

Module 1: Introduction to Cybersecurity & Ethical Hacking

Demo Document 1

edureka!

© Brain4ce Education Solutions Pvt. Ltd.

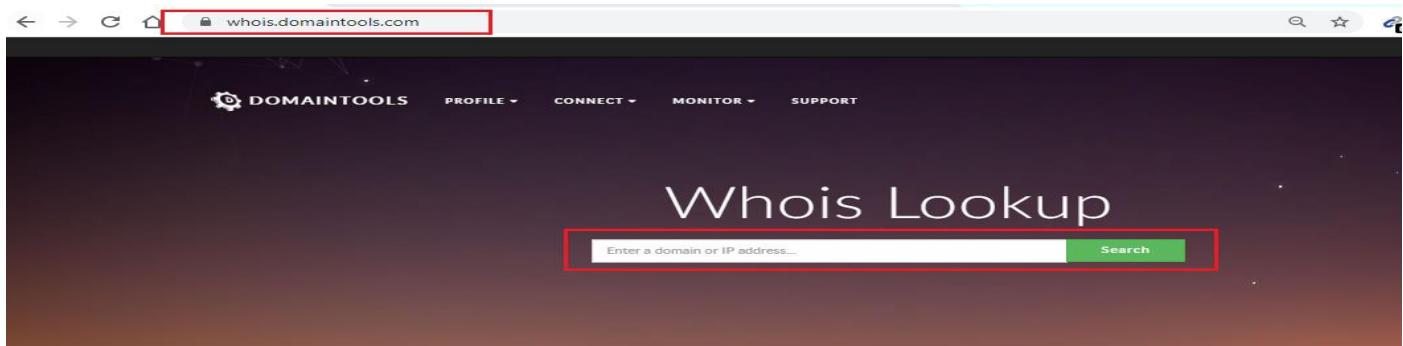
Demo 1: Gathering Information about Website

Problem Statement:

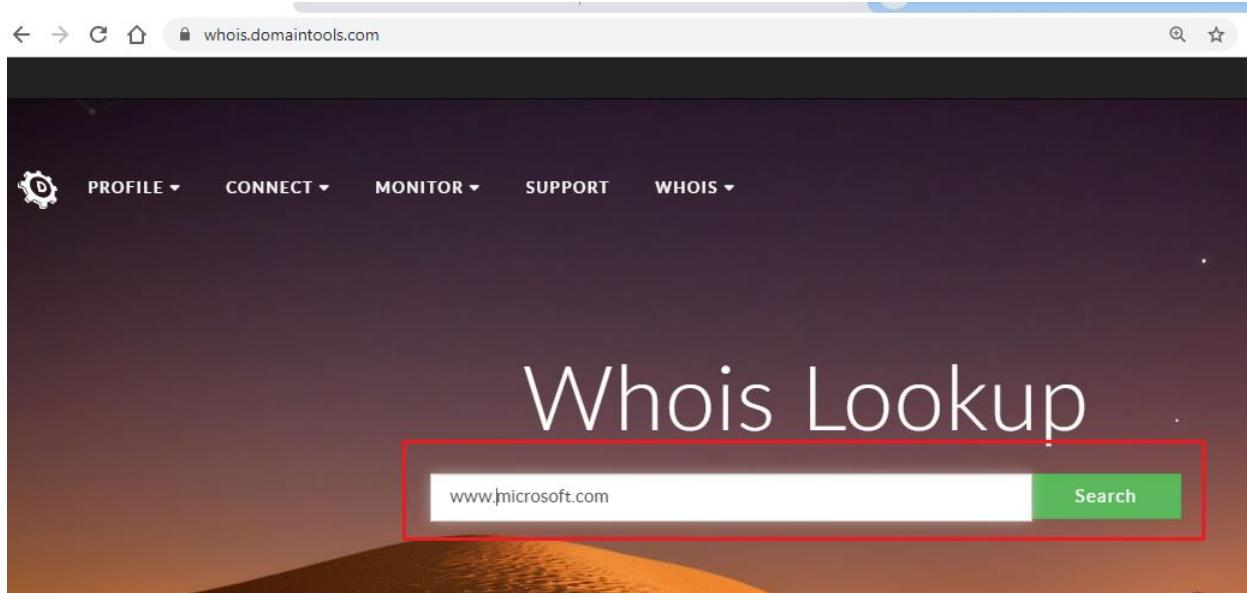
Gathering information about website and server information by using online resources.

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.

Whois Record for Microsoft.com

Domain Profile

Registrar: Domain Administrator
Registrant Org: Microsoft Corporation
Registrant Country: us

Registrar: MarkMonitor, Inc. MarkMonitor Inc.
IANA ID: 292
URL: http://www.markmonitor.com
Whois Server: whois.markmonitor.com
abusecomplaints@markmonitor.com
(p) 12083895770

Registrar Status: clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited

Dates: 10,655 days old
Created on 1991-05-01
Expires on 2021-05-02
Updated on 2020-06-03

Name Servers: NS1-205.AZURE-DNS.COM (has 277,080 domains), NS2-205.AZURE-DNS.NET (has 522 domains), NS3-205.AZURE-DNS.ORG (has 341 domains), NS4-205.AZURE-DNS.INFO (has 399 domains)

Tech Contact: MSN Hostmaster
Microsoft Corporation
One Microsoft Way.,
Redmond, WA, 98052, us
msnhst@microsoft.com
(p) 14258828080 (f) 14259367329

DomainTools Iris: More data. Better context. Faster response. Learn More

Tools: Hosting History, Monitor Domain Properties, Reverse IP Address Lookup, Network Tools

Visit Website: Microsoft Surface products

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.

IP Address: 23.36.249.251 - 5 other sites hosted on this server

IP Location: USA - Virginia - Ashburn - Akamai Technologies Inc.

ASN: AS16625 AKAMAI-AS, US (registered May 30, 2000)

Domain Status: Registered And Active Website

IP History: 244 changes on 244 unique IP addresses over 16 years

Registrar History: 4 registrars with 1 drop

Hosting History: 3 changes on 4 unique name servers over 0 year

Website

Website Title: Microsoft - Official Home Page

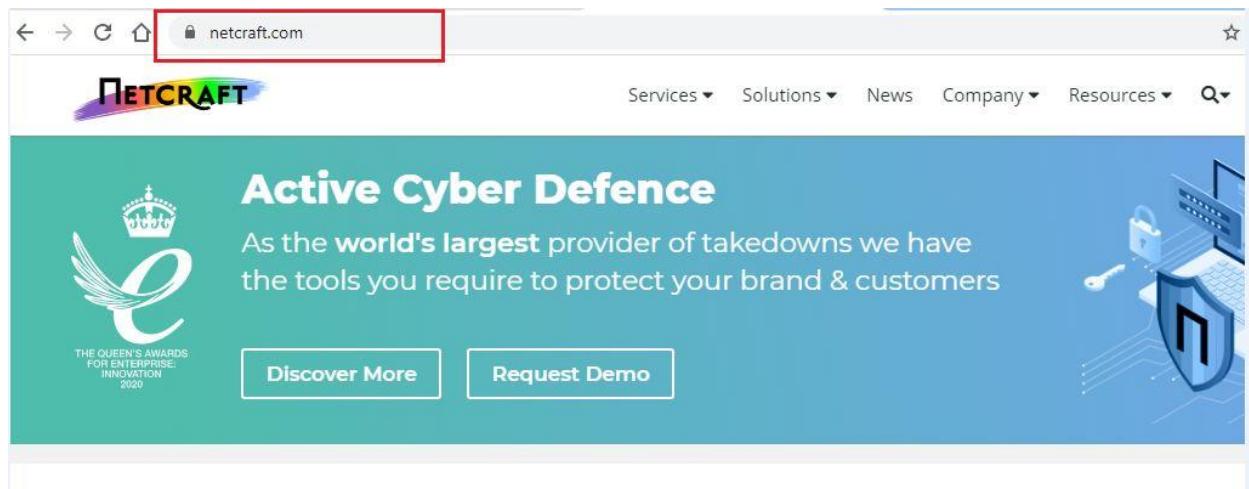
Response Code: 200

Terms: 527 (Unique: 270, Linked: 280)

Images: 24 (Alt tags missing: 2)

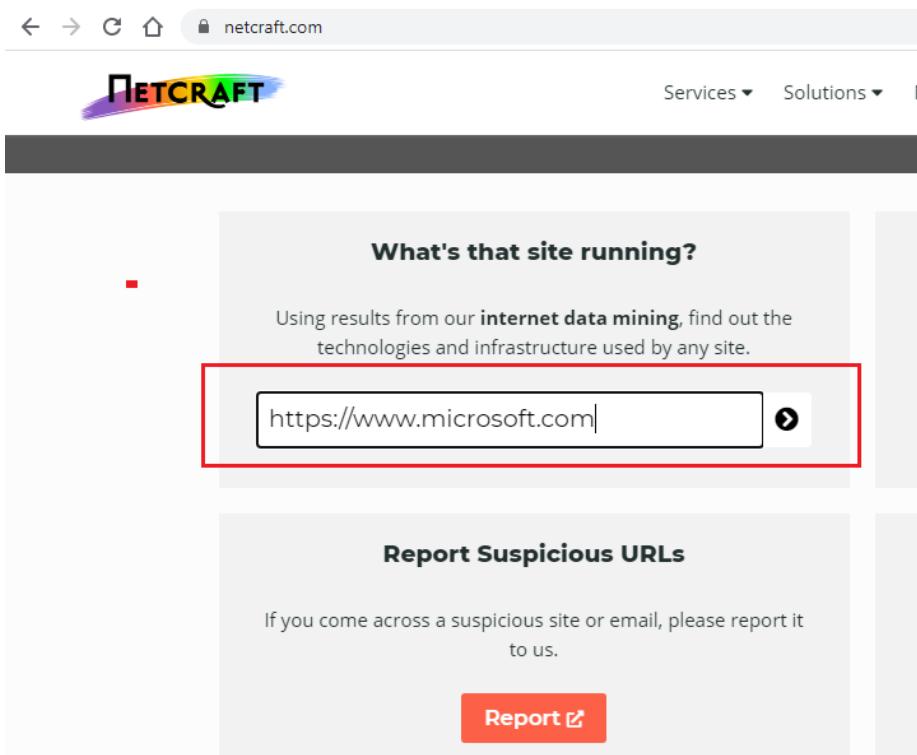
Links: 129 (Internal: 117, Outbound: 12)

Whois Record (last updated on 20200702)



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.

Module 1 – Introduction to Cybersecurity & Ethical Hacking

The screenshot shows the Netcraft Site report for <https://www.microsoft.com>. The page has a green header bar with the title and a search bar. Below it is a blue section titled "Site report for https://www.microsoft.com". It includes a "Background" section with site details like title, rank, and description, and a "Network" section showing domain information such as nameservers and IP addresses.

Site title	Microsoft - Official Home Page	Date first seen	May 2004
Site rank	114	Netcraft Risk Rating	0/10
Description	At Microsoft our mission and values are to help people and businesses throughout the world realize their full potential.		
Primary language	English		

Site	https://www.microsoft.com	Domain registrar	markmonitor.com
Netblock Owner	Akamai Technologies, Inc.	Nameserver organisation	whois.markmonitor.com
Domain	microsoft.com	Organisation	Microsoft Corporation, One Microsoft Way, Redmond, 98052, United States
Nameserver	ns1-205.azure-dns.net	Hosting company	Akamai Technologies
IP address	104.78.177.250 (virusTotal)	Top Level Domain	Commercial entities (.com)
DNS admin	azuredns-hostmaster@microsoft.com	DNS Security Extensions	unknown

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

The screenshot shows the SSL/TLS details for <https://www.microsoft.com>. It includes sections for certificate information, OCSP stapling, cipher suites, and version numbers.

Public key algorithm	rsaEncryption	Certificate Hash	x5rmGtK55x!PaViyOm8jF44h8
Protocol version	TLSv1.2	Public Key Hash	a9751d9b7c107e5008a392d642cc1d06e1b8af026b7f9ce3236e1b41695c593a
Public key length	2048	OCSP servers	http://ocsp.msocsp.com - 100% uptime in the past 24 hours
Certificate check	ok	OCSP stapling response	Certificate valid
Signature algorithm	sha256WithRSAEncryption	OCSP data generated	Jul 2 02:14:58 2020 GMT
Serial number	0xd000c371562c41d9394087f68000000c3715	OCSP data expires	Jul 6 02:14:58 2020 GMT
Cipher	ECDHE-RSA-AES128-GCM-SHA256		
Version number	0x02		

The screenshot shows detailed SSL/TLS configuration for <https://www.microsoft.com>. It includes sections for assurance, common name, organization, state, country, and organizational unit.

Assurance	Organisation validation	Perfect Forward Secrecy	Yes
Common name	www.microsoft.com	Next Protocol Negotiation	h2,h2-14,http/1.1,http/1.0
Organisation	Microsoft Corporation	Supported TLS Extensions	RFC5746 renegotiation info, RFC4366 server name, RFC4492 EC point formats, RFC5077 session ticket, RFC4366 status request, Next Protocol Negotiation
State	WA	Issuing organisation	Microsoft Corporation
Country	US	Issuer common name	Microsoft IT TLS CA 5
Organisational unit	Microsoft Corporation	Issuer unit	Microsoft IT
Subject Alternative Name	wwwqa.microsoft.com, www.microsoft.com, staticview.microsoft.com, is-microsoft.com, microsoft.com, c.s-microsoft.com, privacy.microsoft.com	Issuer location	Redmond
Validity period	From Oct 21 2019 to Oct 21 2021 (24 months)	Issuer country	US
Matches hostname	Yes	Issuer state	Washington
Server	AkamaiGHost	Certificate Revocation List	http://mscr1.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%205.crl http://cri.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%205.crl

Netblock owner

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-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	
Using ASP.NET	ASP.NET is running on the server	www.mayoclinic.org , www.dobreprogramy.pl , www.godaddy.com

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Web Worker	No description	www.pearltrees.com , www.wix.com , editor.wix.com
Asynchronous Javascript	No description	www.researchgate.net , freebitco.in
Local Storage	No description	www.grammarly.com , www.webmd.com , www.tripadvisor.com
Session Storage	No description	www.grammarly.com , www.webmd.com , www.tripadvisor.com
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	t.co

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.

The screenshot shows the Shodan search interface with the URL 'shodan.io' in the address bar and 'microsoft.com' in the search input field. The main heading is 'The search engine for Security'. Below it, there's a sub-headline 'Shodan is the world's first search engine for Internet-connected devices.' On the left, there are four cards: 'Explore the Internet of Things' (cloud icon), 'Monitor Network Security' (eye icon), 'See the Big Picture' (globe icon), and 'Get a Competitive Advantage' (dollar sign icon). The central part of the page displays a globe with numerous red dots representing found devices, with some specific IP addresses like '67.20.69.105' and '50.87.75.184' labeled. A large blue watermark 'EQUICKA!' is overlaid across the middle of the page.

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.

The screenshot shows the Shodan search results for 'microsoft.com'. The top section displays 'TOTAL RESULTS' as 11,077. Below this, there's a 'TOP COUNTRIES' map where most countries are highlighted in red. A table lists the top countries with their counts: United States (5,794), Netherlands (2,594), China (356), Brazil (271), and Australia (184). The 'TOP SERVICES' section shows HTTPS (3,852) and SSH (523) as the most common services. The 'TOP ORGANIZATIONS' section lists Microsoft Azure (7,004) and Amazon.com (455) as the largest organizations. The main content area shows an 'HTTP Status 404 – Not Found' entry for '199.42.13.125' belonging to 'EntServ Deutschland GmbH' from the United States. It includes an SSL certificate section with details about the certificate issuer and supported SSL versions (TLSv1.2). Another 'HTTP Status 404 – Not Found' entry for '51.145.210.11' belonging to 'Microsoft Azure' from the Netherlands is also shown.

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

The screenshot shows the Shodan search interface for the query 'microsoft.com'. It displays a map of the world with red dots indicating found servers. Below the map are sections for 'TOTAL RESULTS' (11,077), 'TOP COUNTRIES', 'TOP SERVICES', and 'TOP ORGANIZATIONS'. On the right, detailed information is shown for two specific servers. The first server, highlighted with a red box, is '199.42.13.125' (EntServ Deutschland GmbH) located in the United States. It has an SSL certificate issued by VR IDENT SSL CA (2018). The second server listed is '51.145.210.11' (Microsoft Azure) located in the Netherlands, Amsterdam. Both entries show supported SSL versions (TLSv1.2).

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.

This screenshot shows the detailed information for the server 199.42.13.125. It includes a table with server details (Country: United States, Organization: EntServ Deutschland GmbH, ISP: EntServ Deutschland GmbH, Last Update: 2020-07-02T17:01:28.394359, ASN: AS6900) and a 'Ports' section showing ports 443 and 8443. The 'Services' section lists Apache Tomcat/Coyote JSP engine (Version: 1.1) running on port 443 (tcp, https). The 'SSL Certificate' section shows an SSL certificate for Microsoft (DigiCert SHA2 Secure Server CA) issued by DigiCert.

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

SSL Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number:
06:d9:c4:e8:6b:b0:a7:e7:70:92:35:e8:95:00:f7:9e:4c:8f:96:7e

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=DE, O=Fiducia & GAD IT AG, OU=VR IDENT, CN=VR IDENT SSL CA 2018

Validity

Not Before: Nov 25 10:46:28 2019 GMT
Not After : Nov 25 10:56:00 2021 GMT

Subject: C=DE, ST=Nordrhein-Westfalen, L=D\xC3\x9CSSELDORF, O=DEUTSCHE APOTHEKER- UN D \xC3\x84RZTEBANK EG, CN=mdm.apobank.de

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:b0:59:60:45:11:4f:04:7b:b3:29:55:69:e2:91:
93:bf:6b:63:87:87:37:f6:57:75:b0:76:8f:a7:
e8:23:09:7a:40:e7:ff:01:1a:95:20:56:b6:d5:f3:
47:df:a6:55:a5:9f:41:d5:01:c2:b8:89:51:fb:29:
45:6b:ea:65:37:09:4b:56:35:ad:69:99:c7:6d:b9:
0f:3e:fd:95:00:24:cd:1f:bd:fa:8a:fd:52:a8:d8:
9c:60:d1:fd:c1:00:24:00:2a:31:75:9b:b1:e7:c1:
c6:0f:fd:cc:2a:83:47:e0:31:35:28:48:a4:f1:11:
6a:93:5d:22:a2:9a:b9:9f:f1:a0:a7:c7:8a:7f:1d:
77:05:37:5c:f1:d7:b2:aab:be:e2:a2:23:7e:9a:26:
4d:e2:bc:44:0e:8e:96:5e:1f:a2:4d:89:10:4e:93:
93:90:9d:c4:26:3c:e9:d5:c7:f8:21:30:12:35:4a:
3c:1b:ee:51:8f:c8:a1:b7:63:6b:21:10:35:50:88:
59:71:06:a0:26:44:06:95:ea:06:46:f7:45:52:00:
a4:ad:c0:69:17:2d:18:76:b7:04:2b:38:1e:ef:c0:
3b:71:d7:55:1b:a2:05:ce:c9:b6:bb:eb:3f:c1:8e:
7d:84:52:99:55:58:43:ab:14:fd:c3:29:9c:58:80:
...

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/>

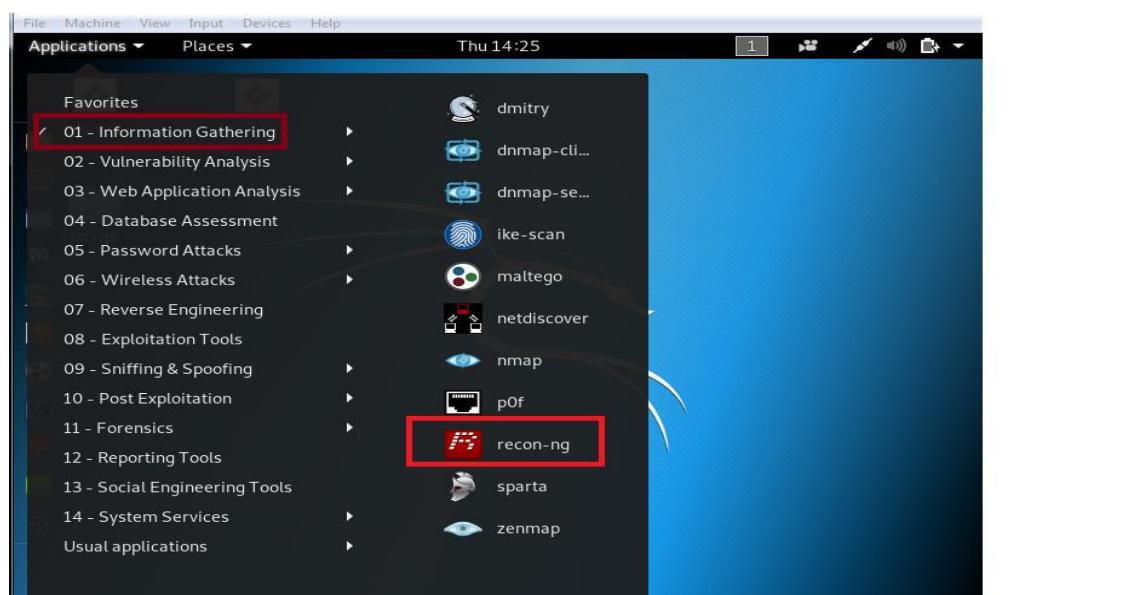
Demo 2: Gathering Information about Domain through Recon-ng Tool in Kali Linux

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



```
root@osboxes:~/recon-ng# ./recon-ng
[*] Database upgraded to version 10.

Sponsored by...
          /\_/\ 
         / \ \_/\ 
        /   \ \_/\ 
       /     \ \_/\ 
      /       \ \_/\ 
     /         \ \_/\ 
    /           \ \_/\ 
   /             \ \_/\ 
  /               \ \_/\ 
 /                 \ \_/\ 
\                 / \_/\ 
 \               / \_/\ 
  \             / \_/\ 
   \           / \_/\ 
    \         / \_/\ 
     \       / \_/\ 
      \     / \_/\ 
       \   / \_/\ 
        \ / \_/\ 
         \ / \_/\ 
          \ / \_/\ 
           \ / \_/\ 
            \ / \_/\ 
             \ / \_/\ 
              \ / \_/\ 
               \ / \_/\ 
                \ / \_/\ 
                 \ / \_/\ 
                  \ / \_/\ 
                   \ / \_/\ 
                    \ / \_/\ 
                     \ / \_/\ 
                      \ / \_/\ 
                       \ / \_/\ 
                        \ / \_/\ 
                         \ / \_/\ 
                          \ / \_/\ 
                           \ / \_/\ 
                            \ / \_/\ 
                             \ / \_/\ 
                              \ / \_/\ 
                               \ / \_/\ 
                                \ / \_/\ 
                                 \ / \_/\ 
                                  \ / \_/\ 
                                   \ / \_/\ 
                                    \ / \_/\ 
                                     \ / \_/\ 
                                      \ / \_/\ 
                                       \ / \_/\ 
                                        \ / \_/\ 
                                         \ / \_/\ 
                                          \ / \_/\ 
                                           \ / \_/\ 
                                            \ / \_/\ 
                                             \ / \_/\ 
                                              \ / \_/\ 
                                               \ / \_/\ 
                                                \ / \_/\ 
                                                 \ / \_/\ 
                                                  \ / \_/\ 
                                                   \ / \_/\ 
                                                    \ / \_/\ 
                                                     \ / \_/\ 
                                                      \ / \_/\ 
                                                       \ / \_/\ 
                                                        \ / \_/\ 
                                                         \ / \_/\ 
                                                          \ / \_/\ 
                                                           \ / \_/\ 
                                                            \ / \_/\ 
                                                             \ / \_/\ 
                                                               \ / \_/\ 
                                                                \ / \_/\ 
                                                                 \ / \_/\ 
                                                                 [recon-ng v5.1.1, Tim Tomes (@lanmaster53)]
```

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-nql][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/woxy_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
```

The screenshot shows a terminal window with a red box highlighting the command history and configuration. Below it, the results for Microsoft.com subdomains are listed under the heading 'MICROSOFT.COM'.

```
[recon-ng][default] >  
[recon-ng][default] > modules load recon/domains-hosts/bing_domain_web  
[recon-ng][default][bing_domain_web] > options set SOURCE microsoft.com  
SOURCE => microsoft.com  
[recon-ng][default][bing_domain_web] > run
```

MICROSOFT.COM

```
[*] URL: https://www.bing.com/search?first=0&q=domain%3Amicrosoft.com  
[*] Country: None  
[*] Host: azure.microsoft.com  
[*] Ip_Address: None  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
-----  
[*] Country: None  
[*] Host: covid19testing.microsoft.com  
[*] Ip_Address: None  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
-----  
[*] Country: None  
[*] Host: www.msdn.microsoft.com  
[*] Ip_Address: None  
[*] Latitude: None
```

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][brute_hosts] > options set SOURCE microsoft.com
```

SOURCE => microsoft.com

```
[recon-ng][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.
[*] ac.microsoft.com => No record found.
[*] accounts.microsoft.com => (CNAME) account.microsoft.com.edgekey.net
[*] 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
```

```
[*] agent.microsoft.com => (A) 134.170.188.221
[*] ajax.microsoft.com => (CNAME) mscomajax.vo.msecnd.net
[*] Country: None
[*] Host: agent.microsoft.com
[*] Ip_Address: 134.170.188.221
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[...]
[*] afiliados.microsoft.com => No record found.
[*] Country: None
[*] Host: mscomajax.vo.msecnd.net
[*] Ip Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[...]
[*] Country: None
[*] Host: ajax.microsoft.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[...]
[*] ajax.microsoft.com => (CNAME) cs22.wpc.v0cdn.net
[*] agenda.microsoft.com => No record found.
[*] Country: None
```

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

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

+-----+
|           Path          | Version | Status | Updated | D | K |
+-----+
| discovery/info_disclosure/interesting_files | 1.1     | installed | 2020-01-13 |   |   |
+-----+

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

[recon-ng][default] > modules install discovery/info_disclosure/interesting_files
Interfaces with installed modules

Usage: modules <load|reload|search> [...]

[recon-ng][default] > modules load discovery/info_disclosure/interesting_files
[recon-ng][interesting_files] > run
```

```
[recon-ng][default][interesting_files] > run
[*] http://azure.microsoft.com:80/robots.txt => 200. 'robots.txt' found!
[*] http://azure.microsoft.com:80/sitemap.xml => 404
[*] http://azure.microsoft.com:80/sitemap.xml.gz => 404
[*] http://azure.microsoft.com:80/crossdomain.xml => 404
[*] http://azure.microsoft.com:80/phpinfo.php => 404
[*] http://azure.microsoft.com:80/test.php => 404
[*] http://azure.microsoft.com:80/elmah.axd => 404
[*] http://azure.microsoft.com:80/server-status => 404
[*] http://azure.microsoft.com:80/jmx-console/ => 404
[*] http://azure.microsoft.com:80/admin-console/ => 404
[*] http://azure.microsoft.com:80/web-console/ => 404
[*] http://covid19testing.microsoft.com:80/robots.txt => 200. 'robots.txt' found but unverified.
[*] http://covid19testing.microsoft.com:80/sitemap.xml => 200. 'sitemap.xml' found but unverified.
[*] http://covid19testing.microsoft.com:80/sitemap.xml.gz => 200. 'sitemap.xml.gz' found but unverified.
[*] http://covid19testing.microsoft.com:80/crossdomain.xml => 200. 'crossdomain.xml' found but unverified.
[*] http://covid19testing.microsoft.com:80/phpinfo.php => 200. 'phpinfo.php' found but unverified.
[*] http://covid19testing.microsoft.com:80/test.php => 200. 'test.php' found but unverified.
[*] http://covid19testing.microsoft.com:80/elmah.axd => 200. 'elmah.axd' found but unverified.
[*] http://covid19testing.microsoft.com:80/server-status => 200. 'server-status' found but unverified.
[*] http://covid19testing.microsoft.com:80/jmx-console/ => 200. 'jmx-console/' found but unverified.
[*] http://covid19testing.microsoft.com:80/admin-console/ => 200. 'admin-console/' found but unverified.
[*] http://covid19testing.microsoft.com:80/web-console/ => 200. 'web-console/' found but unverified.
[*] http://www.msdn.microsoft.com:80/robots.txt => 403
[*] http://www.msdn.microsoft.com:80/sitemap.xml => 403
[*] http://www.msdn.microsoft.com:80/sitemap.xml.gz => 403
[*] http://www.msdn.microsoft.com:80/crossdomain.xml => 403
[*] http://www.msdn.microsoft.com:80/phpinfo.php => 403
[*] http://www.msdn.microsoft.com:80/test.php => 403
[*] http://www.msdn.microsoft.com:80/elmah.axd => 403
```

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

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_poc
2	CHRISTINA		AADLAND	v-chrisa@microsoft.com	Whois contact	Murray, UT	United States	whois_poc
3	Christina		Aadland	v-chrisa@microsoft.com	Whois contact	Redmond, WA	United States	whois_poc
4			Abuse	abuse@microsoft.com	Whois contact	Redmond, WA	United States	whois_poc
5	Melissa		Allison	mallison@ocmcdonald.onmicrosoft.com	Whois contact	Sj, CA	United States	whois_poc
6	Jeffrey		Amels	jamel@microsoft.com	Whois contact	Kent, WA	United States	whois_poc
7	BRAD		AUSTIN	brada@microsoft.com	Whois contact	Charlotte, NC	United States	whois_poc
8	JO		BAKER	jolynb@microsoft.com	Whois contact	Tukwila, WA	United States	whois_poc
9	Ram		Balakrishnan	rambala@microsoft.com	Whois contact	Redmond, WA	United States	whois_poc
10	david		Balko	dbalko@sfscapital.onmicrosoft.com	Whois contact	Rockwall, TX	United States	whois_poc
11	ADAM		BECKER	adam.becker@primew.onmicrosoft.com	Whois contact	Denver, CO	United States	whois_poc

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-nal][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-nal][default] >
[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] > █
```

The screenshot shows a web browser window titled "Recon-ng Reconnaissance Report". The URL in the address bar is "file:///root/.recon-ng/workspaces/default/results.html". The page content is titled "microsoft Recon-ng Reconnaissance Report". Below the title, there is a section titled "[+] Summary" which contains a table with the following data:

table	count
domains	1
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	56
contacts	11
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

At the bottom left of the main content area, there is a link labeled "[+] Domains".

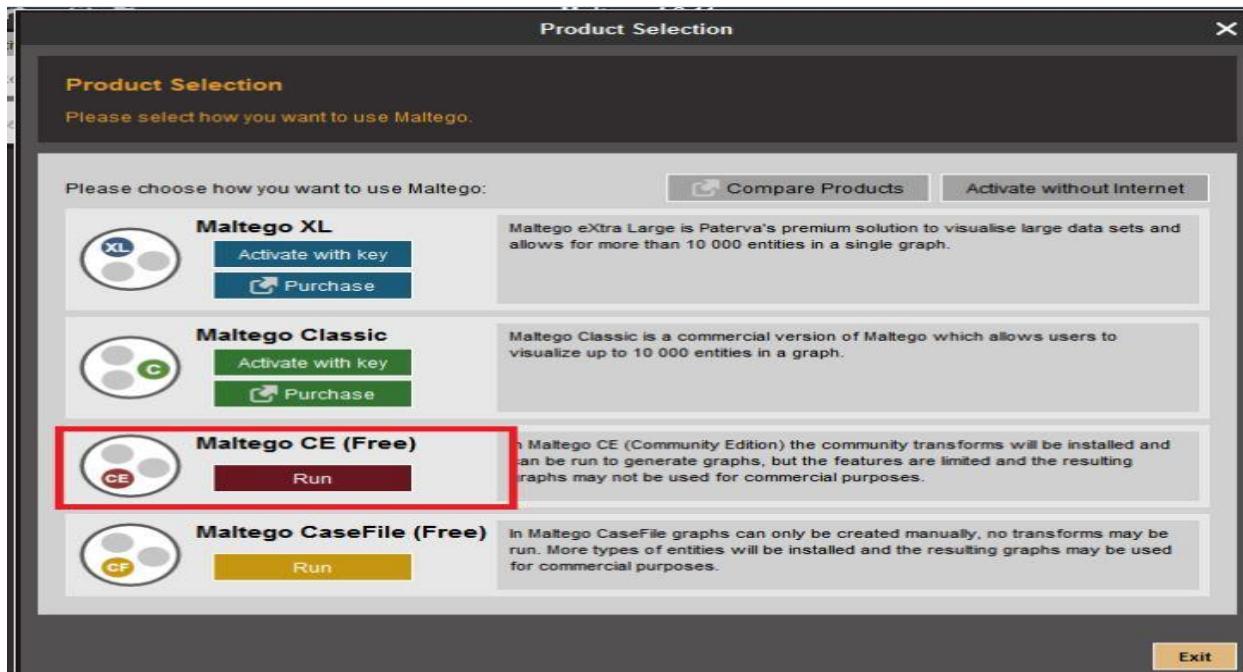
Demo 3: Information Gathering of Domain through Maltego Tool

Problem Statement:

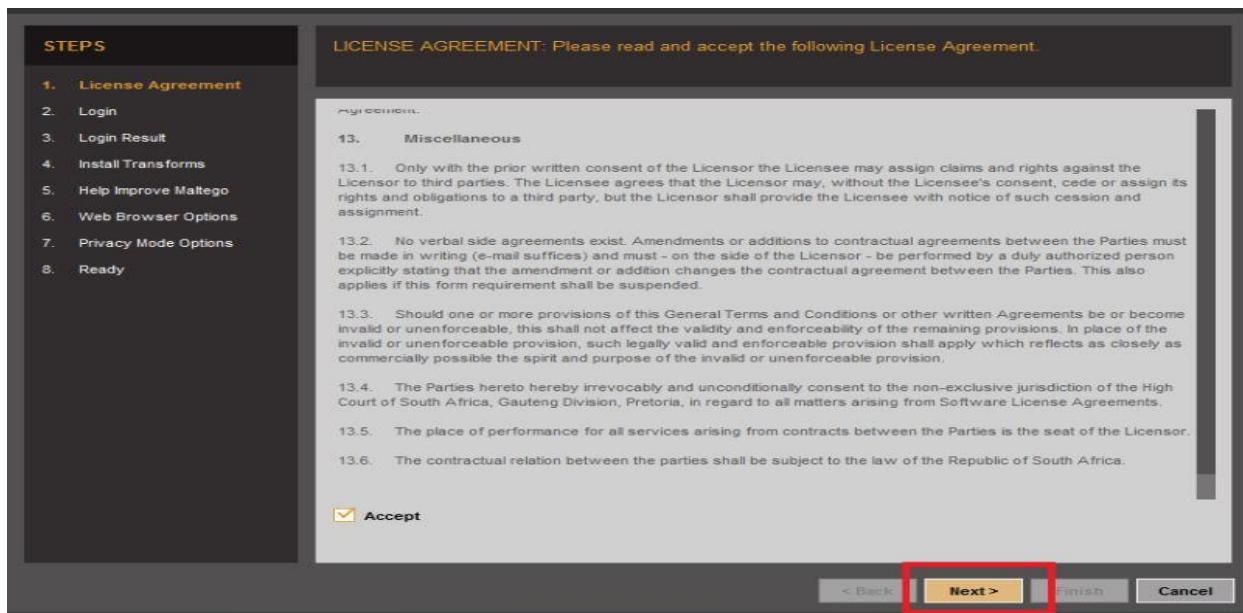
Gathering information about website and server by using the Maltego tool.

Solution:

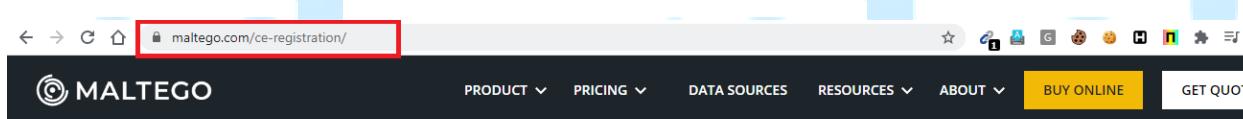
Step 1: Open Kali Linux and search for Maltego Software and click on **Maltego CE (Free)-Community Edition**.



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



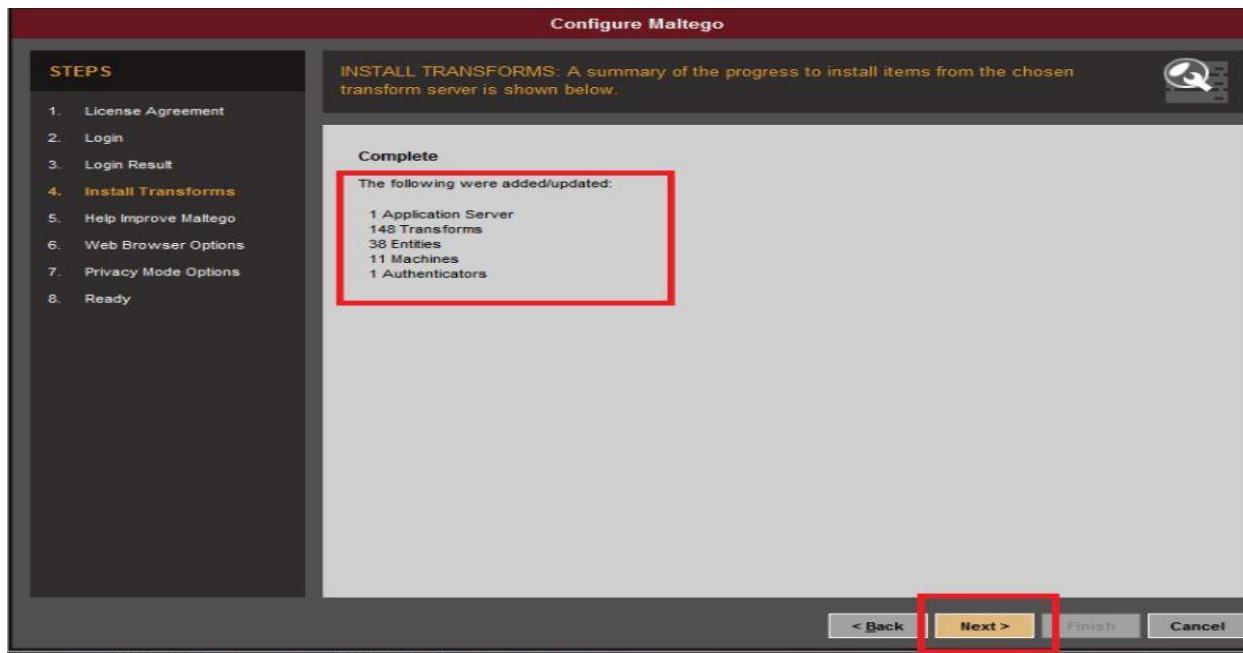
Step 3: Register accounts for Maltego (www.maltego.com/ce-registration/) by providing your details and will get a verification mail to your registered email to confirm your account.



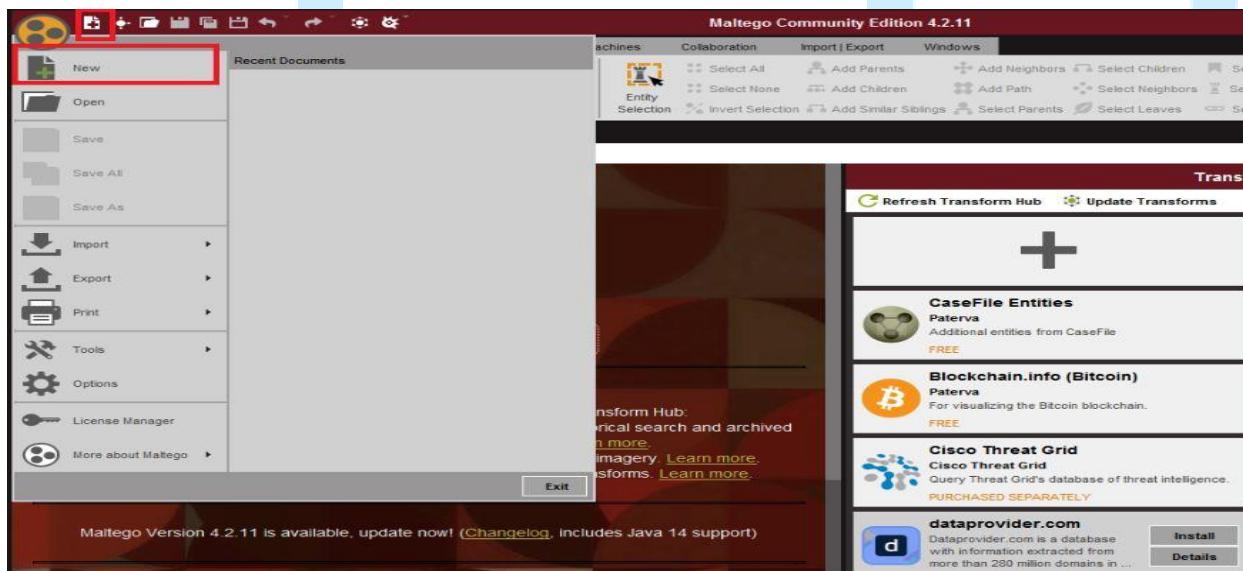
Step 4: Login into the Maltego account in the application and click on **Next**.

The image consists of two vertically stacked screenshots of a software setup wizard for Maltego. Both screenshots show a sidebar on the left with a list of steps: 1. License Agreement, 2. Login, 3. Login Result, 4. Install Transforms, 5. Help Improve Maltego, 6. Web Browser Options, 7. Privacy Mode Options, and 8. Ready. The main area shows a 'LOGIN' screen with a red box highlighting the 'Login' section where email and password are entered. A CAPTCHA image 'A5M' is shown below the fields. The 'Next >' button at the bottom is also highlighted with a red box. The second screenshot shows the 'LOGIN RESULT' screen, which displays a welcome message 'Hello ehacking4all, welcome to Maltego Community Edition!', personal details (First name: ehacking4all, Surname: ehack, Email address: ehacking4all@gmail.com), and a note that the API key is valid until July 16, 2020 at 12:00:00 AM IST. The 'Next >' button here is also highlighted with a red box.

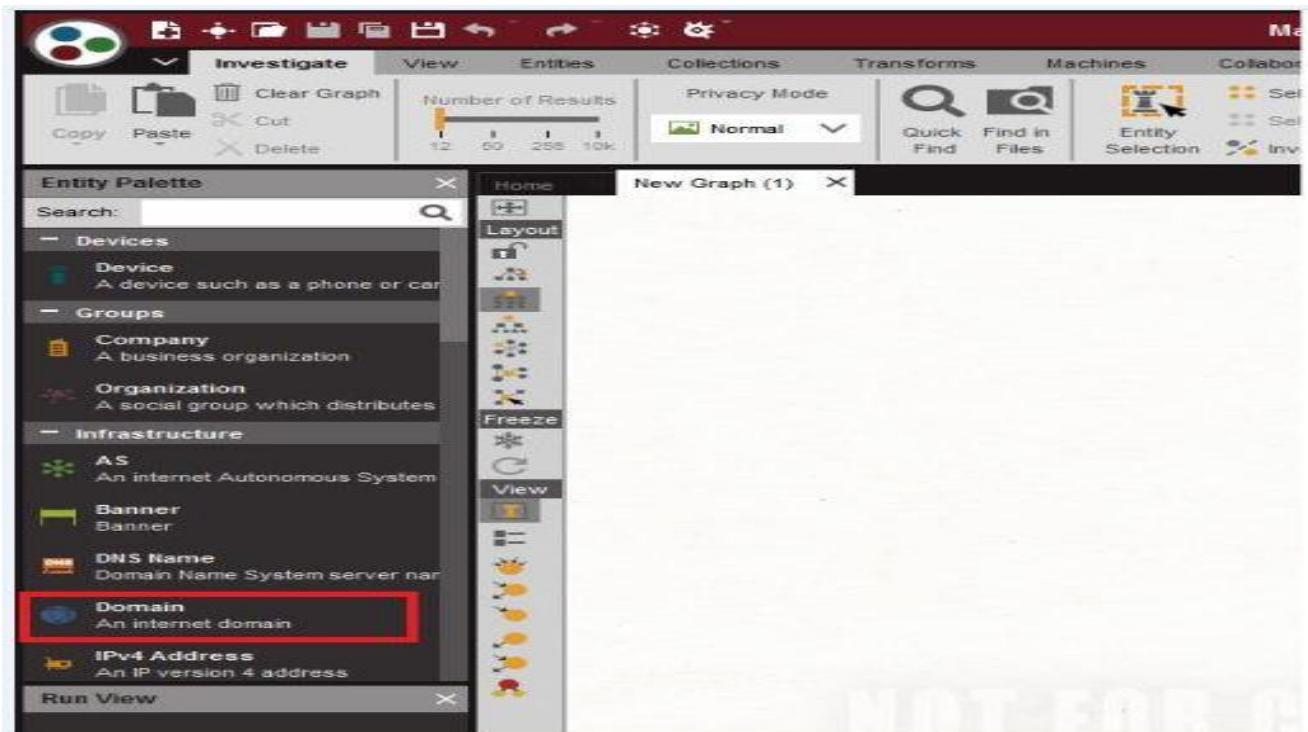
Step 5: Default transforms add-ons will be added and click on **NEXT**.



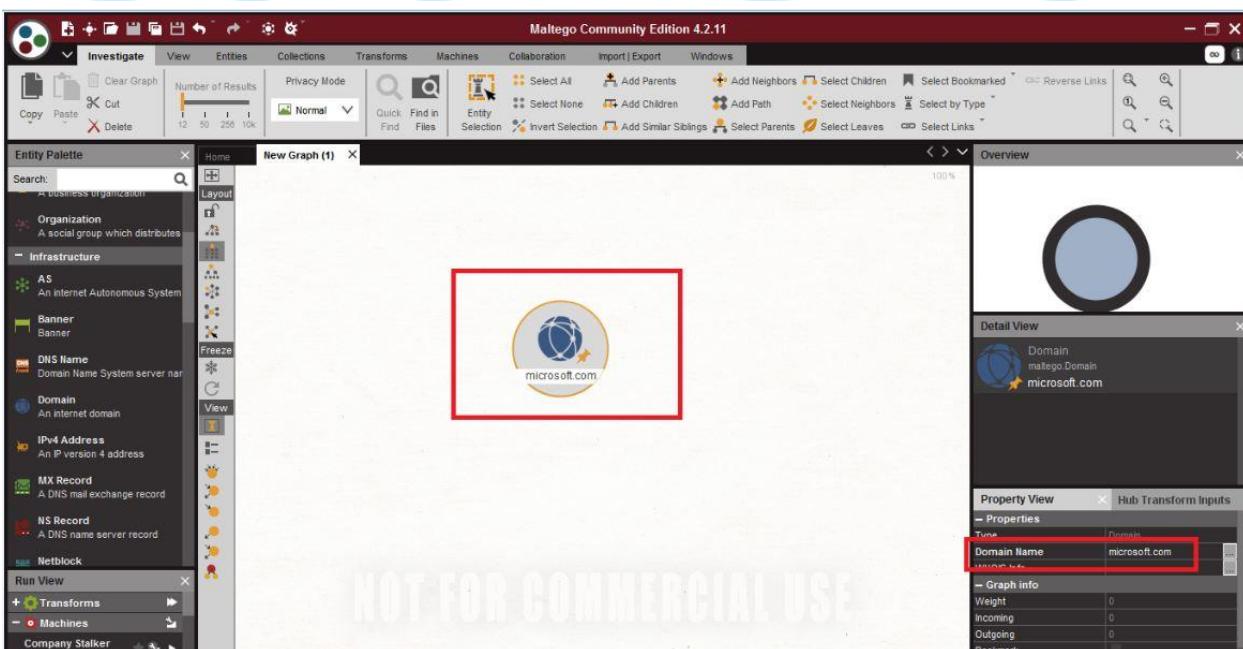
Step 6: Click on **New** for workspace.



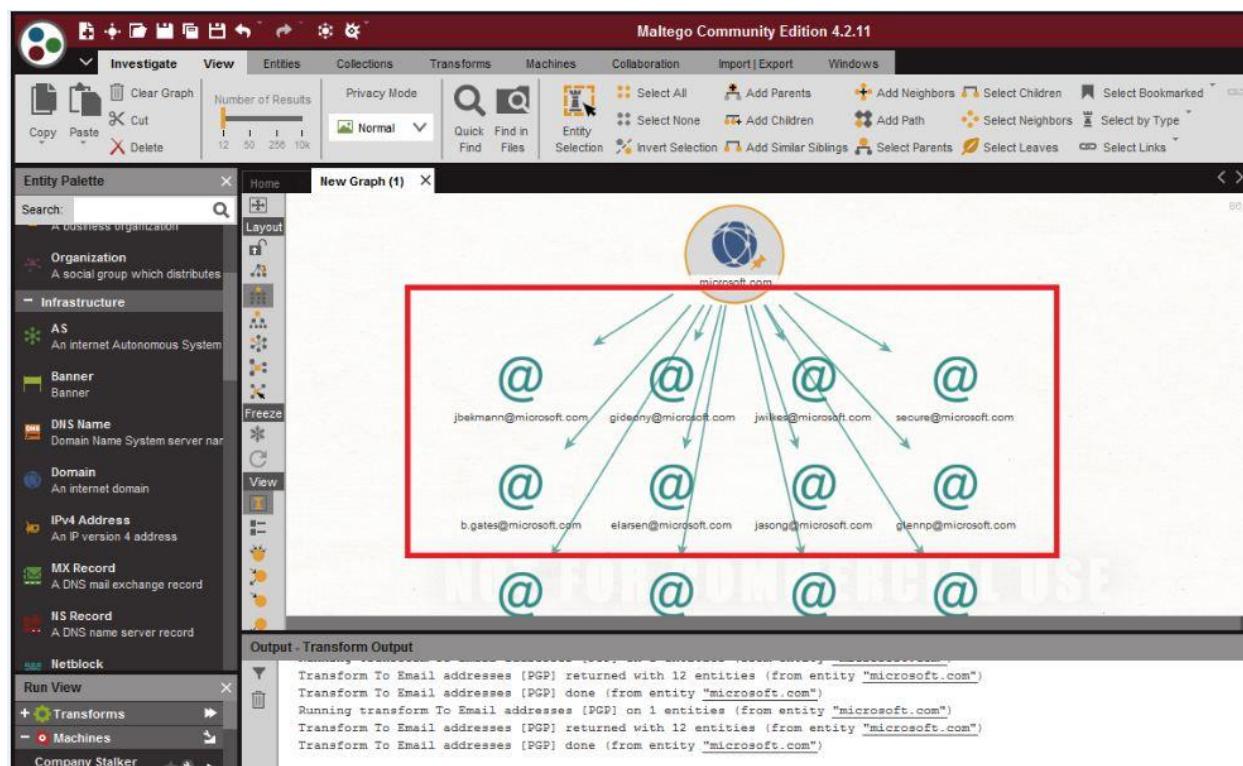
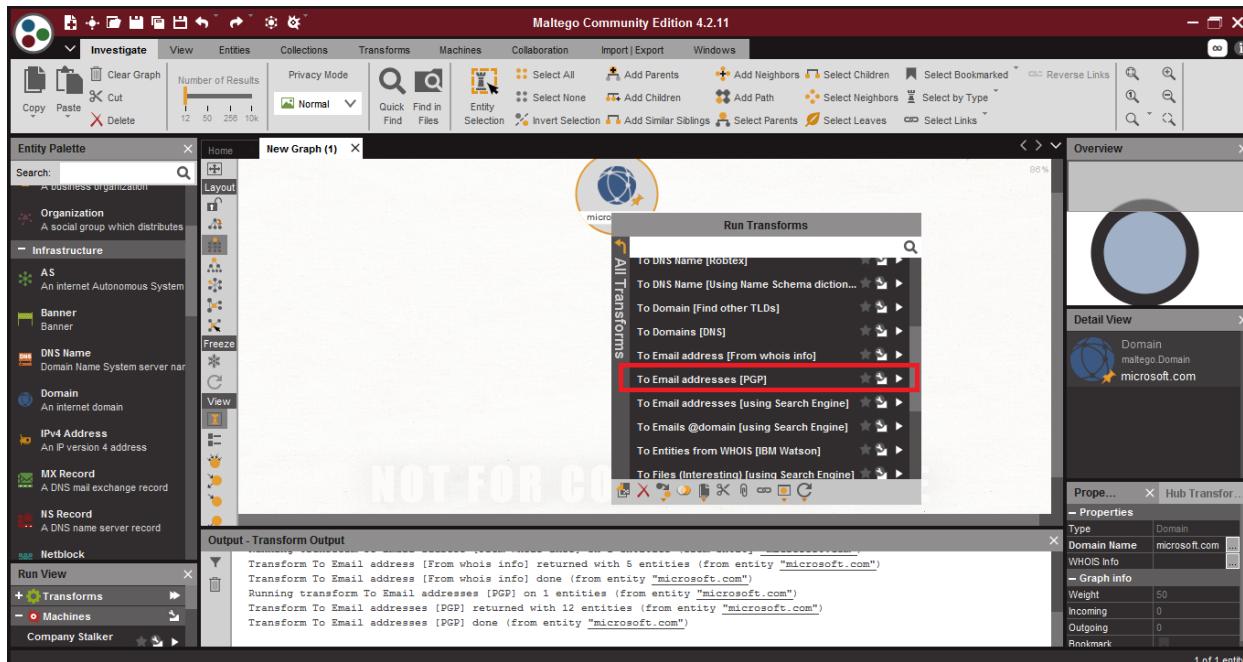
Step 7: Click on Domains in Left panel to gather information.



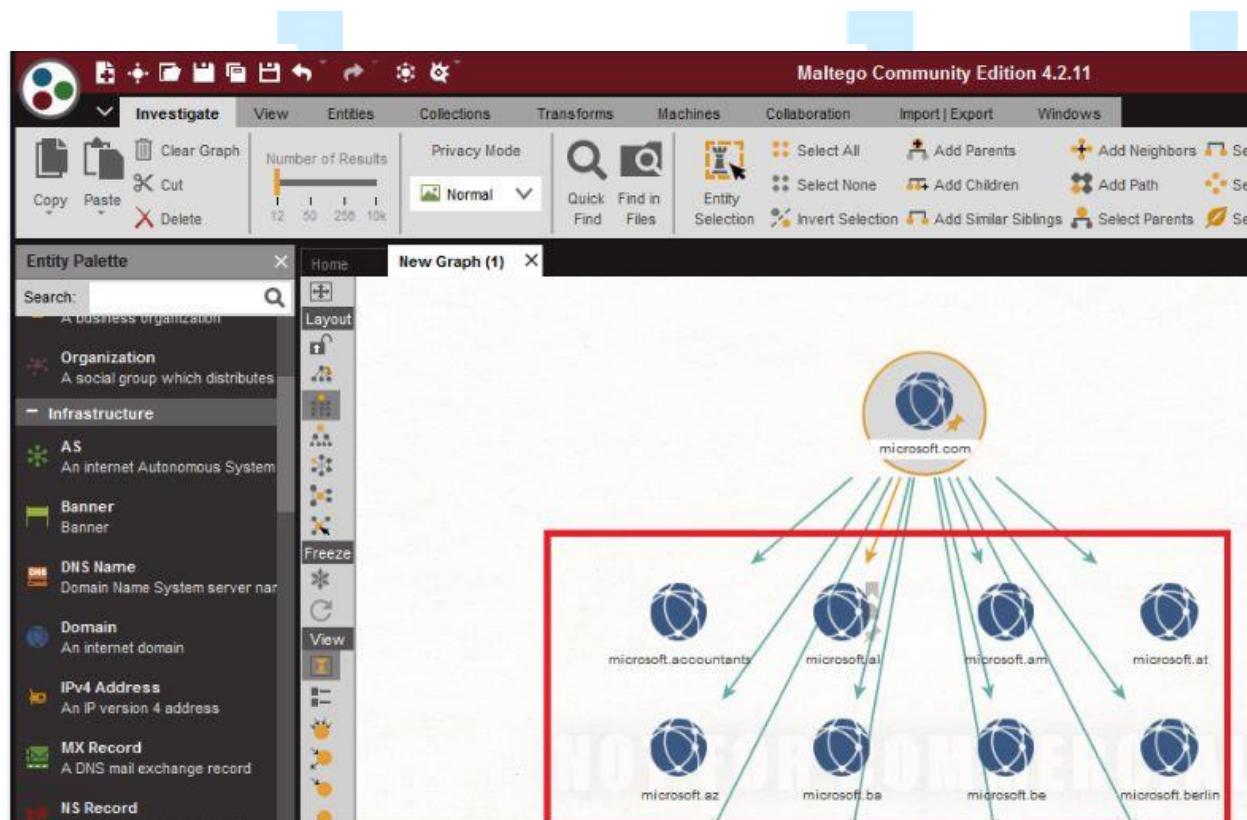
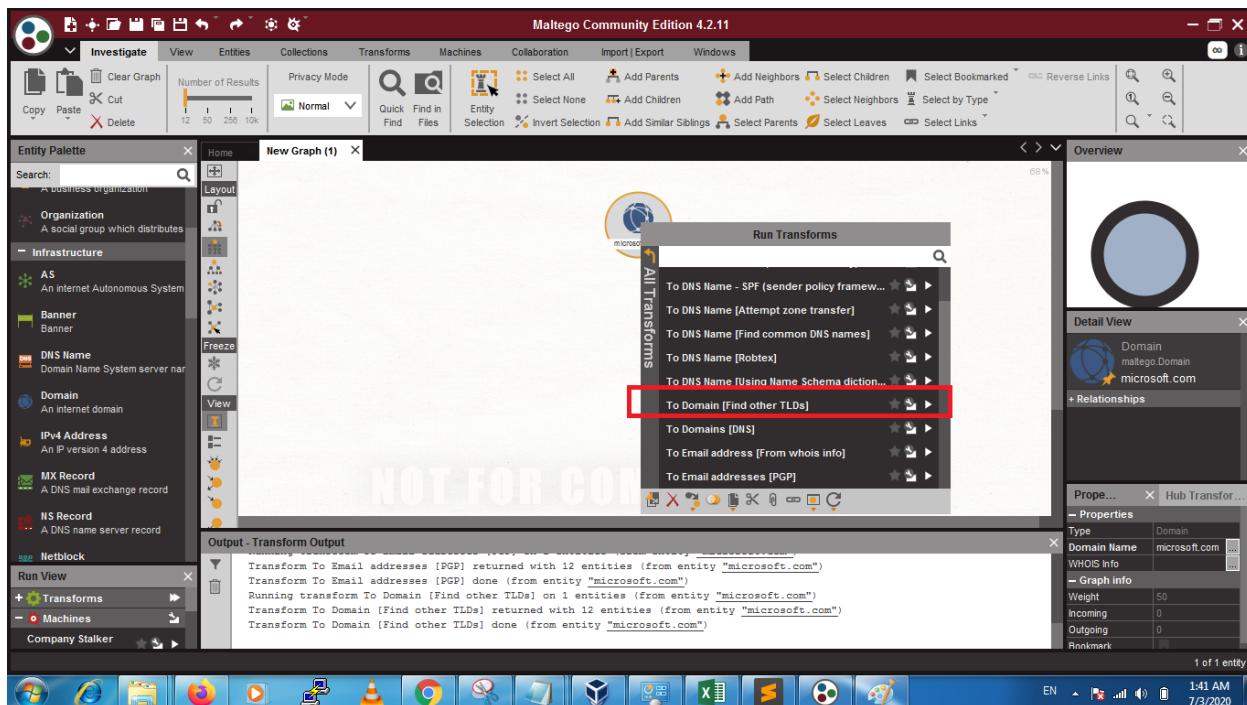
Step 8: Write the domain name (**Microsoft.com**) without www protocol.



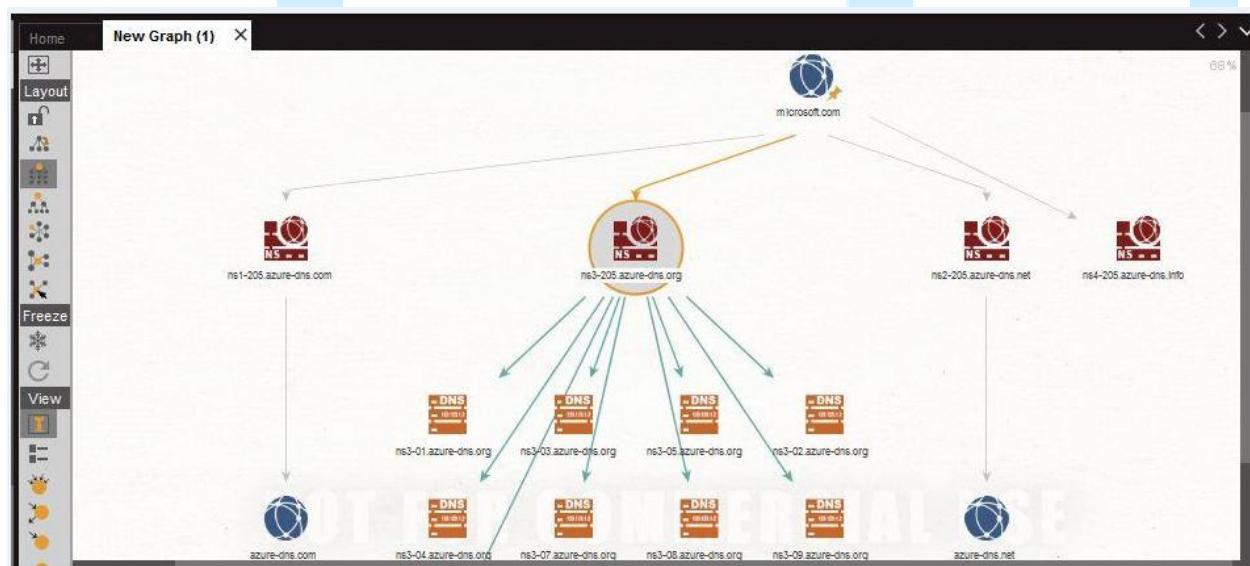
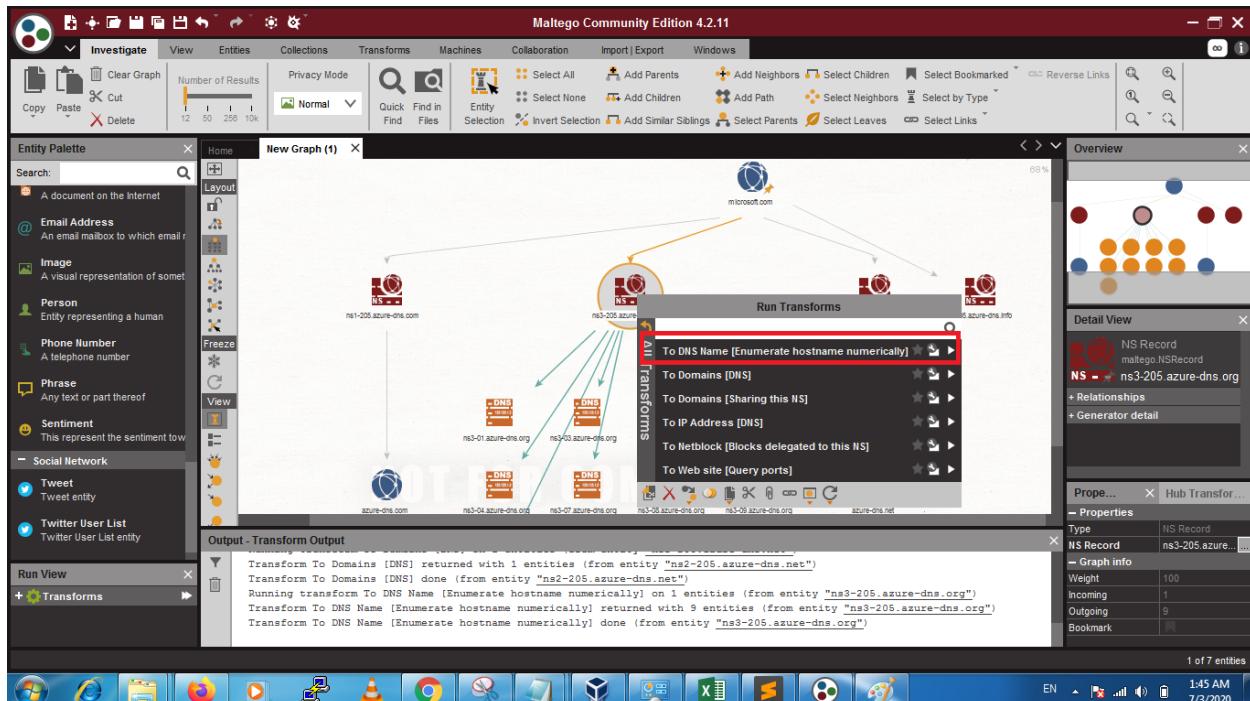
Step 9: Right-click and select the To email addresses (to gather emails related to the domain).



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
```

```
[+] Searching now in Ask..
[+] Searching now in Netcraft..
[+] Searching now in DNSdumpster..
[+] Searching now in Virustotal..
[+] Searching now in ThreatCrowd..
[+] Searching now in SSL Certificates..
[+] Searching now in PassiveDNS..
[+] Total Unique Subdomains Found: 15
www.www.bing.com
0.www.bing.com
10334.www.bing.com
264770464.6461796c6967687477696e64796a616e6540686f746d616message.www.bing.com
a17-250-248-150.www.bing.com
appledirectory.www.bing.com
phcs-intranet.corp.www.bing.com
de.www.bing.com
euro.www.bing.com
https.www.bing.com

img.www.bing.com
inktest.www.bing.com
intranet.www.bing.com
lax。www.bing.com
mc.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
```

```
[+] Searching now in DNSdumpster..  
[+] Searching now in Virustotal..  
[+] Searching now in ThreatCrowd..  
[+] Searching now in SSL Certificates..  
[+] Searching now in PassiveDNS..  
[+] Total Unique Subdomains Found: 15  
[+] Start port scan now for the following ports: 443  
0.www.bing.com - Found open ports: 443  
264770464.6461796c69676874776f6e64796a616e6540686f746d616message.www.bing.com -  
Found open ports: 443  
10334.www.bing.com - Found open ports: 443  
www.www.bing.com - Found open ports: 443  
a17-250-248-150.www.bing.com - Found open ports: 443  
appledirectory.www.bing.com - Found open ports: 443  
de.www.bing.com - Found open ports: 443  
phcs-intranet.corp.www.bing.com - Found open ports: 443  
euro.www.bing.com - Found open ports: 443  
inktest.www.bing.com - Found open ports: 443  
https.www.bing.com - Found open ports: 443  
img.www.bing.com - Found open ports: 443  
intranet.www.bing.com - Found open ports: 443  
lax.www.bing.com - Found open ports: 443  
mc.www.bing.com - Found open ports: 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 (74.125.243.193)  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

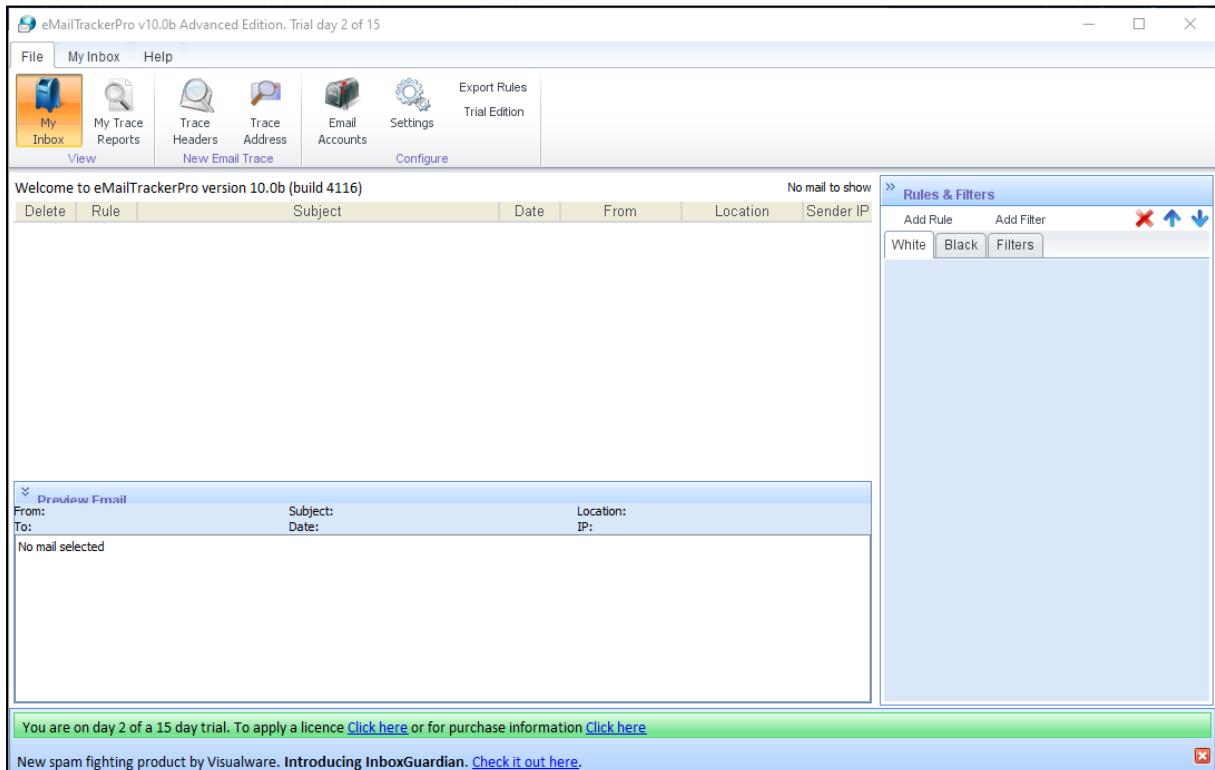
Problem Statement:

Tracking Email using Email Header

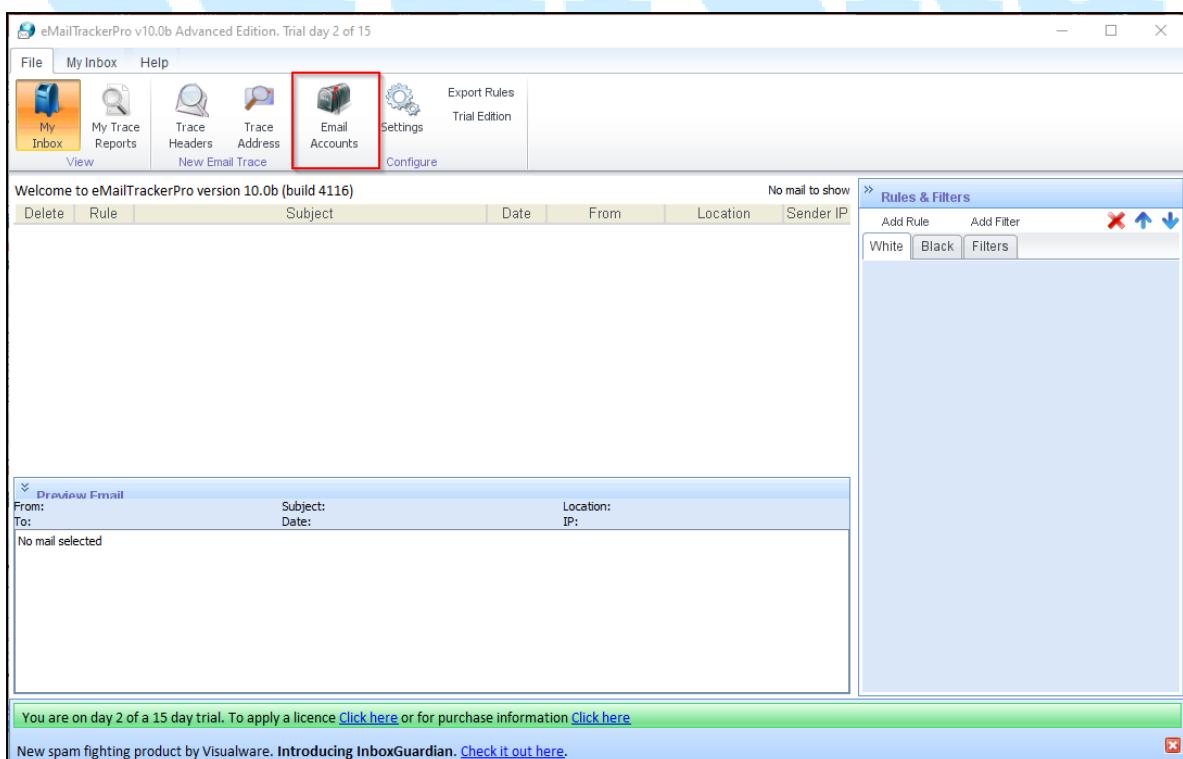
Tool Used: eMail Tracker Pro

Solution:

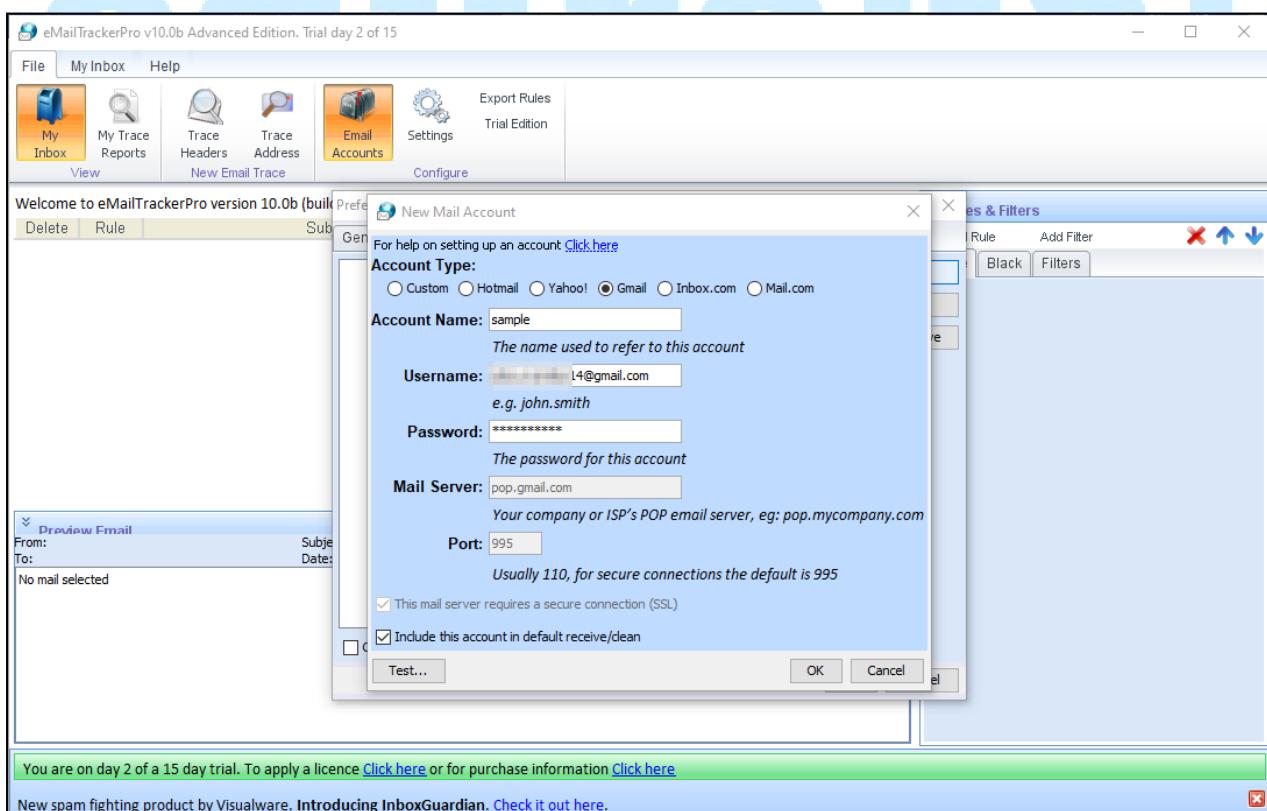
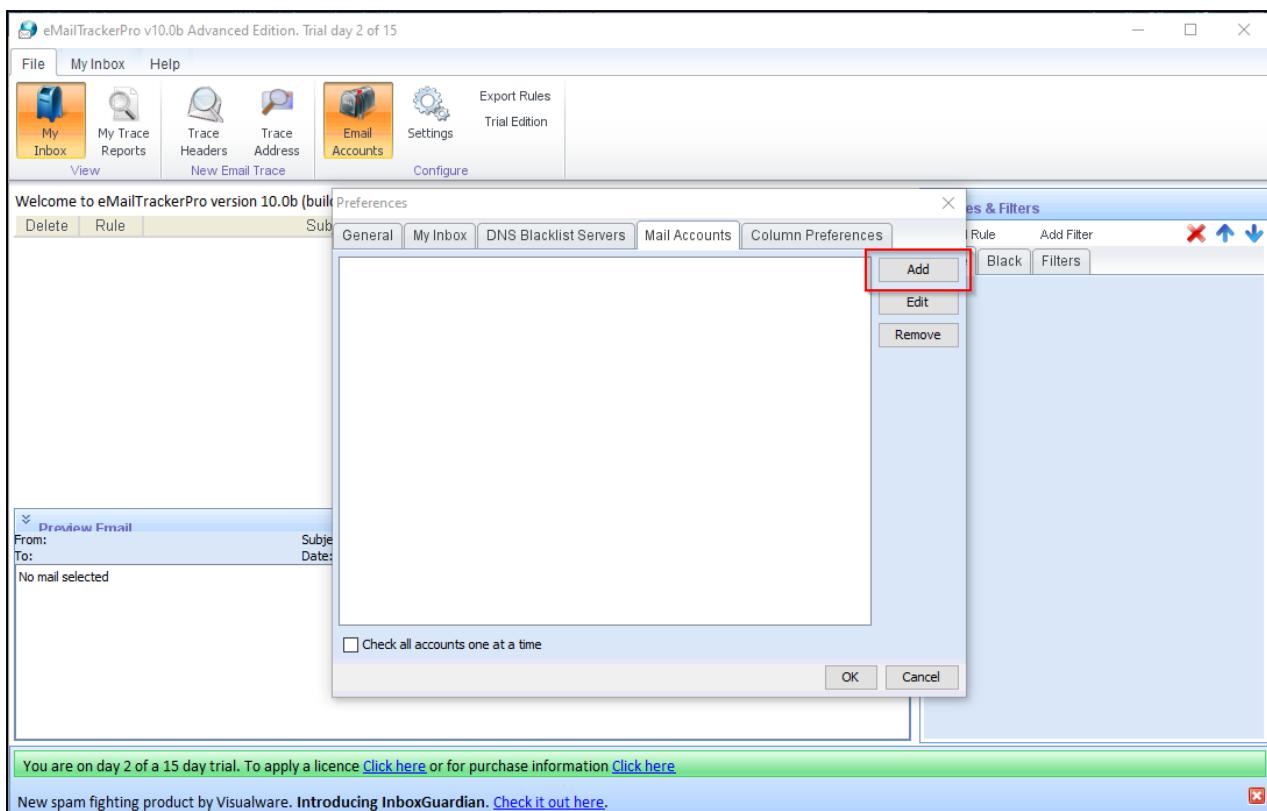
Step 1: Download and install eMail Tracker Pro from <http://www.emailtrackerpro.com/>



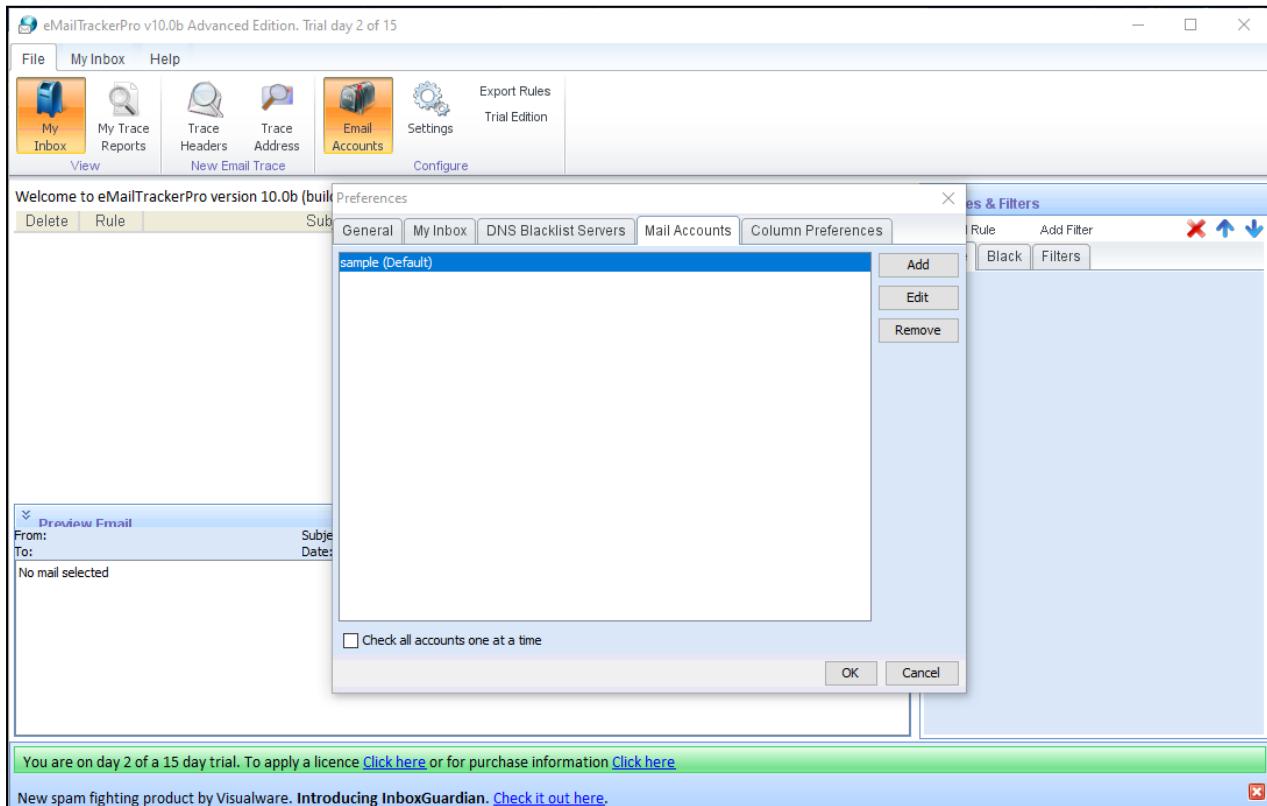
Step 2: After installing go to File>Email Accounts



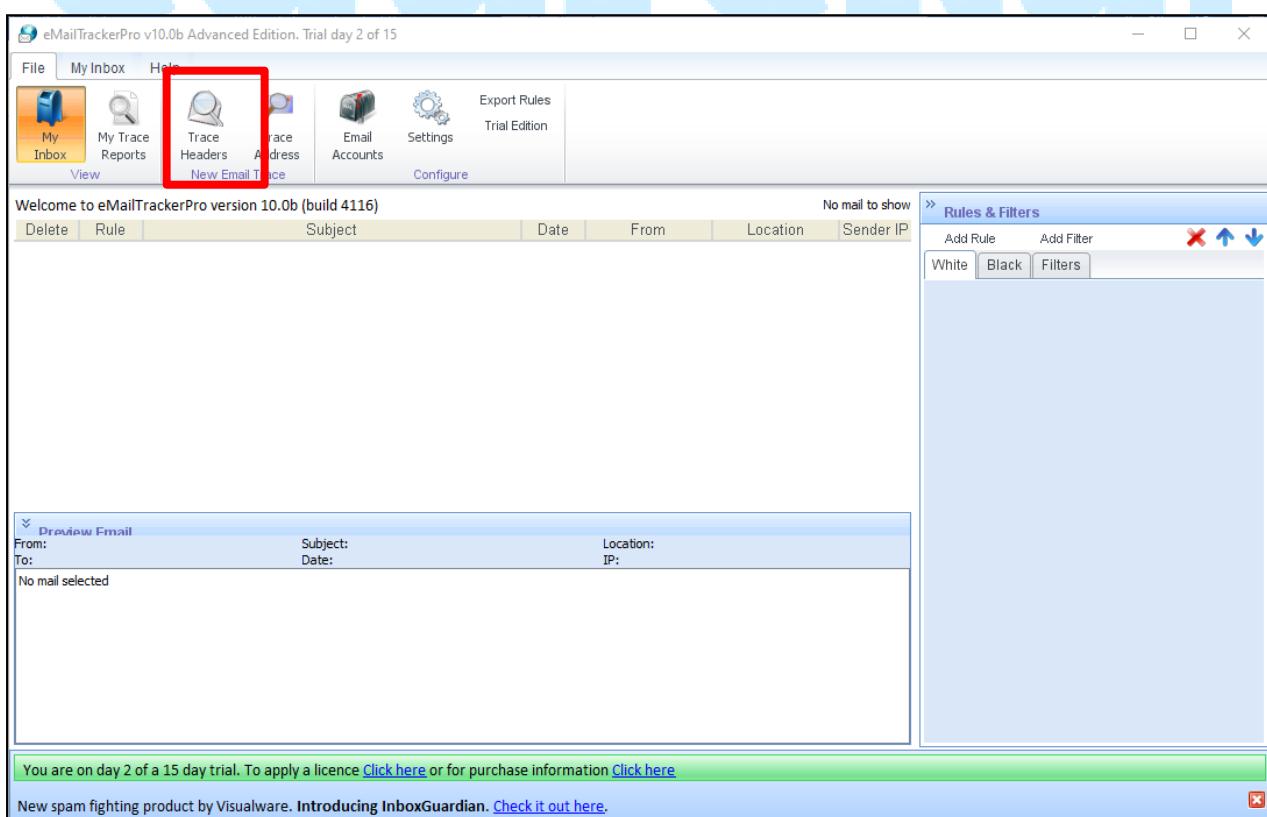
Step 3: Click on add to add an account



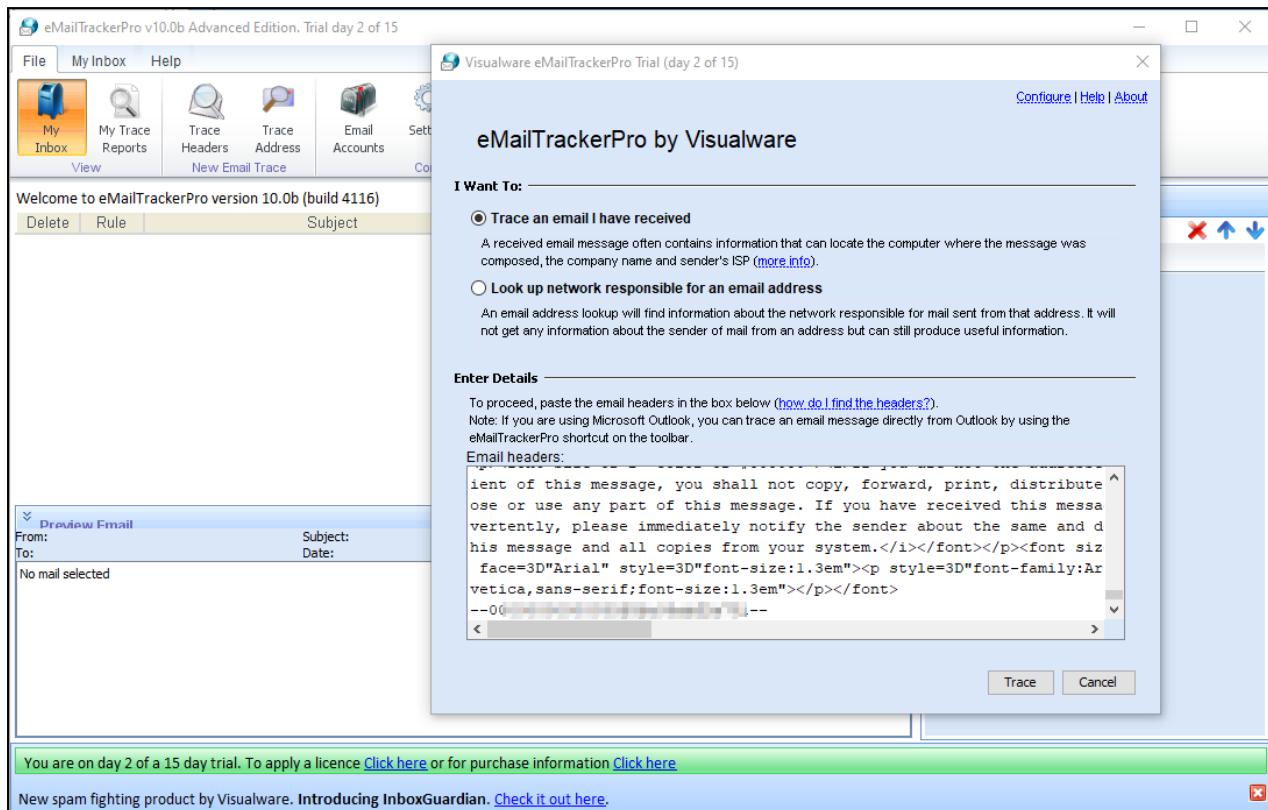
Step 4: After adding the account successfully, it will appear as a list under Mail Accounts Tab. Select it and click ok



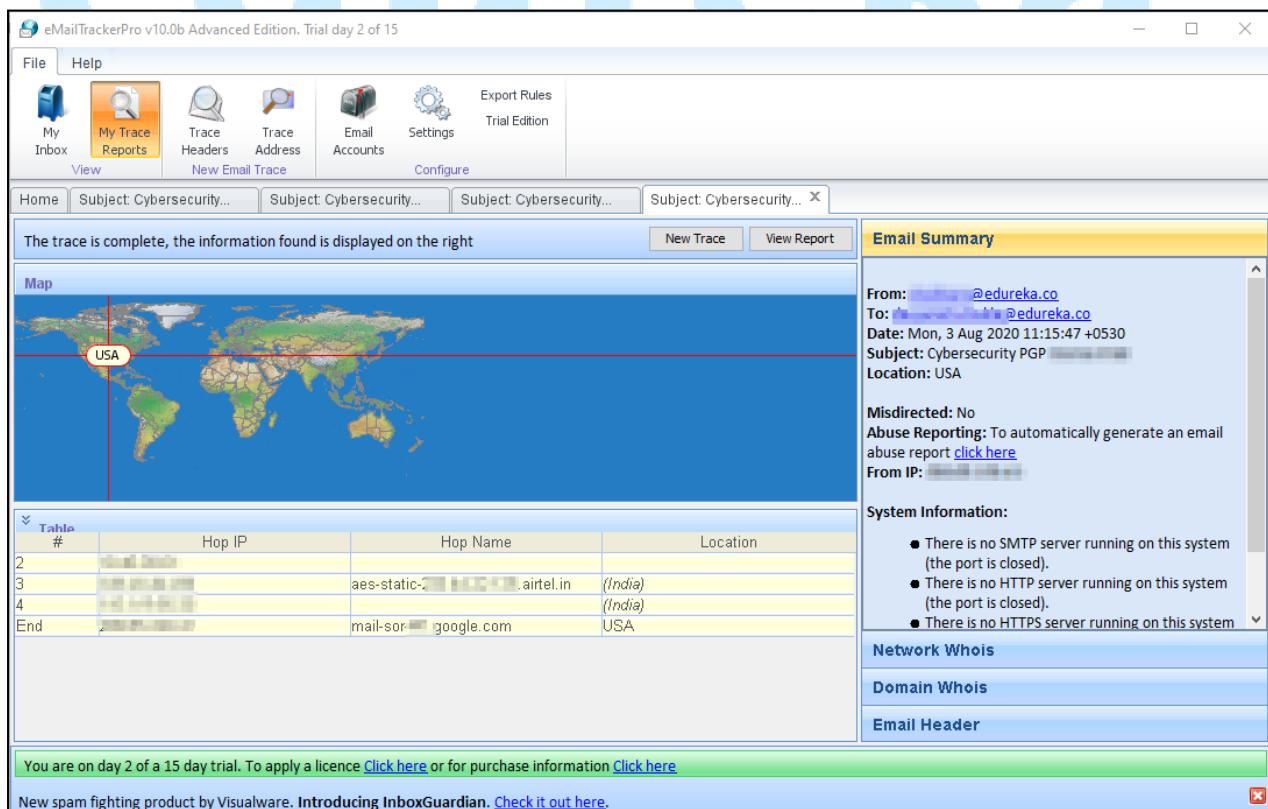
Step 5: Select Trace Headers under File Tab



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

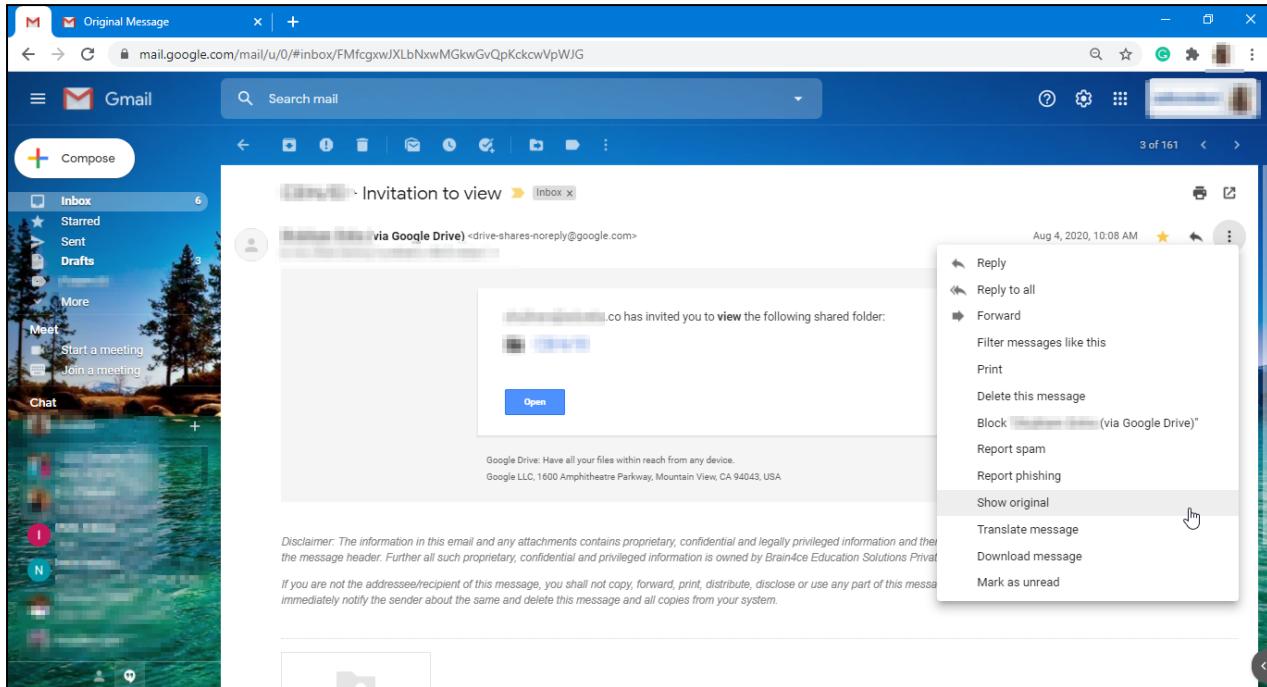


Step 7: The results are now displayed and you can trace them from the Email Summary



(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.

Original Message

Message ID	<0...@google.com>
Created at:	Tue, Aug 4, 2020 at 10:08 AM (Delivered after 1 second)
From:	"S... (via Google Drive)" <drive-shares-noreply@google.com>
To:	a...@edureka.co
Subject:	C... Invitation to view
SPF:	PAS... Learn more
DKIM:	'PASS' with domain google.com Learn more
DMARC:	'PASS' Learn more

[Download Original](#) [Copy to clipboard](#)

Module 1 – Introduction to Cybersecurity & Ethical Hacking

```
Delivered-To: [REDACTED]
Received: by 2002:a5d:538d:0:0:0:0:0 with SMTP id d13csp104482wrw;
Mon, 3 Aug 2020 21:38:05 -0700 (PDT)
X-Received: by 2002:a5d:538d:0:0:0:0:0 with SMTP id 15885662;
Mon, 03 Aug 2020 21:38:05 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=15885662; cv=none;
d=google.com; s=arc-20200803;
b=FqsAm^nh^GQo-PVfENo+2F9OT /w+PTMULPwmpY/V>-R9h74FTWUobwNKPGEKbp
pC2V[REDACTED]iJtLgN7txy7
b+BM[REDACTED]7AvC3SvwluvH
ucuDPn9XLSe/R1TmPT/YISpg4rZCTPv1JTU1Rz5j/smPQJjKVv5zenT3MCCiKwoOd
9uy4q1RjE9bc5qOXPQvM2WiCVCrCLaeTQgqoo9govfhRCGEsj/CSRr2LiC9t5NaIXNN
gkww=
ARC-Message-Signature: [REDACTED].axed/relaxed; d=google.com; s=arc-20200803;
h=cc:to:from:subject:date:message-id:references:reply-to:mime-version
:dkim-signature;
bh=d[REDACTED]; b[REDACTED]; g[REDACTED];
b=r1KYZGfpclK9uuqRewxrj4Zm7lu/LvElnyuqgAUuN1HvPQfmHFU+H32piE2LJ9SSF
JzxB0BAt[REDACTED]qgg3BDkaNwaDXD8s
9bwirNb[REDACTED]i5J6qA0askRTjf7bg1
XXkLDLtocw0F1/o7ymCCyWCSTgcwC9RQ186dByseuPmQh01Pmen/OsLmhniBYFXYRS
3z/z4S6nml4hHDmnoE3RJ1vbahw3p2G34/5ICRHpa96/+Jqy8P1H2rKUI0HP3qlwbkRR
IIIA==

ARC-Authentication-Results: i=1; mx.google.com;
dki=[REDACTED] header.i=@google.com header.s=20161025 header.b=EibugYj5;
spf=pass (google.com: domain of 3loyoxxxqkajs8mdq9-nc5m9n-ijm9kgtbjjbg9.7jh@doclist.bounces.google.com
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: <3LOYoXxQKAjs8MDQ9-NC5M9N-IJm9KGtbjjbg9.7jh@doclist.bounces.google.com>
Received: from mail-sor-10g[REDACTED] ([REDACTED]) by mx.google.com with SMTP id v127[REDACTED] Mon, 03 Aug 2020 21:38:05 -0700 (PDT)
for <[REDACTED]@edureka.co>
(Google Transport Security);
Mon, 03 Aug 2020 21:38:05 -0700 (PDT)
Received-SPF: pass (google.com: domain of 3loyoxxxqkajs8mdq9-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 3loyoxxxqkajs8mdq9-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]
7EEtSa2o9QhNVPeMQZaCur0iMR626Gk0tFYdKxyR[REDACTED]g=
X-Google-Smtp-Source: [REDACTED]FoYdgUtYZHCm95nvpw=
MIME-Version: 1.0
X-Received: by 2002:a5d:538d:0:0:0:0:0 with SMTP id d13csp104482wrw;
Mon, 03 Aug 2020 21:38:04 -0700 (PDT)
Reply-To: [REDACTED]a <[REDACTED]@edureka.co>
X-No-Auto-Attachment: 1
References: <aa[REDACTED]docs-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: [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
```