2. 목표 및 내용

2-2. 내용

2-2-1. 사용자 환경

본 프로그램은 Cross Platform을 지원하고, 설치에 관한 번거로움을 줄이기 위해 Web 어플리케이션의 형태로 제공된다. 이 때, 분석대상이 되는 덤프파일 사이즈가 클 경우, 실제 서버로 업로드 되는 시간이 길어지기 때문에 불편함을 초래할 수 있다. 하지만 웹 환경에서 작동하지 않을 경우, 사용자의 프로그램 접근성이 떨어지게 된다. 이에 따라 제품을 패키지화하여 사용자가 자신의 PC에 패키지를 설치하고 localhost의 지정된 포트를 통해 설치된 패키지를 이용할 수 있게 함으로써 이러한 문제를 해결할 것이며, 이러한 방식은 사용자가 패키지를 자신의 개인PC나 서버에 선택적으로 설치할 수 있게 한다. 이는 사용자가 프로그램을 자신의 스타일에 따라 설치하여 사용할 수 있다는 것을 의미한다.

2-2-2. 전체 프로세스

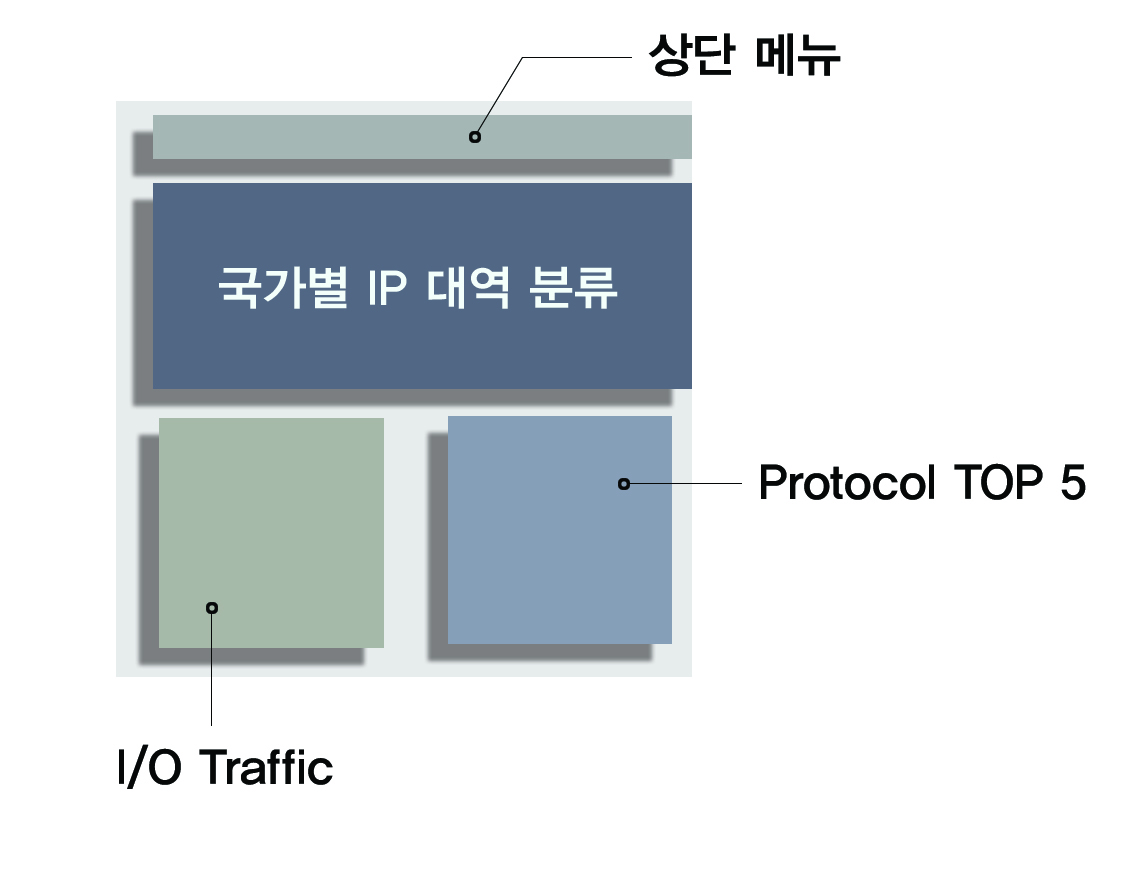
본 프로그램의 전체적인 프로세스는 다음과 같다.

  
[그림 2-1] 프로그램의 전체 흐름도

우선 사용자가 패킷 덤프파일을 업로드 하게 되면 대시보드의 그래프를 출력하기 위해 업로드 된 덤프파일에서 관련 정보를 추출해야 한다. 이를 위해 우선 덤프파일의 파싱작업이 수행되는데 이는 업로드 된 파일이 분석 가능한 덤프파일인지 판별하고, 대표적인 덤프파일의 포맷인 pcap과 pcap-ng포맷을 구분하여 파싱 작업을 수행한다.  
파싱을 하게 되면 덤프파일 내부에 존재하는 패킷들의 정보를 읽어올 수 있는데 각각 패킷별로 분할하여 파싱하게 되면 대시보드에 나타내야 할 정보들을 추출할 수 있다. 이렇게 추출된 정보를 분석결과라고 한다.  
분석결과를 도출하였다면 화면에 표시할 그래프별로 구조화 작업을 수행한다. 구조화 작업이란 Back-End 단에서 도출된 분석결과를 Front-End 단으로 전송하기 위함과 동시에 해당 분석결과를 사용자가 Save/Load 할 수 있도록 제공하기 위한 작업을 말한다. 분석결과를 구조화 할 때는 XML파일형태로 파일을 생성한다. XML파일로 분석결과를 구조화하면, Front-End와의 연동작업 시 간편하게 많은 정보를 체계적으로 전송할 수 있으며, Front-End 단에서 사용자의 분석파일을 Load하여 보여줄 때에도 통일된 모듈로 개발이 가능하다.

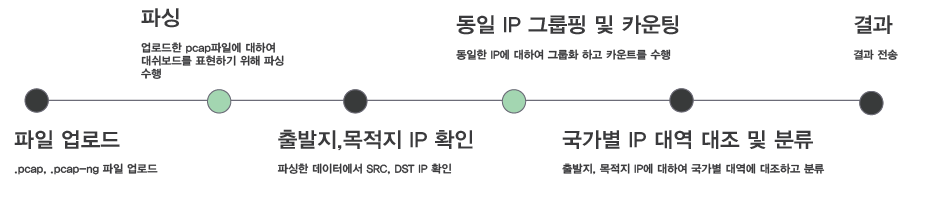
2-2-3. 대시보드 화면

분석 후 사용자에게 제일 처음으로 보여지는 화면이며, 다음 그림과 같이 구성되어 있다.



[그림 2-2] 대시보드 UI 구성

맨 상단에는 네비게이션 바가 위치하고 있다. 이곳에서 사용자가 원하는 형태의 통계정보를 선택적으로 제공받을 수 있다.  
다음으로 국가별 IP 대역 분류 정보가 제공된다. 이곳에서는 세계지도가 렌더링되며 트래픽이 집중된 국가일수록 진한 색으로 표기가 된다. 추가적으로 Inbound Traffic, Outbound Traffic을 구분하여 보여주어 In/Out Traffic의 흐름을 파악 할 수 있다. 국가별 IP 대역 분류는 다음과 같은 프로세스로 진행된다.

  
[그림 2-3] 국가별 IP 대역 분류 프로세스

국가별 IP 대역 분류의 하단에는 Input 및 Output 트래픽의 비율을 원형그래프의 형태로 보여준다. 사용자는 이를 이용해 덤프파일의 패킷흐름을 대략적으로 예측할 수 있다.  
우측에는 덤프파일 내 패킷들의 프로토콜 형태를 분류하여 가장 많이 사용된 5가지의 프로토콜을 보여준다. 사용자는 최종적으로 대시보드 화면을 통해 In/Out Traffic과 사용 Protocol에 대한 흐름 파악이 가능하다.

2-2-4.

