WINSTONSOFT

The group arranged a meeting for each member to make a presentation for the protocol they made research on. Additionally in this meeting, we have worked on the *analysis report* of the project. An additional meeting to write analysis report is arranged, on 30.10.2007, Tuesday. The plan for the next week work is stated for each member. Wireshark is installed to computers of group members and Can HOSGOR made a brief demonstration about the program.

Nazif İlker ERÇİN – 1395003

This week, IMAP RFC is continued to be analyzed. Although it is not finished, an explanation about this protocol is prepared and made to other group friends, a visual presentation (ppt) is not prepared this week but it will be prepared when the RFC research is finished. It is apparent that more research is needed for this protocol by myself. Using "telnet" some commands tried on "mail.metu.edu.tr" IMAP server. While trying these commands, the network traffic is monitored using Wireshark and the sent packets from the client and the received packets from the server are observed clearly. Sent packets(to server) include the sent command and some additional data(IP addresses etc.) and the received packets(from server) include the response of the server and some additional data. The *additional data* parts are not examined in detail yet but there is a unique tag for each command, as a part of the command indeed, as mention in the previous weekly report. These tags do not seem very important but they will gain more importance in identifying process.

Can HOŞGÖR – 1395094

This week, I continued my research on SMTP and almost finished reading its specifications. I prepared a small presentation for my teammates to give them a brief summary about this protocol. Together we discussed common patterns in our protocols and tried to establish a common framework that can be used in the implementation phase of the project. For example, most mails are mime-encoded before they are delivered, thus we will be needing a mime decoder that will be used to extract data, and this module can be shared between all mail protocol related parts. Apart from these, I installed Linux version of Wireshark network sniffer program, and made myself familiar to it. I used this program to capture all network

traffic on my computer, and save its output to a pcap file to get an idea about what a sample input data for our project looks like. I searched the internet for the specifications of pcap file format, and found out that we can benefit from libpcap (pcap file I/O library that Wireshark itself uses) as a throughly tested and portable way of reading pcap files.

Elvan GÜLEN – 1448687

This week, I continued researching for POP3 and I finished reading RFC1939. Also we explained our subjects briefly to each other. We didn't go into details because we didn't want to give unsettled or lacking informations. It's better to observe pcap files first and see how data is stored. After all these observations and knowledge became integrated and took shape, we will put forward what we know to each other again. Other than this, I set up Wireshark Network Protocol Analyzer. Initially, I chose my wireless network connection from Capture->Capture Interfaces. Meanwhile I connected to my metumail through POP3 server and at the same time I tried to observe the packets that my commands and responses stored in. Packets store informations like; mac addresses and IPs of destination&source, header length, identification, fragmented or not, source port, destination port, response string/command string(some part of them or the whole). For ex; after connected POP3 server, it sent this respond: +OK POP3 tenedos.general.services.metu.edu.tr 2006f.96 server ready. This response was stored in one packet. On the other hand, every character in my command came in different packets. I don't know the exact reason but I guess the reason is the arrival of other packets while I'm typing commands into telnet window. In the next week, I'll try to learn more about Wireshark, and spend some time for the analysis report.

Çağla ÇIĞ – 1448554

This week, for my part of the project, I have made a small presentation to my team members about the NNTP RFC research I have conducted last week. I told them about the design and command-response relationship of the protocol. Following that, as all of the members of my team, I have installed Wireshark software on my computer. First, it was hard to distinguish between the packets since there were more than a lot, then however after closing the internet applications other than Thunderbird and doing some filtering I could finally be able to observe the NNTP packets.