



Wireshark 3.0

Wireshark로 배우는 개정판
컴퓨터 네트워크

이재광 · 김봉한 지음

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, 양동글, 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

- 이 책의 저작권은 (주)생능출판사와 지은이에게 있습니다. 무단 복제 및 전재를 금합니다.
- 잘못된 책은 구입한 서점에서 교환해 드립니다.

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

개정판 머리말

3

CHAPTER 01 개요

1. 인터넷의 역사	21
1.1 ARPANET	21
1.2 인터넷의 탄생	21
1.3 TCP/IP	22
1.4 MILNET	23
1.5 CSNET	23
1.6 NSFNET	23
1.7 ANSNET	23
1.8 현재의 인터넷	24
1.9 월드 와이드 웹	25
1.10 인터넷의 성장	26
1.11 국내 인터넷 역사	26
1.12 국가 초고속 정보 통신망	27
2. 프로토콜과 표준	29
2.1 프로토콜	29
2.2 표준	30
3. 표준화 기구	31
3.1 국제 표준	32
3.2 국내 표준	36
4. 인터넷 표준	38
4.1 완성 단계	38
4.2 RFC 요구 단계	40
5. 인터넷 관리	41
5.1 ISOC	42
5.2 IAB	42
5.3 IETF	42
5.4 IRTF	43
5.5 IANA와 ICANN	43

5.6 NIC	43
5.7 국내 인터넷 관리	43
요약	45
연습문제	47

CHAPTER 02 OSI 모델과 TCP/IP 프로토콜

1. 프로토콜 계층구조	53
1.1 계층구조	54
1.2 서비스	55
2. OSI 기본 참조 모델	55
2.1 계층화된 구조	56
2.2 계층-대-계층 통신	57
2.3 캡슐화	58
2.4 OSI 모델의 계층 구조	59
2.5 OSI 계층의 요약	64
3. TCP/IP 프로토콜	65
3.1 OSI와 TCP/IP 그룹 간 비교	66
3.2 TCP/IP 프로토콜의 계층들	67
3.3 전송층	73
4. 주소지정	76
4.1 물리 주소	76
4.2 논리 주소	78
4.3 포트 주소	80
4.4 응용 지정 주소	82
요약	83
연습문제	84

CHAPTER 03 네트워크층 개요

1. 개요	93
2. 교환	94
2.1 회선 교환	94
2.2 패킷 교환	95

3. 네트워크층에서 패킷 교환	95
3.1 비연결형 서비스	95
3.2 연결형 서비스	97
4. 네트워크층 서비스	102
4.1 네트워크층 서비스의 예	102
4.2 논리 주소체계	103
4.3 발신지 컴퓨터에서 제공되는 서비스	104
4.4 각 라우터에서 제공되는 서비스	106
4.5 목적지 컴퓨터에서 제공되는 서비스	107
5. 네트워크층 문제점들	108
5.1 오류 제어	108
5.2 흐름 제어	110
5.3 혼잡 제어	110
5.4 서비스 품질	111
5.5 라우팅	111
5.6 보안	112
요약	113
연습문제	114

CHAPTER 04 IP 주소

1. 개요	118
1.1 주소 공간	119
1.2 표기법	119
1.3 주소의 범위	122
1.4 연산	123
2. 클래스 기반 주소지정	126
2.1 클래스	126
2.2 클래스와 블록	129
2.3 2계층 주소지정	132
2.4 3계층 주소지정: 서브네팅	138
2.5 슈퍼네팅	142
3. 클래스 없는 주소지정	143
3.1 가변 길이 블록	144
3.2 2단계 주소 체계	145
3.3 블록 할당	149

3.4 서브네팅	151
4. 특수 주소	155
4.1 특수 블록	155
4.2 블록에 속하는 특수 주소	158
5. IPv6 주소	159
5.1 표기법	159
5.2 주소 공간	163
5.3 세 가지 주소 유형	164
6. IPv6 주소 공간 할당	164
요약	166
연습문제	167

CHAPTER 05 IP 패킷 전달과 포워딩

1. 연결형과 비연결형 서비스	176
2. 직접 전달과 간접 전달	177
2.1 직접 전달	177
2.2 간접 전달	178
3. 포워딩	179
3.1 목적지 주소 기반 포워딩	179
3.2 레이블 기반 포워딩	199
4. 라우터의 구조	202
요약	207
연습문제	208

CHAPTER 06 와이어샤크 개요 및 설치와 실행

1. 패킷 분석기	217
1.1 패킷 분석기의 종류	218
2. 와이어샤크 개요	219
2.1 와이어샤크의 용도	220
2.2 와이어샤크의 주요 기능	220
2.3 와이어샤크의 장점	221
2.4 와이어샤크의 취약 분야	221