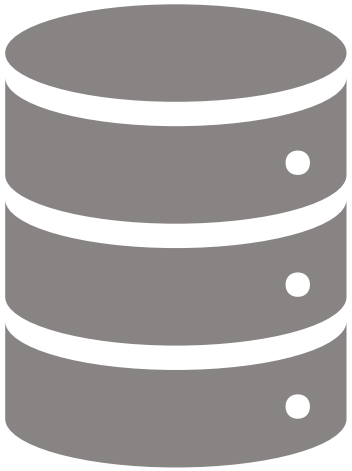
주식회사 제트코
JETCO Technology,Inc.

서버 포렌식의 최신 기술 동향

- RAID 자동 빌드 및 가상 마운트 -

Server Forensic

- Server



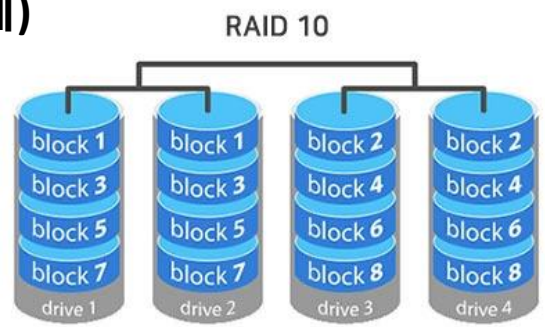
- 애플리케이션 서버
- 웹 서버
- 메일 서버
- 데이터 베이스 서버
- ETC …

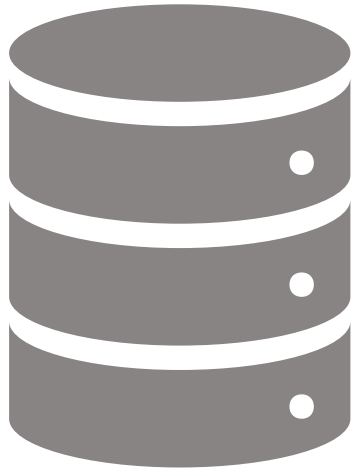
Server Forensic

▪ Server

RAID 구성

예)

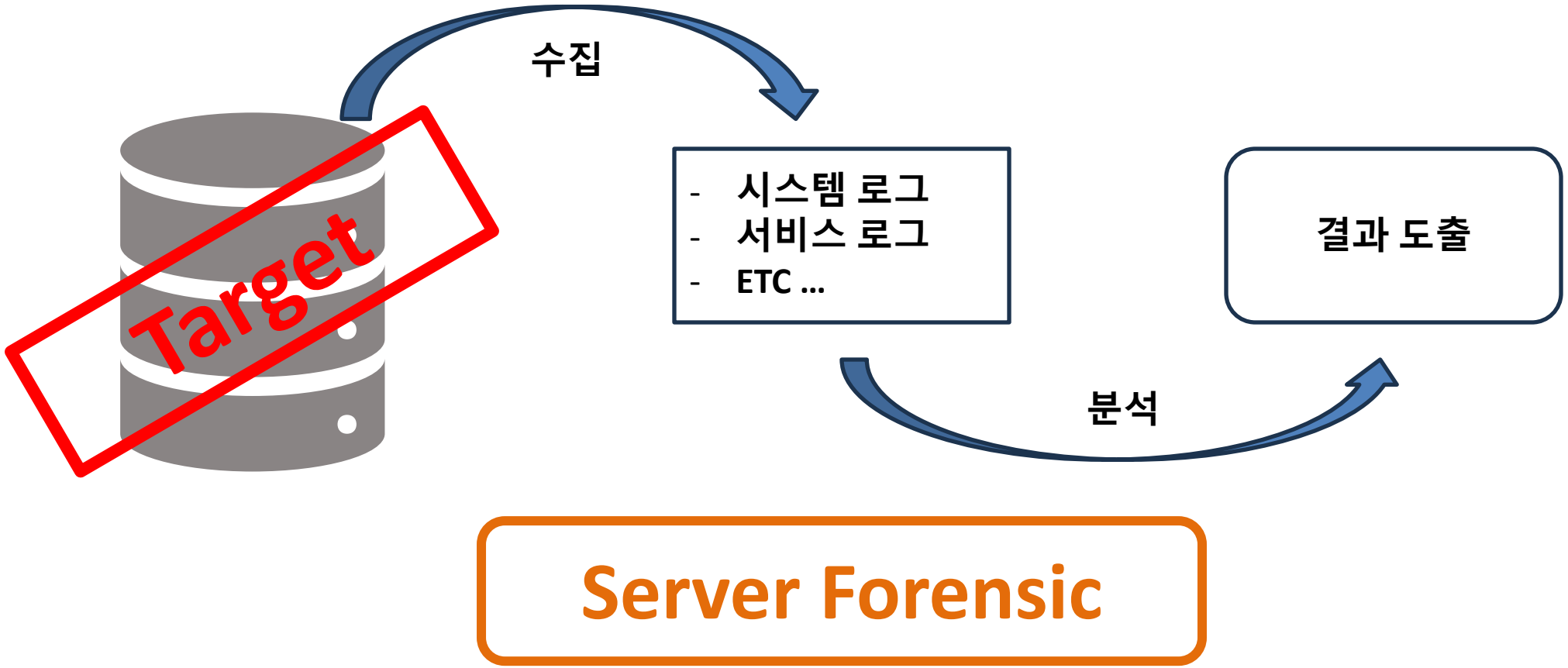




For
- 방대한 양의 데이터 수용
- 데이터의 백업

Server Forensic

▪ Server



Server Forensic 방해 요인

다양한 스토리지 기술

- LVM : 리눅스의 논리적인 볼륨 관리 시스템
- 애플 코어 스토리지 : macOS의 논리적인 볼륨 관리 시스템
- 타임 머신 백업 : macOS에 기본 탑재된
- ETC …

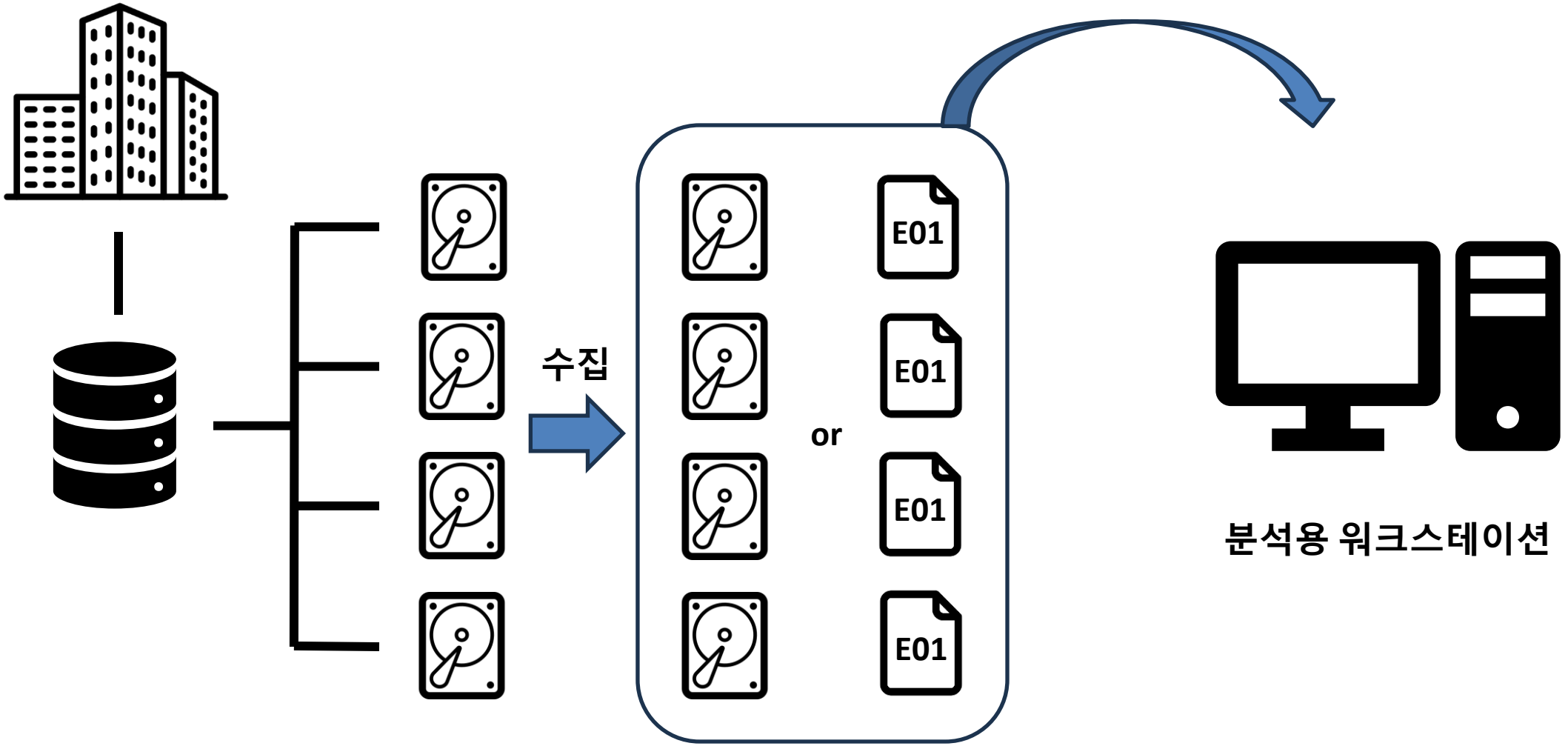
다양한 수준의 RAID

- RAID 0 / 1 / 10 / 3 / 5 / 50 / 6 / 60 / 1E / 5EE / SPANNED …

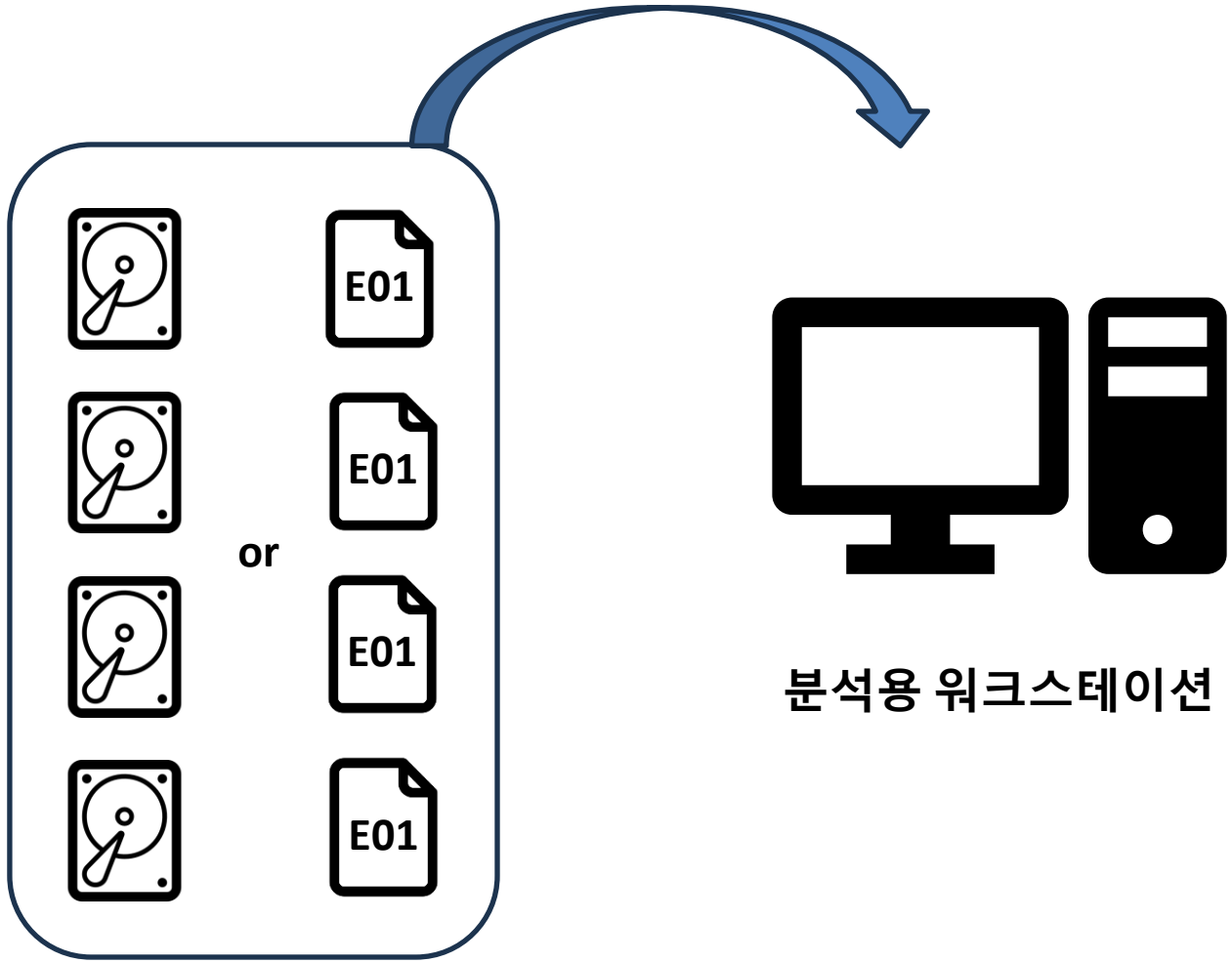
다양한 파일 시스템

- Windows : FAT / FAT32 / exFAT / NTFS / ReFS / FeFS3
- macOS : HFS+ / APFS
- Linux : Ext2 / Ext3 / Ext4 / ReiserFS / XFS /JFS
- FreeBSD : UFS / UFS2
- Sun Solaris : ZFS

Server Forensic RAID

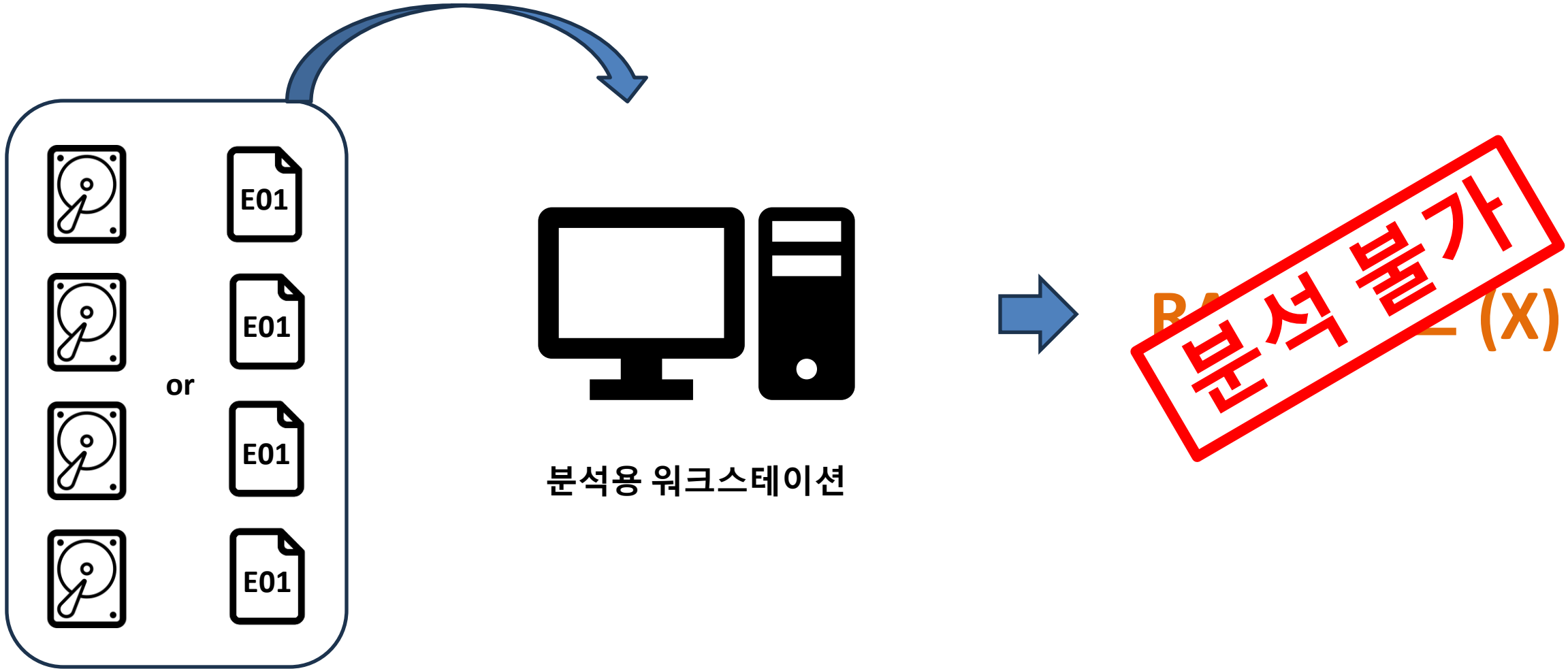


Server Forensic RAID



RAID 빌드 (X)

Server Forensic RAID



Server Forensic 자동 RAID 빌드 및 마운트

자동 RAID 빌드

마운트

지원되는 RAID 수준

- RAID 0 / 1 / 10 / 3 / 5 / 50 / 6 / 60 / 1E / 5EE / SPANNED

지원되는 파일 시스템

- Windows : FAT / FAT32 / exFAT / NTFS / ReFS / FeFS3
- macOS : HFS+ / APFS
- Linux : Ext2 / Ext3 / Ext4 / ReiserFS / XFS /JFS
- FreeBSD : UFS / UFS2
- Sun Solaris : ZFS

시연-1

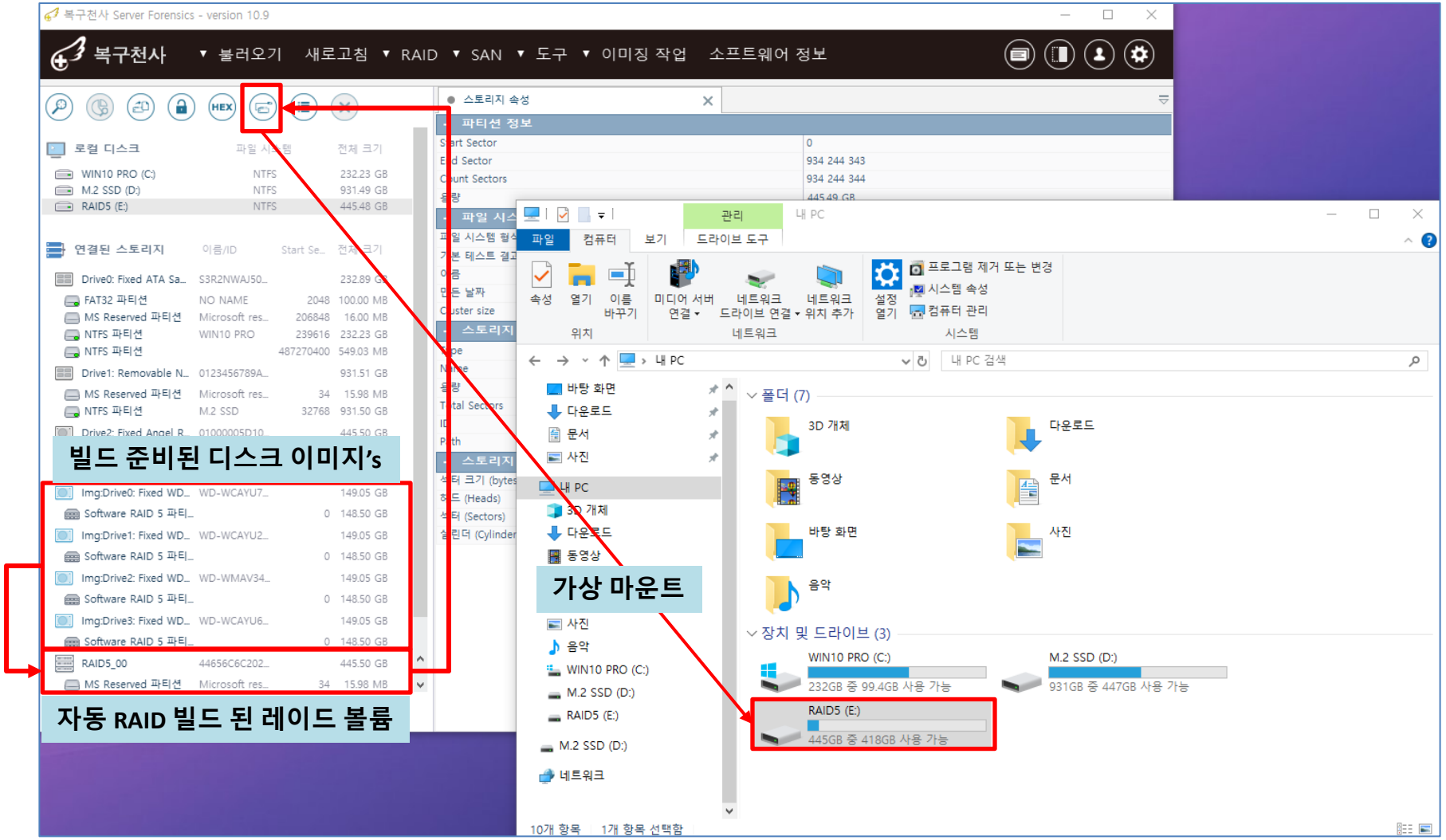
Server Forensic 자동 RAID 빌드 및 마운트

지원되는 메타데이터 형식

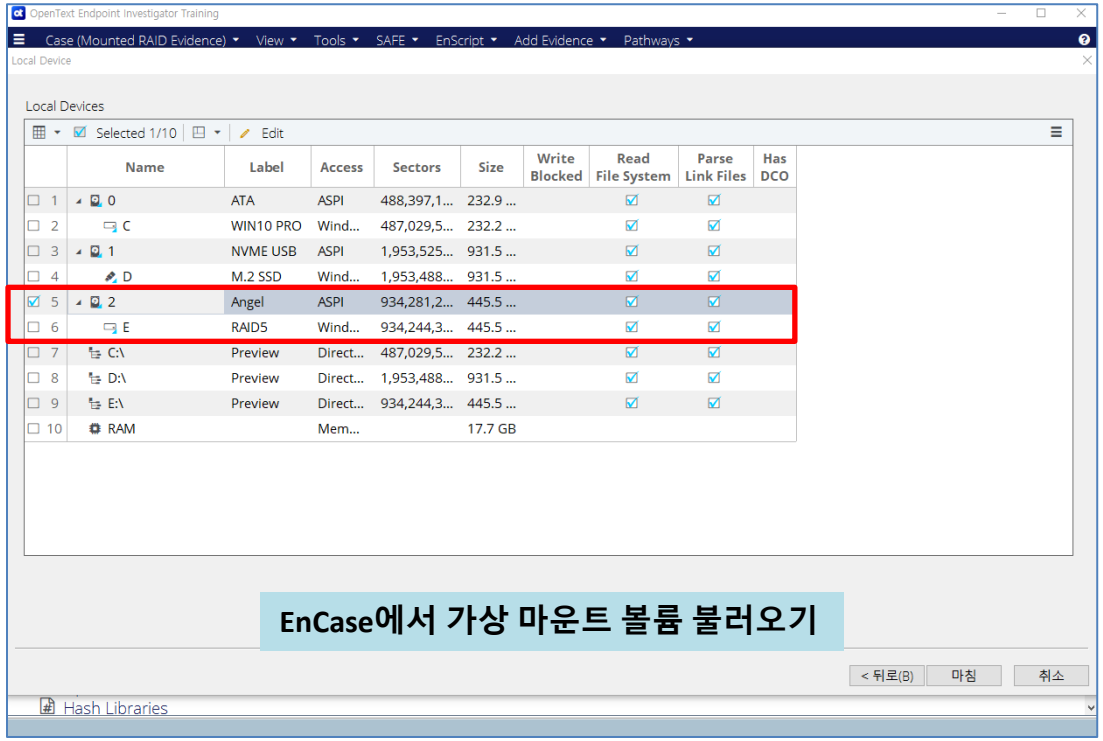
- Synology RAID(클랙식, madadm)
- Apple RAID
- LVM2
- Windows LDM
- Apple Fusion
- Jmicron JMS561
- BSD BIO
- Intel Matrix
- DDF
- Silicon Image
- JMicron
- 3ware
- Areca
- HP SmartArray
- DDF2
- Synology(RAID-F1)
- AIX LVM
- HP / UX LVM
- Dell EqualLogic
- CAPI
- NetAPP

시연-1 Continue...

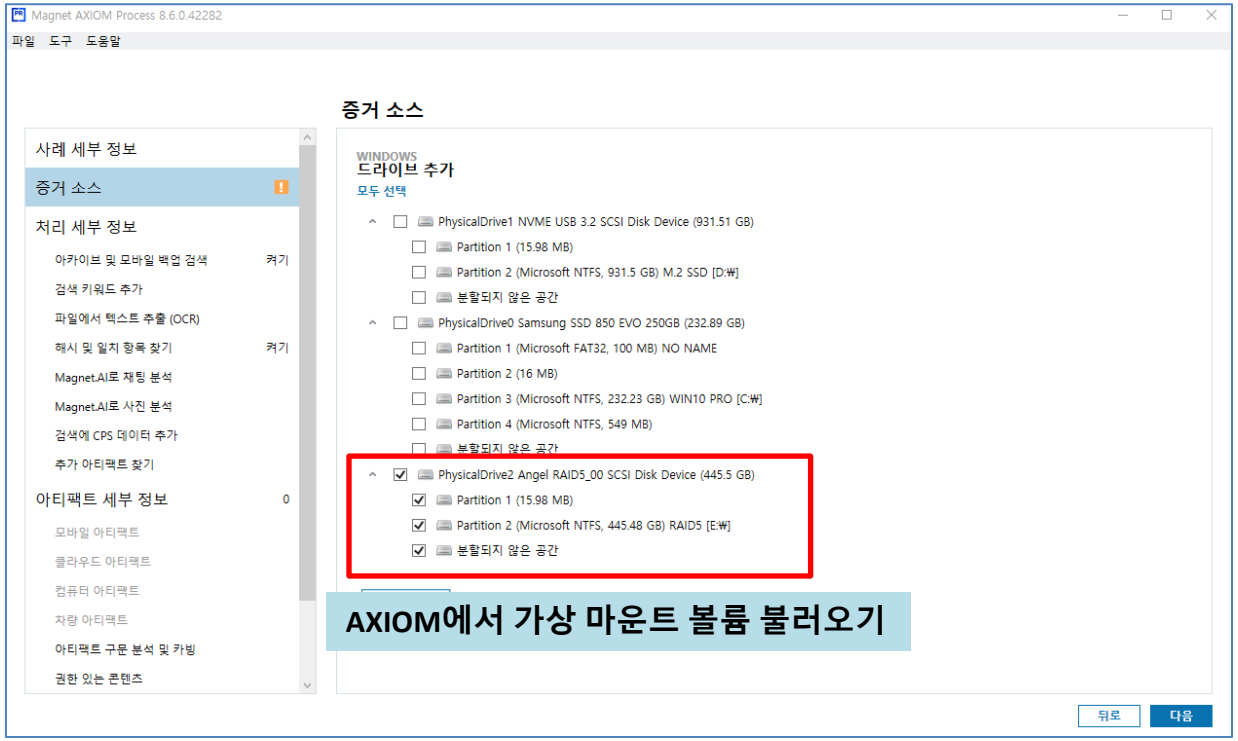
Server Forensic 자동 RAID 빌드 및 마운트



Server Forensic 자동 RAID 빌드 및 마운트

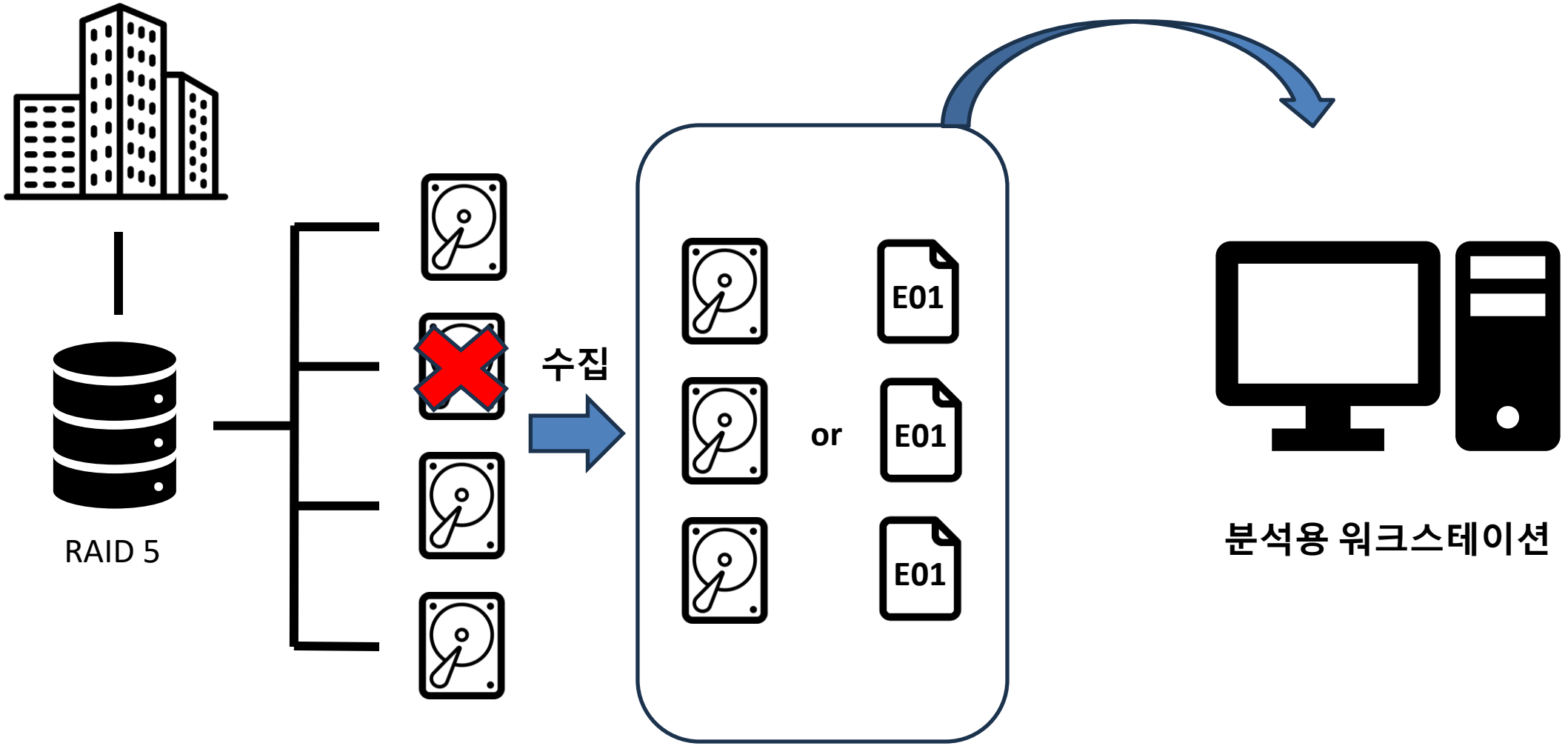


EnCase에서 가상 마운트 볼륨 불러오기

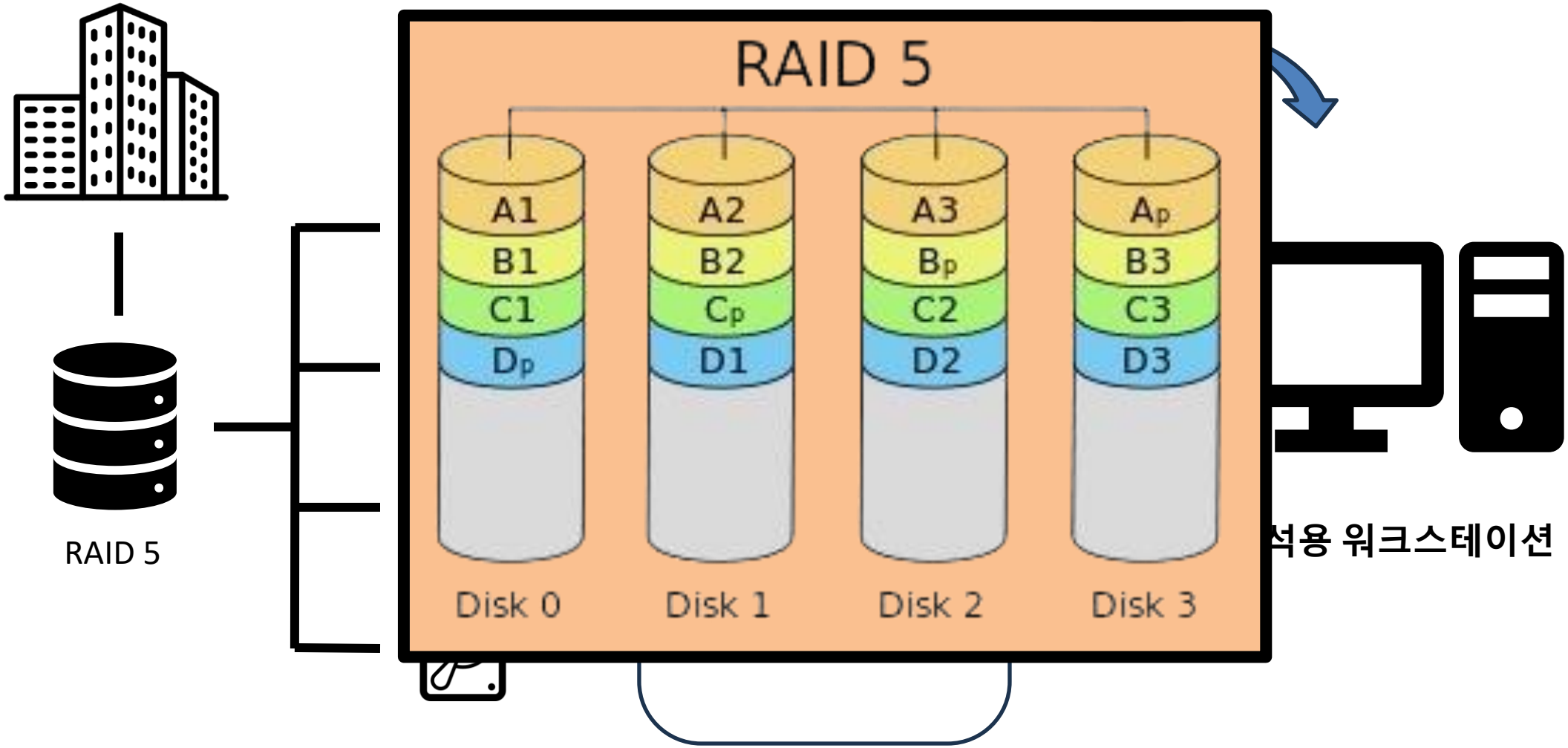


AXIOM에서 가상 마운트 볼륨 불러오기

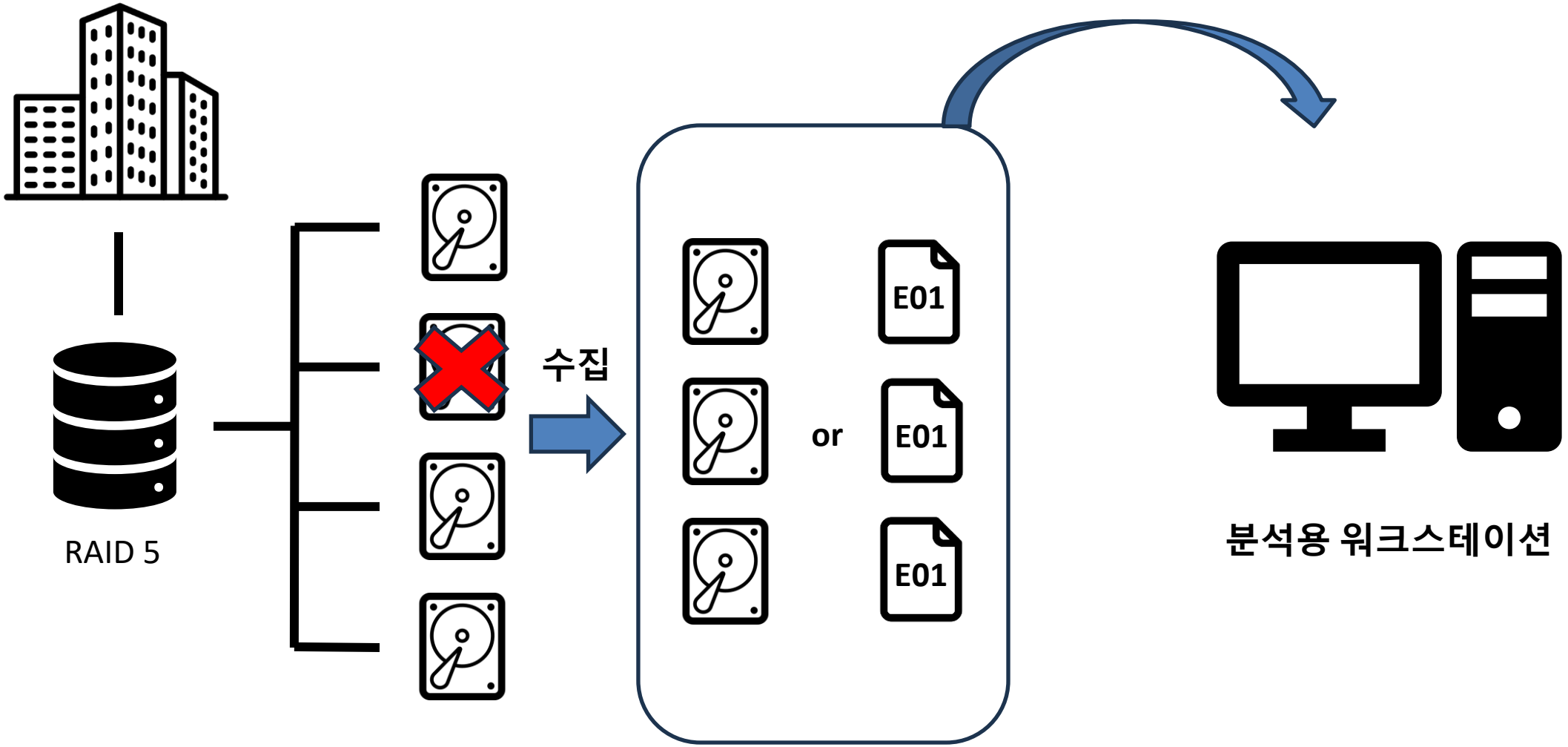
Server Forensic 자동 RAID 빌드 및 마운트



Server Forensic 자동 RAID 빌드 및 마운트

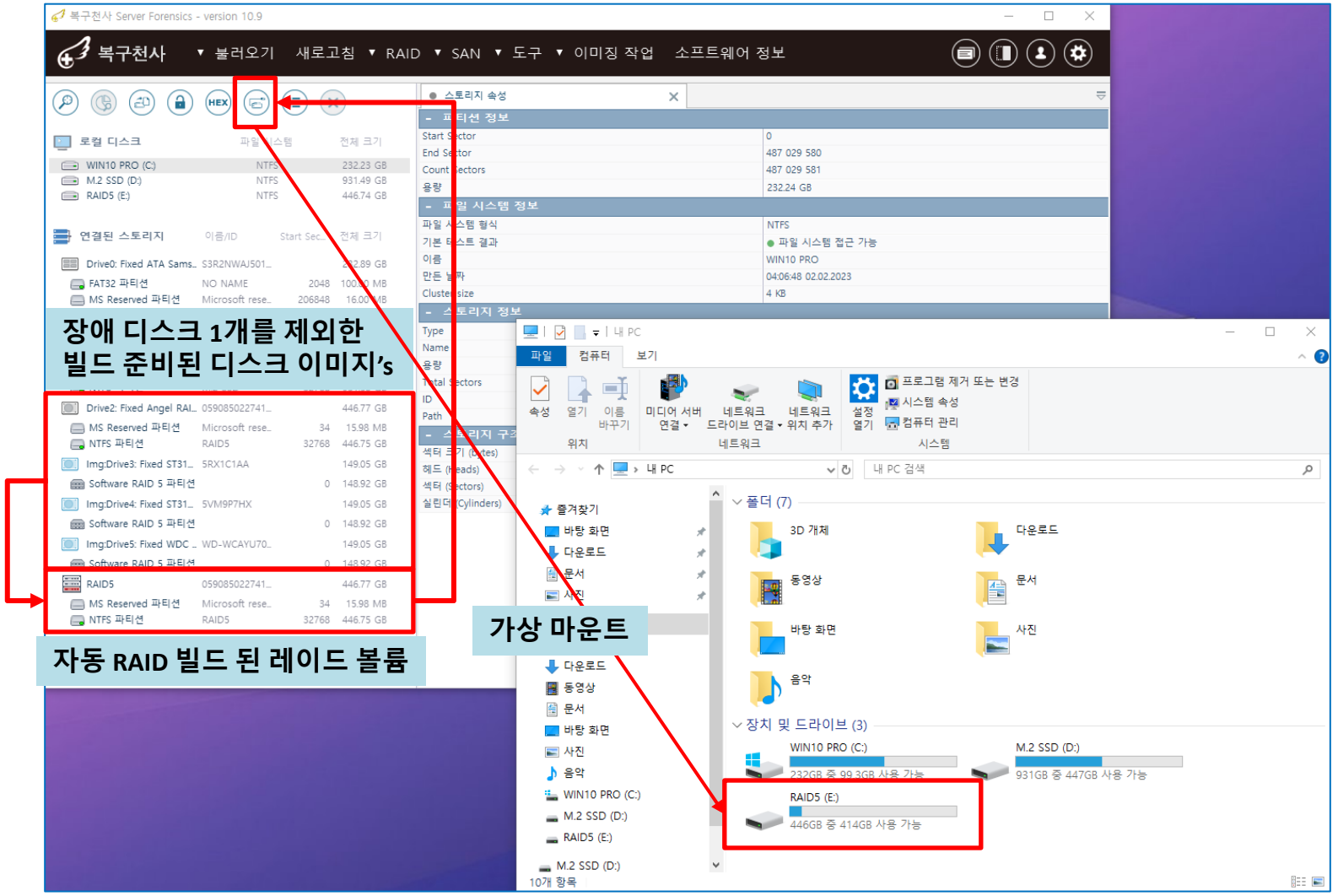


Server Forensic 자동 RAID 빌드 및 마운트

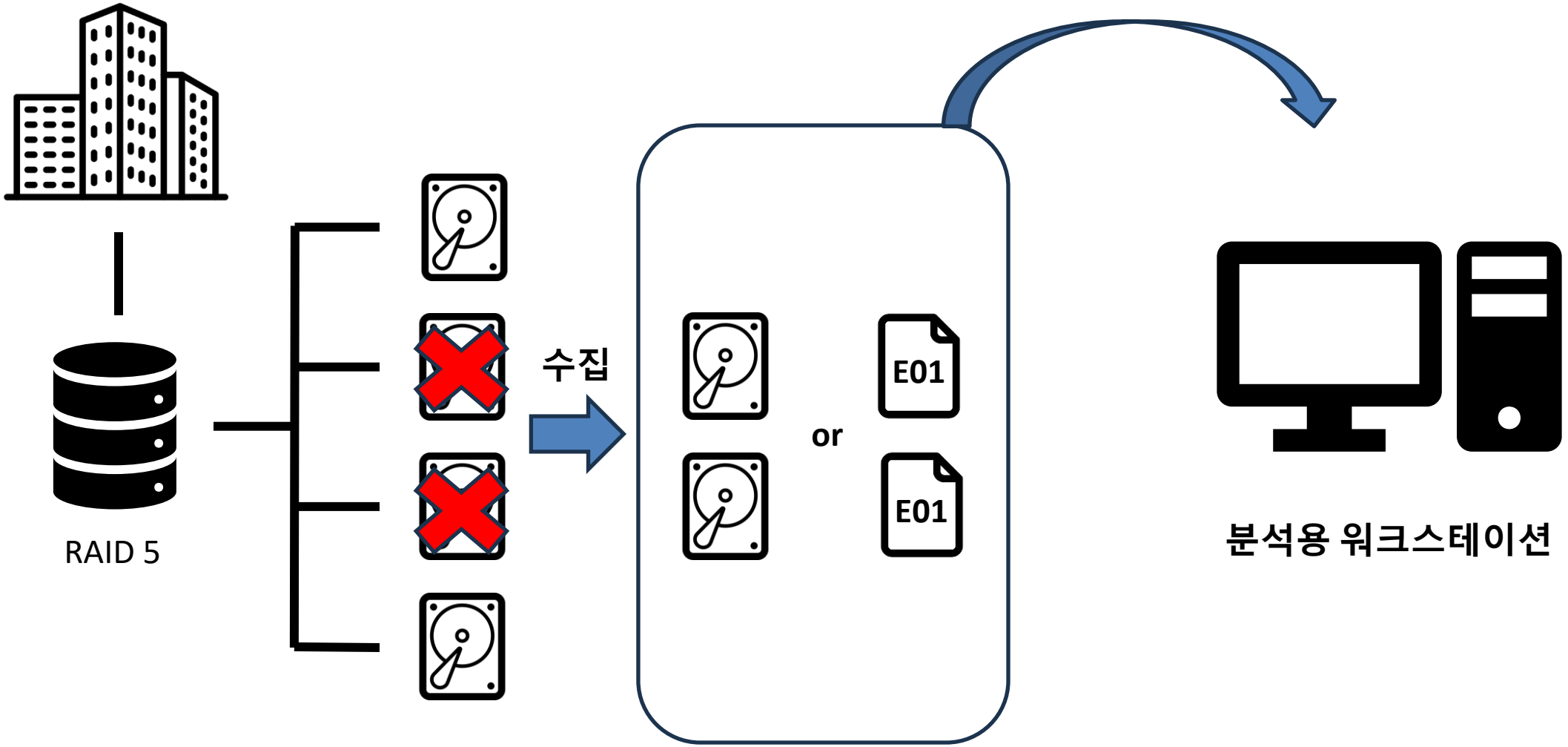


시연-2

Server Forensic 자동 RAID 빌드 및 마운트

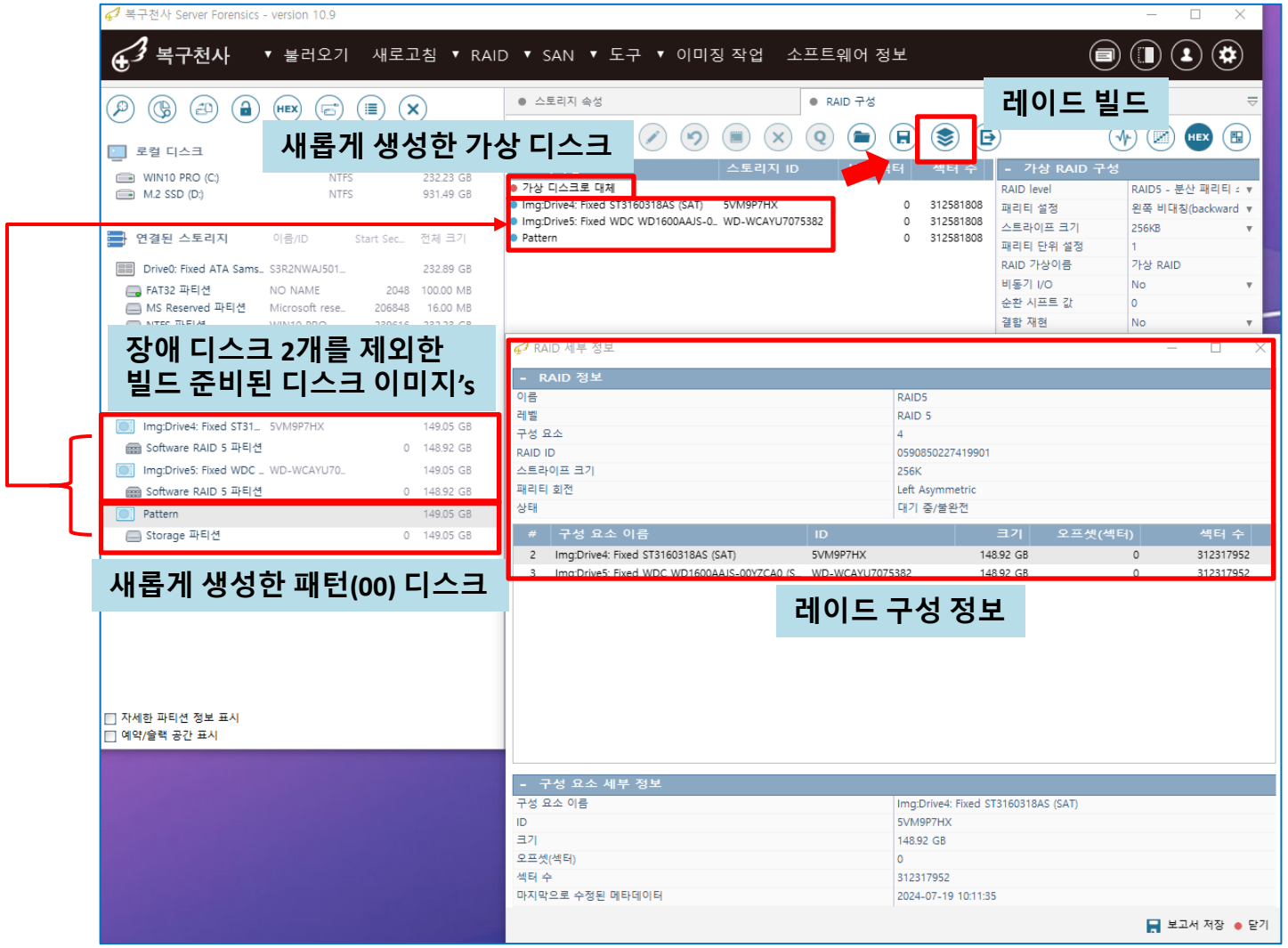


Server Forensic 자동 RAID 빌드 및 마운트



시연-3

Server Forensic 자동 RAID 빌드 및 마운트



Server Forensic SAN Storage

NAS

- SAN 대비 저렴한 가격
- NAS 장치 하나만으로 운용 가능
- 쉬운 운용 및 관리
- 이더넷을 통해 바로 연결, 공유 스토리지를 네트워크 마운트 볼륨으로 제공

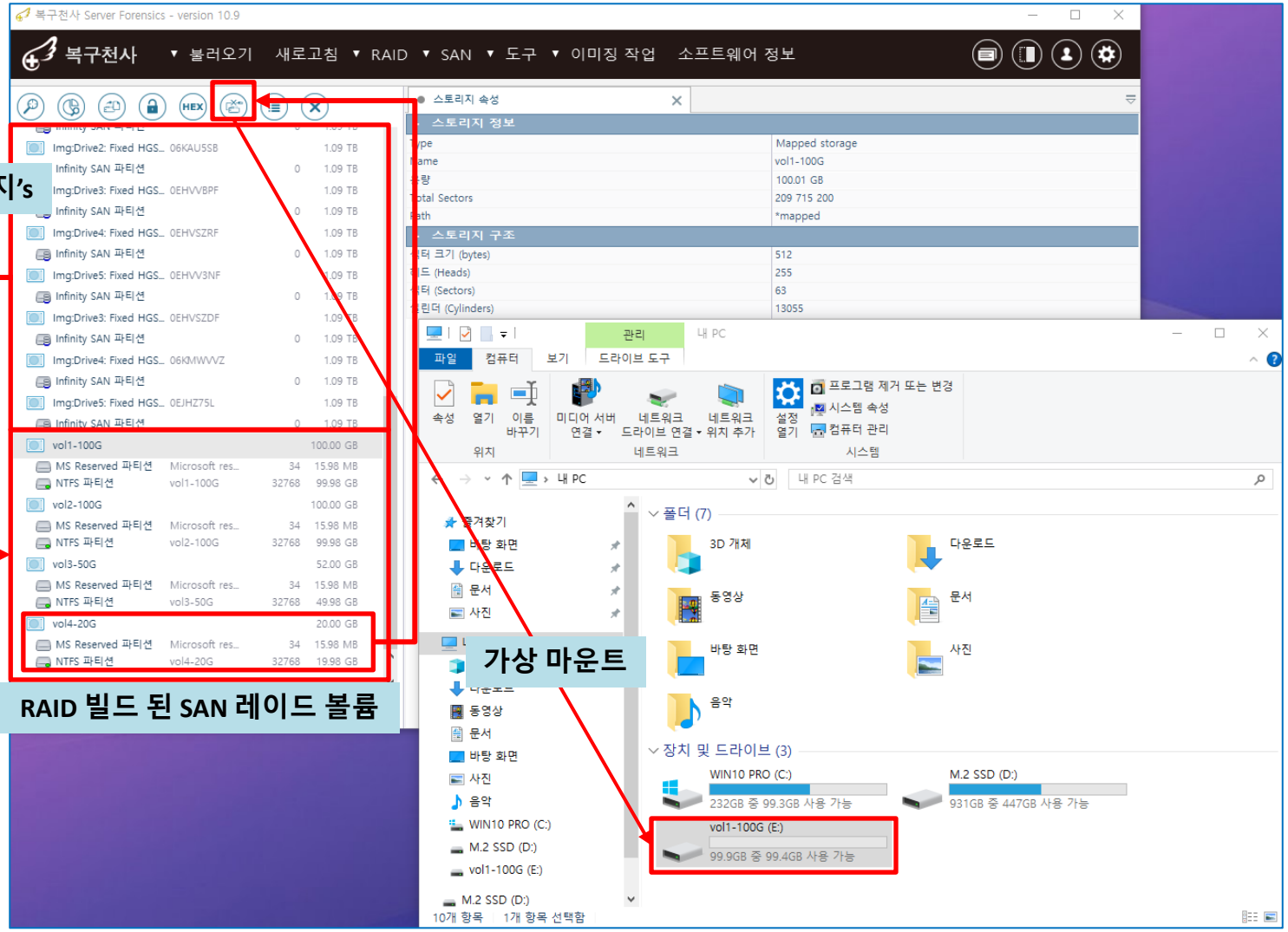
SAN

- 고가의 장비
- SAN을 운용 및 관리하기 위한 별도의 추가적인 장치들 필요
- 복잡한 운용 및 관리
- SAN 전용의 고성능 네트워크를 통해 연결, 연결 디스크를 로컬 드라이브 형태로 제공

시연-4

Server Forensic 자동 RAID 빌드 및 마운트

빌드 준비된 SAN 디스크 이미지's



Thank you