

Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology

Experiment No. : 1

Date: _____

Title : Packet Sniffing using Wireshark

Problem Definition : To capture packets of user-credentials during login process and check whether they are encrypted or not using packet sniffing tool, Wireshark. Perform this on website using HTTP and HTTPS protocol and inspect whether the websites the user-credentials or not.

Pre-requisite : Knowledge about various networking protocols such as HTTP, HTTPS, TCP etc and some knowledge about wireshark tool .

Theory :

Packet sniffing:

Packet sniffing is a form of wire-tap applied to computer networks instead of phone networks. It came into vogue with Ethernet, which is known as a "shared medium" network. This means that traffic on a segment passes by all hosts attached to that segment. Ethernet cards have a filter that prevents the host machine from seeing traffic addressed to other stations. Sniffing programs turn off the filter, and thus see everyone's traffic.

Today's networks may already contain built-in sniffing modules. Most hubs support the RMON standard, which allow the intruder to sniff remotely using SNMP, which has weak authentication. Many corporations employ Network Associates "Distributed Sniffer Servers", which are set up with easy to guess passwords. Windows NT machines often have a "Network Monitoring Agent" installed, which again allows for remote sniffing.

Packets sniffing is difficult to detect, but it can be done. But the difficulty of the solution means that in practice, it is rarely done.

The popularity of packet sniffing stems from the fact that it sees *everything*. Typical items sniffed include:

SMTP, POP, IMAP traffic

Allows intruder to read the actual e-mail.

POP, IMAP, HTTP Basic, Telnet authentication

Reads passwords off the wire in clear-text.

SMB, NFS, FTP traffic

Reads files of the wire.

SQL database

Reads financial transactions and credit card numbers.

Not only can sniffing read information that helps break into a system, it is an intrusion by itself because it reads the very files the intruder is interested in.

Top 10 Packet Sniffing tools:

1: [Wireshark](#)

Wireshark (known as Ethereal until a trademark dispute in Summer 2006) is a fantastic open source network protocol analyzer for Unix and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, delving down into just the level of packet detail you need. Wireshark has several powerful features, including a

Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology

rich display filter language and the ability to view the reconstructed stream of a TCP session. It also supports hundreds of protocols and media types. A tcpdump-like console version named tethereal is included. One word of caution is that Ethereal has suffered from dozens of remotely exploitable security holes, so stay up-to-date and be wary of running it on untrusted or hostile networks (such as security conferences).

<http://media-2.cacotech.com/video/wireshark/introduction-to-wireshark/>

2: [Tcpdump](#)

Tcpdump is the IP sniffer we all used before Ethereal (Wireshark) came on the scene, and many of us continue to use it frequently. It may not have the bells and whistles (such as a pretty GUI or parsing logic for hundreds of application protocols) that Wireshark has, but it does the job well and with fewer security holes. It also requires fewer system resources. While it doesn't receive new features often, it is actively maintained to fix bugs and portability problems. It is great for tracking down network problems or monitoring activity. There is a separate Windows port named WinDump. TCPDump is the source of the Libpcap/WinPcap packet capture library, which is used by [Nmap](#) among many other tools.

3: [Cain and Abel](#)

UNIX users often smugly assert that the best free security tools support their platform first, and Windows ports are often an afterthought. They are usually right, but Cain & Abel is a glaring exception. This Windows-only password recovery tool handles an enormous variety of tasks. It can recover passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols. It is also [well documented](#).

4: [Kismet](#)

Kismet is a console (ncurses) based 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. It identifies networks by passively sniffing (as opposed to more active tools such as [NetStumbler](#)), and can even decloak hidden (non-beaconing) networks if they are in use. It can automatically detect network IP blocks by sniffing TCP, UDP, ARP, and DHCP packets, log traffic in Wireshark/TCPDump compatible format, and even plot detected networks and estimated ranges on downloaded maps. As you might expect, this tool is commonly used for wardriving. Oh, and also warwalking, warflying, and warskating, ...

5: [Dsniff](#)

This popular and well-engineered suite by Dug Song includes many tools. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy passively monitor a network for interesting data (passwords, e-mail, files, etc.). arp spoof, dnsspoof, and macof facilitate the interception of network

Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology

traffic normally unavailable to an attacker (e.g, due to layer-2 switching). sshmitm and webmitm implement active monkey-in-the-middle attacks against redirected ssh and https sessions by exploiting weak bindings in ad-hoc PKI. A separately maintained partial Windows port is available here. Overall, this is a great toolset. It handles pretty much all of your password sniffing needs.

6: [NetStumbler](#)

Netstumbler is the best known Windows tool for finding open wireless access points (“wardriving”). They also distribute a WinCE version for PDAs and such named [Ministumbler](#). The tool is currently free but Windows-only and no source code is provided. It uses a more active approach to finding WAPs than passive sniffers such as [Kismet](#) or [KisMAC](#).

7: [Ettercap](#)

Ettercap is a terminal-based network sniffer/interceptor/logger for ethernet LANs. It supports active and passive dissection of many protocols (even ciphered ones, like ssh and https). Data injection in an established connection and filtering on the fly is also possible, keeping the connection synchronized. Many sniffing modes were implemented to give you a powerful and complete sniffing suite. Plugins are supported. It has the ability to check whether you are in a switched LAN or not, and to use OS fingerprints (active or passive) to let you know the geometry of the LAN.

8: [Ngrep](#)

ngrep strives to provide most of GNU grep’s common features, applying them to the network layer. ngrep is a pcap-aware tool that will allow you to specify extended regular or hexadecimal expressions to match against data payloads of packets. It currently recognizes TCP, UDP and ICMP across Ethernet, PPP, SLIP, FDDI, Token Ring and null interfaces, and understands bpf filter logic in the same fashion as more common packet sniffing tools, such as tcpdump and snoop.

9: [Ntop](#)

Ntop shows network usage in a way similar to what top does for processes. In interactive mode, it displays the network status on the user’s terminal. In Web mode, it acts as a Web server, creating an HTML dump of the network status. It sports a NetFlow/sFlow emitter/collector, an HTTP-based client interface for creating ntop-centric monitoring applications, and RRD for persistently storing traffic statistics.

10: [EtherApe](#)

EtherApe is a graphical network monitor for Unix modeled after etherman. Featuring link layer, IP and TCP modes, EtherApe displays network activity graphically with a color coded protocols display. Hosts and links change in size with traffic. It supports Ethernet, FDDI, Token Ring, ISDN, PPP and SLIP devices. It can filter traffic to be shown, and can read traffic from a file as well as live from the network.

Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology

Wireshark:

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.

You could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course).

Some intended purposes

Here are some examples people use Wireshark for:

- Network administrators use it to *troubleshoot network problems*
- Network security engineers use it to *examine security problems*
- Developers use it to *debug protocol implementations*
- People use it to *learn network protocol* internals

Beside these examples Wireshark can be helpful in many other situations too.

Features

The following are some of the many features Wireshark provides:

- Available for *UNIX* and *Windows*.
- *Capture* live packet data from a network interface.
- *Open* files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.
- *Import* packets from text files containing hex dumps of packet data.
- Display packets with *very detailed protocol information*.
- *Save* packet data captured.
- *Export* some or all packets in a number of capture file formats.
- *Filter packets* on many criteria.
- *Search* for packets on many criteria.
- *Colorize* packet display based on filters.
- Create various *statistics*.
- **...and a lot more!.**

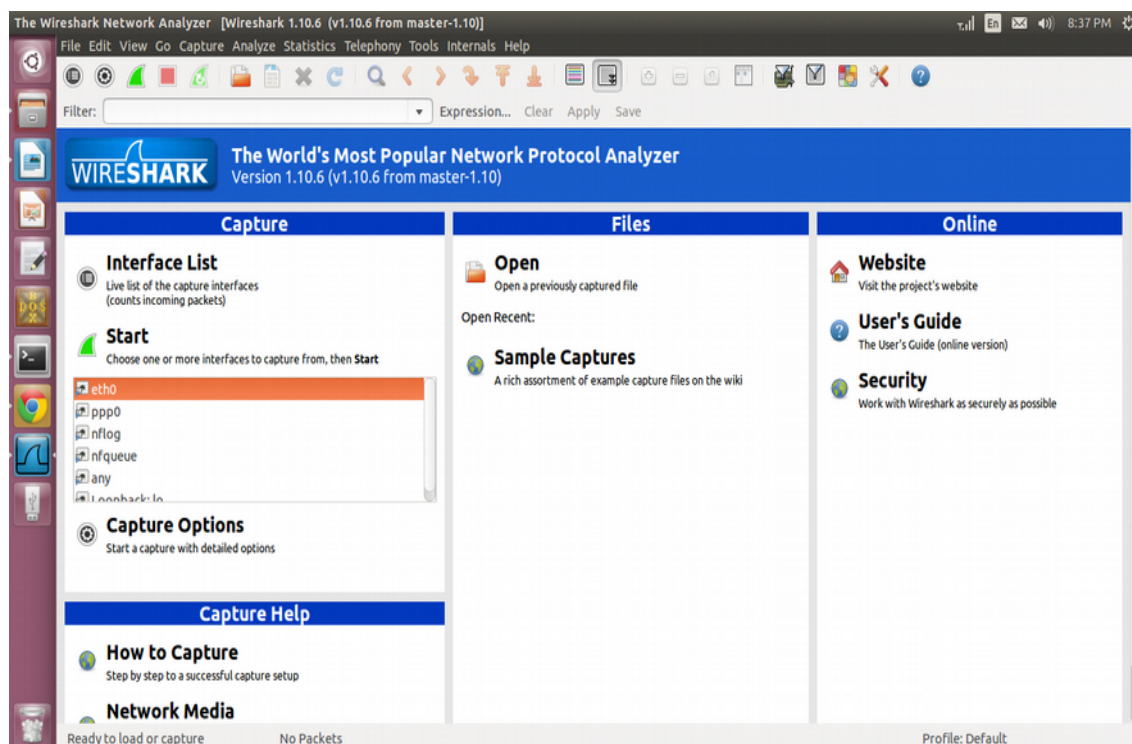
Procedure :

Start Wireshark.

On a Linux or Unix environment, select the Wireshark or Ethereal entry in the desktop environment's menu, or run "wireshark" (or "ethereal") from a root shell in a terminal emulator. Then Configure Wireshark

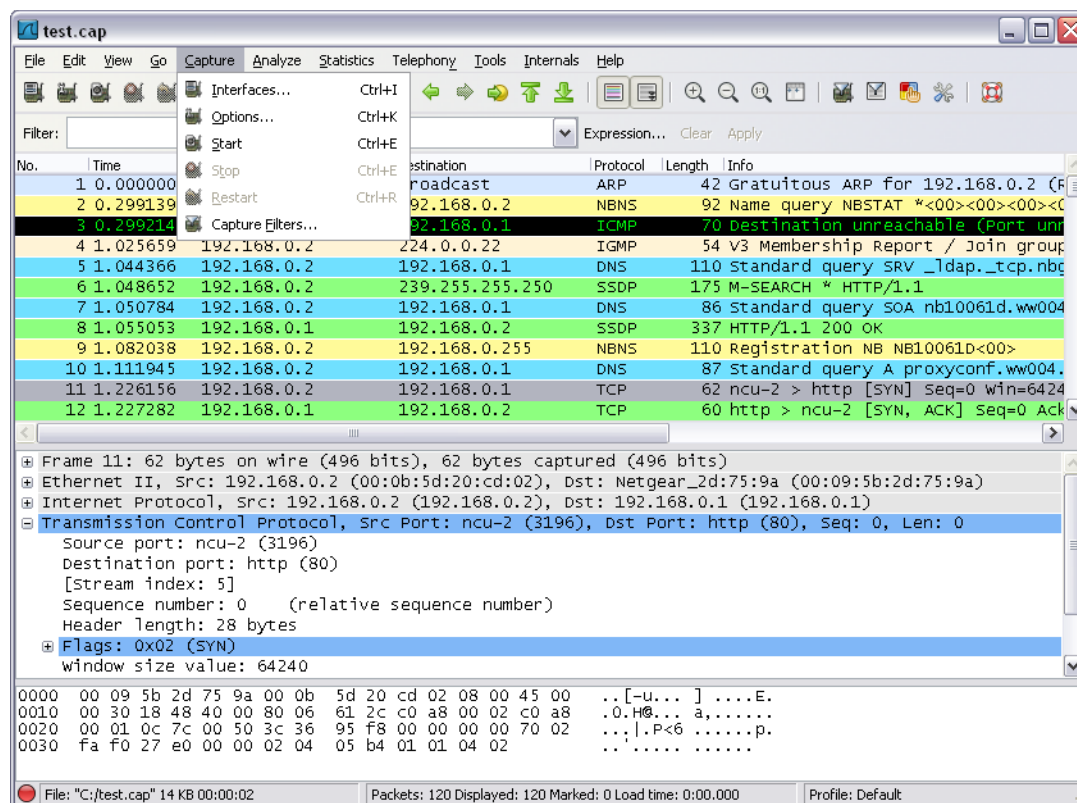
Don Bosco Institute of Technology, Mumbai 400070

Department of Information Technology



After starting Wireshark, do the following:

1. Select Capture | Interfaces



2. Select the interface on which packets need to be captured.
3. If capture options need to be configured, click the Options button for the chosen interface.

Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology

Note the following recommendations for traces that are to be analysed by Novell Technical Services:

- Capture packet in promiscuous mode: This option allows the adapter to capture all traffic not just traffic destined for this workstation. It should be enabled.
 - Limit each packet to: Leave this option unset. Novell Support will always want to see full frames.
 - Filters: Generally, Novell Support prefers an unfiltered trace. For documentation on filters, please refer to TID 10084702 - How to configure a capture filter for Ethereal (formerly NOVL90720).
 - Capture file(s): This allows a file to be specified to be used for the packet capture. By default Wireshark will use temporary files and memory to capture traffic. Specify a file for reliability.
 - Use multiple files, Ring buffer with: These options should be used when Wireshark needs to be left running capturing data for a long period of time. The number of files is configurable. When a file fills up, it will wrap to the next file. The file name should be specified if the ring buffer is to be used.
 - Stop capture after xxx packet(s) captured: Novell Technical Support would most likely never use this option. Leave disabled.
 - Stop capture after xxx kilobyte(s) captured: Novell Technical Support would most likely never use this option. Leave disabled.
 - Stop capture after xxx second(s): Novell Technical Support would most likely never use this option. Leave disabled.
 - Update list of packets in real time: Disable this option if the problem that's being investigated is occurring on the same workstation as where Wireshark is running.
 - Automatic scrolling in live capture: Wireshark will scroll the window so that the most current packet is displayed.
 - Hide capture info dialog: Disable this option so that you can view the count of packets being captured for each protocol.
 - Enable MAC name resolution: Wireshark contains a table to resolve MAC addresses to vendors. Leave enabled.
 - Enable network name resolution: Wireshark will issue DNS queries to resolve IP host names. Also will attempt to resolve network network names for other protocols. Leave disabled.
 - Enable transport name resolution: Wireshark will attempt to resolve transport names. Leave disabled.
4. Now click the Start button to start the capture.
 5. Recreate the problem. The capture dialog should show the number of packets increasing. If not, then stop the capture. Examine the interface list and pick the one that is not associated with the WANIP. It will probably be a long alpha-numeric string. If packets are still not being captured, try removing any filters that have been defined.
 6. Once the problem which is to be analyzed has been reproduced, click on Stop. It might take a few seconds for Wireshark to display the packets captured.

Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology

The image shows a Wireshark packet capture window titled 'test.cap'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help), a toolbar, and a filter field. The main display area shows a list of 12 captured packets. Packet 11 is selected, showing its details: Ethernet II, Internet Protocol, and Transmission Control Protocol. The packet data is displayed in hexadecimal and ASCII at the bottom.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	Broadcast	ARP	42	Gratuitous ARP for 192.168.0.2 (F
2	0.299139	192.168.0.1	192.168.0.2	NBNS	92	Name query NBSTAT *(<00><00><00><00>
3	0.299214	192.168.0.2	192.168.0.1	ICMP	70	Destination unreachable (Port un
4	1.025659	192.168.0.2	224.0.0.22	IGMP	54	v3 Membership Report / Join group
5	1.044366	192.168.0.2	192.168.0.1	DNS	110	Standard query SRV _ldap._tcp.nbg
6	1.048652	192.168.0.2	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
7	1.050784	192.168.0.2	192.168.0.1	DNS	86	Standard query SOA nb10061d.wv004
8	1.055053	192.168.0.1	192.168.0.2	SSDP	337	HTTP/1.1 200 OK
9	1.082038	192.168.0.2	192.168.0.255	NBNS	110	Registration NB NB10061D<00>
10	1.111945	192.168.0.2	192.168.0.1	DNS	87	Standard query A proxyconf.wv004.
11	1.226156	192.168.0.2	192.168.0.1	TCP	62	ncu-2 > http [SYN] Seq=0 Win=6424
12	1.227282	192.168.0.1	192.168.0.2	TCP	60	http > ncu-2 [SYN, ACK] Seq=0 Ack

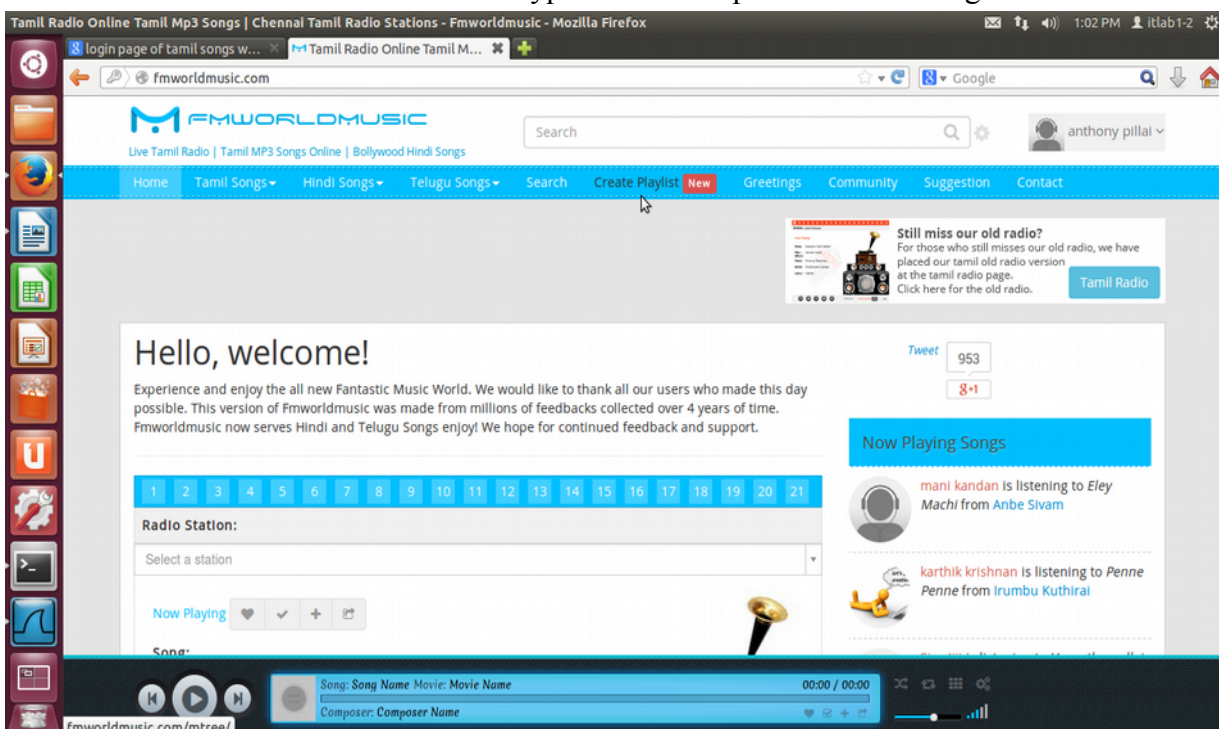
Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0
Source port: ncu-2 (3196)
Destination port: http (80)
[Stream index: 5]
Sequence number: 0 (relative sequence number)
Header length: 28 bytes
Flags: 0x02 (SYN)
window size value: 64240

0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00 ..[-u...]E.
0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 ..0.H8... a.....
0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02 ...|.P<6p.
0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02

File: "C:/test.cap" 14 KB 00:00:02 Packets: 120 Displayed: 120 Marked: 0 Load time: 0:00:00 Profile: Default

Results :

Packet sniffing/snooping was studied and understood. Wireshark tool for sniffing was used. It was studied how to capture specific packets from network traffic, get information about the packets like the protocol used, etc. It was also analysed to find out if websites have secure encryption for their login page, i.e., username and password. It was discovered that oosai .com and fmworldmusic.com were two of the sites that do not use encryption for their password while login.



Don Bosco Institute of Technology, Mumbai 400070

Department of Information Technology

eth0 [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
182	1.616300	10.0.1.22	10.0.1.2	TCP	74	53831 > 8090 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1350983 TSecr=0
183	1.616399	10.0.1.2	10.0.1.22	TCP	60	8090 > 53831 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
184	1.616417	10.0.1.22	10.0.1.2	TCP	54	53831 > 8090 [ACK] Seq=1 Ack=1 Win=29200 Len=0
185	1.616489	10.0.1.22	10.0.1.2	TCP	693	53831 > 8090 [PSH, ACK] Seq=1 Ack=1 Win=29200 Len=639
186	1.616643	10.0.1.2	10.0.1.22	TCP	60	8090 > 53831 [ACK] Seq=1 Ack=640 Win=5840 Len=0
347	2.751262	10.0.1.2	10.0.1.22	TCP	589	8090 > 53831 [PSH, ACK] Seq=1 Ack=640 Win=5840 Len=535
348	2.751284	10.0.1.22	10.0.1.2	TCP	54	53831 > 8090 [ACK] Seq=640 Ack=536 Win=30016 Len=0
349	2.751288	10.0.1.2	10.0.1.22	TCP	270	8090 > 53831 [PSH, ACK] Seq=536 Ack=640 Win=5840 Len=216
350	2.751292	10.0.1.22	10.0.1.2	TCP	54	53831 > 8090 [ACK] Seq=640 Ack=752 Win=31088 Len=0
351	2.751295	10.0.1.2	10.0.1.22	TCP	60	8090 > 53831 [FIN, ACK] Seq=752 Ack=640 Win=5840 Len=0
352	2.751528	10.0.1.22	10.0.1.2	TCP	54	53831 > 8090 [FIN, ACK] Seq=640 Ack=753 Win=31088 Len=0
353	2.751615	10.0.1.2	10.0.1.22	TCP	60	8090 > 53831 [ACK] Seq=753 Ack=641 Win=5840 Len=0

Frame 185: 693 bytes on wire (5544 bits), 693 bytes captured (5544 bits)

Ethernet II, Src: d4:3d:7e:38:c4:a9 (d4:3d:7e:38:c4:a9), Dst: SpeedDra_0e:01:0b (00:13:b3:0e:01:0b)

01b0 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 66 6d 77 error: ht tp://fmw
01c0 6f 72 6c 64 6d 75 73 69 63 2e 63 6f 6d 2f 0d 0a orldmusi c.com/..
01d0 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 Content- Length:
01e0 39 34 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48 50 53 94..Cook ie: PHPS
01f0 45 53 53 49 44 3d 37 6d 72 65 35 63 34 6b 37 6b ESSID=7m re5c4k7k
0200 6e 35 62 39 67 36 75 30 31 63 67 70 39 75 71 36 n5b96u0 1cgp9uq6
0210 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 ..Connection: ke
0220 65 70 2d 61 6c 69 76 65 0d 0a 50 72 61 67 6d 61 ep-alive ..Pragma
0230 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 43 61 63 68 : no-cac he..Cach
0240 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6e 6f 2d 63 61 e-Contro l: no-ca
0250 63 68 65 0d 0a 0d 0a 75 73 65 72 6e 61 6d 65 3d che....u sername=
0260 6a 61 63 71 75 65 6c 69 6e 65 61 6e 74 68 6f 6e jacqueli neantho
0270 79 31 39 39 32 25 34 30 79 61 68 6f 6f 2e 63 6f y1992940 yahoo.co
0280 2e 69 6e 26 70 61 73 73 3d 61 62 63 31 32 33 26 .in&pass =abc123&
0290 61 63 74 69 76 69 74 79 3d 6c 6f 67 69 6e 26 4c activity =login&L
02a0 6f 67 69 6e 3d 4c 6f 67 69 6e 26 72 65 6d 65 6d ogin=Log in&remem
02b0 62 65 72 3d 30 ber=0

File: /tmp/wireshark_eth0_20150... Packets: 592 Displayed: 12 Marked: 0 Dropped: 0 Profile: Default

My Oosai - Oosai.com - A Sound of Tamil Music - Google Chrome

Course: System And v... My Oosai - Oosai.com Google Accounts

www.oosai.com/my_oosai.cfm

oosai.com
A Sound of Tamil Music

HOME SEARCH REGISTER MY OOSAI FEEDBACK

Hi Jacqueline | My Playlist | Signout Free Software Downloads Real One Player

Microsoft
with wide angle, integrated Skype.

OOSAI PANEL

- Tamil Movies
- Tamil Devotional Albums
- Tamil Pop Albums
- Golden Releases
- New Releases
- Actors
- Actresses
- Music Directors
- Singers
- Top Ten Songs
- Last Updates
- Tamil Chat Rooms
- Tamil Music Feeds

SONG OF THE DAY

Song : Muthuna Munjikk
Movie : E

Send Tamil Greetings with
123 Greetings
FREE GREETINGS FOR THE PLANET

My Playlist My Profile Chat Rooms

- My Oosai Play List - Create your own Playlist
- My Profile - Edit your profile, Change Password
- Chat Rooms - Chat while you listen to songs

LAST UPDATES

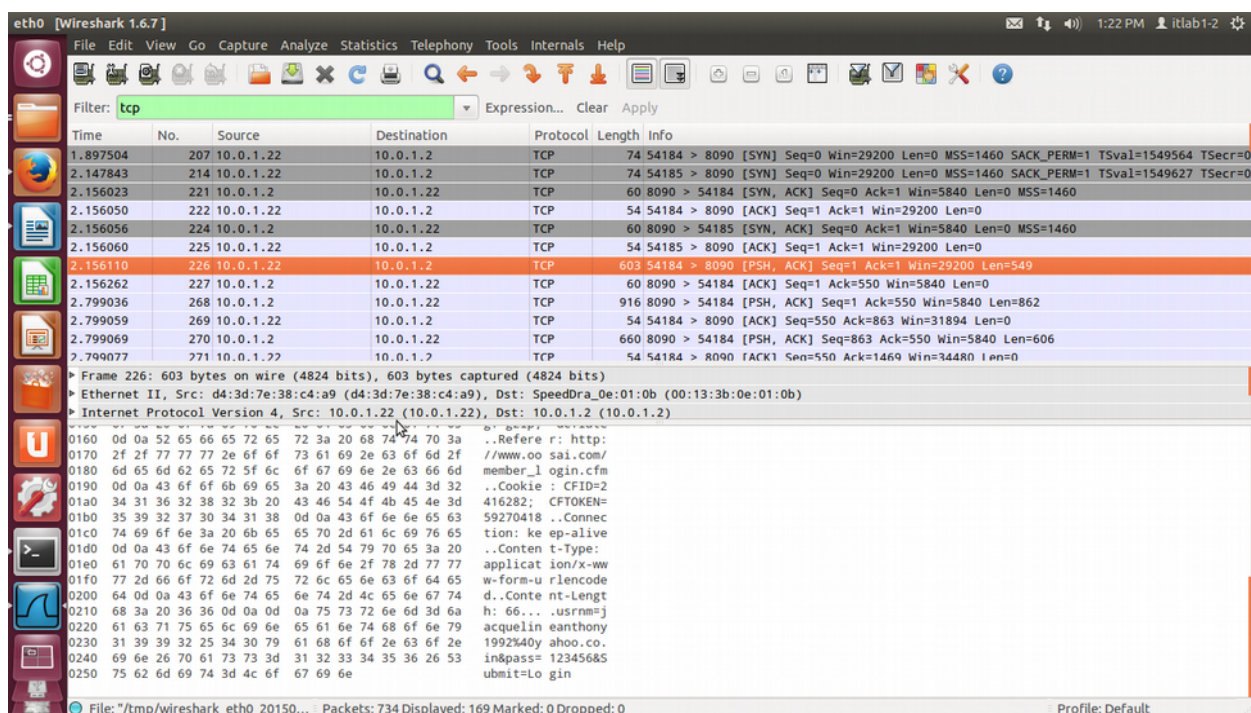
- Africavil Appu Songs
Music : Ilayaraja
- Aruvadai Naal Songs
Music : Ilayaraja
- Chinna Veedu Songs
Music : Ilayaraja
- Dharma Pathini Songs
Music : Ilayaraja
- Vedikundu Murugesan Songs
Music : Dhena
- Eesaa Songs
Music : Haran
- Ilampoyal Songs
Music : Vashanth
- Sarvam Songs
Music : Yuvan Shankar Raja
- Ide Siva Naamam [Devotional] Songs
Music : Oosai
- Nallaiyampathi Paamalaikal [Devotional] Songs
Music : V.S.Udaya

Oosai.com - Online
oosai.co Tamil Songs Portal
Like

1,633 people like Oosai.com - Online
Tamil Songs Portal.

Don Bosco Institute of Technology, Mumbai 400070

Department of Information Technology



References :

- <http://www.linuxjournal.com/content/packet-sniffing-basics>
- <http://www.internetgeeks.org/tech/hacking/top-10-data-packet-sniffing-analyzer-tools-hackers/>
- <https://www.novell.com/support/kb/doc.php?id=3892415>
- https://www.wireshark.org/docs/wsug_html/
- <http://www.oosai.com/default.cfm?act=signout>
- <http://fmworldmusic.com/>

Lab practice (optional) :

Questions (Short, Long, MCQs) (optional) :

- S1. What is Packet sniffing.
- S2. Differentiate promiscuous and non-promiscuous mode.