**Web Brower Based PCAP File Analyzer   
Development Proposal**

**2016. 01. 27**

**Written By : 유진영**

**<< Index >>**

1. **Overview**
   1. **Summary**
   2. **동작과정**
2. **시장조사 및 기존제품**
   1. **시장규모**
   2. **NetworkMiner**
   3. **Captcp**
   4. **Splunk**
   5. **Xplico**
   6. **Pcapr**
   7. **CapAnalysis**
3. **차별점**
4. **주요기능**
5. **기대효과**
6. **예상되는 문제점 및 해결방안**
7. **추후 관리 방안**

**1. Overview**

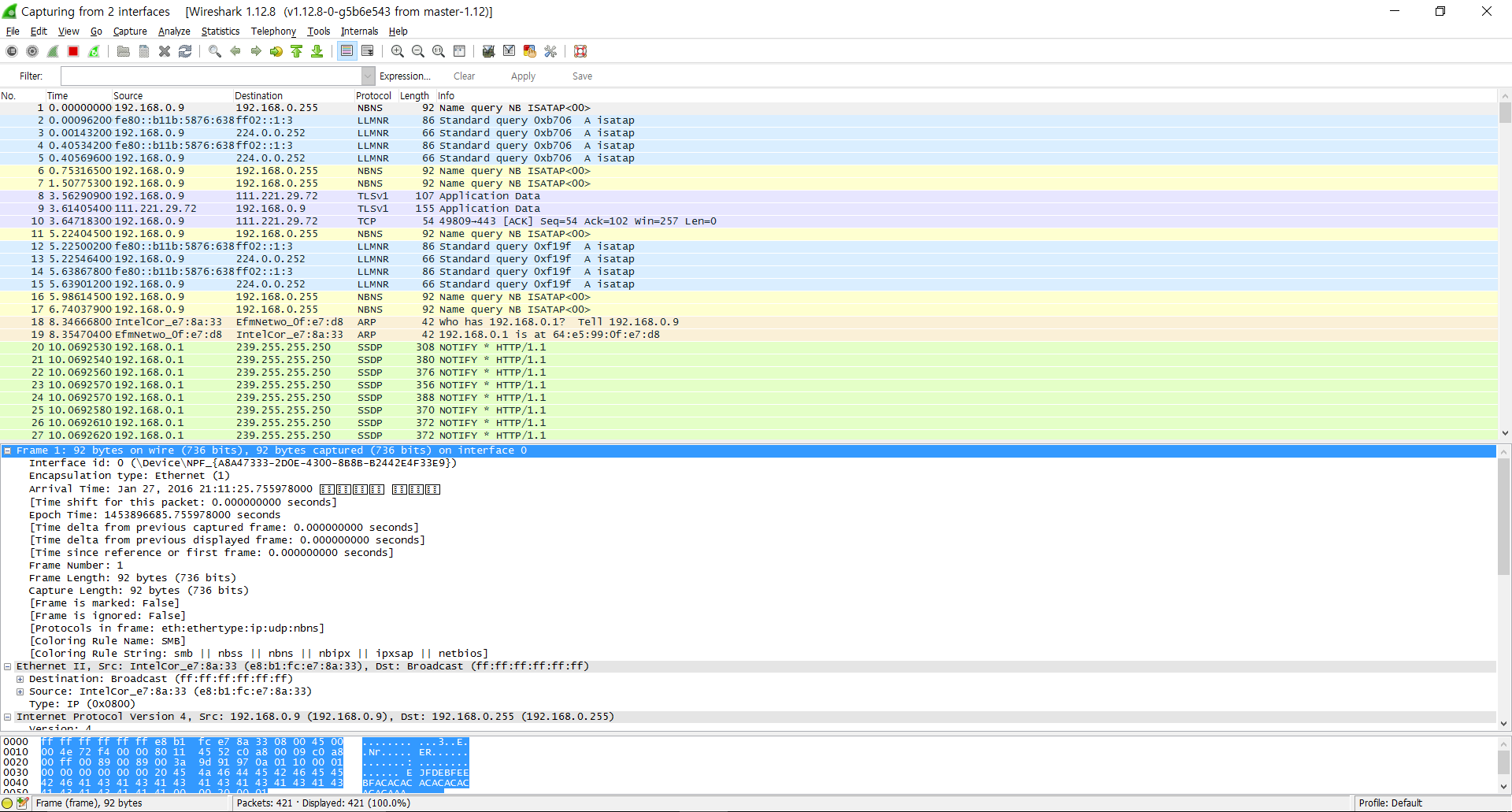
**1-1. Summary**

Digital Forensic 수사를 할 경우나 Capture the Flag(이하 CTF)대회 진행 시 네트워크 통신에 관한 분석 자료는 대부분 Wireshark기반으로 패킷 캡쳐를 하여 pcap 확장자 파일로 제공된다. 이 때 분석가의 편리함을 위해 pcap 파일의 Analyzer를 개발하여 제공하려 한다. 시장에서는 기존 pcap 파일 Analyzer 제품이 상당 수 존재하지만 그들이 공통적으로 제공하는 기능 외에 우리 제품만의 차별화된 기능을 제공함으로써 분석가의 편리함을 도모하고자 한다.

**1-2. 동작과정**

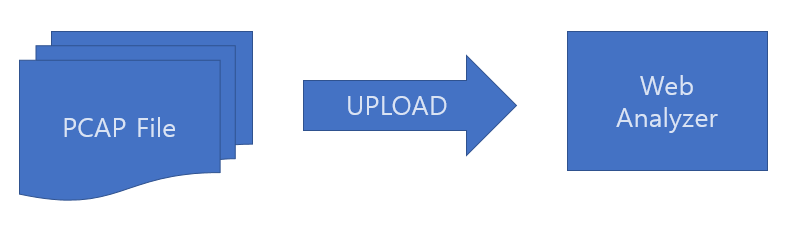
현재 개발하려는 제품은 다음과 같은 과정을 통해 이루어진다.

1. Wireshark를 통한 패킷 캡쳐 파일(PCAP File)생성 혹은 임의의 PCAP 파일 준비



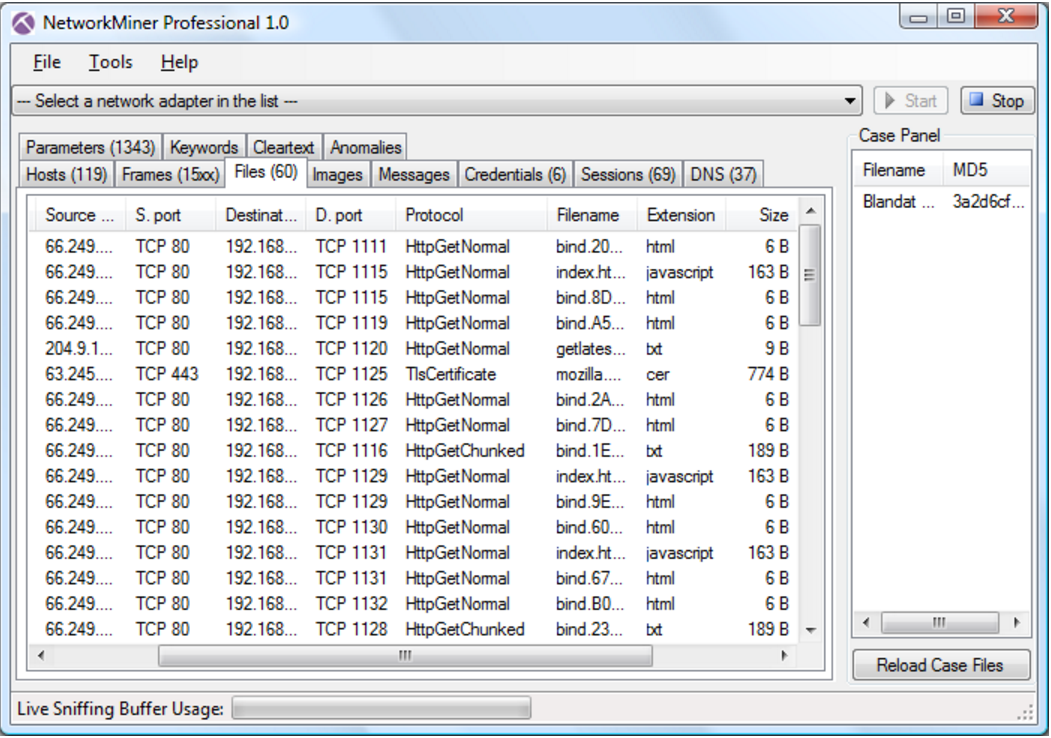
**[그림 1-1] Wireshark 패킷 캡쳐 화면**

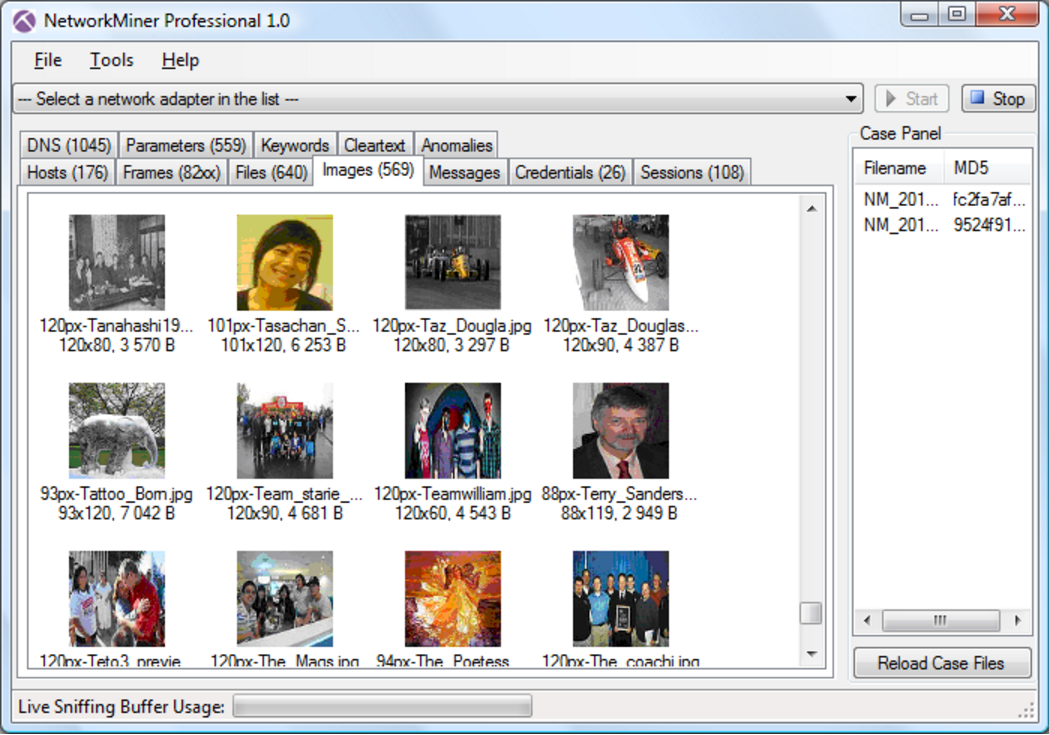
1. Web Site에 PCAP File 업로드.



**[그림 1-2] PCAP File Upload**

1. 생성된 분석보고서 열람





**[그림 1-3] 패킷의 분류에 따라 편리하게 열람할 수 있는 보고서 화면(기존제품 인용)**

**2. 시장조사 및 기존제품**

**2-1. 시장규모**

디지털 기기 사용이 늘어나면서 저장매체나 인터넷에 남아있는 각종 디지털 정보를 분석해 범죄 단서를 찾는 디지털 포렌식 수사가 증가했다. 수사기관에 한정됐던 디지털 포렌식 솔루션 시장은 최근 민간으로 영역을 확장했다. 특히 각종 전자거래 사고 발생시 금융기관이 디지털 증거를 입증해야 해 2015년 시장 규모는 2014년보다 두 배 이상 커질 전망이다. 2014년 디지털 포렌식 시장은 200억원 규모에 달한다. 이러한 디지털 포렌식 시장에서 네트워크 포렌식 시장을 대상으로 하며 해외시장도 고려한다면 충분한 경쟁력을 확보할 수 있을 것으로 기대된다.

**2-2. NetworkMiner**

그림 1-3의 두 가지 캡쳐화면을 보면, NetworkMiner의 주요기능을 한번에 알 수 있다. NetworkMiner는 PCAP파일을 Parse하여 내부에 캡쳐된 파일들을 보여주며, 그것을 다운로드 받을 수 있도록 해준다. 추가적으로 패킷 별 통신현황을 보여주는 기능이 있다.

**2-3. awesome-pcaptools**