LAB 5 - Information Gathering (Recon)

Objectives

In this practical you will perform foot printing activities to collect information about your target.

Duration: 60+min

Requirements

- Lab PC
- Kali Linux (installed)

Tasks

- Task 1: WHOIS
- Task 2: DNS Foot Printing
- Task 3: Maltego (Independent)
- Task 4: SpiderFoot (Independent)

Foot Printing

Student Notes

Foot printing is the process of gathering as much information as possible about a target system (including organizational, contact, and network data).

Common Foot Printing Techniques

- WHOIS
- Internet Search
- DNS
- Social Engineering
- Dumpster Driving
- Website Copy

Active vs. Passive Foot Printing:

Active Foot Printing is an intrusive approach whereby the tester/attacker may leave tracks/evidence of their search.

Passive, on the other hand, is a nonintrusive process that involves public searches and that usually doesn't leave unwanted traces.

Task 1: WHOIS

Task Objectives

- You will use different tools to perform a WHOIS lookup on selected organizations

ICANN & NETCRAFT

ICANN:
ICANN is the Internet Corporation for Assigned Names and Numbers. It is an internationally organized non-profit corporation that, among other things, oversees IP address space allocation and top-level domain (TLD) management.

1. Visit **https://www.iana.org/whois** and type **.ae** in the search field

.ae

Which organization manages the .ae top-level domain (TLD)?	1. Telecommunications and Digital Government Regulatory Authority (TDRA) 2. .ae Domain Administration (.aeDA)
What is the WHOIS directory for this TLD?	provides registration details for domain names for example .com, .org

2. Visit **http://whois.aeda.net.ae** and perform a WHOIS lookup for **HCT**

What is the registrar's name?	hct.gov.ae → Etisalat hct.ac.ae →Etisalat
What is the name server? Name one only	ns1.etisalatdomains.ae

3. Visit **http://whois.icann.org** and perform a WHOIS lookup for **HCT**

Did you get any results back?	No i didnt got any answer
Why or why not?	**because the value entered was not valid**

4. Visit **http://whois.icann.org** and perform a WHOIS lookup for **YouTube** and *Twitter*

5. Fill in the required information in the table below

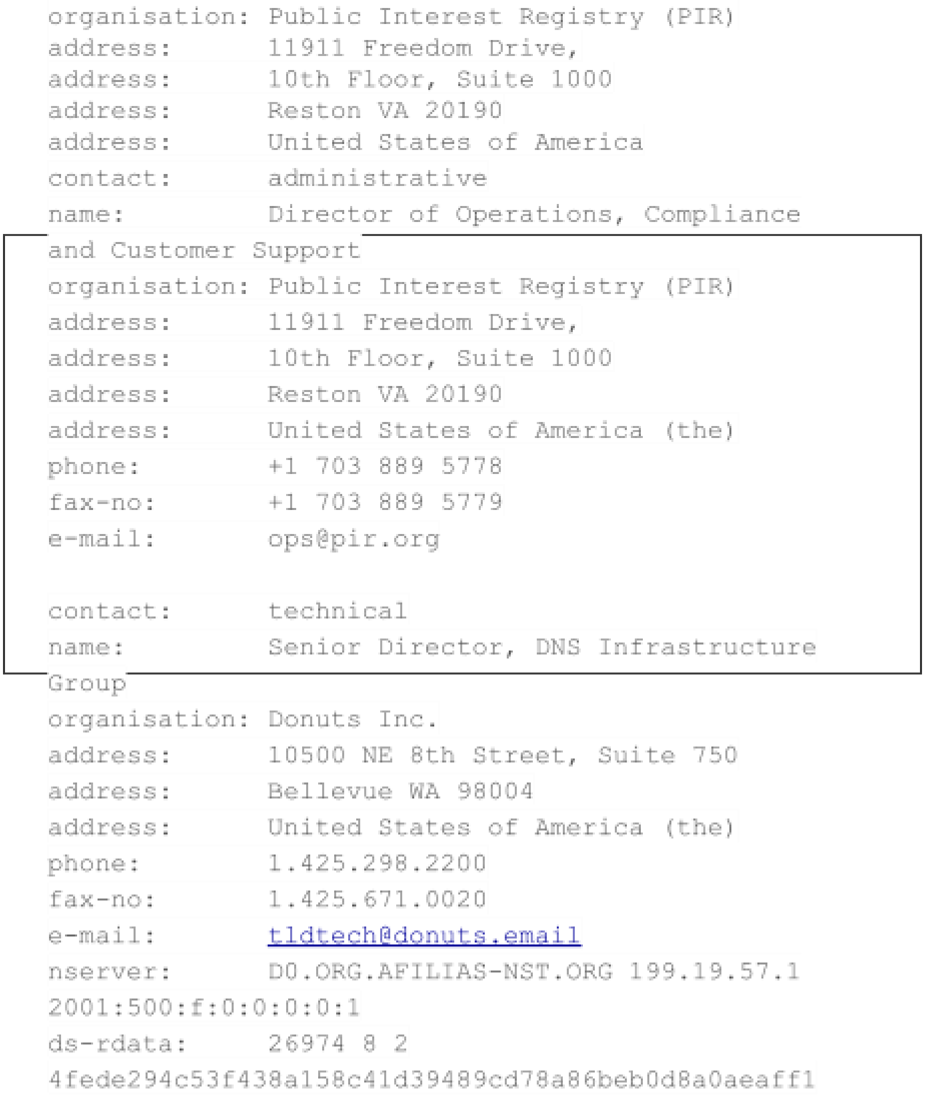
	Youtube.com	**Twitter.com**
Registrant Name	Charleston Road Registry Inc.	Twitter, Inc.
Organization	Charleston Road Registry Inc.	Twitter, Inc.
Phone	+1 404 978 8419	+1.4152229670
Email	iana-contact@google.com	domains@twitter.com
Registrar WHOIS Server	Registration information: https://www.registry.google	Registration information: http://www.verisigninc.com
Registration Expiration Date	2020-04-20	2023-12-07
Name Servers	NS-TLD5.CHARLESTONROADREGISTRY.COM 2001:4860:4805:0:0:0:0:69 216.239.60.105	A.GTLD-SERVERS.NET 192.5.6.30 2001:503:a83e:0:0:0:2:30

6. Visit **http://www.netcraft.com (site report or site dns)**and lookup WHOIS information about **YouTube**
and **Twitter.** Fill in the required information in the table below

	Youtube.com	**Twitter.com**
Hosting Company	Google	Twitter
IP Address	209.85.203.136	104.244.42.129
OS (For IP address)		
Web Server	Google	**TwitterServer**

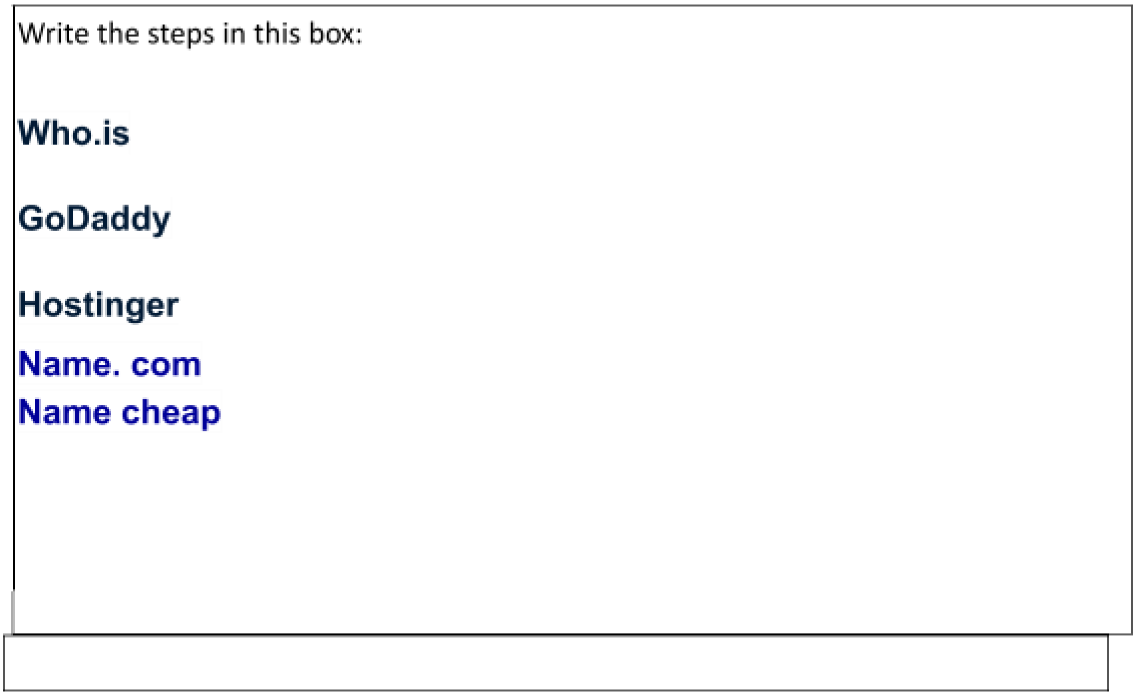
7. Independent Task:

Starting from IANA, find out the WHOIS database and then the domain information for **hackthissite.org**



```
organisation: Public Interest Registry (PIR)
address:      11911 Freedom Drive,
address:      10th Floor, Suite 1000
address:      Reston VA 20190
address:      United States of America
contact:      administrative
name:         Director of Operations, Compliance
and Customer Support
organisation: Public Interest Registry (PIR)
address:      11911 Freedom Drive,
address:      10th Floor, Suite 1000
address:      Reston VA 20190
address:      United States of America (the)
phone:        +1 703 889 5778
fax-no:       +1 703 889 5779
e-mail:       ops@pir.org

contact:      technical
name:         Senior Director, DNS Infrastructure
Group
organisation: Donuts Inc.
address:      10500 NE 8th Street, Suite 750
address:      Bellevue WA 98004
address:      United States of America (the)
phone:        1.425.298.2200
fax-no:       1.425.671.0020
e-mail:       tldtech@donuts.email
nserver:      D0.ORG.AFILIAS-NST.ORG 199.19.57.1
2001:500:f:0:0:0:0:1
ds-rdata:     26974 8 2
4fede294c53f438a158c41d39489cd78a86beb0d8a0aeaff1
```

7. **Independent Task:**
Find 5 additional internet tools and/or sites that provide WHOIS services



Write the steps in this box:

Who.is

GoDaddy

Hostinger

Name. com

Name cheap

Task 2: DNS Foot Printing

Task Objectives

- ▯ You will use tools to perform DNS foot printing on selected targets.

DNS Foot Printing

DNS Lookup Tools:

- DIG
- HOST
- NSLOOKUP

Common DNS Records: ▪

A –IP Address

- NS –Name Server
- MX –Mail Server

- TXT –Generic text record
- RP –Responsible Person
- SOA –Start of Authority
- AXFR –Zone Transfer

1. Power on Kali and open a terminal window
2. Ping **hackthissite.org**

   Note: Ping may be blocked

What is the IP address of the target?	hackthissite.org (137.74.187.102)
Why Ping is NOT enough to get the IP address of a domain?	**ICMP Echo Requests May Be Blocked,Ping Does Not Show All DNS Records,DNS Query Results Depend on Resolver Location**

3. Run the following command: **host hackthissite.org**

What is the IP address of the target? **137.74.187.100**	

Why do you have multiple IP addresses?	because they are handled by different gmail accounts and other names handled by other people
What other information did the HOST command provide?	**we got 4 IPv4 , IPv6 addresses and also the gmails of the site**

How would you find out more about the HOST command and how to use it?	● Find Host Machine IP Address. To find the IP address and related details of the host machine ● Find Host Name Based on IP Address ● Show Addresses for Internet Domain ● Discover DNS Details ● Find Mail Exchange Info ● Look Specific Record Types
What is HOST?	In field of NS host means a command used to gather information about any domain
What options are available for the HOST command?	HostName: Returns the IP address of a host machine Address: Returns the name of the host
What is the –t option?	for type representation
What is the –l (lower case L) option?	-l lists all hosts in a domain, using AXFR

What happens when no type is provided?	**host -t** **host: option requires an argument -- t** **it gives this error and tells what can it help**

Run HOST with the –t a option. What is the command and what is the output?	**host -t a google.com** **google.com has address 172.217.19.206**
Run HOST with the –t mx option. What is the command and what is the output?	**.host -t mx google.com** **google.com mail is handled by 10 smtp.google.com.**
Run HOST with the –t soa option. What is the command and what is the output?	**host -t soa google.com** **google.com has SOA record ns1.google.com.** **dns-admin.google.com. 698728253 900 900 1800 60**
Run HOST with the –t ns option. What is the command and what is the output?	**host -t ns google.com** **google.com name server ns2.google.com.** **google.com name server ns4.google.com.** **google.com name server ns3.google.com.** **google.com name server ns1.google.com.**
Run HOST with the –t rp option. What is the command and what is the output?	**host -t rp google.com** **google.com has no RP record**
Run HOST with the –t txt option. What is the command and what is the output?	**host -t txt google.com** **google.com descriptive text** **"docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"** **google.com descriptive text** **"docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"** **google.com descriptive text** **"MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB"** **google.com descriptive text** **"facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h9**

	5" **google.com descriptive text "onetrust-domain-verification=de01ed21f2fa4d8781cbc3ffb89cf4ef"** **google.com descriptive text "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="** **google.com descriptive text "google-site-verification=4ibFUgB-wXLQ_S7vsXVomSTVamuOXBiVAzpR5IZ87D0"** **google.com descriptive text "google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o"** **google.com descriptive text "apple-domain-verification=30afIBcvSuDV2PLX"** **google.com descriptive text "v=spf1 include:_spf.google.com ~all"** **google.com descriptive text "google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ"** **google.com descriptive text "cisco-ci-domain-verification=479146de172eb01ddee38b1a455ab9e8bb51542ddd7f1fa298557dfa7b22d963"**

4. Another DNS lookup utility is DIG: **dig twitter.com**

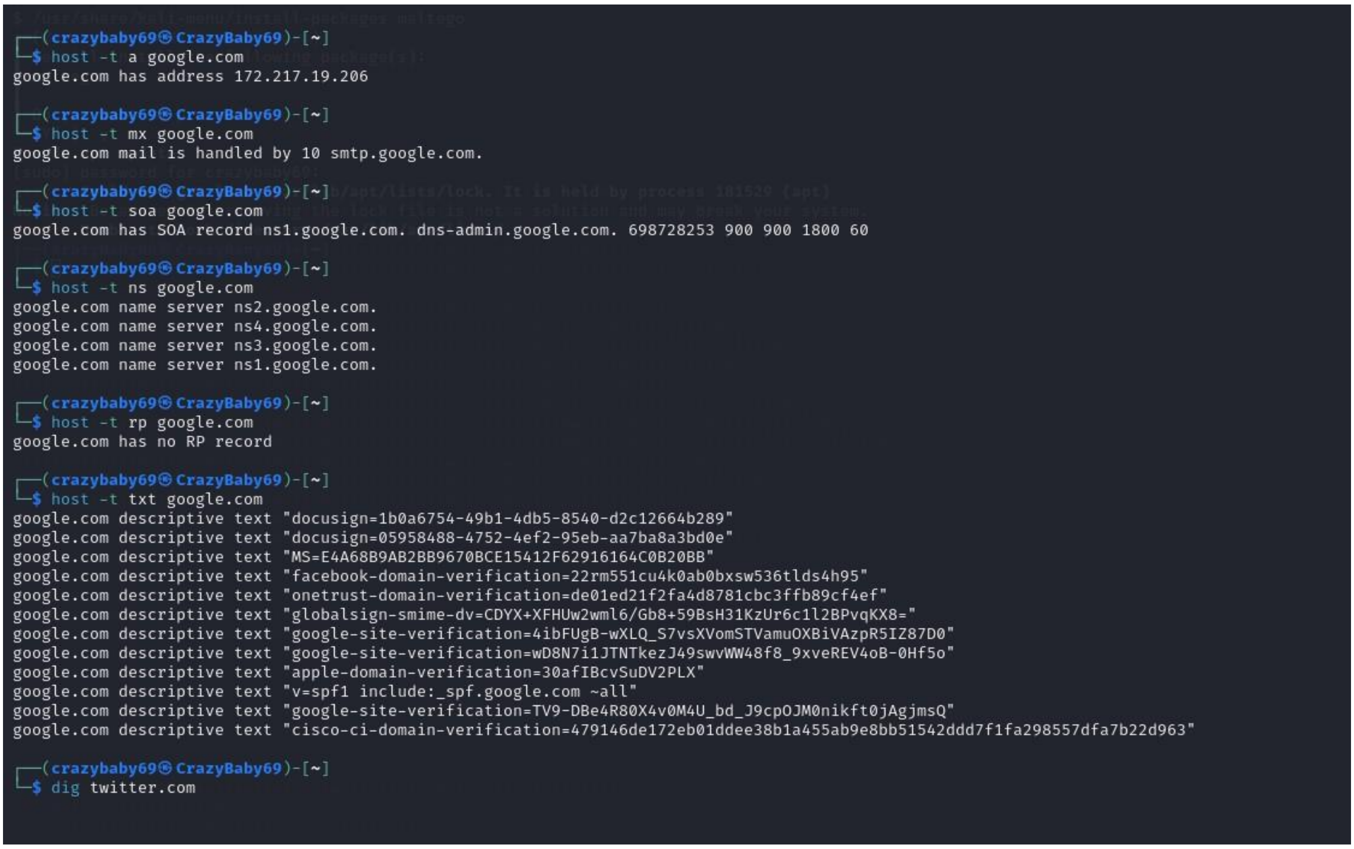
Using DIG, perform the following DNS queries for the target twitter.com

IP Address **Query type** **=**	**Command:** dig twitter.com A
Name Servers **Query type =**	**Command:** dig twitter.com NS
Start of Authority Query type =	**Command:** dig twitter.com SOA
Responsible Person Query type =	**Command:** dig twitter.com RP
Text **Query type =**	**Command:** dig twitter.com TXT
Mail Exchange **Query type =**	**Command:** dig twitter.com MX

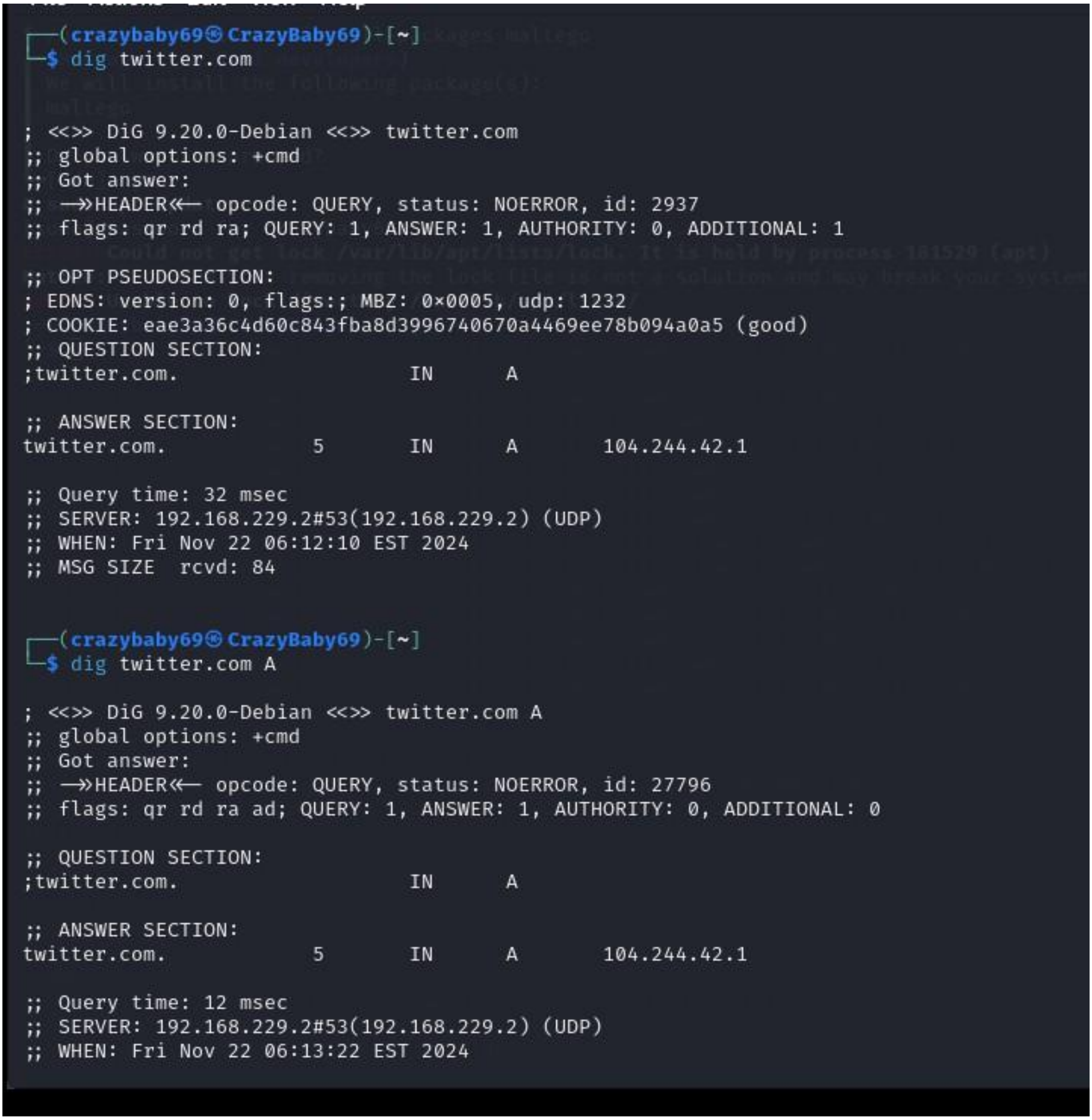
5. A third DNS lookup utility is NSLOOKUP: **nslookup instagram.com**

IP Address **Query type** **=**	**Command:** ns lookup instagram.com
Name Servers **Query type =**	**Command:** nslookup -type=NS instagram.com
Start of Authority Query type =	**Command:** nslookup -type=SOA instagram.com

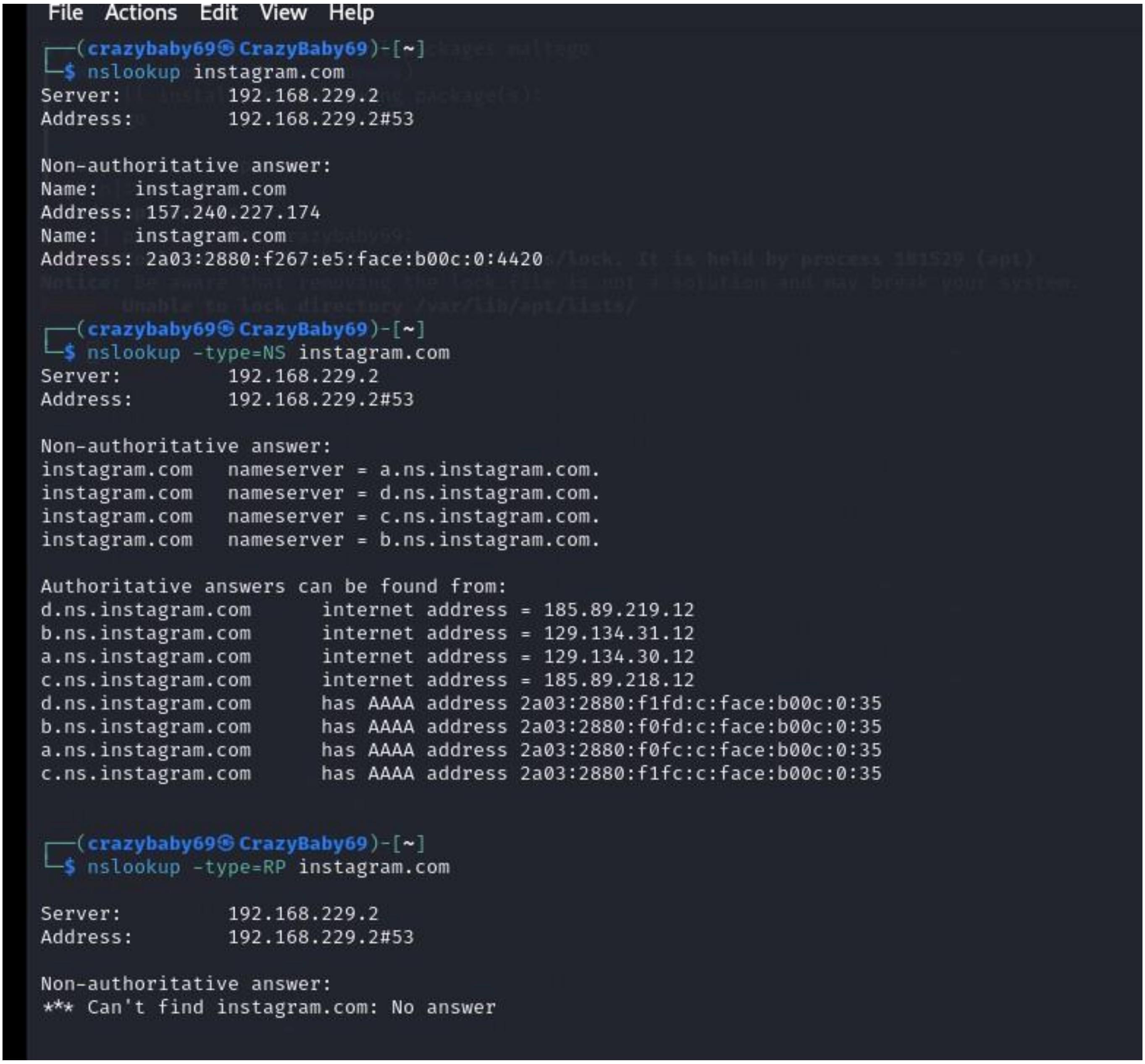
Responsible Person **Query type =**	**Command:** nslookup -type=rp instagram.com
Text **Query type =**	**Command:** nslookup -type=txt instagram.com
Mail Exchange **Query type =**	**Command:** nslookup -type=MX instagram.com



```
┌──(crazybaby69㉿CrazyBaby69)-[~]
└─$ host -t a google.com
google.com has address 172.217.19.206

┌──(crazybaby69㉿CrazyBaby69)-[~]
└─$ host -t mx google.com
google.com mail is handled by 10 smtp.google.com.

┌──(crazybaby69㉿CrazyBaby69)-[~]
└─$ host -t soa google.com
google.com has SOA record ns1.google.com. dns-admin.google.com. 698728253 900 900 1800 60

┌──(crazybaby69㉿CrazyBaby69)-[~]
└─$ host -t ns google.com
google.com name server ns2.google.com.
google.com name server ns4.google.com.
google.com name server ns3.google.com.
google.com name server ns1.google.com.

┌──(crazybaby69㉿CrazyBaby69)-[~]
└─$ host -t rp google.com
google.com has no RP record

┌──(crazybaby69㉿CrazyBaby69)-[~]
└─$ host -t txt google.com
google.com descriptive text "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com descriptive text "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com descriptive text "MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB"
google.com descriptive text "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"
google.com descriptive text "onetrust-domain-verification=de01ed21f2fa4d8781cbc3ffb89cf4ef"
google.com descriptive text "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="
google.com descriptive text "google-site-verification=4ibFUgB-wXLQ_S7vsXVomSTVamuOXBiVAzpR5IZ87D0"
google.com descriptive text "google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o"
google.com descriptive text "apple-domain-verification=30afIBcvSuDV2PLX"
google.com descriptive text "v=spf1 include:_spf.google.com ~all"
google.com descriptive text "google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ"
google.com descriptive text "cisco-ci-domain-verification=479146de172eb01ddee38b1a455ab9e8bb51542ddd7f1fa298557dfa7b22d963"

┌──(crazybaby69㉿CrazyBaby69)-[~]
└─$ dig twitter.com
```



```
┌──(crazybaby69㉿CrazyBaby69)-[~]
└─$ dig twitter.com

; <<>> DiG 9.20.0-Debian <<>> twitter.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2937
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 1232
; COOKIE: eae3a36c4d60c843fba8d3996740670a4469ee78b094a0a5 (good)
;; QUESTION SECTION:
;twitter.com.                   IN      A

;; ANSWER SECTION:
twitter.com.            5       IN      A       104.244.42.1

;; Query time: 32 msec
;; SERVER: 192.168.229.2#53(192.168.229.2) (UDP)
;; WHEN: Fri Nov 22 06:12:10 EST 2024
;; MSG SIZE  rcvd: 84


┌──(crazybaby69㉿CrazyBaby69)-[~]
└─$ dig twitter.com A

; <<>> DiG 9.20.0-Debian <<>> twitter.com A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27796
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;twitter.com.                   IN      A

;; ANSWER SECTION:
twitter.com.            5       IN      A       104.244.42.1

;; Query time: 12 msec
;; SERVER: 192.168.229.2#53(192.168.229.2) (UDP)
;; WHEN: Fri Nov 22 06:13:22 EST 2024
```



```
┌──(crazybaby69㉿CrazyBaby69)-[~]
└─$ nslookup instagram.com
Server:         192.168.229.2
Address:        192.168.229.2#53

Non-authoritative answer:
Name:   instagram.com
Address: 157.240.227.174
Name:   instagram.com
Address: 2a03:2880:f267:e5:face:b00c:0:4420

┌──(crazybaby69㉿CrazyBaby69)-[~]
└─$ nslookup -type=NS instagram.com
Server:         192.168.229.2
Address:        192.168.229.2#53

Non-authoritative answer:
instagram.com   nameserver = a.ns.instagram.com.
instagram.com   nameserver = d.ns.instagram.com.
instagram.com   nameserver = c.ns.instagram.com.
instagram.com   nameserver = b.ns.instagram.com.

Authoritative answers can be found from:
d.ns.instagram.com      internet address = 185.89.219.12
b.ns.instagram.com      internet address = 129.134.31.12
a.ns.instagram.com      internet address = 129.134.30.12
c.ns.instagram.com      internet address = 185.89.218.12
d.ns.instagram.com      has AAAA address 2a03:2880:f1fd:c:face:b00c:0:35
b.ns.instagram.com      has AAAA address 2a03:2880:f0fd:c:face:b00c:0:35
a.ns.instagram.com      has AAAA address 2a03:2880:f0fc:c:face:b00c:0:35
c.ns.instagram.com      has AAAA address 2a03:2880:f1fc:c:face:b00c:0:35


┌──(crazybaby69㉿CrazyBaby69)-[~]
└─$ nslookup -type=RP instagram.com

Server:         192.168.229.2
Address:        192.168.229.2#53

Non-authoritative answer:
*** Can't find instagram.com: No answer
```

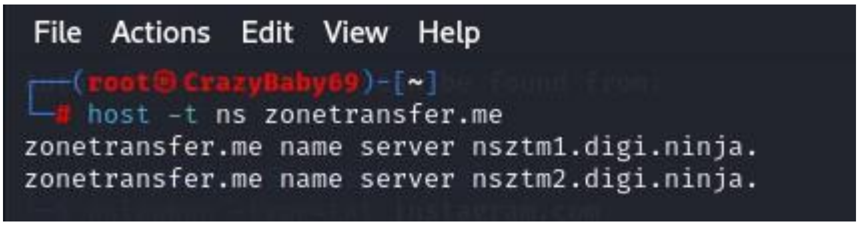
DNS Zone Transfer is an information gathering (foot printing) method to copy entire DNS file (all records). Special record type = AXFR (often used in DNS lookup tools)

Step 1: Get the NS for the target domain

Step 2: Attempt a zone transfer

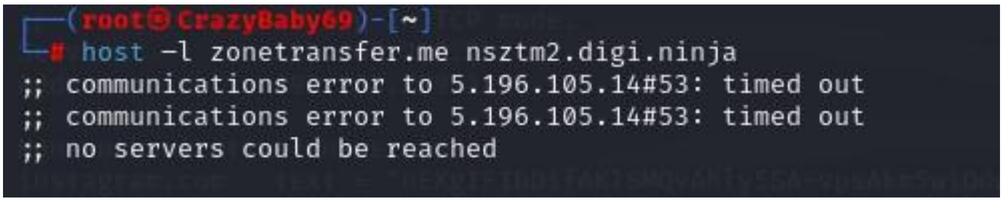
Let’s attempt a zone transfer on the following target: **zonetransfer.me**

6. In a terminal window, type the following command: **host ns zonetransfer.me**



```
┌──(root㉿CrazyBaby69)-[~]
└─# host -t ns zonetransfer.me
zonetransfer.me name server nsztm1.digi.ninja.
zonetransfer.me name server nsztm2.digi.ninja.
```

7. The output of the step above is a list of name servers. Use any in the following command: **host –l zonetransfer.me nsztm2.digi.ninja**

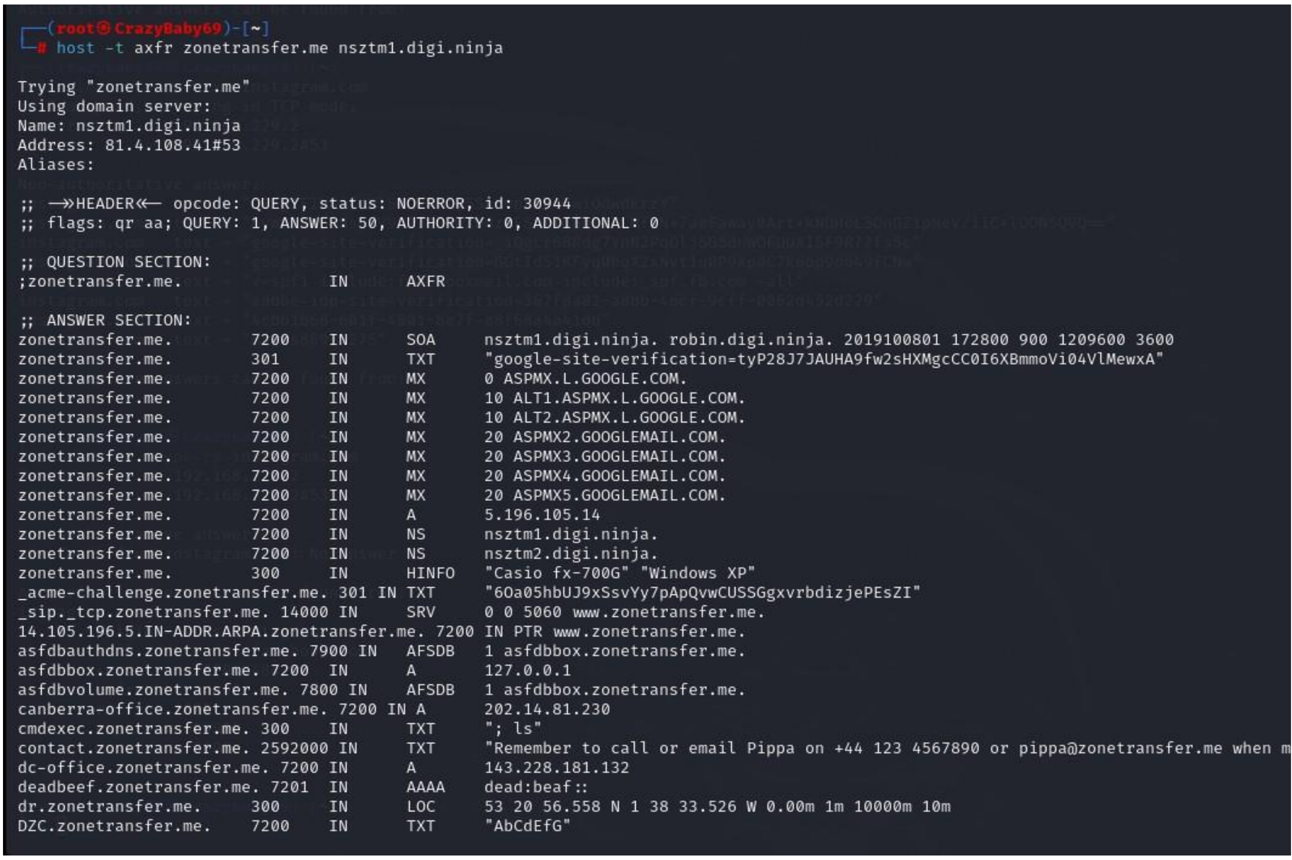


```
┌──(root㉿CrazyBaby69)-[~]
└─# host -l zonetransfer.me nsztm2.digi.ninja
;; communications error to 5.196.105.14#53: timed out
;; communications error to 5.196.105.14#53: timed out
;; no servers could be reached
```

Failed Zone Transfer

Let's try the same target using the AXFR record

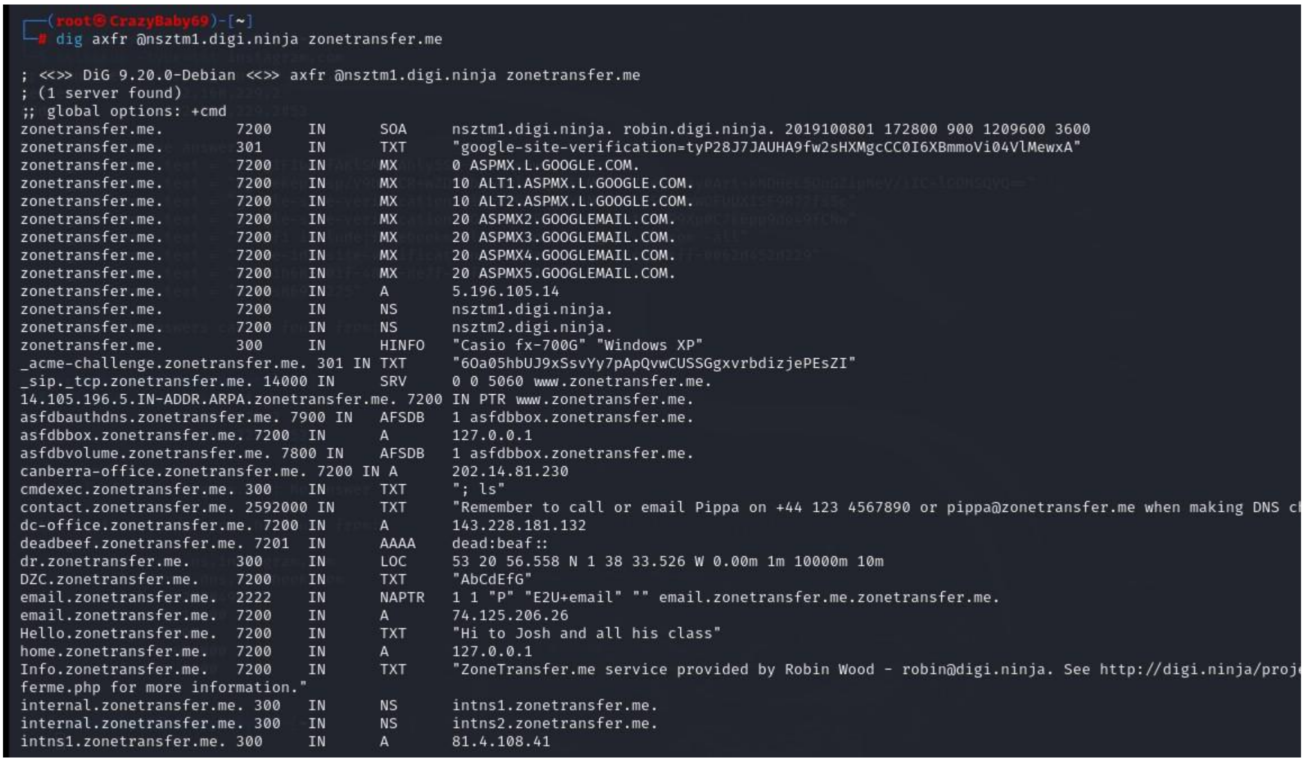
8. In a terminal window, type the following command: **host -t axfr zonetransfer.me nsztm1.digi.ninja**



```
┌──(root㉿CrazyBaby69)-[~]
└─# host -t axfr zonetransfer.me nsztm1.digi.ninja

Trying "zonetransfer.me"
Using domain server:
Name: nsztm1.digi.ninja
Address: 81.4.108.41#53
Aliases:

;; —»HEADER«— opcode: QUERY, status: NOERROR, id: 30944
;; flags: qr aa; QUERY: 1, ANSWER: 50, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;zonetransfer.me.              IN      AXFR

;; ANSWER SECTION:
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2019100801 172800 900 1209600 3600
zonetransfer.me.        301     IN      TXT     "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
zonetransfer.me.        7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      A       5.196.105.14
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows XP"
_acme-challenge.zonetransfer.me. 301 IN TXT     "6Oa05hbUJ9xSsvYy7pApQvwCUSSGgxvrbdizjePEsZI"
_sip._tcp.zonetransfer.me. 14000 IN     SRV     0 0 5060 www.zonetransfer.me.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200 IN PTR www.zonetransfer.me.
asfdbauthdns.zonetransfer.me. 7900 IN   AFSDB   1 asfdbbox.zonetransfer.me.
asfdbbox.zonetransfer.me. 7200  IN      A       127.0.0.1
asfdbvolume.zonetransfer.me. 7800 IN    AFSDB   1 asfdbbox.zonetransfer.me.
canberra-office.zonetransfer.me. 7200 IN A      202.14.81.230
cmdexec.zonetransfer.me. 300    IN      TXT     "; ls"
contact.zonetransfer.me. 2592000 IN     TXT     "Remember to call or email Pippa on +44 123 4567890 or pippa@zonetransfer.me when m
dc-office.zonetransfer.me. 7200 IN      A       143.228.181.132
deadbeef.zonetransfer.me. 7201  IN      AAAA    dead:beaf::
dr.zonetransfer.me.     300     IN      LOC     53 20 56.558 N 1 38 33.526 W 0.00m 1m 10000m 10m
DZC.zonetransfer.me.    7200    IN      TXT     "AbCdEfG"
```

Let's try the same target using DIG

9. In a terminal window, type the following command: **dig axfr @nsztm1.digi.ninja zonetransfer.me**



```
┌──(root㉿CrazyBaby69)-[~]
└─# dig axfr @nsztm1.digi.ninja zonetransfer.me

; <<>> DiG 9.20.0-Debian <<>> axfr @nsztm1.digi.ninja zonetransfer.me
; (1 server found)
;; global options: +cmd
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2019100801 172800 900 1209600 3600
zonetransfer.me.        301     IN      TXT     "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
zonetransfer.me.        7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      A       5.196.105.14
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows XP"
_acme-challenge.zonetransfer.me. 301 IN TXT     "6Oa05hbUJ9xSsvYy7pApQvwCUSSGgxvrbdizjePEsZI"
_sip._tcp.zonetransfer.me. 14000 IN     SRV     0 0 5060 www.zonetransfer.me.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200 IN PTR www.zonetransfer.me.
asfdbauthdns.zonetransfer.me. 7900 IN   AFSDB   1 asfdbbox.zonetransfer.me.
asfdbbox.zonetransfer.me. 7200  IN      A       127.0.0.1
asfdbvolume.zonetransfer.me. 7800 IN    AFSDB   1 asfdbbox.zonetransfer.me.
canberra-office.zonetransfer.me. 7200 IN A      202.14.81.230
cmdexec.zonetransfer.me. 300    IN      TXT     "; ls"
contact.zonetransfer.me. 2592000 IN     TXT     "Remember to call or email Pippa on +44 123 4567890 or pippa@zonetransfer.me when making DNS c
dc-office.zonetransfer.me. 7200 IN      A       143.228.181.132
deadbeef.zonetransfer.me. 7201  IN      AAAA    dead:beaf::
dr.zonetransfer.me.     300     IN      LOC     53 20 56.558 N 1 38 33.526 W 0.00m 1m 10000m 10m
DZC.zonetransfer.me.    7200    IN      TXT     "AbCdEfG"
email.zonetransfer.me.  2222    IN      NAPTR   1 1 "P" "E2U+email" "" email.zonetransfer.me.zonetransfer.me.
email.zonetransfer.me.  7200    IN      A       74.125.206.26
Hello.zonetransfer.me.  7200    IN      TXT     "Hi to Josh and all his class"
home.zonetransfer.me.   7200    IN      A       127.0.0.1
Info.zonetransfer.me.   7200    IN      TXT     "ZoneTransfer.me service provided by Robin Wood - robin@digi.ninja. See http://digi.ninja/proj
ferme.php for more information."
internal.zonetransfer.me. 300   IN      NS      intns1.zonetransfer.me.
internal.zonetransfer.me. 300   IN      NS      intns2.zonetransfer.me.
intns1.zonetransfer.me. 300     IN      A       81.4.108.41
```

It is very unlikely that a zone transfer will work. It is a relatively old technique. By itself, it is not an attack, but rather a way to get data and information that can help in an attack.

Task 3: Maltego (Independent)

Task Objectives

- You will use an open source intelligence tool to gather information about a domain

Maltego

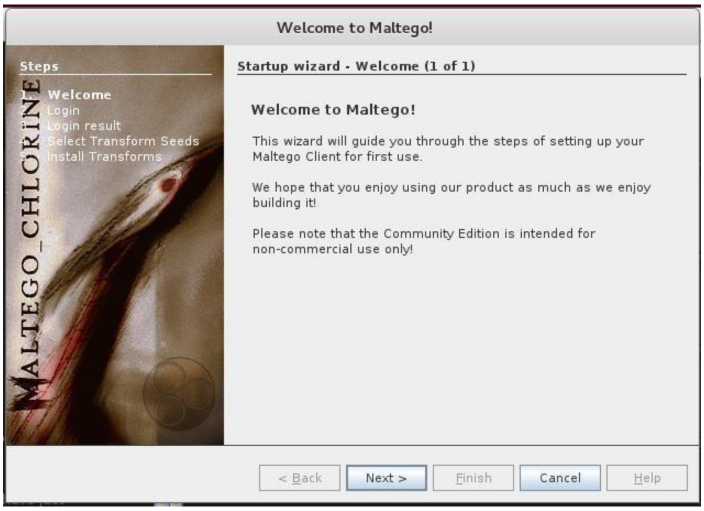
Maltgeo is an Open Source Intelligence Tool (OSIT). It is a tool that can graphically display the links between pieces of data. It can be used to map information regarding networks, organizations, people, and files.

Maltego is a client-server platform whereby the client interface sends XML data to the server which in turn sends the results back to be displayed in the client.

What's powerful about Maltego is its ability to collate data from multiple sources (sometimes as simple as a Google search) and present them to the tester in a visual format.

Among other things, Maltego searches WHOIS records, DNS records, public searches, and so on.

1. Power on Kali and open **Maltego** from **Applications □ 01-Information Gathering**
2. The first time you use Maltego, you will be asked to set it up. Click Next in the Startup wizard



Welcome to Maltego!

Startup wizard - Welcome (1 of 1)

Welcome to Maltego!

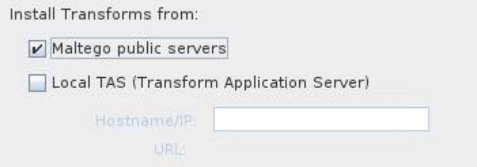
This wizard will guide you through the steps of setting up your Maltego Client for first use.

We hope that you enjoy using our product as much as we enjoy building it!

Please note that the Community Edition is intended for non-commercial use only!

3. Click register and complete your sign up information on the community website
4. You should receive an email confirmation with a link to activate your account
5. Click the link and on the website click the **Activate Account** button
6. Go back to Maltego and login and click **Next**

7. Keep the default Public Server and click **Next**

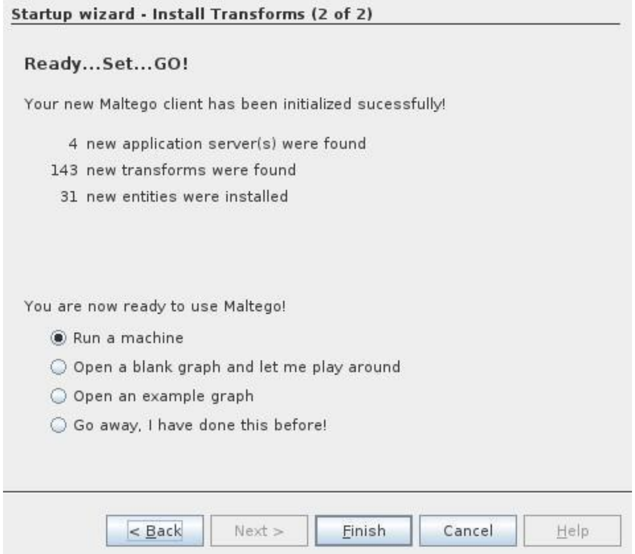


Install Transforms from:

☑ Maltego public servers

□ Local TAS (Transform Application Server)

8. You will get a summary of Maltego initialization. Click **Finish**



Startup wizard - Install Transforms (2 of 2)

Ready...Set...GO!

Your new Maltego client has been initialized sucessfully!

```
  4  new application server(s) were found
143  new transforms were found
 31  new entities were installed
```

You are now ready to use Maltego!

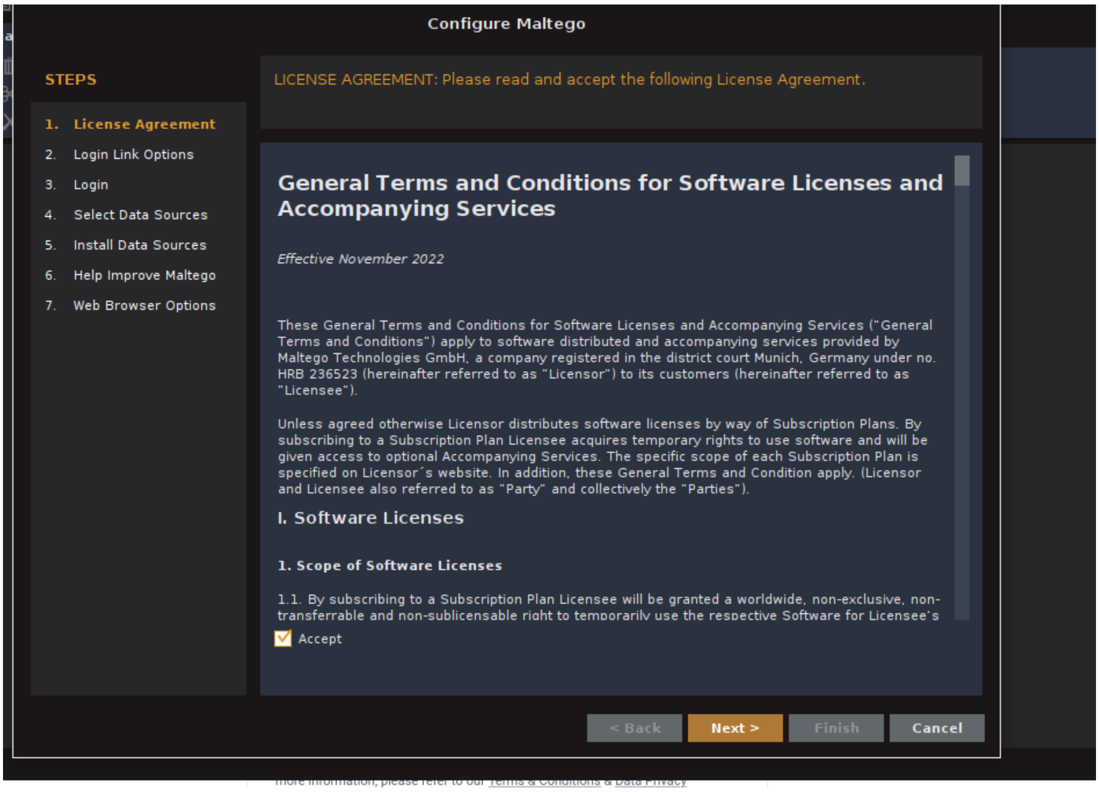
● Run a machine

○ Open a blank graph and let me play around

○ Open an example graph

○ Go away, I have done this before!

9. The **Run a machine** option will run start a machine based on your selection. For now, click Cancel in the **Start a Machine** popup



Configure Maltego

STEPS

1. **License Agreement**
2. Login Link Options
3. Login
4. Select Data Sources
5. Install Data Sources
6. Help Improve Maltego
7. Web Browser Options

LICENSE AGREEMENT: Please read and accept the following License Agreement.

General Terms and Conditions for Software Licenses and Accompanying Services

Effective November 2022

These General Terms and Conditions for Software Licenses and Accompanying Services ("General Terms and Conditions") apply to software distributed and accompanying services provided by Maltego Technologies GmbH, a company registered in the district court Munich, Germany under no. HRB 236523 (hereinafter referred to as "Licensor") to its customers (hereinafter referred to as "Licensee").

Unless agreed otherwise Licensor distributes software licenses by way of Subscription Plans. By subscribing to a Subscription Plan Licensee acquires temporary rights to use software and will be given access to optional Accompanying Services. The specific scope of each Subscription Plan is specified on Licensor´s website. In addition, these General Terms and Condition apply. (Licensor and Licensee also referred to as "Party" and collectively the "Parties").

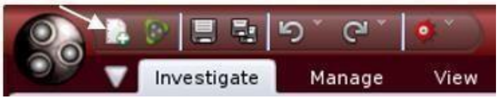
I. Software Licenses

1. Scope of Software Licenses

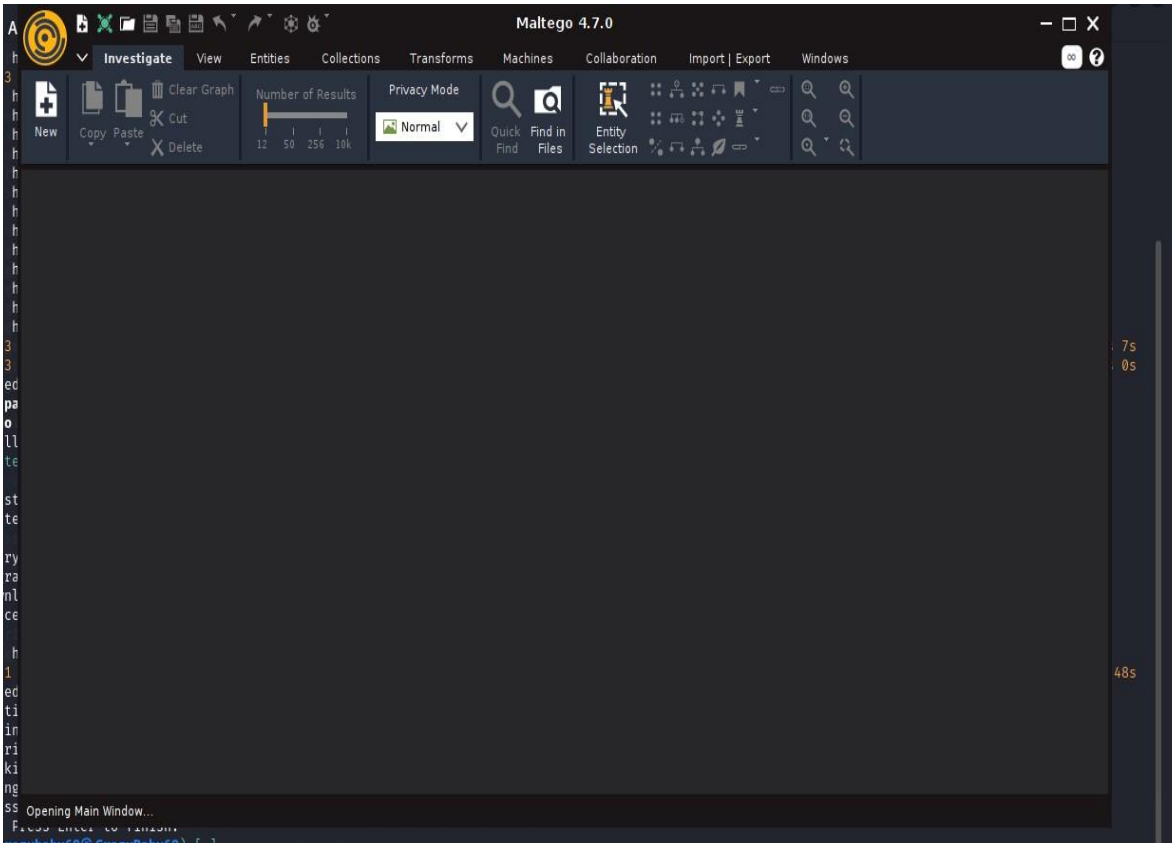
1.1. By subscribing to a Subscription Plan Licensee will be granted a worldwide, non-exclusive, non-transferrable and non-sublicensable right to temporarily use the respective Software for Licensee's

☑ Accept

10. Click the **Create a New Graph** icon



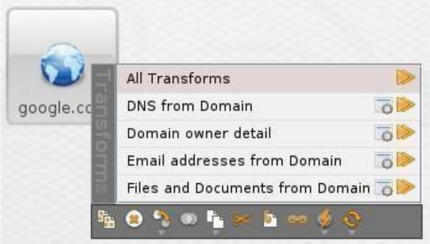
11. From the **Palette** on the left side, select **Domain** and drag it into the empty graph area



Opening Main Window...

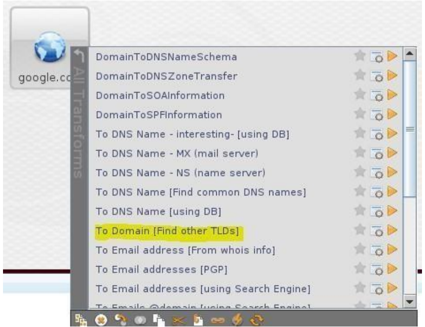
12. The default website is Paterva (the developer of Maltego). To change it, double-click the website name and type in google.com instead

13. To run a Transform on the website, right-click the website icon and select **All Transforms**

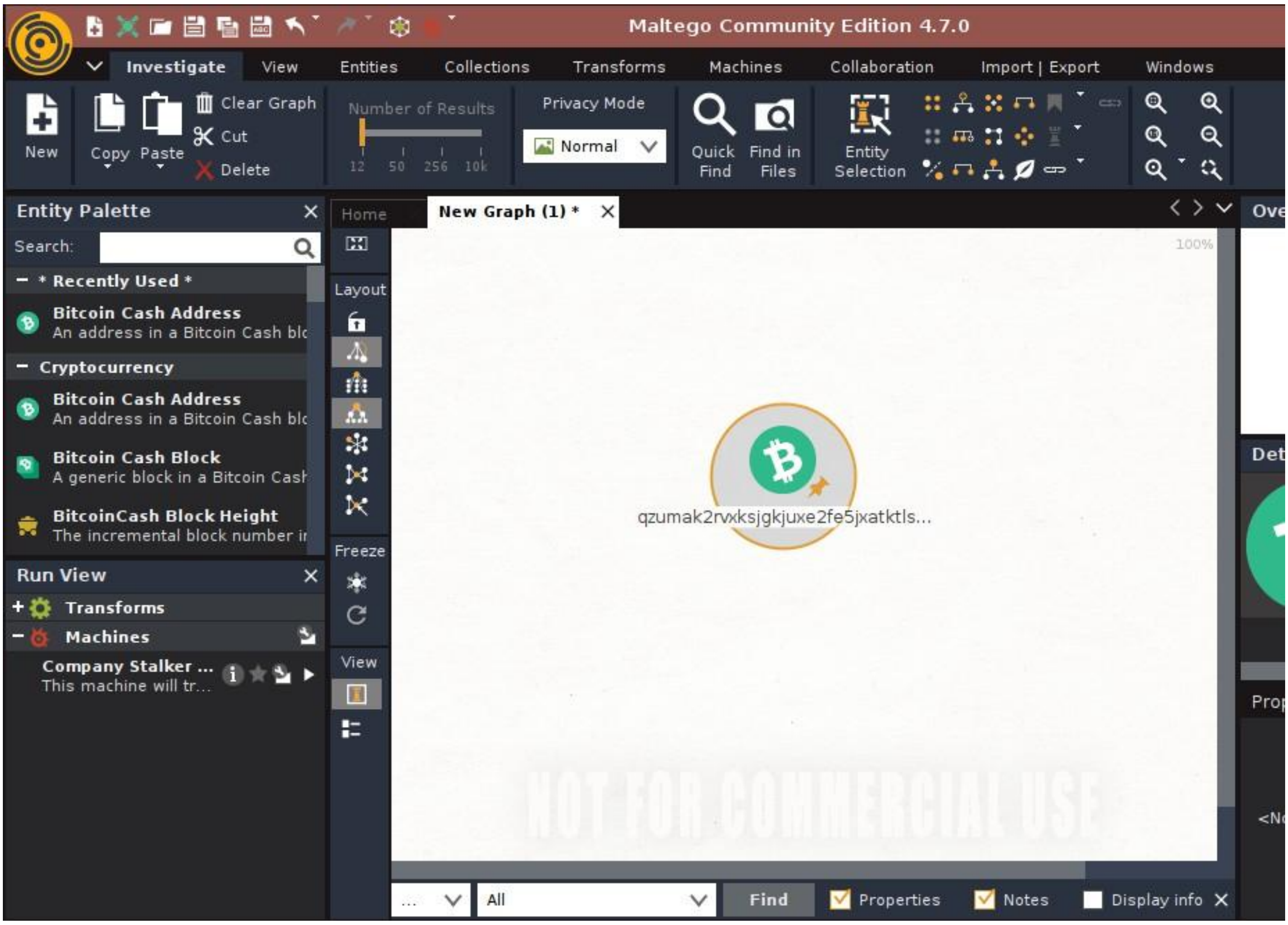


In Maltego, a Transform is a special code that converts results into something of interest to the tester.

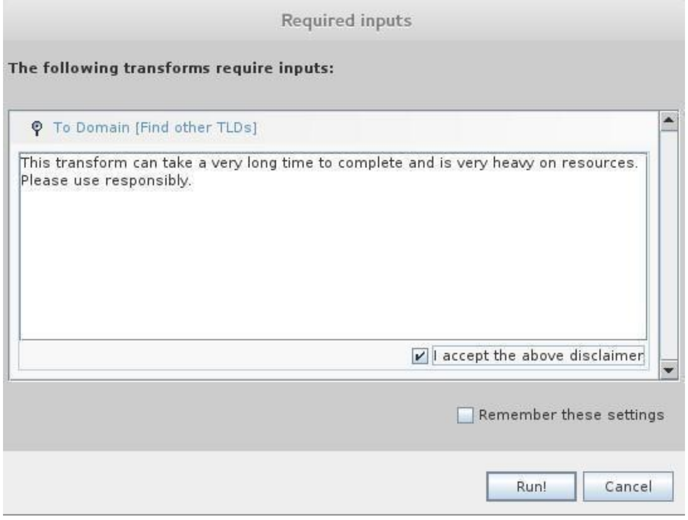
14. From the transforms list, select **To Domain [Find other TLDs]** transform


google.co
All Transforms
DomainToDNSNameSchema
DomainToDNSZoneTransfer
DomainToSOAInformation
DomainToSPFInformation
To DNS Name - interesting- [using DB]
To DNS Name - MX (mail server)
To DNS Name - NS (name server)
To DNS Name [Find common DNS names]
To DNS Name [using DB]
To Domain [Find other TLDs]
To Email address [From whois info]
To Email addresses [PGP]
To Email addresses [using Search Engine]

TLD is a Top Level Domain (e.g. .com or .ae)



15. Check the “I accept…” box and click **Run!**



The following transforms require inputs:

To Domain [Find other TLDs]

This transform can take a very long time to complete and is very heavy on resources. Please use responsibly.

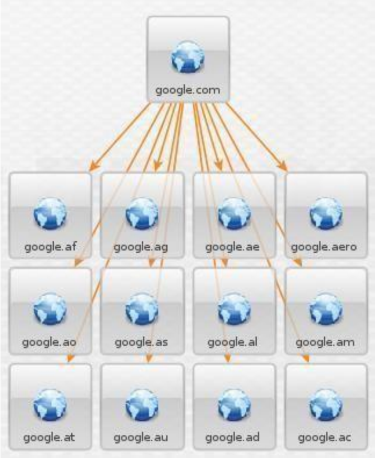
☑ I accept the above disclaimer

□ Remember these settings

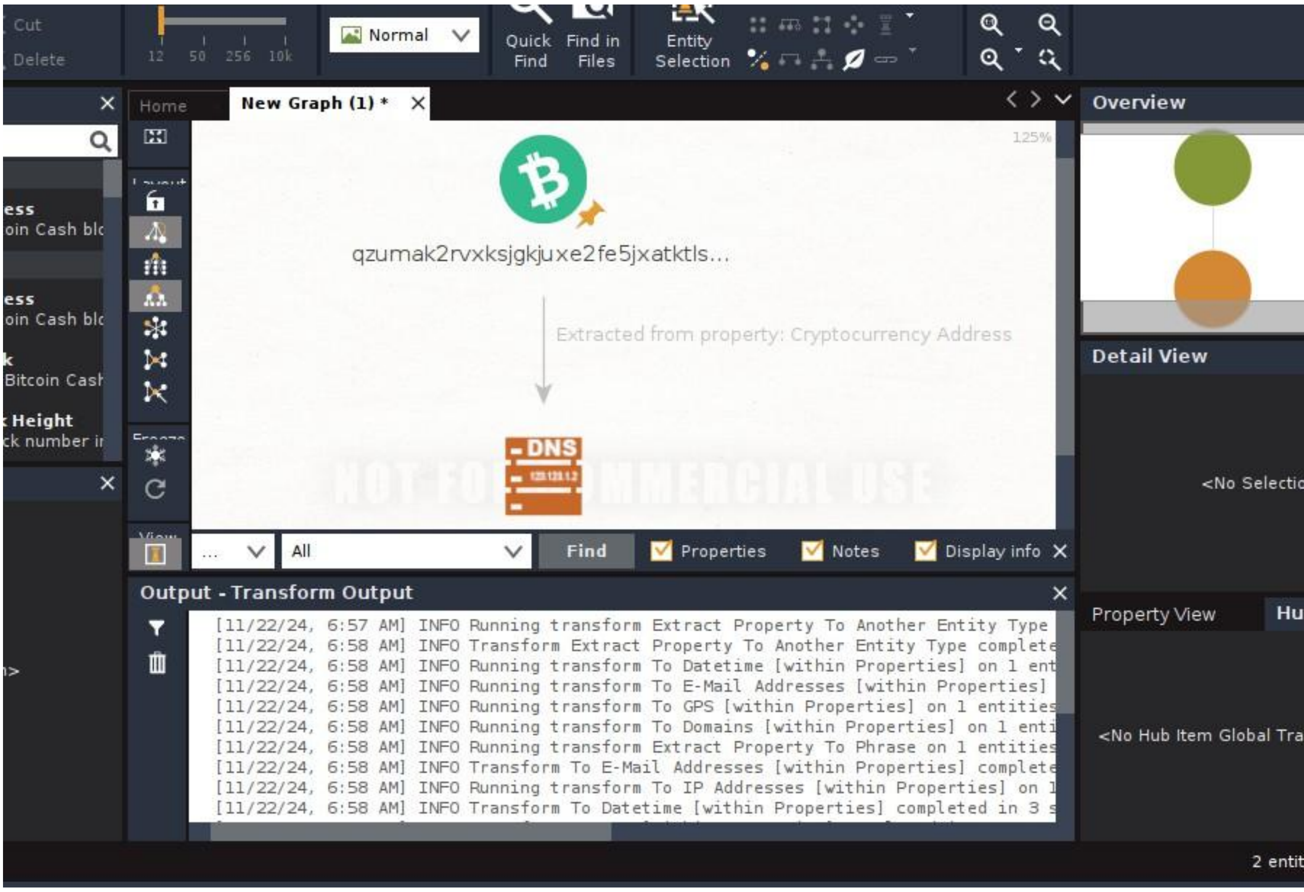
Always read the disclaimer and make sure you understand it!

In the Community edition of Maltego, you are limited to 12 transforms.

16. View the results. Zoom out using the mouse wheel and select all results

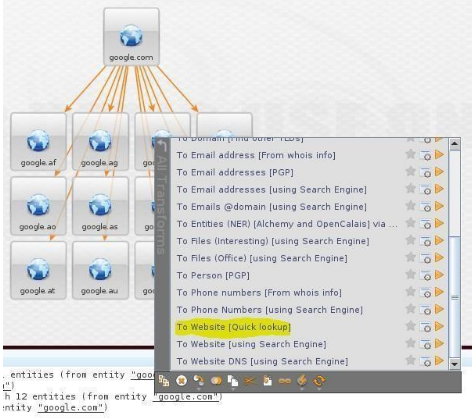


17. Right-click and select All Transforms (as you did before), and then select the **To Website [Quick lookup]** transform



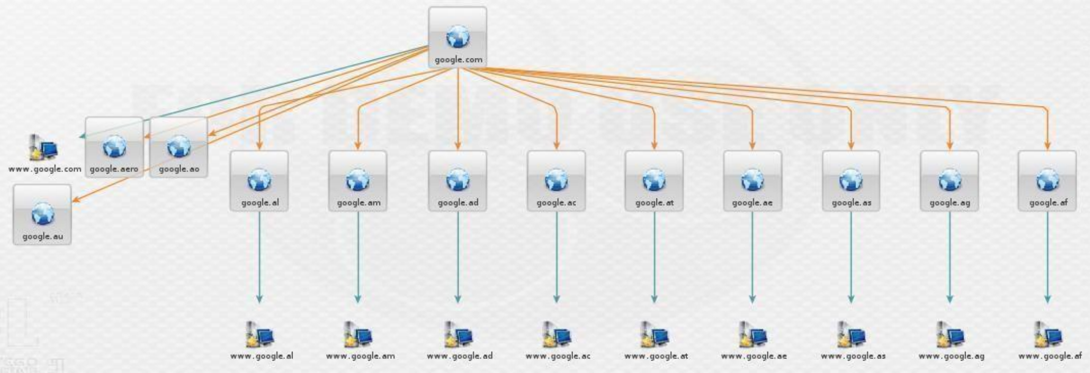
Output - Transform Output

```
[11/22/24, 6:57 AM] INFO Running transform Extract Property To Another Entity Type
[11/22/24, 6:58 AM] INFO Transform Extract Property To Another Entity Type complete
[11/22/24, 6:58 AM] INFO Running transform To Datetime [within Properties] on 1 ent
[11/22/24, 6:58 AM] INFO Running transform To E-Mail Addresses [within Properties]
[11/22/24, 6:58 AM] INFO Running transform To GPS [within Properties] on 1 entities
[11/22/24, 6:58 AM] INFO Running transform To Domains [within Properties] on 1 enti
[11/22/24, 6:58 AM] INFO Running transform Extract Property To Phrase on 1 entities
[11/22/24, 6:58 AM] INFO Transform To E-Mail Addresses [within Properties] complete
[11/22/24, 6:58 AM] INFO Running transform To IP Addresses [within Properties] on 1
[11/22/24, 6:58 AM] INFO Transform To Datetime [within Properties] completed in 3 s
```

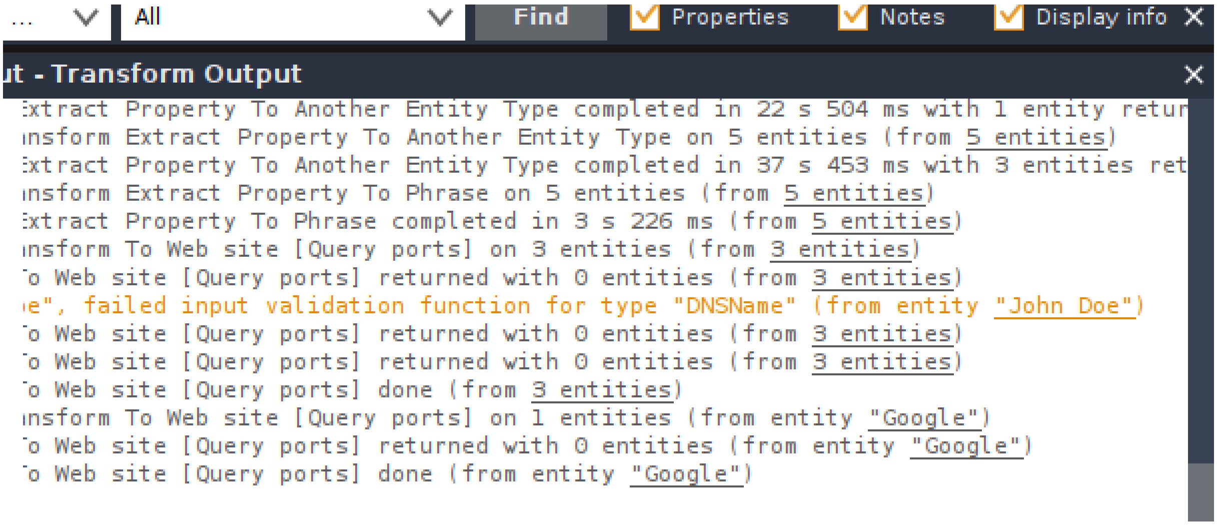

google.com
google.af
google.ag
goo
google.ao
google.as
go
google.at
google.au
goo
All Transforms
To Domain [Find other TLDs]
To Email address [From whois info]
To Email addresses [PGP]
To Email addresses [using Search Engine]
To Emails @domain [using Search Engine]
To Entities (NER) [Alchemy and OpenCalais] via ...
To Files (Interesting) [using Search Engine]
To Files (Office) [using Search Engine]
To Person [PGP]
To Phone numbers [From whois info]
To Phone Numbers [using Search Engine]
To Website [Quick lookup]
To Website [using Search Engine]
To Website DNS [using Search Engine]

```
. entities (from entity "goo
")
h 12 entities (from entity "google.com")
ntity "google.com")
```

This transform checks if there is a WWW entry for these domains



18. Notice that not all TLDs have actual WWW websites. Which ones don't? Hint: look for



```
xtract Property To Another Entity Type completed in 22 s 504 ms with 1 entity retur
insform Extract Property To Another Entity Type on 5 entities (from 5 entities)
xtract Property To Another Entity Type completed in 37 s 453 ms with 3 entities ret
insform Extract Property To Phrase on 5 entities (from 5 entities)
xtract Property To Phrase completed in 3 s 226 ms (from 5 entities)
insform To Web site [Query ports] on 3 entities (from 3 entities)
o Web site [Query ports] returned with 0 entities (from 3 entities)
e", failed input validation function for type "DNSName" (from entity "John Doe")
o Web site [Query ports] returned with 0 entities (from 3 entities)
o Web site [Query ports] returned with 0 entities (from 3 entities)
o Web site [Query ports] done (from 3 entities)
insform To Web site [Query ports] on 1 entities (from entity "Google")
o Web site [Query ports] returned with 0 entities (from entity "Google")
o Web site [Query ports] done (from entity "Google")
```

0 Outgoing connections

We found entities different from each other but one of them was giving invalid

19. Save the output file on Kali's Desktop

What is the Maltego file extension?	.mtgl

20. Run other transforms on other websites

Task 4: SpiderFoot (Independent)

Task Objectives

- You will install and use an open source intelligence tool to collect and analyze information about a target system

SpiderFoot

SpiderFoot:

SpiderFoot is an open source intelligence tool. Its goal is to automate the process of gathering intelligence about a given target, which may be an IP address, domain name, hostname or network subnet.

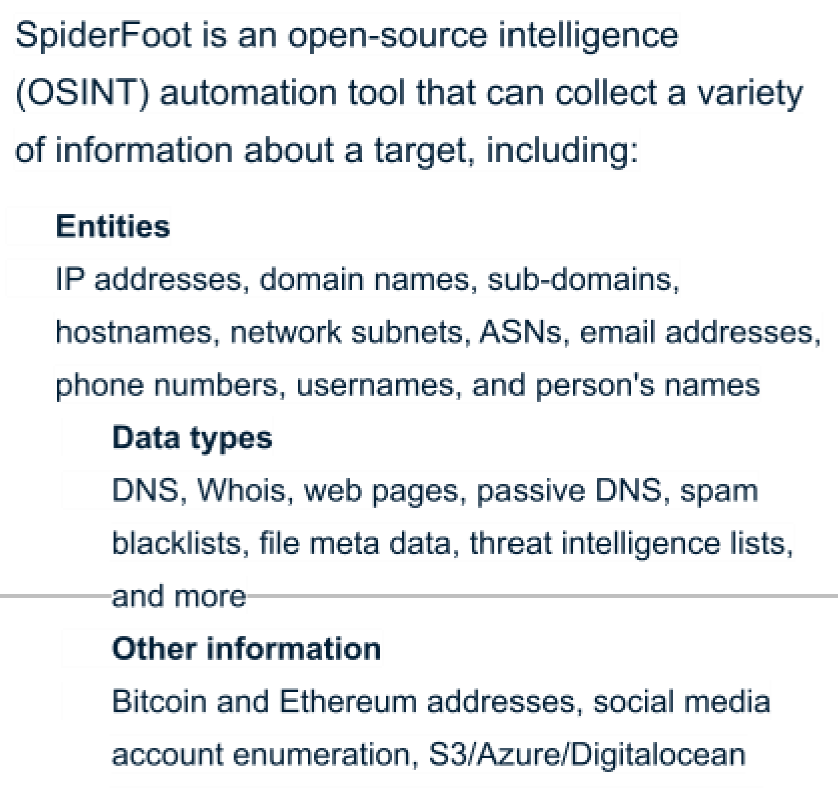
SpiderFoot can be used offensively, i.e. as part of a black-box penetration test to gather information about the target or defensively to identify what information your organisation is freely providing for attackers to use against you.

Source: http://www.spiderfoot.net/documentation/

1. Download the SpiderFoot on linux

```
sudo apt update
sudo apt install spiderfoot
```

2. Or Unzip **SpiderFoot-2.5.1-w32.zip** and install it on the lab (PC windows) [Nixintel Open Source Intelligence & Investigations Getting Started With Spiderfoot – A Beginner's Guide]()
3. Learn what the tool does and hot to use it (**www.spiderfoot.net**)
4. Apply your knowledge
5. What kind of information can you collect using SpiderFoot?



SpiderFoot is an open-source intelligence (OSINT) automation tool that can collect a variety of information about a target, including:

Entities
IP addresses, domain names, sub-domains, hostnames, network subnets, ASNs, email addresses, phone numbers, usernames, and person's names

Data types
DNS, Whois, web pages, passive DNS, spam blacklists, file meta data, threat intelligence lists, and more

Other information
Bitcoin and Ethereum addresses, social media account enumeration, S3/Azure/Digitalocean

Review Questions

The following questions are based on the information and activities performed in the activity you just completed.

1. *Which tool is NOT a DNS foot printing tool?*
    - A. dig
    - B. host
    - C. nbstat
    - D. nslookup

2. *Which query system is used to lookup registered users and domains online?*
    - A. WHOIS
    - B. DNS
    - C. ICANN
    - D. Foot printing

3. *Foot printing is mainly part of what penetration testing phase?*
    - A. Scanning
    - B. Raconnaissance
    - C. Planning
    - D. Assessment

4. *Which DNS record is used to perform a zone transfer?*
    - A. A
    - B. MX
    - C. ZXFR
    - D. AFXR

5. *What application level protocol is used to perform a DIG or HOST query? And what transport level protocol is used?*

Both dig and host uses DNS application level protocol