



# [The Curious Mr.X] Write-Up

작성자	윤지원
분석 일자	2024.05.18
작성 일자	2024.05.18
분석 대상	evidence04.pcap
문서 버전	2.0
작성자 E-mail	<a href="mailto:yoonjw0827@gmail.com">yoonjw0827@gmail.com</a>

0. 목차

1. 문제 .....3

2. 분석 도구 .....3

3. 환경 .....3

4. Write-Up.....4


5. Flag.....8

6. 별도 첨부 .....9

7. Reference ..... 10



## 1. 문제

URL	<a href="https://forensicscontest.com/2010/02/03/puzzle-4-the-curious-mr-x">https://forensicscontest.com/2010/02/03/puzzle-4-the-curious-mr-x</a>
문제 내용	<p>While a fugitive in Mexico, Mr. X remotely infiltrates the Arctic Nuclear Fusion Research Facility's (ANFRF) lab subnet over the Interwebs. Virtually inside the facility (pivoting through a compromised system), he conducts some noisy network reconnaissance. Sadly, Mr. X is not yet very stealthy.</p> <p>Unfortunately for Mr. X, the lab's network is instrumented to capture all traffic (with full content). His activities are discovered and analyzed... by you! <a href="#">Here is the packet capture</a> containing Mr. X's activity. As the network forensic investigator, your mission is to answer the following questions:</p> <ol style="list-style-type: none"> <li>1. What was the IP address of Mr. X's scanner?</li> <li>2. For the FIRST port scan that Mr. X conducted, what type of port scan was it?</li> </ol> <p>Pick one: TCP SYN, TCP ACK, UDP, TCP Connect, TCP XMAS, TCP RST</p> <ol style="list-style-type: none"> <li>3. What were the IP addresses of the targets Mr. X discovered?</li> <li>4. What was the MAC address of the Apple system he found?</li> <li>5. What was the IP address of the Windows system he found?</li> <li>6. What TCP ports were open on the Windows system?</li> </ol>
문제 파일	 evidence04.pcap
문제 유형	Network forensics
난이도	2 / 5

## 2. 분석 도구

도구명	다운로드 링크	Version
Wireshark	<a href="#">Wireshark · Download</a>	3.4.7

## 3. 환경

OS
Windows 11 64-bit

# 4. Write-Up

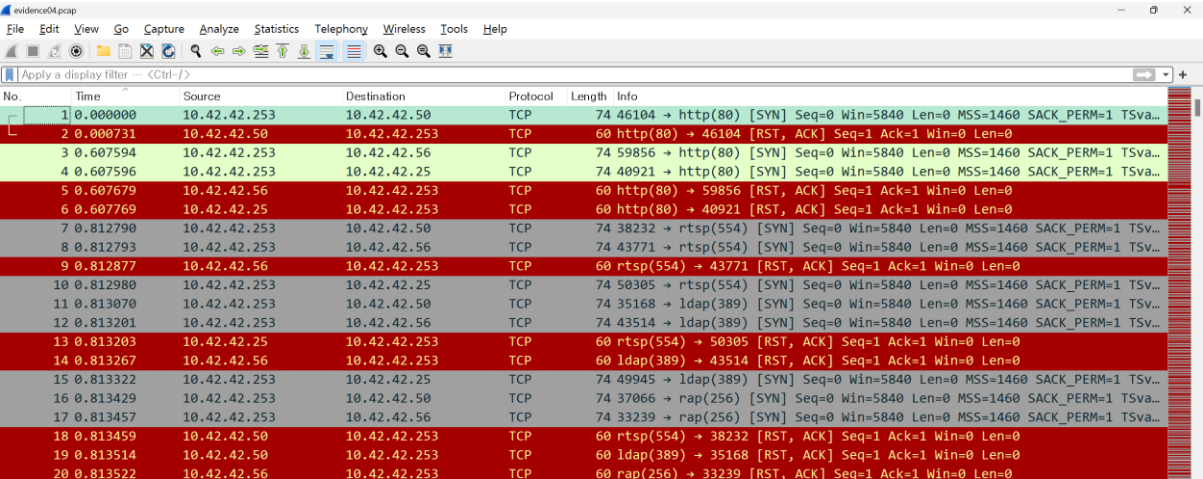
파일명	evidence04.pcap
용량	1.04MB
SHA256	003cfc39ce41f31f633d0bd3a32fe2f7a6f1669c51dd3217bee8439fcbe19b0c
Timestamp	2024-05-18 12:13:33

우선적으로 문제의 배경을 요약해보면 다음과 같다.

'X 씨는 연구실 서버넷에 원격으로 침투한 뒤 네트워크 정찰을 수행한다. 그러나 연구소의 네트워크는 모든 트래픽을 포착할 수 있도록 되어있기 때문에 그의 활동은 발견된다.'

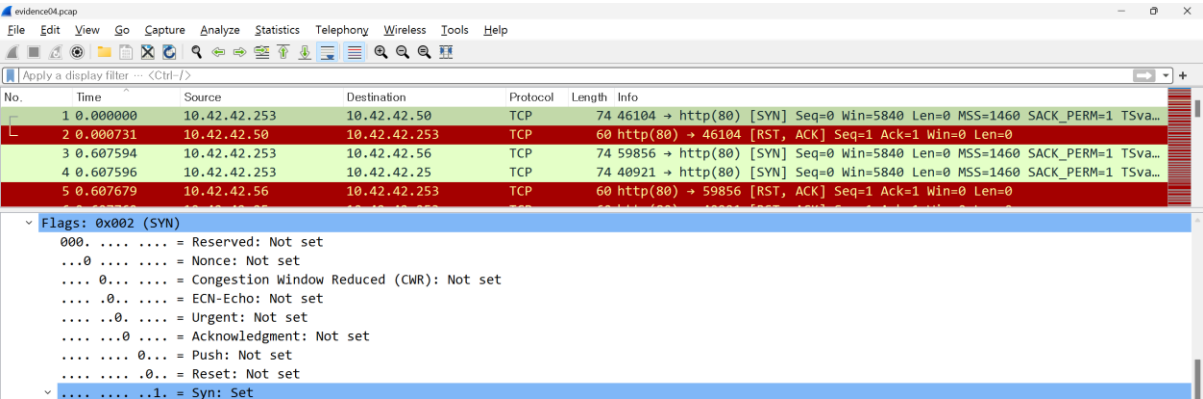
1. What was the IP address of Mr.X's scanner?

우선 evidence04.pcap 파일을 wireshark 를 통해 열어보면, 거의 다 TCP 프로토콜이 차지하고 있다는 것을 알 수 있다. 또한 전송하는 패킷들이 SYN flags 를 계속해서 전송하는 모습을 볼 수 있는데, 이를 더 확실히 하기 위해 패킷 하나를 열어서 Flags 를 살펴보았다.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.42.42.253	10.42.42.50	TCP	74	46104 → http(80) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSva...
2	0.000731	10.42.42.50	10.42.42.253	TCP	60	http(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 → http(80) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSva...
4	0.607596	10.42.42.253	10.42.42.25	TCP	74	40921 → http(80) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSva...
5	0.607679	10.42.42.56	10.42.42.253	TCP	60	http(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	http(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 → rtsp(554) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSv...
8	0.812793	10.42.42.253	10.42.42.56	TCP	74	43771 → rtsp(554) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSv...
9	0.812877	10.42.42.56	10.42.42.253	TCP	60	rtsp(554) → 43771 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10	0.812980	10.42.42.253	10.42.42.25	TCP	74	50305 → rtsp(554) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSv...
11	0.813070	10.42.42.253	10.42.42.50	TCP	74	35168 → ldap(389) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSv...
12	0.813201	10.42.42.253	10.42.42.56	TCP	74	43514 → ldap(389) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSv...
13	0.813203	10.42.42.25	10.42.42.253	TCP	60	rtsp(554) → 50305 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	0.813267	10.42.42.56	10.42.42.253	TCP	60	ldap(389) → 43514 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	0.813322	10.42.42.253	10.42.42.25	TCP	74	49945 → ldap(389) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSv...
16	0.813429	10.42.42.253	10.42.42.50	TCP	74	37066 → rap(256) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSva...
17	0.813457	10.42.42.253	10.42.42.56	TCP	74	33239 → rap(256) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSva...
18	0.813459	10.42.42.50	10.42.42.253	TCP	60	rtsp(554) → 38232 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	0.813514	10.42.42.50	10.42.42.253	TCP	60	ldap(389) → 35168 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	0.813522	10.42.42.56	10.42.42.253	TCP	60	rap(256) → 33239 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

[사진 1] evidence04.pcap를 wireshark로 열어본 모습



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.42.42.253	10.42.42.50	TCP	74	46104 → http(80) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSva...

Flags: 0x002 (SYN)

- 000. .... = Reserved: Not set
- ...0. .... = Nonce: Not set
- ....0... = Congestion Window Reduced (CWR): Not set
- ....0... = ECN-Echo: Not set
- ....0... = Urgent: Not set
- ....0... = Acknowledgment: Not set
- ....0... = Push: Not set
- ....0... = Reset: Not set
- ....1... = Syn: Set

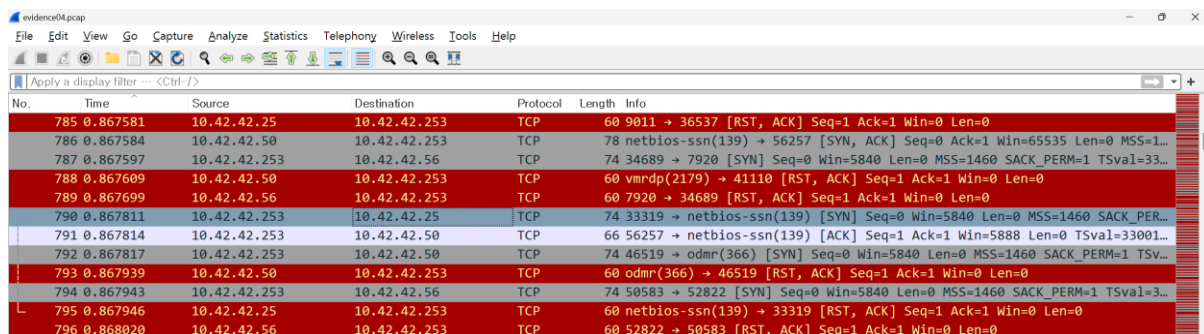
[사진 2] 1번 패킷의 Flags에서 SYN만 Set되어있는 모습

## [WHS-2] .iso

[사진 2]와 같이 SYN flags 만 활성화되어 있는 것을 확인할 수 있다. 따라서 [사진 1]을 고려할 때, 10.42.42.253 에서 10.42.42.50, 10.42.42.56, 10.42.42.25 으로 SYN flags 를 포함한 패킷을 계속해서 전송하면서 접근을 요청하고 있다고 생각했다. 따라서 이는 X 씨의 흔적이라고 볼 수 있기에 X 씨의 스캐너 IP 는 **10.42.42.253** 이다.

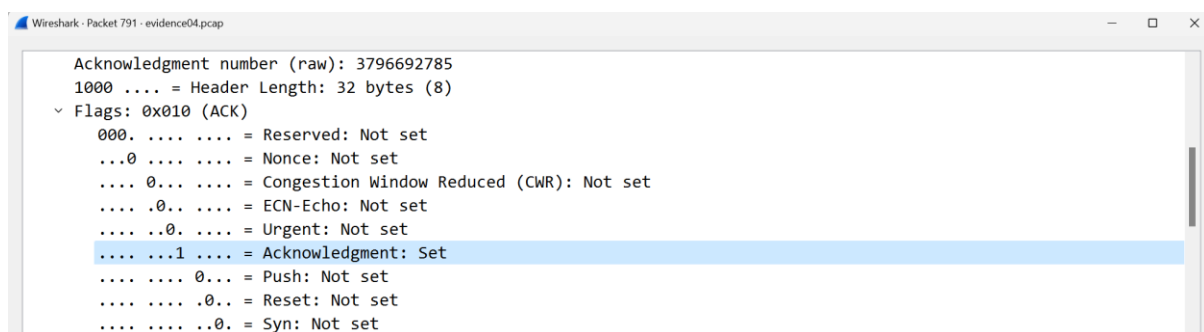
2. For the FIRST port scan that Mr. X conducted, what type of port scan was it? (Note: the scan consisted of many thousands of packets.) Pick one: TCP SYN, TCP ACK, UDP, TCP Connect, TCP XMAS, TCP RST

이 문제의 내용은 X 씨가 처음으로 실시한 포트 스캔이 어떤 유형인지 선택하는 것이다. 우선 SYN flag 를 보내는 것은 별도 첨부 내용을 통해 TCP SYN 또는 TCP Connect 두 가지라는 것을 알 수 있다. 따라서 이 둘 중 하나라는 것을 알아내려면 SYN 뿐만 아니라 RST 또는 ACK 를 전송하는 패킷을 발견해야 했다. 패킷들을 살펴보면 중, 색이 다르고 ACK 를 전송하는 791 번 패킷을 발견할 수 있었다.



No.	Time	Source	Destination	Protocol	Length	Info
785	0.867581	10.42.42.25	10.42.42.253	TCP	60	9011 → 36537 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
786	0.867584	10.42.42.50	10.42.42.253	TCP	78	netbios-ssn(139) → 56257 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1...
787	0.867597	10.42.42.253	10.42.42.56	TCP	74	34689 → 7920 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=33...
788	0.867609	10.42.42.50	10.42.42.253	TCP	60	vmrpd(2179) → 41110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
789	0.867699	10.42.42.56	10.42.42.253	TCP	60	7920 → 34689 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
790	0.867811	10.42.42.253	10.42.42.25	TCP	74	33319 → netbios-ssn(139) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PER...
791	0.867814	10.42.42.253	10.42.42.50	TCP	66	56257 → netbios-ssn(139) [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=33001...
792	0.867817	10.42.42.253	10.42.42.50	TCP	74	46519 → odmr(366) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSV...
793	0.867939	10.42.42.50	10.42.42.253	TCP	60	odmr(366) → 46519 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
794	0.867943	10.42.42.253	10.42.42.56	TCP	74	50583 → 52822 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3...
795	0.867946	10.42.42.25	10.42.42.253	TCP	60	netbios-ssn(139) → 33319 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
796	0.868020	10.42.42.56	10.42.42.253	TCP	60	52822 → 50583 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

[사진 3] 색이 다른 791번 패킷을 찾아낸 모습



Acknowledgment number (raw): 3796692785  
1000 .... = Header Length: 32 bytes (8)  
▼ Flags: 0x010 (ACK)  
000. .... = Reserved: Not set  
...0 .... = Nonce: Not set  
... 0... = Congestion Window Reduced (CWR): Not set  
... .0.. = ECN-Echo: Not set  
... ..0. = Urgent: Not set  
.... ..1. = Acknowledgment: Set  
.... .... = Push: Not set  
.... .... .0.. = Reset: Not set  
.... .... .0. = Syn: Not set

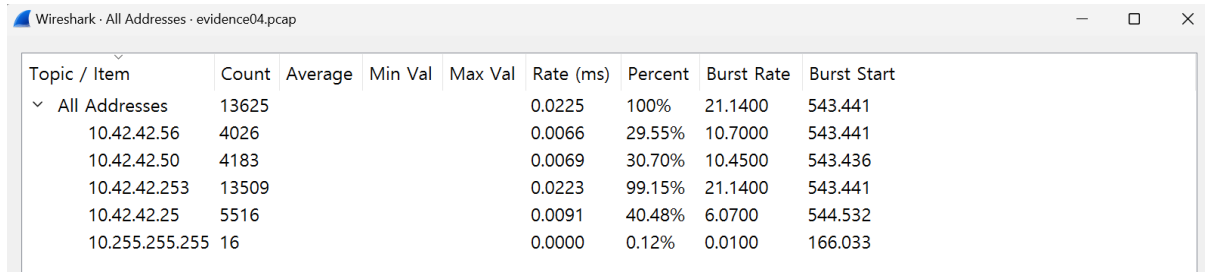
[사진 4] 791번 패킷의 Flags에서 ACK가 활성화된 모습

[사진 4]를 통해 확실하게 ACK 를 전송하고 있다는 것을 알 수 있었다. 따라서 포트 스캔은 ACK 패킷을 전송하는 **TCP Connect** 에 해당한다.

## [WHS-2] .iso

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

이 질문은 X 씨가 발견한 대상의 IP 주소들을 묻는 질문이다. 이는 [사진 1]에서도 확인할 수 있지만, 보다 정확한 증거를 찾기 위해 Statistics - Ipv4 Statistics - All Addresses 과정을 통해 모든 주소에서의 IPv4 통계를 살펴보았다.



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
▼ All Addresses	13625				0.0225	100%	21.1400	543.441
10.42.42.56	4026				0.0066	29.55%	10.7000	543.441
10.42.42.50	4183				0.0069	30.70%	10.4500	543.436
10.42.42.253	13509				0.0223	99.15%	21.1400	543.441
10.42.42.25	5516				0.0091	40.48%	6.0700	544.532
10.255.255.255	16				0.0000	0.12%	0.0100	166.033

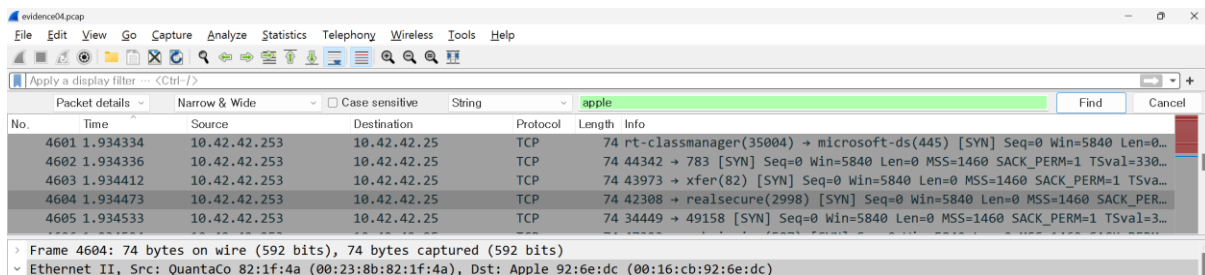
[사진 5] IPv4 통계를 통한 주소 확인

이를 통해 X 씨의 IP 주소를 제외하고 다음과 같은 총 3 개의 IP 주소를 확인할 수 있다.

**10.42.42.56, 10.42.42.50, 10.42.42.25**

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

이 질문은 X 씨가 찾아낸 Apple 시스템의 MAC 주소를 물어보는 질문이다. 그렇다면 이 패킷들 안에 Apple 에 대한 내용이 있을 것이라고 생각하여, packet detail 검색을 이용하여 Apple 을 검색해보았다. 그랬더니 여러 개의 패킷들이 차례대로 검색되었는데, Ethernet 의 도착지 MAC 주소는 모두 **00:16:cb:92:6e:dc**로 동일하였다.



No.	Time	Source	Destination	Protocol	Length	Info
4601	1.934334	10.42.42.253	10.42.42.25	TCP	74	rt-classmanager(35004) → microsoft-ds(445) [SYN] Seq=0 Win=5840 Len=0...
4602	1.934336	10.42.42.253	10.42.42.25	TCP	74	44342 → 783 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=330...
4603	1.934412	10.42.42.253	10.42.42.25	TCP	74	43973 → xfer(82) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSva...
4604	1.934473	10.42.42.253	10.42.42.25	TCP	74	42308 → realsecure(2998) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PER...
4605	1.934533	10.42.42.253	10.42.42.25	TCP	74	34449 → 49158 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3...

▼ Frame 4604: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

▼ Ethernet II, Src: QuantaCo\_82:1f:4a (00:23:8b:82:1f:4a), Dst: Apple\_92:6e:dc (00:16:cb:92:6e:dc)

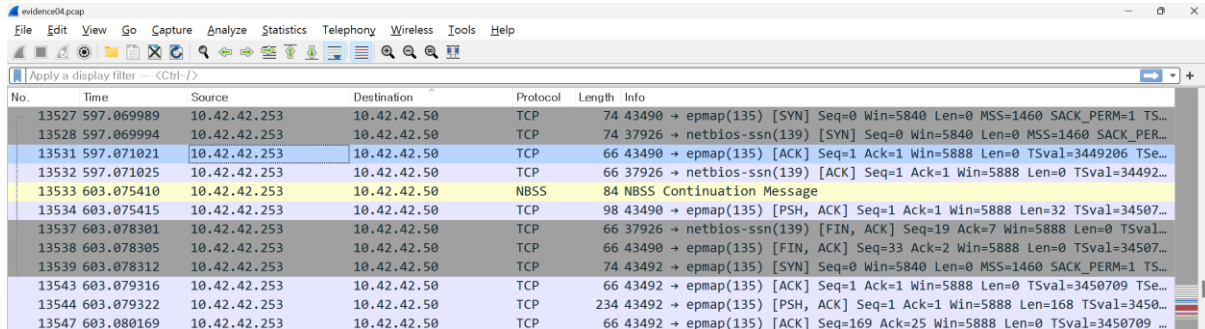
[사진 6] Apple 검색 후 도착지 MAC 주소를 확인하는 모습

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

이 질문은 X 씨가 찾은 Windows 시스템의 IP 주소를 물어보는 질문이다. 앞서 4 번 문제에서 Apple 시스템을 검색할 때 전송된 주소들은 전부 10.42.42.25 였다. 따라서 이것은 Windows 시스템이 아니기 때문에 나머지 10.42.42.50 과 10.42.42.56 중 Windows 시스템이 있을 것이라고

## [WHS-2] .iso

예상하였다. 그래서 동일하게 검색으로 찾아보려고 했지만 검색이 되지 않았다. 둘 중 하나라고 생각했기 때문에 출발지가 10.42.42.253 이고 도착지가 10.42.42.50 인 패킷들을 살펴보니, [사진 7]과 같이 135 와 139 포트로 ACK 를 주고받고 있다는 것을 확인할 수 있었다. 이 포트들은 Windows 시스템에서 기본적으로 오픈 되어 있는 포트들이라는 것을 알아냈다.

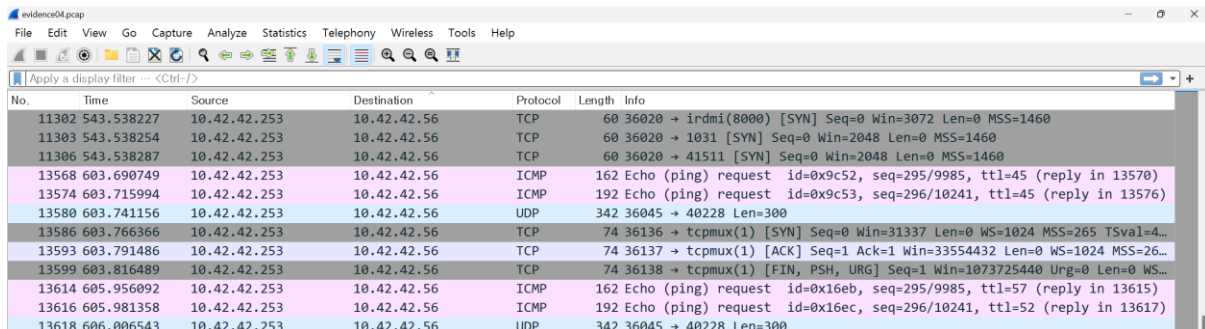


No.	Time	Source	Destination	Protocol	Length	Info
13527	597.069989	10.42.42.253	10.42.42.50	TCP	74	43490 → epmap(135) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TS...
13528	597.069994	10.42.42.253	10.42.42.50	TCP	74	37926 → netbios-ssn(139) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PER...
13531	597.071021	10.42.42.253	10.42.42.50	TCP	66	43490 → epmap(135) [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=3449206 TSe...
13532	597.071025	10.42.42.253	10.42.42.50	TCP	66	37926 → netbios-ssn(139) [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=34492...
13533	603.075410	10.42.42.253	10.42.42.50	NBSS	84	NBSS Continuation Message
13534	603.075415	10.42.42.253	10.42.42.50	TCP	98	43490 → epmap(135) [PSH, ACK] Seq=1 Ack=1 Win=5888 Len=32 TSval=34507...
13537	603.078301	10.42.42.253	10.42.42.50	TCP	66	37926 → netbios-ssn(139) [FIN, ACK] Seq=19 Ack=7 Win=5888 Len=0 TSval...
13538	603.078305	10.42.42.253	10.42.42.50	TCP	66	43490 → epmap(135) [FIN, ACK] Seq=33 Ack=2 Win=5888 Len=0 TSval=34507...
13539	603.078312	10.42.42.253	10.42.42.50	TCP	74	43492 → epmap(135) [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TS...
13543	603.079316	10.42.42.253	10.42.42.50	TCP	66	43492 → epmap(135) [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=3450709 TSe...
13544	603.079322	10.42.42.253	10.42.42.50	TCP	234	43492 → epmap(135) [PSH, ACK] Seq=1 Ack=1 Win=5888 Len=168 TSval=3450...
13547	603.080169	10.42.42.253	10.42.42.50	TCP	66	43492 → epmap(135) [ACK] Seq=169 Ack=25 Win=5888 Len=0 TSval=3450709 ...

[사진 7] 135, 139 포트가 열려 있는 모습

이러한 모습을 보아 Windows 시스템의 IP 주소는 **10.42.42.50**이라는 것을 알 수 있다.

혹시나 해서 출발지가 10.42.42.253이고 도착지가 10.42.42.56인 패킷들도 살펴보았는데, 여기는 ACK에 대한 정상적인 응답이 없었다.



No.	Time	Source	Destination	Protocol	Length	Info
11302	543.538227	10.42.42.253	10.42.42.56	TCP	60	36020 → irdmi(8000) [SYN] Seq=0 Win=3072 Len=0 MSS=1460
11303	543.538254	10.42.42.253	10.42.42.56	TCP	60	36020 → 1031 [SYN] Seq=0 Win=2048 Len=0 MSS=1460
11306	543.538287	10.42.42.253	10.42.42.56	TCP	60	36020 → 41511 [SYN] Seq=0 Win=2048 Len=0 MSS=1460
13568	603.690749	10.42.42.253	10.42.42.56	ICMP	162	Echo (ping) request id=0x9c52, seq=295/9985, ttl=45 (reply in 13570)
13574	603.715994	10.42.42.253	10.42.42.56	ICMP	192	Echo (ping) request id=0x9c53, seq=296/10241, ttl=45 (reply in 13576)
13580	603.741156	10.42.42.253	10.42.42.56	UDP	342	36045 → 40228 Len=300
13586	603.766366	10.42.42.253	10.42.42.56	TCP	74	36136 → tcpmux(1) [SYN] Seq=0 Win=31337 Len=0 WS=1024 MSS=265 TSval=4...
13593	603.791486	10.42.42.253	10.42.42.56	TCP	74	36137 → tcpmux(1) [ACK] Seq=1 Ack=1 Win=33554432 Len=0 WS=1024 MSS=26...
13599	603.816489	10.42.42.253	10.42.42.56	TCP	74	36138 → tcpmux(1) [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS...
13614	605.956092	10.42.42.253	10.42.42.56	ICMP	162	Echo (ping) request id=0x16eb, seq=295/9985, ttl=57 (reply in 13615)
13616	605.981358	10.42.42.253	10.42.42.56	ICMP	192	Echo (ping) request id=0x16ec, seq=296/10241, ttl=52 (reply in 13617)
13618	606.006543	10.42.42.253	10.42.42.56	UDP	342	36045 → 40228 Len=300

[사진 8] 10.42.42.56에서는 응답 받지 못한 모습

6. What TCP ports were open on the Windows system?

이 질문은 Windows 시스템에서 열린 TCP 포트를 질문하고 있다. [사진 7]에서 **135, 139** 포트가 열려 있는 것을 확인할 수 있다.

## 5. Flag

1. 10.42.42.253
2. TCP Connect
3. 10.42.42.56, 10.42.42.50, 10.42.42.25
4. 00:16:cd:92:6e:dc
5. 10.42.42.50
6. 135, 139



## 6. 별도 첨부

TCP SYN : 오픈 포트는 타겟으로부터 SYN + ACK 응답을 받고 RST를 설정한 TCP 패킷을 전송한다. 닫힌 포트는 RST + ACK 응답을 타겟으로부터 받는다.

TCP ACK : 방화벽을 테스트한다.

UDP : ICMP 메시지를 이용하여 UDP 포트의 오픈 여부를 판단한다.

TCP Connect : 오픈 포트는 SYN + ACK 패킷을 수신하고 이에 대한 ACK 패킷을 전송한다. 닫힌 포트는 RST + ACK 응답을 받는다.

TCP XMAS : 연결되어 있지 않은 포트에 탐지 패킷을 전송하기 때문에 SYN을 사용하지 않는다.

TCP RST : 재설정을 하는 과정으로 양방향에서 동시에 일어나는 중단 작업이다.

## 7. Reference

- [URL]