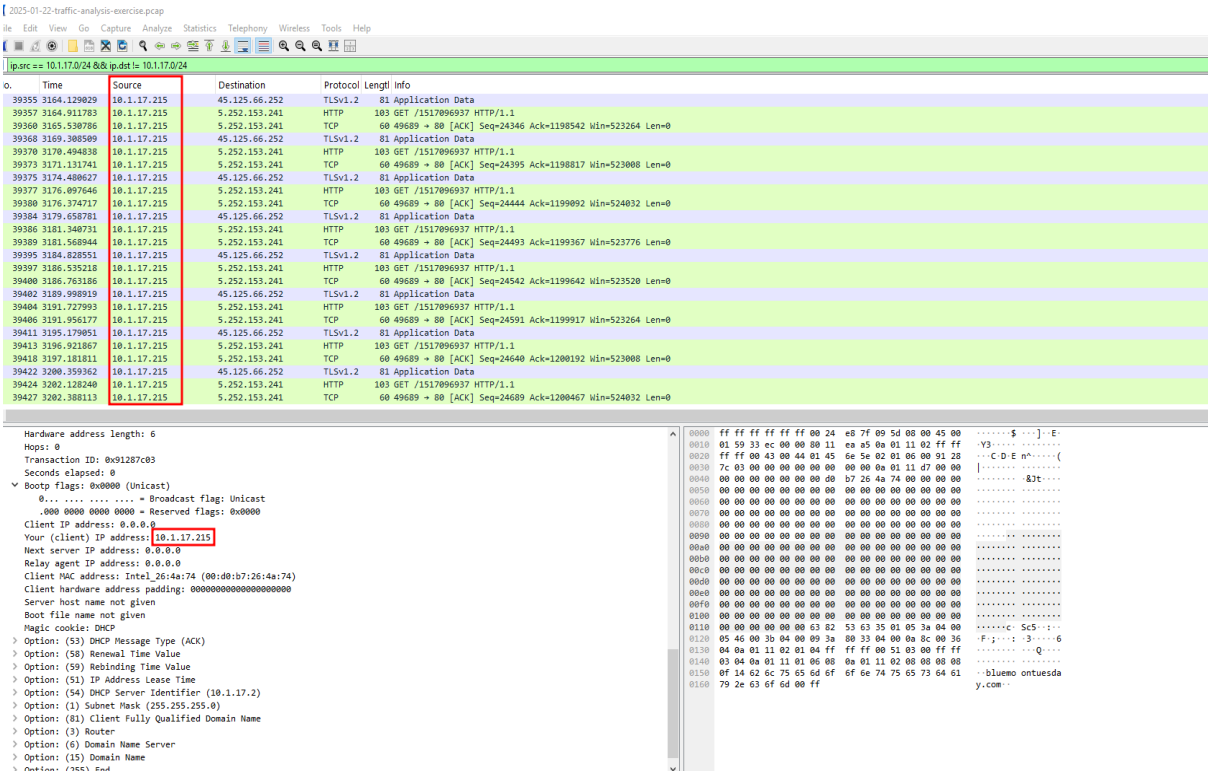
Athanasius Joseph Kojo Gadosey

Week 3

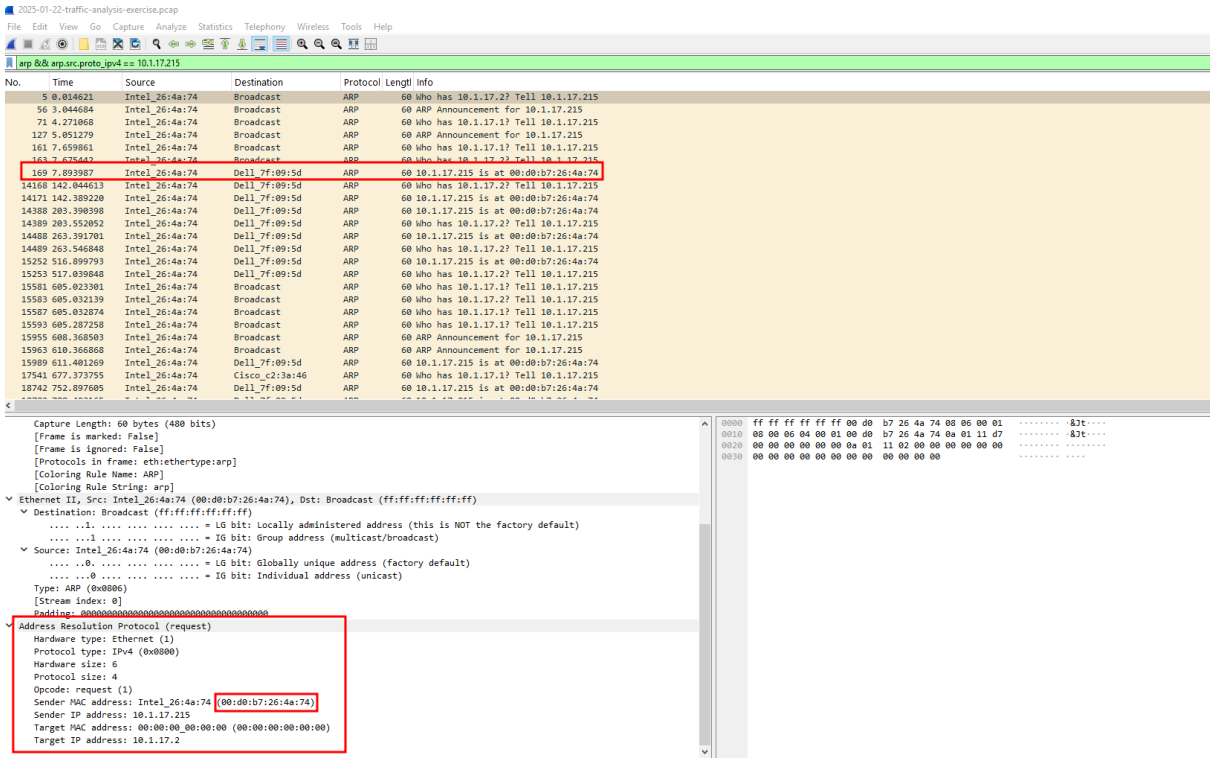
Practical Task: The Suspicious Downloaded PCAP Analysis

The following answers are the analysis of the incident reports:

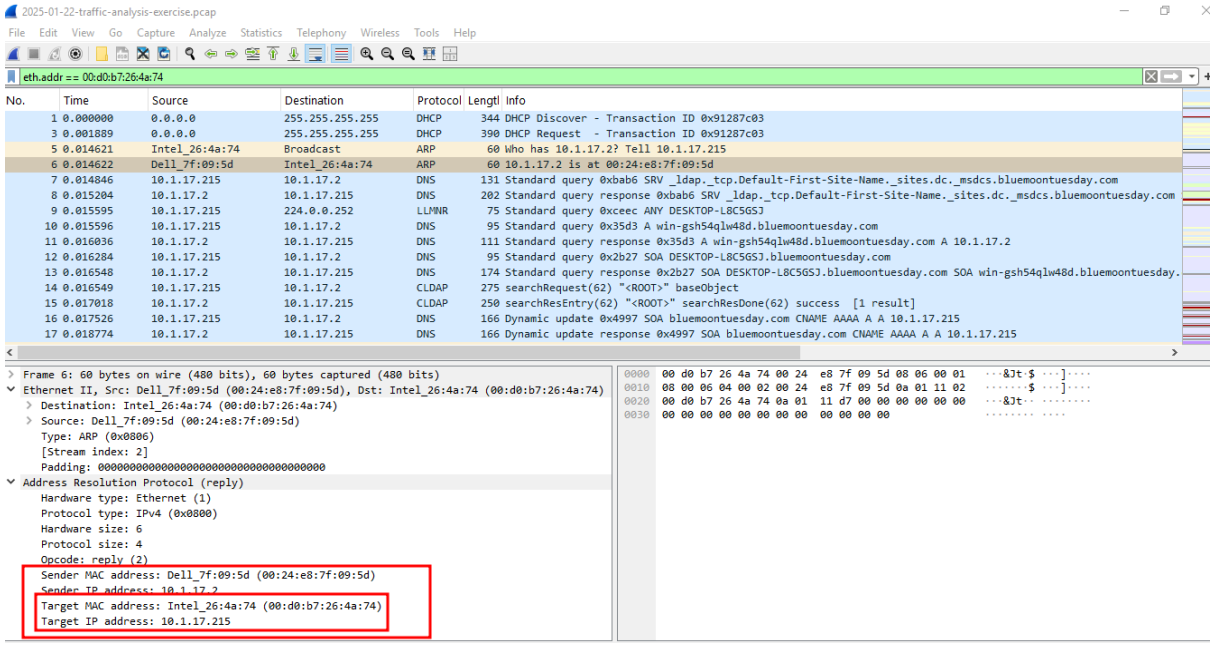
1. The IP address of the infected Windows Client is **10.1.17.215**
   Filter: (*ip.src == 10.1.17.0/24 && ip.dst != 10.1.17.0/24) This command was used to analyse the host IP address communicating to any external networks, which helped us to spot the suspicious outbound connections.*



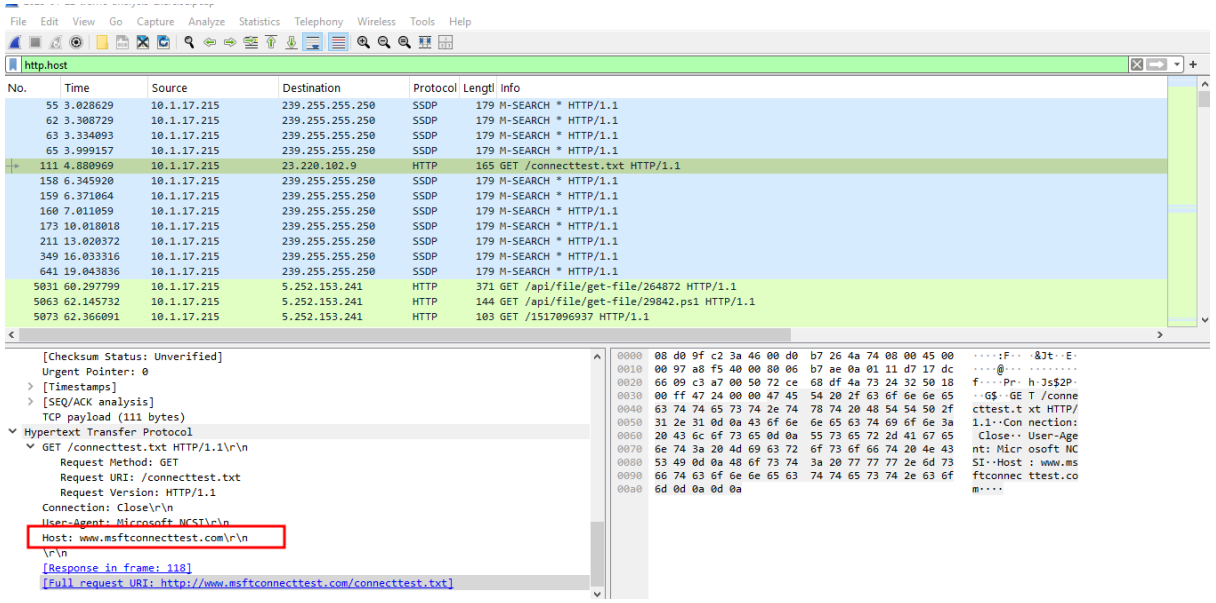
2. The MAC address of the infected Windows Client is **00:d0:b7:26:4a:74**
   Filter: (*arp && arp.src.proto_ipv4 == 10.1.17.215*) This command was to help identify the MAC address of the IP address.



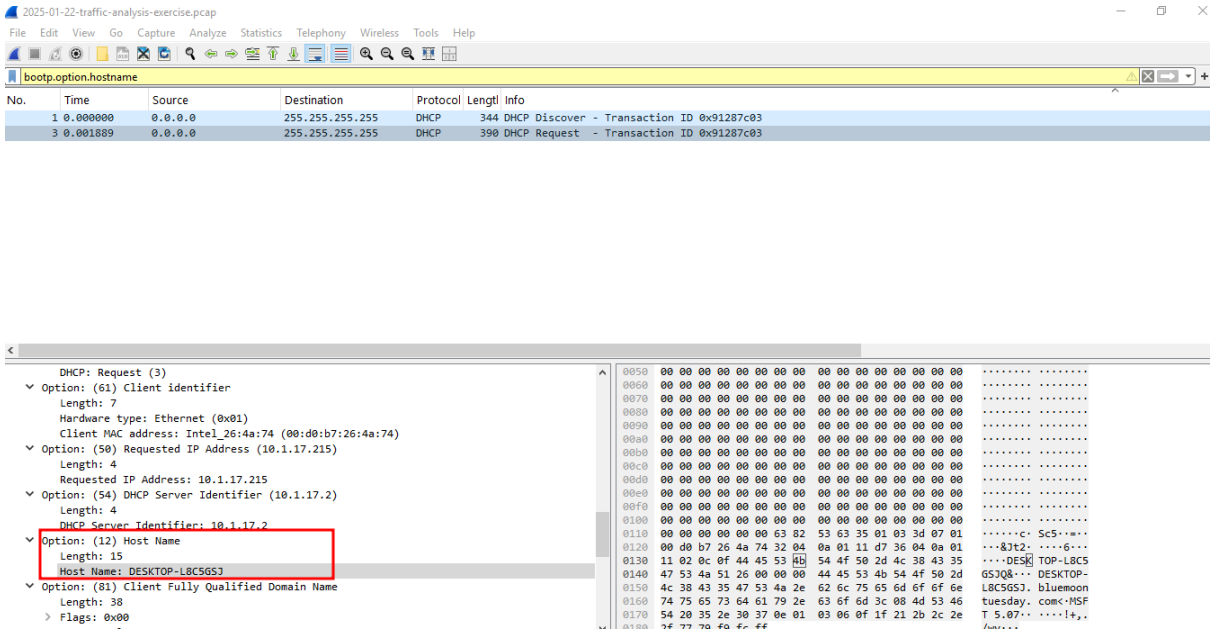
Also, this filter command (*eth.addr == 00:d0:b7:26:4a:74*) was used to confirm the MAC address of the infected Windows client gotten earlier



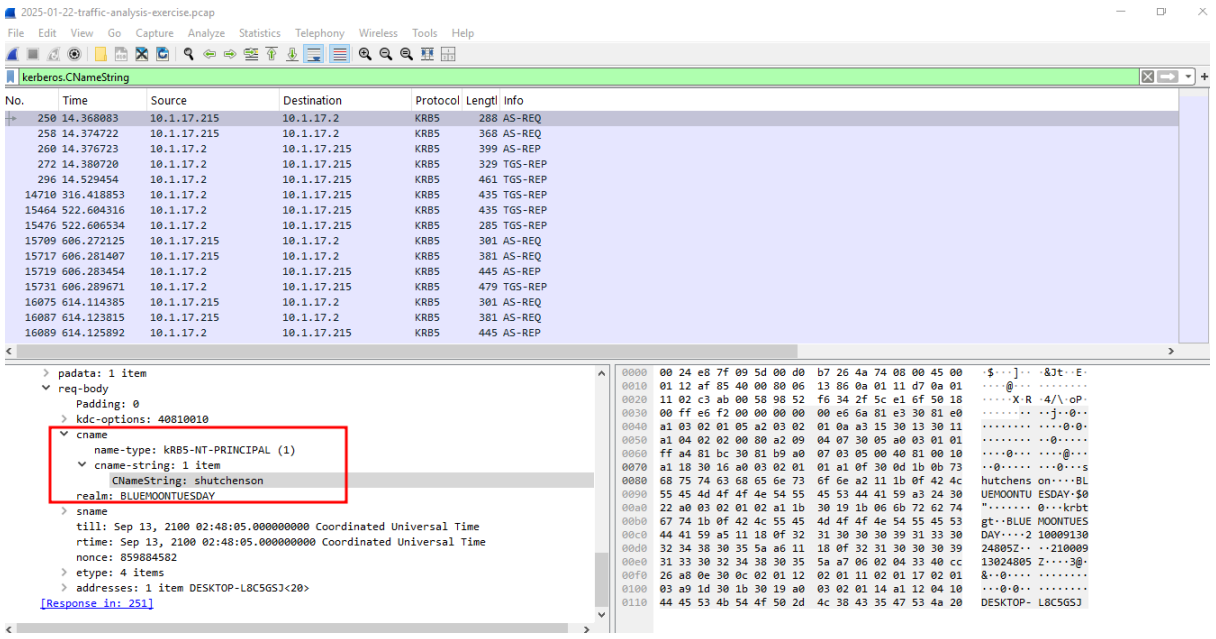
3. The hostname of the infected Windows client is ***www.msfconnecttest.com*** OR DESKTOP-L8C5GSJ



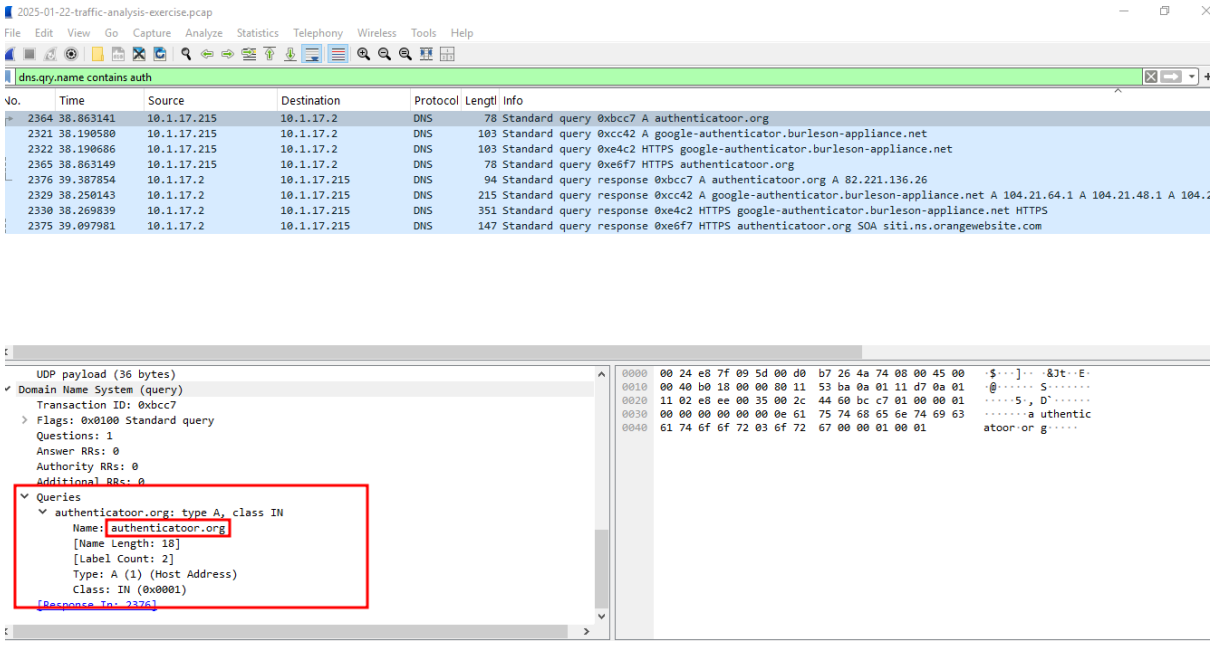
The filter command used is *bootp.option.hostname*



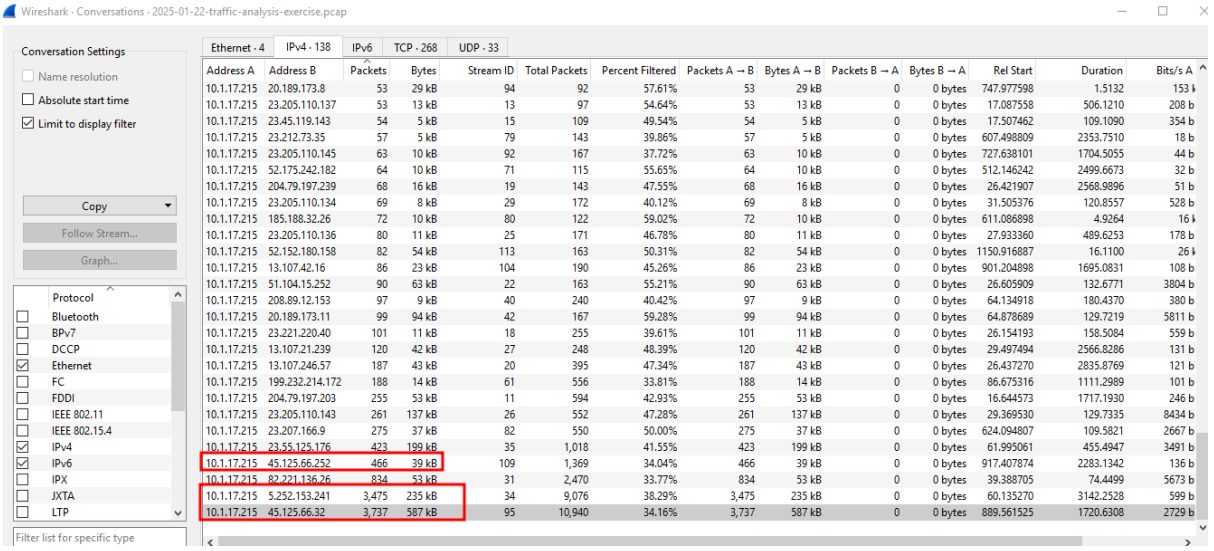
4. The user account name from the infected Windows Client is ***BLUEMOONTUESDAY/shutchenson***
   Filter: (kerberos.CNameString) This command is used because most user accounts can be found or appear in them, and is also known for its reliability.



5. The likely domain name for the fake Google Authenticator page is ***authenticatoor.org***
   Filter: (**dns.qry.name contains auth**) This command was used to query dns of the infected Windows client.



6. The IP addresses used for C2 servers for this infection are `5.252.153.241`, `45.125.66.252` and `45.125.66.32`
   Filter for **outbound traffic to external IP ranges** after the infection.



Address A	Address B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A
10.1.17.215	20.189.173.8	53	29 kB	94	92	57.61%	53	29 kB	0	0 bytes	747.977598	1.5132	153 k
10.1.17.215	23.205.110.137	53	13 kB	13	97	54.64%	53	13 kB	0	0 bytes	17.087558	506.1210	208 b
10.1.17.215	23.45.119.143	54	5 kB	15	109	49.54%	54	5 kB	0	0 bytes	17.507462	109.1090	354 b
10.1.17.215	23.212.73.35	57	5 kB	79	143	39.86%	57	5 kB	0	0 bytes	607.498809	2353.7510	18 b
10.1.17.215	23.205.110.145	63	10 kB	92	167	37.72%	63	10 kB	0	0 bytes	727.638101	1704.5055	44 b
10.1.17.215	52.175.242.182	64	10 kB	71	115	55.65%	64	10 kB	0	0 bytes	512.146242	2499.6673	32 b
10.1.17.215	204.79.197.239	68	16 kB	19	143	47.55%	68	16 kB	0	0 bytes	26.421907	2568.9896	51 b
10.1.17.215	23.205.110.134	69	8 kB	29	172	40.12%	69	8 kB	0	0 bytes	31.505376	120.8557	528 b
10.1.17.215	185.188.32.26	72	10 kB	80	122	59.02%	72	10 kB	0	0 bytes	611.086898	4.9264	16 k
10.1.17.215	23.205.110.136	80	11 kB	25	171	46.78%	80	11 kB	0	0 bytes	27.933360	489.6253	178 b
10.1.17.215	52.152.180.158	82	54 kB	113	163	50.31%	82	54 kB	0	0 bytes	1150.916887	16.1100	26 k
10.1.17.215	13.107.42.16	86	23 kB	104	190	45.26%	86	23 kB	0	0 bytes	901.204898	1695.0831	108 b
10.1.17.215	51.104.15.252	90	63 kB	22	163	55.21%	90	63 kB	0	0 bytes	26.605909	132.6771	3804 b
10.1.17.215	208.89.12.153	97	9 kB	40	240	40.42%	97	9 kB	0	0 bytes	64.134918	180.4370	380 b
10.1.17.215	20.189.173.11	99	94 kB	42	167	59.28%	99	94 kB	0	0 bytes	64.878689	129.7219	5811 b
10.1.17.215	23.221.220.40	101	11 kB	18	255	39.61%	101	11 kB	0	0 bytes	26.154193	158.5084	559 b
10.1.17.215	13.107.21.239	120	42 kB	27	248	48.39%	120	42 kB	0	0 bytes	29.497494	2566.8286	131 b
10.1.17.215	13.107.246.57	187	43 kB	20	395	47.34%	187	43 kB	0	0 bytes	26.437270	2835.8769	121 b
10.1.17.215	199.232.214.172	188	14 kB	61	556	33.81%	188	14 kB	0	0 bytes	86.675316	1111.2989	101 b
10.1.17.215	204.79.197.203	255	53 kB	11	594	42.93%	255	53 kB	0	0 bytes	16.644573	1717.1930	246 b
10.1.17.215	23.205.110.143	261	137 kB	26	552	47.28%	261	137 kB	0	0 bytes	29.369530	129.7335	8434 b
10.1.17.215	23.207.166.9	275	37 kB	82	550	50.00%	275	37 kB	0	0 bytes	624.094807	109.5821	2667 b
10.1.17.215	23.55.125.176	423	199 kB	35	1,018	41.55%	423	199 kB	0	0 bytes	61.995061	455.4947	3491 b
10.1.17.215	45.125.66.252	466	39 kB	109	1,369	34.04%	466	39 kB	0	0 bytes	917.407874	2283.1342	136 b
10.1.17.215	82.221.136.26	834	53 kB	31	2,470	33.77%	834	53 kB	0	0 bytes	39.388705	74.4499	5673 b
10.1.17.215	5.252.153.241	3,475	235 kB	34	9,076	38.29%	3,475	235 kB	0	0 bytes	60.135270	3142.2528	599 b
10.1.17.215	45.125.66.32	3,737	587 kB	95	10,940	34.16%	3,737	587 kB	0	0 bytes	889.561525	1720.6308	2729 b