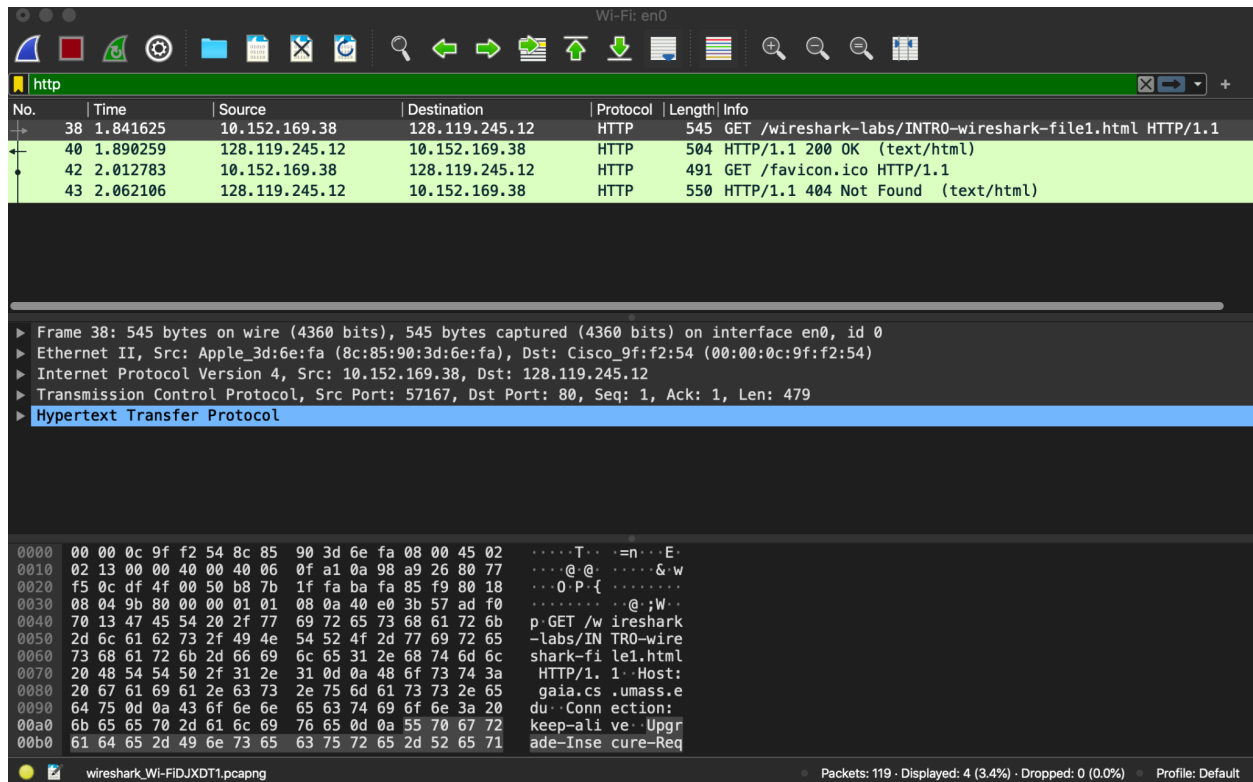


Noah Cunningham
Reese Pearsall
CSCI 466
10/3/22

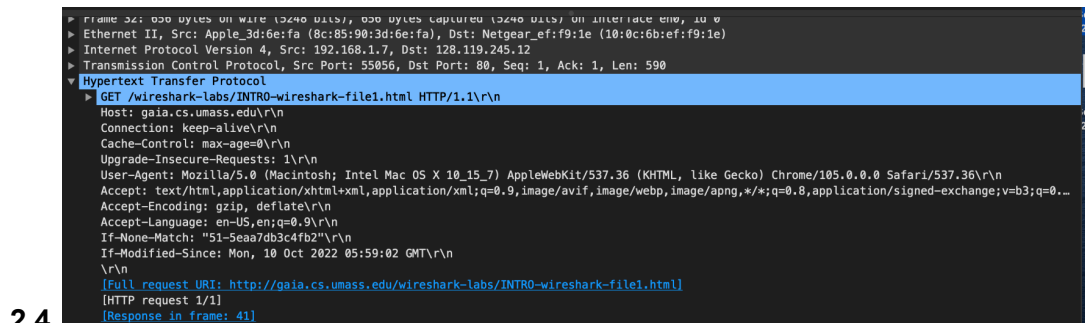
Wireshark Lab 1: HTTP and DNS

Task 1:



Task 2:

- 2.1: 10.152.169.38
- 2.2: 128.119.245.12
- 2.3: Port 80



2.4

Task 3:

- 3.1: 200 OK
- 3.2: (Text/HTML)

3.3: 0.06 seconds

3.4:

```
Internet Protocol Version 4, Src: 160.119.243.12, Dst: 192.168.1.1
Transmission Control Protocol, Src Port: 80, Dst Port: 55503, Seq: 1, Ack: 401, Len: 438
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Date: Tue, 11 Oct 2022 01:15:31 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 10 Oct 2022 05:59:02 GMT\r\n
    ETag: "51-5eaa7db3c4fb2"\r\n
    Accept-Ranges: bytes\r\n
  Content-Length: 81\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.062647000 seconds]
  [Request in frame: 1432]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
  File Data: 81 bytes
```

Task 4:

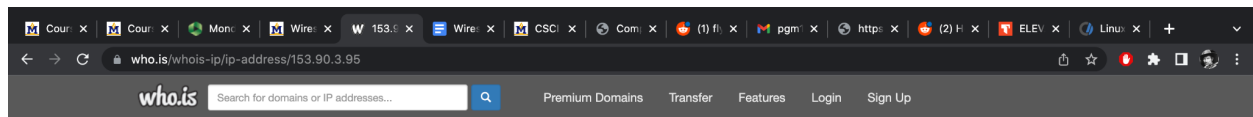
4.1: The server IP address is both 153.90.3.95 and 153.90.2.191, montana.edu uses a round robin setup to distribute server load

```
noahcunningham — -zsh — 80x24
Last login: Sun Sep 25 20:58:21 on console
[noahcunningham@Noahs-MacBook-Pro ~ % nslookup montana.edu
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
Name:   montana.edu
Address: 153.90.3.95
Name:   montana.edu
Address: 153.90.2.191

noahcunningham@Noahs-MacBook-Pro ~ %
```

4.2:



153.90.3.95 address profile

Whois	
Diagnostics	
IP Whois	
cache expires in 10 hours, 42 minutes and 55 seconds	
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

4.3: -type = MX flag displays the MX(mail exchange) record which specifies which email server is responsible for accepting emails. The answer is everything below the Non-Authoritative answer:

```
noahcunningham@Noahs-MacBook-Pro ~ % nslookup -type=MX www.youtube.com
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
www.youtube.com canonical name = youtube-ui.l.google.com.

Authoritative answers can be found from:
1.google.com
  origin = ns1.google.com
  mail addr = dns-admin.google.com
  serial = 480039807
  refresh = 900
  retry = 900
  expire = 1800
  minimum = 60

noahcunningham@Noahs-MacBook-Pro ~ %
```

Taks 5:

```

[noahcunningham@Noahs-MacBook-Pro ~ % ipconfig
usage: ipconfig <command> <args>
where <command> is one of waitall, getifaddr, ifcount, getoption, getpacket, get
v6packet, set, setverbose
[noahcunningham@Noahs-MacBook-Pro ~ % ipconfig /flushdns
usage: ipconfig <command> <args>
where <command> is one of waitall, getifaddr, ifcount, getoption, getpacket, get
v6packet, set, setverbose
[noahcunningham@Noahs-MacBook-Pro ~ % sudo killall -HUP mDNSResponder
[Password:
noahcunningham@Noahs-MacBook-Pro ~ %

```

```

noahcunningham@Noahs-MacBook-Pro ~ % ipconfig getifaddr en0
192.168.1.7
noahcunningham@Noahs-MacBook-Pro ~ %

```

5.1:

Wi-Fi: en0

ip.addr == 192.168.1.7

No.	Time	Source	Destination	Protocol	Length	Info
189	5.365717	192.168.1.7	54.174.157.118	TCP	66	55628 → 443 [ACK] Seq=1 Ack=46 Win=2047 Len=0 TSval=1518973497 TS
190	5.520724	192.168.1.7	192.168.1.1	DNS	72	Standard query 0x584d A www.ietf.org
191	5.520923	192.168.1.7	192.168.1.1	DNS	72	Standard query 0x8796 HTTPS www.ietf.org
192	5.521337	192.168.1.7	192.168.1.1	DNS	72	Standard query 0x2bf4 A www.ietf.org
193	5.729301	192.168.1.1	192.168.1.7	DNS	459	Standard query response 0x2bf4 A www.ietf.org CNAME www.ietf.org.
194	5.731227	192.168.1.1	192.168.1.7	DNS	459	Standard query response 0x584d A www.ietf.org CNAME www.ietf.org.
195	5.731232	192.168.1.1	192.168.1.7	DNS	497	Standard query response 0x8796 HTTPS www.ietf.org CNAME www.ietf.org.
196	5.736582	192.168.1.7	192.168.1.1	DNS	72	Standard query 0x7725 A www.ietf.org
197	5.736642	192.168.1.7	192.168.1.1	DNS	72	Standard query 0xb79f HTTPS www.ietf.org
198	5.741264	192.168.1.1	192.168.1.7	DNS	459	Standard query response 0x7725 A www.ietf.org CNAME www.ietf.org.
199	5.742276	192.168.1.1	192.168.1.7	DNS	497	Standard query response 0xb79f HTTPS www.ietf.org CNAME www.ietf.org.
200	5.742689	192.168.1.7	104.16.45.99	TCP	78	56676 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1518973497
201	5.785943	104.16.45.99	192.168.1.7	TCP	66	443 → 56676 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK

Frame 190: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id 0

Ethernet II, Src: Apple_3d:6e:fa (8c:85:90:3d:6e:fa), Dst: Netgear_ef:f9:1e (10:0c:6b:ef:f9:1e)

Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.1.1

User Datagram Protocol, Src Port: 23209, Dst Port: 53

Source Port: 23209

Destination Port: 53

Length: 38

Checksum: 0xa6d8 [unverified]

[Checksum Status: Unverified]

[Stream index: 7]

[Timestamps]

UDP payload (30 bytes)

Domain Name System (query)

5.2: UDP as shown above

5.3: 53 as shown above

5.4: 192.168.1.1

5.5: There are 5 response messages and 4/5 have 3 answers and 1 has 2 answers

5.6: 192.168.1.7