1.

Record Nr.	UNINA9910637718803321
Autore	Nainar Nagendra Kumar
Titolo	Wireshark for Network Forensics : An Essential Guide for IT and Cloud Professionals / / by Nagendra Kumar Nainar, Ashish Panda
Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2023
ISBN	1-4842-9001-1
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (283 pages)
Disciplina	004.62
Soggetti	Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Ch1:Wireshark Primer -- Ch 2: Packet Capture and Analysis -- Ch 3: Capturing Secured Application for Analysis -- Ch 4: Wireless Packet Capture and Analysis -- Ch 5: Multimedia Capture and Analysis -- Ch 6:Cloud and Cloud-Native Traffic Capture -- Ch 7: Bluetooth Protocol Capture and Analysis -- Ch 8: Wireshark Analysis and Network Forensic. - Ch 9: Writing your own Dissector.
Sommario/riassunto	With the advent of emerging and complex technologies, traffic capture and analysis play an integral part in the overall IT operation. This book outlines the rich set of advanced features and capabilities of the Wireshark tool, considered by many to be the de-facto Swiss army knife for IT operational activities involving traffic analysis. This open-source tool is available as CLI or GUI. It is designed to capture using different modes, and to leverage the community developed and integrated features, such as filter-based analysis or traffic flow graph view. You'll start by reviewing the basics of Wireshark, and then examine the details of capturing and analyzing secured application traffic such as SecureDNS, HTTPS, and IPSec. You'll then look closely at the control plane and data plane capture, and study the analysis of wireless technology traffic such as 802.11, which is the common access technology currently used, along with Bluetooth. You'll also learn ways to identify network attacks, malware, covert communications, perform security incident post mortems, and ways to prevent the same. The book further explains the capture and analysis of secure multimedia traffic, which constitutes around 70% of all overall internet traffic.

Wireshark for Network Forensics provides a unique look at cloud and cloud-native architecture-based traffic capture in Kubernetes, Docker-based, AWS, and GCP environments. You will: Review Wireshark analysis and network forensics Study traffic capture and its analytics from mobile devices Analyze various access technology and cloud traffic Write your own dissector for any new or proprietary packet formats Capture secured application traffic for analysis.