Pcap Programming

2018-07-16 Jinyan*김상민

삽질만하는 네트워크 뉴비

Content

```
1
Pcap?

Libpacp?

Libpacp API
```



Pcap

Pcap (Packet Capture)

- 네트워크상에서 돌아다니는 패킷을 들여다 보는것

Pcap 응용

- Network Traffic Monitoring, Network Debugging



LibPcap

LibPcap (Portable Pocket Capturing Library)

- Libpcap는 간단하게 패킷을 캡쳐하기 위한 함수 모음

Pcap 응용

-BPF에 기초하는 필터링을 지원하고 있음



LibPcap Programming

Device&Network information

- int pcap_lookupnet()

```
int pcap_lookupnet(char *device, bpf_u_int32 *netp, bpf_u_int32 *maksp, char *errbuf)
```

- char* pcap_lookupdev
- Pcap_datalink

int pcap_datalink(pcap_t *p)



LibPcap Programming

Device&Network information

- int pcap_lookupnet()

```
int pcap_lookupnet(char *device, bpf_u_int32 *netp, bpf_u_int32 *maksp, char *errbuf)
```

- char* pcap_lookupdev
- Pcap_datalink

int pcap_datalink(pcap_t *p)



LibPcap Programming

Pcatp initaliztaion API

- pcap_t*pcap_open_live

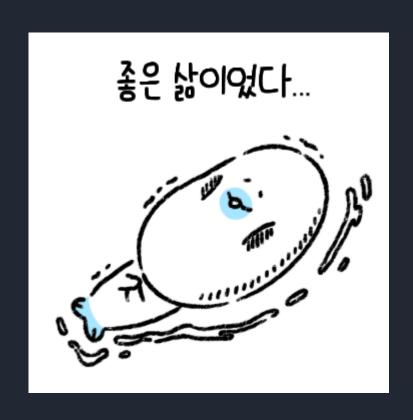
pcap_t *pcap_open_live(char *device, int snaplen, int promisc, int to_ms, char *ebuf)

pcap_t*pcap_open_offline

pcap_t *pcap_open_offline(char *fname, char *ebuf)



Next



- -실질적인 API
- -패킷 필터링 API
- -코드 짜서 실행하는거 발표
- -그 이후 시스템 공부