Module 1: Introduction to Cybersecurity & Ethical Hacking

Demo Document 1

edureka!

© Brain4ce Education Solutions Pvt. Ltd.

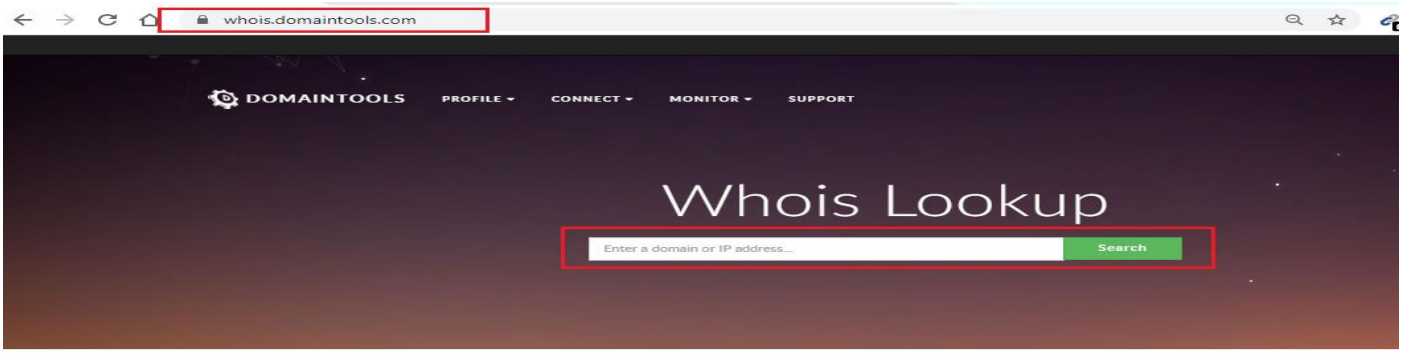
Demo 1: Gathering Information about Website

Problem Statement:

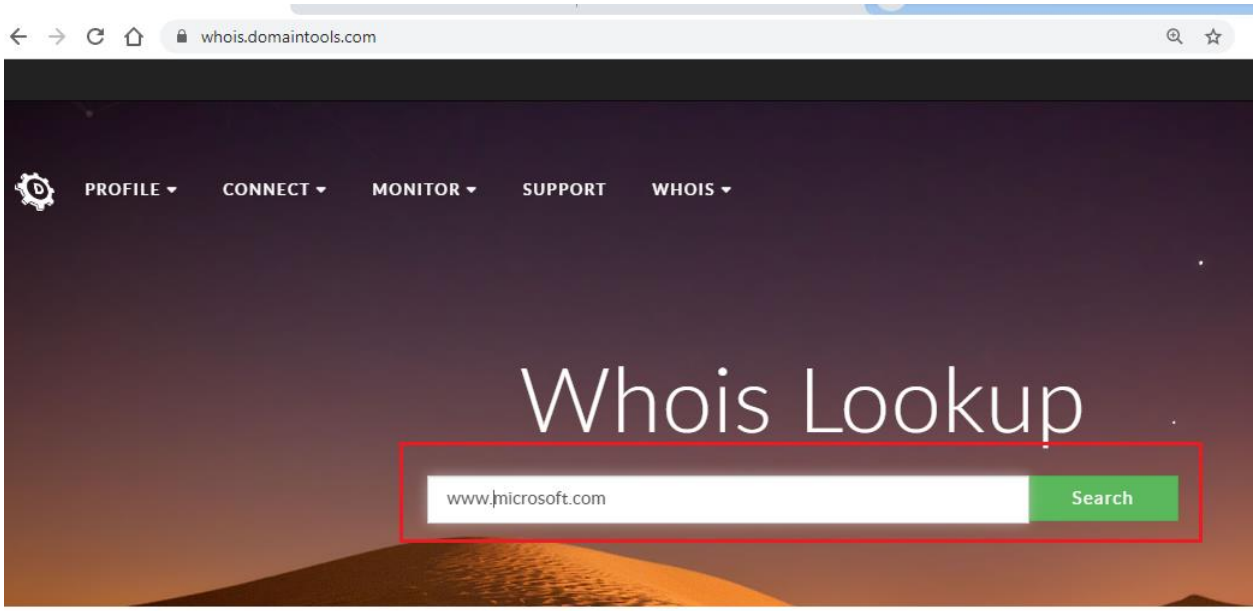
Gathering information about website and server information by using online resources.

Solution:

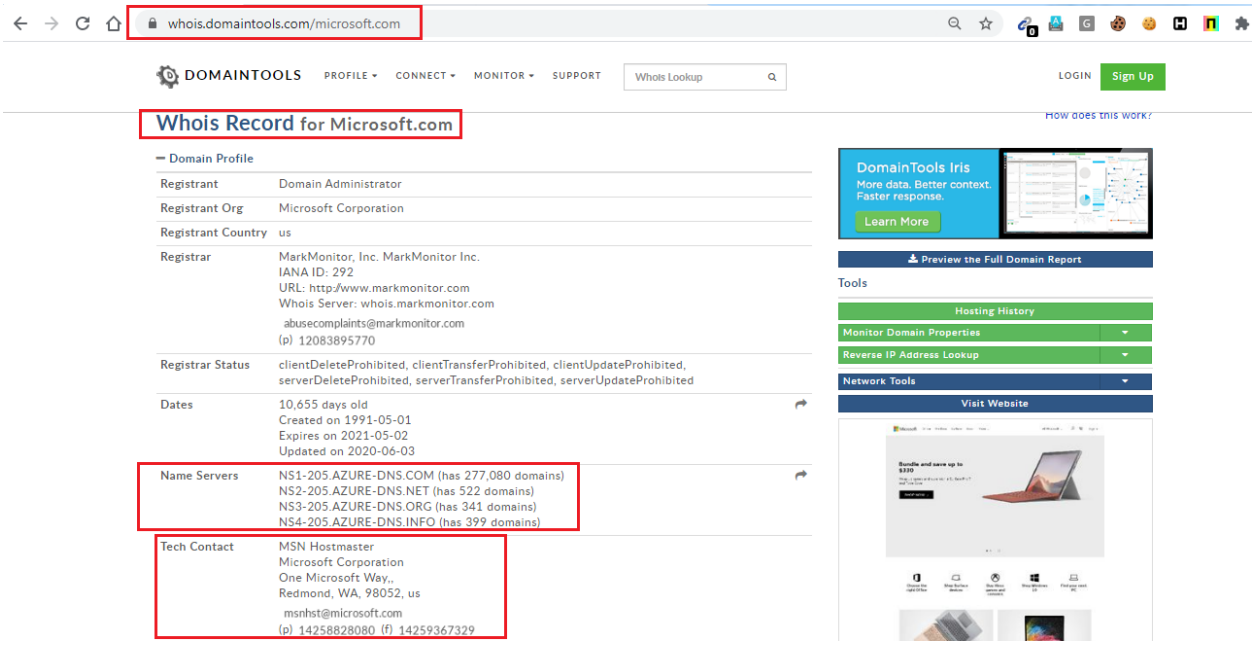
Step 1: Open the browser and go to https://whois.domaintools.com (will collect basic info from Domaintools website).



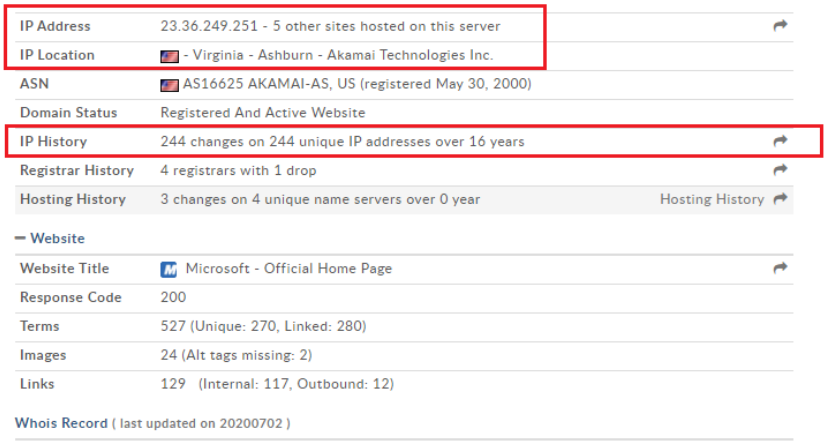
Step 2: Enter the domain name (www.microsoft.com) and click on **search**.

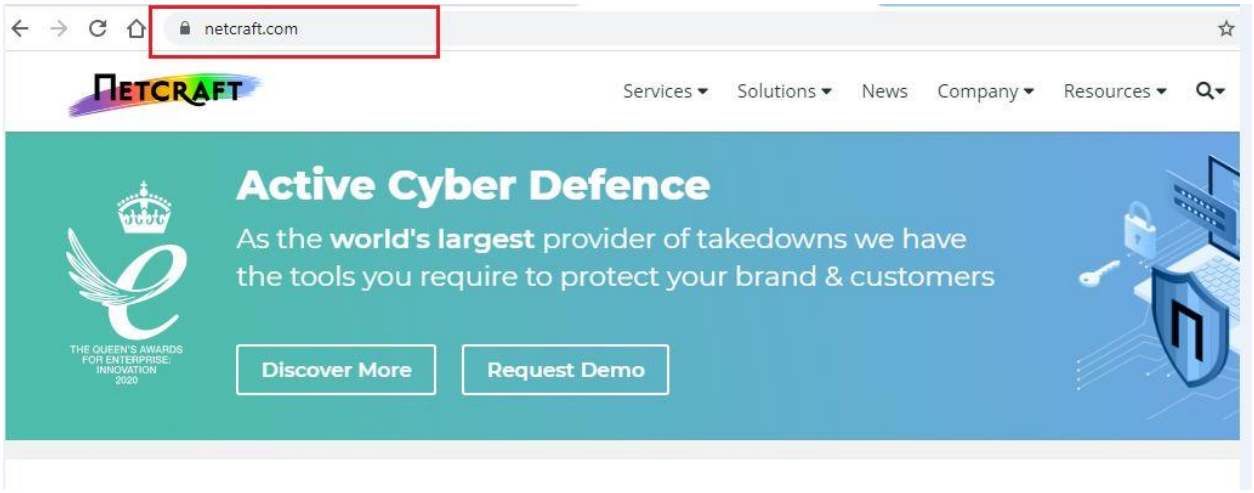


Step 3: Results will be shown in Whois Record for microsoft.com, and you can find the Nameservers and Tech Contact information on the website.



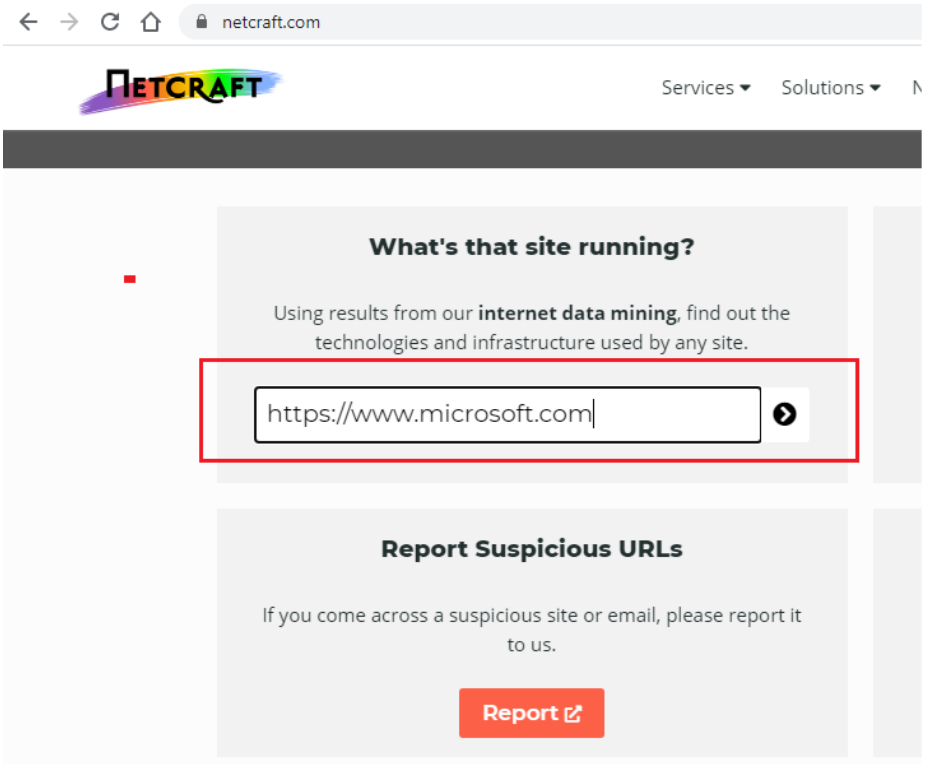
Step 4: You can find the details related to the IP address and location of the IP address, and brief info about IP changes history.



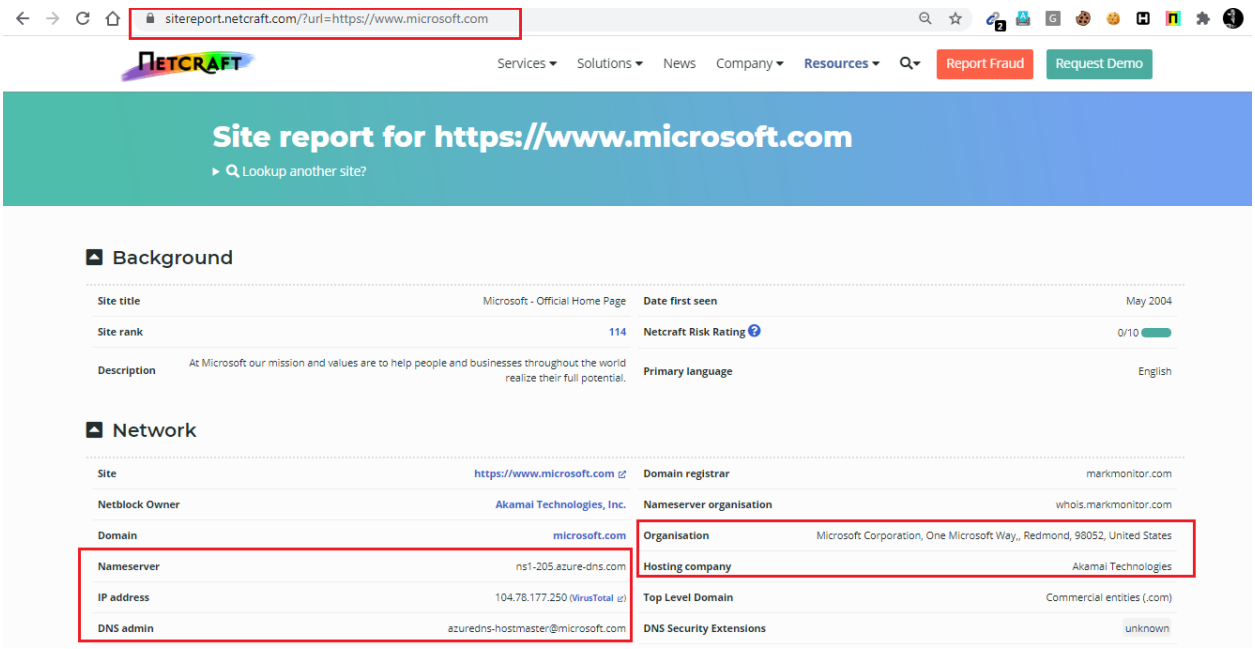


Now we will deep dive into information gathering about domain with (www.netcraft.com).

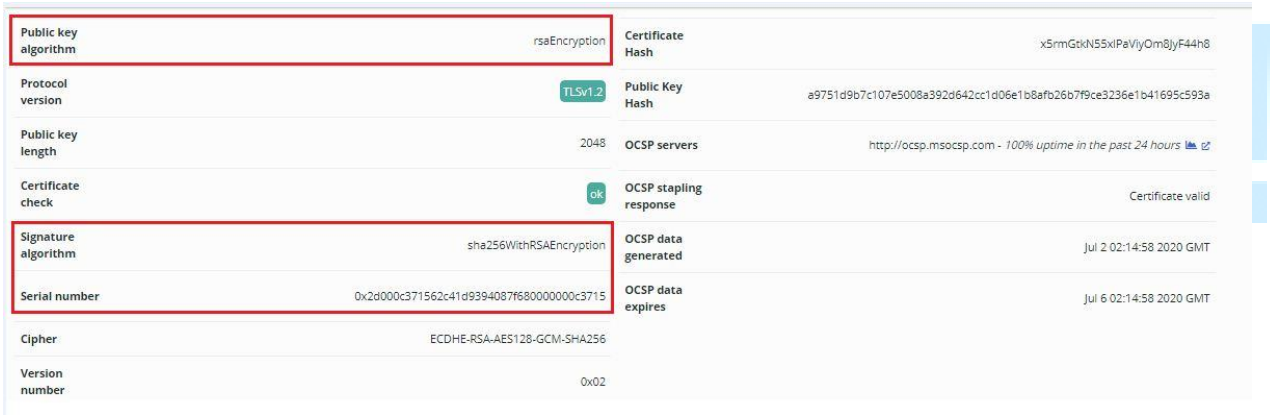
Step 5: Open www.netcraft.com website and scroll down to enter the target website (www.microsoft.com) and click on **Go**.

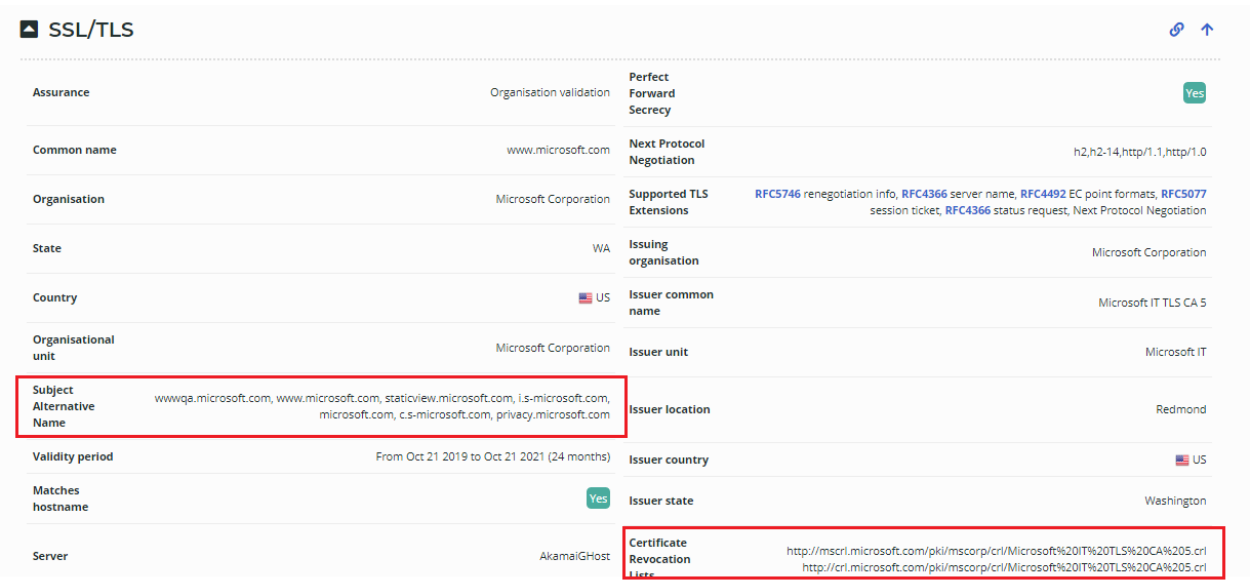


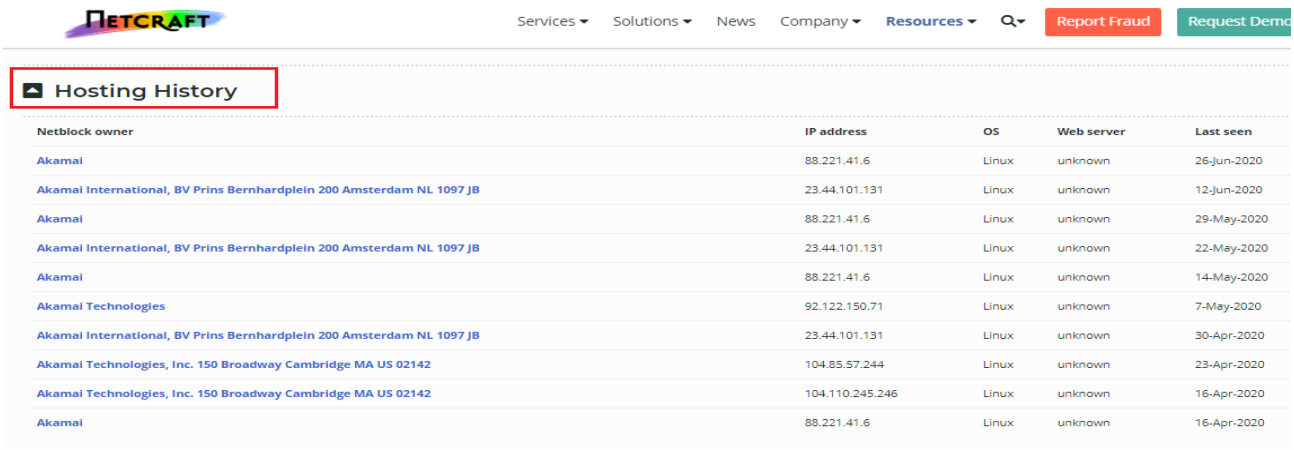
Step 6: Netcraft will generate the report. You can get the NameServer Details, Organization, Hosting Company, and DSN Admin details.



Step 7: You can gather information about the public algorithm, serial number, and IP history details.

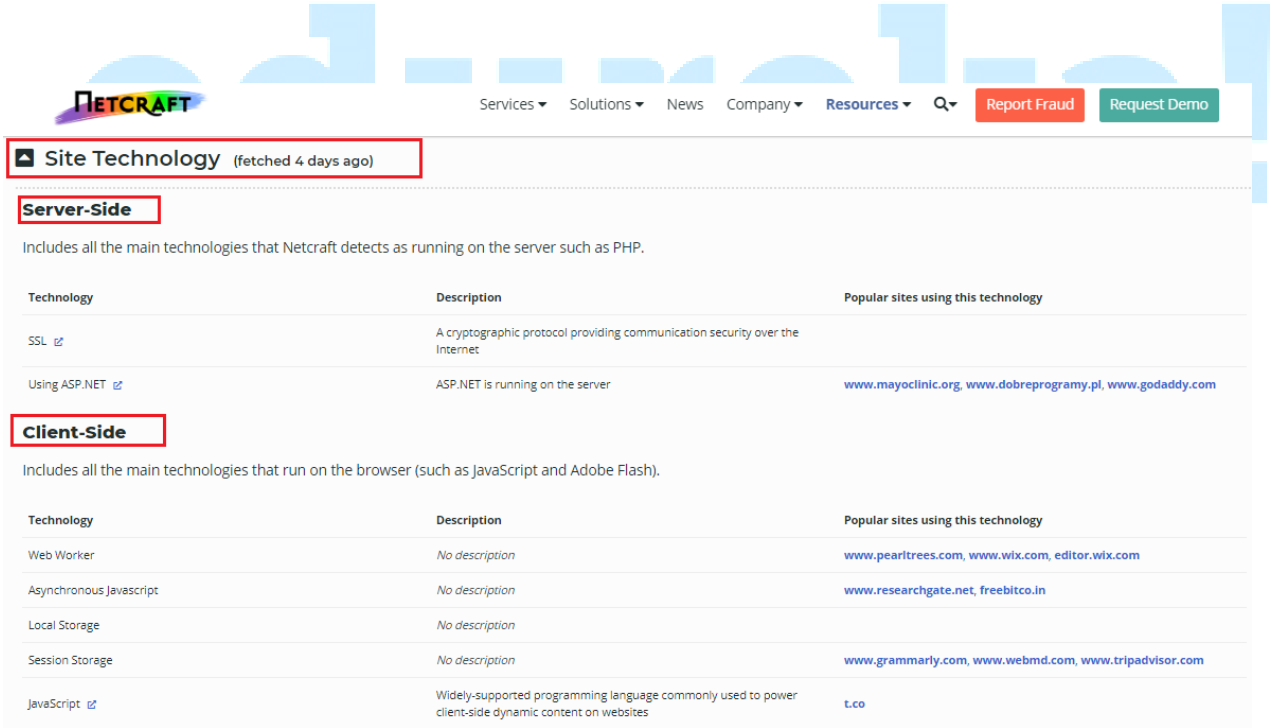






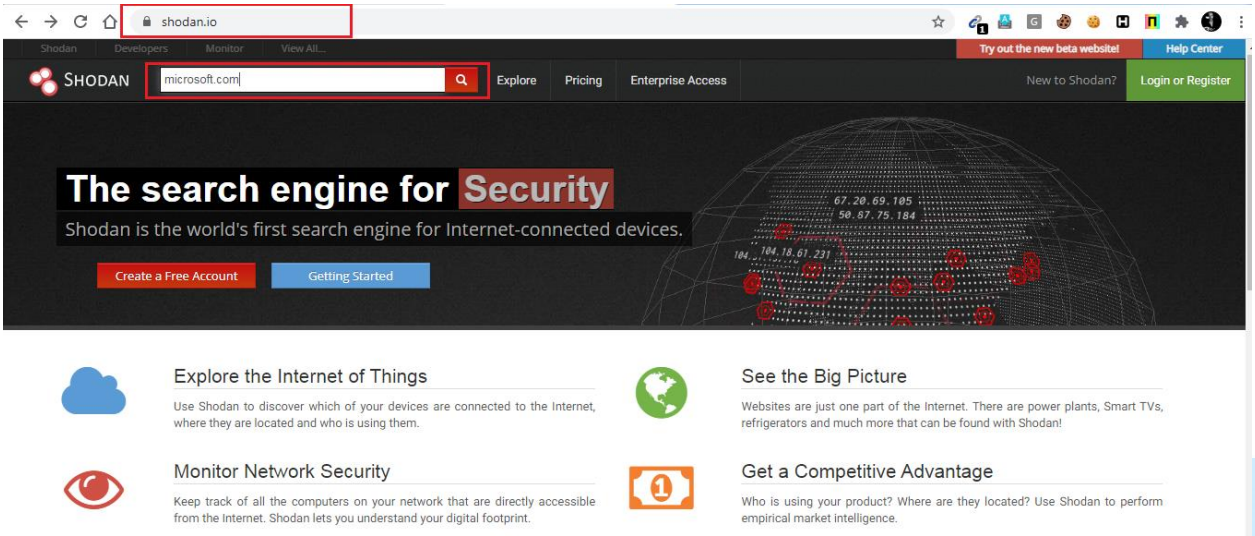
Netblock owner	IP address	OS	Web server	Last seen
Akamai	88.221.41.6	Linux	unknown	26-Jun-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.44.101.131	Linux	unknown	12-Jun-2020
Akamai	88.221.41.6	Linux	unknown	29-May-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.44.101.131	Linux	unknown	22-May-2020
Akamai	88.221.41.6	Linux	unknown	14-May-2020
Akamai Technologies	92.122.150.71	Linux	unknown	7-May-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.44.101.131	Linux	unknown	30-Apr-2020
Akamai Technologies, Inc. 150 Broadway Cambridge MA US 02142	104.85.57.244	Linux	unknown	23-Apr-2020
Akamai Technologies, Inc. 150 Broadway Cambridge MA US 02142	104.110.245.246	Linux	unknown	16-Apr-2020
Akamai	88.221.41.6	Linux	unknown	16-Apr-2020

Step 8: Netcraft will show the details of the server-side and client-side related site technologies used by the developer.

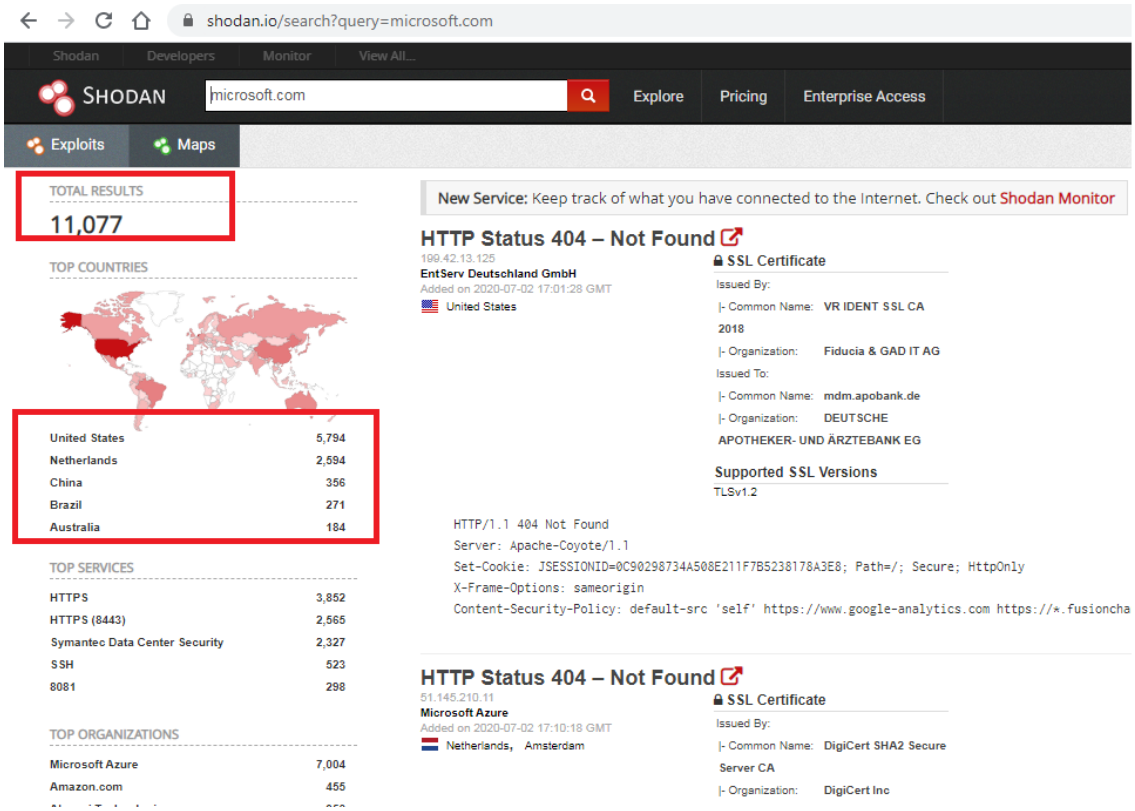


Server Information Gathered from www.shodan.io

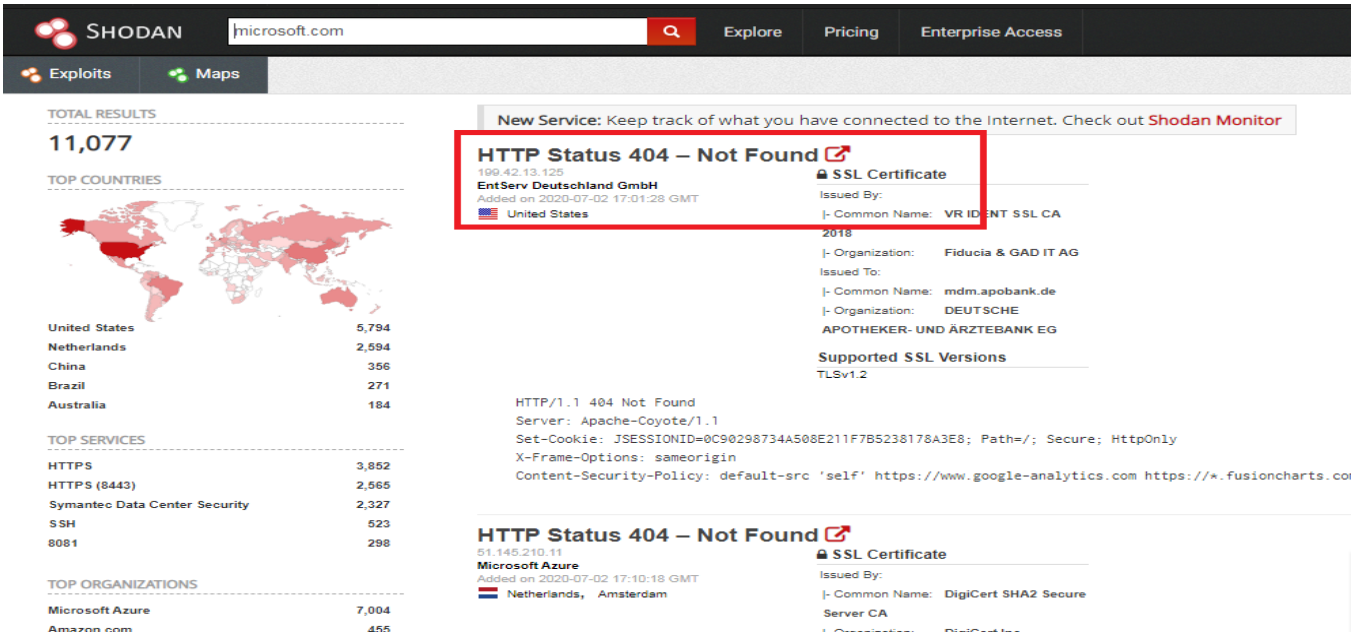
Step 9: Open http://www.shodan.io in the browser and search for Microsoft.com and click on the go.



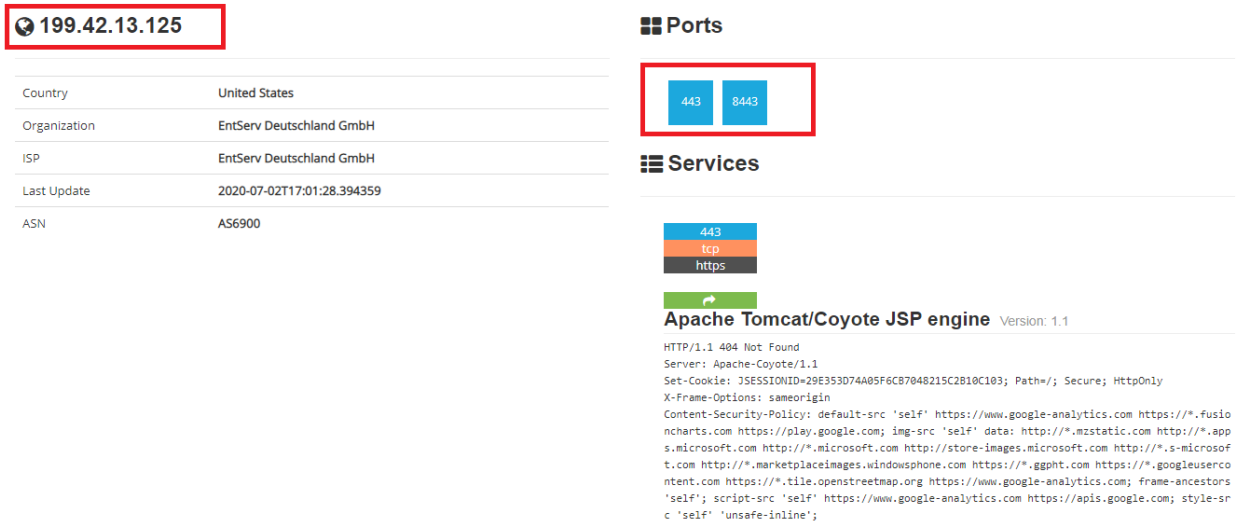
Step 10: The results which will be showing related to servers, here total servers overall Globe Microsoft has 11,077 as of now. You can see the server filtered by country wise.



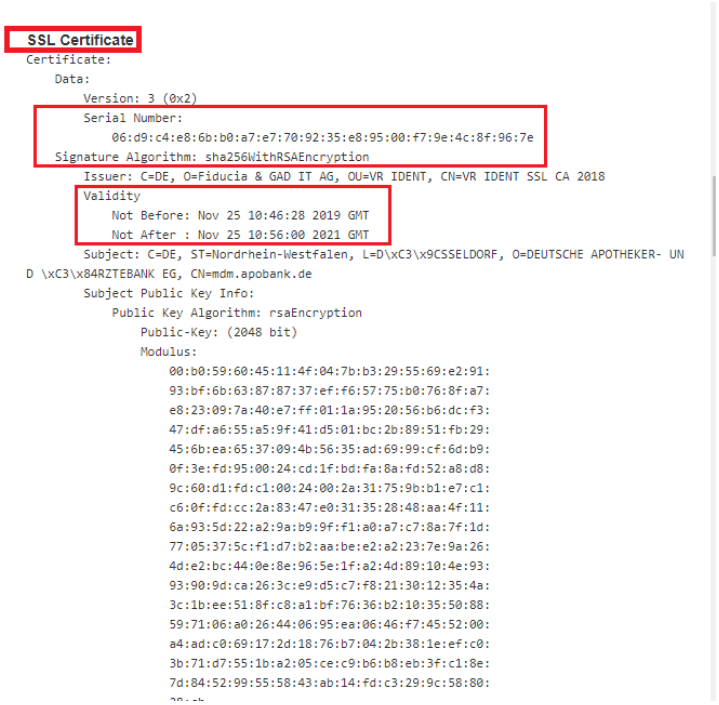
Step 11: Click on the first server information (highlighted).



Step 12: After clicking on the server, you can find the server IP address (Country/ ISP/ Organization) and port numbers, which are in public along with services, here 443 & 8443 ports are opened, and https services are running.



Step 13: Scroll down to see the information related to SSL certificate and serial number and encryption used in the certificate.



In the same way, we have many options available to gather information about domains and people search.
Below are some footprinting websites will be useful for assignments:

Footprinting Websites on Domains:

- https://censys.io
- http://whois.domaintools.com
- https://toolbar.netcraft.com/
- https://www.shodan.io/
- https://www.hybrid-analysis.com/
- https://osintframework.com/
- https://findsubdomains.com/
- https://www.virustotal.com/
- https://suip.biz/

Find People and Background Checks:

- http://www.zabasearch.com/
- https://pipl.com/
- http://www.intelius.com/people-search.html?ReportType=1&searchform=name
- http://www.ussearch.com/?refer=5186
- http://www.123people.com/
- https://records.txdps.state.tx.us/DpsWebsite/CriminalHistory/
- http://socialcatfish.com/

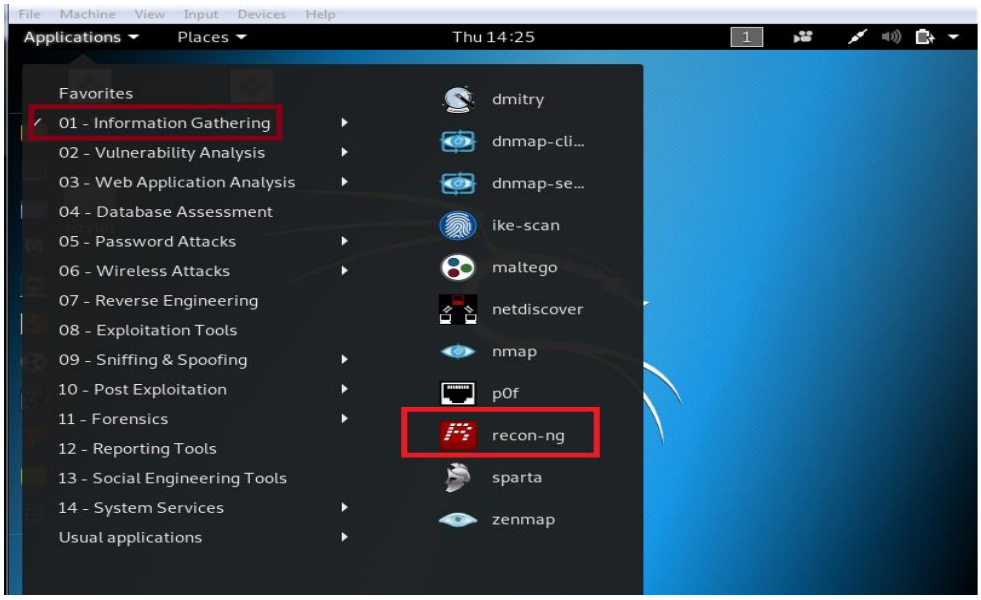
Demo 2: Gathering Information about Domain through Reon-ng Tool in Kali Linux

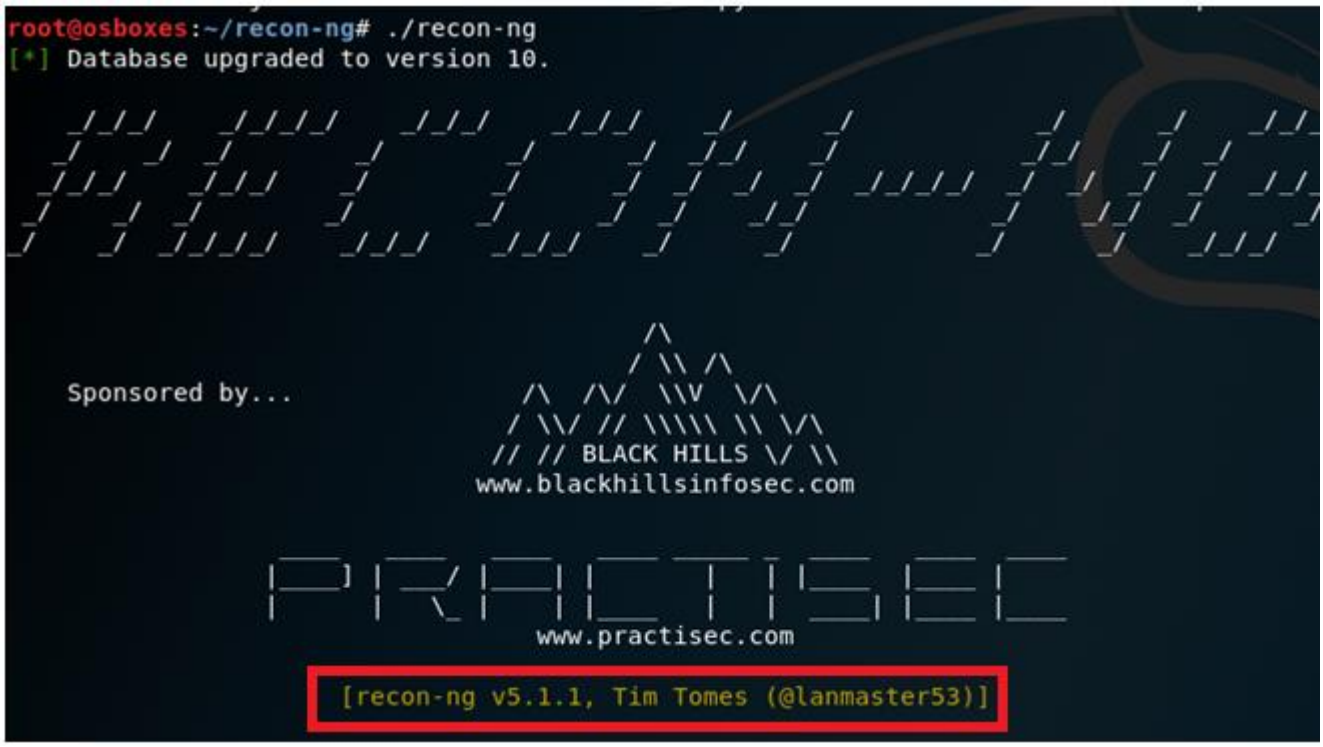
Problem Statement:

Gathering information about website and server information by using Recon-ng tool.

Solution:

Step1: Open Kali Linux go to Applications → Information Gathering →Recon-ng





Step2: Install all modules by using **marketplace install all**

```
[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-hosts/censys_org
[*] Module installed: recon/companies-hosts/censys_tls_subjects
```

Step3: Add domains to scan by using **db insert domains** command. **show domains** command is used to show the added domains:

```
[recon-ng][default] >
[recon-ng][default] > db insert domains
domain (TEXT): microsoft.com
notes (TEXT): for demo
[*] 1 rows affected.
[recon-ng][default] > show domains

  +-------------------------------------------------+
  | rowid |     domain     |     module     |  notes  |
  +-------------------------------------------------+
  | 1     | microsoft.com | user_defined | for demo |
  +-------------------------------------------------+

[*] 1 rows returned
[recon-ng][default] >
```

Step 4: Search for email information related to target domain by using below commands:

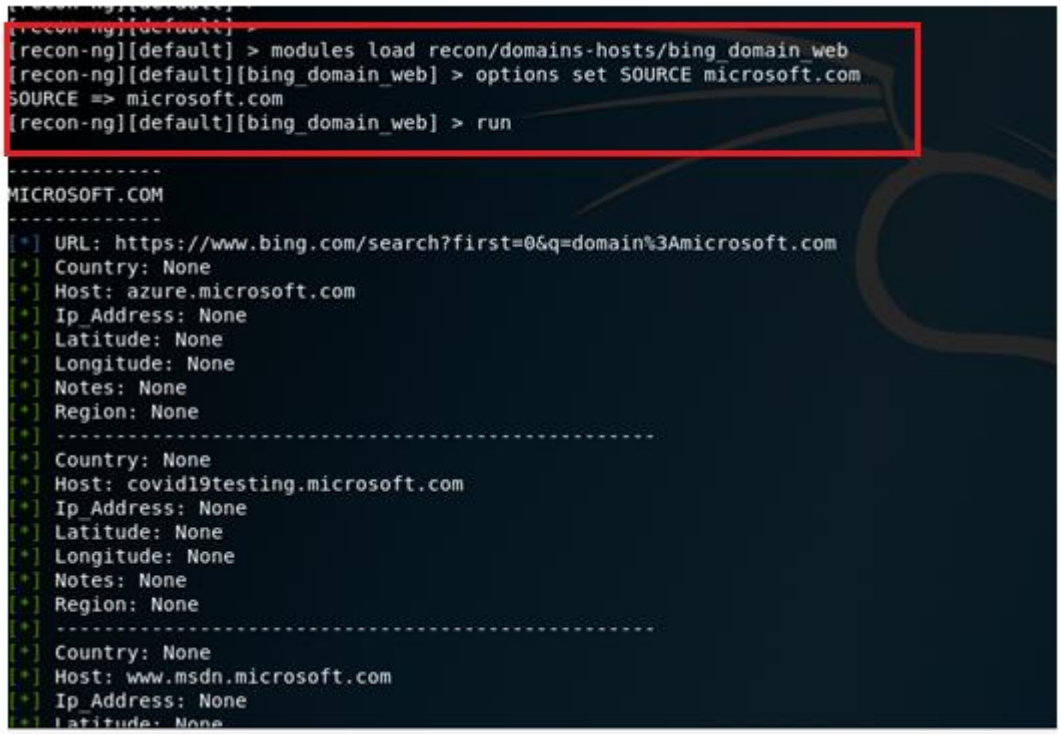
marketplace search whois
marketplace install recon/domains-contacts/whois_pocs
modules load recon/domains-contacts/whois_pocs
options set SOURCE Microsoft.com
run

```
[recon-ng][default] > marketplace search whois
[*] Searching module index for 'whois'...

  +-------------------------------------------------------------------------------+
  |                    Path                    | Version |   Status  | Updated  | D | K |
  +-------------------------------------------------------------------------------+
  | recon/companies-domains/viewdns_reverse_whois | 1.0     | installed | 2019-08-08 |   |   |
  | recon/companies-multi/whois_miner             | 1.1     | installed | 2019-10-15 |   |   |
  | recon/domains-companies/whoxy_whois           | 1.1     | installed | 2020-06-24 |   | * |
  | recon/domains-contacts/whois_pocs             | 1.0     | installed | 2019-06-24 |   |   |
  | recon/netblocks-companies/whois_orgs          | 1.0     | installed | 2019-06-24 |   |   |
  +-------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][default] >
```

```
[recon-ng][default] > marketplace install recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Reloading modules...
[recon-ng][default][whois_pocs] > modules load recon/domains-contacts/whois_pocs
[recon-ng][default][whois_pocs] > options set SOURCE microsoft.com
SOURCE => microsoft.com
[recon-ng][default][whois_pocs] > run

-------------
MICROSOFT.COM
-------------
[*] URL: http://whois.arin.net/rest/pocs;domain=microsoft.com
[*] URL: http://whois.arin.net/rest/poc/AADLA11-ARIN
[*] Country: United States
[*] Email: v-chrisa@microsoft.com
[*] First_Name: CHRIS
[*] Last_Name: AADLAND
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Seattle, WA
[*] Title: Whois contact
[*] ----------------------------------------------------
[*] URL: http://whois.arin.net/rest/poc/AADLA1-ARIN
[*] Country: United States
[*] Email: v-chrisa@microsoft.com
[*] First_Name: CHRISTINA
[*] Last_Name: AADLAND
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Murray, UT
[*] Title: Whois contact
```

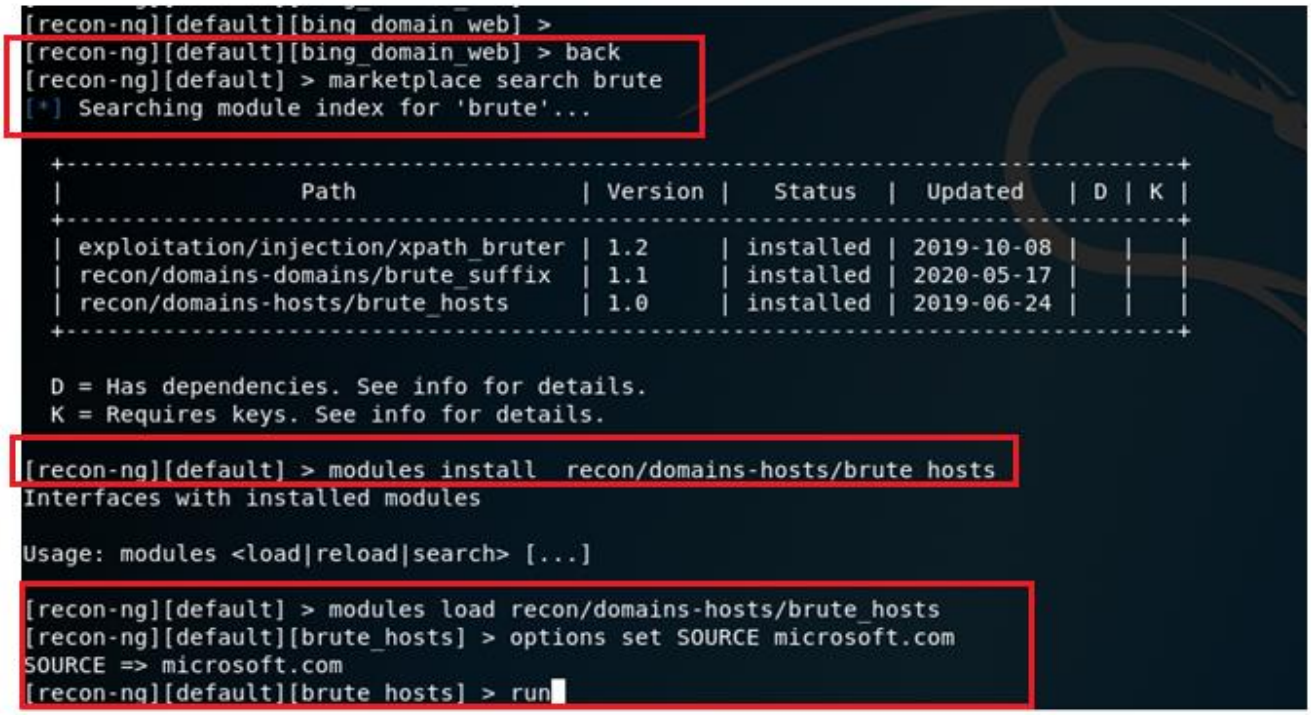
Step 5: To gather about subdomains on target domain

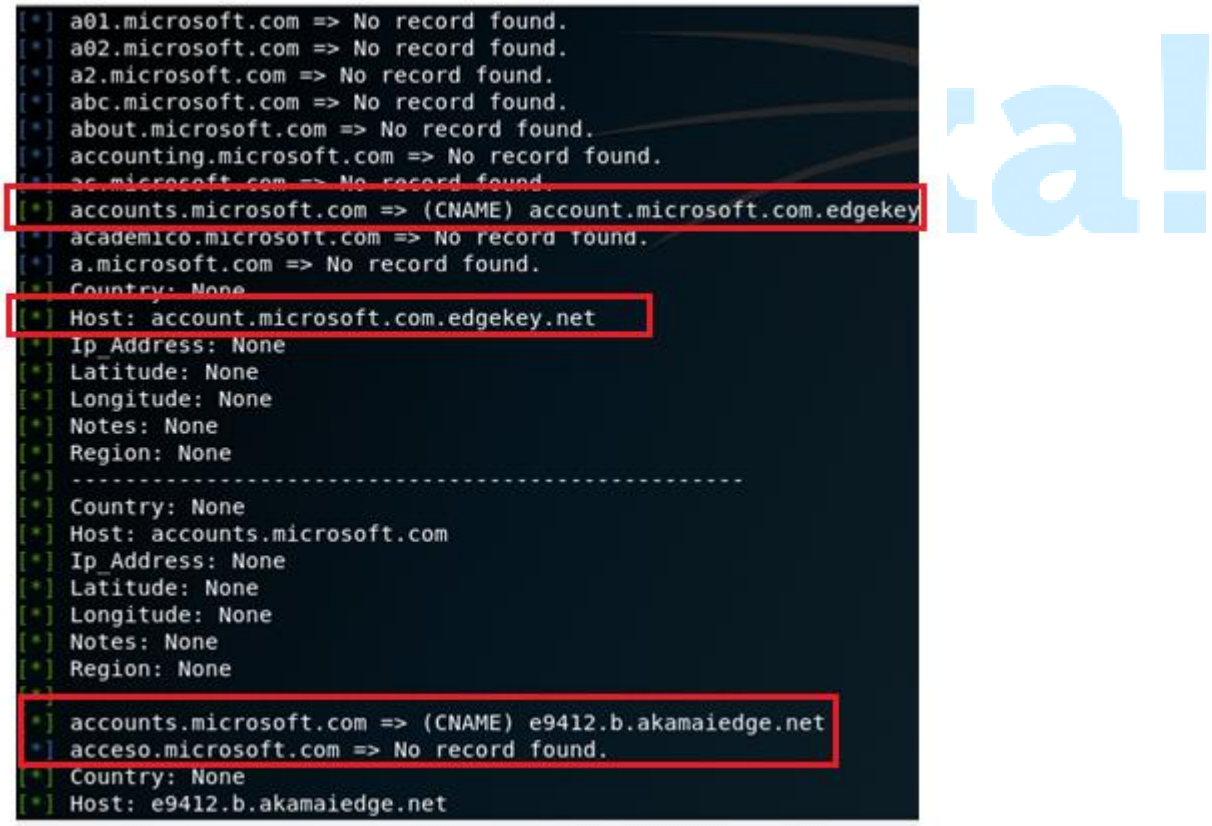
modules load recon/domains-hosts/bing_domain_web
options set SOURCE Microsoft.com
run

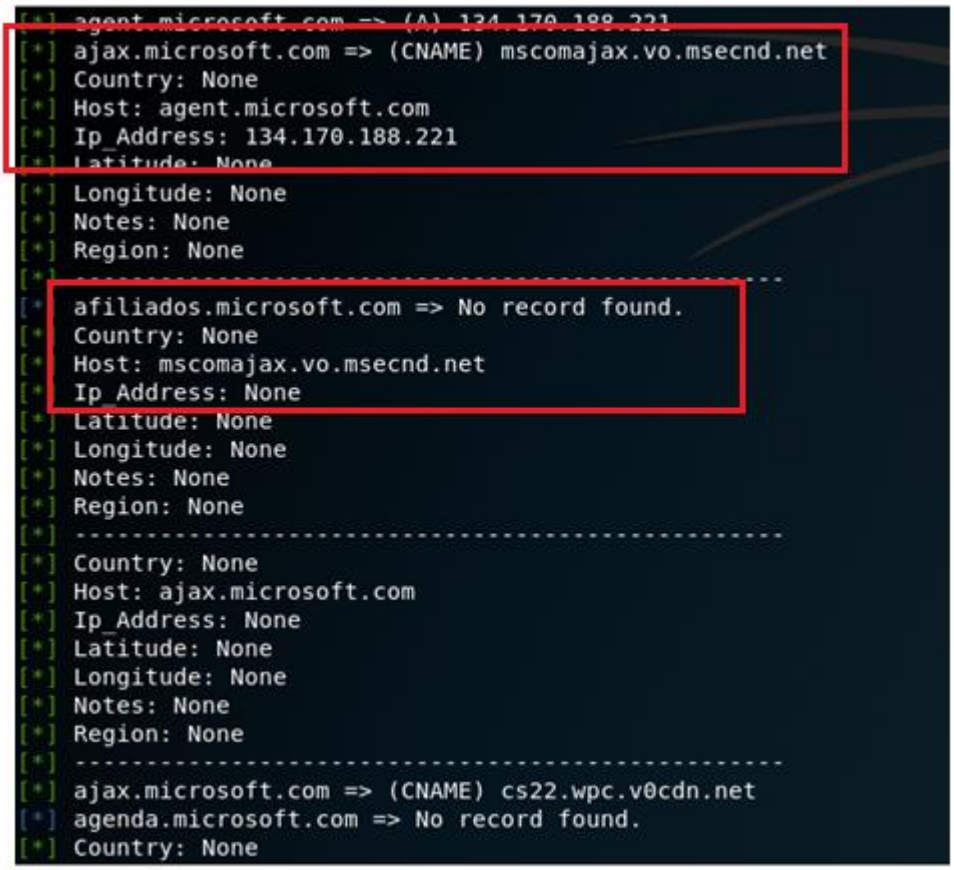


Step 6: To find the MX record and IP address of domains and sub domains use below commands:

back
marketplace search brute
modules install recon/domains-hosts/brute_hosts
modules load recon/domains-hosts/brute_hosts
options set SOURCE Microsoft.com
run

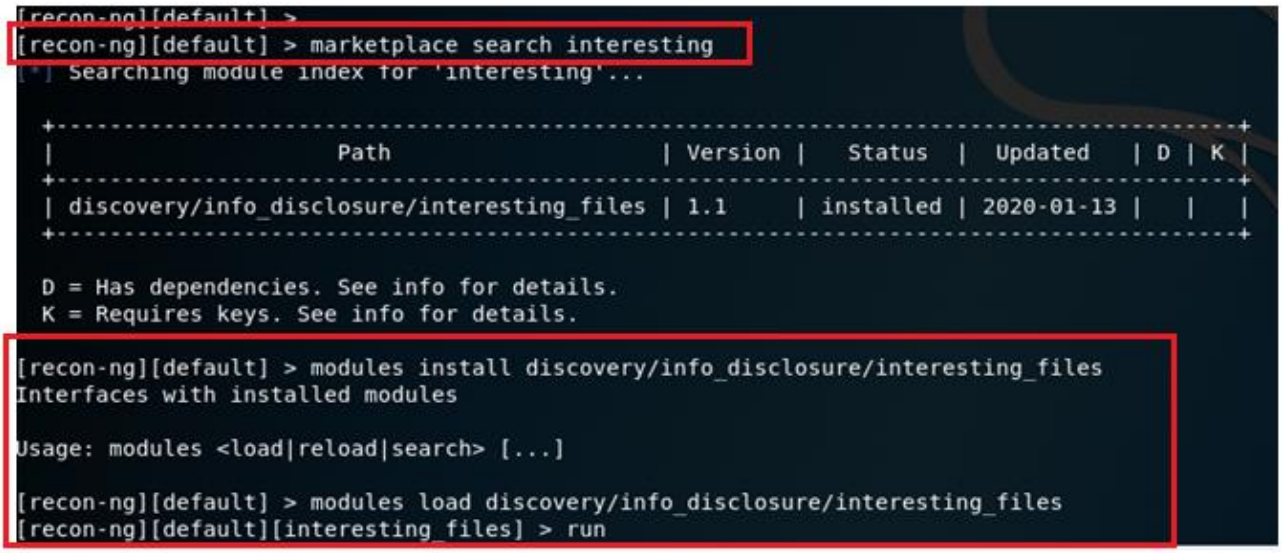

[recon-ng][default][bing_domain_web] >
[recon-ng][default][bing_domain_web] > back
[recon-ng][default] > marketplace search brute
[*] Searching module index for 'brute'...
Path	Version	Status	Updated	D	K
exploitation/injection/xpath_bruter	1.2	installed	2019-10-08		
recon/domains-domains/brute_suffix	1.1	installed	2020-05-17		
recon/domains-hosts/brute_hosts	1.0	installed	2019-06-24		
D = Has dependencies. See info for details.
K = Requires keys. See info for details.
[recon-ng][default] > modules install recon/domains-hosts/brute_hosts
Interfaces with installed modules
Usage: modules <load|reload|search> [...]
[recon-ng][default] > modules load recon/domains-hosts/brute_hosts
[recon-ng][default][brute_hosts] > options set SOURCE microsoft.com
SOURCE => microsoft.com
[recon-ng][default][brute_hosts] > run

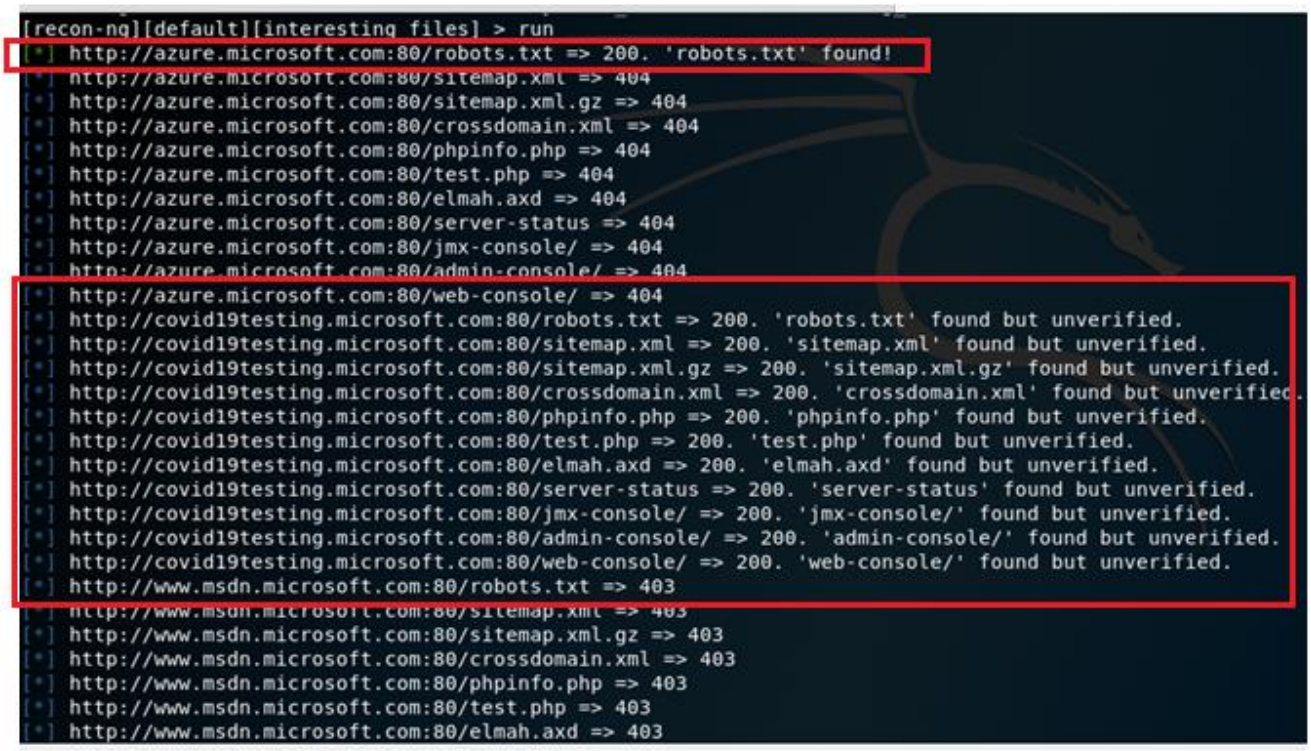

[*] a01.microsoft.com => No record found.
[*] a02.microsoft.com => No record found.
[*] a2.microsoft.com => No record found.
[*] abc.microsoft.com => No record found.
[*] about.microsoft.com => No record found.
[*] accounting.microsoft.com => No record found.
[*] accounts.microsoft.com => (CNAME) account.microsoft.com.edgekey
[*] academico.microsoft.com => No record found.
[*] a.microsoft.com => No record found.
[*] Country: None
[*] Host: account.microsoft.com.edgekey.net
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: accounts.microsoft.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] accounts.microsoft.com => (CNAME) e9412.b.akamaiedge.net
[*] acceso.microsoft.com => No record found.
[*] Country: None
[*] Host: e9412.b.akamaiedge.net



Step 7: To gather information related to server codes on target use below commands:

back
marketplace search interesting
modules install discovery/info_disclosure/interesting_files
modules load discovery/info_disclosure/interesting_files
run





Step 8: To view the dashboard of all results use below commands:

show contacts

```
[recon-ng][default] > show contacts

  +-----------------------------------------------------------------------------------------------------------------------------------------------------------------+
  | rowid | first_name | middle_name |  last_name   |                email                |     title     |     region     |    country    |   module   | notes | phone |
  +-----------------------------------------------------------------------------------------------------------------------------------------------------------------+
  | 1     | CHRIS      |             | AADLAND      | v-chrisa@microsoft.com              | Whois contact | Seattle, WA    | United States | whois_pocs |       |       |
  | 2     | CHRISTINA  |             | AADLAND      | v-chrisa@microsoft.com              | Whois contact | Murray, UT     | United States | whois_pocs |       |       |
  | 3     | Christina  |             | Aadland      | v-chrisa@microsoft.com              | Whois contact | Redmond, WA    | United States | whois_pocs |       |       |
  | 4     |            |             | Abuse        | abuse@microsoft.com                 | Whois contact | Redmond, WA    | United States | whois_pocs |       |       |
  | 5     | Melissa    |             | Allison      | mallison@ocmcdonald.onmicrosoft.com | Whois contact | Sj, CA         | United States | whois_pocs |       |       |
  | 6     | Jeffrey    |             | Amels        | jamels@microsoft.com                | Whois contact | Kent, WA       | United States | whois_pocs |       |       |
  | 7     | BRAD       |             | AUSTIN       | brada@microsoft.com                 | Whois contact | Charlotte, NC  | United States | whois_pocs |       |       |
  | 8     | JO         |             | BAKER        | jolynb@microsoft.com                | Whois contact | Tukwila, WA    | United States | whois_pocs |       |       |
  | 9     | Ram        |             | Balakrishnan | rambala@microsoft.com               | Whois contact | Redmond, WA    | United States | whois_pocs |       |       |
  | 10    | david      |             | Balko        | dbalko@sfscapital.onmicrosoft.com   | Whois contact | Rockwall, TX   | United States | whois_pocs |       |       |
  | 11    | ADAM       |             | BECKER       | adam.becker@primew.onmicrosoft.com  | Whois contact | Denver, CO     | United States | whois_pocs |       |       |
```

show domains

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

  +-------------------------------------------------------+
  | rowid |     domain     |    module    |  notes   |
  +-------------------------------------------------------+
  | 1     | microsoft.com | user_defined | for demo |
  +-------------------------------------------------------+

[*] 1 rows returned
```

show hosts

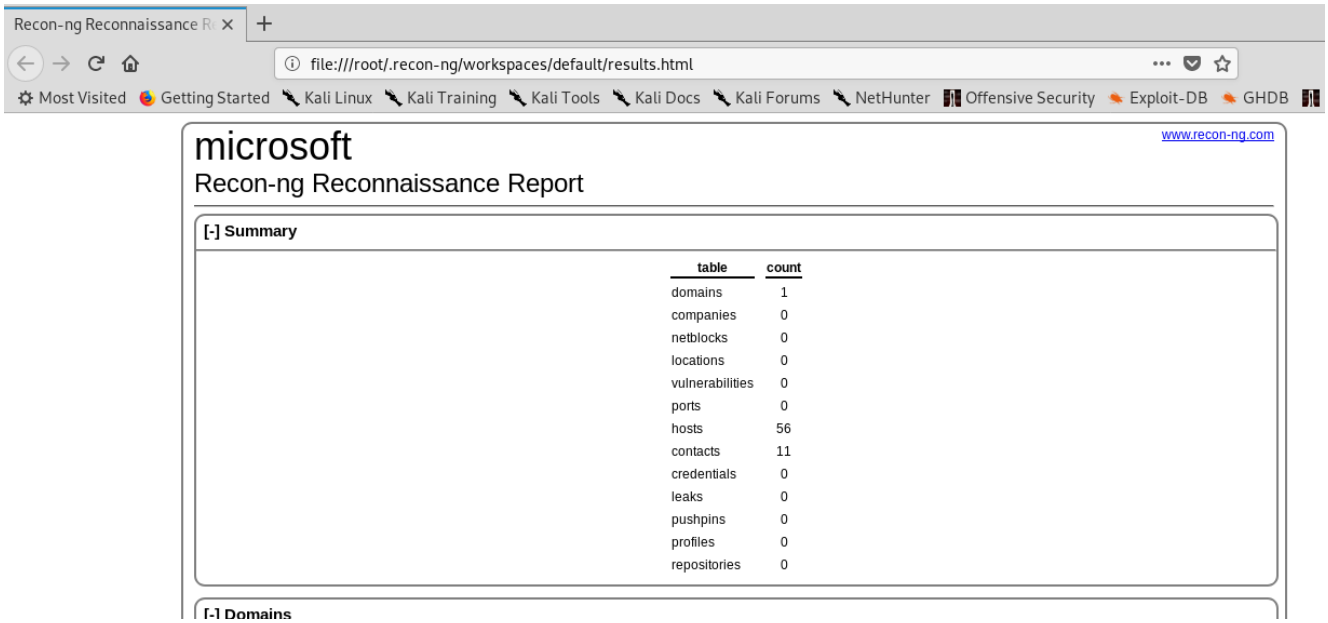
```
[recon-ng][default] >
[recon-ng][default] > show hosts

  +-----------------------------------------------------------------------------------------------------------------------------------------------------+
  | rowid |                  host                  |    ip_address    | region | country | latitude | longitude |      module      | notes |
  +-----------------------------------------------------------------------------------------------------------------------------------------------------+
  | 1     | azure.microsoft.com                    |                  |        |         |          |           | bing_domain_web  |       |
  | 2     | covid19testing.microsoft.com           |                  |        |         |          |           | bing_domain_web  |       |
  | 3     | www.msdn.microsoft.com                 |                  |        |         |          |           | bing_domain_web  |       |
  | 4     | myapps.microsoft.com                   |                  |        |         |          |           | bing_domain_web  |       |
  | 5     | devicemanagement.microsoft.com         |                  |        |         |          |           | bing_domain_web  |       |
  | 6     | update.microsoft.com                   |                  |        |         |          |           | bing_domain_web  |       |
  | 7     | education.microsoft.com                |                  |        |         |          |           | bing_domain_web  |       |
  | 8     | download.microsoft.com                 |                  |        |         |          |           | bing_domain_web  |       |
  | 9     | docs.microsoft.com                     |                  |        |         |          |           | bing_domain_web  |       |
  | 10    | partner.microsoft.com                  |                  |        |         |          |           | bing_domain_web  |       |
  | 11    | workshops.microsoft.com                |                  |        |         |          |           | bing_domain_web  |       |
  | 12    | windowsupdate.microsoft.com            |                  |        |         |          |           | bing_domain_web  |       |
  | 13    | support.microsoft.com                  |                  |        |         |          |           | bing_domain_web  |       |
  | 14    | account.microsoft.com.edgekey.net      |                  |        |         |          |           | brute_hosts      |       |
  | 15    | accounts.microsoft.com                 |                  |        |         |          |           | brute_hosts      |       |
  | 16    | e9412.b.akamaiedge.net                 |                  |        |         |          |           | brute_hosts      |       |
  | 17    | accounts.microsoft.com                 | 104.120.156.189  |        |         |          |           | brute_hosts      |       |
  | 18    | admin-portal.office.com                |                  |        |         |          |           | brute_hosts      |       |
  | 19    | admin.microsoft.com                    |                  |        |         |          |           | brute_hosts      |       |
  | 20    | portal-office365-com.b-0004.b-msedge.net |                |        |         |          |           | brute_hosts      |       |
  | 21    | b-0004.b-msedge.net                    |                  |        |         |          |           | brute_hosts      |       |
  | 22    | admin.microsoft.com                    | 13.107.6.156     |        |         |          |           | brute_hosts      |       |
  | 23    | azure.bingads.trafficmanager.net       |                  |        |         |          |           | brute_hosts      |       |
  | 24    | ads.microsoft.com                      |                  |        |         |          |           | brute_hosts      |       |
```

Step 9: For Reporting (export) the results in html use below commands:

marketplace search report
marketplace install reporting/html
marketplace load reporting/html
options set CREATOR vishwa
options set CUSTOMER microsoft.com
run

```
[recon-ng][default] >
[recon-ng][default] > marketplace search report
[*] Searching module index for 'report'...

+-------------------------------------------------------------------------------+
|                Path                | Version |   Status   |  Updated   | D | K |
+-------------------------------------------------------------------------------+
| recon/hosts-hosts/virustotal       | 1.0     | installed | 2019-06-24 |   | * |
| recon/netblocks-hosts/virustotal   | 1.0     | installed | 2019-06-24 |   | * |
| reporting/csv                      | 1.0     | installed | 2019-06-24 |   |   |
| reporting/html                     | 1.0     | installed | 2019-06-24 |   |   |
| reporting/json                     | 1.0     | installed | 2019-06-24 |   |   |
| reporting/list                     | 1.0     | installed | 2019-06-24 |   |   |
| reporting/proxifier                | 1.0     | installed | 2019-06-24 |   |   |
| reporting/pushpin                  | 1.0     | installed | 2019-06-24 |   | * |
| reporting/xlsx                     | 1.0     | installed | 2019-06-24 |   |   |
| reporting/xml                      | 1.1     | disabled  | 2019-06-24 |   |   |
+-------------------------------------------------------------------------------+

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > marketplace install reporting/html
[*] Module installed: reporting/html
[*] Reloading modules...
```

```
[recon-ng][default] >
[recon-ng][default] > modules load reporting/html
[recon-ng][default][html] > options set CREATOR vishwa
CREATOR => vishwa
[recon-ng][default][html] > options set CUSTOMER microsoft
CUSTOMER => microsoft
[recon-ng][default][html] > run
[*] Report generated at '/root/.recon-ng/workspaces/default/results.html'.
[recon-ng][default][html] >
```



Demo 3: Information Gathering of Domain through Maltego Tool

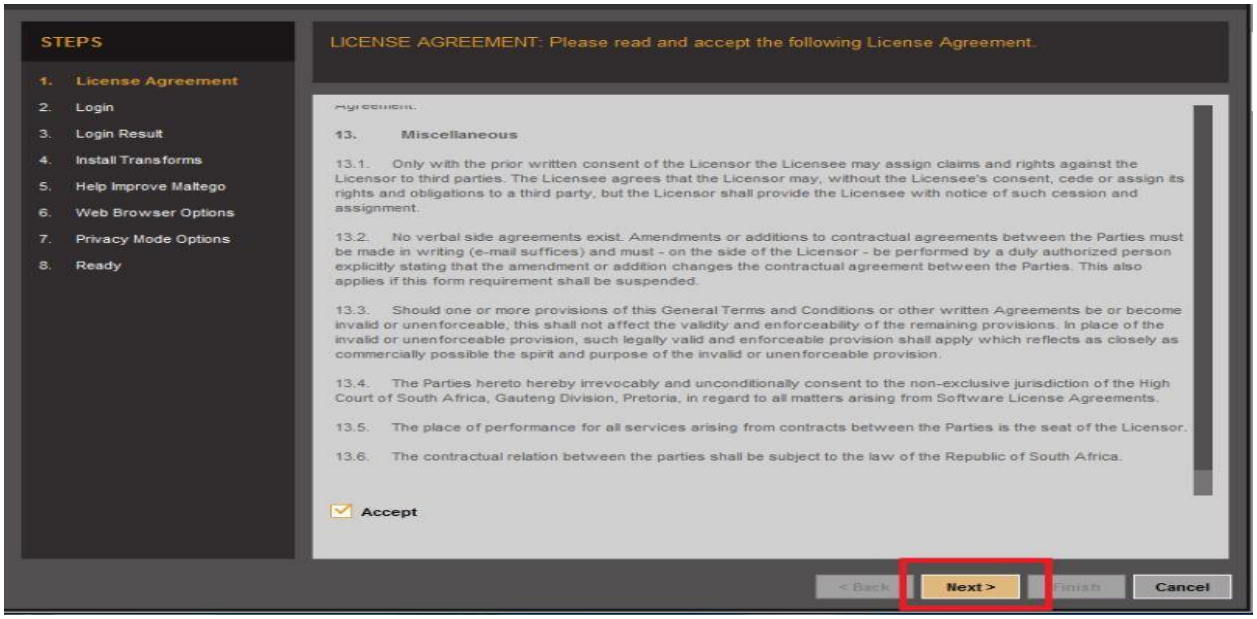
Problem Statement:

Gathering information about website and server by using the Maltego tool.

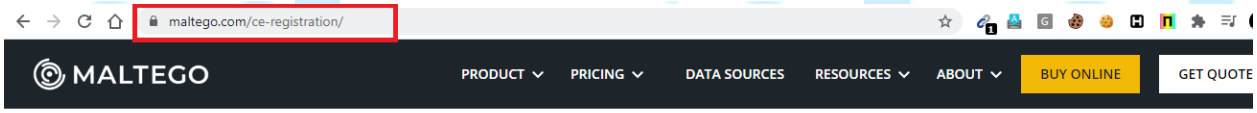
Solution:

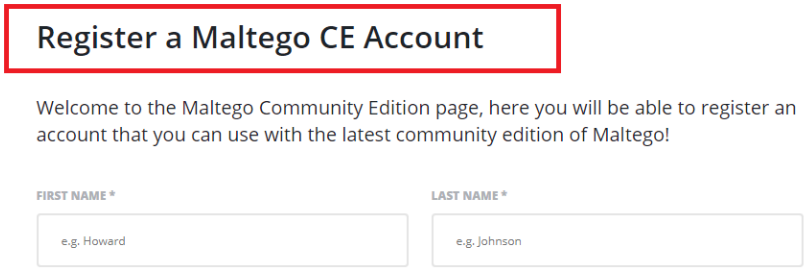
Step 1: Open Kali Linux and search for Maltego Software and click on **Maltego CE (Free)-Community Edition.**

Step 2: Accept the License Agreement by clicking **Next.**

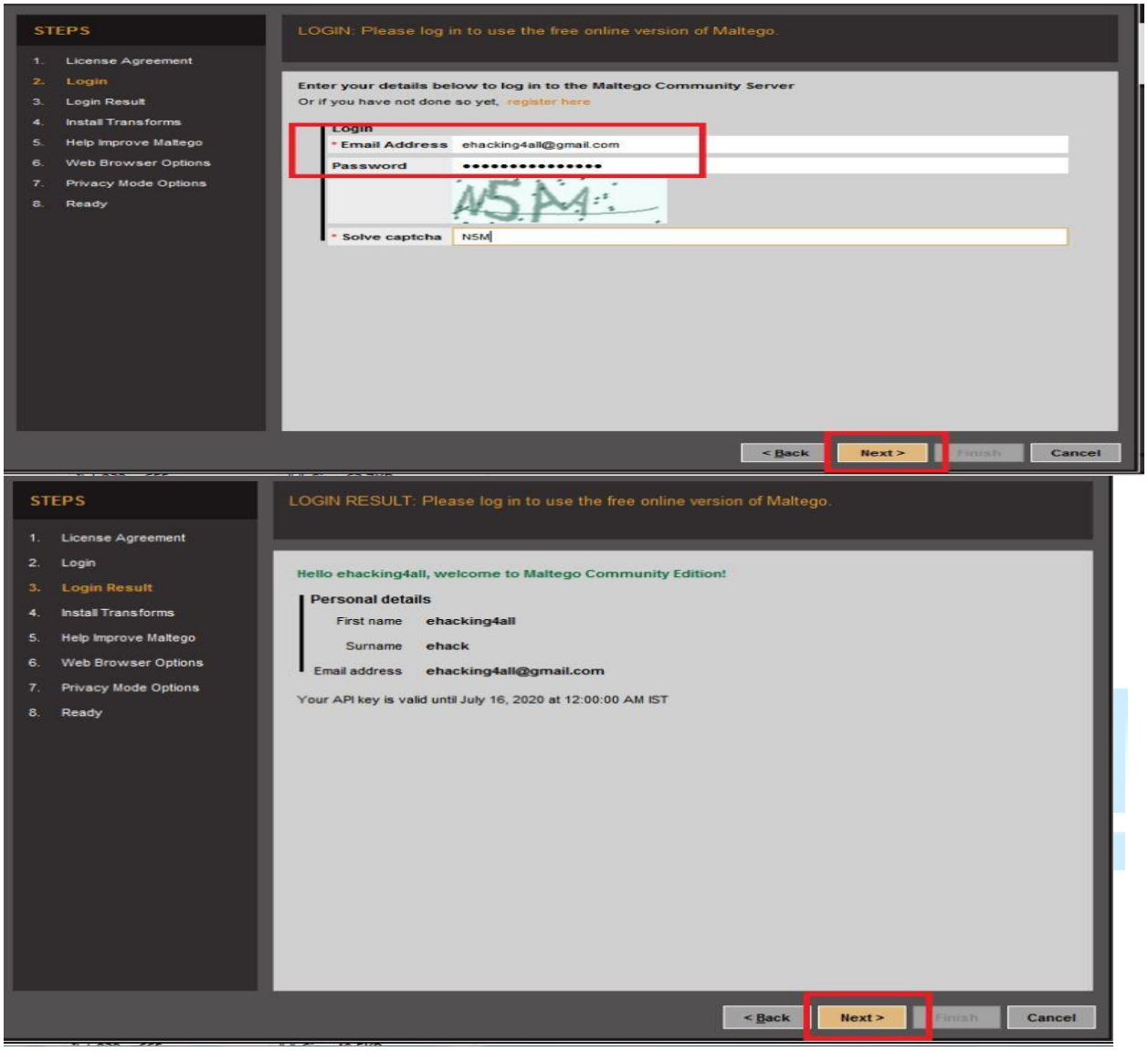


Step 3: Register accounts for Maltego (www.maltego.com/ce-registration/) by providing your details and will get a verification mail to your registered email to confirm your account.

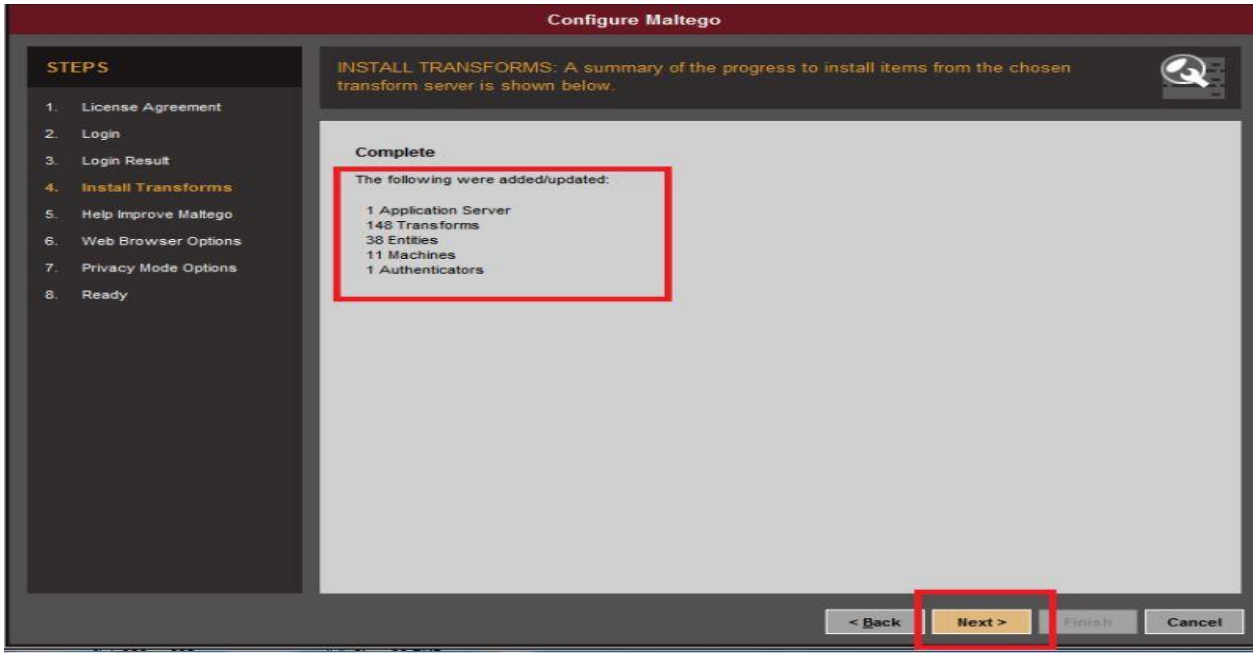




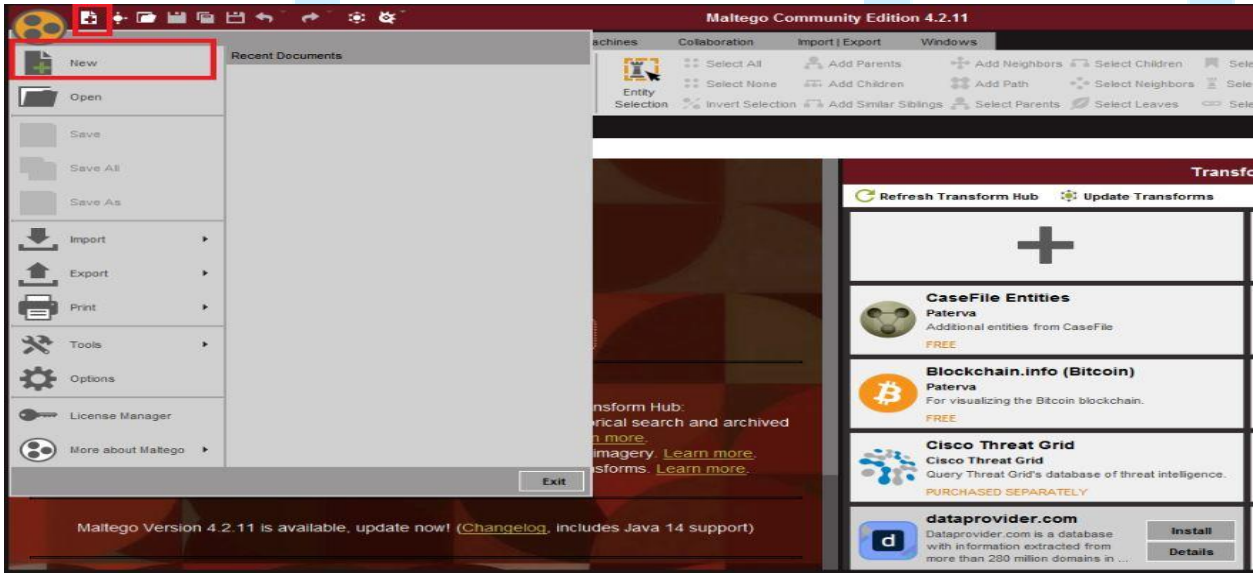
Step 4: Login into the Maltego account in the application and click on **Next**.



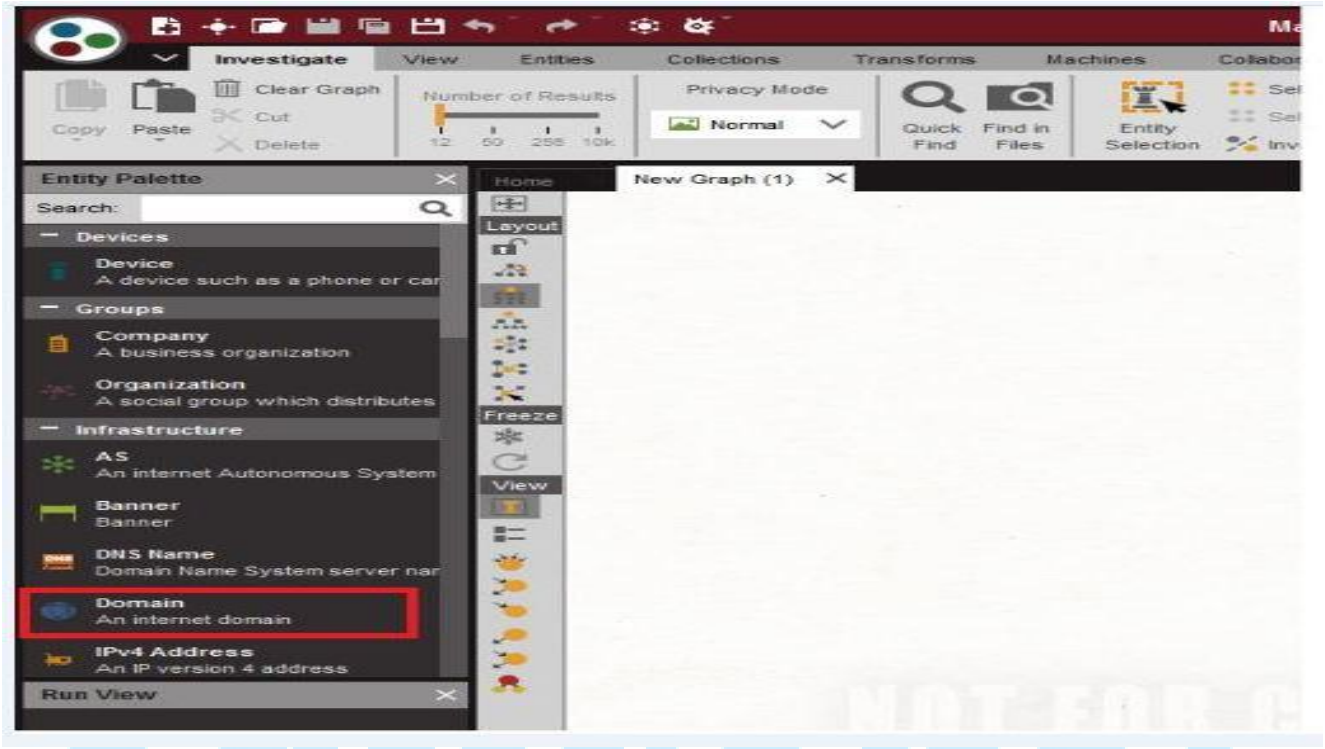
Step 5: Default transforms add-ons will be added and click on **NEXT.**



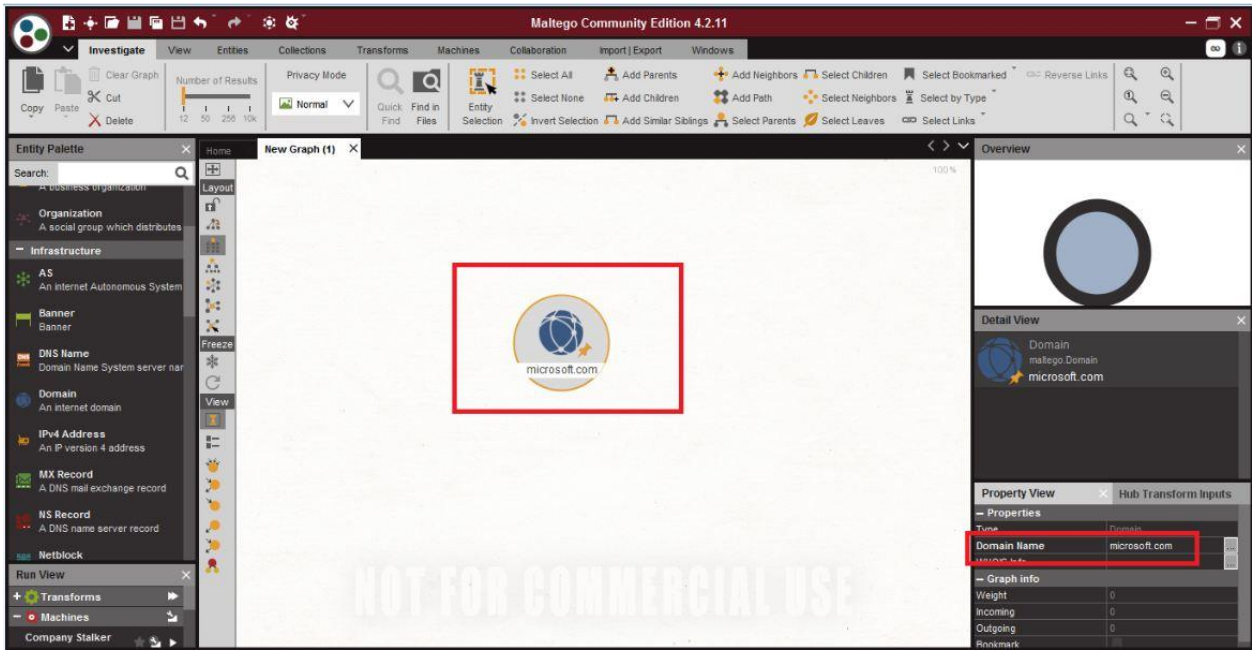
Step 6: Click on **New** for workspace.



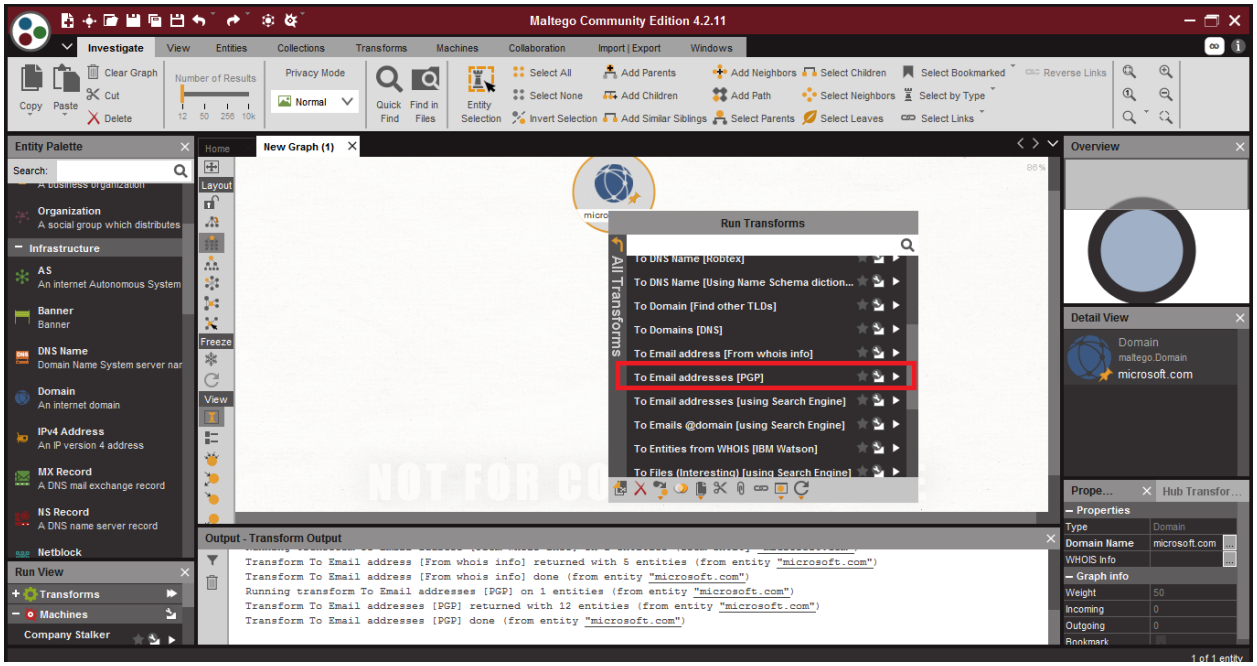
Step 7: Click on **Domains** in Left panel to gather information.

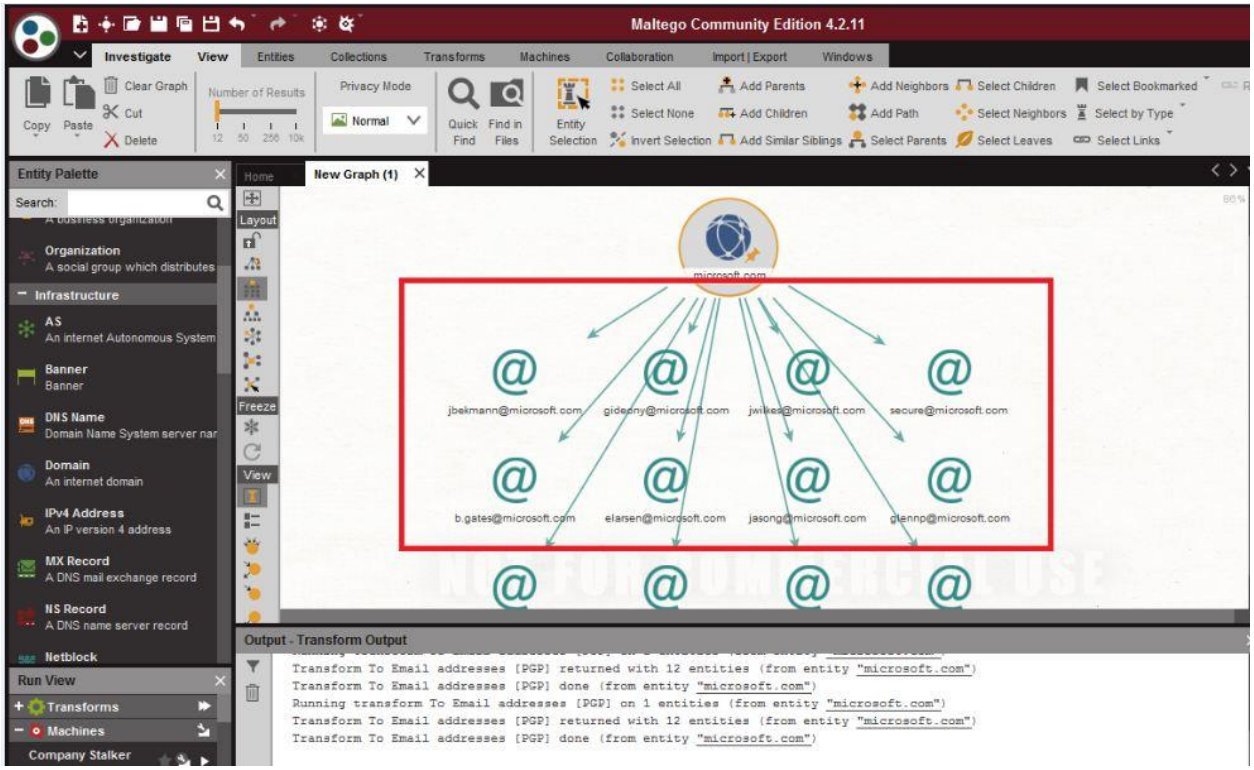


Step 8: Write the domain name (**Microsoft.com**) without www protocol.

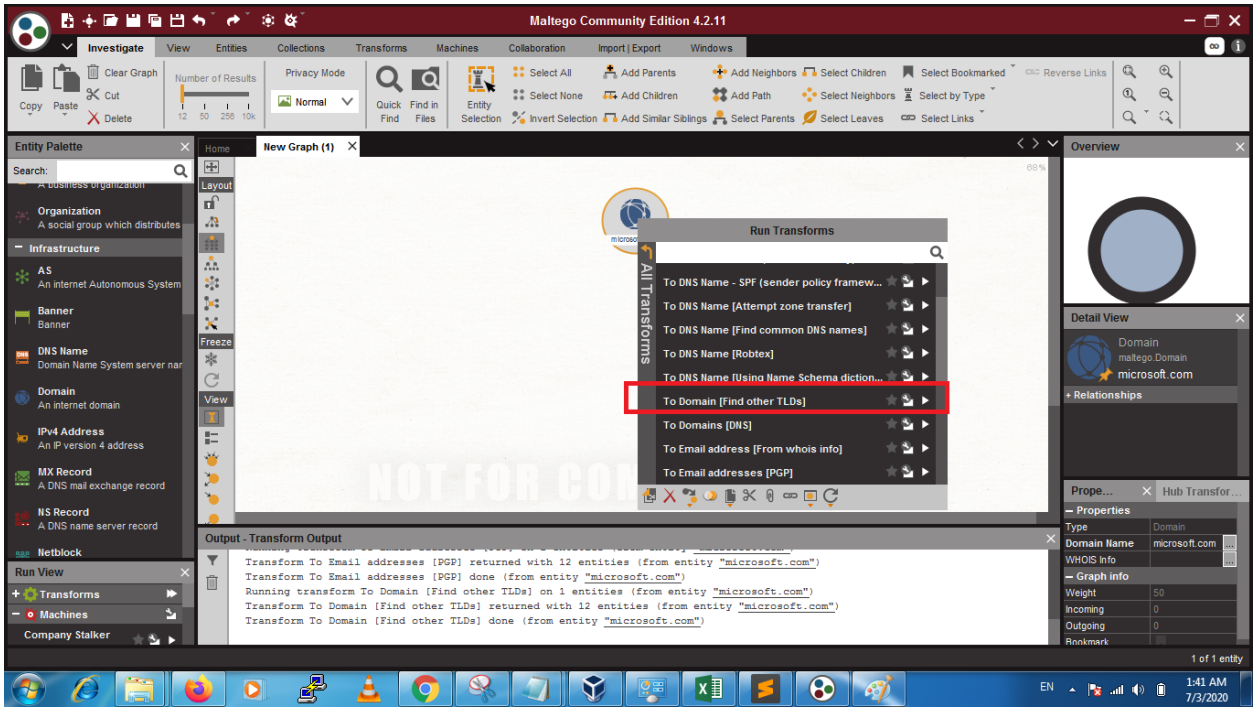


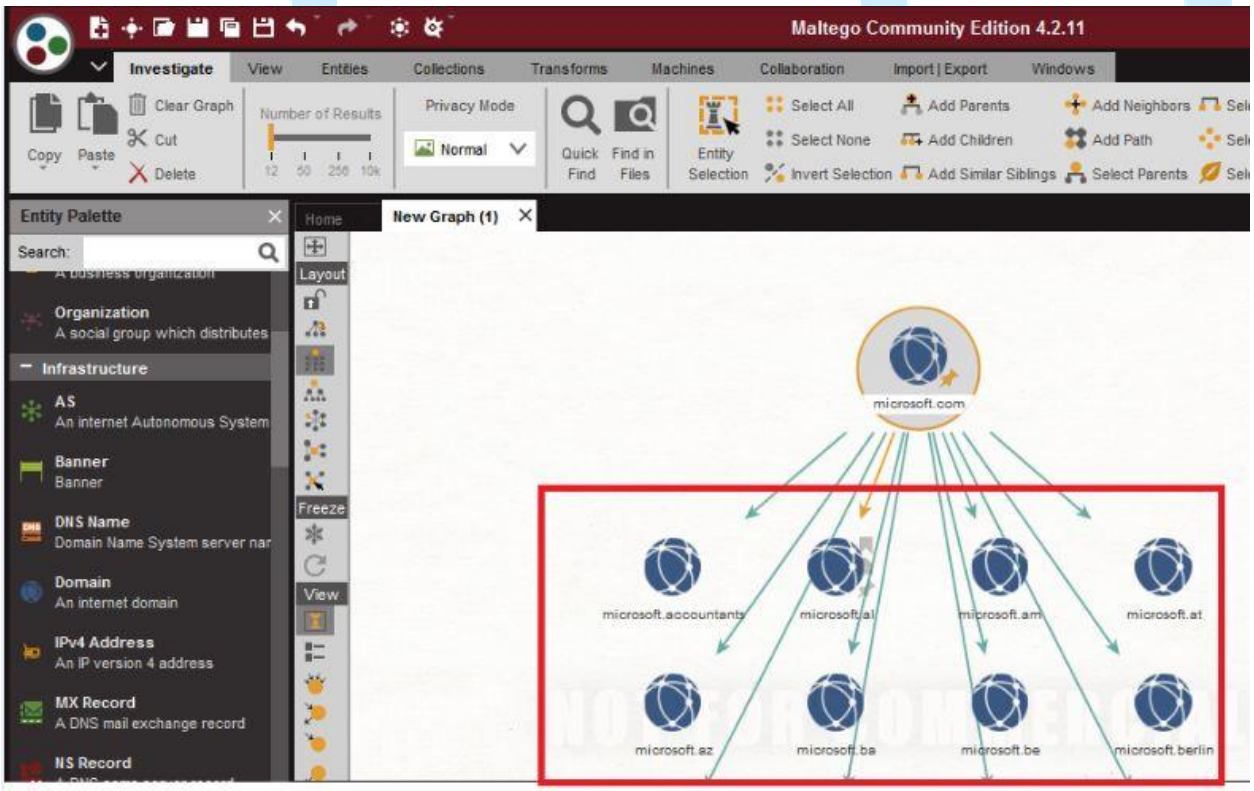
Step 9: Right-click and select the **To email addresses** (to gather emails related to the domain).



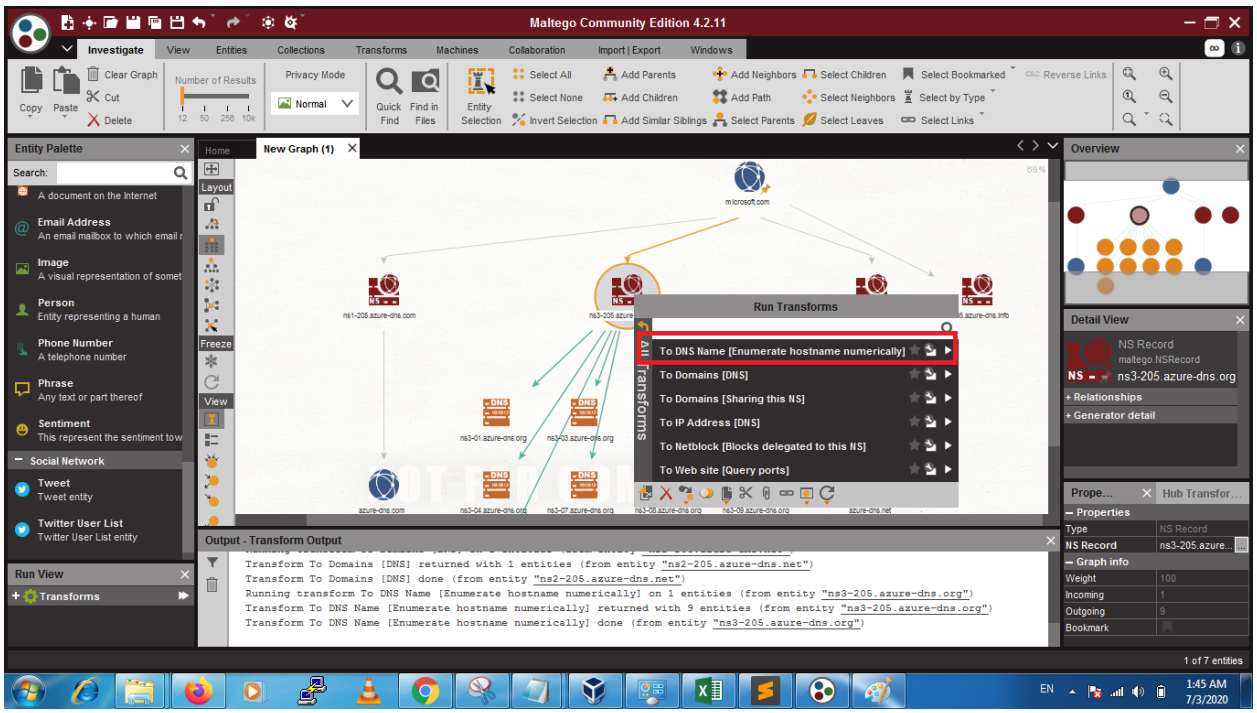


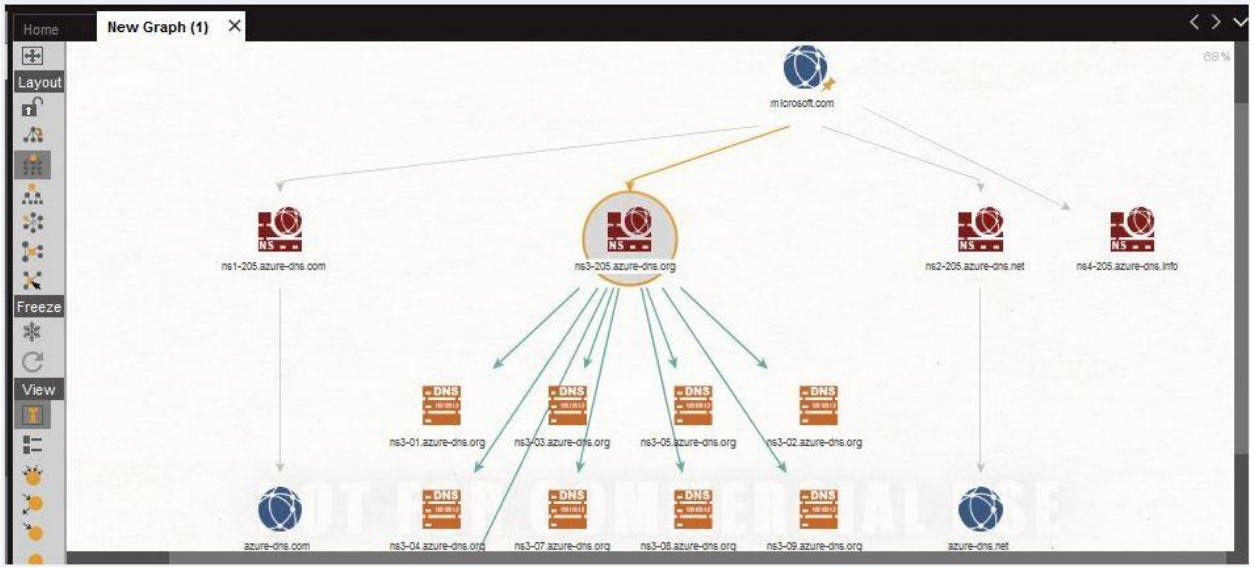
Step 10: Collect all domain server details -> Right-click and select **To Domain (find other TLDs).**





Step 11: To collect the hostnames of the domain, right-click on **Domain** and select **To DNS Name.**





In this way, you can gather more information about the target domain to gather information related to subdomains, hostnames, email id, etc.

Below are the references to work with Maltego Tool:

https://medium.com/@raebaker/a-beginners-guide-to-osint-investigation-with-maltego-6b195f7245cc

Demo 4 – Subdomain information gathering

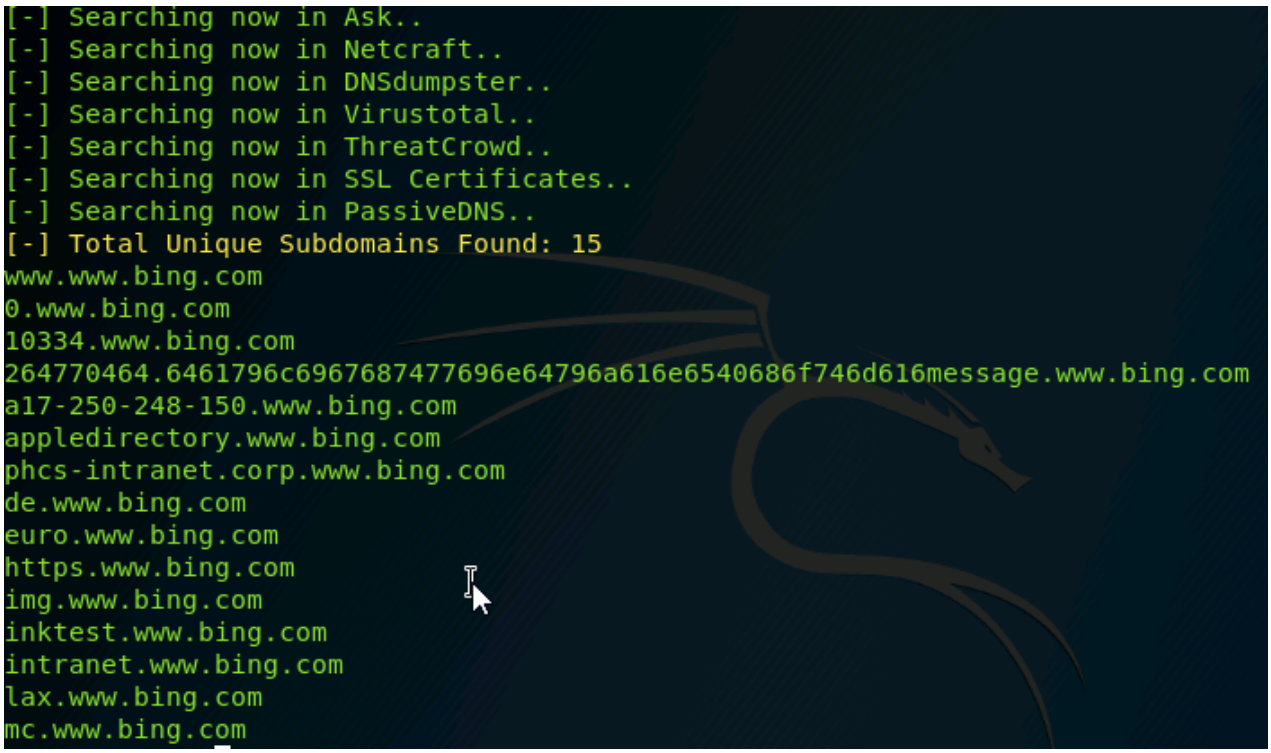
Problem Statement 1

Using Sublist3r tool in Kali linux, find subdomains for www.bing.com. Then use 50 threads to find the subdomains that have port default https open.

Solution

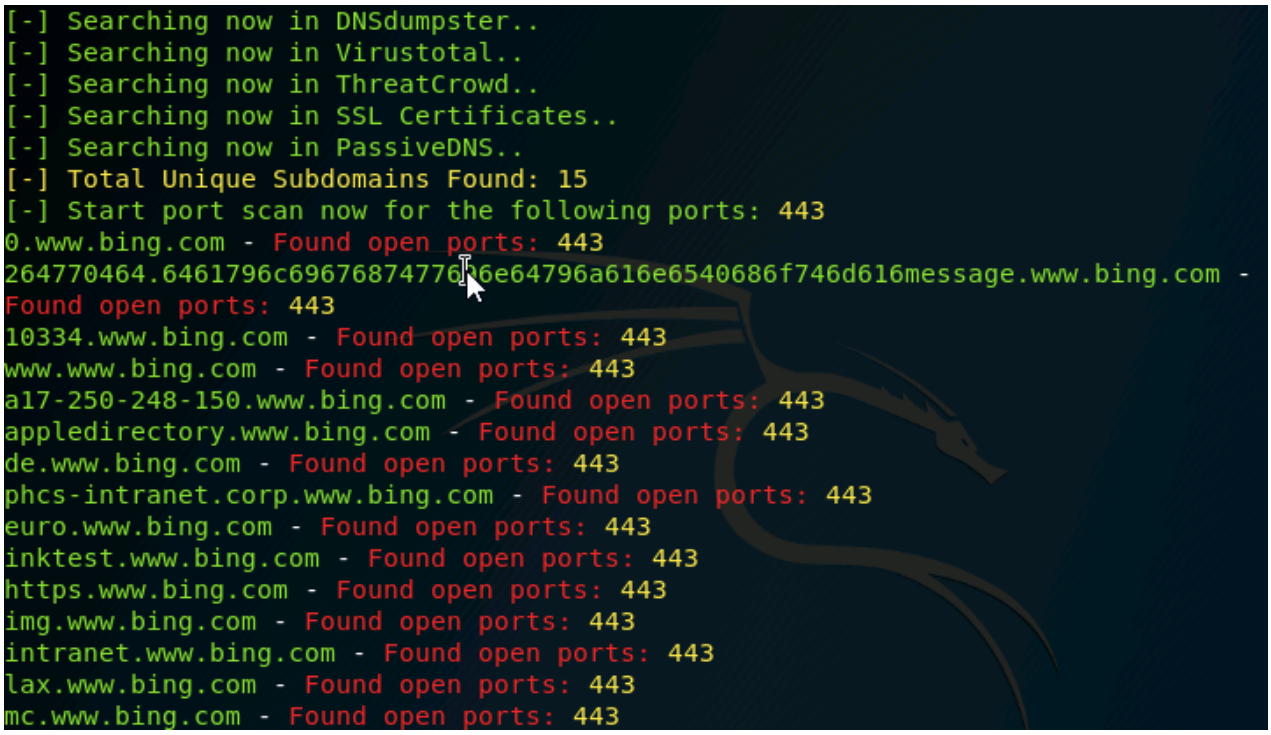
Step 1: Find subdomains for www.bing.com

```
sublist3r -d www.bing.com
```



Step 2: Find subdomains that have https ports open. The default port for https is 443.

```
sublist3r -d www.bing.com -t 50 -p 443
```



Problem Statement 2

Using dnsmap tool in Kali linux, find subdomains for google.com. Then use traceroute to find the route to one of the IP address found in the previous step.

Solution

Command:

```
dnsmap google.com
```

```
root@kali:~# dnsmap google.com
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for google.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

aa.google.com
IPv6 address #1: 2607:f8b0:400a:803::200e

aa.google.com
IP address #1: 172.217.14.238

accounts.google.com
IPv6 address #1: 2607:f8b0:400a:803::200d

accounts.google.com
IP address #1: 172.217.14.237

admin.google.com
IPv6 address #1: 2607:f8b0:400a:809::200e

admin.google.com
IP address #1: 172.217.3.206
```

Find route using traceroute.

`traceroute 172.217.14.237`

```
root@kali:~# traceroute 172.217.14.237
traceroute to 172.217.14.237 (172.217.14.237), 30 hops max, 60 byte packets
 1  lodSense.localdomain (10.10.10.1)  0.284 ms  0.267 ms  0.255 ms
 2  172.18.0.1 (172.18.0.1)  0.496 ms  0.486 ms  0.473 ms
 3  192.168.100.6 (192.168.100.6)  0.533 ms  0.515 ms  0.501 ms
 4  163.47.101.129 (163.47.101.129)  0.755 ms  0.739 ms  0.576 ms
 5  as15169.seattle.megaport.com (206.53.171.8)  1.816 ms  1.800 ms  1.791 ms
 6  74.125.243.177 (74.125.243.177)  1.967 ms  1.967 ms 74.125.243.193 (74.125.2
43.193)  1.051 ms
 7  209.85.254.247 (209.85.254.247)  1.550 ms  2.090 ms  2.072 ms
 8  sea30s02-in-f13.1e100.net (172.217.14.237)  1.202 ms  1.187 ms  1.180 ms
```

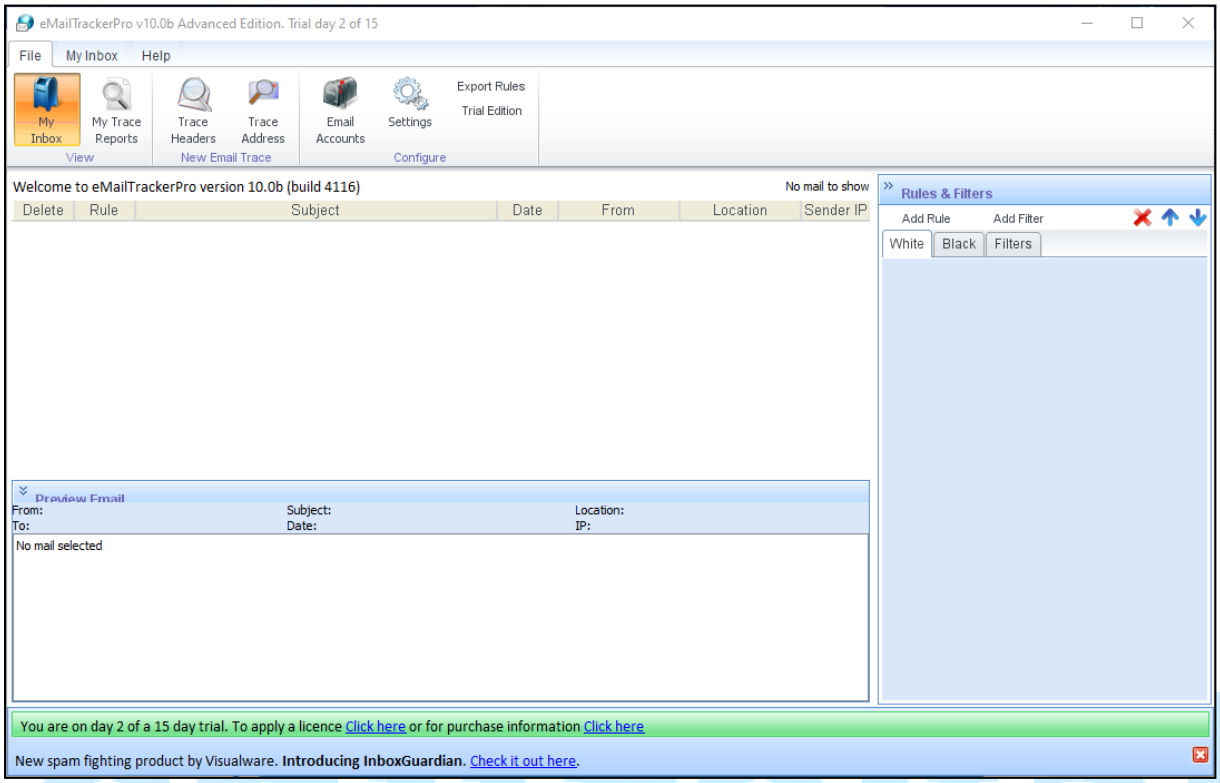
Demo 5: Email Footprinting

Problem Statement:

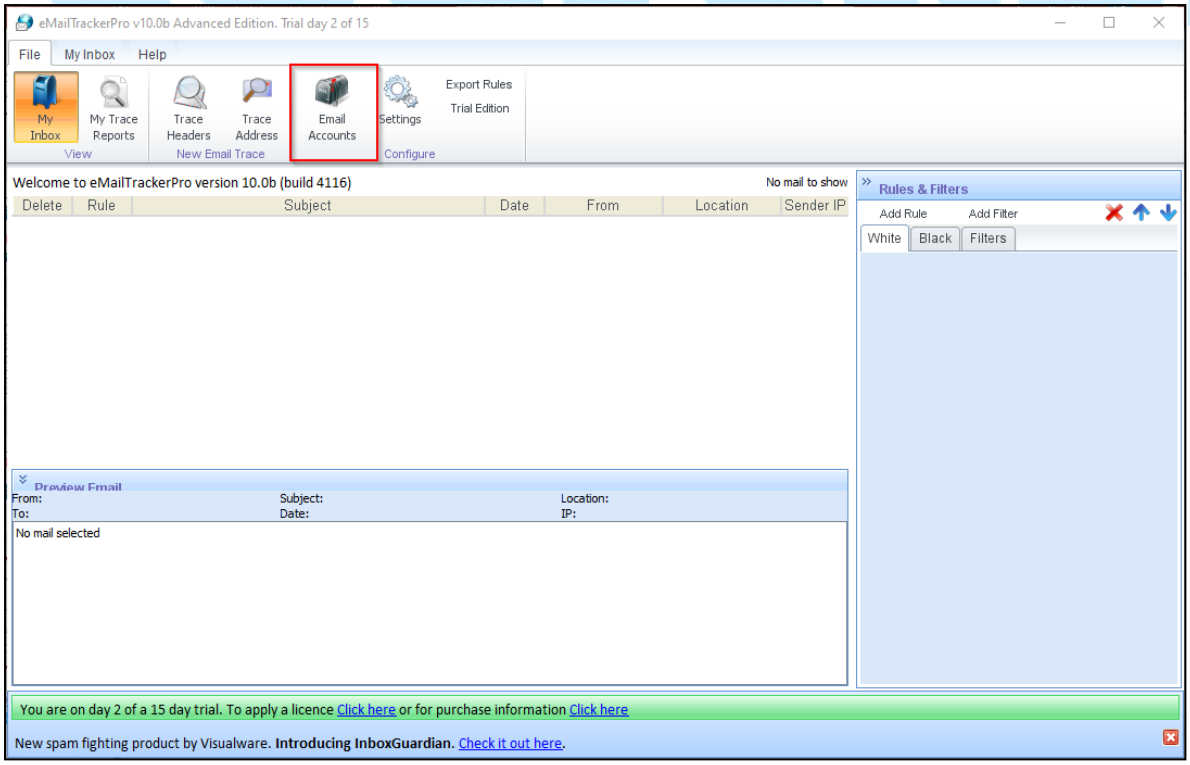
Tracking Email using Email Header
Tool Used: eMail Tracker Pro

Solution:

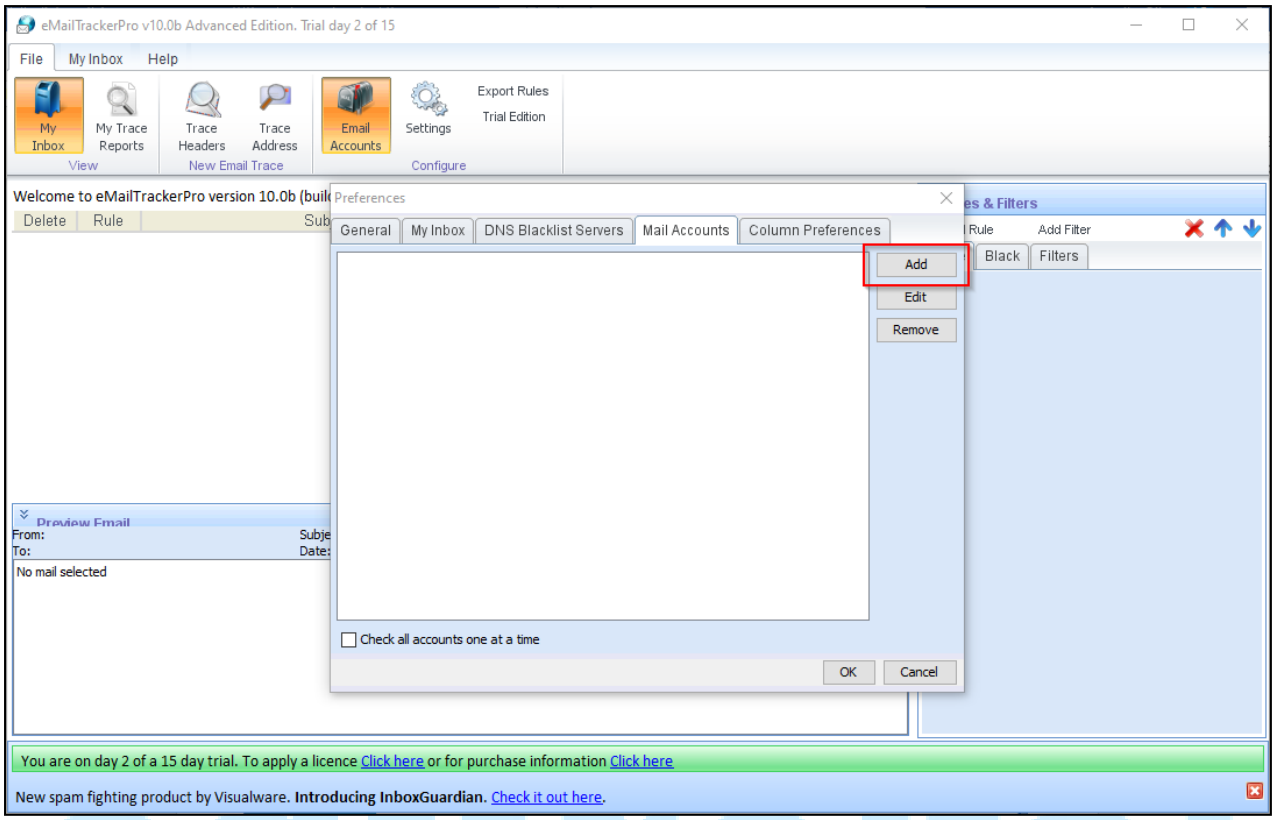
Step 1: Download and install eMail Tracker Pro from http://www.emailtrackerpro.com/

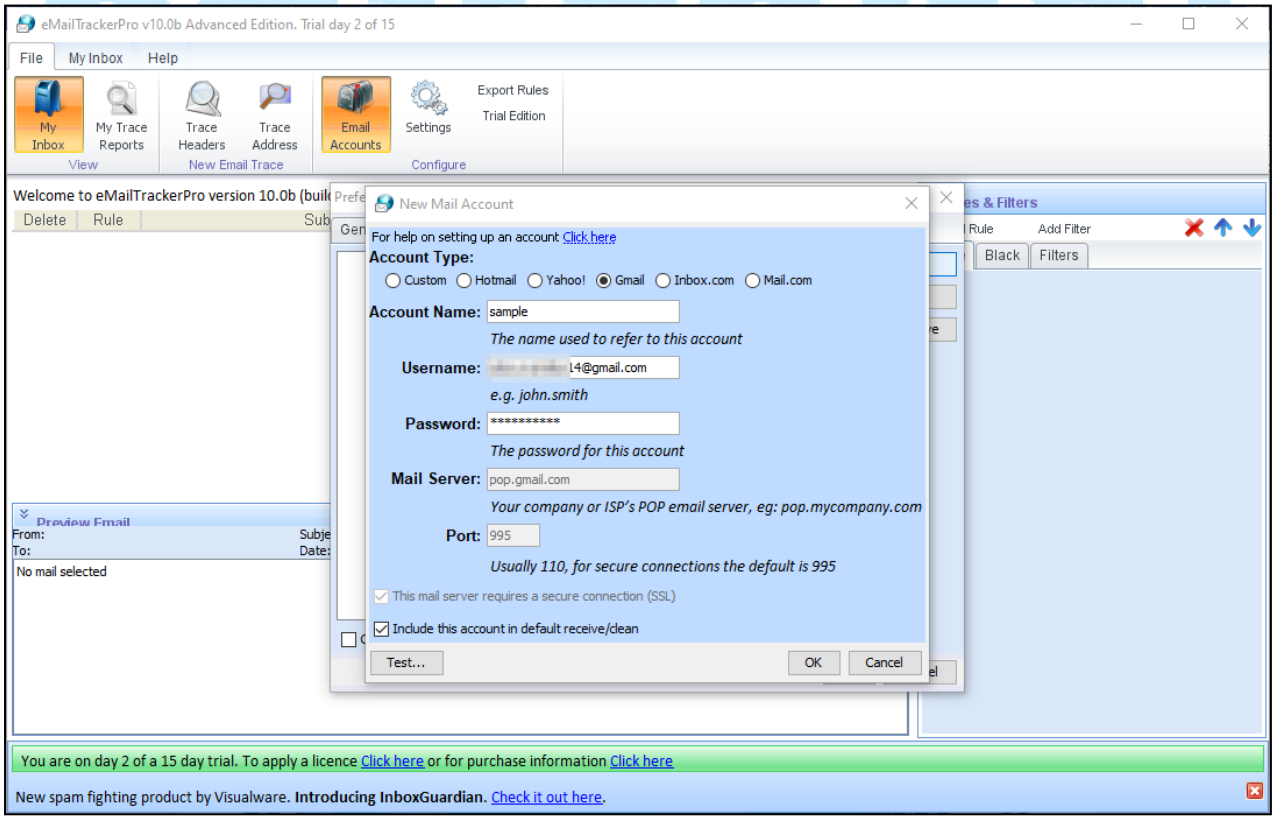


Step 2: After installing go to File>Email Accounts

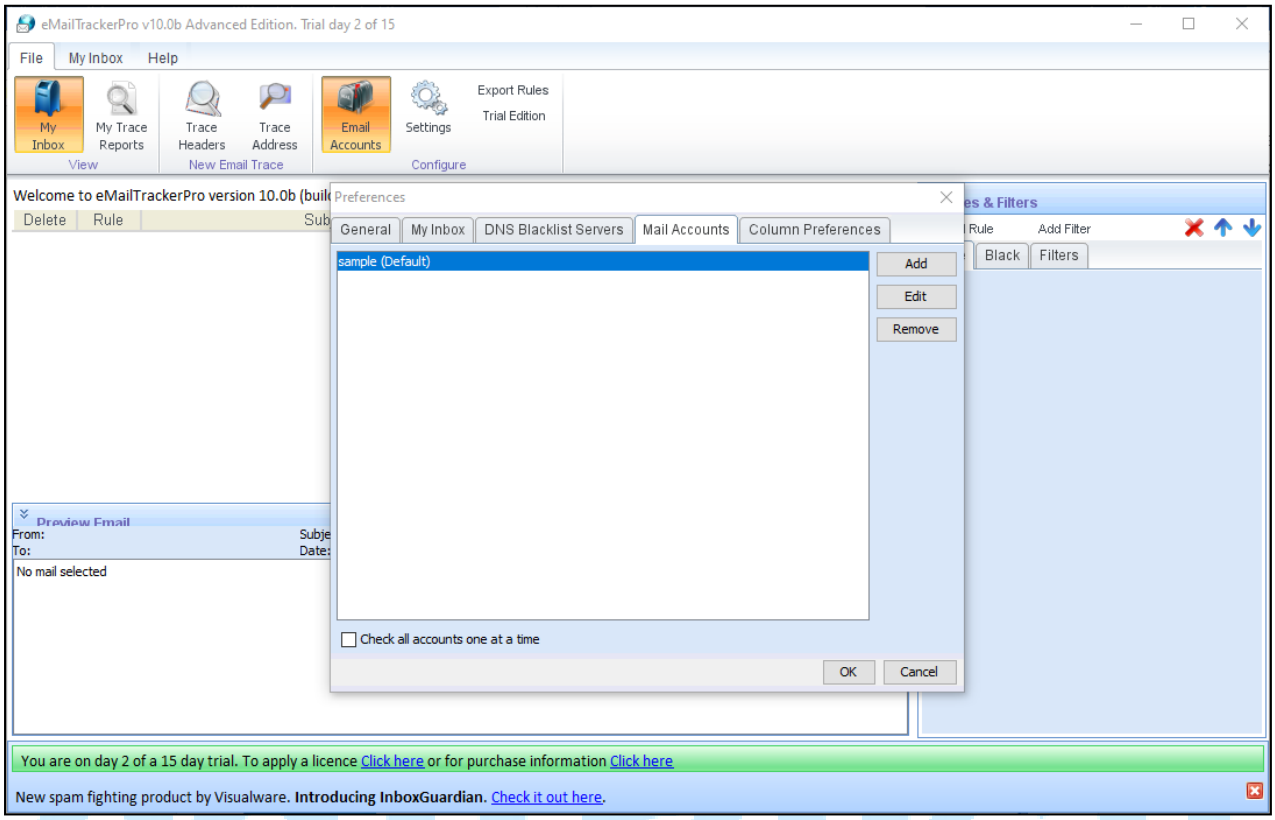


Step 3: Click on add to add an account

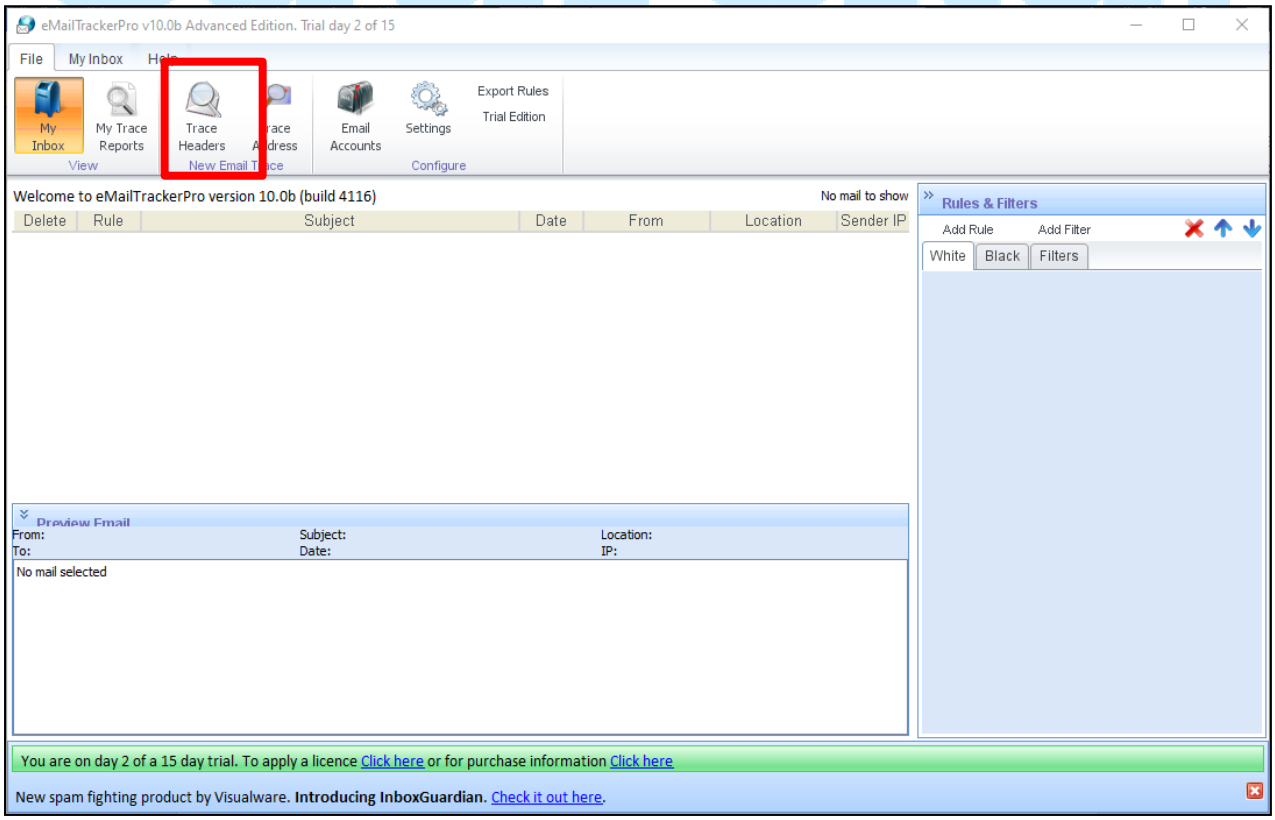




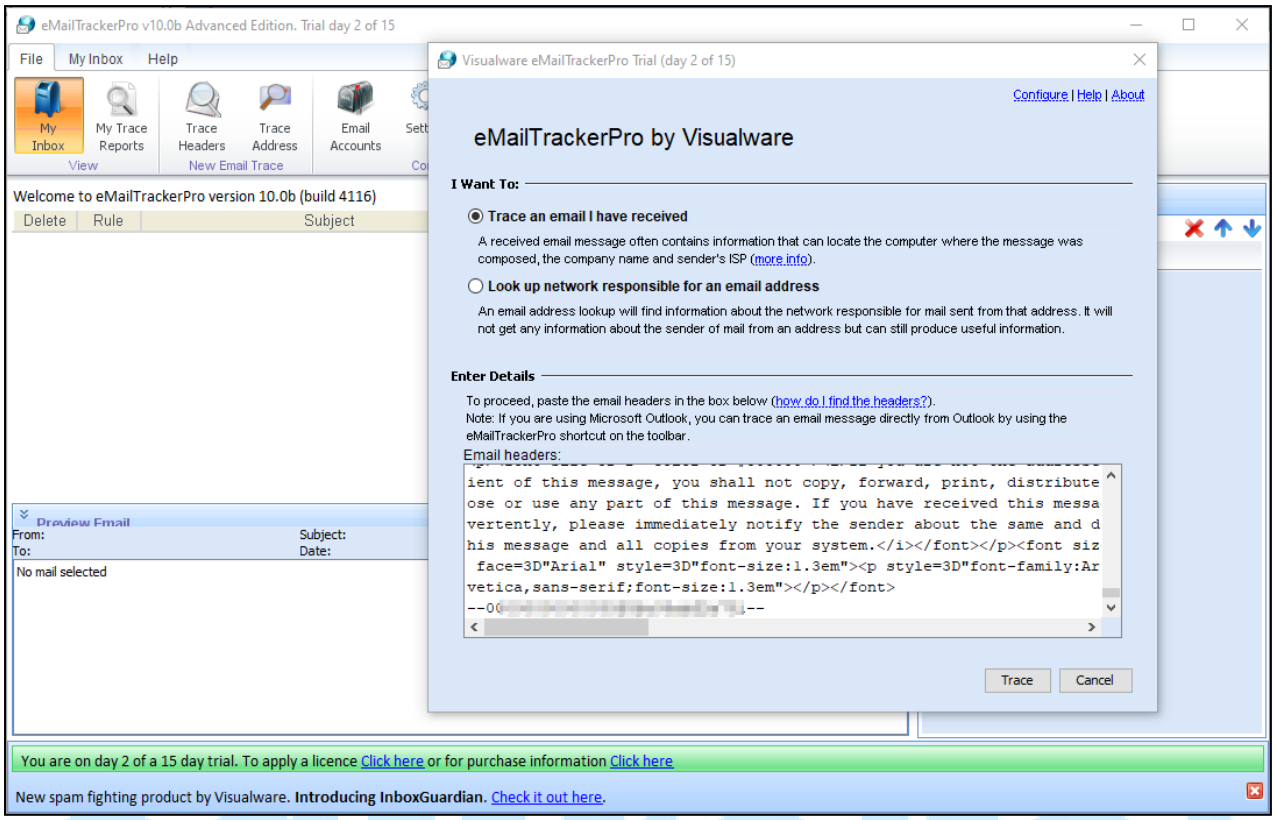
Step 4: After adding the account successfully, it will appear as a list under Mail Accounts Tab. Select it and click ok



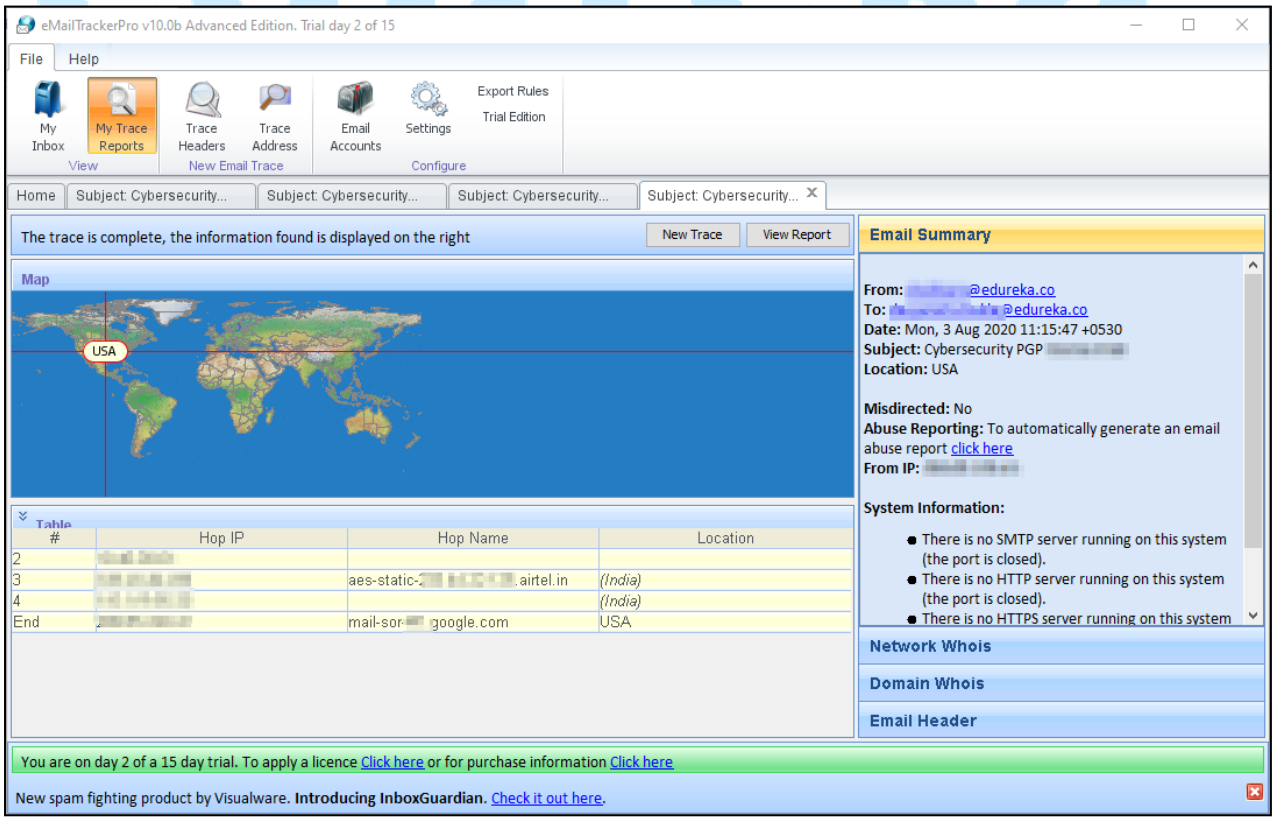
Step 5: Select Trace Headers under File Tab



Step 6: Paste the details of the eMail header you want to track and click Trace

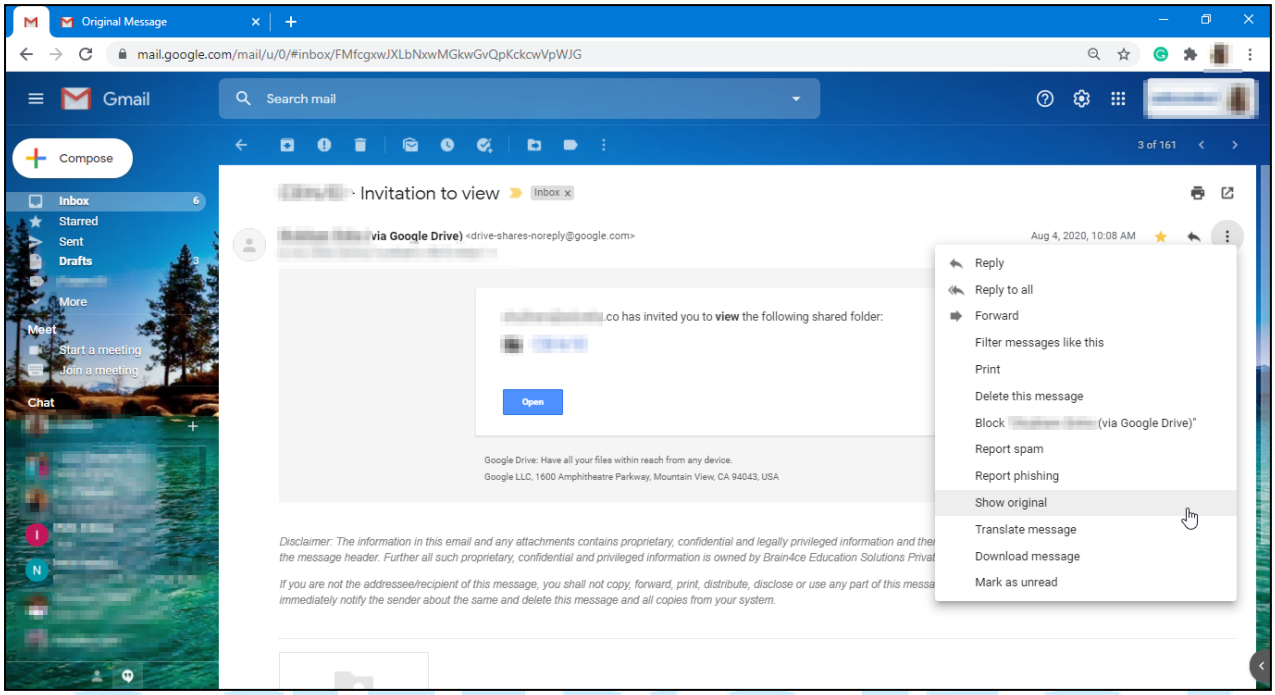


Step 7: The results are now displayed and you can trace them from the Email Summary

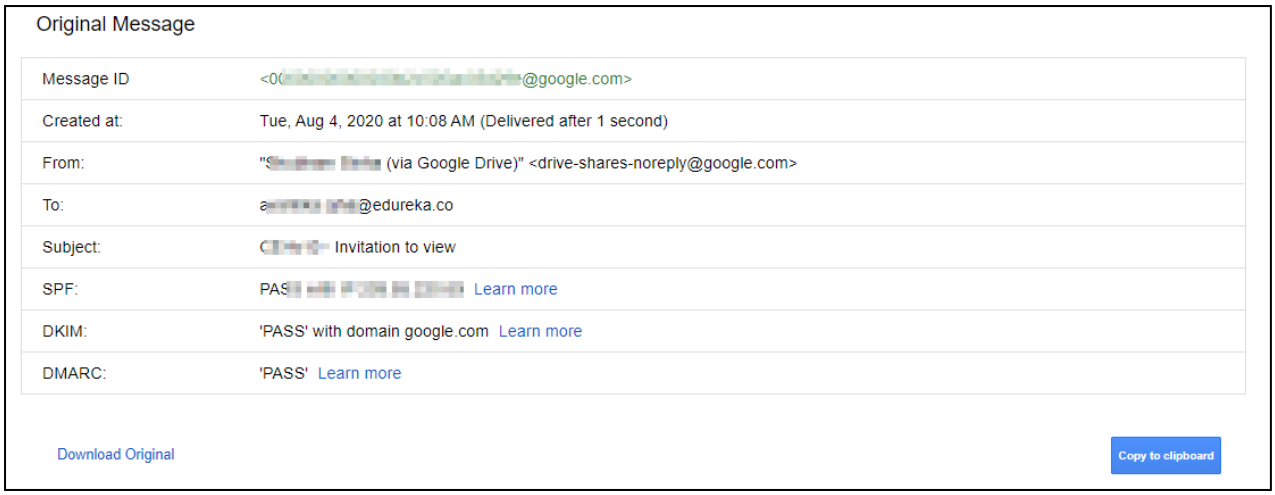


(b) Collecting Information from Email Header

Step 1: Select original message from the Email options



This will open the new window with the original message containing Email Headers which provides information such as Mail Server, Internal IP address Scheme, Sender, Subject, Timestamp, Recipient, Return-Path, DomainKeys Signature, Mime-Version, Message-id etc.



```
Delivered-To: [redacted]
Received: by 2002:a5d:538d:0:0:0:0:0 with SMTP id d13csp104482wrv;
        Mon, 3 [redacted] 2020 21:38:05 -0700 (PDT)
X-Received: by 200[redacted]a:: with SMTP id [redacted]15885662;
        Mon, 03 Aug 2020 21:38:05 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=15[redacted]5; cv=none;
        d=google.com; s=arc-2[redacted]6;
        b=FqsA[redacted]
         pPc2V[redacted]iJtLgN7txyr7
         b+BMT[redacted]7Avc33SwNuvH
         ucuDP0H9XLSE/RItMPY/YYSFg4FZCTpQ1jTUIRZ5J/SHhpQ1jTKvv528nT3MCCiKwoOd
         9uy4qlRjE9bc5qOXPAQvM2WiCVCrCLaeTGQqoo9govfhRCGEsj/CSRr2LiC9t5NaIXNN
         gkww==
ARC-Message-Signature: [redacted]laxed/relaxed; d=google.com; s=arc-[redacted]6;
        h=cc:to:from:subject:date:message-id:references:reply-to:mime-version
         :dkim-signature;
        bh=d[redacted]g=;
        b=ru1KYZGfpclK9uuqRewxrj4Zm7lu/LvElnyuqgAWNr1HvPQfmHFU+H32piE2LJ9SSf
         JzXBoBAt[redacted]qVqq3BDkaNwaDXD8s
         9bWroNb[redacted]5J6qA0AskRTjf7bgl
         XXkLDLtoCw0ri67ymCCyWCSTgCwC9RQi86aBy5euPMQA61Pmen/OsLmhniBTYFXSYR5
         3z/z4S6nml4hHDMnoE3RJlvDahw39a2G34/5ICRHpa96/+Jqy8PlH2rKUI0HP3qWbkRR
         IlIA==
ARC-Authentication-Results: i=1; mx.google.com;
       dki[redacted]
       spf[redacted]7jh@doclist.bounces [redacted]
sender) smtp.mailfrom=3LOYoXxQKAJs8MDQ9-NC5M9N-IJM9KGTBJJBG9.7JH@doclist.bounces.google.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=google.com
Return-Path: <3LOYoXx[redacted]@doclist.bounces.google.com>
Received: from mail-sor-[redacted] [redacted])
        by mx.google.com with SMTPS id v127s[redacted].05
        for <a[redacted]@edureka.co>
        (Google Transport Security);
        Mon, 03 Aug 2020 21:38:05 -0700 (PDT)
Received-SPF: pass (google.com: domain of 3loyoxxqkajs8mdq9-nc5m9n-ijm9kgtbjjbg9.7jh@doclist.bounces.google.com designates 209.85.220.69 as
permitted sender) client-ip=209.85.220.69;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@google.com header.s=20161025 header.b=EibugYj5;
       spf=pass (google.com: domain of 3loyoxxqkajs8mdq9-nc5m9n-ijm9kgtbjjbg9.7jh@doclist.bounces.google.com designates 209.85.220.69 as permitted
sender) smtp.mailfrom=3LOYoXxQKAJs8MDQ9-NC5M9N-IJM9KGTBJJBG9.7JH@doclist.bounces.google.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=google.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
```

```
X-Gm-Message-State: A[redacted]
7EEtSa2o9QWNVPeMQZaCurOiMR626GkOtFYdKxyR[redacted]g=
X-Google-Smtp-Source: A[redacted]FoYdgUtYZHCm95nvpw=
MIME-Version: 1.0
X-Received: by 200[redacted]7; Mon, 03 Aug 2020 21:38:04 -0700 (PDT)
Reply-To: S[redacted]a <s[redacted]@edureka.co>
X-No-Auto-Attachment: 1
References: <aa[redacted]@[redacted]ocs-share.google.com>
Message-ID: <0[redacted]@google.com>
Date: Tue, 04 Aug 2020 04:38:04 +0000
Subject: CEHv10 - Invitation to view
From: "S[redacted]a (via Google Drive)" <drive-shares-noreply@google.com>
To: a[redacted]@edureka.co
Cc: [redacted]@edureka.co, [redacted]@edureka.co, [redacted]edureka.co
Content-Type: multipart/alternative; boundary="000000[redacted]b"

--[redacted]9b
Content-Type: text/plain; charset="UTF-8"; format=flowed; delsp=yes
Content-Transfer-Encoding: quoted-printable

I've shared an item with you:

[redacted]
[redacted]XfIyExUKL4ICoxTrp[redacted]=
p=3Dshari[redacted]

It's not an attachment -- it's stored online. To open this item, just click=
 =20
```

Demo 6: DNS Footprinting

Problem Statement:

Tool Used: **DNS Interrogation Tools**

Domain Name System footprinting, reveals information about DNS zone data. DNS zone data include DNS domain names, computer names, IP addresses, and much more about a particular network.

`Syntax: dnsrecon -d foxnews.co`

```
root@kali:~# dnsrecon -d foxnews.co
[*] Performing General Enumeration of Domain: foxnews.co
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to 72.52.10.14
[!] All queries will resolve to this address!!
[-] DNSSEC is not configured for foxnews.co
[*]      SOA ns1.markmonitor.com 64.124.69.50
[*]      NS ns1.markmonitor.com 64.124.69.50
[*]      NS ns2.markmonitor.com 162.88.60.13
[*]      Bind Version for 162.88.60.13 PowerDNS Authoritative Server 3.4.11 (jenk
ins@autotest.powerdns.com built 20170113105955 root@autotest.powerdns.com)
[*]      NS ns2.markmonitor.com 2600:2000:1000::13
[*]      NS ns3.markmonitor.com 162.88.61.15
[*]      Bind Version for 162.88.61.15 PowerDNS Authoritative Server 3.4.11 (jenk
ins@autotest.powerdns.com built 20170113105955 root@autotest.powerdns.com)
[*]      NS ns3.markmonitor.com 2600:2000:1001::15
[*]      NS ns4.markmonitor.com 162.88.60.15
[*]      Bind Version for 162.88.60.15 PowerDNS Authoritative Server 3.4.11 (jenk
ins@autotest.powerdns.com built 20170113105955 root@autotest.powerdns.com)
[*]      NS ns4.markmonitor.com 2600:2000:1000::15
[*]      NS ns5.markmonitor.com 162.88.61.17
[*]      Bind Version for 162.88.61.17 PowerDNS Authoritative Server 3.4.11 (jenk
ins@autotest.powerdns.com built 20170113105955 root@autotest.powerdns.com)
[*]      NS ns5.markmonitor.com 2600:2000:1001::17
[*]      NS ns6.markmonitor.com 162.88.60.17
[*]      Bind Version for 162.88.60.17 PowerDNS Authoritative Server 3.4.11 (jenk
ins@autotest.powerdns.com built 20170113105955 root@autotest.powerdns.com)
[*]      NS ns7.markmonitor.com 162.88.61.19
```

```
root@kali:~# fierce -dns edureka.co
DNS Servers for edureka.co:
        ns-429.awsdns-53.com
        ns-789.awsdns-34.net
        ns-1218.awsdns-24.org
        ns-1603.awsdns-08.co.uk

Trying zone transfer first...
        Testing ns-429.awsdns-53.com
                Request timed out or transfer not allowed.
        Testing ns-789.awsdns-34.net
                Request timed out or transfer not allowed.
        Testing ns-1218.awsdns-24.org
                Request timed out or transfer not allowed.
        Testing ns-1603.awsdns-08.co.uk
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
52.10.187.101   admin.edureka.co
99.86.47.16     cdn.edureka.co
99.86.47.29     cdn.edureka.co
99.86.47.44     cdn.edureka.co
```