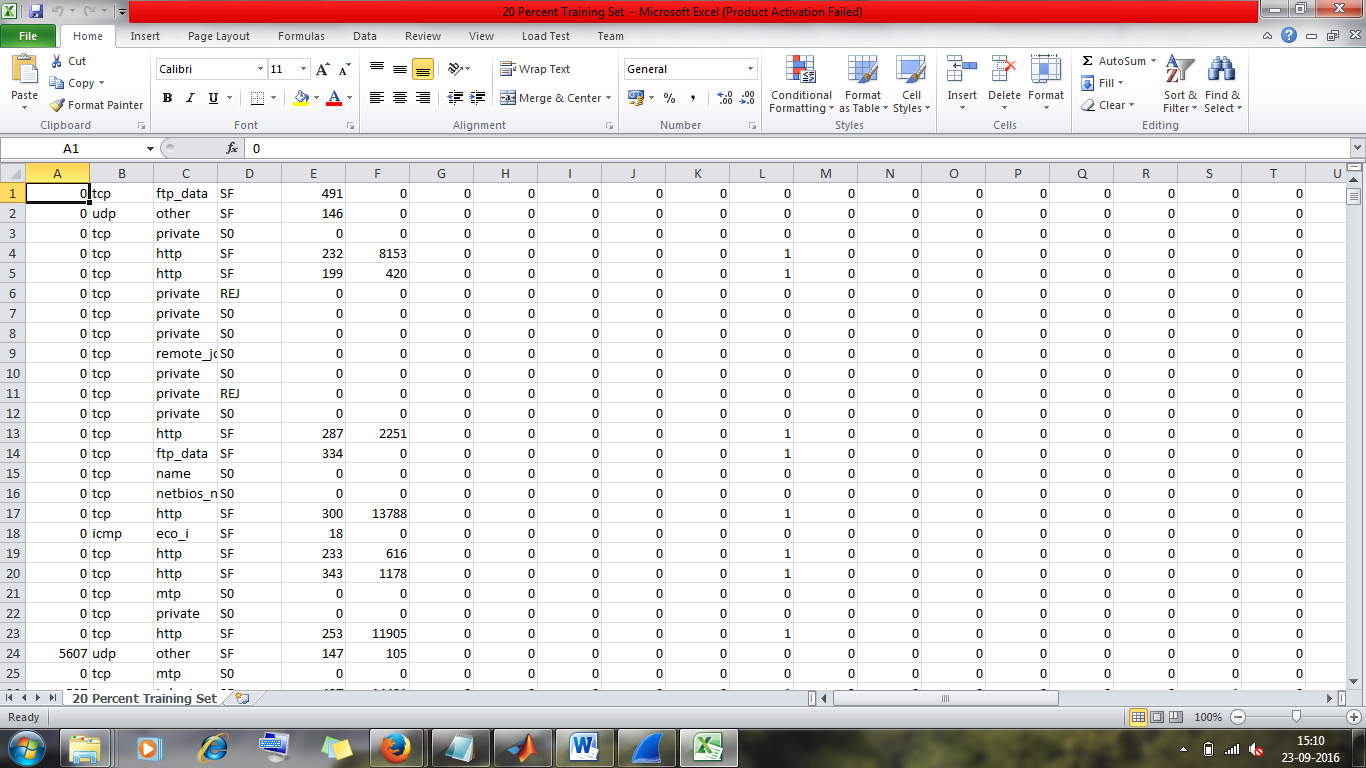
## Definition

The Difference Between **DoS** and **DDos Attacks**. A **Denial of Service** (**DoS**) **attack** is different from a **DDoS attack**. The **DoS attack** typically uses one computer and one Internet connection to flood a targeted system or resource. The **DDoS attack** uses multiple computers and Internet connections to flood the targeted resource.

<http://www.security-faqs.com/dos-vs-ddos-what-is-the-difference.html>

## DoS Dataset

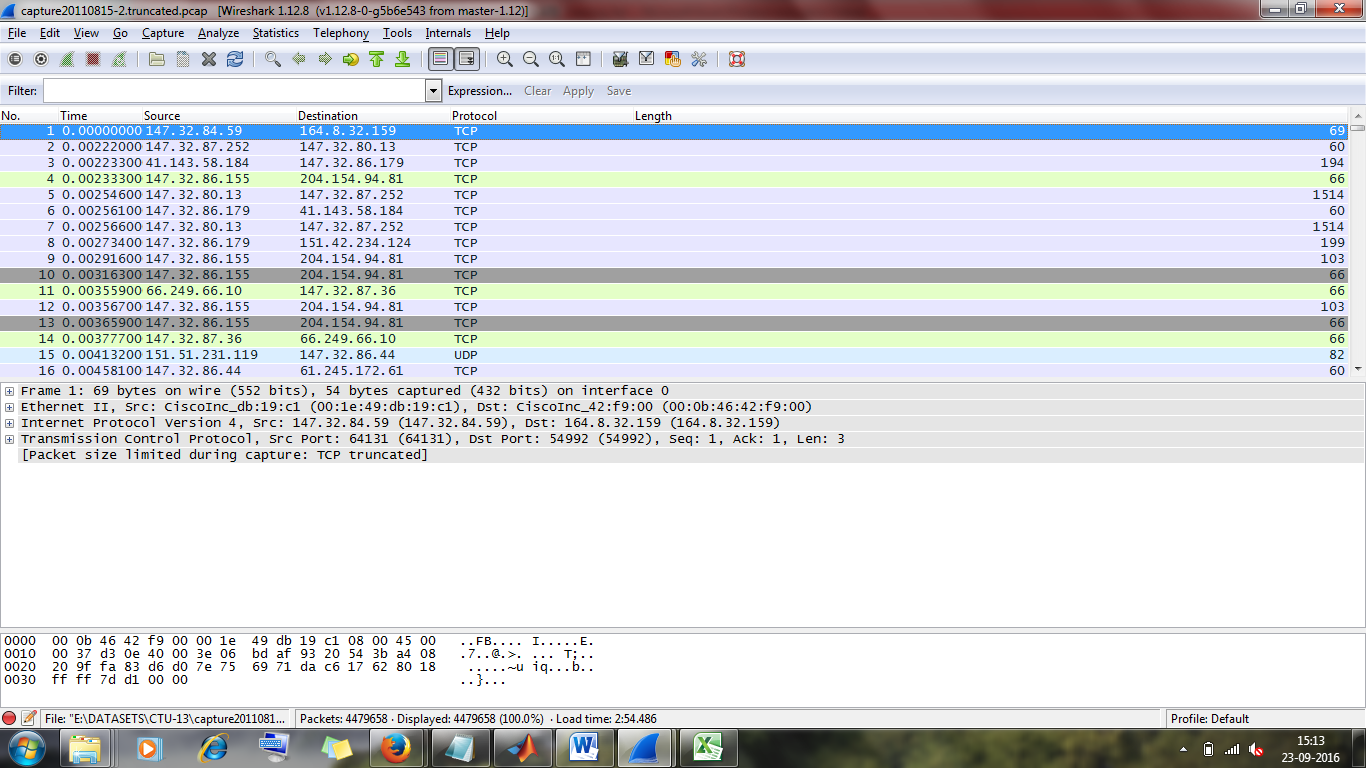


NSL-KDD dataset.

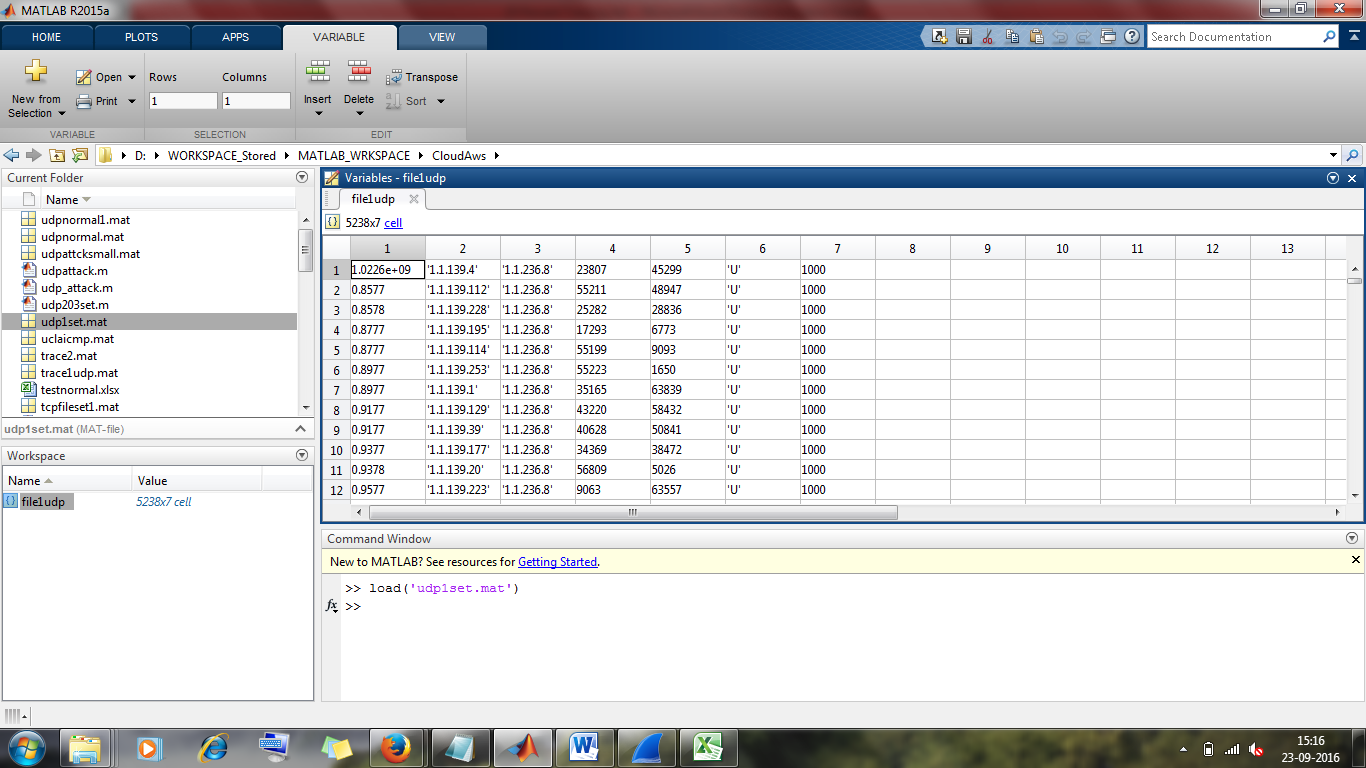
This has 41 features. Here we have different types of attack classes like **DoS, Probe, R2L and U2R.**

## DDoS Dataset

Example 1 – **Caida dataset (pcap file)**



Example 2 - **D-ward lars dataset**



This is from lars website.( <http://www.lasr.cs.ucla.edu/ddos/>)

**This is D-Ward : DDoS Network Attack Recognition and Defense**

Example 3: You have **CTU-13 dataset.**

I can give more examples, but this should suffice.

DDoS datasets do not come with features, we need to calculate them. I had informed you 5 is what iam dealing with as many papers have very less features. You had agreed.

If you want more I told you I have included, only need to show them in the feature table. I mentioned this very clearly in my last mail.

“Coming to features of datasets, i have used flags (17 to 23) for type of attack, datalength and DstLength too. Just need to tabulate them. I can include two more ratios too.”

Now tell me what does your research say? Are you sure you are asking the correct question. Whether this is DDoS or not. Looks like you have not read enough. I have done a lot of research on this.

Remember you asked me to first code using NSL-KDD, when I had completed said we need a different dataset, DDoS dataset so we shifted (think you have forgotten). I have researched enough.

Metrics, I had clearly mentioned and sent you the journal “network anomaly detection using IP flows with Principal component analysis and ant colony optimization” that I will have similar graphs and mentioned that I would include metrics like precision, recall, accuracy, sensitivity, specificity and fscore.

Just see the code you will find these lines for all attacks(matlab code)

Precision = (TP / (TP + FP))\*100;

Accuracy = ((TP+TN)/(TP+TN+FP+FN))\*100;

Sensitivity = (TP/(TP+FN))\*100;

Specificity = (TN/(FP+TN))\*100;

Fscore = ((2\*TP)/(2\*TP+FP+FN))\*100;