

Wireshark: Packet Operations



Lab Summary

In this lab i used Wireshark to analyze network traffic. I practiced using filters to find IP addresses, hostnames, and DNS queries, and checked protocol details and statistics to understand the communication between devices.

Learning Objectives

- Investigate network traffic captures
- View statistics including summary and protocol details
- Uncover and apply packet filtering principles
- Apply protocol filters
- Apply advanced filtering

In this lab, we will use the “Exercise.pcapng” file for analysis.



Lab provided by TryHackMe

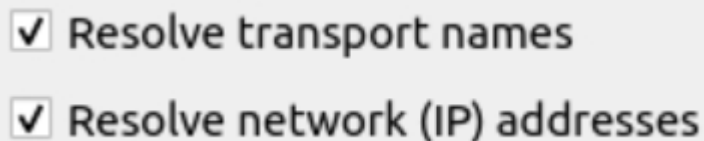
Made and documented by Fábio Vieira

Wireshark: Packet Operations.....	1
Lab Summary	1
Learning Objectives.....	1
Q1. Investigate the resolved addresses. What is the IP address of the hostname starts with "bbc"?	3
Q2. How many bytes (k) were transferred from the "Micro-St" MAC address?	4
Q3. Which IP address is linked with "Blicnet" AS Organisation?	5
Q4. What is the most used IPv4 destination address?	6
Q5. What is the max service request-response time of the DNS packets?	7
Protocol/IP Filters	8
Advanced Filtering.....	9
Conclusion	11

Q1. Investigate the resolved addresses. What is the IP address of the hostname starts with "bbc"?

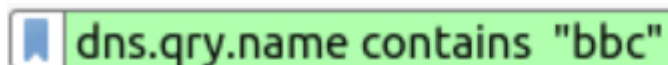
To answer the question, I had to go to **Edit → Preferences → Name Resolution** and enable the options “Resolve transport names” and “Resolve network (IP) addresses.”

This allowed Wireshark to translate IP addresses and port numbers into hostnames and protocol names.



☒ Resolve transport names
☒ Resolve network (IP) addresses

Then, I used the filter **dns.qry.name contains "bbc"** to search for DNS queries related to the hostname.



dns.qry.name contains "bbc"

This allowed me to locate the DNS response associated with bbc, where I found the corresponding IP address in the “Answer” section of the packet details.



Address: **bbc.map.fastly.net (199.232.24.81)**

Q2. How many bytes (k) were transferred from the "Micro-St" MAC address?

To determine how many bytes were transferred from the Micro-St device, I opened Statistics → Conversations → Ethernet in Wireshark.

The MAC address 40:61:86:9a:f1:f5 was identified as the Micro-St device.

In the Ethernet conversations table, I located every row where this MAC appeared, either in the Address A or Address B columns. Then, I added all the bytes where Micro-St sent or received data:

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Sta
00:04:00:81:81:d0	40:61:86:9a:f1:f5	16	1952	8	992	8	960	
00:14:5e:6b:72:00	40:61:86:9a:f1:f5	16	1968	6	558	10	1410	
00:1a:8c:15:f9:80	40:61:86:9a:f1:f5	10421	7466 k	6170	6389 k	4251	1077 k	
01:00:5e:00:00:fc	40:61:86:9a:f1:f5	2	128	0	0	2	128	
01:00:5e:7f:ff:fa	40:61:86:9a:f1:f5	6	996	0	0	6	996	
40:61:86:9a:f1:f5	ff:ff:ff:ff:ff:ff	17	2934	17	2934	0	0	

(992 + 558 + 6389k + 0 + 0) received

(960 + 1410 + 1077k + 128 + 996 + 2934) sent

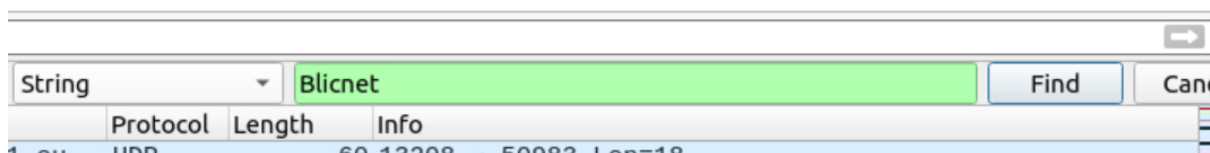
Total bytes:

7,473,978 bytes = ≈ 7474 kB

Q3. Which IP address is linked with "Blicnet" AS Organisation?

To find which IP address was associated with the "Blicnet" AS organisation, I did not filter by protocol. Instead, I searched inside the captured packets by name.

1. In Wireshark I went to Edit → Find Packet.
2. In the search window I selected String (not Display Filter) and searched in Packet bytes (you can also use “Packet details” depending on the lab).



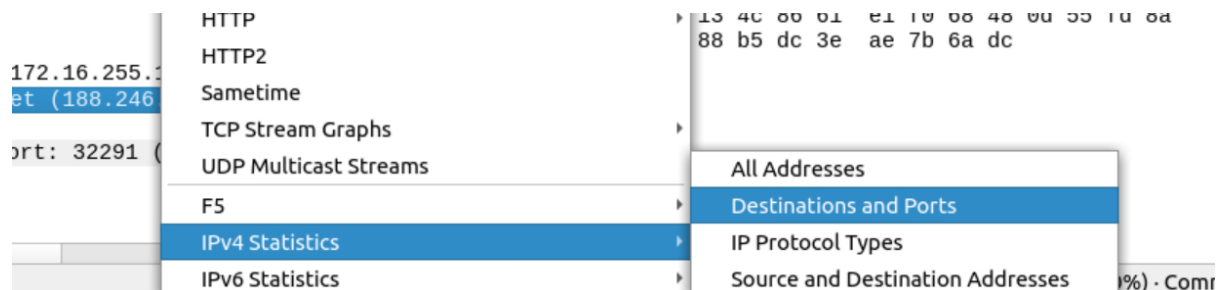
3. Wireshark jumped to the packet where the text "Blicnet" appeared. This text came from the ASN/organisation information present in that conversation.
4. In that same packet/conversation I looked at the IP information (source/destination IP) and identified the IP address that was associated with the “Blicnet” organisation.

broadband.blic.net (188.246.82.7)

Q4. What is the most used IPv4 destination address?

To identify which IPv4 destination address was used the most in the capture, I followed these steps:

1. In Wireshark, I went to Statistics → IPv4 Statistics
→Destinations.



2. This section lists all IPv4 destination addresses along with their respective packet counts.
3. I sorted the column Packets in descending order to see which IP address had the highest number of packets received.
4. The address with the largest count was 10.100.1.33, making it the most used IPv4 destination address in this capture.

Topic / Item	Count ^
▼ Destinations and Ports	81420
▼ 10.100.1.33	29387

Q5. What is the max service request-response time of the DNS packets?

To find the maximum service request–response time for DNS packets, I used Wireshark’s built-in DNS statistics:

1. I opened Statistics → DNS.
2. This section provides several metrics, including payload size, query/response stats, and service stats.
3. Under Service Stats, I looked at the request–response time (secs) field.
4. The Max val column showed the highest measured time for DNS requests and responses.
5. The maximum value shown was **0.467897** seconds.

Topic / Item	Count	Average	Min val	Max val ▼	Rate (m)	Percent
Payload size	171	107.75	29	502	0.0000	100%
▸ Query Stats	0				0.0000	100%
▸ Response Stats	0				0.0000	100%
▼ Service Stats	0				0.0000	100%
request-response time (secs)	85	0.07	0.000075	0.467897	0.0000	
no. of retransmissions	0				0.0000	
no. of unsolicited responses	0				0.0000	
▼ Total Packets	171				0.0000	100%

Protocol/IP Filters

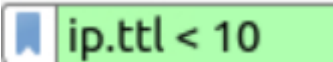
Wireshark supports 3000 protocols and allows packet-level investigation by filtering the protocol fields. This task shows the creation and usage of filters against different protocol fields.

What is the number of IP packets?

 ip

Displayed: 81420

What is the number of packets with a "TTL value less than 10"?

 ip.ttl < 10

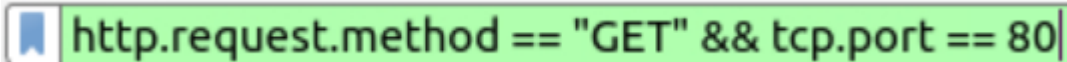
Displayed: 66

What is the number of packets which uses "TCP port 4444"?

 tcp.port == 4444

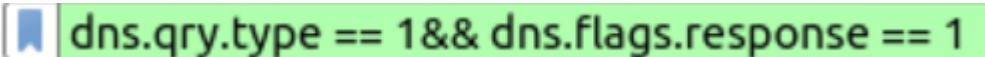
Displayed: 632

What is the number of "HTTP GET" requests sent to port "80"?

 http.request.method == "GET" && tcp.port == 80

Displayed: 527

What is the number of type A DNS Queries"?

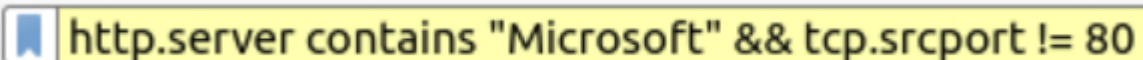
 dns.qry.type == 1&& dns.flags.response == 1

Displayed: 51

Advanced Filtering

Now it is time to focus on specific packet details for the event of interest. Besides the operators and expressions covered in the previous room, Wireshark has advanced operators and functions. These advanced filtering options help the analyst conduct an in-depth analysis of an event of interest.

Find all Microsoft IIS servers. What is the number of packets that did not originate from "port 80"?



```
http.server contains "Microsoft" && tcp.srcport != 80
```

Displayed: 21

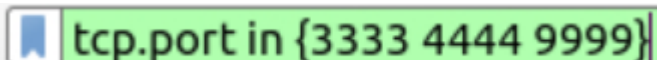
Find all Microsoft IIS servers. What is the number of packets that have "version 7.5"?



```
http.server contains "Microsoft-IIS/7.5"
```

Displayed: 71


What is the total number of packets that use ports 3333, 4444 or 9999?



```
tcp.port in {3333 4444 9999}
```

Displayed: 2235

What is the number of packets with "even TTL numbers"?

 string(ip.ttl) matches "[02468]\$" |

Displayed: 77289

Change the profile to "Checksum Control". What is the number of "Bad TCP Checksum" packets?

Profile	Type
Default	Default
Checksum Control	Personal
Bluetooth	Global
Classic	Global
No Reassembly	Global

 tcp.checksum.status == 0 |

Displayed: 34185

Use the existing filtering button to filter the traffic. What is the number of displayed packets?

 gif/jpeg with http-200 |

Displayed: 261

Conclusion

This lab strengthened my practical skills in network inspection, protocol analysis, and the use of Wireshark as a tool for cybersecurity monitoring and incident investigation.