

문제 6.

6. 증거 사본에서 링크파일(.lnk)파일을 찾고 속성 정보를 기술하시오

- ① 원본파일의 용량 ② 원본파일 저장 경로 ③ 원본파일 시간정보
- ④ 원본파일이 저장되었던 볼륨의 시리얼번호

Autopsy를 활용하여 다음의 링크파일(.lnk)을 찾아 다음과 같은 메타데이터를 얻었다.

 매장보안시스템정보.xlsx - 바로 가기.lnk	0	f3cbaf1395ea0237111085ddad01
 매장보안시스템정보.xlsx - 바로 가기.lnk-slack		

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotate
Metadata								
Name:	/img_복구_022-2-1-168.001/vol_vol2/매장보안시스템정보.xlsx - 바로 가기.lnk							
Type:	File System							
MIME Type:	application/octet-stream							
Size:	972							
File Name Allocation:	Allocated							
Metadata Allocation:	Allocated							
Modified:	2022-10-19 13:32:22 KST							
Accessed:	2022-11-10 16:33:23 KST							
Created:	2022-11-10 16:33:23 KST							
Changed:	2022-10-19 13:32:22 KST							
MD5:	f3cbaf1395ea0237111085ddad001cd1							
SHA-256:	2ec063494476c4304ad7429b7d1bbd5229822b92152664af676988b9005d639							
Hash Lookup Results:	UNKNOWN							
Internal ID:	282							

다음은 해당 링크파일을 추출하여 LNK Parser를 이용해 분석한 결과이다.

LNK Parser							
C:\W\autopsy_case\Scenario2\W\Scenario2\W\Export\W\매장보안시스템정보.xlsx - 바로 가기.lnk							
		File		Folder			
LnkFileName	FileName	FilePath	FileSize(Byte)	TargetCreationTime	TargetAccessTime	TargetWriteTime	DriveSerialNumber
매장보안시스템정보.xlsx - 바로 가기.lnk	매장보안시스템정보.xlsx	H:\W\매장보안시스템정보.xlsx	8261	2022/10/19 13:31:46	2022/10/19 13:31:46	2022/10/19 13:30:42	6e496784

원본파일의 용량	8,261 (Bytes)
원본파일 저장 경로	H:\매장보안시스템정보.xlsx
원본파일 시간정보	TargetCreationTime : 2022-10-19 1:31:46 PM TargetAccessTime : 2022-10-19 1:31:46 PM TargetWriteTime : 2022-10-19 1:30:42 PM
원본파일이 저장되었던 볼륨의 시리얼번호	6e496784