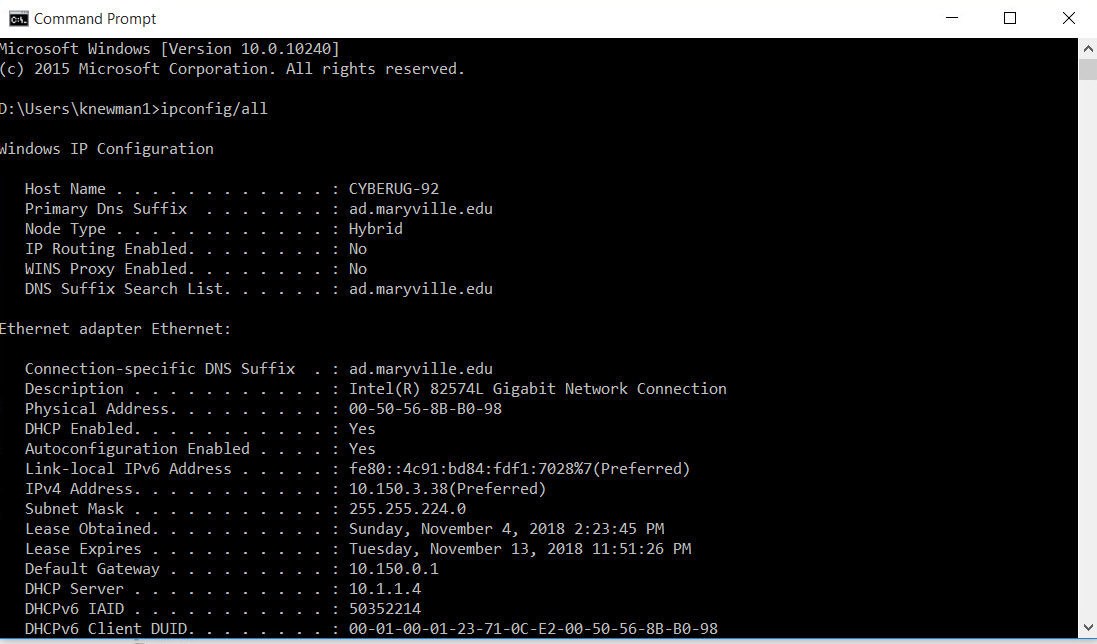
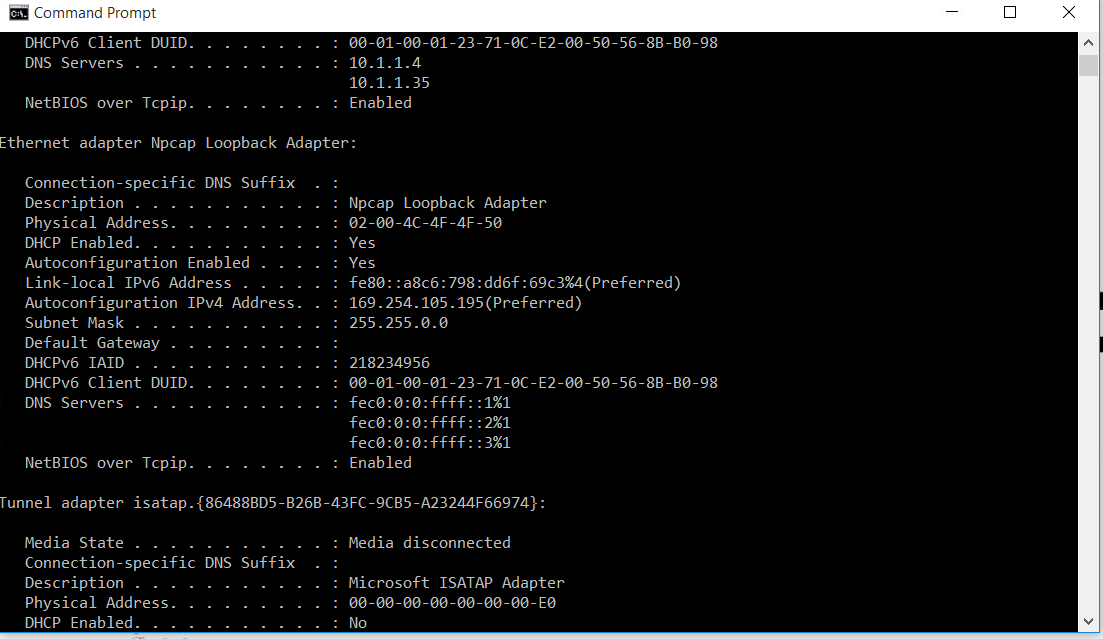
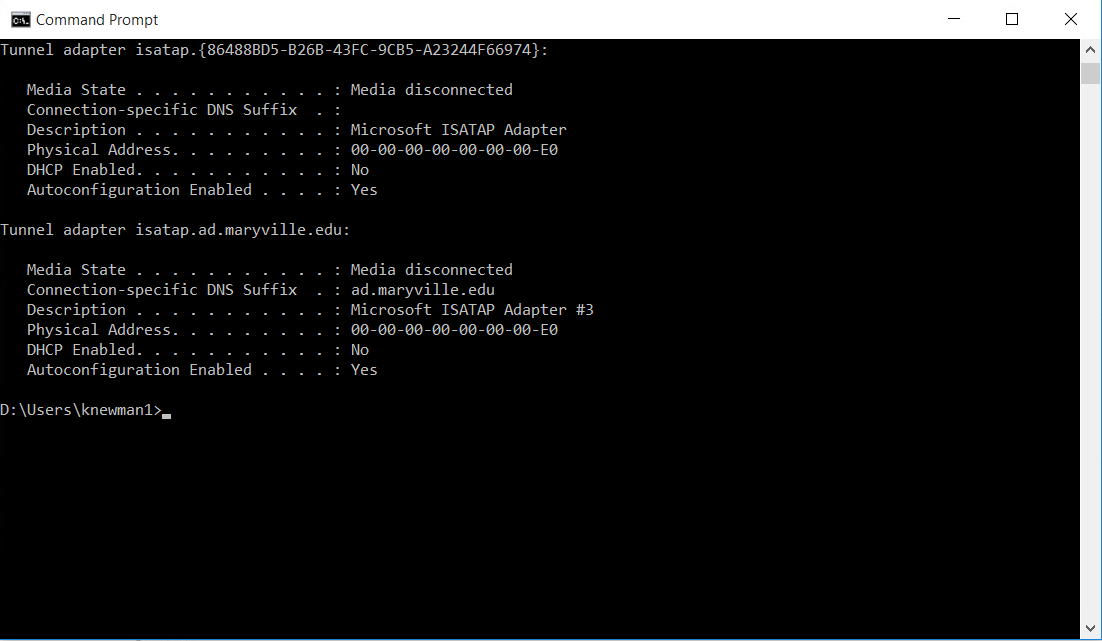
Use the tool **ipconfig** on your Virtual Machine (VM) to determine the following:

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







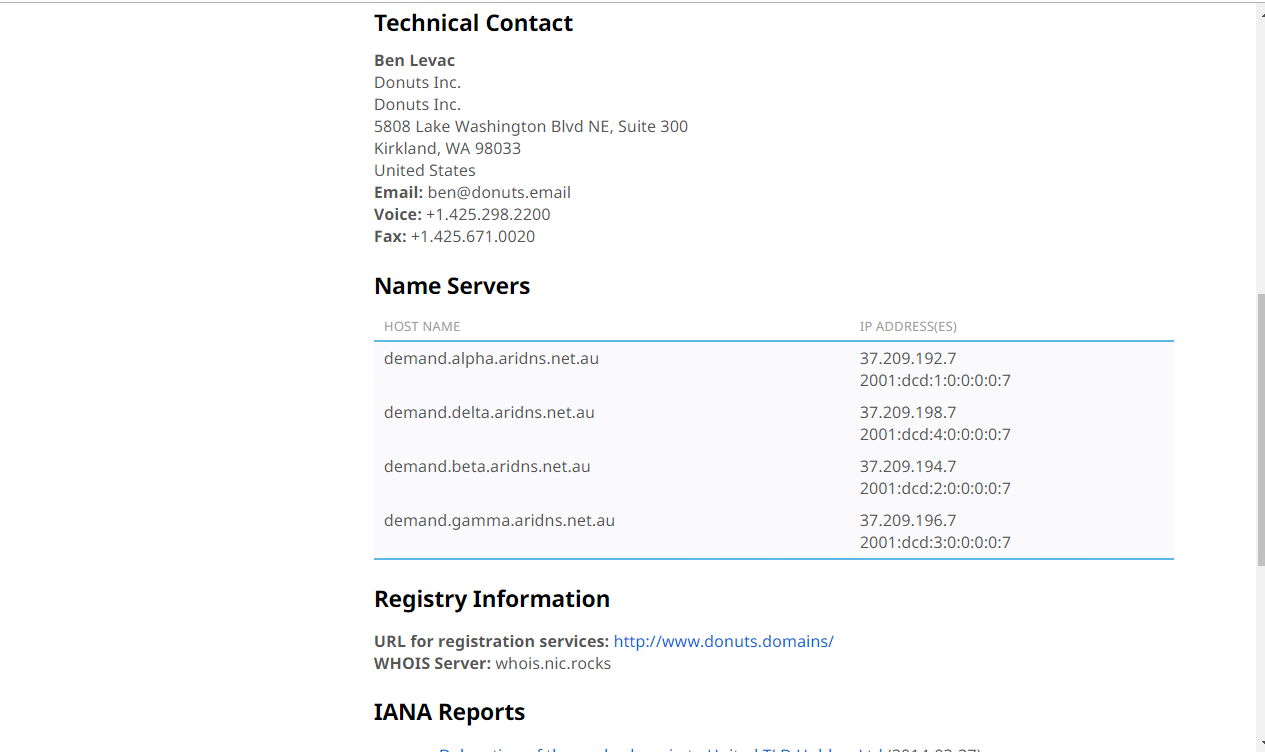
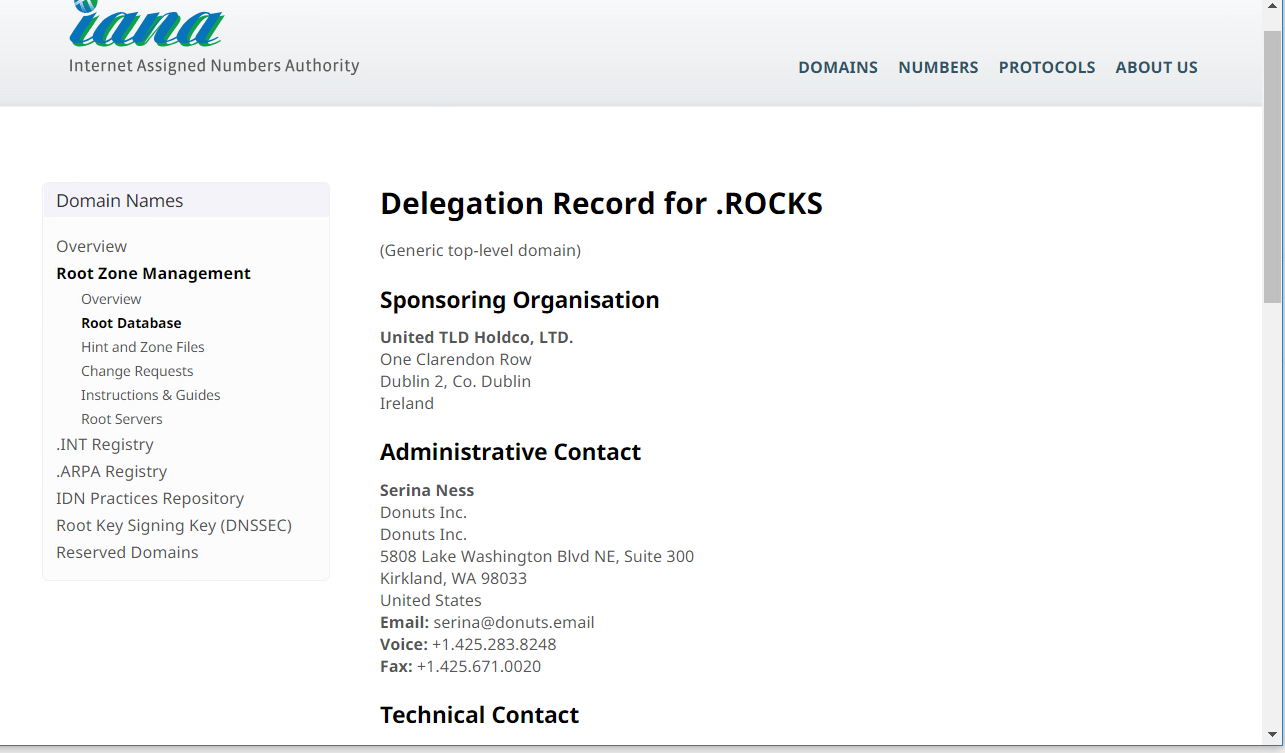
2. During troubleshooting, you notice a domain with a .rocks at the end, such as test.rocks

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

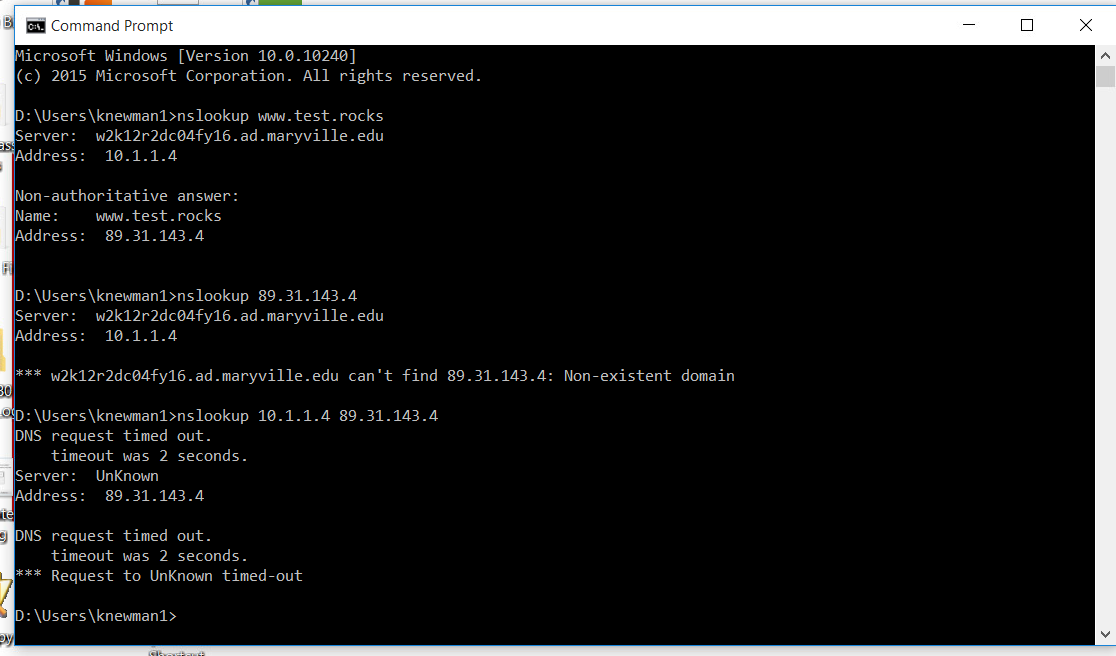
.rocks represents the domain

1. Where did you go to look this up?

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



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

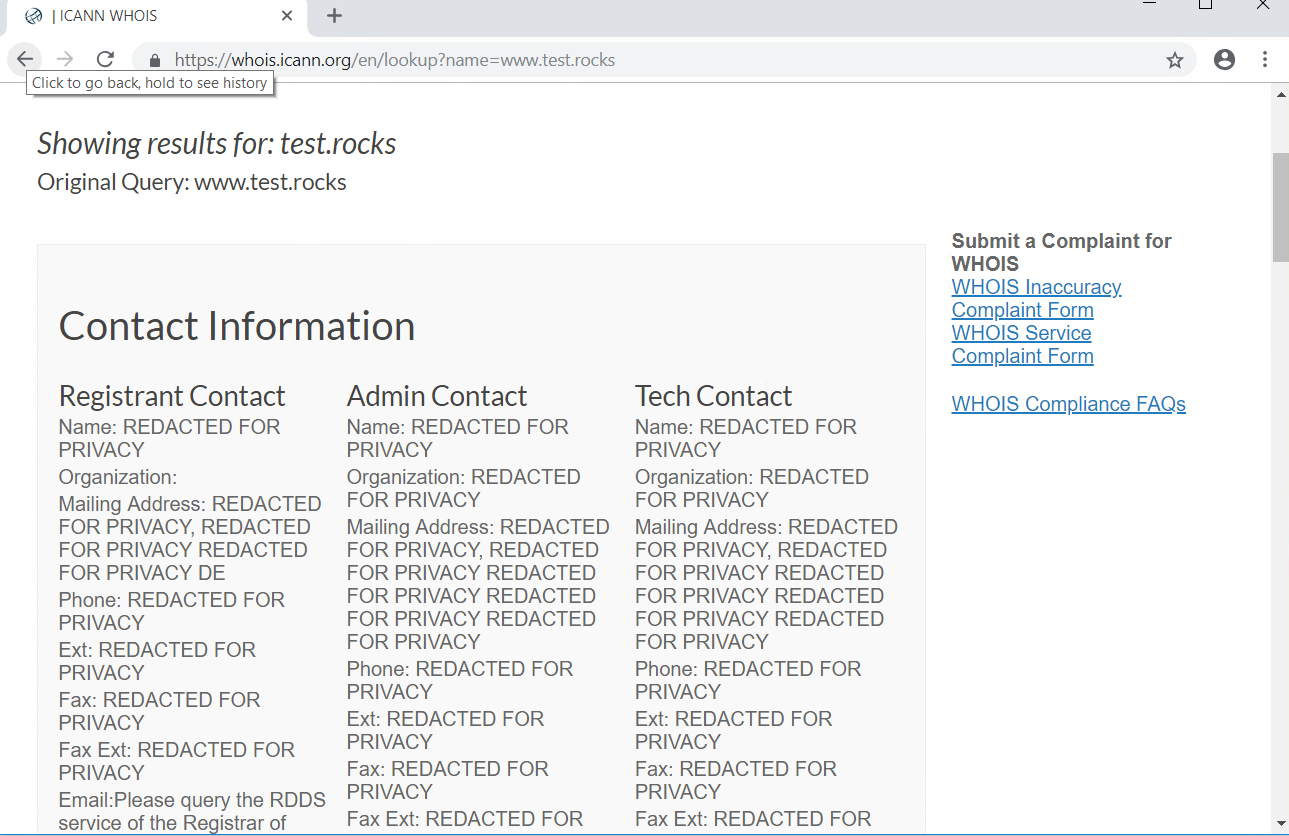


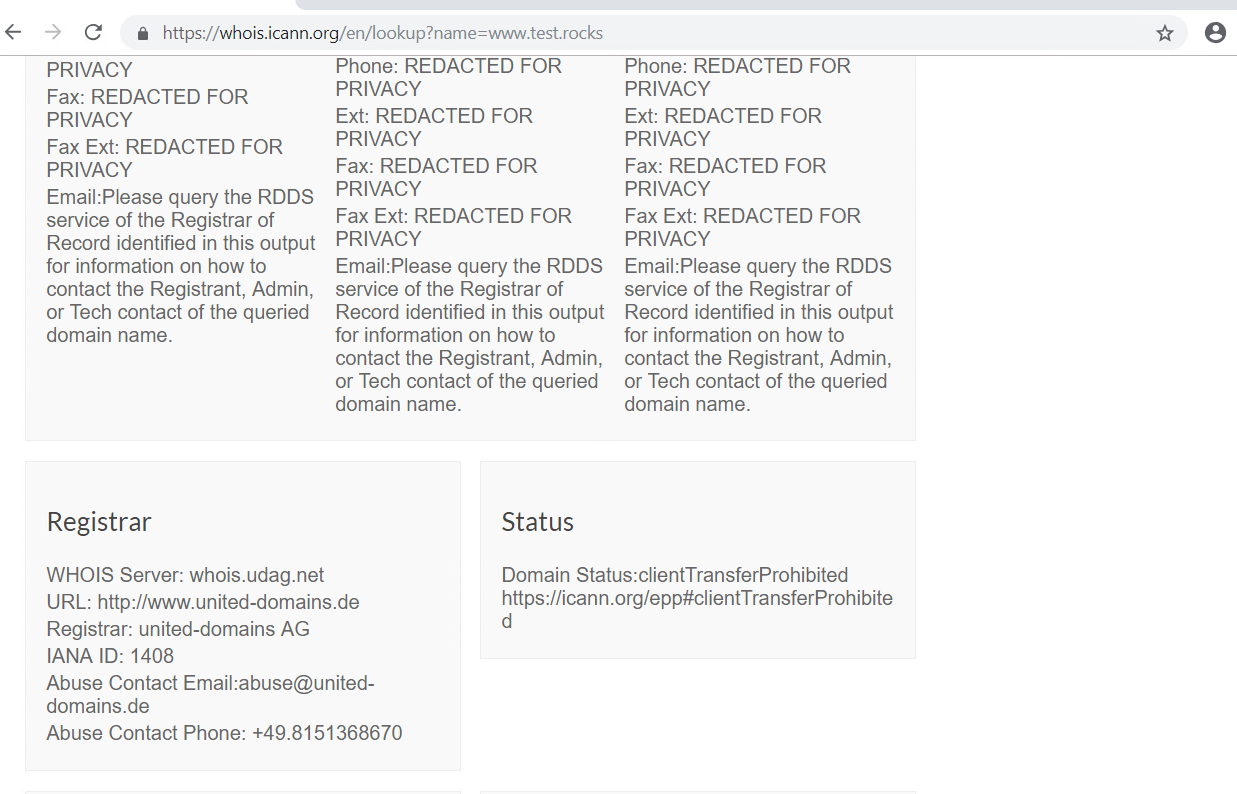
1. Who owns the domain test.rocks you discovered?

Information is Private

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

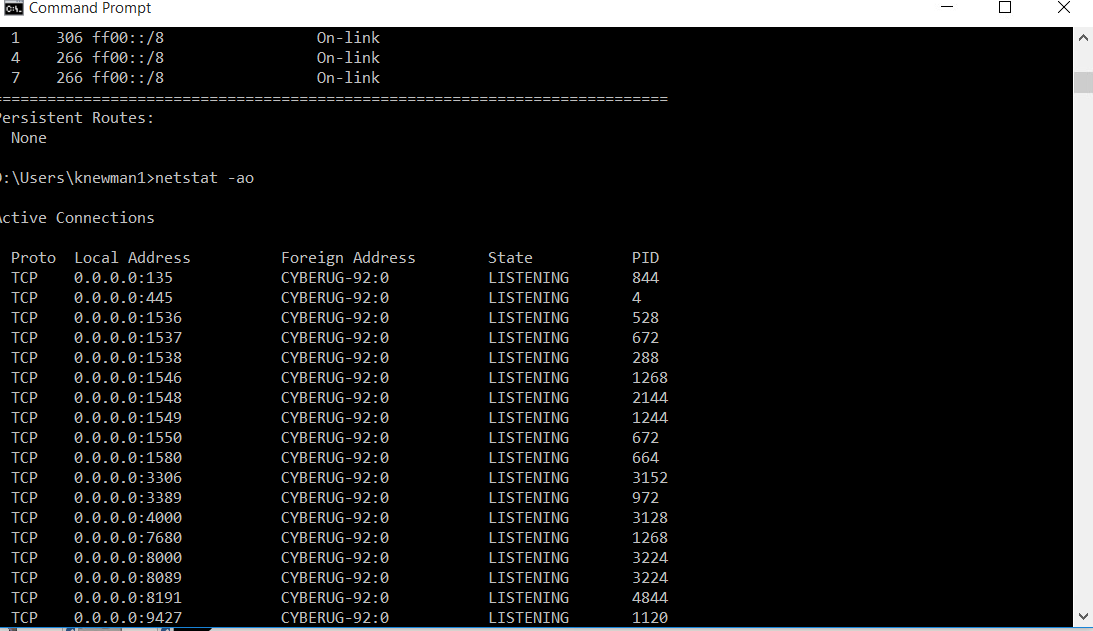
Information is Private

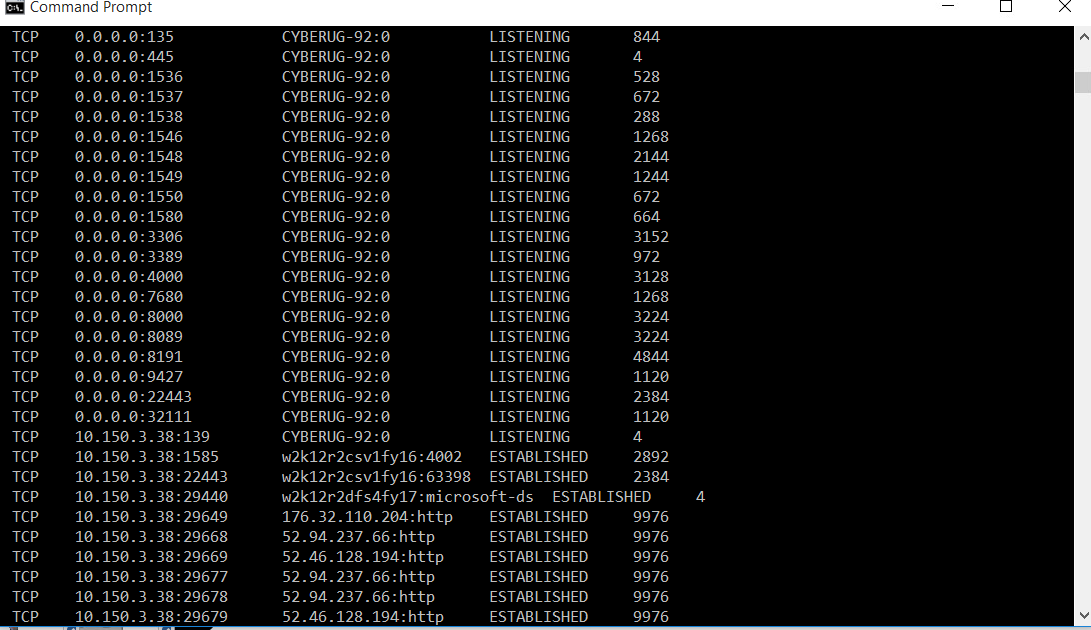




1. Use the tool **netstat**to determine the following:
2. A list of all the active TCP ports your VM is listening on
3. What is the process ID (PID) for TCP port 3389?

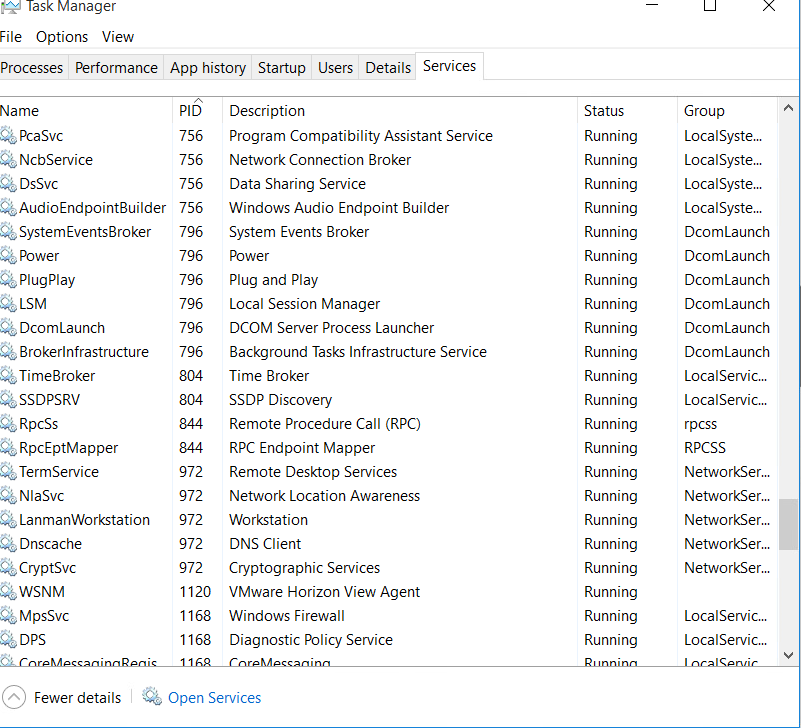
972



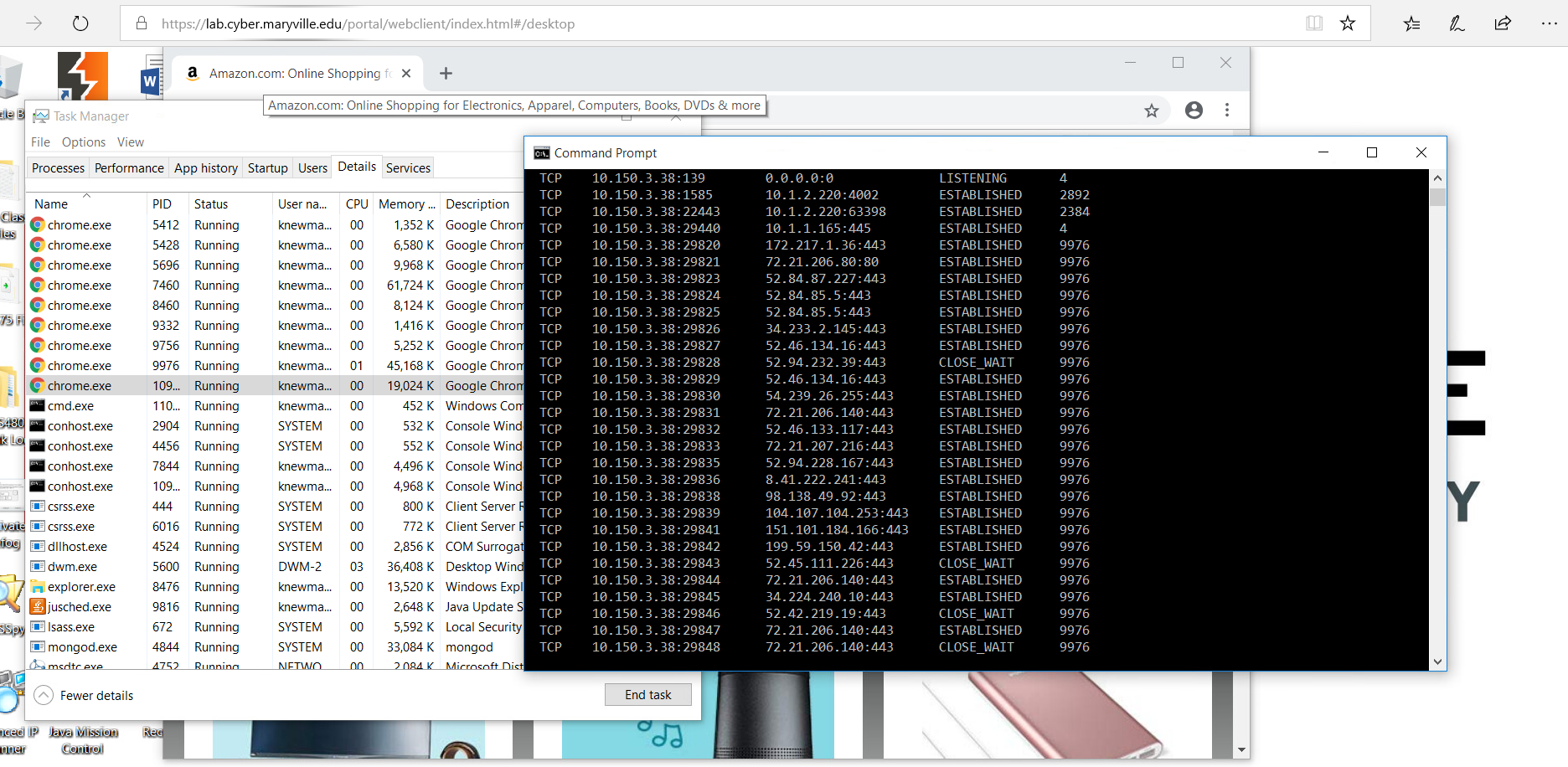


1. What service is running on TCP port 3389?

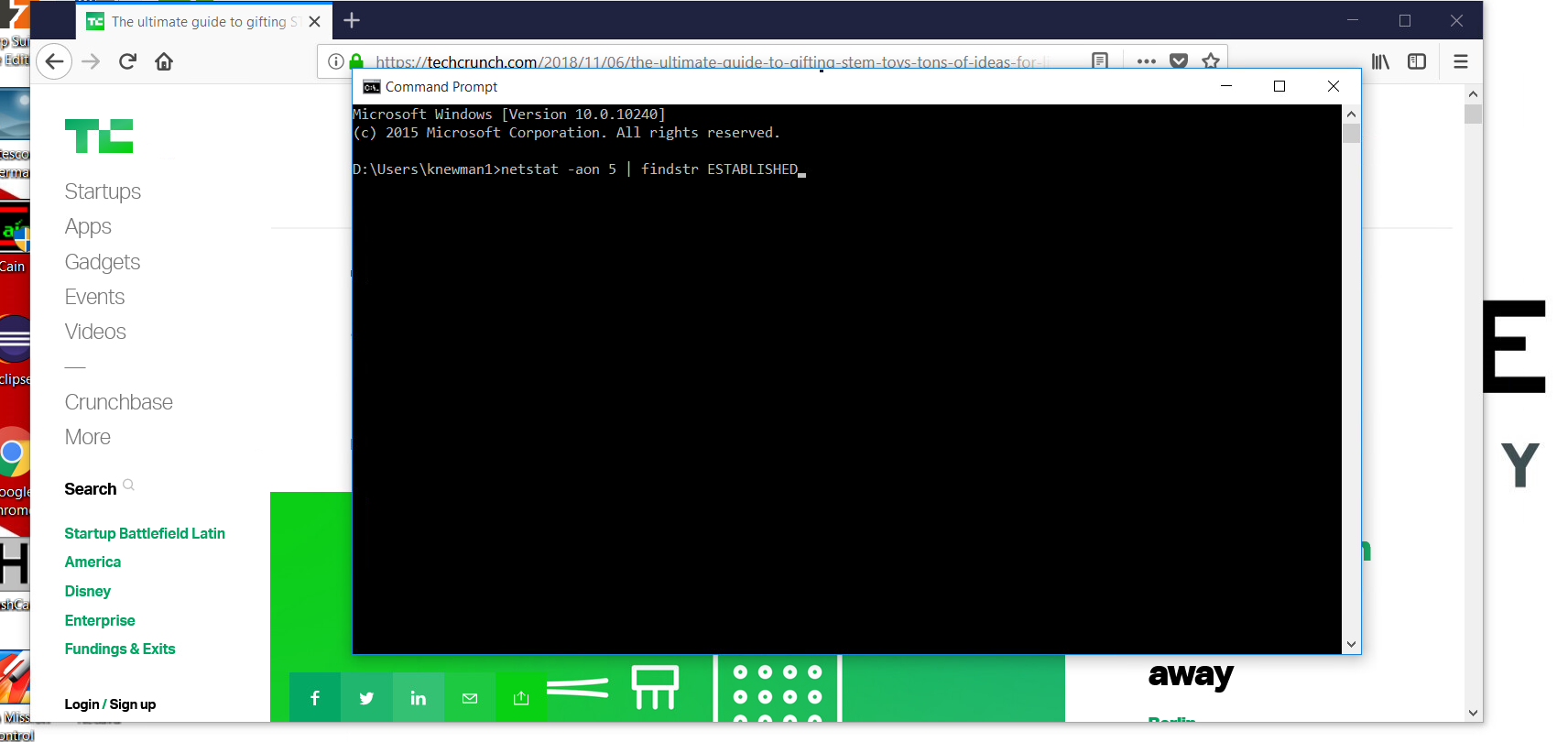
Remote Desktop Services, Network Location Awareness, Workstation, DNS Client, and Cryptographic Services

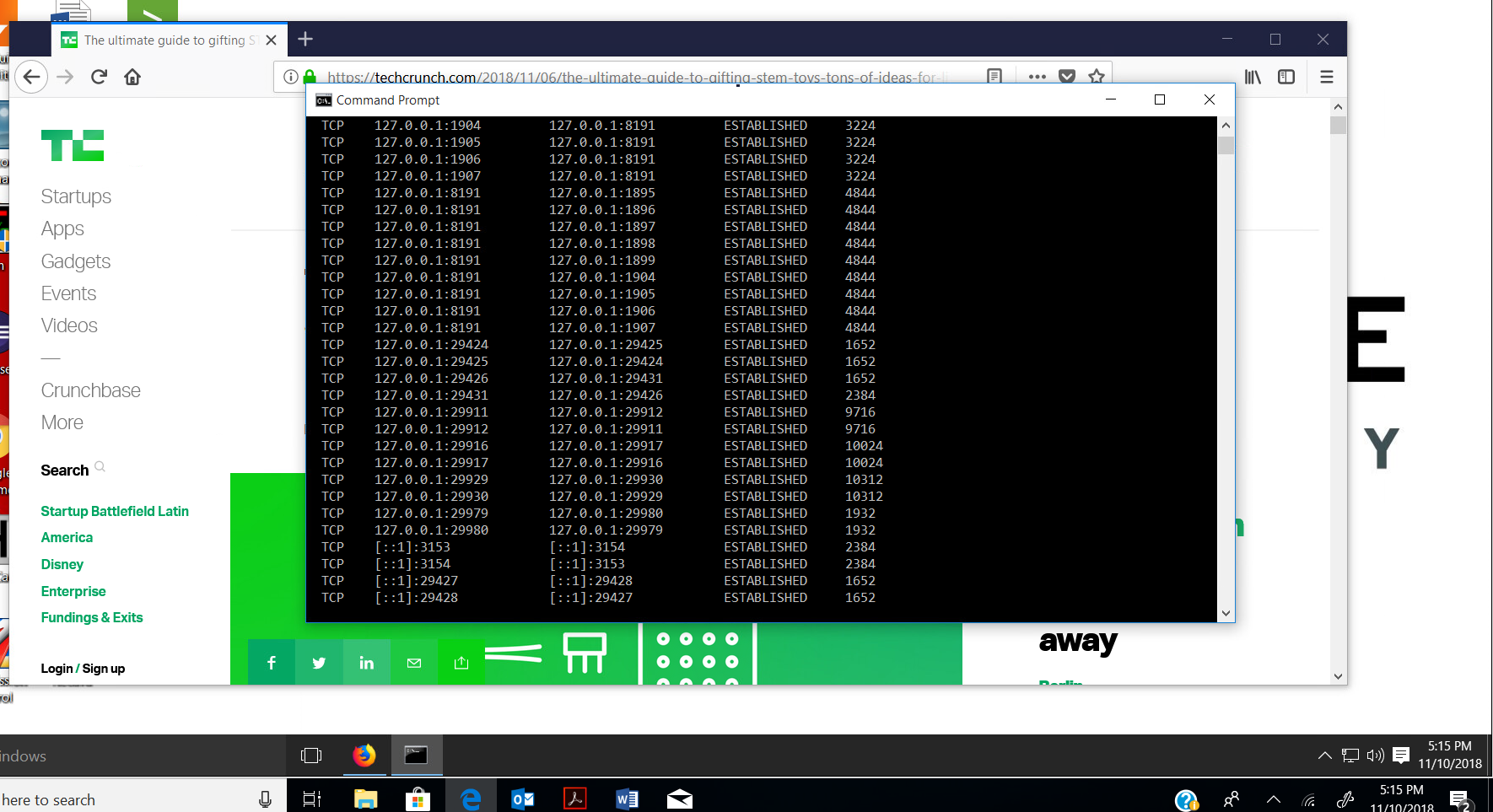


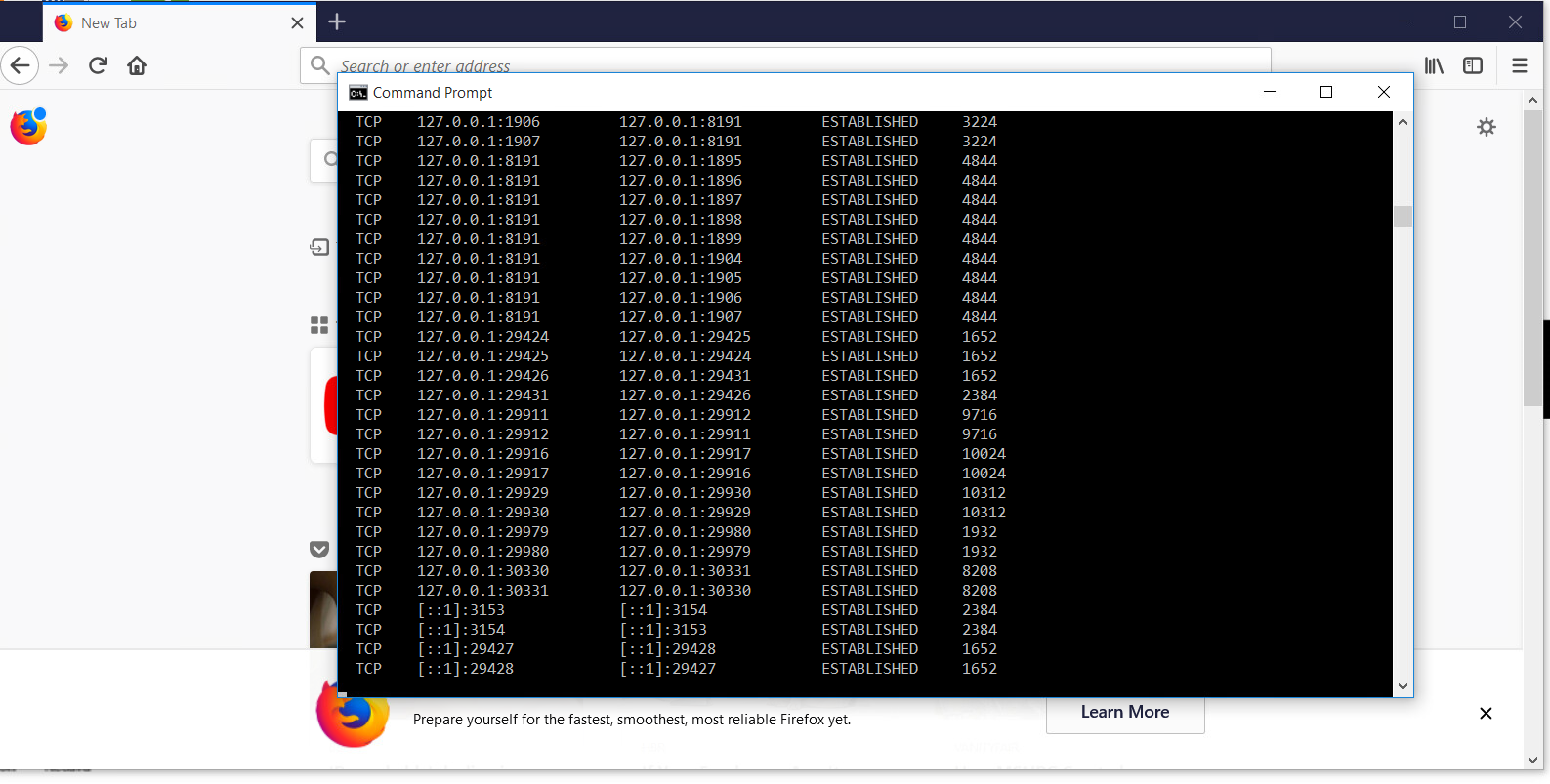
1. Open a browser and connect to amazon.com. Using **netstat**, capture the connection information. What source port are you using? (Hint: to narrow down the established list, determine the PID of the browser. Consider using Task Manager as well to find the PID)



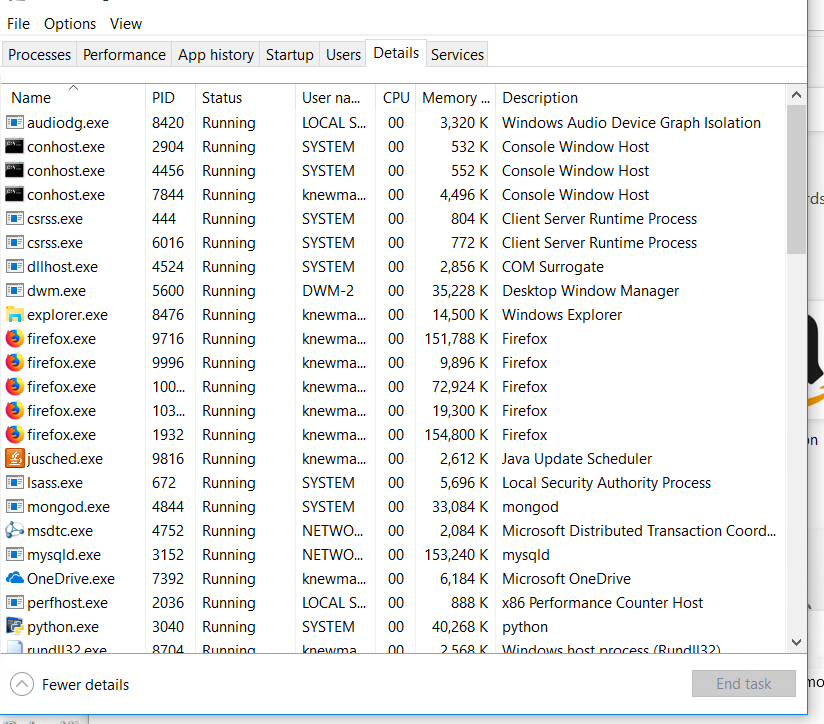
1. If you want **netstat** to filter on connections from the Firefox browser, every 5 seconds, how would you accomplish this?







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



1. From your VM, go to **whatismyip.com** in a browser.
2. Is your VM NAT'd?

yes

1. 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

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

30 hops

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

The IP address connected to local host

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

Only one IP address

