Wireshark Introduction

Presenter: Devarshi R Patel

Project Slide

WIRESHARK

If used wisely then help if not then hinderance

Section 1 About Wireshark

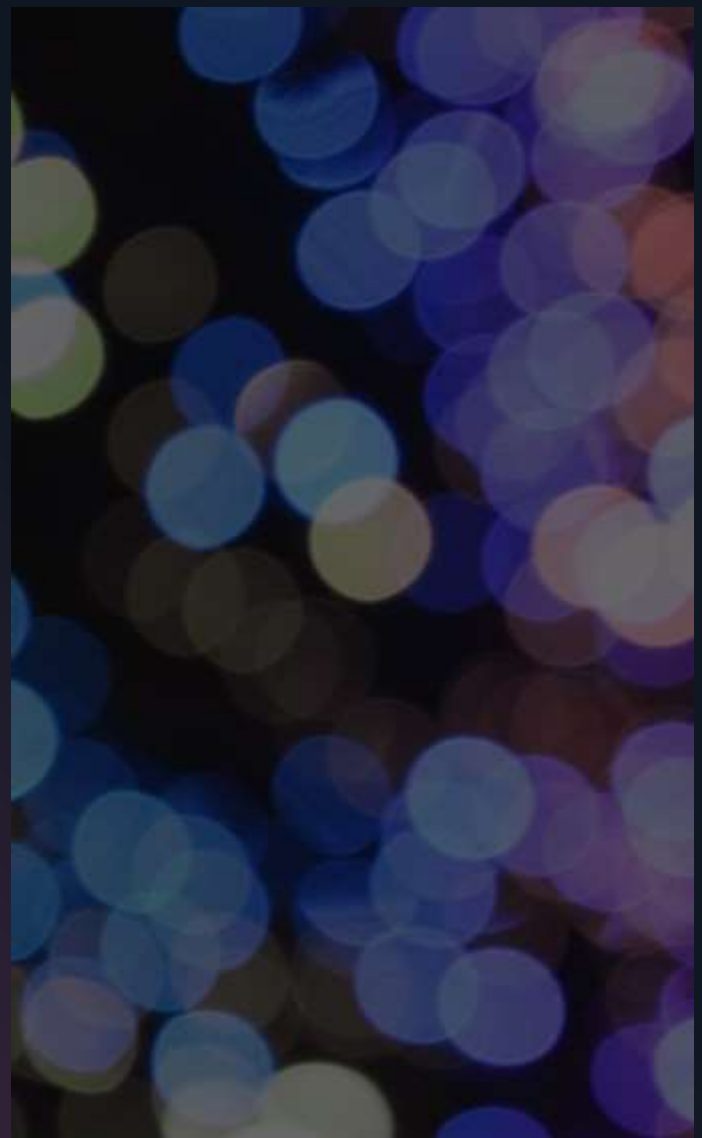
Section 2 Recent Features

Section 3 History

Section 4 Introduction of Wireshark

About Wireshark

Originally named Ethereal, Wireshark is a free and open-source packet analyzer.



Recent Features

Wireshark is cross-platform application

- QT Widget
- TShark.

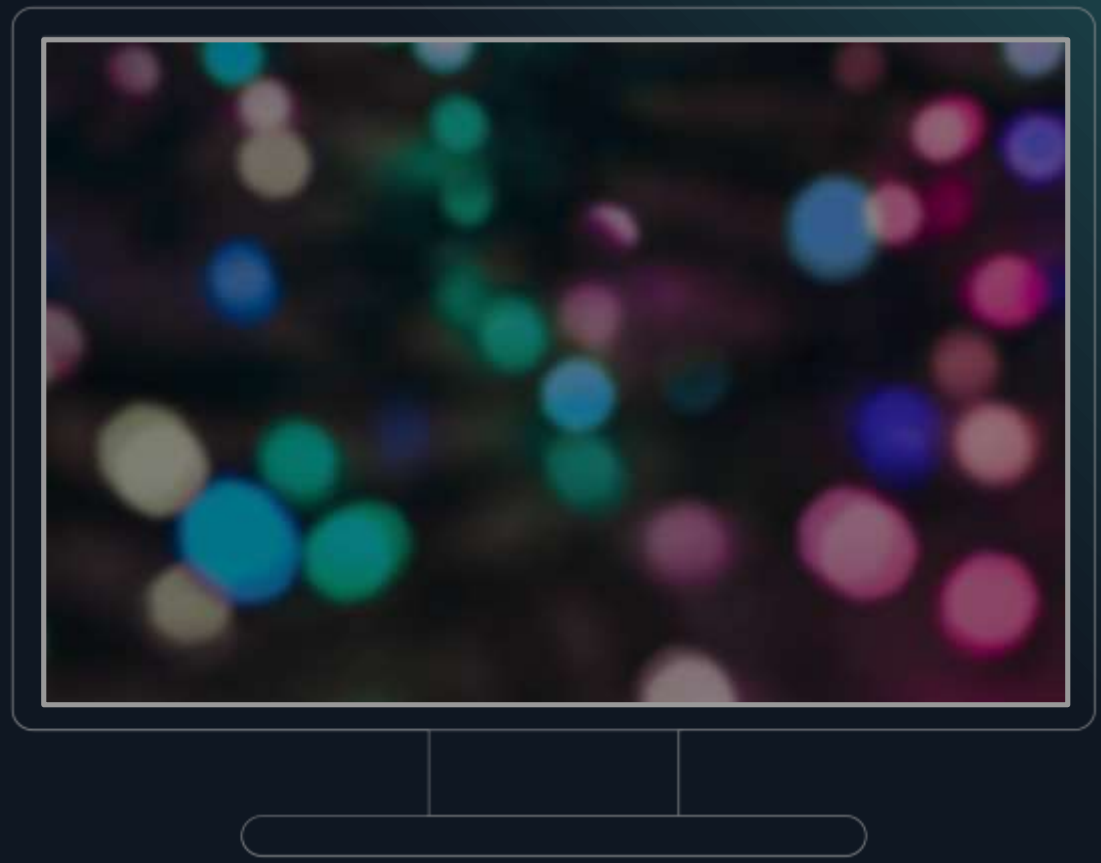
History

- Initially released in 1998.
- Written in C, C++ and Lua.

Wireshark

Introduction of Wireshark's GUI and its basic working/functioning

- For Kali Linux, Wireshark is pre-installed.
- For Windows and Mac-OS visit https://www.wireshark.org and download the respective installer or disk image and complete the installation.



Basic Working and Functions

Wireshark is a packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

1

Step 1

We'll be looking at the GUI and we'll discuss about the different functions present on the GUI.

2

Step 2

We'll open a test target for the purpose of TCP/IP pcap(packet capturing) and we'll look at it's response.

3

Step 3

We'll do the testing on the test target and we'll do the data analysis.

GUI

A Deep Dive Into The GUI Of WireShark

GUI & Its Different Functions

Menu Bar

Tool Bar

Filter Bar

Capture Filter & List

Learn

Version & Status Bar

Test Target

Packet Sniffing

1

Step 1

Get into the Network

2

Step 2

Run the Application

3

Step 3

Do the Analysis

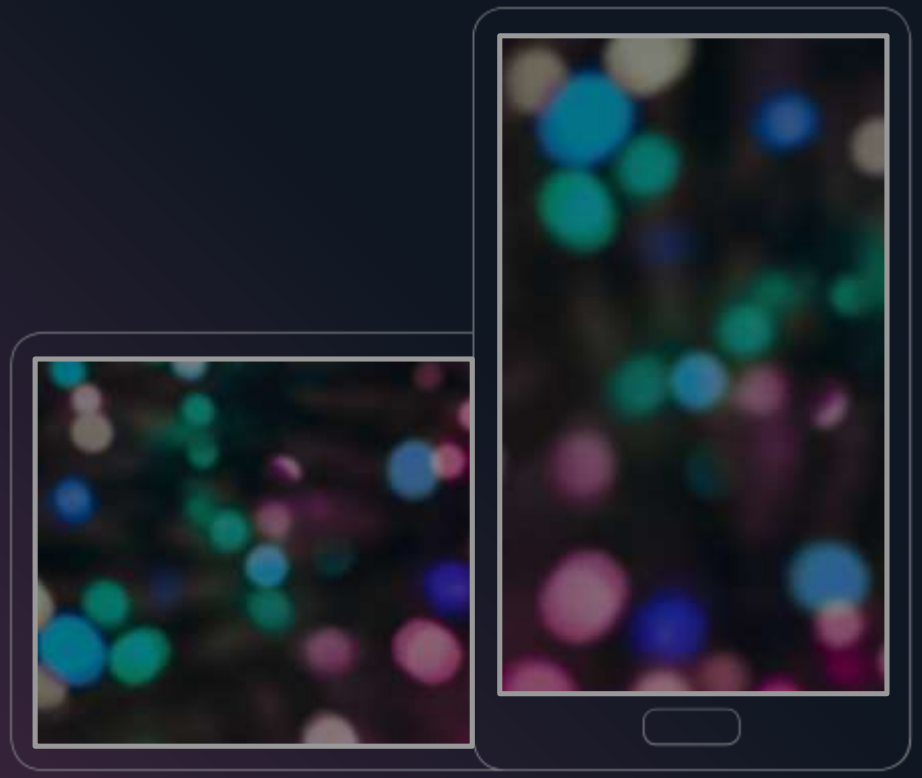
SUMMARY

Originally named Ethereal, Wireshark is a free and open-source packet analyzer.

- It is used for network troubleshooting, analysis, software and communications protocol development, and education.
- It is a very versatile tool to monitor and analyze data packets.
- It works by monitoring the network traffic that is captured and has various protocols available to work with.

CASE STUDY

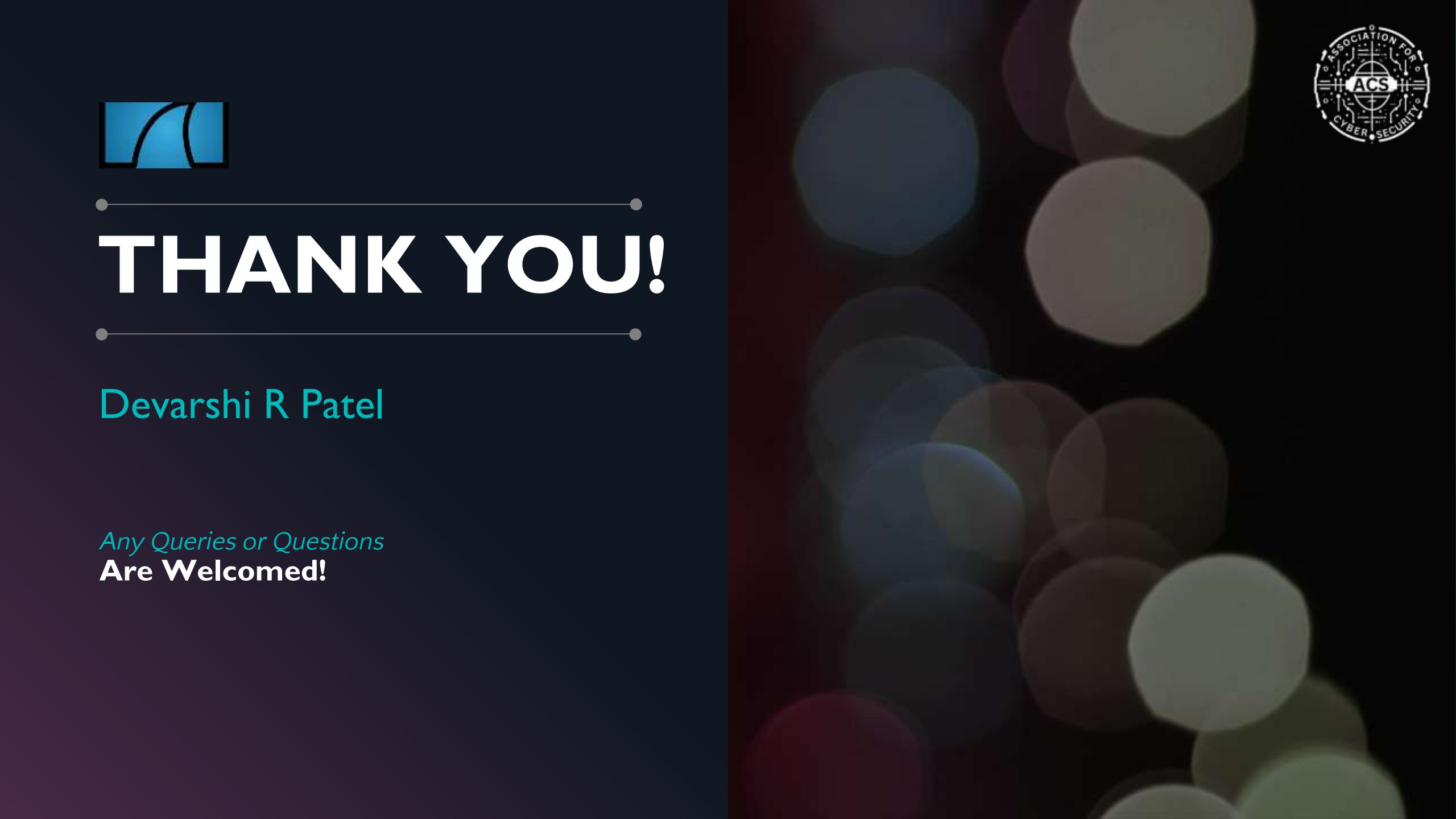
Top 10 use cases of Wireshark and a few functions



MOBILE VERSION

Wireshark is the most popular, free, and open-source packet analyzer, but is not available for Android. But there are some alternatives for Android smartphones.

- zAnti
- cSploit
- Packet Capture
- Debug Proxy
- Wifinspect
- tPacketCapture



THANK YOU!

Devarshi R Patel

Any Queries or Questions
Are Welcomed!