

작성자	TEAM_C
분석 일자	2024.05.30~06.01
작성 일자	2024.06.01
분석 대상	4_QNAP_Disks.zip
문서 버전	1.0
작성자 E-mail	01star01ek@gmail.com

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3




4. Write-Up.....4

5. Flag.....7

6. 별도 첨부8

7. Reference9

1. 문제

URL	-
문제 내용	<p>증거 항목 4 – 4_QNAP_Disks</p> <p>이전에 압수된 증거에 대한 법의학적 분석을 바탕으로 ICC 단지의 제네바에서 관심 장소가 확인되었습니다. 2021년 4월 29일, 제네바 주 경찰은 그 장소를 수색하여 현장에 있던 M. Johann Schmidt를 체포했고, 그들은 3개의 드라이브가 장착된 QNAP NAS를 압수했습니다. 그들은 NAS가 통신 시스템을 호스팅하는 데 사용되었을 수도 있다고 생각합니다. NAS를 종료한 후, Sharepoint에서 개별적으로 다운로드할 수 있는 3개의 드라이브에 대한 물리적 포렌식 복사본을 모두 구입했습니다:</p> <p>시스템을 분석하려면 RAID 어레이의 재구성을 수행해야 할 수도 있습니다.</p>
문제 파일	<div>    </div> <div> 21APR_245-P001.0 21APR_245-P001.0 21APR_245-P001.0 1.E01 2.E01 3.E01 </div>
문제 유형	Drive forensic
난이도	3 / 3

2. 분석 도구

도구명	다운로드 링크	Version
FTK imager	https://www.exterro.com/digital-forensics-software/ftk-imager	4.7.1.2
ufs explorer raid recovery	https://apps.microsoft.com/detail/xp8k0hlc0f0f6g?hl=ko-KR&gl=US	-

3. 환경

OS
Windows 11 Home

4. Write-Up

파일명	4_QNAP_Disks.zip
용량	21.3GB
SHA256	1b30b9e1f2f6b28e2043323ea1892b088a6ebcb9f2b22f5195fce4d605730525
Timestamp	2024-05-30 01:59:10

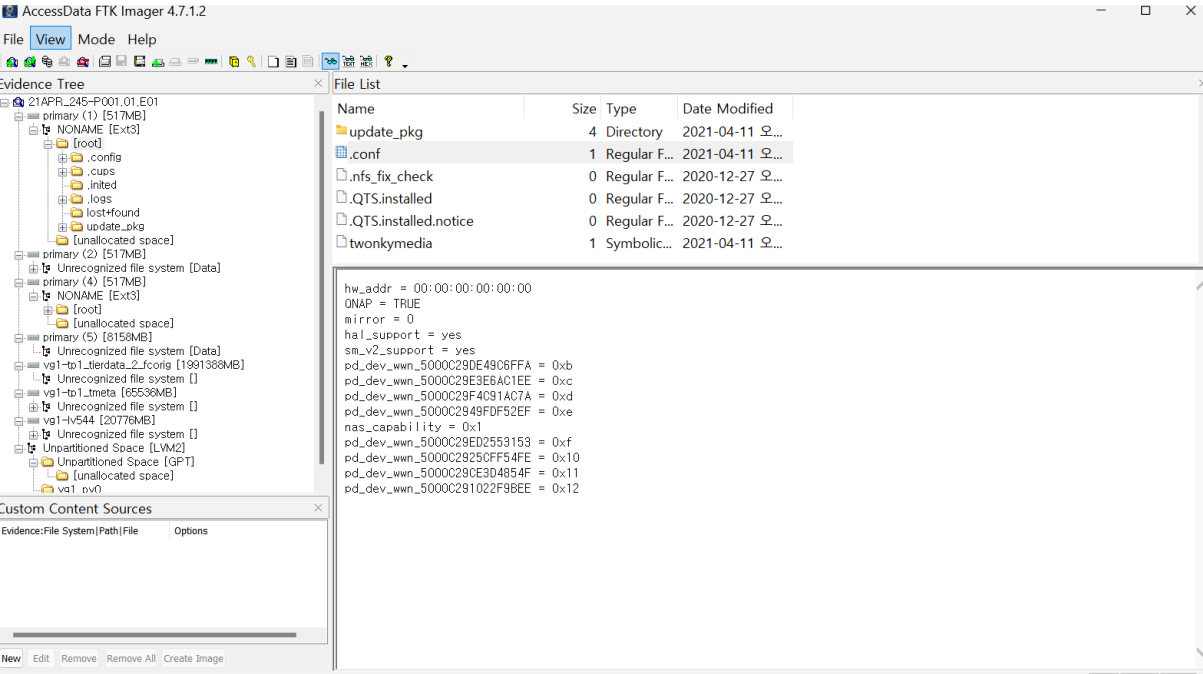
1. 문제 및 파일 파악

먼저 QNAP NAS 라는 이름이 생소하기에 이를 파악하였다. 찾아보니 고품질 네트워크 장비 제공업체에서 제공하는 네트워크 부착 스토리지로써 사진, 비디오, 음악 및 문서와 같은 디지털 파일을 수용하는 데이터 저장 장치를 의미하였다. 또한 RAID 는 여러 드라이브를 하나의 논리적 저장 장치로 결합하여 데이터 손실을 방지할 수 있는 메커니즘을 의미한다고 한다.

주어진 문제 지문을 토대로 생각해보면 3 가지의 디스크를 이용하여 RAID 어레이를 재구성하여 하나의 논리적 드라이브로 결합하는 것이 해결책이겠구나 추측할 수 있었다.

먼저 QNAP 를 직접 설치해보고 이용해보려고 하니 특정 기계가 있어야 가능해 불가능했다.

따라서 일단은 주어진 파일을 분석해보고자 했다.



[사진 1] FTK imager로 열어본 21APR_245-P001.01.E01

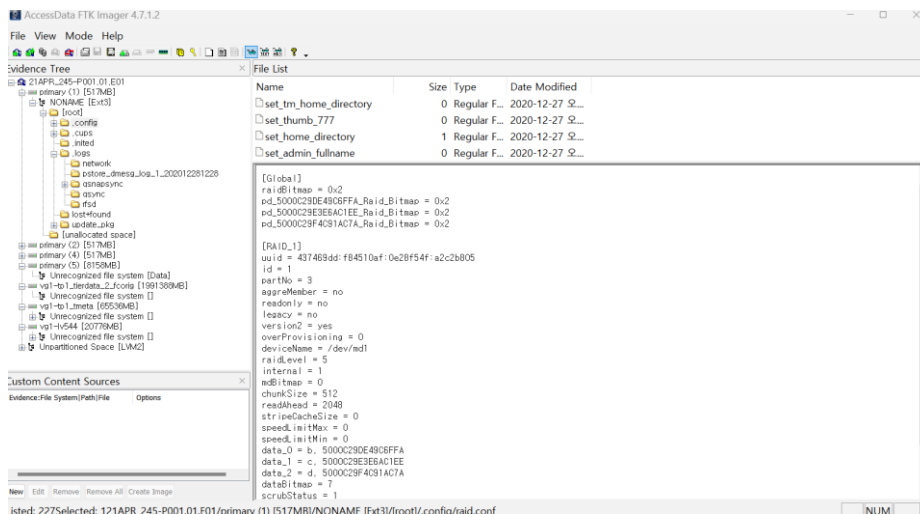
먼저, 21APR_245-P001.01.E01 파일을 FTK imager 로 열어보며 여러 기록들을 확인하던 중 primary – NONMAE – root – conf 에서 QNAP 와 관련된 기록들을 확인 할 수 있었다. 해당 파일은 QNAP

[WHS-2] .iso

NAS 장치의 하드웨어 설정과 디스크 구성 정보를 제공하는 파일로 QNAP = TRUE 라고 되어있기에 이는 **QNAP NAS 장치임을 파악할 수 있다.** 이후에 21APR_245-P001.02.E01 과 21APR_245-P001.03.E01 에서도 같은 경로에 같은 내용의 파일이 발견되었다. 즉 동일한 유형의 장비에서 사용되었음을 나타내는 것이다.

따라서 일전에 추측했던 대로 생각해 보면 3 가지의 디스크를 이용하여 RAID 어레이를 재구성하는 것이 맞겠구나 확신을 가지게 됐다. 이를 위하여 현재 NAS 가 어떠한 RAID 를 사용한건지, 드라이브 순서는 어떻게 되는지 확인하고자 했다.

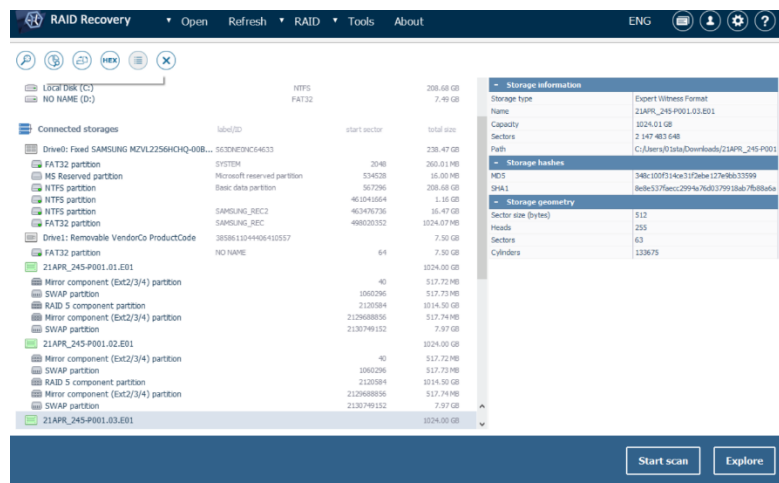
2. Raid 관련 정보 파악



[사진 2] raid.conf 에서 확인한 raid 관련 정보

이를 통해 RAID 5유형을 사용하며 data 0~2를 사용함을 알 수 있다. 일전에 말했던 것과 동일하게 21APR_245-P001.02.E01과 21APR_245-P001.03.E01 에서도 같은 경로에 같은 내용의 파일이 발견되었다.

3. RAID 재구성 시도

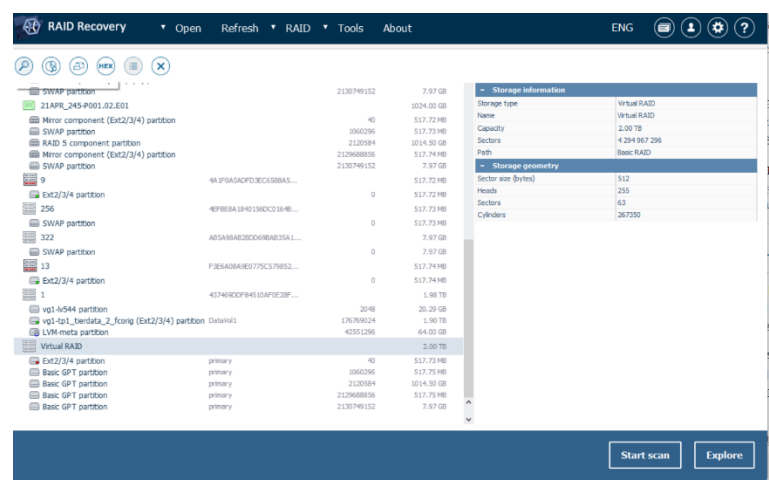


[사진 3] USE Explorer RAID Recovery에 올린 .e01 파일

[WHS-2] .iso

USE Explorer RAID Recovery 에 각각의 파일들을 올린뒤 RAID 재구성을 시도하였다.

순서는 파일명 순으로 하되 아닐 수 있기에 모든 경우를 다 시도해보았다.



[사진 4] RAID를 재구성했을 때의 모습

그러나 안타깝게도 모든 경우들이 다 에러가 발생하였다. 이에 따라 추가적인 정보 수집 및 분석이 필요하다고 생각되었다.

5. Flag

6. 별도 첨부

- 원본 영문 문제

Evidence Item 4 – 4_QNAP_Disks

Based on forensic analysis of previously seized evidence, a location of interest was identified in Geneva at the ICC complex.

On April 29th, 2021, the Geneva state police searched the location and arrested M. Johann Schmidt who was on site, and they seized a QNAP NAS with 3 drives.

They think that the NAS might also have been used to host a communication system.

After shutting down the NAS, they acquired physical forensic copies for all 3 drives, which are available for download individually from Sharepoint:

Filename	MD5 Hash (file)
<u>21APR_245-P001.01.E01</u>	805d0f5fe85a543d3b47b137c26aeb9a
<u>21APR_245-P001.02.E01</u>	296cc86fe5c5db4233771dced33f3985
<u>21APR_245-P001.03.E01</u>	d493d4350c10c274252e59db698745ee

A Zip files of all 3 E01 files is also available (SHA2-256:

1b30b9e1f2f6b28e2043323ea1892b088a6ebcb9f2b22f5195fce4d605730525).

Reconstruction of the RAID array might have to be performed in order to analyze the system.

7. Reference

- QNAP 및 관련 용어 소개 사이트
<https://www.qnap.com/ko-kr/about-qnap>