4.1

What is the total size of 1327 pieces of captured frames?
972kB
- What is the average bandwidth of the network traffic for 6 seconds?
Bandwidth = size/time = 3816 bytes/6 seconds = $\frac{3816\times8}{6}$ = 5088 bits/second
4507
C) How many frames were transferred through the NIC for 6 seconds?
29
D) What is the average frame size transferred for 6 seconds?
$\frac{3816}{29} = 132$
115

Based on the Wireshark capture justify your answer to the following questions:
- What is the compression ratio in the case of pcap and txt file types?
Size of pcap file = 501KB
Size of txt file = 2.3MB
Compression ratio = size of pcap file/size of txt file = $\frac{501}{2300} = 0.2178$
What is the compression ratio in the case of pcap and pcapng file types?
size of pcap file = 501 KB
size of pcapng = 509 KB
Compression ratio = size of pcap file/size of pcapng = $\frac{501}{509} = 0.984$

4.2

Time diagrams
ARP/RARP
ICMP
ICMPv6
IPv4
IPv6
TCP
UDP

What is the OUI code of the Cisco company?
000142
What is the MAC address of the NIC module of your PC?
d0:88:0c:93:d3:1a
Where can you find the MAC OUI identifiers of NIC manufacturing companies on the Internet?
B) Identify the NIC MAC values according to the following questions:
Where can you find the MAC OUI identifiers of NIC manufacturing companies on the Internet?

IEEE Standards Association (IEEE-SA) Registration Authority
Wireshark OUI Lookup

What are the MAC OUI codes of the following NIC manufacturing companies: Cisco, HP, Apple, Xiaomi, Huawei?
Cisco - 00:00:0C Cisco Systems, Inc
HP - 00:16:B9 ProCurve Networking by HP
Apple - 00:03:93 Apple, Inc.
Xiaomi - 00:9E:C8 Xiaomi Communications Co Ltd
Huawei - 00:18:82 Huawei Technologies Co.,Ltd

4.3

A) What is the capture rule which filters the network traffic of your own PC in the case of Wireshark?
Use the filter rule: `host <your_PC_IP_address>`
B) What is the capture rule which filters only those frames that are sent for the broadcast address in the case of Wireshark?
Use the following capture rule: `dst host 255.255.255.255`

4.4

A) What is the display rule which filters the network traffic of your own PC in the case of Wireshark?
Use the following display filter expressions: `ip.src == <your_IP_address> or ip.dst == <your_IP_address>`
B) What is the display rule which filters only those frames that are sent for the broadcast address in the case of Wireshark?
`eth.dst == ff:ff:ff:ff:ff:ff`

4.5

A) In the case of Wireshark where can we find the tail of the captured frame?
In Wireshark, we can find the tail of the captured frame in the ”Frame” section of the packet details pane.
B) What do ”.” characters indicate in the bottom field?
The ”.” characters indicate non-printable characters or bytes that cannot be represented as regular ASCII characters.