Exercise
for Lecture “P2P Systems”

TECHNISCHE UNIVERSITÄT DARMSTADT

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. 5
Published at: 19.05.2015, Submission date: 26.05.2015
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 uses 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 5.1 - Getting data for analysis

Hint: You may reuse the tcpdump from the last lab session. However, please ensure you have a tcpdump.pcap and a logs.zip file before working on this exercise.

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

☐ Download the file logs.zip from Moodle

b) Other course participants*

☐ Download the file tcpdump.pcap from Moodle

☐ Download the file logs.zip from Moodle

Problem 5.2 - Analysis of DHT Traffic

In the following, the traffic of RB-HORST's Distributed Hash Table (DHT) will be analyzed using Wireshark and the tcpdump.pcap file.

a) What types of transport protocols are used by the DHT to communicate? Please write down the answer and Wireshark's filtering expression.

Hint: The DHT is using port 8443

Solution: TCP and UDP, filtering expression: tcp.port == 8443 || udp.port == 8443 or use Statistics > Conversations

b) List the neighbors of the access point in the DHT. Please write down the answer and Wireshark's filtering expression.

Hint: There is traffic related to several other nodes, e.g., the logging server. If you filter for the DHT's port, this side traffic will not be displayed.

Solution: IPs: 84.72.44.30, 130.83.7.207, 130.83.20.2 , 85.2.4.225, 130.83.125.102, 89.217.169.104, 130.83.19.194; ip.dst==192.168.1.218 && (tcp.dstport == 8443 || udp.dstport == 8443)

c) The DHT regularly sends keep-alive messages (PING). Which transport protocol is used for that? Please write down the answer and Wireshark's filtering expression.

Hint: The size of a IP packet that contains a keep-alive message *with* header is 177 bytes.

Solution: UDP, ip.len==177

d) Host 85.2.4.225 signs in to the overlay and stores data on himself in the DHT using TCP. What information on the the host are sent along with the data? Please write down the answer and Wireshark's filtering expression.

Hint: The messages are serialized by Java, which makes them hard to read. However, you can find clear text hints from bytes 00d0 to 01c0, if you have found the right packets.

Solution: Hop Count, longitude and latitude, port, address, IP, MAC; ip.src == 85.2.4.225 && tcp.port==8443

Problem 5.3 - Analysis of RB-HORST internal logs

In the following, the different logs from the access point's internal logging directory are examined using the logs.zip file. The logging directory has the following structure:

```
tmp_1432029691
+-monitoring
 +-cpu_utilization.log
 +-memory_utilization.log
 +-network_utilization.log
 +-prefiltered_eth0.log
 +-storage_utilization.log
+-overall.log
+-social.log
+-unada.log
+-web.log
```

a) Start by examining unada.log. This file contains all debug messages of the RB-HORST application. Can you find out the name of the DHT distribution?

Hint: Look for typical DHT operations.

Solution: TOMP2P based on Netty

b) The social.log file contains all friends of the access point owner. How many friends are listed?

Hint: The first line is the access point owner himself.

Solution: There are 8 friends and the owner himself.

c) The file prefiltered_eth0.log contains preprocessed logs on the accumulated network traffic in bytes on the ethernet interface. The sampling interval is 1 second. Visualize the traffic on interface eth0 using a program of your choice (e.g., Excel, Python or similar). Can you identify a running upload or download?

Solution: Yes, upload and downloads are running.

d) The file overall.log contains the social prediction and caching logs. How many videos have been prefetched?

Solution: 7 videos were prefetched.