[*] You must have the following files

1. df.py
2. script.sh
3. clean.sh
4. allip.html
5. malip.html
6. dport.html
7. sport.html
8. SrcDst.html
9. DOS.html

[*]MD5 for all files present in MD5.txt

```
ab20c75edbc1389bab431becf14f1733  allip.html

327ad219d933d1bc877b30d0e790a559  blacklist.txt

8ac03c9f10eb9890efd96c832a693012  clean.sh

3b69861d4b18f5bd6cf8b660de48cad6  df.py

b3251e381165550818983d95da8c8af6  DOS.html

05e61b639dafdcf0791f2151b1df8dc0  dport.html

acb5ee25d0c90853244c508a6843527e  malip.html

29ba61d79cea70df33f07ebf00827da7  packages.sh

9f7f06560940ff584e442e405c2828b0  script.sh

2194c38a689e2147ffb9b293a5c8ba1f  sport.html

5dfe1bd758b0a79d80c0863c40a41b51  SrcDst.html
```

[*]It is advised run clean.sh first

```
bash clean.sh
```

This program will remove all TSV files outfile.csv all KML files and black_list.txt

[*]./df.py

```
Usage: python df.py -h

Options:

  -h, --help            show this help message and exit

  -p PCAPFILE           PCAP file

  -b BLACKLISTFILE      Blacklisted IP addresses list

  -g GEO                Location of GeoCityLite database

  -t LIMIT              Packet threshold over which DDOS suspected

  -n PORT               Suspected Port number for DDOS attack

  -k KMLFILE            kml file for malicious IP addresses
```

[*] Required Files

1. Path of .PCAP file
2. Path of blacklist file
3. If KML file output is desired path of Geolite database is expected
4. If you want to check for suspected DDOS attacks port number and threshold limit is expected

[*]Dependancies

1. Tshark tool

2. GeoCityLite Database

3. Python Packages used

```
import dpkt
import socket
import urllib2
import optparse
import os
import subprocess
import pygeoip
import simplekml
import sys
import operator
```

[*]Program tested on:

1. Debian GNU/Linux Kali Linux 1.0.6

2. Ubuntu 12.04 LTS

[*] I have provided “packages.sh” bash file

If you have pip installed this script will install all required python packages for this program

[*]PCAP files can be downloaded from:

http://www.netresec.com/?page=PcapFiles

[*] Links to video are in Project.pdf