정보보안론 13주차 강의

! 시험 – CERT가 무엇인지 !

CERT

미국 국방부 고등연구계획국(DARPA)은 컴퓨터와 관련한 침해 사고에 적절히 대응하기 위해 CERT를 만듬

! 시험 – 사전 대응, 등급별 대응 절차 !

사전 대응

기본적인 사전 대응은 침해 대응 체계를 구축하는 것

이를 위해 가장 먼저 할 일은 CERT를 구성하는 것

등급별 대응 절차

1등급 상황 대응 절차 : 시스템 담당자가 CERT 팀장에게 즉시 보고.

2·3등급 상황 대응 절차 : 비인가 접근 시도 및 정보 수집 행위를 발견하면 CERT와 함께 해당 단말기나 IP 조사하여 소속 네트워크와 조직 파악

! 시험 – 포렌식이 무엇인지 !

디지털 포렌식 : 법정 제출을 전제로 디지털 환경과 장비를 이용하여 디지털 증거 자료를 수집·분석하는 기술

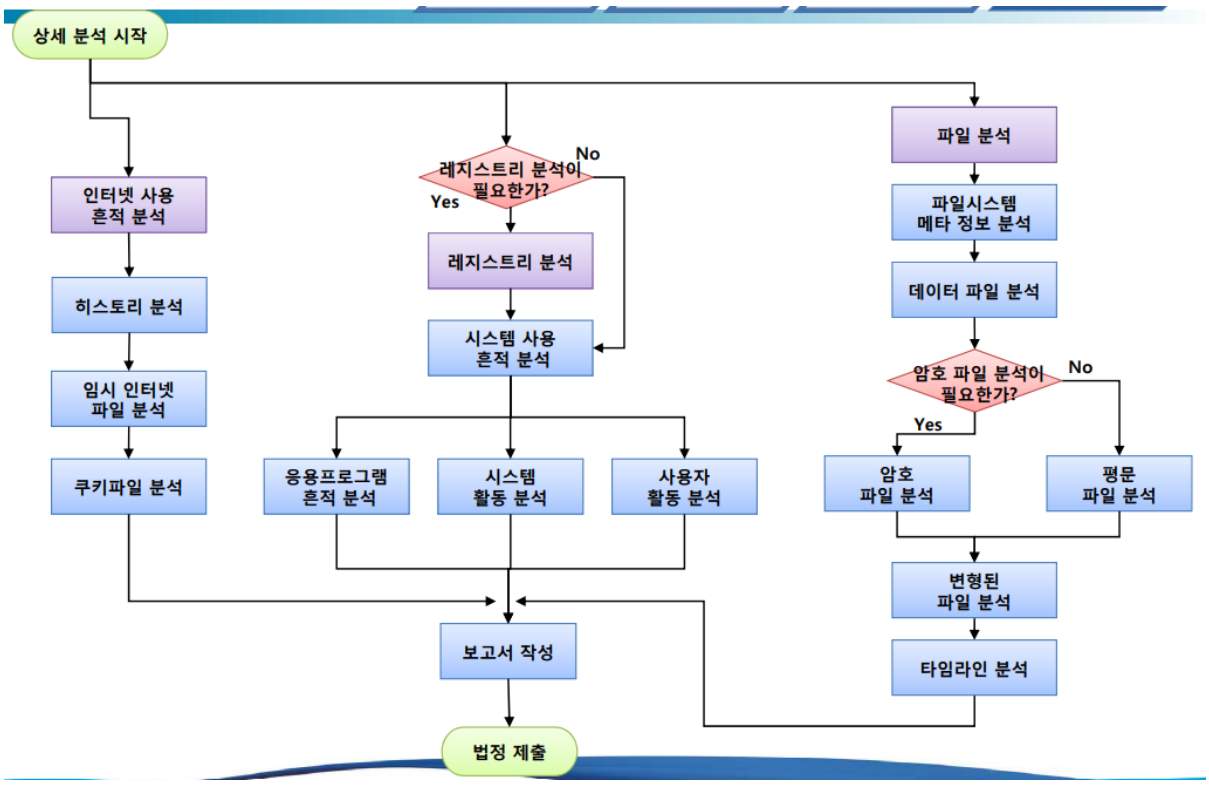
파일이 설치될 때는 오래걸리지만 파일을 삭제할때는 빨리 걸림 -> 파일을 지우지 않음

! 시험 – 사본 디스크 확보 !

- **사본 디스크 확보**
  - 하드디스크에 저장된 데이터를 복구하고 분석할 필요가 있지만 굳이 원본을 확보할 필요가 없는 경우 수행
  - 입수된 하드디스크를 분석 시스템에 연결 하여 조사/분석 과정을 수행하면, 증거물이 손상되므로 복제(사본) 디스크를 생성

- **디스크 이미징(Disk Imaging)을 이용한 사본 생성**
  - 원본 디스크를 복제(Bit by Bit Copy)하여 사본 디스크를 생성
  - 디스크 이미징 H/W 장비를 이용하여 다른 하드디스크에 이를 복제
  - 또는 디스크 이미징 S/W를 사용하여 디스크 이미지 파일을 생성
    - 디스크 이미지 파일 (Disk Image or Forensic Image)
      - 원본 디스크를 복제하여 이미지 파일을 생성하여 사본 디스크를 대신함
      - 원본 디스크와 동일함을 증명하기 위해 검증 과정이 필요 (해쉬함수로 무결성 검증)

! 시험 !



! 시험 !

📊 FAT vs NTFS 비교

구분	FAT/FAT32	NTFS
출시년도	1977년	1993년
최대 파일 크기	4GB (FAT32)	16EB (실제 수 TB)
최대 볼륨 크기	2TB (FAT32)	16EB
호환성	Windows, Linux, macOS, Android 등 대부분 지원	Windows 중심, 다른 OS는 제한적
보안	없음	권한 제어, 암호화 지원
복구 기능	제한적	저널링으로 데이터 복구 가능
적합 환경	USB, SD카드, 외장장치	Windows PC, 서버, 대용량 스토리지

! 시험 !

🔒 NTFS가 복구 가능한 이유

1. **자체 메타데이터 구조**
   - NTFS는 모든 파일과 디렉터리 정보를 **MFT(Master File Table)** 라는 중앙 데이터베이스에 저장합니다.
   - MFT는 파일 이름, 위치, 크기, 속성 등을 기록하는 NTFS의 핵심 구조입니다.
2. **중복 저장**
   - NTFS는 MFT의 중요한 부분을 디스크 여러 위치에 **백업 복사본**으로 저장합니다.
   - 파티션 테이블이 손상되어도, NTFS 내부의 MFT 복사본을 통해 파일 시스템을 재구성할 수 있습니다.
3. **저널링(Journaling)**
   - 파일 시스템 변경 작업을 로그로 기록해 두기 때문에, 갑작스러운 손상 시에도 **일관성 있는 상태로 되돌릴 수 있음.**
   - 이는 FAT에는 없는 기능입니다.

📍 MFT 복사본의 위치

- **첫 번째 MFT:**
  - NTFS 파티션의 **가장 앞쪽(논리적 클러스터 0 근처)**에 위치합니다.
  - 여기서 모든 파일과 디렉터리의 메타데이터를 관리합니다.
- **MFT 미러(MFT Mirror):**
  - NTFS는 MFT의 **첫 4개의 레코드**를 디스크의 **중간 지점(파티션의 절반 위치)**에 복사해 둡니다.
  - 이 복사본을 **MFT Mirror**라고 부르며, 원본 MFT가 손상되었을 때 복구에 사용됩니다.

! 시험 !

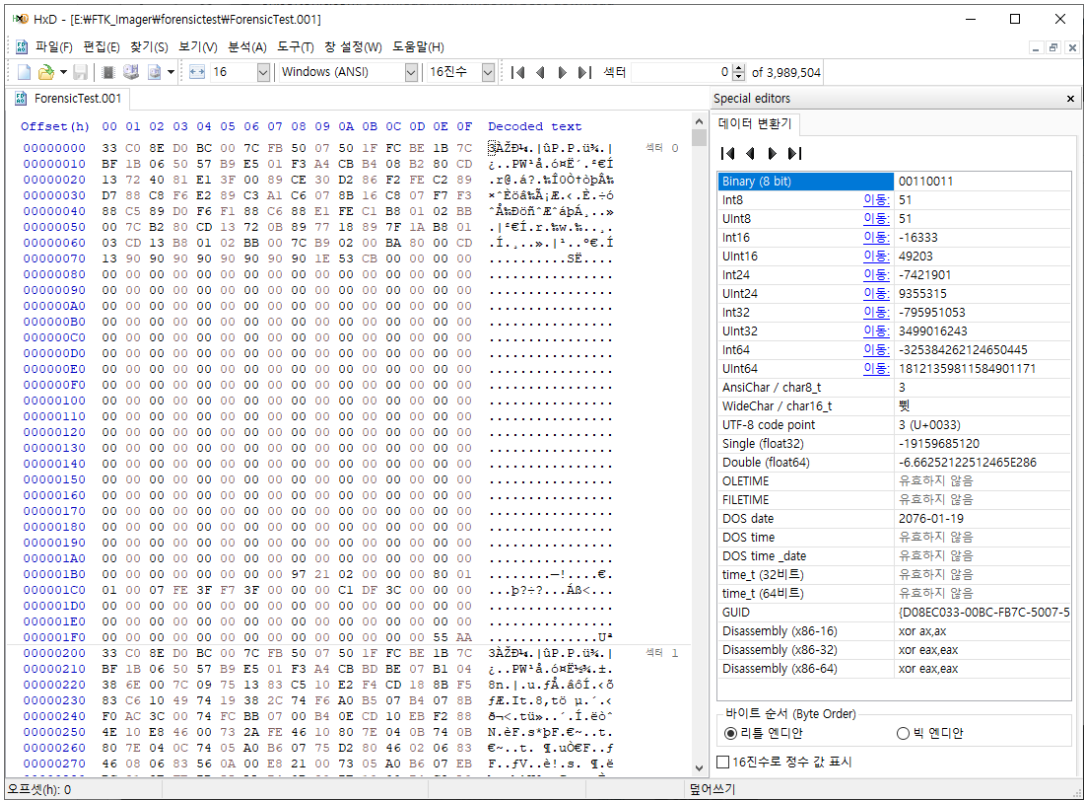
55 AA: 마이크로소프트사의 코드 (MS에서 포맷한 저장장치)

! 시험 – 데이터 전용 저장장치 인지 부팅용 저장장치 인지 구별 !

부트코드가 비어 있으면 데이터 전용 저장장치

부트코드에 꽉 차 있으면 부팅용 저장장치

! 시험 – 사진보고 분석해서 설명 !



-> 파티션이 1개 짜리, 데이터 전용 저장장치

```
0000000000 33 C0 8E D8 8E C0 8E D0-BC 00 7C 8B F4 BF 00 06 3À·Ø·À·Ð¼·|·ô¿··
0000000010 B9 00 01 FC F3 A5 EA 1B-00 60 00 0E 1F 06 E8 95 ¹··üó¥ê··`····è·
0000000020 00 07 80 3E 97 01 01 74-75 80 3E 97 01 02 74 00 ···>···tu·>···t·
0000000030 C6 06 94 01 00 E8 04 01-BE BE 01 B3 04 F6 04 80 Æ····è···¾¾·³·ö··
0000000040 75 0F 83 C6 10 FE CB 75-F4 CD 18 BE 5D 01 E8 FC u··Æ·þËuôÍ·¾]·èü
0000000050 00 BB 00 7C 06 53 50 55-8B EC C7 46 02 00 00 5D ·»·|·SPU·ìÇF···]
0000000060 50 55 8B EC C7 46 02 00-00 5D FF 74 0A FF 74 08 PU·ìÇF···]ÿt·ÿt·
0000000070 06 53 50 55 8B EC C7 46-02 01 00 5D 50 55 8B EC ·SPU·ìÇF···]PU·ì
0000000080 C7 46 02 10 00 5D 16 1F-8B F4 B4 42 CD 13 83 C4 ÇF···]···ô´BÍ··Ä
0000000090 10 EB 00 CB C6 06 95 01-00 E8 A0 00 EB 00 BB 00 ·ë·ËÆ····è ·ë·»·
00000000a0 7C 06 53 B8 01 02 B5 00-B1 05 B6 00 B2 80 CD 13 |·S¸··µ·±·¶·²·Í·
00000000b0 C6 06 94 01 01 CB B8 00-F0 8E C0 33 C0 8B F0 BB Æ····Ë¸·ð·À3À·ð»
00000000c0 FF FF 26 81 3C 53 77 74-08 83 C6 01 4B 75 F3 EB ÿÿ&·<Swt··Æ·Kuóë
00000000d0 1A 26 81 7C 02 53 6D 74-02 EB EE 26 81 7C 04 69 ·&·|·Smt·ëî&·|·i
00000000e0 40 74 02 EB E4 83 C6 06-E8 01 00 C3 1E 57 26 8B @t·ëä·Æ·è··Ã·W&·
00000000f0 14 26 8A 44 03 EE 26 8B-44 07 8E D8 26 8B 44 05 ·&·D·î&·D··Ø&·D·
0000000100 8B F8 C7 05 43 58 C7 45-02 5C 00 26 8A 44 02 EE ·øÇ·CXÇE·\·&·D·î
0000000110 B1 02 8A 65 05 80 FC FF-74 13 80 FC 80 76 0E C7 ±··e··üÿt··ü·v·Ç
0000000120 45 02 5D 00 80 EC 80 88-65 05 EE B1 01 26 8B 14 E·]··ì··e·î±·&··
0000000130 26 8A 44 04 EE 5F 1F 88-0E 97 01 C3 BB 00 06 B8 &·D·î_·····Ã»···¸
0000000140 01 03 B5 00 B1 01 B6 00-B2 80 CD 13 C3 AC 3C 00 ··µ·±·¶·²·Í·Ã¬<·
0000000150 74 0A B4 0E B7 00 B3 07-CD 10 EB F1 C3 4D 69 73 t·´·····³·Í·ëñÃMis
0000000160 73 69 6E 67 20 6F 70 65-72 61 74 69 6E 67 20 73 sing operating s
0000000170 79 73 74 65 6D 00 00 00-00 00 00 00 00 00 00 00 ystem·····
0000000180 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ·····
0000000190 46 44 53 54 00 00 3E 02-00 27 00 00 BC 0A 8D 7E FDST··>··'··¼··~
00000001a0 67 20 6F 70 65 72 61 74-69 6E 67 20 73 79 73 74 g operating syst
00000001b0 65 6D 00 00 00 63 7B 9A-17 56 4A 94 00 00 80 20 em···c{··VJ···· 
00000001c0 21 00 07 DF 13 0C 00 08-00 00 00 20 03 00 00 DF !··ß·····  ···ß
00000001d0 14 0C 07 FE FF FF 00 28-03 00 00 28 03 0C 00 FE ···þÿÿ·(···(···þ
00000001e0 FF FF 84 FE FF FF 00 50-06 0C 00 60 89 00 00 FE ÿÿ·þÿÿ·P···`···þ
00000001f0 FF FF 27 FE FF FF 00 B0-8F 0C 00 10 58 02 55 AA ÿÿ'þÿÿ·°····X·Uª
```

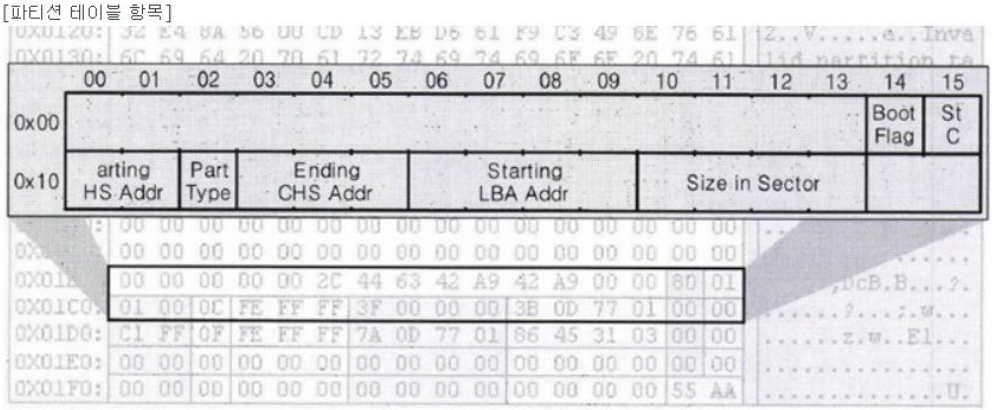
위 그림처럼 16Byte 마다 1나의 파티션에 대한 정보가 들어가게 된다 즉 4개의 파티션까지 기록 가능 하다.

4.DOS 파티션의 구조

1) MS-DOS 파티션 테이블의 구성
[MBR영역 내의 파티션 테이블 구조도]

위치(Byte)	크기(Byte)	설명
0	446	부트코드
446	16	파티션 #1
462	16	파티션 #2
478	16	파티션 #3
494	16	파티션 #4
510	2	MBR Signature(0xAA55)

[파티션 테이블 항목]



! 시험 - MBR의 설명, 구조, 역할 !

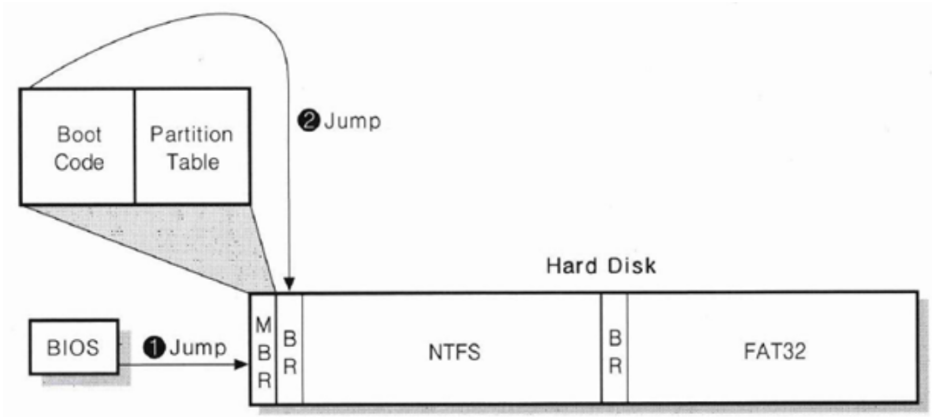
마스터부트레코드의 역할 : 저장장치의 특징이 들어가 있다.

2)MBR의 역할
- 디스크 0번 섹터에 위치하며 부팅에 필요한 부트 코드와 파티션 테이블을 포함하고 있다.
- MBR 영역 내에 프로그램된 부트 코드의 경우 부팅이 목적이며 커널이 적재되기 전까지 하나하나의 과정들의 목표는 부팅 과정에 있어 다음 단계를 호출 하는 것이 된다.
- MBR의 경우 BR을 호출하는 과정을 위한 프로그램이 될 것이다. 따라서 파티션 테이블을 읽고, 각각의 파티션이 부팅 가능한지 확인하며, 파티션이 정상적이지 않거나 부팅 가능한 파티션이 없는 경우 예외 처리도 해야한다.
- 최종적으로 부팅 가능한 파티션의 실제 주소(Address)를 계산하여 해당 파티션의 Boot Record를 호출하는 것이 주요 목적이 될것이다.
- Microsoft의 경우 MBR영역에 파티션 테이블까지 입력하게 되기 때문에 512Byte가 작은 공간이 아닐 것이다.

3)BIOS와 부트 시퀀스
- 부트 시퀀스(Boot Sequence)는 시스템에 전원이 들어오거나 시스템을 재시작하는 경우 커너을 로드하기까지의 일련의 과정이라고 할 수 있다. 이 과정 중에는 주기억장치에서 커널을 메모리에 적재하는 등의 여러 가지 작업들이 있지만, 그 중에서도 가장 선행되는 작업은 BIOS(Basic Input/Output System)에 의해 행해지는 검증 작업니다.
- BIOS는 PC에서 전원이 들어오자마자 구동되는 플래시 메모리(Flash Memory) 내의 펌웨어이며, 보통 ROM BIOS라고도 불리낟.
- BIOS는 CPU 상태를 비롯, 메모리와 여러 장치, 포트 등이 사용가능한지 검증 및 자제 테스트를 진행하고, 커널과 PC 디바이스간의 인터페이스를 제공한다. 즉 우리가 사용하는 OS 내지 응용프로그램에서 하드웨어를 호출할 수 있는 창구 역할을 하게 되는 것이다.

! 시험 !

[MBR 호출 과정]



- PC의 경우 BIOS라는 펌웨어가 시스템 내의 장치들을 검사한 뒤 이상 없다면 저장장치의 가장 앞부분으로 점프할 것이다. 이때 단순히 첫 번째 섹터로 이동하는 것이므로 MBR이든 BR이든 부팅 가능한 프로그램만 실행 될 수 있으면 될것이다.
- 다른 시스템의 경우 나름대로 첫 번째 섹터를 사용하는 방법이 다르고 부르는 말도 다르다.

실습

복구할 폴더를 넣어서 완료한 모습