

COL334 - Assignment 1

Internet Architecture

Akshay Kumar Gupta
2013CS50275

Barun Patra
2013CS10773

Haroun Habeeb
2013CS10225

Q4a. List of applications generating background traffic:

- Adobe Creative Cloud
- Pushbullet
- WifiAgent
- TextMate
- Spotify

Q4b. Analysis of internal IITD webpage download after clearing local DNS cache:

- Servers for which a DNS query was launched: 10.10.1.2 or 10.7.174.111
- Number of HTTP requests generated: 60
- Number of TCP connections opened: 7
- Time taken for downloading webpage: ~ 1 second
- No. of TCP losses / retransmits: 0

Wi-Fi [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: dns Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
28	1.327100000	10.192.57.108	10.10.1.2	DNS	77	Standard query 0xce45 A www.iitd.ernet.in
29	1.328318000	10.10.1.2	10.192.57.108	DNS	202	Standard query response 0xce45 A 10.7.174.111

Questions: 1
 Answer RRs: 1
 Authority RRs: 3
 Additional RRs: 3

Queries

- www.iitd.ernet.in: type A, class IN
 - Name: www.iitd.ernet.in
 - [Name Length: 17]
 - [Label Count: 4]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

Answers

- www.iitd.ernet.in: type A, class IN, addr 10.7.174.111

Authoritative nameservers

Additional records

Figure 1: DNS Query

Frame 33: 387 bytes on wire (3096 bits), 387 bytes captured (3096 bits) on interface 0

Interface id: 0 (\Device\NPF_{001ED2DE-98AA-4576-8796-7F979AE9175B})

Encapsulation type: Ethernet (1)

Arrival Time: Aug 28, 2015 11:17:02.900142000 IST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1440740822.900142000 seconds

[Time delta from previous captured frame: 0.000105000 seconds]

[Time delta from previous displayed frame: 0.000105000 seconds]

[Time since reference or first frame: 1.351628000 seconds]

Frame Number: 33

Frame Length: 387 bytes (3096 bits)

Capture Length: 387 bytes (3096 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: LiteonTe_13:73:2f (2c:d0:5a:13:73:2f), Dst: IETF-VRRP-VRID_de (00:00:5e:00:01:de)

Internet Protocol Version 4, Src: 10.192.57.108 (10.192.57.108), Dst: 10.7.174.111 (10.7.174.111)

Transmission Control Protocol, Src Port: 36379 (36379), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 333

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]

[GET / HTTP/1.1\r\n]

[Severity level: Chat]

[Group: Sequence]

Request Method: GET

Request URI: /

Request Version: HTTP/1.1

Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n

Accept-Language: en-US,en;q=0.5\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.10240\r\n

Accept-Encoding: gzip, deflate\r\n

Host: www.iitd.ernet.in\r\n

Connection: Keep-Alive\r\n

\r\n

[Full request URI: http://www.iitd.ernet.in/]

[HTTP request 1/12]

Figure 2: HTTP Get Request

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ Total HTTP Packets	122				0.0563	100%	0.9300	1.954
Other HTTP Packets	2				0.0009	1.64%	0.0100	0.137
▼ HTTP Response Packets	60				0.0277	49.18%	0.4600	1.956
??? : broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
3xx: Redirection	0				0.0000	0.00%	-	-
▼ 2xx: Success	60				0.0277	100.00%	0.4600	1.956
200 OK	60				0.0277	100.00%	0.4600	1.956
1xx: Informational	0				0.0000	0.00%	-	-
▼ HTTP Request Packets	60				0.0277	49.18%	0.4700	1.954
GET	60				0.0277	100.00%	0.4700	1.954

Figure 3: Number of HTTP requests

▼ Frame 35: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0	
Interface id: 0 (\Device\NPF_{001ED2DE-98AA-4576-8796-7F979AE9175B})	
Encapsulation type: Ethernet (1)	
Arrival Time: Aug 28, 2015 11:17:03.491118000 IST	
[Time shift for this packet: 0.000000000 seconds]	
Epoch Time: 1440740823.491118000 seconds	
[Time delta from previous captured frame: 0.589734000 seconds]	
[Time delta from previous displayed frame: 0.589734000 seconds]	
[Time since reference or first frame: 1.942604000 seconds]	
Frame Number: 35	
Frame Length: 1514 bytes (12112 bits)	
Capture Length: 1514 bytes (12112 bits)	
[Frame is marked: False]	
[Frame is ignored: False]	
[Protocols in frame: eth:ethertype:ip:tcp]	
[Coloring Rule Name: HTTP]	
[Coloring Rule String: http tcp.port == 80 http2]	
▶ Ethernet II, Src: Cisco_c4:09:40 (60:73:5c:c4:09:40), Dst: LiteonTe_13:73:2f (2c:d0:5a:13:73:2f)	
▶ Internet Protocol Version 4, Src: 10.7.174.111 (10.7.174.111), Dst: 10.192.57.108 (10.192.57.108)	
▼ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 36379 (36379), Seq: 1, Ack: 334, Len: 1460	
Source Port: 80 (80)	
Destination Port: 36379 (36379)	
[Stream index: 3]	
[TCP Segment Len: 1460]	
Sequence number: 1 (relative sequence number)	
[Next sequence number: 1461 (relative sequence number)]	
Acknowledgment number: 334 (relative ack number)	
Header Length: 20 bytes	
▼ 0000 0001 0000 = Flags: 0x010 (ACK)	
000. = Reserved: Not set	
...0 = Nonce: Not set	
.... 0... = Congestion Window Reduced (CWR): Not set	
.... .0.. = ECN-Echo: Not set	
.... ..0. = Urgent: Not set	
.... ...1 = Acknowledgment: Set	
.... 0... = Push: Not set	
....0.. = Reset: Not set	
....0. = Syn: Not set	

Figure 4: TCP Header

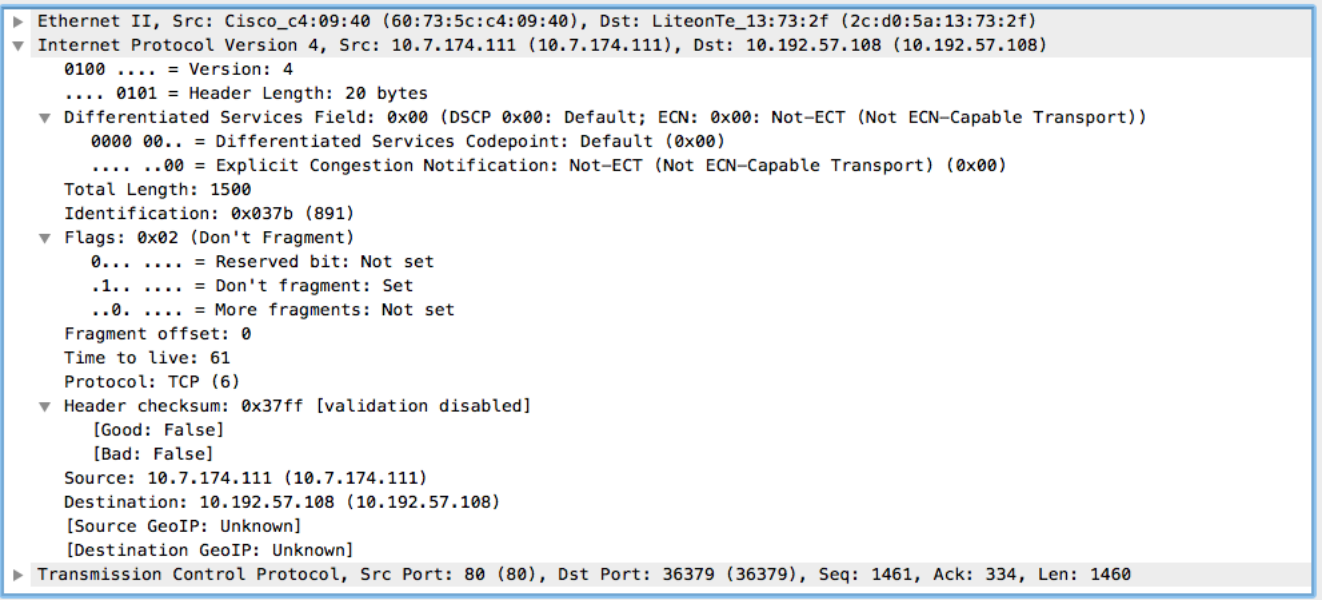


Figure 5: IP Header

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bitz
10.192.57.108	36375	10.10.78.22	3128	13	7399	7	5833	6	1566	0.000000000	1.271626	
10.192.57.108	36373	10.10.78.22	3128	6	3678	3	1015	3	2663	0.001392000	0.135187	
10.192.57.108	36374	10.10.78.22	3128	8	5999	5	5528	3	471	0.009304000	0.008262	
10.192.57.108	36379	10.7.174.111	80	97	90 k	31	7244	66	83 k	1.350219000	0.954628	
10.192.57.108	36380	10.7.174.111	80	68	63 k	24	6114	44	57 k	1.954533000	0.350353	
10.192.57.108	36381	10.7.174.111	80	70	58 k	29	6872	41	51 k	1.954994000	0.348598	
10.192.57.108	36382	10.7.174.111	80	74	75 k	23	4588	51	70 k	1.955863000	0.345287	
10.192.57.108	36383	10.7.174.111	80	125	133 k	33	7190	92	126 k	1.956589000	0.345977	
10.192.57.108	36384	10.7.174.111	80	93	93 k	29	6038	64	87 k	1.957967000	0.345681	
10.192.57.108	36385	10.7.174.111	80	7	1939	4	530	3	1409	2.192992000	0.004020	

Figure 6: TCP Connections