

2021 디지털포렌식개론

Encase를 활용한 컴퓨터 포렌식

신수민

국민대학교 금융정보보안학과, DF&C 연구실

tnals523@kookmin.ac.kr

CONTENTS

1. 컴퓨터 포렌식
2. Encase 개요
3. Encase 기능 소개

1. 컴퓨터 포렌식

▪ 컴퓨터 포렌식이란

- 컴퓨터를 매개로 이루어지는 범죄 행위에 대한 법적 증거자료 확보를 위함
- 컴퓨터 저장매체 등의 컴퓨터 시스템과 네트워크로부터 **자료 수집, 분석 및 보존**하여, 디지털 자료가 법적 증거물로서 제출할 수 있도록 하는 일련의 절차 및 방법



1. 컴퓨터 포렌식

▪ 사례

- 산업 기술 유출

‘자율주행차량 핵심기술 중국 유출’ 혐의 카이스트 교수 구속 기소

등록 : 2020-09-14 18:25

f t ↻ ★ ☰

+ -



한국과학기술원(KAIST). 카이스트 제공

자율주행차량 관련 첨단기술을 중국에 유출한 혐의로 한국과학기술원(KAIST) 교수가 구속기소됐다.

대전지검 특허범죄조사부(부장 김윤희)는 14일 산업기술의 유출 방지 및 보호에 관한 법률과 부정경쟁 방지 및 영업비밀 보호에 관한 법률 위반, 업무상 배임 등 혐의로 구속된 카이스트 이아무개(58) 교수를 재판에 넘겼다.

이 교수는 2017년 11월부터 지난 2월까지 중국의 ‘국가 해외 고급인재 유치 계획’에 따라 외국인 전문가로 선발돼 연구과제를 하던 중 카이스트가 보유한 첨단기술인 자율주행차량 라이다 기술 연구자로 등을 중국의 대학 연구원에게 넘긴 혐의를 받고 있다.

[출처: <https://www.hani.co.kr/arti/area/chungcheong/962121.html>]

1. 컴퓨터 포렌식

▪ 사례

- 산업 기술 유출

[형사] "경쟁 대만업체로 이직하며 영업비밀 유출...대만업체도 벌금 5,000만원"

🕒 기사출고 2020.10.02 10:39



┃ [안산지원] "행위의 결과가 대한민국 영역 안에서 발생한 경우에 해당"

수원지법 안산지원 조준호 판사는 8월 26일 안산시 단원구에 있는 자동차용 LED 제품을 생산하는 A사에서 일하던 직원들이 경쟁회사인 대만 업체 B사로 이직하면서 영업비밀을 유출한 사건과 관련, 부정경쟁방지법상 양벌규정에 따라 기소된 B사에 벌금 5,000만원을 선고했다(2019고단3178).

[출처: <https://www.legaltimes.co.kr/news/articleView.html?idxno=55752>]

1. 컴퓨터 포렌식

▪ 사례

특허청, 영업비밀 유출 피해기업 증거확보 돕는다

✎ 김보현 | ⌚ 입력 2021.04.02 14:38



정부가 영업비밀 유출로 피해를 본 중소기업들이 침해 입증을 손쉽게 할 수 있도록 지원에 나선다.

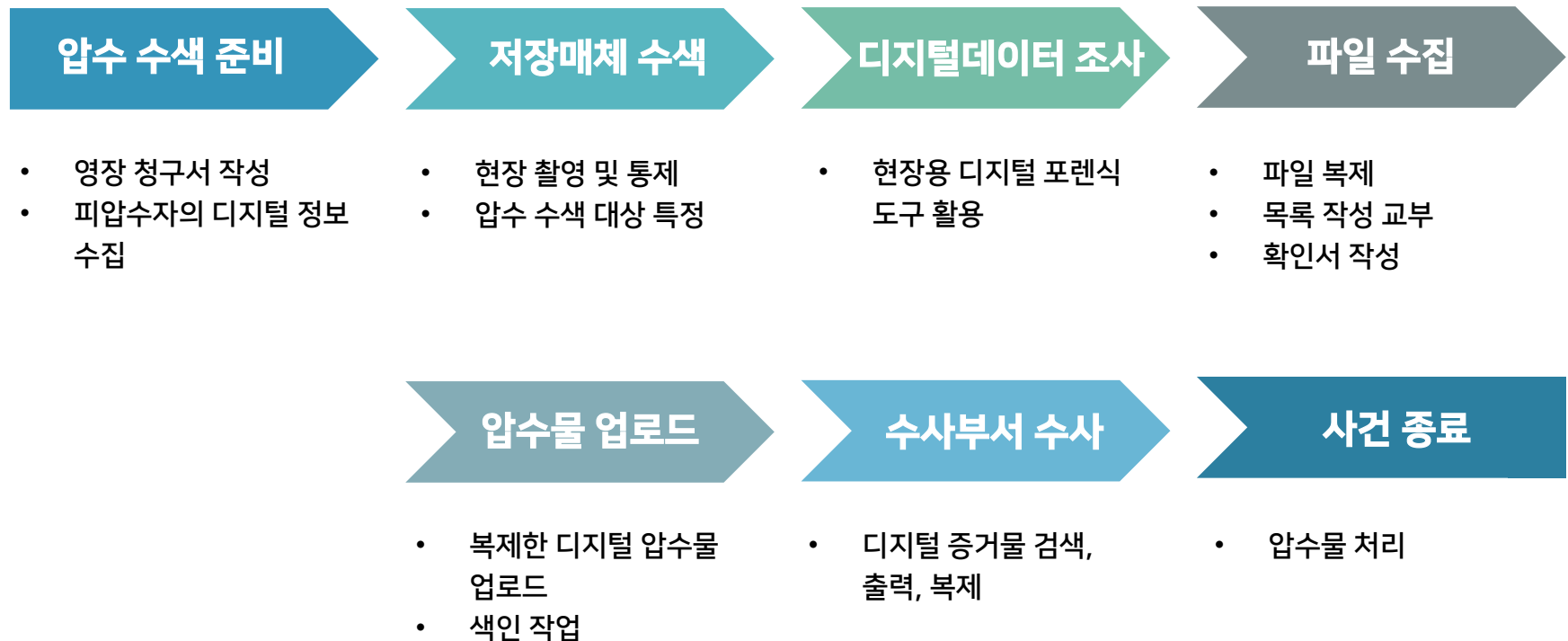
특허청은 중소기업들이 영업비밀 유출 증거를 확보할 수 있도록 스마트폰, PC 등 정보기기에 대한 '디지털 포렌식 지원' 사업을 추진한다고 최근 밝혔다.

특허청에 따르면 영업비밀 소송 판결문을 분석한 결과, 소송의 75% 이상에서 이메일이 중요 증거로 활용되는 등 디지털 증거가 실제 재판에서 영업비밀 침해 입증에 결정적인 역할을 하고 있는 것으로 나타났다. 문제는 중소기업의 경우 영업비밀 유출 피해에도 첨단 포렌식 장비와 이를 운용할 수 있는 전문가가 부족해 소송에 필요한 증거를 자체적으로 확보하는데 상당한 어려움을 겪고 있다는 것이다.

[출처: <http://www.anjunj.com/news/articleView.html?idxno=30137>]

1. 컴퓨터 포렌식

▪ 절차



2. Encase 개요

▪ Encase

- Guidance Software 社에서 제작한 통합 포렌식 도구
- 동글키를 통해 도구 사용 가능
- 지원하는 파일 시스템
 - FAT12, FAT16, FAT32
 - NTFS
 - EXT2, EXT3, EXT4
 - HFS, HFS+, HFSX
 - UFS 등

동글키

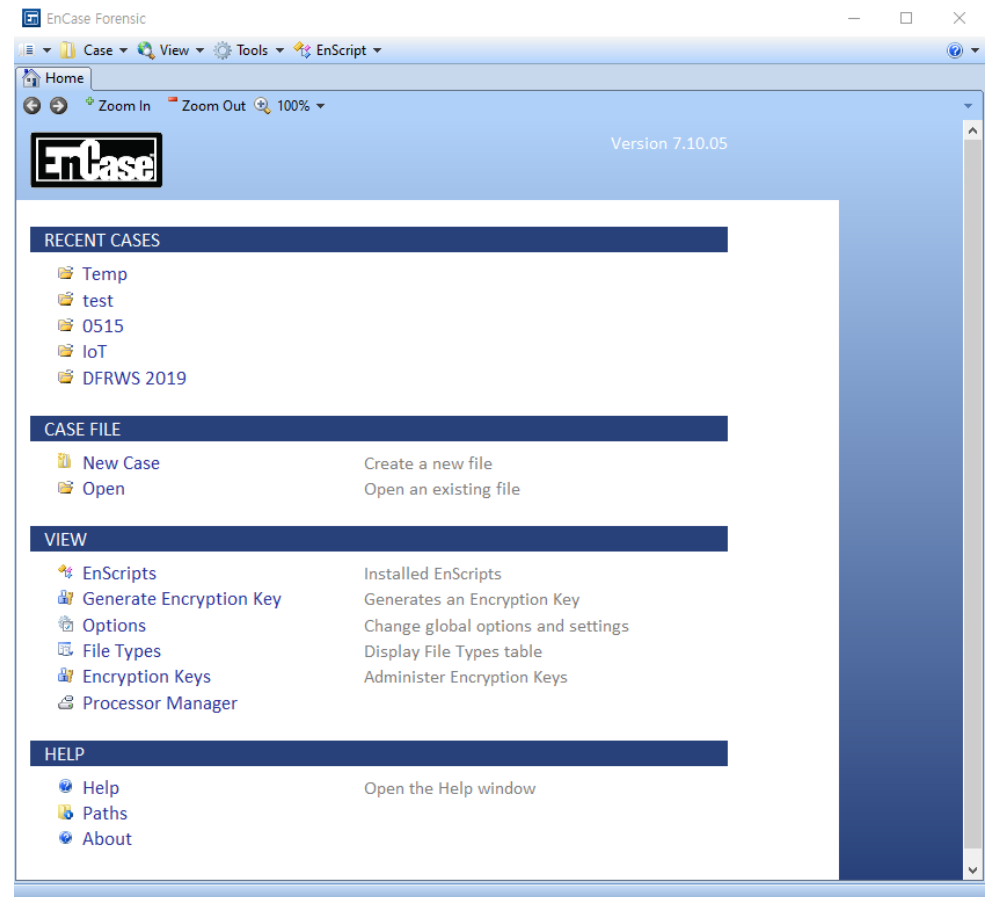


2. Encase 개요

▪ Encase

• 기능

- 증거 이미징 후 분석 가능
- 파일 복구
- 파일의 시그니처 분석
- 파일의 해시 정보
- 이메일 정보
- 인터넷 사용흔적 기록 등



[Encase 실행화면]

2. Encase 소개

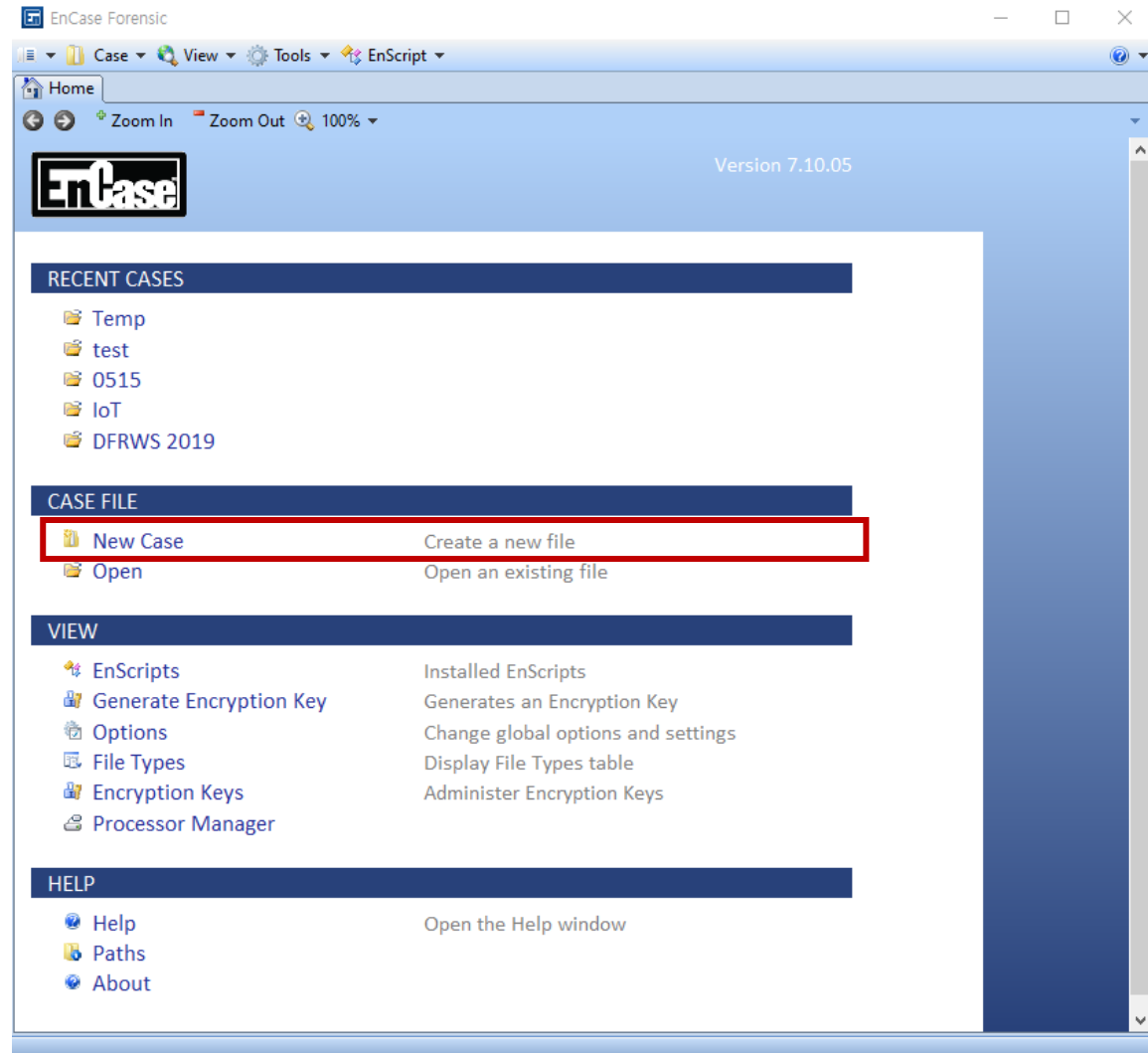
- 기능



3. Encase 기능 소개

■ Case 생성

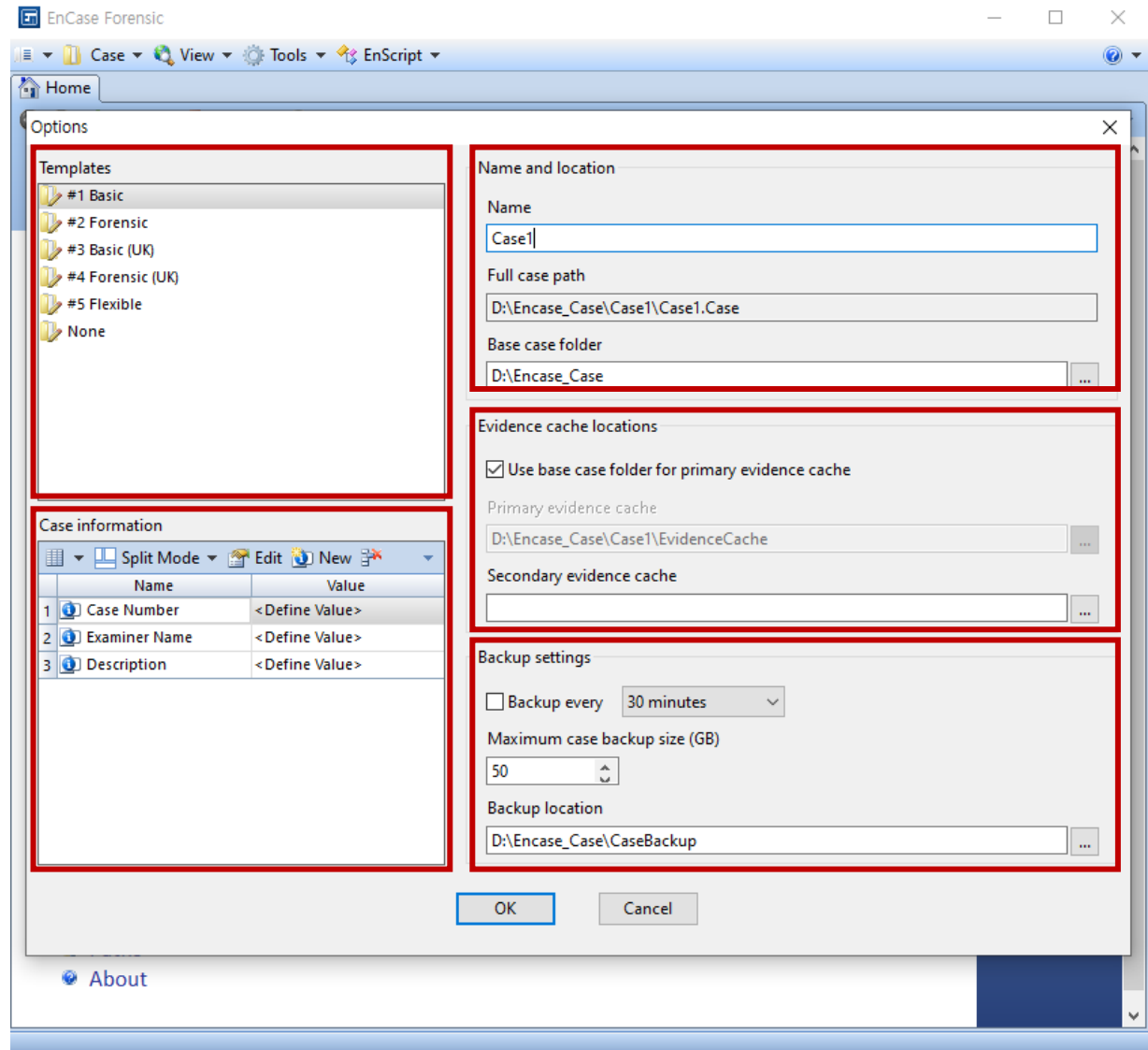
- New Case 선택



3. Encase 기능 소개

■ Case 생성

- Case Option 작성



3. Encase 기능 소개

- Case 생성

- Case Option 작성

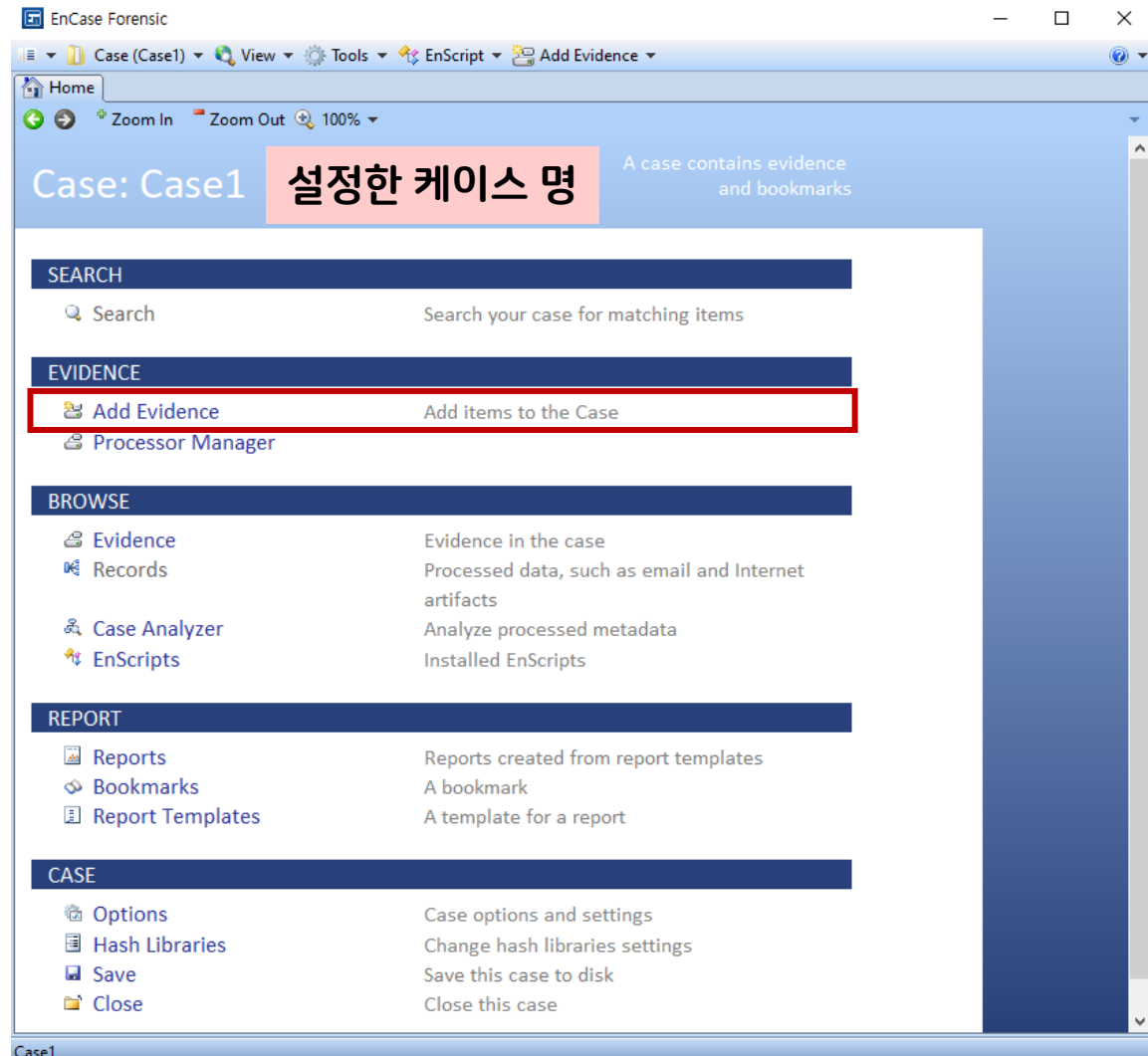
- Templates: 분석이 끝나면 작성해야 하는 보고서의 템플릿
- Case Information: 보고서에 들어갈 정보를 기입
- Name and location: 케이스 명과 경로 설정
- Evidence cache locations: 케이스와 관련된 캐시 데이터를 저장할 경로 설정
- Backup settings: 케이스의 백업 경로 설정

Backup every 체크 시 선택한 시간마다 백업 진행

3. Encase 기능 소개

▪ Evidence 추가

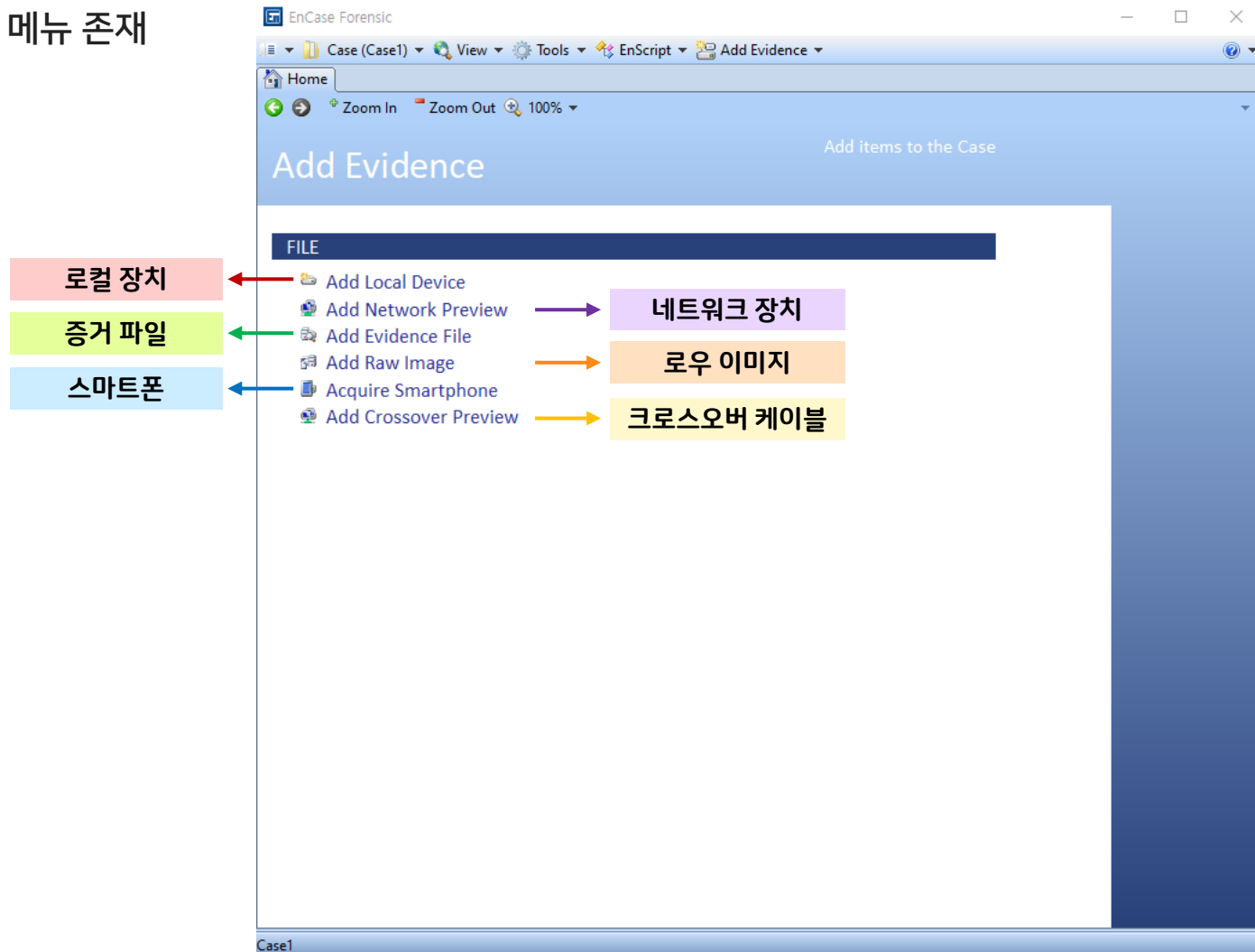
- Add Evidence 선택



3. Encase 기능 소개

▪ Evidence 추가

- 6가지 메뉴 존재

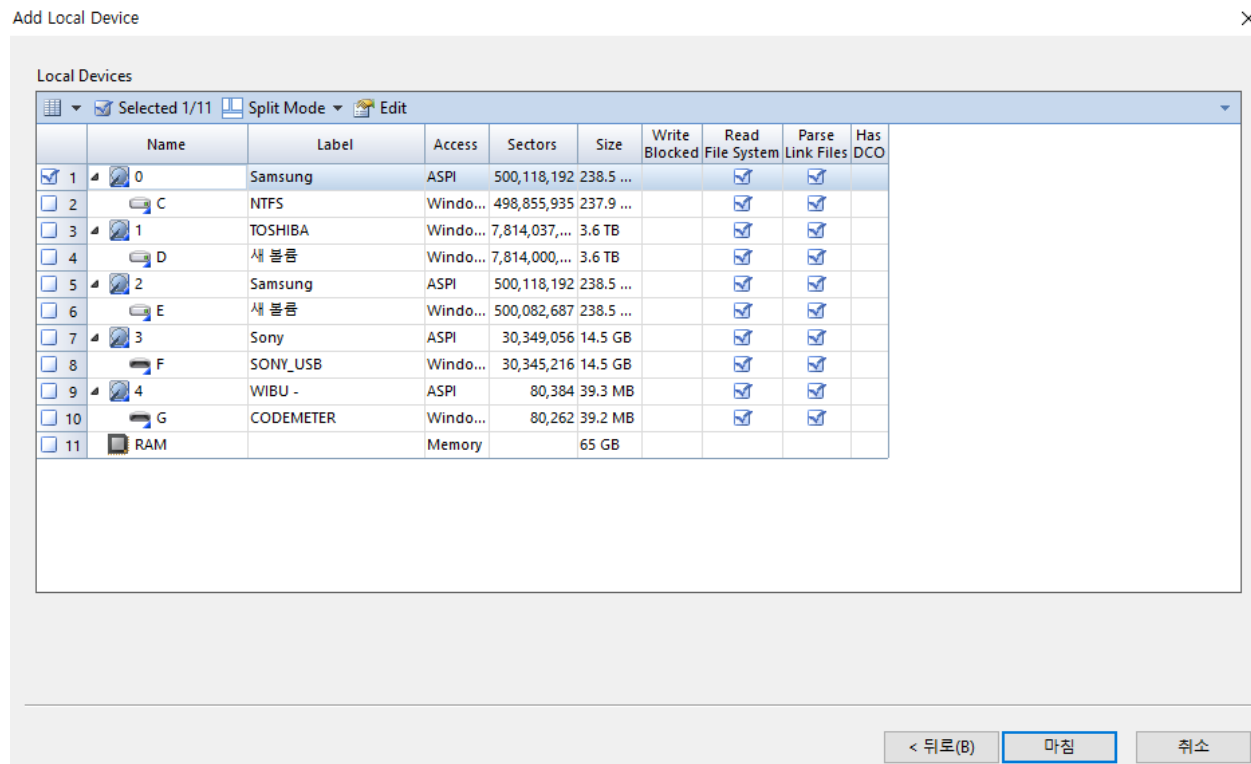


3. Encase 기능 소개

▪ Evidence 추가

- Add Local Device

- 로컬에 마운트되어 있는 장치 추가
- 선택 시 현재 컴퓨터에 존재하는 장치 목록 확인 가능



3. Encase 기능 소개

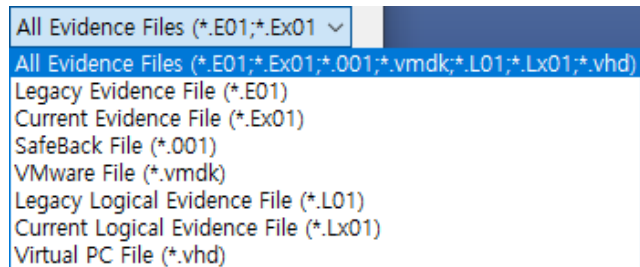
▪ Evidence 추가

- Add Network Preview

- 네트워크 망에 존재하는 다른 컴퓨터들 추가

- Add Evidence File

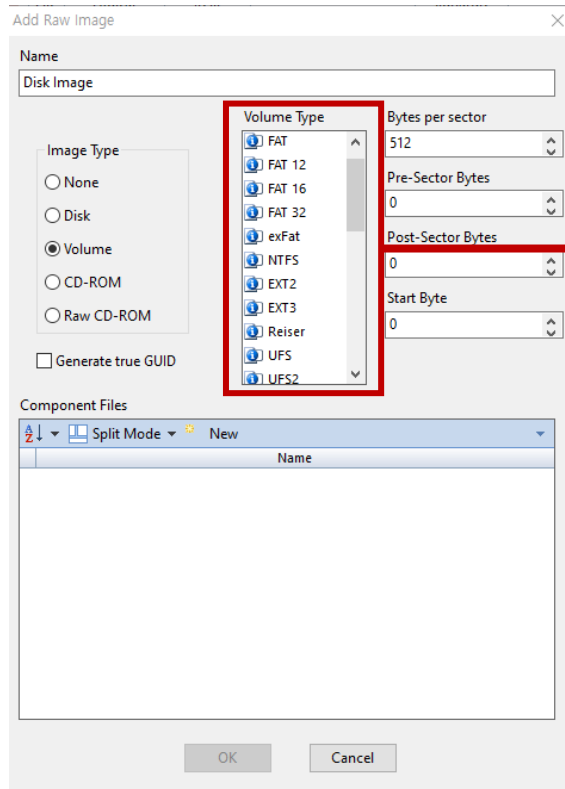
- 기존에 생성한 증거 파일 추가
- Encase 증거 파일 뿐만 아니라 SafeBack, VMware 등의 파일도 지원



3. Encase 기능 소개

▪ Evidence 추가

- Add Raw Image
 - 물리적 장치의 원본 또는 DD (Disk Dump) 이미지 파일 추가



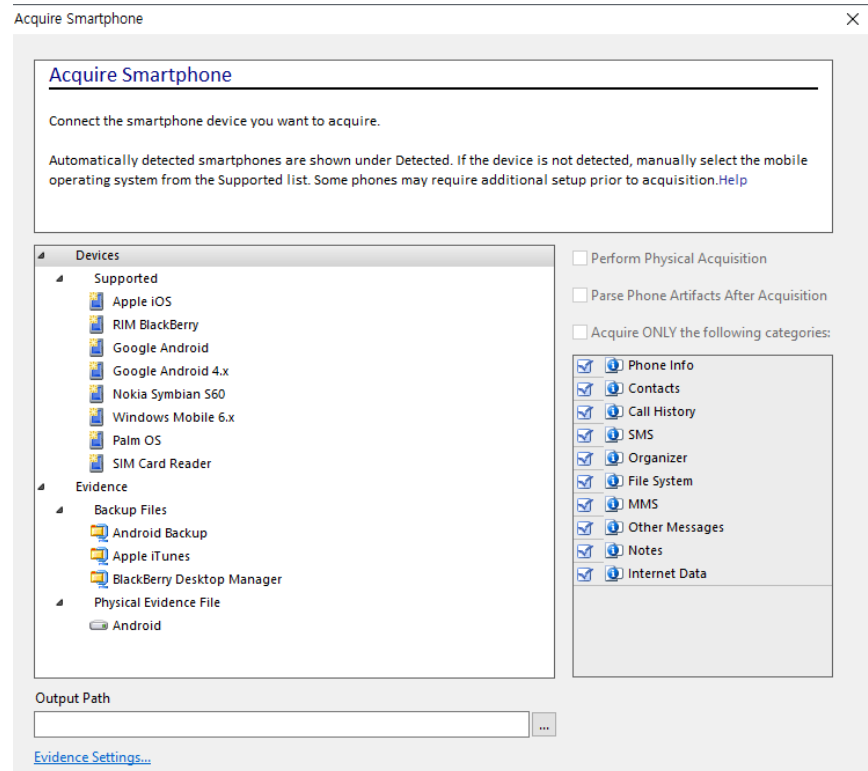
지원하는 파일시스템 목록

3. Encase 기능 소개

▪ Evidence 추가

- Acquire Smartphone

- 스마트폰에 대한 분석
- 스마트폰의 백업 파일 분석 가능



- Add Crossover Preview

- Crossover 케이블을 통해 증거 추가

3. Encase 기능 소개

프로세싱

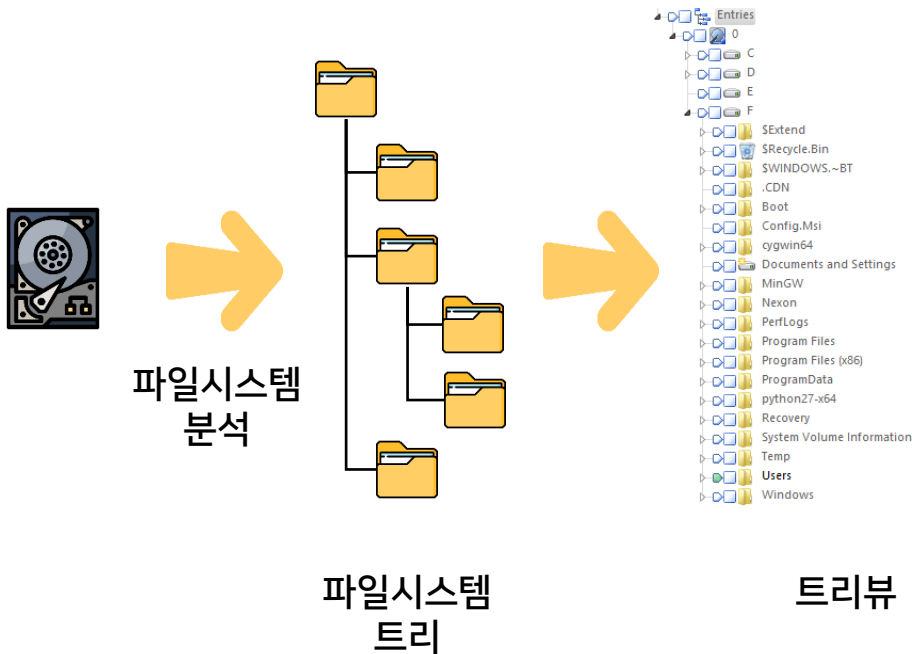


Table					
Selected 0/1860234					
	Name	Tag	File Ext	Logical Size	Category
1	All Users			48	Folder
2	Default			8,192	Folder
3	.dotnet	do...		4,096	Folder
4	TelemetryStorageService			4,096	Folder
5	20210323200148_442af3b79f25459eba0680735a4459...	trn		936	None
6	20210323200226_4666f45251a64375ae0f5a233d17c4...	trn		944	None
7	3.1.407_Machineld.dotnetUserLevelCache	do...		64	None
8	3.1.111_IsDockerContainer.dotnetUserLevelCache	do...		5	None
9	3.1.111_Machineld.dotnetUserLevelCache	do...		64	None
10	3.1.405_Machineld.dotnetUserLevelCache	do...		64	None
11	3.1.112_Machineld.dotnetUserLevelCache	do...		64	None
12	3.1.405_IsDockerContainer.dotnetUserLevelCache	do...		5	None
13	3.1.113_Machineld.dotnetUserLevelCache	do...		64	None
14	3.1.406_Machineld.dotnetUserLevelCache	do...		64	None
15	3.1.112_IsDockerContainer.dotnetUserLevelCache	do...		5	None
16	3.1.113_IsDockerContainer.dotnetUserLevelCache	do...		5	None
17	3.1.406_IsDockerContainer.dotnetUserLevelCache	do...		5	None
18	3.1.407_IsDockerContainer.dotnetUserLevelCache	do...		5	None
19	AppData			240	Folder
20	Local			4,096	Folder
21	Application Data			48	Folder

테이블뷰

3. Encase 기능 소개

■ 증거 분석

The screenshot displays the EnCase Forensic application window. The left pane shows a file tree with 'Pictures' selected. The main pane shows a table of file entries. A red box labeled '트리 창' (Tree View) points to the left pane. Another red box labeled '테이블 창' (Table View) points to the main table. A third red box labeled '보기 창' (View Window) points to the bottom pane showing detailed file information.

	Name	Tag	File Ext	Logical Size	Category	Signature Analysis	File Type	Protected	Protection complex
139	장구.png		png	346,998	Picture				
140	장구.png-Zone.Identifier		ide...	133	None				
141	edongnam_391.jpg		jpg	10,316	Picture				
142	edongnam_391.jpg-Zone.Identifier		ide...	131	None				
143	여피지.jpg		jpg	32,228	Picture				
144	여피지.jpg-Zone.Identifier		ide...	211	None				
145	200511_2.png		png	87,308	Picture				
146	200511_2.png-Zone.Identifier		ide...	50	None				
147	crown.png		png	19,277	Picture				
148	crown.png-Zone.Identifier		ide...	165	None				
149	Diario process.jpg		jpg	318,260	Picture				
150	realm_포인터수정.png		png	22,305	Picture				
151	noun_Files_1158733.png		png	39,822	Picture				
152	noun_Files_1158733.png-Zone.Identifier		ide...	50	None				

Name	Value
S Name	장구.png
S Tag	
S File Ext	png
I Logical Size	346,998
I Category	Picture
I Signature Analysis	
S File Type	
S Protected	
I Protection complexity	
Last Accessed	09/27/19 12:09:35 오전
File Created	09/27/19 12:09:34 오전
Last Written	09/27/19 12:09:35 오전
b Is Picture	.
b Is Indexed	

3. Encase 기능 소개

- 트리 창

- 케이스에 추가한 장치들을 계층적 구조로 표시

- 테이블 창

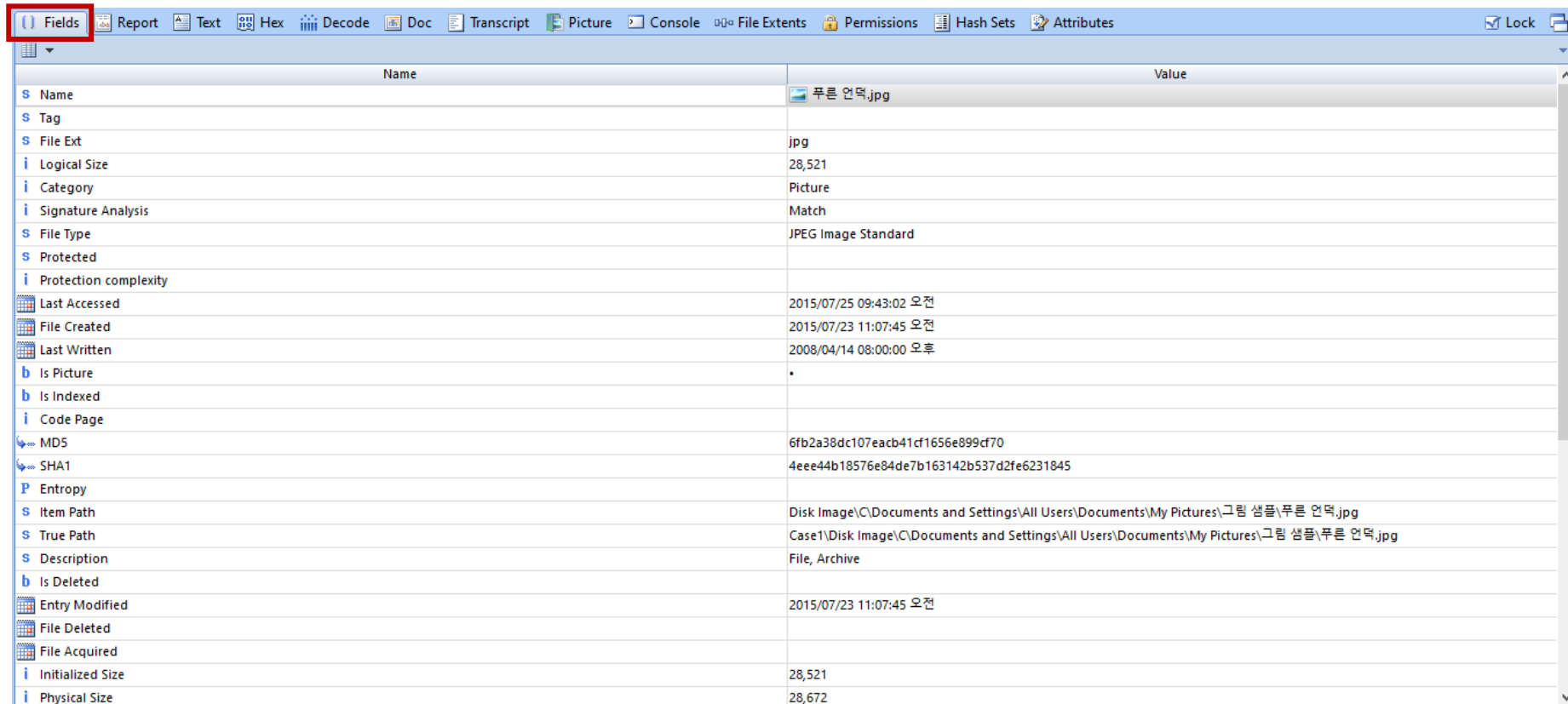
- 파일들의 속성을 알 수 있음

Name	파일의 이름	Protected	암호화 또는 패스워드 보호 여부
File Ext	파일의 확장자	Last Accessed	마지막 접근한 날짜/시간
Logical Size	파일의 실제 크기	File Created	파일이 생성된 날짜/시간
Item Type	증거의 종류 Entry, Email, Record, or Document	Last Written	마지막 파일 수정 날짜/시간
Signature Analysis	파일 시그니처 분석 결과	MD5	파일의 MD5 해시값
File Type	파일 시그니처 확인 후 파일 유형	SHA1	파일의 SHA1 해시값
Item Path	파일명을 포함한 파일의 전체 경로	Is Deleted	파일 삭제 여부

3. Encase 기능 소개

■ 보기 창

- Fields
 - 선택한 대상에 대한 상세 정보 확인 가능



The screenshot shows the 'Fields' window in Encase software. The window has a menu bar with options: Fields, Report, Text, Hex, Decode, Doc, Transcript, Picture, Console, File Exts, Permissions, Hash Sets, Attributes, Lock, and Print. Below the menu bar is a table with two columns: 'Name' and 'Value'. The table lists various file attributes and their corresponding values.

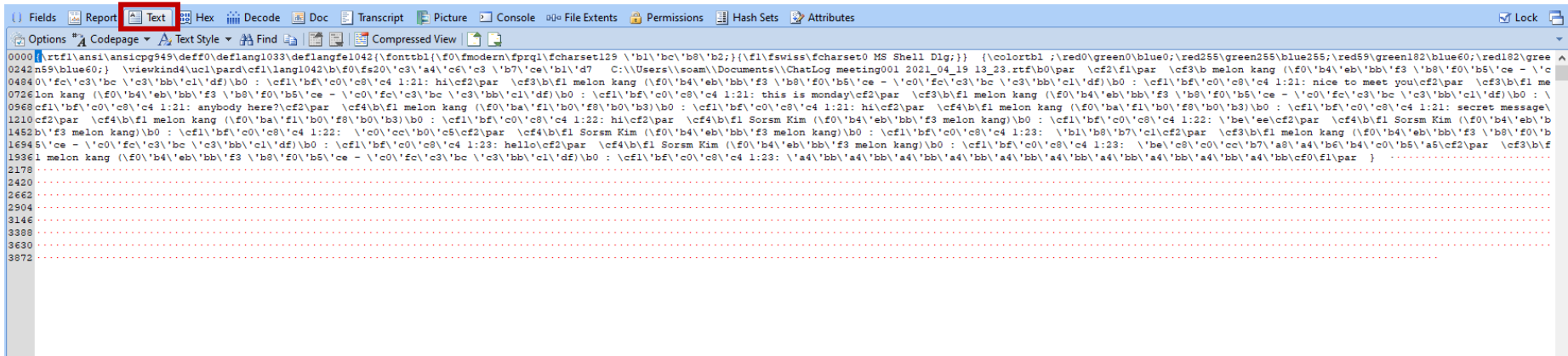
Name	Value
S Name	푸른 언덕.jpg
S Tag	
S File Ext	jpg
i Logical Size	28,521
i Category	Picture
i Signature Analysis	Match
S File Type	JPEG Image Standard
S Protected	
i Protection complexity	
Last Accessed	2015/07/25 09:43:02 오전
File Created	2015/07/23 11:07:45 오전
Last Written	2008/04/14 08:00:00 오후
b Is Picture	•
b Is Indexed	
i Code Page	
MD5	6fb2a38dc107eacb41cf1656e899cf70
SHA1	4eee44b18576e84de7b163142b537d2fe6231845
P Entropy	
S Item Path	Disk Image\C\Documents and Settings\All Users\Documents\My Pictures\그림 샘플\푸른 언덕.jpg
S True Path	Case1\Disk Image\C\Documents and Settings\All Users\Documents\My Pictures\그림 샘플\푸른 언덕.jpg
S Description	File, Archive
b Is Deleted	
Entry Modified	2015/07/23 11:07:45 오전
File Deleted	
File Acquired	
i Initialized Size	28,521
i Physical Size	28,672

3. Encase 기능 소개

■ 보기 창

- Text

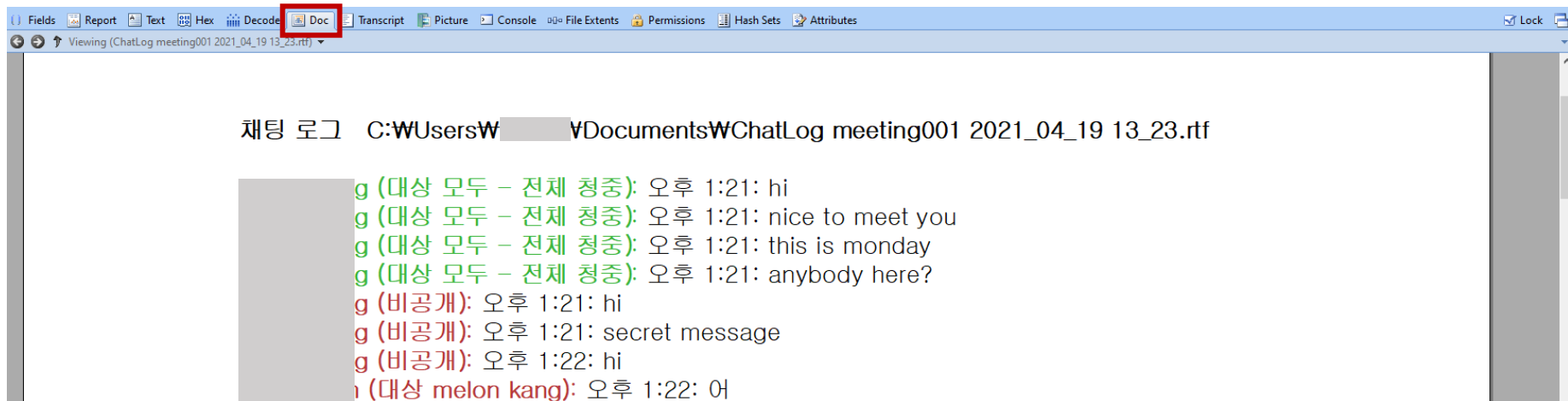
- 선택한 대상의 내용을 텍스트로 확인



3. Encase 기능 소개

■ 보기 창

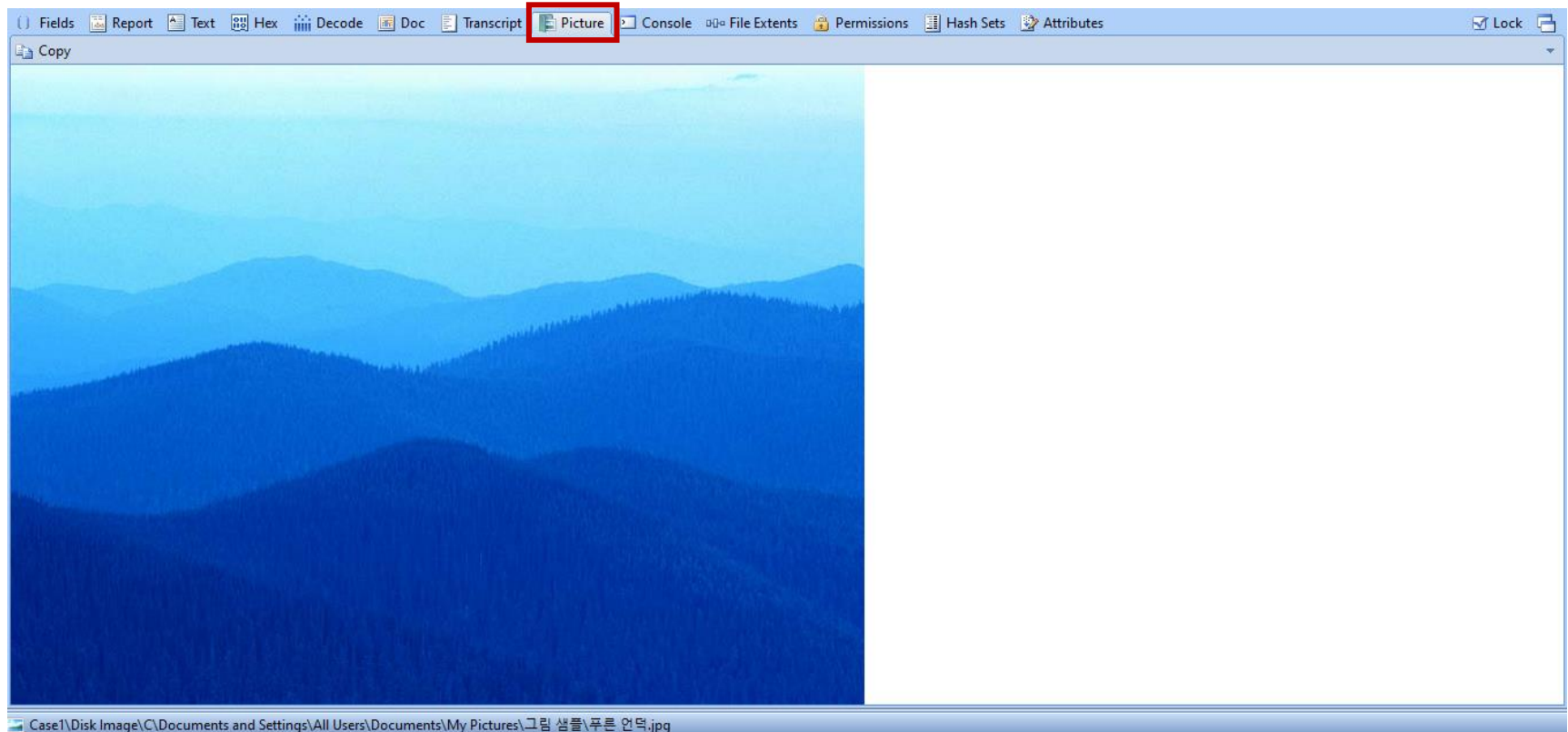
- Doc
 - 선택한 대상의 내용을 문서 형태로 확인 가능



3. Encase 기능 소개

- 보기 창

- Picture
 - 선택한 대상이 사진이면 해당 탭에서 사진 확인 가능



3. Encase 기능 소개

■ 보기 창

- Report

- 선택한 대상의 속성에 대한 세부 보고서

모든 속성을 볼 수 있으며, 파일 권한이 있는 경우에는 파일에 내용도 확인 가능

The screenshot shows the 'Report' tab selected in the Encase interface. The report displays the following details for the file 'ChatLog meeting001 2021_04_19 13_23.rtf':

Name	ChatLog meeting001 2021_04_19 13_23.rtf
File Ext	rtf
Logical Size	2,153
Category	Document
Last Accessed	2021/04/19 01:23:37 오후
File Created	2021/04/19 01:23:37 오후
Last Written	2021/04/19 01:23:37 오후
Item Path	C:\Users\soam\Documents\ChatLog meeting001 2021_04_19 13_23.rtf
True Path	Case1\C\Users\soam\Documents\ChatLog meeting001 2021_04_19 13_23.rtf
Description	File, Archive
Entry Modified	2021/04/19 01:23:48 오후
Initialized Size	2,153
Physical Size	4,096
Starting Extent	0C-C37627
File Extents	1
Permissions	•
Physical Location	154,120,192
Physical Sector	301,016
Evidence File	C
File Identifier	15532
GUID	90c98ed33194a68cbd1a0de0e12c3413
Short Name	CHATLO~2.RTF
Attributes	•
Sequence ID	72

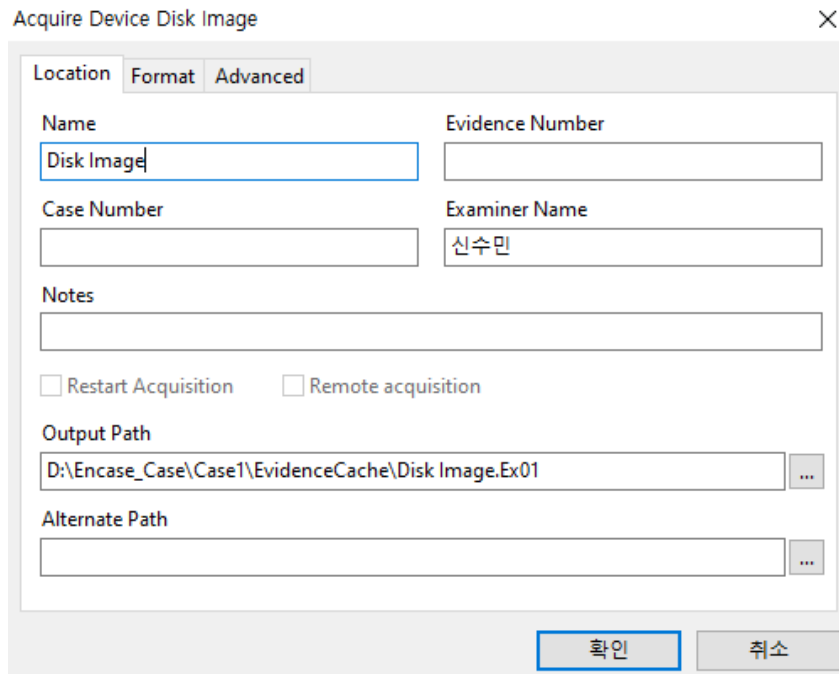
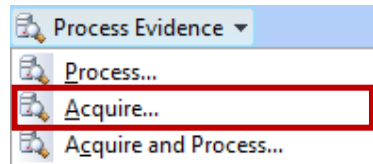
Object Identifiers

Own Id	{68F471DA-A093-11EB-82A7-001A7DDA710F} (Sequence:02A7 Timestamp: 2021/04/18 10:14:14 오후 MAC:00-1A-7D-DA-71-0F)
Birth Volume Id	{8A8E03CA-22D8-4071-8B8C-83D787445E1C}
Birth Object Id	{68F471DA-A093-11EB-82A7-001A7DDA710F} (Sequence:02A7 Timestamp: 2021/04/18 10:14:14 오후 MAC:00-1A-7D-DA-71-0F)

3. Encase 기능 소개

▪ Acquire

- 증거 획득
 - Image 사본 만들기



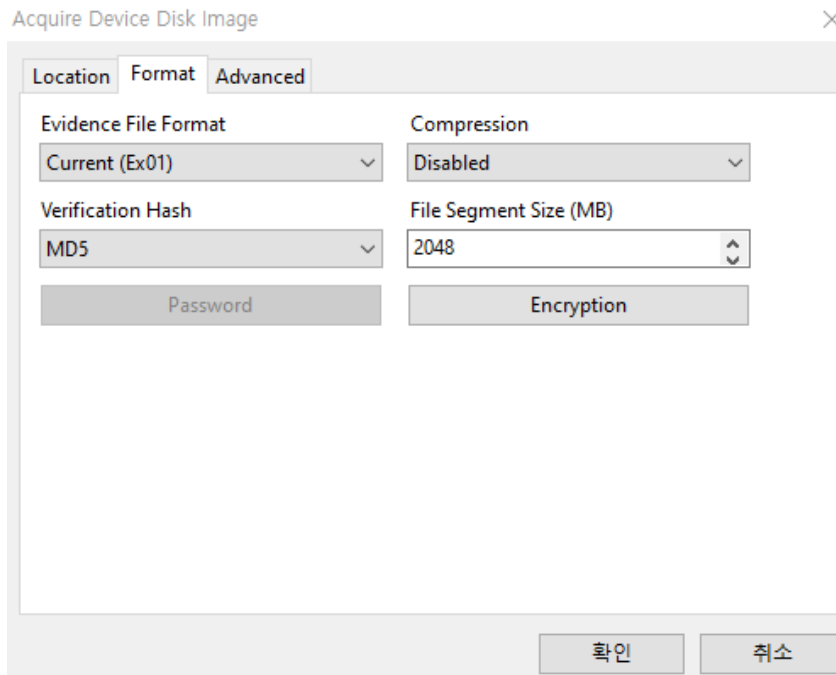
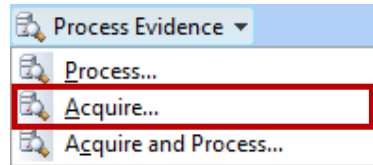
▪ Location

- 증거 파일 이름
- 증거파일 번호
- 사건 번호
- 조사관 이름
- 저장경로

3. Encase 기능 소개

■ Acquire

- 증거 획득
 - Image 사본 만들기



■ Format

- 증거 파일 포맷
 - Ex01
 - E01
- 압축 여부
- 해시 알고리즘
- 비밀번호/암호화

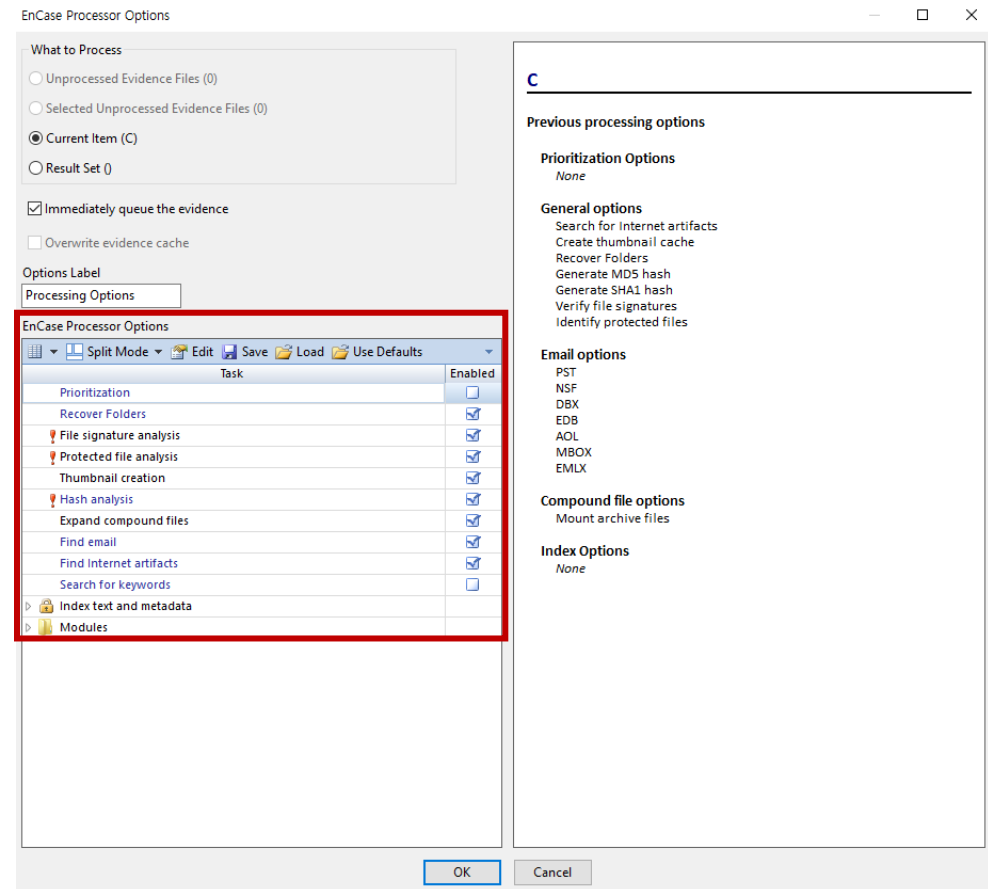
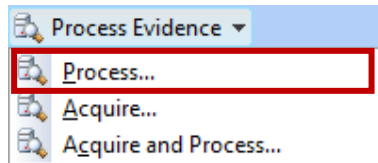


3. Encase 기능 소개

■ Process

- 증거 분석

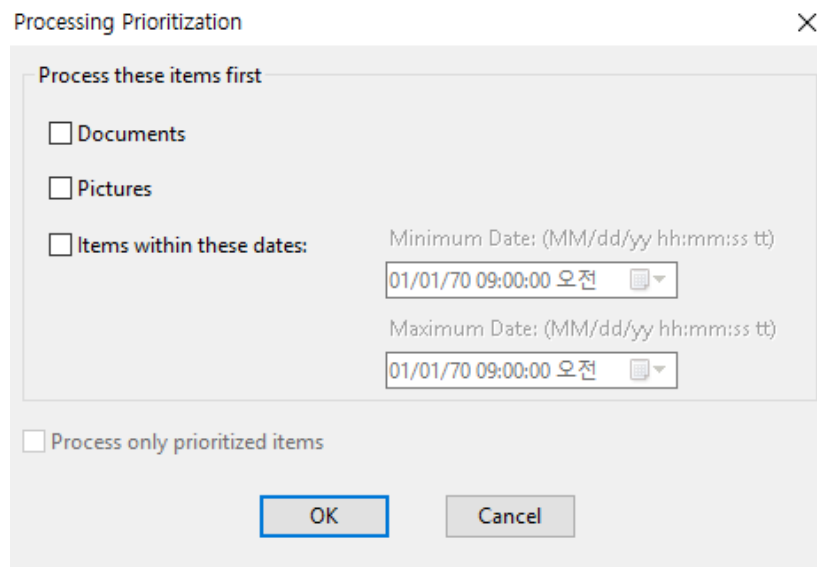
- 증거를 적절하게 조사하기 위해 일련의 과정들을 한번에 수행할 수 있도록 도구들을 모아 놓은 것



3. Encase 기능 소개

▪ Process

- 증거 분석 – Processor Options
 - Prioritization
 - : 우선적으로 먼저 처리할 대상을 선정



3. Encase 기능 소개

▪ Process

- 증거 분석 – Processor Options

- Recovering Folders

- : 폴더 복구

- FAT와 NTFS 파일 시스템에만 사용가능

- 복구 시 원래 폴더 구조로 재구성하여 보여줌

- 해당 옵션을 선택하지 않으면 복구된 파일들을 하나의 그룹으로 묶어서 보여줌

- File signature analysis

- : 파일 확장자, 파일 헤더의 시그니처를 비교함으로써 파일 유형 확인

- Protected file analysis

- : 파일이 암호화되거나 보호된 파일들을 확인

- Hash analysis

- : 파일들의 해시값, 엔트로피 계산

3. Encase 기능 소개

▪ Process

- 증거 분석 – Processor Options

- Expand compound files

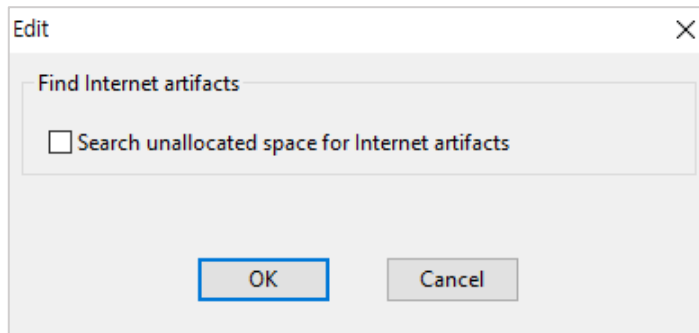
: ZIP 파일과 같은 복합 파일들을 모두 트리 형태로 풀어서 보여줌

- Find email

: PST, NSF, DBX, EDB, EMLX, AQL, MBOX 파일에 대해 이메일 파싱

- Find Internet artifacts

: 브라우저 종류에 대해 인터넷 검색 기록 확인 가능



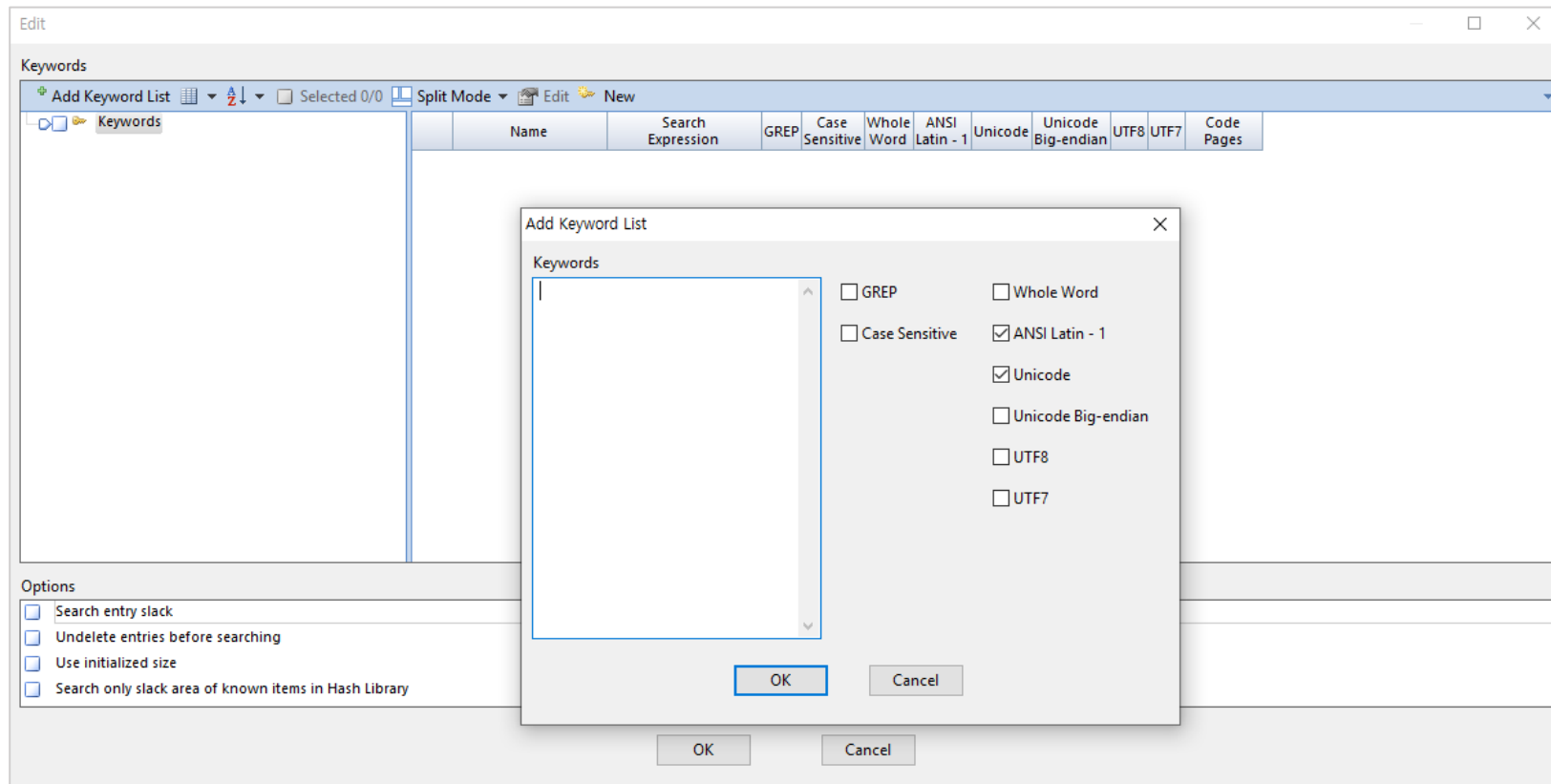
3. Encase 기능 소개

▪ Process

- 증거 분석 – Processor Options

- Search for keywords

: 키워드를 넣어서 미리 검색어를 프로세싱



3. Encase 기능 소개

▪ Process

- 증거 분석 – Processor Options

- Modules

: Disk 내 포함된 운영 체제에 대해서 log나 레지스트리 등 아티팩트를 볼 수 있음

Modules	
System Info Parser	<input checked="" type="checkbox"/>
IM Parser	<input type="checkbox"/>
File Carver	<input checked="" type="checkbox"/>
Windows Event Log Parser	<input checked="" type="checkbox"/>
Windows Artifact Parser	<input checked="" type="checkbox"/>
Unix Login	<input type="checkbox"/>
Linux Syslog Parser	<input type="checkbox"/>
OS X Artifact Parser	<input checked="" type="checkbox"/>

3. Encase 기능 소개

▪ Process

- 증거 분석

- 선택한 옵션에 대한 Process 결과를 Records 탭에서 결과 확인 가능

The diagram illustrates the EnCase Forensic interface and its various record views. On the left, the main interface shows the 'Records' tab selected in the left sidebar, with a tree view containing 'Archive', 'Internet', 'Thumbnails', 'Evidence Processor Module Results', and 'Email'. A large orange arrow points from this interface to five example record views on the right.

[Archive]

	Name
1	\$ROR05Z8.zip
2	G973NKSU3ASII_G973NOKR3ASII_KOO.zip
3	Acrobat DC_en_GB_WIN_64.zip

[Internet]

	Name
1	Internet Explorer (Windows)
2	Chrome (Windows)

[Thumbnails]

	Is Deleted	Name
16184		tb_btn_add.png
16185		tb_btn_bugreporter.png
16186		tb_btn_codepage.png

[Evidence Processor Module Results]

	Name
1	Windows Artifact Parser - Records
2	Windows Event Log Parser - Records

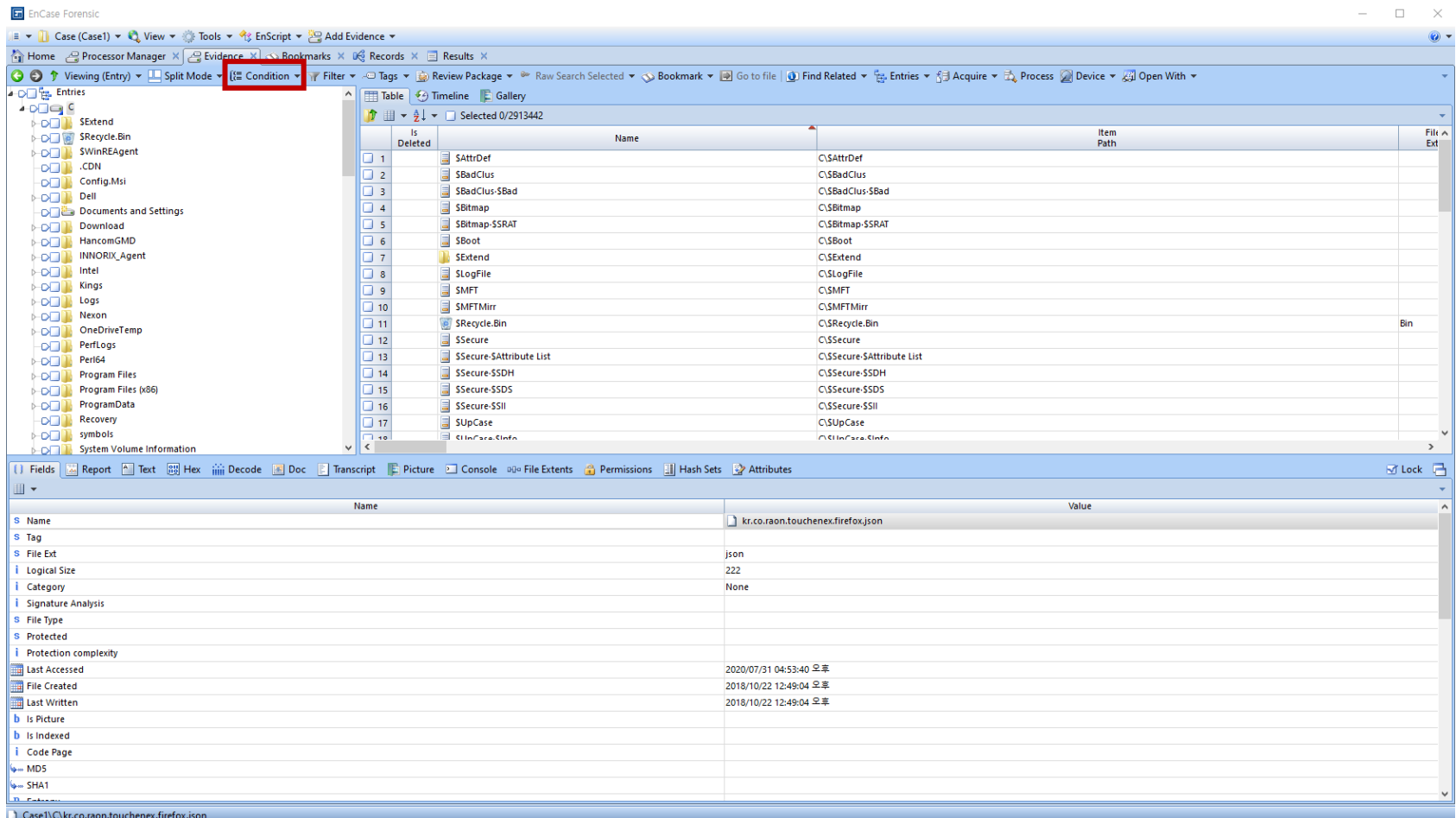
[Email]

	Name
1	Outlookimap.gmail.com-00000003.pst
2	backup.pst
3	backup.pst
4	Outlook.pst

3. Encase 기능 소개

▪ Condition

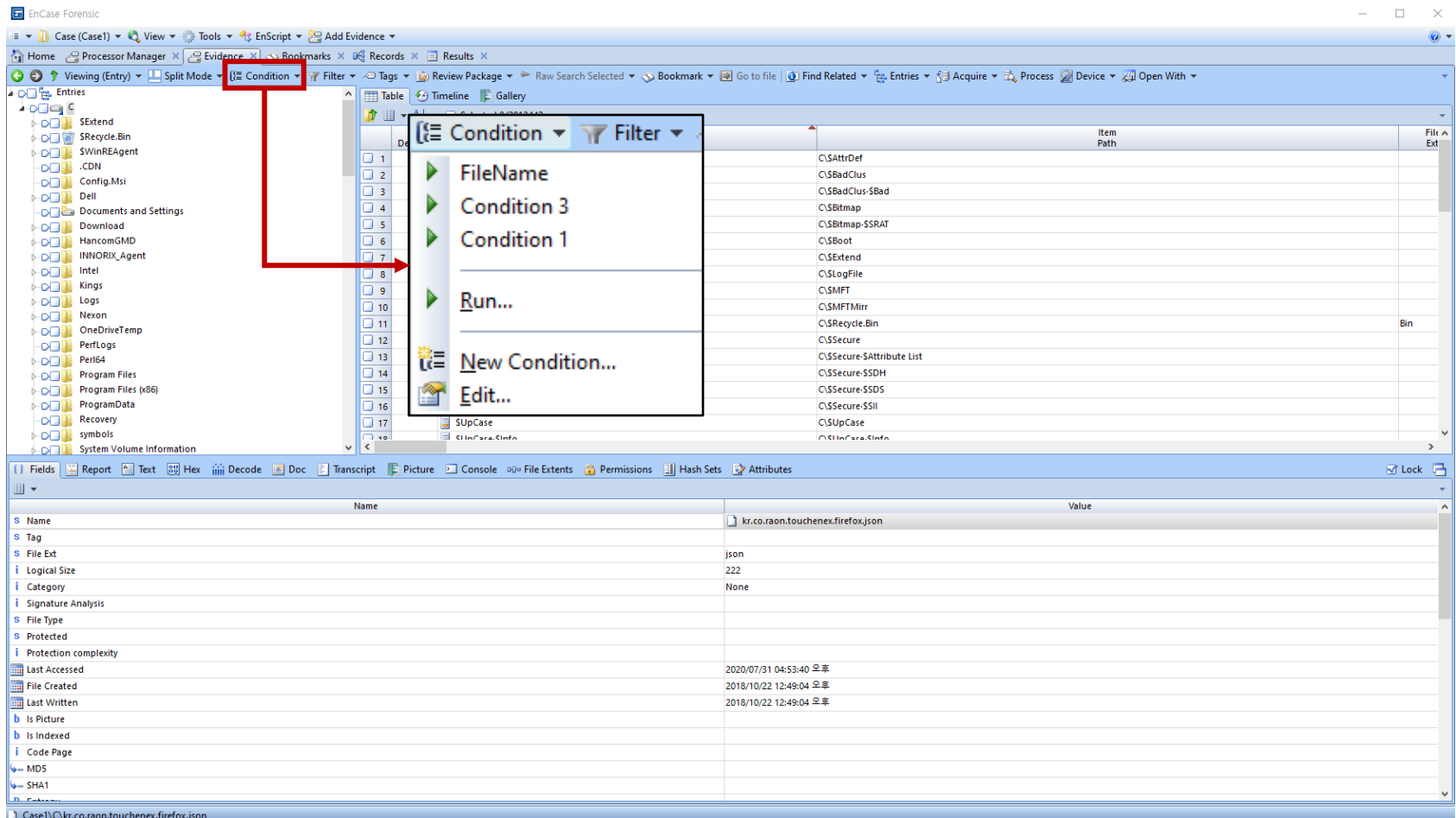
- 파일에 대해 조건문을 수행



3. Encase 기능 소개

■ Condition

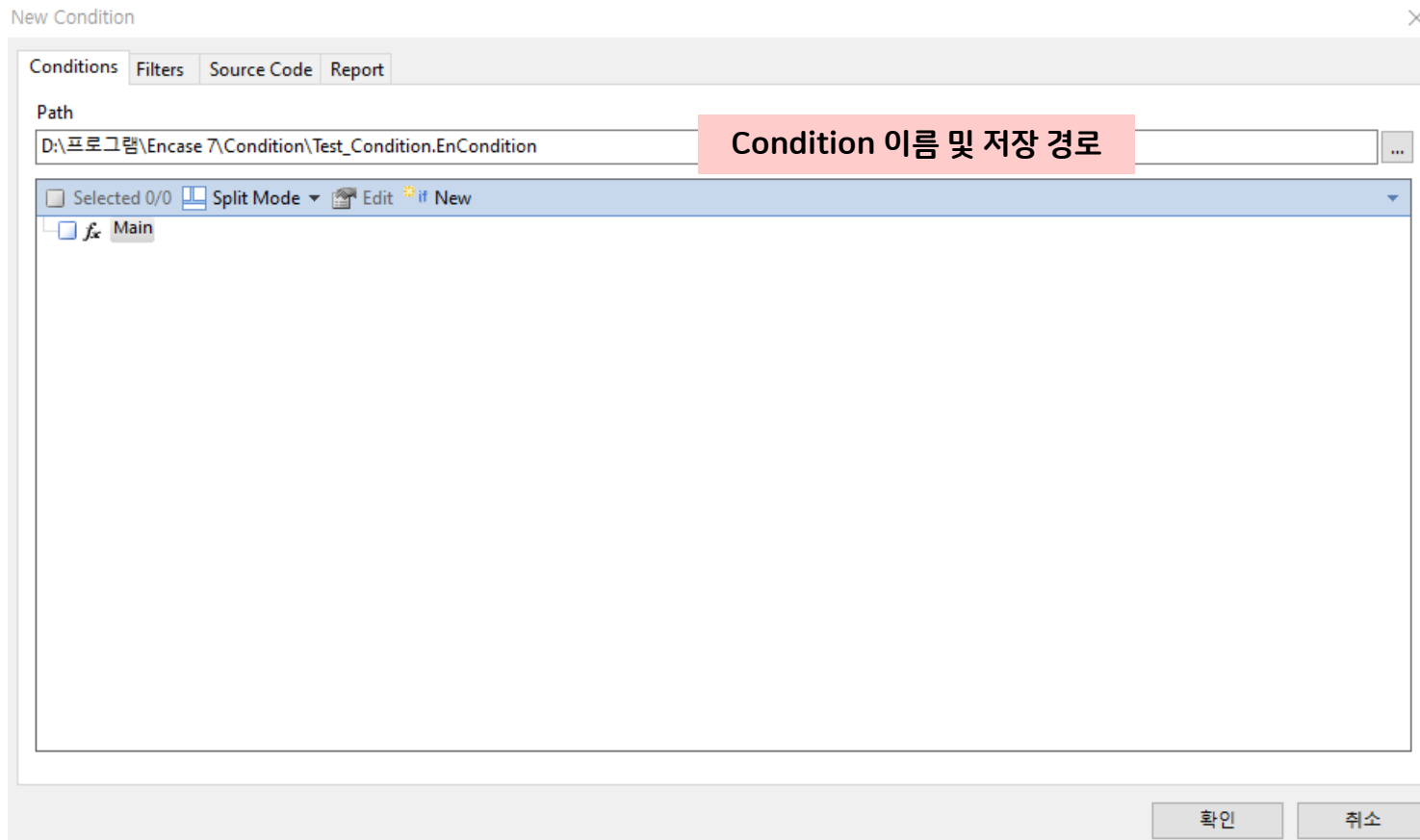
- 파일에 대해 조건문을 수행



3. Encase 기능 소개

▪ Condition

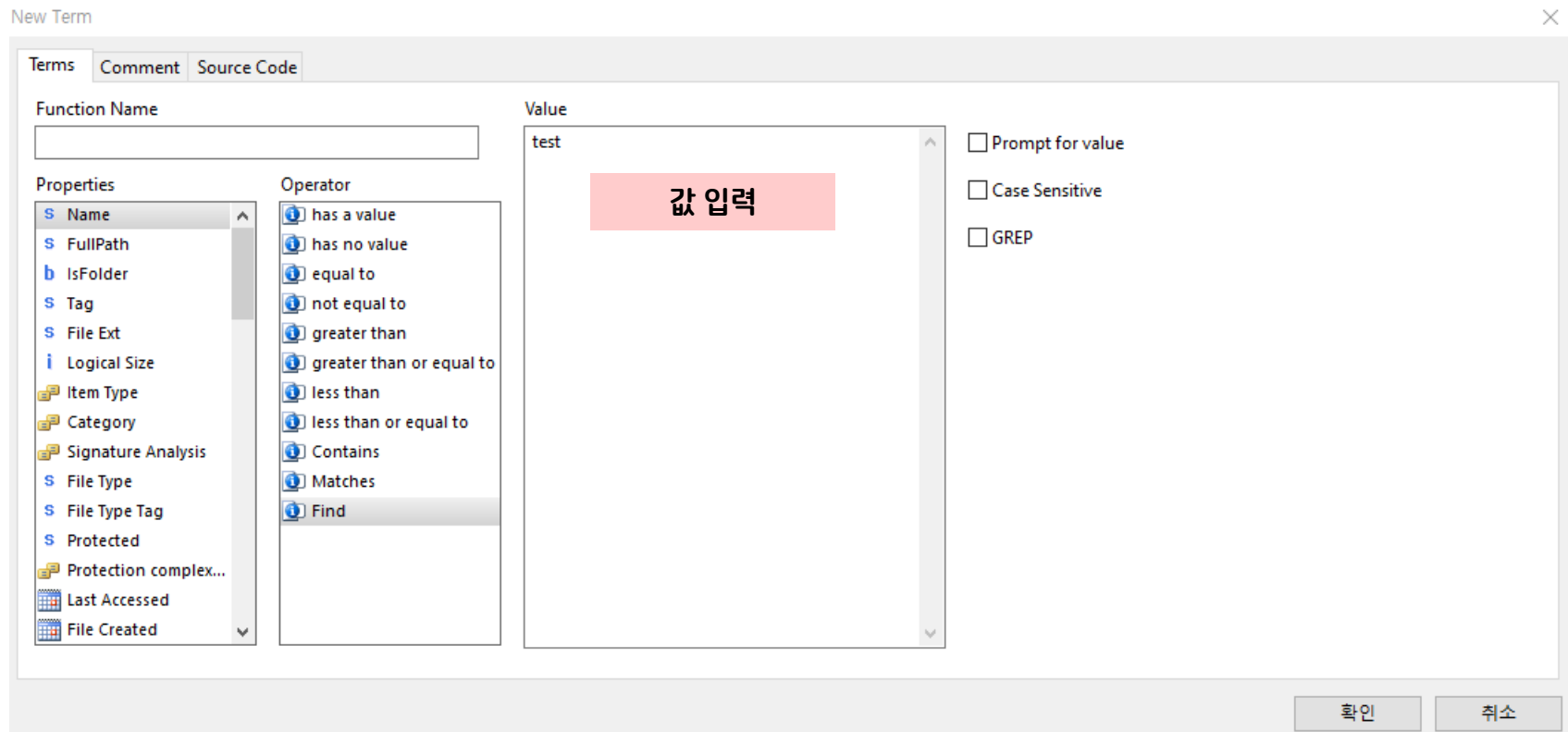
- New Condition 생성



3. Encase 기능 소개

▪ Condition

- New Condition 생성

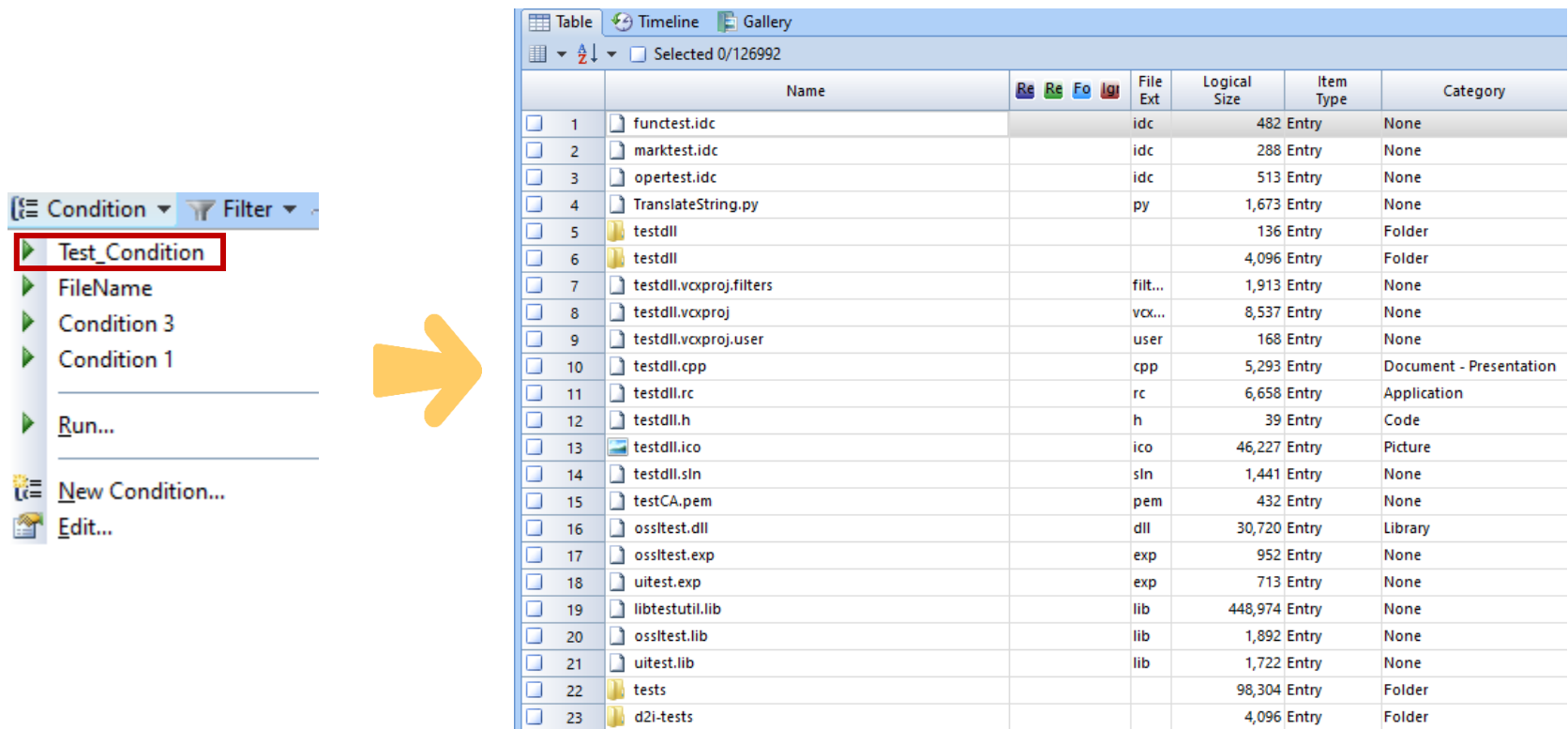


⇒ 파일명에 test가 포함되는 파일 찾기

3. Encase 기능 소개

▪ Condition

- Condition 실행 결과



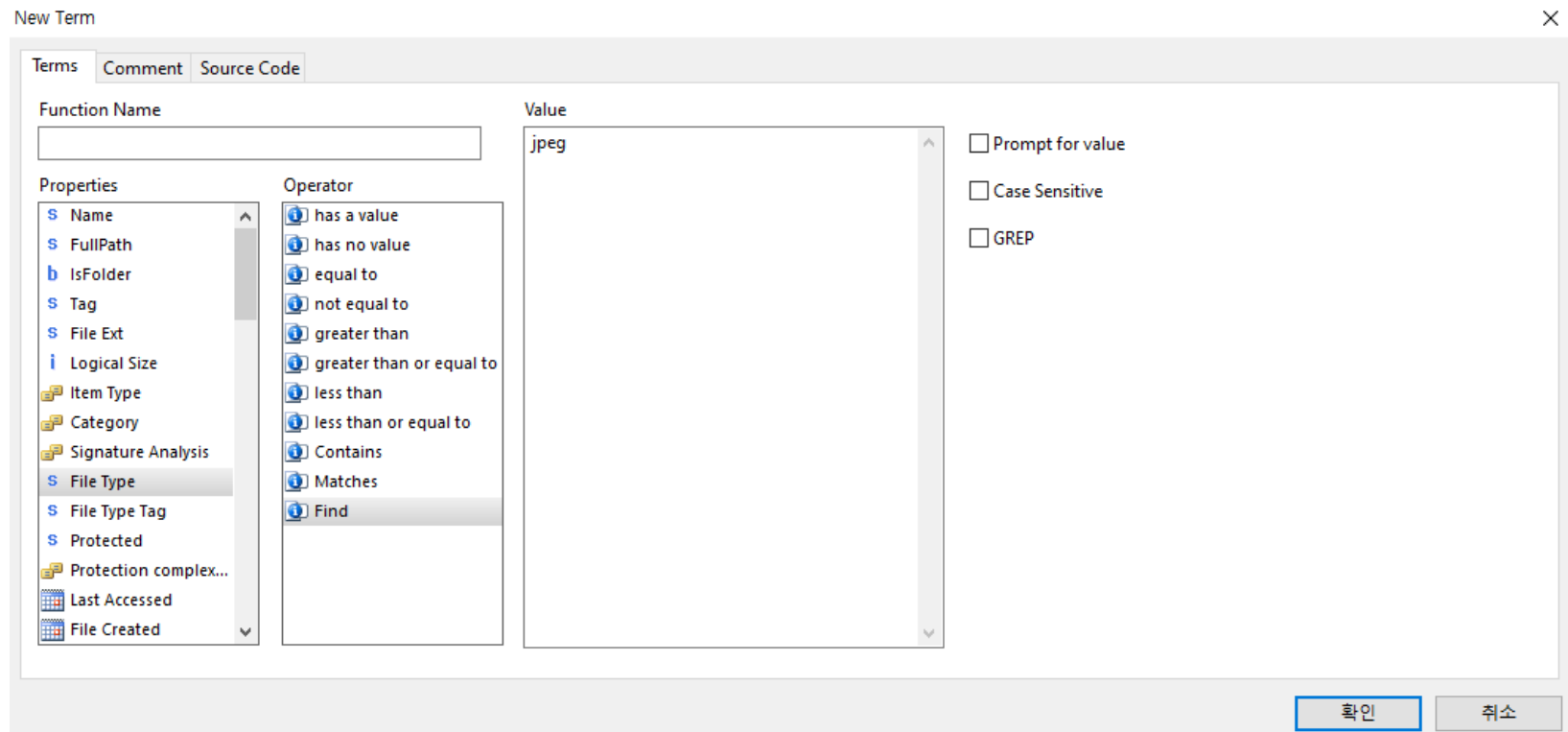
	Name	Re	Re	Fo	Log	File Ext	Logical Size	Item Type	Category
<input type="checkbox"/> 1	functest.idc					idc	482	Entry	None
<input type="checkbox"/> 2	marktest.idc					idc	288	Entry	None
<input type="checkbox"/> 3	opertest.idc					idc	513	Entry	None
<input type="checkbox"/> 4	TranslateString.py					py	1,673	Entry	None
<input type="checkbox"/> 5	testdll						136	Entry	Folder
<input type="checkbox"/> 6	testdll						4,096	Entry	Folder
<input type="checkbox"/> 7	testdll.vcxproj.filters					filt...	1,913	Entry	None
<input type="checkbox"/> 8	testdll.vcxproj					vcx...	8,537	Entry	None
<input type="checkbox"/> 9	testdll.vcxproj.user					user	168	Entry	None
<input type="checkbox"/> 10	testdll.cpp					cpp	5,293	Entry	Document - Presentation
<input type="checkbox"/> 11	testdll.rc					rc	6,658	Entry	Application
<input type="checkbox"/> 12	testdll.h					h	39	Entry	Code
<input type="checkbox"/> 13	testdll.ico					ico	46,227	Entry	Picture
<input type="checkbox"/> 14	testdll.sin					sin	1,441	Entry	None
<input type="checkbox"/> 15	testCA.pem					pem	432	Entry	None
<input type="checkbox"/> 16	osstest.dll					dll	30,720	Entry	Library
<input type="checkbox"/> 17	osstest.exp					exp	952	Entry	None
<input type="checkbox"/> 18	uittest.exp					exp	713	Entry	None
<input type="checkbox"/> 19	libtestutil.lib					lib	448,974	Entry	None
<input type="checkbox"/> 20	osstest.lib					lib	1,892	Entry	None
<input type="checkbox"/> 21	uittest.lib					lib	1,722	Entry	None
<input type="checkbox"/> 22	tests						98,304	Entry	Folder
<input type="checkbox"/> 23	d2i-tests						4,096	Entry	Folder

[Condition 실행 결과]

3. Encase 기능 소개

▪ Condition

- New Condition 생성




⇒ 파일 유형에 jpeg가 포함되는 파일 찾기

3. Encase 기능 소개

▪ Condition

- Condition 실행 결과



The image shows the 'Condition' menu on the left with 'Test2_Condition' highlighted. A yellow arrow points from this menu item to the 'Table' view of the Encase interface on the right. The 'Table' view displays a list of files with columns for Name, File Ext, Logical Size, Item Type, Category, Signature Analysis, File Type, and File Type Tag. The 'File Type' column is highlighted with a blue box.

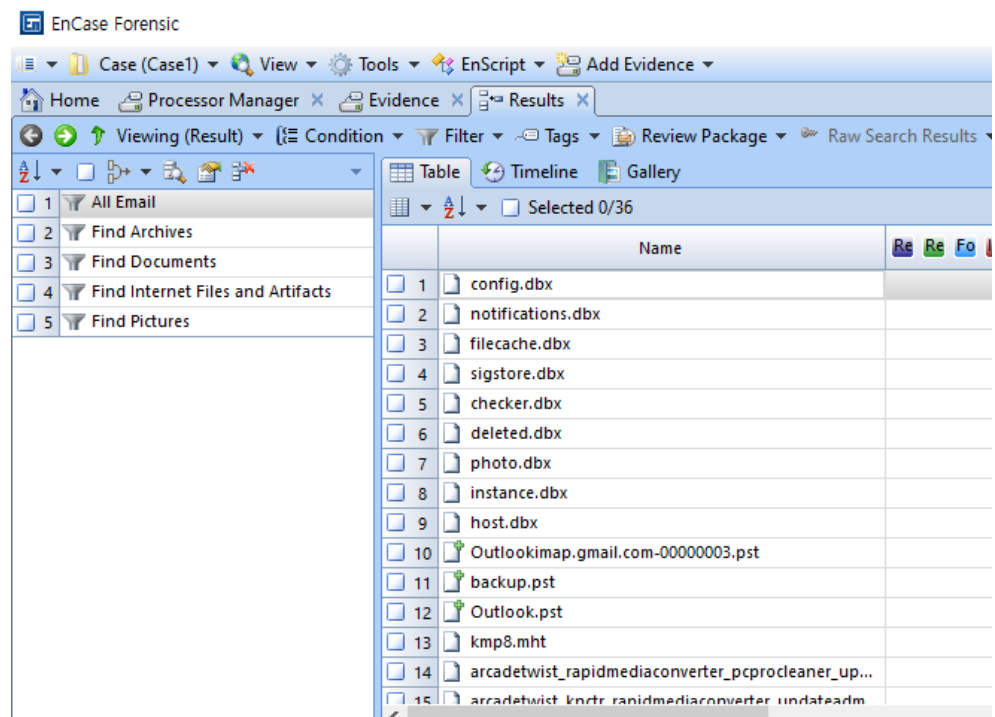
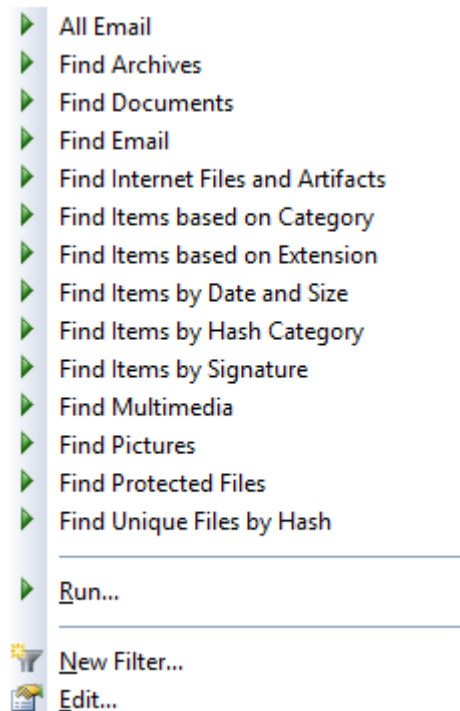
	Name	File Ext	Logical Size	Item Type	Category	Signature Analysis	File Type	File Type Tag
67	xq5CQOo18FGzhrbQiroOvyHG00.cnt.jpg	jpg	76,842	Entry	Picture	Match	JPEG Image Non-Standard	pg
68	1djou0ePxsB8TeAcfjAghgbTjiA.cnt	cnt	165,155	Entry	Picture	Alias	JPEG Image Non-Standard	pg
69	6dRkZGnwLOIC59ZlvMO6qJa5bjs.cnt	cnt	154,584	Entry	Picture	Alias	JPEG Image Standard	pg1
70	2f757d3b8c27b313eac51fc751e470c219c369bbf06c5...	0	5,832	Entry	Picture	Alias	JPEG Image Standard	pg1
71	69a0e3f50050a1570d1ad82d1b404b4e855a18e9fce1...	0	5,801	Entry	Picture	Alias	JPEG Image Standard	pg1
72	5a5ece553897464929f0699be398f955		220,472	Entry	Picture	Alias	JPEG Image Non-Standard	pg
73	914c093f6571a4facad59705ccc32aae		220,472	Entry	Picture	Alias	JPEG Image Non-Standard	pg
74	28acec758dc49c83b9a8eb7c533a064c		244,937	Entry	Picture	Alias	JPEG Image Non-Standard	pg
75	042b0ad8dfb3d1625603595858fe002c		44,913	Entry	Picture	Alias	JPEG Image Non-Standard	pg
76	icon_add_lightgray.png	png	558	Entry	Picture	Alias	JPEG Image Standard	pg1
77	icon_add_darkgray.png	png	634	Entry	Picture	Alias	JPEG Image Standard	pg1
78	icon_minus_lightgray.png	png	496	Entry	Picture	Alias	JPEG Image Standard	pg1
79	icon_minus_darkgray.png	png	520	Entry	Picture	Alias	JPEG Image Standard	pg1
80	DoubleButton.png	png	72,558	Entry	Picture	Alias	JPEG Image Standard	pg1
81	CountDown.png	png	79,227	Entry	Picture	Alias	JPEG Image Standard	pg1
82	Fold.png	png	148,033	Entry	Picture	Alias	JPEG Image Standard	pg1
83	Logo.png	png	16,181	Entry	Picture	Alias	JPEG Image Standard	pg1
84	BottomLineBar.png	png	171,848	Entry	Picture	Alias	JPEG Image Standard	pg1
85	Checkbox.png	png	102,286	Entry	Picture	Alias	JPEG Image Standard	pg1
86	icon_add_lightgray.png	png	558	Entry	Picture	Alias	JPEG Image Standard	pg1
87	icon_add_darkgray.png	png	634	Entry	Picture	Alias	JPEG Image Standard	pg1
88	icon_minus_lightgray.png	png	496	Entry	Picture	Alias	JPEG Image Standard	pg1
89	icon_minus_darkgray.png	png	520	Entry	Picture	Alias	JPEG Image Standard	pg1

[Condition 실행 결과]

3. Encase 기능 소개

▪ Filter

- 증거 내 파일 중 원하는 데이터를 필터링하여 확인 가능
 - 이메일, 아카이브 파일, 문서 파일 등과 관련된 파일들을 필터링
 - Results 탭에서 확인 가능



3. Encase 기능 소개

■ Filter

- All Email

- 이메일과 관련된 파일 필터링 결과

The screenshot displays the EnCase Forensic interface with the 'Results' pane showing a list of files filtered by 'All Email'. The table below represents the data shown in the results pane.

	Name	File Ext	Logical Size	Item Type	Category	Signature Analysis	File Type	File Type Tag	Prot
1	config.dbx	dbx	9,216 Entry	Email	Bad signature				
2	notifications.dbx	dbx	2,048 Entry	Email	Bad signature				
3	filecache.dbx	dbx	67,584 Entry	Email	Bad signature				
4	sigstore.dbx	dbx	21,504 Entry	Email	Bad signature				
5	checker.dbx	dbx	11,264 Entry	Email	Bad signature				
6	deleted.dbx	dbx	7,168 Entry	Email	Bad signature				
7	photo.dbx	dbx	17,408 Entry	Email	Bad signature				
8	instance.dbx	dbx	5,120 Entry	Email	Bad signature				
9	host.dbx	dbx	253 Entry	Email	Bad signature				
10	Outlookimap.gmail.com-00000003.pst	pst	2,556,928 Entry	Email	Match		Outlook Personal Folder	pst	
11	backup.pst	pst	271,360 Entry	Email	Match		Outlook Personal Folder	pst	
12	Outlook.pst	pst	1,033,216 Entry	Email	Match		Outlook Personal Folder	pst	
13	kmp8.mht	mht	6,350 Entry	Email	Alias		MBox	mbox	
14	arcadewist_rapidmediconverter_pcprocleaner_up...	mht	76,211 Entry	Email	Alias		MBox	mbox	
15	arcadewist_kodr_rapidmediconverter_updateadm	mht	76,154 Entry	Email	Alias		MBox	mbox	

The bottom pane shows the details for the selected file 'config.dbx':

Name	Value
Name	config.dbx
Tag	
File Ext	dbx
Logical Size	9,216
Item Type	Entry
Category	Email
Signature Analysis	Bad signature
File Type	
File Type Tag	
Protected	
Protection complexity	
Last Accessed	2015/07/31 07:18:14 오후

Case1\Disk Image\C:\Documents and Settings\Administrator\Local Settings\Application Data\Dropbox\instance1\config.dbx

3. Encase 기능 소개

■ Filter

- Find Archives

- 아카이브 파일(압축 파일) 필터링 결과

The screenshot displays the EnCase Forensic interface. The top menu bar includes Case (Case1), View, Tools, EnScript, and Add Evidence. The main toolbar shows options like Home, Processor Manager, Evidence, Results, and various search and analysis tools. The left sidebar contains a tree view with categories like All Email, Find Archives, Find Documents, Find Internet Files and Artifacts, and Find Pictures. The main pane shows a table of search results for archives.

Name	File Ext	Logical Size	Item Type	Category	Signature Analysis	File Type	File Type Tag	Pr
1 rdrmessage.zip	zip	37,952 Entry	Archive	Match	ZIP Compressed	zip		
2 94308059B57B3142E455B38A6E892015		50,015 Entry	Archive	Alias	Microsoft Compressed	cab		
3 f_000cde		64,623 Entry	Archive	Alias	GZIP Compressed Archive	gz		
4 f_000cea		22,739 Entry	Archive	Alias	GZIP Compressed Archive	gz		
5 f_000ceb		135,293 Entry	Archive	Alias	GZIP Compressed Archive	gz		
6 f_000cee		16,820 Entry	Archive	Alias	GZIP Compressed Archive	gz		
7 f_000cef		21,264 Entry	Archive	Alias	GZIP Compressed Archive	gz		
8 f_000cd7		29,534 Entry	Archive	Alias	GZIP Compressed Archive	gz		
9 f_000c15		20,679 Entry	Archive	Alias	GZIP Compressed Archive	gz		
10 f_00028e		42,927 Entry	Archive	Alias	GZIP Compressed Archive	gz		
11 f_00072a		27,372 Entry	Archive	Alias	GZIP Compressed Archive	gz		
12 f_00007a		26,737 Entry	Archive	Alias	GZIP Compressed Archive	gz		
13 f_000e48		29,225 Entry	Archive	Alias	GZIP Compressed Archive	gz		
14 f_000e3d		31,140 Entry	Archive	Alias	GZIP Compressed Archive	gz		
15 f_000e3a		67,019 Entry	Archive	Alias	GZIP Compressed Archive	gz		

The bottom pane shows the details for the selected file, 'rdrmessage.zip'. It lists various attributes such as Name, Tag, File Ext, Logical Size, Item Type, Category, Signature Analysis, File Type, File Type Tag, Protected, Protection complexity, and Last Accessed.

Name	Value
S Name	rdrmessage.zip
S Tag	
S File Ext	zip
i Logical Size	37,952
i Item Type	Entry
i Category	Archive
i Signature Analysis	Match
S File Type	ZIP Compressed
S File Type Tag	zip
S Protected	
i Protection complexity	
Last Accessed	2015/07/27 09:36:01 오전

The status bar at the bottom indicates the current case and file path: Case1\Disk Image\C:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\10.0\rdrmessage.zip.

3. Encase 기능 소개

■ Filter

- Find Documents

- 문서 파일 필터링 결과

The screenshot displays the EnCase Forensic interface. The 'Viewing (Result)' pane shows a list of files found during a search. The 'Fields' pane at the bottom provides detailed information for the selected file, 'TMGrpPrm.sav'.

Name	File Ext	Logical Size	Item Type	Category	Signature Analysis	File Type	File Type Tag
1 TMGrpPrm.sav	sav	54 Entry	Document	Alias	Adobe PDF	pdf	
2 TMDocs.sav	sav	36 Entry	Document	Alias	Adobe PDF	pdf	
3 Outlook.xml	xml	2,629 Entry	Document	Match	XML Document	xml1	
4 Outlook.srs	srs	3,072 Entry	Document	Alias	Compound Document File	doc	
5 Normal.dot	dot	32,256 Entry	Document	Match	Microsoft Word Template	dot	
6 ~\$Normal.dot	dot	162 Entry	Document	Bad signature			
7 FAEMFNZY.txt	txt	206 Entry	Document	Match	Text	txt	
8 9JCS9LX3.txt	txt	117 Entry	Document	Match	Text	txt	
9 OLSX63VN.txt	txt	278 Entry	Document	Match	Text	txt	
10 2CSRPCOK.txt	txt	130 Entry	Document	Match	Text	txt	
11 D4731AIA.txt	txt	826 Entry	Document	Match	Text	txt	
12 5AHS1P31.txt	txt	83 Entry	Document	Match	Text	txt	
13 GUDTO9R1.txt	txt	284 Entry	Document	Match	Text	txt	
14 VAGB3XE1.txt	txt	574 Entry	Document	Match	Text	txt	
15 F4VINC64H.txt	txt	471 Entry	Document	Match	Text	txt	

Name	Value
S Name	TMGrpPrm.sav
S Tag	
S File Ext	sav
i Logical Size	54
i Item Type	Entry
i Category	Document
i Signature Analysis	Alias
S File Type	Adobe PDF
S File Type Tag	pdf
S Protected	
i Protection complexity	
Last Accessed	2015/07/27 09:47:38 오전

3. Encase 기능 소개

■ Filter

- Find Internet Files and Artifacts

- 인터넷 기록 관련 파일 필터링 결과
- index.dat 파일들이 존재

The screenshot displays the EnCase Forensic interface. The 'Filter' pane on the left shows the 'Find Internet Files and Artifacts' filter selected. The main pane shows a table of search results for index.dat files.

Name	File Ext	Logical Size	Item Type	Category	Signature Analysis	File Type	File Type Tag	Prot
1 index.dat	dat	49,152 Entry	Internet	Match	IE History DAT File	dat3		
2 index.dat	dat	16,384 Entry	Internet	Match	IE History DAT File	dat3		
3 index.dat	dat	262,144 Entry	Internet	Match	IE History DAT File	dat3		
4 index.dat	dat	32,768 Entry	Internet	Match	IE History DAT File	dat3		
5 index.dat	dat	32,768 Entry	Internet	Match	IE History DAT File	dat3		
6 index.dat	dat	49,152 Entry	Internet	Match	IE History DAT File	dat3		
7 index.dat	dat	32,768 Entry	Internet	Match	IE History DAT File	dat3		
8 index.dat	dat	32,768 Entry	Internet	Match	IE History DAT File	dat3		
9 index.dat	dat	32,768 Entry	Internet	Match	IE History DAT File	dat3		
10 index.dat	dat	32,768 Entry	Internet	Match	IE History DAT File	dat3		
11 index.dat	dat	32,768 Entry	Internet	Match	IE History DAT File	dat3		
12 index.dat	dat	81,920 Entry	Internet	Match	IE History DAT File	dat3		
13 index.dat	dat	16,384 Entry	Internet	Match	IE History DAT File	dat3		
14 index.dat	dat	16,384 Entry	Internet	Match	IE History DAT File	dat3		
15 index.dat	dat	32,768 Entry	Internet	Match	IE History DAT File	dat3		

The bottom pane shows the details for the selected 'index.dat' file:

Name	Value
S Name	index.dat
S Tag	
S File Ext	dat
i Logical Size	49,152
i Item Type	Entry
i Category	Internet
i Signature Analysis	Match
S File Type	IE History DAT File
S File Type Tag	dat3
S Protected	
i Protection complexity	
Last Accessed	2015/07/23 11:11:07 오전

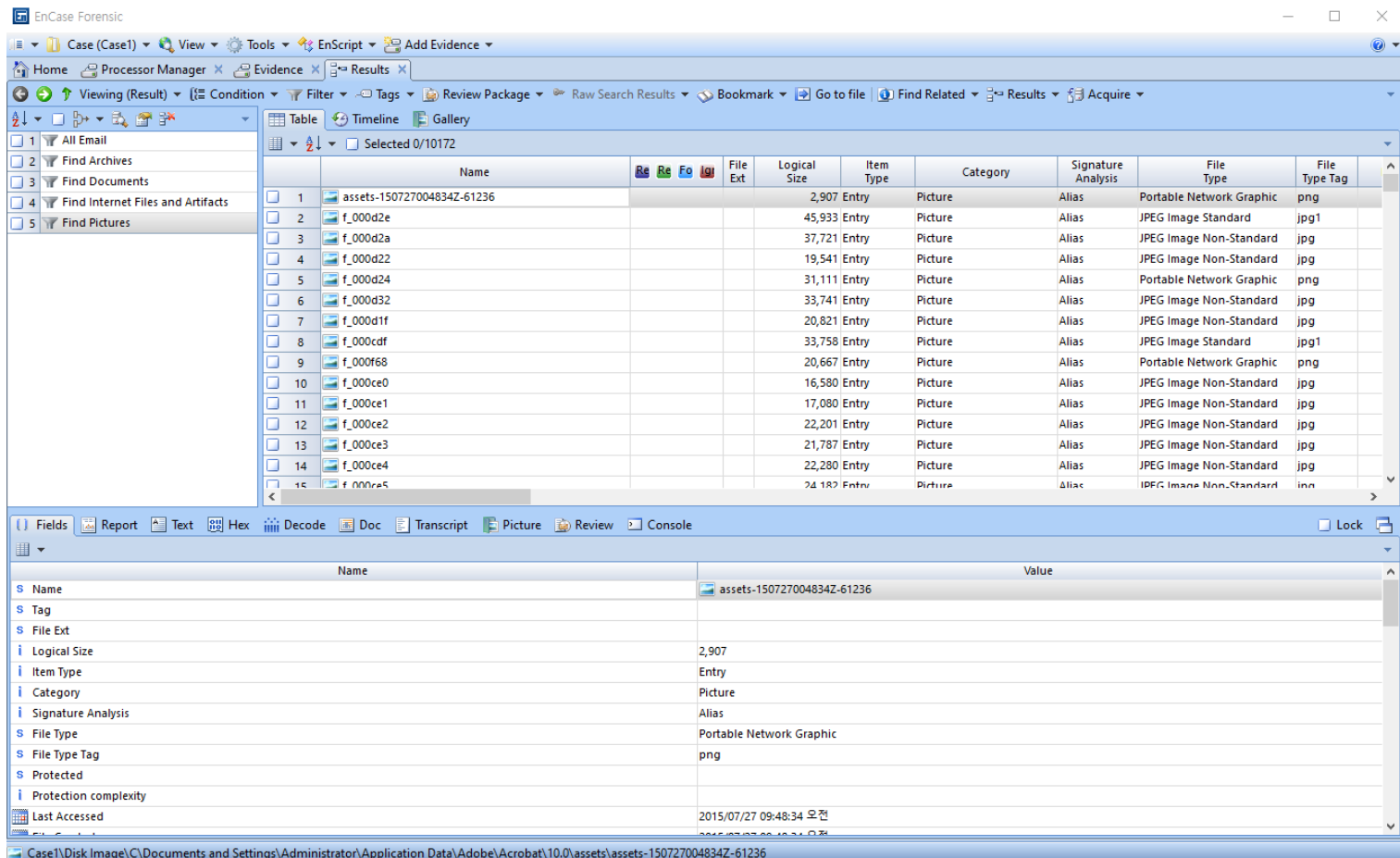
Case1\Disk Image\C:\Documents and Settings\Administrator\Cookies\index.dat

3. Encase 기능 소개

■ Filter

- Find Pictures

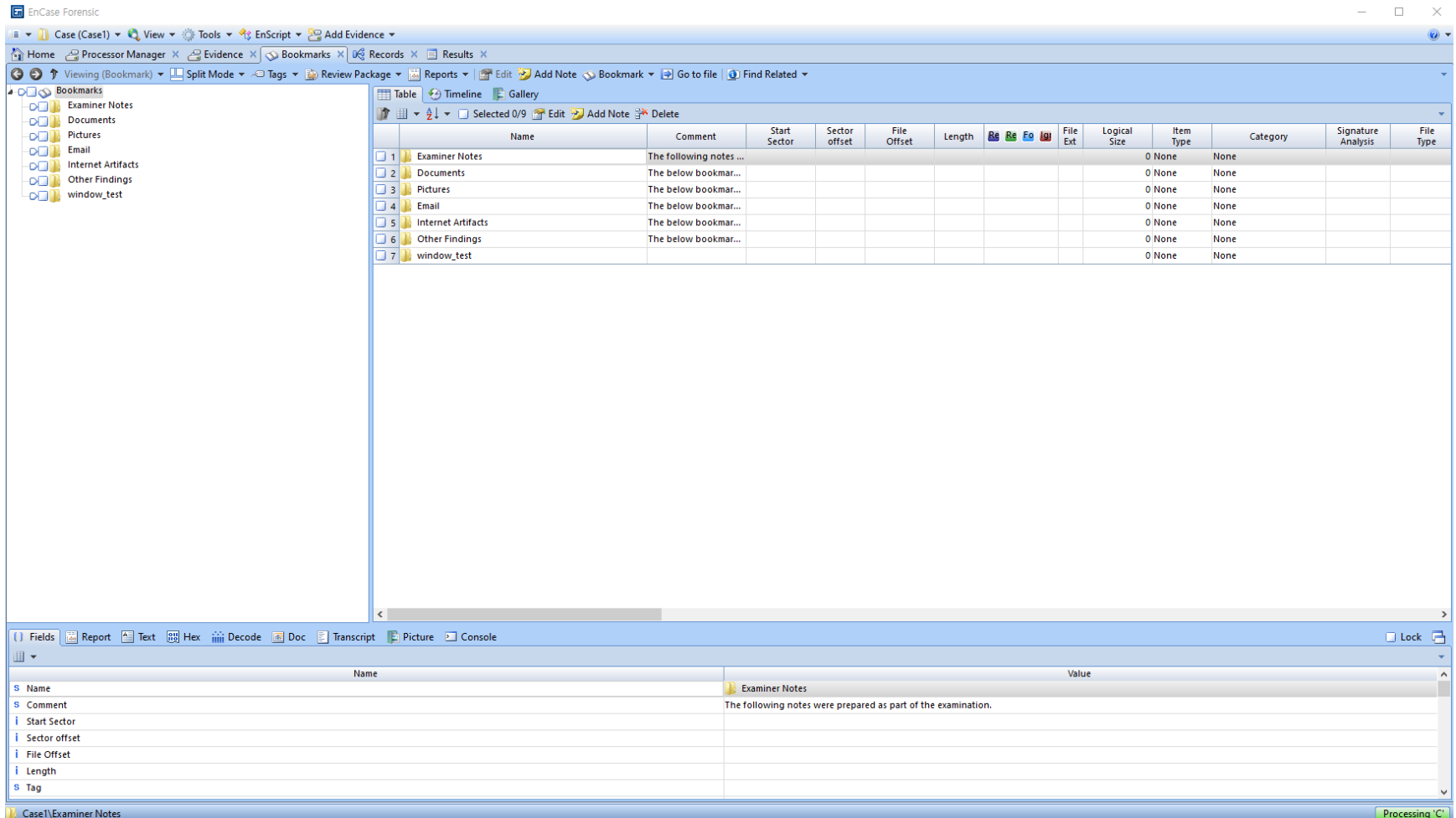
- 사진 파일 필터링 결과



3. Encase 기능 소개

■ Bookmark

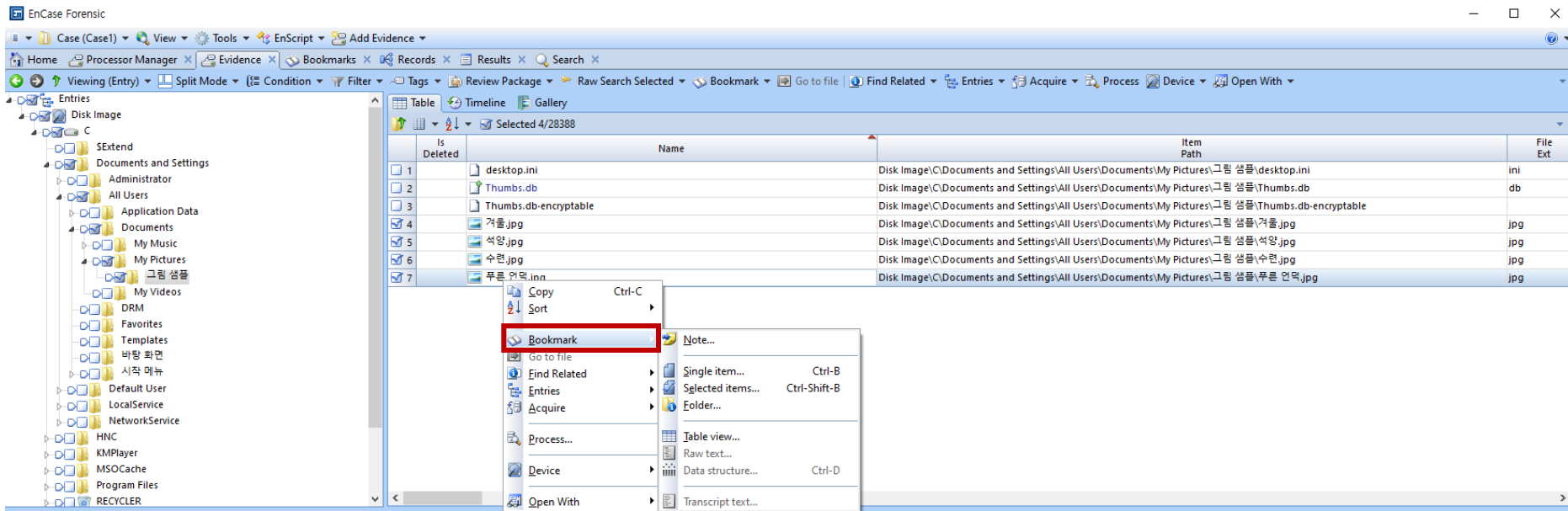
- 데이터를 분석하다가 나중에도 다시 봐야 할 데이터를 표시해두는 기능



3. Encase 기능 소개

■ Bookmark

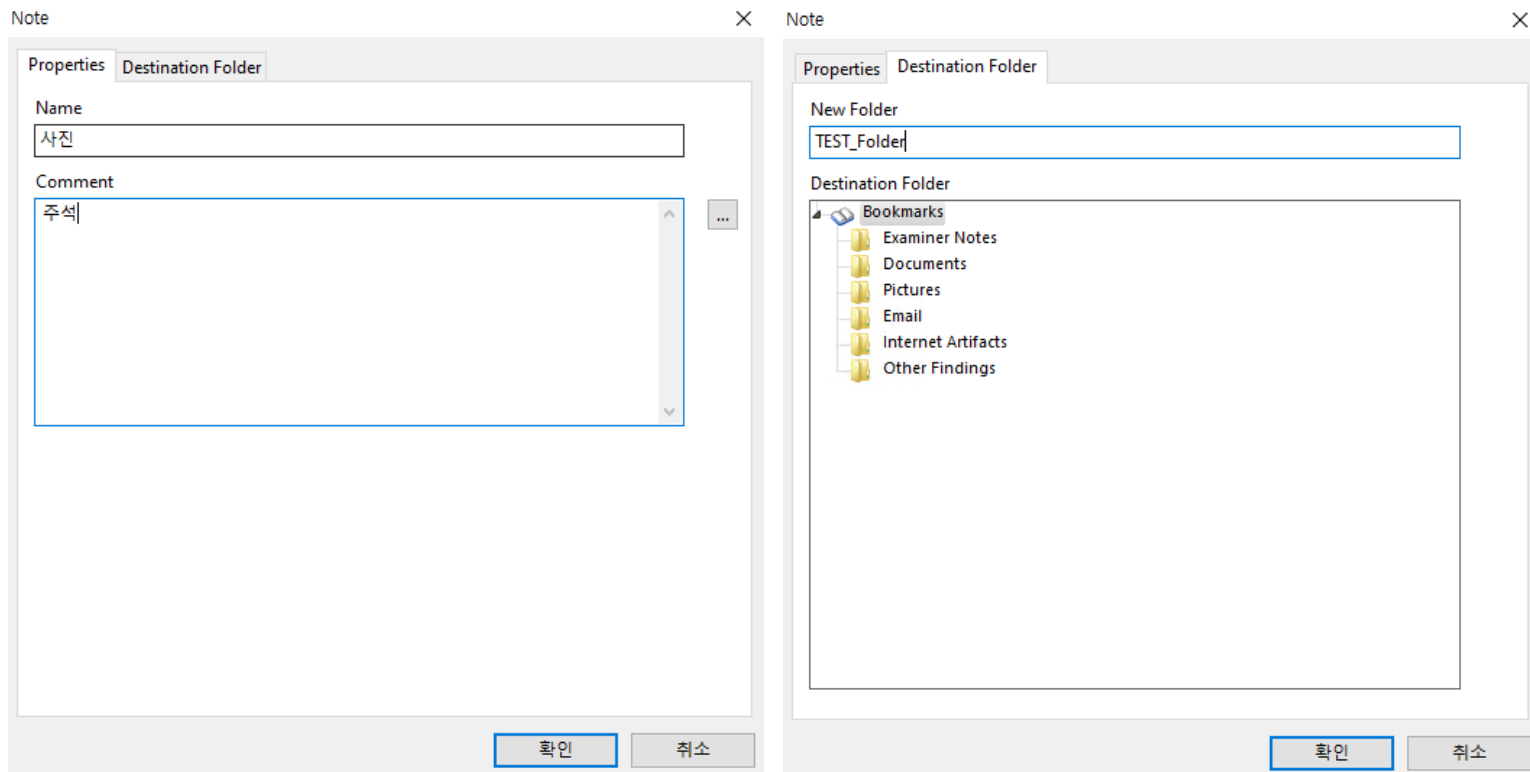
- 원하는 파일 체크 후 마우스 오른쪽 클릭



3. Encase 기능 소개

▪ Bookmark

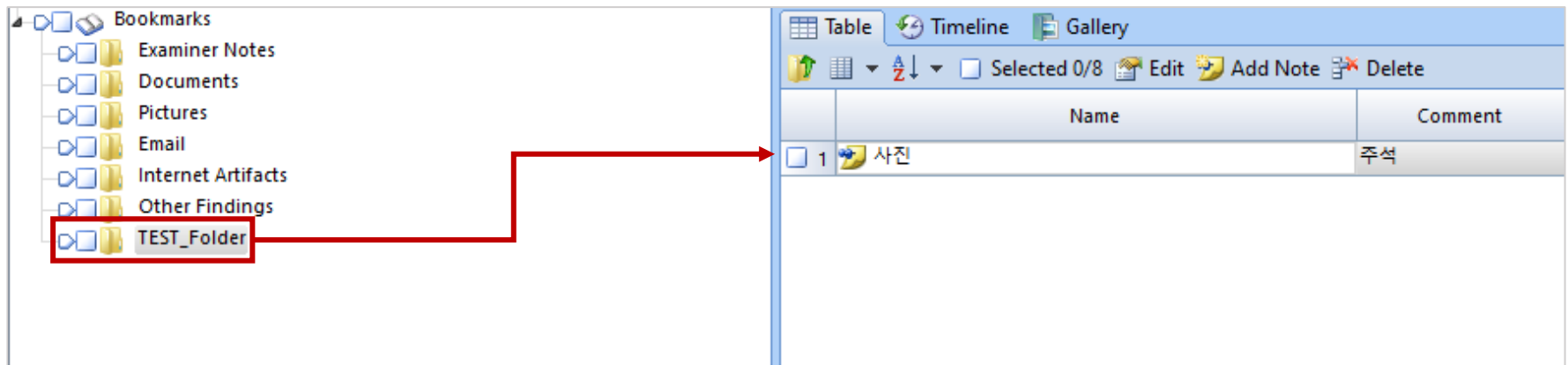
- 원하는 파일 체크 후 마우스 오른쪽 클릭
 - Note: 주석 기능



3. Encase 기능 소개

▪ Bookmark

- 원하는 파일 체크 후 마우스 오른쪽 클릭
 - Note: 주석 기능

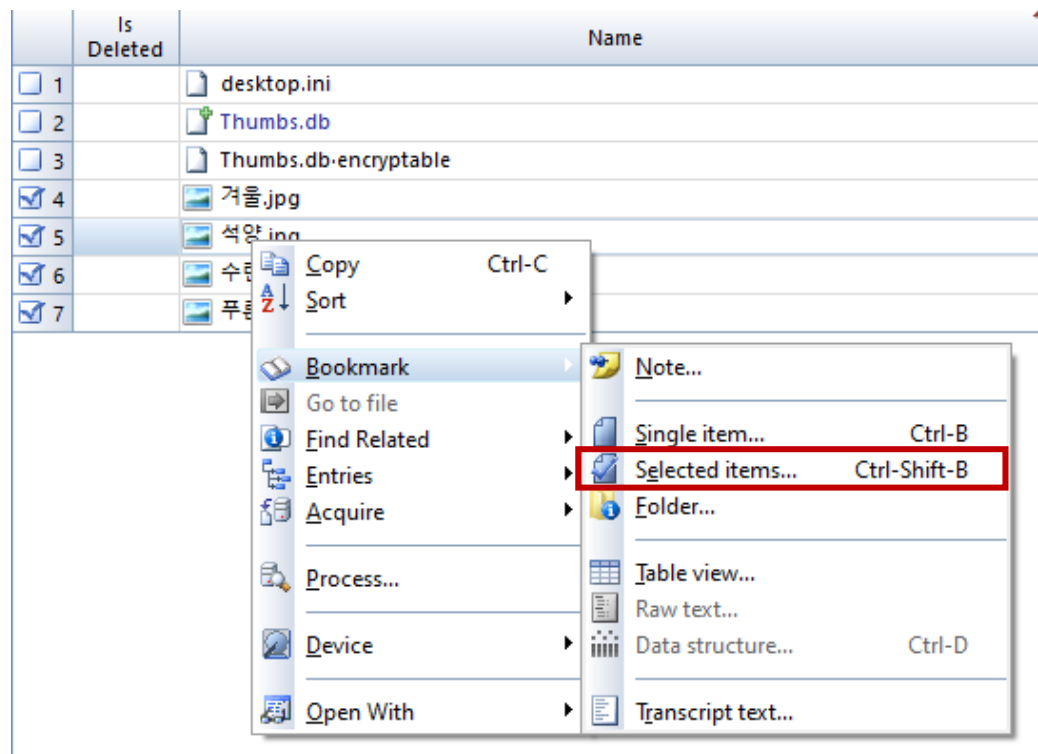


[결과]

3. Encase 기능 소개

▪ Bookmark

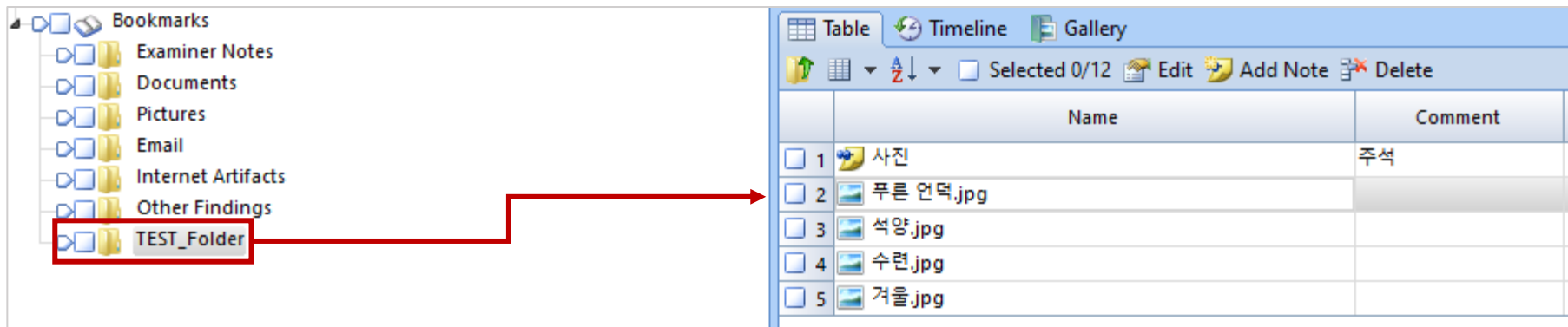
- 원하는 파일 체크 후 마우스 오른쪽 클릭
 - Selected items: 선택한 파일을 폴더에 추가하기



3. Encase 기능 소개

▪ Bookmark

- 원하는 파일 체크 후 마우스 오른쪽 클릭
 - Selected items: 선택한 파일을 폴더에 추가하기

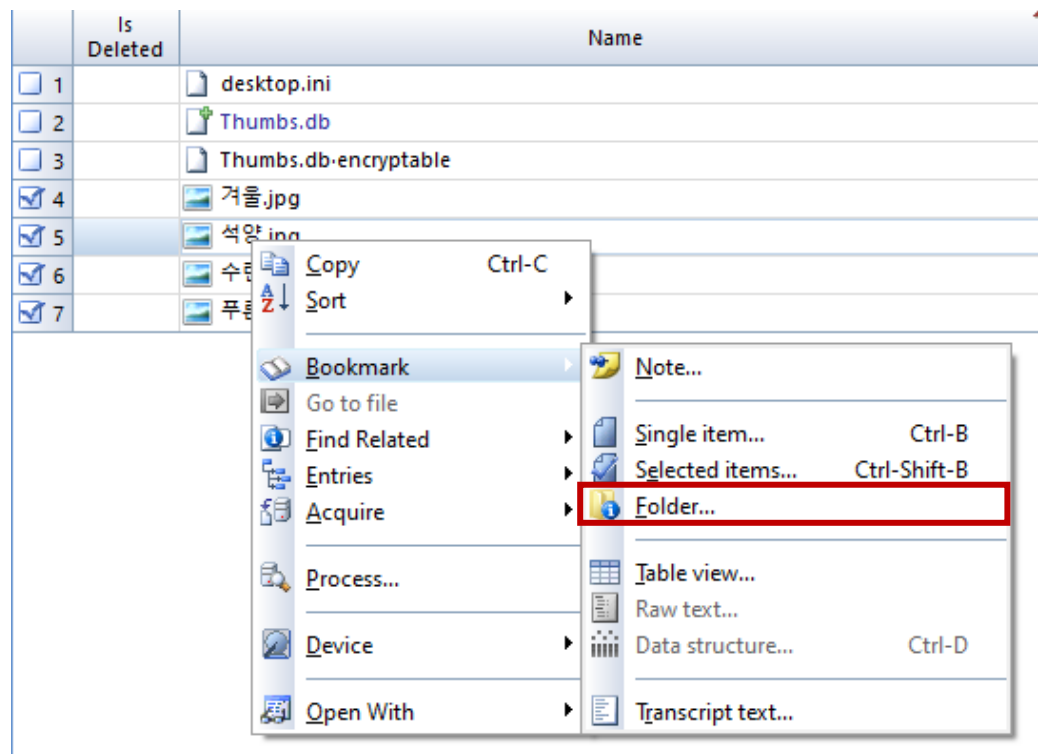


[결과]

3. Encase 기능 소개

▪ Bookmark

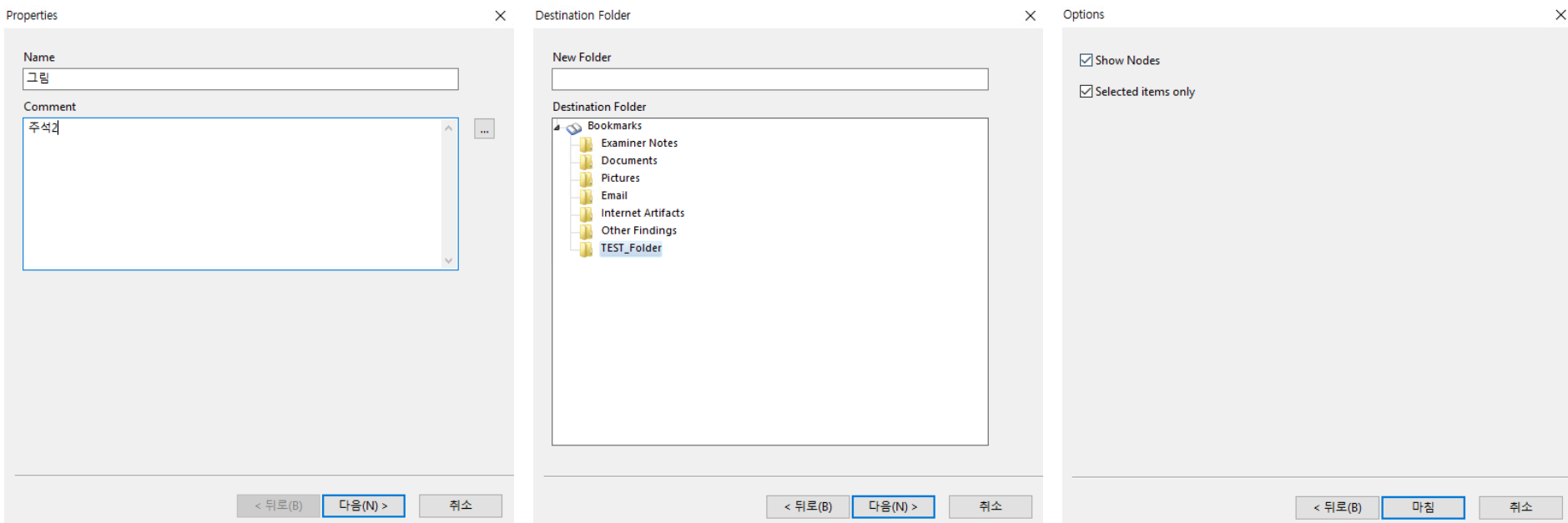
- 원하는 파일 체크 후 마우스 오른쪽 클릭
 - Folder: 선택한 파일을 폴더로 묶어서 추가



3. Encase 기능 소개

▪ Bookmark

- 원하는 파일 체크 후 마우스 오른쪽 클릭
 - Folder: 선택한 파일을 폴더로 묶어서 추가

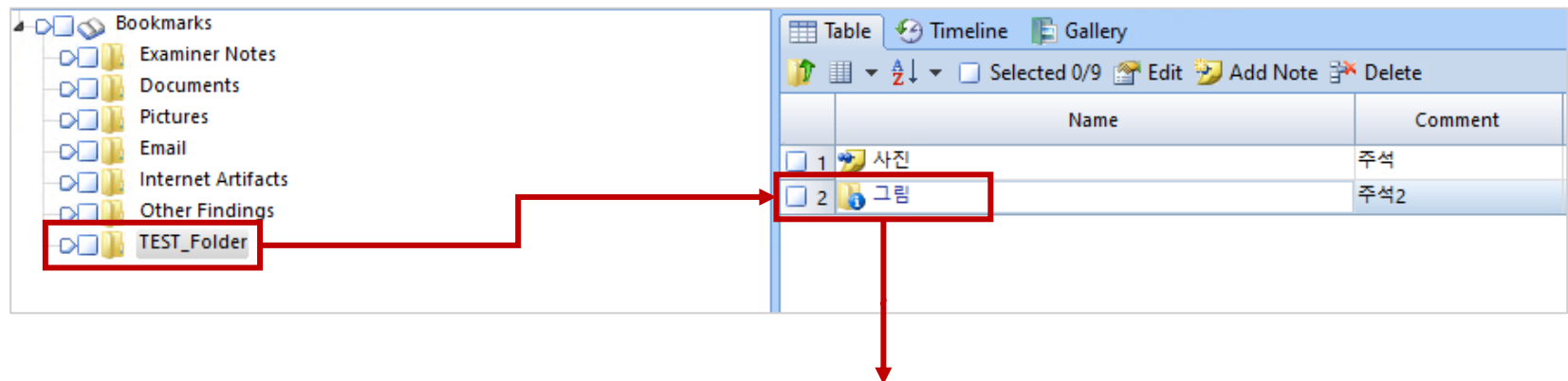


⇒ 폴더명 및 주석, 위치, 옵션 선택 가능

3. Encase 기능 소개

▪ Bookmark

- 원하는 파일 체크 후 마우스 오른쪽 클릭
 - Folder: 선택한 파일을 폴더로 묶어서 추가

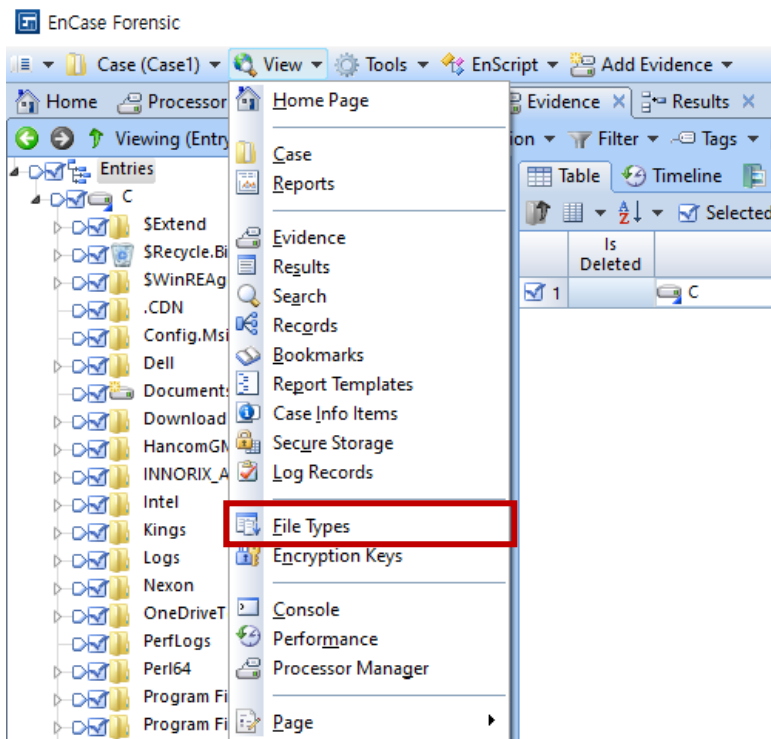


[결과]

3. Encase 기능 소개

■ 증거분석 - 파일 시그니처 분석

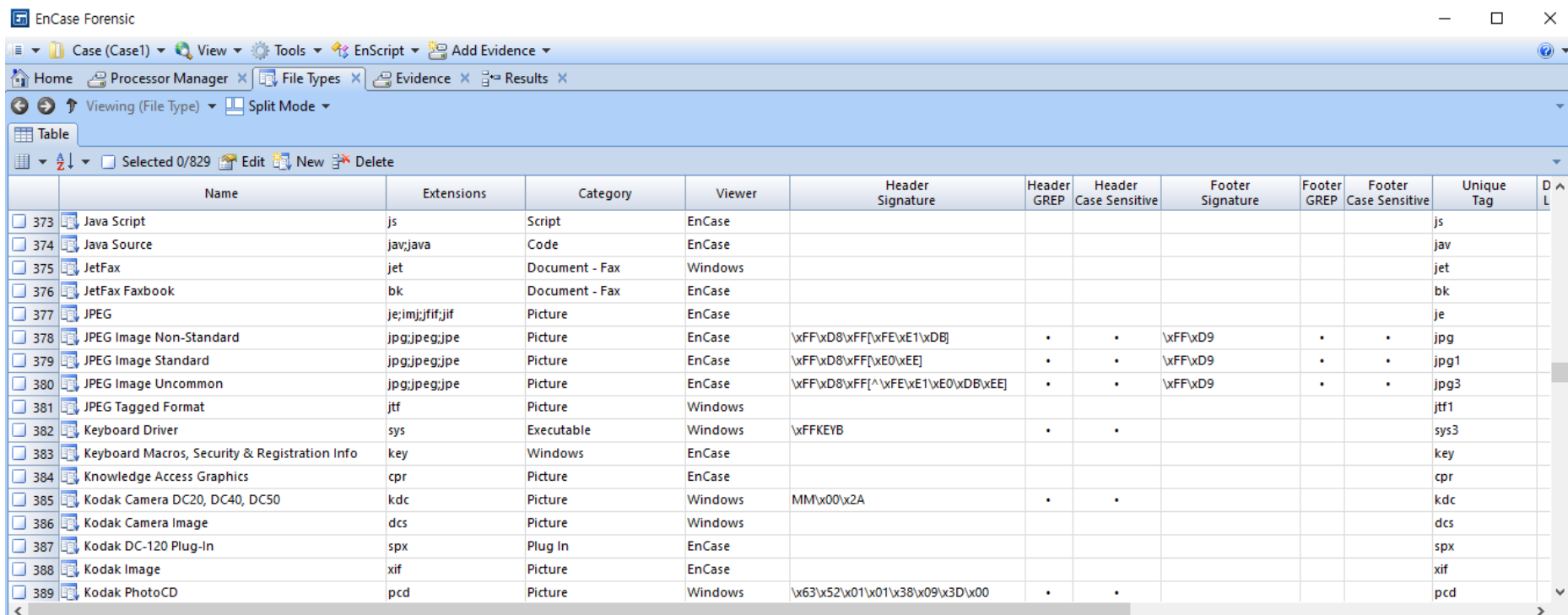
- Encase는 헤더가 존재하면 파일 헤더를 확장자와 비교
- 이 정보는 Encase의 FileTypes.ini 파일에 저장되어 있는 파일 시그니처와 확장자의 데이터베이스와 비교
- View 탭에서 File Types 메뉴로 이동



3. Encase 기능 소개

■ 증거분석 - 파일 시그니처 분석

- File Types는 파일 확장자, 카테고리, 이름와 푸터 및 메타데이터로 구성된 테이블(데이터베이스)

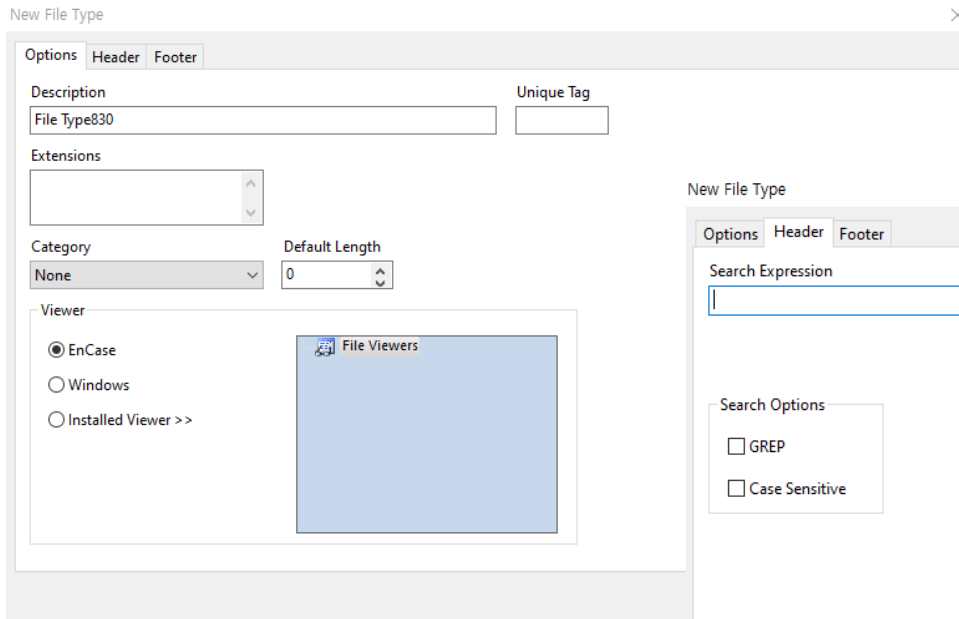


The screenshot shows the EnCase Forensic interface with the 'File Types' table open. The table lists various file types with their extensions, categories, viewers, and signatures. The table is sorted by Name.

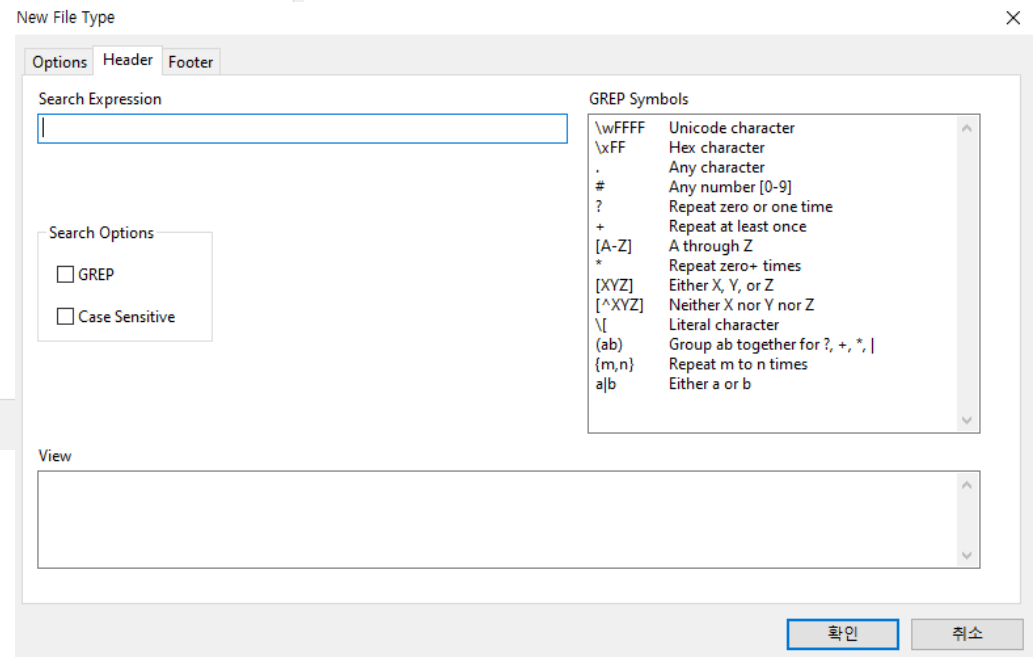
	Name	Extensions	Category	Viewer	Header Signature	Header GREP	Header Case Sensitive	Footer Signature	Footer GREP	Footer Case Sensitive	Unique Tag	D L
373	Java Script	js	Script	EnCase							js	
374	Java Source	jav;java	Code	EnCase							jav	
375	JetFax	jet	Document - Fax	Windows							jet	
376	JetFax Faxbook	bk	Document - Fax	EnCase							bk	
377	JPEG	je;imj;jfif;jif	Picture	EnCase							je	
378	JPEG Image Non-Standard	jpg;jpeg;jpe	Picture	EnCase	\xFF\xD8\xFF[\xFE\xE1\xDB]	•	•	\xFF\xD9	•	•	jpg	
379	JPEG Image Standard	jpg;jpeg;jpe	Picture	EnCase	\xFF\xD8\xFF[\xE0\xEE]	•	•	\xFF\xD9	•	•	jpg1	
380	JPEG Image Uncommon	jpg;jpeg;jpe	Picture	EnCase	\xFF\xD8\xFF[^\xFE\xE1\xE0\xDB\xEE]	•	•	\xFF\xD9	•	•	jpg3	
381	JPEG Tagged Format	jtf	Picture	Windows							jtf1	
382	Keyboard Driver	sys	Executable	Windows	\xFFKEYB	•	•				sys3	
383	Keyboard Macros, Security & Registration Info	key	Windows	EnCase							key	
384	Knowledge Access Graphics	cpr	Picture	EnCase							cpr	
385	Kodak Camera DC20, DC40, DC50	kdc	Picture	Windows	MM\x00\x2A	•	•				kdc	
386	Kodak Camera Image	dcs	Picture	Windows							dcs	
387	Kodak DC-120 Plug-In	spx	Plug In	EnCase							spx	
388	Kodak Image	xif	Picture	EnCase							xif	
389	Kodak PhotoCD	pcd	Picture	Windows	\x63\x52\x01\x01\x38\x09\x3D\x00	•	•				pcd	

3. Encase 기능 소개

- 증거분석 - 파일 시그니처 분석
 - 새로운 파일 유형을 추가하기 위해선 New 탭 클릭



[확장자 및 카테고리 입력]



[헤더 및 푸터 시그니처 입력]

3. Encase 기능 소개

- 증거분석 - 파일 시그니처 분석

- 파일 시그니처 분석은 Encase 실행 시 항상 실행(디폴트 옵션)
- 파일 시그니처 분석이 실행되는 동안 Encase는 증거 처리를 위해 선택한 장치에 있는 모든 파일을 조사하고 파일의 헤더가 데이터베이스에 있는 헤더와 일치하는지 확인
 - 데이터베이스에 있다면 헤더의 확장자와 비교하여 일치할 경우 **Match**
 - 파일 시그니처 데이터베이스에서 파일 헤더를 찾기 못하고 또한 데이터베이스에서 파일의 확장자도 찾을 수 없다면 **Unknown**

3. Encase 기능 소개

- 증거분석 - 파일 시그니처 분석
 - 결과

	Name	Re	Re	Re	Re	File Ext	Logical Size	Category	Signature Analysis	File Type
7	논문작성						4,096	Folder		
8	대학입학관련자료						4,096	Folder		
9	리제싱						4,096	Folder		
10	인강 시론 1 vol2					vol2	8,192	Folder		
11	강심량파일						8,192	Folder		
12	정보보호프로젝트						4,096	Folder		
13	포렌식						4,096	Folder		
14	12049596_10201425773443189_71114206570233628...					jpg	116,808	Picture		
15	12049596_10201425773443189_71114206570233628...					Ide...	26	None		
16	WPCaInker.lnk					Ink	1,651	Windows		
17	디펜스로그노리거.txt					txt	77	Document		
18	AccessData FTK Imager.lnk					Ink	1,946	Windows		
19	IL6.pptx					pptx	2,565,487	Document - Presentation		
20	desktop.ini					ini	282	Windows		
21	desktop.ini\$F\$P_DATA						56	Unknown		
22	커리큘럼.lnk					Ink	1,129	Windows		
23	현장용 디지털증거 분석도구(오전)패용.zip					zip	13,189,626	Archive		
24	현장용 디지털증거 분석도구(오전)패용.zip.1...					Ide...	26	None		
25	Chrome.lnk					Ink	2,233	Windows		
26	Encase7.10.06.lnk					Ink	950	Windows		
27	12114472_910959385281577_7912177137878370803...					jpg	74,224	Picture		

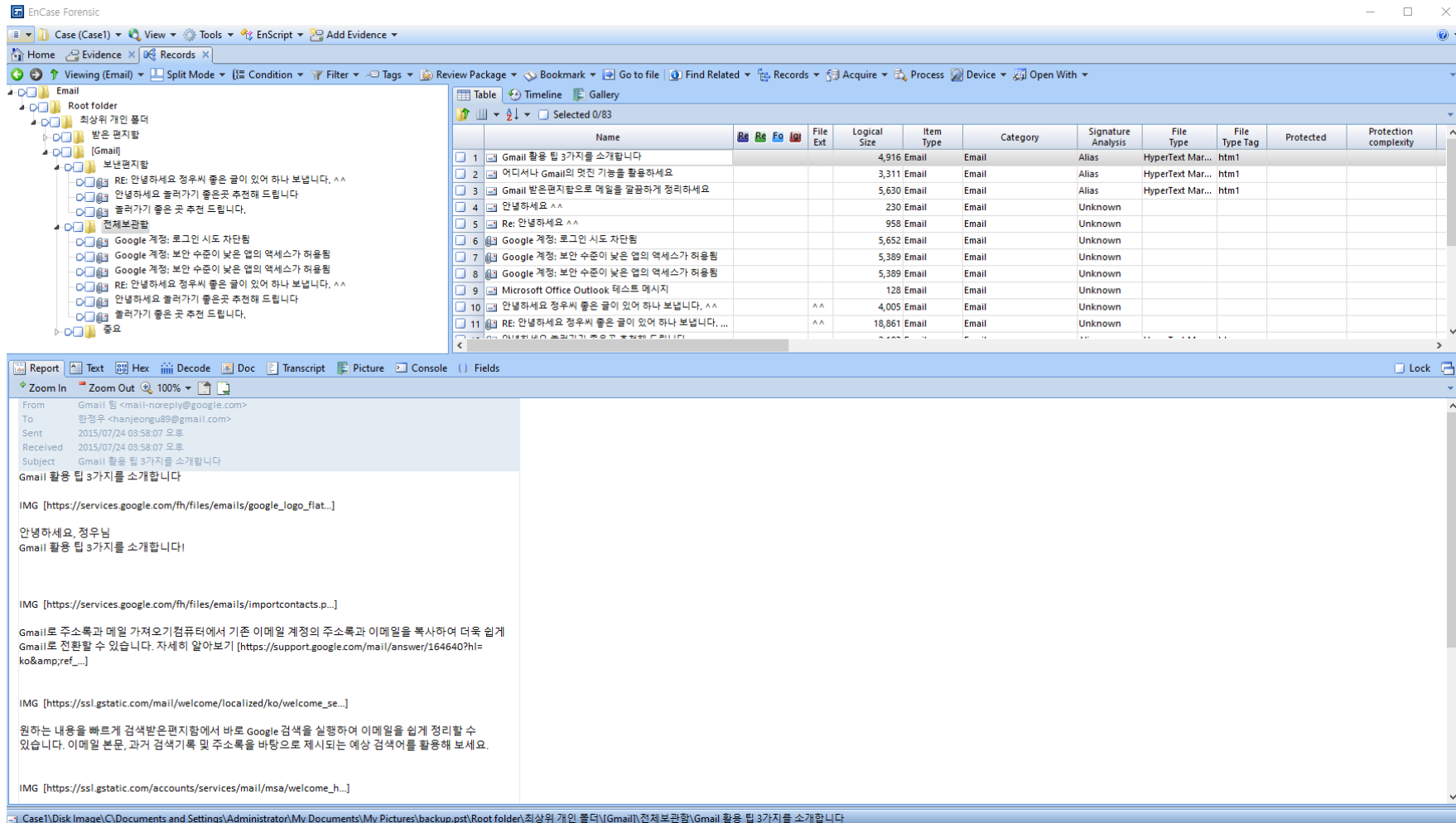
Category	Signature Analysis	File Type
Folder	Unknown	
Folder	Unknown	
Folder	Unknown	
Folder	Unknown	
Folder	Unknown	
Folder		
Folder		
Picture	Match	JPEG Image Un...
None	Unknown	
Windows	Match	Windows File ...
Document	Match	Text
Windows	Match	Windows File ...
Document - Presentation	Match	Microsoft Pow...
Windows	Alias	Registry Data
Unknown	Unknown	
Windows	Match	Windows File ...
Archive	Match	ZIP Compressed
None	Unknown	
Windows	Match	Windows File ...
Windows	Match	Windows File ...
Picture	Match	IDEC Image Sta



3. Encase 기능 소개

■ 증거분석 - 이메일 분석

- 수/발신 이메일 목록 확인 가능



3. Encase 기능 소개

- 증거분석 - 이메일 분석
 - 메일 내용 확인 가능

From: Google <no-reply@accounts.google.com>
To: hanjeongu89@gmail.com <hanjeongu89@gmail.com>
Sent: 2015/07/27 04:09:10 오후
Received: 2015/07/27 04:09:19 오후
Subject: Google 계정: 로그인 시도 차단됨

IMG [cid:google]한정우 IMG [cid:profilephoto]

정우님, 안녕하세요. 최근 Google 계정 [hanjeongu89@gmail.com] 로그인 시도가 차단되었습니다. 로그인 시도 세부정보
날짜 및 시간: 7월 27일 월요일 오후 4:09 GMT+9 위치: 대한민국 서울특별시

본인이 아닌 경우
계정 활동기록 페이지(<https://security.google.com/settings/security/activity>)를 검토하여 의심스러운 활동이 있는지 살펴보세요. 내 계정에 로그인을 시도한 사람은 내 비밀번호를 알고 있는 것이므로 즉시 비밀번호를 변경하시기 바랍니다.

본인인 경우
계정에 액세스할 때 Gmail과 같이 Google에서 만든 앱으로 전환하거나(권장), <https://www.google.com/settings/security/lesssecureapps>에서 계정에 더 이상 최신 보안 표준이 적용되지 않도록 설정을 변경할 수 있습니다.

자세한 내용은 <https://support.google.com/accounts/answer/6010255> 페이지를 참조하세요. 감사합니다. Google 계정 팀

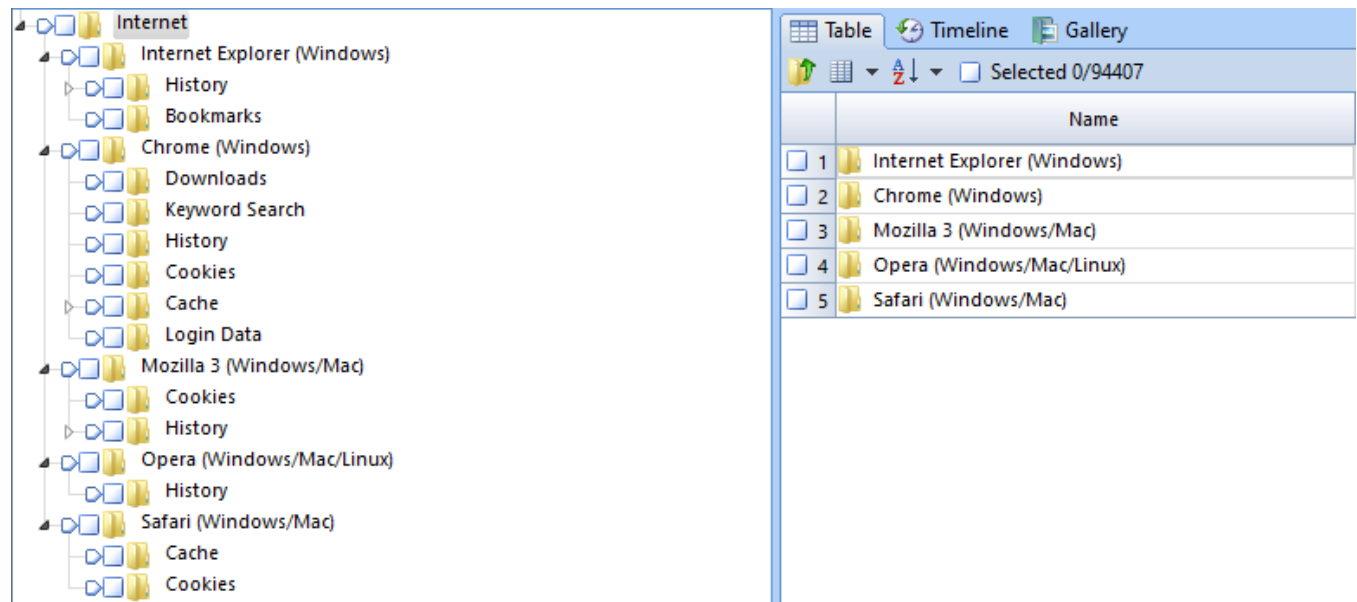
이 이메일은 발신 전용입니다. 자세히 알아보려면 Google 계정 도움말 센터(<https://support.google.com/accounts/answer/6010255>)를 참조하세요.



- From: 보낸 사람
- To: 받는 사람
- Subject: 메일 제목
- Sent: 보낸 날짜
- Received: 받은 날짜
- Attachment: 첨부 파일

3. Encase 기능 소개

- 증거 분석 - 인터넷 히스토리 기록 분석
 - 브라우저별 인터넷 히스토리 기록 확인 가능
 - Internet Explorer
 - Chrome
 - Mozilla
 - Opera
 - Safari



3. Encase 기능 소개

- 증거 분석 - 인터넷 히스토리 기록 분석
 - Cache

The screenshot displays the Encase Forensic interface. On the left, a tree view shows the file system structure, with 'Internet Explorer (Windows)' expanded and 'Cache' selected. The main pane shows a table of files in the cache, including various image and document files. A preview of a selected image (msn logo) is shown at the bottom.

Name	File Ext	Logical Size	Item Type	Category	Signature Analysis	File Type	File Type Tag	Protected	Protection complexity	Last Access
AAdmm0[1].jpg	jpg	2,826 Document	Picture	Match	JPEG Image Sta...	jpg1				
AAdmo2[1].jpg	jpg	6,029 Document	Picture	Match	JPEG Image Sta...	jpg1				
AAGuXm[1].png	png	533 Document	Picture	Match	Portable Netw...	png				
AAdmX8[1].jpg	jpg	2,345 Document	Picture	Match	JPEG Image Sta...	jpg1				
AAdmH1[1].jpg	jpg	2,388 Document	Picture	Match	JPEG Image Sta...	jpg1				
AAdmzuy[1].jpg	jpg	8,306 Document	Picture	Match	JPEG Image Sta...	jpg1				
AAdHq[1].jpg	jpg	2,332 Document	Picture	Match	JPEG Image Sta...	jpg1				
AAdm7k[1].jpg	jpg	1,934 Document	Picture	Match	JPEG Image Sta...	jpg1				
AAdmE8[1].jpg	jpg	2,673 Document	Picture	Match	JPEG Image Sta...	jpg1				
AAdmz7m[1].jpg	jpg	2,372 Document	Picture	Match	JPEG Image Sta...	jpg1				
AAdmz7m[1].jpg	jpg	2,397 Document	Picture	Match	JPEG Image Sta...	jpg1				
AAdmz7m[1].jpg	jpg	2,207 Document	Picture	Match	JPEG Image Sta...	jpg1				
4f1880[1].ico	ico	4,286 Document	Picture	Match	Windows icon	ico				
fed248130748b0e5dca0641f4bbaeed3[1].jpg	jpg	26,923 Document	Picture	Match	JPEG Image No...	jpg				
AAdmP8[1].jpg	jpg	6,773 Document	Picture	Match	JPEG Image Sta...	jpg1				
AAdmz7m[1].jpg	jpg	2,656 Document	Picture	Match	JPEG Image Sta...	jpg1				
AAdmz7m[1].jpg	jpg	2,698 Document	Picture	Match	JPEG Image Sta...	jpg1				
AAdmz7m[1].jpg	jpg	2,535 Document	Picture	Match	JPEG Image Sta...	jpg1				
B854j52[1].png	png	777 Document	Picture	Match	Portable Netw...	png				

3. Encase 기능 소개

- 증거 분석 - 인터넷 히스토리 기록 분석

Cache	웹 사이트 접속 시, 방문 사이트로부터 데이터를 자동으로 다운 받는 것 이미지 파일, 텍스트파일, 아이콘, HTML 파일 등
History	사용자가 방문한 웹사이트의 접속 정보
Cookie	웹사이트에 의해 컴퓨터 시스템에 저장된 데이터
Download	사용자가 의도적으로 선택해서 자신의 컴퓨터로 다운받은 파일에 대한 정보

Thank you
