Wireshark로 배우는 컴퓨터 네트워크

개정판

이재광 · 김봉한 지음

생능출판

저자 소개

이재광
한남대학교 공과대학 컴퓨터공학과

김봉한
청주대학교 공과대학 디지털보안전공

Wireshark로 배우는 컴퓨터 네트워크(개정판)

초판발행 2020년 8월 7일
제2판1쇄 2021년 7월 21일

지은이 이재광, 김봉한
펴낸이 김승기
펴낸곳 생능출판사 / **주소** 경기도 파주시 광인사길 143
출판사 등록일 2005년 1월 25일 / **신고번호** 제406-2005-000002호
대표전화 (031)955-0761 / **팩스** (031)955-0768
홈페이지 www.booksr.co.kr

책임편집 권소정 / **편집** 신성민, 양둥글, 유제훈 / **디자인** 유준범
마케팅 최복락, 김민수, 심수경, 차종필, 백수정, 최태웅, 명하나, 김범용, 김민정
인쇄 · 제본 (주)상지사P&B

ISBN 978-89-7050-500-8 93560
정가 35,000원

개정판 머리말

인터넷은 지난 수십 년 동안 우리의 삶에 엄청난 변화를 가져왔다. 최근에 우리는 거의 매일 인터넷을 사용하여 많은 일을 처리하고 있다. 하지만 우리가 이용하고 있는 웹서핑, 검색, 파일 전송, 이메일, 메신저, SNS, 유튜브, 페이스북 등이 실제로 인터넷에서 어떠한 형태로 전달되는지 확인해 본 적이 있는가? 대부분 학생은 학교에서 인터넷, TCP/IP, 컴퓨터 네트워크, 컴퓨터 통신 등에 대해 배우고 있지만, TCP/IP 프로토콜을 통하여 주고받는 내용을 실제로 확인하면서 프로토콜을 보다 분명하게 이해하는 과정을 접해본 학생들은 많지 않을 것이다. 그뿐만 아니라 대부분 대학에서 진행되고 있는 강의가 이론 중심으로 이루어지고 있어서 실제 프로토콜에 따라 진행되는 내용이 어떻게 이루어지는지 궁금한 생각을 하는 학생들이 많을 것으로 생각된다. TCP/IP 프로토콜을 보다 분명하게 이해한다면 인터넷에서 일어날 수 있는 트러블슈팅을 할 수 있거나 보안 침해 사고 발생 시에도 적절하게 대처할 수 있는 전문가가 될 수 있을 것이다.

최근 와이어샤크(Wireshark)는 sectools.org에서 TOP 125 네트워크 보안 툴에서 수년 동안 당당히 1위를 차지하고 있는 아주 유명한 네트워크 분석 툴이다. 네트워크 트래픽 분석은 모든 IT 엔지니어들이 갖추어야 할 핵심 기술이며, 이것을 이용하면 유/무선 트래픽을 실제로 캡처하여 네트워크를 효과적으로 분석할 수 있다.

이 책은 IT 전문가가 되고자 하는 학생들이 트러블슈팅, 보안 및 네트워크 최적화를 위해서 사용하는 필수 도구인 와이어샤크에 대해 설명한 책으로 이 책에서 설명한 내용을 차근차근 따라하다 보면 TCP/IP 프로토콜을 정확하게 이해할 뿐만 아니라 각종 문제점을 잘 해결할 수 있는 전문가가 될 수 있을 것으로 생각한다. 와이어샤크 홈페이지에 접속해서 프로그램을 다운로드하고, 설치하는 방법에서부터 와이어샤크가 가지고 있는 다양한 기능들을 익힌 다음, 실제로 패킷을 캡처해서 계층별 프로토콜을 하나하나씩 익혀나가면 컴퓨터 네트워크 전체의 계층을 종합적으로 이해할 수 있는 IT 전문가로서 성장할 수 있을 것이다.

이 책은 Wireshark 3.4.4를 기반으로 작성하였다. 현재 6월 초에 3.4.6 버전이 발표되었다. 버전-업은 되었지만 익히는 데는 큰 차이가 없어서 3.4.4 버전을 중심으로 작성되었다. 버전-업이 지속적으로 이루어지고 있지만 3.4.4 버전을 중심으로 익혀나간다면 큰 어려움은 없을 것이다. 이 책이 많은 독자에게 큰 도움이 될 수 있기를 기대해 본다.

끝으로 이 책이 출간되어 나오는 데 많은 도움을 준 분들에게 진심으로 고마운 마음을 드리며, 이 책을 출판하여주신 생능출판사와 담당 직원분들께도 감사를 드린다. 끝으로 나름 좋은 책을 만들고자 노력했지만, 책의 내용 중에 잘못된 부분이 있는 경우에는 좀 더 좋은 책을 만들 수 있도록 저자의 메일 주소로 보내주시기를 기대한다.

2021년 7월

한남대학교 공과대학 컴퓨터공학과 이재광교수
jklee@hnu.kr
청주대학교 공과대학 디지털보안 전공 김봉한교수
bhkim@cju.ac.kr

차례