201 – Shredder Test

Team Information

Team Name : DogeCoin

Team Member : Dongbin Oh, Donghyun Kim, Donghyun Kim, Yeongwoong Kim

Email Address : dfc-dogecoin@naver.com

Instructions

Description Analyze the given USB Image and answer the questions.

Target	Hash (MD5)
Test_shredder.zip	B9FA593627CC6471C612CF7F55D7B12E

Questions

1. By analyzing the traces of the use of wiping (shredder) programs, identify which programs were used. Hint: some of the following listed tools were used (default setting, freeware/demo license). (150 points)

ace utilities	ashampoo winoptimizer	winutilities file shredder
BlankAndSecure	ss data eraser	delete files permanently
file shredder by Pow Tools	super file shredder	freeraser
hardwipe	hard disk scrubber	kernel file shredder
pc shredder	remo file eraser	sdelete
securely file shredder	secure eraser	protectstar data shredder
wisecare 365	bcwipe	bitkiller
eraser	glary utilities	Moo0 FileShredder
TweakNow securedelete	wipefile	

2. List the files deleted by the user in order of deletion time. Describe all artifacts that indicate the deletion time. (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:	NTFS Log Tracker	**Publisher:**	Junghoon Oh
Version:	1.6		
URL:	https://sites.google.com/site/forensicnote/ntfs-log-tracker		

Name:	Winhex	**Publisher:**	X-Ways Software Technology
Version:	20.2		
URL:	https://x-ways.net/winhex/		

Name:	SQLite DB Browser	**Publisher:**	Mauricio Piacentini
Version:	3.12.2		
URL:	https://sqlitebrowser.org/		

Step-by-step methodology:

1. **By analyzing the traces of the use of wiping (shredder) programs, identify which programs were used. Hint: some of the following listed tools were used (default setting, freeware/demo license). (150 points)**

26가지 파일 완전 삭제 도구는 “파일 명 변화”, “시간 변화”, “실 데이터 변화”에 따라 각자의 특징을 가지고 있으며 이에 대하여 비교분석 후 정리하였음 이후 확인한 특징을 기반으로 파일 완전 삭제 도구를 특정할 수 있음

Oh et al.[1]을 포함하여 많은 완전 삭제 탐지 도구에서 파일시스템 기반의 탐지를 시도하였다. 본 문제 역시 $logfile과 $MFT를 이용한 파일 이름 변화와 같은 메타데이터 변화 및 데이터 영역의 변화를 통해 완전 도구들이 남기는 fingerprint를 확인할 수 있다. 이하는 실제 분석 내역이다.

[1] Oh, Dong Bin, Kyung Ho Park, and Huy Kang Kim. "De-Wipimization: Detection of data wiping traces for investigating NTFS file system." *Computers & Security* 99 (2020): 102034.

- ace utilities

1. 메타데이터 변화

2021-05-15 12:...	Renaming File	5.jpg → 2.JRM	2.JRM	...					Create Attribute	0x89a6
	File Deletion		2.JRM	...	2000-01-01 16:00:00	2000-01-01 16:00:00	2021-05-15 12:24:22	2000-01-01 16:...	Delete Index Ent...	0x0
	Renaming File	2.JRM → M.0LD	M.0LD	...					Create Attribute	0x89a6
	File Deletion		M.0LD	...	2000-01-01 16:00:00	2000-01-01 16:00:00	2021-05-15 12:24:22	2000-01-01 16:...	Delete Index Ent...	0x1
	Renaming File	M.0LD → B.9##	B.9##	...					Create Attribute	0x89a6
	File Deletion		B.9##	...	2000-01-01 16:00:00	2000-01-01 16:00:00	2021-05-15 12:24:22	2000-01-01 16:...	Delete Index Ent...	0x1
	Renaming File	B.9## → @.X78	@.X78	...					Create Attribute	0x89a6
	File Deletion		@.X78	...	2000-01-01 16:00:00	2000-01-01 16:00:00	2021-05-15 12:24:22	2000-01-01 16:...	Delete Index Ent...	0x1
	Renaming File	@.X78 → R.%%$	R.%%$	...					Create Attribute	0x89a6
	File Deletion		R.%%$	...	2000-01-01 16:00:00	2000-01-01 16:00:00	2021-05-15 12:24:22	2000-01-01 16:...	Delete Index Ent...	0x1
	Renaming File	R.%%$ → 8.N6I	8.N6I	...					Create Attribute	0x89a6
	File Deletion		8.N6I	...	2000-01-01 16:00:00	2000-01-01 16:00:00	2021-05-15 12:24:22	2000-01-01 16:...	Delete Index Ent...	0x1
	Renaming File	8.N6I → H.GMV	H.GMV	...					Create Attribute	0x89a6
	File Deletion		H.GMV	...	2000-01-01 16:00:00	2000-01-01 16:00:00	2021-05-15 12:24:22	2000-01-01 16:...	Delete Index Ent...	0x1
			H.GMV	...	2000-01-01 16:00:00	2000-01-01 16:00:00	2021-05-15 12:24:22	2000-01-01 16:...	Deallocate File R...	0x89a6

[그림 1] ace utilites 사용에 따른 메타데이터 변화

대문자, 숫자, 특수 문자가 Random 하게 파일명을 구성하고 파일이름에서 확장자의 길이와 파일 이름의 길이 모두 보존된다. MAC 타임 중 일부가 '2000-01-01 16:00:00'으로 변경된 것을 확인할 수 있다. (실험 환경이 UTC-08:00:00이라 16시로 기록된 것으로 추정)

2. 데이터 영역 변화

```
056156000  EA 8D 80 75 D4 67 5B AA  E5 82 82 B6 96 C4 DA D2  ê ▮uÔg[ªå▮▮¶▮ÄÚÒ
056156010  16 E8 47 E9 D8 2B EF D7  CB 35 51 04 F7 47 41 2A   èGéØ+ï×Ë5Q ÷GA*
056156020  6E 0B 50 9E DE CB 82 E8  C2 7B 98 85 52 F2 79 6D  n ▮PÞË▮èÂ{▮▮Ròym
056156030  11 76 98 2C A3 CA 45 C8  95 B4 C3 4E 7E 02 AF 41  ▮v▮,£ÊE▮´ÃN~ ¯A
056156040  35 80 E1 FD 51 1E 66 73  85 57 06 0F AF BD 17 80  5▮áýQ fs▮W ¯½ ▮
056156050  51 85 00 09 0A 05 6C BE  58 63 20 2E 46 EE C9 2D  Q▮    l¾Xc .FîÉ-
056156060  FC 4F 75 07 F4 C2 54 59  C4 74 FB 84 1B 1C ED 7F  üOu ôÂTYÄtû▮  í
056156070  65 B5 BC C9 13 DA 72 F8  80 01 38 53 E4 5D 3E EE  eµ¼É Úrø▮ 8Sä]>î
056156080  AC 6F B9 32 3D 7B 1B 93  71 41 FD 2A B4 D4 11 C3  ¬o¹2={ ▮qAý*´Ô Ã
056156090  95 1D CA 6F E0 3B C2 7F  30 1A C0 40 41 57 AE 79  ▮ Êoà;Â 0 À@AW®y
0561560A0  58 97 81 65 DB 54 38 E4  16 27 DC D6 6C 32 41 0D  X▮ eÛT8ä 'ÜÖl2A
0561560B0  B6 04 85 4E 8F C0 DF 05  C5 BB D6 BB 8F 9E 6C 45  ¶ ▮N Àß Å»Ö» ▮lE
0561560C0  9A AE 48 EE 19 52 6B 04  2D 1D E5 2C 10 C7 20 17  ▮®Hî Rk - å, Ç
0561560D0  55 0C 11 9B 8E F7 35 10  49 EF 4E B0 61 4B 3A 49  U ▮▮÷5 IïN°aK:I
0561560E0  B5 A8 11 4F A3 A8 FA 62  73 2A 22 56 15 E1 99 1A  µ¨ O£¨úbs*"V á▮
0561560F0  33 08 E0 3A 77 FA E7 2E  3B CA 12 C5 B6 0F 5F 3C  3 à:wúç.;Ê Å¶ _<
056156100  CA FB 32 B5 06 1F 9F 56  13 89 CC CD 34 24 11 08  Êû2µ  ▮V ▮ÌÍ4$
056156110  39 A9 3F AC 8A 56 81 16  AA 42 8E F1 12 7A 01 AB  9©?¬▮V ªB▮ñ z «
056156120  54 56 4E 08 81 F8 F6 74  AF 03 20 9A 49 4B A2 62  TVN øöt¯  ▮IK¢b
056156130  73 AF B8 4F FB 89 9E A1  77 8C 20 A9 76 9F 63 50  s¯¸Oû▮▮iw▮ ©v▮cP
056156140  E5 28 16 00 65 58 1A E2  67 61 B0 8D 3D 78 5D 3D  å(  eX âga° =x]=
056156150  8E F2 92 38 5C 1F AA 89  58 E3 48 F2 00 2B D3 32  ▮ò´8\ ª▮XãHò +Ó2
056156160  A4 39 DE 08 1F 6F AD 43  24 64 F5 7C 11 00 F8 4D  ¤9Þ o-C$dõ|  øM
056156170  CC 12 A5 7E AB 16 21 BE  72 5F 87 0F A0 DF 12 CB  Ì ¥~« !¾r_▮  ß Ë
056156180  6A 91 07 0F 27 35 DF A4  81 90 77 F9 0B 1C 26 22  j´  '5ß¤  wù  &"
056156190  DE EA 1B C1 EF E3 76 60  97 94 E9 46 EA 95 60 39  Þê Áïãv`▮▮éFê▮`9
0561561A0  EB 75 80 8A 6F BF 85 19  EE 9B 7E 11 26 83 47 48  ëu▮▮o¿▮ î▮~ &▮GH
```

[그림 2] ace utilites 사용에 따른 데이터 영역 변화

Random Data로 Overwrite 되는 것을 확인할 수 있다.

- ashampoo winoptimizer

1. 메타데이터 변화

EventTime	Event	Detail	FileName	IP	CreateTime	ModifiedTime	MFT_ModifiedTime	AccessTime	RedoInfo	TargetVCN
	필터	필터	필터		필터	필터	필터	필터	필터	필터
	File Deletion		3165255438353309767		2021-05-14 13:36:18	2021-05-15 12:20:14	2021-05-15 12:20:14	2021-05-15 12:20:14	Delete Index Ent...	0x1
			3165255438353309767		2021-05-14 13:36:18	2021-05-15 12:20:14	2021-05-15 12:20:14	2021-05-15 12:20:14	Deallocate File R...	0x89a5
	File Deletion		42.jpg		2021-05-14 13:36:18	2021-05-15 12:20:14	2021-05-15 12:20:14	2021-05-15 12:20:14	Delete Index Ent...	0x1
21-05-15 12:20:14	Renaming File	42.jpg -> 64916...	64916610911156254						Create Attribute	0x89a5
	File Deletion		64916610911156254		2021-05-14 13:36:18	2021-05-15 12:20:14	2021-05-15 12:20:14	2021-05-15 12:20:14	Delete Index Ent...	0x1
			64916610911156254		2021-05-14 13:36:18	2021-05-15 12:20:14	2021-05-15 12:20:14	2021-05-15 12:20:14	Deallocate File R...	0x89a5
	File Deletion		43.jpg		2021-05-14 13:36:18	2021-05-15 12:20:14	2021-05-15 12:20:14	2021-05-15 12:20:14	Delete Index Ent...	0x1
21-05-15 12:20:14	Renaming File	43.jpg -> 30369...	30369740737255436						Create Attribute	0x89a5
	File Deletion		30369740737255436		2021-05-14 13:36:18	2021-05-15 12:20:14	2021-05-15 12:20:14	2021-05-15 12:20:14	Delete Index Ent...	0x1
			30369740737255436		2021-05-14 13:36:18	2021-05-15 12:20:14	2021-05-15 12:20:14	2021-05-15 12:20:14	Deallocate File R...	0x89a5
	File Deletion		1.jpg		2021-05-14 13:36:18	2021-05-15 12:20:14	2021-05-15 12:20:14	2021-05-15 12:20:14	Delete Index Ent...	0x0
21-05-15 12:20:14	Renaming File	1.jpg -> 212804...	21280416934863511						Create Attribute	0x899d
	File Deletion		21280416934863511		2021-05-14 13:36:18	2021-05-15 12:20:14	2021-05-15 12:20:14	2021-05-15 12:20:14	Delete Index Ent...	0x0
			21280416934863511		2021-05-14 13:36:18	2021-05-15 12:20:14	2021-05-15 12:20:14	2021-05-15 12:20:14	Deallocate File R...	0x899d

[그림 3] ashampoo winoptimizer 사용에 따른 메타 데이터 변화

파일명이 숫자로 된 파일로 변경되는 것을 확인할 수 있다. MAC 타임이나 Redo Info 상 특이점은 보이지 않는다.

2. 데이터 영역 변화

```
056182000 AA BA BA 69 59 13 42 0A  C2 C8 14 30 CC 35 00 02  ªººiY B ÂÈ 0Ì5
056182010 01 C1 26 3C 07 8B 52 3C  27 D7 8C 55 CA 15 F5 47   Á&< ‹R<'×ŒUÊ õG
056182020 F6 18 5E 4D D5 1A 72 0B  2E DE C0 15 E8 50 C8 44  ö ^MÕ r .ÞÀ èPÈD
056182030 8C B8 E9 70 C3 90 25 68  D4 E3 80 0D 26 05 A2 7B  Œ¸épÃ %hÔã€ & ¢{
056182040 C2 35 0A 56 D1 DA 07 3C  1A 8E 8B 1F 84 70 D3 57  Â5 VÑÚ < ŽŒ pÓW
056182050 98 C6 4D 69 FF 06 B8 29  FF 22 34 6C 02 F1 14 1B  ˜ÆMiÿ ¸)ÿ"4l ñ
056182060 0E 41 C6 73 4D 43 E7 00  85 88 A8 4D A0 04 E4 62   AÆsMCç …ˆ¨M äb
056182070 25 1B DF 2D BB DD 86 74  AC 44 D7 1E 5E 49 01 23  % ß-»Ý†t¬D× ^I #
056182080 DB 6A D3 1B 49 44 16 41  72 7D F5 32 3C 7D 0E 13  ÛjÓ ID Ar}õ2<}
056182090 31 E6 C3 29 F7 04 11 11  D8 F8 A4 03 3A 7E 4C 2D  1æÃ)÷  Øø¤ :~L-
0561820A0 27 E3 6C 1D C5 CD 7C 0D  DE 1C BA 3B 58 4A 79 7C  'ãl ÅÍ| Þ º;XJy|
0561820B0 BD 57 7C 13 B3 6C 97 28  83 EF A1 64 96 FF CD 16  ½W| ³l—(ƒï¡d–ÿÍ
0561820C0 F2 D9 87 5E C1 CF A4 50  CA 16 68 1C F4 DB 1C 44  òÙ‡^ÁÏ¤PÊ h ôÛ D
0561820D0 C9 9F A2 3D EF 04 DD 58  AF D8 5C 5A 72 3D 0F 6D  É¢=ï ÝX¯Ø\Zr= m
0561820E0 3F 7F 93 00 3D 3A 7A 06  35 1B 5B 68 10 A2 83 11  ? “ =:z 5 [h ¢ƒ
0561820F0 54 EE AA 4F AB BD E6 4F  5B 64 AE 56 CE A7 0B 24  TîªO«½æO[d®VΧ $
056182100 0A 03 39 6D 39 FD 0A 7C  21 DA 98 50 AC 0C 8A 48    9m9ý |!Ú˜P¬ ŠH
056182110 60 73 A3 66 E7 86 BB 6F  87 42 79 57 AA AE F0 13  `s£fç†»o‡ByWª®ð
056182120 56 95 1B 4B B5 08 47 17  8E 03 91 0A C8 8B 1E 0B  V• Kµ G Ž ‘ È‹
056182130 ED 5E F4 1D A3 50 24 7A  33 23 6A 41 06 C2 DD 3E  í^ô £P$z3#jA ÂÝ>
056182140 22 66 98 5A B1 4C C0 26  79 47 DD 5E 64 8F 01 03  "f˜Z±LÀ&yGÝ^d
056182150 F9 E0 1F 00 DF 0A 6C 44  5F B6 B7 62 E2 51 A4 5E  ùà  ß lD_¶·bâQ¤^
056182160 6F A5 86 3A 2D B9 6A 39  E5 55 01 60 80 87 85 73  o¥†:-¹j9åU `€‡…s
056182170 84 29 82 5F 9B A5 1F 73  0C AC E2 1D 3E CE 87 3A  „)‚_›¥ s ¬â >Î‡:
056182180 3B 83 F7 14 29 3E 5C 7E  D1 DE 2A 49 1C E4 4E 13  ;ƒ÷ )>\~ÑÞ*I äN
056182190 91 68 11 17 D7 10 CE 3D  38 B4 75 3C 1A A7 FD 44  ‘h  × Î=8´u< §ýD
0561821A0 87 2F F6 33 A5 CB 8C 2C  3E 92 F1 04 38 15 14 2E  ‡/ö3¥ËŒ,>’ñ 8  .
```

[그림 4] ashampoo winoptimizer 사용에 따른 데이터 영역 변화

Random Data로 Overwrite 되는 것을 확인할 수 있다.

- winutilities file shredder

1. 메타데이터 변화

Renaming File	7.jpg→{216F90...	{216F902A-190C-4C65-A73F-20E0DB2F23E3}					Create Attribute	0x89a6
File Deletion		{216F902A-190C-4C65-A73F-20E0DB2F23E3}	2021-05-14 13:36:18	2021-05-14 14:27:30	2021-05-14 14:27:30	2021-05-14 14:27:30	Delete Index Ent...	0x1
Writing Content ...	Data Runs(in Vol...						Update Mapping...	0x89a6
File Deletion		8.jpg	2021-05-14 13:36:18	2021-05-14 14:27:30	2021-05-14 14:27:30	2021-05-14 14:27:30	Delete Index Ent...	0x1
Renaming File	8.jpg→{937C5...	{937C5872-3EB8-4BA8-8CD9-B49A8477A25B}					Create Attribute	0x89a6
File Deletion		{937C5872-3EB8-4BA8-8CD9-B49A8477A25B}	2021-05-14 13:36:18	2021-05-14 14:27:30	2021-05-14 14:27:30	2021-05-14 14:27:30	Delete Index Ent...	0x1
Writing Content ...	Data Runs(in Vol...						Update Mapping...	0x89a7
File Deletion		9.jpg	2021-05-14 13:36:18	2021-05-14 14:27:30	2021-05-14 14:27:30	2021-05-14 14:27:30	Delete Index Ent...	0x1
Renaming File	9.jpg→{0B997C...	{0B997CEB-77E8-413E-9AC4-4F577AC197DB}					Create Attribute	0x89a7
File Deletion		{0B997CEB-77E8-413E-9AC4-4F577AC197DB}	2021-05-14 13:36:18	2021-05-14 14:27:30	2021-05-14 14:27:30	2021-05-14 14:27:30	Delete Index Ent...	0x1

[그림 5] winutilities file shredder 사용에 따른 메타 데이터 변화

파일 명이 중괄호({})를 포함한 문자열로 변하는 것을 확인할 수 있다. 이외 MAC 타임 등 메타데이터 상 특이점은 확인되지 않는다.

2. 데이터 영역 변화

```
056B5E000  FF D8 FF E0 00 10 4A 46  49 46 00 01 01 01 00 48  ÿØÿà  JFIF     H
056B5E010  00 48 00 00 FF E2 0C 58  49 43 43 5F 50 52 4F 46   H  ÿâ XICC_PROF
056B5E020  49 4C 45 00 01 01 00 00  0C 48 4C 69 6E 6F 02 10  ILE      HLino
056B5E030  00 00 6D 6E 74 72 52 47  42 20 58 59 5A 20 07 CE    mntrRGB XYZ  Î
056B5E040  00 02 00 09 00 06 00 31  00 00 61 63 73 70 4D 53         1  acspMS
056B5E050  46 54 00 00 00 00 49 45  43 20 73 52 47 42 00 00  FT    IEC sRGB
056B5E060  00 00 00 00 00 00 00 00  00 00 00 00 F6 D6 00 01              öÖ
056B5E070  00 00 00 00 D3 2D 48 50  20 20 00 00 00 00 00 00     Ó-HP
056B5E080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
056B5E090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
056B5E0A0  00 00 00 00 00 00 00 00  00 11 63 70 72 74 00 00            cprt
056B5E0B0  01 50 00 00 00 33 64 65  73 63 00 00 01 84 00 00  P   3desc   ▌
056B5E0C0  00 6C 77 74 70 74 00 00  01 F0 00 00 00 14 62 6B   lwtpt   ð     bk
056B5E0D0  70 74 00 00 02 04 00 00  00 14 72 58 59 5A 00 00  pt         rXYZ
056B5E0E0  02 18 00 00 00 14 67 58  59 5A 00 00 02 2C 00 00        gXYZ   ,
056B5E0F0  00 14 62 58 59 5A 00 00  02 40 00 00 00 14 64 6D    bXYZ   @     dm
056B5E100  6E 64 00 00 02 54 00 00  00 70 64 6D 64 64 00 00  nd   T   pdmdd
056B5E110  02 C4 00 00 00 88 76 75  65 64 00 00 03 4C 00 00   Ä   ▌vued   L
056B5E120  00 86 76 69 65 77 00 00  03 D4 00 00 00 24 6C 75   ▌view   Ô   $lu
056B5E130  6D 69 00 00 03 F8 00 00  00 14 6D 65 61 73 00 00  mi   ø     meas
056B5E140  04 0C 00 00 00 24 74 65  63 68 00 00 04 30 00 00       $tech   0
056B5E150  00 0C 72 54 52 43 00 00  04 3C 00 00 08 0C 67 54    rTRC   <     gT
056B5E160  52 43 00 00 04 3C 00 00  08 0C 62 54 52 43 00 00  RC   <     bTRC
056B5E170  04 3C 00 00 08 0C 74 65  78 74 00 00 00 00 43 6F   <     text     Co
056B5E180  70 79 72 69 67 68 74 20  28 63 29 20 31 39 39 38  pyright (c) 1998
056B5E190  20 48 65 77 6C 65 74 74  2D 50 61 63 6B 61 72 64   Hewlett-Packard
056B5E1A0  20 43 6F 6D 70 61 6E 79  00 00 64 65 73 63 00 00   Company  desc
```

[그림 6] winutilities file shredder 사용에 따른 데이터 영역 변화

기본 설정에서는 실제 데이터가 삭제되지 않고 잔재하는 것으로 확인되었다.

- BlankAndSecure

1. 메타데이터 변화

Renaming File	1.jpg → 3.426	3.426	...					Create Attribute	0x899d	0
Renaming File	3.426 → 5.062	5.062	...					Create Attribute	0x899d	0
Renaming File	5.062 → 3.353	3.353	...					Create Attribute	0x899d	0
Renaming File	3.353 → 6.145	6.145	...					Create Attribute	0x899d	0
Renaming File	6.145 → 3.056	3.056	...					Create Attribute	0x899d	0
Renaming File	3.056 → 3.123	3.123	...					Create Attribute	0x899d	0
Renaming File	3.123 → 3.613	3.613	...					Create Attribute	0x899d	0
		3.613	...	1981-01-01 16:00:00	1981-01-01 16:00:00	2021-05-15 12:00:49	1981-01-01 16:...	Deallocate File Record Segment	0x899d	0

[그림 7] BlankAndSecure 사용에 따른 메타 데이터 변화

파일 명이 숫자로 이루어진 파일명으로 변하며, 파일 이름과 확장자 길이를 모두 보존한다. MAC 타임의 일부를 1981-01-01 16:00:00으로 변경하며 Deallocate File Record Segment를 사용하는 것으로 확인할 수 있다. (실험 환경이 UTC-08:00:00이라 16시로 기록된 것으로 추정)

2. 데이터 영역 변화

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
3962DF000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01
3962DF010	00	01	00	00	FF	E1	00	18	45	78	69	66	00	00	49	49
3962DF020	2A	00	08	00	00	00	00	00	00	00	00	00	00	00	FF	DB
3962DF030	00	43	00	06	04	04	04	05	04	06	05	05	06	09	06	05
3962DF040	06	09	0B	08	06	06	08	0B	0C	0A	0A	0B	0A	0A	0C	10
3962DF050	0C	0C	0C	0C	0C	0C	10	0C	0E	0F	10	0F	0E	0C	13	13
3962DF060	14	14	13	13	1C	1B	1B	1B	1C	1F	1F	1F	1F	1F	1F	1F
3962DF070	1F	1F	1F	FF	DB	00	43	01	07	07	07	0D	0C	0D	18	10
3962DF080	10	18	1A	15	11	15	1A	1F	1F	1F	1F	1F	1F	1F	1F	1F
3962DF090	1F	1F	1F	1F	1F	1F	1F	1F	1F	1F	1F	1F	1F	1F	1F	1F
3962DF0A0	1F	1F	1F	1F	1F	1F	1F	1F	1F	1F	1F	1F	1F	1F	1F	1F
3962DF0B0	1F	1F	1F	1F	1F	1F	1F	1F	FF	C2	00	11	08	03	97	07
3962DF0C0	80	03	01	11	00	02	11	01	03	11	01	FF	C4	00	1B	00
3962DF0D0	00	01	05	01	01	00	00	00	00	00	00	00	00	00	00	00
3962DF0E0	03	00	01	02	04	05	06	07	FF	C4	00	1A	01	00	03	01
3962DF0F0	01	01	01	00	00	00	00	00	00	00	00	00	00	00	01	02
3962DF100	03	04	05	06	FF	DA	00	0C	03	01	00	02	10	03	10	00
3962DF110	00	01	F3	19	BB	B8	F4	54	D7	01	5C	5A	CB	69	27	4F
3962DF120	6E	77	4E	EE	1B	D4	DB	11	B9	D0	CB	73	CD	B3	49	8D
3962DF130	02	A1	26	90	CC	48	40	98	93	4D	B2	49	36	69	03	09
3962DF140	D8	C0	2A	81	56	6E	39	CB	74	D9	89	8C	93	31	03	30
3962DF150	93	7B	58	69	B9	CF	7A	F8	5E	9E	76	74	42	5C	28	66
3962DF160	45	8D	42	62	91	9A	8B	A1	24	0B	A0	8E	BD	3A	7A	E5
3962DF170	07	2F	14	59	76	22	A3	49	81	89	B2	2C	FD	25	22	4D
3962DF180	4D	51	A5	C9	B8	8A	BE	91	4D	AA	7A	67	4A	E6	8E	91
3962DF190	5A	A5	34	E8	43	4D	38	3B	22	26	07	1B	A2	45	4D	B4
3962DF1A0	0E	24	D2	1B	B1	DC	A1	B8	A4	1D	32	5E	AF	2B	CB	0B

[그림 8] BlankAndSecure 사용에 따른 데이터 영역 변화

기본 세팅에서는 파일 데이터가 overwrite 되지 않고 존재하는 것을 확인하였다.

- ss data eraser

1. 메타데이터 변화

File Deletion		1.jpg	2021-05-14 13:36:18	2021-05-14 14:39:27	2021-05-14 14:39:27	2021-05-14 14:39:27	Delete Index Ent...	0x0	0
Renaming File	1.jpg -> A.AAA	A.AAA					Create Attribute	0x899d	0
File Deletion		A.AAA	2021-05-14 13:36:18	2021-05-14 14:39:27	2021-05-14 14:39:27	2021-05-14 14:39:27	Delete Index Ent...	0x1	0
Renaming File	A.AAA -> B.BBB	B.BBB					Create Attribute	0x899d	0
File Deletion		B.BBB	2021-05-14 13:36:18	2021-05-14 14:39:27	2021-05-14 14:39:27	2021-05-14 14:39:27	Delete Index Ent...	0x1	0
Renaming File	B.BBB -> C.CCC	C.CCC					Create Attribute	0x899d	0
File Deletion		EE.EEE	2021-05-14 13:36:18	2021-05-14 14:39:28	2021-05-14 14:39:28	2021-05-14 14:39:28	Delete Index Ent...	0x1	0

[그림 9] ss data eraser 사용에 따른 메타 데이터 변화

파일명이 대문자 A부터 Z까지 변경되며 파일 이름과 확장자 길이가 모두 보존된다. MAC 타임이나 Redo Flag 상의 특이점은 없다.

2. 데이터 영역 변화

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
056CA0000	8E	84	B8	C4	86	6A	51	AF	8E	74	D6	F3	CB	2C	8E	DA
056CA0010	FD	61	B2	EA	9F	87	8E	C5	3D	1A	0D	04	B2	81	70	0A
056CA0020	35	F1	48	07	5D	3E	F3	AE	8D	B1	36	4F	79	3B	B2	5B
056CA0030	A5	A9	47	8B	0E	A6	B5	22	70	C0	FA	09	C8	B3	4A	C9
056CA0040	0E	A0	A0	8E	42	14	36	B9	44	EA	78	C6	1F	74	33	69
056CA0050	B7	7F	11	3C	F6	09	B8	62	02	D8	FE	E8	07	31	1D	D9
056CA0060	97	6C	DD	48	C7	23	06	CA	6F	2B	AE	10	3C	AE	20	B3
056CA0070	8B	FF	76	5D	22	09	2D	D2	4A	6D	36	8C	E6	B4	65	FB
056CA0080	83	31	30	8B	72	63	22	FC	7D	00	7D	CA	C2	01	DE	90
056CA0090	B0	49	F1	B6	52	C1	7D	DF	50	0F	52	C5	53	38	F0	99
056CA00A0	B8	D0	DF	0D	BB	92	1E	91	93	7D	1F	76	16	CE	25	F9
056CA00B0	E4	7F	11	71	38	10	E6	1D	D3	D3	96	45	AE	FE	DF	BD
056CA00C0	51	2E	41	EC	10	32	60	ED	88	36	63	79	14	B7	03	8C
056CA00D0	1D	C8	78	1C	7B	9A	78	42	44	51	DA	A5	CA	8A	AA	18
056CA00E0	9C	35	C3	A7	D1	88	25	9A	E7	47	A9	1C	08	A1	D6	8B
056CA00F0	84	4F	DE	A8	B7	C6	1B	28	C9	A4	89	5F	EF	A5	1B	FC
056CA0100	1D	D0	E7	22	53	9D	7B	43	EF	4C	E8	8D	B5	B8	54	DC
056CA0110	75	43	0E	6D	7B	C0	85	D0	3B	6C	A3	D2	DA	5C	50	63
056CA0120	8A	F1	42	A7	E1	3F	46	B9	96	68	AA	DC	52	69	85	08
056CA0130	80	D7	E5	24	49	77	46	5B	27	CE	BC	42	BA	FD	BC	E8
056CA0140	CD	8E	7C	E0	B6	FF	3D	F2	81	41	0D	FE	87	68	C5	3C
056CA0150	6A	42	58	EC	99	9E	BE	0F	D0	71	FC	D6	34	1F	24	C9
056CA0160	04	9E	51	E0	04	34	EC	05	0D	01	C2	CE	74	AB	C4	4C
056CA0170	2C	BF	6D	47	D7	AE	23	59	2C	81	1F	99	60	9A	A4	EC
056CA0180	84	1F	94	18	F0	F5	B1	30	4A	56	0F	08	AB	6C	87	AC
056CA0190	F2	8C	3F	1C	60	E1	7E	C6	E2	AE	74	7B	CB	89	A8	D8
056CA01A0	D1	12	28	62	94	22	C1	D4	FA	71	CE	4E	30	2A	66	76

[그림 10] ss data eraser 사용에 따른 데이터 영역 변화

Random Data로 Overwrite 되는 것을 확인할 수 있다.

- delete files permanently

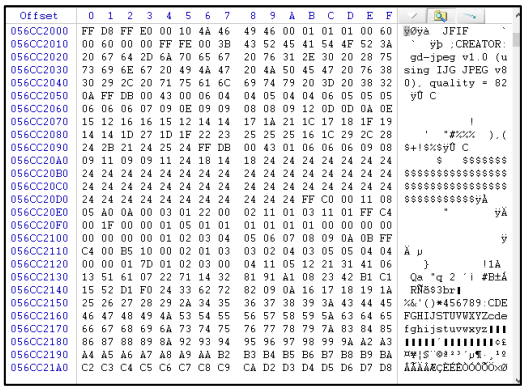
1. 메타데이터 변화

	File Deletion		1.jpg	2000-01-01 16:00:00	2000-01-01 16:00:00	2021-05-14 14:43:46	2000-01-01 16:00:00	Delete Index Ent...	0x0	0
2021-05-14 14:...	Renaming File	1.jpg -> v3eFf	v3eFf					Create Attribute	0x899d	0
	File Deletion		v3eFf	2000-01-01 16:00:00	2000-01-01 16:00:00	2021-05-14 14:43:46	2000-01-01 16:00:00	Delete Index Ent...	0x1	0
	Writing Content ...	Data Runs in Vol...						Update Mapping...	0x899f	4
	File Deletion		2.jpg	2000-01-01 16:00:00	2000-01-01 16:00:00	2021-05-14 14:43:46	2000-01-01 16:00:00	Delete Index Ent...	0x0	0
2021-05-14 14:...	Renaming File	2.jpg -> dCbEP	dCbEP					Create Attribute	0x899f	4
	File Deletion		dCbEP	2000-01-01 16:00:00	2000-01-01 16:00:00	2021-05-14 14:43:46	2000-01-01 16:00:00	Delete Index Ent...	0x1	0

[그림 11] delete files permanently 사용에 따른 메타 데이터 변화

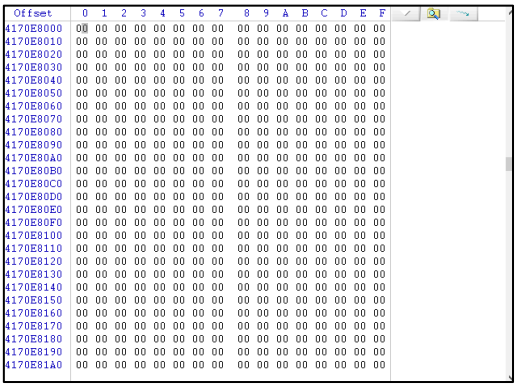
영어 소문자와 대문자로 이루어진 랜덤한 파일명으로 변경한다. “.”을 포함한 총 파일이름 길이는 유지된다. MAC 타임에 있어서 일부를 2000-01-01 16:00:00으로 변경하며 Redo Flag상 특이점은 보이지않는다. (실험 환경이 UTC-08:00:000이라 16시로 기록된 것으로 추정)

2. 데이터 영역 변화



[그림 12] delete files permanently 사용에 따른 데이터 영역 변화 (기본 옵션)

기본으로 설정된 U.S. DOD 5220.22(M)에서는 돌려본 결과 실제 데이터가 삭제되지 않고 잔재하는 것으로 확인되었다. 일부 설정에서는 아래와 같이 zeroize하는 것을 확인하였다.



[그림 13] delete files permanently 사용에 따른 데이터 영역 변화 (일부 옵션)

- file shredder by Pow Tools

1. 메타데이터 변화

Renaming File	1.jpg -> 159098...	1590983.ZZZ						Create Attribute	0x899d	0
File Deletion		1590983.ZZZ		2021-05-14 13:36:18	2021-05-14 14:59:22	2021-05-14 14:59:22	2021-05-14 14:59:22	Delete Index Entry Allocation	0x0	0
File Deletion		2.jpg		2021-05-14 13:36:18	2021-05-14 14:59:22	2021-05-14 14:59:22	2021-05-14 14:59:22	Delete Index Entry Allocation	0x0	0
Renaming File	2.jpg -> 159278...	1592787.ZZZ						Create Attribute	0x899f	4
File Deletion		1592787.ZZZ		2021-05-14 13:36:18	2021-05-14 14:59:22	2021-05-14 14:59:22	2021-05-14 14:59:22	Delete Index Entry Allocation	0x0	0
File Deletion		3.jpg		2021-05-14 13:36:18	2021-05-14 14:59:22	2021-05-14 14:59:22	2021-05-14 14:59:22	Delete Index Entry Allocation	0x1	0
Renaming File	3.jpg -> 159086...	1590863.ZZZ						Create Attribute	0x89a2	2
File Deletion		1590863.ZZZ		2021-05-14 13:36:18	2021-05-14 14:59:22	2021-05-14 14:59:22	2021-05-14 14:59:22	Delete Index Entry Allocation	0x0	0
File Deletion		4.jpg		2021-05-14 13:36:18	2021-05-14 14:59:22	2021-05-14 14:59:22	2021-05-14 14:59:22	Delete Index Entry Allocation	0x1	0

[그림 14] file shredder by Pow Tools 사용에 따른 메타 데이터 변화

파일 이름의 경우 랜덤한 숫자, 파일 확장자의 경우 ZZZ의 형식으로 변하는 것을 확인하였다. MAC 타임과 Redo Flag 상 특이점은 없다.

2. 데이터 영역 변화

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
056DAA000	87	3F	39	7C	A5	07	C2	61	A2	35	E5	DB	4E	B6	41	BF
056DAA010	66	16	AF	7E	78	1B	7B	C9	DE	F4	97	C3	C5	F1	F4	C4
056DAA020	42	D2	DF	AF	7B	9E	6F	D5	DD	11	03	65	6A	98	D6	75
056DAA030	06	DD	9D	8F	E6	DF	35	DD	09	A4	60	D3	B5	6B	9E	7B
056DAA040	1D	80	02	42	F9	95	25	5F	4E	AB	2A	C4	28	90	C6	A7
056DAA050	75	EB	67	8F	F3	D5	5D	F9	20	07	1D	90	43	92	8F	EA
056DAA060	85	31	71	E1	1A	1D	BF	73	74	7D	3D	36	8E	60	FC	5D
056DAA070	44	4A	02	4A	B6	4C	F1	B4	C4	B6	D0	57	95	4B	D5	38
056DAA080	2E	10	42	7C	14	A8	5C	C9	0F	40	62	38	E6	09	A4	DA
056DAA090	41	42	9F	CF	85	D7	2C	E2	D5	8C	BF	C3	16	B4	BA	C8
056DAA0A0	04	84	C9	40	5F	E7	54	56	1E	EE	FB	88	B8	CC	2A	A7
056DAA0B0	7D	5E	B5	6C	F9	48	89	9A	73	A2	6C	B5	6A	33	CB	42
056DAA0C0	39	3A	9A	99	B2	CD	45	4F	E1	C2	AD	24	CA	2D	39	87
056DAA0D0	47	67	F5	AD	EA	AF	C5	32	FB	52	9B	4B	7C	66	D3	8A
056DAA0E0	3C	1A	88	37	07	8B	0B	2A	D8	35	5B	49	25	EC	BD	81
056DAA0F0	2F	68	56	62	70	60	DA	3F	12	36	51	DF	71	32	DE	C7
056DAA100	BC	4E	A7	06	93	92	BF	9D	C4	01	29	75	10	0C	E1	DA
056DAA110	05	AA	09	98	E1	EB	06	97	92	27	CF	13	B3	B5	38	5E
056DAA120	AB	40	4B	35	D0	96	C0	9F	A3	1E	7A	67	13	CD	14	1A
056DAA130	D7	B6	82	9C	D7	23	C3	4F	9F	3F	9C	C2	E9	55	6C	F5
056DAA140	37	99	07	31	74	86	A8	64	B5	C7	F2	1B	F5	B2	FD	03
056DAA150	F7	58	76	FC	29	19	CD	BE	96	D8	7A	0B	FA	B0	47	73
056DAA160	CF	44	AF	A8	78	96	54	62	7A	76	76	D0	BF	7D	8B	9D
056DAA170	F5	97	D7	86	ED	1F	21	79	19	8C	6D	4B	10	AB	D3	FC
056DAA180	25	6A	57	89	14	37	DD	50	B2	E5	29	03	B9	30	E9	2F
056DAA190	9F	BE	DB	48	7D	C6	F8	56	07	34	B8	21	8F	65	5D	F6
056DAA1A0	28	75	53	00	BE	1A	A3	22	5C	0E	6F	72	69	0B	82	3C

[그림 15] file shredder by Pow Tools 사용에 따른 데이터 영역 변화

Random Data로 Overwrite 되는 것을 확인할 수 있다.

- super file shredder

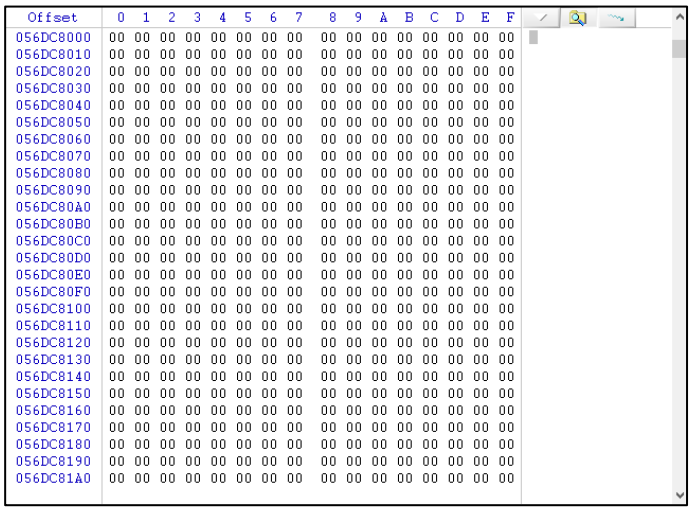
1. 메타데이터 변화

File Deletion		4.jpg	2021-05-14 13:36:18	2021-05-14 14:53:25	2021-05-14 14:53:25	2021-05-14 14:53:25	Delete Index Entry Allocation	0x1	0
Renaming File	4.jpg → 1070E0...	1070E08F2008					Create Attribute	0x89a4	6
File Deletion		1070E08F2008	2021-05-14 13:36:18	2021-05-14 14:53:25	2021-05-14 14:53:25	2021-05-14 14:53:25	Delete Index Entry Allocation	0x0	0
File Deletion		3.jpg	2021-05-14 13:36:18	2021-05-14 14:53:25	2021-05-14 14:53:25	2021-05-14 14:53:25	Delete Index Entry Allocation	0x1	0
File Deletion		2.jpg	2021-05-14 13:36:18	2021-04-03 08:27:21	2021-04-03 08:27:21	2021-05-14 14:53:21	Delete Index Entry Root	0x899c	6
Renaming File	3.jpg → 1070E0...	1070E08F5262					Create Attribute	0x89a2	2
File Deletion		1070E08F5262	2021-05-14 13:36:18	2021-05-14 14:53:25	2021-05-14 14:53:25	2021-05-14 14:53:25	Delete Index Entry Allocation	0x0	0
File Deletion		2.jpg	2021-05-14 13:36:18	2021-05-14 14:53:25	2021-05-14 14:53:25	2021-05-14 14:53:25	Delete Index Entry Allocation	0x0	0
Renaming File	2.jpg → 1070E0...	1070E08F1691					Create Attribute	0x899f	4
File Deletion		1070E08F1691	2021-05-14 13:36:18	2021-05-14 14:53:25	2021-05-14 14:53:25	2021-05-14 14:53:25	Delete Index Entry Allocation	0x0	0
File Deletion		1.jpg	2021-05-14 13:36:18	2021-05-14 14:53:25	2021-05-14 14:53:25	2021-05-14 14:53:25	Delete Index Entry Allocation	0x0	0
Renaming File	1.jpg → 1070E0...	1070E08F6749					Create Attribute	0x899d	0
File Deletion		1070E08F6749	2021-05-14 13:36:18	2021-05-14 14:53:25	2021-05-14 14:53:25	2021-05-14 14:53:25	Delete Index Entry Root	0x899c	6

[그림 16] super file shredder 사용에 따른 메타 데이터 변화

1070E08 이라는 문자열 뒤 랜덤 숫자 4자리를 파일명으로 사용한다. MAC과 redo Flag 상 특이점은 보이지 않는다.

2. 데이터 영역 변화



[그림 17] super file shredder 사용에 따른 데이터 영역 변화

Zeroize를 통해 해당 영역을 0x00으로 wiping한다.

- freeraser

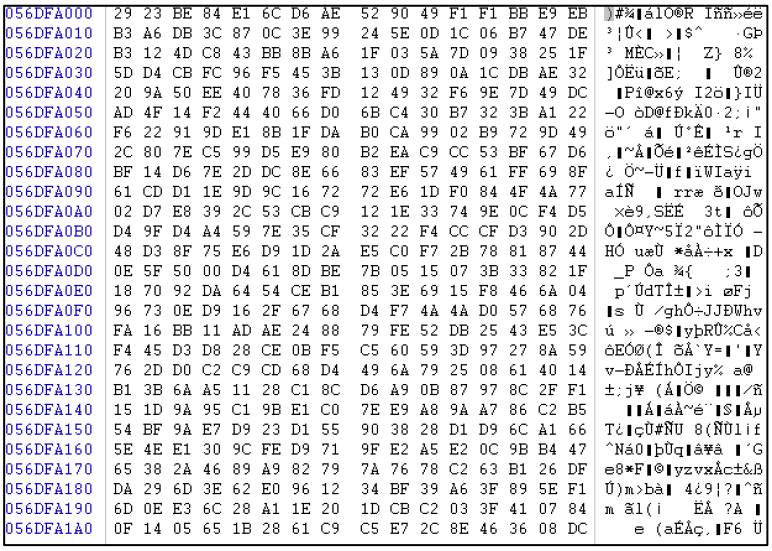
1. 메타데이터 변화

File Creation		FREERASER....	...	2021-05-14 15:05:48	2021-05-14 15:05:48	2021-05-14 15:05:48	2021-05-14 15:05:48	Initialize File Record Segment	0x89a8	6
Writing Content ...	Dat...	FREERASER....	...					Update Mapping Pairs	0x89a8	6
Writing Content ...	Dat...							Update Mapping Pairs	0x5264	6
File Deletion		1.jpg	...	2021-05-14 13:36:18	2021-05-14 15:05:51	2021-05-14 15:05:51	2021-05-14 15:05:51	Delete Index Entry Allocation	0x0	0
File Deletion		2.jpg	...	2021-05-14 13:36:18	2021-05-14 15:05:51	2021-05-14 15:05:51	2021-05-14 15:05:51	Delete Index Entry Allocation	0x0	0
File Deletion		3.jpg	...	2021-05-14 13:36:18	2021-05-14 15:05:52	2021-05-14 15:05:52	2021-05-14 15:05:52	Delete Index Entry Allocation	0x1	0
File Deletion		4.jpg	...	2021-05-14 13:36:18	2021-05-14 15:05:52	2021-05-14 15:05:52	2021-05-14 15:05:52	Delete Index Entry Allocation	0x1	0
File Deletion		5.jpg	...	2021-05-14 13:36:18	2021-05-14 15:05:52	2021-05-14 15:05:52	2021-05-14 15:05:52	Delete Index Entry Allocation	0x1	0
File Deletion		6.png	...	2021-05-14 13:36:18	2021-05-14 15:05:52	2021-05-14 15:05:52	2021-05-14 15:05:52	Delete Index Entry Allocation	0x1	0
File Deletion		7.jpg	...	2021-05-14 13:36:18	2021-05-14 15:05:52	2021-05-14 15:05:52	2021-05-14 15:05:52	Delete Index Entry Allocation	0x1	0
File Deletion		8.jpg	...	2021-05-14 13:36:18	2021-05-14 15:05:52	2021-05-14 15:05:52	2021-05-14 15:05:52	Delete Index Entry Allocation	0x1	0
File Deletion		9.jpg	...	2021-05-14 13:36:18	2021-05-14 15:05:52	2021-05-14 15:05:52	2021-05-14 15:05:52	Delete Index Entry Allocation	0x1	0
File Deletion		10.jpg	...	2021-05-14 13:36:18	2021-05-14 15:05:52	2021-05-14 15:05:52	2021-05-14 15:05:52	Delete Index Entry Allocation	0x0	0
File Deletion		11.jpg	...	2021-05-14 13:36:18	2021-05-14 15:05:52	2021-05-14 15:05:52	2021-05-14 15:05:52	Delete Index Entry Allocation	0x0	0
File Deletion		12.jpg	...	2021-05-14 13:36:18	2021-05-14 15:05:52	2021-05-14 15:05:52	2021-05-14 15:05:52	Delete Index Entry Allocation	0x0	0

[그림 18] freeraser 사용에 따른 메타 데이터 변화

특이점 없이 Delete Index Entry Allocation을 통해 파일을 삭제한다. 파일 명 변화나 MAC 타임의 변화는 발견되지않는다.

2. 데이터 영역 변화



[그림 19] freeraser 사용에 따른 데이터 영역 변화

Random Data로 Overwrite 되는 것을 확인할 수 있다.

- hardwipe

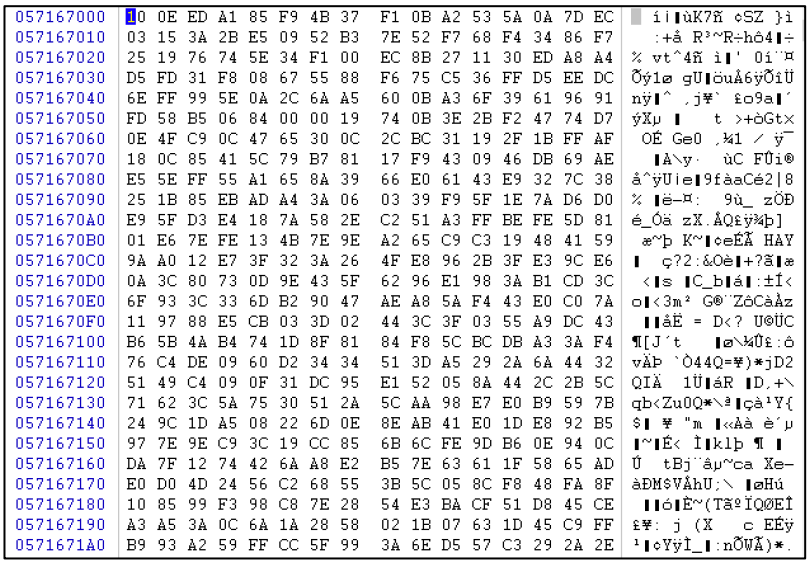
1. 메타데이터 변화

File Deletion		1.jpg	2021-05-14 13:36:18	2021-05-14 15:11:09	2021-05-14 15:11:09	2021-05-14 15:...	Delete Index Entry Allocation	0x0	0
Renaming File	1.jpg → gjfqcnpi	gjfqcnpi					Create Attribute	0x899d	0
File Deletion		gjfqcnpi	2021-05-14 13:36:18	2021-05-14 15:11:09	2021-05-14 15:11:09	2021-05-14 15:...	Delete Index Entry Allocation	0x1	0
Renaming File	gjfqcnpi → etjigrrq	etjigrrq					Create Attribute	0x899d	0
File Deletion		etjigrrq	2021-05-14 13:36:18	2021-05-14 15:11:09	2021-05-14 15:11:09	2021-05-14 15:...	Delete Index Entry Allocation	0x1	0
Renaming File	etjigrrq → otrmu...	otrmutbi					Create Attribute	0x899d	0
File Deletion		otrmutbi	2021-05-14 13:36:18	2021-05-14 15:11:09	2021-05-14 15:11:09	2021-05-14 15:...	Delete Index Entry Allocation	0x1	0

[그림 20] hardwipe 사용에 따른 메타 데이터 변화

영어 소문자로만 구성된 파일 명을 사용한다. 파일 이름의 길이와는 무관하며 MAC time과 Redo Flag 또한 관련이 적다

2. 데이터 영역 변화



[그림 21] hardwipe 사용에 따른 데이터 영역 변화

Random Data로 Overwrite 되는 것을 확인할 수 있다.

- hard disk scrubber

1. 메타데이터 변화

2021-05-14 15:15:31	File Deletion	6.png	2021-05-14 13:36:18	2021-05-14 15:15:29	2021-05-14 15:15:29	2021-05-14 15:15:29	Delete Index Entry Allocation	0x1	0
2021-05-14 15:15:31	File Deletion	7.jpg	2021-05-14 13:36:18	2021-05-14 15:15:29	2021-05-14 15:15:29	2021-05-14 15:15:29	Delete Index Entry Allocation	0x1	0
2021-05-14 15:15:31	File Deletion	8.jpg	2021-05-14 13:36:18	2021-05-14 15:15:29	2021-05-14 15:15:29	2021-05-14 15:15:29	Delete Index Entry Allocation	0x1	0
2021-05-14 15:15:31	File Deletion	9.jpg	2021-05-14 13:36:18	2021-05-14 15:15:29	2021-05-14 15:15:29	2021-05-14 15:15:29	Delete Index Entry Allocation	0x1	0
2021-05-14 15:15:31	File Deletion	10.jpg	2021-05-14 13:36:18	2021-05-14 15:15:29	2021-05-14 15:15:29	2021-05-14 15:15:29	Delete Index Entry Allocation	0x0	0
2021-05-14 15:15:31	File Deletion	11.jpg	2021-05-14 13:36:18	2021-05-14 15:15:29	2021-05-14 15:15:29	2021-05-14 15:15:29	Delete Index Entry Allocation	0x0	0
2021-05-14 15:15:31	File Deletion	12.jpg	2021-05-14 13:36:18	2021-05-14 15:15:29	2021-05-14 15:15:29	2021-05-14 15:15:29	Delete Index Entry Allocation	0x0	0
2021-05-14 15:15:31	File Deletion	13.jpg	2021-05-14 13:36:18	2021-05-14 15:15:29	2021-05-14 15:15:29	2021-05-14 15:15:29	Delete Index Entry Allocation	0x0	0
2021-05-14 15:15:31	File Deletion	14.jpg	2021-05-14 13:36:18	2021-05-14 15:15:29	2021-05-14 15:15:29	2021-05-14 15:15:29	Delete Index Entry Allocation	0x0	0
2021-05-14 15:15:31	File Deletion	15.jpeg	2021-05-14 13:36:18	2021-05-14 15:15:30	2021-05-14 15:15:30	2021-05-14 15:15:30	Delete Index Entry Allocation	0x0	0
2021-05-14 15:15:31	File Deletion	16.jpg	2021-05-14 13:36:18	2021-05-14 15:15:30	2021-05-14 15:15:30	2021-05-14 15:15:30	Delete Index Entry Allocation	0x0	0
2021-05-14 15:15:31	File Deletion	17.jpg	2021-05-14 13:36:18	2021-05-14 15:15:30	2021-05-14 15:15:30	2021-05-14 15:15:30	Delete Index Entry Allocation	0x0	0
2021-05-14 15:15:31	File Deletion	19.jpg	2021-05-14 13:36:18	2021-05-14 15:15:30	2021-05-14 15:15:30	2021-05-14 15:15:30	Delete Index Entry Allocation	0x0	0

[그림 22] hard disk scrubber 사용에 따른 메타 데이터 변화

특이점 없이 Delete Index Entry Allocation을 통해 파일을 삭제한다. 파일 명 변화나 MAC 타임의 변화는 발견되지않는다.

2. 데이터 영역 변화

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
054A79000	D8	F2	C2	7D	A8	AC	88	C1	7A	E8	8B	5A	8C	DB	CD	D4
054A79010	FF	AA	31	33	61	75	E3	D9	00	72	15	26	AD	26	47	F0
054A79020	C7	09	AD	45	A8	1C	4F	1A	D4	43	F9	E1	82	6B	2B	22
054A79030	64	CB	84	95	B9	C6	6F	56	19	44	FA	2D	84	83	2D	11
054A79040	A3	B5	47	52	47	F1	A5	15	86	46	52	10	1D	FD	7A	B3
054A79050	E2	4E	39	25	6E	25	83	C7	57	AF	28	24	97	C5	23	7E
054A79060	F6	86	BD	64	A1	A3	37	F3	3C	28	FB	C4	0C	DB	90	97
054A79070	24	6D	CC	3E	9F	13	00	69	48	51	17	42	56	FF	F1	01
054A79080	0C	DF	60	EE	5A	39	97	6C	E3	6F	FF	0E	02	64	A8	D1
054A79090	9B	35	E3	EC	F0	A3	A8	EB	BB	1C	E2	F1	38	5C	C3	57
054A790A0	F8	F6	A3	19	96	54	3A	A9	B0	F8	0B	32	B6	0C	60	57
054A790B0	79	87	42	F2	8A	7C	23	72	C6	57	4B	D0	B5	18	29	31
054A790C0	8F	D8	21	BF	00	24	79	49	16	F4	70	A9	E2	58	BA	16
054A790D0	B6	19	D5	C4	18	DC	FD	96	C0	9D	B3	B2	4A	84	17	34
054A790E0	6A	64	95	70	C6	6F	91	5C	D3	E6	25	1F	47	E5	1C	EB
054A790F0	0E	74	AA	8D	CA	91	A4	63	46	DA	22	9C	77	04	E7	F9
054A79100	E7	4E	E0	71	9A	8F	A3	6B	E3	A8	C3	75	A7	5F	50	AB
054A79110	00	F5	F5	2B	55	FF	6B	59	38	53	46	CB	C3	12	53	0D
054A79120	27	1C	08	B8	B1	71	B5	6E	89	65	87	C0	C8	8C	85	1C
054A79130	D0	CF	0C	2E	EF	1F	8A	6D	BC	9D	6C	AC	B5	3B	7D	F2
054A79140	0F	29	34	F1	C6	99	B0	D3	4C	9E	55	48	77	40	4C	F9
054A79150	84	05	69	DD	56	7C	1C	05	39	A2	8A	E1	DB	1F	E8	1C
054A79160	4A	A6	B2	7B	17	1B	61	7D	F6	28	B0	89	81	68	9D	F2
054A79170	E9	71	AB	31	C9	36	21	FF	5C	A2	36	43	C6	72	7D	F4
054A79180	45	96	F2	6B	65	A2	7A	C3	96	29	C4	35	B9	02	D1	A9
054A79190	8E	C2	96	D7	0C	00	7A	AA	15	2D	AC	DA	0A	FF	88	D8
054A791A0	31	CF	89	88	F7	6B	8F	6D	7E	20	5D	2F	F8	21	A6	B6

[그림 23] hard disk scrubber 사용에 따른 데이터 영역 변화

Random Data로 Overwrite 되는 것을 확인할 수 있다.

- kernel file shredder

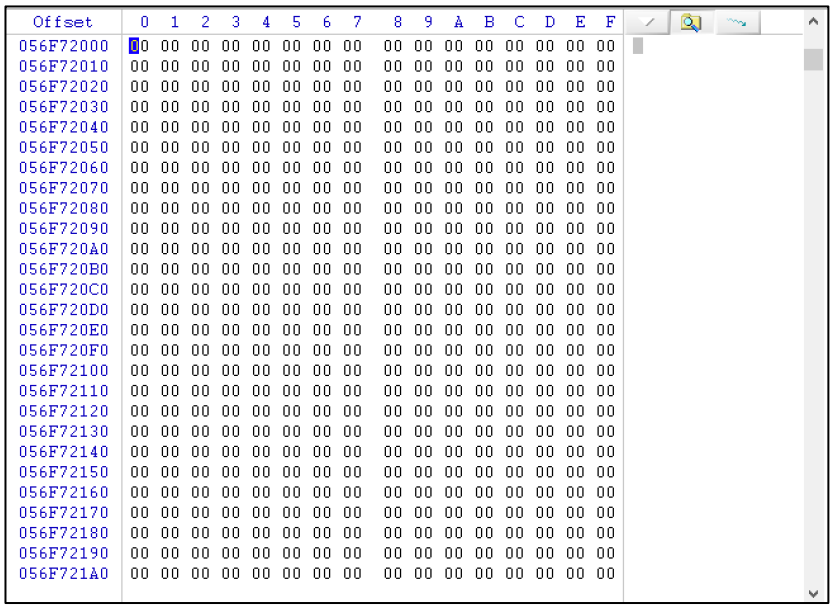
1. 메타데이터 변화

Event	Detail	FileName	IP	CreateTime	ModifiedTime	MFT_ModifiedTime	AccessTime	RedoInfo	TargetVCN	MFT_ClusterIndex
필터	필터	필터		필터	필터	필터	필터	필터	필터	필터
		30.jpg		2021-05-14 01:04:38	2021-04-04 19:12:44	2021-04-04 19:12:44	2021-05-14 13:36:19	Update Resident Value	0x8995	4
		36.jpg		2021-05-14 01:04:38	2021-04-03 08:20:20	2021-04-03 08:20:20	2021-05-14 13:36:19	Update Resident Value	0x8995	6
		35.jpg		2021-05-14 01:04:38	2021-04-04 19:20:57	2021-04-04 19:20:57	2021-05-14 13:36:19	Update Resident Value	0x8996	0
		34.jpg		2021-05-14 01:04:38	2021-04-04 19:19:56	2021-04-04 19:19:56	2021-05-14 13:36:19	Update Resident Value	0x8996	2
		22.png		2021-05-14 01:04:36	2021-04-04 19:21:18	2021-04-04 19:21:18	2021-05-14 13:36:19	Update Resident Value	0x8996	4
		24.png		2021-05-14 01:04:36	2021-04-03 08:21:42	2021-04-03 08:21:42	2021-05-14 13:36:19	Update Resident Value	0x8996	6
		39.jpeg		2021-05-14 01:04:38	2021-04-04 19:10:57	2021-04-04 19:10:57	2021-05-14 13:36:19	Update Resident Value	0x8997	0
		15.jpeg		2021-05-14 01:04:37	2021-04-04 19:09:07	2021-04-04 19:09:07	2021-05-14 13:36:19	Update Resident Value	0x8997	2
		9.jpg		2021-05-14 13:32:34	2021-04-03 08:20:46	2021-04-03 08:20:46	2021-05-14 13:36:19	Update Resident Value	0x8997	4
		8.jpg		2021-05-14 01:04:36	2021-04-03 08:20:46	2021-04-03 08:20:46	2021-05-14 13:36:19	Update Resident Value	0x8997	6
		5.jpg		2021-05-14 01:04:37	2021-04-04 19:11:50	2021-04-04 19:11:50	2021-05-14 13:36:19	Update Resident Value	0x8998	0
		43.jpg		2021-05-14 01:04:38	2021-04-03 08:20:58	2021-04-03 08:20:58	2021-05-14 13:36:19	Update Resident Value	0x8998	2
		4.jpg		2021-05-14 01:04:36	2021-04-04 19:11:31	2021-04-04 19:11:31	2021-05-14 13:36:19	Update Resident Value	0x8998	4
		42.jpg		2021-05-14 01:04:38	2021-04-03 08:18:25	2021-04-03 08:18:25	2021-05-14 13:36:19	Update Resident Value	0x8998	6
		7.jpg		2021-05-14 01:04:36	2021-04-03 08:18:58	2021-04-03 08:18:58	2021-05-14 13:36:19	Update Resident Value	0x8999	0
		40.jpg		2021-05-14 13:34:03	2021-04-03 08:19:43	2021-04-03 08:19:43	2021-05-14 13:36:19	Update Resident Value	0x8999	2
		1.jpg		2021-05-14 13:32:11	2021-04-03 08:27:21	2021-04-03 08:27:21	2021-05-14 13:36:19	Update Resident Value	0x8999	4
		3.jpg		2021-05-14 01:04:36	2021-04-03 08:27:28	2021-04-03 08:27:28	2021-05-14 13:36:19	Update Resident Value	0x8999	6

[그림 24] kernel file shredder 사용에 따른 메타 데이터 변화

Update Resident Value라는 Redo 방식을 통해 wiping을 진행한다. MAC time이나 파일 명에 특이점은 존재하지 않는다.

2. 데이터 영역 변화



[그림 25] kernel file shredder 사용에 따른 데이터 영역 변화

Zeroize를 통해 해당 영역을 0x00으로 wiping한다.

- pc shredder

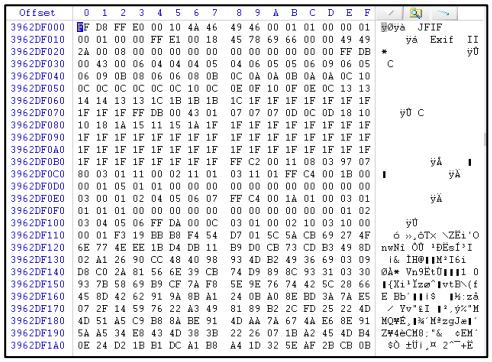
1. 메타데이터 변화

	File Deletion		1.jpg	2021-05-14 13:36:18	2021-05-14 15:22:50	2021-05-14 15:22:50	2021-05-14 15:...	Delete Index Ent...	0x0
2021-05-14 15:22:50	Renaming File	1.jpg -> _temp4...	_temp41865644161					Create Attribute	0x899d
	File Deletion		_temp41865644161	2021-05-14 13:36:18	2021-05-14 15:22:50	2021-05-14 15:22:50	2021-05-14 15:...	Delete Index Ent...	0x1
	File Deletion		2.jpg	2021-05-14 13:36:18	2021-05-14 15:22:50	2021-05-14 15:22:50	2021-05-14 15:...	Delete Index Ent...	0x0
2021-05-14 15:22:50	Renaming File	2.jpg -> _temp1...	_temp18505443671					Create Attribute	0x899f
	File Deletion		_temp18505443671	2021-05-14 13:36:18	2021-05-14 15:22:50	2021-05-14 15:22:50	2021-05-14 15:...	Delete Index Ent...	0x1
	File Deletion		3.jpg	2021-05-14 13:36:18	2021-05-14 15:22:50	2021-05-14 15:22:50	2021-05-14 15:...	Delete Index Ent...	0x1
2021-05-14 15:22:50	Renaming File	3.jpg -> _temp3...	_temp39735858071					Create Attribute	0x89a2
	File Deletion		_temp39735858071	2021-05-14 13:36:18	2021-05-14 15:22:50	2021-05-14 15:22:50	2021-05-14 15:...	Delete Index Ent...	0x1
	File Deletion		4.jpg	2021-05-14 13:36:18	2021-05-14 15:22:50	2021-05-14 15:22:50	2021-05-14 15:...	Delete Index Ent...	0x1

[그림 26] pc shredder 사용에 따른 메타 데이터 변화

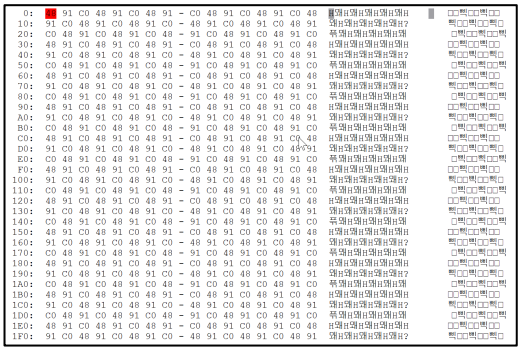
파일 명을 _temp397358580710이라는 값으로 변경하는 특징이 있다. MAC time이나 Redo 관련 특이점은 없다

2. 데이터 영역 변화



[그림 27] pc shredder 사용에 따른 데이터 영역 변화 (기본 세팅)

기본 세팅에서는 파일 데이터가 overwrite 되지 않고 존재하는 것을 확인하였다.



[그림 28] pc shredder 사용에 따른 데이터 영역 변화 (일부 세팅)

일부 세팅에서는 데이터 영역이 0x4891c0과 같이 일정한 문자열 패턴으로 wiping 되어 있음을 확인했다

- remo file eraser

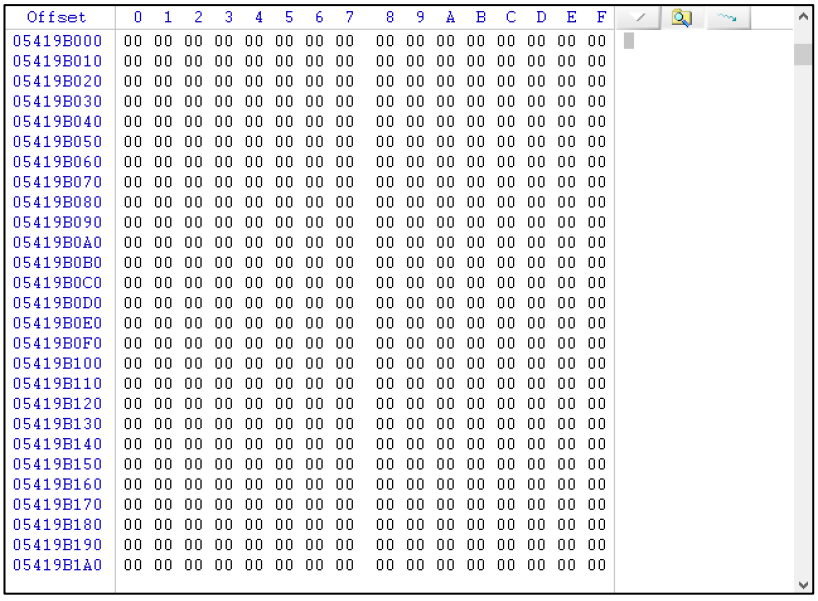
1. 메타데이터 변화

2021-05-14 15:28:37	Renaming File	6.png → x.xxx	x.xxx					Create Attribute	0x89a6	2
	File Deletion		x.xxx	2021-05-14 13:36:18	2021-05-14 15:28:37	2021-05-14 15:28:37	2021-05-14 15:...	Delete Index Ent...	0x1	0
	File Deletion		5.jpg	2021-05-14 13:36:18	2021-05-14 15:28:38	2021-05-14 15:28:38	2021-05-14 15:...	Delete Index Ent...	0x1	0
2021-05-14 15:28:38	Renaming File	5.jpg → x.xxx	x.xxx					Create Attribute	0x89a6	0
	File Deletion		x.xxx	2021-05-14 13:36:18	2021-05-14 15:28:38	2021-05-14 15:28:38	2021-05-14 15:...	Delete Index Ent...	0x1	0
	File Deletion		4.jpg	2021-05-14 13:36:18	2021-05-14 15:28:38	2021-05-14 15:28:38	2021-05-14 15:...	Delete Index Ent...	0x1	0
2021-05-14 15:28:38	Renaming File	4.jpg → x.xxx	x.xxx					Create Attribute	0x89a4	6
	File Deletion		x.xxx	2021-05-14 13:36:18	2021-05-14 15:28:38	2021-05-14 15:28:38	2021-05-14 15:...	Delete Index Ent...	0x1	0
	File Deletion		3.jpg	2021-05-14 13:36:18	2021-05-14 15:28:39	2021-05-14 15:28:39	2021-05-14 15:...	Delete Index Ent...	0x1	0
	File Deletion		2.jpg	2021-05-14 13:36:18	2021-04-03 08:27:21	2021-04-03 08:27:21	2021-05-14 15:...	Delete Index Ent...	0x899c	6
	Renaming File	3.jpg → x.xxx	x.xxx					Create Attribute	0x89a2	2
	File Deletion		x.xxx	2021-05-14 13:36:18	2021-05-14 15:28:39	2021-05-14 15:28:39	2021-05-14 15:...	Delete Index Ent...	0x0	0
	File Deletion		2.jpg	2021-05-14 13:36:18	2021-05-14 15:28:40	2021-05-14 15:28:40	2021-05-14 15:...	Delete Index Ent...	0x0	0
2021-05-14 15:28:40	Renaming File	2.jpg → x.xxx	x.xxx					Create Attribute	0x899f	4
	File Deletion		x.xxx	2021-05-14 13:36:18	2021-05-14 15:28:40	2021-05-14 15:28:40	2021-05-14 15:...	Delete Index Ent...	0x0	0
	File Deletion		1.jpg	2021-05-14 13:36:18	2021-05-14 15:28:40	2021-05-14 15:28:40	2021-05-14 15:...	Delete Index Ent...	0x0	0
	Renaming File	1.jpg → x.xxx	x.xxx					Create Attribute	0x899d	0
	File Deletion		x.xxx	2021-05-14 13:36:18	2021-05-14 15:28:40	2021-05-14 15:28:40	2021-05-14 15:...	Delete Index Ent...	0x899c	6

[그림 29] remo file eraser 사용에 따른 메타 데이터 변화

파일 명을 소문자 x로 변경하며 파일 이름과 확장자의 길이 모두 보존한다. MAC Time이나 redo Flag 상의 특이점은 없다.

2. 데이터 영역 변화



[그림 30] remo file eraser 사용에 따른 데이터 영역 변화

Zeroize를 통해 해당 영역을 0x00으로 wiping한다.

- sdelete

1. 메타데이터 변화

File Deletion		2.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x0	0
File Deletion		20.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x0	0
File Deletion		21.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x0	0
File Deletion		23.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x0	0
File Deletion		25.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x0	0
File Deletion		26.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x0	0
File Deletion		27.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x0	0
File Deletion		24.png	...	2021-05-14 13:36:18	2021-04-03 08:21:42	2021-04-03 08:21:42	2021-05-14 15:35:08	Delete Index Entry Allocation	0x0	0
File Deletion		28.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Root	0x899c	6
File Deletion		29.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x1	0
File Deletion		3.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x1	0
File Deletion		30.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x1	0
File Deletion		31.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x1	0
File Deletion		32.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x1	0
File Deletion		33.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x1	0
File Deletion		34.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x1	0
File Deletion		35.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x1	0
File Deletion		36.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x1	0
File Deletion		38.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x1	0
File Deletion		4.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x1	0
File Deletion		40.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x1	0
File Deletion		42.jpg	...	2021-05-14 13:36:18	2021-05-14 15:35:18	2021-05-14 15:35:18	2021-05-14 15:35:18	Delete Index Entry Allocation	0x1	0

[그림 31] sdelete 사용에 따른 메타 데이터 변화

특이점 없이 Delete Index Entry Allocation을 통해 파일을 삭제한다. 파일 명 변화나 MAC 타임의 변화는 발견되지않는다.

2. 데이터 영역 변화

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
056FBC000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC0A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC0B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC0C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC0D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC0E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC0F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FBC1A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

[그림 32] sdelete 사용에 따른 데이터 영역 변화

Zeroize를 통해 해당 영역을 0x00으로 wiping한다.

- securely file shredder

1. 메타데이터 변화

File Deletion		1.jpg	2021-05-14 13:36:18	2021-05-14 15:42:20	2021-05-14 15:42:20	2021-05-14 15:42:20	Delete Index Ent...	0x0	0
Renaming File	1.jpg -> aaaaaa.aaa	aaaaaa.aaa					Create Attribute	0x899d	0
File Deletion		aaaaaa.aaa	2021-05-14 13:36:18	2021-05-14 15:42:20	2021-05-14 15:42:20	2021-05-14 15:42:20	Delete Index Ent...	0x1	0
Renaming File	aaaaaa.aaa -> bbb...	bbbbbb.bbb					Create Attribute	0x899d	0
File Deletion		bbbbbb.bbb	2021-05-14 13:36:18	2021-05-14 15:42:20	2021-05-14 15:42:20	2021-05-14 15:42:20	Delete Index Ent...	0x1	0
Renaming File	bbbbbb.bbb -> cc...	cccccc.ccc					Create Attribute	0x899d	0
File Deletion		cccccc.ccc	2021-05-14 13:36:18	2021-05-14 15:42:20	2021-05-14 15:42:20	2021-05-14 15:42:20	Delete Index Ent...	0x1	0
Renaming File	cccccc.ccc -> ddd...	dddddd.ddd					Create Attribute	0x899d	0
File Deletion		dddddd.ddd	2021-05-14 13:36:18	2021-05-14 15:42:20	2021-05-14 15:42:20	2021-05-14 15:42:20	Delete Index Ent...	0x1	0
Renaming File	dddddd.ddd -> ee...	eeeeee.eee					Create Attribute	0x899d	0
File Deletion		eeeeee.eee	2021-05-14 13:36:18	2021-05-14 15:42:20	2021-05-14 15:42:20	2021-05-14 15:42:20	Delete Index Ent...	0x1	0
Renaming File	eeeeee.eee -> ffff...	ffffff.fff					Create Attribute	0x899d	0
File Deletion		ffffff.fff	2021-05-14 13:36:18	2021-05-14 15:42:20	2021-05-14 15:42:20	2021-05-14 15:42:20	Delete Index Ent...	0x1	0
Renaming File	ffffff.fff -> gggggg...	gggggg.ggg					Create Attribute	0x899d	0
File Deletion		gggggg.ggg	2021-05-14 13:36:18	2021-05-14 15:42:20	2021-05-14 15:42:20	2021-05-14 15:42:20	Delete Index Ent...	0x1	0
Renaming File	gggggg.ggg -> hh...	hhhhhh.hhh					Create Attribute	0x899d	0
File Deletion		hhhhhh.hhh	2021-05-14 13:36:18	2021-05-14 15:42:20	2021-05-14 15:42:20	2021-05-14 15:42:20	Delete Index Ent...	0x1	0
Renaming File	hhhhhh.hhh -> iiii...	iiiiii.iii					Create Attribute	0x899d	0
File Deletion		iiiiii.iii	2021-05-14 13:36:18	2021-05-14 15:42:20	2021-05-14 15:42:20	2021-05-14 15:42:20	Delete Index Ent...	0x1	0
Renaming File	iiiiii.iii -> jjjjjj.jjj	jjjjjj.jjj					Create Attribute	0x899d	0
File Deletion		jjjjjj.jjj	2021-05-14 13:36:18	2021-05-14 15:42:20	2021-05-14 15:42:20	2021-05-14 15:42:20	Delete Index Ent...	0x1	0
Renaming File	jjjjjj.jjj -> kkkkkk....	kkkkkk.kkk					Create Attribute	0x899d	0
File Deletion		kkkkkk.kkk	2021-05-14 13:36:18	2021-05-14 15:42:20	2021-05-14 15:42:20	2021-05-14 15:42:20	Delete Index Ent...	0x1	0
Renaming File	kkkkkk.kkk -> llllll...	llllll.lll					Create Attribute	0x899d	0
File Deletion		llllll.lll	2021-05-14 13:36:18	2021-05-14 15:42:20	2021-05-14 15:42:20	2021-05-14 15:42:20	Delete Index Ent...	0x1	0
Renaming File	llllll.lll -> mmmm...	mmmmmm.mmm					Create Attribute	0x899d	0

[그림 33] securely file shredder 사용에 따른 메타 데이터 변화

소문자 a부터 z까지 증가하며 파일이름을 변경한다 파일이름 6글자 확장자 3글자를 고정으로 사용하며 MAC Time이나 Redo 상 특이점은 없다.

2. 데이터 영역 변화

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
056FD0000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD00A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD00B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD00C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD00D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD00E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD00F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD0190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
056FD01A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

[그림 34] securely file shredder 사용에 따른 데이터 영역 변화

Zeroize를 통해 해당 영역을 0x00으로 wiping한다.

- secure eraser

1. 메타데이터 변화

21..05..14 15:...	Renaming File	2.jpg → x.xxx	x.xxx	\Us...					Create Attribute	0x899f	4
	File Deletion		x.xxx	\Us...	2021..05..14 13:36:18	2021..05..14 15:46:38	2021..05..14 15:46:38	2021..05..14 15:...	Delete Index Entry Allocation	0x0	0
	Renaming File	x.xxx → y.yyy	y.yyy	\Us...					Create Attribute	0x899f	4
	File Deletion		y.yyy	\Us...	2021..05..14 13:36:18	2021..05..14 15:46:38	2021..05..14 15:46:38	2021..05..14 15:...	Delete Index Entry Allocation	0x0	0
	Renaming File	y.yyy → z.zzz	z.zzz	\Us...					Create Attribute	0x899f	4
	File Deletion		z.zzz	\Us...	2021..05..14 13:36:18	2021..05..14 15:46:38	2021..05..14 15:46:38	2021..05..14 15:...	Delete Index Entry Allocation	0x0	0
	Renaming File	z.zzz → 8.888	8.888	\Us...					Create Attribute	0x899f	4
	File Deletion		8.888	\Us...	2021..05..14 13:36:18	2021..05..14 15:46:38	2021..05..14 15:46:38	2021..05..14 15:...	Delete Index Entry Allocation	0x0	0
	Renaming File	8.888 → 9.999	9.999	\Us...					Create Attribute	0x899f	4
	File Deletion		9.999	\Us...	2021..05..14 13:36:18	2021..05..14 15:46:38	2021..05..14 15:46:38	2021..05..14 15:...	Delete Index Entry Allocation	0x0	0
	Renaming File	9.999 → 0.000	0.000	\Us...					Create Attribute	0x899f	4
	File Deletion		0.000	\Us...	2021..05..14 13:36:18	2021..05..14 15:46:38	2021..05..14 15:46:38	2021..05..14 15:...	Delete Index Entry Allocation	0x0	0
	Renaming File	0.000 → X.XXX	X.XXX	\Us...					Create Attribute	0x899f	4
	File Deletion		X.XXX	\Us...	2021..05..14 13:36:18	2021..05..14 15:46:38	2021..05..14 15:46:38	2021..05..14 15:...	Delete Index Entry Allocation	0x0	0
	Renaming File	X.XXX → Y.YYY	Y.YYY	\Us...					Create Attribute	0x899f	4
	File Deletion		Y.YYY	\Us...	2021..05..14 13:36:18	2021..05..14 15:46:38	2021..05..14 15:46:38	2021..05..14 15:...	Delete Index Entry Allocation	0x0	0
21..05..14 15:...	Renaming File	Y.YYY → Z.ZZZ	Z.ZZZ	\Us...					Create Attribute	0x899f	4
	File Deletion		Z.ZZZ	\Us...	2021..05..14 13:36:18	2021..05..14 15:46:38	2021..05..14 15:46:38	2021..05..14 15:...	Delete Index Entry Allocation	0x0	0

[그림 35] secure eraser 사용에 따른 메타 데이터 변화

파일 이름과 확장자 길이를 원본 파일것과 동일하게 사용한 상태에서 내용만 (x->y->z->8->9->0->X->Y->Z) 로 바꾸는 패턴을 보인다. MAC과 redo flag상 특이점은 없다

2. 데이터 영역 변화

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
057041000	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041010	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041020	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041030	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041040	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041050	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041060	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041070	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041080	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041090	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
0570410A0	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
0570410B0	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
0570410C0	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
0570410D0	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
0570410E0	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
0570410F0	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041100	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041110	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041120	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041130	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041140	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041150	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041160	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041170	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041180	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
057041190	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
0570411A0	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA

[그림 36] secure eraser 사용에 따른 데이터 영역 변화

특정 값(0xAA)을 통해 해당 영역을 wiping한다.

- protectstar data shredder

1. 메타데이터 변화

File Deletion		1.jpg	2021-05-14 13:36:18	2021-05-14 15:52:11	2021-05-14 15:52:11	2021-05-14 15:52:11	Delete Index Ent...	0x0	0
Renaming File	1.jpg → EBBCD	EBBCD					Create Attribute	0x899d	0
File Deletion		EBBCD	2021-05-14 13:36:18	2021-05-14 15:52:11	2021-05-14 15:52:11	2021-05-14 15:52:11	Delete Index Ent...	0x1	0
File Deletion		10.jpg	2021-05-14 13:36:18	2021-05-14 15:52:11	2021-05-14 15:52:11	2021-05-14 15:52:11	Delete Index Ent...	0x0	0
Renaming File	10.jpg → EDBBCD	EDBBCD					Create Attribute	0x899d	2
File Deletion		EDBBCD	2021-05-14 13:36:18	2021-05-14 15:52:11	2021-05-14 15:52:11	2021-05-14 15:52:11	Delete Index Ent...	0x1	0

[그림 37] protectstar data shredder 사용에 따른 메타 데이터 변화

고정된 파일이름(대문자, 파일 이름 길이 유지) 상태로 변경하여 wiping 한다. MAC이나 Redo 상 특이점은 존재하지 않는다.

2. 데이터 영역 변화

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0544E8000	DA	6E	01	34	03	60	71	39	25	5E	BC	1C	F0	D3	A6	6D
0544E8010	9A	52	E2	68	C8	F4	A3	79	BC	F2	65	F1	C2	85	FB	03
0544E8020	D6	FC	DB	04	99	1E	A8	E3	75	C1	00	E4	0E	A9	86	A3
0544E8030	EB	A4	30	47	63	E5	D4	05	CC	A0	F0	D6	E0	E5	B8	7B
0544E8040	72	C0	64	B0	50	91	B9	AE	7A	A7	D8	E6	83	22	45	FA
0544E8050	46	08	39	FD	CC	A7	2B	EE	7B	2D	9A	71	82	84	1F	CF
0544E8060	83	72	B2	2F	81	F0	3B	14	0B	C9	5B	18	A8	75	7B	E9
0544E8070	84	36	14	83	5B	72	3E	AE	A4	52	7D	B9	00	9A	CA	77
0544E8080	E4	CA	DF	79	84	74	C6	8C	01	DF	A3	74	D5	DB	C0	E9
0544E8090	7D	E5	D8	D0	67	7E	A7	BD	1D	C7	B0	A7	B1	5F	4F	EC
0544E80A0	6B	7F	02	87	B0	56	F2	8F	33	A1	C7	F1	61	8C	AC	70
0544E80B0	08	CF	9F	DC	49	03	FC	91	BF	43	4B	32	EE	0B	48	A5
0544E80C0	F0	4B	32	50	5D	CC	58	93	7A	C6	DF	88	A5	C0	D7	F8
0544E80D0	FE	AA	80	A0	58	38	D7	A4	61	80	66	52	0F	D5	4C	1A
0544E80E0	4C	E4	89	CC	E4	0E	8E	12	AE	07	03	30	F8	AF	D9	F9
0544E80F0	36	2F	92	13	ED	56	CF	6D	DC	34	19	00	6B	F6	F3	C4
0544E8100	57	03	1E	F4	9D	56	2D	84	A6	1D	4B	E1	B3	91	4B	EA
0544E8110	89	16	EF	2D	5F	95	7C	65	07	18	7C	32	5A	A6	D4	1A
0544E8120	E8	60	09	BE	DF	DA	CD	60	3A	BE	D0	93	2D	9D	C3	43
0544E8130	CF	17	AE	E7	07	2D	76	03	BB	E4	A8	E2	35	1D	89	94
0544E8140	D8	B2	62	25	03	D4	07	1E	43	A2	A8	3F	BF	0C	DA	7C
0544E8150	DF	E9	E7	37	3D	56	55	BF	CF	50	B3	08	54	92	A9	AA
0544E8160	FE	B3	41	1E	60	7A	71	36	99	83	EC	DC	C0	16	29	0E
0544E8170	91	45	B2	18	58	47	B1	11	1C	13	B6	9B	0E	3F	CC	D5
0544E8180	33	19	BE	A3	4F	05	A5	21	13	17	B4	62	89	F3	47	70
0544E8190	BF	E4	27	7F	B1	39	22	72	7A	E6	CA	93	BC	5A	8A	8C
0544E81A0	4F	9D	F1	AB	28	AC	3A	56	8A	18	19	CA	72	DB	CB	1A

[그림 38] protectstar data shredder 사용에 따른 데이터 영역 변화

Random Data로 Overwrite 되는 것을 확인할 수 있다.

- wisecare 365

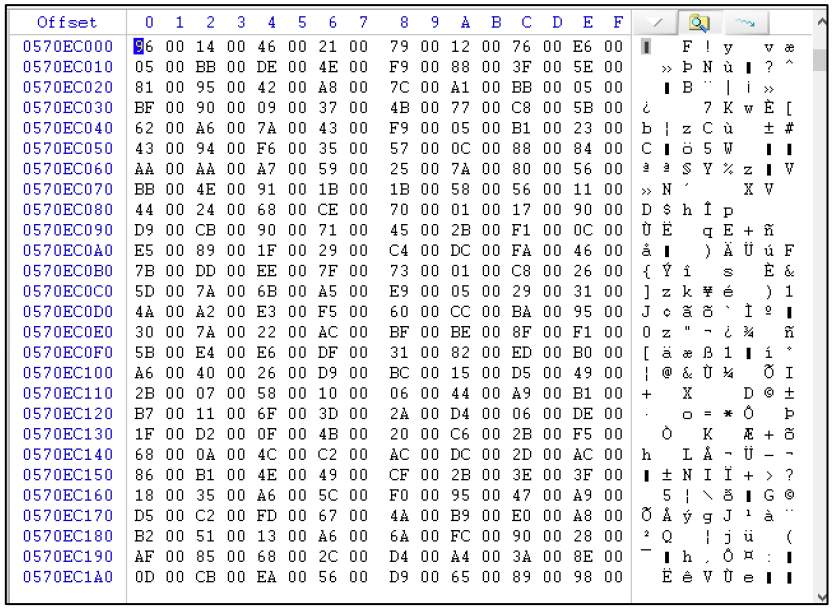
1. 메타데이터 변화

	File Deletion		1.jpg	...	2021-05-14 13:36:18	2021-05-14 15:56:32	2021-05-14 15:56:32	2021-05-14 15:56:32	Delete Index Ent...	0x0	0
021-05-14 15:...	Renaming File	1.jpg -> pyogifcq	pyogifcq	...					Create Attribute	0x899d	0
	File Deletion		pyogifcq	...	2021-05-14 13:36:18	2021-05-14 15:56:32	2021-05-14 15:56:32	2021-05-14 15:56:32	Delete Index Ent...	0x1	0
	Renaming File	pyogifcq -> crok...	crokwnte	...					Create Attribute	0x899d	0
	File Deletion		crokwnte	...	2021-05-14 13:36:18	2021-05-14 15:56:32	2021-05-14 15:56:32	2021-05-14 15:56:32	Delete Index Ent...	0x1	0
	Renaming File	crokwnte -> tihnj...	tihnjjom	...					Create Attribute	0x899d	0
	File Deletion		tihnjjom	...	2021-05-14 13:36:18	2021-05-14 15:56:32	2021-05-14 15:56:32	2021-05-14 15:56:32	Delete Index Ent...	0x1	0
	Renaming File	tihnjjom -> xvwh...	xvwhwuao	...					Create Attribute	0x899d	0
	File Deletion		xvwhwuao	...	2021-05-14 13:36:18	2021-05-14 15:56:32	2021-05-14 15:56:32	2021-05-14 15:56:32	Delete Index Ent...	0x1	0
	Renaming File	xvwhwuao -> nx...	nxkmtliy	...					Create Attribute	0x899d	0
	File Deletion		nxkmtliy	...	2021-05-14 13:36:18	2021-05-14 15:56:32	2021-05-14 15:56:32	2021-05-14 15:56:32	Delete Index Ent...	0x1	0
	Renaming File	nxkmtliy -> wen...	wenzpioa	...					Create Attribute	0x899d	0
	File Deletion		wenzpioa	...	2021-05-14 13:36:18	2021-05-14 15:56:32	2021-05-14 15:56:32	2021-05-14 15:56:32	Delete Index Ent...	0x1	0
	Renaming File	wenzpioa -> lshk...	lshkybpz	...					Create Attribute	0x899d	0
	File Deletion		lshkybpz	...	2021-05-14 13:36:18	2021-05-14 15:56:32	2021-05-14 15:56:32	2021-05-14 15:56:32	Delete Index Ent...	0x1	0
	Renaming File	lshkybpz -> aiczj...	aiczjtyc	...					Create Attribute	0x899d	0
	File Deletion		aiczjtyc	...	2021-05-14 13:36:18	2021-05-14 15:56:32	2021-05-14 15:56:32	2021-05-14 15:56:32	Delete Index Ent...	0x1	0
021-05-14 15:...	Renaming File	aiczjtyc -> pngfe...	pngferdj	...					Create Attribute	0x899d	0
	File Deletion		pngferdj	...	2021-05-14 13:36:18	2021-05-14 15:56:32	2021-05-14 15:56:32	2021-05-14 15:56:32	Delete Index Ent...	0x1	0
	Renaming File	pngferdj -> cecfy...	cecfyzqz	...					Create Attribute	0x899d	0
	File Deletion		cecfyzqz	...	2021-05-14 13:36:18	2021-05-14 15:56:32	2021-05-14 15:56:32	2021-05-14 15:56:32	Delete Index Ent...	0x1	0

[그림 39] wisecare 365 사용에 따른 메타 데이터 변화

영어 소문자로 구성된 파일 이름을 사용 후 delete하는 것을 확인할 수 있으며 Redo Flag나 MAC time 상 특이점은 없다

2. 데이터 영역 변화



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0570EC000	96	00	14	00	46	00	21	00	79	00	12	00	76	00	E6	00
0570EC010	05	00	BB	00	DE	00	4E	00	F9	00	88	00	3F	00	5E	00
0570EC020	81	00	95	00	42	00	A8	00	7C	00	A1	00	BB	00	05	00
0570EC030	BF	00	90	00	09	00	37	00	4B	00	77	00	C8	00	5B	00
0570EC040	62	00	A6	00	7A	00	43	00	F9	00	05	00	B1	00	23	00
0570EC050	43	00	94	00	F6	00	35	00	57	00	0C	00	88	00	84	00
0570EC060	AA	00	AA	00	A7	00	59	00	25	00	7A	00	80	00	56	00
0570EC070	BB	00	4E	00	91	00	1B	00	1B	00	58	00	56	00	11	00
0570EC080	44	00	24	00	68	00	CE	00	70	00	01	00	17	00	90	00
0570EC090	D9	00	CB	00	90	00	71	00	45	00	2B	00	F1	00	0C	00
0570EC0A0	E5	00	89	00	1F	00	29	00	C4	00	DC	00	FA	00	46	00
0570EC0B0	7B	00	DD	00	EE	00	7F	00	73	00	01	00	C8	00	26	00
0570EC0C0	5D	00	7A	00	6B	00	A5	00	E9	00	05	00	29	00	31	00
0570EC0D0	4A	00	A2	00	E3	00	F5	00	60	00	CC	00	BA	00	95	00
0570EC0E0	30	00	7A	00	22	00	AC	00	BF	00	BE	00	8F	00	F1	00
0570EC0F0	5B	00	E4	00	E6	00	DF	00	31	00	82	00	ED	00	B0	00
0570EC100	A6	00	40	00	26	00	D9	00	BC	00	15	00	D5	00	49	00
0570EC110	2B	00	07	00	58	00	10	00	06	00	44	00	A9	00	B1	00
0570EC120	B7	00	11	00	6F	00	3D	00	2A	00	D4	00	06	00	DE	00
0570EC130	1F	00	D2	00	0F	00	4B	00	20	00	C6	00	2B	00	F5	00
0570EC140	68	00	0A	00	4C	00	C2	00	AC	00	DC	00	2D	00	AC	00
0570EC150	86	00	B1	00	4E	00	49	00	CF	00	2B	00	3E	00	3F	00
0570EC160	18	00	35	00	A6	00	5C	00	F0	00	95	00	47	00	A9	00
0570EC170	D5	00	C2	00	FD	00	67	00	4A	00	B9	00	E0	00	A8	00
0570EC180	B2	00	51	00	13	00	A6	00	6A	00	FC	00	90	00	28	00
0570EC190	AF	00	85	00	68	00	2C	00	D4	00	A4	00	3A	00	8E	00
0570EC1A0	0D	00	CB	00	EA	00	56	00	D9	00	65	00	89	00	98	00

[그림 40] wisecare 365 사용에 따른 데이터 영역 변화

Random data를 사용하여 WIPING 하나 홀수열(1,3,5…,E)의 경우 0x00을 사용하여 wiping한다

- bcwipe

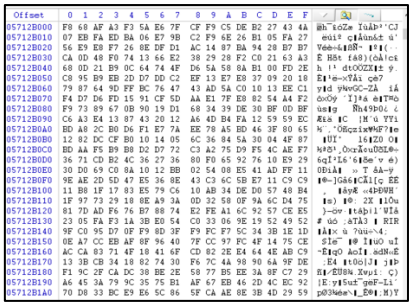
1. 메타데이터 변화

File Deletion		6.png	2021..05..14 13:36:18	2021..04..03 08:22:19	2021..04..03 08:22:19	2021..05..16 18:39:47	Delete Index Ent...	0x1
Renaming File	6.png -> oijloeg...	oijloegh.wwp					Create Attribute	0x89a6
		oijloegh.wwp	1986..04..30 20:43:13	1986..04..30 20:43:13	2021..05..16 18:40:11	1986..04..30 20:43:13	Deallocate File R...	0x89a6
		RUBY.EXE.468488C3.pf	2019..03..19 22:23:25	2021..05..16 18:40:10	2021..05..16 18:40:10	2021..05..16 18:40:10	Set New Attribut...	0x799c
		settings.dat	2019..03..19 22:00:25	2021..05..16 18:40:10	2019..03..20 06:53:25	2021..05..16 18:40:10	Update Resident...	0x5235
File Deletion		BCO6A1787A6.tmp	2021..05..16 18:40:10	2021..05..16 18:40:10	2021..05..16 18:40:10	2021..05..16 18:40:10	Delete Index Ent...	0xd
File Creation		TM6A179CC1.tmp	2021..05..16 18:40:11	2021..05..16 18:40:11	2021..05..16 18:40:11	2021..05..16 18:40:11	Initialize File Rec...	0x45
File Creation		BCO6A179C82.tmp	2021..05..16 18:40:11	2021..05..16 18:40:11	2021..05..16 18:40:11	2021..05..16 18:40:11	Initialize File Rec...	0x8e
		settings.dat.LOG1	2019..03..19 22:20:13	2019..03..19 22:20:13	2019..03..19 22:20:13	2021..05..16 18:39:01	Update Resident...	0x3b8e
File Deletion		7.jpg	2021..05..14 13:36:18	2021..04..03 08:18:58	2021..04..03 08:18:58	2021..05..16 18:39:47	Delete Index Ent...	0x1
Renaming File	7.jpg -> jmvisixp...	jmvisixp.mun					Create Attribute	0x89a6
		jmvisixp.mun	1986..04..30 20:43:13	1986..04..30 20:43:13	2021..05..16 18:40:12	1986..04..30 20:43:13	Deallocate File R...	0x89a6
File Deletion		BCO6A179C82.tmp	2021..05..16 18:40:11	2021..05..16 18:40:11	2021..05..16 18:40:11	2021..05..16 18:40:11	Delete Index Ent...	0xd
File Creation		TM6A1791FC.tmp	2021..05..16 18:40:12	2021..05..16 18:40:12	2021..05..16 18:40:12	2021..05..16 18:40:12	Initialize File Rec...	0x45
File Creation		BCO6A1791E3.tmp	2021..05..16 18:40:12	2021..05..16 18:40:12	2021..05..16 18:40:12	2021..05..16 18:40:12	Initialize File Rec...	0x8e

[그림 41] bcwipe 사용에 따른 메타 데이터 변화

영어 소문자로 이루어진 파일 명을 사용한다. MAC time 상 특이점은 없으나, 중간 tmp 파일을 생성하며, Initialize File Record 관련 Redo를 사용하는 것을 확인할 수 있다.

2. 데이터 영역 변화



[그림 42] bcwipe 사용에 따른 데이터 영역 변화

Random Data로 Overwrite 되는 것을 확인할 수 있다.

3. 기타 변화

555778100		Writing Content ...	Data Runs in Vol...							Update Mapping...
555778517		Writing Content ...	Data Runs in Vol...							Update Mapping...
555778944		Writing Content ...	Data Runs in Vol...							Update Mapping...
556557781		Writing Content ...	Data Runs in Vol...							Update Mapping...
557780862				BCWipeLib2.dll	\Program Files (...	2021..02..10 15:...	2021..02..10 15:...	2021..05..14 16:...	2021..05..14 13:...	Update Resident...
557781271	2021..05..14 13:...	Directory Creation		~BCWipe.tmp	\~BCWipe.tmp	2021..05..14 13:...	2021..05..14 13:...	2021..05..14 13:...	2021..05..14 13:...	Initialize File Rec...
557781842	2021..05..14 13:...	File Creation		LOGFILEWIPER		2021..05..14 13:...	2021..05..14 13:...	2021..05..14 13:...	2021..05..14 13:...	Initialize File Rec...
557782157		Writing Content ...	Data Runs in Vol...	LOGFILEWIPER						Update Mapping...
557782730		Writing Content ...	Data Runs in Vol...	LOGFILEWIPER						Update Mapping...
557783155		Writing Content ...	Data Runs in Vol...	LOGFILEWIPER						Update Mapping...
557783580		Writing Content ...	Data Runs in Vol...	LOGFILEWIPER						Update Mapping...
557783997		Writing Content ...	Data Runs in Vol...	LOGFILEWIPER						Update Mapping...
557784423		Writing Content ...	Data Runs in Vol...	LOGFILEWIPER						Update Mapping...
557784852		Writing Content ...	Data Runs in Vol...	LOGFILEWIPER						Update Mapping...

[그림 43] bcwipe 사용에 따른 기타 변화

기본적으로 Logfile을 wiping 해주는 기능을 가지고 있다. Writing Content 이후에 BCWIPE.tmp와 같은 파일 생성 및 LOGFILEWIPER라는 파일도 생성하는 것을 확인할 수 있다.

- bitkiller

1. 메타데이터 변화

File Deletion		5.jpg	2021-05-14 13:36:18	2021-05-14 16:23:52	2021-05-14 16:23:52	2021-05-14 16:23:52	Delete Index Entry Allocation	0x1	0
Renaming File	5.jpg -> xgmsbdi...	xgmsbdicx.xxc					Create Attribute	0x89a6	0
File Deletion		xgmsbdicx.xxc	2021-05-14 13:36:18	2021-05-14 16:23:52	2021-05-14 16:23:52	2021-05-14 16:23:52	Delete Index Entry Allocation	0x1	0
Renaming File	xgmsbdicx.xxc -...	qtcyfctiw.vbw					Create Attribute	0x89a6	0
File Deletion		qtcyfctiw.vbw	2021-05-14 13:36:18	2021-05-14 16:23:52	2021-05-14 16:23:52	2021-05-14 16:23:52	Delete Index Entry Allocation	0x1	0
Renaming File	qtcyfctiw.vbw -> ...	csqveyomn.rgh					Create Attribute	0x89a6	0
File Deletion		csqveyomn.rgh	2021-05-14 13:36:18	2021-05-14 16:23:52	2021-05-14 16:23:52	2021-05-14 16:23:52	Delete Index Entry Allocation	0x1	0
Renaming File	csqveyomn.rgh -...	dvtkbsddj.bbh					Create Attribute	0x89a6	0
File Deletion		dvtkbsddj.bbh	2021-05-14 13:36:18	2021-05-14 16:23:52	2021-05-14 16:23:52	2021-05-14 16:23:52	Delete Index Entry Allocation	0x1	0
Renaming File	dvtkbsddj.bbh -> ...	biwlouwcb.rrj					Create Attribute	0x89a6	0
File Deletion		biwlouwcb.rrj	2021-05-14 13:36:18	2021-05-14 16:23:52	2021-05-14 16:23:52	2021-05-14 16:23:52	Delete Index Entry Allocation	0x1	0
Renaming File	biwlouwcb.rrj -> ...	cvchnxlep.eem					Create Attribute	0x89a6	0
File Deletion		cvchnxlep.eem	2021-05-14 13:36:18	2021-05-14 16:23:52	2021-05-14 16:23:52	2021-05-14 16:23:52	Delete Index Entry Allocation	0x1	0
Renaming File	cvchnxlep.eem -> ...	fkjahwdgy.ivq					Create Attribute	0x89a6	0
File Deletion		fkjahwdgy.ivq	2021-05-14 13:36:18	2021-05-14 16:23:52	2021-05-14 16:23:52	2021-05-14 16:23:52	Delete Index Entry Allocation	0x1	0
Renaming File	fkjahwdgy.ivq -> ...	fsejrbpkn.yxb					Create Attribute	0x89a6	0
File Deletion		fsejrbpkn.yxb	2021-05-14 13:36:18	2021-05-14 16:23:52	2021-05-14 16:23:52	2021-05-14 16:23:52	Delete Index Entry Allocation	0x1	0
Renaming File	fsejrbpkn.yxb -> ...	difhgyjxx.twy					Create Attribute	0x89a6	0
File Deletion		difhgyjxx.twy	2021-05-14 13:36:18	2021-05-14 16:23:52	2021-05-14 16:23:52	2021-05-14 16:23:52	Delete Index Entry Allocation	0x1	0
Renaming File	difhgyjxx.twy -> ...	pmodepdob.jbj					Create Attribute	0x89a6	0
File Deletion		pmodepdob.jbj	2021-05-14 13:36:18	2021-05-14 16:23:52	2021-05-14 16:23:52	2021-05-14 16:23:52	Delete Index Entry Allocation	0x1	0

[그림 44] bitkiller 사용에 따른 메타 데이터 변화

파일 이름을 다수 변경하고, 영어 소문자로만 이루어진 파일 이름을 사용하는 것을 확인할 수 있다. MAC과 Redo 상 특이점은 없다.

2. 데이터 영역 변화

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
05713E000	29	23	BE	84	E1	6C	D6	AE	52	90	49	F1	F1	BB	E9	EB
05713E010	B3	A6	DB	3C	87	0C	3E	99	24	5E	0D	1C	06	B7	47	DE
05713E020	B3	12	4D	C8	43	BB	8B	A6	1F	03	5A	7D	09	38	25	1F
05713E030	5D	D4	CB	FC	96	F5	45	3B	13	0D	89	0A	1C	DB	AE	32
05713E040	20	9A	50	EE	40	78	36	FD	12	49	32	F6	9E	7D	49	DC
05713E050	AD	4F	14	F2	44	40	66	D0	6B	C4	30	B7	32	3B	A1	22
05713E060	F6	22	91	9D	E1	8B	1F	DA	B0	CA	99	02	B9	72	9D	49
05713E070	2C	80	7E	C5	99	D5	E9	80	B2	EA	C9	CC	53	BF	67	D6
05713E080	BF	14	D6	7E	2D	DC	8E	66	83	EF	57	49	61	FF	69	8F
05713E090	61	CD	D1	1E	9D	9C	16	72	72	E6	1D	F0	84	4F	4A	77
05713E0A0	02	D7	E8	39	2C	53	CB	C9	12	1E	33	74	9E	0C	F4	D5
05713E0B0	D4	9F	D4	A4	59	7E	35	CF	32	22	F4	CC	CF	D3	90	2D
05713E0C0	48	D3	8F	75	E6	D9	1D	2A	E5	C0	F7	2B	78	81	87	44
05713E0D0	0E	5F	50	00	D4	61	8D	BE	7B	05	15	07	3B	33	82	1F
05713E0E0	18	70	92	DA	64	54	CE	B1	85	3E	69	15	F8	46	6A	04
05713E0F0	96	73	0E	D9	16	2F	67	68	D4	F7	4A	4A	D0	57	68	76
05713E100	FA	16	BB	11	AD	AE	24	88	79	FE	52	DB	25	43	E5	3C
05713E110	F4	45	D3	D8	28	CE	0B	F5	C5	60	59	3D	97	27	8A	59
05713E120	76	2D	D0	C2	C9	CD	68	D4	49	6A	79	25	08	61	40	14
05713E130	B1	3B	6A	A5	11	28	C1	8C	D6	A9	0B	87	97	8C	2F	F1
05713E140	15	1D	9A	95	C1	9B	E1	C0	7E	E9	A8	9A	A7	86	C2	B5
05713E150	54	BF	9A	E7	D9	23	D1	55	90	38	28	D1	D9	6C	A1	66
05713E160	5E	4E	E1	30	9C	FE	D9	71	9F	E2	A5	E2	0C	9B	B4	47
05713E170	65	38	2A	46	89	A9	82	79	7A	76	78	C2	63	B1	26	DF
05713E180	DA	29	6D	3E	62	E0	96	12	34	BF	39	A6	3F	89	5E	F1
05713E190	6D	0E	E3	6C	28	A1	1E	20	1D	CB	C2	03	3F	41	07	84
05713E1A0	0F	14	05	65	1B	28	61	C9	C5	E7	2C	8E	46	36	08	DC

[그림 45] bitkiller 사용에 따른 데이터 영역 변화

Random Data로 Overwrite 되는 것을 확인할 수 있다.

- eraser

1. 메타데이터 변화

Renaming File	13.jpg -> OAldmW	OAldmW						Create Attribute	0x899e	0
Temp Event		OAldmW						Delete Attribute	0x899e	0
Renaming File	OAldmW -> Wbl}Sa	Wbl}Sa						Create Attribute	0x899e	0
Temp Event		Wbl}Sa						Delete Attribute	0x899e	0
Renaming File	Wbl}Sa -> a-4LM	a-4LM						Create Attribute	0x899e	0
Temp Event		a-4LM						Delete Attribute	0x899e	0
Renaming File	a-4LM -> L(Vg`-	L(Vg`-						Create Attribute	0x899e	0
Temp Event		L(Vg`-						Delete Attribute	0x899e	0
Renaming File	L(Vg`-- -> 3ekby	3ekby						Create Attribute	0x899e	0
Temp Event		3ekby						Delete Attribute	0x899e	0
Renaming File	3ekby -> cdT0/+	cdT0/+						Create Attribute	0x899e	0
Temp Event		14.jpg						Delete Attribute	0x899e	2

[그림 46] eraser 사용에 따른 메타 데이터 변화

특수문자가 포함된 랜덤한 파일이름을 사용한다. 확장자를 포함한 파일이름 길이를 그대로 사용하며 Create Attribute와 Delete Attribute만 사용한다. MAC time은 확인되지 않는다.

2. 데이터 영역 변화

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0545CD000	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD010	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD020	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD030	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD040	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD050	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD060	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD070	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD080	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD090	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD0A0	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD0B0	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD0C0	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD0D0	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD0E0	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD0F0	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD100	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD110	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD120	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD130	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD140	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD150	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD160	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD170	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD180	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD190	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66
0545CD1A0	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66

[그림 47] eraser 사용에 따른 데이터 영역 변화

0x66을 이용하여 해당 영역을 Overwrite wiping 한다

- glary utilities

1. 메타데이터 변화

2021-05-14 16:...	Renaming File	1.jpg -> A.AAA	A.AAA						Create Attribute	0x899d
	File Deletion		A.AAA	2021-05-14 13:36:18	2021-05-14 16:07:00	2021-05-14 16:07:00	2021-05-14 16:07:00		Delete Index Ent...	0x1
	Renaming File	A.AAA -> B.BBB	B.BBB						Create Attribute	0x899d
	File Deletion		B.BBB	2021-05-14 13:36:18	2021-05-14 16:07:00	2021-05-14 16:07:00	2021-05-14 16:07:00		Delete Index Ent...	0x1
	Renaming File	B.BBB -> C.CCC	C.CCC						Create Attribute	0x899d
	File Deletion		C.CCC	2021-05-14 13:36:18	2021-05-14 16:07:00	2021-05-14 16:07:00	2021-05-14 16:07:00		Delete Index Ent...	0x1
	Renaming File	C.CCC -> D.DDD	D.DDD						Create Attribute	0x899d
	File Deletion		D.DDD	2021-05-14 13:36:18	2021-05-14 16:07:00	2021-05-14 16:07:00	2021-05-14 16:07:00		Delete Index Ent...	0x1
	Renaming File	D.DDD -> E.EEE	E.EEE						Create Attribute	0x899d
	File Deletion		E.EEE	2021-05-14 13:36:18	2021-05-14 16:07:00	2021-05-14 16:07:00	2021-05-14 16:07:00		Delete Index Ent...	0x1
	Renaming File	E.EEE -> F.FFF	F.FFF						Create Attribute	0x899d
	File Deletion		F.FFF	2021-05-14 13:36:18	2021-05-14 16:07:00	2021-05-14 16:07:00	2021-05-14 16:07:00		Delete Index Ent...	0x1
	Renaming File	F.FFF -> G.GGG	G.GGG						Create Attribute	0x899d
	File Deletion		G.GGG	2021-05-14 13:36:18	2021-05-14 16:07:00	2021-05-14 16:07:00	2021-05-14 16:07:00		Delete Index Ent...	0x1
	Renaming File	G.GGG -> H.HHH	H.HHH						Create Attribute	0x899d
	File Deletion		H.HHH	2021-05-14 13:36:18	2021-05-14 16:07:00	2021-05-14 16:07:00	2021-05-14 16:07:00		Delete Index Ent...	0x1
	Renaming File	H.HHH -> I.III	I.III						Create Attribute	0x899d
	File Deletion		I.III	2021-05-14 13:36:18	2021-05-14 16:07:00	2021-05-14 16:07:00	2021-05-14 16:07:00		Delete Index Ent...	0x1
	Renaming File	I.III -> J.JJJ	J.JJJ						Create Attribute	0x899d
	File Deletion		J.JJJ	2021-05-14 13:36:18	2021-05-14 16:07:00	2021-05-14 16:07:00	2021-05-14 16:07:00		Delete Index Ent...	0x1
	Renaming File	J.JJJ -> K.KKK	K.KKK						Create Attribute	0x899d
	File Deletion		K.KKK	2021-05-14 13:36:18	2021-05-14 16:07:00	2021-05-14 16:07:00	2021-05-14 16:07:00		Delete Index Ent...	0x1
	Renaming File	K.KKK -> L.LLL	L.LLL						Create Attribute	0x899d
	File Deletion		L.LLL	2021-05-14 13:36:18	2021-05-14 16:07:00	2021-05-14 16:07:00	2021-05-14 16:07:00		Delete Index Ent...	0x1

[그림 48] glary utilities 사용에 따른 메타 데이터 변화

대문자 (A->Z)까지 파일이름을 변경하며 파일 이름과 확장자 길이를 모두 보존한다. 파일 변경 시 MAC time 의 second를 0으로 setting한다. 이외 Redo 상 특이점은 없다.

2. 데이터 영역 변화

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0545F6000	26	AE	5C	AE	18	6A	AF	5F	41	78	2D	30	36	A7	B9	80
0545F6010	A4	7F	0B	3E	93	77	0D	B6	EC	69	85	AA	39	42	F5	A5
0545F6020	AD	FE	BF	8C	64	D4	8D	76	EB	AD	F0	BD	03	DB	48	56
0545F6030	A2	08	E3	5D	3B	6C	69	F4	3F	44	77	4E	E4	7F	8A	07
0545F6040	25	BA	1F	B7	0A	6E	18	C6	29	68	62	82	6D	7A	D5	6E
0545F6050	16	71	5B	DD	01	46	55	C0	2A	99	3A	BD	6F	5A	81	81
0545F6060	97	CA	C2	56	92	A2	18	F8	02	91	C9	A4	FB	EC	29	73
0545F6070	07	A2	BB	E6	6E	6E	9A	C2	B4	50	17	1E	62	3D	A4	BA
0545F6080	0A	16	F1	92	85	D7	54	B3	7F	11	6E	4E	36	9A	0C	0B
0545F6090	7E	82	4B	9F	09	4A	00	A1	E5	51	56	99	46	8F	B9	5B
0545F60A0	86	85	F3	93	6A	74	95	A0	A7	CE	99	A6	A4	EA	45	DE
0545F60B0	82	FB	53	31	5A	43	4E	06	C5	84	3F	58	A2	B8	89	0B
0545F60C0	13	01	12	80	C9	E3	A3	67	82	B1	92	D4	CF	45	9E	95
0545F60D0	1B	F4	1A	C4	E9	C2	4E	98	5D	D1	1A	80	FE	20	DC	73
0545F60E0	BA	72	94	81	2B	8B	46	AF	18	A2	A0	01	3F	14	DD	D8
0545F60F0	51	56	E9	7E	3F	2D	C6	00	B4	21	2E	3C	E2	2F	7A	3A
0545F6100	82	BE	C2	C0	16	D4	46	20	72	8A	0C	55	7A	BD	CB	4E
0545F6110	2D	07	08	8A	E3	ED	7F	E5	D2	5A	C4	B2	D7	4D	2A	09
0545F6120	74	CE	E4	62	15	26	6A	63	97	4F	1F	F7	0A	AA	30	A0
0545F6130	B6	F0	BF	0E	5D	6B	41	F0	C0	66	24	0A	64	E2	B5	88
0545F6140	96	8A	42	92	AD	E9	7B	20	8F	DB	1E	10	77	41	D4	76
0545F6150	F5	F9	56	33	36	0E	D3	C9	85	2B	96	6D	12	56	E4	5E
0545F6160	F2	DA	23	76	68	85	42	FE	63	14	54	C7	47	EC	7E	76
0545F6170	F0	0B	14	20	F5	3D	FF	17	29	93	62	03	68	11	7D	34
0545F6180	90	A7	D1	36	CD	63	84	A6	1A	E4	08	45	04	12	F8	4B
0545F6190	B1	0C	42	FE	22	62	8B	82	B5	85	CF	F3	EE	7B	48	B1
0545F61A0	76	D7	92	FB	64	E9	0C	C0	BC	32	81	B1	35	1A	08	9B

[그림 49] glary utilities 사용에 따른 데이터 영역 변화

Random Data로 Overwrite 되는 것을 확인할 수 있다.

- Moo0 FileShredder

1. 메타데이터 변화

File Deletion		2.jpg	2021-05-14 13:36:18	2021-05-14 16:10:56	2021-05-14 16:10:56	2021-05-14 16:10:56	Delete Index Ent...	0x0	0
Renaming File	2.jpg → N.JwJ	N.JwJ					Create Attribute	0x899f	4
File Deletion		N.JwJ	2021-05-14 13:36:18	2021-05-14 16:10:56	2021-05-14 16:10:56	2021-05-14 16:10:56	Delete Index Ent...	0x1	0
Renaming File	N.JwJ → h.rWZ	h.rWZ					Create Attribute	0x899f	4
File Deletion		h.rWZ	2016-09-09 01:09:10	2017-05-18 02:35:58	2021-05-14 16:10:56	2018-12-06 01:43:36	Delete Index Ent...	0x1	0
File Deletion		3.jpg	2021-05-14 13:36:18	2021-05-14 16:10:56	2021-05-14 16:10:56	2021-05-14 16:10:56	Delete Index Ent...	0x1	0
Renaming File	3.jpg → s.GD7	s.GD7					Create Attribute	0x89a2	2
File Deletion		s.GD7	2021-05-14 13:36:18	2021-05-14 16:10:56	2021-05-14 16:10:56	2021-05-14 16:10:56	Delete Index Ent...	0x1	0
Renaming File	s.GD7 → 6.KOK	6.KOK					Create Attribute	0x89a2	2
File Deletion		6.KOK	2015-11-29 17:52:06	2016-03-08 09:22:04	2021-05-14 16:10:56	2020-04-20 18:18:51	Delete Index Ent...	0x1	0
File Deletion		4.jpg	2021-05-14 13:36:18	2021-05-14 16:10:56	2021-05-14 16:10:56	2021-05-14 16:10:56	Delete Index Ent...	0x1	0

[그림 50] Moo0 FileShredder 사용에 따른 메타 데이터 변화

소문자와 대문자, 숫자를 모두 활용한 File name을 사용하며 확장자 파일이름의 길이는 보존한다. MAC time이나 Redo 상 특이점은 없다.

2. 데이터 영역 변화

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
054890000	A9	8D	0F	EA	68	43	72	F3	EB	BD	C7	05	FC	F8	5D	31
054890010	58	6B	59	C4	46	22	99	D6	25	70	00	65	28	5D	F3	5E
054890020	38	3E	46	36	1F	04	84	EF	62	7A	38	7D	D5	A3	1A	AC
054890030	FB	BE	D8	BF	00	9A	6E	EB	6C	5F	87	22	66	2C	4D	E0
054890040	04	98	D3	A0	89	27	A4	1A	0C	DF	D1	56	FA	34	7B	12
054890050	21	72	2B	D7	B7	0A	17	5C	29	B0	02	1C	4D	79	27	18
054890060	CC	FE	61	D3	93	46	3A	0A	F6	EB	16	93	CA	E8	00	FA
054890070	F3	AC	66	3F	E3	80	3B	95	07	6B	56	0F	80	7A	CD	14
054890080	26	66	AC	65	5B	6D	A5	41	6F	76	4D	BC	2F	A0	93	6E
054890090	EA	AC	AE	E8	65	F1	F7	FD	A6	6D	31	5B	24	F5	A2	31
0548900A0	5A	DD	1C	EA	A3	7B	F1	AC	80	57	FF	34	0C	A3	A5	A8
0548900B0	65	E3	D1	14	93	70	9E	0C	AD	52	A5	C7	59	BF	7B	0F
0548900C0	81	F1	B5	FA	0A	24	62	D4	3F	11	62	05	07	3A	EE	35
0548900D0	2A	20	DC	A5	B9	B9	B5	F9	AC	83	7F	51	E1	60	1F	68
0548900E0	40	5D	B8	EB	58	9D	63	15	C6	84	72	9A	22	5A	9B	A4
0548900F0	13	D8	98	7F	5D	ED	1F	4A	FD	63	CD	33	64	BA	E8	87
054890100	95	31	5D	6C	43	AA	2F	44	4A	B5	EB	BE	CB	43	B8	A8
054890110	F9	4D	06	D3	6A	1F	70	65	74	EE	D0	D4	34	99	6D	45
054890120	20	4C	62	C0	A6	9A	07	A8	2F	08	E6	4F	8E	B0	BA	21
054890130	63	5C	82	F5	28	A8	7C	F1	3B	1E	2B	F2	CA	93	74	96
054890140	71	D0	5D	13	FC	41	CC	4E	99	6B	94	8F	DA	AC	75	0B
054890150	E3	25	2D	AB	7E	A6	10	80	F2	35	07	AC	B5	F5	14	DB
054890160	3B	6D	A2	84	AD	60	09	2A	0C	FD	77	7E	90	96	91	8B
054890170	35	CB	84	6E	8F	66	72	43	DB	3D	30	64	A6	68	56	9B
054890180	57	23	B4	00	E1	AE	77	D7	D0	6A	55	8C	1A	3D	AF	73
054890190	8B	A8	0D	BB	F2	3B	EF	15	4A	2C	3A	8A	DB	C4	83	03
0548901A0	C0	26	4A	4E	96	B4	43	F3	B6	B7	92	46	BB	07	01	C0

[그림 51] Moo0 FileShredder 사용에 따른 데이터 영역 변화

Random Data로 Overwrite 되는 것을 확인할 수 있다.

- TweakNow securedelete

1. 메타데이터 변화

	File Deletion		1.jpg	2021-05-14 13:36:18	2021-05-14 16:14:29	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x0	0
2021-05-14 16:...	File Deletion		2.jpg	2021-05-14 13:36:18	2021-05-14 16:14:29	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x0	0
2021-05-14 16:...	File Deletion		3.jpg	2021-05-14 13:36:18	2021-05-14 16:14:29	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x1	0
2021-05-14 16:...	File Deletion		4.jpg	2021-05-14 13:36:18	2021-05-14 16:14:29	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x1	0
2021-05-14 16:...	File Deletion		5.jpg	2021-05-14 13:36:18	2021-05-14 16:14:29	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x1	0
2021-05-14 16:...	File Deletion		6.png	2021-05-14 13:36:18	2021-05-14 16:14:29	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x1	0
2021-05-14 16:...	File Deletion		7.jpg	2021-05-14 13:36:18	2021-05-14 16:14:29	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x1	0
2021-05-14 16:...	File Deletion		8.jpg	2021-05-14 13:36:18	2021-05-14 16:14:29	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x1	0
2021-05-14 16:...	File Deletion		9.jpg	2021-05-14 13:36:18	2021-05-14 16:14:29	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x1	0
	File Deletion		icnE6C4.tmp	2019-03-19 22:00:19	2021-05-14 16:14:18	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x0	0
2021-05-14 16:...	File Deletion		10.jpg	2021-05-14 13:36:18	2021-05-14 16:14:30	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x0	0
2021-05-14 16:...	File Deletion		11.jpg	2021-05-14 13:36:18	2021-05-14 16:14:31	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x0	0
2021-05-14 16:...	File Deletion		12.jpg	2021-05-14 13:36:18	2021-05-14 16:14:31	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x0	0
2021-05-14 16:...	File Deletion		13.jpg	2021-05-14 13:36:18	2021-05-14 16:14:31	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x0	0
2021-05-14 16:...	File Deletion		14.jpg	2021-05-14 13:36:18	2021-05-14 16:14:31	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x0	0
2021-05-14 16:...	File Deletion		15.jpeg	2021-05-14 13:36:18	2021-05-14 16:14:31	2021-05-14 16:...	2021-05-14 16:...	Delete Index Ent...	0x0	0

[그림 52] TweaakNow securedelete 사용에 따른 메타 데이터 변화

특이점 없이 Delete Index Entry Allocation을 통해 파일을 삭제한다. 파일 명 변화나 MAC 타임의 변화는 발견되지않는다.

2. 데이터 영역 변화

```
0548B3000 51 E0 63 D8 67 42 CA BA  9E 7F 13 96 A6 5D E9 28  ñàcØgBÊº▮  ▮¦]é(
0548B3010 49 B1 9F 85 75 BA 3B 8F  EC C0 C6 B9 2E EE D3 FD  I±▮▮uº; ìÀÆ¹.îÓý
0548B3020 A7 6C 4E 1A 15 C0 87 13  3D 66 7F E4 CE AF 72 87  §lN  À▮ =f äÎ¯r▮
0548B3030 95 D7 A5 28 E3 6A 71 A4  3C D9 90 48 41 57 A7 C7  ▮×¥(ãjq¤<Ù HAW§Ç
0548B3040 DF FA 14 7C B9 0F FB E2  D4 BE 8B 51 82 DF 96 FB  ßú |¹ ûâÔ¾▮Q▮ß▮û
0548B3050 91 1B 51 26 B4 47 68 AC  31 FD 45 B0 CC 7D A2 A2  ´ Q&´Gh¬1ýE°Ì}¢¢
0548B3060 F3 C2 4D 76 2C E8 3B 20  BC BE D1 53 9A A7 6E 7B  óÂMv,è; ¼¾ÑS▮§n{
0548B3070 93 B6 3C F9 BE 0A 38 9E  23 66 80 6A A7 15 DD 86  ▮¶<ù¾ 8▮#f▮j§ Ý▮
0548B3080 3A FD 90 7F 45 02 62 C5  4E 9E E6 63 EE BE 11 01  :ý  E bÅN▮æcî¾
0548B3090 F5 DF FE 17 DB 69 FA 73  6A 4C D7 EE AA D9 6F 6B  õßþ ÛiúsjLx×î ªÙok
0548B30A0 0D E2 76 10 DB 16 85 C8  E1 96 64 F9 56 DC 98 83  â▮v Û ▮Èá▮dùVÜ▮▮
0548B30B0 0D CE 2E F9 E1 1E C6 23  5E E5 E2 B4 AD 80 71 48  Î.ùá Æ#^åâ´-▮qH
0548B30C0 C2 AA 97 A1 C8 DA BF 23  CC DF E3 8D AA BA 1B FA  Âª▮¡ÈÚ¿#Ìßãªºú
0548B30D0 35 BC 64 17 AA E1 B3 A6  57 6B 3A 34 88 C2 FA 16  5¼d ªá³¦Wk:4▮Âú
0548B30E0 B2 8C 8A AA E3 08 26 CC  69 B0 FB 97 C2 0F B1 5D  ²▮▮ªã &Ìi°û▮Â ±]
0548B30F0 C4 E0 3A E9 0D 68 DA F4  AD 15 77 E5 13 58 23 CE  Äà:é hÚô- wå X#Î
0548B3100 35 C0 E7 A3 04 57 D2 BC  0F 42 43 8E 76 94 73 A6  5Àç£ WÒ¼ BC▮v▮s¦
0548B3110 12 72 45 E7 E2 6D 52 04  B9 1C 30 41 26 F9 03 66  rEçâmR ¹ 0A&ù f
0548B3120 A4 7E 47 03 03 80 DC EB  16 CB 53 EB 9E FF 78 CB  ¤~G  ▮Üë ËSë▮ÿxË
0548B3130 76 AB 20 88 01 A7 34 D0  D1 B7 FE BE 99 5D B3 D6  v«  ▮ §4ÐÑ·þ¾▮]³Ö
0548B3140 55 FF 42 44 B8 3A 5C 51  D6 85 C4 26 12 0A D9 C6  UÿBD¸:\QÖ▮Ä&  ÙÆ
0548B3150 4A C1 61 45 42 CF 98 4E  4F 1E 78 D5 44 3D 4B 18  JÁaEBÏ▮NO xÕD=K
0548B3160 A2 7A 6F DC FB 3D 69 E6  A7 A8 2E B7 AB 6D AD 8D  ¢zoÜû=iæ§¨.·«m-
0548B3170 E5 EF A0 96 7D 9C 95 77  89 89 37 FD 00 50 E2 22  åï ▮}▮▮w▮▮7ý Pâ"
0548B3180 E1 27 67 44 A4 42 1C A1  E1 6A 28 16 3F DE 0D 18  á'gD¤B ¡áj( ?Þ
0548B3190 A0 6A 76 F3 8A C6 43 43  D9 31 D3 B0 A3 4E 91 EE  jvó▮ÆCCÙ1Ó°£N´î
0548B31A0 6C 3F C1 F4 8B 00 8D 7B  DC 05 4B BA A7 17 11 61  l?Áô▮  {Ü K§  a
```

[그림 53] TweaakNow securedelete 사용에 따른 데이터 영역 변화

Random Data로 Overwrite 되는 것을 확인할 수 있다.

- wipefile

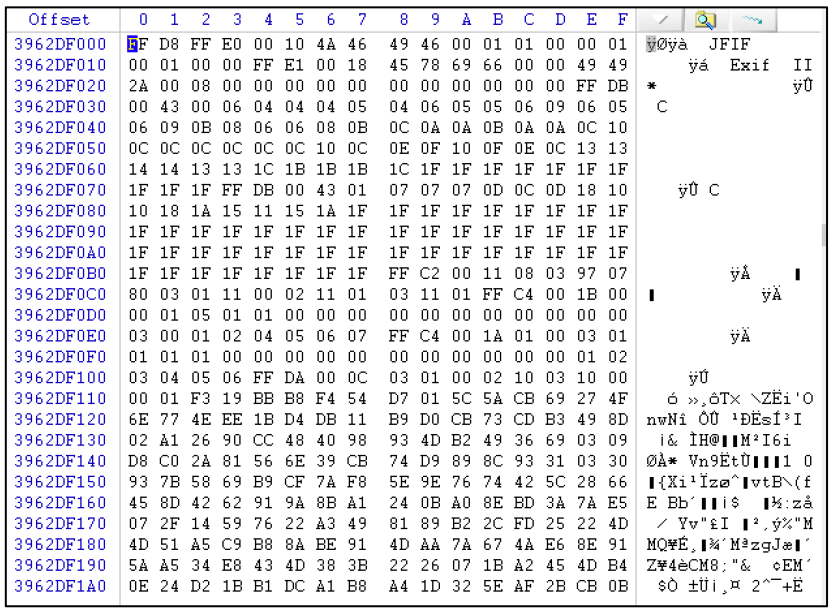
1. 메타데이터 변화

	File Deletion		1.jpg	2021-05-14 13:36:18	2021-05-14 16:17:59	2021-05-14 16:17:59	2021-05-14 16:17:59	Delete Index Ent...	0x0
2021-05-14 16:17:59	Renaming File	1.jpg->w.MWc	w.MWc					Create Attribute	0x899d
2021-05-14 16:17:59	File Deletion		w.MWc	2000-01-01 09:00:00	2000-01-01 09:00:00	2021-05-14 16:17:59	2000-01-01 09:00:00	Delete Index Ent...	0x1
	File Deletion		10.jpg	2021-05-14 13:36:18	2021-05-14 16:17:59	2021-05-14 16:17:59	2021-05-14 16:17:59	Delete Index Ent...	0x0
2021-05-14 16:17:59	Renaming File	10.jpg->Sh.OM0	Sh.OM0					Create Attribute	0x899d
	File Deletion		Sh.OM0	2000-01-01 09:00:00	2000-01-01 09:00:00	2021-05-14 16:17:59	2000-01-01 09:00:00	Delete Index Ent...	0x1
	File Deletion		11.jpg	2021-05-14 13:36:18	2021-05-14 16:17:59	2021-05-14 16:17:59	2021-05-14 16:17:59	Delete Index Ent...	0x0
2021-05-14 16:17:59	Renaming File	11.jpg->zT.kdJ	zT.kdJ					Create Attribute	0x899d
	File Deletion		zT.kdJ	2000-01-01 09:00:00	2000-01-01 09:00:00	2021-05-14 16:17:59	2000-01-01 09:00:00	Delete Index Ent...	0x1
	File Deletion		12.jpg	2021-05-14 13:36:18	2021-05-14 16:17:59	2021-05-14 16:17:59	2021-05-14 16:17:59	Delete Index Ent...	0x0
2021-05-14 16:17:59	Renaming File	12.jpg->XT.8rM	XT.8rM					Create Attribute	0x899d
	File Deletion		XT.8rM	2000-01-01 09:00:00	2000-01-01 09:00:00	2021-05-14 16:17:59	2000-01-01 09:00:00	Delete Index Ent...	0x1
	File Deletion		13.jpg	2021-05-14 13:36:18	2021-05-14 16:17:59	2021-05-14 16:17:59	2021-05-14 16:17:59	Delete Index Ent...	0x0
2021-05-14 16:17:59	Renaming File	13.jpg->TN.Nxt	TN.Nxt					Create Attribute	0x899e
	File Deletion		TN.Nxt	2000-01-01 09:00:00	2000-01-01 09:00:00	2021-05-14 16:17:59	2000-01-01 09:00:00	Delete Index Ent...	0x1
	File Deletion		14.jpg	2021-05-14 13:36:18	2021-05-14 16:17:59	2021-05-14 16:17:59	2021-05-14 16:17:59	Delete Index Ent...	0x0
2021-05-14 16:17:59	Renaming File	14.jpg->vK.nj2	vK.nj2					Create Attribute	0x899e
	File Deletion		vK.nj2	2000-01-01 09:00:00	2000-01-01 09:00:00	2021-05-14 16:17:59	2000-01-01 09:00:00	Delete Index Ent...	0x1

[그림 54] wipefile 사용에 따른 메타 데이터 변화

파일 이름 길이와 확장자 길이를 보존하며 소문자 대문자 숫자를 모두 활용한 랜덤 문자열을 파일이름으로 사용한다. 또한 MAC time 일부를 2000-01-01 09:00:00으로 setting하는 것을 확인할 수 있다.

2. 데이터 영역 변화



[그림 55] wipefile 사용에 따른 데이터 영역 변화

기본 세팅에서는 파일 데이터가 overwrite 되지 않고 존재하는 것을 확인하였다.

https://drive.google.com/drive/folders/1dPXX_b0FZnaF3J7SEqjw5LOKtqBLtYXn?usp=sharing 실험을 위해 사용된 Data 는 다음과 같다.

문제에서 주어진 test_shredder.e01은 NTFS 파티션을 이미징한 파일이다. 해당 이미지 내에 $LOGFILE과 $MFT를 발견하여 추출할 수 있었고, NTFS Log Tracker를 이용해 전처리를 수행하여 SQLITE 형태로 변환하였다. 해당 SQLITE는 초반부에는 아래와 같은 형상을 나타내었다.

7839781		Writing Content ...	Data Runs(in Vol...							Update Mapping...
7840098		Writing Content ...	Data Runs(in Vol...							Update Mapping...
7840423		Writing Content ...	Data Runs(in Vol...							Update Mapping...
7840740		Writing Content ...	Data Runs(in Vol...							Update Mapping...
7841065		Writing Content ...	Data Runs(in Vol...							Update Mapping...
7841394		Writing Content ...	Data Runs(in Vol...							Update Mapping...
7841711		Writing Content ...	Data Runs(in Vol...							Update Mapping...
7842140				LOGFILEWIPER		1601-01-01 09:...	1601-01-01 09:...	1601-01-01 09:...	1601-01-01 09:...	Deallocate File R...
7843032				~BCWipe.tmp	\~BCWipe.tmp	1601-01-01 09:...	1601-01-01 09:...	1601-01-01 09:...	2021-04-08 11:...	Deallocate File R...

[그림 56] NTFS Log Tracker 수행 결과

위의 부분은 BCWipe에 의해 wiping된 내역과 유사한 것을 알 수 있다. 즉 BCwipe에 의해 삭제가 수행되며 $LogFILE의 삭제 역시 함께 수행된 것을 확인할 수 있다.

	File Deletion		37.jpg	\37.jpg	2000-01-01 00:...	2000-01-01 00:...	2021-04-08 11:...	2000-01-01 00:...	Delete Index Ent...
2021-04-08 11:...	Renaming File	37.jpg -> Xb2nLU	Xb2nLU	\Xb2nLU					Create Attribute
			12.jpg	\12.jpg	2021-04-08 11:...	2021-04-04 19:...	2021-04-08 03:...	2021-04-08 11:...	Update Resident...
			41.png	\41.png	2021-04-08 11:...	2021-04-03 08:...	2021-04-08 03:...	2021-04-08 11:...	Update Resident...
			13.jpg	\13.jpg	2021-04-08 11:...	2021-04-03 08:...	2021-04-08 03:...	2021-04-08 11:...	Update Resident...
			8.jpg	\8.jpg	2021-04-08 11:...	2021-04-03 08:...	2021-04-08 03:...	2021-04-08 11:...	Update Resident...
			35.jpg	\35.jpg	2021-04-08 11:...	2021-04-04 19:...	2021-04-08 03:...	2021-04-08 11:...	Update Resident...
2021-04-08 11:...	File Deletion		Xb2nLU	\Xb2nLU	2000-01-01 00:...	2000-01-01 00:...	2021-04-08 11:...	2000-01-01 00:...	Delete Index Ent...
			Xb2nLU	\Xb2nLU	2000-01-01 00:...	2000-01-01 00:...	2021-04-08 11:...	2000-01-01 00:...	Deallocate File R...
	File Deletion		9.jpg	\9.jpg	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	Delete Index Ent...
2021-04-08 11:...	Renaming File	9.jpg -> _temp4...	_temp4186564...	_temp418656...					Create Attribute
2021-04-08 11:...	File Deletion		_temp4186564...	_temp418656...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	Delete Index Ent...
			_temp4186564...	_temp418656...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	Deallocate File R...
	File Deletion		40.jpg	\40.jpg	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	Delete Index Ent...
2021-04-08 11:...	Renaming File	40.jpg -> sS.W2d	sS.W2d	\sS.W2d					Create Attribute
			39.jpeg	\39.jpeg	2021-04-08 11:...	2021-04-04 19:...	2021-04-08 03:...	2021-04-08 11:...	Update Resident...
2021-04-08 11:...	File Deletion		sS.W2d	\sS.W2d	2000-01-01 09:...	2000-01-01 09:...	2021-04-08 11:...	2000-01-01 09:...	Delete Index Ent...
			sS.W2d	\sS.W2d	2000-01-01 09:...	2000-01-01 09:...	2021-04-08 11:...	2000-01-01 09:...	Deallocate File R...
	File Deletion		1.jpg	\1.jpg	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	Delete Index Ent...
2021-04-08 11:...	Renaming File	1.jpg -> _temp4...	_temp4186564...	_temp418656...					Create Attribute
			.	\.	1601-01-01 09:...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	Update Resident...
	File Deletion		_temp4186564...	_temp418656...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	Delete Index Ent...
			$ObjId						Delete Index Ent...
			_temp4186564...	_temp418656...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	Deallocate File R...
			$Tops	\$Extend\$Rm...	2021-04-08 04:...	2021-04-08 04:...	2021-04-08 04:...	2021-04-08 04:...	Update Resident...

[그림 57] 완전 삭제 도구와 관련된 것으로 확인되는 NTFS Transaction Log

위의 내역은 BCWIPE의 LOGFILE Wiping이 진행된 이후의 $LOGFILE에 기록된 NTFS Transaction LOG이다. File renaming에 영향 받은 파일은 '37.jpg', '9.jpg', '40.jpg', '1.jpg'가 있다.

'37.jpg'의 경우 파일명 변경 시 총 이름 글자 6글자를 유지하며 랜덤 문자열로 대문자, 소문자, 숫자를 모두 사

용하는 것으로 확인하였다. 또한 메타데이터 중 MAC time의 일부를 '2000-01-01 00:00:00' 으로 변하는 것으로 보아 이는 UTC+0 을 사용한다는 가정하에 delete file permanently 를 사용했음을 추정할 수 있다.

'9.jpg'와 '1.jpg'의 경우 임시 파일 문자열로 "_temp41865644161"을 사용하는 것으로 보아, pc shredder를 사용하고 있음을 추정할 수 있다.

'40.jpg'의 경우 파일 명으로 대문자 소문자 숫자를 모두 사용하지만 확장자의 길이와 본 파일 명의 길이를 모두 보존한다는 특징을 가지고 있고 생성된 temp 파일의 MAC 시간이 '2000-01-01 09:00:00' 인 것으로 보아 wipefile로 wiping 하였음을 추정할 수 있다. 뿐만 아니라 파일이 존재한 MFT_Cluster Index를 통해 확인한 봐 아래와 같은 패턴을 확인하였다. 실험에서 wipefile의 경우 original 데이터가 그대로 잔재하였지만, 프로그램 버전 등에 의한 차이로 실제 동작 과정이 차이가 존재할 수 있다.

[그림 58] MFT_Cluster Index에 나타난 패턴

즉 파일 삭제를 위해 사용된 프로그램은 **"BCWipe","delete file permanently","pc shredder","wipefile"**이다.

2. List the files deleted by the user in order of deletion time. Describe all artifacts that indicate the deletion time. (50 points)

완전 삭제 도구들이 사용하는 Temp 파일의 메타데이터, Modified, Accessed, Created, MFT Modified값을 이용해 도구의 완전 삭제 시간을 유추할 수 있다.

삭제된 시각을 파악하기 위해서는 file wiping 도구들이 사용하는 Temp 파일의 메타데이터 시간을 통해 유추할 수 있다.

7839781		Writing Content ...	Data Runs(in Vol...							Update Mapping...
7840098		Writing Content ...	Data Runs(in Vol...							Update Mapping...
7840423		Writing Content ...	Data Runs(in Vol...							Update Mapping...
7840740		Writing Content ...	Data Runs(in Vol...							Update Mapping...
7841065		Writing Content ...	Data Runs(in Vol...							Update Mapping...
7841394		Writing Content ...	Data Runs(in Vol...							Update Mapping...
7841711		Writing Content ...	Data Runs(in Vol...							Update Mapping...
7842140				LOGFILEWIPER		1601-01-01 09:...	1601-01-01 09:...	1601-01-01 09:...	1601-01-01 09:...	Deallocate File R...
7843032				~BCWipe.tmp	\~BCWipe.tmp	1601-01-01 09:...	1601-01-01 09:...	1601-01-01 09:...	2021-04-08 11:...	Deallocate File R...

[그림 59] BCWipe.tmp에 대한 메타 데이터 시간 확인

BCwipe.tmp의 경우, ~BCWipe.tmp 파일의 Access Time 을 통해 삭제된 시간을 유추할 수 있다. 2021-04-08 11:11:58 에 삭제가 수행되었으나 실제 어떤 파일이 지워졌는지는 알 수 없다.

	File Deletion		37.jpg	\37.jpg	2000-01-01 00:...	2000-01-01 00:...	2021-04-08 11:...	2000-01-01 00:...	Delete Index Ent...
2021-04-08 11:...	Renaming File	37.jpg -> Xb2nLU	Xb2nLU	\Xb2nLU					Create Attribute
			12.jpg	\12.jpg	2021-04-08 11:...	2021-04-04 19:...	2021-04-08 03:...	2021-04-08 11:...	Update Resident...
			41.png	\41.png	2021-04-08 11:...	2021-04-03 08:...	2021-04-08 03:...	2021-04-08 11:...	Update Resident...
			13.jpg	\13.jpg	2021-04-08 11:...	2021-04-03 08:...	2021-04-08 03:...	2021-04-08 11:...	Update Resident...
			8.jpg	\8.jpg	2021-04-08 11:...	2021-04-03 08:...	2021-04-08 03:...	2021-04-08 11:...	Update Resident...
			35.jpg	\35.jpg	2021-04-08 11:...	2021-04-04 19:...	2021-04-08 03:...	2021-04-08 11:...	Update Resident...
2021-04-08 11:...	File Deletion		Xb2nLU	\Xb2nLU	2000-01-01 00:...	2000-01-01 00:...	2021-04-08 11:...	2000-01-01 00:...	Delete Index Ent...
			Xb2nLU	\Xb2nLU	2000-01-01 00:...	2000-01-01 00:...	2021-04-08 11:...	2000-01-01 00:...	Deallocate File R...

[그림 60] delete file permanently에 대한 메타 데이터 시간 확인

delete file permanently의 경우에는 MFT_ModifiedTime을 이용하여 삭제 시간을 유추할 수 있다. 37.jpg의 이름이 변형된 Xb2nLU의 경우 원본과 Temp 파일의 MACB 메타데이터 중 MFT_ModifiedTime이 관련된 시간임을 파악할 수 있다. “2021-04-08 11:12:21”

2021-04-08 11:...	Renaming File	9.jpg -> _temp4...	_temp4186564...	_temp418656...					Create Attribute
2021-04-08 11:...	File Deletion		_temp4186564...	_temp418656...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	Delete Index Ent...
			_temp4186564...	_temp418656...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	Deallocate File R...

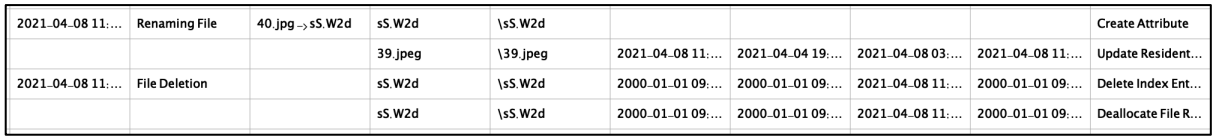
	File Deletion		1.jpg	\1.jpg	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	Delete Index Ent...
2021-04-08 11:...	Renaming File	1.jpg -> _temp4...	_temp4186564...	_temp418656...					Create Attribute
			.	\.	1601-01-01 09:...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	Update Resident...
	File Deletion		_temp4186564...	_temp418656...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	Delete Index Ent...
			$ObjId						Delete Index Ent...
			_temp4186564...	_temp418656...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	2021-04-08 11:...	Deallocate File R...
			$Tops	\$Extend\$Rm...	2021-04-08 04:...	2021-04-08 04:...	2021-04-08 04:...	2021-04-08 04:...	Update Resident...

[그림 61] pc shredder에 대한 메타 데이터 시간 확인

pc shredder의 경우 _temp41865644161과 원본 파일의 ModifiedTime, MFT_ModifiedTime, Access Time을 통하여 삭제가 수행된 시간을 확인할 수 있다. 원본과 temp 파일의 ModifiedTime, MFT_ModifiedTime, Access Time이 동일한 것을 통해 유추할 수 있다.

1.jpg -> _temp41865644161 : 2021-04-08 11:12:50

9.jpg -> _temp41865644161 : 2021-04-08 11:12:31



2021-04-08 11:...	Renaming File	40.jpg -> sS.W2d	sS.W2d	\sS.W2d					Create Attribute
			39.jpeg	\39.jpeg	2021-04-08 11:...	2021-04-04 19:...	2021-04-08 03:...	2021-04-08 11:...	Update Resident...
2021-04-08 11:...	File Deletion		sS.W2d	\sS.W2d	2000-01-01 09:...	2000-01-01 09:...	2021-04-08 11:...	2000-01-01 09:...	Delete Index Ent...
			sS.W2d	\sS.W2d	2000-01-01 09:...	2000-01-01 09:...	2021-04-08 11:...	2000-01-01 09:...	Deallocate File R...

[그림 62] Wipefile에 대한 메타 데이터 시간 확인

Wipefile의 경우 원본 파일은 ModifiedTime, MFT_ModifiedTime, AccessTime, temp 파일의 경우는 MFT_ModifiedTime을 통해 삭제된 시간을 유추할 수 있다. 2021-04-08 11:12:43

결과를 표로 나타내면 다음과 같다.

[표 1] 타임라인 별 사용 완전 삭제도구 및 MACB 타임스탬프 정보

TimeLine	Tool name	Filename	Source	MACB Timestamp			
				Modified	Accessed	Created	MFT Modified
2021-04-08 11:11:58	BCWipe	-	Original	X	X	X	X
		~BCWipe.tmp	Temp	X	O	X	X
		LOGFILEWIPER	Temp	X	X	X	X
2021-04-08 11:12:21	delete file permanently	37.jpg	Original	X	X	X	O
		Xb2nLU	Temp	X	X	X	O
2021-04-08 11:12:31	pc shredder	1.jpg	Original	O	O	X	O
		_temp41865644161	Temp	O	O	X	O
2021-04-08 11:12:43	Wipefile	40.jpg	Original	O	O	X	O
		sS.W2d	Temp	X	X	X	O
2021-04-08 11:12:50	pc shredder	1.jpg	Original	O	O	X	O
		_temp41865644161	Temp	O	O	X	O