EnCase Seminar #3
(EnCase Concepts & Environment)

FORENSIC-PROOF.COM

PRONEER

Welcome to EnCase Seminar!!

Security is a people problem….

Introduction

Outline

- ✓ ~~**Week 1 : Hardware and File system Analysis (Chapter 1, 2)**~~
- ✓ ~~**Week 2 : Acquiring Digital Evidence (Chapter 4)**~~
- ✓ Week 3 : EnCase Concepts and Environment (Chapter 5, 6)
- ✓ Week 4 : Actual Test
- ✓ Week 5 : Actual Test
- ✓ Week 6 : Actual Test
- ✓ Week 7 : Actual Test
- ✓ ..
- ✓ PS : EnScripting

EnCase Concepts

- *EnCase Evidence File*
- *CRC and MD5*
- *EnCase Evidence File Format*
- *Evidence File Verification*
- *Hashing Disks and Volumes*
- *EnCase Case File*
- *EnCase Backup File*
- *Configuration, or .ini, files*

EnCase Concepts

- ***EnCase Evidence File***
- *CRC and MD5*
- *EnCase Evidence File Format*
- *Evidence File Verification*
- *Hashing Disks and Volumes*
- *EnCase Case File*
- *EnCase Backup File*
- *Configuration, or .ini, files*

EnCase Concepts

EnCase Evidence File Format

✓ **dd (disk dump) vs. EnCase Evidence File**

- **dd image** : bit-for-bit 복사
- **EnCase Evidence File** : bit-for-bit 복사 + “chain of custody”를 위한 정보

EnCase Concepts

- *EnCase Evidence File*
- ***CRC and MD5***
- *EnCase Evidence File Format*
- *Evidence File Verification*
- *Hashing Disks and Volumes*
- *EnCase Case File*
- *EnCase Backup File*
- *Configuration, or .ini, files*

EnCase Concepts

CRC and MD5

✓ **MD5 (Message Digest 5)**

- 스트림 데이터(파일, 장치 등)에 적용할 수 있는 암호학적인 해쉬 알고리즘
- 출력은 128-bit(32 characters) 16진수 값 (2^{128})
- 데이터 스트림의 무결성을 입증하기 위한 방안

✓ **CRC (Cyclical Redundancy Check)**

- MD5 와 같이 스트림 데이터의 무결성을 입증하기 위한 해쉬 함수
- 출력은 32-bit 16진수 값 (2^{32})

✓ MD5는 CRC에 비해 많은 계산량이 요구되며 느린 단점

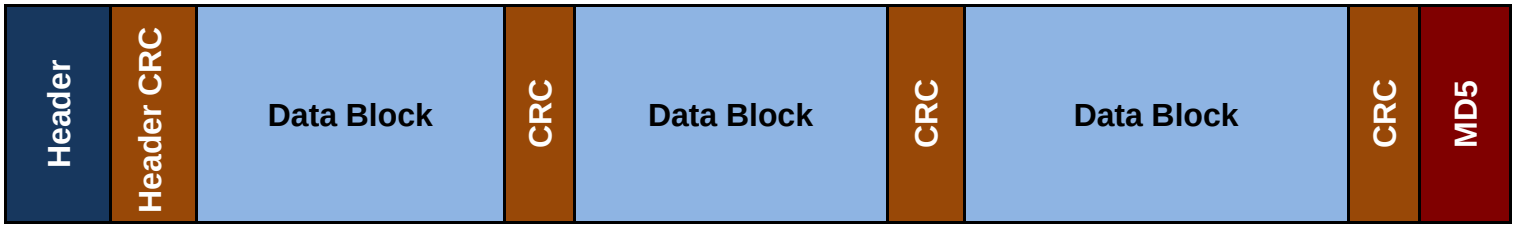
✓ EnCase Evidence File은 MD5와 CRC를 사용하여 효율적으로 증거 이미지 파일의 무결성 입증

EnCase Concepts

- *EnCase Evidence File*
- *CRC and MD5*
- ***EnCase Evidence File Format***
- *Evidence File Verification*
- *Hashing Disks and Volumes*
- *EnCase Case File*
- *EnCase Backup File*
- *Configuration, or .ini, files*

EnCase Concepts

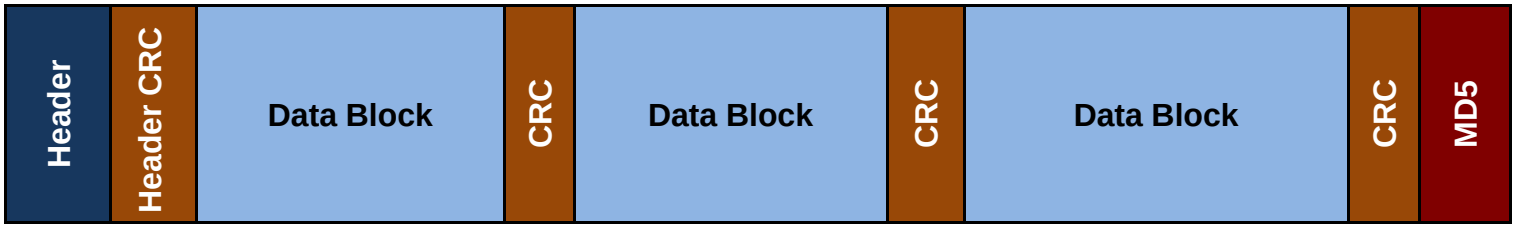
EnCase File Components and Function



- ✓ 헤더와 각 데이터 블럭마다 CRC 값이 계산되어 저장
- ✓ 증거 이미지의 마지막에 CRC를 제외한 데이터 블록만으로 계산한 MD5 값 포함

EnCase Concepts

EnCase File Components and Function

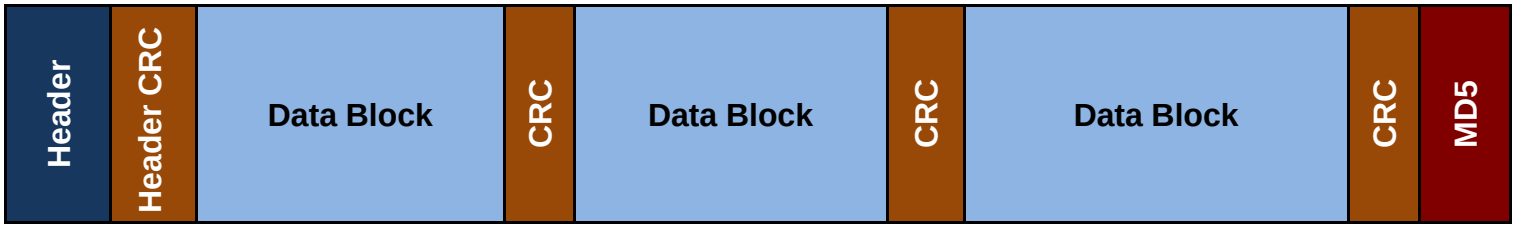


✓ **Header Information**

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

EnCase Concepts

EnCase File Components and Function

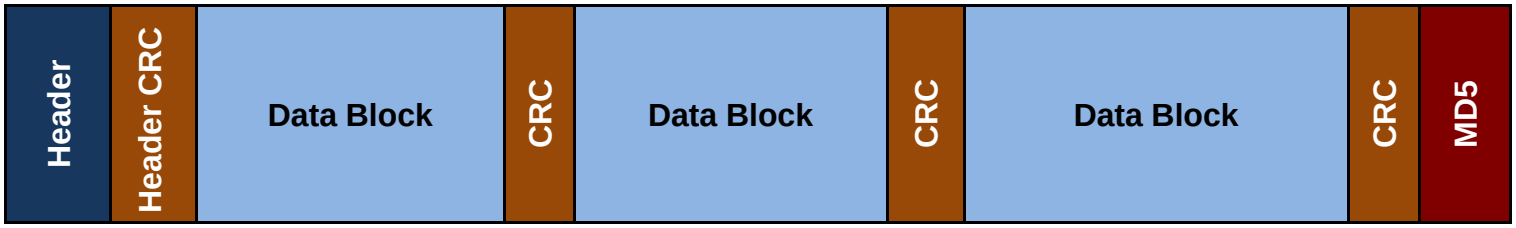


✓ **Data Block**

- Block Size : Default 64 sectors (maximum 32,768 sectors)
- 데이터 블록이 메모리에 로드된 후 CRC와 MD5(누적)를 계산

EnCase Concepts

EnCase File Components and Function



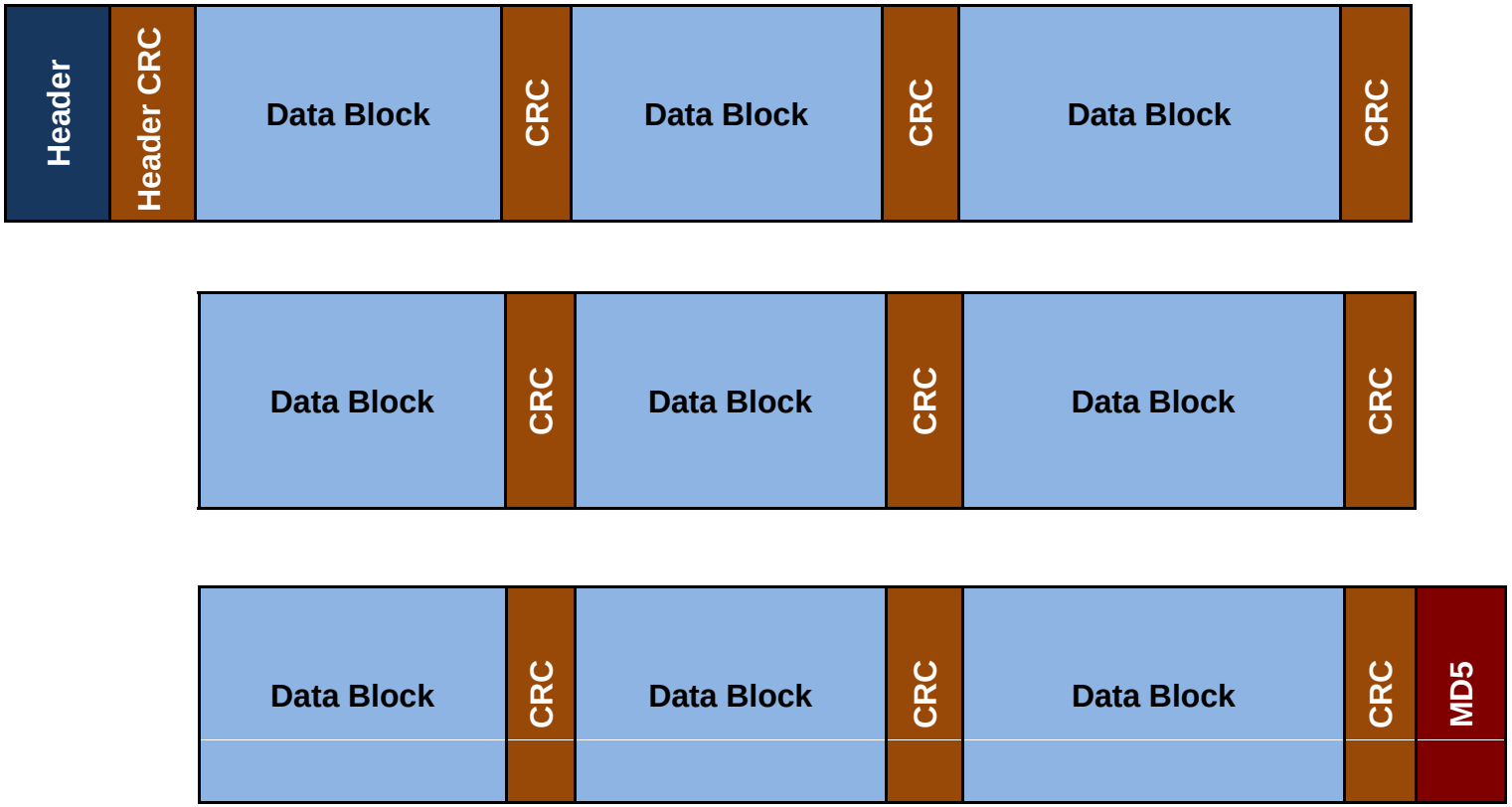
✓ **Compress**

- 평균적으로 "best" 압축 방식을 사용할 경우 50%의 효율을 보임
- 비할당 영역이 0을 많이 포함할 수록 압축률 향상
- 압축을 할 경우 증거 획득(이미징) 속도 증가
- "best" 압축 방식일 경우 약 3배 가량 늦어짐
- 압축을 할 경우 데이터만 압축될 것인가? 아님 CRC 까지 함께 압축될 것인가?

  ➔ CRC 도 함께 압축되어 저장

EnCase Concepts

- EnCase File Components and Function



EnCase Concepts

EnCase File Components and Function

✓ **EnCase Evidence File 이름 생성 규칙**

- < 100 : .e01 ~ .e99
- > 100 : .eaa, .eab, .eac…

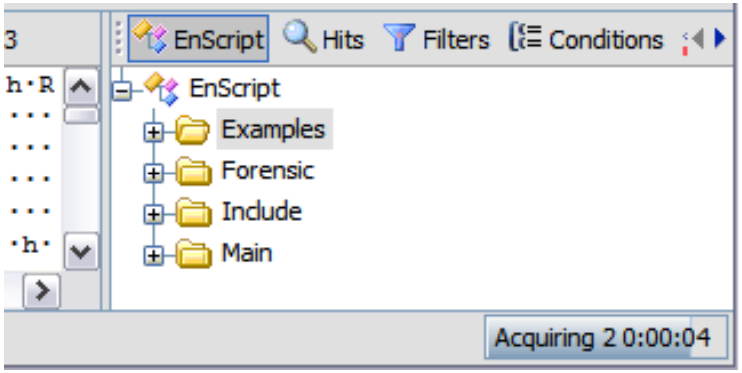
✓ **100 GB 하드디스크를 이미징 할 경우**

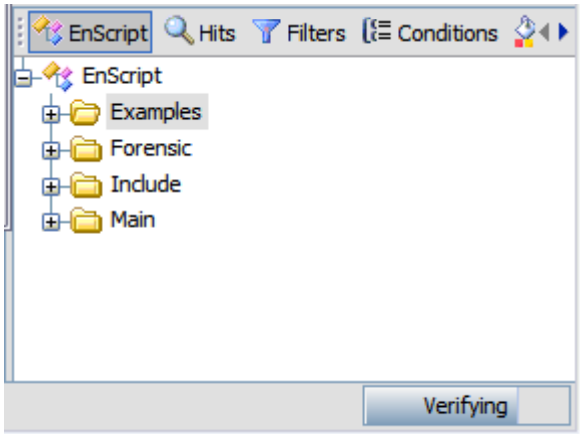
- 100 GB 보다 큰 저장용 디스크 필요 (부가적인 정보)
- 60 GB 하드디스크 2개 사용 가능 (Alternate Path)
- 압축을 사용할 경우 75 GB의 저장용 디스크를 준비하는 것이 적절

EnCase Concepts

- *EnCase Evidence File*
- *CRC and MD5*
- *EnCase Evidence File Format*
- ***Evidence File Verification***
- *Hashing Disks and Volumes*
- *EnCase Case File*
- *EnCase Backup File*
- *Configuration, or .ini, files*

Evidence File Verification





✓ 증거 파일(.EXX)을 Case 에 추가할 때 자동으로 증거 파일에 대한 검증

Evidence File Verification

Text | Hex | Doc | Transcript | Picture | Report | Console | Details | Output | Lock | Codepage | 0/647607

Target Date	09/25/09 11:08:18오후
File Path	C:\Documents and Settings\proneer\바탕 화면\2.E01
Case Number	Case 1
Evidence Number	2
Examiner Name	PRONEER
Label	SanDisk
Model	Cruzer Mini
Drive Type	Fixed
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	405783148e85830660cc1334266eacc6
Verification MD5	405783148e85830660cc1334266eacc6
GUID	7660e752ff984c44bd3215cf46257f5f
EnCase Version	6.13
System Version	Windows XP
Is Physical	•
Raid Stripe Size	0
Error Granularity	64
Process ID	0
Index File	C:\Program Files\EnCase6\Index\2-7660e752ff984c44bd3215cf46257f5f.Index
Read Errors	0
Missing Sectors	0
CRC Errors	0
Compression	Good
Total Size	256,900,608 Bytes (245MB)
Total Sectors	501,759
Disk Signature	00000000
Partitions	Valid

Evidence File Verification

Text | Hex | Doc | Transcript | Picture | Report | Console | Details | Output | Lock | Codepage | 0/647607

Target Date	09/25/09 11:08:18오후
File Path	C:\Documents and Settings\proneer\바탕 화면\2.E01
Case Number	Case 1
Evidence Number	2
Examiner Name	PRONEER
Label	SanDisk
Model	Cruzer Mini
Drive Type	Fixed
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	405783148e85830660cc1334266eacc6
Verification MD5	405783148e85830660cc1334266eacc6
GUID	7660e752ff984c44bd3215cf46257f5f
EnCase Version	6.1
System Version	Wir
Is Physical	•
Raid Stripe Size	0
Error Granularity	64
Process ID	0
Index File	C:\F
Read Errors	0
Missing Sectors	0
CRC Errors	0
Compression	Goo
Total Size	256
Total Sectors	501
Disk Signature	000
Partitions	Vali

Acquire

Status: Completed
Start: 09/25/09 11:08:18오후
Stop: 09/25/09 11:08:50오후
Time: 0:00:32
Name: 2
Path: C:₩Documents and Settings₩proneer₩바탕 화면₩2.E01
GUID: 7660E752FF984C44BD3215CF46257F5F
Acquisition MD5: 405783148E85830660CC1334266EACC6

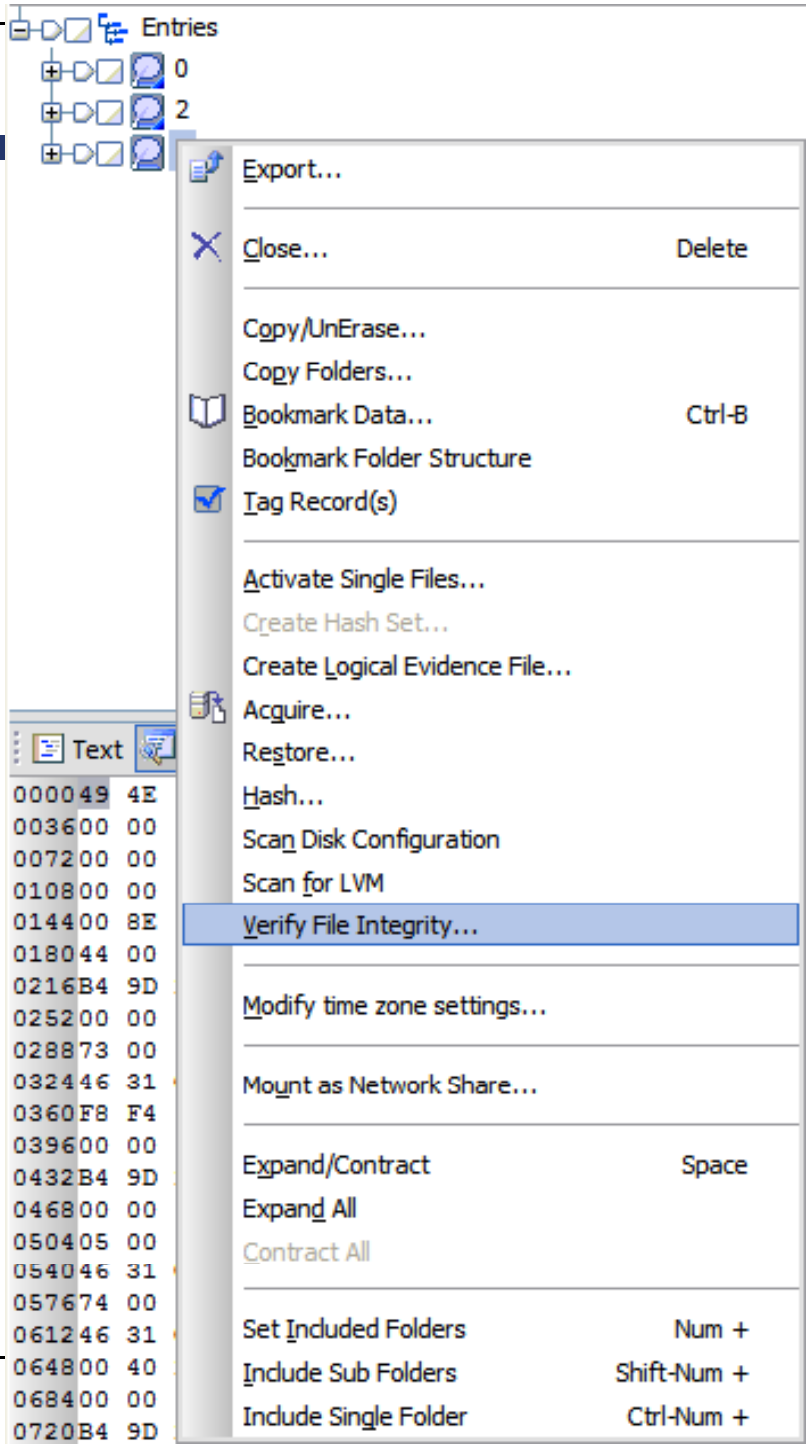
☐ Console
☐ Note
☐ Log Record

OK | Cancel

EnCase Concepts

Evidence File Verification

✓ 획득한 이후 파일의 무결성 검증



EnCase Concepts

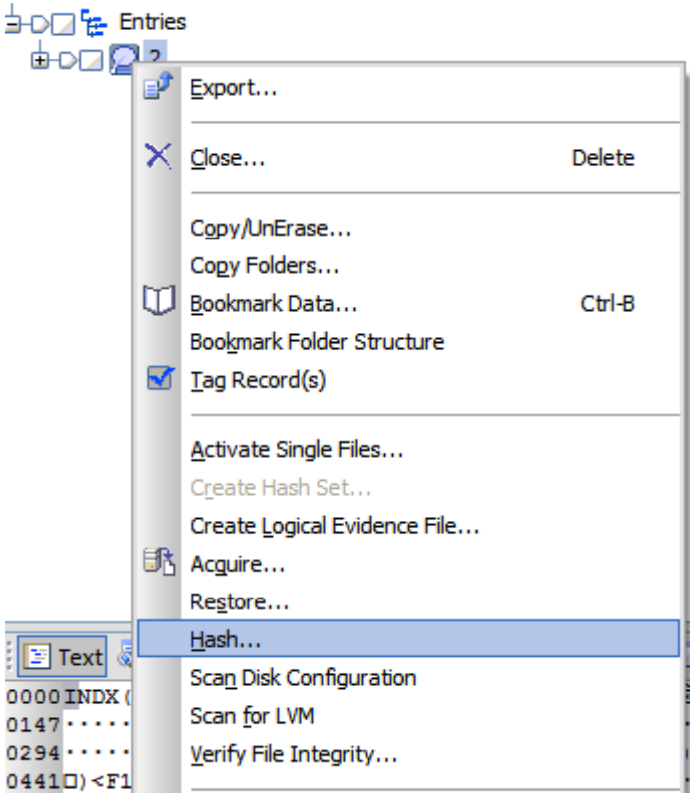
- **Evidence File Verification**

  - ✓ Exercise 5.1 ➔ Go Go~~

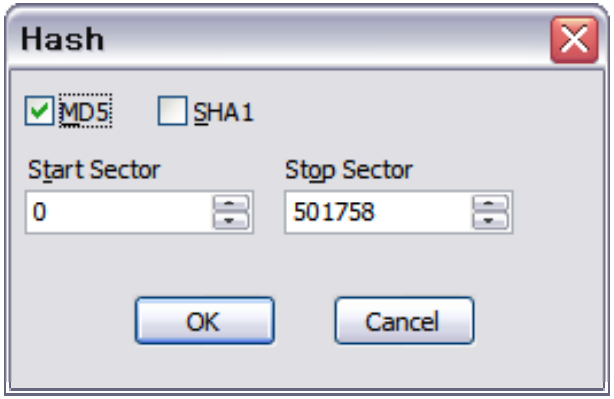
EnCase Concepts

- *EnCase Evidence File*
- *CRC and MD5*
- *EnCase Evidence File Format*
- *Evidence File Verification*
- ***Hashing Disks and Volumes***
- *EnCase Case File*
- *EnCase Backup File*
- *Configuration, or .ini, files*

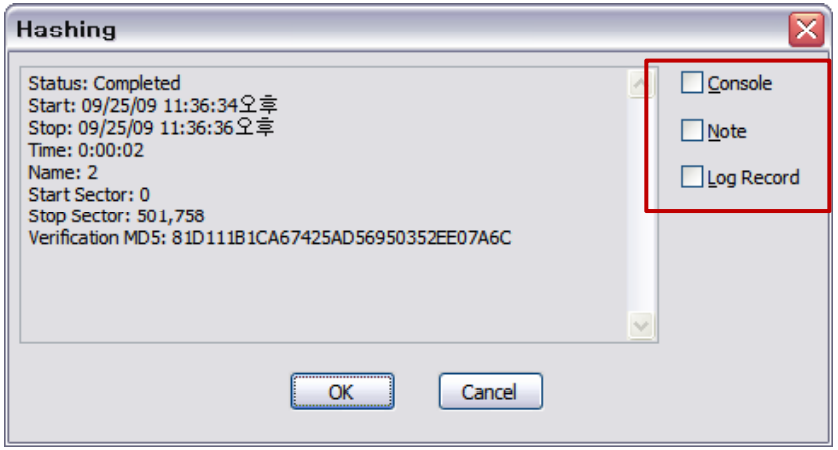
Hashing Disks and Volumes



- ✓ **Verify File Integrity** : 장치 레벨에서의 전체 해쉬
- ✓ **Hash** : 정해진 영역의 해쉬 가능



Hashing Disks and Volumes



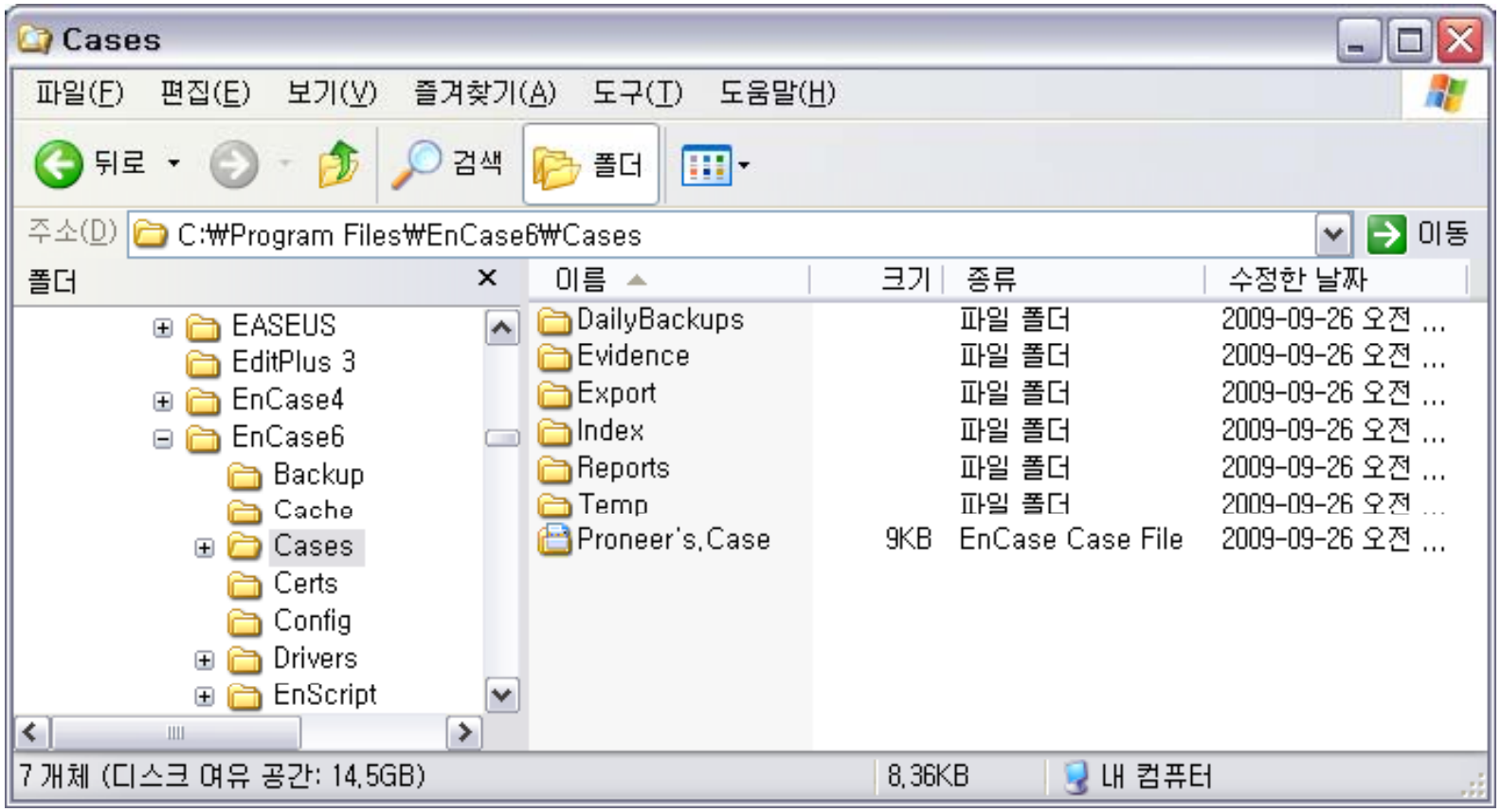
- ✓ Console : 콘솔 창에 출력
- ✓ Note : Bookmarks ➔ Logs 에 내용 저장
- ✓ Log Record ?

EnCase Concepts

- *EnCase Evidence File*
- *CRC and MD5*
- *EnCase Evidence File Format*
- *Evidence File Verification*
- *Hashing Disks and Volumes*
- ***EnCase Case File***
- *EnCase Backup File*
- *Configuration, or .ini, files*

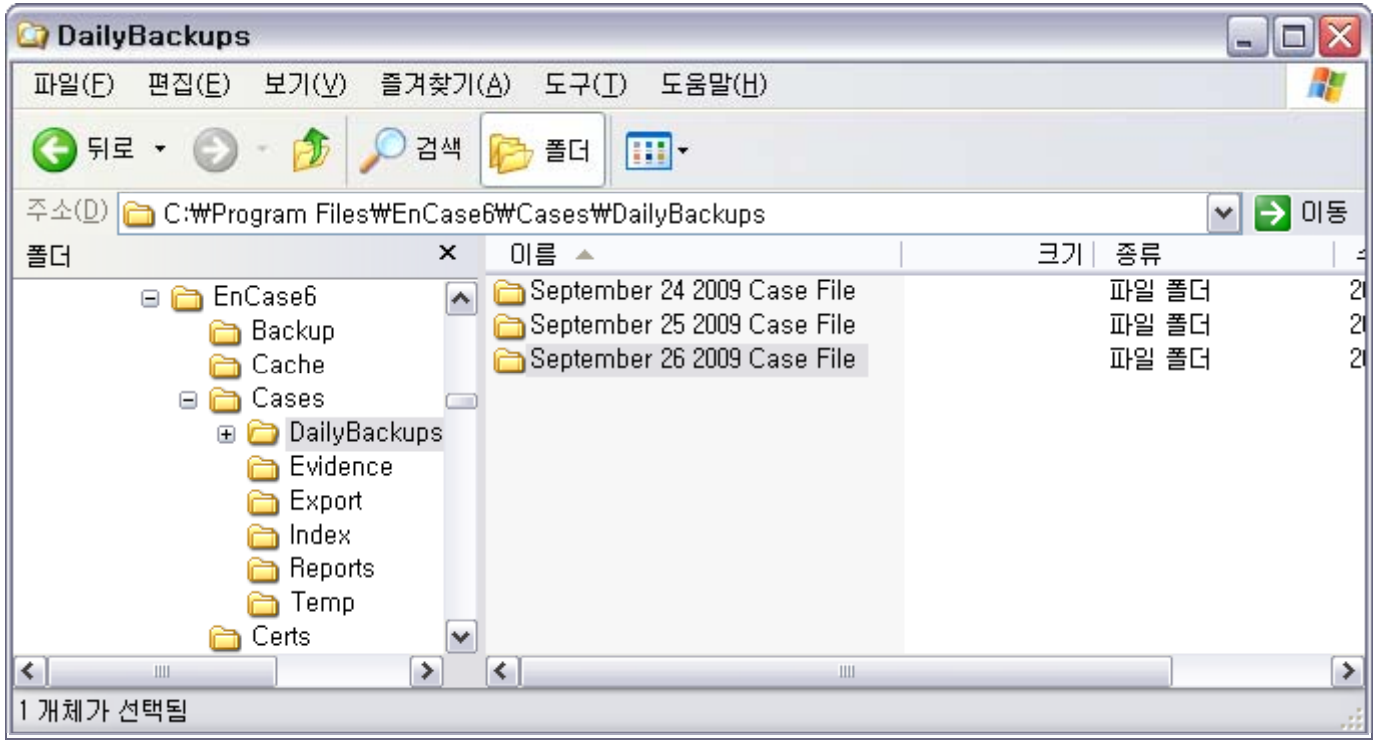
EnCase Concepts

EnCase Case Files

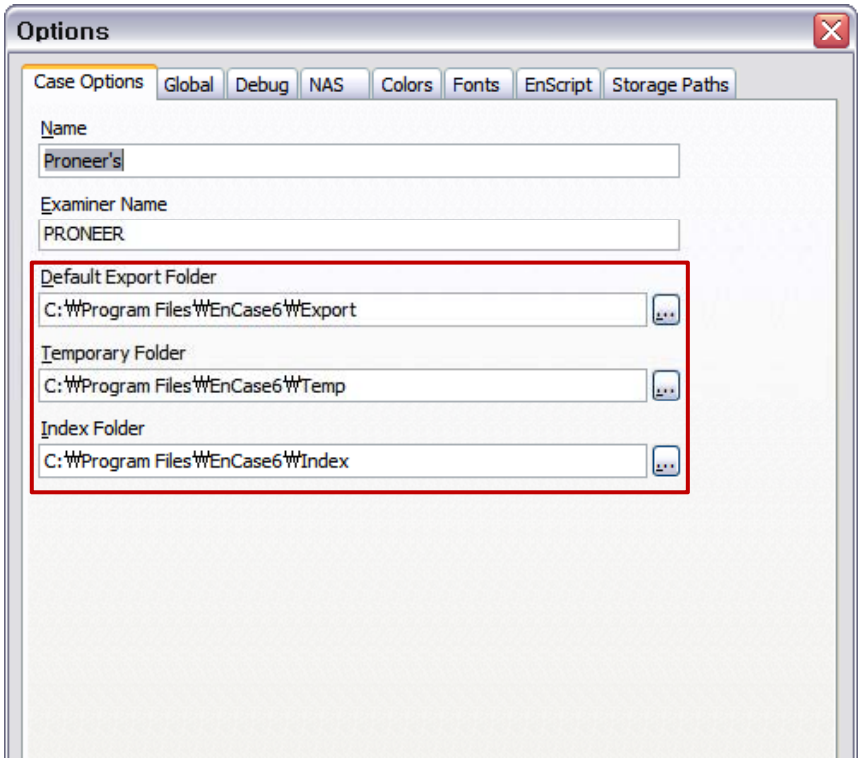


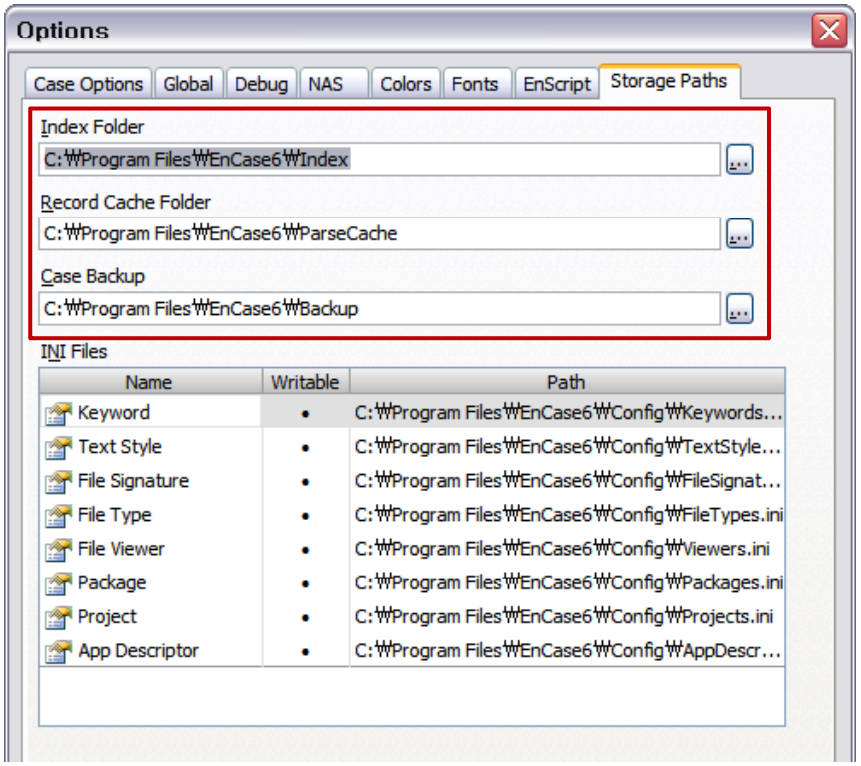
EnCase Concepts

EnCase Case Files



EnCase Case Files

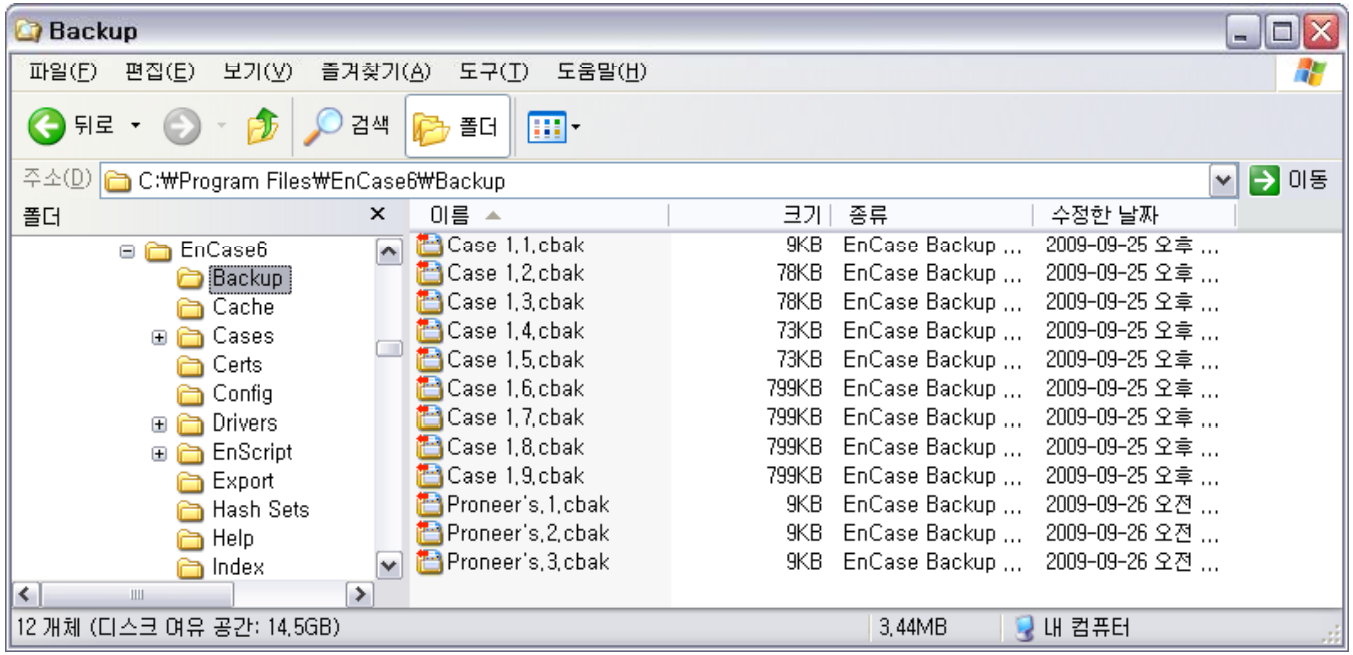


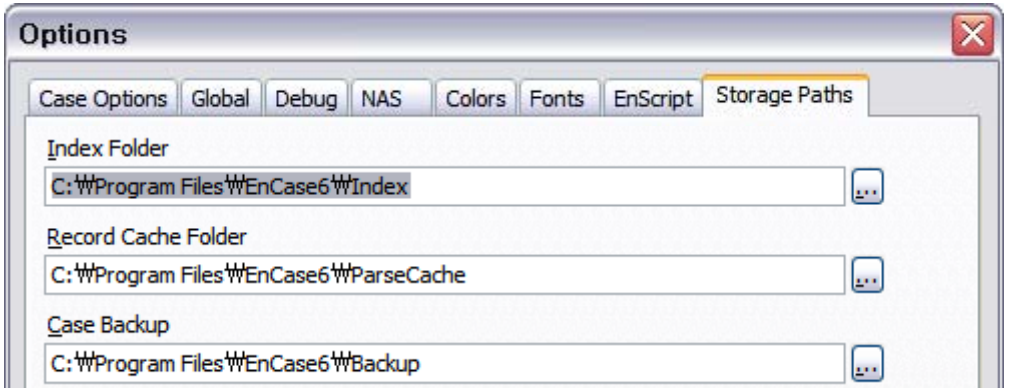


EnCase Concepts

- *EnCase Evidence File*
- *CRC and MD5*
- *EnCase Evidence File Format*
- *Evidence File Verification*
- *Hashing Disks and Volumes*
- *EnCase Case File*
- ***EnCase Backup File***
- *Configuration, or .ini, files*

EnCase Backup File (.cbak)





EnCase Concepts

EnCase Backup File (.cbak)

✓ **Auto Save Minutes**

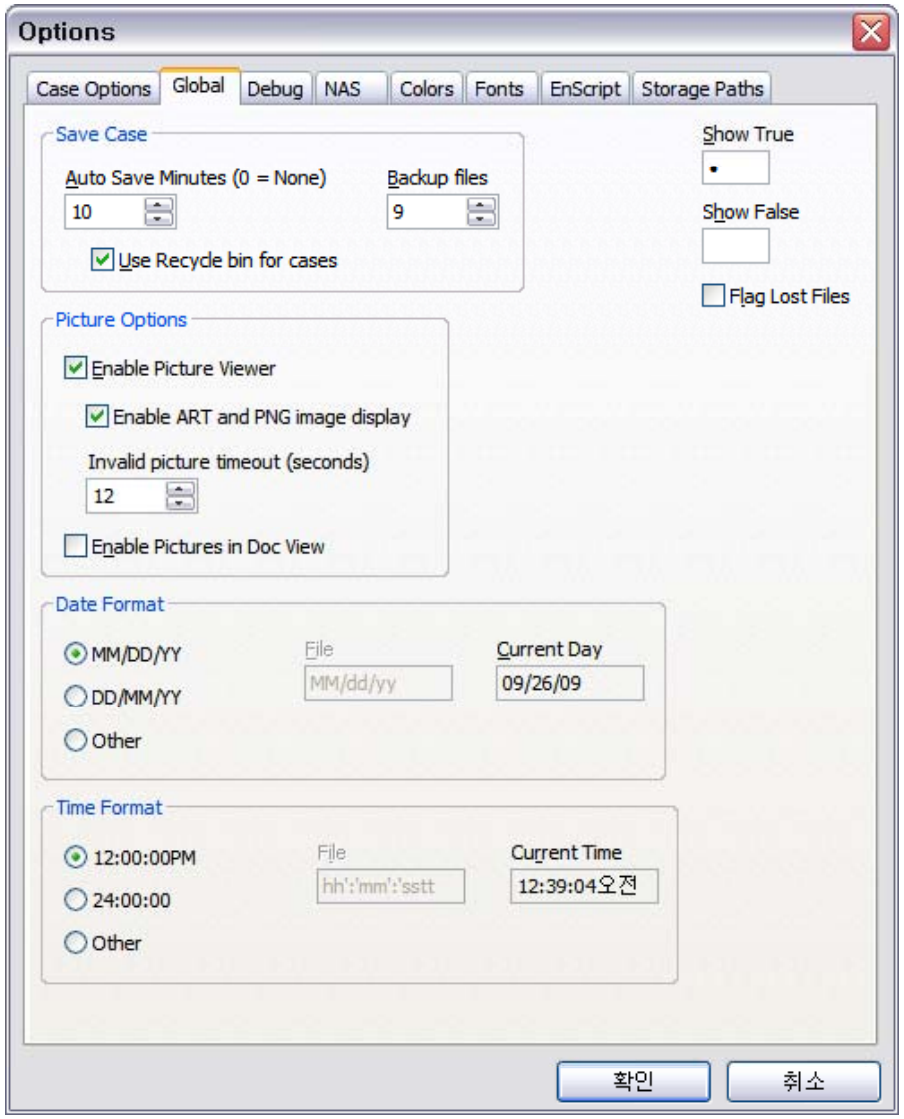
- 자동 백업 시간 (default 10)
- 0일 경우 백업하지 않음

✓ **Backup files**

- 생성하는 백업 파일 개수
- 자동적으로 덮어 쓰여짐

✓ **Use Recycle bin for cases**

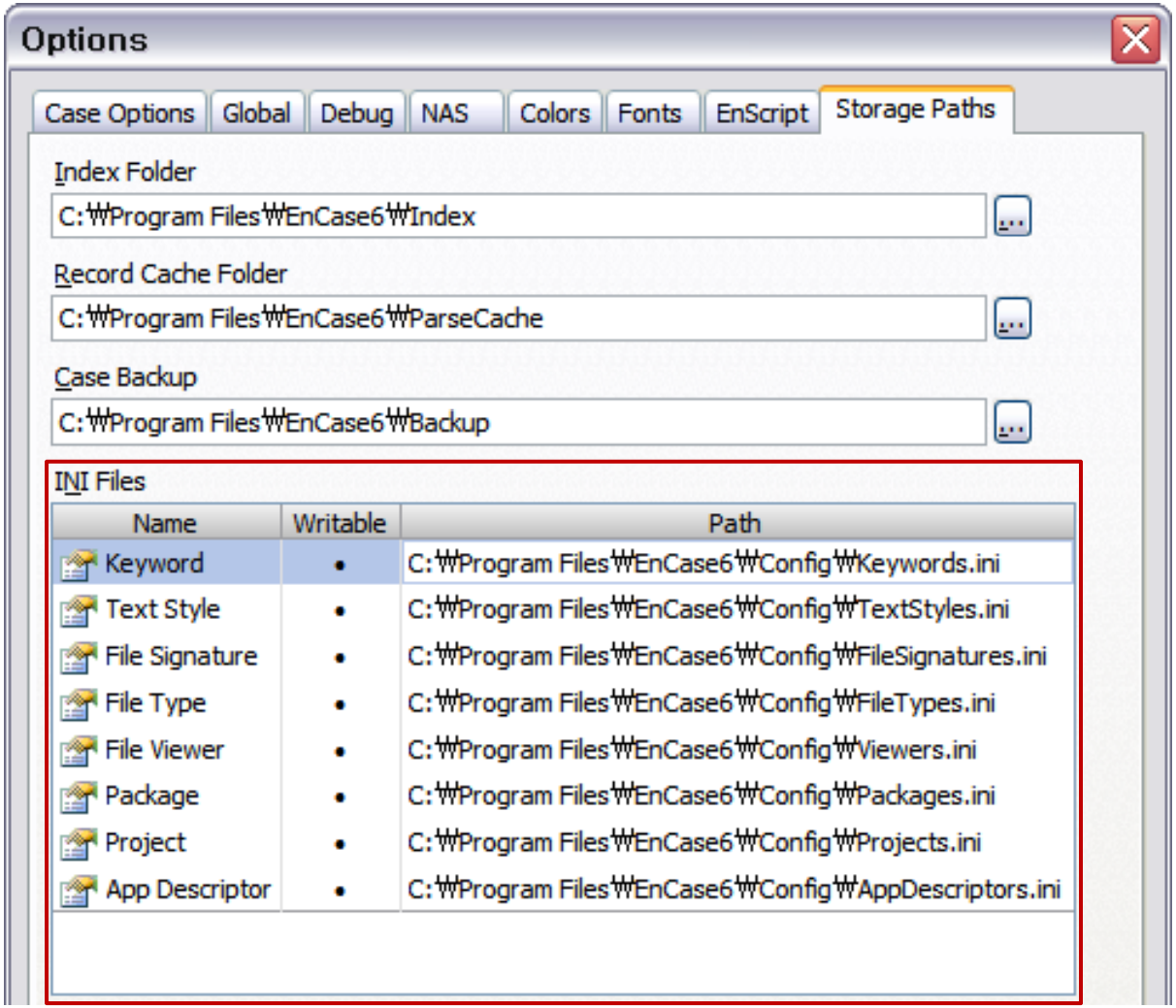
- 이전 .CASE 파일을 휴지통으로 이동



EnCase Concepts

- *EnCase Evidence File*
- *CRC and MD5*
- *EnCase Evidence File Format*
- *Evidence File Verification*
- *Hashing Disks and Volumes*
- *EnCase Case File*
- *EnCase Backup File*
- ***Configuration, or .ini, files***

EnCase Configuration Files



EnCase Concepts

EnCase Configuration Files

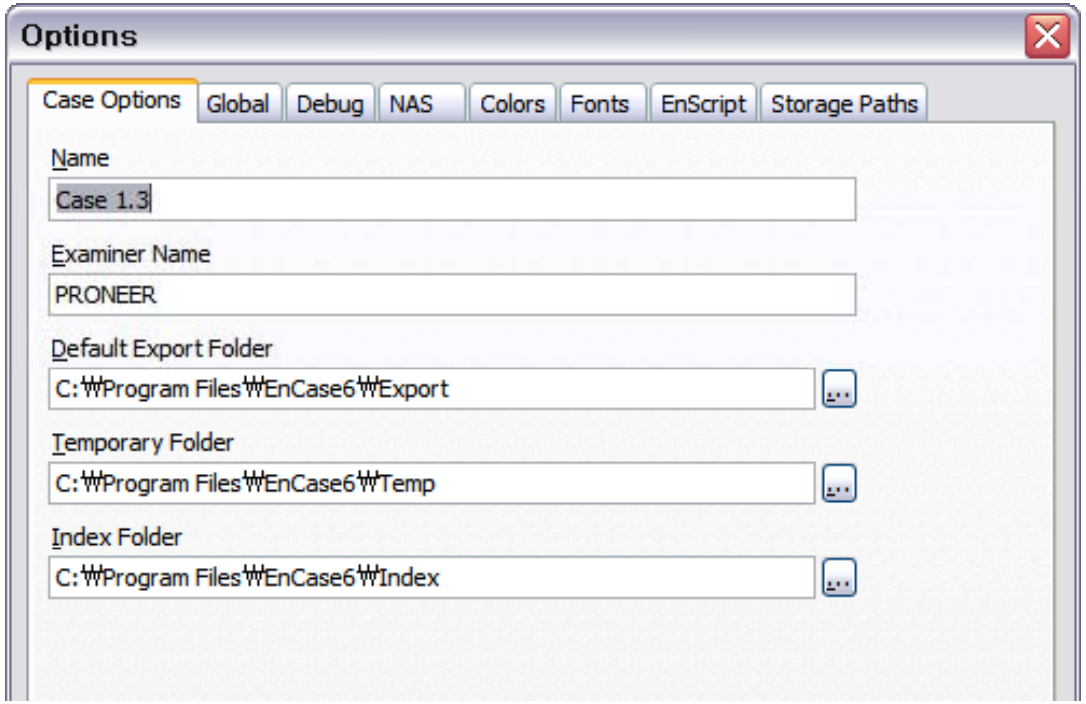
- ✓ **AppDescriptors.ini** : OS별 파일 해시 값 저장
- ✓ **Keyword.ini** : global keyword 저장 (EnCase Version 4+)
- ✓ **TextStyle.ini** : Text Styles Tab에 포함된 내용 저장
- ✓ **FileSignatures.ini** : File Signature Tab에 포함된 내용 저장
- ✓ **FileTypes.ini** : File Types Tab에 포함된 내용 저장 (EnCase or Windows 선택)
- ✓ **Filters.ini** : Filters Tab에 포함된 내용 저장
- ✓ **Local.ini** : EnCase의 전체적인 설정 내용
- ✓ **Profiles.ini** : 개인 프로필 설정 값
- ✓ **Projects.ini** : 프로젝트 설정 값

EnCase Concepts

- *EnCase Evidence File*
- *CRC and MD5*
- *EnCase Evidence File Format*
- *Evidence File Verification*
- *Hashing Disks and Volumes*
- *EnCase Case File*
- *EnCase Backup File*
- *Configuration, or .ini, files*
- ***Options….***

EnCase Concepts

- **Options ➔ Case Options**



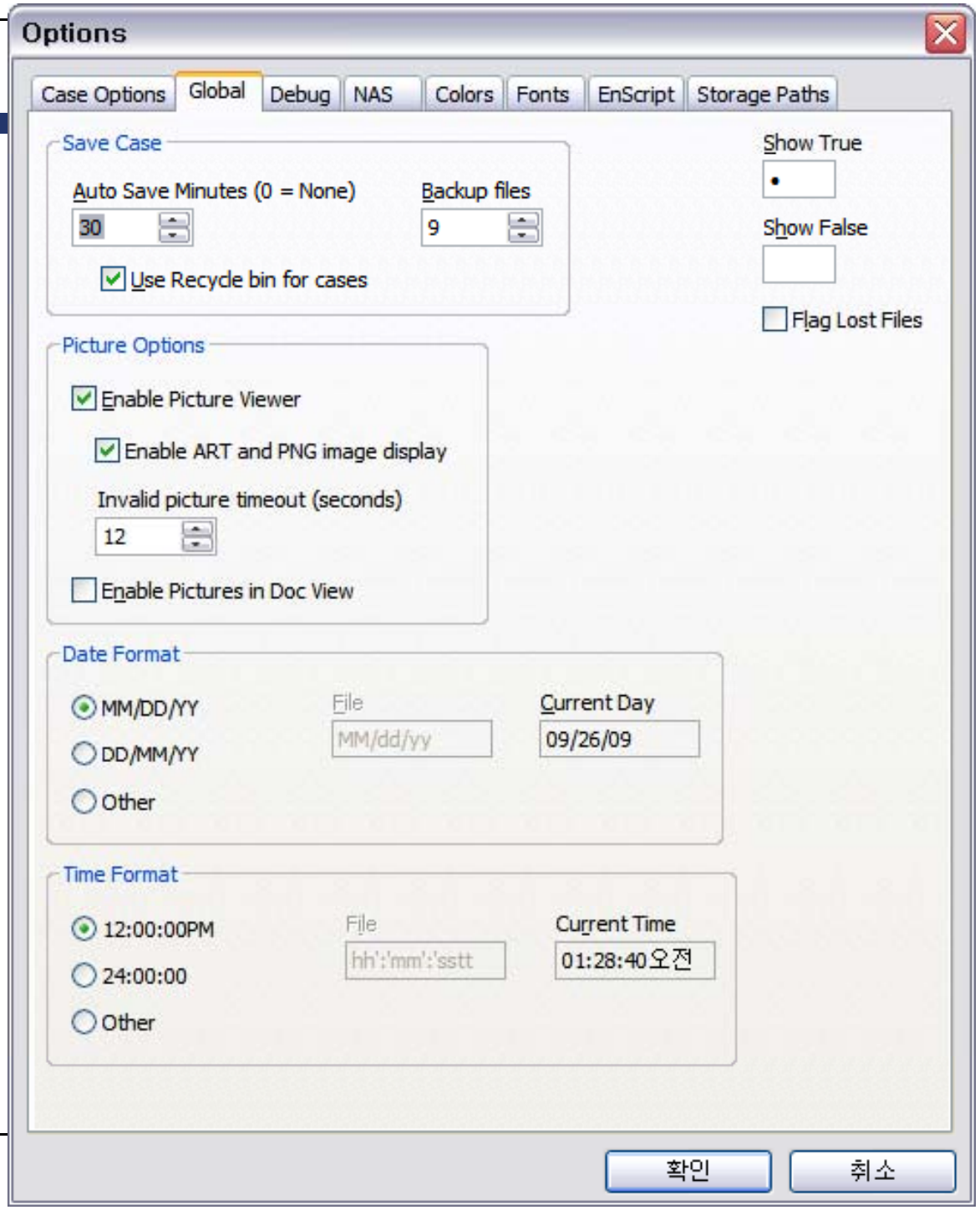
✓ **Export Folder :** Copy/UnErase 선택 시 기본 저장 폴더, EnScript 사용시 출력 폴더

✓ **Temporary Folder** : 외부 Viewer 사용시 파일 임시 저장 폴더

✓ **Index Folder** : 데이터 인덱싱을 할 경우 인덱싱 내용 저장 폴더

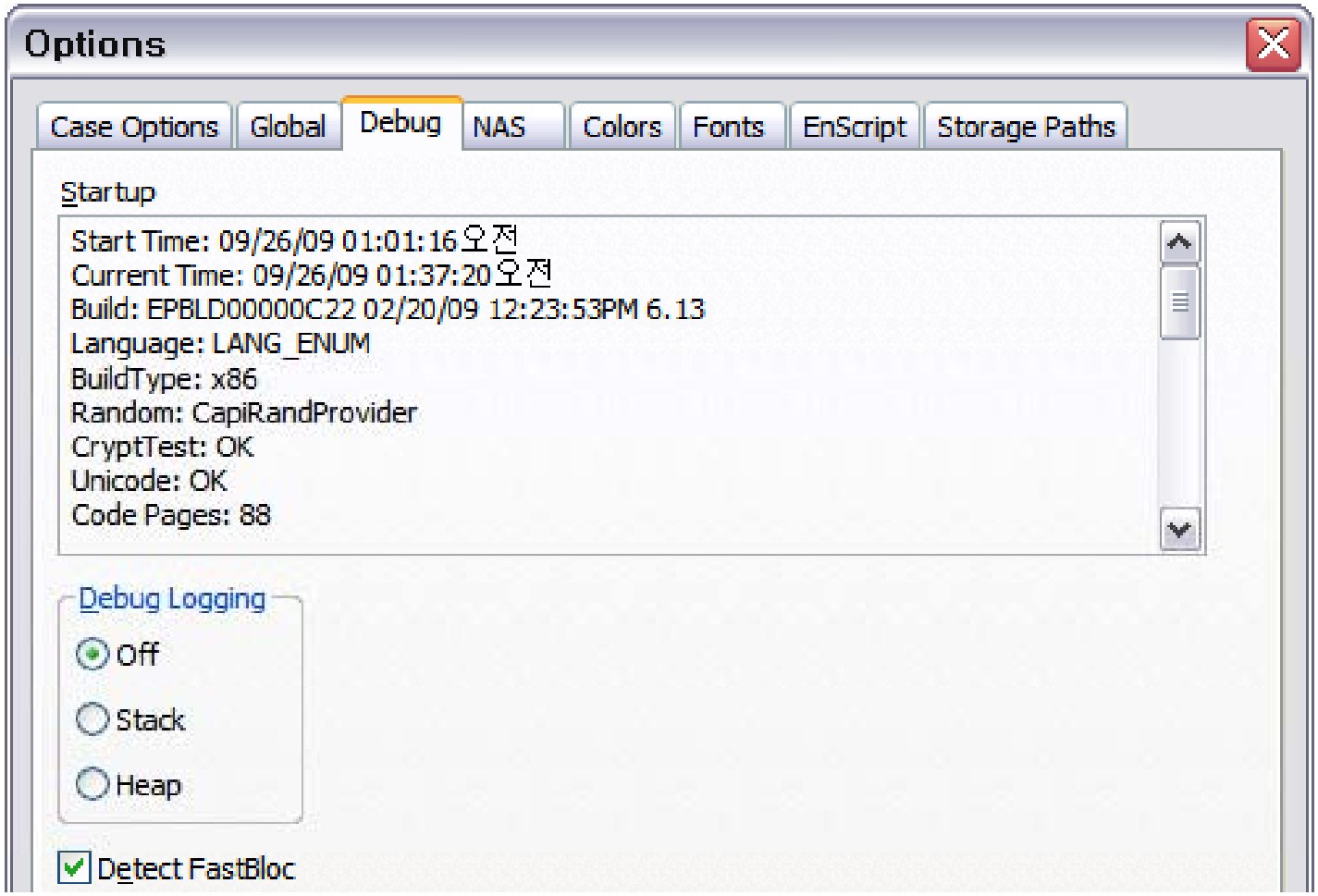
EnCase Concepts

- **Options ➔ Global**



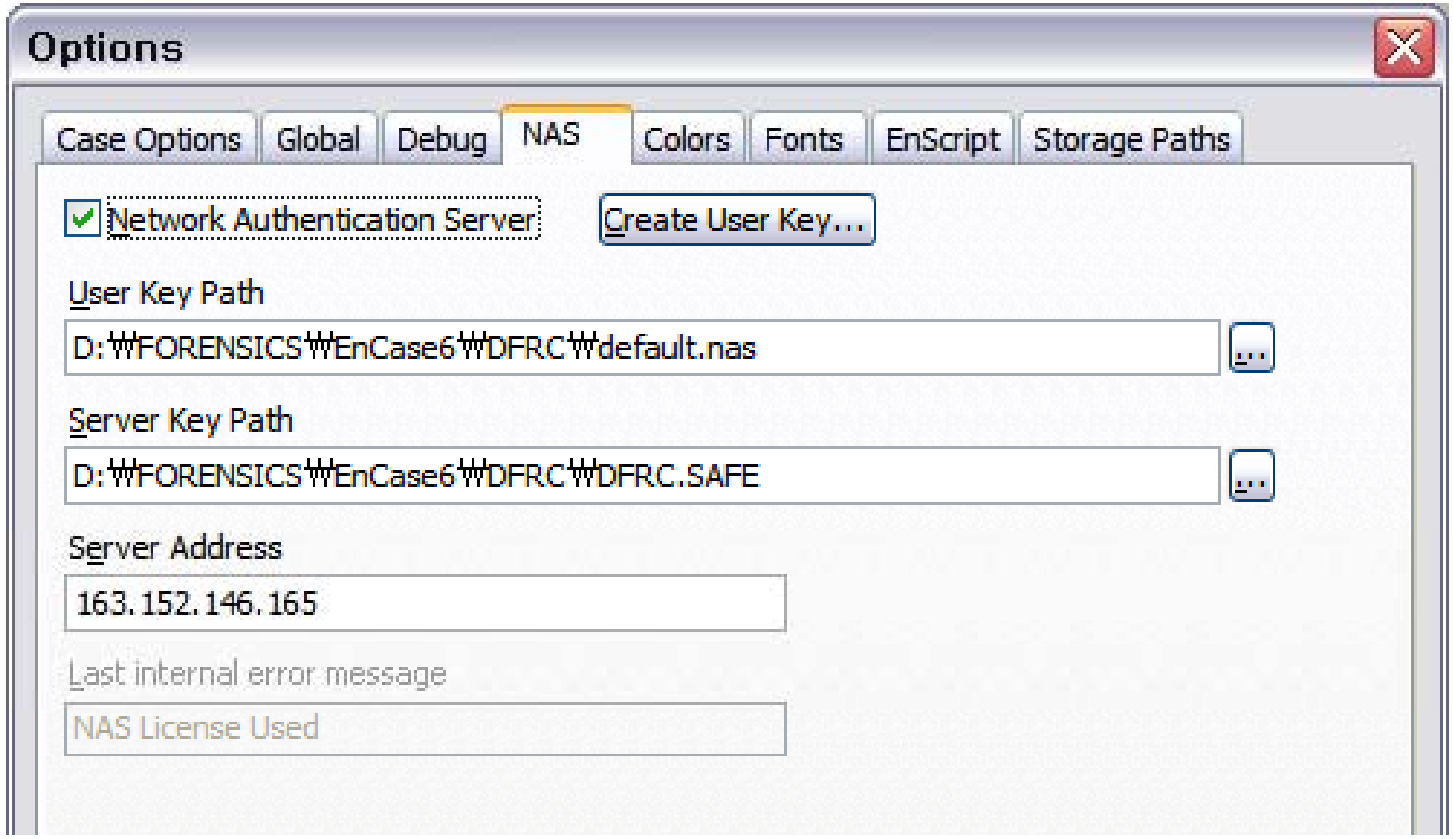
EnCase Concepts

- **Options ➔ Debug**

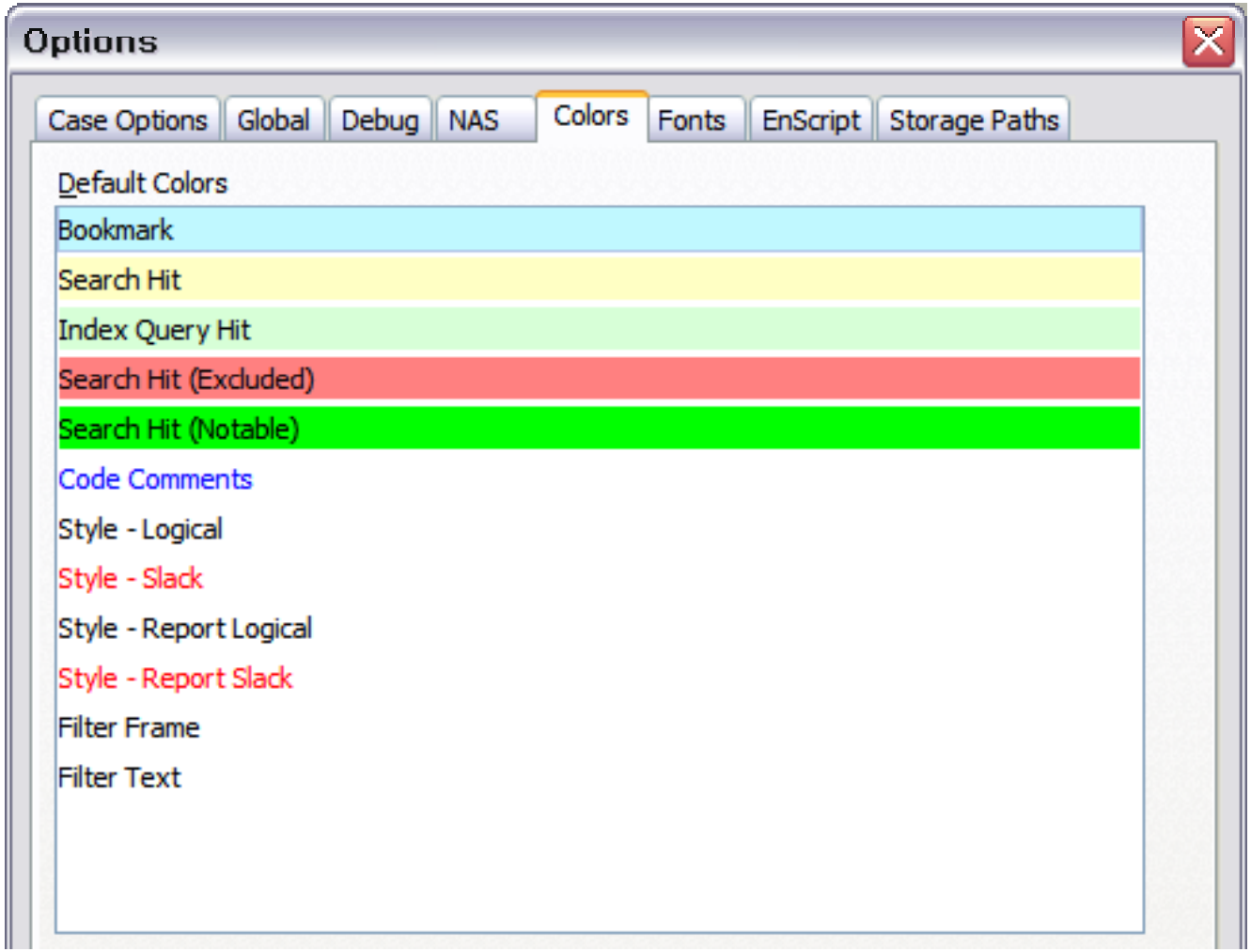


EnCase Concepts

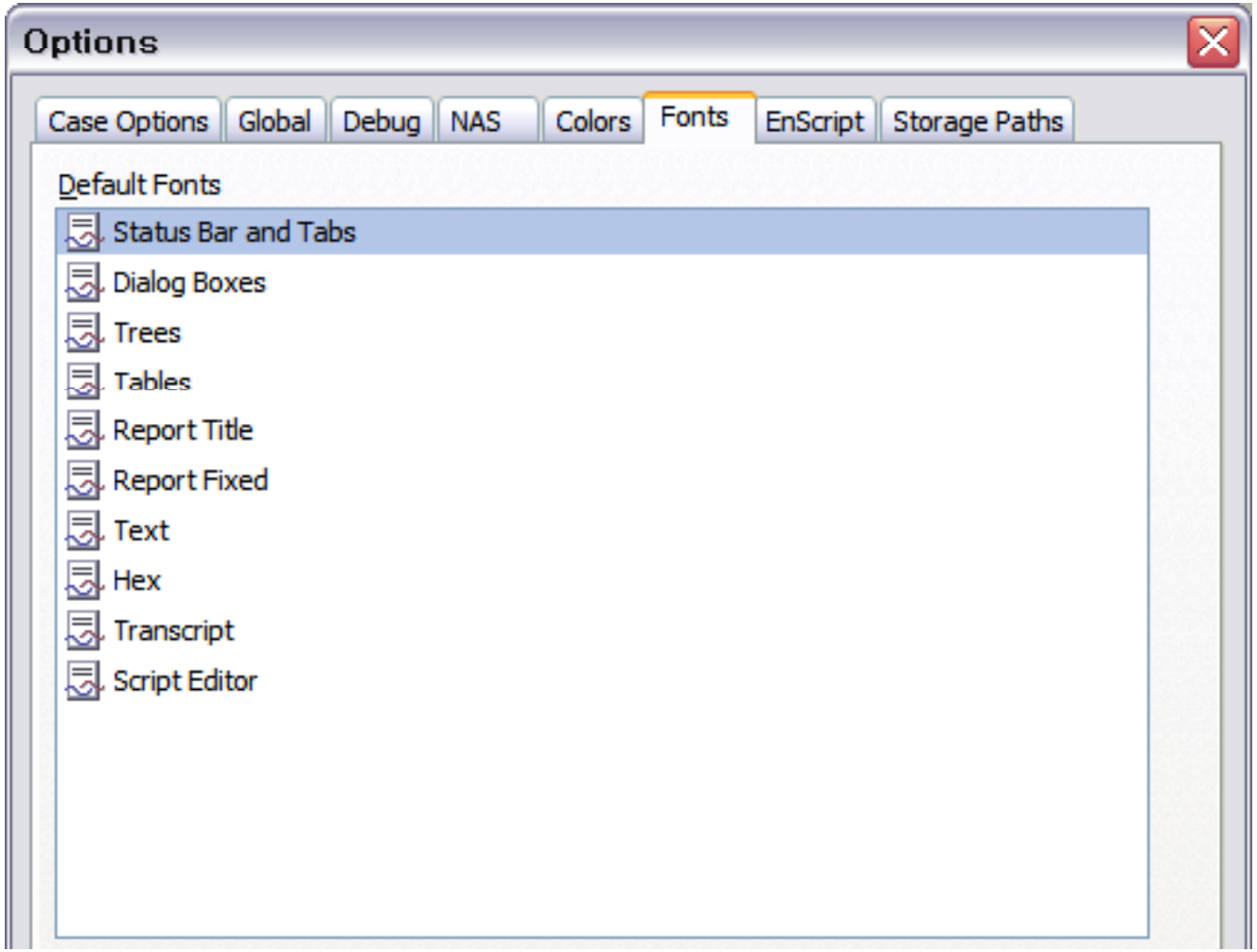
- **Options ➔ NAS**



- **Options ➔ Colors**

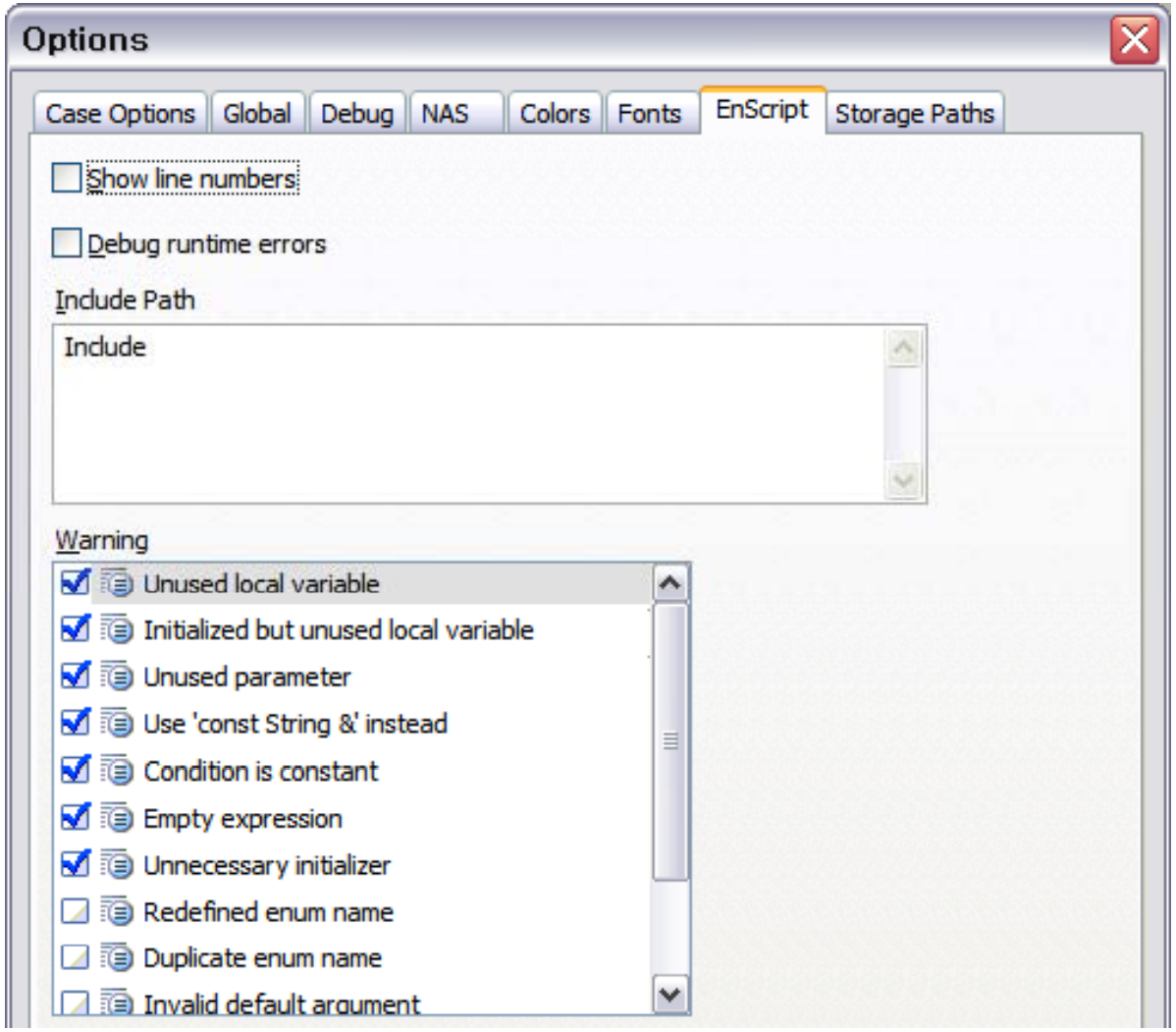


- **Options ➔ Fonts**



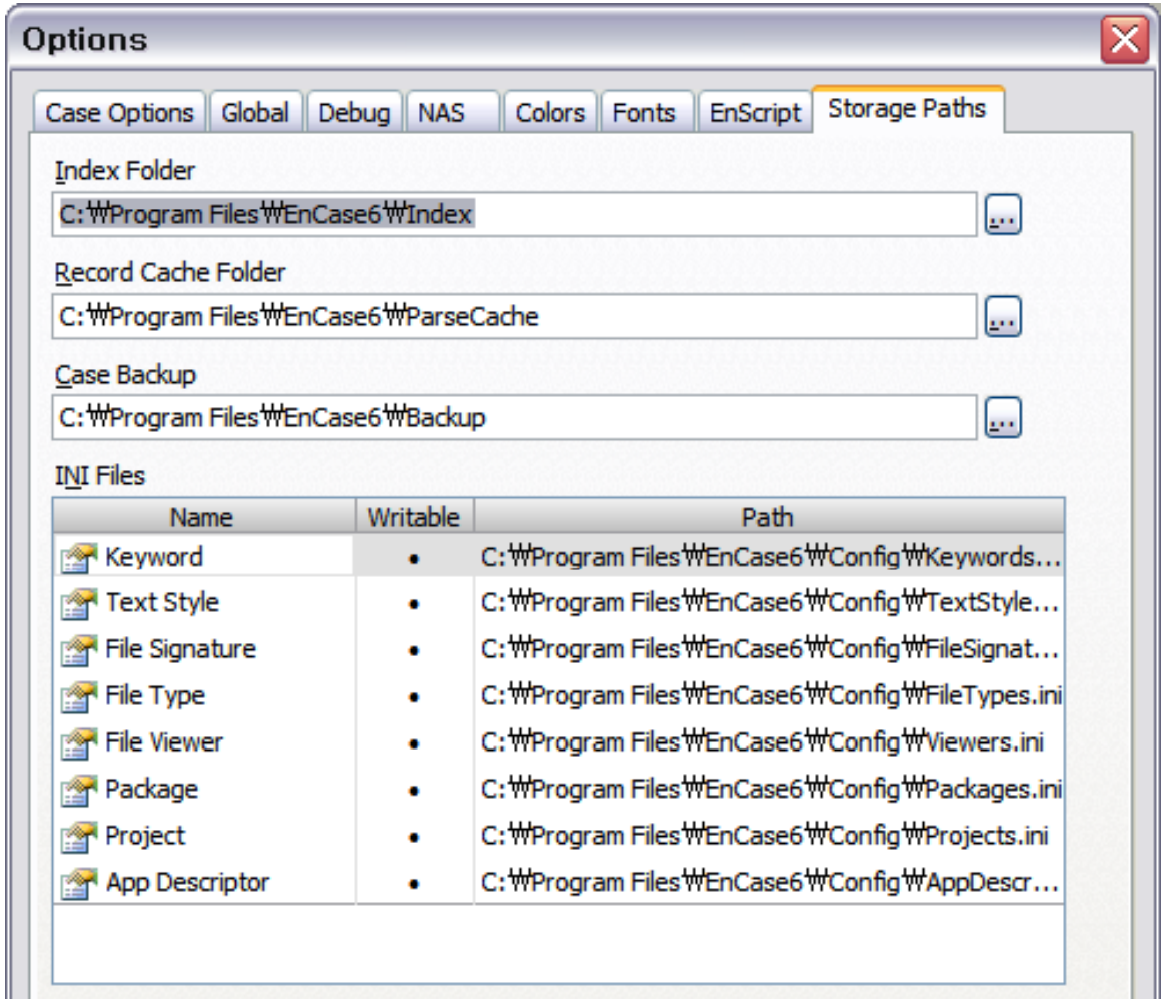
EnCase Concepts

- **Options ➔ EnScript**



EnCase Concepts

- **Options ➔ Storage Paths**



Homework

- **HW #1**
  - ✓ ??

Forward Planning

- **Outline**

  - ✓ ~~**Week 1 : Hardware and File system Analysis (Chapter 1, 2)**~~
  - ✓ ~~**Week 2 : Acquiring Digital Evidence (Chapter 4)**~~
  - ✓ ~~**Week 3 : EnCase Concepts and Environment (Chapter 5, 6)**~~
  - ✓ Week 4 : Actual Test
  - ✓ Week 5 : Actual Test
  - ✓ Week 6 : Actual Test
  - ✓ Week 7 : Actual Test
  - ✓ ..
  - ✓ PS : EnScripting

Forward Planning

Outline

- ✓ ~~Week 1 : Hardware and File system Analysis (Chapter 1, 2)~~
- ✓ ~~Week 2 : Acquiring Digital Evidence (Chapter 4)~~
- ✓ ~~Week 3 : EnCase Concepts and Environment (Chapter 5, 6)~~
- ✓ Week 4 : Actual Test
  - 문제를 해결하기 위한 사전 준비 내용 학습
  - 문제는 과제로 제출 (HWP, DOC 문서 작성 후 PDF 형식으로 변환 후 제출)

Question and Answer