1.	Record Nr.	UNINA9910551825803321
	Autore	Jain Vinit
	Titolo	Wireshark fundamentals : a network engineer's handbook to analyzing network traffic / / Vinit Jain
	Pubbl/distr/stampa	Berkeley, California : , : Apress L. P., , [2022] ©2022
	ISBN	1-4842-8002-4
	Descrizione fisica	1 online resource (267 pages) : illustrations
	Disciplina	004.62
	Soggetti	Computer network protocols Packet switching (Data transmission) Computer networks - Monitoring Packet transport networks
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di contenuto	Intro -- Table of Contents -- About the Author -- About the Technical Reviewers -- Acknowledgments -- Introduction -- Chapter 1: Introduction to Wireshark -- Introduction to Network Traffic Analysis -- Network Sniffing -- Sniffer Placement -- Number of Sniffer Placements -- Network Tap -- Overview of Wireshark -- Installing Wireshark -- Installing Wireshark on Windows -- Installing Wireshark on Mac -- Installing Wireshark on Ubuntu -- Setting Up Port Mirroring -- SPAN on Cisco IOS/IOS-XE -- SPAN on Cisco Nexus Switches -- Enabling Port Mirroring on Arista EOS -- Enabling Port Mirroring on JunOS -- Summary -- References in This Chapter -- Chapter 2: Getting Familiar with Wireshark -- Overview of Wireshark Tool -- Wireshark Preferences -- Appearance -- Capture -- Expert -- Filter Buttons -- Name Resolution -- Protocols -- RSA Keys -- Statistics -- Advanced -- Performing Packet Capture Using Wireshark -- Dissectors -- Configuration Profiles -- Filtering with Wireshark -- Capture Filters -- Display Filters -- Working with Wireshark Capture Files -- PCAP vs. PCAPng -- Capture from Multiple Interfaces -- Timestamps -- Embedding Comments -- Metadata -- Extendable Format -- Splitting Packet Captures into Multiple Files -- Merging Multiple Capture Files --

Sommario/riassunto

Understand the fundamentals of the Wireshark tool that is key for network engineers and network security analysts. This book explains how the Wireshark tool can be used to analyze network traffic and teaches you network protocols and features. Author Vinit Jain walks you through the use of Wireshark to analyze network traffic by expanding each section of a header and examining its value. Performing packet capture and analyzing network traffic can be a complex, time-consuming, and tedious task. With the help of this book, you will use the Wireshark tool to its full potential. You will be able to build a strong foundation and know how Layer 2, 3, and 4 traffic behave, how various routing protocols and the Overlay Protocol function, and you will become familiar with their packet structure. Troubleshooting engineers will learn how to analyze traffic and identify issues in the network related to packet loss, bursty traffic, voice quality issues, etc. The book will help you understand the challenges faced in any network environment and how packet capture tools can be used to identify and isolate those issues. This hands-on guide teaches you how to perform various lab tasks. By the end of the book, you will have in-depth knowledge of the Wireshark tool and its features, including filtering and traffic analysis through graphs. You will know how to analyze traffic, find patterns of offending traffic, and secure your network. What You Will Learn Understand the architecture of Wireshark on different operating systems Analyze Layer 2 and 3 traffic frames Analyze routing protocol traffic Troubleshoot using Wireshark Graphs Who This Book Is For Network engineers, security specialists, technical support engineers, consultants, and cyber security engineers.