**Branch :- Computer Sci. & Engg. Class :- Final Year**

**Subject :-System and Software Security Lab manual Sem :- VII**

**Teacher Manual**

**PRACTICAL NO 04**

**Practical no. 2**

**Aim :-** Evaluate wireshark sniffer to capture network traffic.

**Software Required:-** Wireshark

**THEORY:-**

**Wireshark:**

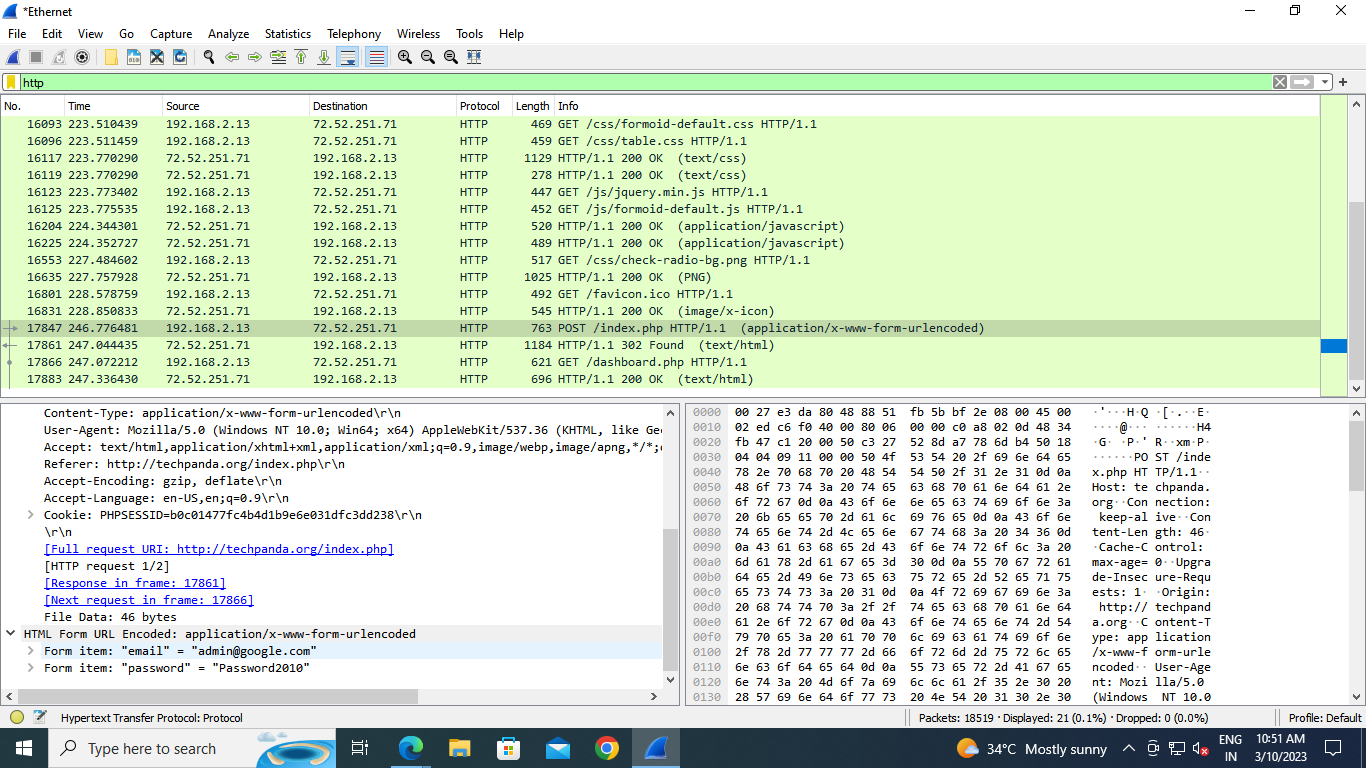
Wireshark is a [free and open-source](https://en.wikipedia.org/wiki/Free_and_open-source_software) [packet analyzer](https://en.wikipedia.org/wiki/Packet_analyzer). It is used for [network](https://en.wikipedia.org/wiki/Computer_network) troubleshooting, analysis, software and [communications protocol](https://en.wikipedia.org/wiki/Communications_protocol) development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.[[5]](https://en.wikipedia.org/wiki/Wireshark#cite_note-5)

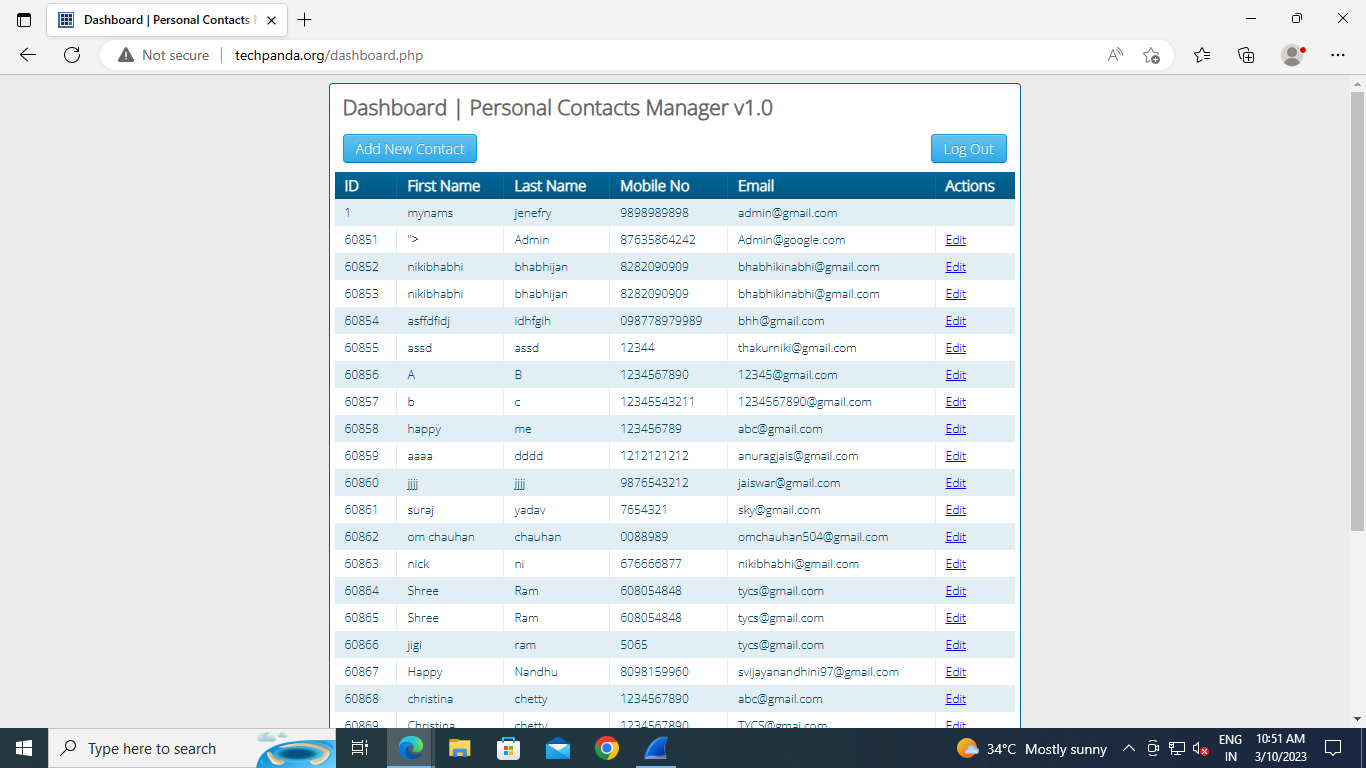
Wireshark is [cross-platform](https://en.wikipedia.org/wiki/Cross-platform), using the [Qt](https://en.wikipedia.org/wiki/Qt_(software)) [widget toolkit](https://en.wikipedia.org/wiki/Widget_toolkit) in current releases to implement its user interface, and using [pcap](https://en.wikipedia.org/wiki/Pcap) to capture packets; it runs on [Linux](https://en.wikipedia.org/wiki/Linux), [macOS](https://en.wikipedia.org/wiki/MacOS), [BSD](https://en.wikipedia.org/wiki/BSD), [Solaris](https://en.wikipedia.org/wiki/Solaris_(operating_system)), some other [Unix-like](https://en.wikipedia.org/wiki/Unix-like) operating systems, and [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows). There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are [free software](https://en.wikipedia.org/wiki/Free_software), released under the terms of the [GNU General Public License](https://en.wikipedia.org/wiki/GNU_General_Public_License) version 2 or any later version.

Steps :

1. Download wireshark from the given link : [https://www.wireshark.org/download.html](https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqa3A2RzNGb09Ed2FvUEVia0pSQlFraWdFWVdhd3xBQ3Jtc0trMUh6M3NPenNvOFVqbWRUcjFHZ1ZKTWFYb1p1aXBFMmRwMXhBOVpwTHBEYnI0X3VrRndfQjhyUWZucERvMUJVb0QtVGFfVWJ2ajdrZXRDSkxKZWVfN1NzN0ZtenQ2bTdfVWVQZ0RjbHowRjF5Q1pMYw&q=https://www.wireshark.org/download.html&v=6VNSzcMfyxs)
2. Install and open Wireshark.
3. Go to capture and select Interface option.
4. In capture Interface, Select local area connection/Ethernet and click on start.
5. The source destination and protocols of the packets in the LAN network will be displayed.
6. Open a website "[http://www.techpanda.org/index.php](https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqbm9zU0VKbER5NVlnUXRVbV9uNGdkakdpajdPUXxBQ3Jtc0tseEw5UWxLY2NiXzRiV2Z1SUFjNzcydEE4NmFIdURvRTBjamFyaUxqSkxIMFVNYnlXUDVaQ2drYnkweXdoN1lMdGFLcUo1R0VjRHpsSXBaQ09fUnZGaEt4N1duMDIyNkltUnFodjNseDZ2aDBXazduZw&q=http://www.techpanda.org/index.php&v=6VNSzcMfyxs)" in a new window and enter the username and password. The login address is admin@google.com, and the password is Password2010 and submit.
7. Now stop the tool and to stop recording.
8. Select the filter as http to make the search easier and apply.
9. Search for the POST method under "Info" column where you will get your entered credentials.

**Screenshots:-**





**CONCLUSION:-** Thus, we have evaluated wireshark sniffer to capture network traffic.