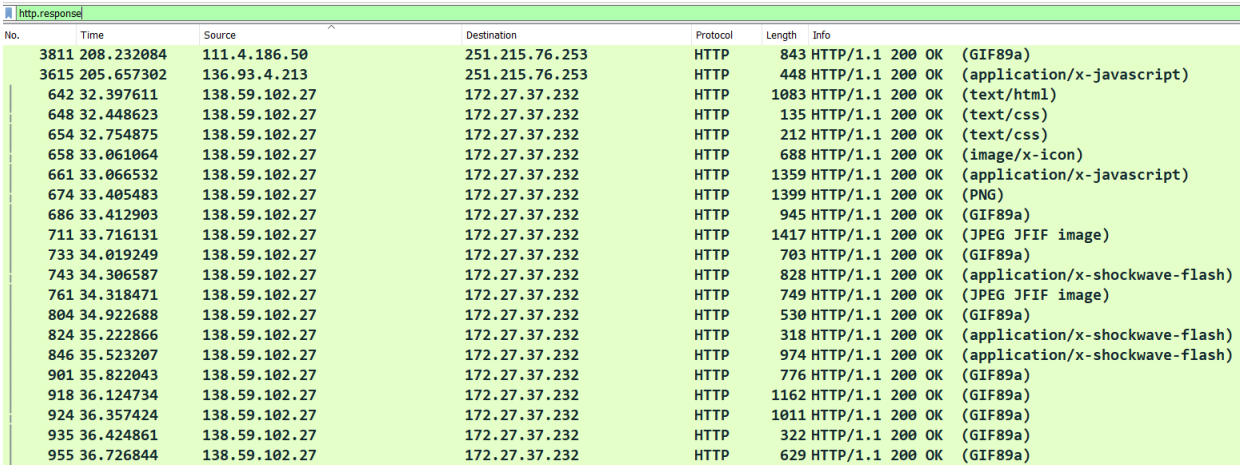
Part1:

1. Command: http.response



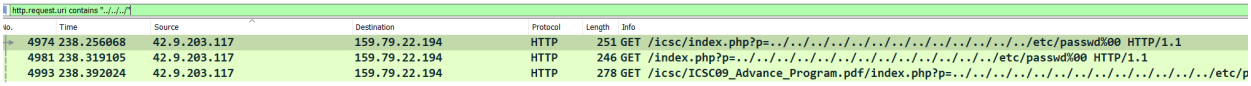
No.	Time	Source	Destination	Protocol	Length	Info
3811	208.232084	111.4.186.50	251.215.76.253	HTTP	843	HTTP/1.1 200 OK (GIF89a)
3615	205.657302	136.93.4.213	251.215.76.253	HTTP	448	HTTP/1.1 200 OK (application/x-javascript)
642	32.397611	138.59.102.27	172.27.37.232	HTTP	1083	HTTP/1.1 200 OK (text/html)
648	32.448623	138.59.102.27	172.27.37.232	HTTP	135	HTTP/1.1 200 OK (text/css)
654	32.754875	138.59.102.27	172.27.37.232	HTTP	212	HTTP/1.1 200 OK (text/css)
658	33.061064	138.59.102.27	172.27.37.232	HTTP	688	HTTP/1.1 200 OK (image/x-icon)
661	33.066532	138.59.102.27	172.27.37.232	HTTP	1359	HTTP/1.1 200 OK (application/x-javascript)
674	33.405483	138.59.102.27	172.27.37.232	HTTP	1399	HTTP/1.1 200 OK (PNG)
686	33.412903	138.59.102.27	172.27.37.232	HTTP	945	HTTP/1.1 200 OK (GIF89a)
711	33.716131	138.59.102.27	172.27.37.232	HTTP	1417	HTTP/1.1 200 OK (JPEG JFIF image)
733	34.019249	138.59.102.27	172.27.37.232	HTTP	703	HTTP/1.1 200 OK (GIF89a)
743	34.306587	138.59.102.27	172.27.37.232	HTTP	828	HTTP/1.1 200 OK (application/x-shockwave-flash)
761	34.318471	138.59.102.27	172.27.37.232	HTTP	749	HTTP/1.1 200 OK (JPEG JFIF image)
804	34.922688	138.59.102.27	172.27.37.232	HTTP	530	HTTP/1.1 200 OK (GIF89a)
824	35.222866	138.59.102.27	172.27.37.232	HTTP	318	HTTP/1.1 200 OK (application/x-shockwave-flash)
846	35.523207	138.59.102.27	172.27.37.232	HTTP	974	HTTP/1.1 200 OK (application/x-shockwave-flash)
901	35.822043	138.59.102.27	172.27.37.232	HTTP	776	HTTP/1.1 200 OK (GIF89a)
918	36.124734	138.59.102.27	172.27.37.232	HTTP	1162	HTTP/1.1 200 OK (GIF89a)
924	36.357424	138.59.102.27	172.27.37.232	HTTP	1011	HTTP/1.1 200 OK (GIF89a)
935	36.424861	138.59.102.27	172.27.37.232	HTTP	322	HTTP/1.1 200 OK (GIF89a)
955	36.726844	138.59.102.27	172.27.37.232	HTTP	629	HTTP/1.1 200 OK (GIF89a)

Result:

111.4.186.50	136.93.4.213	138.59.102.27	142.165.192.177	142.165.192.188
143.138.4.147	143.138.66.97	143.179.11.189	154.27.68.55	154.87.109.177
154.87.109.40	155.111.186.252	155.231.237.70	159.70.229.173	159.79.22.194
159.79.22.198	159.79.22.249	205.232.201.218	205.232.203.30	205.234.49.157
248.78.109.66	251.235.172.148	33.247.152.101	33.247.152.113	34.30.235.180
35.183.215.204	37.120.175.85	37.199.226.67	40.187.57.142	44.111.85.82
44.131.48.102	44.131.51.161	44.131.51.48	93.119.134.44	93.199.112.45
97.145.19.119				

The result shows all the IP addresses of servers that made HTTP responses.

2. Command: http.request.uri contains “../../../”

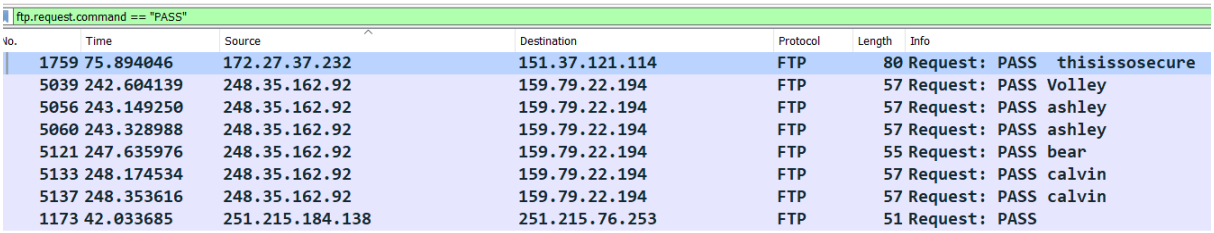


No.	Time	Source	Destination	Protocol	Length	Info
4974	238.256068	42.9.203.117	159.79.22.194	HTTP	251	GET /icsc/index.php?p=../../../../../../../../../../../../etc/passwd%00 HTTP/1.1
4981	238.319105	42.9.203.117	159.79.22.194	HTTP	246	GET /index.php?p=../../../../../../../../../../../../etc/passwd%00 HTTP/1.1
4993	238.392024	42.9.203.117	159.79.22.194	HTTP	278	GET /icsc/ICSC09_Advance_Program.pdf/index.php?p=../../../../../../../../../../../../etc/p

Result: 42.9.203.117

The IP address is the very host that made this type of attack.

3. Command: ftp.request.command == “PASS”



No.	Time	Source	Destination	Protocol	Length	Info
1759	75.894046	172.27.37.232	151.37.121.114	FTP	80	Request: PASS thisissosecure
5039	242.604139	248.35.162.92	159.79.22.194	FTP	57	Request: PASS Volley
5056	243.149250	248.35.162.92	159.79.22.194	FTP	57	Request: PASS ashley
5060	243.328988	248.35.162.92	159.79.22.194	FTP	57	Request: PASS ashley
5121	247.635976	248.35.162.92	159.79.22.194	FTP	55	Request: PASS bear
5133	248.174534	248.35.162.92	159.79.22.194	FTP	57	Request: PASS calvin
5137	248.353616	248.35.162.92	159.79.22.194	FTP	57	Request: PASS calvin
1173	42.033685	251.215.184.138	251.215.76.253	FTP	51	Request: PASS

Result:

251.215.184.138 PASS

172.27.37.232 PASS thisissosecure

248.35.162.92 PASS Volley

248.35.162.92 PASS ashley

248.35.162.92 PASS ashley

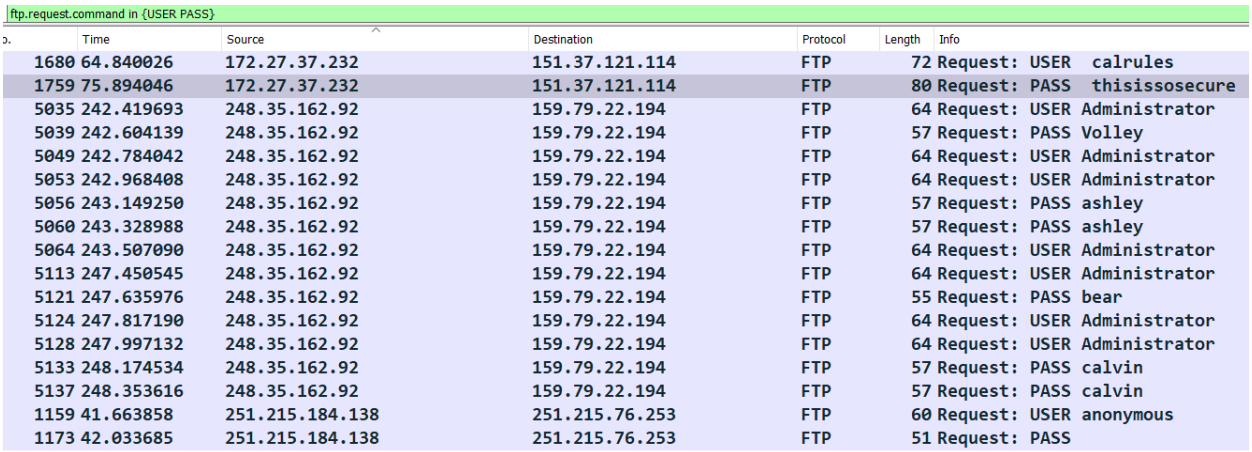
248.35.162.92 PASS bear

248.35.162.92 PASS calvin

248.35.162.92 PASS calvin

By observation, the host with 248.35.162.92 continued guessing the password.

4. Command: ftp.request.command in {USER PASS}



ftp.request.command in {USER PASS}

No.	Time	Source	Destination	Protocol	Length	Info
1680	64.840026	172.27.37.232	151.37.121.114	FTP	72	Request: USER calrules
1759	75.894046	172.27.37.232	151.37.121.114	FTP	80	Request: PASS thisissosecure
5035	242.419693	248.35.162.92	159.79.22.194	FTP	64	Request: USER Administrator
5039	242.604139	248.35.162.92	159.79.22.194	FTP	57	Request: PASS Volley
5049	242.784042	248.35.162.92	159.79.22.194	FTP	64	Request: USER Administrator
5053	242.968408	248.35.162.92	159.79.22.194	FTP	64	Request: USER Administrator
5056	243.149250	248.35.162.92	159.79.22.194	FTP	57	Request: PASS ashley
5060	243.328988	248.35.162.92	159.79.22.194	FTP	57	Request: PASS ashley
5064	243.507090	248.35.162.92	159.79.22.194	FTP	64	Request: USER Administrator
5113	247.450545	248.35.162.92	159.79.22.194	FTP	64	Request: USER Administrator
5121	247.635976	248.35.162.92	159.79.22.194	FTP	55	Request: PASS bear
5124	247.817190	248.35.162.92	159.79.22.194	FTP	64	Request: USER Administrator
5128	247.997132	248.35.162.92	159.79.22.194	FTP	64	Request: USER Administrator
5133	248.174534	248.35.162.92	159.79.22.194	FTP	57	Request: PASS calvin
5137	248.353616	248.35.162.92	159.79.22.194	FTP	57	Request: PASS calvin
1159	41.663858	251.215.184.138	251.215.76.253	FTP	60	Request: USER anonymous
1173	42.033685	251.215.184.138	251.215.76.253	FTP	51	Request: PASS

Result:

251.215.184.138 251.215.76.253 USER anonymous	251.215.184.138 251.215.76.253 PASS
172.27.37.232 151.37.121.114 USER calrules	172.27.37.232 151.37.121.114 PASS thisissosecure
248.35.162.92 159.79.22.194 USER Administrator	248.35.162.92 159.79.22.194 PASS Volley
248.35.162.92 159.79.22.194 USER Administrator	248.35.162.92 159.79.22.194 USER Administrator
248.35.162.92 159.79.22.194 PASS ashley	248.35.162.92 159.79.22.194 PASS ashley
248.35.162.92 159.79.22.194 USER Administrator	248.35.162.92 159.79.22.194 USER Administrator
248.35.162.92 159.79.22.194 PASS bear	248.35.162.92 159.79.22.194 USER Administrator
248.35.162.92 159.79.22.194 USER Administrator	248.35.162.92 159.79.22.194 PASS calvin
248.35.162.92 159.79.22.194 PASS calvin	

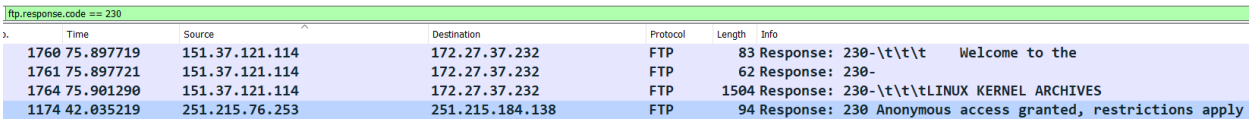
The result shows all login requests of username and password. Based on the result of question 3, we can just consider two cases below:

251.215.184.138 251.215.76.253 USER anonymous	251.215.184.138 251.215.76.253 PASS

172.27.37.232 151.37.121.114 USER calrules	172.27.37.232 151.37.121.114 PASS thisissosecure

So I continue to find the response from the corresponding servers and the result is below:

Command: ftp.response.code == 230



ftp.response.code == 230

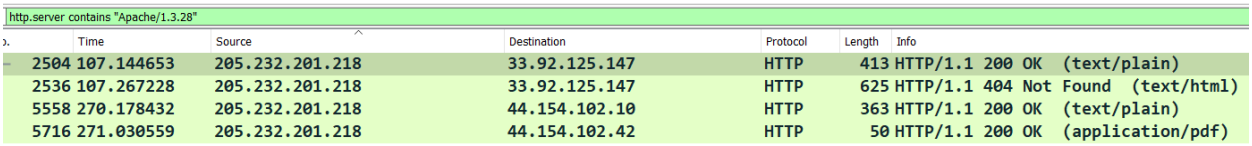
	Time	Source	Destination	Protocol	Length	Info
1760	75.897719	151.37.121.114	172.27.37.232	FTP	83	Response: 230-\t\t\t Welcome to the
1761	75.897721	151.37.121.114	172.27.37.232	FTP	62	Response: 230-
1764	75.901290	151.37.121.114	172.27.37.232	FTP	1504	Response: 230-\t\t\tLINUX KERNEL ARCHIVES
1174	42.035219	251.215.76.253	251.215.184.138	FTP	94	Response: 230 Anonymous access granted, restrictions apply

Result:

251.215.76.253	251.215.184.138	Anonymous access granted, restrictions apply
151.37.121.114	172.27.37.232	\t\t\t Welcome to the
151.37.121.114	172.27.37.232	
151.37.121.114	172.27.37.232	\t\t\tLINUX KERNEL ARCHIVES

By observation, both two login requests are successful. (anonymous,) (calrules, thisissosecure)

5. Command: http.server contains “Apache/1.3.28”



http.server contains "Apache/1.3.28"

	Time	Source	Destination	Protocol	Length	Info
2504	107.144653	205.232.201.218	33.92.125.147	HTTP	413	HTTP/1.1 200 OK (text/plain)
2536	107.267228	205.232.201.218	33.92.125.147	HTTP	625	HTTP/1.1 404 Not Found (text/html)
5558	270.178432	205.232.201.218	44.154.102.10	HTTP	363	HTTP/1.1 200 OK (text/plain)
5716	271.030559	205.232.201.218	44.154.102.42	HTTP	50	HTTP/1.1 200 OK (application/pdf)

Result: 205.232.201.218

As the filter specified, the host with above ip address runs the oldest version of Apache (Apache 1.3.28).

The below ip addresses are other hosts that also run Apache 1.3 but higher than 1.3.28.

143.179.11.189	155.231.237.70	159.79.22.194	159.79.22.198
248.78.109.66	251.235.172.148	33.247.152.113	

6. Command: dns && udp.srcport == 53

dns && udp.srcport == 53

No.	Time	Source	Destination	Protocol	Length	Info
77	13.054524	205.232.183.50	172.27.37.232	DNS	271	Standard query response 0x9166
92	13.365134	205.232.183.50	172.27.37.232	DNS	267	Standard query response 0x3131
172	19.356426	205.232.183.50	172.27.37.232	DNS	397	Standard query response 0xa834
183	19.565048	205.232.183.50	172.27.37.232	DNS	425	Standard query response 0xa436
191	19.733957	205.232.183.50	172.27.37.232	DNS	421	Standard query response 0xb62b
203	19.785624	205.232.183.50	172.27.37.232	DNS	329	Standard query response 0x3393
266	20.807855	205.232.183.50	172.27.37.232	DNS	274	Standard query response 0xe6fd
356	27.016861	205.232.183.50	172.27.37.232	DNS	406	Standard query response 0x2a8e
544	29.903457	205.232.183.50	172.27.37.232	DNS	190	Standard query response 0x3ca7
547	29.988007	205.232.183.50	205.232.201.195	DNS	300	Standard query response 0x18aa
764	34.334230	205.232.183.50	172.27.37.232	DNS	212	Standard query response 0x992c
904	35.881408	205.232.183.50	172.27.37.232	DNS	167	Standard query response 0x48a3
963	36.990300	205.232.183.50	172.27.37.232	DNS	394	Standard query response 0xebd1
1019	37.709038	205.232.183.50	172.27.37.232	DNS	156	Standard query response 0xd546
1048	38.126415	205.232.183.50	172.27.37.232	DNS	155	Standard query response 0x05f5
1193	42.628556	205.232.183.50	172.27.37.232	DNS	483	Standard query response 0x97a8
1600	52.794639	205.232.183.50	172.27.37.232	DNS	263	Standard query response 0xbf4b
1813	80.041264	205.232.183.50	205.232.201.195	DNS	138	Standard query response 0x6464
3192	167.785078	205.232.183.50	172.27.37.232	DNS	124	Standard query response 0xa3a1
3194	167.785758	205.232.183.50	172.27.37.232	DNS	252	Standard query response 0x7d2f
3215	169.166150	205.232.183.50	172.27.37.232	DNS	126	Standard query response 0xcdcd

Result:

205.232.183.50	205.232.183.94	251.215.76.60

By observation, there are three DNS resolvers using default source port 53. Using the command and results above, we can obtain further results below through combining their IP addresses.

205.232.183.50 34 times

251.215.76.60 404 times

By observation, 205.232.183.50 and 251.215.76.60 are exactly the two such DNS resolvers.

7.

tcp.flags.syn == 1

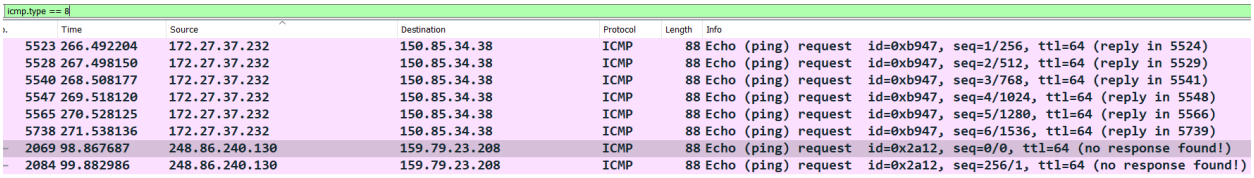
No.	Time	Source	Destination	Protocol	Length	Info
559	30.203541	138.59.102.27	172.27.37.232	TCP	64	80 → 58295 [SYN, ACK] Seq=2100324274 Ack=3
602	31.840997	138.59.102.27	172.27.37.232	TCP	64	80 → 58296 [SYN, ACK] Seq=2094560678 Ack=3
358	27.047499	143.138.66.97	172.27.37.232	TCP	50	80 → 58294 [SYN, ACK] Seq=3146666519 Ack=3
1602	52.798159	151.37.121.114	172.27.37.232	TCP	64	21 → 54556 [SYN, ACK] Seq=1091616842 Ack=3
1879	83.949950	151.37.121.114	172.27.37.232	TCP	64	20 → 58305 [SYN, ECN, CWR] Seq=1112118926
1978	95.178066	151.37.121.114	172.27.37.232	TCP	64	20 → 58306 [SYN, ECN, CWR] Seq=1125738097
2374	105.992164	151.37.121.114	172.27.37.232	TCP	64	20 → 58307 [SYN, ECN, CWR] Seq=1143895365
2624	110.902595	151.37.121.114	172.27.37.232	TCP	64	20 → 58308 [SYN, ECN, CWR] Seq=1141563997
2885	124.515966	151.37.121.114	172.27.37.232	TCP	64	20 → 58309 [SYN, ECN, CWR] Seq=1159532682
3002	154.066123	151.37.121.114	172.27.37.232	TCP	64	20 → 58310 [SYN, ECN, CWR] Seq=1183194761
921	36.175304	154.87.109.177	172.27.37.232	TCP	68	80 → 58298 [SYN, ACK] Seq=1593413079 Ack=3
794	34.635513	154.87.109.40	172.27.37.232	TCP	68	80 → 58297 [SYN, ACK] Seq=1626969031 Ack=3
1026	37.883361	155.231.237.70	172.27.37.232	TCP	64	80 → 58300 [SYN, ACK] Seq=442621493 Ack=30
1063	38.292594	155.231.237.70	172.27.37.232	TCP	64	80 → 58301 [SYN, ACK] Seq=440945856 Ack=30
1195	42.637254	159.70.229.173	172.27.37.232	TCP	64	80 → 58303 [SYN, ACK] Seq=1680117033 Ack=3
4967	238.080602	159.79.22.194	42.9.203.117	TCP	68	80 → 24945 [SYN, ACK] Seq=1881908354 Ack=4
4970	238.175099	159.79.22.194	42.9.203.117	TCP	68	80 → 41520 [SYN, ACK] Seq=1882045970 Ack=4
4980	238.318951	159.79.22.194	42.9.203.117	TCP	68	80 → 41527 [SYN, ACK] Seq=1882241366 Ack=4
5073	243.688189	159.79.22.194	248.35.162.92	TCP	52	21 → 44171 [SYN, ACK] Seq=2020069998 Ack=3
5107	247.052313	159.79.22.194	248.35.162.92	TCP	52	[TCP Retransmission] 21 → 44171 [SYN, ACK]
5042	242.710457	159.79.22.198	251.215.153.250	TCP	68	80 → 55996 [SYN, ACK] Seq=1121491243 Ack=2
5757	275.935041	159.79.22.249	251.215.153.250	TCP	64	80 → 57699 [SYN, ACK] Seq=1545980164 Ack=3
5796	280.355602	159.79.22.249	251.215.153.250	TCP	64	80 → 58055 [SYN, ACK] Seq=1544994167 Ack=1
5806	280.359532	159.79.22.249	251.215.153.250	TCP	64	80 → 58057 [SYN, ACK] Seq=1555932108 Ack=2
5922	309.263460	159.79.22.249	251.215.153.250	TCP	64	80 → 60123 [SYN, ACK] Seq=1601576306 Ack=8
5932	313.710396	159.79.22.249	251.215.153.250	TCP	64	80 → 60410 [SYN, ACK] Seq=1602214428 Ack=4
5942	313.723832	159.79.22.249	251.215.153.250	TCP	64	80 → 60412 [SYN, ACK] Seq=1600931174 Ack=1

By observation, the hosts with IP addresses below made more than 5 attempts.

IP address	Max Seq #	Min Seq #
151.37.121.114	1183194761	1091616842
159.79.22.194	2020069998	1881908354
159.79.22.249	1610371867	1545980164
172.27.37.232	3233147232	3068021923
205.232.201.195	3365621251	3129360678
248.35.162.92	344892887	342128287
248.78.109.66	4270370641	1041403085
251.215.153.250	3932559224	1161183537

Obviously, the broadest one is 248.78.109.66.

8. Command: icmp.type == 8



Result:

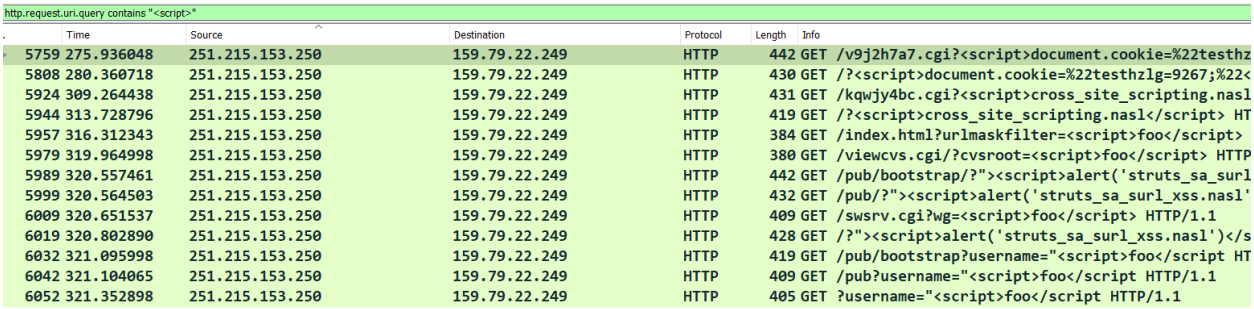
172.27.37.232 248.86.240.130

By checking ICMP request, we obtain two hosts that may traceroute. So, I first observe 172.27.37.232 using command “ip.dst ==172.27.37.232”. The result shows that it is not the host I want because:

(1) It does not have ICMP request packet with TTL=1.
(2) It does not have UDP packet with TTL=1.
(3) It does not have TCP-SYN packet with Seq=0.

However, the result of 248.86.240.130 shows that it sends UDP packet with TTL from 1 to 64 many times to 159.79.23.208. Thus, the answer is (248.86.240.130, 159.79.23.208).

9. Command: http.request.uri.query contains “<script>”



http.request.uri.query contains "<script>"

	Time	Source	Destination	Protocol	Length	Info
5759	275.936048	251.215.153.250	159.79.22.249	HTTP	442	GET /v9j2h7a7.cgi?<script>document.cookie=%22testhz
5808	280.360718	251.215.153.250	159.79.22.249	HTTP	430	GET /?<script>document.cookie=%22testhzlg=9267;%22<
5924	309.264438	251.215.153.250	159.79.22.249	HTTP	431	GET /kqwjy4bc.cgi?<script>cross_site_scripting.nasl
5944	313.728796	251.215.153.250	159.79.22.249	HTTP	419	GET /?<script>cross_site_scripting.nasl</script> HT
5957	316.312343	251.215.153.250	159.79.22.249	HTTP	384	GET /index.html?urlmaskfilter=<script>foo</script>
5979	319.964998	251.215.153.250	159.79.22.249	HTTP	380	GET /viewcvs.cgi/?cvsroot=<script>foo</script> HTTP
5989	320.557461	251.215.153.250	159.79.22.249	HTTP	442	GET /pub/bootstrap/?"><script>alert('struts_sa_surl
5999	320.564503	251.215.153.250	159.79.22.249	HTTP	432	GET /pub/?"><script>alert('struts_sa_surl_xss.nasl'
6009	320.651537	251.215.153.250	159.79.22.249	HTTP	409	GET /swsrv.cgi?wg=<script>foo</script> HTTP/1.1
6019	320.802890	251.215.153.250	159.79.22.249	HTTP	428	GET /?"><script>alert('struts_sa_surl_xss.nasl')</s
6032	321.095998	251.215.153.250	159.79.22.249	HTTP	419	GET /pub/bootstrap?username="<script>foo</script HT
6042	321.104065	251.215.153.250	159.79.22.249	HTTP	409	GET /pub?username="<script>foo</script HTTP/1.1
6052	321.352898	251.215.153.250	159.79.22.249	HTTP	405	GET ?username="<script>foo</script HTTP/1.1

The result clearly shows the server with address 159.79.22.249 has the vulnerability.

Part2:

1.

Command:

tshark -r "project2_part2.pcap" -T fields -e eth.src -e ip.src | sort /unique

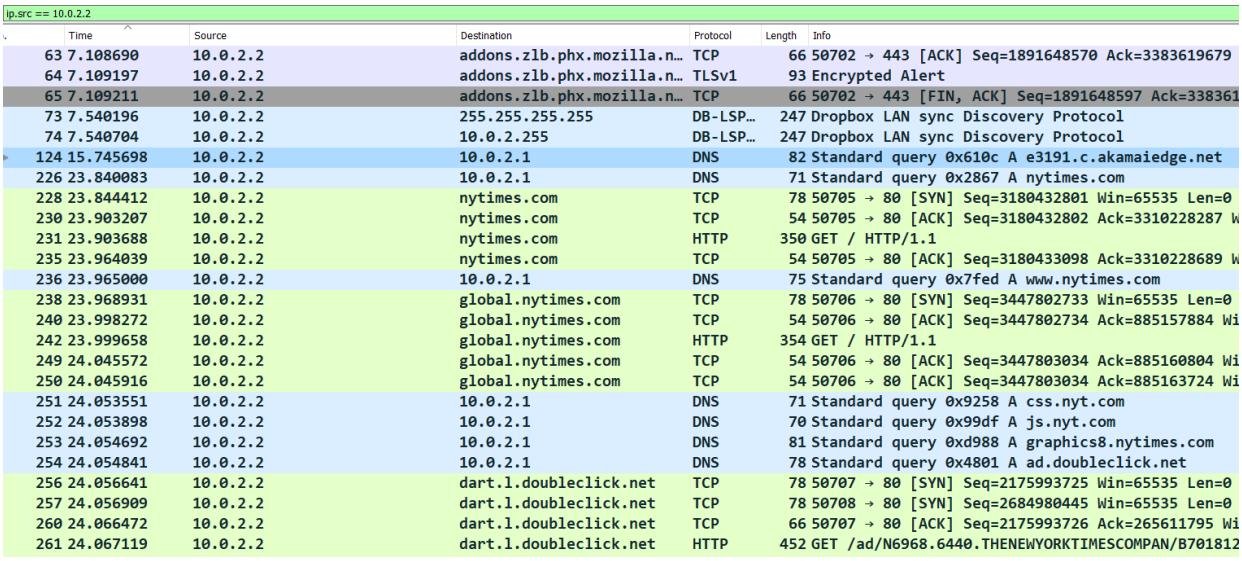
Result:

	MAC addresse	IP Address
Device 1 (gate)	00:26:08:e5:66:07	0.0.0.0 10.0.2.1
Device 2	04:0c:ce:d8:0f:fa	10.0.2.2
Device 3	8c:a9:82:50:f0:a6	10.0.2.3

When using the command above, we get 3 MAC address paired with multiple IP address. However, only the four IP addresses are the corresponding ones. Other IP addresses, particularly for Device 1, are the responses from servers outside the LAN.

2.

Base on the results above, we can observe that there are two devices connecting to the gate and all the requests and responses from those two devices go through the gate. Thus, the network should be a LAN, but the devices can connect to remote servers through the gate. For example, the picture below shows that Device 2 send DNS queries to Device 1 when it wants to talk with any remote servers.



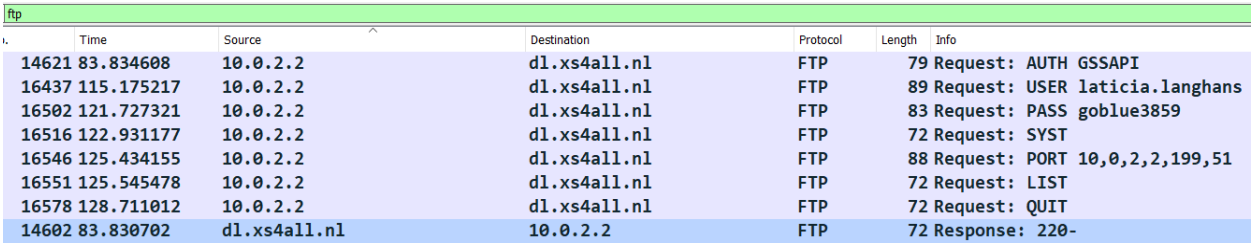
ip.src == 10.0.2.2

	Time	Source	Destination	Protocol	Length	Info
63	7.108690	10.0.2.2	addons.zlb.phx.mozilla.n…	TCP	66	50702 → 443 [ACK] Seq=1891648570 Ack=3383619679
64	7.109197	10.0.2.2	addons.zlb.phx.mozilla.n…	TLSv1	93	Encrypted Alert
65	7.109211	10.0.2.2	addons.zlb.phx.mozilla.n…	TCP	66	50702 → 443 [FIN, ACK] Seq=1891648597 Ack=338361
73	7.540196	10.0.2.2	255.255.255.255	DB-LSP…	247	Dropbox LAN sync Discovery Protocol
74	7.540704	10.0.2.2	10.0.2.255	DB-LSP…	247	Dropbox LAN sync Discovery Protocol
124	15.745698	10.0.2.2	10.0.2.1	DNS	82	Standard query 0x610c A e3191.c.akamaiedge.net
226	23.840083	10.0.2.2	10.0.2.1	DNS	71	Standard query 0x2867 A nytimes.com
228	23.844412	10.0.2.2	nytimes.com	TCP	78	50705 → 80 [SYN] Seq=3180432801 Win=65535 Len=0
230	23.903207	10.0.2.2	nytimes.com	TCP	54	50705 → 80 [ACK] Seq=3180432802 Ack=3310228287 W
231	23.903688	10.0.2.2	nytimes.com	HTTP	350	GET / HTTP/1.1
235	23.964039	10.0.2.2	nytimes.com	TCP	54	50705 → 80 [ACK] Seq=3180433098 Ack=3310228689 W
236	23.965000	10.0.2.2	10.0.2.1	DNS	75	Standard query 0x7fed A www.nytimes.com
238	23.968931	10.0.2.2	global.nytimes.com	TCP	78	50706 → 80 [SYN] Seq=3447802733 Win=65535 Len=0
240	23.998272	10.0.2.2	global.nytimes.com	TCP	54	50706 → 80 [ACK] Seq=3447802734 Ack=885157884 Wi
242	23.999658	10.0.2.2	global.nytimes.com	HTTP	354	GET / HTTP/1.1
249	24.045572	10.0.2.2	global.nytimes.com	TCP	54	50706 → 80 [ACK] Seq=3447803034 Ack=885160804 Wi
250	24.045916	10.0.2.2	global.nytimes.com	TCP	54	50706 → 80 [ACK] Seq=3447803034 Ack=885163724 Wi
251	24.053551	10.0.2.2	10.0.2.1	DNS	71	Standard query 0x9258 A css.nyt.com
252	24.053898	10.0.2.2	10.0.2.1	DNS	70	Standard query 0x99df A js.nyt.com
253	24.054692	10.0.2.2	10.0.2.1	DNS	81	Standard query 0xd988 A graphics8.nytimes.com
254	24.054841	10.0.2.2	10.0.2.1	DNS	78	Standard query 0x4801 A ad.doubleclick.net
256	24.056641	10.0.2.2	dart.l.doubleclick.net	TCP	78	50707 → 80 [SYN] Seq=2175993725 Win=65535 Len=0
257	24.056909	10.0.2.2	dart.l.doubleclick.net	TCP	78	50708 → 80 [SYN] Seq=2684980445 Win=65535 Len=0
260	24.066472	10.0.2.2	dart.l.doubleclick.net	TCP	66	50707 → 80 [ACK] Seq=2175993726 Ack=265611795 Wi
261	24.067119	10.0.2.2	dart.l.doubleclick.net	HTTP	452	GET /ad/N6968.6440.THENEWYORKTIMESCOMPAN/B701812

3.

(a)

DNS hostname: dl.xs4all.nl (Command: ftp)

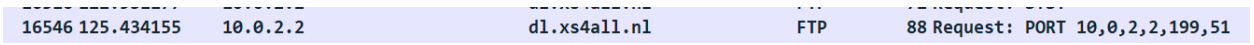


ftp

	Time	Source	Destination	Protocol	Length	Info
14621	83.834608	10.0.2.2	dl.xs4all.nl	FTP	79	Request: AUTH GSSAPI
16437	115.175217	10.0.2.2	dl.xs4all.nl	FTP	89	Request: USER laticia.langhans
16502	121.727321	10.0.2.2	dl.xs4all.nl	FTP	83	Request: PASS goblue3859
16516	122.931177	10.0.2.2	dl.xs4all.nl	FTP	72	Request: SYST
16546	125.434155	10.0.2.2	dl.xs4all.nl	FTP	88	Request: PORT 10,0,2,2,199,51
16551	125.545478	10.0.2.2	dl.xs4all.nl	FTP	72	Request: LIST
16578	128.711012	10.0.2.2	dl.xs4all.nl	FTP	72	Request: QUIT
14602	83.830702	dl.xs4all.nl	10.0.2.2	FTP	72	Response: 220-

(b)

Active, since the client tells the server issues the PORT command and tells the server IP address (10.0.2.2) and port (50995) it will be listening on.



16546	125.434155	10.0.2.2	dl.xs4all.nl	FTP	88	Request: PORT 10,0,2,2,199,51

(c)

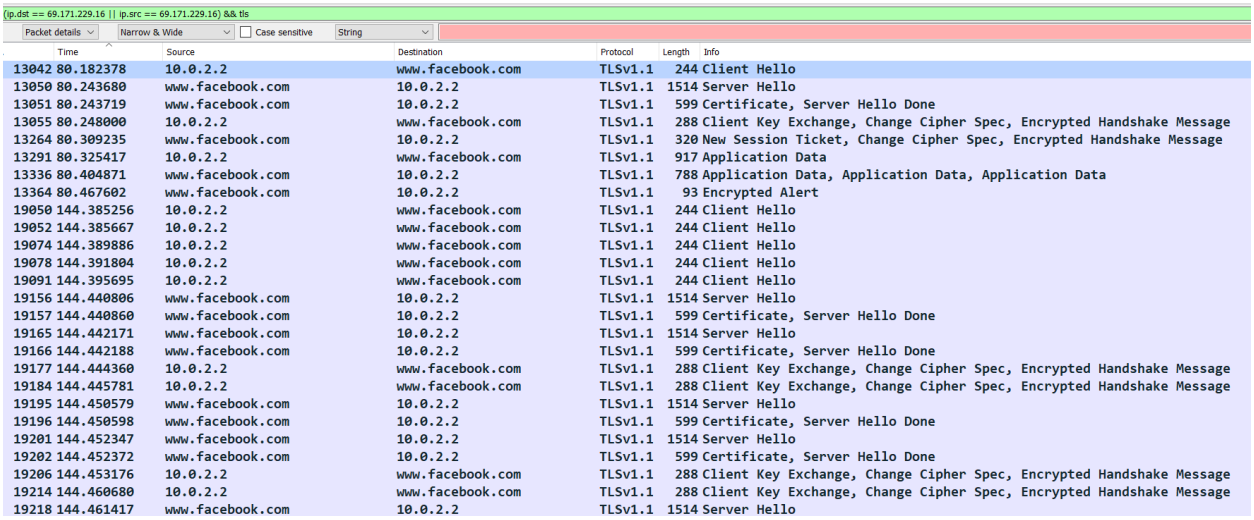
Anonymous authentication is an FTP vulnerability that allows users to log in with a username of FTP or anonymously. Typically, users will provide their email address as the password. However, a user's login credentials (username and password) and the commands used unencrypted, visible, and vulnerable to access. At the same time, any data sent through FTP or is hosted on an anonymous FTP server is also left unprotected.

```
136 Response: 220-Welcome to the XS4ALL archive,  Please login as `anonymous' with
130 Response: 220-your E-mail address as the password to access the archive.
 72 Response: 220-
143 Response: 220-All anonymous transfers are logged with your host name and whatever you
144 Response: 220-entered for the password. If you don't like this policy, disconnect now!
 73 Response: 220-
```

(d)

HTTPS, TLS/SSL and SSH are the network protocols which are more secure that FTP.

4.



(ip.dst == 69.171.229.16 || ip.src == 69.171.229.16) && tls

Packet details | Narrow & Wide | Case sensitive | String

	Time	Source	Destination	Protocol	Length	Info
13042	80.182378	10.0.2.2	www.facebook.com	TLSv1.1	244	Client Hello
13050	80.243680	www.facebook.com	10.0.2.2	TLSv1.1	1514	Server Hello
13051	80.243719	www.facebook.com	10.0.2.2	TLSv1.1	599	Certificate, Server Hello Done
13055	80.248000	10.0.2.2	www.facebook.com	TLSv1.1	288	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
13264	80.309235	www.facebook.com	10.0.2.2	TLSv1.1	320	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
13291	80.325417	10.0.2.2	www.facebook.com	TLSv1.1	917	Application Data
13336	80.404871	www.facebook.com	10.0.2.2	TLSv1.1	788	Application Data, Application Data, Application Data
13364	80.467602	www.facebook.com	10.0.2.2	TLSv1.1	93	Encrypted Alert
19050	144.385256	10.0.2.2	www.facebook.com	TLSv1.1	244	Client Hello
19052	144.385667	10.0.2.2	www.facebook.com	TLSv1.1	244	Client Hello
19074	144.389886	10.0.2.2	www.facebook.com	TLSv1.1	244	Client Hello
19078	144.391804	10.0.2.2	www.facebook.com	TLSv1.1	244	Client Hello
19091	144.395695	10.0.2.2	www.facebook.com	TLSv1.1	244	Client Hello
19156	144.440806	www.facebook.com	10.0.2.2	TLSv1.1	1514	Server Hello
19157	144.440860	www.facebook.com	10.0.2.2	TLSv1.1	599	Certificate, Server Hello Done
19165	144.442171	www.facebook.com	10.0.2.2	TLSv1.1	1514	Server Hello
19166	144.442188	www.facebook.com	10.0.2.2	TLSv1.1	599	Certificate, Server Hello Done
19177	144.444360	10.0.2.2	www.facebook.com	TLSv1.1	288	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
19184	144.445781	10.0.2.2	www.facebook.com	TLSv1.1	288	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
19195	144.450579	www.facebook.com	10.0.2.2	TLSv1.1	1514	Server Hello
19196	144.450598	www.facebook.com	10.0.2.2	TLSv1.1	599	Certificate, Server Hello Done
19201	144.452347	www.facebook.com	10.0.2.2	TLSv1.1	1514	Server Hello
19202	144.452372	www.facebook.com	10.0.2.2	TLSv1.1	599	Certificate, Server Hello Done
19206	144.453176	10.0.2.2	www.facebook.com	TLSv1.1	288	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
19214	144.460680	10.0.2.2	www.facebook.com	TLSv1.1	288	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
19218	144.461417	www.facebook.com	10.0.2.2	TLSv1.1	1514	Server Hello

(a)

The password is cached by the web browser, at a minimum for the length of the window process. (Can be silently reused by any other request to the server, e.g. CSRF)

(b)

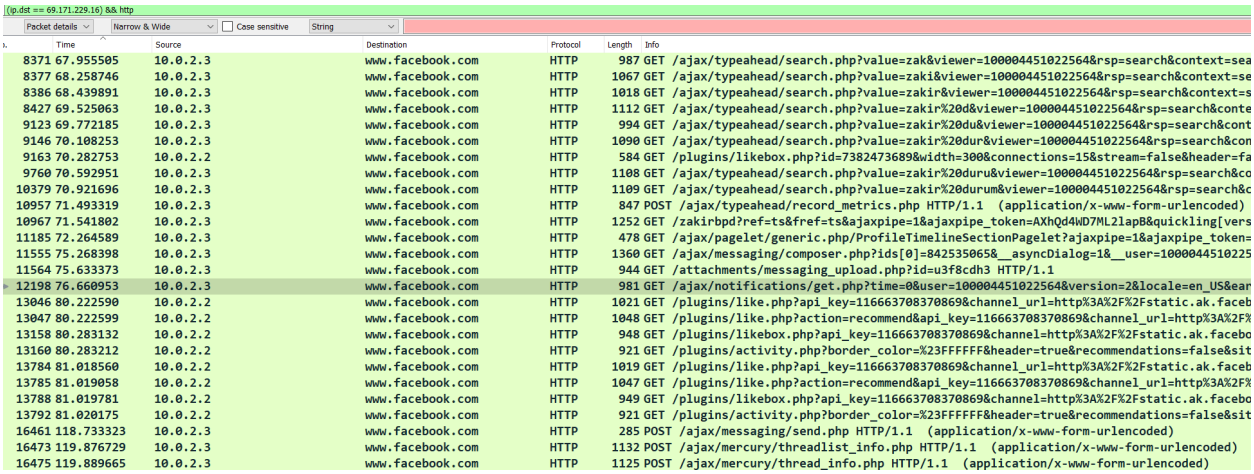
An attacker can run unauthorized commands as an authorized user. In other words, an attacker may trick the users of a web application into executing actions of the attacker's choosing.

(c)

Using Anti-CSRF Token or the Same-Site Flag in Cookies to secure the communication between users and web applications. For the token, it is a random string that is only known by the user’s browser and the web application. For the Same-Site Flag in cookies, each session cookie is unique for every user and the web application uses it to distinguish different users from each other, and to determine if you are logged in as well.

(d)

The user searched some people and check their like boxes. Also, the user attached a file, and get a notification, and sent message to others. In the end, the user loaded old messages.



(ip.dst == 69.171.229.16) && http

Packet details | Narrow & Wide | Case sensitive | String

	Time	Source	Destination	Protocol	Length	Info
8371	67.955505	10.0.2.3	www.facebook.com	HTTP	987	GET /ajax/typeahead/search.php?value=zak&viewer=100004451022564&rsp=search&context=sea
8377	68.258746	10.0.2.3	www.facebook.com	HTTP	1067	GET /ajax/typeahead/search.php?value=zaki&viewer=100004451022564&rsp=search&context=se
8386	68.439891	10.0.2.3	www.facebook.com	HTTP	1018	GET /ajax/typeahead/search.php?value=zakir&viewer=100004451022564&rsp=search&context=s
8427	69.525063	10.0.2.3	www.facebook.com	HTTP	1112	GET /ajax/typeahead/search.php?value=zakir%20d&viewer=100004451022564&rsp=search&conte
9123	69.772185	10.0.2.3	www.facebook.com	HTTP	994	GET /ajax/typeahead/search.php?value=zakir%20du&viewer=100004451022564&rsp=search&cont
9146	70.108253	10.0.2.3	www.facebook.com	HTTP	1090	GET /ajax/typeahead/search.php?value=zakir%20dur&viewer=100004451022564&rsp=search&con
9163	70.282753	10.0.2.2	www.facebook.com	HTTP	584	GET /plugins/likebox.php?id=7382473689&width=300&connections=15&stream=false&header=fa
9760	70.592951	10.0.2.3	www.facebook.com	HTTP	1108	GET /ajax/typeahead/search.php?value=zakir%20duru&viewer=100004451022564&rsp=search&co
10379	70.921696	10.0.2.3	www.facebook.com	HTTP	1109	GET /ajax/typeahead/search.php?value=zakir%20durum&viewer=100004451022564&rsp=search&c
10957	71.493319	10.0.2.3	www.facebook.com	HTTP	847	POST /ajax/typeahead/record_metrics.php HTTP/1.1 (application/x-www-form-urlencoded)
10967	71.541802	10.0.2.3	www.facebook.com	HTTP	1252	GET /zakirbpd?ref=ts&fref=ts&ajaxpipe=1&ajaxpipe_token=AXhQd4WD7ML2lapB&quickling[vers
11185	72.264589	10.0.2.3	www.facebook.com	HTTP	478	GET /ajax/pagelet/generic.php/ProfileTimelineSectionPagelet?ajaxpipe=1&ajaxpipe_token=
11555	75.268398	10.0.2.3	www.facebook.com	HTTP	1360	GET /ajax/messaging/composer.php?ids[0]=842535065&__asyncDialog=1&__user=1000044510225
11564	75.633373	10.0.2.3	www.facebook.com	HTTP	944	GET /attachments/messaging_upload.php?id=u3f8cdh3 HTTP/1.1
12198	76.660953	10.0.2.3	www.facebook.com	HTTP	981	GET /ajax/notifications/get.php?time=0&user=100004451022564&version=2&locale=en_US&ear
13046	80.222590	10.0.2.2	www.facebook.com	HTTP	1021	GET /plugins/like.php?api_key=1166637083708 69&channel_url=http%3A%2F%2Fstatic.ak.faceb
13047	80.222599	10.0.2.2	www.facebook.com	HTTP	1048	GET /plugins/like.php?action=recommend&api_key=1166637083708 69&channel_url=http%3A%2F%
13158	80.283132	10.0.2.2	www.facebook.com	HTTP	948	GET /plugins/likebox.php?api_key=1166637083708 69&channel=http%3A%2F%2Fstatic.ak.facebo
13160	80.283212	10.0.2.2	www.facebook.com	HTTP	921	GET /plugins/activity.php?border_color=%23FFFFFF&header=true&recommendations=false&sit
13784	81.018560	10.0.2.2	www.facebook.com	HTTP	1019	GET /plugins/like.php?api_key=1166637083708 69&channel_url=http%3A%2F%2Fstatic.ak.faceb
13785	81.019058	10.0.2.2	www.facebook.com	HTTP	1047	GET /plugins/like.php?action=recommend&api_key=1166637083708 69&channel_url=http%3A%2F%
13788	81.019781	10.0.2.2	www.facebook.com	HTTP	949	GET /plugins/likebox.php?api_key=1166637083708 69&channel=http%3A%2F%2Fstatic.ak.facebo
13792	81.020175	10.0.2.2	www.facebook.com	HTTP	921	GET /plugins/activity.php?border_color=%23FFFFFF&header=true&recommendations=false&sit
16461	118.733323	10.0.2.3	www.facebook.com	HTTP	285	POST /ajax/messaging/send.php HTTP/1.1 (application/x-www-form-urlencoded)
16473	119.876729	10.0.2.3	www.facebook.com	HTTP	1132	POST /ajax/mercury/threadlist_info.php HTTP/1.1 (application/x-www-form-urlencoded)
16475	119.889665	10.0.2.3	www.facebook.com	HTTP	1125	POST /ajax/mercury/thread_info.php HTTP/1.1 (application/x-www-form-urlencoded)