

문제 3.

### 3. 증거매체의 볼륨 정보를 기술하시오

- ① 파일시스템의 종류 ② 볼륨 시리얼 넘버 ③ 총 섹터수 ④ 총 용량  
⑤ 단위 클러스터의 크기 ⑥ 볼륨의 이름

FTK Imager를 활용하여 문제 2에서 복구한 이미지파일을 불러온 결과 아래와 같음을 확인.

The left screenshot shows the 'Evidence Tree' with the following structure:

- 복구\_022-2-1-168.001
  - Partition 1 [1021MB]
    - jewel [NTFS]
      - [orphan]
      - [root]
      - [unallocated space]
    - Unpartitioned Space [basic disk]

The right screenshot shows the 'Properties' window for 'Partition 1' with the following 'File System Information':

Property	Value
Cluster Size	4,096
Cluster Count	261,375
Free Cluster Count	240,409
Dirty Flag	False
Volume Label	jewel
Volume Serial Number	26A1-5D6B
File System Version	Windows XP (NTFS 3.1)
UTC Timestamps	True

The bottom screenshot shows the 'Properties' window for 'Partition 1' with the following 'Partition Information':

Property	Value
Starting Sector	128
Sector Count	2,091,008

파일시스템의 종류	NTFS
볼륨 시리얼 넘버	26A1-5D6B
총 섹터수	2,091,008
총 용량	(4,096(Cluster Size) * 261,375(Cluster Count) =) 1,070,592,000 (Bytes)
단위 클러스터의 크기	4,096 (Bytes)
볼륨의 이름	jewel