Подводные камни при парсинге NTFS и реестра

Максим Суханов,
ведущий эксперт CICADA8, MTC RED

ОБО МНЕ

- Ранее работал в BI.ZONE, Group-IB
- 13 лет в сферах Digital Forensics, Incident Response, Malware Analysis, Threat Intelligence
- Занимался обратной разработкой форматов NTFS, FAT12/16/32, exFAT, реестра Windows, теневых копий
- Создаю утилиты и библиотеки:
  - yarp (парсер файлов реестра Windows),
  - dfir_ntfs (парсер томов NTFS, FAT12/16/32 exFAT, а также теневых копий),
  - winmem_decompress (распаковщик сжатых страниц из дампов памяти),
  - и многое другое…
- Ищу и нахожу уязвимости в парсерах файловых систем и загрузчиках

МАКСИМ СУХАНОВ

Ведущий эксперт инновационного центра Future Crew компании МТС RED

masuhano@mts.ru

КОМАНДА CICADA8

- Эксперты с мировым именем в сообществе ИБ
- Цитируемость в иностранных источниках
- Уникальные соревновательные и педагогические программы
- Опыт расследования сложных инцидентов
- Внедрение процессов безопасной разработки и управления уязвимостями
- Разработка с нуля и внедрение процессов управления рисками ИБ
- Проведение комплексных проектов по анализу защищенности
- Взаимодействие с SOC в крупных организациях в различных сферах
- Адаптация количественной оценки риска ИБ для компаний

CICADA8

MTC RED — ЭКОСИСТЕМА ТЕХНОЛОГИЙ, СЕРВИСОВ И УСЛУГ

БЛОК CORE BUSINESS

развитие зарекомендовавших себя продуктов
и сервисов кибербезопасности

- Услуги
- Продукты
- Сервисы

FUTURE CREW

разработка инновационных технологий,
которые уже завтра станут стандартом

- Персональная кибербезопасность
- Интеллектуальные системы
- Анализ защищенности

CICADA8

01

«НОВЫЕ ФИЧИ»

CICADA8

СКОЛЬКО РАЗ УВЕЛИЧИВАЛСЯ НОМЕР ВЕРСИИ?

Начиная с Windows XP...

- Для формата файлов кустов реестра: 1 раз.
- Для формата файловой системы NTFS: 0 раз.

Изменения, нарушающие обратную совместимость:

- Для формата файлов кустов реестра: 2 раза.
- Для формата файловой системы NTFS: 3 раза.

А еще есть незначительные изменения!

ЖУРНАЛИРОВАНИЕ РЕЕСТРА

СТАРЫЙ ФОРМАТ ЖУРНАЛА:

Измененные данные

Запись №1 → Файл журнала (перезапись целиком)

Запись №2 → Основной файл (перезапись нужной области)

Число записанных байтов в 2 раза больше, чем измененных...

НОВЫЙ ФОРМАТ:

Измененные данные

Запись → Файл журнала (добавление в конец)

Раз в час:

Все измененные за час данные

Запись → Основной файл

КУСТЫ РЕЕСТРА

WINDOWS 10 И 11:

- В ядро добавлена функциональность контейнеризации реестра.
  - Номер версии изменен, чтобы файл куста-оверлея нельзя было подключить как обычный.

Основной куст + Куст-оверлей = **Видимое в контейнере представление реестра**

↑

Новая версия формата!

NTFS

WINDOWS 8, 8.1, 10 И 11:

- Изменен формат журнала транзакций ($LogFile).
- Раньше журналирование операций требовало их тройной записи. Сейчас в большинстве случаев требуются две.
- Изменен номер версии журнала, но не формата файловой системы!
  - Новый номер версии журнала принимается старыми драйверами (например, в Windows 7).
  - Но не поддерживается и «исправляется»…

Additional Background

As discussed in the prior section, a change was made to the NTFS Log File structure in Windows 8 to reduce I/O counts, improving system performance, and with potentially reduced power consumption. However, a side effect of this change is that the new log format is unrecognizable with prior versions of Windows, which may result in a prior version of NTFS marking the volume as corrupt (since the contents of the log is in an unrecognized format). This will trigger a chkdsk run upon reboot to ensure that file system metadata is consistent, which will clear the corrupted state of the log file and return the file system to a clean state.

https://social.technet.microsoft.com/wiki/contents/articles/15645.windows-8-volume-compatibility-considerations-with-prior-versions-of-windows.aspx

NTFS

WINDOWS 10 И 11:

- Добавлена поддержка очень больших кластеров (вплоть до 2M).
- Добавлена поддержка директорий с регистрозависимыми именами файлов.

NTFS

МЕНЕЕ ЗНАЧИТЕЛЬНЫЕ ИЗМЕНЕНИЯ:

- Митигация целого класса уязвимостей, использующих симлинки (EoP через TOCTOU).
- Внедрение функции Storage Reserve:
  - резервирование пространства для служебных целей;
  - снижение доступного для пользователя размера свободного пространства.

РЕЗЮМЕ

CIDADA[8]

ЕСТЬ ЛИ У ВАС...

Поддержка журналов транзакций реестра?

- Если нет, то вы не увидите текущее состояние куста (отставание будет до часа).
- А вывод парсера будет ожидаемым, но некорректным!

Поддержка кустов реестра из контейнеров?

- The Registry Hives You May be MSIX-ING: Registry Redirection with MS MSIX
- zerofox.com/blog/the-registry-hives-you-may-be-msix-ing-registry-redirection-with-ms-msix/

Поддержка журнала $LogFile?

- Если да, то что там с новым форматом?

02

«НЕИЗВЕСТНОЕ СТАРОЕ»

CICADA8

ВРЕМЕННЫЕ МЕТКИ ФАЙЛОВ В NTFS

- **4** временных метки (MACE) в атрибуте $STANDARD_INFORMATION в файловой записи.
- **4** временных метки в атрибуте $FILE_NAME в файловой записи.
- **4** временных метки в атрибуте $FILE_NAME в индексной записи.
- **1** временная метка последнего доступа в оперативной памяти (хранится до отложенной записи на диск).
- А еще:
  - **1** временная метка в атрибуте $OBJECT_ID в файловой записи;
  - временные метки операций в записях USN;
  - временные метки в записях $LogFile...

ВРЕМЕННЫЕ МЕТКИ ФАЙЛОВ В NTFS

СКОЛЬКО ВРЕМЕННЫХ МЕТОК ПОКАЗЫВАЕТ ВАШ ПАРСЕР?

ОСТАТОЧНЫЕ ДАННЫЕ В ИНДЕКСНЫХ ЗАПИСЯХ

ДВА ТИПА ВОССТАНАВЛИВАЕМЫХ ДАННЫХ:

- удаленные атрибуты $FILE_NAME;
- фрагменты имен файлов.

ДВА ИСТОЧНИКА:

- нерезидентные индексы;
- зазоры файловых записей (резидентные индексы).


000001f0 01 00 00 00 00 00 00 00 ff ff ff ff 82 79 33 00 |.....y3.|
00000200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000210 00 00 00 10 00 00 00 00 19 00 41 00 61 00 64 00 |.....A.a.d.|
00000220 52 00 65 00 63 00 6f 00 76 00 65 00 72 00 79 00 |R.e.c.o.v.e.r.y.|
00000230 50 00 61 00 73 00 73 00 77 00 6f 00 72 00 64 00 |P.a.s.s.w.o.r.d.|
00000240 44 00 65 00 6c 00 65 00 74 00 65 00 61 00 74 00 |D.e.l.e.t.e.a.t.|
00000250 28 00 00 00 00 00 01 00 90 00 7e 00 00 00 00 00 |(.....~.....|
00000260 24 00 00 00 00 00 01 00 17 06 94 90 42 ca d6 01 |$.....B...|
00000270 17 06 94 90 42 ca d6 01 5a 7b 94 90 42 ca d6 01 |....B...Z{..B...|
00000280 5a 7b 94 90 42 ca d6 01 00 00 00 00 00 00 00 00 |Z{..B.....|
00000290 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 |.....|
000002a0 1e 00 43 00 6c 00 69 00 65 00 6e 00 74 00 52 00 |..C.l.i.e.n.t.R.|
000002b0 65 00 63 00 6f 00 76 00 65 00 72 00 79 00 50 00 |e.c.o.v.e.r.y.P.|
000002c0 61 00 73 00 73 00 77 00 6f 00 72 00 64 00 52 00 |a.s.s.w.o.r.d.R.|
000002d0 6f 00 74 00 61 00 74 00 69 00 6f 00 6e 00 00 00 |o.t.a.t.i.o.n...|
000002e0 2a 00 00 00 00 00 01 00 78 00 64 00 00 00 00 00 |*.....x.d.....|
000002f0 24 00 00 00 00 00 01 00 f2 74 b3 90 42 ca d6 01 |$.....t..B...|
00000300 0e 9c b3 90 42 ca d6 01 0e 9c b3 90 42 ca d6 01 |....B.....B...|
00000310 1c c3 b3 90 42 ca d6 01 50 00 00 00 00 00 00 00 |....B...P.....|
00000320 4c 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 |L..... .....|
00000330 11 00 49 00 6e 00 64 00 65 00 78 00 65 00 72 00 |..I.n.d.e.x.e.r.|
00000340 56 00 6f 00 6c 00 75 00 6d 00 65 00 47 00 75 00 |V.o.l.u.m.e.G.u.|
00000350 69 00 64 00 00 00 00 00 26 00 00 00 00 00 01 00 |i.d.....&.....|
00000360 70 00 5e 00 00 00 00 00 24 00 00 00 00 00 01 00 |p.^.....$.....|
00000370 58 aa 05 03 42 ca d6 01 7a f8 05 03 42 ca d6 01 |X...B...z...B...|
00000380 7a f8 05 03 42 ca d6 01 e6 90 93 90 42 ca d6 01 |z...B.....B...|
00000390 10 00 00 00 00 00 00 00 0c 00 00 00 00 00 00 00 |.....|
000003a0 20 00 00 00 00 00 00 00 0e 00 57 00 50 00 53 00 | .....W.P.S.|
000003b0 65 00 74 00 74 00 69 00 6e 00 67 00 73 00 2e 00 |e.t.t.i.n.g.s...|
000003c0 64 00 61 00 74 00 00 00 00 00 00 00 00 00 00 00 |d.a.t.....|
000003d0 10 00 00 00 02 00 00 00 ff ff ff ff 82 79 47 11 |.....yG.|
000003e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
000003f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 33 00 |.....3.|
Конец данных файловой записи
Оставшиеся атрибуты $FILE_NAME
Предыдущий конец

ОСТАТОЧНЫЕ ДАННЫЕ В ИНДЕКСНЫХ ЗАПИСЯХ

File record /Users/Public/Music

Slack /Users/Public/Music/**pw.txt**

Slack /Users/Public/Music/Sample Music

Slack /Users/Public/Music/SAMPLE~1

Slack <Unknown, likely the same as above>/<Can be partially overwritten or start with a wrong character>**ipsec_<удалено>.zip**

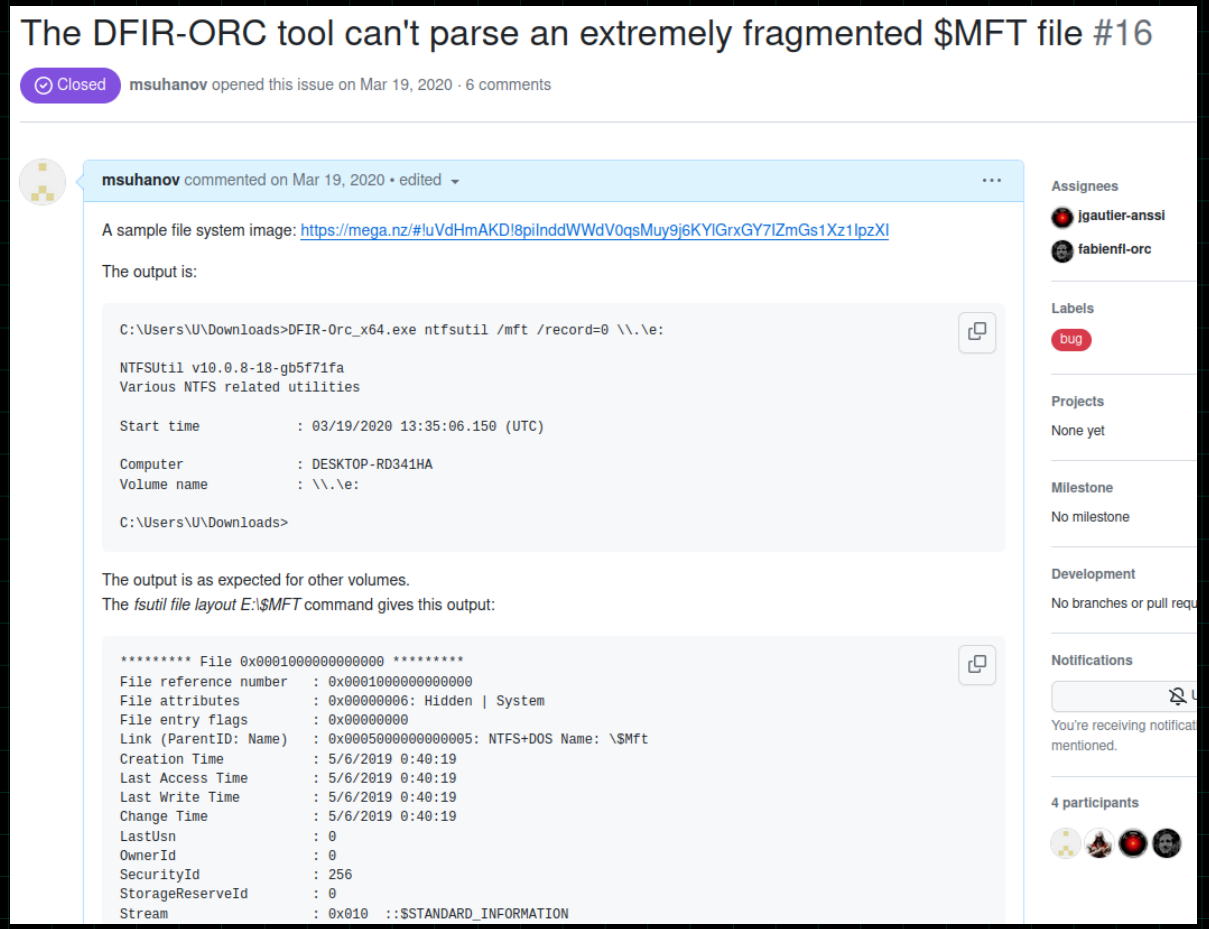
File record /Users/Public/Music/Sample Music

СИЛЬНАЯ ФРАГМЕНТАЦИЯ $MFT

- Любой файл может быть фрагментирован, в т. ч. $MFT.
- Алгоритм чтения $MFT отличается от случаев с другими файлами:
  - $MFT описывает себя;
  - чтобы прочитать второй фрагмент $MFT, нужно прочитать первый фрагмент $MFT (и т. д.);
  - таких итераций может быть много...

СИЛЬНАЯ ФРАГМЕНТАЦИЯ $MFT

```
$ATTRIBUTE_LIST Attribute Values:
Type: 16-0      MFT Entry: 0          VCN: 0
Type: 48-3      MFT Entry: 0          VCN: 0
Type: 128-6     MFT Entry: 0          VCN: 0
Type: 128-0     MFT Entry: 15         VCN: 18067970
Type: 128-0     MFT Entry: 34799618   VCN: 41006314
Type: 176-0     MFT Entry: 16         VCN: 0
Type: 176-0     MFT Entry: 17         VCN: 708
Type: 176-0     MFT Entry: 18         VCN: 1416
Type: 176-0     MFT Entry: 19         VCN: 2124
Type: 176-0     MFT Entry: 20         VCN: 2832
Type: 176-0     MFT Entry: 21         VCN: 3540
Type: 176-0     MFT Entry: 22         VCN: 4248
Type: 176-0     MFT Entry: 34799617   VCN: 4956
Type: 176-0     MFT Entry: 34799619   VCN: 5664
```



The DFIR-ORC tool can't parse an extremely fragmented $MFT file #16

Closed · msuhanov opened this issue on Mar 19, 2020 · 6 comments

msuhanov commented on Mar 19, 2020 • edited

A sample file system image: https://mega.nz/#!uVdHmAKD!8piInddWWdV0qsMuy9j6KYlGrxGY7lZmGs1Xz1lpzXI

The output is:

```
C:\Users\U\Downloads>DFIR-Orc_x64.exe ntfsutil /mft /record=0 \\.\e:

NTFSUtil v10.0.8-18-gb5f71fa
Various NTFS related utilities

Start time            : 03/19/2020 13:35:06.150 (UTC)

Computer              : DESKTOP-RD341HA
Volume name           : \\.\e:

C:\Users\U\Downloads>
```

The output is as expected for other volumes.
The *fsutil file layout E:\$MFT* command gives this output:

```
********* File 0x0001000000000000 *********
File reference number   : 0x0001000000000000
File attributes         : 0x00000006: Hidden | System
File entry flags        : 0x00000000
Link (ParentID: Name)   : 0x0005000000000005: NTFS+DOS Name: \$Mft
Creation Time           : 5/6/2019 0:40:19
Last Access Time        : 5/6/2019 0:40:19
Last Write Time         : 5/6/2019 0:40:19
Change Time             : 5/6/2019 0:40:19
LastUsn                 : 0
OwnerId                 : 0
SecurityId              : 256
StorageReserveId        : 0
Stream                  : 0x010  ::$STANDARD_INFORMATION
```

Assignees: jgautier-anssi, fabienfl-orc
Labels: bug
Projects: None yet
Milestone: No milestone
Development: No branches or pull requ
Notifications: You're receiving notificat mentioned.
4 participants

CIOADA8

ТЕНЕВЫЕ КОПИИ В ОФЛАЙНЕ

Сценарий с экспортом NTDS.DIT через теневую копию:

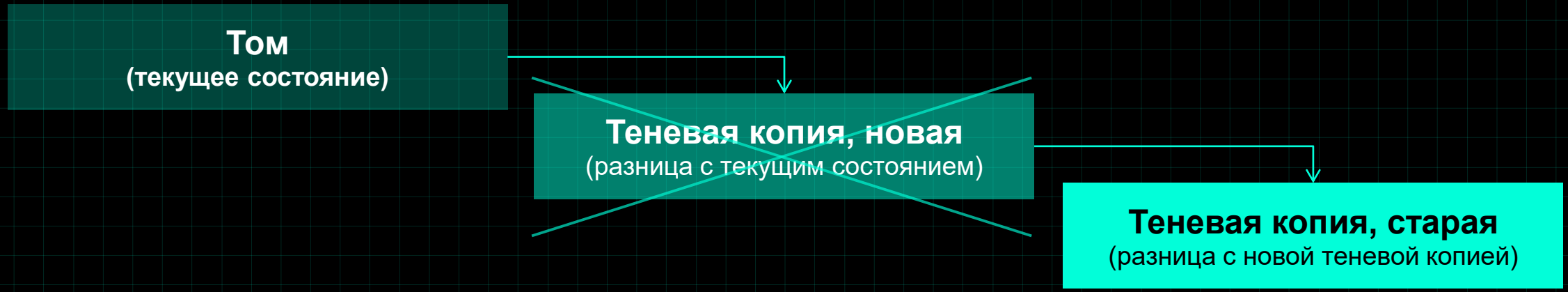
- создаем теневую копию;
- копируем из нее NTDS.DIT;
- удаляем теневую копию.

ЧТО СЛУЧИЛОСЬ С ЭТОЙ ТЕНЕВОЙ КОПИЕЙ?

ТЕНЕВЫЕ КОПИИ В ОФЛАЙНЕ

Теневая копия все еще существует, но она отсутствует в выводе «*vssadmin list shadows*».

- Это отметка «офлайн».
- Теневые копии, от которых зависят другие теневые копии, не удаляются, но становятся невидимыми.



msuhanov commented on Aug 18, 2022

Hello.

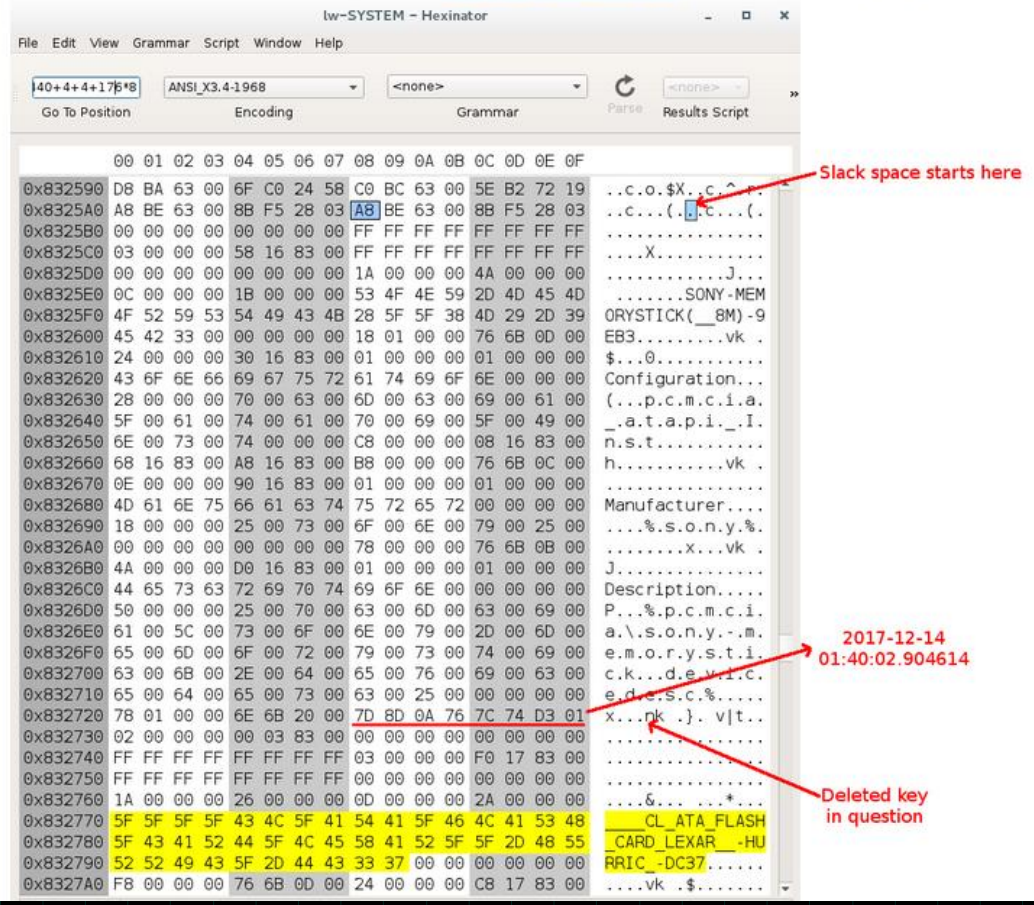
The bug is here:

Registry/Registry/Other/HBinRecord.cs
Line 325 in 1a301f3

```
325     if (Math.Abs(size) <= 3 || remainingData.Length - actualStart < size)
```

If the `remainingData.Length - actualStart < size` condition is met, the deleted item isn't processed. This condition can be true for a valid deleted key/value if its cell has been merged with a preceding one and then the resulting cell is split to hold a subkeys list, so the deleted key/value goes to the slack of this list (i.e., stored after its last item).

Here is an example (this is the SYSTEM hive file from the 2018 Lone Wolf Scenario, *without* transaction log files applied):



Assignees
No one assig

Labels
None yet

Projects
None yet

Milestone
No milestone

Developmer
No branches

Notification
You're receiv
thread.

2 participan

CIOADA8


CIDADA8
ВОПРОСЫ?