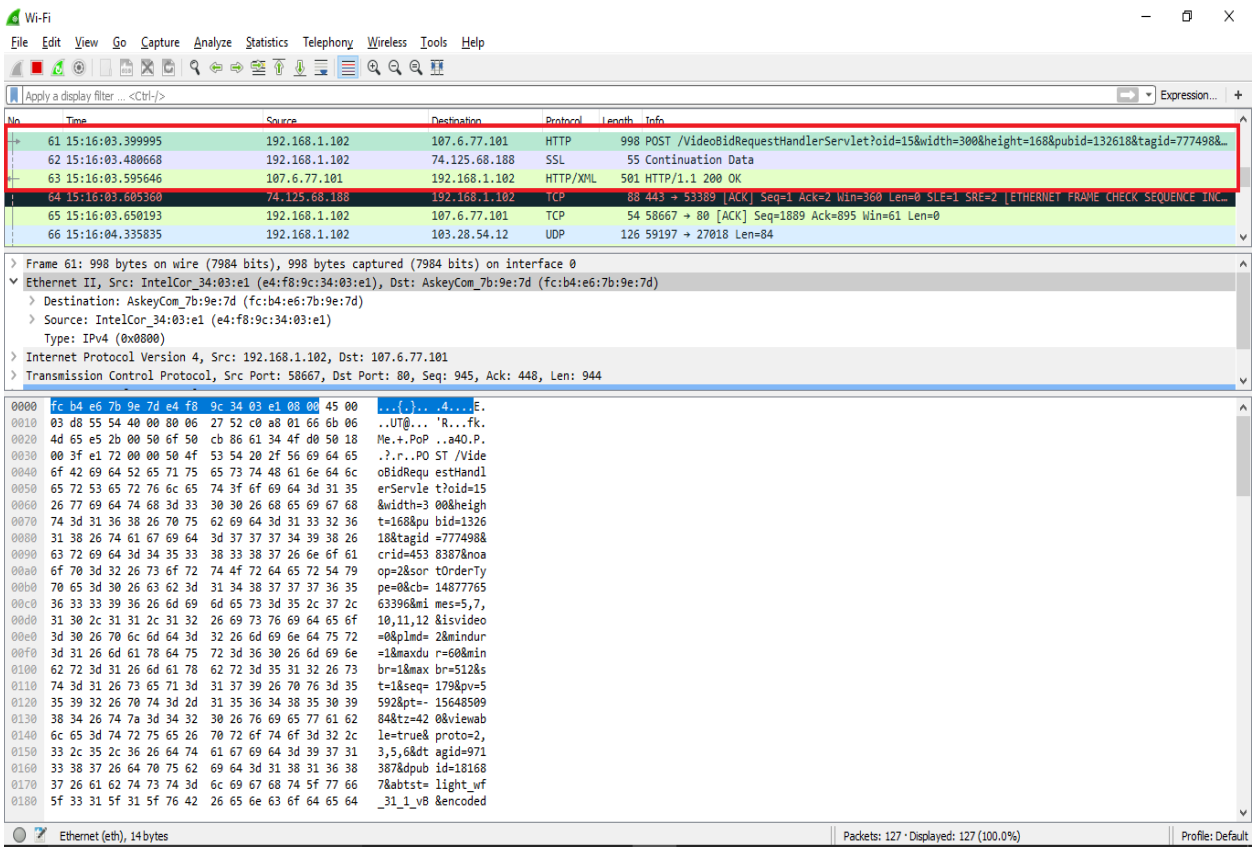
Họ Và Tên: Trần Văn Hiếu
Mã SV: 15021897

1. List the different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
   Answer:
   - HTTP
   - TCP
   - ARP
   - UDP
   - TLS
   - QUIC
   - SSDP
   - IGMP
   - MDNS
   - DNS
2. 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 packetlisting 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.)
   Answer:
   - As show in the screen below, the HTTP was sent at 03.399995 and the reply was received at 03.595646. The delay was 0.195651.



3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?
   Answer:
   Internet address gaia.cs.umass.edu: 125.235.4.59
   Internet address my computer: 192.168.1.1

4. Print the two HTTP messages displayed in step 9 above. To do so, select Print from the Wireshark File command menu, and select “Selected Packet Only” and “Print as displayed” and then click OK.
   Answer:
   GET HTTP:
   28567 15:55:24.658682 192.168.1.102 125.235.36.170 HTTP 355 GET /appinfo/568880/sha/ dfb6b9bcb01e5dc4fd6ec0fcc0eac5d0a1193c3e.txt.gz HTTP/1.1 Frame 28567: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface 0 Interface id: 0 (\Device\NPF_{88AC6491-510A-4D87-A6EF-

C4ECD466ECD9}) Encapsulation type: Ethernet (1) Arrival Time: Feb 22, 2017 22:55:24.658682000 SE Asia Standard Time [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1487778924.658682000 seconds [Time delta from previous captured frame: 0.000330000 seconds] [Time delta from previous displayed frame: 0.000330000 seconds] [Time since reference or first frame: 482.582714000 seconds] Frame Number: 28567 Frame Length: 355 bytes (2840 bits) Capture Length: 355 bytes (2840 bits) [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: eth:ethertype:ip:tcp:http] [Coloring Rule Name: HTTP] [Coloring Rule String: http || tcp.port == 80 || http2] Ethernet II, Src: IntelCor_34:03:e1 (e4:f8:9c:34:03:e1), Dst: AskeyCom_7b:9e:7d (fc:b4:e6:7b:9e:7d) Destination: AskeyCom_7b:9e:7d (fc:b4:e6:7b:9e:7d) Source: IntelCor_34:03:e1 (e4:f8:9c:34:03:e1) Type: IPv4 (0x0800) Internet Protocol Version 4, Src: 192.168.1.102, Dst: 125.235.36.170 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 341 Identification: 0x0876 (2166) Flags: 0x02 (Don't Fragment) Fragment offset: 0 Time to live: 128 Protocol: TCP (6) Header checksum: 0x8c89 [validation disabled] [Header checksum status: Unverified] Source: 192.168.1.102 Destination: 125.235.36.170 [Source GeoIP: Unknown] [Destination GeoIP: Unknown] Transmission Control Protocol, Src Port: 58937, Dst Port: 80, Seq: 1, Ack: 1, Len: 301 Hypertext Transfer Protocol GET /appinfo/568880/sha/dfb6b9bcb01e5dc4fd6ec0fcc0eac5d0a1193c3e.txt.gz HTTP/1.1\r\n Host: clientconfig.akamai.steamstatic.com\r\n Accept: text/html,*/*;q=0.9\r\n Accept-Encoding: gzip,identity,*;q=0\r\n Accept-Charset: ISO-8859-1,utf-8,*;q=0.7\r\n Connection: keep-alive\r\n User-Agent: Valve/Steam HTTP Client 1.0\r\n \r\n [Full request URI: http://clientconfig.akamai.steamstatic.com/appinfo/568880/sha/dfb6b9bcb01e5dc4fd6ec0fcc0eac5d0a1193c3e.txt.gz] [HTTP request 1/1] [Response in frame: 28570]
HTTP OK:
28570 15:55:24.663918 125.235.36.170 192.168.1.102 HTTP 1452 HTTP/1.1 200 OK (application/gzip) Frame 28570: 1452 bytes on wire (11616 bits), 1452 bytes captured (11616 bits) on interface 0 Interface

id: 0 (\Device\NPF_{88AC6491-510A-4D87-A6EF-C4ECD466ECD9}) Encapsulation type: Ethernet (1) Arrival Time: Feb 22, 2017 22:55:24.663918000 SE Asia Standard Time [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1487778924.663918000 seconds [Time delta from previous captured frame: 0.000002000 seconds] [Time delta from previous displayed frame: 0.005236000 seconds] [Time since reference or first frame: 482.587950000 seconds] Frame Number: 28570 Frame Length: 1452 bytes (11616 bits) Capture Length: 1452 bytes (11616 bits) [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: eth:ethertype:ip:tcp:http:media] [Coloring Rule Name: HTTP] [Coloring Rule String: http || tcp.port == 80 || http2] Ethernet II, Src: AskeyCom_7b:9e:7d (fc:b4:e6:7b:9e:7d), Dst: IntelCor_34:03:e1 (e4:f8:9c:34:03:e1) Destination: IntelCor_34:03:e1 (e4:f8:9c:34:03:e1) Source: AskeyCom_7b:9e:7d (fc:b4:e6:7b:9e:7d) Type: IPv4 (0x0800) Internet Protocol Version 4, Src: 125.235.36.170, Dst: 192.168.1.102 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 1438 Identification: 0x4f68 (20328) Flags: 0x02 (Don't Fragment) Fragment offset: 0 Time to live: 58 Protocol: TCP (6) Header checksum: 0x874e [validation disabled] [Header checksum status: Unverified] Source: 125.235.36.170 Destination: 192.168.1.102 [Source GeoIP: Unknown] [Destination GeoIP: Unknown] Transmission Control Protocol, Src Port: 80, Dst Port: 58937, Seq: 1, Ack: 302, Len: 1398 Hypertext Transfer Protocol HTTP/1.1 200 OK\r\n Content-Type: application/gzip\r\n Content-Length: 1232\r\n Cache-Control: max-age=1208822\r\n Date: Wed, 22 Feb 2017 15:55:23 GMT\r\n Connection: keep-alive\r\n \r\n [HTTP response 1/1] [Time since request: 0.005236000 seconds] [Request in frame: 28567] File Data: 1232 bytes Media Type