



NTNU

# Using the object ID index as an investigative approach for NTFS file systems

Rune Nordvik, NTNU/PHS

Fergus Toolan, PHS

Stefan Axelsson, NTNU/Halmstad University

# Connect hard disk to computer(s)



78:AC:C0:41:8C:DE



81:EF:CC:59:EA:A6



5E:9D:F5:E8:BA:63

## Seized external device

NTFS



No OS

- To which computer(s) has this external hard disk been attached?
- Can we document any user activity?



FD:04:5C:E1:9F:C2



08:00:27:4D:5D:2C

# The system file \$ObjId

Type	Important	Remarks
Object ID	Boot time, sequence, MAC address, etc	Could change
Birth Volume Object ID	CrossVolumeMoveFlag	Should not change
Birth Object ID	Boot time, sequence, MAC address, etc	Should not change
Domain ID	Reserved	Should be zeros
MFT record reference	Connect \$ObjId entry to \$MFT record entry	

# Object ID: Manual interpretation

- **7783f50bb0cbe81197dd0800270e1302**

Boot time:

0x01e8cbb00bf58377 - 0x146BF33E42C000

= 0x1D45FBCCDB2C377 = Tue, 09 Oct 2018 10:42:41 UTC

**Object Id order:**

0x8377 = 33655

**Version:**

0x01

**Variant:**

**Bits** 1001<sub>b</sub> = 10<sub>b</sub> =

The type specified in RFC4122

**Clock Sequence:**

0x17DD (BE) = 6109




MAC addr.: 08-00-27-0e-13-02


1000<sub>b</sub> = Lsb of first byte = 0,  
means Unicast address






NTNU

EnCase 8.02

Permissions  Hash Sets  Attributes Lock 

Browse Data 

	Name	Value
<input type="checkbox"/> 1 	Own Id	{0BF58377-CBB0-11E8-97DD-0800270E1302} (Sequence:17DD Timestamp: 09/10/18 10:42:41 MAC:08-00-27-0E-13-02 )
<input type="checkbox"/> 2 	Birth Volume Id	{090C1215-8FA0-4614-9880-9DF0A2993C1F}
<input type="checkbox"/> 3 	Birth Object Id	{0BF58377-CBB0-11E8-97DD-0800270E1302} (Sequence:17DD Timestamp: 09/10/18 10:42:41 MAC:08-00-27-0E-13-02 )

- ✓ Sequence: 0x17DD = 6109
- ✓ Timestamp: 09/10/18 10:42:41 UTC
- ✓ MAC address: 08-00-27-0E-13-02
- ✗ Object ID order not shown
- ✗ Do not describe what the timestamp mean
- ✗ Own Id should be Object Id
- ✗ Do not detect CrossVolumeMoveFlag
- ✗ Do not describe where OIDs were found

## NTFSObjectIDParser 0.1-2

MFT Record	Byte Offset	Attribute or Type	MFT Header Flags	Volume Action	Name	Created	dif	M	es	MAC Address	ObjectID Order	Clock Sequence
38	ObjectID\$O ...	ObjectID	0		7783f50bb0cbe81197dd0800270e1302	Tue Oct 9 10:42:41 2018				08-00-27-0e-13-02	33655	6109
38	ObjectID\$O ...	BirthVolumeID	0	Moved to volume	15120c09a08f144698809df0a2993c1f							
38	ObjectID\$O ...	BirthObjectID	0		7783f50bb0cbe81197dd0800270e1302	Tue Oct 9 10:42:41 2018				08-00-27-0e-13-02	33655	6109
38	ObjectID\$O ...	DomainObj...	0		00000000000000000000000000000000							
38	MFT offset =...	SIA	Allocated File			Tue Oct 9 19:56:04 2018						
38	MFT offset =...	FNA	Allocated File		\\test2.rtf	Tue Oct 9 19:56:40 2018						
38	MFT offset =...	OIA	Allocated File		7783f50bb0cbe81197dd0800270e1302	Tue Oct 9 10:42:41 2018				08-00-27-0e-13-02	33655	6109



# Object ID

{0BF58377-CBB0-11E8-97DD-0800270E1302}  
Timestamp: 10/09/2018 12:42:41 +2, Seq: 6109  
MAC Address: 08 00 27 0E 13 02

- ✓ Sequence: 6109

✓ Timestamp: 09/10/18 12:42:41 +2

✓ MAC address: 08-00-27-0E-13-02
- ✗ Object ID order not shown

✗ Do not describe what the timestamp mean

✗ Do not detect CrossVolumeMoveFlag

✗ Do not describe where OIDs were found

✗ Miss the Birth Volume ID or Birth Object ID

## NTFSObjectIDParser 0.1-2

MFT Record	Byte Offset	Attribute or Type	MFT Header Flags	Volume Action	Name	Created	dif	M	es	MAC Address	ObjectID Order	Clock Sequence
38	ObjectID\$O ...	ObjectID	0		7783f50bb0cbe81197dd0800270e1302	Tue Oct 9 10:42:41 2018				08-00-27-0e-13-02	33655	6109
38	ObjectID\$O ...	BirthVolumeID	0	Moved to volume	15120c09a08f144698809df0a2993c1f							
38	ObjectID\$O ...	BirthObjectID	0		7783f50bb0cbe81197dd0800270e1302	Tue Oct 9 10:42:41 2018				08-00-27-0e-13-02	33655	6109
38	ObjectID\$O ...	DomainObj...	0		00000000000000000000000000000000							
38	MFT offset =...	SIA	Allocated File			Tue Oct 9 19:56:04 2018						
38	MFT offset =...	FNA	Allocated File		\\test2.rtf	Tue Oct 9 19:56:40 2018						
38	MFT offset =...	OIA	Allocated File		7783f50bb0cbe81197dd0800270e1302	Tue Oct 9 10:42:41 2018				08-00-27-0e-13-02	33655	6109

# Extracting \$ObjId index

```
Runes-iMac:NTFS runenordvik$ fls -o 65664 mount/ewf1 11
r/r 25-144-5: $ObjId:$0
r/r 24-144-3: $Quota:$0
r/r 24-144-2: $Quota:$Q
r/r 26-144-2: $Reparse:$R
d/d 27-144-2: $RmMetadata
r/r 39-128-3: $UsnJrnl:$J
r/r 39-128-4: $UsnJrnl:$Max
Runes-iMac:NTFS runenordvik$ icat -o 65664 mount/ewf1 25-160 > ObjectID-IA.bin
Runes-iMac:NTFS runenordvik$ icat -o 65664 mount/ewf1 25-144 > ObjectID-IR.bin
Runes-iMac:NTFS runenordvik$ icat -o 65664 mount/ewf1 0 > MFT.bin
```

Less than 7 Object ID entries:

Attribute not found in file (tsk\_fs\_attrlist\_get: Attribute 160 not found)

# \$ObjId – Index Allocation

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
006400h	46	49	4C	45	30	00	03	00	08	1C	22	00	00	00	00	00	FILE0
006410h	01	00	01	00	38	00	0D	00	D8	01	00	00	00	04	00	00	8
006420h	00	00	00	00	00	00	00	00	06	00	00	00	19	00	00	00	
006430h	06	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	
006440h	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	
006450h	67	E5	87	27	D8	5F	D4	01	67	E5	87	27	D8	5F	D4	01	gagc' + Logagc' + L
006460h	67	E5	87	27	D8	5F	D4	01	67	E5	87	27	D8	5F	D4	01	gagc' + L Logagc' + L
006470h	26	00	00	20	00	00	00	00	00	00	00	00	00	00	00	00	
006480h	00	00	00	00	01	01	00	00	00	00	00	00	00	00	00	00	
006490h	00	00	00	00	00	00	00	00	30	00	00	00	68	00	00	00	
0064A0h	00	00	00	00	00	00	01	00	4E	00	00	00	18	00	01	00	
0064B0h	0B	00	00	00	00	00	0B	00	67	E5	87	27	D8	5F	D4	01	
0064C0h	67	E5	87	27	D8	5F	D4	01	67	E5	87	27	D8	5F	D4	01	gagc' + L Logagc' + L
0064D0h	67	E5	87	27	D8	5F	D4	01	00	00	00	00	00	00	00	00	gagc' + L
0064E0h	00	00	00	00	00	00	00	00	26	00	00	20	00	00	00	00	
0064F0h	06	00	24	00	4F	00	62	00	6A	00	49	00	64	00	00	00	
006500h	90	00	00	00	58	00	00	00	00	02	18	00	00	00	05	00	E X \$ O t *
006510h	38	00	00	00	20	00	00	00	24	00	4F	00	00	00	00	00	8 \$ O
006520h	00	00	00	00	13	00	00	00	00	10	00	00	01	00	00	00	!! > @
006530h	10	00	00	00	28	00	00	00	28	00	00	00	01	00	00	00	> ( ( @
006540h	00	00	00	00	00	00	00	00	18	00	00	00	03	00	00	00	> ↑ @
006550h	00	00	00	00	00	00	00	00	A0	00	00	00	50	00	00	00	↑ a P
006560h	01	02	40	00	00	00	03	00	00	00	00	00	00	00	00	00	@ @ @
006570h	00	00	00	00	00	00	00	00	48	00	00	00	00	00	00	00	H
006580h	00	10	00	00	00	00	00	00	00	10	00	00	00	00	00	00	> >
006590h	00	10	00	00	00	00	00	00	24	00	4F	00	00	00	00	00	> \$ O
0065A0h	31	01	0E	43	01	00	00	00	B0	00	00	00	28	00	00	00	leapce (
0065B0h	00	02	18	00	00	00	04	00	08	00	00	00	20	00	00	00	↑ ♦ □
0065C0h	24	00	4F	00	56	D6	02	4C	01	00	00	00	00	00	00	00	\$ O V L

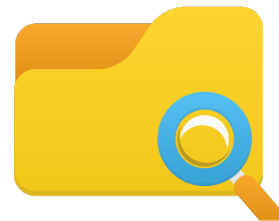
- 0x0: 4 bytes: 0xA0 (Attribute type)
- 0x4: 4 bytes: 0x50 (Size of Attribute)
- 0x8: 1 byte: 0x01 (Non-Resident flag)
- 0x9: 1 byte: 0x02 (Size of name in Unicode chars)
- 0xA: 2 bytes: 0x40 (Offset to name)
- 0xC: 2 bytes: 0x00 (Flags)
- 0xE: 2 bytes: 0x03 (Attribute ID)
- 
- 0x10: 8 bytes: 0x00 (Starting VCN)
- 0x18: 8 bytes: 0x00 (Ending VCN)
- 0x20: 2 bytes: 0x48 (Offset to run list)
- 0x22: 2 bytes: 0x00 (Compression)
- 0x24: 4 bytes: 0x00 (Unused)
- 0x28: 8 bytes: 0x1000 (Allocated size)
- 0x30: 8 bytes: 0x1000 (Actual Size)
- 0x38: 8 bytes: 0x1000 (Initial Size)
- 0x40: 4 bytes: \$0 (Attribute name)
- 0x44: 4 bytes: 0x00 (padding)
- 0x48: 8 bytes: 0x31010E4301 (Data run)



# Experiments - User activity

- We performed experiments to document what kind of user activity creates or modifies Object IDs
- Sample: W7 (ver 6.1.7601) / W10 (ver 10.0.17134):
  - File Explorer and LibreOffice 5.2
  - CMD prompt, Notepad and VeraCrypt 1.23

# Results - File Explorer



OS	Impact	Exist OIDs	Pre- served	New target OIDs	Operation
W10	OID, BOID, BVOID	NO	N/A	YES*	File New (File or Directory) <b>* If \$Volume OID=0 ==&gt; BVOID is 0.</b>
W7/W10	OID, BOID, BVOID	NO YES	N/A YES*	YES* NO	Open using double click <b>* If \$Volume OID=0 ==&gt; BVOID is 0.</b>
W7/W10	OID, BOID, BVOID	NO YES	N/A NO	NO NO	Ctrl+Drag and drop within same/ other volume
W7/W10	OID, BOID, BVOID	NO YES	N/A YES	NO NO	Shift+Drag and drop to same volume
W7/W10	OID, BOID, BVOID	NO YES	N/A YES*	NO BVOID Lsb=1	Shift+Drag and drop to other volume <b>* If target \$Volume OID=0 =&gt; new set of OIDs, and BVOID is 0.</b>
W7/10	OID, BOID, BVOID	YES	NO	NO	Delete

# Results – LibreOffice 5.2



OS	Impact	Exist OIDs	Pre- served	New target OIDs	Operation
W7/W10	OID, BOID, BVOID	NO	N/A	YES	File New * If \$Volume OID=0 ==> BVOID is 0.
W7/W10	OID, BOID, BVOID	NO YES	N/A YES	YES NO	File Open * If \$Volume OID=0 ==> BVOID is 0.
W7/W10	OID, BOID, BVOID	NO YES	N/A NO	YES YES	Copy a file using File Save As to same/other volume * If \$Volume OID=0 ==> BVOID is 0.

Moving or deleting is not applicable in LibreOffice

# Results – VeraCrypt 1.23



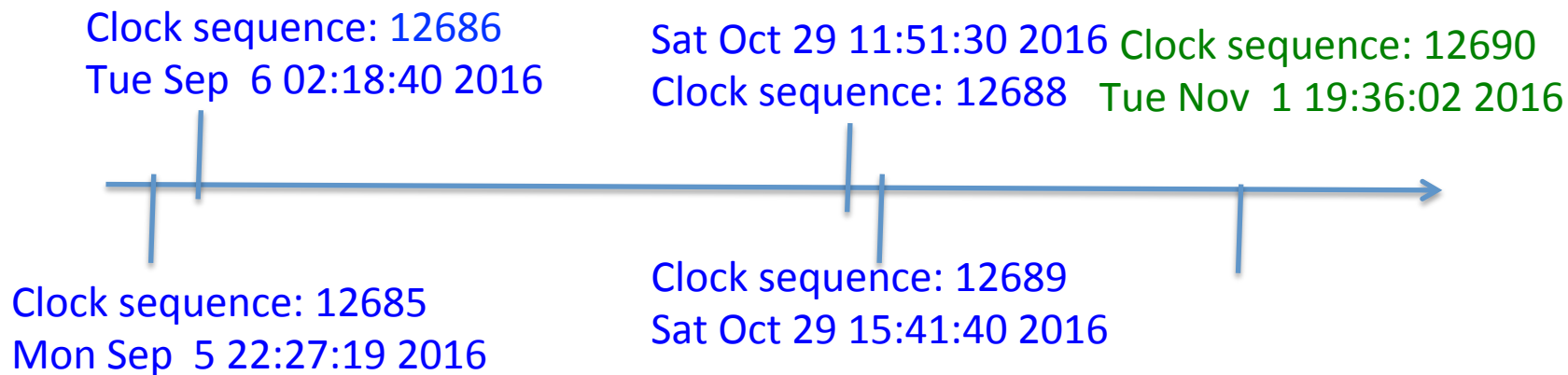
OS	Impact	Exist OIDs	Pre- served	New target OIDs	Operation
W7/W10	OID, BOID, BVOID	NO	N/A	NO	File New (Create a new container)
W7/W10	OID, BOID, BVOID	NO YES	N/A YES	NO NO	File Open (Select File and mount, then dismount)

Copying, Moving or deleting is not applicable in VeraCrypt

# Timeline creation

MAC Addr: 78-ac-c0-41-8c-de

MAC Addr: 08-00-27-4d-5d-2c



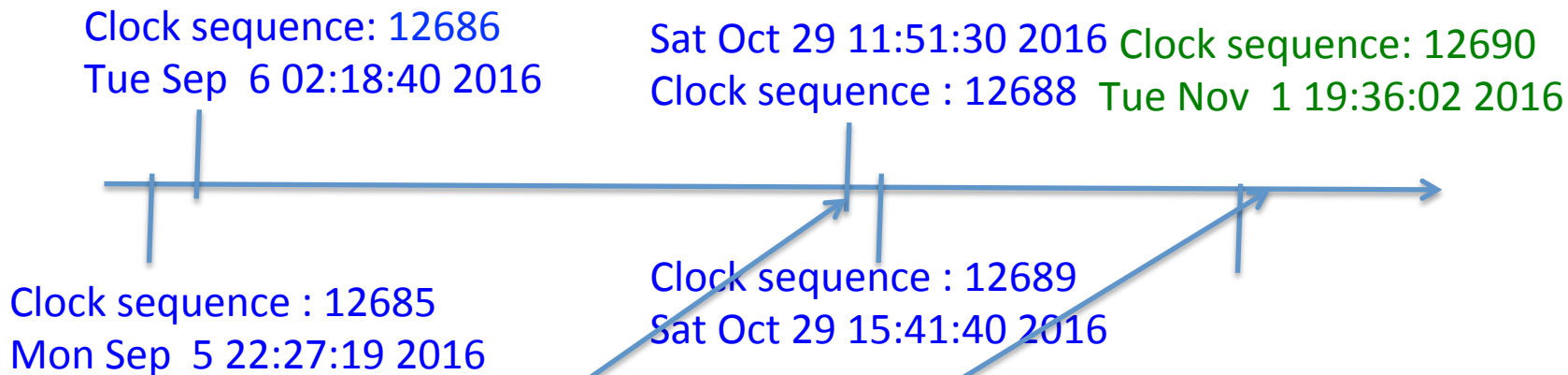
The computer with MAC **78-ac-c0-41-8c-de** had been booted at least 4 times

All entries had BVOID: 467715a14727d1428769d8eef6d3fde4

# Manipulation

MAC Addr: 78-ac-c0-41-8c-de

MAC Addr: 08-00-27-4d-5d-2c



**Manipulated.docx:** File Created: Nov 1 19:40:05 2016, connected Object ID say Oct 29 11:51:30 2016. Clock Sequence is 12688.  
 CrossVolumeMoveFlag=0 and Birth Volume Object ID != 0

# Triage Tool

- Use the \$ObjId \$O index as a triage tool to find all allocated files that have an Object ID entry.
- Specially good approach for LibreOffice documents, or where the user uses File Explorer to open documents
- Word (2007) or Excel (2007) generates Object IDs on file creation, but not when exporting to PDF (Parsonage 2008).

# Limitations

- MAC addresses can be modified by user
- Not all user activity creates Object IDs
- We have experimented using a few applications
- We have only tested using specific versions of Windows 7 and Windows 10



# Questions?