102 – File Wiper

Team Information

Team Name : ForensicGPT

Team Member : Eungchang Lee, Donghyun HA, Hyunwoo Shin, Jinhyeok Son

Email Address : forensicgpt@googlegroups.com

Instructions

Description While analyzing the suspect's PC, I found that several files had been wiped. I need your help on what tool to use to wipe it.

Target	Hash (MD5)
2023-04-26T042142_DFC2023-102.7z	DD66FDC3156EBE961CEBF85E223D3B96

Questions

1) When was File Wiping Tool installed? (UTC+0) (50 points)
2) When was File Wiping Tool run? (UTC+0) (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:	FTK Imager	Publisher:	AccessData® FTK® Imager
Version:	4.7.1.2		
URL:	https://go.exterro.com/l/43312/2023-05-03/fc4b78		

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

Name:	Dcode	Publisher:	Digital Detective
Version:	5.5.21194.40		
URL:	https://www.digital-detective.net/dcode/		

Name:	VMware Workstation 17 Pro	Publisher:	VMware, Inc.
Version:	17.0.0 build-20800274		
URL:	https://www.vmware.com/		

VM(Test) PC used:

OS:	Windows 11 pro	Version:	22621.525
System Name:	DESKTOP-44TQ06L		

Step-by-step methodology:

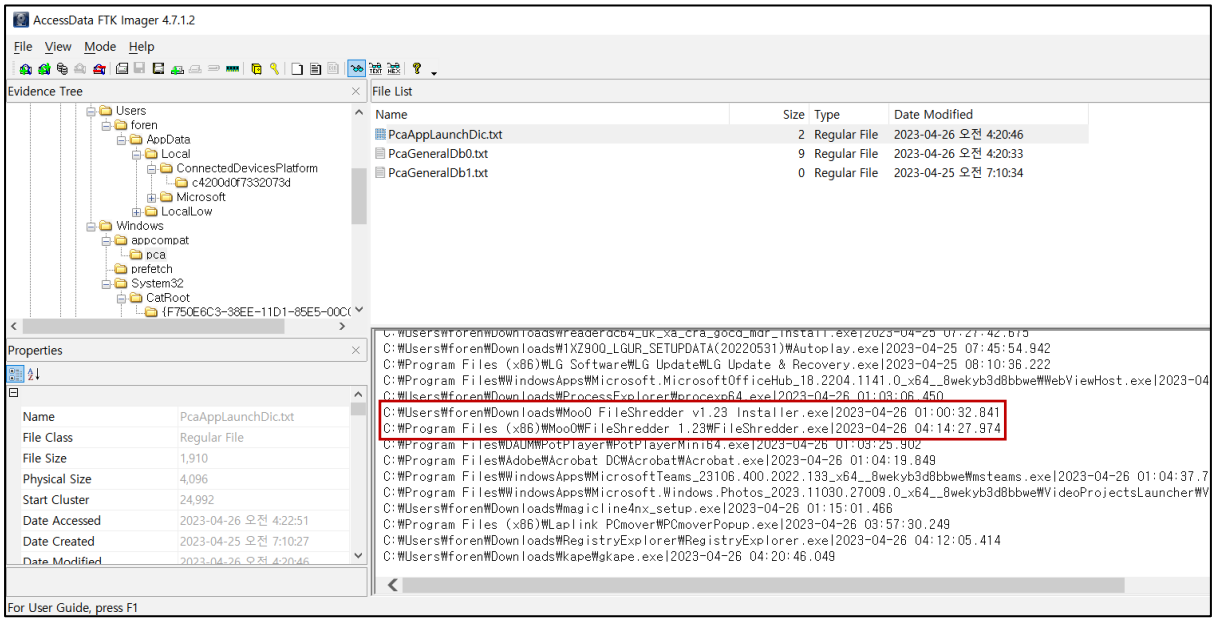
다운받은 7z파일을 압축해제 하게 되면 vhdx 파일을 획득할 수 있습니다. 해당 파일의 해시 값은 다음과 같습니다.

File Name	Hash Value
2023-04-26T042142_DFC2023-102.vhdx	MD5 : EF106327D96A8560C090A2B18C407644
	SHA-1 : 58D6B1F79394DC8FBF200EE06D28CE320B67B2A5

[표 1] vhdx 파일의 hash 값

1) When was File Wiping Tool installed? (UTC+0) (50 points)

File Wiping Tool이 설치된 흔적을 찾기 위해 FTK Imager 도구로 vhdx파일을 열어주었습니다. 명확하게 File wiping tool이 설치된 시각이 기록된 아티팩트를 찾기 위해 Windows\appcomat\pca 폴더에 생성되어 있는 PcaAppLaunchDic.txt를 발견할 수 있었습니다.

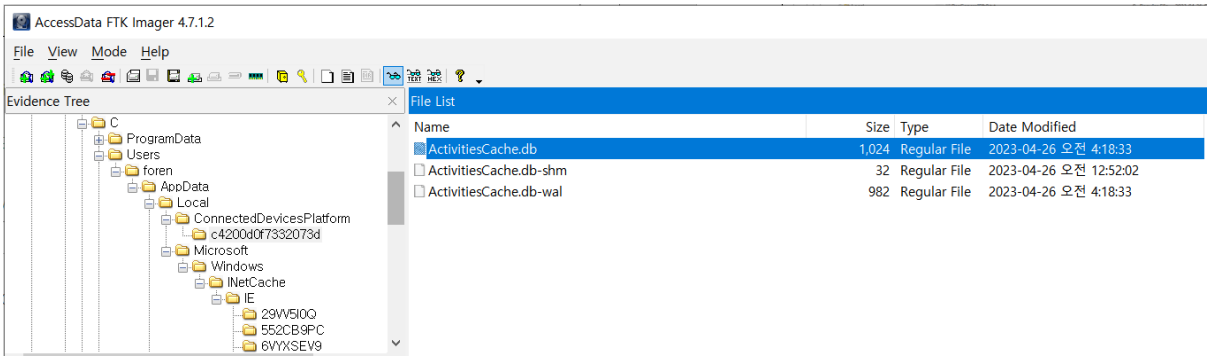


[그림 1] FTK Imager 도구로 살펴본 PcaAppLaunchDic.txt 내 File Wiping tool

PcaAppLaunchDic.txt 파일에서 Moo0 FileShredder v1.23 Installer.exe와 FileShredder.exe 에 대한 시간 정보가 기록되어 있는 것을 알 수 있습니다. appcompat의 pca 폴더는 Windows 11 의 22H2 버전부터 새롭게 추가된 아티팩트입니다. PcaAppLaunchDic.txt 에는 응용 프로그램의 마지막 실행 시간과 데이터의 파일 경로를 한 쌍으로 포함하고 있습니다. 해당 파일에 기록되는 시간 정보는 매번 응용프로그램을 실행할 때 마다 업데이트 되고, UTC+0 으로 기록됩니다.

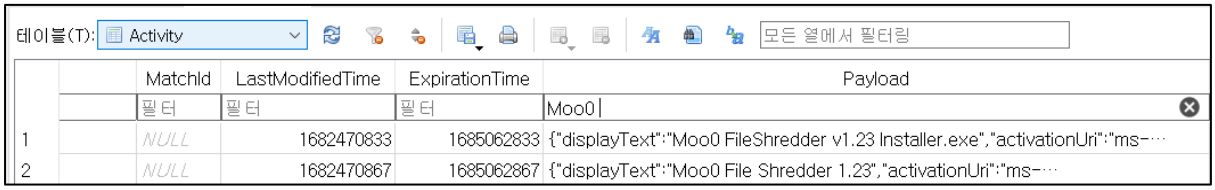
해당 아티팩트에서 File wiping tool로 의심되는 Moo0 FileShreadder v1.23 Installer.exe의 마지막 실행 시각은 **2023-04-26 01:00:32.841(UTC+0)**이며, FileShredder.exe의 마지막 실행 시각은 **2023-04-26 04:14:27.974(UTC+0)** 임을 확인할 수 있습니다.

cross-check를 위해 다른 아티팩트도 살펴보았습니다.



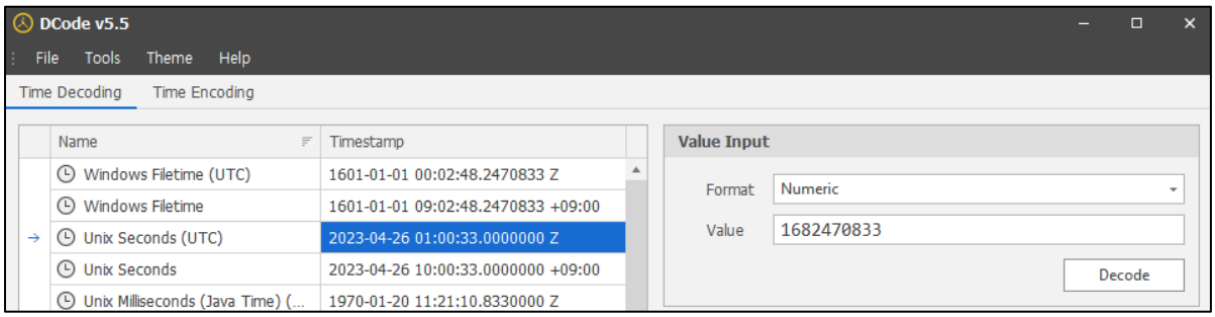
[그림 2] ActivitiesCache.db 파일 확인

Windows 11에서는 지원 중단되었지만 Windows 10에서는 현재 실행 중인 앱 및 지난 활동을 표시하는 ActivitiesCache.db 파일을 ConnectedDevicesPlatfotm\c4200d0f7332073d 경로에서 찾을 수 있었습니다.



[그림 3] ActivitiesCache.db 내 File wiping tool 실행중인 앱 시각 확인

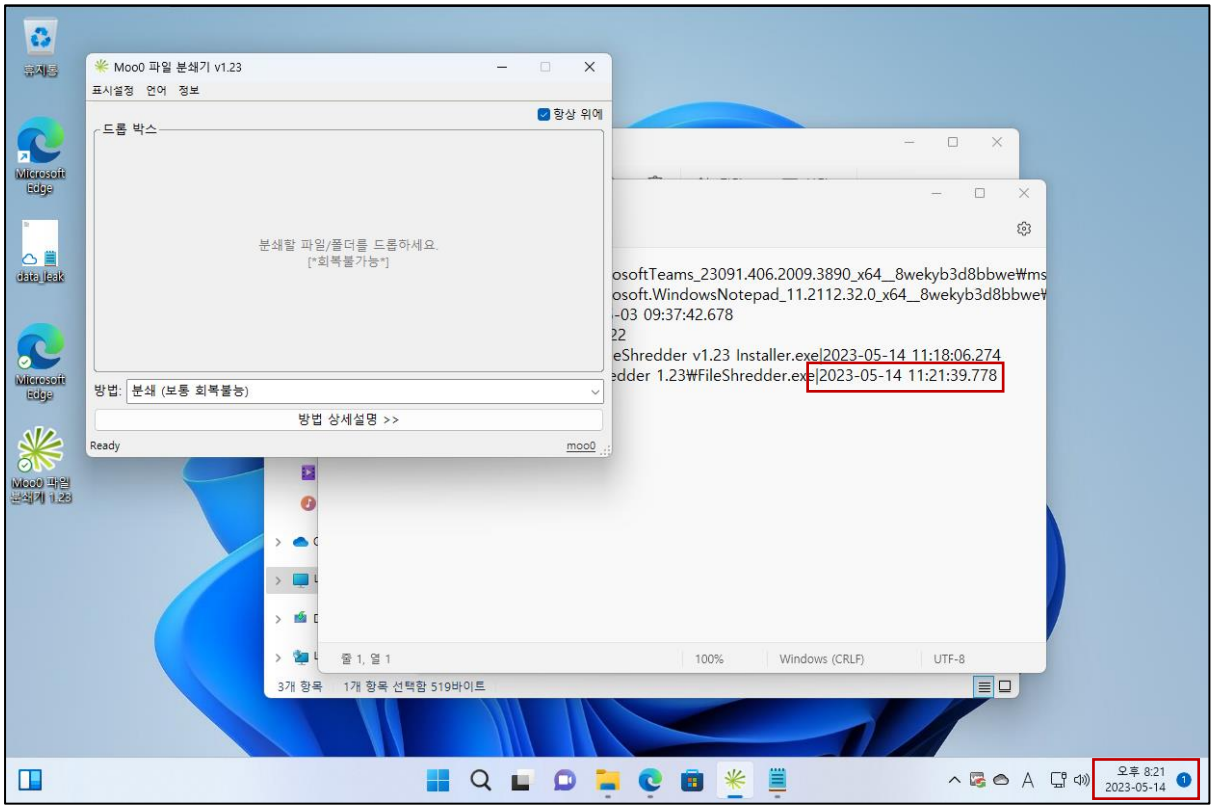
ActivitiesCache.db 내에서는 활동이 마지막으로 수정된 시간인 LastModifiedTime을 확인할 수 있습니다.



[그림 4] File wiping tool 설치 파일 활동 시각 변환

Moo0 FileShredder v1.23 Installer.exe의 last modified time이 1682470833인 것을 통해 Dcode 도구를 사용해서 Unix timestamp를 변환해주면 설치 파일 활동 시각이 2023-04-26 01:00:33.0000000(UTC+0) 이라는 것을 알 수 있습니다. 이를 통해, 앞서 살펴본 Pcaapplaunchdic.txt 파일에서 기록된 마지막 실행 시각보다 이후라는 점을 확인할 수 있습니다.

또한, Windows 11을 VMware 가상환경에서 구동하여 의심되는 file wiping tool을 실행해보면서 pcaapplaunchdic.txt가 실시간으로 변경되는 것을 확인할 수 있었습니다.



[그림 5] 가상환경 상에서 재현 테스트

따라서, 지금껏 살펴본 흔적과 재현 테스트를 통해 도출한 1번 문제의 답은 다음과 같다고 판단하는 바입니다.

File Name	Install time
Moo0 FileShredder v1.23 Installer.exe	2023-04-26 01:00:32.841(UTC+0)

[표 2] File wiping tool 설치 시각

2) When was File Wiping Tool run? (UTC+0) (50 points)

2번 문제는 File wiping tool 실행 시각을 묻는 문제입니다. 앞서 살펴본 ActivitiesCache.db에서는 도구 활동 시각이 1682470867로 이는 2023-04-26 01:01:07.0000000 Z(UTC+0)을 나타내고 있습니다. 하지만, pcaapplaunchdic.txt 에 기록된 file wiping tool의 마지막 실행 시각은 2023-04-26 04:14:27.974(UTC+0)으로 그 이후를 나타내고 있습니다.

ActivitiesCache.db에 기록된 시각은 Installer 상에서 설치 후 "지금 실행하기" 옵션이 선택되어 file wiping tool이 실행되었기 때문에 설치 시각과 비슷하게 도구 활동 시각이 기록되었다고 추측됩니다. 또한, 실행 시각 증거가 아닌 실행중인 도구의 활동 시각 증거이기 때문에 정확한 답이 아니라고 판단하였습니다. 같은 맥락으로 ActivitiesCache.db에 존재하는 "sdelete64" wiping tool 활동 시각도 문제의 답에서 배제할 수 있었습니다.

따라서, 앞서 1번 문제에서 답으로 채택한 pcaapplaunchdic.txt 아티팩트 증거와 file wiping tool을 Moo0 fileshredder v1.23으로 판단한 점에 기반하여 2번 문제의 답도 해당 증거에 따라 다음과 같은 판단을 내렸습니다.

File Name	Install time
FileShredder.exe	**2023-04-26 04:14:27.974(UTC+0)**

[표 3] File wiping tool 실행 시각