

EnCase Fundamental



JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

1. 기본 정보(Basics)
2. 케이스 정보 (EnCase Case)
3. 증거 추가 (Add Evidence)
4. 사용 환경 (Environment)
5. 증거 획득 (Acquiring Evidence)
6. 증거 파일 포맷 (Evidence File Format)
7. 증거 파일 검증 (Evidence File Verification)

기본 정보

Security is a people problem...

동글키(Dongle Key)

- EnCase v6.x : HASP



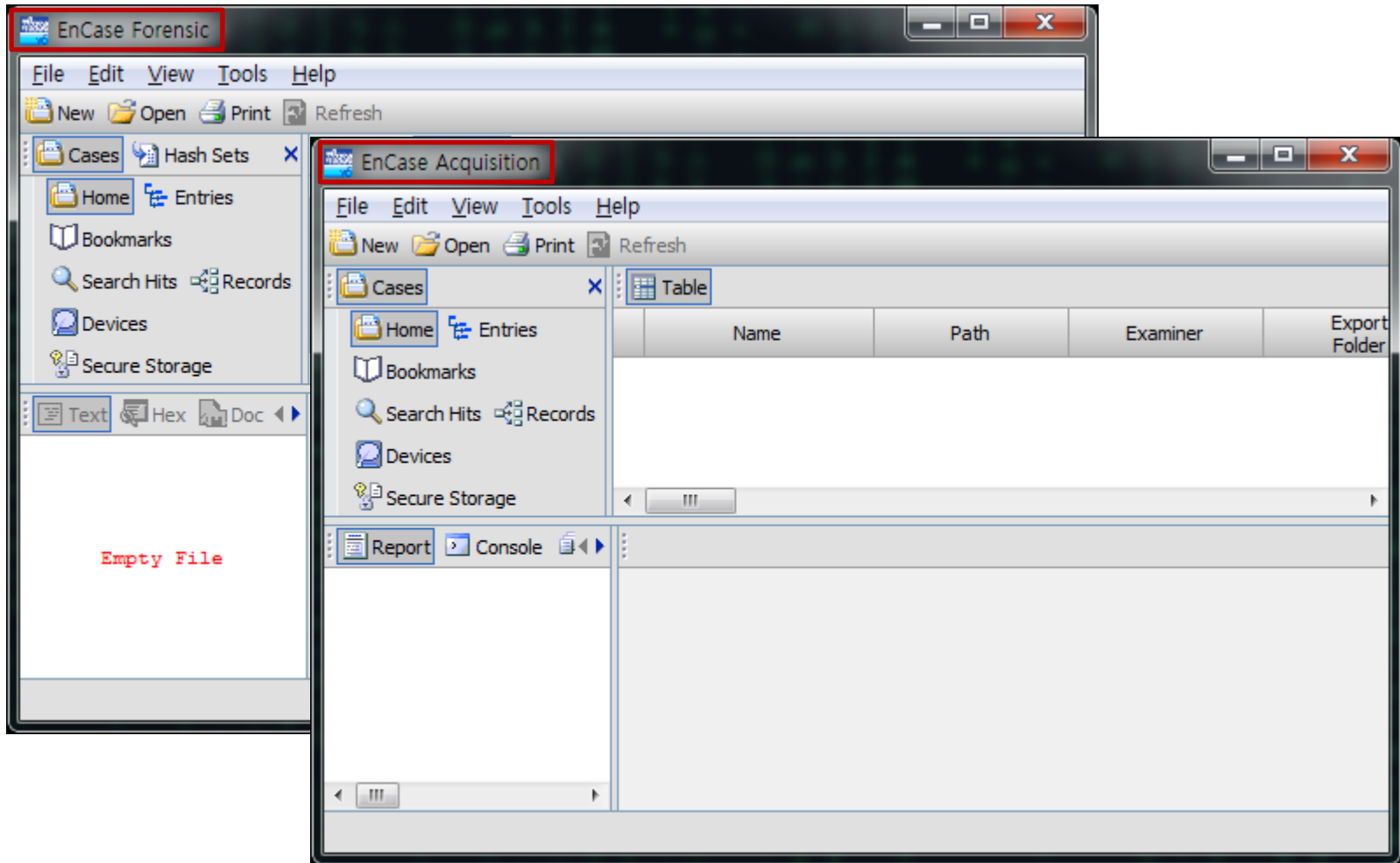
- EnCase v7.x, Portable : CODEMETER



dongle키(Dongle Key)

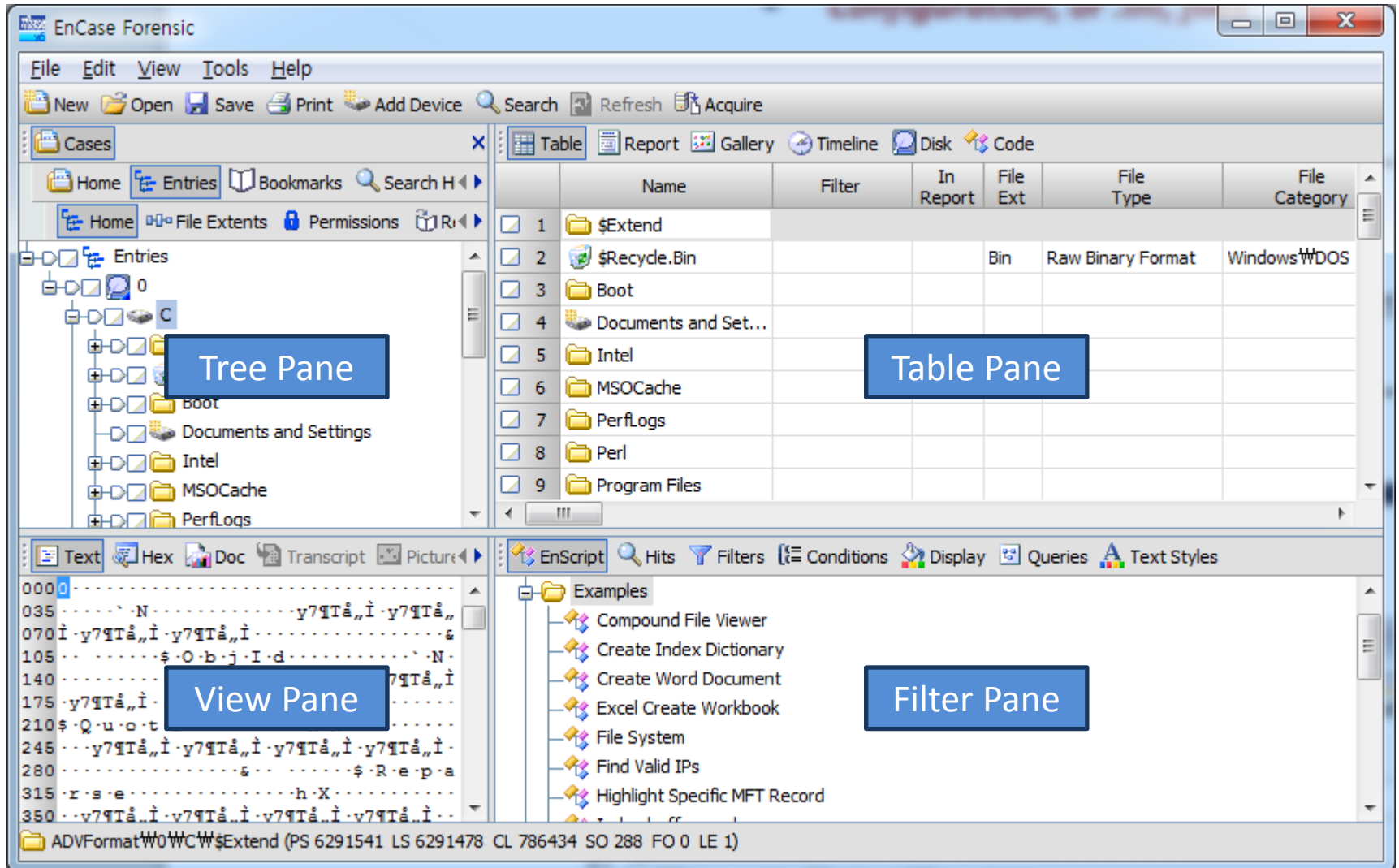
- **EnCase v7.x dongle키로 v6.x 사용**
 - CODEMETER dongle키 인식을 위해 Runtime-Kit 설치
 - <http://www.codemeter.de/us/service/downloads.html>

동글키(Dongle Key)



기본 정보

주요 창



케이스 정보

Security is a people problem...

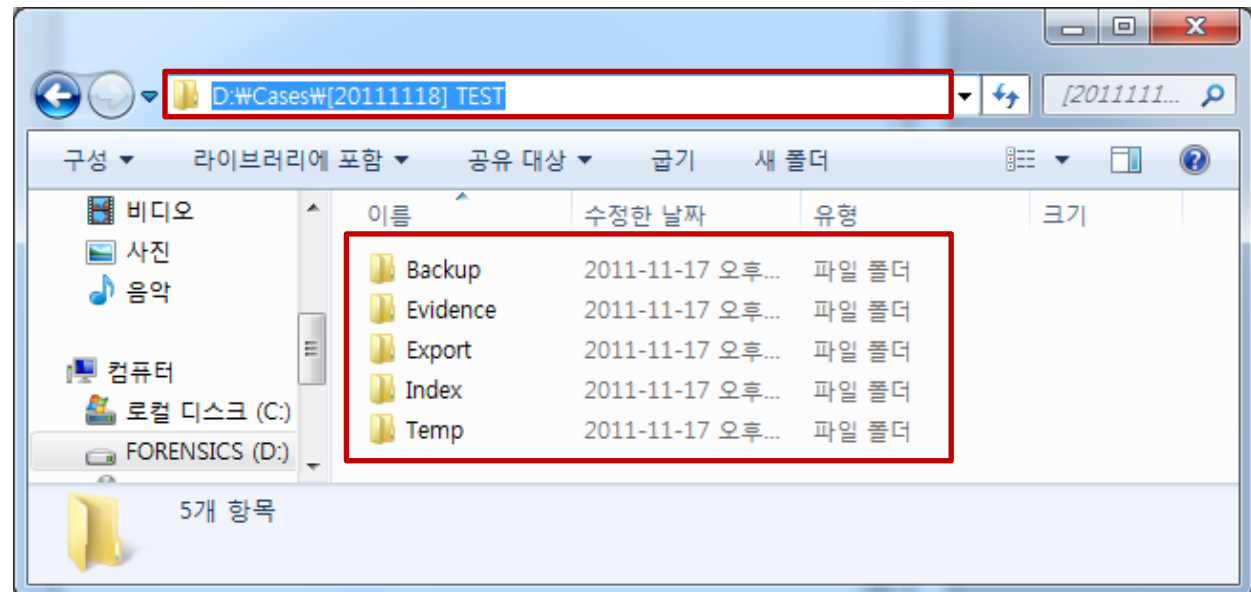
케이스 정보

케이스 주요 폴더 생성

- 케이스 폴더 생성
 - 예) [날짜] 사건이름_사건번호

- 케이스 하위 폴더 생성

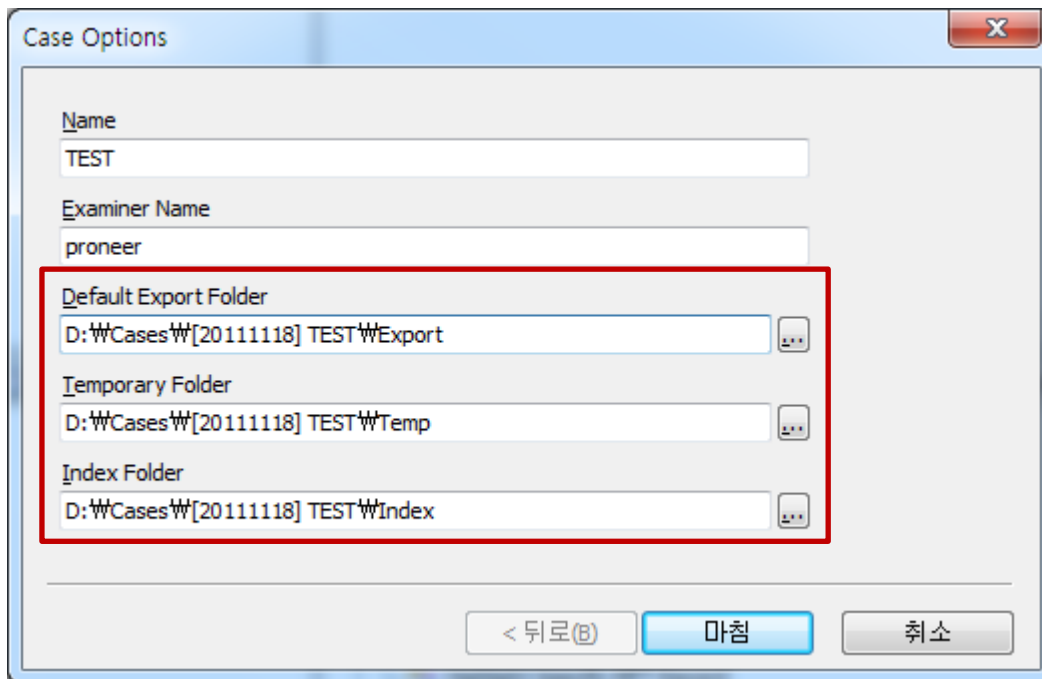
- Backup
- Evidence
- Export
- Index
- Temp



케이스 정보

케이스 생성 (File → New)

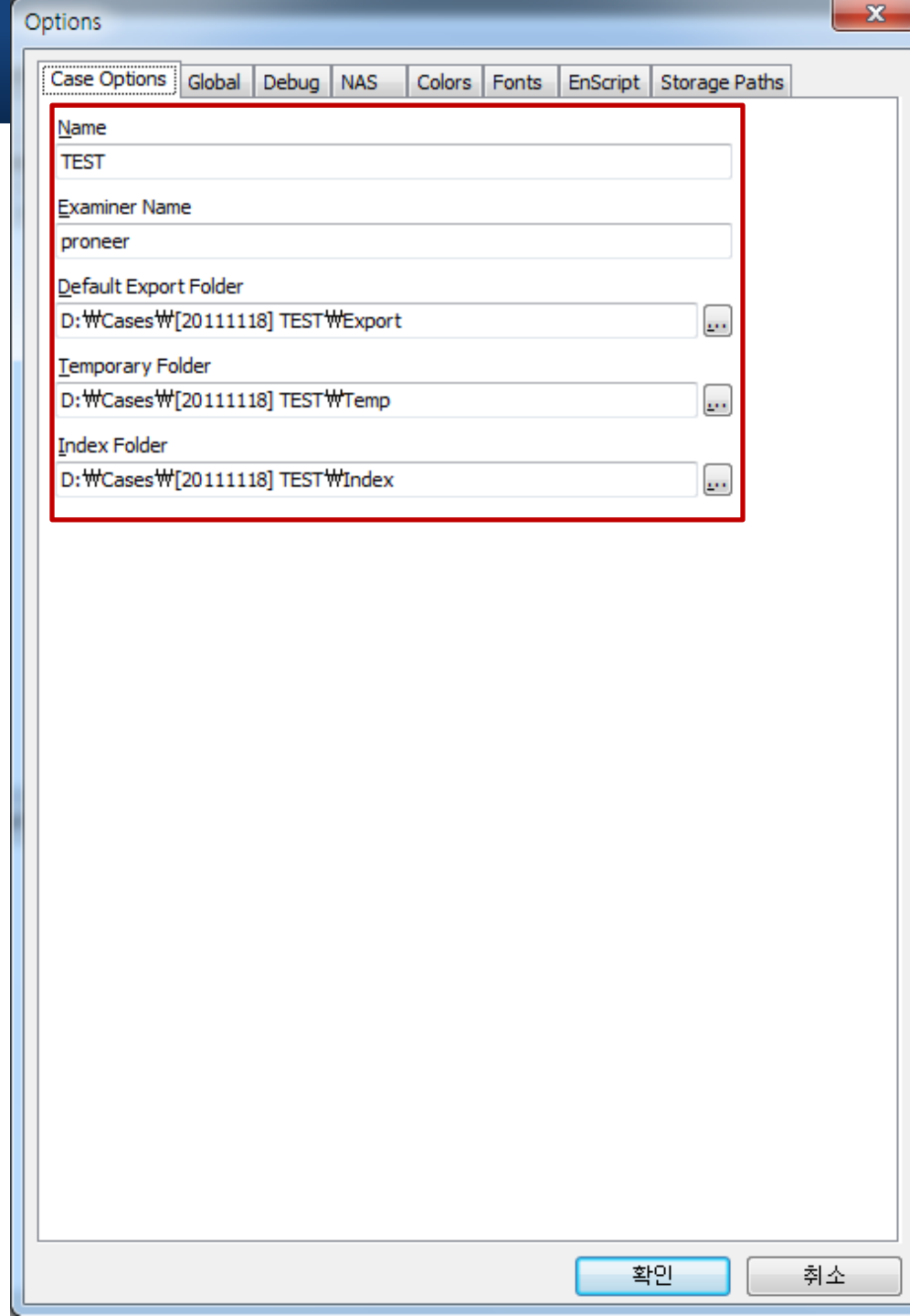
- 미리 생성한 케이스 폴더의 하위 폴더 지정
- 생성 후 케이스 파일을 케이스 폴더에 저장 (File→Save, Ctrl+S)



케이스 정보

케이스 옵션 (Tools → Options)

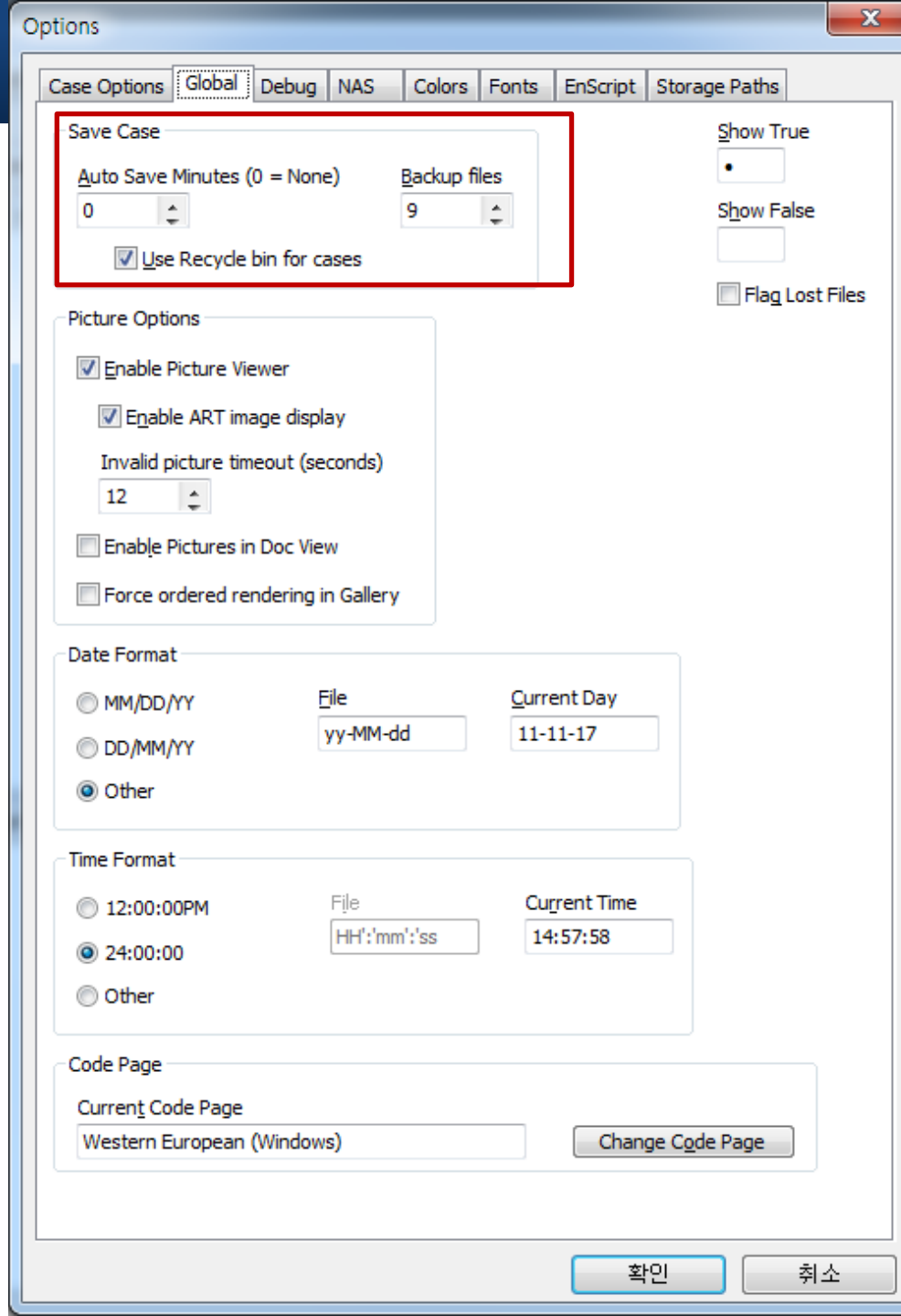
- **Case Options 탭**
 - 케이스 기본 정보
 - **Export Folder**
 - Copy/UnErase시 기본 저장 폴더
 - EnScript 출력 폴더
 - **Temporary Folder**
 - 외부 뷰어 사용 시 파일 임시 저장
 - **Index Folder**
 - 키워드 검색 시 인덱싱 정보 저장



케이스 정보

케이스 옵션 (Tools → Options)

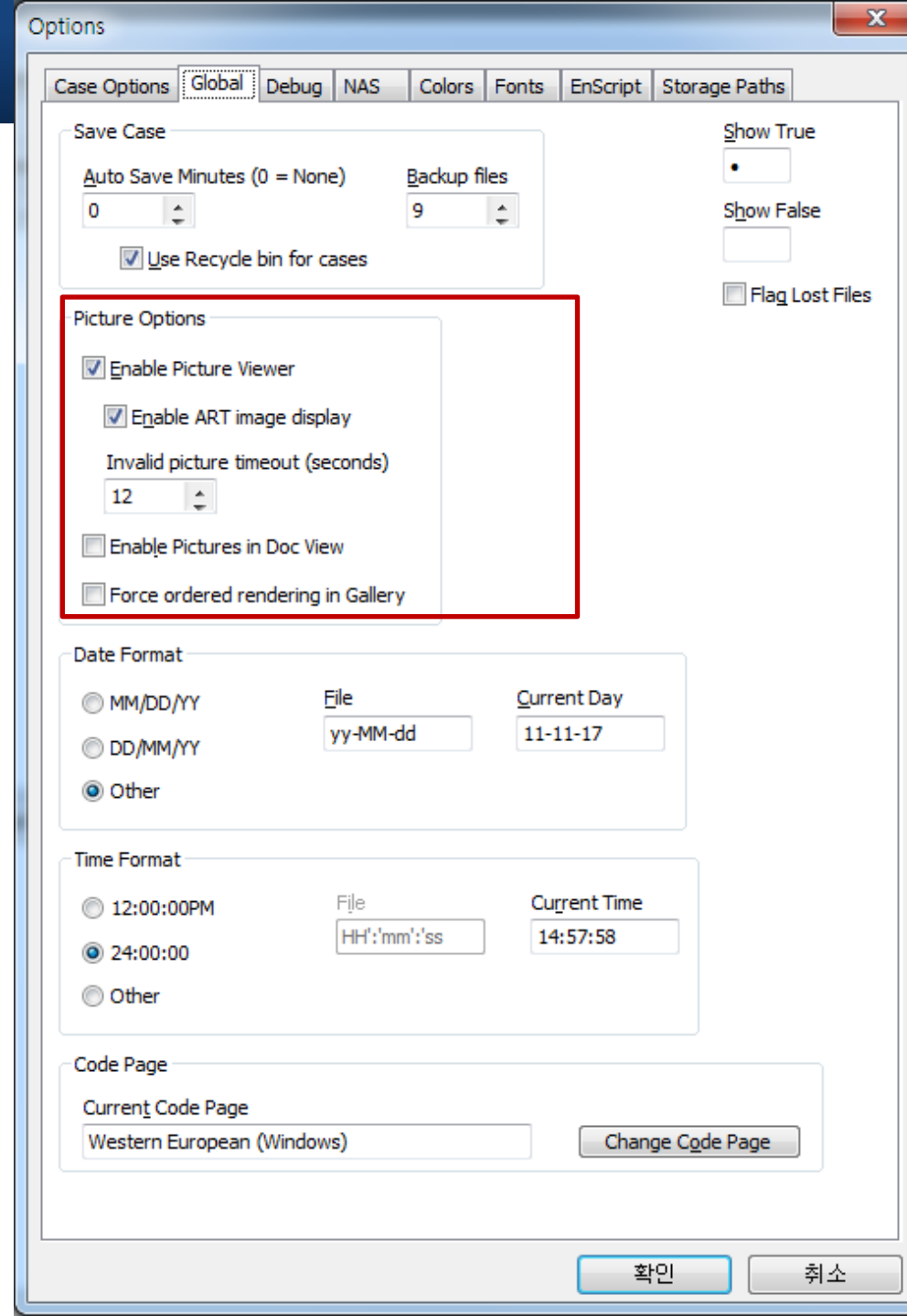
- **Global 탭 → Save Case**
 - **Auto Save Minutes**
 - 자동 백업 시간 (0일 경우 백업 X)
 - **Backup files**
 - 유지할 백업 파일 수
 - 낮은 숫자가 가장 최근 백업
- **Use Recycle bin for cases**
 - 케이스 파일 삭제 시 휴지통 이동 여부



케이스 정보

케이스 옵션 (Tools → Options)

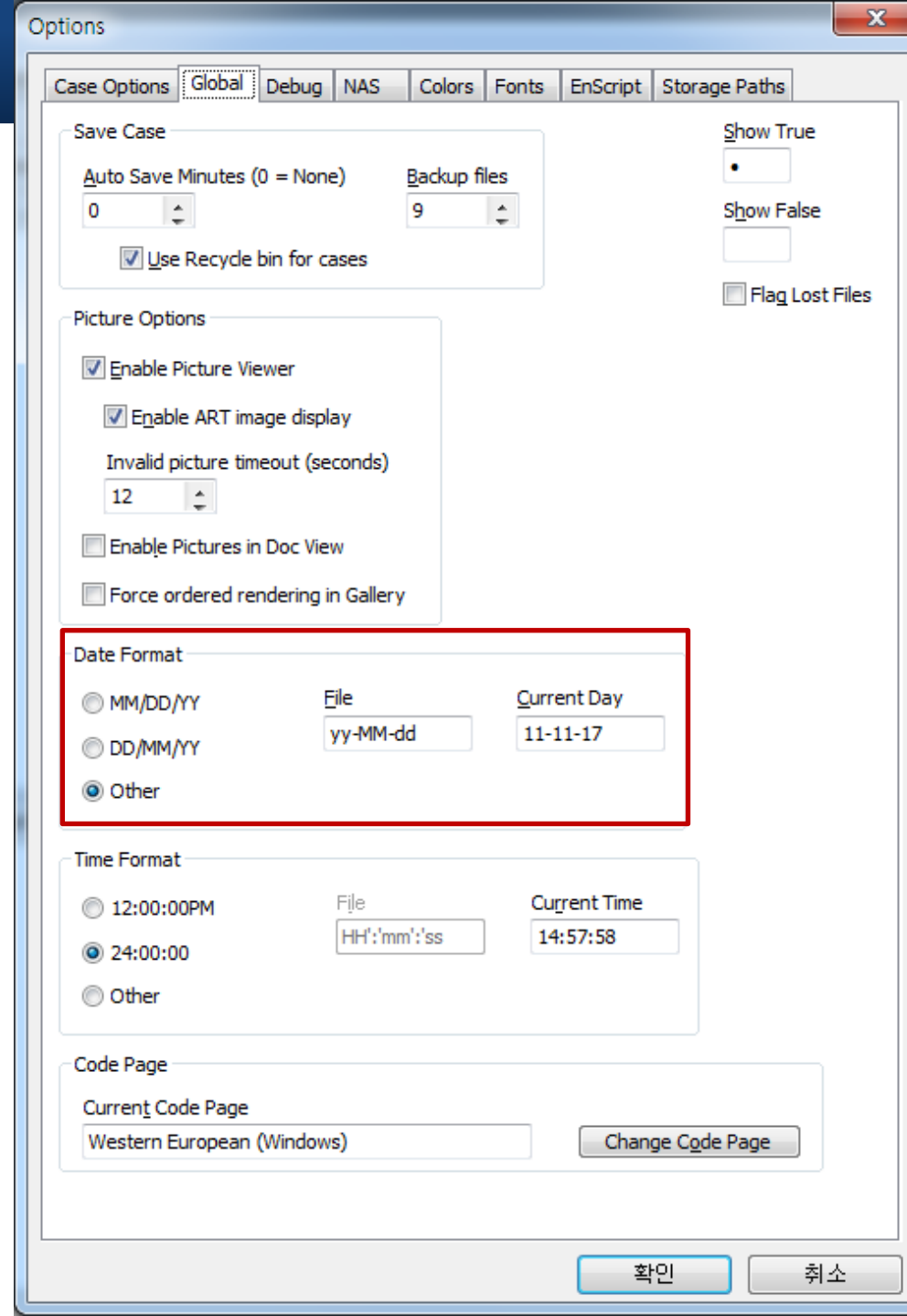
- **Global 탭 → Picture Options**
 - **Enable Picture Viewer**
 - 그래픽 뷰어 활성화 여부
 - **Enable ART image display**
 - America Online(AOL) 파일 지원여부
 - **Invalid picture timeout**
 - 잘못된 파일일 경우 타임아웃 시간
 - **Enable Pictures in Doc View**
 - Doc 탭에서 그래픽 표시 여부
 - **Force ordered rendering in Gallery**
 - Gallery 탭에서 파일 순서대로 렌더링



케이스 정보

케이스 옵션 (Tools → Options)

- Global 탭 → Date Format
 - File, Current Day
 - 사용자 정의 날짜 형식
 - MM/DD/yy (기본)
 - yy-MM-dd (권장)



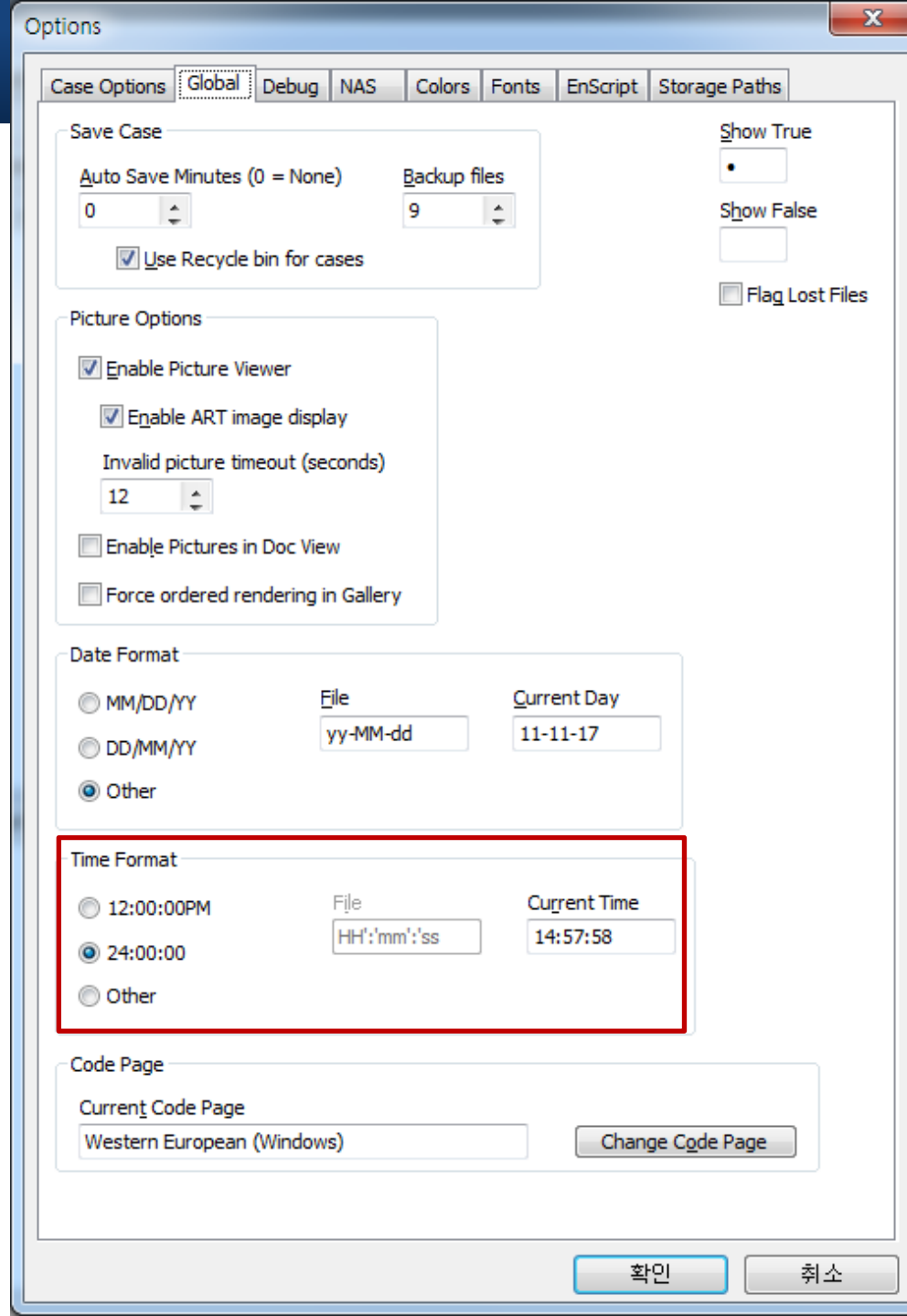
케이스 정보

케이스 옵션 (Tools → Options)

- Global 탭 → Time Format

- Current Time

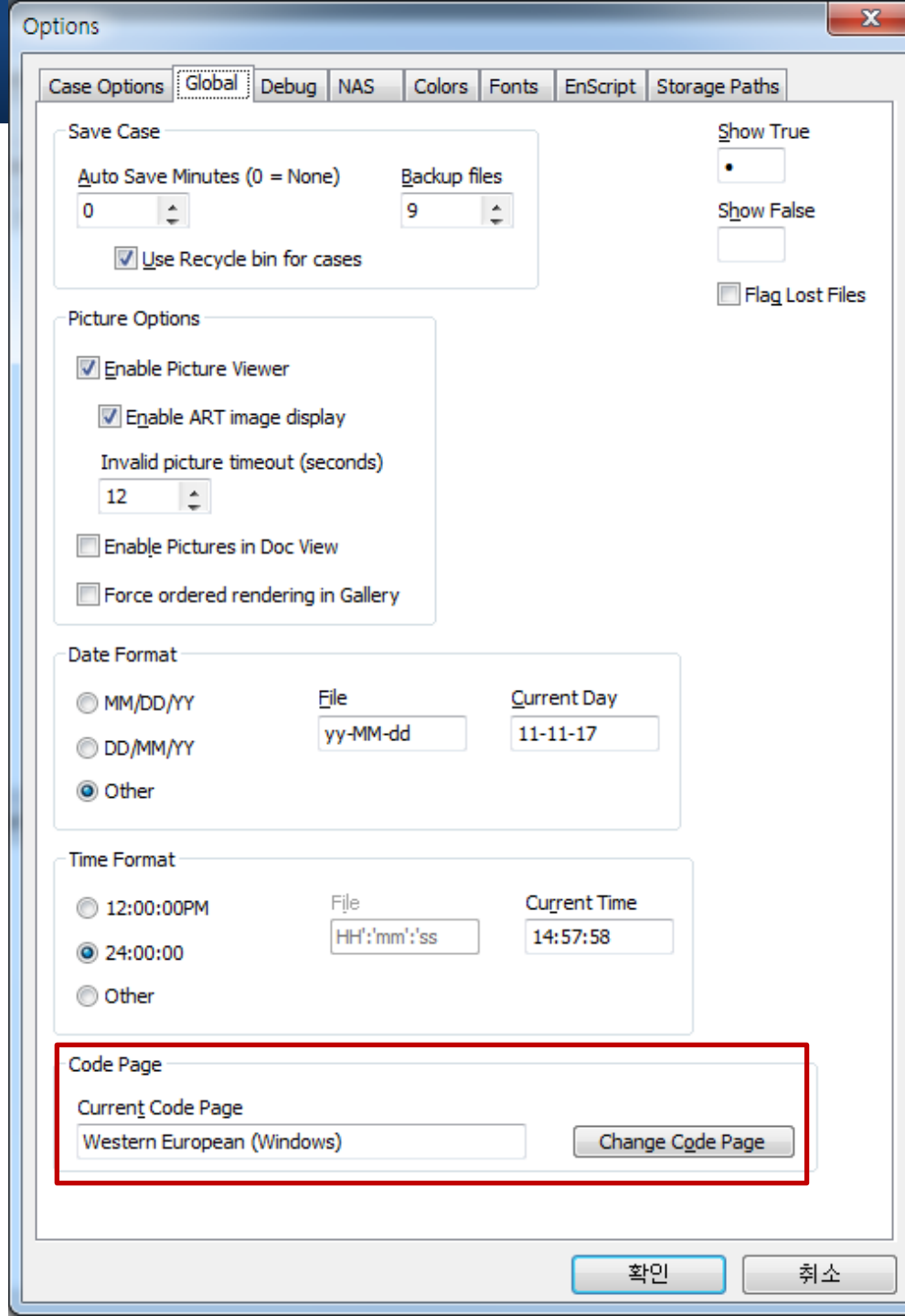
- 사용자 정의 시간 형식
 - 12::00:00PM (기본)
 - 24:00:00 (권장)



케이스 정보

케이스 옵션 (Tools → Options)

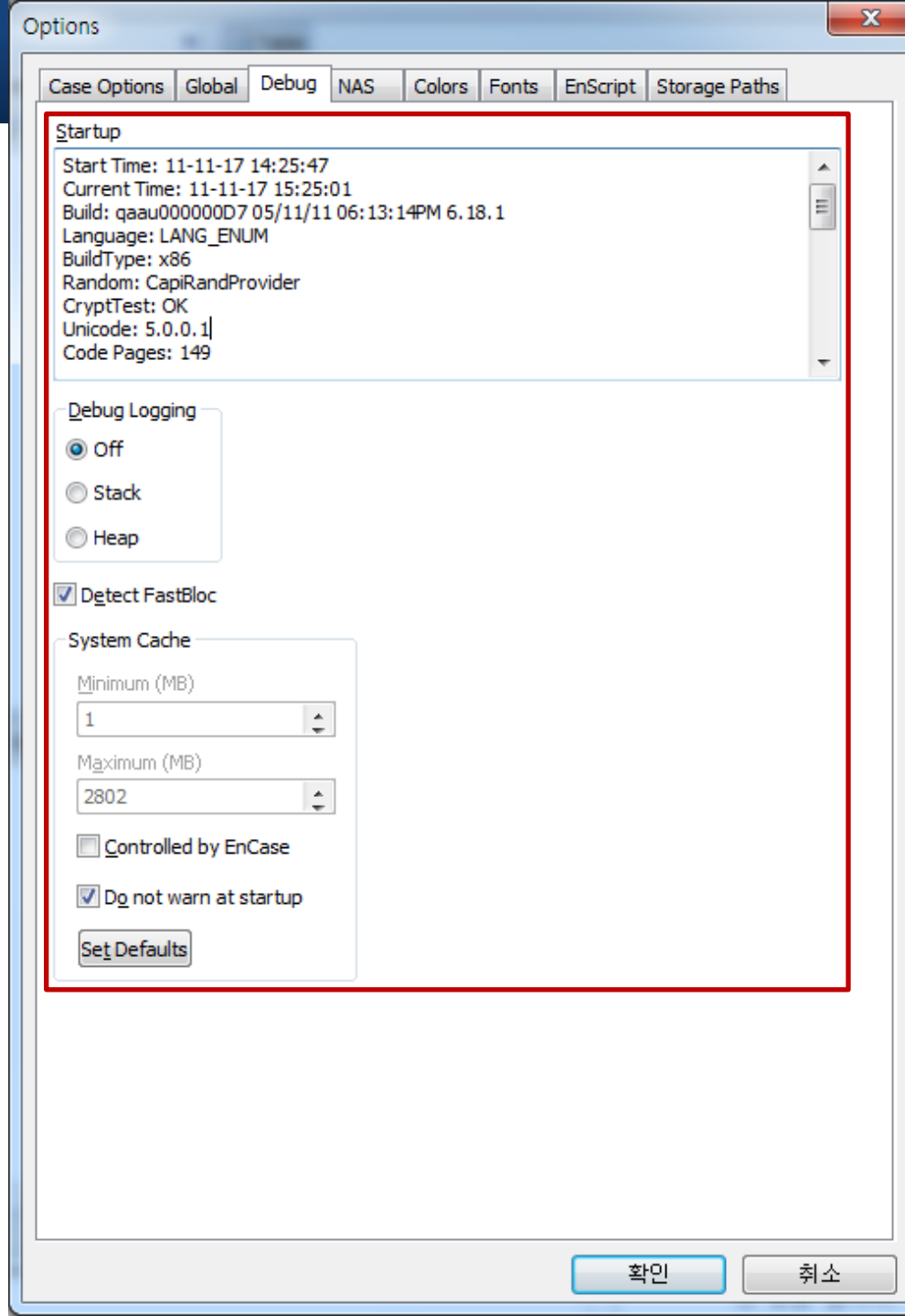
- Global 탭 → Code Page
 - Western European (기본)



케이스 정보

케이스 옵션 (Tools → Options)

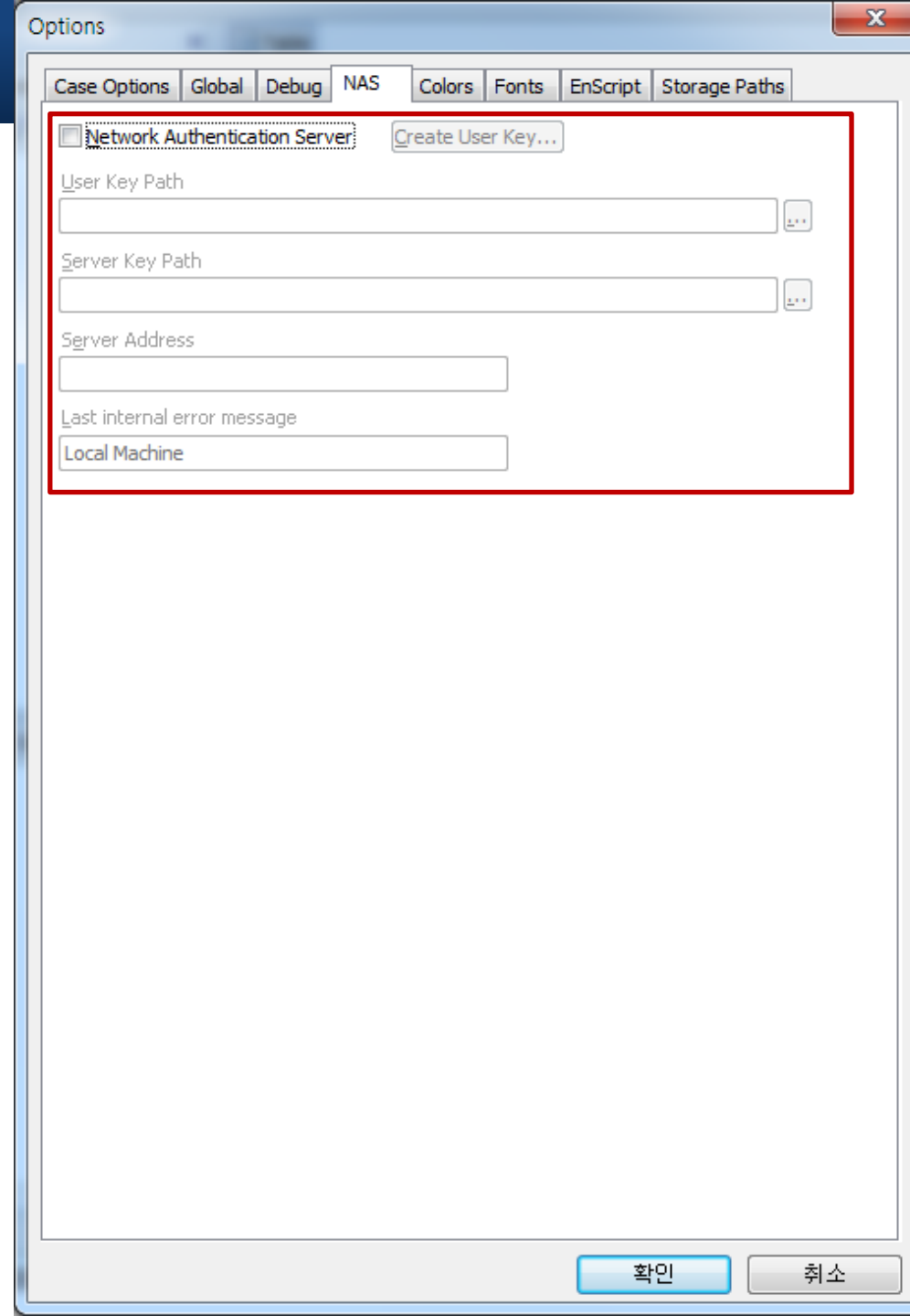
- **Debug 탭**
 - 비정상적인 종료, 프로그램 오류 시
 - 디버깅 정보 유지 여부



케이스 정보

케이스 옵션 (Tools → Options)

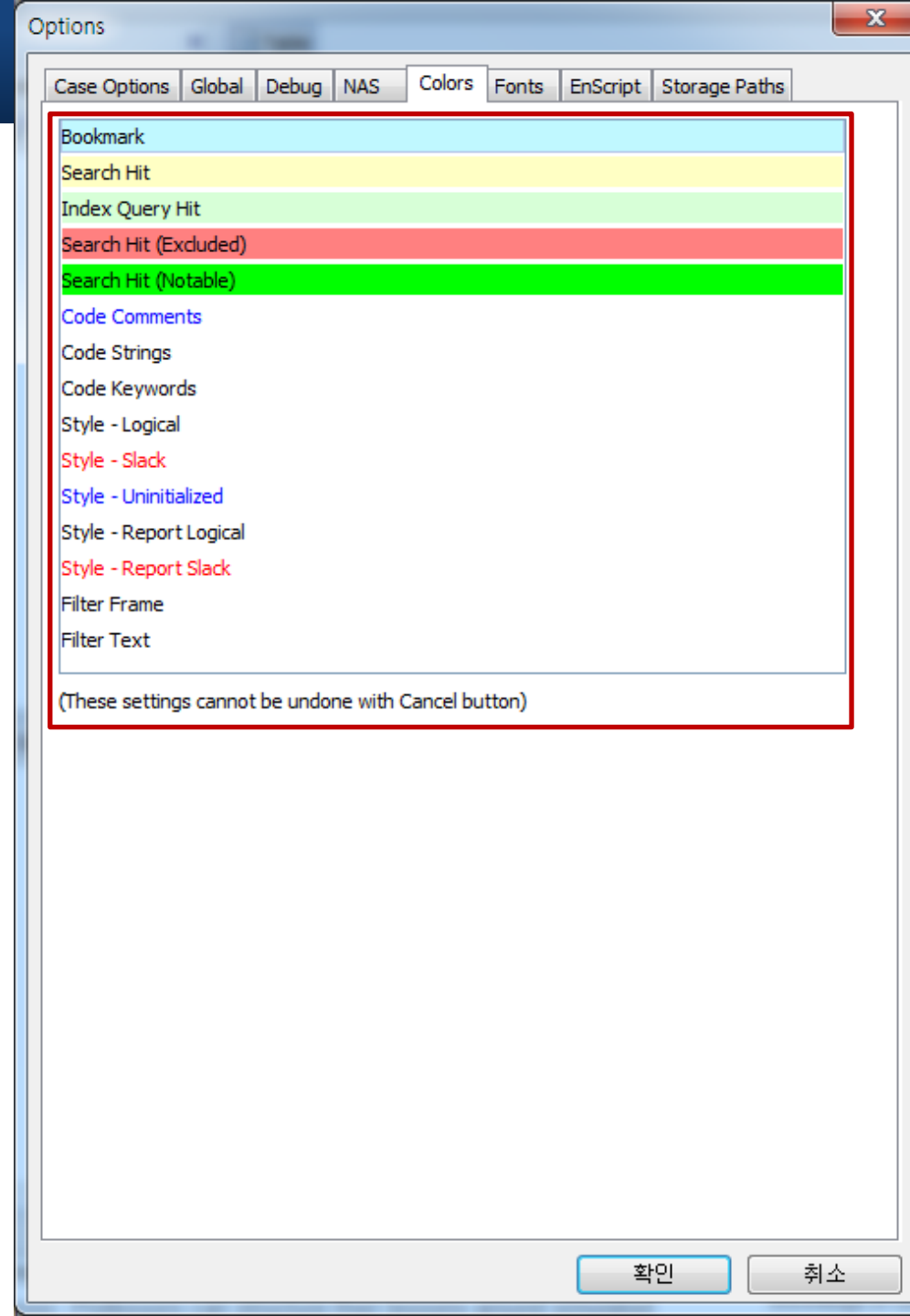
- NAS 탭
 - EnCase Lab 환경 설정 탭
 - 하나의 인증 키로 여러 EnCase 인증



케이스 정보

케이스 옵션 (Tools → Options)

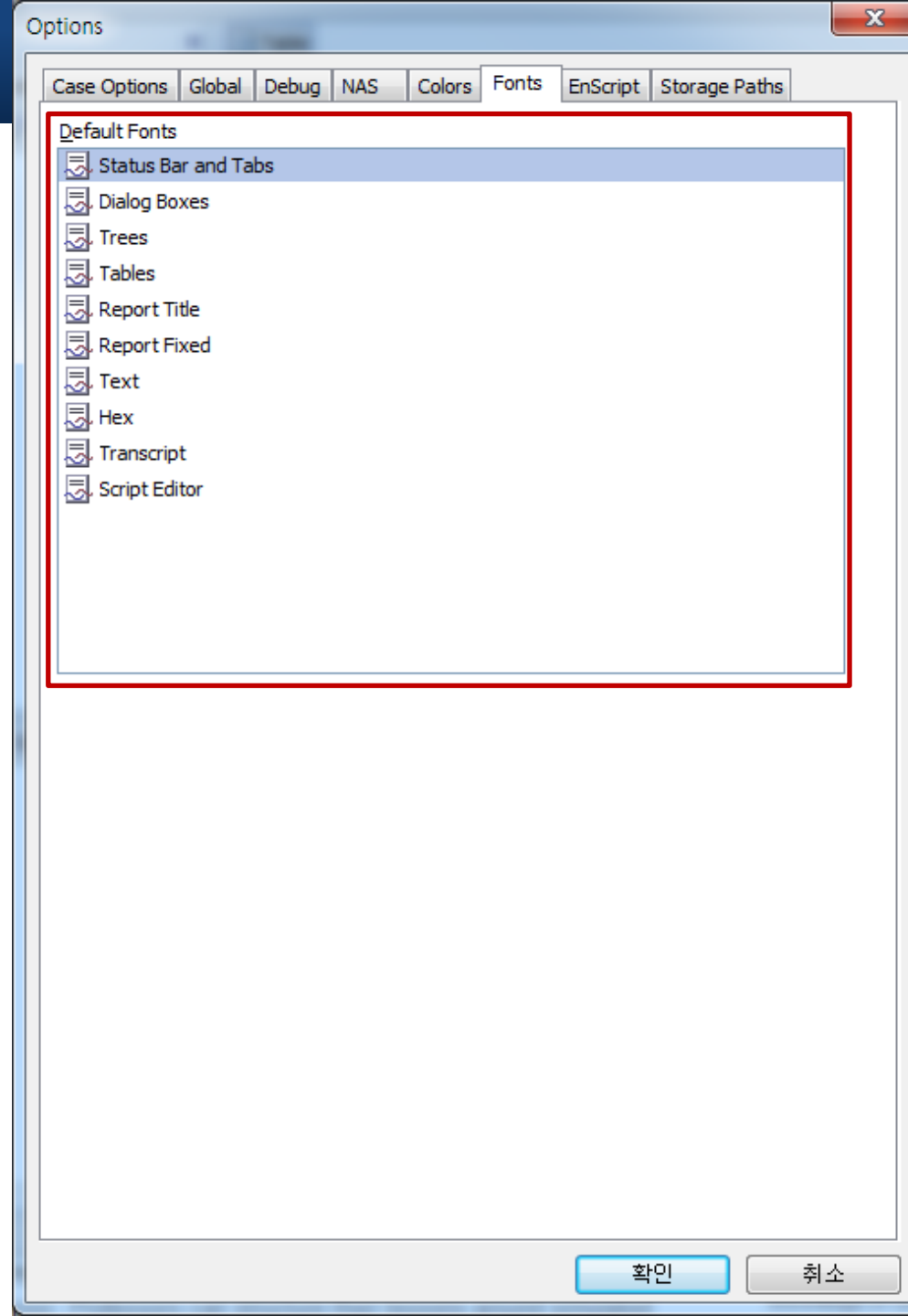
- Colors 탭
 - 북마크, 검색 결과, 필터, 키워드 등
 - 각 요소 별 색상 설정 기능



케이스 정보

케이스 옵션 (Tools → Options)

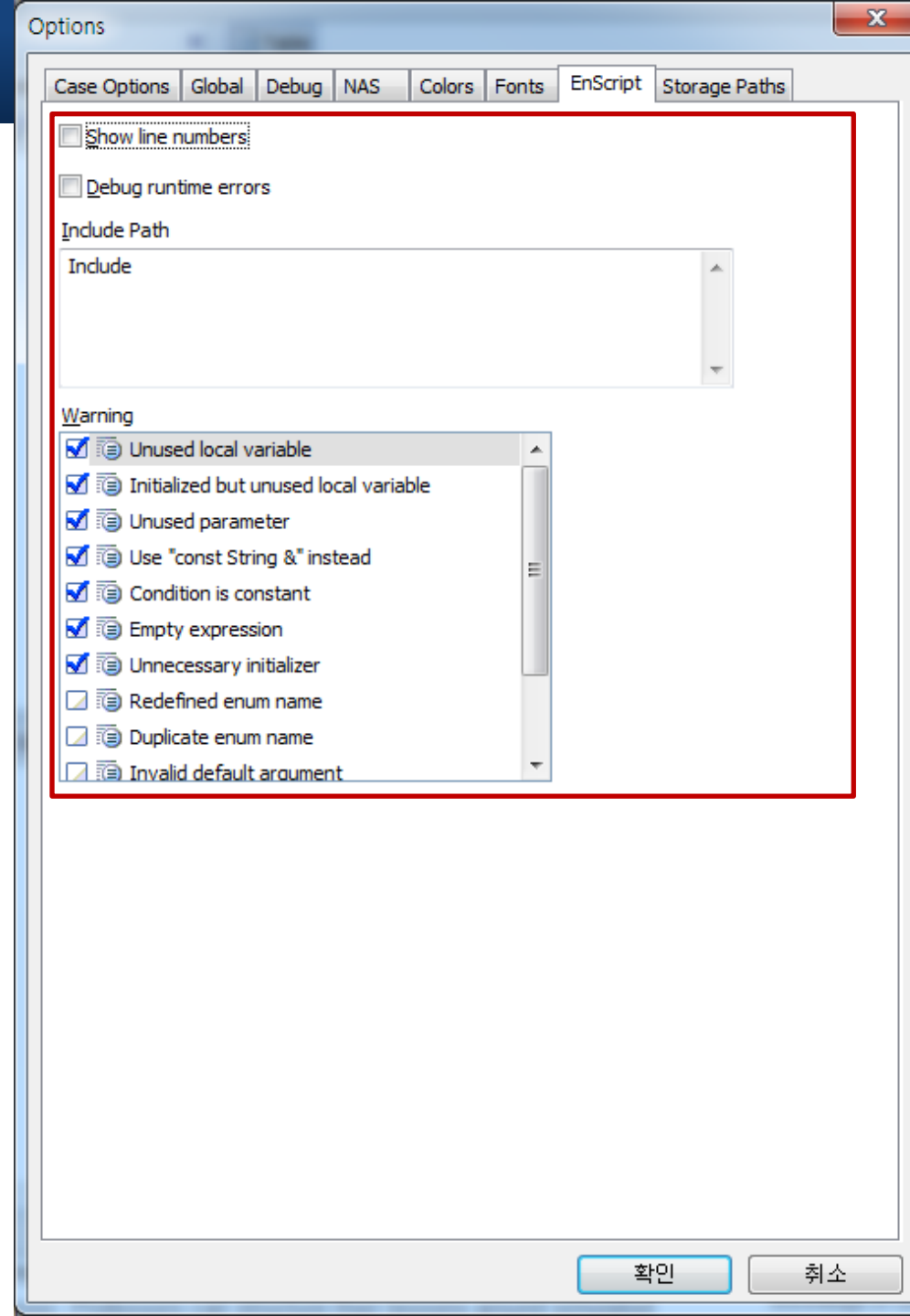
- **Fonts 탭**
 - 상태바, 트리, 테이블, 보고서 등
 - 각 요소 별 폰트 설정 기능



케이스 정보

케이스 옵션 (Tools → Options)

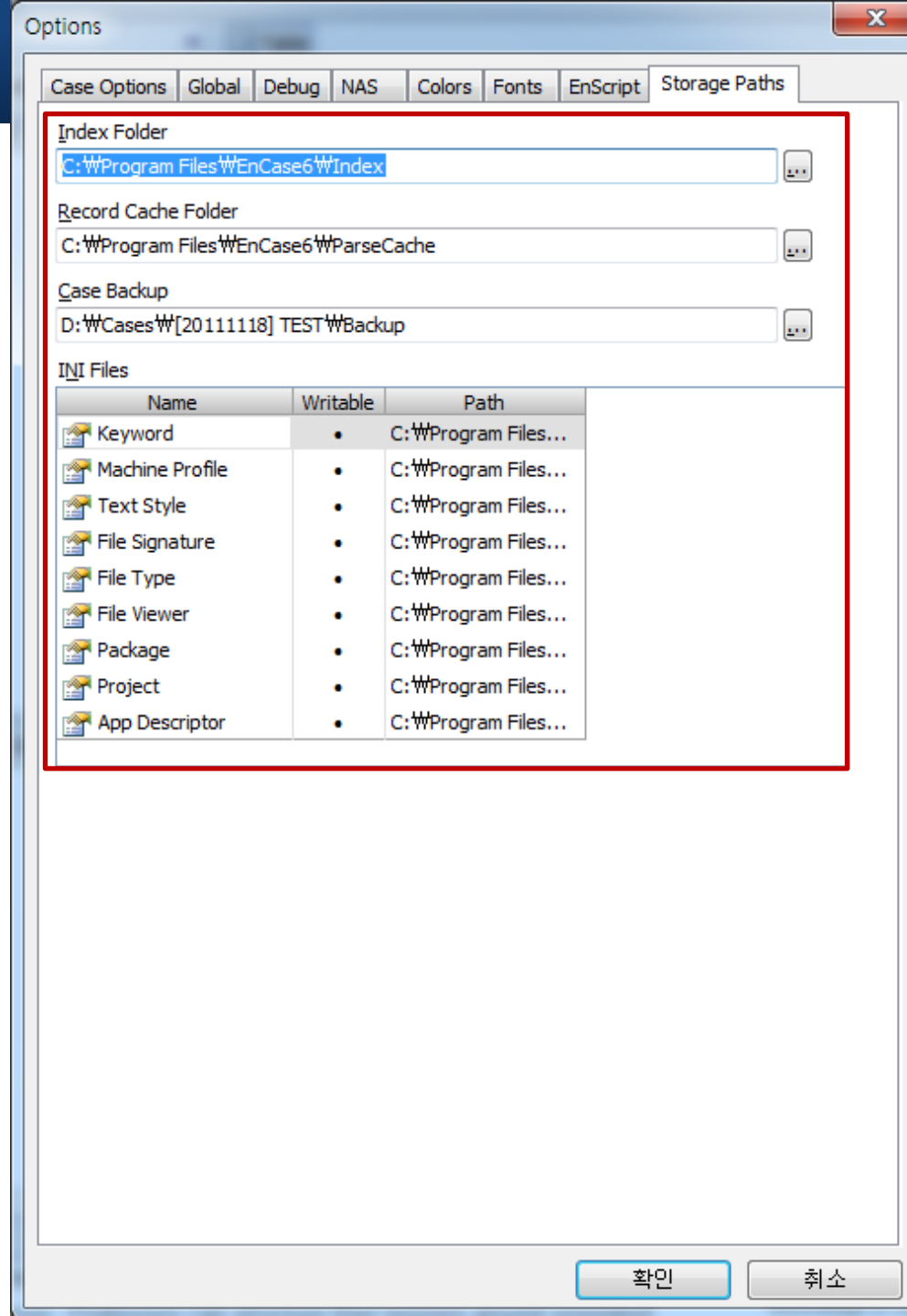
- **EnScript 탭**
 - EnScript 라이브러리 경로
 - EnScript 동작 레벨 설정



케이스 정보

케이스 옵션 (Tools → Options)

- **Storage Paths 탭**
 - **Index Folder**
 - 인덱스 정보 저장 폴더
 - **Record Cache Folder**
 - 레코드 캐시 폴더
 - **Case Backup**
 - 백업 폴더 지정
 - 미리 생성한 백업 폴더 지정 (권장)
 - **INI Files**
 - 다양한 설정 INI 파일



케이스 옵션 (Tools → Options)

- **INI Files (C:\Program Files\WinCase6\Config)**
 - **AppDescriptors.ini** : OS 별 파일 해쉬값 저장
 - **FileSignatures.ini** : File Signature Tab의 내용 저장
 - **FileTypes.ini** : File Types Tab의 내용 저장
 - **Filters.ini** : Filters Tab의 내용 저장
 - **Keywords.ini** : Keyword Tab에 내용 저장(Global Keyword)
 - **Local.ini** : 전체적인 설정값 저장
 - **Profiles.ini** : 개인 프로필 설정값
 - **TextStyles.ini** : Text Styles Tab의 내용 저장

증거 추가

Security is a people problem...

증거 추가

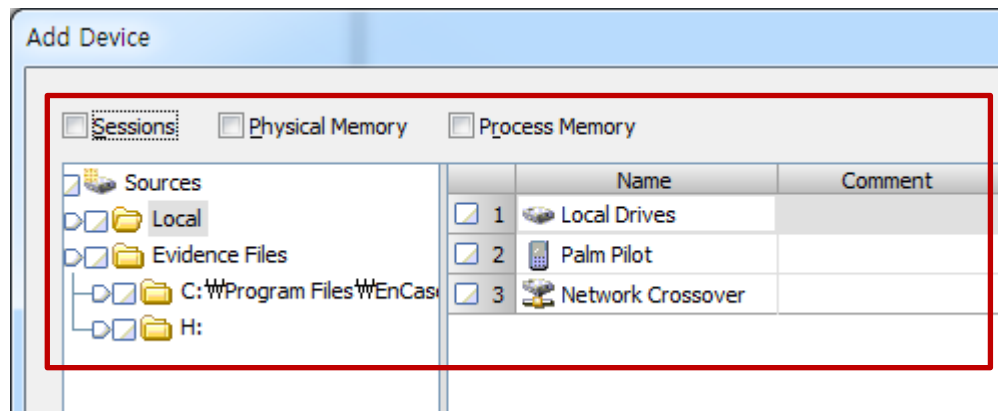
장치 추가 (File → Add Device)

- 장치 형식

- **Sessions** : 장치 및 증거 추가에 대한 세션 관리 기능
- **Physical Memory** : 물리메모리 추가
- **Process Memory** : 프로세스 메모리 추가

- 원본 형식

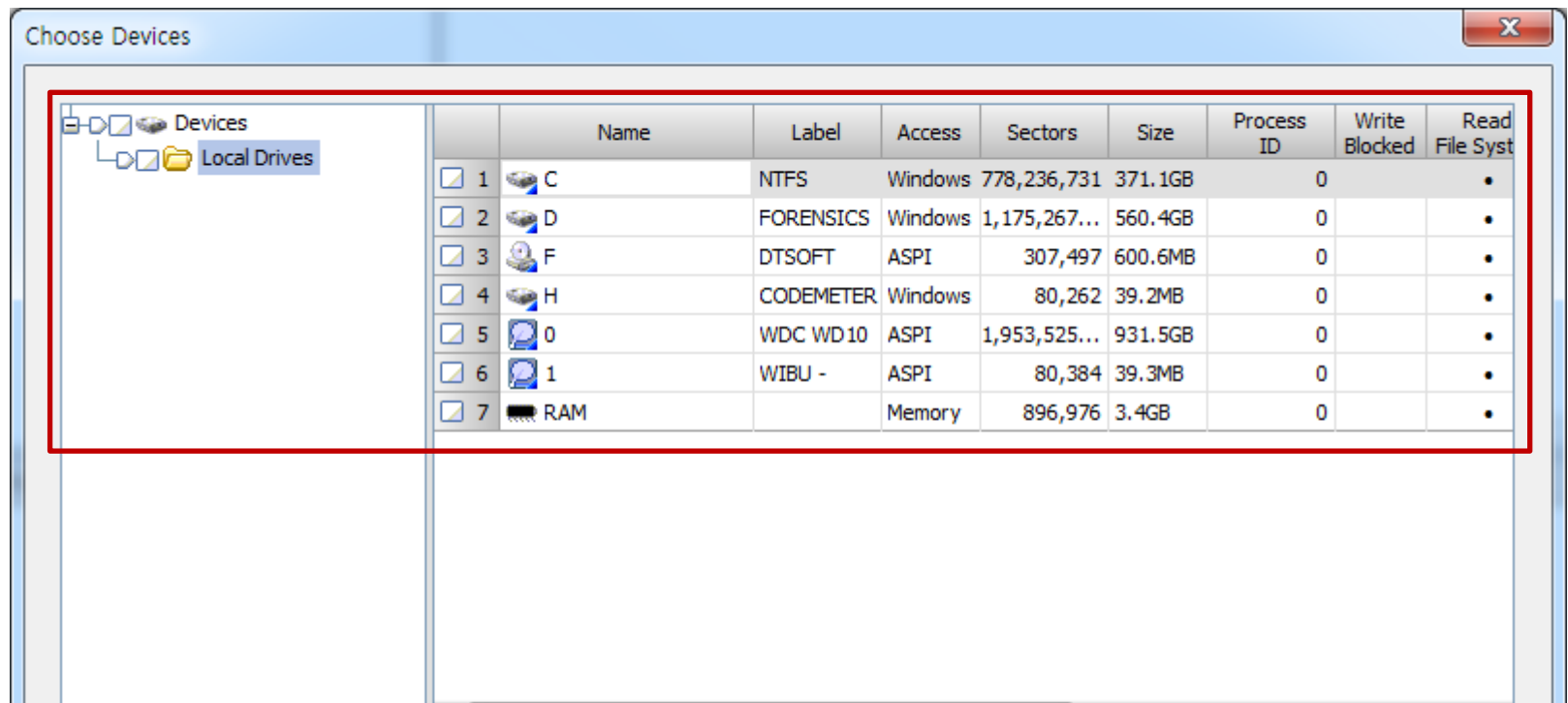
- 로컬 드라이브(Local), 증거 이미지(Evidence Files)
- 휴대용 기기(Palm Drives, COM 포트 연결)
- 네트워크 연결 (Network Crossover)



증거 추가

장치 추가 (File → Add Device)

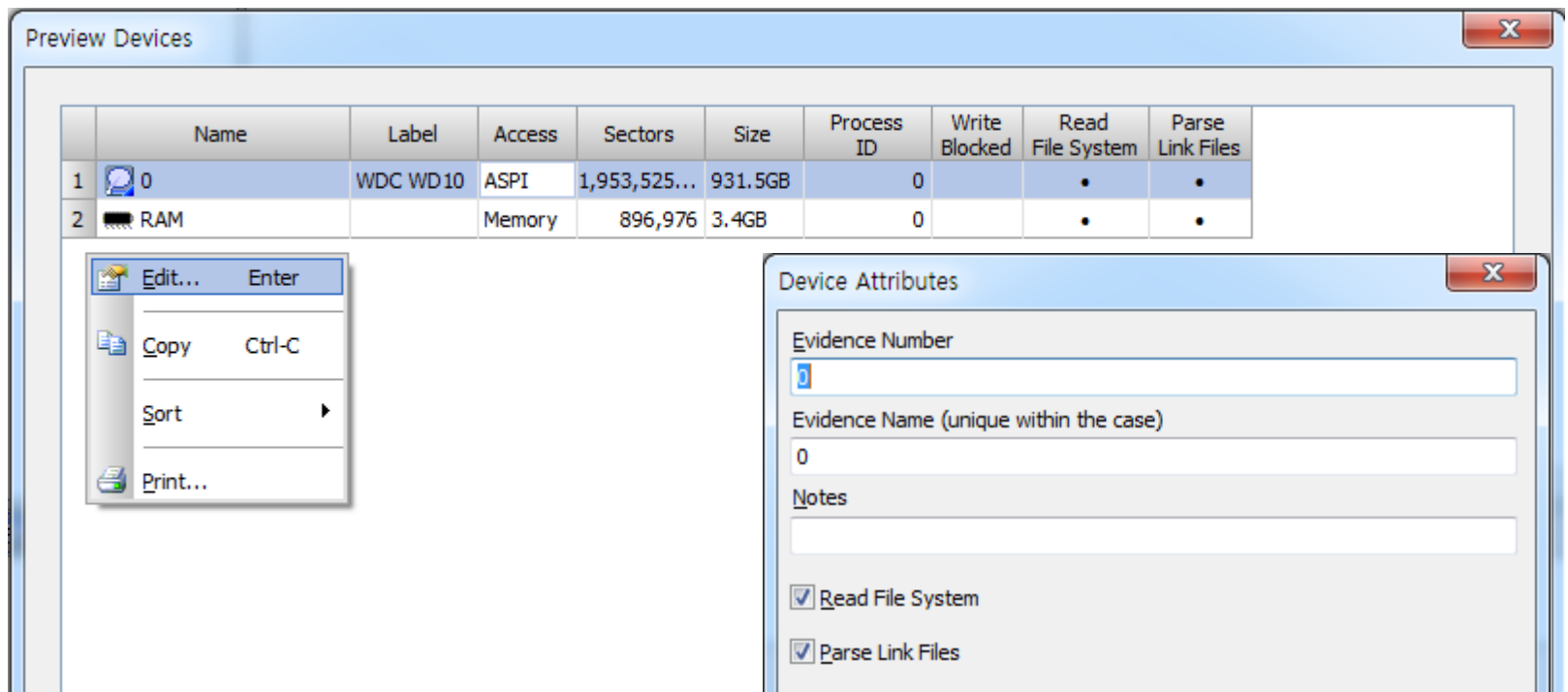
- 로컬 드라이브 추가
 - 물리메모리 체크 후 로컬 드라이브 선택
 - 마운트된 장치, 볼륨, 메모리(선택 시) 열거
 - 추가하고자 하는 장치 선택



증거 추가

장치 추가 (File → Add Device)

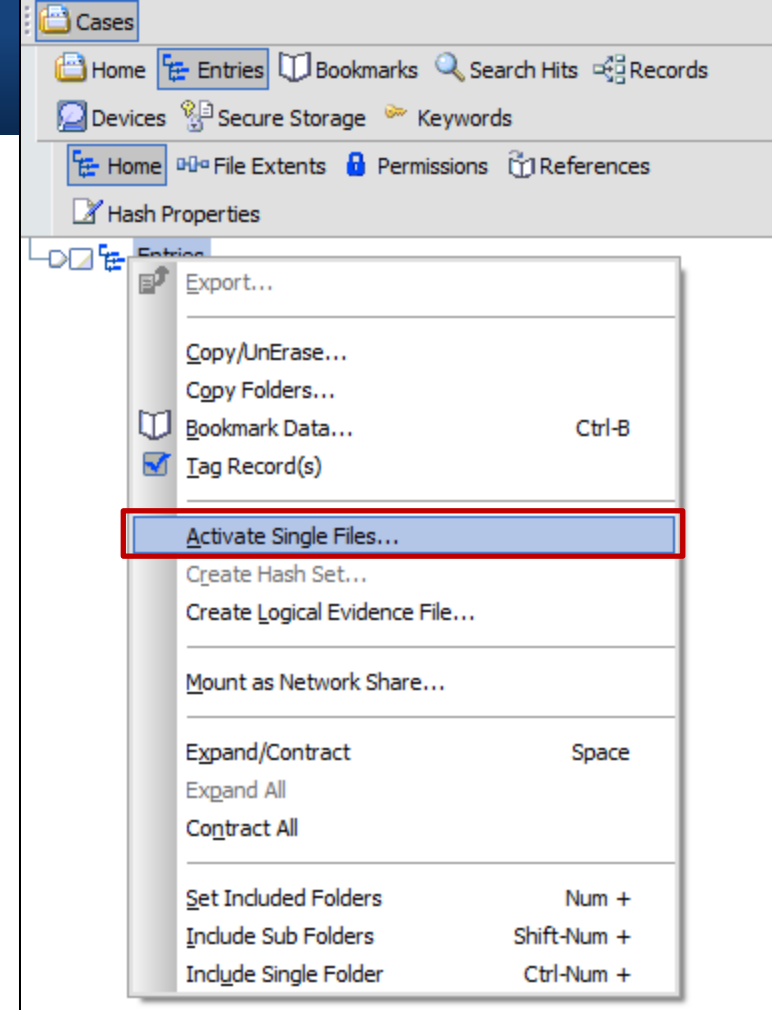
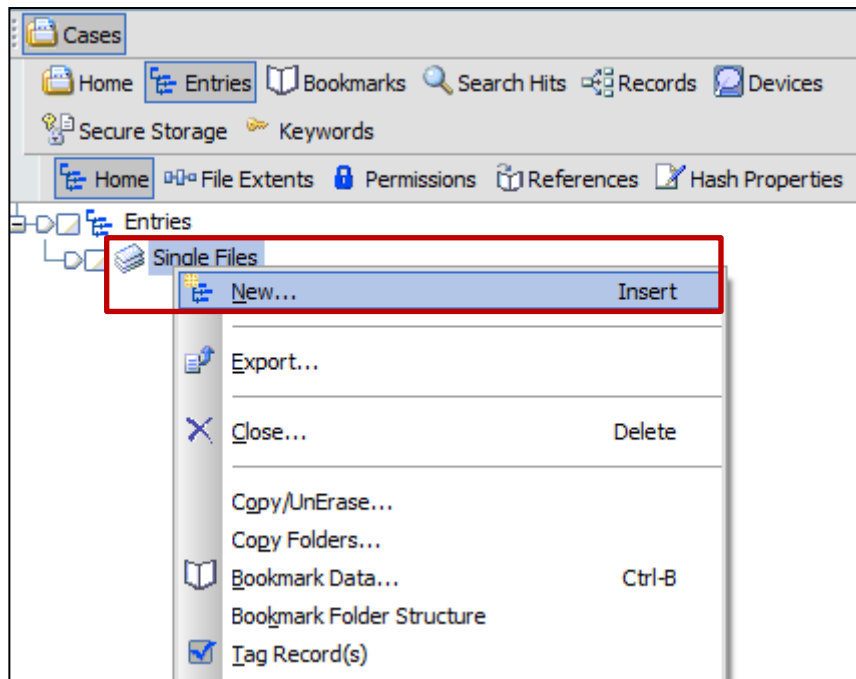
- 선택한 장치 정보
 - 레이블, 접근 방식, 물리적 섹터, 크기, 쓰기방지장치 사용 여부, 파일시스템 읽기, LNK 파싱
 - 증거 번호, 증거 이름, 메모 정보 수정 가능
 - 파일시스템 해석 여부(Read File System), 링크 파일 파싱 여부(Parse Link Files) 결정



파일 추가 (Entries → Activate Single Files)

- Single Files

- 장치, 볼륨이 아닌 개별파일 추가 기능
- 로그, 레지스트리, 이메일 등

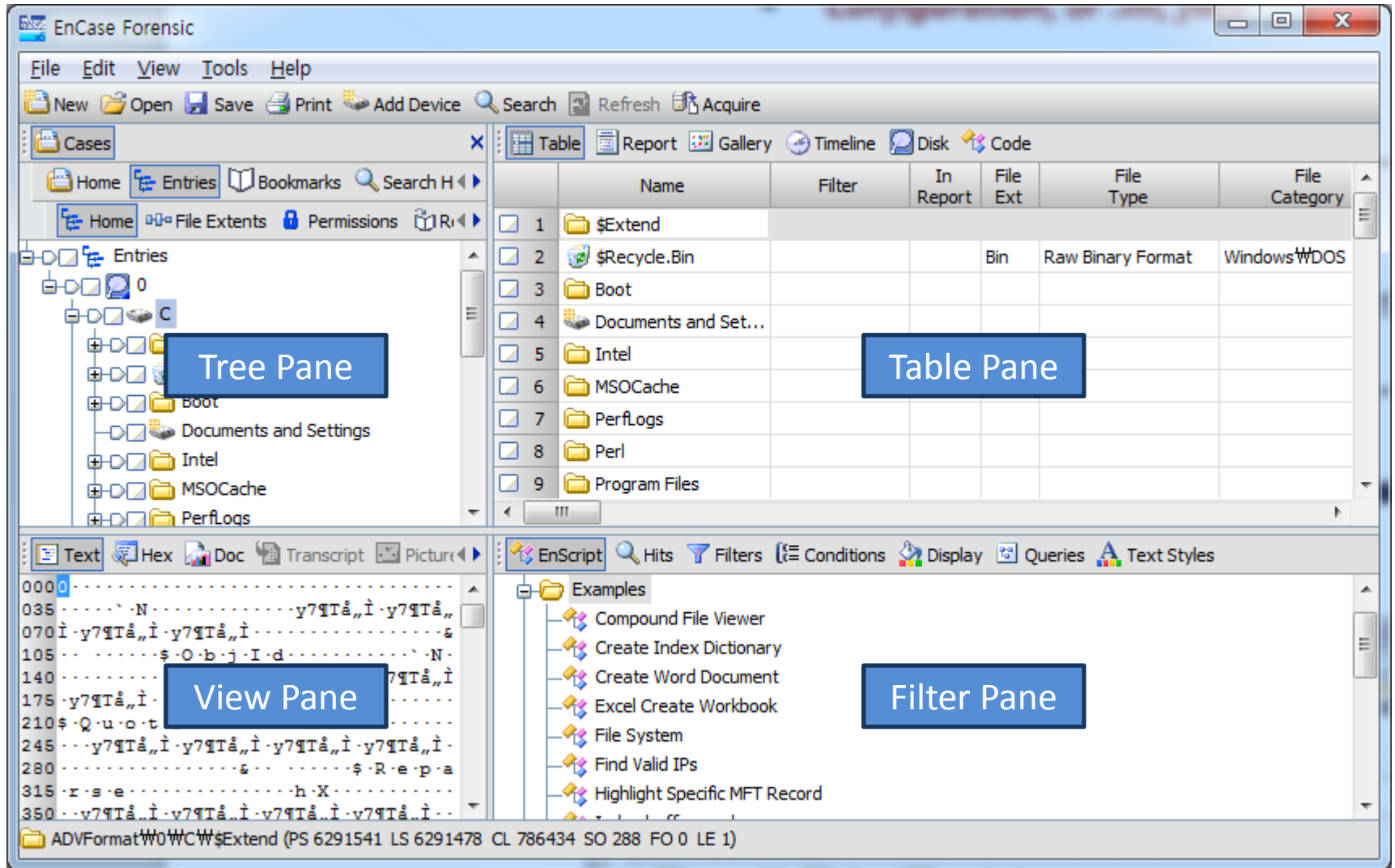


사용 환경

Security is a people problem...

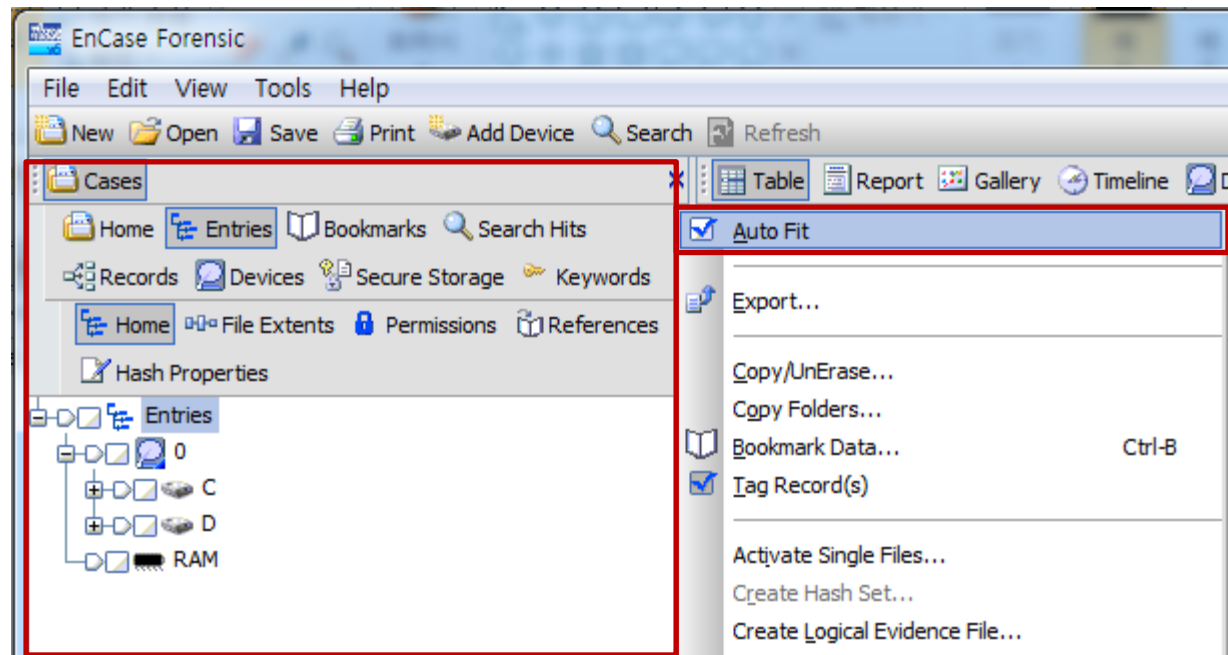
사용 환경

주요 창



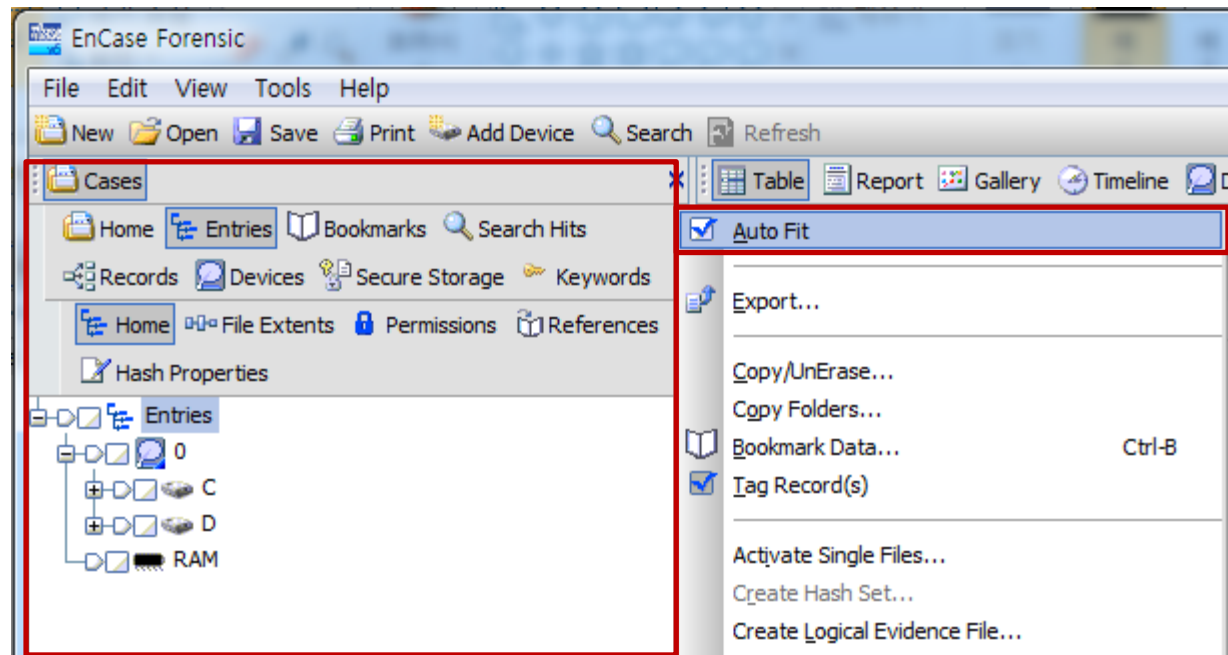
트리 패인 (Auto Fit 적용)

- **Home** : 기본 케이스 정보
- **Entries** : 파일시스템 트리 구조, 선택한 파일 속성, 권한, 참조, 해쉬 정보 표시
- **Bookmarks** : 사용자가 추가한 북마크 정보 표시
- **Search Hits** : 키워드 검색 결과



트리 패인 (Auto Fit 적용)

- **Records** : 증거와 관련된 추가적인 관리 정보
- **Devices** : 디스크 구성 설정(RAID, LVM 등), 하드웨어 정보
- **Secure Storage** : 시스템에서 보안과 관련된 정보
- **Keywords** : 사용자 추가 검색 키워드 (현재 케이스에만 적용)

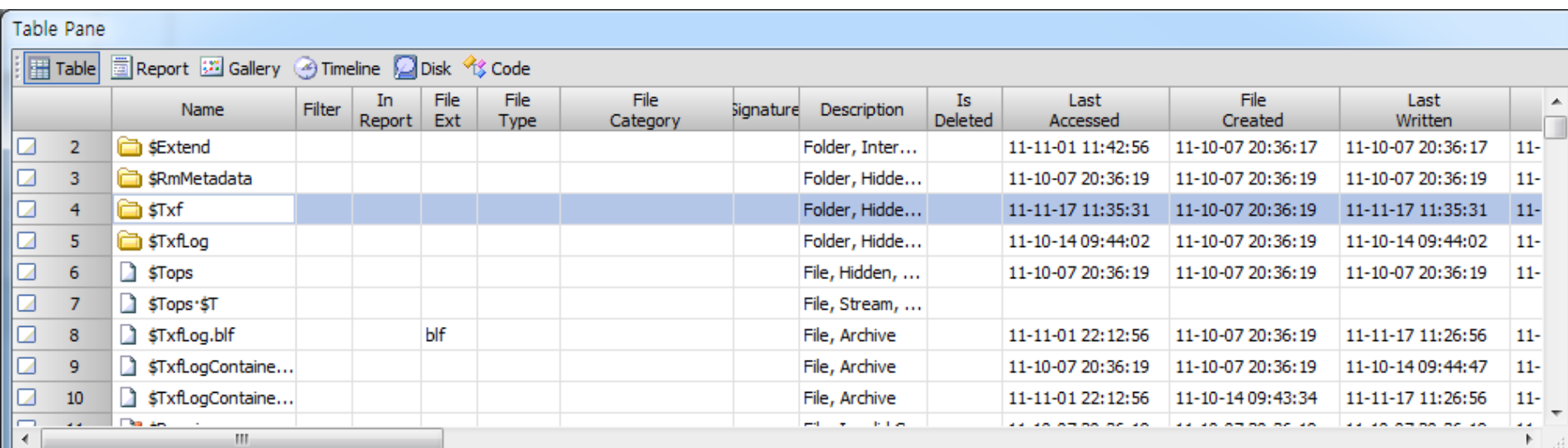


사용 환경

테이블 패인

- Table 탭

- 선택한 폴더 및 파일의 다양한 속성 정보 표시
- **39개 속성** : Name, Filter, In Report, File Ext, File Type, File Category, Signature, Description, Is Deleted, Last Accessed, File Created, Last Written, Entry Modified, File Deleted, File Acquired, Logical Size, Initialized Size, Physical Size, Starting Extend, File Extents, Permissions, References, Physical Location, Physical Sector, Evidence File, File Identifier, Code Page, Hash Value, Hash Category, Hash Properties, Full Path, Short Name, Unique Name, Original Path, Symbolic Link, Is Duplicate, Is Internal, Is Overwritten



The screenshot shows a software interface titled 'Table Pane'. It features a tabbed menu at the top with 'Table' selected, along with 'Report', 'Gallery', 'Timeline', 'Disk', and 'Code'. Below the menu is a table with 14 columns: an index column, 'Name', 'Filter', 'In Report', 'File Ext', 'File Type', 'File Category', 'Signature', 'Description', 'Is Deleted', 'Last Accessed', 'File Created', 'Last Written', and an additional column. The table lists several items, including folders like '\$Extend', '\$RmMetadata', '\$Txf', and '\$TxfLog', and files like '\$Tops', '\$Tops*\$T', '\$TxfLog.blf', and '\$TxfLogContaine...'. Row 4, corresponding to '\$Txf', is highlighted in blue.

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	Last Accessed	File Created	Last Written	
<input checked="" type="checkbox"/> 2	\$Extend							Folder, Inter...		11-11-01 11:42:56	11-10-07 20:36:17	11-10-07 20:36:17	11-
<input checked="" type="checkbox"/> 3	\$RmMetadata							Folder, Hidde...		11-10-07 20:36:19	11-10-07 20:36:19	11-10-07 20:36:19	11-
<input checked="" type="checkbox"/> 4	\$Txf							Folder, Hidde...		11-11-17 11:35:31	11-10-07 20:36:19	11-11-17 11:35:31	11-
<input checked="" type="checkbox"/> 5	\$TxfLog							Folder, Hidde...		11-10-14 09:44:02	11-10-07 20:36:19	11-10-14 09:44:02	11-
<input checked="" type="checkbox"/> 6	\$Tops							File, Hidden, ...		11-10-07 20:36:19	11-10-07 20:36:19	11-10-07 20:36:19	11-
<input checked="" type="checkbox"/> 7	\$Tops*\$T							File, Stream, ...					
<input checked="" type="checkbox"/> 8	\$TxfLog.blf			blf				File, Archive		11-11-01 22:12:56	11-10-07 20:36:19	11-11-17 11:26:56	11-
<input checked="" type="checkbox"/> 9	\$TxfLogContaine...							File, Archive		11-10-07 20:36:19	11-10-07 20:36:19	11-10-14 09:44:47	11-
<input checked="" type="checkbox"/> 10	\$TxfLogContaine...							File, Archive		11-11-01 22:12:56	11-10-14 09:43:34	11-11-17 11:26:56	11-

사용 환경

테이블 패인

- **Report 탭**
 - 케이스 기본 정보, 북마크된 정보 등에 대한 보고서

Table Pane

Table Report Gallery Timeline Disk Code

Import File

Import File Page 1

Import File

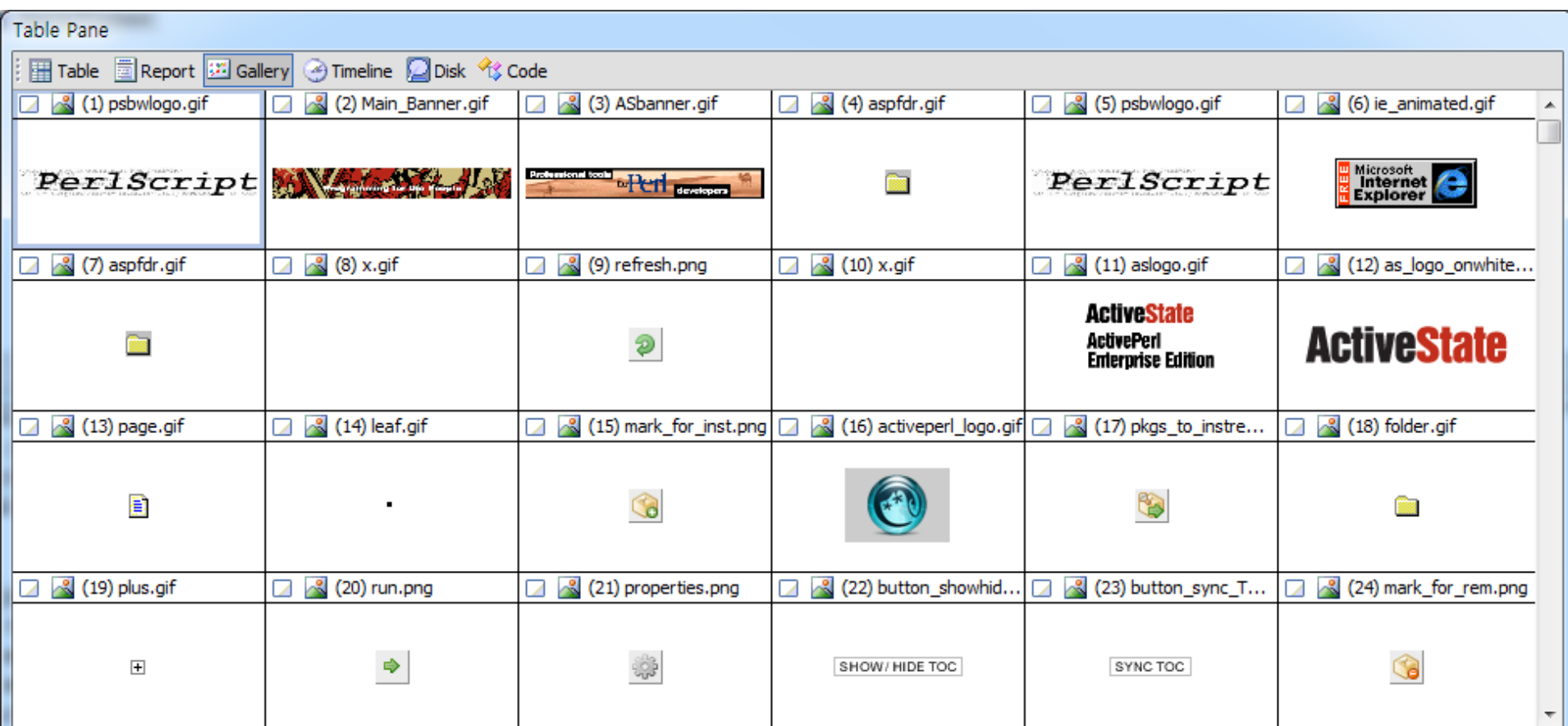
Name \$TxfLogContainer00000000000000000002
File Type
Signature
Last Accessed 11-10-07 20:36:19
File Created 11-10-07 20:36:19
Last Written 11-10-14 09:44:47
Logical Size 10,485,760
Physical Size 10,485,760
Full Path TEST\0\C\Extend\SRmMetadata\STxfLog\STxfLogContainer00000000000000000002

Name \$Repair-\$Config
File Type
Signature
Last Accessed
File Created
Last Written

사용 환경

테이블 패인

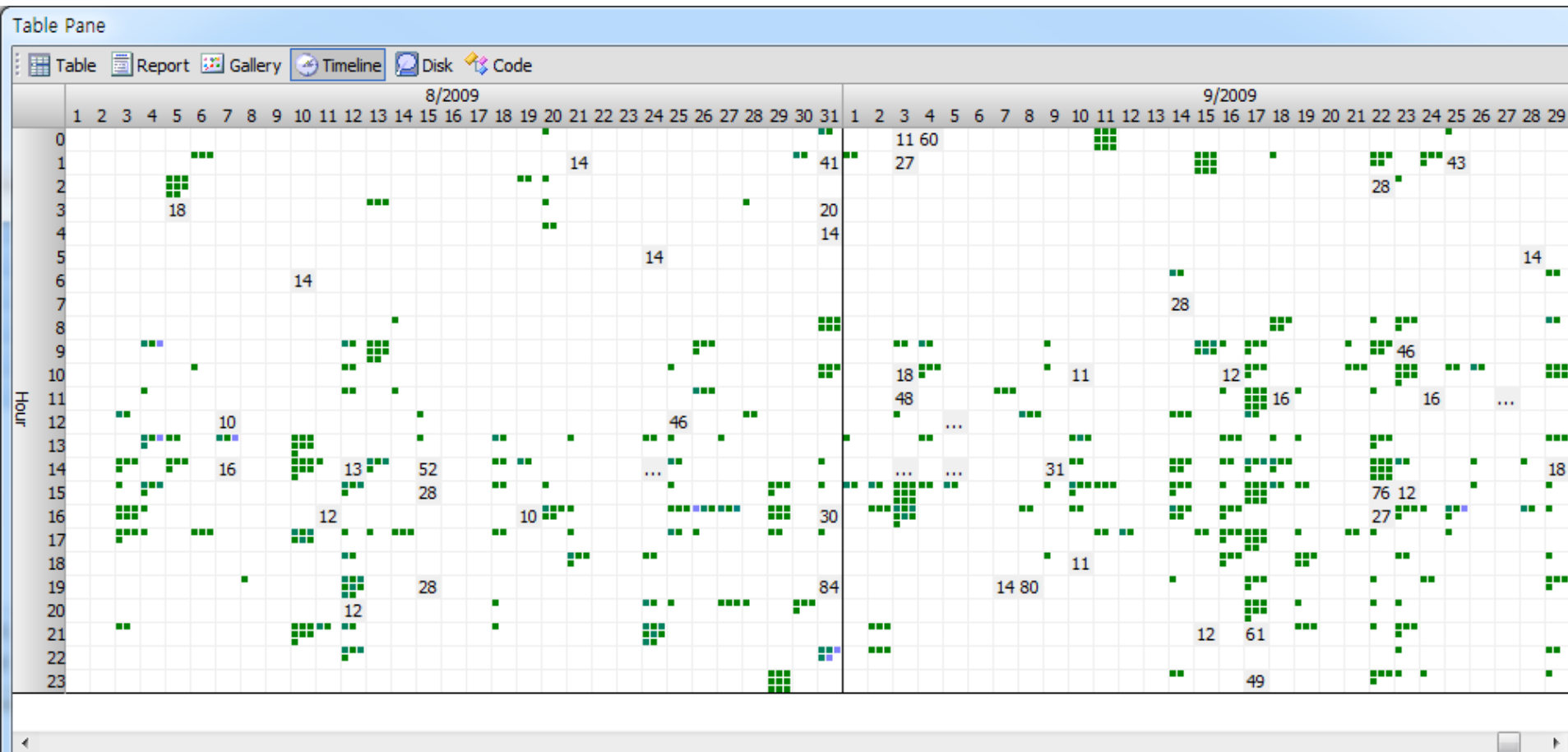
- Gallery 탭
 - 추가한 드라이브, 폴더 하위의 그래픽 파일 표시



사용 환경

테이블 패인

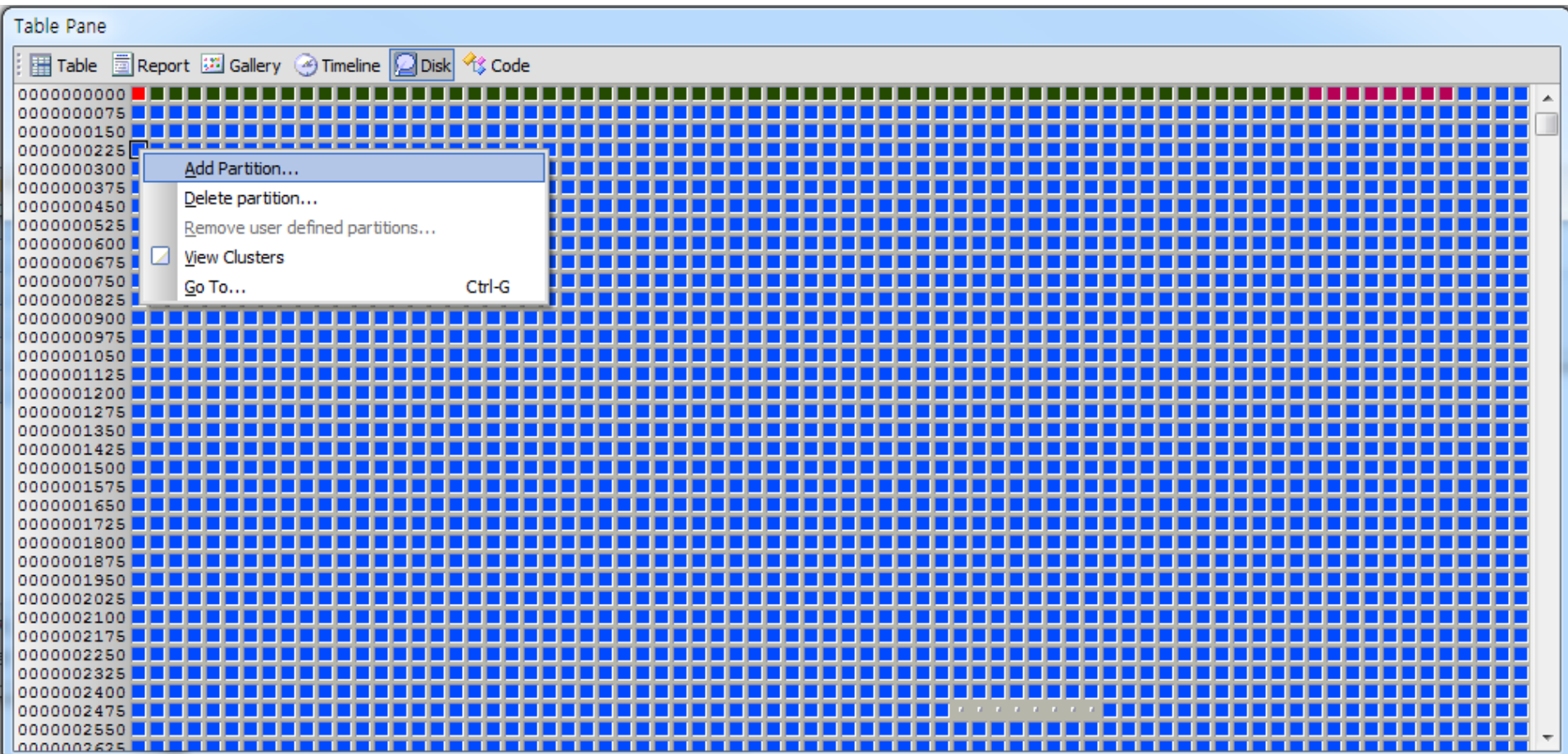
- **Timeline 탭**
 - 테이블 패인에 추가된 파일에 대한 타임라인 정보



사용 환경

테이블 패인

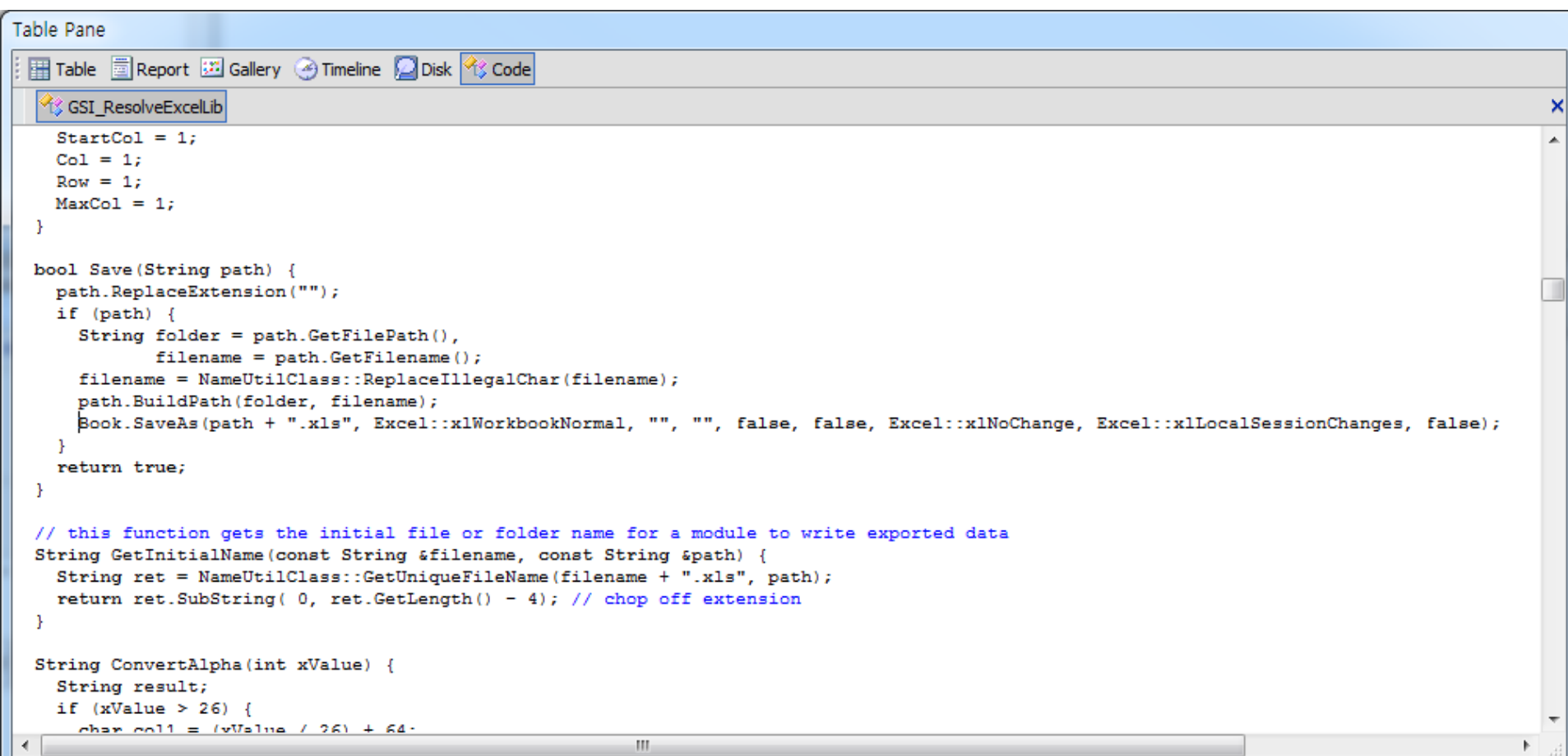
- **Disk 탭**
 - 선택한 드라이브의 디스크 구성



사용 환경

테이블 패인

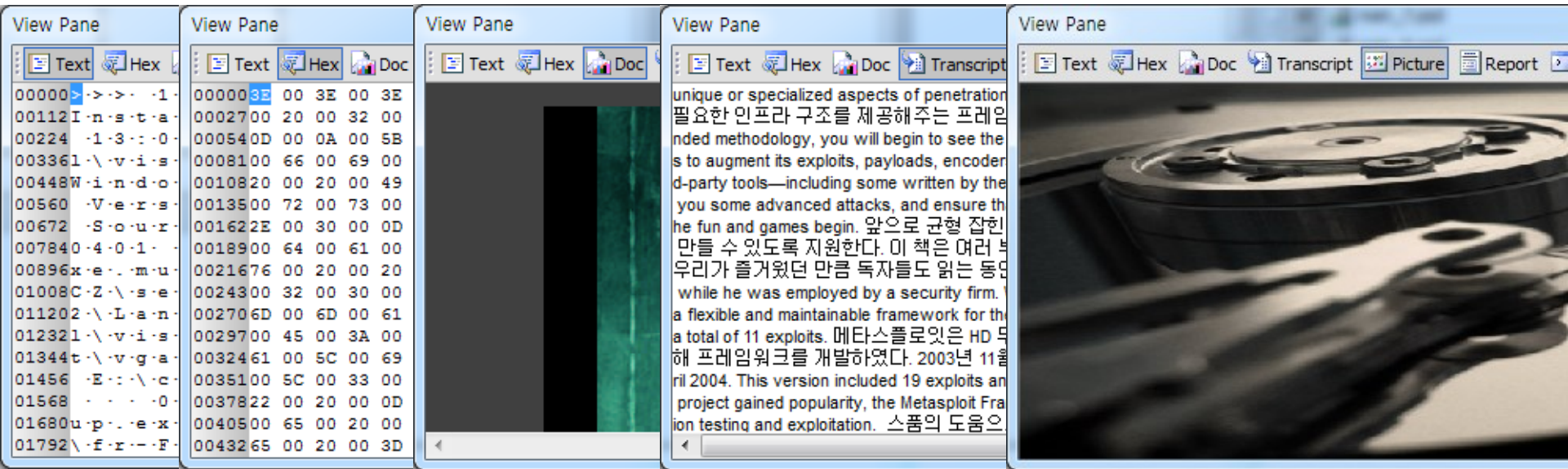
- Code 탭
 - EnScript 코드 관리 탭



사용 환경

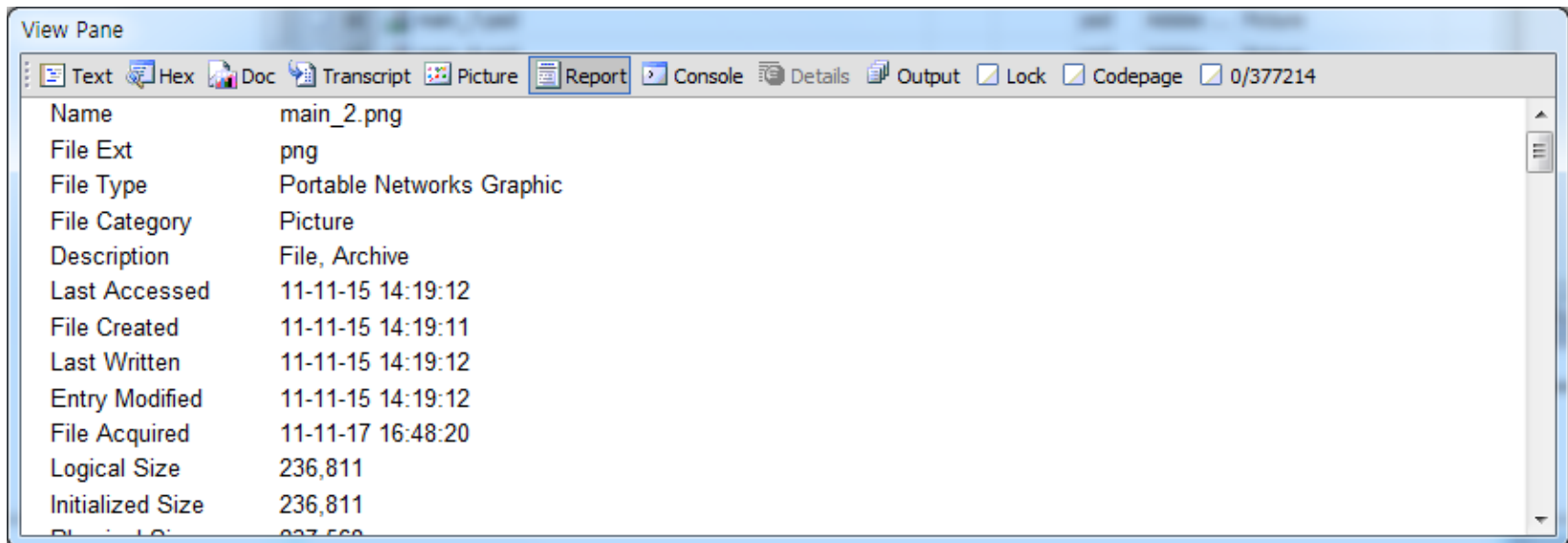
뷰 패인

- **Text 탭** : 선택한 파일 및 폴더의 텍스트 정보
- **Hex 탭** : 선택한 파일 및 폴더의 Hex 데이터 정보
- **Doc 탭**: 문서 파일(doc, excel, ppt, pdf 등)의 뷰어 기능
- **Transcript 탭** : 출력 가능한 문자로 표현
- **Picture 탭** : 그래픽 파일 표시



뷰 패인

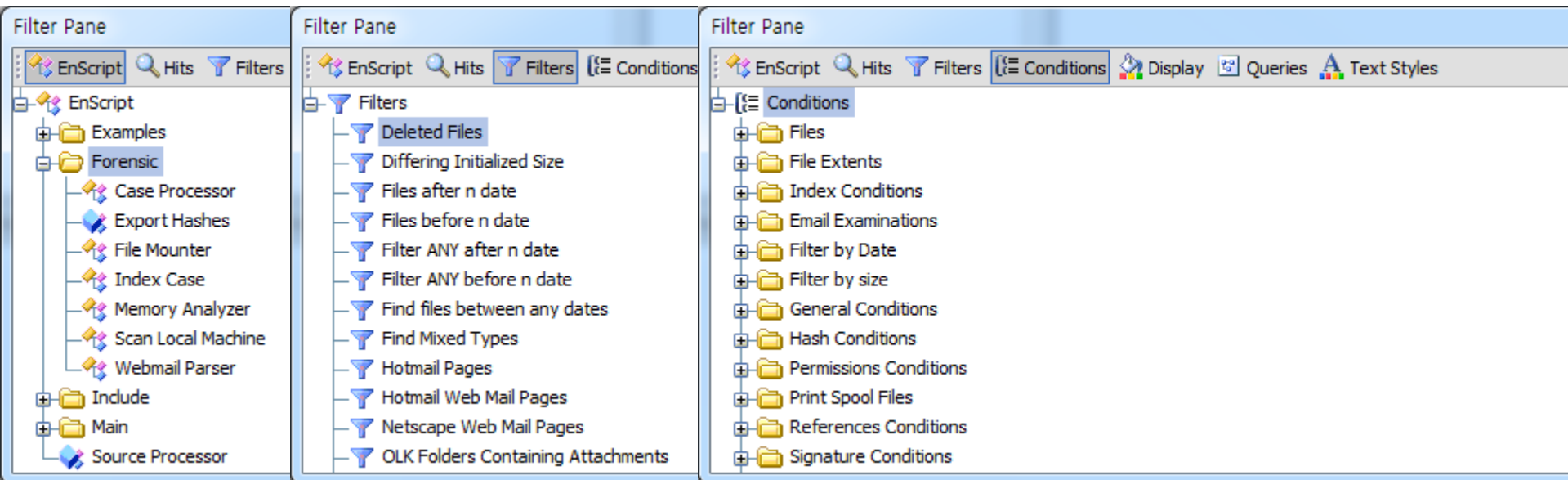
- **Report 탭** : 선택한 파일이나 볼륨의 세부 정보
- **Console 탭** : 검색, 해쉬, 검증 등의 기능 수행 후 출력 내용
- **Lock 체크박스** : 특정 탭 고정 기능
- **Dixon 체크박스** : 선택한 아이템 표시 및 해제 기능



사용 환경

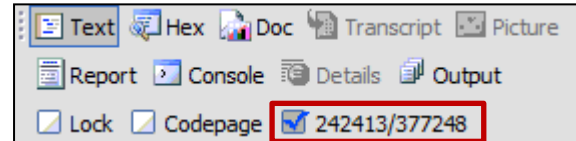
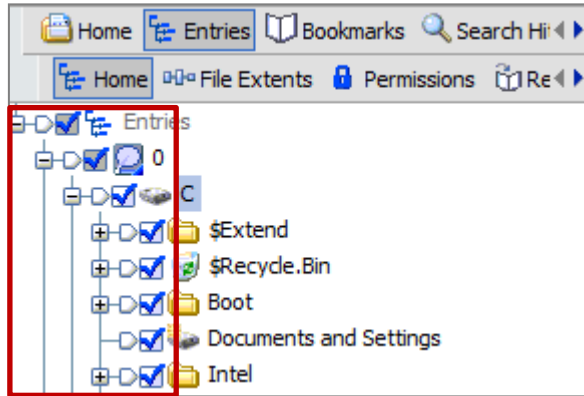
필터 패인

- **EnScript 탭** : 기본 및 사용자 정의 EnScript 관리 탭
- **Filters 탭** : 적용 가능한 필터 목록 (EnScript로 작성)
- **Conditions 탭** : 적용 가능한 조건 목록 (테이블 속성 별 정의 가능)
- **Display 탭** : 활성화된 필터, 조건 목록
- **Text Styles 탭** : 뷰 패인에 표시하는 텍스트 스타일 정의



체크 박스

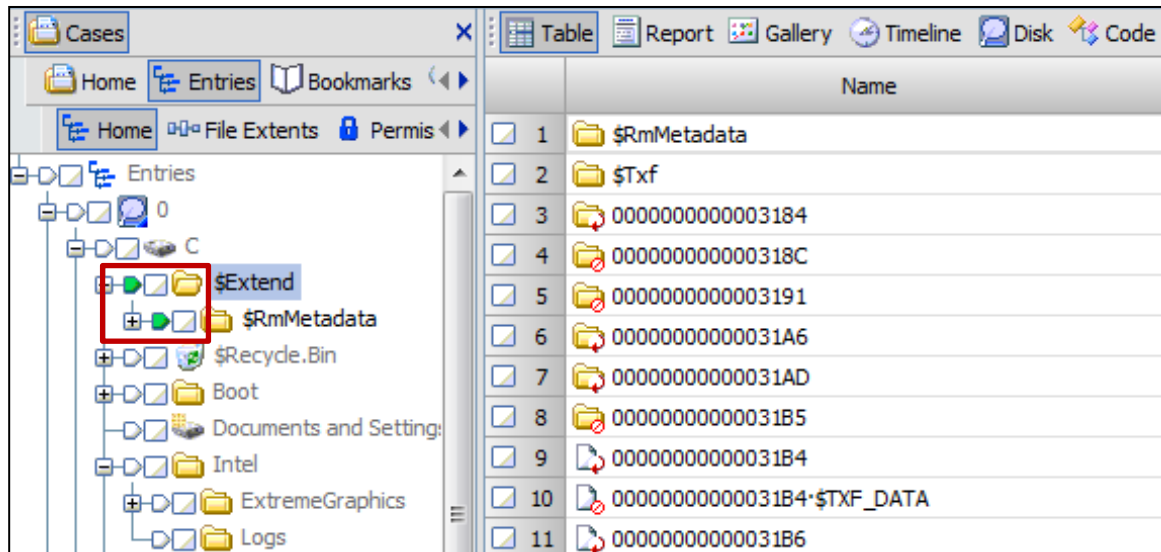
- 체크 박스



- 검색, 해쉬 계산, 시그니처 검사, 파일 카빙과 같은 작업 수행 시 대상 선택 기능
- 반드시 Dixon 박스와 연계하여 확인 필요

테이블에 폴더 추가

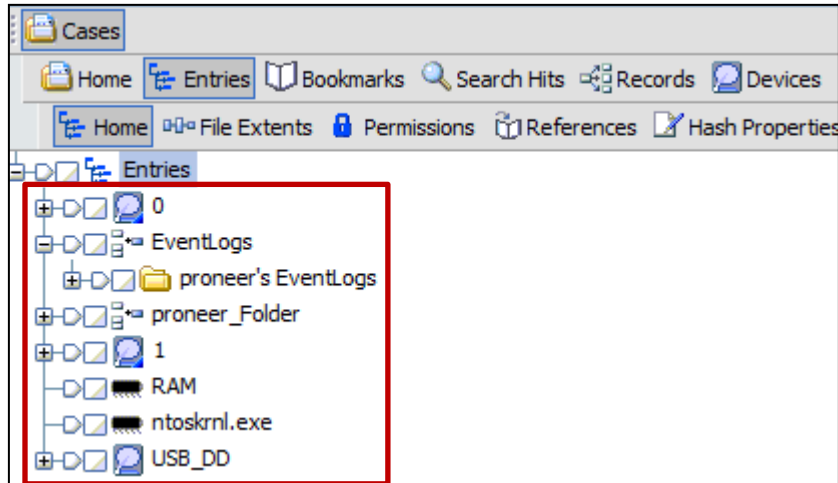
- 테이블에 폴더 추가 (Set Include Folder)



- 선택한 하위 폴더의 모든 내용을 테이블 패인에 추가
- 필터, 조건 등의 기능은 테이블 패인에 추가된 아이템에만 적용됨

증거 형태

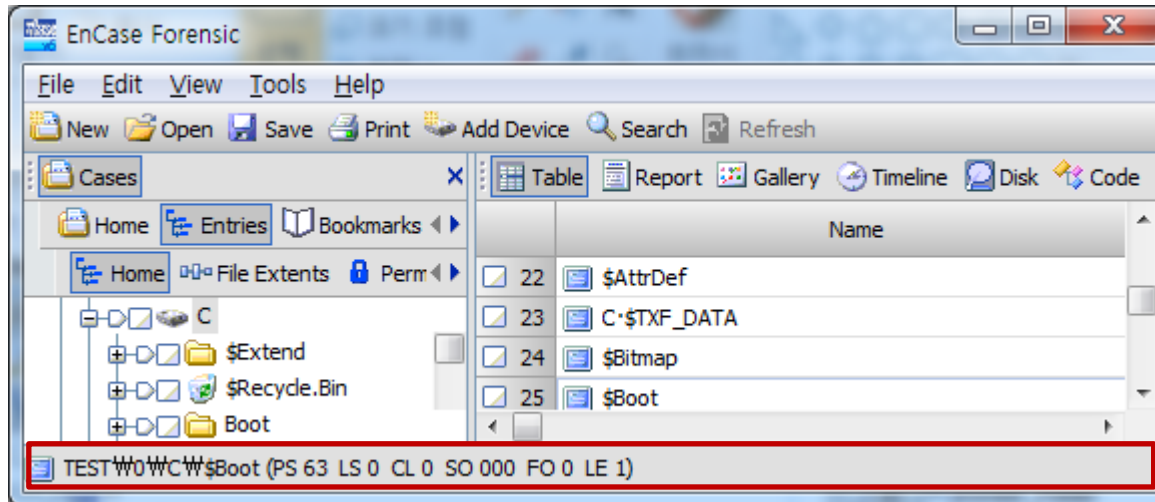
- 증거 형태 구분



- 로컬에서 라이브로 추가한 항목(장치, 볼륨)은 아이콘 오른쪽 하단에 파란색의 삼각형 표시
- 파일 형태의 이미지에서 마운트된 항목은 아이콘만 표시

네비게이션

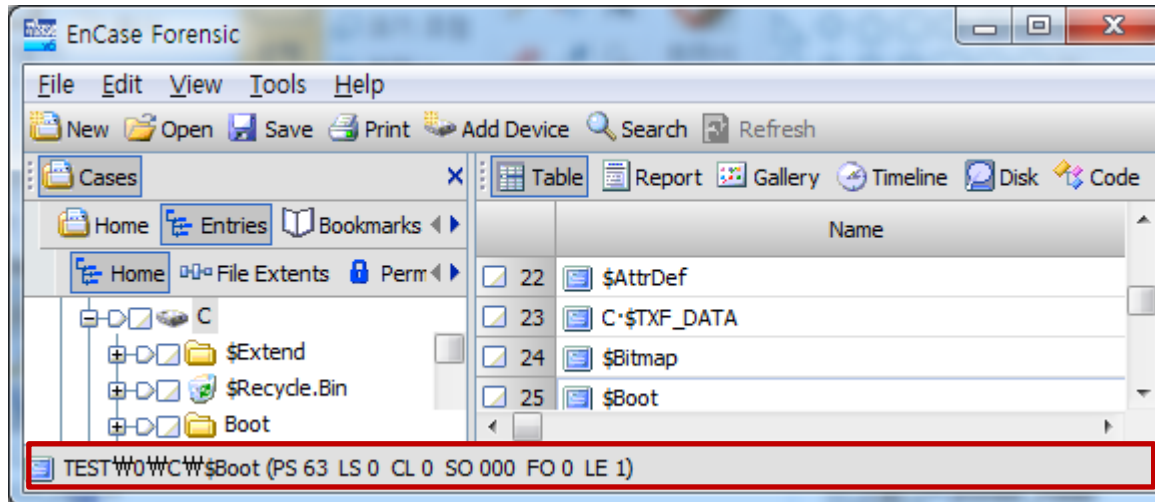
- 네비게이션(GPS) 상태바



- **PS** : RAW 이미지나 혹은 장치의 시작을 기준으로 한 섹터 위치 (물리적 섹터 위치)
- **LS** : 각 볼륨의 시작을 기준으로 한 섹터 위치 (논리적 섹터 위치)
- **CL** : 각 볼륨의 시작을 기준으로 한 클러스터 위치

네비게이션

- 네비게이션(GPS) 상태바



- **SO** : 선택한 파일을 섹터로 나누었을 때 현재 접근하는 섹터 내 바이트 위치 (최대 : 512)
- **FO** : 선택한 파일의 시작을 기준으로 한 바이트 위치 (최대 : 파일 크기)
- **LE** : 선택한 바이트 크기 (일반적으로 1, 마우스로 드래그할 경우 드래그한 크기)

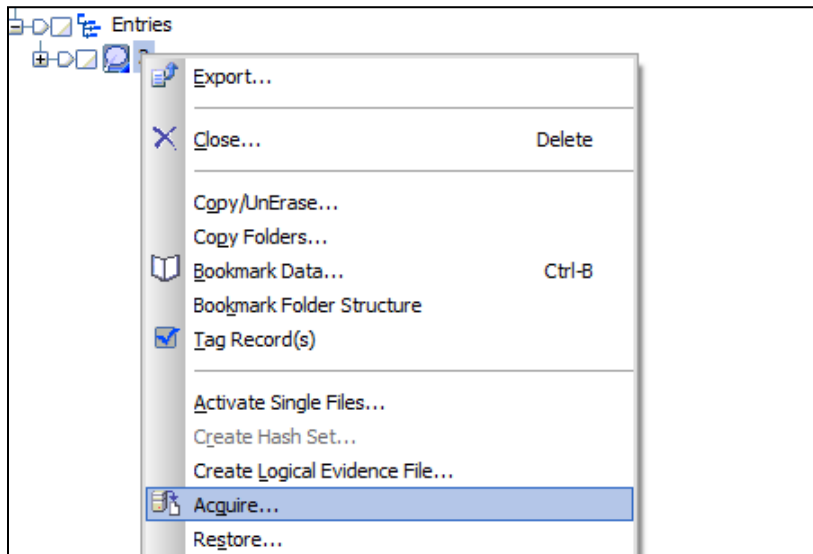
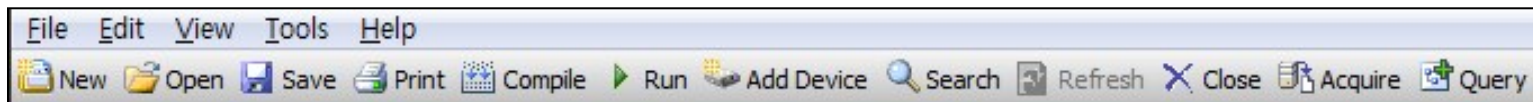
증거 획득

Security is a people problem...

이미징하기

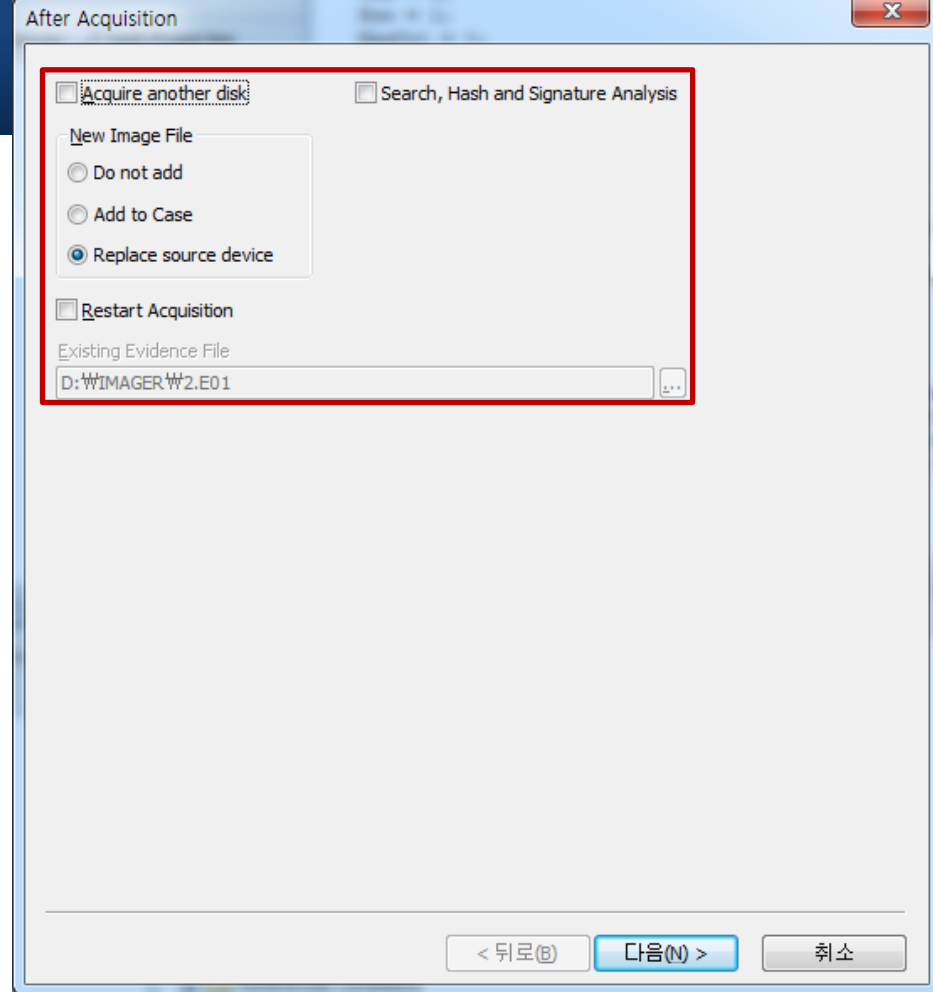
- **이미징 방법**

1. 이미징하고자 하는 대상(장치, 볼륨)을 마운트
2. "Acquire(Edit → Acquire)" 기능으로 이미징 수행



이미징 옵션 – After Acquisition

- **Acquire another disk**
 - 여러 디스크를 이미징 할 경우
- **Search, Hash and Signature Analysis**
 - 이미징과 함께 검색, 해쉬, 시그니처 분석
- **New Image File**
 - **Do not add** : 현재 케이스에 추가 X
 - **Add to Case** : 현재 케이스에 추가
 - **Replace source device** : 현재 케이스에 추가되어있는 원본 장치와 교체
- **Restart Acquisition**
 - 이미지 작업 재시작 (이미징 작업이 중단된 경우 다시 재시작 기능)



이미징 옵션 – Options

- **Name, Evidence Number, Notes**

- 이미지 파일명, 증거 번호, 메모

- **File Segment Size (MB)**

- 파일 조각 크기 (1MB ~ 2000MB)

- **Start Sector, Stop Sector**

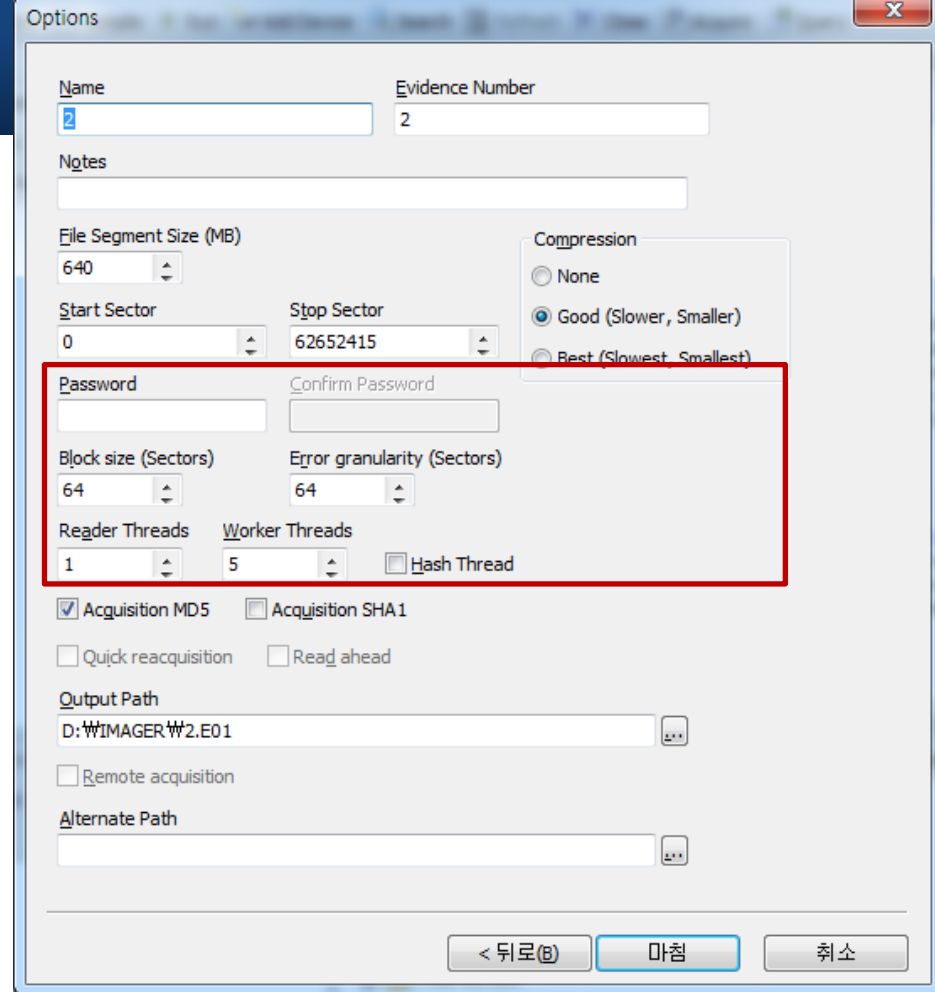
- 이미징 범위 지정

- **Compression**

- 압축(deflate) 여부 – None, Good, Best
- 압축을 하는 것/안 하는 것 중 어느 것이 이미징 시간을 줄여줄까?

이미징 옵션 – Options

- **Password**
 - 증거 파일을 패스워드로 보호(암호화 X)
- **Block Size (Sectors)**
 - 이미징 시 사용할 블록 크기
- **Error granularity (Sectors)**
 - 읽기 에러 발생 시 처리 방식
 - 사본에 영향을 미치는 정도
- **Reader Threads, Worker Threads, Hash Thread**
 - 읽기 스레드 수, 작업 스레드 수, 해쉬 작업에 할당할 스레드 생성 여부



이미징 옵션 – Options

- **Acquisition MD5**
 - 이미징 시 MD5 계산 여부
- **Acquisition SHA1**
 - 이미징 시 SHA1 계산 여부
- **Quick reacquisition**
 - 옵션 수정 후 재이미징
- **Read ahead**
 - 쓰기 작업 동안 원본의 읽기 작업을 수행
- **Output Path, Alternate Path**
 - 이미지 저장 경로, 저장 경로의 용량 부족 시 대체할 경로

Options

Name: [2] Evidence Number: [2]

Notes: []

File Segment Size (MB): [640]

Start Sector: [0] Stop Sector: [62652415]

Password: [] Confirm Password: []

Block size (Sectors): [64] Error granularity (Sectors): [64]

Reader Threads: [1] Worker Threads: [5] Hash Thread: []

☒ Acquisition MD5 ☐ Acquisition SHA1

☐ Quick reacquisition ☐ Read ahead

Output Path: [D:\WIMAGER\W2.E01] []

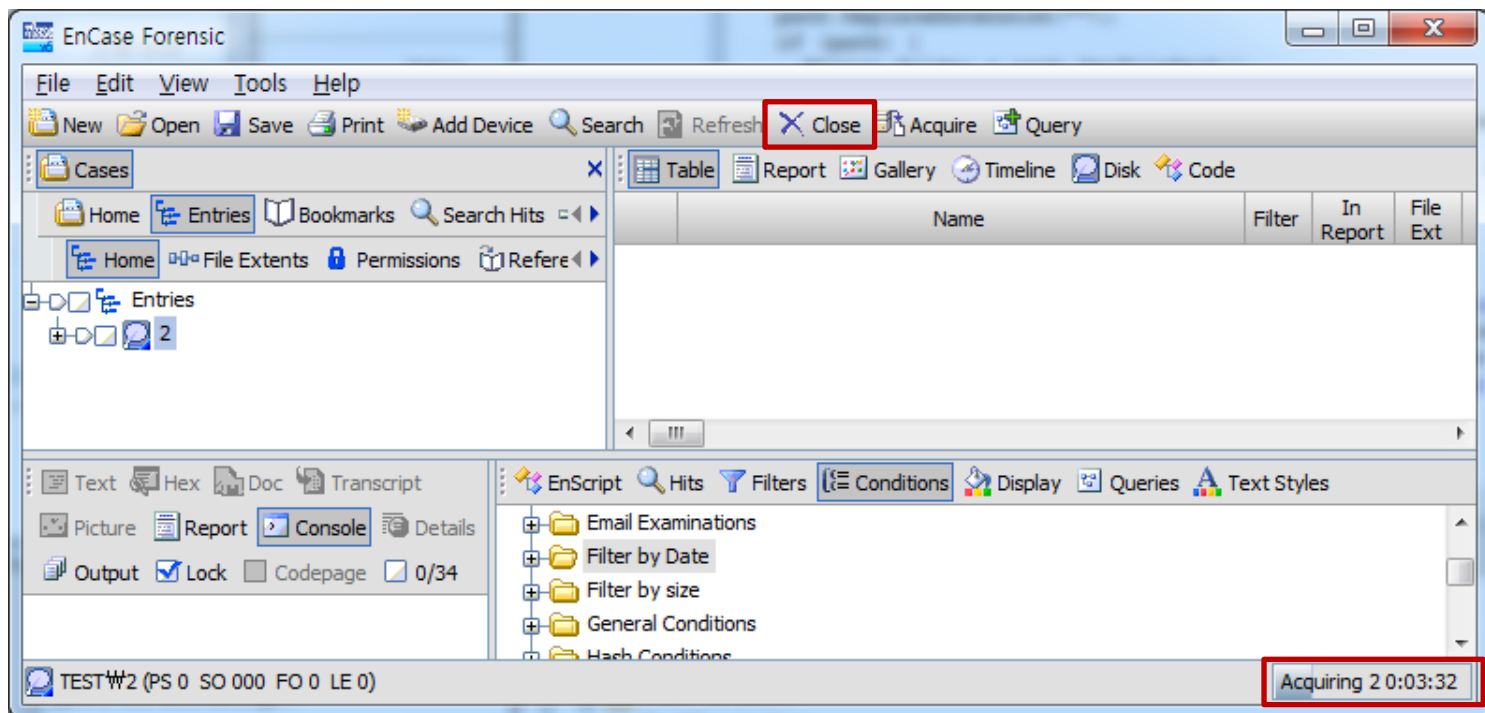
☐ Remote acquisition

Alternate Path: [] []

< 뒤로(B) 마침 취소

이미징 수행

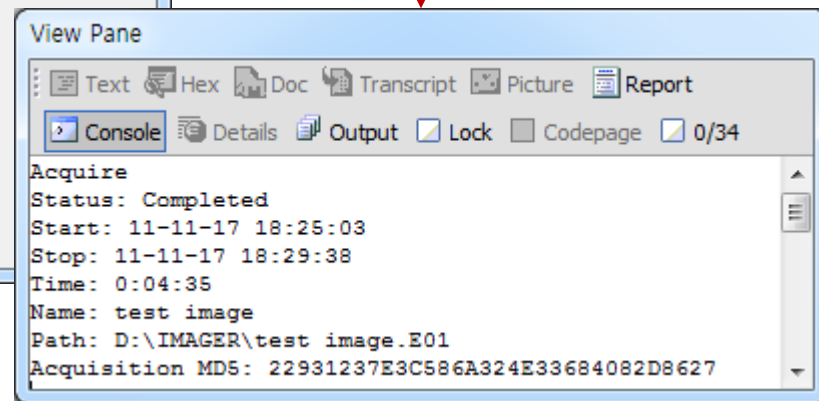
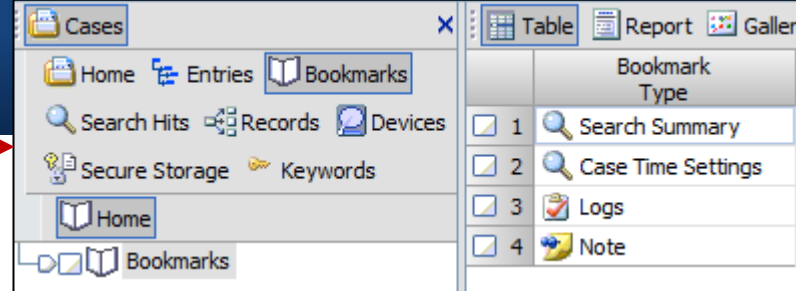
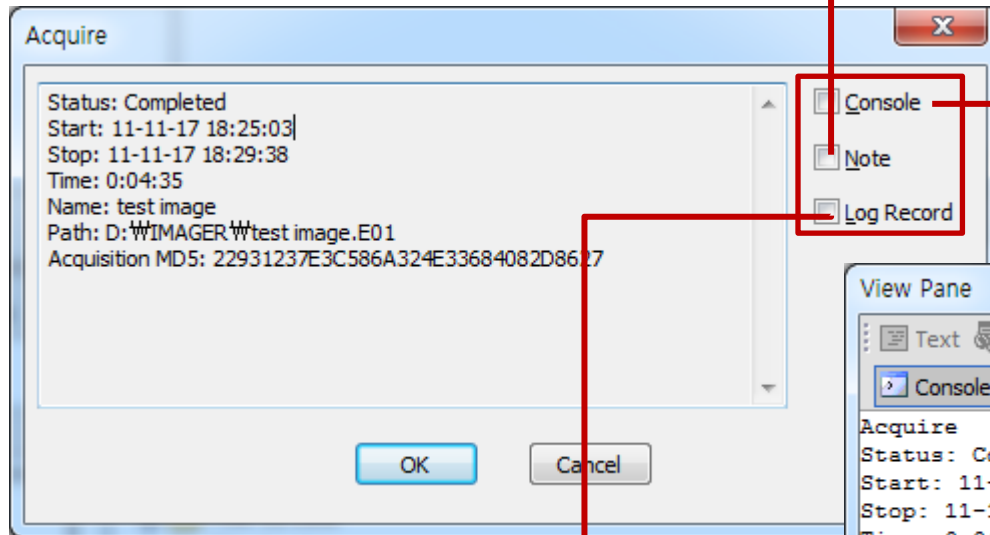
- 이미징 작업 중지
 - Edit → Close
 - 오른쪽 하단의 진행 프로그레스 바 더블 클릭



증거 획득

이미징 수행

- 이미징 작업 완료

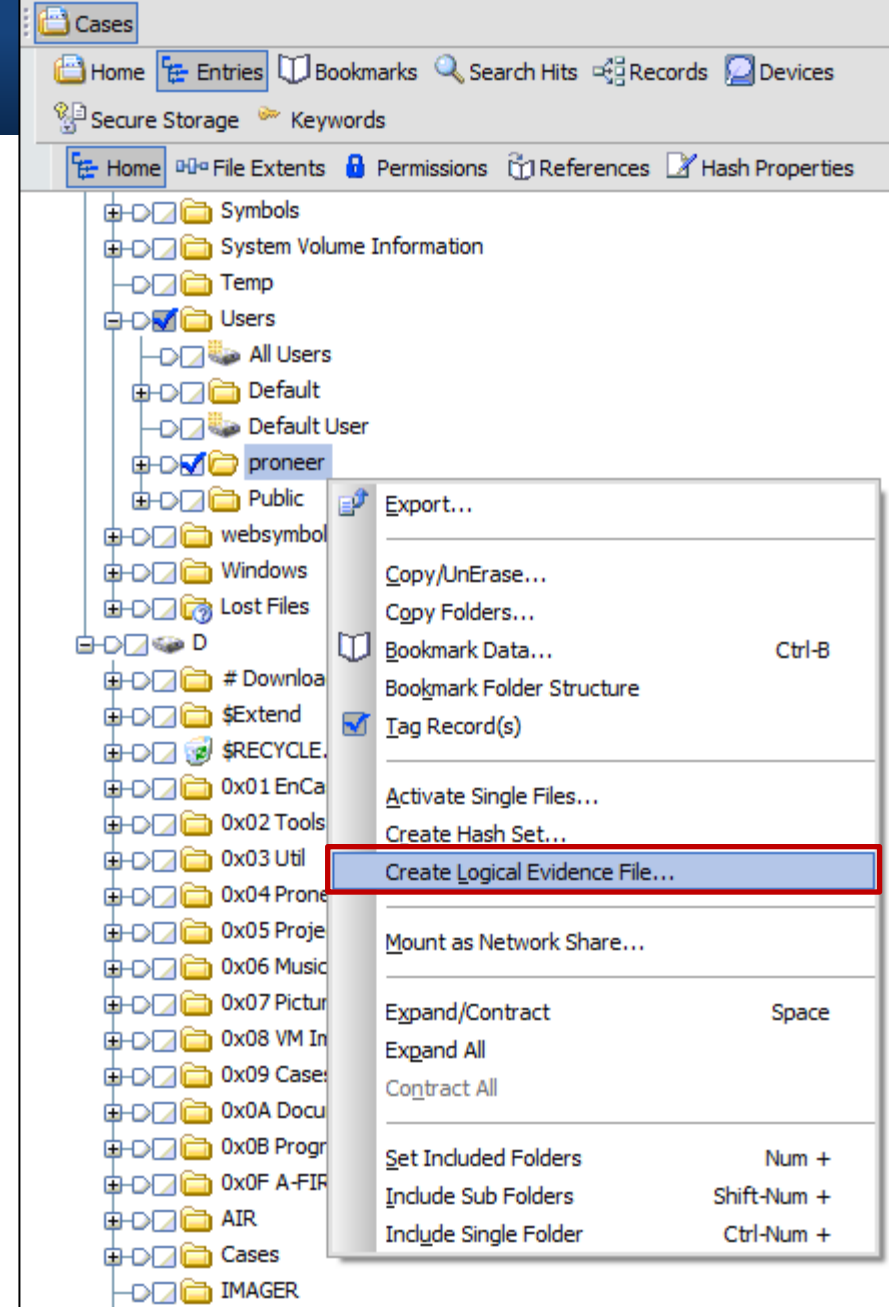


The 'Log Records' pane shows a table of acquisition logs:

	Name	Comment	Value	Created	Accessed
1	Status	Completed		11-11-17 18:29:38	
2	Start	11-11-17 18:25:03		11-11-17 18:29:38	
3	Stop	11-11-17 18:29:38		11-11-17 18:29:38	
4	Time	0:04:35		11-11-17 18:29:38	
5	Name	test image		11-11-17 18:29:38	
6	Path	D:\IMAGER\test im...		11-11-17 18:29:38	
7	Acquisition MD5	22931237E3C586A32...		11-11-17 18:29:38	

논리적 증거 파일 생성하기

- **Create Logical Evidence File...**
 - 생성하고자 하는 대상 폴더 선택
 - 마우스 우클릭 후 메뉴 선택



논리적 증거 파일 생성하기

- **Source, Files**

- 선택한 폴더 정보

- **Target folder within Evidence File**

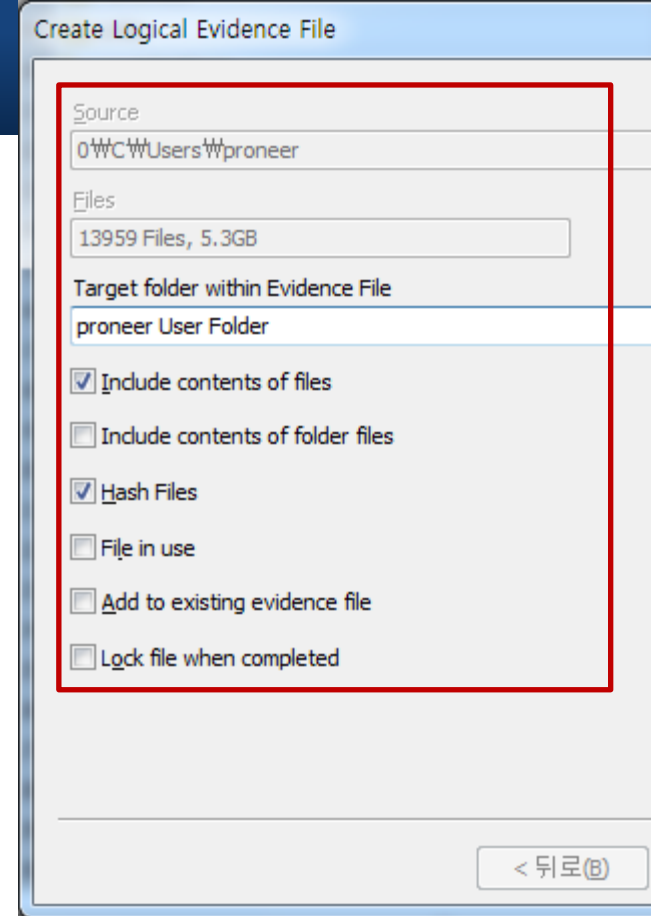
- EnCase에 로드 시 표시되는 폴더 이름

- **Include contents of files (default)**

- 파일의 내용 포함 여부(해제한다면 파일 이름만 포함)

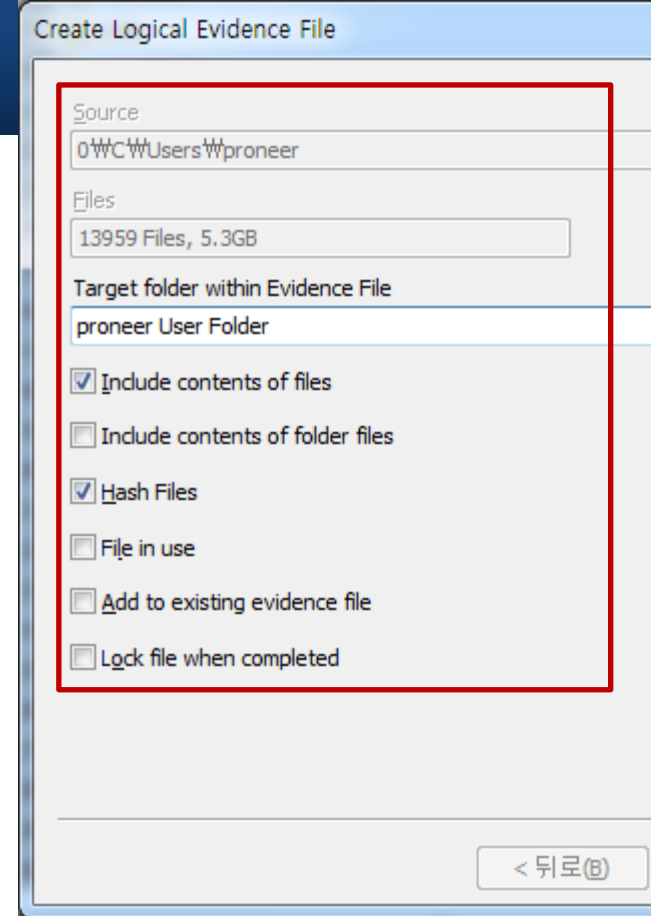
- **Hash Files (default)**

- 선택한 파일의 해쉬값 계산 (이미 계산된 경우에는 계산 없이 추가)



논리적 증거 파일 생성하기

- **Include contents of folder files**
 - 폴더에 대한 바이너리 데이터 포함 여부
- **File in use**
 - 추가된 파일이 사용되고 있는 파일인지 여부
- **Add to existing evidence file**
 - 이미 생성한 논리적 증거파일에 덧붙임
- **Lock file when completed**
 - 새로운 증거 파일을 추가하지 못하도록 닫음
 - CD, DVD의 멀티세션 기능



증거 획득

논리적 증거 파일 생성하기

- **Name, Evidence Number, Notes**

- 증거 파일명, 증거 번호, 메모

- **File Segment Size (MB)**

- 파일 조각 크기

- **Output Path**

- 증거 파일 저장 경로

- **Compression**

- 압축 여부 (None, Good, Best)

Create Logical Evidence File

Name: Evidence Number:

Notes:

File Segment Size (MB): 640

Compression:

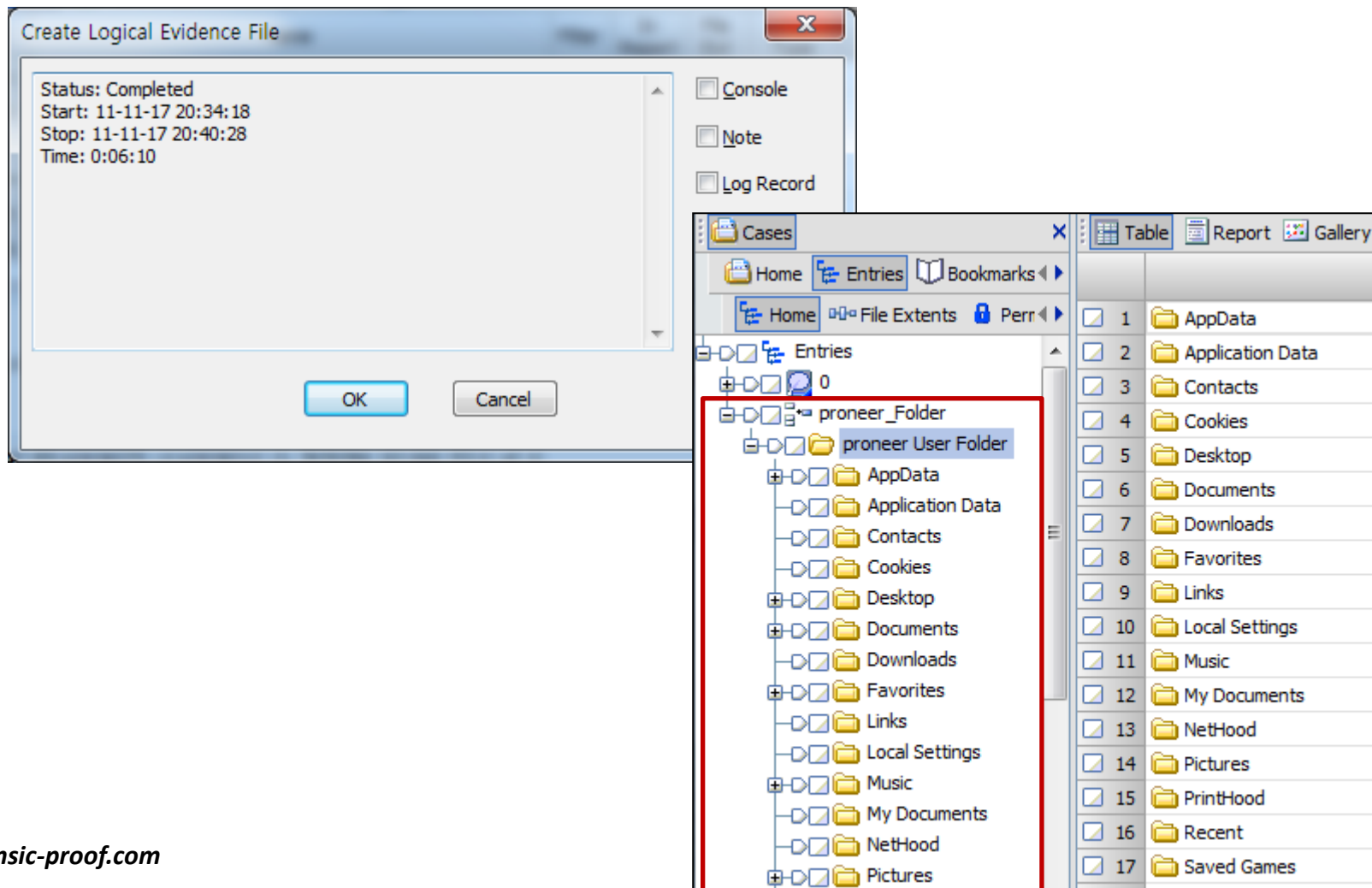
- ☐ None
- ☒ Good (Slower, Smaller)
- ☐ Best (Slowest, Smallest)

Output Path:

< 뒤로(B) 마침 취소

논리적 증거 파일 생성하기

- 생성 완료



실습

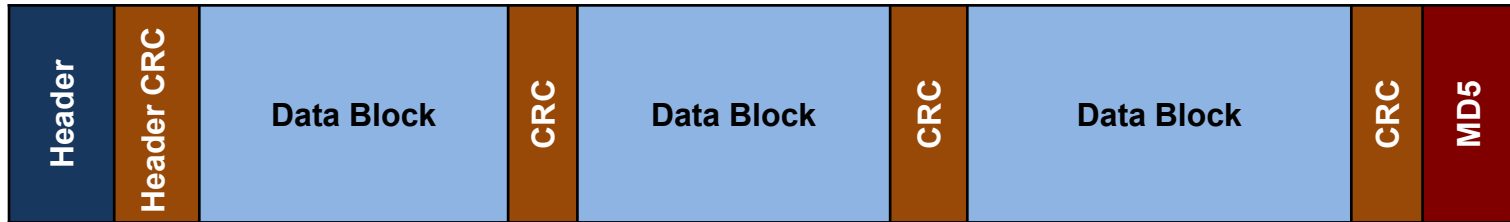
- **Single File을 이용한 논리적 증거 파일 생성**
 - 이벤트 로그 파일(시스템, 애플리케이션, 보안)을 "Single File"로 케이스에 추가한 후 논리적 증거 파일을 생성하라.
 - **이벤트 로그 파일 경로**
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\
 - 하위키 System, Application, Security의 "File" 값 확인
 - **이벤트 로그 기본 경로**
 - **Windows XP 이하** : %SystemRoot%\System32\config\
 - **Windows Vista 이상** : %SystemRoot%\System32\winevt\Logs\

증거 파일 포맷

Security is a people problem...

E01 파일 포맷

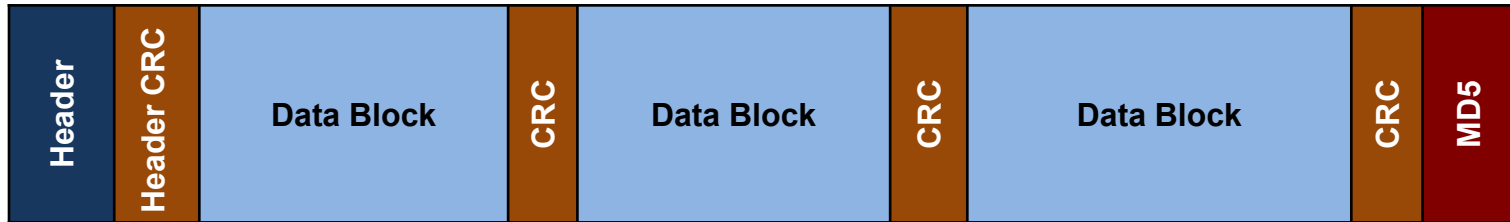
- 포맷 구조



- 헤더와 각 블록마다 CRC 값이 계산되어 저장
- 파일의 마지막에 CRC를 제외하고 데이터 블록만 가지고 계산한 MD5 값 저장

E01 파일 포맷

- 포맷 구조

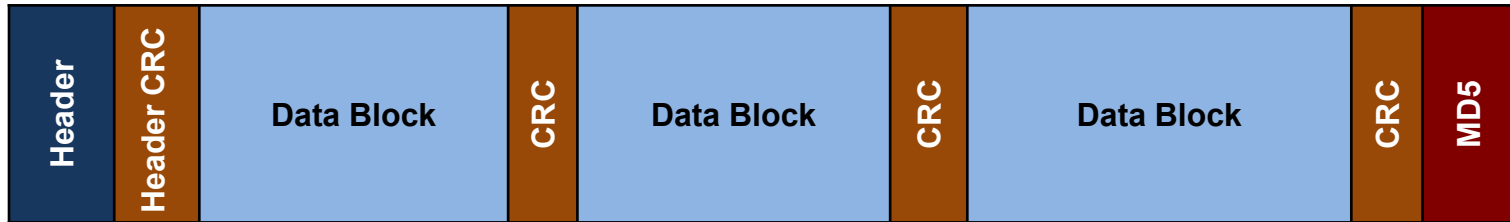


- 헤더에 포함되는 정보

- Evidence Name
- Evidence Number
- Notes
- Date / Time of acquisition
- Version of EnCase used for acquisition
- Operating System

E01 파일 포맷

- 포맷 구조

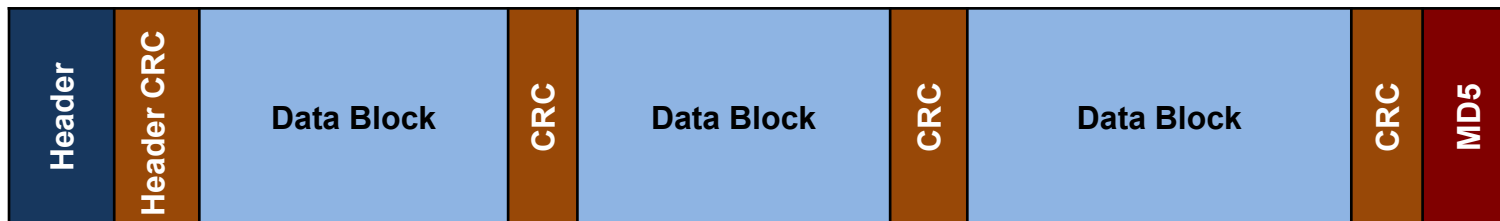


- 데이터 블록

- 블록 크기 : 기본적으로 64 섹터 (최대 32,768 섹터)
 - 데이터 블록을 메모리 로드 후, CRC와 MD5(누적) 계산

E01 파일 포맷

- 포맷 구조

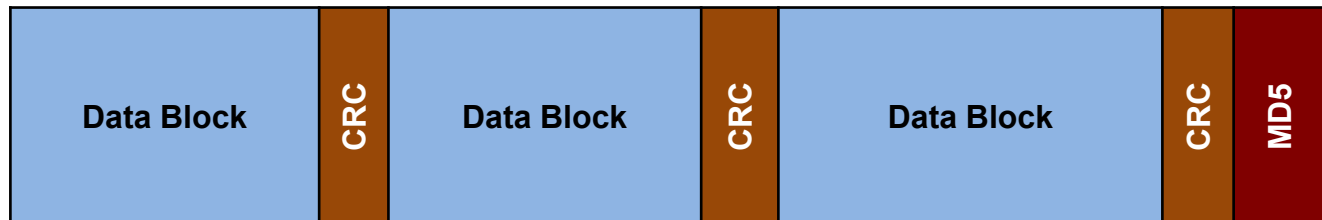
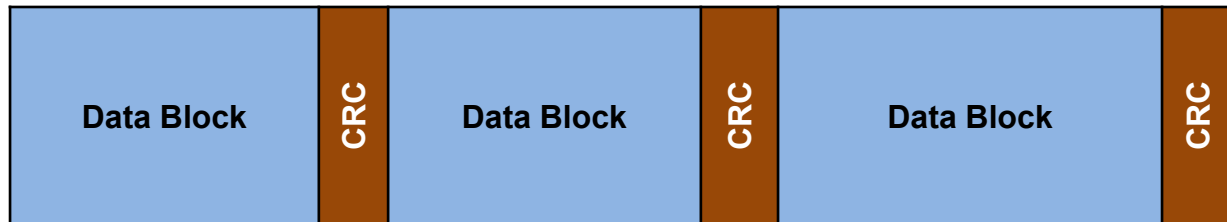
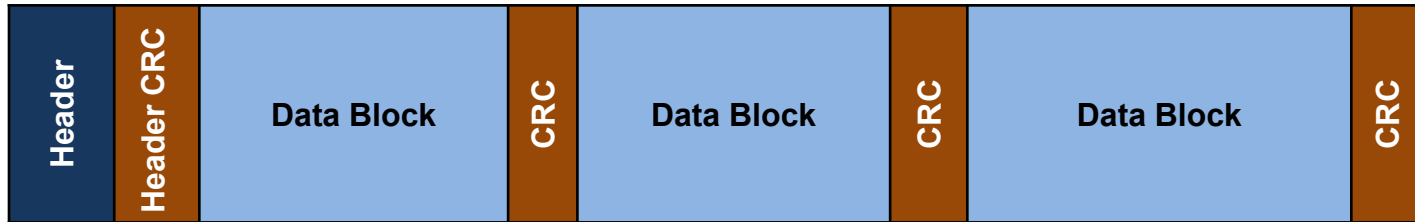


- 압축

- 평균적으로 "Best" 압축을 사용할 경우, 50%의 압축 효율을 보임
- 비할당 영역이 0을 많이 포함할수록 압축률 향상
- 압축을 사용할 경우("Good"), 일반적으로 이미징 속도 향상
- "Best" 압축의 경우에는 약 3배가량 늦어짐
- 압축시 데이터 블록만 압축되는가? 아니면 CRC 까지도 압축되는가?

E01 파일 포맷

- 포맷 구조



증거 파일 정보

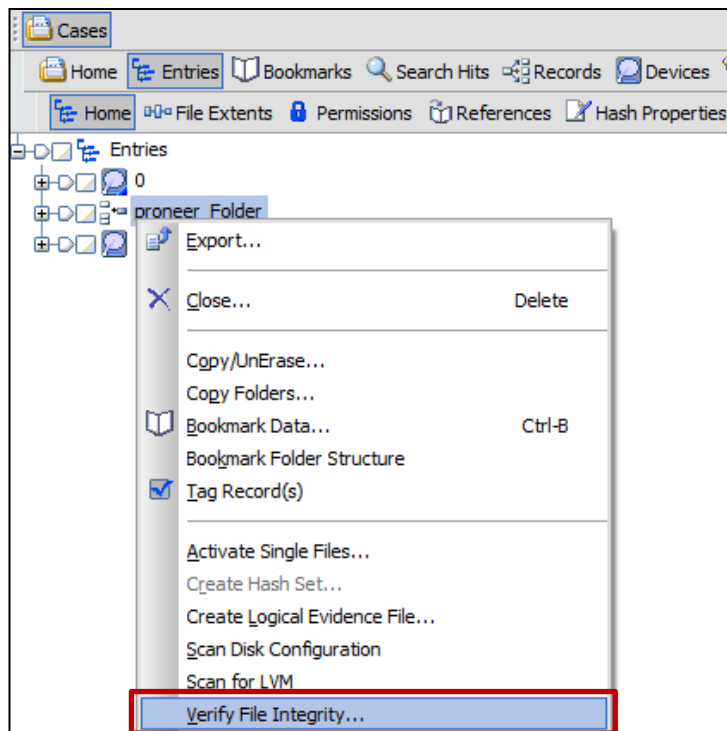
- **E01 파일명 생성 규칙**
 - < 100 : e01 – e99
 - > 100 : eaa – eff
- **1 TB의 저장매체를 이미징할 경우**
 - 1 TB보다 큰 저장매체 필요
 - 500 GB 저장매체 2개 사용 가능 (Alternate Path)
 - 압축을 사용할 경우, 750 GB의 저장매체를 준비하는 것이 적절

증거 파일 검증

Security is a people problem...

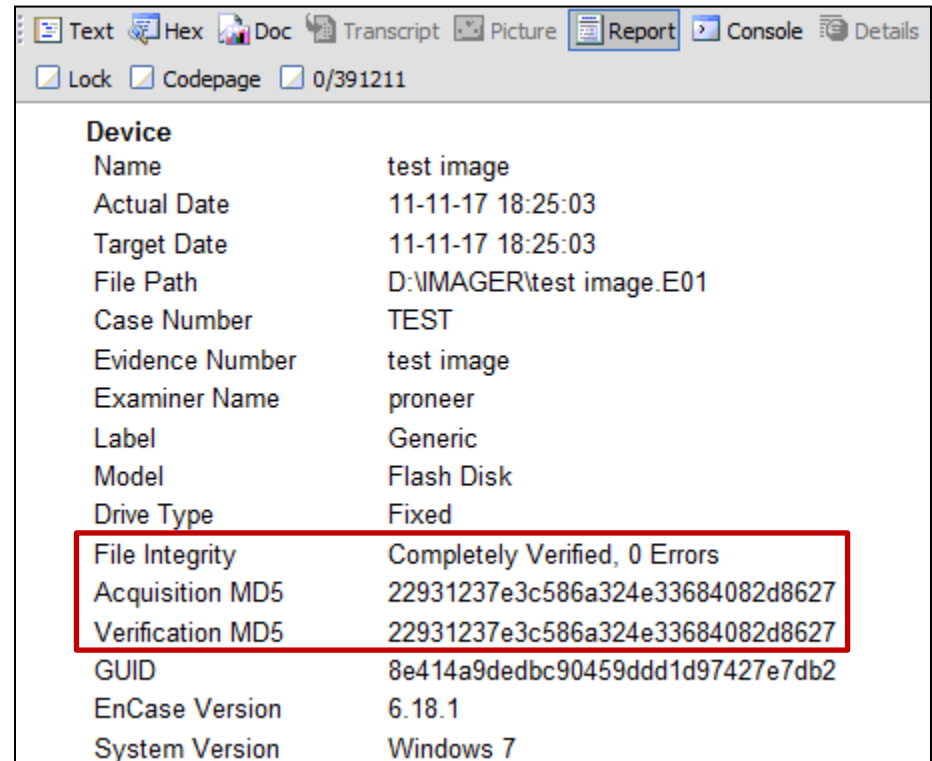
파일 무결성 검사

- 무결성 검사 방법
 - 증거 파일 추가 시 자동으로 파일 무결성 검증
 - 증거(이미지, 논리적 증거 파일) 우클릭 후 "Verify File Integrity..." 선택

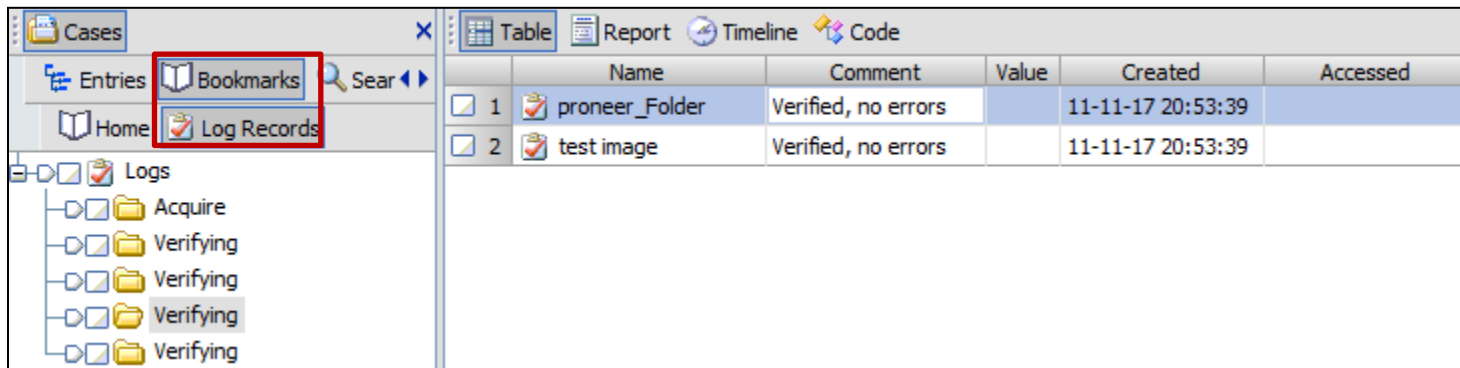


파일 무결성 검사

- 무결성 검사 결과 확인
 - 장치 보고서를 통해 확인
 - 북마크 "Log Records"를 통해 확인



Device	
Name	test image
Actual Date	11-11-17 18:25:03
Target Date	11-11-17 18:25:03
File Path	D:\IMAGER\test image.E01
Case Number	TEST
Evidence Number	test image
Examiner Name	proneer
Label	Generic
Model	Flash Disk
Drive Type	Fixed
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	22931237e3c586a324e33684082d8627
Verification MD5	22931237e3c586a324e33684082d8627
GUID	8e414a9dedbc90459ddd1d97427e7db2
EnCase Version	6.18.1
System Version	Windows 7



Cases					
Entries	Bookmarks	Search			
Home	Log Records				
Logs					
Acquire					
Verifying					
Verifying					
Verifying					
Verifying					

	Name	Comment	Value	Created	Accessed
1	proneer_Folder	Verified, no errors		11-11-17 20:53:39	
2	test image	Verified, no errors		11-11-17 20:53:39	

