기술문서	2016-10-21

quiz 프로젝트

최종 보고서

작성자 : quiz 프로젝트

KITRI 제13기 모의해킹 과정

김남용

개 정 이 력

개정번호	개정 내용 요약	개정일자
1.0	최초 제정 승인	2016-10-21
1.1	단어 수정	2016-10-21

문 서 규 칙

KITRI 지식경제부 산하기관 한국정보기술연구원	quiz 프로젝트 최종 보고서			④
	Category	첨부파일 버전	문서 최종 수정일	
	①	②	③	

- 작성 및 확인은 Microsoft Word 2007으로 작성 되어 졌으며, Acrobat Reader로 읽는다.
- Category(①)에는 Manual, Utility, Tip, Analysis Report 로 구분하며, 기재된 정보가 Manual과 Utility가 혼합된 경우에는 "Manual + Utility" 라고 표기되며, 머리글의 Category에 해당 구분 정보를 표기된다.
- 본 문서의 주제가 되는 대상은 오른쪽 큰 여백에 기재된다. (④)
- 첨부 파일 버전(②)은 첨부 파일이 존재하는 경우에 기재되며, 첨부 파일의 버전이 표기된다. (유틸리티의 경우 최종 버전은 날짜 표기 대신 버전으로 대체한다)
- 문서 최종 수정일(③)에는 문서의 최종 수정날짜가 표기된다.

목 차

그림목차

1. 개요

가. 의의

quiz 프로젝트를 통한 패킷 분석 프로젝트 작성

나. 목적

▶ wireshark 분석하는 방법을 알아본다.

▶ 패킷 분석을 통한 문제풀이와 프로젝트 경험을 쌓는다.

▶ 효율적인 툴의 사용 예시를 보여준다.

▶ 분석 과정을 바탕으로 파일 분석 과정을 정리하여 제시한다.

2. quiz프로젝트 분석 과정

가. 분석 환경

▶ VMWare 11.0

▶ Windows XP SP3 32bit

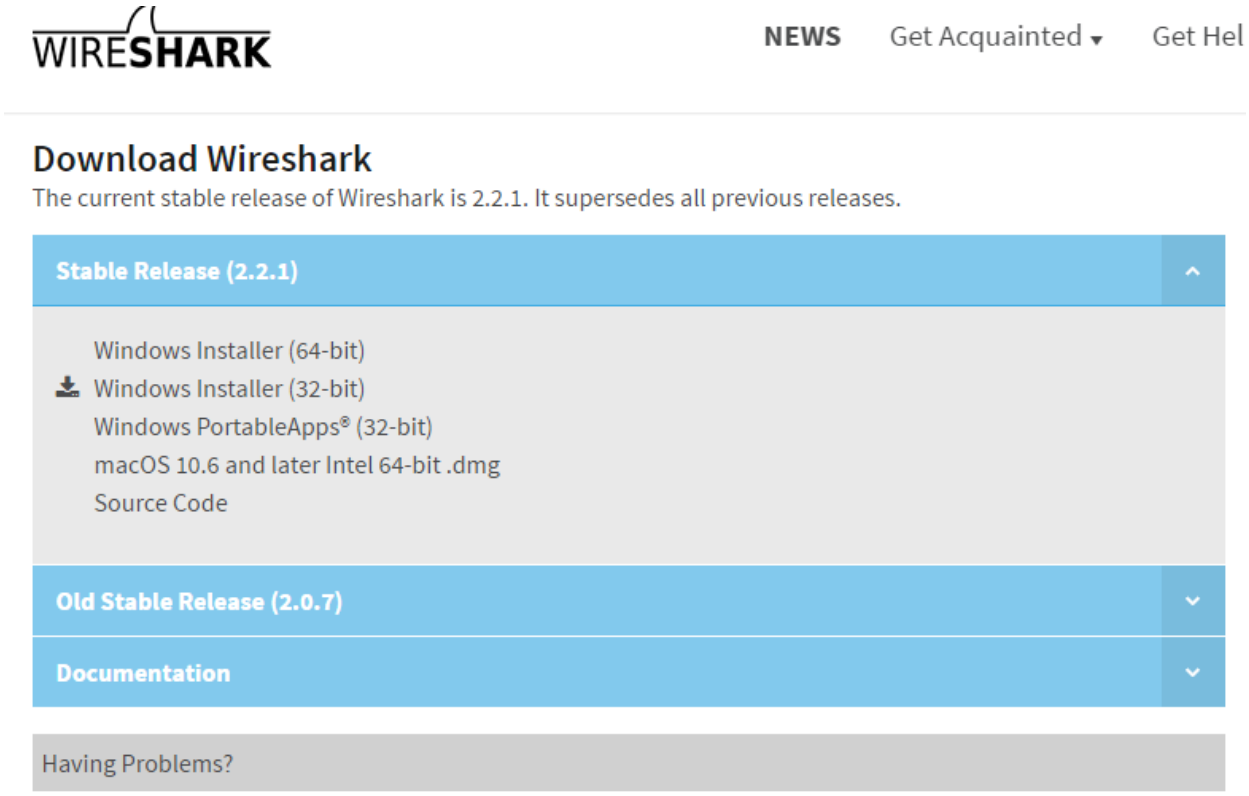
나. 분석 도구

명칭	설명	UI
WireShark	패킷 분석을 통한 분석 과정 정리 다운로드 사이트	

다. 분석 도구 활용

1) WireShark 사용

패킷 분석하기 위해 먼저 wireshark 다운 받은 후 압축을 해제하면 [그림-1]의 파일들을 확인할 수 있다.



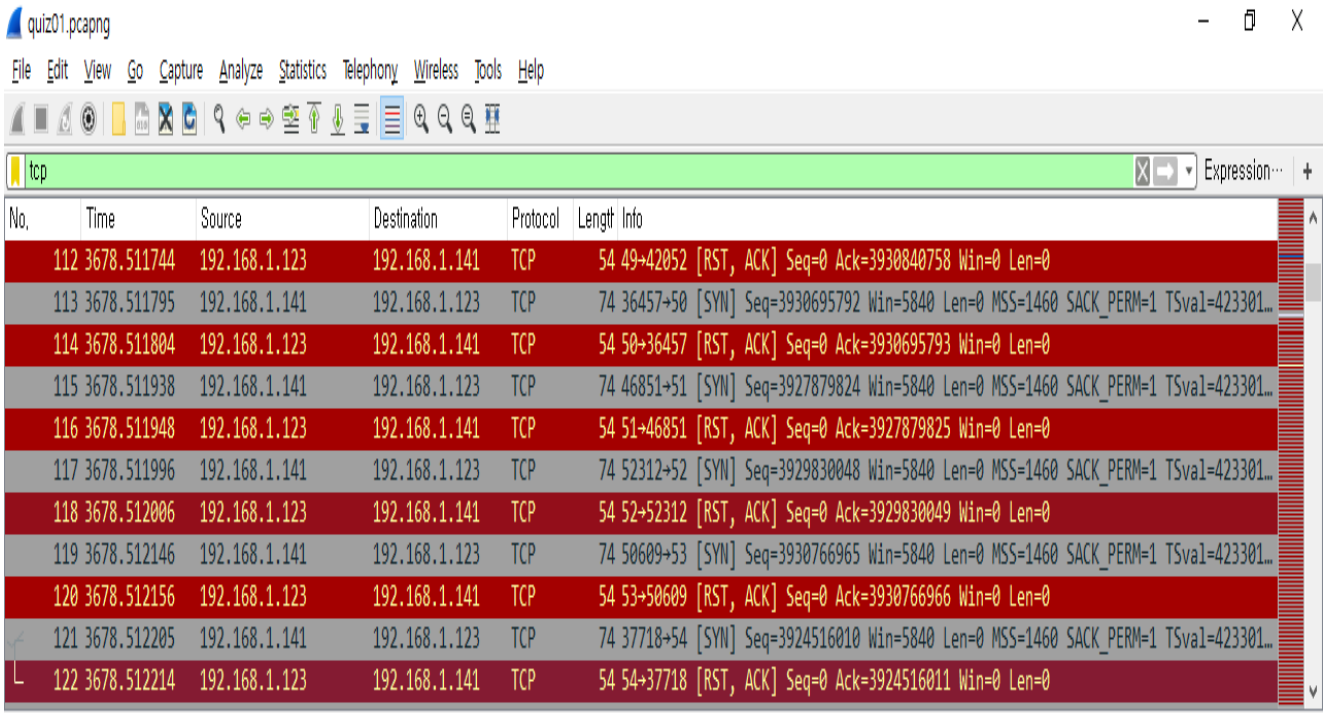
[그림-1. WireShark]

WireShark를 다운로드를 통해 분석을 시작 할 수 있습니다.

3. 패킷 분석 사례

가. Quiz01 문제 풀이

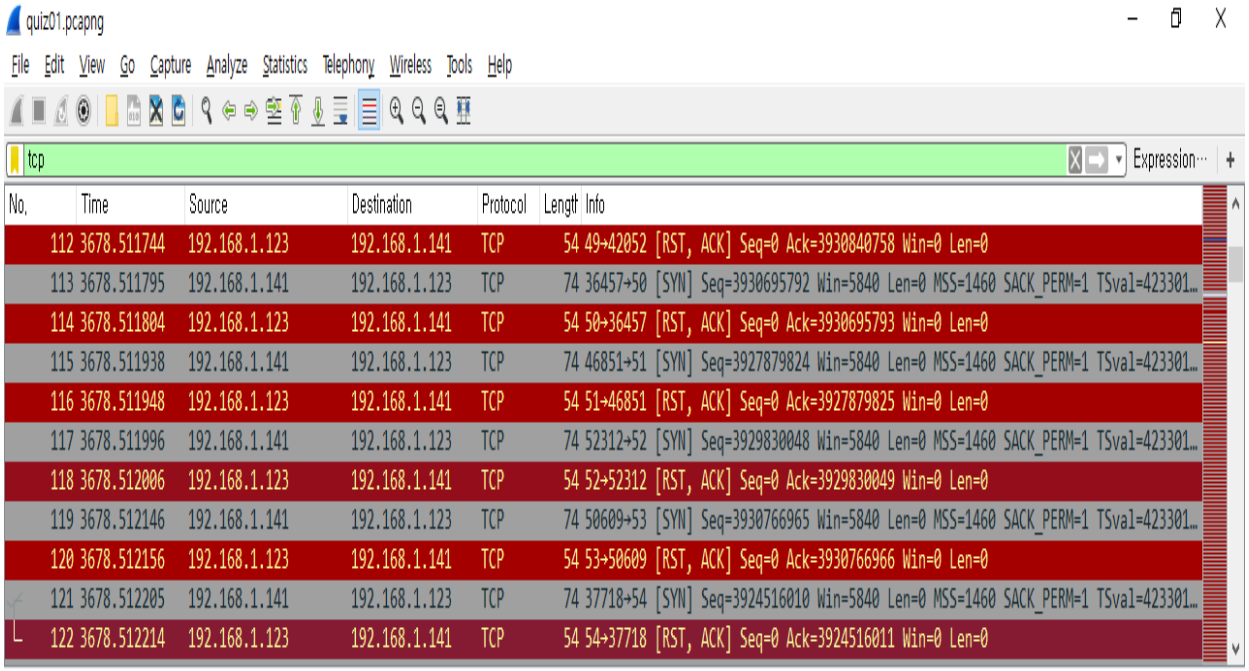
1) 공격자 호스트의 IP 주소는 무엇인가?



[그림-2. 공격자 호스트 IP 주소]

계속적인 포트 스캔으로 192.168.1.123 -> 192.168.1.141 공격하는 모습을 보여준다.

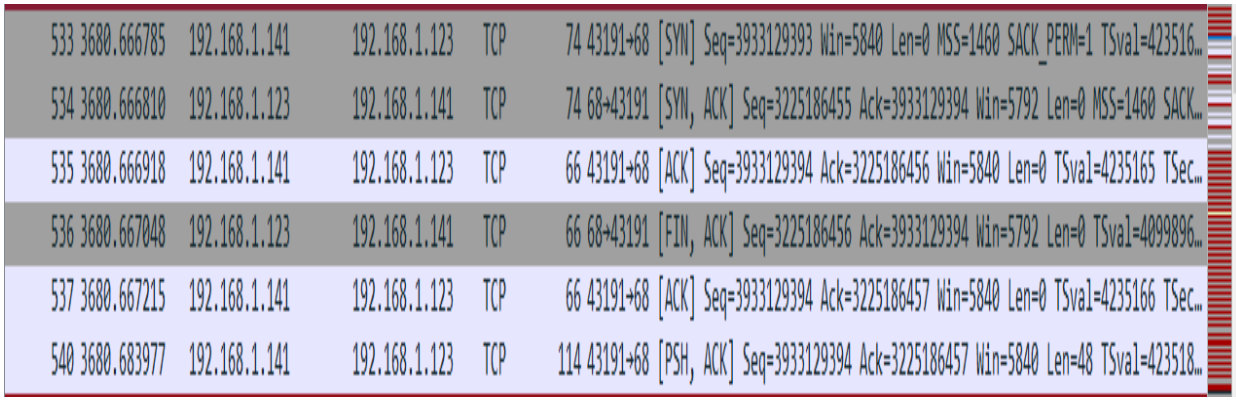
2) 대상 호스트의 IP 주소는 무엇인가?



[그림-3. 대상자 호스트 IP 주소]

계속적인 포트 스캔으로 192.168.1.141 -> 192.168.1.123 공격받는 모습을 보여준다.

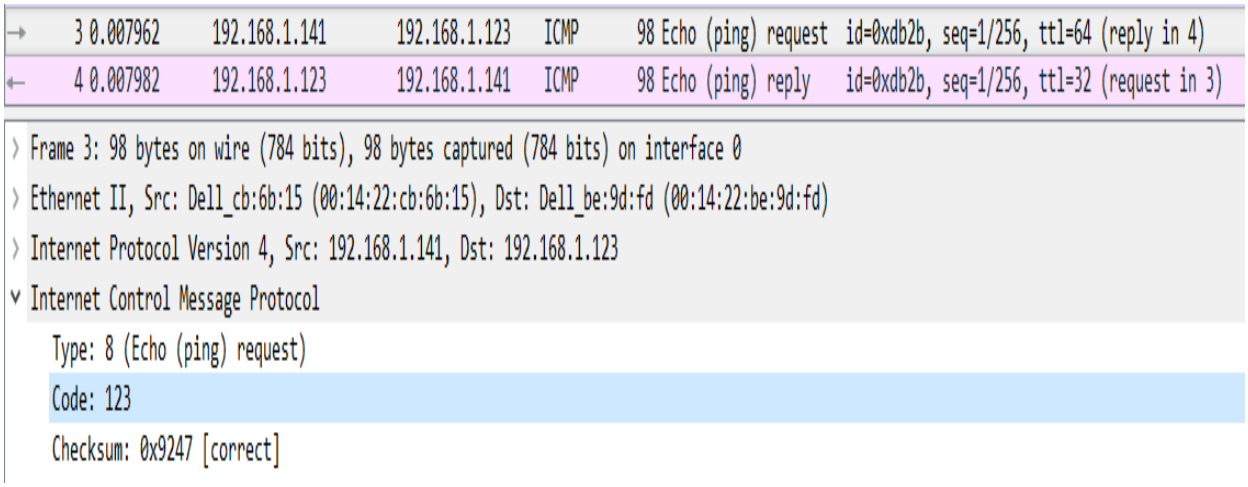
3) 대상의 어떤 TCP 포트가 열려 있는가?



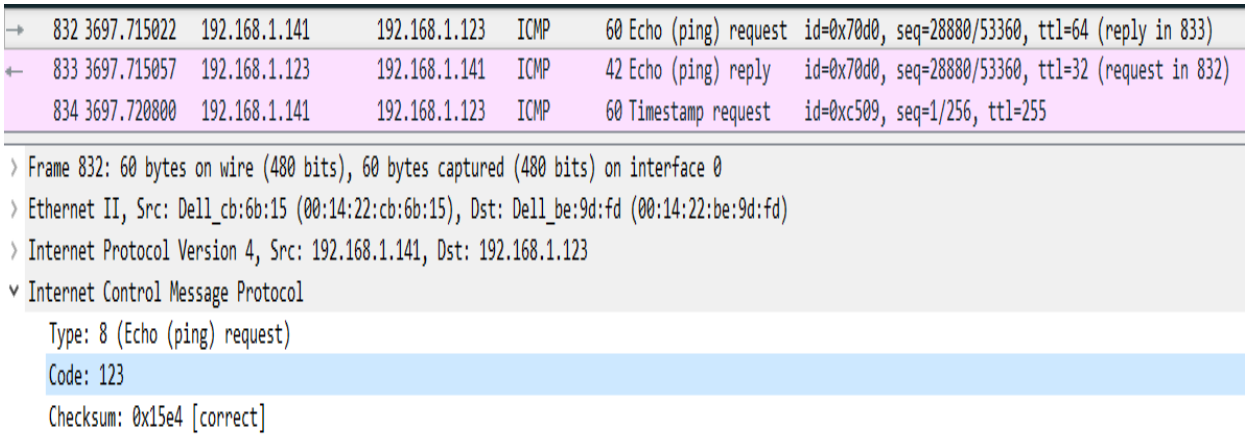
[그림-4. 열려있는 포트]

68(UDP)포트가 열려있으며, 요청,요청+응답,응답,마침+응답,응답 상태로 제대로 통신이 오가며, 열려있는 포트임을 확인할 수 있습니다.

4) 어떤 ICMP의 비 표준형 / 코드 번호가 포함되어 있는가?



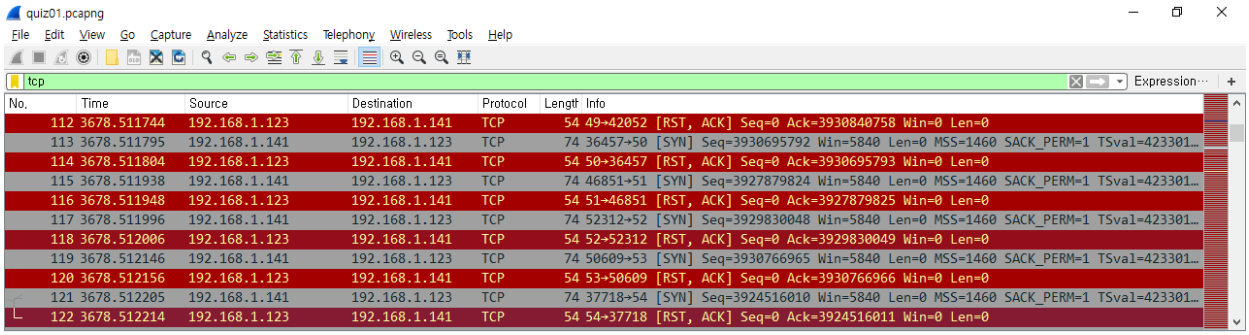
[그림-5. ICMP 비 표준형과 코드번호]



[그림-6. ICMP 비 표준형과 코드번호]

ICMP 프로토콜에서 Code : 123은 비표준형 코드이며 그것의 코드번호는 3,4번과 832,833번을 발견할 수 있습니다.

5) 대상을 스캔 하는데 어떤 소프트웨어를 사용 하였는가?

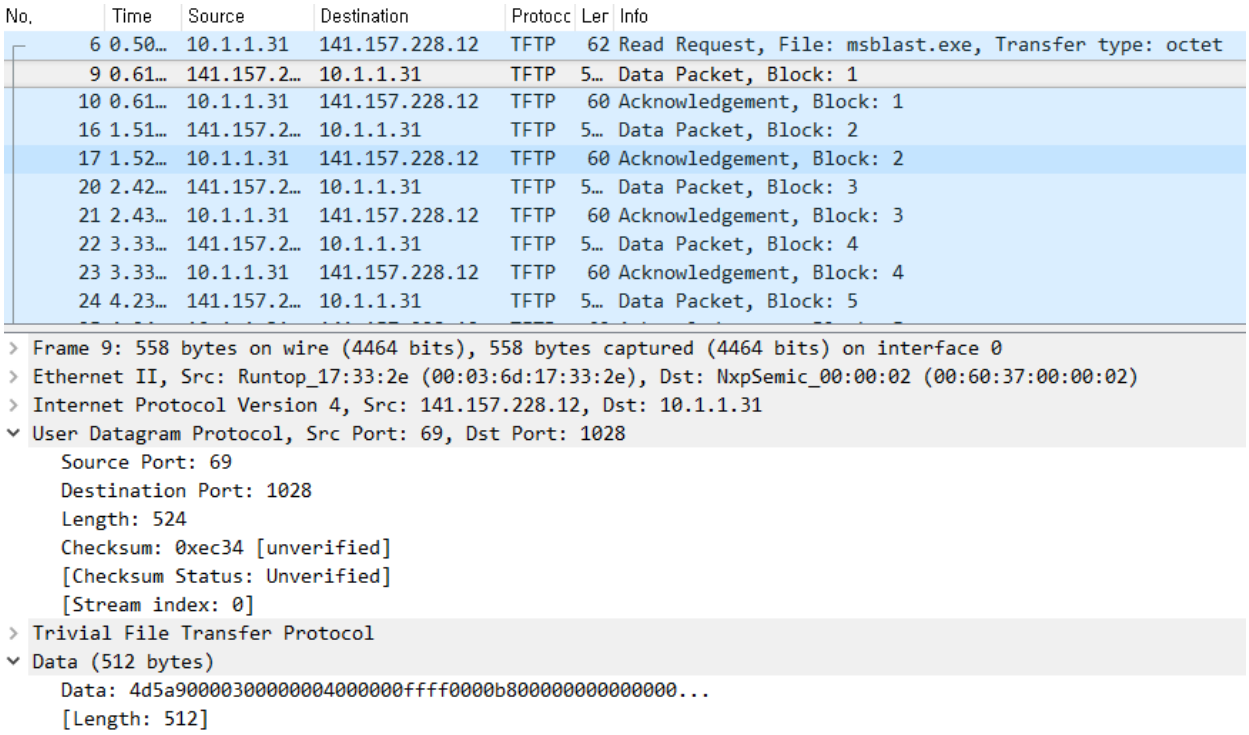


[그림-7. 포트 스캔 nmap 사용]

짧은 시간 동안 많은 패킷이 유입되었으며, 그 중 1 ~ 8081 그 이상까지 포트 스캔된 것을 확인하면 nmap을 통한 포트 스캔이 이루어졌다는 것을 확인 할 수 있습니다.

나. Quiz02 문제 풀이

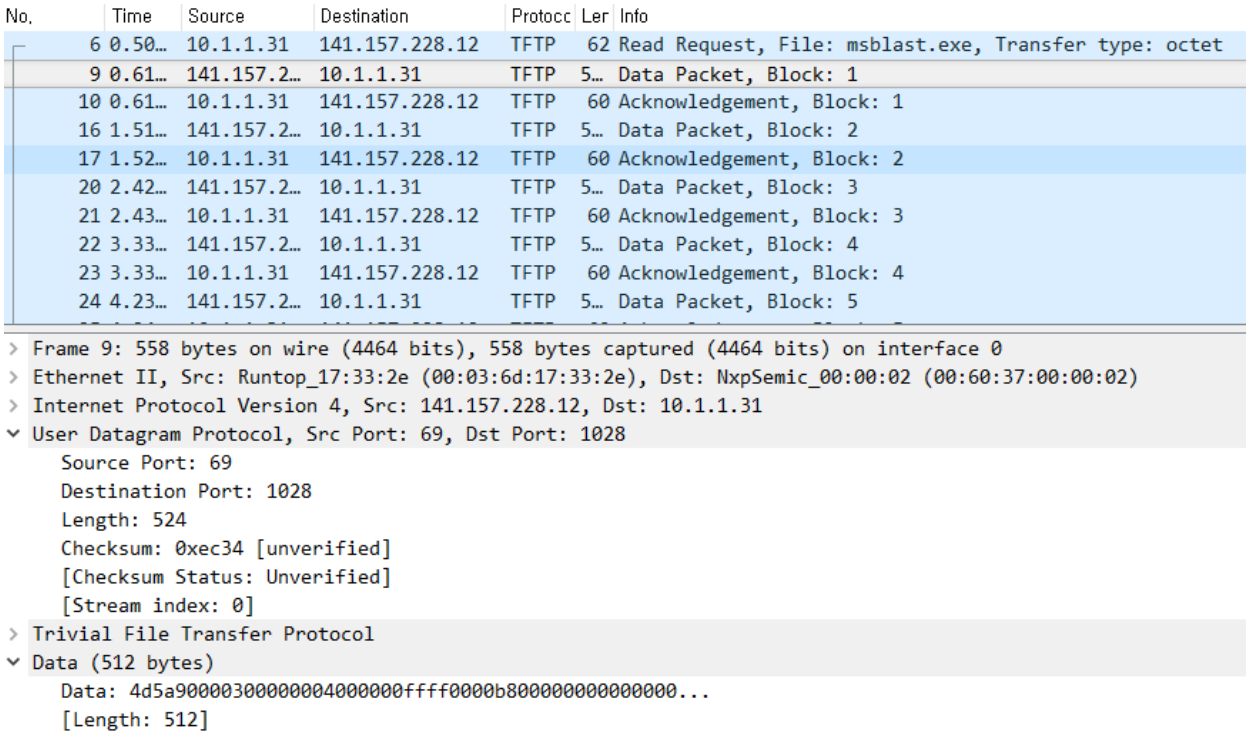
1) 어떤 응용 프로그램을 이용하여 파일을 전송 하였는가?



[그림-8. tftp파일 전송]

Tftp를 통하여 파일을 전송하는 모습이다.

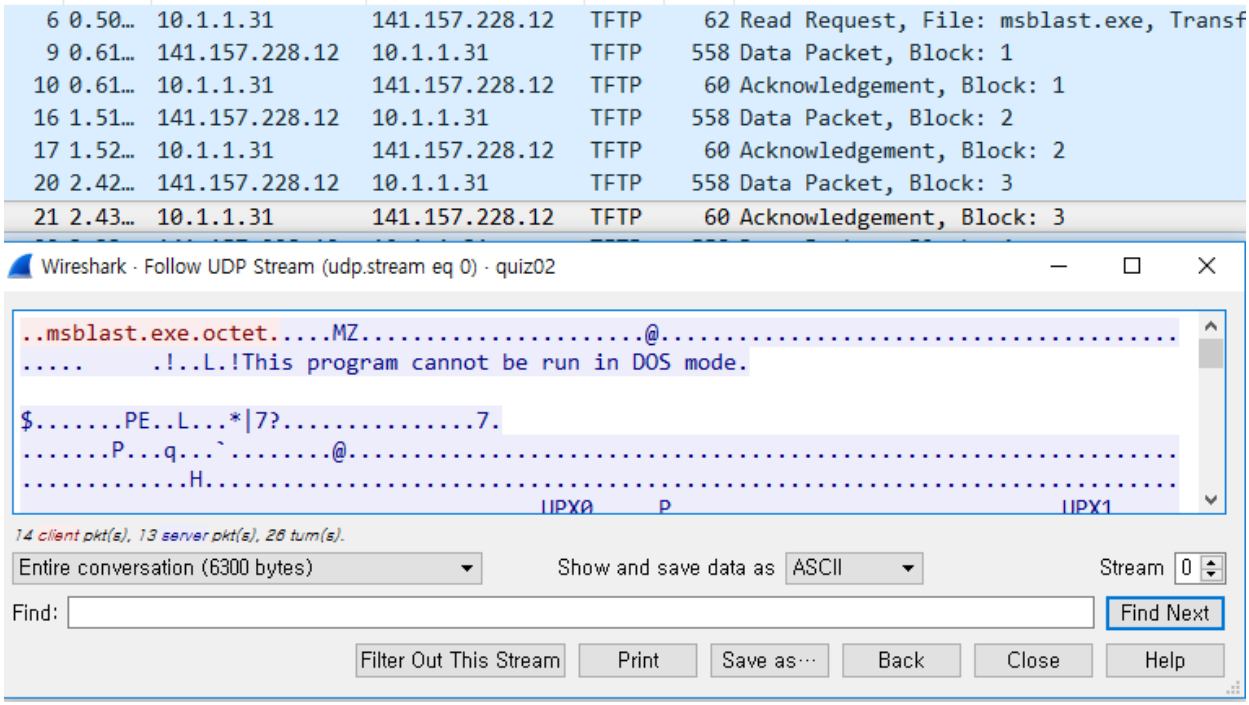
2) 파일을 수신하는 호스트의 IP 주소는 무엇인가?



[그림-9. 파일을 수신하는 호스트 IP 주소]

141.157.228.12 -> 10.1.1.31 에서 파일을 수신을 받고 있습니다.

3) 전송되는 파일의 이름은 무엇입니까?



[그림-10. Follow udp 상태]

Tftp를 오른쪽 클릭 후에 follow stream UDP로 하였더니 위와 같이 파일의 이름인 msblast.exe 프로그램을 전송되었습니다.

4. 결론

Quiz01, quiz02 번 문제를 통해 패킷 분석을 자세히 알게 되었으며, 전체적인 문서 작성 요령법까지 도움이 되었습니다.

5. 참고 문헌

http://www.naver.com 네이버의 힘

http://www.google.com 구글링의 힘