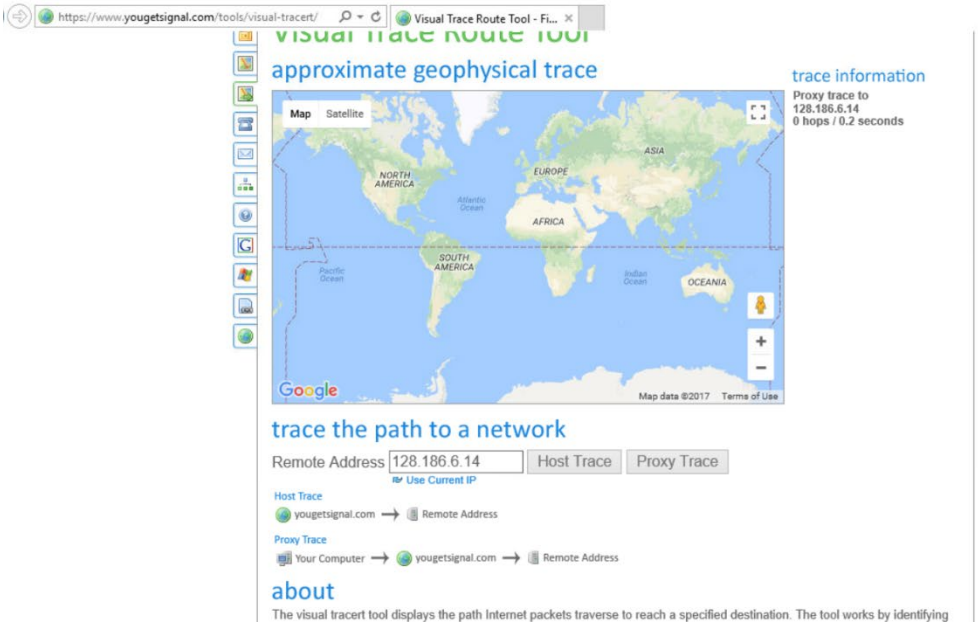
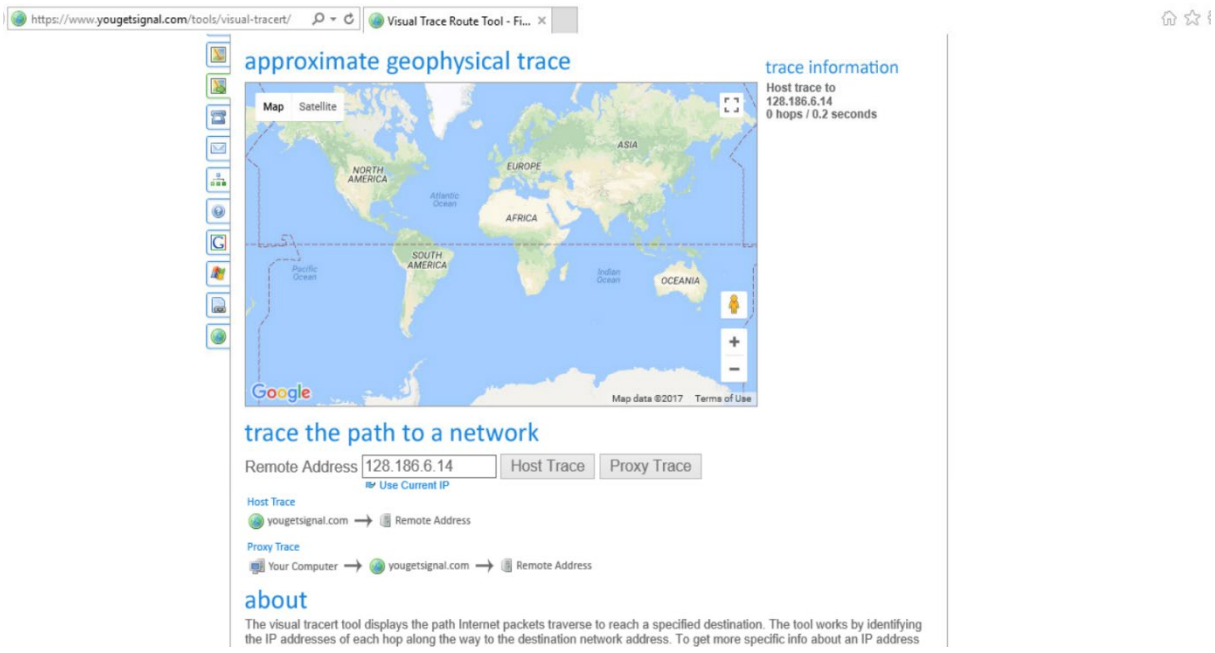
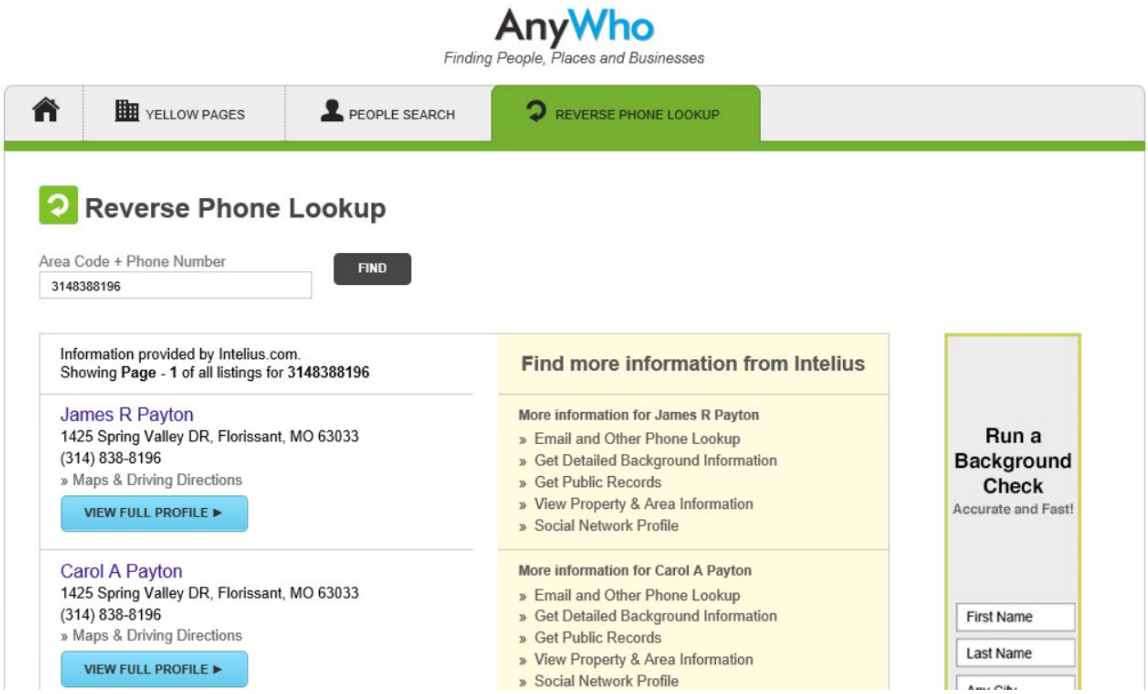
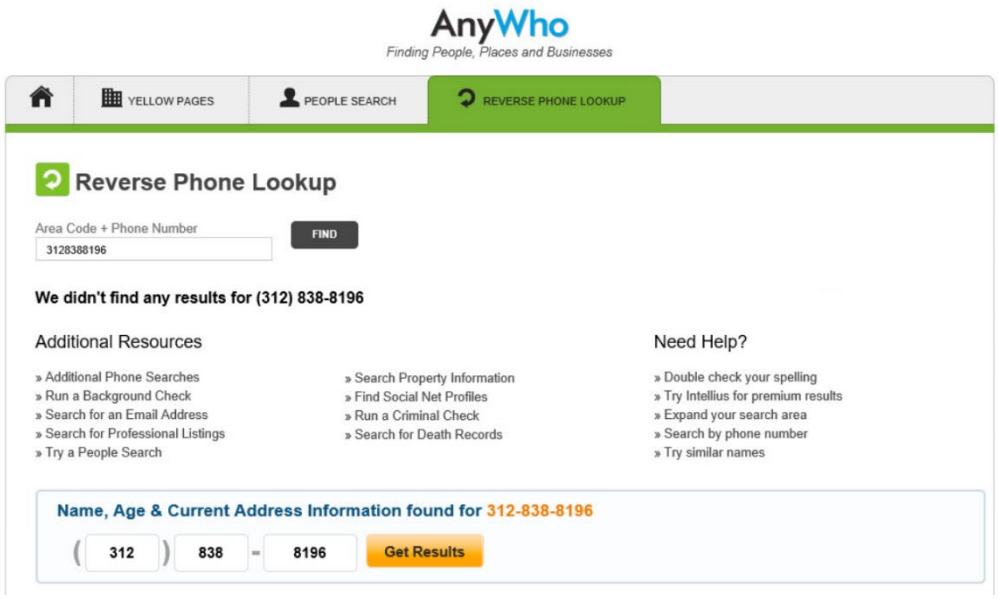
9.1 Trace Route to the Source

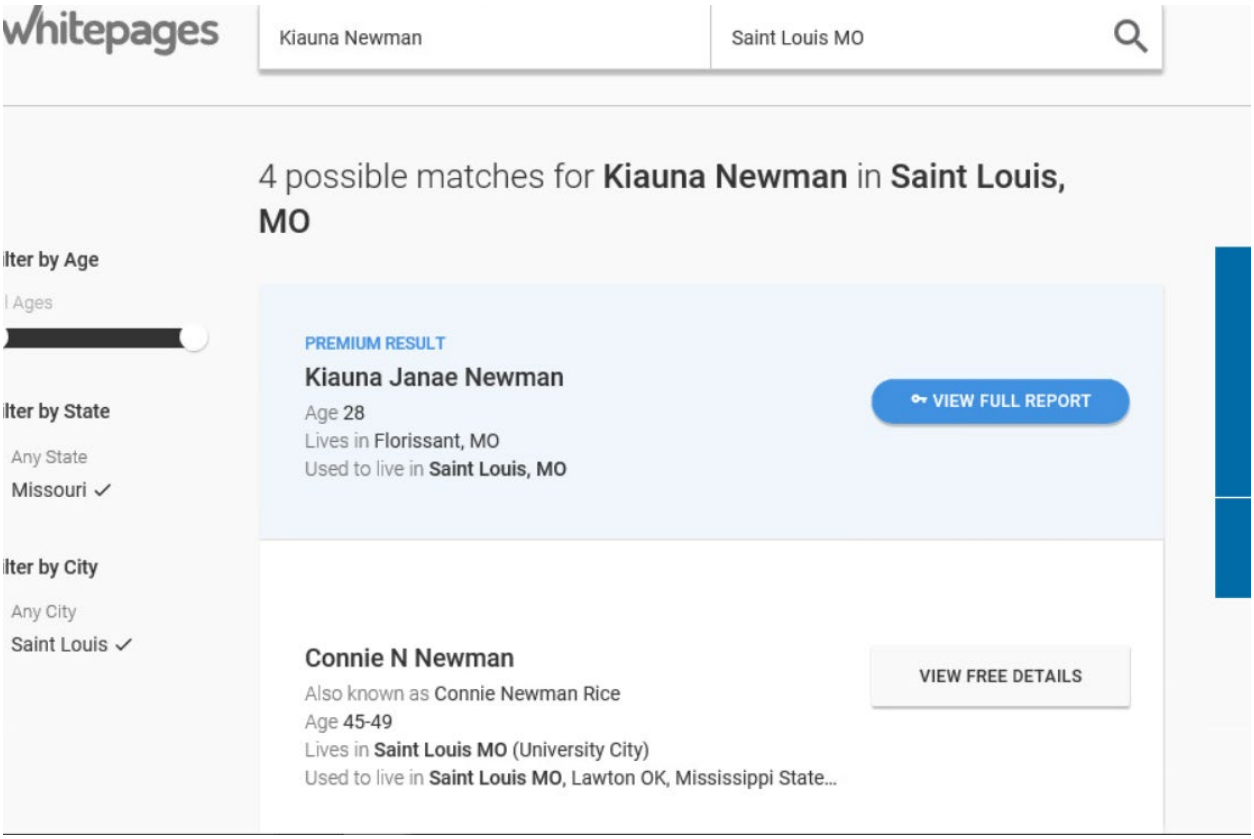


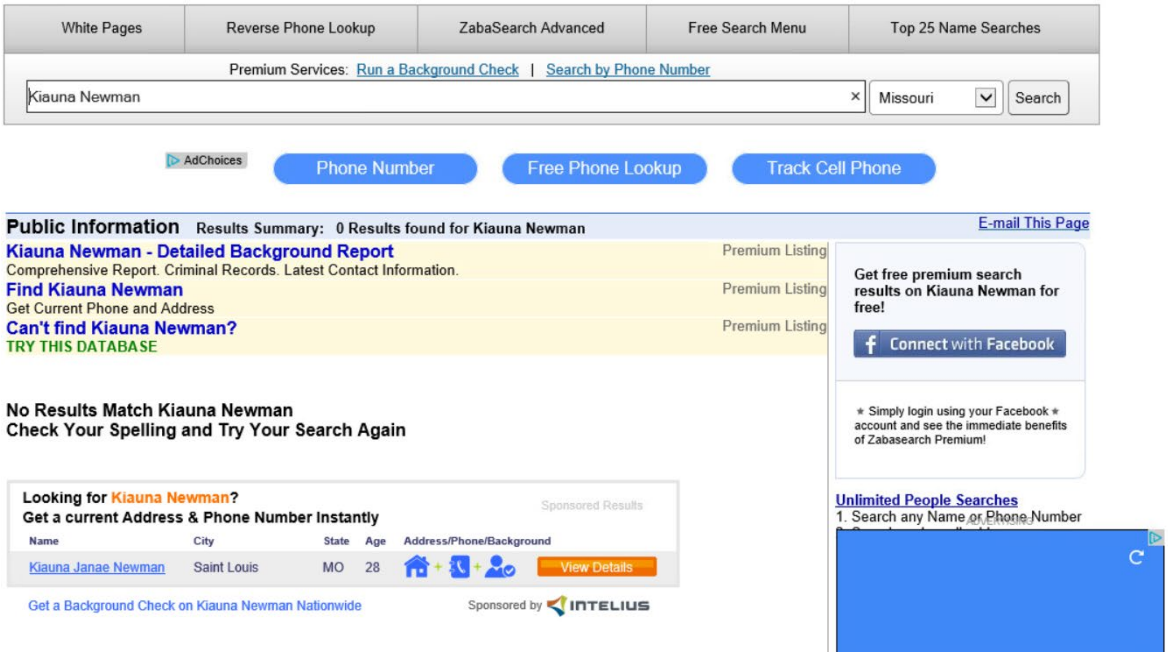



9.2 Trace a Phone Number



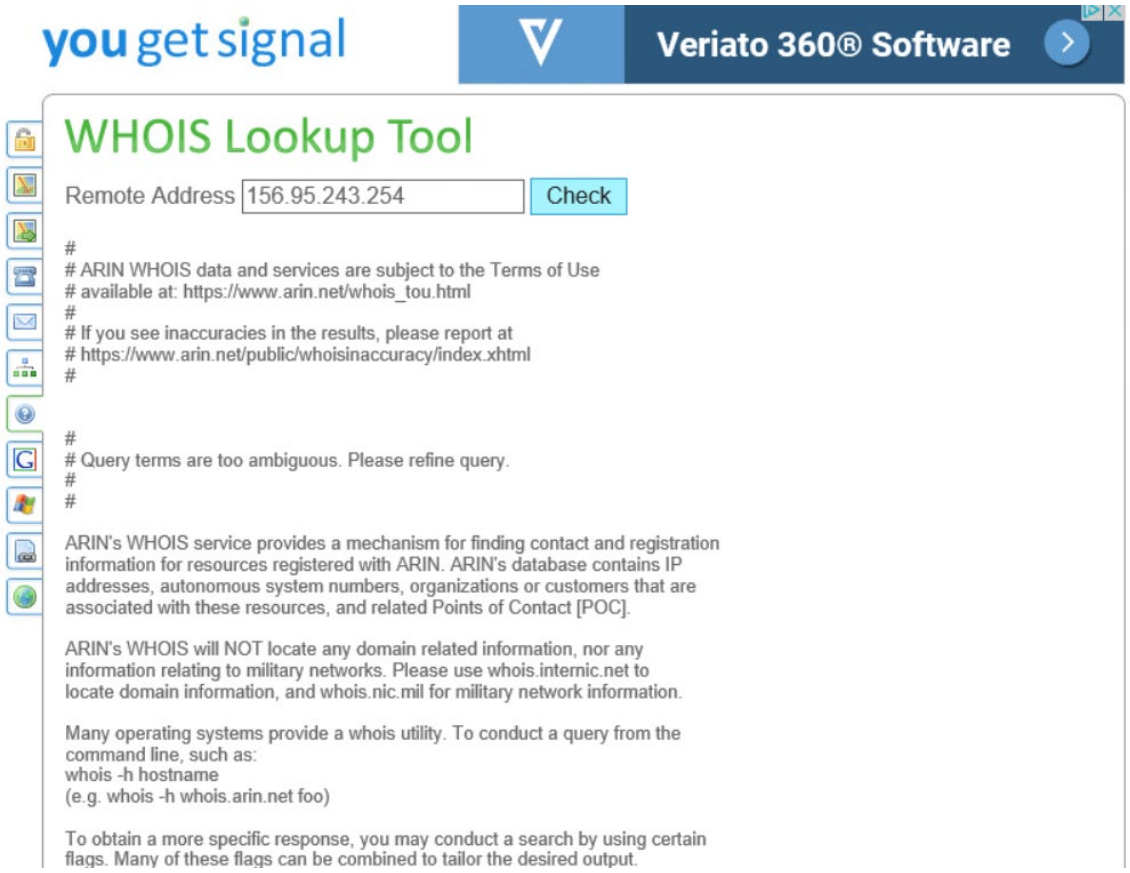

whitepages
Kiauna Newman
Saint Louis MO
4 possible matches for Kiauna Newman in Saint Louis, MO
lter by Age
l Ages
lter by State
Any State
Missouri ✓
lter by City
Any City
Saint Louis ✓
PREMIUM RESULT
Kiauna Janae Newman
Age 28
Lives in Florissant, MO
Used to live in Saint Louis, MO
VIEW FULL REPORT
Connie N Newman
Also known as Connie Newman Rice
Age 45-49
Lives in Saint Louis MO (University City)
Used to live in Saint Louis MO, Lawton OK, Mississippi State...
VIEW FREE DETAILS


White Pages
Reverse Phone Lookup
ZabaSearch Advanced
Free Search Menu
Top 25 Name Searches
Premium Services: Run a Background Check | Search by Phone Number
Kiauna Newman
Missouri
Search
AdChoices
Phone Number
Free Phone Lookup
Track Cell Phone
Public Information Results Summary: 0 Results found for Kiauna Newman
E-mail This Page
Kiauna Newman - Detailed Background Report
Comprehensive Report. Criminal Records. Latest Contact Information.
Premium Listing
Find Kiauna Newman
Get Current Phone and Address
Premium Listing
Can't find Kiauna Newman?
TRY THIS DATABASE
Premium Listing
No Results Match Kiauna Newman
Check Your Spelling and Try Your Search Again
Looking for Kiauna Newman?
Get a current Address & Phone Number Instantly
Sponsored Results
Name
City
State
Age
Address/Phone/Background
Kiauna Janae Newman
Saint Louis
MO
28
View Details
Get a Background Check on Kiauna Newman Nationwide
Sponsored by INTELIUS
Get free premium search results on Kiauna Newman for free!
Connect with Facebook
* Simply login using your Facebook * account and see the immediate benefits of Zabasearch Premium!
Unlimited People Searches
1. Search any Name or Phone Number

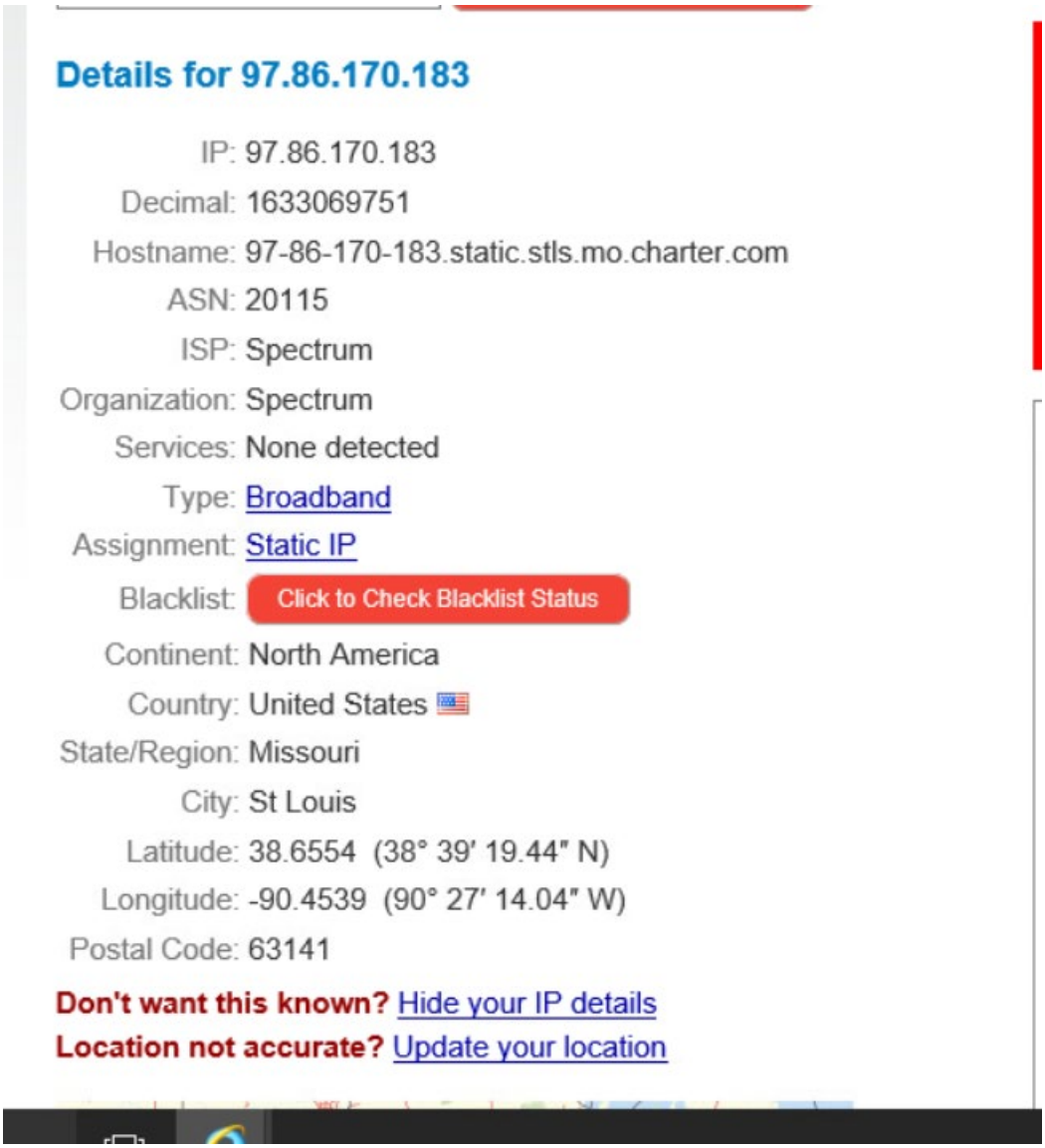
9.3 WhoIS


you get signal
Veriato 360® Software
WHOIS Lookup Tool
Remote Address 97.86.170.152
Check
#
# 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
# https://www.arin.net/public/whoisinaccuracy/index.xhtml
#
#
# Query terms are too ambiguous. Please refine query.
#
#
ARIN's WHOIS service provides a mechanism for finding contact and registration information for resources registered with ARIN. ARIN's database contains IP addresses, autonomous system numbers, organizations or customers that are associated with these resources, and related Points of Contact [POC].
ARIN's WHOIS will NOT locate any domain related information, nor any information relating to military networks. Please use whois.internic.net to locate domain information, and whois.nic.mil for military network information.
Many operating systems provide a whois utility. To conduct a query from the command line, such as:
whois -h hostname
(e.g. whois -h whois.arin.net foo)
To obtain a more specific response, you may conduct a search by using certain flags. Many of these flags can be combined to tailor the desired output.
Flags must be separated from each other and from the search term by a space.


you get signal
Veriato 360® Software
WHOIS Lookup Tool
Remote Address 155.97.243.201
Check
#
# 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
# https://www.arin.net/public/whoisinaccuracy/index.xhtml
#
#
# Query terms are too ambiguous. Please refine query.
#
#
ARIN's WHOIS service provides a mechanism for finding contact and registration information for resources registered with ARIN. ARIN's database contains IP addresses, autonomous system numbers, organizations or customers that are associated with these resources, and related Points of Contact [POC].
ARIN's WHOIS will NOT locate any domain related information, nor any information relating to military networks. Please use whois.internic.net to locate domain information, and whois.nic.mil for military network information.
Many operating systems provide a whois utility. To conduct a query from the command line, such as:
whois -h hostname
(e.g. whois -h whois.arin.net foo)
To obtain a more specific response, you may conduct a search by using certain flags. Many of these flags can be combined to tailor the desired output.
Task View


you get signal
Veriato 360® Software
WHOIS Lookup Tool
Remote Address 156.95.243.254
Check
#
# 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
# https://www.arin.net/public/whoisinaccuracy/index.xhtml
#
#
# Query terms are too ambiguous. Please refine query.
#
#
ARIN's WHOIS service provides a mechanism for finding contact and registration information for resources registered with ARIN. ARIN's database contains IP addresses, autonomous system numbers, organizations or customers that are associated with these resources, and related Points of Contact [POC].
ARIN's WHOIS will NOT locate any domain related information, nor any information relating to military networks. Please use whois.internic.net to locate domain information, and whois.nic.mil for military network information.
Many operating systems provide a whois utility. To conduct a query from the command line, such as:
whois -h hostname
(e.g. whois -h whois.arin.net foo)
To obtain a more specific response, you may conduct a search by using certain flags. Many of these flags can be combined to tailor the desired output.

9.4 Locate an IP Address Sources



## Details for 155.97.243.201

IP: 155.97.243.201
Decimal: 2606887881
Hostname: dhcp-663usa-189.usa.utah.edu
ASN: 17055
ISP: University of Utah
Organization: University of Utah
Services: None detected
Type: Broadband
Assignment: Static IP
Blacklist: Click to Check Blacklist Status
Continent: North America
Country: United States
State/Region: Utah
City: Salt Lake City
Latitude: 40.7855 (40° 47′ 7.80″ N)
Longitude: -111.7367 (111° 44′ 12.12″ W)
Postal Code: 84108

105.97.243.201 Lookup IP Address

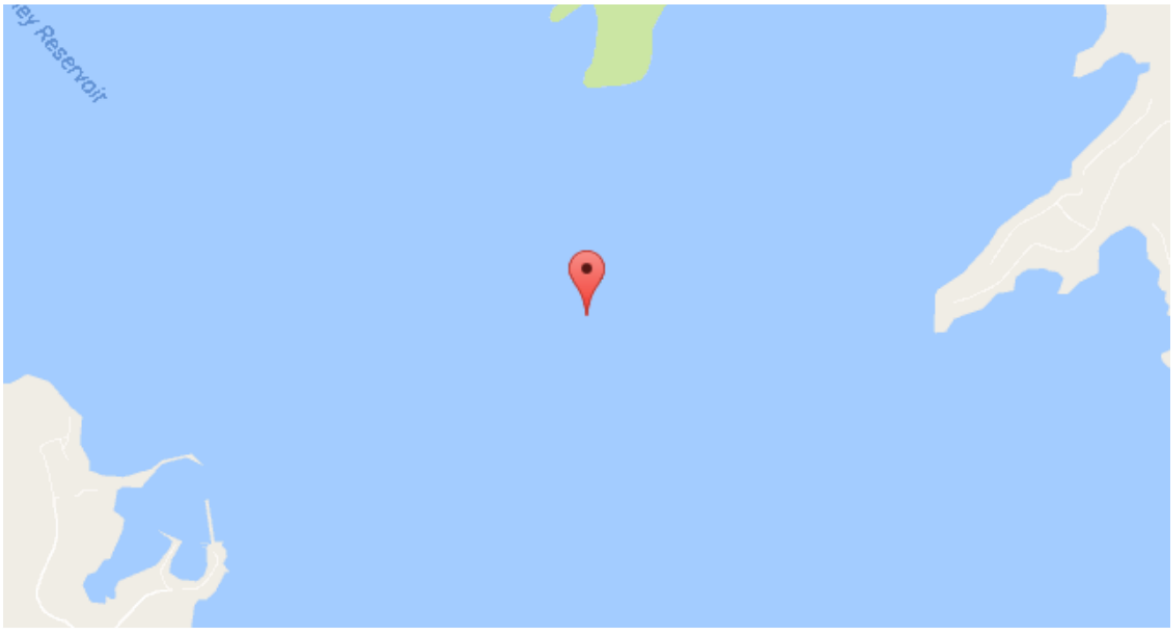
## Details for 105.97.243.201

IP: 105.97.243.201
Decimal: 1768027081
Hostname: 105.97.243.201
ASN: 36947
ISP: Telecom Algeria
Organization: Telecom Algeria
Services: None detected
Type: Broadband
Assignment: Static IP
Blacklist: Click to Check Blacklist Status
Continent: Africa
Country: Algeria
Latitude: 36.7642 (36° 45′ 51.12″ N)
Longitude: 3.1468 (3° 8′ 48.48″ E)

## 9.5 Locate an Email Source

### Trace Email Result

At Sat, 23 Sep 2017 11:19:44 -0500, **tnturfdocs@gmail.com** sent you an email from the IP Address 209.85.220.176. View Email Owner




| | |
|---|---|
| **IP Address:** | 209.85.220.176 |
| **Host of this IP:** | mail-qk0-f176.google.com |

BAC

ipaddress.com/trace-email.html

Calculator

**Email Tools**
- Trace Email Address
- Verify Email Address

**APIs**
- Free My IP API
- IP Address To Country API

**Miscellaneous**
- Articles
- Speed Test
- About Us
- Privacy Policy
- Contact Us
- Advertising
- Sitemap

Want to trace an email? Our trace email tool can find the IP address of the sender and help you determine where the email came from using that IP information. Simply copy and paste the header of the email into the box provided below and our email tracer will do the rest, pinpointing the location of the sender's **IP address** in seconds

Enter Email Header to trace an Email

```
X-MS-Exchange-Transport-CrossTenantHeadersStamped: CY4PR20MB1479
X-MS-Exchange-Organization-AuthSource: BY2NAM05FT025.eop-nam05.prod.protection.outlook.com
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-Exchange-Transport-EndToEndLatency: 00:00:04.5217012
X-MS-Exchange-Processed-By-BccFoldering: 15.20.0077.011
X-Microsoft-Exchange-Diagnostics:
        1;BN6PR20MB1473;9:1zyYuN6M4AETWAmbL3XcOSdypJeumC6x5U1AqdWF+nxk3Bu9lndzMwK6kH6iMc4A0VT40NA
DT9Vj7hcnwKvEax0fFBIV/zxIRi79msGo5D9JQjR6yENXy++Jexlyr02q
X-Microsoft-Exchange-Diagnostics:
        1;BN6PR20MB1473;27:5njMJcQnJF62fpkOXscMVc4oQBOD4Nj+kUYVJXhcFyu7rSulv/MemNLNnqrG6YowjjmULt
fWBp5LpwUvC36nuAAQAlsQEnzpLb72vWYZFiQJmQkGnw4WgXBai8PoIR4J
```

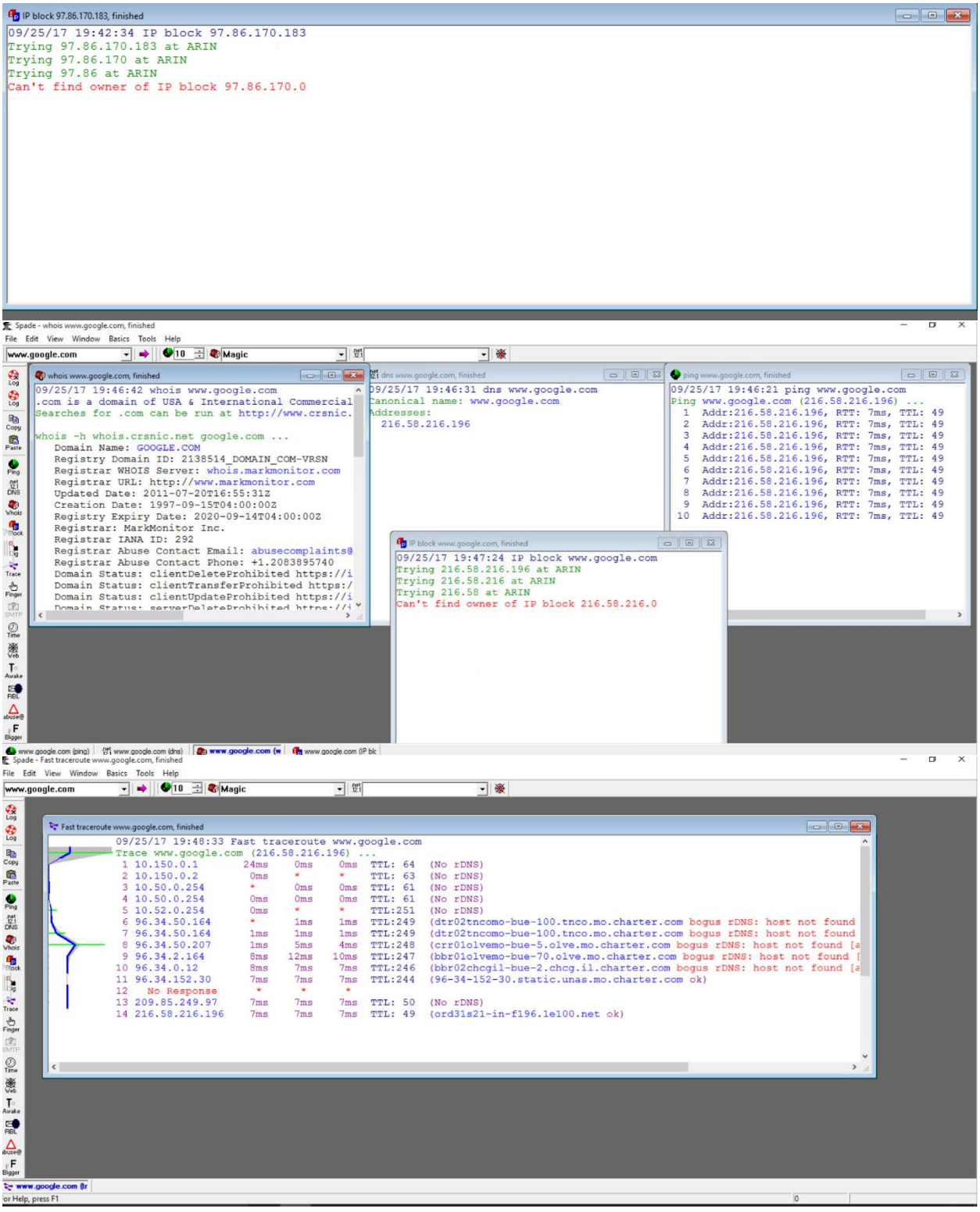
Trace Email Sender | View Email Owner | Reset

At IPAddress.com, we are well-aware of the online scams floating around online; and it for this reason that we have come up with an easy-to-use Email IP Lookup tool that can help you trace email addresses with great ease. Thanks to our tool, with just a few clicks, you will be able to determine whether you have received a genuine email or it's just another SPAM email that has made its way to your inbox.

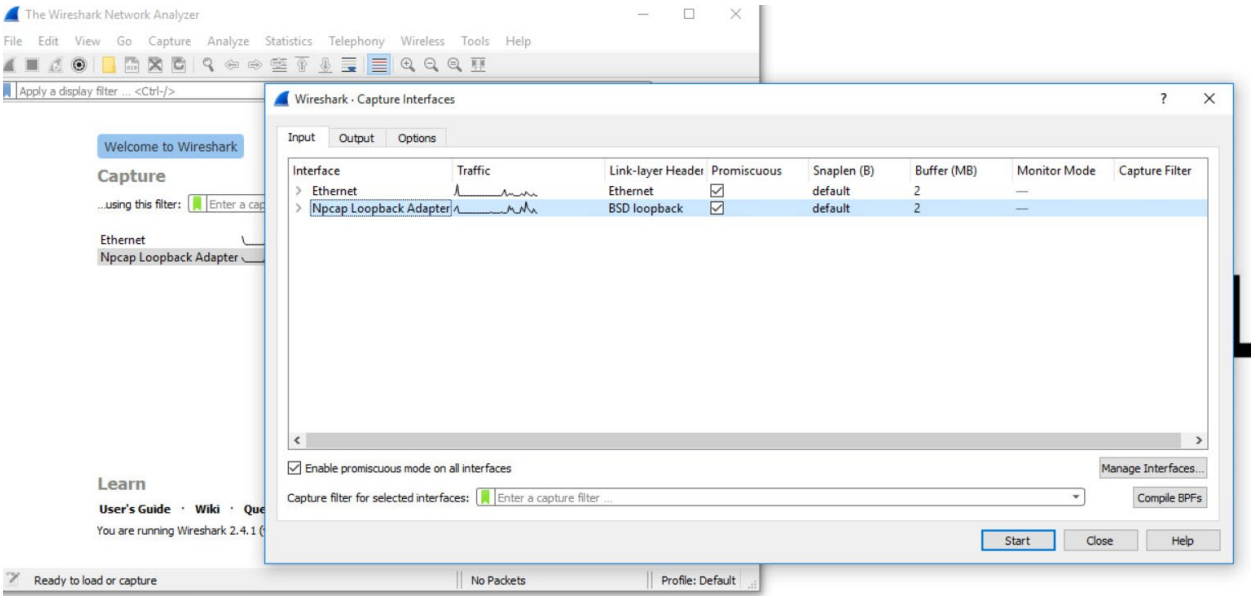
Why you may need our tool for email lookups you ask?

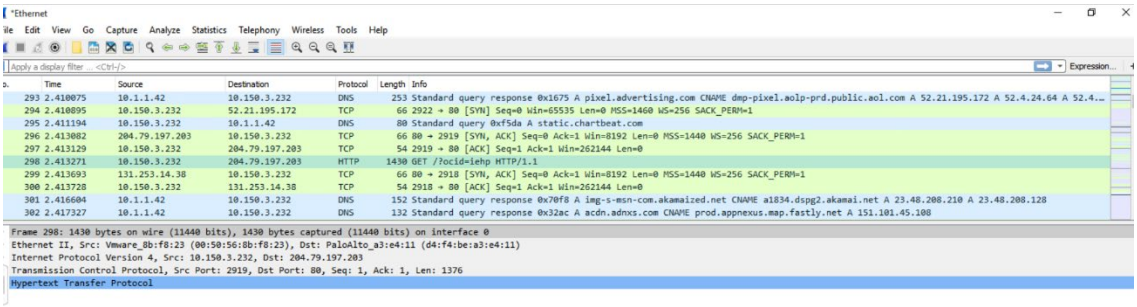
Email fraud is still on the rise; therefore, it is advisable that you think twice before trusting any of the emails you receive from unknown senders. Our tool can help you in making this much-needed distinction between good and bad by finding the location of the sender. Furthermore, when you trace an IP address with our tool, you can also determine the place of origin as far as the email is concerned.

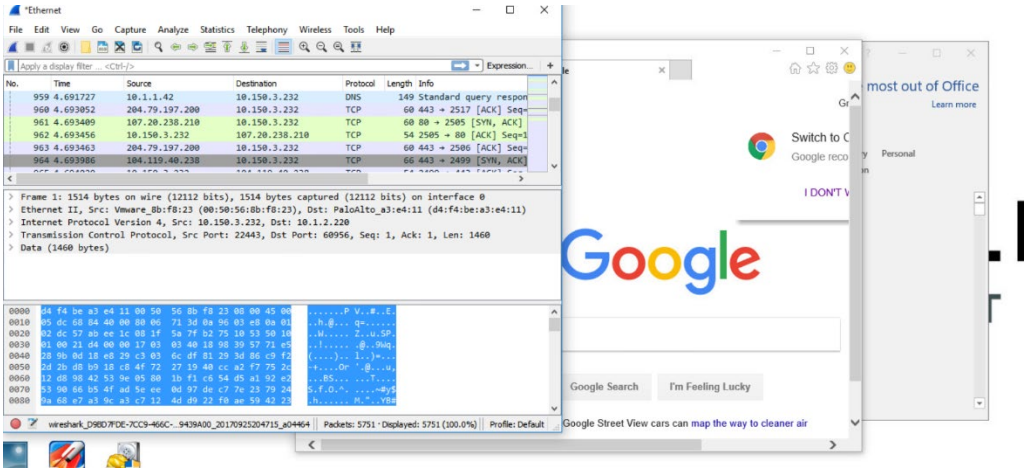
9.6 Sam Spade


IP block 97.86.170.183, finished
09/25/17 19:42:34 IP block 97.86.170.183
Trying 97.86.170.183 at ARIN
Trying 97.86.170 at ARIN
Trying 97.86 at ARIN
Can't find owner of IP block 97.86.170.0
Spade - whois www.google.com, finished
File Edit View Window Basics Tools Help
www.google.com
Magic
whois www.google.com, finished
09/25/17 19:46:42 whois www.google.com
.com is a domain of USA & International Commercial
Searches for .com can be run at http://www.crsnic.
whois -h whois.crsnic.net google.com ...
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2011-07-20T16:55:31Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2020-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://i
Domain Status: clientTransferProhibited https:/
Domain Status: clientUpdateProhibited https://i
dns www.google.com, finished
09/25/17 19:46:31 dns www.google.com
Canonical name: www.google.com
Addresses:
216.58.216.196
ping www.google.com, finished
09/25/17 19:46:21 ping www.google.com
Ping www.google.com (216.58.216.196) ...
1 Addr:216.58.216.196, RTT: 7ms, TTL: 49
2 Addr:216.58.216.196, RTT: 7ms, TTL: 49
3 Addr:216.58.216.196, RTT: 7ms, TTL: 49
4 Addr:216.58.216.196, RTT: 7ms, TTL: 49
5 Addr:216.58.216.196, RTT: 7ms, TTL: 49
6 Addr:216.58.216.196, RTT: 7ms, TTL: 49
7 Addr:216.58.216.196, RTT: 7ms, TTL: 49
8 Addr:216.58.216.196, RTT: 7ms, TTL: 49
9 Addr:216.58.216.196, RTT: 7ms, TTL: 49
10 Addr:216.58.216.196, RTT: 7ms, TTL: 49
IP block www.google.com, finished
09/25/17 19:47:24 IP block www.google.com
Trying 216.58.216.196 at ARIN
Trying 216.58.216 at ARIN
Trying 216.58 at ARIN
Can't find owner of IP block 216.58.216.0
Spade - Fast traceroute www.google.com, finished
Fast traceroute www.google.com, finished
09/25/17 19:48:33 Fast traceroute www.google.com
Trace www.google.com (216.58.216.196) ...
1 10.150.0.1 24ms 0ms 0ms TTL: 64 (No rDNS)
2 10.150.0.2 0ms * * TTL: 63 (No rDNS)
3 10.50.0.254 * 0ms 0ms TTL: 61 (No rDNS)
4 10.50.0.254 0ms 0ms 0ms TTL: 61 (No rDNS)
5 10.52.0.254 0ms * * TTL:251 (No rDNS)
6 96.34.50.164 * 1ms 1ms TTL:249 (dtr02tncomo-bue-100.tnco.mo.charter.com bogus rDNS: host not found
7 96.34.50.164 1ms 1ms 1ms TTL:249 (dtr02tncomo-bue-100.tnco.mo.charter.com bogus rDNS: host not found
8 96.34.50.207 1ms 5ms 4ms TTL:248 (crr01olvemo-bue-5.olve.mo.charter.com bogus rDNS: host not found [a
9 96.34.2.164 8ms 12ms 10ms TTL:247 (bbr01olvemo-bue-70.olve.mo.charter.com bogus rDNS: host not found [
10 96.34.0.12 8ms 7ms 7ms TTL:246 (bbr02chcgil-bue-2.chcg.il.charter.com bogus rDNS: host not found [a
11 96.34.152.30 7ms 7ms 7ms TTL:244 (96-34-152-30.static.unas.mo.charter.com ok)
12 No Response * * *
13 209.85.249.97 7ms 7ms 7ms TTL: 50 (No rDNS)
14 216.58.216.196 7ms 7ms 7ms TTL: 49 (ord31s21-in-f196.1e100.net ok)

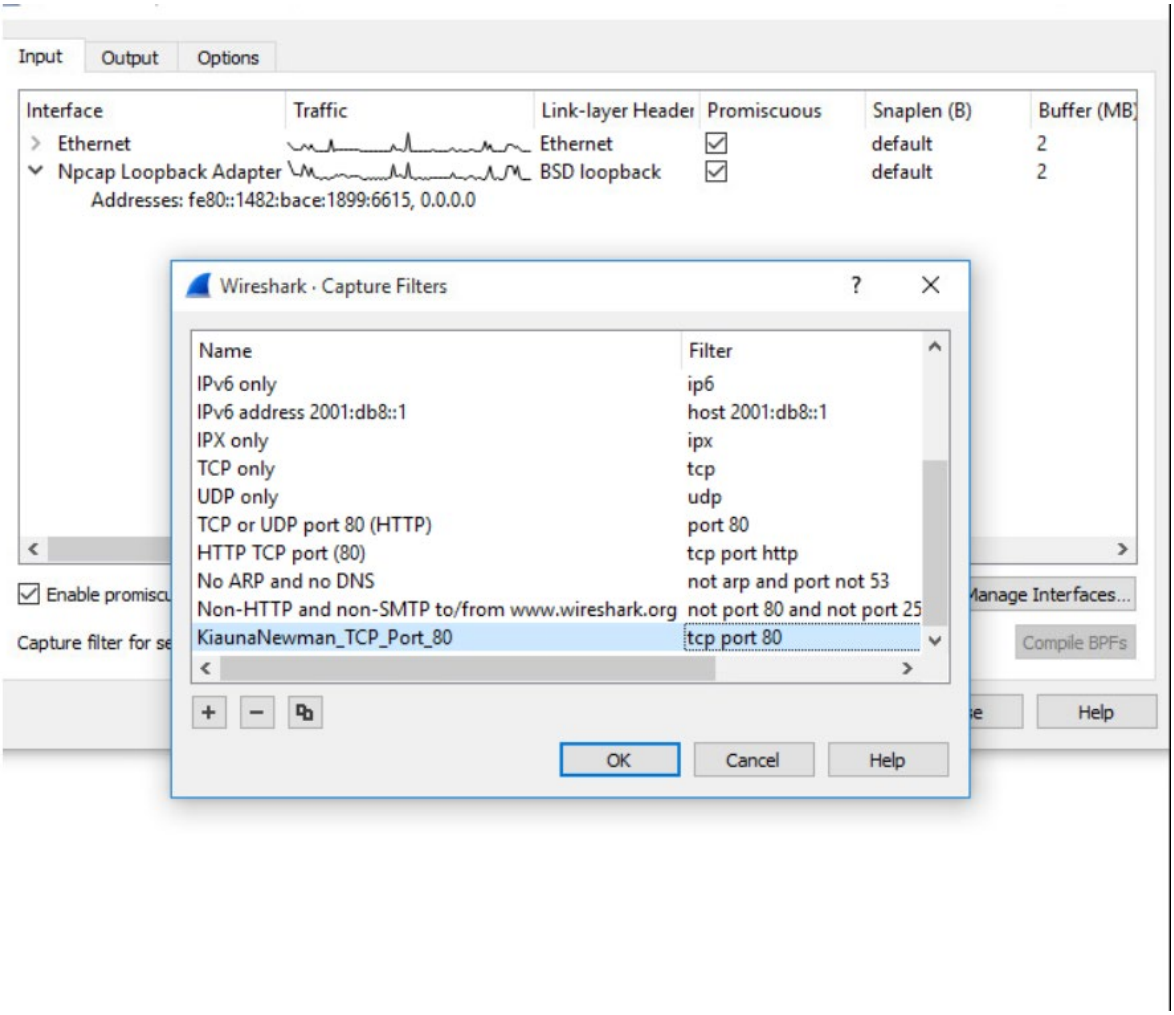
## 10.1 Packet Capture (Wireshark)

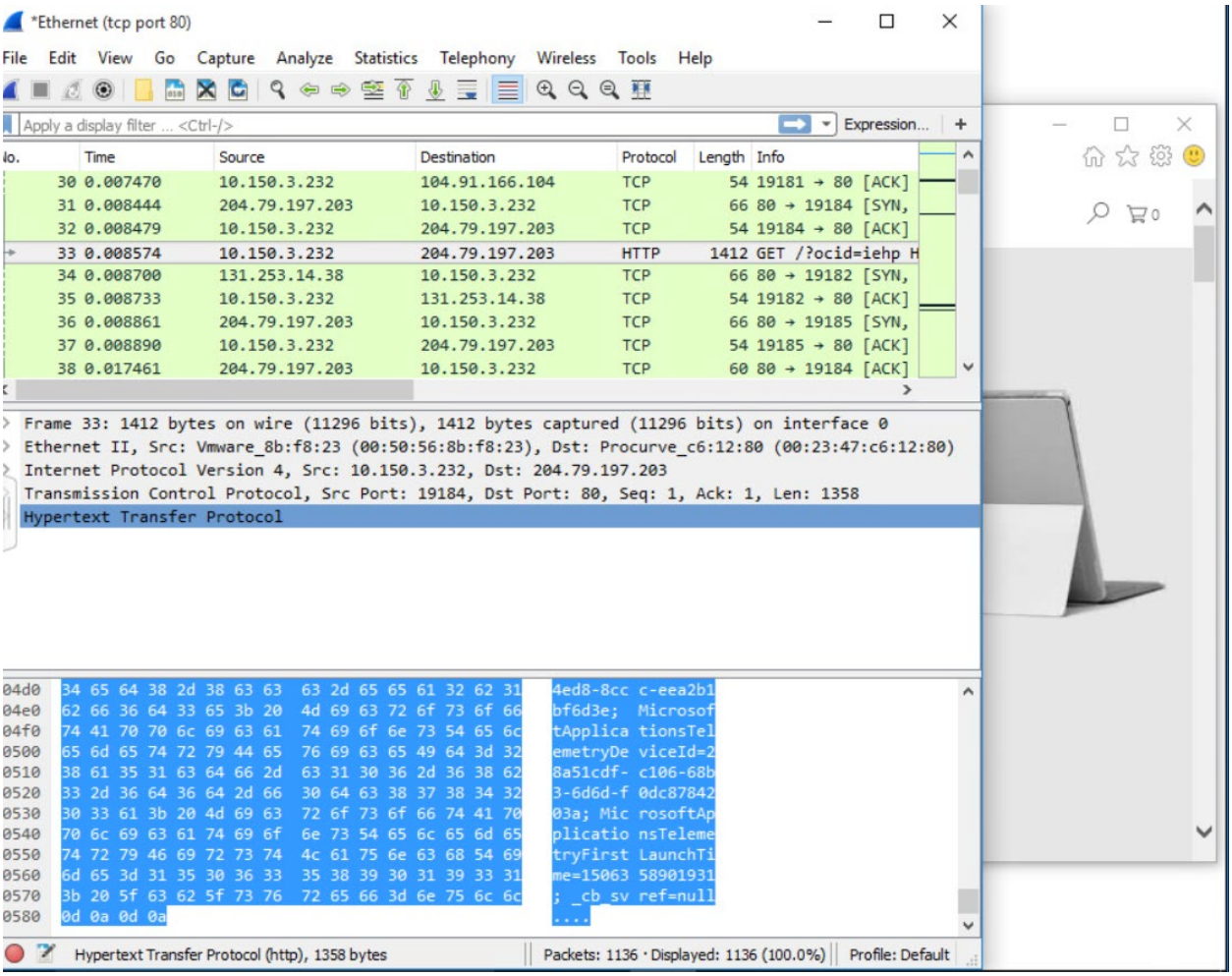


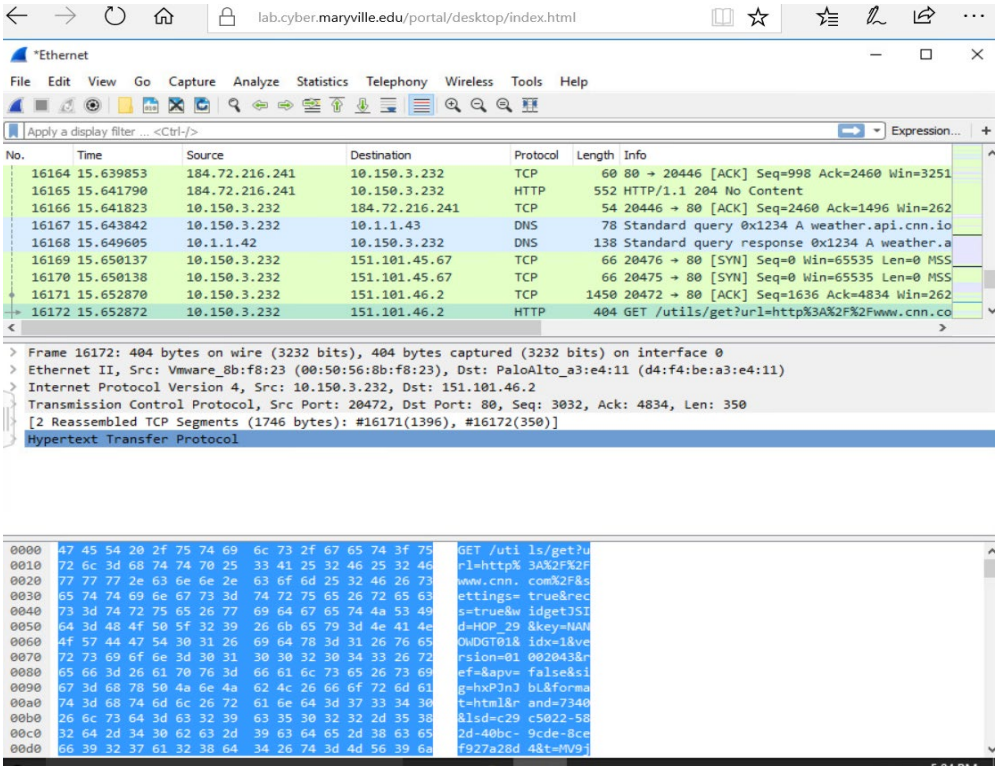




10.2 Capture Web Traffic (Wireshark)



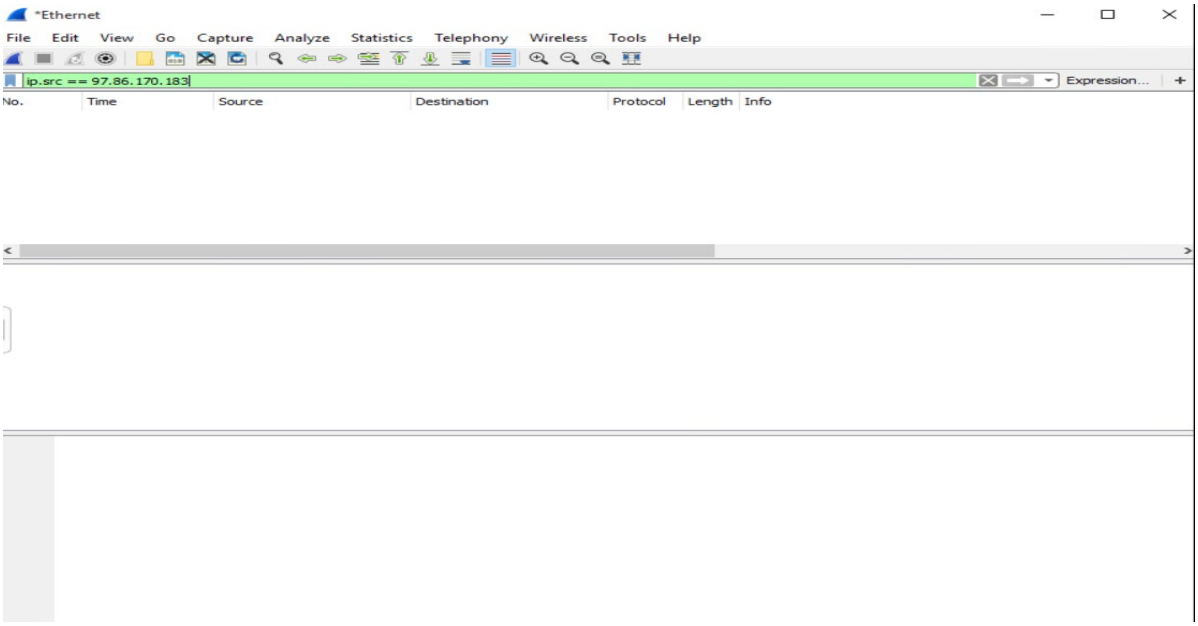

*Ethernet (tcp port 80)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
30 0.007470 10.150.3.232 104.91.166.104 TCP 54 19181 → 80 [ACK]
31 0.008444 204.79.197.203 10.150.3.232 TCP 66 80 → 19184 [SYN,
32 0.008479 10.150.3.232 204.79.197.203 TCP 54 19184 → 80 [ACK]
33 0.008574 10.150.3.232 204.79.197.203 HTTP 1412 GET /?ocid=iehp H
34 0.008700 131.253.14.38 10.150.3.232 TCP 66 80 → 19182 [SYN,
35 0.008733 10.150.3.232 131.253.14.38 TCP 54 19182 → 80 [ACK]
36 0.008861 204.79.197.203 10.150.3.232 TCP 66 80 → 19185 [SYN,
37 0.008890 10.150.3.232 204.79.197.203 TCP 54 19185 → 80 [ACK]
38 0.017461 204.79.197.203 10.150.3.232 TCP 60 80 → 19184 [ACK]
Frame 33: 1412 bytes on wire (11296 bits), 1412 bytes captured (11296 bits) on interface 0
Ethernet II, Src: Vmware_8b:f8:23 (00:50:56:8b:f8:23), Dst: Procurve_c6:12:80 (00:23:47:c6:12:80)
Internet Protocol Version 4, Src: 10.150.3.232, Dst: 204.79.197.203
Transmission Control Protocol, Src Port: 19184, Dst Port: 80, Seq: 1, Ack: 1, Len: 1358
Hypertext Transfer Protocol
04d0 34 65 64 38 2d 38 63 63 63 2d 65 65 61 32 62 31 4ed8-8cc c-eea2b1
04e0 62 66 36 64 33 65 3b 20 4d 69 63 72 6f 73 6f 66 bf6d3e; Microsof
04f0 74 41 70 70 6c 69 63 61 74 69 6f 6e 73 54 65 6c tApplica tionsTel
0500 65 6d 65 74 72 79 44 65 76 69 63 65 49 64 3d 32 emetryDe viceId=2
0510 38 61 35 31 63 64 66 2d 63 31 30 36 2d 36 38 62 8a51cdf- c106-68b
0520 33 2d 36 64 36 64 2d 66 30 64 63 38 37 38 34 32 3-6d6d-f 0dc87842
0530 30 33 61 3b 20 4d 69 63 72 6f 73 6f 66 74 41 70 03a; Mic rosoftAp
0540 70 6c 69 63 61 74 69 6f 6e 73 54 65 6c 65 6d 65 plicatio nsTeleme
0550 74 72 79 46 69 72 73 74 4c 61 75 6e 63 68 54 69 tryFirst LaunchTi
0560 6d 65 3d 31 35 30 36 33 35 38 39 30 31 39 33 31 me=15063 58901931
0570 3b 20 5f 63 62 5f 73 76 72 65 66 3d 6e 75 6c 6c ; _cb_sv ref=null
0580 0d 0a 0d 0a ....
Hypertext Transfer Protocol (http), 1358 bytes
Packets: 1136 · Displayed: 1136 (100.0%)
Profile: Default

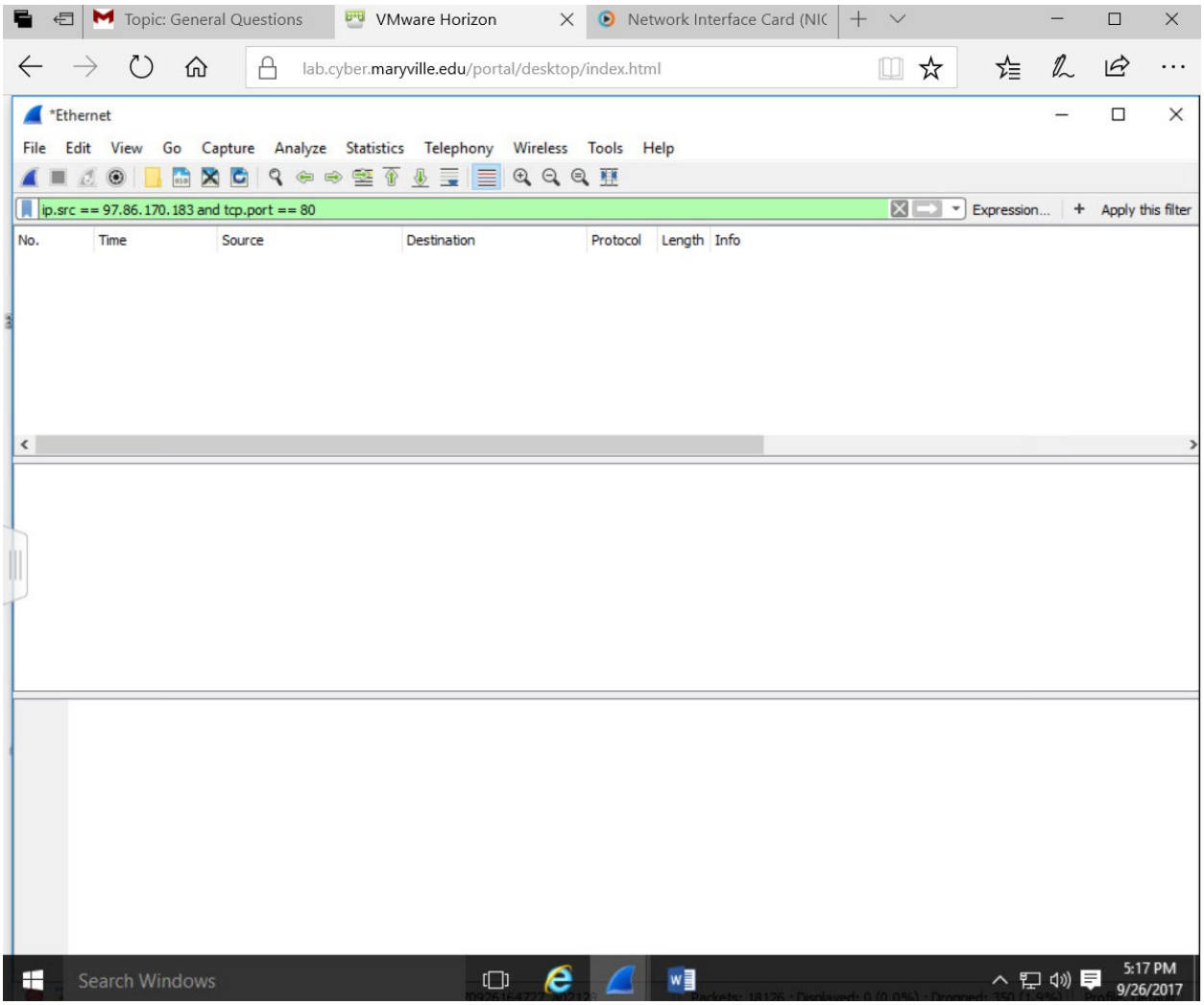
## 10.4 Display Filtering (Wireshark)



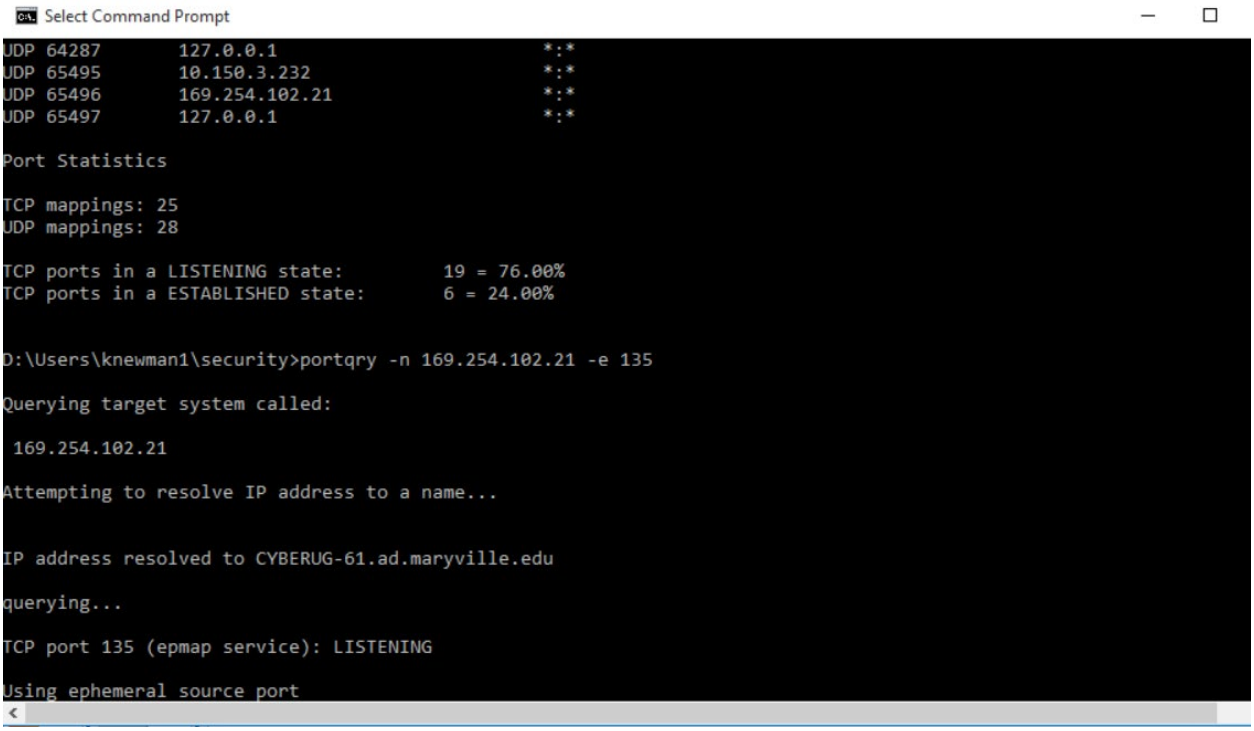


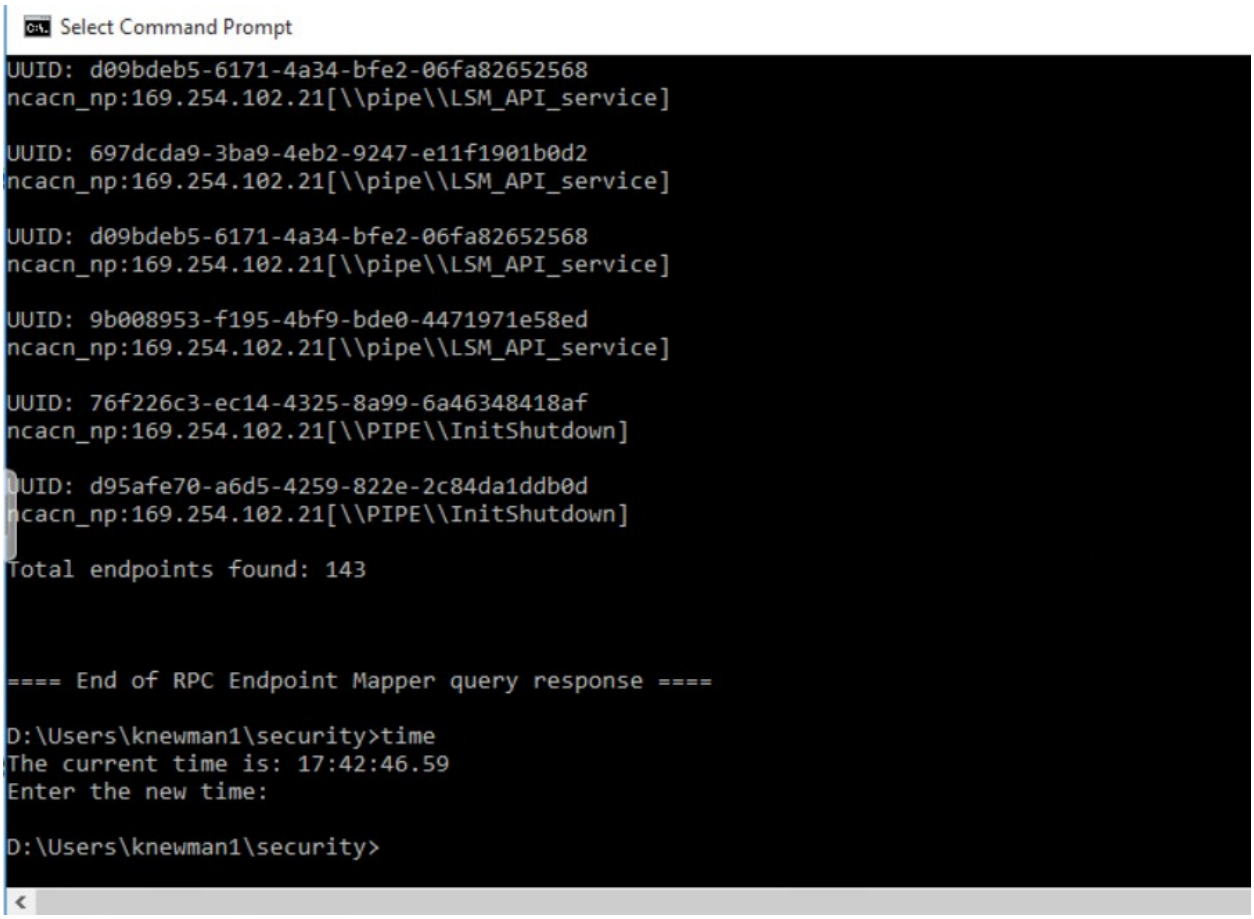


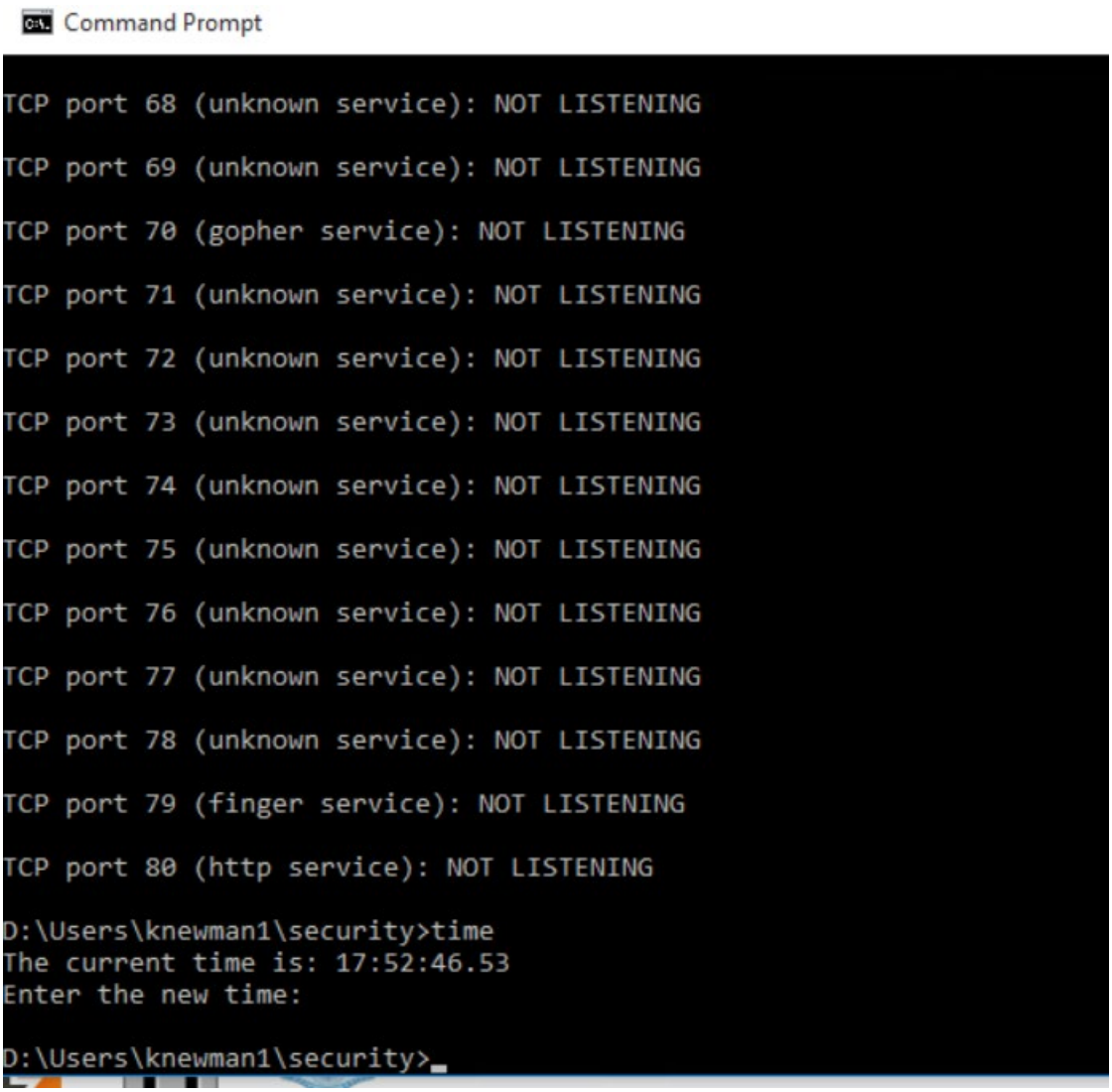



Topic: General Questions
VMware Horizon
Network Interface Card (NIC
lab.cyber.maryville.edu/portal/desktop/index.html
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src == 97.86.170.183 and tcp.port == 80
Expression...
Apply this filter
No. Time Source Destination Protocol Length Info
Search Windows
5:17 PM
9/26/2017

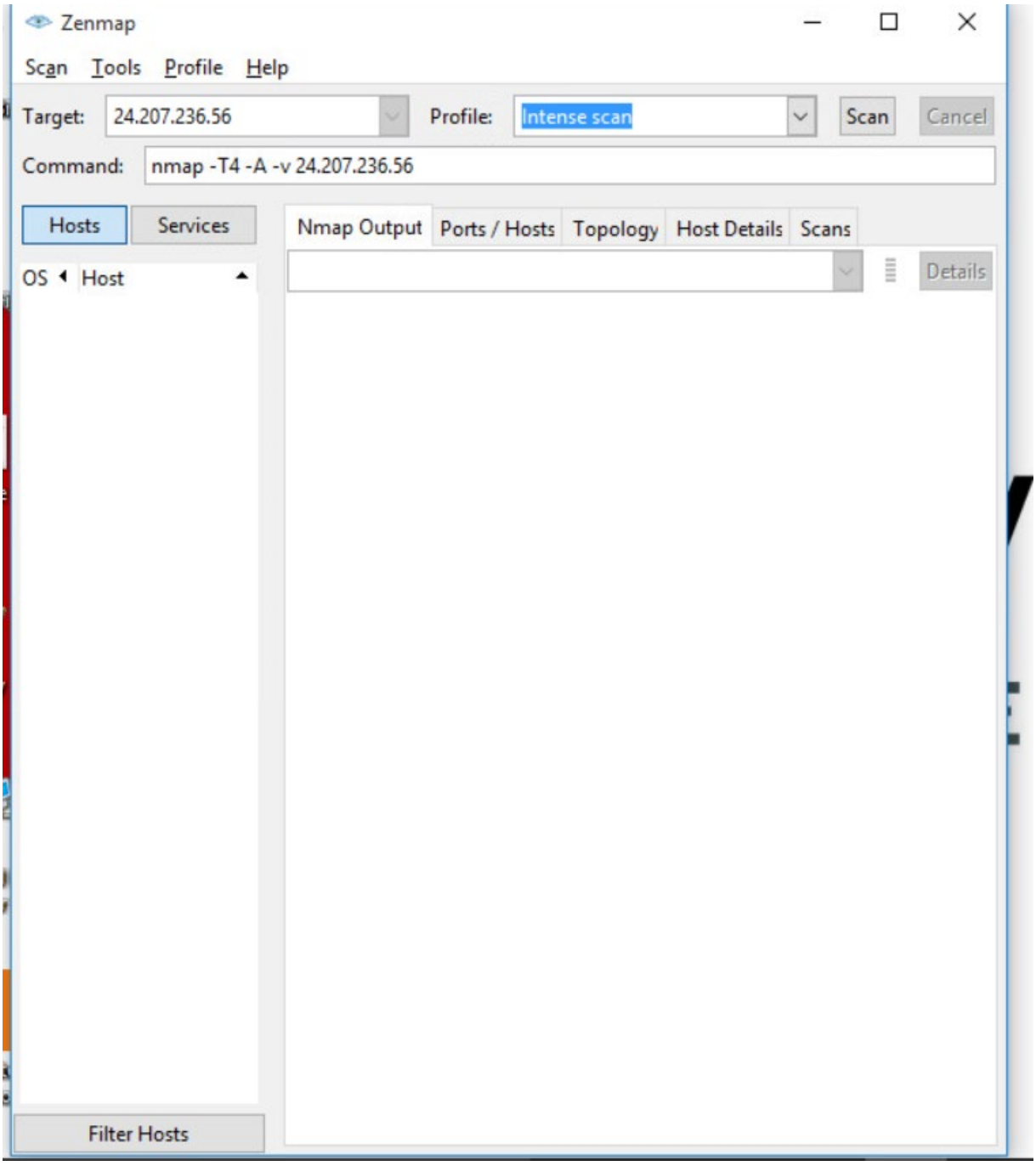
11.1 PORTQRY

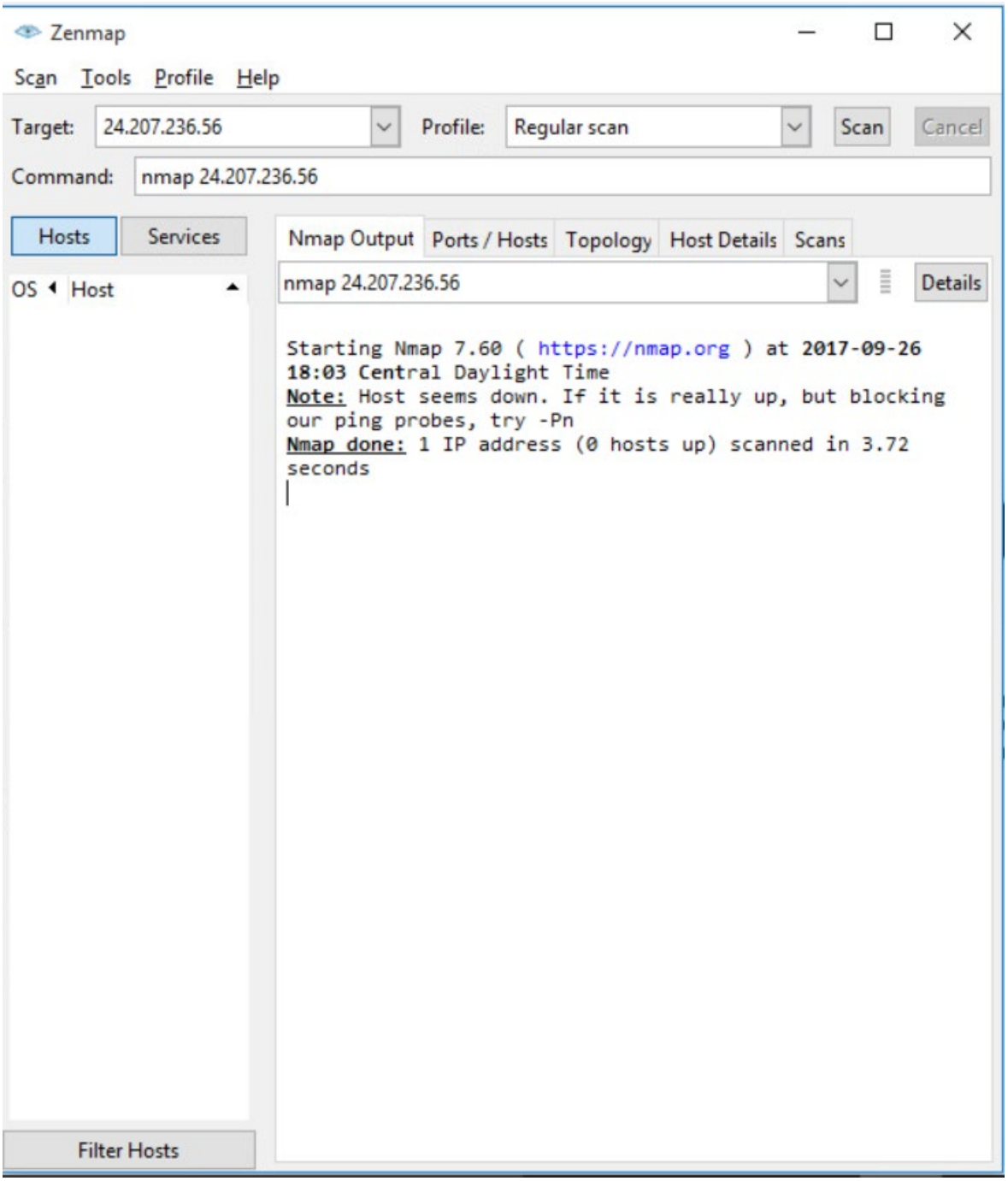

Select Command Prompt
UDP 64287 127.0.0.1 *:*
UDP 65495 10.150.3.232 *:*
UDP 65496 169.254.102.21 *:*
UDP 65497 127.0.0.1 *:*
Port Statistics
TCP mappings: 25
UDP mappings: 28
TCP ports in a LISTENING state: 19 = 76.00%
TCP ports in a ESTABLISHED state: 6 = 24.00%
D:\Users\knewman1\security>portqry -n 169.254.102.21 -e 135
Querying target system called:
169.254.102.21
Attempting to resolve IP address to a name...
IP address resolved to CYBERUG-61.ad.maryville.edu
querying...
TCP port 135 (epmap service): LISTENING
Using ephemeral source port

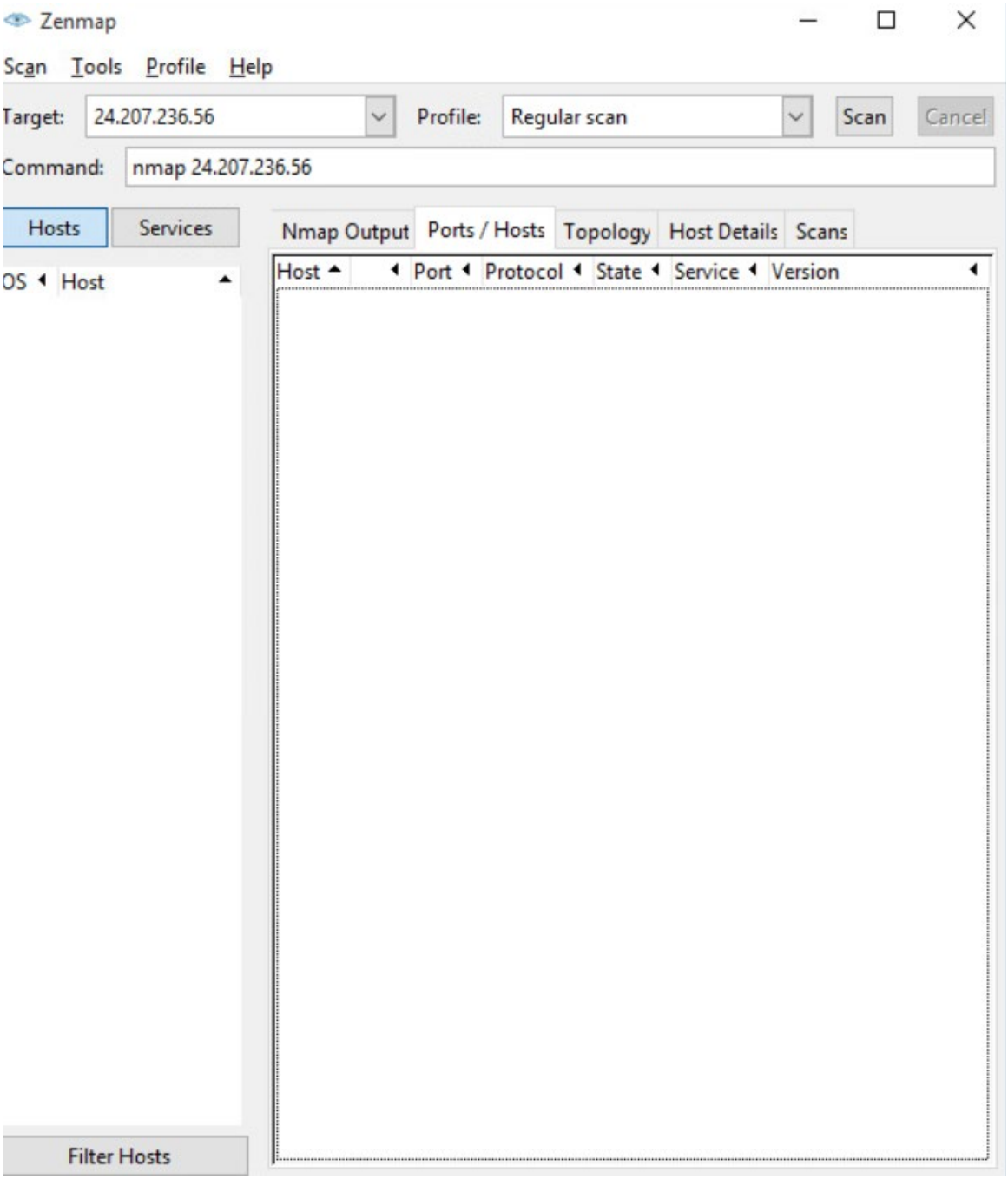

Select Command Prompt
UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568
ncacn_np:169.254.102.21[\\pipe\\LSM_API_service]
UUID: 697dcda9-3ba9-4eb2-9247-e11f1901b0d2
ncacn_np:169.254.102.21[\\pipe\\LSM_API_service]
UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568
ncacn_np:169.254.102.21[\\pipe\\LSM_API_service]
UUID: 9b008953-f195-4bf9-bde0-4471971e58ed
ncacn_np:169.254.102.21[\\pipe\\LSM_API_service]
UUID: 76f226c3-ec14-4325-8a99-6a46348418af
ncacn_np:169.254.102.21[\\PIPE\\InitShutdown]
UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d
ncacn_np:169.254.102.21[\\PIPE\\InitShutdown]
Total endpoints found: 143
==== End of RPC Endpoint Mapper query response ====
D:\Users\knewman1\security>time
The current time is: 17:42:46.59
Enter the new time:
D:\Users\knewman1\security>

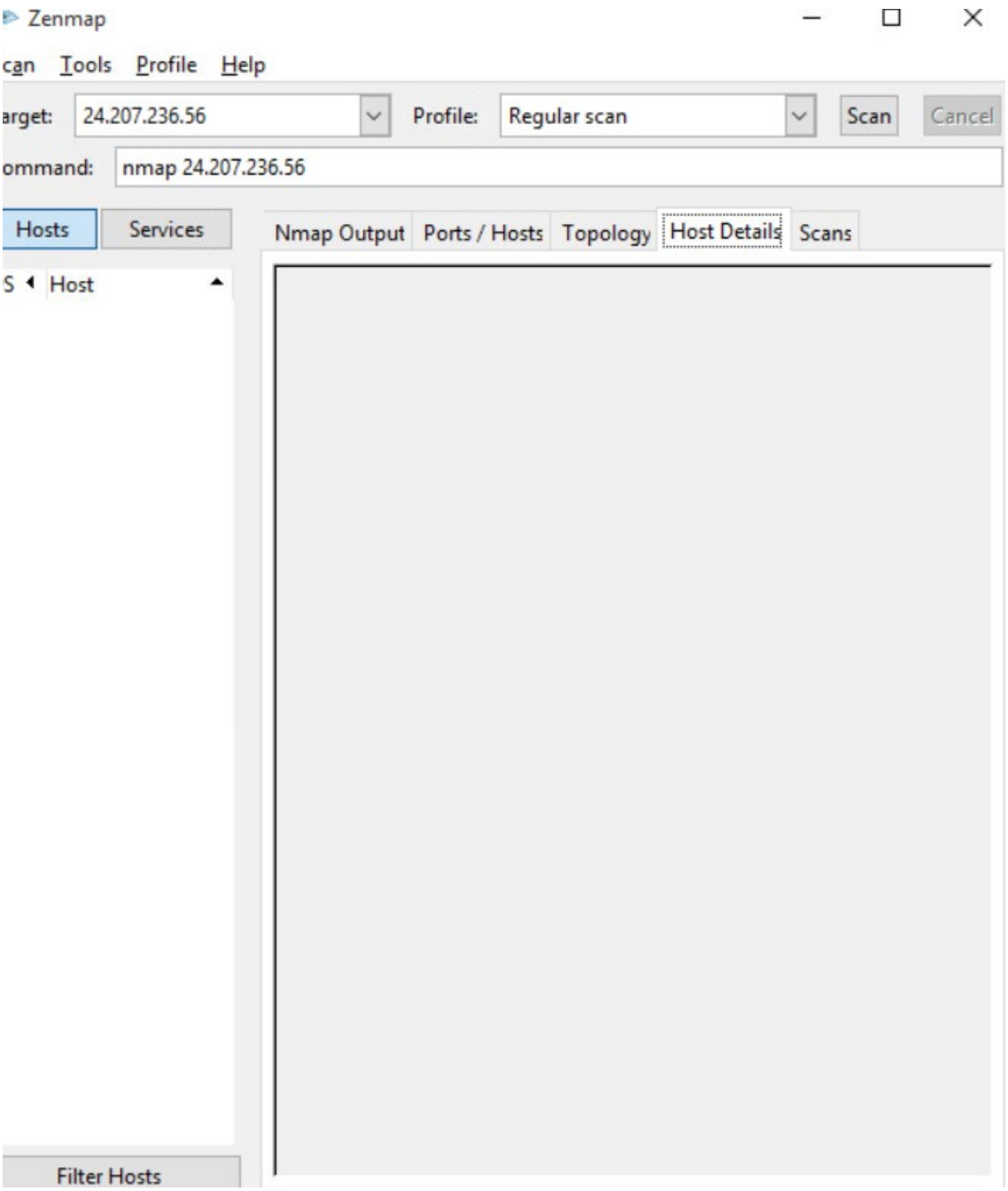

Command Prompt
TCP port 68 (unknown service): NOT LISTENING
TCP port 69 (unknown service): NOT LISTENING
TCP port 70 (gopher service): NOT LISTENING
TCP port 71 (unknown service): NOT LISTENING
TCP port 72 (unknown service): NOT LISTENING
TCP port 73 (unknown service): NOT LISTENING
TCP port 74 (unknown service): NOT LISTENING
TCP port 75 (unknown service): NOT LISTENING
TCP port 76 (unknown service): NOT LISTENING
TCP port 77 (unknown service): NOT LISTENING
TCP port 78 (unknown service): NOT LISTENING
TCP port 79 (finger service): NOT LISTENING
TCP port 80 (http service): NOT LISTENING
D:\Users\knewman1\security>time
The current time is: 17:52:46.53
Enter the new time:
D:\Users\knewman1\security>

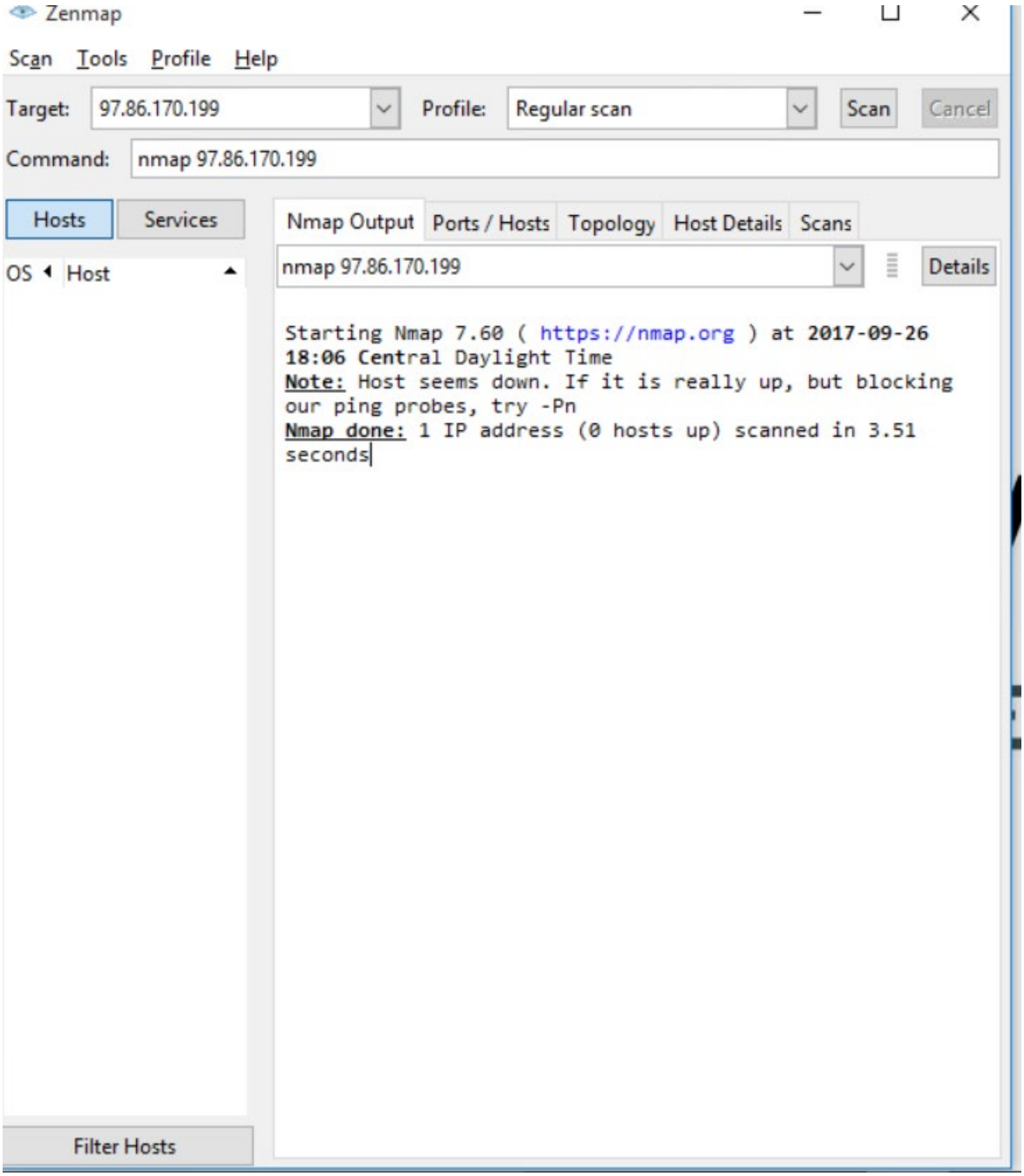
11.2 NMAP


Zenmap
Scan Tools Profile Help
Target: 24.207.236.56
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 24.207.236.56
Hosts
Services
OS Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
Filter Hosts

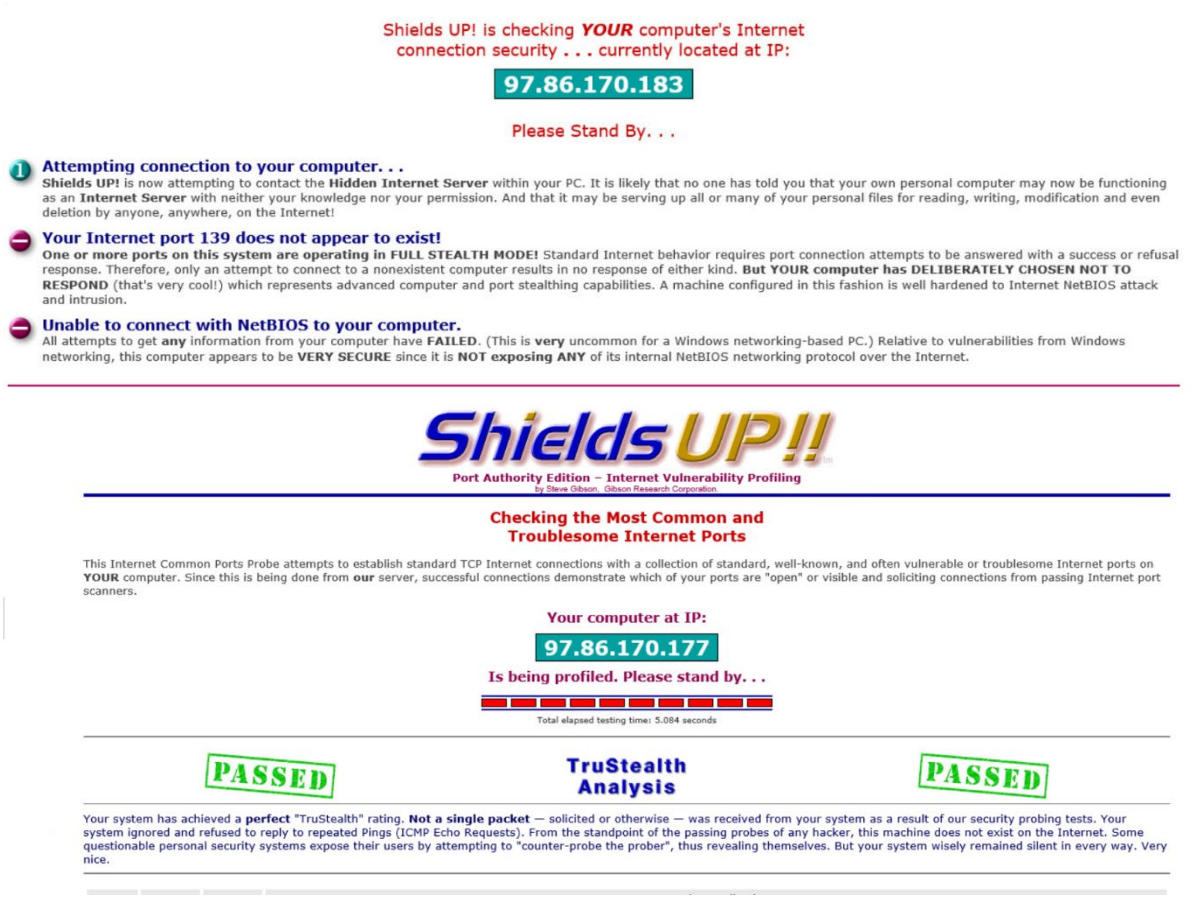

Zenmap
Scan Tools Profile Help
Target: 24.207.236.56
Profile: Regular scan
Scan
Cancel
Command: nmap 24.207.236.56
Hosts
Services
OS Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap 24.207.236.56
Details
Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-26 18:03 Central Daylight Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.72 seconds
Filter Hosts


Zenmap
Scan Tools Profile Help
Target: 24.207.236.56
Profile: Regular scan
Scan
Cancel
Command: nmap 24.207.236.56
Hosts
Services
OS
Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Host
Port
Protocol
State
Service
Version
Filter Hosts


Zenmap
can Tools Profile Help
arget: 24.207.236.56
Profile: Regular scan
Scan
Cancel
ommand: nmap 24.207.236.56
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
S Host
Filter Hosts


Zenmap
Scan Tools Profile Help
Target: 97.86.170.199
Profile: Regular scan
Scan
Cancel
Command: nmap 97.86.170.199
Hosts
Services
OS Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap 97.86.170.199
Details
Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-26 18:06 Central Daylight Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.51 seconds
Filter Hosts

11.6 Shields Up



Shields UP! is checking ***YOUR*** computer's Internet connection security . . . currently located at IP:

**97.86.170.183**

Please Stand By. . .

**Attempting connection to your computer. . .**
**Shields UP!** is now attempting to contact the **Hidden Internet Server** within your PC. It is likely that no one has told you that your own personal computer may now be functioning as an **Internet Server** with neither your knowledge nor your permission. And that it may be serving up all or many of your personal files for reading, writing, modification and even deletion by anyone, anywhere, on the Internet!

**Your Internet port 139 does not appear to exist!**
**One or more ports on this system are operating in FULL STEALTH MODE!** Standard Internet behavior requires port connection attempts to be answered with a success or refusal response. Therefore, only an attempt to connect to a nonexistent computer results in no response of either kind. **But YOUR computer has DELIBERATELY CHOSEN NOT TO RESPOND** (that's very cool!) which represents advanced computer and port stealthing capabilities. A machine configured in this fashion is well hardened to Internet NetBIOS attack and intrusion.

**Unable to connect with NetBIOS to your computer.**
All attempts to get **any** information from your computer have **FAILED**. (This is **very** uncommon for a Windows networking-based PC.) Relative to vulnerabilities from Windows networking, this computer appears to be **VERY SECURE** since it is **NOT exposing ANY** of its internal NetBIOS networking protocol over the Internet.

Shields UP!!

Port Authority Edition – Internet Vulnerability Profiling
by Steve Gibson, Gibson Research Corporation

**Checking the Most Common and Troublesome Internet Ports**

This Internet Common Ports Probe attempts to establish standard TCP Internet connections with a collection of standard, well-known, and often vulnerable or troublesome Internet ports on **YOUR** computer. Since this is being done from **our** server, successful connections demonstrate which of your ports are "open" or visible and soliciting connections from passing Internet port scanners.

**Your computer at IP:**

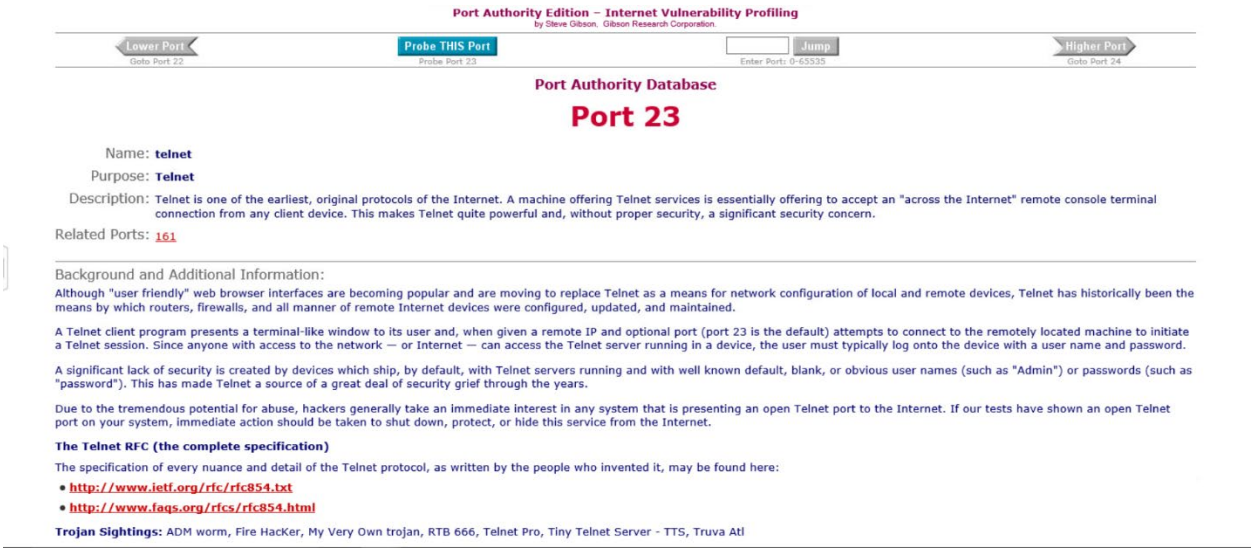
**97.86.170.177**

**Is being profiled. Please stand by. . .**

Total elapsed testing time: 5.084 seconds

PASSED — **TruStealth Analysis** — PASSED

Your system has achieved a **perfect** "TruStealth" rating. **Not a single packet** — solicited or otherwise — was received from your system as a result of our security probing tests. Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests). From the standpoint of the passing probes of any hacker, this machine does not exist on the Internet. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system wisely remained silent in every way. Very nice.



Port Authority Edition – Internet Vulnerability Profiling
by Steve Gibson. Gibson Research Corporation.

Lower Port (Goto Port 22) | Probe THIS Port (Probe Port 23) | Jump (Enter Port: 0-65535) | Higher Port (Goto Port 24)

Port Authority Database

# Port 23

Name: **telnet**

Purpose: **Telnet**

Description: Telnet is one of the earliest, original protocols of the Internet. A machine offering Telnet services is essentially offering to accept an "across the Internet" remote console terminal connection from any client device. This makes Telnet quite powerful and, without proper security, a significant security concern.

Related Ports: 161

Background and Additional Information:

Although "user friendly" web browser interfaces are becoming popular and are moving to replace Telnet as a means for network configuration of local and remote devices, Telnet has historically been the means by which routers, firewalls, and all manner of remote Internet devices were configured, updated, and maintained.

A Telnet client program presents a terminal-like window to its user and, when given a remote IP and optional port (port 23 is the default) attempts to connect to the remotely located machine to initiate a Telnet session. Since anyone with access to the network — or Internet — can access the Telnet server running in a device, the user must typically log onto the device with a user name and password.

A significant lack of security is created by devices which ship, by default, with Telnet servers running and with well known default, blank, or obvious user names (such as "Admin") or passwords (such as "password"). This has made Telnet a source of a great deal of security grief through the years.

Due to the tremendous potential for abuse, hackers generally take an immediate interest in any system that is presenting an open Telnet port to the Internet. If our tests have shown an open Telnet port on your system, immediate action should be taken to shut down, protect, or hide this service from the Internet.

**The Telnet RFC (the complete specification)**

The specification of every nuance and detail of the Telnet protocol, as written by the people who invented it, may be found here:

- http://www.ietf.org/rfc/rfc854.txt
- http://www.faqs.org/rfcs/rfc854.html

**Trojan Sightings:** ADM worm, Fire HacKer, My Very Own trojan, RTB 666, Telnet Pro, Tiny Telnet Server - TTS, Truva Atl

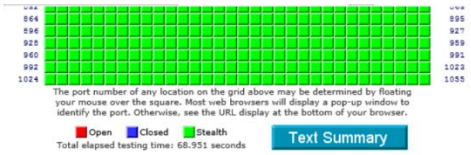
PASSED

TruStealth Analysis

PASSED

our system has achieved a **perfect** "TruStealth" rating. **Not a single packet** — solicited or otherwise — was received from your system as a result of our security probing tests. Your ystem ignored and refused to reply to repeated Pings (ICMP Echo Requests). From the standpoint of the passing probes of any hacker, this machine does not exist on the Internet. Some uestionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system wisely remained silent in every way. Very ice.

| Port | Service | Status | Security Implications |
|---|---|---|---|
| 0 | <nil> | Stealth | There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address! |
| 21 | FTP | Stealth | There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address! |
| 22 | SSH | Stealth | There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address! |
| 23 | Telnet | Stealth | There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address! |
| 25 | SMTP | Stealth | There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address! |
| 79 | Finger | Stealth | There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address! |
| 80 | HTTP | Stealth | There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address! |
| 110 | POP3 | Stealth | There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address! |
| 113 | IDENT | Stealth | There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address! |
| 119 | NNTP | Stealth | There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address! |
| 135 | RPC | Stealth | There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address! |
| 139 | Net | Stealth | There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address! |




PASSED

**TruStealth Analysis**

PASSED

Your system has achieved a **perfect** "TruStealth" rating. **Not a single packet** — solicited or otherwise — was received from your system as a result of our security probing tests. Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests). From the standpoint of the passing probes of any hacker, this machine does not exist on the Internet. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system wisely remained silent in every way. Very nice.

### Why the first 1056 Ports?

Internet ports are numbered from 1 through 65535, but the first 1023 ports are special. By tradition, and some enforcement, ports 1 through 1023 are generally reserved for the acceptance of incoming connections by services running on the receiving system. Internet services "listen" on various standard low-numbered ports so that clients wishing to have access to those services know where they may be found. Web servers traditionally listen on port 80, eMail servers listen on ports 25 and 110, FTP servers listen on port 21 and Telnet servers listen on port 23. And the list goes on. Here's the official Internet Assigned Numbers Authority (IANA) port assignment list.

Although it is possible to have higher-numbered ports listening for incoming connections, our scan of the entire "service port range" will detect all standard services running and listening on the standard service ports.

Due to the insecure behavior of Microsoft's Windows operating systems, we have added an additional 33 ports to these first 1023 ports, bringing the total to 1056. Windows has a tendency to

**Shields UP!!**

Port Authority Edition – Internet Vulnerability Profiling
by Steve Gibson, Gibson Research Corporation

**Windows Messenger**
**"Spam Yourself"**
**Test Page**

### Messenger Spam?

Yes, unfortunately . . . Microsoft Windows Messenger Spam.

I will not repeat, here, the extensive information that appears on our "**Shoot The Messenger**" page. If you are not already familiar with Windows Messenger Spam (Windows' latest security annoyance and concern) our "Shoot The Messenger" page provides the entire story and offers another of my free, tiny Windows utilities to assist with managing the problem. Please check it out.

You are presumably here because you already understand the problem created by Microsoft's various servers that are open and running, by default, on port 135. So you would either like to verify that Windows Messenger spam can not reach the system you are currently using, or you are just curious and want to play around with it a bit — receiving Windows Messenger packets from someone you trust — before returning to your regular, secure, and Messenger-Spam-free environment.

**So . . . Spam Yourself:**

The button below will send four small UDP-protocol Internet packets to port 135 of your computer, currently located at IP address "**97.86.170.177**". Four packets are sent in case one or more are lost along the way. Being UDP protocol, their individual delivery is not verifiable.

Each packet will contain the text appearing in the field below. You can leave it as it is, or customize it to anything you desire:

Windows Messenger note received from www.grc.com

Spam Me with this Note

If your Internet service provider (ISP), personal computer system, personal firewall, NAT router, or network is not currently blocking UDP traffic into port 135, and if you are running a version

### Your Browser's Request for THIS Page:

Here is the entire contents of **your** browser's request for this page:

```
Cache-Control: no-cache
Connection: Keep-Alive
Content-Length: 31
Content-Type: application/x-www-form-urlencoded
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: en-US
Cookie: tpag=abtrexcrfa0z5; ppag=abtrexcrfa0z5; tcss=abtrexcrfa0z5; pcss=abtrexcrfa0z5
Host: www.grc.com
Referer: https://www.grc.com/x/ne.dll?rh1dkyd2
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
FirstParty: https://www.grc.com
ThirdParty: https://www.grctech.com
Secure: https://www.grc.com
Nonsecure: http://www.grc.com
Session: fvgy1o4iygv0f
```

This information may be easily marked and copied for subsequent pasting.