2019-2학기 컴퓨터 네트워크

TCP/IP 프로토콜 분석 프로그램 구현 계획서

9팀
2014154037 한승우
2016154010 김지우
2016156032 전유미
2017152049 정하림

INDEX

- 과제 목표

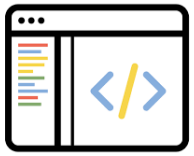
네트 워크 상에서 전달되는 TCP/IP 패킷을 캡처하고,
대상 프로토콜의 네트워크 계층부터 응용 계층의 페이로드까지
상향식 순차 분석하는 프로그램 개발

- 대상 프로토콜 3종

대상 프로토콜	링크 계층	네트워크 계층	전송 계층	응용 계층	응용 계층 페이로드
1. HTTP	Ethernet	IP	TCP	HTTP	HTTP 페이로드
2. DNS	Ethernet	IP	UDP	DNS	DNS 페이로드
3. icmp	Ethernet	IP/icmp	-	-	IP 내용 일부

Virtual Box

Wire Shark



raw socket

http, https, DNS, icmp

Web Server
210.93.48.51

Windows PC

DNS Server
210.93.48.196

VM Ware
WorkStation
[가상 머신]

우분투
[OS]

Linux gcc
[컴파일러]

http://

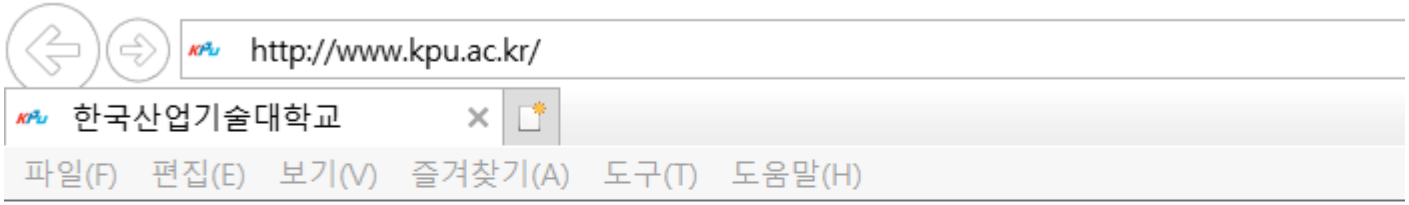
HTTP

https://

HTTPS

DNS

icmp



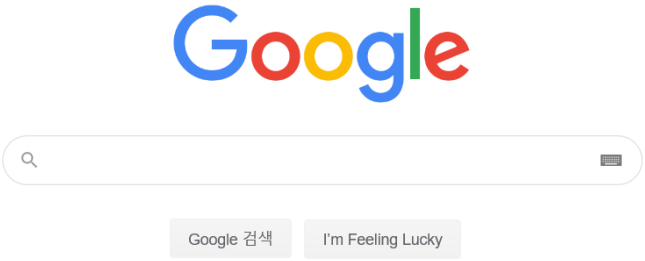
기업을 품는 산학융합 선도대학
KPU 한국산업기술대학교

시나리오

http://

HTTP

1. www.kpu.ac.kr 웹 서버 주소를 사용한다. (210.93.48.51)
2. 웹 브라우저는 우분투의 기본 브라우저를 사용한다. (VM Ware)
3. 패킷 캡처 후에 IP 헤더 정보, TCP 헤더 정보, HTTP의 Payload를 분석 한다.

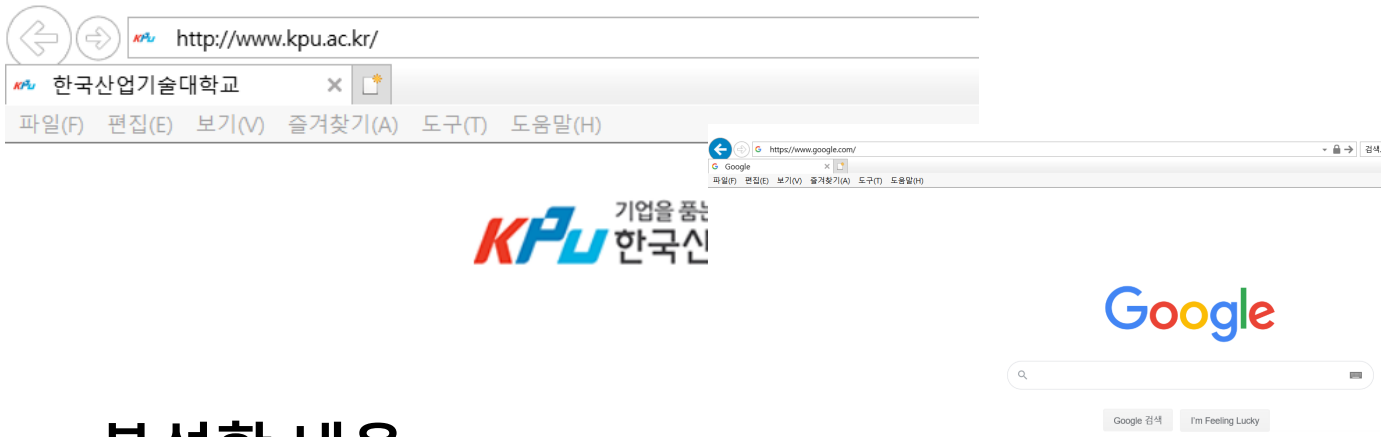


시나리오

https://

HTTPS

1. www.google.com의 웹 서버 주소를 사용한다. (172.217.25.68)
2. 웹 브라우저는 우분투의 기본 브라우저를 사용한다. (VM Ware)
3. 패킷 캡처 후에 IP 헤더 정보, TCP 헤더 정보, HTTPS의 Payload를 분석 한다.



분석할 내용

http://

https://

HTTP / HTTPS

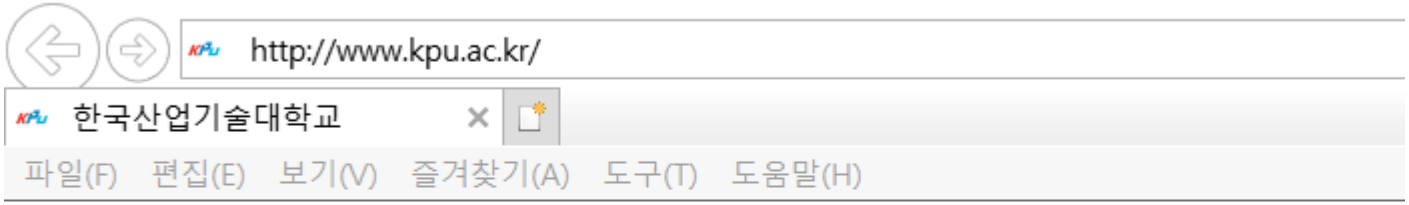
IP 헤더

- 출발지 IP 주소
- 목적지 IP주소
- IP 버전
- IP 헤더 길이
- 서비스 타입
- IP 전체 길이
- Time To Live
- 프로토콜 번호
- 체크섬

TCP헤더

- 출발지 포트번호
- 도착지 포트번호
- sequence Number
- acknowledge Number
- TCP 헤더 길이
- acknowledge flag
- Finish Flag
- 체크섬

Payload

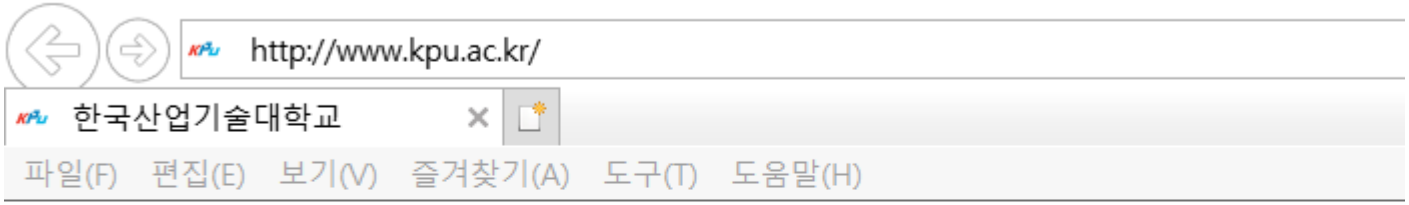


기업을 품는 산학융합 선도대학 한국산업기술대학교

DNS

시나리오

1. ns.kpu.ac.kr 의 주소를 사용한다. (210.93.48.196)
2. nslookup 명령어를 사용 한다.
3. 해당 도메인 또는 IP 주소를 얻는다.
4. 패킷 캡처 후에 IP 헤더 정보, UDP 헤더 정보, DNS의 Payload를 분석 한다.
5. 다른 DNS 주소 3~4개를 찾아 분석한다



기업을 품는 산학융합 선도대학 한국산업기술대학교

분석할 내용

DNS

IP 헤더

- 출발지 IP 주소
- 목적지 IP주소
- IP 버전
- IP 헤더 길이
- 서비스 타입
- IP 전체 길이
- Time To Live
- 프로토콜 번호
- 체크섬

UDP 헤더

- 출발지 포트번호
- 도착지 포트번호
- UDP 헤더 길이
- 체크섬

Payload

시나리오

1. VM Ware에서 ping 명령어를 실행 한다.
2. 사용할 주소는 www.google.com이다.
3. 패킷 캡처 후에 IP 헤더 정보, ICMP 헤더 정보, IP 내용 일부를 분석한다.

icmp

분석할 내용

icmp

IP 헤더

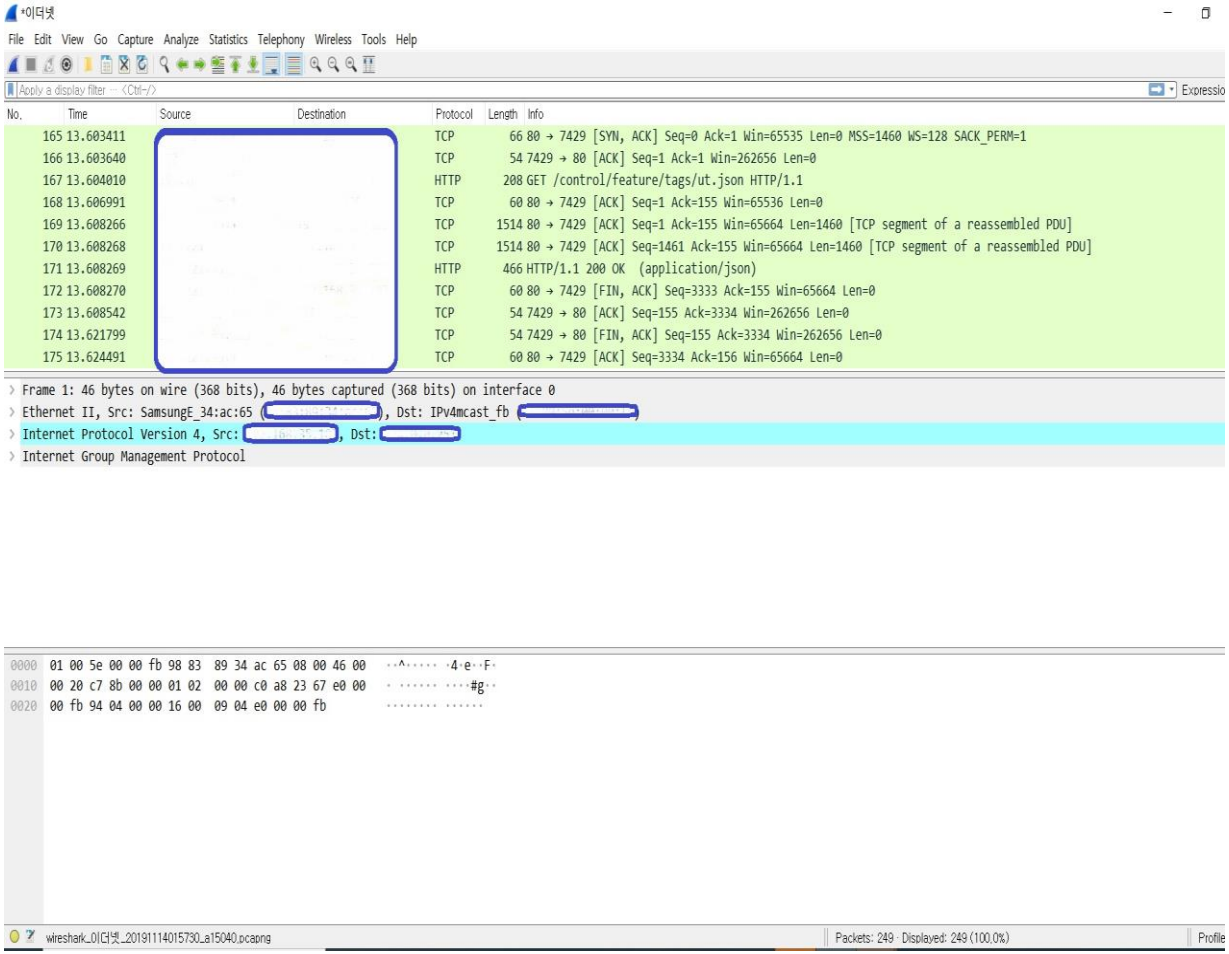
- 출발지 IP 주소
- 목적지 IP주소
- IP 버전
- IP 헤더 길이
- 서비스 타입
- IP 전체 길이
- Time To Live
- 프로토콜 번호
- 체크섬

ICMP 헤더

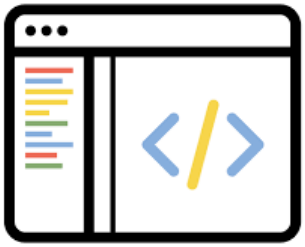
- ICMP 타입
- ICMP 코드
- 체크섬
- (응답의 경우)응답시간

IP 내용 일부

Wire Shark


*이더넷
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
165 13.603411 TCP 66 80 → 7429 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
166 13.603640 TCP 54 7429 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
167 13.604010 HTTP 208 GET /control/feature/tags/ut.json HTTP/1.1
168 13.606991 TCP 60 80 → 7429 [ACK] Seq=1 Ack=155 Win=65536 Len=0
169 13.608266 TCP 1514 80 → 7429 [ACK] Seq=1 Ack=155 Win=65664 Len=1460 [TCP segment of a reassembled PDU]
170 13.608268 TCP 1514 80 → 7429 [ACK] Seq=1461 Ack=155 Win=65664 Len=1460 [TCP segment of a reassembled PDU]
171 13.608269 HTTP 466 HTTP/1.1 200 OK (application/json)
172 13.608270 TCP 60 80 → 7429 [FIN, ACK] Seq=3333 Ack=155 Win=65664 Len=0
173 13.608542 TCP 54 7429 → 80 [ACK] Seq=155 Ack=3334 Win=262656 Len=0
174 13.621799 TCP 54 7429 → 80 [FIN, ACK] Seq=155 Ack=3334 Win=262656 Len=0
175 13.624491 TCP 60 80 → 7429 [ACK] Seq=3334 Ack=156 Win=65664 Len=0
Frame 1: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface 0
Ethernet II, Src: SamsungE_34:ac:65
, Dst: IPv4mcast_fb
Internet Protocol Version 4, Src:
, Dst:
Internet Group Management Protocol
0000 01 00 5e 00 00 fb 98 83 89 34 ac 65 08 00 46 00
0010 00 20 c7 8b 00 00 01 02 00 00 c0 a8 23 67 e0 00
0020 00 fb 94 04 00 00 16 00 09 04 e0 00 00 fb
wireshark_0이더넷_20191114015730_a15040.pcapng
Packets: 249 · Displayed: 249 (100.0%)
Profile

프로그램 구현 절차

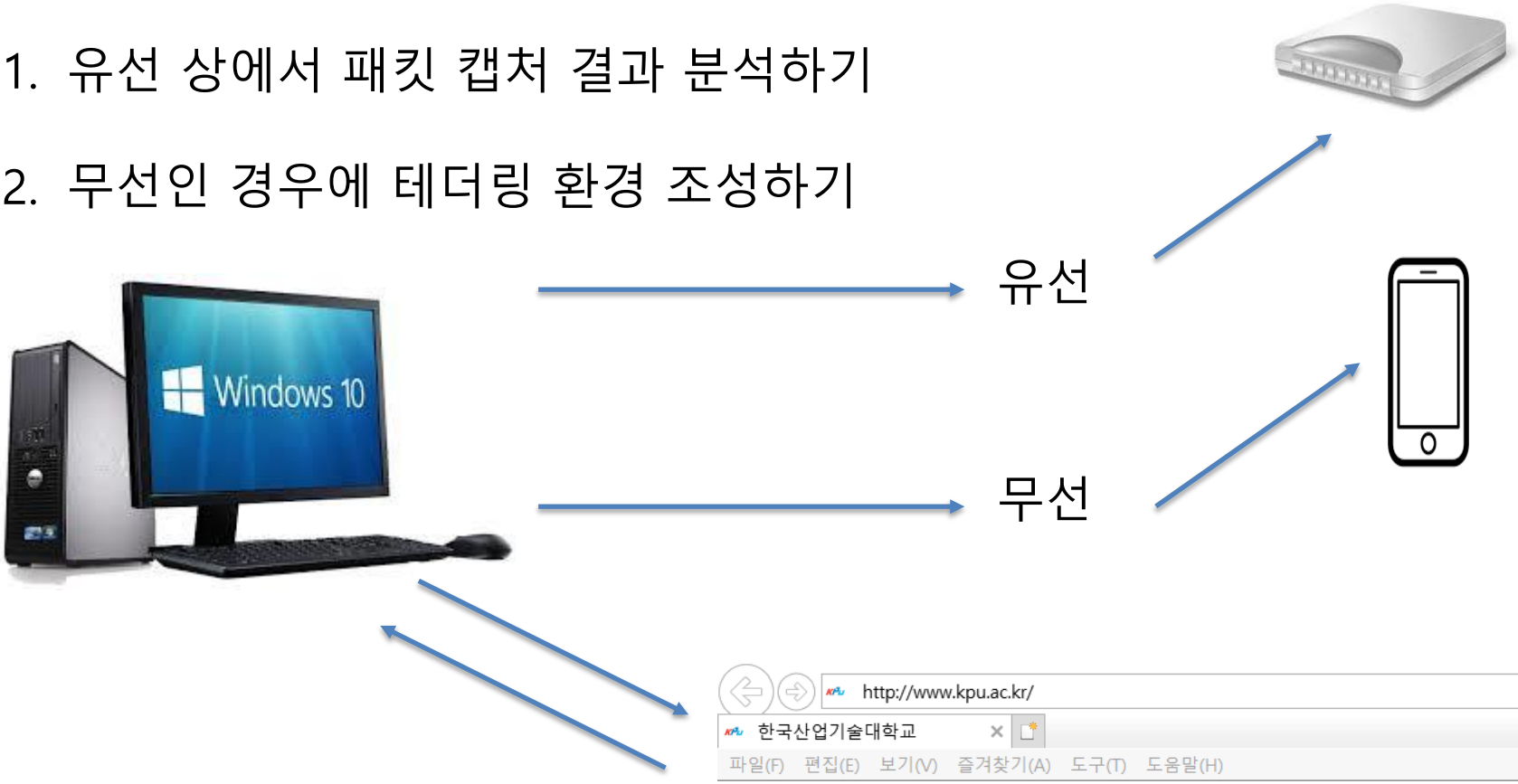


raw socket

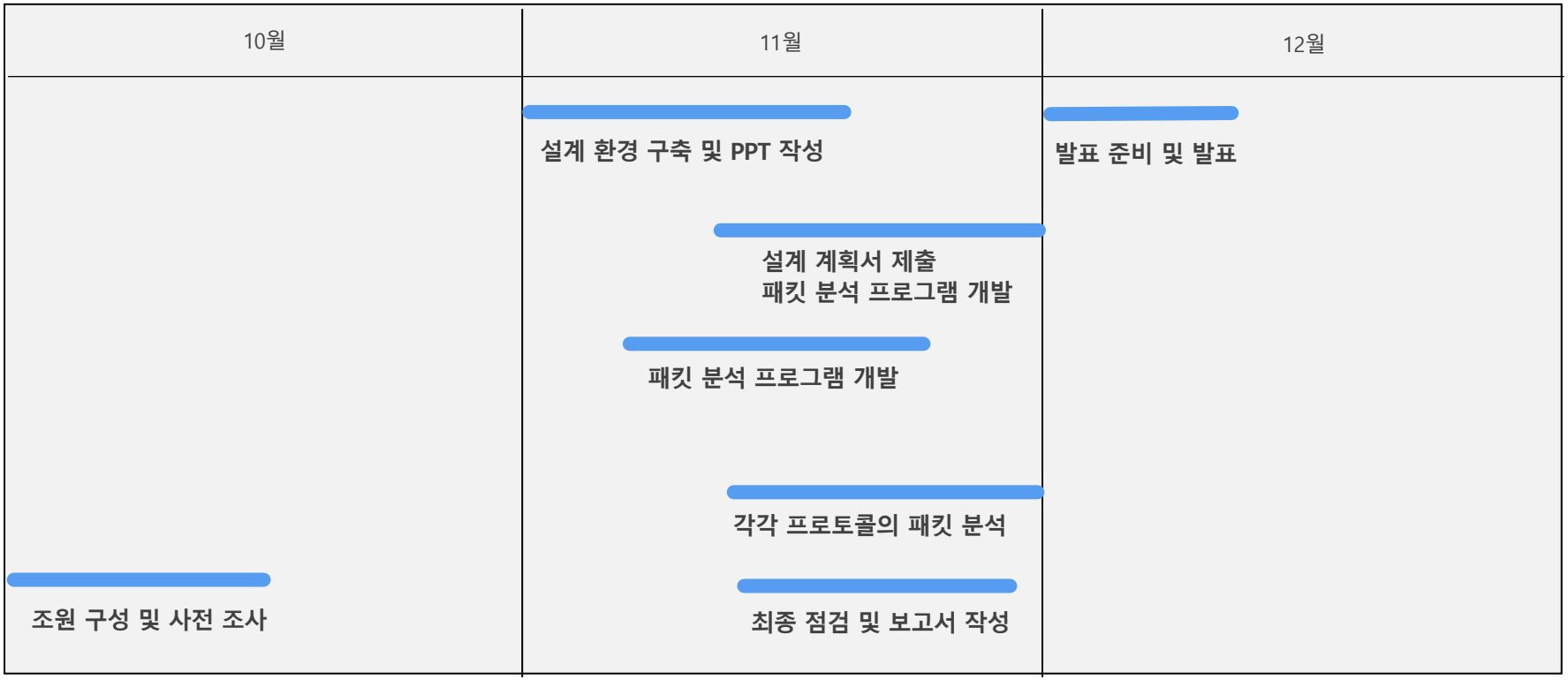
1. raw socket을 생성 한다.
2. Recvfrom() 루프 문을 실행하여 메시지를 수신한다.
3. ProcessPacket() 메소드로 분석하고 호출한다.
4. 각 프로토콜 별로 포인터를 이동 시키고, 그 값들을 읽는다.
5. 로그 파일로 만들어서 캡처 내용을 저장한다.

유, 무선에서 구현 방향

1. 유선 상에서 패킷 캡처 결과 분석하기
2. 무선인 경우에 테더링 환경 조성하기



04 추진 일정


10월
11월
12월
설계 환경 구축 및 PPT 작성
발표 준비 및 발표
설계 계획서 제출
패킷 분석 프로그램 개발
패킷 분석 프로그램 개발
각각 프로토콜의 패킷 분석
조원 구성 및 사전 조사
최종 점검 및 보고서 작성

예상 위험 요소

- 윈도우 환경에서 리눅스 환경으로 전환될 때 패킷 손실이 발생한다.

- 패킷 캡처 시 HTTP/1.1 302 Found (Redirection)가 발생한다.

- Wire Shark를 실행하는 것에 있어서 미숙함으로 인한 불필요한 정보들을 얻을 수 있다.

재설정이 발생하는 이유

1. 한쪽에 있는 TCP가 존재하지 않는 포트에 대해 연결 요청을 받은 경우
2. 한쪽 TCP가 비정상적인 상황 때문에 연결 중지를 원할 경우 (이 이유에 해당)
3. 한쪽에 있는 TCP가 다른 쪽에 있는 TCP가 오랫동안 유휴 상태인 것을 발견할 경우

해결 방안

- 패킷 손실 발생 시 VM Ware의 대역폭을 조절하여 해결할 수 있다.

- 호출하는 쪽에서 새로운 URL로 redirect처리를 해줘야 한다.

- 조원들 간의 그룹 Study를 통한 Wire Shark 사용 방법을 숙지한다.

한승우

PPT 작성
분석 프로그램
개발

김지우

설계 환경 구축
분석 프로그램
개발

전유미

PPT 작성
분석 프로그램
개발

정하림

설계 환경 구축
분석 프로그램
개발

- 여러 가지 네트워크 패킷 캡처 및 분석 가능
- 분석된 패킷의 구조와 내용을 한 눈에 확인 가능
- 프로토콜에서 사용하는 여러 가지 명령어 습득
- 네트워크 과목에 대한 이해도 향상
- 네트워크 프로그래밍 실력 향상
- 네트워크 보안에 대한 관심도 증가

Q & A

2019-2
컴퓨터
네트워크

감사합니다