Introduction to Wireshark

Francesco Musumeci

Wireshark Lab

- It is useful to be able to “view the protocols in action” and be able to “play with the protocols”
- To do this, the ideal is a message manipulation tool (Protocol Data Unit - PDU)
- With Wireshark it is possible to observe the network protocols in action on your computer, interact and exchange messages with the protocol entities running both on the local PC and somewhere else on the Internet

Packet sniffer

- The basic tool of Wireshark captures (sniffs) messages received and transmitted from your PC
- It is an entirely passive module
  - It cannot send packets on its own
  - The packets it receives are not explicitly addressed to the sniffer (it is “transparent” to protocols)
  - It does not change the action of the protocols: the packets it intercepts are copied (dumped), but regularly delivered to the true destination

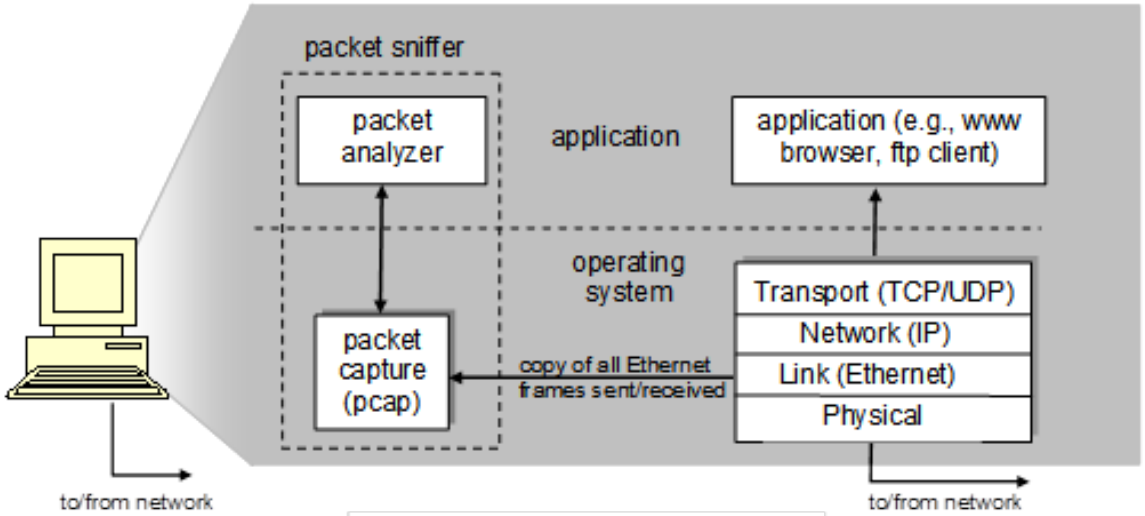


Figure 1: Packet sniffer structure

Packet sniffer

- It consists of two parts
- Packet capture library
  - It receives a copy of all the data-link frames received/transmitted by the PC
- Packet analyzer
  - It is able to recognize the structure of protocol messages
  - It shows the contents of all fields of a captured protocol message

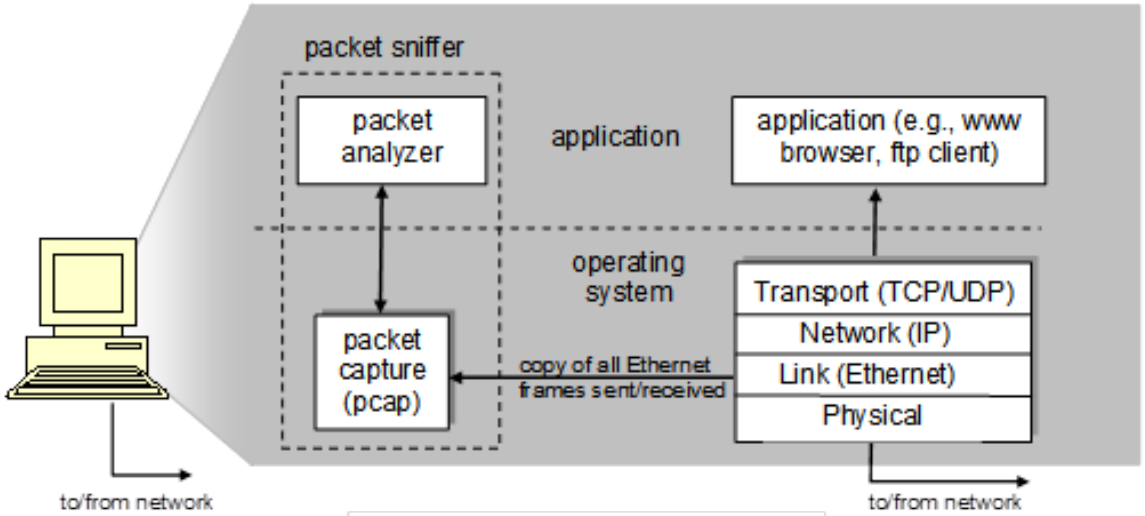


Figure 1: Packet sniffer structure

Message analysis

- The Packet Analyzer exploits the recursive encapsulation carried out by the protocol levels
- It allows you to analyze a message captured at multiple protocol levels (onion skin approach)
- Example
  - Ethernet frame
  - IP packet
  - TCP segment
  - HTTP message
  - Content of the HTTP message

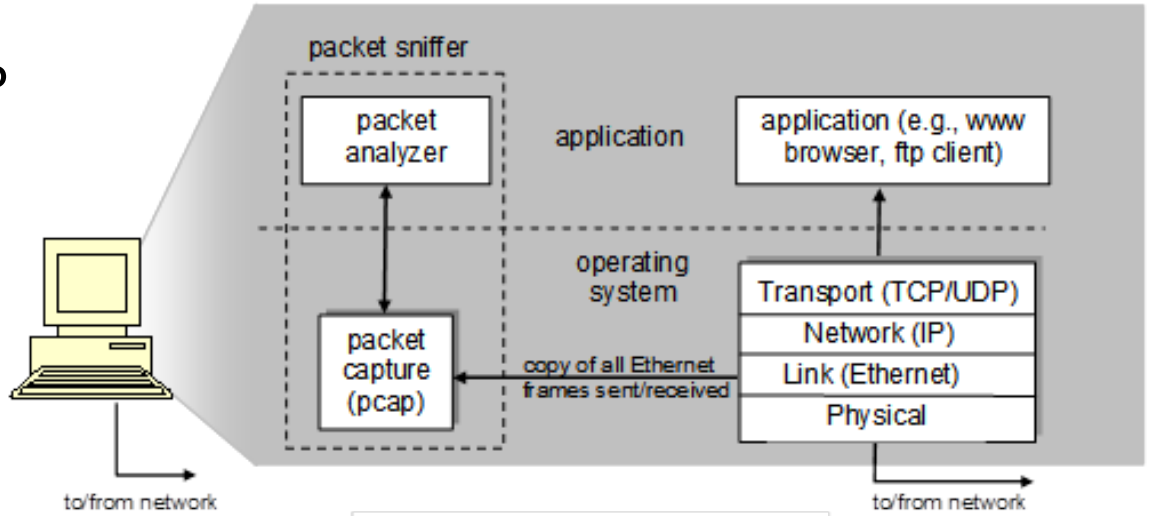


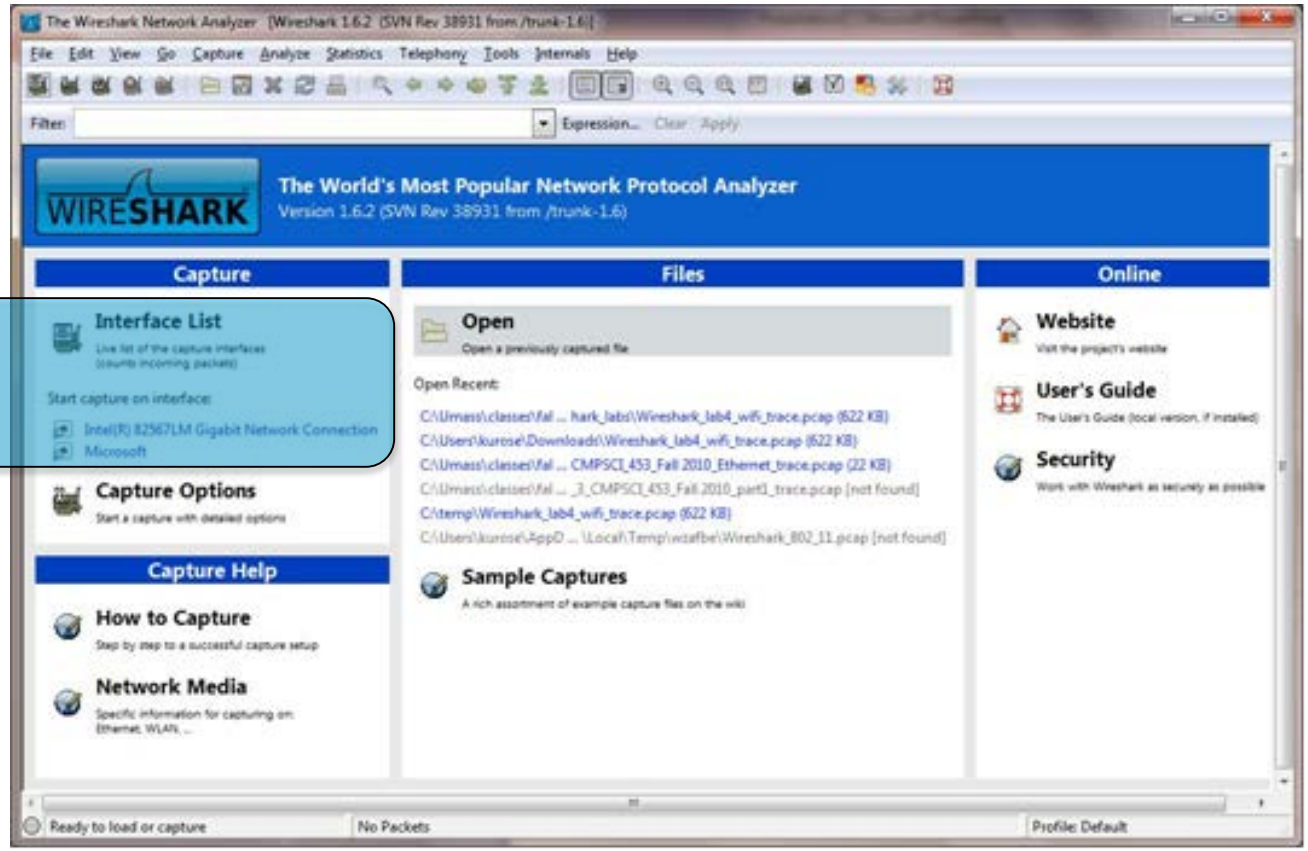
Figure 1: Packet sniffer structure

Wireshark

- Most popular open-source free-ware sniffer program
  - http://www.wireshark.org/
- It uses the *Packet Capture Library* vavailable in the operating system
  - Windows (WinPCap)
  - Linux/Unix (libpcap)
  - Mac (libpcap)
- Well documented and with a large community of users
  - User guide: http://www.wireshark.org/docs/wsug_html_chunked/
  - Man pages: http://www.wireshark.org/docs/man-pages/
  - Detailed FAQ: http://www.wireshark.org/faq.html
- The analyzer supports the formats of hundreds of protocols
- It can operate on many different network interfaces including: Ethernet, PPP and SLIP, 802.11 WiFi

Wireshark

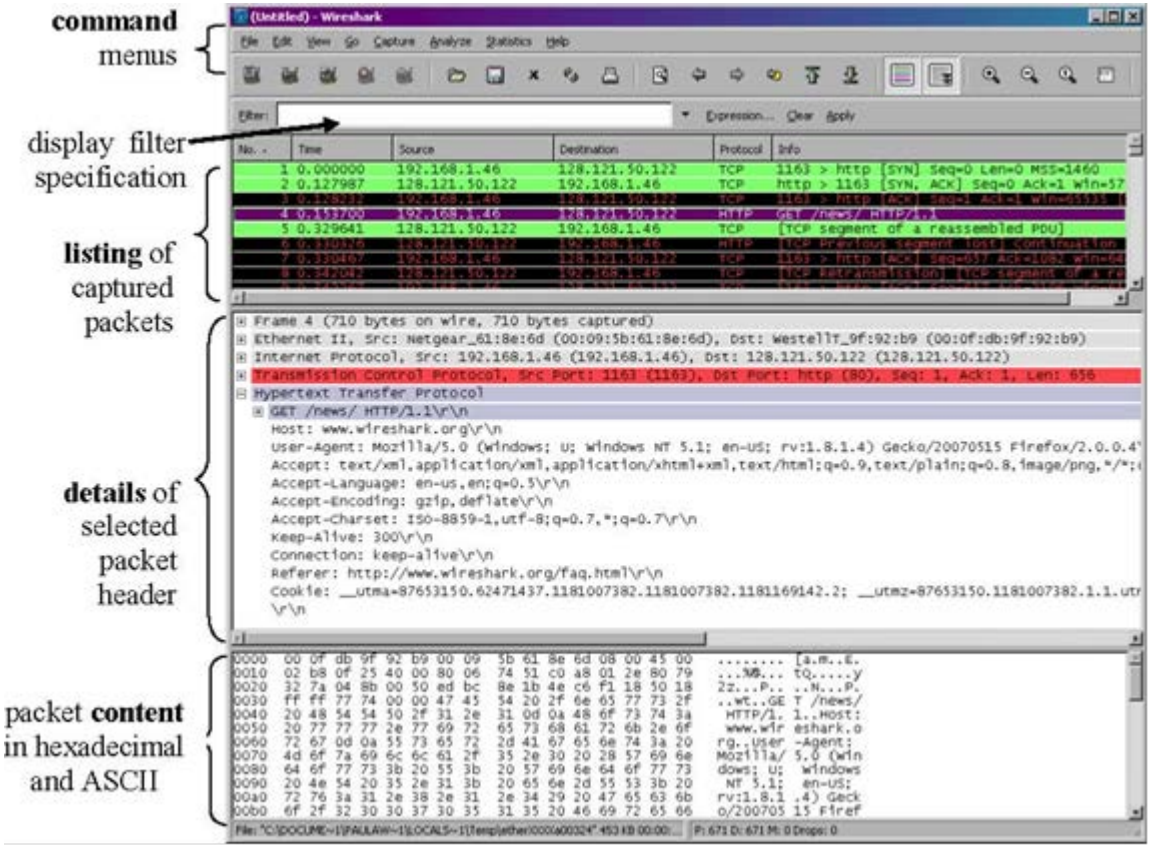
- Installation (http://www.wireshark.org/download.html)
  - The necessary Lan Packet Capture Library is automatically installed in the OS if not already present
- Startup screen (Win):



PC interface list. Clicking twice on one, the capture starts

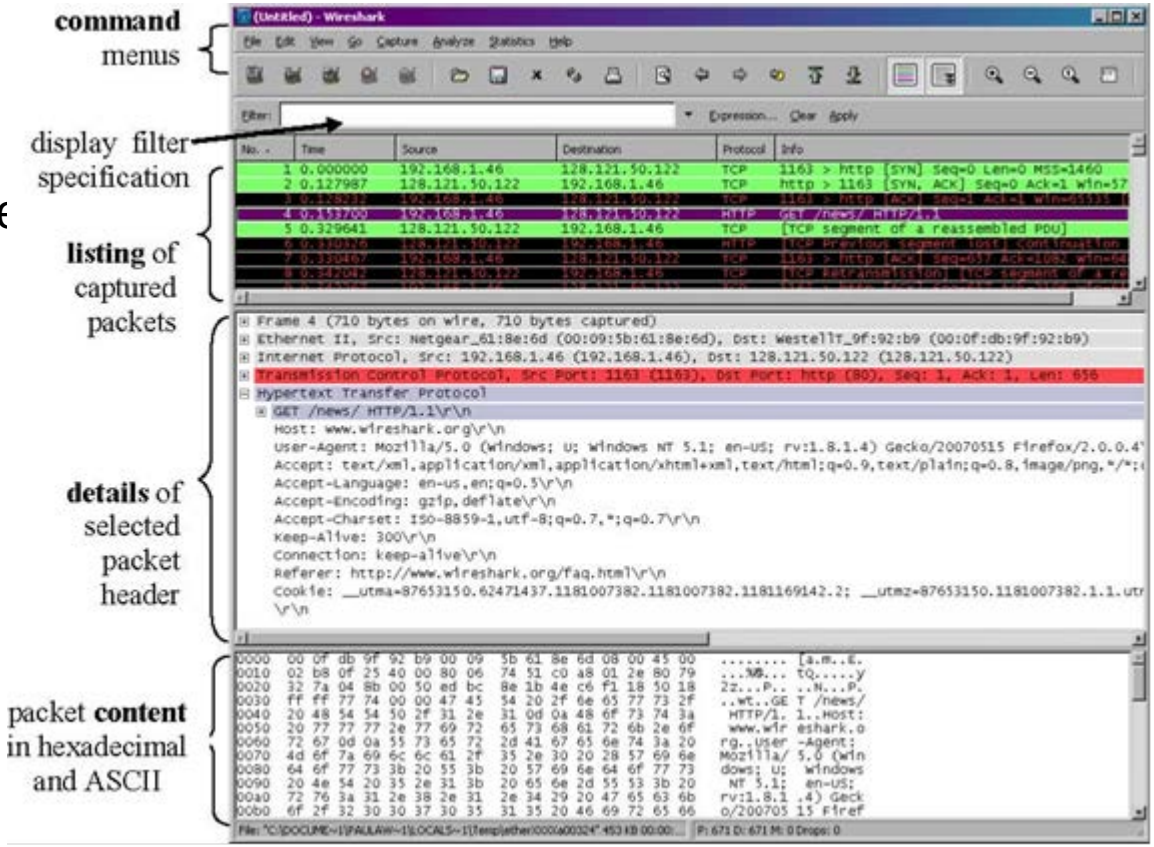
Capture display

- Command menu
  - File: to save or open captures
  - Capture: to start capturing
  - ...
- Packet List
  - Packet number (assigned by Ws), capture time, source/destination addresses, protocol, specific fields
  - It can be ordered
  - Protocol type shows the highest level that caused the sending



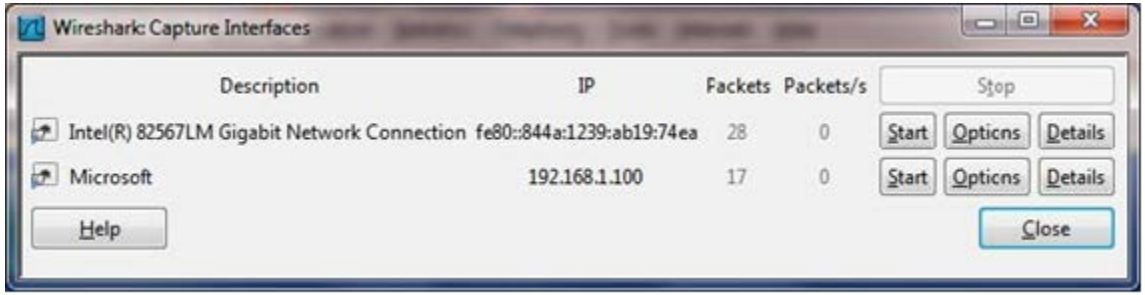
Capture display

- Header details
  - Details on the selected packet
  - Info about the frame, IP packet, and UDP/TCP segment that contain the message
    - They can expanded or compressed
  - Info on high level protocol
  - Packet contents
    - In ASCII and hexadecimal format
  - Filter fields
    - To select or hide packets based on various filtering criteria



Exercise: test run

- Open a browser
- Start Ws
- Menu: Capture → Intreface
  - Start on the interface you want to use
- In the browser, enter the URL
- http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
  - After the INTRO-wireshark-file1.html page appears in the browser, stop the Ws capture



Exercise: test run

- Write “http” in the filter window
- Look for the response to the HTTP GET message that contains the phrase that is displayed in the browser