



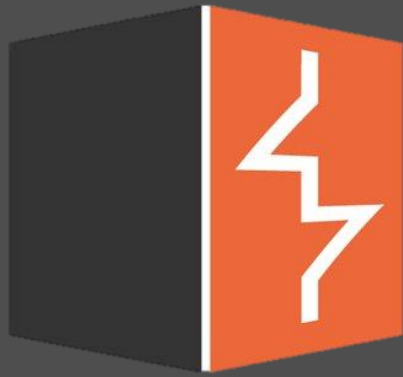
# Netteok

김우종, 문승재, 서민재, 이유경

# 목차

1. 프로젝트 개요
  - 1) 프로젝트 소개
  - 2) 프로젝트 일정
  
2. 프로젝트 설계
  - 1) 프로젝트 구상
  - 2) 프로젝트 화면 정의서
  
3. 프로젝트 목표
  - 1) 프로젝트 산출물
  - 2) 기대효과

# 프로젝트 소개



## Burp Suite

HTTP 패킷을 받아 변조할 수 있다.

모든 패킷을 받아 확인할 수 없다.

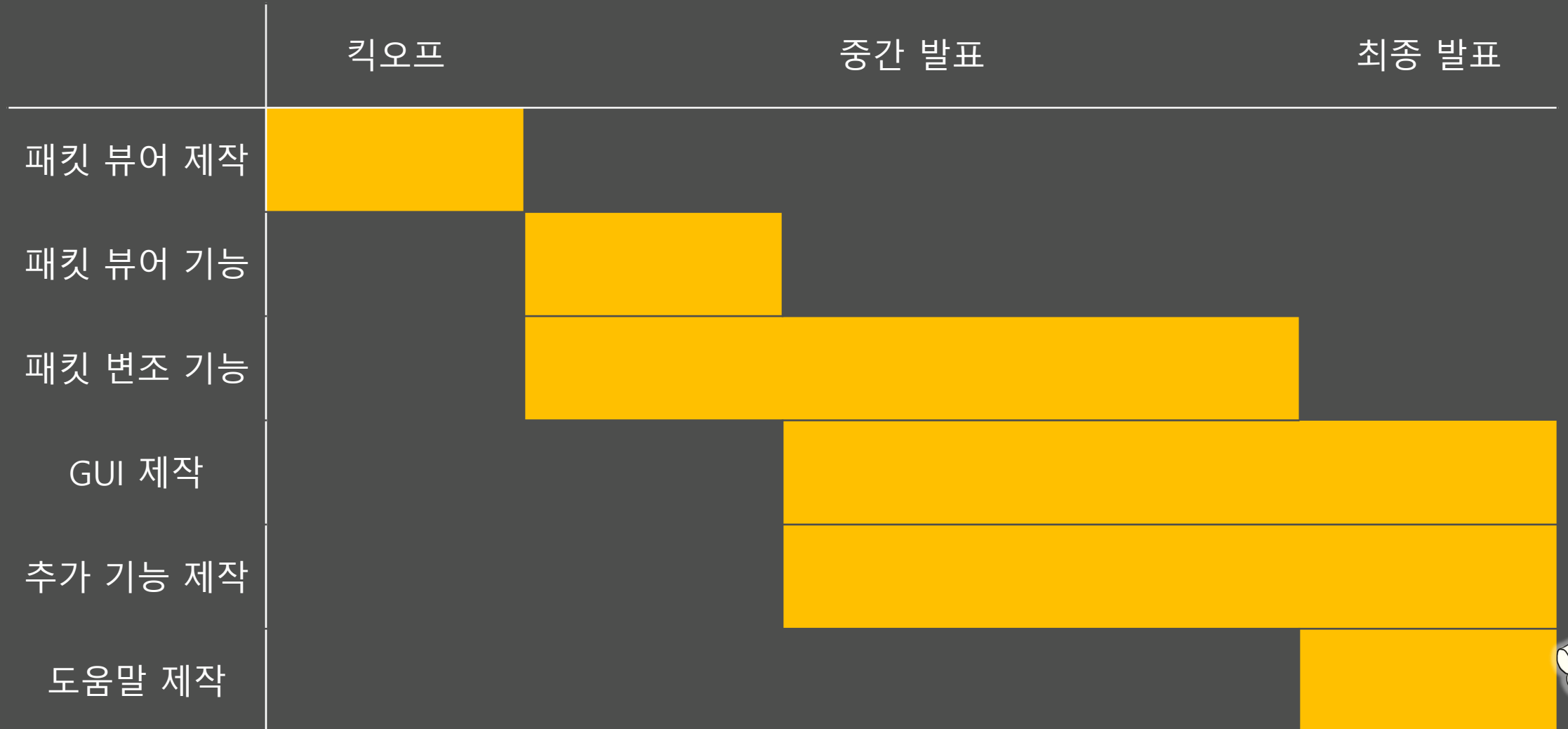


## Wireshark

패킷에 대한 변조 기능이 없다.

모든 패킷을 받아 확인할 수 있다

# 프로젝트 일정



# 프로젝트 산출물



개발 환경

Windows 10



개발 언어

Python3.8.3



인터페이스

GUI (pyQt5)



# 프로젝트 구상

## 패킷 뷰어 제작

사용 모듈 : dpkt, pcap

## 패킷 뷰어 기능

패킷 필터링 : 조건에 맞는 패킷 출력

패킷 저장 : pcap 확장자 이용



프록시 : 8080 포트 사용

추가 기능 : 디코더, 반복요청

## 패킷 변조 기능

Dos 공격  
ARP 스푸핑

## 추가 기능 제작

# 프로젝트 화면 정의서

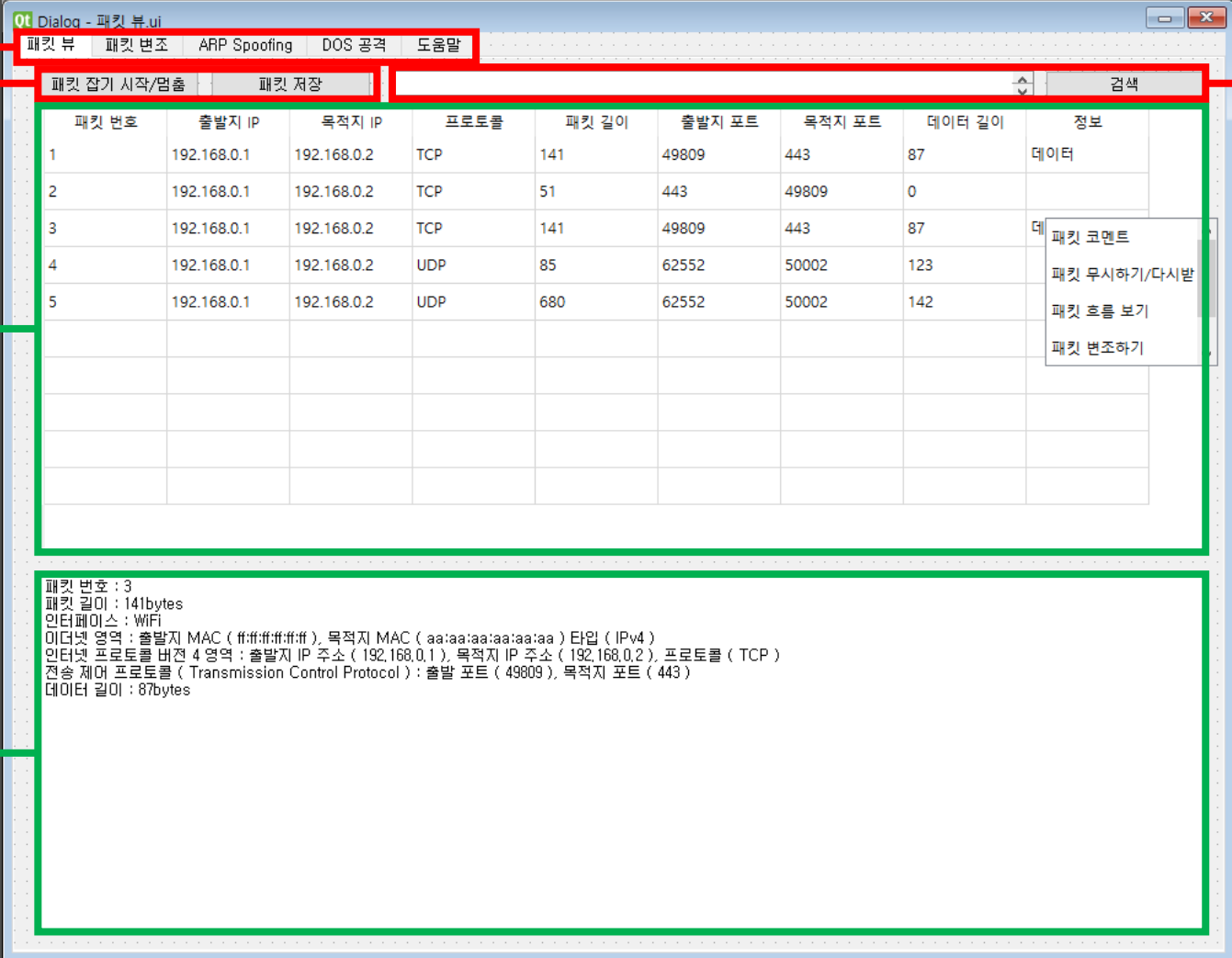
기능 탭

패킷 잡기/멈춤  
패킷 저장

패킷 검색 기능

패킷 뷰어 영역

패킷 디테일 영역

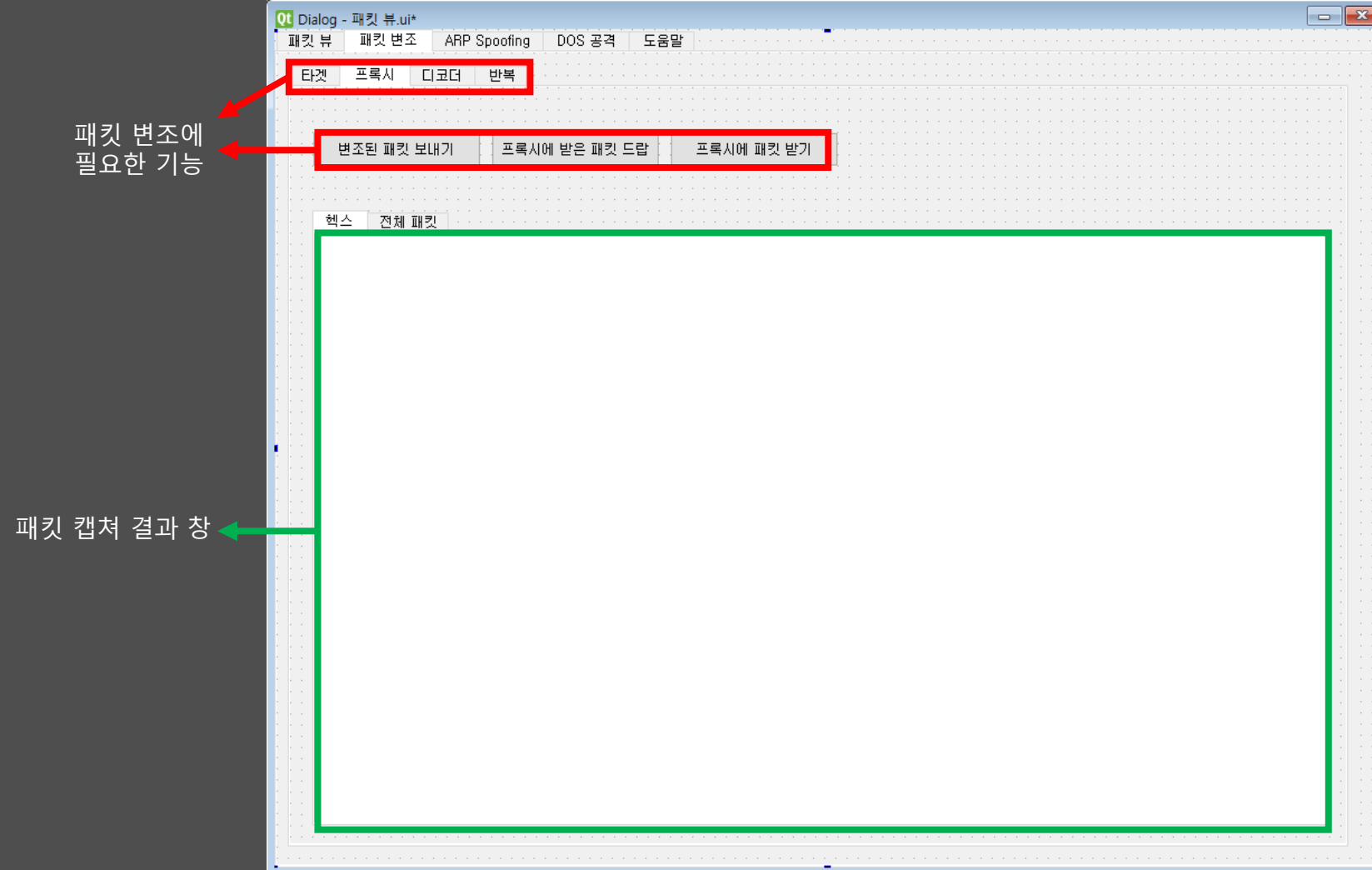


The screenshot shows a software interface for packet analysis. At the top, there are tabs for '패킷 뷰' (selected), '패킷 변조', 'ARP Spoofing', 'DOS 공격', and '도움말'. Below the tabs are buttons for '패킷 잡기 시작/멈춤' and '패킷 저장', followed by a search bar labeled '검색'. The main area contains a table with columns: '패킷 번호', '출발지 IP', '목적지 IP', '프로토콜', '패킷 길이', '출발지 포트', '목적지 포트', '데이터 길이', and '정보'. The table lists 5 packets. A context menu is open over the '정보' column of packet 3, showing options: '패킷 코멘트', '패킷 무시하기/다시받', '패킷 흐름 보기', and '패킷 변조하기'. Below the table is a detailed view for '패킷 번호 : 3', showing '패킷 길이 : 141bytes', '인터페이스 : WiFi', '이더넷 영역 : 출발지 MAC ( ff:ff:ff:ff:ff:ff ), 목적지 MAC ( aa:aa:aa:aa:aa:aa ) 타입 ( IPv4 )', '인터넷 프로토콜 버전 4 영역 : 출발지 IP 주소 ( 192.168.0.1 ), 목적지 IP 주소 ( 192.168.0.2 ), 프로토콜 ( TCP )', '전송 제어 프로토콜 ( Transmission Control Protocol ) : 출발 포트 ( 49809 ), 목적지 포트 ( 443 )', and '데이터 길이 : 87bytes'.

패킷 번호	출발지 IP	목적지 IP	프로토콜	패킷 길이	출발지 포트	목적지 포트	데이터 길이	정보
1	192.168.0.1	192.168.0.2	TCP	141	49809	443	87	데이터
2	192.168.0.1	192.168.0.2	TCP	51	443	49809	0	
3	192.168.0.1	192.168.0.2	TCP	141	49809	443	87	데
4	192.168.0.1	192.168.0.2	UDP	85	62552	50002	123	
5	192.168.0.1	192.168.0.2	UDP	680	62552	50002	142	

패킷 번호 : 3  
 패킷 길이 : 141bytes  
 인터페이스 : WiFi  
 이더넷 영역 : 출발지 MAC ( ff:ff:ff:ff:ff:ff ), 목적지 MAC ( aa:aa:aa:aa:aa:aa ) 타입 ( IPv4 )  
 인터넷 프로토콜 버전 4 영역 : 출발지 IP 주소 ( 192.168.0.1 ), 목적지 IP 주소 ( 192.168.0.2 ), 프로토콜 ( TCP )  
 전송 제어 프로토콜 ( Transmission Control Protocol ) : 출발 포트 ( 49809 ), 목적지 포트 ( 443 )  
 데이터 길이 : 87bytes

# 프로젝트 화면 정의서





# 프로젝트 화면 정의서

예시 패킷 사진

예시에 대한 설명

이전 설명 버튼

Qt Dialog - 패킷 뷰.ui\*

패킷 뷰
패킷 변조
ARP Spoofing
DOS 공격
도움말

예시 1

패킷 번호	출발지 IP	목적지 IP	프로토콜	패킷 길이	출발지 포트	목적지 포트	데이터 길이	정보
1	192.168.0.1	192.168.0.2	TCP	141	49809	443	87	SYN
2	192.168.0.1	192.168.0.2	TCP	51	443	49809	0	SYN + ACK
3	192.168.0.1	192.168.0.2	TCP	141	49809	443	87	ACK

패킷 번호 : 3  
패킷 길이 : 141bytes  
인터페이스 : WiFi  
이더넷 영역 : 출발지 MAC ( ff:ff:ff:ff:ff:ff ), 목적지 MAC ( aa:aa:aa:aa:aa:aa ) 타입 ( IPv4 )  
인터넷 프로토콜 버전 4 영역 : 출발지 IP 주소 ( 192.168.0.1 ), 목적지 IP 주소 ( 192.168.0.2 ), 프로토콜 ( TCP )  
전송 제어 프로토콜 ( Transmission Control Protocol ) : 출발 포트 ( 49809 ), 목적지 포트 ( 443 )  
데이터 길이 : 87bytes

대충 SYN 이 있고 SYN + ACK 패킷 왔고 ACK 패킷을 보내는 걸로 대충 쓰리웨이 핸드셰이크라는 설명설명설명

prev

next

다음 설명 버튼



# 프로젝트 산출물



Netteok 툴 배포



가이드라인 문서화



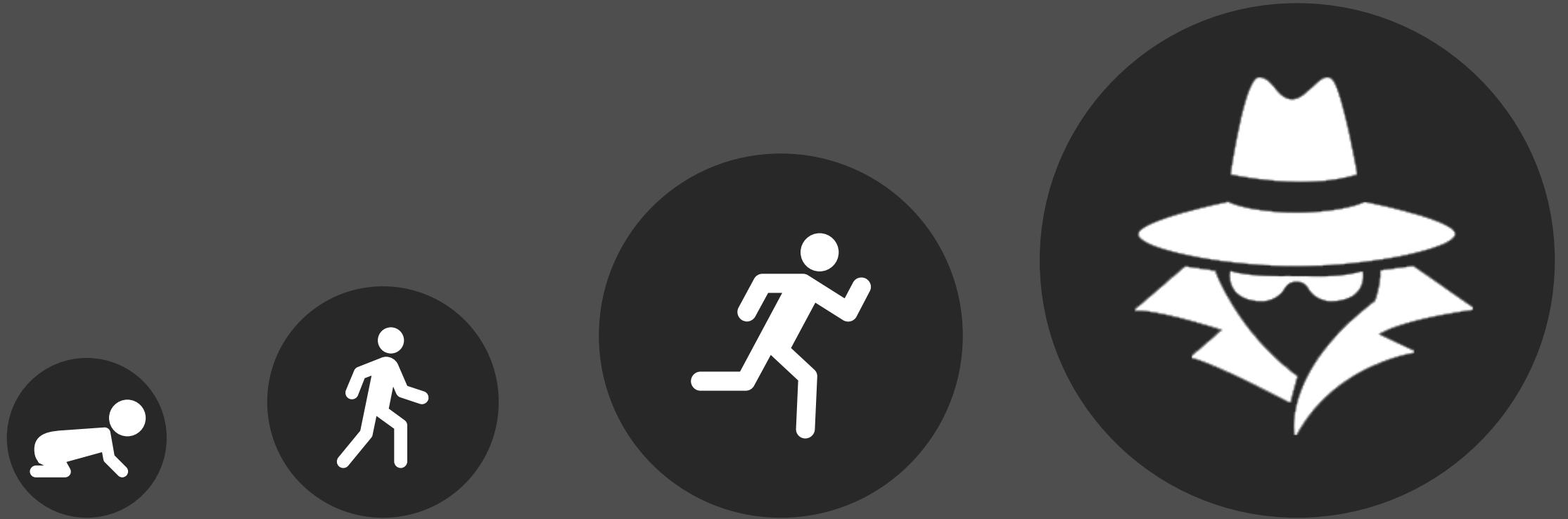
오픈소스 배포

# 기대효과



네트워크 공부로 인한 팀원의 성장

# 기대효과



네트워크 초심자의 네트워크 해킹 분야 빠른 진입



