

MetaData Spoofing

By Blazer Catzen

Research by
Blazer Catzen
and
Greg Dominguez

Goals

- Understanding MS Office (2010) internal metadata
 - User editable and how
 - Effect of edits (hash)
 - Failure to Update (reliability?)
 - Internal structure
- Internal metadata updates ?
 - Cross application file compatibility
 - Print
 - Word Count
- Understand the “spoof”
 - Educated user to IT Professional
- Detection of Spoofing

MS Office Word 2010 in Windows 7

Philip Blazer CatzenCV.docx Properties

General Security Details Previous Versions

Property	Value
Description	
Title	
Subject	Specify the subject
Tags	Add a tag
Categories	
Comments	
Origin	
Authors	Your User Name
Last saved by	Your User Name
Revision number	7
Version number	
Program name	Microsoft Office Word
Company	Catzen Computer Consulting
Manager	
Content created	7/8/2011 11:40 AM
Date last saved	10/27/2011 10:23 AM
Last printed	8/30/2011 12:25 PM
Total editing time	00:30:00

[Remove Properties and Personal Information](#)

OK Cancel Apply

Editable

Philip Blazer CatzenCV.docx Properties

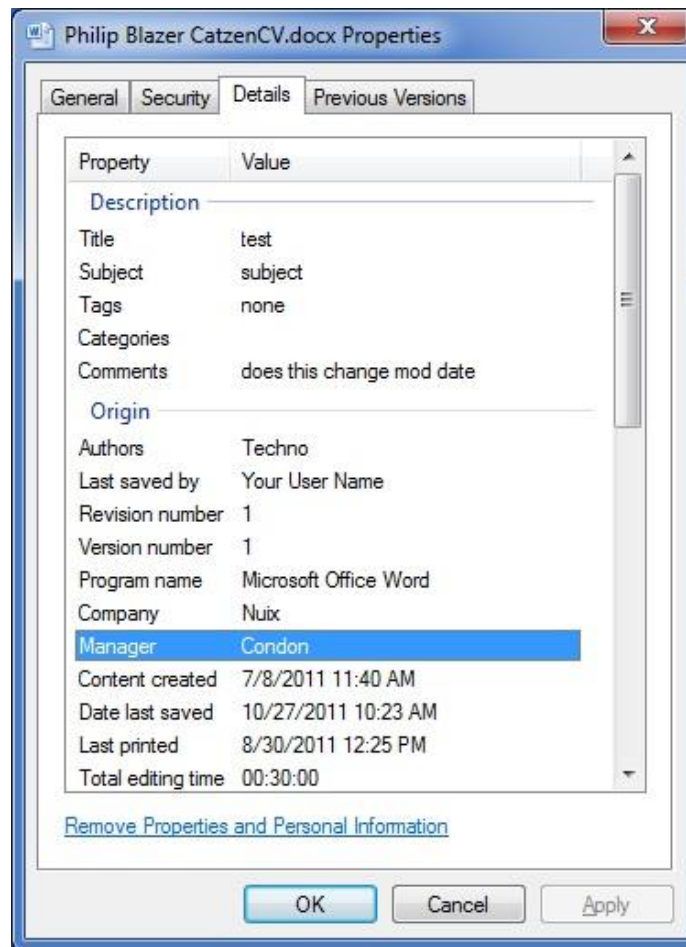
General Security Details Previous Versions

Property	Value
Content	
Content status	
Content type	
Pages	3
Word count	636
Character count	3629
Line count	30
Paragraph count	8
Template	CatzenForensicLetterHead.dot
Scale	No
Links dirty?	No
Language	
File	
Size	26.3 KB
Date created	2/6/2014 1:15 PM
Date modified	10/27/2011 10:23 AM
Date accessed	2/6/2014 1:15 PM
Offline availability	

[Remove Properties and Personal Information](#)

OK Cancel Apply

Post Edit



After Close and Re-Open

- Note FS – Modified changed
- Content Did not
 - Files MD5 Changed

File	
Size	26.3 KB
Date created	2/6/2014 1:15 PM
Date modified	5/29/2014 8:54 AM
Date accessed	2/6/2014 1:15 PM
Offline availability	
Offline status	
Shared with	
Computer	FORENSIC4 (this computer)

Content created	7/8/2011 11:40 AM
Date last saved	10/27/2011 10:23 AM
Last printed	8/30/2011 12:25 PM
Total editing time	00:30:00

Full Word metadata listing

Properties ▾

Size	26.3KB
Pages	3
Words	568
Total Editing Time	30 Minutes
Title	test
Tags	none
Comments	does this change mod date
Template	CatzenForensicLetterHead.dot
Status	Add text
Categories	Add a category
Subject	subject
Hyperlink Base	Add text
Company	Nuix

Related Dates

Last Modified	10/27/2011 10:23 AM
Created	7/8/2011 11:40 AM
Last Printed	8/30/2011 12:25 PM

Related People

Manager	Condon Specify the manager
Author	Techno Add an author
Last Modified By	Your User Name

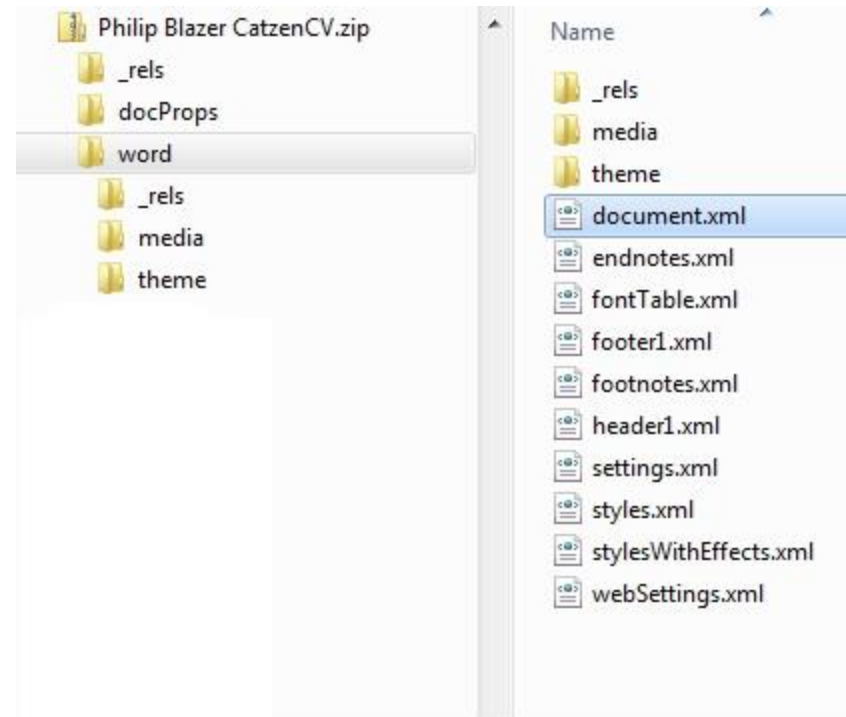
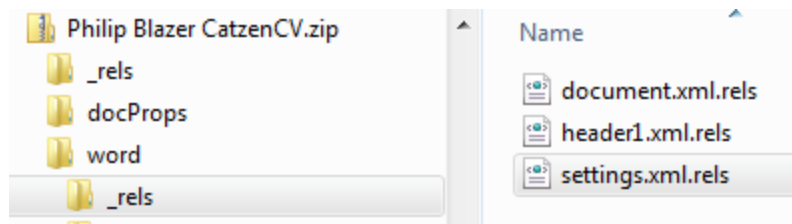
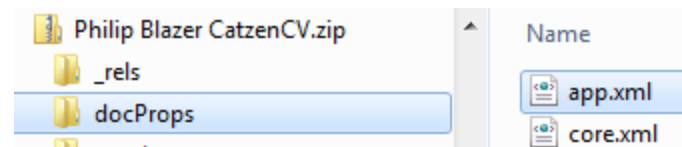
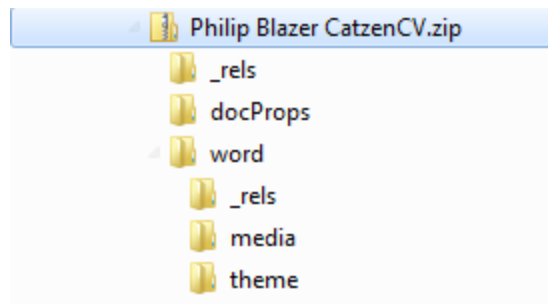
Related Documents

 [Open File Location](#)

[Show Fewer Properties](#)

Component parts

- Internal structure



Metadata location

- Core.xml
 - Title
 - Subject
 - Creator (Author)
 - Tag
 - Comment
 - Last modification by
 - Revisions
 - Dates (GMT)
 - Created
 - Modified
 - Category
 - Status

Metadata location

- App.xml -notable
 - Template name
 - Total time (accuracy?)
 - Words (not always accurate)
 - Characters (includes CRLF)
 - Characters with spaces
 - Version

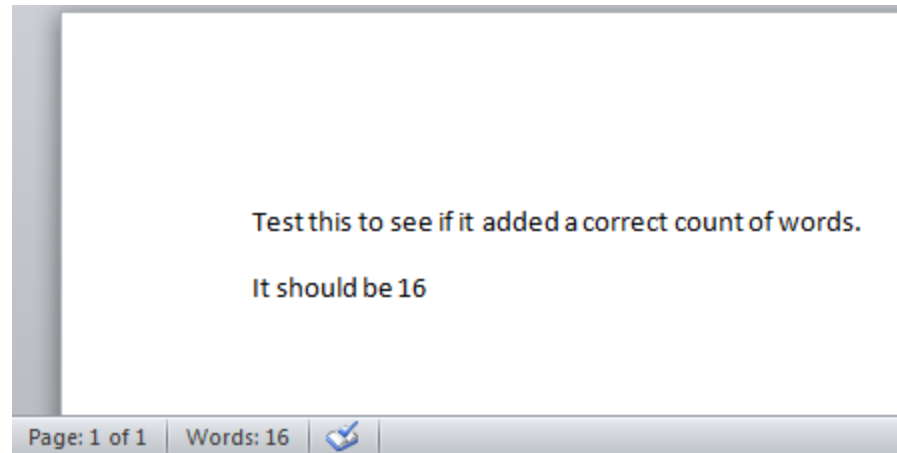
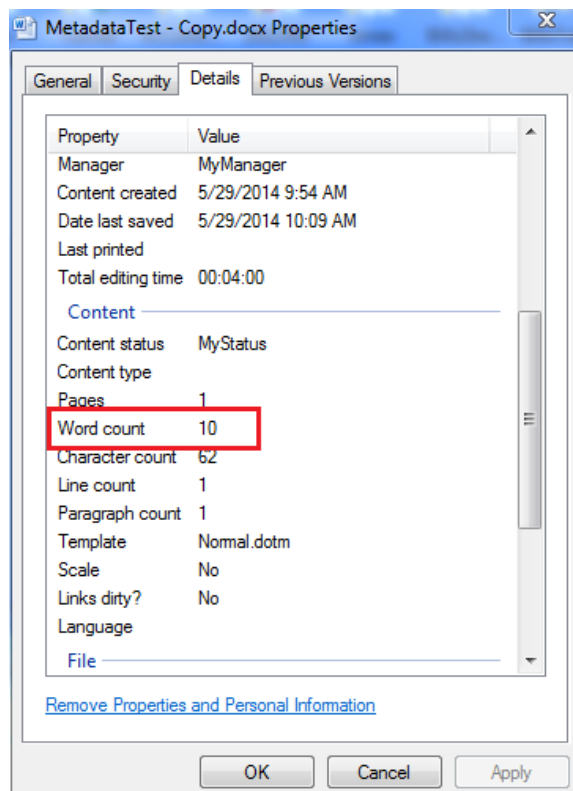
Metadata Location

- Document.xml
 - Actual content
- Word/Media
 - Embedded images etc
- Word/_rels/Settings.xml.rels
 - Identifying path to custom template
 - May help identify original source

Target="file:///C:\Documents%20and%20Settings\BlazerC.Catzen\Desktop\CatzenForensicLetterHead.dot"

Not Always Accurate

- Given version number testing is essential



Changing the “protected” data

- Note Zip Header

Volume	File	Preview	Details	Gallery	Calendar	Legend	Sync										
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	CP 1252
00000000	50	4B	03	04	14	00	06	00	08	00	00	00	21	00	09	24	PK[- ! \$
00000016	87	82	81	01	00	00	8E	05	00	00	13	00	08	02	5B	43	[C
00000032	6F	6E	74	65	6E	74	5F	54	79	70	65	73	5D	2E	78	6D	content_Types].xml
00000048	6C	20	A2	04	02	28	A0	00	02	00	00	00	00	00	00	00	1 0(
00000064	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

- Change to zip and extract core.xml
- Edit core.xml
- Return to zip

How can we tell

- Internal modified time has changes on core.xml
- Before

Name	Attr.	Created	Modified	Accessed
..				
<input type="checkbox"/> core.xml	c			
<input type="checkbox"/> app.xml	c			



- After

Name	Attr.	Created	Modified	Accessed
..				
<input type="checkbox"/> core.xml	cA		05/28/2014 16:11:18 -5	
<input type="checkbox"/> app.xml	c			

Internal Dates

- 1st challenge was to find the dates presented
 - Located them in 2 places
 - 10 Bytes in from start internal PK markers
 - Dos 32 bit Date format
 - Zeroing out sets date to 1/1/1980 00:00:00

00019680	FF FF 03 00 50 4B 03 04 14 00 00 00 08 00 69 89	ÿÿ PK i
00019696	BC 44 2A D5 70 10 3F 01 00 00 81 02 00 00 11 00	¼D*ÖP+?
00019712	08 01 64 6F 63 50 72 6F 70 73 2F 63 6F 72 65 2E	docProps/core.
00019728	78 6D 6C 20 A2 04 01 28 A0 00 01 00 00 00 00 00	xml (

Value to Decode:	<input type="text" value="6989BC44"/>	
Date & Time:	<input type="text" value="Wed, 28 May 2014 17:11:18 Local"/>	

Dos Date Time Stamp refresher

- 16 bit date
 - yyyyyyyym mmmddddd
 - y = Years from 1980
 - m = Months 1-12
 - d = Days 1-31
- 16 bit time
 - hhhhhmmmm mmmbbb
 - h= hours 0-23
 - m= minutes 0-59
 - b= 2 second intervals 0-29

Hacking the time stamps

- Default date time 00 00 21 00
 - Shown in unhacked file

```
00019680 FF FF 03 00 50 4B 03 04 14 00 06 00 08 00 00 00 yy PK - 
00019696 21 00 0F 9E 54 CA 51 01 00 00 87 02 00 00 11 00 ! TÈC 
00019712 08 01 64 6F 63 50 72 6F 70 73 2F 63 6F 72 65 2E docProps/core.
.....

00024080 68 45 66 66 65 63 74 73 2E 78 6D 6C 50 4B 01 02 hEffects.xmlPK 
00024096 2D 00 14 00 06 00 08 00 00 00 21 00 0F 9E 54 CA - - ! TÈ
00024112 51 01 00 00 87 02 00 00 11 00 00 00 00 00 00 00 Q 
00024128 00 00 00 00 00 00 E4 4C 00 00 64 6F 63 50 72 6F äL docPro
00024144 70 73 2F 63 6F 72 65 2E 78 6D 6C 50 4B 01 02 2D ps/core.xmlPK 
.....
```

- 0x21 0x00 = 100001 000000000
 - Referring back to dos date = year 0 month 1 day 1
 - Jan 1, 1980 – should be 0x00000000

After the hack

00024064	66 66 65 63 74 73 2E 78 6D 6C 50 4B 01 02 14 00	ffects.xmlPK
00024080	14 00 00 00 08 00 00 00 21 00 2A D5 70 10 3F 01	*ÖP+?
00024096	00 00 81 02 00 00 11 00 00 00 00 00 00 01 00	
00024112	20 00 00 00 E4 4C 00 00 64 6F 63 50 72 6F 70 73	äL docProps
00024128	2F 63 6F 72 65 2E 78 6D 6C 50 4B 01 02 14 00 14	/core.xmlPK

\USN\rmIParsingHackedFixed.docx\docProps					
ID	Name	Attr.	Created	Modified	Accessed
	..				
8	core.xml	cA			
11	app.xml	c			

Real world application




- Copy document
- Edit document
- Edit core.xml –
- Remove archive bit (new as of 6-1)
- Hack date time stamps of core.xml in PK container
- Move to FAT
- Hack directory entry for file to change modified date
 - We are going to make modified date 4-23-12 @12:00
 - 40 97 60 0D

More


- Now we have File on FAT 32 volume and can move back to NTFS Volume with created and modified intact.
- Optionally since move will give new MFT record number we could tunnel over original file and adopt original file MFT record SIA created date
 - In this instance there is no need to hack the created date time but still have FNA or tunnel in journal

Source File and Copy to FAT

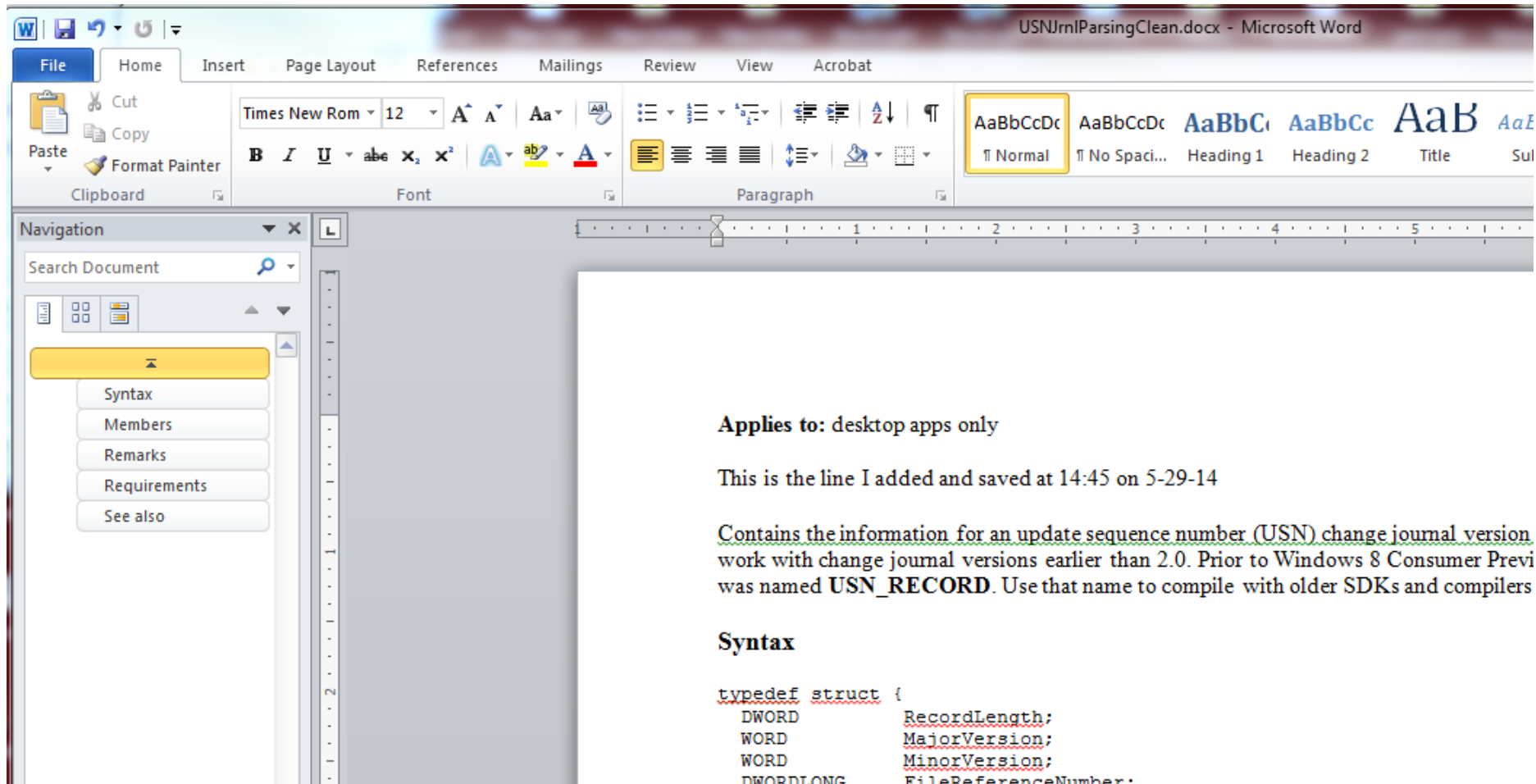
- Source File

Name	Date modified	Type	Size	Date created
 USNjrnlParsingClean.docx	4/23/2012 12:00 PM	Microsoft Word D...	24 KB	4/23/2012 12:00 PM
 USNjrnlParsingHackedFixed.docx	5/28/2014 5:37 PM	Microsoft Word D...	24 KB	5/28/2014 5:15 PM
 USNjrnlParsingHackedUnfixed.docx	5/28/2014 5:13 PM	Microsoft Word D...	24 KB	5/28/2014 5:06 PM

- Copied to new directory

Name	Date modified	Type	Size	Date created
 USNjrnlParsingClean.docx	4/23/2012 12:00 PM	Microsoft Word D...	24 KB	5/29/2014 2:43 PM

Edit Document



The screenshot shows the Microsoft Word 2010 interface. The title bar at the top reads "USN_Jrnl_Parsing_Clean.docx - Microsoft Word". The ribbon includes tabs for File, Home, Insert, Page Layout, References, Mailings, Review, View, and Acrobat. The Home tab is active, displaying the Font and Paragraph groups. The Font group shows "Times New Roman" font and "12" size. The Paragraph group shows various alignment and spacing options. The Styles group on the right shows "Normal" as the selected style. The Navigation pane on the left is open, showing a search bar and a list of document sections: Syntax, Members, Remarks, Requirements, and See also. The main document area contains the following text:

Applies to: desktop apps only

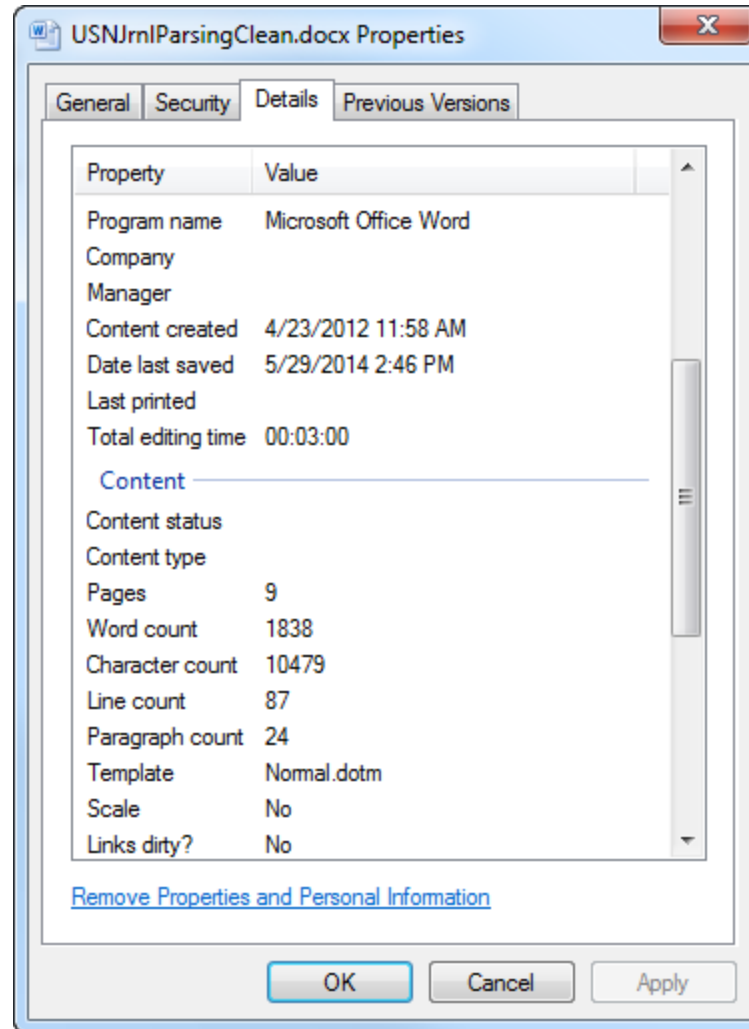
This is the line I added and saved at 14:45 on 5-29-14

Contains the information for an update sequence number (USN) change journal version.
work with change journal versions earlier than 2.0. Prior to Windows 8 Consumer Preview
was named **USN_RECORD**. Use that name to compile with older SDKs and compilers

Syntax

```
typedef struct {  
    DWORD      RecordLength;  
    WORD       MajorVersion;  
    WORD       MinorVersion;  
    DWORDLONG  FileReferenceNumber;  
}
```

Note metadata

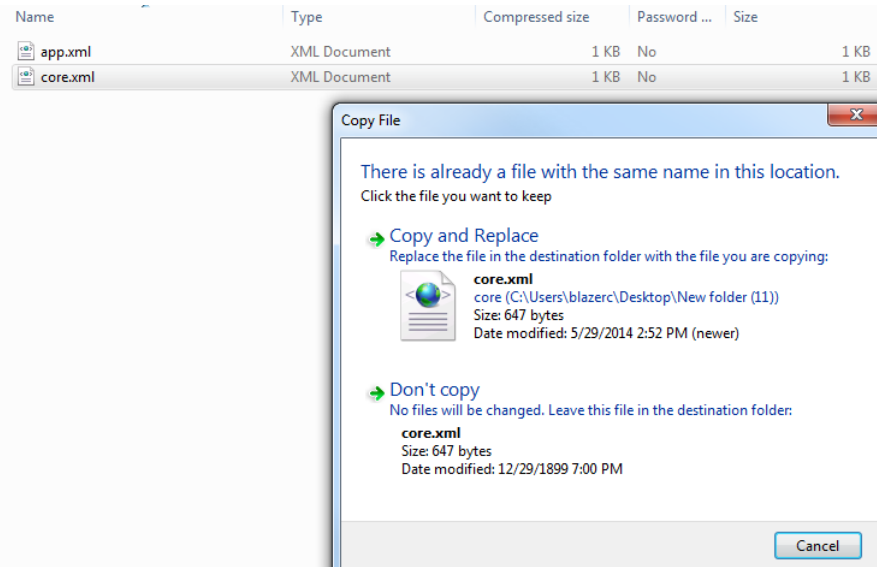


Hack metadata (core.xml)

- change core.xml content

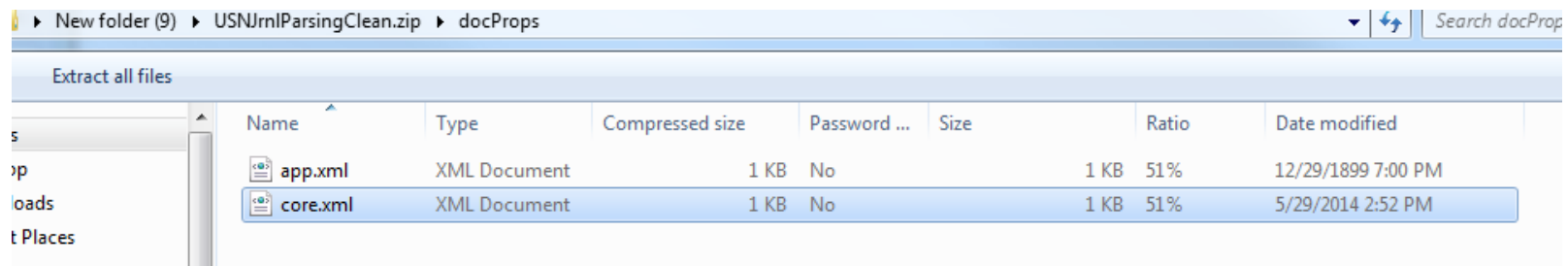
```
<dcterms:modified xsi:type="dcterms:w3cPTF">2012-04-23T15:58:00Z</dcterms:modified>
```

- Add back into zip

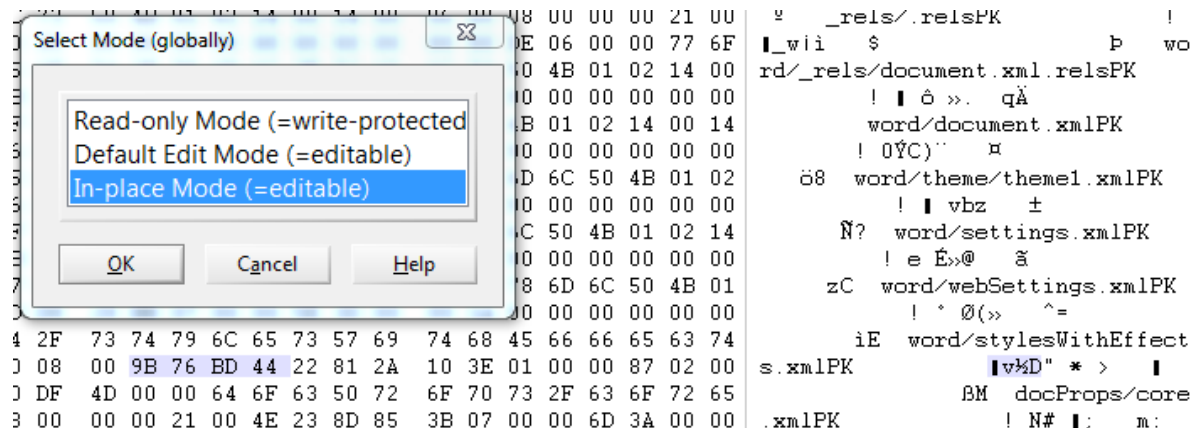


Hack internal dates

- UI view before



- Edit Date



After Edit

73 74 79 6C 65 73 57 69 74 68 45 66 66 65 63 74	iE word/stylesWithEffect
00 00 00 21 00 22 81 2A 10 3E 01 00 00 87 02 00	s.xmlPK ! " * >
4D 00 00 64 6F 63 50 72 6F 70 73 2F 63 6F 72 65	BM docProps/core
00 00 21 00 4E 23 8D 85 3B 07 00 00 6D 3A 00 00	.xmlPK ! N# ; m:
00 00 77 6F 72 64 2F 73 74 79 6C 65 73 2E 78 6D	TP word/styles.xml
00 FE AF 7B DD EC 01 00 00 AE 05 00 00 12 00 00	lPK ! p-{Ÿi @
6F 72 64 2F 66 6F 6E 74 54 61 62 6C 65 2E 78 6D	¼W word/fontTable.xml
00 F6 9D EC 4E E8 01 00 00 E3 03 00 00 10 00 00	lPK ä iNä ä


Information about USNJrnlParsingClean

C:\Users\blazerc\Desktop\New folder (9)\USNJrnlParsingClean.docx

Related Dates

Last Modified	4/23/2012 11:58 AM
Created	4/23/2012 11:58 AM
Last Printed	Never

Print E-mail Burn New folder

Name	Date modified	Type	Size	Date created
 USNJrnlParsingClean.docx	5/29/2014 3:00 PM	Microsoft Word D...	25 KB	5/29/2014 2:43 PM

Fat32 Directory Entry

Second (and last) long entry

0x42	w	n	.	f	o	0x0F	0x00	Check sum	x
0x0000	0xFFFF	0xFFFF	0xFFFF	0xFFFF	0x0000	0xFFFF	0xFFFF		
0x01	T	h	e		q	0x0F	0x00	Check sum	u
i	c	k		b	0x0000		r		o
T	H	E	Q	U	I	~	1	F	O
X	0x20	NT	Create time						
Create date	Last access date	0x0000	Last modi- fied time	Last modi- fied date	First cluster	File size			

Short entry

First long entry

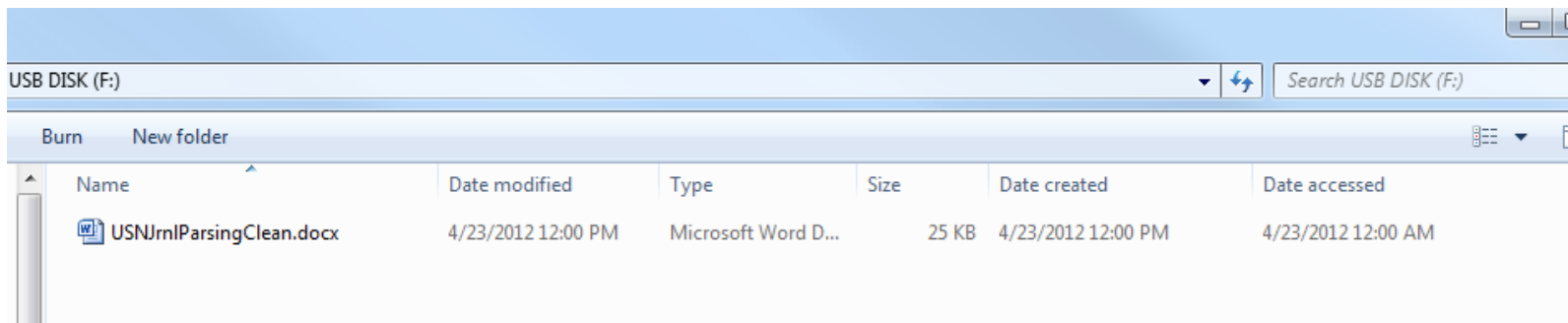
Fix date time in FAT

- Open in HEX Editor and change dir entry




```
01 55 00 53 00 4E 00 4A 00 72 00 0F 00 96 6E 00 6C 00 50 00 61 00 72 00 73 00 00 00 69 00 6E 00
55 53 4E 4A 52 4E 7E 31 44 4F 43 20 00 5B 6A 75 BD 44 BD 44 00 00 0C 78 BD 44 03 00 15 60 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```




```
-----
Bg C l e a   I n . d o c x       yy
U S N J r   I n l P a r s   i n
USNJRN~1DOC [ju%D%D   x%D   `
```

```
01 55 00 53 00 4E 00 4A 00 72 00 0F 00 96 6E 00 6C 00 50 00 61 00 72 00 73 00 00 00 69 00 6E 00
55 53 4E 4A 52 4E 7E 31 44 4F 43 20 00 5B 00 60 97 40 97 40 00 00 00 60 97 40 03 00 15 60 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```



Inspect File

<input type="checkbox"/>  (Root directory)						
<input type="checkbox"/>  USNJsonlParsingClean.docx (12)	A	04/23/2012 12:00:00 LT	04/23/2012 12:00:00 LT	04/23/2012 LT		04/23/2012 10:58:00 -5
<input type="checkbox"/>  Free space (net)						

Name	Attr.	Created	Modified	Accessed	Record update	Content created ▲
 ..						
<input type="checkbox"/>  core.xml	cA					
<input type="checkbox"/>  app.xml	c					

Detection

- Since we have figured out how to remove the archive bit, the only artifact left is a date time stamp mid document associated with the internal structure as shown below.

00011280	FF FF 03 00 50 4B 03 04 14 00 00 00 08 00 03 3B	ÿÿ PK ;
00011296	C1 44 3D 7D 0A 78 3E 01 00 00 87 02 00 00 11 00	AD=} x>
00011312	00 00 64 6F 63 50 72 6F 70 73 2F 63 6F 72 65 2E	docProps/core.
00011328	78 6D 6C 9D 92 51 4B C3 30 14 85 DF 05 FF 43 C9	xml 'QKÃ0 B ŸCÉ

Questions



Blazer Catzen

blazer@catzen.com

410-891-1680