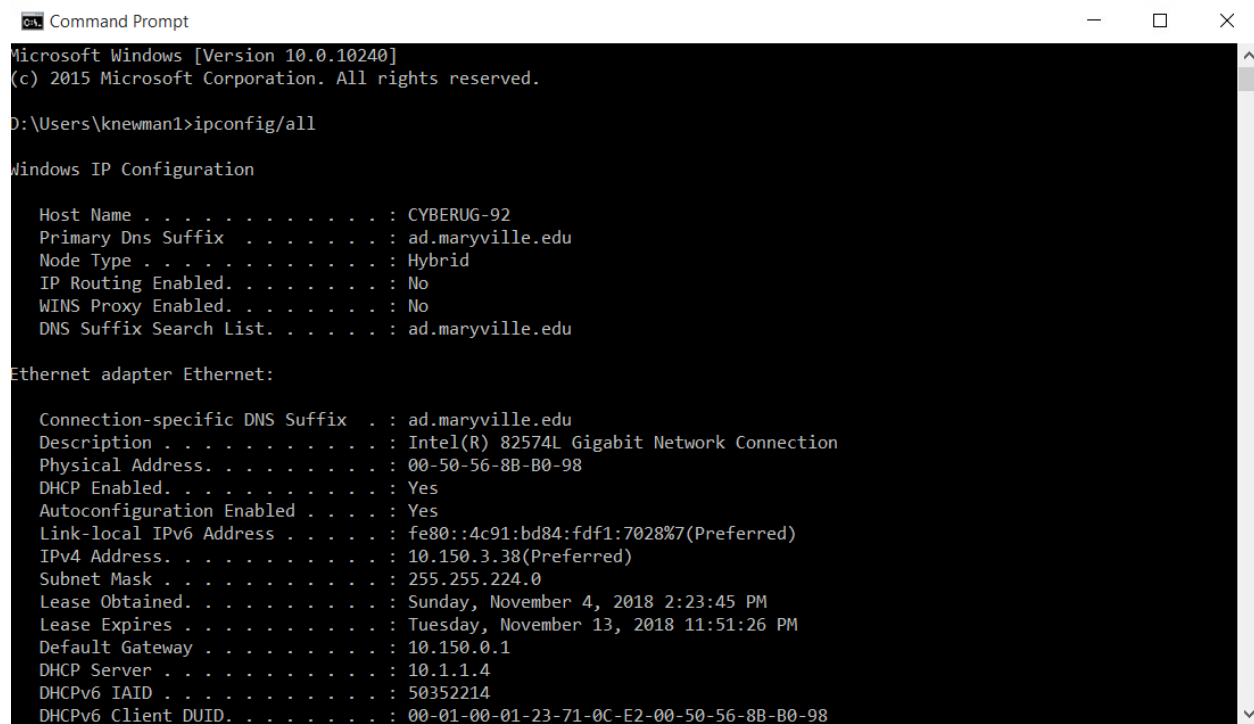


Use the tool **ipconfig** on your Virtual Machine (VM) to determine the following:

1. Your MAC address
2. Your Default Gateway
3. Your IP Address
4. Your Subnet Mask
5. Your DHCP Server



```
Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

D:\Users\knewman1>ipconfig/all

Windows IP Configuration

Host Name . . . . . : CYBERUG-92
Primary Dns Suffix . . . . . : ad.maryville.edu
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : ad.maryville.edu

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : ad.maryville.edu
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-50-56-8B-B0-98
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4c91:bd84:fd1:7028%7(Preferred)
IPv4 Address. . . . . : 10.150.3.38(Preferred)
Subnet Mask . . . . . : 255.255.224.0
Lease Obtained. . . . . : Sunday, November 4, 2018 2:23:45 PM
Lease Expires . . . . . : Tuesday, November 13, 2018 11:51:26 PM
Default Gateway . . . . . : 10.150.0.1
DHCP Server . . . . . : 10.1.1.4
DHCPv6 IAID . . . . . : 50352214
DHCPv6 Client DUID. . . . . : 00-01-00-01-23-71-0C-E2-00-50-56-8B-B0-98
```

```
Command Prompt

DHCPv6 Client DUID. . . . . : 00-01-00-01-23-71-0C-E2-00-50-56-8B-B0-98
DNS Servers . . . . . : 10.1.1.4
                        10.1.1.35
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Npcap Loopback Adapter:

Connection-specific DNS Suffix . :
Description . . . . . : Npcap Loopback Adapter
Physical Address. . . . . : 02-00-4C-4F-4F-50
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::a8c6:798:dd6f:69c3%4(Preferred)
Autoconfiguration IPv4 Address. . : 169.254.105.195(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 218234956
DHCPv6 Client DUID. . . . . : 00-01-00-01-23-71-0C-E2-00-50-56-8B-B0-98
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{86488BD5-B26B-43FC-9CB5-A23244F66974}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
```

```
Command Prompt

Tunnel adapter isatap.{86488BD5-B26B-43FC-9CB5-A23244F66974}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Tunnel adapter isatap.ad.maryville.edu:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : ad.maryville.edu
Description . . . . . : Microsoft ISATAP Adapter #3
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

D:\Users\knewman1>
```


2. During troubleshooting, you notice a domain with a .rocks at the end, such as test.rocks

1. What does the **.rocks** represent?

.rocks represents the domain

2. Where did you go to look this up?

I went to the Internet Assigned Numbers Authority and searched for the domain.



Internet Assigned Numbers Authority

DOMAINS NUMBERS PROTOCOLS ABOUT US

Domain Names

Overview

Root Zone Management

Overview

Root Database

Hint and Zone Files

Change Requests

Instructions & Guides

Root Servers

.INT Registry

.ARPA Registry

IDN Practices Repository

Root Key Signing Key (DNSSEC)

Reserved Domains

Delegation Record for .ROCKS

(Generic top-level domain)

Sponsoring Organisation

United TLD Holdco, LTD.
One Clarendon Row
Dublin 2, Co. Dublin
Ireland

Administrative Contact

Serina Ness
Donuts Inc.
Donuts Inc.
5808 Lake Washington Blvd NE, Suite 300
Kirkland, WA 98033
United States
Email: serina@donuts.email
Voice: +1.425.283.8248
Fax: +1.425.671.0020

Technical Contact

Technical Contact

Ben Levac
Donuts Inc.
Donuts Inc.
5808 Lake Washington Blvd NE, Suite 300
Kirkland, WA 98033
United States
Email: ben@donuts.email
Voice: +1.425.298.2200
Fax: +1.425.671.0020

Name Servers

HOST NAME	IP ADDRESS(ES)
demand.alpha.aridns.net.au	37.209.192.7 2001:dcd:1:0:0:0:0:7
demand.delta.aridns.net.au	37.209.198.7 2001:dcd:4:0:0:0:0:7
demand.beta.aridns.net.au	37.209.194.7 2001:dcd:2:0:0:0:0:7
demand.gamma.aridns.net.au	37.209.196.7 2001:dcd:3:0:0:0:0:7

Registry Information

URL for registration services: <http://www.donuts.domains/>
WHOIS Server: whois.nic.rocks

IANA Reports

1. Use **nslookup** to determine the IP address for test.rocks

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

D:\Users\knewman1>nslookup www.test.rocks
Server: w2k12r2dc04fy16.ad.maryville.edu
Address: 10.1.1.4

Non-authoritative answer:
Name: www.test.rocks
Address: 89.31.143.4

D:\Users\knewman1>nslookup 89.31.143.4
Server: w2k12r2dc04fy16.ad.maryville.edu
Address: 10.1.1.4

*** w2k12r2dc04fy16.ad.maryville.edu can't find 89.31.143.4: Non-existent domain

D:\Users\knewman1>nslookup 10.1.1.4 89.31.143.4
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 89.31.143.4

DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

D:\Users\knewman1>
```

4. Who owns the domain test.rocks you discovered?

Information is Private

5. Who is the registrant contact? What is his email address?

Information is Private

ICANN WHOIS

https://whois.icann.org/en/lookup?name=www.test.rocks

Showing results for: test.rocks
Original Query: www.test.rocks

Contact Information		
Registrant Contact Name: REDACTED FOR PRIVACY Organization: Mailing Address: REDACTED FOR PRIVACY, REDACTED FOR PRIVACY REDACTED FOR PRIVACY DE Phone: REDACTED FOR PRIVACY Ext: REDACTED FOR PRIVACY Fax: REDACTED FOR PRIVACY Fax Ext: REDACTED FOR PRIVACY Email: Please query the RDDS service of the Registrar of	Admin Contact Name: REDACTED FOR PRIVACY Organization: REDACTED FOR PRIVACY Mailing Address: REDACTED FOR PRIVACY, REDACTED FOR PRIVACY REDACTED FOR PRIVACY REDACTED FOR PRIVACY Phone: REDACTED FOR PRIVACY Ext: REDACTED FOR PRIVACY Fax: REDACTED FOR PRIVACY Fax Ext: REDACTED FOR	Tech Contact Name: REDACTED FOR PRIVACY Organization: REDACTED FOR PRIVACY Mailing Address: REDACTED FOR PRIVACY, REDACTED FOR PRIVACY REDACTED FOR PRIVACY REDACTED FOR PRIVACY Phone: REDACTED FOR PRIVACY Ext: REDACTED FOR PRIVACY Fax: REDACTED FOR PRIVACY Fax Ext: REDACTED FOR

Submit a Complaint for WHOIS
[WHOIS Inaccuracy Complaint Form](#)
[WHOIS Service Complaint Form](#)
[WHOIS Compliance FAQs](#)

← → ↻ <https://whois.icann.org/en/lookup?name=www.test.rocks> ☆ ⓘ

PRIVACY Fax: REDACTED FOR PRIVACY Fax Ext: REDACTED FOR PRIVACY Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.	Phone: REDACTED FOR PRIVACY Ext: REDACTED FOR PRIVACY Fax: REDACTED FOR PRIVACY Fax Ext: REDACTED FOR PRIVACY Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.	Phone: REDACTED FOR PRIVACY Ext: REDACTED FOR PRIVACY Fax: REDACTED FOR PRIVACY Fax Ext: REDACTED FOR PRIVACY Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
--	--	--

Registrar

WHOIS Server: whois.udag.net
 URL: <http://www.united-domains.de>
 Registrar: united-domains AG
 IANA ID: 1408
 Abuse Contact Email: abuse@united-domains.de
 Abuse Contact Phone: +49.8151368670

Status

Domain Status: clientTransferProhibited
<https://icann.org/epp#clientTransferProhibited>

3. Use the tool **netstat** to determine the following:
 1. A list of all the active TCP ports your VM is listening on
 2. What is the process ID (PID) for TCP port 3389?
- 972

```

Command Prompt
1  306 ff00::/8          On-link
4  266 ff00::/8          On-link
7  266 ff00::/8          On-link
=====
Persistent Routes:
None

C:\Users\knewman1>netstat -ao

Active Connections

Proto Local Address           Foreign Address         State       PID
TCP   0.0.0.0:135             CYBERUG-92:0           LISTENING   844
TCP   0.0.0.0:445             CYBERUG-92:0           LISTENING   4
TCP   0.0.0.0:1536            CYBERUG-92:0           LISTENING   528
TCP   0.0.0.0:1537            CYBERUG-92:0           LISTENING   672
TCP   0.0.0.0:1538            CYBERUG-92:0           LISTENING   288
TCP   0.0.0.0:1546            CYBERUG-92:0           LISTENING   1268
TCP   0.0.0.0:1548            CYBERUG-92:0           LISTENING   2144
TCP   0.0.0.0:1549            CYBERUG-92:0           LISTENING   1244
TCP   0.0.0.0:1550            CYBERUG-92:0           LISTENING   672
TCP   0.0.0.0:1580            CYBERUG-92:0           LISTENING   664
TCP   0.0.0.0:3306            CYBERUG-92:0           LISTENING   3152
TCP   0.0.0.0:3389            CYBERUG-92:0           LISTENING   972
TCP   0.0.0.0:4000            CYBERUG-92:0           LISTENING   3128
TCP   0.0.0.0:7680            CYBERUG-92:0           LISTENING   1268
TCP   0.0.0.0:8000            CYBERUG-92:0           LISTENING   3224
TCP   0.0.0.0:8089            CYBERUG-92:0           LISTENING   3224
TCP   0.0.0.0:8191            CYBERUG-92:0           LISTENING   4844
TCP   0.0.0.0:9427            CYBERUG-92:0           LISTENING   1120
  
```

Command Prompt

TCP	0.0.0.0:135	CYBERUG-92:0	LISTENING	844
TCP	0.0.0.0:445	CYBERUG-92:0	LISTENING	4
TCP	0.0.0.0:1536	CYBERUG-92:0	LISTENING	528
TCP	0.0.0.0:1537	CYBERUG-92:0	LISTENING	672
TCP	0.0.0.0:1538	CYBERUG-92:0	LISTENING	288
TCP	0.0.0.0:1546	CYBERUG-92:0	LISTENING	1268
TCP	0.0.0.0:1548	CYBERUG-92:0	LISTENING	2144
TCP	0.0.0.0:1549	CYBERUG-92:0	LISTENING	1244
TCP	0.0.0.0:1550	CYBERUG-92:0	LISTENING	672
TCP	0.0.0.0:1580	CYBERUG-92:0	LISTENING	664
TCP	0.0.0.0:3306	CYBERUG-92:0	LISTENING	3152
TCP	0.0.0.0:3389	CYBERUG-92:0	LISTENING	972
TCP	0.0.0.0:4000	CYBERUG-92:0	LISTENING	3128
TCP	0.0.0.0:7680	CYBERUG-92:0	LISTENING	1268
TCP	0.0.0.0:8000	CYBERUG-92:0	LISTENING	3224
TCP	0.0.0.0:8089	CYBERUG-92:0	LISTENING	3224
TCP	0.0.0.0:8191	CYBERUG-92:0	LISTENING	4844
TCP	0.0.0.0:9427	CYBERUG-92:0	LISTENING	1120
TCP	0.0.0.0:22443	CYBERUG-92:0	LISTENING	2384
TCP	0.0.0.0:32111	CYBERUG-92:0	LISTENING	1120
TCP	10.150.3.38:139	CYBERUG-92:0	LISTENING	4
TCP	10.150.3.38:1585	w2k12r2csv1fy16:4002	ESTABLISHED	2892
TCP	10.150.3.38:22443	w2k12r2csv1fy16:63398	ESTABLISHED	2384
TCP	10.150.3.38:29440	w2k12r2dfs4fy17:microsoft-ds	ESTABLISHED	4
TCP	10.150.3.38:29649	176.32.110.204:http	ESTABLISHED	9976
TCP	10.150.3.38:29668	52.94.237.66:http	ESTABLISHED	9976
TCP	10.150.3.38:29669	52.46.128.194:http	ESTABLISHED	9976
TCP	10.150.3.38:29677	52.94.237.66:http	ESTABLISHED	9976
TCP	10.150.3.38:29678	52.94.237.66:http	ESTABLISHED	9976
TCP	10.150.3.38:29679	52.46.128.194:http	ESTABLISHED	9976

3. What service is running on TCP port 3389?
 Remote Desktop Services, Network Location Awareness, Workstation, DNS Client, and
 Cryptographic Services

Task Manager

File Options View

Processes Performance App history Startup Users Details **Services**

Name	PID	Description	Status	Group
PcaSvc	756	Program Compatibility Assistant Service	Running	LocalSystem
NcbService	756	Network Connection Broker	Running	LocalSystem
DsSvc	756	Data Sharing Service	Running	LocalSystem
AudioEndpointBuilder	756	Windows Audio Endpoint Builder	Running	LocalSystem
SystemEventsBroker	796	System Events Broker	Running	DcomLaunch
Power	796	Power	Running	DcomLaunch
PlugPlay	796	Plug and Play	Running	DcomLaunch
LSM	796	Local Session Manager	Running	DcomLaunch
DcomLaunch	796	DCOM Server Process Launcher	Running	DcomLaunch
BrokerInfrastructure	796	Background Tasks Infrastructure Service	Running	DcomLaunch
TimeBroker	804	Time Broker	Running	LocalService
SSDPsrv	804	SSDP Discovery	Running	LocalService
RpcSs	844	Remote Procedure Call (RPC)	Running	rpcss
RpcEptMapper	844	RPC Endpoint Mapper	Running	RPCSS
TermService	972	Remote Desktop Services	Running	NetworkService
NlaSvc	972	Network Location Awareness	Running	NetworkService
LanmanWorkstation	972	Workstation	Running	NetworkService
Dnscache	972	DNS Client	Running	NetworkService
CryptSvc	972	Cryptographic Services	Running	NetworkService
WSNM	1120	VMware Horizon View Agent	Running	
MpsSvc	1168	Windows Firewall	Running	LocalService
DPS	1168	Diagnostic Policy Service	Running	LocalService
CoreMessagingSvc	1168	CoreMessaging	Running	LocalService

⬆ Fewer details | ⚙ Open Services

4. Open a browser and connect to amazon.com. Using **netstat**, capture the connection information. What source port are you using? (Hint: to narrow down the established list, determine the PID of the browser. Consider using Task Manager as well to find the PID)

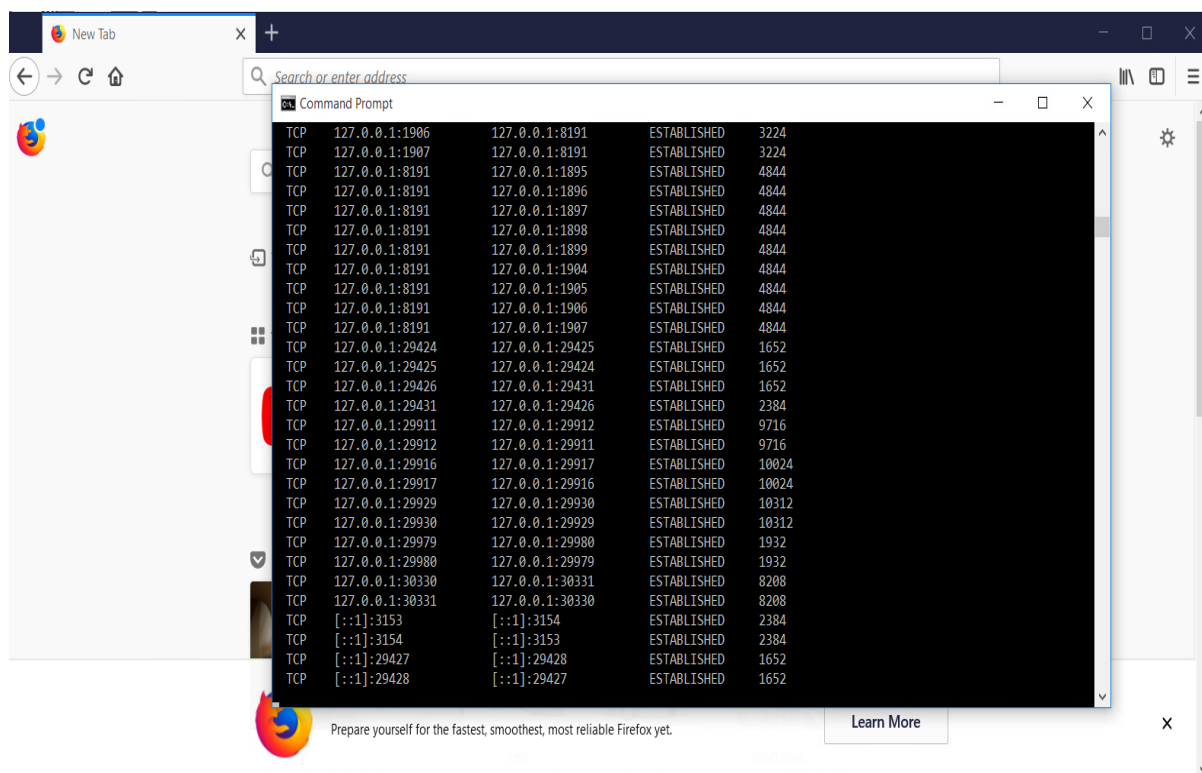
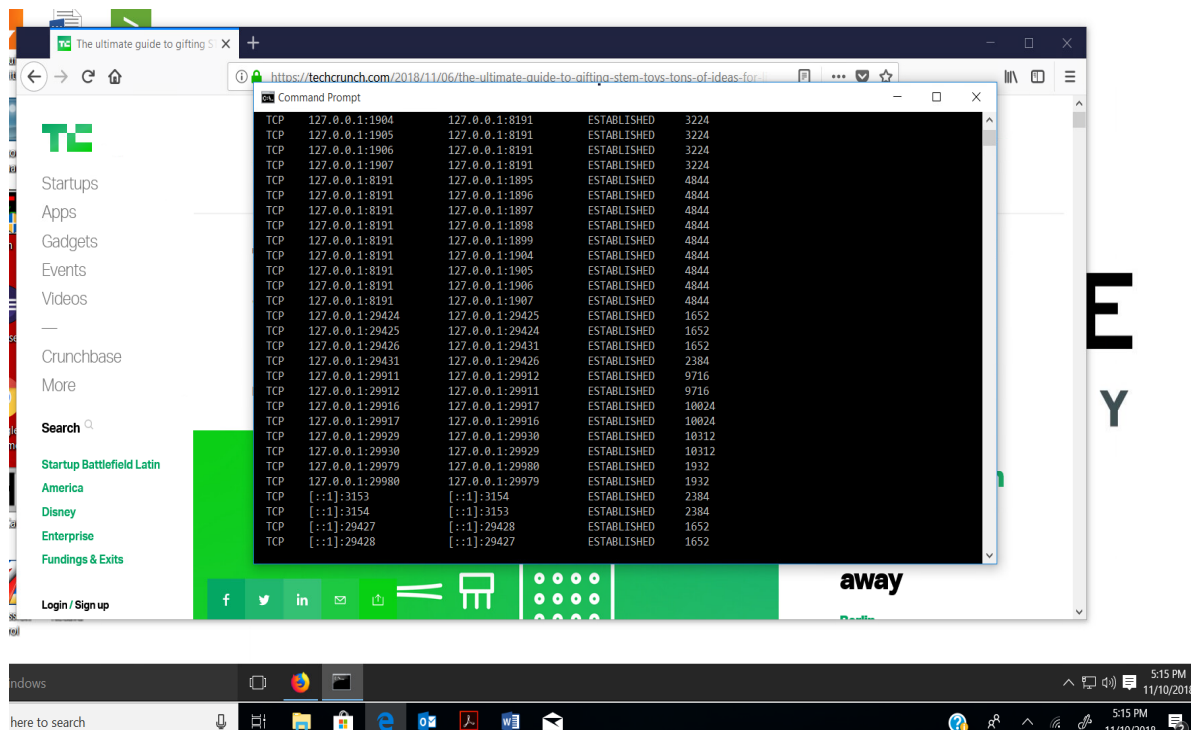
The screenshot shows a Windows desktop with three windows open. The browser window at the top displays the Amazon.com homepage. Below it, the Task Manager window is open, showing the 'Processes' tab. The 'Processes' tab lists several instances of 'chrome.exe' running. The Command Prompt window is open in the foreground, displaying the output of the 'netstat' command. The output shows a list of network connections, including the source IP address, destination IP address, destination port, and the state of the connection. The source port is listed as 4976 for the connection to Amazon.com.

Name	PID	Status	User name	CPU	Memory	Description
chrome.exe	5412	Running	kneuma...	00	1,352 K	Google Chrom...
chrome.exe	5428	Running	kneuma...	00	6,580 K	Google Chrom...
chrome.exe	5696	Running	kneuma...	00	9,968 K	Google Chrom...
chrome.exe	7460	Running	kneuma...	00	61,724 K	Google Chrom...
chrome.exe	8460	Running	kneuma...	00	8,124 K	Google Chrom...
chrome.exe	9332	Running	kneuma...	00	1,416 K	Google Chrom...
chrome.exe	9756	Running	kneuma...	00	5,252 K	Google Chrom...
chrome.exe	9976	Running	kneuma...	01	45,168 K	Google Chrom...
cmd.exe	109...	Running	kneuma...	00	19,024 K	Google Chrom...
cmd.exe	2904	Running	SYSTEM	00	452 K	Windows Com...
conhost.exe	2904	Running	SYSTEM	00	532 K	Console Wind...
conhost.exe	4456	Running	SYSTEM	00	552 K	Console Wind...
conhost.exe	7844	Running	SYSTEM	00	4,496 K	Console Wind...
conhost.exe	109...	Running	SYSTEM	00	4,968 K	Console Wind...
csrss.exe	444	Running	SYSTEM	00	800 K	Client Server F...
csrss.exe	6016	Running	SYSTEM	00	772 K	Client Server F...
dllhost.exe	4524	Running	SYSTEM	00	2,856 K	COM Surrogat...
dwm.exe	5600	Running	DWM-2	03	36,408 K	Desktop Wind...
explorer.exe	8476	Running	SYSTEM	00	13,520 K	Windows Expl...
lsass.exe	9816	Running	SYSTEM	00	2,648 K	Local Security...
lsass.exe	672	Running	SYSTEM	00	5,592 K	Local Security...
mongod.exe	4844	Running	SYSTEM	00	33,084 K	mongod
netmon.exe	4752	Running	SYSTEM	00	2,784 K	Microsoft Net...

5. If you want **netstat** to filter on connections from the Firefox browser, every 5 seconds, how would you accomplish this?

The screenshot shows a Windows desktop with three windows open. The browser window at the top displays the TechCrunch website. Below it, the Task Manager window is open, showing the 'Processes' tab. The 'Processes' tab lists several instances of 'firefox.exe' running. The Command Prompt window is open in the foreground, displaying the output of the 'netstat' command. The output shows a list of network connections, including the source IP address, destination IP address, destination port, and the state of the connection. The source port is listed as 4976 for the connection to TechCrunch.

Name	PID	Status	User name	CPU	Memory	Description
firefox.exe	5412	Running	kneuma...	00	1,352 K	Google Chrom...
firefox.exe	5428	Running	kneuma...	00	6,580 K	Google Chrom...
firefox.exe	5696	Running	kneuma...	00	9,968 K	Google Chrom...
firefox.exe	7460	Running	kneuma...	00	61,724 K	Google Chrom...
firefox.exe	8460	Running	kneuma...	00	8,124 K	Google Chrom...
firefox.exe	9332	Running	kneuma...	00	1,416 K	Google Chrom...
firefox.exe	9756	Running	kneuma...	00	5,252 K	Google Chrom...
firefox.exe	9976	Running	kneuma...	01	45,168 K	Google Chrom...
cmd.exe	109...	Running	kneuma...	00	19,024 K	Google Chrom...
cmd.exe	2904	Running	SYSTEM	00	452 K	Windows Com...
conhost.exe	2904	Running	SYSTEM	00	532 K	Console Wind...
conhost.exe	4456	Running	SYSTEM	00	552 K	Console Wind...
conhost.exe	7844	Running	SYSTEM	00	4,496 K	Console Wind...
conhost.exe	109...	Running	SYSTEM	00	4,968 K	Console Wind...
csrss.exe	444	Running	SYSTEM	00	800 K	Client Server F...
csrss.exe	6016	Running	SYSTEM	00	772 K	Client Server F...
dllhost.exe	4524	Running	SYSTEM	00	2,856 K	COM Surrogat...
dwm.exe	5600	Running	DWM-2	03	36,408 K	Desktop Wind...
explorer.exe	8476	Running	SYSTEM	00	13,520 K	Windows Expl...
lsass.exe	9816	Running	SYSTEM	00	2,648 K	Local Security...
lsass.exe	672	Running	SYSTEM	00	5,592 K	Local Security...
mongod.exe	4844	Running	SYSTEM	00	33,084 K	mongod
netmon.exe	4752	Running	SYSTEM	00	2,784 K	Microsoft Net...



Firefox is using PID's [9716, 9996, 10024, 10312, and 1932]

File Options View

Processes	Performance	App history	Startup	Users	Details	Services
Name	PID	Status	User na...	CPU	Memory ...	Description
audiodg.exe	8420	Running	LOCAL S...	00	3,320 K	Windows Audio Device Graph Isolation
conhost.exe	2904	Running	SYSTEM	00	532 K	Console Window Host
conhost.exe	4456	Running	SYSTEM	00	552 K	Console Window Host
conhost.exe	7844	Running	knewma...	00	4,496 K	Console Window Host
csrss.exe	444	Running	SYSTEM	00	804 K	Client Server Runtime Process
csrss.exe	6016	Running	SYSTEM	00	772 K	Client Server Runtime Process
dllhost.exe	4524	Running	SYSTEM	00	2,856 K	COM Surrogate
dwm.exe	5600	Running	DWM-2	00	35,228 K	Desktop Window Manager
explorer.exe	8476	Running	knewma...	00	14,500 K	Windows Explorer
firefox.exe	9716	Running	knewma...	00	151,788 K	Firefox
firefox.exe	9996	Running	knewma...	00	9,896 K	Firefox
firefox.exe	100...	Running	knewma...	00	72,924 K	Firefox
firefox.exe	103...	Running	knewma...	00	19,300 K	Firefox
firefox.exe	1932	Running	knewma...	00	154,800 K	Firefox
jusched.exe	9816	Running	knewma...	00	2,612 K	Java Update Scheduler
lsass.exe	672	Running	SYSTEM	00	5,696 K	Local Security Authority Process
mongod.exe	4844	Running	SYSTEM	00	33,084 K	mongod
msdtc.exe	4752	Running	NETWO...	00	2,084 K	Microsoft Distributed Transaction Coord...
mysqld.exe	3152	Running	NETWO...	00	153,240 K	mysqld
OneDrive.exe	7392	Running	knewma...	00	6,184 K	Microsoft OneDrive
perfhst.exe	2036	Running	LOCAL S...	00	888 K	x86 Performance Counter Host
python.exe	3040	Running	SYSTEM	00	40,268 K	python
rundll32.exe	8704	Running	knewma...	00	2,568 K	Windows host process (Rundll32)

^ Fewer details End task

4. From your VM, go to **whatismyip.com** in a browser.

1. Is your VM NAT'd?

yes

2. Use the tool **tracert** to go to the IP address shown on whatismyip.com. What are you trace routing to?

10.150.3.38 Cyberbug-92.ad.maryville.edu

3. Do you notice anything interesting (Hint: maybe a loop of some sort) in the results? Explain.

30 hops

4. What does the first IP address represent in the trace route?

The IP address connected to local host

5. Who owns the last IP address in the trace route?

Only one IP address

