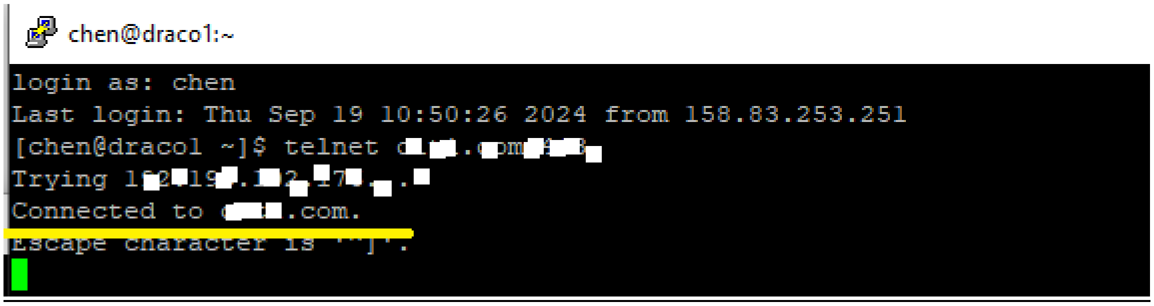
CMSC3180: Data Communication and Networking
Assignment 2 Due in class on Wednesday (09/25)

Policies:

1. Discussions on these questions are welcomed and encouraged. However, you should NOT ask any other person to write solution for you or copy solutions from any other person directly. You should write the names from whom you received help and cite the references used if any.
2. Late turn in will cause a 10% deduction on your grade for each late day.
3. Either turn in hard-copy in class or submit e-copy to D2L dropbox.

Question 1. (**10 points**) Use telnet on DRACO1, a Unix server available to students in this course (if you have a Mac, telnet is already included) to check which ports are open on a machine (***any machine, not necessary at pennwest.edu)***. You need to find at least **three different** ports that are open. These three ports don't need to be on the same machine, e.g., port number #1 could be on machine 1 and port #2 could be on machine 2. If a port is open, you will see "Connected to …." (see image below). Your solution to this question will be screenshots showing the "Connected to " a particular port.

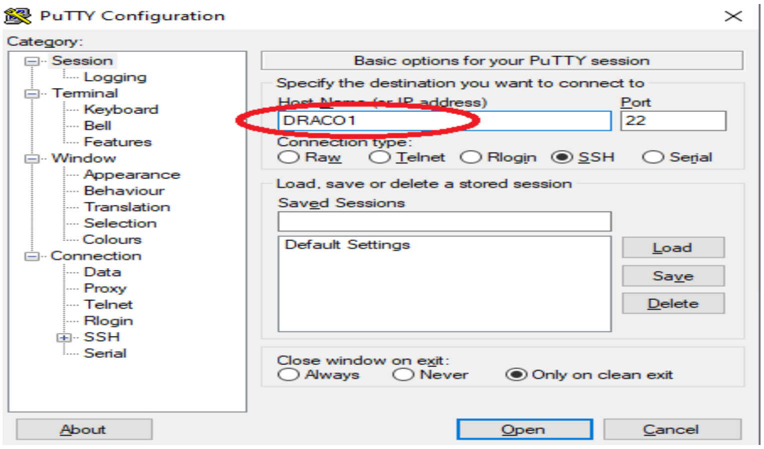


```
chen@draco1:~
login as: chen
Last login: Thu Sep 19 10:50:26 2024 from 158.83.253.251
[chen@draco1 ~]$ telnet [redacted]
Trying [redacted]
Connected to [redacted].com.
Escape character is '^]'.
```

<u>**Hints**</u>:

- Install VPN https://pennwest.samanage.com/solutions/1326719-student-vpn-instructions
- To login to DRACO1, download Putty.exe https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

  Type "DRACO1" in host, then click "Open". Then login with your PennWest email account (only the ABC1234, without @pennwest.edu)



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): DRACO1 Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

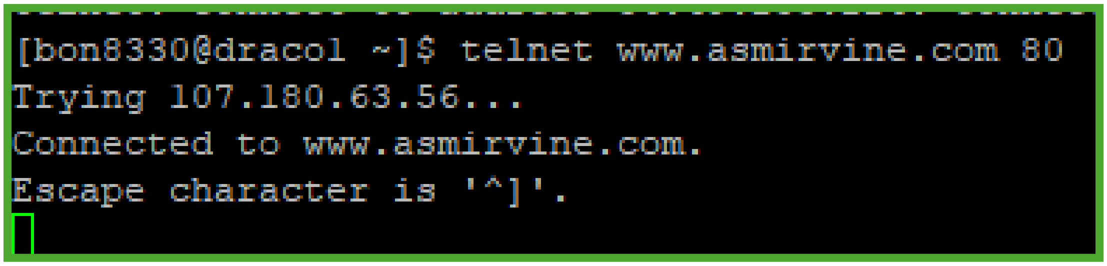
Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

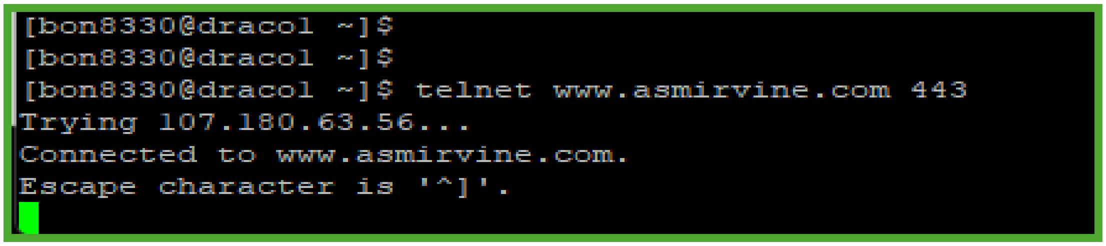
- A list of common port https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
- The machine you telnet to CANNOT be the same machine where you type the Telnet

Connection 1: *Port 80*



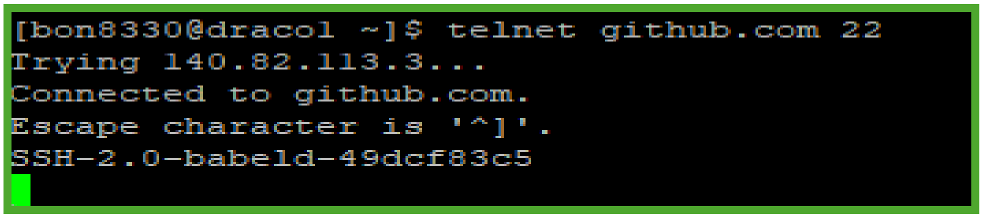
```
[bon8330@dracol ~]$ telnet www.asmirvine.com 80
Trying 107.180.63.56...
Connected to www.asmirvine.com.
Escape character is '^]'.
```

Connection 2: *Port 443*



```
[bon8330@dracol ~]$
[bon8330@dracol ~]$
[bon8330@dracol ~]$ telnet www.asmirvine.com 443
Trying 107.180.63.56...
Connected to www.asmirvine.com.
Escape character is '^]'.
```

Connection 3: *Port 22*

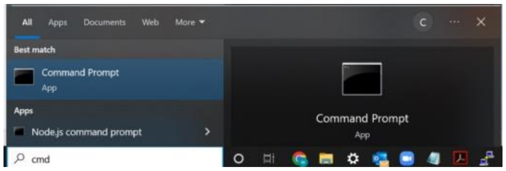


```
[bon8330@dracol ~]$ telnet github.com 22
Trying 140.82.113.3...
Connected to github.com.
Escape character is '^]'.
SSH-2.0-babeld-49dcf83c5
```

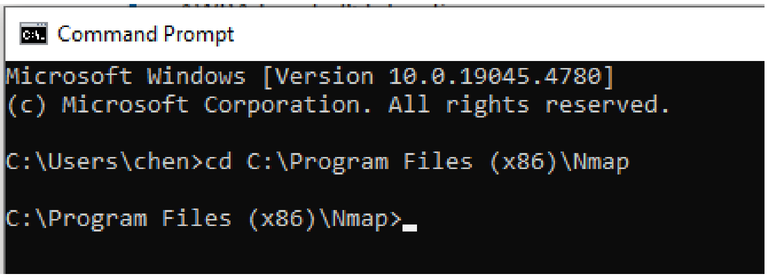
Question 2. (**10 points**) Following the demo in class (slide #2-31 of Chapter 2, screenshots of live demo are attached here), use Command Prompt (type CMD in Windows search) or Terminal in Mac to connect to a webserver (port 80) and use the GET command to request a webpage. Try one successful response (i.e., 200 OK) and one bad response (e.g, 301, 400, 404 or 505). Your solution to this question will be screenshots showing your HTTP interaction with one successful response from the server and one bad response. **Note:** your request webpage can't be the one already shown on slide #2-31, nor the one demoed in class students.pennwest.du/chen/index.htm

1. Install NAMP https://nmap.org/download. Remember where it is installed. For example, it is installed on my C:\Program Files (x86)\Nmap"

2. Launch CMD by typing CMD in your Windows search

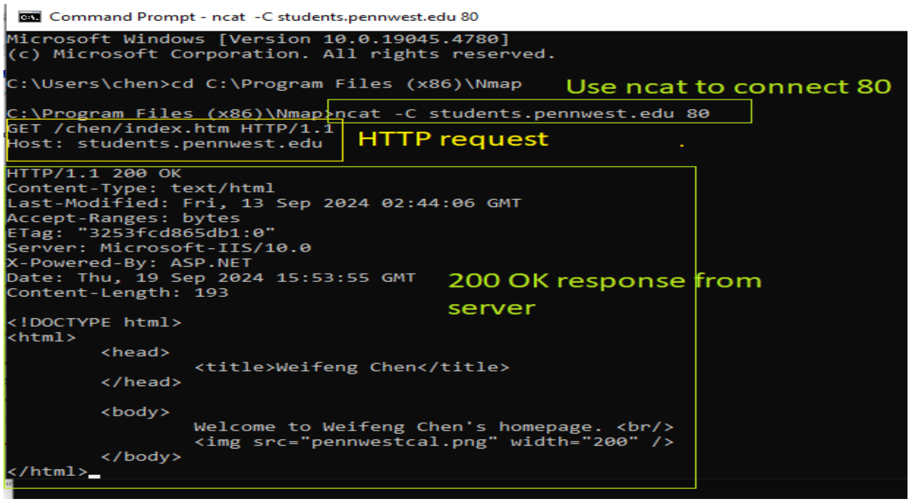


3. Change your location to Nmap's location



```
Microsoft Windows [Version 10.0.19045.4780]
(c) Microsoft Corporation. All rights reserved.

C:\Users\chen>cd C:\Program Files (x86)\Nmap

C:\Program Files (x86)\Nmap>_
```

4. Type "ncat -C students.pennwest.edu 80" to connect to HTTP server on students.pennwest.edu and follow what demoed in the class:



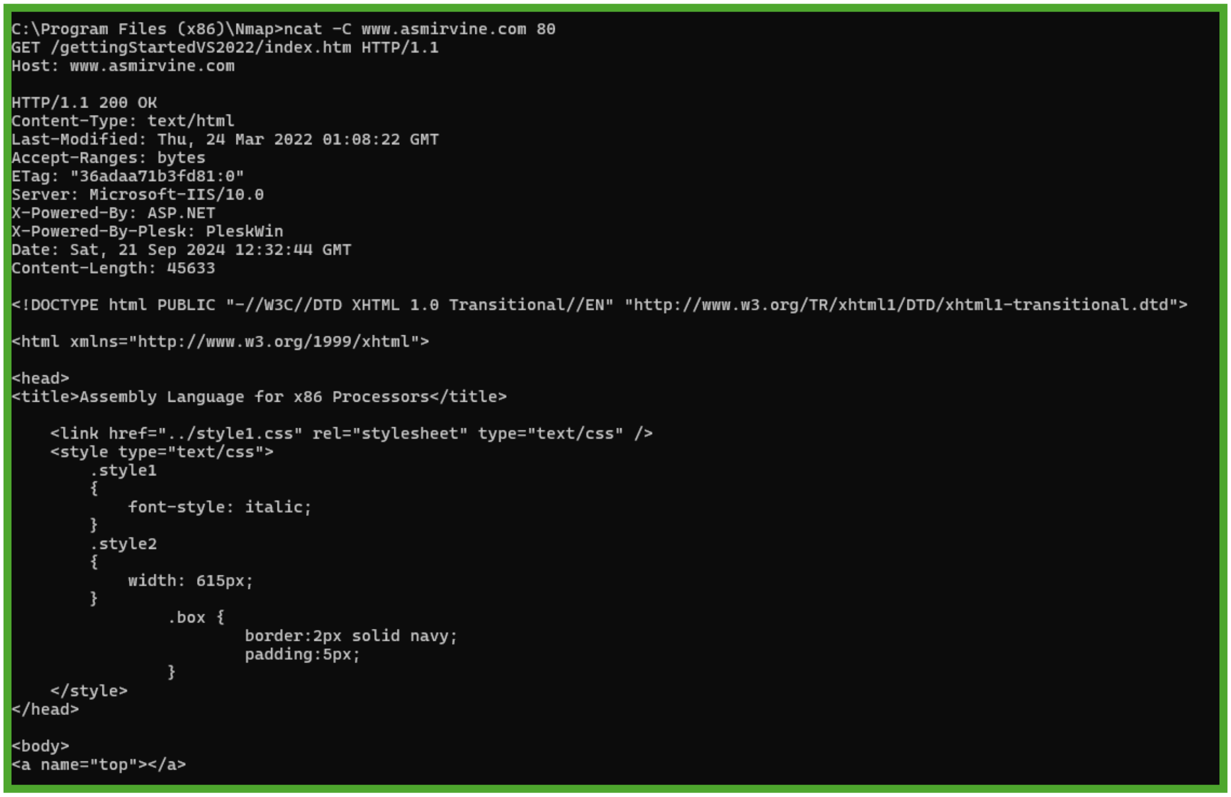
```
Microsoft Windows [Version 10.0.19045.4780]
(c) Microsoft Corporation. All rights reserved.

C:\Users\chen>cd C:\Program Files (x86)\Nmap

C:\Program Files (x86)\Nmap>ncat -C students.pennwest.edu 80
GET /chen/index.htm HTTP/1.1
Host: students.pennwest.edu

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Fri, 13 Sep 2024 02:44:06 GMT
Accept-Ranges: bytes
ETag: "3253fcd865db1:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Thu, 19 Sep 2024 15:53:55 GMT
Content-Length: 193

<!DOCTYPE html>
<html>
        <head>
                <title>Weifeng Chen</title>
        </head>
        <body>
                Welcome to Weifeng Chen's homepage. <br/>
                <img src="pennwestcal.png" width="200" />
        </body>
</html>_
```

Use ncat to connect 80

HTTP request

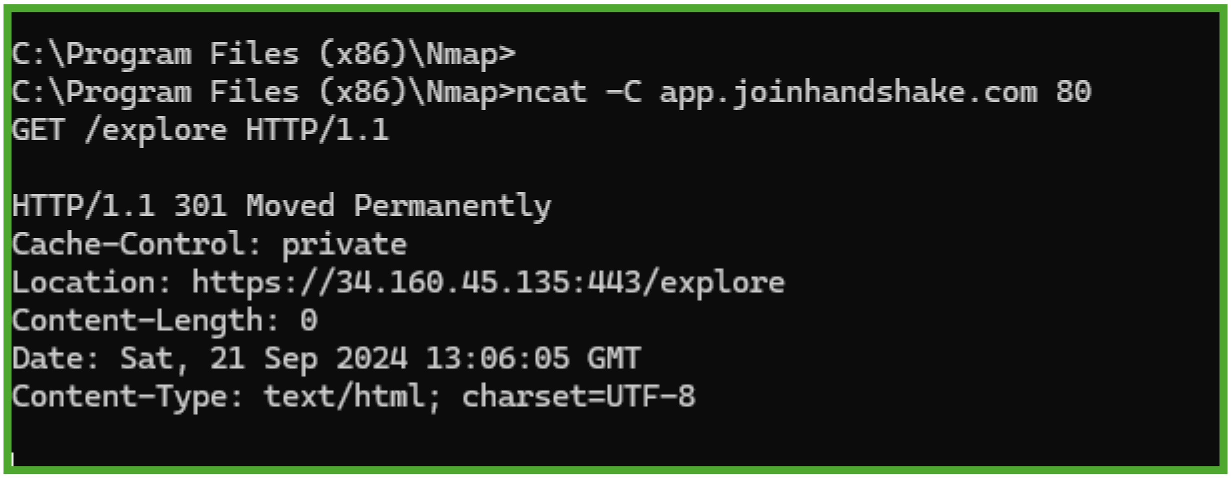
200 OK response from server

Question2: *Good Response- 200 OK*



```
C:\Program Files (x86)\Nmap>ncat -C www.asmirvine.com 80
GET /gettingStartedVS2022/index.htm HTTP/1.1
Host: www.asmirvine.com

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Thu, 24 Mar 2022 01:08:22 GMT
Accept-Ranges: bytes
ETag: "36adaa71b3fd81:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Powered-By-Plesk: PleskWin
Date: Sat, 21 Sep 2024 12:32:44 GMT
Content-Length: 45633

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>
<title>Assembly Language for x86 Processors</title>

    <link href="../style1.css" rel="stylesheet" type="text/css" />
    <style type="text/css">
        .style1
        {
            font-style: italic;
        }
        .style2
        {
            width: 615px;
        }
                .box {
                        border:2px solid navy;
                        padding:5px;
                }
    </style>
</head>

<body>
<a name="top"></a>
```

Question2: *Bad Response- 301*



```
C:\Program Files (x86)\Nmap>
C:\Program Files (x86)\Nmap>ncat -C app.joinhandshake.com 80
GET /explore HTTP/1.1

HTTP/1.1 301 Moved Permanently
Cache-Control: private
Location: https://34.160.45.135:443/explore
Content-Length: 0
Date: Sat, 21 Sep 2024 13:06:05 GMT
Content-Type: text/html; charset=UTF-8
```

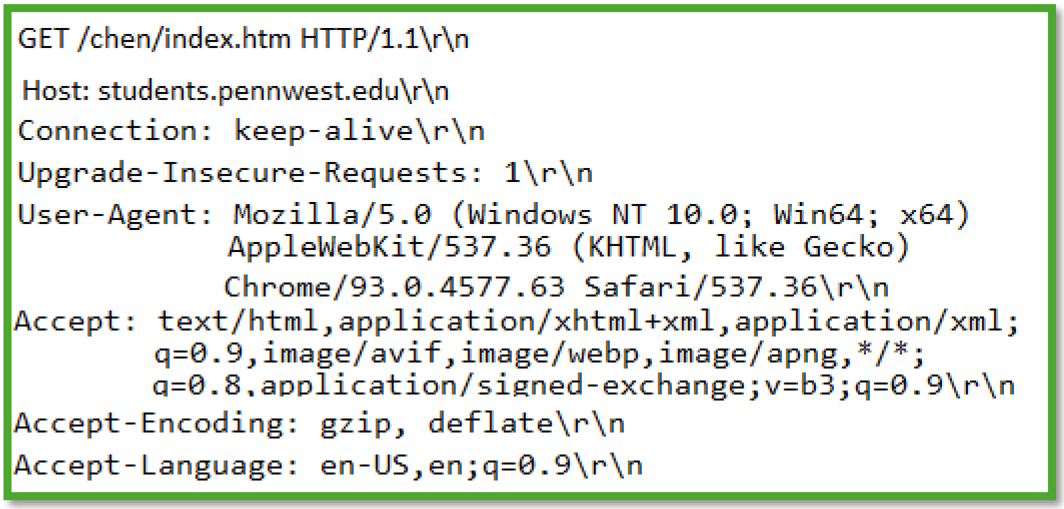
Question 3. (**10 points**) Consider the following string of ASCII characters that were captured by Wireshark when the browser sent an HTTP GET message (i.e., this is the actual content of an HTTP GET message). The characters *"\r\n"* are carriage return and line-feed characters. Answer the following questions, indicating where in this HTTP GET message you find the answer.

a. What is the URL of the document requested by the browser?

b. What version of HTTP is the browser running?

c. Does the browser request a non-persistent or a persistent connection?

d. Can you tell the IP address of the host on which the browser is running, based on this GET message?



```
GET /chen/index.htm HTTP/1.1\r\n
Host: students.pennwest.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
            AppleWebKit/537.36 (KHTML, like Gecko)
            Chrome/93.0.4577.63 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;
        q=0.9,image/avif,image/webp,image/apng,*/*;
        q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
```

Question 3 Answers:

a. /chen/index.html

b. HTTP version 1.1

c. Keep-alive = persistent

d. No, you cannot tell the IP address of this GET message since the domain (students.pennwest.edu) is used and not the IP address.