102 – File Wiper

Team Information

Team Name: kimbabasaksaksak

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

Email Address: uaaoong@gmail.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:

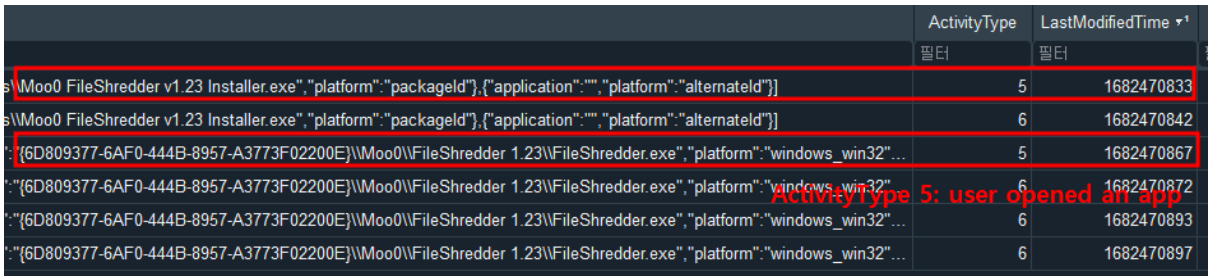
Name:	FTK Imager	Publisher:	exterro
Version:	4.5.0.3		
URL:	https://www.exterro.com/ftk-imager		

Name:	DB Browser for SQLite	Publisher:	sqlitebrowser
Version:	4.5.0.3		
URL:	https://sqlitebrowser.org		

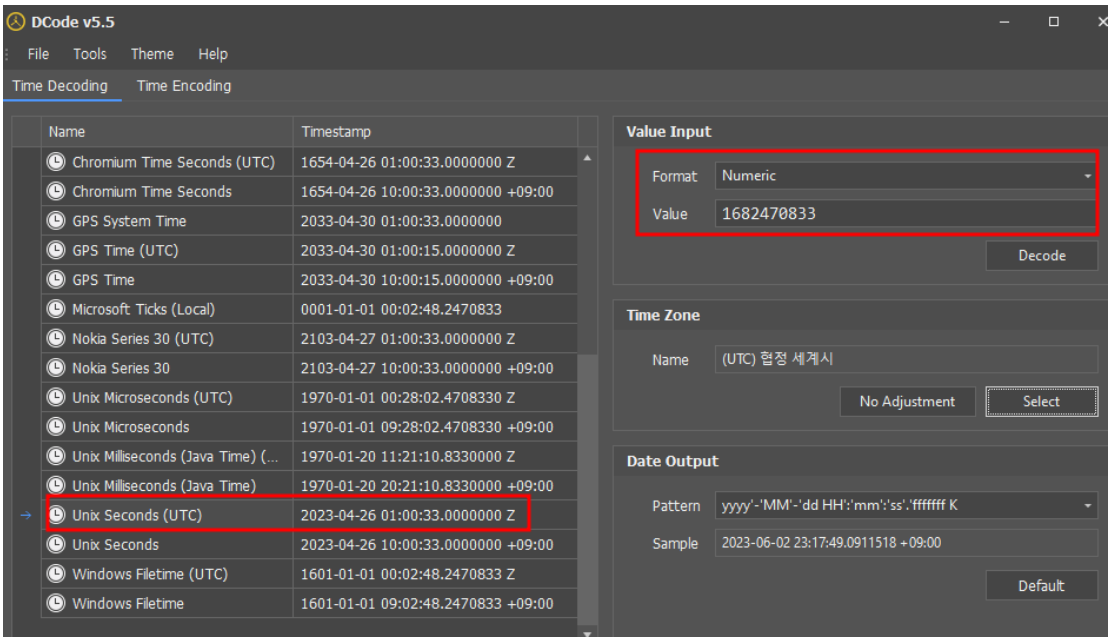
Step-by-step methodology:

Q1. When was File Wiping Tool installed? (UTC+0) (50 points)

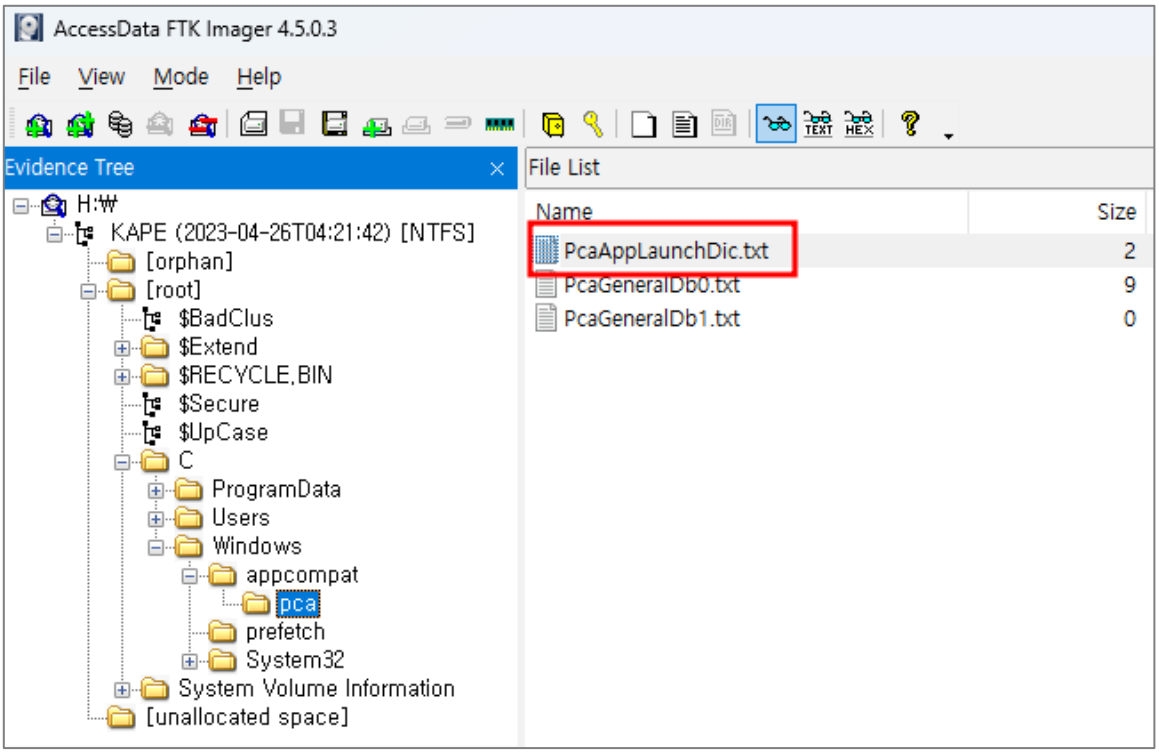
윈도우 타임라인 아티팩트인 '₩Users₩foren₩AppData₩Local₩ConnectedDevicesPlatform₩c4200d0f7332073d₩ActivitiesCache.db'를 분석한 결과, 파일 와이핑 도구 'Moo0 FileShredder v1.23'가 설치되고 실행되었던 것을 확인할 수 있다.



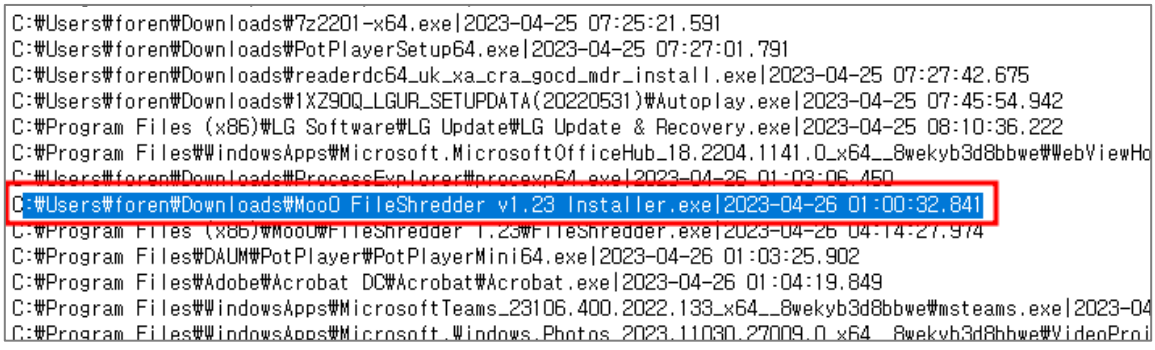
'Moo0 FileShredder v1.23' 설치 파일인 'Moo0 FileShredder v1.23 Installer.exe'가 실행된 시각은 윈도우 타임라인 아티팩트 상에서는 **'2023-04-26 01:00:33 UTC+0'**로 확인된다.



또한, 파일 실행 시각은 PCA 아티팩트인 '₩Windows₩appcompat₩pca₩PcaAppLaunchDic.txt'에서도 확인할 수 있다. 해당 파일은 지정된 응용 프로그램의 마지막 실행 시각을 제공한다.

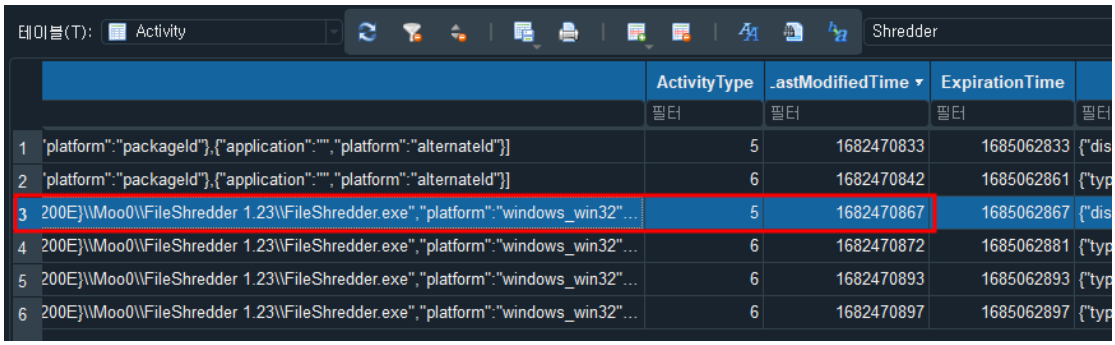


'pcaAppLaunchDic.txt' 파일을 확인한 결과, 'Moo0 FileShredder v1.23 Installer.exe'가 실행된 시각은 윈도우 타임라인 아티팩트에서 확인한 시각과 일치하는 '**2023-04-26 01:00:32.841 UTC+0**'로 확인된다.

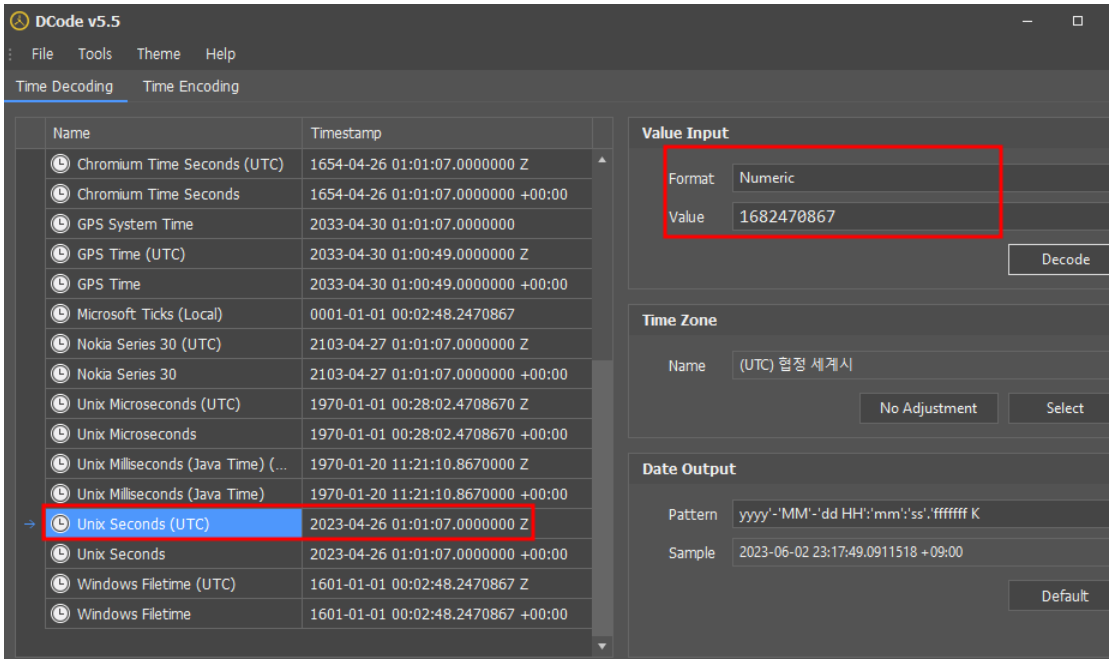


Q2. When was File Wiping Tool run? (UTC+0) (50 points)

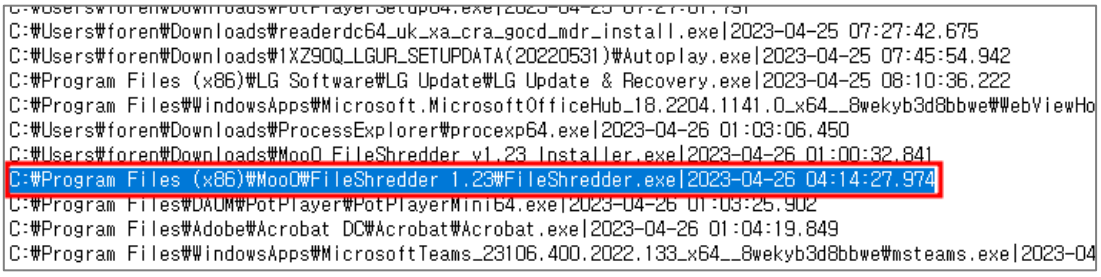
윈도우 타임라인 상에서 'Moo0 FileShredder v1.23'가 실행된 시각은 '2023-04-26 01:01:07 UTC+0'이다. 이 시각은 'Moo0 FileShredder v1.23'가 설치된 직후 시각이므로, 설치 프로그램에서 '설치 완료 후 응용 프로그램 시작' 옵션이 체크되어 실행된 것으로 추정된다.



		ActivityType	LastModifiedTime	ExpirationTime	
		필터	필터	필터	필터
1	'platform":"packageId"},{"application":"","platform":"alternateId"}]	5	1682470833	1685062833	{"dis
2	'platform":"packageId"},{"application":"","platform":"alternateId"}]	6	1682470842	1685062861	{"typ
3	200E}\\Moo0\\FileShredder 1.23\\FileShredder.exe","platform":"windows_win32"...	5	1682470867	1685062867	{"dis
4	200E}\\Moo0\\FileShredder 1.23\\FileShredder.exe","platform":"windows_win32"...	6	1682470872	1685062881	{"typ
5	200E}\\Moo0\\FileShredder 1.23\\FileShredder.exe","platform":"windows_win32"...	6	1682470893	1685062893	{"typ
6	200E}\\Moo0\\FileShredder 1.23\\FileShredder.exe","platform":"windows_win32"...	6	1682470897	1685062897	{"typ



또한, 'pcaAppLaunchDic.txt' 파일을 확인하면 'Moo0 FileShredder v1.23'가 추가로 실행된 시각을 확인할 수 있다. 'Moo0 FileShredder v1.23'가 실행된 시각은 '**2023-04-26 04:14:27.974 UTC+0**'이다. 이는 사용자가 파일 와이핑을 진행하기 위해 실행한 시각으로 추정된다.



```
C:¥Users¥foren¥Downloads¥readerdc64_uk_xa_cra_gocd_mdr_install.exe|2023-04-25 07:27:42.675
C:¥Users¥foren¥Downloads¥1XZ90Q_LGUR_SETUPDATA(20220531)¥Autoplay.exe|2023-04-25 07:45:54.942
C:¥Program Files (x86)¥LG Software¥LG Update¥LG Update & Recovery.exe|2023-04-25 08:10:36.222
C:¥Program Files¥WindowsApps¥Microsoft.MicrosoftOfficeHub_18.2204.1141.0_x64__8wekyb3d8bbwe¥WebViewHo
C:¥Users¥foren¥Downloads¥ProcessExplorer¥procexp64.exe|2023-04-26 01:03:06.450
C:¥Users¥foren¥Downloads¥Moo0_FileShredder_v1.23_Installer.exe|2023-04-26 01:00:32.841
C:¥Program Files (x86)¥Moo0¥FileShredder 1.23¥FileShredder.exe|2023-04-26 04:14:27.974
C:¥Program Files¥DAUM¥PotPlayer¥PotPlayerMini64.exe|2023-04-26 01:03:25.902
C:¥Program Files¥Adobe¥Acrobat DC¥Acrobat¥Acrobat.exe|2023-04-26 01:04:19.849
C:¥Program Files¥WindowsApps¥MicrosoftTeams_23106.400.2022.133_x64__8wekyb3d8bbwe¥msteams.exe|2023-04
```