153 – Partition Finder

Team Information

Team Name: kimbabasaksaksak

Team Member: Jaeheon Kim, Donghyun Kim, Soyoung Yoo, Minhee Lee

Email Address: uaaoong@gmail.com

Instructions

Description Analyze the RAW disk image file to answer the question. (The filesystem for Windows was formatted in Windows 10.)

Target	Hash (MD5)
PartitionFinder.7z	C8FAEAF9C286CB90FF5B9D671E74E7E8

Questions

1) Find all deleted partitions, and analyze the following information for each partition. (100 points)
   - Partition type, volume serial number, formatted date/time, capacity, 1st sector(physical)
2) Which volumes are connected to more than one system? Analyze the following information for those volumes. (50 points)
   - Partition type, 1st sector(physical)

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

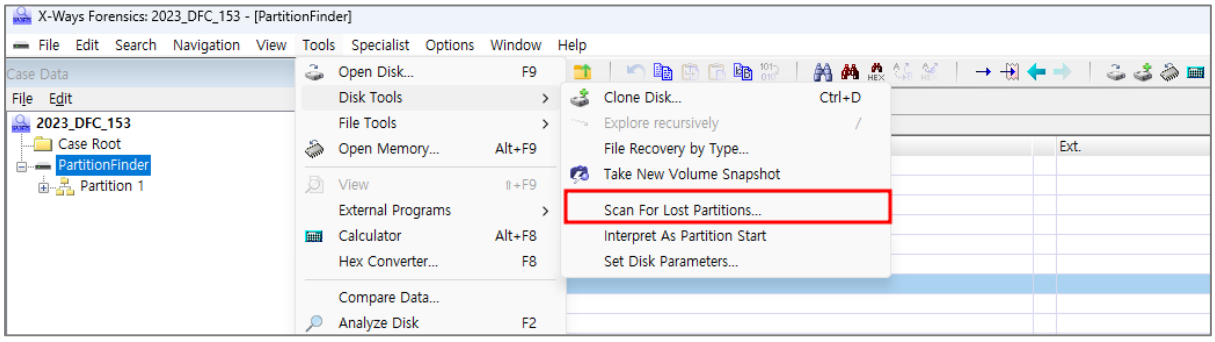
Tools used:

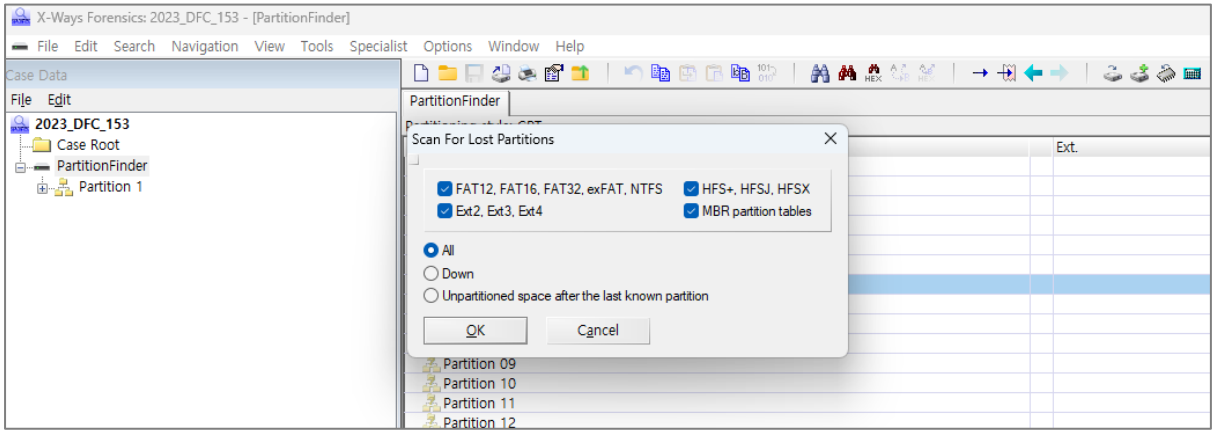
Name:	X-Ways Forensics	Publisher:	X-Ways Software Technology
Version:	20.0		
URL:	https://www.x-ways.net		

Step-by-step methodology:

Q1. Find all deleted partitions, and analyze the following information for each partition. (100 points)

X-Ways Forensics 도구의 Scan For Lost Partitions 기능을 사용하여 삭제된 파티션을 복구한다.





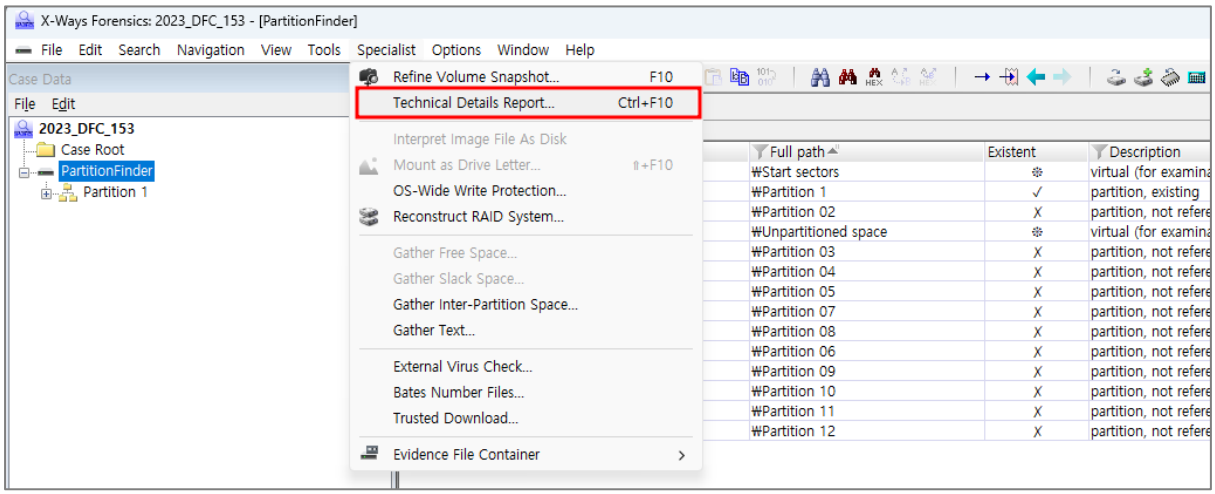
복구된 파티션 중, Partition 6과 Partition 9는 동일한 파티션으로 복구된 파티션은 총 10개이다.

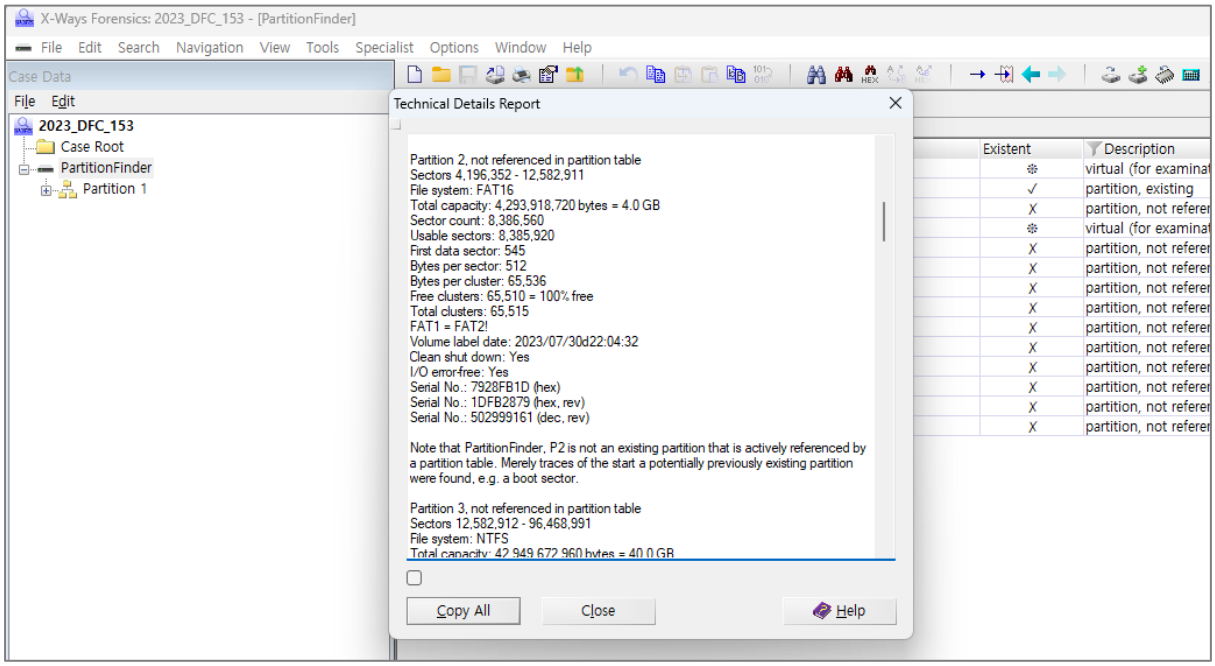
PartitionFinder

Partitioning style: GPT

Name	Path	Full path	Existent	Description	Ext.	Type
Start sectors	₩	₩Start sectors	❄	virtual (for examination purposes)		
Partition 1	₩	₩Partition 1	✓	partition, existing		FAT16
Partition 02	₩	₩Partition 02	X	partition, not referenced in partition table		FAT16
Unpartitioned space	₩	₩Unpartitioned space	❄	virtual (for examination purposes)		
Partition 03	₩	₩Partition 03	X	partition, not referenced in partition table		NTFS
Partition 04	₩	₩Partition 04	X	partition, not referenced in partition table		NTFS
Partition 05	₩	₩Partition 05	X	partition, not referenced in partition table		Ext4
Partition 07	₩	₩Partition 07	X	partition, not referenced in partition table		FAT16
Partition 08	₩	₩Partition 08	X	partition, not referenced in partition table		NTFS
Partition 06	₩	₩Partition 06	X	partition, not referenced in partition table		exFAT
Partition 09	₩	₩Partition 09	X	partition, not referenced in partition table		exFAT
Partition 10	₩	₩Partition 10	X	partition, not referenced in partition table		FAT16
Partition 11	₩	₩Partition 11	X	partition, not referenced in partition table		Ext2
Partition 12	₩	₩Partition 12	X	partition, not referenced in partition table		NTFS

복구된 파티션들의 상세 정보는 Technical Detail Report 기능을 사용하여 확인할 수 있다.





@ Answer 1

- partition type: FAT16
- volume serial number: 79 28 FB 1D (hex)
- formatted date/time: 2023/07/30 22:20:32 (UTC+0)

  * 추가설명: 윈도우 파일시스템은 윈도우10 환경에서 포맷되었다고 문제에서 주어졌으므로, System Volume Information 폴더의 생성 시각이 파일시스템이 포맷된 시각이라고 할 수 있다.

- capacity: 4,293,918,720 bytes = 4.0 GB
- 1st sector(physical): 4,196,352

@ Answer 2

- partition type: NTFS
- volume serial number: C0 0E EB 1D 34 C3 D9 01 (hex)
- formatted date/time: 2023/07/30 22:20:59 (UTC+0)

  * 추가설명: 포맷 시각은 $MFT가 생성된 시각

- capacity: 42,949,672,960 bytes = 40.0 GB
- 1st sector(physical): 12,582,912

@ Answer 3

- partition type: NTFS
- volume serial number: 90 E6 54 94 ED C2 D9 01 (hex)
- formatted date/time: 2010/05/04 03:24:57 (UTC+0)

  * 추가설명: 포맷 시각은 $MFT가 생성된 시각

- capacity: 37,580,960,256 bytes = 35.0 GB
- 1st sector(physical): 41,943,040

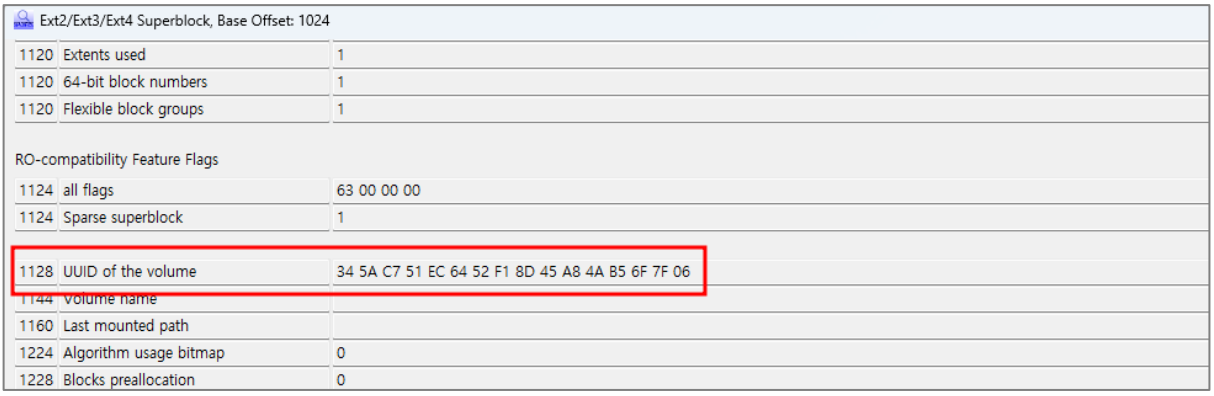
@ Answer 4

- partition type: Ext4

- volume serial number: 없음

  * 추가설명: Ext4 파일시스템은 FAT이나 NTFS 파일시스템처럼 Volume Serial Number가 없다. 하지만, 파일시스템 볼륨의 고유한 식별자인 UUID(Universally Unique Identifier) 값이 있다. UUID는 superblock에 저장되어 있다.

  - UUID: 34 5A C7 51 EC 64 52 F1 8D 45 A8 4A B5 6F 7F 06 (hex)



- formatted date/time: 2023/07/30 22:25:41 (UTC+0)

  * 추가설명: 포맷 시각은 .journal이 생성된 시각

- capacity: 32,212,254,720 bytes = 30.0 GB

- 1st sector(physical): 96,468,992

@ Answer 5

- partition type: FAT16

- volume serial number: B0 ED 13 C7 (hex)

- formatted date/time: 2023/07/30 22:57:28 (UTC+0)

  * 추가설명: 윈도우 파일시스템은 윈도우10 환경에서 포맷되었다고 문제에서 주어졌으므로, System Volume Information 폴더의 생성 시각이 파일시스템이 포맷된 시각이라고 할 수 있다.

- capacity: 4,293,918,720 bytes = 4.0 GB

- 1st sector(physical): 115,343,360

@ Answer 6

- partition type: NTFS
- volume serial number: 10 E2 4B 05 41 C3 D9 01 (hex)
- formatted date/time: 2023/07/30 23:53:21 (UTC+0)

  * 추가설명: 포맷 시각은 $MFT가 생성된 시각

- capacity: 64,692,944,896 bytes = 60.3 GB
- 1st sector(physical): 123,729,920

@ Answer 7

- partition type: exFAT
- volume serial number: 4D 20 01 1E (hex)
- formatted date/time: 2023/07/30 13:26:23 (UTC+0)

  * 추가설명: 윈도우 파일시스템은 윈도우10 환경에서 포맷되었다고 문제에서 주어졌으므로, System Volume Information 폴더의 생성 시각이 파일시스템이 포맷된 시각이라고 할 수 있다.

- capacity: 46,439,333,888 bytes = 43.3 GB
- 1st sector(physical): 159,383,552

@ Answer 8

- partition type: FAT16
- volume serial number: A5 3A 01 1E (hex)
- formatted date/time: 2023/07/30 22:26:51 (UTC+0)

  * 추가설명: 윈도우 파일시스템은 윈도우10 환경에서 포맷되었다고 문제에서 주어졌으므로, System Volume Information 폴더의 생성 시각이 파일시스템이 포맷된 시각이라고 할 수 있다.

- capacity: 2,147,483,648 bytes = 2.0 GB

- 1st sector(physical): 184,549,376

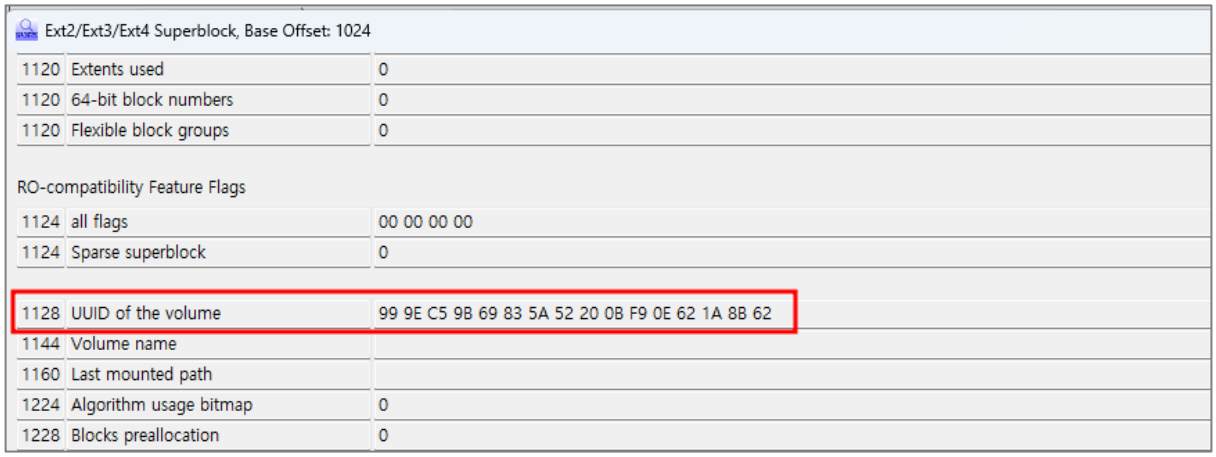
@ Answer 9

- partition type: Ext2

- volume serial number: 없음

  * 추가설명: Ext2 파일시스템은 FAT이나 NTFS 파일시스템처럼 Volume Serial Number가 없다. 하지만, 파일시스템 볼륨의 고유한 식별자인 UUID(Universally Unique Identifier) 값이 있다. UUID는 superblock에 저장되어 있다.

  - UUID: 99 9E C5 9B 69 83 5A 52 20 0B F9 0E 62 1A 8B 62 (hex)



Ext2/Ext3/Ext4 Superblock, Base Offset: 1024

1120	Extents used	0
1120	64-bit block numbers	0
1120	Flexible block groups	0
	RO-compatibility Feature Flags	
1124	all flags	00 00 00 00
1124	Sparse superblock	0
1128	UUID of the volume	99 9E C5 9B 69 83 5A 52 20 0B F9 0E 62 1A 8B 62
1144	Volume name	
1160	Last mounted path	
1224	Algorithm usage bitmap	0
1228	Blocks preallocation	0

- formatted date/time: 알 수 없음

  * 추가설명: 타임스탬프를 가진 파일시스템 메타데이터 파일이 존재하지 않아, 포맷된 시각을 추정할 수 없다.

- capacity: 12,884,901,888 bytes = 12.0 GB

- 1st sector(physical): 188,743,680

@ Answer 10

- partition type: NTFS

- volume serial number: 80 06 24 3B 35 C3 D9 01 (hex)

- formatted date/time: 2023/07/30 22:28:57 (UTC+0)

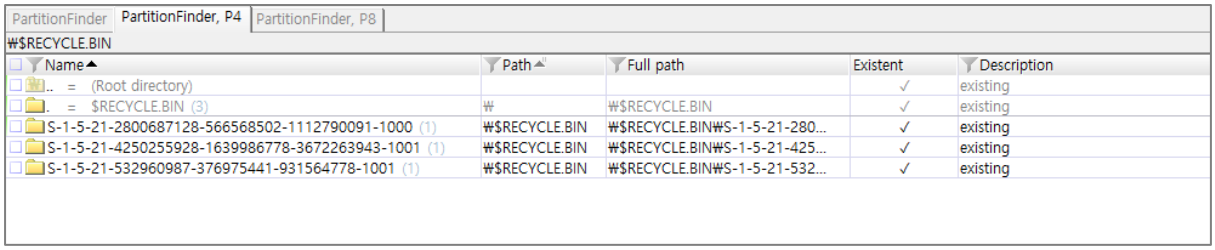
  * 추가설명: 포맷 시각은 $MFT가 생성된 시각

- capacity: 18,520,997,888 bytes = 17.2 GB

- 1st sector(physical): 213,909,504

Q2. Which volumes are connected to more than one system? Analyze the following information for those volumes. (50 points)

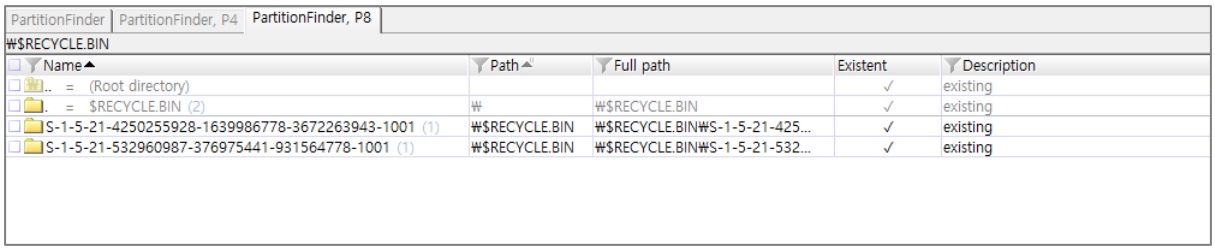
복구된 파티션 중, $RECYCLE.BIN 폴더에 SID 폴더가 여러 개 존재하는 파티션들이 있다.



PartitionFinder | PartitionFinder, P4 | PartitionFinder, P8

₩$RECYCLE.BIN

Name	Path	Full path	Existent	Description
.. = (Root directory)			✓	existing
. = $RECYCLE.BIN (3)	₩	₩$RECYCLE.BIN	✓	existing
S-1-5-21-2800687128-566568502-1112790091-1000 (1)	₩$RECYCLE.BIN	₩$RECYCLE.BIN₩S-1-5-21-280...	✓	existing
S-1-5-21-4250255928-1639986778-3672263943-1001 (1)	₩$RECYCLE.BIN	₩$RECYCLE.BIN₩S-1-5-21-425...	✓	existing
S-1-5-21-532960987-376975441-931564778-1001 (1)	₩$RECYCLE.BIN	₩$RECYCLE.BIN₩S-1-5-21-532...	✓	existing



PartitionFinder | PartitionFinder, P4 | PartitionFinder, P8

₩$RECYCLE.BIN

Name	Path	Full path	Existent	Description
.. = (Root directory)			✓	existing
. = $RECYCLE.BIN (2)	₩	₩$RECYCLE.BIN	✓	existing
S-1-5-21-4250255928-1639986778-3672263943-1001 (1)	₩$RECYCLE.BIN	₩$RECYCLE.BIN₩S-1-5-21-425...	✓	existing
S-1-5-21-532960987-376975441-931564778-1001 (1)	₩$RECYCLE.BIN	₩$RECYCLE.BIN₩S-1-5-21-532...	✓	existing

SID는 Windows에서 보안 주체 (예: 사용자, 그룹, 서비스 등)를 고유하게 식별하는 데 사용되는 고유한 값이다. SID의 구조는 여러 부분으로 나눌 수 있다. 예를 들어, S-1-5-21-4250255928-1639986778-3672263943-1001에서:

S: SID 문자열의 시작을 나타낸다.

1: 버전 번호이다.

5: 리비전 수이다.

21: 기관의 식별자이다.

그 다음의 3개 값 (4250255928-1639986778-3672263943)은 시스템을 고유하게 식별하는 로컬 컴퓨터의 식별자이다.

맨 마지막 숫자 (1001)는 해당 시스템 내에서의 고유한 계정 번호를 나타낸다.

위 파티션들은 시스템을 고유하게 식별하는 로컬 컴퓨터의 식별자(예: 4250255928-1639986778-3672263943)가 다른 SID 폴더들이 2개 이상 존재하므로, 둘 이상의 시스템에 연결되었던 파티션들이다.

@ Answer 1

- partition type: NTFS
- 1st sector(physical): 41,943,040

@ Answer 2

- partition type: NTFS
- 1st sector(physical): 123,729,920