

202 – Reconstruct RAID

Team Information

Team Name : LuckyVicky

Team Member : Eungchang Lee, Hyun Yi, Juho Heo, Dongkyu Lee

Email Address : dfc_luckyvicky@googlegroups.com

Instructions

Description Reconstruct a RAID Array using the given image files.

Target	Hash (MD5)
DFC_NAS_01.E01	5ab004d27d19db6a7285966703140cd0
DFC_NAS_02.E01	37d6cd7bca1ff54802798e1eb74d1c0b
DFC_NAS_03.E01	164af7a910d1ce03666db1f4aa37b88b

Questions

1. What is the manufacturer and product name of the NAS from which the given image was collected? (10 points)
2. What is the ID and email address of the account currently active on the NAS? (10 points)
3. When was the RAID created? (UTC+0) (10 points)
4. What is the RAID level? (10 points)
5. What is the filesystem of the RAID volume you reconstructed? (10 points)
6. What are the MD5 hash values of the following two files? (100 points)
 - A. IMG_6715.jpg
 - B. IMG_2386.MOV
7. What picture files are deleted from a reconstructed RAID volume?

(50 points)

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:	Hashtab	Publisher:	Implbits Software
Version:	V6.0.0		
URL:	http://implbits.com		

Name:	Vmware workstation	Publisher:	Broadcom
Version:	17.5.2 build-23775571		
URL:	https://www.vmware.com/		

Name:	Ubuntu18.04	Publisher:	Canonical
Version:	Ubuntu-18.04-desktop		
URL:	https://ubuntu.com		

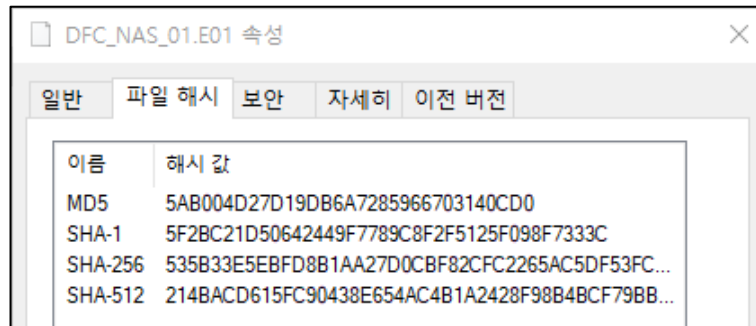
Name:	mdadm	Publisher:	neilbrown
Version:	v4.1-rc1		
URL:	https://github.com/neilbrown/mdadm		

Name:	VScode	Publisher:	Microsoft
Version:	1.92.2		
URL:	https://code.visualstudio.com/		

Name:	DB Browser for SQLite	Publisher:	Mauricio Piacentini
Version:	3.12.2		
URL:	https://sqlitebrowser.org/		

Name:	QEMU	Publisher:	QEMU Community
Version:	9.0.92		
URL:	https://www.qemu.org/		

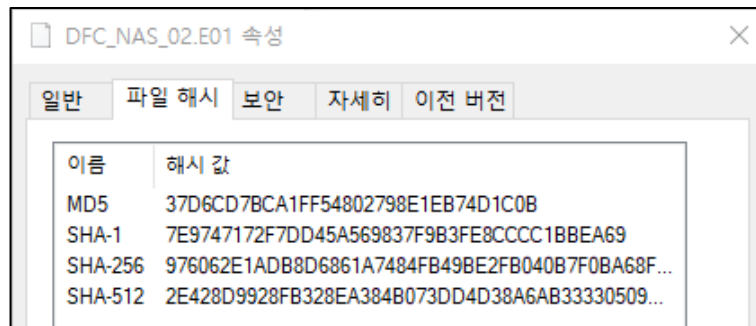
Step-by-step methodology:



DFC_NAS_01.E01 속성

이름	해시 값
MD5	5AB004D27D19DB6A7285966703140CD0
SHA-1	5F2BC21D50642449F7789C8F2F5125F098F7333C
SHA-256	535B33E5EBFD8B1AA27D0CBF82CFC2265AC5DF53FC...
SHA-512	214BACD615FC90438E654AC4B1A2428F98B4BCF79BB...

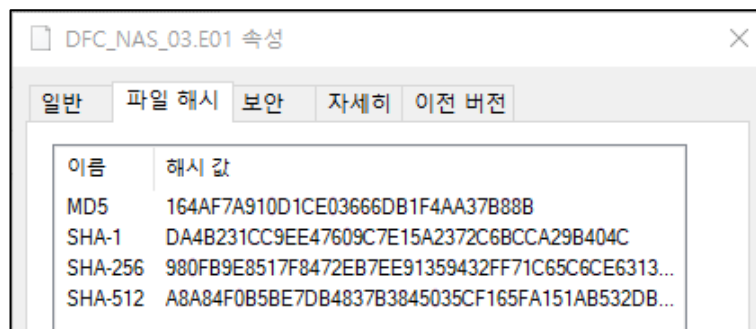
[그림 1] DFC_NAS_01.E01 파일의 해시 값



DFC_NAS_02.E01 속성

이름	해시 값
MD5	37D6CD7BCA1FF54802798E1EB74D1C0B
SHA-1	7E9747172F7DD45A569837F9B3FE8CCCC1BBEA69
SHA-256	976062E1ADB8D6861A7484FB49BE2FB040B7F0BA68F...
SHA-512	2E428D9928FB328EA384B073DD4D38A6AB33330509...

[그림 2] DFC_NAS_02.E01 파일의 해시 값



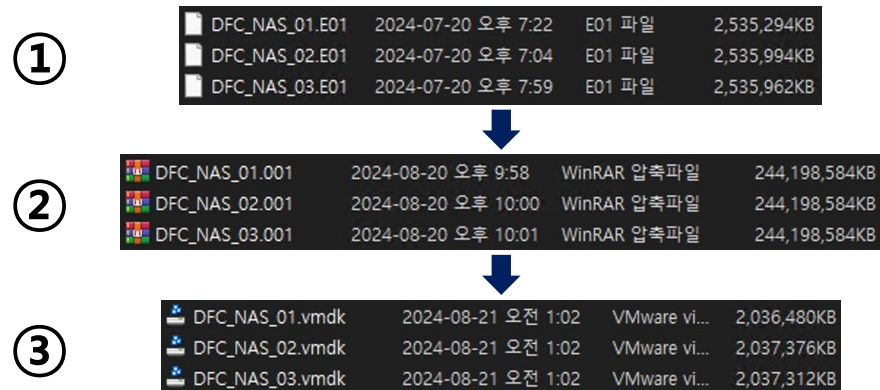
DFC_NAS_03.E01 속성

이름	해시 값
MD5	164AF7A910D1CE03666DB1F4AA37B88B
SHA-1	DA4B231CC9EE47609C7E15A2372C6BCCA29B404C
SHA-256	980FB9E8517F8472EB7EE91359432FF71C65C6CE6313...
SHA-512	A8A84F0B5BE7DB4837B3845035CF165FA151AB532DB...

[그림 3] DFC_NAS_03.E01 파일의 해시 값

분석 대상 파일에 대한 MD5 해시 값이 일치함을 확인하였습니다.

Synology 사의 NAS 제품들은 기본적으로 리눅스의 소프트웨어 RAID 관리 도구인 mdadm 을 사용하여 RAID 를 구성합니다.



[그림 4] 변환 과정

본 작업에서는 RAID 재구성을 위해 다음 과정을 수행했습니다. 먼저 FTK Imager 를 사용하여 E01 이미지를 dd 형식으로 변환했습니다. 이어서 qemu-img 도구로 dd 파일을 VMDK 파일로 변환했습니다. 마지막으로, VMware 의 Ubuntu 18.04 가상머신에서 RAID 재구성 작업을 수행하였습니다.

```
<raid path="/dev/md2" uuid="178d3e5f:99673cc1:5b3a0931:78f13f1b" level="raid6" version="1.2" layout="2">
  <disks>
    <disk status="normal" dev_path="/dev/sata1p3" physical_location="0-3" model="Blue SA510 2.5 250GB"
      serial="24022H441404" partition_version="9" partition_start="21241856" partition_size="466950496"
      slot="2">
    </disk>
    <disk status="normal" dev_path="/dev/sata2p3" physical_location="0-4" model="Blue SA510 2.5 250GB"
      serial="24022H441307" partition_version="9" partition_start="21241856" partition_size="466950496"
      slot="3">
    </disk>
    <disk status="normal" dev_path="/dev/sata3p3" physical_location="0-1" model="Blue SA510 2.5 250GB"
      serial="24022H440110" partition_version="9" partition_start="21241856" partition_size="466950496"
      slot="0">
    </disk>
    <disk status="normal" dev_path="/dev/sata4p3" physical_location="0-2" model="Blue SA510 2.5 250GB"
      serial="24022H441607" partition_version="9" partition_start="21241856" partition_size="466950496"
      slot="1">
    </disk>
  </disks>
</raid>
```

[그림 5] /etc/space/space_history_20240720_172830.xml 파일

RAID6 는 데이터 보호를 위해 이중 패리티 블록을 사용합니다. 데이터 스트라이핑과 두 개의 패리티 블록 유지를 위해 최소 4 개의 디스크가 필요합니다. 분석 대상 이미지에서도 RAID 생성 시 4 개의 디스크를 사용한 것으로 확인되었습니다.

```

root@ubuntu:/dev# mdadm --detail /dev/md2
/dev/md2:
    Version : 1.2
    Raid Level : raid0
    Total Devices : 3
    Persistence : Superblock is persistent

    State : inactive
    Working Devices : 3

    Name : DFC-NAS:2
    UUID : 178d3e5f:99673cc1:5b3a0931:78f13f1b
    Events : 22

    Number Major Minor RaidDevice
    -      -      -      -
    -      8       51     -      /dev/sdd3
    -      8       35     -      /dev/sdc3
    -      8       19     -      /dev/sdb3

```

[그림 6] 연결된 RAID 정보

앞서 생성한 VMDK 파일을 Ubuntu 가상머신에 연결했습니다. 생성된 RAID 파일의 정보를 확인한 결과, UUID 정보가 일치함을 확인했습니다. 또한, 디스크 한 개가 부족한 상태임을 파악하고 강제 재구성을 진행했습니다.

```

root@ubuntu:/dev# mdadm --assemble --run --force /dev/md2 /dev/sdd3 /dev/sdc3 /dev/sdb3
mdadm: /dev/md2 has been started with 3 drives (out of 4).

```

[그림 7] RAID 배열 강제 재구성

```

root@ubuntu:/dev# mdadm --detail /dev/md2
/dev/md2:
    Version : 1.2
    Creation Time : Sat Jul 20 17:28:29 2024
    Raid Level : raid6
    Array Size : 466948352 (445.32 GiB 478.16 GB)
    Used Dev Size : 233474176 (222.66 GiB 239.08 GB)
    Raid Devices : 4
    Total Devices : 3
    Persistence : Superblock is persistent

```

[그림 8] 재구성 완료 후 RAID 정보

3 개의 디스크만으로 RAID 재구성을 완료했습니다. 그러나 원래 4 개의 디스크로 구성된 RAID 6 를 3 개의 디스크로 재구성하면 이중 패리티 보호 기능이 상실됩니다. 이로 인해 한 개의 디스크 고장만 복구할 수 있다는 제한이 생깁니다.

1. What is the manufacturer and product name of the NAS from which the given image was collected? (10 points)

```
upnpdevicetype="Synology NAS"
upnpfriendlyname="Synology NAS Device"
upnpmanufacturerurl="http://www.synology.com/"
upnpmodeldescription="Synology NAS UPnP Device"
upnpmodelname="DS423+"
```

[그림 9] /etc/synoinfo.conf 파일

```
2024-07-20T01:06:00-07:00 SynologyNAS kernel: [ 70.205405] Brand: Synology
2024-07-20T01:06:00-07:00 SynologyNAS kernel: [ 70.208520] Model: DS-423+
```

[그림 10] /var/log/messages 파일

제조사와 제품명은 위의 그림에서 볼 수 있듯이 시스템 내 여러 경로에서 확인할 수 있습니다.

Manufacturer: Synology

Product Name of the NAS: DS423+

2. What is the ID and email address of the account currently active on the NAS? (10 points)

```
##$_@UID__INDEX@_$_1026$
admin:0:
butfit:0:7emp0rary@gmail.com
```

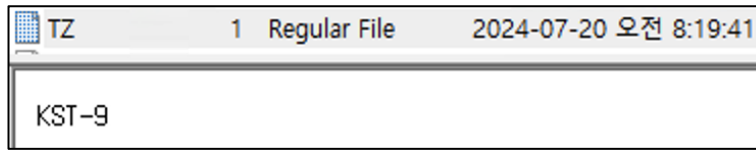
[그림 11] /etc/synouser.info 파일

사용자의 ID와 Email 정보는 "/etc/synouser.info"에서 확인할 수 있습니다.

ID: butfit

Email Address: 7emp0rary@gmail.com

3. When was the RAID created? (UTC+0) (10 points)



[그림 12] /etc/TZ 파일

```
root@ubuntu:~# mdadm --detail /dev/md2
/dev/md2:
    Version : 1.2
    Creation Time : Sat Jul 20 17:28:29 2024
    Raid Level : raid6
    Array Size : 466948352 (445.32 GiB 478.16 GB)
    Used Dev Size : 233474176 (222.66 GiB 239.08 GB)
    Raid Devices : 4
    Total Devices : 3
    Persistence : Superblock is persistent
```

[그림 13] RAID 생성 시각(KST)

```
var > log > ≡ space_operation.log
1 2024-07-20T17:28:29+09:00 DFC-NAS synoscgi_SYNO.Storage.CGI.Volume_1_create[19943]
2 2024-07-20T17:28:29+09:00 DFC-NAS synoscgi_SYNO.Storage.CGI.Volume_1_create[19964]
3 2024-07-20T17:28:29+09:00 DFC-NAS synoscgi_SYNO.Storage.CGI.Volume_1_create[19967]
4 2024-07-20T17:28:29+09:00 DFC-NAS synoscgi_SYNO.Storage.CGI.Volume_1_create[19965]
5 2024-07-20T17:28:29+09:00 DFC-NAS synoscgi_SYNO.Storage.CGI.Volume_1_create[19969]
6 2024-07-20T17:28:29+09:00 DFC-NAS synoscgi_SYNO.Storage.CGI.Volume_1_create[19964]
7 2024-07-20T17:28:29+09:00 DFC-NAS synoscgi_SYNO.Storage.CGI.Volume_1_create[19965]
8 2024-07-20T17:28:29+09:00 DFC-NAS synoscgi_SYNO.Storage.CGI.Volume_1_create[19967]
9 2024-07-20T17:28:29+09:00 DFC-NAS synoscgi_SYNO.Storage.CGI.Volume_1_create[19969]
```

[그림 14] /var/log/space_operation.log 파일

분석 대상 이미지는 KST(UTC+9)를 사용하고 있었습니다. 정확한 시간 분석을 위해 분석용 우분투 가상머신에도 동일한 타임존을 적용하여 진행하였습니다.

mdadm 도구로 앞서 재구성한 RAID의 생성 시각을 확인한 결과, 2024년 7월 20일 17:28:29에 생성되었음을 알 수 있었습니다. 또한, 그림 14의 파일에서 RAID 생성 당시 발생한 로그들을 확인할 수 있었습니다

답: 2024-07-20 08:28:29 (UTC+0)

4. What is the RAID level? (10 points)

```
etc > space > space_history_20240720_175014.xml
1  <?xml version="1.0" encoding="UTF-8"?>
2  <spaces>
3    <space path="/dev/vg1" reference="@storage_pool" uuid="GfJd8I-E2t5-5gHY-kCS9-dfb1-IZ5R-ukNVLt" device_type="2"
      drive_type="1" container_type="2" limited RAIDgroup_num="24" space_id="reuse_1" >
4      <device>
5        <lvm path="/dev/vg1" uuid="GfJd8I-E2t5-5gHY-kCS9-dfb1-IZ5R-ukNVLt" designed_pv_counts="1" status="normal"
          total_size="478150656000" free_size="322961408" pe_size="4194304" expansible="0" max_size="466948352">
6          <raids>
7            <raid path="/dev/md2" uuid="178d3e5f:99673cc1:5b3a0931:78f13f1b" level="raid6" version="1.2"
              layout="2">
8              <disks>
9                <disk status="normal" dev_path="/dev/sata1p3" physical_location="0-3" model="Blue SA510 2.5
                  250GB" serial="24022H441404" partition_version="9" partition_start="21241856"
                  partition_size="466950496" slot="2">
10               </disk>
11               <disk status="normal" dev_path="/dev/sata2p3" physical_location="0-4" model="Blue SA510 2.5
                  250GB" serial="24022H441307" partition_version="9" partition_start="21241856"
                  partition_size="466950496" slot="3">
12               </disk>
```

[그림 15] /etc/space/space_history_20240720_172830.xml 파일

```
root@ubuntu:~# mdadm --detail /dev/md2
/dev/md2:
    Version : 1.2
    Creation Time : Sat Jul 20 17:28:29 2024
    Raid Level : raid6
    Array Size : 466948352 (445.32 GiB 478.16 GB)
    Used Dev Size : 233474176 (222.66 GiB 239.08 GB)
    Raid Devices : 4
    Total Devices : 3
    Persistence : Superblock is persistent
```

[그림 16] mdadm으로 확인한 RAID level

그림 15의 파일은 RAID 생성 당시 발생한 로그를 보여주며, 여기서 raid6을 사용했음을 확인할 수 있습니다. 또한, mdadm 도구로 재구성한 RAID 장치에서도 raid6 사용을 확인할 수 있습니다.

답: raid6

5. What is the filesystem of the RAID volume you reconstructed? (10 points)

RAID 6	≥ 4	2	<ul style="list-style-type: none"> 데이터 패리티 레이어 두 개를 구현하여 드라이브 두 개 크기와 동일한 중복 데이터를 저장하므로 RAID 5보다 데이터 중복 정도가 더 큼니다. 최대 1PB 크기의 Btrfs 볼륨 생성을 지원하며, 특정 Synology NAS 모델 및 특정 조건에서만 사용할 수 있습니다. 	(N - 2) x (가장 작은 드라이브 크기)
--------	----------	---	---	---------------------------

[그림 17] Synology사의 지식센터에서 안내하는 RAID 6 정보

```
root@ubuntu:/dev# cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
md2 : active raid6 sdc3[0] sdd3[3] sdb3[1]
      466948352 blocks super 1.2 level 6, 64k chunk, algorithm 2 [4/3] [UU_U]

unused devices: <none>
root@ubuntu:/dev# lvs
  LV          VG Attr      LSize   Pool Origin Data%  Meta%   Move Log Cpy%Sync Convert
syno_vg_reserved_area vg1 -wi-a----- 12.00m
volume_1      vg1 -wi-a----- 445.00g
```

[그림 18] RAID 배열 정보 및 LV 정보

```
root@ubuntu:/dev# ls -al /dev/vg1/
total 0
drwxr-xr-x  2 root root   80 Aug 30 12:45 .
drwxr-xr-x 19 root root 4300 Aug 30 12:45 ..
lrwxrwxrwx  1 root root    7 Aug 30 12:45 syno_vg_reserved_area -> ../dm-0
lrwxrwxrwx  1 root root    7 Aug 30 12:45 volume_1 -> ../dm-1
root@ubuntu:/dev# file -s /dev/dm-1
/dev/dm-1: BTRFS Filesystem label "2024.07.20-08:28:30 v69057", sectorsize 4096, nodesize 16384, leafsize 16384, UUID=4328681a-a687-41c2-87c6-937418fec657, 691269632/477815111680 bytes used, 1 devices
```

[그림 19] 파일 시스템 확인

md2 RAID 6 배열이 LVM을 통해 관리되고 있음을 확인했습니다. 해당 LVM 논리 볼륨인 volume_1이 /dev/dm-1 장치로 매핑되어 있었습니다. /dev/dm-1의 파일 시스템 타입을 확인한 결과, BTRFS가 사용되고 있음을 알 수 있었습니다. 이는 Synology사의 지식센터에서 제공하는 정보와 일치하는데, RAID 6에서 BTRFS 파일 시스템을 지원한다고 명시되어 있습니다.

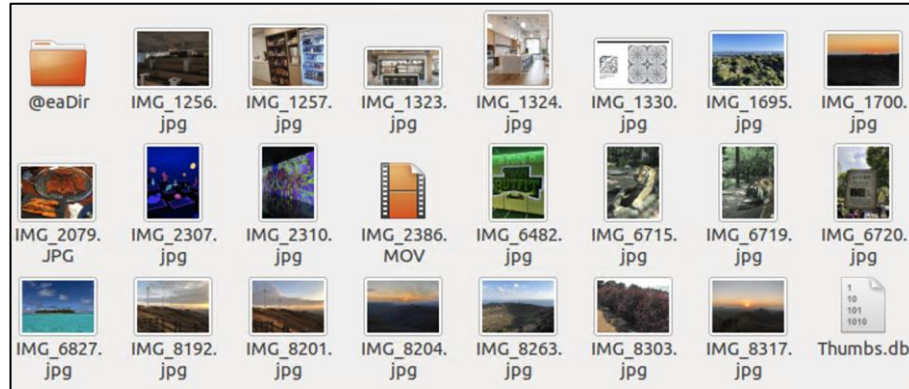
답: BTRFS

6. What are the MD5 hash values of the following two files? (100 points)

```
root@ubuntu:/home/ /Desktop# mount /dev/vg1/volume_1 /home/ /Desktop/volume_1 -o ro
```

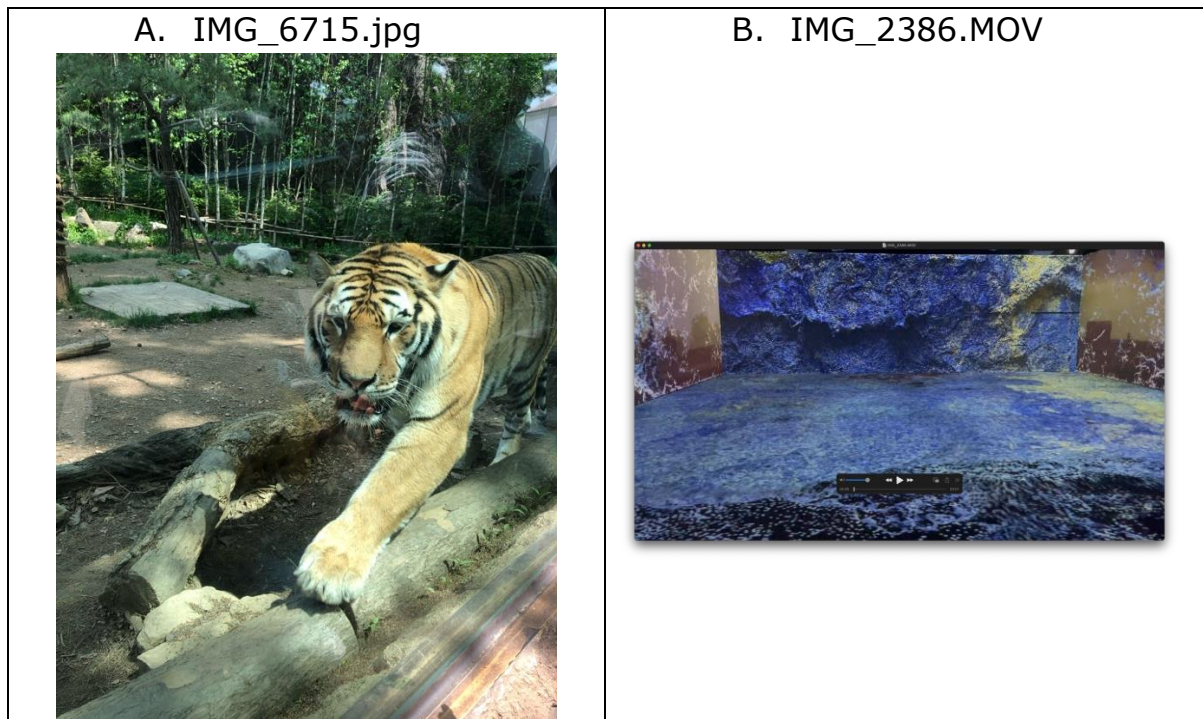
[그림 20] 볼륨 마운트

앞서 확인한 volume_1 논리 볼륨을 마운트하여 추가 분석을 진행했습니다.



[그림 21] /volume_1/homes/butfit/Photos 디렉토리

마운트된 볼륨에서 그림 21에 표시된 디렉토리 구조를 확인할 수 있었습니다.



[표 1] IMG_6715.jpg 파일, IMG_2386.MOV 파일

A. IMG_6715.jpg MD5: 601298440b6ff3ab9ee1117118f81d22

B. IMG_2386.MOV MD5: ce5cae8f320c402eabcda76667cda186

7. What picture files are deleted from a reconstructed RAID volume?
(50 points)



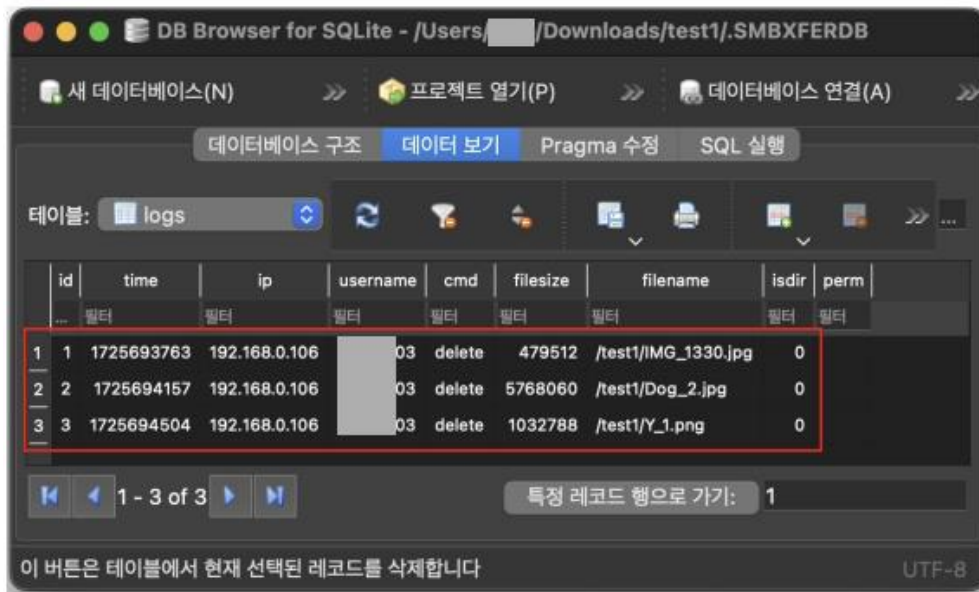
[그림 22] File Station 로깅 옵션

Synology NAS는 각 볼륨별로 File Station의 활동 로그를 기록하는 옵션을 제공합니다.

```
ash-4.4# pwd
/volume1/@database/synolog
ash-4.4# ls -al
total 528
drwxr-xr-x 1 system log      164 Sep  7 16:22 .
drwxr-xr-x 1 root  root     120 Dec 28  2023 ..
-rw-r--r-- 1 system log    4096 Sep  7 15:49 .DSMFMXFERDB
-rw-r--r-- 1 system log   32768 Sep  7 16:16 .DSMFMXFERDB-shm
-rw-r--r-- 1 system log  379072 Sep  7 16:16 .DSMFMXFERDB-wal
-rw-r--r-- 1 system log    4096 Sep  7 16:22 .SMBXFERDB
-rw-r--r-- 1 system log   32768 Sep  7 16:29 .SMBXFERDB-shm
-rw-r--r-- 1 system log   82432 Sep  7 16:29 .SMBXFERDB-wal
```

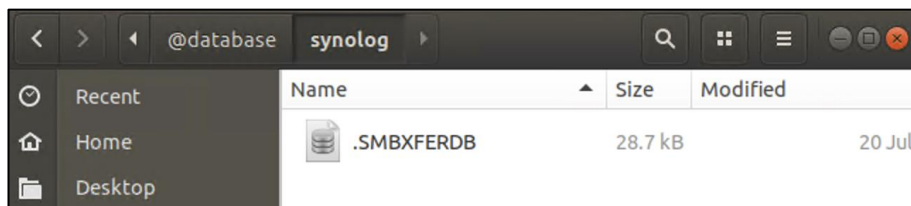
[그림 23] File Station SMB 서비스 로그 파일

이 옵션을 활성화하면, SMB 서비스를 통해 볼륨 내에서 파일 삭제와 같은 이벤트가 발생할 때 해당 정보가 [그림 23]의 파일에 기록됩니다.



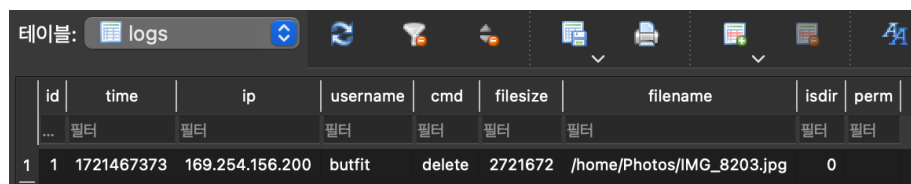
[그림 24] .SMBXFERDB 파일

해당 파일은 SQLite 데이터베이스 형식으로 저장되어 있습니다. 이 데이터베이스를 조회하면 위 그림과 같이 삭제된 파일들의 내역을 확인할 수 있습니다.



[그림 25] /volume_1/@database/synolog 디렉토리

앞서 분석한 방법을 적용하여, 마운트한 volume_1 볼륨의 synolog 디렉토리에서 상기 언급된 .SMBXFERDB 파일을 확인했습니다.



[그림 26] .SMBXFERDB

2024년 7월 20일 18시 22분 53초(UTC+09:00)에 butfit 사용자가 SMB 서비스를 통해 /home/Photos 디렉토리에서 IMG_8203.jpg 파일을 삭제한 것을 확인했습니다.

답: IMG_8203.jpg