Advanced \$UsnJrnl Forensics

blueangel

blueangel1275@gmail.com

http://forensic-note.blogspot.kr/

Junghoon Oh





1. \$UsnJrnl

- 2. \$UsnJrnl Record Carving
- 3. NTFS Log Tracker v1.4
- 4. Conclusion



Journal(Change) Log File of NTFS

• This file is used to determine whether any change is occurred in a specific file by applications.

From Win7, Journal Function is activated by default

- In case of deactivation setting(in Win XP), it is possible to activate through "Fsutil".
 - > fsutil usn [createjournal] m=<MaxSize> a=<AllocationDelta> <VolumePath>
- For more information about "Fsutil" : <u>http://technet.microsoft.com/en-us/library/cc788042.aspx</u>

• The file is composed of "\$Max" attribute and "\$J" attribute

- \$Max : The meta data of change log is stored.
- \$J : The actual change log records are stored.
 - ✓ Each record has USN(Update Sequence Number) information.
 - $\checkmark~$ The record order is determined with USN.
 - ✓ USN = the offset value of a record within J attribute
 - ✓ USN information is also stored in then \$STANDARD_INFORMATION attribute of a MFT record



Journal(Change) Log File of NTFS(continue...)

Location

• The file is located under "\$Extend" folder.

É+D⊡ 🧐 C É+D⊡ 🎯 \$Extend	Name	File Created	Last Written	Entry Modified	Last Accessed	Logical Size
	🗋 \$UsnJrnl•\$J					1,246,483,680
	🕽 \$UsnJrnl•\$Max					32

• The size of log data(generally...)

- In case of full time use(24 hours/day), the log for 1~2 days are recorded.
- In case of regular use(8 hours/day), the log for 4~5 days are recorded.

Forensic Readiness

• changing log size bigger(more than 1 GB??)

Digital Forensic Profit

• The investigator can confirm every NTFS's events(creation, deletion, modification...) in specific period.



The Structure of \$Max attribute

- The size of \$Max attribute
 - 32 Bytes fixed size

• The format of \$Max attribute

Offset	Size	Stored Information	Detail
0x00	8	Maximum Size	The maximum size of log data
0x08	8	Allocation Size	The size of allocated area when new log data is saved.
0x10	8	USN ID	The creation time of "\$UsnJrnl" file(FILETIME)
0x18	8	Lowest Valid USN	The least value of USN in current records With this value, investigator can approach the start point of first record within "\$J" attribute



The Structure of \$J attribute

- The log records of variable size are listed consecutively.
- • The zero-filled "Sparse Area" occupies front part of an attribute.



- The reason for this structure is because the operating system keeps the same size of the log data saved in the \$J attribute.
- The record allocation policy of \$J attribute
 - 1. The new log records are added at the end of the attribute.
 - 2. If the total size of the added records exceeds "Allocation Size", the operation system assures that the size of the entire log data exceeds "Maximum Size".
 - 3. If the size of the entire log data exceeds "Maximum Size", the front area of attribute is occupied by zero as much as size of "Allocation Size".(Actually, disk area is not filled by zero.)
- Thus, the logical size of \$J attribute grow continuously, but the size of area saving actual data is kept constant.
- The general size of log data is $0x200000 \sim 0x23FFFFF$



The Structure of \$J attribute(continue...)

• After Logical area, there are valid data...

	Name	Initialized Size	Logical Size	Physical Size
1	🕞 \$ObjId	0	0	0
2	\$ObjId \$O	393,216	393,216	393,216
23	🙀 \$Quota	0	0	0
4	\$Quota \$O	88	88	88
2 5	🗋 \$Quota \$Q	208	208	208
26	📑 \$Reparse	0	0	0
7	\$Reparse \$R	4,096	4,096	4,096
28	🚞 \$RmMetadata	336	336	336
2 9	🔐 \$UsnJrnl	0	0	0
🛛 10	🗋 \$UsnJrnl·\$J	17,568,031,880	17,568,031,880	17,568,301,056
🛛 11	🗋 \$UsnJrnl•\$Max	32	32	32

E Text	: 🐺 I	Hex		Doc	9	Tra	nscri	ipt [ے P	ictur	e	R	epor	t 🖻	Co	nsole		Details 🗊 Output 🖂 🕩
1756803	1728	D8	E3	22	17	04	00	00	00	EC	73	EC	75	CE	00	DO	01	Øã"····ìsìuηз 🔺
1756803	1744	00	01	00	80	00	00	00	00	00	00	00	00	20	00	00	00	
1756803	1760	1A	00	3C	00	68	00	6F	00	74	00	5F	00	76	00	31	00	··<·h·o·t·_·v·1·
1756803	1776	5F	00	33	00	2E	00	6C	00	6F	00	63	00	6B	00	00	00	3l-o-c-k
1756803	1792	58	00	00	00	02	00	00	00	56	84	0C	00	00	00	2C	00	x · · · · · · V · · · · , ·
1756803	1808	29	FC	0B	00	00	00	07	00	30	E4	22	17	04	00	00	00)ü0ä"
1756803	1824	OD	C2	EC	75	CE	00	DO	01	00	02	00	80	00	00	00	00	ÂìuÎ Đ····
1756803	1840	00	00	00	00	20	00	00	00	1A	00	3C	00	68	00	6F	00	···· ·································
1756803	1856	74	00	5F	00	76	00	31	00	5F	00	33	00	2E	00	6C	00	t · _ · v · 1 · _ · 3 · . · 1 ·
1756803	1872	6F	00	63	00	6B	00	00	00	68	00	00	00	02	00	00	00	o·c·k···h·····
1756803	1888	2 A	7E	03	00	00	00	42	00	92	99	01	00	00	00	01	00	*~···B· ·····
1756803	1904	88	E4	22	17	04	00	00	00	1C	A1	7D	77	CE	00	DO	01	ä"····;}wηз
1756803	1920	03	81	00	00	00	00	00	00	00	00	00	00	00	20	00	00	
1756803	1936	28	00	3C	00	4 F	00	54	00	65	00	6C	00	65	00	44	00	(·< ·O ·T ·e ·l ·e ·D ·
1756803	1952	61	00	74	00	61	00	5F	00	33	00	34	00	38	00	30	00	a.t.a3.4.8.0.
1756803	1968	5F	00	37	00	2E	00	65	00	74	00	6C	00	00	00	00	00	7e.t.1
1756803	1984	68	00	00	00	02	00	00	00	6F	7E	0B	00	00	00	63	00	hc.
1756803	2000	92	99	01	00	00	00	01	00	FO	E4	22	17	04	00	00	00	·····ðā"·····
175 6002	2010	10	7.1	75		07	0.0	DO	0.1	0.0	0.1	0.0	00	0.0	0.0	00	0.0	and part

- Extracting \$J attribute by Encase 6(default "Logical File Only")
 - There is no valid data which is located after logical area.

Сору	Character Mask
Logical File Only	None
Entire Physical File	O Do not Write Non-ASCII Characters
🔘 RAM and Disk Slack	Replace Non-ASCII Characters With DOT
RAM Slack Only	Show Errors

\$UsnJml-\$J		Offset	0	1	2	3	- 4	5	6	7	8	9	Α	В	С	D	Е	F					
E:\Sample		41722E300	33	00	2E	00	74	00	73	00	69	00	64	00	78	00	00	00	3 . t	s	i d	х	
		41722E310	70	00	00	00	02	00	00	00	56	84	0C	00	00	00	2B	00	р		٧L		+
File size:	16.4 GB	41722E320	1D	C1	OB	00	00	00	31	00	10	EЗ	22	17	04	00	00	00	Á	1	ã"		
17,568	,031,880 bytes	41722E330	EC	73	EC	75	CE	00	DO	01	00	02	00	80	00	00	00	00	ìsìuÎ	Ð		1	
Default Edit Mode		41722E340	00	00	00	00	20	00	00	00	30	00	ЗC	00	73	00	70	00			0 <	s	р
State:	original	41722E350	6C	00	75	00	6E	00	6B	00	2D	00	6E	00	65	00	65	00	lun	k	- n	е	e
Undo level:		41722E360	64	00	2D	00	6F	00	70	00	74	00	69	00	6D	00	69	00	d - o	р	t i	m	i
Undo reverses:	0 n/a	41722E370	7A	00	65	00	2E	00	64	00	61	00	74	00	00	00	00	00	ze.	d	a t		
	100	41722E380	58	00	00	00	02	00	00	00	56	84	0C	00	00	00	2C	00	Х		۷L		,
Creation time:	2013-04-25	41722E390	29	FC	0B	00	00	00	07	00	80	EЗ	22	17	04	00	00	00)ü		١ã"		
	14:13:20	41722E3A0	EC	73	EC	75	CE	00	DO	01	00	01	00	00	00	00	00	00	ìsiuÎ	Ð			
Last write time:	2013-04-25	41722E3B0	00	00	00	00	20	00	00	00	1A	00	3C	00	68	00	6F	00			<	h	o
	14:13:20	41722E3C0	74	00	5F	00	76	00	31	00	5F	00	33	00	2E	00	6C	00	t_v	1	_ 3		1
Attributes:	А	41722E3D0	6F	00	63	00	6B	00	00	00	58	00	00	00	02	00	00	00	ock		Х		
lcons:	0	41722E3E0	56	84	0C	00	00	00	2C	00	29	FC	OB	00	00	00	07	00	VI	,)ü		
		41722E3F0	D8	EЗ	22	17	04	00	00	00	EC	73	EC	75	CE	00	DO	01	0ã"		isì	ıÎ	Ð
Mode: Character set:	hexadecimal ANSI ASCII	41722E400	00	01	00	80	00	00	00	00	00	00	00	00	20	00	00	00	- I				
Offsets:	hexadecimal	41722E410	1A	00	ЗC	00	68	00	6F	00	74	00	5F	00	76	00	31	00	< h	0	t _	v	1
Bytes per page:	46x16=736	41722E420	5F	00	33	00	2E	00	6C	00	6F	00	63	00	6B	00	00	00	_ 3 .	1	οс	k	
Window #:	1	41722E430	58	00	00	00	02	00	00	00	56	84	0C	00	00	00	2C	00	Х		V		,
No. of windows:	1	41722E440	29	FC	0B	00	00	00	07	00	30	Ε4	22	17	04	00	00	00)ü		0ä"		
		41722E450	OD	C2	EC	75	CE	00	DO	01	00	02	00	80	00	00	00	00	ÂìuÎ	Ð		1	
Clipboard:	available	41722E460	00	00	00	00	20	00	00	00	1A	00	ЗC	00	68	00	6F	00			<	h	ο
TEMP folder:	103 GB free	41722E470	74	00	5F	00	76	00	31	00	5F	00	33	00	2E	00	6C	00	t _ v	1	_ 3		1
3LUEAN~1\AppDa	ita\Local\Temp	41722E480	6F	00	63	00	6B	00	00	00									ock				



Collection of \$UsnJrnl

• Encase

• Extract \$J attribute after selecting "Entire Physical File" option

Winhex

• Default, this tool extracts file by Physical Size

ExtractUsnJrnl (<u>https://github.com/jschicht/ExtractUsnJrnl</u>)

• This tool can extract only valid data except sparse area.

이름	수정한 날짜	유형	크기
🗋 \$UsnJrnl_\$J.bin	2014-11-05 오전	BIN 파일	34,598KB



The format of record (<u>http://msdn.microsoft.com/en-us/library/aa365722.aspx</u>)

Offset	Size	Stored Information	Detail
0x00	4	Size of Record	
0x04	2	Major Version	2(Change Journal Software's major version)
0x06	2	Minor Version	2(Change Journal Software's major version)
0x08	8	MFT Reference Number	"MFT Reference Number" of file or directory that effected by currently change event.
0x10	8	Parent MFT Reference Number	"MFT Reference Number" of parent directory of file and directory that effected by currently change event. The full path information can be obtained with this information and \$MFT.
0x18	8	USN	Update Sequence Number
0x20	8	TimeStamp(FILETIME)	Event Time(UTC +0)
0x28	4	Reason Flag	The flag of change event
0x2C	4	Source Information	The subject that triggers change of event
0x30	4	Security ID	
0x34	4	File Attributes	The attribute information of the object effected by current event. Generally, it is used for classifying the object into a file or directory.
0x38	2	Size of Filename	The size of object name effected by current event
0x3A	2	Offset to Filename	The offset of object name within record
0x3C	N	Filename	The object(file or directory) name effected by current event

- The reason for using "Parent MFT Reference Number" instead of "MFT Reference Number"
 - ✓ If "MFT Reference Number" is used, full path information may not be obtained when relevant file is deleted.



Reason Flag (http://msdn.microsoft.com/en-us/library/aa365722.aspx)

Flag	Description
0x01	The file was overwritten.
0x02	The file or directory was added to
0x04	The file or directory was truncated.
0x10	The named data streams for a file is overwritten.
0x20	A named data streams for the file were added.
0x40	A named data streams for the file was truncated
0x100	The file or directory was created for the first time.
0x200	The file or directory was deleted.
0x400	The file's or directory's extended attributes were changed.
0x800	The access rights to the file or directory was changed.
0x1000	The file or directory was renamed.(previous name)
0x2000	The file or directory was renamed.(new name)
0x4000	A user changed the FILE_ATTRIBUTE_NOT_CONTENT_INDEXED attribute.
0x8000	A user has either changed one or more file or directory attributes or one or more time stamps.
0x10000	A hard link was added to or removed from the file or directory
0x20000	The compression state of the file or directory was changed from or to compressed.
0x40000	The file or directory was encrypted or decrypted.
0x80000	The object identifier of the file or directory was changed.
0x100000	The reparse point contained in the file or directory was changed, or a reparse point was added to or deleted from the file or directory.
0x200000	A named stream has been added to or removed from the file, or a named stream has been renamed.
0x8000000	The file or directory was closed.



Source Information (<u>http://msdn.microsoft.com/en-us/library/aa365722.aspx</u>)

Flag	Description
0x00	Normal Event
0x01	The operation provides information about a change to the file or directory made by the operating system
0x02	The operation adds a private data stream to a file or directory.
0x04	The operation creates or updates the contents of a replicated file.



File Attribute (<u>http://msdn.microsoft.com/en-us/library/gg258117.aspx</u>)

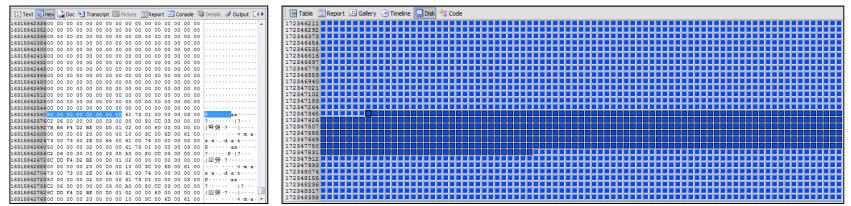
Value	Description
0x01	A file that is read-only.
0x02	The file or directory is hidden
0x04	A file or directory that the operating system uses a part of, or uses exclusively.
0x10	The handle that identifies a directory.
0x20	An archive file or directory.
0x40	This value is reserved for system use
0x80	A file that does not have other attributes set.
0x100	A file that is being used for temporary storage.
0x200	A file that is a sparse file.
0x400	A file or directory that has an associated reparse point, or a file that is a symbolic link.
0x800	A file or directory that is compressed.
0x1000	This attribute indicates that the file data is physically moved to offline storage.
0x2000	The file or directory is not to be indexed by the content indexing service.
0x4000	A file or directory that is encrypted.
0x8000	The directory or user data stream is configured with integrity (only supported on ReFS volumes).
0x10000	0 This value is reserved for system use.
0x20000	The user data stream not to be read by the background data integrity scanner (AKA scrubber).

\$UsnJrnl Record Carving

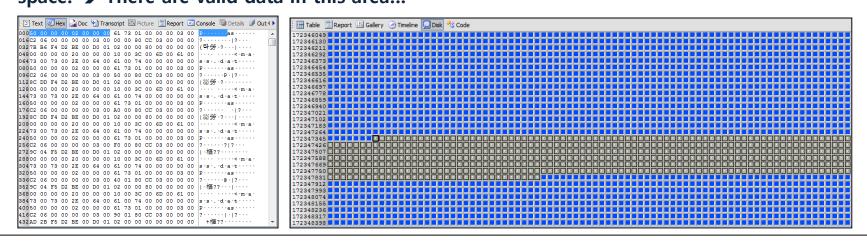
\$UsnJrnl Record Carving

\$UsnJrnl records in Unallocated Area

The location of first \$UsnJrnl record in disk : 172347352 sector



In a couple of hours... → the space which saves \$Usnjrnl record is changed to unallocated space. → There are valid data in this area...



forensicinsight.org

Existing Tool 1

- Carving function of USN Record in X-way forensics(Tool→Disk Tool→File Recovery by Type)
 - After record carving, the tool saves the records into many files.

File Header Search on Drive C:		이름	수정한 날짜	양유	크기
File type(s): Signatures	•	이름 000001.usnjrnl 000002.usnjrnl 000003.usnjrnl 000004.usnjrnl 000005.usnjrnl 000006.usnjrnl 000007.usnjrnl 000008.usnjrnl	수정한 날짜 2014-11-18 오후 2014-11-18 오후 2014-11-18 오후 2014-11-18 오후 2014-11-18 오후 2014-11-18 오후 2014-11-18 오후 2014-11-18 오후 2014-11-18 오후	USNJRNL 파일 USNJRNL 파일 USNJRNL 파일 USNJRNL 파일 USNJRNL 파일 USNJRNL 파일 USNJRNL 파일 USNJRNL 파일	∃7 512KB 512KB 56KB 528KB 556KB 452KB 128KB 748KB 372KB
····· Snapshot Prop (.snapprop) ···· Windows Prefetch (.pf) ···· Task Scheduler (.job) ···· SI Recycler (.recycler)		000010.usnjml 0000011.usnjml 000001.usnjml	2014-11-18 오후 2014-11-18 오후	USNJRNL 파일	512KB 12KB
Windows Shortcut (.lnk) [b] Windows Shortcut (.lnk) [b] Internet Shortcut (.url,ulk) Internet Shortcut (.url) Apple download cache (.waf) Change Log (.clog;log)		000001.usnjml 00000 D\Sample\TESTusnjml 00000 File size: 0.5 MB 00000 524.288 bytes 00000 DOS name: 000001~1.USN 00000	000 88 00 00 02 00 00 03 010 BD F3 02 00		.00 7÷ 100 ½6 -Ò 100 01 Đ 100 H<98 100 10b14aaf
Ubuntu Trash (trashinfo) KDE cache (kdecache) PList (XML) (plist)	E	Default Edit Mode 00000 State: original 00000 Undo level: 0 00000 Undo reverses: n/a 00000 Creation time: 2014-11-18 00000 16.45:56 00000	060 39 00 33 00 39 00 66 00 070 62 00 38 00 63 00 65 00 30 080 6D 00 70 00	33 00 33 00 35 00 61 39 00 30 00 2E 00 74 38 00 00 00 02 00 00 30 74 20 00 02 00 00 30 74 20 00 00 00 00 00 30 74 30 30 00 00 00 00 00 00 46 74 31 03 30 00	:00 b8ce90.t 00 mp I 00 7÷ ½6 01 I-Ò 01Đ
PList (binary) (bplist;plist) Plist (bplist;plist)		Last write time: 2014-11-18 00000 16:45:56 00000 Attributes: A 00000 Icons: 0 00000 00000	000 48 00 3C 00 39 00 38 00 30 0D0 34 00 61 00 66 00 6 00 6 00 6 00 6 00 6 00 6 00 6 00 6 00 6 00 6 00 6 00 6 00 0 00	31 00 30 00 62 00 31 52 00 36 00 65 00 38 39 00 33 00 39 00 66 52 00 38 00 63 00 65 52 00 38 00 63 00 65 50 00 70 00 00 00 00	. 00 H < 9 8 1 0 b 1 . 00 4 a a f b 6 e 8 . 00 4 2 b f 9 3 9 f . 00 c 3 5 a b 8 c e . 00 9 0 . t m p
Wirtual HD (.vhd) Wirtual HD (.vhd) Wirtual Disk (.vmdk) Macintosh Disk Image (.dmf;dmg)	-	Character set: ANSIASCII 00000 Offsets: hexadedmal 00000 Bytes per page: 47x16=752 00000 Window #: 1 00000 No. of windows: 1 00000	120 36 F7 02 00 00 01 00 130 12 4F 00 31 03 03 00 10 1 140 00 00 00 02 20 00 00 10 150 74 00 73 00 63 00 64 00 6C 00 6C 02 20 00 64	0 01 2D D2 03 00 00 3 A1 00 00 00 00 00 22 00 3C 00 61 00 64 55 00 6D 00 61 00 2E 50 00 75 00 69 00 00	00 " <ad 00 tschema. 00 dll.mui</ad
OK Cancel		Clipboard: available 00000 TEMP folder: 66.4 GB free 00000 >HJUNG~1\AppData\Local\Temp 00000 00000 00000 00000 00000	180 2A 91 02 00 00 00 0C 00 7 190 1E 4F 0D 31 03 3D 01 0 1A0 00 00 00 00 20 00 00 0	31 91 02 00 00 00 0A 70 01 2D D2 03 00 00 02 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 3C 00 73 00 63 73 00 64 00 00 00 00	100 ** p-Ò 100 01 Đ 100 <sc< th=""></sc<>



\$UsnJrnl Record Carving

Existing Tool 2

- FCNS_UsnJrnl EnScript
 - EnPack for Encase 7
 - There is no full path information of file or directory.
 - L01, CSV output

FCNS_UsnJrnl v1.0 (www.kazamiya.net)		이름		수정한 날짜	유형 크기					
Target	Other Ø \$UsnJrnl-\$J	FCNS_UsnJrnl_Data.L01		2014-11-18 오후	EnCase Logical Evidence Fi	ile		2,0	96,995KB	
Other	🕼 \$LogFile	FCNS_UsnJrnl_Data.L02		2014-11-18 오후 LO2 파일			19,570,272KB			
▼ pagefile.sys		ECNS_UsnJrnl_Records.	➡ FCNS_UsnJrnl_Records.csv 2014-11-18 오후 Microsoft Excel 쉼표로 구분된 값 파일 1,177,528KB							
	Unallocated Clusters	ItemPath	PS	SO TimeStamp	FileName	FileID	ParentID	Reason	Reason(String)	
-Filtering Option		C#Unallocated Clusters	0	0		1				
From:	To:	pnidevdolocsemfrmotblopoahshgupgua	6881385	655471 000a0030	ADS					
01/01/70 09:00:00 9		C₩Unallocated Clusters	3459424		3	162023		8000000		
01/01/70 09:00:00 3	2천 11/18/14 09:00:00 오전	CWUnallocated Clusters	3459426		5 5	141286		80000002		
Skip duplication	records (slow if it found many records)	CWUnallocated Clusters	3459426		5	39515			CREATE	
	,,	C₩Unallocated Clusters	3459427		3	124844			DATA	
Export		C₩Unallocated Clusters	3459427			39515			CREATE	
LEF File		C₩Unallocated Clusters	3459428		3	192015			B DATA	
C:\Users\ohiungho	on\Documents\EnCase\Cases\test\	C₩Unallocated Clusters	3459428			39515		80000200		
		C₩Unallocated Clusters	3459429			141286		8000000		
TSV File		CWUnallocated Clusters	3459429		3	124844		8000000		
C:\Users\ohjunghoon\Documents\EnCase\Cases\test\		CWUnallocated Clusters	3459430			141286		8000000		
		CWUnallocated Clusters	3459431	160 11/17/14 03:15:06 오루	agent.dbf-journal	39515	5 141611	10:	CREATE	
Integrate output records (TSV File)										
0	K Cancel									



Record Carving

Offset	Size	Stored Information	Detail
0x00	4	Size of Record	
0x04	2	Major Version	2(Change Journal Software's major version)
0x06	2	Minor Version	2(Change Journal Software's major version)
0x08	8	MFT Reference Number	"MFT Reference Number" of file or directory that effected by currently change event.
0x10	8	Parent MFT Reference Number	"MFT Reference Number" of parent directory of file and directory that effected by currently change event. The full path information can be obtained with this information and \$MFT.
0x18	8	USN	Update Sequence Number
0x20	8	TimeStamp(FILETIME)	Event Time(UTC +0)
0x28	4	Reason Flag	The flag of change event
0x2C	4	Source Information	The subject that triggers change of event
0x30	4	Security ID	
0x34	4	File Attributes	The attribute information of the object effected by current event. Generally, it is used for classifying the object into a file or directory.
0x38	2	Size of Filename	The size of object name effected by current event
0x3A	2	Offset to Filename	The offset of object name within record
0x3C	Ν	Filename	The object(file or directory) name effected by current event

- Signature : ₩x??₩x??₩x00₩x00₩x02₩x00₩x00₩x00
- Sub-checking Point : USN, TimeStamp, Source Information, Size/Offset of Filename





The Result of Record Carving

System	The size of Unallocated Area	The number of recovered records(De-Duplication)	The period of recovered records
A(Win7 64bit)	72G(HDD)	32,379,635	2014-02-10 ~ 2014-11-03
B(Win7 64bit)	120G(HDD)	36,650,278	2014-01-28 ~ 2014-11-10
C(Win7 64bit)	269G(HDD)	24,907,010	2014-01-28 ~ 2014-11-13
D(Win7 64bit)	120G(HDD)	22,310,563	2013-10-27 ~ 2014-12-23

• There are about 30,000,000 records in unallocated space.

- There are some records before 10~11 months.
- Generally, there are 300,000 records in \$UsnJrnl:\$J on average.
- There are some records before formatting current system.



NTFS Log Tracker v1.4

Updated List (<u>https://sites.google.com/site/forensicnote/ntfs-log-tracker</u>)

1. \$UsnJrnl record carving from unallocated space

- Carving result is printed out by page unit. (500,000 records by one page)
- The full path information is printed out. (from \$MFT)
- Indexing page information(In case of more than 3 pages)
 - ✓ After ordering by USN, first and last record's time information are recorded.

\$LogFile \$UsnJrnl:\$] \$LogFile(Search Result) \$UsnJrnl:\$](Search Result)						
	Page : (1 / 65)	Peroid : 2014-10-20 21:25:43 ~ 2014-02-20 22:24	÷01	5 Page : 2014-04-16 10:37:40 ~ 2014-04-21 18:40:41	•	
TimeStamp	USN	File Name	Full Path(from	6 Page : 2014-04-21 18:40:41 ~ 2014-04-24 14:35:53		
2014-04-08 22:08:41 2014-04-08 22:08:41 2014-04-08 22:08:41 2014-04-08 22:08:41 2014-04-08 22:08:41 2014-04-08 22:08:41 2014-04-08 22:08:41 2014-04-08 22:08:41 2013-10-24 10:15:52 2013-10-24 10:15:52 2013-11-01 10:48:47 2013-11-01 10:48:47 2013-12-02 17:32:33 2013-12-13 10:16:43 2013-12-13 10:16:43 2013-12-13 10:16:43 2013-12-13 10:16:43 2013-10-10 10:04:28 2014-01-16 10:27:33 2014-01-16 10:27:33	1802751288 1802751376 1802751376 1802751552 180275152 1802751728 1802751904 1910371648 1910371648 1910371728 2191398504 2191398504 2191398504 2191398800 2953309496 3268405920 4588088264 4816802896 4816803296	0001000F.wid sbshield.log sbshield.log sbshield.log sbshield.log sbshield.log sbshield.log sbshield.log sbshield.log sbshield.log Report.wer NonCritical_7.5.7601.17514_33fee1c1607943搭e4 NonCritical_7.5.7601.17514_33fee1c1607943搭e4 NonCritical_7.5.7601.17514_33fee1c16079435e41 Report.wer Report.wer TMP0000004C331406EEFB995D2E mass.dat mass.dat Report.wer.tmp NonCritical_80072ee4_6c3d89d03e7a5a22ed7994 Report.wer	₩ProgramDat ₩ProgramDat ₩Windows₩T ₩ProgramDat	7 Page: 2014-04-24 14:35:53 2014-04-24 21:42:59 8 Page: 2014-04-24 21:42:59 2014-05-04 12:19:08 9 Page: 2014-05-04 12:19:08 2014-05-05 10:21:9:11 11 Page: 2014-05-05 10:11:28 2014-05-05 10:21:9:14 11 Page: 2014-05-05 10:11:28 2014-05-06 10:10:128 11 Page: 2014-05-06 10:10:128 2014-05-06 10:12:47 13 Page: 2014-05-06 09:02:46 2014-05-06 10:12:47 13 Page: 2014-05-06 09:02:46 2014-05-06 16:35:25 15 Page: 2014-05-06 16:35:25 2014-05-16 16:35:25 15 Page: 2014-05-16 16:35:25 2014-05-23 18:24:21 17 Page: 2014-05-15 12:27:28 2014-05-23 18:24:21 19 Page: 2014-05-23 18:24:21 2014-05-23 18:24:21 21 Page: 2014-05-24 11:24:51 22 Page:	≡ 16 16	
2014-01-29 10:15:02	5415903688	AmAgent.log	WProgram File	34 Page : 2014-07-31 13:29:50 ~ 2014-07-31 13:25:50	Ψ.	

- 2. Supporting source file extracted by "ExtractUsnJrnl" tool
- 3. Changing interface of keyword search
- 4. Supporting Korean keyword search
- 5. Tab bug is fixed.

NTFS Log Tracker v1.4

User interface

Parsine File SLogFile File Path Submits 1 File Path Unable acted Dump Path Opening SQLte DB File	🐼 NTFS Log Tracker v1.4	
Summits File Path Parsing Source File for Parsing Summits File Path Parsing SMFT for SMFT File Path Opening SQLte DB File SMFT for SQLte DB File SQLte DB File Opening SQLte DB File SMFT for SQLte DB File Opening SQLte DB File SMFT for SQLte DB File Path Opening SQLte DB File Opening DB file Search Keyword Search CSV Export Exporting CSV format StogFile Susnimts3 StogFile(Search Result) Event Time Event Time Parsed Data Output		
Unallocated Dump Path (for \$UsnJm(Carving)) Ontion \$MFT File Path Opening SQLite DB File SQLite DB File Path Search Keyword Search StogFile (Susnim:\$3) \$LogFile(Search Result) CSV Export Exporting CSV format Exporting CSV format	él len Irel-él Eile Dath	Source File for Parsing
Obtion \$MFT File Path SMFT for Full Path Construction Opening SQLte DB File Opening DB file Opening DB file SQLte DB File Path Open Opening DB file Opening DB file SQLte DB File Path Open Exporting CSV format StogFile \$UspTime Event Detail File Name File Name Image: I	Unallocated Dump Path :	
Opening SQLite DB File SQLite DB File Path Search Keyword Search		
SQLite DB File Path Open Opening DB file created by this tool Search CSV Export Exporting CSV format \$LogFile \$UsnJml:\$1 \$LogFile(Search Result) \$UsnJml:\$1(Search Result) Exporting CSV format V Page : Image: The Name Image: The Name Image: Im	\$MFT File Path :	
SQLite DB File Path Open created by this tool Search Keyword Search Search Keyword Search CSV Export StogFile \$UsnJml:\$3] \$LogFile(Search Result) \$UsnJml:\$3(Search Result) <	Opening SQLite DB File	Opening DB file
SV Export \$LogFile \$UsnJml:\$3 \$LogFile(Search Result) \$UsnJml:\$3(Search Result) Image: IsN Event Time Page: Page: Page: Parsed Data Output	SQLite DB File Path : Open	
\$LogFile \$UsnJml:\$3 \$LogFile(Search Result) \$UsnJml:\$3(Search Result) <	Search Keyword Search	Exporting CSV format
LSN Event Time Event Detail File Name		
LSN Event Time Event Detail File Name Parsed Data Output	< > Page :	
		Parsed Data Output
Croated by Jungheen Ob(bluespeel 275@gmail.com)	٠	
Created by Sunghoon On(Dideangeriz/Sugmail.com)	Created by Junghoon Oh(blueangel1275@gmail.com)	



NTFS Log Tracker v1.4



Keyword Search

Search	\$LogFile \$UsnJrnl:\$3	\$LogFile(Search	Result) \$UsnJrnl:\$J(Search Result)		
\$LogFile		Page : (1/1)	Peroid : 2014-04-08 22:08:41 ~ 2014-11	-03 19:47:12	
LSN :	TimeStamp	USN	FileName	Full Path(from \$MFT)	Event
	2014-10-27 14:05:03	15264548896	USERINIT.EXE-2257A3E7.pf	₩Windows₩Prefetch₩USERINIT.EXE-2257A3E7.pf	File_Created, File_Added
Event Time :	2014-10-27 14:05:03	3 15264549096	USERINIT.EXE-2257A3E7.pf	₩Windows₩Prefetch₩USERINIT.EXE-2257A3E7.pf	File_Created, File_Added, File_Closed
	2014-10-27 14:05:03	3 15264549400	DWM.EXE-6FFD3DA8.pf	₩Windows₩Prefetch₩DWM.EXE-6FFD3DA8.pf	File_Created
File Name :	2014-10-27 14:05:03	15264549504	DWM.EXE-6FFD3DA8.pf	₩Windows₩Prefetch₩DWM.EXE-6FFD3DA8.pf	File_Created, File_Added
	2014-10-27 14:05:03	15264549608	DWM.EXE-6FFD3DA8.pf	₩Windows₩Prefetch₩DWM.EXE-6FFD3DA8.pf	File_Created, File_Added, File_Closed
Full Path :	2014-10-27 14:05:03	15264550912	IMAGESAFERSTART_X86.EXE-5D5364FB.pf	WWindowsWPrefetchWIMAGESAFERSTART_X86.EXE-5D5364FB.pf	File_Truncated
	2014-10-27 14:05:03	3 15264551048	IMAGESAFERSTART_X86.EXE-5D5364FB.pf	WWindowsWPrefetchWIMAGESAFERSTART_X86.EXE-5D5364FB.pf	File_Added, File_Truncated
	2014-10-27 14:05:03	3 15264551272	IMAGESAFERSTART_X86.EXE-5D5364FB.pf	WWindowsWPrefetchWIMAGESAFERSTART_X86.EXE-5D5364FB.pf	File_Added, File_Truncated, File_Clos
ŚUsnJrnl	2014-10-27 14:05:03	3 15264551408	IMAGESAFERSTART_X64.EXE-6BC30D77.pf	WWindowsWPrefetchWIMAGESAFERSTART_X64.EXE-6BC30D77.pf	File_Truncated
	2014-10-27 14:05:03	3 15264551544	IMAGESAFERSTART_X64.EXE-6BC30D77.pf	WindowsWPrefetchWIMAGESAFERSTART_X64.EXE-6BC30D77.pf	File_Added, File_Truncated
TimeStamp : 2014-10-27	2014-10-27 14:05:03	3 15264551680	IMAGESAFERSTART_X64.EXE-6BC30D77.pf	WindowsWPrefetchWIMAGESAFERSTART_X64.EXE-6BC30D77.pf	File_Added, File_Truncated, File_Clo
Theodemp : Los : to s.	2014-10-27 14:05:05	15264560024	RUNDLL32.EXE-DE9673F9.pf	WindowsWPrefetchWRUNDLL32.EXE-DE9673F9.pf	File_Created
USN :	2014-10-27 14:05:05	15264560136	RUNDLL32.EXE-DE9673F9.pf	WindowsWPrefetchWRUNDLL32.EXE-DE9673F9.pf	File_Created, File_Added
0.514	2014-10-27 14:05:05	15264560248	RUNDLL32.EXE-DE9673F9.pf	WindowsWPrefetchWRUNDLL32.EXE-DE9673F9.pf	File_Created, File_Added, File_Close
File Name : .pf	2014-10-27 14:05:05	15264560552	EXPLORER.EXE-A80E4F97.pf	WindowsWPrefetchWEXPLORER.EXE-A80E4F97.pf	File_Truncated
rie Namepr	2014-10-27 14:05:05	15264560664	EXPLORER.EXE-A80E4F97.pf	₩Windows₩Prefetch₩EXPLORER.EXE-A80E4F97.pf	File_Added, File_Truncated
	2014-10-27 14:05:05	15264560776	EXPLORER.EXE-A80E4F97.pf	₩Windows₩Prefetch₩EXPLORER.EXE-A80E4F97.pf	File_Added, File_Truncated, File_Clo
Full Path :	2014-10-27 14:05:08	15264572984	DLLHOST.EXE-5E46FA0D.pf	₩Windows₩Prefetch₩DLLHOST.EXE-5E46FA0D.pf	File_Truncated
	2014-10-27 14:05:08	15264573096	DLLHOST.EXE-5E46FA0D.pf	₩Windows₩Prefetch₩DLLHOST.EXE-5E46FA0D.pf	File_Added, File_Truncated
	2014-10-27 14:05:08	15264573208	DLLHOST.EXE-5E46FA0D.pf	₩Windows₩Prefetch₩DLLHOST.EXE-5E46FA0D.pf	File_Added, File_Truncated, File_Clos
G	Cancel 2014-10-27 14:05:14	15264629496	CONSENT.EXE-531BD9EA.pf	₩Windows₩Prefetch₩CONSENT.EXE-531BD9EA.pf	File_Created
	2014-10-27 14:05:14	15264629608	CONSENT.EXE-531BD9EA.pf	₩Windows₩Prefetch₩CONSENT.EXE-531BD9EA.pf	File_Created, File_Added
	2014-10-27 14:05:14	15264629720	CONSENT.EXE-531BD9EA.pf	WWindows WPrefetch WCONSENT. EXE-531BD9EA.pf	File_Created, File_Added, File_Closed

- Target field of keyword search
 - ✓ \$LogFile : LSN, Event Time, File Name, Full Path
 - ✓ \$UsnJrnl : TimeStamp, USN, File Name, Full Path
- Using LIKE operation of SQL
- If multi-keyword are entered, the keywords are used by "AND" operation.

Conclusion

Conclusion

Tracking NTFS's history with \$UsnJrnl

- Creation, deletion, modification, renaming and moving of file and directory
- It is possible to find trace of deleted file.
- The event of program execution and opening document can be found through tracking prefetch file and LNK file's history.

Collection of \$UsnJrnl:\$J

- Encase or Winhex
- ExtractUsnJrnl

\$UsnJrnl record carving from unallocated space

- There are mass \$UsnJrnl records in unallocated space.
- Tracking old file system history(before several months) through \$UsnJrnl record carving



