www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 5 Issue -03 March, 2016 Page No. 16041-16046

Comparison: Wireshark on different parameters

Ajay Kumar, Jai Bhagwan Yadav

Department of Computer Science
Shivaji College, University of Delhi, India
ajay.cs@shivaji.du.ac.in

Department of Computer Science
Shivaji College, University of Delhi, India
jaibhagwan.yadav@shivaji.du.ac.in

***Abstract*---Wireshark is a network protocol analyser. Wireshark is able to intercept packets transmitted over the network and compile statistics about network usage, allow the user to view content that is being accessed by other network users, and store usage information for offline access. This paper depicts the comparison of Wireshark, with one other similar tool, Network Miner, which is a Network Forensic Analysis Tool (NFAT), based on different parameters: graphical user interface (basic), packet information and traffic analysis. Network Miner can be used as a passive network sniffer/packet capturing tool and can parse PCAP files for off-line analysis.**

***Keywords*---Packet Information, Passive Network Sniffer, PCAP file, Traffic Analysis.**

I. Introduction

AS company intranets continue to grow it is increasingly important that network administrators are aware of and have a handle on the different types of traffic that is traversing their networks. Traffic monitoring and analysis is essential in order to more effectively troubleshoot and resolve issues when they occur, so as to not bring network services to a stand still for extended periods of time.

1.1 Importance of Network Monitoring and Analysis:

Network monitoring is a difficult and demanding task that is a vital part of a Network Administrators job. Network Administrators are constantly striving to maintain smooth operation of their networks. If a network were to be down even for a small period of time, productivity within a company would decline, and in the case of public service departments the ability to provide essential services would be compromised. In order to be proactive rather than reactive, administrators need to monitor traffic movement and performance throughout the network and verify that security breaches do not occur within the network.

1.2 Packet analyser

A packet analyser (also known as a network analyser, protocol analyser or packet sniffer or for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program that can intercept and log traffic that passes over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyses its content.

1.3 Here are some examples showing why these packet analysers are used for:

i. Network administrators use it to *troubleshoot network problems*
ii. Network security engineers use it to *examine security problems*
iii. Developers use it to *debug protocol implementations*
iv. People use it to *learn network protocol* internals

1.4 Two network packet analyser softwares used here:

(i) Wireshark

(download from: https://www.wireshark.org/#download)
Wireshark is perhaps one of the best open source packet analyzers available today

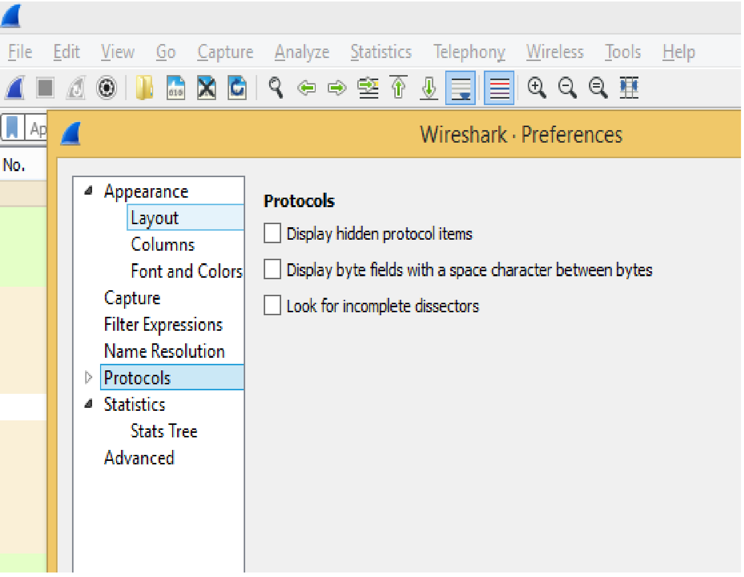
(ii) Netresec Network Miner Packet Tracer

(available at http://www.netresec.com/?page=Networkminer)

1.5 The following are some of the many features Wireshark provides:

i. Available for *UNIX* and *Windows*.
ii. *Capture* live packet data from a network interface.
iii. Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.
iv. Import packets from text files containing hex dumps of packet data.
v. Display packets with very detailed protocol information.
vi. Save packet data captured.

vii. Export some or all packets in a number of capture file formats.
viii. Filter packets on many criteria.
ix. Search for packets on many criteria.
x. Colorize packet display based on filters.



Protocols
☐ Display hidden protocol items
☐ Display byte fields with a space character between bytes
☐ Look for incomplete dissectors

1.6 Features in Network Miner (A brief introduction):

i. Available for Windows only.
ii. Capture live packet data from a network interface but <u>not able to save the packets in any format for later use, it can analyse any packets file which is saved by any other software, then it can analyse the file only</u>.
iii. Open files containing packet data captured. Wireshark, and a number of other packet capture programs.
iv. Export results to CSV / Excel / XML only
v. Display packets with protocol information.
vi. Can't filter packets on many criteria.
vii. No search for packets on many criteria.
viii. Colorize packet display based on filters but only on paid version.

1.7 Requirements for the system:

The amount of resources Wireshark needs depends on your environment and on the size of the capture file you are analysing. The values below should be fine for small to medium-sized capture files no more than a few hundred MB. Larger capture files will require more memory and disk space. Working with a busy network can easily produce huge capture files. A fast processor, lots of memory and disk space is always a good idea. If Wireshark runs out of memory it will crash.

1.8 The .pcap file extension:

Pcap stands for "packet capture". Acapture **file** saved by Wireshark in this **format,** can be read by applications that understand that **format, such as tcpdump.**

II. ANALYSIS

2.1 Analysis on the basis of graphical user interface (basic):

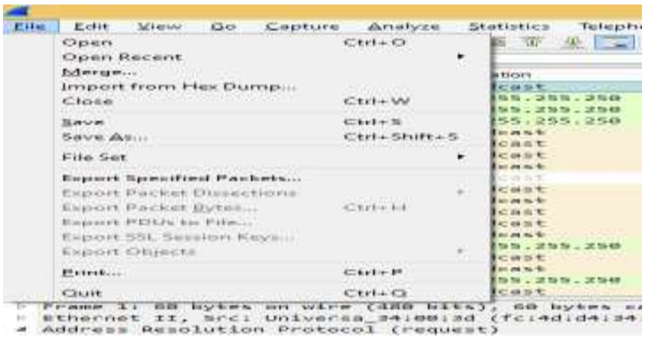
(i) File/Edit: This menu contains items to find a packet, time reference or <u>mark one or more packets</u>, handle configuration profiles, and set the preferences.

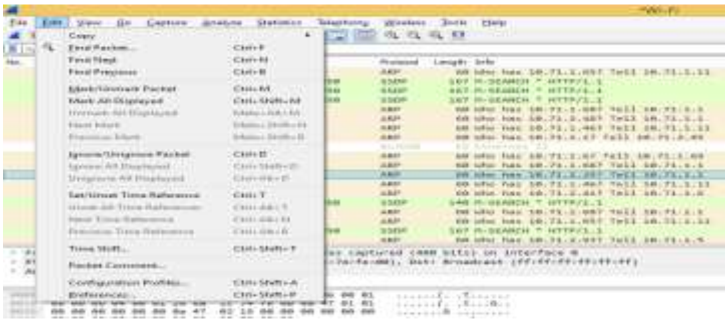
Not available on Network Miner

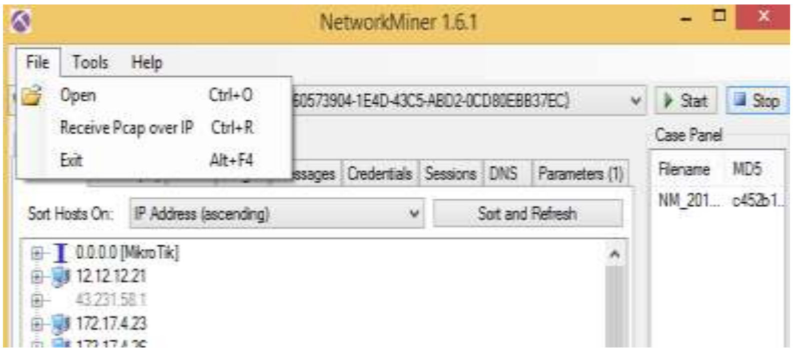
(ii) Merge: This menu item lets you merge a capture file into the currently loaded one.

Not available on Network Miner.

(iii) Packet Comment: This will let you add a comment to a single packet. Note that the ability to save packet comments depends on your file format.
Not available on Network Miner.







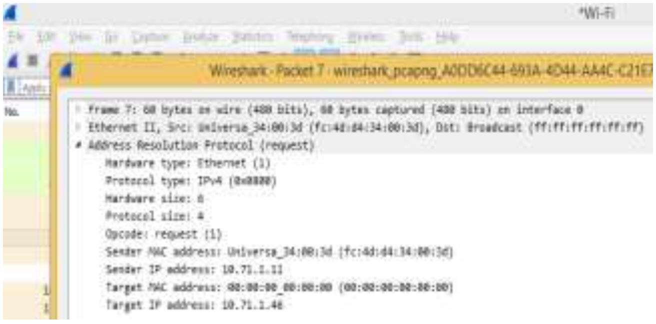
(iv) Expand Sub trees: This menu item expands the currently selected sub tree in the packet details tree.

Also available on Network Miner.

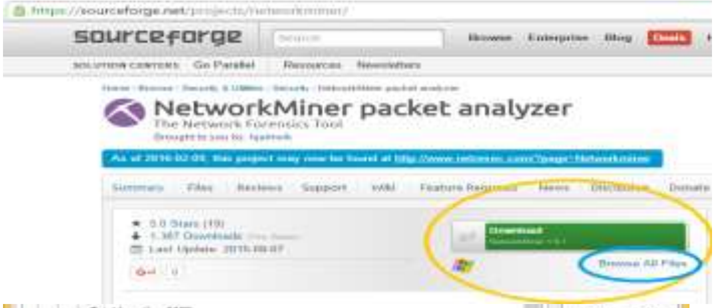
(v) Changing Preferences:
(Shortcut key for Preferences: Shift+Ctrl+P)
This menu item brings up a dialog box that allows you to set preferences for many parameters that control Wireshark. You can also save your preferences so Wireshark will use them the next time you start it.
Network Miner doesn't provides much user prefereces, to change. To make any changement, the user needs to change the source code himself. The source code for the Neteresc Network Miner is available on the site:

Network Miner software is in C# and can be executed from the Miscrosoft Visual Studio.

If Wireshark source code is also needed to be changed-according-to-the-user it can also be changed. Wireshak source code is in C. It can also very well executes in Linux platforms.


*Wi-Fi
Wireshark · Packet 7 · wireshark_pcapng_A0DD6C44-691A-4D44-AA4C-C21E7

```
▷ Frame 7: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▷ Ethernet II, Src: Universa_34:00:3d (fc:4d:d4:34:00:3d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
◢ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Universa_34:00:3d (fc:4d:d4:34:00:3d)
    Sender IP address: 10.71.1.11
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.71.1.46
```

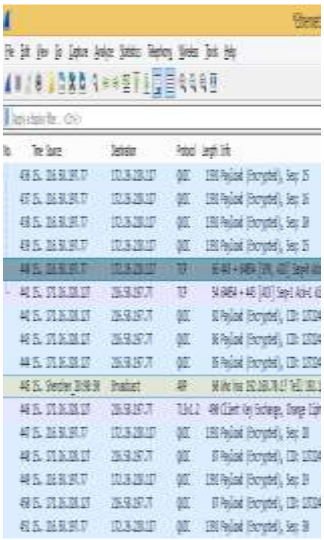


```
    Total Length = 1109
    TTL = 45
    Source IP = 216.58.197.74
    Destination IP = 10.71.5.155
⊞ TCP [34-1122]
  Unknown [54-1122]
```

The source codes of both these softwares can be modified according to one's own taste and use.

III. Experimental Setup

3.1 Analysis: Packet information/Traffic:
(i) Open a website on the web browser, while Wireshark and Network Miner running on the background, to analyse packets in both the softwares.



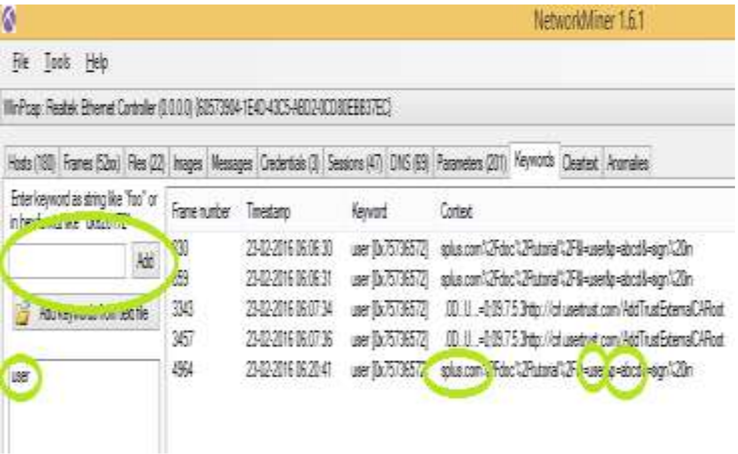
(ii) Use of filter toolbar to filter packets:
Open a website and login it with a wrong username and password. Now try to see it in Wireshark by using filter toolbar. In my case I goes to www.cplusplus.com and logged it in using the user name: "user" and password: "abcd".

Now stop wireshark from capturing more packets. Now, go to filter toolbar and type "frame contains cplusplus" and press enter.
Now select the packet and then right click on it->Follow->TCP Stream.

You can see the password there (below), in Wireshark:

And in Network Miner click on Keywords tab and then type user in the search option->Add
->Reload Case Files.
You can see the password there (below), in Network Miner:

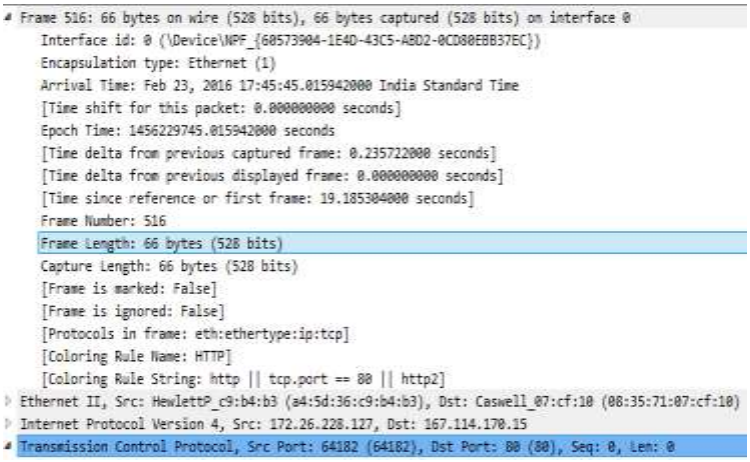
DOI: 10.18535/ijecs/v5i3.33


NetworkMiner 1.6.1
File Tools Help
WinPcap: Realtek Ethernet Controller (0.0.0.0) {60573904-1E4D-43C5-ABD2-0CD80EBB37EC}
Hosts (180) Frames (52xx) Files (22) Images Messages Credentials (3) Sessions (47) DNS (69) Parameters (201) Keywords Cleartext Anomalies
Enter keyword as string like "foo" or in hexadecimal like "0x00..."
Add
Add keywords from text file
user

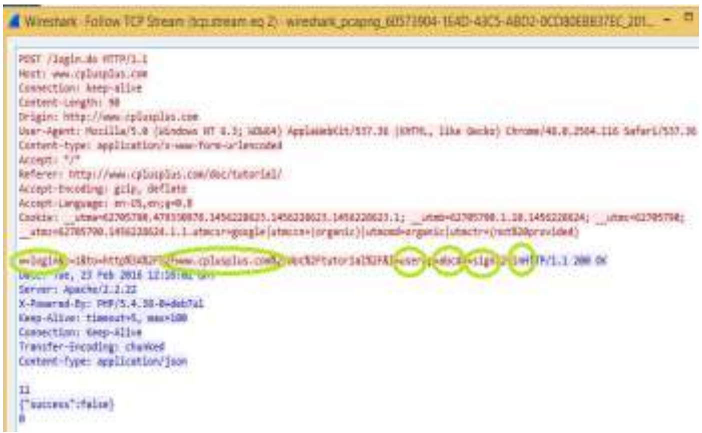
Frame number	Timestamp	Keyword	Context
330	23-02-2016 06:06:30	user [0x75736572]	splus.com%2Fdoc%2Ftutorial%2F&l=user&p=abcd&=sign%20in
359	23-02-2016 06:06:31	user [0x75736572]	splus.com%2Fdoc%2Ftutorial%2F&l=user&p=abcd&=sign%20in
3343	23-02-2016 06:07:34	user [0x75736572]	.0D..U...=&09.7.5.3http://crl.usertrust.com/AddTrustExternalCARoot
3457	23-02-2016 06:07:36	user [0x75736572]	.0D..U...=&09.7.5.3http://crl.usertrust.com/AddTrustExternalCARoot
4964	23-02-2016 06:20:41	user [0x75736572]	splus.com%2Fdoc%2Ftutorial%2F&l=user&p=abcd&=sign%20in

In Wireshark every detail of the packets can be studied. In this case, password can not be seen for those websites which uses a high encryption techniques. As whenever the password is filled, the password is sent in highly encrypted form, for eg.: Gmail, Facebook.

(iii) In wireshark and Network Miner, different packets can be sorted out according to the network tcp/ip protocols, which shows the frame summary, tcp/ip layers related data.



```
▲ Frame 516: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
    Interface id: 0 (\Device\NPF_{60573904-1E4D-43C5-ABD2-0CD80EBB37EC})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 23, 2016 17:45:45.015942000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1456229745.015942000 seconds
    [Time delta from previous captured frame: 0.235722000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 19.185304000 seconds]
    Frame Number: 516
    Frame Length: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
▷ Ethernet II, Src: HewlettP_c9:b4:b3 (a4:5d:36:c9:b4:b3), Dst: Caswell_07:cf:10 (08:35:71:07:cf:10)
▷ Internet Protocol Version 4, Src: 172.26.228.127, Dst: 167.114.170.15
▲ Transmission Control Protocol, Src Port: 64182 (64182), Dst Port: 80 (80), Seq: 0, Len: 0
```


Wireshark · Follow TCP Stream (tcp.stream eq 2) · wireshark_pcapng_60573904-1E4D-43C5-ABD2-0CD80EBB37EC_201...

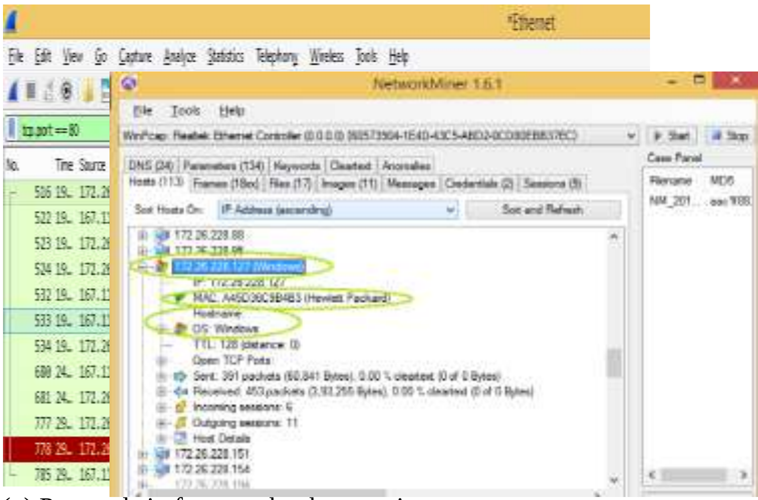
```
POST /login.do HTTP/1.1
Host: www.cplusplus.com
Connection: keep-alive
Content-Length: 90
Origin: http://www.cplusplus.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.116 Safari/537.36
Content-type: application/x-www-form-urlencoded
Accept: */*
Referer: http://www.cplusplus.com/doc/tutorial/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: __utma=62705790.478350076.1456228625.1456228625.1456228625.1; __utmb=62705790.1.10.1456228624; __utmc=62705790;
__utmz=62705790.1456228624.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)

w=login&=1&to=http%3A%2F%2Fwww.cplusplus.com%2Fdoc%2Ftutorial%2F&l=user&p=abcd&a=sign%20inHTTP/1.1 200 OK
Date: Tue, 23 Feb 2016 12:16:02 GMT
Server: Apache/2.2.22
X-Powered-By: PHP/5.4.38-0+deb7u1
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/json

11
{"success":false}
0
```

Information which can be retrieved from the picture (Wireshark), above:

(i) Frame number: 516
(ii) Frame length: 66 bytes
(iii) Captured length of the frame: 66 bytes
(iv) Arrival time: Feb 23, 2016 17:45:45 IST

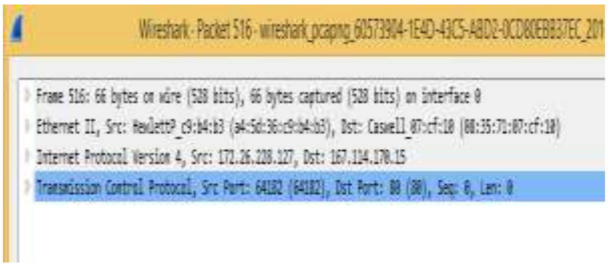

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port==80
No. Time Source
516 19.. 172.26
522 19.. 167.11
523 19.. 172.26
524 19.. 172.26
532 19.. 167.11
533 19.. 167.11
534 19.. 172.26
680 24.. 167.11
681 24.. 172.26
777 29.. 172.26
778 29.. 172.26
785 29.. 167.11
NetworkMiner 1.6.1
File Tools Help
WinPcap: Realtek Ethernet Controller (0.0.0.0) {60573904-1E4D-43C5-ABD2-0CD80EBB37EC}
Start
Stop
DNS (24) Parameters (134) Keywords Cleartext Anomalies
Hosts (113) Frames (18xx) Files (17) Images (11) Messages Credentials (2) Sessions (8)
Sort Hosts On: IP Address (ascending)
Sort and Refresh
Case Panel
Filename MD5
NM_201... aac788...

```
⊞ 172.26.228.88
⊞ 172.26.228.98
⊟ 172.26.228.127 (Windows)
    IP: 172.26.228.127
    MAC: A45D36C9B4B3 (Hewlett Packard)
    Hostname:
    OS: Windows
    TTL: 128 (distance: 0)
  ⊞ Open TCP Ports
  ⊞ Sent: 391 packets (60,841 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  ⊞ Received: 453 packets (3,93,256 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  ⊞ Incoming sessions: 6
  ⊞ Outgoing sessions: 11
  ⊞ Host Details
⊞ 172.26.228.151
⊞ 172.26.228.154
⊞ 172.26.228.156
```

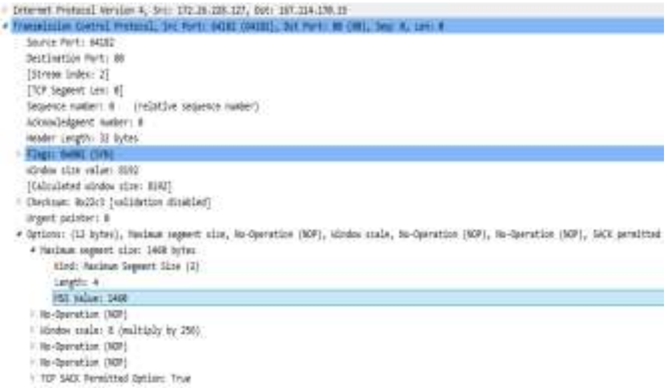
(v) Protocols in frame: eth:ethertype:ip:tcp

On the Ethernet Layer, the information retrieved is (in Wireshark), above:
(i) Destination address: 08:35:71:07:cf:10
(ii) Source address: a4:5d:36:c9:b4:b3

On Network Layer, the information retrieved (in Wireshark), above:
(i) IP version: 4
(ii) Header length: 20 bytes (0101 in binary)
(iii)Total length: 52
(iv) Time to live: 128


Wireshark · Packet 516 · wireshark_pcapng_60573904-1E4D-43C5-ABD2-0CD80EBB37EC_201

```
▷ Frame 516: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▷ Ethernet II, Src: HewlettP_c9:b4:b3 (a4:5d:36:c9:b4:b3), Dst: Caswell_07:cf:10 (08:35:71:07:cf:10)
▷ Internet Protocol Version 4, Src: 172.26.228.127, Dst: 167.114.170.15
▷ Transmission Control Protocol, Src Port: 64182 (64182), Dst Port: 80 (80), Seq: 0, Len: 0
```



```
▷ Internet Protocol Version 4, Src: 172.26.228.127, Dst: 167.114.170.15
▲ Transmission Control Protocol, Src Port: 64182 (64182), Dst Port: 80 (80), Seq: 0, Len: 0
    Source Port: 64182
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 32 bytes
  ▷ Flags: 0x002 (SYN)
    Window size value: 8192
    [Calculated window size: 8192]
  ▷ Checksum: 0x22c3 [validation disabled]
    Urgent pointer: 0
  ▲ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    ▲ Maximum segment size: 1460 bytes
        Kind: Maximum Segment Size (2)
        Length: 4
        MSS Value: 1460
    ▷ No-Operation (NOP)
    ▷ Window scale: 8 (multiply by 256)
    ▷ No-Operation (NOP)
    ▷ No-Operation (NOP)
    ▷ TCP SACK Permitted Option: True
```

On Transport Layer, the information retrieved (in Wireshark), above:
(i) Source port: 64182
(ii) Destination port: 80

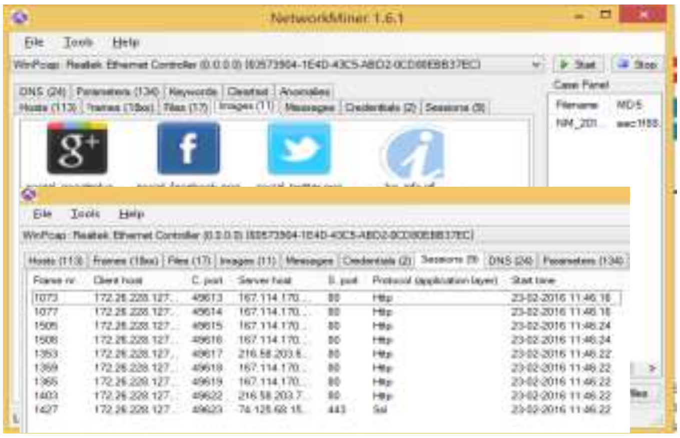
DOI: 10.18535/ijecs/v5i3.33

(iii) TCP segment length: 2
(iv) TCP header length: 32 bytes
(v) MSS value: 1460

In Wireshark, also the connection establishment by 3-Way Handshake and connection termination can be seen, but not in Network Miner.

In Network Miner, there is an option to sort hosts by IP address, MAC address, hostname, Operating System etc.

On the Hosts tab, one can see a list of hosts connected to the network. To see detailed information, like its MAC address, hostname, Operating System, TTL, Open ports, packets sent, received etc., expand any host by clicking on it, as shown in the picture below (in Network Miner):


NetworkMiner 1.6.1
File Tools Help
WinPcap: Realtek Ethernet Controller (0.0.0.0) {60573904-1E4D-43C5-ABD2-0CD80EBB37EC}
Start
Stop
DNS (24) Parameters (134) Keywords Cleartext Anomalies
Hosts (113) Frames (18xx) Files (17) Images (11) Messages Credentials (2) Sessions (9)
Case Panel
Filename MD5
NM_201... aac1f88...

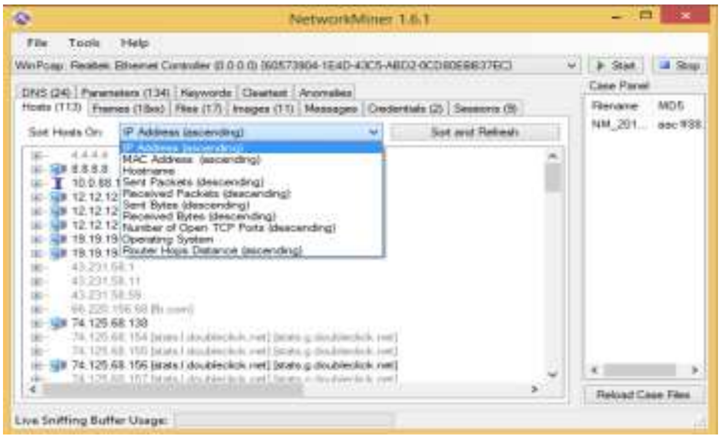
Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
1073	172.26.228.127...	49613	167.114.170....	80	Http	23-02-2016 11:46:18
1077	172.26.228.127...	49614	167.114.170....	80	Http	23-02-2016 11:46:18
1505	172.26.228.127...	49615	167.114.170....	80	Http	23-02-2016 11:46:24
1508	172.26.228.127...	49616	167.114.170....	80	Http	23-02-2016 11:46:24
1353	172.26.228.127...	49617	216.58.203.6...	80	Http	23-02-2016 11:46:22
1359	172.26.228.127...	49618	167.114.170....	80	Http	23-02-2016 11:46:22
1365	172.26.228.127...	49619	167.114.170....	80	Http	23-02-2016 11:46:22
1403	172.26.228.127...	49622	216.58.203.7...	80	Http	23-02-2016 11:46:22
1427	172.26.228.127...	49623	74.125.68.15...	443	Ssl	23-02-2016 11:46:22

There is a separate tab for images, as shown in the figure below (in Network Miner):

Information like DNS Query, DNS Answer, TTL, Client and Server IP addresses can be seen by clicking on the DNS tab, as shown below (in Network Miner):

Client port, source port can be seen by clicking on the Sessions tab, as shown below (in Network Miner):

Active and Passive sniffing:


NetworkMiner 1.6.1
File Tools Help
WinPcap: Realtek Ethernet Controller (0.0.0.0) {60573904-1E4D-43C5-ABD2-0CD80EBB37EC}
Start
Stop
DNS (24) Parameters (134) Keywords Cleartext Anomalies
Hosts (113) Frames (18xx) Files (17) Images (11) Messages Credentials (2) Sessions (9)
Sort Hosts On:
IP Address (ascending)
Sort and Refresh
IP Address (ascending)
MAC Address (ascending)
Hostname
Sent Packets (descending)
Received Packets (descending)
Sent Bytes (descending)
Received Bytes (descending)
Number of Open TCP Ports (descending)
Operating System
Router Hops Distance (ascending)
4.4.4.4
8.8.8.8
10.0.88.1
12.12.12
12.12.12
12.12.12
19.19.19
19.19.19
43.231.58.1
43.231.58.11
43.231.58.59
66.220.156.68
74.125.68.138
74.125.68.154 [stats.l.doubleclick.net] [stats.g.doubleclick.net]
74.125.68.155 [stats.l.doubleclick.net] [stats.g.doubleclick.net]
74.125.68.156 [stats.l.doubleclick.net] [stats.g.doubleclick.net]
Case Panel
Filename MD5
NM_201... aac1f88...
Reload Case Files
Live Sniffing Buffer Usage:

Sniffing is a technique for gathering network information through capturing network packets.

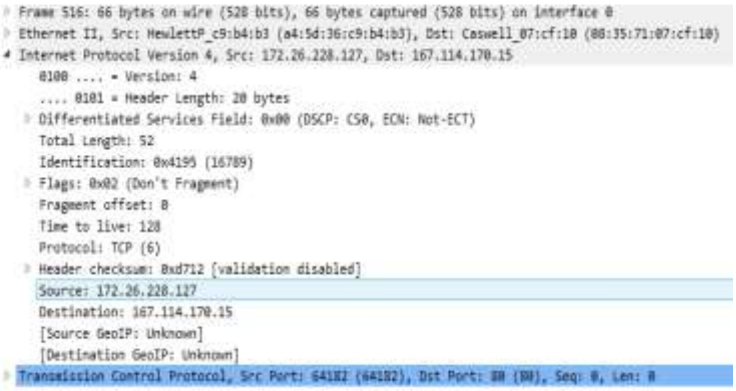
There are two types of sniffing:
(i) active sniffing and
(ii) passive sniffing

In active sniffing, the packet sniffing software sends request over the network and then in response calculates the packets passing through the network.

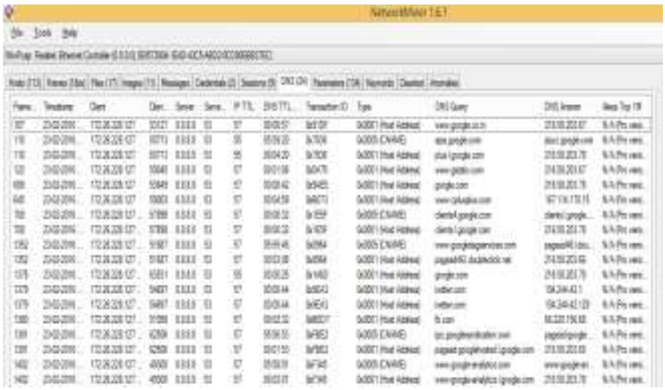
Passive sniffing does not rely on sending requests. This technique scans the network traffic without being detected on the network. Passive technique can be useful in places where networks are running critical systems like process control, radar systems, medical equipment or telecommunication, etc.

IV. Conclusion

In this paper we analysed two network analysing tools: Wireshark and Network Miner, based on different parameters: graphical user interface (basic), packet information and traffic analysis. Both the tools discussed here are passive sniffers. Both the tools can be used to reconstruct the webpage from the captured data. Network Miner is also able to do O.S. fingerprinting. Also any active scanning should be avoided since it might affect the performance of the network or hosts on the network. These network sniffers can be utilised for: (i) Analysing network problems (ii) Detect network intrusion attempts. And a large memory space may be required to properly analyse the data.



```
Frame 516: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: HewlettP_c9:b4:b3 (a4:5d:36:c9:b4:b3), Dst: Caswell_07:cf:10 (00:35:71:07:cf:10)
Internet Protocol Version 4, Src: 172.26.228.127, Dst: 167.114.170.15
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 52
  Identification: 0x4195 (16789)
  Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0xd712 [validation disabled]
  Source: 172.26.228.127
  Destination: 167.114.170.15
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 64182 (64182), Dst Port: 80 (80), Seq: 0, Len: 0
```



DOI: 10.18535/ijecs/v5i3.33

V. REFERENCES

[1] Performance analysis of VoIP spoofing attacks using classification algorithms, G. Vennila, N. Supriya Shalini, MSK. Manikandan, IEEE 2014.

[2] Study of Computer Network Issues And Improvising Drop Rate Of TCP Packets Using NS2, Shweta Gambhir, Kuldeep Tomar, DOI:10.5121/ijfcst.2014.4407.

[3] Converting PCAPs into Weka Mineable Data, Charles A. Fowler and Robert J. Hammell II, IEEE 2014.

[4] Modeling and Simulating MPLS Networks, Azeddien M. Sllame, IEEE 2014.

[5] Design and Implementation of a forensic framework for Cloud in OpenStack cloud platform, Saibharath S, GeethaKumari G, IEEE 2014.

[6] Development and Experimentation of TCP Initial Window Function, Runa Barik, Dinil Mon Divakaran, IEEE 2013.