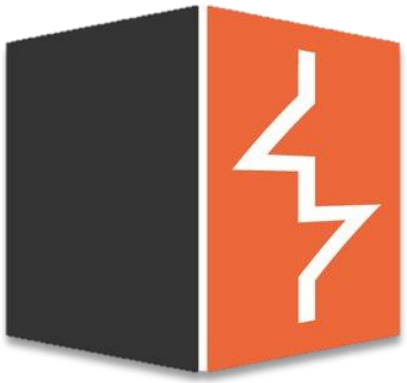
Netteok

최종 발표

김우종(PM)
문승재
서민재
이유경

Contents

1-1. 프로젝트 소개



Burp Suite

웹 패킷을 받아 변조할 수 있다.

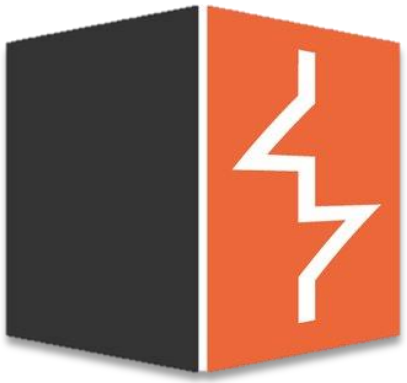
모든 패킷을 받아 확인할 수 없다.

WireShark

패킷에 대한 변조 기능이 없다.

모든 패킷을 받아 확인할 수 있다.

1-1. 프로젝트 소개



Burp Suite

기능 설명이 부족하다.

초심자가 사용하기 벅찬 많은 기능이 있다.

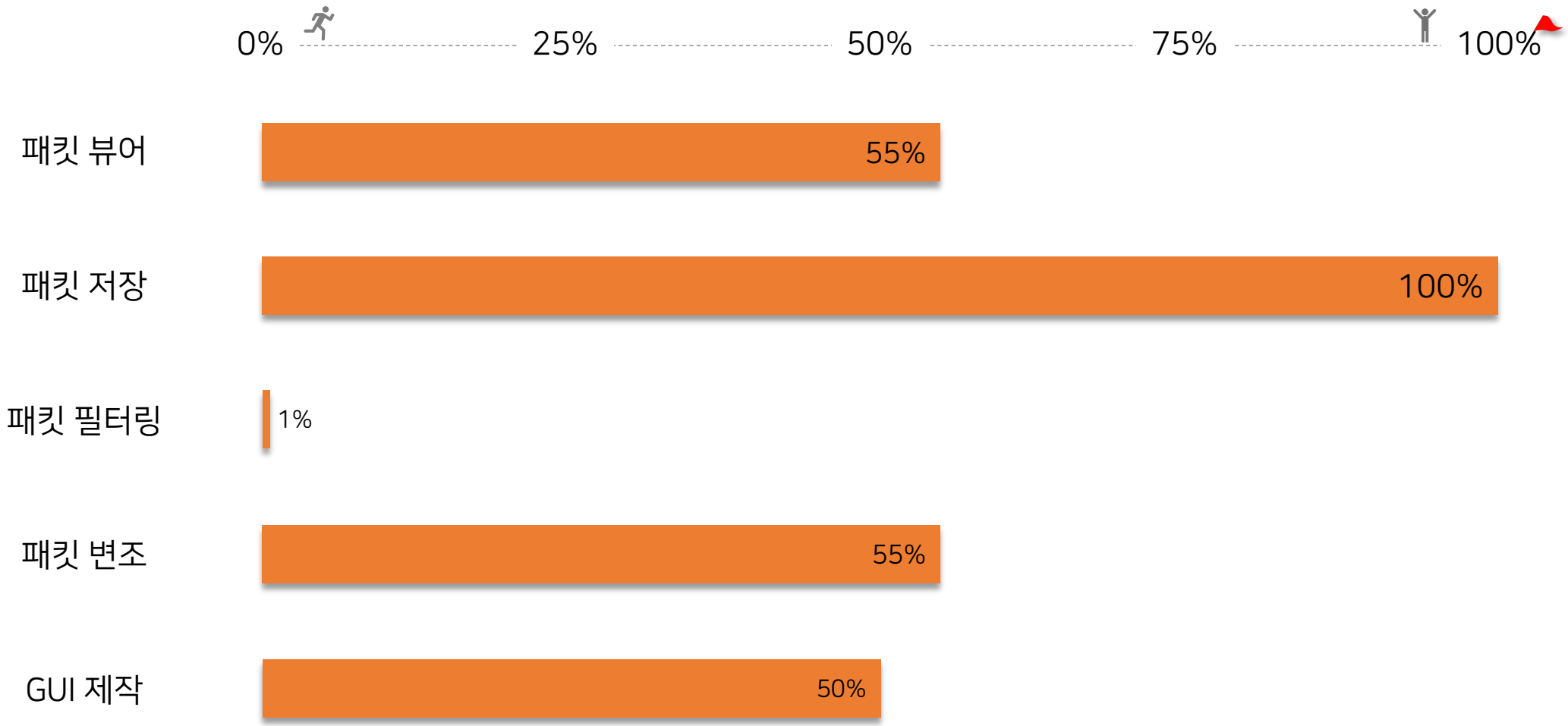
WireShark

네트워크 패킷 필드 구분이 직관적이지 않다.

1-2. 프로젝트 수행 절차

기획 및 설계	분석 및 개발	성과
네트워크 도구 불편함 인식 네트워크 도구 개발 선정	운영체제 분류	화면, 기능 명세서 작성 완료 목표 도구 개발 미완성
툴 사용자 선정 방향 수립 분석 방향 수립	Protocol 분석 Pcap 파일 분석 변조 과정 분석	
개발 자료 조사 및 수집	GUI 모듈 설계 모듈 개발	

1-3. 프로젝트 완성도



2-1. 기획 및 설계

운영체제

Windows 10

개발 언어

Python3.8.3

인터페이스

GUI (pyQt5)

2-1. 기획 및 설계

패킷 뷰어

- 받은 패킷들을 리스트 화
- 각 패킷에 대한 디테일한 내용 출력
- 패킷들을 Hex와 Binary 값으로 표현

패킷 변조

2-1. 기획 및 설계

패킷 변조

- IP주소와 포트 번호를 입력 받아 프록시로 통신
- 클라이언트가 전송한 데이터를 프록시에서 받아, 프로그램에 Raw값과 Hex값으로 표현
- 프록시와 서버를 연결하여 변조한 데이터를 전송

인터페이스

2-1. 기획 및 설계

인터페이스

- 초심자를 위한 GUI
- 직관적인 시각적 효과

추가 기능

2-2. 분석 (Protocol)

TCP / IP 4계층	Protocol
Application Layer	Telnet / FTP / HTTP / SMTP
Transport Layer	TCP / UDP
Internet Layer	ICMP / ARP / RARP / IP
Network Interface	물리적 연결 구성

2-2. 분석 (Ethernet)

```
0000  00 1a 1e 01 42 e8 3c f0  11 27 f7 63 08 00 45 00   ····B·<· ·'·c··E·
0010  01 fd 16 2c 40 00 80 06  5e 78 ac 1f 05 3b af d5   ···,@··· ^x···;··
0020  23 27 c2 9c 00 50 3a c8  39 f3 b2 1d 2f cc 50 18   #'···P:· 9···/·P·
0030  02 02 a6 f4 00 00 47 45  54 20 2f 20 48 54 54 50   ····GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 74 65 73 74   /1.1··Ho st: test
0050  2e 67 69 6c 67 69 6c 2e  6e 65 74 0d 0a            .gilgil. net··
```

목적지 MAC 주소 [6byte]	출발지 MAC 주소 [6byte]	Ether Type [2byte]	DATA

Ethernet Header

2-2. 분석 (IP)

```
0000  00 1a 1e 01 42 e8 3c f0  11 27 f7 63 08 00 45 00   ····B·<· ·'·c··E·
0010  01 fd 16 2c 40 00 80 06  5e 78 ac 1f 05 3b af d5   ···,@··· ^x···;··
0020  23 27 c2 9c 00 50 3a c8  39 f3 b2 1d 2f cc 50 18   #'···P:· 9···/·P·
0030  02 02 a6 f4 00 00 47 45  54 20 2f 20 48 54 54 50   ····GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 74 65 73 74   /1.1··Ho st: test
0050  2e 67 69 6c 67 69 6c 2e  6e 65 74 0d 0a            .gilgil. net··
```

VER	IHL	TOS	Total Length			
Identification			0	DF	MF	Fragment Offset
TTL		Protocol ID	Header Checksum			
Source IP						
Destination IP						
IP Option and Padding						

IP Header

2-2. 분석 (TCP)

```
0000  00 1a 1e 01 42 e8 3c f0  11 27 f7 63 08 00 45 00   ····B·<· ·'·c··E·
0010  01 fd 16 2c 40 00 80 06  5e 78 ac 1f 05 3b af d5   ···,@··· ^x···;··
0020  23 27 c2 9c 00 50 3a c8  39 f3 b2 1d 2f cc 50 18   #'···P:· 9···/·P·
0030  02 02 a6 f4 00 00 47 45  54 20 2f 20 48 54 54 50   ·····GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 74 65 73 74   /1.1··Ho st: test
0050  2e 67 69 6c 67 69 6c 2e  6e 65 74 0d 0a            .gilgil. net··
```

출발지 포트번호								목적지 포트번호
Sequence number								
Acknowledgement number								
HLEN	예약	URG	ACK	PSH	RST	SYN	FIN	Window size
Checksum								Urgent pointer
Options and Padding								

TCP Header

2-2. 분석 (HTTP)

```
0000  00 1a 1e 01 42 e8 3c f0  11 27 f7 63 08 00 45 00   ····B·<· ·'·c··E·
0010  01 fd 16 2c 40 00 80 06  5e 78 ac 1f 05 3b af d5   ···,@··· ^x···;··
0020  23 27 c2 9c 00 50 3a c8  39 f3 b2 1d 2f cc 50 18   #'···P:· 9···/·P·
0030  02 02 a6 f4 00 00 47 45  54 20 2f 20 48 54 54 50   ·····GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 74 65 73 74   /1.1··Ho st: test
0050  2e 67 69 6c 67 69 6c 2e  6e 65 74 0d 0a            .gilgil. net··
```

Request line
Header
₩n
Body

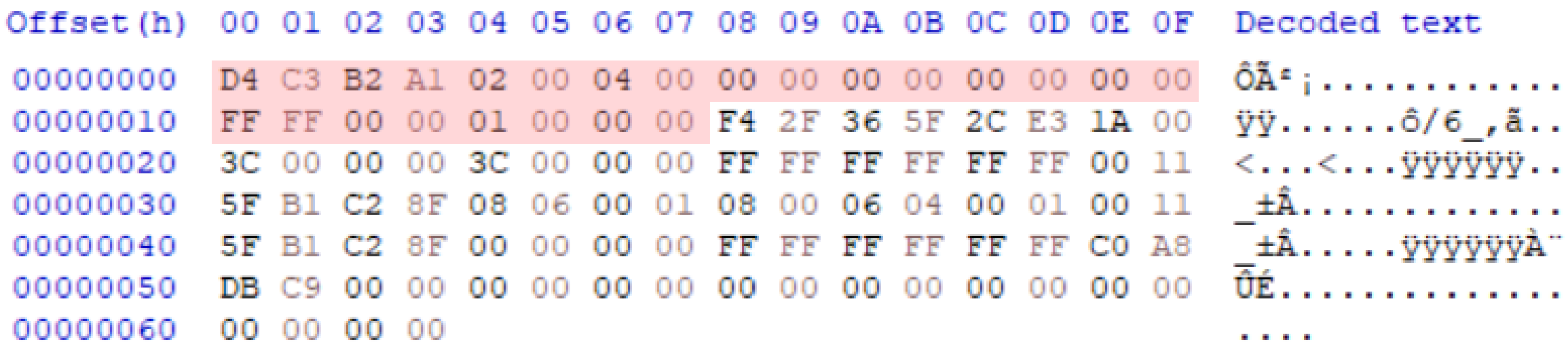
HTTP Header

2-2. Pcap 파일 분석

Global Header
Packet Header [0]
Packet data [0]
Packet Header [1]
Packet data [1]

Pcap 파일 구조

2-2. Pcap 파일 분석 (Global Header)



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	D4	C3	B2	A1	02	00	04	00	00	00	00	00	00	00	00	00	ÔÃ²¡.....
00000010	FF	FF	00	00	01	00	00	00	F4	2F	36	5F	2C	E3	1A	00	ÿÿ.....ô/6_,ã..
00000020	3C	00	00	00	3C	00	00	00	FF	FF	FF	FF	FF	FF	00	11	<...<...ÿÿÿÿÿÿ..
00000030	5F	B1	C2	8F	08	06	00	01	08	00	06	04	00	01	00	11	_±Â.....
00000040	5F	B1	C2	8F	00	00	00	00	FF	FF	FF	FF	FF	FF	C0	A8	_±Â.....ÿÿÿÿÿÿÀ¨
00000050	DB	C9	00	00	00	00	00	00	00	00	00	00	00	00	00	00	ÛÉ.....
00000060	00	00	00	00													....

Magic Number D4 C3 B2 A1	Major / Minor [4byte]	Time zone [4byte]	Time Stamps [4byte]
Snap Length [4byte]	Link Type [4byte]		

2-2. Pcap 파일 분석 (Packet Header)

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	D4	C3	B2	A1	02	00	04	00	00	00	00	00	00	00	00	00	ÔÃ²¡.....
00000010	FF	FF	00	00	01	00	00	00	F4	2F	36	5F	2C	E3	1A	00	ÿÿ.....ô/6_,ã..
00000020	3C	00	00	00	3C	00	00	00	FF	FF	FF	FF	FF	FF	00	11	<...<...ÿÿÿÿÿÿ..
00000030	5F	B1	C2	8F	08	06	00	01	08	00	06	04	00	01	00	11	_±Â.....
00000040	5F	B1	C2	8F	00	00	00	00	FF	FF	FF	FF	FF	FF	C0	A8	_±Â.....ÿÿÿÿÿÿÀ¨
00000050	DB	C9	00	00	00	00	00	00	00	00	00	00	00	00	00	00	ÛÉ.....
00000060	00	00	00	00													....

Time Stamp [8byte]	Capture Length [4byte]	Packet Length [4byte]

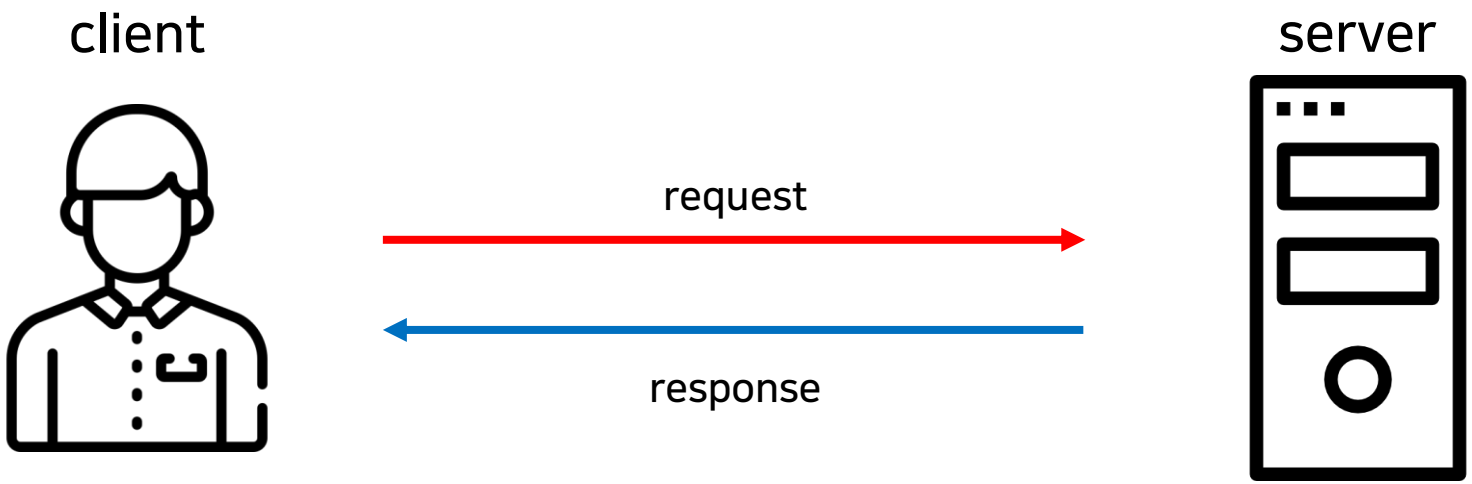
2-2. Pcap 파일 분석 (Packet data)

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	D4	C3	B2	A1	02	00	04	00	00	00	00	00	00	00	00	00	ÔÃ²¡.....
00000010	FF	FF	00	00	01	00	00	00	F4	2F	36	5F	2C	E3	1A	00	ÿÿ.....ô/6_,ã..
00000020	3C	00	00	00	3C	00	00	00	FF	FF	FF	FF	FF	FF	00	11	<...<...ÿÿÿÿÿÿ..
00000030	5F	B1	C2	8F	08	06	00	01	08	00	06	04	00	01	00	11	_±Â.....
00000040	5F	B1	C2	8F	00	00	00	00	FF	FF	FF	FF	FF	FF	C0	A8	_±Â.....ÿÿÿÿÿÿÀ¨
00000050	DB	C9	00	00	00	00	00	00	00	00	00	00	00	00	00	00	ÛÉ.....
00000060	00	00	00	00													....

Data

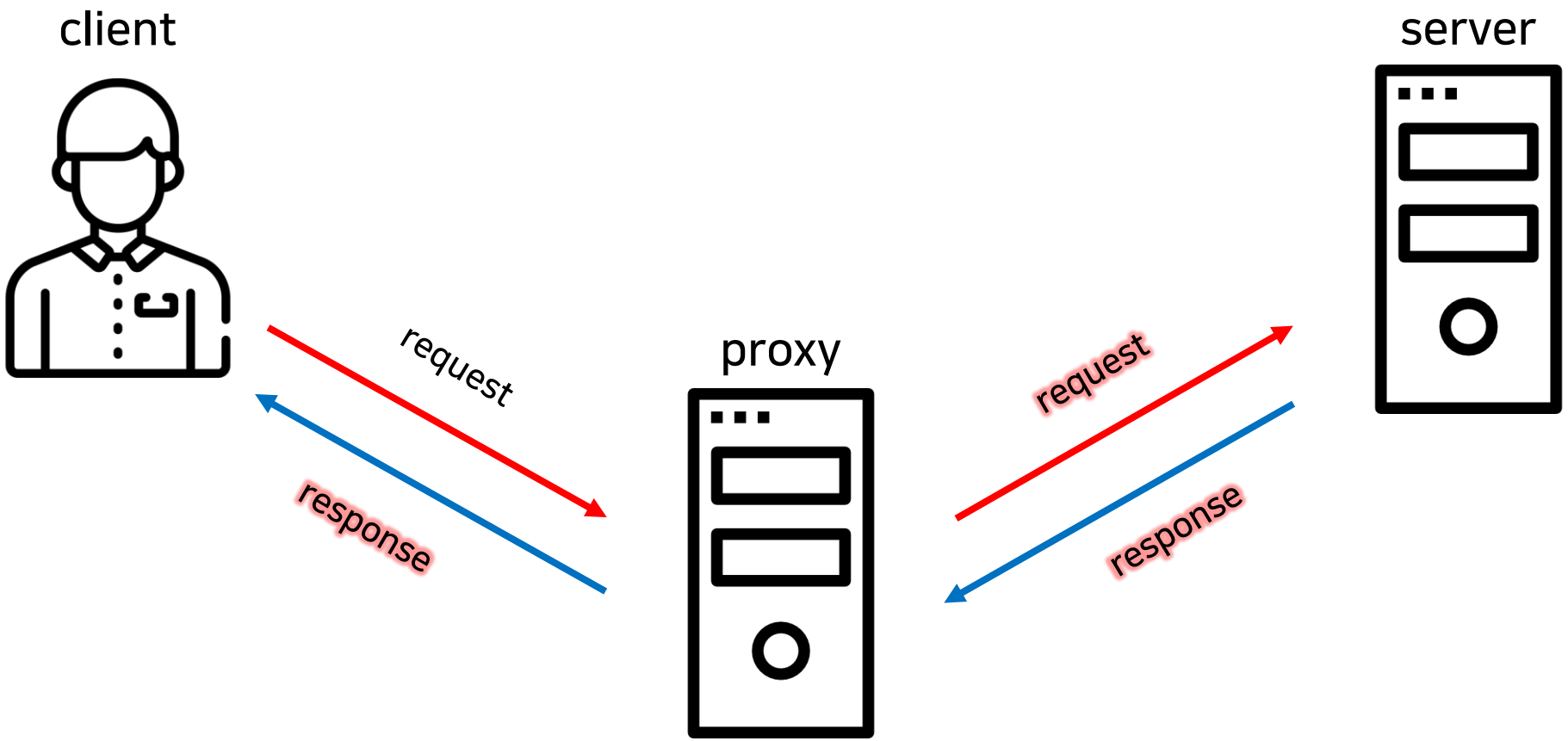
2-2. 변조 기능 분석

General.ver

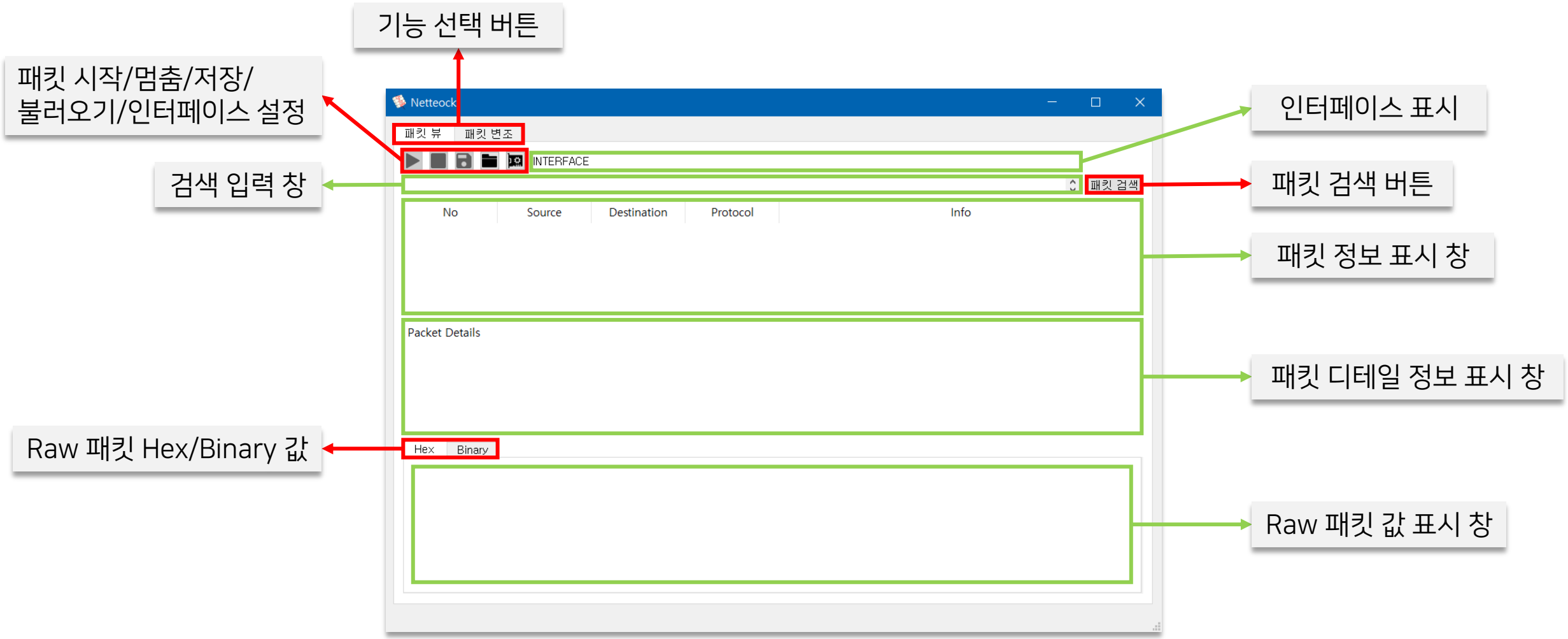


2-2. 변조 기능 분석

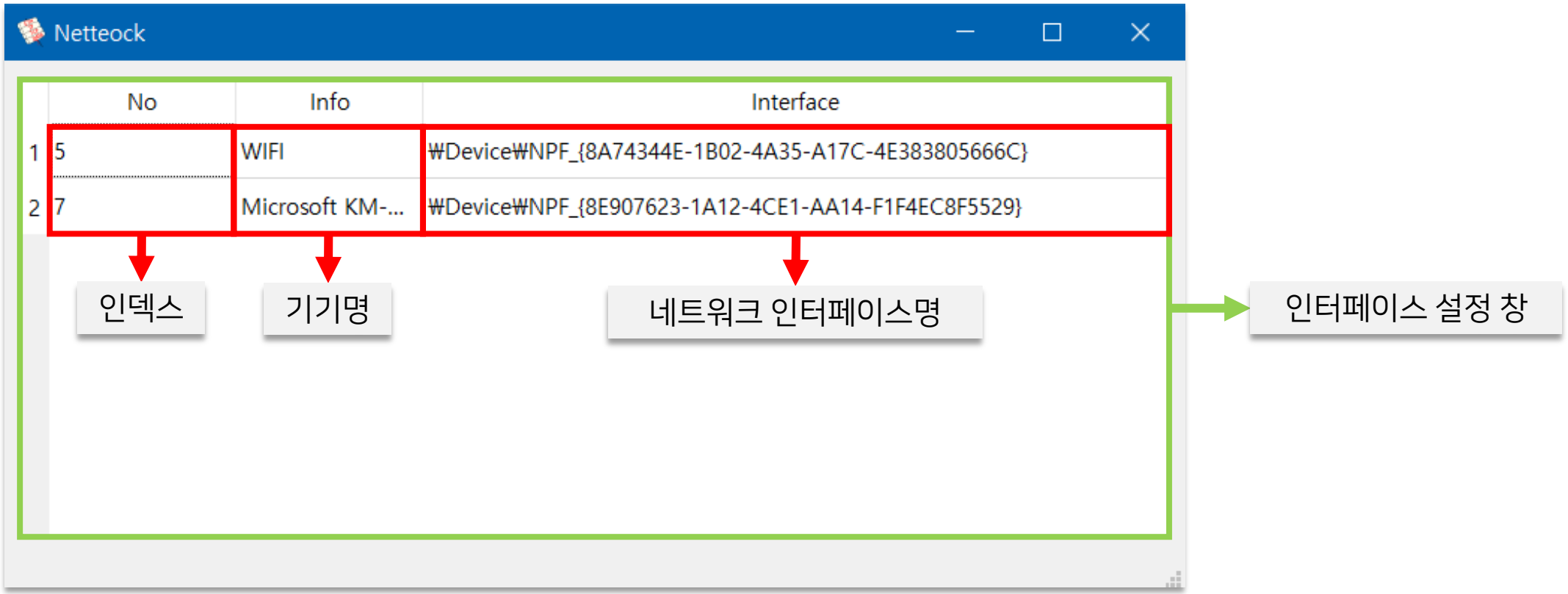
Proxy.ver



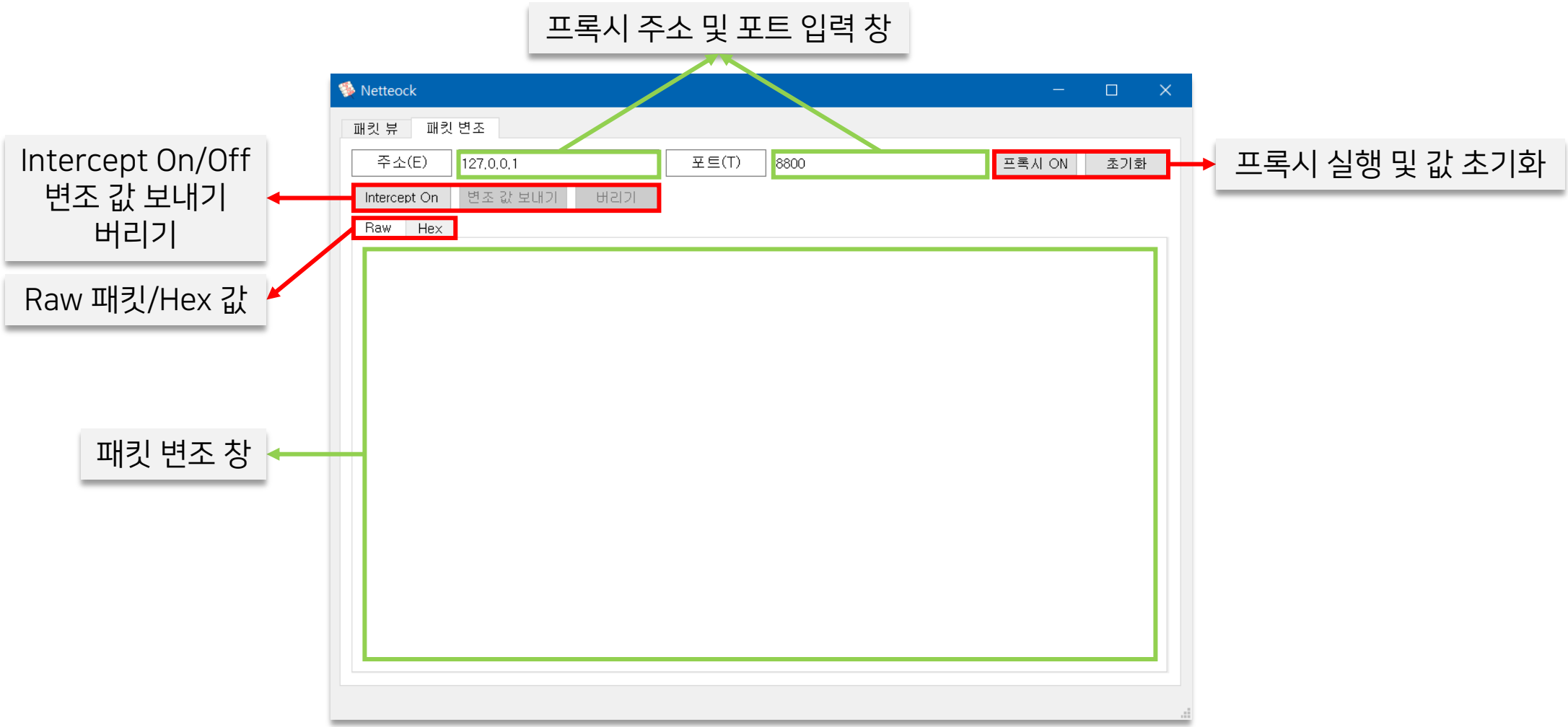
2-3. 모듈 개발 (화면, 기능)


기능 선택 버튼
패킷 시작/멈춤/저장/
불러오기/인터페이스 설정
검색 입력 창
Raw 패킷 Hex/Binary 값
Netteock
패킷 뷰
패킷 변조
INTERFACE
패킷 검색
No
Source
Destination
Protocol
Info
Packet Details
Hex
Binary
인터페이스 표시
패킷 검색 버튼
패킷 정보 표시 창
패킷 디테일 정보 표시 창
Raw 패킷 값 표시 창

2-3. 모듈 개발 (화면, 기능)

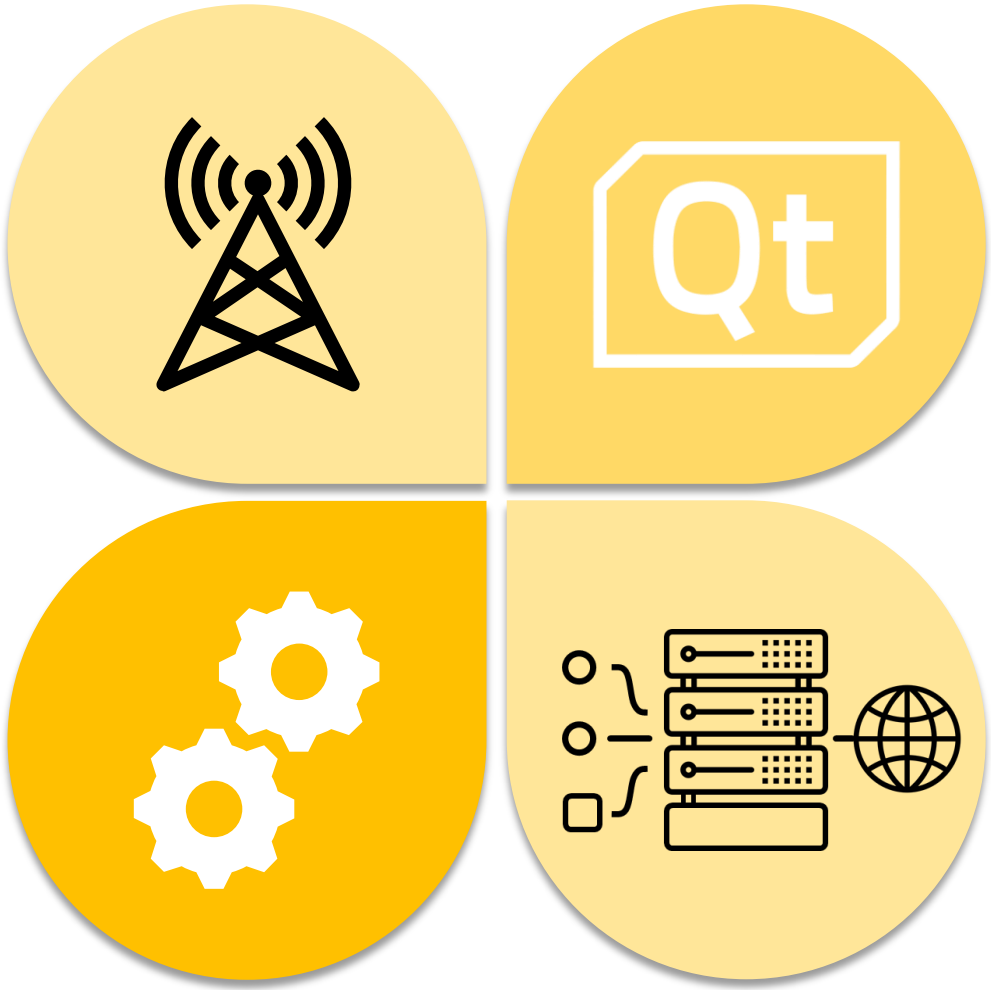

Netteock
No
Info
Interface
1
5
WIFI
₩Device₩NPF_{8A74344E-1B02-4A35-A17C-4E383805666C}
2
7
Microsoft KM-...
₩Device₩NPF_{8E907623-1A12-4CE1-AA14-F1F4EC8F5529}
인덱스
기기명
네트워크 인터페이스명
인터페이스 설정 창

2-3. 모듈 개발 (화면, 기능)


프록시 주소 및 포트 입력 창
Netteock
패킷 뷰
패킷 변조
주소(E)
127.0.0.1
포트(T)
8800
프록시 ON
초기화
Intercept On
변조 값 보내기
버리기
Raw
Hex
Intercept On/Off
변조 값 보내기
버리기
Raw 패킷/Hex 값
패킷 변조 창
프록시 실행 및 값 초기화

3-1. 성과

Network

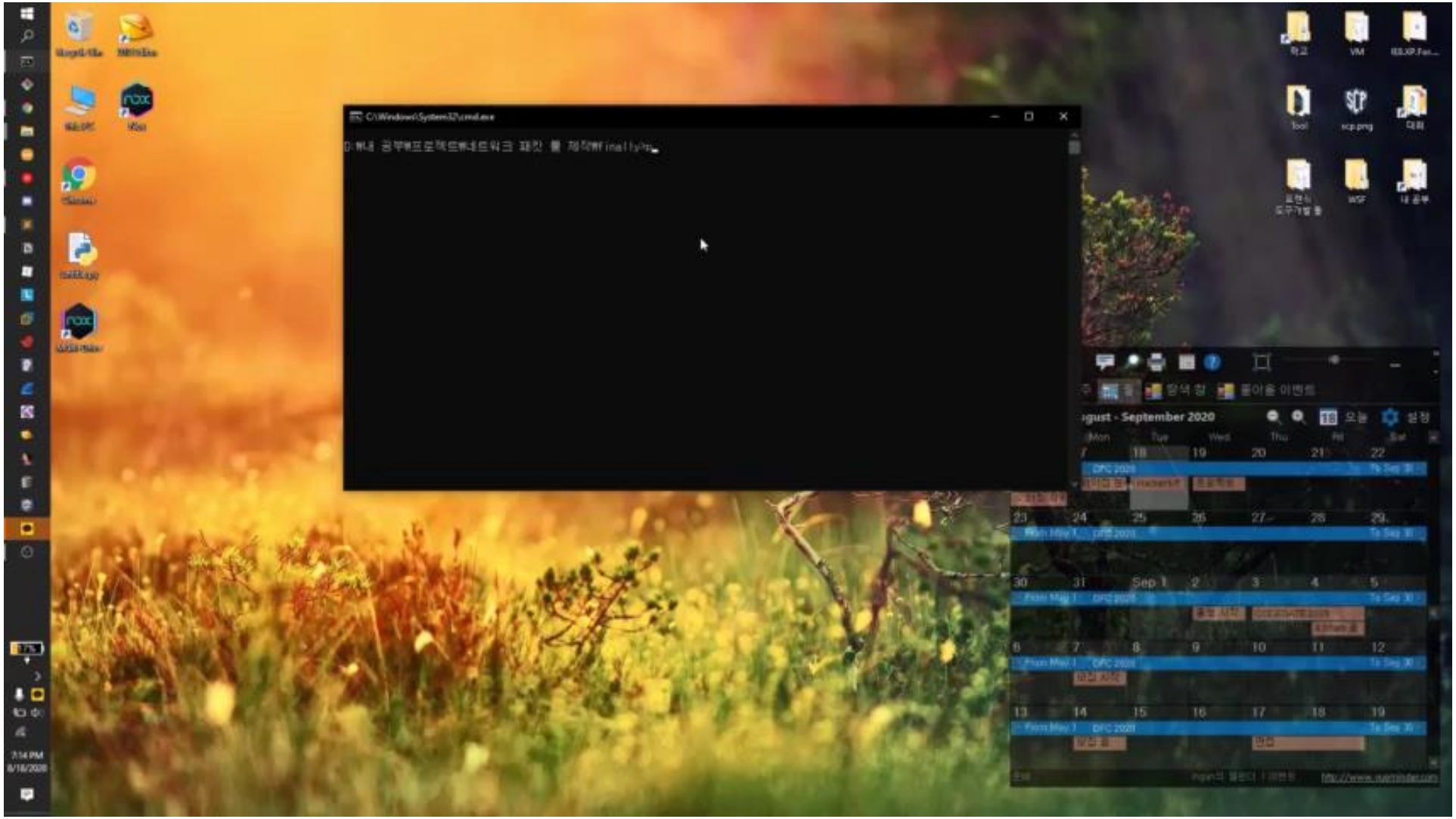


GUI

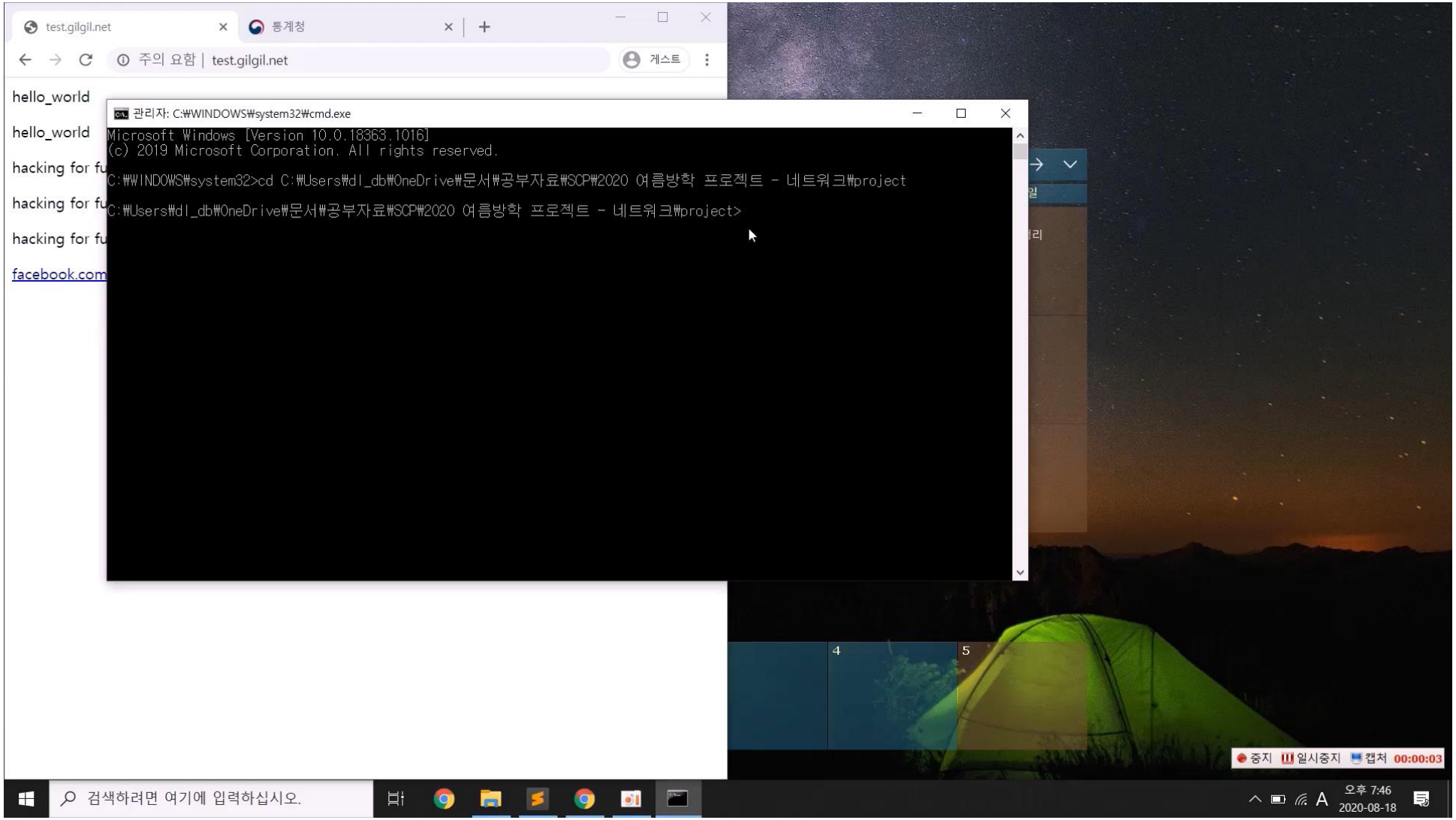
Threading

Proxy

3-2. 시연 영상 (뷰어)

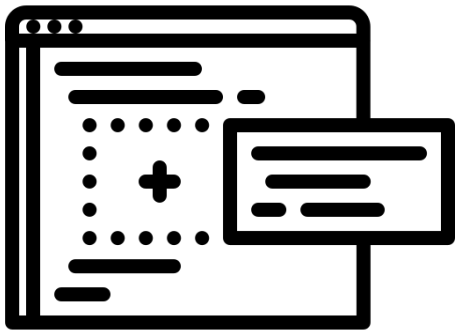


3-2. 시연 영상 (변조)

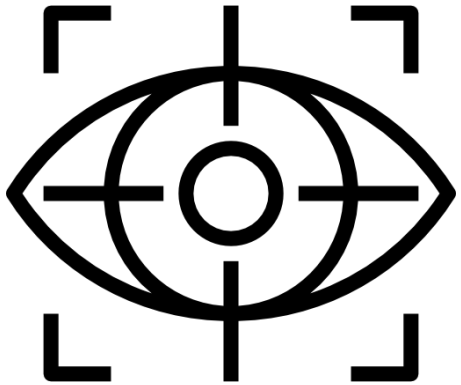

test.gilgil.net
통계청
주의 요함 | test.gilgil.net
게스트
hello_world
hello_world
hacking for fu
hacking for fu
hacking for fu
facebook.com
관리자: C:₩WINDOWS₩system32₩cmd.exe
Microsoft Windows [Version 10.0.18363.1016]
(c) 2019 Microsoft Corporation. All rights reserved.
C:₩WINDOWS₩system32>cd C:₩Users₩dl_db₩OneDrive₩문서₩공부자료₩SCP₩2020 여름방학 프로젝트 - 네트워크₩project
C:₩Users₩dl_db₩OneDrive₩문서₩공부자료₩SCP₩2020 여름방학 프로젝트 - 네트워크₩project>
4
5
중지
일시중지
캡처
00:00:03
검색하려면 여기에 입력하십시오.
오후 7:46
2020-08-18

4-1. 향후 계획

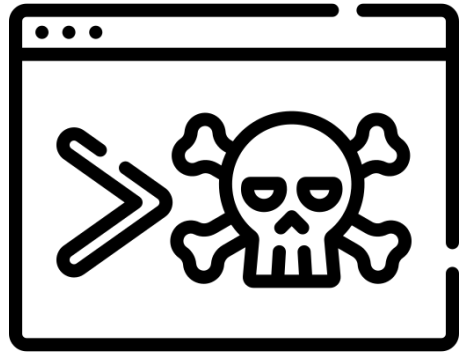
뷰어 / 변조 완성



초심자용 시각화



공격 기법 추가



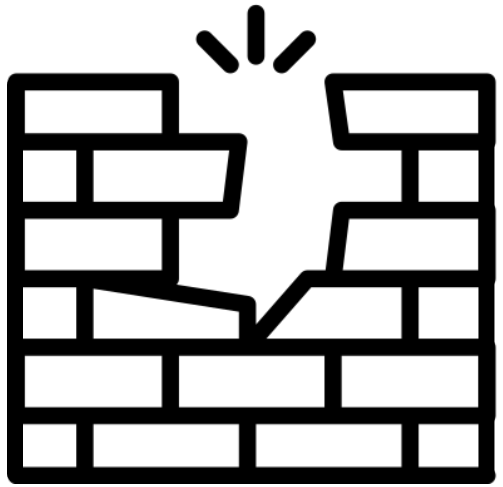
4-1. 향후 계획

툴 완성

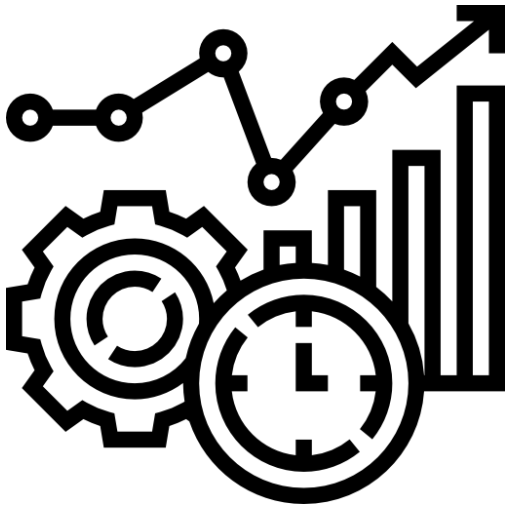
오픈소스 배포

4-2. 기대 효과

초심자의 네트워크 해킹 분야 빠른 진입



네트워크 툴의 통합으로 활용성 증가



THANK YOU

QUESTION