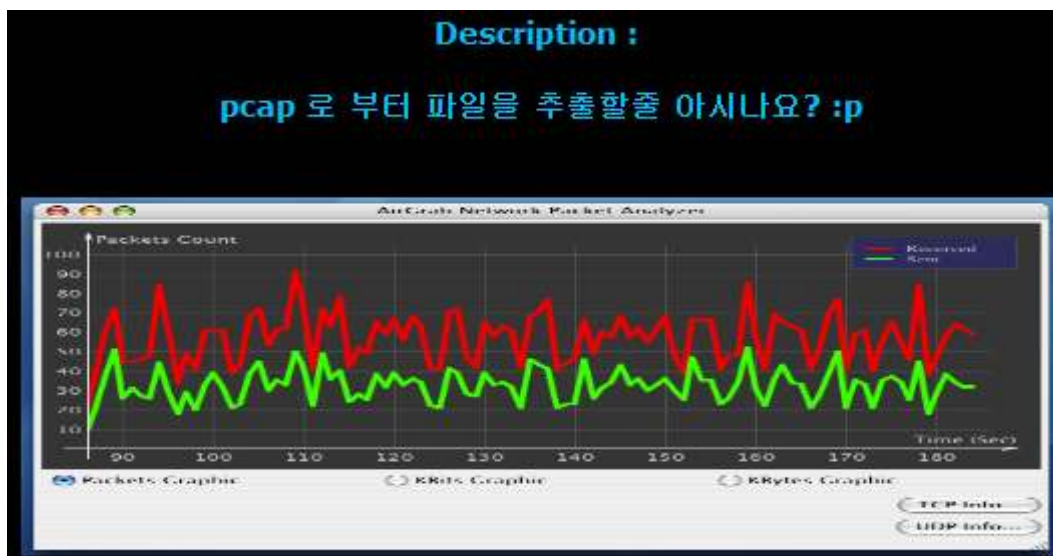


Hack-me.org 4번 Extract file from pcap

Sonic
2011.09.16

다음과 같이 pcap에서 파일을 추출하라 한다.

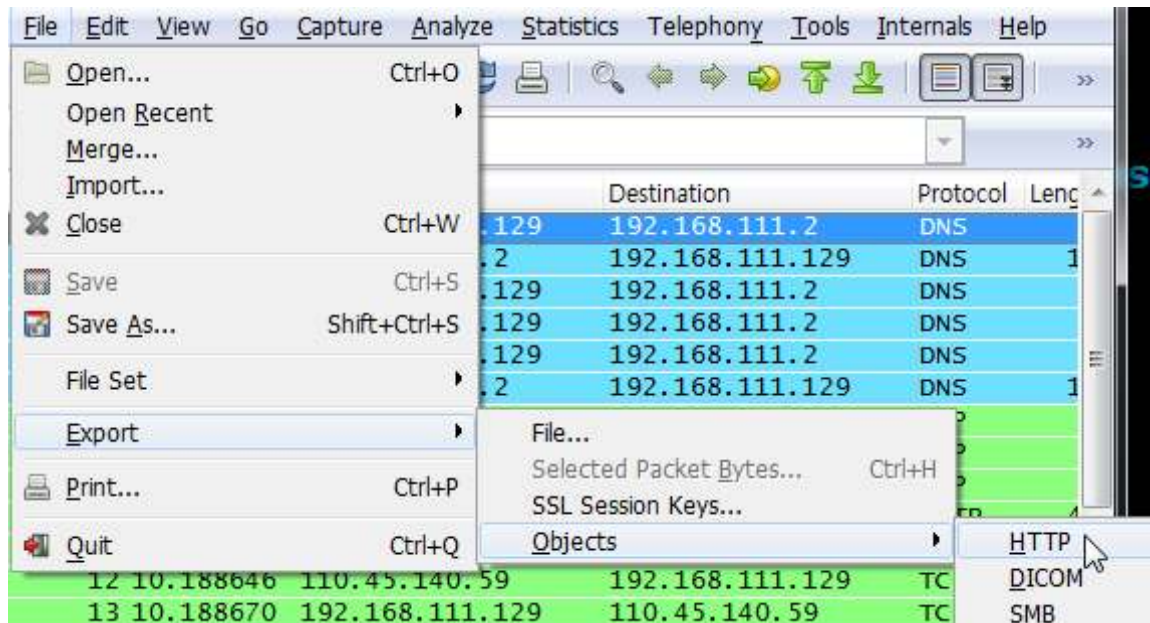


나는 다음과 같이 와이어샤크를 이용해서 열었다.

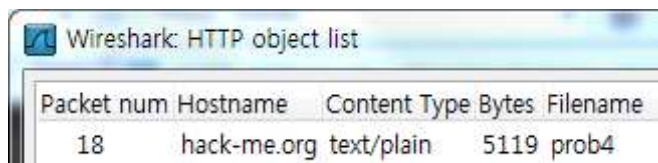
prob8_A221CD105C14E044D52F6371BA23EDE0.pcap [Wireshark 1.6.2 (SVN...)]

No.	Time	Source	Destination	Protocol	Length
1	0.000000	192.168.111.129	192.168.111.2	DNS	
2	0.094693	192.168.111.2	192.168.111.129	DNS	1
3	0.094842	192.168.111.129	192.168.111.2	DNS	
4	5.100697	192.168.111.129	192.168.111.2	DNS	
5	10.103734	192.168.111.129	192.168.111.2	DNS	
6	10.126875	192.168.111.2	192.168.111.129	DNS	1
7	10.128691	192.168.111.129	110.45.140.59	TCP	
8	10.159285	110.45.140.59	192.168.111.129	TCP	
9	10.159324	192.168.111.129	110.45.140.59	TCP	
10	10.159580	192.168.111.129	110.45.140.59	HTTP	4

File탭의 Export의 Objects에서 HTTP로 추출을 하였다.



다음과 같이 파일 하나만이 보인다.
추출해서 저장해보자.



확장자를 모르기에 hex스 에디터로 열어서 파일 시그니처를 보니 .ELF였다.

7F 45 4C 46 01 01 01 00 00 00 00 00 00 00 00 .ELF....

다음의 사이트에서 검색해보니 Linux상의 exe파일이였다.

http://www.garykessler.net/library/file_sigs.html

7F 45 4C 46 .ELF
n/a [Executable and Linking Format executable file \(Linux/Unix\)](http://www.garykessler.net/library/file_sigs.html#ELF)

chmod로 실행권한을 준 뒤에 실행시켜보니 password가 나왔다.

