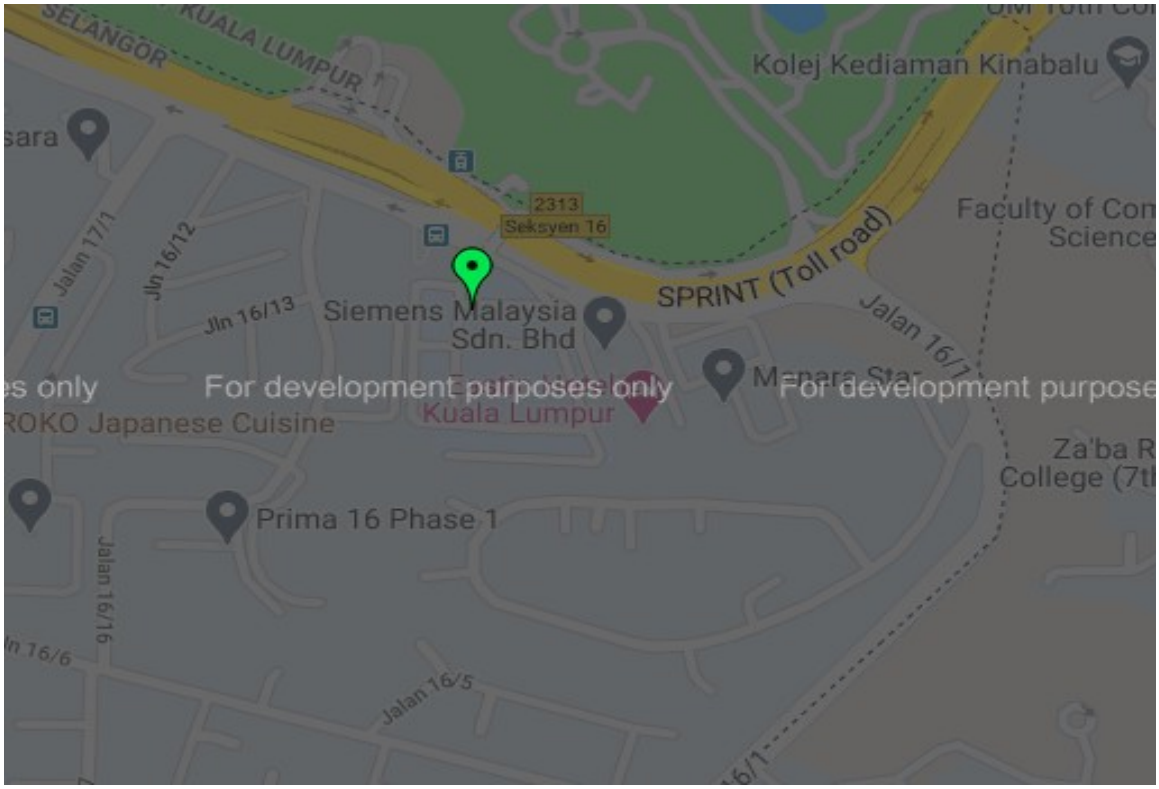



```
Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  RADIUS  1              yes       radius in kilometers
  SOURCE  default        yes       source of input (see 'show info' for details)

Source Options:
  default        SELECT DISTINCT latitude || ',' || longitude FROM locations WHERE latitude IS NOT
NULL AND longitude IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][nsa][picasa] > run
```

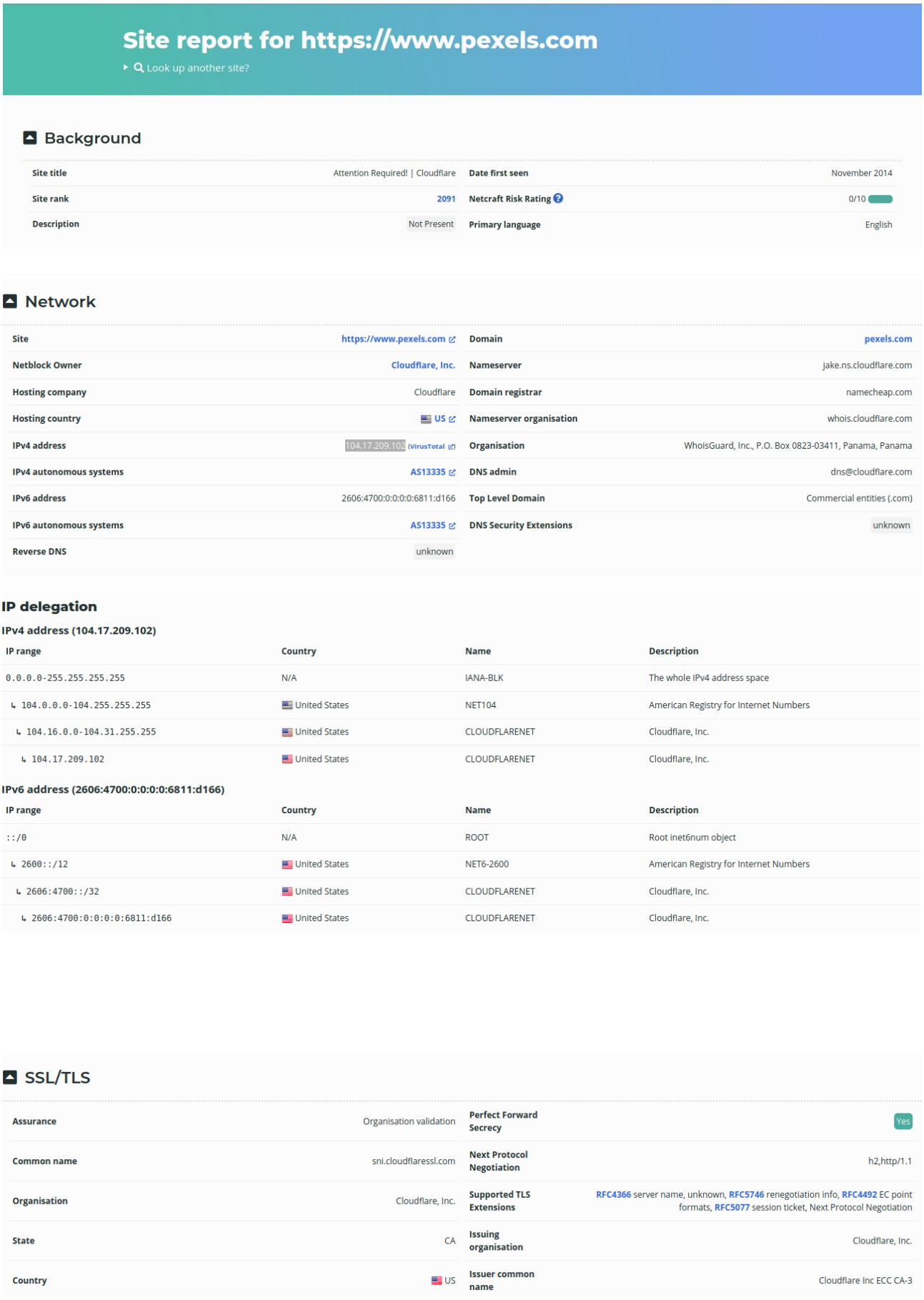

bill@bill-Latitude-E5440: ~
File Edit View Search Terminal Help
[recon-ng][nsa][picasa] > show dashboard
Activity Summary
Module | Runs
recon/locations-locations/geocode | 2
recon/locations-pushpins/picasa | 1
Results Summary
Category | Quantity
Domains | 0
Companies | 0
Netblocks | 0
Locations | 1
Vulnerabilities | 0
Ports | 0
Hosts | 0
Contacts | 0
Credentials | 0
Leaks | 0
Pushpins | 0
Profiles | 0
Repositories | 0
[recon-ng][nsa][picasa] > load reporting/pushpin
[recon-ng][nsa][pushpin] > show options
Name Current Value Required Description
LATITUDE yes latitude of the epicenter
LONGITUDE yes longitude of the epicenter
MAP_FILENAME /home/bill/.recon-ng/workspaces/nsa/pushpin_map.html yes path and filename for pushpin map report


bill@bill-Latitude-E5440: ~
File Edit View Search Terminal Help
[recon-ng][nsa][picasa] > load reporting/pushpin
[recon-ng][nsa][pushpin] > show options
Name Current Value Required Description
LATITUDE yes latitude of the epicenter
LONGITUDE yes longitude of the epicenter
MAP_FILENAME /home/bill/.recon-ng/workspaces/nsa/pushpin_map.html yes path and filename for pushpin map report
MEDIA_FILENAME /home/bill/.recon-ng/workspaces/nsa/pushpin_media.html yes path and filename for pushpin media report
RADIUS yes radius from the epicenter in kilometers
[recon-ng][nsa][pushpin] > set LATITUDE 39.1089382
LATITUDE => 39.1089382
[recon-ng][nsa][pushpin] > set LONGITUDE -76.7713429
LONGITUDE => -76.7713429
[recon-ng][nsa][pushpin] > set RADIUS 1
RADIUS => 1
[recon-ng][nsa][pushpin] > show options
Name Current Value Required Description
LATITUDE 39.1089382 yes latitude of the epicenter
LONGITUDE -76.7713429 yes longitude of the epicenter
MAP_FILENAME /home/bill/.recon-ng/workspaces/nsa/pushpin_map.html yes path and filename for pushpin map report
MEDIA_FILENAME /home/bill/.recon-ng/workspaces/nsa/pushpin_media.html yes path and filename for pushpin media report
RADIUS 1 yes radius from the epicenter in kilometers
[recon-ng][nsa][pushpin] > run
[*] Media data written to '/home/bill/.recon-ng/workspaces/nsa/pushpin_media.html'
[*] Mapping data written to '/home/bill/.recon-ng/workspaces/nsa/pushpin_map.html'
[recon-ng][nsa][pushpin] > load youtube
[recon-ng][nsa][youtube] > show options
Name Current Value Required Description
RADIUS 1 yes radius in kilometers
SOURCE default yes source of input (see 'show info' for details)
[recon-ng][nsa][youtube] > run


National Cryptologic Museum
Temporarily closed
ARGONNE HILLS
Argonne Hills Chapel Center
Visitor Center 1
NSA Headquarters
National Security Agency
For development purposes only
For development purposes only
For development purposes only
The House of Five Hats Dining Facility
Parking Lot
Emory Rd
Canine Rd
Rockenbach Rd
29th Division Rd
Hall St
Pan Noy Loop
Dennis Rd
Baker St
3rd Cavalry Rd
O'Brien Rd
Love Rd
Wenger St
Samford Rd


SELANGOR
KUALA LUMPUR
Kolej Kediaman Kinabalu
2313
Seksyen 16
SPRINT (Toll road)
Jalan 17/1
Jln 16/12
Jln 16/13
Siemens Malaysia Sdn. Bhd
Jalan 16/1
For development purposes only
For development purposes only
ROKO Japanese Cuisine
Kuala Lumpur
Prima 16 Phase 1
Jalan 16/16
Jalan 16/5
Faculty of Com Science
College (7t

Automated Fingerprinting of an Organization Using Netcraft



Site report for https://www.pexels.com

Look up another site?

Background

Site title	Attention Required! | Cloudflare	**Date first seen**	November 2014
Site rank	2091	**Netcraft Risk Rating**	0/10
Description	Not Present	**Primary language**	English

Network

Site	https://www.pexels.com	**Domain**	pexels.com
Netblock Owner	Cloudflare, Inc.	**Nameserver**	jake.ns.cloudflare.com
Hosting company	Cloudflare	**Domain registrar**	namecheap.com
Hosting country	US	**Nameserver organisation**	whois.cloudflare.com
IPv4 address	104.17.209.102 (VirusTotal)	**Organisation**	WhoisGuard, Inc., P.O. Box 0823-03411, Panama, Panama
IPv4 autonomous systems	AS13335	**DNS admin**	dns@cloudflare.com
IPv6 address	2606:4700:0:0:0:0:6811:d166	**Top Level Domain**	Commercial entities (.com)
IPv6 autonomous systems	AS13335	**DNS Security Extensions**	unknown
Reverse DNS	unknown		

IP delegation

IPv4 address (104.17.209.102)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 104.0.0.0-104.255.255.255	United States	NET104	American Registry for Internet Numbers
↳ 104.16.0.0-104.31.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 104.17.209.102	United States	CLOUDFLARENET	Cloudflare, Inc.

IPv6 address (2606:4700:0:0:0:0:6811:d166)

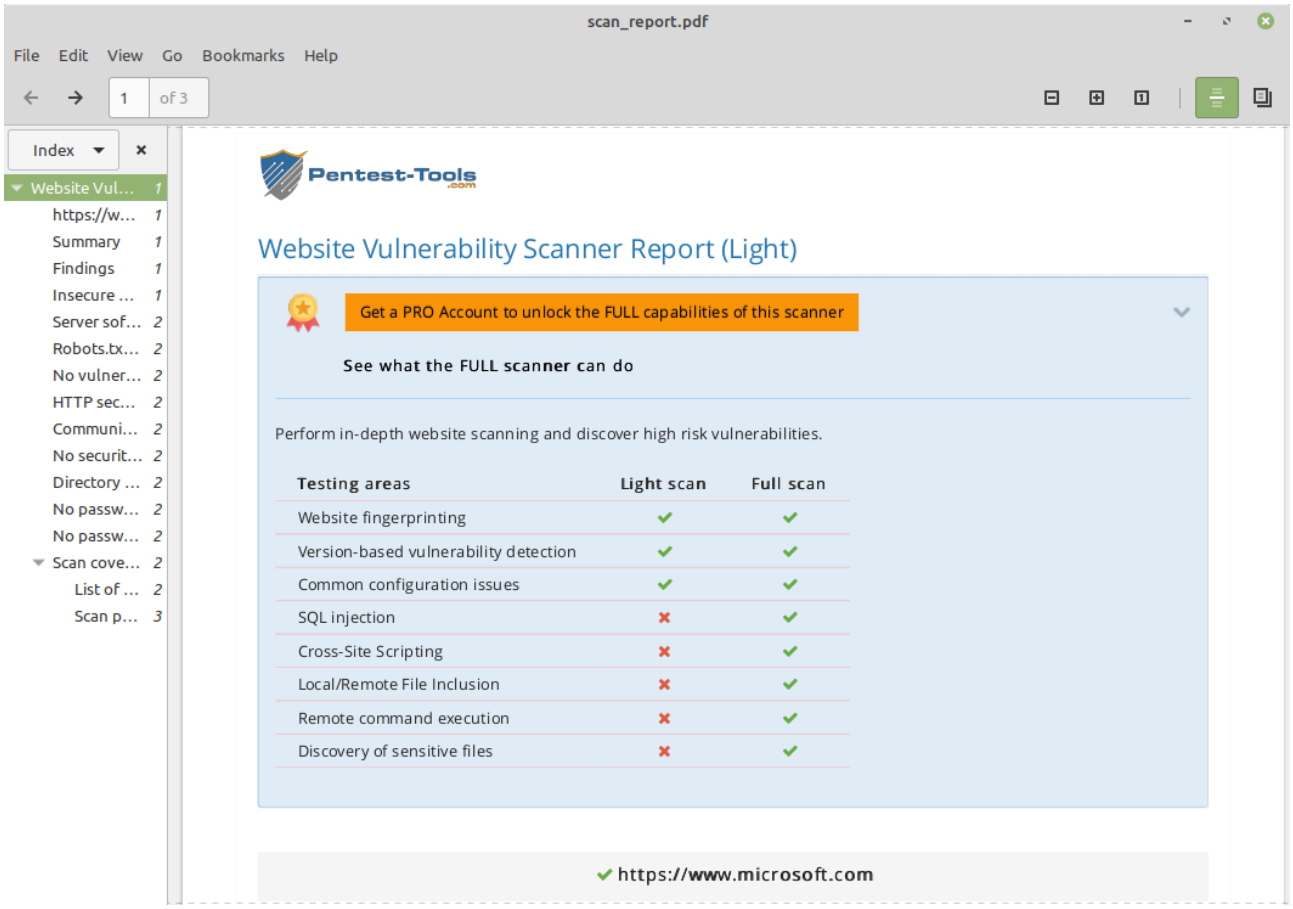
IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
↳ 2600::/12	United States	NET6-2600	American Registry for Internet Numbers
↳ 2606:4700::/32	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 2606:4700:0:0:0:0:6811:d166	United States	CLOUDFLARENET	Cloudflare, Inc.

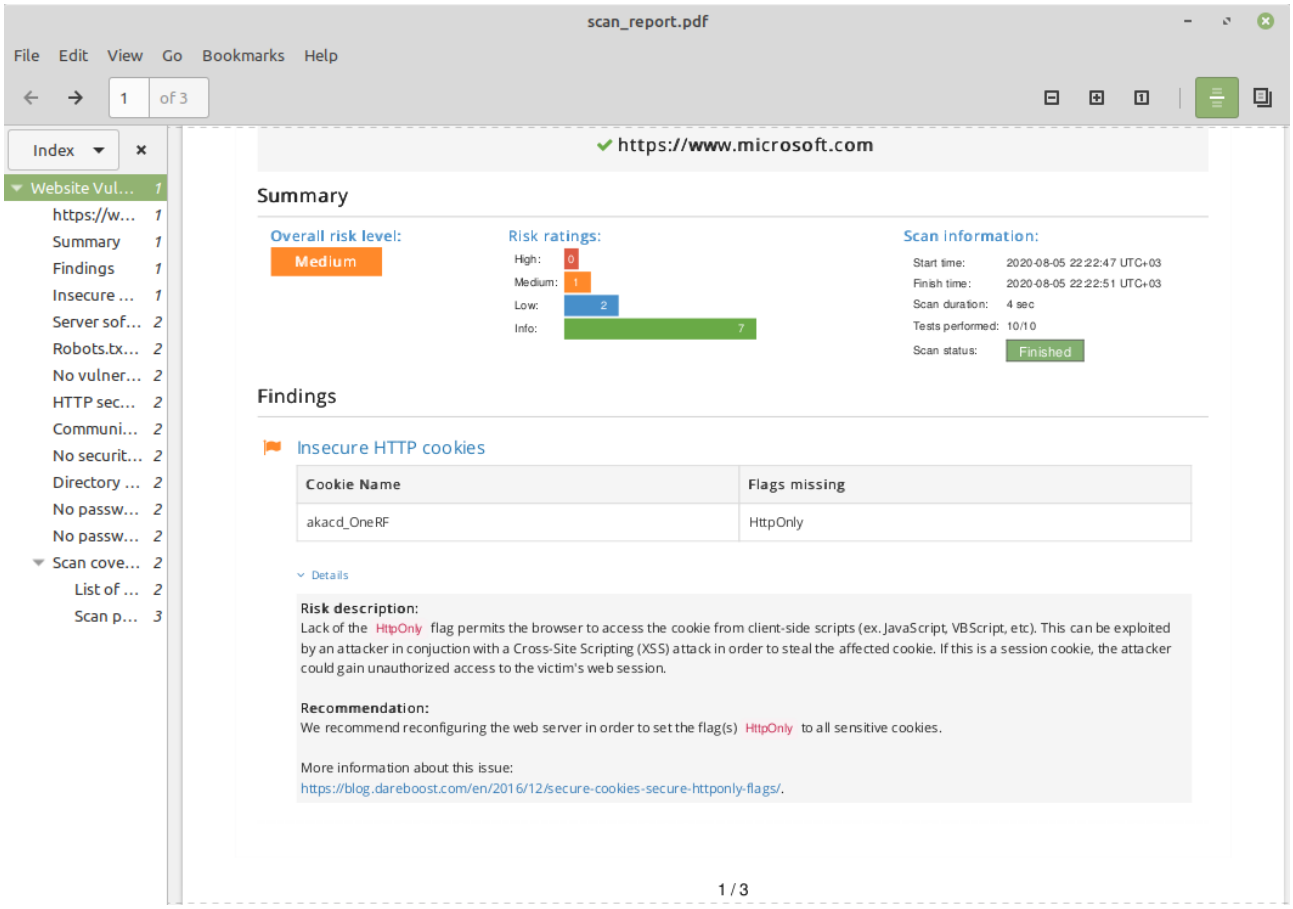
SSL/TLS

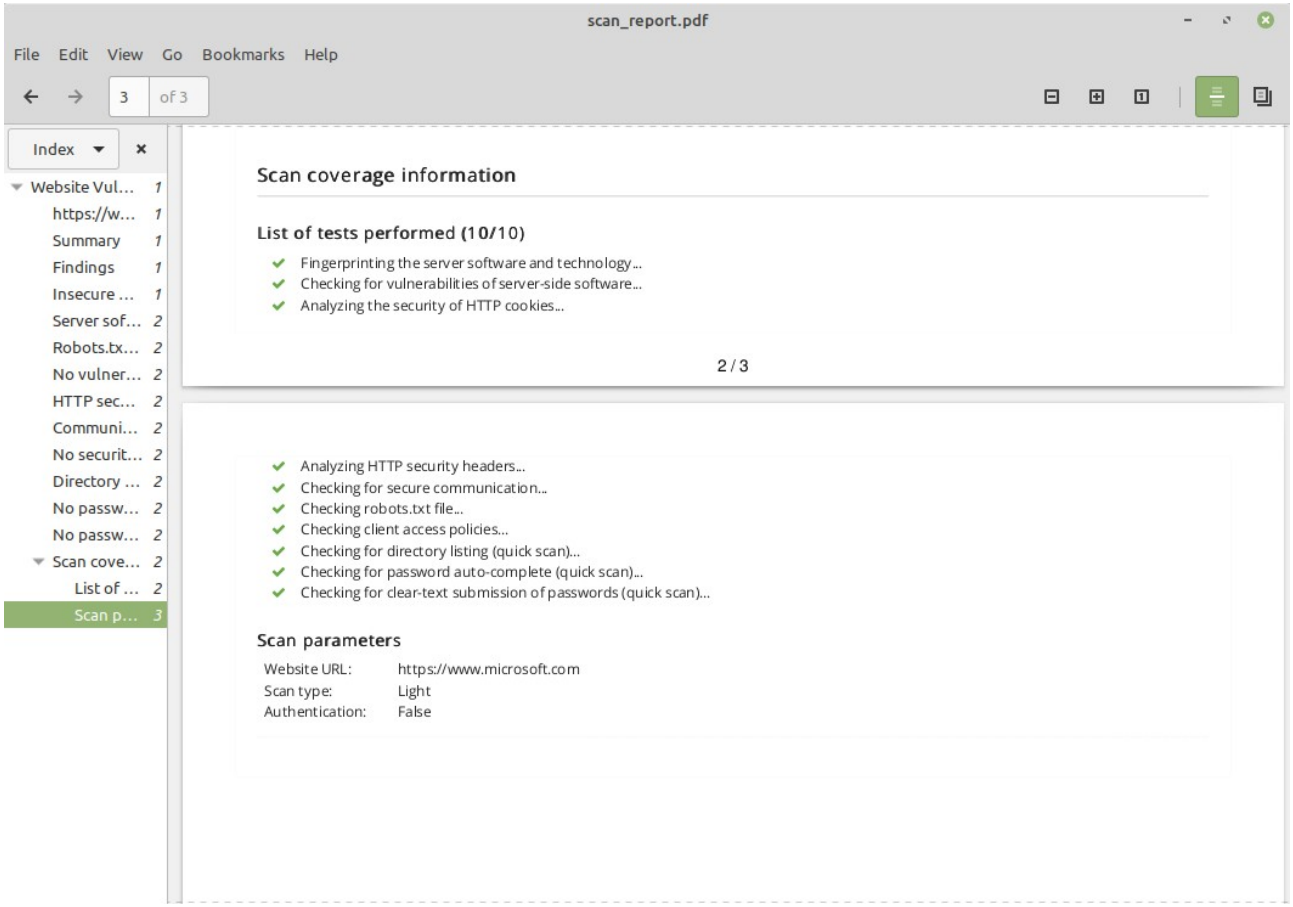
Assurance	Organisation validation	**Perfect Forward Secrecy**	Yes
Common name	sni.cloudflaressl.com	**Next Protocol Negotiation**	h2,http/1.1
Organisation	Cloudflare, Inc.	**Supported TLS Extensions**	RFC4366 server name, unknown, RFC5746 renegotiation info, RFC4492 EC point formats, RFC5077 session ticket, Next Protocol Negotiation
State	CA	**Issuing organisation**	Cloudflare, Inc.
Country	US	**Issuer common name**	Cloudflare Inc ECC CA-3

Organisational unit	Not Present	**Issuer unit**	Not Present
Subject Alternative Name	*.pexels.com, pexels.com, sni.cloudflaressl.com	**Issuer location**	Not Present
Validity period	From Aug 5 2020 to Aug 5 2021 (12 months)	**Issuer country**	US
Matches hostname	Yes	**Issuer state**	Not Present
Server	cloudflare	**Certificate Revocation Lists**	http://crl3.digicert.com/CloudflareIncECCCA-3.crl http://crl4.digicert.com/CloudflareIncECCCA-3.crl
Public key algorithm	id-ecPublicKey	**Certificate Hash**	moBky8OcfH3Hw7PnfP9Y7b87mAM
Protocol version	TLSv1.2	**Public Key Hash**	6e9f2b46904c54ea13c5cc89ba0059be905850801ed12ad9481863361709ba72
Public key length	256	**OCSP servers**	http://ocsp.digicert.com - *100% uptime in the past 24 hours*
Certificate check	ok	**OCSP stapling response**	No response received

Identifying Vulnerabilities and Information Disclosures in Search Engines Using Website Vulnerability Scanner


scan_report.pdf
File Edit View Go Bookmarks Help
1 of 3
Index
Website Vul... 1
https://w... 1
Summary 1
Findings 1
Insecure ... 1
Server sof... 2
Robots.tx... 2
No vulner... 2
HTTP sec... 2
Communi... 2
No securit... 2
Directory ... 2
No passw... 2
No passw... 2
Scan cove... 2
List of ... 2
Scan p... 3
Pentest-Tools .com
Website Vulnerability Scanner Report (Light)
Get a PRO Account to unlock the FULL capabilities of this scanner
See what the FULL scanner can do
Perform in-depth website scanning and discover high risk vulnerabilities.
Testing areas
Light scan
Full scan
Website fingerprinting
Version-based vulnerability detection
Common configuration issues
SQL injection
Cross-Site Scripting
Local/Remote File Inclusion
Remote command execution
Discovery of sensitive files
https://www.microsoft.com


scan_report.pdf
File Edit View Go Bookmarks Help
1 of 3
Index
Website Vul... 1
https://w... 1
Summary 1
Findings 1
Insecure ... 1
Server sof... 2
Robots.tx... 2
No vulner... 2
HTTP sec... 2
Communi... 2
No securit... 2
Directory ... 2
No passw... 2
No passw... 2
Scan cove... 2
List of ... 2
Scan p... 3
https://www.microsoft.com
Summary
Overall risk level:
Medium
Risk ratings:
High: 0
Medium: 1
Low: 2
Info: 7
Scan information:
Start time: 2020-08-05 22:22:47 UTC+03
Finish time: 2020-08-05 22:22:51 UTC+03
Scan duration: 4 sec
Tests performed: 10/10
Scan status: Finished
Findings
Insecure HTTP cookies
Cookie Name
Flags missing
akacd_OneRF
HttpOnly
Details
Risk description:
Lack of the HttpOnly flag permits the browser to access the cookie from client-side scripts (ex. JavaScript, VBScript, etc). This can be exploited by an attacker in conjuction with a Cross-Site Scripting (XSS) attack in order to steal the affected cookie. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.
Recommendation:
We recommend reconfiguring the web server in order to set the flag(s) HttpOnly to all sensitive cookies.
More information about this issue:
https://blog.dareboost.com/en/2016/12/secure-cookies-secure-httponly-flags/.
1 / 3


scan_report.pdf
File Edit View Go Bookmarks Help
3 of 3
Index
Website Vul... 1
https://w... 1
Summary 1
Findings 1
Insecure ... 1
Server sof... 2
Robots.tx... 2
No vulner... 2
HTTP sec... 2
Communi... 2
No securit... 2
Directory ... 2
No passw... 2
No passw... 2
Scan cove... 2
List of ... 2
Scan p... 3
Scan coverage information
List of tests performed (10/10)
Fingerprinting the server software and technology...
Checking for vulnerabilities of server-side software...
Analyzing the security of HTTP cookies...
2 / 3
Analyzing HTTP security headers...
Checking for secure communication...
Checking robots.txt file...
Checking client access policies...
Checking for directory listing (quick scan)...
Checking for password auto-complete (quick scan)...
Checking for clear-text submission of passwords (quick scan)...
Scan parameters
Website URL: https://www.microsoft.com
Scan type: Light
Authentication: False