EnCase 개요 및 기능 소개

손 태 식

Introduction : Guidance software

Guidance Software, Inc.

- was a public company (NASDAQ: GUID**) founded in 1997**. Headquartered in Pasadena, Calif. the company developed and provided **software solutions for digital investigations** primarily in the United States, Europe, the Middle East, Africa, and the Asia/Pacific Rim. Guidance Software had offices in **Brazil, Chicago, Houston, New York City, San Francisco, Singapore, United Kingdom and Washington, D.C**. and employed approximately 371 employees. On September 14 2017 the company was acquired by "**OpenText"**
- **Best known for its EnCase digital investigations software**, Guidance Software's product line was organized around four markets: digital forensics, endpoint security analytics, cyber security incident response, and e-discovery. The company served law-enforcement and government agencies, as well as corporations in various industries, such as financial and insurance services, technology, defense contracting, telecom, pharmaceutical, healthcare, manufacturing, and retail. The company operated through four business segments: products, professional services, training and maintenance, and operates two certification programs for the EnCase® Certified Examiner (EnCE®) and EnCase® Certified eDiscovery Practitioner (EnCEP®) designations.

Introduction : Encase

EnCase : Tool for Computer Forensic Investigation & Analysis

- **Guidance** created the category for digital investigation software with EnCase Forensic in 1998. EnCase has maintained its reputation as the gold standard in criminal investigations and was named the Best Computer Forensic Solution for seven consecutive years by SC Magazine. No other solution offers the same level of functionality, flexibility, and has the track record of court-acceptance as EnCase Forensic. With EnCase offering mobile forensics, investigators have the flexibility and convenience they need to complete their investigations quickly and efficiently.
- **EnCase Forensic** is recognized globally as the Gold Standard for digital forensics and is the only court-proven solution built for deep-level digital forensic investigation, powerful processing, and integrated investigation workflows with flexible reporting options. It is built with a deep understanding of the digital investigation lifecycle and the importance of maintaining evidence integrity. With its new user interface and streamlined workflows, EnCase Forensic empowers any examiner to seamlessly complete any investigation, even those involving mobile devices.

Introduction : Encase

EnCase : Tool for Computer Forensic Investigation & Analysis

Reliable Acquisition of Evidence

With EnCase Forensic, examiners can be confident that the integrity of the evidence will not be compromised. All evidence captured with EnCase Forensic is stored in the court accepted EnCase evidence file formats.

Deep Forensic Analysis

EnCase Forensic is known for its ability to uncover evidence that may go unnoticed if analyzed with other solutions. As the Gold Standard in digital forensics, EnCase has been used in over 100 court cases.

Mobile Collection

NEW! With over 26,000 mobile device profiles supported, EnCase Forensic supports the latest smartphones and tablets, all while empowering the examiner to conduct logical and physical acquisitions. From new investigator to the seasoned examiner, each level of user can find the evidence they need with mobile acquisitions in EnCase Forensic.

Broad OS/Decryption Support

Offering the broadest support of operating and file systems, artifacts, and encryption types, EnCase Forensic enables the investigator to provide conclusive results with a detailed analysis of findings.

Swift Evidence Processing

Powered by an indexing engine built for scale and performance, investigators can automate complex queries across their varied evidence sources in one step to reduce case backlogs and increase efficiency.

Easy Reporting

A completed case is only as good as its final report. Using customizable templates with EnCase Forensic, examiners can create compelling, easy to read, professional reports that can be shared for every case.

Extensibility

EnCase Forensic offers extensibility through EnScripts. EnScripts are automated code commands that streamline tasks and can be created by developers through AppCentral. This is helpful as EnScripts extend the capabilities of EnCase Forensic to help the examiners complete investigations more efficiently.

Workflow Automation

Saving time is critical during an investigation. With investigation workflows and default conditions, examiners can easily navigate through EnCase Forensic to enhance the way they uncover evidence.

GUIDANCE SOFTWARE is now opentext™

Introduction : Encase

Enhanced Indexing Engine

The EnCase Enhanced Indexing Engine provides powerful processing speeds, improved language support, and advanced keyword searching so that the time it takes investigators to complete their analysis drastically decreases, resulting in less time spent on cases and lower costs.

Mobile Acquisitions

The moment you've been waiting for. EnCase Forensic 8 now features mobile acquisition capabilities, supporting ALL smartphone operating systems, and over 26,000+ device profiles. You can now logically or physically acquire data such as text messages, pictures,app data, deleted data and much more to gather the critical evidence you need for your case.

In today's world, you need a tool that can collect from any device, and EnCase Forensic is here to help.

Investigation Workflows

With new investigation workflows, known as Pathways, built into Forensic 8 examiners of any skill, from experts to the most junior member of the team, can complete the most common tasks associated with a triage or comprehensive investigation. With a few clicks an examiner can take a case from adding and processing evidence through creating a report of their findings. The most important part of the investigation remains the examiners ability to uncover evidence using their expertise, however with Pathways, examiners can rest assured that navigating EnCase Forensic will not slow down their progress.

NEW Add-On Solution

EnCase Mobile Investigator

Being able to review, bookmark, parse, and report on mobile evidence is critical in an investigation to uncover findings. Sold separately, EnCase Mobile Investigator allows investigators to easily review EnCase Forensic 8 acquired evidence from all types of digital devices without having to process the evidence. When used with EnCase Forensic, you can save time and allow case agents, attorneys, or other third parties to easily review data.

ADDITIONAL ENHANCEMENTS INCLUDE:

- Integration with Project VIC
- RAW Image Support
- EnScript Launcher
- Bookmark as Image

GUIDANCE SOFTWARE is now opentext™

What's new in
EnCase® Forensic 8.06

Encase Certificate Introduction

국제 자격증

- **CFSR(Certified Forensics Security Responder)**
  - Cyber security professionals who want to advance their careers are making it a top priority to get certified with cutting-edge techniques in real-world, digital forensic applications. The Certified Forensic Security Responder(CFSR™) will equip you with the breadth and depth of knowledge that you need to become a highly sought-after cyber security forensics expert.
  - **Prerequisites:** Host Intrusion Methodology and Investigation + Incident Investigation Classroom / vClass or 12 Months of Qualified Work Experience
- **EnCE(The Encase Certified Examiner)**
  - The EnCase® Certified Examiner(EnCE®) program certifies both public and private sector professionals in the use of Guidance Software's EnCase computer forensic software. EnCE certification acknowledges that professionals have mastered computer investigation methodology as well as the use of EnCase software during complex computer examinations. Recognized by both the law enforcement and corporate communities as a symbol of in-depth computer forensics knowledge, EnCE certification illustrates that an investigator is a skilled computer examiner.
  - **Prerequisites:**
    64 hours of authorized Computer Forensic Training or 12 Months of Qualified Work Experience

Encase Certificate Introduction

국제 자격증

- **EnCEP(The Encase eDiscovery Practitioner)e eDiscovery training course**
  - The EnCase® Certified eDiscovery Practitioner(EnCEP®) program certifies private and public sector professionals in the use of Guidance Software's EnCase® eDiscovery software as well as their proficiency in e-discovery planning, project management, and best practices, spanning legal hold to load file creation. EnCase eDiscovery is the leading e-discovery solution for the search, collection, preservation, and processing of electronically stored information(ESI). Earning the EnCEP certification illustrates that a practitioner is skilled in the application of the solution to manage and successfully complete all sizes of e-discovery matters in accordance with the Federal Rules of Civil Procedure.
  - **Prerequisites:**
    EnCase eDiscovery v5 Classroom / vClass + 3 Months of Qualified Work Experience

국내 포렌식 자격증

국내 자격증

- **디지털 포렌식 전문가 1급(100점 만점 60점이상,연 1회)**
  - 필기 : 총 3과목 180분 디스크 포렌식, 증거법, 선택 1과목
    (DB 포렌식, 네트워크 포렌식, 모바일 포렌식 침해사고 대응 포렌식)
  - 실기 : 총 2과목 240분 디스크 포렌식, 선택 1과목
    (DB 포렌식, 네트워크 포렌식, 모바일 포렌식 침해사고 대응 포렌식)

자격명 : 디지털포렌식 전문가 1급
자격의 종류 : 민간자격
등록번호 : 2011-0185
자격발급기관 : (사)한국포렌식학회
검정(응시)료
필기시험 : 10만원
실기시험 : 25만원

기관명 : 한국포렌식학회
대표자 : 노명선
연락처 : 02-740-1809 (이메일 kforensic@gmail.com)
소재지 : 서울특별시 종로구 명륜3가 성균관대학교 법학관 304호
홈페이지 : forensickorea.org

국내 포렌식 자격증

국내 자격증

- **디지털 포렌식 전문가 2급(100점 만점 60점이상,연 2회)**
  - 필기 : 총 5과목 120분 디지털 포렌식 개론, 데이터베이스, 응용 프로그램과 네트워크의 이해, 파일시스템과 운영체제, 컴퓨터구조와 디지털저장매체
  - 실기: 총 1과목 240분 디지털 포렌식 기초 실무

자격명 : 디지털포렌식 전문가 2급
자격의 종류 : 국가공인 민간자격
등록번호 : 2011-0185
자격발급기관 : (사)한국포렌식학회/한국인터넷진흥원
검정(응시)료
필기시험 : 6만원
실기시험 : 15만원

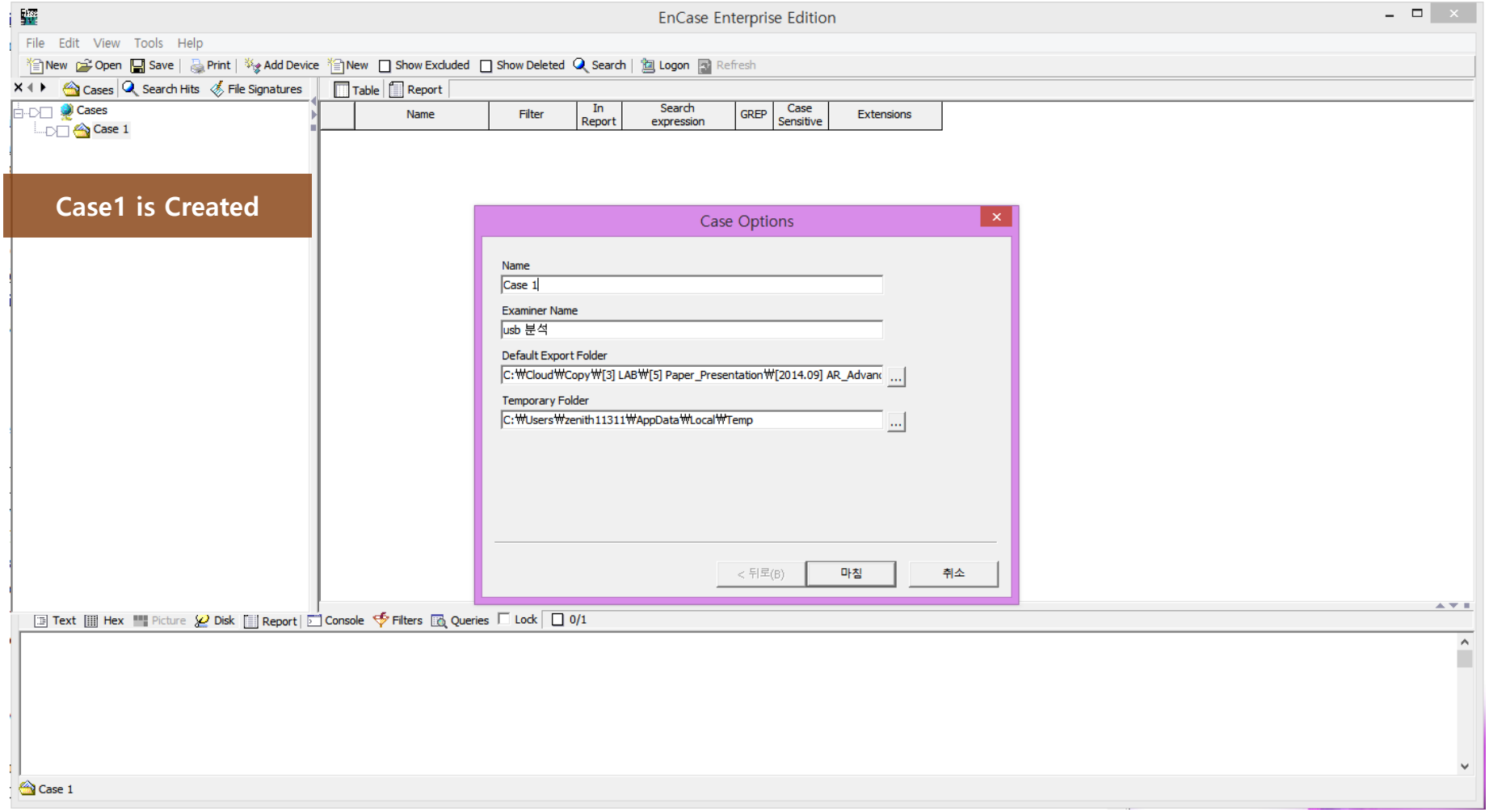
Enfuse : conference

Enfuse®

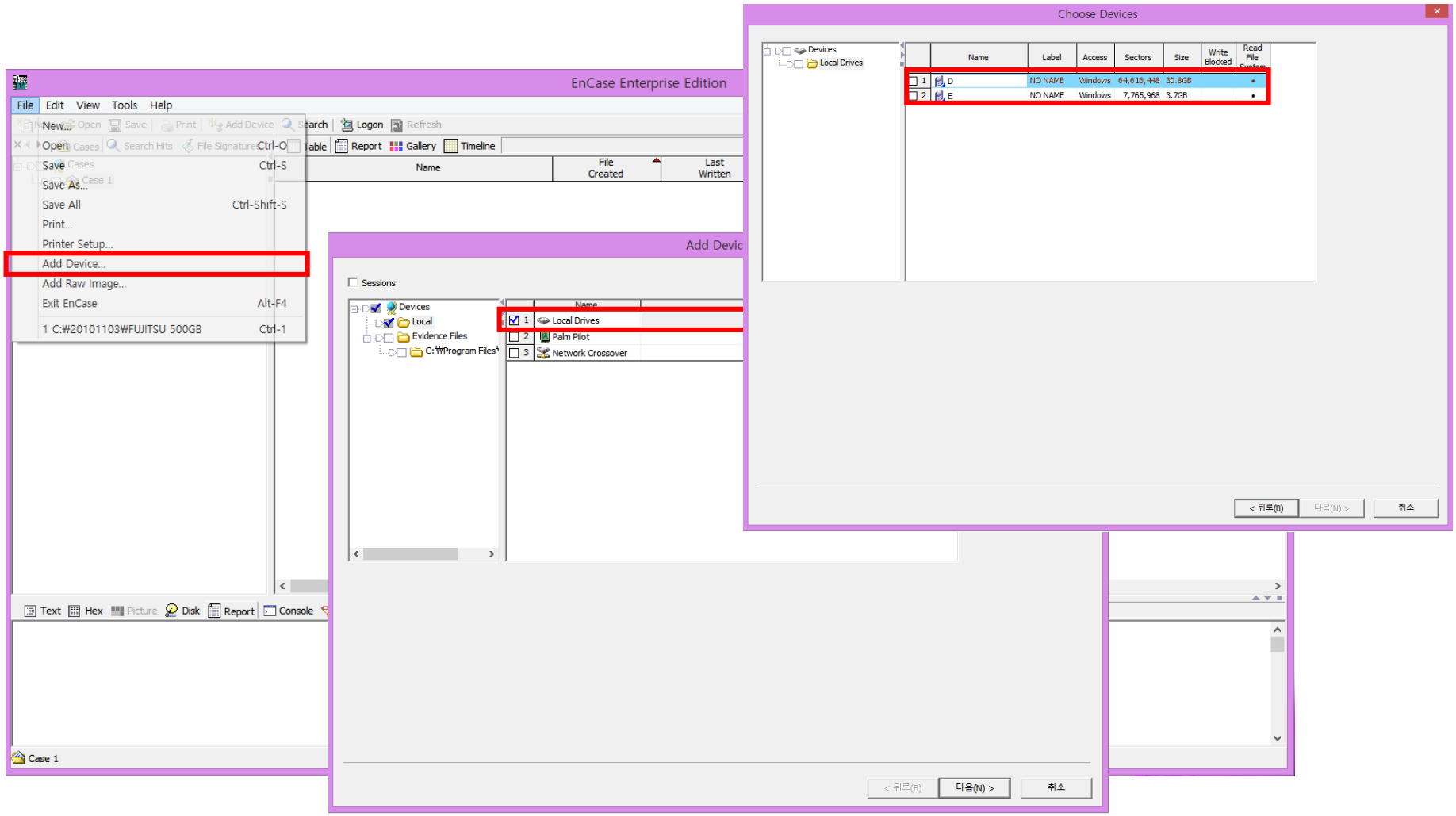
- is a three-day security, digital investigations, and eDiscovery conference where specialists, executives, and experts break new ground for the year ahead. It's a global event. It's a community. It's where problems get solved. Attend Enfuse to take your work.
- Enfuse 2018, May 21-24, Las Vegas
- Topics
  - Endpoint Detection, Threat Hunting, Incident Response, Data & Risk, Compliance, Forensic Investigations, eDiscovery, Content Analysis, EnCase Products, Integrations, Artificial Intelligence, Mobile, Regulatory, Industrial Control Systems, Point of Sale, Enscripts, Digital Crime, IoT, Biometrics, GDPR

Digital Forensics Using EnCase

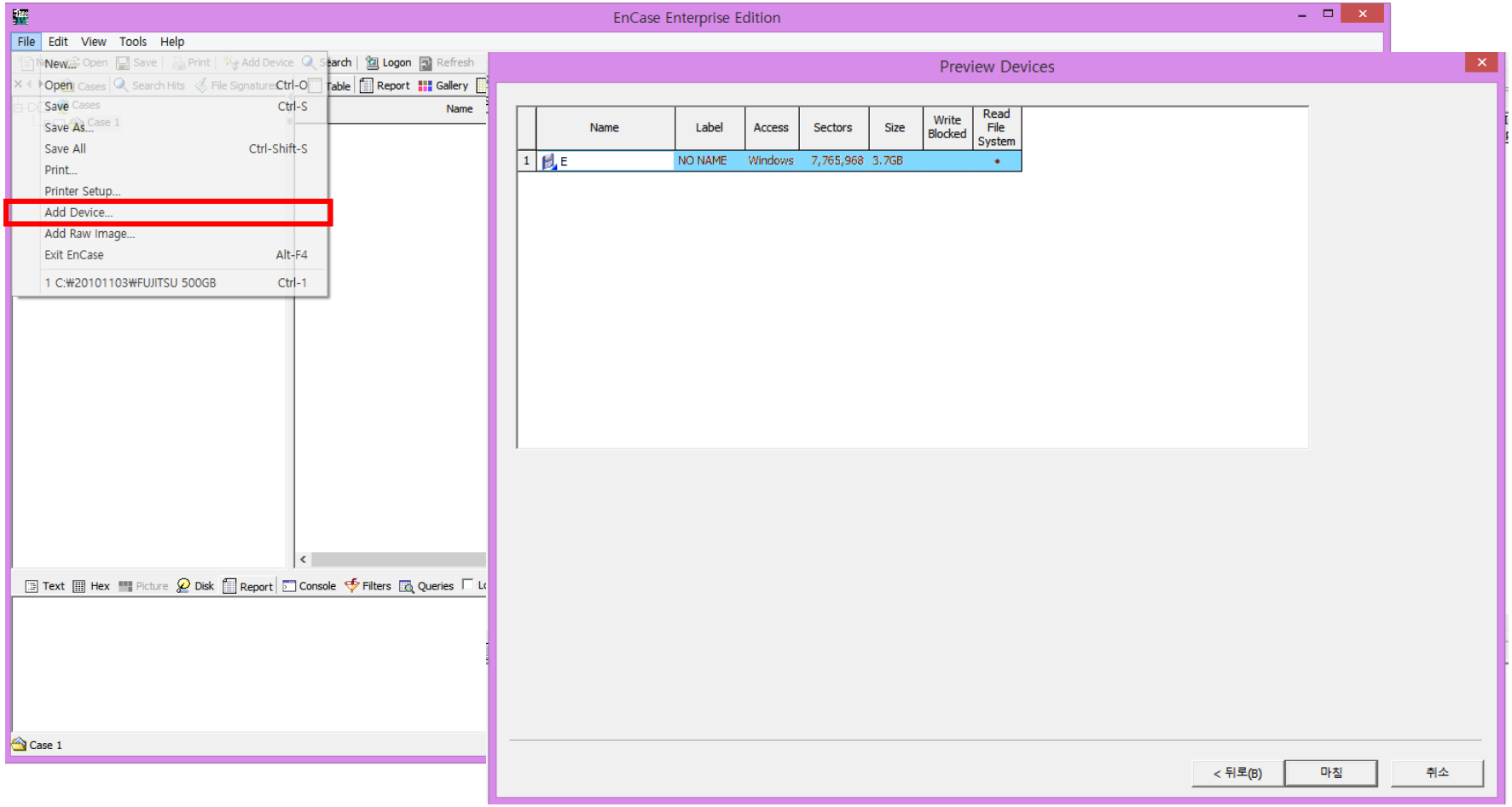
Encase – Creating case



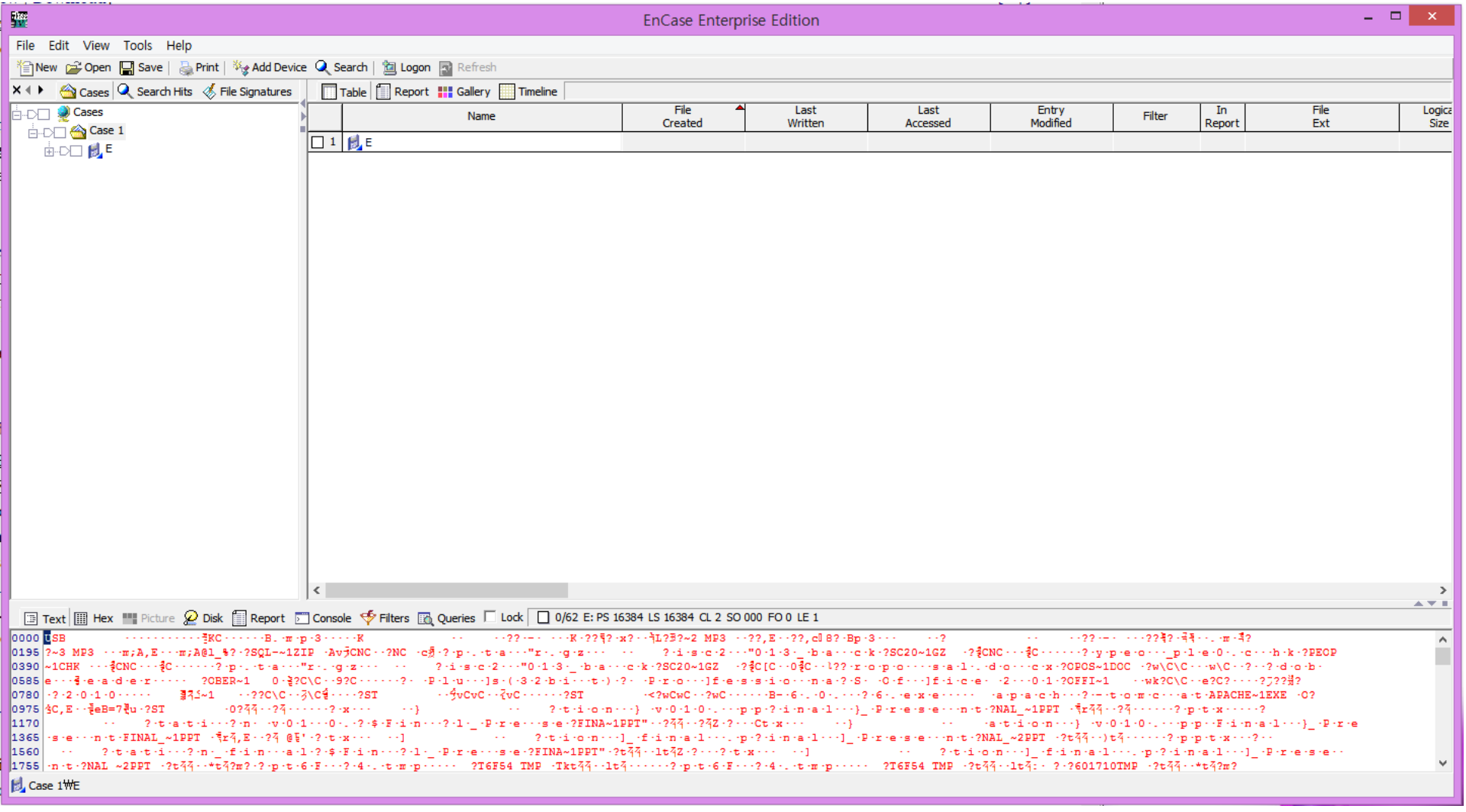
Encase – Adding local device



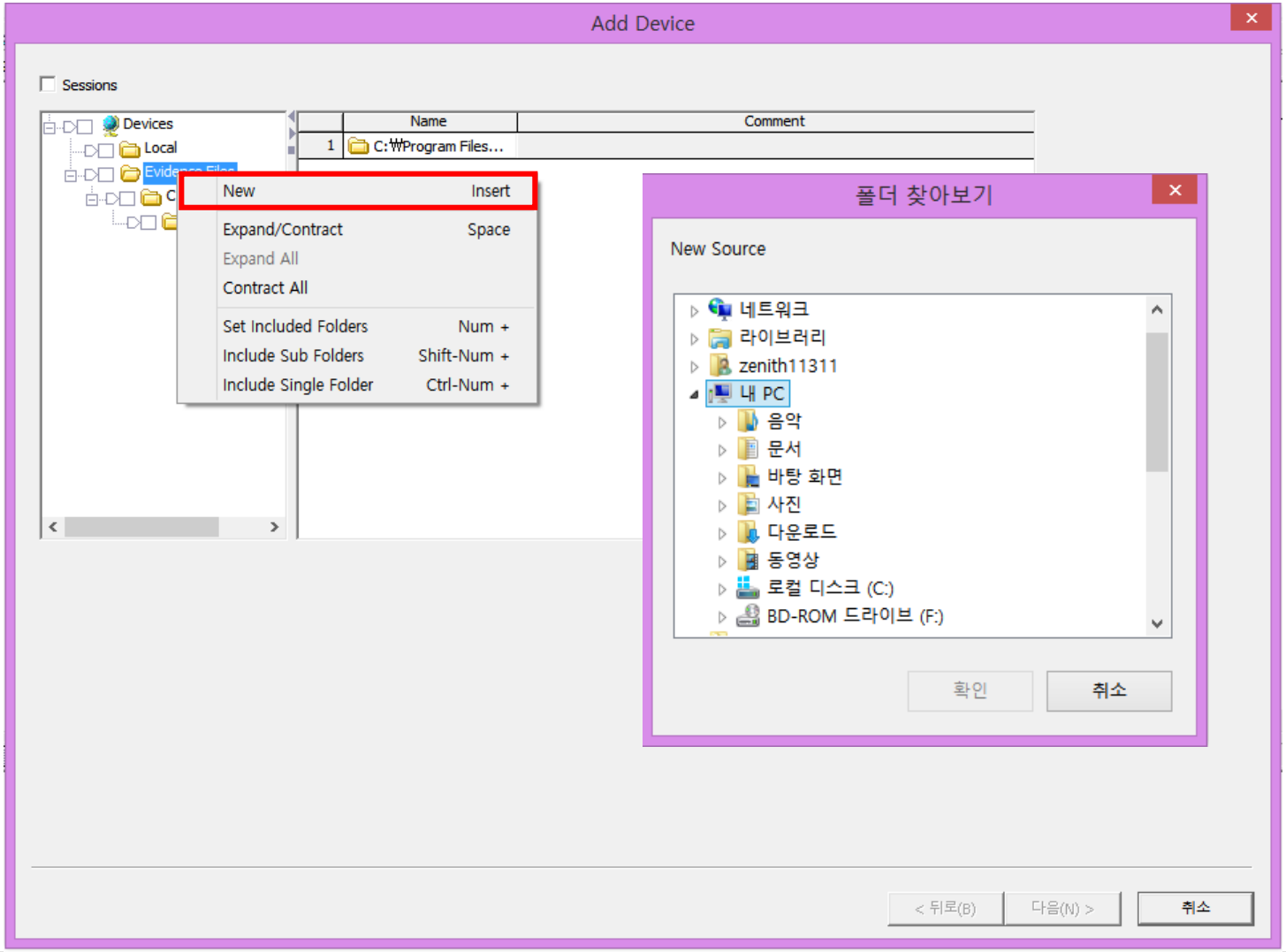
Encase – Adding local device



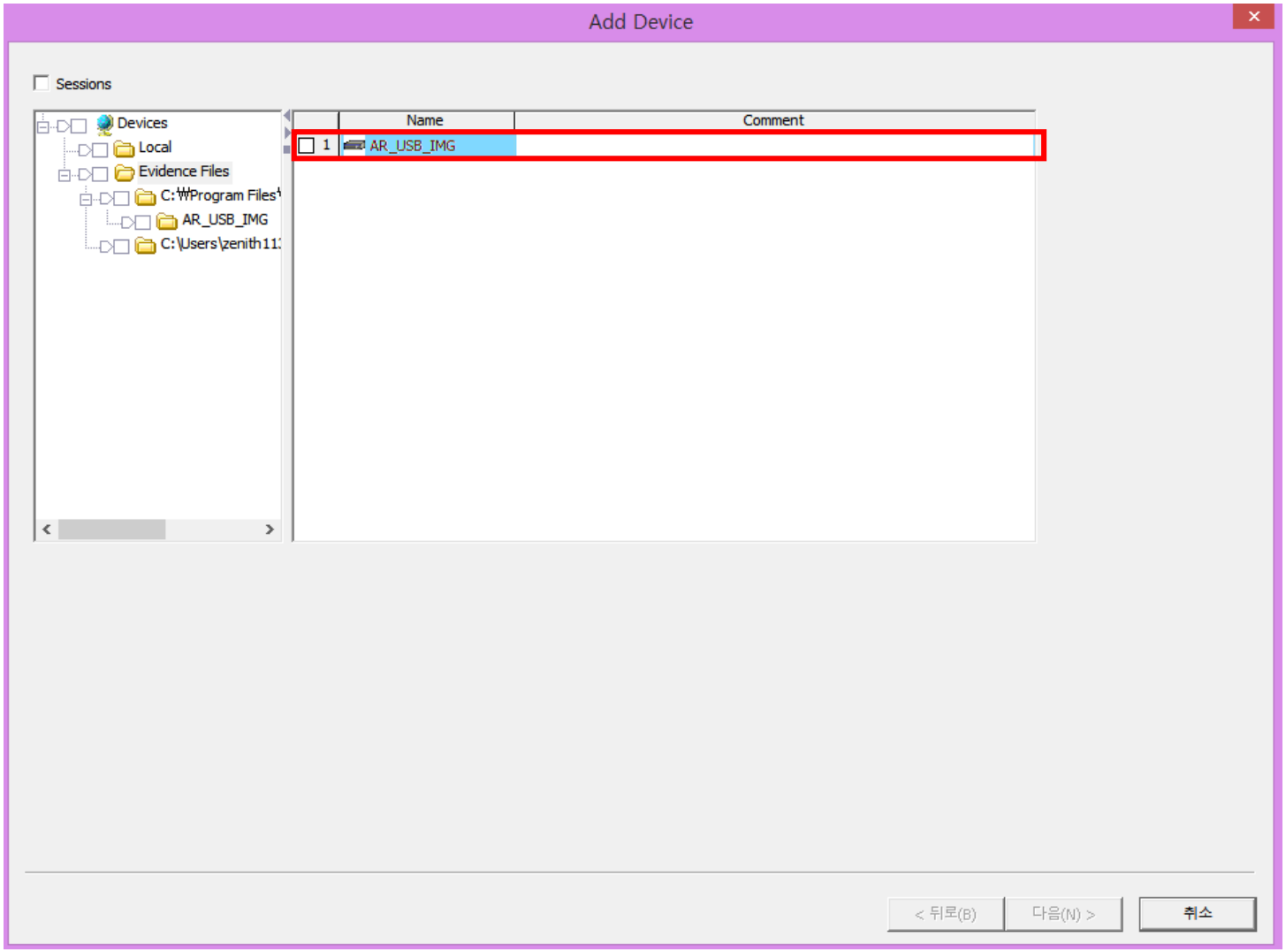
Encase – Adding local device



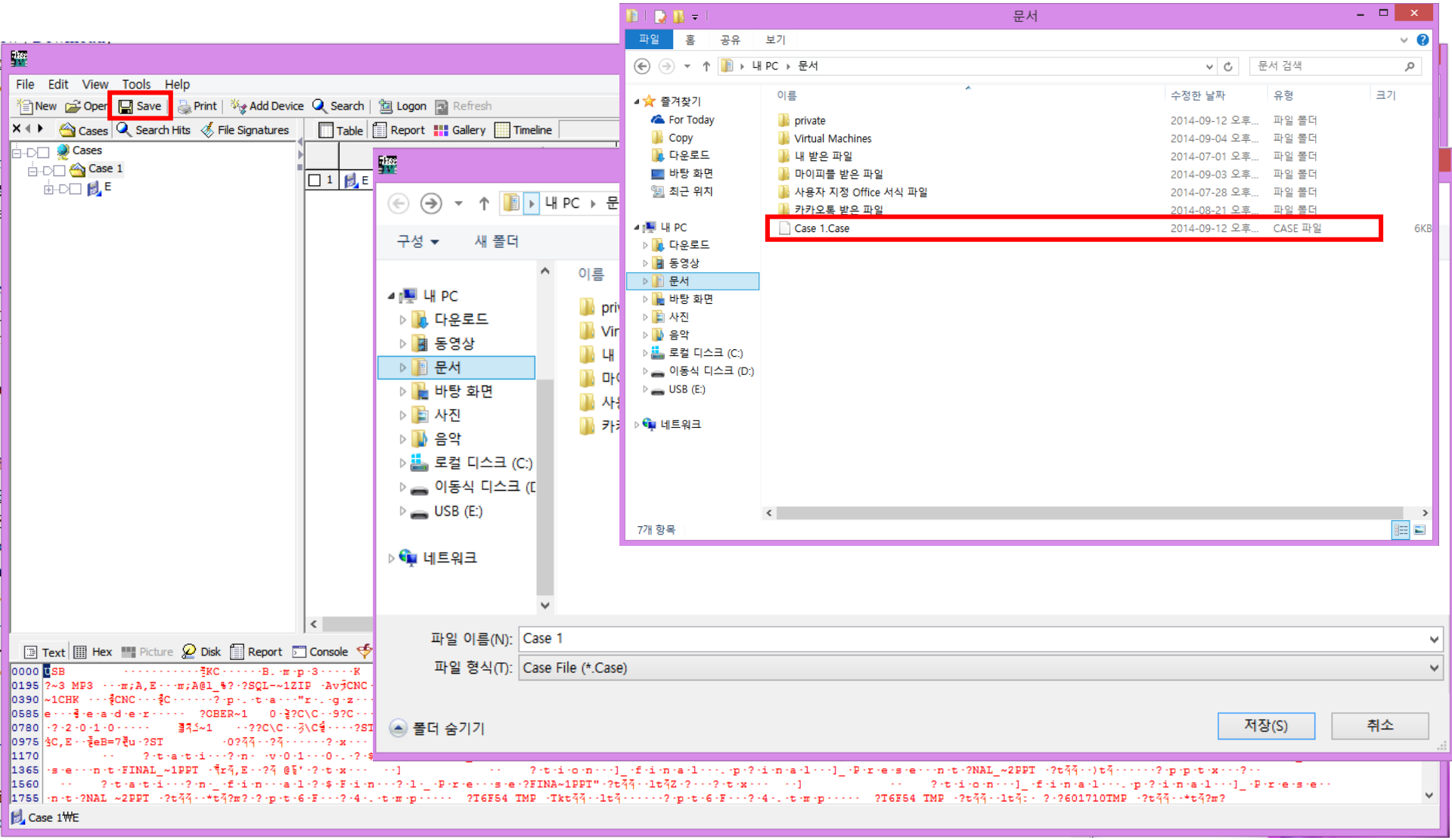
Encase – Adding image file



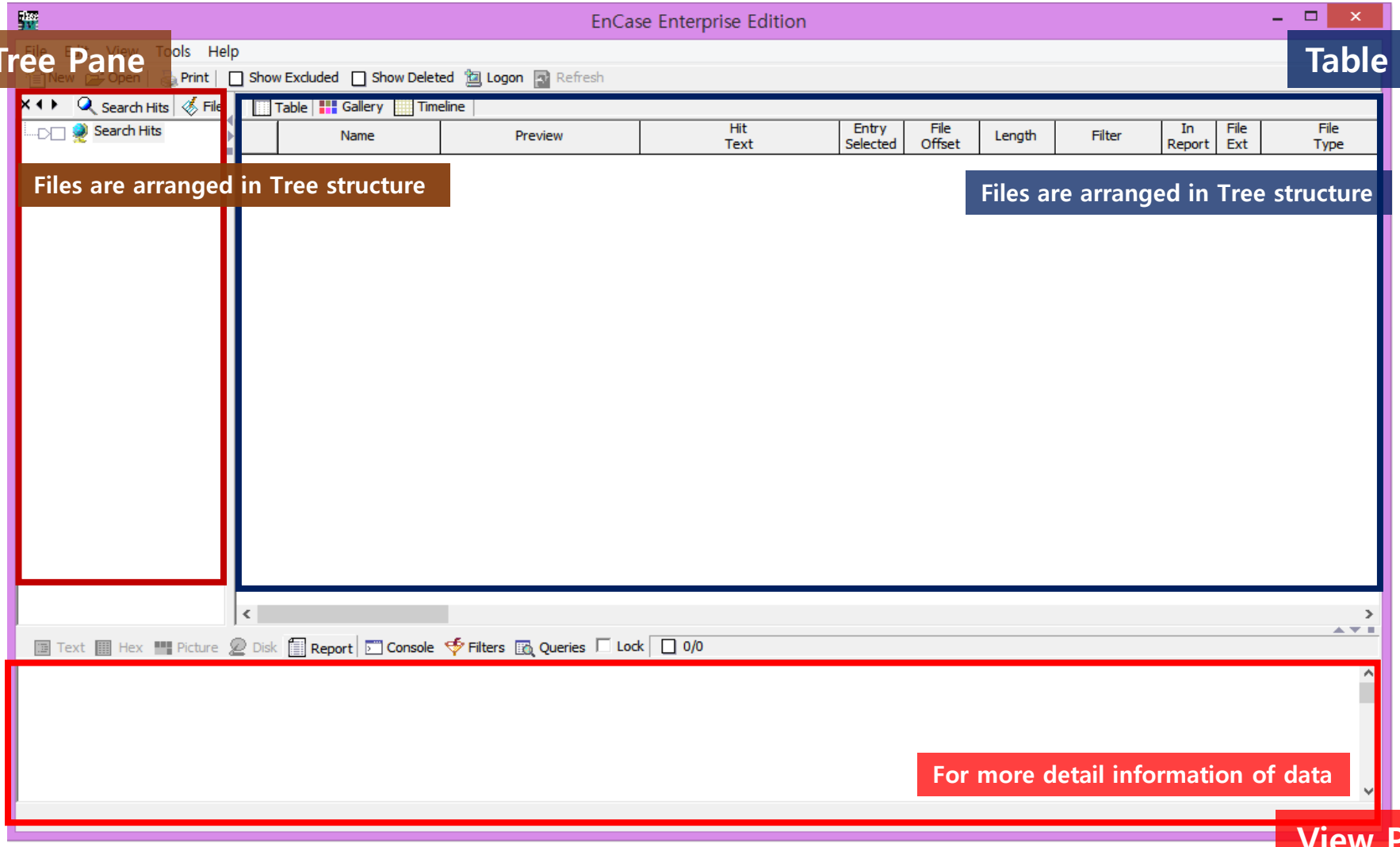
Encase – Adding image file



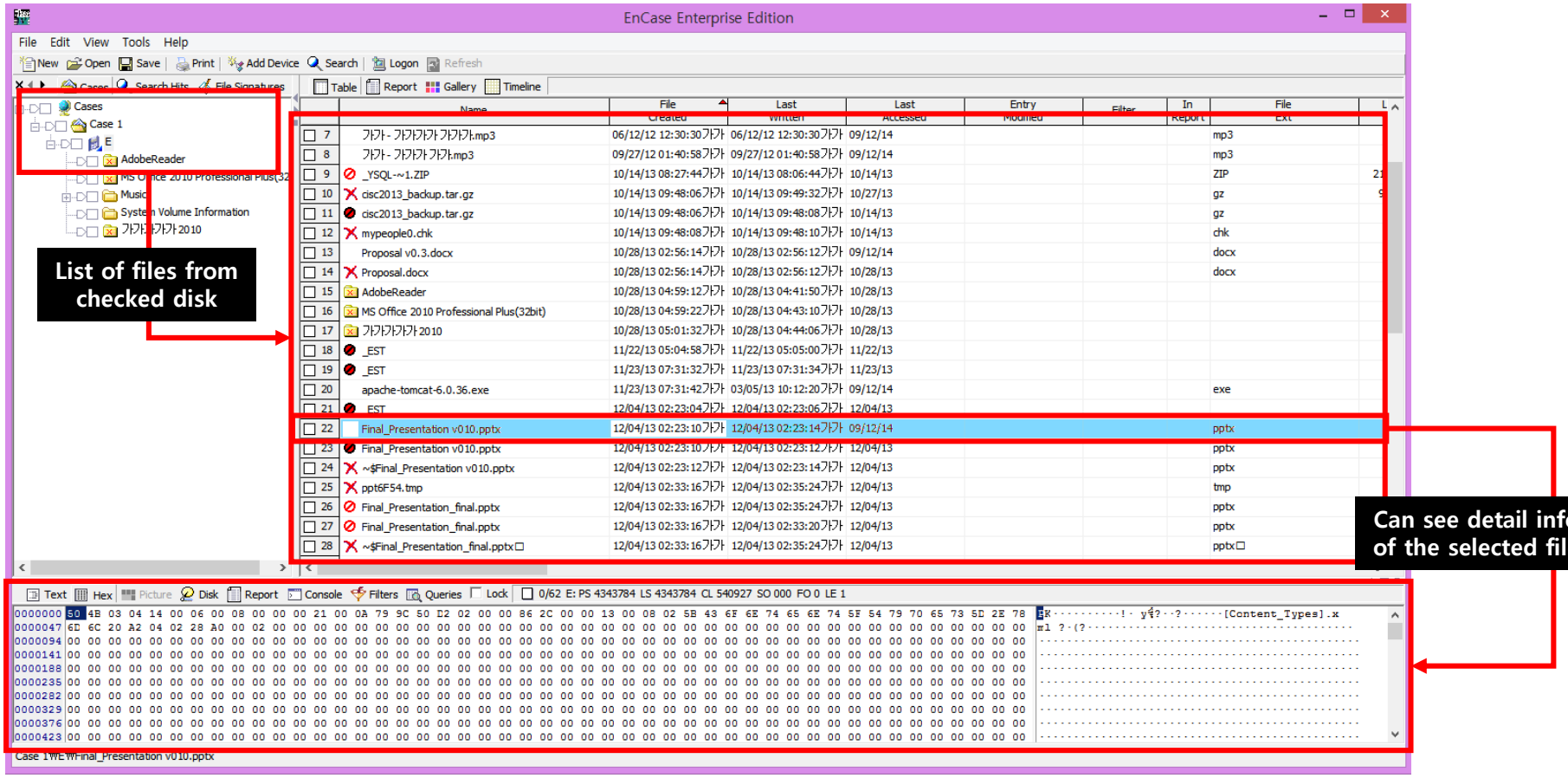
Encase – Saving case



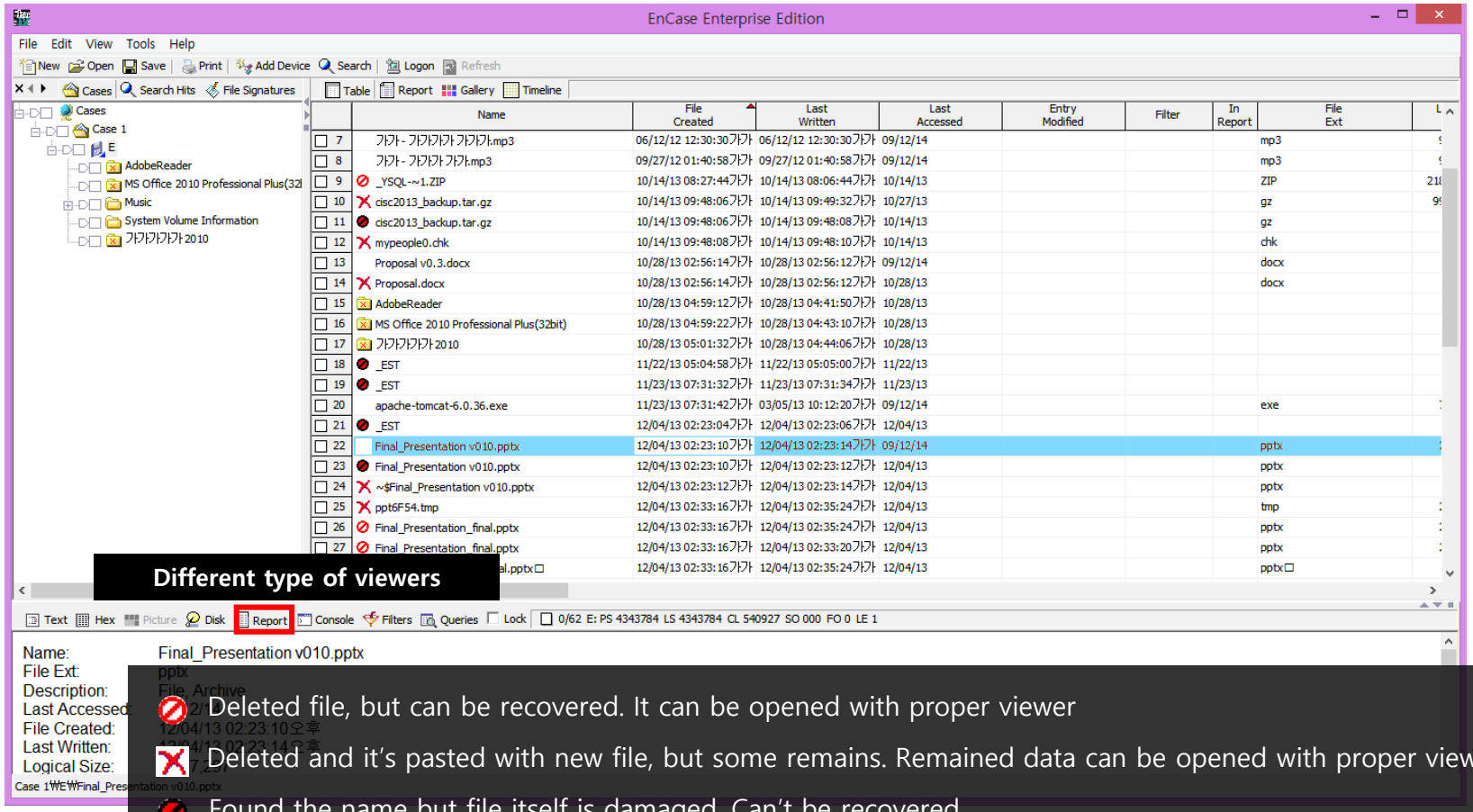
Encase – Tool layout overview



Encase – Tool layout overview



Encase – Tool layout overview



Deleted file, but can be recovered. It can be opened with proper viewer

Deleted and it's pasted with new file, but some remains. Remained data can be opened with proper viewer

Found the name but file itself is damaged. Can't be recovered

Deleted folder, name is found but the contents are lost

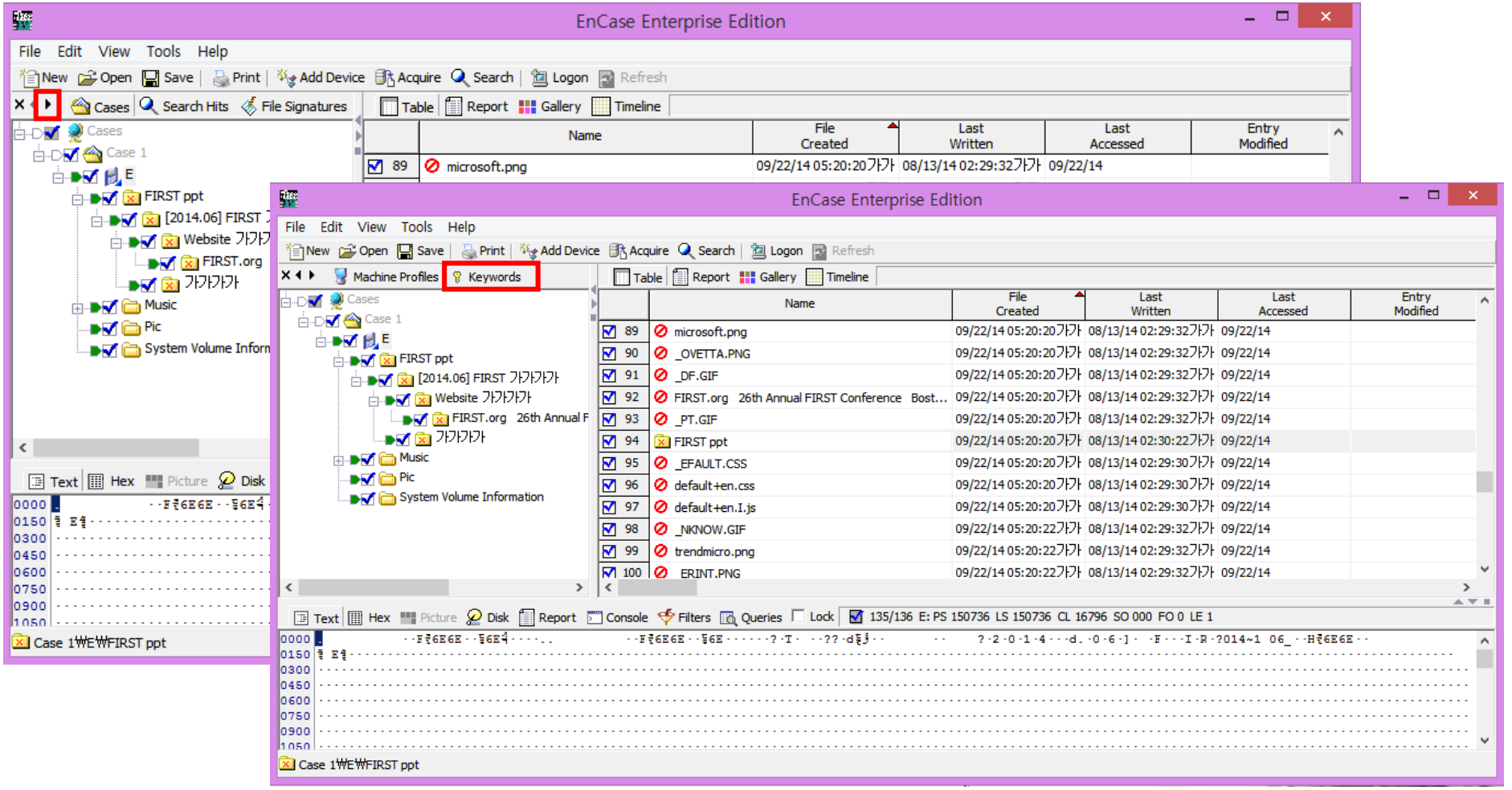
Hard Link file, points directly to original file's inode

EnCase

PDF 파일 검색 후 추출

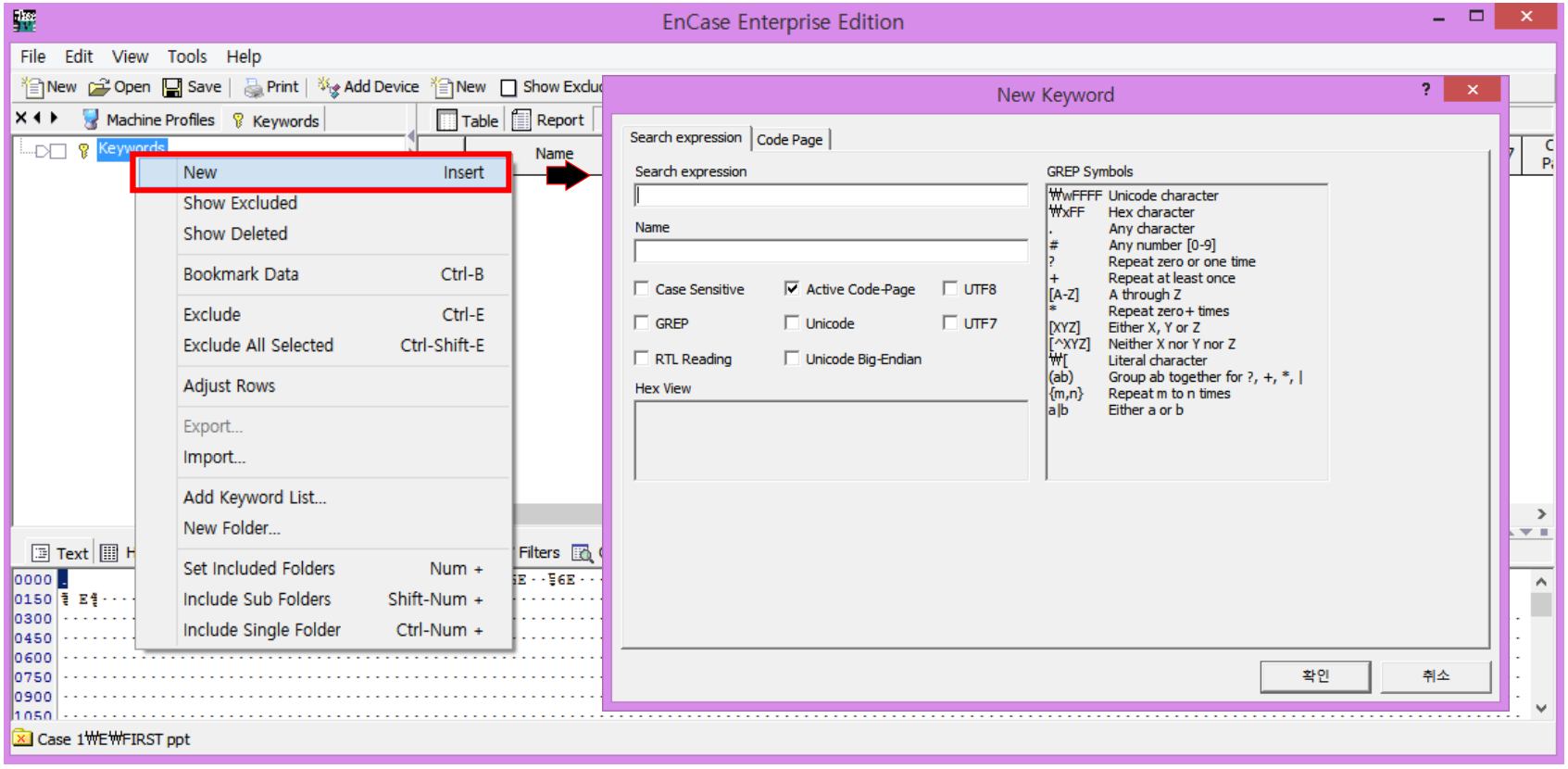
Encase – Using keyword search

Registering Keywords



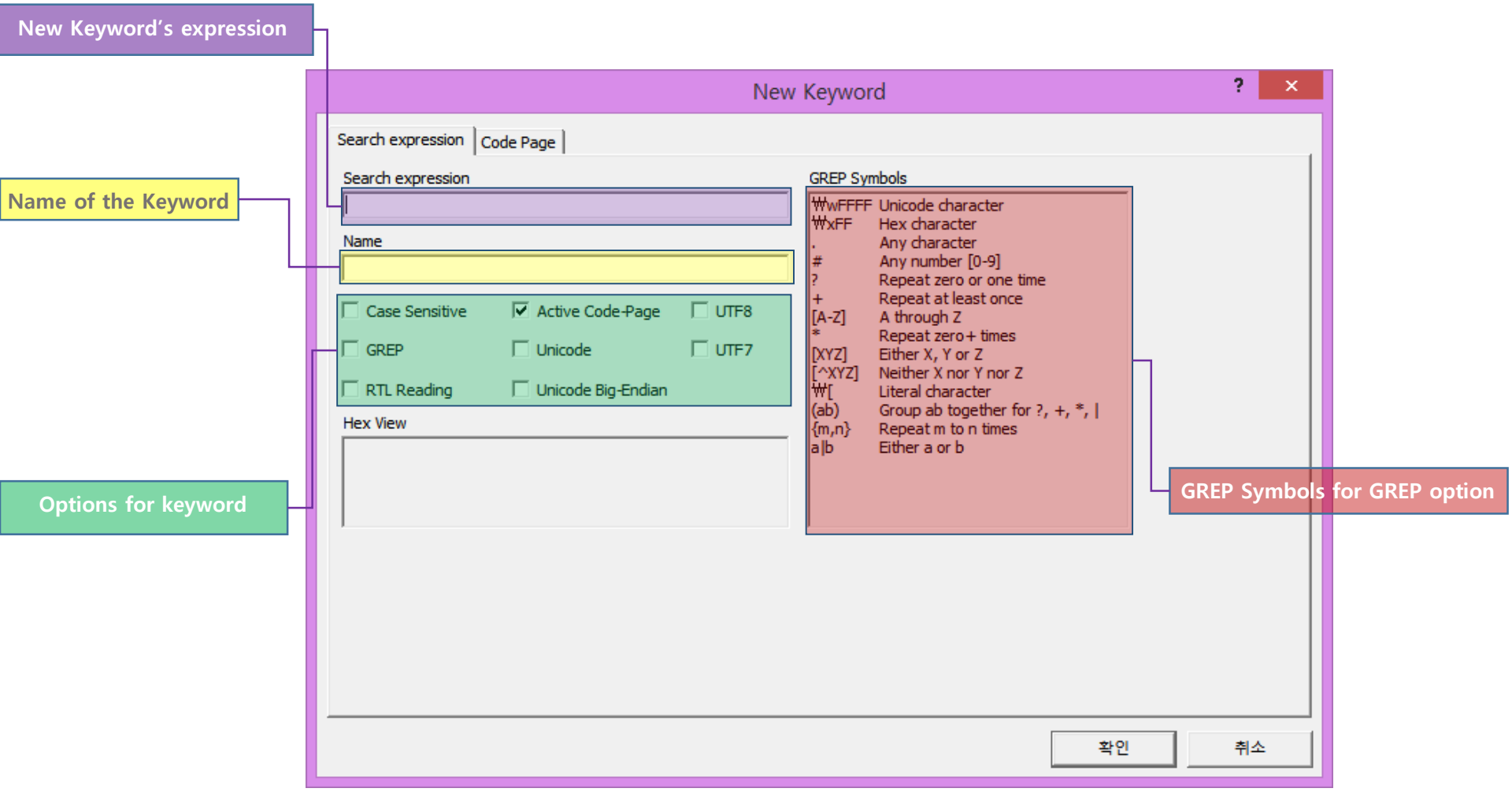
Encase – Using keyword search

Registering Keywords



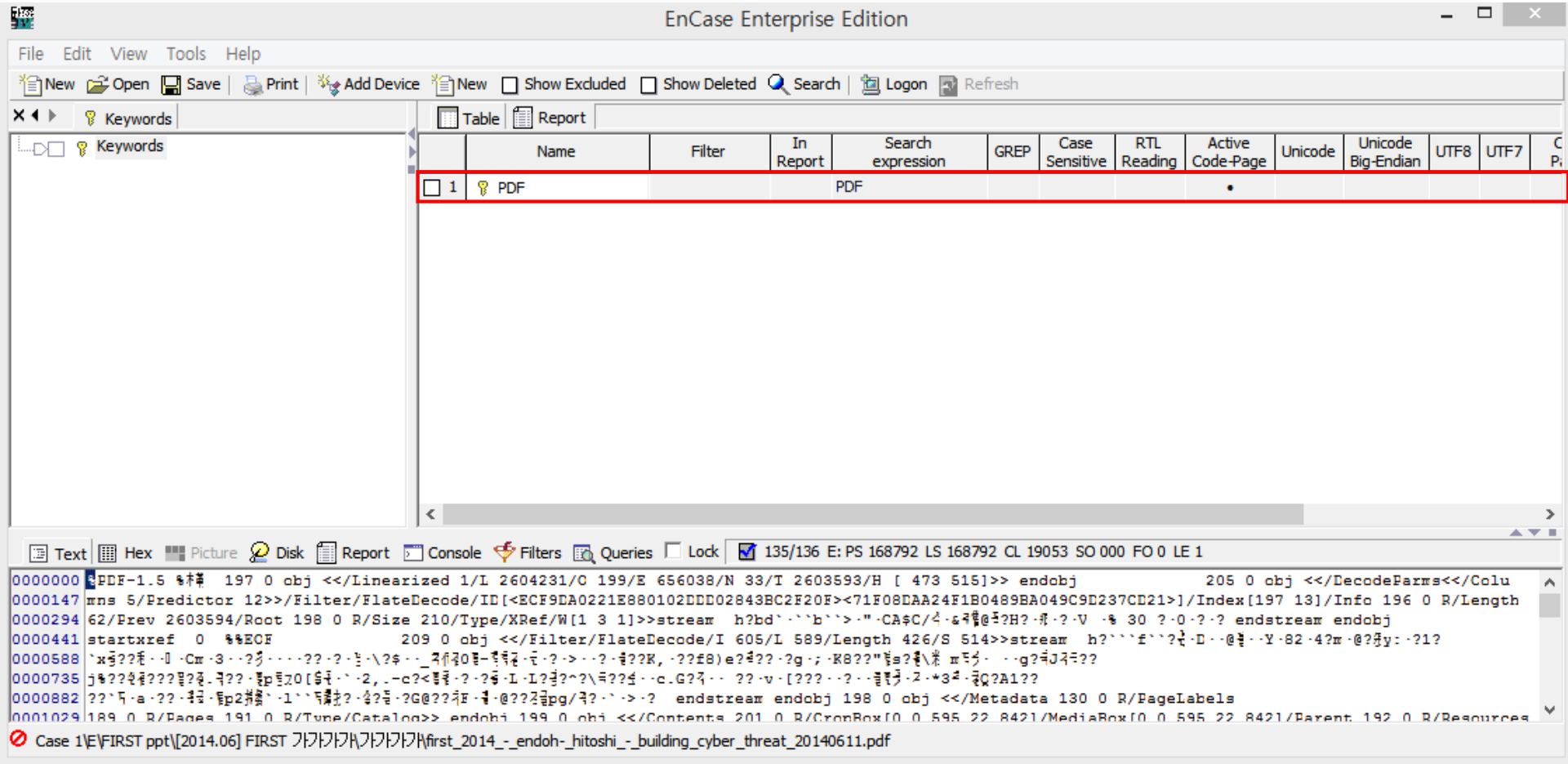
Encase – Using keyword search

Registering Keywords



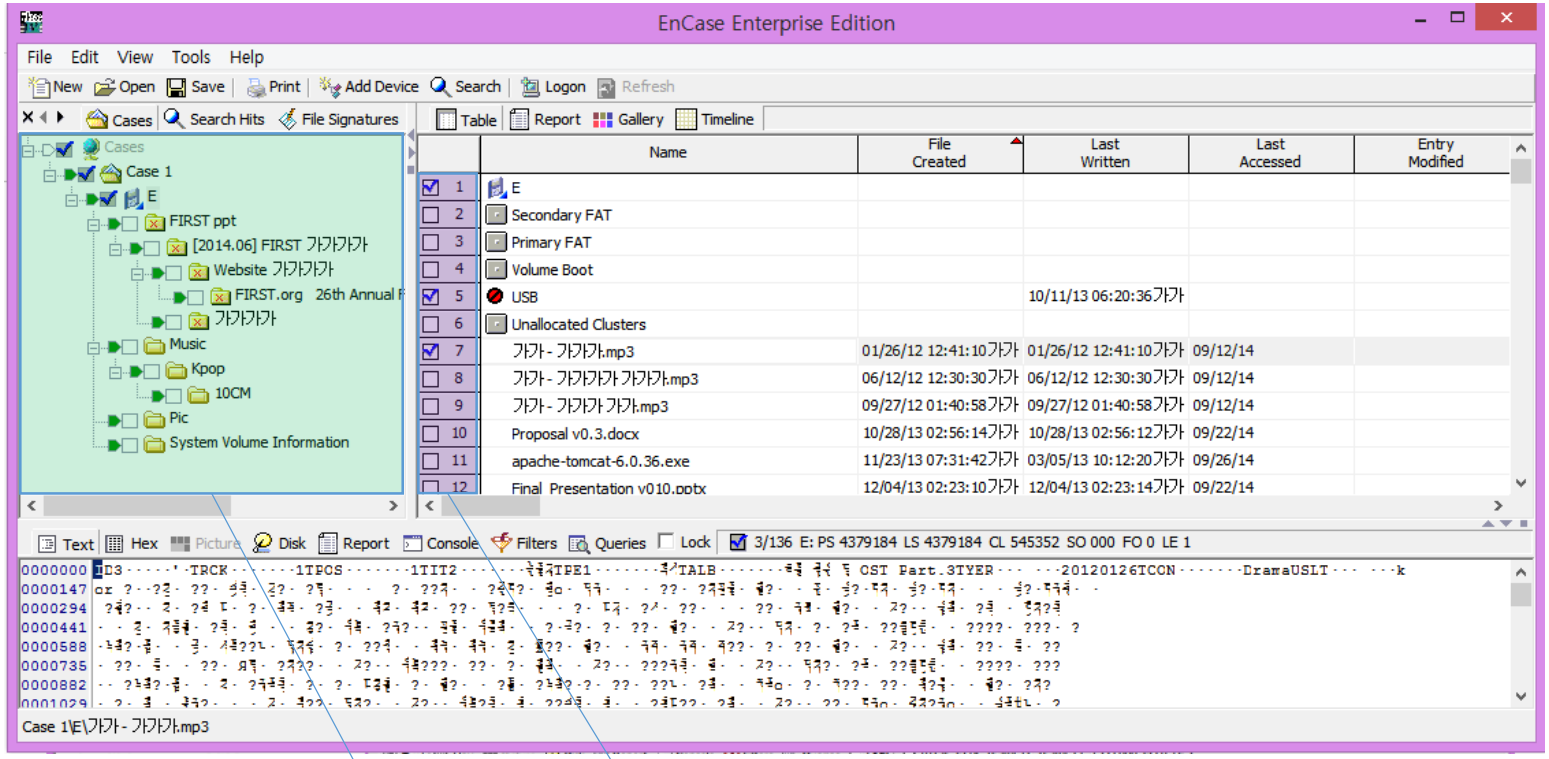
Encase – Using keyword search

Registering Keywords



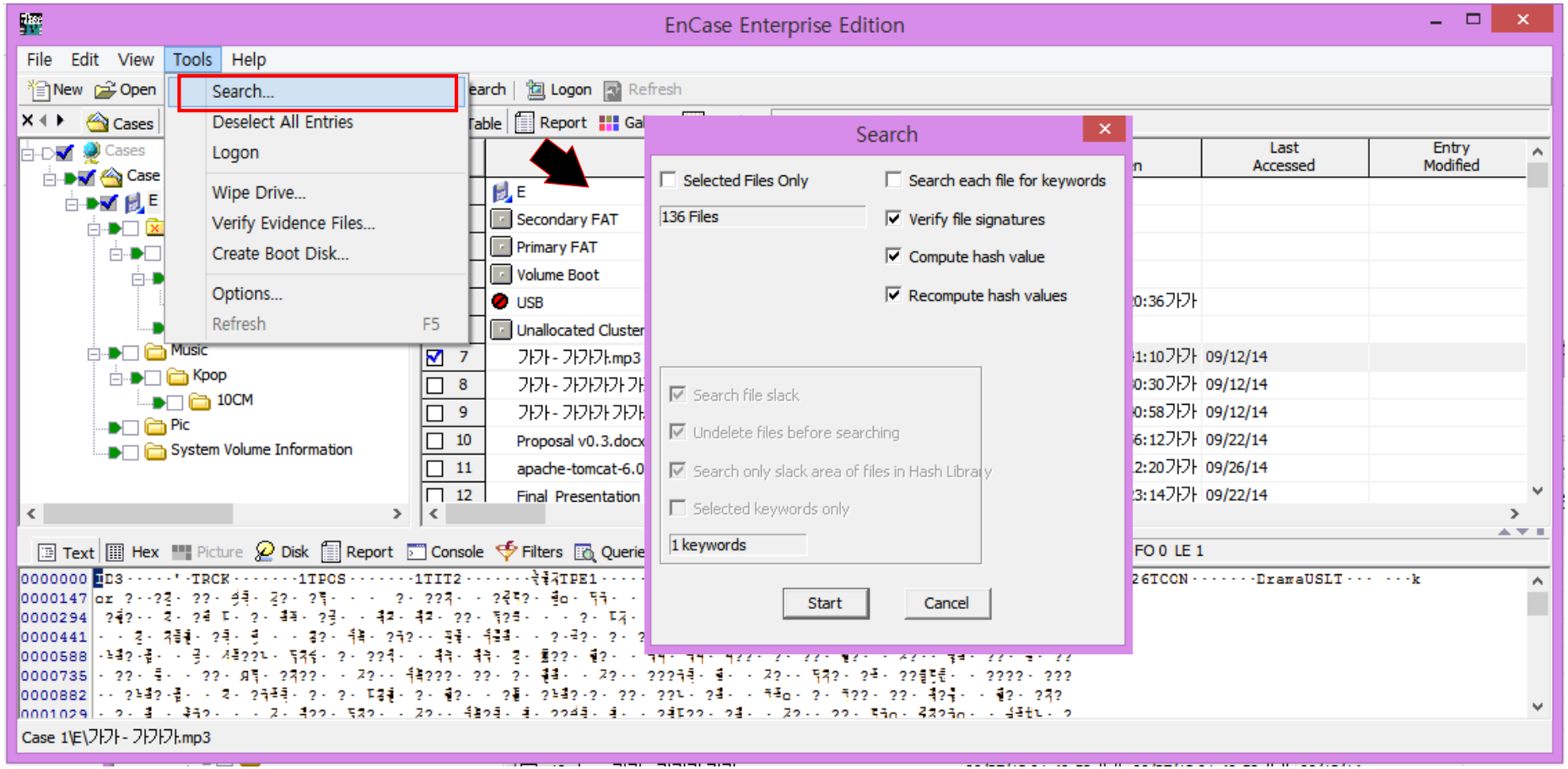
Encase – Using keyword search

Searching Keyword



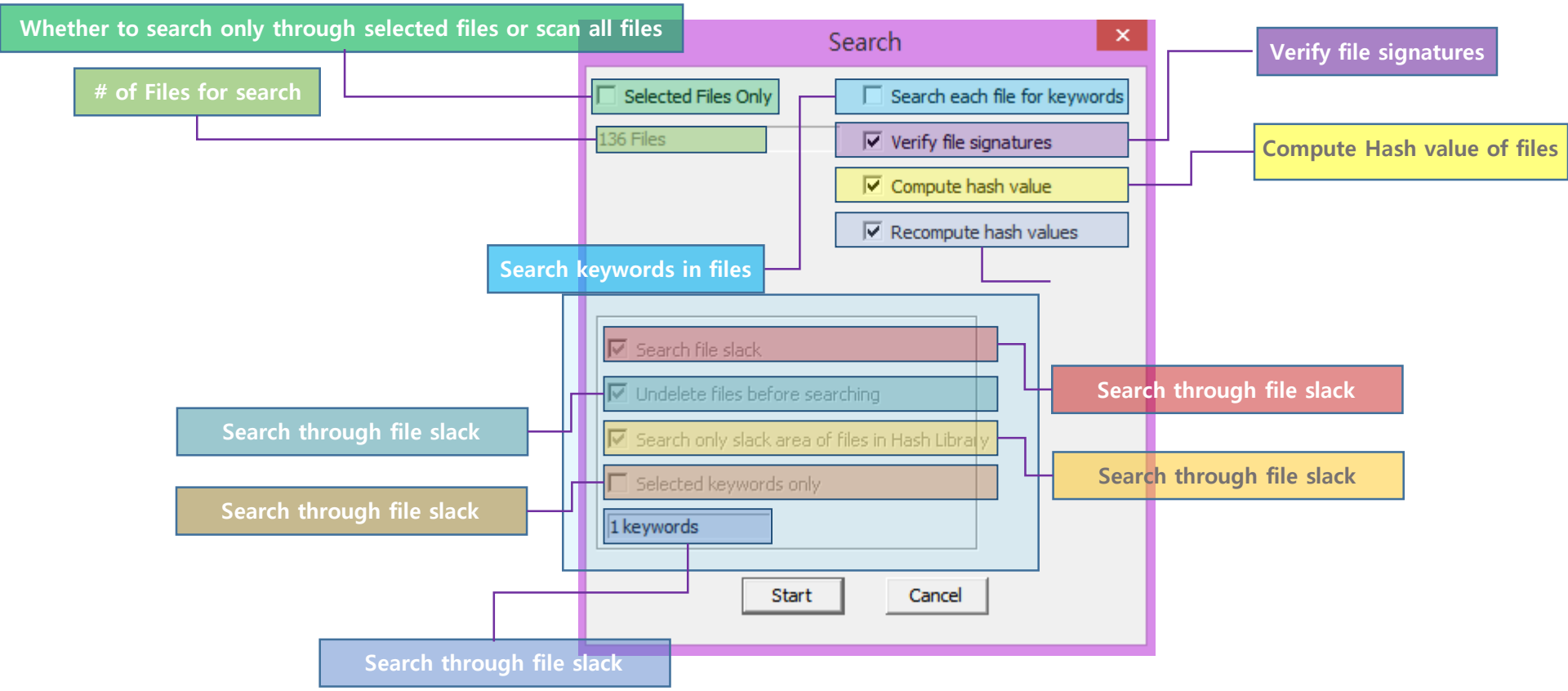
Encase – Using keyword search

Searching Keyword



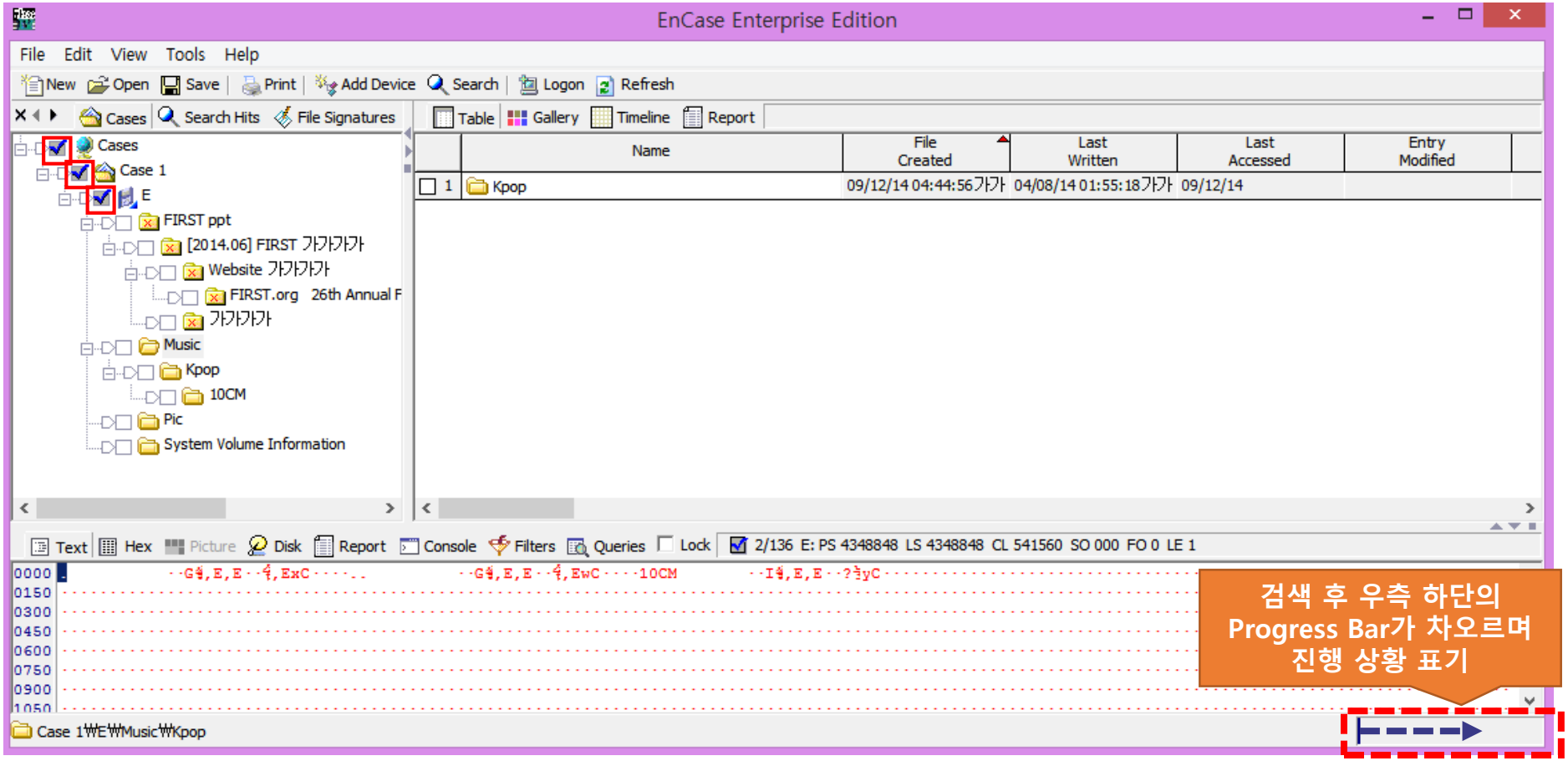
Encase – Using keyword search

Setting Search Options



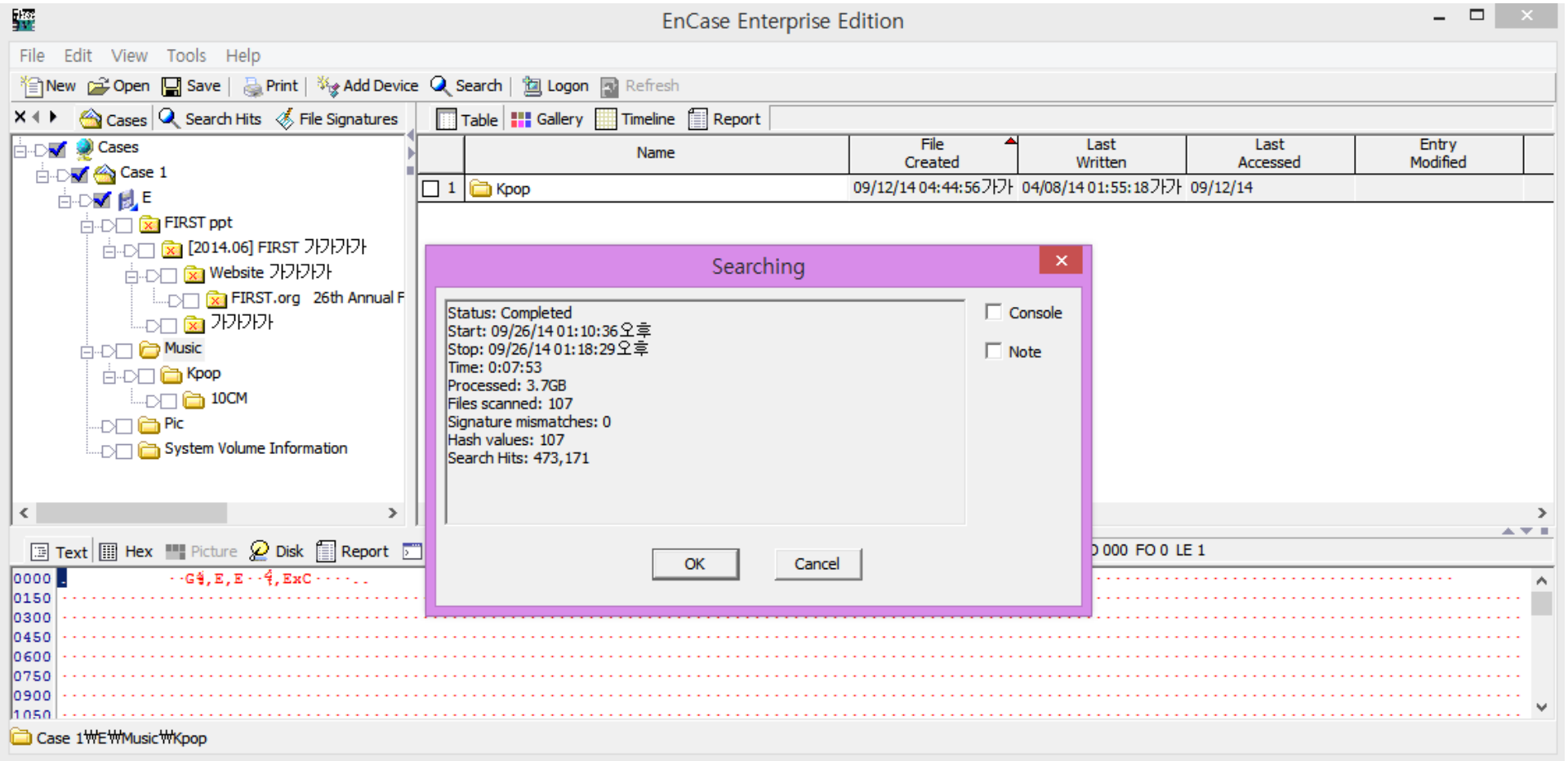
Encase – Using keyword search

Progress Bar



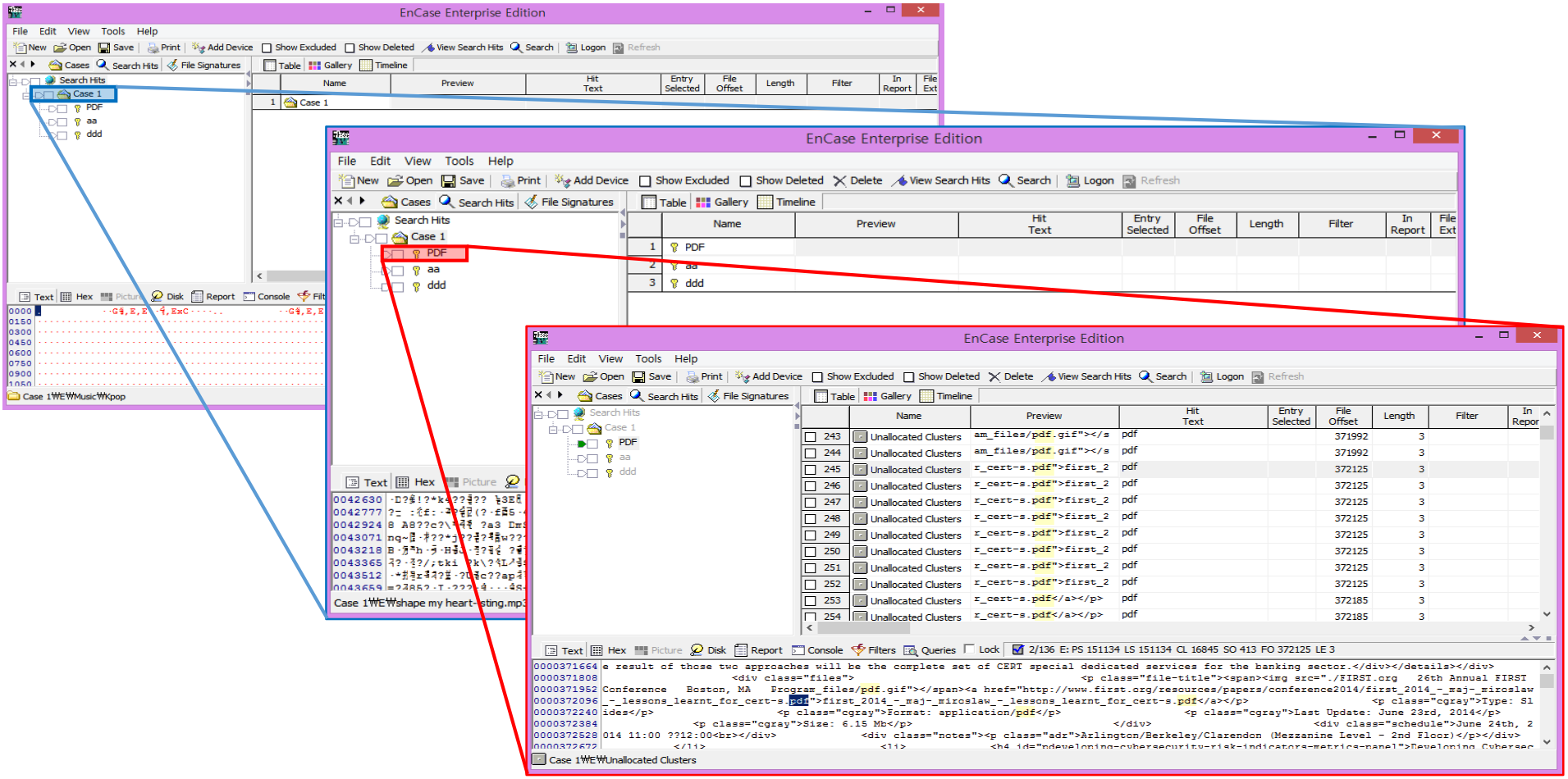
Encase – Using keyword search

Searching Results



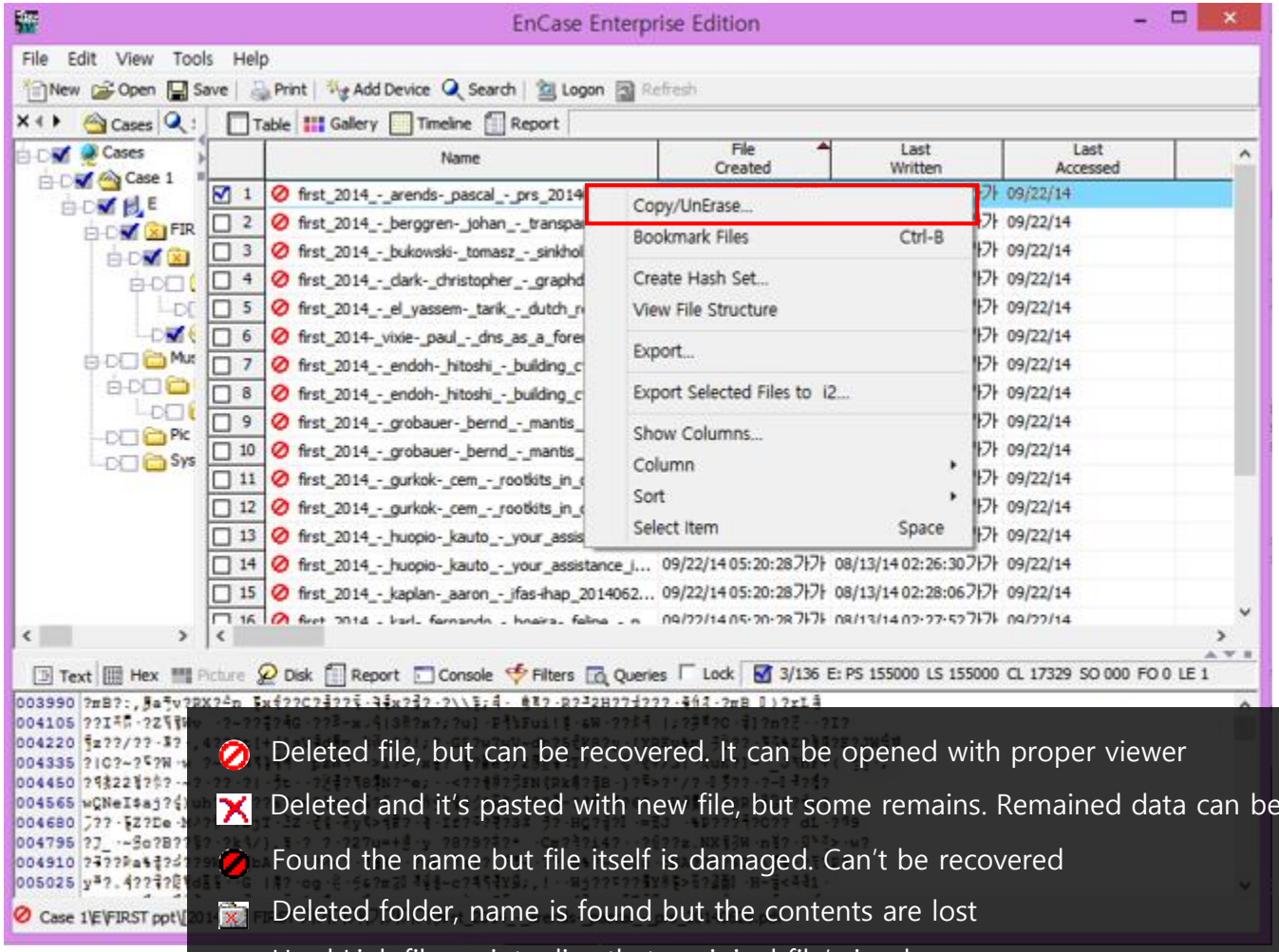
Encase – Using keyword search

Keyword : “pdf” 검색 결과



Encase – Copy/UnErase & Extracting File

Select Target File



Select & Right Click

Choose ***Copy/UnErase...***

Deleted file, but can be recovered. It can be opened with proper viewer

Deleted and it's pasted with new file, but some remains. Remained data can be opened with proper viewer

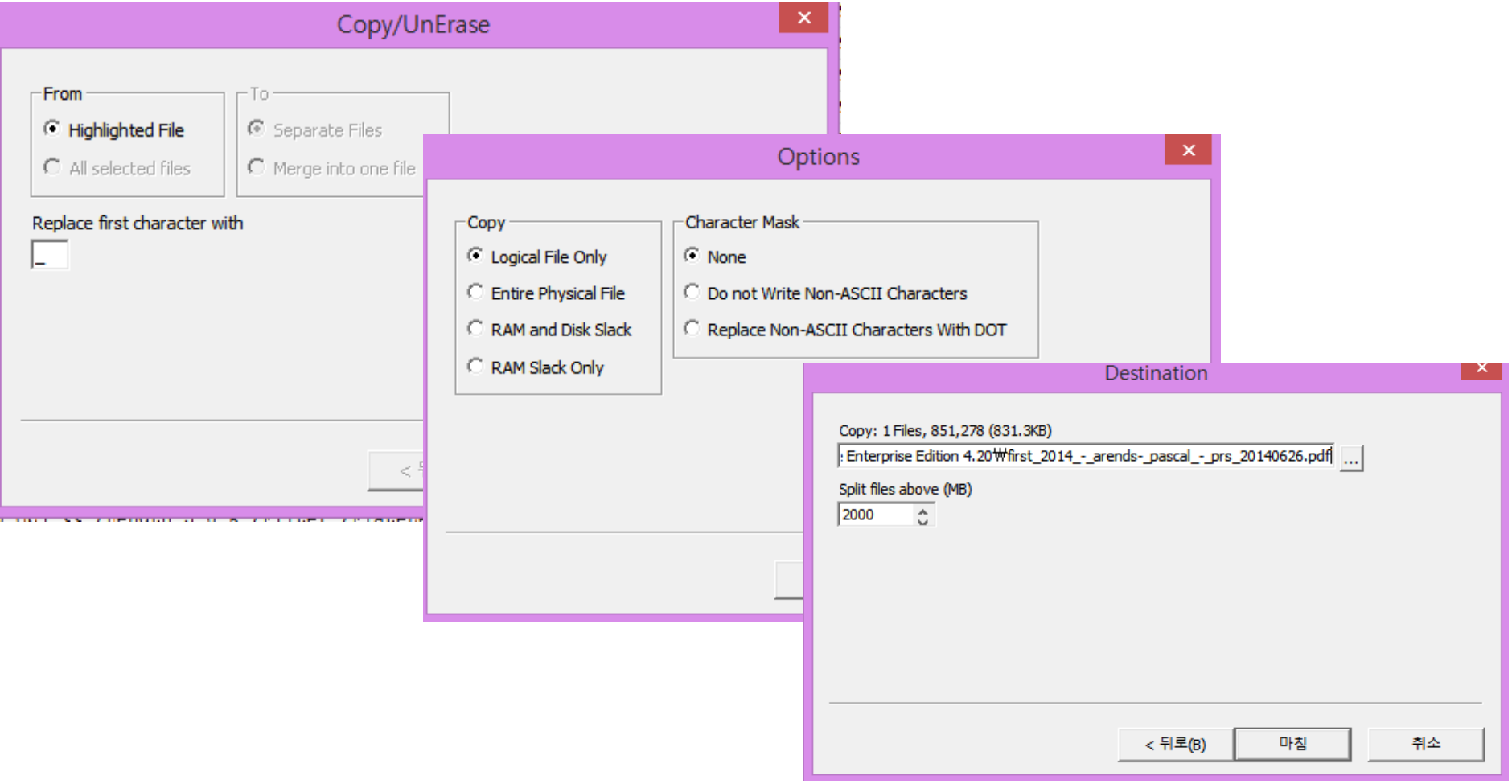
Found the name but file itself is damaged. Can't be recovered

Deleted folder, name is found but the contents are lost

Hard Link file, points directly to original file's inode

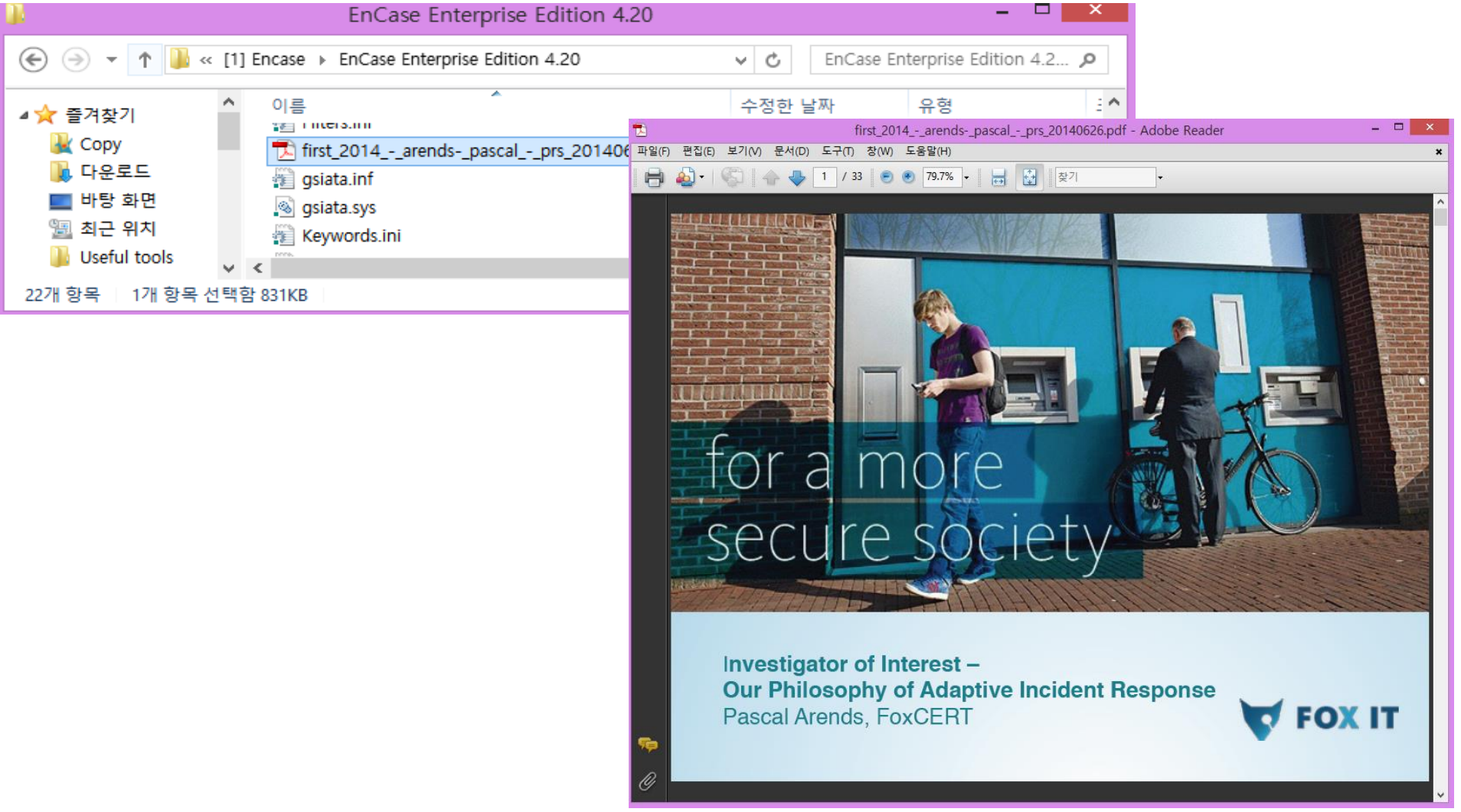
Encase – Copy/UnErase & Extracting File

Select Copy/UnErase Options



Encase – Copy/UnErase & Extracting File

Copy/UnErase Results



감사합니다