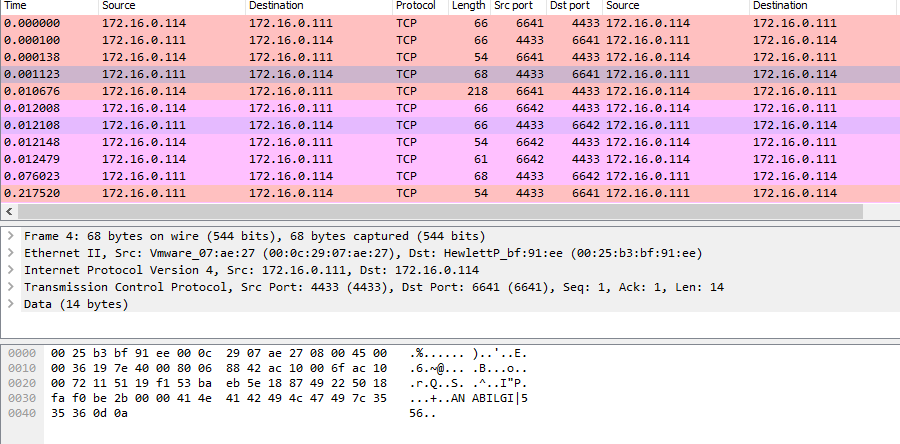
Experimental Analysis

# Dataset:

For our project we used Remote Access Trojan (RAT) infected PCAP file:

[ratinfected.pcap](http://www.chrissanders.org/captures/ratinfected.pcap)

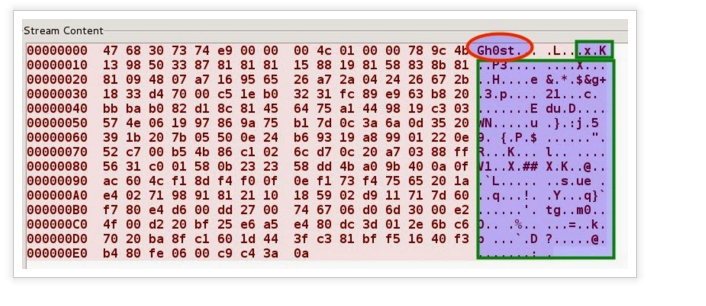
This file has the presence of CYBEREXE RAT virus which can only be detected by the presence of the word ”ANABILGI” (Meaning: Basic information in Turkish language) in the 5-bytes information area of every packet. Below you can see the image of Wireshark where ANABILGI is present.



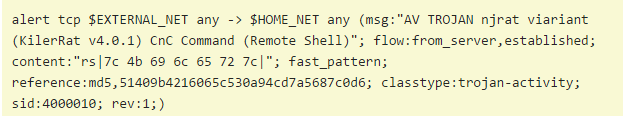
# Relevant RAT Virus:

There are lot of RAT virus which comes in various forms. To name them a few

## Gh0st:

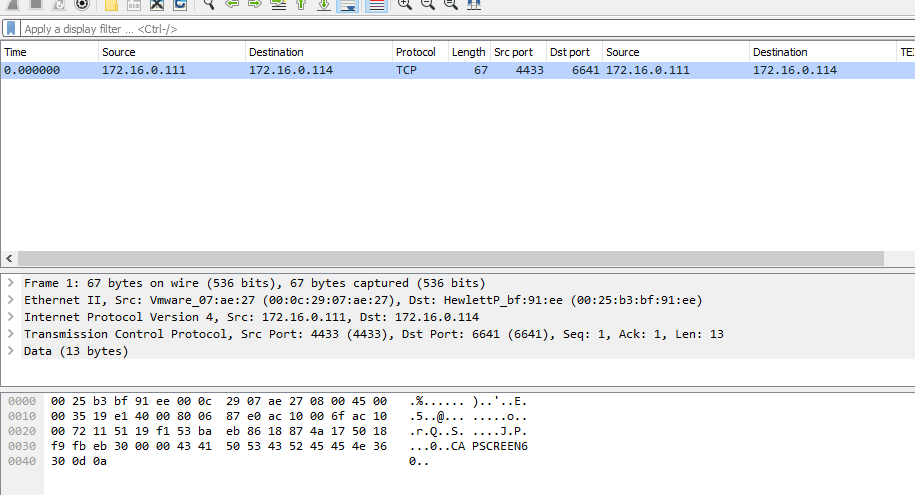


## NjRAT:



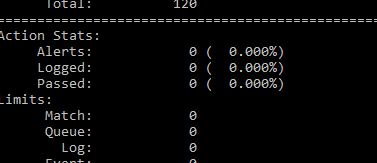
# Snort Detection:

In normal Snort, these virus packets are difficult to detect. We should write manual rules to find the particular content in the 5 bytes information field. Below you can see the Wireshark display of the Snort IDS alert log.



Here Snort listed only 1 IP packet which it alerted as Anomaly and it couldn’t be able to sense the other virus packets because it was unable to detect the Header information without the rules.

We changed the approach and extracted a small part of the ratinfected file (having only 1 conversation between SYN and ACK) and fed to snort. Now it became worse and didn’t even alert for it.



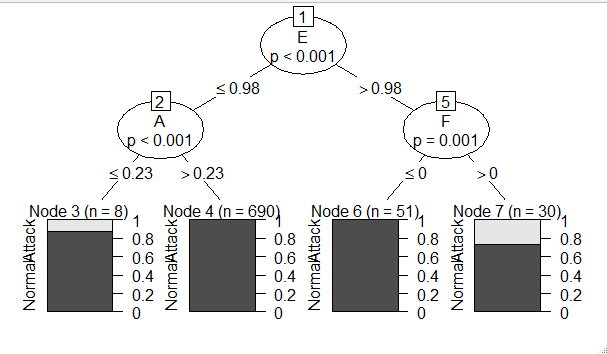
Data Mining - Decision Tree :

To make the system robust, we decided to build a classifier which will predict the attack by looking at the whole attribute and not just the 5-bytes information header of the packet.

For our initial analysis, Decision tree was built using Party package in R language.

We parsed the dataset using Regular expression and Text analytics in I- Python and extracted those into Excel spreadsheet. To make it a machine learning format, it was preprocessed and Info gain feature selection was run for removing the unwanted columns.

Below you can see the results of the Tree formed.



We also ran the dataset with Mahout- Random forest classifier and got 99 percentage accuracy.

