Abinash Gupta

120CS0157

Computer Networks Lab (S1)

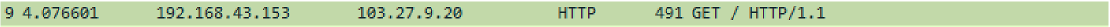
Q1: Answer the following questionsfor captured file http.pcap (HTTP Protocol)

1.List3 different protocolsthat appear in theprotocol column in the unfiltered packet-listing window in step 7 above.

Ans :- ARP , TCP , HTTP

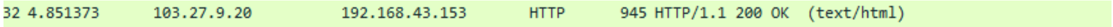
2. Howlongdid it takefrom when the HTTP GETmessagewas sent untilthe HTTP OK replywas received?(Bydefault, the value ofthe Time column in the packet-listingwindow is the amount of time, in seconds, sinceWireshark tracing began. To displaythe Timefield in time-of-dayformat, select the Wireshark Viewpull down menu, then selectTime DisplayFormat, then select Time-of-day.)

Ans - Sent GET



```
9 4.076601      192.168.43.153      103.27.9.20         HTTP      491 GET / HTTP/1.1
```

Rceived OK



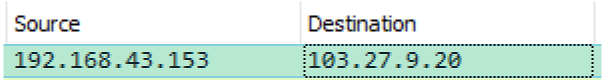
```
32 4.851373      103.27.9.20          192.168.43.153       HTTP      945 HTTP/1.1 200 OK  (text/html)
```

Time Taken :- 0.774772

3.What is theInternet address of iitd.ac.in?Whatis theInternet address of your computer?

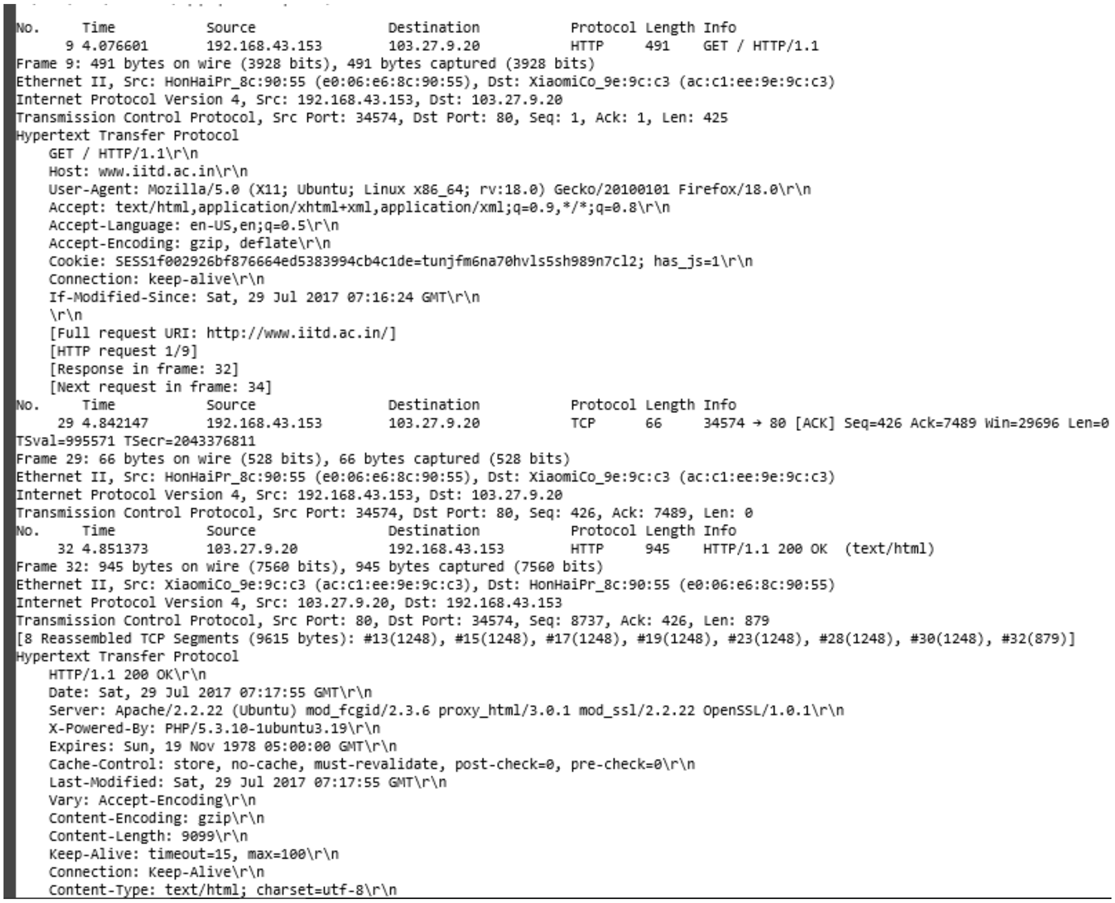
Ans :- Inntternet Adddress of iitd.ac.in :103.27.9.20

Internet Address of Computer : 192.168.43.153



Source	Destination
192.168.43.153	103.27.9.20

4.Printthe two HTTP messages (GETand OK) referred to in question 2 above. To do so, select Printfrom the Wireshark Filecommand menu, and selectthe “SelectedPacketOnly”and “Printasdisplayed”radial buttons, and then click OK.

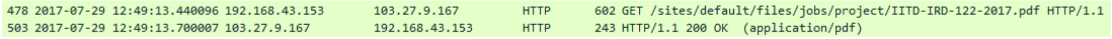


```
No.     Time           Source                Destination           Protocol Length Info
      9 4.076601       192.168.43.153        103.27.9.20           HTTP     491    GET / HTTP/1.1
Frame 9: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits)
Ethernet II, Src: HonHaiPr_8c:90:55 (e0:06:e6:8c:90:55), Dst: XiaomiCo_9e:9c:c3 (ac:c1:ee:9e:9c:c3)
Internet Protocol Version 4, Src: 192.168.43.153, Dst: 103.27.9.20
Transmission Control Protocol, Src Port: 34574, Dst Port: 80, Seq: 1, Ack: 1, Len: 425
Hypertext Transfer Protocol
    GET / HTTP/1.1\r\n
    Host: www.iitd.ac.in\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Cookie: SESS1f002926bf876664ed5383994cb4c1de=tunjfm6na70hvls5sh989n7cl2; has_js=1\r\n
    Connection: keep-alive\r\n
    If-Modified-Since: Sat, 29 Jul 2017 07:16:24 GMT\r\n
    \r\n
    [Full request URI: http://www.iitd.ac.in/]
    [HTTP request 1/9]
    [Response in frame: 32]
    [Next request in frame: 34]
No.     Time           Source                Destination           Protocol Length Info
     29 4.842147       192.168.43.153        103.27.9.20           TCP      66     34574 → 80 [ACK] Seq=426 Ack=7489 Win=29696 Len=0
TSval=995571 TSecr=2043376811
Frame 29: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: HonHaiPr_8c:90:55 (e0:06:e6:8c:90:55), Dst: XiaomiCo_9e:9c:c3 (ac:c1:ee:9e:9c:c3)
Internet Protocol Version 4, Src: 192.168.43.153, Dst: 103.27.9.20
Transmission Control Protocol, Src Port: 34574, Dst Port: 80, Seq: 426, Ack: 7489, Len: 0
No.     Time           Source                Destination           Protocol Length Info
     32 4.851373       103.27.9.20           192.168.43.153        HTTP     945    HTTP/1.1 200 OK  (text/html)
Frame 32: 945 bytes on wire (7560 bits), 945 bytes captured (7560 bits)
Ethernet II, Src: XiaomiCo_9e:9c:c3 (ac:c1:ee:9e:9c:c3), Dst: HonHaiPr_8c:90:55 (e0:06:e6:8c:90:55)
Internet Protocol Version 4, Src: 103.27.9.20, Dst: 192.168.43.153
Transmission Control Protocol, Src Port: 80, Dst Port: 34574, Seq: 8737, Ack: 426, Len: 879
[8 Reassembled TCP Segments (9615 bytes): #13(1248), #15(1248), #17(1248), #19(1248), #23(1248), #28(1248), #30(1248), #32(879)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sat, 29 Jul 2017 07:17:55 GMT\r\n
    Server: Apache/2.2.22 (Ubuntu) mod_fcgid/2.3.6 proxy_html/3.0.1 mod_ssl/2.2.22 OpenSSL/1.0.1\r\n
    X-Powered-By: PHP/5.3.10-1ubuntu3.19\r\n
    Expires: Sun, 19 Nov 1978 05:00:00 GMT\r\n
    Cache-Control: store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
    Last-Modified: Sat, 29 Jul 2017 07:17:55 GMT\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
    Content-Length: 9099\r\n
    Keep-Alive: timeout=15, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=utf-8\r\n
```

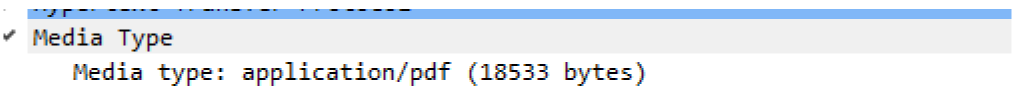
5. 5. Find the packet number that includes HTTP GET message for a file IITD-IRD-122-2017.pdf. Also find the length of the file in bytes and time when file is

downloadedsuccessfully.

Ans :



```
478 2017-07-29 12:49:13.440096 192.168.43.153       103.27.9.167        HTTP       602 GET /sites/default/files/jobs/project/IITD-IRD-122-2017.pdf HTTP/1.1
503 2017-07-29 12:49:13.700007 103.27.9.167         192.168.43.153      HTTP       243 HTTP/1.1 200 OK  (application/pdf)
```



```
✔ Media Type
    Media type: application/pdf (18533 bytes)
```

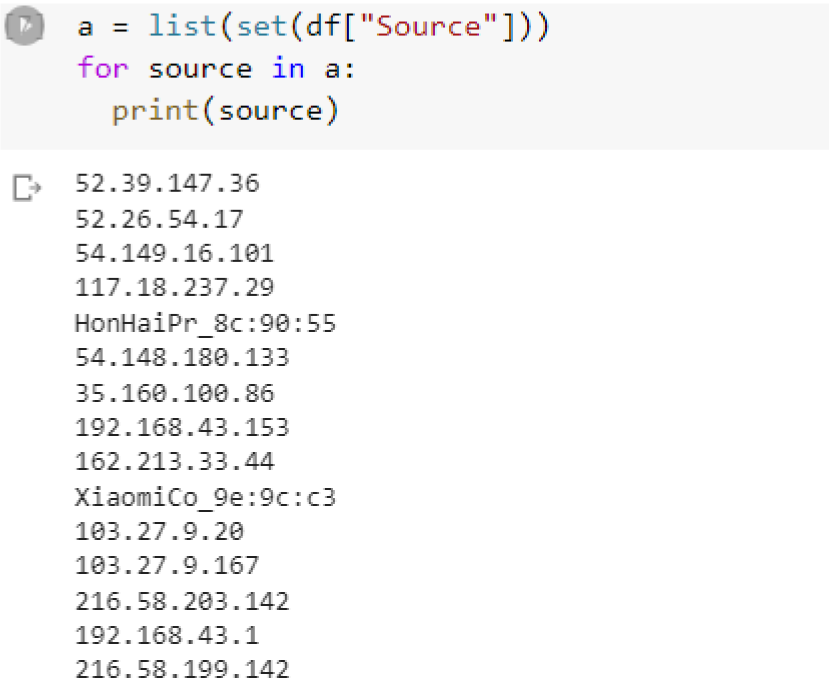
HTTP GET Packet: 478

Length of File :18533 bytes

Time : 12:49:13 Date - 29/07/2017

Q2 . Open the http.pcap file given in study material in Wireshark. Use File->Export Packet Dissections to save the data in csv file format. Write a C/C++/Java/Python code to read the data in csv file and print a. source IP addresses and destination IP addresses

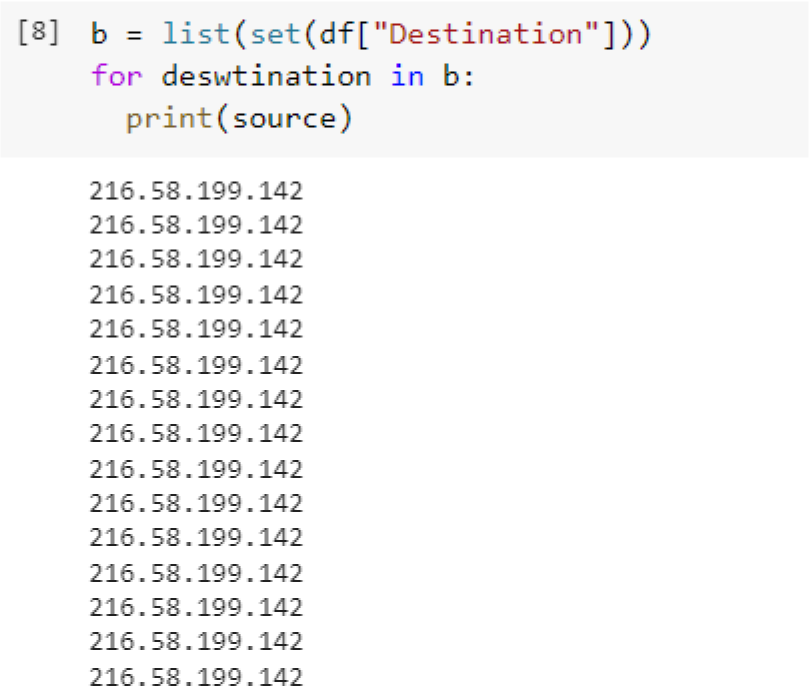
SOURCE IP ADDRESSES



```
a = list(set(df["Source"]))
for source in a:
  print(source)
```

```
52.39.147.36
52.26.54.17
54.149.16.101
117.18.237.29
HonHaiPr_8c:90:55
54.148.180.133
35.160.100.86
192.168.43.153
162.213.33.44
XiaomiCo_9e:9c:c3
103.27.9.20
103.27.9.167
216.58.203.142
192.168.43.1
216.58.199.142
```

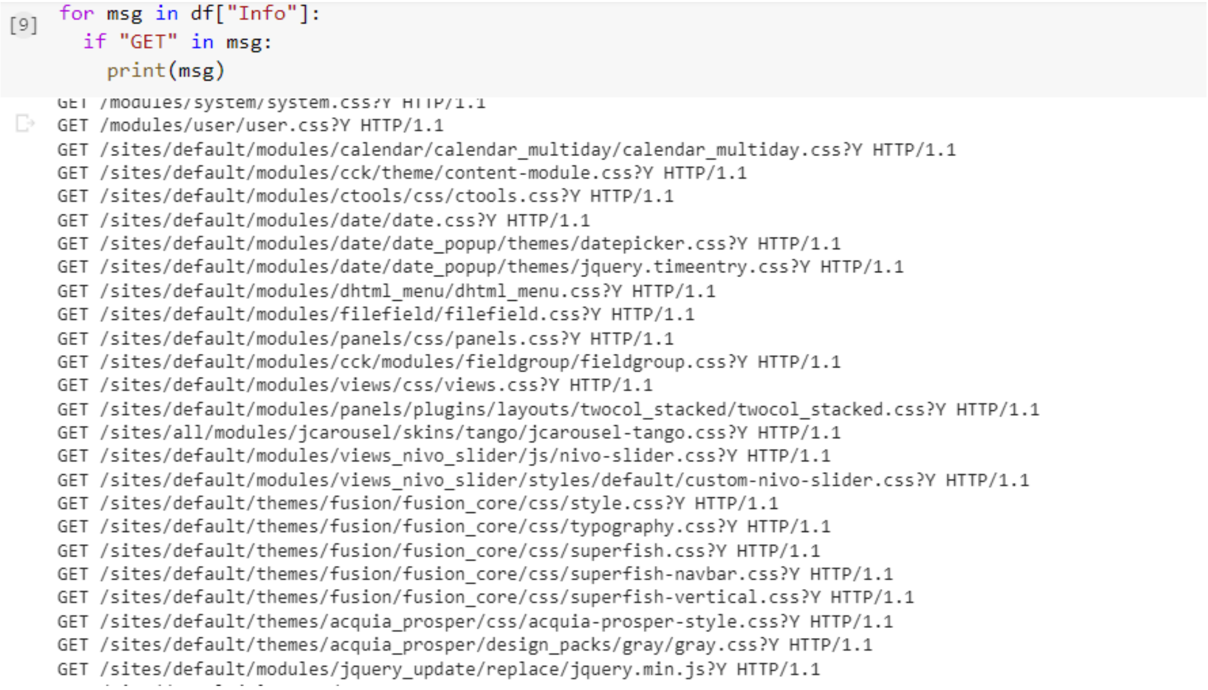
DESTINATION IP ADDRESS



```
[8]  b = list(set(df["Destination"]))
     for deswtination in b:
       print(source)
```

```
216.58.199.142
216.58.199.142
216.58.199.142
216.58.199.142
216.58.199.142
216.58.199.142
216.58.199.142
216.58.199.142
216.58.199.142
216.58.199.142
216.58.199.142
216.58.199.142
216.58.199.142
216.58.199.142
216.58.199.142
```

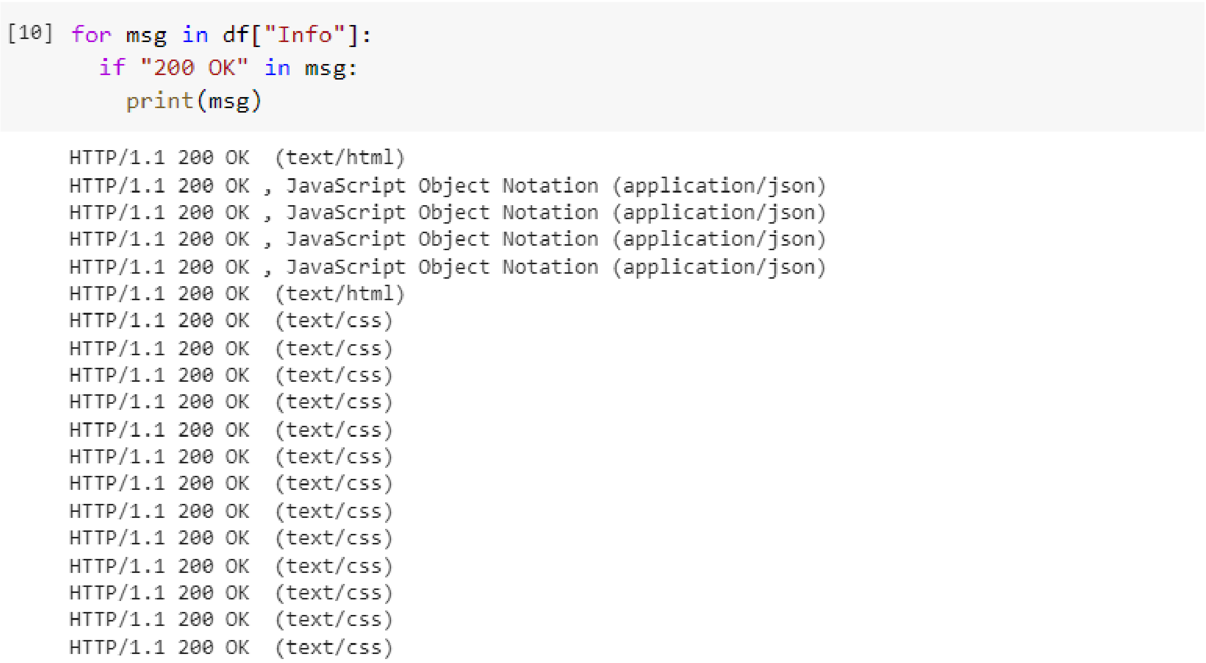
C . HTTP REQUESTS



```
[9] for msg in df["Info"]:
      if "GET" in msg:
        print(msg)
```

```
GET /modules/system/system.css?Y HTTP/1.1
GET /modules/user/user.css?Y HTTP/1.1
GET /sites/default/modules/calendar/calendar_multiday/calendar_multiday.css?Y HTTP/1.1
GET /sites/default/modules/cck/theme/content-module.css?Y HTTP/1.1
GET /sites/default/modules/ctools/css/ctools.css?Y HTTP/1.1
GET /sites/default/modules/date/date.css?Y HTTP/1.1
GET /sites/default/modules/date/date_popup/themes/datepicker.css?Y HTTP/1.1
GET /sites/default/modules/date/date_popup/themes/jquery.timeentry.css?Y HTTP/1.1
GET /sites/default/modules/dhtml_menu/dhtml_menu.css?Y HTTP/1.1
GET /sites/default/modules/filefield/filefield.css?Y HTTP/1.1
GET /sites/default/modules/panels/css/panels.css?Y HTTP/1.1
GET /sites/default/modules/cck/modules/fieldgroup/fieldgroup.css?Y HTTP/1.1
GET /sites/default/modules/views/css/views.css?Y HTTP/1.1
GET /sites/default/modules/panels/plugins/layouts/twocol_stacked/twocol_stacked.css?Y HTTP/1.1
GET /sites/all/modules/jcarousel/skins/tango/jcarousel-tango.css?Y HTTP/1.1
GET /sites/default/modules/views_nivo_slider/js/nivo-slider.css?Y HTTP/1.1
GET /sites/default/modules/views_nivo_slider/styles/default/custom-nivo-slider.css?Y HTTP/1.1
GET /sites/default/themes/fusion/fusion_core/css/style.css?Y HTTP/1.1
GET /sites/default/themes/fusion/fusion_core/css/typography.css?Y HTTP/1.1
GET /sites/default/themes/fusion/fusion_core/css/superfish.css?Y HTTP/1.1
GET /sites/default/themes/fusion/fusion_core/css/superfish-navbar.css?Y HTTP/1.1
GET /sites/default/themes/fusion/fusion_core/css/superfish-vertical.css?Y HTTP/1.1
GET /sites/default/themes/acquia_prosper/css/acquia-prosper-style.css?Y HTTP/1.1
GET /sites/default/themes/acquia_prosper/design_packs/gray/gray.css?Y HTTP/1.1
GET /sites/default/modules/jquery_update/replace/jquery.min.js?Y HTTP/1.1
```

RESPONSE MESSAGES



```
[10] for msg in df["Info"]:
       if "200 OK" in msg:
         print(msg)
```

```
HTTP/1.1 200 OK  (text/html)
HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
HTTP/1.1 200 OK  (text/html)
HTTP/1.1 200 OK  (text/css)
HTTP/1.1 200 OK  (text/css)
HTTP/1.1 200 OK  (text/css)
HTTP/1.1 200 OK  (text/css)
HTTP/1.1 200 OK  (text/css)
HTTP/1.1 200 OK  (text/css)
HTTP/1.1 200 OK  (text/css)
HTTP/1.1 200 OK  (text/css)
HTTP/1.1 200 OK  (text/css)
HTTP/1.1 200 OK  (text/css)
HTTP/1.1 200 OK  (text/css)
HTTP/1.1 200 OK  (text/css)
HTTP/1.1 200 OK  (text/css)
```