



# Wireshark Fundamentals

# Wireshark Fundamentals

## » Welcome!

## » Wireshark fundamentals

- What is a protocol analyzer used for?
- Why use Wireshark?
- What do I need to know to use Wireshark?

## » Advanced topics

- Wireshark Advanced Technology Course

# Wireshark Fundamentals

The image displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main packet list shows three HSRP (Hot Standby Router Protocol) packets (No. 282, 283, 284) with source addresses 10.121.90.2, 10.121.90.3, and 10.121.78.3, all destined to 224.0.0.2. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Hot Standby Router Protocol. The packet bytes pane shows the raw data. The bottom pane displays the Protocol Hierarchy Statistics, showing the distribution of protocols in the capture. The Local Area Connection - Graph Analysis pane shows a timeline of network activity, including an M-SEARCH \* HTTP packet and a Who has 10.121.90.1 packet.

Filter:  Expression... Clear Apply Save TCP Full ARP Filter

802.11 Channel:  Channel Offset:  FCS Filter: All Frames  None  Wireless Settings... Decryption Keys...

No.	Time	Source	Destination	Protocol	Address
282	0.013815000	10.121.90.2	224.0.0.2	HSRP	01:00:5e:00:00:02,00:
283	0.107386000	10.121.90.3	224.0.0.2	HSRP	01:00:5e:00:00:02,10:
284	0.103823000	10.121.78.3	224.0.0.2	HSRP	01:00:5e:00:00:02,10:

Protocol Hierarchy Statistics

Display filter: none

	% Packets	Packets	% Bytes
Internet Protocol Version 4	100.00 %	298	100.00 %
Transmission Control Protocol	85.91 %	256	94.40 %
TCP Reset Sequence	64.43 %	192	56.10 %
Text Transfer Protocol	12.08 %	36	23.60 %
Domain Name Service	6.04 %	18	2.75 %
Hot Standby Router Protocol	25.51 %	79	10.80 %

Local Area Connection - Graph Analysis

Time

10.121.90.69 239.255.255.250 Ibm\_71:b5:d6 Broadcast

M-SEARCH \* HTTP/1.1 (57030) (1900)

Who has 10.121.90.1 (0) (0)

# Wireshark Fundamentals

## » WCNA exam

## » What is the exam about?


- Exam details
- How to prepare
- Exam prep

## » Course goals

- Learn how to use Wireshark and pass the WCNA exam

# Wireshark Fundamentals

## Section 1: Network Analysis Overview

- ✓ Define the Purpose of Network Analysis
- ✓ List Troubleshooting Tasks for the Network Analyst 
- ✓ List Security Tasks for the Network Analyst
- ✓ List Optimization Tasks for the Network Analyst
- ✓ List Application Analysis Tasks for the Network Analyst
- ✓ Define Legal Issues of Listening to Network Traffic
- ✓ Overcome the "Needle in the Haystack " Issue
- ✓ Understand General Network Traffic Flows
- ✓ Review a Checklist of Analysis Tasks

## Section 2: Introduction to Wireshark

- ✓ Describe Wireshark's Purpose
- ✓ Know How to Obtain the Latest Version of Wireshark
- ✓ Compare Wireshark Release and Development Versions

# Questions?