

# Netteok

중간 발표

김우종(PM)

문승재

서민재

이유경

# Contents

## 1. 프로젝트 개요

- 1-1. 일정 변경 사유
- 1-2. 변경 일정
- 1-3. 구상 및 설계

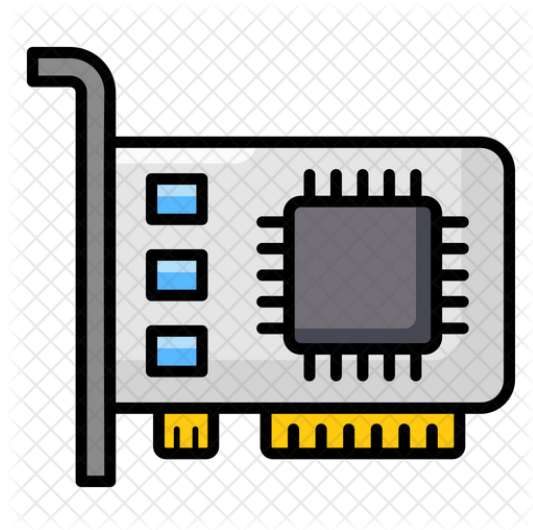
## 2. 프로젝트 수행과정

- 2-1. 분석
- 2-2. GUI

## 3. 향후 계획

## 1. 프로젝트 개요

### 1-1. 일정 변경 사유



네트워크 인터페이스 선택 기능 추가 개발

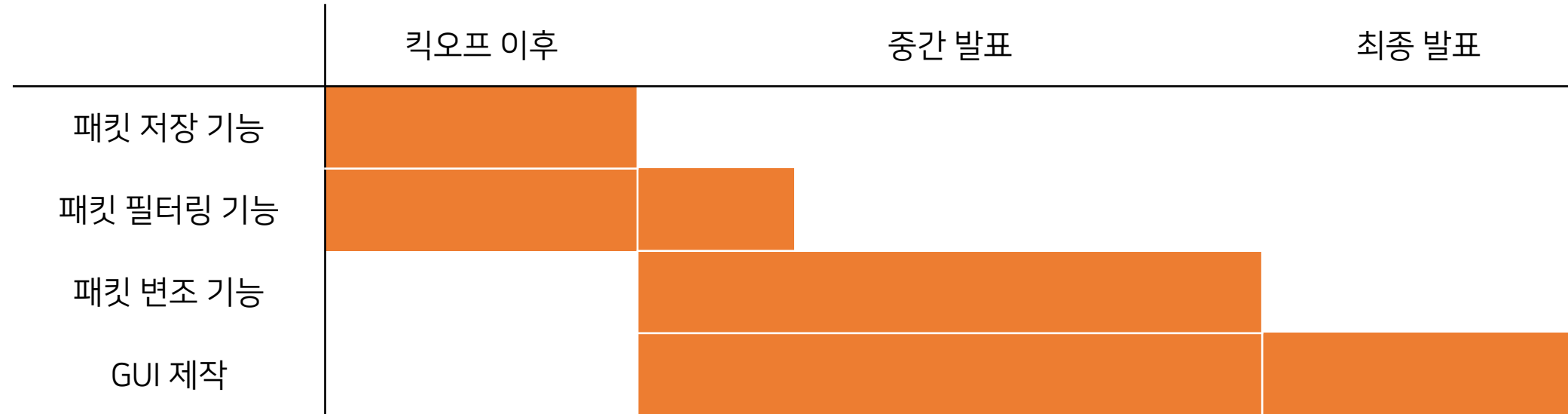


스레드 사용을 위한 GUI 우선 개발

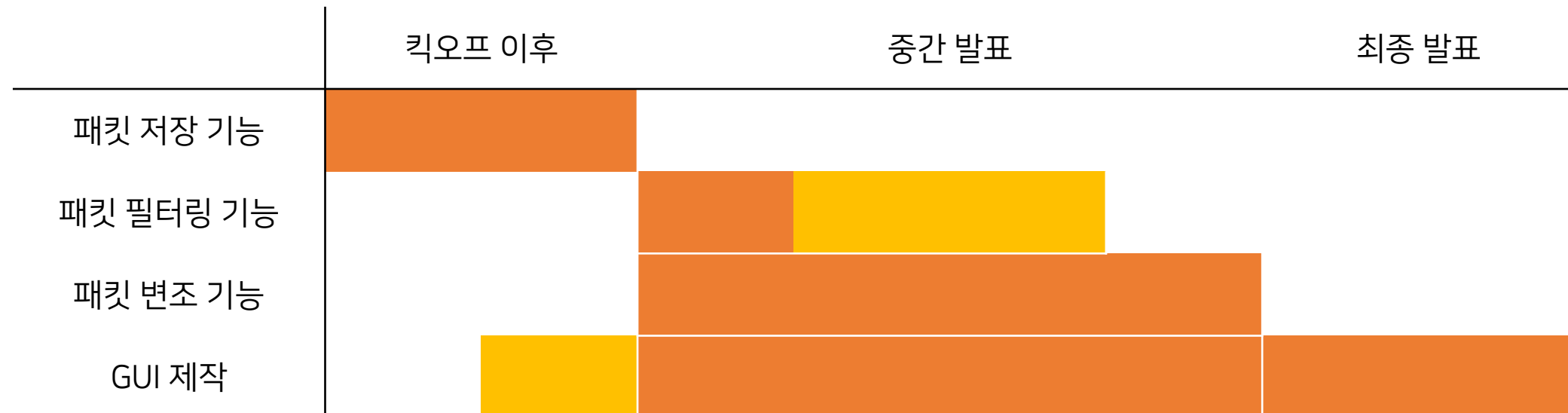
## 1. 프로젝트 개요

# 1-2. 변경 일정

기  
존  
계  
획

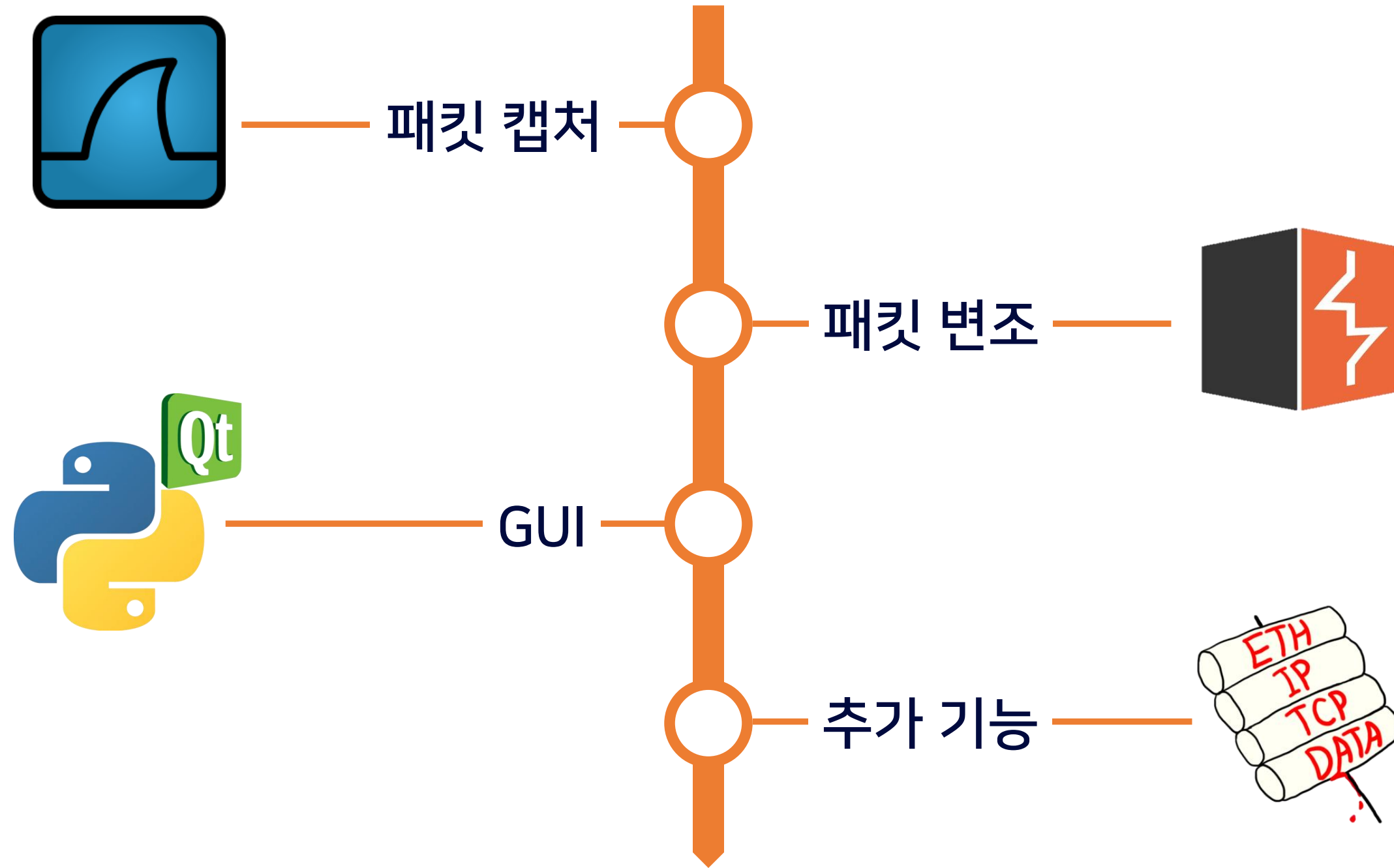


현  
재  
계  
획

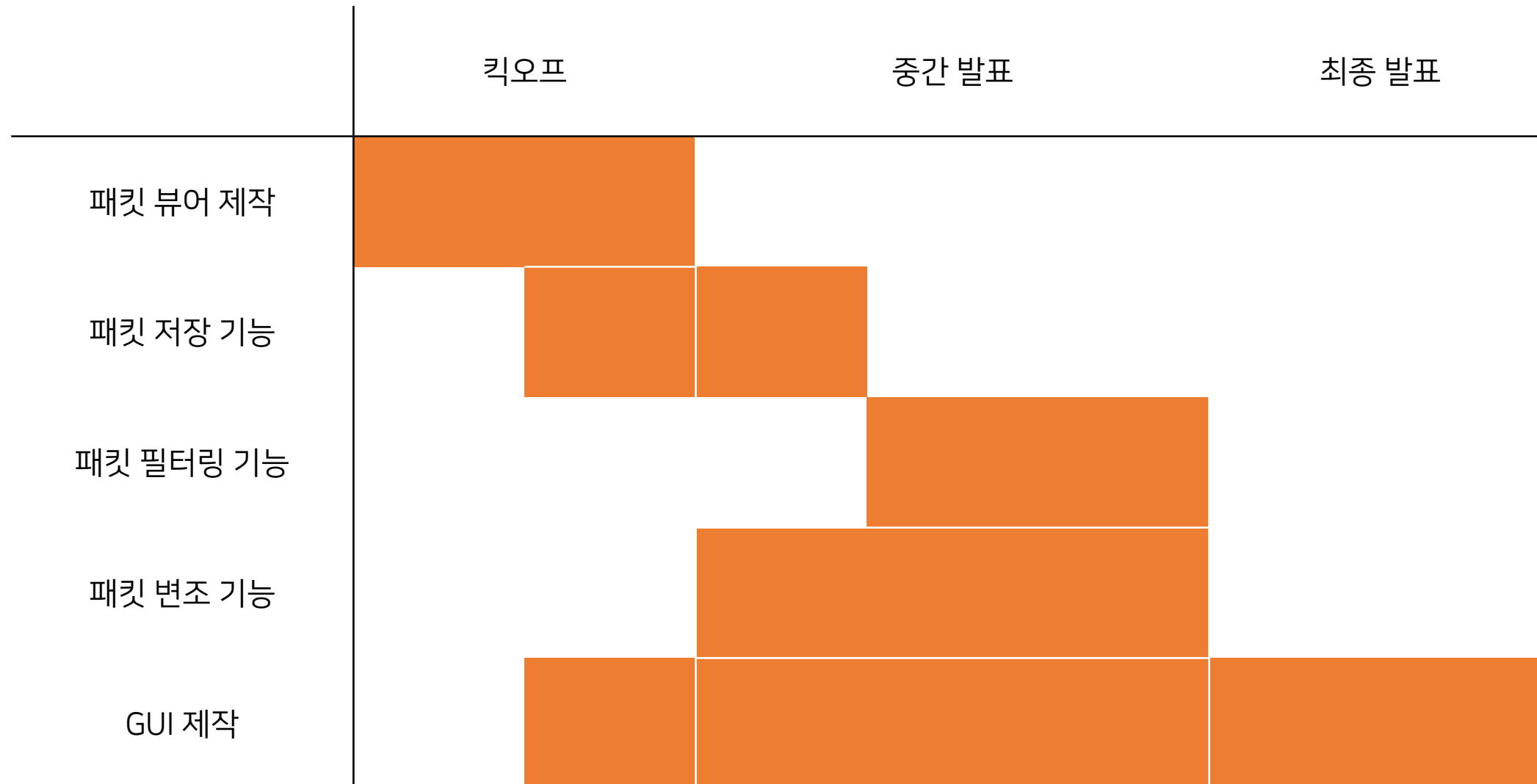


## 1. 프로젝트 개요

### 1-3. 구상 및 설계

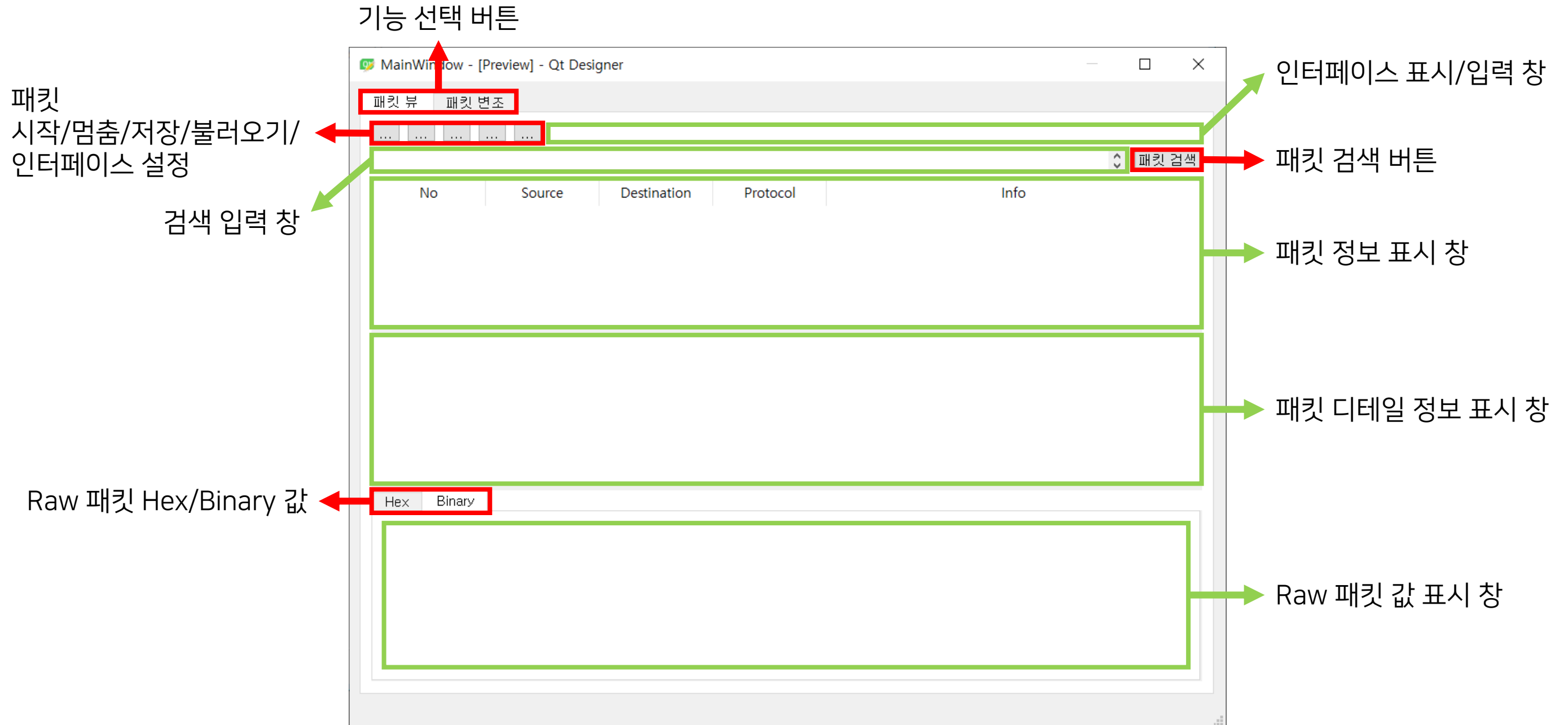


## 2. 프로젝트 수행과정



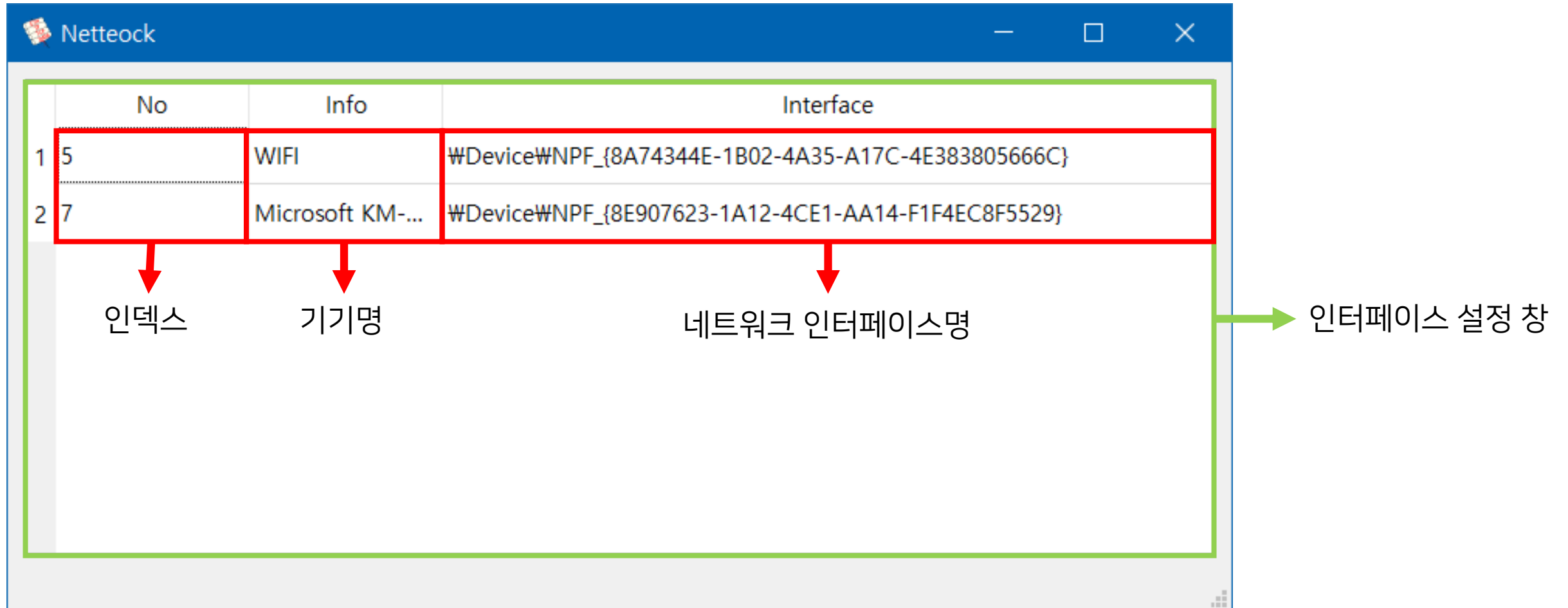
## 2. 프로젝트 수행과정

### 2-1. GUI



## 2. 프로젝트 수행과정

### 2-1. GUI



Netteock

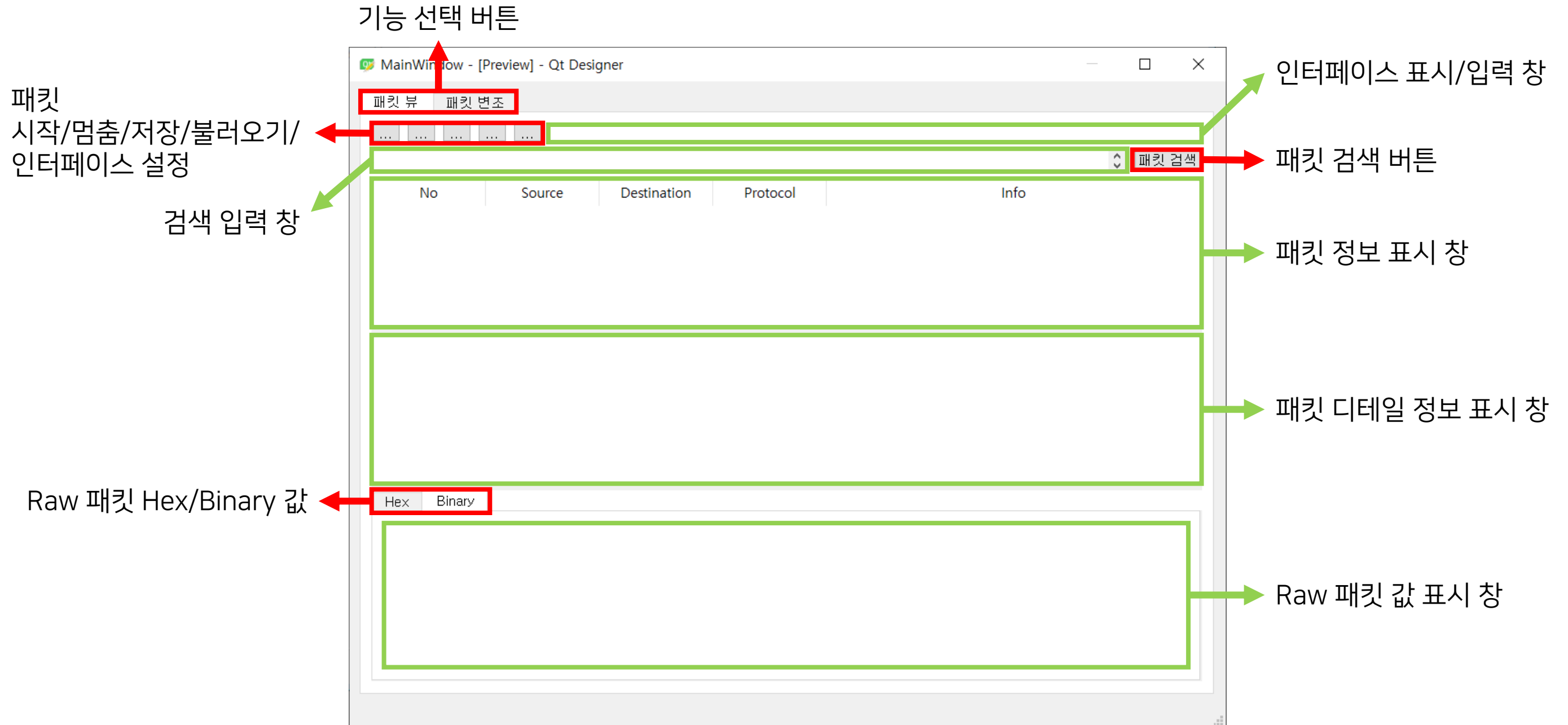
No	Info	Interface
1 5	WIFI	\Device\NPF_{8A74344E-1B02-4A35-A17C-4E383805666C}
2 7	Microsoft KM-...	\Device\NPF_{8E907623-1A12-4CE1-AA14-F1F4EC8F5529}

인덱스      기기명      네트워크 인터페이스명      인터페이스 설정 창



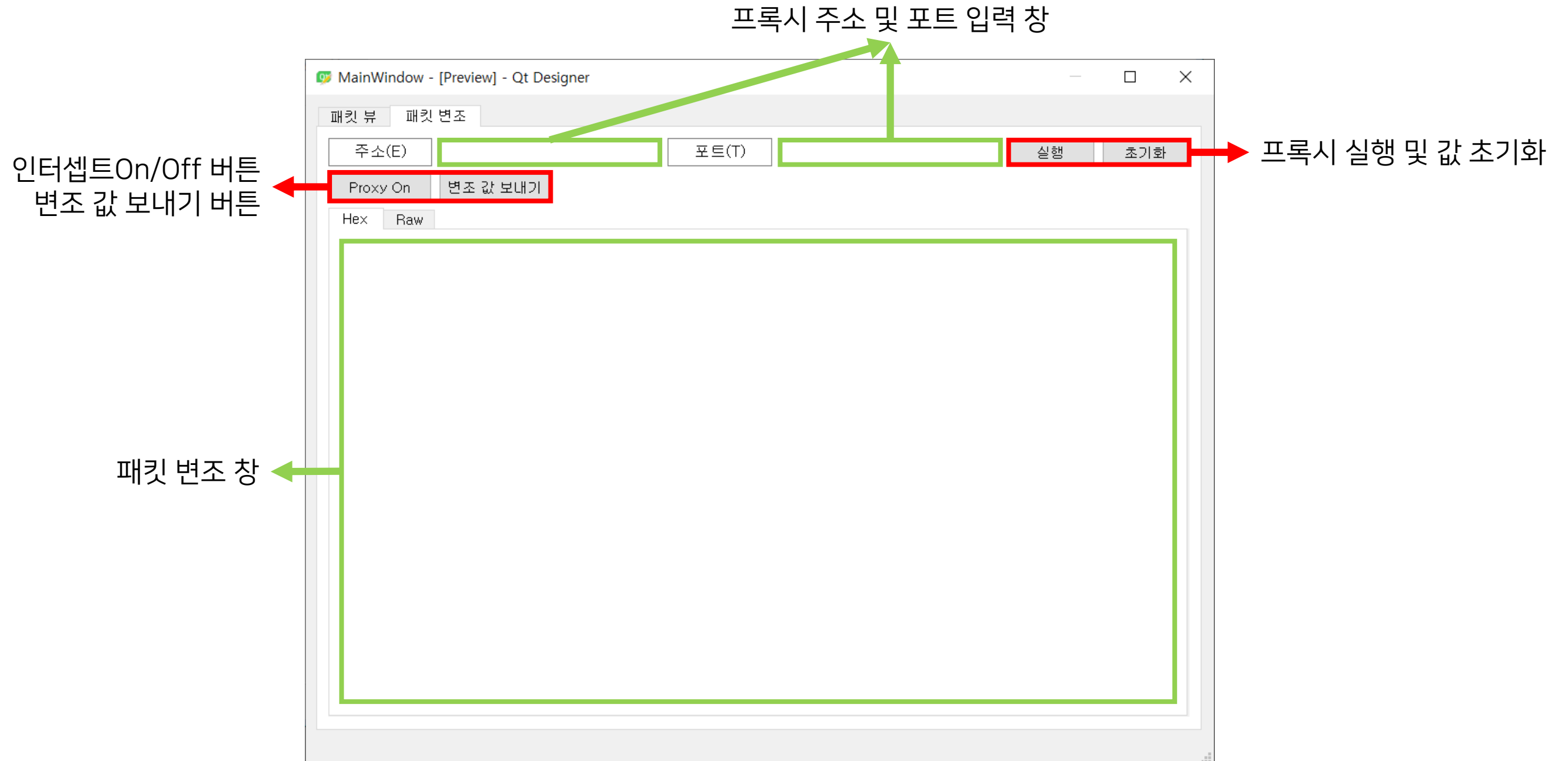
## 2. 프로젝트 수행과정

### 2-1. GUI



## 2. 프로젝트 수행과정

### 2-1. GUI



## 2. 프로젝트 수행과정

### 2-2. 분석(protocol)

	계층	프로토콜
Layer 7	Application (응용)	HTTP, FTP, DNS
Layer 6	Presentation (표현)	TELNET, SSL
Layer 5	Session (세션)	SSH, TLS
Layer 4	Transport (전송)	TCP, UDP
Layer 3	Network (네트워크)	IP
Layer 2	Data Link (데이터 링크)	Ethernet
Layer 1	Physical (물리)	하드웨어

## 2. 프로젝트 수행과정

### 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..Host: 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
-----------------------	-----------------------	-----------------------	------

## 2. 프로젝트 수행과정

### 2-2. 분석(IP)

```

0000  00 1a 1e 01 42 e8 3c f0 11 27 f7 63 08 00 45 00
0010  01 fd 16 2c 40 00 80 06 5e 78 ac 1f 05 3b af d5
0020  23 27 c2 9c 00 50 3a c8 39 f3 b2 1d 2f cc 50 18
0030  02 02 a6 f4 00 00 47 45 54 20 2f 20 48 54 54 50
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74
0050  2e 67 69 6c 67 69 6c 2e 6e 65 74 0d 0a
  
```

```

...B<...'c..E.
...,@...^X...;..
#'...P:..9.../.P.
.....GE T / HTTP
/1.1..Ho st: test
.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						

## 2. 프로젝트 수행과정

## 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									

## 2. 프로젝트 수행과정

### 2-2. 분석(HTTP)

```

0000  00 1a 1e 01 42 e8 3c f0 11 27 f7 63 08 00 45 00
0010  01 fd 16 2c 40 00 80 06 5e 78 ac 1f 05 3b af d5
0020  23 27 c2 9c 00 50 3a c8 39 f3 b2 1d 2f cc 50 18
0030  02 02 a6 f4 00 00 47 45 54 20 2f 20 48 54 54 50
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74
0050  2e 67 69 6c 67 69 6c 2e 6e 65 74 0d 0a
  
```

```

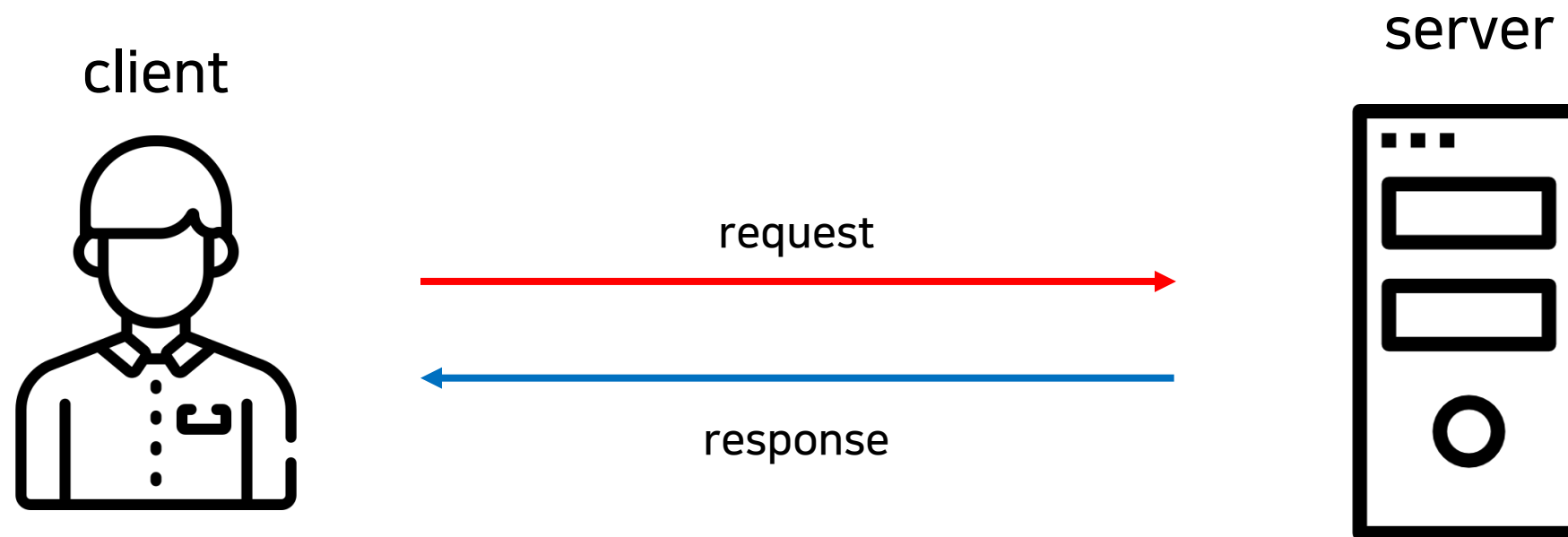
...B<... 'c...E...
... ,@... ^x...;...
# '...P: 9.../P...
...GE T / HTTP
/1.1...Host: test
.gilgil.net...
  
```

Request line
Header
␣n
Body

## 2. 프로젝트 수행과정

### 2-2. 분석(변조)

General.ver

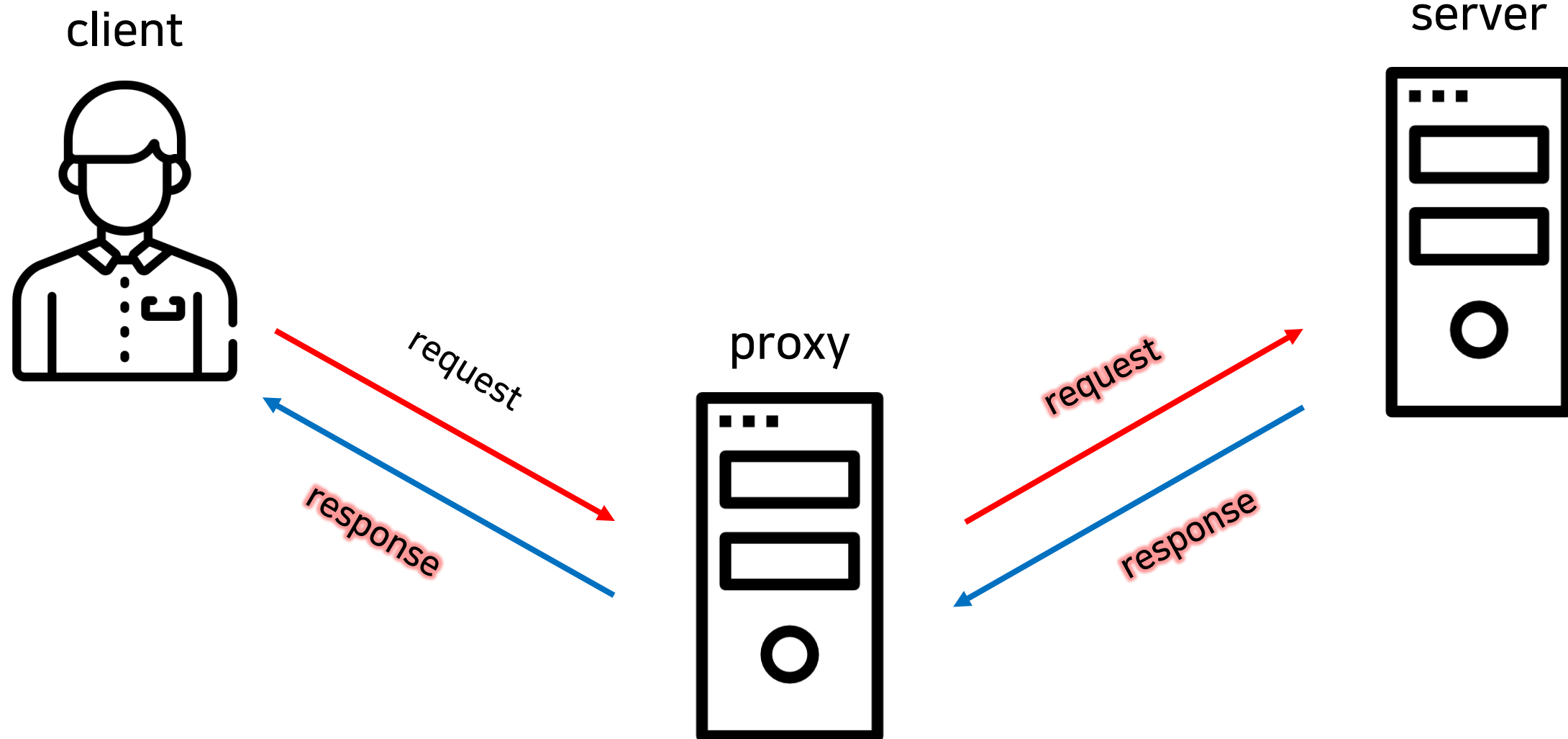




## 2. 프로젝트 수행과정

## 2-2. 분석(변조)

Proxy.ver

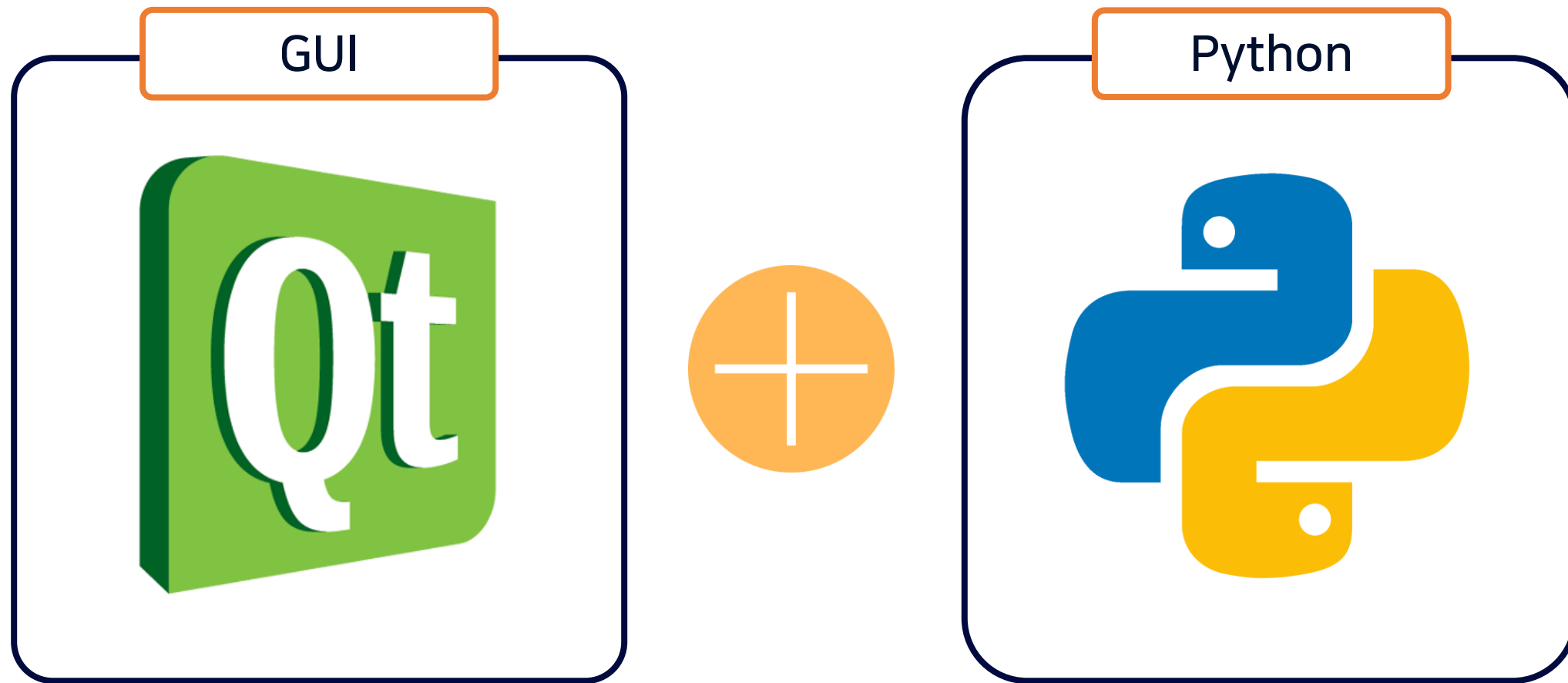


# 3. 향후 계획

- GUI + Python
- 기능 완성
- Hex 뷰어 제작
- 추가 기능 제작

### 3. 향후 계획

## 3-1. GUI + Python

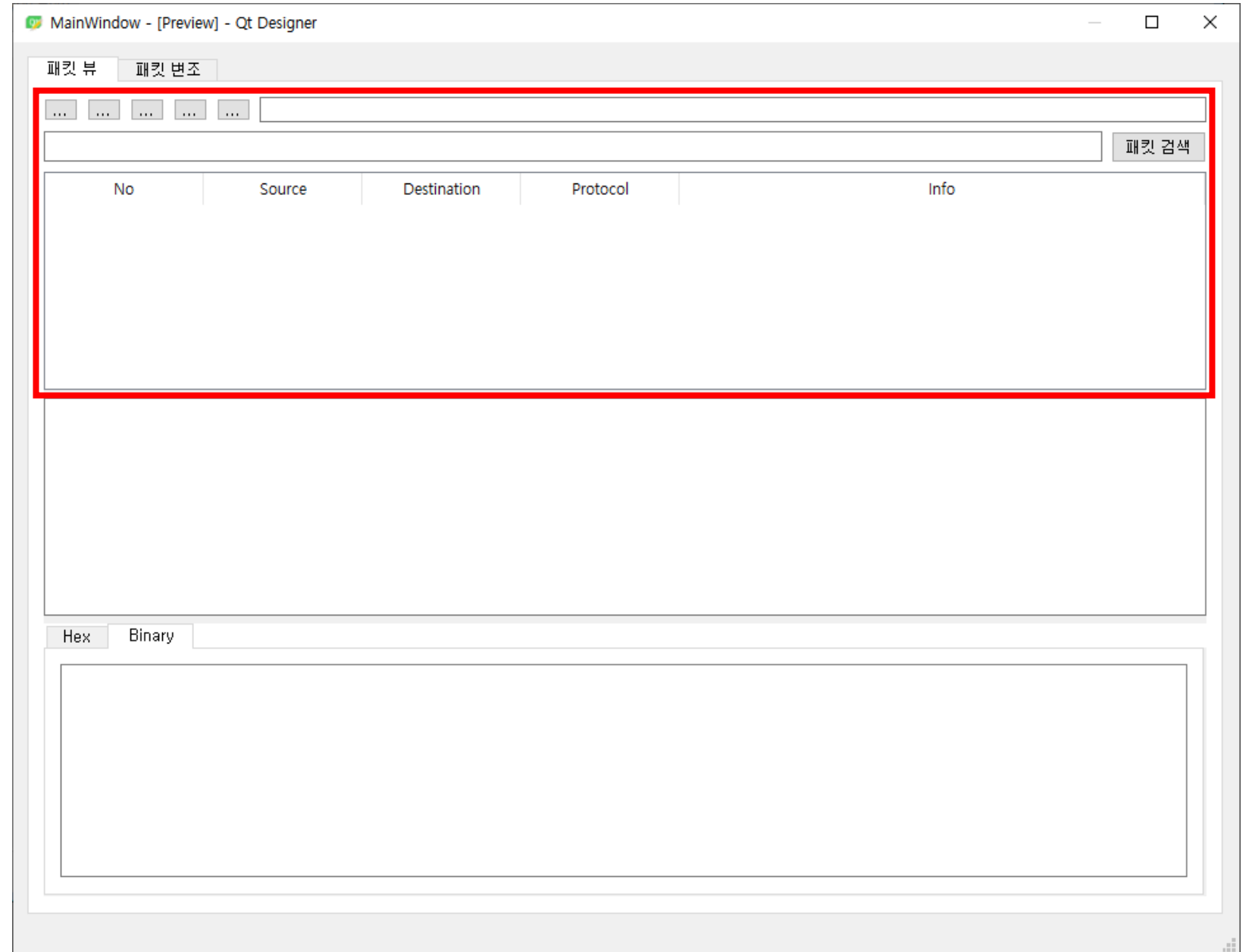


### 3. 향후 계획

## 3-2. 기능 완성

### • 필터링

1. GUI에 표시된 패킷 정보  
리스트 화
2. 검색 문자열을 바탕으로  
필터링



### 3. 향후 계획

## 3-2. 기능 완성

- Pcap 파일 불러오기

1. Pcap 글로벌 헤더 제거
2. Pcap 패킷 헤더 제거
3. 남겨진 Raw 패킷 분석
4. GUI에 표시

```
#      Pcap Global Header Format :  
#      ( magic number +  
#      major version number +  
#      minor version number +  
#      GMT to local correction +  
#      accuracy of timestamps +  
#      max length of captured #packets, in octets +  
#      data link type)  
#  
#  
PCAP_GLOBAL_HEADER_FMT = '@ I H H i I I I '  
  
# Global Header Values  
PCAP_MAGICAL_NUMBER = 2712847316  
PCAP_MJ_VERN_NUMBER = 2  
PCAP_MI_VERN_NUMBER = 4  
PCAP_LOCAL_CORRECTIN = 0  
PCAP_ACCUR_TIMESTAMP = 0  
PCAP_MAX_LENGTH_CAP = 65535  
PCAP_DATA_LINK_TYPE = 1
```

### 3. 향후 계획

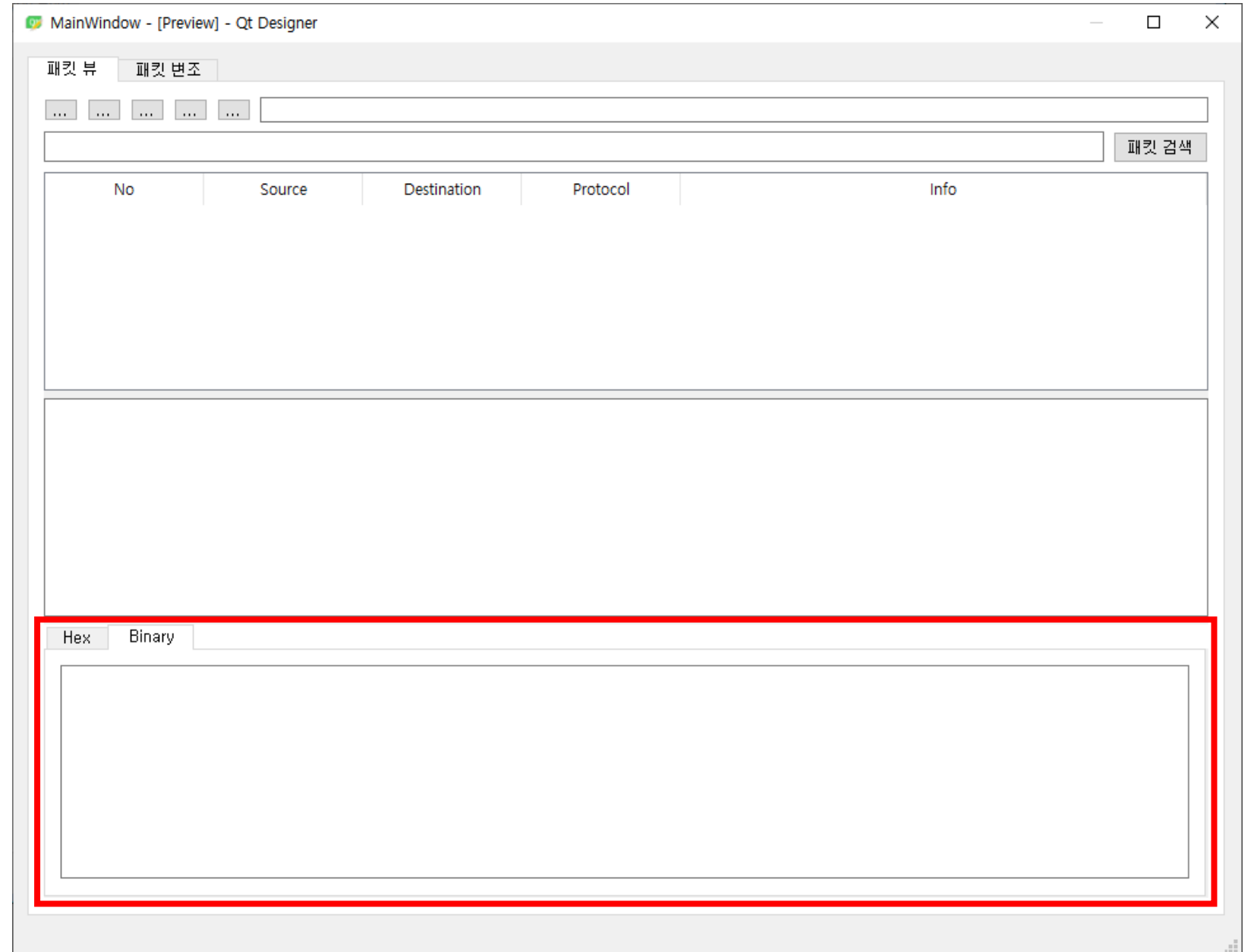
## 3-3. Hex 뷰어 제작

- Hex 뷰어 제작

- GUI에 표시

- Binary 뷰어 제작

- GUI에 표시



### 3. 향후 계획

## 3-4. 추가 기능 제작

- 공격 버튼
- Hex 뷰어 필드 값 구분(색상)
- 이해도 향상을 위한 통신 과정 이미지 추가
- 네트워크 인터페이스 위젯 수정

# QnA