



|            |  |
|------------|--|
| 작성자        | 김서영, 윤지원   |
| 분석 일자      | 2024.06.06   |
| 작성 일자      | 2024.06.06   |
| 분석 대상      | Auir.zip   |
| 문서 버전      | 2.0  |
| 작성자 E-mail | <a href="mailto:yoonjw0827@gmail.com">yoonjw0827@gmail.com</a> |

0. 목차

1. 문제 .....3

2. 분석 도구 .....3

3. 환경 .....3


4. Write-Up.....4

5. Flag..... 10

6. 별도 첨부..... 11

7. Reference ..... 12

### 1. 문제

|       |  |
|-------|--|
| URL   | -  |
| 문제 내용 | <p>1)What options did the suspect reset his PC with? What is the evidence to support your argument?</p> <p>2)How was Windows installed? What is the evidence to support your argument?</p> <p>3)Did the suspect set any additional options in the 'Choose settings' step? What is the evidence to support your argument?</p> |
| 문제 파일 | <br>Auir.zip  |
| 문제 유형 | Disk forensics   |
| 난이도   | 3 / 3  |

### 2. 분석 도구

| 도구명        | 다운로드 링크   | Version |
|------------|---|---------|
| FTK Imager | <a href="https://www.exterro.com/digital-forensics-software/ftk-imager">https://www.exterro.com/digital-forensics-software/ftk-imager</a> | 4.7.1.2 |
| VirtualBox | <a href="https://www.virtualbox.org/wiki/Downloads">https://www.virtualbox.org/wiki/Downloads</a>   | 7.0.18  |
|            |   |         |

### 3. 환경

| OS                |
|-------------------|
| Windows 11 64-bit |

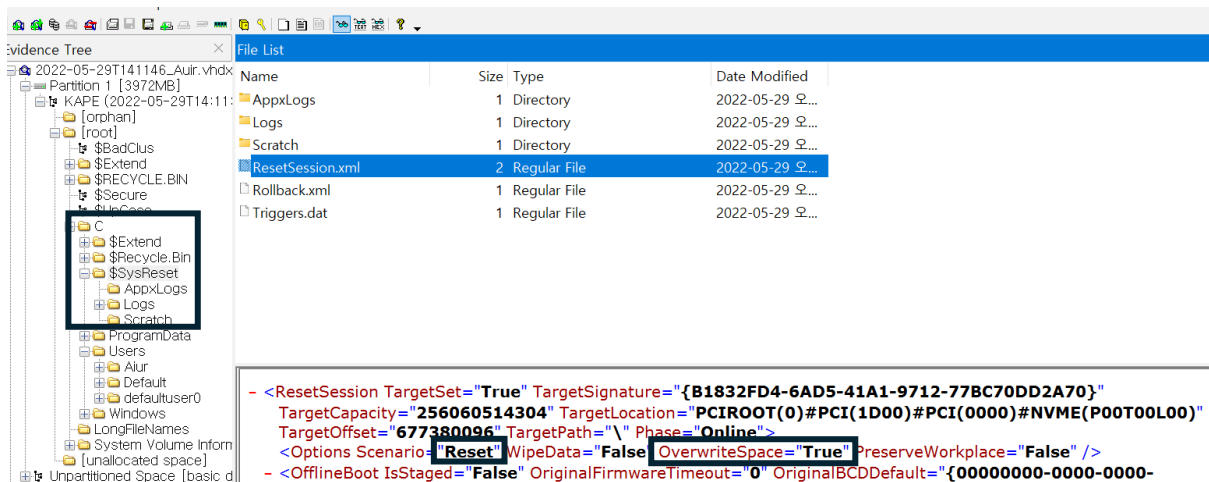
## 4. Write-Up

|           |  |
|-----------|--|
| 파일명       | Auir.zip   |
| 용량        | 77.9MB   |
| SHA256    | 9f7a185925b4f6394047e2c91564f965a05f385ed55c7032cf56d5a75a5ece42 |
| Timestamp | 2022-05-30 15:50:46  |

1. 용의자는 어떤 옵션으로 PC 를 재설정했으며, 그 증거는 무엇인가?

Auir.zip이 압축을 풀자 2022-05-29T141146\_Auir.vhdx 라는 파일이 생성되었다. 처음 보는 파일 확장자였기에 검색을 통해 알아보았더니, 일반적으로 vmdk라는 확장자로 변환하여 이미지 파일처럼 가상머신에 넣고 열 수 있다는 사실을 알아냈다. 그래서 힘들게 여러 방법을 동원하여 확장자도 바꿔서 가상머신에 여는 것까지 성공하였으나 FTK Imager로 여는 것과 별반 다를 것이 없다고 생각하여 가독성을 위해 FTK Imager로 열어보았다.

파일을 열어 둘러보던 중, 파일 초기화와 관련 있는 \$SysReset 폴더를 발견하였고, 그 안에는 ResetSession.xml이라는 파일 확인할 수 있었다. 여기서 옵션 시나리오가 Reset으로 설정되어 있는 것으로 보아 PC 초기화와 관련 있다는 사실을 알았고, 초기화에 여러 옵션들에 대한 내용으로 보였다.



[사진 1] 문제 파일의 ResetSession.xml

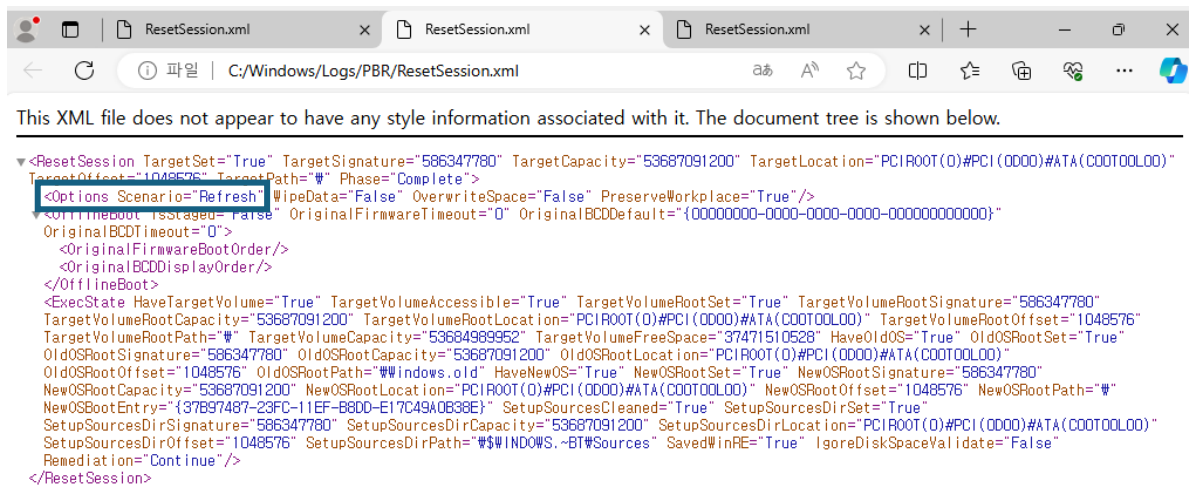
초기화 옵션에 대해 잘 알지 못해서 실제로 가상머신에서 PC 초기화를 해보기로 하였다. VirtualBox 를 이용하였고, window 이미지 파일과 문제 파일을 같이 넣어두었다. [설정] - [업데이트 및 보안] - [복구] - [PC 초기화]를 통해 초기화를 진행하였다.

초기화를 진행하려고 보니, 총 3 차례로 옵션을 결정할 수 있고, 여기서 어떤 옵션을 선택하느냐에 따라서 출력되는 결과가 달라질 것이라고 생각했다. (초기화 옵션은 별도 첨부에 기재하였다.

따라서 일단 처음에는 아무 옵션으로 초기화를 진행해보아야겠다 생각하여 [내 파일 유지] - [로컬 다시 설치] 옵션을 선택한 다음 초기화를 진행하였다.

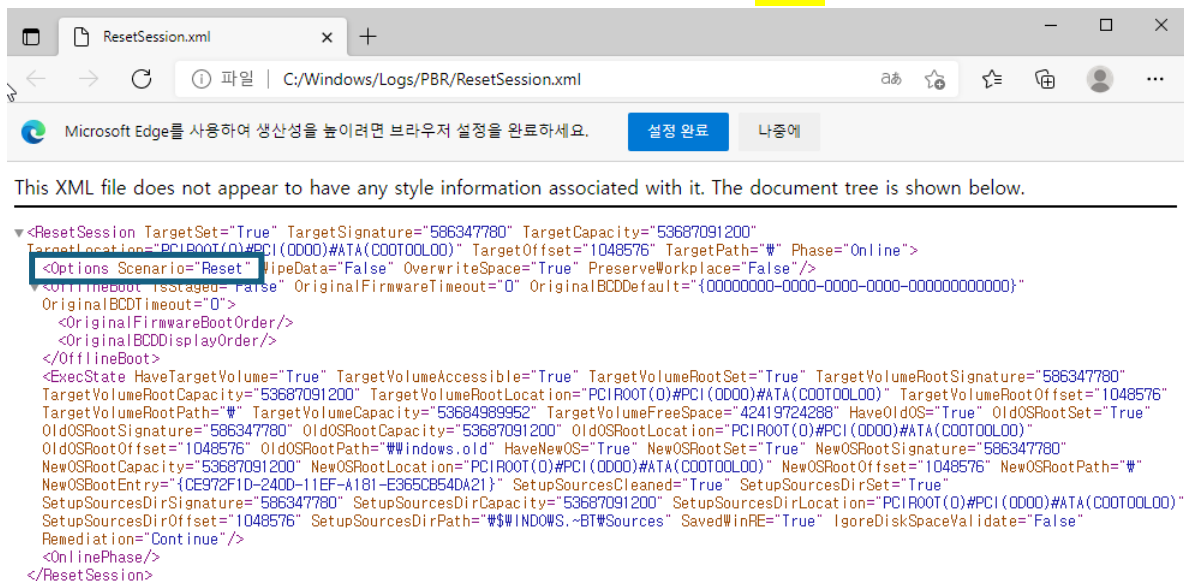
## [WHS-2] .iso

초기화 후, 내 PC 에서 검색을 통해 \$SysReset 파일을 찾을 수 있었다. 그 안에서 새로 생성된 ResetSession.xml 파일을 열어보았고, 시나리오 옵션이 **Refresh** 인 것을 확인하였다.



### [사진 2] [내 파일 유지] 옵션의 ResetSession.xml

이와 같은 방식으로 두 번째 초기화를 진행하였는데, 첫 번째 초기화와 차별점을 두기 위해 옵션을 다르게 하였다. **[모든 항목 제거] - [클라우드 다운] - [데이터 정리]** 로 설정한 두 번째 초기화의 ResetSession.xml은 [사진 3]과 같다. 여기서는 시나리오 옵션이 **Reset**인 것을 확인할 수 있다.



### [사진 3] [모든 항목 제거] 옵션의 ResetSession.xml

따라서 **문제 파일의 옵션 시나리오가 Reset**이었기 때문에, 우선 이 파일은 **[모든 항목 제거]**를 선택하여 초기화된 것임이 증명되었다.

## [WHS-2] .iso

### 2. 윈도우는 어떻게 설치되었으며, 증거는 무엇인가?

이번에는 윈도우 설치 방법에 대해 묻고 있기 때문에, 초기화의 두 번째 옵션을 묻고 있는 것이라고 생각하였다. 앞서 진행한 두 번의 초기화에서 다행히 이 옵션을 다르게 했기 때문에 해당 자료들을 그대로 사용하였다.

문제 파일의 \$SysReset 폴더를 더 살펴보다가, AppxLog 에 RestoreDownlevelAllUserStore.log 라는 파일이 혼자 존재하는 것을 보고 뭔가 의미가 있을 것이라고 생각하였다. 내용을 보니 윈도우 앱과 관련된 로그인 것 같다. RemoveAllAppsFromSystemSis 라는 로그도 있는 것으로 보아, 앱 패키지에 대한 로그 또한 표시되는 것 같다. 해당 파일을 export 하여 더 자세히 살펴보았지만, 특징을 발견하지 못해서 앞선 두 번의 초기화 기록에서의 RestoreDownlevelAllUserStore.log 를 살펴보기로 했다.

RestoreDownlevelAllUserS... 7,339 Regular File 2022-05-29 오...

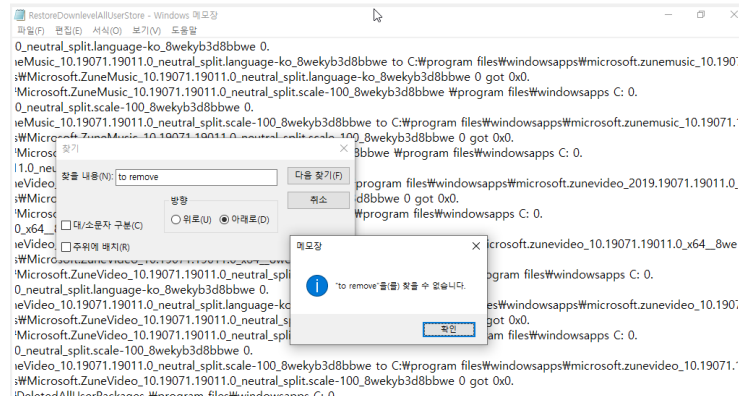
```
2022/05/29 12:34:37.391 Begin RestoreDownlevelAllUserStore.log.
2022/05/29 12:34:37.391 In RestoreDownlevelAllUserStore C:\Windows.old C:\.
2022/05/29 12:34:37.391 Normalized system roots C:\Windows.old C:.
2022/05/29 12:34:37.391 In RestoreFoldersAndRegistry C:\Windows.old C:.
2022/05/29 12:34:37.391 In RemoveAllAppsFromSystemSis C:.
2022/05/29 12:34:37.391 GetSystemSisPath got C:\Program Files\Windowsapps, 0x0.
```

#### [사진 4] 문제 파일의 RestoreDownlevelAllUserStore.log

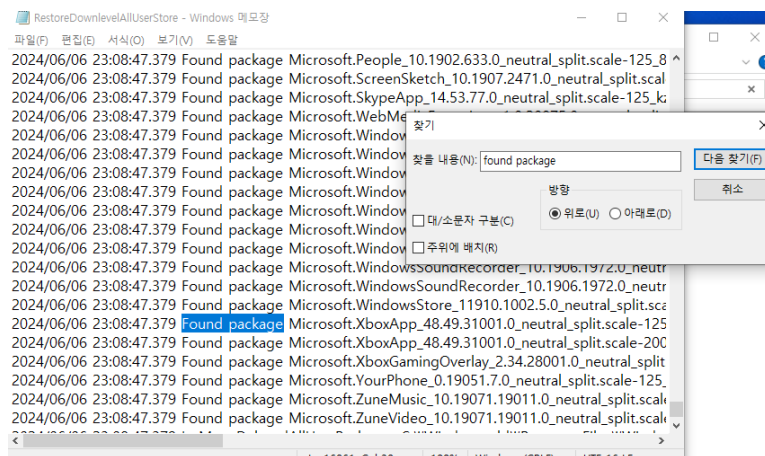
윈도우 설치 옵션은 [클라우드 다운]과 [로컬 다시 설치]인데, 이 둘의 가장 큰 차이는 기존 시스템 파일의 삭제 유무이다. [클라우드 다운]은 서버에서 다운받은 새 시스템 파일을 이용하고, [로컬 다시 설치]는 말 그대로 PC에 이미 있는 시스템 파일을 이용한다. 따라서 [클라우드 다운]에서는 기존 시스템 파일이 삭제된다는 점을 이용하여 두 RestoreDownlevelAllUserStore.log를 비교하기로 했다.

첫 번째 초기화의 [로컬 다시 설치] 옵션의 로그를 보면서 파일 삭제 기록을 보기 위해 [사진 5]와 같이 to remove를 검색해보았다. 예상과 같이 검색 기록을 찾을 수 없었다. 두 번째 초기화의 [클라우드 다운] 옵션의 로그에서도 to remove를 검색하였는데, 많은 기록들이 나왔다.

이 많은 기록들 중에서 기존 시스템 파일 삭제를 의미하는 기록이 정확히 어떤 것일지 궁금해졌다. RestoreDownlevelAllUserStore.log가 앱의 패키지 로그인 점을 이용하여 앱 패키지를 삭제하기 위해 이를 탐색하지 않을까라는 생각이 들어, 삭제할 앱 패키지를 탐색하는 로그를 검색하였다. Found package로 검색하여 [사진 6]과 같이 확인이 가능했다. 이를 통해 [클라우드 다운]에서 기존 시스템 파일이 삭제된다는 것을 확실하게 알 수 있었다.

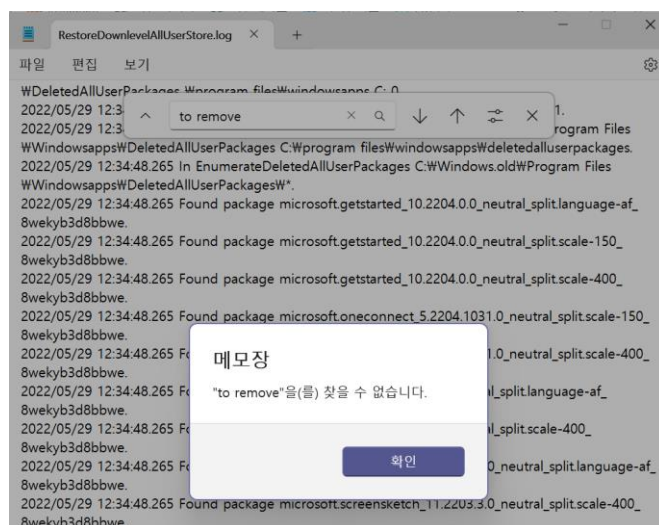


[사진 5] [로컬 다시 설치] 옵션의 RestoreDownlevelAllUserStore.log



[사진 6] [클라우드 다운] 옵션의 RestoreDownlevelAllUserStore.log

이제 두 옵션의 차이점을 알았으니, 문제 파일의 RestoreDownlevelAllUserStore.log 파일에서 to remove를 검색해보았다. 찾을 수 없다는 결과가 나왔기 때문에 기존 시스템 파일을 삭제하지 않는 **[로컬 다시 설치] 옵션을 선택**했다는 것을 알 수 있다.



[사진 7] 문제 파일의 ResotreDownlevelAllUserStore.log

3. 용의자가 설정 선택 단계에서 추가 옵션을 설정했는가? 그 증거는 무엇인가?

마지막으로 어떤 추가 옵션을 설정했는지 묻는 문제이다. 첫 번째 옵션에 따라 추가 옵션 종류도 바뀌게 되는데, 문제 파일에서는 처음에 [모든 항목 제거]를 선택했기 때문에 세 가지 옵션들을 고려하면 된다.

두 번째 초기화에서 적용한 [데이터 정리] 옵션을 우선적으로 살펴보겠다. 문제 파일의 \$SysReset에는 Log 폴더가 존재하는데, 이곳에 두 가지의 로그 파일이 존재하여 이를 살펴보았다. 이 중 **setupact.log**가 **초기화 중에 일어난 일을 기록**하는 파일이라는 것을 알 수 있었고, 이를 통해 추가 옵션에 대해 알 수 있을 것 같았다.

|               |        |              |                 |
|---------------|--------|--------------|-----------------|
| setupact.log  | 48,429 | Regular File | 2022-05-29 오... |
| setuperr.log  | 5      | Regular File | 2022-05-29 오... |
| Timestamp.xml | 1      | Regular File | 2022-05-29 오... |

```

00000000 EF BB BF 32 30 32 32 2D 30 35 2D 32 39 20 31 32 i\2022-05-29 12
00000010 3A 32 32 3A 33 33 2C 20 49 6E 66 6F 20 20 20 20 :22:33, Info
00000020 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000030 20 20 20 20 20 20 4C 6F 67 53 65 73 73 69 6F 6E 3A
00000040 20 53 74 61 72 74 69 6E 67 20 61 20 6E 65 77 20
00000050 6C 6F 67 20 73 65 73 73 69 6F 6E 20 61 74 20 5B
00000060 43 3A 5C 24 53 79 73 52 65 73 65 74 5C 4C 6F 67
00000070 73 5D 0D 0A 32 30 32 32 2D 30 35 2D 32 39 20 31
00000080 32 3A 32 32 3A 33 33 2C 20 49 6E 66 6F 20 20 20
00000090 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
000000a0 20 20 20 20 20 20 52 65 67 69 73 74 72 79 3A 20
000000b0 4C 6F 61 64 69 6E 67 20 53 4F 46 54 57 41 52 45
000000c0 20 68 69 76 65 20 66 72 6F 6D 20 6F 6E 6C 69 6E
000000d0 65 20 4F 53 0D 0A 32 30 32 32 2D 30 35 2D 32 39
000000e0 20 31 32 3A 32 32 3A 33 33 2C 20 49 6E 66 6F 20
  
```

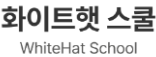
[사진 8] 문제 파일의 setupact.log

이 setupact.log파일을 export하여 살펴보다가 초반부에 [사진 9]와 같은 목록을 발견하였다. 해당 목록은 시스템 리미테이션과 관련된 작업을 기록한 로그로, 각종 작업이 실행된 시간과 작업에 따른 디스크 사용량 변화를 보여준다. 이 중에서 24번째에 EraseFilesystem이라는 부분이 보여서 앞서 확인한 대로 파일 시스템 삭제가 이루어졌음을 다시 한번 확인할 수 있었다.

| 파일                        | 편집 | 보기  |
|---------------------------|----|---|
| 2022-05-29 12:23:45, Info |    | Total number of operations: [28]:   |
| 2022-05-29 12:23:45, Info |    | 0: [Set remediation strategy: roll back to old OS] (SetRemediationStrategy): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]  |
| 2022-05-29 12:23:45, Info |    | 1: [Clear storage reserve] (ClearStorageReserve): Peak disk: [0 byte(s)], Disk delta: [-8229150720 byte(s)]   |
| 2022-05-29 12:23:45, Info |    | 2: [Delete OS uninstall image] (DeleteUninstall): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]   |
| 2022-05-29 12:23:45, Info |    | 3: [Enable Rollback Execution] (EnableRollbackExecution): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]   |
| 2022-05-29 12:23:45, Info |    | 4: [Set 'In-Progress' environment key] (MarkInProgress): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]  |
| 2022-05-29 12:23:45, Info |    | 5: [Back up WinRE information] (SaveWinRE): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]   |
| 2022-05-29 12:23:45, Info |    | 6: [Archive user data files] (ArchiveUserData): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]   |
| 2022-05-29 12:23:45, Info |    | 7: [Reconstruct Windows from packages] (ExecSetup): Peak disk: [2970621952 byte(s)], Disk delta: [2970621952 byte(s)]   |
| 2022-05-29 12:23:45, Info |    | 8: [Save flighted build number to new OS] (SaveFlight): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]   |
| 2022-05-29 12:23:45, Info |    | 9: [Persist install type in new OS registry] (SetInstallType): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]  |
| 2022-05-29 12:23:45, Info |    | 10: [Notify OOBE not to prompt for a product key] (SkipProductKeyPrompt): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]   |
| 2022-05-29 12:23:45, Info |    | 11: [Migrate setting-related files and registry data] (MigrateSettings): Peak disk: [65425364 byte(s)], Disk delta: [65425364 byte(s)]                              |
| 2022-05-29 12:23:45, Info |    | 12: [Execute PBR plugins] (ExecutePbrPlugin): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]   |
| 2022-05-29 12:23:45, Info |    | 13: [Migrate AppX Provisioned Apps] (MigrateProvisionedApps): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]   |
| 2022-05-29 12:23:45, Info |    | 14: [Migrate OEM PBR extensions] (MigrateOEMExtensions): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]  |
| 2022-05-29 12:23:45, Info |    | 15: [Submit request to interactively clear TPM on next boot] (ClearTPM): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]  |
| 2022-05-29 12:23:45, Info |    | 16: [Set 'In-Progress' environment key] (MarkInProgress): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]   |
| 2022-05-29 12:23:45, Info |    | 17: [Restore boot manager settings] (RestoreBootSettings): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]  |
| 2022-05-29 12:23:45, Info |    | 18: [Restore WinRE information] (RestoreWinRE): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]   |
| 2022-05-29 12:23:45, Info |    | 19: [Install WinRE on target OS] (InstallWinRE): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]  |
| 2022-05-29 12:23:45, Info |    | 20: [Execute OEM extensibility command: [AfterImageApply_BD80C1E8-6951-46C4-A87F-C07829F462FD.cmd]] (RunExtension): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)] |
| 2022-05-29 12:23:45, Info |    | 21: [Set remediation strategy: show data wipe warning, then continue] (SetRemediationStrategy): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]                     |
| 2022-05-29 12:23:45, Info |    | 22: [Delete user data files] (DeleteUserData): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]  |
| 2022-05-29 12:23:45, Info |    | 23: [Delete old OS files] (DeleteOldOS): Peak disk: [0 byte(s)], Disk delta: [-52564566016 byte(s)]   |
| 2022-05-29 12:23:45, Info |    | 24: [Overwrite free space on [C:]] (EraseFilesystem): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]   |
| 2022-05-29 12:23:45, Info |    | 25: [Delete Encryption Opt-Out marker in OS volume] (DeleteEncryptionOptOut): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]                                       |
| 2022-05-29 12:23:45, Info |    | 26: [Trigger WipeWarning remediation if a marker file is set] (TriggerWipeWarning): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]                                 |
| 2022-05-29 12:23:45, Info |    | 27: [Set remediation strategy: ignore and continue] (SetRemediationStrategy): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)]                                       |

[사진 9] setupact.log의 EraseFilesystem 부분





해당 부분에 Overwrite free space가 있어서 이게 무엇을 의미하는지 알아봤는데, 이는 C에 있는 free space를 덮어쓴 것으로 보인다. Free space는 파일이 삭제되고 남은 공간이기 때문에 파일이 삭제된 로그를 의미한다. 또한 [사진 1]의 표시된 부분을 잘 살펴보면, **overwritespace="True"**로 설정된 것을 볼 수 있다. 따라서 [데이터 정리] 옵션을 설정하고 초기화하였다고 생각했다.

```
setupact - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말

-- End ExecState dump
Session: Offline operation queue:
Total number of operations: [26]:
0: [Clear storage reserve] (ClearStorageReserve): Peak disk: [0 byte(s)], Disk delta: [-70:
1: [Delete OS uninstall image] (DeleteUninstall): Peak disk: [0 byte(s)], Disk delta: [0 byt
2: [Set remediation strategy: roll back to old OS] (SetRemediationStrategy): Peak disk:
3: [Set 'In-Progress' environment key] (MarkInProgress): Peak disk: [0 byte(s)], Disk del
4: [Back up WinRE information] (SaveWinRE): Peak disk: [0 byte(s)], Disk delta: [0 byte(s)
5: [Archive user data files] (ArchiveUserData): Peak disk: [0 byte(s)], Disk delta: [0 byte(
6: [Reconstruct Windows from packages] (ExecSetup): Peak disk: [2696208384 byte(s)],
7: [Save flighted build number to new OS] (SaveFlight): Peak disk: [0 byte(s)], Disk del
8: [Persist install type in new OS registry] (SetInstallType): Peak disk: [0 byte(s)], Disk d
9: [Notify OOB not to prompt for a product key] (SkipProductKeyPrompt): Peak disk:
10: [Migrate setting-related files and registry data] (MigrateSettings): Peak disk: [4176
11: [Migrate AppX Provisioned Apps] (MigrateProvisionedApps): Peak disk: [0 byte(s)],
12: [Migrate OEM PBR extensions] (MigrateOEMExtensions): Peak disk: [0 byte(s)], Disk de
13: [Migrate power settings] (MigratePowerSettings): Peak disk: [0 byte(s)], Disk delta:
14: [Submit request to interactively clear TPM on next boot] (ClearTPM): Peak disk: [0
15: [Set 'In-Progress' environment key] (MarkInProgress): Peak disk: [0 byte(s)], Disk de
16: [Restore boot manager settings] (RestoreBootSettings): Peak disk: [0 byte(s)], Disk b
17: [Restore WinRE information] (RestoreWinRE): Peak disk: [0 byte(s)], Disk delta: [0 byt
18: [Install WinRE on target OS] (InstallWinRE): Peak disk: [0 byte(s)], Disk delta: [0 byt
19: [Set remediation strategy: show data wipe warning, then continue] (SetRemediatio
20: [Delete user data files] (DeleteUserData): Peak disk: [0 byte(s)], Disk delta: [0 byte(s
21: [Delete old OS files] (DeleteOldOS): Peak disk: [0 byte(s)], Disk delta: [-2191434956
22: [Overwrite free space on [C:] ] (EraseFilesystem): Peak disk: [0 byte(s)], Disk delta:
23: [Delete Encryption Opt-Out marker in OS volume] (DeleteEncryptionOptOut): Peak
24: [Trigger WipeWarning remediation if a marker file is set] (TriggerWipeWarning): Pe
25: [Set remediation strategy: ignore and continue] (SetRemediationStrategy): Peak di
```

따라서 [데이터 정리] 옵션을 설정하고 초기화 한 두 번째 초기화 PC의 setupact.log를 살펴보았다. [사진 10]가 같이 overwrite free space를 발견할 수 있었다. 따라서 문제 파일은 [데이터 정리] 옵션을 설정하고 초기화하였음을 알 수 있다.

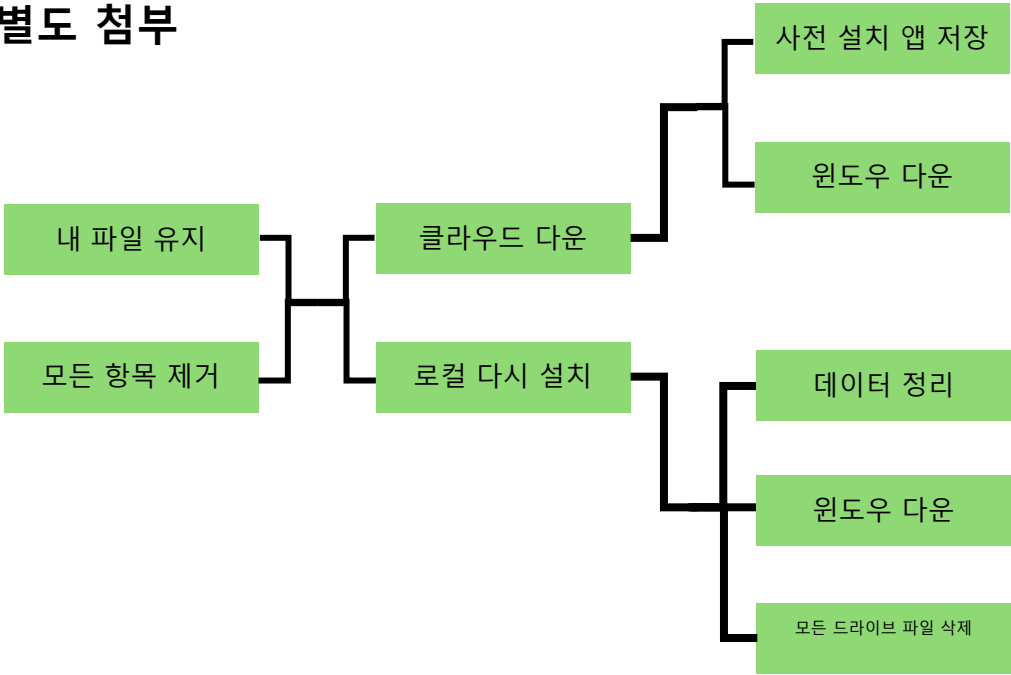
마지막 추가 옵션인 **[모든 드라이브 파일 삭제]** 옵션의 경우, setupact.log에서 overwrite free space가 존재하면 [모든 드라이브 파일 삭제]를 의미하는 로그가 나타나지 않는다는 사실을 알 수 있었다. 문제 파일은 [데이터 정리] 옵션을 선택하여 setupact.log에 overwrite free space가 존재하기 때문에 **[모든 드라이브 파일 삭제]** 옵션을 설정하지 않았음을 알 수 있다.

9

## 5. Flag

1. [모든 항목 제거] – [Remove everything]
2. [로컬 다시 설치] – [Local reinstall]
3. [데이터 정리] – [Clean Data]

6. 별도 첨부



[그림 1] 윈도우 PC 초기화 설정 옵션

## 7. Reference

- [URL]