침해 지속 아티팩트

JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

개요

1. 루트킷
2. 악성코드 선호 경로
3. 비정상 파일
4. 슬랙 공간
5. 시간 조작
6. 자동 실행 목록
7. 작업 스케줄러
8. 이벤트 로그

루트킷

▪ 루트킷 소개

- 시스템 상에서 탐지되지 않도록 만들어진 프로그램

- **루트킷 종류**
  - ✓ 부트킷
  - ✓ 사용자 레벨 루트킷
  - ✓ 커널 레벨 루트킷

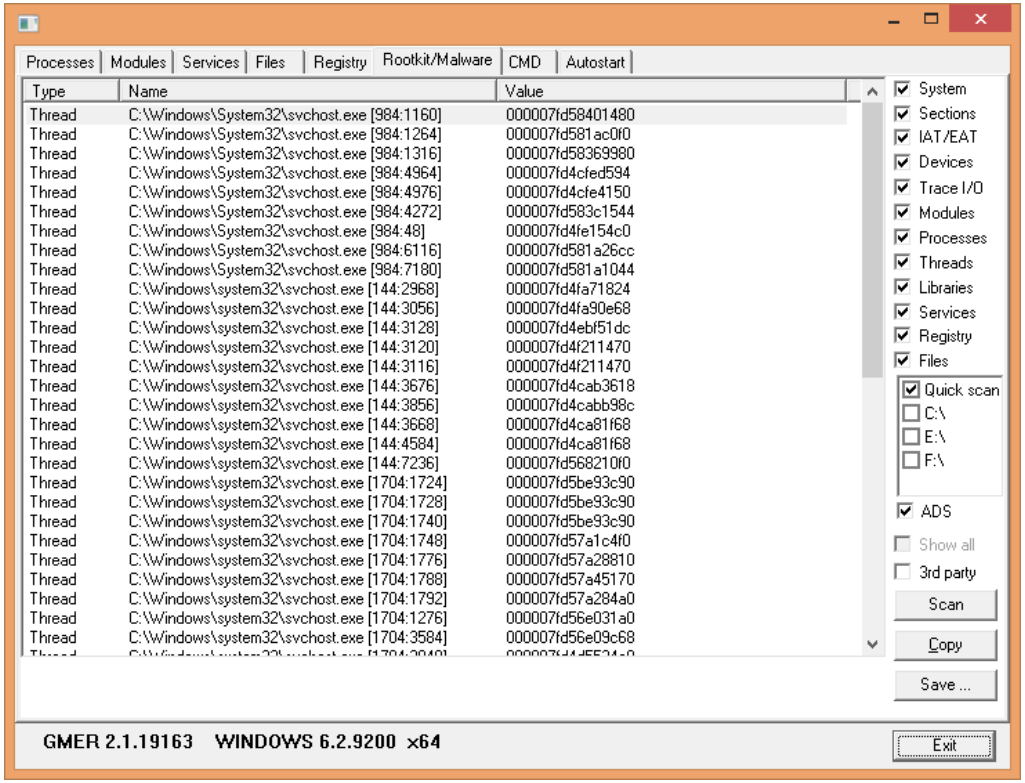
- **탐지 방법**
  - ✓ 시그니처 기반
  - ✓ 행위 기반
  - ✓ 차이점 기반
  - ✓ 무결성 체크
  - ✓ 메모리 덤프

루트킷

- **루트킷 분석 도구**
  - **다양한 루트킷 탐지 도구**
    - ✓ http://grandstreamdreams.blogspot.kr/2014/01/advanced-anti-rootkit-tool-list-mostly.html
  - **GMER**
    - ✓ http://www.gmer.net/
  - **Rootkit Removal** – SOPHOS
    - ✓ http://www.sophos.com/en-us/products/free-tools/sophos-anti-rootkit.aspx
  - **TDSSKiller** – Kaspersky
    - ✓ http://support.kaspersky.com/5350?el=88446
  - **aswMBR** – Avast
    - ✓ http://public.avast.com/~gmerek/aswMBR.htm
  - **Rootkit Revealer** – Windows Sysinternals
    - ✓ http://technet.microsoft.com/ko-kr/sysinternals/bb897445.aspx

루트킷

- **루트킷 탐지 도구 – GMER, http://www.gmer.net/**
  - **검사 항목**
    - ✓ 숨겨진 프로세스
    - ✓ 숨겨진 스레드
    - ✓ 숨겨진 모듈
    - ✓ 숨겨진 서비스
    - ✓ 숨겨진 파일
    - ✓ 숨겨진 디스크 섹터(MBR)
    - ✓ 숨겨진 대체데이터스트림(ADS)
    - ✓ 숨겨진 레지스트리 키
    - ✓ SSDT 드라이버 후킹
    - ✓ IDT 드라이버 후킹
    - ✓ IRP 호출 드라이버 후킹
    - ✓ 인라인 후킹



악성코드 선호 경로

악성코드 선호 경로

- **선호 경로?**
  - **흔하지 않은, 주로 사용하지 않는 경로에 파일 생성**
    - ✓ AV 실시간 탐지를 우회하기 위한 목적
    - ✓ 사용자에게 인지되지 않고 장기간 은닉하기 위한 목적
  - **분석 방법**
    - ✓ 선호 경로를 수시로 모니터링
    - ✓ 선호 경로에 위치한 실행 파일을 수집하여 분석
    - ✓ 특정 경로에 실행 파일이 위치할 경우, 99% 악성코드일 가능성

악성코드 선호 경로

- **주요 선호 경로**
  - **시스템 폴더**
    - ✓ %SystemRoot₩
    - ✓ %SystemRoot₩System₩
    - ✓ %SystemRoot₩System32₩
    - ✓ %SystemRoot₩System32₩dllcache₩
    - ✓ %SystemRoot₩System32₩drivers₩
  - **WoW64**
    - ✓ %SystemRoot₩SysWOW64₩
    - ✓ %SystemRoot₩SysWOW64₩dllcache₩
    - ✓ %SystemRoot₩SysWOW64₩drivers₩

악성코드 선호 경로

- **주요 선호 경로**
  - **사용자 프로파일 폴더**
    - ✓ %SystemDrive%₩Default₩
    - ✓ %SystemDrive%₩Public₩
    - ✓ %SystemDrive%₩<USER>₩
  - **사용자 데이터 폴더**
    - ✓ %UserProfile%₩AppData₩
    - ✓ %UserProfile%₩AppData₩Local₩
    - ✓ %UserProfile%₩AppData₩Roaming₩
  - **휴지통 폴더**
    - ✓ %SystemDrive%₩$Recycle.Bin₩

악성코드 선호 경로

- **주요 선호 경로**
  - **프로그램 데이터 폴더**
    - ✓ %SystemDrive%₩ProgramData₩(%SystemDrive%₩All Users₩)
  - **시스템 볼륨 정보 폴더**
    - ✓ %SystemDrive%₩System Volume Information₩
  - **임시 폴더**
    - ✓ %UserProfile%₩AppData₩Local₩Temp₩
    - ✓ %SystemRoot%₩Temp₩
  - **인터넷 캐시 폴더**
    - ✓ %UserProfile%₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩

악성코드 선호 경로

- **주요 선호 경로**
  - **액티브X 폴더**
    - ✓ %SystemRoot%₩Downloaded Program Files₩
  - **시작 프로그램 폴더**
    - ✓ %UserProfile%₩AppData₩Roaming₩Microsoft₩Windows₩Start Menu₩Programs₩Startup₩
  - **작업 스케줄러 폴더**
    - ✓ %SystemRoot%₩Tasks₩
  - **알려진 폴더**
    - ✓ %SystemDrive%₩Intel₩

비정상 파일

비정상 파일

- **비정상 파일?**
  - **파일 메타정보 조작을 통해 은닉**
    - ✓ 보안 솔루션을 우회하기 위한 목적
    - ✓ 단순한 파일명이나 확장자 기반의 탐지룰을 우회하기 위한 목적
  - **분석 방법**
    - ✓ 생성되는 파일이 악성 패턴을 갖는지 검사
    - ✓ 네트워크로 전송되는 파일이 악성 패턴을 갖는지 검사

비정상 파일

- **비정상 파일 패턴**
  - **한 글자 파일명**
    - ✓ a.gif, b.jpg, g.exe, v.exe, …
  - **랜덤한 문자나 숫자로만 이뤄진 파일명**
    - ✓ hdpfoi.exe, yyr.exe, 3378.exe, 499389.exe, …
  - **확장자 변경으로 시그니처 불일치**
    - ✓ abc.jpg, gcc.gif – PE 파일
  - **대체 데이터 스트림(ADS, Alternative Data Stream)**
    - ✓ C:₩Windows₩System32:scvhost.exe

비정상 파일

- **비정상 파일 패턴**
  - **“svchost.exe”와 유사한 악성 파일명**

svchost	svcehost	svchostc32	svghost
svch0st	svphost	szchostc	svchostms
svchosts	svchostdll	svehost	svchostxxx
scvhost	svvhosti	srvchost	suchostp
svhost	sach0st	svchosts32	suchosts
svohost	swchost	scvhosv	smsvchost
svchest	servehost	ssvichosst	svchost0
svchost32	svsh0st	svrhost	svchost64
suchost	svchsot	svichosst	svchöst
svshost	scchostc	svchoxt	s_host
svchast	snvhost	svchost_cz	svchost”
svcnost	scchost	schost	svphostu
syshost	svvhost	ssvchost	svchosting
svchcst	svahost	sv±hest	sachostc
svchost	svcinit	shhost	sachostw
svchon32	ssvch0st	svchostt	svshoct
svchost2	svchots	svchosf	svchpst
Svcchost	svdhost	svchostþ	svohcst
sxhost	svchostv	sachostp	scanost
svchost31	scvchusts	sachosts	schosts
syschost	svchostxi	sachostx	svcroot
svchîst	st#host	swhost	svschost
synchost	svchost3	scvh0st	scvhosts

http://www.hexacorn.com/blog/2013/07/04/the-typographical-and-homomorphic-abuse-of-svchost-exe/

은닉 데이터

은닉 데이터

- **숨긴/암호화 파일**
  - 사용자의 의도적인 행위가 포함됐을 가능성

  - **숨긴 파일 탐색**
    - ✓ **FAT** – 디렉터리 엔트리의 속성 값이 0x02를 갖는 파일 탐색
    - ✓ **exFAT** – 파일 디렉터리 엔트리의 속성 값이 0x02를 갖는 파일 탐색
    - ✓ **NTFS** – $STANDARD_INFORMATION 속성의 플래그 값이 0x0002를 갖는 파일 탐색

  - **암호화된 파일 탐색**
    - ✓ **NTFS** – $STANDARD_INFORMATION 속성의 플래그 값이 0x4000을 갖는 파일 탐색
      - 레지스트리의 암호화된 private key 복호화 (무차별 대입)
      - EFS0.TMP 파일 조사

- **메타데이터 조작**
  - **시그니처 변조**
    - ✓ 파일 시그니처와 확장자가 일치하는지 검사
    - ✓ 윈도우는 확장자 기반의 애플리케이션 바인딩 사용
    - ✓ 확장자를 변경해 파일을 은폐하거나 사용자의 클릭 유도!!
    - ✓ **확장자 위치**
      - **FAT** – 디렉터리 엔트리
      - **exFAT** – 파일 이름 확장 디렉터리 엔트리
      - **NTFS** – $FILE_NAME 속성

은닉 데이터

- **메타데이터 조작**
  - **$Boot**
    - ✓ $Boot는 부트 섹터의 내용을 저장 (VBR의 부트 섹터 위치를 가르킴)
    - ✓ $Boot 파일 크기는 제한이 없음 ➔ 크기를 늘려 데이터 은닉
  - **$BadClus**
    - ✓ $BadClus는 배드섹터가 포함된 클러스터를 관리
    - ✓ 정상 클러스터를 $BadClus에 등록한 후 의도적인 데이터 저장

은닉 데이터

- **파일시스템 상의 낭비되는 공간**
  - **FAT12/16/32**
    - ✓ 예약된 영역의 낭비되는 섹터(0,1,2,6,7,8 섹터 제외) 조사
    - ✓ FSINFO 섹터(1,7 섹터)의 사용되지 않는 영역 조사
    - ✓ 추가 부트 코드 섹터(2,8 섹터) 영역 조사
  - **exFAT**
    - ✓ VBR의 확장 부트 코드 영역(1~8 섹터)와 예약된 영역(10 섹터) 분석
    - ✓ 백업 VBR 영역 조사
  - **NTFS**
    - ✓ VBR의 낭비되는 영역 조사
    - ✓ MFT 레코드 12~15번 영역 조사
    - ✓ 백업 VBR 영역 조사
  - **HPA(Host Protected Area), DCO(Device Configuration Overlay) 조사**

▪ 슬랙 공간

• 슬랙이란?

- ✓ 물리적인 구조와 논리적인 구조의 차이로 발생하는 낭비되는 공간
- ✓ 의도적으로 삽입한 데이터나 이전 파일의 데이터가 남아 있을 가능성
- ✓ 파일 기반의 슬랙 이외에 DB 레코드 슬랙, 파일시스템 구조 슬랙 등 다양한 부분 조사

• 슬랙 종류

- ✓ MBR 슬랙
- ✓ 램 슬랙, 드라이브 슬랙
- ✓ 파일시스템 슬랙
- ✓ 볼륨 슬랙
- ✓ MFT 슬랙, INDX 슬랙
- ✓ … …

은닉 데이터

- **MBR 슬랙**

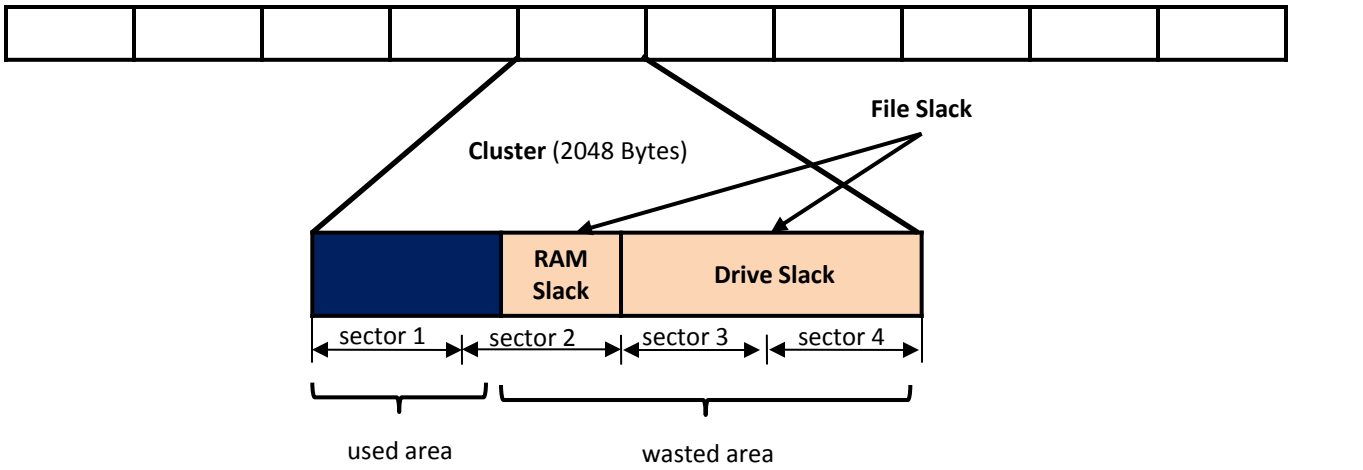
- MBR과 첫 번째 볼륨 사이에 낭비되는 공간

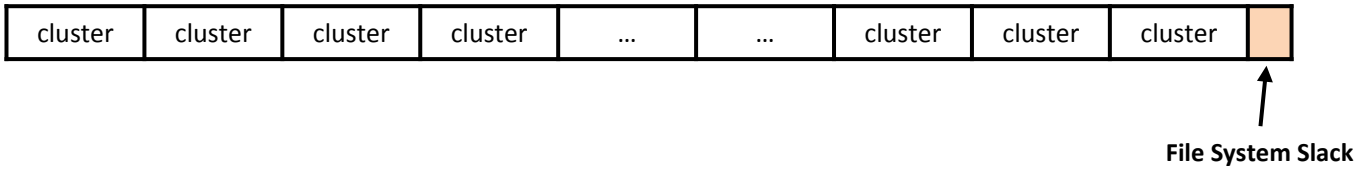
- **윈도우 2K/XP**
  - ✓ 과거 FDISK는 트랙 할당 방식
  - ✓ 62섹터의 빈 공간 발생

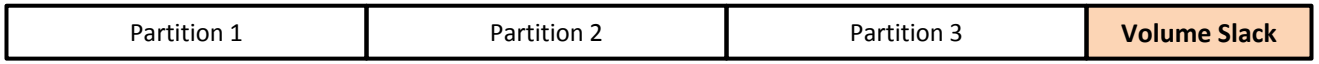
- **윈도우 Vista 이후**
  - ✓ 최근 1MiB 할당 방식
  - ✓ 2047섹터의 빈 공간 발생

은닉 데이터

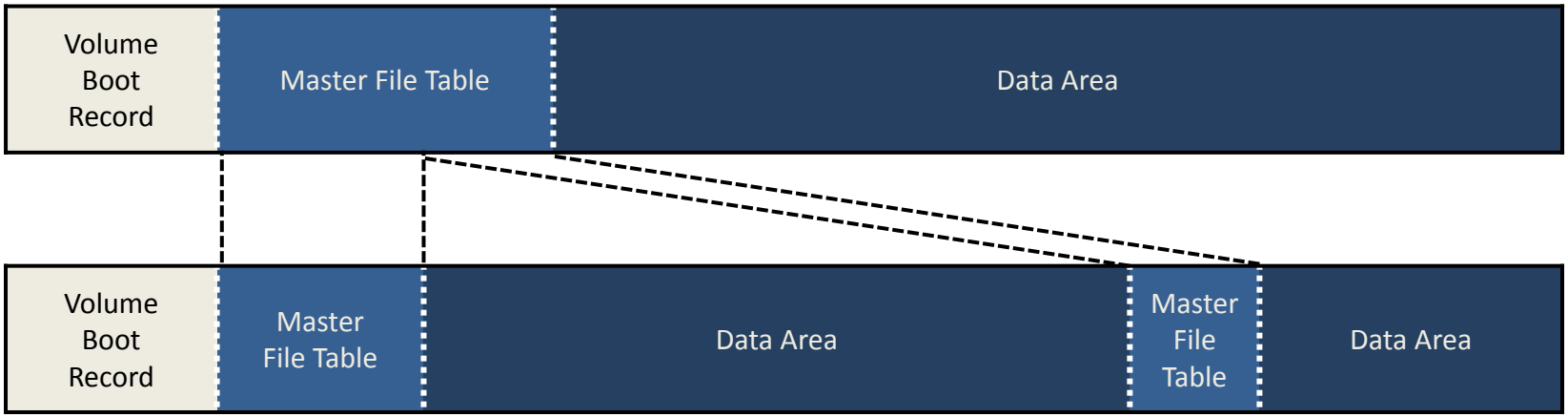
- 램/드라이브/파일시스템/볼륨 슬랙





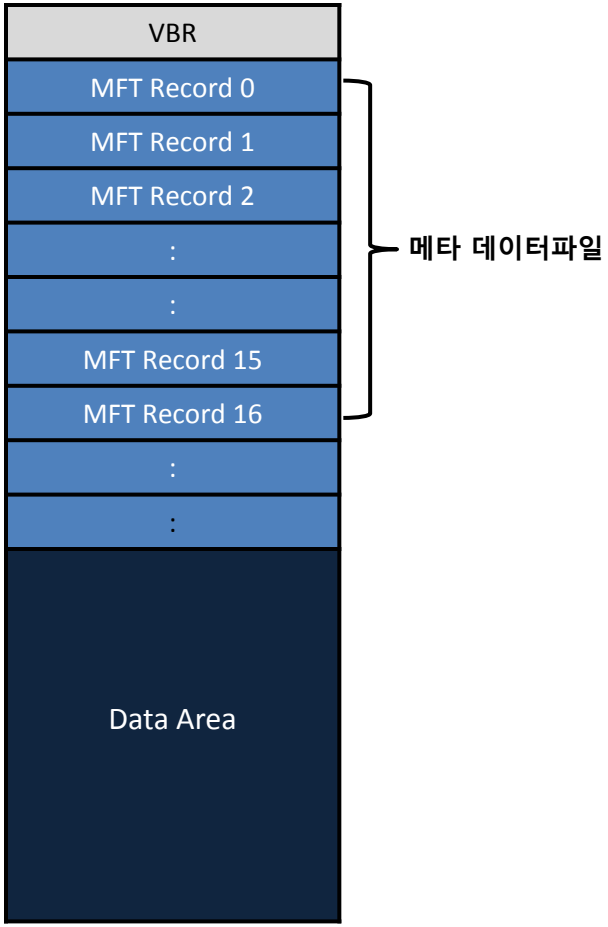


- **MFT 슬랙**
  - **NTFS 파일시스템 추상화 구조**



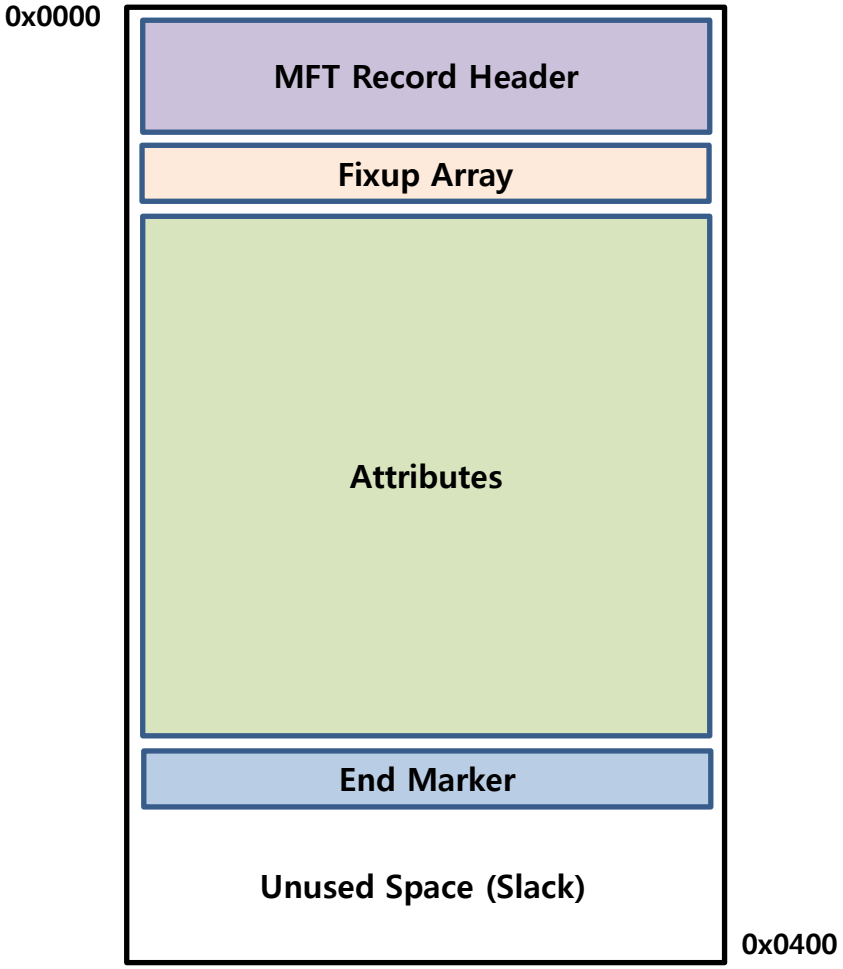
- **MFT 슬랙**

  - **MFT 레코드**



번호	이름	설명
0	$MFT	MFT에 대한 MFT Entry
1	$MFTMirr	$MFT 파일의 일부 백업본
2	$LogFile	메타데이터(MFT)의 트랜잭션 저널 정보
3	$Volume	볼륨의 레이블, 식별자, 버전 등의 정보
4	$AttrDef	속성의 식별자, 이름, 크기 등의 정보
5	.	볼륨의 루트 디렉터리
6	$Bitmap	볼륨의 클러스터 할당 정보
7	$Boot	볼륨이 부팅 가능할 경우 부트 섹터 정보
8	$BadClus	배드 섹터를 가지는 클러스터 정보
9	$Secure	파일의 보안, 접근 제어와 관련된 정보
10	$Upcase	모든 유니코드 문자의 대문자
11	$Extend	$ObjID, $Quota, $Reparse points, $UsnJrnl 등의 추가적인 파일의 정보를 기록하기 위해 사용
12 – 15		미래를 위해 예약
16 -		포맷 후 생성되는 파일의 정보를 위해 사용
-	$ObjId	파일 고유의 ID 정보 (Windows 2000 -)
-	$Quota	사용량 정보 (Windows 2000 -)
-	$Reparse	Reparse Point 에 대한 정보 (Windows 2000 -)
-	$UsnJrnl	파일, 디렉터리의 변경 정보 (Windows 2000 -)

- MFT 슬랙
  - MFT 레코드 구조

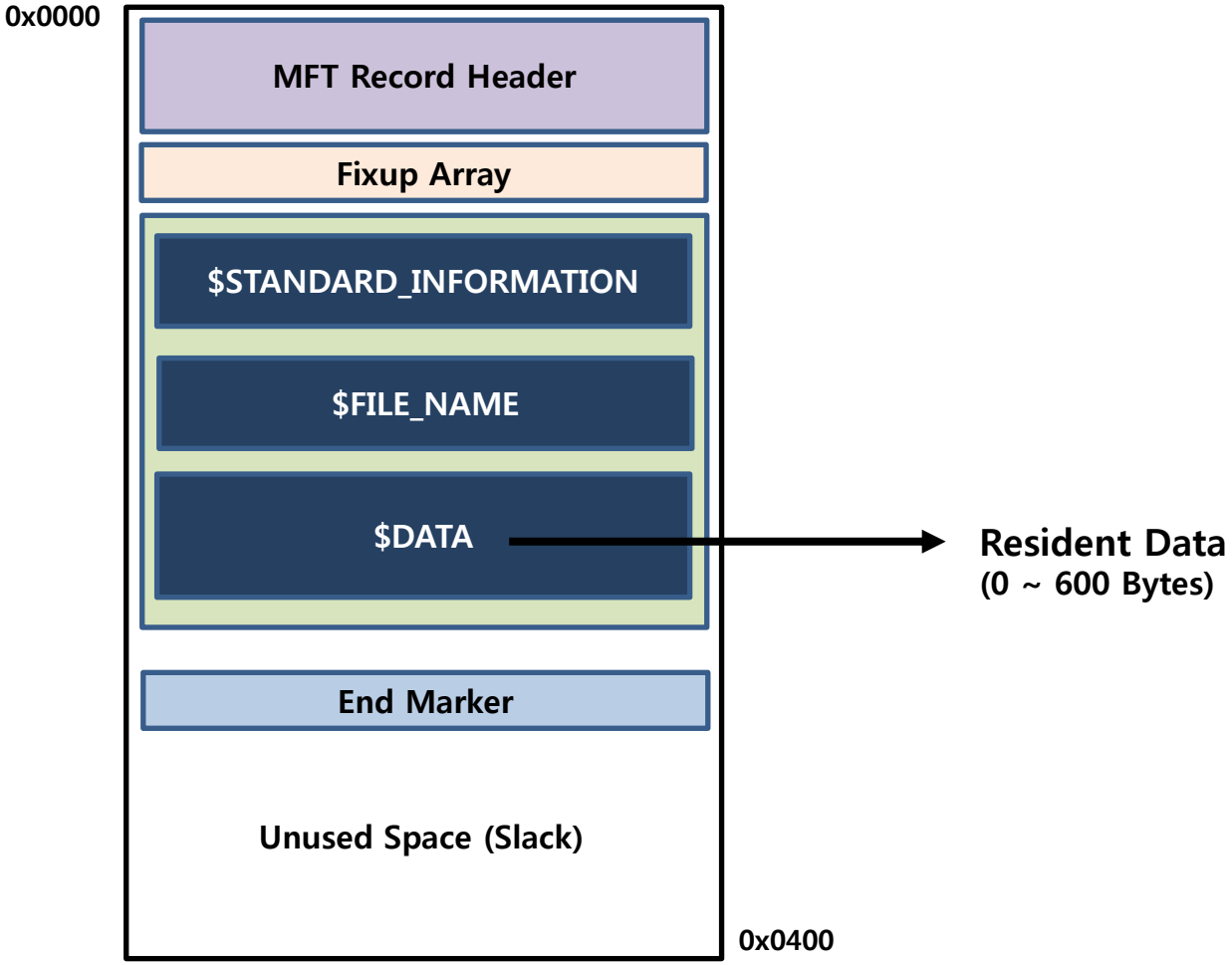


▪ MFT 슬랙

• MFT 레코드 속성

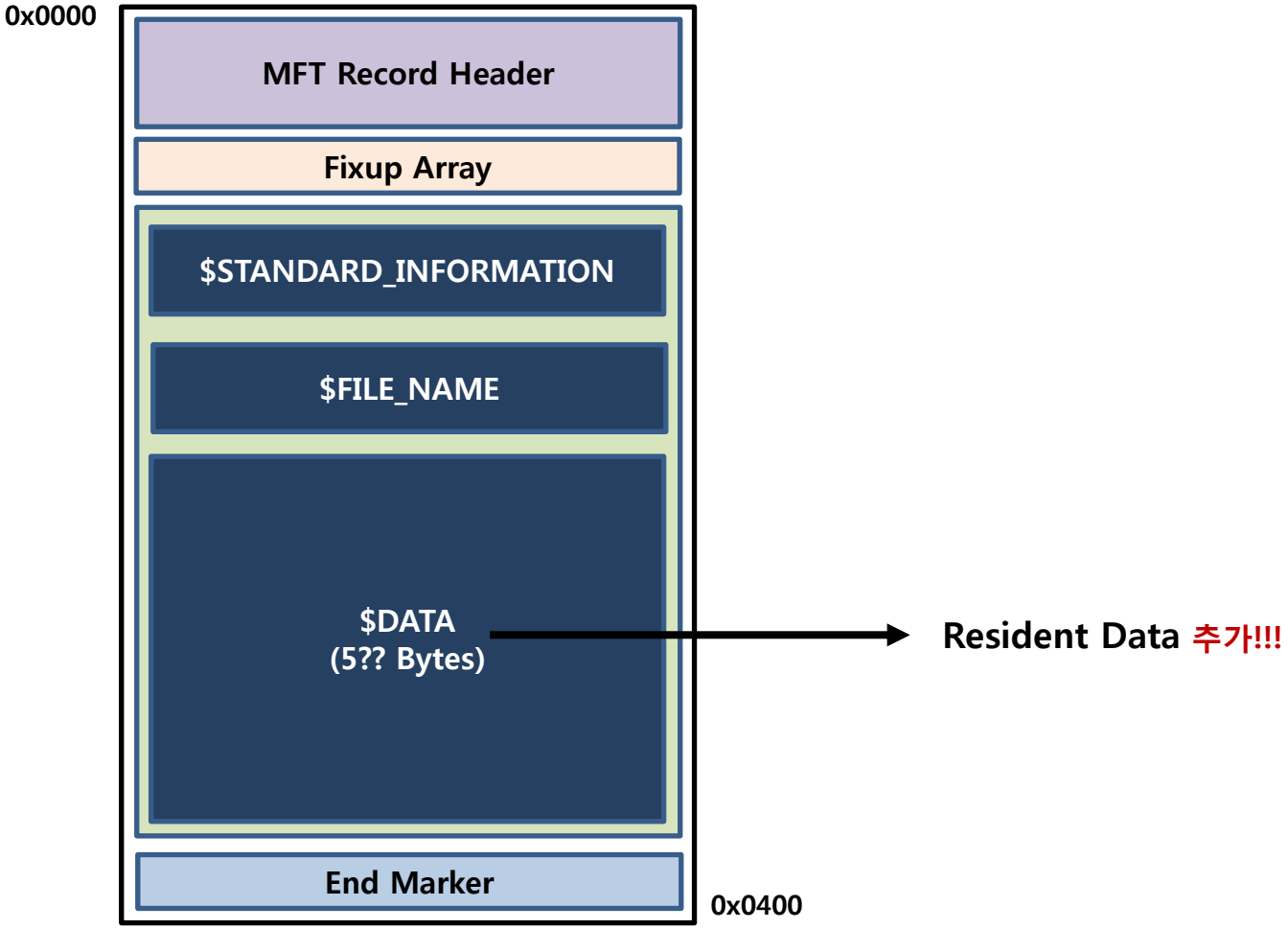
속성 식별값		속성이름	설명
16	0x10	**$STANDARD_INFORMATION**	파일의 생성.접근.수정 시간, 소유자 등의 일반적인 정보
32	0x20	**$ATTRIBUTE_LIST**	추가적인 속성들의 리스트
48	0x30	**$FILE_NAME**	파일 이름(유니코드), 파일의 생성.접근.수정 시간
64	0x40	**$VOLUME_VERSION**	볼륨 정보 (Windows NT 1.2 버전에만 존재)
64	0x40	**$OBJECT_ID**	16바이트의 파일, 디렉터리의 고유 값, 3.0 이상에서만 존재
80	0x50	**$SECURITY_DESCRIPTOR**	파일의 접근 제어와 보안 속성
96	0x60	**$VOLUME_NAME**	볼륨 이름
112	0x70	**$VOLUME_INFORMATION**	파일 시스템의 버전과 다양한 플래그
128	0x80	**$DATA**	파일 내용
144	0x90	**$INDEX_ROOT**	인덱스 트리의 루트 노드
160	0xA0	**$INDEX_ALLOCATION**	인덱스 트리의 루트와 연결된 노드
176	0xB0	**$BITMAP**	$MFT와 인덱스의 할당 정보 관리
192	0xC0	**$SYMBOLIC_LINK**	심볼릭 링크 정보 (Windows 2000+)
192	0xC0	**$REPARSE_POINT**	심볼릭 링크에서 사용하는 reparse point 정보 (Windows 2000+)
208	0xD0	**$EA_INFORMATION**	OS/2 응용 프로그램과 호환성을 위해 사용 (HPFS)
224	0xE0	**$EA**	OS/2 응용 프로그램과 호환성을 위해 사용 (HPFS)
256	0x100	**$LOGGED_UTILITY_STREAM**	암호화된 속성의 정보와 키 값 (Windows 2000+)

- MFT 슬랙
  - MFT 레코드 구조 ➔ 일반 파일



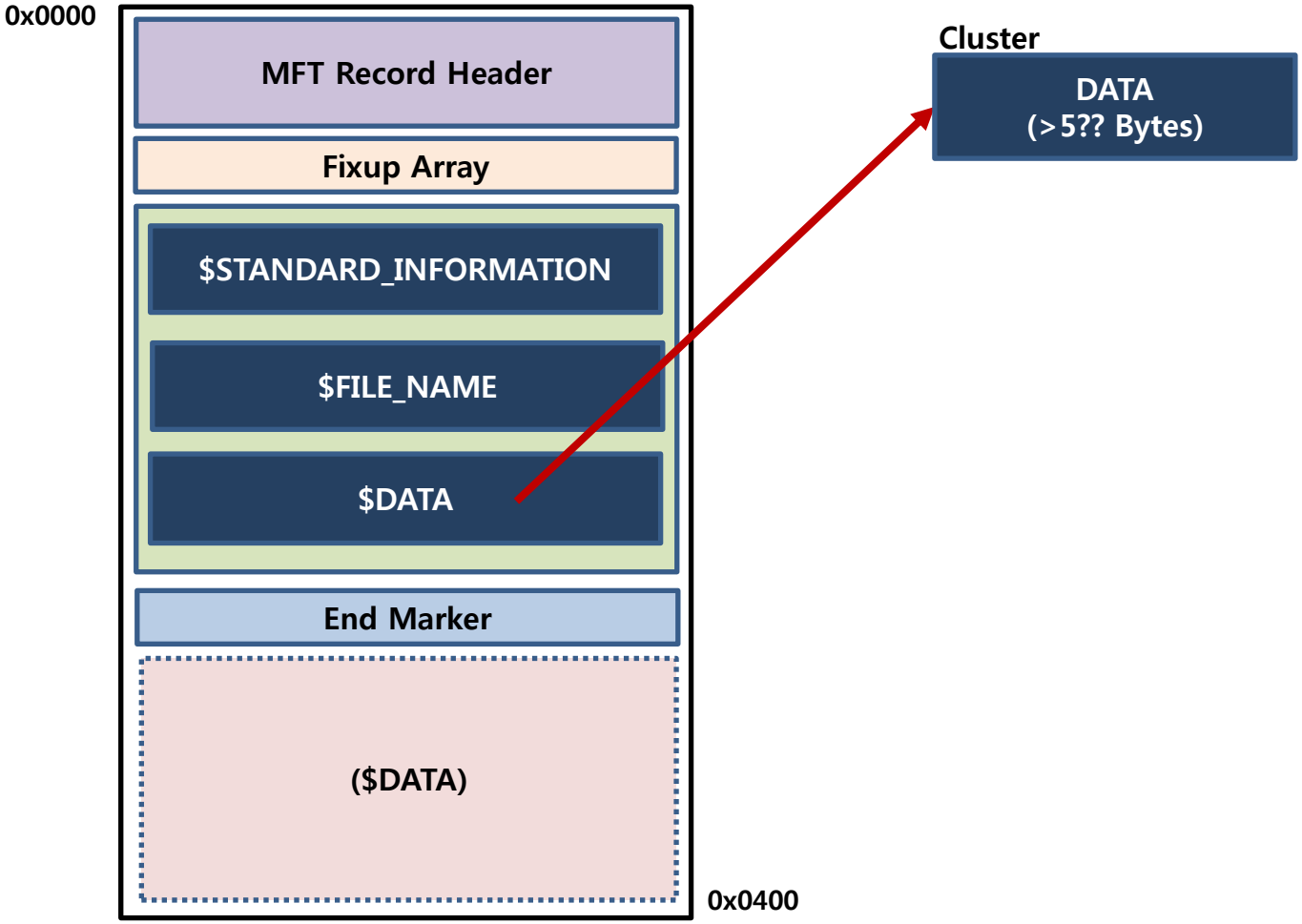
은닉 데이터

- MFT 슬랙
  - MFT 레코드 구조 ➔ 일반 파일

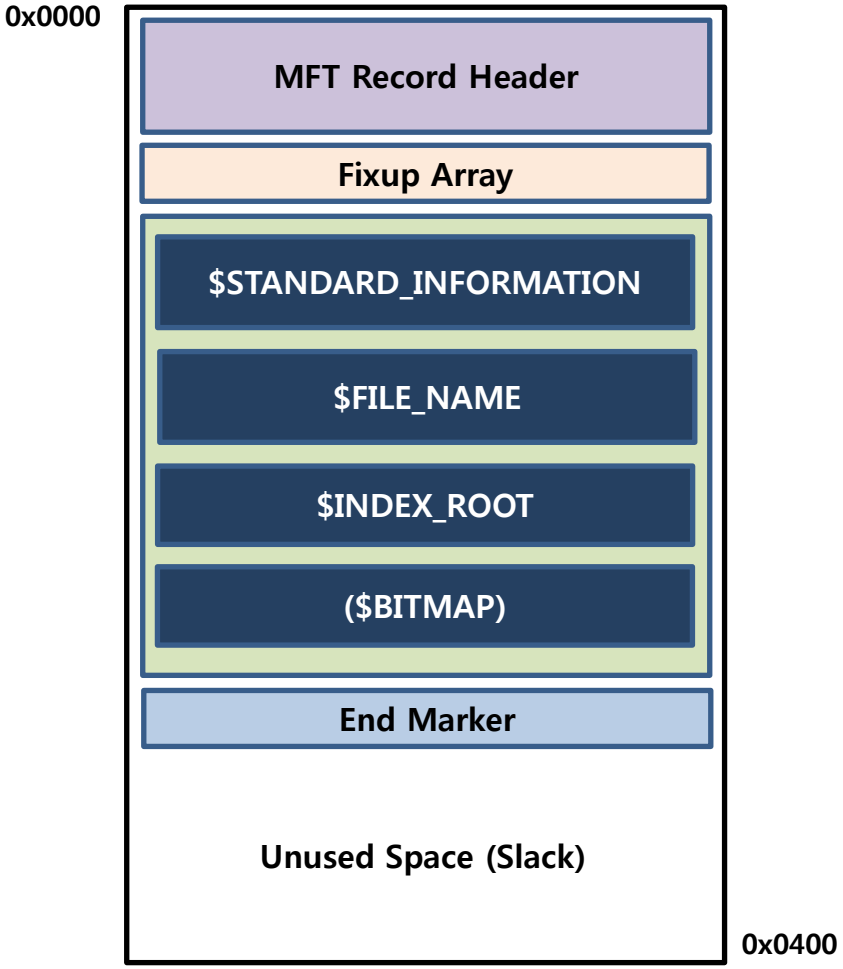


은닉 데이터

- MFT 슬랙
  - MFT 레코드 구조 ➔ 일반 파일

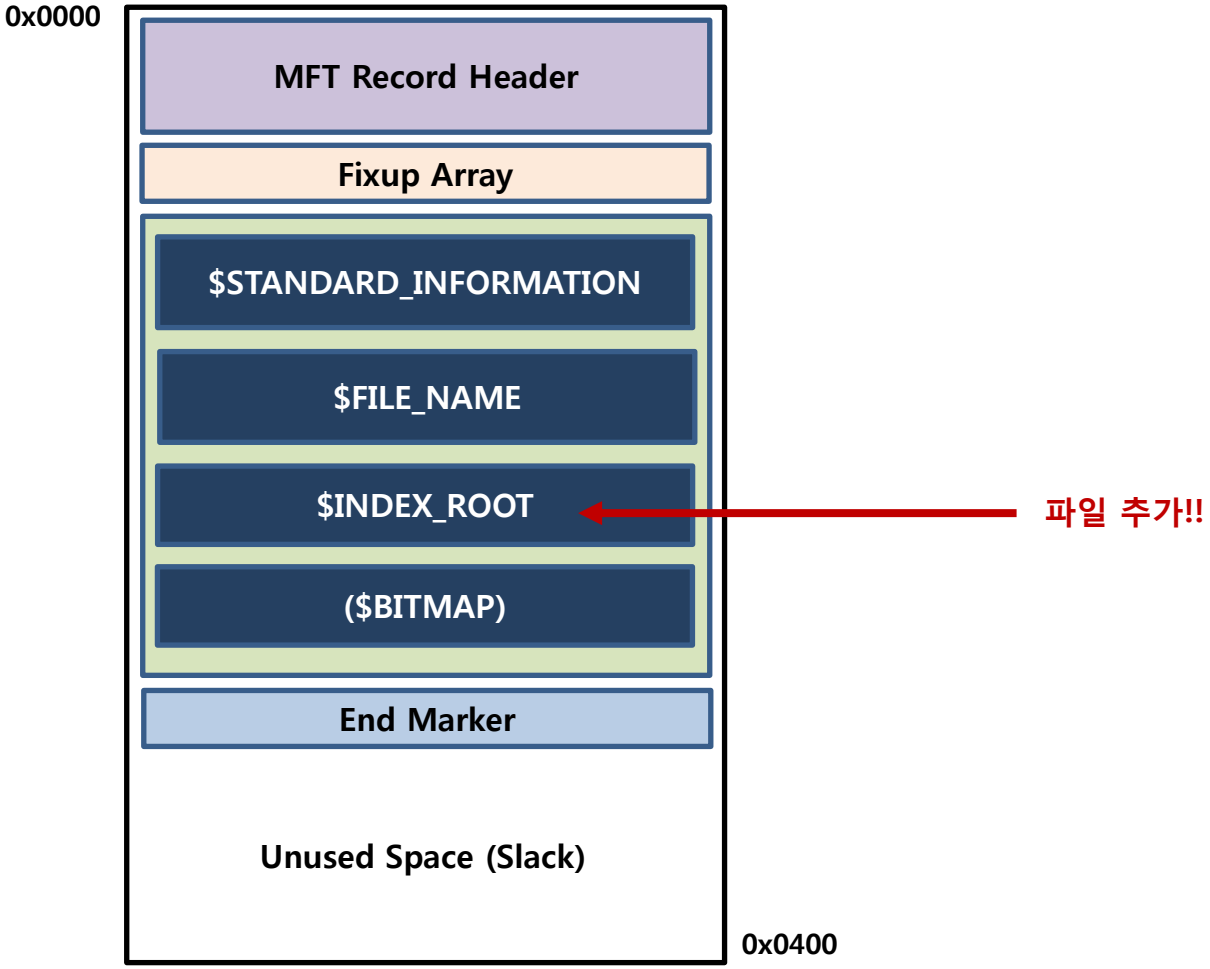


- MFT 슬랙
  - MFT 레코드 구조 ➔ 폴더

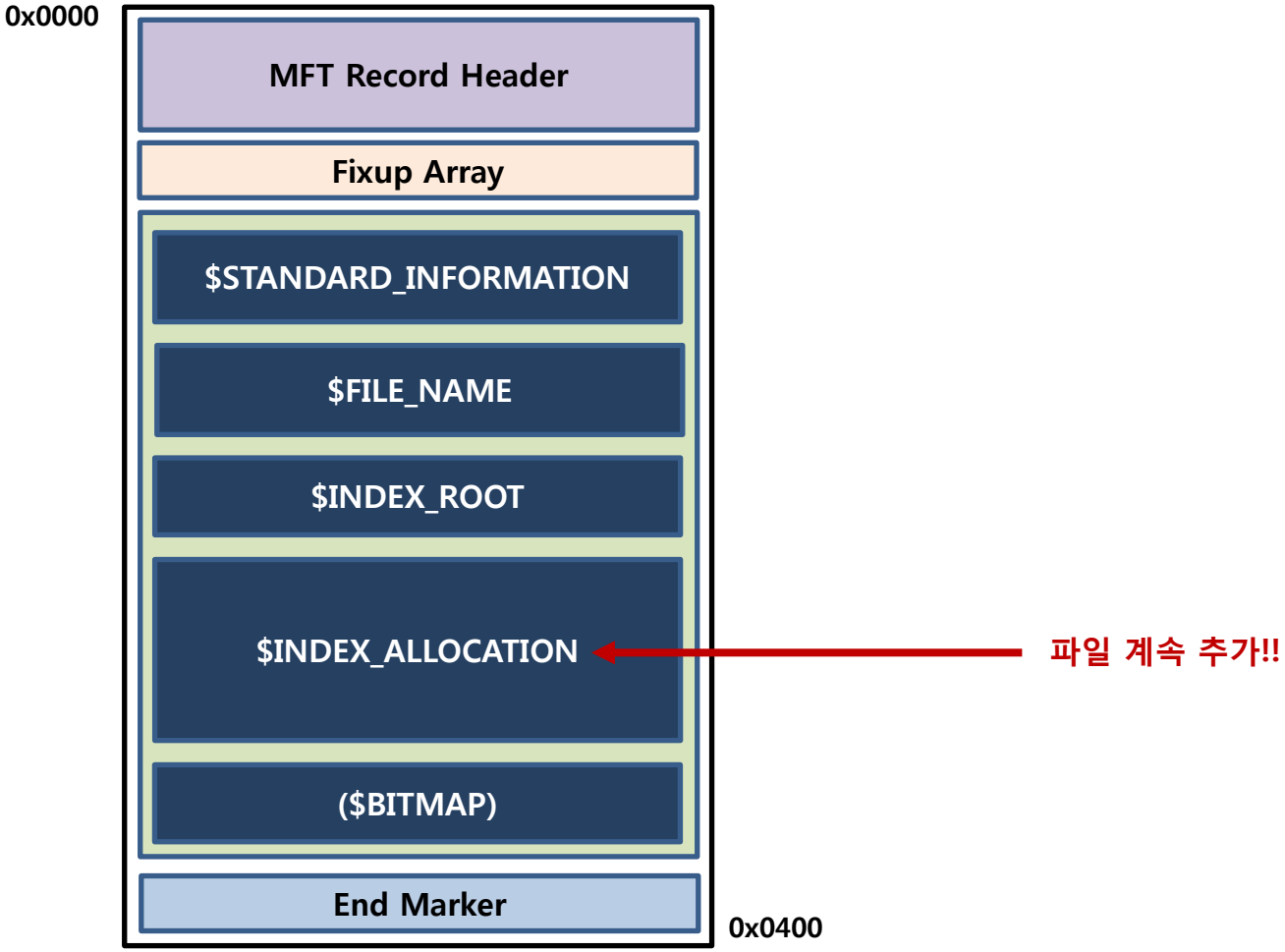


은닉 데이터

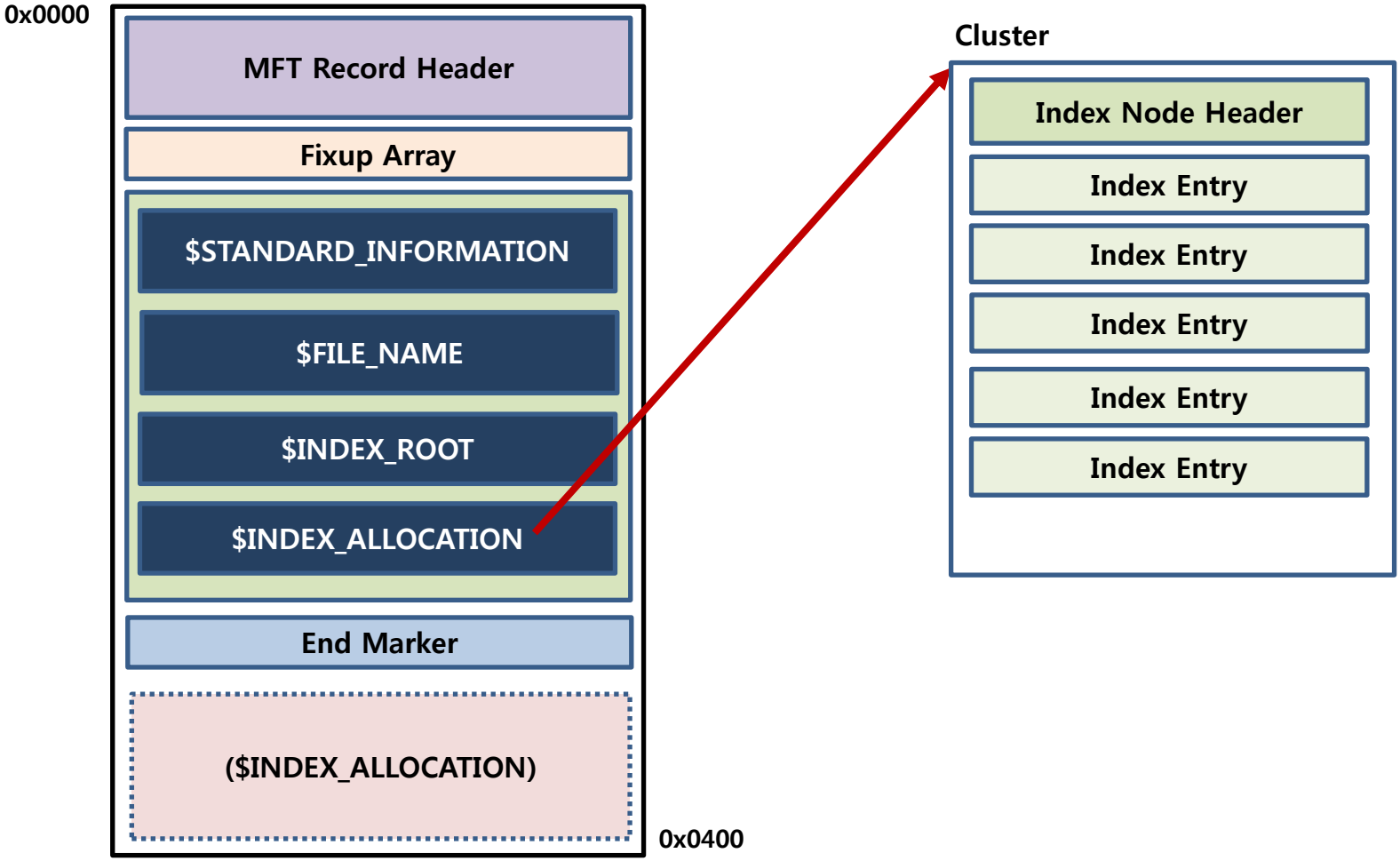
- MFT 슬랙
  - MFT 레코드 구조 ➔ 폴더



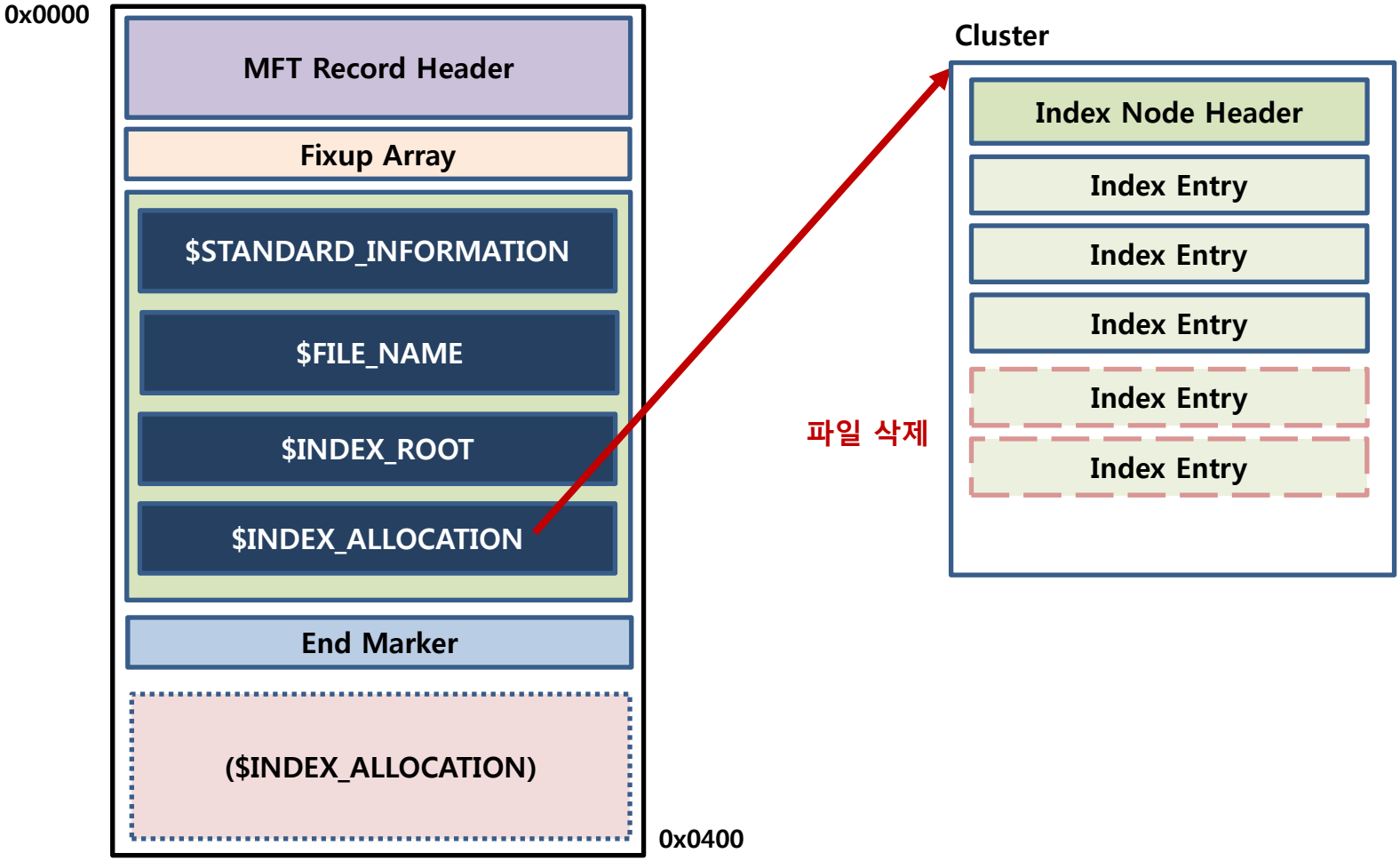
- MFT 슬랙
  - MFT 레코드 구조 ➔ 폴더



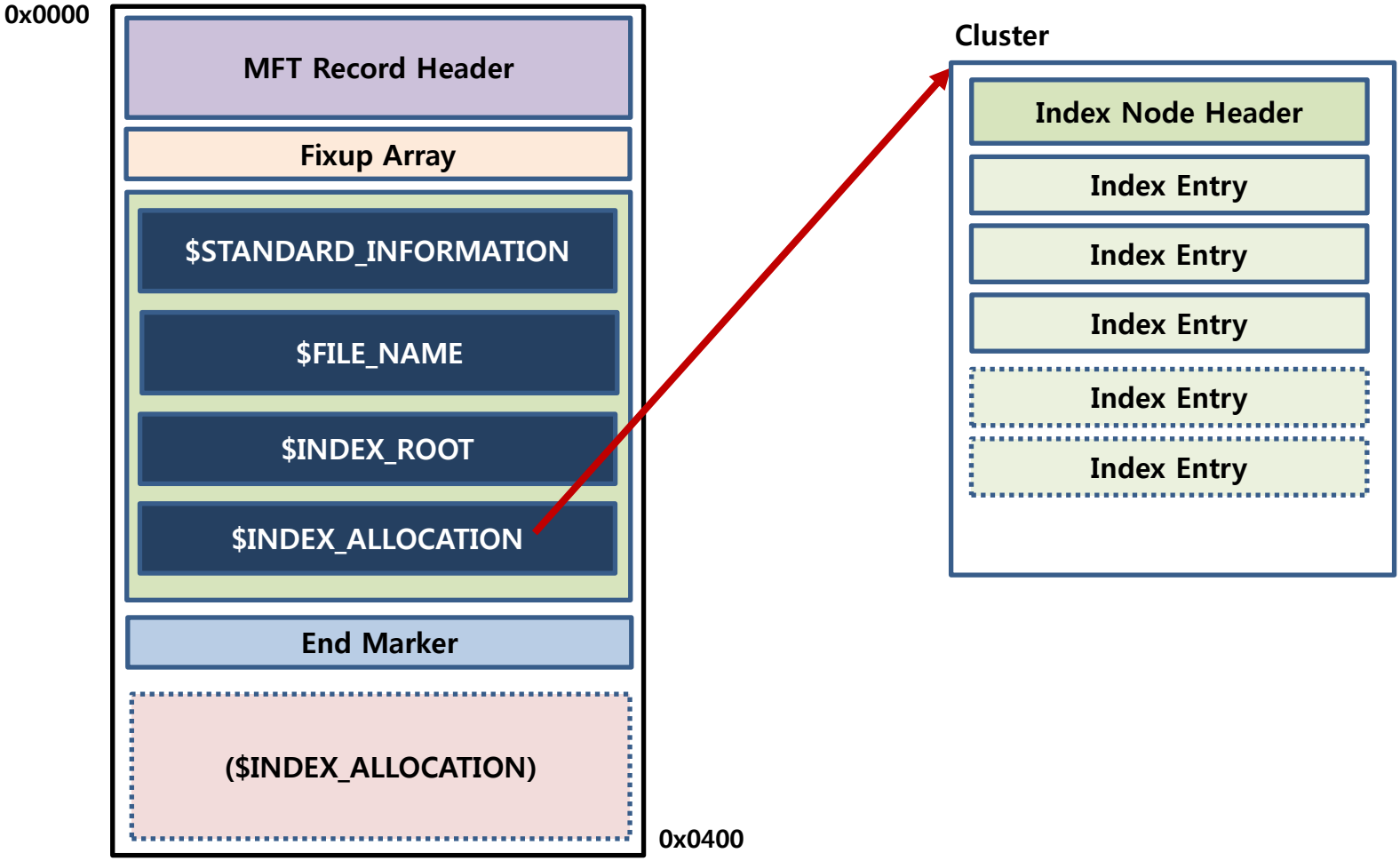
- MFT 슬랙
  - MFT 레코드 구조 ➔ 폴더



- MFT 슬랙
  - MFT 레코드 구조 ➔ 폴더



- MFT 슬랙
  - MFT 레코드 구조 ➔ 폴더



은닉 데이터

- **슬랙 분석 도구**
  - **NTFS INDX Parsing** – williballenthin.com
    - ✓ http://www.williballenthin.com/forensics/indx/index.html
  - **Windows INDX Slack Parser (wisp)** – TZWorks
    - ✓ https://www.tzworks.net/prototype_page.php?proto_id=21

➔ 실습

- **라이브 시스템에서 슬랙 공간 분석하기!!**
  - ✓ MBR 슬랙 확인
  - ✓ 램/드라이브 슬랙 확인
  - ✓ MFT 슬랙 테스트
  - ✓ INDX 슬랙 테스트

은닉 데이터

- **대체 데이터 스트림 (ADS, Alternate Data Stream)**

- MAC 클라이언트를 지원하기 위한 기능으로 $DATA 속성을 2개 이상 가질 수 있음
- ADS 속성을 고유한 이름을 통해 접근 ➔ $DATA 속성의 이름을 가져야 함
- ADS를 데이터 은닉에 활용 ➔ 악성코드에서 활용한 예

- **ADS 활용**
  - ✓ ₩005SummaryInformation
  - ✓ ₩005DocumentSummaryInformation
  - ✓ Zone.Identifier
  - ✓ Thumbs.db.encryptable
  - ✓ Favicon
  - ✓ … …

은닉 데이터

- **대체 데이터 스트림 (ADS, Alternate Data Stream)**
  - **파일에 ADS 생성**

```
$> echo "This is ADS"  >  proneer.txt:ads.txt
$> type c:₩windows₩notepad.exe  >  proneer.txt:ads.exe
```

  - **폴더에 ADS 생성**

```
$> echo "This is attached to directory list"  >  :ads3
$> echo "This is malware" > C:₩Windows₩System32:svchost.exe
```

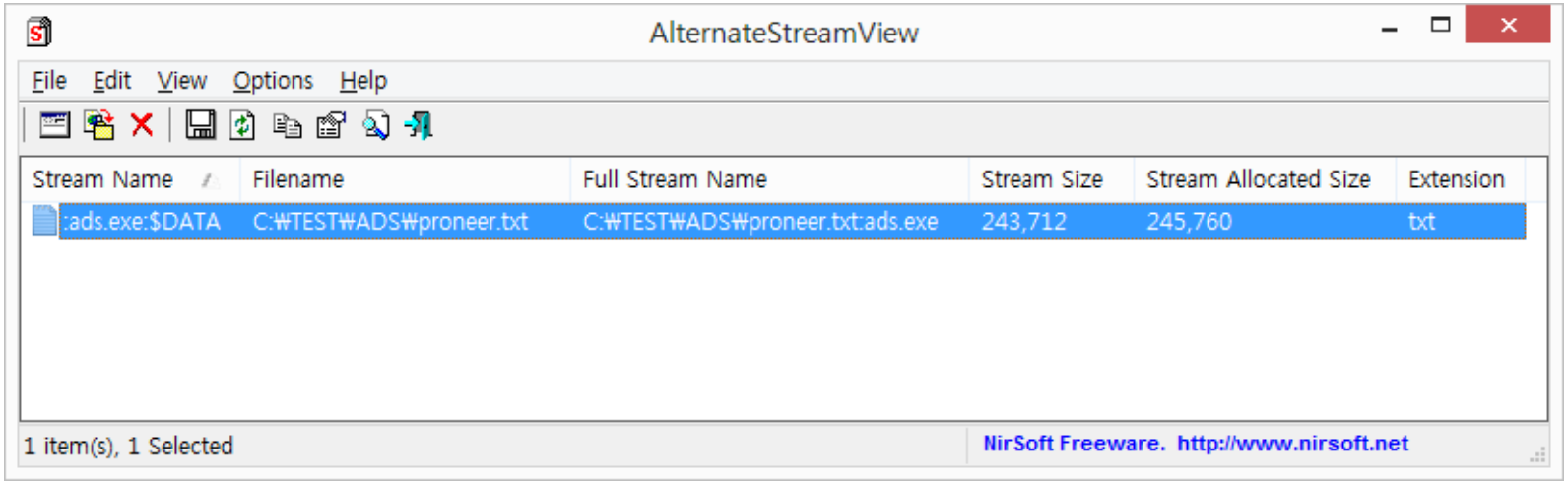
  - **ADS 내용 확인**

```
$> more < proneer.txt:ads1
```

  - **ADS 존재 여부 확인**

```
$> dir  /R  [folder]
```

- **대체 데이터 스트림 (ADS, Alternate Data Stream)**
  - **ADS 삭제**
    - ✓ NTFS 이외의 볼륨으로 복사
    - ✓ 메인스트림 삭제
    - ✓ ADS 관련 도구 이용 (AlternateStreamView, http://www.nirsoft.net/utils/alternate_data_streams.html)



➔ 실습

- **라이브 시스템의 ADS 확인하기!!**
  - ✓ Zone.Identifier 확인하기
  - ✓ Favicon 확인하기

시간 조작

시간 조작

▪ 파일시스템 시간 조작

- 악성코드는 자신을 은닉하기 위해 시스템 파일(ntdll.dll,rundll32.exe 등)과 시간 동기화

- **SetFileTime() API (Kernel32.dll)**
  - ✓ 생성, 수정, 접근 시간만 수정 가능
  - ✓ MFT 레코드 수정 시간을 이용해 쉽게 탐지 가능

- **NtSetInformationFile() API (NTDLL.dll)**
  - ✓ 생성, 수정, 접근, MFT 레코드 수정 시간 모두 변경 가능
  - ✓ $FILE_NAME 속성을 이용해 탐지 가능

- $STANDARD_INFORMATION, $FILE_NAME 속성의 **8개 시간을 모두 수정한 경우**는?

시간 조작

- **파일시스템 시간 조작**
  - 악성코드는 자신을 은닉하기 위해 시스템 파일(ntdll.dll,rundll32.exe 등)과 시간 동기화
  - $SIA($STANDARD_INFORMATION_ATTRIBUTE) – M, A, C, E
  - $FNA($FILE_NAME) – M, A, C, E
  - **M** (Last Modified Time) : 수정 시각
  - **A** (Last Accessed Time) : 접근 시각
  - **C** (Created Time) : 생성 시각
  - **E** (MFT Entry, Record Modified Time) : MFT 레코드 변경 시각

시간 조작

- **파일시스템 시간 조작 탐지**
  - MFT 레코드 수정 시간으로 정렬하여 주요 시스템 파일과 동기화된 의심 파일 확인
  - 주요 시스템 파일의 시간 정보를 기준으로 악성코드 흔적 확인

Drive C:

Windows\System32 — 21 days ago

Name	Ext.	Size	Created	Modified	Accessed	Record update	Attr.	1st sector
PSHED.DLL	DLL	56.1 KB	2009-07-14 08:19:28	2009-07-14 10:45:45	2009-07-14 08:19:28	2012-03-04 10:07:36	A	185792
clfsw32.dll	dll	77.5 KB	2009-07-14 08:19:34	2009-07-14 10:40:15	2009-07-14 08:19:34	2012-03-04 10:06:59	A	139017...
txfw32.dll	dll	11.5 KB	2009-07-14 08:19:38	2009-07-14 10:41:55	2009-07-14 08:19:38	2012-03-04 10:07:44	A	8168856
services.exe	exe	321 KB	2009-07-14 08:19:46	2009-07-14 10:39:37	2009-07-14 08:19:46	2012-03-04 10:07:39	A	226920
csrss.exe	exe	7.5 KB	2009-07-14 08:19:49	2009-07-14 10:39:02	2009-07-14 08:19:49	2012-03-04 10:07:00	A	119760
smss.exe	exe	110 KB	2009-07-14 08:19:50	2009-07-14 10:39:41	2009-07-14 08:19:50	2012-03-04 10:07:41	A	436696
clfs.sys	sys	359 KB	2009-07-14 08:19:59	2009-07-14 10:52:31	2009-07-14 08:19:59	2012-03-04 10:06:59	A	367256
api-ms-win-security-lsal...	dll	3.5 KB	2009-07-14 08:20:47	2009-07-14 10:24:53	2009-07-14 08:20:47	2012-03-04 10:06:55	HA	110636...
api-ms-win-security-sdd...	dll	3.0 KB	2009-07-14 08:20:47	2009-07-14 10:24:53	2009-07-14 08:20:47	2012-03-04 10:06:55	HA	110666...
sechost.dll	dll	111 KB	2009-07-14 08:20:52	2009-07-14 10:41:53	2009-07-14 08:20:52	2012-03-04 10:07:39	A	332464
cryptbase.dll	dll	43.0 KB	2009-07-14 08:20:54	2009-07-14 10:40:24	2009-07-14 08:20:54	2012-03-04 10:07:00	A	94720
profapi.dll	dll	43.0 KB	2009-07-14 08:20:57	2009-07-14 10:41:53	2009-07-14 08:20:57	2012-03-04 10:07:36	A	134208
netevent.dll	dll	18.5 KB	2009-07-14 08:20:58	2009-07-14 10:30:47	2009-07-14 08:20:58	2012-03-04 10:07:19	A	144538...
nsi.dll	dll	13.5 KB	2009-07-14 08:21:05	2009-07-14 10:41:53	2009-07-14 08:21:05	2012-03-04 10:07:33	A	103296
RpcEpMap.dll	dll	65.5 KB	2009-07-14 08:21:05	2009-07-14 10:41:53	2009-07-14 08:21:05	2012-03-04 10:07:37	A	133952
winnsi.dll	dll	25.5 KB	2009-07-14 08:21:08	2009-07-14 10:41:56	2009-07-14 08:21:08	2012-03-04 10:07:48	A	176744
dhcpcsvc6.dll	dll	53.0 KB	2009-07-14 08:21:09	2009-07-14 10:40:28	2009-07-14 08:21:09	2012-03-08 08:32:33	A	192704
dhcpcsvc.dll	dll	85.0 KB	2009-07-14 08:21:09	2009-07-14 10:40:28	2009-07-14 08:21:09	2012-03-08 08:32:33	A	151104
dhcpcore6.dll	dll	219 KB	2009-07-14 08:21:13	2009-07-14 10:40:28	2009-07-14 08:21:13	2012-03-08 08:32:33	A	447512
IPHLPAPI.DLL	DLL	143 KB	2009-07-14 08:21:13	2009-07-14 10:41:10	2009-07-14 08:21:13	2012-03-04 10:07:11	A	276512
dhcpcore.dll	dll	307 KB	2009-07-14 08:21:15	2009-07-14 10:40:28	2009-07-14 08:21:15	2012-03-04 10:07:02	A	446896
api-ms-win-core-ums-l1...	dll	3.0 KB	2009-07-14 08:21:15	2009-07-14 10:24:53	2009-07-14 08:21:15	2012-03-04 10:06:55	HA	110257...
shimeng.dll	dll	6.5 KB	2009-07-14 08:21:19	2009-07-14 10:41:54	2009-07-14 08:21:19	2012-03-08 08:32:37	A	8033728

시간 조작

- **파일시스템 시간 조작 도구**
  - **setMACE**
    - ✓ http://reboot.pro/files/file/91-setmace/
  - **TimeStomp**
    - ✓ http://www.offensive-security.com/metasploit-unleashed/Timestomp

자동 실행 목록

자동 실행 목록

- **자동 실행 (Autoruns)**
  - 운영체제 혹은 응용프로그램 시작과 함께 자동 실행되는 항목
  - 악성코드는 지속적인 실행을 위해 자동 실행 항목 이용

  - **자동 실행 항목**
    - ✓ 파일시스템
    - ✓ 레지스트리

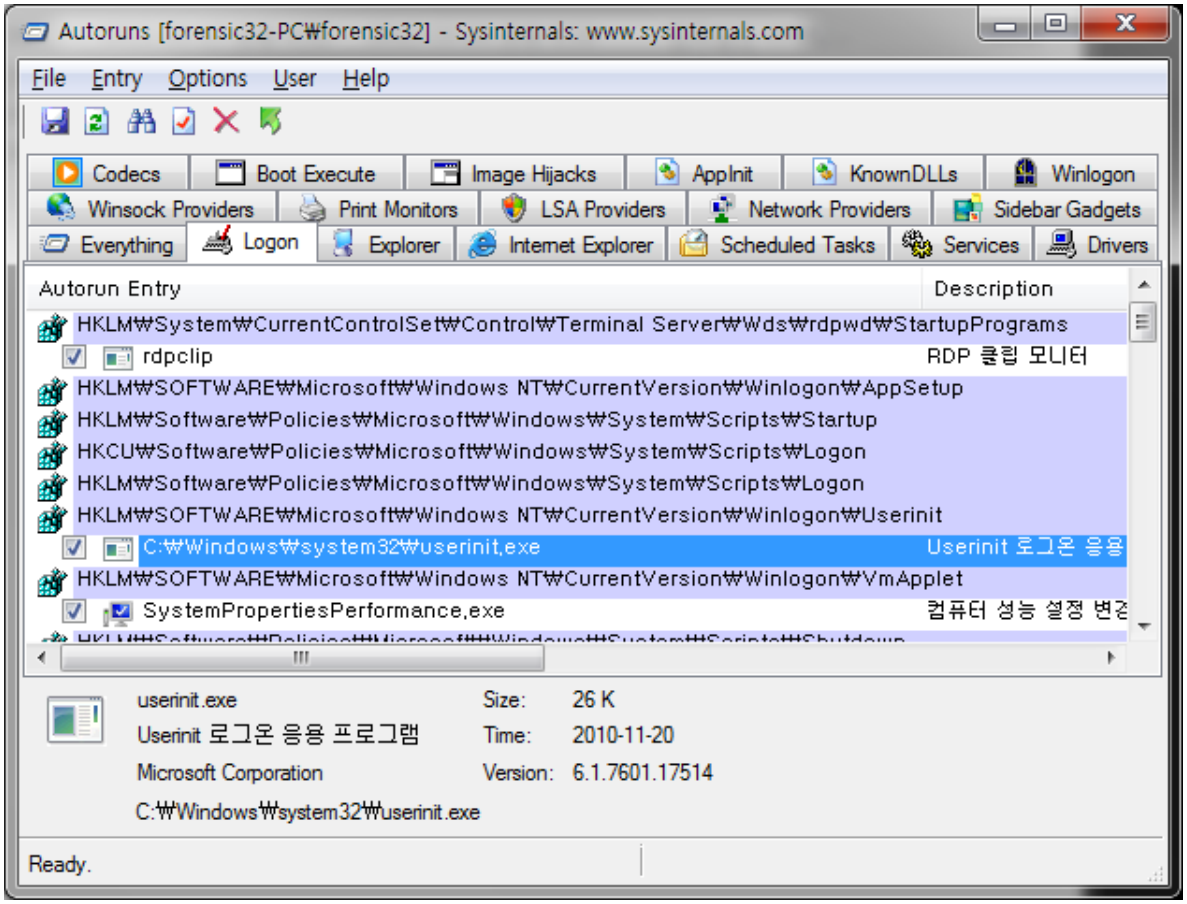
  - **관련 도구**
    - ✓ **Autoruns** – 2013년 8월 현재 189개 자동실행 항목 점검

자동 실행 목록

- **자동 실행 분석 도구**
  - **Autoruns, Autorunsc** – Windows Sysinternals
    - ✓ http://technet.microsoft.com/ko-KR/sysinternals/bb963902.aspx
  - **REGA** – 4n6Tech
    - ✓ http://4n6tech.com/pro_kr/info/info.php?pn=1&sn=1&dn=3
  - **RegRipper ASEPs Plugin** – Corey Harrell
    - ✓ https://code.google.com/p/regripper/wiki/ASEPs

자동 실행 목록

- **자동 실행 분석 도구**
  - **Autoruns 점검 항목**
    - ✓ Logon
    - ✓ Explorer
    - ✓ Internet Explorer
    - ✓ Services
    - ✓ Scheduled Tasks
    - ✓ AppInit DLLs
    - ✓ Boot Execute
    - ✓ Image Hijacks
    - ✓ Known DLLs
    - ✓ Winlogon Notifications
    - ✓ Winsock Providers
    - ✓ LSA Providers



작업 스케줄러

작업 스케줄러

작업 스케줄러 소개

- 특정 이벤트가 발생할 때 또는 특정 시간에 자동화된 작업을 예약

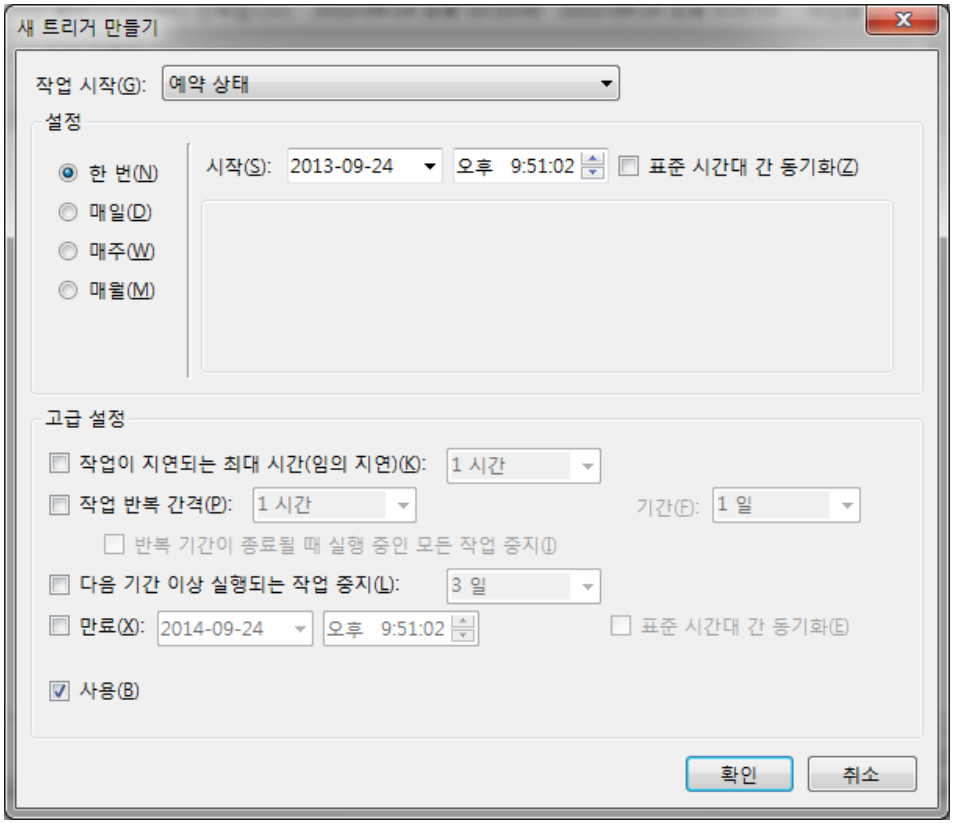
- **두 가지 주요 개념**
  - ✓ **트리거**
    - 작업이 실행되는 조건
  - ✓ **동작**
    - 작업이 실행될 때 수행하는 동작

작업 스케줄러

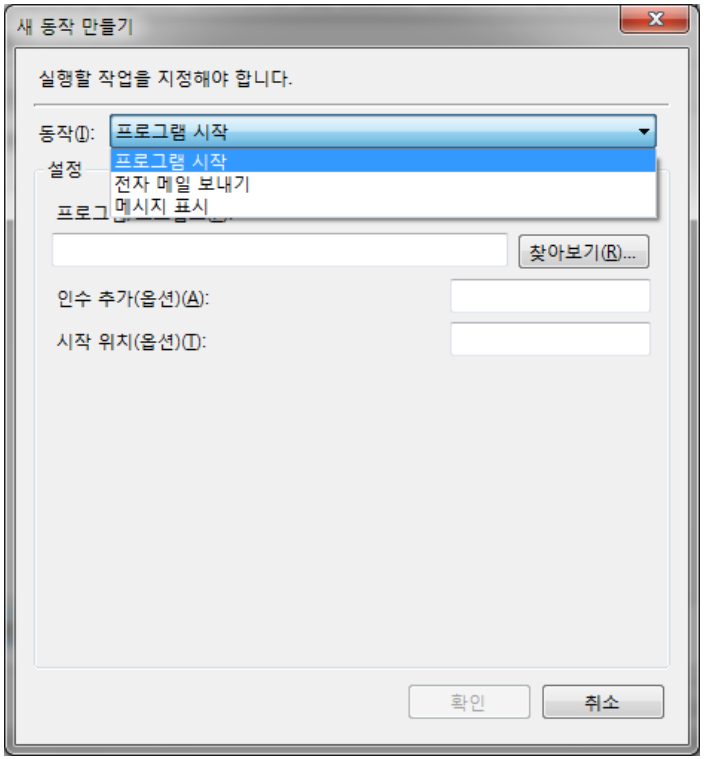
- **트리거 설정**
  - **트리거 조건**
    - ✓ **예약 상태** – 한번, 매일, 매주, 매월 등 일정에 따라
    - ✓ **로그온할** 때 – 사용자가 컴퓨터에 로그온할 때
    - ✓ **시작할 때** – 컴퓨터가 시작될 때
    - ✓ **유휴 상태** – 컴퓨터가 유휴 상태로 전환된 후
    - ✓ **이벤트 상태** – 특정 이벤트가 발생할 때
    - ✓ **작업 만들기/수정하기에서** – 작업이 만들어지는 즉시 또는 수정될 때
    - ✓ **터미널 서버 세션 연결** – 로컬 컴퓨터나 원격 데스크톱 연결에서 사용자 세션이 연결될 때
    - ✓ **터미널 서버 세션 연결 해제** – 로컬 컴퓨터/원격 데스크톱 연결에서 사용자 세션이 끊어질 때
    - ✓ **워크스테이션 잠금** – 컴퓨터가 잠길 때
    - ✓ **워크스테이션 잠금 해제** – 컴퓨터 잠금이 해제될 때

작업 스케줄러

- **트리거 설정**
  - **트리거 고급 설정**
    - ✓ 작업 지연 시간
    - ✓ 작업 반복 간격
    - ✓ 다음 기간 이상 실행되는 작업 중지
    - ✓ 활성화
    - ✓ 만료
    - ✓ 사용



- **동작 설정**
  - **동작 상태**
    - ✓ **프로그램 시작** – 프로그램이나 스크립트를 시작
    - ✓ **전자메일 보내기** – 전자메일을 보냄
    - ✓ **메시지 표시** – 지정한 메시지 및 제목과 함께 메시지 상자 표시



작업 스케줄러

- **작업 스케줄러 경로**
  - **%SystemRoot%₩Tasks**
    - ✓ AT 명령으로 생성한 작업 위치
    - ✓ 바이너리 형식
  - **%SystemRoot%₩system32₩Tasks**
    - ✓ Schtasks, Taskschd.msc로 생성한 작업 위치
    - ✓ XML 형식

작업 스케줄러

- **작업 스케줄러 관련 도구**
  - **작업 스케줄러 생성/관리 도구**
    - ✓ **At** – Internal Windows Command
    - ✓ **Schtasks** – Internal Windows Command
    - ✓ **Taskschd.msc**
      - [제어판] ➔ [관리 도구] ➔ [작업 스케줄러]
  - **Job 파일 분석 도구**
    - ✓ **Jobparser** – Gleeda
      - https://raw.github.com/gleeda/misc-scripts/master/misc_python/jobparser.py

작업 스케줄러

➔ 실습

- **라이브 시스템에서 작업 스케줄러 생성/분석하기!!**
  - ✓ AT 명령으로 작업 생성하기
  - ✓ SCHTASKS 명령으로 작업 생성하기
  - ✓ 생성된 작업 분석하기

질문 및 답변