102 – File Wiper

Team Information

Team Name ____

Team Member ____

____

____

Email Address ____

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:

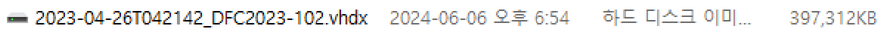
Name:		Publisher**:**	

Version:	
URL:	

Step-by-step methodology:

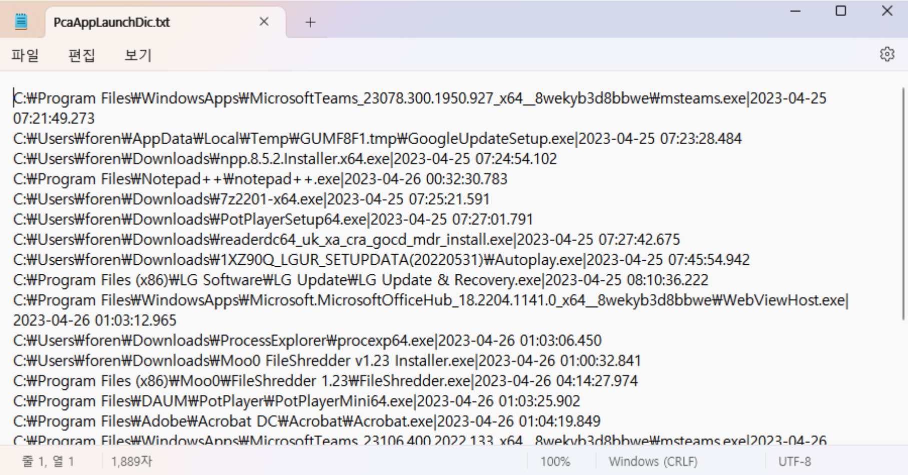
1. When was File Wiping Tool installed? (UTC+0) (50 points)

메모 포함[오전1]: 1.파일 와이핑 툴이 설치된 시간은 언제입니까? (UTC+0)



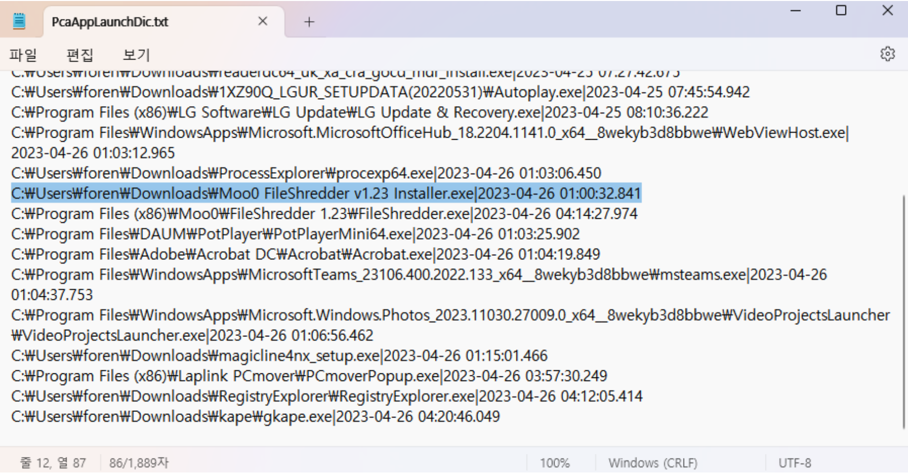
2023-04-26T042142_DFC2023-102.vhdx 2024-06-06 오후 6:54 하드 디스크 이미... 397,312KB

압축을 풀면 하드디스크 이미지가 나온다.



```
C:₩Program Files₩WindowsApps₩MicrosoftTeams_23078.300.1950.927_x64__8wekyb3d8bbwe₩msteams.exe|2023-04-25
07:21:49.273
C:₩Users₩foren₩AppData₩Local₩Temp₩GUMF8F1.tmp₩GoogleUpdateSetup.exe|2023-04-25 07:23:28.484
C:₩Users₩foren₩Downloads₩npp.8.5.2.Installer.x64.exe|2023-04-25 07:24:54.102
C:₩Program Files₩Notepad++₩notepad++.exe|2023-04-26 00:32:30.783
C:₩Users₩foren₩Downloads₩7z2201-x64.exe|2023-04-25 07:25:21.591
C:₩Users₩foren₩Downloads₩PotPlayerSetup64.exe|2023-04-25 07:27:01.791
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₩WebViewHost.exe|
2023-04-26 01:03:12.965
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|2023-04-26
```

D:₩C₩Windows₩appcompat₩pca₩PcaAppLaunchDic.txt를 확인하였다.



```
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₩WebViewHost.exe|
2023-04-26 01:03:12.965
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|2023-04-26
01:04:37.753
C:₩Program Files₩WindowsApps₩Microsoft.Windows.Photos_2023.11030.27009.0_x64__8wekyb3d8bbwe₩VideoProjectsLauncher
₩VideoProjectsLauncher.exe|2023-04-26 01:06:56.462
C:₩Users₩foren₩Downloads₩magicline4nx_setup.exe|2023-04-26 01:15:01.466
C:₩Program Files (x86)₩Laplink PCmover₩PCmoverPopup.exe|2023-04-26 03:57:30.249
C:₩Users₩foren₩Downloads₩RegistryExplorer₩RegistryExplorer.exe|2023-04-26 04:12:05.414
C:₩Users₩foren₩Downloads₩kape₩gkape.exe|2023-04-26 04:20:46.049
```

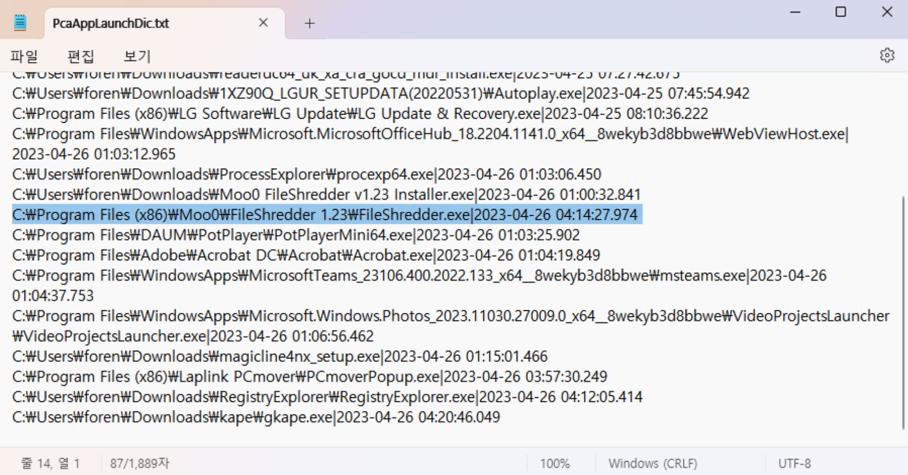
File Wiping Tool처럼 보이는 Moo0 FileShredder v1.23 Installer.exe 파일을 발견하였다.

*FileShredder은 회사 파일을 파쇄하는 빠르고 안정적인 도구이다.

2023-04-26 01:00:32.841 에 다운로드 되었다.

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

메모 포함[오전2]: 2. 파일 와이핑 툴이 실행된 시간은 언제입니까? (UTC+0)



```
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₩WebViewHost.exe|
2023-04-26 01:03:12.965
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|2023-04-26
01:04:37.753
C:₩Program Files₩WindowsApps₩Microsoft.Windows.Photos_2023.11030.27009.0_x64__8wekyb3d8bbwe₩VideoProjectsLauncher
₩VideoProjectsLauncher.exe|2023-04-26 01:06:56.462
C:₩Users₩foren₩Downloads₩magicline4nx_setup.exe|2023-04-26 01:15:01.466
C:₩Program Files (x86)₩Laplink PCmover₩PCmoverPopup.exe|2023-04-26 03:57:30.249
C:₩Users₩foren₩Downloads₩RegistryExplorer₩RegistryExplorer.exe|2023-04-26 04:12:05.414
C:₩Users₩foren₩Downloads₩kape₩gkape.exe|2023-04-26 04:20:46.049
```

파일이 다운로드 된 후 경로가 변경되었다.

FileShredder.exe 파일을 실행한 시간은 **2023-04-26 04:14:27.974** 이다.

The deadline for this problem is June 30.

Please do not post your write-up before the deadline for fair competition!

*** Delete this box when submitting your answer.**