TECHNISCHE UNIVERSITÄT BERLIN
Fakultät IV – Elektrotechnik und Informatik
Fachgebiet Intelligente Netze
Prof. Anja Feldmann, Marco Canini, Petr Kuznetsov, Stefan Schmid
Arne Ludwig, Oliver Hohlfeld, Juhoon Kim, Thomas Krenc, Enric Pujol, Felix Poloczek

8th Assignment: Network Protocols and Architectures, WS 12/13

Question 1: $(15 + 10 + 10 + 15 + 20 + 20 + 10 = 100$ points) *Traffic Analysis*

You are now going to analyse real traffic using the traffic analysis tool Wireshark[1]. To begin with, open `u08-trace.pcap`[2] using Wireshark. Wireshark provides a huge set of analysers that are useful for various analysis tasks. However, for the sake of understanding the core concepts, start using them once you understand how they work and you know how to get the same result manually using pure display filters.

The following analysers will be very useful for this exercise:

- Select a single flow: right click on a packet and select *Follow TCP Stream* in the context menu
- Plot sequence diagrams: Statistics → Flow Graph → TCP flow → OK

This list is not exhaustive and much more analysers can be applied when solving this assignment—although they do not need to. Moreover, you will need to define display filters. Please find an introduction in the Wireshark manual[3].

Important note: The journey is the reward; just stating the solution to the questions posed below is *not* a sufficient answer. You must include a description on how the results were obtained in your solution. For instance, when you used display filters, copy them into your solution. This description should also reflect the methodology you were using, e.g., how and why different filters were combined.

(a) How many TCP connections are contained in the trace? When do the connections start, when are they terminated? How do you detect the start / end of a TCP connection? Are there any parallel connections? Are there any UDP flows?

Solve this problem for one flow using display filters only (Hint: filter by connection flags). For the others, you *can* use automatic analysers.

(b) Do you observe packet losses in TCP flows? Give one example.

(c) Which hosts exist in the trace? Which services does each host provide? Which application layer protocols are used? What are the servers and what are the clients?

(d) Obtain the DNS names of the observed hosts only by information contained in the trace. Show for one host how analysing DNS traffic reveals the answer. Describe how you infer this information from the DNS traffic. Automatic analysers of Wireshark can be used to resolve the names of the remaining hosts. Which hosts do not have an DNS name?

(e) For each connection you observe, answer the following questions: i) What is the user doing / what is requested? ii) Which information is disclosed (passwords, etc.)? This is not possible for all flows. If you cannot reveal this information, justify why this is not possible.

(f) What can you infer about the network topology by considering layer 2 information: The traffic was captured in one LAN, which other hosts are located in the same LAN? Hint: filter by MAC addresses and analyse their usage. Remember how MAC addresses are used for addressing and when they are rewritten. Which hosts have multiple IP addresses?

[1] `http://www.wireshark.org/`
[2] `https://www.isis.tu-berlin.de/mod/resource/view.php?id=302686`
[3] `http://www.wireshark.org/docs/wsug_html_chunked/ChWorkDisplayFilterSection.html`

(g) Analyse packets 18 to 20. Which application layer protocol is used here? What is the semantic of those packets? Can you find evidence for this semantic to be applied in the remainder of the connection?

Due Date: Thursday, December, 20th 2012 only until 13:55 h s. t.

- **As PDF files (no MS Office or OpenOffice files):** Uploaded via ISIS (`https://www.isis.tu-berlin.de/course/view.php?id=7028`)
- **On paper:** Postbox in the Telefunkenhochhaus (basement, behind the doorman right)
- Put your name, StudentID number (Matrikelnummer) **and** the name of your tutor on your solution.