1. Record Nr. UNINA9910788098203321

Autore	Baxter James H.
Titolo	Wireshark essentials : get up and running with Wireshark to analyze network packets and protocols effectively / / James H. Baxter
Pubbl/distr/stampa	Birmingham : , : Packt Publishing, , 2014
ISBN	1-78355-464-9
Edizione	[1st edition]
Descrizione fisica	1 online resource (194 p.)
Collana	Community experience distilled
Disciplina	004.66
Soggetti	Computer networks - Management Computer network protocols
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover; Copyright; Credits; About the Author; About the Reviewers; www.PacktPub.com; Table of Contents; Preface; Chapter 1: Getting Acquainted with Wireshark; Installing Wireshark; Installing Wireshark on Windows; Installing Wireshark on Mac OS X; Installing Wireshark on Linux/Unix; Performing your first packet capture; Selecting a network interface; Performing the packet capture; Wireshark user interface essentials; Filtering out the noise; Applying a display filter; Saving the packet trace; Summary; Chapter 2: Networking for Packet Analysts; The OSI model - why it matters; Network protocols The seven OSI layersLayer 1 - the physical layer; Layer 2 - the data-link layer; Layer 3 - the network layer; Layer 4 - the transport layer; Layer 5 - the session layer; Layer 6 - the presentation layer; Layer 7 - the application layer; IP networks and subnets; Switching and routing packets; Ethernet frames and switches; IP addresses and routers; WAN links; Wireless networking; Summary; Chapter 3: Capturing All the Right Packets; Picking the best capture point; User location; Server location; Other capture locations; Mid-network captures; Both sides of specialized network devices TAPs and switch port mirroringTest Access Port; Switch port mirroring; Capturing packets on high traffic rate links; Capturing interfaces, filters, and options; Selecting the correct network interface; Using capture filters; Configuring capture filters; Capture options; Capturing filenames and locations; Multiple file options; Ring buffer; Stop capture

options; The display options; Name resolution options; Verifying a good capture; Saving the bulk capture file; Isolating conversations of interest; Using the Conversations window; The Ethernet tab; The TCP and UDP tabs; The WLAN tab
Wireshark display filtersThe Display Filter window; The display filter syntax; Typing in a display filter; Display filters from a Conversations or Endpoints window; The filter expression buttons; Using the Expressions window button; Right-click menus on specific packet fields; Following TCP/UDP/SSL streams; Marking and ignoring packets; Saving filtered traffic; Summary; Chapter 4: Configuring Wireshark; Working with packet timestamps; How Wireshark saves timestamps; Wireshark time display options; Adding a time column; Conversation versus displayed packet time options
Choosing the best Wireshark time display optionUsing the Time Reference option; Colorization and coloring rules; Packet colorization; Wireshark preferences; Wireshark profiles; Creating a Wireshark profile; Selecting a Wireshark profile; Summary; Chapter 5: Network Protocols; The OSI and DARPA reference models; Network layer protocols; Wireshark IPv4 filters; Wireshark ARP filters; Internet Group Management Protocol; Wireshark IGMP filters; Internet Control Message Protocol; ICMP pings; ICMP traceroutes; ICMP control message types; ICMP redirects; Internet Protocol Version 6; IPv6 addressing
IPv6 address types

Sommario/riassunto

This book is aimed at IT professionals who want to develop or enhance their packet analysis skills. Basic familiarity with common network and application services terms and technologies is assumed; however, expertise in advanced networking topics or protocols is not required. Readers in any IT field can develop the analysis skills specifically needed to complement and support their respective areas of responsibility and interest.