Discrete Analysis and Modern Assessment of Packet Sniffer and Network Monitoring Tools-A Comparative Survey

Mohd Muntjir

Department of Information Technology, College of Computers and Information Technology Taif University, Kingdom of Saudi Arabia

Abstract—*Network monitoring signifies to the practice of managing the procedure of a computer network using specified management software tools. As network persist to grow,it isvery important that network administrators are responsive of the various types of traffic that is navigating their networks ,and offers appropriate resources for decision making system. Network monitoring systems are operated to confirm availability and inclusive enactment of computers and network facilities. In modern days there are more than billions of packets moving throughout the web sky. A significant numbers of them are of malicious focused. These packets assist us to comprehend when there are prominent security or presentation procedures occurring on the network and also to find out collective network complications such as loss of connectivity and slow network etc. These paper emphases on the comparative study of diverse packet analyzers, that are accessible in current market and how we can select amongst them rendering to our necessities. Network monitoring for a commercial network is a analytical IT function that can save money in network functioning, employee efficiency and organization cost overruns. Traffic monitoring and analysis is very important in order to more efficiently troubleshoot and solve issues when they happen. A number of tools are accessible to help administrators to monitor and evaluation of network traffic in network. This paper presents a comparative analysis of some present packet sniffers with their functioning.*

Keywords—Packet analysis, Sniffer Traffic Flow, Packet capturing, Wireshark, Tcpdump, Etherape, capsa, libpcap,snoop.

I. INTRODUCTION

Network monitoring can be accomplished using different software or an arrangement of plug-and-play hardware and software application elucidations. Furthermore, virtually it is easy to monitor any kind of network. It doesn't matter whether it's wireless or wired network, a commercial Local Area Network, Virtual Private Network or service provider Wide Area Network. Anyone can monitor devices on different operating systems with a variety of functions, oscillating from IPhone to BlackBerrys and other cell phones, and from routers and switches, to servers. The Consequences that enable a corporate are to address numerous and various requirements comprising meeting agreement necessities, stomping out core security threats and delivering more operative reflectivity. Deciding precisely what to monitor on our network is as important as stipulating network monitoring a overall turndown. We must be sure that our business network topology map is up to date and working accurately. That map should precisely lay out the different types of networks to be observed, which servers are running in a good manner and which applications on which operating system are working fine, and how many desktops must to be considered into the mix and what kind of remote devices have entrance for each network. To specify a precise view on each tool we have isolated them into distinctive categories such as console based, Graphical User Interface based or both types based. We conducted a inclusive evaluation of different tools such as wireshark, tcpdump, etherape, netsniff-ng, capsa, snoop and many more different tools. The packet capturing libraries used by these tools are winpcap, libpcap, libc etc.

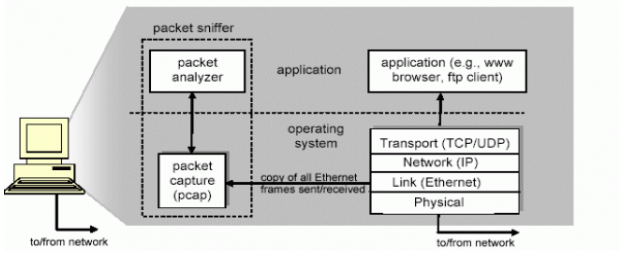

Fig.1: Pcap sniffer structure

The languages in which these tools are created such as C++, C, perl and the operating system they support such as Unix, Linux, windows, and we have also

considered the auspicious and the opposed factors; or advantages and disadvantagesof each tool over the other which will advantage the users to choose the packet analyzer according to their necessity [1]. The objective of network performance monitoring tools is to stipulate a description of operations so potential problems can be proactively evaded, and irregularities that do occur can be perceived, separated, and determined with a minimum mean-time-to-repair.

II. CAPTURING LIBRARIES USED BY DIFFERENT TOOLS

2.1 Capturing Libraries by Wireshark

Wireshark is a network protocol analyzer tool, and is the standard in many enterprises. It is the extension of a project that started in 1998[4]. Thousands of developers around the world have subsidized to it and it is still under vigorous expansion. Wireshark network analyzer is useful for analyzing network complications, discovering network intrusions, and network misuse, monitor usage and gather information.This is a very powerful tool that specifies network and upper layer protocols observation about data captured in a network. It observes the pcap network library to capture packets in a network [5].

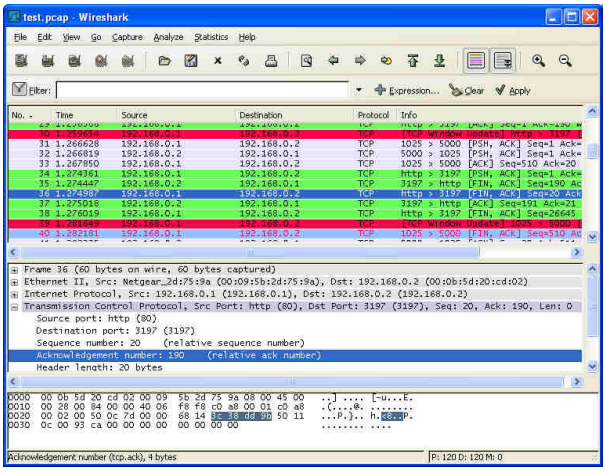

Fig.2 : Wirshark

2.2 Capturing libraries by Tcpdump

Tcpdumpis a collective packet analyzer tool that runs under the command line option. It permits the user to capture and demonstrate TCP/IP and other packets being spread or acknowledged over a network to which the computer is covered. Tcpdump uses libpcap packet capturing library to capture the packets. WinDump is the Windows version of TCPDump. Tcpdump publishes the subjects of network packets. It can read packets from a network interface card or from a earlier established saved packet files. Tcpdump can write packets to standard output.TCPDump uses the WinPcap library that is the Windows version of libpcap [2].

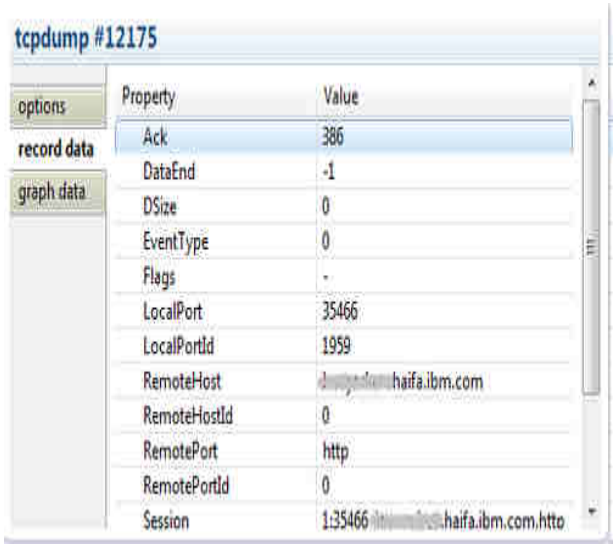

Fig:TcpDump

2.3 Capturing libraries by Netsniff-ng

Netsniff-ng is a zero copy analyzer tool that captures the packets and replayer that supports the pcap file format. Netsniff-ng is a network analyzer and networking toolkit. The toolkit presently comprises of a packet capturere and replayer, network analyzer, an encrypted multuser IP tunnel, a wire-rate traffic generator, networking statistic tools, a Barkeley Packet compiler, and an autonomous system trace route [7].

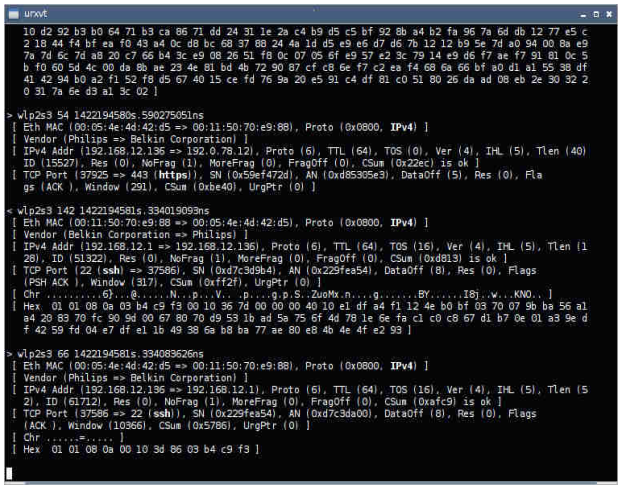

Fig.3:Netsniff-ng

2.4 Capturing libraries by EtherApe

EtherApe is graphical network monitor for UNIX sculpted after etherman. Performing link layer, IP and TCP approaches, it demonstrations network action graphically, Hosts and links variation in size with traffic. It supports Ethernet, Token Ring, FDDI, ISDN, SLIP, PPP, and WLAN devices, plus several encapsulation structures. It can filter traffic to be presented, and can deliver packets from a file as well as

live from networks. EtherApe is free and open source software established under the GNU General Public License [8].

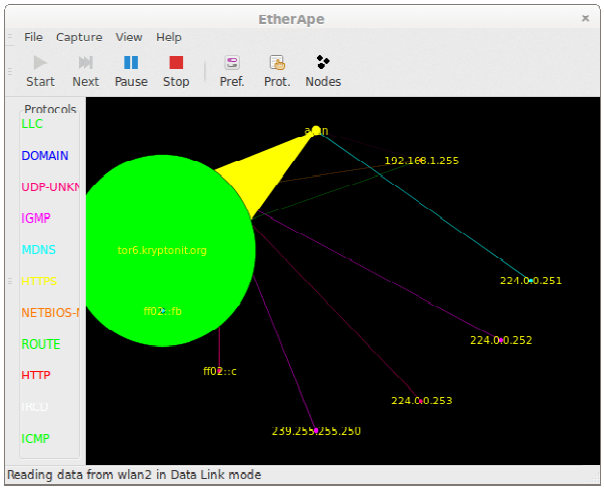

Fig.4: EtherApe

2.5 Capturing libraries by Capsa

Capsa is from a family of packet analyzer tool developed by Colasoft to analyze, troubleshoot and observe wired and wireless network. Capsa Network Analyzer is a very easy; Ethernet packet sniffer for network monitoring and troubleshooting reasons. It accomplishes real time packet capturing, reliable network forensics, full time network monitoring, full in-depth packet decoding, inevitable expert analyzing ,and unconventional protocol analyzing. By giving us insights into all of our network's procedures, Capsa creates it easy to segregate and resolve network complications, and identify network holdup and bandwidth use [9].

Fig.5: Capsa

2.6 Capturing libraries by Snoop

Snoop is a more effective and useful monitoring tool because it has a much better user interface and displaying proficiencies. Snoop is a very adaptable command line packet sniffer tool comprised as part of Sun Microsystems' Solaris Operating system. It delivers powerful filters for analysis of problems associated to NFS, NIS and RPC. It is pretty cable sniffer tool equal or better than TCPdump. The snoop network analyzer tool hustled with Solaris captures packets from the network and shows them in numerous forms according to the set of filters stipulated.In its modest form; snoop captures and displays all packets current on the network interface.By default snoop demonstrations only a concise of the data relating to the highest level protocols. It displays the source and destination of the network packet in the form source to destination. This Snoop tool maps the IP address to the hostname when possible else it displays the IP address. Snoop lists the highest level protocol category[13].

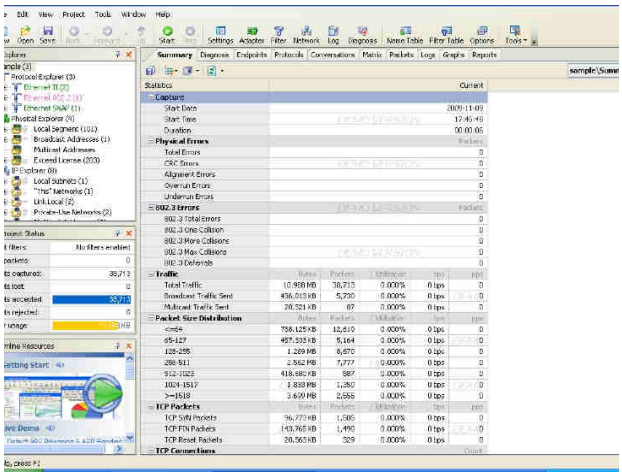

Fig.6: Snoop

III. OPERATING SYSTEM SUPPORT

To isolate each tool on the origin of operating systems they maintain, will assist the user to appreciate and use each tool according to their requirements.

3.1 Operating System Supported by Wireshark:

Wiresharksupports any version of Windows. This includes Windows 10, Windows 8, Windows 7, Windows Vista, Windows Server 2016, Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008.Wireshark runs on most UNIX and UNIX-based platforms comprising OS X and Linux. The system requirements should be comparable to the Windows standards listed beyond. Furthermore,binary packages are available for most Unix and Linux distributions including the following platforms:Debian GNU/Linux, Gentoo Linux, FreeBSD, Mandriva Linux, HP-UX,NetBSD, Red Hat Enterprise/Fedora Linux

,OpenPKG, , Sun Solaris/SPARC,Sun Solaris/i386, Canonical Ubuntu.Wireshark also works on Apple OS X[1].

3.2 Operating System Supported by Tcpdump:
Tcpdump succeeds on most Unix-like operating systems: Solaris, Linux, BSD, OS X, HP-UX, AIX, and Android among others.In those methods, tcpdump used the libpcap library to capture packets.The port of tcp dump for Windows is called WinDump.it operates WinPcap, that is called the Windows port of libpcap.The use of tcpdump is mostly due to its capability to measure packet timestamps in an OS's kernel space. At least from kernel version 2.1.96, Linux supports a packet capture method called Linux Socket Filter which is based on BPF and delivers kernel level packet categorizing [2].

3.3 Operating System Supported by Netsniff-ng
is originally created as a network sniffer with support of the Linux kernel packet mmap interface for network packets, but now days; more tools have been enhanced to create it a convenient toolkit such as the iproute2suite. Distribution specific packages are accessible for all main operating system allocations such as Debian and Fedora Li. It has also been enhanced to Xplico's Network Forensic Toolkit, SecurityOnion, and GRML Linux to the Network Security Toolkit .The netsniff-ng toolkit is also benefited in academia.

3.4 Operating System Supported by EtherApe:
EtherApe was developed by Juan Toledo.EtherApe is a packet sniffer or network traffic monitoring tool, acquired for Unix and Unix like operating systems. EtherApe is free and open source software developed under the GNU General Public License [3].

3.5 Operating System Supported by Capsa
Capsais an Ethernet packet analyzer designed by Colasoft for personal usage. it supports both Ethernet and Wireless Local Area networks(WLAN).Capsa packet analyzer supports all Microsoft Windows Operating Systemss for instance as Microsoft Windows XP,Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1,and Microsoft Windows 10 Operating Systems.

3.6 Operating System Supported by Snoop:
snoop is a flexible command line packet analyzer tool, included as part of Sun Microsystems'Solaris Operating System. The source code for Snoop network analyzer is available via the OpenSolaris projects.The snoop command line can come very convenient to observe the network traffic to troubleshoot any network related subjects like packet drops, and high network potential etc.

IV. KEY FEATURES

4.1 Features of Wireshark
Wireshark is software that comprehends the structure of different networking protocols in a network system. It can analyze and demonstrate the fields with their meanings as stated by different networking protocols. Wireshark procedures pcap to capture packets hence it can only capture packets on the types of networks that pcap verifies[10].
The following are some characteristics Wireshark delivers:

- Available for Windows and UNIX
- Open files comprising packet data captured with tcpdump.
- Capture live packet data from a network interface.
- Demonstrate the packets with comprehension protocol information.
- Import packets from text files comprising hex dumps of packet data.
- Save packet data apprehended.
- Export some or all packets in a number of capture file formats.
- Exploration for packets on many standards.
- Filter packets on many criteria.
- Construct numerous statistics.
- Live capture from many different network media
- Colorize packet display constructed on filters.
- Import files from other capture programs
- Data can be captured from the wire and from a live network connection.
- Export files for many other apprehension program
- On-screen data can be recite from a different types of networks, incorporating IEEE 802.11, Ethernet, (PPP)Point ot Point Protocol, and loopback address.
- Captured files can be programmatically edited via command-line switches to the editcap program.
- Data display can be improved via a display filter.
- Captured network data can be glanced via a Graphical User Interface (GUI) or via the command line terminal.
- Raw USB traffic can be captured.

- Wireless connections can also be filtered as long as they crosswise the monitored Ethernet.
- VoIPcalls in the captured traffic can be perceived.
- Several settings, filters and timers can be set that confirm only triggered traffic appear.

4.2 Features of Tcpdump

Tcpdump is a effective packet sniffer and a common tool operated by system administrators to resolve network problems and explore traffic in a network. It can be operated with Boolean expressions to capture only those packets you are interested.It is the most commonly expended network sniffer tool.

- It is command line-based tool and runs on UNIX-based operating systems.
- It was created by the Network Research Group (NRG) of the Information and Computing Sciences Division at Lawrence Berkeley National Laboratory and is now being dynamically created and provided at www.tcpdump.org.
- An important feature of tcpdump is a filter that consents to display only the packets you want to see and captures.
- Some of the features comprise the capability to read capture files from tcpdump.
- Ethereal has numerous powerful characteristics, comprising a rich flaunt filter language and the ability to understand the recreated stream of a TCP session.TCPDump can be expended to read live packets from the wire.
- It also uses a very widespread filter language.
- The detail and length of the TCPDump output can be controlled by various options including -vvv, -vv, –v,-q and -X [6].

4.3 Features of Netsniff-ng

The netsniff-ng toolkit comprises of the following functionalities:

- Netsniff-ng is a fast network analyzer established on packet mmap (2) appliances. It can record pcap files to disc, repeat them and also do an offline and online investigation. Capturing, investigating or replay of raw 802.11 frames is maintained very well. Pcap files are also well-matched with tcpdump. Netsniff-ng procedures those pcap signs either in scatter-gather mmap (2) I/O or by I/O.
- Trafgen- is a multithreaded network traffic generator constructed on packet mmap (2) proceduress. It has its own elastic and macro-based low-level packet arrangement language. Additions of raw 802.11 frames are verified very well. It has a expressively higher speed than mausezahn and comes more closer to pktgen, however runs from user place. Pcap suggestions can also be transformed into a trafgen packet arrangement.
- Mausezahn- is a high-level packet creator that can run on a hardware and software purpose and comes with a Cisco-like Command Line Interface. It can make nearly each promising or impossible packetS. Hence, it can be used to test network behaviour under bizarre conditions or to test hardware software utilizations for different kind of attacks.
- Bpfc-is a Berkeley Packet Filter compiler that comprehends the innovative Berkeley Packet Filter language created by McCanne and Jacobson. It admits Berkeley Packet Filter prompts and changes them into kernel/netsniff-ng readable Berkeley Packet Filter ``opcodes''. This can exclusively be useful for more intricated filters that high level filters fail to reinforce.
- Ifpps- is a tool which regularly delivers top like networking and system statistics from the kernel in Linux. It collects statistical data immediately from procfs files and does not relate any user space traffic monitoring that would misrepresent statistics on high packet rates.
- Flowtop- is a top-like connection chasing tool that can run on an end host or router in a network. It is capable to impart TCP or UDP flows that have been gathered by the kernel's netfilter structure. GeoIP and TCP state machine information is demonstrated. Although, on end hosts flowtop can show PIDs and application names that flows associate to. No user space traffic monitoring is completed, hence all data is collected by the kernel in Linux.
- Curvetun- is a frivolous, high speed ECDH multiuser tunnel for Linux OS. Curvetun helps the Linux TUN/TAP interface and reinforces {IPv4 and IPv6} over {IPv4 and IPv6} with UDP or TCP as carrier protocols in a network. Packets are encoded end-to-end by a symmetric stream cipher and validated by a MAC (Poly1305); where keys have formerly been calculated with the ECDH key agreement protocol.
- Astraceroute- is an autonomous system (AS) trace route efficiency. Dissimilar to traceroute or tcptraceroute; it not only display hops, however also their AS information they belong to as well as GeoIP information and other fascinating things. On other wa; it operates a TCP analysis packet and falls back to ICMP analyses in case no ICMP answer has been expected[14].

4.4 Features of Etherape

Etherape has the features in a following given order:

- Network traffic is demonstrated graphically. The more talkative a node is, the larger its demonstration.
- Node and link color shows the most expended protocol.
- You may either observe at traffic within your network; end to end IP or even port to port TCP.
- User may select what level of the protocol stack to essence on.
- Live data can be read from ethernet, WLAN interfaces, FDDI, Point to Point Protocol, SLIP and plus several other incapsulated formats.
- Data can be captured "off the wire" from a live network link, or interpret from a tcpdump capture file.
- The following frame and packet types are currently supported: ETH_II, 802.2, 803.3, IP, X25L3,IPv6, REVARP, ARP, AARP ,ATALK, , IPX, TRAIN, LOOP, VINES, ICMP, VLAN, GGP, IPIP,IGMP, EGP, TCP, PUP, IDP, UDP, TP, RSVP, GRE, ROUTING,ESP, EON, AH, VINES,OSPF, , EIGRP, ENCAP, IPCOMP, PIM,VRRP; and most TCP and UDP services, as TELNET, HTTP, FTP, NNTP, POP3, NETBIOS, DOMAIN, IRC, SNMP, etc.
- Protocol summary dialog presents global traffic statistics by protocol.
- Data display can be improved using a network filter using pcap syntax.
- Clicking on a node opens a detail dialog showing protocol breakdown and other traffic information.
- Display averaging and node resolve times are fully configurable.
- Node statistics export to XML file.
- Node summary dialog displays traffic statistics by node.
- A single node can be centered on the display.

4.5 Features of Capsa:

- Wired & wireless network real-time packet capturing
- Captures packets from a single or multiple network adapters
- Traffic & bandwidth monitoring
- Multiple network behaviour monitoring
- Advanced protocol analysis
- Expert network diagnosis
- Email contents preservation
- Quick & intuitive reports
- Provides statistics on MAC & IP address
- Network activity logging
- Analyse Protocol (Data link to Application Layer)
- Analyses the header & contents of each packet
- Presents statistics in graphs
- Alerts Computer network anomalies
- In-depth packet decoding
- Logs DNS, web browsing, Email, FTP & IM services
- Outputs packets & logs to files

4.6 Features of Snoop

- The snoop capture file format is explained in RFC 1761.
- Snoop can demonstrate the packets as soon as they are received or saved.
- Snoop itself can be use read and explain the file.
- It has pretty effective packet filtering engine.
- The snoop command can capture both IPv4 and IPv6 packets.
- It can display IPv6 extension headers, IPv6 headers, ICMPv6 headers and neighbor detection protocol data.
- By stating the ip or ip6 protocol keywords, the snoop command displays only IPv4 or IPv6 packets.
- Other then IPv6 traffic snoop competences are very comparable to tcpdump and output formats are almost equal.

V. MECHANISM

5.1 Mechanism of Wireshark,

- Previously known as Ethereal, proposed a sophisticated interface and industrial strength proficiencies, plus it is as good as any packet sniffer that costs thousands of Euros[11].
- Wireshark is very similar to tcpdump, but has a graphical front end plus some combined sorting and filtering selections.
- If a remote machine captures packets and broadcasts the encapsulated packets to a machine running Wireshark using the TZSP protocol Wireshark separates those packets, therefore it can investigate packets captured on a remote machine at the time that they are captured.
- Packet capture specifies information about network data packets; such as the source, destination, transmit time, protocol types (TCP, IGMP and HTTP) and "header" data such as classification and responses.

- Wireshark will normally demonstrate the information in three panels: 1- transmission overview, 2-packet details and 3-a pane showing raw hex.
- If we need to see what is inside the packets; we're going to have to plug a host into the network anywhere along the path navigated by the packets.
- In Wireshark users can also create and save filters for later use in his network.
- Wireshark supports built in explorations to improve in on specific data or environments, and will even construct I/O graphs to display usage by packet type [1], [2].

5.2 Mechanism of Tcpdump

- Tcpdumpcaptures packets on the network by retaining a local interface in uninhibited mode.
- Generally, our network interface will disregard any pockets that aren't adapted to our network. By placing our interface in promiscuous mode, tcpdump apprehends all packets, irrespective of address and acknowledges us to inspect their headers.
- The tcpdump program also consents you to excerpt specific types of network traffic based on header information.
- In some Unix-like operating systems, a user must have superuser rights to use tcpdump because the packet capturing mechanisms on those systems require preeminent privileges.
- tcpdump uses libpcap to do packet capture;
- libpcap uses some mechanism in the Operating System kernel to do packet capture; that mechanism has, for each capture in progress on each network interface, buffers into which copies of packets are placed.
- The libpcap interface supports a filtering mechanism created on the framework in the BSD packet filter.

5.3 Netsniff-ng

- Netsniff-ng was originally created as a network sniffer with support of the Linux kernel zero-copy interface for network packets but later on; more tools have been enhanced to construct it a useful toolkit such as the iproute2 suite.
- The toolkit basically comprises of a network analyser, packet capturer and replayer, an encrypted multiuser IP tunnel, networking statistic tools, a Berkeley Packet Filter (BPF) compiler, a wire-rate traffic generator, an autonomous system trace route and man more.
- The gain of performance is reached by zero-copy mechanisms, so that the kernel does not essential to copy packets from kernel space to user space.
- Programs using libpcap also use that mechanism on Linux.
- If geographical IP location is expended, the built-in database update mechanism will be evoked to obtain Maxmind's modern database with the help of –U option.

5.4 Etherape:

- Etherape is a network traffics are displayed using a graphical interface. Every node denotes a exclusive host.
- Links characterize connections to hosts.
- Nodes and links are colour coded to exemplify different protocols establishing the numerous categories of traffic on the network.
- Distinctive nodes and their connecting links transmit and shrink in size with enlargements and cutbacks in network traffics.
- It supports Ethernet, Token Ring, FDDI, ISDN, and SLIP, PPP and WLAN devices plus numerous encapsulation formats.
- It can filter traffic to be presented, and can read packets from a file as well as live from the network [8].

5.5 Capsa:Colasoft Capsa utilizes such a appliance to capture packets in a network. It receipts every network component, such as IP addresses, packets, MAC addresses, protocols, as network objects, and incorporates them into a project. Hence, every tiny change on the network will be monitored and investigated to the project.

- Capsa is an easy to use convenient network analyzer.
- It is a perfect network tool for real-time network monitoring, troubleshooting and network analysis. Capsa suggestions a inclusive reflectivity of your LAN or WLAN networks.
- The leading proficiencies of Capsa network analyzer include in-depth packet interpreting, progressive protocol analysis and impulsive expert diagnosis [9].

5.6 Snoop: Snoop demonstrates the packets in a single line summary form otherwise in verbose multi line arrangements.

- Snoop itself can be used read and explain the file for example; publish summar, consumed summary and full packets dumps.
- Snoop has more powerful packet filtering engine.
- Another tool Ethereal's editcap program can be used for inducing the snoop file to a tcpdump file.Although,it is only packets for which the expression is true that are elected. If no expression is released it is presumed to be true.
- Given a filter expression, the snoop produces code for either the kernel packet filter, or for its own internal filter. This filter is instigated as a streams element, upstream of the buffer element.
- The buffer element collects packets until it becomes full and passes the packets on to snoop.
- If packets are read from a capture file by the -i option then only the packet filter for snoop is managed.

VI. CONCLUSION

Wireshark is alike to tcpdump, although with extra descriptions such as graphical user interface (GUI) and many innovative sorting and filtering choices, while wireshark is easier to use than tcpdump, it still limits the size of target evaluating files. wireshark cannot analyze more than two days network actions in individual computers. To observe more than two-day actions, network managers must control wireshark by repeating capturing and analyzing processes regularly to evade extreme system memory uses. Tcpdump is a powerful tool that permits administrators sniff network packets and make some statistical investigation out of those dumps. The main disadvantage to tcpdump is the size of the flat file comprising the text output while the other disadvantage is that tcpdump runs under the command line mode. TcpDumpdoes not have a user friendly Graphical User Interface (GUI)[12]. Hence the user has to study essential commands and get familiar with the command prompt. On the other hand Wireshark has a very good user approachable Graphical User Interface..Netsniff-ng- It is a very useful sniffing tool. But it has one disadvantage of performance deprivation and bigger memory footmark for the ring buffer. Note that this does'nt affects (pcap) capturing mode; sincetpacket in version 3 is used.Etherape's is also a very valuable sniffer tools to monitoring the network and packet analyzer. The real benefit to Capsa is the user interface.colasoft capsa has a lot of other benefits, but two general advantages of capsa are –first, the information evaluated by capsa is more comfortable to retrieve and inspect, and second advantage is; the porgram itself is very user accessible and easy to understand. Snoop is a well-organized and useful monitoring tool since it has a much better user interface and displaying capabilities. The only disadvantage being that since it is tightly integrated within the Solaris kernel, its use is largely limited to Sun based systems.

ACKNOWLEDGEMENTS

I would like to gratefully and sincerely thank The Dean of ourCollege, Chairman of IT Department for his guidance, understanding, patience, and most importantly, his friendly nature during this research paper writing at Taif University. I would also like to thank all of the members of the research group and friends who have always supported me for giving the opportunity to write this research paper.

REFERENCES

[1] Network Traffic Monitoring ieee paperwww.ijarcsse.com/docs/papers/january2012/V2I1059.pdf by Prof. Radha S. Shirbhate
[2] WiresharkIntroduction: http://en.wikipedia.org/wiki/Ettercap_%28computing%29wireshark
[3] A Survey of Network Traffic Monitoring and Analysis Tools www.cse.wustl.edu/~jain/cse567-06/ftp/net...monitors3/index.html
[4] Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection by Usha Banerjee
[5] Wiresharkmachanisms:http://en.wikipedia.org/wiki/Wireshark
[6] Tcpdumpintroduction: .http://en.wikipedia.org/wiki/Tcpdump
[7] Netsniff-ng –the packet sniffing beast:-.http://netsniff-ng.org/
[8] Etherape introduction and key features:-http://en.wikipedia.org/wiki/Etherape
[9] Capsa:-.http://en.wikipedia.org/wiki/Capsa
[10] WiresharkFeatures:.http://www.wireshark.com/wireshark-reviews downloads.html
[11] http://www.wireshark.org/about.html
[12] OludeleAwodele, OtusileOluwabukola, A.C Ogbonna, and AjayiAdebowale, Ilishan-Remo ,"Packet Sniffer –A Comparative Characteristic Evaluation Study" ,Issues in Informing Science and Information Technology ,page 91-100 ,Volume 10, 2013
[13] ShrutikaSuri, VandnaBatra, "Comparative Study of Network Monitoring Tools", International Journal of Innovative Technology and Exploring Engineering,page 63-65, Volume-1, Issue-3, August 2012

[14] Dr. CharuGandhi,GauravSuri, Rishi P. Golyan,PupulSaxena ,Bhavya K. Saxena, "Packet Sniffer – A Comparative Study", International Journal of Computer Networks and Communications Security, page 179-187, VOL. 2, NO. 5, MAY 2014,