# Exercise
# for Lecture “P2P Systems”

**Prof. Dr. David Hausheer**
**Dipl.-Wirtsch.-Inform. Matthias Wichtlhuber, Leonhard Nobach, M. Sc., Dipl.-Ing. Fabian Kaup, Christian Koch, M. Sc., Dipl.-Wirtsch.-Inform. Jeremias Blendin**

**Summer Term 2015**
**Exercise No. 4**
**Published at: 12.05.2015, Submission date: 19.05.2015**
**Submission via Moodle.**
**Contact:** [mwichtlh|lnobach|fkaup|ckoch|jblendin]@ps.tu-darmstadt.de
**Web:** http://www.ps.tu-darmstadt.de/teaching/p2p/
**– Example Solution –**

*Prerequisite:* In this exercise traces from an RB-Horst social access point will be analyzed. Therefore it is required to install Wireshark (from: https://www.wireshark.org)

*Note:* Tasks marked with † are to be submitted by students participating in the RB-Horst study. The tasks marked with ∗ are to be submitted by all other course participants.

## Problem 4.1 - Getting data for analysis

### a) Study participants†

☐ Connect with your laptop to your RB-Horst AP.

☐ Go to http://192.168.1.40:8082/tcpdump/

☐ Click "start tcpdump" to record a 30 second sample of network activity

☐ Download the file after the tcpdump has returned

### b) Other course participants*

☐ Download the file tcpdump.pcap from Moodle

## Problem 4.2 - Analysing a TCP dump using wireshark

In the following, the recorded TCP dumps will be analyzed to determine basic information on the exchanged information, participating devices, and network configuration.

### a) What types of communication can you observe in the dumps according to the OSI/ISO layers?

The OSI communication model defines a layered architecture for communcation between networked devices. The available TCP dumps contain information recorded on the network interface of the RB-Horst access point. Above which layer according to the OSI model is communication visible in the TCP dump?

- ☐ all above layer 1
- ☐ all above layer 2
- ☐ all above layer 3
- ☐ all above layer 4

**Solution:** Answer 1 (Physical Layer)

### b) Give an example of a network protocol found in the dump working on the following layers:

Data transmisssions in communication networks are based on a layered architecture according to the OSI network layers. These are visible in the recorded TCP dumps. Give an example of a communication protocol working on the respective OSI layer as indicated in the following list:

1 **Solution:** Ethernet/IEEE 802.3

2 **Solution:** ARP/IEEE 802.3

3 **Solution:** IP

4 **Solution:** TCP/UDP

>4 **Solution:** HTTPs, DNS

**Solution:** Check `https://en.wikipedia.org/wiki/OSI_model` and determine, which protocols from each layer can be found in the dump

## c) Basic network configuration

All network configuration is conducted via the network itself. Hence, a majority of network configuration parameters can be derived from the recorded TCP dump. Analyze the dump and derive the following configuration parameters:

MAC: **Solution:** 00:1e:06:ce:44:ee

IP: **Solution:** 192.168.1.218

Gateway: **Solution:** 192.168.1.1

DNS server: **Solution:** 192.168.1.1

**Solution:** The network configuration can be determined in a variety of ways.

A) Search for ARP packets to determine the MAC addresses (clearly, TP-Link is the router, hence the address ending in `ce:44:ee` is the local machine). From this, also the local IP and the IP of the gateway can be derived.

B) DNS requests are sent from the local machine (192.168.1.218) to 192.168.1.1, hence this machine works as a DNS server. This packet also conatains the MAC and respective IP addresses.

## d) Analysis of communication patterns

Which versions of the IP protocol are configured on the RB-Horst access point?

**Solution:** IPv4, no IPv6 packets can be found (filter: `ipv6`)

On which ports is the RB-Horst access point listening/receiving data? Also give the filter expression used!

**Solution:** 8443, 57821

Detailed solution: First filter for packets received (`ip.dst == 192.168.1.218`) and find port 8443. Then filter out these packets (`ip.dst == 192.168.1.218 && tcp.dstport != 8443`) to determine other ports receiving data.

Can you find an SSL certificate in the recorded dump? If yes, for which domain is it issued? Also give the filter expression used!

**Solution:** find using filter: "ssl.handshake.certificate", certificate for websrv.ps.tu-darmstadt.de

By which IPs is the RB-Horst access point contacted? Give at least three IPs. Also give the filter expression used! (*Hint:* lots of communication involves port 8443)

**Solution:** Two alternatives:

A) filter `ip.dst == 192.168.1.218 && tcp.dstport == 8443` and write down IPs

B) Easier: Select "Statistics" > "Conversations" > Select Tab "IPv4" > Write down IPs

84.72.44.30, 130.83.7.207, 130.83.20.2, ...

How many packets are exchanged during each of these transactions? Describe the typical communcation pattern on port 8443! Particularly observe the TCP flags and conclude, what is happening!

**Solution:** Two possible solutions:

A) Find using filter `tcp.port == 8443`

B) Right-click on a TCP packet and select "Follow TCP Stream"

Number of packets typically exchanged: 8 TCP: SYN, SYN-ACK, ACK, PSH-ACK, ACK, PSH-ACK, ACK, RST-ACK; only two of them containing data frames. 3 Packets for connection establishment, 2x Data + ACK, 1x connection close.