Technische Universität München
Lehrstuhl Informatik VIII
Prof. Dr.-Ing. Georg Carle
Christian Grothoff, Ph.D.
Stephan M. Günther, M.Sc.

Master Course Computer Networks

Homework 1
(submission until November 5th into INBOX located in front of 03.05.052)

Note: Subproblems marked by * can be solved without preceding results.

Understanding encapsulation (Doing what Wireshark does)

Figure 1 shows the hexdump of some frame captured on a wired network (Ethernet II frame format). The dump contains the whole frame (except its FCS) beginning with the target MAC address. Now we will figure out the contents ...

```
0000   00 25 90 57 1f dc 28 37   37 02 32 41 08 00 45 00
0010   00 42 99 a8 00 00 40 11   b6 9e 83 9f 14 59 83 9f
0020   0e cd d4 1e 00 35 00 2e   c2 25 c2 51 01 00 00 01
0030   00 00 00 00 00 00 06 73   6c 61 63 6b 79 03 6e 65
0040   74 02 69 6e 03 74 75 6d   02 64 65 00 00 01 00 01
```

Figure 1: Hexdump, leftmost column indicates the hex offset from the beginning of the frame.

a)* Sketch the Ethernet II frame format, i. e. header fields and their length.

b)* What is the FCS being used for?

Here is a list of RFCs that might be helpful in decoding the frame:

- http://www.ietf.org/rfc/rfc791.txt
- http://www.ietf.org/rfc/rfc768.txt
- http://www.ietf.org/rfc/rfc1034.txt

The following two links help you figuring out which protocols are encapsulated by the Ethernet header:

- http://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.xml
- http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml

c) Figure out everything about this frame you can!

If you don't know what Wireshark is, it's time to figure it out. Play around with this tool. In case you are using a good OS, you might also want to have a look at `tcpdump` (might be useful for the project).