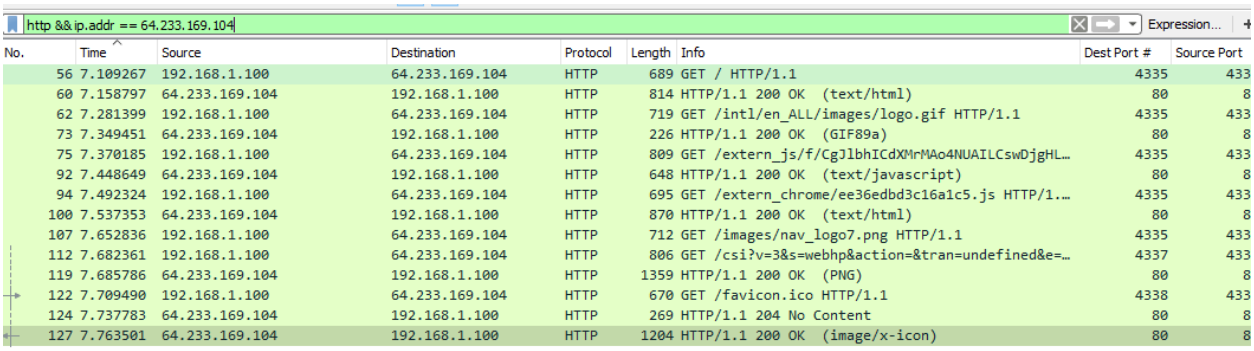
Christopher Desir

No.	Time	Source	Destination	Protocol	Length	Info
1	2009-09-20 16:43:00.269135	192.168.1.100	10.119.240.64	SNMP	120	get-request 1.3.6…
2	2009-09-20 16:43:01.394032	192.168.1.100	68.87.71.230	DNS	91	Standard query 0x…
3	2009-09-20 16:43:01.407400	68.87.71.230	192.168.1.100	DNS	211	Standard query re…
4	2009-09-20 16:43:01.409437	192.168.1.100	74.125.91.113	TCP	66	4330 → 80 [SYN] S…
5	2009-09-20 16:43:01.476953	74.125.91.113	192.168.1.100	TCP	66	80 → 4330 [SYN, A…
6	2009-09-20 16:43:01.477008	192.168.1.100	74.125.91.113	TCP	54	4330 → 80 [ACK] S…
7	2009-09-20 16:43:01.477175	192.168.1.100	74.125.91.113	HTTP	1035	POST /safebrowsin…
8	2009-09-20 16:43:01.528505	Cisco-Li_45:1f:1b	HonHaiPr_0d:ca:8f	ARP	60	Who has 192.168.1…
9	2009-09-20 16:43:01.528522	HonHaiPr_0d:ca:8f	Cisco-Li_45:1f:1b	ARP	42	192.168.1.100 is …
10	2009-09-20 16:43:01.538810	74.125.91.113	192.168.1.100	TCP	60	80 → 4330 [ACK] S…

1. 192.168.1.249



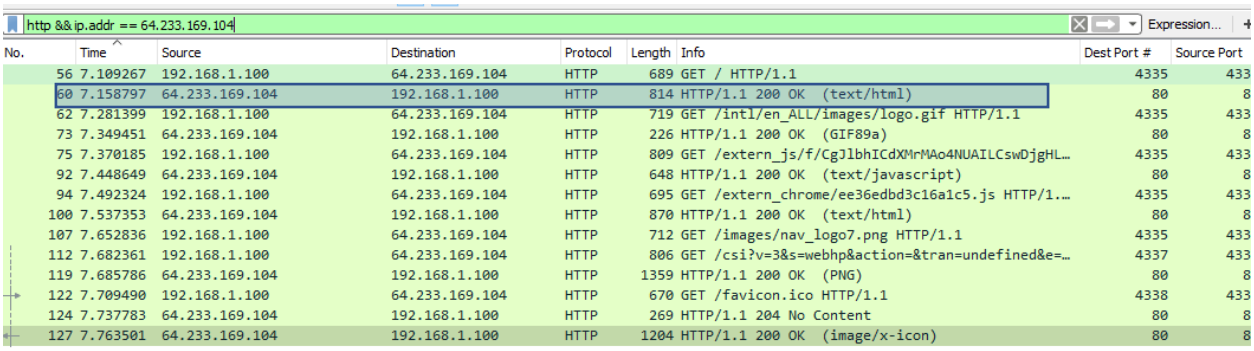
No.	Time	Source	Destination	Protocol	Length	Info	Dest Port #	Source Port
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1	4335	433
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)	80	8
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1	4335	433
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a)	80	8
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHL…	4335	433
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascript)	80	8
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.…	4335	433
100	7.537353	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK (text/html)	80	8
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7.png HTTP/1.1	4335	433
112	7.682361	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=webhp&action=&tran=undefined&e=…	4337	433
119	7.685786	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK (PNG)	80	8
122	7.709490	192.168.1.100	64.233.169.104	HTTP	670	GET /favicon.ico HTTP/1.1	4338	433
124	7.737783	64.233.169.104	192.168.1.100	HTTP	269	HTTP/1.1 204 No Content	80	8
127	7.763501	64.233.169.104	192.168.1.100	HTTP	1204	HTTP/1.1 200 OK (image/x-icon)	80	8

2.

3. Source is 192.168.1.100 Port 4334, Destination is 64.233.169.104 80

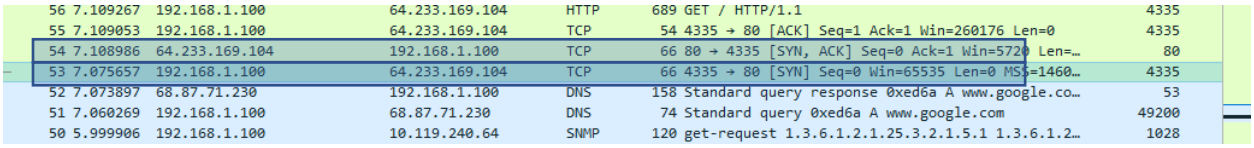
128	7.763537	192.168.1.100	64.233.169.104	TCP	54 4338 → 80 [ACK] Seq=617 Ack=1409 Win=258768 Le…
129	7.811354	192.168.1.100	74.125.91.113	TCP	54 4336 → 80 [ACK] Seq=656 Ack=126 Win=260048 Len…
130	7.811374	192.168.1.100	64.233.169.104	TCP	54 4335 → 80 [ACK] Seq=3355 Ack=36558 Win=258868 …
131	7.911938	192.168.1.100	64.233.169.104	TCP	54 4337 → 80 [ACK] Seq=753 Ack=216 Win=259960 Len…
132	12.005621	192.168.1.100	68.87.71.230	DNS	79 Standard query 0xcdc8 A anise.nsm.umass.edu

4.



No.	Time	Source	Destination	Protocol	Length	Info	Dest Port #	Source Port
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1	4335	433
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)	80	8
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1	4335	433
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a)	80	8
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHL…	4335	433
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascript)	80	8
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.…	4335	433
100	7.537353	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK (text/html)	80	8
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7.png HTTP/1.1	4335	433
112	7.682361	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=webhp&action=&tran=undefined&e=…	4337	433
119	7.685786	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK (PNG)	80	8
122	7.709490	192.168.1.100	64.233.169.104	HTTP	670	GET /favicon.ico HTTP/1.1	4338	433
124	7.737783	64.233.169.104	192.168.1.100	HTTP	269	HTTP/1.1 204 No Content	80	8
127	7.763501	64.233.169.104	192.168.1.100	HTTP	1204	HTTP/1.1 200 OK (image/x-icon)	80	8

Source is 64.233.169.104 Port 80, Destination is 192.168.100 Port 4335

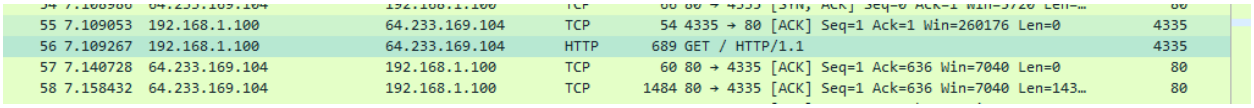


56	7.109267	192.168.1.100	64.233.169.104	HTTP	689 GET / HTTP/1.1	4335
55	7.109053	192.168.1.100	64.233.169.104	TCP	54 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0	4335
54	7.108986	64.233.169.104	192.168.1.100	TCP	66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=…	80
53	7.075657	192.168.1.100	64.233.169.104	TCP	66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460…	4335
52	7.073897	68.87.71.230	192.168.1.100	DNS	158 Standard query response 0xed6a A www.google.co…	53
51	7.060269	192.168.1.100	68.87.71.230	DNS	74 Standard query 0xed6a A www.google.com	49200
50	5.999906	192.168.1.100	10.119.240.64	SNMP	120 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2…	1028

5) SYN : Time: 7.075657 Source is 192.168.1.100 Port 4335, Destination is 64.233.169.104 Port 80.

ACK: Time: 7.108986, Source is 64.233.169.104 Port 80 Destination is 192.168.1.100 Port 4335

6)



55	7.109053	192.168.1.100	64.233.169.104	TCP	54 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0	4335
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689 GET / HTTP/1.1	4335
57	7.140728	64.233.169.104	192.168.1.100	TCP	60 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0	80
58	7.158432	64.233.169.104	192.168.1.100	TCP	1484 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=143…	80

Source for GET Request 71.192.34.104 Port 4335 Destination Is 64.233.169.104 Port 80. What changed was the source IP.

7)No, No, No, No, Yes. The value of the check will change when the source IP changes.

8) Source IP is 64.233.169.104 Port 80 Destination: is 71.192.34.104 port 4335 . What changed was the Destination IP.

9) ?

10)

NAT Table

WAN	Lan
71.192.34.104 at Port 4335	192.168.1.100 at Port 4335