

```
1  #!/bin/sh
2
3  clear
4  echo "Processing the pcap file..."
5
6  #write the header to the file
7  header="Date,Time,Priority,Classification,Description,Source IP,Destination
... IP"
8  echo $header > alert_data.csv
9
10 #read lines from the pcap file
11 input="fast_short.pcap"
12 while IFS= read -r line
13 do
14     date=${line:0:5}
15     time=${line:6:5}
16     priority=$(echo $line | cut -d "[" -f 6)
17     priority=${priority:10:1}
18     classification=$(echo $line | cut -d "[" -f 5)
19     classification=${classification:16:-2}
20     description=$(echo $line | cut -d "]" -f 3)
21     description=${description:1:-4}
22     line=$(echo $line | tr "]" "|")
23     both_ip=$(echo $line | cut -d "|" -f 2)
24     source_ip=$(echo $both_ip | cut -d ">" -f 1)
25     source_ip=${source_ip:0:-2}
26     destination_ip=$(echo $both_ip | cut -d ">" -f 2)
27     destination_ip=${destination_ip:1}
28
... line_out="$date,$time,$priority,$classification,$description,$source_ip,$
... destination_ip"
29     echo $line_out >> alert_data.csv
30 done < $input
31
32 clear
33 echo -e "The pcap file has been processed\n"
34
```