

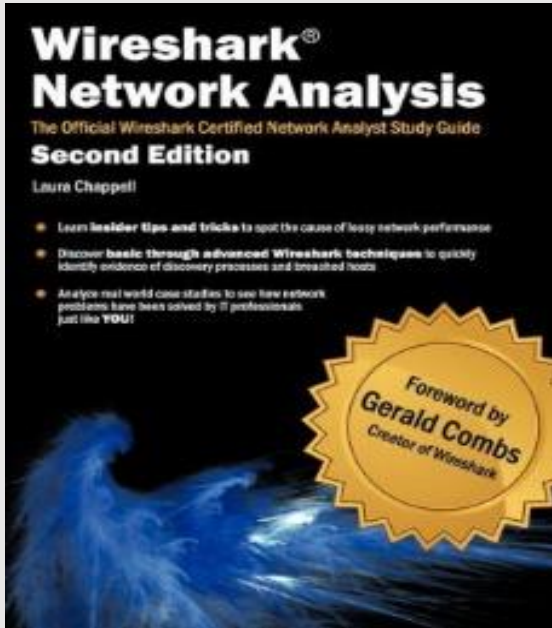
# Wireshark



# Topics of Discussion

- Network Analysis
  - Network Analyzer
  - Network Analyzer Components
  - Who Uses Network Analyzers
  - Introduction to Wireshark
  - Features of Wireshark
  - Applications of Wireshark
  - Display Filtering
  - Capture Filtering
  - Packet Colorization
  - Demo (Wireshark GUI)
  - Wireshark Command Line
  - Demo (Wireshark Command Line)
-

# Recommended Reading



- Wireshark Network Analysis (Second Edition)
- Author: Laura Chappell
- “Wireshark is a FIRST RESPONDER tool”
- Who is always there to listen to you with a patient and understanding silence when you are crying in your latte because the user keep complaining about network performance?

Wireshark!

# Network Analysis

- Process of capturing, decoding, and analyzing network traffic.
  - Why is the network slow?
  - What is the network traffic pattern?
  - How is the traffic being shared between nodes?

*“Network analysis is a key skill that every IT professional should possess and Wireshark is the world’s most popular network analyzer tool.”*

*Laura Chappell*

Also called:

- traffic analysis
- packet analysis
- eavesdropping
- protocol analysis
- sniffing

# Network Analyzer

A combination of hardware and software tools which can detect, decode, and manipulate traffic on the network.

- Passive monitoring (detection) - Difficult to detect
- Active (attack)

Mainly software-based (utilizing OS and NIC).

- Also known as sniffer
- A program that monitors the data traveling through the network passively.

Common network analyzers are Wireshark | Ethereal | Windump | Etherpeak | Dsniff

# Network Analyzer Components

Components includes:

## Hardware

Special hardware devices

- Monitoring voltage fluctuation
- Jitter (**variation** in the **delay** of **received packets**)
- Jabber (**failure** to **handle electrical signals**)
- CRC and Parity Errors

NIC Card

Capture driver

- capturing the data

# Network Analyzer Components

## Buffer

- memory or disk-based.

## Real-time analysis

- **analyzing** the traffic in **real time**; detecting any intrusions.

## Decoder

- making data **readable**.

# Who Uses Network Analyzers

## System administrators

- Understand system problems and performance.

## Malicious individuals (Threat Actors)

- Capture clear text data.
- Passively collect data on vulnerable protocols.
  - FTP, POP3, IMAP, SMTP, rlogin, HTTP, etc.
  - Capture VoIP data.
- Traffic pattern discovery.
- Actively break into the network (backdoor techniques).

## Network Engineers

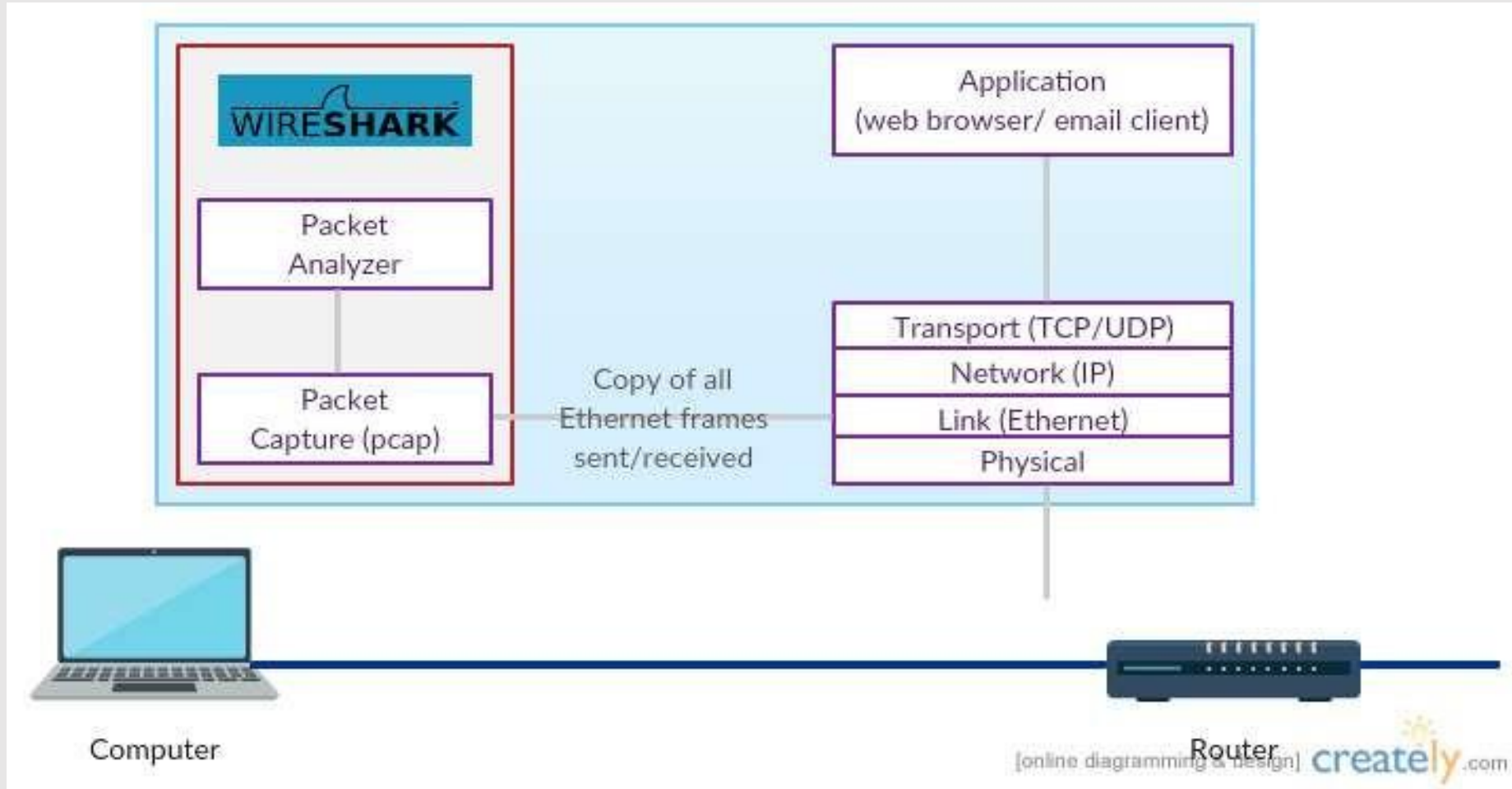
- Network Troubleshooting
- Network Auditing and Forensics



# Introduction to Wireshark

- It is a **packet sniffer** Computer application (open source program).
- Initiated by **Gerald Combs** under the name **Ethereal**.
- First version was released in 1998.
- The name Wireshark was adopted in June 2006.
- Has a GUI front-end and many more information sorting and filtering options.
- “eWeek” Labs named Wireshark one of "The Most Important Open-Source Apps of All Time" as of May 2, 2007.
- Supports command-line(**tshark**) and GUI interfaces.

# How Wireshark works?



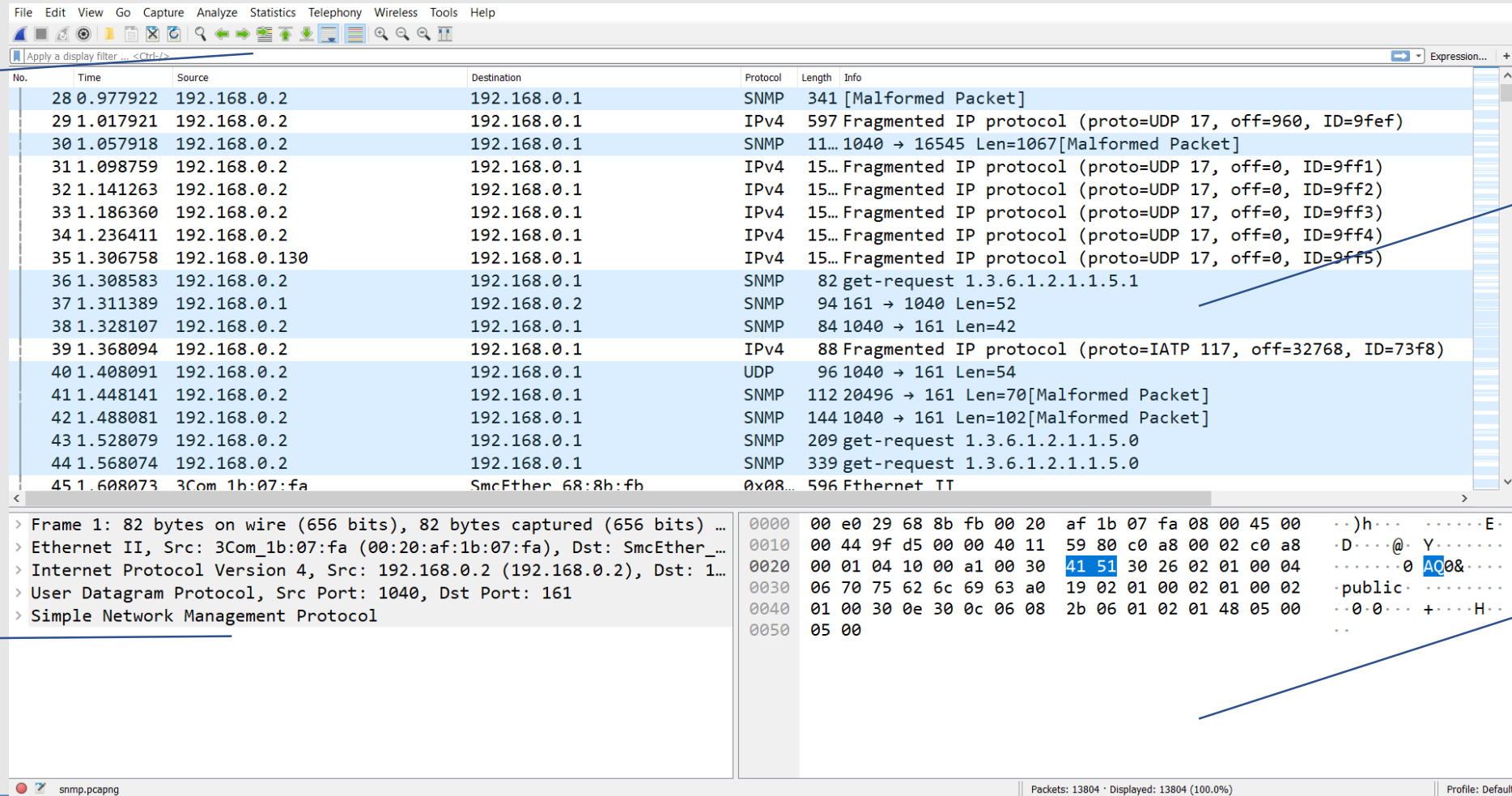
# Wireshark User Interface

Filter  
Toolbar

Packet  
List

Packet  
Byte Pane

Selected  
Packet  
Details



The screenshot displays the Wireshark User Interface with the following components:

- Filter Toolbar:** Located at the top left, it includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with icons for various functions. Below the toolbar is a display filter input field containing "Apply a display filter ... <Ctrl-F>".
- Packet List:** A table showing a list of captured packets. The columns are No., Time, Source, Destination, Protocol, Length, and Info. The list includes packets from 192.168.0.2 to 192.168.0.1, including SNMP and IPv4 fragments.
- Selected Packet Details:** A pane on the left showing the details of the selected packet (No. 41). It lists the frame structure: Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) ... Ethernet II, Src: 3Com\_1b:07:fa (00:20:af:1b:07:fa), Dst: SmcEther\_... Internet Protocol Version 4, Src: 192.168.0.2 (192.168.0.2), Dst: 1... User Datagram Protocol, Src Port: 1040, Dst Port: 161 Simple Network Management Protocol.
- Packet Byte Pane:** A pane on the right showing the raw bytes of the selected packet. It displays hexadecimal and ASCII representations of the data, with the selected packet (No. 41) highlighted in blue.

At the bottom of the interface, there is a status bar showing "snmp.pcapng", "Packets: 13804 · Displayed: 13804 (100.0%)", and "Profile: Default".

# Features of Wireshark

- It is **cross-platform** and understands the structure of different network protocols.
  - **Capture live packet data** from a network interface.
  - Open files containing packet data captured with other packet capture programs (tcpdump/WinDump/Network General Sniffer®).
  - Save packet data captured.
  - Display packets with very detailed protocol information.
  - **Export** some or all **packets** in a number of capture file formats.
  - **Filter packets** on many criteria.
  - Search for packets on many criteria.
  - Create various statistics.
-

# Application of Wireshark

- 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.
- Exposing VOIP problems.
- Supports Malware Detection.
- Helps recognize DOS attack.
- Wireshark isn't an intrusion detection system.
- Wireshark will not manipulate things on the network, it will only "measure" things from it.

# Display Filtering

- Arranging the display sort field in the Packet list it will order base on that specific field:
  - Sort order of **time/packet number**
  - Sort order per **IP/MAC address** of **source/destination**
  - Sort order per **protocol**
- Marking specific packets manually filters on Wireshark
- Configuring filters for:
  - Address
  - Protocol
  - Frame length
  - String

# Display Filtering

Some of the basic filter field examples:

ip.src → Source IP address

ip.dst → Destination IP address

Ip.addr → IP address (source or destination)

Eth.dst → Destination MAC address

UDP, TCP, SIP, HTTP, H225, H245

H263.dbq, sip.method, h323.fastStart, rtp.payload, and more

# Display Filtering

## Filter Comparison operators

- English operators

Equal ( <b>eq</b> )	Not equal ( <b>ne</b> )	Greater than ( <b>gt</b> )
Less than ( <b>lt</b> )	Greater than or equal ( <b>ge</b> )	Less than or equal ( <b>le</b> )

- C-like operators

Equal ( <b>==</b> )	Not equal ( <b>!=</b> )	Greater than ( <b>&gt;</b> )
Less than ( <b>&lt;</b> )	Greater than or equal ( <b>&gt;=</b> )	Less than or equal ( <b>&lt;=</b> )



# Display Filtering

## Some Filter Examples:

- `ip.addr == 234.78.12.78`
- `ip.src != 10.0.0.2`
- `sip.Method == REGISTER`
- `h263.unrestricted_motion_vector == 0`
- `sip.from.addr == "sip:39260722@10.7.0.4"`
- `h245.masterSlaveDetermination`

# Display Filtering

## Logical Operators

and	&&	Logical and
or		Logical or
xor	^^	Logical XOR
not	!	Logical Not
[...]		Substring operator

# Capture Filtering

- When capturing, packets are stored in temporary files on the computer.
- We can configure Wireshark to capture packets directly to a single or multiple files.
- For heavy traffic network capturing or long time capturing the file/buffer sizes might overwhelm the computer or might even crash it.
- To prevent accumulating huge file/files, if we know what we are looking for we should apply capture filtering. This is where tcpdump is a better use case.

# Capture Filtering

## Capture Filter syntax Examples:

- host 192.168.122.23
  - Capture packets from/to IP address 192.168.122.23
- src host 10.0.0.5
  - Capture packets from IP 10.0.0.5
- tcp port 23 and host 10.0.0.5
- ether src 00:11:6b:80:47:96
- tcp port 23 and not src host 10.0.0.5

# Packet Colorization

- A very useful mechanism available in Wireshark is packet colorization.
- You can set up Wireshark so that it will colorize packets according to a display filter.
- This allows you to emphasize the packets you might be interested in.
- There are two types of coloring rules in Wireshark:
  - temporary rules that are only in effect until you quit the program.
  - permanent rules that are saved in a preference file so that they are available the next time you run Wireshark.

# Coloring Rules-Default

[illegible]

# Demo

## (Wireshark GUI)

# TShark

## Wireshark Command Line



# TShark

- You can start Wireshark from the **command line/terminal**.
- **TShark** is a terminal oriented version of Wireshark designed for capturing and displaying packets.
- Use when an interactive user interface isn't necessary or available.
- It **supports the same options as Wireshark**.

# TShark

- **tshark -D**  
List available capture interfaces.
- **tshark -i**  
Capture all the interfaces.
- **tshark -i <interface\_name>**  
Captures only a given interface.
- **tshark -c <packet\_count>**  
Captures specific number of packets.

# TShark

- `tshark -a <condition>`
  - conditions:
    - `duration:NUM` - stop after NUM seconds.
    - `filesize:NUM` - stop this file after NUM KB.
    - `files:NUM` - stop after NUM files.
- `tshark -Y <display_filter>`

Add a display filter for the capturing.

# TShark

- **tshark -n**

Disable all name resolutions (default: all enabled).

- **tshark -N**

Enable specific name resolution(s).

- **tshark -w <file\_path>**

write captured data to a file.

- **tshark -r <file\_path>**

Read a file contains captured packet details.

# TShark

- **tshark -v**  
display the version.
- **tshark -h**  
Display help.
- **tshark -Y "ip.addr==10.0.0.34" -w:/users/hsenid/desktop/mycap.pcap**
- **tshark -Y "ip.src==10.0.0.34 and ip.dst==239.255.255.250" -r C:/users/hsenid/desktop/mycap.pcap"**

# Questions

