Puzzle #4: The Curious Mr.X

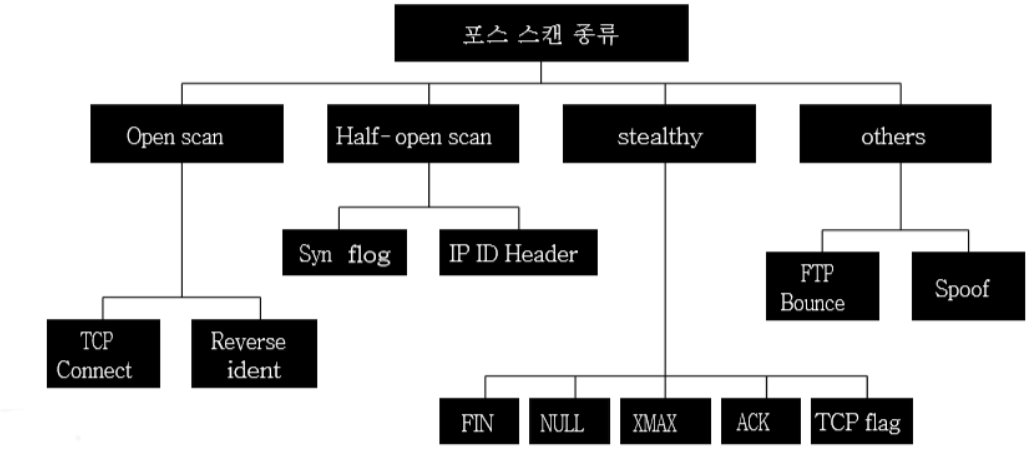
http://forensicscontest.com/2010/02/03/puzzle-4-the-curious-mr-x

1. What was the IP address of Mr. X's scanner?

10.42.42.253 이 10.42.42.50, 10.42.42.56, 10.42.42.25 에 계속 포트를 바꿔가며 TCP 연결을 시도하고 있다. 10.42.42.253 이 포트 스캐닝을 하고 있다는 것을 알 수 있다. 따라서 Mr.X 의 스캐너 ip 주소는 10.42.42.254 이다.

2. For the FIRST port scan that Mr. X conducted, what type of port scan was it? (Note: the scan consisted of many thousands of packets.) Pick one:

- TCP SYN
- TCP ACK
- UDP
- TCP Connect
- TCP XMAS
- TCP RST

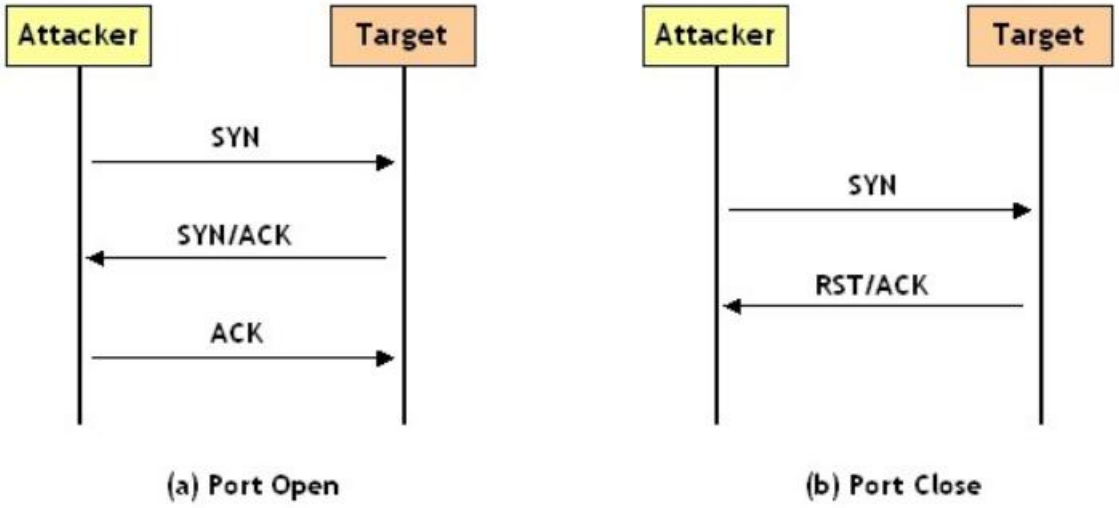


포트 스캔하는 방법은, 여러가지가 있다. 여기서는 TCP Connect 또는 TCP Syn 중 하나로 스캐닝을 시도하는 것을 바로 알 수 있다. 패킷의 플래그를 자세히 보면, TCP 세션을 요청하는 Syn 와 세션을 거부하는 Rst + Ack 를 많이 볼 수 있기 때문이다.

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.42.42.253	10.42.42.50	TCP	74	46104→80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SA
2	0.000731	10.42.42.50	10.42.42.253	TCP	60	80→46104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	0.607594	10.42.42.253	10.42.42.56	TCP	74	59856→80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SA
4	0.607596	10.42.42.253	10.42.42.25	TCP	74	40921→80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SA
5	0.607679	10.42.42.56	10.42.42.253	TCP	60	80→59856 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	0.607769	10.42.42.25	10.42.42.253	TCP	60	80→40921 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	0.812790	10.42.42.253	10.42.42.50	TCP	74	38232→554 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 S
8	0.812793	10.42.42.253	10.42.42.56	TCP	74	43771→554 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 S
9	0.812877	10.42.42.56	10.42.42.253	TCP	60	554→43771 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

보통 TCP 연결을 할 때, 3-way handshake 를 하는데 서버의 포트가 닫혀있을 경우 클라이언트가 Syn 를 보냈을 때 서버는 Rst + Ack 을 응답으로 보낸다.
여기서 TCP Connect 와 TCP syn 스캐닝을 자세히 알아보자.

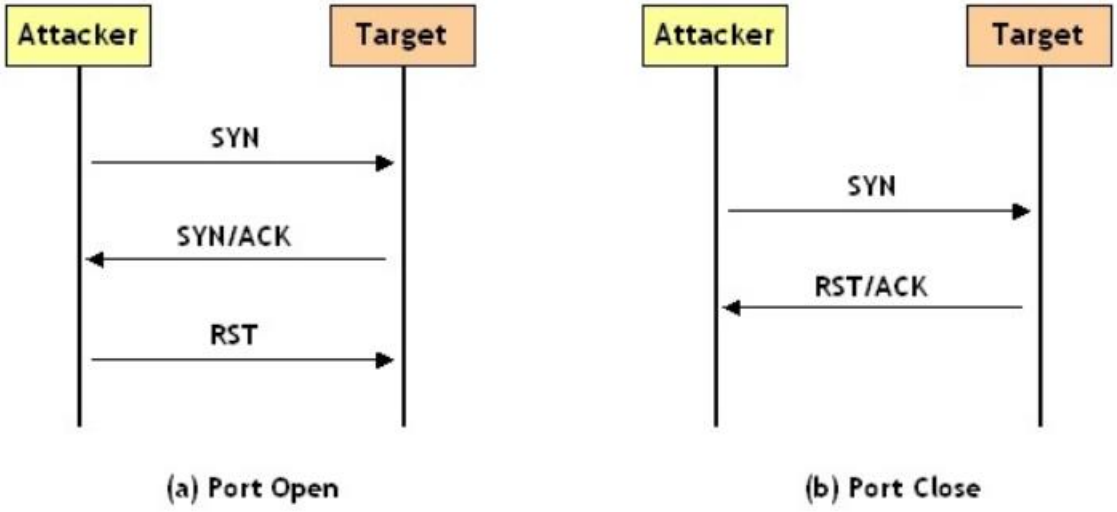
TCP connect 스캐닝은 Open Scan 중 하나의 기법이다.



(a) Port Open (b) Port Close

위의 그림처럼 포트가 열려있을 때와 닫혀있을 때를 구분하여 열린 포트 정보를 수집한다.

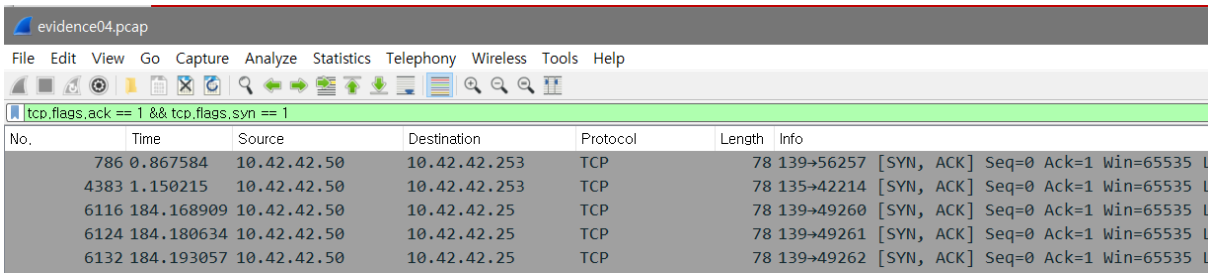
TCP Syn 스캐닝은 Half-Open scan 중 하나의 기법이다.



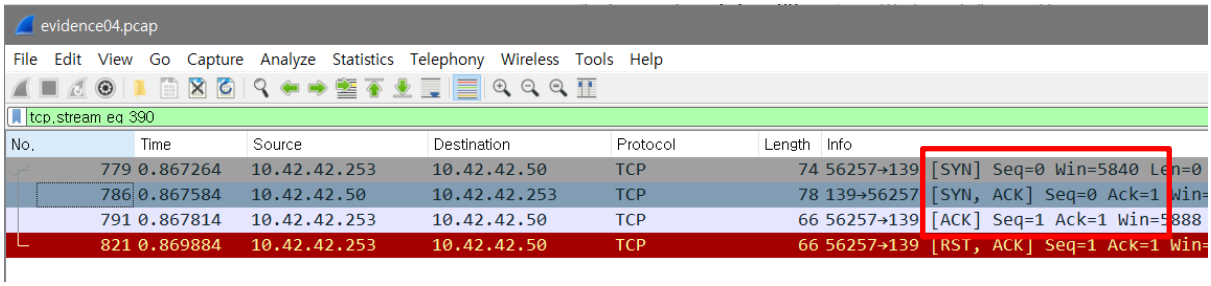
(a) Port Open (b) Port Close

TCP Connect 와 마찬가지로, 포트가 열려있을 때와 닫혀있을 때를 구분하여 열린 포트 정보를 수집한다. 하지만, 여기서 포트가 열려있을 때, 클라이언트에서 TCP 세션 연결을 거부하는 Rst 를 클라이언트에서 보낸다. 이것은 TCP 연결이 성공하면 상대방의 로그에 기록이 남기 때문에 Rst 을 먼저 보내 세션이 연결 되는 것을 막는 것이다.

따라서, Syn + Ack 플래그를 필터링해서 TCP Stream 을 확인하면 어떻게 통신하는지 볼 수 있다.



필터링을 해주고, 맨위에 있는 패킷의 TCP Stream 을 확인하였다.



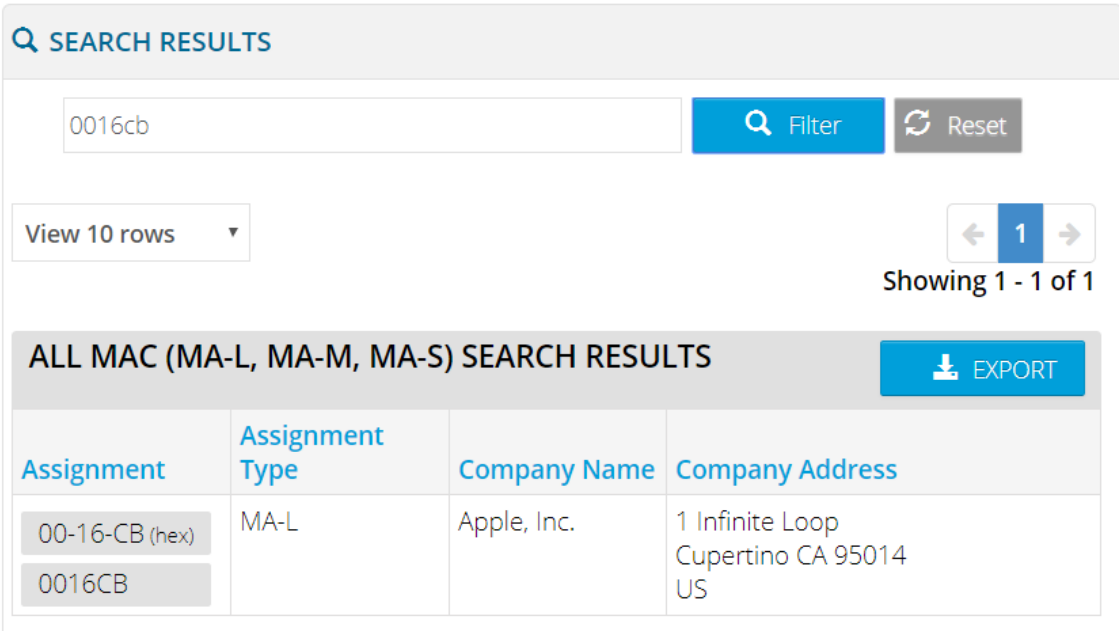
TCP Connect 스캐닝을 이용하여 스캐닝 한 것을 볼 수 있었다.

3. What were the IP addresses of the targets Mr. X discovered?

1 번에서 설명했듯이 10.42.42.253 이 10.42.42.50, 10.42.42.56, 10.42.42.25 에게 포트번호를 바꿔가며 굉장히 많은 패킷을 보내는 것을 볼 수 있다. 따라서 10.42.42.50, 10.42.42.56, 10.42.42.25 가 공격의 대상이라는 것을 알 수 있다.

4. What was the MAC address of the Apple system he found?

MAC 주소의 앞 3 바이트를 통해 제조사를 알 수 있었다.



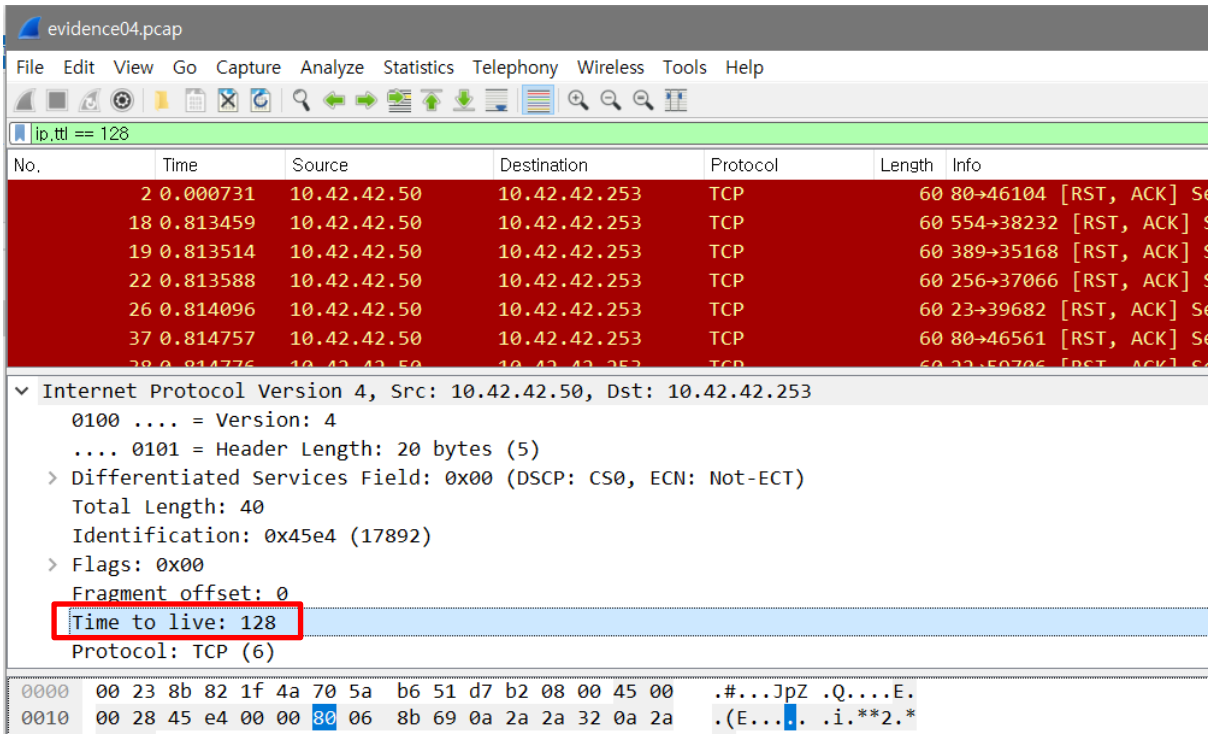
* https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries 에서 검색할 수 있다.

MAC 주소의 앞 3 바이트를 검색하여 10.42.42.25 가 Apple system 이라는 것을 확인 할 수 있었다.

5. What was the IP address of the Windows system he found?

패킷에서 운영체제를 확인 하는 방법은 TTL 값을 확인하는 방법이다. 운영체제마다 TTL 값이 다르다.

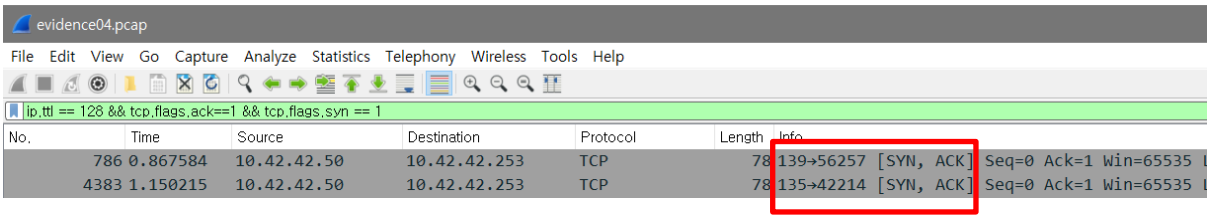
Linux = 64, Windows = 128, Cisco = 256 을 갖는다.



Ip.ttl == 128 로 필터링 해주면 10.42.42.50 이 윈도우 시스템인 것을 알 수 있다.

6. What TCP ports were open on the Windows system? (Please list the decimal numbers from lowest to highest.)

윈도우 시스템이면서 (TTL = 128), Syn + Ack 플래그가 1 로 세팅된 패킷을 필터링하였다.



10.42.42.50 에서 135, 139 두개의 포트에서 Syn + Ack 응답을 보냈다. 따라서 135,139 번 포트가 열려있다는 것을 알 수 있다.