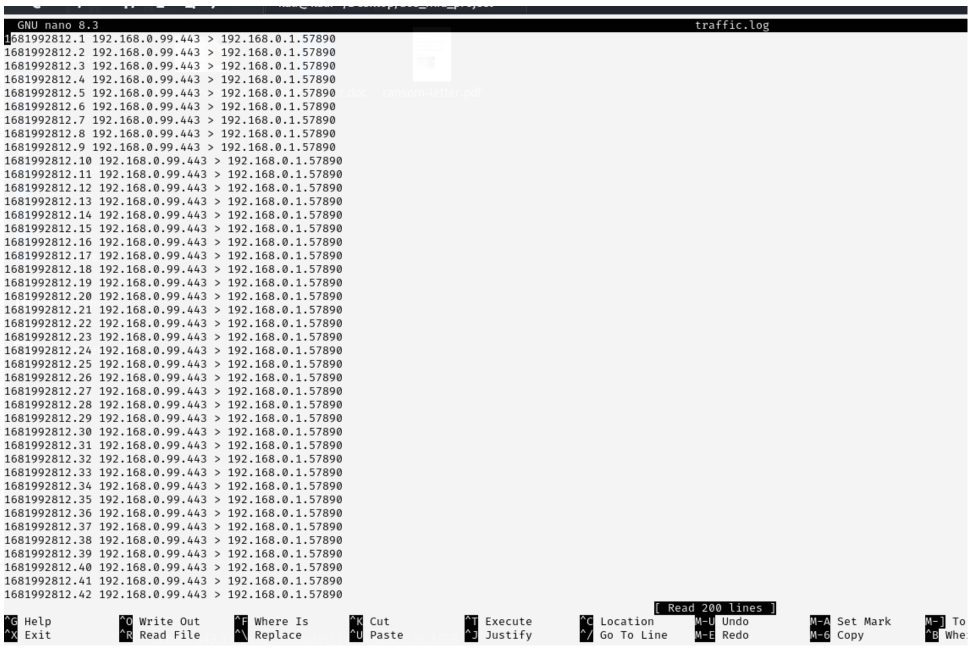
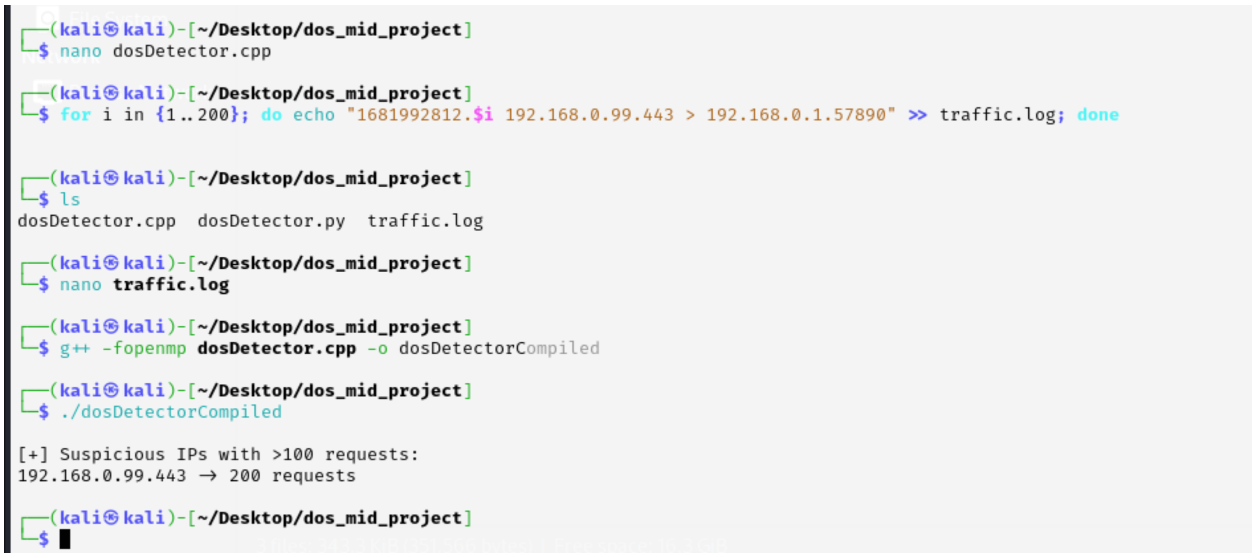
Manually generated log file :



```
  GNU nano 8.3                                                                    traffic.log
1681992812.1 192.168.0.99.443 > 192.168.0.1.57890
1681992812.2 192.168.0.99.443 > 192.168.0.1.57890
1681992812.3 192.168.0.99.443 > 192.168.0.1.57890
1681992812.4 192.168.0.99.443 > 192.168.0.1.57890
1681992812.5 192.168.0.99.443 > 192.168.0.1.57890
1681992812.6 192.168.0.99.443 > 192.168.0.1.57890
1681992812.7 192.168.0.99.443 > 192.168.0.1.57890
1681992812.8 192.168.0.99.443 > 192.168.0.1.57890
1681992812.9 192.168.0.99.443 > 192.168.0.1.57890
1681992812.10 192.168.0.99.443 > 192.168.0.1.57890
1681992812.11 192.168.0.99.443 > 192.168.0.1.57890
1681992812.12 192.168.0.99.443 > 192.168.0.1.57890
1681992812.13 192.168.0.99.443 > 192.168.0.1.57890
1681992812.14 192.168.0.99.443 > 192.168.0.1.57890
1681992812.15 192.168.0.99.443 > 192.168.0.1.57890
1681992812.16 192.168.0.99.443 > 192.168.0.1.57890
1681992812.17 192.168.0.99.443 > 192.168.0.1.57890
1681992812.18 192.168.0.99.443 > 192.168.0.1.57890
1681992812.19 192.168.0.99.443 > 192.168.0.1.57890
1681992812.20 192.168.0.99.443 > 192.168.0.1.57890
1681992812.21 192.168.0.99.443 > 192.168.0.1.57890
1681992812.22 192.168.0.99.443 > 192.168.0.1.57890
1681992812.23 192.168.0.99.443 > 192.168.0.1.57890
1681992812.24 192.168.0.99.443 > 192.168.0.1.57890
1681992812.25 192.168.0.99.443 > 192.168.0.1.57890
1681992812.26 192.168.0.99.443 > 192.168.0.1.57890
1681992812.27 192.168.0.99.443 > 192.168.0.1.57890
1681992812.28 192.168.0.99.443 > 192.168.0.1.57890
1681992812.29 192.168.0.99.443 > 192.168.0.1.57890
1681992812.30 192.168.0.99.443 > 192.168.0.1.57890
1681992812.31 192.168.0.99.443 > 192.168.0.1.57890
1681992812.32 192.168.0.99.443 > 192.168.0.1.57890
1681992812.33 192.168.0.99.443 > 192.168.0.1.57890
1681992812.34 192.168.0.99.443 > 192.168.0.1.57890
1681992812.35 192.168.0.99.443 > 192.168.0.1.57890
1681992812.36 192.168.0.99.443 > 192.168.0.1.57890
1681992812.37 192.168.0.99.443 > 192.168.0.1.57890
1681992812.38 192.168.0.99.443 > 192.168.0.1.57890
1681992812.39 192.168.0.99.443 > 192.168.0.1.57890
1681992812.40 192.168.0.99.443 > 192.168.0.1.57890
1681992812.41 192.168.0.99.443 > 192.168.0.1.57890
1681992812.42 192.168.0.99.443 > 192.168.0.1.57890
                                                                                [ Read 200 lines ]
^G Help        ^O Write Out   ^F Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark   M-] To
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy       ^B Whe
```

Execution:



```
┌──(kali㉿kali)-[~/Desktop/dos_mid_project]
└─$ nano dosDetector.cpp

┌──(kali㉿kali)-[~/Desktop/dos_mid_project]
└─$ for i in {1..200}; do echo "1681992812.$i 192.168.0.99.443 > 192.168.0.1.57890" >> traffic.log; done


┌──(kali㉿kali)-[~/Desktop/dos_mid_project]
└─$ ls
dosDetector.cpp  dosDetector.py  traffic.log

┌──(kali㉿kali)-[~/Desktop/dos_mid_project]
└─$ nano traffic.log

┌──(kali㉿kali)-[~/Desktop/dos_mid_project]
└─$ g++ -fopenmp dosDetector.cpp -o dosDetectorCompiled

┌──(kali㉿kali)-[~/Desktop/dos_mid_project]
└─$ ./dosDetectorCompiled

[+] Suspicious IPs with >100 requests:
192.168.0.99.443 → 200 requests

┌──(kali㉿kali)-[~/Desktop/dos_mid_project]
└─$ █
```

OpenMP-based DDoS Detection (C++) using PCAP logs

If you want to **use OpenMP**, your best bet is to:

1. **Capture traffic** using tcpdump or Wireshark into a .pcap or .txt file.
2. Process that file using a **C++ OpenMP program** to detect DDoS patterns.

Parallel log file analysis

Use **C++ + OpenMP**

1. **Parallelization:** #pragma omp parallel for used to analyze log lines concurrently.
2. **Locking:** omp_lock_t ensures thread-safe access to unordered_map.
3. **Output Format:** IP address → number of requests.
4. **Performance Tip:** Compare speed with and without OpenMP using omp_get_wtime().