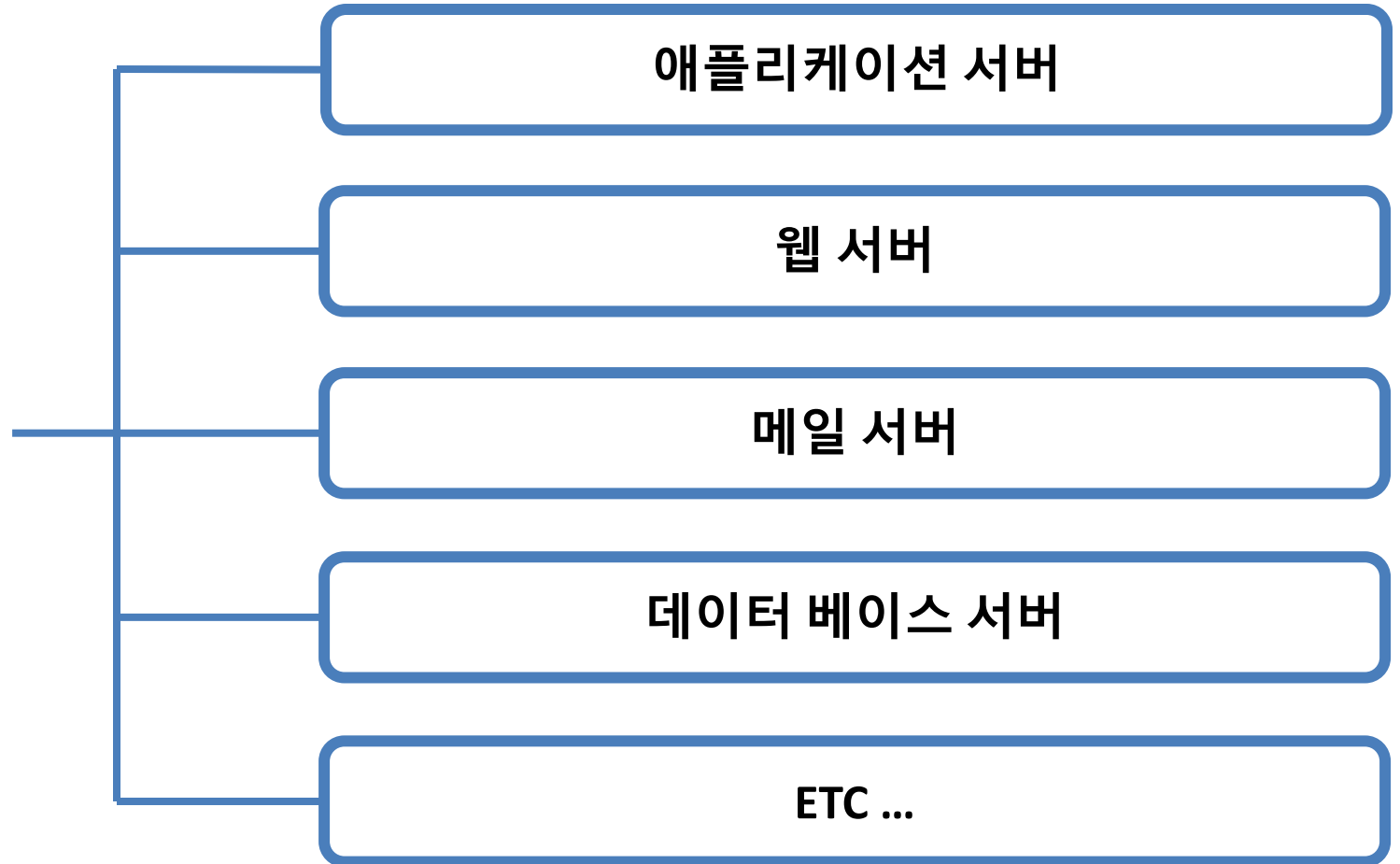
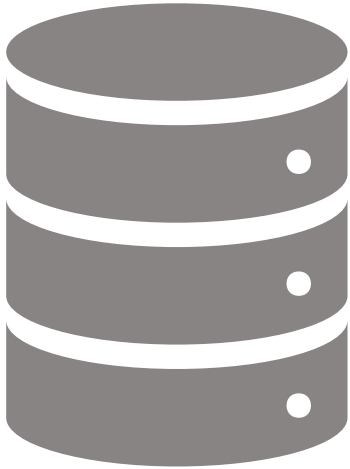


# 서버 포렌식의 최신 기술 동향

- RAID 자동 빌드 및 가상 마운트 -

# Server Forensic

## ■ Server

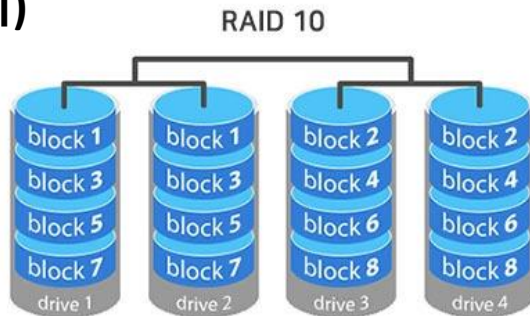


# Server Forensic

## ■ Server

### RAID 구성

예)



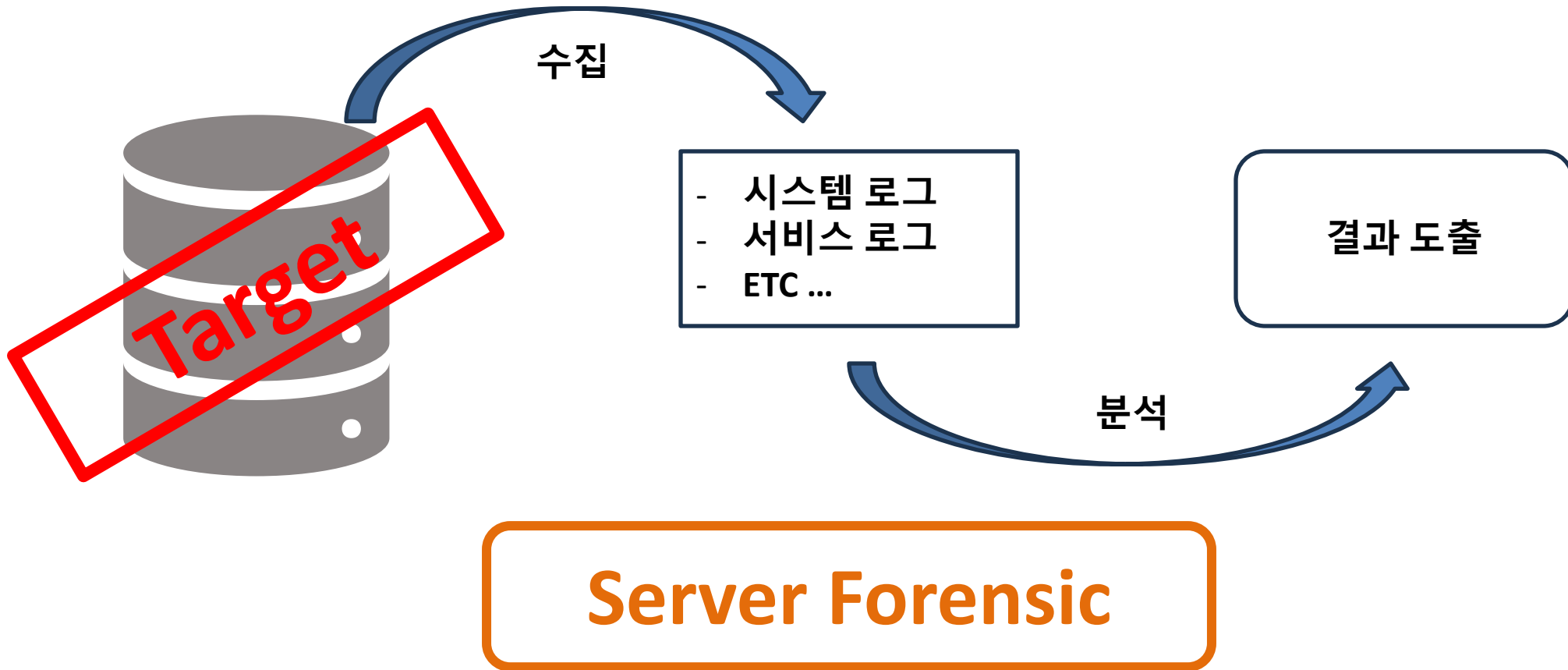
For

- 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

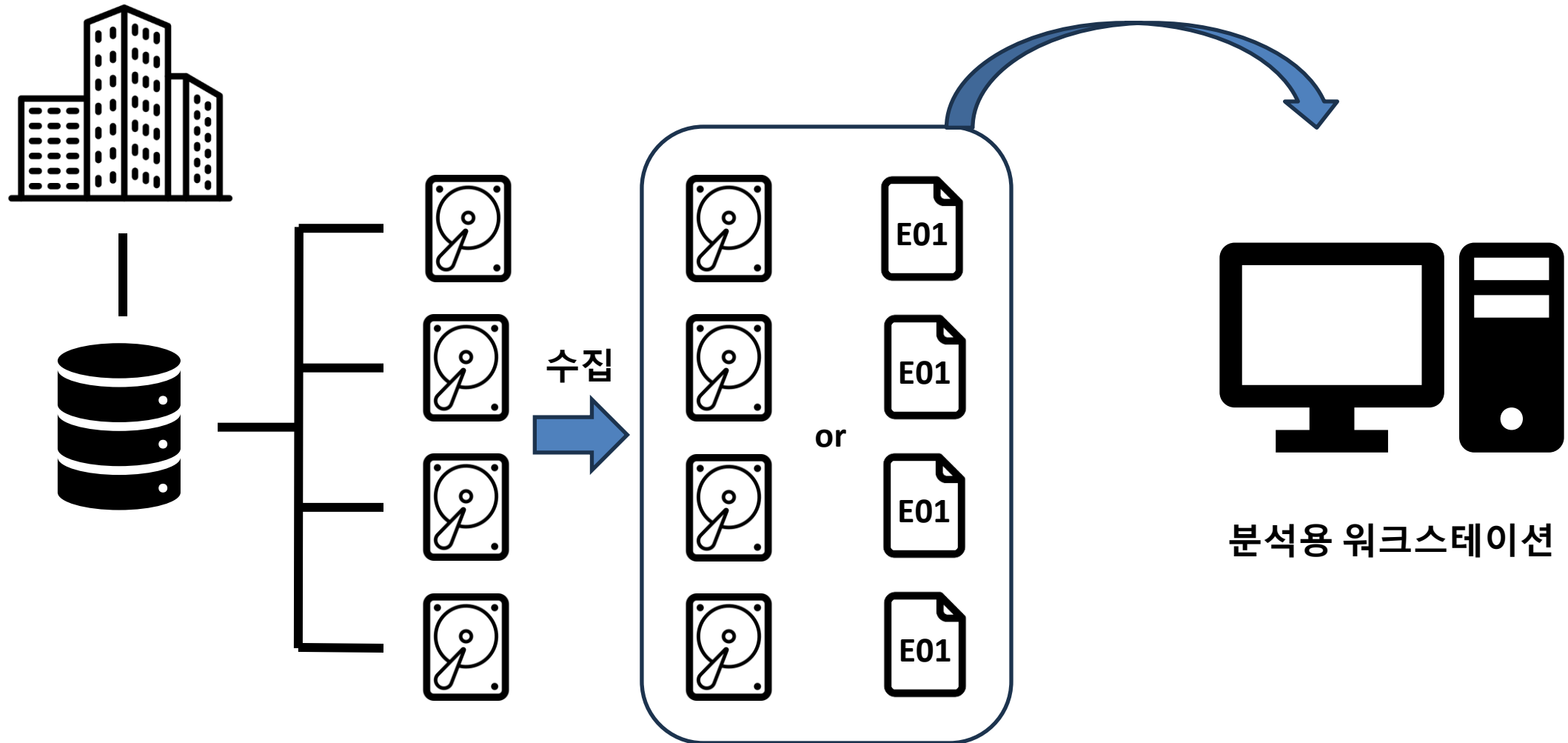
- RAID 0 / 1 / 10 / 3 / 5 / 50 / 6 / 60 / 1E / 5EE / SPANNED ...

## 다양한 파일 시스템

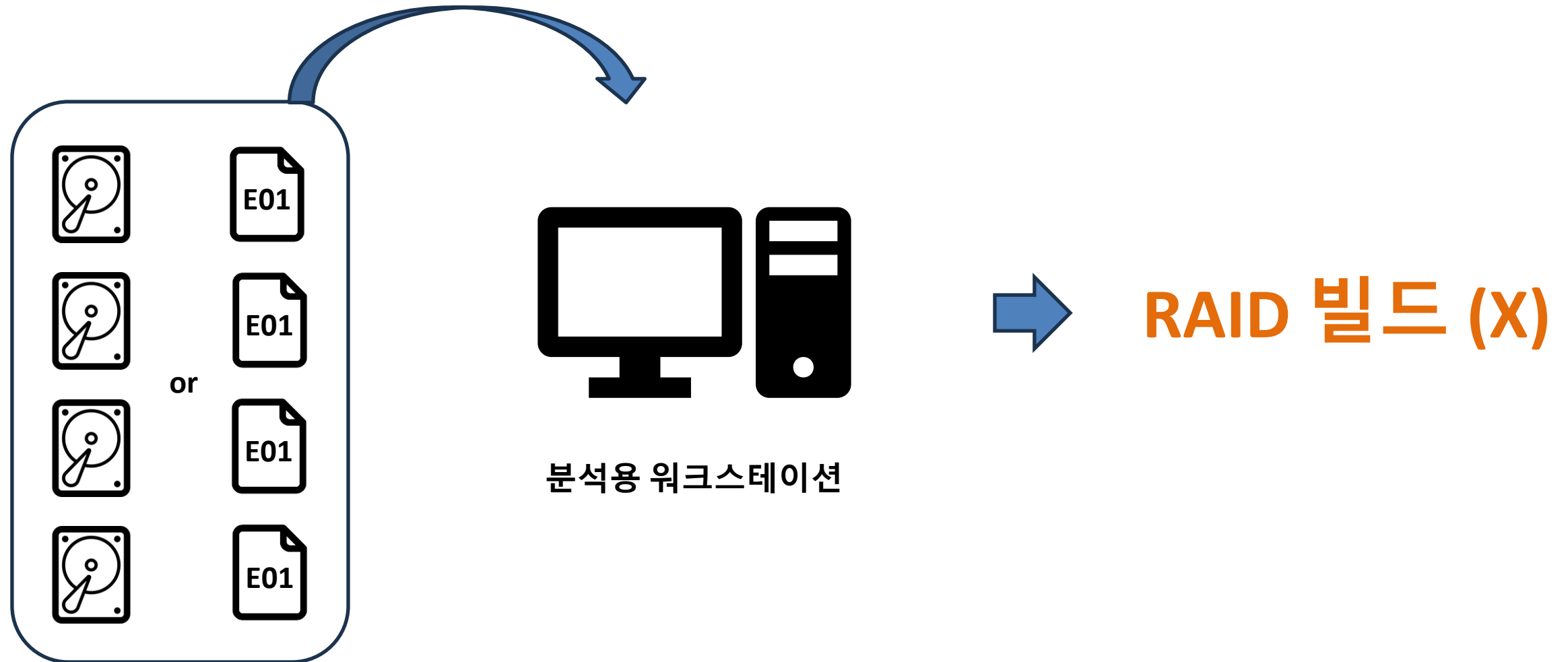
- Windows : FAT / FAT32 / exFAT / NTFS / ReFS / FeFS3
- macOS : HFS+ / APFS
- Linux : Ext2 / Ext3 / Ext4 / ReiserFS / XFS / JFS
- FreeBSD : UFS / UFS2
- Sun Solaris : ZFS



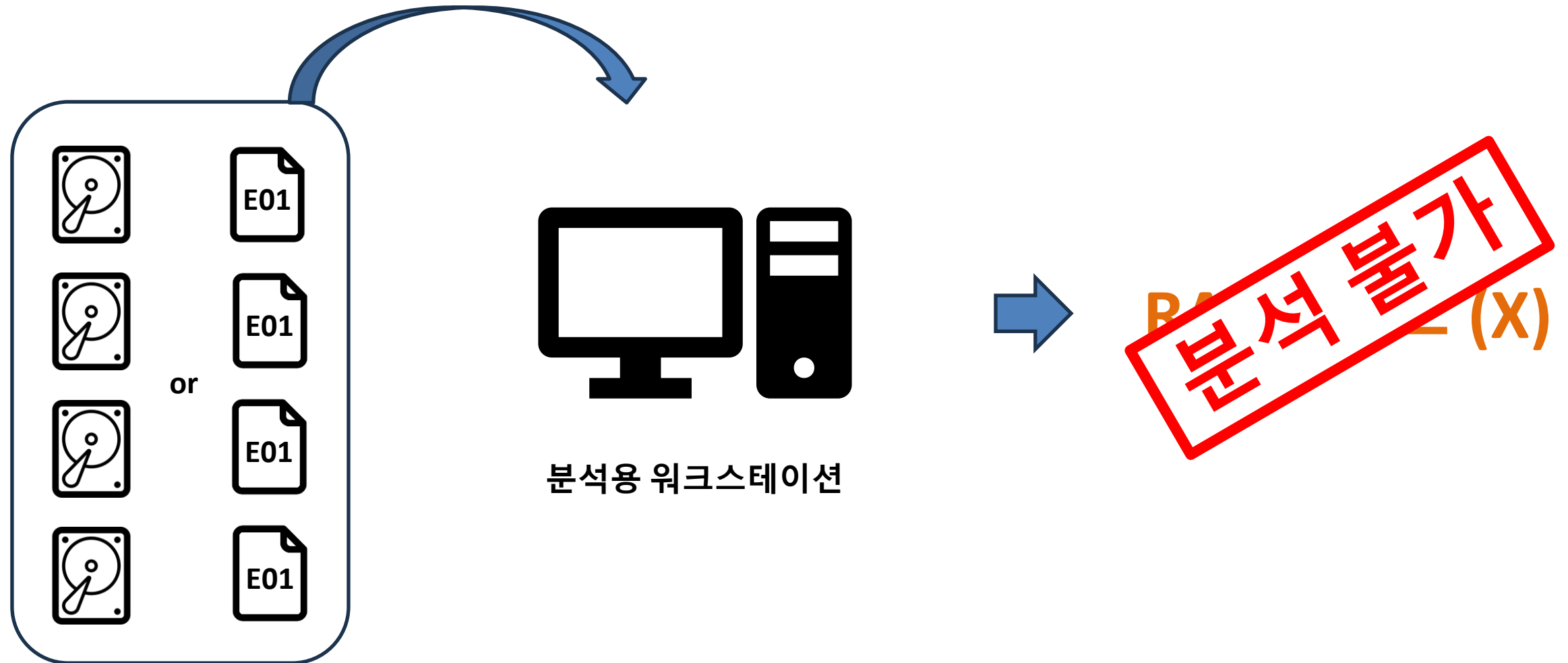
# Server Forensic RAID



# Server Forensic RAID



# 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(클래식, 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

The screenshot displays the '복구천사 Server Forensics - version 10.9' interface. The top menu bar includes '복구천사', '불러오기', '새로고침', 'RAID', 'SAN', '도구', '이미징 작업', and '소프트웨어 정보'. The left sidebar shows a list of disks and partitions. A red box highlights the 'RAID' icon in the top toolbar. Another red box highlights the '가상 마운트' (Virtual Mount) button in the '도구' (Tools) section. A third red box highlights the 'RAID5\_00' entry in the '자동 RAID 빌드 된 레이드 볼륨' (Automatically built RAID volumes) list. The main window shows the '스토리지 속성' (Storage Properties) dialog for the 'RAID5 (E:)' volume, indicating it is a 'Software RAID 5' with a total capacity of 445GB and 418GB available. The '장치 및 드라이브 (3)' (Devices and Drives) section shows the 'WIN10 PRO (C:)' and 'M.2 SSD (D:)' drives, along with the 'RAID5 (E:)' volume.

복구천사 Server Forensics - version 10.9

복구천사 ▾ 불러오기 새로고침 ▾ RAID ▾ SAN ▾ 도구 ▾ 이미징 작업 소프트웨어 정보

로컬 디스크

디스크	파일 시스템	전체 크기
WIN10 PRO (C:)	NTFS	232.23 GB
M.2 SSD (D:)	NTFS	931.49 GB
RAID5 (E:)	NTFS	445.48 GB

연결된 스토리지

이름/ID	Start Se...	전체 크기
Drive0: Fixed ATA Sa...	S3R2NWAJ50...	232.89 GB
FAT32 파티션	NO NAME	2048 100.00 MB
MS Reserved 파티션	Microsoft res...	206848 16.00 MB
NTFS 파티션	WIN10 PRO	239616 232.23 GB
NTFS 파티션	487270400	549.03 MB
Drive1: Removable N...	0123456789A...	931.51 GB
MS Reserved 파티션	Microsoft res...	34 15.98 MB
NTFS 파티션	M.2 SSD	32768 931.50 GB
Drive2: Fixed Angel R...	01000005D10...	445.50 GB

빌드 준비된 디스크 이미지's

이름	크기	
Img:Drive0: Fixed WD...	149.05 GB	
Software RAID 5 파티...	0 148.50 GB	
Img:Drive1: Fixed WD...	149.05 GB	
Software RAID 5 파티...	0 148.50 GB	
Img:Drive2: Fixed WD...	149.05 GB	
Software RAID 5 파티...	0 148.50 GB	
Img:Drive3: Fixed WD...	149.05 GB	
Software RAID 5 파티...	0 148.50 GB	
RAID5_00	446566C202...	445.50 GB
MS Reserved 파티션	Microsoft res...	34 15.98 MB

자동 RAID 빌드 된 레이드 볼륨

가상 마운트

스토리지 속성

파티션 정보

Start Sector	End Sector	Count Sectors
0	934 244 343	934 244 344
총량 445.48 GB		

파일 시스템

파일 시스템 형식

기본 테스트 결과

이름

일단 날짜

Cluster size

스토리지

내 PC

바탕 화면

다운로드

문서

사진

3D 개체

동영상

바탕 화면

음악

장치 및 드라이브 (3)

WIN10 PRO (C:)

232GB 중 99.4GB 사용 가능

M.2 SSD (D:)

931GB 중 447GB 사용 가능

RAID5 (E:)

445GB 중 418GB 사용 가능

10개 항목 | 1개 항목 선택함

# Server Forensic 자동 RAID 빌드 및 마운트

OpenText Endpoint Investigator Training

Case (Mounted RAID Evidence) View Tools SAFE EnScript Add Evidence Pathways

Local Device

Local Devices

	Name	Label	Access	Sectors	Size	Write Blocked	Read File System	Parse Link Files	Has DCO
<input type="checkbox"/>	0	ATA	ASPI	488,397,1...	232.9 ...		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	C	WIN10 PRO	Wind...	487,029,5...	232.2 ...		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	1	NVME USB	ASPI	1,953,525...	931.5 ...		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	D	M.2 SSD	Wind...	1,953,488...	931.5 ...		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	2	Angel	ASPI	934,281,2...	445.5 ...		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	E	RAID5	Wind...	934,244,3...	445.5 ...		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	C:\	Preview	Direct...	487,029,5...	232.2 ...		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	D:\	Preview	Direct...	1,953,488...	931.5 ...		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	E\	Preview	Direct...	934,244,3...	445.5 ...		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	RAM	Mem...			17.7 GB				

EnCase에서 가상 마운트 볼륨 불러오기

< 뒤로(B) 마침 취소

Hash Libraries

Magnet AXIOM Process 8.6.0.42282

파일 도구 도움말

증거 소스

사레 세부 정보

증거 소스

처리 세부 정보

아카이브 및 모바일 백업 검색

검색 키워드 추가

파일에서 텍스트 추출 (OCR)

해시 및 일치 항목 찾기

Magnet.AI로 재형 분석

Magnet.AI로 사진 분석

검색에 CPS 데이터 추가

추가 아티팩트 찾기

아티팩트 세부 정보

모바일 아티팩트

클라우드 아티팩트

컴퓨터 아티팩트

차량 아티팩트

아티팩트 구분 분석 및 카빙

권한 있는 콘텐츠

증거 소스

WINDOWS 드라이브 추가

모두 선택

☐ PhysicalDrive1 NVME USB 3.2 SCSI Disk Device (931.51 GB)

☐ Partition 1 (15.98 MB)

☐ Partition 2 (Microsoft NTFS, 931.5 GB) M.2 SSD [D:\]

☐ 분할되지 않은 공간

☐ PhysicalDrive0 Samsung SSD 850 EVO 250GB (232.89 GB)

☐ Partition 1 (Microsoft FAT32, 100 MB) NO NAME

☐ Partition 2 (16 MB)

☐ Partition 3 (Microsoft NTFS, 232.23 GB) WIN10 PRO [C:\]

☐ Partition 4 (Microsoft NTFS, 549 MB)

☐ 분할되지 않은 공간

☒ PhysicalDrive2 Angel RAID5\_00 SCSI Disk Device (445.5 GB)

☒ Partition 1 (15.98 MB)

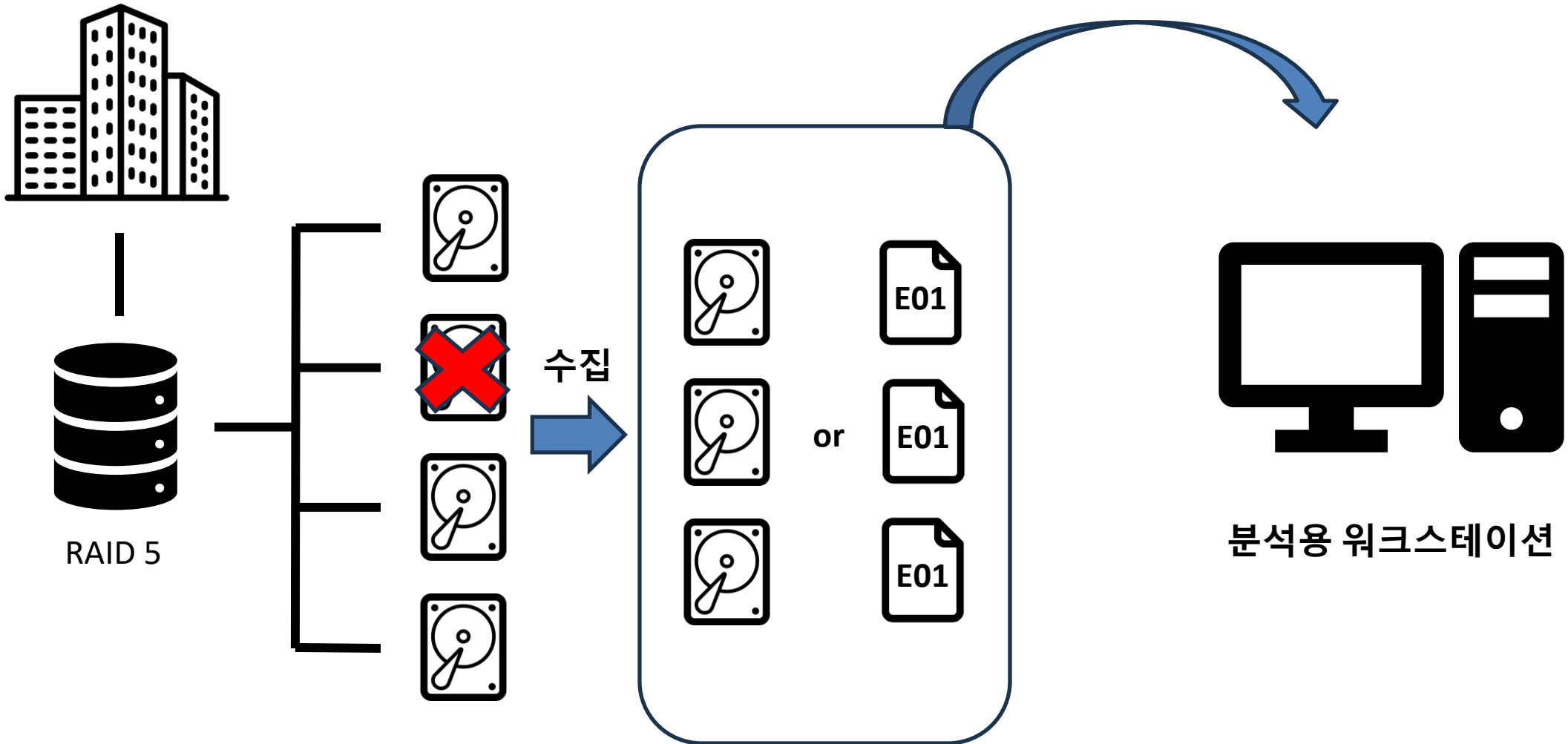
☒ Partition 2 (Microsoft NTFS, 445.48 GB) RAID5 [E:\]

☒ 분할되지 않은 공간

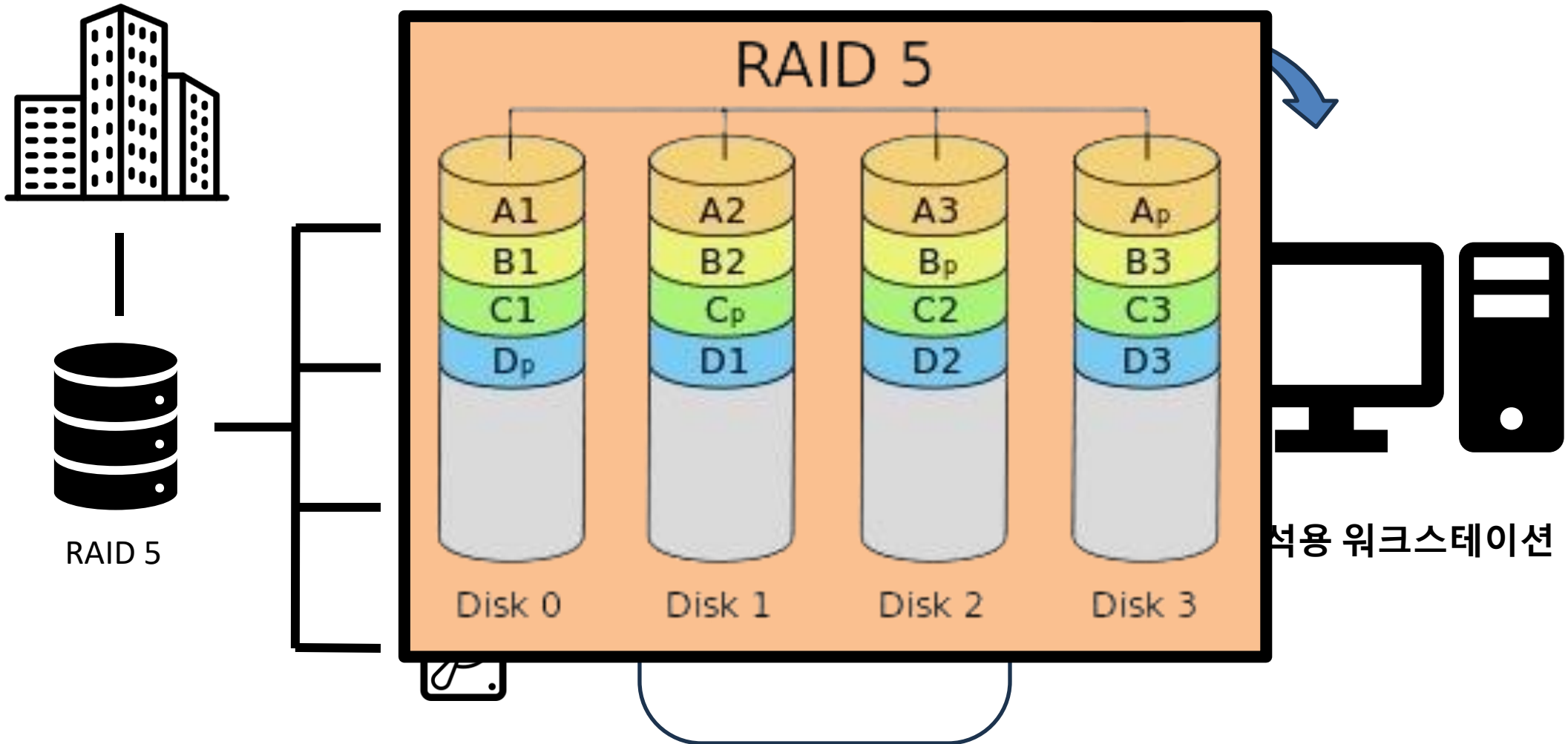
AXIOM에서 가상 마운트 볼륨 불러오기

뒤로 다음

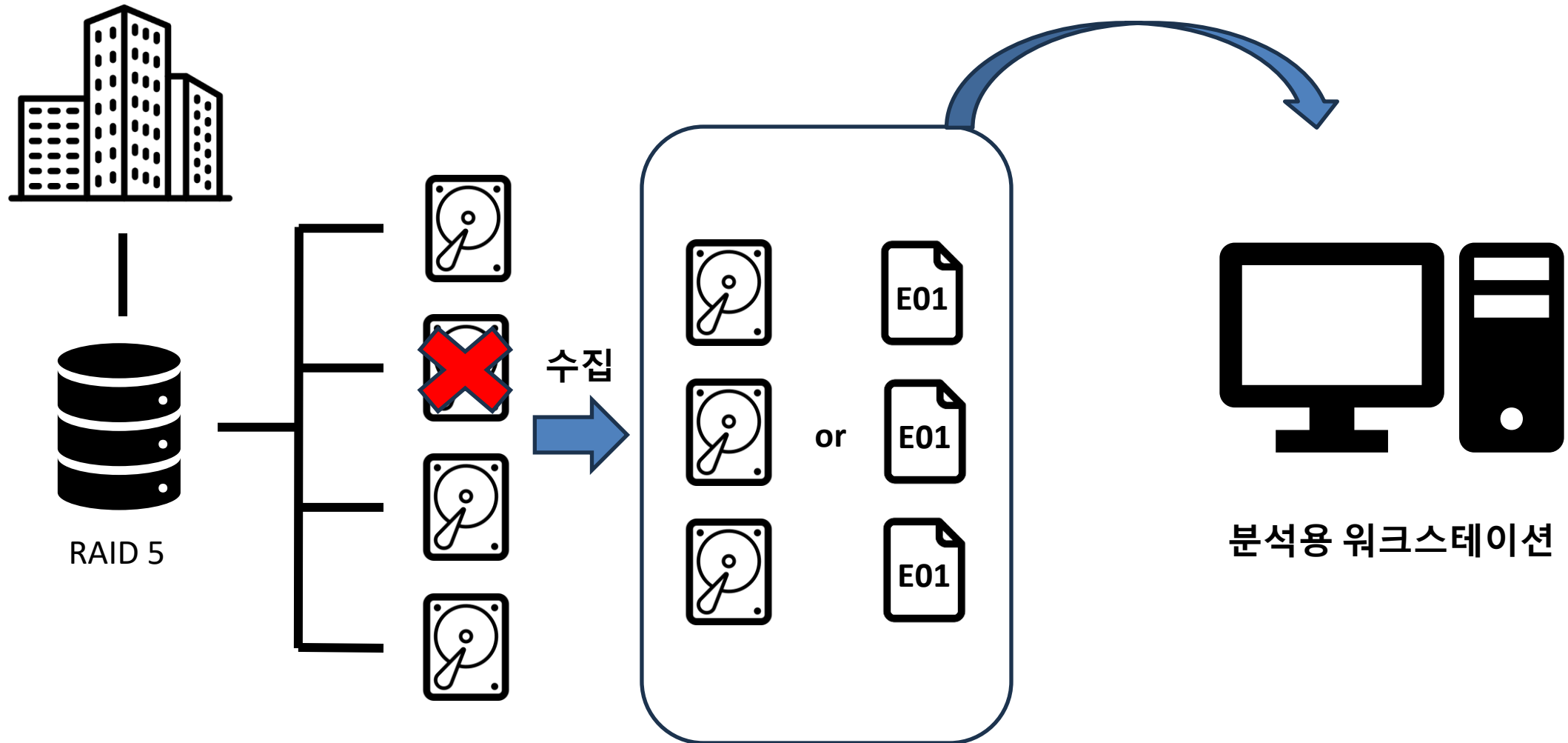
# Server Forensic 자동 RAID 빌드 및 마운트



# Server Forensic 자동 RAID 빌드 및 마운트



# Server Forensic 자동 RAID 빌드 및 마운트



시연-2

# Server Forensic 자동 RAID 빌드 및 마운트

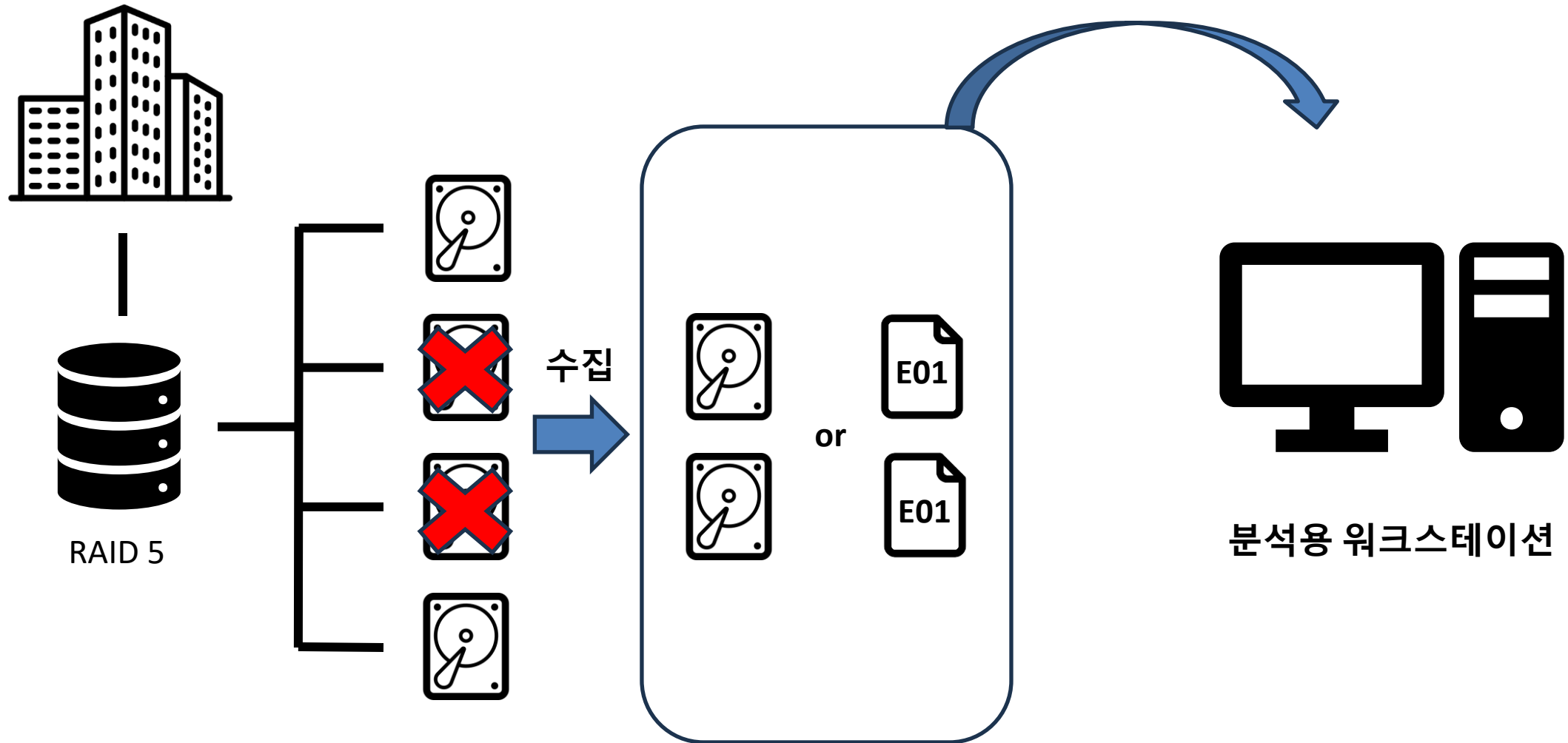
The screenshot displays the 복구천사 Server Forensics version 10.9 interface. The main window is divided into several sections:

- Left Panel:** Lists available disks and partitions. A red box highlights the 'RAID5 (E)' partition, which is 446.74 GB in size.
- Top Panel:** Shows the '스토리지 속성' (Storage Properties) window. It displays details for the selected RAID5 (E) partition, including its start sector (0), end sector (487 029 580), and count of sectors (487 029 581).
- Bottom Panel:** Shows the '가상 마운트' (Virtual Mount) window. It displays the '자동 RAID 빌드 된 레이드 볼륨' (Automatically built RAID volume) and lists the disks involved in the RAID: Drive2 (Fixed Angel RAL...), MS Reserved 파티션 (Microsoft rese...), NTFS 파티션 (RAID5), and Software RAID 5 파티션 (0).

Red arrows indicate the workflow: from the RAID5 (E) partition in the left panel, to the '스토리지 속성' window, and finally to the '가상 마운트' window.



# Server Forensic 자동 RAID 빌드 및 마운트



시연-3

# Server Forensic 자동 RAID 빌드 및 마운트

복구천사 Server Forensics - version 10.9

복구천사 볼러오기 새로고침 RAID SAN 도구 이미지 작업 소프트웨어 정보

스토리지 속성 RAID 구성

로컬 디스크

이름/ID	Start Sec...	현재 크기
Drive0: Fixed ATA Sams... S3R2NWAJ501...		232.89 GB
FAT32 파티션	NO NAME	2048 100.00 MB
MS Reserved 파티션	Microsoft rese...	206848 16.00 MB
NTFS 파티션	WIN10 PRO	232.89 GB

연결된 스토리지

새롭게 생성한 가상 디스크

가상 디스크로 대체	스토리지 ID	타	섹터 수
ImgDrive4: Fixed ST3160318AS (SAT) SVM9P7HX	0	312581808	
ImgDrive5: Fixed WDC WD1600AAJS-0L WD-WCAYU7075382	0	312581808	
Pattern	0	312581808	

가상 RAID 구성

RAID level	RAID5 - 분산 패리티
패리티 설정	왼쪽 비대칭(backward)
스트라이프 크기	256KB
패리티 단위 설정	1
RAID 가상이름	가상 RAID
비동기 I/O	No
순환 시프트 값	0
결합 재현	No

장애 디스크 2개를 제외한 빌드 준비된 디스크 이미지's

이름	크기
ImgDrive4: Fixed ST31... SVM9P7HX	149.05 GB
Software RAID 5 파티션	0 148.92 GB
ImgDrive5: Fixed WDC... WD-WCAYU70...	149.05 GB
Software RAID 5 파티션	0 148.92 GB
Pattern	149.05 GB
Storage 파티션	0 149.05 GB

새롭게 생성한 패턴(00) 디스크

RAID 세부 정보

- RAID 정보	
이름	RAID5
레벨	RAID 5
구성 요소	4
RAID ID	0590850227419901
스트라이프 크기	256K
패리티 회전	Left Asymmetric
상태	대기 중/불완전

#	구성 요소 이름	ID	크기	오프셋(섹터)	섹터 수
2	ImgDrive4: Fixed ST3160318AS (SAT)	SVM9P7HX	148.92 GB	0	312317952
3	ImgDrive5: Fixed WDC WD1600AAJS-00YZCA0 / S...	WD-WCAYU7075382	148.92 GB	0	312317952

레이드 구성 정보

- 구성 요소 세부 정보	
구성 요소 이름	ImgDrive4: Fixed ST3160318AS (SAT)
ID	SVM9P7HX
크기	148.92 GB
오프셋(섹터)	0
섹터 수	312317952
마지막으로 수정된 메타데이터	2024-07-19 10:11:35

보고서 저장 • 닫기

## NAS

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

- 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

## SAN

시연-4

# Server Forensic 자동 RAID 빌드 및 마운트

빌드 준비된 SAN 디스크 이미지's

The screenshot displays the JETCO Server Forensics v10.9 interface. On the left, a list of prepared SAN disk images is shown, including 'ImgDrive2: Fixed HGS\_06KAU5S8' through 'ImgDrive5: Fixed HGS\_0EJHZ75L' and 'vol1-100G' through 'vol4-20G'. A red box highlights the 'vol1-100G' entry. A red arrow points from this entry to the '가상 마운트' (Virtual Mount) button in the center. Below the list, a table shows the RAID build status for 'vol1-100G' and 'vol4-20G'. A red box highlights the 'vol1-100G' entry in this table. A red arrow points from this entry to the '가상 마운트' button. On the right, the '스토리지 속성' (Storage Properties) window is open, showing details for 'vol1-100G'. Below this, the '내 PC' (This PC) window is open, showing the '장치 및 드라이브' (Devices and Drives) section. A red box highlights the 'vol1-100G (E:)' entry in this section, indicating it has been successfully mounted.

이름	용량	상태
vol1-100G	100.00 GB	가상 마운트
vol2-100G	100.00 GB	가상 마운트
vol3-50G	52.00 GB	가상 마운트
vol4-20G	20.00 GB	가상 마운트

이름	용량	상태
vol1-100G	100.00 GB	가상 마운트
vol2-100G	100.00 GB	가상 마운트
vol3-50G	52.00 GB	가상 마운트
vol4-20G	20.00 GB	가상 마운트

RAID 빌드 된 SAN 레이드 볼륨

가상 마운트

---

# Thank you