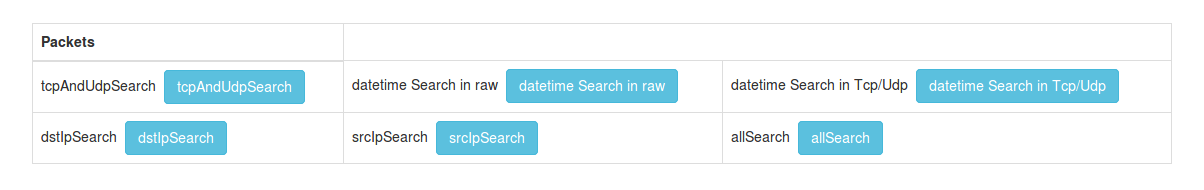
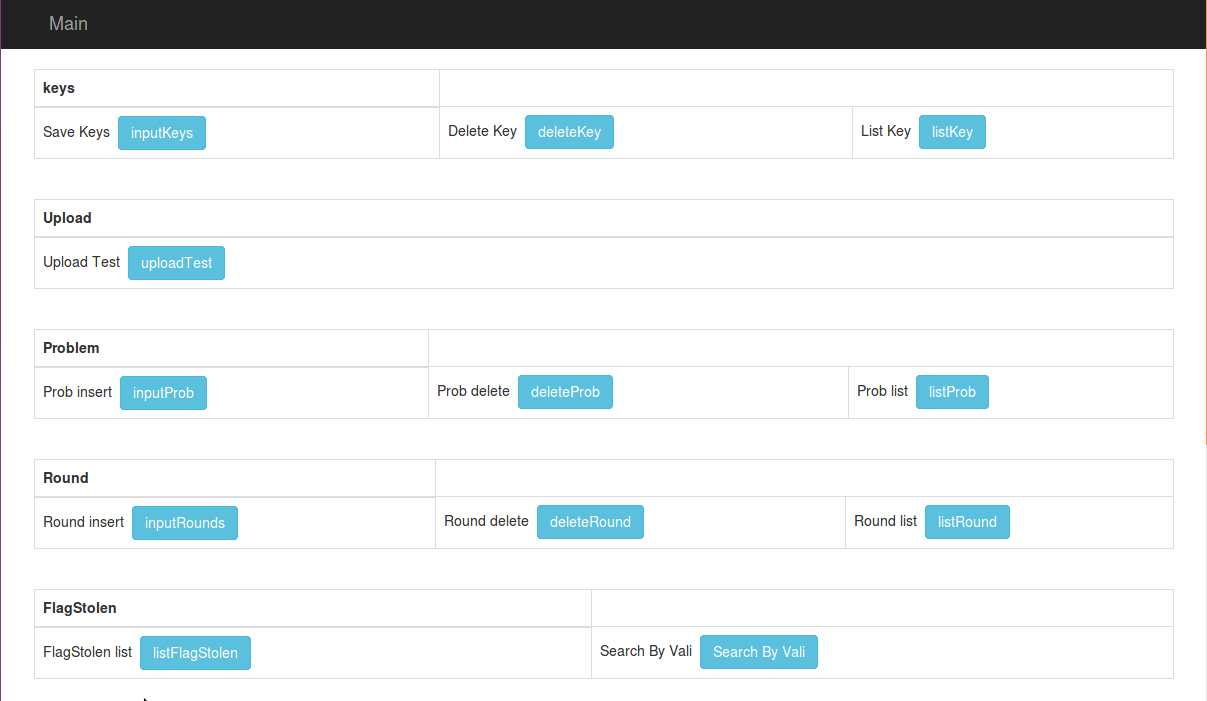
프론트 사용 설명

Main 화면



Main 화면 설명:

Keys: 플래그 키(값), 문제 아이디, 플래그 라운드와 관련된 기능 제공

Save Keys: DB에 입력 받은 문제 아이디, 플래그 라운드, 플래그 키(값) 저장

기능 사용을 위해 정해진 패스워드 입력 필요.

(KUICS 에서만 사용 하는게 좋을 것 같아 막아 두었습니다)

Delete Key: 문제 아이디, 플래그 라운드를 입력 받고 해당 (row)데이터를 DB에서 삭제

기능 사용을 위해 정해진 패스워드 입력 필요.

List Key: DB에 있는 플래그 키(값), 문제 아이디, 플래그 라운드로 구성된 row들을 보여줌

문제 아이디, 플래그 라운드를 입력해 특정 row 조회 가능

Upload: pcap 파일을 업로드 하는 기능 제공

Problem: 문제 아이디와 문제 이름 과 관련된 기능 제공

Prob insert: DB에 입력 받은 문제 아이디와 문제 이름 저장

기능 사용을 위해 정해진 패스워드 입력 필요

Prob delete: 문제 아이디를 입력 받아 해당 (row)데이터를 DB에서 삭제

기능 사용을 위해 정해진 패스워드 입력 필요

Prob list: DB에 있는 문제 아이디와 문제 이름으로 구성된 row들을 보여줌

문제 아이디를 입력해 특정 row 조회 가능

Round: 라운드 수, 라운드 시작 시간, 라운드 끝 시간과 관련된 기능 제공

Round insert: DB에 입력 받은 라운드 수, 라운드 시작 시간, 라운드 끝 시간 저장

기능 사용을 위해 정해진 패스워드 입력 필요

Round delete: 라운드 수를 입력 받아 해당 (row)데이터를 DB에서 삭제

기능 사용을 위해 정해진 패스워드 입력 필요

Round list: DB에 있는 라운드 수, 라운드 시작 시간, 라운드 끝 시간으로 구성된 row들을

보여줌. 라운드 수를 입력해 특정 row 조회 가능

FlagStolen: 백핸드에서 넣은 공격 패킷에 대한 정보를 조회하는 기능 제공

FlagStolen list: 모든 문제에서 공격을 받았는지 검색 후 공격을 받았으면 관련 데이터 제공

Search By Vali: 공격 패킷을 위험성에 따라서 관련 데이터 제공

Packets: DB에 저장된 패킷들과 관련된 정보를 조회하는 기능 제공

tcpAndUdpSearch: 전체 패킷을 tcp나 udp로 분류해서 조회한다.

datetime Search in raw: 시작 시간과 끝 시간을 5분 간격 이내로 지정하면 그 시간대 내

raw패킷을 조회하는 기능을 제공한다.

datetime Search in Tcp/Udp: 시작 시간과 끝 시간을 5분 간격 이내로 지정하면 그 시간대

안에 있는 Tcp/Udp 패킷을 조회하는 기능을 제공한다.

dstIpSearch: 패킷의 목적지 IP와 포트를 입력하면 해당 패킷을 조회하는 기능을 제공한다.

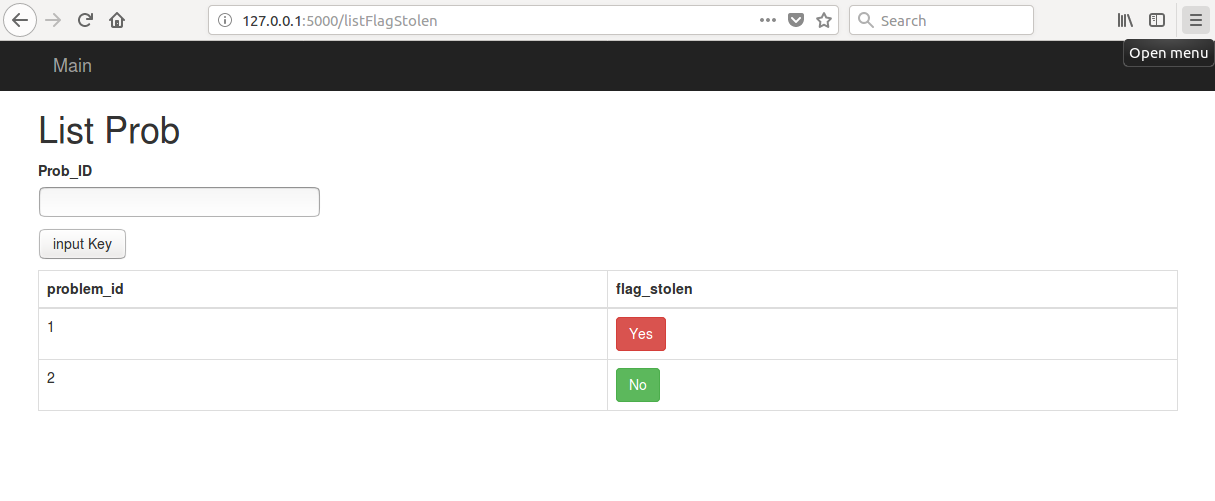
srcIpSearch: 패킷의 출발지 IP와 포트를 입력하면 해당 패킷을 조회하는 기능을 제공한다.

allSearch: IP와 포트 2쌍을 입력하면 해당 IP와 포트로 통신한 패킷들을 조회하는 기능을

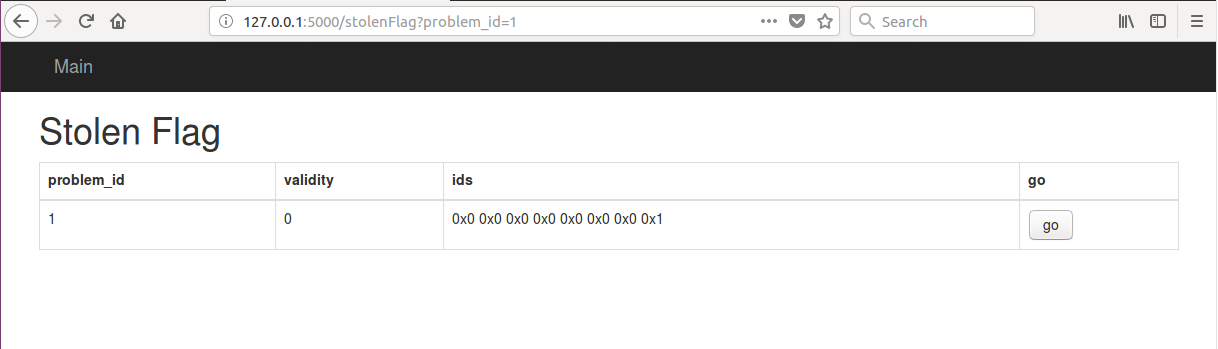
제공한다.

주요 기능 상세 설명

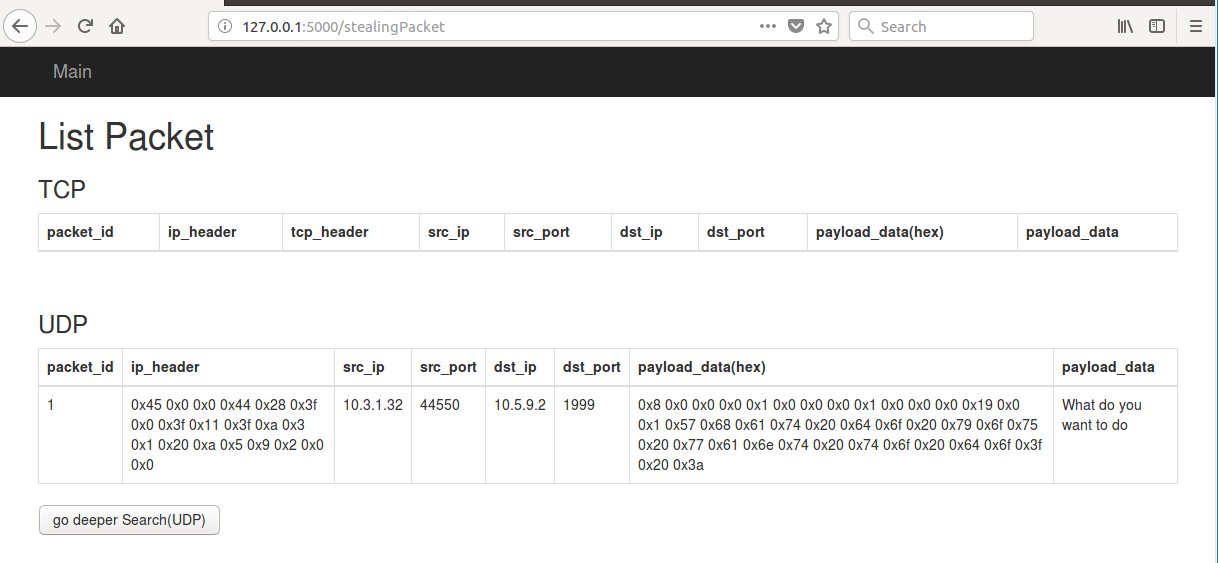
1. FlagStolen list



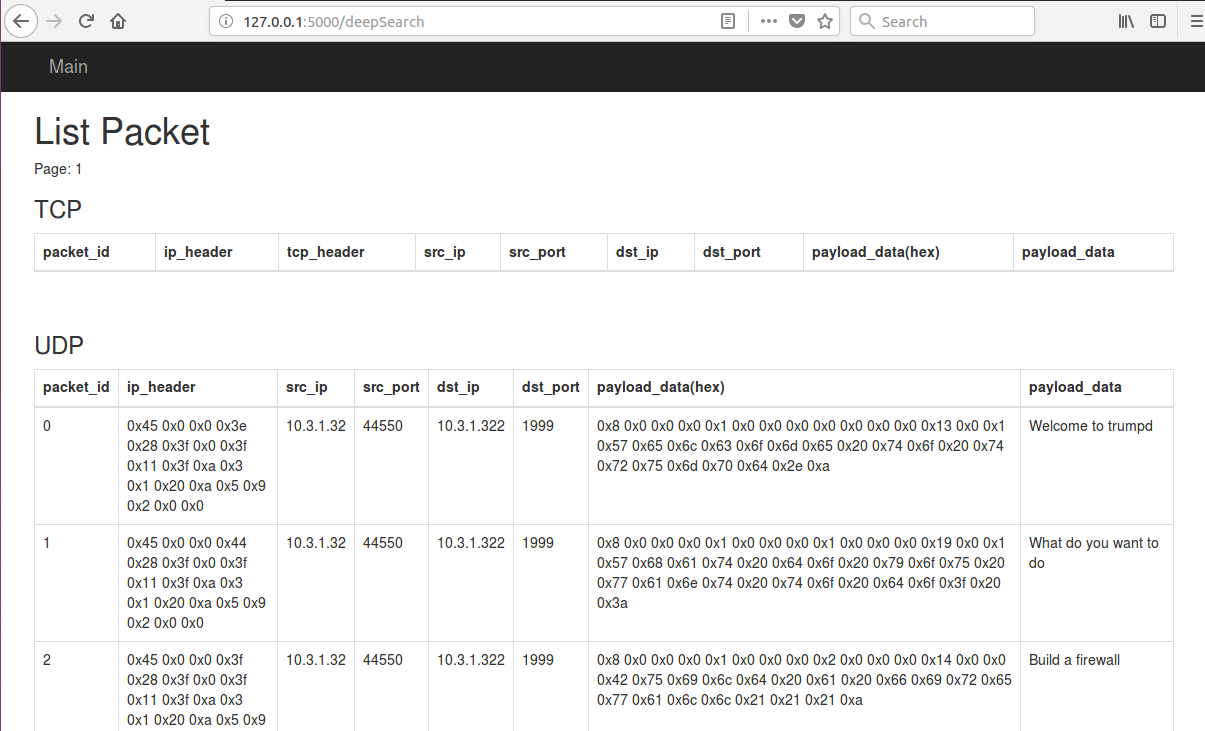
백에서 DB에 저장된 공격 패킷을 조회하는 기능을 제공합니다. 만약 해당 문제가 공격받지 않은 것으로 판단되면 No 라는 버튼이, 공격을 받은 것으로 판단 되면 Yes라는 버튼이 생성되어 어떤 패킷으로 공격 하였는지 조회 할 수 있습니다.



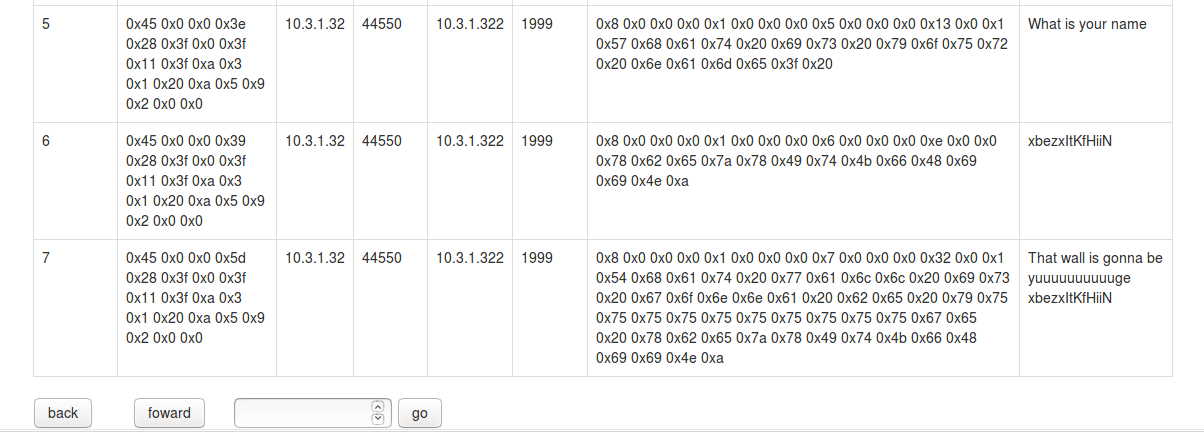
Yes라는 버튼을 누르면 공격 받은 문제 아이디, 공격의 위험성(유효성), 공격한 패킷 id들을 8비트 단위로 기록한 ids를 보여준다. Go 라는 버튼을 누르면 ids에서 공격 패킷 아이디를 가져와 상세 정보를 보여준다.



Go를 눌렀을 때 보여주는 화면이다. ids에서 패킷 아이디들을 꺼내 각 패킷 타입에 따라 TCP 테이블이나 UDP 테이블에 넣어 준다. 여기서 go deeper Search 버튼을 누르면 출발지 IP와 포트 도착지 IP와 포트를 쌍으로 서로 주고 받은 패킷을 보여준다.



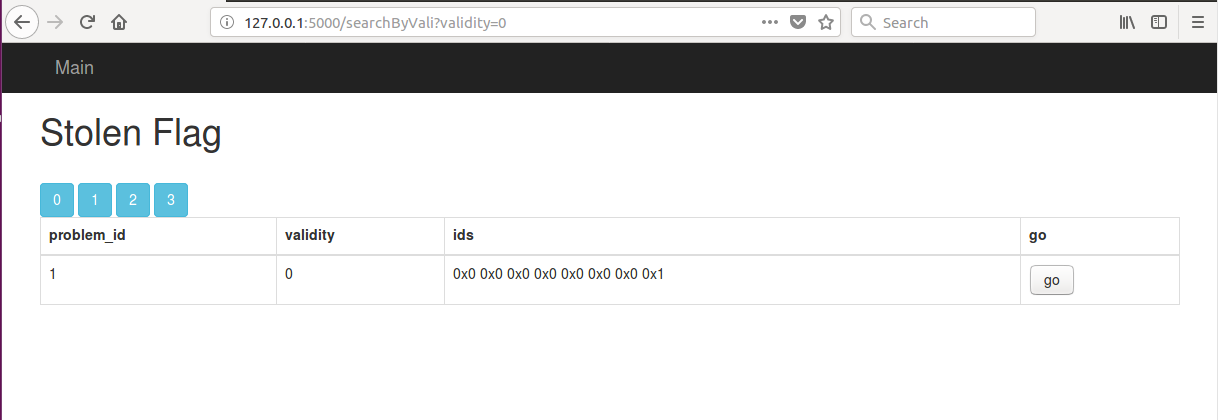
(/deepSearch의 윗부분)



(/deepSearch의 아랫부분)

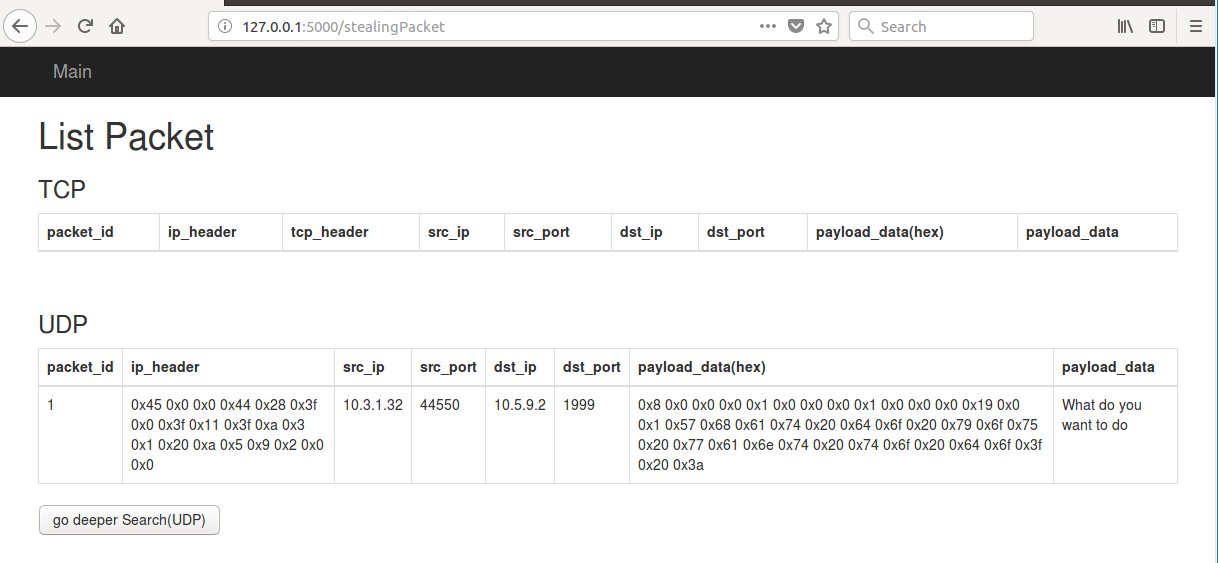
Go deeper Search 버튼을 눌렀을 시 이동하는 페이지이다. 패킷을 10개씩 페이지로 나뉘어서 조회 할 수 있도록 되어 있으며, 전 페이지나 바로 앞의 페이지로 가는 버튼들과 원하는 페이지 번호를 입력해 이동 할 수 있는 것이 제공된다.

2. Search By Vali



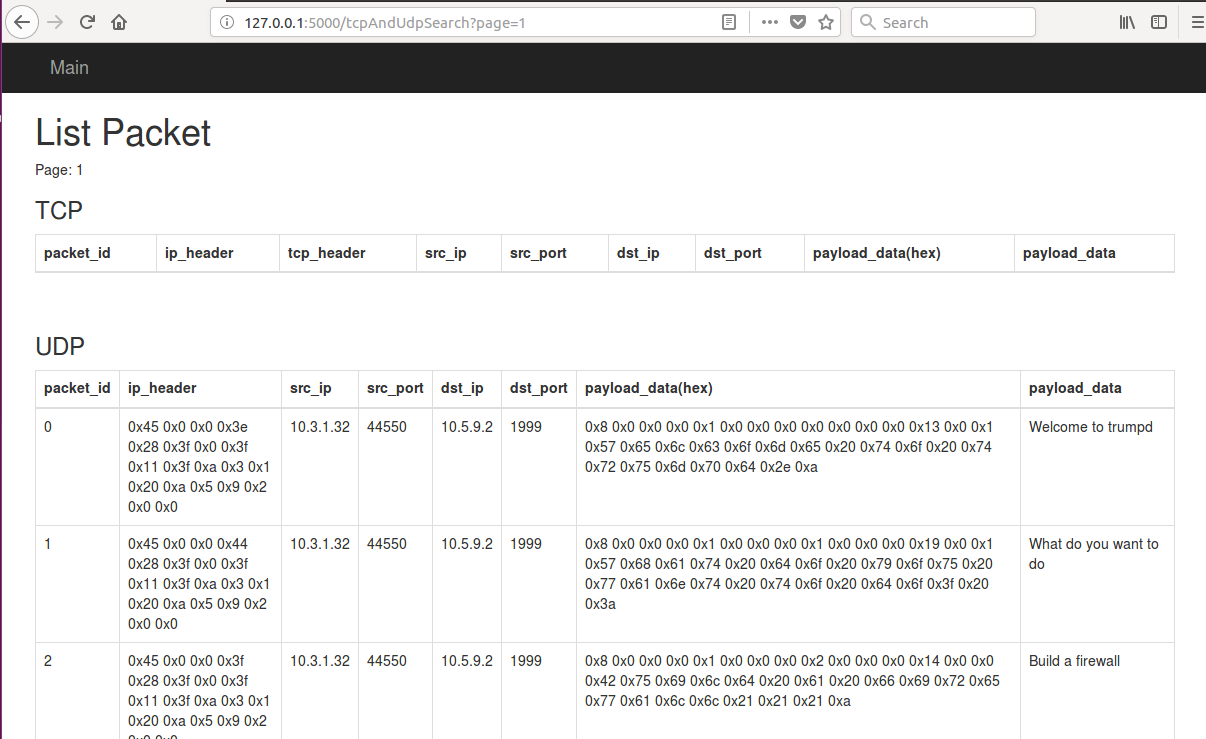
공격의 위험성(유효성)을 기반으로 검색하는 기능이다. 공격의 위험성(유효성)은 0~3의 값으로 정해지며 각 버튼을 누르면 각 값의 공격의 위험성(유효성)을 가진 공격들을 보여준다. Main 화면에서 넘어왔을 때는 0의 공격의 위험성(유효성)을 가진 것들을 검색한다.

Go 버튼을 눌렀을 시에는 ids에서 공격한 패킷 아이디들을 뽑아내 검색한다.

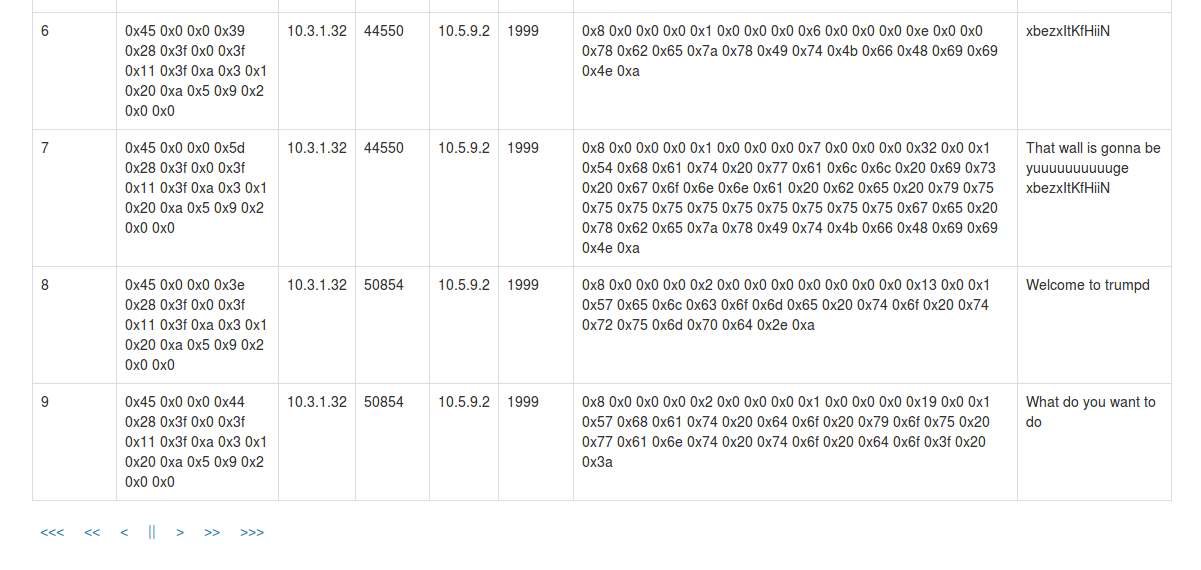


Go 버튼을 눌렀을 시에는 FlagStolen list의 경우에서와 같은 곳으로 이동하며(/stealingPacket) go deeper Search 또한 같은 기능을 제공한다.

3. tcpAndUdpSearch



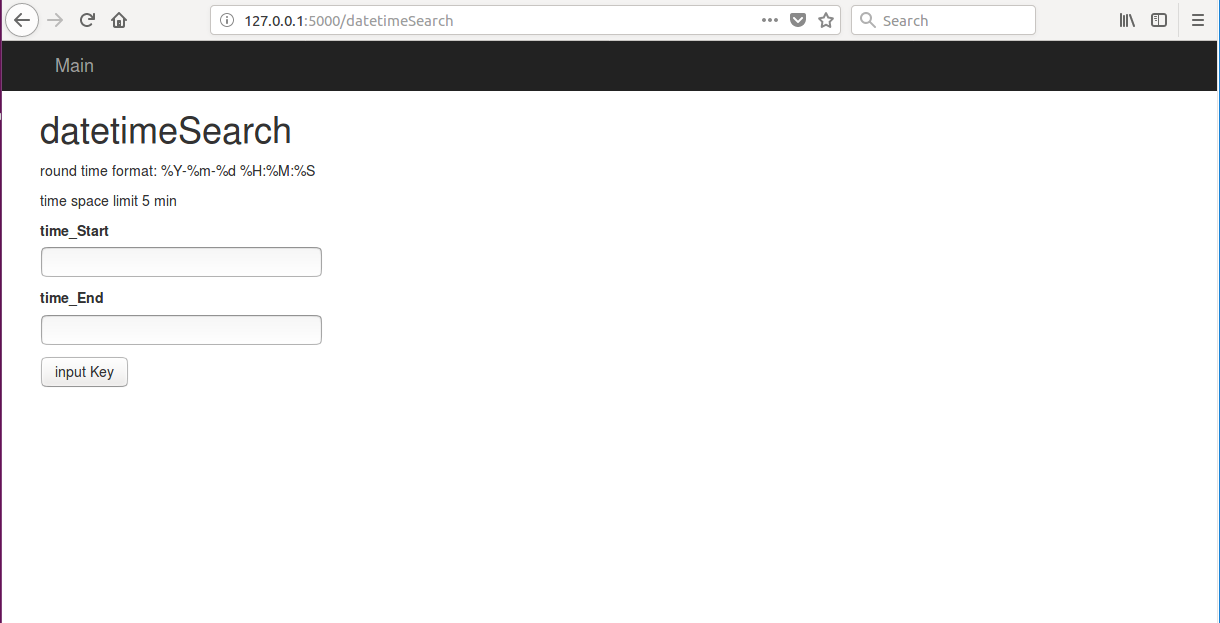
(/tcpAndUdpSearch 의 윗부분)



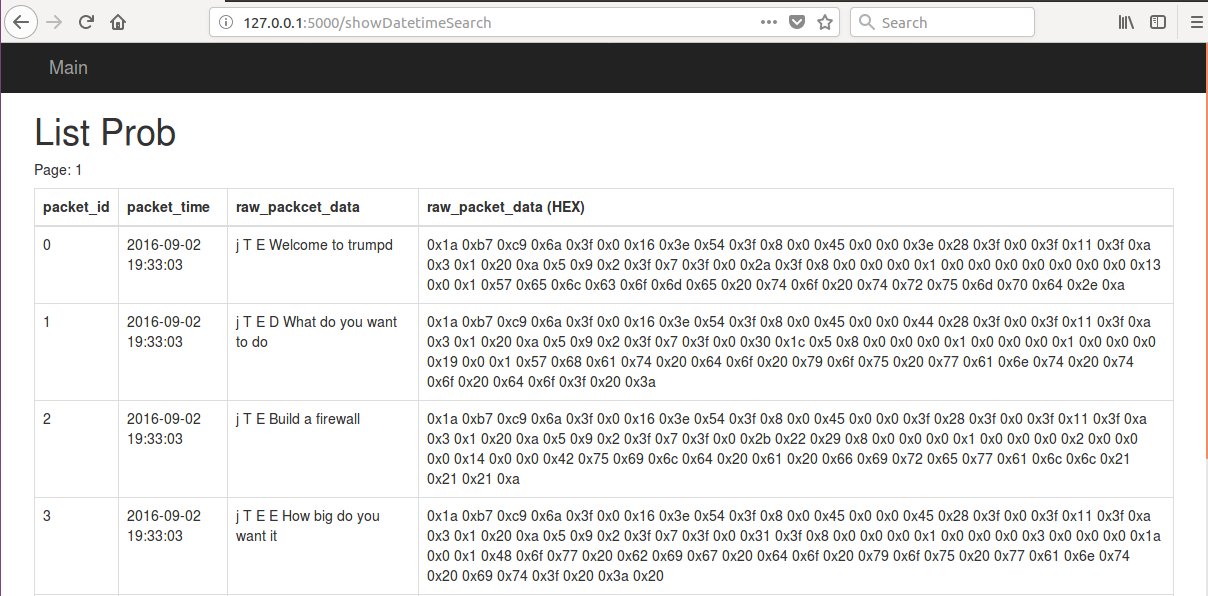
(/tcpAndUdpSearch 의 아랫부분)

이것은 지금까지의 패킷 전체를 10개씩 페이지 단위로 조회 할 수 있는 기능을 제공한다. 위의 <<<, <<, < 은 각각 3페이지, 2페이지, 1페이지 전으로 가는 링크이고 | |은 지금 페이지, >, >>, >>>는 각각 1페이지, 2페이지, 3페이지 앞으로 가는 링크이다. url인 /tcpAndUdpSearch?page=X 인 부분에서 X 부분을 바꾸어서 페이지를 이동 할 수도 있다.

4. datetime Search in raw / datetime Search in Tcp/Udp



5분의 시간 간격을 가진 검색할 시간대를 입력하면 그 시간대에 있는 패킷들을 보여주는 기능을 제공한다 time\_Start은 시작 시간 time\_End는 끝 시간이며 %Y-%m-%d %H:%M:%S의 형식(예: 2018-08-10 13:51:12)으로 입력해주면 된다

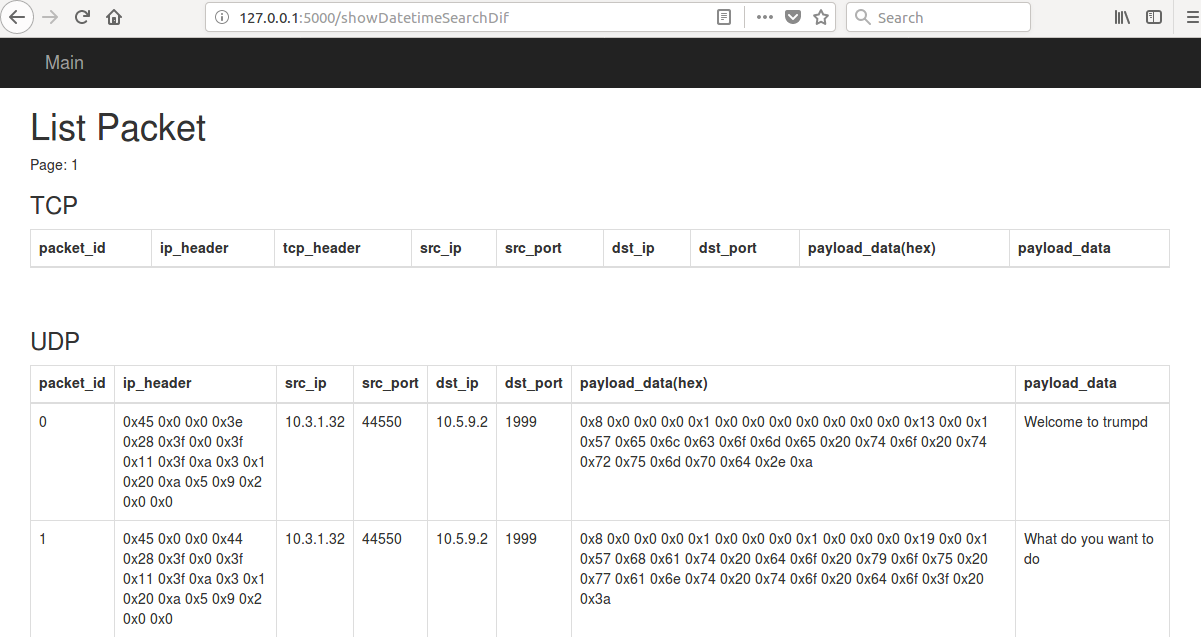


(/showDatetimeSearch 상단부)

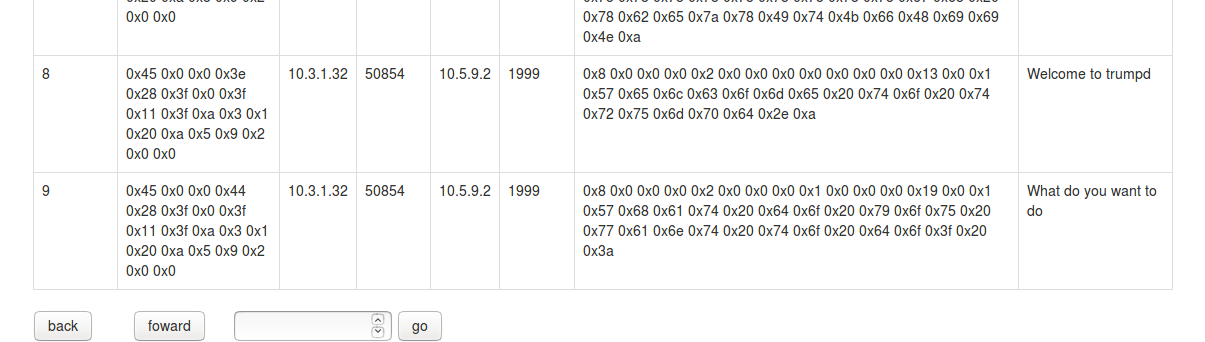


(/showDatetimeSearch 하단부)

datetime Search in raw는 설정한 시간대의 raw 패킷을 10개씩 페이지 단위로 보여주는 기능을 제공한다. 하단에는 바로 전이나 바로 앞의 페이지로 이동하는 버튼과 입력한 페이지로 이동하는 버튼이 있다.



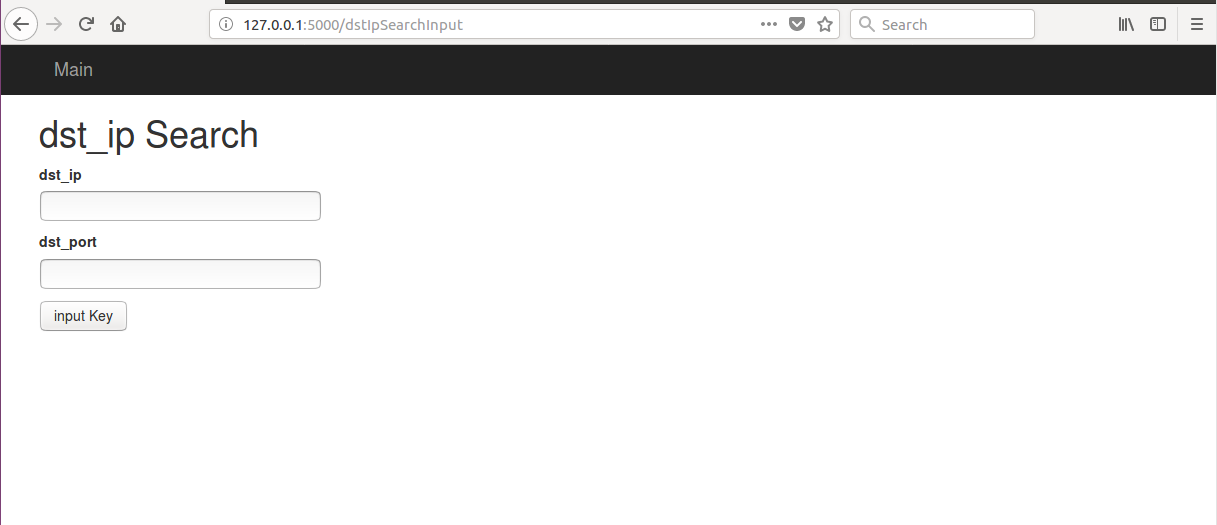
(/showDatetimeSearchDif 상단부)



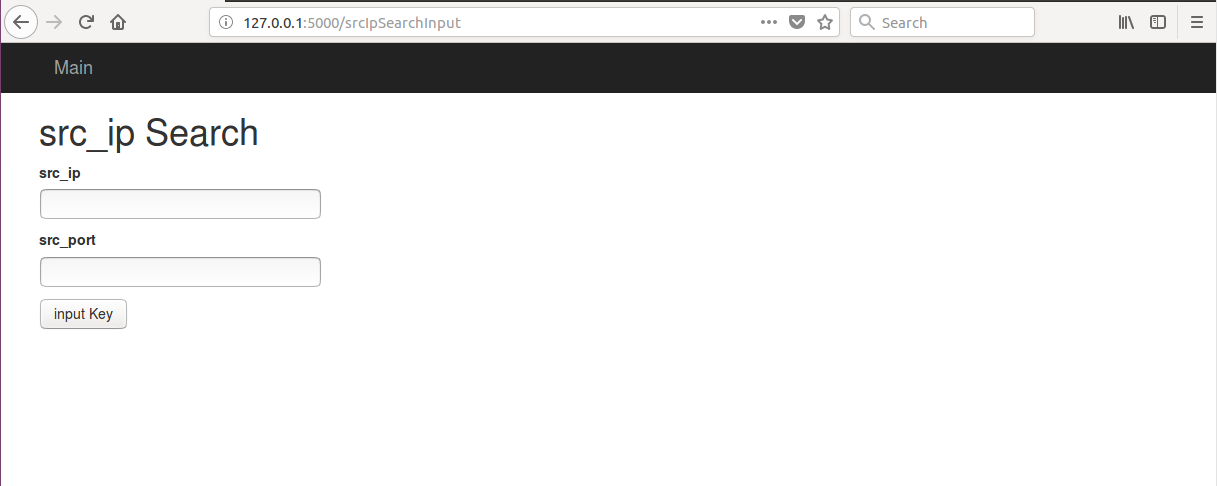
(/showDatetimeSearchDif 하단부)

datetime Search in Tcp/Udp는 raw 패킷이 아닌 tcp나 udp 패킷을 조회할 수 있게 해주는 차이가 있다.

5. dstIpSearch / srcIpSearch

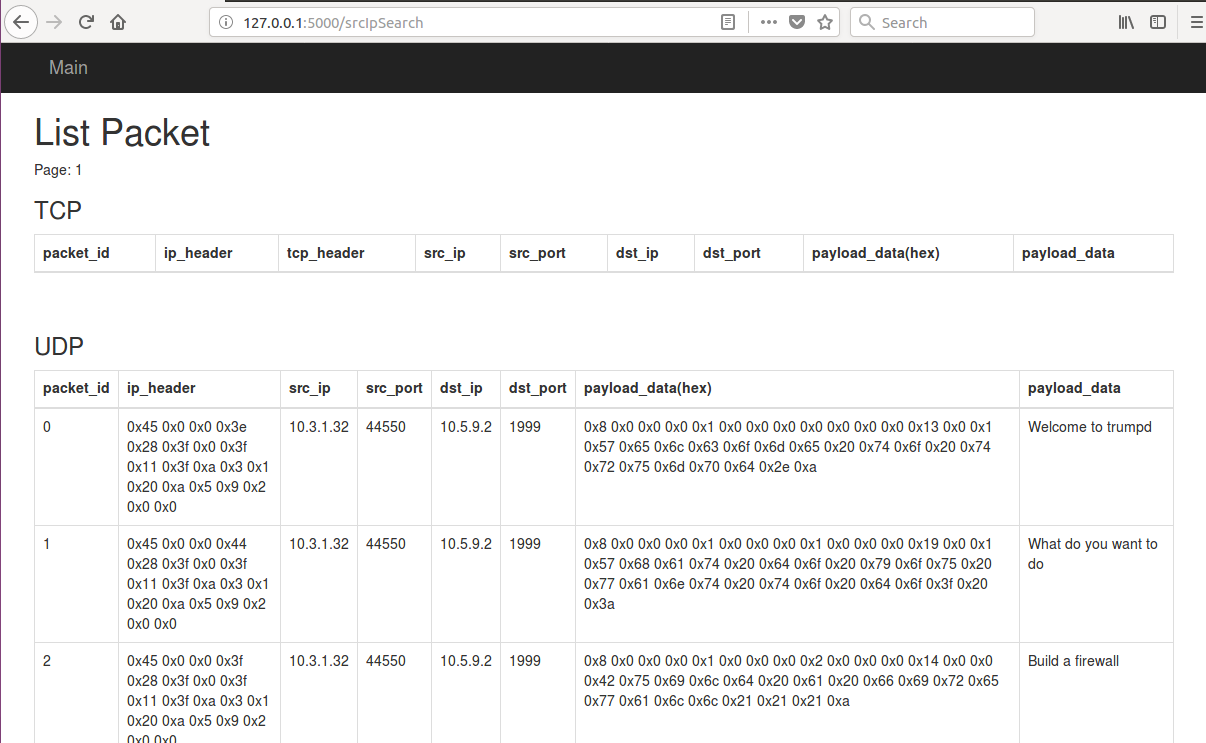


(/dstIpSearchInput)



(/srcIpSearchInput)

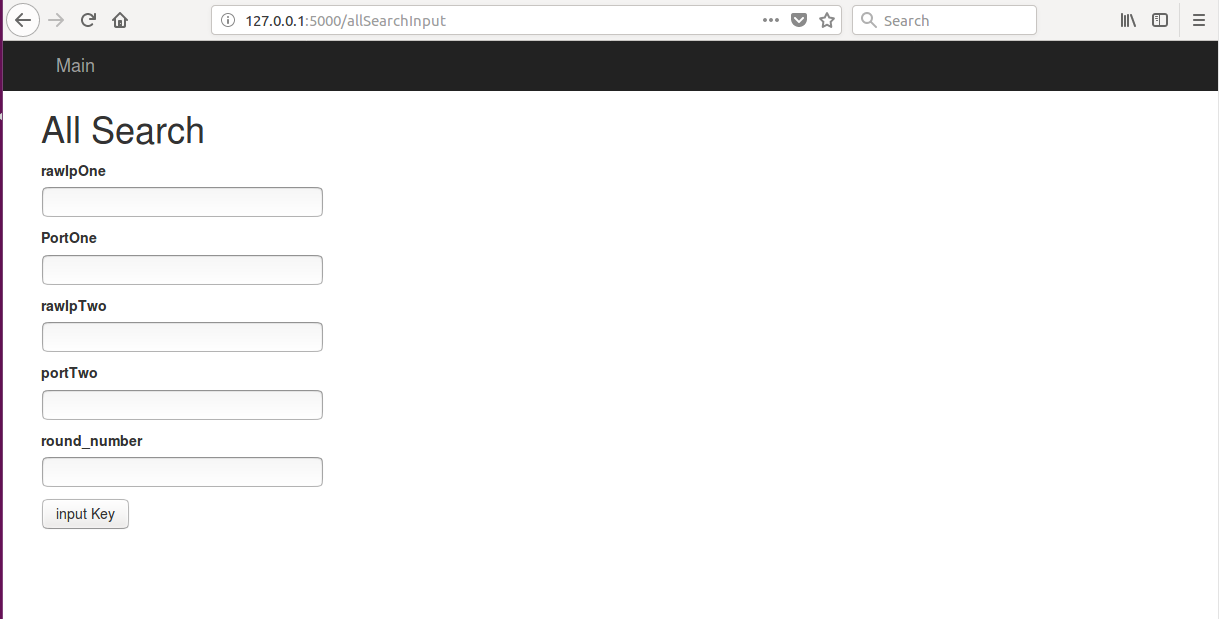
dstIpSearch에서는 목적지 IP와 포트 번호를, srcIpSearch에서는 출발지 IP와 포트 번호를 입력해 해당하는 패킷을 찾는 기능을 제공한다.



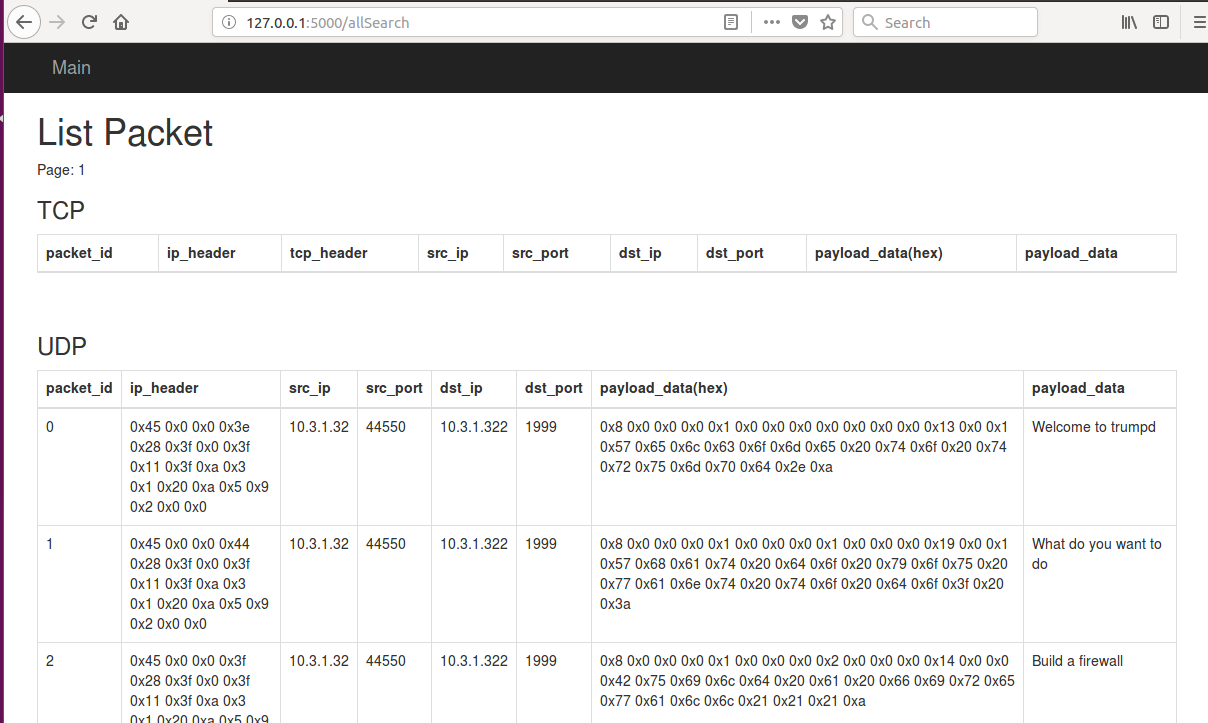
(/srcIpSearch 예시)

다른 조회 기능과 같이 dstIpSearch와 srcIpSearch는 입력에 맞는 (TCP or UDP)패킷을 10개씩 페이지 단위로 보여준다. 밑에는 바로 앞이나 바로 뒤의 페이지로 가는 버튼과 입력한 값의 페이지로 이동하는 버튼이 존재한다.

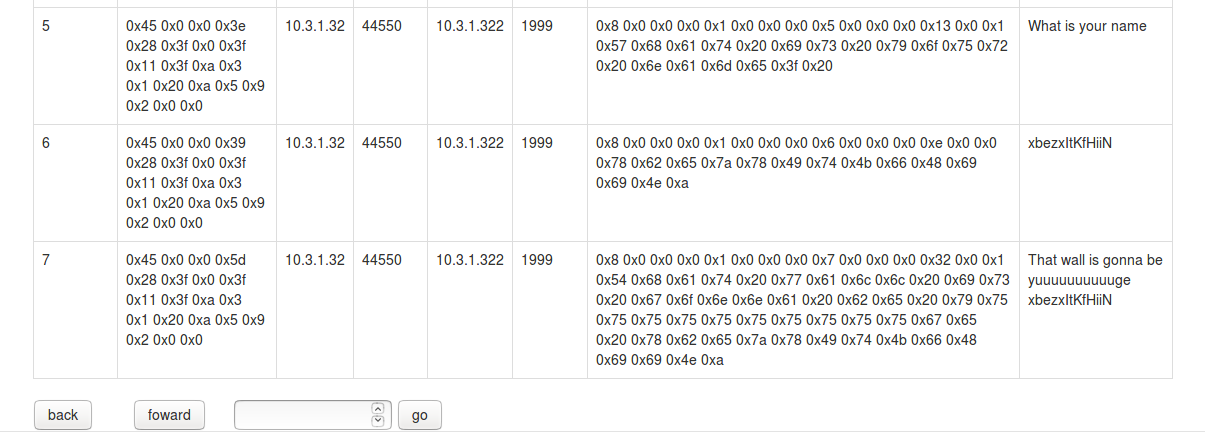
6. allSearch



allSearch에서는 라운드 수와 IP와 포트 두 쌍을 입력 받아 해당 라운드 내에서 해당 IP 포트를 가진 것들 사이의 통신 패킷을 조회하는 기능을 제공한다.



(/allSearch 상단부)



(/allSearch 하단부)

다른 패킷 조회 기능과 마찬가지로 10개씩 페이지 별로 (TCP or UDP)패킷이 조회가 되며, 하단부에는 바로 이전 페이지와 바로 이후 페이지로 넘어가는 버튼과 입력한 값의 페이지로 이동하는 버튼이 존재한다.