EnCase Seminar #2
(Acquiring Digital Evidence)

FORENSIC-PROOF.COM

PRONEER

Welcome to EnCase Seminar!!

Security is a people problem….

Introduction

Outline

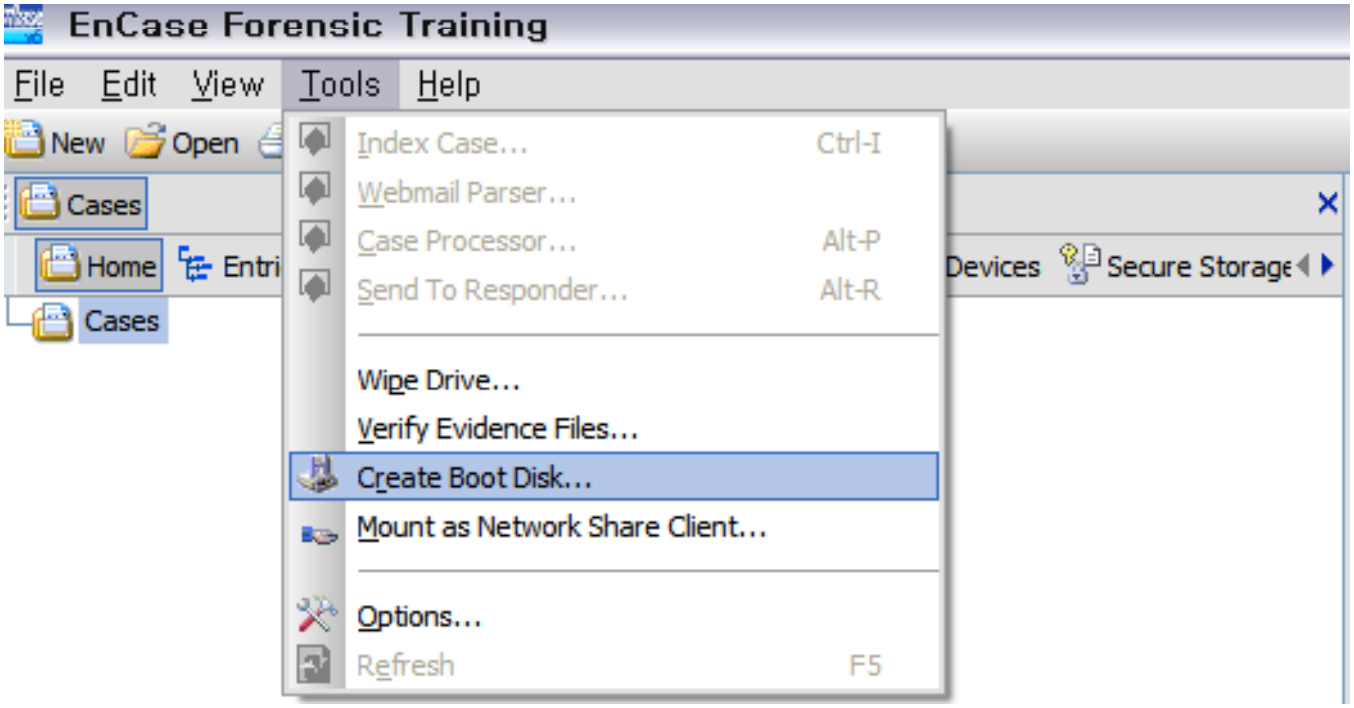
- ~~Week 1 : Hardware and File system Analysis (Chapter 1, 2)~~
- **Week 2 : Acquiring Digital Evidence (Chapter 4)**
- Week 3 : EnCase Concepts and Environment (Chapter 5, 6)
- Week 4 : Actual Test
- Week 5 : Actual Test
- Week 6 : Actual Test
- Week 7 : Actual Test
- ..
- PS : EnScripting

Acquiring Digital Evidence

- *Creating EnCase DOS boot disks*
- *Booting computers using EnCase DOS boot disks*
- *Drive-to-drive Acquisitions*
- *Network Acquisitions*
- *FastBloc Acquisitions*
- *FastBloc SE Acquisitions*
- *LinEn Acquisitions*
- *Enterprise and FIM Acquisitions*

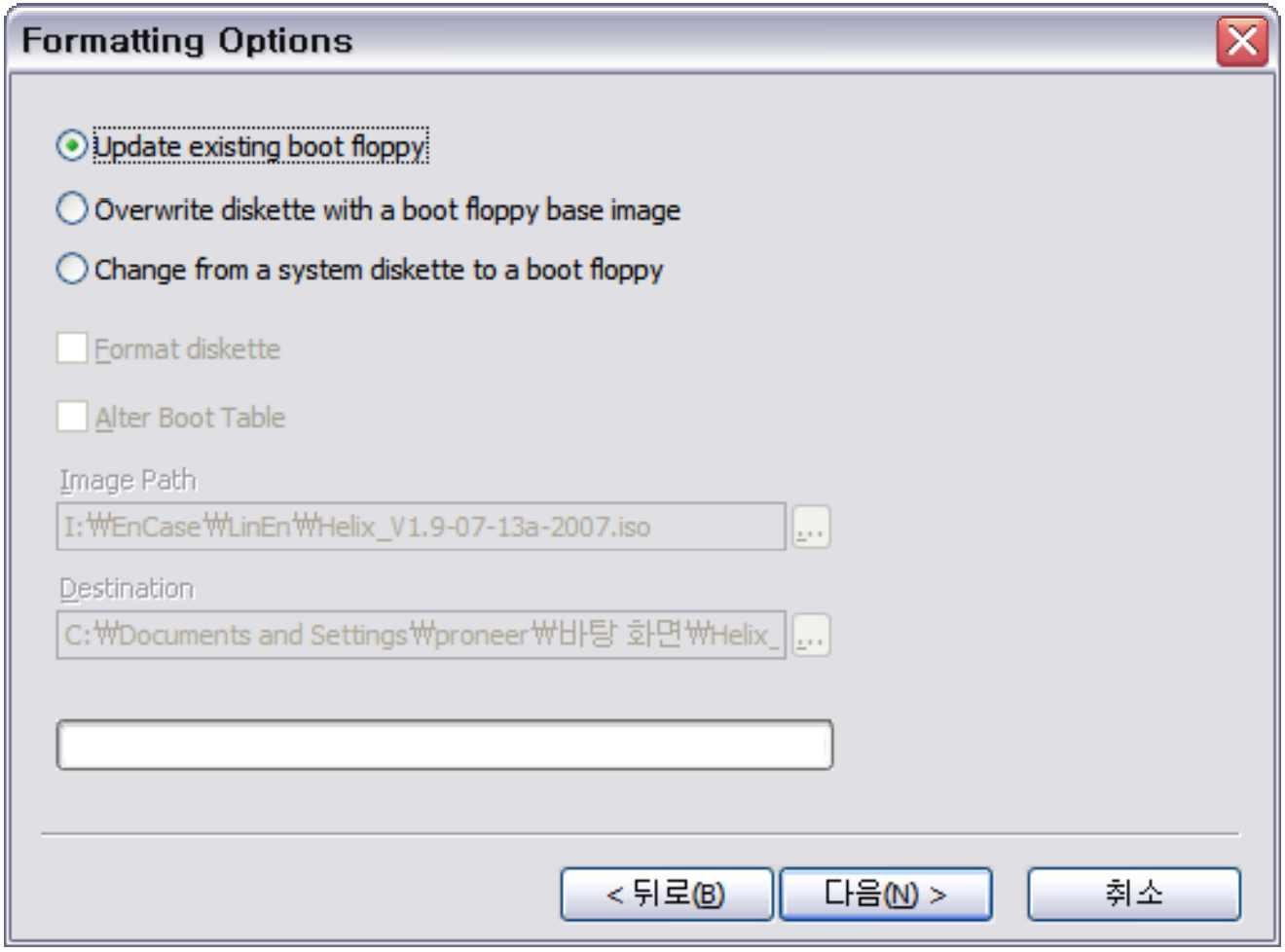
Creating EnCase DOS boot disks

- **Create Boot Disk**



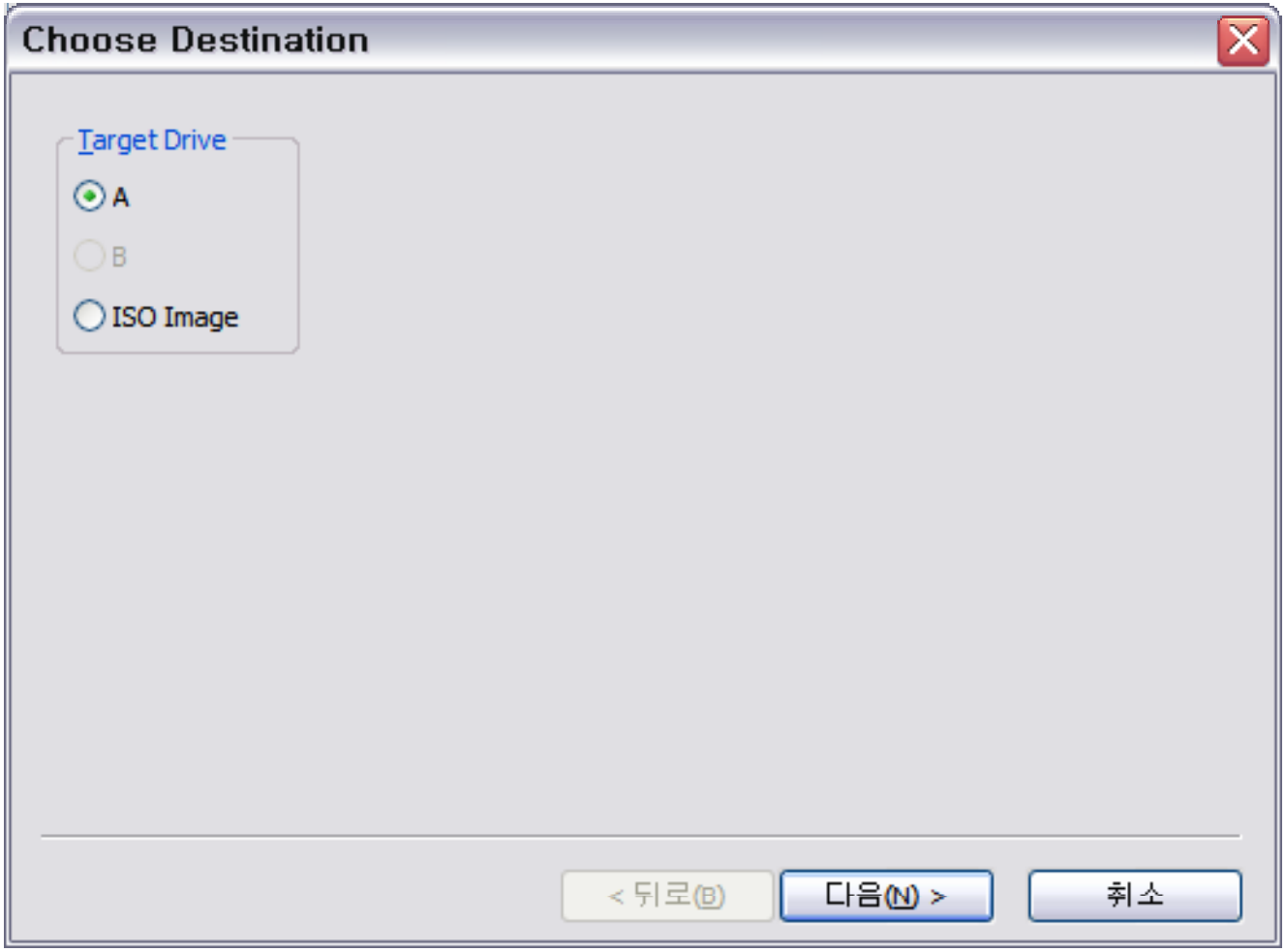
Creating EnCase DOS boot disks

- **Choose Destination ➔ Select A**



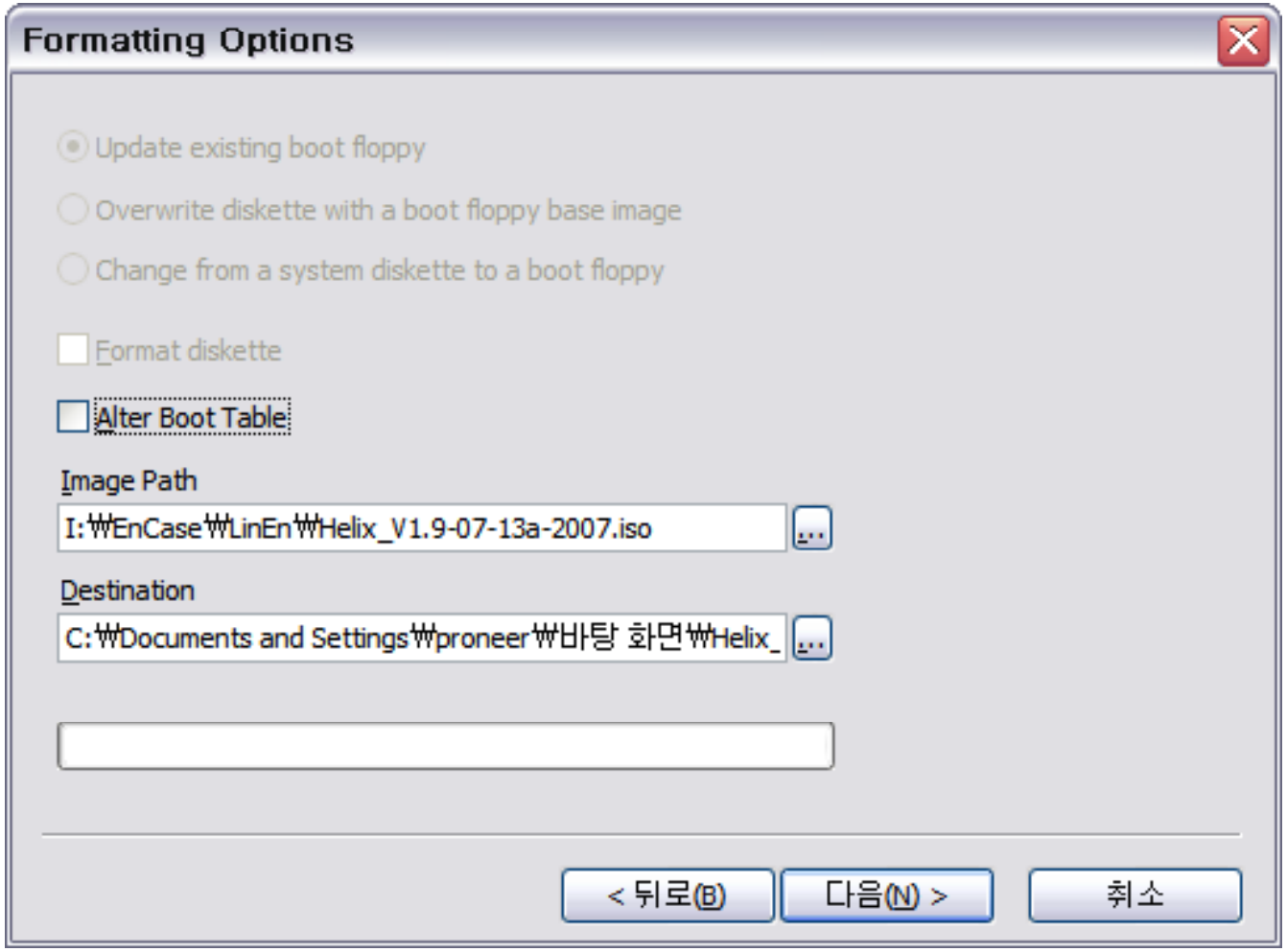
Creating EnCase DOS boot disks

- **Choose Destination**



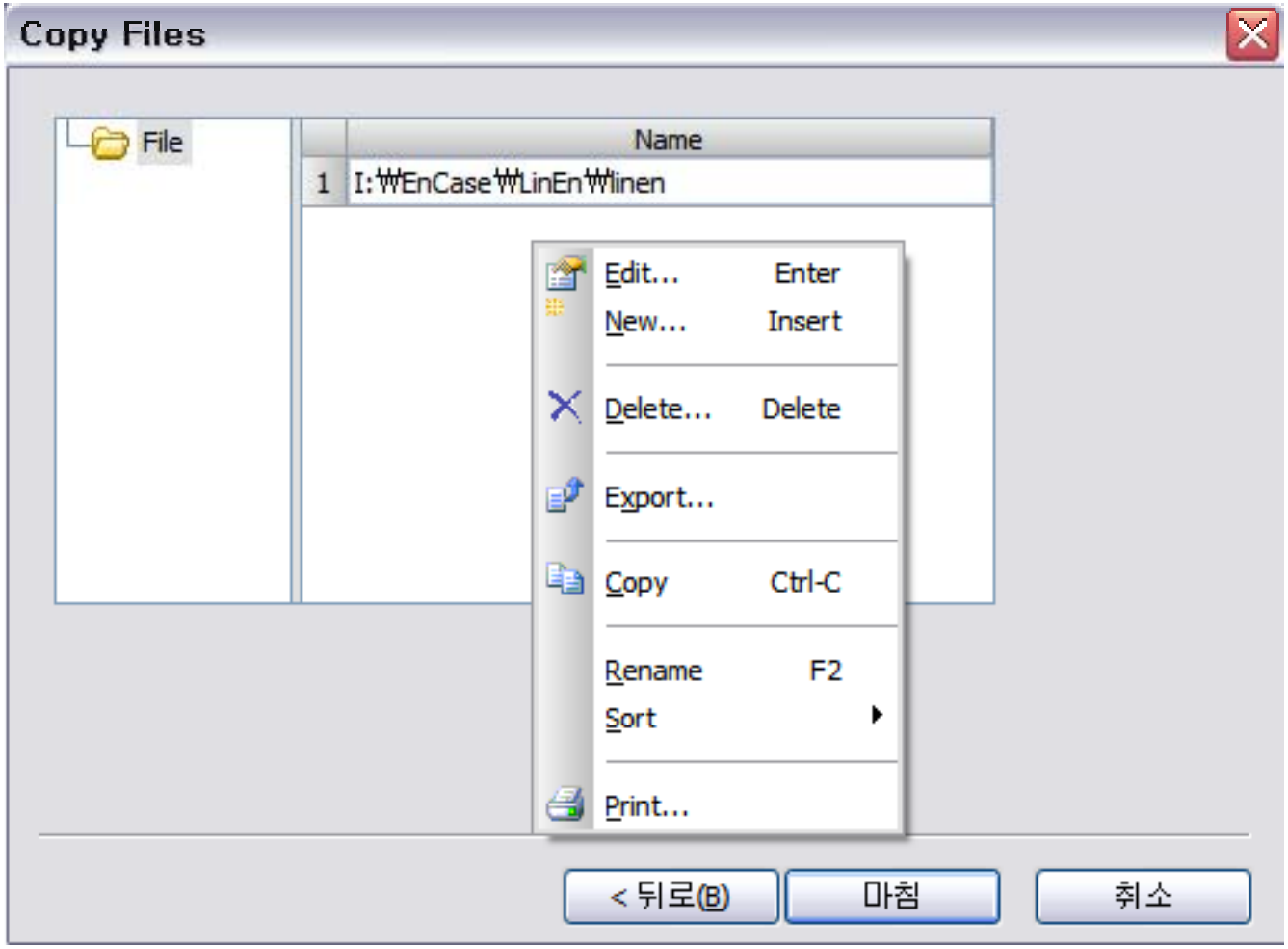
Creating EnCase DOS boot disks

- **Choose Destination ➔ Select ISO Image**



Creating EnCase DOS boot disks

- Choose Destination ➔ Copy Files



Acquiring Digital Evidence

- *Creating EnCase DOS boot disks*
- *Booting computers using EnCase DOS boot disks*
- *Drive-to-drive Acquisitions*
- *Network Acquisitions*
- *FastBloc Acquisitions*
- *FastBloc SE Acquisitions*
- *LinEn Acquisitions*
- *Enterprise and FIM Acquisitions*

Booting computers using EnCase DOS boot disks

Need a DOS boot

✓ 윈도우 환경에서 증거를 획득하기 위한 방안은 이미 존재 (using write-blocking method)

✓ DOS Boot가 필요한 경우

1. 호스트(host) BIOS와 용의자(suspect or Target) 시스템 BIOS 간의 Geometry가 불일치
2. 용의자의 저장매체가 호스트 메인보드의 보안 스키마에 영향을 받는 경우
3. 저장매체가 RAID 구성인 경우 (EnCase 미지원)

Booting computers using EnCase DOS boot disks

HPA and DCO data

- ✓ HPA (Host Protected Area)
  - ATA-4 표준에서 소개
  - 저장매체 일정 영역을 시스템 벤더에서 사용 (recovery, security, registration, 등)
  - Pheonix FirstBIOS
  - BEER(boot engineering extension record)
  - PARTIES(protected area run-time interface extension services)
  - Dell 노트북은 Dell MediaDirect 저장 용도로 사용
  - IBM, LG는 복구 영역으로 사용

Booting computers using EnCase DOS boot disks

HPA and DCO data

- ✓ DCO (Device Configuration Overlay)
  - ATA-6 표준에서 소개
  - 제조한 저장매체와 다르게 용량을 구성하도록 지원

- ✓ HPA, DCO 모두 BIOS에 의해 접근 불가능
- ✓ DirectATA를 통해 접근해야 함 (HPA, DCO를 생성하기 위한 ATA 명령 모드)

Booting computers using EnCase DOS boot disks

Other Reasons for Using a DOS boot

✓ HPA, DCO 영역 탐지 방법

- Total LBA Sectors 보다 EnCase에서 보여주는 섹터가 적은 경우
- 제조업체에서 제공하는 상세서와 EnCase에서 보여주는 섹터가 다른 경우

✓ 용의자의 시스템에서 부팅을 하는 경우 항상 잠재된 위험을 고려

➔ **DOS Boot 가 필요**

Booting computers using EnCase DOS boot disks

Steps for Using a DOS boot

1. 조사 컴퓨터를 정상 종료 (Chapter 3 참고)
2. 컴퓨터의 뒷부분의 전원선을 제거, 케이스를 열어 드라이브와 연결 상태를 점검

   추가적인 드라이브가 존재하는지 점검
3. 하나 이상의 드라이브가 존재한다면 레이블을 붙인 후 모두 제거 (전원, 데이터 케이블 모두)
4. 클립이나 별도의 장비를 이용해 드라이브를 연 후 부팅 디스크를 삽입
5. 모든 드라이브를 연결 해제, 부팅 디스크가 삽입되었다면 전원 연결

   BIOS Setup 메뉴로 진입
   - F1 (for IBMs and many clones)
   - F2 or Delete (Dells, HPs, and other clone)
   - F10 (Compaqs)

Booting computers using EnCase DOS boot disks

Steps for Using a DOS boot

6. 부트 디스크를 실행을 위해 부트 순서 변경
7. 설정 저장 후 BIOS Setup 종료
8. 부트 디스크가 정상적으로 부팅되는지 테스트
9. 정상 부팅되는 것을 확인한 후 다시 전원선 제거
10. 각 단계가 모두 정상적이라면 드라이브를 연결 ➔ 부팅

    만약 부트 디스크가 부팅되지 않는다면 바로 전원선 제거

✓ 드라이브 연결 전 확인해야 할 사항

- 드라이브가 FAT으로 포맷되어 있는지 (EnCase for DOS ➔ NTFS 인식 불가)
- 드라이브가 구별 가능한 볼륨 레이블을 가지는지
- 이미지를 저장할 디렉터리가 존재하는지

Acquiring Digital Evidence

- *Creating EnCase DOS boot disks*
- *Booting computers using EnCase DOS boot disks*
- *Drive-to-drive Acquisitions*
- *Network Acquisitions*
- *FastBloc Acquisitions*
- *FastBloc SE Acquisitions*
- *LinEn Acquisitions*
- *Enterprise and FIM Acquisitions*

Drive-to-drive Acquisitions

why it's drive-to-drive

- ✓ 대상 드라이브와 이미지를 저장할 드라이브가 같은 메인보드에 연결된 경우
- ✓ EnCase 부트 디스크와 이미지 저장 드라이브가 필요
- ✓ 대부분의 조사관들에 의해 기존에 사용되었던 방법
- ✓ 증거 획득(이미징) 속도는 시스템 구성 하드웨어에 의존
- ✓ 구성 방법
  - 서로 다른 채널 상의 master-to-master 연결
  - 같은 채널 상의 master-to-slave 연결

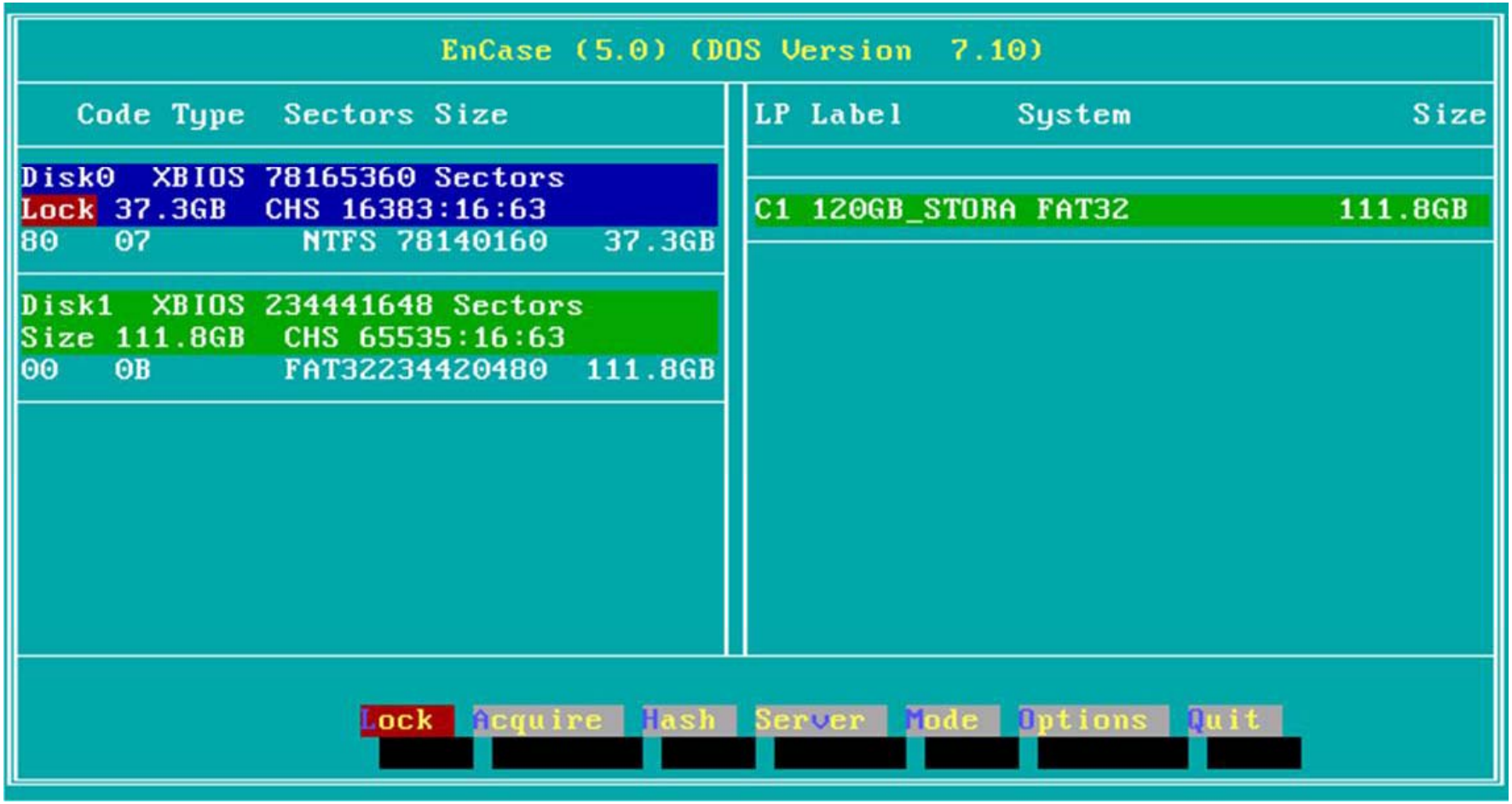
Drive-to-drive Acquisitions

Steps for Drive-to-Drive DOS Acquisition

1. "Booting a Computer Using the EnCase Boot Disk" 방법으로 부팅할 준비
2. 저장할 드라이브를 연결
   - master-to-master > master-to-slave
   - EnCase for DOS 는 FAT 만 인식 가능
   - 구별 가능한 볼륨 이름을 사용
   - 반드시 저장 드라이브에 저장할 디렉터리를 미리 생성
3. 드라이브 연결이 완료되면 부트 디스크를 삽입 ➔ 부팅, 정상적이지 않다면 바로 전원선 제거
4. 성공적인 부팅 후 A: 프롬프트가 나오면 "en"이라고 치고, EnCase for DOS로 진입

Drive-to-drive Acquisitions

- **Steps for Drive-to-Drive DOS Acquisition**



Drive-to-drive Acquisitions

Steps for Drive-to-Drive DOS Acquisition

5. FastBloc을 통해 모든 섹터에 대한 접근이 불가능 했다면 DirectATA 모드로 변경
6. EnCase for DOS는 모든 장치에 대한 software write-block 이 적용

   write-block이 적용 ➔ "Lock" 문자 표시, 증거 획득 후 저장 드라이브는 "Unlock"

   ➔ 각 드라이브는 구별 가능한 볼륨 레이블을 설정
7. 이미지를 저장할 드라이브가 "Unlock" 되었다면 "A"를 눌러 수집
8. 사건 번호, 조사자 이름, 증거 번호 등을 입력한다.
9. 다음으로 시스템 날짜와 시간 확인 ➔ 정확하지 않다면 변경 (증거 획득에 활용)
10. 증거 파일 압축 옵션을 선택 (압축을 사용하면 공간은 절약되지만 좀 더 많은 시간 필요)
11. 획득할 때 MD5를 계산할 것인지 선택
10. 획득한 증거를 패스워드로 보호할지 설정

Drive-to-drive Acquisitions

Steps for Drive-to-Drive DOS Acquisition

11. Segment size 설정(1 MB ~ 2,000 MB(GB))

    (기본 설정 640 MB)

14. 획득 범위 설정 (Start/Stop sector)

15. Block Size, Error Granularity (EnCase 5+)

16. 획득 시작

    ➔ 수집되는 증거 파일은 파일 조각 크기에 따라 .E01, .E02의 확장자

    ➔ E99가 넘어가면 EAA, EAB, EAC 로 확장자가 생성된다.

Drive-to-drive Acquisitions

Supplemental Information About Drive-to-Drive DOS Acquisition

- ✓ Mac, Unix, BSD 계열의 드라이브도 EnCase for DOS를 통해 획득 가능

  획득 후 EnCase for Windows를 통해 파일 구조 확인

- ✓ SCSI 드라이브의 경우에는 부트 디스크 생성 시 해당 SCSI 드라이버를 포함

  추가적인 Adapter Card 필요

- ✓ 증거 수집 완료 후 문서화, 레이블 작성, 안전한 가방에 보관

- ✓ **Acquiring a Mac Drive Using FireWire**

Acquiring Digital Evidence

- *Creating EnCase DOS boot disks*
- *Booting computers using EnCase DOS boot disks*
- *Drive-to-drive Acquisitions*
- *Network Acquisitions*
- *FastBloc Acquisitions*
- *FastBloc SE Acquisitions*
- *LinEn Acquisitions*
- *Enterprise and FIM Acquisitions*

Network Acquisitions

Reasons to Use Network Acquisitions

- ✓ Network Cable로 가능한 범위에서 수집
- ✓ 용의자 시스템(EnCase for DOS)과 호스트 시스템(EnCase for Windows) 간의 수집
- ✓ Network Acquisition 이 사용되는 경우
  - Acquiring invisible HPA or DCO data
  - Acquiring data from a laptop hard drive (include security scheme)
  - Acquiring data quickly
  - Previewing data before acquiring

Network Acquisitions

Understanding Network Cables

- ✓ EnCase 각 버전마다 yellow crossover cable 포함
- ✓ 같은 장비를 연결하기 위해서 crossover network cable 사용
- ✓ 그럼 다른 장비를 연결하기 위한 케이블은 ? Straight-Through Cable

- ✓ Network Acquisitions을 위해 준비 사항
  - 대상 시스템에 NIC(Network Interface Card)가 장착되어 있는지 확인
  - NIC 드라이버가 포함된 EnCase 부트 디스크 생성

Network Acquisitions

Preparing an EnCase Network Boot Disk

- ✓ ENBD(EnCase Network Boot Disk) / ENBCD(EnCase Network Boot CD) 다운로드
- ✓ 다운 받은 각 파일에는 기본적인 NIC 드라이버가 포함
- ✓ Create Boot Disk를 통해 부트 디스크 생성

Network Acquisitions

Steps for Network Acquisition – Booting Up

1. Windows를 부팅 후 EnCase for Windows는 실행하지 않고 대기
2. 대상 시스템에 Drive-to-Drive에서 했었던 준비작업을 수행

   ➔ 드라이브를 모두 제거하고 부트 순서를 변경한 후 DOS 부트가 되는지 테스트

3. 준비가 완료되면 드라이브를 연결하고 두 시스템 간에 crossover cable을 연결
4. 전원선을 연결하고 전원선을 잡고 있다가 부팅 디스크로 부팅되지 않으면 확 뽑아 버림
5. 정상 부팅되었다면 다음의 메뉴 확인 가능
   - *Network Support*
   - *USB – Acquisition*
   - *USB – Destination*
   - *Clean Boot*

Network Acquisitions

Steps for Network Acquisition – Setting Up Acquisition

1. Network Support를 선택 ➔ SCSI 드라이버 로드 ➔ NIC 드라이버 로드
2. HPA/DCO 영역이 존재할 경우 임시적으로 서버 종료 후 DirectATA 모드로 변경

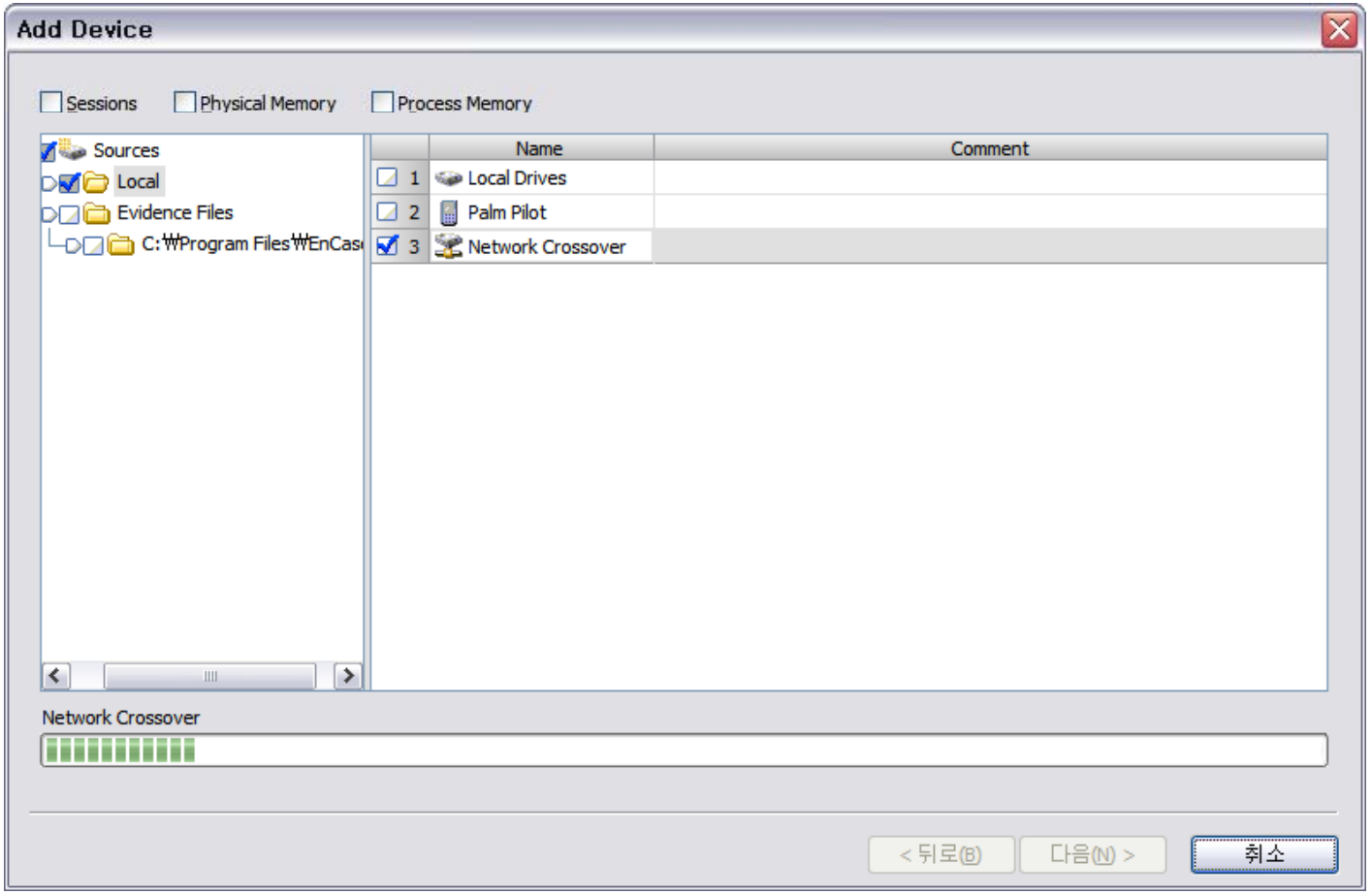
   ➔ 접속 대기 상태
3. 호스트 시스템에서 EnCase for Windows 수행을 위해 방화벽 설정

   ➔ EnCase.exe에 대해 네트워크 접속을 허락
4. EnCase는 자동적으로 네트워크 설정을 수행하지만 문제가 발생할 경우 다음과 같이 설정
   - IP : 10.0.0.50
   - Subnet Mask : 255.255.255.0
   - DNS, WINS는 제거

Network Acquisitions

Steps for Network Acquisition – Setting Up Acquisition

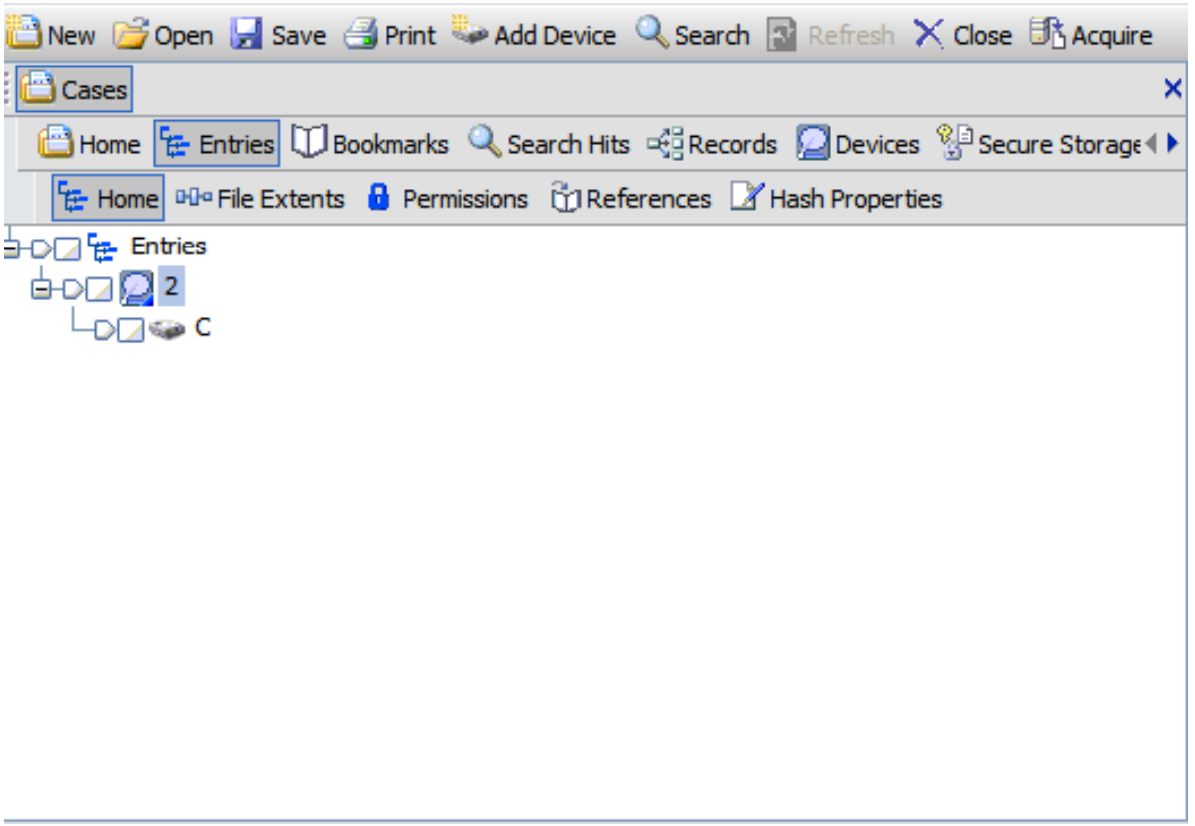
5. New ➔ Add Device



Network Acquisitions

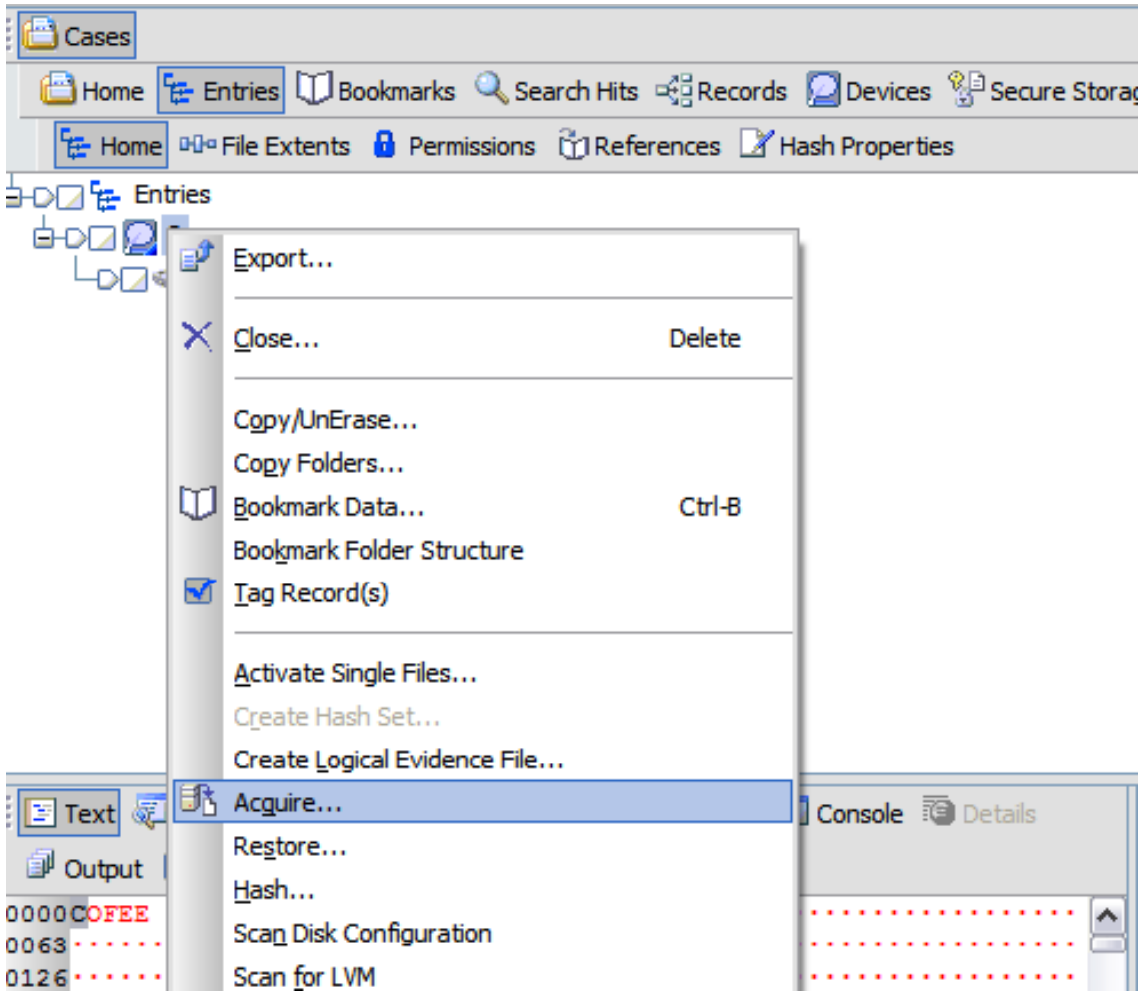
Steps for Network Acquisition – Setting Up Acquisition

6. Network Crossover로 연결된 목록에서 대상 시스템 선택 후 로컬 드라이브처럼 사용 가능

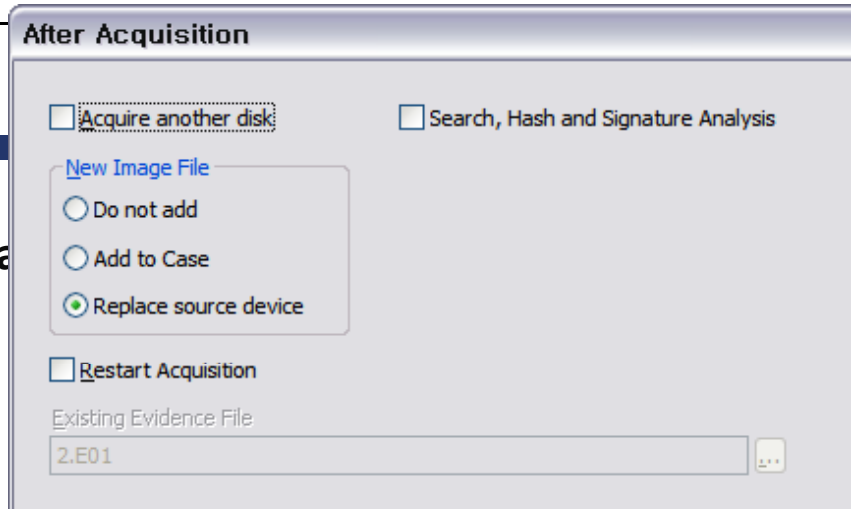


Network Acquisitions

- **Steps for Network Acquisition – Specifying Data Acquisition Options**



Network Acquisitions

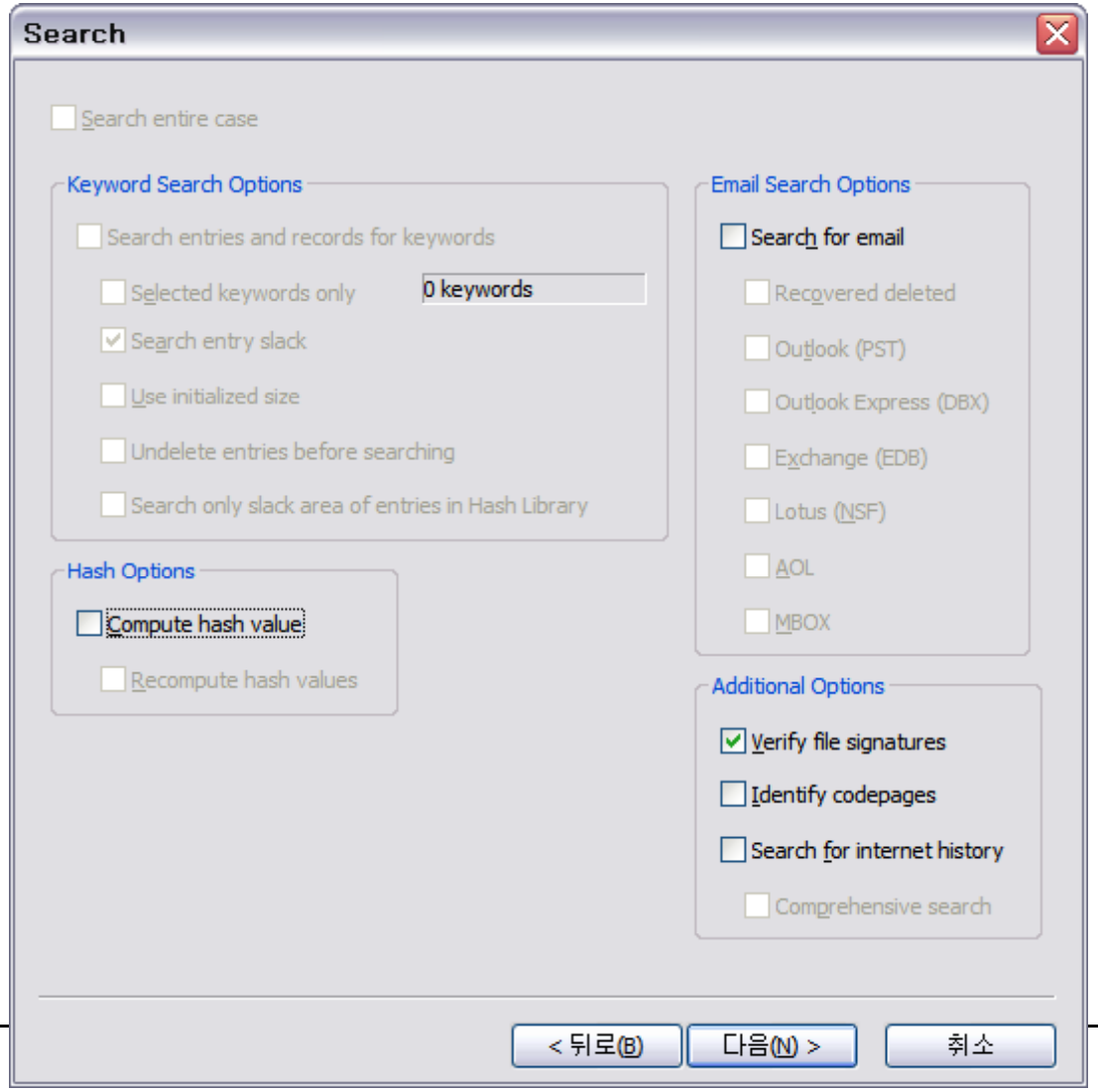


Steps for Network Acquisition – Specifying Data

- ✓ Acquire another disk : 하나 이상의 디스크 획득
- ✓ New Image File
  - Do not add : 획득 이후에 증거 파일을 Case에 추가하지 않음
  - Add to Case : 획득 이후에 수집한 증거 파일을 Case에 추가
  - Replace source device : 획득 이후에 수집한 장치와 증거 파일을 교체
- ✓ Search, Hash and Signature Analysis : 획득한 증거 파일에서 분석
- ✓ Restart Acquisition : 이전 획득하던 파일에 이어서 수집

Network Acquisitions

- **Steps for Network Acquisition – Specifying Data Acquisition Options**



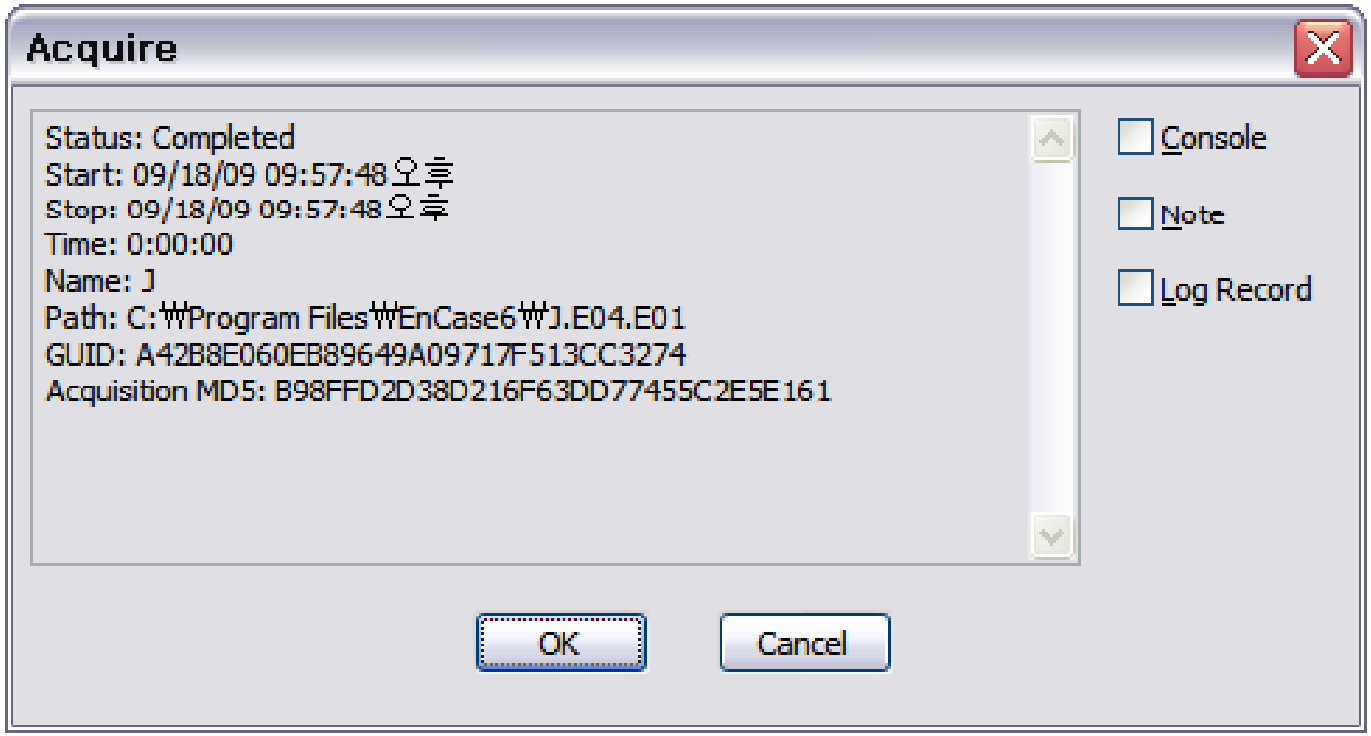
Network Acquisitions

Steps for Network Acquisition – Specifying Data Acquisition Options

- ✓ File Segment Size (default 640 MB)
- ✓ Compression
- ✓ Start/Stop Sector
- ✓ Password
- ✓ Block Size
- ✓ Error granularity
- ✓ Acquisition MD5 & SHA1
- ✓ Quick Reacquisition
- ✓ Read Ahead (only using EE and FIM)
- ✓ Output Path
- ✓ Alternate Path

Network Acquisitions

- **Steps for Network Acquisition – Specifying Data Acquisition Options**



Acquiring Digital Evidence

- *Creating EnCase DOS boot disks*
- *Booting computers using EnCase DOS boot disks*
- *Drive-to-drive Acquisitions*
- *Network Acquisitions*
- *FastBloc Acquisitions*
- *FastBloc SE Acquisitions*
- *LinEn Acquisitions*
- *Enterprise and FIM Acquisitions*

FastBloc Acquisitions

Available FastBloc Models

- ✓ *FastBloc* : GuidanceSoftware에서 개발한 독립된 하드웨어 Write-blocker
- ✓ *FastBloc Classic* : SCSI interface 지원, 현재 구입 불가능
- ✓ *FastBloc LE (Lab Edition)* : IDE interface 지원 (DOS or Windows)
- ✓ *FastBloc FE (Field Edition)* : USB-2 or 1394a (FireWire) 지원

FastBloc Acquisitions

Steps for FastBloc Acquisition

1. FastBloc을 USB, 1394a 등의 인터페이스를 활용하여 컴퓨터에 연결
2. 대상 드라이브(Parallel ATA)를 연결
3. FastBloc과 드라이브 간의 DC 전원 연결
4. FastBloc과 드라이브 간에 데이터 케이블 연결
5. FastBloc에 전원을 공급 (Plug and Play)
6. Device Manager를 통해 연결 드라이브 확인
7. EnCase for Windows 실행
8. Add Device ➔ Preview ➔ Acquire

Acquiring Digital Evidence

- *Creating EnCase DOS boot disks*
- *Booting computers using EnCase DOS boot disks*
- *Drive-to-drive Acquisitions*
- *Network Acquisitions*
- *FastBloc Acquisitions*
- *FastBloc SE Acquisitions*
- *LinEn Acquisitions*
- *Enterprise and FIM Acquisitions*

Acquiring Digital Evidence

- *Creating EnCase DOS boot disks*
- *Booting computers using EnCase DOS boot disks*
- *Drive-to-drive Acquisitions*
- *Network Acquisitions*
- *FastBloc Acquisitions*
- *FastBloc SE Acquisitions*
- *LinEn Acquisitions*
- *Enterprise and FIM Acquisitions*

LinEn Acquisitions

LinEn

- ✓ EnCase 6 부터 EnCase for DOS(EN.EXE)를 더 이상 지원하지 않음
- ✓ 대신에 LinEn을 지원
  - DOS : 16-bit OS
  - Linux : 32-bit OS

LinEn Acquisitions

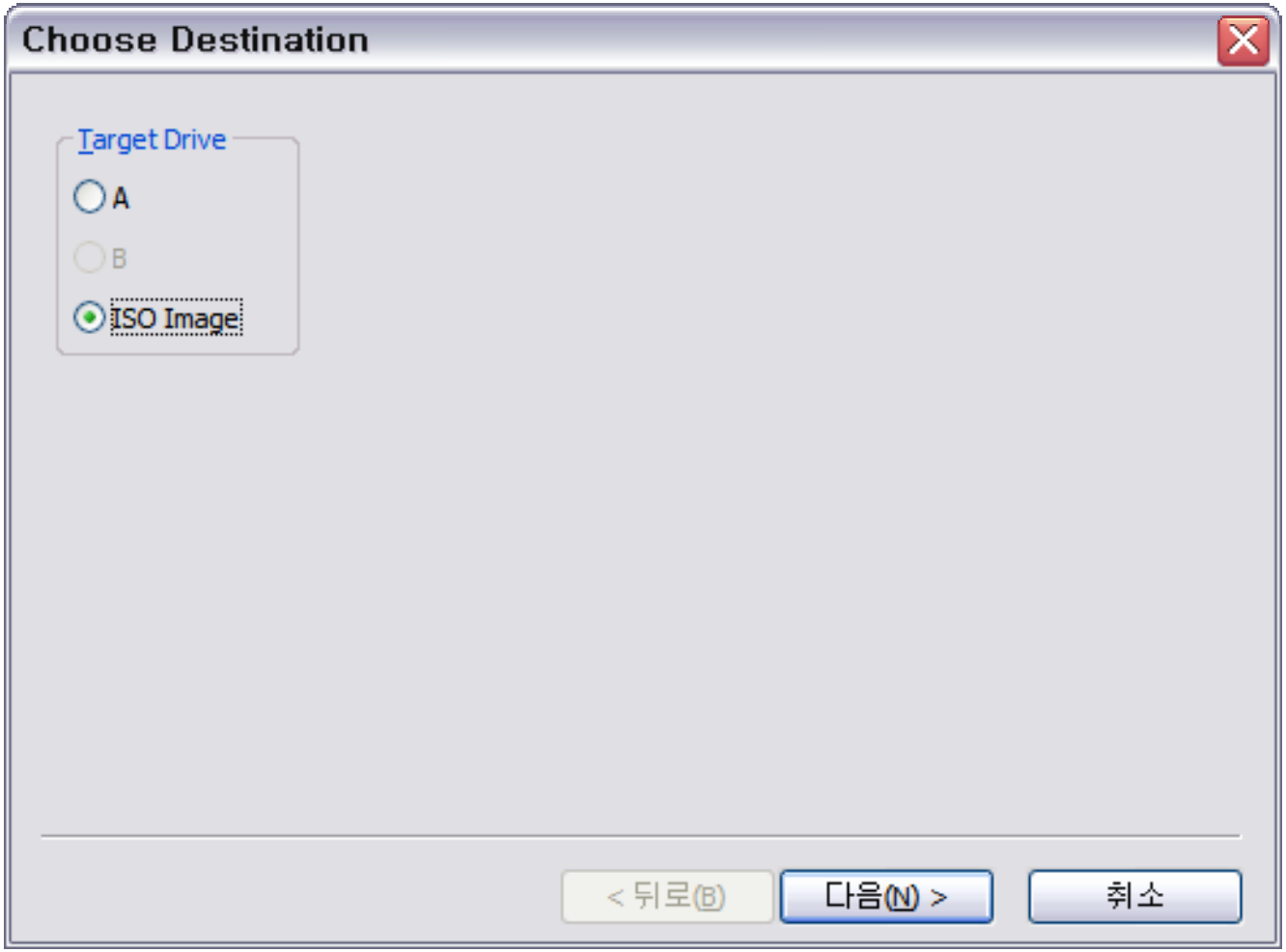
Mounting a File System as Read-Only

- ✓ Linux의 경우 Read-Only 마운트를 통해 운영체제로부터 쓰기 방지
- ✓ Read-Only 마운트를 위해서는 리눅스의 자동 마운트 기능을 제거
- ✓ 대부분 직접 Read-Only 마운트보다 리눅스 배폰판에서 지원하는 부트 디스크 이용

  ➔ Helix, Knoppix, SPADA, 등
- ✓ 최근 Helix Pro 버전에서는 기본적으로 LinEn 지원

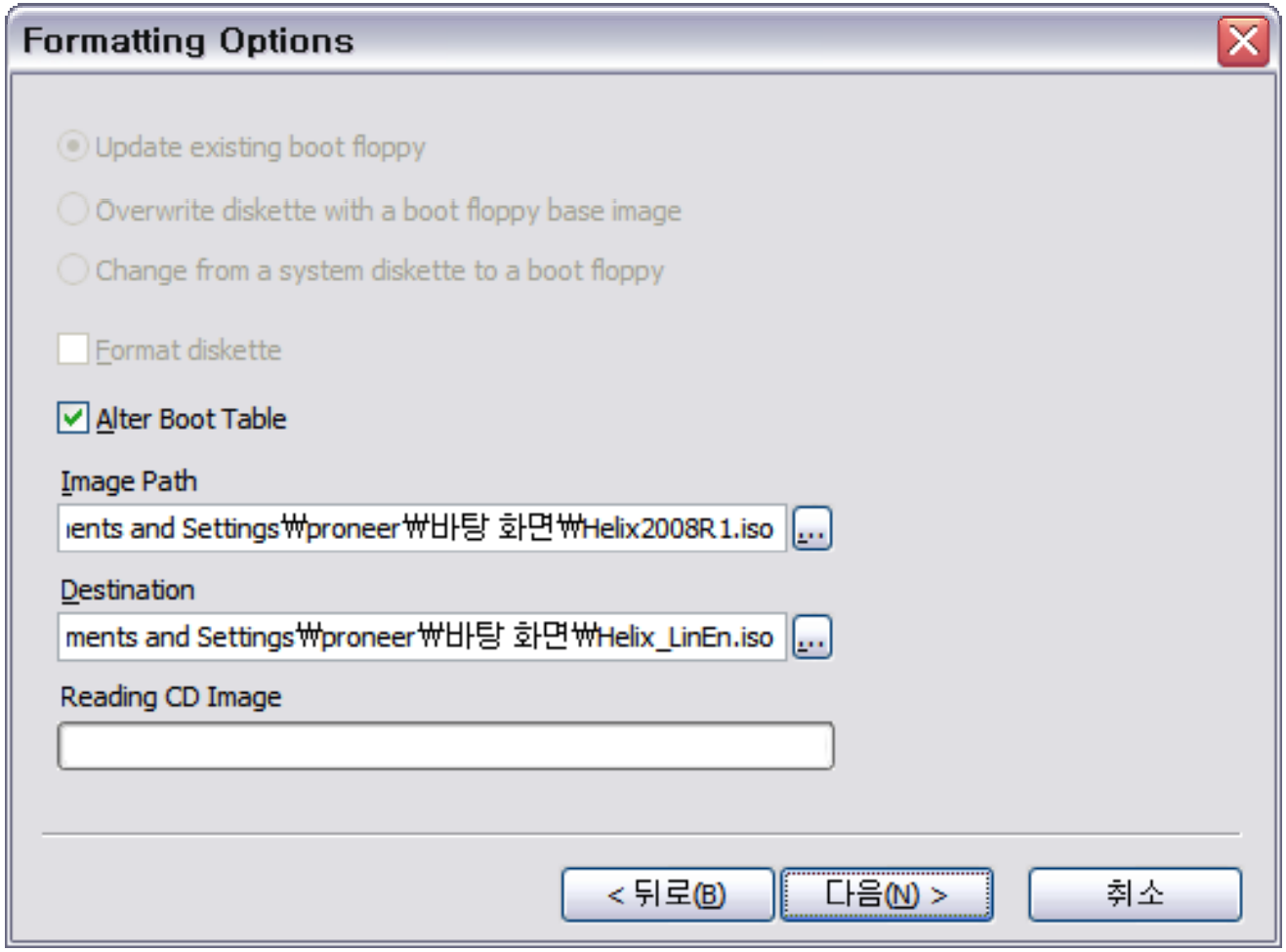
LinEn Acquisitions

- **Updating a Linux Boot CD with the Lastest Version of LinEn**



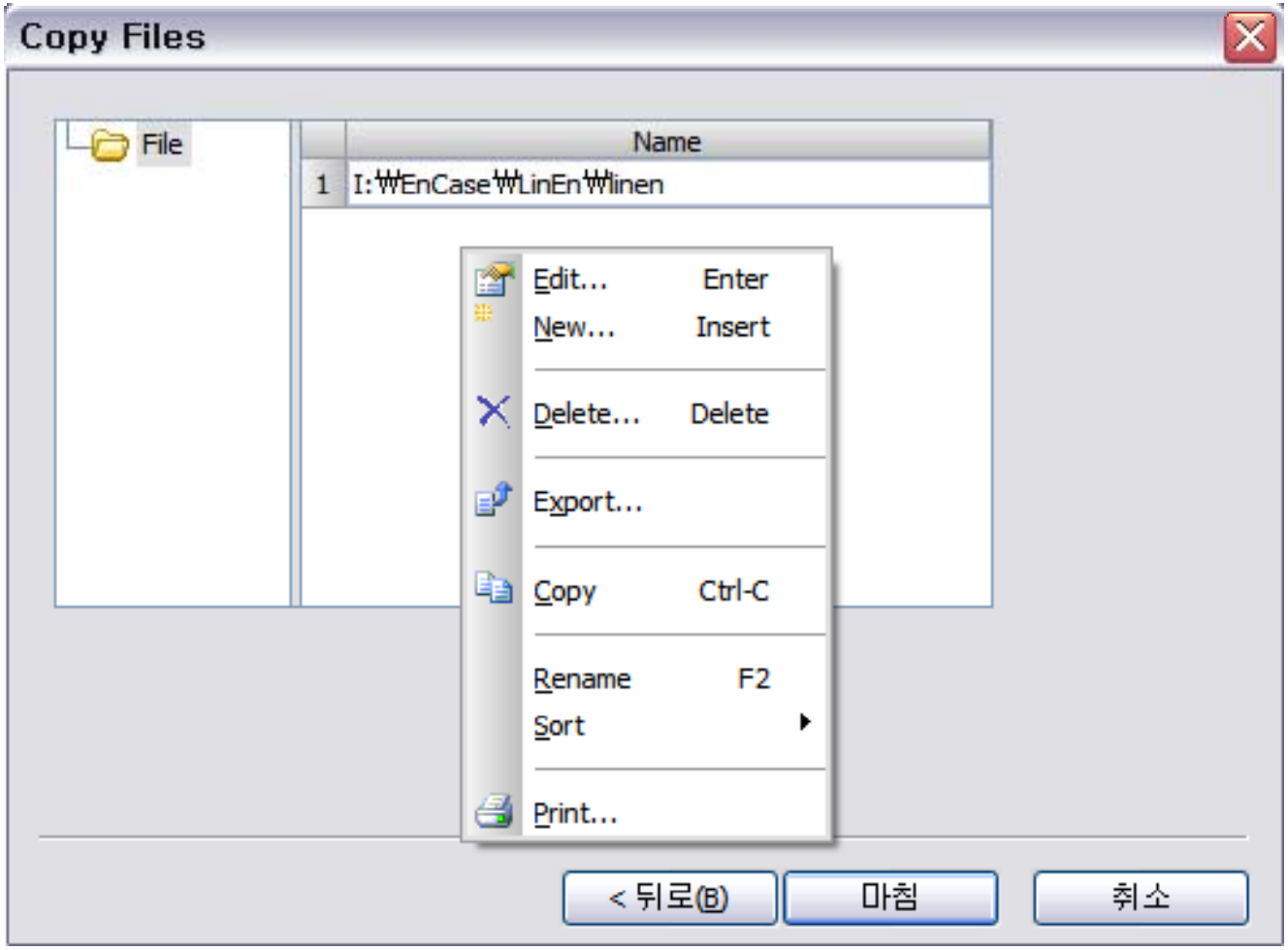
LinEn Acquisitions

- **Updating a Linux Boot CD with the Lastest Version of LinEn**



LinEn Acquisitions

- **Updating a Linux Boot CD with the Lastest Version of LinEn**



LinEn Acquisitions

Running LinEn

- ✓ root 권한으로 실행해야 하며 제한된 리소스 사용을 위해 콘솔 모드 사용 권장

  ➔ 부팅 runlevel 변경

- ✓ LinEn 실행 전 드라이브 확인
  - hda : Primary Master
  - hdb : Primary Slave
  - hdc : Secondary Master
  - hdd : Secondary Slave
  - hdc1 : Secondary Master First Partition
  - hda3 : Primary Master Third Partition

LinEn Acquisitions

Running LinEn

- ✓ 획득 이미지의 오염(cross-contamination)을 방지하기 위해 완전삭제 후 획득 권장
- ✓ FAT32 볼륨에 획득 파일(이미지 파일)을 저장하는 것을 권장
  - 왜? NTFS, EXT2/3 ?
- ✓ LinEn 실행 준비 과정
  1. autofs(automounting of file systems) 기능 해제
  2. 콘솔모드로 리눅스 부팅
  3. 대상 드라이브 연결
  4. 저장할 드라이브(FAT32) 연결
  5. LinEn 실행

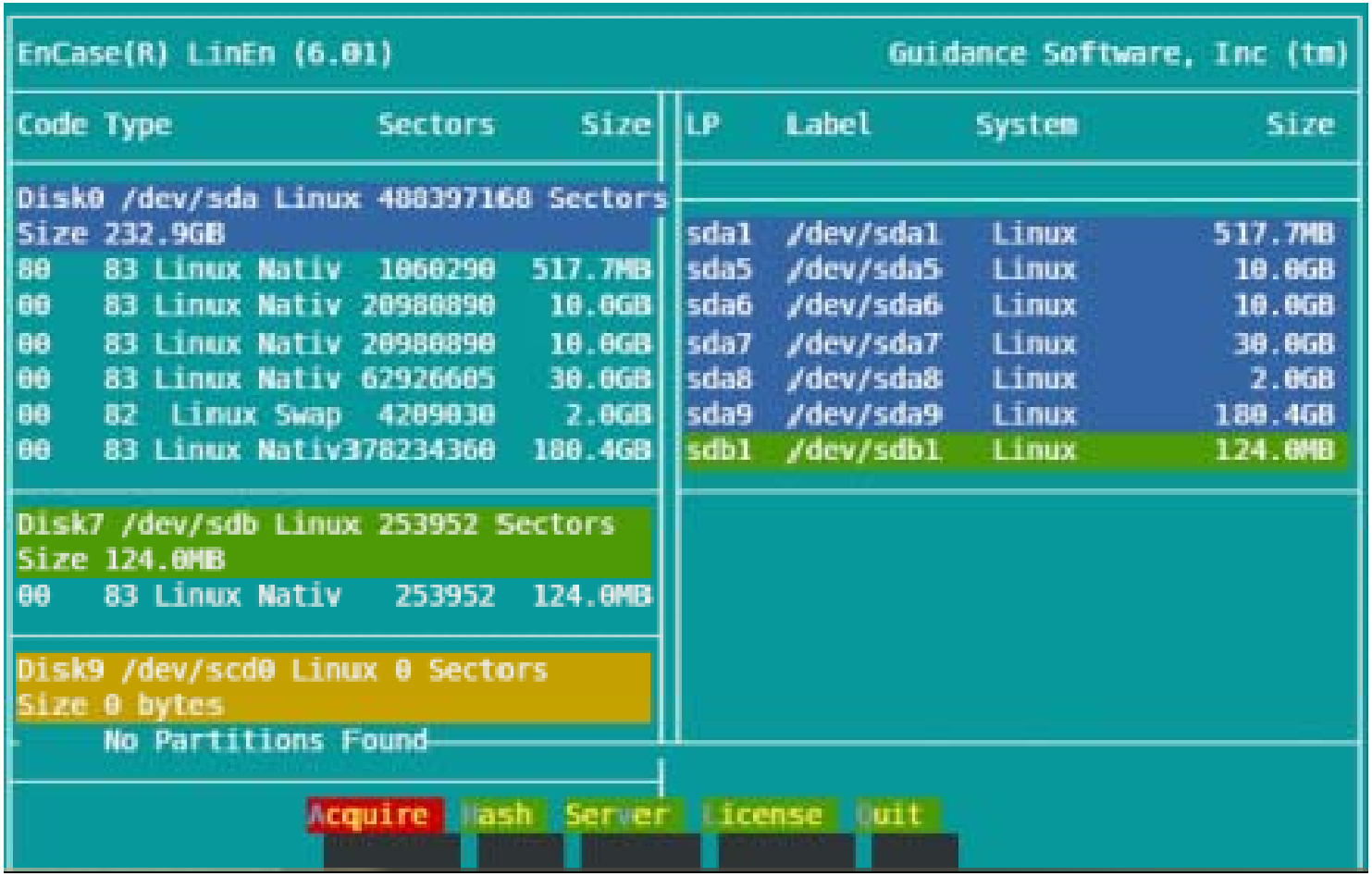
LinEn Acquisitions

Steps for LinEn Acquisition

1. 리눅스를 콘솔 모드로 부팅 한 후 root로 로그인
2. 마운트된 파일시스템 확인 (mount)
3. 마운트 가능한 드라이브 확인 (fdisk –l)
4. 드라이브 마운트 (mount /dev/hda1 /mnt/fat32)
5. 증거 파일(이미징 파일)을 저장할 디렉터리 생성 (mkdir /mnt/fat32/evidence)
6. linen 파일이 있는 폴더로 이동 (cd /mnt/fat32/encase)
7. linen 실행 (./linen)

LinEn Acquisitions

- **Steps for LinEn Acquisition**



LinEn Acquisitions

Steps for LinEn Acquisition

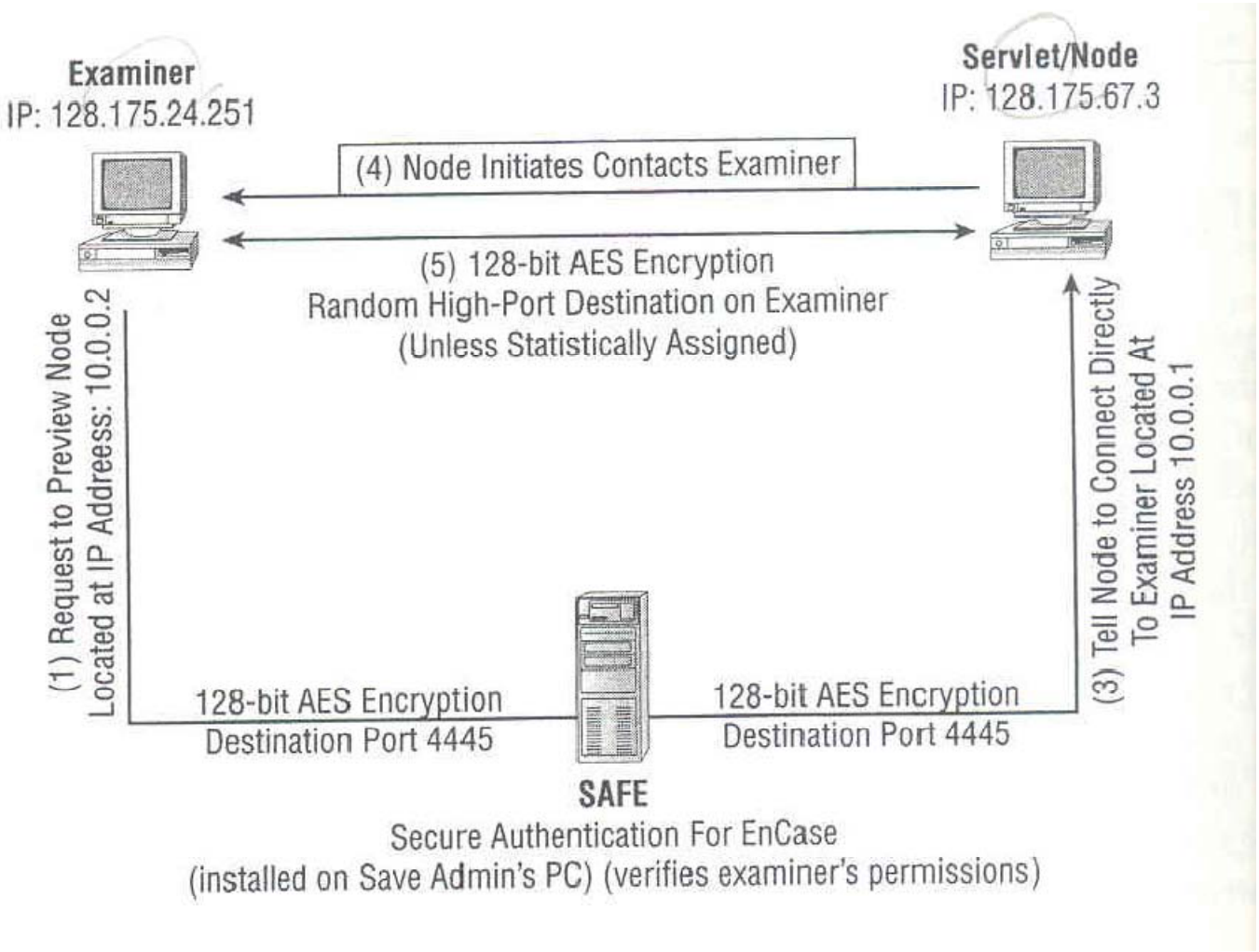
8. Hash 메뉴를 이용해 Hash 계산 가능 (물리, 논리 드라이브)
9. "A" 키를 누르면 Acquire 수행
10. EnCase for DOS의 수행과 같음
11. 추가적으로 Network cable을 통한 수집 지원
    - ifconfig eth0 10.0.0.1 netmask 255.0.0.0
    - ifconfig eth0
    - LinEn 재시작, EnCase for Windows 재시작
    - Network Acquisition 과 같은 방법으로 수집 가능

Acquiring Digital Evidence

- *Creating EnCase DOS boot disks*
- *Booting computers using EnCase DOS boot disks*
- *Drive-to-drive Acquisitions*
- *Network Acquisitions*
- *FastBloc Acquisitions*
- *FastBloc SE Acquisitions*
- *LinEn Acquisitions*
- *Enterprise and FIM Acquisitions*

Enterprise and FIM Acquisitions

- **EE and FIM**



Homework

HW #1

- ✓ LinEn을 활용하여 자신의 USB에 대한 증거 파일 획득
  - 1 USB : Target USB
  - 2 USB : Storage USB

- ✓ 획득 절차와 획득한 증거 파일에 대한 정보(시간, 크기, Hash 값 등)
- ✓ HWP, DOC 2장 이내로 작성하여 PDF 변환 후 제출 ➔ 다음 주 목요일 까지

Homework

HW #2

- ✓ LinEn을 활용하여 Network Acquisition 획득
  - Target : LinEn 실행되고 있는 시스템의 USB 메모리

- ✓ 획득 절차와 획득한 증거 파일에 대한 정보(시간, 크기, Hash 값 등)
- ✓ HWP, DOC 2장 이내로 작성하여 PDF 변환 후 제출 ➔ 다음 주 목요일 까지

Homework

HW #3

- ✓ FastBloc FE를 통한 증거 파일 획득
  - 메모리카드, 노트북 HDD, IDE, SATA 등의 드라이브 가능

- ✓ 획득 절차와 획득한 증거 파일에 대한 정보(시간, 크기, Hash 값 등)
- ✓ HWP, DOC 2장 이내로 작성하여 PDF 변환 후 제출 ➔ 다음 주 목요일 까지

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)**
  - EnCase Evidence File Format
  - CRC and MD5
  - Evidence File Components and Function
  - Evidence File Verification
  - Hashing Disks and Volumes
  - EnCase Case Files
  - EnCase Backup File (.cbak)
  - EnCase Comfiguration Files
  - EnCase Record Cache Folder
  - EnCase Layout
  - Tree Pane
  - Table Pane
  - View Pane

Question and Answer