*USER's MANUAL*

## Getting a capture file with the date of the capture

The first modification made to Tethereal is the *option -W* which returns a capture file with the date of beginning of the capture period. This is a little modification to standard option -w and what it has been done is to get the local time from the computer when the analysis begin and makes unnecessary to supply the file argument. The pattern for the name of the file name is the following

**capture_*month-day_hour:minute*.tet**

- month : (01 - 12 )
- day :day of the month (01- 31 )
- hour : ( 00 - 23 )
- minute : ( 00 - 59 )
- This date format is also used for the file result of the analysis.
- The capture file will be stored in the current PATH.

As it is supposed to be done with the standard option of Tethereal, we have to give an auto stop condition that will stop the capture some how.
As an example of how does it work suppose the local time when we launch the following command is 9:00 July 30, and we type :

**tethereal -W -a duration:300**

then the output file for that command would be *capture_07-30_09:00.tet*

## Protocols and Communications Network analysis

This analysis it's performed giving the *option -C* at the command line. This analysis is *not intended to be done capturing traffic from the wire ( real time )* because the

CPU and MEMORY loads are very high and if the packet flow is quite big we can start loosing packets getting wrong results for the analysis. Instead we can save the capture to a file and perform the analysis later on reading from the file and there would be no problem at all. The module associated to this analysis is called com_stats and the functionality is explained in the appendix.
This analysis gives as result a file divided in two sections each of them with the results of one the analysis made. The content of each section is the following:

**Section 1: Protocol Hierarchy Statistics**

Is the list of protocols used to send information during the capture time. They are organised in tree structure and the information shown for each protocol is the following

- **Protocol** Name of the protocol. The protocols shown ranges from the link layer to the application layer. They are organised in a tree structure were the root node is the frame, after that comes the link layer protocol, network layer, transport layer and application layer. The protocols of an upper layer are grouped under the protocol that has encapsulated it for the transmission.
- **Packets** Total number of packets that had been send using this protocol
- **Bytes** Total amount of Bytes sent using the current protocol.
- **End_Packets** Number of packets sent with the current protocol that doesn't encapsulate another protocol of a higher layer. For instance, if we have a packet TCP, it can be packet containing exclusively transport level information ( communication handling) or it can encapsulate information of a HTTP connection to what ever other protocol of application layer that means that it isn't a end packet.
- **End_Bytes** Length in Bytes of all the end packets.
- **% Packets** Percentage of packets sent with the current protocol respect of the total packets captured.
- **% Bytes** Percentage of bytes sent with the current protocol respect of the total information

- **Kbytes/second** Bit rate in Kbytes per second. This is an average for the total capture period, which means that we take the total time in seconds of the capture to calculate the bit rate.

**Section 2: IP communications**

This section is a list of communications with the following columns of information:

- **Src Addr** IP source address of the communication
- **Src Port** Source port of the communication
- **Dst Addr** IP destination address of the communication
- **Dst Port** Destination port of the communication
- **Protocol** Transport protocol used for the communication
- **Packets** Number of packets sent through the communication
- **Bytes** Size in Bytes of all the packets sent through the actual communication

The following fields in order sort the output list : src addr, src port, dst addr, dst port

If we are actually dealing with a *TCP connection* there is some other interesting information that are shown. This information remains empty if another transport protocol is used

- **Attempts** Number of connection request (TCP packet with Flag SYN active) sent. This a really interesting information in order to know if there are any problems for establishing certain connections or if there are certain hours in which generally it's difficult to establish a connection.
- **Length** Period of time in which the connection was active. This field will remain empty if the connection has not been started or ended during the capture period.
- **Max delay** This is statistical information, in this field we show the maximum

inter-packet delay during the connection. This means that once the connection is established we look for the delay between the arrival of one packet and next one.

The file name will also following pattern :
**com_stats_*month-day_hour:minute.*txt**

Since the analysis is not intended to be done in real time, the way of getting the name to give the name to the result file is slightly different because if we get the local time when we perform the analysis that will have not meaning for the result file because the information was captured in another period of time. The method used to avoid this problem is to get absolute time ( UTC ) from the first frame that was captured ( it doesn't matter if the analysis is done in real time or not ). That way the name given to the result file will be correlative to the period in which the information was captured.
Let's say we have the capture *file* called *capture_07-30_09:00.tet* and we want to obtain the protocol statistics and the IP communications that have been done during the capture period, then we type :

**tethereal -n -r capture_07-30_09:00.tet -C**

This command will return a *file* called *com_stats_07-30_09:00.txt.* The file will be divided in two sections as it has been say already. Each of the sections are shown in the next two pages

########################################################################################################################
Section1 : Protocol Hierarchy Statistics
########################################################################################################################

| Protocol | Packets | Bytes | End Packets | End Bytes | % Packets | % Bytes | KBytes/sec |
|---|---|---|---|---|---|---|---|
| Frame | 302114 | 212834884 | 0 | 0 | 100,00% | 100,00% | 709,45 |
| Ethernet | 302106 | 212834132 | 0 | 0 | 100,00% | 100,00% | 709,45 |
| Internet Protocol | 301884 | 212819850 | 0 | 0 | 99,92% | 99,99% | 709,40 |
| Transmission Control Protocol | 297687 | 212091818 | 128992 | 8120188 | 98,53% | 99,65% | 706,97 |
| Data | 122468 | 157425821 | 122468 | 157425821 | 40,54% | 73,97% | 524,75 |
| Hypertext Transfer Protocol | 36986 | 41791280 | 36986 | 41791280 | 12,24% | 19,64% | 139,30 |
| Real Time Streaming Protocol | 1764 | 1659065 | 1764 | 1659065 | 0,58% | 0,78% | 5,53 |
| File Transfer Protocol (FTP) | 699 | 199267 | 699 | 199267 | 0,23% | 0,09% | 0,66 |
| Internet Relay Chat | 121 | 12244 | 121 | 12244 | 0,04% | 0,01% | 0,04 |
| Post Office Protocol | 1263 | 153346 | 1263 | 153346 | 0,42% | 0,07% | 0,51 |
| Simple Mail Transfer Protocol | 1045 | 657440 | 1045 | 657440 | 0,35% | 0,31% | 2,19 |
| Short Frame | 493 | 59724 | 493 | 59724 | 0,16% | 0,03% | 0,20 |
| Secure Socket Layer | 2461 | 1537507 | 199 | 15198 | 0,81% | 0,72% | 5,13 |
| Short Frame | 1315 | 455178 | 1315 | 455178 | 0,44% | 0,21% | 1,52 |
| Unreassembled Fragmented Packet | 947 | 1067131 | 947 | 1067131 | 0,31% | 0,50% | 3,56 |
| AOL Instant Messenger | 384 | 38726 | 368 | 34679 | 0,13% | 0,02% | 0,13 |
| Short Frame | 16 | 4047 | 16 | 4047 | 0,01% | 0,00% | 0,01 |
| Unreassembled Fragmented Packet | 18 | 1197 | 18 | 1197 | 0,01% | 0,00% | 0,00 |
| Network News Transfer Protocol | 935 | 417658 | 935 | 417658 | 0,31% | 0,20% | 1,39 |
| Telnet | 14 | 2341 | 14 | 2341 | 0,00% | 0,00% | 0,01 |
| Universal Computer Protocol | 6 | 7134 | 6 | 7134 | 0,00% | 0,00% | 0,02 |
| Internet Message Access Protocol | 28 | 6324 | 28 | 6324 | 0,01% | 0,00% | 0,02 |
| Border Gateway Protocol | 8 | 584 | 8 | 584 | 0,00% | 0,00% | 0,00 |
| FTP Data | 1 | 458 | 1 | 458 | 0,00% | 0,00% | 0,00 |
| DCE RPC | 1 | 1514 | 1 | 1514 | 0,00% | 0,00% | 0,01 |
| User Datagram Protocol | 3280 | 606363 | 0 | 0 | 1,09% | 0,28% | 2,02 |
| Domain Name Service | 3193 | 597396 | 859 | 63453 | 1,06% | 0,28% | 1,99 |
| Short Frame | 2334 | 533943 | 2334 | 533943 | 0,77% | 0,25% | 1,78 |
| Data | 19 | 2621 | 19 | 2621 | 0,01% | 0,00% | 0,01 |
| NetBIOS Name Service | 68 | 6346 | 0 | 0 | 0,02% | 0,00% | 0,02 |
| Short Frame | 68 | 6346 | 68 | 6346 | 0,02% | 0,00% | 0,02 |
| Internet Control Message Protocol | 613 | 67028 | 613 | 67028 | 0,20% | 0,03% | 0,22 |
| Generic Routing Encapsulation | 304 | 54641 | 0 | 0 | 0,10% | 0,03% | 0,18 |
| Internet Protocol | 304 | 54641 | 0 | 0 | 0,10% | 0,03% | 0,18 |
| Enhanced Interior Gateway Routing Protocol | 129 | 12642 | 0 | 0 | 0,04% | 0,01% | 0,04 |
| Short Frame | 129 | 12642 | 129 | 12642 | 0,04% | 0,01% | 0,04 |
| Internet Group Management Protocol | 59 | 4225 | 19 | 1290 | 0,02% | 0,00% | 0,01 |
| Protocol Independent Multicast | 20 | 1430 | 20 | 1430 | 0,01% | 0,00% | 0,00 |
| Distance Vector Multicast Routing Protocol | 20 | 1505 | 15 | 1065 | 0,01% | 0,00% | 0,01 |
| Short Frame | 5 | 440 | 5 | 440 | 0,00% | 0,00% | 0,00 |
| User Datagram Protocol | 70 | 34020 | 0 | 0 | 0,02% | 0,02% | 0,11 |
| Routing Information Protocol | 70 | 34020 | 0 | 0 | 0,02% | 0,02% | 0,11 |
| Short Frame | 70 | 34020 | 70 | 34020 | 0,02% | 0,02% | 0,11 |
| Protocol Independent Multicast | 43 | 3292 | 26 | 1768 | 0,01% | 0,00% | 0,01 |
| Short Frame | 17 | 1524 | 17 | 1524 | 0,01% | 0,00% | 0,01 |
| Cisco Interior Gateway Routing Protocol | 3 | 462 | 0 | 0 | 0,00% | 0,00% | 0,00 |
| Short Frame | 3 | 462 | 3 | 462 | 0,00% | 0,00% | 0,00 |
| Logical-Link Control | 161 | 10605 | 0 | 0 | 0,05% | 0,00% | 0,04 |
| Spanning Tree Protocol | 148 | 8880 | 148 | 8880 | 0,05% | 0,00% | 0,03 |
| Cisco Discovery Protocol | 5 | 1245 | 0 | 0 | 0,00% | 0,00% | 0,00 |
| Short Frame | 5 | 1245 | 5 | 1245 | 0,00% | 0,00% | 0,00 |
| Data | 8 | 480 | 8 | 480 | 0,00% | 0,00% | 0,00 |
| Data | 61 | 3677 | 61 | 3677 | 0,02% | 0,00% | 0,01 |
| Cisco ISL | 8 | 752 | 0 | 0 | 0,00% | 0,00% | 0,00 |
| Ethernet | 8 | 752 | 0 | 0 | 0,00% | 0,00% | 0,00 |
| Logical-Link Control | 8 | 752 | 0 | 0 | 0,00% | 0,00% | 0,00 |

################################################################################################################

Section2 : IP Communications

################################################################################################################

| Src Addr | Src Port | Dst Addr | Dst Port | Protocol | Attempts | Packets | Bytes | Length (secs) | max_delay |
|---|---|---|---|---|---|---|---|---|---|
| 192.44.75.179 | 2470 | 66.77.81.137 | 80 | TCP | 0 | 4 | 264 | -------------- | ---------- |
| 192.44.75.179 | 2472 | 216.239.33.101 | 80 | TCP | 1 | 11 | 4582 | 0.344 | 0.300055 |
| 192.44.75.179 | 2473 | 216.239.33.101 | 80 | TCP | 1 | 11 | 1412 | 0.194 | 0.165839 |
| 192.44.75.179 | 2474 | 216.239.33.101 | 80 | TCP | 1 | 11 | 1412 | 0.191 | 0.167761 |
| 192.44.75.179 | 2475 | 216.239.33.101 | 80 | TCP | 1 | 11 | 1412 | 0.199 | 0.165705 |
| 192.44.75.179 | 2476 | 216.239.33.101 | 80 | TCP | 1 | 11 | 1411 | 0.182 | 0.169614 |
| 192.44.75.179 | 2477 | 216.239.33.101 | 80 | TCP | 1 | 11 | 1418 | 0.175 | 0.172684 |
| 192.44.75.179 | 2478 | 216.239.33.101 | 80 | TCP | 1 | 11 | 1416 | 0.171 | 0.169543 |
| 192.44.75.179 | 2479 | 216.239.33.101 | 80 | TCP | 1 | 11 | 1419 | 0.177 | 0.165376 |
| 192.44.75.179 | 2480 | 216.239.33.101 | 80 | TCP | 1 | 11 | 1417 | 0.171 | 0.169338 |
| 192.44.75.179 | 2482 | 216.239.33.101 | 80 | TCP | 1 | 14 | 6188 | 0.341 | 0.164849 |
| 192.44.75.179 | 2483 | 216.239.33.101 | 80 | TCP | 1 | 11 | 2710 | 10.176 | 0.166079 |
| 192.44.75.179 | 2484 | 129.187.161.201 | 80 | TCP | 1 | 152 | 122166 | 5.137 | 1.628800 |
| 192.44.75.179 | 2485 | 129.187.161.201 | 80 | TCP | 1 | 810 | 761265 | 19.859 | 0.185209 |
| 192.44.75.191 | 1092 | 195.101.94.80 | 80 | TCP | 1 | 38 | 25376 | 0.942 | 0.418081 |
| 192.44.75.191 | 1093 | 195.101.94.80 | 80 | TCP | 1 | 39 | 19465 | 2.387 | 0.379321 |
| 192.44.75.191 | 1094 | 195.101.94.80 | 80 | TCP | 1 | 9 | 1623 | 0.129 | 0.027112 |
| 192.44.75.191 | 1095 | 195.101.94.80 | 80 | TCP | 1 | 18 | 5406 | 1.475 | 0.398501 |
| 192.44.75.191 | 1097 | 193.252.117.12 | 80 | TCP | 1 | 12 | 1921 | 0.092 | 0.072982 |
| 192.44.75.191 | 1099 | 195.101.94.237 | 80 | TCP | 1 | 23 | 13525 | 0.353 | 0.120169 |
| 192.44.75.191 | 1100 | 193.252.117.12 | 80 | TCP | 1 | 12 | 1845 | 0.086 | 0.049013 |
| 192.44.75.191 | 1102 | 193.252.117.66 | 80 | TCP | 1 | 11 | 5288 | 0.049 | 0.020551 |
| 192.44.75.191 | 1103 | 195.101.94.80 | 80 | TCP | 1 | 34 | 21903 | 0.990 | 0.202518 |
| 192.44.75.191 | 1104 | 193.252.117.12 | 80 | TCP | 1 | 12 | 1852 | 0.108 | 0.068602 |
| 192.44.75.191 | 1105 | 195.101.94.80 | 80 | TCP | 1 | 26 | 12081 | 8.289 | 0.792857 |
| 192.44.75.191 | 1107 | 195.101.94.76 | 80 | TCP | 1 | 6 | 1105 | 0.825 | 0.017864 |
| 192.44.75.191 | 1108 | 193.252.117.66 | 80 | TCP | 1 | 5 | 300 | 0.824 | 0.000000 |
| 192.44.75.191 | 1109 | 193.252.117.12 | 80 | TCP | 1 | 12 | 1912 | 0.088 | 0.043732 |
| 192.44.75.191 | 1111 | 195.101.94.245 | 80 | TCP | 1 | 10 | 1599 | 0.031 | 0.027084 |
| 192.44.75.191 | 1112 | 193.252.117.66 | 80 | TCP | 1 | 8 | 1194 | 0.021 | 0.000952 |
| 192.44.75.191 | 1114 | 195.101.94.80 | 80 | TCP | 1 | 16 | 5407 | 6.762 | 0.038928 |
| 192.44.75.191 | 1115 | 195.101.94.245 | 80 | TCP | 1 | 10 | 1599 | 0.198 | 0.170664 |
| 192.44.75.191 | 1116 | 195.101.94.80 | 80 | TCP | 1 | 9 | 1737 | 0.029 | 0.027480 |
| 192.44.75.191 | 1118 | 195.101.94.79 | 80 | TCP | 1 | 10 | 1503 | 3.335 | 3.307801 |
| 192.44.75.191 | 1119 | 193.252.158.1 | 80 | TCP | 1 | 55 | 37875 | 2.539 | 0.853664 |
| 192.44.75.191 | 1120 | 193.252.158.1 | 80 | TCP | 1 | 35 | 19015 | 2.333 | 0.783340 |
| 192.44.75.191 | 1121 | 193.252.117.12 | 80 | TCP | 1 | 10 | 1164 | 0.100 | 0.052009 |
| 192.44.75.191 | 1122 | 193.252.158.1 | 80 | TCP | 1 | 30 | 15768 | 1.554 | 0.735666 |
| 192.44.75.191 | 1123 | 193.252.158.1 | 80 | TCP | 1 | 24 | 10133 | 1.654 | 0.858093 |
| 192.44.75.191 | 1125 | 195.154.195.80 | 80 | TCP | 1 | 8 | 979 | 0.087 | 0.069466 |
| 192.44.75.191 | 1126 | 193.252.158.1 | 80 | TCP | 1 | 10 | 1920 | 0.025 | 0.015523 |
| 192.44.75.191 | 1127 | 193.252.158.1 | 80 | TCP | 1 | 5 | 1262 | -------------- | ---------- |
| 192.44.75.191 | 1128 | 195.101.94.201 | 80 | TCP | 1 | 3 | 180 | -------------- | ---------- |
| 192.44.75.191 | 1129 | 193.252.158.1 | 80 | TCP | 1 | 40 | 28389 | 0.680 | 0.209634 |
| 192.44.75.191 | 1130 | 193.252.158.1 | 80 | TCP | 1 | 18 | 5695 | 1.587 | 0.652627 |
| 192.44.75.191 | 1131 | 193.252.117.12 | 80 | TCP | 1 | 10 | 1164 | 0.079 | 0.061638 |
| 192.44.75.191 | 1132 | 193.252.158.1 | 80 | TCP | 1 | 10 | 1782 | 0.661 | 0.498116 |
| 192.44.75.191 | 1133 | 193.252.158.1 | 80 | TCP | 1 | 19 | 11486 | 2.773 | 1.961013 |

## Network Traffic Analysis

The execution of this analysis is done when the *option -T* is given. This option requires extra argument interval length in which we count the number of packets and the bytes transmitted. This time has to be given in seconds and usually would be a value between 1 and 10 seconds. It should be no problem to perform this analysis either from a real time capture or from a capture. The output of this analysis file that contains the list of intervals with the following information

- **Start second** Second (relative to the beginning of capture time period ) in which starts the current interval. We will store information in the current interval until the seconds passed as arguments (interval) have passed. Once this has happened we create a new element.
- **Packets** Number of packets sent in the current interval.
- **Bytes** Length in Bytes of all the packets captured during this interval.

The name for the output file is obtained the same fashion as with the protocol and communication statistics output file name reading the absolute time from the first frame captured. The patter is quite similar :
**traffic_i-*interval_month-day_hour:minute*.txt**

The output file is quite simple because it is intended to be used as input for a mathematic application like Mathlab in order to observe how varies the amount of traffic during the capture. Those programs can only import plain text files and use the first column as the index for the x-axis (can be also y-axis ) and the other columns should be the information to be displayed.

To make the analysis in real time, we is required to give an auto stop condition, for instance

**tethereal -n -a duration:300 -T 1**

If  analysis is going to be performed over a capture fill, for instance the one in which we have generate before, the command will be :

**tethereal -n -r capture_07-30_09:00.tet -T 1**

This command will generate an output file called *traffic_i-1_07-30_09:00.txt* with a new entry each second. Since the capture has taken place during 5 minutes (300 seconds) we should get a file with 300 entries. As part of the output file we will have the following output

```
 0     694    502973
 1    1088    755506
 2    1084    799687
 3     984    758686
 4     933    726709
 5     907    684998
 6     961    665051
 7    1030    719591
 8    1015    711195
 9    1090    753506
10    1150    739292
11    1073    652584
12     900    644754
13     956    737420
14     963    702393
15    1011    763975
16    1248    893557
17     984    745114
18    1024    679306
19    1182    890896
20    1248    918408
21     995    691294
22     861    652244
23     898    654498
24    1035    783760
25    1049    784513
26     958    711584
27     919    702791
28    1280    915003
29    1202    835164
30    1164    805298
31    1071    801833
32     878    671305
33     996    665693
34    1055    740021
35    1008    739074
36     852    638474
37     890    657070
38     865    650374
39    1107    860077
40    1028    792949
41     970    716277
42     926    689048
43     847    626562
44    1057    769606
45    1024    755568
46    1033    782298
47    1047    794051
48    1125    869844
49     896    695935
50     937    656816
51     892    643920
52    1275    971183
53    1269    900514
54    1357   1050187
55    1039    743563
56    1136    824803
57    1197    914398
58    1005    710997
59    1064    779519
60    1462   1028036
61    1337    901847
62    1024    688748
63    1112    745491
64    1147    801735
65    1291    922634
```

| | | |
|---|---|---|
| 66 | 1151 | 788471 |
| 67 | 1135 | 791795 |
| 68 | 1150 | 788873 |