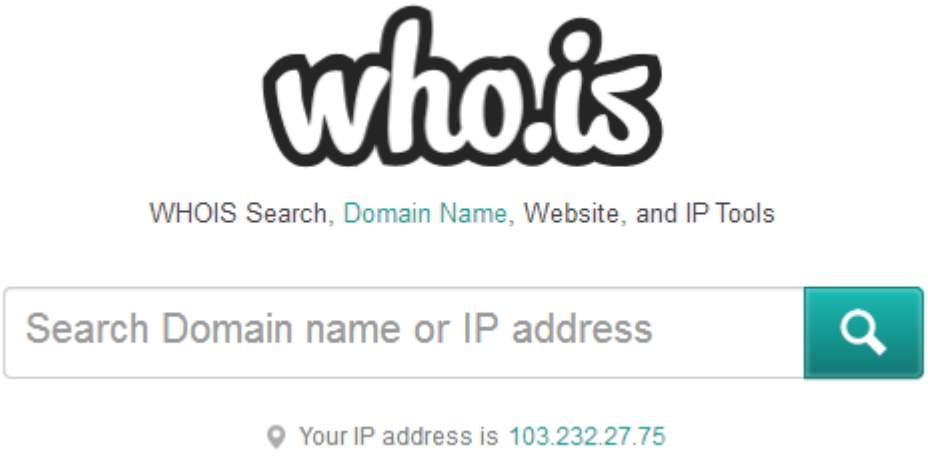
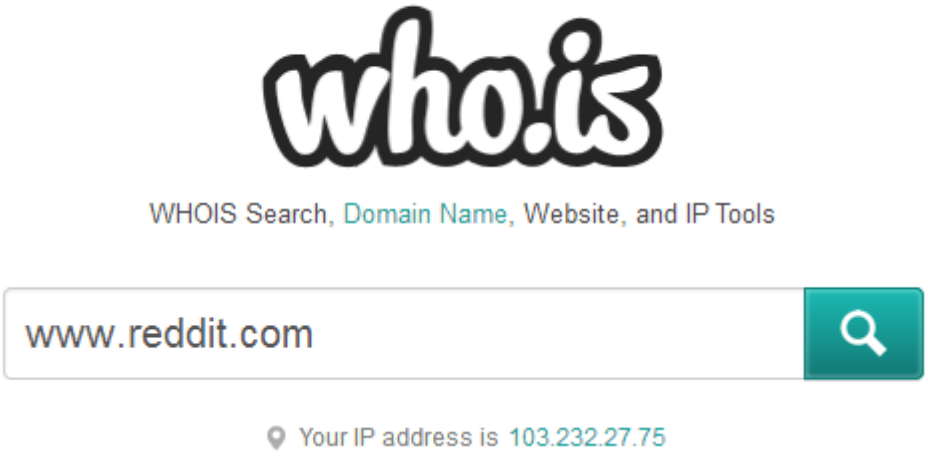
Practical-1

Aim:-Using the tools for WHOis, traceroute, email tracking.

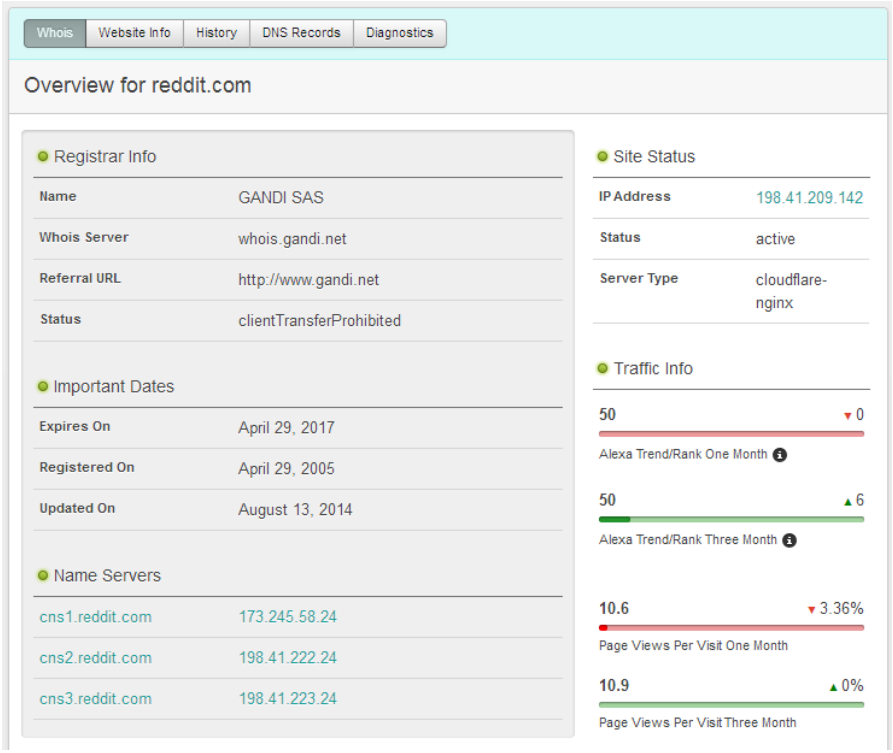
Step 1: Open the WHOis website.

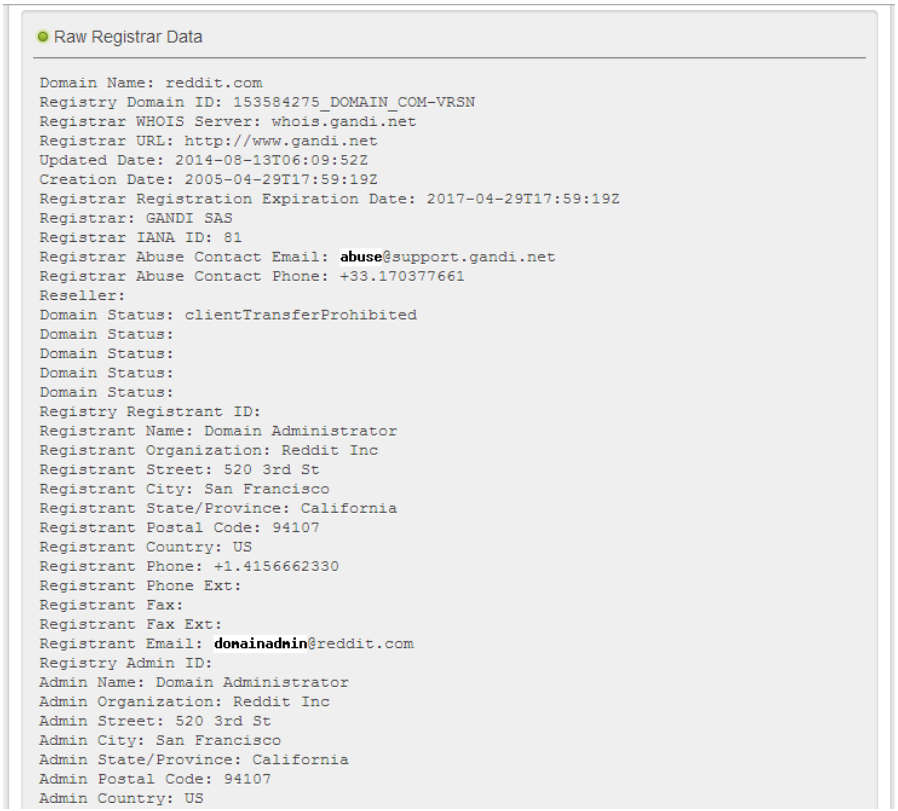


Step 2: Enter the website name and hit the “enter button”.



Step 3: Show you information about reddit.com in whois tab.



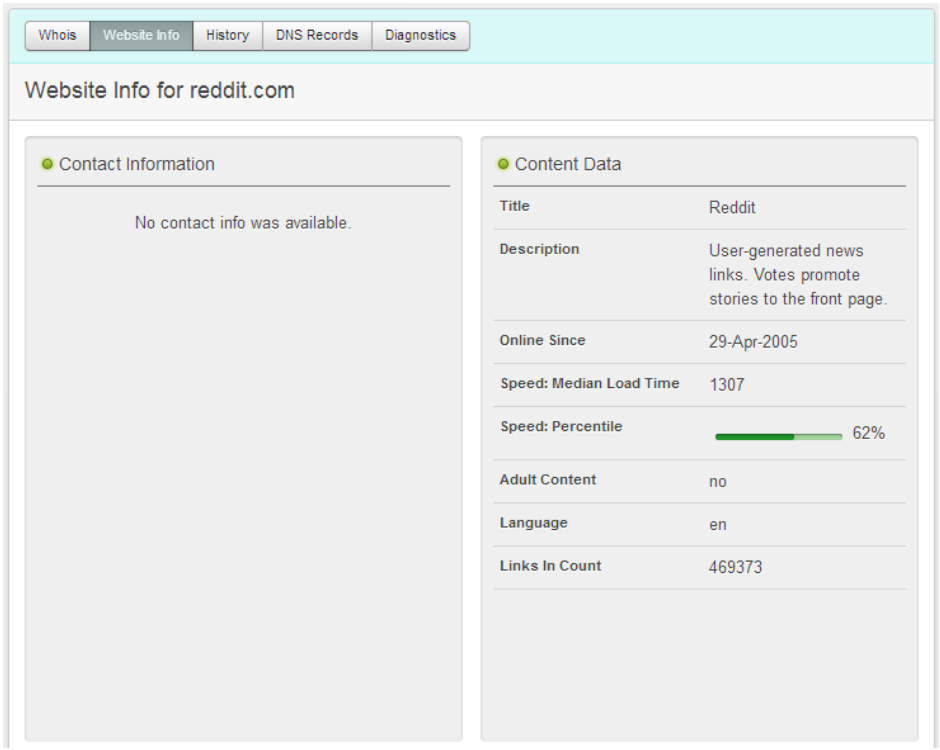


```
Admin Country: US
Admin Phone: +1.4156662330
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domainadmin@reddit.com
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: Reddit Inc
Tech Street: 520 3rd St
Tech City: San Francisco
Tech State/Province: California
Tech Postal Code: 94107
Tech Country: US
Tech Phone: +1.4156662330
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: domainadmin@reddit.com
Name Server: CNS1.REDDIT.COM
Name Server: CNS2.REDDIT.COM
Name Server: CNS3.REDDIT.COM
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
DNSSEC: Unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2014-09-02T06:18:01Z <<<

Reseller Email:
Reseller URL:

Personal data access and use are governed by French law, any use for
the purpose of unsolicited mass commercial advertising as well as any
mass or automated inquiries (for any intent other than the
registration or modification of a domain name) are strictly forbidden.
Copy of whole or part of our database without Gandi's endorsement is
```


```
Personal data access and use are governed by French law, any use for
the purpose of unsolicited mass commercial advertising as well as any
mass or automated inquiries (for any intent other than the
registration or modification of a domain name) are strictly forbidden.
Copy of whole or part of our database without Gandi's endorsement is
```


```
strictly forbidden.
The owner of a domain is the person specified as "Registrant Name" for
a natural person and "Registrant Organization" for a legal person.
Domain ownership disputes should be settled using ICANN's Uniform
Dispute Resolution Policy: http://www.icann.org/en/help/dndr#udrp

Information Updated: Tue, 2 Sep 2014 06:18:01 UTC
```

Step 4: Show you information about reddit.com in website information tab



Page Views Per Million	1.00 ▲2.7%
Page Views Per User	10.64 ▼3.36%

7 Days

Rank	50 ▼2
Reach Rank	50 ▲2
Page Views Rank	39 ▼1
Reach Per Million	19.00 ▲1.6%
Page Views Per Million	1.00 ▼1.91%
Page Views Per User	10.22 ▼3.49%

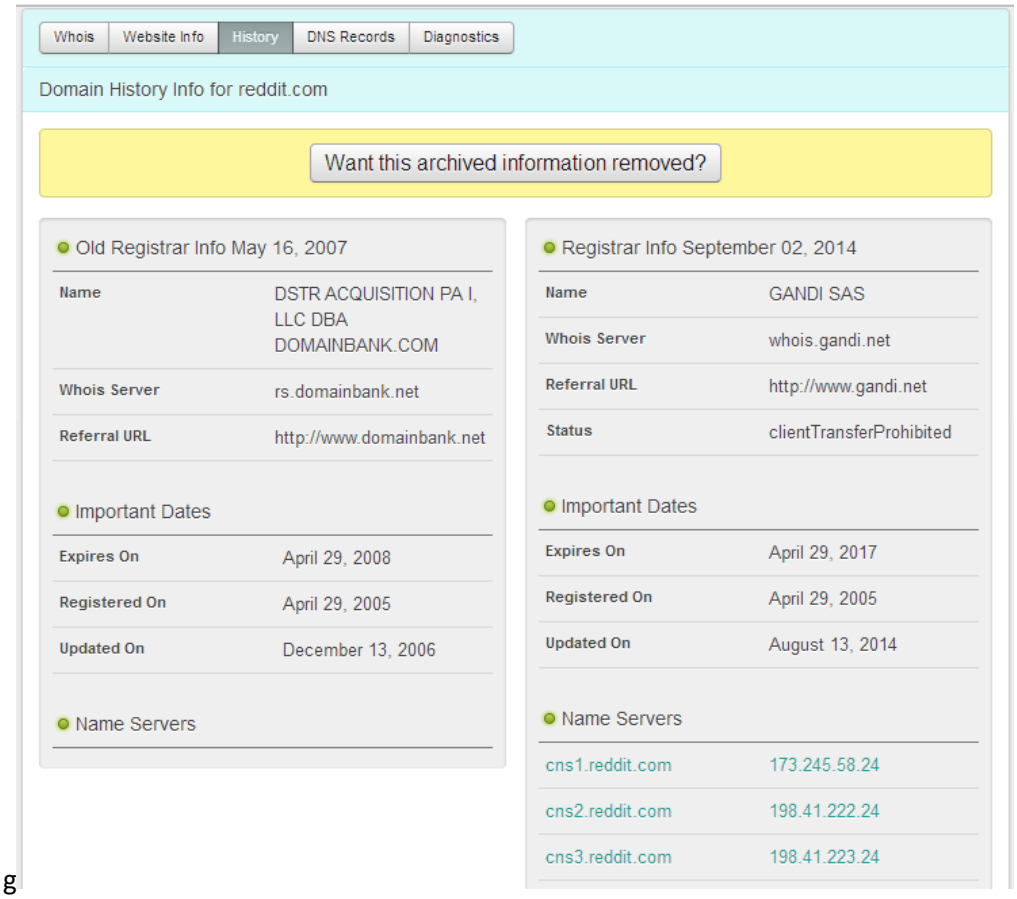
1 Days

Rank	42 ▲4
Reach Rank	48 ▲1
Page Views Rank	34 ▲4
Reach Per Million	20.00 ▲8%
Page Views Per Million	2.00 ▲9.3%
Page Views Per User	10.80 ▲1%

Subdomains

	Reach	Page Views	Page Views Per User
reddit.com	98.91%	97.78%	10.73
np.reddit.com	3.67%	0.86%	2.55
ssl.reddit.com	2.74%	0.38%	1.51
pay.reddit.com	0.17%	0.23%	15.2
fr.reddit.com	0.20%	0.23%	12.6
us.reddit.com	0.10%	0.14%	15
nl.reddit.com	0.03%	0.07%	22
OTHER		0.30%	

Step 5: Show you information about reddit.com in history tab.



g

Old Raw Registrar Data May 16, 2007

```
The information in this whois database
is provided for the sole
purpose of assisting you in obtaining
information about domain
name registration records. This
information is available "as is,"
and we do not guarantee its accuracy.
By submitting a whois
query, you agree that you will use this
data only for lawful
purposes and that, under no
circumstances will you use this data
to: (1) enable high volume, automated,
electronic processes that
stress or load this whois database
system providing you this
information; or (2) allow,enable, or
otherwise support the
transmission of mass, unsolicited,
commercial advertising or
solicitations via facsimile, electronic
mail, or by telephone to
entitites other than your own existing
customers.  The
compilation, repackaging, dissemination
or other use of this data
is expressly prohibited without prior
written consent from this
company. We reserve the right to modify
these terms at any
time. By submitting an inquiry, you
agree to these terms of usage
and limitations of warranty.  Please
limit your queries to 10 per
minute and one connection.

   Domain Services Provided By:
      Domain Bank, support
      @domainbank.com
      http:///www.domainbank.com

Registrant:
   CONDENET INC
   Four Times Square
   New York, NY  10036
   US

   Registrar: DOMAINBANK
   Domain Name: REDDIT.COM
      Created on: 29-APR-05
      Expires on: 29-APR-08
      Last Updated on: 13-DEC-06

   Administrative Contact:
      ,   domain_admin@advancemags.com
      Advance Magazine Group
      4 Times Square
      23rd Floor
      New York, New York  10036
      US
      2122862860

   Technical Contact:
      ,   domains@advancemags.com
      Advance Magazine Group
      1201 N. Market St
      Wilmington, DE  19801
      US
      3028304630


   Domain servers in listed order:
      NS2.ADVANCEMAGS.COM
      NS3.ADVANCEMAGS.COM
      NS4.ADVANCEPUBS.NET

End of Whois Information
```

Raw Registrar Data September 02, 2014

```
Domain Name: reddit.com
Registry Domain ID:
153584275_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2014-08-13T06:09:52Z
Creation Date: 2005-04-29T17:59:19Z
Registrar Registration Expiration Date:
2017-04-29T17:59:19Z
Registrar: GANDI SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse
@support.gandi.net
Registrar Abuse Contact Phone:
+33.170377661
Reseller:
Domain Status: clientTransferProhibited
Domain Status:
Domain Status:
Domain Status:
Domain Status:
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Reddit Inc
Registrant Street: 520 3rd St
Registrant City: San Francisco
Registrant State/Province: California
Registrant Postal Code: 94107
Registrant Country: US
Registrant Phone: +1.4156662330
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domainadmin@reddit.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Reddit Inc
Admin Street: 520 3rd St
Admin City: San Francisco
Admin State/Province: California
Admin Postal Code: 94107
Admin Country: US
Admin Phone: +1.4156662330
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domainadmin@reddit.com
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: Reddit Inc
Tech Street: 520 3rd St
Tech City: San Francisco
Tech State/Province: California
Tech Postal Code: 94107
Tech Country: US
Tech Phone: +1.4156662330
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: domainadmin@reddit.com
Name Server: CNS1.REDDIT.COM
Name Server: CNS2.REDDIT.COM
Name Server: CNS3.REDDIT.COM
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
DNSSEC: Unsigned
URL of the ICANN WHOIS Data Problem
Reporting System:
http://wdprs.internic.net/
>>> Last update of WHOIS database:
2014-09-02T06:18:01Z <<<
```

End of Whois Information

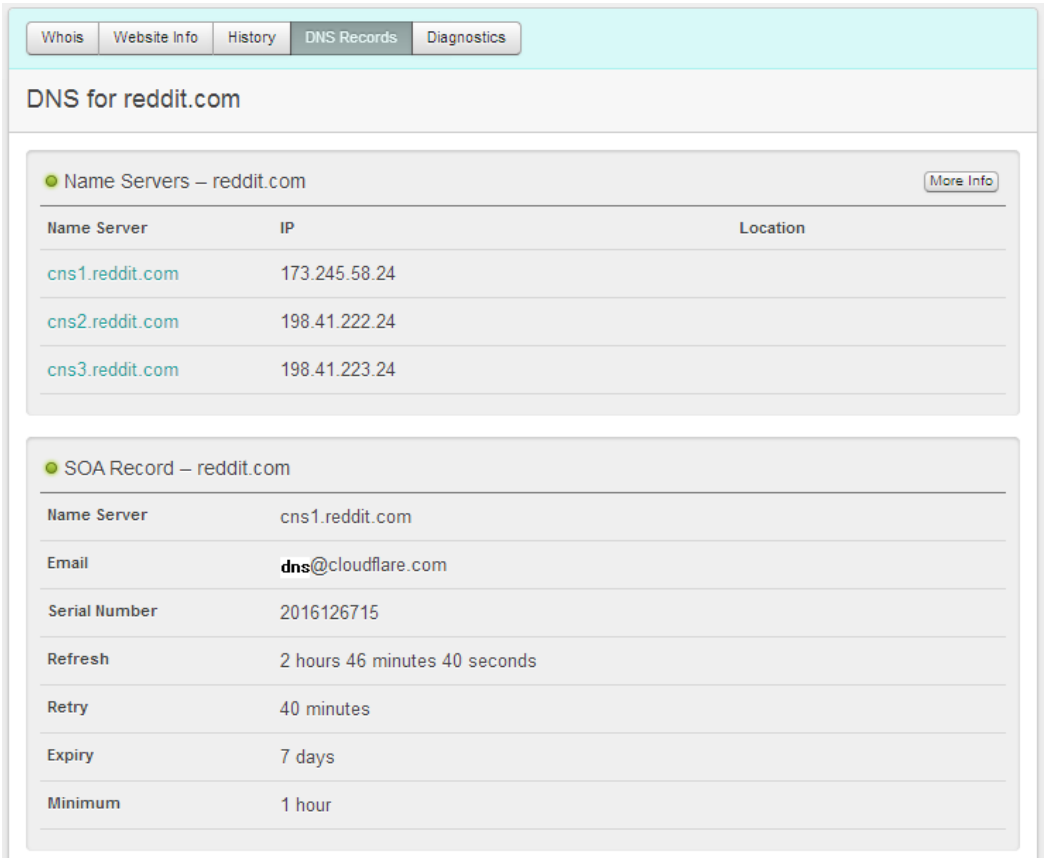
Information Updated: Tue, 2 Sep 2014 06:18:01 UTC

Reseller Email:
Reseller URL:

Personal data access and use are governed by French law, any use for the purpose of unsolicited mass commercial advertising as well as any mass or automated inquiries (for any intent other than the registration or modification of a domain name) are strictly forbidden. Copy of whole or part of our database without Gandi's endorsement is strictly forbidden.
The owner of a domain is the person specified as "Registrant Name" for a natural person and "Registrant Organization" for a legal person.
Domain ownership disputes should be settled using ICANN's Uniform Dispute Resolution Policy:
http://www.icann.org/en/help/dndr#udrp

Information Updated: Tue, 2 Sep 2014 06:18:01 UTC

Step 6: Show you information about reddit.com in dns records tab.



DNS Records – REDDIT.COM

Record	Type	TTL	Priority	Content
reddit.com	A	5 minutes		198.41.209.140 ()
reddit.com	A	5 minutes		198.41.209.143 ()
reddit.com	A	5 minutes		198.41.208.140 ()
reddit.com	A	5 minutes		198.41.208.142 ()
reddit.com	A	5 minutes		198.41.209.136 ()
reddit.com	A	5 minutes		198.41.209.137 ()
reddit.com	A	5 minutes		198.41.208.143 ()
reddit.com	A	5 minutes		198.41.208.138 ()
reddit.com	A	5 minutes		198.41.209.141 ()
reddit.com	A	5 minutes		198.41.208.141 ()
reddit.com	A	5 minutes		198.41.209.139 ()
reddit.com	A	5 minutes		198.41.209.138 ()
reddit.com	A	5 minutes		198.41.208.139 ()
reddit.com	A	5 minutes		198.41.209.142 ()
reddit.com	A	5 minutes		198.41.208.137 ()
reddit.com	MX	5 minutes	5	alt2.aspmx.l.google.com
reddit.com	MX	5 minutes	10	aspmx3.googlemail.com
reddit.com	MX	5 minutes	10	aspmx3.googlemail.com
reddit.com	MX	5 minutes	1	aspmx.l.google.com
reddit.com	MX	5 minutes	5	alt1.aspmx.l.google.com
reddit.com	MX	5 minutes	10	aspmx2.googlemail.com
reddit.com	NS	1 day		cns3.reddit.com
reddit.com	NS	1 day		cns2.reddit.com
reddit.com	NS	1 day		cns1.reddit.com
cns3.reddit.com	A	15 minutes		198.41.223.24 ()
cns3.reddit.com	AAAA	15 minutes		2400:cb00:2049:1::c629:df18
cns2.reddit.com	AAAA	15 minutes		2400:cb00:2049:1::c629:de18
cns2.reddit.com	A	15 minutes		198.41.222.24 ()
cns1.reddit.com	A	15 minutes		173.245.58.24 ()
cns1.reddit.com	AAAA	15 minutes		2400:cb00:2049:1::adf5:3a18
reddit.com	SOA	1 day		cns1.reddit.com. dns.cloudflare.com. 2016126715 10000 2400 604800 3600
reddit.com	TXT	5 minutes		v=spf1 include:_spf.google.com a:mail.reddit.com include:helpscoutemail.com -all
*.reddit.com	A	5 minutes		198.41.209.139 ()
*.reddit.com	A	5 minutes		198.41.208.140 ()
*.reddit.com	A	5 minutes		198.41.208.143 ()

*.reddit.com	A	5 minutes	198.41.209.136 ()
*.reddit.com	A	5 minutes	198.41.209.138 ()
*.reddit.com	A	5 minutes	198.41.209.143 ()
*.reddit.com	A	5 minutes	198.41.208.139 ()
*.reddit.com	A	5 minutes	198.41.209.140 ()
*.reddit.com	A	5 minutes	198.41.209.142 ()
*.reddit.com	A	5 minutes	198.41.208.137 ()
*.reddit.com	A	5 minutes	198.41.209.141 ()
*.reddit.com	A	5 minutes	198.41.208.141 ()
*.reddit.com	A	5 minutes	198.41.208.138 ()
*.reddit.com	A	5 minutes	198.41.209.137 ()
*.reddit.com	A	5 minutes	198.41.208.142 ()
blog.reddit.com	A	5 minutes	198.41.209.138 ()
blog.reddit.com	A	5 minutes	198.41.209.141 ()
blog.reddit.com	A	5 minutes	198.41.208.138 ()
blog.reddit.com	A	5 minutes	198.41.208.140 ()
blog.reddit.com	A	5 minutes	198.41.209.137 ()
blog.reddit.com	A	5 minutes	198.41.209.140 ()
blog.reddit.com	A	5 minutes	198.41.209.136 ()

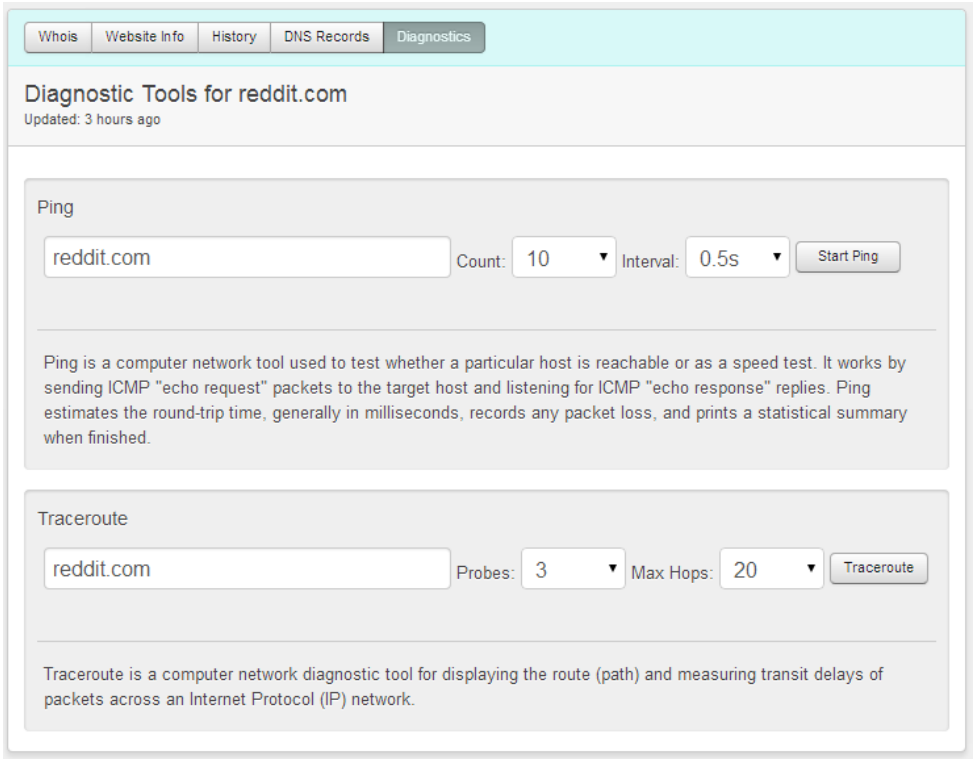
blog.reddit.com	A	5 minutes	198.41.209.136 ()
blog.reddit.com	A	5 minutes	198.41.209.143 ()
blog.reddit.com	A	5 minutes	198.41.208.139 ()
blog.reddit.com	A	5 minutes	198.41.208.137 ()
blog.reddit.com	A	5 minutes	198.41.209.139 ()
blog.reddit.com	A	5 minutes	198.41.208.143 ()
blog.reddit.com	A	5 minutes	198.41.208.141 ()
blog.reddit.com	A	5 minutes	198.41.209.142 ()
forum.reddit.com	A	5 minutes	198.41.209.137 ()
forum.reddit.com	A	5 minutes	198.41.208.137 ()
forum.reddit.com	A	5 minutes	198.41.209.142 ()
forum.reddit.com	A	5 minutes	198.41.209.139 ()
forum.reddit.com	A	5 minutes	198.41.208.139 ()
forum.reddit.com	A	5 minutes	198.41.209.141 ()
forum.reddit.com	A	5 minutes	198.41.208.143 ()
forum.reddit.com	A	5 minutes	198.41.208.140 ()
forum.reddit.com	A	5 minutes	198.41.209.138 ()
forum.reddit.com	A	5 minutes	198.41.209.136 ()
forum.reddit.com	A	5 minutes	198.41.209.140 ()

forum.reddit.com	A	5 minutes	198.41.208.138 ()
forum.reddit.com	A	5 minutes	198.41.209.143 ()
forum.reddit.com	A	5 minutes	198.41.208.141 ()
help.reddit.com	A	5 minutes	198.41.209.141 ()
help.reddit.com	A	5 minutes	198.41.208.143 ()
help.reddit.com	A	5 minutes	198.41.208.137 ()
help.reddit.com	A	5 minutes	198.41.209.142 ()
help.reddit.com	A	5 minutes	198.41.208.140 ()
help.reddit.com	A	5 minutes	198.41.209.137 ()
help.reddit.com	A	5 minutes	198.41.209.136 ()
help.reddit.com	A	5 minutes	198.41.209.139 ()
help.reddit.com	A	5 minutes	198.41.209.138 ()
help.reddit.com	A	5 minutes	198.41.209.143 ()
help.reddit.com	A	5 minutes	198.41.208.139 ()
help.reddit.com	A	5 minutes	198.41.209.140 ()
help.reddit.com	A	5 minutes	198.41.208.141 ()
help.reddit.com	A	5 minutes	198.41.208.138 ()
mail.reddit.com	A	5 minutes	174.129.203.189 (Seattle, WA, US)
test.reddit.com	A	5 minutes	198.41.209.140 ()

test.reddit.com	A	5 minutes	198.41.209.140 ()
test.reddit.com	A	5 minutes	198.41.208.139 ()
test.reddit.com	A	5 minutes	198.41.209.141 ()
test.reddit.com	A	5 minutes	198.41.209.136 ()
test.reddit.com	A	5 minutes	198.41.208.141 ()
test.reddit.com	A	5 minutes	198.41.208.140 ()
test.reddit.com	A	5 minutes	198.41.209.137 ()
test.reddit.com	A	5 minutes	198.41.209.143 ()
test.reddit.com	A	5 minutes	198.41.208.143 ()
test.reddit.com	A	5 minutes	198.41.209.139 ()
test.reddit.com	A	5 minutes	198.41.209.142 ()
test.reddit.com	A	5 minutes	198.41.209.138 ()
test.reddit.com	A	5 minutes	198.41.208.138 ()
test.reddit.com	A	5 minutes	198.41.208.137 ()
www.reddit.com	A	5 minutes	198.41.208.137 ()
www.reddit.com	A	5 minutes	198.41.209.138 ()
www.reddit.com	A	5 minutes	198.41.208.139 ()
www.reddit.com	A	5 minutes	198.41.209.140 ()
www.reddit.com	A	5 minutes	198.41.209.136 ()

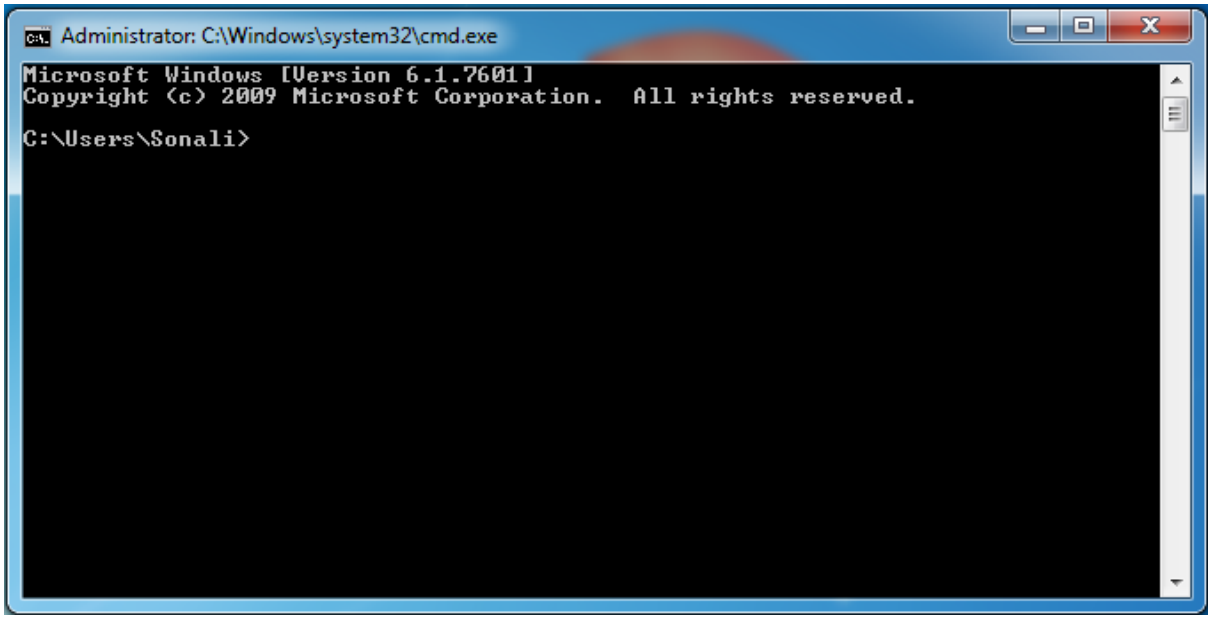
www.reddit.com	A	5 minutes	198.41.209.136 ()
www.reddit.com	A	5 minutes	198.41.208.141 ()
www.reddit.com	A	5 minutes	198.41.209.143 ()
www.reddit.com	A	5 minutes	198.41.208.140 ()
www.reddit.com	A	5 minutes	198.41.209.142 ()
www.reddit.com	A	5 minutes	198.41.208.143 ()
www.reddit.com	A	5 minutes	198.41.208.138 ()
www.reddit.com	A	5 minutes	198.41.209.141 ()
www.reddit.com	A	5 minutes	198.41.209.139 ()
www.reddit.com	A	5 minutes	198.41.209.137 ()

Step 7: Show you information about reddit.com in diagnosis tab.



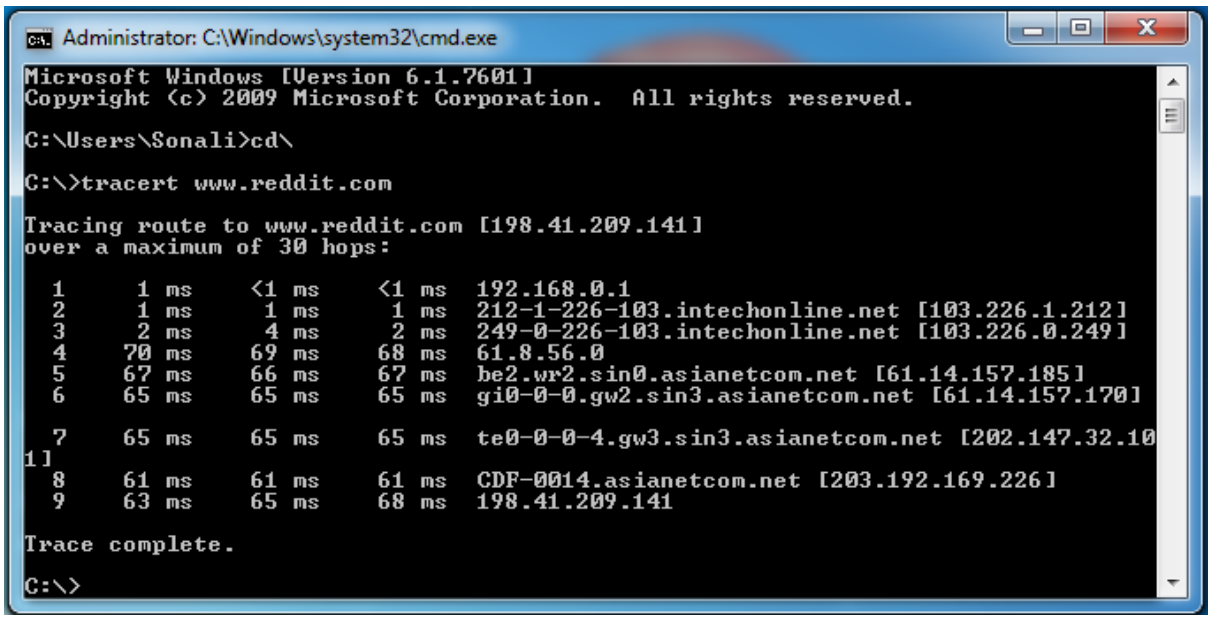
USING TRACE ROUTE

Step 1: Open cmd prompt.

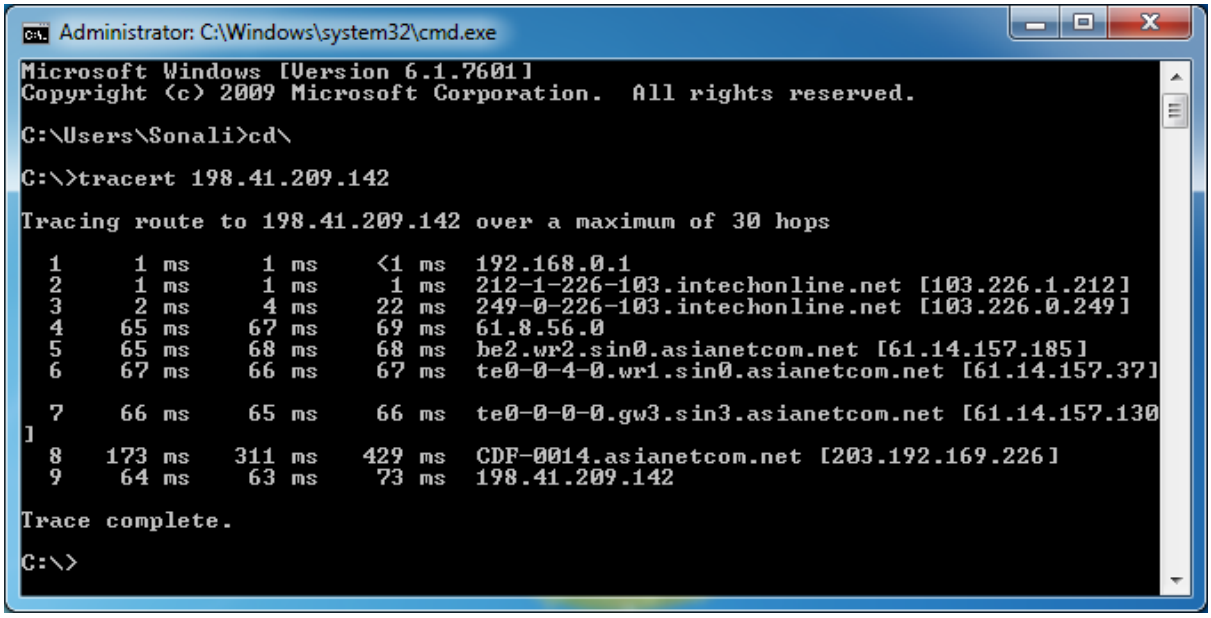


Step 2: Type cd\ and enter it will redirect to “C/directory”.

Step 3: Type tracert command and type www.reddit.com and press “Enter”.

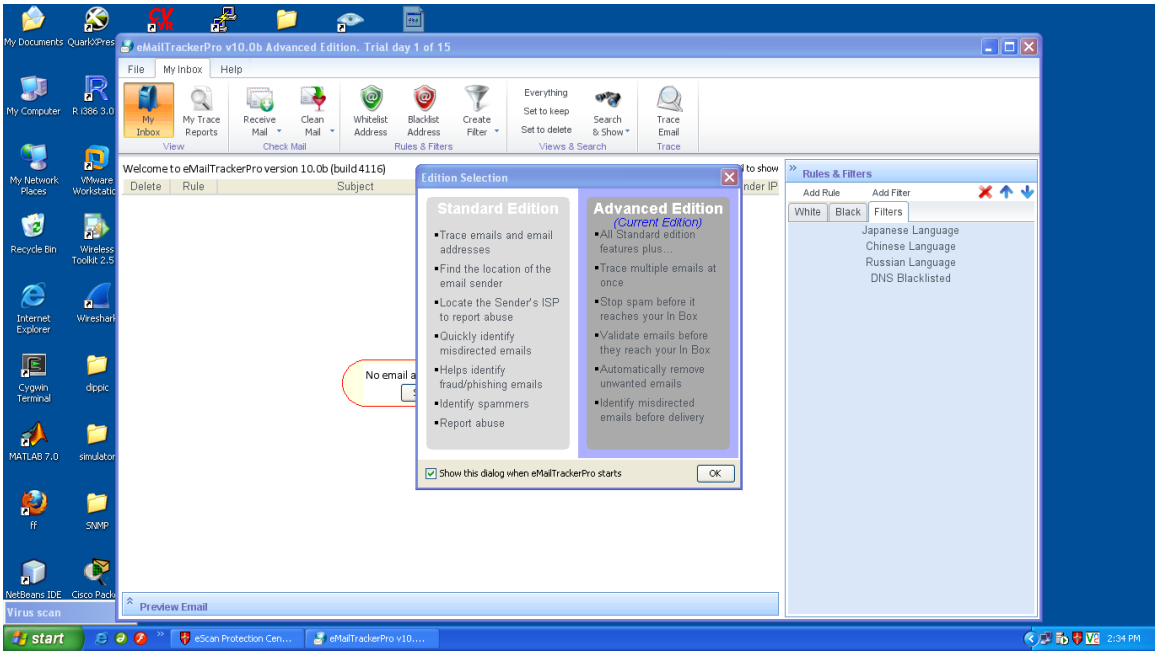


Step 4: Type tracert command and type ipaddress of reddit.com and press “Enter”.

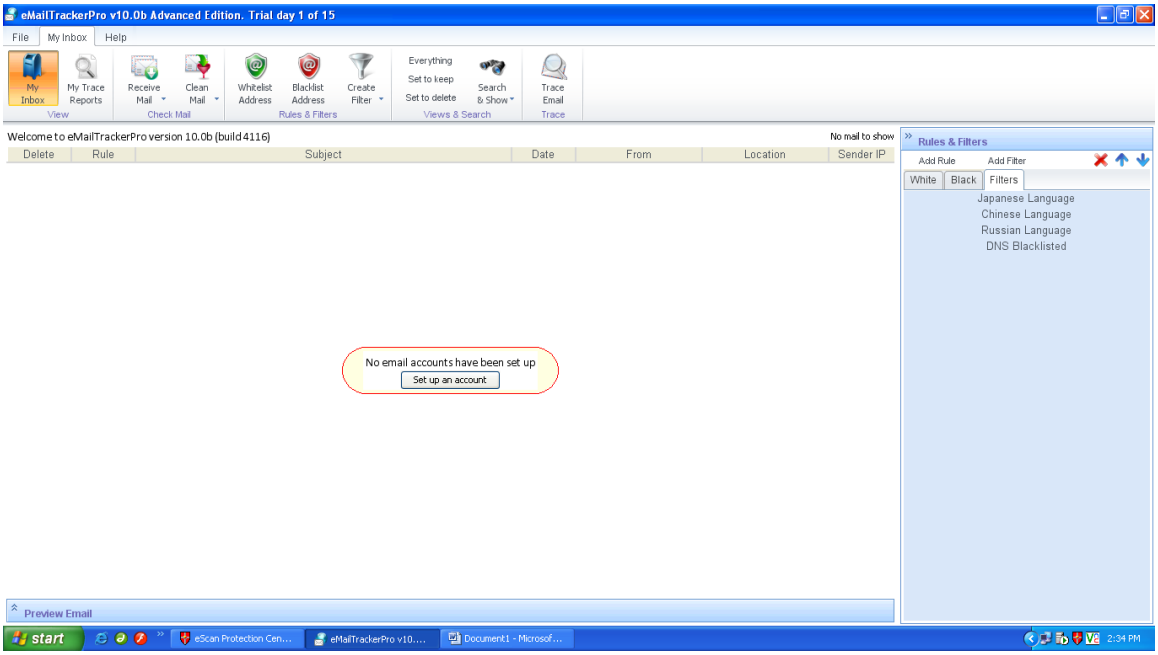


USING EMAIL TRACKER

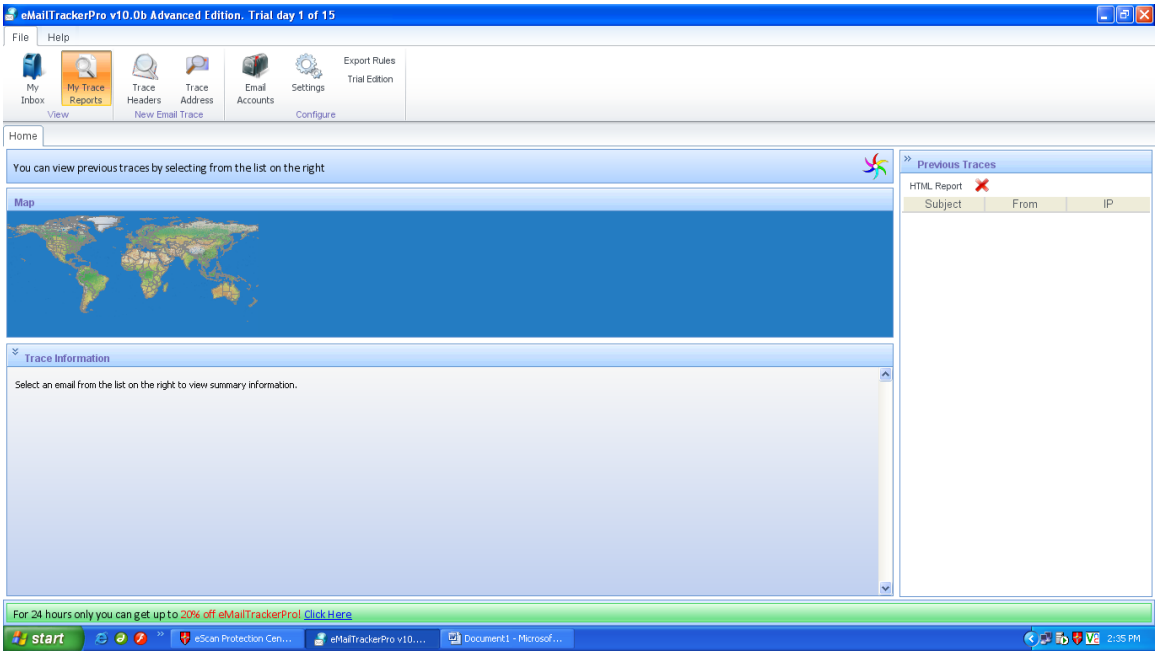
Step 1: Open emailTracker.



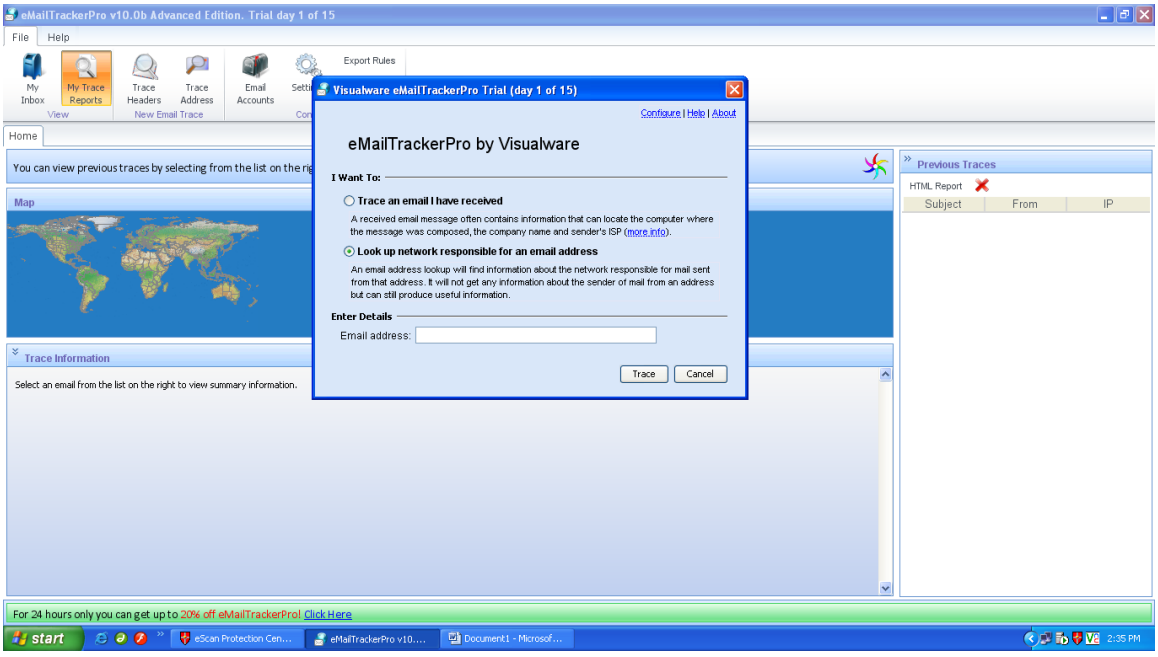
Step 2: Check if there are any reports generated previously.



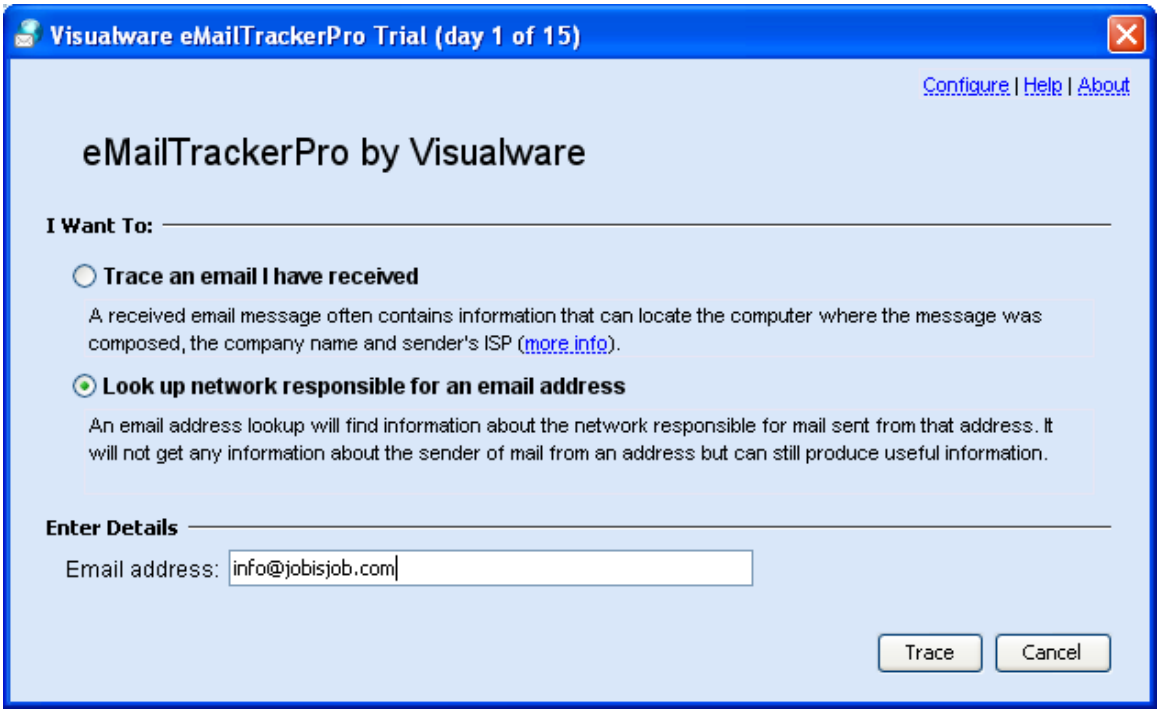
Step 3: Check for My trace Reports.



Step 4: Click on Trace address, a new window will open.



Step 5: Click on second option and enter email address you want to trace and click on trace button.



Step 6: The eMailTracker will search for the location and information about the email address entered.

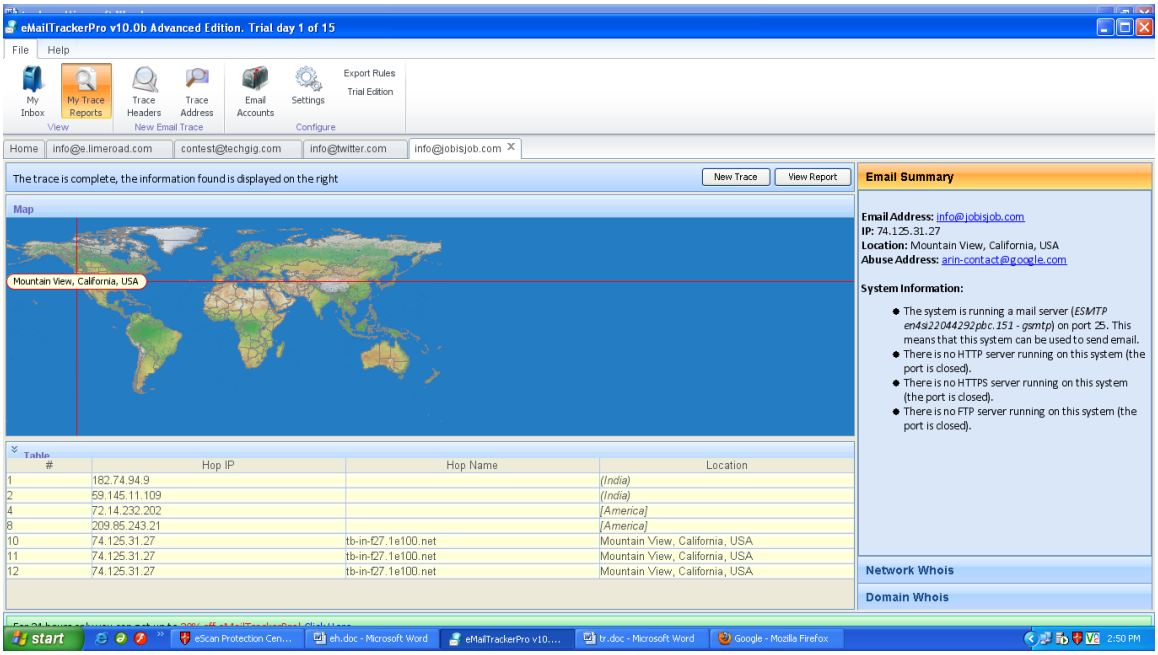


Figure: Location details and email summary.

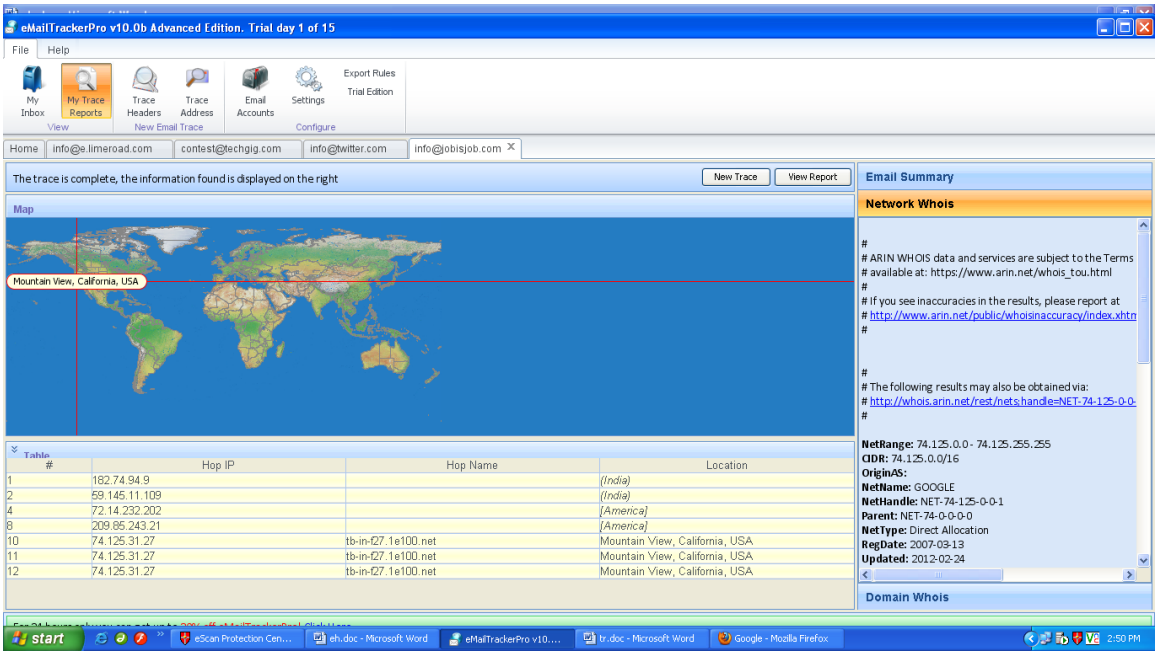


Figure: Location details and network summary.

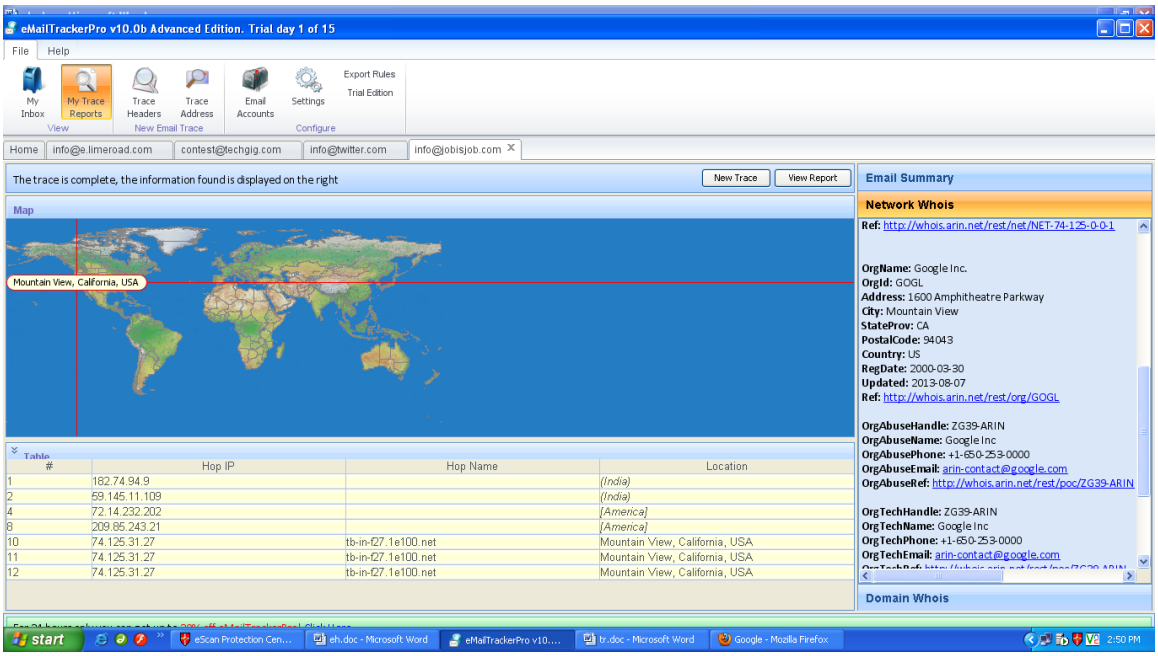


Figure: Location details and network summary.

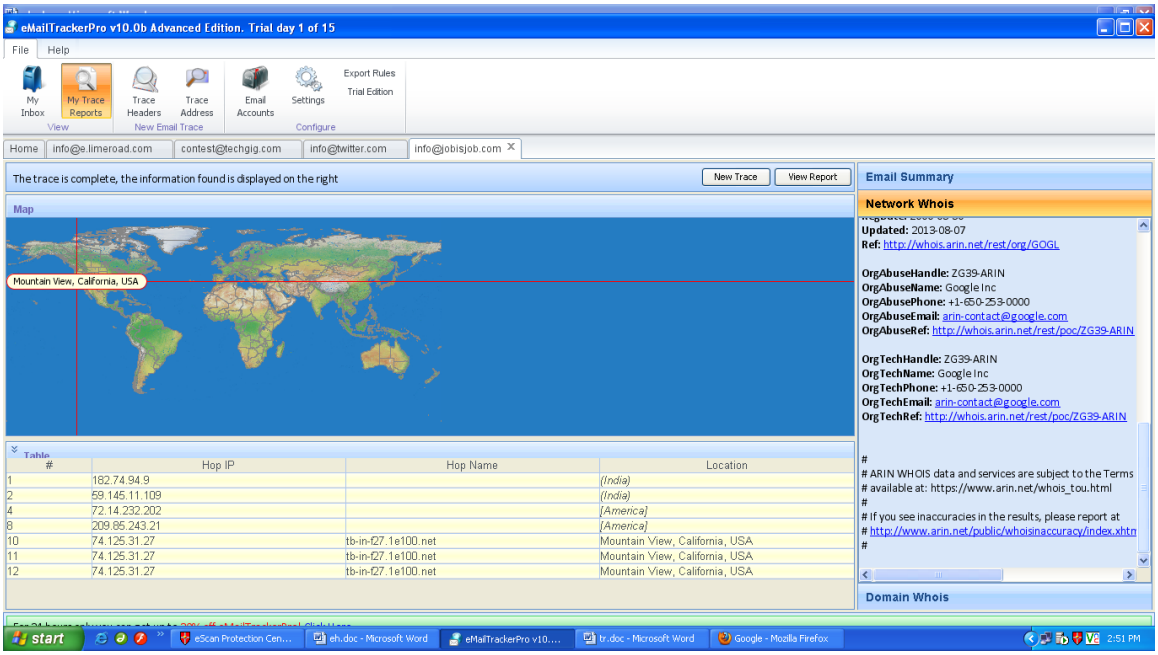


Figure: Location details and network summary.

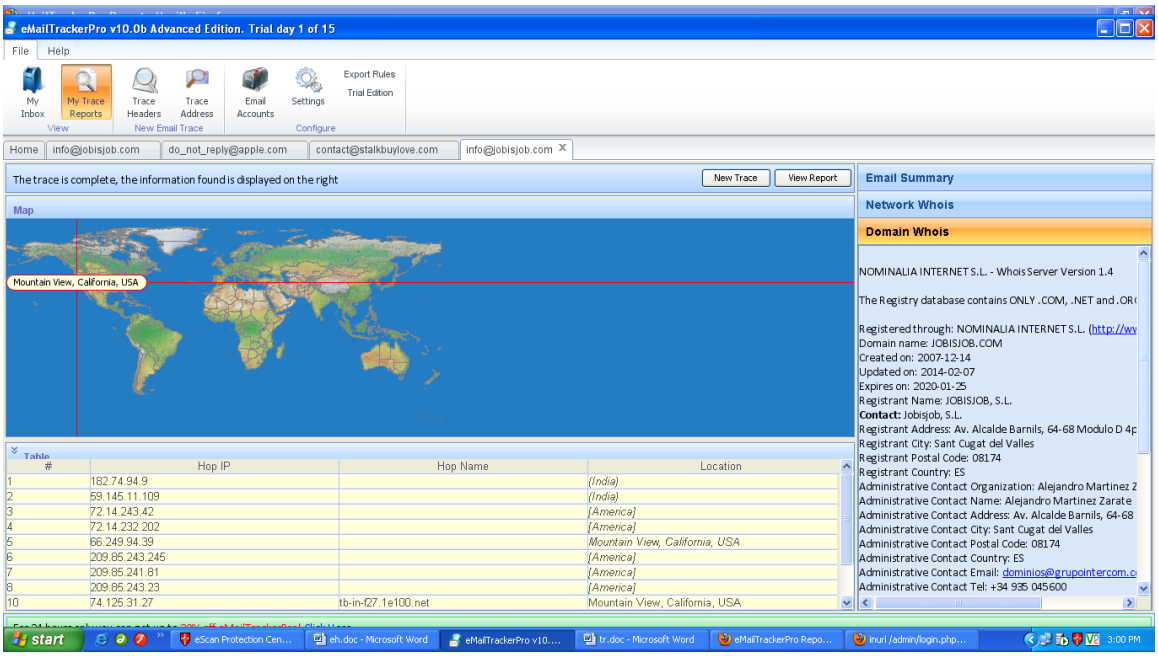


Figure: Location details and domain summary.

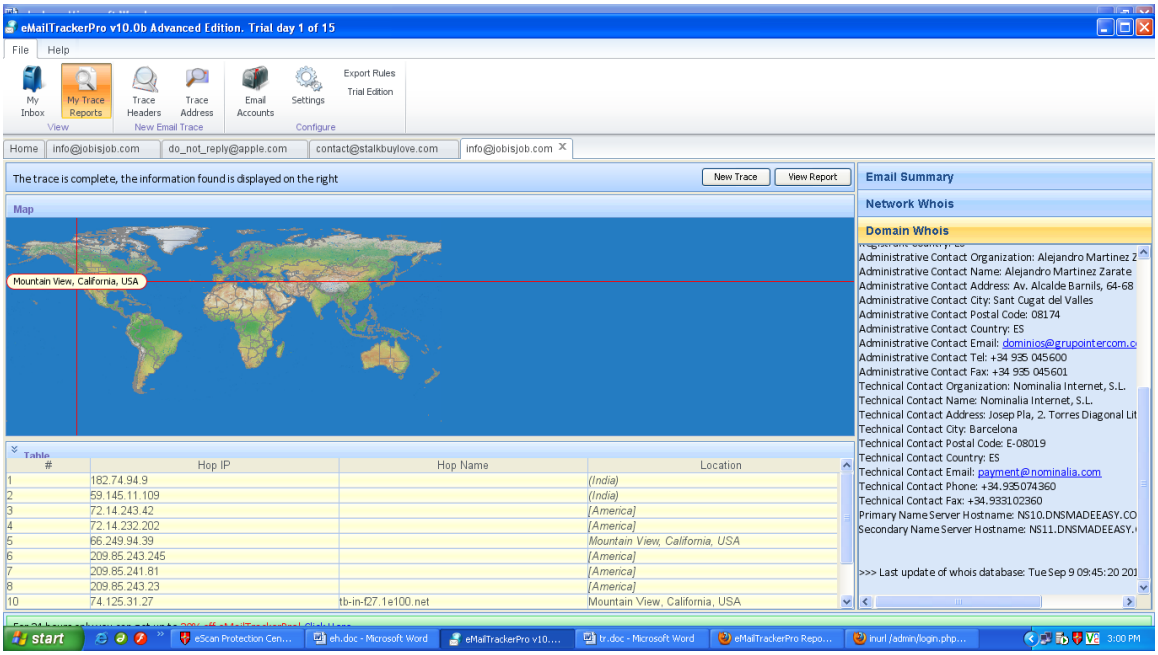
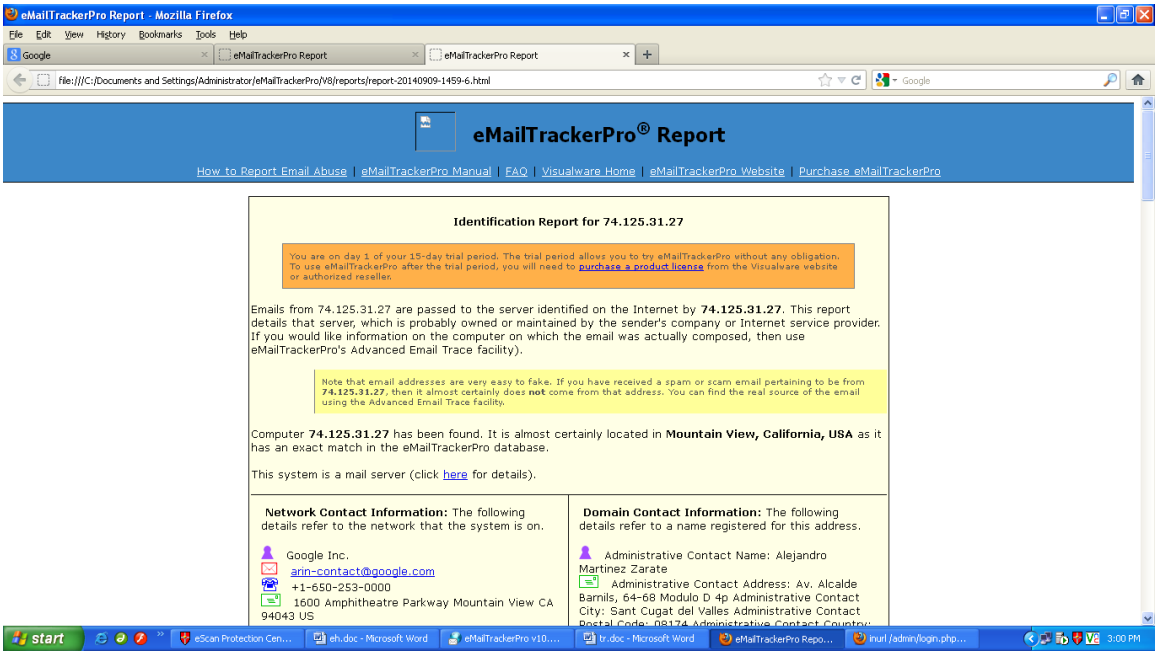
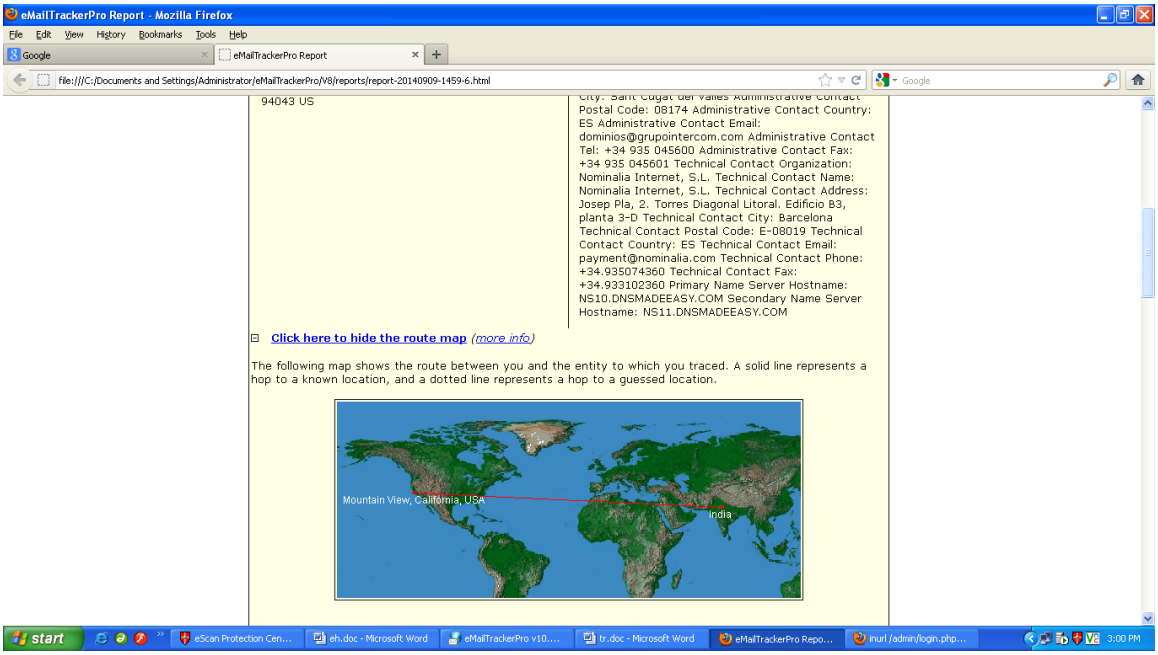
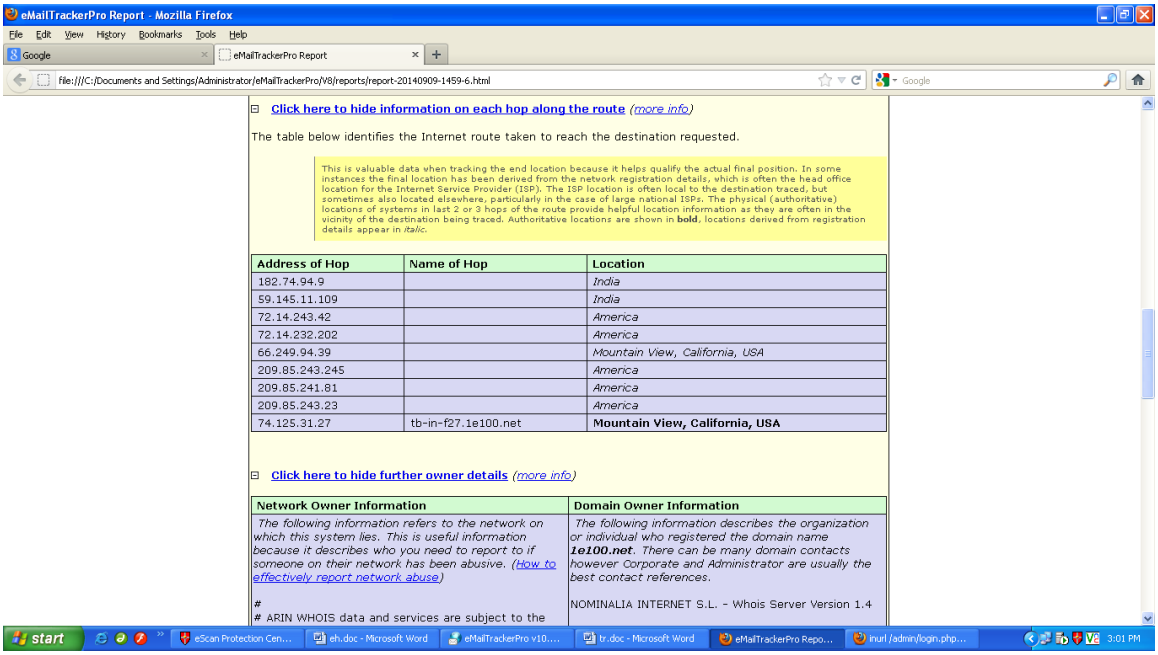


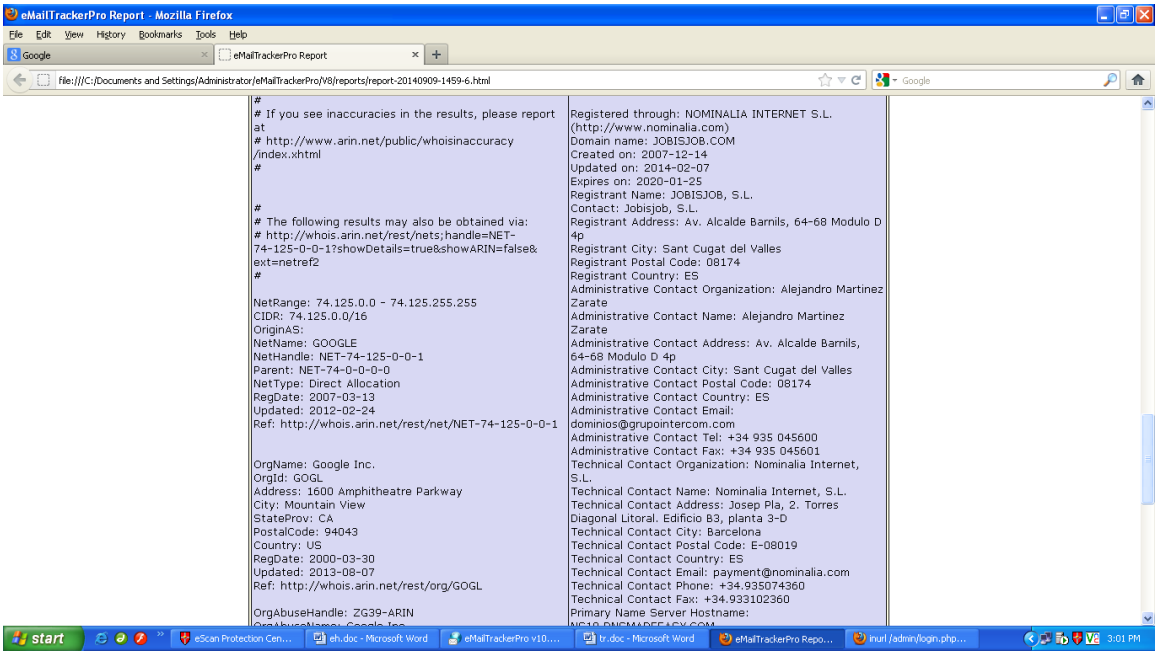
Figure: Location details and domain summary.

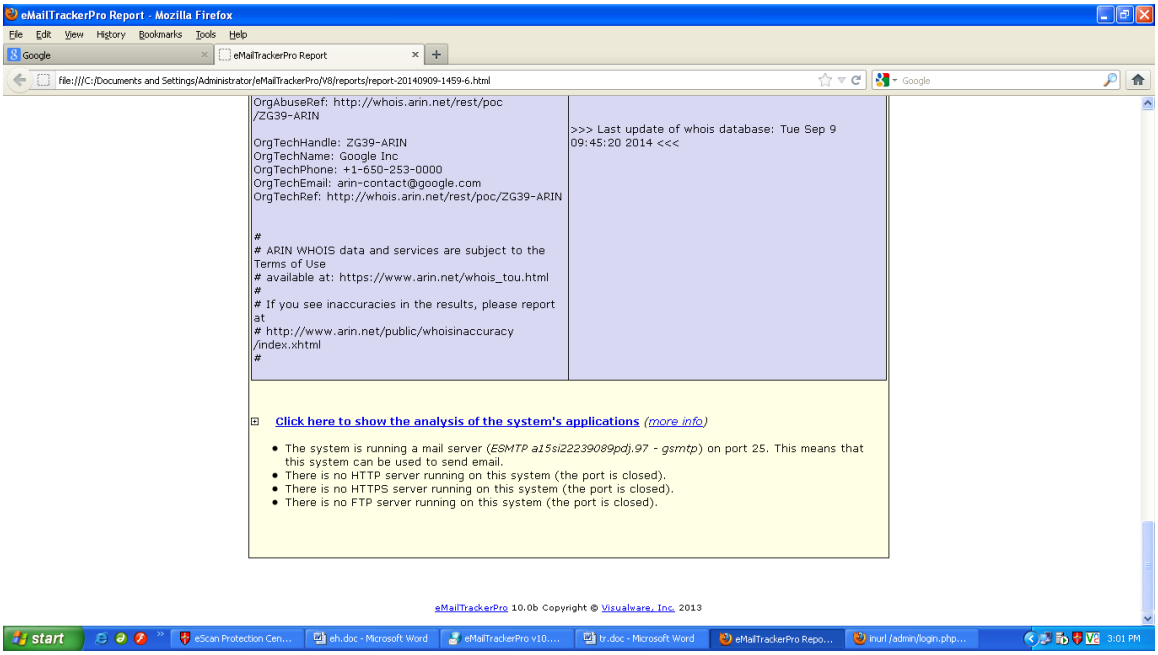
Step 7: Now click on View report and the following report will be generated in browser.




eMailTrackerPro Report - Mozilla Firefox
File Edit View History Bookmarks Tools Help
eMailTrackerPro Report
file:///C:/Documents and Settings/Administrator/eMailTrackerPro/V8/reports/report-20140909-1459-6.html
94043 US
Postal Code: 08174 Administrative Contact Country: ES Administrative Contact Email: dominios@grupointercom.com Administrative Contact Tel: +34 935 045600 Administrative Contact Fax: +34 935 045601 Technical Contact Organization: Nominalia Internet, S.L. Technical Contact Name: Nominalia Internet, S.L. Technical Contact Address: Josep Pla, 2. Torres Diagonal Litoral. Edificio B3, planta 3-D Technical Contact City: Barcelona Technical Contact Postal Code: E-08019 Technical Contact Country: ES Technical Contact Email: payment@nominalia.com Technical Contact Phone: +34.935074360 Technical Contact Fax: +34.933102360 Primary Name Server Hostname: NS10.DNSMADEEASY.COM Secondary Name Server Hostname: NS11.DNSMADEEASY.COM
Click here to hide the route map (more info)
The following map shows the route between you and the entity to which you traced. A solid line represents a hop to a known location, and a dotted line represents a hop to a guessed location.
Mountain View, California, USA
India
start
3:00 PM


eMailTrackerPro Report - Mozilla Firefox
File Edit View History Bookmarks Tools Help
eMailTrackerPro Report
file:///C:/Documents and Settings/Administrator/eMailTrackerPro/V8/reports/report-20140909-1459-6.html
Click here to hide information on each hop along the route (more info)
The table below identifies the Internet route taken to reach the destination requested.
This is valuable data when tracking the end location because it helps qualify the actual final position. In some instances the final location has been derived from the network registration details, which is often the head office location for the Internet Service Provider (ISP). The ISP location is often local to the destination traced, but sometimes also located elsewhere, particularly in the case of large national ISPs. The physical (authoritative) locations of systems in last 2 or 3 hops of the route provide helpful location information as they are often in the vicinity of the destination being traced. Authoritative locations are shown in bold, locations derived from registration details appear in italic.
Address of Hop | Name of Hop | Location
182.74.94.9 | | India
59.145.11.109 | | India
72.14.243.42 | | America
72.14.232.202 | | America
66.249.94.39 | | Mountain View, California, USA
209.85.243.245 | | America
209.85.241.81 | | America
209.85.243.23 | | America
74.125.31.27 | tb-in-f27.1e100.net | Mountain View, California, USA
Click here to hide further owner details (more info)
Network Owner Information
The following information refers to the network on which this system lies. This is useful information because it describes who you need to report to if someone on their network has been abusive. (How to effectively report network abuse)
#
ARIN WHOIS data and services are subject to the
Domain Owner Information
The following information describes the organization or individual who registered the domain name 1e100.net. There can be many domain contacts however Corporate and Administrator are usually the best contact references.
NOMINALIA INTERNET S.L. - Whois Server Version 1.4
start
3:01 PM

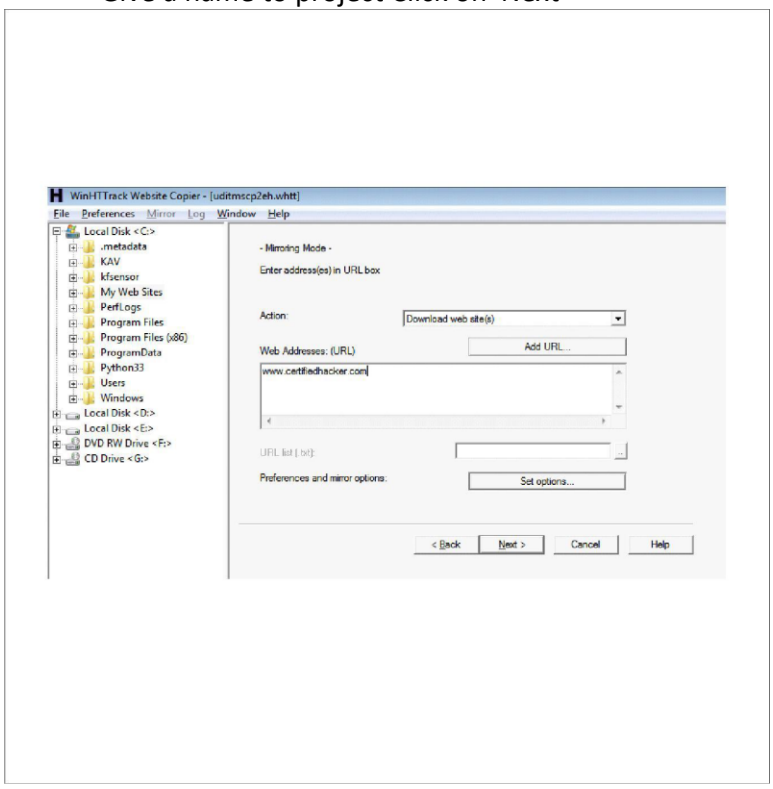

eMailTrackerPro Report - Mozilla Firefox
File Edit View History Bookmarks Tools Help
eMailTrackerPro Report
file:///C:/Documents and Settings/Administrator/eMailTrackerPro/V8/reports/report-20140909-1459-6.html
#
If you see inaccuracies in the results, please report at
http://www.arin.net/public/whoisinaccuracy/index.xhtml
#
#
The following results may also be obtained via:
http://whois.arin.net/rest/nets;handle=NET-74-125-0-0-1?showDetails=true&showARIN=false&ext=netref2
#
NetRange: 74.125.0.0 - 74.125.255.255
CIDR: 74.125.0.0/16
OriginAS:
NetName: GOOGLE
NetHandle: NET-74-125-0-0-1
Parent: NET-74-0-0-0-0
NetType: Direct Allocation
RegDate: 2007-03-13
Updated: 2012-02-24
Ref: http://whois.arin.net/rest/net/NET-74-125-0-0-1
OrgName: Google Inc.
OrgId: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View
StateProv: CA
PostalCode: 94043
Country: US
RegDate: 2000-03-30
Updated: 2013-08-07
Ref: http://whois.arin.net/rest/org/GOGL
OrgAbuseHandle: ZG39-ARIN
Registered through: NOMINALIA INTERNET S.L. (http://www.nominalia.com)
Domain name: JOBISJOB.COM
Created on: 2007-12-14
Updated on: 2014-02-07
Expires on: 2020-01-25
Registrant Name: JOBISJOB, S.L.
Contact: Jobisjob, S.L.
Registrant Address: Av. Alcalde Barnils, 64-68 Modulo D 4p
Registrant City: Sant Cugat del Valles
Registrant Postal Code: 08174
Registrant Country: ES
Administrative Contact Organization: Alejandro Martinez Zarate
Administrative Contact Name: Alejandro Martinez Zarate
Administrative Contact Address: Av. Alcalde Barnils, 64-68 Modulo D 4p
Administrative Contact City: Sant Cugat del Valles
Administrative Contact Postal Code: 08174
Administrative Contact Country: ES
Administrative Contact Email: dominios@grupointercom.com
Administrative Contact Tel: +34 935 045600
Administrative Contact Fax: +34 935 045601
Technical Contact Organization: Nominalia Internet, S.L.
Technical Contact Name: Nominalia Internet, S.L.
Technical Contact Address: Josep Pla, 2. Torres Diagonal Litoral. Edificio B3, planta 3-D
Technical Contact City: Barcelona
Technical Contact Postal Code: E-08019
Technical Contact Country: ES
Technical Contact Email: payment@nominalia.com
Technical Contact Phone: +34.935074360
Technical Contact Fax: +34.933102360
Primary Name Server Hostname:
start
eScan Protection Cen...
eh.doc - Microsoft Word
eMailTrackerPro v10....
tr.doc - Microsoft Word
eMailTrackerPro Repo...
inurl /admin/login.php...
3:01 PM


eMailTrackerPro Report - Mozilla Firefox
File Edit View History Bookmarks Tools Help
eMailTrackerPro Report
file:///C:/Documents and Settings/Administrator/eMailTrackerPro/V8/reports/report-20140909-1459-6.html
OrgAbuseRef: http://whois.arin.net/rest/poc/ZG39-ARIN
OrgTechHandle: ZG39-ARIN
OrgTechName: Google Inc
OrgTechPhone: +1-650-253-0000
OrgTechEmail: arin-contact@google.com
OrgTechRef: http://whois.arin.net/rest/poc/ZG39-ARIN
#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/whois_tou.html
#
If you see inaccuracies in the results, please report at
http://www.arin.net/public/whoisinaccuracy/index.xhtml
#
>>> Last update of whois database: Tue Sep 9 09:45:20 2014 <<<
Click here to show the analysis of the system's applications (more info)
The system is running a mail server (ESMTP a15si2223908pdj.97 - gsmtp) on port 25. This means that this system can be used to send email.
There is no HTTP server running on this system (the port is closed).
There is no HTTPS server running on this system (the port is closed).
There is no FTP server running on this system (the port is closed).
eMailTrackerPro 10.0b Copyright © Visualware, Inc. 2013
start
eScan Protection Cen...
eh.doc - Microsoft Word
eMailTrackerPro v10....
tr.doc - Microsoft Word
eMailTrackerPro Repo...
inurl /admin/login.php...
3:01 PM

HTTrack Website Copier

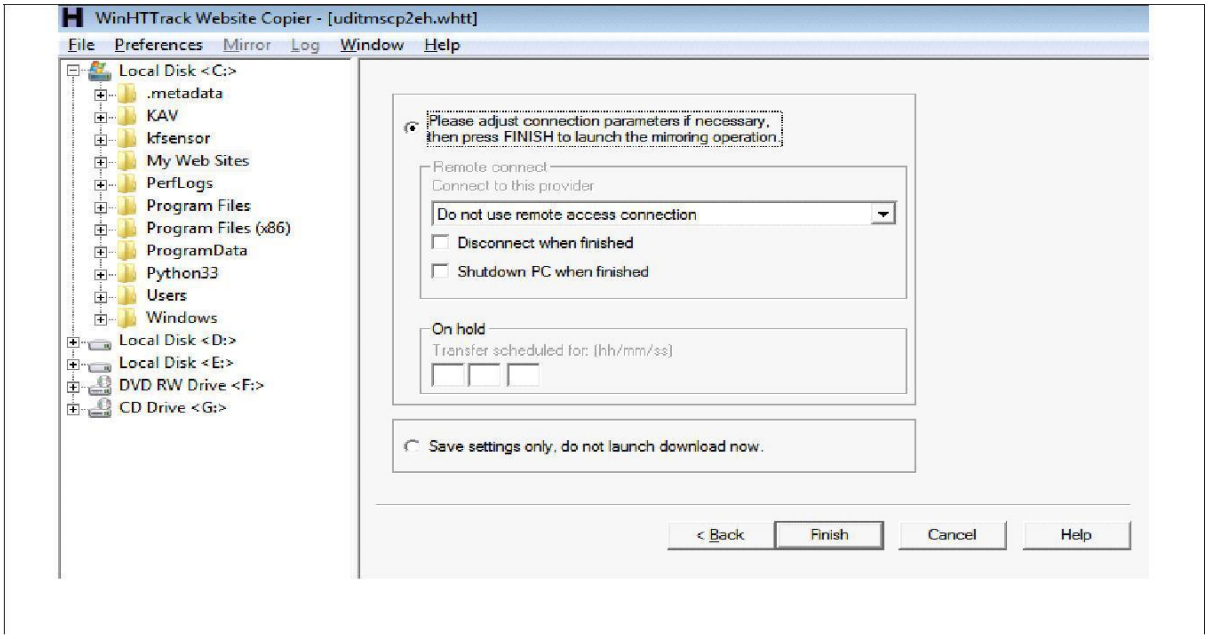
Start > Programs >

- HTTrack Website Copier
- Click on 'Next' to create Project
- Give a name to project Click on 'Next'

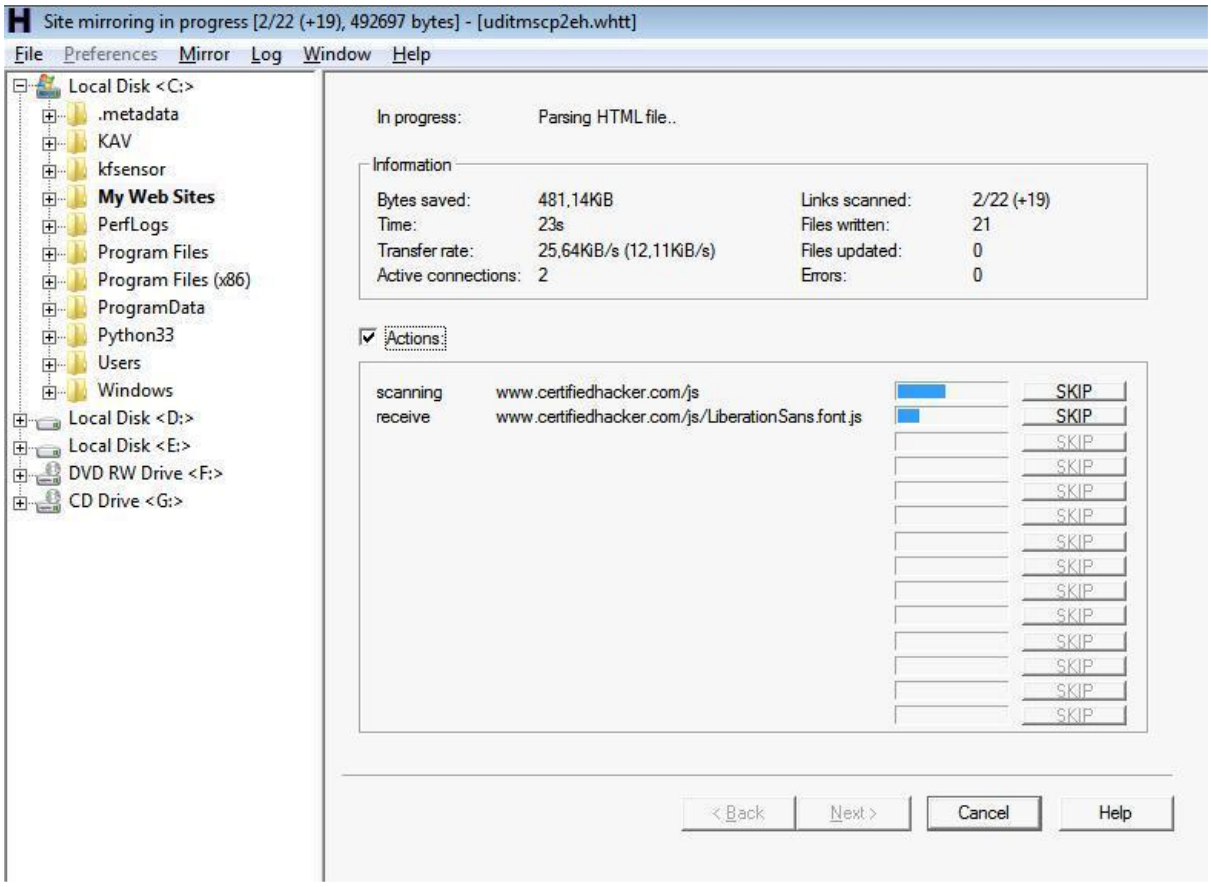


- Click on ‘Add URL’ and give the UR
- Any additional options that need t
- Then click 'Next'

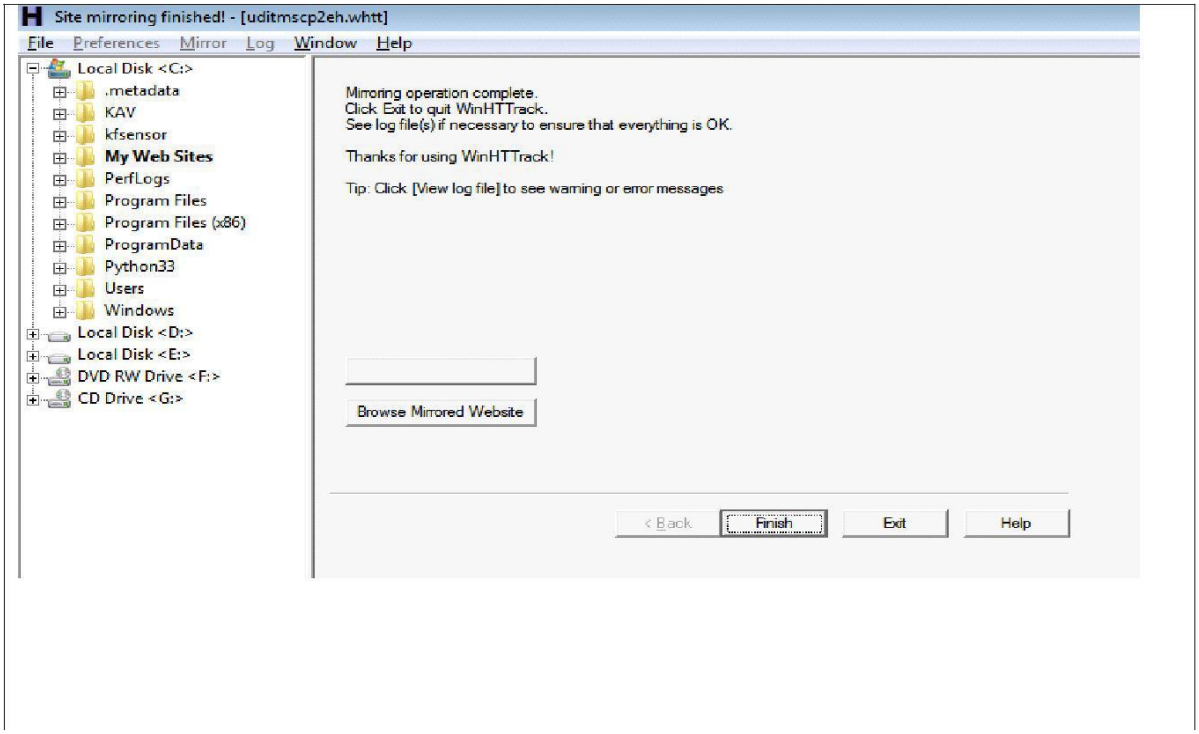
- By default, the radio button will be selected for Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation.



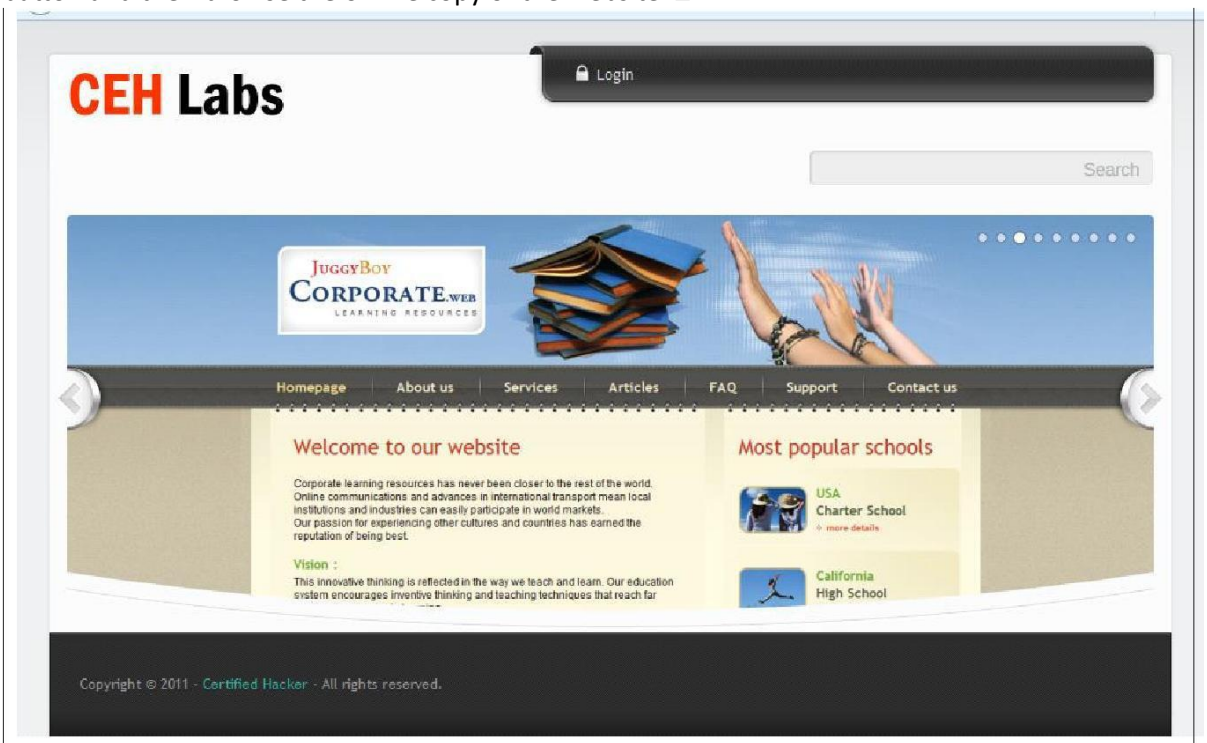
The mirroring of the site now begins. The site will be downloaded and be saved in the C:\My Web Sites\<Project Name>



 Process of mirroring the website.

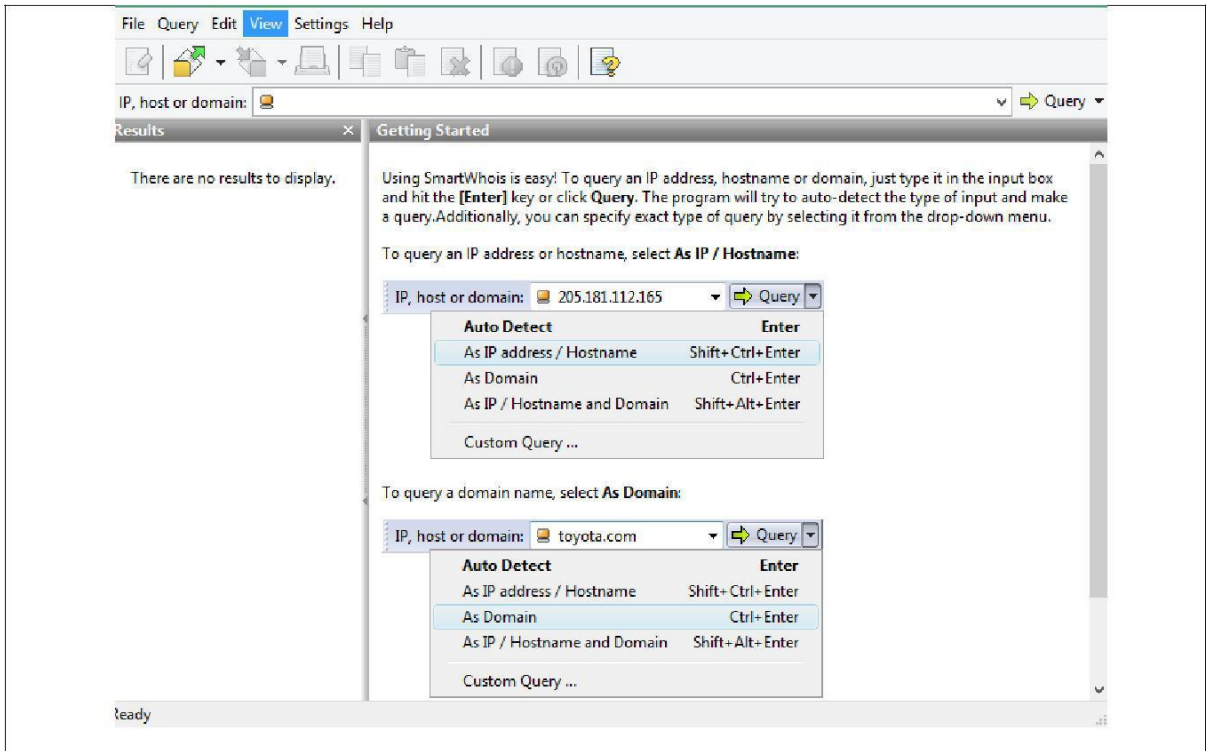


Once the Website Mirroring has been completed, you can click on the Browse Mirrored Website button and then browse the offline copy of the website.

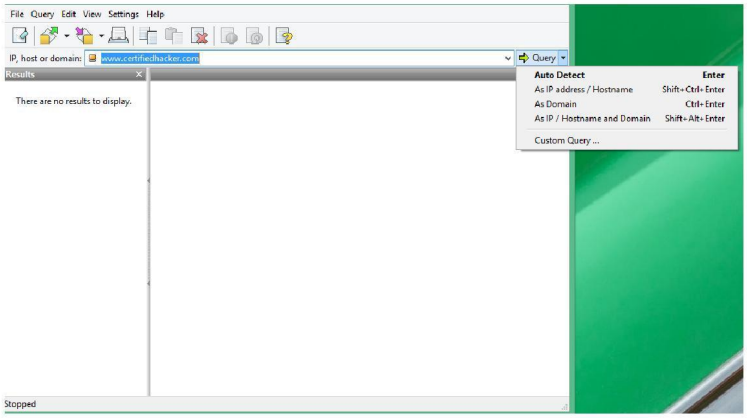


SmartWHOis

- SmartWHOis is used to perform WHOIS Footprinting against an entered IP Address or a Domain Name
- Run it from, Start > Programs > SmartWhois

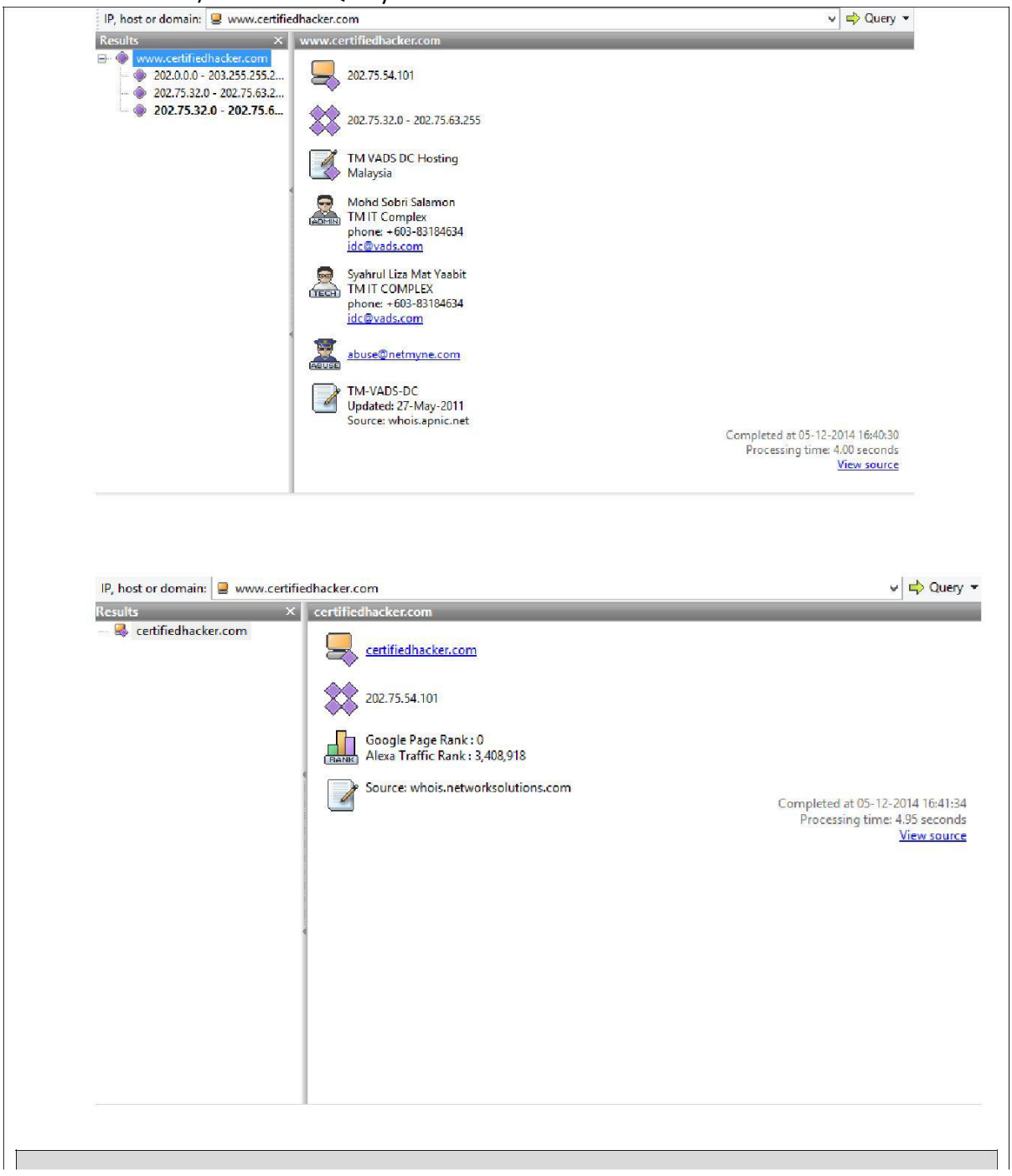


Type an IP address, hostname, or domain name in the address bar



- Different queries will return different results.

- IP Address / Hostname Query results



5. Ping

This practical is used to find out the MTU of the destination machine.

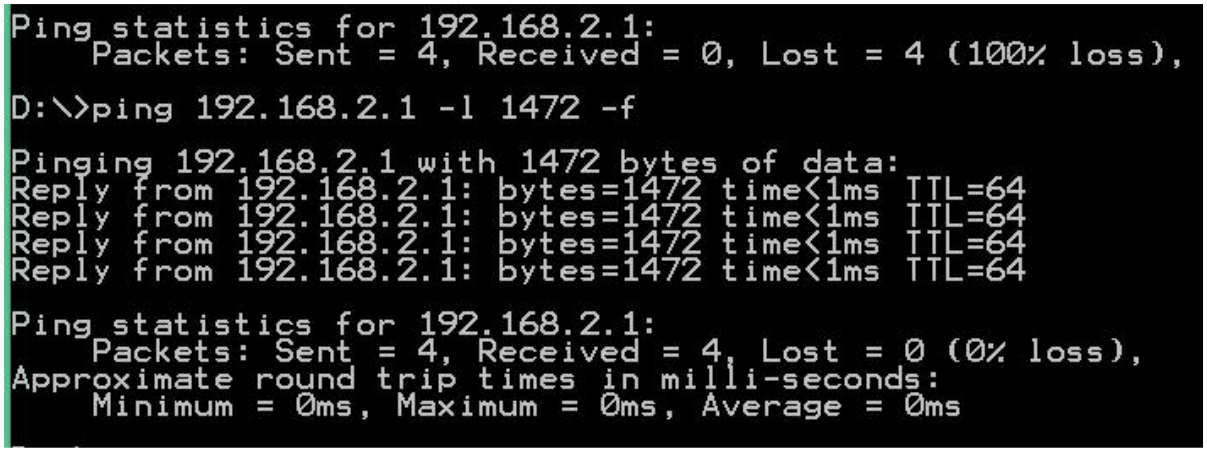
- We ping a computer using the ‘p
- To specify the data length in bytes we use –lswitch
- To specify that the packet should not be fragmented we use –f

```
D:\>ping 192.168.2.1 -l 1500 -n 1

Pinging 192.168.2.1 with 1500 bytes of data:
Reply from 192.168.2.1: bytes=1500 time<1ms TTL=64

Ping statistics for 192.168.2.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\>ping 192.168.2.1 -l 1500 -n 1 -f

Pinging 192.168.2.1 with 1500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 192.168.2.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
```

- We now have to adjust the –lvalue till we get a reply. The border where the reply is received is said to be its MTU

```
D:\>ping 192.168.2.1 -l 1478 -f

Pinging 192.168.2.1 with 1478 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

D:\>ping 192.168.2.1 -l 1474 -f

Pinging 192.168.2.1 with 1474 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- Response is received at –l1472, hence the MTU size is 1472 Bytes


Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
D:\>ping 192.168.2.1 -l 1472 -f
Pinging 192.168.2.1 with 1472 bytes of data:
Reply from 192.168.2.1: bytes=1472 time<1ms TTL=64
Reply from 192.168.2.1: bytes=1472 time<1ms TTL=64
Reply from 192.168.2.1: bytes=1472 time<1ms TTL=64
Reply from 192.168.2.1: bytes=1472 time<1ms TTL=64
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

TraceRoute using Ping

- We can perform traceroute by using the –n and –Iswitches.
- -n means number of replies to show and –Imeans obtain reply from the machine in the next hop
- Open command prompt
- Ping certifiedhacker.com –n 1 –I1

```
D:\>ping certifiedhacker.com -n 1 -i 1

Pinging certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 192.168.0.1: TTL expired in transit.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

- Above, the local router replies back.
- Keep on increasing the I value until the certiedhacker.com site directly replies to the ping.
- At each I value, the device in the route will reply back

```
D:\>ping certifiedhacker.com -n 1 -i 2

Pinging certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Request timed out.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

D:\>ping certifiedhacker.com -n 1 -i 3

Pinging certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Request timed out.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

D:\>ping certifiedhacker.com -n 1 -i 4

Pinging certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 121.241.80.6: TTL expired in transit.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

- At i=4, reply comes back from 121.241.80.6
- At i=14, the reply comes from the server hosting the certifiedhacker site

```
D:\>ping certifiedhacker.com -n 1 -i 14

Pinging certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 202.75.54.101: bytes=32 time=155ms TTL=114

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 155ms, Maximum = 155ms, Average = 155ms
```

Node	IP
1	192.168.0.1
2	219.91.185.1
3	203.187.223.1
4	121.241.80.6
5	172.17.169.202
6	Timed Out
7	180.87.12.53
8	180.87.12.2
9	180.87.112.1
10	116.0.67.174
11	10.55.208.148
12	1.9.244.26
13	Timed Out
14	202.75.54.101 (Destination)

NSLookup

- NSLookup is used to perform DNS Foorprinting by using the windows command **nslookup**
- When we type nslookup, it shows us our current DNS Server

```
D:\>nslookup
Default Server:  UnKnown
Address:  192.168.0.1
```

- To specify the DNS query type we want, we use the command
  set type = <recordname> followed by the website name on the next line
  Set type = mx Certifiedhacker.com

```
> set type=mx
> certifiedhacker.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
certifiedhacker.com     MX preference = 10, mail exchanger = mail.certifiedhacke
r.com
```

- We can set the **query type** as A, ANY, CNAME, MX, NS, PTR, SOA, SRV
  A Record

```
> set type=a
> certifiedhacker.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    certifiedhacker.com
Address:  202.75.54.101
```

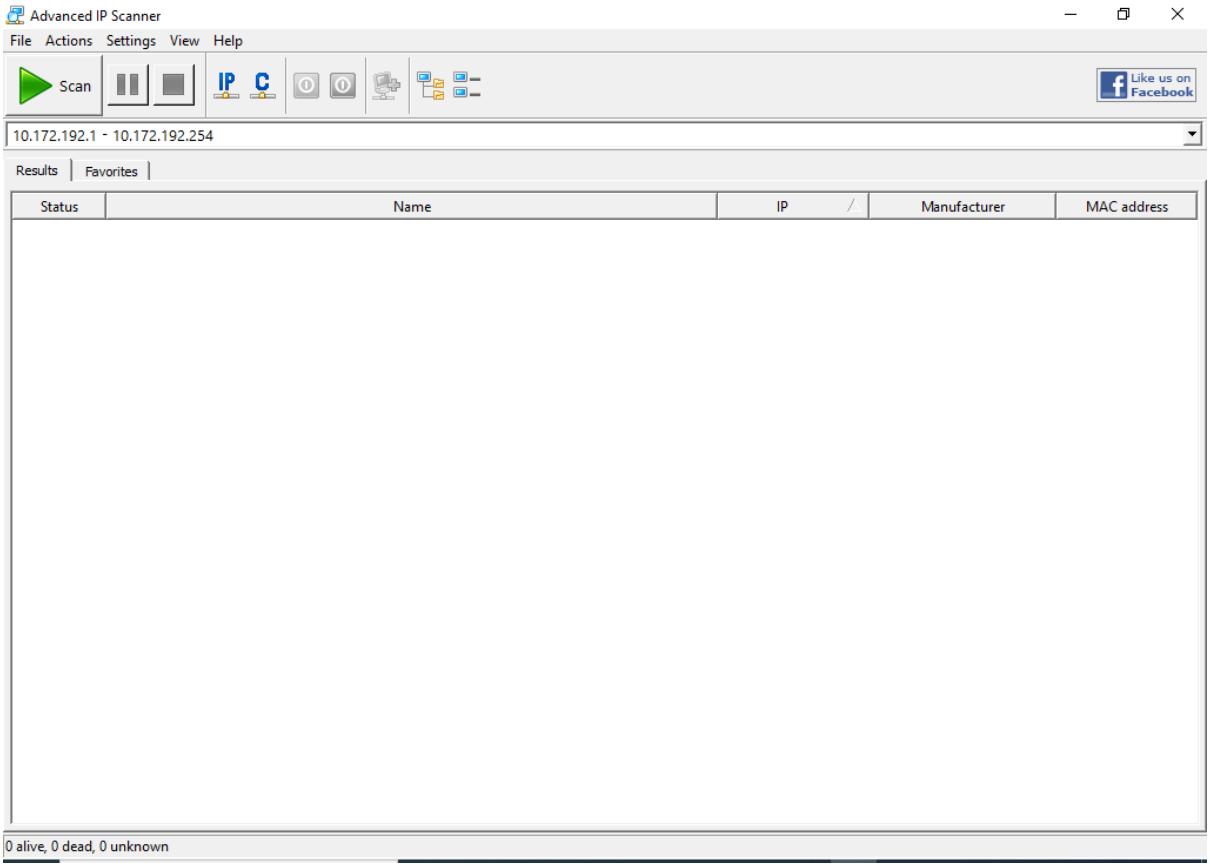
SOA Record

```
> set type=soa
> certifiedhacker.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
certifiedhacker.com
        primary name server = ns3.noyearlyfees.com
        responsible mail addr = hostmaster.noyearlyfees.com
        serial  = 10
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
```

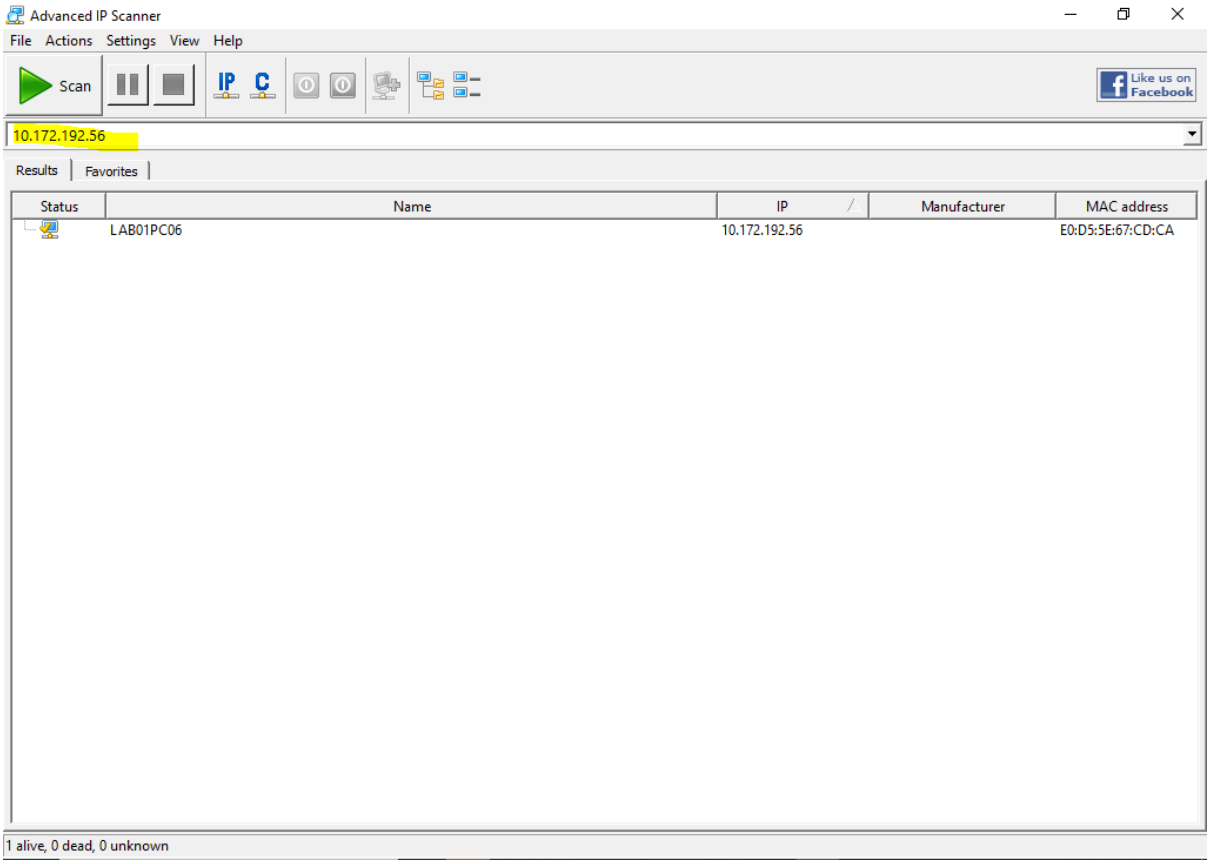
NameServer (NS) Record

```
> set type=ns
> certifiedhacker.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
certifiedhacker.com     nameserver = ns3.noyearlyfees.com
certifiedhacker.com     nameserver = ns0.noyearlyfees.com
```

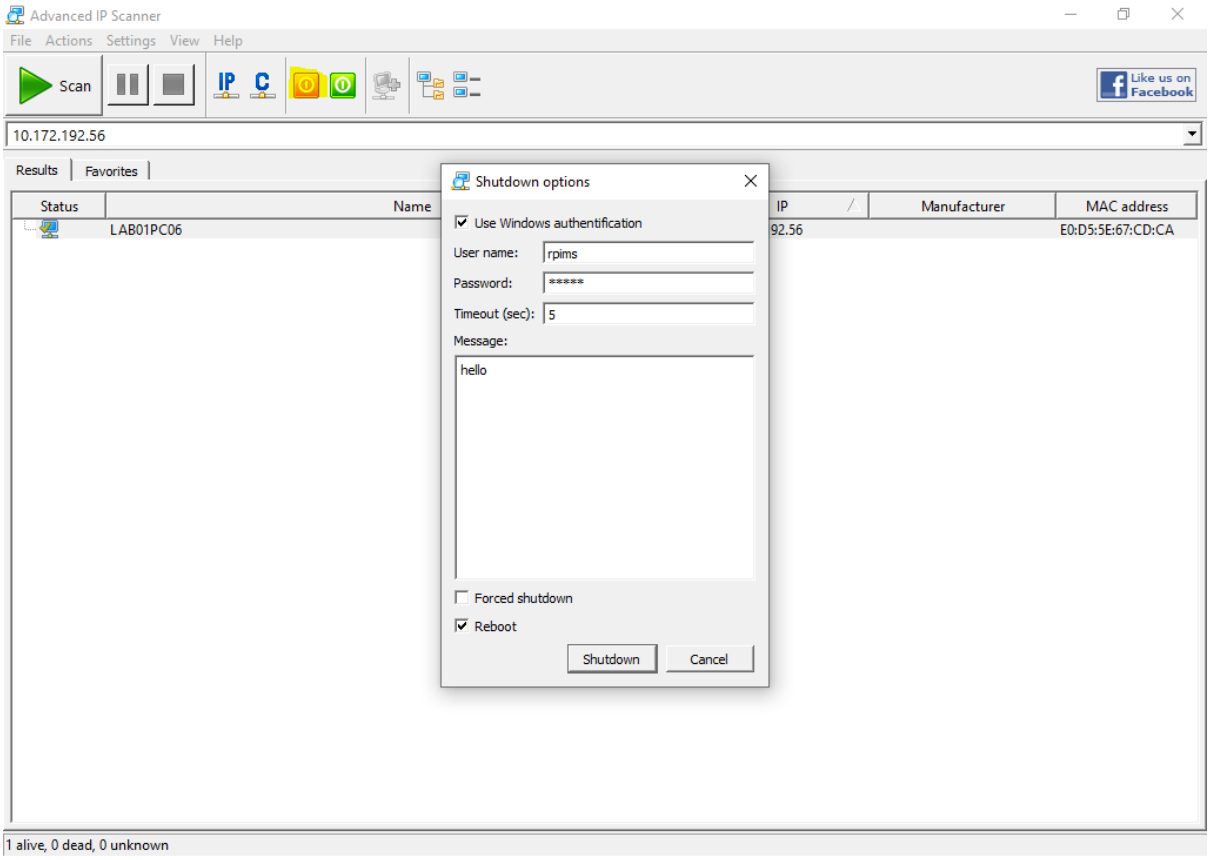
Advance ip scanner:



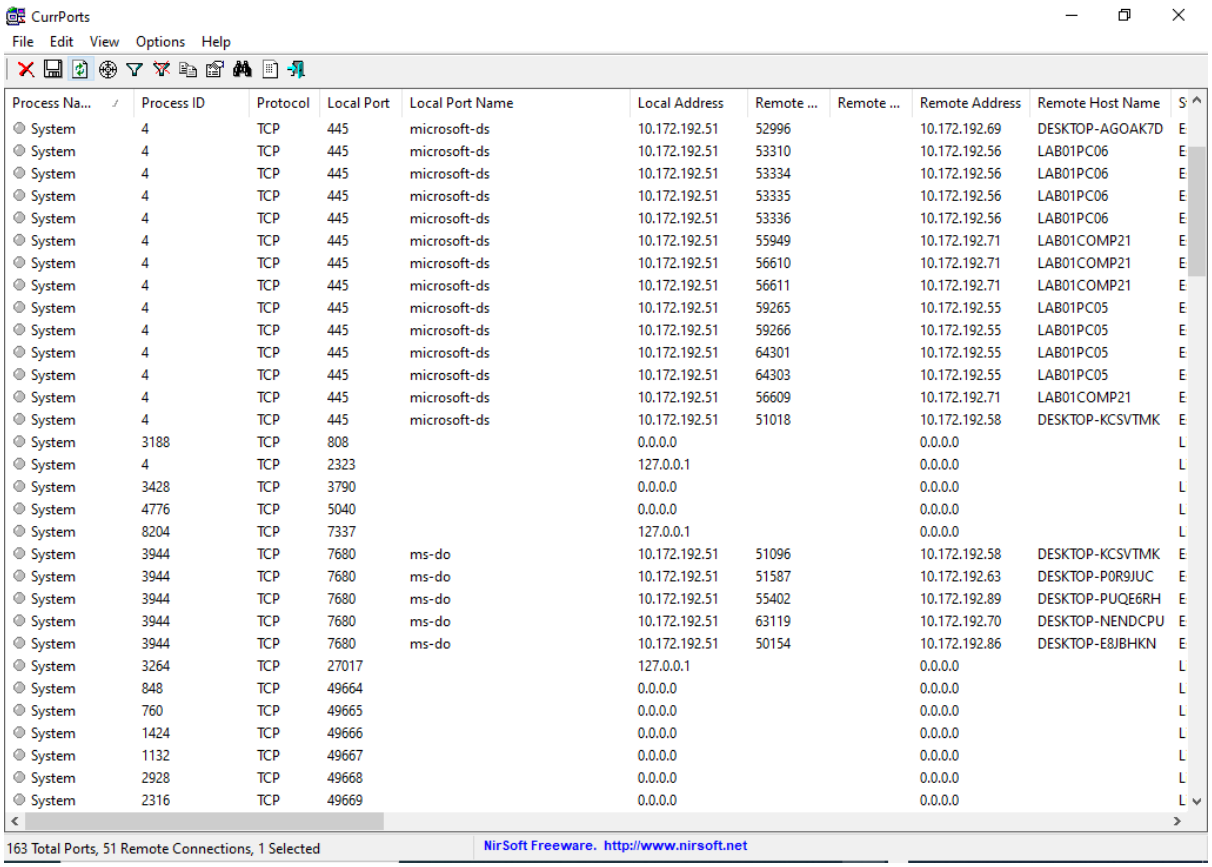
Insert ihte desired ip to be scan:



The clisk o the turnoff icon to shutdown the system:



CurrPorts:



Print the repot form _> view then HTML Report-All Items