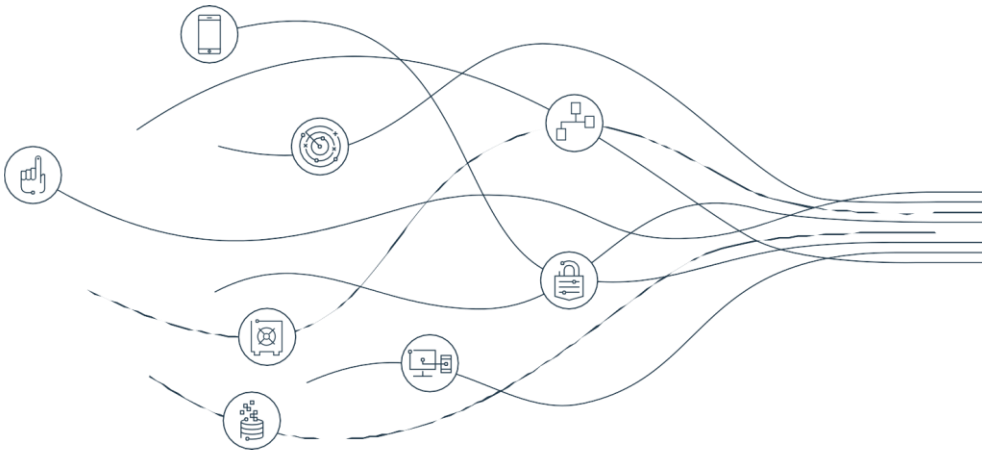
Network Security Tools

Lab 2

Version: 2021.02.08



The information contained in this document has not been submitted to any formal IBM test and is distributed on an “as is” basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer’s ability to evaluate and integrate them into the customer’s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will result elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Contents

Preface

Overview

To begin this lab, we are going to discover, first-hand, some of the information anyone can pull from your IP address using centralops.net. We will then dive into our personal computers Command Line Interface (CLI) in order to use further commands revolving around our IP Address and security. Cyber threats are always out there; we will utilize Nmap and Wireshark to showcase ways that criminals scan for weaknesses. We will then end the lab with Network Security Best Practices.

Estimated Time to Complete: 60 mins

Dependency

This lab leverages concepts imparted in the *Cyber Resilience Framework and Lifecycle* lecture.

Objectives

There are four Milestones you must complete:

1. Understand the data behind IP Addresses
2. Explore your personal Command Line Interface
3. Learn about basic tools attackers use to infiltrate your network security
4. Cement industry Best Practices into your mind such as enabling a DNS

Tools

Zenmap

Zenmap is the official cross-platform GUI for the *Nmap Security Scanner*. It is a multi-platform free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users.

Wireshark

Wireshark is a free and open-source packet analyser; often referred to as a “sniffer”. It is used for network troubleshooting analysis, software and communications protocol development, and education. Wireshark is used to examine the details of traffic as data is sent from one connection to the other.

Flow

1. The user will access Central Ops and perform ping test, Trace Route and Name Server Lookup.
2. The User will access Zenmap through their internet browser and download NMAP software for on premise usage.
3. The User will access Wireshark through their internet browser and download the software for on premise usage.

Milestone 1: The Data Behind Your IP Address

Milestone Overview

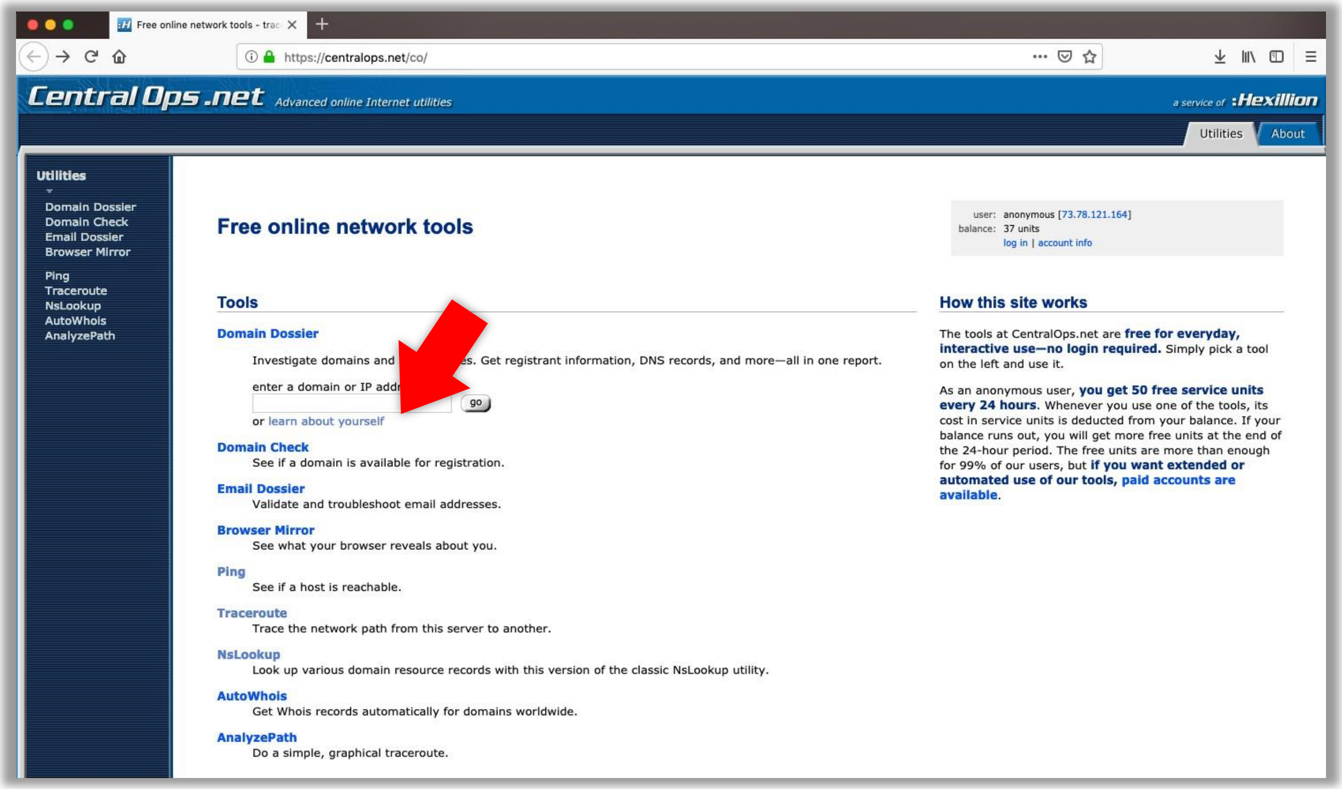
This lab requires you to complete four Milestones:

1. **The Data Behind Your IP Address**
2. Command Line Interface (CLI)
3. Offensive Network Tools
4. Network Protection Practices

In this Milestone we will introduce a tool for investigating, exploring, and troubleshooting Internet addresses such as domain names, IP addresses, email addresses, and URLs.

Explore Central Ops

1. Navigate to centralops.net
2. The first thing we are going to do is find your IP Address.
3. Under the first section *Domain Dossier*, click on “learn about yourself.”



Free online network tools

user: anonymous [73.78.121.164]
balance: 37 units
log in | account info

Tools

Domain Dossier
Investigate domains and [illegible]es. Get registrant information, DNS records, and more—all in one report.
enter a domain or IP addr
or learn about yourself

Domain Check
See if a domain is available for registration.

Email Dossier
Validate and troubleshoot email addresses.

Browser Mirror
See what your browser reveals about you.

Ping
See if a host is reachable.

Traceroute
Trace the network path from this server to another.

NsLookup
Look up various domain resource records with this version of the classic NsLookup utility.

AutoWhois
Get Whois records automatically for domains worldwide.

AnalyzePath
Do a simple, graphical traceroute.

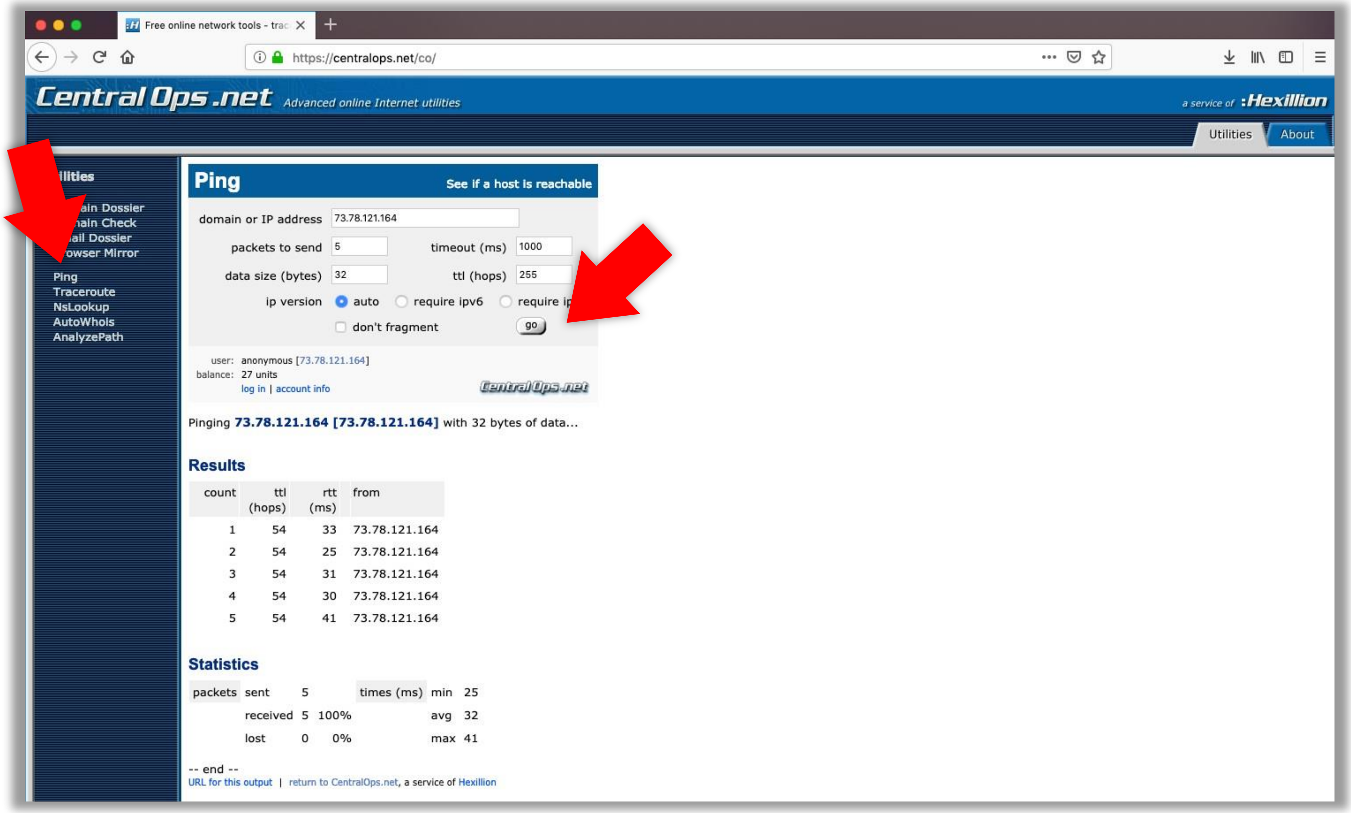
How this site works

The tools at CentralOps.net are **free for everyday, interactive use—no login required.** Simply pick a tool on the left and use it.

As an anonymous user, **you get 50 free service units every 24 hours**. Whenever you use one of the tools, its cost in service units is deducted from your balance. If your balance runs out, you will get more free units at the end of the 24-hour period. The free units are more than enough for 99% of our users, but **if you want extended or automated use of our tools, paid accounts are available**.

Figure 1-1 **Central Ops Website**

4. Once you have located your own address return to the main menu and navigate to the “Ping” section.
5. Input your personal IP Address and hit go.
6. Read the results. What was the average and max response time? Was there any packet loss?



Ping See if a host is reachable

domain or IP address 73.78.121.164

packets to send 5 timeout (ms) 1000

data size (bytes) 32 ttl (hops) 255

ip version ● auto ○ require ipv6 ○ require ip

□ don't fragment

user: anonymous [73.78.121.164]
balance: 27 units
log in | account info

Pinging **73.78.121.164 [73.78.121.164]** with 32 bytes of data...

Results

count	ttl (hops)	rtt (ms)	from
1	54	33	73.78.121.164
2	54	25	73.78.121.164
3	54	31	73.78.121.164
4	54	30	73.78.121.164
5	54	41	73.78.121.164

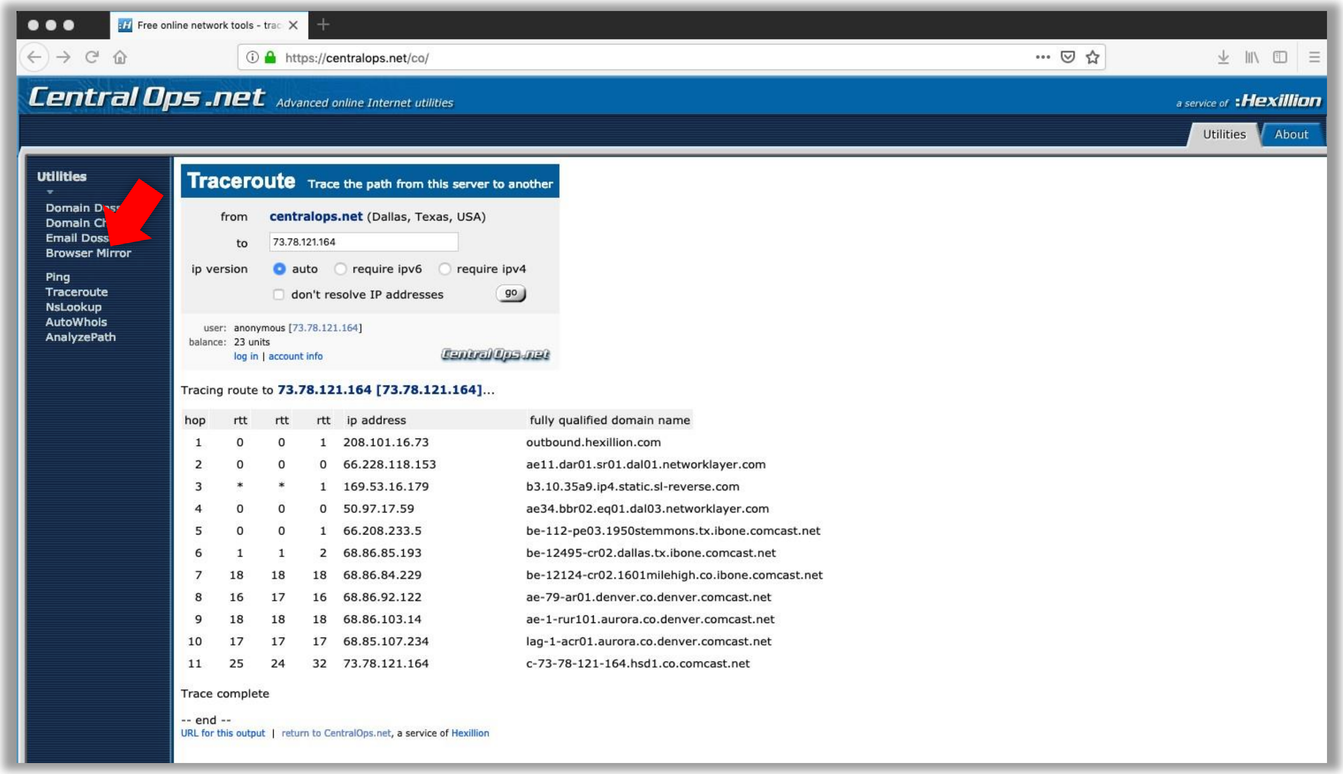
Statistics

packets	sent	5		times (ms)	min	25
	received	5	100%		avg	32
	lost	0	0%		max	41

-- end --
URL for this output | return to CentralOps.net, a service of Hexillion

Figure 1-2 **Ping Test Results**

7. The next tool from the menu we are going to explore is traceroute. From here we can see all the different hops we make as we connect from the CentralOps server in Texas to whichever IP we desire. For this lab input your personal IP Address and hit go.



Traceroute Trace the path from this server to another

from centralops.net (Dallas, Texas, USA)

to 73.78.121.164

ip version ● auto ○ require ipv6 ○ require ipv4

□ don't resolve IP addresses

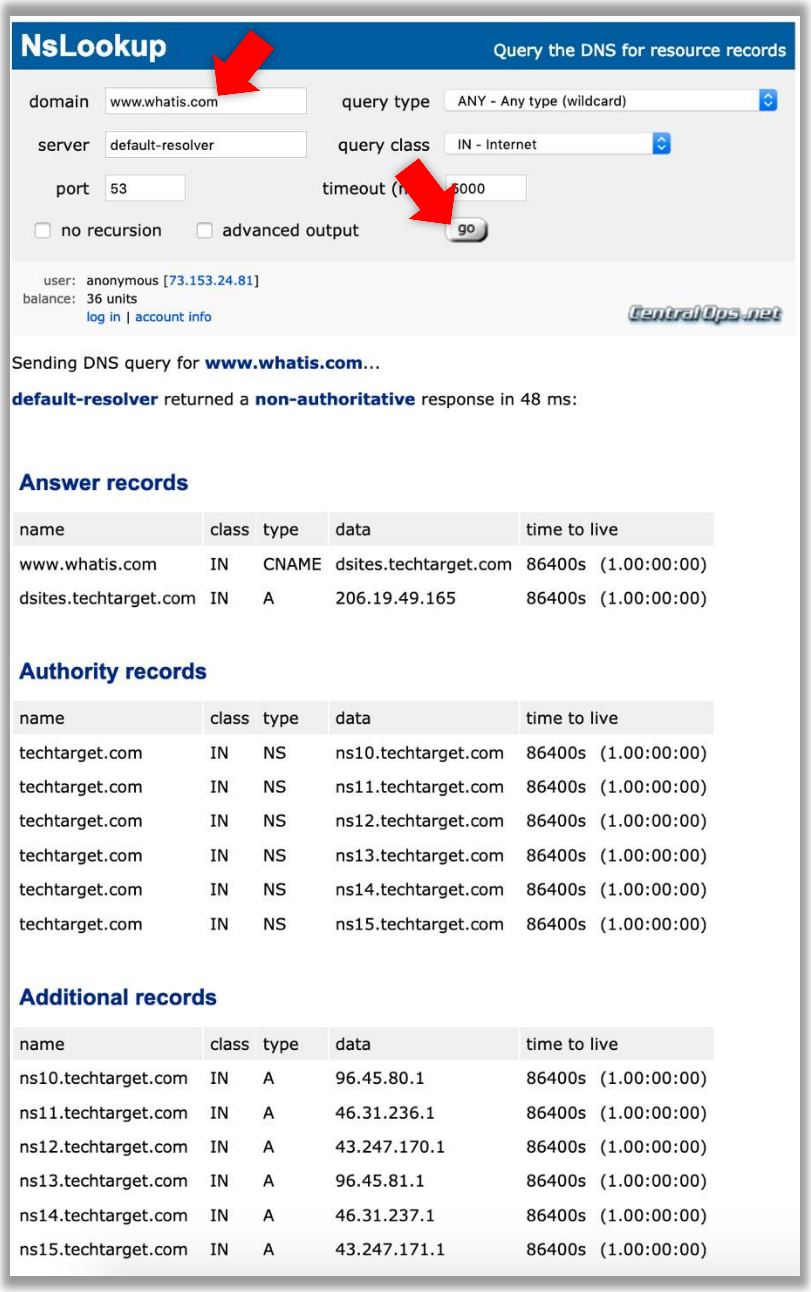
user: anonymous [73.78.121.164]
balance: 23 units

```
Tracing route to 73.78.121.164 [73.78.121.164]...

hop  rtt  rtt  rtt  ip address        fully qualified domain name
  1    0    0    1  208.101.16.73     outbound.hexillion.com
  2    0    0    0  66.228.118.153    ae11.dar01.sr01.dal01.networklayer.com
  3    *    *    1  169.53.16.179     b3.10.35a9.ip4.static.sl-reverse.com
  4    0    0    0  50.97.17.59       ae34.bbr02.eq01.dal03.networklayer.com
  5    0    0    1  66.208.233.5      be-112-pe03.1950stemmons.tx.ibone.comcast.net
  6    1    1    2  68.86.85.193      be-12495-cr02.dallas.tx.ibone.comcast.net
  7   18   18   18  68.86.84.229      be-12124-cr02.1601milehigh.co.ibone.comcast.net
  8   16   17   16  68.86.92.122      ae-79-ar01.denver.co.denver.comcast.net
  9   18   18   18  68.86.103.14      ae-1-rur101.aurora.co.denver.comcast.net
 10   17   17   17  68.85.107.234     lag-1-acr01.aurora.co.denver.comcast.net
 11   25   24   32  73.78.121.164     c-73-78-121-164.hsd1.co.comcast.net

Trace complete

-- end --
```

Figure 1-3 **Trace Route Results**

The last command we will use from centralops.net menu will be the Nslookup (Name Server Lookup).

8. Enter the domain of a website you would like to run nslookup against. (I am using www.whatis.com).
9. Hit "go".
10. Review the Answer records, Authority records, and Additional Records.
11. Authority Records will give a little more information on what DNS the server is using.
12. Additional Records are other name servers that the site does not recognize as one of their own authorities.



domain www.whatis.com query type ANY - Any type (wildcard)

server default-resolver query class IN - Internet

port 53 timeout (m 5000

□ no recursion □ advanced output

user: anonymous [73.153.24.81]
balance: 36 units
log in | account info

Sending DNS query for **www.whatis.com**...

default-resolver returned a **non-authoritative** response in 48 ms:

Answer records

name	class	type	data	time to live
www.whatis.com	IN	CNAME	dsites.techtarget.com	86400s (1.00:00:00)
dsites.techtarget.com	IN	A	206.19.49.165	86400s (1.00:00:00)

Authority records

name	class	type	data	time to live
techtarget.com	IN	NS	ns10.techtarget.com	86400s (1.00:00:00)
techtarget.com	IN	NS	ns11.techtarget.com	86400s (1.00:00:00)
techtarget.com	IN	NS	ns12.techtarget.com	86400s (1.00:00:00)
techtarget.com	IN	NS	ns13.techtarget.com	86400s (1.00:00:00)
techtarget.com	IN	NS	ns14.techtarget.com	86400s (1.00:00:00)
techtarget.com	IN	NS	ns15.techtarget.com	86400s (1.00:00:00)

Additional records

name	class	type	data	time to live
ns10.techtarget.com	IN	A	96.45.80.1	86400s (1.00:00:00)
ns11.techtarget.com	IN	A	46.31.236.1	86400s (1.00:00:00)
ns12.techtarget.com	IN	A	43.247.170.1	86400s (1.00:00:00)
ns13.techtarget.com	IN	A	96.45.81.1	86400s (1.00:00:00)
ns14.techtarget.com	IN	A	46.31.237.1	86400s (1.00:00:00)
ns15.techtarget.com	IN	A	43.247.171.1	86400s (1.00:00:00)

Figure 1-4 **NsLookup Results**

Milestone Summary

This network tool can be used to investigate domains and IP addresses, trace the information path from one server to the other and perform Query the DNS for resource records.

In the next section we will use Command Line Interface (CLI) to learn how to find network information from our own computer.

Milestone 2: Command Line Interface (CLI)

Milestone Overview

This lab requires you to complete four Milestones:

1. The Data Behind Your IP Address
2. **Command Line Interface (CLI)**
3. Offensive Network Tools
4. Network Protection Practices

In this Milestone we will introduce a way to find network information from our own computer.

Exploring Command Interpreters

The following section will be completed in your personal computer. Windows users will utilize their Command Prompt and MacOS users will utilize their Terminal.

Windows users will find their Command Prompt by tapping the search button on the taskbar and typing cmd. Choose Command Prompt from the menu.

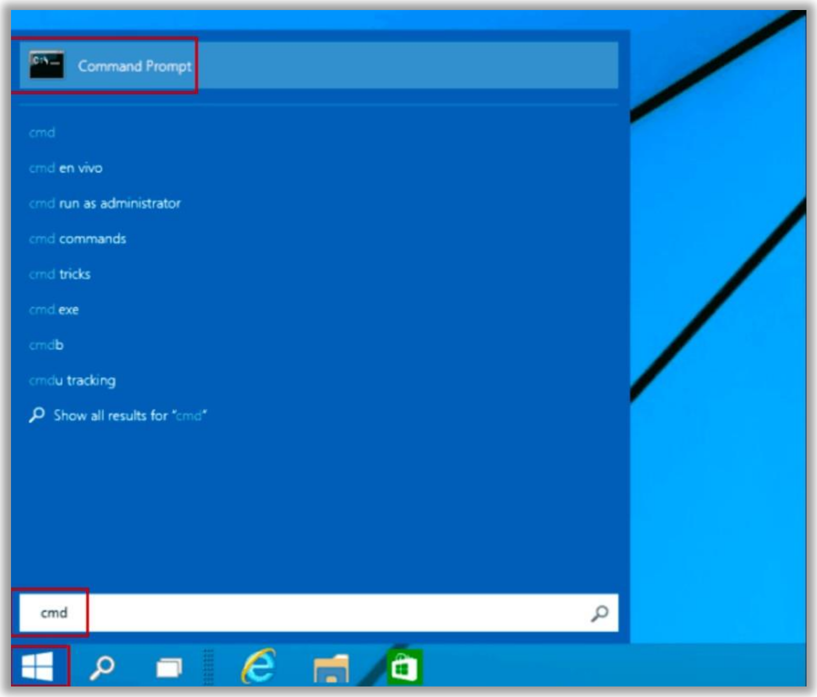
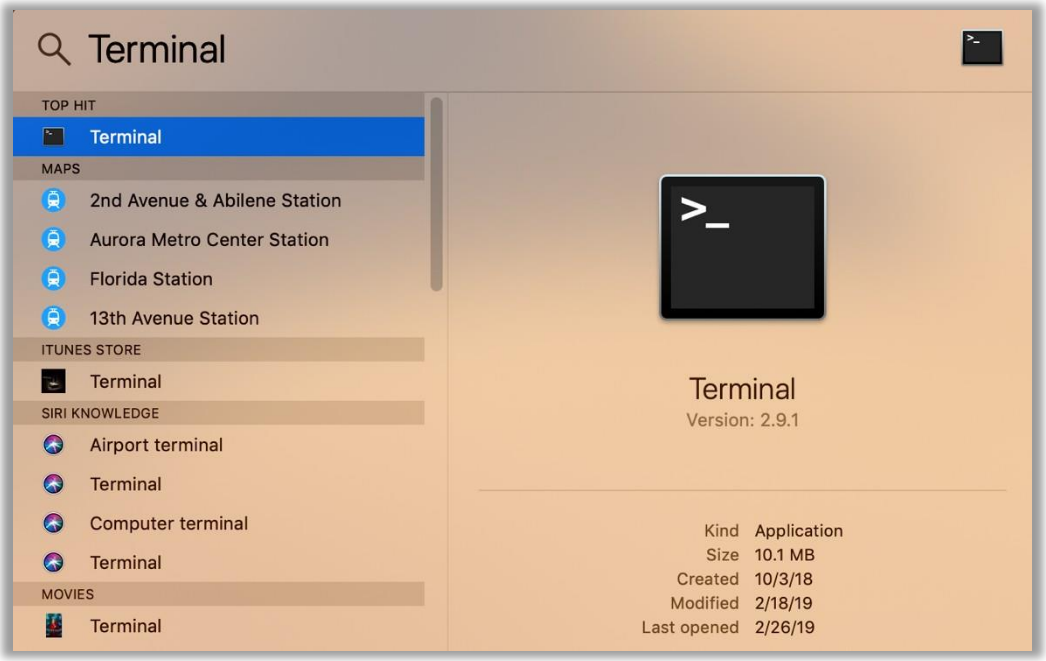


Figure 2-1 **Windows Command Prompt Navigation**

Mac users will find their Terminal by tapping the magnify glass on the top right of their screen. Type Terminal and hit return.



Kind Application
Size 10.1 MB
Created 10/3/18
Modified 2/18/19
Last opened 2/26/19

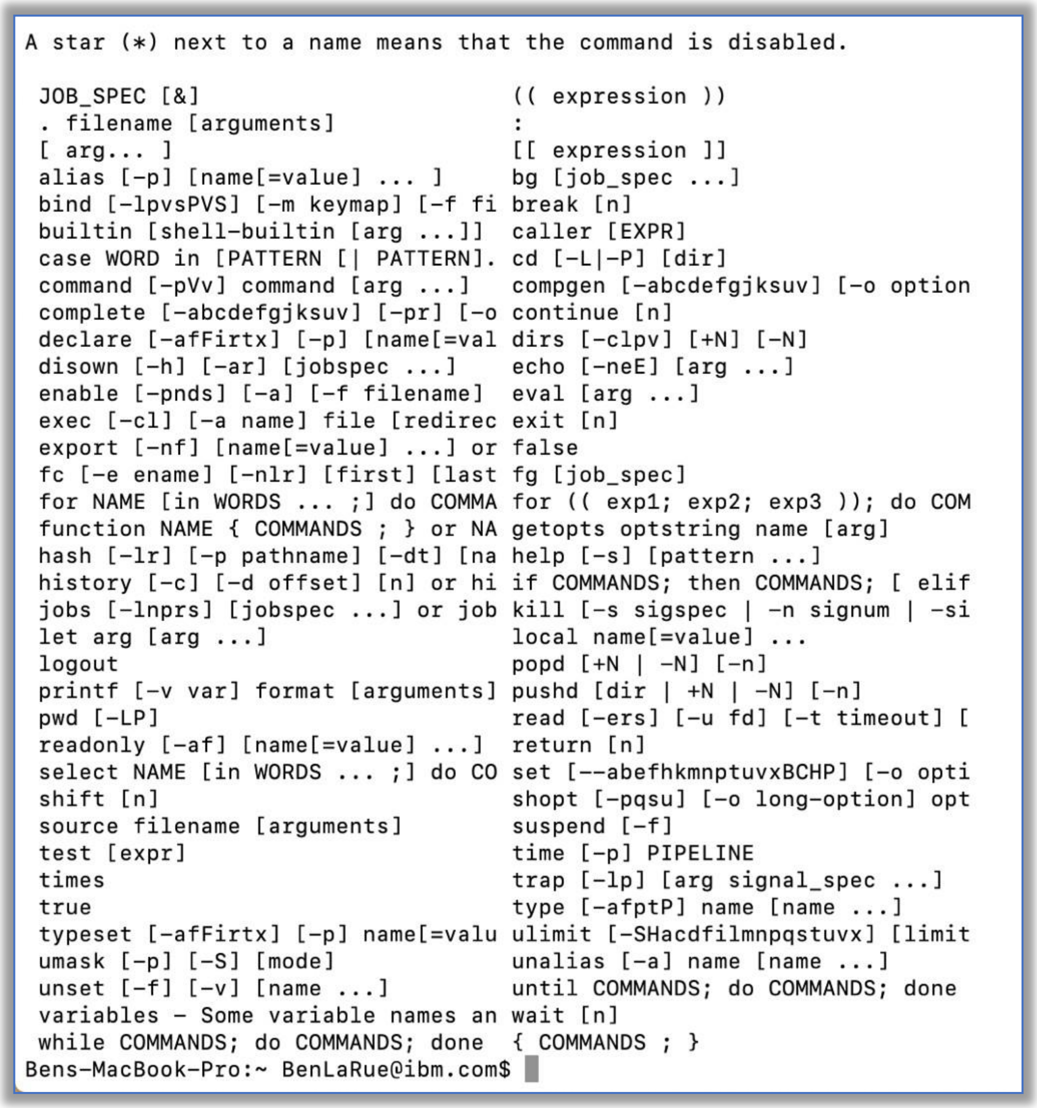
Figure 2-2 **Mac Terminal Navigation**

1. The first and most useful command we will utilize is help. This command will provide a menu of all the options you can perform inside your Command Line Interface.

   In the command line input:

```
help
```

Skim the available options. We will not go through all of them during this lab, but we will be hitting a few from this list.



```
A star (*) next to a name means that the command is disabled.

 JOB_SPEC [&]                       (( expression ))
 . filename [arguments]             :
 [ arg... ]                         [[ expression ]]
 alias [-p] [name[=value] ... ]     bg [job_spec ...]
 bind [-lpvsPVS] [-m keymap] [-f fi break [n]
 builtin [shell-builtin [arg ...]]  caller [EXPR]
 case WORD in [PATTERN [| PATTERN]. cd [-L|-P] [dir]
 command [-pVv] command [arg ...]   compgen [-abcdefgjksuv] [-o option
 complete [-abcdefgjksuv] [-pr] [-o continue [n]
 declare [-afFirtx] [-p] [name[=val dirs [-clpv] [+N] [-N]
 disown [-h] [-ar] [jobspec ...]    echo [-neE] [arg ...]
 enable [-pnds] [-a] [-f filename]  eval [arg ...]
 exec [-cl] [-a name] file [redirec exit [n]
 export [-nf] [name[=value] ...] or false
 fc [-e ename] [-nlr] [first] [last fg [job_spec]
 for NAME [in WORDS ... ;] do COMMA for (( exp1; exp2; exp3 )); do COM
 function NAME { COMMANDS ; } or NA getopts optstring name [arg]
 hash [-lr] [-p pathname] [-dt] [na help [-s] [pattern ...]
 history [-c] [-d offset] [n] or hi if COMMANDS; then COMMANDS; [ elif
 jobs [-lnprs] [jobspec ...] or job kill [-s sigspec | -n signum | -si
 let arg [arg ...]                  local name[=value] ...
 logout                             popd [+N | -N] [-n]
 printf [-v var] format [arguments] pushd [dir | +N | -N] [-n]
 pwd [-LP]                          read [-ers] [-u fd] [-t timeout] [
 readonly [-af] [name[=value] ...]  return [n]
 select NAME [in WORDS ... ;] do CO set [--abefhkmnptuvxBCHP] [-o opti
 shift [n]                          shopt [-pqsu] [-o long-option] opt
 source filename [arguments]        suspend [-f]
 test [expr]                        time [-p] PIPELINE
 times                              trap [-lp] [arg signal_spec ...]
 true                               type [-afptP] name [name ...]
 typeset [-afFirtx] [-p] name[=valu ulimit [-SHacdfilmnpqstuvx] [limit
 umask [-p] [-S] [mode]             unalias [-a] name [name ...]
 unset [-f] [-v] [name ...]         until COMMANDS; do COMMANDS; done
 variables - Some variable names an wait [n]
 while COMMANDS; do COMMANDS; done  { COMMANDS ; }
Bens-MacBook-Pro:~ BenLaRue@ibm.com$
```

Figure 2-3 **Available Help Options**

2. In the spirit of the previous section let’s continue looking at IP commands

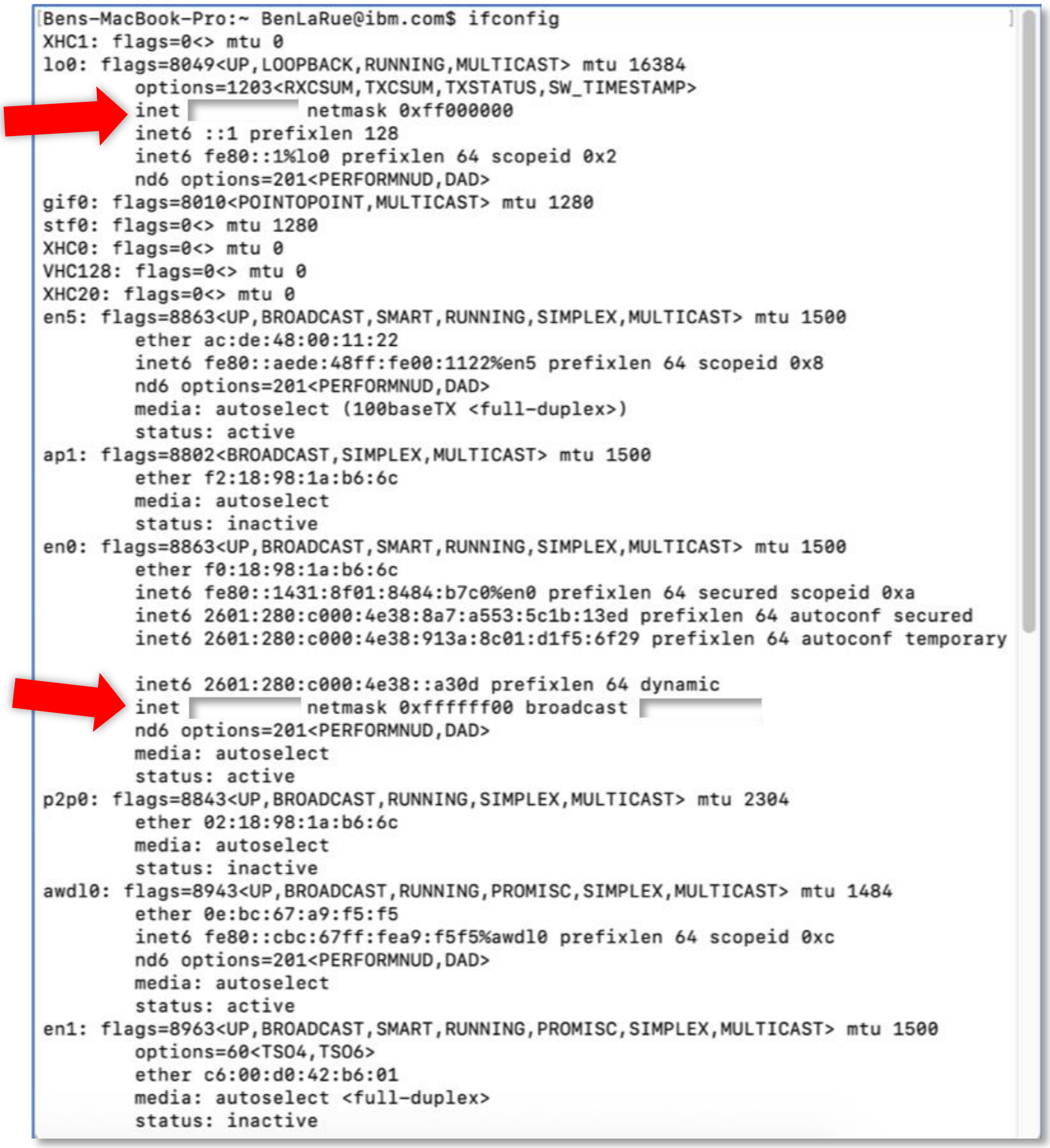
   Mac users: In the command line input:

```
ifconfig
```

   Windows users: In the command line input:

```
ipconfig
```

The ipconfig or ifconfig displays all current TCP/IP network configuration values and refreshes the Dynamic Host Configuration Protocol (DHCP) as well as the Domain Name System (DNS) settings.



```
Bens-MacBook-Pro:~ BenLaRue@ibm.com$ ifconfig
XHC1: flags=0<> mtu 0
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet [redacted] netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
XHC0: flags=0<> mtu 0
VHC128: flags=0<> mtu 0
XHC20: flags=0<> mtu 0
en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether ac:de:48:00:11:22
        inet6 fe80::aede:48ff:fe00:1122%en5 prefixlen 64 scopeid 0x8
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (100baseTX <full-duplex>)
        status: active
ap1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
        ether f2:18:98:1a:b6:6c
        media: autoselect
        status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether f0:18:98:1a:b6:6c
        inet6 fe80::1431:8f01:8484:b7c0%en0 prefixlen 64 secured scopeid 0xa
        inet6 2601:280:c000:4e38:8a7:a553:5c1b:13ed prefixlen 64 autoconf secured
        inet6 2601:280:c000:4e38:913a:8c01:d1f5:6f29 prefixlen 64 autoconf temporary

        inet6 2601:280:c000:4e38::a30d prefixlen 64 dynamic
        inet [redacted] netmask 0xffffff00 broadcast [redacted]
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
        ether 02:18:98:1a:b6:6c
        media: autoselect
        status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
        ether 0e:bc:67:a9:f5:f5
        inet6 fe80::cbc:67ff:fea9:f5f5%awdl0 prefixlen 64 scopeid 0xc
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=60<TSO4,TSO6>
        ether c6:00:d0:42:b6:01
        media: autoselect <full-duplex>
        status: inactive
```

Figure 2-4 **Network Configuration**

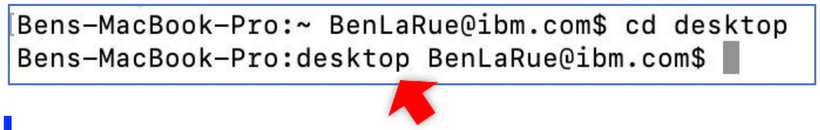
The Command Line Interface also lets us make changes to the computer and pull stored data. For instance, with two simple commands I can see all of the files stored in any directory.

3. First, we need to choose the directory we want to view (I am going to use my desktop)

   In the command line input:

```
cd desktop
```

You will know you are successful if the designated directory now shows before your username



```
[Bens-MacBook-Pro:~ BenLaRue@ibm.com$ cd desktop
Bens-MacBook-Pro:desktop BenLaRue@ibm.com$ 
```

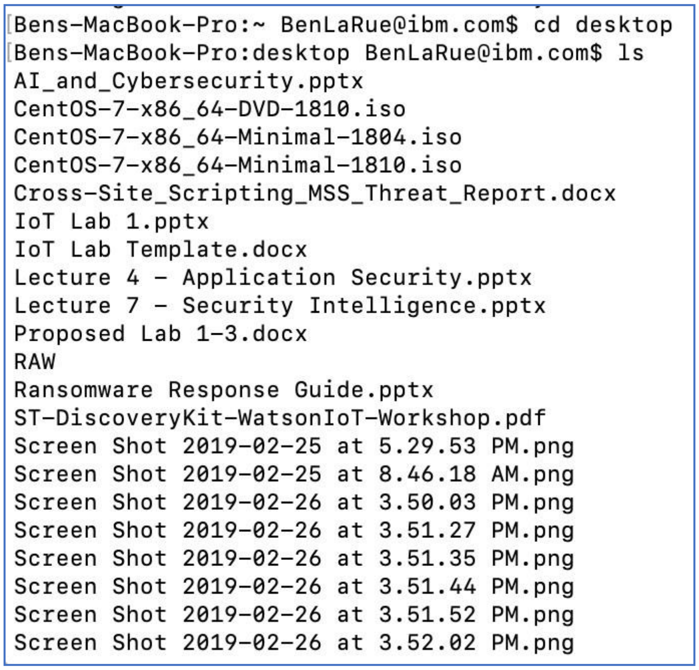
Figure 2-5 **Terminal (with desktop as designated directory)**

4. Once you have confirmed the directory has been designated

   In the command line input:

```
ls
```

As you can see my desktop is in serious need of cleaning. How is yours? How are you other directories? Try connecting to at least one other directory before moving on.



```
[Bens-MacBook-Pro:~ BenLaRue@ibm.com$ cd desktop
[Bens-MacBook-Pro:desktop BenLaRue@ibm.com$ ls
AI_and_Cybersecurity.pptx
CentOS-7-x86_64-DVD-1810.iso
CentOS-7-x86_64-Minimal-1804.iso
CentOS-7-x86_64-Minimal-1810.iso
Cross-Site_Scripting_MSS_Threat_Report.docx
IoT Lab 1.pptx
IoT Lab Template.docx
Lecture 4 - Application Security.pptx
Lecture 7 - Security Intelligence.pptx
Proposed Lab 1-3.docx
RAW
Ransomware Response Guide.pptx
ST-DiscoveryKit-WatsonIoT-Workshop.pdf
Screen Shot 2019-02-25 at 5.29.53 PM.png
Screen Shot 2019-02-25 at 8.46.18 AM.png
Screen Shot 2019-02-26 at 3.50.03 PM.png
Screen Shot 2019-02-26 at 3.51.27 PM.png
Screen Shot 2019-02-26 at 3.51.35 PM.png
Screen Shot 2019-02-26 at 3.51.44 PM.png
Screen Shot 2019-02-26 at 3.51.52 PM.png
Screen Shot 2019-02-26 at 3.52.02 PM.png
```

Figure 2-6 **Terminal (showing list of files after ls command)**

Milestone Summary

In this milestone, we learned how to access our network information without the need for an interface, just by entering commands to the computer.

In the next section, we will install and familiarize ourselves with Offensive Network Tools.

Milestone 3: Offensive Network Tools

Milestone Overview

This lab requires you to complete four Milestones:

1. The Data Behind Your IP Address
2. Command Line Interface (CLI)
3. **Offensive Network Tools**
4. Network Protection Practices

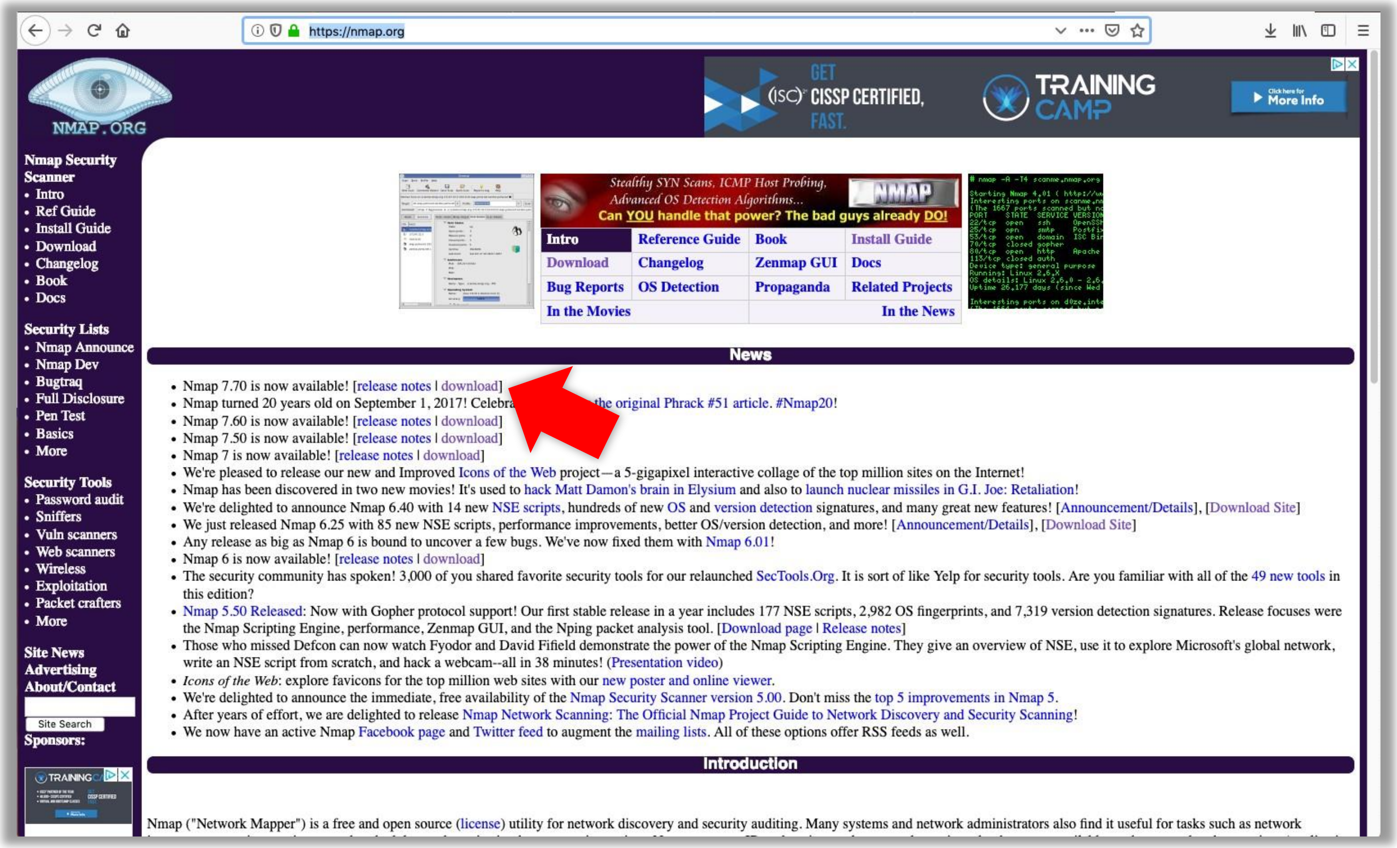
In this Milestone, we will learn how to download and use both NMAP, a network mapping tool, and Wireshark, a packet sniffer.

Zenmap

Nmap (Network Mapped) is a free and open source tool for network discovery and security auditing. Nmap was designed to rapidly scan large networks and provide reports of what services the network is hosting, what operating system they are running, and what type of packet filters or firewalls are in place. This makes it a great tool for taking network inventory, but it also makes an excellent tool for attackers to scan your network and get a general view of your security such as open ports.

Install Zenmap

1. Navigate to nmap.org.



News

- Nmap 7.70 is now available! [release notes | download]
- Nmap turned 20 years old on September 1, 2017! Celebra the original Phrack #51 article. #Nmap20!
- Nmap 7.60 is now available! [release notes | download]
- Nmap 7.50 is now available! [release notes | download]
- Nmap 7 is now available! [release notes | download]
- We're pleased to release our new and Improved Icons of the Web project—a 5-gigapixel interactive collage of the top million sites on the Internet!
- Nmap has been discovered in two new movies! It's used to hack Matt Damon's brain in Elysium and also to launch nuclear missiles in G.I. Joe: Retaliation!
- We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new OS and version detection signatures, and many great new features! [Announcement/Details], [Download Site]
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [Announcement/Details], [Download Site]
- Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with Nmap 6.01!
- Nmap 6 is now available! [release notes | download]
- The security community has spoken! 3,000 of you shared favorite security tools for our relaunched SecTools.Org. It is sort of like Yelp for security tools. Are you familiar with all of the 49 new tools in this edition?
- Nmap 5.50 Released: Now with Gopher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,982 OS fingerprints, and 7,319 version detection signatures. Release focuses were the Nmap Scripting Engine, performance, Zenmap GUI, and the Nping packet analysis tool. [Download page | Release notes]
- Those who missed Defcon can now watch Fyodor and David Fifield demonstrate the power of the Nmap Scripting Engine. They give an overview of NSE, use it to explore Microsoft's global network, write an NSE script from scratch, and hack a webcam--all in 38 minutes! (Presentation video)
- *Icons of the Web*: explore favicons for the top million web sites with our new poster and online viewer.
- We're delighted to announce the immediate, free availability of the Nmap Security Scanner version 5.00. Don't miss the top 5 improvements in Nmap 5.
- After years of effort, we are delighted to release Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning!
- We now have an active Nmap Facebook page and Twitter feed to augment the mailing lists. All of these options offer RSS feeds as well.

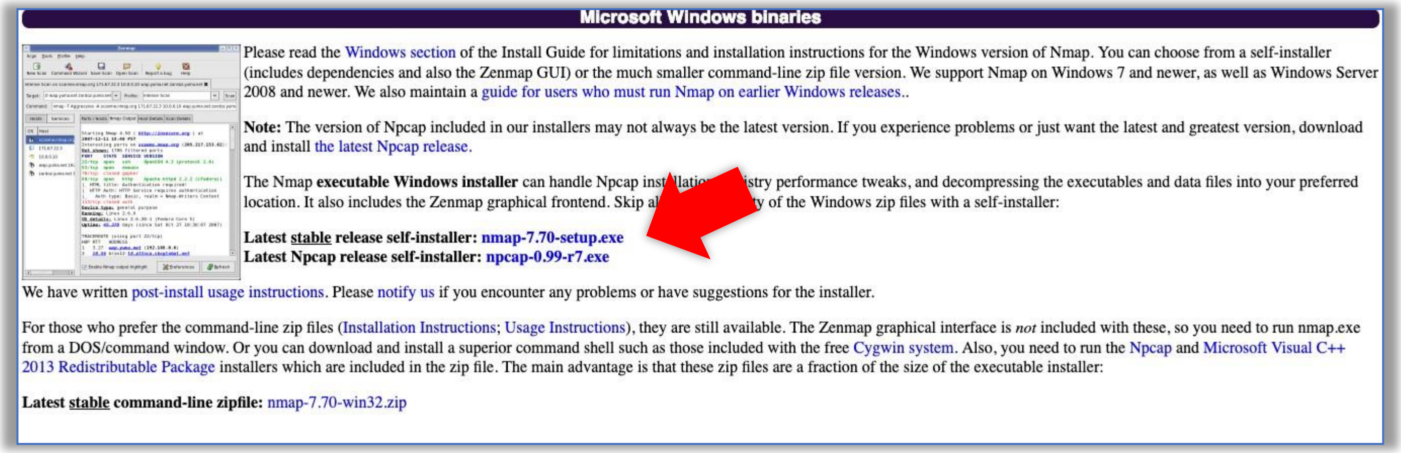
Introduction

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network

Figure 3-1 **Nmap Webpage**

2. Click on the "download" link next to Nmap 7.7.
3. Scroll down to the download file for your operating system.

Windows users will click on the "Latest stable releaseself-installer."


Microsoft Windows binaries

Please read the Windows section of the Install Guide for limitations and installation instructions for the Windows version of Nmap. You can choose from a self-installer (includes dependencies and also the Zenmap GUI) or the much smaller command-line zip file version. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 and newer. We also maintain a guide for users who must run Nmap on earlier Windows releases..

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install the latest Npcap release.

The Nmap **executable Windows installer** can handle Npcap inst llatio istry performance tweaks, and decompressing the executables and data files into your preferred location. It also includes the Zenmap graphical frontend. Skip al y of the Windows zip files with a self-installer:

Latest stable release self-installer: nmap-7.70-setup.exe
Latest Npcap release self-installer: npcap-0.99-r7.exe

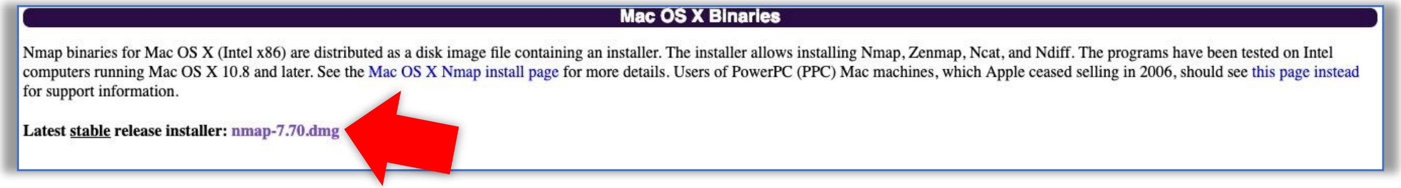
We have written post-install usage instructions. Please notify us if you encounter any problems or have suggestions for the installer.

For those who prefer the command-line zip files (Installation Instructions; Usage Instructions), they are still available. The Zenmap graphical interface is *not* included with these, so you need to run nmap.exe from a DOS/command window. Or you can download and install a superior command shell such as those included with the free Cygwin system. Also, you need to run the Npcap and Microsoft Visual C++ 2013 Redistributable Package installers which are included in the zip file. The main advantage is that these zip files are a fraction of the size of the executable installer:

Latest stable command-line zipfile: nmap-7.70-win32.zip

Figure 3-2 **Nmap Windows Download**

Mac users will click on the “Latest stable release installer.”



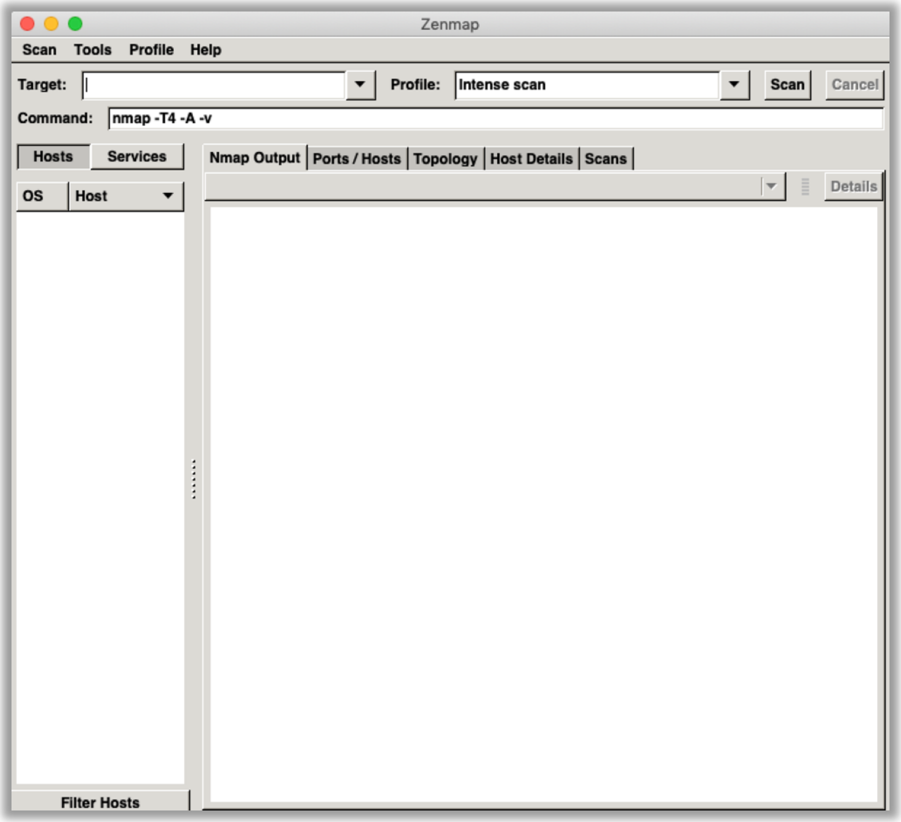
Mac OS X Binaries

Nmap binaries for Mac OS X (Intel x86) are distributed as a disk image file containing an installer. The installer allows installing Nmap, Zenmap, Ncat, and Ndiff. The programs have been tested on Intel computers running Mac OS X 10.8 and later. See the Mac OS X Nmap install page for more details. Users of PowerPC (PPC) Mac machines, which Apple ceased selling in 2006, should see this page instead for support information.

Latest stable release installer: nmap-7.70.dmg

Figure 3-3 **Nmap Mac Download**

4. Follow the directions of the installer, and once finished, open Zenmap.



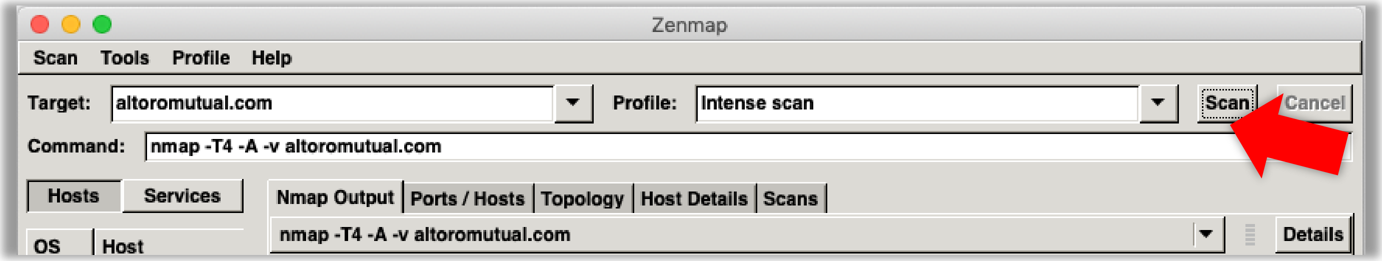
Profile: Intense scan

Command: nmap -T4 -A -v

Figure 3-4 **Zenmap**

Zenmap Basic Functionality

1. Inside the target box input either a domain or IP Address (we will be using altoromutual.com) and hit scan.



Target: altoromutual.com

Profile: Intense scan

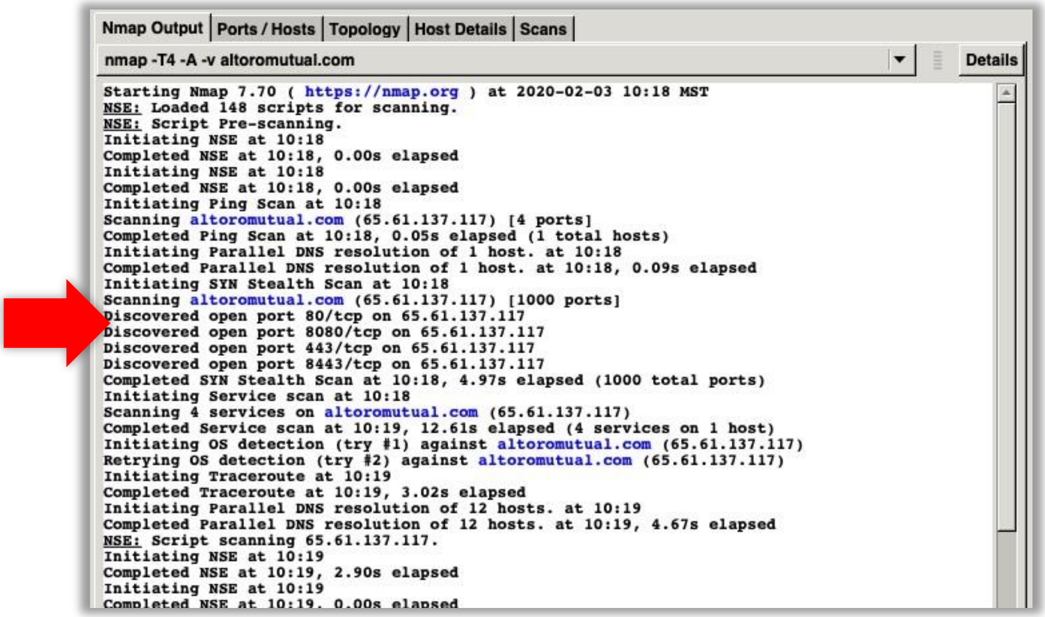
Command: nmap -T4 -A -v altoromutual.com

nmap -T4 -A -v altoromutual.com

Figure 3-4 **Zenmap targeting AltoroMutual**

2. Watch as Zenmap starts it's scan and goes through multiple CLI commands such as Ping and Traceroute.

3. The report may have been generated to fast to follow but scroll up and check if Zenmap found any open ports.



nmap -T4 -A -v altoromutual.com

```
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-03 10:18 MST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:18
Completed NSE at 10:18, 0.00s elapsed
Initiating NSE at 10:18
Completed NSE at 10:18, 0.00s elapsed
Initiating Ping Scan at 10:18
Scanning altoromutual.com (65.61.137.117) [4 ports]
Completed Ping Scan at 10:18, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:18
Completed Parallel DNS resolution of 1 host. at 10:18, 0.09s elapsed
Initiating SYN Stealth Scan at 10:18
Scanning altoromutual.com (65.61.137.117) [1000 ports]
Discovered open port 80/tcp on 65.61.137.117
Discovered open port 8080/tcp on 65.61.137.117
Discovered open port 443/tcp on 65.61.137.117
Discovered open port 8443/tcp on 65.61.137.117
Completed SYN Stealth Scan at 10:18, 4.97s elapsed (1000 total ports)
Initiating Service scan at 10:18
Scanning 4 services on altoromutual.com (65.61.137.117)
Completed Service scan at 10:19, 12.61s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against altoromutual.com (65.61.137.117)
Retrying OS detection (try #2) against altoromutual.com (65.61.137.117)
Initiating Traceroute at 10:19
Completed Traceroute at 10:19, 3.02s elapsed
Initiating Parallel DNS resolution of 12 hosts. at 10:19
Completed Parallel DNS resolution of 12 hosts. at 10:19, 4.67s elapsed
NSE: Script scanning 65.61.137.117.
Initiating NSE at 10:19
Completed NSE at 10:19, 2.90s elapsed
Initiating NSE at 10:19
Completed NSE at 10:19, 0.00s elapsed
```

Figure 3-4 **Zenmap discovering open ports**

Wireshark

Wireshark is a free and open-source packet analyser; often referred to as a “sniffer”. It is used for network troubleshooting analysis, software and communications protocol development, and education. Wireshark is used to examine the details of traffic as data is sent from one connection to the other.

Install Wireshark

1. Navigate to wireshark.org

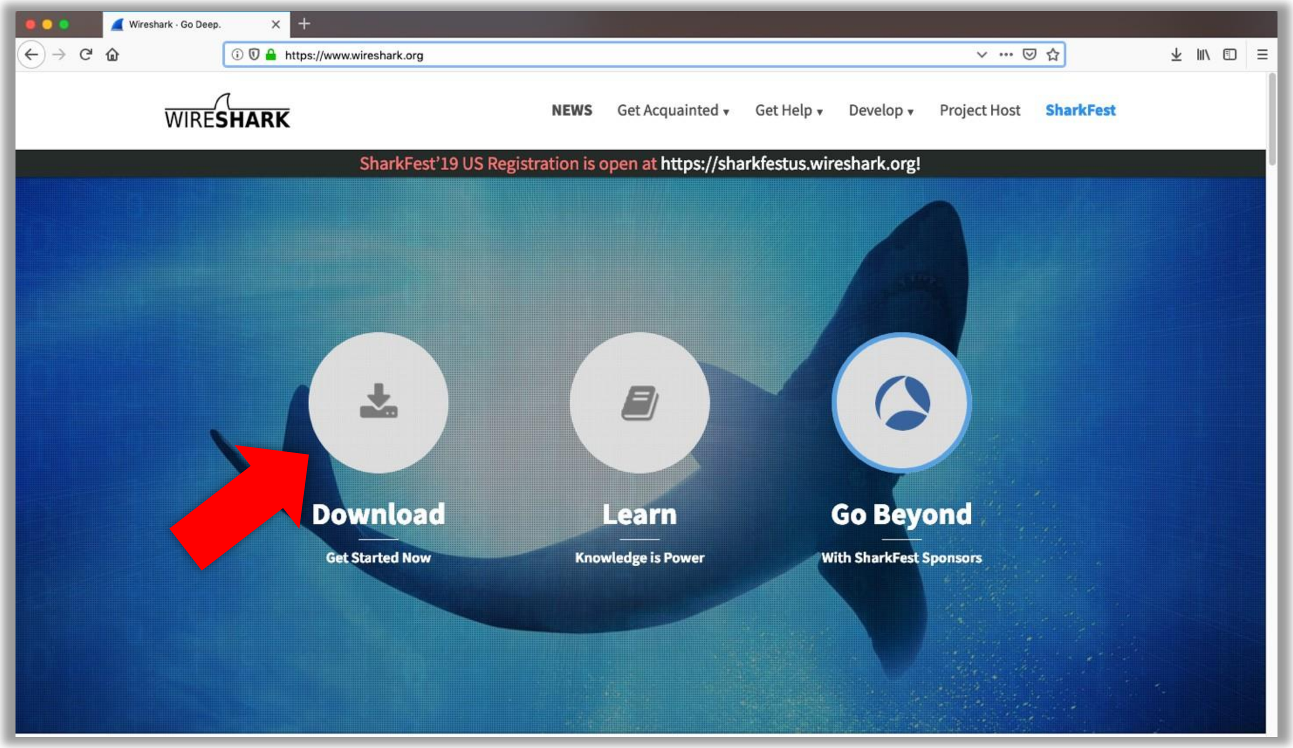
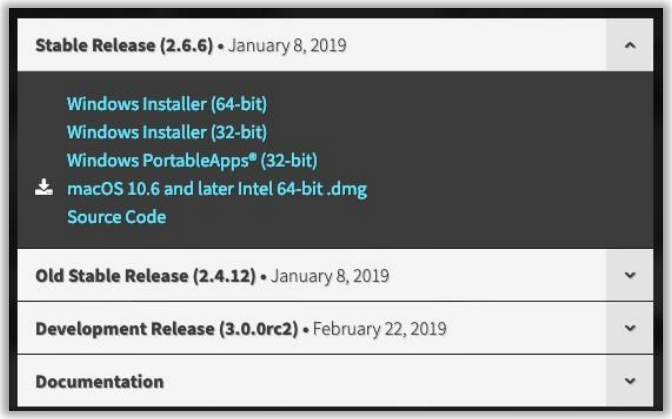


Figure 3-5 **Wireshark Webpage**

2. Click on “Download”

3. Select the most current stable release for your operating system



Stable Release (2.6.6) • January 8, 2019

Windows Installer (64-bit)
Windows Installer (32-bit)
Windows PortableApps® (32-bit)
macOS 10.6 and later Intel 64-bit .dmg
Source Code

Old Stable Release (2.4.12) • January 8, 2019

Development Release (3.0.0rc2) • February 22, 2019

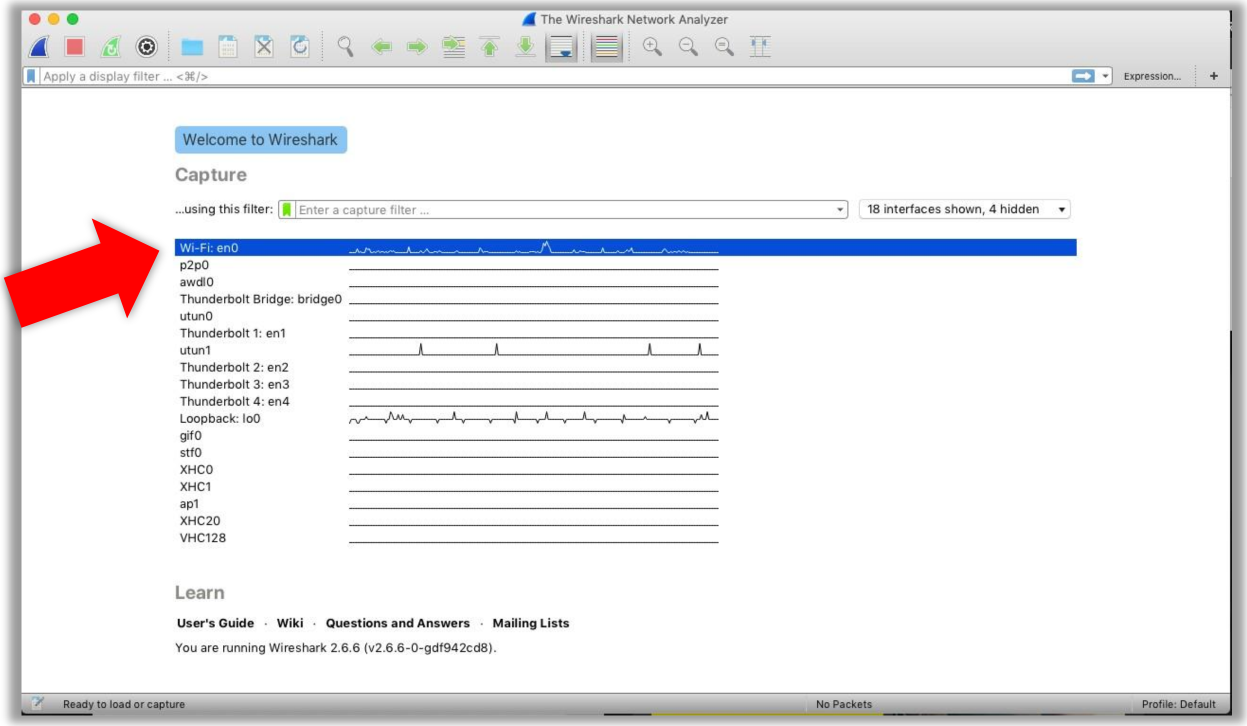
Documentation

Figure 3-6 **Wireshark Downloads**

4. Run the file and click through the installation process.

Wireshark Basic Functionality

1. Open Wireshark.
2. From the list of interfaces shown select your internet network.



The Wireshark Network Analyzer
Apply a display filter ... <⌘/>
Expression...
+

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ...

18 interfaces shown, 4 hidden

Wi-Fi: en0
p2p0
awdl0
Thunderbolt Bridge: bridge0
utun0
Thunderbolt 1: en1
utun1
Thunderbolt 2: en2
Thunderbolt 3: en3
Thunderbolt 4: en4
Loopback: lo0
gif0
stf0
XHC0
XHC1
ap1
XHC20
VHC128

Learn

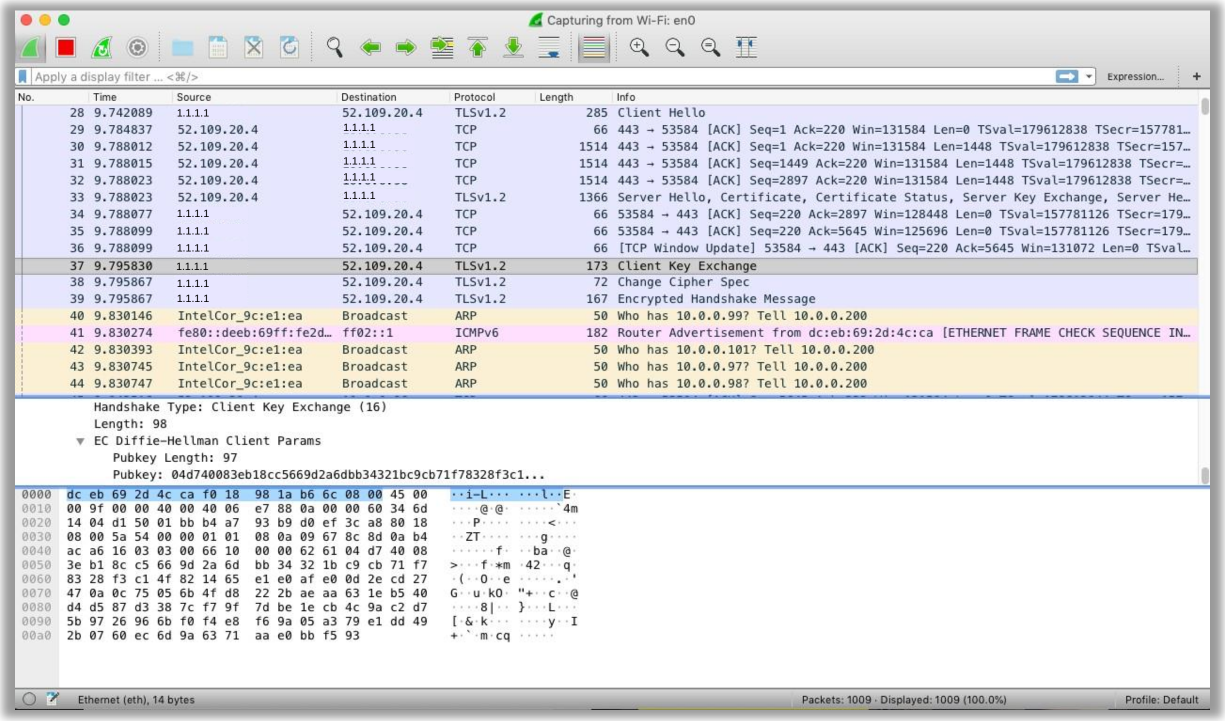
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.6.6 (v2.6.6-0-gdf942cd8).

Ready to load or capture | No Packets | Profile: Default

Figure 3-7 **Wireshark Internet Network Options**

Wireshark will immediately begin capturing data.



```
No.   Time      Source                 Destination   Protocol  Length  Info
   28 9.742089  1.1.1.1                52.109.20.4   TLSv1.2      285  Client Hello
   29 9.784837  52.109.20.4            1.1.1.1       TCP           66  443 → 53584 [ACK] Seq=1 Ack=220 Win=131584 Len=0 TSval=179612838 TSecr=157781…
   30 9.788012  52.109.20.4            1.1.1.1       TCP         1514  443 → 53584 [ACK] Seq=1 Ack=220 Win=131584 Len=1448 TSval=179612838 TSecr=157…
   31 9.788015  52.109.20.4            1.1.1.1       TCP         1514  443 → 53584 [ACK] Seq=1449 Ack=220 Win=131584 Len=1448 TSval=179612838 TSecr=…
   32 9.788023  52.109.20.4            1.1.1.1       TCP         1514  443 → 53584 [ACK] Seq=2897 Ack=220 Win=131584 Len=1448 TSval=179612838 TSecr=…
   33 9.788023  52.109.20.4            1.1.1.1       TLSv1.2     1366  Server Hello, Certificate, Certificate Status, Server Key Exchange, Server He…
   34 9.788077  1.1.1.1                52.109.20.4   TCP           66  53584 → 443 [ACK] Seq=220 Ack=2897 Win=128448 Len=0 TSval=157781126 TSecr=179…
   35 9.788099  1.1.1.1                52.109.20.4   TCP           66  53584 → 443 [ACK] Seq=220 Ack=5645 Win=125696 Len=0 TSval=157781126 TSecr=179…
   36 9.788099  1.1.1.1                52.109.20.4   TCP           66  [TCP Window Update] 53584 → 443 [ACK] Seq=220 Ack=5645 Win=131072 Len=0 TSval…
   37 9.795830  1.1.1.1                52.109.20.4   TLSv1.2      173  Client Key Exchange
   38 9.795867  1.1.1.1                52.109.20.4   TLSv1.2       72  Change Cipher Spec
   39 9.795867  1.1.1.1                52.109.20.4   TLSv1.2      167  Encrypted Handshake Message
   40 9.830146  IntelCor_9c:e1:ea      Broadcast     ARP           50  Who has 10.0.0.99? Tell 10.0.0.200
   41 9.830274  fe80::deeb:69ff:fe2d…  ff02::1       ICMPv6       182  Router Advertisement from dc:eb:69:2d:4c:ca [ETHERNET FRAME CHECK SEQUENCE IN…
   42 9.830393  IntelCor_9c:e1:ea      Broadcast     ARP           50  Who has 10.0.0.101? Tell 10.0.0.200
   43 9.830745  IntelCor_9c:e1:ea      Broadcast     ARP           50  Who has 10.0.0.97? Tell 10.0.0.200
   44 9.830747  IntelCor_9c:e1:ea      Broadcast     ARP           50  Who has 10.0.0.98? Tell 10.0.0.200
```

```
        Handshake Type: Client Key Exchange (16)
        Length: 98
      ▼ EC Diffie-Hellman Client Params
          Pubkey Length: 97
          Pubkey: 04d740083eb18cc5669d2a6dbb34321bc9cb71f78328f3c1...
```

```
0000  dc eb 69 2d 4c ca f0 18  98 1a b6 6c 08 00 45 00   ··i-L··· ···l··E·
0010  00 9f 00 00 40 00 40 06  e7 88 0a 00 00 60 34 6d   ····@·@· ·····`4m
0020  14 04 d1 50 01 bb b4 a7  93 b9 d0 ef 3c a8 80 18   ···P···· ····<···
0030  08 00 5a 54 00 00 01 01  08 0a 09 67 8c 8d 0a b4   ··ZT···· ···g····
0040  ac a6 16 03 03 00 66 10  00 00 62 61 04 d7 40 08   ······f· ··ba··@·
0050  3e b1 8c c5 66 9d 2a 6d  bb 34 32 1b c9 cb 71 f7   >···f·*m ·42···q·
0060  83 28 f3 c1 4f 82 14 65  e1 e0 af e0 0d 2e cd 27   ·(··O··e ·····.·'
0070  47 0a 0c 75 05 6b 4f d8  22 2b ae aa 63 1e b5 40   G··u·kO· "+··c··@
0080  d4 d5 87 d3 38 7c f7 9f  7d be 1e cb 4c 9a c2 d7   ····8|·· }···L···
0090  5b 97 26 96 6b f0 f4 e8  f6 9a 05 a3 79 e1 dd 49   [·&·k··· ····y··I
00a0  2b 07 60 ec 6d 9a 63 71  aa e0 bb f5 93            +·`·m·cq ·····
```

Figure 3-8 **Wireshark Screen Showing the Data Captured**

Please be careful where you point Wireshark as it is illegal to scan a network you do not have authorization to scan. Once Wireshark is running you can click into any of these packet instances to dive deeper into the information that was shared. Can you find sensitive information? Can you find encrypted information?

Milestone Summary

Nmap is a software that performs port scans to check network security and can also be used to discover services and servers on a computer network. Wireshark captures data, in what is called a "packet", each organized by protocol, to analyze network traffic.

Milestone 4: Network Protection Practices

Milestone Overview

This lab requires you to complete four Milestones:

1. The Data Behind Your IP Address
2. Command Line Interface (CLI)
3. Offensive Network Tools
4. **Network Protection Practices**

With so many tools that attackers can use to scan our networks there must be something we can do to protect ourselves and verify that the domain we wish to connect to is indeed the correct connection. A Domain Name System is our answer. Quad9 provides security for DNS queries by automatically blocking websites that are known to steal personal information, infect users with malware, or conduct illegal activity.

Installing Quad9 on Windows

1. Open your control panel
2. Select "Network and Internet"

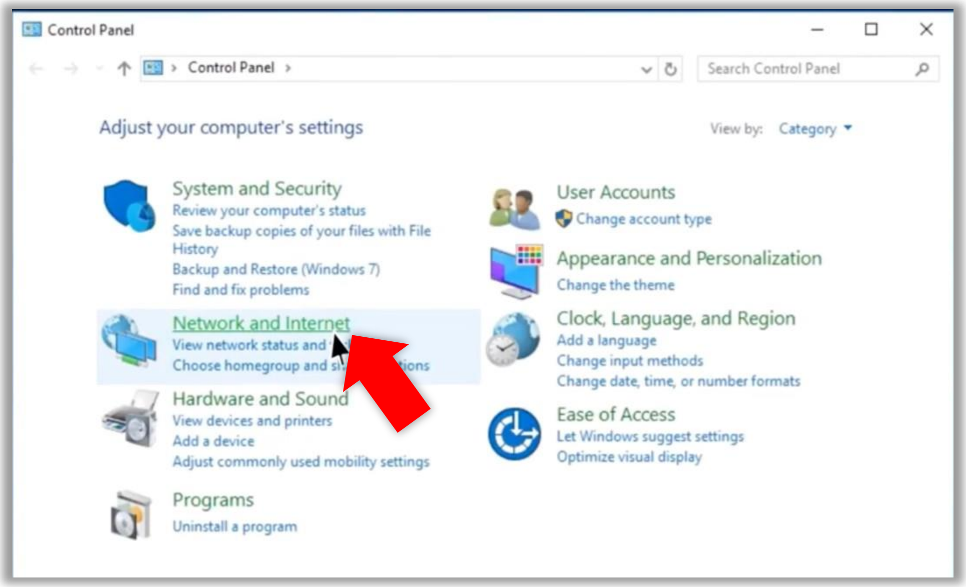


Figure 4-1 **Windows Control Panel**

3. Click “Network and Sharing Center”

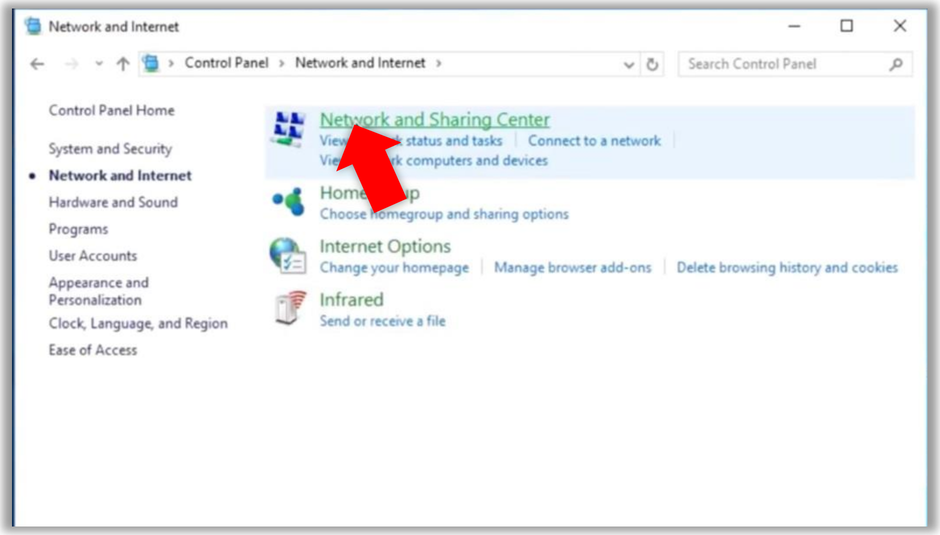
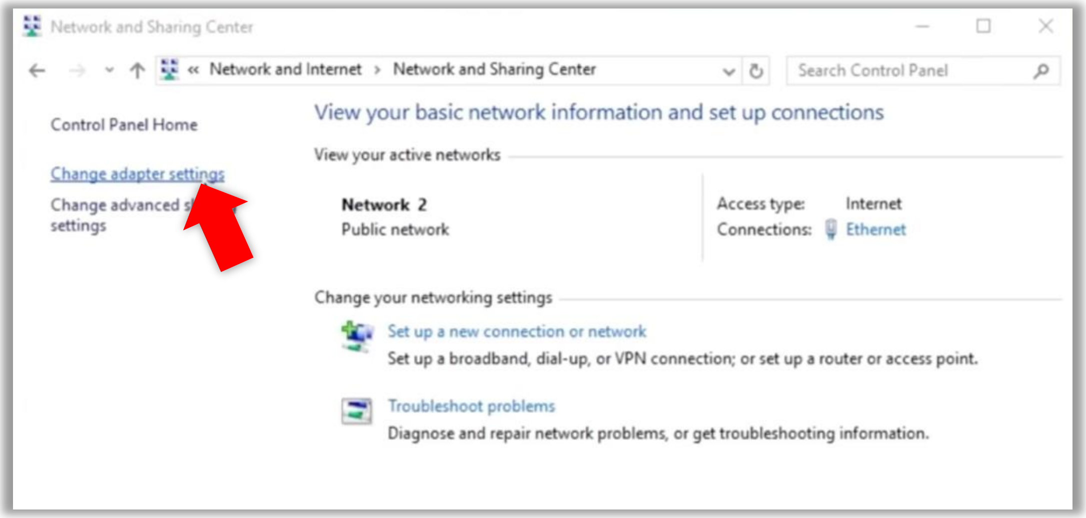


Figure 4-2 **Windows Network and Internet**

4. Click “Change adapter settings” on the left side-menu


Network and Sharing Center
« Network and Internet > Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
View your active networks
Network 2
Public network
Access type: Internet
Connections: Ethernet
Change your networking settings
Set up a new connection or network
Troubleshoot problems

Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Diagnose and repair network problems, or get troubleshooting information.

Figure 4-3 **Windows Network and Sharing Center**

5. Right-click on your internet connection and click into “Properties”

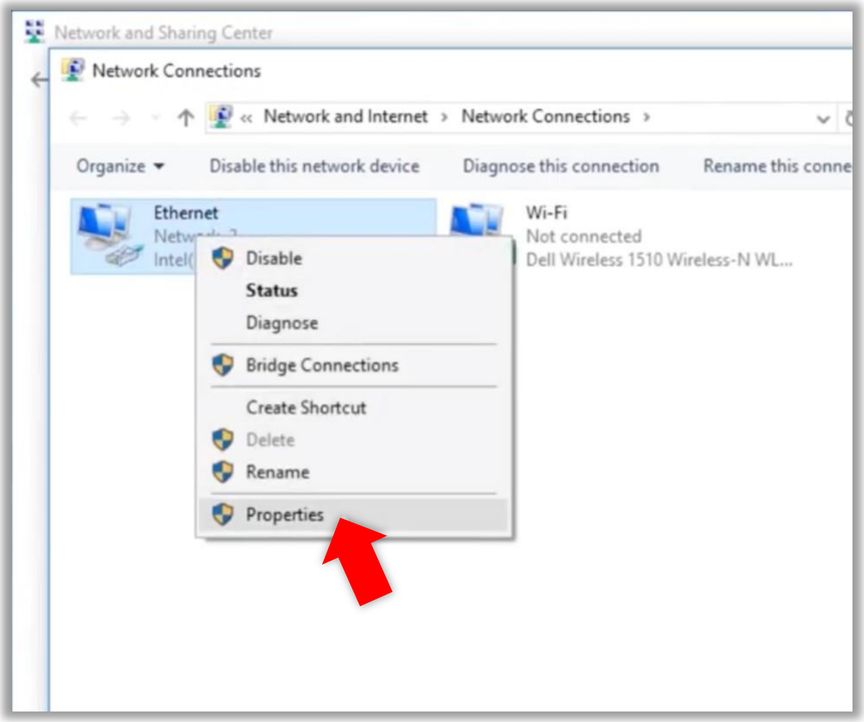
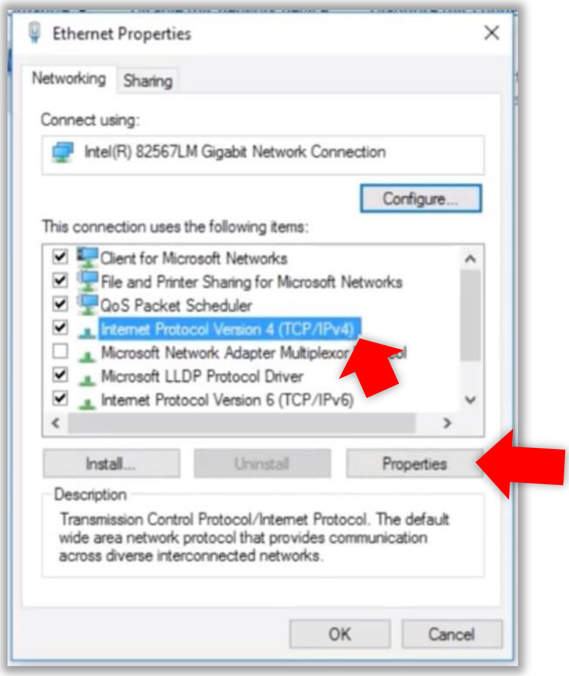


Figure 4-4 **Windows Change Adapter Settings**

6. Select “Internet Protocol Version 4 (TCP/IPv4)” and then click “Properties”



Connect using:

Intel(R) 82567LM Gigabit Network Connection

This connection uses the following items:

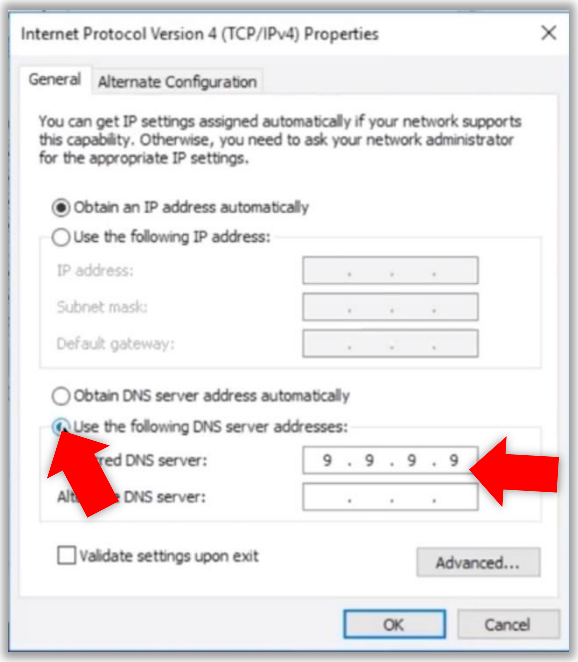
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor ...ol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Figure 4-5 **Windows Adapter Settings Properties**

7. Select “Use the following DNS server addresses” and type “9.9.9.9” and hit “OK” then close to save your settings.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 9 . 9 . 9 . 9

Alternate DNS server: . . .

□ Validate settings upon exit

Figure 4-6 **Internet Protocol Version 4 (TCP/IPv4) Properties**

You are now protected by Quad9 DNS!

Installing Quad9 on Mac

1. Go to System Preferences and select “Network”

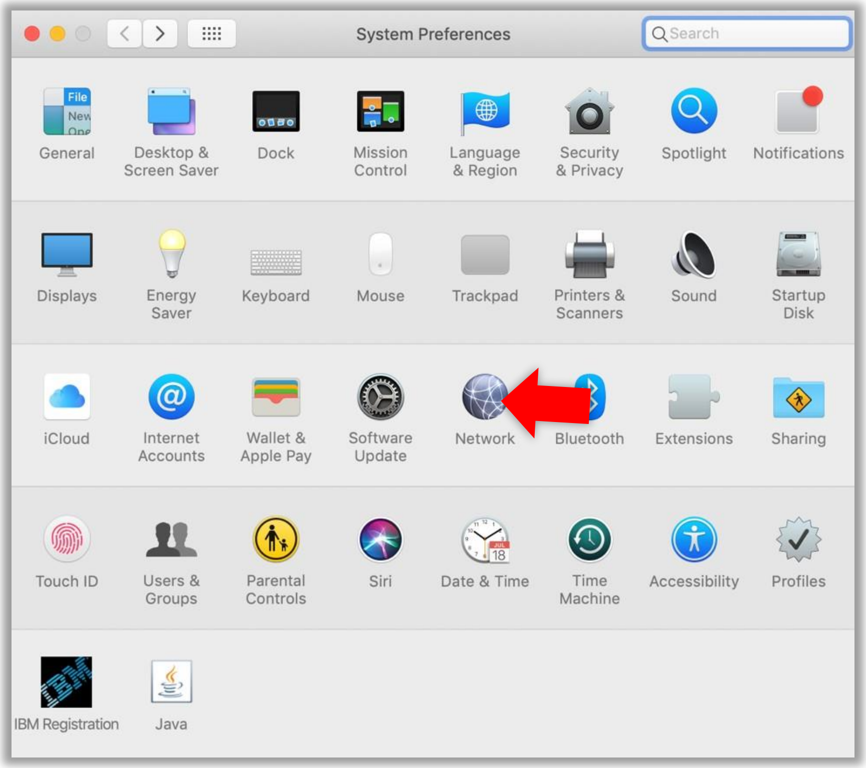
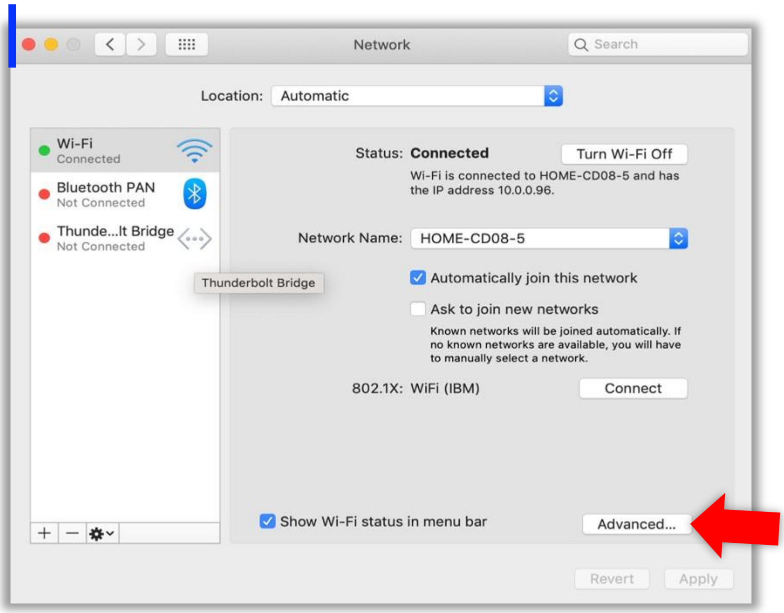


Figure 4-7 **Mac System Preferences**

2. Inside Network click “Advanced”



Location: Automatic

Wi-Fi Connected

Bluetooth PAN Not Connected

Thunde...lt Bridge Not Connected

Status: **Connected**

Wi-Fi is connected to HOME-CD08-5 and has the IP address 10.0.0.96.

Network Name: HOME-CD08-5

☑ Automatically join this network

□ Ask to join new networks

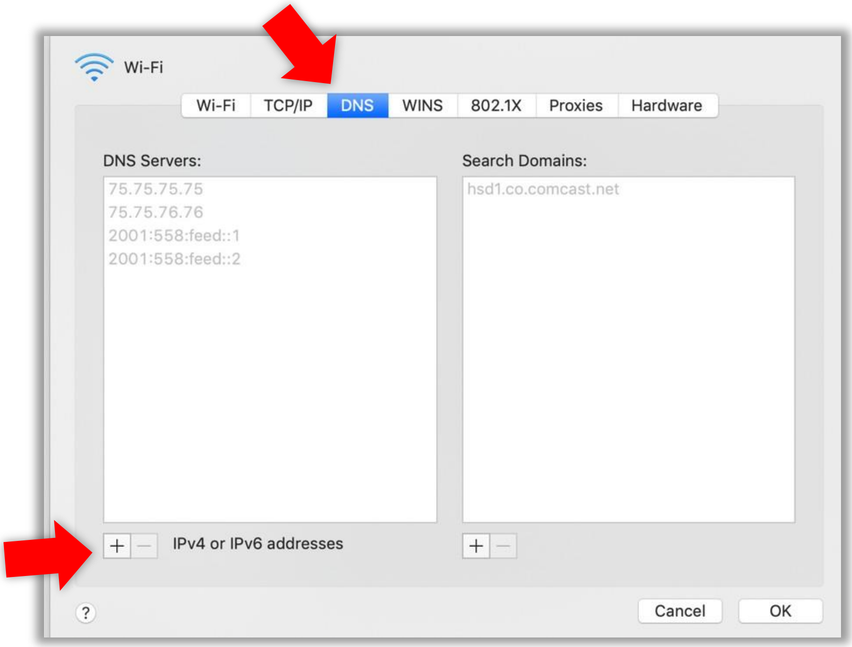
Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.

802.1X: WiFi (IBM)

☑ Show Wi-Fi status in menu bar

Figure 4-8 **Mac - Network**

3. Select “DNS” from the top menu and click on the “+” sign to add a new DNS server

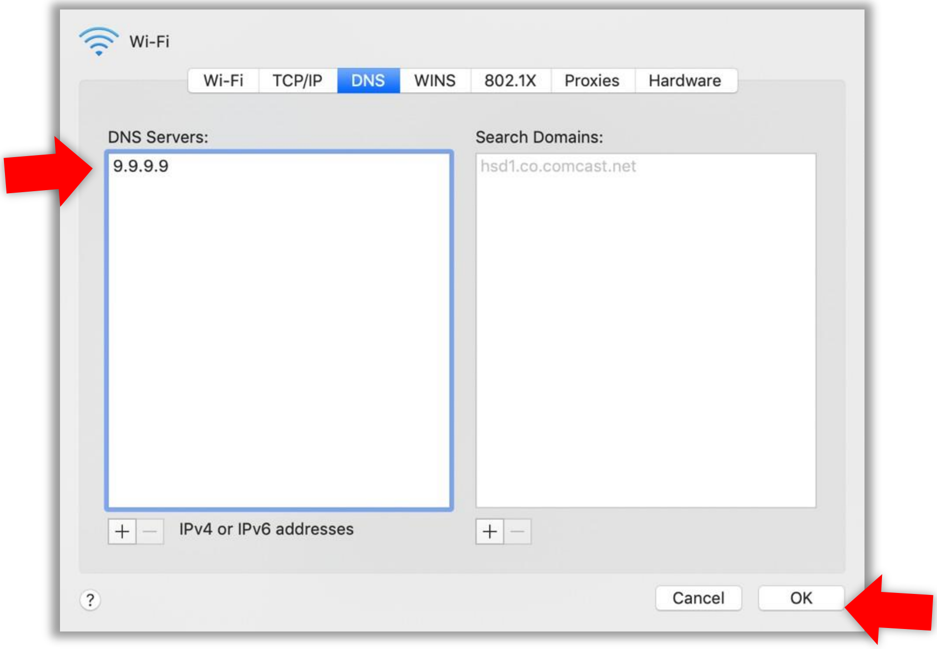


DNS Servers:
75.75.75.75
75.75.76.76
2001:558:feed::1
2001:558:feed::2

Search Domains:
hsd1.co.comcast.net

Figure 4-9 **Mac – Advanced Network**

4. Enter 9.9.9.9 at the top of the list and hit “OK” to exit and hit “Apply” to save



DNS Servers:
9.9.9.9

Search Domains:
hsd1.co.comcast.net

Figure 4-10 **Mac – Advanced Network - DNS**

You are now protected by Quad9 DNS!

Milestone Summary

Quad9 provides security for DNS queries by automatically blocking websites that are known to steal personal information, infect users with malware, or conduct illegal activity. By adding Quad9, we have quickly and easily brought another level of security into our network.

The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. This information is based on current IBM product plans and strategy, which are subject to change by IBM without notice. Product release dates and/or capabilities referenced in these materials may change at any time at IBM’s sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way.