



Lab 1

BÁO CÁO BÀI THỰC HÀNH SỐ 1

Làm quen với Wireshark

Wireshark Getting Started

Môn học: Nhập môn Mạng máy tính

Sinh viên thực hiện	Lại Quan Thiên (22521385)
Thời gian thực hiện	04/10/2023 – 05/10/2023
Tự chấm điểm	10/10

File 22521385-Bail.pcapng:

1. Tổng thời gian bắt gói tin và tổng số gói tin bắt được là bao nhiêu?

- Tổng thời gian bắt gói tin: 2.650154 giây
- Tổng số gói tin bắt được: 162 gói

No.	Time	Source	Destination	Protocol	Length	Info
130	1.373969	8.8.8.8	192.168.1.3	TCP	60	443 → 64130 [ACK] Seq=2536 Ack=1136 Win=1845 Len=0 TSval=2646237173 TSecr=1937524397
131	1.375659	8.8.8.8	192.168.1.3	TCP	66	443 → 64130 [ACK] Seq=2536 Ack=1299 Win=1845 Len=0 TSval=2646237174 TSecr=1937524399
132	1.376187	8.8.8.8	192.168.1.3	TLSv1.2	372	Application Data
133	1.376189	8.8.8.8	192.168.1.3	TLSv1.2	565	Application Data
134	1.376190	8.8.8.8	192.168.1.3	TLSv1.2	97	Application Data
135	1.376190	8.8.8.8	192.168.1.3	TLSv1.2	385	Application Data
136	1.376191	8.8.8.8	192.168.1.3	TLSv1.2	149	Application Data
137	1.376191	8.8.8.8	192.168.1.3	TLSv1.2	598	Application Data
138	1.376666	8.8.8.8	192.168.1.3	TLSv1.2	150	Application Data
139	1.376667	8.8.8.8	192.168.1.3	TLSv1.2	565	Application Data
140	1.376667	8.8.8.8	192.168.1.3	TLSv1.2	97	Application Data
141	1.424845	192.168.1.3	8.8.8.8	TCP	66	64130 → 443 [ACK] Seq=1299 Ack=438 Win=2018 Len=0 TSval=1937524486 TSecr=2646237176
142	1.432589	192.168.1.3	8.8.8.8	TLSv1.2	185	Application Data
143	1.440449	192.168.1.3	128.119.245.12	TCP	78	64216 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=578808218 TSecr=0 SACK_PERM
144	1.450947	8.8.8.8	192.168.1.3	TCP	97	[TCP Spurious Retransmission] 443 → 64130 [PSH, ACK] Seq=4487 Ack=1299 Win=1845 Len=0 TSval=2646237176 TSecr=1937524404
145	1.452716	192.168.1.3	8.8.8.8	TCP	78	[TCP Dup ACK 141#] 64130 → 443 [ACK] Seq=1330 Ack=438 Win=2018 Len=0 TSval=1937524518 TSecr=2646237176
146	1.474683	8.8.8.8	192.168.1.3	TCP	60	443 → 64130 [ACK] Seq=4430 Ack=1330 Win=1845 Len=0 TSval=2646237174 TSecr=1937524404
147	1.492353	2403:300:a41:c801::	2403:300:a41:c801::	TCP	1586	443 → 57806 [ACK] Seq=6773 Ack=3459 Win=64128 Len=1428 TSval=1629964831 TSecr=1441539900 [TCP segm
148	1.492355	2403:300:a41:c801::	2403:300:a41:c801::	TLSv1.2	404	Application Data
149	1.505047	2403:300:a41:c801::	2403:300:a41:c801::	TCP	1586	[TCP Spurious Retransmission] 57806 → 443 [PSH, ACK] Seq=6773 Ack=3459 Win=64128 Len=1428 TSval=1629964831 TSecr=1441539900
150	1.505051	2403:300:a41:c801::	2403:300:a41:c801::	TCP	60	57806 → 443 [ACK] Seq=3459 Ack=6773 Win=64128 Len=0 TSval=1629964831 TSecr=1441539900
151	1.647070	2403:300:a41:c801::	2403:300:a41:c801::	TCP	98	[TCP Dup ACK 127#] 443 → 57806 [ACK] Seq=6511 Ack=3459 Win=64128 Len=0 TSval=1629964831 TSecr=1441539900
152	1.780449	128.119.245.12	192.168.1.3	TCP	66	80 → 64216 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM WS=128
153	1.781598	192.168.1.3	128.119.245.12	TCP	54	64216 → 80 [ACK] Seq=1 Ack=1 Win=202144 Len=0
154	1.786283	192.168.1.3	128.119.245.12	HTTP	558	GET /wiresark-labs/INTRO-wiresark-file.html HTTP/1.1
155	1.718855	192.168.1.3	128.119.245.12	TCP	78	64217 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3388128867 TSecr=0 SACK_PERM
156	2.4029754	128.119.245.12	192.168.1.3	TCP	54	80 → 64216 [ACK] Seq=1 Ack=585 Win=38336 Len=0
157	2.4029755	128.119.245.12	192.168.1.3	HTTP	293	HTTP/1.1 304 Not Modified
158	2.829929	192.168.1.3	128.119.245.12	TCP	54	64216 → 80 [ACK] Seq=585 Ack=248 Win=26188 Len=0
159	2.829932	192.168.1.3	128.119.245.12	TCP	66	80 → 64217 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM WS=128
160	2.321448	fe80::a86:da29:1db:f802::16	ff02::16	IGMPv6	170	Multicast Listener Report Message v2
161	2.649732	128.119.245.12	192.168.1.3	TCP	66	80 → 64217 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM WS=128
162	2.650154	192.168.1.3	128.119.245.12	TCP	54	64217 → 80 [ACK] Seq=1 Ack=1 Win=202144 Len=0

2. Liệt kê ít nhất 3 giao thức khác nhau xuất hiện trong cột giao thức (Protocol).

Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.

- 3 giao thức khác nhau trong cột Protocol: HTTP, UDP, TCP

- Mô tả:

+ HTTP (Hypertext Transfer Protocol):

Chức năng: HTTP là giao thức sử dụng trong trình duyệt web và máy chủ web để truyền tải dữ liệu giữa client và server. Nó được sử dụng chủ yếu để truy cập và trao đổi thông tin trên World Wide Web.

Đặc điểm chính: HTTP hoạt động dựa trên mô hình yêu cầu/hỏi đáp (request/response). Client gửi yêu cầu HTTP đến server, và server gửi phản hồi HTTP chứa dữ liệu trang web hoặc thông tin cần thiết trở lại cho client. Giao thức này thường sử dụng cổng 80 cho kết nối.

+ UDP (User Datagram Protocol):

Chức năng: UDP là giao thức truyền tải dữ liệu qua mạng mà không đảm bảo tính toàn vẹn hoặc giao diện. Nó thường được sử dụng cho các ứng dụng cần truyền tải dữ liệu nhanh và không cần đảm bảo mọi gói dữ liệu đều đến đích.

Đặc điểm chính: UDP là giao thức không kết nối, nghĩa là không có quá trình thiết lập kết nối như TCP. Nó truyền gói dữ liệu (datagram) độc lập, không đảm bảo thứ tự hoặc tính toàn vẹn dữ liệu. UDP sử dụng cổng để xác định dịch vụ hoặc ứng dụng cụ thể.

+ TCP (Transmission Control Protocol):

Chức năng: TCP là giao thức truyền tải dữ liệu qua mạng với tính toàn vẹn, đảm bảo thứ tự và kiểm soát lưu lượng. Nó thường được sử dụng cho các ứng dụng cần độ tin cậy trong việc truyền tải dữ liệu.

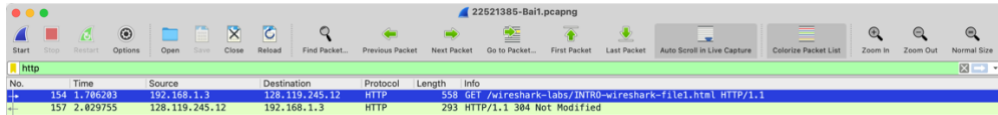
Đặc điểm chính: TCP hoạt động dựa trên mô hình kết nối, bắt đầu bằng quá trình thiết lập kết nối giữa client và server. Nó đảm bảo rằng dữ liệu được chia thành các gói, gửi đúng thứ tự và đảm bảo tính toàn vẹn. TCP sử dụng cổng để xác định dịch vụ hoặc ứng dụng cụ thể và thường sử dụng cổng 80 cho HTTP.

Gõ “http” vào packet-display filter sau đó chọn Apply để Wireshark chỉ hiển thị các thông điệp HTTP trong packet-listing window. Sau đó trả lời các câu hỏi sau:

3. Có bao nhiêu gói tin HTTP? Tỉ lệ % số gói tin HTTP/Tổng số gói tin?

- Có 2 gói tin HTTP trên tổng số 162 gói
- Tỉ lệ: 1,23%

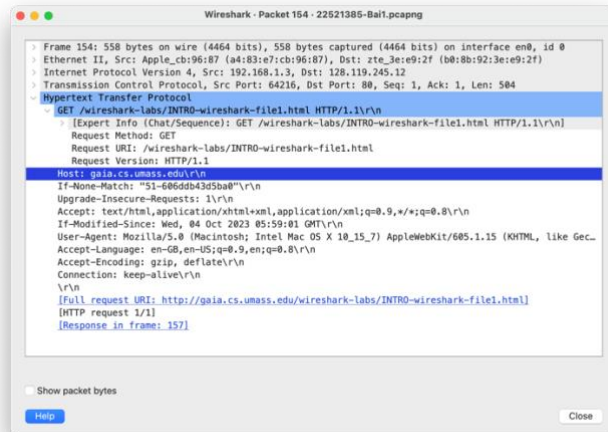
4. Có bao nhiêu gói tin HTTP GET? Có 1 gói tin HTTP GET.



5. Tìm và xác định gói tin HTTP GET đầu tiên được gửi đến web server gaia.cs.umass.edu?

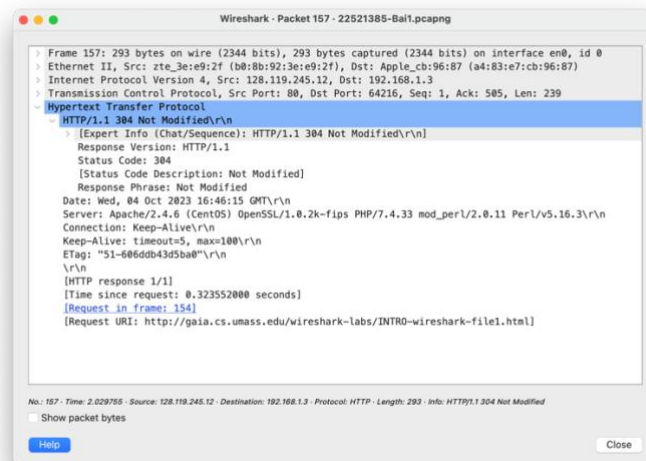
Một số thông tin của gói tin này (xem ảnh):

- Số: 154
- Host: gaia.cs.umass.edu



6. Xác định gói tin phản hồi cho gói HTTP GET ở trên (Câu 5)?

Một số thông tin của gói tin này (xem ảnh):



7. Mất bao lâu từ lúc gửi gói tin HTTP GET (Câu 5) đến khi nhận được gói tin phản hồi (Câu 6)? Mất 0,323552 giây

8. Dự đoán địa chỉ IP của gaia.cs.umass.edu là gì? Địa chỉ IP của máy tính đang sử dụng là gì? Tại sao?

No.	Time	Source	Destination	Protocol	Length	Info
154	1.706203	192.168.1.3	128.119.245.12	HTTP	558	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
157	2.029755	128.119.245.12	192.168.1.3	HTTP	293	HTTP/1.1 304 Not Modified

- Địa chỉ IP của “gaia.cs.umass.edu” là: 128.119.245.12

+ Xem trong phần Destination của WireShark

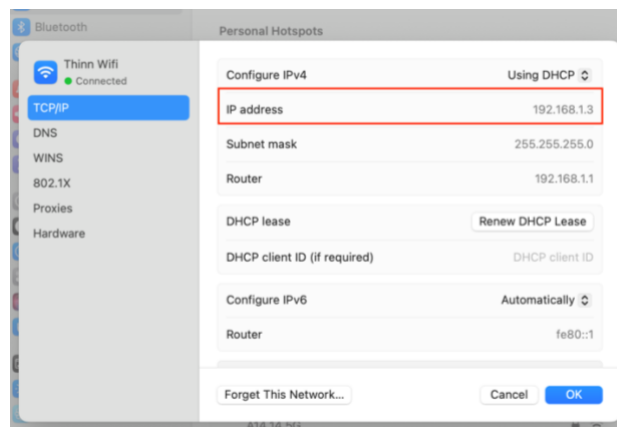
+ Hoặc dùng lệnh “nslookup gaia.cs.umass.edu” trên Terminal macOS

- Địa chỉ IP của máy tính đang sử dụng: 192.168.1.3

+ Xem trong phần Source của WireShark

+ Hoặc vào System Settings -> Wifi -> Details -> TCP/IP -> IP address

- Giải thích: Ta biết rằng, Source là địa chỉ nguồn và Destination là địa chỉ đích. Do đó, khi truy cập trang web, IP từ máy tính sẽ gửi Request đến trang web ta cần truy cập, ở đây có host là gaia.cs.umass.edu và nó cũng là địa chỉ đích. Dựa vào điều này, ta có thể dự đoán/xác định được địa chỉ IP của máy tính và trang web. Ngoài ra, ta có thể dùng lệnh trên Terminal để xác định (như đã trình bày ở trên)



File 22521385-Bai2.pcapng:

9. Tổng thời gian bắt gói tin và tổng số gói tin bắt được là bao nhiêu?

- Tổng thời gian bắt gói tin: 3,933490 giây
- Tổng số gói tin bắt được: 56 gói

No.	Time	Source	Destination	Protocol	Length	Info
24	3.588693	118.69.123.142	192.168.1.3	HTTP	708	Continuation
25	3.589184	192.168.1.3	118.69.123.142	TCP	66	64153 → 80 [ACK] Seq=478 Ack=10270 Win=123648 Len=0 TSval=1608494265 TSecr=3775872171
26	3.591280	192.168.1.3	118.69.123.142	TCP	66	[TCP Window Update] 64153 → 80 [ACK] Seq=478 Ack=10270 Win=131072 Len=0 TSval=1608494269 TSecr=3775872171
27	3.668126	192.168.1.3	8.8.8.8	TLSv1.2	249	Application Data
28	3.673389	192.168.1.3	8.8.8.8	TLSv1.2	258	Application Data
29	3.702917	192.168.1.3	118.69.123.142	HTTP	544	GET /select2/ajax/get_settings HTTP/1.1
30	3.705952	8.8.8.8	192.168.1.3	TCP	66	443 → 64130 [ACK] Seq=1 Ack=184 Win=807 Len=0 TSval=2645530655 TSecr=1936817798
31	3.707761	118.69.123.142	192.168.1.3	TCP	66	80 → 64153 [ACK] Seq=10270 Ack=956 Win=31104 Len=0 TSval=3775872292 TSecr=1608494380
32	3.710734	8.8.8.8	192.168.1.3	TCP	66	443 → 64130 [ACK] Seq=1 Ack=368 Win=814 Len=0 TSval=2645530571 TSecr=1936817803
33	3.712603	8.8.8.8	192.168.1.3	TLSv1.2	172	Application Data
34	3.712606	8.8.8.8	192.168.1.3	TLSv1.2	565	Application Data
35	3.712809	192.168.1.3	8.8.8.8	TCP	66	64130 → 443 [ACK] Seq=368 Ack=606 Win=2038 Len=0 TSval=1936817842 TSecr=2645530573
36	3.712896	8.8.8.8	192.168.1.3	TLSv1.2	97	Application Data
37	3.712897	8.8.8.8	192.168.1.3	TLSv1.2	105	Application Data
38	3.713800	192.168.1.3	8.8.8.8	TCP	66	64130 → 443 [ACK] Seq=368 Ack=676 Win=2046 Len=0 TSval=1936817842 TSecr=2645530573
39	3.714110	192.168.1.3	8.8.8.8	TLSv1.2	105	Application Data
40	3.743182	2405:4802:a47d:54e::	2a02:26f7:16:2:a::	UDP	601	60072 → 443 Len=539
41	3.755972	8.8.8.8	192.168.1.3	TLSv1.2	158	Application Data
42	3.755974	8.8.8.8	192.168.1.3	TLSv1.2	565	Application Data
43	3.756216	8.8.8.8	192.168.1.3	TLSv1.2	97	Application Data
44	3.756218	8.8.8.8	192.168.1.3	TLSv1.2	105	Application Data
45	3.756970	192.168.1.3	8.8.8.8	TCP	66	64130 → 443 [ACK] Seq=407 Ack=1337 Win=2037 Len=0 TSval=1936817886 TSecr=2645530616
46	3.757472	192.168.1.3	8.8.8.8	TLSv1.2	105	Application Data
47	3.793054	2a02:26f7:16:2:a::	2405:4802:a47d:54e::	UDP	94	443 → 60072 Len=32
48	3.799227	8.8.8.8	192.168.1.3	TCP	66	443 → 64130 [ACK] Seq=1337 Ack=446 Win=814 Len=0 TSval=2645530659 TSecr=1936817886
49	3.803411	2a02:26f7:16:2:a::	2405:4802:a47d:54e::	UDP	207	443 → 60072 Len=145
50	3.803739	2a02:26f7:16:2:a::	2405:4802:a47d:54e::	UDP	163	443 → 60072 Len=101
51	3.803740	2a02:26f7:16:2:a::	2405:4802:a47d:54e::	UDP	136	443 → 60072 Len=74
52	3.826458	2405:4802:a47d:54e::	2a02:26f7:16:2:a::	UDP	96	60072 → 443 Len=34
53	3.827171	2405:4802:a47d:54e::	2a02:26f7:16:2:a::	UDP	134	60072 → 443 Len=72
54	3.827445	2a02:26f7:16:2:a::	2405:4802:a47d:54e::	UDP	94	443 → 60072 Len=32
55	3.931203	118.69.123.142	192.168.1.3	HTTP/1.1	1442	HTTP/1.1 200 OK, JavaScript Object Notation (application/json)
56	3.933490	192.168.1.3	118.69.123.142	TCP	66	64153 → 80 [ACK] Seq=956 Ack=11646 Win=129664 Len=0 TSval=1608494611 TSecr=3775872515

10. Liệt kê ít nhất 3 giao thức khác nhau xuất hiện trong cột giao thức (Protocol). Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.

- 3 giao thức khác nhau trong cột Protocol: HTTP, UDP, TCP
- Mô tả:

+ HTTP (Hypertext Transfer Protocol):

Chức năng: HTTP là giao thức sử dụng trong trình duyệt web và máy chủ web để truyền tải dữ liệu giữa client và server. Nó được sử dụng chủ yếu để truy cập và trao đổi thông tin trên World Wide Web.

Đặc điểm chính: HTTP hoạt động dựa trên mô hình yêu cầu/hồi đáp (request/response). Client gửi yêu cầu HTTP đến server, và server gửi phản hồi HTTP chứa dữ liệu trang web hoặc thông tin cần thiết trở lại cho client. Giao thức này thường sử dụng cổng 80 cho kết nối.

+ UDP (User Datagram Protocol):

Chức năng: UDP là giao thức truyền tải dữ liệu qua mạng mà không đảm bảo tính toàn vẹn hoặc giao diện. Nó thường được sử dụng cho các ứng dụng cần truyền tải dữ liệu nhanh và không cần đảm bảo mọi gói dữ liệu đều đến đích.

Đặc điểm chính: UDP là giao thức không kết nối, nghĩa là không có quá trình thiết lập kết nối như TCP. Nó truyền gói dữ liệu (datagram) độc lập, không đảm bảo thứ tự hoặc tính toàn vẹn dữ liệu. UDP sử dụng cổng để xác định dịch vụ hoặc ứng dụng cụ thể.

+ TCP (Transmission Control Protocol):

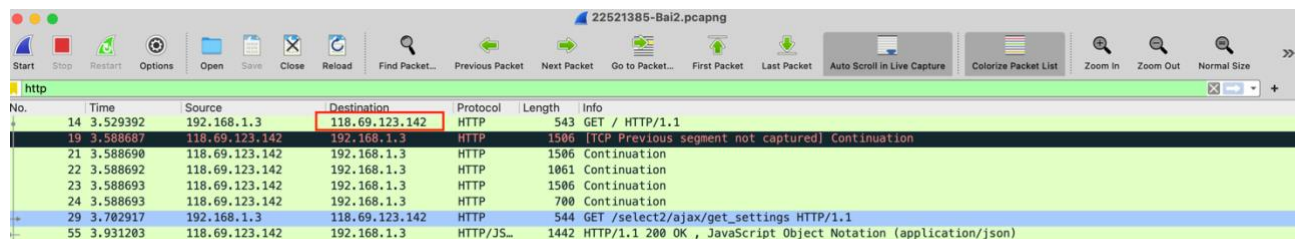
Chức năng: TCP là giao thức truyền tải dữ liệu qua mạng với tính toàn vẹn, đảm bảo thứ tự và kiểm soát lưu lượng. Nó thường được sử dụng cho các ứng dụng cần độ tin cậy trong việc truyền tải dữ liệu.

Đặc điểm chính: TCP hoạt động dựa trên mô hình kết nối, bắt đầu bằng quá trình thiết lập kết nối giữa client và server. Nó đảm bảo rằng dữ liệu được chia thành các gói, gửi đúng thứ tự và đảm bảo tính toàn vẹn. TCP sử dụng cổng để xác định dịch vụ hoặc ứng dụng cụ thể và thường sử dụng cổng 80 cho HTTP.

11. Tìm cách để xác định địa chỉ IP của trang web đã chọn ở Bước 8. Địa chỉ IP trang web đã chọn là gì?

- Cách xác định địa chỉ IP của trang web celuit.edu.vn:

+ Xem trong phần Destination của WireShark:



No.	Time	Source	Destination	Protocol	Length	Info
14	3.529392	192.168.1.3	118.69.123.142	HTTP	543	GET / HTTP/1.1
19	3.588687	118.69.123.142	192.168.1.3	HTTP	1506	[TCP Previous segment not captured] Continuation
21	3.588690	118.69.123.142	192.168.1.3	HTTP	1506	Continuation
22	3.588692	118.69.123.142	192.168.1.3	HTTP	1061	Continuation
23	3.588693	118.69.123.142	192.168.1.3	HTTP	1506	Continuation
24	3.588693	118.69.123.142	192.168.1.3	HTTP	700	Continuation
29	3.702917	192.168.1.3	118.69.123.142	HTTP	544	GET /select2/ajax/get_settings HTTP/1.1
55	3.931203	118.69.123.142	192.168.1.3	HTTP/JS	1442	HTTP/1.1 200 OK, JavaScript Object Notation (application/json)

+ Hoặc dùng lệnh “nslookup celuit.edu.vn” trên Terminal macOS:

```
Last login: Wed Oct 4 23:20:02 on ttys000
thinnn@Thinnn-Mac ~ % nslookup celuit.edu.vn
Server:      8.8.8.8
Address:     8.8.8.8#53
```

Non-authoritative answer:

Name: celuit.edu.vn

Address: 118.69.123.142

- Do đó, địa chỉ IP của “celuit.edu.vn” là:

+ Name: celuit.edu.vn

+ IP Address: 118.69.123.142

12. Số lượng gói tin và khối lượng dữ liệu được gửi (trao đổi) giữa Địa chỉ trang web ở trên (Câu 11) và máy tính đang sử dụng ?

- Địa chỉ trang web đã chọn ở Bước 8: 118.69.123.142

- Địa chỉ máy tính đang sử dụng: 192.168.1.3

- Vậy số lượng gói tin trao đổi là 20, khối lượng dữ liệu là 14kB

Wireshark - Conversations - 22521385-Bai2.pcapng

Conversation Settings

☐ Name resolution

☐ Absolute start time

☒ Limit to display filter

Ethernet · 1

IPv4 · 1

IPv6

TCP · 1

UDP

Address A	Address B	Packets ▾	Bytes	Total Packets	Percent Filtered
192.168.1.3	118.69.123.142	20	14 kB	20	100.00%