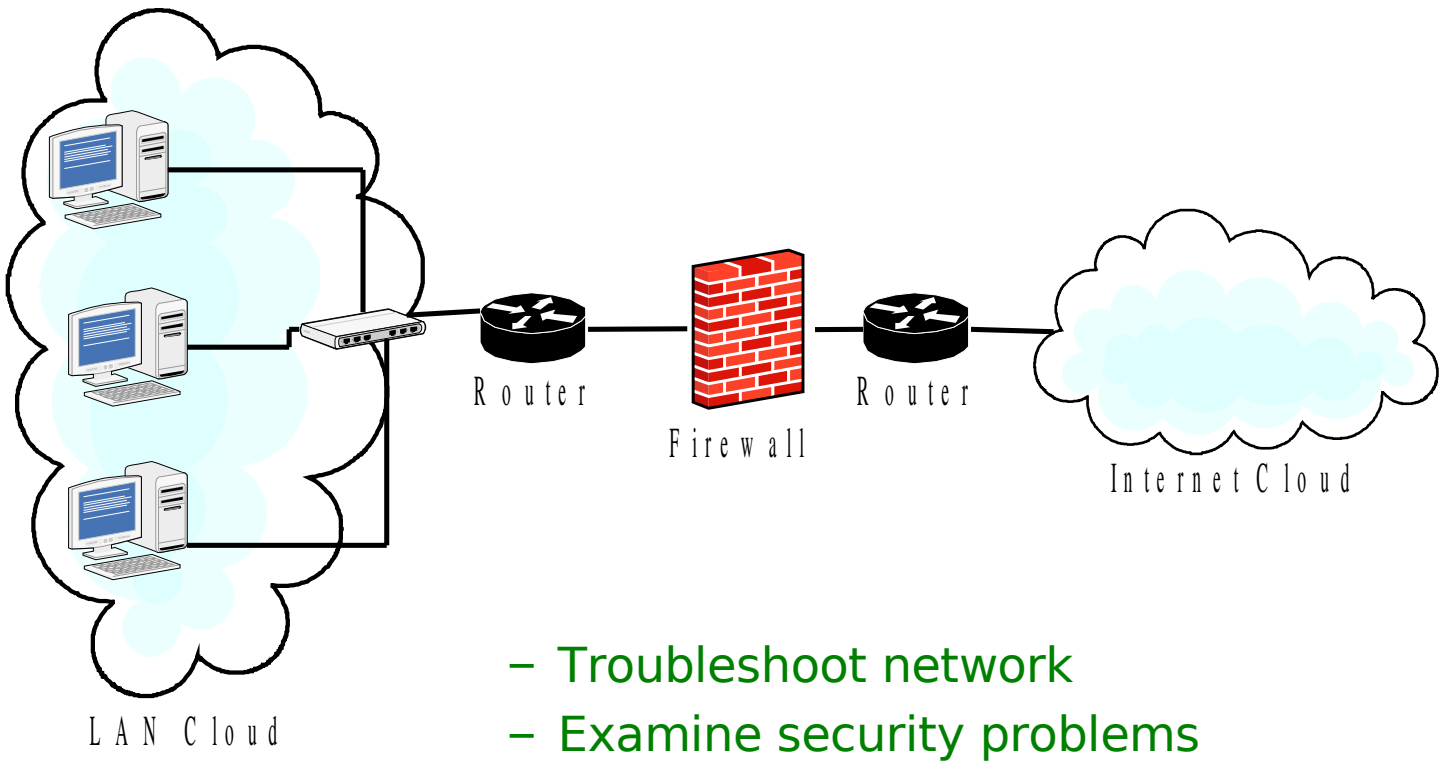
# Wireshark ( Ethereal )

AU – KBC Research Centre

# Overview

- Why Network Analyzers
- How to Analyze Network
- Wireshark ( Ethereal )
- History
- Components
- Functional Flow
- Setting Up and capturing
- Sniffing in Wireless Network
- GUI / Menu Details
- Filters
- Analysis

# Why Network Analyzers




- Troubleshoot network
- Examine security problems
- Debug protocol implementations
- Learn network protocol internals
- Analysis of test conditions

# How to Analyze Network

- By Listening the network (Sniffing)

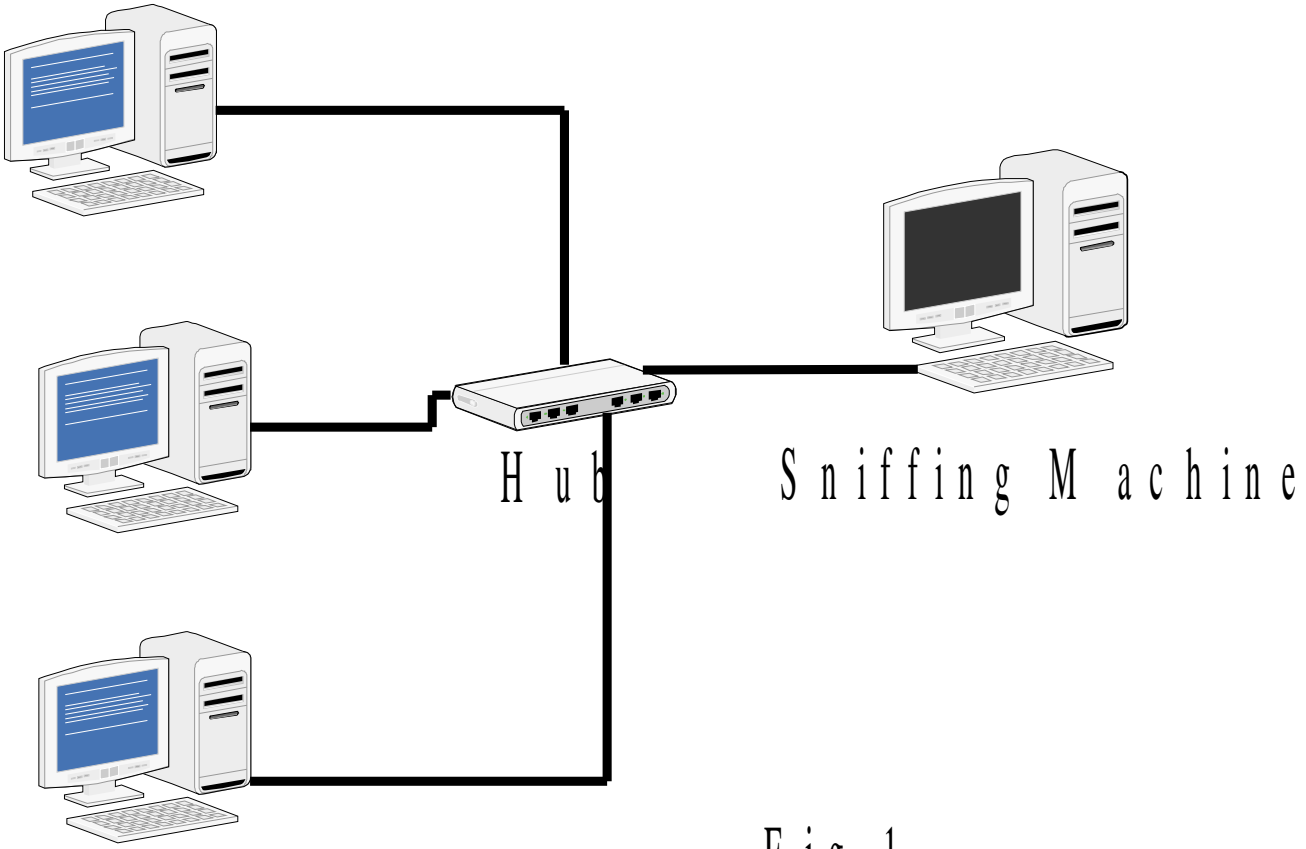



Fig 1

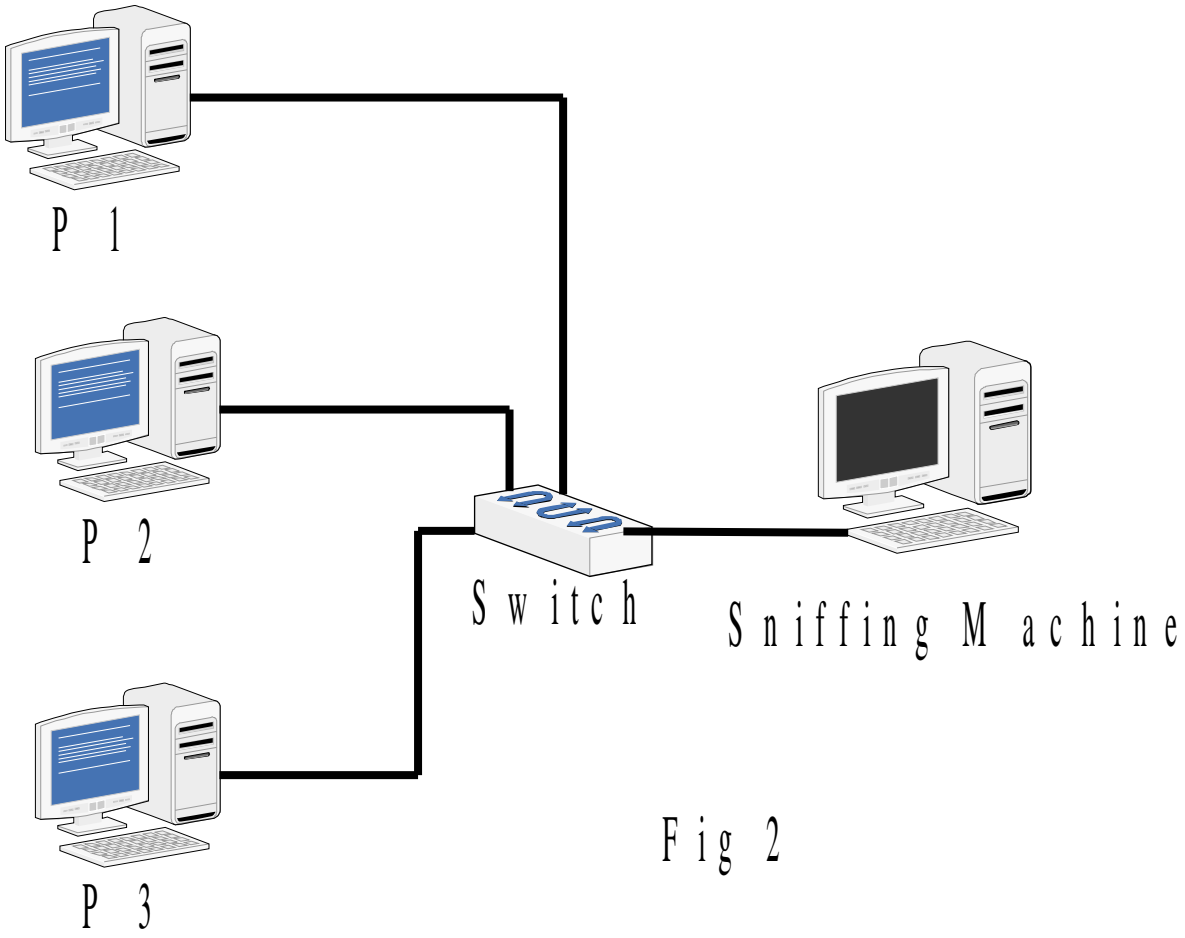



Fig 2

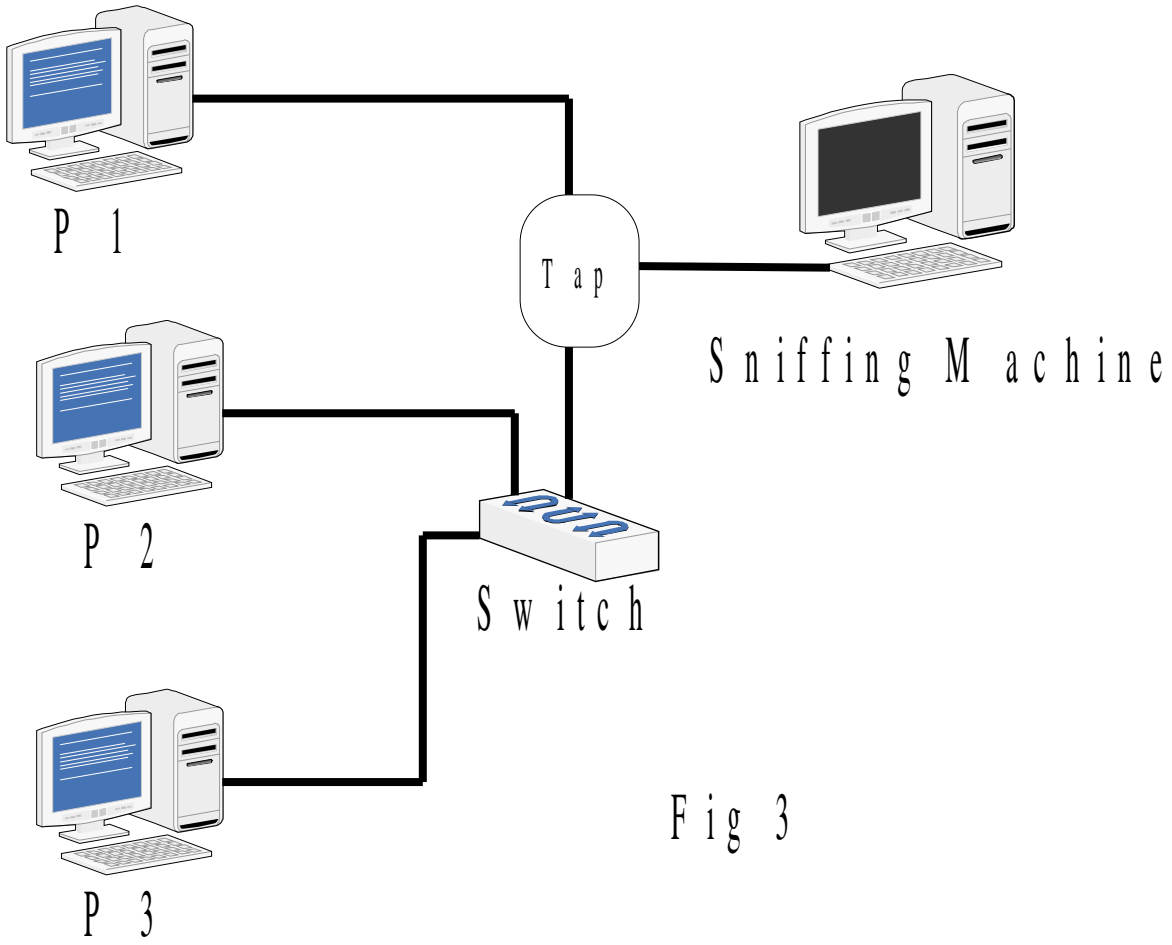



Fig 3

# Wireshark ( Ethereal )

- A famous Network Analyzers
- Work for all six layers of protocols (except physical layer )
- Capable to add new protocols as a module

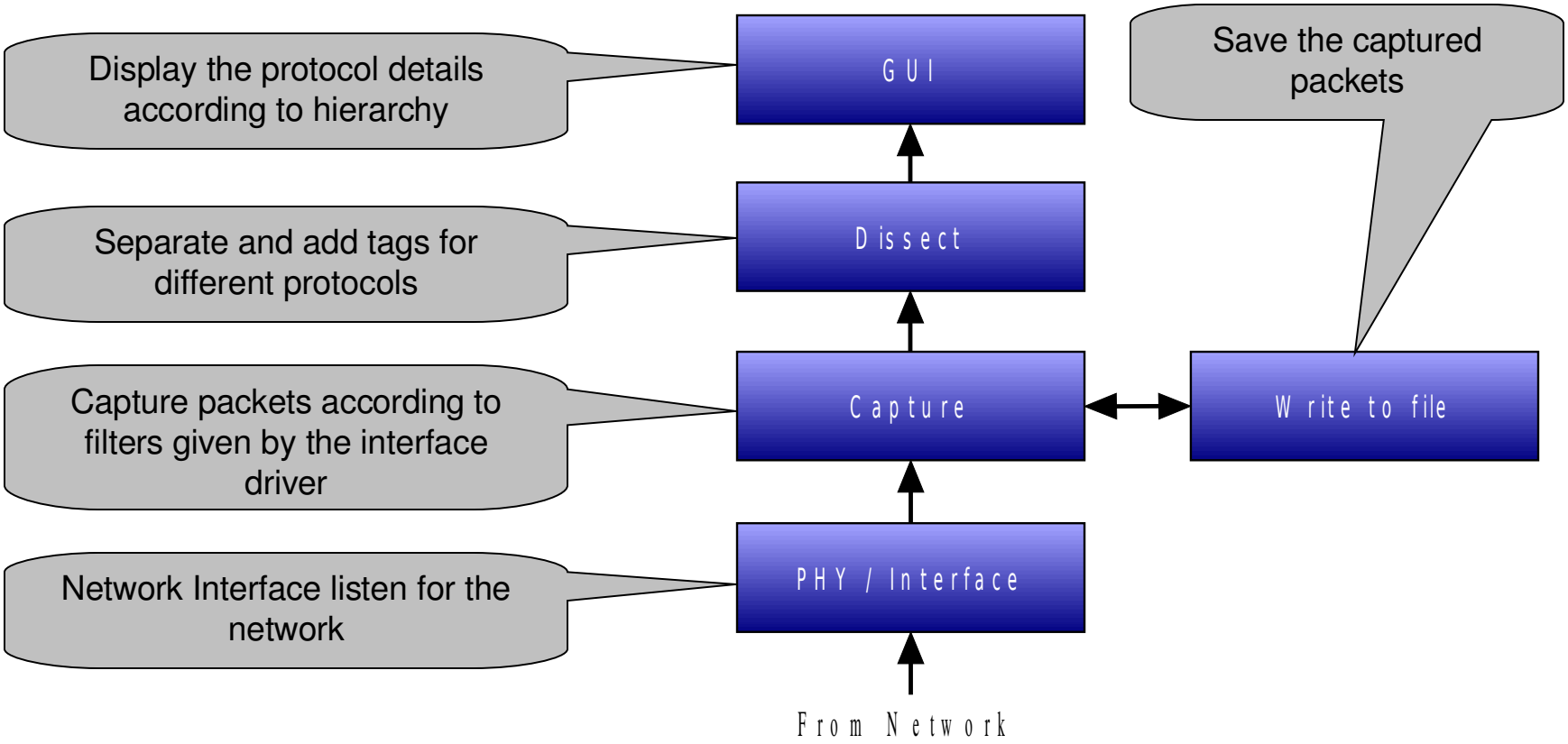
# History of Wireshark

- In 1997, Gerald Combs started developing Ethereal to track down network problems.

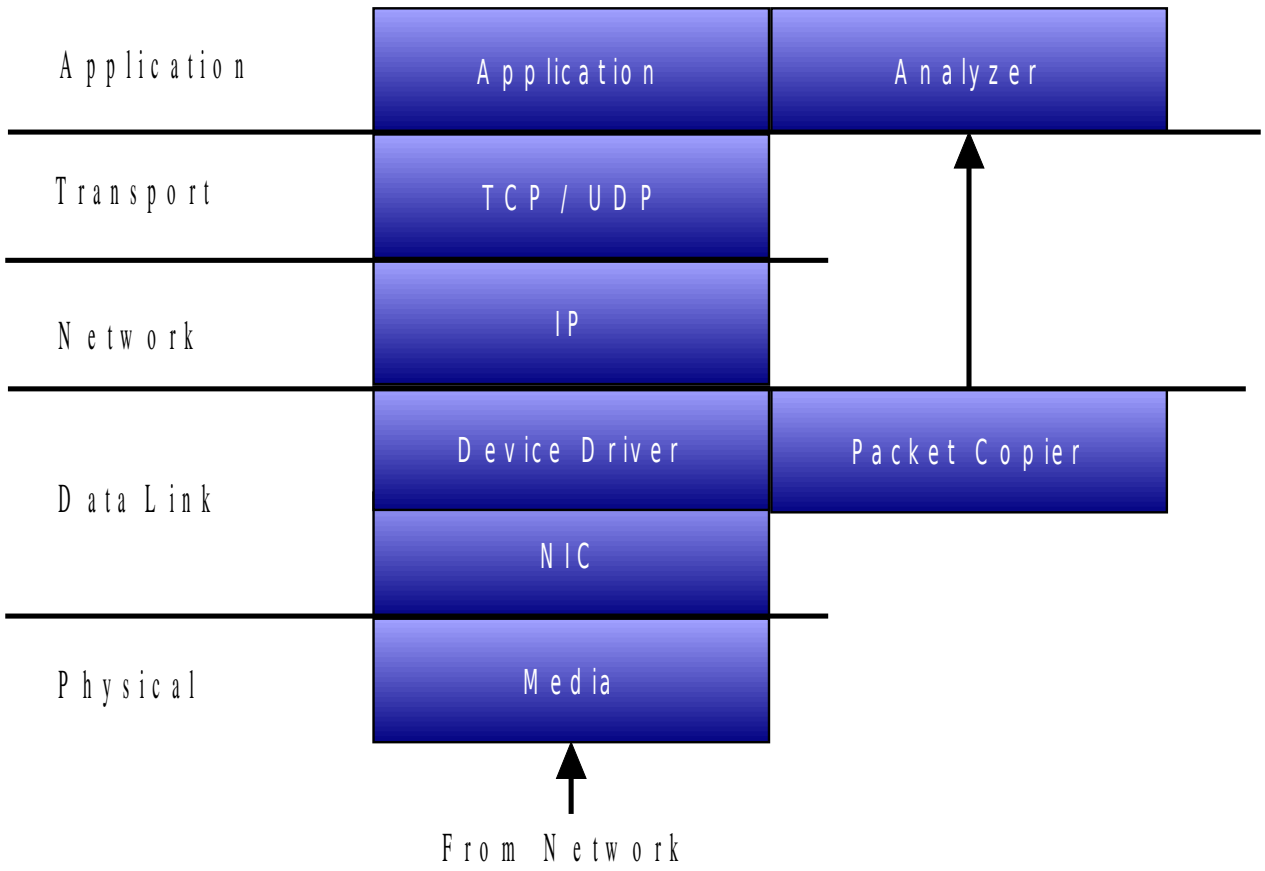
- Gilbert Ramirez contributed a low-level dissector to it
- Now dissector made to a level any new protocol can be added easy

- In June 2006 the project was renamed from Ethereal to Wireshark due to trademark issues

# Components


Display the protocol details according to hierarchy
GUI
Save the captured packets
Separate and add tags for different protocols
Dissect
Capture packets according to filters given by the interface driver
Capture
Write to file
Network Interface listen for the network
PHY / Interface
From Network

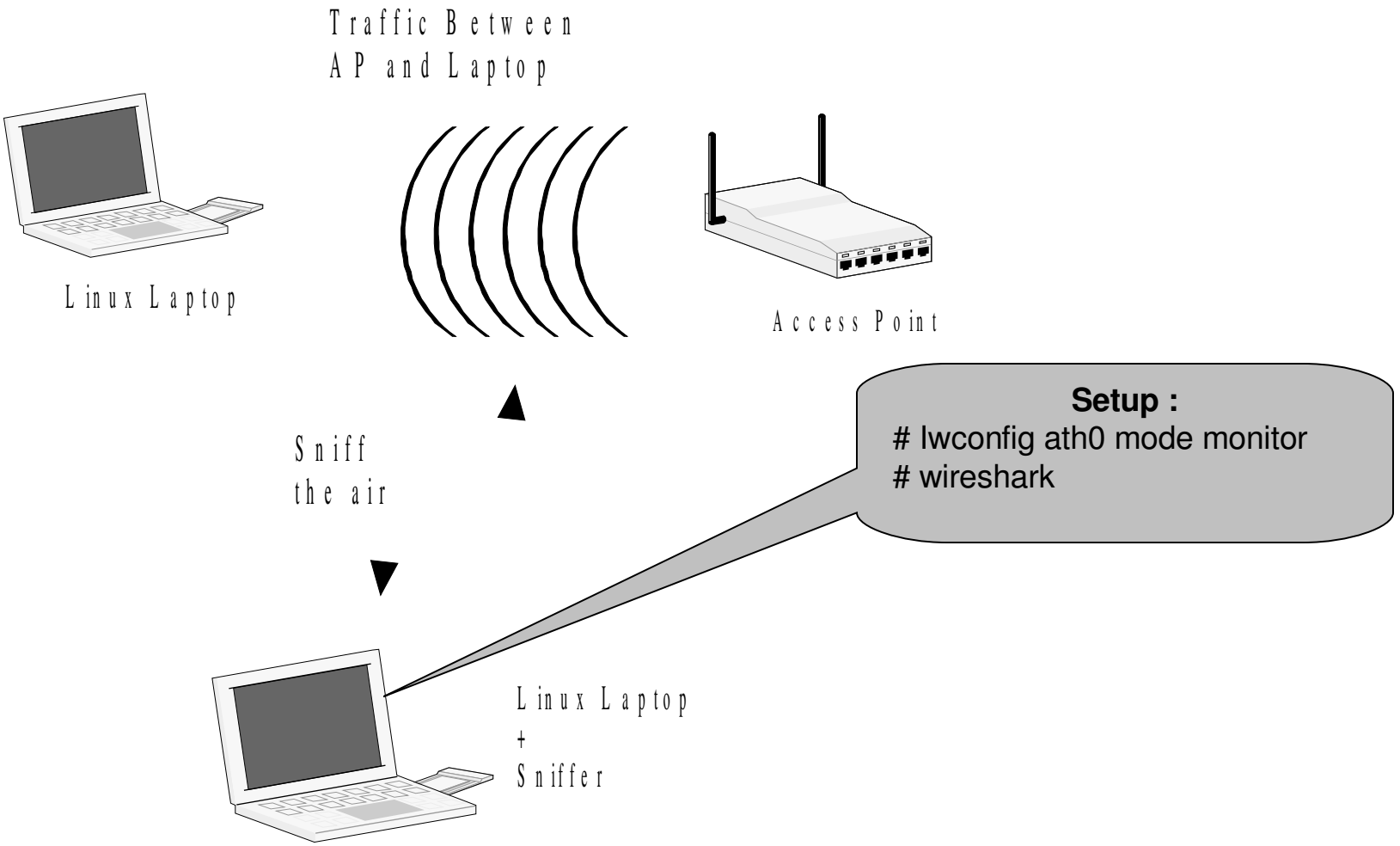
# Functional Flow



# Setting Up and capturing

- Installation
  - Proper driver
  - Ethereal and dependency
- Configuration
  - Network Interface
    - Placing in proper location (logical)
  - Driver
    - Configuring / Setting the NIC to work properly
    - Modes of Sniffing selection
      - » Active
      - » Passive
  - Ethereal
    - Prepare the device / configuration

# Sniffing in Wireless Network



# GUI / Menu Details

- Main window
- Packet List pane
- Packet Details pane
- Packet Bytes pane
- Statusbar
- Menu
  - File
  - Edit
  - View
  - Go
  - Capture
  - Analyze
  - Statistics
  - Help
- Main toolbar
- Filter toolbar

# Filters

- Capture Filters
  - Capture based on
    - Protocol
    - Source, Destination
    - Based on length, etc.
- Display Filters
  - Display based on
    - Protocol
    - Source, Destination
    - Based on length, etc

# Analysis

- Flow Diagram
- Protocol Hierarchy
- Endpoints
- Conversations
- I/O Diagram

# Flow Diagram

- Show a conversation diagram
- Show between hosts
- Show based on time

# Protocol Hierarchy

- This is a tree of all the protocols in the capture. Each row contains the statistical values of one protocol. The following columns containing the statistical values are available:
  - Protocol
  - % Packets
  - Packets
  - Bytes
  - MBit/s
  - End Packets
  - End Bytes
  - End MBit/s

# Endpoints

- A network endpoint is the logical endpoint of separate protocol traffic of a specific protocol layer

# Conversations

- A network conversation is the traffic between two specific endpoints
- An IP conversation is all the traffic between two IP addresses

# I/O Diagram

- User configurable graph of the captured network packets
- Can define up to five differently colored graphs