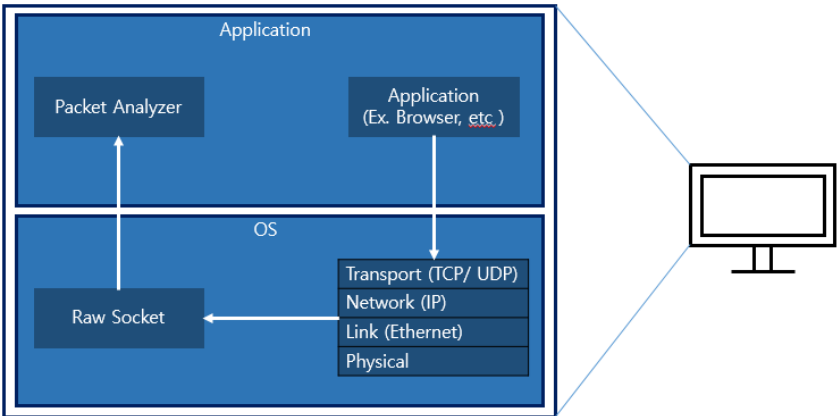
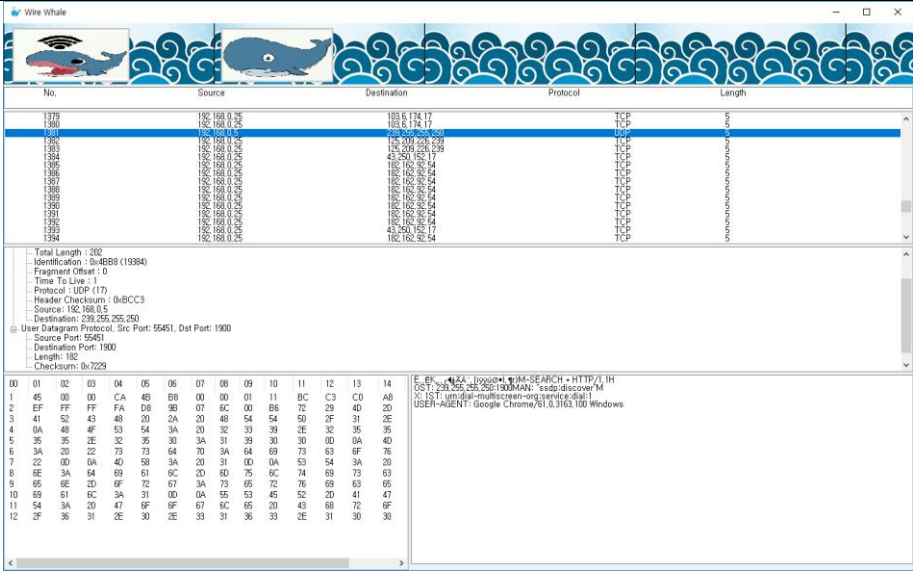


# 네트워크 패킷 스니퍼

프로젝트명	Packet Sniffer		
개발기간	2016.03 ~ 2016.04 - 1개월	개발인원	1명
개발환경	.NET Framework Winform		
개발 목적	<p>현대 시대에 대부분의 컴퓨터는 인터넷을 통해 연결되어 있으며, 이러한 인터넷은 많은 위험을 노출한 영역이다.</p> <p>다른 컴퓨터를 공격하기 위한 수단으로 대부분 네트워크를 통해 접근하며 이를 위해 네트워크 보안에 대한 이해가 필요하다. 따라서 네트워크에서 교환되는 패킷을 시각적으로 확인할 수 있는 프로그램을 구현하였다.</p>		
아키텍처	 <p>The diagram illustrates the architecture of the packet sniffer. It is divided into two main sections: 'Application' and 'OS'. In the 'Application' layer, there is a 'Packet Analyzer' and an 'Application (Ex. Browser, etc.)'. In the 'OS' layer, there is a 'Raw Socket' and a stack of protocols: 'Transport (TCP/UDP)', 'Network (IP)', 'Link (Ethernet)', and 'Physical'. Arrows show data flow: from the Application to the OS stack, and from the Raw Socket back to the Packet Analyzer. A computer icon is shown to the right, representing the host.</p>		
개발내용	 <p>The screenshot shows the Wireshark interface with a list of captured packets. The selected packet is a UDP packet from 192.168.0.5 to 192.168.0.5. The packet details pane shows the 'User Datagram Protocol' section. The packet bytes pane shows the raw data in hexadecimal and ASCII.</p> <ul style="list-style-type: none"> <li>- 원시 소켓을 이용한 패킷 캡처</li> <li>- 프로토콜에 따른 패킷 파싱 (Ethernet, IP, TCP, UDP 프로토콜 파서 구현)</li> </ul>		
소스코드	X		
시연영상	X		