COMPUTER NETWORK

컴퓨터 네트워크 패킷 캡처 프로그램 설계계획서

작성일: 2020-11-11

학과	이름
소프트웨어학과	최한규
소프트웨어학과	김영민
소프트웨어학과	이형석
소프트웨어학과	황규빈

컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-

패킷 캡쳐 프로그램이란?

1. 패킷이란?
2. 패킷 캡쳐 프로그램이란?

설계할 패킷 캡처 프로그램의 목표

1. 설계 목표
2. 설계 가이드

컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-

패킷 캡쳐 프로그램이란?

1. 패킷이란?

네트워크 전송의 용량 단위로서, 전송될 때 서로 교환되는 실제의 내용물

조각조각 분할된 파일 데이터에 주소와 에러 데이터 등이 기록

2. 패킷 캡쳐 프로그램이란?

네트워크에서 이동하는 패킷을 수집하고 분석하도록 도와주는 프로그램.

수집, 변환, 분석의 절차를 통해 네트워크 데이터의 프로토콜을 검증하고, 프로토콜의 특징과 내용을 분석함

설계할 패킷 캡쳐 프로그램의 목표

1. 설계 목표

"TCP/IP 프로토콜 스택 구조 기반으로, HTTP, DNS, ICMP 등의 애플리케이션 계층에서 상호 통신하는 서버와 클라이언트 간에 송수신되는 패킷을 수집, 분석 및 표시하는 패킷 캡처 프로그램 구현"
> 저희 팀만의 색으로 구현할 예정

2. 설계 가이드

- 패킷 캡처 및 저장 기능
- 수집 패킷 분석 기능
- 개발 프로그래밍 언어
- 구현된 패킷 캡처 소스를 도입하여 활용하는 경우

설계 방향

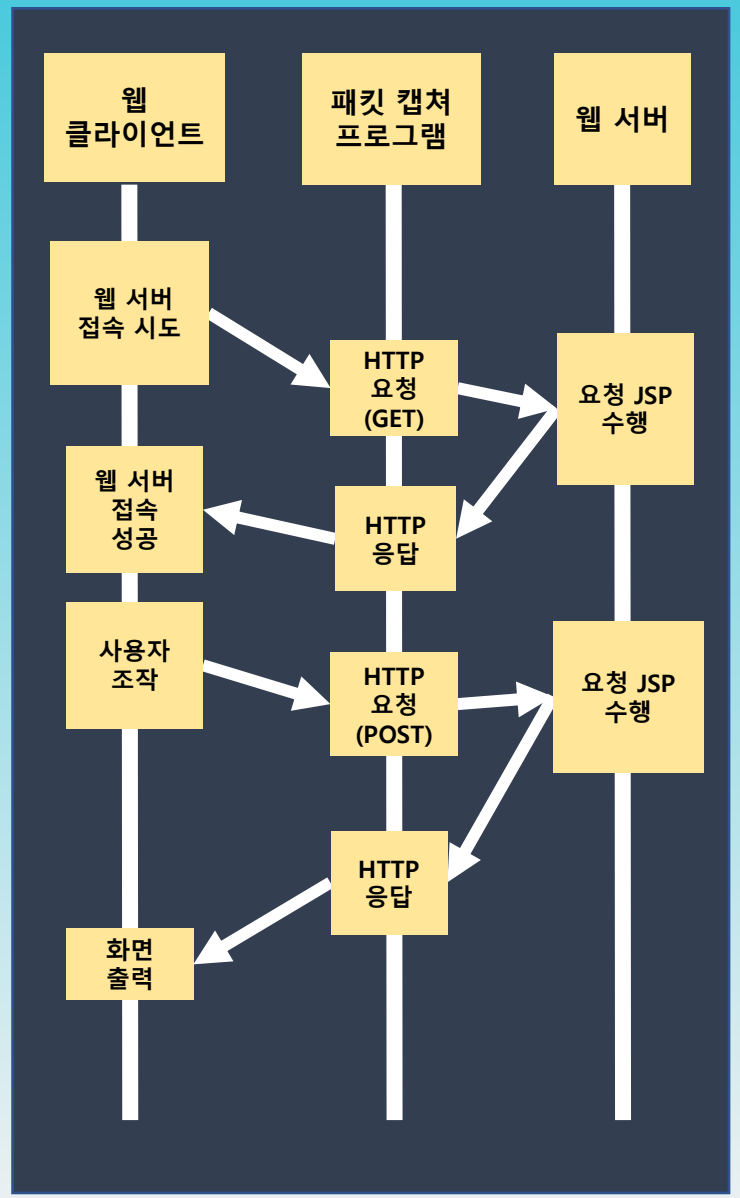
프로토콜별 패킷 캡쳐 수행 동작도

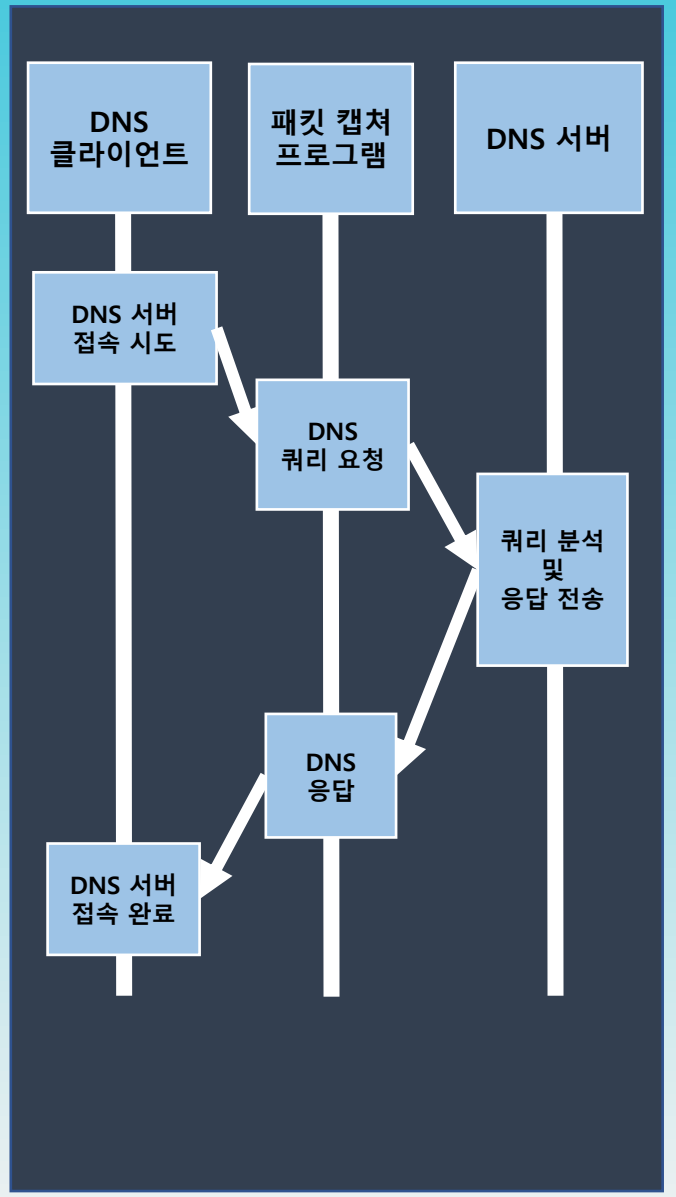
(1) HTTP

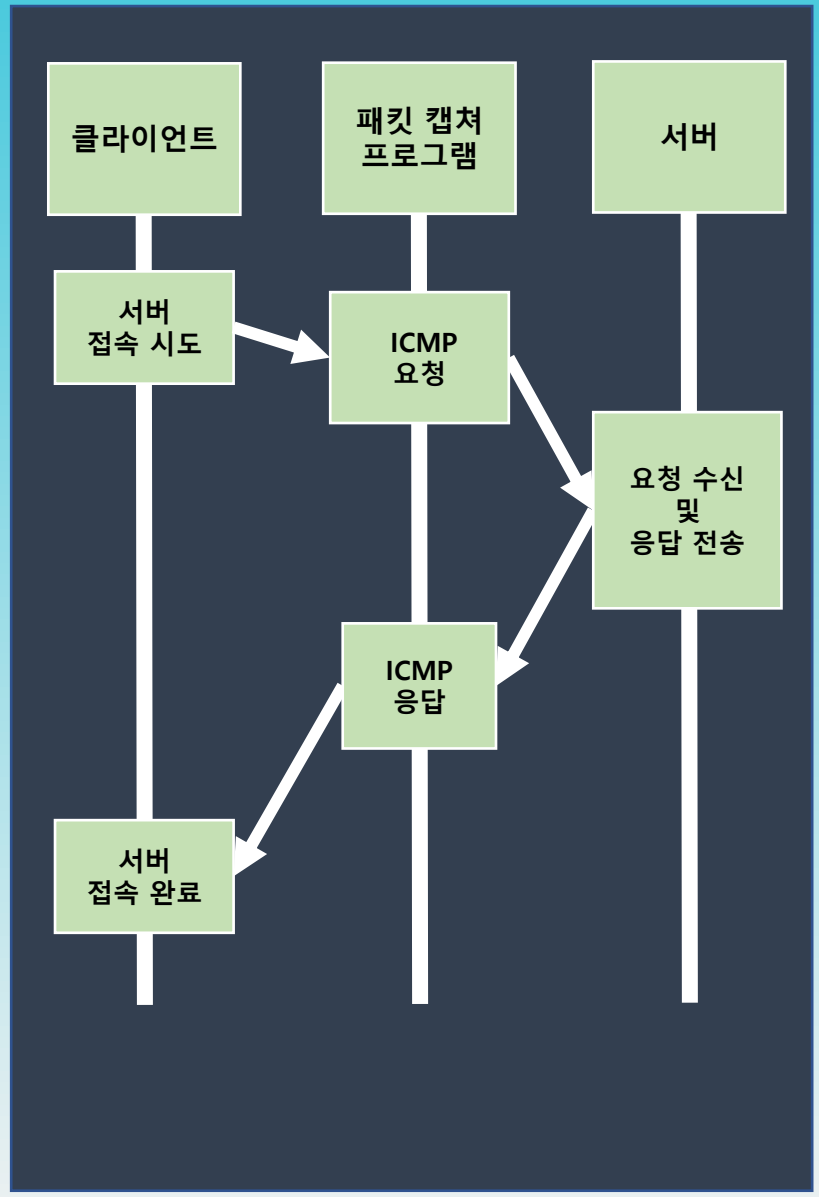
(2) DNS

(3) ICMP

컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-







컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-

HTTP 프로토콜

1. HTTP 프로토콜
2. HTTP 프로토콜 패킷 수집
3. HTTP 프로토콜 패킷 분석
4. HTTP 프로토콜 요청/응답

DNS 프로토콜

1. DNS 프로토콜
2. DNS 프로토콜 패킷 수집
3. DNS 프로토콜 패킷 분석
4. DNS 프로토콜 쿼리/응답 과정

Raw Socket

1. RAW 소켓이란
2. Root 계정으로만
   Raw 소켓을 만들 수 있는 이유
1. 패킷 수집 방법
2. 패킷 수집 절차

컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-

HTTP 프로토콜

1) 인터넷에서 데이터를 주고받을 수 있는 프로토콜

2) 클라이언트가 url을 통해 요청을 하면 서버가 요청 사항에 맞는 응답을 통해 동작

3) 연결 상태가 유지되지 않는 비 연결성 프로토콜이고, 이 점을 보완하기 위해 쿠키와 세션이 추가됨

4) 포트는 80번을 사용하고 요청시에 요청 메소드를 사용, 응답시에 응답 코드와 함께 돌아온다.

```
HTTP/1.1 304 Not Modified
Date: Wed, 11 Nov 2020 16:39:15 GMT
```

HTTP 프로토콜 패킷 수집

1) 수집할 HTTP 패킷을 필터링 하기 위해 80번 포트를 사용하는 패킷으로 필터링

2) 클라이언트에서 요청을 보낸 패킷에 대한 응답 패킷을 시간 순서에 맞게 출력

3) 해당 패킷의 IP, 시간, 패킷 내용 표시하고 요청 패킷의 경우 상태 코드 표시

컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-

HTTP 프로토콜 패킷 분석

1) 요청 메시지
-> 요청 라인과 헤더라인으로 구성
-> 요청 라인은 메소드 (GET, POST), URL, HTTP 버전(HTTP/1.1)로 구성
-> 헤더 라인은 connection, user-agent, Accept language 로 구성

2) 응답 메시지
-> 상태 라인, 헤더라인, 바디로 나뉘어짐
-> 상태 라인은 버전 필드와 상태 코드로 구성
-> 헤더라인은 Connection, Date, Server, Last-Modified, Content-Length, Content-Type으로 구성

HTTP 프로토콜 요청/응답

컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-

DNS 프로토콜

1) 호스트의 도메인 이름을 호스트의 네트워크 주소를 변환시켜주는 프로토콜

2) DNS는 UDP나 TCP를 통해 실행하며 주로 UDP 사용

3) 일반적으로 UDP를 이용하는 DNS 쿼리 패킷과 응답 패킷을 확인한다.

4) 53번 포트를 사용하며, 여러가지 계층 구조로 이루어져 있다.

DNS 프로토콜 패킷 수집

1) 수집할 DNS 패킷을 필터링하기 위해 UDP로 통신하며 53번 port를 사용한 패킷으로 필터링

2) 수집한 DNS 패킷을 수집된 시간으로 정렬

3) 해당 패킷의 IP, 시간, 패킷 내용 표시

컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-

DNS 프로토콜 패킷 분석

1) DNS 쿼리 패킷
   -> 클라이언트가 DNS를 요청하는 패킷
   -> Query name string , Type, class로 구성

2) DNS 응답 패킷
   -> 쿼리 패킷과는 달리 요청지와 목적지가 바뀐다.
   -> 헤더, 질의, 응답, 책임, 부가 정보 이렇게 5가지의 데이터로 구성
   -> 질의 메시지와는 동일한 포맷으로 구성되어 있으나 쿼리 메시지와는 다른 응답, 책임, 부가 정보는 RR 포맷 형식으로 묶여 구성

3) ㄴㅇㄹ

DNS 프로토콜 쿼리/응답 과정

클라이언트가 호스트의 IP 주소를 얻기 위해 DNS 서버에 쿼리를 전송한다.

```
[Response In: 23]
Transaction ID: 0x0c9d
⊞ Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
```

DNS 서버는 정보에 대해 응답하거나 다른 DNS 서버에 요청을 한다.

```
[Request In: 22]
[Time: 0.004097000 seconds]
Transaction ID: 0x0c9d
⊞ Flags: 0x8180 (Standard query response, No error)
Questions: 1
Answer RRs: 7
Authority RRs: 0
Additional RRs: 0
```

컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-

ICMP 프로토콜

1) 인터넷/통신 상에서 발생한 일반적인 상황에 대한 보고

2) IP 프로토콜을 이용하여 ICMP 메시지 전달

3) 네트워크 계층에 속하여 네트워크 관리 프로토콜의 역할 수행

ICMP 프로토콜 패킷 수집

1) IP 헤더 다음에 오는 유형, 코드, 체크섬으로 구성돼 있다.

2) type : ICMP 패킷의 용도(제어, 에러)를 구분하여 출력

3) code : Type의 세부 내용을 나타내며 목적과 용도를 출력

4) 체크섬 : ICMP 메시지의 이상 유무를 판단하는 내용 출력

5) ICMP 메시지 내용 출력

컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-

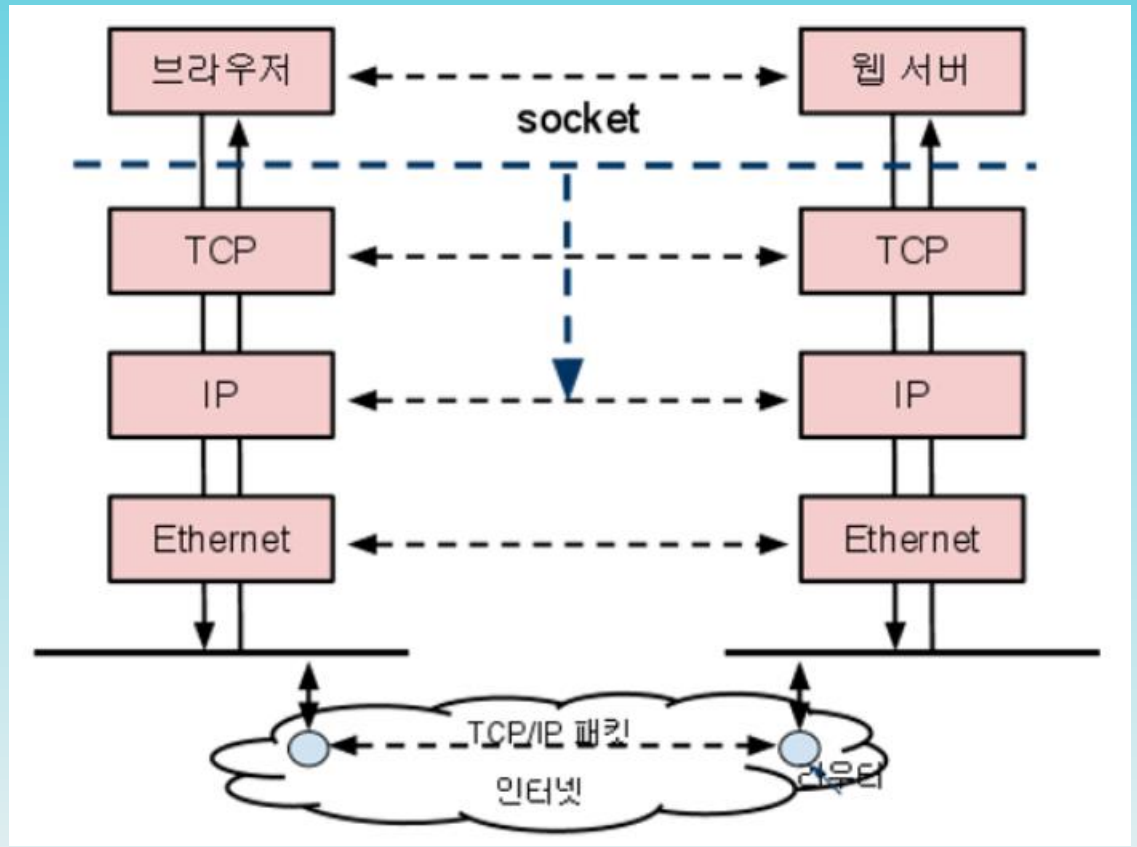
RAW 소켓이란

1) 어느 특정한 프로토콜 용의 전송 계층 포맷팅 없이 인터넷 프로토콜 패킷을 직접적으로 주고 받게 해주는 소켓

2) 각 4계층의 헤더 정보들에 대해 프로그래머가 직접 제어할 수 있게 해준다.

3) 사용자 데이터 취급을 받기 때문에 여러 계층으로 접근이 가능하다.

4) Root 계정으로만 사용 가능하다.



컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-

Root 계정으로만 Raw 소켓을 만들 수 있는 이유

RAW 소켓을 구현하기 위해서는 TCP/IP 스택을 제어해야 하는데 TCP/IP 스택을 제공하는 곳이 커널이므로 커널에 접근 가능한 root 계정으로만 RAW 소켓 생성이 가능하다.

컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-

패킷 수집 방법

1. socket() 함수를 이용하여 소켓 생성

- 두 번째 인자(type)을 SOCK_RAW로 지정
- 세 번째 인자(protocol)을 IPPROTO_RAW나 htons(ETH_P_ALL)로 지정

ex) raw_sock = socket(AF_INET, SOCK_RAW, IPPROTO_RAW)

2. setsockopt() 함수로 직접 헤더의 값을 지정할 수 있도록 소켓의 옵션 변경

ex) setsockopt(raw_sock, IPPROTO_IP, IP_HDRINCL, (char*)&value, sizeof(value))

3. 구조체의 값을 채우고 필터링

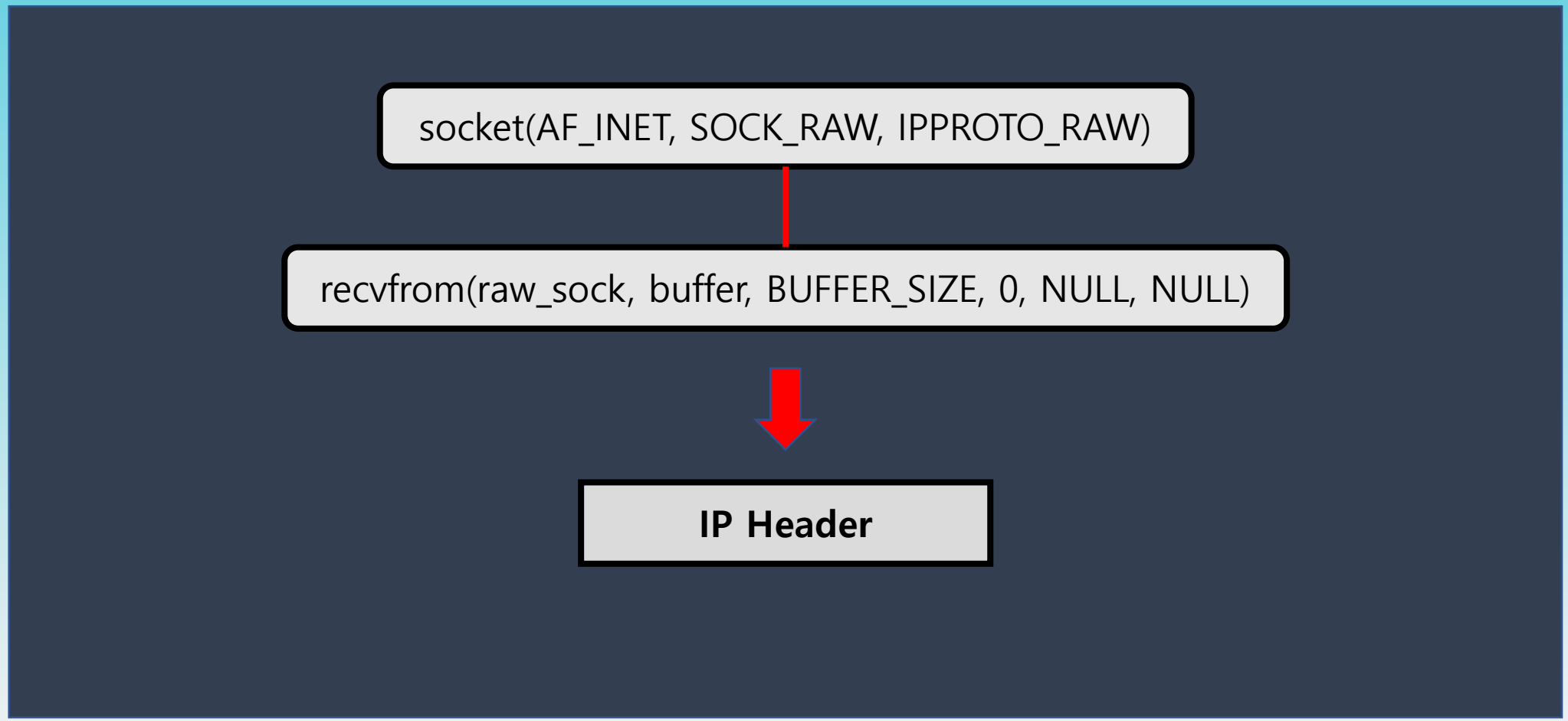
IP Header 구조체의 값을 직접 채운다.

TCP Header 구조체의 값을 직접 채운다.
- 수집한 패킷이 HTTP인지 필터링 한다.

UDP Header 구조체의 값을 직접 채운다.
- 수집한 패킷이 DNS인지 필터링 한다.
- 수집한 패킷이 ICMP인지 필터링 한다.

컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-

패킷 수집 절차



컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-

개발 환경 – 우분투 16v 64bit

개발 에디터

Leafpad : GPL 라이선스로 작성된 무료 소프트웨어로 약 100KB의 초소형 용량의 단순한 GUI 텍스트 편집기이다.

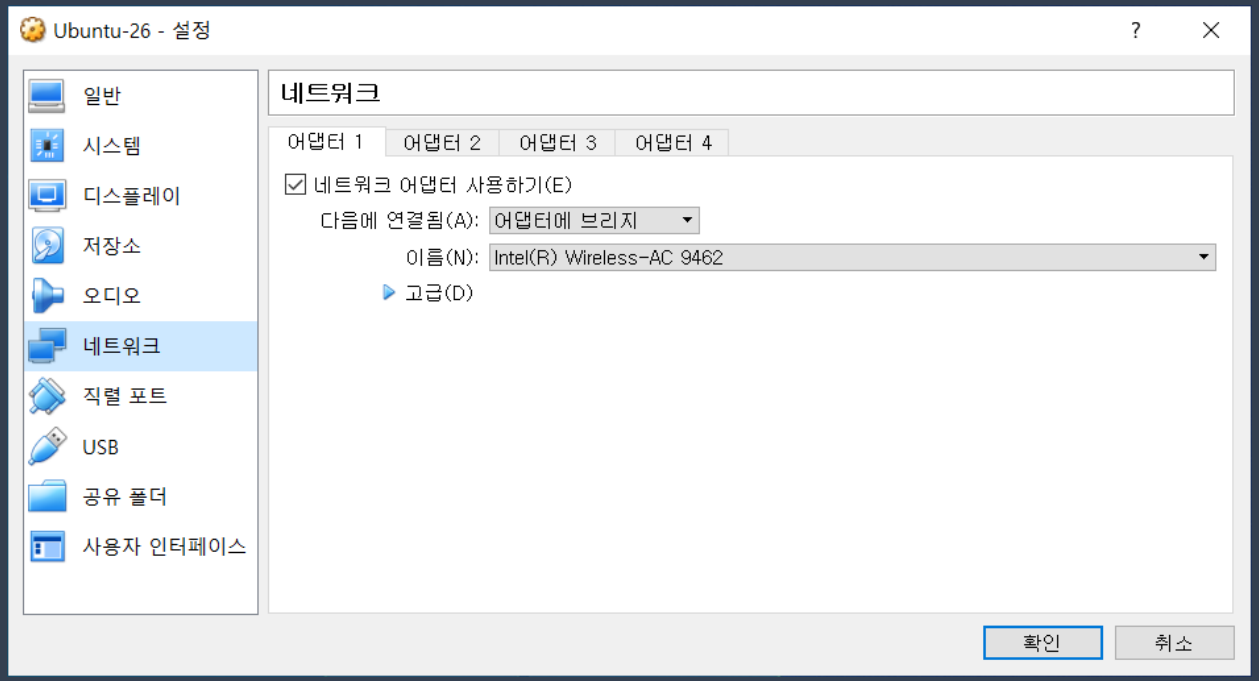
컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-

설계 환경 – 우분투 16v 64bit

네트워크 설정

어댑터에 브릿지 :

가상머신이 독립적인 네트워크 IP를 가지게 된다.



컴퓨터 네트워크 설계 과제 – 2차 과제 : 패킷 캡처 프로그램 설계계획서-

패킷 수집

패킷 수집 구조