



작성자	윤지원, 김서영
분석 일자	2024.05.31.
작성 일자	2024.05.31.
분석 대상	evidence08.pcap
문서 버전	1.0
작성자 E-mail	yoonjw0827@gmail.com

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3


4. Write-Up.....4

5. Flag..... 12

6. 별도 첨부 13

7. Reference 14

1. 문제

URL	https://forensicscontest.com/2011/04/27/puzzle-8
문제 내용	You are the forensic investigator. Your team got a tip that InterOptik might be hunkered down in the area and contacted local admins concerning suspicious network activity. Joe has provided you with his packet capture and helpfully tells you that his own MAC address is 00:11:22:33:44:55. Can you figure out what's going on and track the attacker's activities?
문제 파일	 evidence08.pcap
문제 유형	Network forensics
난이도	2 / 3

2. 분석 도구

도구명	다운로드 링크	Version
Wireshark	https://www.wireshark.org/download.html	3.4.7
Aircrack-ng	https://www.aircrack-ng.org/	1.7
vmware	Download VMware Workstation Player VMware	17.5.2
networkminer	NetworkMiner - The NSM and Network Forensics Analysis Tool ↗ (netresec.com)	2.9.0

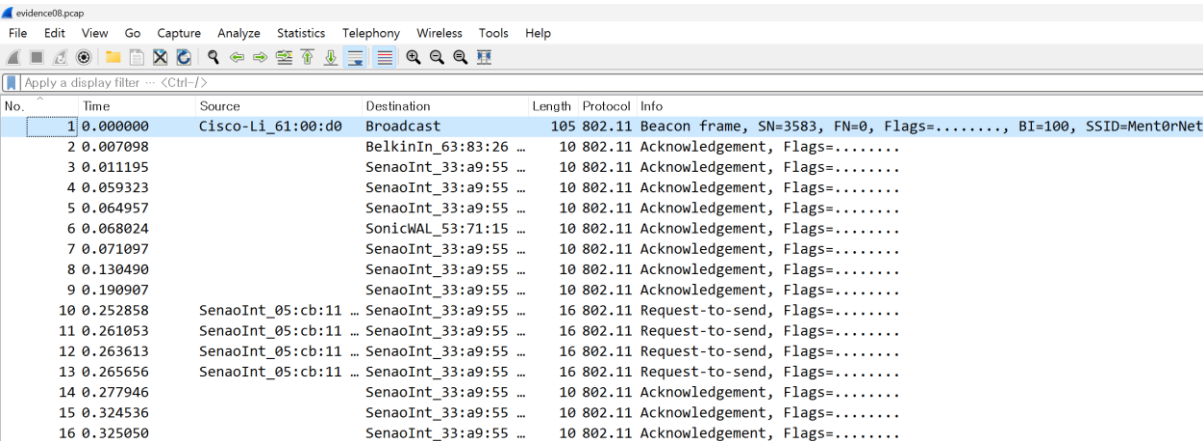
3. 환경

OS
Windows 11 64-bit

4. Write-Up

파일명	evidence08.pcap
용량	8.28MB
SHA256	969f82205739e4d912f7a4bddf3d22f591bfa8fa09c9690c88117d7477263b8b
Timestamp	2024-05-31 18:56:47

이 문제는 내가 법의학 수사관으로써 InterOpt1k 의 의심스러운 네트워크 활동을 살펴보는 것이다. 힌트는 MAC 주소가 00:11:22:33:44:55 라는 것이다. 우선 문제 파일부터 열어보았다.



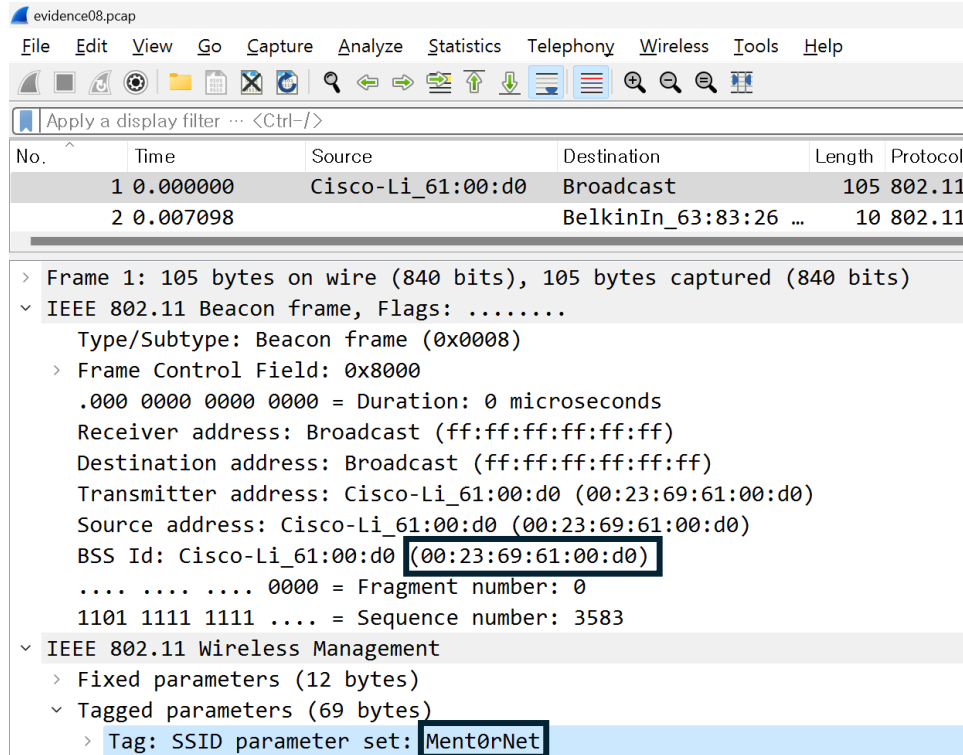
[사진 1] evidence08.pcap

처음 보는 형태의 패킷들이어서 알아보니 프로토콜 802.11로 무선 통신을 하고 있었다는 사실을 알 수 있었다. 이제 하위 문제들을 풀어보자.

1. Joe's WAP is beaconing. Based on the contents of the packet capture, what are:
- a. The SSID of his access point?
 - b. The BSSID of his access point?

문제를 해석해보면 Joe 의 WAP 이 수신중인 패킷 캡처 내용을 살펴보았을 때 접근 지점의 SSID와 BSSID를 알아내는 것이다. 첫 번째 패킷의 세부 내용을 확인해보니 BSS Id와 SSID를 쉽게 발견할 수 있었다. 따라서 [사진 2]에 따라 **SSID 는 Mnet0rNet, BSS ID 는 00:23:69:61:00:d0** 이다.

[WHS-2] .iso



[사진 2] SSID와 BSS ID

2. How long is the packet capture, from beginning to end (in SECONDS – please round to the nearest full second)?

이 문제는 패킷이 처음부터 끝까지 캡처되는 시간을 물어보고 있다. 따라서 정말 간단하게 가장 마지막 패킷의 시간을 보면 된다.

No.	Time
133068	413.576954

[사진 3] 마지막 패킷의 시간

따라서 답은 413.576954 를 반올림한 414 이다.

3. How many WEP-encrypted data frames are there total in the packet capture?

패킷 캡처에 총 몇 개의 WEP 암호화 데이터 프레임이 있는지 물어보는 문제이다. 검색을 통해 프로토콜이 802.11 로 WEP 암호화되어 있을 때, protected flag 가 1 로 설정된다는 것을 알 수 있었다. 또한, 일반적으로 데이터 프레임 영역을 찾기 위해 wlan.fc.type_subtype == 20 을 이용한다는 사실도 알 수 있었다. 이 조건들을 합쳐서 검색문을 다음과 같이 만들어보았다.

[WHS-2] .iso

wlan.fc.type_subtype == 0x20 && wlan.fc.protected == 1

No.	Time	Source	Destination	Length	Protocol	Info
98	6.553469	Cisco-Li_61:00:ce	IPv4mcast_7f:ff:fa	352	802.11	Data, SN=3650, FN=0, Flags=.p....F.
99	6.557567	Cisco-Li_61:00:ce	IPv4mcast_7f:ff:fa	361	802.11	Data, SN=3652, FN=0, Flags=.p....F.
100	6.563199	Cisco-Li_61:00:ce	IPv4mcast_7f:ff:fa	424	802.11	Data, SN=3653, FN=0, Flags=.p....F.
101	6.566783	Cisco-Li_61:00:ce	IPv4mcast_7f:ff:fa	416	802.11	Data, SN=3654, FN=0, Flags=.p....F.
102	6.569852	Cisco-Li_61:00:ce	IPv4mcast_7f:ff:fa	361	802.11	Data, SN=3655, FN=0, Flags=.p....F.
103	6.573439	Cisco-Li_61:00:ce	IPv4mcast_7f:ff:fa	400	802.11	Data, SN=3656, FN=0, Flags=.p....F.
104	6.577023	Cisco-Li_61:00:ce	IPv4mcast_7f:ff:fa	432	802.11	Data, SN=3657, FN=0, Flags=.p....F.
105	6.580607	Cisco-Li_61:00:ce	IPv4mcast_7f:ff:fa	361	802.11	Data, SN=3658, FN=0, Flags=.p....F.
106	6.584190	Cisco-Li_61:00:ce	IPv4mcast_7f:ff:fa	420	802.11	Data, SN=3659, FN=0, Flags=.p....F.
108	6.587774	Cisco-Li_61:00:ce	IPv4mcast_7f:ff:fa	426	802.11	Data, SN=3660, FN=0, Flags=.p....F.

[사진 4] WEP 암호화된 데이터 프레임 영역 찾기

Packets: 133068 · Displayed: 59274 (44.5%)

[사진 5] 필터링을 걸쳐 display된 패킷 수

필터링 이후에 하단을 보면 [사진 5]와 같이 결과적으로 출력되는 패킷의 수를 알 수 있다. 따라서 **59274개**의 WEP 암호화 데이터 프레임이 있다는 것을 알아냈다.

4. How many *unique* WEP initialization vectors are there TOTAL in the packet capture relating to JOE's access point?

JOE 의 access point 에 WEP 초기화 벡터가 있는 패킷은 몇 개인지 물어보는 문제이다. 이것 wireshark 에서 필터링을 통해 알아낼 수도 있지만, 이렇게 하면 중복되는 값도 포함된다는 것을 알 수 있다. 문제에서는 중복 초기화 값들을 제외해달라고 했기 때문에, 따로 코드를 짜거나 tshark 를 이용해야 했다. 나는 tshark 를 이용하는 방법을 선택하였고, 명령어는 다음과 같았다.

```
C:\Users\윤지원\OneDrive\바탕 화면\화이트햇\프로젝트\문제>tshark -r evidence08.pcap -Y "wlan.fc.type_subtype == 0x20 && wlan.fc.protected == 1" -T fields -e wlan.wep.iv | sort | uniq | wc -l
29719
```

[사진 6] WEP 초기화 벡터 패킷 수

Tshark -r evidence08.pcap -Y "wlan.fc.type_subtype == 0x20 && wlan.fc.protected == 1" -T fields -e wlan.wep.iv : WEP 초기화 벡터가 포함된 데이터 프레임을 필터링한 후, WEP 초기화 벡터만 출력

| sort : 출력된 초기화 벡터 값 정렬

| uniq : 중복된 초기화 벡터 값 제외

| wc -l : 고유한 초기화 벡터 값 개수 세기

이 명령어를 실행하면 [사진 6]과 같이 **29719**라는 수가 나오고 이것이 정답임을 알 수 있다.

[WHS-2] .iso

5. What was the MAC address of the station executing the Layer 2 attacks?

레이어 2 공격을 실행하는 스테이션의 MAC 주소를 물어보고 있다. 공격에 대해 알아보기 위해서는 무선랜 패킷의 암호를 풀어야 한다고 생각했다. 따라서 이를 분석할 수 있는 도구인 aircrack-ng를 사용하였다. Aircrack-ng GUI의 Aircrack-ng에 evidence08.pcap를 넣어 암호화 키를 얻었다.

```
Aircrack-ng 1.7

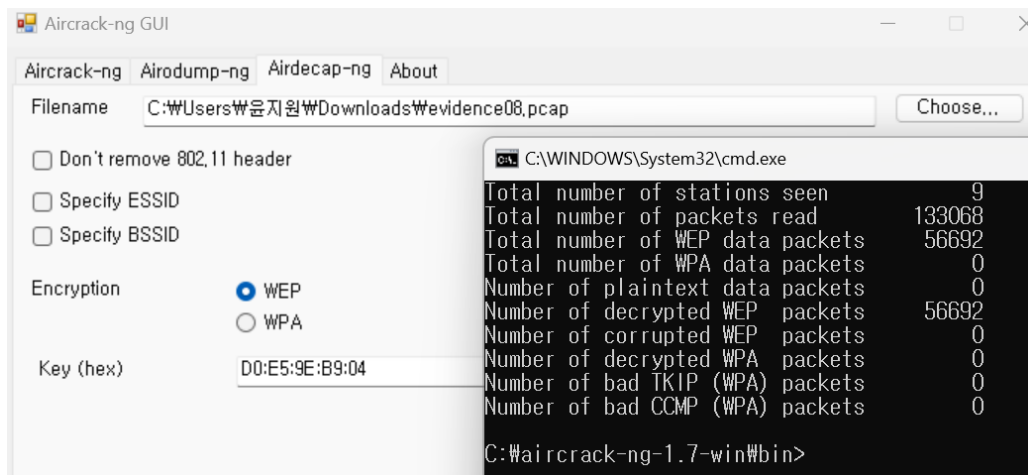
[00:00:00] Tested 587 keys (got 26805 IVs)

KB   depth  byte(vote)
0    3/ 4    D0(33536) BC(33024) 27(33024) 1F(33024) 7B(31744) 2F(31744) FF(31488) CA(30976) 96(30720)
1    0/ 1    E5(38656) 82(33024) 0C(32256) 3C(32000) EB(31744) 42(31488) 8B(31232) 3D(31232) 8C(31232)
2    0/ 5    9E(34048) 27(33792) 7A(32768) E9(32512) 8B(31744) C3(31744) D0(31488) 7B(31488) 2B(31488)
3    0/ 3    B9(35328) 57(35072) B1(34048) 7C(33024) 00(32768) 06(32512) CF(32256) 9C(31744) 09(31488)
4    8/ 10   A9(31488) B9(31232) 10(31232) 95(30976) A5(30976) 7A(30976) 08(30720) E1(30720) C8(30720)

KEY FOUND! [ D0:E5:9E:B9:04 ]
Decrypted correctly: 100%
```

[사진 7] 패킷 파일의 암호화 키

이 암호화 키를 다시 Aircrack-ng에 넣어서 복호화시켜주었다.



[사진 8] 패킷 파일 복호화

이 복호화를 진행해주었더니, **evidence08-dec.pcap**라는 파일이 생성되었다. 이 패킷 파일을 wireshark로 열어보았다. ARP 프로토콜로 필터링을 한 결과 [사진 9]와 같이 나타났는데, 694번 패킷과 같은 형태의 패킷들이 대부분을 이루고 있는 것을 확인할 수 있었다. 따라서 이를 자세히 살펴본 결과, **1c:4b:d6:69:cd:07**이라는 MAC 주소를 발견할 수 있었다.

[WHS-2] .iso

evidence08-dec.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Length	Protocol	Info
26	17.572994	Cisco-Li_61:00:ce	Broadcast	42	ARP	Who has 192.168.1.100? Tell 192.168.1.1
33	21.583238	CIMSYS_33:44:55	Broadcast	42	ARP	Who has 192.168.1.1? Tell 192.168.1.100
34	21.584257	CIMSYS_33:44:55	Broadcast	42	ARP	Who has 192.168.1.1? Tell 192.168.1.100
35	21.584252	Cisco-Li_61:00:ce	CIMSYS_33:44:55	42	ARP	192.168.1.1 is at 00:23:69:61:00:ce
693	174.578114	Cisco-Li_61:00:ce	Broadcast	42	ARP	Who has 192.168.1.100? Tell 192.168.1.1
694	174.581146	AzureWav_69:cd:07	Broadcast	42	ARP	Who has 192.168.1.100? Tell 192.168.1.1
695	174.979009	AzureWav_69:cd:07	Broadcast	42	ARP	Who has 192.168.1.100? Tell 192.168.1.1
696	174.980033	AzureWav_69:cd:07	Broadcast	42	ARP	Who has 192.168.1.100? Tell 192.168.1.1
697	174.983103	AzureWav_69:cd:07	Broadcast	42	ARP	Who has 192.168.1.100? Tell 192.168.1.1
698	174.987200	AzureWav_69:cd:07	Broadcast	42	ARP	Who has 192.168.1.100? Tell 192.168.1.1
699	174.988185	AzureWav_69:cd:07	Broadcast	42	ARP	Who has 192.168.1.100? Tell 192.168.1.1
700	174.989207	AzureWav_69:cd:07	Broadcast	42	ARP	Who has 192.168.1.100? Tell 192.168.1.1
701	174.990785	AzureWav_69:cd:07	Broadcast	42	ARP	Who has 192.168.1.100? Tell 192.168.1.1

> Frame 694: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)

> Ethernet II, Src: AzureWav_69:cd:07 (1c:4b:d6:69:cd:07), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Destination: Broadcast (ff:ff:ff:ff:ff:ff)

> Source: AzureWav_69:cd:07 (1c:4b:d6:69:cd:07)

> Type: ARP (0x0806)

> Address Resolution Protocol (request)

[사진 9] evidence08-dec.pcap

6. How many *unique IVs were generated (relating to Joe's access point)

JOE의 access point에 중복 제외 초기화 벡터들이 몇 개 생성되었는지 물어보는 문제이다.

a. By the attacker station?

공격자 측면에서 초기화 벡터를 구하며 쓴 명령어는 다음과 같다.

```
seoyoung@seoyoung-virtual-machine:~/Downloads$ tshark -r evidence08.pcap -Y "(wlan.bssid == 00:23:69:61:00:d0) && (wlan.sa == 1c:4b:d6:69:cd:07) && wlan.wep.iv" -T fields -e wlan.wep.iv | sort -u | wc -l
14133
```

[사진 10] attacker 측면 iv 개수 구하는 명령어

문제4와 마찬가지로 초기화 벡터(iv)를 구하기 위해 tshark를 사용했다. 사용한 명령어 내용은 다음과 같다.

-r evidence08.pcap: 'evidence08.pcap' 파일 읽기

-Y "(wlan.bssid == 00:23:69:61:00:d0) && (wlan.sa == 1c:4b:d6:69:cd:07) && wlan.wep.iv"

: (BSSID가 00:23:69:61:00:d0인 패킷을 필터링하고) && (소스 주소가 1c:4b:d6:69:cd:07인 패킷을 필터링하고) && (WEP IV 필드를 포함하는 패킷을 필터링하기)

-T fields: 출력 형식을 필드로 지정

[WHS-2] .iso

-e wlan.wep.iv: 출력할 필드로 WEP IV를 지정

| sort -u: 출력된 IV값을 정렬하고 고유한 값만 남기기

| wc -l: 고유한 IV값의 개수를 세기

명령어 사용 결과, 공격자 측면 IV 개수는 14133개이다.

b. By all *other* stations combined?

```
seoyoung@seoyoung-virtual-machine:~/Downloads$ tshark -r evidence08.pcap -Y "(wlan.bssid == 00:23:69:61:00:d0) && (wlan.sa != 1c:4b:d6:69:cd:07) && wlan.wep.iv" -T fields -e wlan.wep.iv | sort -u | wc -l  
15587
```

[사진 11] attacker 측면 iv 개수 구하는 명령어

공격자 외 측면에서 IV개수를 구하기 위한 명령어는 6-a와 명령어가 거의 비슷하지만, 공격자 주소 주소인 1c:4b:d6:69:cd:07에 해당하지 않는 패킷을 구하기 위해 !=를 사용하였다.

공격자 외 측면 IV 개수는 15587개이다.

이 둘을 합치면 총 개수는 $14133 + 15587 = 29,720$ 개이다.

7. What was the WEP key of Joe's WAP?

5 번 문제를 풀이하며 aircrack-ng 를 통해 [사진 7]에서 패킷 파일의 암호화 키를 이미 찾았었다.

8. What were the administrative username and password of the targeted wireless access point?

문제에서 설명하는 WAP 의 관리자는 Joe 이다.

문제에 나와있는 Joe 의 Mac 주소를 검색하여 Joe 의 IP 주소를 찾아보았다. IP 주소를 찾기 위해 Wireshark 에서 DHCP 프로토콜을 살펴보았다. DHCP 프로토콜은 호스트에게 IP 를 할당하기 위한 프로토콜이기 때문이다.

24	17.568897	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x8bb8710d
25	17.572482	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x8bb8710d
26	17.572994	CiscoLinksys_61:00:...	Broadcast	ARP	42 Who has 192.168.1.100? Tell 192.168.1.1
27	18.565307	192.168.1.1	192.168.1.100	DHCP	342 DHCP Offer - Transaction ID 0x8bb8710d
28	18.570434	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request - Transaction ID 0x8bb8710d
29	18.574018	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request - Transaction ID 0x8bb8710d
30	18.574524	192.168.1.1	192.168.1.100	DHCP	342 DHCP ACK - Transaction ID 0x8bb8710d

[사진 12] wireshark DHCP packet

DHCP 프로토콜의 단계인 Discover-Offer-Request-Ack 까지 전 과정을 찾았다. 마지막 단계인 ACK 단계 패킷에서 할당된 IP 를 확인하였다.

```

Dynamic Host Configuration Protocol (ACK)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x8bb8710d
  Seconds elapsed: 0
  ▶ Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.1.100
  Next server IP address: 192.168.1.1
  Relay agent IP address: 0.0.0.0
  Client MAC address: CIMSYS_33:44:55 (00:11:22:33:44:55)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  
```

[사진 13] DHCP ACK단계 패킷

[사진 13]에서 보이듯이 Joe의 IP주소는 192.168.1.100이다.

문제 5 번을 풀며 evidence08.pcap 를 복호화한 [사진 9] evidence08-dec.pcap 를 NetworkMiner 로 열어보았다.

Hosts (12)	Files (103)	Images (62)	Messages	Credentials (3)	Sessions (157)	DNS	Parameters (1595)	Keywords	Anomalies
<input checked="" type="checkbox"/> Show Cookies	<input checked="" type="checkbox"/> Show NTLM challenge-response	<input type="checkbox"/> Mask Passwords							
Client	Server	Protocol	Username	Password	Valid login	First Login			
192.168.1.100 [bt]	192.168.1.1 [bt] [192.168.1.1]	HTTP	admin	admin	Unknown	2010-09-17 15:57:09 UTC			
192.168.1.109 [bt]	192.168.1.1 [bt] [192.168.1.1] [WRT54G2]	HTTP	admin	admin	Unknown	2010-09-17 16:02:17 UTC			
192.168.1.109 [bt]	192.168.1.1 [192.168.1.1]	HTTP Cookie	sMode=3	N/A	Unknown	2010-09-17 16:02:27 UTC			

[사진 14] NetworkMiner로 열어본 evidence08-dec.pcap – Credentials 결과창

NetworkMiner-Credentials 창에서 Joe 의 IP 주소인 192.168.1.100 에 해당하는 Username 과 Password 를 모두 구할 수 있었다.

9. What was the WAP administrative passphrase changed to?

Passphrase 는 무선 네트워크를 보호하기 위해 사용되는 암호이다.

Wireshark 검색 필터로 String 을 선택하고 패킷의 자세한 정보에서 passphrase 를 검색해보았다.

No.	Time	Source	Destination	Protocol	Length	Info
56670	379.573498	192.168.1.1	192.168.1.109	TCP	74	80 → 49616 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=1 TSval=5343 TSecr=55407
56671	379.573971	192.168.1.109	192.168.1.1	TCP	66	49616 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=55407 TSecr=5343
56672	379.574482	192.168.1.109	192.168.1.1	HTTP	692	POST /Security.tri HTTP/1.1 (application/x-www-form-urlencoded)
56673	379.607803	192.168.1.1	192.168.1.109	HTTP	224	Continuation

[사진 15] evidence08-dec.pcap에서 String - passphrase 검색 결과

Passphrase 검색 결과 가장 마지막 패킷이 56672번 패킷이었다. 56672번 패킷을 자세히 살펴보았다.

```
▶ Transmission Control Protocol, Src Port: 49616, Dst Port: 80, Seq: 1, Ack: 1, Len: 626
▶ Hypertext Transfer Protocol
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "SecurityMode" = "3"
  ▶ Form item: "CipherType" = "1"
  ▶ Form item: "PassPhrase" = "hahp0wnedJ00"
  ▶ Form item: "GkuInterval" = "3600"
  ▶ Form item: "layout" = "en"
```

[사진 16] PassPhrase

PassPhrase 는 hahp0wnedJ00 임을 찾았다.

5. Flag

1번 : SSID – Mnet0rNet, BSS ID – 00:23:69:61:00:d0

2번 : 414초

3번 : 59274

4번 : 29719

5번 : 1c:4b:d6:69:cd:07

6번 : a) 14133, b) 15587

7번 : D0:E5:9E:B9:04

8번 : admin, admin

9번 : hahp0wnedJ00

6. 별도 첨부

<개별 문제 목록>

- 1) Joe's WAP is beaconing. Based on the contents of the packet capture, what are:
 - a. The SSID of his access point?
 - b. The BSSID of his access point?
- 2) How long is the packet capture, from beginning to end (in SECONDS – please round to the nearest full second)?
- 3) How many WEP-encrypted data frames are there total in the packet capture?
- 4) How many *unique* WEP initialization vectors (IVs) are there TOTAL in the packet capture relating to Joe's access point?
- 5) What was the MAC address of the station executing the Layer 2 attacks?
- 6) How many *unique* IVs were generated (relating to Joe's access point):
 - a. By the attacker station?
 - b. By all *other* stations combined?
- 7) What was the WEP key of Joe's WAP?
- 8) What were the administrative username and password of the targeted wireless access point?
- 9) What was the WAP administrative passphrase changed to?

7. Reference

- [URL]