EECS 3482

Lab 1

Name : AKALPIT SHARMA

ID: 212650628

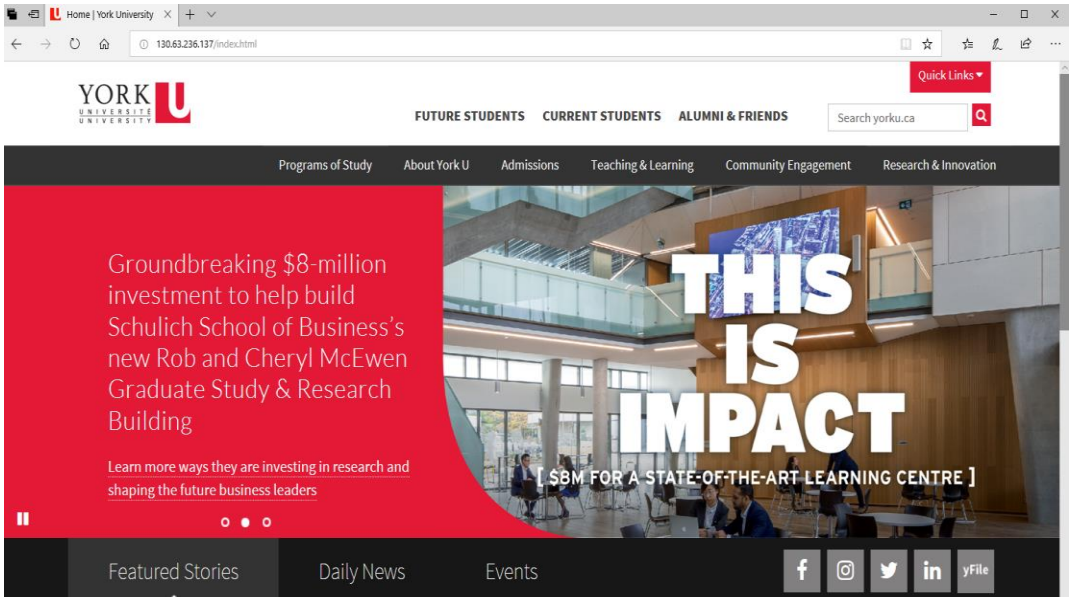
Part 1: Network and Server Discovery

1. Start a browser session.
1.1 Retrieve the resource: www.network-tools.com.

a. Select Express and specify the server as www.yorku.ca ➔ Click Go

i. What is the IP address of the server? 130.63.236.137

ii. Open a browser session and paste the IP address in the address bar of the browser, document the output using a screen snapshot.



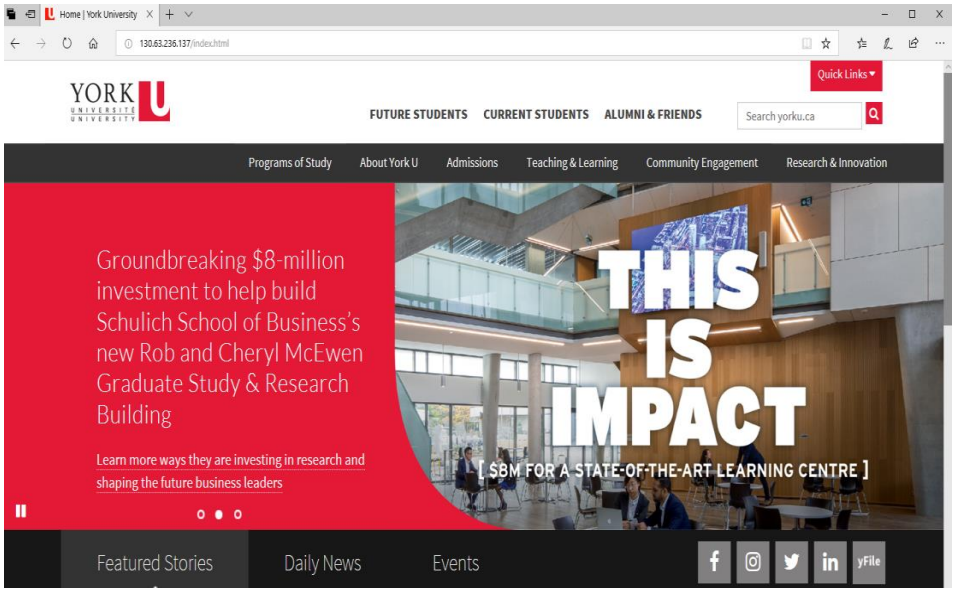
iii. What is the source of the server that performed resolution of whois utility?
whois.arin.net

iv. What is the network name?
YORKU

v. What is the Organization's name?
York University (YORKUN)

vi. From the Tools menu, select Nslookup and specify www.yorku.ca for the host name and select All for Query Type.

1. What type of records does the server has (A or AAAA)? A
2. What is the IP address of the server? 130.63.236.137
3. Attempt to browse the home page of the server using its IP address and document the output using a screen snapshot.



4. What is the 1st domain server's name?
optera.ccs.yorku.ca

5. What is the 2nd domain server's name?
www.yorku.ca

Records

optera.ccs.yorku.ca	A	130.63.236.137	0 s
www.yorku.ca	CNAME		0 s

vii. From the Tools menu, select Nslookup and specify www.iis.se for the host name and select All for Query Type.

1. What type of records does the server has?
for ipv4 its 'A' and for ipv6 'AAAA'

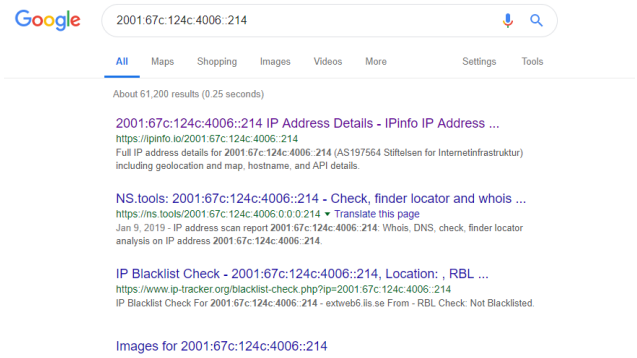
2. What is/are the IP address of the server?
ipv4 : 91.226.37.214
ipv6 : 2001:67c:124c:4006::214

www.iis.se	A	91.226.37.214	0 s
www.iis.se	AAAA	2001:67c:124c:4006::214	0 s

3. Attempt to browse the home page of the server using its IP addresses IPv4 and IPv6 and document the output using a screen snapshot.

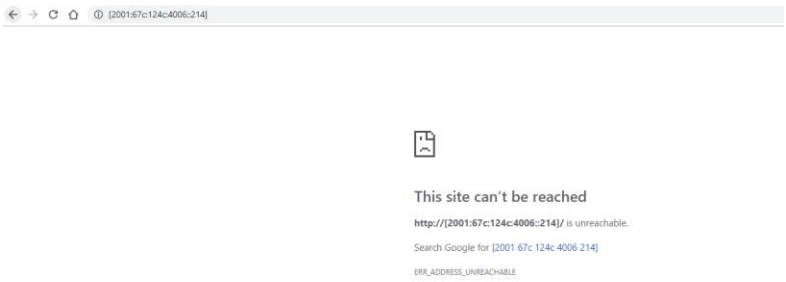
using ipv4

using ipv6



4. Reattempt to brows the home page using [IPv6], you should include the IPv6 in the brackets in the address bar of the browser.

nothing showed up due to security reason



5. What is the 1st domain server's name?
   www.iis.se

6. What is the 2nd domain server's name?
   www.iis.se

7. Test connectivity to the server using the Ping utility and IPv6.

Click the "Ping" button and then "Go."

Round trip time to www.iis.se: 0.55ms
Round trip time to www.iis.se: 0.31ms
Round trip time to www.iis.se: 0.31ms
Round trip time to www.iis.se: 0.3ms
Round trip time to www.iis.se: 0.29ms
Round trip time to www.iis.se: 0.3ms
Round trip time to www.iis.se: 0.3ms
Round trip time to www.iis.se: 0.29ms
Round trip time to www.iis.se: 0.29ms
Round trip time to www.iis.se: 0.3ms

Average time: 0.32ms.

☐ Convert Base-10 to IP

www.iis.se

ipv6 are not currently supported in NSLook up website

viii. Using the resource https://tools.keycdn.com/geo,

1. find the geographical location of the server www.yorku.ca by name and by IPv4
    a. What is the host name?
    b. What is AS number of the network?
    c. What are the city, country, content, and latitude/longitude coordinates values.

geographical location by name

IP address or hostname www.yorku.ca Lookup

IP	130.63.236.137	Hostname	emotionfocusedinstitute.com	ASN	802
Country	Canada (CA)	Provider	York University	Continent Code	NA
City	Toronto	Latitude	43.7694	Continent Name	North America
Region	Ontario (ON)	Longitude	-79.4921	TimeZone	America/Toronto
Postal Code	M3J	Metro Code		DateTime	2019-01-23 11:51:15

geographical location by ipv4

IP address or hostname 130.63.236.137 Lookup

IP	130.63.236.137	Hostname	problematiquejournal.com	ASN	802
Country	Canada (CA)	Provider	York University	Continent Code	NA
City	Toronto	Latitude	43.7694	Continent Name	North America
Region	Ontario (ON)	Longitude	-79.4921	TimeZone	America/Toronto
Postal Code	M3J	Metro Code		DateTime	2019-01-23 11:50:20

2. Find the geographical location of the server www.iis.se by the server name, IPv4, and IPv6.

    a. What is the host name?
    b. What is AS number of the network?
    c. What are the city, country, content, and latitude/longitude coordinates values?

by server name

IP address or hostname www.iis.se Lookup

IP	91.226.37.214	Hostname	extweb6.iis.se	ASN	197564
Country	Sweden (SE)	Provider	Stiftelsen for Internetinfrastruktur	Continent Code	EU
City	Stockholm	Latitude	59.3333	Continent Name	Europe
Region	Stockholm (AB)	Longitude	18.05	TimeZone	Europe/Stockholm
Postal Code	173 11	Metro Code		DateTime	2019-01-23 18:00:36

by ipv4

IP address or hostname 91.226.37.214 Lookup

IP	91.226.37.214	Hostname	extweb6.iis.se	ASN	197564
Country	Sweden (SE)	Provider	Stiftelsen for Internetinfrastruktur	Continent Code	EU
City	Stockholm	Latitude	59.3333	Continent Name	Europe
Region	Stockholm (AB)	Longitude	18.05	TimeZone	Europe/Stockholm
Postal Code	173 11	Metro Code		DateTime	2019-01-23 18:01:08

by ipv6

IP address or hostname 2001:67c:124c:4006::214 Lookup

IP	2001:67c:124c:4006::214	Hostname	extweb6.iis.se	ASN	197564
Country	Sweden (SE)	Provider	Stiftelsen for Internetinfrastruktur	Continent Code	EU
City		Latitude	62	Continent Name	Europe
Region		Longitude	15	TimeZone	Europe/Stockholm
Postal Code		Metro Code		DateTime	2019-01-23 18:01:53

due to security reason ipv6 hide the sensitive information

ix. Using the resource https://network-tools.com/, select HTTP Headers and specify the server name yorku.ca as the server name.

1. What is the HTTP protocol version running on the server? HTTP/1.1
2. What type of web server is running on the server? Apache/2.4.29
3. What type of operating system is running on the server? Ubuntu
4. Has the server reported any error messages? If so, search the code and attempt to interpret its meaning? Yes, 302 found : means it indicating that the requested resource has been temporarily moved to different URL

x. Using the resource https://network-tools.com/, select HTTP Headers and specify the server name www.iis.se as the server name.

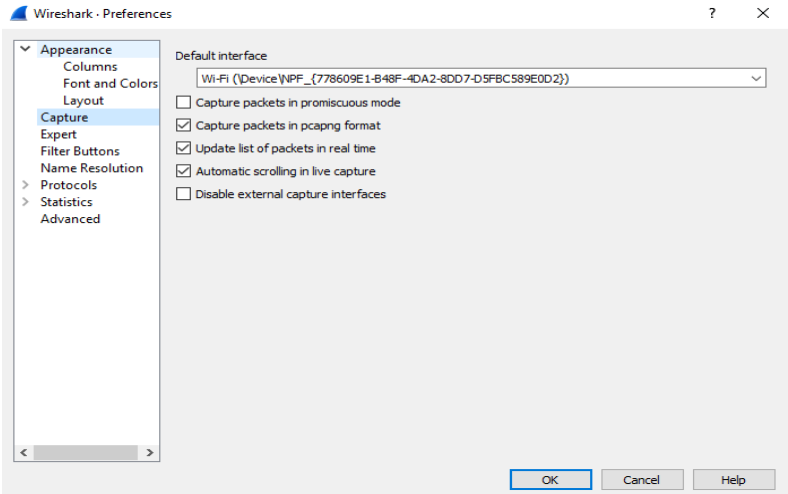
1. What is the HTTP protocol version running on the server? HTTP/1.1
2. What type of web server is running on the server? Apache/2.4.7
3. What type of operating system is running on the server? Ubuntu
4. Has the server reported any error messages? If so, search the code and attempt to interpret its meaning? Yes, 301 moved permanently: indicating that the requested resource has been moved permanently to a new URL provided by the location response header.
5. Re-attempt requesting the headers using https://www.iis.se instead of www.iis.se; has the server reported any messages; if so, what is the message code? status changed to OK

Part- 2 PACKET ANALYSIS

- What is promiscuous mode ?
  It is a network interface mode. It is for sniffing packets in LAN segment.

- Document your steps involved
  1) I first opened the wire shark.
  2) Then I clicked the Wi-Fi (since thats the one where I will be capturing data)

  3) then I follow what lab has mentioned to follow



  4) Then Wire Shark started capturing the data
  5) Then as mentioned in the lab I clicked on "Interfaces List" and capturing service was started for all physical interfaces on the computer.

Part 2: HTTP Deomonstration

1.8 From the hyper link extract the URI for the putty server:

link -> https://the.earth.li/~sgtatham/putty/latest/w64/puttytel.exe

Extracted URL: the.earth.li

1.9

```
C:\Users\Owner>ping the.earth.li

Pinging the.earth.li [2001:41c8:10:b1f:c0ff:ee:15:900d] with 32 bytes of data:
Reply from 2001:41c8:10:b1f:c0ff:ee:15:900d: time=97ms
Reply from 2001:41c8:10:b1f:c0ff:ee:15:900d: time=93ms
Reply from 2001:41c8:10:b1f:c0ff:ee:15:900d: time=98ms
Reply from 2001:41c8:10:b1f:c0ff:ee:15:900d: time=90ms

Ping statistics for 2001:41c8:10:b1f:c0ff:ee:15:900d:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 90ms, Maximum = 98ms, Average = 94ms
```

1.10 Identify the IP address of the pinged server: 46.43.34.31

1.11 Identify the port number of the server: 443

1.12

669	0.956238	10.24.240.205	46.43.34.31	TCP	54 59655 → https(443) [ACK] Seq=1692 Ack=570060 Win=809472 Len=0
670	2.976721	46.43.34.31	10.24.240.205	TLSv1.2	85 Encrypted Alert
671	2.977347	46.43.34.31	10.24.240.205	TCP	54 https(443) → 59655 [FIN, ACK] Seq=570091 Ack=1692 Win=32512 Len=0
672	2.977389	10.24.240.205	46.43.34.31	TCP	54 59655 → https(443) [ACK] Seq=1692 Ack=570092 Win=809472 Len=0
673	4.375805	10.24.240.205	130.63.10.18	DNS	77 Standard query 0xd3cd A sb-ssl.google.com
674	4.382844	130.63.10.18	10.24.240.205	DNS	364 Standard query response 0xd3cd A sb-ssl.google.com CNAME sb-ssl.l.google.com A 172.217.1.14 NS ns3.goog
675	4.383882	10.24.240.205	172.217.1.14	TCP	66 59658 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
676	4.388527	172.217.1.14	10.24.240.205	TCP	66 https(443) → 59658 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1363 SACK_PERM=1 WS=256
677	4.388622	10.24.240.205	172.217.1.14	TCP	54 59658 → https(443) [ACK] Seq=1 Ack=1 Win=66560 Len=0
678	4.389160	10.24.240.205	172.217.1.14	TLSv1.2	586 Client Hello
679	4.393535	172.217.1.14	10.24.240.205	TCP	54 https(443) → 59658 [ACK] Seq=1 Ack=533 Win=61952 Len=0

Part2: FTP Demonstration

1.20 From the hyperlink extract the URL for the putty server:
ftp://ftp.chiark.greenend.org.uk/users/sgtatham/putty-latest/w32/puttytel.exe

1.21

Command Prompt

```
C:\Users\Owner>ping ftp.chiark.greenend.org.uk

Pinging service-name.chiark.greenend.org.uk [212.13.197.229] with 32 bytes of data:
Reply from 212.13.197.229: bytes=32 time=119ms TTL=52
Reply from 212.13.197.229: bytes=32 time=99ms TTL=52
Reply from 212.13.197.229: bytes=32 time=99ms TTL=52
Reply from 212.13.197.229: bytes=32 time=105ms TTL=52

Ping statistics for 212.13.197.229:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 99ms, Maximum = 119ms, Average = 105ms

C:\Users\Owner>
```

1.22 Identify the assigned IP address of the pinged server:
212.13.197.229

1.23 Display the segment of frames for that particular IP using the wire shark captured data.

693	18.773871	212.13.197.229	10.24.240.205	FTP-DA…	1417	FTP Data: 1363 bytes (PASV) (TYPE I)
694	18.773874	212.13.197.229	10.24.240.205	FTP-DA…	472	FTP Data: 418 bytes (PASV) (TYPE I)
695	18.773945	10.24.240.205	212.13.197.229	TCP	54	59611 → 33753 [ACK] Seq=1 Ack=515634 Win=730368 Len=0
696	18.774119	10.24.240.205	212.13.197.229	TCP	54	59611 → 33753 [FIN, ACK] Seq=1 Ack=515634 Win=730368 Len=0
697	18.804907	10.24.240.205	209.87.209.212	TCP	54	59576 → 443 [ACK] Seq=1 Ack=11673 Win=258 Len=0
698	18.854802	212.13.197.229	10.24.240.205	FTP	78	Response: 226 Transfer complete.
699	18.855096	212.13.197.229	10.24.240.205	TCP	54	33753 → 59611 [ACK] Seq=515634 Ack=2 Win=29312 Len=0
700	18.855100	10.24.240.205	212.13.197.229	FTP	60	Request: QUIT
701	18.937454	212.13.197.229	10.24.240.205	FTP	105	Response: 221-You have transferred 515632 bytes in 1 files.
702	18.937693	212.13.197.229	10.24.240.205	FTP	205	Response: 221-Total traffic for this session was 517355 bytes in 1 transfers.
703	18.937769	10.24.240.205	212.13.197.229	TCP	54	59610 → 21 [ACK] Seq=228 Ack=1717 Win=66304 Len=0
704	18.937928	10.24.240.205	212.13.197.229	TCP	54	59610 → 21 [FIN, ACK] Seq=228 Ack=1717 Win=66304 Len=0
705	19.020150	212.13.197.229	10.24.240.205	TCP	54	21 → 59610 [ACK] Seq=1717 Ack=229 Win=29312 Len=0
706	19.486690	209.87.209.212	10.24.240.205	TLSv1.2	123	Application Data
707	19.528579	10.24.240.205	209.87.209.212	TCP	54	59576 → 443 [ACK] Seq=1 Ack=11742 Win=258 Len=0
708	19.532583	184.29.65.129	10.24.240.205	TLSv1.2	85	Encrypted Alert
709	19.532719	184.29.65.129	10.24.240.205	TCP	54	443 → 59569 [FIN, ACK] Seq=32 Ack=2 Win=314 Len=0
710	19.532760	10.24.240.205	184.29.65.129	TCP	54	59569 → 443 [ACK] Seq=2 Ack=33 Win=260 Len=0
711	19.629590	209.87.209.212	10.24.240.205	TLSv1.2	123	Application Data
712	19.673915	10.24.240.205	209.87.209.212	TCP	54	59576 → 443 [ACK] Seq=1 Ack=11811 Win=258 Len=0

1.24 Demonstrate the port number of the server.

Since we are dealing with ftp protocol and we know source port number is 21. destination port number is 54755

1.25 Identify the IP address of the server using wire shark

212.13.197.229