Assignment 1 : Computer Networks (COL 334)

Sukriti Gupta (2016CS50084)
Chinmay Rai (2016CS50615)

Local Network Analysis

a1) Ethernet

```
traceroute to www.iitd.ac.in (10.7.174.111), 30 hops max, 60 byte packets
 1  _gateway (10.208.20.1)  1.063 ms  1.123 ms  1.202 ms
 2  10.254.208.1 (10.254.208.1)  0.923 ms  0.886 ms  0.931 ms
 3  10.254.236.18 (10.254.236.18)  0.603 ms  0.840 ms  1.069 ms
 4  www.iitd.ac.in (10.7.174.111)  0.253 ms  0.242 ms  0.212 ms
```

b1) Ethernet

	1:30pm 9/8/19	4:30pm 9/8/19	8:30pm 9/8/19	12:00am 11/8	Trends
10.208.20.1	_gateway (10.208.20.1) desh.cse.iitd.ernet.in (10.208.20.2) genie.cse.iitd.ernet.in (10.208.20.3) bahar.cse.iitd.ernet.in (10.208.20.4) sri.cse.iitd.ernet.in (10.208.20.5) bhairav.cse.iitd.ernet.in (10.208.20.6) poorvi.cse.iitd.ernet.in (10.208.20.8) palasi.cse.iitd	10.208.20.1 10.208.20.4 10.208.20.5 bhairav.cse.iitd.ernet.in (10.208.20.6) poorvi.cse.iitd.ernet.in (10.208.20.8) palasi.cse.iitd.ernet.in (10.208.20.9) mavi.cse.iitd.ernet.in (10.208.20.10) 10.208.20.13 10.208.20.14 10.208.20.17 smtp.cse.iitd.ernet.in	10.208.20.1 10.208.20.4 10.208.20.5 bhairav.cse.iitd.ernet.in (10.208.20.6) 10.208.20.8 10.208.20.9 10.208.20.10 godfather.cse.iitd.ernet.in (10.208.20.13) licmanager.cse.iitd.ernet.in (10.208.20.14) 10.208.20.17 smtp.cse.iitd.ernet.in (10.208.20.18	10.208.20.1 10.208.20.4 10.208.20.5 bhairav.cse.iitd.ernet.in (10.208.20.6) poorvi.cse.iitd.ernet.in (10.208.20.8) palasi.cse.iitd.ernet.in (10.208.20.9) mavi.cse.iitd.ernet.in (10.208.20.10) godfather.cse.iitd.ernet.in (10.208.20.13) licmanager.cs	This is the output from the GCL ethernet. As we can see some of them like poorvi, bhairav are up all the time while the others go down at different times. The maximum number is up in late evening and the minimum number is at

	.ernet.in (10.208.20.9) mavi.cse.iitd.ernet.in (10.208.20.10) godfather.cse.iitd.ernet.in (10.208.20.13) licmanager.cse.iitd.ernet.in (10.208.20.14) 10.208.20.17 smtp.cse.iitd.ernet.in (10.208.20.18) desh2.cse.iitd.ernet.in (10.208.20.19) poorvinew.cse.iitd.ernet.in (10.208.20.20) sambaad.cse.iitd.ernet.in (10.208.20.40) apc40kvaups1.cse.iitd.ernet.in (10.208.20.42) vsphere.cse.iitd.ernet.in (10.208.20.50	(10.208.20.18) desh2.cse.iitd.ernet.in (10.208.20.19) 10.208.20.43 10.208.20.44 10.208.20.60 10.208.20.100 bmlogs.cse.iitd.ernet.in (10.208.20.101) gamma.cse.iitd.ernet.in (10.208.20.248) 10.208.20.249 10.208.20.250 10.208.20.251 21 hosts are up	) 10.208.20.19 10.208.20.44 10.208.20.133 10.208.20.x 10.208.20.138 10.208.20.139 10.208.20.141 durga.cse.iitd.ernet.in (10.208.20.142) gowla.cse.iitd.ernet.in (10.208.20.143) 10.208.20.156 10.208.20.159 10.208.20.182 10.208.20.217 10.208.20.218 10.208.20.240 26 hosts are up	e.iitd.ernet.in (10.208.20.14) 10.208.20.17 smtp.cse.iitd.ernet.in (10.208.20.18) desh2.cse.iitd.ernet.in (10.208.20.19) sambaad.cse.iitd.ernet.in (10.208.20.40) 10.208.20.43 vsphere.cse.iitd.ernet.in (10.208.20.50) bmlogs.cse.iitd.ernet.in (10.208.20.101) 10.208.20.133 10.208.20.250 10.208.20.251 (19 hosts up)	odd timings like midnight.

	) bmgclserver.cse.iitd.ernet.in (10.208.20.172) gclprinter1.cse.iitd.ernet.in (10.208.20.240) 20 hosts are up				
10.254.208.1	10.254.208.1 10.254.208.2 10.254.208.5 10.254.208.6 (4 hosts up)	10.254.208.1 10.254.208.2 10.254.208.5 10.254.208.6 (4 hosts up)	10.254.208.1 10.254.208.2 10.254.208.5 10.254.208.6 (4 hosts up)	10.254.208.1 10.254.208.2 10.254.208.5 10.254.208.6 (4 hosts up)	These are iitd routers/switches. They are permanently up.
10.254.236.18	10.254.236.9 10.254.236.10 10.254.236.13 10.254.236.14 10.254.236.17 10.254.236.18 10.254.236.21 10.254.236.22 (8 hosts up)	10.254.236.9 10.254.236.10 10.254.236.13 10.254.236.14 10.254.236.17 10.254.236.18 10.254.236.21 10.254.236.22 (8 hosts up)	10.254.236.9 10.254.236.10 10.254.236.13 10.254.236.14 10.254.236.17 10.254.236.18 10.254.236.21 10.254.236.22 (8 hosts up)	10.254.236.9 10.254.236.10 10.254.236.13 10.254.236.14 10.254.236.17 10.254.236.18 10.254.236.21 10.254.236.22 (8 hosts up)	These are iitd network switches. They are permanently up.

10.7.174.111	www.iitd.ac.in (10.7.174.111) 10.7.174.113 (2 hosts up)	(www.iitd.ac.in (10.7.174.111) 10.7.174.113 (2 hosts up)	www.iitd.ac.in (10.7.174.111) 10.7.174.113 (2 hosts up)	www.iitd.ac.in (10.7.174.111) 10.7.174.113 (2 hosts up)	These are the servers on which the iitd website is hosted. Two are up all the time.

c1)Ethernet:

	Transitory Devices	Permanent Devices
10.208.20.1	desh.cse.iitd.ernet.in (10.208.20.2) No exact OS matches for host. The TCP/IP fingerprint was shown genie.cse.iitd.ernet.in (10.208.20.3) No exact OS matches for host. The TCP/IP fingerprint was shown sambaad.cse.iitd.ernet.in (10.208.20.40) No exact OS matches for host. The TCP/IP fingerprint was shown apc40kvaups1.cse.iitd.ernet.in (10.208.20.42) No exact OS matches for host. The TCP/IP fingerprint was shown vsphere.cse.iitd.ernet.in (10.208.20.50) No exact OS matches for host.	10.208.20.1 Aggressive OS guesses: Cisco Catalyst 2950 switch (IOS 12.1) (97%), Cisco ASR 1002 router (97%), Cisco Catalyst 1900, 2820, 2960, 3560, 3750, 4500, or 6513 switch (IOS 12.2) (96%), Cisco uBR10012 broadband router (95%), Cisco Catalyst 2960 switch (IOS 12.2) (95%), Cisco 2960 switch (IOS 12.2) (95%), Cisco IOS 12.4 or IOS-XE 15.3 (94%), Cisco Catalyst 3560 or 6500-series switch (IOS 12.1 - 12.2) (94%), Cisco 7600 router (IOS 12.2) (94%), Cisco 2950, 2960, 3550, 3560, 3750, or 4500 switch or 6500 router (IOS 12.1 - 15.0); or Adaptive Security Appliance firewall (94%) No exact OS matches for host (test conditions non-ideal). 10.208.20.4 No exact OS matches for host. The TCP/IP fingerprint was shown 10.208.20.5 No exact OS matches for host. The TCP/IP fingerprint was shown bhairav.cse.iitd.ernet.in (10.208.20.6) No exact OS matches for host. The TCP/IP fingerprint was shown poorvi.cse.iitd.ernet.in (10.208.20.8) No exact OS matches for host. The TCP/IP fingerprint was shown

	The TCP/IP fingerprint was shown	
10.254.208.1	-	10.254.208.1 Running: Cisco NX-OS 5.X|6.X OS details: Cisco Nexus 7000 switch (NX-OS 5.2(4)), Cisco Nexus switch (NX-OS 6.0(2)) 10.254.208.2 No exact OS matches for host. The TCP/IP fingerprint was shown 10.254.208.5 Running: Cisco NX-OS 5.X|6.X OS details: Cisco Nexus 7000 switch (NX-OS 5.2(4)), Cisco Nexus switch (NX-OS 6.0(2)) 10.254.208.6 No exact OS matches for host. The TCP/IP fingerprint was shown
10.254.236.18	-	10.254.236.9 Running: Cisco NX-OS 5.X|6.X OS details: Cisco Nexus 7000 switch (NX-OS 5.2(4)), Cisco Nexus switch (NX-OS 6.0(2)) 10.254.236.10 Running: Cisco NX-OS 5.X|6.X OS details: Cisco Nexus 7000 switch (NX-OS 5.2(4)), Cisco Nexus switch (NX-OS 6.0(2)) 10.254.236.13 Running: Cisco NX-OS 6.X OS details: Cisco Nexus switch (NX-OS 6.0(2)) 10.254.236.14 Running: Cisco NX-OS 5.X|6.X OS details: Cisco Nexus 7000 switch (NX-OS 5.2(4)), Cisco Nexus switch (NX-OS 6.0(2))

		10.254.236.17 Running: Cisco NX-OS 5.X|6.X OS details: Cisco Nexus 7000 switch (NX-OS 5.2(4)), Cisco Nexus switch (NX-OS 6.0(2))
10.7.174.111	-	No exact OS matches for host for both the servers. The TCP/IP fingerprint was shown

a2) WiFi:

```
traceroute to www.iitd.ac.in (10.7.174.111), 30 hops max, 60 byte packets
 1  10.194.32.14 (10.194.32.14)  1.481 ms  2.163 ms  2.123 ms
 2  10.254.238.5 (10.254.238.5)  2.616 ms  2.576 ms  2.518 ms
 3  10.254.236.14 (10.254.236.14)  3.471 ms  3.448 ms 10.254.236.22 (10.254.236.22)  2.410 ms
 4  www.iitd.ac.in (10.7.174.111)  1.815 ms  1.783 ms  1.727 ms
```

b2) WiFi

	00:30 (8/9)	14:30 (9/8)	16:30 (9/8)	20:30 (9/8)	00:15 (11/8)	14:30 (14/8)
10.194.32.14 The number of devices is very variable. The maximum number of devices seem to be up around afternoon and the least around midnight.	_gateway (10.194.32.1) 10.194.32.2 10.194.32.13 10.194.32.14 (4 hosts up)	_gateway (10.194.32.1) 10.194.32.2 10.194.32.13 10.194.32.14 10.194.32.61 10.194.32.77 10.194.32.89 10.194.32.105 10.194.32.108 10.194.32.117 10.194.32.129 10.194.32.132 10.194.32.142 10.194.32.149 10.194.32.150 10.194.32.186 10.194.32.218 10.194.32.237 10.194.32.252 (19 hosts up)	_gateway (10.194.32.1) 10.194.32.2 10.194.32.13 10.194.32.14 10.194.32.90 10.194.32.92 10.194.32.106 10.194.32.117 10.194.32.127 10.194.32.132 10.194.32.133 10.194.32.138 10.194.32.142 10.194.32.179 10.194.32.188 10.194.32.237 (16 hosts up)	_gateway (10.194.32.1) 10.194.32.2 10.194.32.13 10.194.32.14 10.194.32.77 10.194.32.90 10.194.32.138 (7 hosts up)	_gateway 10.194.32.1 10.194.32.2 10.194.32.13 10.194.32.14 10.194.32.77 10.194.32.90 10.194.32.102 10.194.32.193 (8 hosts up)	_gateway (10.194.32.1) 10.194.32.2 10.194.32.13 10.194.32.14 10.194.32.67 10.194.32.69 10.194.32.70 10.194.32.82 10.194.32.84 10.194.32.89 10.194.32.90 10.194.32.117 10.194.32.150 10.194.32.157 10.194.32.168 (15 hosts up)
10.254.238.5 These are iitd routers/s	10.254.238.1. **Running: Cisco NX-OS 6.X** 10.254.238.2	10.254.238.1 10.254.238.2 10.254.238.5 10.254.238.6 10.254.238.9 10.254.238.10	10.254.238.1 10.254.238.2 10.254.238.5 10.254.238.6 10.254.238.9	10.254.238.1 10.254.238.2 10.254.238.5 10.254.238.6 10.254.238.9	10.254.238.1 10.254.238.2 10.254.238.5 10.254.238.6 10.254.238.9 10.254.238.10	10.254.238.1 10.254.238.2 10.254.238.5 10.254.238.6 10.254.238.9 10.254.238.10

witches. They are permanently up.	10.254.238.5 10.254.238.6 10.254.238.9 10.254.238.10 (6 hosts up)	(6 hosts up)	10.254.238.10 (6 hosts up)	10.254.238.10 (6 hosts up)	(6 hosts up)	
10.254.236.22 10.254.236.14 These are iitd routers/switches. They are permanently up.	10.254.236.9 10.254.236.10 10.254.236.13 10.254.236.14 10.254.236.17 10.254.236.18 10.254.236.21 10.254.236.22 (8 hosts up)	10.254.236.9 10.254.236.10 10.254.236.13 10.254.236.14 10.254.236.17 10.254.236.18 10.254.236.21 10.254.236.22 (8 hosts up)	10.254.236.9 10.254.236.10 10.254.236.13 10.254.236.14 10.254.236.17 10.254.236.18 10.254.236.21 10.254.236.22 (8 hosts up)	10.254.236.9 10.254.236.10 10.254.236.13 10.254.236.14 10.254.236.17 10.254.236.18 10.254.236.21 10.254.236.22 (8 hosts up)	10.254.236.9 10.254.236.10 10.254.236.13 10.254.236.14 10.254.236.17 10.254.236.18 10.254.236.21 10.254.236.22 (8 hosts up)	10.254.236.9 10.254.236.10 10.254.236.13 10.254.236.14 10.254.236.17 10.254.236.18 10.254.236.21 10.254.236.22
10.7.174.111	www.iitd.ac.in (10.7.174.111	www.iitd.ac.in (10.7.174.111) 10.7.174.113	www.iitd.ac.in (10.7.174.111) 10.7.174.113	www.iitd.ac.in (10.7.174.11	www.iitd.ac.in (10.7.174.111) 10.7.174.113	www.iitd.ac.in (10.7.174.111) 10.7.174.113

These are the servers on which the iitd website is hosted. Two are up all the time.	) 10.7.174.113 (2 hosts up)	(2 hosts up)	(2 hosts up)	1) 10.7.174.113 (2 hosts up)	(2 hosts up)	(2 hosts up)

c2)WiFi

	Transitory	Permanent
10.194.32.14	10.194.32.117 All 1000 scanned ports on 10.194.32.117 are closed MAC Address: AC:C1:EE:BE:14:ED (Xiaomi Communications) Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port Device type: general purpose Running: Linux 2.4.X|2.6.X OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6 OS details: Linux 2.4.20, Linux 2.6.14 - 2.6.34, Linux 2.6.17 (Mandriva), Linux 2.6.23, Linux 2.6.24 10.194.32.133	10.194.32.1 Running: Cisco IOS 12.X OS details: Cisco Catalyst 2950 switch (IOS 12.1) 10.194.32.2 Running (JUST GUESSING): Cisco AireOS (88%), Cisco embedded (88%), Asus embedded (87%), Linux 2.6.X (87%) Aggressive OS guesses: Cisco 2500-series Wireless LAN Controller (AireOS) (88%), Cisco Wireless LAN Controller (88%), Asus RT-AC66U router (Linux 2.6) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux 2.6) (87%), Tomato 1.28 (Linux 2.6.22) (87%) No exact OS matches for host (test conditions non-ideal). 10.194.32.13 Running: Cisco IOS 12.X OS details: Cisco Catalyst 2950 switch (IOS 12.1)

	All 1000 scanned ports on 10.194.32.133 are closed MAC Address: C4:0B:CB:6C:A5:8D (Xiaomi Communications) Too many fingerprints match this host to give specific OS details 10.194.32.237 All 1000 scanned ports on 10.194.32.237 are filtered MAC Address: A8:96:75:7D:61:FB (Motorola Mobility, a Lenovo Company) Too many fingerprints match this host to give specific OS details 10.194.32.246 All 1000 scanned ports on 10.194.32.246 are closed MAC Address: 08:25:25:05:C9:A7 (Unknown) Too many fingerprints match this host to give specific OS details 10.194.32.250 Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port Device type: media device|general purpose Running: Asus embedded, Linux 2.6.X	10.194.32.14 Running: Cisco IOS 12.X OS details: Cisco Catalyst 2950 switch (IOS 12.1)

	OS details: Asus O!Play media player (Linux 2.6.12), Linux 2.6.14 - 2.6.34, Linux 2.6.17 (Mandriva), Linux 2.6.22, Linux 2.6.24 - 2.6.28	
10.254.238.5	-	10.254.238.1 Running: Cisco NX-OS 6.X OS details: Cisco Nexus switch (NX-OS 6.0(2)) 10.254.238.2 Running: Cisco IOS 12.X OS details: Cisco Catalyst 2950 switch (IOS 12.1) 10.254.238.5 Running: Cisco NX-OS 5.X|6.X OS details: Cisco Nexus 7000 switch (NX-OS 5.2(4)), Cisco Nexus switch (NX-OS 6.0(2)) 10.254.238.6 Running: Cisco IOS 12.X OS details: Cisco Catalyst 2950 switch (IOS 12.1) 10.254.238.9 Aggressive OS guesses: Cisco Catalyst 2950 switch (IOS 12.1) (98%), Cisco ASR 1002 router (98%), Cisco Catalyst 2960, 3560, or 6500 switch (IOS 12.2) (95%), Cisco Catalyst 3560 or 6500-series switch (IOS 12.1 - 12.2) (95%), Cisco 7600 router (IOS 12.2) (95%), Cisco 2950, 2960, 3550, 3560, 3750, or 4500 switch or 6500 router (IOS 12.1 - 15.0); or Adaptive Security Appliance firewall (95%), Cisco C7200 router (IOS 15.2) (95%), Cisco 3550 switch (IOS 12.1) (95%), Cisco IOS 12.4 or IOS-XE 15.3 (95%), Cisco 860 or 870 router (IOS 12.4) (94%)

		No exact OS matches for host (test conditions non-ideal).
10.254.236.22 10.254.236.14	-	10.254.236.9 Running: Cisco NX-OS 5.X|6.X OS details: Cisco Nexus 7000 switch (NX-OS 5.2(4)), Cisco Nexus switch (NX-OS 6.0(2)) 10.254.236.10 Running: Cisco NX-OS 5.X|6.X OS details: Cisco Nexus 7000 switch (NX-OS 5.2(4)), Cisco Nexus switch (NX-OS 6.0(2)) 10.254.236.13 Running: Cisco NX-OS 6.X OS details: Cisco Nexus switch (NX-OS 6.0(2)) 10.254.236.14 Running: Cisco NX-OS 5.X|6.X OS details: Cisco Nexus 7000 switch (NX-OS 5.2(4)), Cisco Nexus switch (NX-OS 6.0(2)) 10.254.236.17 Running: Cisco NX-OS 5.X|6.X OS details: Cisco Nexus 7000 switch (NX-OS 5.2(4)), Cisco Nexus switch (NX-OS 6.0(2))
10.7.174.111	-	No exact OS matches for host for both the servers. The TCP/IP fingerprint was shown

Internet Architecture

IP address

	www.uwaterloo.ca	www.uct.ac.za	www.iitd.ac.in	www.google.com	www.facebook.com
Germany: http://www.han.de/cgi-bin/nph-trace.cgi	129.97.208.23	137.158.154.230	103.27.9.20	216.58.208.36	31.13.92.36
Atlanta (US) (http://www.cogentco.com/en/network/looking-glass)	129.97.208.23	137.158.154.230	103.27.9.20	172.217.7.196	31.13.65.36
KINX Seoul (http://www.lg.he.net/)	129.97.208.23	137.158.154.230	103.27.9.20	172.217.0.36	157.240.22.35
Mobile Network	129.97.208.23	137.158.154.230	103.27.9.20	172.217.167.4	157.240.198.35

No. of Hops and Latencies

	www.uwaterloo.ca		www.uct.ac.za		www.iitd.ac.in		www.google.com		www.facebook.com	
	Hop	Latency (ms)	Hop	Latency	Hop	Latency	Hop	Latency	Hop	Latency
Germany: http://www.han.de/cgi-bin/nph-trace.cgi	17	99.577	14	153.236	30	NA***	8	4.021	10	3.679
Atlanta (US) (http://www.cogentco.com/en/network/looking-glass)	13	33.704	15	238.840	30	NA***	14	17.975	8	0.948

KINX Seoul (http://www.lg.he.net/)	12	170	15	338	16	261	11	133	8	130
Mobile Network	15	409.678	17	409.678	Max Hops Limit (64) : Exceeded	NA	9	46.365	9	43.061

Whois Analysis:

1) Traceroute from KINX Seoul (http://www.lg.he.net/) to www.iitd.ac.in:

100ge6-1.core1.sjc2.he.net (72.52.92.58)	California - Fremont - Hurricane Electric Llc
100ge10-2.core1.nyc4.he.net (184.105.81.217)	California - Fremont - Hurricane Electric Llc
100ge8-1.core1.nyc6.he.net (184.105.64.178)	United States New York City Hurricane Electric
peer1.nyc6.flagtel.com (198.32.160.88)	United States New York City Telehouse Intml.
xe-2-0-3.0.pjr03.ldn001.flagtel.com (85.95.25.82)	United Kingdom London Reliance Globalcom
xe-0-0-1.0.pjr03.mmb004.flagtel.com (85.95.26.234)	India Mumbai Reliance Globalcom
62.216.147.78	Reliance Globalcom Limited, Mumbai
*	
115.248.54.101	Reliance Infocom Ltd., Mumbai
10.152.7.37	Indian Institute of Technology Delhi
*	
*	
*	
*	
103.27.9.20	Indian Institute of Technology Delhi
103.27.9.20	Indian Institute of Technology Delhi
103.27.9.20	Indian Institute of Technology Delhi

2) Traceroute from Atlanta(US)(http://www.cogentco.com/en/network/looking-glass) to www.uct.ac.za :

gi0-0-1-7.3500.agr22.atl01.atlas.cogentco.com (66.28.3.233)	Cogent Communications Atlanta
be3373.ccr42.atl01.atlas.cogentco.com (154.54.44.77)	Cogent Communications Atlanta
be2113.ccr42.dca01.atlas.cogentco.com (154.54.24.221)	Cogent Communications Atlanta
be2806.ccr41.jfk02.atlas.cogentco.com (154.54.40.105)	Cogent Communications NY City
be2807.ccr42.jfk02.atlas.cogentco.com (154.54.40.109)	Cogent Communications NY City
be2490.ccr42.lon13.atlas.cogentco.com (154.54.42.86)	Cogent Communications NY City
be2870.ccr22.lon01.atlas.cogentco.com (154.54.58.174)	Cogent Communication London
be2186.rcr21.b015534-1.lon01.atlas.cogentco.com (154.54.61.69)	Cogent Communication DC
tenet.demarc.cogentco.com (149.14.146.194)	Cogent Communication London
ae1-1001-cpt1-ir1.net.tenet.ac.za (155.232.1.82)	Tenet, Mtunzini, South Africa
be1-cpt1-pe1.net.tenet.ac.za (155.232.64.69)	Tenet, Ellisras, South Africa
155.232.32.14 (155.232.32.14)	Tenet, Cape Town, South Africa
137.158.248.97 (137.158.248.97)	Tenet, Cape Town, South Africa
10.1.23.42 (10.1.23.42) 10.1.23.34 (10.1.23.34)	NA
137.158.154.1 (137.158.154.1)	Tenet, Cape Town, South Africa
ecm-vip-prd.uct.ac.za (137.158.154.230)	Tenet, Cape Town, South Africa

3) Traceroute from Mobile Hotspot (Airtel 4G) to www.uwaterloo.ca :

192.168.43.1	Bharti Airtel Ltd. Delhi
10.0.232.4	NA
*	
10.206.30.205	NA
125.17.210.37	Bharti Infotel Ltd. Bangalore
182.79.222.237	Bharti Infotel Ltd. Delhi
206.82.104.25	DE-CIX North America Inc. New York City
10.10.0.89	
74.123.93.154	Zerofail, Montreal, Canada
172.16.31.110	NA
172.16.16.65	NA
172.16.16.7	NA
172.16.16.27	NA
129.97.208.23	University of Waterloo, Waterloo
129.97.208.23	University of Waterloo, Waterloo

Thus we can conclude from the above analysis that the traffic first gets into the local ISPs like Airtel in India, Hurricane Electric & Cogent Communications in the US. Thereafter it transits across the continents. ISPs like Reliance, Tenet provide inter-continental connections . Finally the traffic reaches the location of web server using local ISP's of that location, eg: Zerofail, Tenet, Reliance.

a) Google and facebook have consistently lower number of hops than the others. They would have peered with the local ISPs of various countries, mirroring their websites in multiple places for fast access. The other option (for smaller organisations) can be CDNs like fastly to have their websites hosted across the world. It takes significantly lesser number of hops to reach the uwaterloo website from the US as compared to Germany due to the large physical distance between the two.

b) The latency does seem to be related to the number of hops, though a direct proportionality does not exist. This is probably due to the fact that even if two data packets take the exact same route, due to the unbounded delay nature of the internet, it may take very different times for the packets to traverse their paths.

c) The webservers of uwaterloo, uct and iitd resolve to the same ip addresses. Google and facebook are resolved to different ip addresses. There are two reasons for this. One, since big companies have their websites hosted at multiple data centres, it is attempted that the closest ip is returned. Therefore, queries from different continents often resolve to different ip addresses. Second, even for a single location, there are usually multiple ip addresses, which are resolved in a round-robin fashion for load balancing.

d) www.google.com was resolved to two different IP's when using two different traceroute servers:

4G India routes wwww.google.com to 172.217.167.4 (Netherlands)
While US (Atlanta) routes www.google.com to 172.217.7.196.

It takes almost 13ms from US Atlanta to 172.217.7.196 (US Atlanta to www.google.com)

```
1  gi0-0-1-7.3500.agr22.atl01.atlas.cogentco.com (66.28.3.233)  0.656 ms  0.727 ms
 2  be3371.ccr41.atl01.atlas.cogentco.com (154.54.29.121)  0.570 ms  0.713 ms
 3  be2847.ccr41.atl04.atlas.cogentco.com (154.54.6.102)  0.704 ms  0.704 ms
 4  tata.atl04.atlas.cogentco.com (154.54.11.226)  0.461 ms  0.471 ms
 5  if-ae-43-2.tcore1.a56-atlanta.as6453.net (64.86.113.149)  1.060 ms  0.670 ms
 6  209.85.173.168 (209.85.173.168)  0.667 ms  0.859 ms
 7  108.170.249.44 (108.170.249.44)  1.530 ms 108.170.249.35 (108.170.249.35)  1.434 ms
 8  209.85.248.247 (209.85.248.247)  1.707 ms 108.170.236.128 (108.170.236.128)  4.587 ms
 9  216.239.40.131 (216.239.40.131)  14.497 ms 216.239.40.133 (216.239.40.133)  15.348 ms
10  216.239.48.3 (216.239.48.3)  15.436 ms 216.239.48.7 (216.239.48.7)  17.745 ms
```

```
11  209.85.244.166 (209.85.244.166)  14.375 ms 209.85.240.62 (209.85.240.62)  32.718 ms
12  108.170.240.97 (108.170.240.97)  15.119 ms  15.123 ms
13  216.239.54.107 (216.239.54.107)  13.821 ms  13.792 ms
14  iad30s10-in-f196.1e100.net (172.217.7.196)  13.839 ms  13.836 ms
```

Tracerouting from US Atlanta to 172.217.167.4 gives us:

```
1  gi0-0-1-7.3500.agr22.atl01.atlas.cogentco.com (66.28.3.233)  0.575 ms  0.593 ms
2  be3371.ccr41.atl01.atlas.cogentco.com (154.54.29.121)  0.485 ms
be3373.ccr42.atl01.atlas.cogentco.com (154.54.44.77)  0.699 ms
3  be2847.ccr41.atl04.atlas.cogentco.com (154.54.6.102)  0.944 ms
be2848.ccr41.atl04.atlas.cogentco.com (154.54.6.118)  0.995 ms
 4  tata.atl04.atlas.cogentco.com (154.54.11.226)  2.029 ms  0.445 ms
 5  if-ae-43-2.tcore1.a56-atlanta.as6453.net (64.86.113.149)  0.751 ms  0.747 ms
 6  64.86.113.106 (64.86.113.106)  0.491 ms  0.513 ms
 7  108.170.249.98 (108.170.249.98)  0.898 ms 108.170.249.108 (108.170.249.108)  1.470 ms
 8  64.233.175.251 (64.233.175.251)  2.669 ms 216.239.59.153 (216.239.59.153)  1.589 ms
 9  209.85.240.16 (209.85.240.16)  26.026 ms  26.018 ms
10  72.14.237.135 (72.14.237.135)  35.506 ms  35.488 ms
11  74.125.37.83 (74.125.37.83)  68.036 ms  68.038 ms
12  108.170.235.221 (108.170.235.221)  157.184 ms 108.170.236.119 (108.170.236.119)
153.281 ms
13  66.249.94.141 (66.249.94.141)  218.035 ms 216.239.63.97 (216.239.63.97)  222.934 ms
14  74.125.251.156 (74.125.251.156)  252.698 ms 72.14.233.122 (72.14.233.122)  249.294 ms
15  172.253.68.94 (172.253.68.94)  290.757 ms  288.627 ms
16  108.170.251.113 (108.170.251.113)  294.398 ms  292.353 ms
17  72.14.233.31 (72.14.233.31)  290.563 ms  290.523 ms
18  del03s15-in-f4.1e100.net (172.217.167.4)  293.064 ms  295.311 ms
```

As we can see, the latency is significantly higher and so are the number of hops. The path is very different and longer when we route from the US to Google's server in the Netherlands. Using the whois service, we get to know that US Atlanta routes to Google Mountain View server in the US which is closer than the Netherlands.

e) Google and facebook seems to have peered with a lot of ISPs around the world. We routed from: https://www.locaping.com/

Country	Hops to www.google.com	Latency shown (ms) www.google.com	Hops www.facebook.com	Latency shown www.facebook.com
Amsterdam, North Holland, Netherlands	11	22.846	10	12.125
Dallas, Texas, United States	7	1.072	7	0.978
Frankfurt, Hesse, Germany	6	1.102	7	0.446
Hong Kong	7	2.346	8	3.273
London, England, United Kingdom	7	0.866	8	1.784
Madrid, Spain	6	8.496	9	33.322
Milan, Lombardia, Italy	8	0.350	12	10.03
Montreal, Quebec, Canada	9	1.29	11	10.250
Moscow, Moscow City, Russian Federation	12	46.754	9	53.67
Paris, Île-de-France, France	15	9.310	11	9.131
Singapore	17	1.956	8	0.833
Stockholm, Stockholms Lan, Sweden	7	0.777	10	21.475
Tokyo, Kanto, Japan	7	1.262	11	51.502

traceroute www.facebook.com from Tokyo Japan

```
traceroute to 157.240.15.35 (157.240.15.35), 20 hops max, 60 byte packets
1 50.31.252.1.static.vps.net (50.31.252.1)
2 0.ge-1-0-2.cr1.tko1.scnet.net (75.102.60.17)
3 SRV-0001.10026.telstraglobal.net (203.192.150.81)
4 202.47.216.145 (202.47.216.145)
5 i-15657.hkck-core01.telstraglobal.net
6 202.84.153.26 (202.84.153.26)
7 134.159.205.242 (134.159.205.242)
8 po141.asw03.hkg3.tfbnw.net (74.119.76.218)
9 po216.psw04.hkg3.tfbnw.net (157.240.52.151)
10 157.240.39.93 (157.240.39.93)
11 edge-star-mini-shv-02-hkg3.facebook.com (157.240.15.35)
```

Since we can see that the traceroute goes through HongKong, that implies that the local ISP in Japan has not peered with facebook.

f) The latency for cellular networks is surprisingly high. Especially in the case of servers of the university servers. Google and Facebook servers are comparatively easy to reach probably because of the presence of CDN or ISP peering. The largest contributor to the latency is the initial set of nodes, which signify the local ISP’s network. This indicates congestion in the network of our local ISP.

g) We find that routes to frequently visited websites like facebook and google are quicker and shorter than those of University websites. This indicates that our ISP tries to establish faster links with servers which host frequently accessed data, by means of Content Distribution Network (CDN) or peering.

Packet analysis

3a)

i)

Time	Source	Destination	Protocol	Length	Info.
17.571461	10.194.44.216	10.10.2.2	DNS	85	Standard query 0xe2ac A www.iitd.ac.in OPT
17.571578	10.194.44.216	10.10.2.2	DNS	85	Standard query 0x4fe6 AAAA www.iitd.ac.in OPT
17.574680	10.10.2.2	10.194.44.216	DNS	138	Standard query response 0x4fe6 AAAA www.iitd.ac.in SOA intdns.iitd.ac.in OPT
17.574698	10.10.2.2	10.194.44.216	DNS	101	Standard query response 0xe2ac A www.iitd.ac.in A 10.7.174.111 OPT

Time taken :

A type query : 3.237159 ms AAAA type query : 3.10255 ms

ii) Almost 82 http request-response pairs were observed as the page was rendered. By looking at the chronological ordering of different types of content we can say that webpages are structured in such a way that first a basic layout is rendered after which details like images are filled in. First the html is fetched and parsed, after which the styling attributes are fetched from css, followed by application/javascript code after which images are fetched.

iii) The filter we applied was:

((ip.src==10.194.44.216 && ip.dst==10.7.174.111) ||
(ip.src==10.7.174.111 && ip.dst==10.194.44.216)) && tcp

We found that 6 tcp channels were opened between our browser and the webserver. We were able to identify this by observing (SYN, SYN/ACK, ACK) handshakes that happened on channels with different port numbers. We also noticed that these channels were opened in the initial phase of downloading the page after which each of there were being extensively used to transfer various kinds of content. This also indicates that the browser tries to optimize the download time by using multiple tcp channels for fetching data. Also using the same channels helps save the 1.5 RTT required to setup a TCP connection iv)

Time	Source	Destination	Protocol	Information
18.601281	10.194.44.216	10.10.1.2	DNS	Standard query www.iitd.ac.in OPT
20.281667	10.7.174.111	10.194.44.216	HTTP	HTTP/1.1 200 OK (image/x-icon)

It took 1.680385986 seconds to load the entire page, right from the DNS query to the last content-based response.

v) When we tried to look into the packets exchanged while accessing www.indianexpress.com , we found that there were very few requests which had “http” as there protocol. Moreover it was interesting to find that their content was also forbidden for us to see.
We instead found a lot of requests-response pairs of “OCSP” protocol, which is related to digital certificates. This suggests that there is some kind of encryption of data taking place.
Javascript is not mentioned specifically. We do see application data which is encrypted

On the other hand, we were able to see the entire packet data for iitd.ac.in: The html request could be directly used to get the entire html code of the webpage and javascript code can also be extracted.