

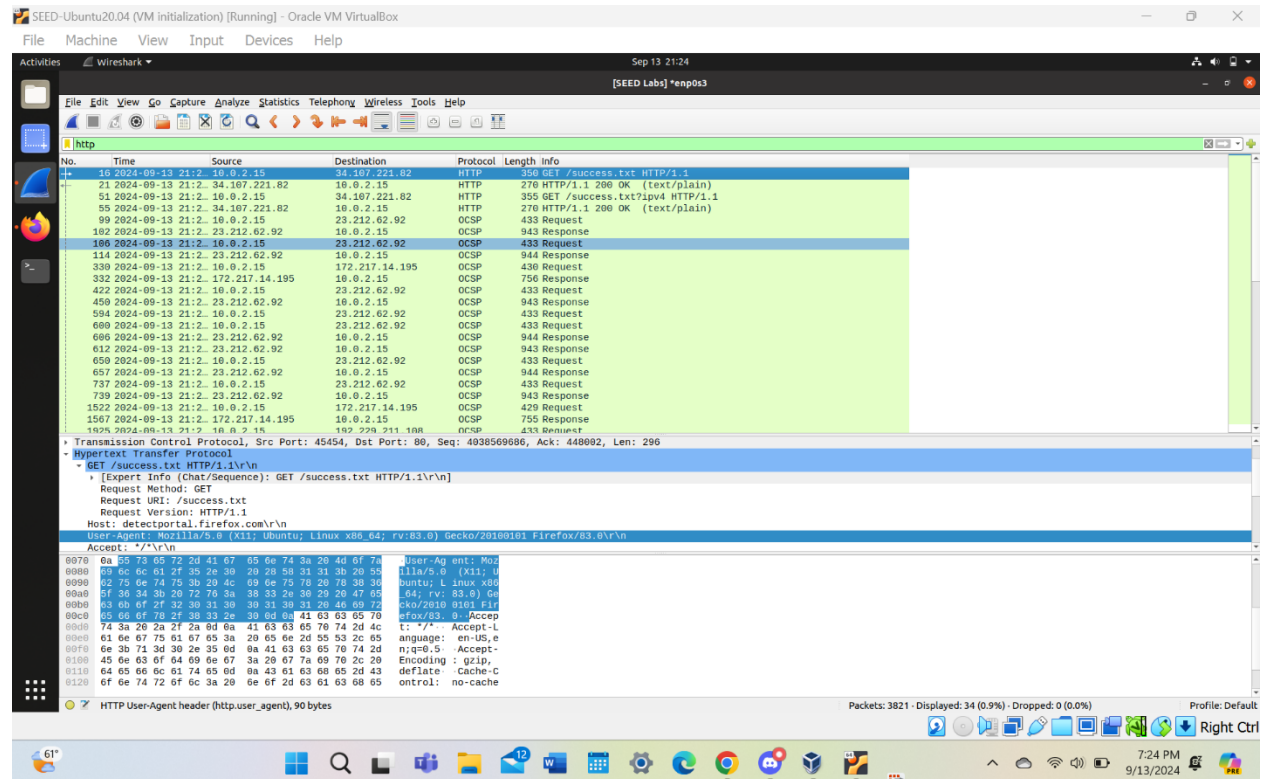
Aden Hartman & Willow Berryessa

CSCI 466

Lab 1

9/13/24

## Task 1:



## Task 2:

2.1) What is the IP address of gaia.cs.umass.edu?

34.107.221.82

2.2) What's the IP address of your machine?

10.0.2.15

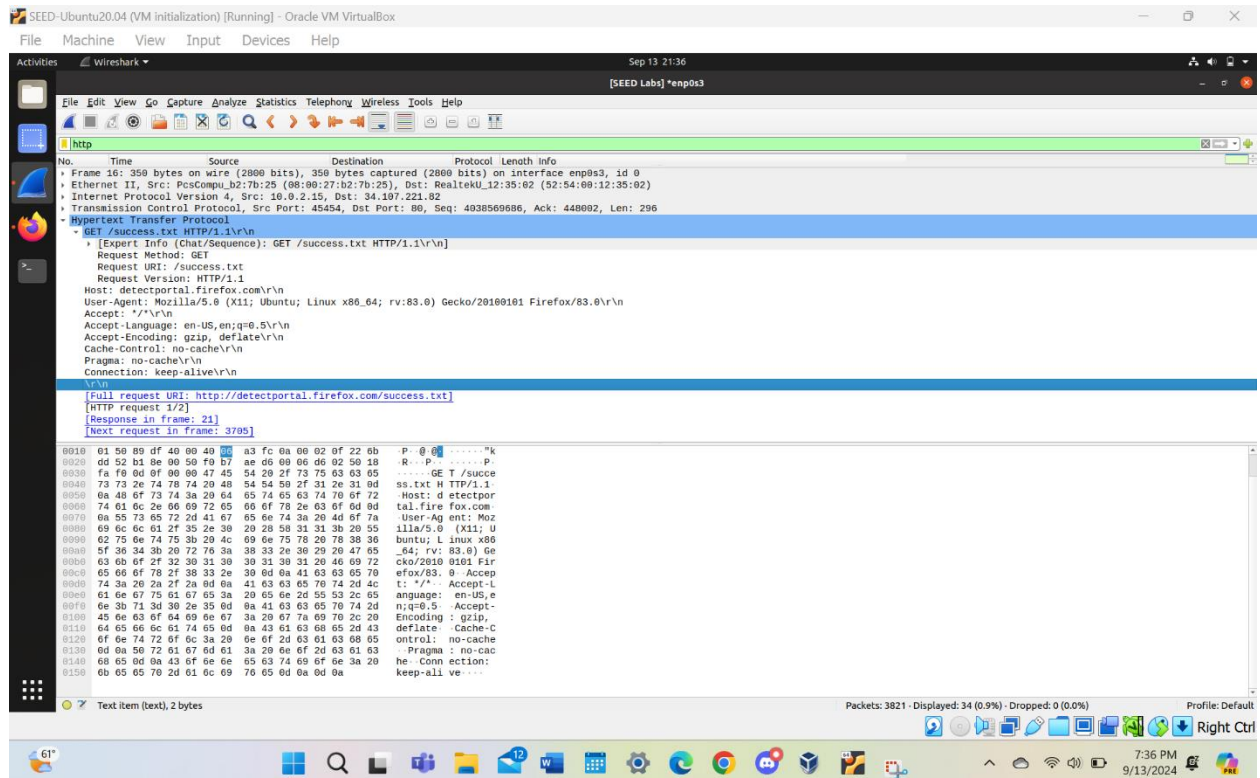
2.3) What is the destination port for this packet?

80

2.4) What version of http is being used for the request?

V1.1

2.5)



2.6)

13	2024-09-13 21:2...	10.0.2.15	34.107.221.82	TCP	74 45454 → 80 [SYN] Seq=4038569685 Win=64240 Len=0 MSS=1460 SACK
14	2024-09-13 21:2...	34.107.221.82	10.0.2.15	TCP	60 80 → 45454 [SYN, ACK] Seq=448001 Ack=4038569686 Win=65535 Len...
15	2024-09-13 21:2...	10.0.2.15	34.107.221.82	TCP	54 45454 → 80 [ACK] Seq=4038569686 Ack=448002 Win=64240 Len=0

## Task 3

3.1) What is the response code?

200

3.2) What type of content was returned from this response message?

Application/ocsp-response/r/n

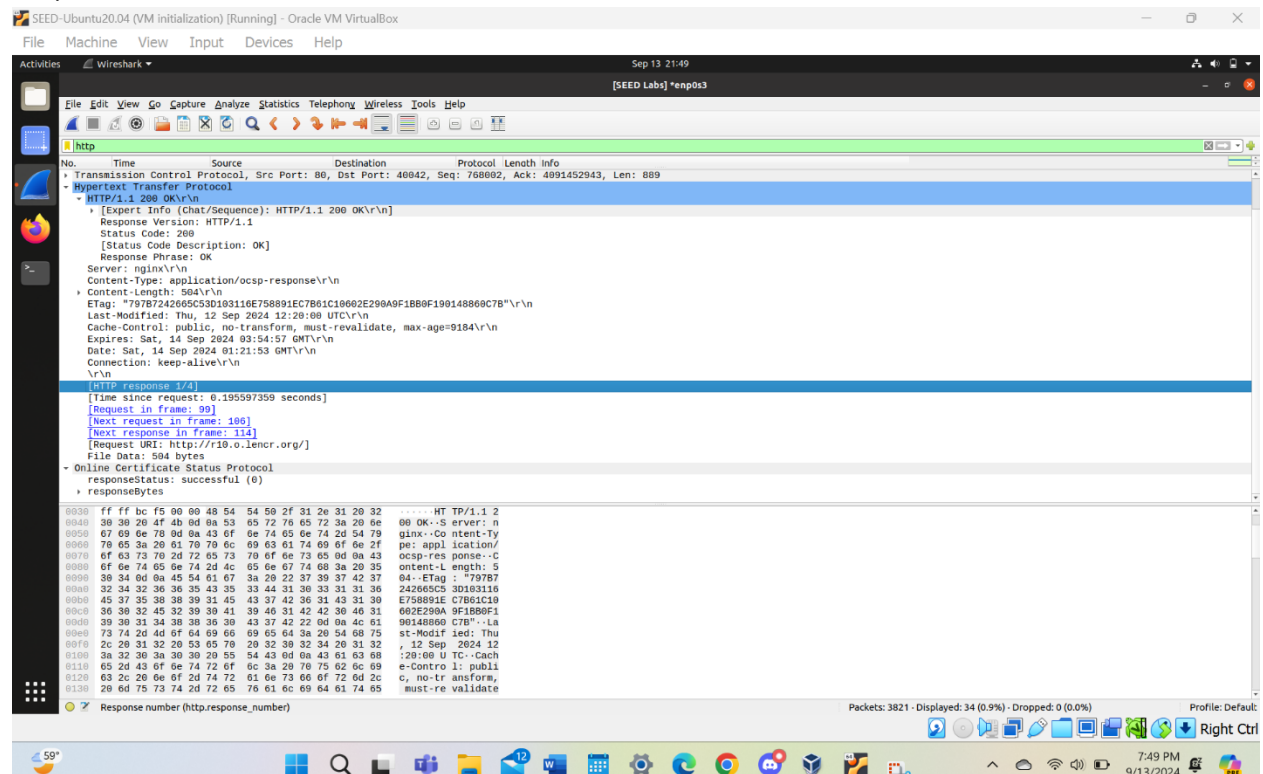
3.3) How long did it take from the get message being sent to receive the response?

0.195597359

3.4) What version of http is being used for the response?

V1.1

3.5)

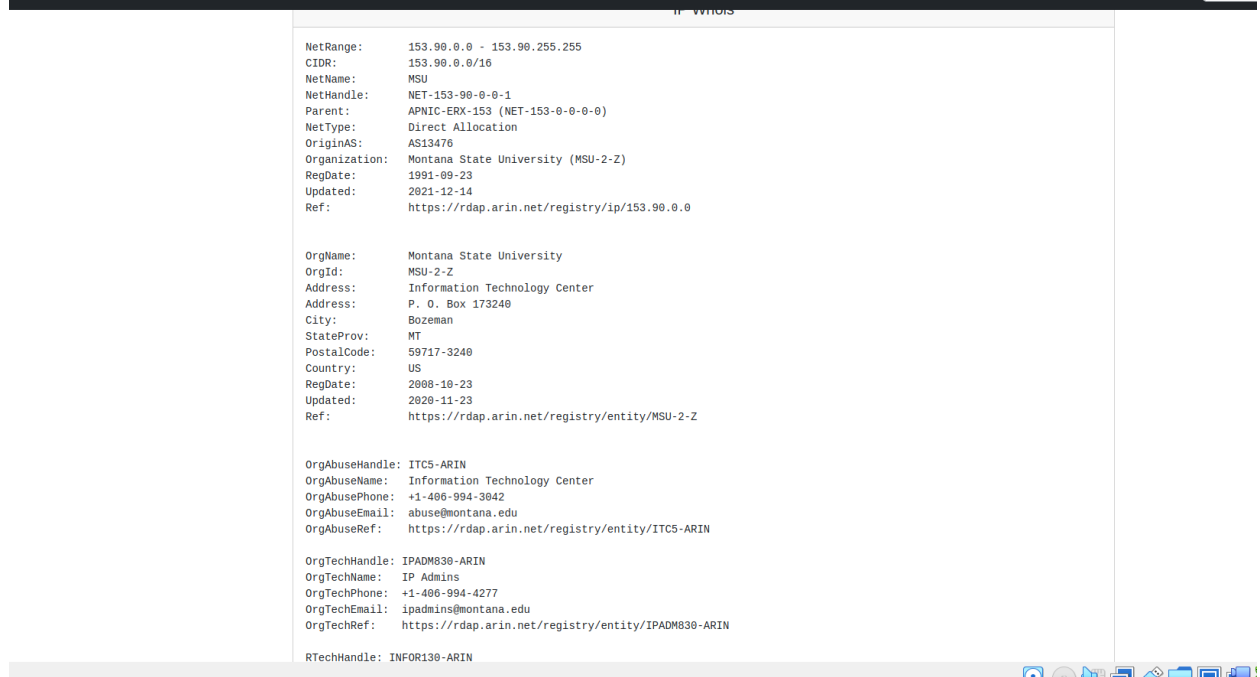


## Task 4:

4.1)



4.2)



```
NetRange: 153.90.0.0 - 153.90.255.255
CIDR: 153.90.0.0/16
NetName: MSU
NetHandle: NET-153-90-0-0-1
Parent: APNIC-ERX-153 (NET-153-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS13476
Organization: Montana State University (MSU-2-Z)
RegDate: 1991-09-23
Updated: 2021-12-14
Ref: https://rdap.arin.net/registry/ip/153.90.0.0

OrgName: Montana State University
OrgId: MSU-2-Z
Address: Information Technology Center
Address: P. O. Box 173240
City: Bozeman
StateProv: MT
PostalCode: 59717-3240
Country: US
RegDate: 2008-10-23
Updated: 2020-11-23
Ref: https://rdap.arin.net/registry/entity/MSU-2-Z

OrgAbuseHandle: ITC5-ARIN
OrgAbuseName: Information Technology Center
OrgAbusePhone: +1-406-994-3042
OrgAbuseEmail: abuse@montana.edu
OrgAbuseRef: https://rdap.arin.net/registry/entity/ITC5-ARIN

OrgTechHandle: IPADM830-ARIN
OrgTechName: IP Admins
OrgTechPhone: +1-406-994-4277
OrgTechEmail: ipadmins@montana.edu
OrgTechRef: https://rdap.arin.net/registry/entity/IPADM830-ARIN

RTechHandle: INFOR130-ARIN
```

4.3)

```
[09/13/24]seed@VM:~$ nslookup -type=NS montana.edu
Server: 127.0.0.53
Address: 127.0.0.53#53
```

Non-authoritative answer:

```
montana.edu      nameserver = dns1.msu.montana.edu.
montana.edu      nameserver = cudess2.umn.edu.
montana.edu      nameserver = dns2.msu.montana.edu.
```

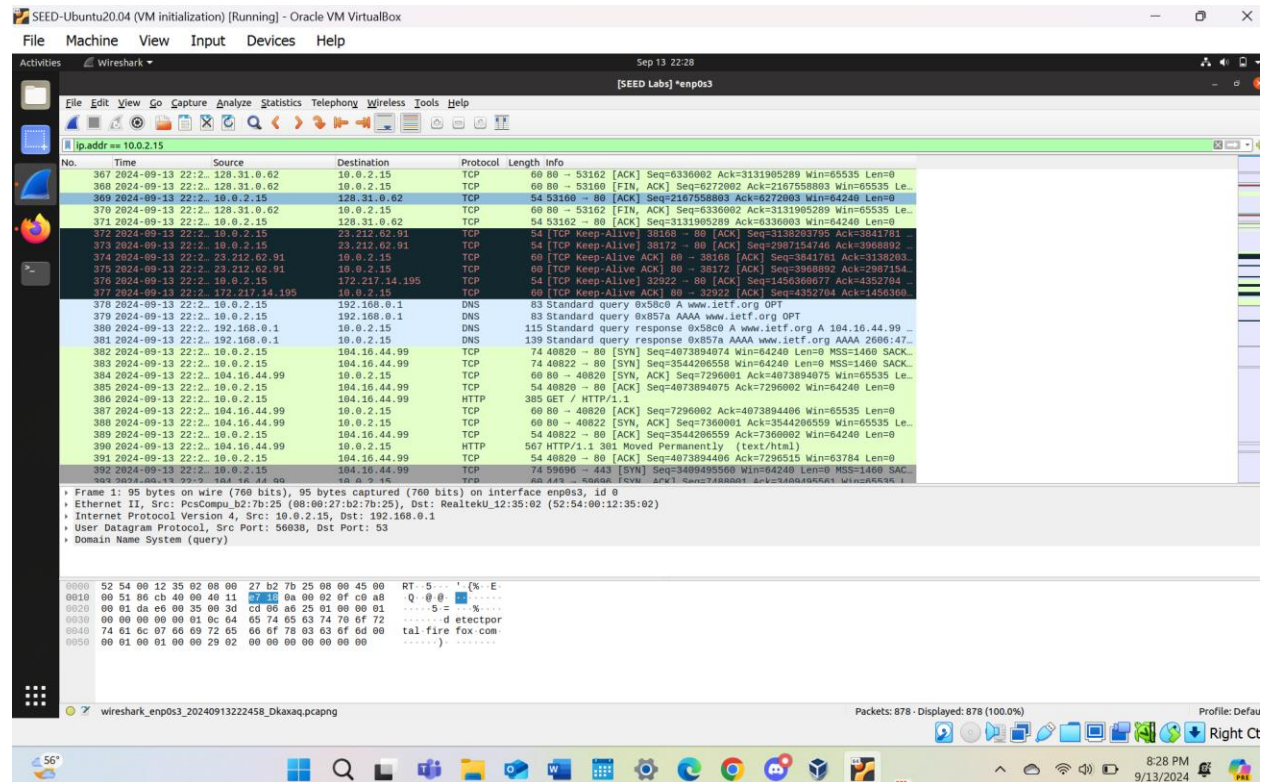
Authoritative answers can be found from:

4.4) What does the -type=MX flag mean? What was the answer for the DNS query you requested?

The type flag stands for mail exchange, and the answer for the DNS query was a list of hostnames for mail servers that handle email for the domain.

## Task 5

## 5.1)



## 5.2) Are the DNS query and response messages sent over UDP or TCP?

User Datagram Protocol

## 5.3) What is the destination port for the DNS query?

53

## 5.4) To what IP address is the DNS query message sent?

192.168.0.1

## 5.5) How many answers are provided in the DNS response message?

2 RRs

## 5.6) What is an IP address for ietf.org?

104.16.44.99

## Task 6

6.1)

The screenshot shows the Wireshark interface with the 'Endpoints - enp0s3' window open. The window displays a table of network endpoints with columns for Address, Packets, Bytes, Tx Packets, Rx Packets, Rx Bytes, Country, City, AS Number, and AS Organization. The table lists various IP addresses and their corresponding statistics, such as 10.0.2.15, 23.212.62.91, 34.107.221.82, etc.

Address	Packets	Bytes	Tx Packets	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
10.0.2.15	878	1,331 k	438	43 k	440	1,288 k	—	—	—
23.212.62.91	49	6,632	23	4,031	26	2,601 —	—	—	—
34.107.221.82	46	4,688	22	2,158	24	2,530 —	—	—	—
34.107.243.93	40	9,353	19	5,966	21	3,387 —	—	—	—
34.149.100.209	25	6,039	12	4,496	13	1,543 —	—	—	—
34.160.144.191	3	188	1	60	2	128 —	—	—	—
35.190.72.216	33	6,962	16	4,946	17	2,016 —	—	—	—
104.16.44.99	359	1,238 k	196	1,225 k	163	13 k	—	—	—
104.16.45.99	44	11 k	21	8,483	23	2,866 —	—	—	—
128.31.0.62	14	832	6	360	8	472 —	—	—	—
142.251.33.110	46	9,755	22	6,636	3,119	—	—	—	—
142.251.211.228	69	17 k	35	13 k	34	3,861 —	—	—	—
142.251.211.232	6	376	2	120	4	256 —	—	—	—
172.217.14.195	38	4,342	18	2,471	20	1,871 —	—	—	—
185.199.108.153	31	7,198	13	5,092	18	2,106 —	—	—	—
185.199.109.153	3	188	1	60	2	128 —	—	—	—
185.199.110.153	15	940	5	300	10	640 —	—	—	—
185.199.111.153	3	188	1	60	2	128 —	—	—	—
192.168.0.1	54	6,858	27	4,374	27	2,484 —	—	—	—