Assignment 2-1: Network Discovery

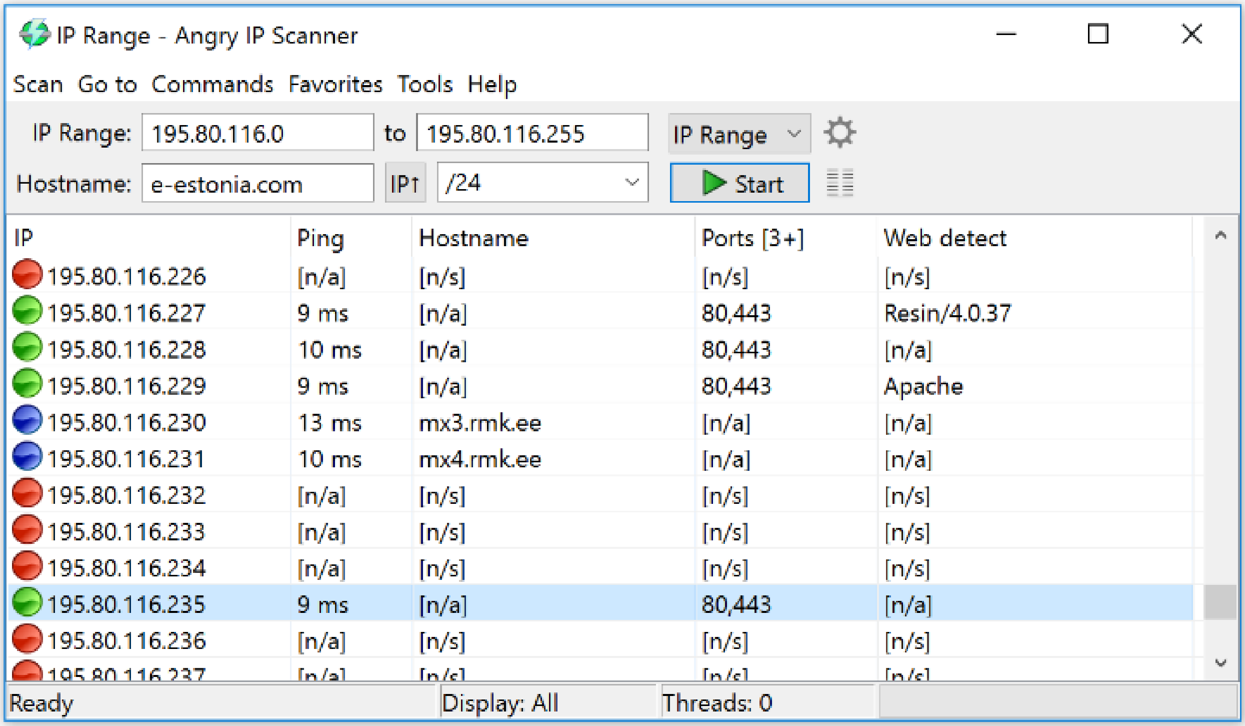
Name: ____

Objective

The purpose of this lab is to introduce you to tools for discovering what devices are on your current network. It will also give you additional information that would be useful to a network administrator, troubleshooter, or someone up to no good.

Background

You will need to install a small application called Angry IP Scanner that is available for both Windows and Mac machines, preferably a laptop.


IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range
IP↑
Start

IP Range: 195.80.116.0 to 195.80.116.255

Hostname: e-estonia.com /24

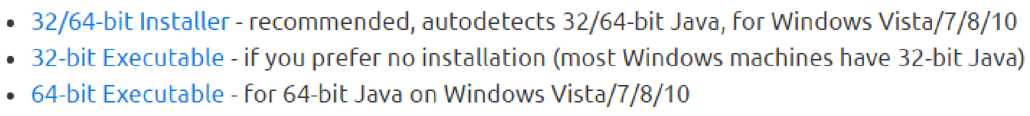
IP	Ping	Hostname	Ports [3+]	Web detect
🔴 195.80.116.226	[n/a]	[n/s]	[n/s]	[n/s]
🟢 195.80.116.227	9 ms	[n/a]	80,443	Resin/4.0.37
🟢 195.80.116.228	10 ms	[n/a]	80,443	[n/a]
🟢 195.80.116.229	9 ms	[n/a]	80,443	Apache
🔵 195.80.116.230	13 ms	mx3.rmk.ee	[n/a]	[n/a]
🔵 195.80.116.231	10 ms	mx4.rmk.ee	[n/a]	[n/a]
🔴 195.80.116.232	[n/a]	[n/s]	[n/s]	[n/s]
🔴 195.80.116.233	[n/a]	[n/s]	[n/s]	[n/s]
🔴 195.80.116.234	[n/a]	[n/s]	[n/s]	[n/s]
🟢 195.80.116.235	9 ms	[n/a]	80,443	[n/a]
🔴 195.80.116.236	[n/a]	[n/s]	[n/s]	[n/s]
🔴 195.80.116.237	[n/a]	[n/s]	[n/s]	[n/s]

Ready | Display: All | Threads: 0

Part 1

First, we will download and install the software.

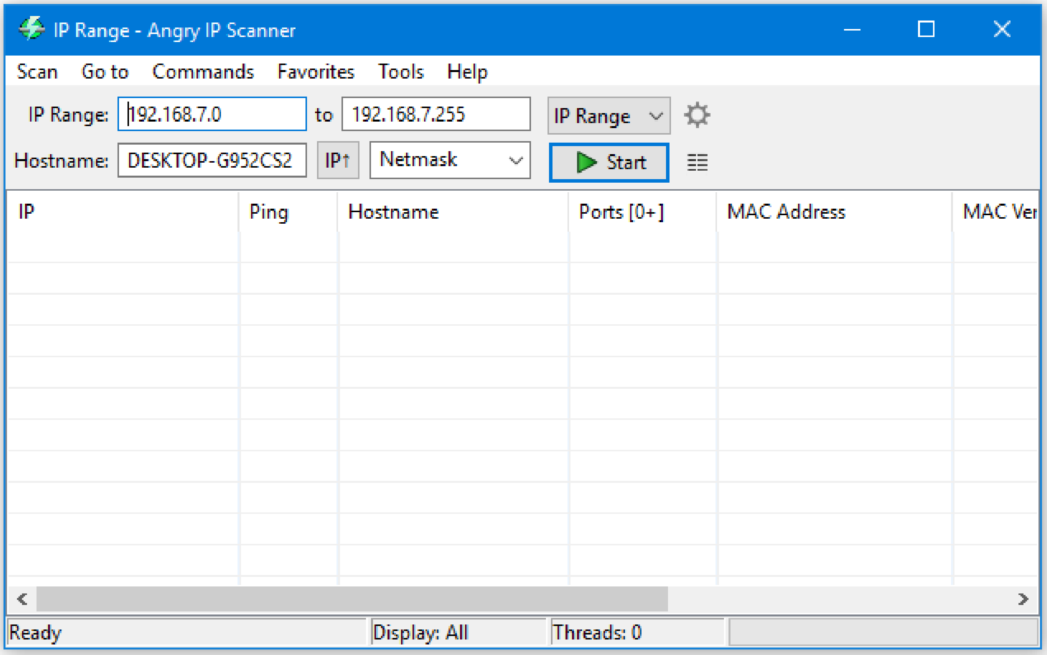
1. Go to http://angryip.org/ and look over the home page.
2. Click on the **Free Download** button.
3. On the next screen, you see choices of Linux, Mac, and Windows – mine was already open to Windows. If not click on the bar with your operating system on it and read any instruction
4. Windows users might as well select the first option. It will download a file to your Downloads folder or wherever you direct it.



- 32/64-bit Installer - recommended, autodetects 32/64-bit Java, for Windows Vista/7/8/10
- 32-bit Executable - if you prefer no installation (most Windows machines have 32-bit Java)
- 64-bit Executable - for 64-bit Java on Windows Vista/7/8/10

5. Double-click on the downloaded file to launch the installer. Accept any defaults including the one to run the program when finished. A few pages of information will appear the first time.
6. The window will look something like this. Note that it detected the IP address pool (IP Range) of the connected network – it always runs on the current network.

   To see what it does, click on **Start** and wait.



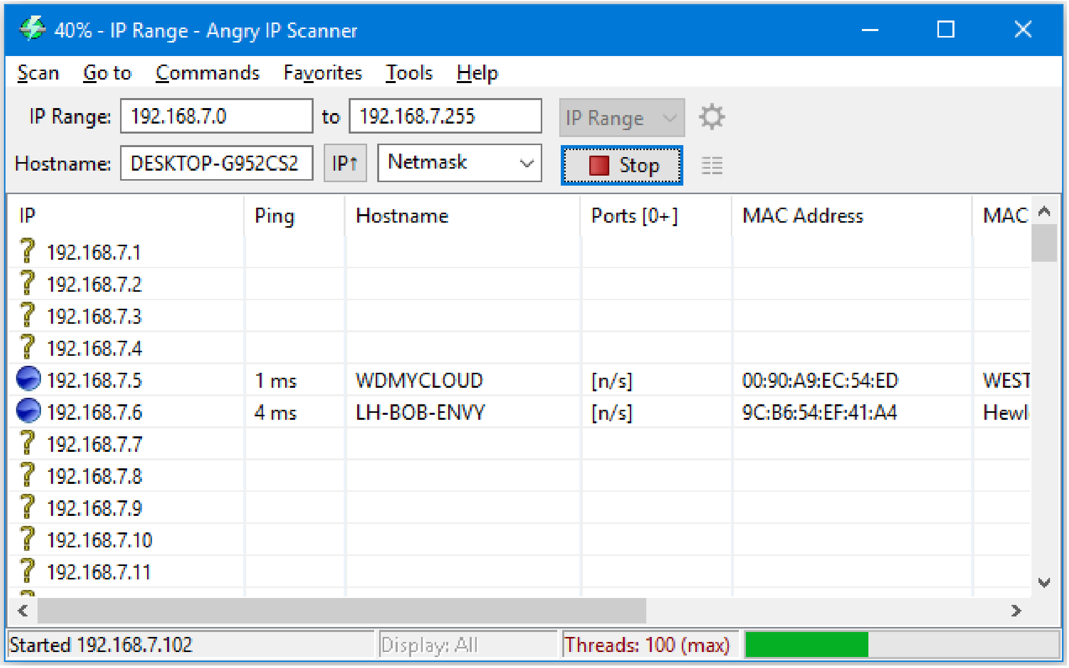
IP Range: 192.168.7.0 to 192.168.7.255

Hostname: DESKTOP-G952CS2 IP↑ Netmask

IP	Ping	Hostname	Ports [0+]	MAC Address	MAC Ver

Ready | Display: All | Threads: 0

Depending on the size of the network this can take a minute or two. It is pinging every address in the range in sequential order. The counter in the upper-left corner and the green bar in the lower right show the progress.



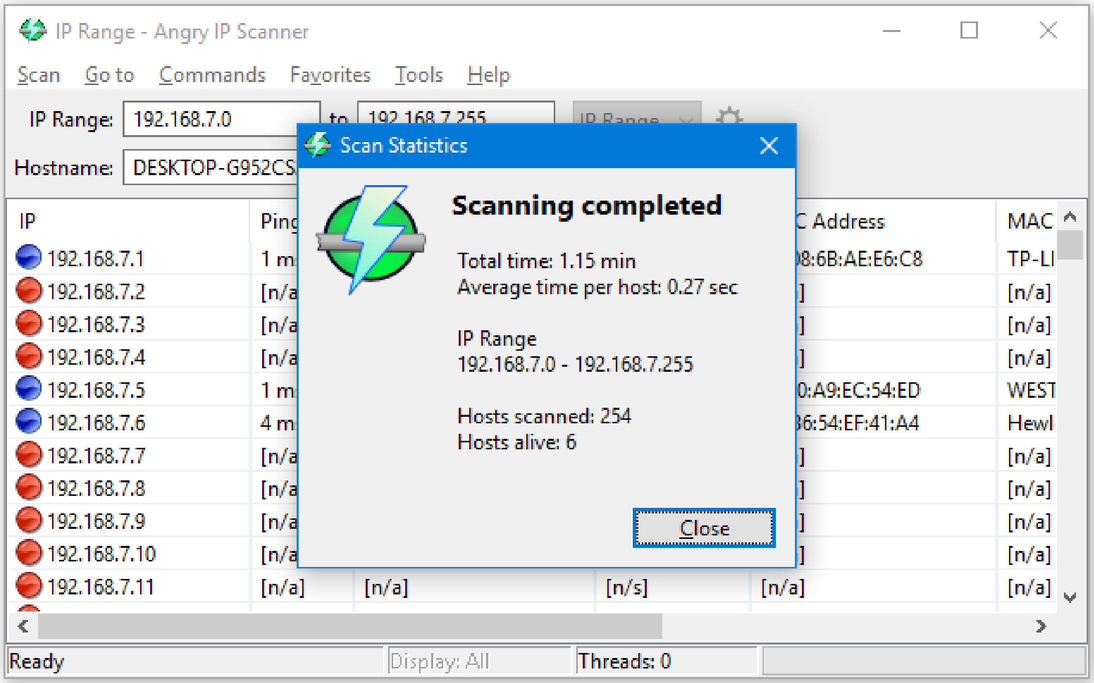
IP Range: 192.168.7.0 to 192.168.7.255

Hostname: DESKTOP-G952CS2 IP↑ Netmask

IP	Ping	Hostname	Ports [0+]	MAC Address	MAC
? 192.168.7.1					
? 192.168.7.2					
? 192.168.7.3					
? 192.168.7.4					
● 192.168.7.5	1 ms	WDMYCLOUD	[n/s]	00:90:A9:EC:54:ED	WEST
● 192.168.7.6	4 ms	LH-BOB-ENVY	[n/s]	9C:B6:54:EF:41:A4	Hewl
? 192.168.7.7					
? 192.168.7.8					
? 192.168.7.9					
? 192.168.7.10					
? 192.168.7.11					

Started 192.168.7.102 | Display: All | Threads: 100 (max)

When it finishes, it will look like this with Statistics shield summarizing the results – close it whenever you want. Blue balls indicate an alive device; red means no response.



IP Range: 192.168.7.0 to 192.168.7.255

Hostname: DESKTOP-G952CS

Scan Statistics

Scanning completed

Total time: 1.15 min
Average time per host: 0.27 sec

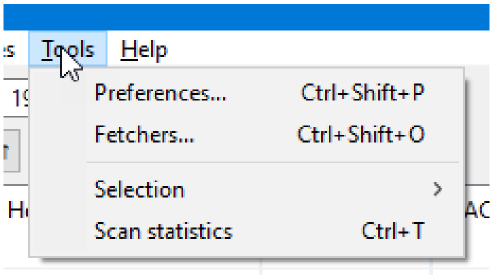
IP Range
192.168.7.0 - 192.168.7.255

Hosts scanned: 254
Hosts alive: 6

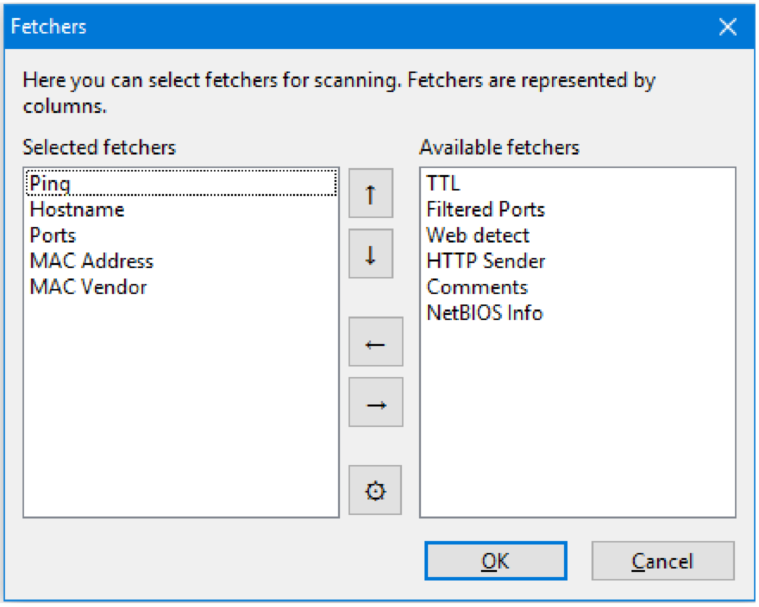
IP	Ping			C Address	MAC
● 192.168.7.1	1 m			)8:6B:AE:E6:C8	TP-LI
● 192.168.7.2	[n/a			]	[n/a]
● 192.168.7.3	[n/a			]	[n/a]
● 192.168.7.4	[n/a			]	[n/a]
● 192.168.7.5	1 m			0:A9:EC:54:ED	WEST
● 192.168.7.6	4 m			36:54:EF:41:A4	Hewl
● 192.168.7.7	[n/a			]	[n/a]
● 192.168.7.8	[n/a			]	[n/a]
● 192.168.7.9	[n/a			]	[n/a]
● 192.168.7.10	[n/a			]	[n/a]
● 192.168.7.11	[n/a]	[n/a]	[n/s]	[n/a]	[n/a]

Ready | Display: All | Threads: 0

7. To get more information, click on the Tools menu and choose Fetchers.



The current columns are the **Fetchers** on the left; other items are on the right.



Here you can select fetchers for scanning. Fetchers are represented by columns.

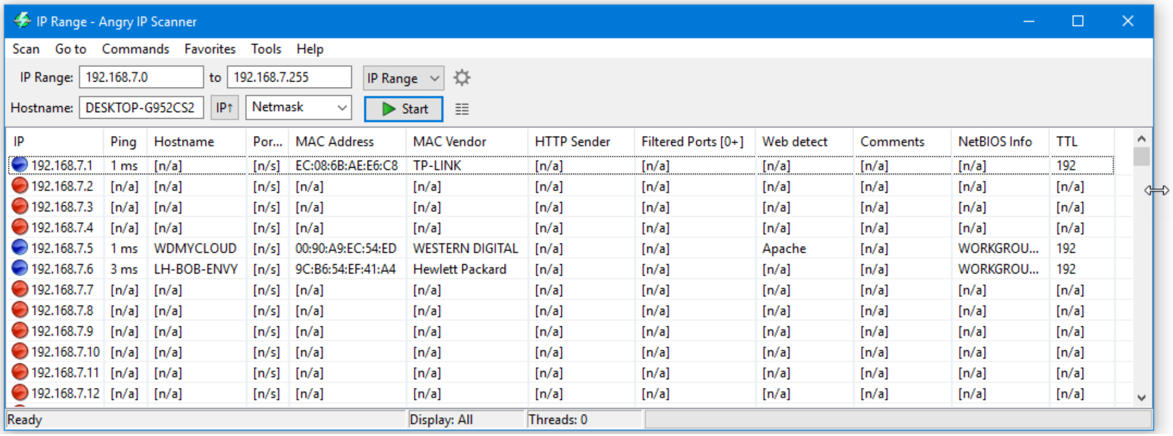
Selected fetchers

- Ping
- Hostname
- Ports
- MAC Address
- MAC Vendor

Available fetchers

- TTL
- Filtered Ports
- Web detect
- HTTP Sender
- Comments
- NetBIOS Info

8. Double-click on any item will move it over to the other box – it works both ways. You can also select one or more items and click on the arrow pointing towards the other box. For the time being, move everything into the Selected Fetchers.
9. Select an item near the middle of the list and note the up/down arrow buttons between the windows will change their order. That will be handy once we know what we are looking at. Click **OK**.
10. Click **Start** to get it to rescan and pull the new data. You will notice that you will want to make the window wider to see the new columns. You can drag an edge to make it wider or Maximize it to fill the screen.



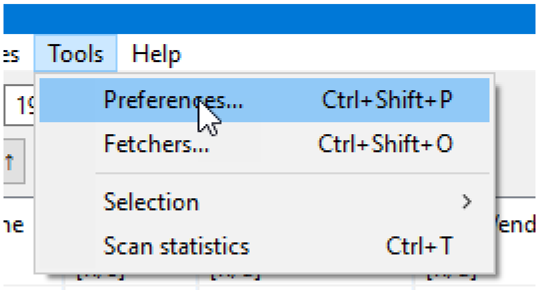
IP Range: 192.168.7.0 to 192.168.7.255

Hostname: DESKTOP-G952CS2 Netmask

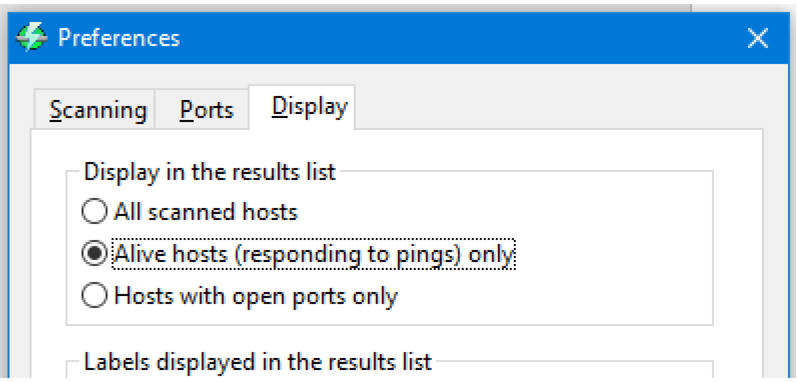
IP	Ping	Hostname	Por...	MAC Address	MAC Vendor	HTTP Sender	Filtered Ports [0+]	Web detect	Comments	NetBIOS Info	TTL
🔵 192.168.7.1	1 ms	[n/a]	[n/s]	EC:08:6B:AE:E6:C8	TP-LINK	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	192
🔴 192.168.7.2	[n/a]	[n/a]	[n/s]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]
🔴 192.168.7.3	[n/a]	[n/a]	[n/s]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]
🔴 192.168.7.4	[n/a]	[n/a]	[n/s]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]
🔵 192.168.7.5	1 ms	WDMYCLOUD	[n/s]	00:90:A9:EC:54:ED	WESTERN DIGITAL	[n/a]	[n/a]	Apache	[n/a]	WORKGROU...	192
🔵 192.168.7.6	3 ms	LH-BOB-ENVY	[n/s]	9C:B6:54:EF:41:A4	Hewlett Packard	[n/a]	[n/a]	[n/a]	[n/a]	WORKGROU...	192
🔴 192.168.7.7	[n/a]	[n/a]	[n/s]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]
🔴 192.168.7.8	[n/a]	[n/a]	[n/s]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]
🔴 192.168.7.9	[n/a]	[n/a]	[n/s]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]
🔴 192.168.7.10	[n/a]	[n/a]	[n/s]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]
🔴 192.168.7.11	[n/a]	[n/a]	[n/s]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]
🔴 192.168.7.12	[n/a]	[n/a]	[n/s]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]

Ready | Display: All | Threads: 0

11. Scroll up and down to see all the rows. Except on very busy networks, you will find a lot of inactive IP addresses. Let's get rid of those from our display. Choose **Tools | Preferences**.



12. In the next window, choose the **Display** tab and make the following choice. Before clicking OK, look over the other options. Notice there is an option near the bottom to turn off the Statistics pop-up when it is finished scanning. It doesn't bother me, but you can turn it off. Click **OK** and start another scan.



Display in the results list

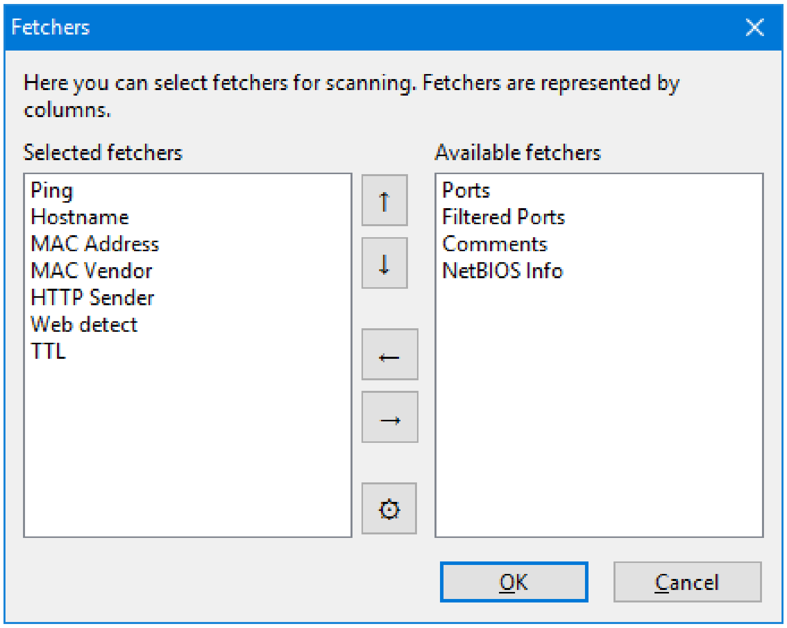
○ All scanned hosts

● Alive hosts (responding to pings) only

○ Hosts with open ports only

Labels displayed in the results list

13. To get rid of some of the blank columns go back into **Tools | Fetchers** and make the following choices – feel free to omit or add any that you want. Change the column order if you have any preferences.



Here you can select fetchers for scanning. Fetchers are represented by columns.

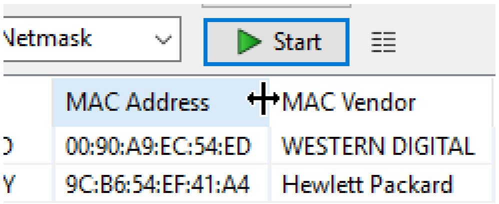
Selected fetchers

- Ping
- Hostname
- MAC Address
- MAC Vendor
- HTTP Sender
- Web detect
- TTL

Available fetchers

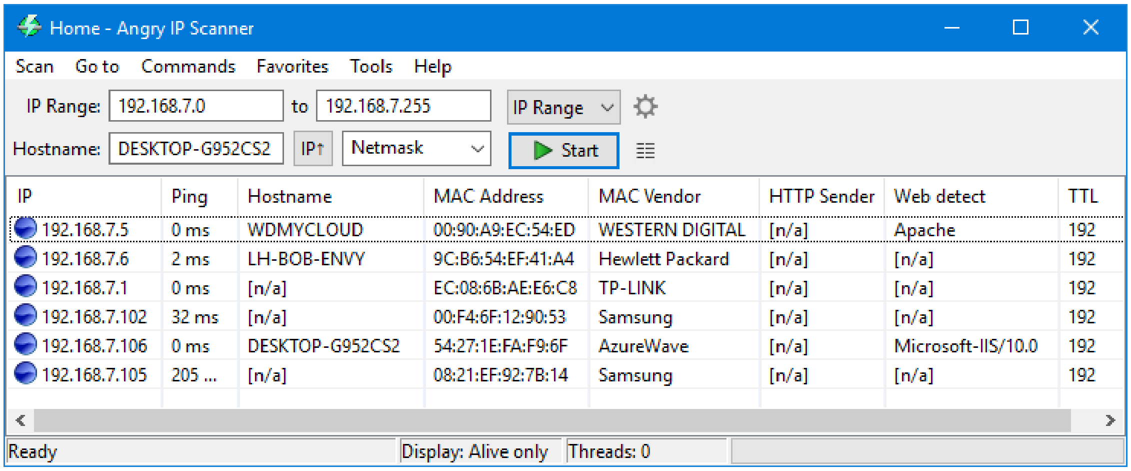
- Ports
- Filtered Ports
- Comments
- NetBIOS Info

14. Rerun your scan but before resizing your window, not that you can adjust column widths exactly like in Excel. Putting your mouse on the right edge of a column heading (note two-headed arrow), you can drag it smaller, larger, or you can double-click, and it will set to the widest visible data. It doesn't consider the label width, though, so wide labels with narrow data can get hidden.



MAC Address	MAC Vendor
00:90:A9:EC:54:ED	WESTERN DIGITAL
9C:B6:54:EF:41:A4	Hewlett Packard

15. You should be able to create a nice compact display for documentation purposes.



IP Range: 192.168.7.0 to 192.168.7.255 IP Range

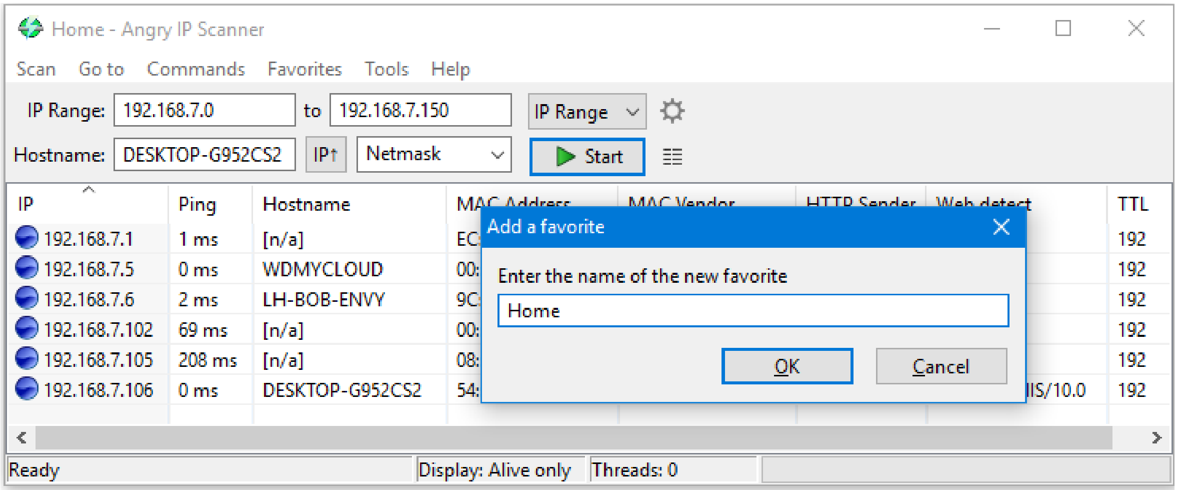
Hostname: DESKTOP-G952CS2 Netmask

IP	Ping	Hostname	MAC Address	MAC Vendor	HTTP Sender	Web detect	TTL
192.168.7.5	0 ms	WDMYCLOUD	00:90:A9:EC:54:ED	WESTERN DIGITAL	[n/a]	Apache	192
192.168.7.6	2 ms	LH-BOB-ENVY	9C:B6:54:EF:41:A4	Hewlett Packard	[n/a]	[n/a]	192
192.168.7.1	0 ms	[n/a]	EC:08:6B:AE:E6:C8	TP-LINK	[n/a]	[n/a]	192
192.168.7.102	32 ms	[n/a]	00:F4:6F:12:90:53	Samsung	[n/a]	[n/a]	192
192.168.7.106	0 ms	DESKTOP-G952CS2	54:27:1E:FA:F9:6F	AzureWave	[n/a]	Microsoft-IIS/10.0	192
192.168.7.105	205 ...	[n/a]	08:21:EF:92:7B:14	Samsung	[n/a]	[n/a]	192

Ready | Display: Alive only | Threads: 0

16. Note that you can sort the output on any column by clicking on the heading label. The first time will sort in ascending order. The second dime will **Change Sort Direction**.

17. If you have a scan that you plan to do frequently, you can save the **IP Range** by using **Favorites | Add current…** and give it a name. Notice that before I named this one *Home*, I changed the last IP to test for 192.168.7.150 (instead of 255) to speed up the results since there will never be an IP bigger than 150. It doesn't save your Fetcher choices or sort, though.



IP Range: 192.168.7.0 to 192.168.7.150

Hostname: DESKTOP-G952CS2

IP	Ping	Hostname	MAC Address	MAC Vendor	HTTP Sender	Web detect	TTL
192.168.7.1	1 ms	[n/a]	EC:				192
192.168.7.5	0 ms	WDMYCLOUD	00:				192
192.168.7.6	2 ms	LH-BOB-ENVY	9C:				192
192.168.7.102	69 ms	[n/a]	00:				192
192.168.7.105	208 ms	[n/a]	08:				192
192.168.7.106	0 ms	DESKTOP-G952CS2	54:			IIS/10.0	192

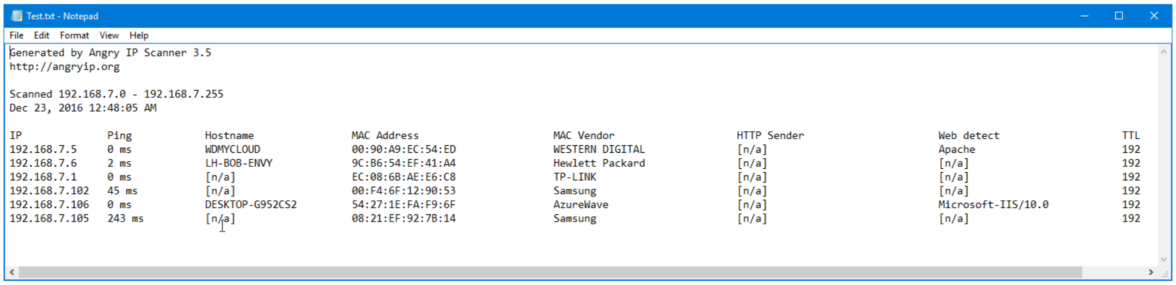
Add a favorite

Enter the name of the new favorite

Home

OK Cancel

18. You can use **Scan |Export all…** or **Selection…** and create a text file of the output.



```
Generated by Angry IP Scanner 3.5
http://angryip.org

Scanned 192.168.7.0 - 192.168.7.255
Dec 23, 2016 12:48:05 AM

IP              Ping            Hostname                MAC Address                     MAC Vendor                      HTTP Sender                     Web detect                      TTL
192.168.7.5     0 ms            WDMYCLOUD               00:90:A9:EC:54:ED               WESTERN DIGITAL                 [n/a]                           Apache                          192
192.168.7.6     2 ms            LH-BOB-ENVY             9C:B6:54:EF:41:A4               Hewlett Packard                 [n/a]                           [n/a]                           192
192.168.7.1     0 ms            [n/a]                   EC:08:6B:AE:E6:C8               TP-LINK                         [n/a]                           [n/a]                           192
192.168.7.102   45 ms           [n/a]                   00:F4:6F:12:90:53               Samsung                         [n/a]                           [n/a]                           192
192.168.7.106   0 ms            DESKTOP-G952CS2         54:27:1E:FA:F9:6F               AzureWave                       [n/a]                           Microsoft-IIS/10.0              192
192.168.7.105   243 ms          [n/a]                   08:21:EF:92:7B:14               Samsung                         [n/a]                           [n/a]                           192
```

19. Take a few minutes and look over the menu options. You can't hurt anything.

Part 2

Run these same tests in couple locations where you have an Internet connection. Maybe school or a WiFi hotspot. Possibly do it at the same time as any other assignments that might ask for multiple locations. Summarize and share your results.

Part 3

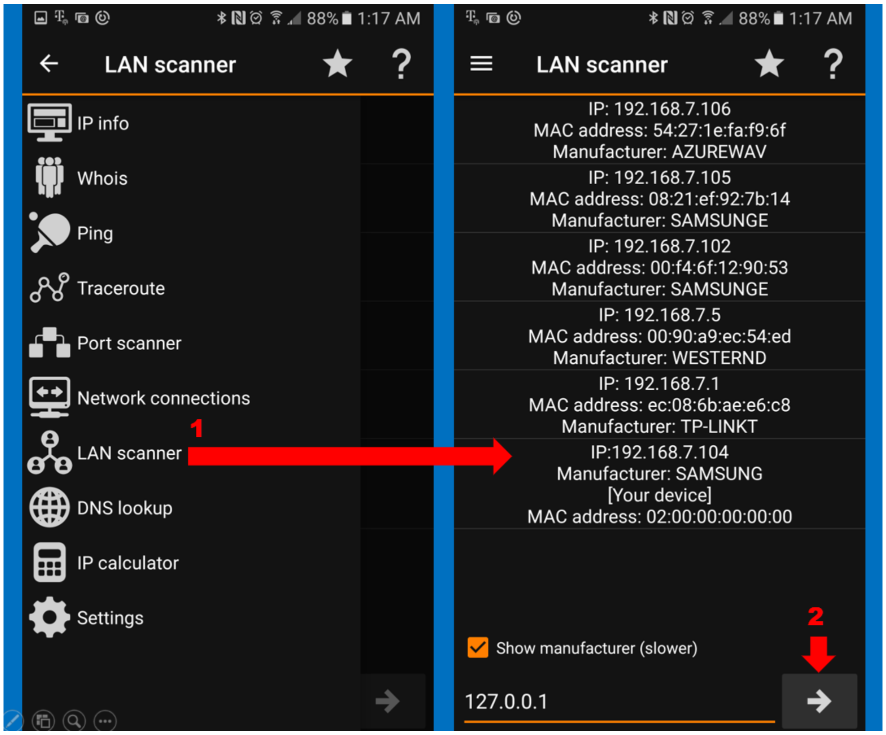
Using the **IP Tools** app on your phone or tablet from the Module 1 assignments.

1. From the List icon menu, choose **LAN scanner**.
2. Click on the arrow in the lower-right corner to run it on the current network (that is what the 127.0.0.1 means – the loopback address of the local host).

   Note in the following output I checked the **Show manufacture (slower)** to have the MAC addresses resolved to show who made the interfaces.

   The app doesn't detect as much information, but it tells us what devices are on the network and a bit about them – and it is always with you.

When you run your tests for **Part 2**, compare one or two to the app.



```
IP: 192.168.7.106
MAC address: 54:27:1e:fa:f9:6f
Manufacturer: AZUREWAV
IP: 192.168.7.105
MAC address: 08:21:ef:92:7b:14
Manufacturer: SAMSUNGE
IP: 192.168.7.102
MAC address: 00:f4:6f:12:90:53
Manufacturer: SAMSUNGE
IP: 192.168.7.5
MAC address: 00:90:a9:ec:54:ed
Manufacturer: WESTERND
IP: 192.168.7.1
MAC address: ec:08:6b:ae:e6:c8
Manufacturer: TP-LINKT
IP:192.168.7.104
Manufacturer: SAMSUNG
[Your device]
MAC address: 02:00:00:00:00:00
```

☑ Show manufacturer (slower)

127.0.0.1