MIC0003: Computer Networking
Homework II: Network Traffic Analysis

Deadline: 30 May, 2011

The goal of this homework is for you to learn the basics of network traffic analysis, to familiarize yourselves with one of the most widely used traffic capture and analysis tool, as well as to have an overall impression of the amount and type of data that crosses the network day-to-day.

1 Assignment

For this homework you'll be required to analyze a pre-captured network traffic using the Wireshark[1] program. You are free to structure your final report as you like, but it should be clear and to the point. Figures and images are also very welcome. As a starting point, you might consider these questions:

- What IP and MAC addresses do you encounter?
- Is the network topology reconstructable (hosts, names, gateways, servers, etc.)?
- Did a certain computer use Ethernet or WiFi?
- What kind of higher and lower level protocols are present?
- Which connections use TCP and which UDP? Why?
- What kind of transport layer protocols are present?
- Does the IP segmentation provide any information?
- What information can you gather about the hosts (OS, browser, etc.)?
- Can you reconstruct any data from the captured traffic?
- Is there any sensitive information?
- What other interesting things can you find in the trace file?

2 Notes

- Quality is preferred over quantity (i.e. you get points on the information content, not the length of the report).
- Figures are strongly suggested, at least for the network topology.

[1] http://www.wireshark.org/

3 Deliverables

The final report is due on the date specified in the header, delivered personally. Late submissions result in a failed assignment.

The report can either be hand written or prepared in a digital form (i.e. pdf), but in either case it should have a professional look. The minimal administrative information it must contain are your names, usernames and groups.