103 – Reset Your PC

Team Information

Team Name : ISEGYE_IDOL

Team Member : Eungchang Lee, Sojeong Kim, Mingyu Seong, Donghyun HA

Email Address : dfc-isegyeidol@googlegroups.com

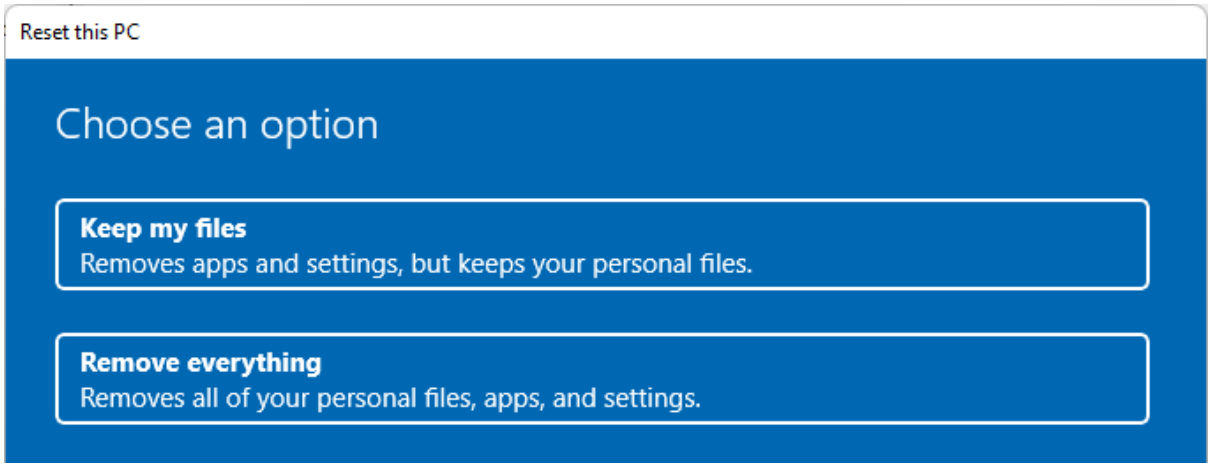
Instructions

Description It seems that the suspect's PC was recently reset with the 'Reset this PC' function. What method was used?

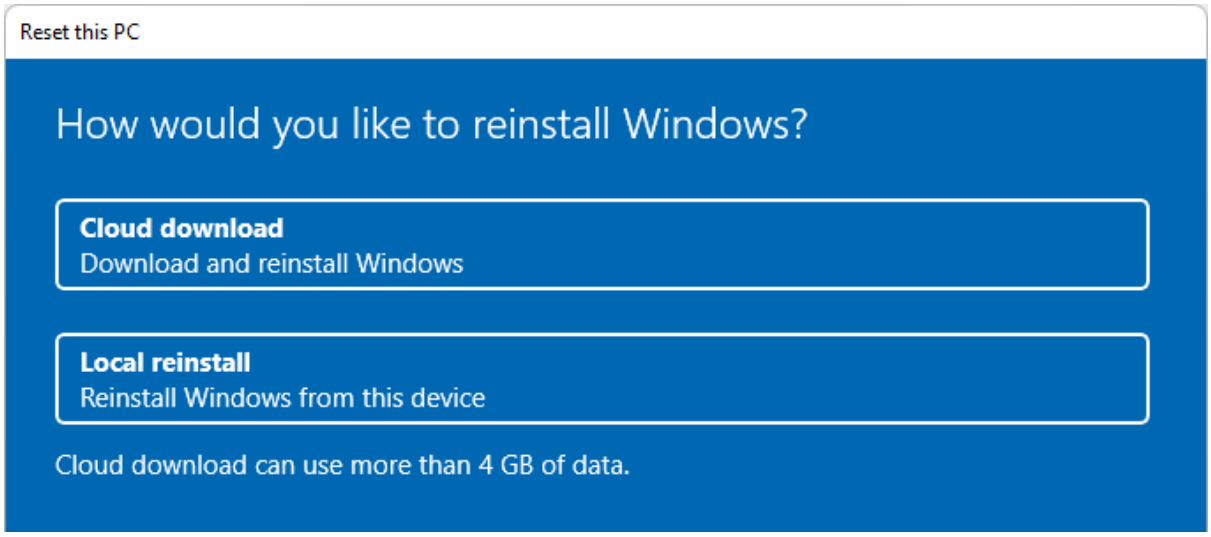
Target	Hash (MD5)
Auir.zip	b7bd1674b27b0e27514bb91ab2c81cb9

Questions

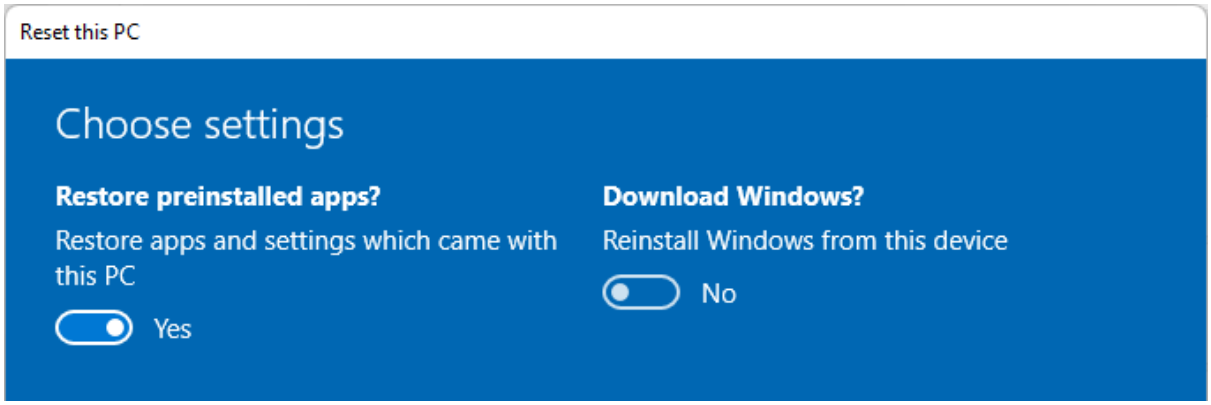
1) What options did the suspect reset his PC with? What is the evidence to support your argument? (30 points)

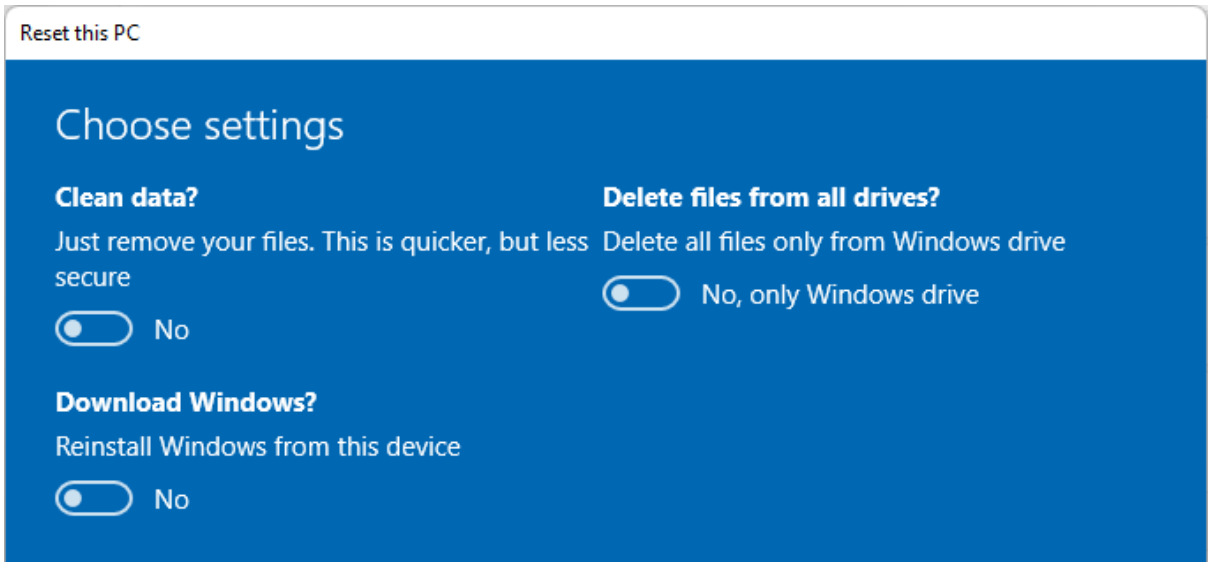


2) How was Windows installed? What is the evidence to support your argument? (30 points)



3) Did the suspect set any additional options in the 'Choose settings' step? What is the evidence to support your argument? (40 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://accessdata.com/product-download/ftk-imager-version-4-5		

Name:	Sublime Text	Publisher:	Sublime HQ Pty Ltd
Version:	Build 4126		
URL:	https://www.sublimetext.com/download		

Name:	VMware Workstation 16 Pro	Publisher:	VMware, Inc.
Version:	16.2.3 build-19376536		
URL:	https://www.vmware.com/		

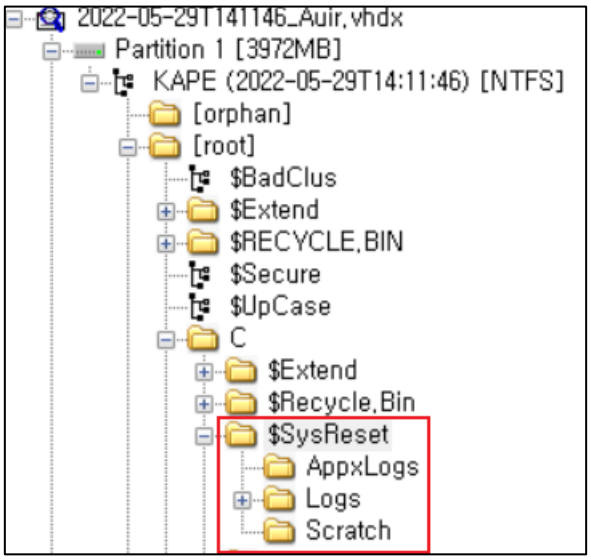
VM(Test) PC used:

OS:	Windows 10 Pro	Version:	10.0.19044 Build 19044.1826
System Name:	DESKTOP-DR9PJ51		

Step-by-step methodology:

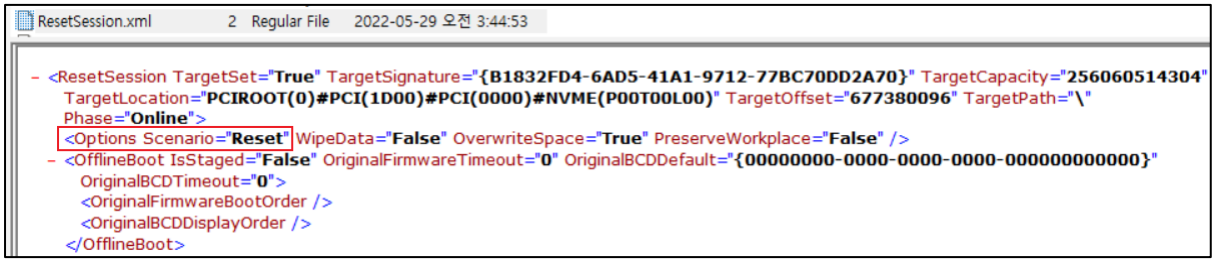
1) What options did the suspect reset his PC with? What is the evidence to support your argument? (30 points)

대상자 PC의 [C] 디렉터리 하위에 [$SysReset] 디렉터리가 존재한다. [$SysReset]는 PC 초기화 작업에 사용한 파일과 초기화 작업에 대한 마이그레이션 로그가 저장된다. 따라서 대상자가 설정한 초기화 옵션을 찾기 위해 해당 디렉터리를 살펴볼 필요가 있다.



[그림 1] 대상자 PC의 [C] 하위 [$SysReset] 디렉터리 (FTK Imager)

[$SysReset] 하위 ResetSession.xml 파일을 살펴보니, <Options> 태그의 <Scenario> 속성은 "Reset"으로 설정되어 있다.

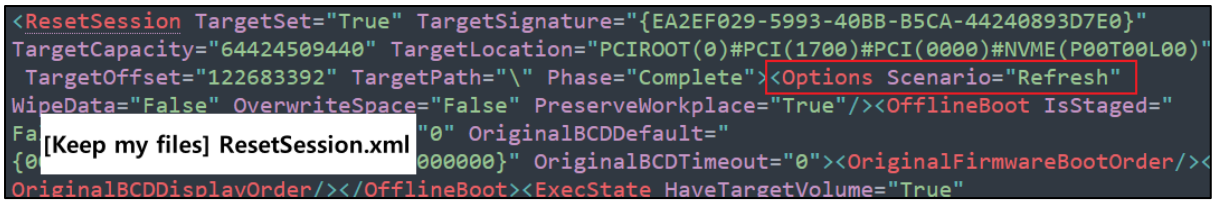


[그림 2] 대상자 PC의 [$SysReset] 하위 ResetSession.xml (FTK Imager)

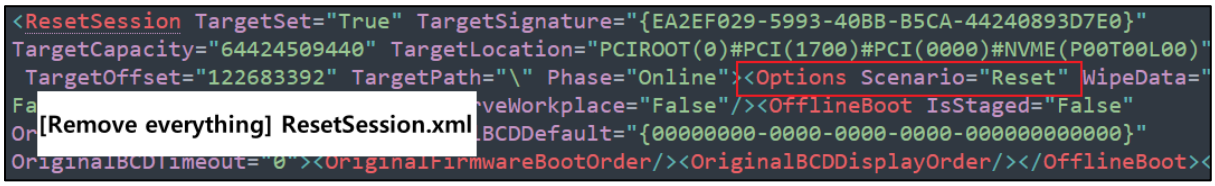
실제로 [PC 초기화] 기능을 실행하면 첫 번째 옵션으로 [keep my files], [Remove everything] 중 선택이 필요하다. 본 분석가는 분석 PC에 VMware Workstation을 이용하여 초기화 실험을 세팅하

였고, 두 옵션의 선택에 따른 Options 태그의 Scenario 속성 기록을 검증하였다.

[Keep my files]을 선택한 파일의 경우 Scenario 속성이 "Refresh"로 기록되며, [Remove everything]을 선택한 파일의 경우 "Reset"으로 기록된다.



[그림 2] [Keep my files]의 Scenario 속성 "Refresh" (Sublime Text)



[그림 3] [Remove everything]의 Scenario 속성 "Reset" (Sublime Text)

Num	Choose an option	ResetSession.xml 내 Options Scenario 태그
1	[Keep my files]	**Refresh**
2	[Remove everything]	**Reset**

[표 1] 초기화 첫 번째 옵션 테스트 결과

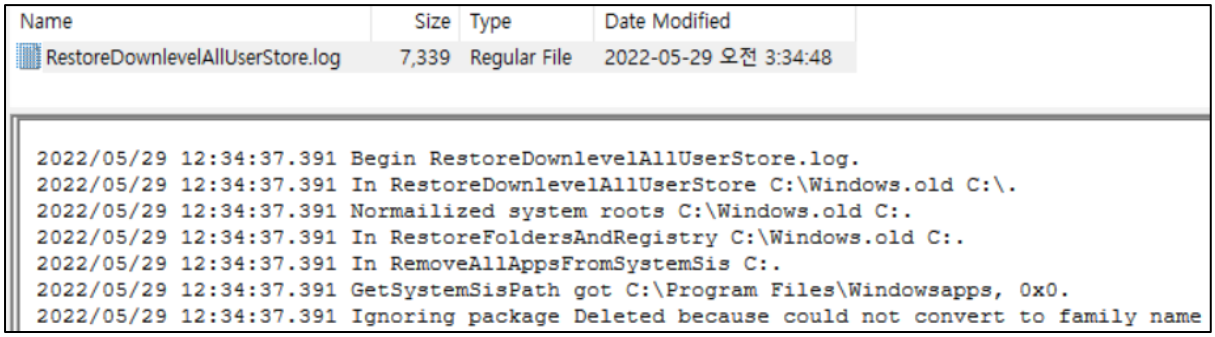
따라서 대상자 PC의 [$SysReset] 하위 ResetSsion.xml 파일의 Sceanario 속성이 "Reset"인 것과 테스트 결과를 비교한 결과, 대상자는 [PC 초기화] 기능에서 **[Remove everything]**을 선택하였음을 증명하였다.

참고로 Windows 10 이전 버전은 PC 복구(이하 Refresh)와 PC 초기화(이하 Reset)로 항목을 나누어 각 서비스를 제공했지만, Windows 10 이상부터 [PC 초기화] 기능으로 합쳐져 첫 번째 옵션으로 복구 및 초기화 선택을 제공한다. 첫 번째 옵션에서 [Keep my files] 옵션은 Refresh이며, [Remove everything] 옵션은 Reset을 뜻하는 것이다.

2) How was Windows installed? What is the evidence to support your argument? (30 points)

[Cloud download]의 경우, Windows가 Microsoft 서버에서 새로운 시스템 파일을 다운로드하고, 이를 사용하여 PC에 Windows를 다시 설치한다.[1] 반면 [Local reinstall]의 경우, PC에 이미 있는 시스템 파일을 사용하여 Windows를 다시 설치하는 것이므로 기존 시스템 파일을 찾아 새로운 Windows 시스템으로 재조립한다. 따라서 기존 시스템 파일을 삭제하고 재설치하는 로그를 확인하여 두 번째 옵션을 증명하고자 한다.

[$SysReset] 하위 [AppxLog] 디렉터리에는 RestoreDownlevelAllUserStore.log 파일이 있는데, 이 파일은 Windows 앱 패키지 로그로서 초기화 작업 중에 앱 패키지 관련 행위를 기록한다.

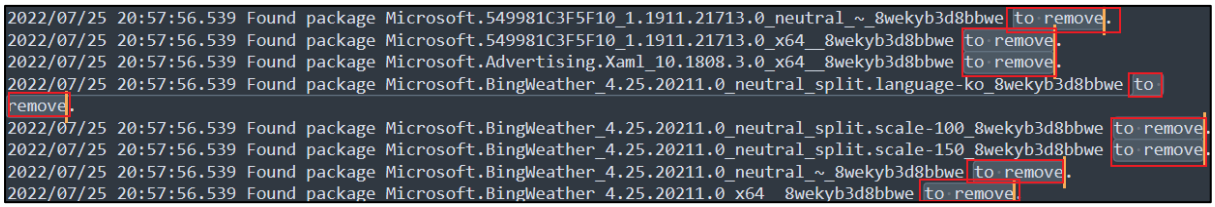


[그림 4] 대상자 PC의 [$SysReset₩AppxLogs] 하위 RestoreDownlevelAllUserStore.log (FTK Imager)

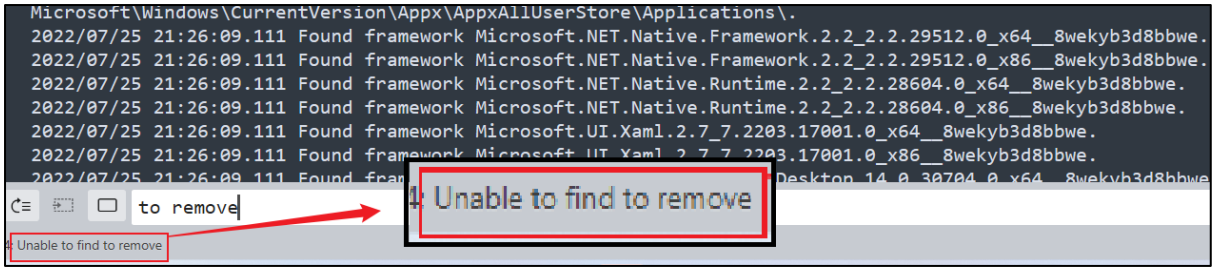
본 분석가는 VMware Workstation을 이용하여 [PC 초기화]를 실행하였으며, 두 번째 옵션(Cloud download, Local reinstall)에 따른 RestoreDownlevelAllUserStore.log 파일을 분석하였다.

[Cloud download]를 선택한 파일의 경우, 삭제할 앱 패키지를 검색하는 행위가 발견되었으며, 로그에는 "Found package [App package] to remove" 문구로 기록되었다. 반면 [Local reinstall]를 선택한 파일의 경우, Windows 앱 패키지를 유지하기 때문에 위 행위가 발견되지 않았다. 이는 Sublime Text 편집기에서 텍스트 검색 기능으로 "to remove" 키워드 검색 결과 단 하나도 발견되지 않았기 때문이다.

[1] https://www.howtogeek.com/754424/should-you-use-cloud-download-or-local-reinstall-on-windows/



[그림 5] [Cloud download]의 RestoreDownlevelAllUserStore.log 내 삭제 행위 발견 (Sublime Text)

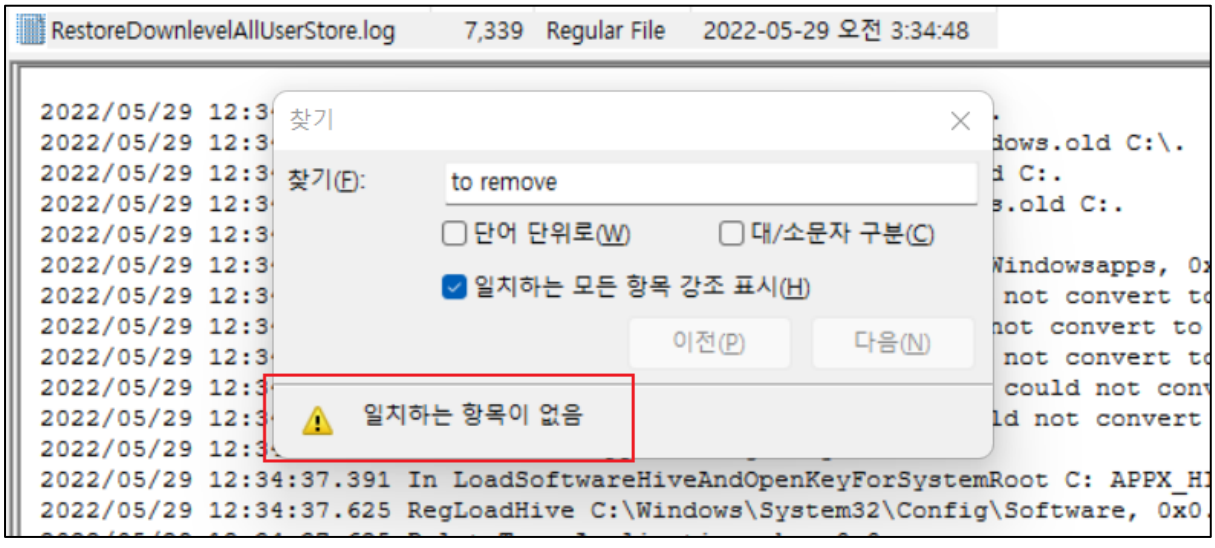


[그림 6] [Local reinstall]의 RestoreDownlevelAllUserStore.log 내 삭제 행위 미 발견 (Sublime Text)

Num	Choose an option	RestoreDownlevelAllUserStore.log 내 삭제 행위 발견
1	[Cloud download]	O
2	[Local reinstall]	X

[표 2] 초기화 두 번째 옵션 테스트 결과

위 테스트 결과를 바탕으로, 대상자 PC의 RestoreDownlevelAllUserStore.log에 적용해보니 해당 로그에서 Windows 앱 패키지 삭제 행위를 발견하지 못했다. 따라서 초기화 작업 시 Windows 패키지를 그대로 이용한 것으로 보아, 대상자는 시스템 파일을 새로 다운로드 받지 않는 **[Local reinstall]**을 선택하였음을 증명하였다.



[그림 7] 대상자 PC 내 RestoreDownlevelAllUserStore.log 내 삭제 행위 미 발견 (FTK Imager)

3) Did the suspect set any additional options in the 'Choose settings' step? What is the evidence to support your argument? (40 points)

앞서 1번 문항에서 언급했던 것과 같이 [PC 초기화] 작업의 첫 번째 옵션으로 [Keep my files], [Remove everything]의 선택지가 존재한다. 이때, 각 옵션에 따라 세부 세팅 옵션의 차이가 있다.

Choose an option (First)	Choose settings (Third)
Keep my files	● Restore preinstalled apps? ● Download Windows?
Remove everything	● **Clean data?** ● **Delete files from all drives?** ● **Download Windows?**

[표 3] 초기화 첫 번째 옵션에 따른 세 번째 옵션 목록 정리

대상자 PC의 경우 첫 번째 옵션으로 [Remove everything]을, 두 번째 옵션으로 [Local reinstall]을 선택하였으므로, 세 번째 옵션은 [Remove everything]의 선택 결과로 따라오는 **세 가지 세부 옵션 (Clean data/Delete files from all drives/Download Windows)**에서 설정했을 것으로 추정한다.

- Clean data?

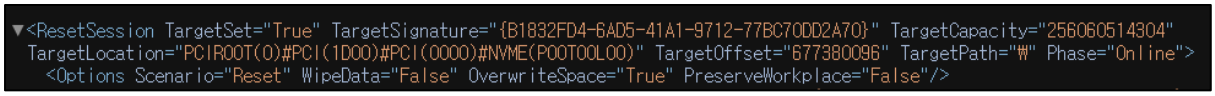
[$SysReset₩Logs] 하위 setupact.log 파일은 Windows 초기화 중에 수행된 작업을 기록하기 때문에, 대상자가 선택한 세부 옵션의 흔적을 찾을 수 있어 위 로그 파일을 바탕으로 분석하였다.

대상자 PC 내의 setupact.log에 의하면, Operation [24] [EraseFilesystem]을 수행하면서 [C:₩]에 있는 free space를 덮어쓴다. free space란 파일이 삭제되면 파일이 차지하고 있는 공간을 free space로 표시하여, 다른 파일이 해당 블록을 사용할 수 있다. 이러한 free space를 Overwrite하여 완벽하게 데이터를 삭제한 이력이 발견되었다.

```
2022-05-29 12:25:34, Info    Operation [22] ([DeleteUserData] - [Delete user data files]): Estimated Runtime: [360] seconds
2022-05-29 12:25:34, Info    Operation [23] ([DeleteOldOS] - [Delete old OS files]): Estimated Runtime: [720] seconds
2022-05-29 12:25:34, Info    Operation [24] ([EraseFilesystem] - [Overwrite free space on [C:₩]]): Estimated Runtime: [6405] seconds
```

[그림 8] 대상자 PC 내 [setupact.log] – Overwrite free space on [C:₩]

또한, [$Sysreset] 하위 Resetsession.xml 파일을 살펴보면 OverwriteSpace="True"로 설정되어 있다.

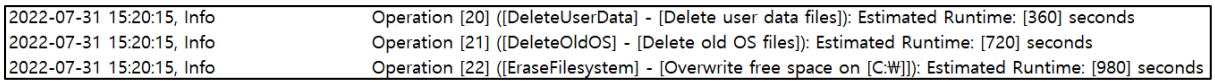


[그림 9] 대상자 PC 내 [ResetSession.xml] – [OverwriteSpace="True"]

Setupact.log 파일과 Resetsession.xml 파일을 분석함으로써 대상자 PC에 [Overwrite]가 수행되었음을 파악하였는데, 이는 [Clean data] 옵션이 전체 드라이브에 [0x00]을 덮어쓴다는 사실[2]에 있어서 대상자 PC에는 **[Clean data] 옵션**을 **설정**하여 초기화를 진행하였음을 추정할 수 있다.

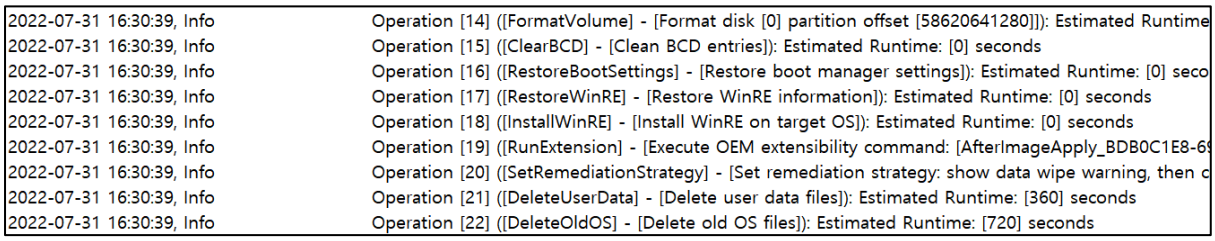
위 추정을 증명하기 위해 본 분석가는 VMware Workstation에서 [Clean data] 옵션의 유무로 로그 파일을 비교 분석하였고, 분석 결과 대상자 PC의 로그 결과와 동일하게 기록되었음을 입증하였다.

1) **Clean data [Yes],** Delete files from all drives [No]의 경우



[그림 10] 분석가 PC 내 [setupact.log] – Overwrite free space on [C:₩] 발견

2) **Clean data [No],** Delete files from all drives [Yes]



[그림 11] 분석가 PC 내 [setupact.log] – Overwrite free space on [C:₩] 미 발견

- Delete files from all drives?

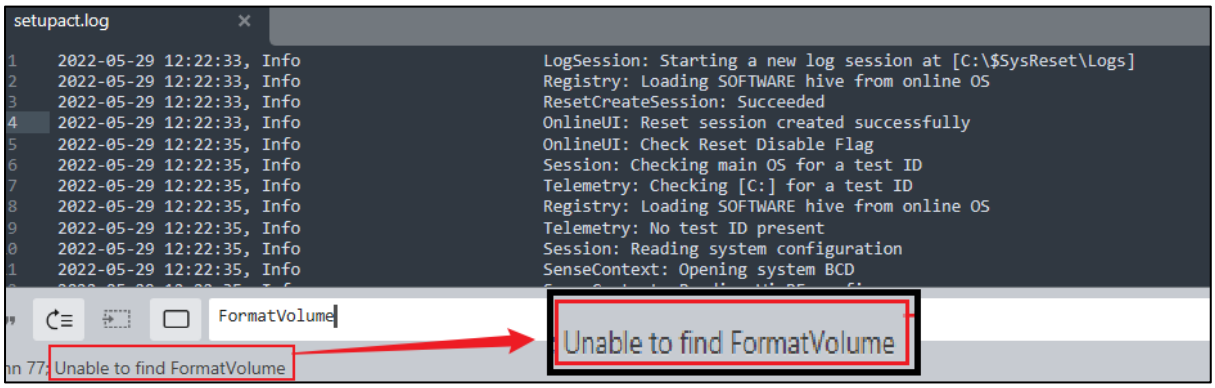
[Clean data] 테스트의 두 번째 테스트[3]에서, [Clean data]를 [No]로 설정한 동시에 [Delete files from all drives]는 [Yes]로 설정하여 진행되었다. 이때 해당 로그(setupact.log)에는 [C:₩]를

[2] https://answers.microsoft.com/en-us/windows/forum/all/difference-between-just-remove-files-and-remove/01b7cda3-2e07-4caf-869f-f2adc36b77f3

[3] [그림 10] 참고

Overwrite한다는 [EraseFilesystem] Operation이 없는 대신, Operation [14] [FormatVolume]이 기록되었다. [FormatVolume] Operation은 [Clean data] 옵션이 활성화(Yes)일 상황에서는 나타나지 않는 옵션으로서, 이는 [Delete files from all drives]를 특정할 수 있는 초기화 옵션 흔적이다.

대상자 PC 내 setupact.log에는 [FormatVolume] Operation이 발견되지 않는 것으로 보아, 대상자는 초기화 작업 시 **[Delete files from all drives]**를 **설정하지 않았음**을 입증한다.



[그림 12] 대상자 PC 내 [setupact.log] – FormatVolume 미 발견 (Sublime Text)

- Download Windows?

앞서 1번, 2번 문항에서 입증한 내용에 따르면, 대상자 PC는 [PC 초기화] 기능의 첫 번째 옵션으로 [Remove everything]을, 두 번째 옵션으로 [Local reinstall]을 선택하였다.

세 번째 세부 옵션 중 [Download Windows] 옵션을 테스트하기 위해 위 순서의 옵션대로 초기화 작업을 시도하였지만, "클라우드 다운로드에서 4GB이상의 데이터를 사용할 수 있습니다." 라는 문구가 적힌 창을 띄워주면서 실패하였다. 이는 [Local reinstall] 옵션을 선택 시, [Download Windows] 옵션이 [No]로 default 적용되기 때문이다. 따라서 앞선 2번 항목에서 [Local Reinstall]로 판명했기 때문에 **[Download Windows] 옵션**은 **설정되지 않고** 초기화 작업이 진행되었음을 입증하였다.

최종적으로 대상자가 선택한 세 번째 세부 옵션은 다음과 같이 정리한다.

Num	Choose an option	Option 선택 여부
1	[Clean Data]	**O(Yes)**
2	[Delete files from all drives]	**X(No)**
3	[Download Windows]	**X(No)**

[표 4] 대상자가 선택한 초기화 작업의 세 번째 옵션

앞서 여러 입증 과정을 통해, 다음과 같은 사실을 입증하였다.

PC 대상자는 [PC 초기화] 작업을 진행하면서,

- 첫 번째 옵션으로 **[Remove everything]**을,
- 두 번째 옵션으로 **[Local reinstall]**을,
- 세 번째 옵션으로 **[Clean Data]**만을 선택하여 초기화 작업을 진행하였다.