WINSTONSOFT, WEEKLY REPORT 4

As we have worked on the Requirements Analysis Report until Sunday, we have not worked individually, but as a group. After finishing the analysis report, we continued literature survey.

During our work on the analysis report, we have found a very useful paper about port independent protocol identification[1]. In this paper written by *Holger Dreger* and *Anja Feldmann, et. al,* dynamic application-layer protocol analysis aimed for network intrusion detection, we faced with a whole new approach towards our project topic. During our market research we saw that the scope of the projects previously built for network analysis and protocol identification was limited to *port depentent* algorithms. However, upon finding this paper we noticed another approach aimed for *port independent protocol identification* using *byte level signatures* to "flag" what protocol it appears to be. Prior to reading this paper it was planned to implement AI algorithms like pattern recognition etc., for identifiying protocols but in this paper, they achieved a similar goal using a simpler approach.

We expect an urgent feedback about this paper.

[1] Dreger H., Feldmann A., et.al, "Dynamic Application-Layer Protocol Analysis for Network Intrusion Detection"
http://cs.northwestern.edu/~ychen/classes/cs450-s07/lectures/pia.ppt
http://www.icir.org/robin/papers/usenix06.pdf