

# 디지털 포렌식 현황과 전망



*JK Kim*

*@pr0neer*

*forensic-proof.com*

*proneer@gmail.com*

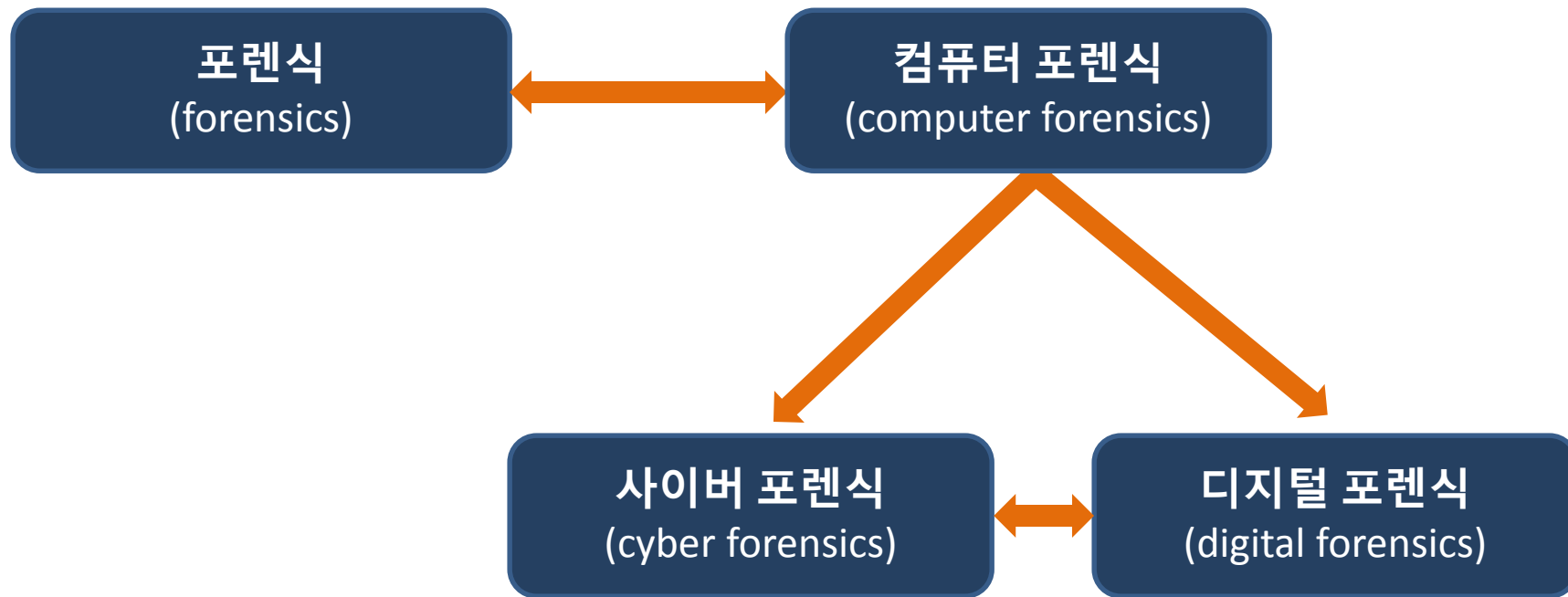
1. 디지털 포렌식 정의
2. 디지털 포렌식 산업 현황
3. 디지털 포렌식 기술 전망
4. 포렌식 관점에서 바라 본 3.20 사이버테러

# 디지털 포렌식 정의

*Security is a people problem...*

# 디지털 포렌식 정의

## 다양한 포렌식 용어



# 디지털 포렌식 정의

## 다양한 디지털 포렌식 정의 (Cont'd)

- **Wikipedia**

Digital forensics (sometimes known as digital forensic science) is **a branch of forensic science encompassing the recovery and investigation** of material found in digital devices, often in relation to computer crime. The term digital forensics was originally **used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.**

- **Techopedia**

Digital forensics is **the process of uncovering and interpreting electronic data for use in a court of law.** The goal of the process is **to preserve any evidence in its most original form** while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.

# 디지털 포렌식 정의

## 다양한 디지털 포렌식 정의

- 일반적 정의

디지털기기를 매개체로 하여 발생한 특정 행위의 사실 관계를 **법정에서** 규명하고 증명하기 위한 절차와 방법

- 재정의

디지털기기를 매개체로 하여 발생한 특정 행위의 사실 관계를 규명하고 증명하기 위한 절차와 방법

# 디지털 포렌식 산업 현황

*Security is a people problem...*

# 디지털 포렌식 산업 현황

## 다양한 디지털 포렌식 산업





## 수사기관 (Cont'd)

### ■ 검찰

- 대검찰청 디지털 포렌식 센터(DFC, Digital Forensic Center) , 약 100여명
  - ✓ 사이버범죄수사단
  - ✓ 디지털수사담당관실 – 디스크 분석팀, DB 분석팀, 모바일 분석팀, 통화/계좌 분석팀, 사이버팀, 교육연구팀
  - ✓ 과학수사담당관실
  - ✓ DNA 담당관실
- 대전/대구/부산/광주고등검찰청, 서울 중앙/인천/수원지방검찰청, 각 3~4명
  - ✓ 디지털포렌식 수사팀

## 수사기관 (Cont'd)

### ▪ 경찰

- 경찰청 사이버테러대응센터(CTRC, Cyber Terror Response Center), 약 65명
  - ✓ 협력운영팀, 수사팀, 기획수사팀, 기술지원팀
- 지방경찰청, 약 1,000 여명 (경찰서 포함)
  - ✓ 사이버수사대
- 경찰서
  - ✓ 사이버수사팀
- 해양경찰청
  - ✓ 과학수사팀

## 수사기관 (Cont'd)

### ▪ 국방부

#### • 국방부조사본부

- ✓ 수사단 내 사이버범죄수사대

#### • 기무사령부

- ✓ 군사보안, 군 방첩, 군관련 첩보 수집, 특정범죄 수사, 매년 국방해킹방어대회 개최

#### • 헌병 수사기관

- ✓ 육군 중앙수사대, 해군 헌병단, 공군 헌병단

#### • 군 검찰

- ✓ 육군/해군/공군 고등검찰부 디지털 포렌식팀

#### • 국군사이버사령부

- ✓ 군사망 침해사고 예방, 조사, 대응 업무

## 수사기관

- 국가정보원
  - 국가사이버안전센터
    - ✓ 국가사이버안전 정책 총괄
    - ✓ 사이버위치 예방활동
    - ✓ 사이버공격 탐지활동
    - ✓ 사고조사 및 복구지원

## 준수사기관 (특별사법경찰관)

- 국세청
- 관세청
- 금융감독원
- 공정거래위원회
- 저작권위원회
- 방송통신위원회
- 선거관리위원회
- 한국마사회
- 식약청

## 법률, 회계 관련

### ▪ 회계관련

- 4대 회계법인 중심

- ✓ 안진 딜로이트, 삼일 PwC, 삼정 KPMG, 언스트앤영 한영

### ▪ 법률관련

- 대형로펌

- ✓ 김앤장, 율촌, 태평양, 세종, 화우

- IT 전문로펌

- ✓ 행복마루, 테크앤로, 민후, 평강

## 이디스커버리

### ■ 이디스커버리 절차 지원

- 유빅 (UBIC), 콜랩스리걸 (Kollabs Legal)
- 4대 회계법인
- 더존정보보호서비스

### ■ 이디스커버리 관련 솔루션

- 이메일 아카이빙
  - ✓ 시만텍 볼트(Vault), EMC 소스원(SourceOne), 다우기술 테라스(Terrace), ARTEC EMA 등
- 리뷰 솔루션
  - ✓ Clearwell, Guidance Software, ZyLAB, UBIC, Case Central, Nuix 등
- 정보 저장소

## 침해사고 대응

- **KISA 인터넷침해대응센터**
  - 침해사고대응단 내 해킹대응팀
- **안랩**
  - 솔루션서비스팀 내 A-FIRST 파트
- **인포섹**
  - MSS 사업본부 내 MSS 포렌식팀



## 디지털포렌식 서비스 및 솔루션

### ▪ 장비/솔루션 리셀링

- 제트코, 더존정보보호서비스, 징코스테크놀로지, 인섹시큐리티, 엔씨클시스템즈, 쿠퍼스시스템즈, 레드아이포렌식, 벨정보

### ▪ 디지털포렌식 솔루션

- 더존정보보호서비스, 지엠디시스템, 파이널데이터, 포앤식스테크, 이스턴웨어, 모바일캡스

### ▪ 디지털 증거 분석

- 더존정보보호서비스, 지엠디시스템, 레드아이포렌식, KDL컴퓨터포렌식

### ▪ 데이터 복구

- 명정보기술, 데이터닥터

# 디지털 포렌식 산업 현황

## 디지털포렌식 교육

### ▪ 대학

- 경기대학교, 호원대학교, 광주대학교, 군산대학교, 영산대학교, 한국IT전문대학

### ▪ 대학원

- 고려대학교 정보보호대학원, 동국대 국제정보대학원

### ▪ 민간교육기관

- 제트코, 더존정보보호서비스, 코어시큐리티, 한국정보보호교육센터, 아이제론, 인섹시큐리티

### ▪ 정기교육

- KITRI 지식정보보안양성과정, KISA 아카데미 디지털포렌식 시니어/주니어 과정, 고려대 정보보호 교육지역센터 침해사고대응 및 디지털포렌식 과정

## 디지털포렌식 학회/협회

### ■ 한국포렌식학회

- 대검찰청, 성균관대 주도로 처음 만듦
- 디지털포렌식 전문가 자격 운영

### ■ 한국디지털포렌식학회

- 경찰청, 고려대 주도로 처음 만듦
- 디지털포렌식 연구 발간

### ■ 사이버포렌식전문가협회

- 동국대 주도로 만듦
- CFPA 자격 운영

## 보안/감사

### ▪ 기업 보안/감사팀

- 대기업을 중심으로 보안팀, 감사팀에서 포렌식 교육 이수, 인력 채용
- 전문 포렌식 관련 팀 구성

# 디지털 포렌식 기술 전망

*Security is a people problem...*

	수집	처리	분석
저장장치	이미징 복제 쓰기방지 논리적 증거 획득	하드디스크 복구 메모리 장치 복구 삭제된 데이터 복구 데이터 카빙	메모리 분석 디스크 암호화 분석 은닉 영역 탐지
시스템	라이브 데이터 수집 메모리 수집 라이브 CD/USB 시스템 로그 수집 데이터 선별 수집	인덱싱 기술 참조데이터세트 레인보우 테이블 패스워드 사전 파일시스템 복구 이벤트 재구성	로그 분석 파일시스템 분석 시스템 아티팩트 분석 시스템 암호 해독 타임라인 분석 디지털 프로파일링 역공학
애플리케이션	데이터베이스 수집 애플리케이션 로그 수집 데이터 선별 수집	데이터 분류 데이터 정규화 데이터 마이닝 이벤트 재구성	애플리케이션 암호 해독 파일 포맷 분석 데이터베이스 분석 스테가노그래피 분석 이미지, 동영상 분석 역공학
네트워크	유선 네트워크 패킷 수집 무선 네트워크 패킷 수집 네트워크 장비 이미징 네트워크 로그 수집 원격 포렌식 수집	네트워크 로그 분류 대용량 패킷 처리 암호 통신 복호화 데이터 마이닝 데이터 정규화	시각화 네트워크 로그 분석 디지털 프로파일링

## #To Do – 표준 및 인증 방안

### ▪ 디지털포렌식 표준 마련 (NIST와 같은)

- 민.형사 소송에서 CoC를 보장할 수 있는 합리적인 절차 마련
- 디지털 증거의 무결성을 인정받을 수 있는 데이터 수집, 처리, 분석 방법

### ▪ 포렌식 장비/솔루션 인증

- 어느 기관이 맡을 것인가? 어떤 기준으로?

### ▪ 포렌식 자격 인증

- (사) 한국포렌식학회 디지털포렌식전문가자격?

### ▪ 포렌식 분석 인증

- 국과수와 같은 모델이 필요한가?

## #To Do – 연구 시장 마련

### ▪ 연구 발표 및 토론의 장 부족

- 논문/학회지?
- 컨퍼런스/세미나?

### ▪ 이분화된 학회 운용

- 한국포렌식학회
- 한국디지털포렌식학회



## #To Do – 수집 방안

### ▪ 논리적 볼륨 & 엔터프라이즈 저장소 수집 방안

- RAID(0, 1, 2, 3, 4, 5, Hybrid), LVM, JBOD, Dynamic Disk
- NAD, DAS, SAN, iSCSI

### ▪ 암호화 디스크 수집 기술

- SafeBoot Device Encryption, HP ProtectTools 2009, Bitlocker, PointSec, Truecrypt, GuardianEdge, Symantec Endpoint Encryption, SafeGuardEasy & PGP Whole Disk Encryption, Lenovo FDE

### ▪ 논리적 증거 (선별) 수집 방안

- DRM, DLP, FDE, 소극적 영상 등

### ▪ 원격 수집 방안

## #To Do – 분석 방안

- 업무별 자동화된 프레임워크 개발
  - 사용자 행위, 기밀 유출, 침해사고 등
- 대용량 데이터 검색, 인덱싱 방안
- 데이터 별 다양한 시각화 연구
- 안티안티포렌식 기법 연구
- 가상화 포렌식 연구
- 데이터 정규화, 마이닝 연구
- 엔터프라이즈 포렌식 연구
- 융합 연구 필요
  - 자연어 처리, 신호 처리, 마이닝, 시각화 등

## 3.20 사이버테러

*Security is a people problem...*

## 3.20 사이버테러

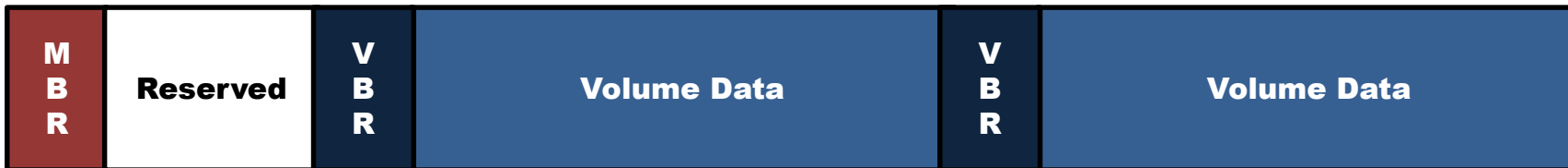
### 데이터 복구 관점에서 (Cont'd)

- **분석 대상**
  - 3.20 사이버테러에 피해 받은 총 7개 디스크
- **복구전문업체와 연간 서비스 계약**
  - 디스크당 10만원 초반
  - 보통 2~3일 소요
- **빠른 복구를 위해 의뢰**

## 3.20 사이버테러

### 데이터 복구 관점에서 (Cont'd)

- 저장매체의 일반적인 구조

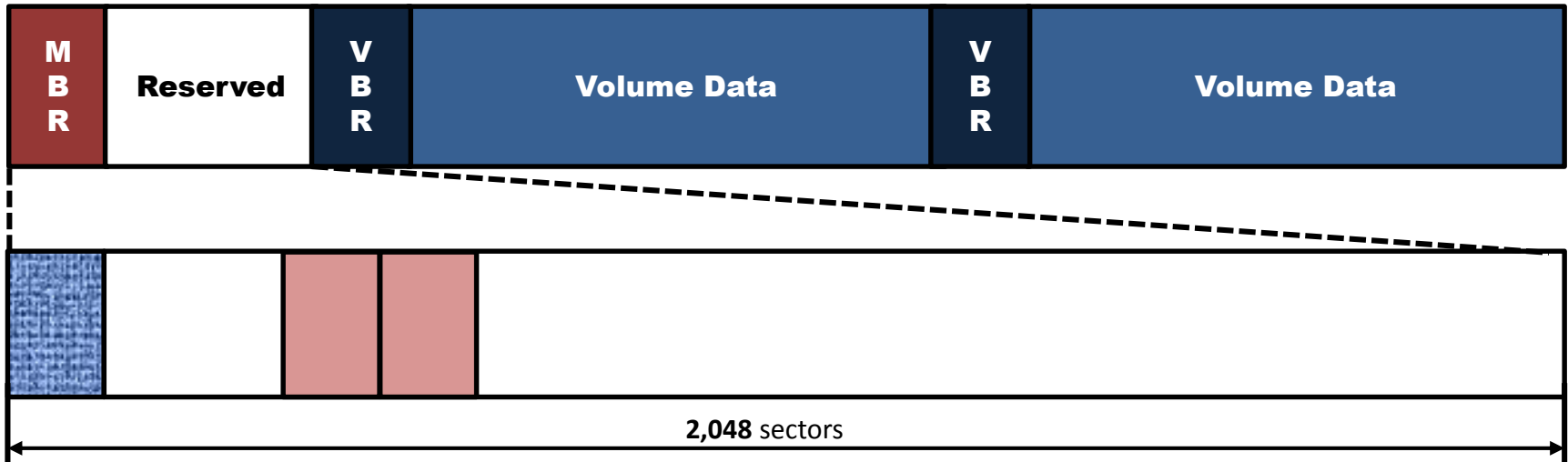


- **MBR (Master Boot Record)**
  - ✓ 저장매체 첫 512 바이트
- **Reserved/MBR Slack**
  - ✓ 윈도우 XP : 63 섹터
  - ✓ 윈도우 Vista/7 : 2,048 섹터
- **VBR (Volume Boot Record)**
  - ✓ 볼륨의 첫 클러스터
  - ✓ VBR의 첫 섹터는 부트 섹터(Boot Sector)

## 3.20 사이버테러

### 데이터 복구 관점에서 (Cont'd)

- 공통된 흔적



- MBR (Master Boot Record)

- ✓ 특정 문자로 덮어써짐

- Backup MBR

- ✓ 보안솔루션에 의해 4, 5번 섹터에 MBR 백업 (4 - 정상 MBR, 5 - 부트코드 일부 손상)

# 3.20 사이버테러

## 데이터 복구 관점에서 (Cont'd)

### ■ 공통된 흔적



### 로마시대 중무장 보병

1열 : HASTATI

2열 : PRINCIPES

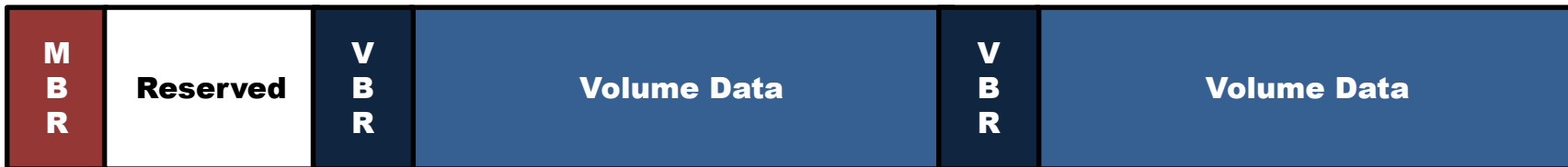
3열 : TRIARII

0000000600	33 C0 8E D8 8E C0 8E D0	BC 00 7C 8B F4 BF 00 06	3A101A1B4   10c
0000000610	B9 00 01 FC F3 A5 EA 1B	00 60 00 0E 1F 06 E8 95	' uóWé ' èI
0000000620	00 07 80 3E 97 01 01 74	75 80 3E 97 01 02 74 00	I>I tuI>I t
0000000630	C6 06 94 01 00 E8 04 01	BE BE 01 B3 04 F6 04 80	Æ I ' è ææ ' ó I
0000000640	75 0F 83 C6 10 FE CB 75	F4 CD 18 BE SD 01 E8 FC	u IÆ pEuóí æ] èü
0000000650	00 BB 00 7C 06 53 50 55	8B EC C7 46 02 00 00 5D	»   SPUIiÇF ]
0000000660	50 55 8B EC C7 46 02 00	00 5D FF 74 0A FF 74 08	PUi iÇF ]ýt ýt
0000000670	06 53 50 55 8B EC C7 46	02 01 00 5D 50 55 8B EC	SPUIiÇF ]PUi
0000000680	C7 46 02 10 00 5D 16 1F	8B F4 B4 42 CD 13 83 C4	ÇF ] Ió BÍ IÄ
0000000690	10 EB 00 CB C6 06 95 01	00 E8 A0 00 EB 00 BB 00	è ÈÆ I ' è »
00000006A0	7C 06 53 B8 01 02 B5 00	B1 05 B6 00 B2 80 CD 13	S, µ ± ¶ ² Ií
00000006B0	C6 06 94 01 01 CB B8 00	F0 8E C0 33 C0 8B F0 BB	Æ I ' È, äIÄ3ÄIä»
00000006C0	FF FF 26 81 3C 53 77 74	08 83 C6 01 4B 75 F3 EB	ÿÿ& <Swt IÆ Kuóé
00000006D0	1A 26 81 7C 02 53 6D 74	02 EB EE 26 81 7C 04 69	&   Smt èi&   i
00000006E0	40 74 02 EB E4 83 C6 06	E8 01 00 C3 1E 57 26 8B	@t éaIÆ è Ä W&I
00000006F0	14 26 8A 44 03 EE 26 8B	44 07 8E D8 26 8B 44 05	&ID i&ID I0&ID
0000000700	8B F8 C7 05 43 58 C7 45	02 5C 00 26 8A 44 02 EE	IæÇ CXÇE \ &ID i
0000000710	B1 02 8A 65 05 80 FC FF	74 13 80 FC 80 76 0E C7	± Ie Iüÿt Iülv Ç
0000000720	45 02 5D 00 80 EC 80 88	65 05 EE B1 01 26 8B 14	E ] Iille i± &I
0000000730	26 8A 44 04 EE 5F 1F 88	0E 97 01 C3 BB 00 06 B8	&ID i_ I I I Ä»
0000000740	01 03 B5 00 B1 01 B6 00	B2 80 CD 13 C3 AC 3C 00	µ ± ¶ ² Ií Ä-<
0000000750	74 0A B4 0E B7 00 B3 07	CD 10 EB F1 C3 4D 69 73	t ' ' ' í èñÄMis
0000000760	73 69 6E 67 20 6F 70 65	72 61 74 69 6E 67 20 73	sing operating s
0000000770	79 73 74 65 6D 00 00 00	00 00 00 00 00 00 00 00	ystem
0000000780	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0000000790	46 44 53 54 00 00 3E 00	00 12 00 00 BC 0A 8D 7E	FDST > 'æ ~
00000007A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000007B0	00 00 00 00 00 2C 44 63	82 A3 92 FC 00 00 00 20	
00000007C0	21 00 12 8A F1 FF 00 08	00 00 00 00 40 01 80 8A	! Iñÿ @ II
00000007D0	F2 FF 07 20 EF FF 00 08	40 01 00 00 C0 0D 00 20	öÿ iÿ @ Ä
00000007E0	F0 FF 07 2A E9 FF 00 08	00 0F 00 48 1C 0E 00 00	öÿ *éÿ H
00000007F0	00 00 00 00 00 00 00 00	00 00 00 00 00 55 AA	U&

## 3.20 사이버테러

### 데이터 복구 관점에서 (Cont'd)

- VBR 흔적



- Case #1 – 부트섹터만 덮어써짐

- ✓ VBR의 부트섹터 512 바이트만 특정 문자열로 덮어써짐

- Case #2 – 부트섹터부터 200개 섹터가 덮어써짐

- ✓ VBR의 부트섹터부터 200개 섹터가 특정 문자열로 덮어써짐

- Case #3 – 랜덤 데이터로 덮어써짐

- ✓ VBR의 부트섹터부터 상당히 많은 섹터가 랜덤데이터로 덮어써짐



## 3.20 사이버테러

### 데이터 복구 관점에서 (Cont'd)

#### ■ VBR 흔적 Case #1

- 부트섹터만 덮어써짐

- 백업 VBR이 있을 경우

손쉽게 복구

- 백업 VBR이 없을 경우

BPB 영역 복구

- 포렌식 도구를 이용하면

낮은 수준의 검증만

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	✓
0000100000	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100010	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100020	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100030	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100040	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100050	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100060	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100070	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100080	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100090	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
00001000A0	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
00001000B0	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
00001000C0	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
00001000D0	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
00001000E0	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
00001000F0	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100100	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100110	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100120	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100130	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100140	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100150	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100160	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100170	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100180	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
0000100190	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
00001001A0	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
00001001B0	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
00001001C0	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
00001001D0	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
00001001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00001001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000100200	07	00	42	00	4F	00	4F	00	54	00	4D	00	47	00	52	00	B O O T M G R
0000100210	04	00	24	00	49	00	33	00	30	00	00	D4	00	00	00	24	\$ I 3 0 Ô \$
0000100220	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000100230	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

## 3.20 사이버테러

### 데이터 복구 관점에서 (Cont'd)

#### ■ VBR 흔적 Case #2

- 부트섹터부터 200개 섹터
- 남아있는 MFT 레코드를 이용
- 파일 카빙을 이용해 복구

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
03C0100000	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	PRINCIPES PRINCI
03C0100010	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	PES PRINCIPES PR
03C0100020	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	INCIPES PRINCIPLE
03C0100030	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	S PRINCIPES PRIN
03C0100040	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	CIPES PRINCIPES
03C0100050	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	PRINCIPES PRINCI
03C0100060	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	PES PRINCIPES PR
03C0100070	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	INCIPES PRINCIPLE
03C0100080	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	S PRINCIPES PRIN
03C0100090	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	CIPES PRINCIPES
03C01000A0	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	PRINCIPES PRINCI
03C01000B0	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	PES PRINCIPES PR
03C01000C0	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	INCIPES PRINCIPLE
03C01000D0	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	S PRINCIPES PRIN
03C01000E0	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	CIPES PRINCIPES
03C01000F0	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	PRINCIPES PRINCI
03C0100100	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	PES PRINCIPES PR
03C0100110	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	INCIPES PRINCIPLE
03C0100120	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	S PRINCIPES PRIN
03C0100130	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	CIPES PRINCIPES
03C0100140	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	PRINCIPES PRINCI
03C0100150	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	PES PRINCIPES PR
03C0100160	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	INCIPES PRINCIPLE
03C0100170	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	S PRINCIPES PRIN
03C0100180	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	CIPES PRINCIPES
03C0100190	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	PRINCIPES PRINCI
03C01001A0	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	PES PRINCIPES PR
03C01001B0	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	INCIPES PRINCIPLE
03C01001C0	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	S PRINCIPES PRIN
03C01001D0	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	CIPES PRINCIPES
03C01001E0	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	PRINCIPES PRINCI
03C01001F0	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	PES PRINCIPES PR
03C0100200	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	PRINCIPES PRINCI
03C0100210	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	PES PRINCIPES PR
03C0100220	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	INCIPES PRINCIPLE
03C0100230	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	S PRINCIPES PRIN

## 3.20 사이버테러

### 데이터 복구 관점에서 (Cont'd)

#### ■ VBR 흔적 Case #3

- 부트섹터부터 랜덤한 영역이

랜덤데이터로

- 남아있는 MFT 레코드를 이용

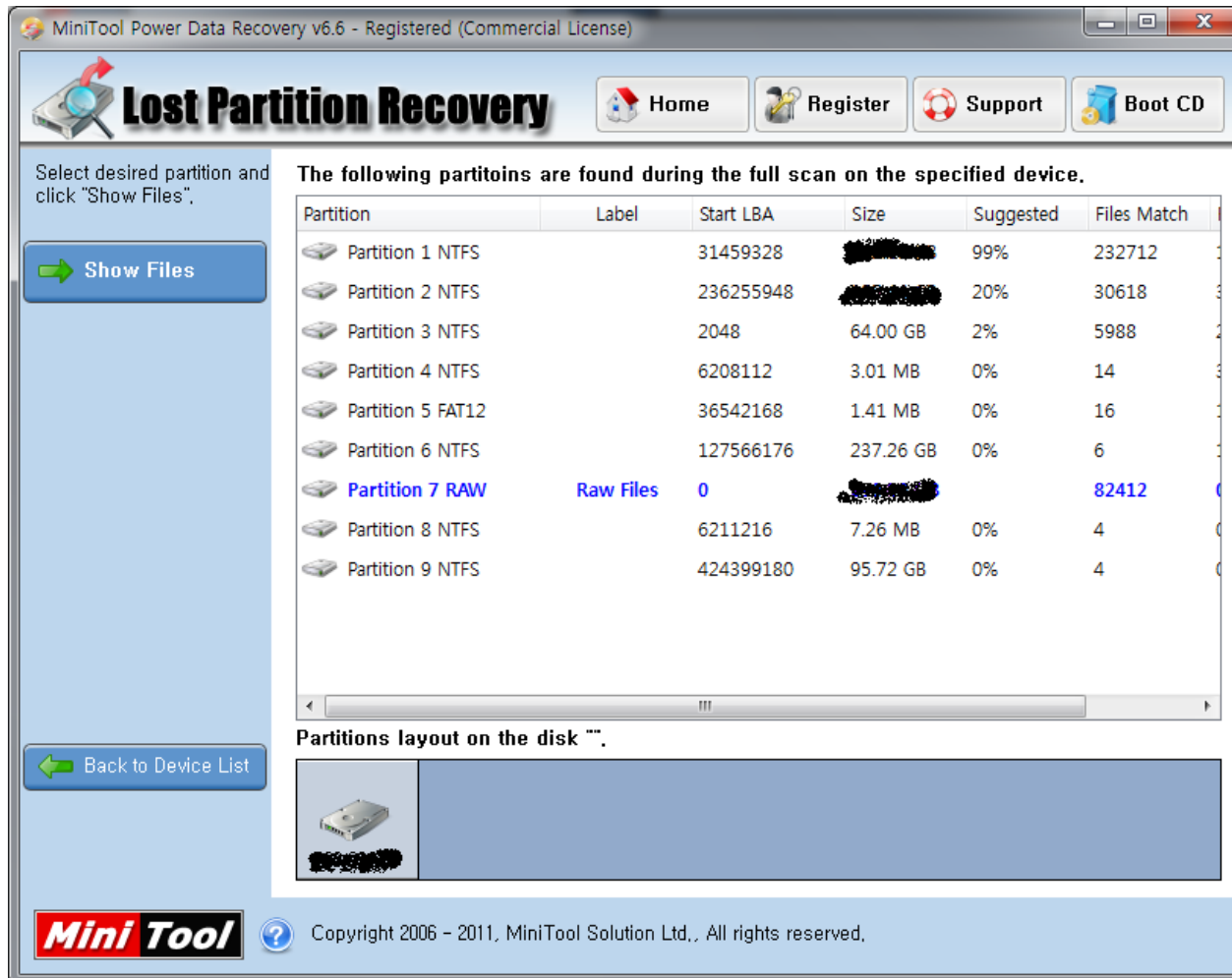
- 파일 카빙을 이용해 복구

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0A00100000	5A	BC	00	C7	C7	CD	CF	CD	C7	C6	CF	00	DC	CE	D1	CF	Z4 ÇİİİÇAI UINI
0A00100010	D1	CA	C9	C9	00	C4	AD	9A	92	90	8B	9A	AC	00	9A	8D	NÉÉÉ Ä-I' II~ I
0A00100020	89	9A	8D	D1	9A	87	00	9A	C4	3F	3F	40	14	DF	38	00	II ÑII IÄ??@ B8
0A00100030	3E	48	31	4E	28	48	5A	C4	00	CD	C7	CF	C9	C8	CD	DF	>H1N(HZÄ İÇİÉÉİB
0A00100040	9D	00	86	8B	9A	C4	AB	B8	AD	A6	00	B0	B8	B1	9E	9A	IIIA<,-  °,±II
0A00100050	A8	A5	BA	00	9B	AA	9B	A9	AB	B8	C6	AD	00	9E	B8	A5	"¶º IaI@«„Æ- I,¶
0A00100060	89	AD	95	98	C2	00	C4	BD	96	8B	AB	97	96	9A	02	99	I-İİÄ Ä½II«III I
0A00100070	10	86	CE	CA	CD	CC	CB	CB	02	CF	03	88	A9	B8	9B	CE	İİÉİİÉÉ İ İO,İİ
0A00100080	A9	B9	00	97	AA	A8	A9	8F	C9	B1	93	00	9B	92	AD	94	@: Ia"© É±I I'-I
0A00100090	B9	88	9A	A9	00	A9	CC	9D	92	8C	C2	C4	8D	0A	8C	02	'II© ©İ 'İÄÄ I
0A001000A0	87	CC	11	44	CD	CB	CD	CA	04	CF	CB	03	44	A5	CD	AD	İİ DİÉİÉ İÉ D¶İ-
0A001000B0	A5	9B	00	93	A9	8C	9A	A8	CA	CE	9E	00	B7	98	86	A8	¶I IOİİ'Éİİ .II"
0A001000C0	B8	97	A6	AA	00	A8	94	CA	AD	95	94	C2	C4	08	AF	BC	,I a "İÉ-İİÄÄ ¶¼
0A001000D0	DF	03	D4	DF	BC	90	91	20	8B	8D	90	93	93	12	D9	CE	B ÖB¼ ' I Iİ Üİ
0A001000E0	C6	10	CF	C6	C8	C9	83	27	AC	A7	B9	00	CB	AE	93	97	Æ İÆÉÉİ-Ş¹ ÉÖII
0A001000F0	CE	AD	B7	B9	00	CE	9E	93	B9	A8	AE	CE	97	80	BA	AA	İ-..¹ İİİ"®İİİİa
0A00100100	BA	CE	A8	B0	BB	80	27	80	BE	85	8A	8D	9A	8A	8C	90	qİ"°»I'İ½II III
0A00100110	49	12	CC	80	20	CD	C7	03	21	9D	BA	C7	00	86	A5	A9	I İİ İÇ ! qÇ I¶º
0A00100120	97	B5	9C	B7	AE	02	CC	00	21	8A	9B	CC	B1	B2	B2	00	IµI·@ İ İİİ±²²
0A00100130	BA	97	C9	AC	BA	C7	C2	C4	00	92	96	8C	8C	93	9A	9A	qİÉ-²ÇÄÄ 'IIIIII
0A00100140	92	40	9A	8C	8C	9A	91	98	04	47	C4	00	C6	CB	CD	C8	'@IIII'I GÄ ÆÉİÉ
0A00100150	CE	CE	CD	C4	00	A8	96	8C	85	AD	B8	A5	B3	00	AC	CC	İİİÄ "III-,¶³ -İ
0A00100160	93	8F	AE	93	BD	AA	00	AE	CC	AD	A6	AE	85	93	B4	08	I @I½a ©İ- @II'
0A00100170	9B	CF	AA	1D	1D	9E	92	AD	9E	00	AE	94	B1	85	9E	95	Iİa I'-I @İ±III
0A00100180	B2	CF	00	AA	B9	93	B1	9E	A9	B1	87	C0	B1	94	B9	A9	²İ a¹I±I©±İÄ±¹©
0A00100190	AC	B9	00	5C	93	3A	02	C8	00	3E	C8	CC	C9	C4	B1	B7	-¹ \I: É >ÉİÉÄ±·
0A001001A0	00	97	86	AC	AA	87	85	A8	94	00	A5	B3	9B	95	B1	87	II~aII'I ¶³II±I
0A001001B0	9B	CF	00	B5	B1	9B	CF	C6	B4	AD	93	02	90	5D	1D	B3	Iİ µ±İİÆ'-I ] ³
0A001001C0	CD	94	8D	AA	B8	00	AD	9E	9B	CC	A5	B3	AA	CF	00	AD	ÍI a, -İİİ¶³aİ -
0A001001D0	97	B2	94	87	95	A5	AB	20	B1	97	9B	CF	BA	9D	0E	A5	I²IIII¶« ±IIİº ¶
0A001001E0	B8	00	C6	A8	AB	CE	AD	8B	9C	AA	00	AE	86	AD	95	A9	,Æ"«İ-İİa @I-İ©
0A001001F0	BB	A5	A9	00	A5	8F	A5	92	CE	AF	AC	CE	02	A6	98	0E	»¶º ¶ ¶İ'-İ Iİ
0A00100200	C9	C9	CF	CF	C4	A5	00	CC	BD	94	AD	CF	A5	CA	9D	00	ÉÉİİÄ¶ İ½I-İ¶É
0A00100210	BB	9B	AA	A5	A8	90	CE	B2	00	AA	A9	91	9A	AA	CE	A9	»Ia¶" İ² a©'İaİ©
0A00100220	B1	04	BA	B6	5D	1D	9B	BA	CE	BB	9D	00	AB	BD	AA	9B	± ²¶I] I²İ» «½aI

## 3.20 사이버테러

### 데이터 복구 관점에서 (Cont'd)

- MiniTools Power Data Recovery



The screenshot displays the MiniTool Power Data Recovery v6.6 - Registered (Commercial License) window. The interface includes a navigation bar with 'Home', 'Register', 'Support', and 'Boot CD' buttons. The main area is titled 'Lost Partition Recovery' and contains a table of found partitions. A sidebar on the left has a 'Show Files' button and a 'Back to Device List' button. The table lists partitions 1 through 9, with Partition 7 highlighted as 'RAW' and 'Raw Files'. Below the table, there is a section for 'Partitions layout on the disk' with a visual representation of the disk layout.

MiniTool Power Data Recovery v6.6 - Registered (Commercial License)

**Lost Partition Recovery**

Select desired partition and click "Show Files".

[Show Files](#)

[Back to Device List](#)

The following partitions are found during the full scan on the specified device.

Partition	Label	Start LBA	Size	Suggested	Files Match
Partition 1 NTFS		31459328	[REDACTED]	99%	232712
Partition 2 NTFS		236255948	[REDACTED]	20%	30618
Partition 3 NTFS		2048	64.00 GB	2%	5988
Partition 4 NTFS		6208112	3.01 MB	0%	14
Partition 5 FAT12		36542168	1.41 MB	0%	16
Partition 6 NTFS		127566176	237.26 GB	0%	6
<b>Partition 7 RAW</b>	<b>Raw Files</b>	<b>0</b>	<b>[REDACTED]</b>		<b>82412</b>
Partition 8 NTFS		6211216	7.26 MB	0%	4
Partition 9 NTFS		424399180	95.72 GB	0%	4

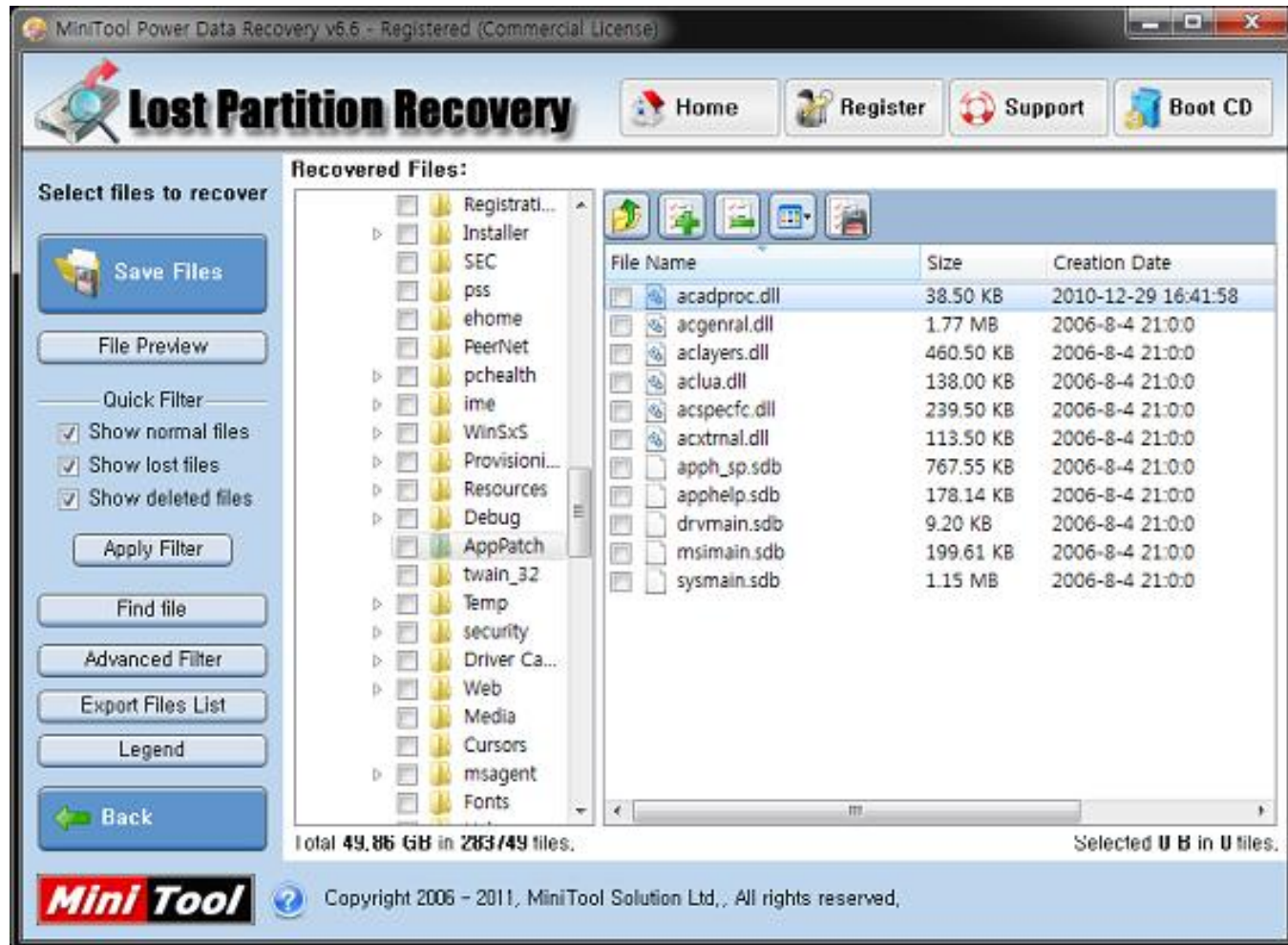
Partitions layout on the disk "".

**MiniTool** Copyright 2006 - 2011, MiniTool Solution Ltd., All rights reserved.

## 3.20 사이버테러

### 데이터 복구 관점에서

- MiniTools Power Data Recovery



## 3.20 사이버테러

### 침해사고 분석 관점에서 (Cont'd)

- 침해사고 포렌식 분석

- 침해원인을 찾으려면 파일시스템 메타데이터 분석이 필수 → 타임라인 분석
- 복구 도구의 MFT 레코드 복구 기능을 지원하는 포렌식 도구는?
- 남아있는 유효한 MFT Record가 없다면?
  - ✓ 타임라인 생성에 필요한 아티팩트 카빙
- 통합 포렌식 도구 이해
  - ✓ 도구는 어디까지 검증하는가? → 어디까지 복원해야 하는가?

## 3.20 사이버테러

### 침해사고 분석 관점에서

- 포렌식 도구로 로드하려면



1. VBR BPB(BIOS Parameter Block) 복원
2. MFTMirr(\$MFT, \$MFTMirr, \$LogFile, \$Volume Record)를 이용해 MFT Record 0(\$MFT) 복원

