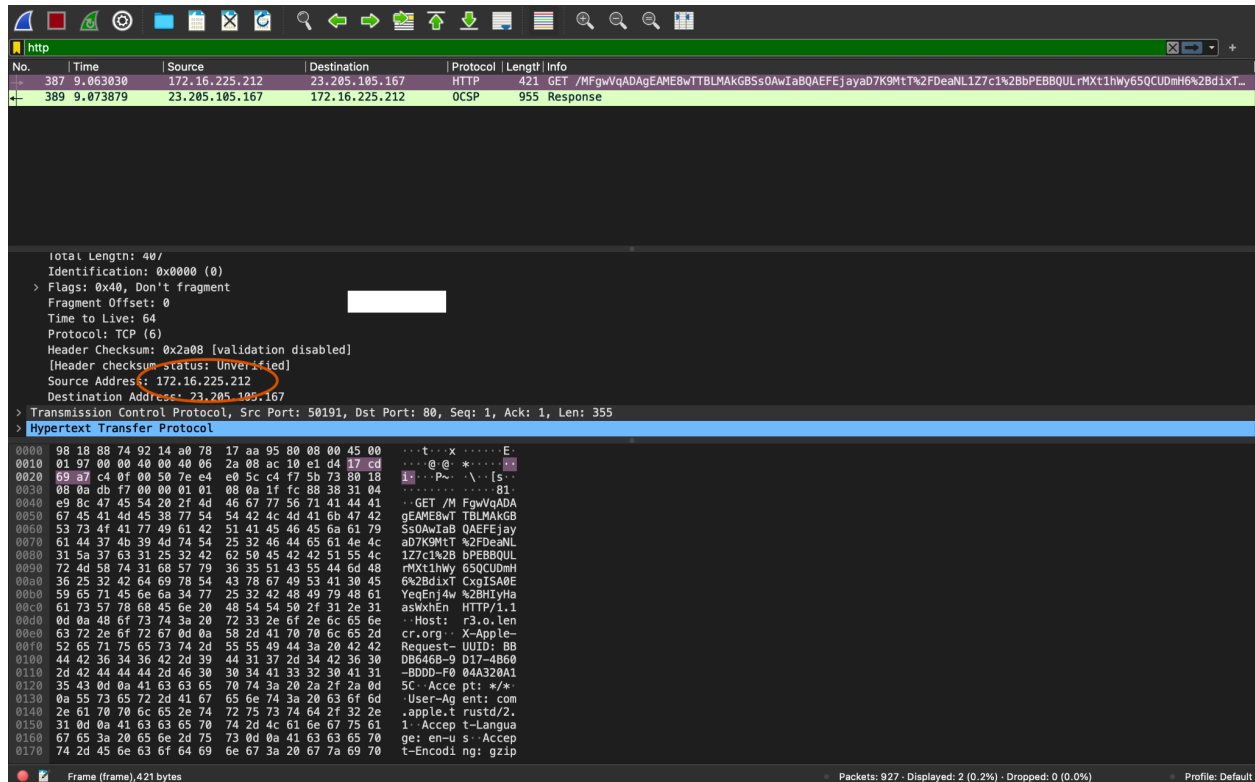


William Wright

IT-120

Lab 3

1. What is the Internet address of your computer?



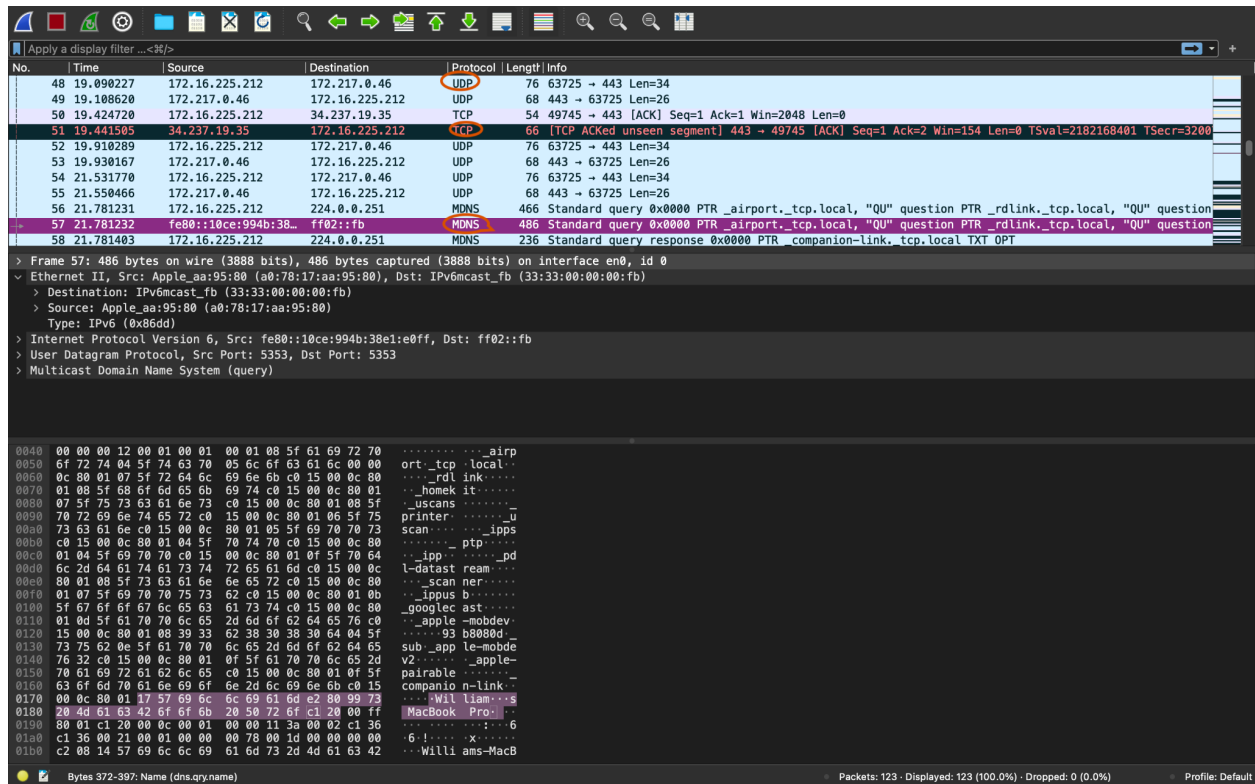
```
No. | Time | Source | Destination | Protocol | Length | Info
---|---|---|---|---|---|---
387 | 9.063030 | 172.16.225.212 | 23.205.105.167 | HTTP | 421 | GET /MFgwVqADAgEAME8wTTBLMAKGBSS0AwIaBQAEFEjayaD7K9MtT%2FDeaNL127c1%2BbPEBBQULrMXt1hwy65QCUDmH6%2Bd1xT...
389 | 9.073879 | 23.205.105.167 | 172.16.225.212 | OCSP | 955 | Response

Total Length: 40/
Identification: 0x0000 (0)
> Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x2a08 [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.16.225.212
Destination Address: 23.205.105.167
> Transmission Control Protocol, Src Port: 50191, Dst Port: 80, Seq: 1, Ack: 1, Len: 355
> Hypertext Transfer Protocol

0000  98 18 88 74 92 14 a0 78 17 aa 95 80 08 00 45 00  ...t...x.....E:
0010  01 97 00 00 40 00 40 06 2a 08 ac 10 e1 d4 17 cd  ...@.@ *.....-
0020  69 a7 c4 0f 00 50 7e e4 e0 5c c4 f7 5b 73 80 18  1...P... \...[s-
0030  08 0a db f7 00 00 01 01 08 0a 1f fc 88 38 31 04  ... ..-...-B1
0040  e9 8c 47 45 54 20 2f 4d 46 07 77 56 71 41 44 41  ...GET /M FgwVqADA
0050  67 45 41 4d 45 38 77 54 54 42 4c 4d 41 6b 47 42  gEAME8wTTBLMAKGB
0060  53 73 4f 41 77 49 61 42 51 41 45 46 45 6a 61 79  SsQAwIaB QAEFEjay
0070  61 44 37 4b 39 4d 74 54 25 32 46 44 65 61 4e 4c  aD7K9MtT %2FDeaNL
0080  31 5a 37 63 31 25 32 42 62 50 45 42 42 51 55 4c  127c1%2B bPEBBQUL
0090  72 4d 58 74 31 68 57 79 36 35 51 43 55 44 6d 48  rMXt1hwy 65QCUDmH
00a0  36 25 32 42 64 69 78 54 43 78 67 49 53 41 30 45  6%2Bd1xT CxgISA0E
00b0  59 65 71 45 6e 6a 34 77 25 32 42 48 49 79 48 61  YeqEnj4w %2BHIyHa
00c0  61 73 57 78 68 45 6e 20 48 54 50 2f 31 2e 31 2e  asWxhEn HTTP/1.1
00d0  0d 0a 48 6f 73 74 3a 20 72 33 2e 6f 2e 6c 65 6e  ..Host: r3.o.len
00e0  63 72 2e 6f 72 67 0d 0a 58 2d 41 70 70 6c 65 2d  cr.org: X-Apple-
00f0  52 65 71 75 65 73 74 2d 55 55 49 44 3a 20 42 42  Request: UUID: Bb
0100  44 42 36 34 36 42 2d 39 44 31 37 2d 34 42 36 30  DB6468-9 D17-4860
0110  2d 42 44 44 44 2d 46 30 30 34 41 33 32 30 41 31  -BDDD-F0 04A320A1
0120  35 43 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d  5C..Acce pt: */*
0130  0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 63 6f 6d  .User-Ag ent: com
0140  2e 61 70 70 6c 65 2e 74 72 75 73 74 64 2f 32 2e  .apple.t rustd/2.
0150  31 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61  1..Accep t-Langua
0160  67 65 3a 20 65 6e 2d 75 73 0d 0a 41 63 63 65 70  ge: en-u s..Accep
0170  74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70  t-Encodi ng: gzip
```

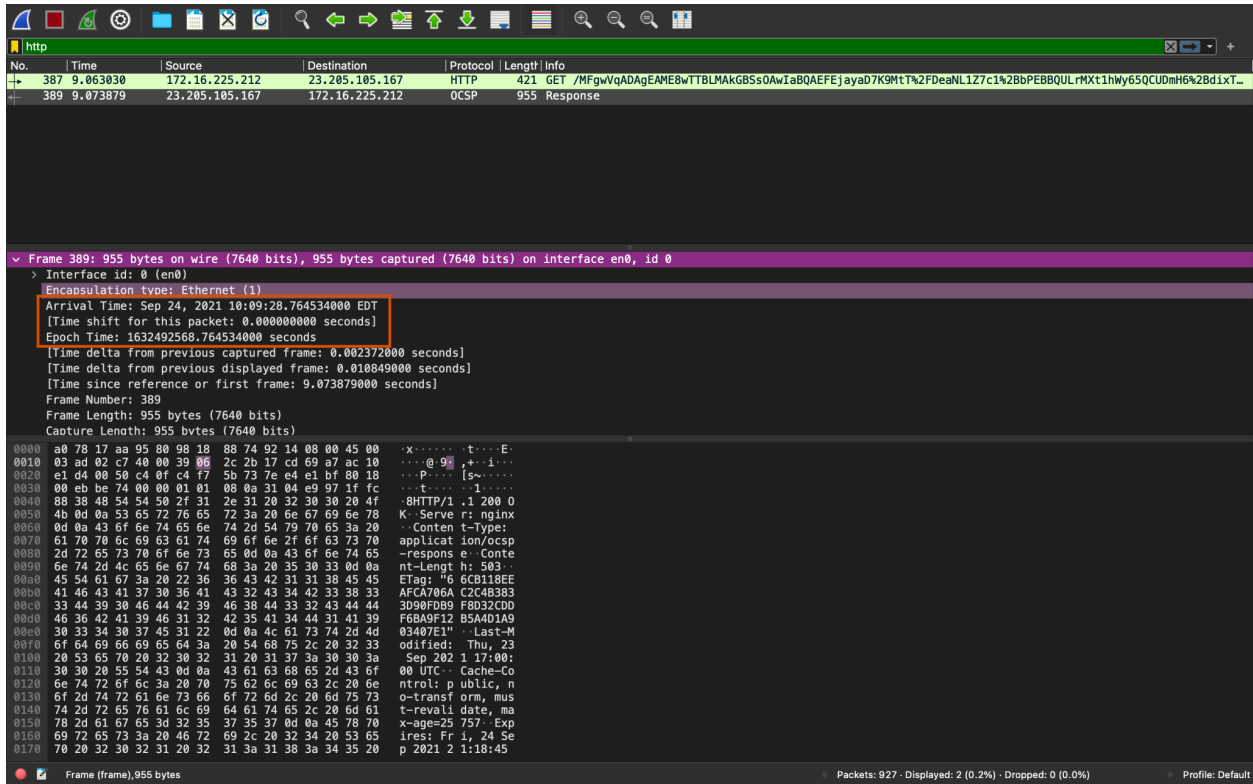
172.16.225.212

2. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.



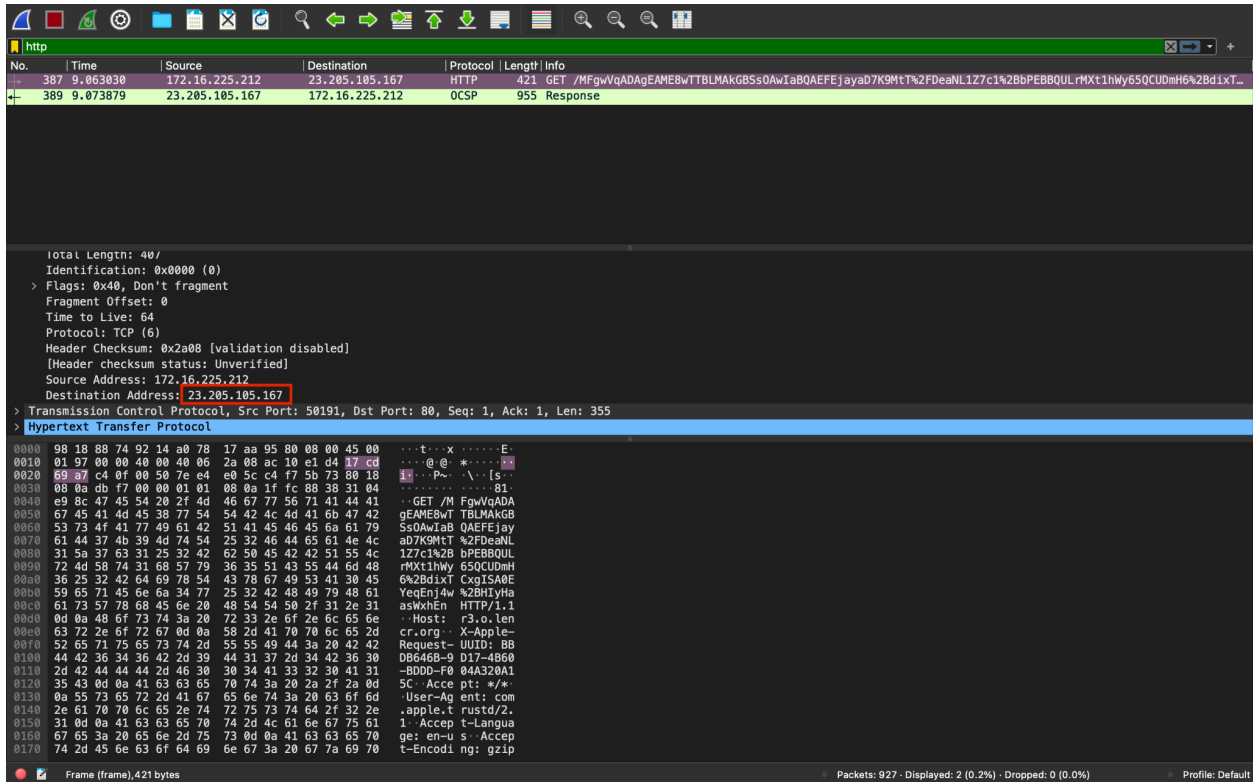
UDP, TCP, MDNS

3. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)



0.0000 seconds passed from the arrival to the epoch time.

4. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)?



23.205.105.167

5. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.

Wireshark interface showing network traffic analysis. The top pane displays a list of captured packets, with packet 389 selected. The middle pane shows the details of the selected packet, including the Ethernet II header and the HTTP GET request. The bottom pane displays the raw packet data in hexadecimal and ASCII.

Packets List:

No.	Time	Source	Destination	Protocol	Length	Info
387	9.063030	172.16.225.212	23.205.105.167	HTTP	421	GET /MfgwVqADAgEAME8wTTBLMAKGBSsQAwIaBQAEFEjayaD7K9MtT%2FDeaNL1Z7c1%2BbPEBBQULrMxt1hWy65QCUDmH6%2Bd1xT...
389	9.073879	23.205.105.167	172.16.225.212	OCSP	955	Response

Frame 389: 955 bytes on wire (7640 bits), 955 bytes captured (7640 bits) on interface en0, id 0

Ethernet II, Src: en0, Dst: 08:00:27:00:00:00, Length: 955

Arrival Time: Sep 24, 2021 10:09:28.764534000 EDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1632492568.764534000 seconds
[Time delta from previous captured frame: 0.002372000 seconds]
[Time delta from previous displayed frame: 0.010840000 seconds]
[Time since reference or first frame: 9.073879000 seconds]
Frame Number: 389
Frame Length: 955 bytes (7640 bits)
Capture Length: 955 bytes (7640 bits)

HTTP, GET /MfgwVqADAgEAME8wTTBLMAKGBSsQAwIaBQAEFEjayaD7K9MtT%2FDeaNL1Z7c1%2BbPEBBQULrMxt1hWy65QCUDmH6%2Bd1xT...

OCSP, Response

Raw Data:

```
0000  a0 70 17 aa 95 00 00 10 80 74 92 14 00 00 45 00  x-----t---E-
0010  03 ad 02 c7 40 00 39 00 2c 2b 17 cd 69 a7 ac 10  ---@.9---+..i---
0020  e1 d4 00 50 c4 0f c4 f7 5b 73 7e e4 e1 bf 80 18  ...P---[s~-----
0030  00 eb be 74 00 00 01 01 08 0a 31 04 e9 97 1f fc  ...t---.1-----
0040  88 38 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f  .8HTTP/1.1 200 0
0050  4b 0d 0a 53 65 72 76 65 72 3a 20 6e 67 69 6e 78  K--Serve r: nginx
0060  0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20  -Conten t-Type:
0070  61 70 70 6c 69 63 61 74 69 6f 6e 2f 6f 63 73 70  applicat ion/ocsp
0080  2d 72 65 73 70 6f 6e 73 65 0d 0a 43 6f 6e 74 65  -respons e--Conte
0090  6e 74 2d 4c 65 6e 67 74 68 3a 20 35 30 33 0d 0a  nt-Lengt h: 503..
00a0  45 54 61 67 3a 20 22 36 36 43 42 31 31 38 45 45  ETag: "6 6CB118EE
00b0  41 46 43 41 37 30 36 41 43 32 43 34 42 33 30 33  AfcA706A C2C4B383
00c0  33 44 39 30 46 44 42 39 46 38 44 33 32 43 44 44  3090FD89 F8D32CDD
00d0  46 36 42 41 39 46 31 32 42 35 41 34 44 31 41 39  F6BA9F12 B5A4D1A9
00e0  30 33 34 30 37 45 31 22 0d 0a 4c 61 73 74 2d 4d  03407E1" ..Last-M
00f0  6f 64 69 66 69 65 64 3a 20 54 68 75 2c 20 32 33  odified: Thu, 23
0100  20 53 65 70 20 32 30 32 31 20 31 37 3a 30 30 3a  Sep 2021 17:00:
0110  30 30 20 55 54 43 0d 0a 43 61 63 68 65 2d 43 6f  00 UTC -Cache-Co
0120  6e 74 72 6f 6c 3a 20 70 75 62 6c 69 63 2c 20 6e  ntrol: p ublic, n
0130  6f 2d 74 72 61 6e 73 66 6f 72 6d 2c 20 6d 75 73  o-transf orm, mus
0140  74 2d 72 65 76 61 6c 69 64 61 74 65 2c 20 6d 61  t-revali date, ma
0150  78 2d 61 67 65 3d 32 35 37 35 37 0d 0a 45 78 70  x-age=25 757-Exp
0160  69 72 65 73 3a 20 46 72 69 2c 20 32 34 20 53 65  ires: Fri, 24 Se
0170  70 20 32 30 32 31 20 32 31 3a 31 38 3a 34 35 20  p 2021 2 11:18:45
```