

AM.EN.P2CSN20020

3 Try to download a big file (say one book) and observe how many http requests are sent. Mark the GET messages and corresponding responses. What are the IP addresses from where the responses come from?

Answer: 19 HTTP requests are sent.

IP addresses – 5.45.74.67, 94.242.222.225 and 194.247.175.25

GET message has been highlighted in the below figure.

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The middle pane shows the details of the selected packet (Frame 79), which is an HTTP GET request. The bottom pane shows the raw data of the selected packet.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
17	2.152160	192.168.0.106	5.45.74.67	HTTP	884	GET /dl/1104483/e66266 HTTP/1.1
35	2.361131	5.45.74.67	192.168.0.106	HTTP	594	HTTP/1.1 302 Found (text/html)
79	2.606164	192.168.0.106	94.242.222.225	HTTP	971	GET /genesis/483000/caae8bc0813fa4dd8b14864aab94fd58/_as/[Bernard_Jaffe]_Crucibles_The...
368	7.485007	192.168.0.106	5.45.74.67	HTTP	10...	GET /css/dropdown/themes/flickr.com/images/nav-arrow-down-open.png HTTP/1.1
374	7.909376	192.168.0.106	194.247.175.25	HTTP	811	GET /pagestat/PageStatEntry?cookie=E82FBC0052434BD49BABA01332CEC2B3&time=1601310176088...
501	11.657128	5.45.74.67	192.168.0.106	HTTP	388	HTTP/1.1 200 OK (PNG)
513	11.956702	194.247.175.25	192.168.0.106	HTTP	276	HTTP/1.1 200 OK (application/json)
533	12.046964	5.45.74.67	192.168.0.106	HTTP	388	[TCP Spurious Retransmission] HTTP/1.1 200 OK (PNG)
540	12.058889	194.247.175.25	192.168.0.106	HTTP	276	[TCP Spurious Retransmission] HTTP/1.1 200 OK (application/json)
552	12.081718	5.45.74.67	192.168.0.106	HTTP	388	[TCP Spurious Retransmission] HTTP/1.1 200 OK (PNG)
560	12.094415	194.247.175.25	192.168.0.106	HTTP	276	[TCP Spurious Retransmission] HTTP/1.1 200 OK (application/json)
589	12.131475	5.45.74.67	192.168.0.106	HTTP	388	[TCP Spurious Retransmission] HTTP/1.1 200 OK (PNG)
13...	22.924018	192.168.0.106	194.247.175.25	HTTP	275	GET /pagestat/PageStatEntry?cookie=E82FBC0052434BD49BABA01332CEC2B3&time=1601310191102...
13...	23.136666	194.247.175.25	192.168.0.106	HTTP	276	HTTP/1.1 200 OK (application/json)
74...	52.913591	192.168.0.106	194.247.175.25	HTTP	275	GET /pagestat/PageStatEntry?cookie=E82FBC0052434BD49BABA01332CEC2B3&time=1601310221098...

**Packet Details (Frame 79):**

- Frame 79: 971 bytes on wire (7768 bits), 971 bytes captured (7768 bits) on interface \Device\NPF\_{8DD29CF6-2337-4B28-9F1E-596458C8B67C}, id 0
- Ethernet II, Src: IntelCor\_06:0b:53 (5c:87:9c:06:0b:53), Dst: Tp-LinkT\_64:16:70 (98:da:c4:64:16:70)
- Internet Protocol Version 4, Src: 192.168.0.106, Dst: 94.242.222.225
- Transmission Control Protocol, Src Port: 5164, Dst Port: 80, Seq: 1, Ack: 1, Len: 917
- Hypertext Transfer Protocol
  - GET /genesis/483000/caae8bc0813fa4dd8b14864aab94fd58/\_as/[Bernard\_Jaffe]\_Crucibles\_The\_Story\_of\_Chemistry\_(BookFi).pdf HTTP/1.1\r\n
  - [Expert Info (Chat/Sequence): GET /genesis/483000/caae8bc0813fa4dd8b14864aab94fd58/\_as/[Bernard\_Jaffe]\_Crucibles\_The\_Story\_of\_Chemistry\_(BookFi).pdf
  - Request Method: GET
  - Request URI: /genesis/483000/caae8bc0813fa4dd8b14864aab94fd58/\_as/[Bernard\_Jaffe]\_Crucibles\_The\_Story\_of\_Chemistry\_(BookFi).pdf
  - Request Version: HTTP/1.1
  - Host: dl.lux.bookfi.net\r\n
  - Connection: keep-alive\r\n

**Raw Data:**

HTTP Request HTTP-Version (http.request.version), 8 bytes

Packets: 15481 · Displayed: 19 (0.1%) · Dropped: 0 (0.0%)

Profile: Default

22:14  
28-09-2020

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
17	2.152160	192.168.0.106	5.45.74.67	HTTP	884	GET /dl/1104483/e66266 HTTP/1.1
35	2.361131	5.45.74.67	192.168.0.106	HTTP	594	HTTP/1.1 302 Found (text/html)
79	2.606164	192.168.0.106	94.242.222.225	HTTP	971	GET /genesis/483000/caae8bc0813fa4dd8b14864aab94fd58/_as/[Bernard_Jaffe]_Crucibles_The_Story_of_Chemistry_(BookFi).pdf HTTP/1.1
368	7.485007	192.168.0.106	5.45.74.67	HTTP	1008	GET /css/dropdown/themes/flickr.com/images/nav-arrow-down-open.png HTTP/1.1
374	7.909376	192.168.0.106	194.247.175.25	HTTP	811	GET /pagestat/PageStatEntry?cookie=E82FBC0052434BD498ABA01332CEC2B3&time=1601310176088&location=http%3A%2F%2Fen.bookfi.net%2Fbook%2F... HTTP/1.1
501	11.657128	5.45.74.67	192.168.0.106	HTTP	388	HTTP/1.1 200 OK (PNG)
513	11.956702	194.247.175.25	192.168.0.106	HTTP	276	HTTP/1.1 200 OK (application/json)
533	12.046964	5.45.74.67	192.168.0.106	HTTP	388	[TCP Spurious Retransmission] HTTP/1.1 200 OK (PNG)
540	12.058889	194.247.175.25	192.168.0.106	HTTP	276	[TCP Spurious Retransmission] HTTP/1.1 200 OK (application/json)
552	12.081718	5.45.74.67	192.168.0.106	HTTP	388	[TCP Spurious Retransmission] HTTP/1.1 200 OK (PNG)
560	12.094415	194.247.175.25	192.168.0.106	HTTP	276	[TCP Spurious Retransmission] HTTP/1.1 200 OK (application/json)
589	12.131475	5.45.74.67	192.168.0.106	HTTP	388	[TCP Spurious Retransmission] HTTP/1.1 200 OK (PNG)
1354	22.924018	192.168.0.106	194.247.175.25	HTTP	275	GET /pagestat/PageStatEntry?cookie=E82FBC0052434BD498ABA01332CEC2B3&time=1601310191102&location=http%3A%2F%2Fen.bookfi.net%2Fbook%2F... HTTP/1.1
1369	23.136666	194.247.175.25	192.168.0.106	HTTP	276	HTTP/1.1 200 OK (application/json)
7471	52.913591	192.168.0.106	194.247.175.25	HTTP	275	GET /pagestat/PageStatEntry?cookie=E82FBC0052434BD498ABA01332CEC2B3&time=1601310221098&location=http%3A%2F%2Fen.bookfi.net%2Fbook%2F... HTTP/1.1
7512	53.120956	194.247.175.25	192.168.0.106	ICMP	590	Destination unreachable (Host administratively prohibited)
7599	53.789174	194.247.175.25	192.168.0.106	HTTP	276	HTTP/1.1 200 OK (application/json)
14405	112.916832	192.168.0.106	194.247.175.25	HTTP	277	GET /pagestat/PageStatEntry?cookie=E82FBC0052434BD498ABA01332CEC2B3&time=1601310281102&location=http%3A%2F%2Fen.bookfi.net%2Fbook%2F... HTTP/1.1
14417	113.126610	194.247.175.25	192.168.0.106	HTTP	276	HTTP/1.1 200 OK (application/json)

> Transmission Control Protocol, Src Port: 5164, Dst Port: 80, Seq: 1, Ack: 1, Len: 917

> Hypertext Transfer Protocol

GET /genesis/483000/caae8bc0813fa4dd8b14864aab94fd58/\_as/[Bernard\_Jaffe]\_Crucibles\_The\_Story\_of\_Chemistry\_(BookFi).pdf HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /genesis/483000/caae8bc0813fa4dd8b14864aab94fd58/\_as/[Bernard\_Jaffe]\_Crucibles\_The\_Story\_of\_Chemistry\_(BookFi).pdf HTTP/1.1\r\n[GET /genesis/483000/caae8bc0813fa4dd8b14864aab94fd58/\_as/[Bernard\_Jaffe]\_Crucibles\_The\_Story\_of\_Chemistry\_(BookFi).pdf HTTP/1.1\r\n[Severity Level: Chat][Group: Sequence]Request Method: GETRequest URI: /genesis/483000/caae8bc0813fa4dd8b14864aab94fd58/\_as/[Bernard\_Jaffe]\_Crucibles\_The\_Story\_of\_Chemistry\_(BookFi).pdfRequest Version: HTTP/1.1Host: dl.lux.bookfi.net\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Edg/85.0.564.63\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\nReferer: http://en.bookfi.net/book/1104483\r\n

Total count of HTTP requests: 19

Formatted text (http.chat)

Packets: 15481 · Displayed: 19 (0.1%) · Dropped: 0 (0.0%) Profile: Default

Type here to search

22:17 28-09-2020