نهمين سمينار آموزشي شبكه علمي غرب آسيا

آشنايي با برخي ابزارها و روش هاي هک و جاسوسي الکترونيک و نحوه مقابله با آن

بخش پنجم

ارائه دهنده : حيدرعلي کورنگي

www.newtechnology.ir
www.itseminar.ir
koorangi@newtechnology.ir

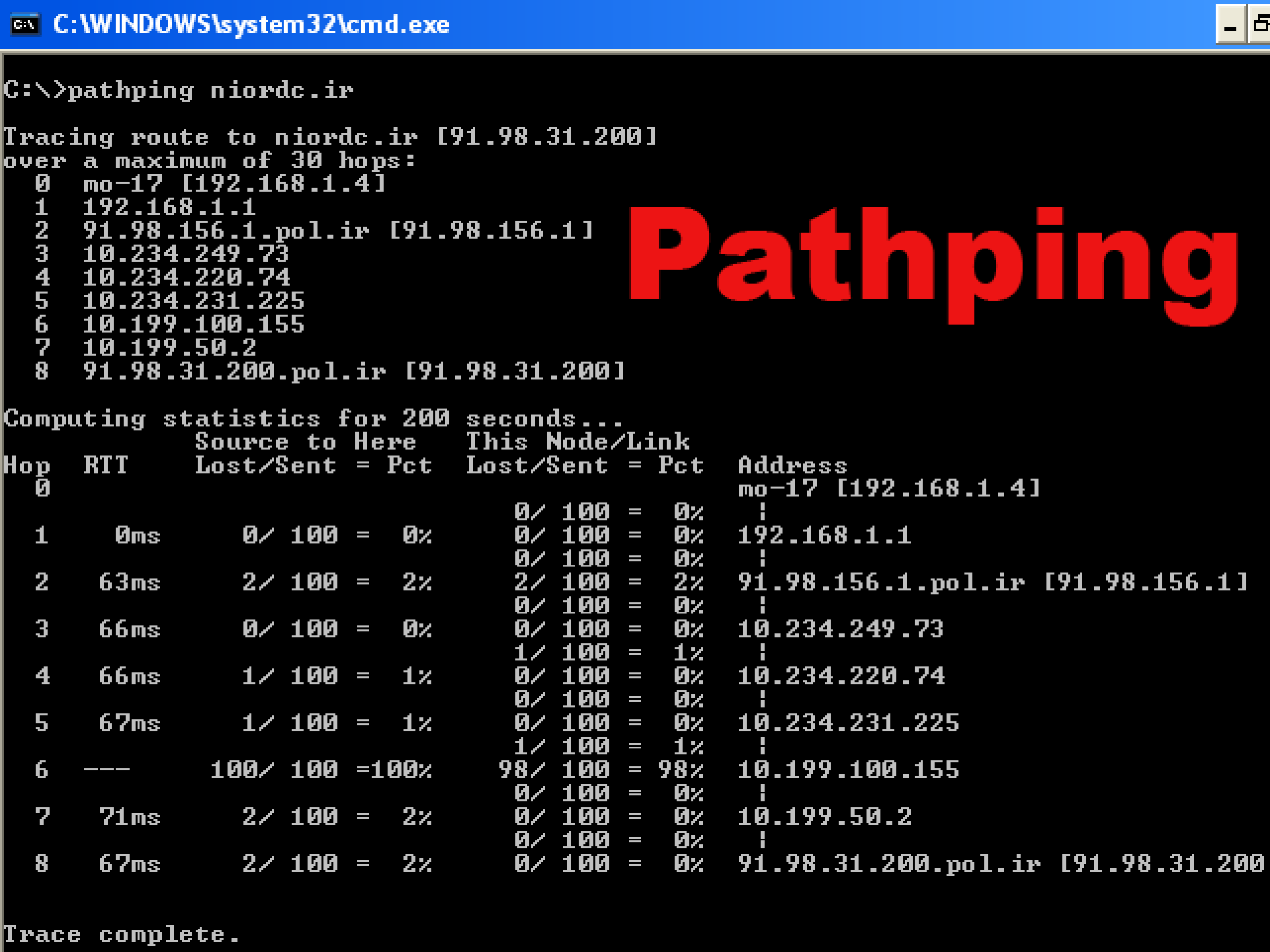
www.newtechnology.ir

آشنايي با برخي دستورات

پرکاربرد در خط فرمان

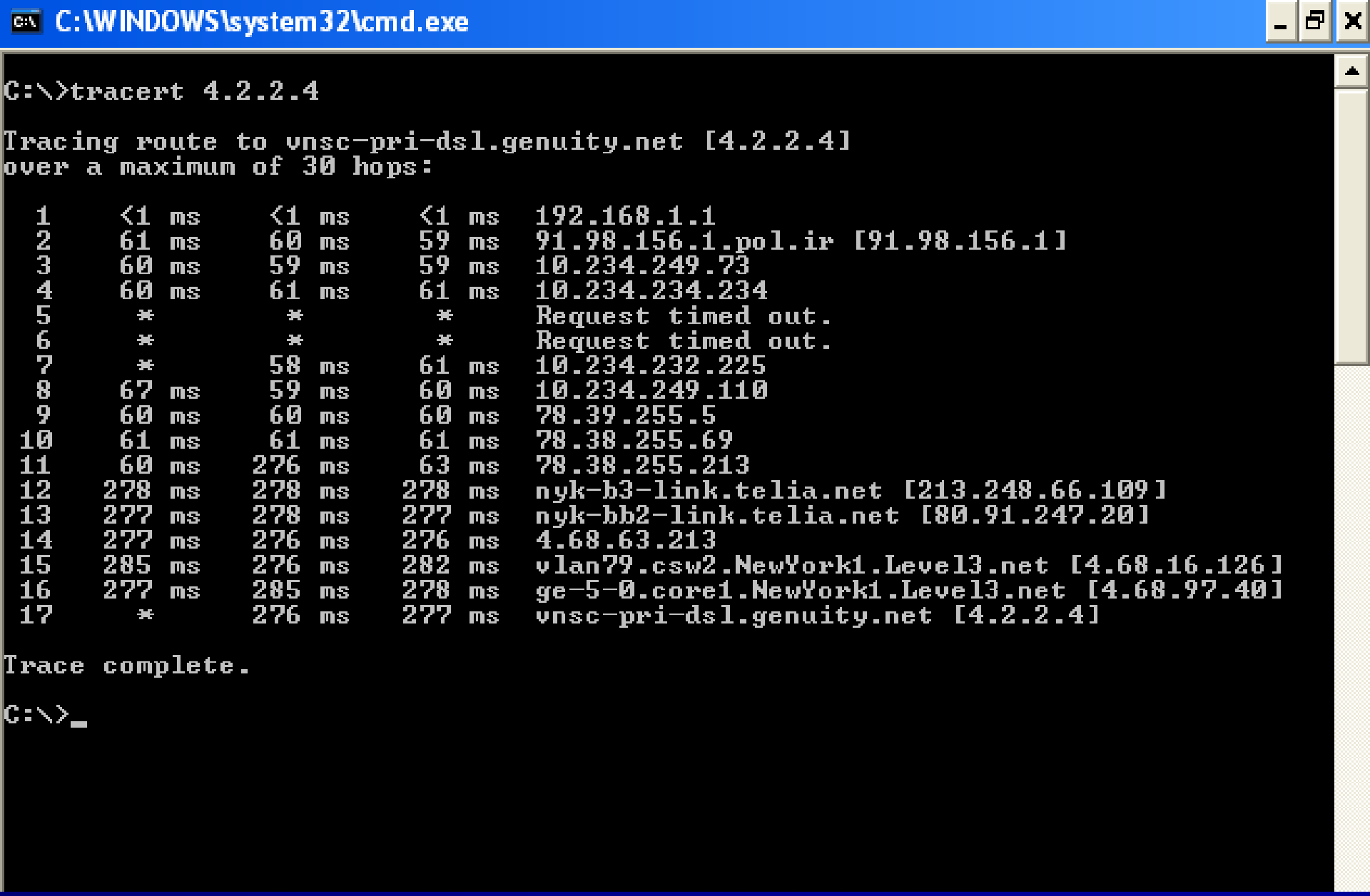
C:\WINDOWS\system32\cmd.exe

```
C:\>ping niordc.ir

Pinging niordc.ir [91.98.31.200] with 32 bytes of data:

Reply from 91.98.31.200: bytes=32 time=66ms TTL=121
Reply from 91.98.31.200: bytes=32 time=64ms TTL=121
Reply from 91.98.31.200: bytes=32 time=65ms TTL=121
Reply from 91.98.31.200: bytes=32 time=64ms TTL=121

Ping statistics for 91.98.31.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 64ms, Maximum = 66ms, Average = 64ms

C:\>
```

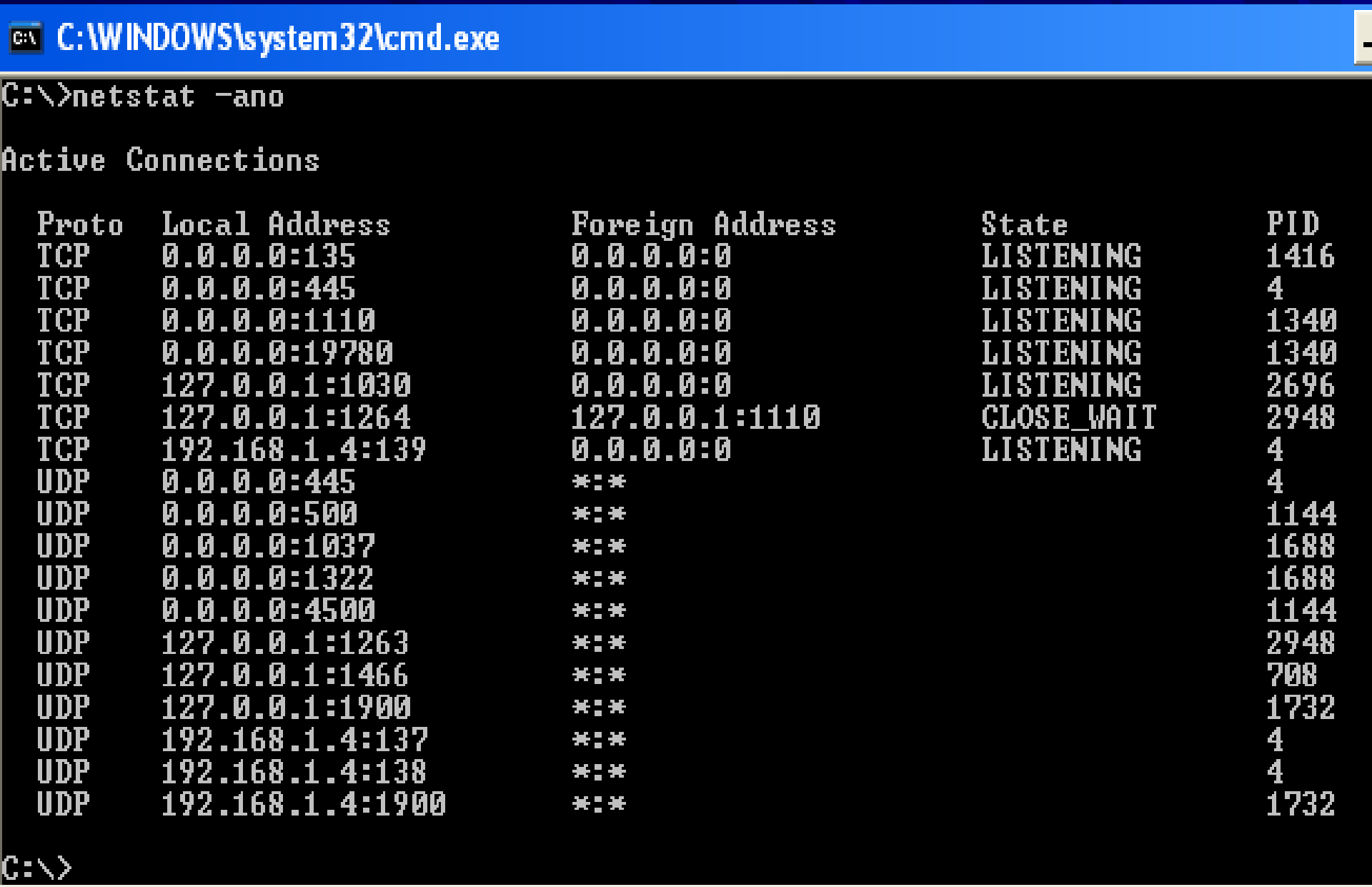

C:\WINDOWS\system32\cmd.exe
C:\>pathping niordc.ir
Tracing route to niordc.ir [91.98.31.200]
over a maximum of 30 hops:
0 mo-17 [192.168.1.4]
1 192.168.1.1
2 91.98.156.1.pol.ir [91.98.156.1]
3 10.234.249.73
4 10.234.220.74
5 10.234.231.225
6 10.199.100.155
7 10.199.50.2
8 91.98.31.200.pol.ir [91.98.31.200]
Pathping
Computing statistics for 200 seconds...
Source to Here This Node/Link
Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address
0 mo-17 [192.168.1.4]
0/ 100 = 0% |
1 0ms 0/ 100 = 0% 0/ 100 = 0% 192.168.1.1
0/ 100 = 0% |
2 63ms 2/ 100 = 2% 2/ 100 = 2% 91.98.156.1.pol.ir [91.98.156.1]
0/ 100 = 0% |
3 66ms 0/ 100 = 0% 0/ 100 = 0% 10.234.249.73
1/ 100 = 1% |
4 66ms 1/ 100 = 1% 0/ 100 = 0% 10.234.220.74
0/ 100 = 0% |
5 67ms 1/ 100 = 1% 0/ 100 = 0% 10.234.231.225
1/ 100 = 1% |
6 --- 100/ 100 =100% 98/ 100 = 98% 10.199.100.155
0/ 100 = 0% |
7 71ms 2/ 100 = 2% 0/ 100 = 0% 10.199.50.2
0/ 100 = 0% |
8 67ms 2/ 100 = 2% 0/ 100 = 0% 91.98.31.200.pol.ir [91.98.31.200
Trace complete.

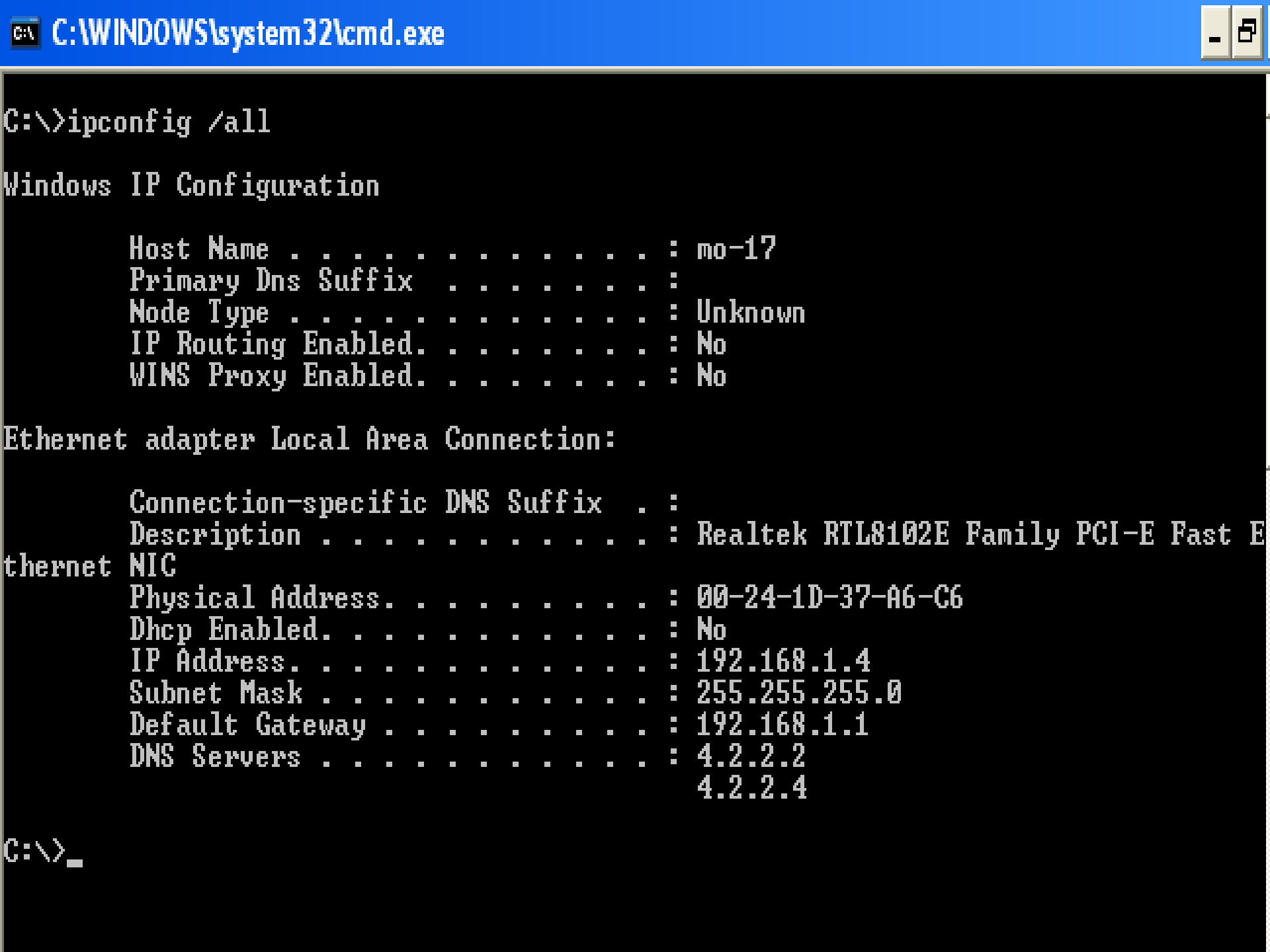
C:\WINDOWS\system32\cmd.exe

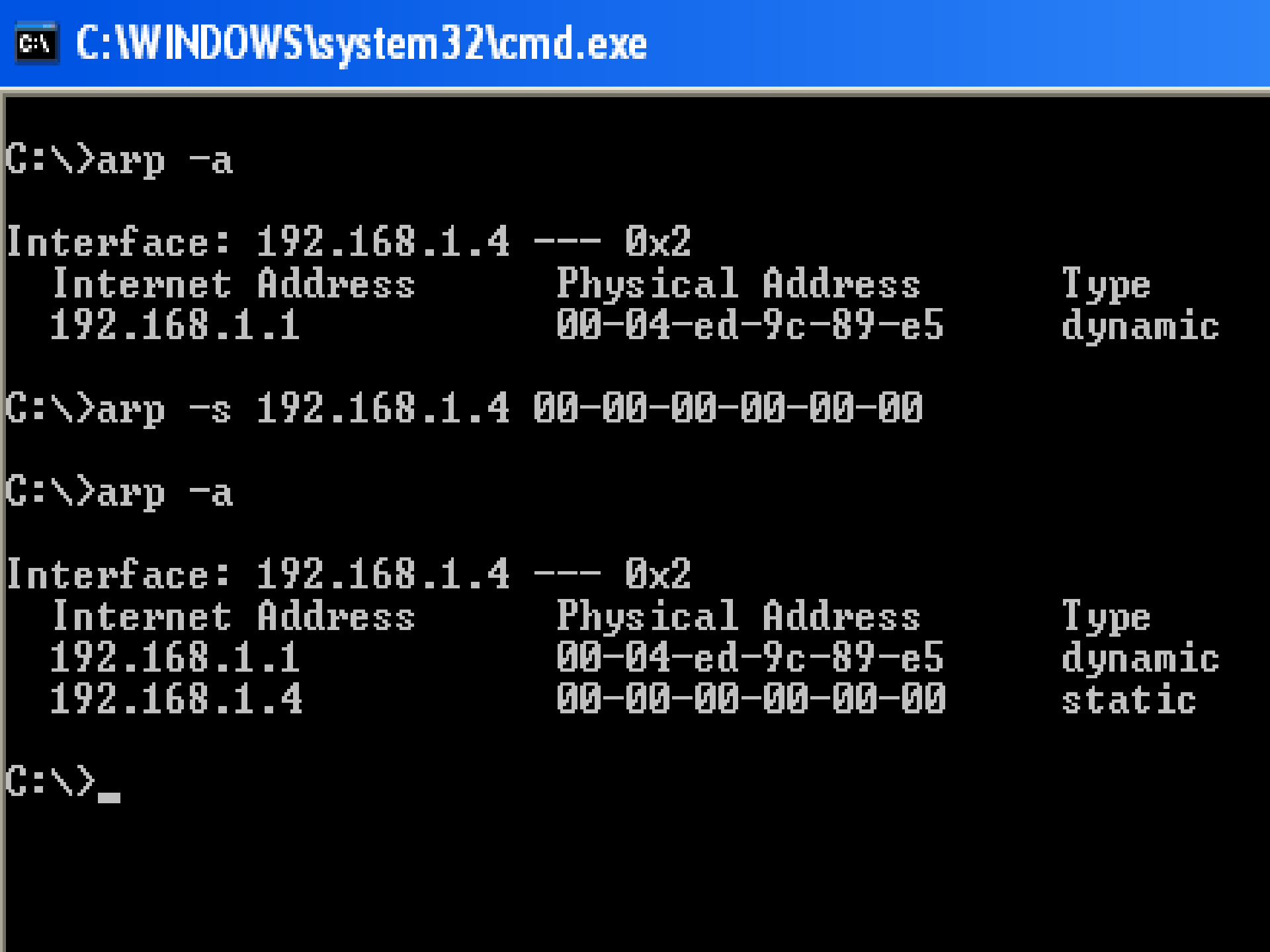
```
C:\>nslookup niordc.ir
Server:  vnsc-bak.sys.gtei.net
Address:  4.2.2.2

Non-authoritative answer:
Name:    niordc.ir
Address:  91.98.31.200


C:\>_
```



از دستور فوق بمنظور مسير يابي يک بسته اطلاعاتي تارسيدن به مقصد مورد نظر استفاده ميشود .


C:\WINDOWS\system32\cmd.exe
C:\>netstat -ano
Active Connections
Proto Local Address Foreign Address State PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 1416
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:1110 0.0.0.0:0 LISTENING 1340
TCP 0.0.0.0:19780 0.0.0.0:0 LISTENING 1340
TCP 127.0.0.1:1030 0.0.0.0:0 LISTENING 2696
TCP 127.0.0.1:1264 127.0.0.1:1110 CLOSE_WAIT 2948
TCP 192.168.1.4:139 0.0.0.0:0 LISTENING 4
UDP 0.0.0.0:445 *:* 4
UDP 0.0.0.0:500 *:* 1144
UDP 0.0.0.0:1037 *:* 1688
UDP 0.0.0.0:1322 *:* 1688
UDP 0.0.0.0:4500 *:* 1144
UDP 127.0.0.1:1263 *:* 2948
UDP 127.0.0.1:1466 *:* 708
UDP 127.0.0.1:1900 *:* 1732
UDP 192.168.1.4:137 *:* 4
UDP 192.168.1.4:138 *:* 4
UDP 192.168.1.4:1900 *:* 1732
C:\>


C:\WINDOWS\system32\cmd.exe
C:\>ipconfig /all
Windows IP Configuration
Host Name . . . . . : mo-17
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Description . . . . . : Realtek RTL8102E Family PCI-E Fast E
thernet NIC
Physical Address. . . . . : 00-24-1D-37-A6-C6
Dhcp Enabled. . . . . : No
IP Address. . . . . : 192.168.1.4
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DNS Servers . . . . . : 4.2.2.2
4.2.2.4
C:\>


C:\WINDOWS\system32\cmd.exe
C:\>arp -a
Interface: 192.168.1.4 --- 0x2
Internet Address Physical Address Type
192.168.1.1 00-04-ed-9c-89-e5 dynamic
C:\>arp -s 192.168.1.4 00-00-00-00-00-00
C:\>arp -a
Interface: 192.168.1.4 --- 0x2
Internet Address Physical Address Type
192.168.1.1 00-04-ed-9c-89-e5 dynamic
192.168.1.4 00-00-00-00-00-00 static
C:\>_

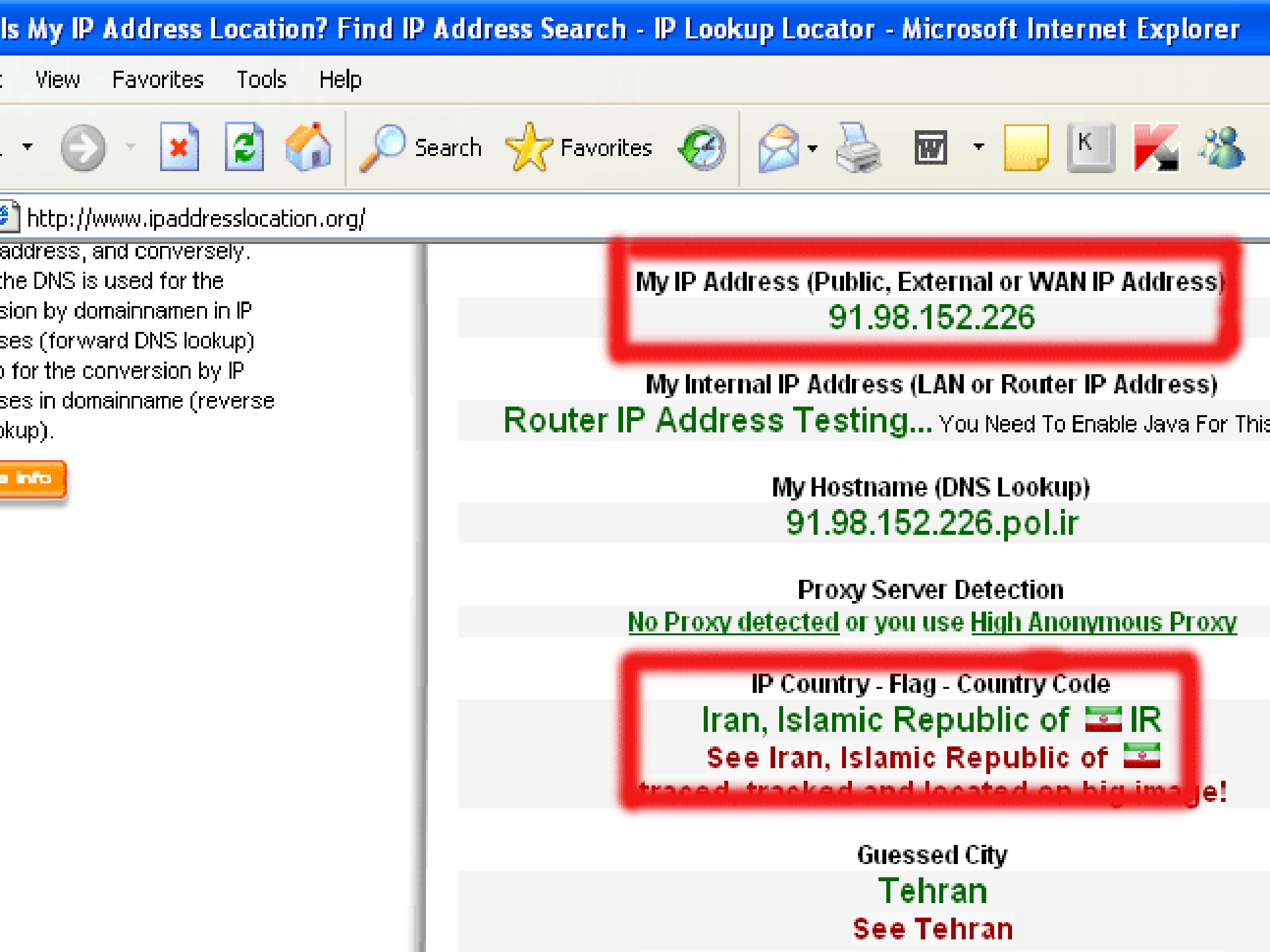
www.newtechnology.ir

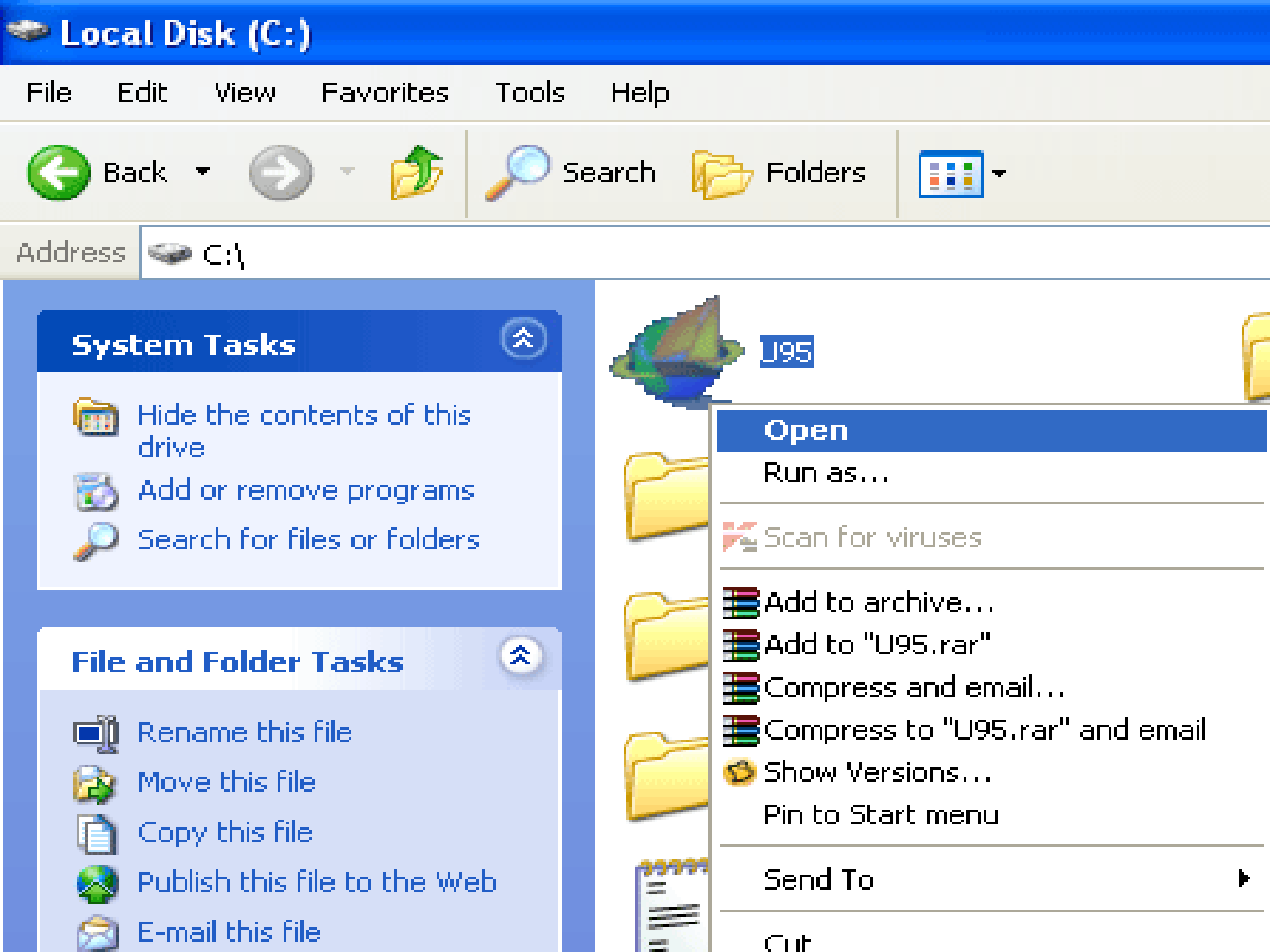
آغاز اجراي يک حمله با

IP Spoofing

(جعل IP)


Is My IP Address Location? Find IP Address Search - IP Lookup Locator - Microsoft Internet Explorer
View Favorites Tools Help
Search Favorites
http://www.ipaddresslocation.org/
Go
IP Address Location - Find My IP Address - IP Lookup
IP واقعی
91.98.152.226
My IP: 91.98.152.226
sponsored links
Ads by Google
Nixu Software's Warning
Running IPAM as virtual machine is known to cause feelings of joy.
www.nixusoftware.com
Galveston Texas Apts
Local-Fast-Free+20 Years experience specials, locations, availability
www.rentbuysell-galvestont
Uw Logo/Visual tracken?
We specialize in IP PBXs in Japan Rich feature set, low cost.
www.denphone.com
Nixu Software's Warning
Running IPAM as virtual machine is known to cause feelings of joy.
www.nixusoftware.com
Modbus Libraries / Driver


ls My IP Address Location? Find IP Address Search - IP Lookup Locator - Microsoft Internet Explorer
View
Favorites
Tools
Help
Search
Favorites
http://www.ipaddresslocation.org/
address, and conversely.
the DNS is used for the
sion by domainnamen in IP
ses (forward DNS lookup)
for the conversion by IP
ses in domainname (reverse
kup).
My IP Address (Public, External or WAN IP Address)
91.98.152.226
My Internal IP Address (LAN or Router IP Address)
Router IP Address Testing... You Need To Enable Java For This
My Hostname (DNS Lookup)
91.98.152.226.pol.ir
Proxy Server Detection
No Proxy detected or you use High Anonymous Proxy
IP Country - Flag - Country Code
Iran, Islamic Republic of IR
See Iran, Islamic Republic of
Guessed City
Tehran
See Tehran


Local Disk (C:)
File Edit View Favorites Tools Help
Back
Search
Folders
Address
C:\
System Tasks
Hide the contents of this drive
Add or remove programs
Search for files or folders
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
U95
Open
Run as...
Scan for viruses
Add to archive...
Add to "U95.rar"
Compress and email...
Compress to "U95.rar" and email
Show Versions...
Pin to Start menu
Send To
Cut

ress C:\

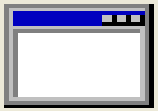
System Tasks

Hide the contents of this

U95

Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?



Name: U95.exe

Publisher: **Unknown Publisher**

Type: Application

From: C:\

Run Cancel

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

http://www.ultrareach.net/search_iran.htm

UltraSurf™

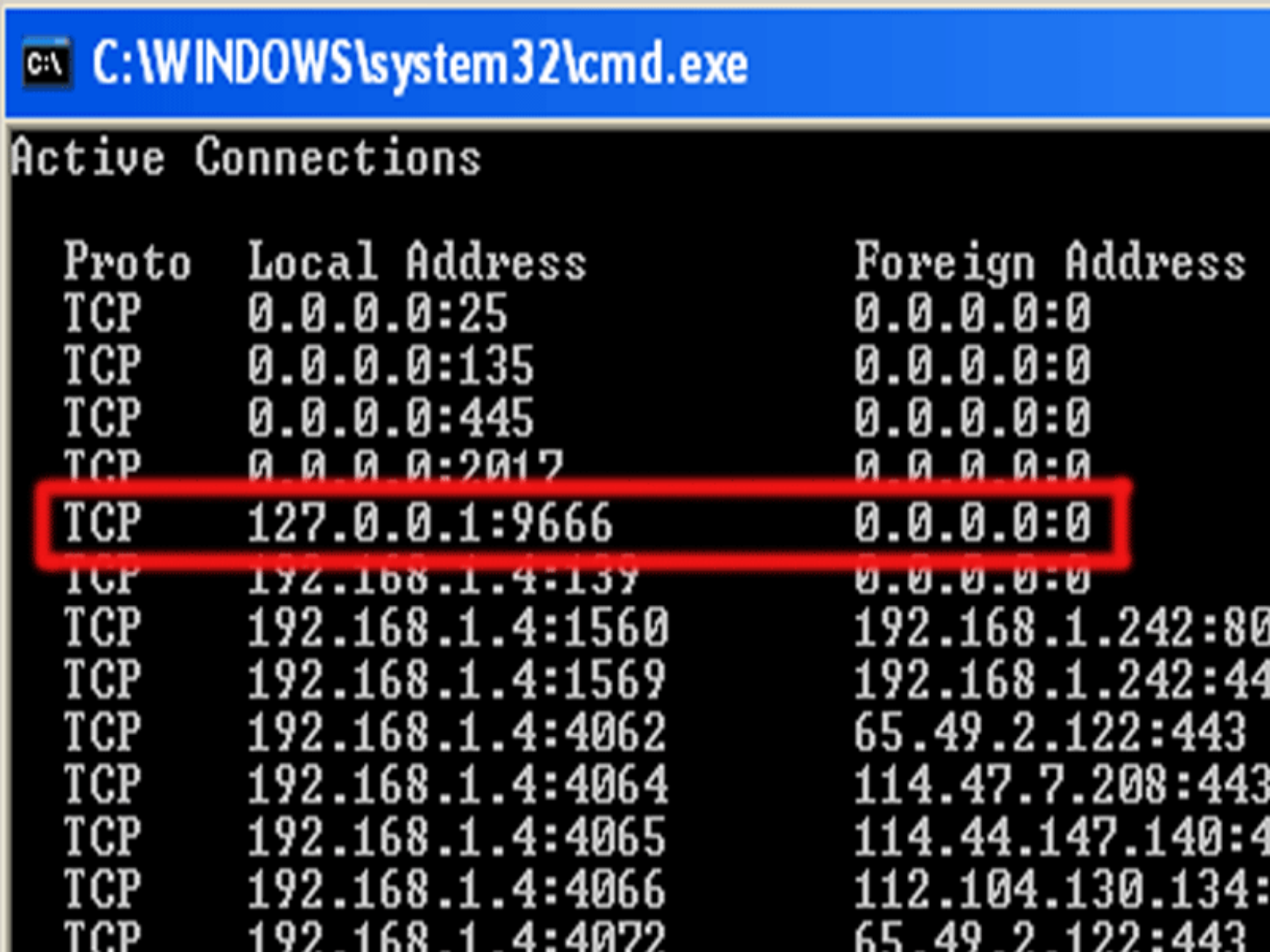
Privacy, Security and Freedom

Google Search | Advanced Search

New!(01/08/2010) Please upgrade to the latest release version of UltraSurf 9.92 (md5sum: 11f0901ce03eed2e71f72b754b56164c)

Hom... About

C... ...ed.


C:\WINDOWS\system32\cmd.exe
Active Connections
Proto Local Address Foreign Address
TCP 0.0.0.0:25 0.0.0.0:0
TCP 0.0.0.0:135 0.0.0.0:0
TCP 0.0.0.0:445 0.0.0.0:0
TCP 127.0.0.1:9666 0.0.0.0:0
TCP 192.168.1.4:1560 192.168.1.242:80
TCP 192.168.1.4:1569 192.168.1.242:44
TCP 192.168.1.4:4062 65.49.2.122:443
TCP 192.168.1.4:4064 114.47.7.208:443
TCP 192.168.1.4:4065 114.44.147.140:4
TCP 192.168.1.4:4066 112.104.130.134:


What Is My IP Address Location? Find IP Address Search - IP Lookup Locator - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.ipaddresslocation.org/
IP Address Location - Find My IP Address - IP Lookup
ipaddress location
جعلی IP
65.49.2.22
My IP: 65.49.2.22
sponsored links
Ads by
Locate
Find IF
My Cor
IP Trac
Other
Support IP .
with donati
IP address
provide ren
Make A Donation
Get IP location, map, trace, track and traceroute any IP address.
whatismyipaddress.com
IP Geo Location Server
Determine the real-time geographic Location of

t Is My IP Address Location? Find IP Address Search - IP Lookup Locator - Microsoft Internet Explorer

dit View Favorites Tools Help

ck Search Favorites

http://www.ipaddresslocation.org/

P address, and conversely.
y the DNS is used for the
ersion by domainnamen in IP
esses (forward DNS lookup)
so for the conversion by IP
esses in domainname (reverse
ookup).

ore info

My IP Address (Public, External or WAN IP Address)

65.49.2.22

My Internal IP Address (LAN or Router IP Address)

Router IP Address Testing... You Need To Enable Java For This To Work

My Hostname (DNS Lookup)

65.49.2.22

Proxy Server Detection

No Proxy detected or you use High Anonymous Proxy

IP Country - Flag - Country Code

United States US

See United States

traced, tracked and located on big image!

Guessed City

Cheyenne

See Cheyenne

tracked, traced and located on big image!