201 – Log and Found

Team Information

Team Name: kimbabasaksaksak

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

Email Address : uaaoong@gmail.com

Instructions

Description Kate is a server administrator at a fashion design company and recently underwent an internal audit within the company due to an incident where design files stored on the server were leaked. The company has requested a digital forensics analysis of the server's volume to resolve this issue. Please provide the analysis results for each question.

Target	Hash (MD5)
draft_server.001	4e6354ddcf52c2f0e436c60f2c5878ac

Questions

1) List the original and changed file names of the renamed files. (50 points)
2) List the file names of the deleted files. (50 points)
3) Provide the deleted time for each file. (100 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:	R-STUDIO Technician	Publisher:	R-Tools Technology
Version:	9.2.191153		
URL:	www.r-studio.com		

Name:	Vmware Workstation	Publisher:	Vmware
Version:	16.2.5 build-20904516 Pro		
URL:	www.vmware.com/kr.html		

Name:	Windows Server 2022 ISO	Publisher:	Microsoft
Version:			
URL:	www.microsoft.com/ko-kr/evalcenter/download-windows-server-2022		

Name:	010 Editor	Publisher:	SweetScape Software
Version:	13.0.2		
URL:	www.sweetscape.com		

Step-by-step methodology:

※ Additional information

- 참고자료

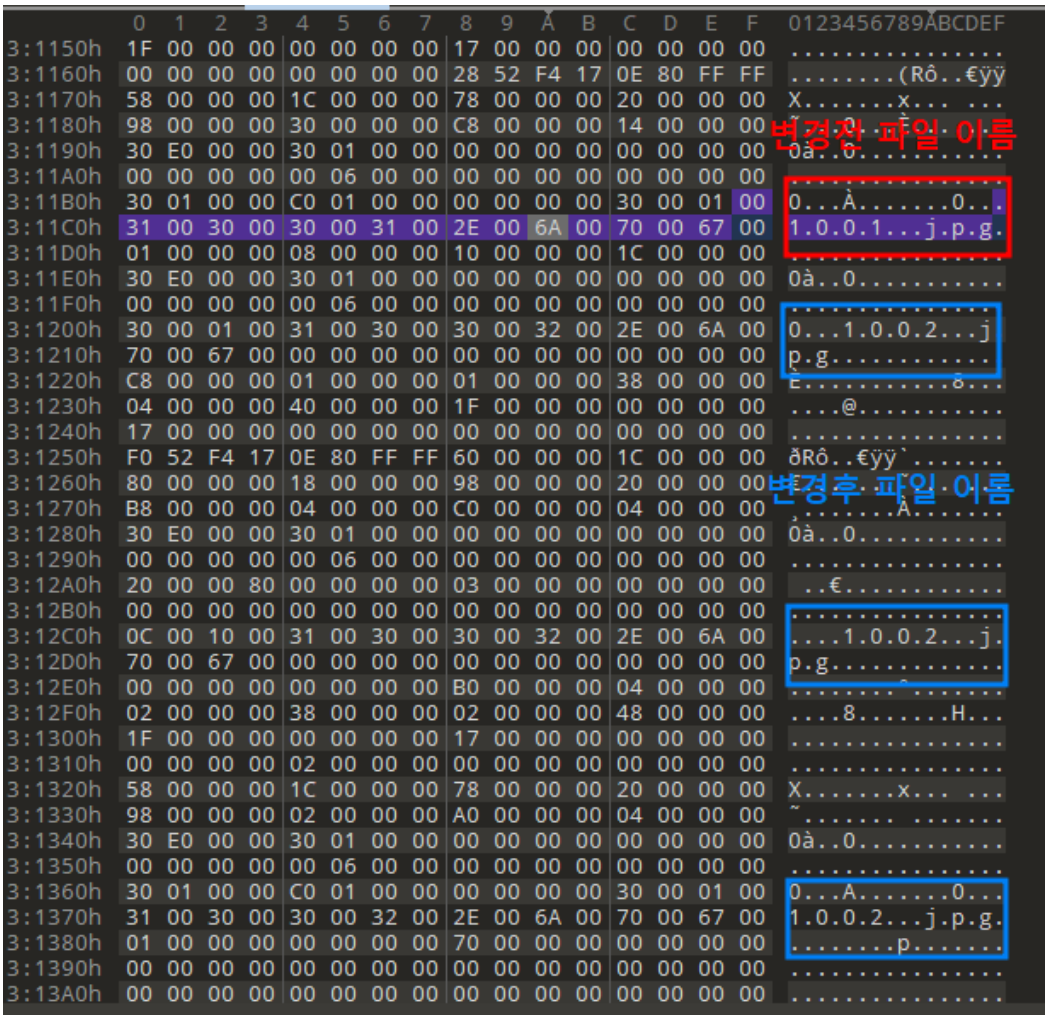
DFRWS APAC 2021 Author Preprint: Forensic Analysis of ReFS Journaling

- 테스트 환경

ReFS 파일시스템에서 파일 생성, 파일 이름 변경, 파일 삭제 이벤트 발생 시 $Logfile에 기록되는 데이터를 확보하기 위하여, Vmware에 Windows Server 2022를 설치하여 테스트를 진행했다. Windows Server 2022에서 1GB VHD 파일을 생성 후, ReFS 파일시스템으로 포맷하여 VHD 내에서 이벤트를 발생시켰다. 각 이벤트 별로 생성된 $Logfile 레코드들을 추출하여 본 문제에서 주어진 레코드들과 비교 분석하는데 사용하였다.

Q1. List the original and changed file names of the renamed files. (50 points)

ReFS 파일시스템 테스트 환경을 구축하여 파일 생성 및 파일 이름 변경 이벤트를 발생시킨 후, $Logfile을 분석하였다. 그 결과, 파일 이름이 변경되면, 변경전 파일 이름과 변경후 파일 이름이 하나의 Logfile Entry 내에 기록되는 특징을 발견했다.



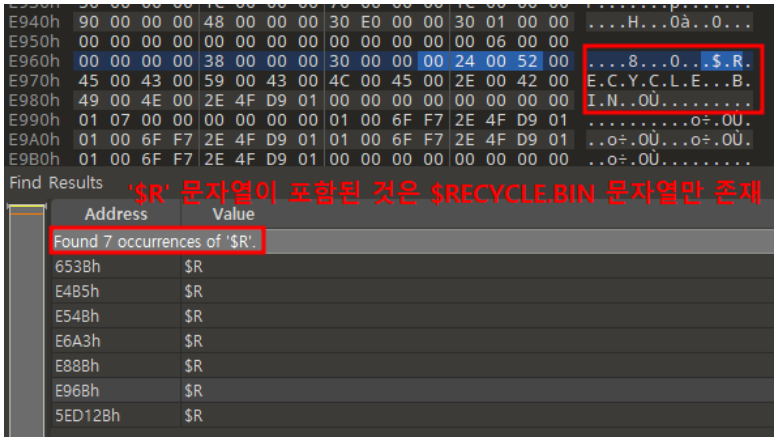
또한, 파일이 생성되고 추가 이벤트가 발생되지 않은 파일보다, 파일 이름 변경 이벤트가 발생한 파일이 $Logfile에 더 많은 파일 이름이 기록되어 있다는 특징이 있다. R-STUDIO 도구로 문제에서 주어진 이미지 파일에서 $Logfile 추출하여 분석한 결과, 파일이 생성되고 추가 이벤트가 발생하지 않은 파일은 $Logfile에 파일 이름이 10번 등장한다는 특징을 발견했다. 또한, 파일 이름 변경 이벤트가 발생한 파일은 $Logfile에 파일 이름이 11번 등장하는 특징을 발견했다.

앞서 언급한 특징들을 기반으로 $Logfile을 분석하여 파일 이름 변경 이력을 추적하였다.

변경전 파일명	변경후 파일명
1008022_B.jpg	1008023_B.jpg
1012200_B.jpg	1012201_B.jpg
1012211_B.jpg	1012210_B.jpg
1012343_B.jpg	1012341_B.jpg
1012377_B.jpg	1012378_B.jpg
1013282_B.jpg	1013283_B.jpg
1014097_B.jpg	1014098_B.jpg
1014179_B.jpg	1014180_B.jpg
1014394_B.jpg	1014398_B.jpg
1015100_B.jpg	1015101_B.jpg

Q2. List the file names of the deleted files. (50 points)

참고자료(Forensic Analysis of ReFS Journaling)를 확인하면, 파일 삭제는 휴지통으로 이동 후 삭제와 파일 완전 삭제로 구분해야 된다고 한다. 휴지통으로 이동 후 삭제되는 파일은 파일 이름이 $R로 시작되는 파일 이름으로 변경된다. 하지만, 문제에서 주어진 $Logfile에는 $R로 시작되는 파일 이름으로 변경된 기록이 존재하지 않는다. 그러므로 삭제된 모든 파일들은 완전 삭제되었음을 알 수 있다.



테스트 환경에서 파일을 완전 삭제한 후 $Logfile에 기록되는 패턴을 확인한 결과, 삭제된 파일과 관련된 Logfile Entry 중에서 가장 마지막에 생성된 Logfile Entry에는 파일 이름이 여러 번 기록되는 특징을 발견하였다.

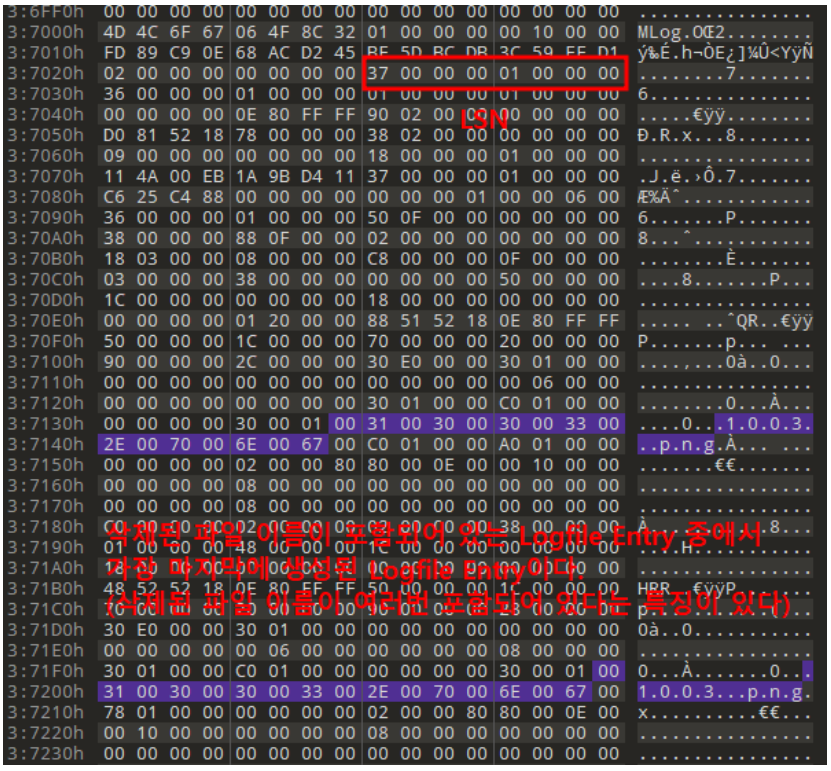
또한, 문제에서 주어진 $Logfile에서는 파일 완전 삭제 이벤트가 발생한 파일은 파일 이름이 14번 등장하는 특징을 발견했다.

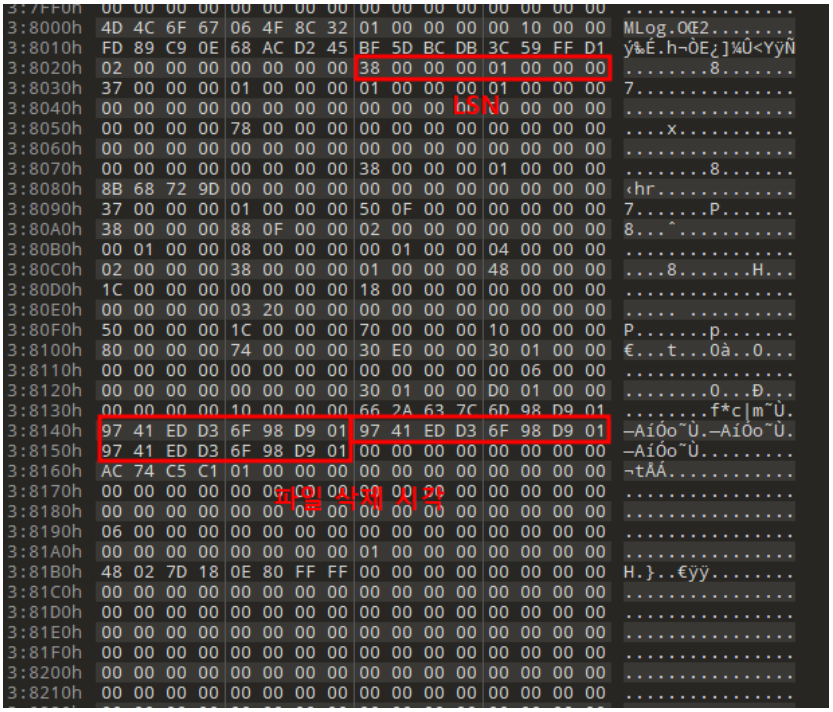
앞서 언급한 특징들을 기반으로 $Logfile을 분석하여 파일 삭제 이력을 추적하였다.

파일명	파일 삭제 유형
1008103_B.jpg	파일 완전 삭제
1012353_B.jpg	파일 완전 삭제
1013029_B.jpg	파일 완전 삭제
1013191_B.jpg	파일 완전 삭제
1014381_B.jpg	파일 완전 삭제

Q3. Provide the deleted time for each file. (100 points)

테스트 환경에서 파일을 완전 삭제한 후 $Logfile에 기록되는 데이터를 분석하여, 파일 삭제 시각이 기록되는 위치를 확인하였다. 파일 삭제 시각은 삭제된 파일 이름이 포함되어 있는 Logfile Entry 중에서 가장 마지막에 생성된 Logfile Entry의 바로 다음 Logfile Entry에 저장되어 있다.





앞서 언급한 내용들을 기반으로 $Logfile을 분석하여 파일 삭제 시각을 추적하였다.

파일명	파일 삭제 시각 (UTC+0)
1008103_B.jpg	2023-04-05 11:09:13
1012353_B.jpg	2023-04-05 11:08:43
1013029_B.jpg	2023-04-05 11:09:38
1013191_B.jpg	2023-04-05 11:08:17
1014381_B.jpg	2023-04-05 11:10:06