Architecture, Operating Systems & Networking Report CA3

TU259

<Yuanshuo Du>
<D22125495>

School of Computer Science
TU Dublin – City Campus

<20230507>

Table of Contents

Part 1 – Cisco Packet Tracer (10%): 4

Task 1: Create the Marketing subnet 4

Task 2: Create the Sales subnet 5

Task 3: Communication 7

Task 4: Web Server 8

Task 5: DHCP 10

Part 2 – Wireshark Packet Capture Analysis (10%): 13

Question 1: What is the IP address of the host machine? 13

Question 2: What is the Hostname of the host machine? 13

Question 3: What http sites did this machine visit? 14

Question 4: What UTC date/time did the host first visit code.mccarthywebsites.com? 15

Question 5: What files were downloaded? 16

Question 6: List the times/dates the http web pages were visited. 17

Question 7: Why is it not possible to view all the https traffic? 17

Question 8: Recover all content and pages visited by the host machine. 17

Question 9: What are the domain names and IP addresses of the sites visited? 19

Question 10: Why do two of the sites have the same IP address? 19

Declaration

I hereby declare that the work described in this report is, except where otherwise stated, entirely my own work and has not been submitted as an exercise for a degree at this or any other university.

Signed:

_____Yuanshuo Du_____

<Yuanshuo Du>

<20230507>

Architecture, Operating Systems and Networks

TU259 - Continuous Assessment 3 (20% of module total)

Due Date: Sunday 7th May 2023 @ 23:59

This document can be used as a template to offer the solution for Part 1 and Part 2.

Part 1 – Cisco Packet Tracer (10%):

Create two subnets for a marketing and Sales departments using CIDR notation.
In the project report briefly describe how you will setup your 2 subnets.

Requirements:
Add 3 PC's to each subnet. All PC's to get their IP address from a DHCP server.
Each subnet must contain a switch and a router.
Add a printer to each subnet.
All servers and printers get a static address.

The development of the network consists of the following tasks. Each task carries equal marks. The Cisco Packet Tracer video examples on Brightspace (week 12) will help with this part of the CA.

Task 1: Create the Marketing subnet
It should use 10.8.0.0
It must contain:

- 1 switch
- 1 router
- 3 PC's
- 1 Printer
- DHCP solution (preferably a server)

To create the Marketing subnet with 10.8.0.0 network address, we need to deploy a network infrastructure that includes a switch, a router, three PCs, a printer, and a DHCP server.

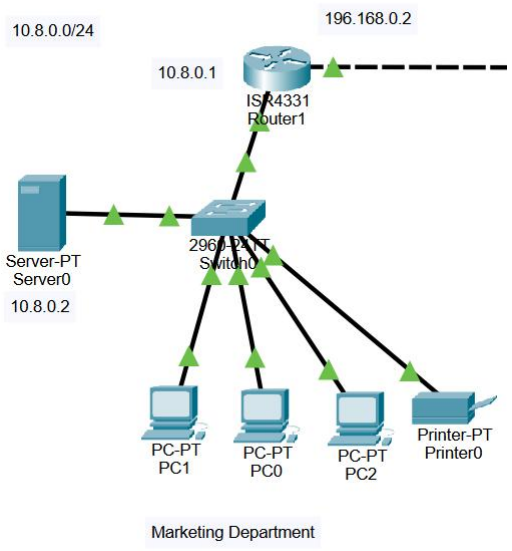
First, we need to connect the switch and router together. The switch will act as a central hub to which all devices will connect, and the router will act as a gateway to connect the subnet to other networks or the internet. We can use GigabitEthernet00 interface on the router to connect to the switch.

Next, we can connect the three PCs and the printer to the switch using FastEthernet interfaces. We should ensure that the IP addresses of each device are within the same subnet, i.e., 10.8.0.0/24.

To provide dynamic IP addresses to the devices in the subnet, we can deploy a DHCP server. This server can be a dedicated physical server or a virtual machine running a DHCP service. We need to connect the server to the switch using another FastEthernet interface.

Once all the devices are connected, we need to configure the router with a static route for any traffic that needs to be forwarded outside the subnet. We can use a default gateway as the next hop for traffic destined for networks other than the local subnet.

It is important to ensure that all devices in the Marketing subnet have their network settings correctly configured, including the IP address, subnet mask, default gateway,



Task 2: Create the Sales subnet
It should use 10.16.0.0
It must contain:

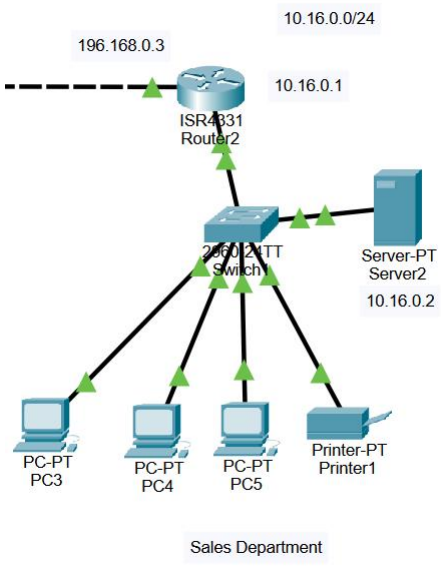
- 1 switch
- 1 router
- 3 PC's
- 1 Printer
- DHCP solution (preferably a server)

To create the Sales subnet, we need to follow the same steps as we did for the Marketing subnet. First, we need to deploy a switch and a router, connect the router to the switch, and then connect the switch to three PCs and a printer. We also need to set up a DHCP server by deploying a server and connecting it to the switch.

Similar to the Marketing subnet, the PCs and printer in the Sales subnet will also be connected to the switch's FastEthernet ports, while the switch will be connected to the router's GigabitEthernet00 port. The Sales subnet will be assigned the IP address range 10.16.0.0.

It is important to note that the two subnets are separate and should not be able to communicate with each other without explicit configuration. To achieve this, we can use

static routes on the routers to specify the route to the other subnet. For example, the Marketing subnet router can be configured with a static route to the Sales subnet

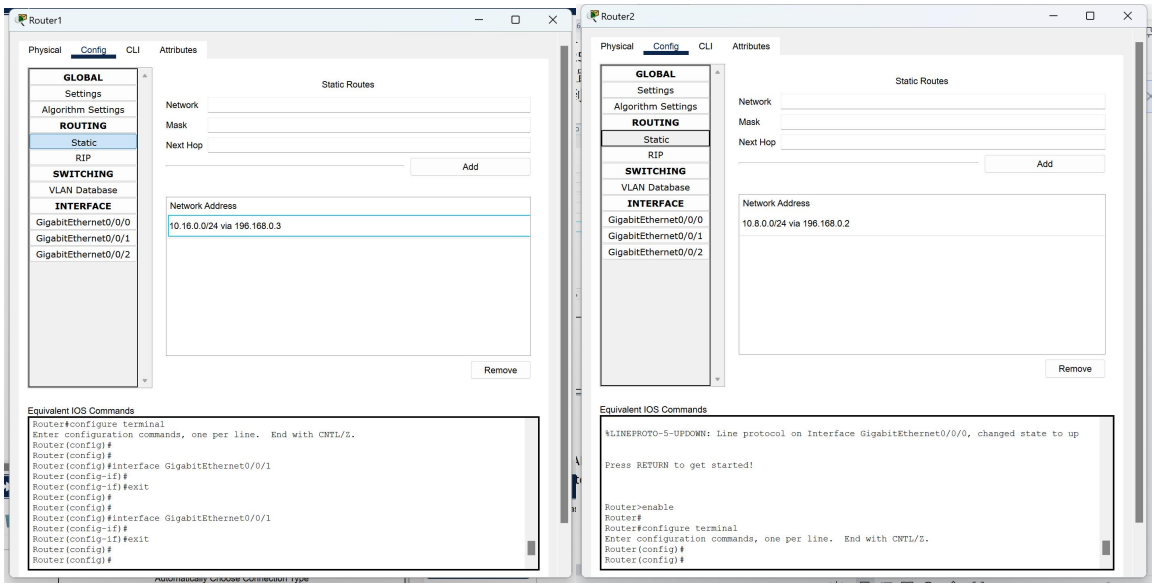


Task 3: Communication
It must be possible to communicate between the two subnets (ie: send and receive packets)

To connect the two subnets, we need to use another network segment to connect the two routers of the subnets. Here, I used 196.168.0.2 as the output port of the router for the marketing department and 196.168.0.3 as the output port of the router for the sales department. That is, the GigabitEthernet01 port of Router1 has an IP address of 196.168.0.2 with a subnet mask of 255.255.255.0. The GigabitEthernet01 port of Router2 has an IP address of 196.168.0.3 with a subnet mask of 255.255.255.0.

In addition, we need to configure the static routes of Router1 and Router2. For Router1, we should configure the static route for Network: 10.16.0.0, Mask: 255.255.255.0, and next hop: 196.168.0.3. For Router2, we should configure the static route for Network: 10.8.0.0, Mask: 255.255.255.0, and next hop: 196.168.0.2. These configurations need to be added to the network address.

By configuring these settings, communication between the two subnets should be possible, and packets can be sent and received. For example, a PC in the marketing subnet can communicate with a PC in the sales subnet by sending packets to the default gateway of its own subnet (the IP address of its own router). The router will then forward the packets to the other subnet based on the static routing configuration.



Test communication between two subnets：

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:96FF:FE15:48AE
   IPv6 Address.....: ::
   IPv4 Address.....: 10.8.0.10
   Subnet Mask.....: 255.0.0.0
   Default Gateway.....: ::
                                 10.8.0.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 10.16.0.10

Pinging 10.16.0.10 with 32 bytes of data:

Reply from 10.16.0.10: bytes=32 time<1ms TTL=126
Reply from 10.16.0.10: bytes=32 time<1ms TTL=126
Reply from 10.16.0.10: bytes=32 time<1ms TTL=126
Reply from 10.16.0.10: bytes=32 time<1ms TTL=126

Ping statistics for 10.16.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

the communication between the Marketing and Sales subnets has been successfully established. The ping command is being used to test the connectivity between two devices, one from the Marketing subnet with an IP address of 10.8.0.10 and another from the Sales subnet with an IP address of 10.16.0.10. The ping command is successful in both directions means that packets are being sent and received between the two subnets.

Task 4: Web Server

A web server should be added to the LAN. It should contain pages for the marketing and sales departments. It must be possible to view the web server content from both subnets.

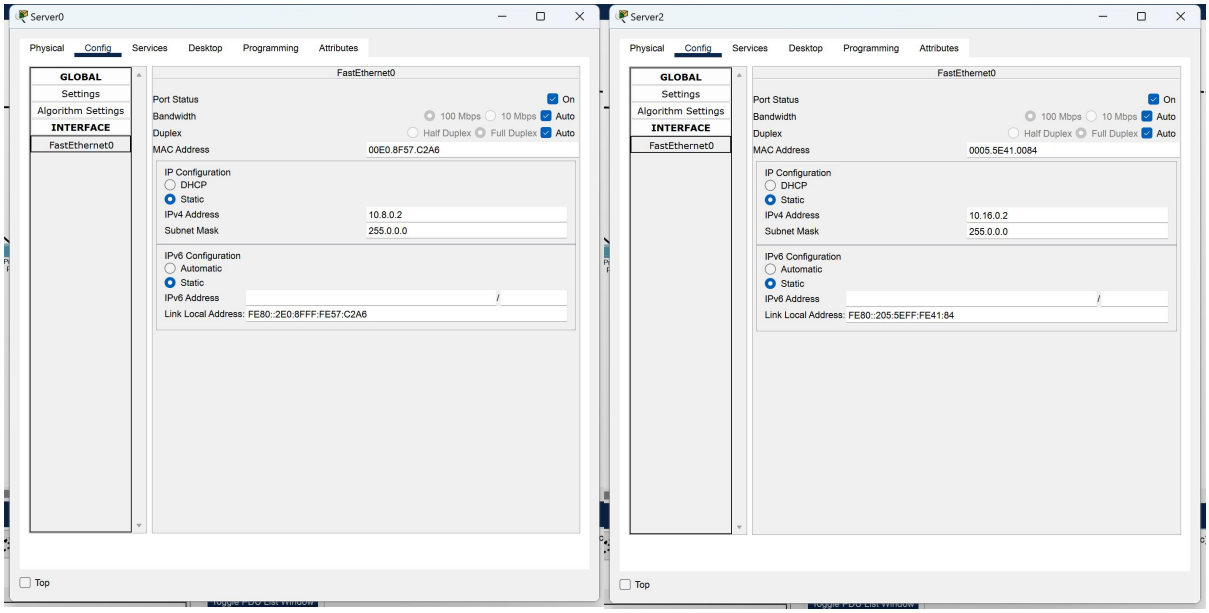
Answer:

In this task, we are adding a web server to the LAN that will contain pages for the marketing and sales departments. The main requirement for this task is that it must be possible to view the web server content from both subnets.

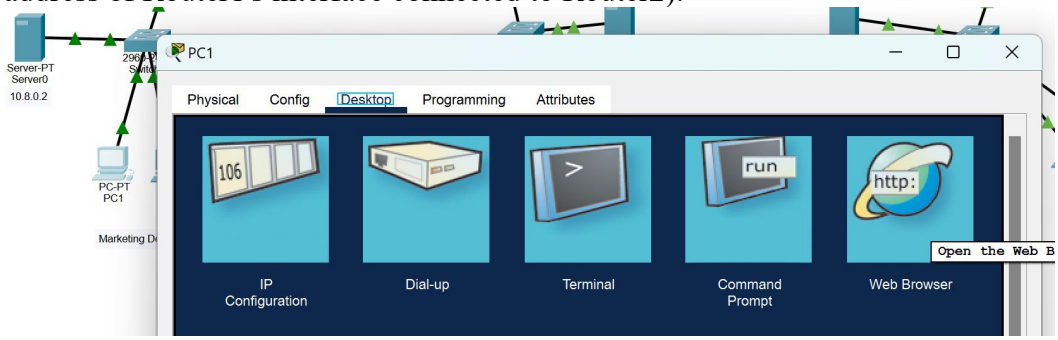
To accomplish this task, we need to add two web servers, one for the marketing department and the other for the sales department. The web servers should be configured with the appropriate pages for each department.

For the marketing department web server, we will use Server0. We will set its default gateway to 10.8.0.1 and configure the FastEthernet0 interface with a static IPv4 address of 10.8.0.2 and subnet mask of 255.0.0.0.

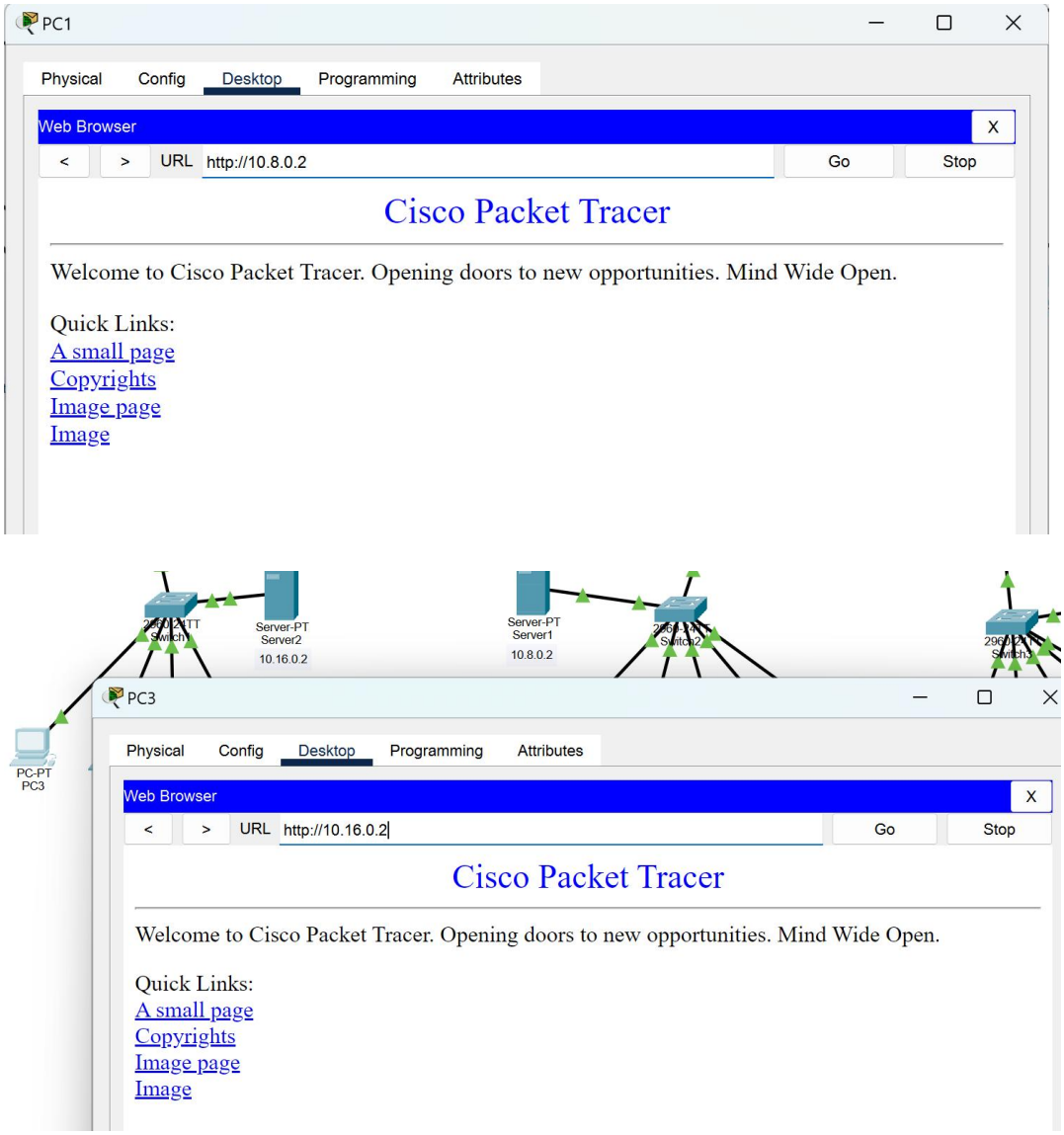
For the sales department web server, we will use Server2. We will set its default gateway to 10.16.0.1 and configure the FastEthernet0 interface with a static IPv4 address of 10.16.0.2 and subnet mask of 255.0.0.0.



To ensure that both subnets can access the web servers, we need to configure the routing on the routers. We can add a static route on Router1 for the 10.16.0.0/24 subnet with a next hop of 196.168.0.3 (the IP address of Router2's interface connected to Router1). Similarly, we can add a static route on Router2 for the 10.8.0.0/24 subnet with a next hop of 196.168.0.2 (the IP address of Router1's interface connected to Router2).



Once the web servers and routing are configured, we can test by accessing the web server content from each subnet. For example, from a PC on the marketing department subnet (subnet1), we can open a web browser and enter the IP address of the marketing department web server (10.8.0.2) to access its content. Similarly, from a PC on the sales department subnet (subnet2), we can open a web browser and enter the IP address of the sales department web server (10.16.0.2) to access its content.



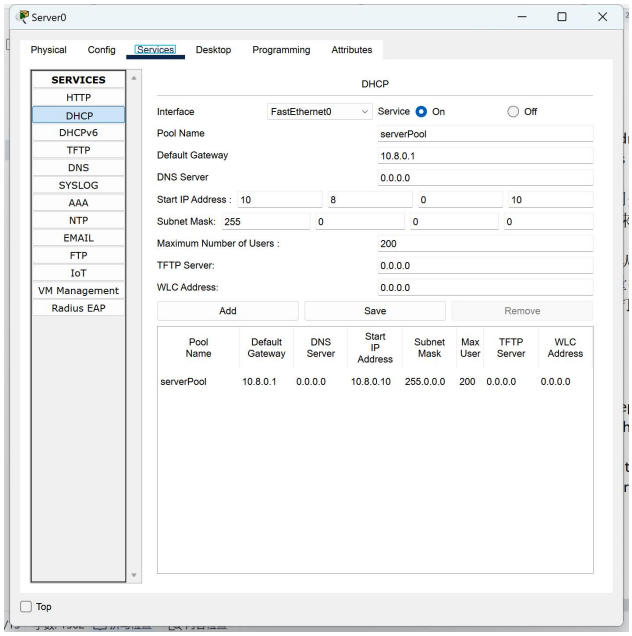
Task 5: DHCP

A DHCP solution should be put in place to offer IP address leases to the PC's in both domains. The IP addresses allocated must follow the IP address ranges specified above.

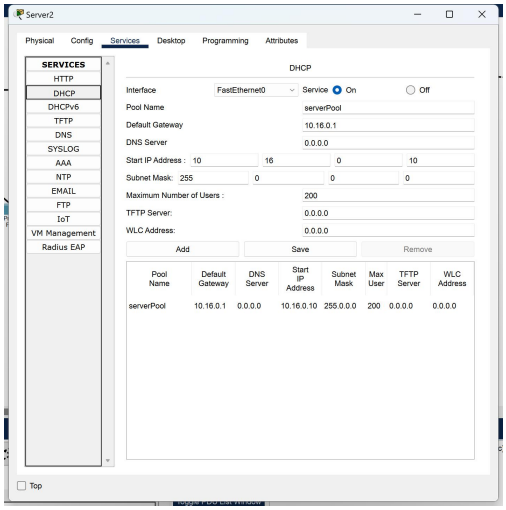
Answer:

Task 5 requires setting up a DHCP solution to offer IP address leases to the PCs in both departments. DHCP (Dynamic Host Configuration Protocol) is a network protocol used to automatically assign IP addresses to devices on a network. With DHCP, network administrators can manage IP addresses and provide network settings to devices in a centralized manner. DHCP allows devices to obtain IP addresses automatically without manual configuration, which reduces the workload of network administrators.

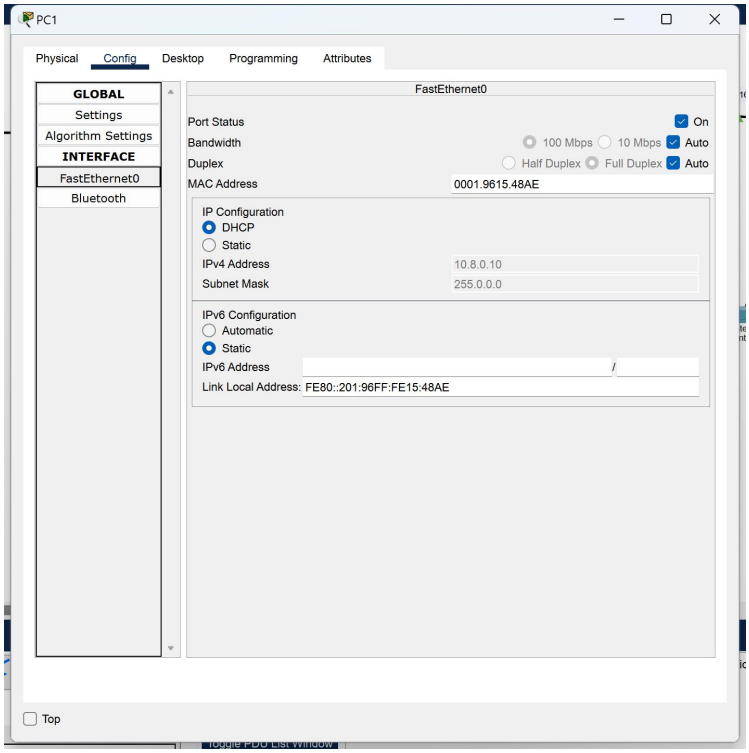
To set up DHCP on the server for the market department, we need to configure the DHCP panel. The default gateway should be set to 10.8.0.1, and the initial IP address should be set to 10.8.0.10 with a subnet mask of 255.0.0.0. We can set the maximum number of users according to the situation. Here we set it to 200 like the example in the video provided by the lecturer. Turn on the DHCP function of the server to make the Service in the On state, and click Save to add it to the pool.



Similarly, for the sales department, we need to configure the DHCP panel by setting the default gateway to 10.16.0.1, the starting IP address to 10.16.0.10, and the subnet mask to 255.0.0.0. The maximum number of users should be set to 200. We also need to enable DHCP on the server and add it to the pool.



After configuring the DHCP settings on the server, we need to enable the DHCP feature on each PC and printer. Each device will automatically obtain an IP address from the server's pool based on the DHCP configuration. This eliminates the need for manually configuring IP addresses on each device, which can be a tedious and time-consuming task.


PC1
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.9615.48AE
IP Configuration
DHCP
Static
IPv4 Address
10.8.0.10
Subnet Mask
255.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::201:96FF:FE15:48AE
Top

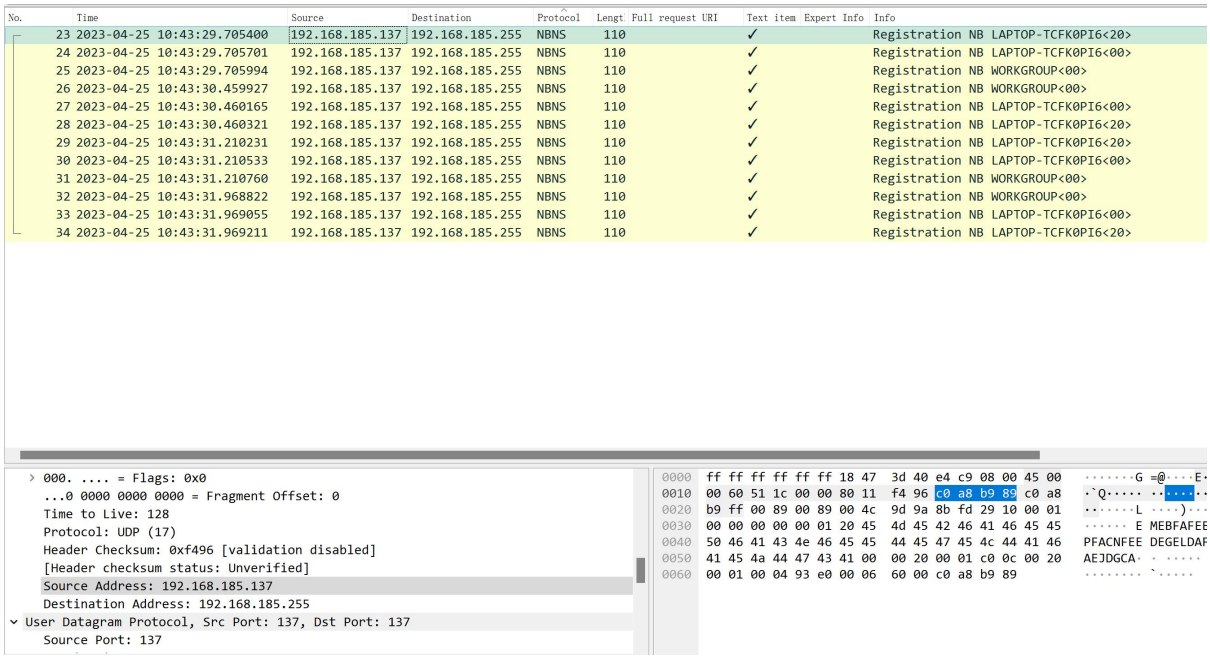
Part 2 – Wireshark Packet Capture Analysis (10%):

Requirements:
You are required to **create complete the following questions in examining the network packet capture** provided on Brightspace(CA4_Packet_Capture). Any techniques/methods used should describe their purpose and their use in the examination. In your answer describe how the different network parameters can be used with Wireshark to help trace network traffic to identify the answers to the questions below.

A screen shot and a description of how each question was answered should be provided in the answer offered. Each question carries equal marks.

Question 1: What is the IP address of the host machine?

Answer:
The host machine's IP can be found from the source address. From the picture, source Address is: 192.168.185.137



No.	Time	Source	Destination	Protocol	Lengt	Full request URI	Text item	Expert Info	Info
23	2023-04-25 10:43:29.705400	192.168.185.137	192.168.185.255	NBNS	110		✓		Registration NB LAPTOP-TCFK0PI6<20>
24	2023-04-25 10:43:29.705701	192.168.185.137	192.168.185.255	NBNS	110		✓		Registration NB LAPTOP-TCFK0PI6<00>
25	2023-04-25 10:43:29.705994	192.168.185.137	192.168.185.255	NBNS	110		✓		Registration NB WORKGROUP<00>
26	2023-04-25 10:43:30.459927	192.168.185.137	192.168.185.255	NBNS	110		✓		Registration NB WORKGROUP<00>
27	2023-04-25 10:43:30.460165	192.168.185.137	192.168.185.255	NBNS	110		✓		Registration NB LAPTOP-TCFK0PI6<00>
28	2023-04-25 10:43:30.460321	192.168.185.137	192.168.185.255	NBNS	110		✓		Registration NB LAPTOP-TCFK0PI6<20>
29	2023-04-25 10:43:31.210231	192.168.185.137	192.168.185.255	NBNS	110		✓		Registration NB LAPTOP-TCFK0PI6<20>
30	2023-04-25 10:43:31.210533	192.168.185.137	192.168.185.255	NBNS	110		✓		Registration NB LAPTOP-TCFK0PI6<00>
31	2023-04-25 10:43:31.210760	192.168.185.137	192.168.185.255	NBNS	110		✓		Registration NB WORKGROUP<00>
32	2023-04-25 10:43:31.968822	192.168.185.137	192.168.185.255	NBNS	110		✓		Registration NB WORKGROUP<00>
33	2023-04-25 10:43:31.969055	192.168.185.137	192.168.185.255	NBNS	110		✓		Registration NB LAPTOP-TCFK0PI6<00>
34	2023-04-25 10:43:31.969211	192.168.185.137	192.168.185.255	NBNS	110		✓		Registration NB LAPTOP-TCFK0PI6<20>

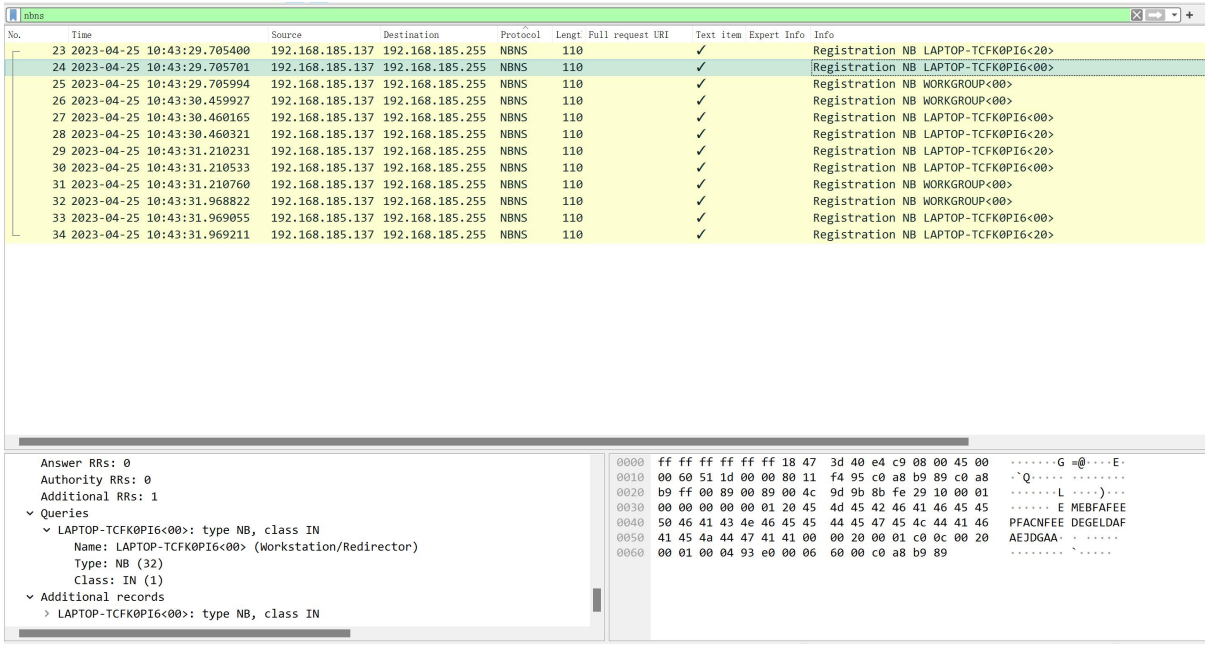
```
> 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0xf496 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.185.137
  Destination Address: 192.168.185.255
v User Datagram Protocol, Src Port: 137, Dst Port: 137
  Source Port: 137
```

```
0000  ff ff ff ff ff ff 18 47  3d 40 e4 c9 08 00 45 00   .......G =@....E.
0010  00 60 51 1c 00 00 80 11  f4 96 c0 a8 b9 89 c0 a8   .`Q..... ........
0020  b9 ff 00 89 00 89 00 4c  9d 9a 8b fd 29 10 00 01   .......L ....)...
0030  00 00 00 00 00 01 20 45  4d 45 42 46 41 46 45 45   ...... E MEBFAFEE
0040  50 46 41 43 4e 46 45 45  44 45 47 45 4c 44 41 46   PFACNFEE DEGELDAF
0050  41 45 4a 44 47 43 41 00  00 20 00 01 c0 0c 00 20   AEJDGCA. . ......
0060  00 01 00 04 93 e0 00 06  60 00 c0 a8 b9 89         ........ `.....
```

Question 2: What is the Hostname of the host machine?

Answer:

To filter the package, we need to fill "nbns"in the filter. Using the filter, the protocol analyzer tool was able to identify the hostname of the host machine as "LAPTOP-TCFK0PI6". The additional information provided in parentheses indicates that the host machine is a workstation/redirector:
Name: LAPTOP-TCFK0PI6 (Workstation/Redirector)



Question 3: What http sites did this machine visit?

In the given packet capture, we can see http.request made by the host machine. The HTTP requests are visible in the protocol column as "Full request URL". By expanding the HTTP request section, we can see the actual website or URL that the host machine is trying to access. In this case, we can see that the host machine has visited the following HTTP sites:

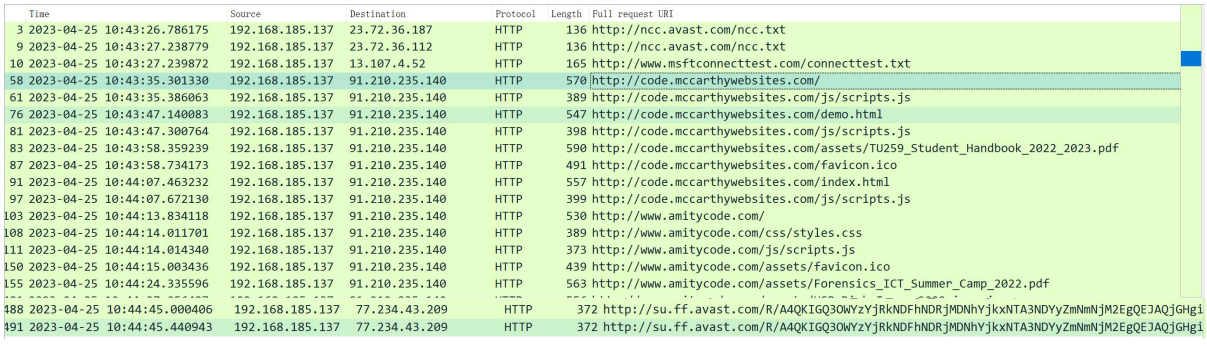
http://ncc.avast.com/

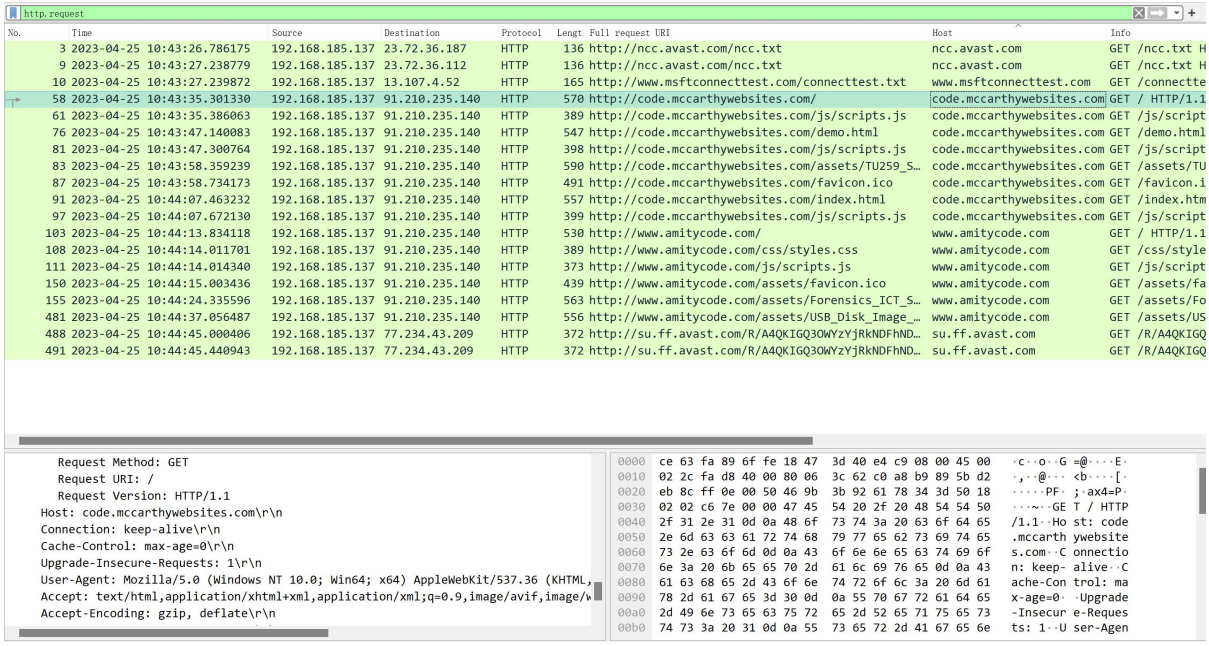
http://www.msftconnecttest.com/

http://code.mccarthywebsites.com/

http://www.amitycode.com/

http://su.ff.avast.com/



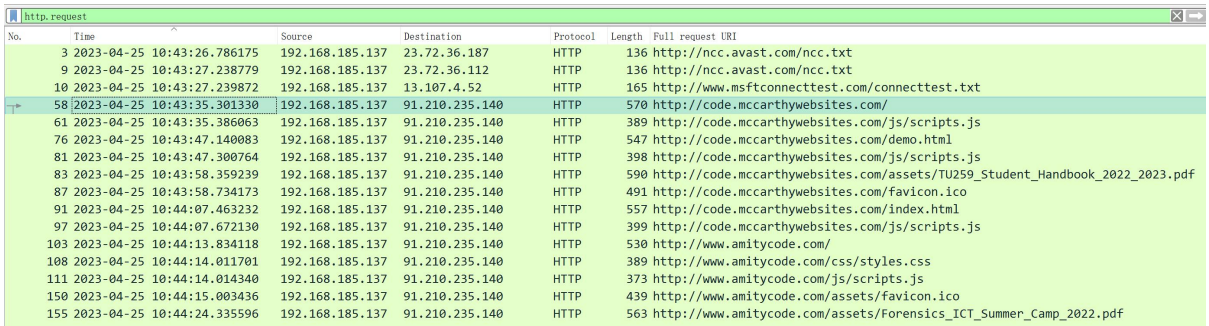


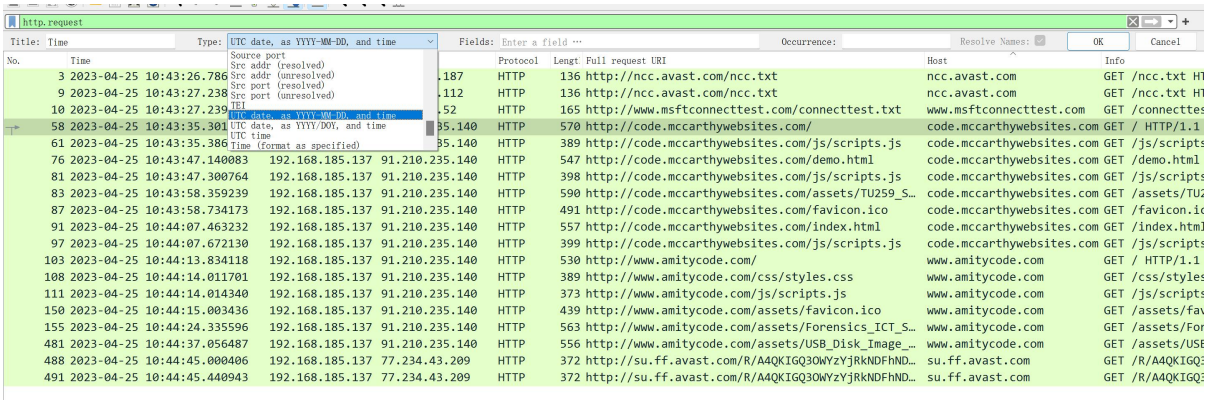
Question 4: What UTC date/time did the host first visit code.mccarthywebsites.com?

In order to answer this question, we need to analyze the packet capture and look for HTTP requests to code.mccarthywebsites.com. By examining the packets, we can determine the timestamp of the first HTTP request to this domain.

To do this, we can use Wireshark's filter “http.request” out all the packets related to this domain and examine them in chronological order. We can then look for the earliest HTTP request made to the domain.

Once we have located the first HTTP request to code.mccarthywebsites.com, we can examine the timestamp of the packet to determine the date and time the host first visited the website. We change the format of time to the format of year-month-date hours:minites:seconds. In this case, the timestamp shows that the host first visited code.mccarthywebsites.com on 2023-04-25 at 10:43:35.301330 UTC.





Question 5: What files were downloaded?

File-->Export Objects-->HTTP

The files were downloaded shows below:

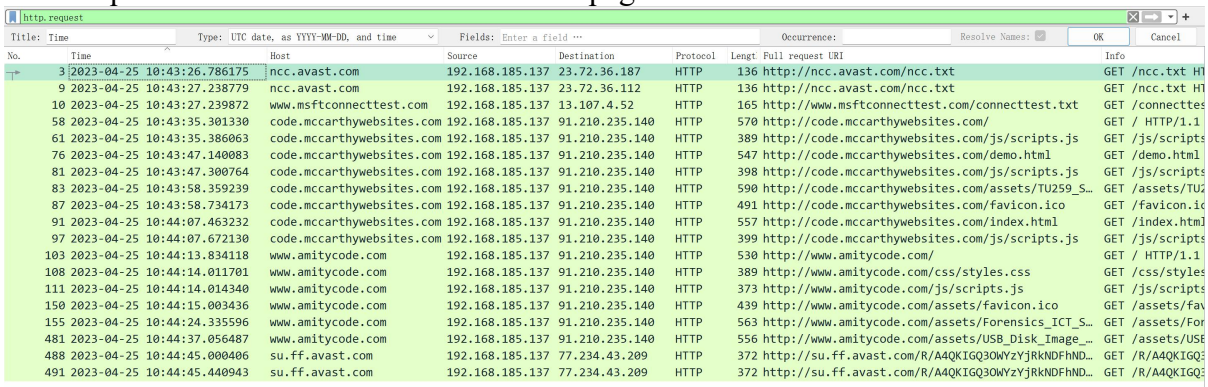
A4QKIGQ3OWYzYjRkNDFhNDRjMDNhYjkxNTA3NDYyZmNmNjM2EgQEJAQjGHgi
Af4qCAgEEOqZoKoBKggIAxD64qKmASoICAIQ_ObbqQEyCwgEEOqZoKoBGIAKOJyv
sLABQiDsxeo2hHJ_1MbxcHywStPHV-wDodWrC98WjgeObxD0vkiAgyg="
connecttest.txt"
demo.html"
favicon(1).ico"
favicon.ico"
index.html"
ncc(1).txt"
ncc.txt"
scripts(1).js"
scripts(2).js"
scripts(3).js"
scripts.js"
styles.css"
TU259_Student_Handbook_2022_2023.pdf"
%5c"
A4QKIGQ3OWYzYjRkNDFhNDRjMDNhYjkxNTA3NDYyZmNmNjM2EgQEJAQjGHgi
Af4qCAgEEJaXoKoBKggIAxD64qKmASoICAIQ_ObbqQEyCwgEEJaXoKoBGIAKOJyvs
LABQiDsxeo2hHJ_1MbxcHywStPHV-wDodWrC98WjgeObxD0vkiAgyg="

Wireshark · Export · HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
4	ncc.avast.com	text/html	26 bytes	ncc.txt
11	ncc.avast.com	text/html	26 bytes	ncc.txt
12	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt
65	code.mccarthywebsites.com	text/html	1238 bytes	scripts.js
80	code.mccarthywebsites.com	text/html	30 kB	demo.html
82	code.mccarthywebsites.com	text/html	1238 bytes	scripts.js
84	code.mccarthywebsites.com	text/html	1238 bytes	TU259_Student_Handbook_2022_2023.pdf
88	code.mccarthywebsites.com	text/html	1238 bytes	favicon.ico
96	code.mccarthywebsites.com	text/html	30 kB	index.html
98	code.mccarthywebsites.com	text/html	1238 bytes	scripts.js
105	www.amitycode.com	text/html	6110 bytes	\
137	www.amitycode.com	text/html	1238 bytes	scripts.js
145	www.amitycode.com	text/css	206 kB	styles.css
154	www.amitycode.com	image/x-icon	23 kB	favicon.ico
490	su.ff.avast.com	application/octet-stream	2213 bytes	A4QKIGQ3OWYzYjRkNDFhNDRjMDNhYjkxNTA3N
492	su.ff.avast.com	text/html	219 bytes	A4QKIGQ3OWYzYjRkNDFhNDRjMDNhYjkxNTA3N

Question 6: List the times/dates the http web pages were visited.
We change the format of time to the format of year-month-date hours:minites:seconds. And "Full request URL" column contains the web pages were visited as follow:



http.request

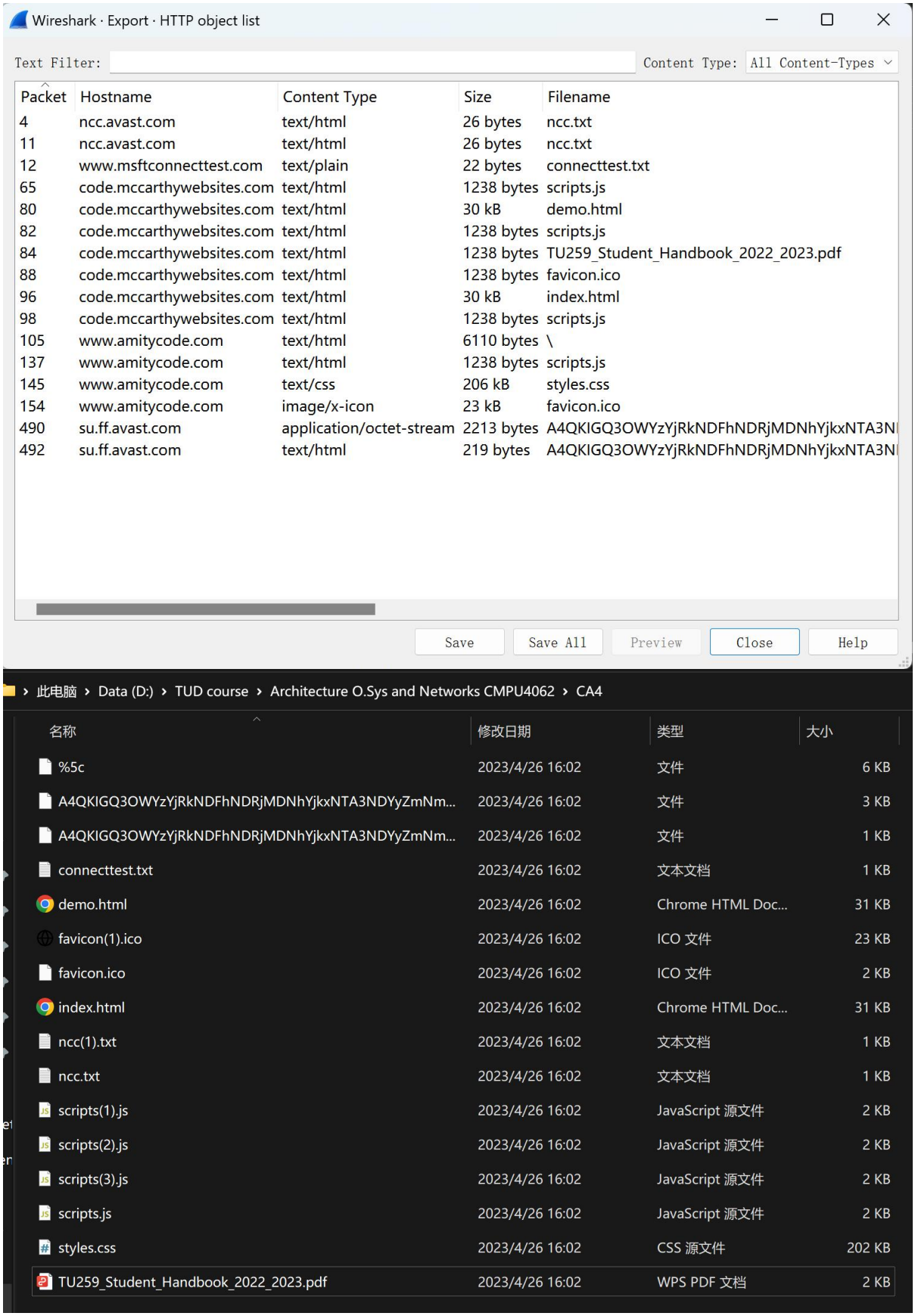
Title: Time Type: UTC date, as YYYY-MM-DD, and time Fields: Enter a field ··· Occurrence: Resolve Names: OK Cancel

No.	Time	Host	Source	Destination	Protocol	Lengt	Full request URI	Info
3	2023-04-25 10:43:26.786175	ncc.avast.com	192.168.185.137	23.72.36.187	HTTP	136	http://ncc.avast.com/ncc.txt	GET /ncc.txt HT
9	2023-04-25 10:43:27.238779	ncc.avast.com	192.168.185.137	23.72.36.112	HTTP	136	http://ncc.avast.com/ncc.txt	GET /ncc.txt HT
10	2023-04-25 10:43:27.239872	www.msftconnecttest.com	192.168.185.137	13.107.4.52	HTTP	165	http://www.msftconnecttest.com/connecttest.txt	GET /connecttes
58	2023-04-25 10:43:35.301330	code.mccarthywebsites.com	192.168.185.137	91.210.235.140	HTTP	570	http://code.mccarthywebsites.com/	GET / HTTP/1.1
61	2023-04-25 10:43:35.386063	code.mccarthywebsites.com	192.168.185.137	91.210.235.140	HTTP	389	http://code.mccarthywebsites.com/js/scripts.js	GET /js/scripts
76	2023-04-25 10:43:47.140083	code.mccarthywebsites.com	192.168.185.137	91.210.235.140	HTTP	547	http://code.mccarthywebsites.com/demo.html	GET /demo.html
81	2023-04-25 10:43:47.300764	code.mccarthywebsites.com	192.168.185.137	91.210.235.140	HTTP	398	http://code.mccarthywebsites.com/js/scripts.js	GET /js/scripts
83	2023-04-25 10:43:58.359239	code.mccarthywebsites.com	192.168.185.137	91.210.235.140	HTTP	590	http://code.mccarthywebsites.com/assets/TU259_S…	GET /assets/TU2
87	2023-04-25 10:43:58.734173	code.mccarthywebsites.com	192.168.185.137	91.210.235.140	HTTP	491	http://code.mccarthywebsites.com/favicon.ico	GET /favicon.ic
91	2023-04-25 10:44:07.463232	code.mccarthywebsites.com	192.168.185.137	91.210.235.140	HTTP	557	http://code.mccarthywebsites.com/index.html	GET /index.html
97	2023-04-25 10:44:07.672130	code.mccarthywebsites.com	192.168.185.137	91.210.235.140	HTTP	399	http://code.mccarthywebsites.com/js/scripts.js	GET /js/scripts
103	2023-04-25 10:44:13.834118	www.amitycode.com	192.168.185.137	91.210.235.140	HTTP	530	http://www.amitycode.com/	GET / HTTP/1.1
108	2023-04-25 10:44:14.011701	www.amitycode.com	192.168.185.137	91.210.235.140	HTTP	389	http://www.amitycode.com/css/styles.css	GET /css/styles
111	2023-04-25 10:44:14.014340	www.amitycode.com	192.168.185.137	91.210.235.140	HTTP	373	http://www.amitycode.com/js/scripts.js	GET /js/scripts
150	2023-04-25 10:44:15.003436	www.amitycode.com	192.168.185.137	91.210.235.140	HTTP	439	http://www.amitycode.com/assets/favicon.ico	GET /assets/fav
155	2023-04-25 10:44:24.335596	www.amitycode.com	192.168.185.137	91.210.235.140	HTTP	563	http://www.amitycode.com/assets/Forensics_ICT_S…	GET /assets/For
481	2023-04-25 10:44:37.056487	www.amitycode.com	192.168.185.137	91.210.235.140	HTTP	556	http://www.amitycode.com/assets/USB_Disk_Image_…	GET /assets/USB
488	2023-04-25 10:44:45.000406	su.ff.avast.com	192.168.185.137	77.234.43.209	HTTP	372	http://su.ff.avast.com/R/A4QKIGQ3OWYzYjRkNDFhND…	GET /R/A4QKIGQ3
491	2023-04-25 10:44:45.440943	su.ff.avast.com	192.168.185.137	77.234.43.209	HTTP	372	http://su.ff.avast.com/R/A4QKIGQ3OWYzYjRkNDFhND…	GET /R/A4QKIGQ3

Question 7: Why is it not possible to view all the https traffic?

It is not possible to view all HTTPS traffic because HTTPS traffic is encrypted and cannot be read by anyone except the intended recipient. However, there are some tools that can be used to decrypt HTTPS traffic such as Wireshark and Fiddler.

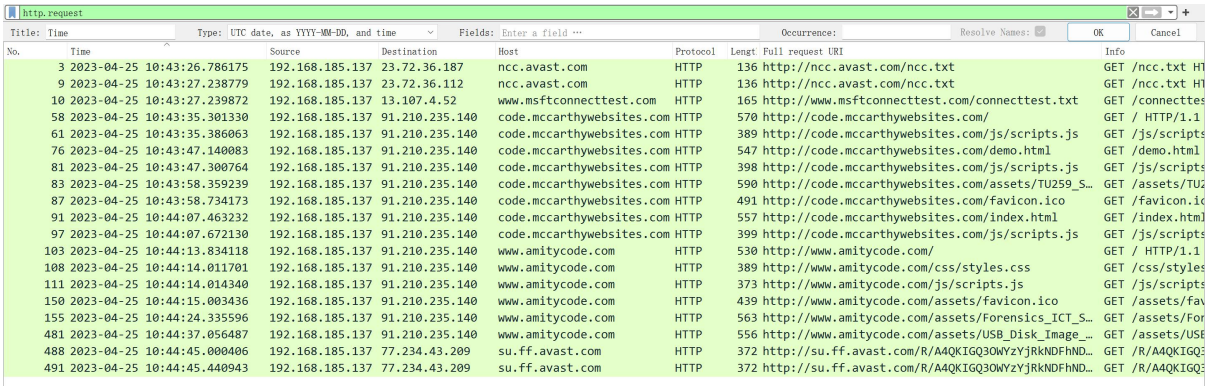
Question 8: Recover all content and pages visited by the host machine.



According to question 5, we find that all content and pages visited by the host machine. Click "save all" to save the content to local computer.

Question 9: What are the domain names and IP addresses of the sites visited?

Through filter “http.request”, we could find “Destination”, it is the IP address of the sites visited, and the “Host” is the domain names of the sites.
Domain name and IP addresses：



http.request

Title: Time Type: UTC date, as YYYY-MM-DD, and time Fields: Enter a field ··· Occurrence: Resolve Names: OK Cancel

No.	Time	Source	Destination	Host	Protocol	Lengt	Full request URI	Info
3	2023-04-25 10:43:26.786175	192.168.185.137	23.72.36.187	ncc.avast.com	HTTP	136	http://ncc.avast.com/ncc.txt	GET /ncc.txt HT
9	2023-04-25 10:43:27.238779	192.168.185.137	23.72.36.112	ncc.avast.com	HTTP	136	http://ncc.avast.com/ncc.txt	GET /ncc.txt HT
10	2023-04-25 10:43:27.239872	192.168.185.137	13.107.4.52	www.msftconnecttest.com	HTTP	165	http://www.msftconnecttest.com/connecttest.txt	GET /connecttes
58	2023-04-25 10:43:35.301330	192.168.185.137	91.210.235.140	code.mccarthywebsites.com	HTTP	570	http://code.mccarthywebsites.com/	GET / HTTP/1.1
61	2023-04-25 10:43:35.386063	192.168.185.137	91.210.235.140	code.mccarthywebsites.com	HTTP	389	http://code.mccarthywebsites.com/js/scripts.js	GET /js/scripts
76	2023-04-25 10:43:47.140083	192.168.185.137	91.210.235.140	code.mccarthywebsites.com	HTTP	547	http://code.mccarthywebsites.com/demo.html	GET /demo.html
81	2023-04-25 10:43:47.300764	192.168.185.137	91.210.235.140	code.mccarthywebsites.com	HTTP	398	http://code.mccarthywebsites.com/js/scripts.js	GET /js/scripts
83	2023-04-25 10:43:58.359239	192.168.185.137	91.210.235.140	code.mccarthywebsites.com	HTTP	590	http://code.mccarthywebsites.com/assets/TU259_S…	GET /assets/TU2
87	2023-04-25 10:43:58.734173	192.168.185.137	91.210.235.140	code.mccarthywebsites.com	HTTP	491	http://code.mccarthywebsites.com/favicon.ico	GET /favicon.ic
91	2023-04-25 10:44:07.463232	192.168.185.137	91.210.235.140	code.mccarthywebsites.com	HTTP	557	http://code.mccarthywebsites.com/index.html	GET /index.html
97	2023-04-25 10:44:07.672130	192.168.185.137	91.210.235.140	code.mccarthywebsites.com	HTTP	399	http://code.mccarthywebsites.com/js/scripts.js	GET /js/scripts
103	2023-04-25 10:44:13.834118	192.168.185.137	91.210.235.140	www.amitycode.com	HTTP	530	http://www.amitycode.com/	GET / HTTP/1.1
108	2023-04-25 10:44:14.011701	192.168.185.137	91.210.235.140	www.amitycode.com	HTTP	389	http://www.amitycode.com/css/styles.css	GET /css/styles
111	2023-04-25 10:44:14.014340	192.168.185.137	91.210.235.140	www.amitycode.com	HTTP	373	http://www.amitycode.com/js/scripts.js	GET /js/scripts
150	2023-04-25 10:44:15.003436	192.168.185.137	91.210.235.140	www.amitycode.com	HTTP	439	http://www.amitycode.com/assets/favicon.ico	GET /assets/fav
155	2023-04-25 10:44:24.335596	192.168.185.137	91.210.235.140	www.amitycode.com	HTTP	563	http://www.amitycode.com/assets/Forensics_ICT_S…	GET /assets/For
481	2023-04-25 10:44:37.056487	192.168.185.137	91.210.235.140	www.amitycode.com	HTTP	556	http://www.amitycode.com/assets/USB_Disk_Image_…	GET /assets/USB
488	2023-04-25 10:44:45.000406	192.168.185.137	77.234.43.209	su.ff.avast.com	HTTP	372	http://su.ff.avast.com/R/A4QKIGQ3OWYzYjRkNDFhND…	GET /R/A4QKIGQ3
491	2023-04-25 10:44:45.440943	192.168.185.137	77.234.43.209	su.ff.avast.com	HTTP	372	http://su.ff.avast.com/R/A4QKIGQ3OWYzYjRkNDFhND…	GET /R/A4QKIGQ3

Question 10: Why do two of the sites have the same IP address?

When multiple domains point to one IP address, it is because HTTP requests sent from browsers include the host name. The server is able to identify it and serve the respective content. In our world we have very limited IPV4 addresses but more websites. A web hosting company usually serves over hundreds of websites from the same server (same IP).

It is possible for two or more websites to have the same IP address because of the use of shared hosting. Shared hosting is a type of web hosting where multiple websites are hosted on the same server and share the same IP address. In this case, the server is configured to route incoming traffic to the correct website based on the domain name specified in the HTTP request.

When a user types in a domain name, a DNS lookup is performed to resolve the domain name to an IP address. In the case where multiple websites share the same IP address, the DNS server will return the same IP address for each website. However, when the HTTP request is sent to the server, the server will use the domain name to determine which website the request is intended for, and route the traffic to the appropriate website.