

Digital

Forensic

대학원분 장경배
1791234 양유진
1791319 최정은

목차

01

디지털 포렌식

02

네트워크 포렌식

- Wireshark
- Colasoft
- 실습 I
- 실습 II

03

디스크 포렌식

- 기본 개념
- 실습 III

01 디지털 포렌식

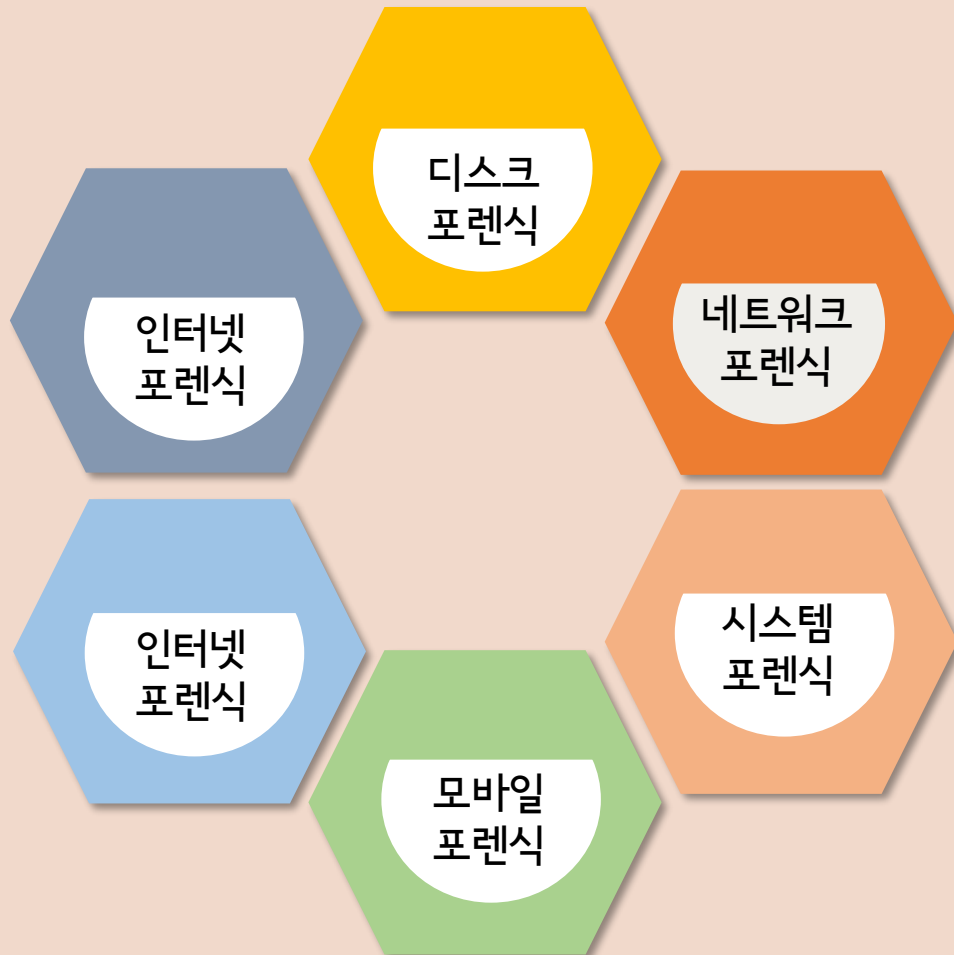
디지털 포렌식이란?

범죄와 관련된 디지털 자료를 과학적 지식과 기술을
활용하여 수집하고 분석하는 제반 행위

디지털
포렌식
기본 원칙

- 정당성의 원칙 : 증거가 적법한 절차에 의해 수집되었는가?
- 재현의 원칙 : 같은 조건과 상황에서 항상 동일한 결과가 나오는가?
- 신속성의 원칙 : 디지털 포렌식의 전 과정이 신속하게 진행되었는가?
- 절차 연속성의 원칙 : 증거물의 수집, 이동, 보관, 분석, 법정 제출의 각 단계에서 담 당사 및 책임자가 명확한가?
- 무결성의 원칙 : 수집된 증거가 위·변조되지 않았는가?

디지털 포렌식 유형



디스크 포렌식

(하드디스크, DVD 등)

- 물리적인 저장장치에서 증거를 수집하고 분석하는 포렌식 분야

시스템 포렌식

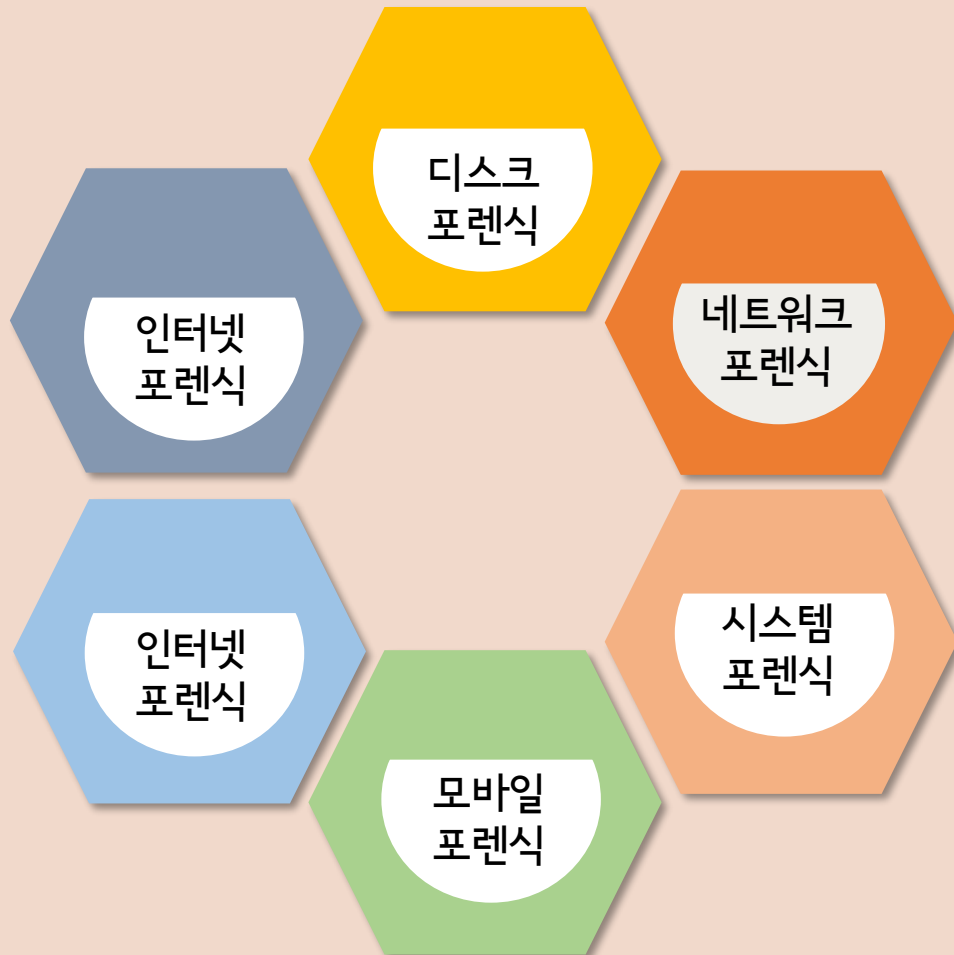
- 컴퓨터의 운영체제, 응용 프로그램, 프로세스를 분석하여 증거를 확보하는 포렌식 분야

모바일 포렌식

(휴대폰, 메모리 카드 등)

- 휴대용 기기에서 필요한 정보를 입수하여 분석하는 포렌식 분야

디지털 포렌식 유형



인터넷 포렌식

(WWW, FTP 등)

- 인터넷 응용 프로토콜을 사용하는 분야에서 증거를 수집하는 포렌식 분야

데이터베이스 포렌식

- 데이터베이스에서 데이터를 추출, 분석하여 증거를 획득하는 포렌식 분야
- 기업의 횡령, 탈세 등을 수사할 때 필수적인 과정

02 네트워크 포렌식

네트워크 포렌식이란?

네트워크 정보와 전송 데이터를 수집하여
필요한 증거를 추출하고 분석하는 포렌식 분야

네트워크
포렌식
특징

- 네트워크 데이터 자료(패킷, 로그)의 법적 증거력을 높여줌
- 네트워크 문제 해결, 공격/위협 감지에 활용됨



- 와이어 샤크(Wireshark)라는 오픈툴을 많이 사용함

네트워크 포렌식 조사 방법론

정보 수집 > 전략 수집 > 증거 수집 > 분석 > 보고서 > 수사 지원 & 보안

- 정보 수집 : 사건, 주변 환경에 대한 정보 수집
- 전략 수집 : 증거 출처의 우선순위 결정 및 증거 수집 계획 세움
- 증거 수집 : 계획을 바탕으로 증거 수집
- 분석 : 수집한 증거를 분석
- 보고서 : 분석에 대한 결과를 문서화함
 - 비전문가도 이해할 수 있는 내용으로 작성해야 함
- 수사 지원 및 보안 : 보고서 결과를 바탕으로 취약점 보안

(1) Wireshark

Wireshark 란?

네트워크를 분석하는 데 사용되는 공개된
패킷 스니핑(packet sniffing) 프로그램

Wireshark 장점

- 다양한 프로토콜 지원 : 대략 850개 지원
- 사용자 환경을 제공
 - Wireshark의 인터페이스는 가장 쉬운 패킷 스니핑 애플리케이션 중 하나.
 - GUI 방식이며 다양한 특징 있음
- 비용 장점 : 무료 배포 소프트웨어로 제공되는 오픈소스 프로그램

(1) Wireshark interface

The image displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into three panes:

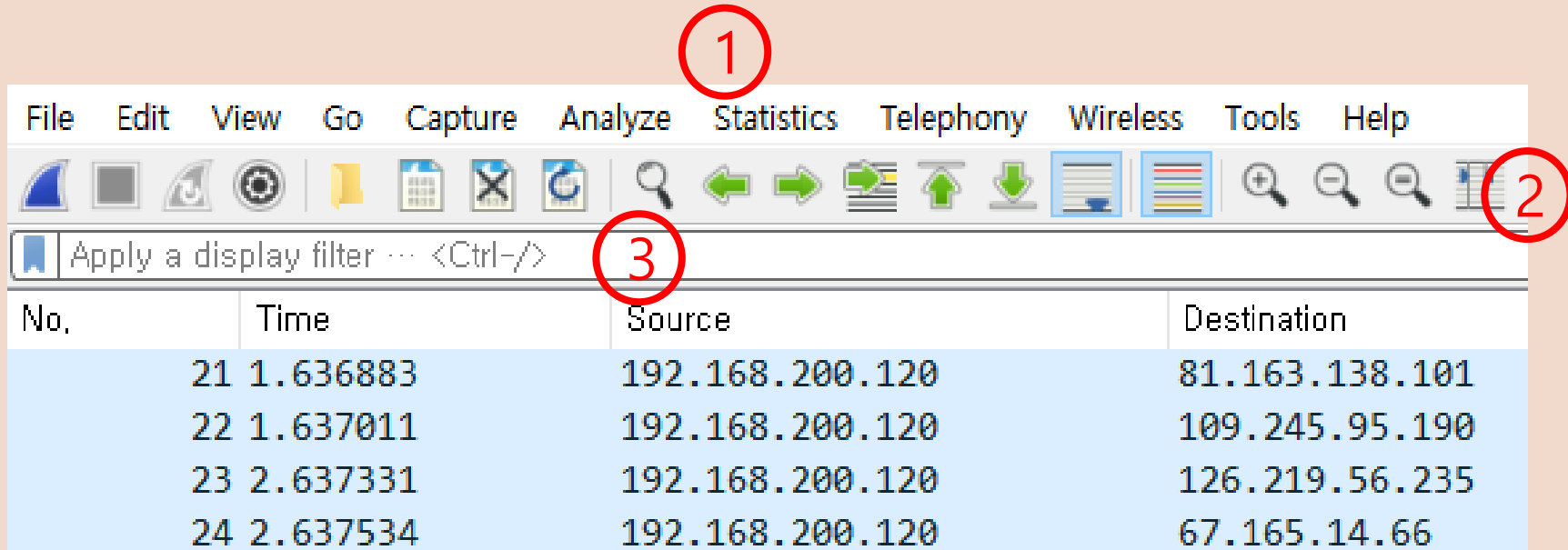
- Packet List Pane:** Shows a list of captured packets. The columns are No., Time, Source, Destination, Protocol, Length, Info, and S_Country. The selected packet is number 21, a UDP packet from 192.168.200.120 to 81.163.138.101.
- Packet Details Pane:** Shows the hierarchical structure of the selected packet. It includes the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol header. The UDP header shows Source Port: 58286 and Destination Port: 6881.
- Packet Bytes Pane:** Shows the raw data of the selected packet in hexadecimal and ASCII. The data starts with 54 d1 63 d2 a2 78 74 e5 f9 ae 1e 1f 08 00 45 00.

No.	Time	Source	Destination	Protocol	Length	Info	S_Country
21	1.636883	192.168.200.120	81.163.138.101	UDP	58286	→ 6881 Len=101	
22	1.637011	192.168.200.120	109.245.95.190	UDP	58286	→ 28692 Len=101	
23	2.637331	192.168.200.120	126.219.56.235	UDP	58286	→ 16371 Len=101	
24	2.637534	192.168.200.120	67.165.14.66	UDP	58286	→ 63578 Len=101	
25	2.637673	192.168.200.120	119.197.198.206	UDP	58286	→ 23178 Len=101	
26	2.638944	192.168.200.120	46.107.223.39	UDP	58286	→ 51413 Len=101	
27	2.639047	192.168.200.120	189.216.249.73	UDP	58286	→ 54131 Len=101	
28	2.646240	119.197.198.206	192.168.200.120	UDP	23178	→ 58286 Len=287	South Korea
29	2.646534	192.168.200.120	23.111.182.106	UDP	58286	→ 60137 Len=101	

Header checksum: 0xe97b [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.200.120
Destination: 81.163.138.101
[Destination GeoIP: Athens, GR, ASN 6799, OTEnet S.A.]
[Destination GeoIP City: Athens]
[Source or Destination GeoIP City: Athens]
[Destination GeoIP Country: Greece]
[Source or Destination GeoIP Country: Greece]
[Destination GeoIP ISO Two Letter Country Code: GR]
[Source or Destination GeoIP ISO Two Letter Country Code: GR]
[Destination GeoIP AS Number: 6799]
[Source or Destination GeoIP AS Number: 6799]
[Destination GeoIP AS Organization: OTEnet S.A.]
[Source or Destination GeoIP AS Organization: OTEnet S.A.]
[Destination GeoIP Latitude: 37.9833]
[Source or Destination GeoIP Latitude: 37.9833]
[Destination GeoIP Longitude: 23.7333]
[Source or Destination GeoIP Longitude: 23.7333]
> User Datagram Protocol, Src Port: 58286, Dst Port: 6881

```
0000 54 d1 63 d2 a2 78 74 e5 f9 ae 1e 1f 08 00 45 00
0010 00 81 60 76 00 00 80 11 e9 7b c0 a8 c8 78 53 eb
0020 13 6e e3 ae 1a e1 00 6d 01 04 64 31 3a 61 64 32
0030 3a 69 64 32 30 3a 68 6c d8 65 d7 6f 02 81 76 dd
0040 1d b5 0c 47 05 56 a3 4c d7 9f 36 3a 74 61 72 67
0050 65 74 32 30 3a 6c 06 44 97 b6 f6 96 f4 87 46 68
0060 1a 59 4e 44 44 8c c9 53 c1 65 31 3a 71 39 3a 66
0070 69 6e 64 5f 6e 6f 64 65 31 3a 74 32 3a 07 a9 31
0080 3a 76 34 3a 4c 54 00 0f 31 3a 79 31 3a 71 65
```

(1) Wireshark interface



- ① 메인 메뉴(Main Menu) : 표준 메뉴
- ② 메인 툴바(Main Toolbar) : 아이콘
- ③ 디스플레이 필터 영역과 필터 표현식 영역(Display Filter Area and Filter Expressions Area) : 특정 트래픽에 초점을 맞춤

(1) Wireshark interface

Apply a display filter ... <Ctrl-/>									
No.	Time	Source	Destination	Protocol	Length	Info	S_Country	D_Country	
21	1.636883	192.168.200.120	81.163.138.101	UDP		143 58286 → 6881 Len=101		Russia	
22	1.637011	192.168.200.120	109.245.95.190	UDP		143 58286 → 28692 Len=101		Serbia	
23	2.637331	192.168.200.120	126.219.56.235	UDP		143 58286 → 16371 Len=101		Japan	
24	2.637534	192.168.200.120	67.165.14.66	UDP		143 58286 → 63578 Len=101		United States	
25	2.637673	192.168.200.120	119.197.198.206	UDP		143 58286 → 23178 Len=101		South Korea	
26	2.638944	192.168.200.120	46.107.223.39	UDP		143 58286 → 51413 Len=101		Hungary	
27	2.639047	192.168.200.120	189.216.249.73	UDP		143 58286 → 54131 Len=101		Mexico	

이름	설명	이름	설명	이름	설명
No.	패킷의 일련 번호를 표시	Destination	패킷의 목적지 주소	Info	Wireshark가 스스로 분석하여 패킷에서 가장 중요한 정보를 판단하여 보여줌
Time	패킷 캡처를 시작하고 걸린 시간	Protocol	프로토콜의 이름		
Source	패킷의 출발지 주소	Length	패킷의 길이(크기)를 bytes로 나타냄	S_Country	패킷의 출발지 나라
				D_Country	패킷의 목적지 주소

(1) Wireshark interface

```
Header checksum: 0xe97b [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.200.120
Destination: 83.235.19.110
▼ [Destination GeoIP: Athens, GR, ASN 6799, OTEnet S.A.]
    [Destination GeoIP City: Athens]
    [Source or Destination GeoIP City: Athens]
    [Destination GeoIP Country: Greece]
    [Source or Destination GeoIP Country: Greece]
    [Destination GeoIP ISO Two Letter Country Code: GR]
    [Source or Destination GeoIP ISO Two Letter Country Code: GR]
    [Destination GeoIP AS Number: 6799]
    [Source or Destination GeoIP AS Number: 6799]
    [Destination GeoIP AS Organization: OTEnet S.A.]
    [Source or Destination GeoIP AS Organization: OTEnet S.A.]
    [Destination GeoIP Latitude: 37.9833]
    [Source or Destination GeoIP Latitude: 37.9833]
    [Destination GeoIP Longitude: 23.7333]
    [Source or Destination GeoIP Longitude: 23.7333]
```

패킷 상세 영역(Packet Details)

- Packet List 영역에서 패킷을 선택했을 때, 선택된 패킷의 상세 한 것을 알려줌
- TCP/IP 4계층을 나누었을 때 각각 계층에 있는 프로토콜들을 알려줌

(1) Wireshark interface

000 = Reserved Not set																
0000	74	e5	f9	ae	1e	1f	54	d1	63	d2	a2	78	08	00	45 00	t.....T. c..x..E.
0010	00	34	07	91	40	00	7f	06	e1	a5	c0	a8	c8	c3	c0 a8	·4··@·····
0020	c8	78	ff	50	e8	73	49	5a	d6	e0	00	00	00	00	80 02	·x·P·sIZ
0030	44	10	10	73	00	00	02	04	05	b4	01	03	03	08	01 01	D··s····· ··
0040	04	02														..

패킷 데이터 영역(Packet Bytes)

- 선택된 패킷을 16진수나 ASCII 문자 코드 등으로 표시
- 맨 좌측의 회색 숫자 부분은 패킷의 위치를 나타냄
- 중앙의 16진수로 표시된 부분은 실제 데이터 보여줌
- 우측 문자 + 기호 부분은 데이터의 내용을 ASCII 문자로 표시해 주는 영역

표준 ASCII 코드표

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	NUL	SOH	STX	ETX	END	ENQ	ACK	BEL	BS	TAB	LF	VT	FF	CR	SO	SI
1	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2		!	"	#	\$	%	&	'	()	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;		=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{		}	~	DEL

(2) ColaSoft

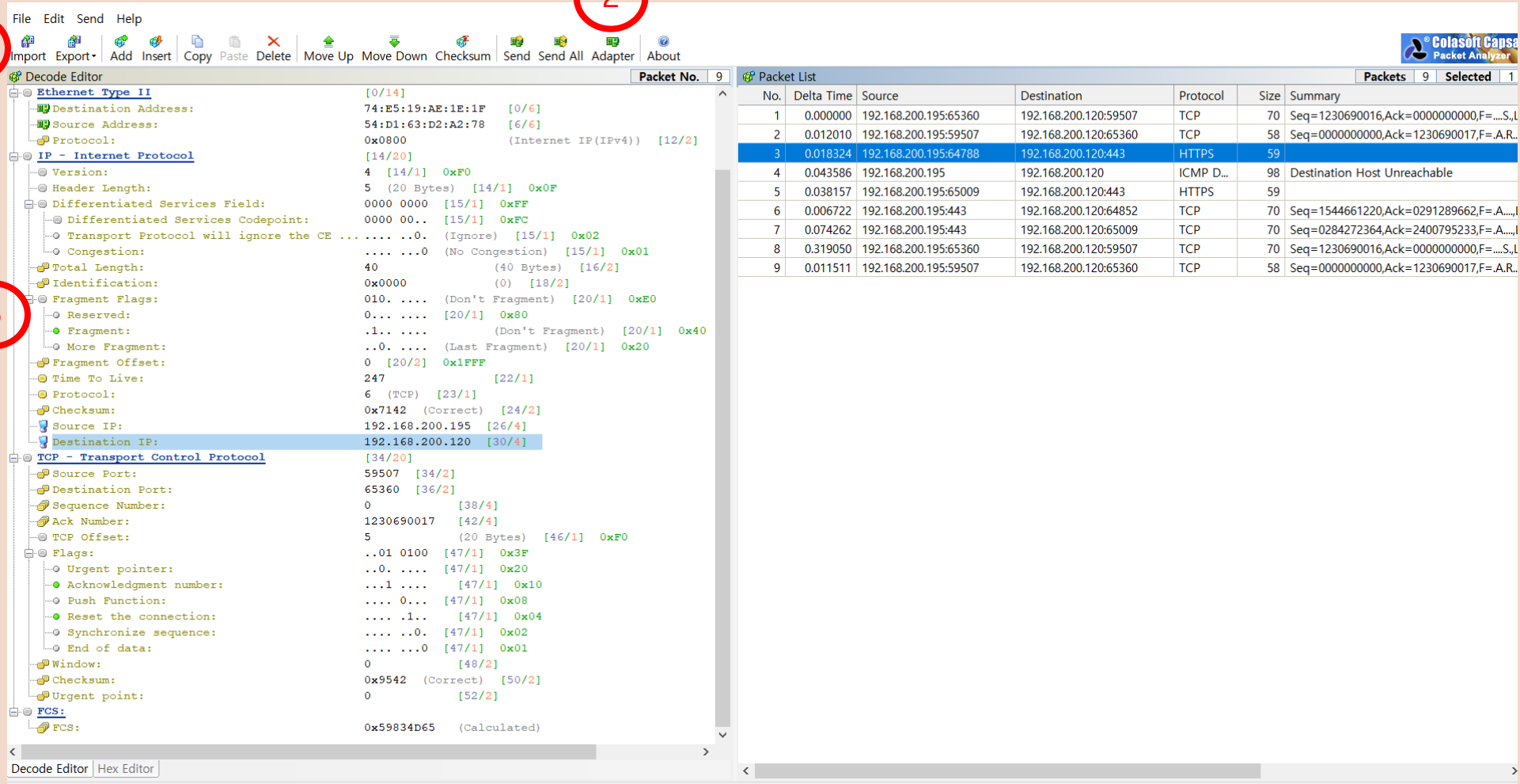
04 Colasoft 란?

사용자 지정 네트워크 패킷을
생성 및 수정할 수 있는 프로그램

Colasoft
기능

- 공격과 침입자에 대한 네트워크 보호를 점검 할 수 있음
- Colasoft Packet Builder는 매우 강력한 편집 기능 포함
- 일반적인 HEX 편집 원시 데이터 외, 디코딩 편집기가 특징
- 사용자가 특정 프로토콜 필드 값을 훨씬 더 쉽게 편집 가능

(2) Colasoft 란?

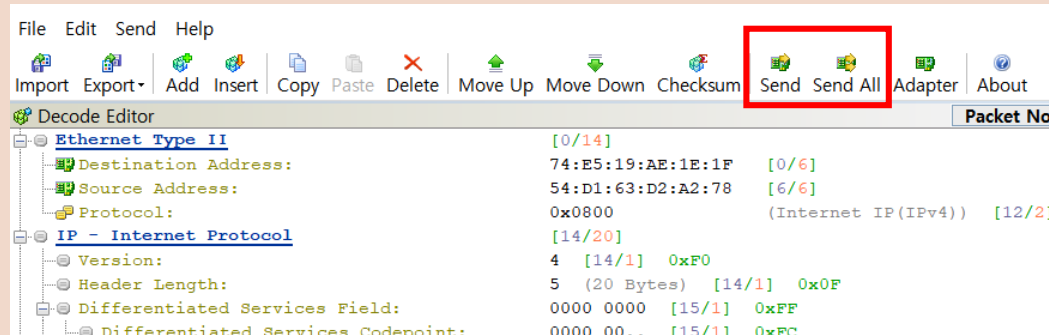


① Import : 패킷 파일 가져오기

② Adapter : 패킷 전송을 위한
활성 네트워크 어댑터

③ 패킷 정보를 변경할 수 있는 창

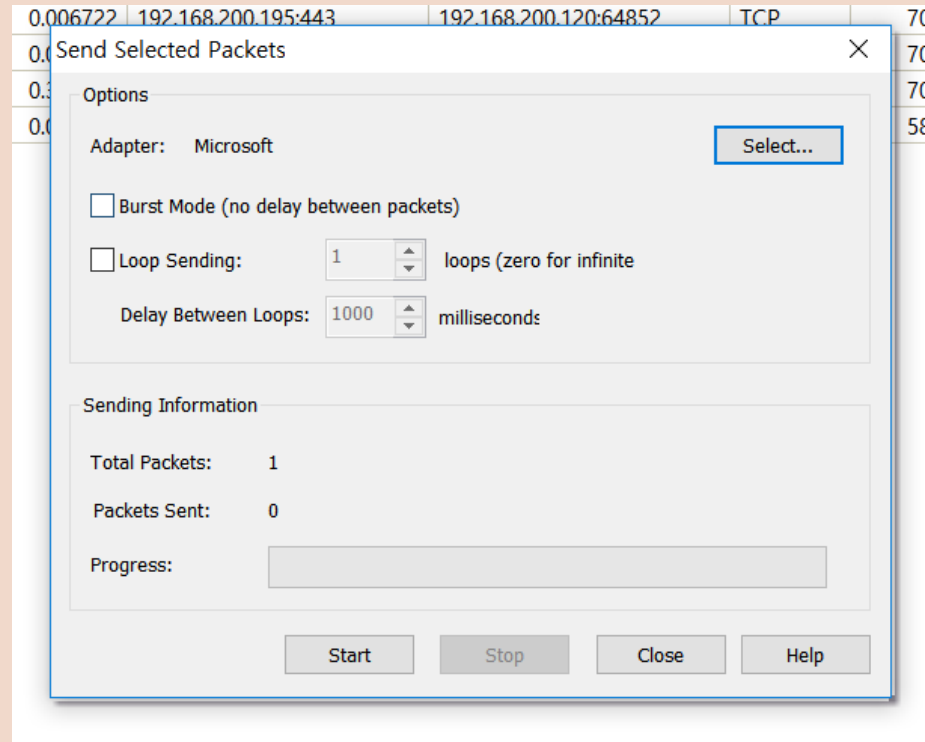
(2) Colasoft 란?



Packet List							Packets
No.	Delta Time	Source	Destination	Protocol	Size	Summary	
1	0.000000	192.168.200.195:65360	192.168.200.120:59507	TCP	70	Seq=1230690016,Ack=0000000000,F=....S.,Len= 28,Win=17520	
2	0.012010	192.168.200.195:59507	192.168.200.120:65360	TCP	58	Seq=0000000000,Ack=1230690017,F=.A.R.,Len= 0,Win= 0	
3	0.018324	192.168.200.195:64788	192.168.200.120:443	HTTPS	59		
4	0.043586	192.168.200.195	192.168.200.120	ICMP D...	98	Destination Host Unreachable	
5	0.038157	192.168.200.195:65009	192.168.200.120:443	HTTPS	59		
6	0.006722	192.168.200.195:443	192.168.200.120:64852	TCP	70	Seq=1544661220,Ack=0291289662,F=.A...,Len= 0,Win= 343	
7	0.074262	192.168.200.195:443	192.168.200.120:65009	TCP	70	Seq=0284272364,Ack=2400795233,F=.A...,Len= 0,Win= 265	
8	0.319050	192.168.200.195:65360	192.168.200.120:59507	TCP	70	Seq=1230690016,Ack=0000000000,F=....S.,Len= 0,Win=17424	
9	0.011511	192.168.200.195:59507	192.168.200.120:65360	TCP	58	Seq=0000000000,Ack=1230690017,F=.A.R.,Len= 0,Win= 0	

전송할 패킷을 고르면 Send 나 Send All 버튼을 누름

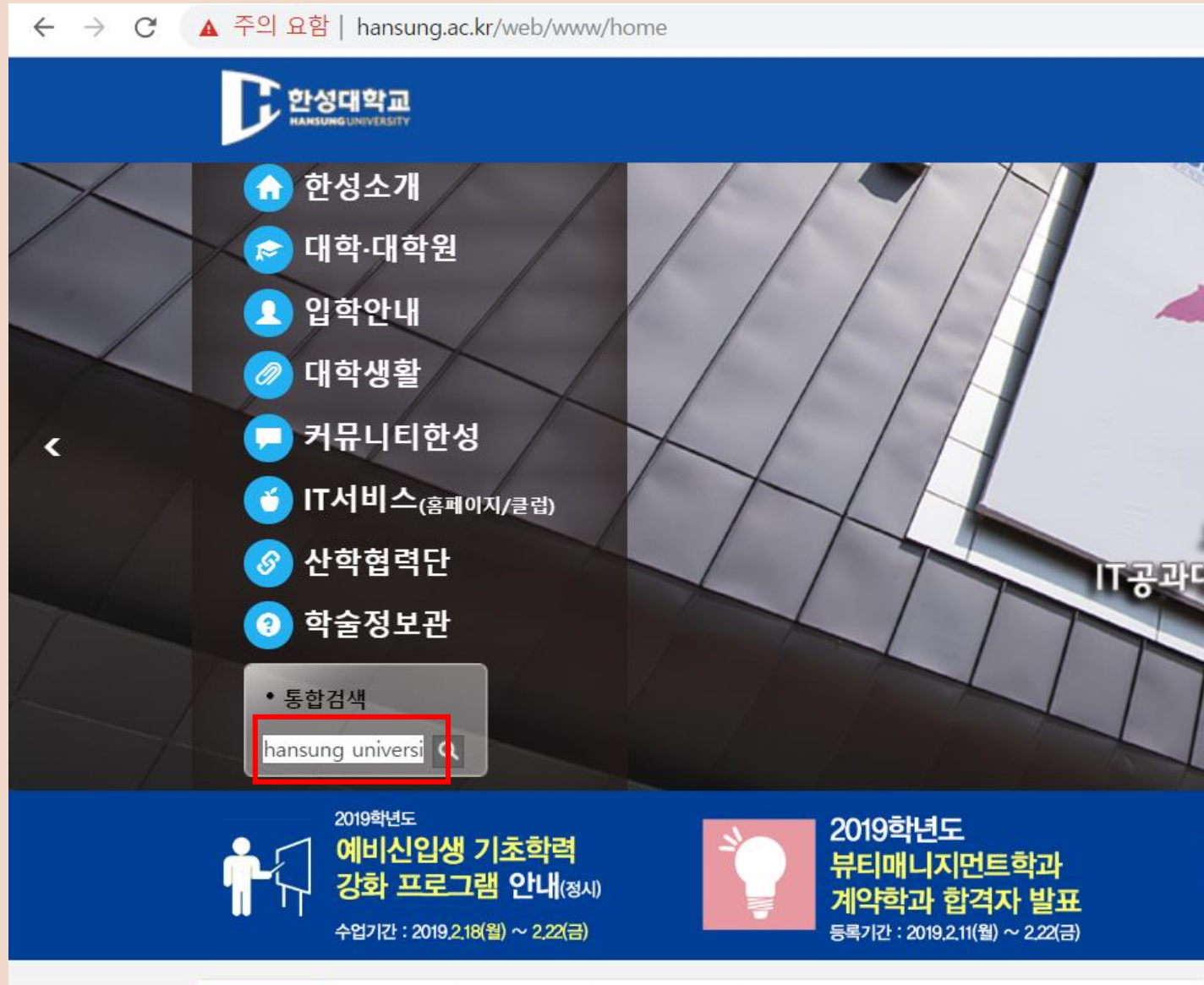
(2) Colasoft 란?



-
- Burst Mode : 체크 시 대기 없이 패킷을 차례로 보냄
 - Loop Sending : 패킷 파일의 루프타임을 지정
 - 패킷을 수동으로 정지할 때까지 계속 송신하고자 하는 경우 0 입력
 - Delay Between Loops : 모든 루프 사이의 간격


(3) 실습 I

(3) 실습 I - 스니핑(Sniffing)




(3) 실습 I - 스니핑(Sniffing)

← → ↺ ⓘ 주의 요함 | hansung.ac.kr/web/www/search_01?gSearch=hansung%20university




한성대학교
HANSUNG UNIVERSITY

LOGIN MYPAGE SITEMAP



- 한성소개
- 대학 · 대학원
- 입학안내
- 대학생활
- 커뮤니티 한성
- IT서비스
- 산학협력단




홈페이지 내 검색


🏠 > 기타 > 검색 > 홈페이지 내 검색

×🔍

About 31,200 results (0.32 seconds) Sort by: **Relevance** ▾



home - Hansung University (English Version)
<https://www.hansung.ac.kr/web/english/home>
University. College of Liberal Arts · College of Social Sciences · College of arts · School of Engineering · liberal art and science department ...



Hansung University - Hansung University (English Version)
https://www.hansung.ac.kr/web/english/intro_h
Hansung University Station, Subway Line 4. Shuttle bus : bus stop at Hansung University

한성소식
HANSUNG NEWS


한성공지 학사공지 장학공

- 2019년 한국마사회장학관
- 2019학년도 신입생 학부
- 학술정보관 3기 서포터즈
- 지식재산&벤처창업 교과
- 2019학년도 뷰티매니지먼트


낙산메아리 +

- 창업대상/ 넥스트데이 네
- 컴공 1학기 캡스톤(졸작)
- 19년 상반기 농협 직원 차
- [한성대신문사] 🍌 'Hello, M
- [한성대신문사] 🍌 장학금

HSU ISSUE +



국제교류원,
국제교류원,
프로그램 최
교(총장 이상
기계시스템공



TOP
기계시스템공
한기두레, 사
펼쳐 한성대

한성인

(3) 실습 I - 스니핑(Sniffing)

The image shows a Wireshark network traffic capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A red box highlights the 'http' filter in the packet list pane. The packet list pane displays a table of captured packets, with the selected packet (No. 2860) highlighted in blue. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
2847	21.570914	192.168.35.5	220.66.102.11	TCP	54	53592 → 80 [ACK] Seq=...
2848	21.572659	220.66.102.11	192.168.35.5	TCP	1434	80 → 53592 [ACK] Seq=... Sou
2849	21.572662	220.66.102.11	192.168.35.5	TCP	1434	80 → 53592 [ACK] Seq=... Sou
2850	21.572667	220.66.102.11	192.168.35.5	TCP	1434	80 → 53592 [ACK] Seq=... Sou
2851	21.572845	192.168.35.5	220.66.102.11	TCP	54	53592 → 80 [ACK] Seq=...
2852	21.574133	220.66.102.11	192.168.35.5	TCP	1434	80 → 53592 [ACK] Seq=... Sou
2853	21.574135	220.66.102.11	192.168.35.5	TCP	1199	80 → 53592 [PSH, ACK]... Sou
2854	21.574140	220.66.102.11	192.168.35.5	TCP	1434	80 → 53592 [ACK] Seq=... Sou
2855	21.574141	220.66.102.11	192.168.35.5	TCP	1434	80 → 53592 [ACK] Seq=... Sou
2856	21.574330	192.168.35.5	220.66.102.11	TCP	54	53592 → 80 [ACK] Seq=...
2857	21.575595	220.66.102.11	192.168.35.5	TCP	1434	80 → 53592 [ACK] Seq=... Sou
2858	21.575599	220.66.102.11	192.168.35.5	TCP	1434	80 → 53592 [ACK] Seq=... Sou
2859	21.575605	220.66.102.11	192.168.35.5	TCP	1238	80 → 53592 [PSH, ACK]... Sou
2860	21.575875	192.168.35.5	220.66.102.11	TCP	54	53592 → 80 [ACK] Seq=...

<

- > Frame 2822: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- > Ethernet II, Src: IntelCor_ae:1e:1f (74:e5:f9:ae:1e:1f), Dst: Hfr_32:77:58 (00:23:aa:32:77:58)
- > Internet Protocol Version 4, Src: 192.168.35.5, Dst: 220.66.102.11
- > Transmission Control Protocol, Src Port: 53592, Dst Port: 80, Seq: 0, Len: 0

(3) 실습 I - 스니핑(Sniffing)

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info	S_Country	D_Country
32	6.774954	192.168.35.5	220.66.102.11	HTTP	999	GET /web/www/search_0...		South Korea
117	7.107898	220.66.102.11	192.168.35.5	HTTP	1296	HTTP/1.1 200 OK (tex...	South Korea	
174	7.904280	192.168.35.5	172.217.31.174	HTTP	1093	GET /generate_204 HTT...		United States
177	7.938589	172.217.31.174	192.168.35.5	HTTP	137	HTTP/1.1 204 No Conte...	United States	
255	8.594824	192.168.35.5	211.115.106.78	HTTP	451	GET /jk?c=62&p=GUE8WB...		South Korea
261	8.596191	192.168.35.5	211.115.106.78	HTTP	451	GET /jk?c=62&p=GUE8WB...		South Korea
262	8.596283	192.168.35.5	211.115.106.78	HTTP	451	GET /jk?c=62&p=GUE8WB...		South Korea
264	8.599191	211.115.106.78	192.168.35.5	HTTP	406	HTTP/1.1 200 OK	South Korea	
267	8.599894	211.115.106.78	192.168.35.5	HTTP	406	HTTP/1.1 200 OK	South Korea	
270	8.600318	192.168.35.5	211.115.106.78	HTTP	451	GET /jk?c=62&p=GUE8WB...		South Korea
271	8.600620	211.115.106.78	192.168.35.5	HTTP	406	HTTP/1.1 200 OK	South Korea	
273	8.604940	211.115.106.78	192.168.35.5	HTTP	406	HTTP/1.1 200 OK	South Korea	

<

> Frame 262: 451 bytes on wire (3608 bits), 451 bytes captured (3608 bits) on interface 0
> Ethernet II, Src: IntelCor_ae:1e:1f (74:e5:f9:ae:1e:1f), Dst: Hfr_32:77:58 (00:23:aa:32:77:58)
> Internet Protocol Version 4, Src: 192.168.35.5, Dst: 211.115.106.78
> Transmission Control Protocol, Src Port: 53686, Dst Port: 80, Seq: 1, Ack: 1, Len: 397
> Hypertext Transfer Protocol
> GET /jk?c=62&p=GUE8WBGa9pLWrdut6KZINNxbEAsTt13S9KmiBUInKQO=&k=1 HTTP/1.1\r\n
Accept: */*\r\n
User-Agent: MeDCore\r\n
Connection: keep-alive\r\n

(3) 실습 I - 스니핑(Sniffing)

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info	S_Country	D_Country
32	6.774954	192.168.35.5	220.66.102.11	HTTP	999	GET /web/www/search_0...		South Korea
117	7.107898	220.66.102.11	192.168.35.5	HTTP	1296	HTTP/1.1 200 OK (tex...	South Korea	
174	7.904280	192.168.35.5	172.217.31.174	HTTP	1093	GET /generate_204 HTT...		United States
177	7.938589	172.217.31.174	192.168.35.5	HTTP	137	HTTP/1.1 204 No Conte...	United States	
255	8.594824	192.168.35.5	211.115.106.78	HTTP	451	GET /jk?c=62&p=Gue8WB...		South Korea
261	8.596191	192.168.35.5	211.115.106.78	HTTP	451	GET /jk?c=62&p=Gue8WB...		South Korea
262	8.596283	192.168.35.5	211.115.106.78	HTTP	451	GET /jk?c=62&p=Gue8WB...		South Korea
264	8.599191	211.115.106.78	192.168.35.5	HTTP	406	HTTP/1.1 200 OK	South Korea	
267	8.599894	211.115.106.78	192.168.35.5	HTTP	406	HTTP/1.1 200 OK	South Korea	
270	8.600318	192.168.35.5	211.115.106.78	HTTP	451	GET /jk?c=62&p=Gue8WB...		South Korea
271	8.600620	211.115.106.78	192.168.35.5	HTTP	406	HTTP/1.1 200 OK	South Korea	
273	8.604940	211.115.106.78	192.168.35.5	HTTP	406	HTTP/1.1 200 OK	South Korea	

< >

> Frame 32: 999 bytes on wire (7992 bits), 999 bytes captured (7992 bits) on interface 0
> Ethernet II, Src: IntelCor_ae:1e:1f (74:e5:f9:ae:1e:1f), Dst: Hfr_32:77:58 (00:23:aa:32:77:58)
> Internet Protocol Version 4, Src: 192.168.35.5, Dst: 220.66.102.11
> Transmission Control Protocol, Src Port: 53675, Dst Port: 80, Seq: 1, Ack: 1, Len: 945
> Hypertext Transfer Protocol
> GET /web/www/search_01?Search=hansung%20university HTTP/1.1\r\nHost: hansung.ac.kr\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\nReferer: http://hansung.ac.kr/web/www/home\r\nAccept-Encoding: gzip, deflate\r\n

검색어 확인 가능

(4) 실습 II

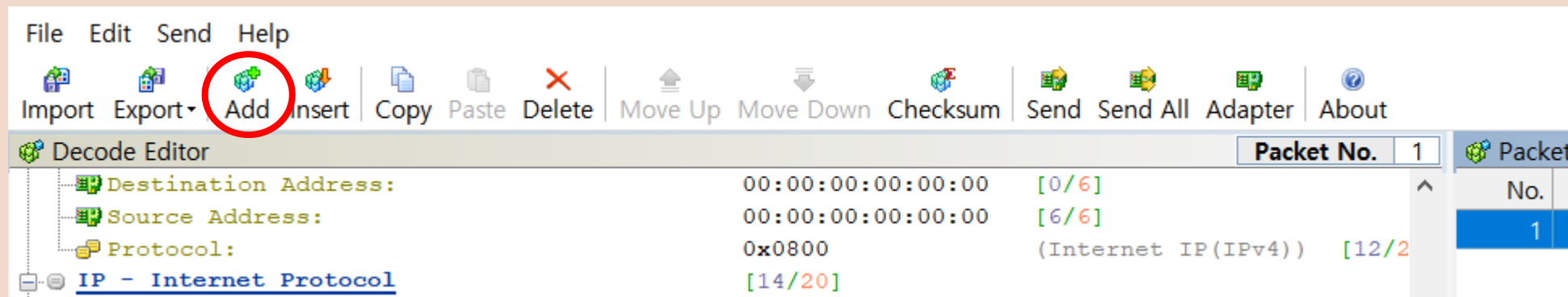
(4) 실습 II - SYN Flooding Attack

SYN Flooding Attack 란?

DoS(Denial of Service)공격 중 하나.

TCP 연결과정에서 무수히 많은 SYN 패킷을 서버에게 전송함으로써
서버의 원활한 통신을 방해하는 공격

(4) 실습 II - SYN Flooding Attack



Colasoft를 이용하여 TCP 패킷을 만들어 준다.

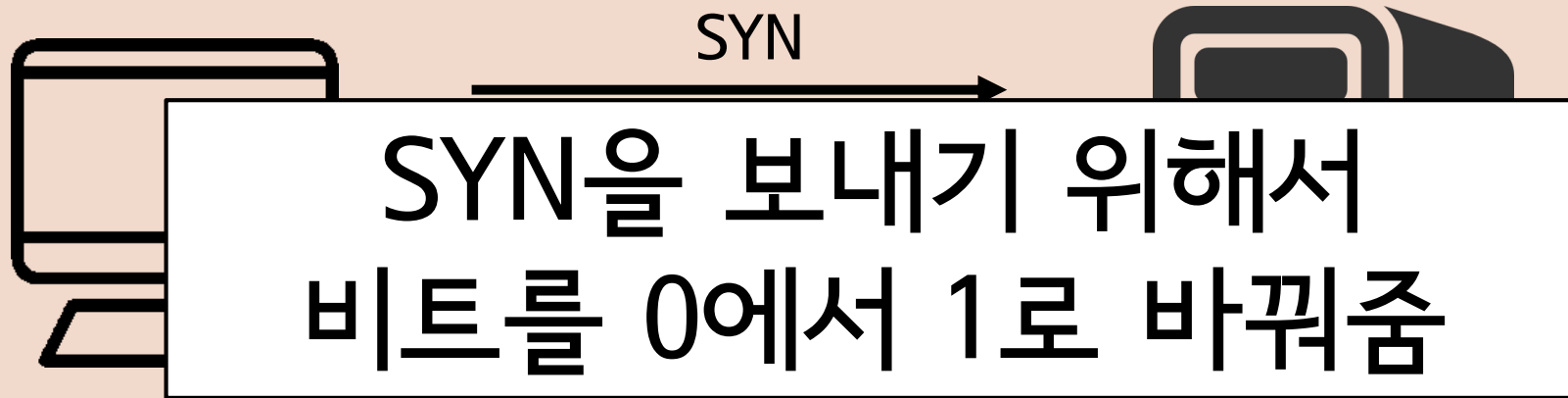
(4) 실습 II - SYN Flooding Attack

Destination Address:	00:00:00:00:00:00	[0/6]
Source Address:	00:00:00:00:00:00	[6/6]
Protocol:	0x0800	(Internet IP(IPv4))
IP - Internet Protocol		
[14/20]		
Version:	4	[14/1] 0xF0
Header Length:	5 (20 Bytes)	[14/1] 0x0F
Differentiated Services Field:	0000 0000	[15/1] 0xFF
Differentiated Services Codepoint:	0000 00..	[15/1] 0xFC
Transport Protocol will ignore the CE0.	(Ignore) [15/1] 0x02
Congestion:0	(No Congestion) [15/1] 0x01
Total Length:	46	(46 Bytes) [16/2]
Identification:	0x0000	(0) [18/2]
Fragment Flags:	010.	(Don't Fragment) [20/1] 0xE0
Reserved:	0...	[20/1] 0x80
Fragment:	.1..	(Don't Fragment) [20/1]
More Fragment:	..0.	(Last Fragment) [20/1] 0x20
Fragment Offset:	0	[20/2] 0x1FFF
Time To Live:	64	[22/1]
Protocol:	6 (TCP)	[23/1]
Checksum:	0x0000	(#Error, should be 0xAC72) [24/2]
Source IP:	192.168.234.1	[26/4]
Destination IP:	192.168.35.5	[30/4]
TCP - Transport Control Protocol		
[34/20]		
Source Port:	0	[34/2]
Destination Port:	0	[36/2]
Sequence Number:	0	[38/4]
[Next Sequence Number:]	6	
Ack Number:	0	[42/4]
TCP Offset:	5	(20 Bytes) [46/1] 0xF0
Flags:	..00 0010	[47/1] 0x3F
Urgent pointer:	..0.	[47/1] 0x20
Acknowledgment number:	...0	[47/1] 0x10
Push Function: 0...	[47/1] 0x08
Reset the connection:0..	[47/1] 0x04
Synchronize sequence:1.	[47/1] 0x02
End of data:0	[47/1] 0x01
Window:	65532	[48/2]
Checksum:	0x0000	(#Error, should be 0x2188) [50/2]
Urgent point:	0	[52/2]

공격대상을 설정해준 뒤, TCP Flag의 Syn sequence 비트를 0에서 1로 바꿔 줌으로써 SYN packet traffic 생성준비 완료

(4) 실습 II - SYN Flooding Attack

Syn sequence 비트를 0에서 1로 바꿔주는 이유는?



3-Way hand shake라는 TCP 고유의 연결방식 때문이다.

1. Client가 Server에게 동기화를 요청(SYN)
2. Server가 Client의 요청을 받아들인다 대답(ACK) + Client에게 동기화 요청(SYN)
3. Client가 Server의 동기화 요청을 응답(ACK)

➡ Client와 Server 사이에 세션이 이루어짐

(4) 실습 II - SYN Flooding Attack

Send Selected Packets

Options

Adapter: Microsoft Select...

☒ Burst Mode (no delay between packets)

☒ Loop Sending: 10000 loops (zero for infinite)

Delay Between Loops: 0.0001 milliseconds

Sending Information

Total Packets: 1 * 10000 = 10000

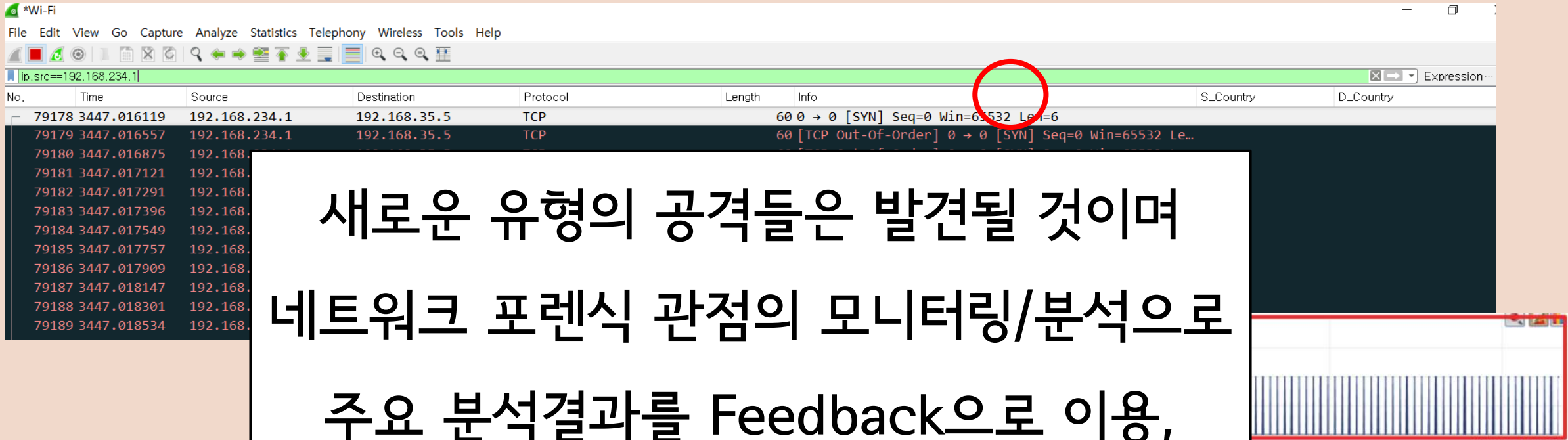
Packets Sent: 0

Progress:

Start Stop Close Help

반복적으로 SYN packet 전송

(4) 실습 II - SYN Flooding Attack



새로운 유형의 공격들은 발견될 것이며
네트워크 포렌식 관점의 모니터링/분석으로
주요 분석결과를 Feedback으로 이용,
기존정책의 지속적 보완이 필요

➡ 비정상적인 네트워크 트래픽으로 판단

03 디스크 포렌식

(1) 기본개념

MBR 란?

마스터 부트 레코드(Master Boot Record, MBR) 또는 파티션 섹터 (Partition Sector)는 파티션 된 기억 장치(이른테면 하드 디스크)의 첫 섹터인 512 바이트 시동 섹터

→ 하드 디스크 드라이브의 기억 공간

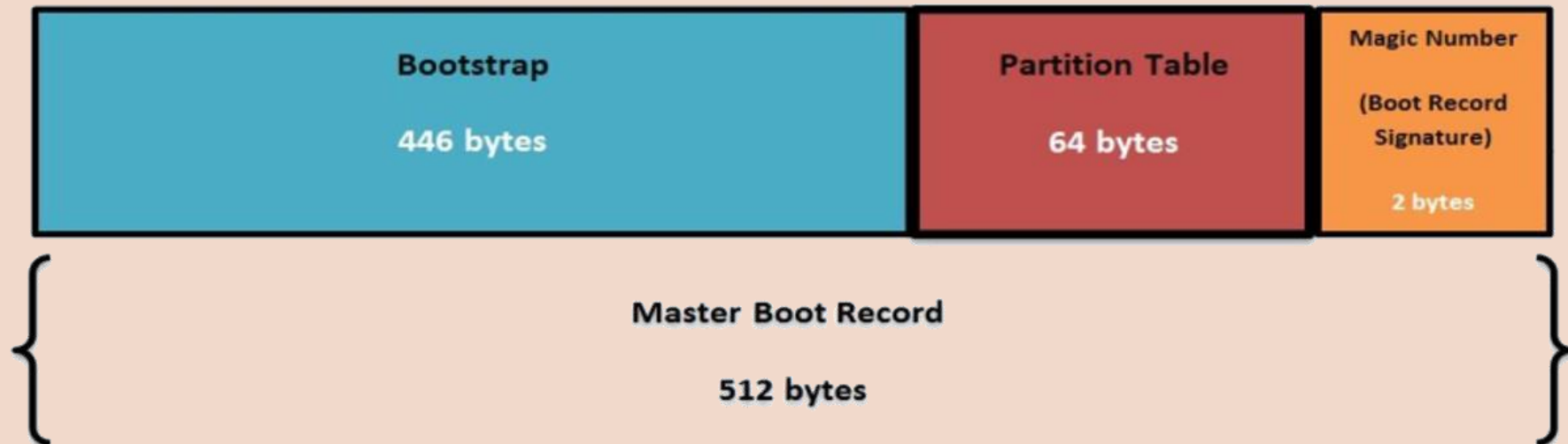


(1) 기본개념

BR 란?

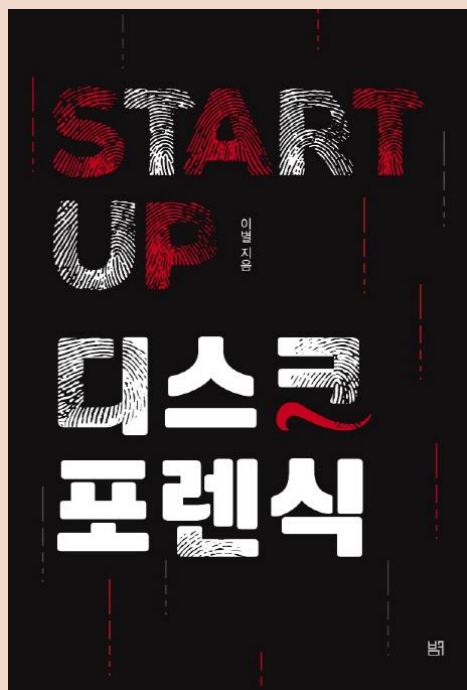
부트 레코드(Boot Record, BR)의 약자로 디스크의 운영 체계를
컴퓨터 시스템에 설치하기 위한 명령어를 저장하고 있는 곳이다.



컴퓨터를 부팅할 때 맨 처음 읽히는 레코드



(2) 실습 III

사용한 프로그램



- vmware (가상머신) 
 - 악성코드에 감염된 이미지 파일을 안전하게 실행해볼 수 있음
- HxD Editor 
 - 2진 파일을 읽을 수 있는 무료 에디터 프로그램
 - 이미지 파일의 특정 섹터를 확인하거나 수정할 때 사용됨
- FTK Imager 
 - 디스크 이미징 작업에 쓰이는 프로그램

(2) 실습 설명

악성코드 감염 MBR 복구

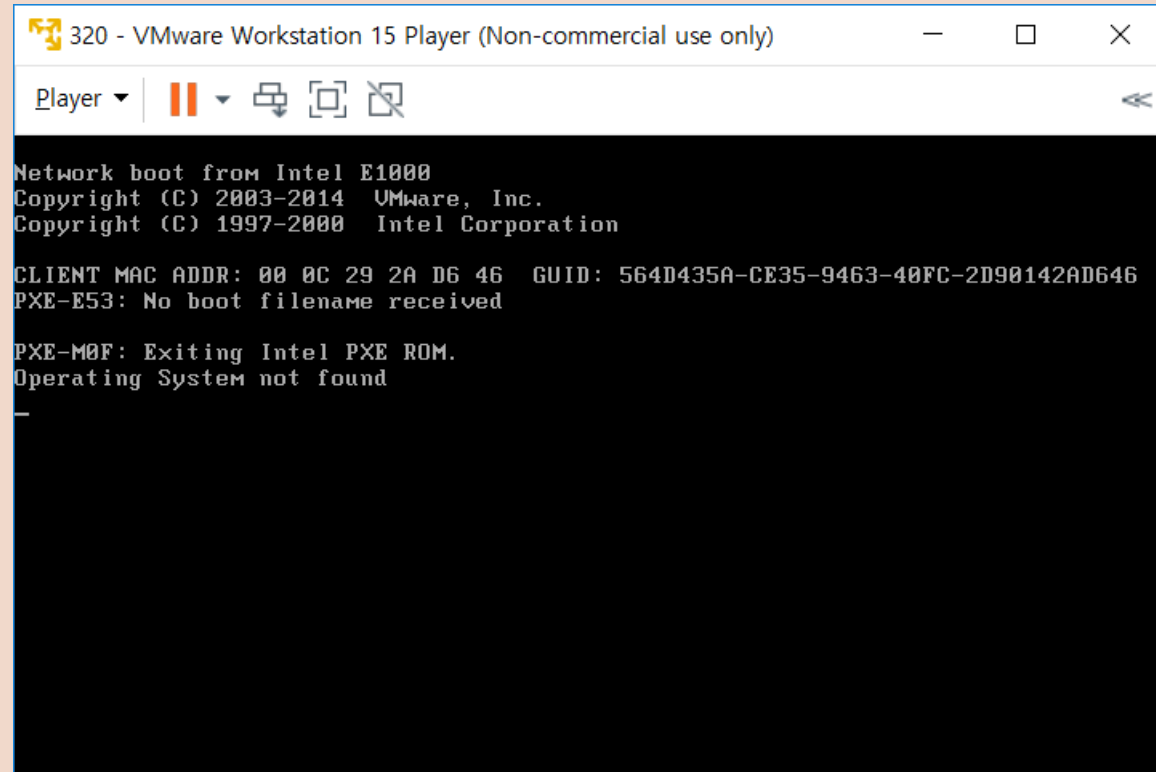
악성코드

: MBR영역과 VBR(Volume Boot Record, 파티션 시작위치(BR) 을
모두 특정 문자열로 덮어쓰워 부팅이 불가능하도록 한 악성코드

MBR 및 BR 영역이 모두 손상된 파티션 복구 → 부팅 가능케 함

(2) 실습 설명

악성코드 감염 MBR 복구



VMWare를 통해 불러온 부팅에 실패한 모습

(2) 실습 진행 과정

-  STEP 1 MBR 영역 확인
-  STEP 2 첫 번째 파티션 복구
-  STEP 3 두 번째 파티션 복구
-  STEP 4 복구 및 GUID 확인

(2) STEP1) MBR영역 확인

HxD에서 파티션 테이블의 Boot Flag 변경

MBR_446byte																	Decoded text
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000060	26	66	68	00	00	00	00	66	FF	76	08	68	00	00	68	00	&fh....fÿv.h..h.
00000070	7C	68	01	00	68	10	00	B4	42	8A	56	00	8B	F4	CD	13	h..h..'BŠV.<ôí.
00000080	9F	83	C4	10	9E	EB	14	B8	01	02	BB	00	7C	8A	56	00	ŸfÄ.žě...». ŠV.
00000090	8A	76	01	8A	4E	02	8A	6E	03	CD	13	66	61	73	1C	FE	Šv.ŠN.Šn.í.fas.p
000000A0	4E	11	75	0C	80	7E	00	80	0F	84	8A	00	B2	80	EB	84	N.u.€~.€..Š.°eë„
000000B0	55	32	E4	8A	56	00	CD	13	5D	EB	9E	81	3E	FE	7D	55	U2äŠV.í.]ěž.>p}U
000000C0	AA	75	6E	FF	76	00	E8	8D	00	75	17	FA	B0	D1	E6	64	*unÿv.è..u.ú°Ñäd
000000D0	E8	83	00	B0	DF	E6	60	E8	7C	00	B0	FF	E6	64	E8	75	èf.°Bæ`è .°ÿädèu
000000E0	00	FB	B8	00	BB	CD	1A	66	23	C0	75	3B	66	81	FB	54	.û,.»í.f#Äu;f.ûT
000000F0	43	50	41	75	32	81	F9	02	01	72	2C	66	68	07	BB	00	CPAu2.ù..r,fh.».
00000100	00	66	68	00	02	00	00	66	68	08	00	00	00	66	53	66	.fh....fh....fSf
00000110	53	66	55	66	68	00	00	00	66	68	00	7C	00	00	66	66	SfUfh....fh. ..f
00000120	61	68	00	00	07	CD	1A	5A	32	F6	EA	00	7C	00	00	CD	ah...í.Z2öè. ..í
00000130	18	A0	B7	07	EB	08	A0	B6	07	EB	03	A0	B5	07	32	E4	. . .ë. ¶.ë. p.2ä
00000140	05	00	07	8B	F0	AC	3C	00	74	09	BB	07	00	B4	0E	CD	...<ð-<.t.»...'.í
00000150	10	EB	F2	F4	EB	FD	2B	C9	E4	64	EB	00	24	02	E0	F8	.ëöðëÿ+Éädë.\$.àø
00000160	24	02	C3	49	6E	76	61	6C	69	64	20	70	61	72	74	69	\$.ÄInvalid parti
00000170	74	69	6F	6E	20	74	61	62	6C	65	00	45	72	72	6F	72	tion table.Error
00000180	20	6C	6F	61	64	69	6E	67	20	6F	70	65	72	61	74	69	loading operati
00000190	6E	67	20	73	79	73	74	65	6D	00	4D	69	73	73	69	6E	ng system.Missin
000001A0	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	g operating syst
000001B0	65	6D	00	00	00	63	7B	9A	78	6D	EF	00	00	00	00	00	em...c{šxmi.....
000001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AAU*

Offset(h): 60

MBR_446byte																	Decoded text
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000060	26	66	68	00	00	00	00	66	FF	76	08	68	00	00	68	00	&fh....fÿv.h..h.
00000070	7C	68	01	00	68	10	00	B4	42	8A	56	00	8B	F4	CD	13	h..h..'BŠV.<ôí.
00000080	9F	83	C4	10	9E	EB	14	B8	01	02	BB	00	7C	8A	56	00	ŸfÄ.žě...». ŠV.
00000090	8A	76	01	8A	4E	02	8A	6E	03	CD	13	66	61	73	1C	FE	Šv.ŠN.Šn.í.fas.p
000000A0	4E	11	75	0C	80	7E	00	80	0F	84	8A	00	B2	80	EB	84	N.u.€~.€..Š.°eë„
000000B0	55	32	E4	8A	56	00	CD	13	5D	EB	9E	81	3E	FE	7D	55	U2äŠV.í.]ěž.>p}U
000000C0	AA	75	6E	FF	76	00	E8	8D	00	75	17	FA	B0	D1	E6	64	*unÿv.è..u.ú°Ñäd
000000D0	E8	83	00	B0	DF	E6	60	E8	7C	00	B0	FF	E6	64	E8	75	èf.°Bæ`è .°ÿädèu
000000E0	00	FB	B8	00	BB	CD	1A	66	23	C0	75	3B	66	81	FB	54	.û,.»í.f#Äu;f.ûT
000000F0	43	50	41	75	32	81	F9	02	01	72	2C	66	68	07	BB	00	CPAu2.ù..r,fh.».
00000100	00	66	68	00	02	00	00	66	68	08	00	00	00	66	53	66	.fh....fh....fSf
00000110	53	66	55	66	68	00	00	00	66	68	00	7C	00	00	66	66	SfUfh....fh. ..f
00000120	61	68	00	00	07	CD	1A	5A	32	F6	EA	00	7C	00	00	CD	ah...í.Z2öè. ..í
00000130	18	A0	B7	07	EB	08	A0	B6	07	EB	03	A0	B5	07	32	E4	. . .ë. ¶.ë. p.2ä
00000140	05	00	07	8B	F0	AC	3C	00	74	09	BB	07	00	B4	0E	CD	...<ð-<.t.»...'.í
00000150	10	EB	F2	F4	EB	FD	2B	C9	E4	64	EB	00	24	02	E0	F8	.ëöðëÿ+Éädë.\$.àø
00000160	24	02	C3	49	6E	76	61	6C	69	64	20	70	61	72	74	69	\$.ÄInvalid parti
00000170	74	69	6F	6E	20	74	61	62	6C	65	00	45	72	72	6F	72	tion table.Error
00000180	20	6C	6F	61	64	69	6E	67	20	6F	70	65	72	61	74	69	loading operati
00000190	6E	67	20	73	79	73	74	65	6D	00	4D	69	73	73	69	6E	ng system.Missin
000001A0	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	g operating syst
000001B0	65	6D	00	00	00	63	7B	9A	78	6D	EF	00	00	00	00	00	em...c{šxmi...e
000001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AAU*

Offset(h): 1Bf * Modi

정상적인 OS를 가진 MBR의 Boot Flag를 80으로 변경 → 부팅 가능하게 함

(2) STEP1) MBR영역 확인

“ **HASTATI.** ” 검색했을 때 총 3곳에서 문자열 검색 됨

- 첫 번째 : MBR 영역
- 두 번째 : 첫 번째 파티션 시작 위치
- 세 번째 : 두 번째 파티션 시작 위치

Custom Content Sources

Evidence:File System Path File	Options
0000ffff	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00010000	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
00010001	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
00010002	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
00010003	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
00010004	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
00010005	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
00010006	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
00010007	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
00010008	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
00010009	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
0001000a	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
0001000b	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
0001000c	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
0001000d	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
0001000e	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
0001000f	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
00010010	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.
00010011	48 41 53 54 41 54 49 2E 48 41 53 54 41 54 49 2E HASTATI. HASTATI.

Cursor pos = 1048575; phy sec = 2048

첫 번째 파티션 시작 위치 : 2048 섹터

(2) STEP2) 첫 번째 파티션 복구

파티션 복구를 위해서 필요한 사항

- 부팅가능 여부 확인
- 파티션 타입 확인
- 파티션 시작주소 확인
- 파티션 총 섹터 수 확인



파티션 테이블(16byte)와 손상된 BR영역 복구



부팅가능 여부 : 80으로 변경하여 부팅 가능해짐

(2) STEP2) 첫 번째 파티션 복구 ① 파티션 시작주소 확인

Custom Content Sources

Evidence:File System|Path|File Options

New Edit Remove Remove All Create Image

Properties Hex Value I... Custom Co...

For User Guide, press F1

0000ffff0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 ...
000100000 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E HASTATI. HASTATI.
000100010 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E HASTATI. HASTATI.
000100020 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E HASTATI. HASTATI.
000100030 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E HASTATI. HASTATI.
000100040 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E HASTATI. HASTATI.
000100050 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E HASTATI. HASTATI.
000100060 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E HASTATI. HASTATI.
000100070 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E
000100080 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E
000100090 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E
0001000a0 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E
0001000b0 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E
0001000c0 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E
0001000d0 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E
0001000e0 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E
0001000f0 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E HASTATI. HASTATI.
000100100 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E HASTATI. HASTATI.
000100110 48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E HASTATI. HASTATI.

Cursor pos = 1048575; phy sec = 2048

Ctrl+F : HASTATI. 검색
- 두 번째로 나오는 영역이
첫 번째 손상된 BR 영역

첫 번째 파티션 시작주소 : 0x100000

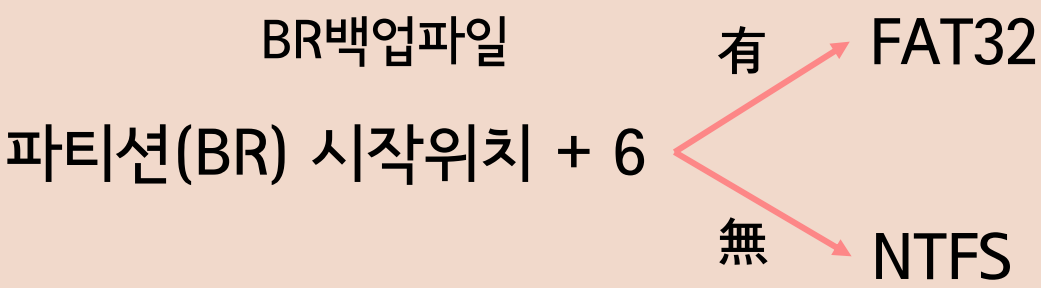
디스크는 섹터 단위로 이동함 → 16진수를 섹터 단위로 변환해야 함



$$0x100000 / 0x200 = 0x800$$

섹터 단위 : 512 byte (=0x200)

(2) STEP2) 첫 번째 파티션 복구 ② 파티션 타입 확인



$$2048(\text{첫번째 파티션 시작 위치}) + 6 = 2054$$

Custom Content Sources

Evidence:File System|Path|File Options

New Edit Remove Remove All Create Image

Properties Hex Value l... Custom Co...

000100cc0	66 0F B7 0E 10 02 66 BA-12 02 00 00 E8 16 F8 EB	f.....f°.....è.øë
000100cd0	33 90 66 33 D2 66 8B C1-66 8B CB 66 50 66 53 E8	3.f30f.Äf.ËfPfsè
000100ce0	23 00 66 5B 66 5F 66 0B-C0 0F 84 17 00 1E 07 E8	#.f[f.f.Ä.....è
000100cf0	35 FD 66 8B C7 66 0F B7-0E 10 02 66 BA 12 02 00	5ýf.Çf.....f°...
000100d00	00 E8 E1 F7 C3 66 52 66-51 66 BB 20 00 00 00 66	.èä+ÄfRfQf»...f
000100d10	B9 00 00 00 00 66 BA 00-00 00 00 E8 C7 F7 66 0Bf°.....èÇ+f.
000100d20	C0 0F 84 63 00 66 8B D8-1E 07 66 8B 3E 1A 02 66	Ä..c.f.Ø..f.>..f
000100d30	33 C0 E8 59 F8 1E 07 66-8B 1E 1A 02 66 59 66 5A	3ÀèYø..f...fYfZ
000100d40	26 66 39 0F 0F 85 0C 00-26 66 39 57 08 0F 84 31	æf9.....æf9W...l
000100d50	00 EB 13 90 26 66 83 3F-FF 0F 84 2F 00 26 83 7F	.è...æf.¿ÿ../.æ..
000100d60	04 00 0F 84 26 00 26 66-0F B7 47 04 03 D8 8B C3æ.f..G..Ø.Ä
000100d70	25 00 80 74 CB 8C C0 05-00 08 8E C0 81 E3 FF 7Fæf.....æf.....
000100d80	EB BE 26 66 8B 47 10 C3-66 59 66 5A 66 33 C0 C3æf.....æf.....
000100d90	66 50 66 51 66 8B C7 66-C1 E8 04 06 59 03 C8 51æf.....æf.....
000100da0	07 66 83 E7 0F 66 59 66-58 C3 60 06 BE BD 0D BFæf.....æf.....
000100db0	00 20 1E 07 B9 0D 00 90-F3 A5 07 61 C3 01 23 45æf.....æf.....
000100dc0	67 89 AB CD EF FE DC BA-98 76 54 32 10 F0 E1 D2	g.«îipÜ°·vI2·ðáÖ
000100dd0	C3 00 00 00 00 20 20 60-8B 36 18 20 26 8A 05 88	Ä.....`·6.æ...
000100de0	04 47 46 66 FF 06 14 20-81 FE 60 20 75 06 E8 5B	·Gffÿ...·b`u·è[

Cursor pos = 1052080; phy sec = 2054

NTFS

Ctrl+S : 입력한 섹터로 이동

(2) STEP2) 첫 번째 파티션 복구 ③ 파티션 총 섹터 수

Name	Size	Type	Date Modif...
0064ffdf0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
0064ffe00	EB 52 90 4E 54 46 53 20-20 20 20 00 02 08 00 00	NTFS	
0064ffe10	00 00 00 00 00 00 F8 00 00-3F 00 FF 00 00 08 00 00		
0064ffe20	00 00 00 00 80 00 80 00-FF 1F 03 00 00 00 00 00		
0064ffe30	55 21 00 00 00 00 00 00-02 00 00 00 00 00 00 00		
0064ffe40	F6 00 00 00 01 00 00 00-AD 8B 44 46 B9 44 46 66		
0064ffe50	00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB 68 C0 07		
0064ffe60	1F 1E 68 66 00 CB 88 16-0E 00 66 81 3E 03 00 4E		
0064ffe70	54 46 53 75 15 B4 41 BB-AA 55 CD 13 72 0C 81 FB		
0064ffe80	55 AA 75 06 F7 C1 01 00-75 03 E9 DD 00 1E 83 EC		
0064ffe90	18 68 1A 00 B4 48 8A 16-0E 00 8B F4 16 1F CD 13		
0064ffea0	9F 83 C4 18 9E 58 1F 72-E1 3B 06 0B 00 75 DB A3		
0064ffeb0	0F 00 C1 2E 0F 00 04 1E-5A 33 DB B9 00 20 2B C8		
0064ffec0	66 FF 06 11 00 03 16 0F-00 8E C2 FF 06 16 00 E8		
0064ffed0	4B 00 2B C8 77 EF B8 00-BB CD 1A 66 23 C0 75 2D		
0064ffee0	66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16		
0064ffef0	68 07 BB 16 68 70 0E 16-68 09 00 66 53 66 53 66		
0064fff00	55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF		
0064fff10	28 10 B9 D8 0F FC F3 AA-E9 5F 01 90 90 66 60 1E		
0064fff20	06 66 A1 11 00 66 03 06-1C 00 1E 66 68 00 00 00		
0064fff30	00 66 50 06 53 68 01 00-68 10 00 B4 42 8A 16 0E		
0064fff40	00 16 1F 8B F4 CD 13 66-59 5B 5A 66 59 66 59 1F		
0064fff50	0F 82 16 00 66 FF 06 11-00 03 16 0F 00 8E C2 FF		
0064fff60	0E 16 00 75 BC 07 1F 66-61 C3 A0 F8 01 E8 09 00		
0064fff70	A0 FB 01 E8 03 00 F4 EB-FD B4 01 8B F0 AC 3C 00		
0064fff80	74 09 B4 0E BB 07 00 CD-10 EB F2 C3 0D 0A 41 20		
0064fff90	64 69 73 6B 20 72 65 61-64 20 65 72 72 6F 72 20		
0064fffa0	6F 63 63 75 72 72 65 64-00 0D 0A 42 4F 4F 54 4D		
0064fffb0	47 52 20 69 73 20 6D 69-73 73 69 6E 67 00 0D 0A		
0064fffc0	42 4F 4F 54 4D 47 52 20-69 73 20 63 6F 6D 70 72		
0064fffd0	65 73 73 65 64 00 0D 0A-50 72 65 73 73 20 43 74		
0064fffe0	72 6C 2B 41 6C 74 2B 44-65 6C 20 74 6F 20 72 65		
0064ffff0	73 74 61 72 74 0D 0A 00-8C A9 BE D6 00 00 55 AA		
006500000	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E		

Sel start = 105905667, len = 4; phy sec = 206847

총 섹터 개수 : (두 번째 파티션 시작주소) - (첫 번째 파티션 시작주소)



$$(0x6500000 - 0x100000) / 0x200 = 0x32000$$

섹터 단위 : 512 byte (=0x200)

(2) STEP3) 두 번째 파티션 복구 ① 파티션 시작주소 확인

0064ffff0	73 74 61 72 74 0D 0A 00-8C A9 BE D6 00 00 55 AA	start...@%0..U*
006500000	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500010	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500020	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500030	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500040	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500050	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500060	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500070	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500080	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500090	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
0065000a0	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
0065000b0	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
0065000c0	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
0065000d0	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
0065000e0	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
0065000f0	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500100	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500110	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500120	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500130	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500140	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500150	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500160	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500170	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500180	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
006500190	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
0065001a0	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.
0065001b0	48 41 53 54 41 54 49 2E-48 41 53 54 41 54 49 2E	HASTATI.HASTATI.

Cursor pos = 105906271; phy sec = 206848

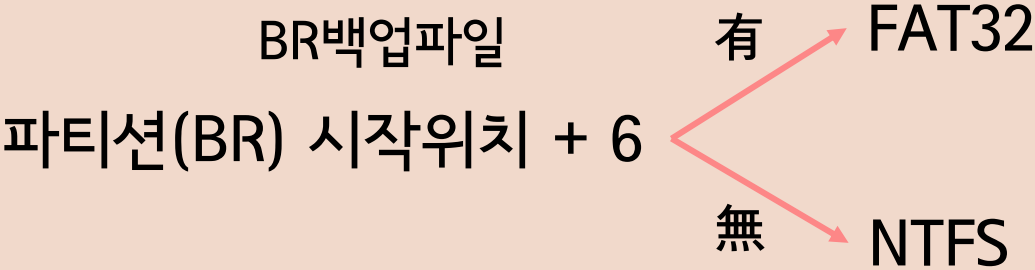
Ctrl+F : HASTATI. 검색
- 세 번째로 나오는 영역이
두 번째 손상된 BR 영역

두 번째 파티션 시작주소 : 0x6500000



$0x6500000 / 0x200 = 0x32800$

(2) STEP3) 두 번째 파티션 복구 ② 파티션 타입 확인



$$206848(\text{첫번째 파티션 시작 위치}) + 6 = 206854$$

006500bb0	5A 66 5B C3 66 0B C9 0F 85 01 00 C3 66 51 66 56	Zf[Äf·É···ÄfQfV
006500bc0	67 83 3E 61 0F 8C 0C 00 67 83 3E 7A 0F 8F 04 00	g·>a···g·>z···
006500bd0	67 83 2E 20 66 83 C6 02 E2 E6 66 5E 66 59 C3 66	g·. f·E·äaf^fYÄf
006500be0	50 66 51 66 8B D0 66 A1 32 02 67 66 8D 58 10 67	PfQf·Df;2·gf·X·g
006500bf0	03 43 04 67 66 8D 40 10 66 8B DA E8 44 F9 66 0B	·C·gf·@·f·UèDüf·
006500c00	C0 0F 84 05 00 66 59 66 59 C3 66 A1 36 02 66 0B	Ä···fyfYÄf;6·f·
006500c10	C0 0F 85 08 00 66 59 66 59 66 33 C0 C3 66 8B 16	Ä···fyfYf3ÄÄf·
006500c20	36 02 67 66 8D 52 10 67 66 8B 42 18 66 33 D2 66	6·gf·R·gf·B·f3Öf
006500c30	F7 36 6E 02 66 33 F6 66 50 66 56 66 58 66 5E 66	+6n·f3ÖfPfVfXf^f
006500c40	3B C6 0F 84 3A 00 66 56 66 40 66 50 66 48 E8 1B	;E····fvf@fPfHè·
006500c50	FE 72 E8 E8 EB FD 66 5A 66 5E 66 59 66 5B 66 53	prèèèyfZf^fyf[fS
006500c60	66 51 66 56 66 52 66 A1 46 02 67 66 8D 40 18 E8	fQfVfRf;F·gf·@·è
006500c70	D0 F8 66 0B C0 74 C4 66 59 66 59 66 59 66 59 C3	Døf·ÄtÄfyfYfyfYÄ
006500c80	66 59 66 59 66 33 C0 C3 66 51 66 50 66 B8 05 00	fyfYf3ÄÄfQfPf,·
006500c90	00 00 1E 07 66 8B F9 E8 8D FD 66 8B C1 66 BB 20	···
006500ca0	00 00 00 66 B9 00 00 00 00 66 BA 00 00 00 00 E8	···
006500cb0	33 F8 66 5B 66 59 66 85 C0 0F 85 15 00 66 8B C1	3øf
006500cc0	66 0F B7 0E 10 02 66 BA 12 02 00 00 E8 16 F8 EB	f·
006500cd0	33 90 66 33 D2 66 8B C1 66 8B CB 66 50 66 53 E8	3·f3
006500ce0	23 00 66 5B 66 5F 66 0B C0 0F 84 17 00 1E 07 E8	#·f[f_f·Ä·····è
006500cf0	35 FD 66 8B C7 66 0F B7 0E 10 02 66 BA 12 02 00	5yf·Çf·····f°···
006500d00	00 E8 E1 F7 C3 66 52 66 51 66 BB 20 00 00 00 66	·èä+ÄfRfQf»···f
006500d10	B9 00 00 00 00 66 BA 00 00 00 00 E8 C7 F7 66 0B	····f°·····èÇ+f·
006500d20	C0 0F 84 63 00 66 8B D8 1E 07 66 8B 3E 1A 02 66	Ä··c·f·@·f·>·f
006500d30	33 C0 E8 59 F8 1E 07 66 8B 1E 1A 02 66 59 66 5A	3ÄèYø··f···fyfZ
006500d40	26 66 39 0F 0F 85 0C 00 26 66 39 57 08 0F 84 31	æf9·····æf9W···l
006500d50	00 EB 13 90 26 66 83 3F FF 0F 84 2F 00 26 83 7F	·è···æf·?y·/·æ·
006500d60	04 00 0F 84 26 00 26 66 0F B7 47 04 03 D8 8B C3	···æ·æf·G·@·Ä
006500d70	25 00 80 74 CB 8C C0 05 00 08 8E C0 81 E3 FF 7F	%··tE·Ä···Ä·äy·

NTFS

Ctrl+S : 입력한 섹터로 이동

Cursor pos = 105909248 phy sec = 206854

(2) STEP3) 두 번째 파티션 복구 ③ 파티션 총 섹터 수

File List									
Name	Size	Type	Date Modif...						
9ffffe00	EB 52 90 4E 54 46 53	20-20	20 20 00 02 08 00 00	ER NTFS					
9ffffe10	00 00 00 00 00 00 F8 00	00-3F	00 FF 00 00 28 03 00ø-?·ÿ·(-					
9ffffe20	00 00 00 00 80 00 80 00	00-FF	CF FC 04 00 00 00 00yü					
9ffffe30	00 00 0C 00 00 00 00 00	00-02	00 00 00 00 00 00 00					
9ffffe40	F6 00 00 00 01 00 00 00	00-D8	29 5E FC 61 5E FC E8	ö.....ø)üaüè					
9ffffe50	00 00 00 00 FA 33 C0 8E	D0 BC	00 7C FB 68 C0 07úÅ·D·üHÄ·					
9ffffe60	1F 1E 68 66 00 CB 88 16	0E 00	66 81 3E 03 00 4E	...hf·È.....f>·N					
9ffffe70	54 46 53 75 15 B4 41 BB	AD 55	CD 13 72 0C 81 FB	TESu·Å·üü·r·ö					
9ffffe80									
9ffffe90									
9ffffea0									
9ffffeb0									
9ffffec0									
9ffffed0	4B 00 2B C8 77 EF B8 00	BB CD 1A 66 23 C0 75 2D	K·ëwí·»í·f#Au-						
9ffffee0	66 81 FB 54 43 50 41 75	24 81 F9 02 01 72 1E 16	f·üTCPAuö·ü·r·						
9ffffef0	68 07 BB 16 68 70 0E 16	68 09 00 66 53 66 53 66	h·»·hp·h·fSsf						
9fffff00	55 16 16 16 68 B8 01 66	61 0E 07 CD 1A 33 C0 BF	U··h·fa·í·3Å						
9fffff10	28 10 B9 D8 0F FC F3 AA	E9 5F 01 90 90 66 60 1E	(·ø·üö·ë.....f·						
9fffff20	06 66 A1 11 00 66 03 06	1C 00 1E 66 68 00 00 00	·fj··ö·ö·fh·						
9fffff30	00 66 50 06 53 68 01 00	68 10 00 B4 42 8A 16 0E	·fP·Sh·h··B·						
9fffff40	00 16 1F 8B F4 CD 13 66	59 5B 5A 66 59 66 59 1F	...öí·fy[ZfYfy						
9fffff50	0F 82 16 00 66 FF 06 11	00 03 16 0F 00 8E C2 FF	...fý·ö·ö·Äy						
9fffff60	0E 16 00 75 BC 07 1F 66	61 C3 A0 F8 01 E8 09 00	...u··faÅ·ø·è·						
9fffff70	A0 FB 01 E8 03 00 F4 EB	FD B4 01 8B F0 AC 3C 00	ü·è·öëý··ö·ö·						
9fffff80	74 09 B4 0E BB 07 00 CD	10 EB F2 C3 0D 0A 41 20	t··»·í·ëöÅ·A						
9fffff90	64 69 73 6B 20 72 65 61	64 20 65 72 72 6F 72 20	disk read error						
9fffffa0	6F 63 63 75 72 72 65 64	00 0D 0A 42 4F 4F 54 4D	occurred...BOOTM						
9fffffb0	47 52 20 69 73 20 6D 69	73 73 69 6E 67 00 0D 0A	GR is missing...						
9fffffc0	42 4F 4F 54 4D 47 52 20	69 73 20 63 6F 6D 70 72	BOOTMGR is compr						
9fffffd0	65 73 73 65 64 00 0D 0A	50 72 65 73 73 20 43 74	essed...Press Ct						
9fffffe0	72 6C 2B 41 6C 74 2B 44	65 6C 20 74 6F 20 72 65	rl+Alt+Del to re						
9fffff00	73 74 61 72 74 0D 0A 00	8C A9 BE D6 00 00 55 AA	start...%ö·U·ü·						
9fff00000	00 00 00 00 00 00 00 00								
9fff00010	00 00 00 00 00 00 00 00								

Ctrl+F : NTFS BR 시그니처 검

Sel start = 42948623872, len = 7; phy sec = 83884031

BR 백업 정보

두 번째 파티션 = 마지막 파티션
→ 첫 번째 파티션처럼 총 섹터 수를 구할 수 없음



Ctrl+F : NTFS BR 시그니처 검색 (Hex)

BR의 시그니처 기반으로 백업본 위치 찾기

NTFS의 BR 시그니처 : [EB 52 90 4E 54 46 53]

총 섹터 개수 : (해당 섹터 끝나는 주소) - (두 번째 파티션 시작주소)



$(0x9fff00000 - 0x65000000) / 0x200 = 0x04fcd000$

(2) STEP4) 복구 ① MBR영역 복구

내용	오프셋
부팅정보	80
CHS 시작주소	00 00 00
파티션 타입	07
CHS 마지막 주소	00 00 00
BR 시작 주소	00 80 00 00
총 섹터 개수	00 20 03 00

첫 번째 파티션 테이블정보

내용	오프셋
부팅정보	80
CHS 시작주소	00 00 00
파티션 타입	07
CHS 마지막 주소	00 00 00
BR 시작 주소	00 28 03 00
총 섹터 개수	00 D0 FC 04

두 번째 파티션 테이블정보

(2) STEP4) 복구 ① MBR영역 복구

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000060	26	66	68	00	00	00	00	66	FF	76	08	68	00	00	68	00	&fh....fÿv.h..h.
00000070	7C	68	01	00	68	10	00	B4	42	8A	56	00	8B	F4	CD	13	h..h..'BŠV.<ôí.
00000080	9F	83	C4	10	9E	EB	14	B8	01	02	BB	00	7C	8A	56	00	ŸfĂ.zë...». ŠV.
00000090	8A	76	01	8A	4E	02	8A	6E	03	CD	13	66	61	73	1C	FE	Šv.ŠN.Šn.í.fas.p
000000A0	4E	11	75	0C	80	7E	00	80	0F	84	8A	00	B2	80	EB	84	N.u.ë~.ë..„Š.„ëë„
000000B0	55	32	E4	8A	56	00	CD	13	5D	EB	9E	81	3E	FE	7D	55	U2ăŠV.í.)ěž.>p}U
000000C0	AA	75	6E	FF	76	00	E8	8D	00	75	17	FA	B0	D1	E6	64	*unÿv.è..u.ú°Ñæd
000000D0	E8	83	00	B0	DF	E6	60	E8	7C	00	B0	FF	E6	64	E8	75	èf.°Bæ`è .°ÿædèu
000000E0	00	FB	B8	00	BB	CD	1A	66	23	C0	75	3B	66	81	FB	54	.û,.»í.f#Àu;f.ûT
000000F0	43	50	41	75	32	81	F9	02	01	72	2C	66	68	07	BB	00	CPAu2.û..r,fh.».
00000100	00	66	68	00	02	00	00	66	68	08	00	00	00	66	53	66	.fh....fh....fSf
00000110	53	66	55	66	68	00	00	00	00	66	68	00	7C	00	00	66	SfUfh....fh. ..f
00000120	61	68	00	00	07	CD	1A	5A	32	F6	EA	00	7C	00	00	CD	ah...í.Z2ôë. ..í
00000130	18	A0	B7	07	EB	08	A0	B6	07	EB	03	A0	B5	07	32	E4	. .ë. ħ.ë. u.2ă
00000140	05	00	07	8B	F0	AC	3C	00	74	09	BB	07	00	B4	0E	CD	...<ð~<.t.»..'í
00000150	10	EB	F2	F4	EB	FD	2B	C9	E4	64	EB	00	24	02	E0	F8	.ëòôëÿ+Ëädë.\$.àø
00000160	24	02	C3	49	6E	76	61	6C	69	64	20	70	61	72	74	69	\$.ĂInvalid parti
00000170	74	69	6F	6E	20	74	61	62	6C	65	00	45	72	72	6F	72	tion table.Error
00000180	20	6C	6F	61	64	69	6E	67	20	6F	70	65	72	61	74	69	loading operati
00000190	6E	67	20	73	79	73	74	65	6D	00	4D	69	73	73	69	6E	ng system.Missin
000001A0	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	g operating syst
000001B0	65	6D	00	00	00	63	7B	9A	78	6D	EF	00	00	00	80	00	em...c{šxmí...ë.
000001C0	00	00	07	00	00	00	00	08	00	00	00	20	03	00	80	00ë.
000001D0	00	00	07	00	00	00	00	28	03	00	00	D0	FC	04	00	00 (...Đü...
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001F0	B0	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AAUª

Offset(h): 1F0

* Modi

MBR_446 파일의 10,368 섹터의 파티션 테이블 수정

(2) STEP4) 복구 ① MBR영역 복구

Offset(h): 10368

Windows 7.vmdk MBR_recovery Windows 7.vmdk

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00050FFD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00050FFE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00050FFFO	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000510000	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510010	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510020	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510030	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510040	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510050	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510060	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510070	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510080	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510090	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0005100A0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0005100B0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0005100C0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0005100D0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0005100E0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0005100F0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510100	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510110	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510120	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510130	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510140	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510150	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510160	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000510170	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.

Find

Text-string Hex-values Integer number Floating point

Search for: HASTATI

Options

Text encoding: (Editor encoding)

☐ Case sensitive

Search

☐ All

☒ Forward

☐ Back

OK Search all

Offset(h): 0

복사(Ctrl+C) → 붙여넣기(Ctrl+B)

첫 번째 검색하여 나온 10,368섹터 : MBR 영역

(2) STEP4) 복구 ② 첫 번째 파티션 영역 복구

복사(Ctrl+C) → 붙여넣기(Ctrl+B)

0064ffde0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0064ffdf0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0064ffe00	EB 52 90 4E 54 46 53 20-20 20 20 00 02 08 00 00 00	ER-NIFS
0064ffe10	00 00 00 00 00 00 F8 00 00-3F 00 FF 00 00 08 00 00-?·ÿ.....
0064ffe20	00 00 00 00 00 80 00 80 00-FF 1F 03 00 00 00 00 00ÿ.....
0064ffe30	55 21 00 00 00 00 00 00 00-02 00 00 00 00 00 00 00	U!.....-DF·D.....
0064ffe40	F6 00 00 00 01 00 00 00-AD 8B 44 46 B9 44 46 66	ö.....ú3À·D·lùh.....
0064ffe50	00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB 68 C0 07hf·E.....f>·N.....
0064ffe60	1F 1E 68 66 00 CB 88 16-0E 00 66 81 3E 03 00 4E	TFSu·A·UÍ·r·û.....
0064ffe70	54 46 53 75 15 B4 41 BB-AA 55 CD 13 72 0C 81 FB	U·u·A·u·éY·i.....
0064ffe80	55 AA 75 06 F7 C1 01 00-75 03 E9 DD 00 1E 83 EC	·h·H.....ô·í·.....
0064ffe90	18 68 1A 00 B4 48 8A 16-0E 00 8B F4 16 1F CD 13	·A·X·rá;·uÛz.....
0064ffea0	9F 83 C4 18 9E 58 1F 72-E1 3B 06 0B 00 75 DB A3	·A·...Z3Û·+E.....
0064ffeb0	0F 00 C1 2E 0F 00 04 1E-5A 33 DB B9 00 20 2B C8	fÿ.....Äy·è.....
0064ffec0	66 FF 06 11 00 03 16 0F-00 8E C2 FF 06 16 00 E8	K·+Ewí;·»í·f#Au-.....
0064ffed0	4B 00 2B C8 77 EF B8 00-BB CD 1A 66 23 C0 75 2D	f·ûTCPAu\$·ù·r·.....
0064ffee0	66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16	h·»·hp·h·fSfSf.....
0064ffef0	68 07 BB 16 68 70 0E 16-68 09 00 66 53 66 53 66	U·h;·fa·í·3Äz.....
0064fff00	55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF	(··ø·üó·é_·f·.....
0064fff10	28 10 B9 D8 0F FC F3 AA-E9 5F 01 90 90 66 60 1E	·f;·f·...fh·...·
0064fff20	06 66 A1 11 00 66 03 06-1C 00 1E 66 68 00 00 00	·fP·Sh·h·B·...·
0064fff30	00 66 50 06 53 68 01 00-68 10 00 B4 42 8A 16 0E	·...ôí·fY[ZfYfY·...
0064fff40	00 16 1F 8B F4 CD 13 66-59 5B 5A 66 59 66 59 1F	·...fÿ·...·Äy.....
0064fff50	0F 82 16 00 66 FF 06 11-00 03 16 0F 00 8E C2 FF	·u·faÄ ø·è·...·
0064fff60	0E 16 00 75 BC 07 1F 66-61 C3 A0 F8 01 E8 09 00	û·è·øëý··ø-<·...
0064fff70	A0 FB 01 E8 03 00 F4 EB-FD B4 01 8B F0 AC 3C 00	t··»·í·eöÄ·A.....
0064fff80	74 09 B4 0E BB 07 00 CD-10 EB F2 C3 0D 0A 41 20	disk read error.....
0064fff90	64 69 73 6B 20 72 65 61-64 20 65 72 72 6F 72 20	occurred··BOOTM.....
0064fffa0	6F 63 63 75 72 72 65 64-00 0D 0A 42 4F 4F 54 4D	

Cursor pos = 105905664 phy sec = 206847

The screenshot shows a hex editor window with a search for 'HASTATI' in a file named 'Windows 7.vmdk'. The search results show the string 'HASTATI.HASTATI.' repeated multiple times. A 'Find' dialog box is open, showing the search criteria and options.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000520000	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520010	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520020	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520030	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520040	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520050	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520060	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520070	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520080	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520090	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0005200A0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0005200B0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0005200C0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0005200D0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0005200E0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0005200F0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520100	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520110	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520120	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520130	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520140	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520150	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520160	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520170	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520180	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
000520190	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0005201A0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.

두 번째 검색하여 나온 10,496섹터 : 첫 번째 파티션 영역

첫 번째 BR 백업본 : 206,847 (206,848섹터 바로 전 섹터)

(2) STEP4) 복구 ③ 두 번째 파티션 영역 복구

복사(Ctrl+C) → 붙여넣기(Ctrl+B)

9ffffde0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
9ffffdf0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
9ffffe00	EB 52 90 4E 54 46 53 20-20 20 20 00 02 08 00 00	ER.NTFS
9ffffe10	00 00 00 00 00 00 F8 00-00 3F 00 FF 00 00 28 03 00-?·ÿ·(·
9ffffe20	00 00 00 00 00 80 00 80 00-FF CF FC 04 00 00 00 00ÿü·
9ffffe30	00 00 0C 00 00 00 00 00-02 00 00 00 00 00 00 00
9ffffe40	F6 00 00 00 01 00 00 00-08 29 5E FC 61 5E FC E8	ö·.....·)·^üa·üè
9ffffe50	00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB 68 C0 07	·...ú3Ä·D·%· üñ
9ffffe60	1F 1E 68 66 00 CB 88 16-0E 00 66 81 3E 03 00 4E	··hf·Ë·...f·>·
9ffffe70	54 46 53 75 15 B4 41 BB-AA 55 CD 13 72 0C 81 FB	TFSu·A·»·Uí·r·ü
9ffffe80	55 AA 75 06 F7 C1 01 00-75 03 E9 DD 00 1E 83 EC	U·u·+Ä·u·éÿ··i
9ffffe90	18 68 1A 00 B4 48 8A 16-0E 00 8B F4 16 1F CD 13	·h·»·H·...ö·í·
9ffffea0	9F 83 C4 18 9E 58 1F 72-E1 3B 06 0B 00 75 DB A3	··Ä·X·rá;··uÛé
9ffffeb0	0F 00 C1 2E 0F 00 04 1E-5A 33 DB B9 00 20 2B C8	··Ä·...·23Ü··+È
9ffffec0	66 FF 06 11 00 03 16 0F-00 8E C2 FF 06 16 00 E8	fÿ·...··Äÿ·...è
9ffffed0	4B 00 2B C8 77 EF B8 00-BB CD 1A 66 23 C0 75 2D	K·+Ëwí··»í·f#Au·
9ffffee0	66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16	f·üTCPAu\$·ù·r·
9ffffef0	68 07 BB 16 68 70 0E 16-68 09 00 66 53 66 53 66	h·»·hp·h·fSfSf
9fffff00	55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF	U·...h··fa·í·3Ä¿
9fffff10	28 10 B9 D8 0F FC F3 AA-E9 5F 01 90 90 66 60 1E	(·¹Ø·üó·é·...f·
9fffff20	06 66 A1 11 00 66 03 06-1C 00 1E 66 68 00 00 00	·f;··f·...·fh·
9fffff30	00 66 50 06 53 68 01 00-68 10 00 B4 42 8A 16 0E	·fP·Sh·h·...·B·
9fffff40	00 16 1F 8B F4 CD 13 66-59 5B 5A 66 59 66 59 1F	·...öí·fY[ZfYfY·
9fffff50	0F 82 16 00 66 66 FF 06 11-00 03 16 0F 00 8E C2 FF	·...fÿ·...··Äÿ
9fffff60	0E 16 00 75 BC 07 1F 66-61 C3 A0 F8 01 E8 09 00	··u·...faÄ·ø·è·
9fffff70	A0 FB 01 E8 03 00 F4 EB-FD B4 01 8B F0 AC 3C 00	û·è··öéÿ·...ö·<·
9fffff80	74 09 B4 0E BB 07 00 CD-10 EB F2 C3 0D 0A 41 20	t·'·»··í·èöÄ··A
9fffff90	64 69 73 6B 20 72 65 61-64 20 65 72 72 6F 72 20	disk read error
9fffffa0	6F 63 63 75 72 72 65 64-00 0D 0A 42 4F 4F 54 4D	occurred···BOOTM

Cursor pos = 42948623872; phy sec = 83884031

Windows 7.vmdk MBR_recovery Windows 7.vmdk Partition1

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0007A0000	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0001	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0002	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0003	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0004	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0005	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0006	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0007	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0008	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0009	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A000A	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A000B	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A000C	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A000D	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A000E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A000F	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0010	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0011	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0012	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0013	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0014	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0015	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
0007A0016	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.

Find

Text-string Hex-values Integer number Floating point number

Search for: HASTATI

Options

Text encoding: (Editor encoding)

☐ Case sensitive

Search direction

☐ All

☒ Forward

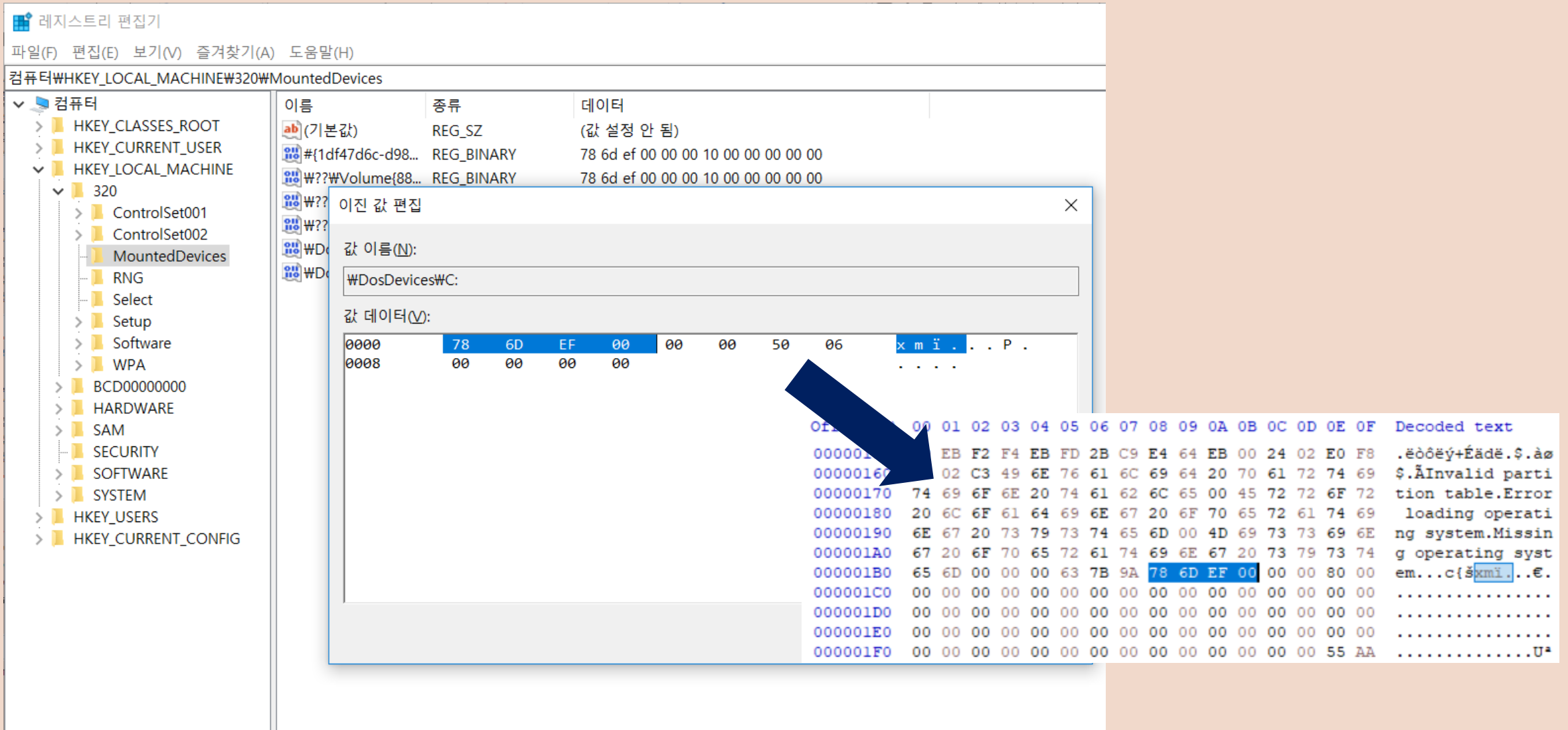
☐ Backward

OK Search all Cancel

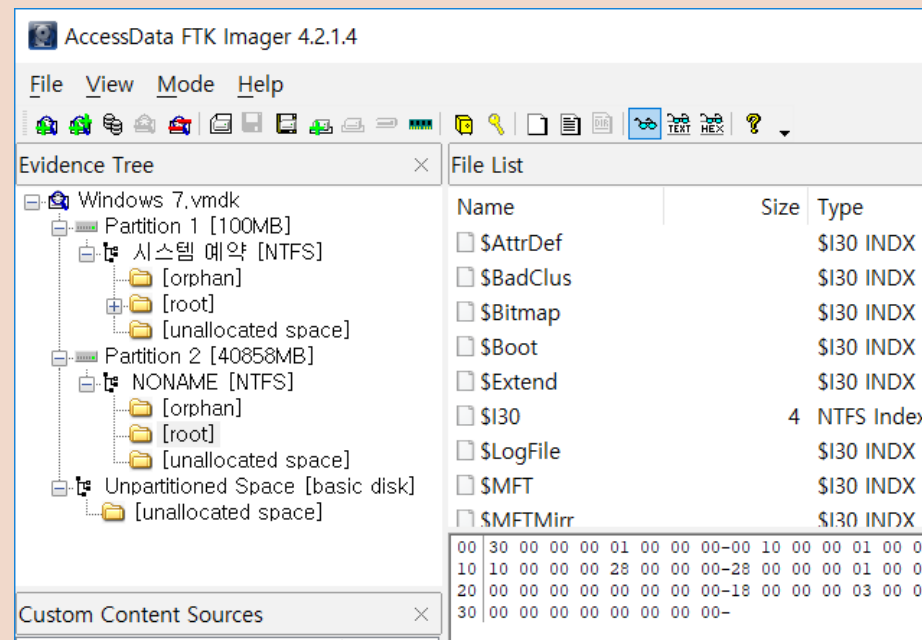
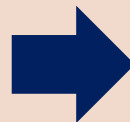
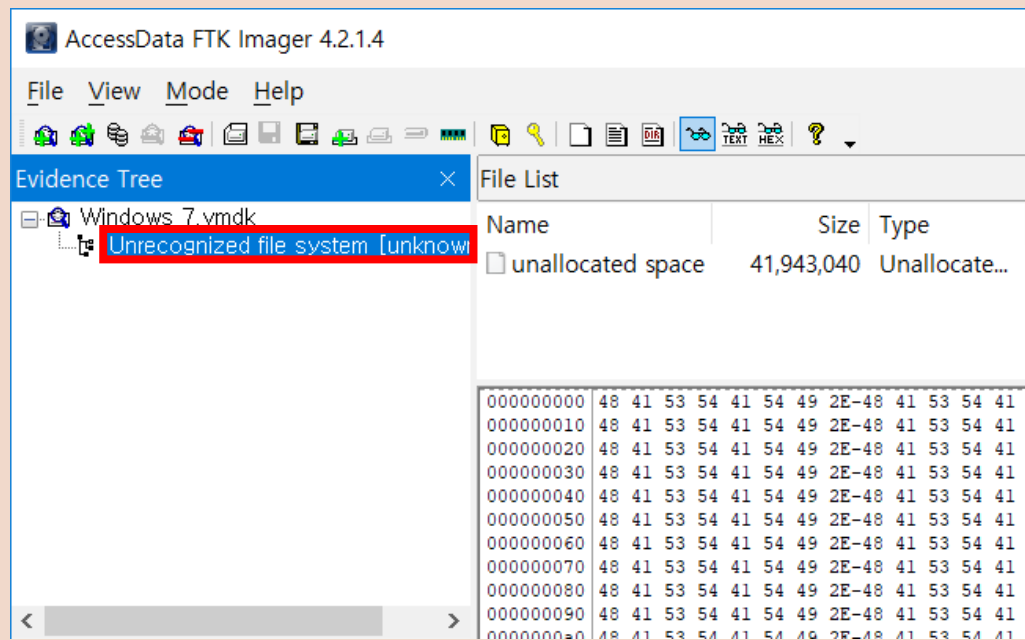
세 번째 검색하여 나온 15,616섹터 : 두 번째 파티션 영역

두 번째 BR 백업본 : 83884031 (0x9fff0000 포함한 섹터)

(2) STEP4) 복구 ④ GUID (Globally Unique Identifier, 고유의 하드디스크 값)



(2) 실습 결과



파티션 정보가 손상되었음 & 부팅되지 않음

파티션 정보가 복구되었음 & 부팅됨

감사합니다

