

Microsoft Office Security, part two

Khushbu Jithra 2006-08-29

1. Continuing from part one

The flood of recent Microsoft Office vulnerabilities has brought forth the need to understand the mechanics of the MS Office security architecture and the possible fault injection points. [The first part of this article](#) primarily discussed Microsoft Office's OLE Structured Storage and the nature of recent dropper programs and other exploit agents, in an effort to scrutinize the workings of some of the recent MS Office exploits. Now the second part looks at some forensic investigation avenues with different MS Office features. Parts of the article sample different MS Office vulnerabilities to discuss their nature and the method of exploitation.

2. Avenues for MS Office forensic investigation

During the 'analysis' phase of a forensic investigation involving MS Office files, some features which investigators would fancy are explained below. Known to aid the efficiency of the software, these features can turn out to be excellent sources for information for vital evidence.

2.1 Track Changes turned on (Tools > Track Changes) (Ctrl+Shift+E)

Feature: 'Track Changes' is used in case several revisions are made to the same document by one or more users. It displays all modifications made to the document including any insertions, deletions, changed lines and comments.

Investigator's Interest: If the 'Track Changes' feature is turned on, even after distributing the file (via e-mail, on the local network or through a physical device), by default, the file opens in the 'Track Changes' mode to reveal all changes made. It also shows up with all the comments, if added, by other authors/reviewers of the document along with the name of the author.

2.1.1 Turn off 'Track Changes' (Tools > Options > Security)

Note that for continuity with part one of this article, which had five illustrations, we'll start with Figure 6.

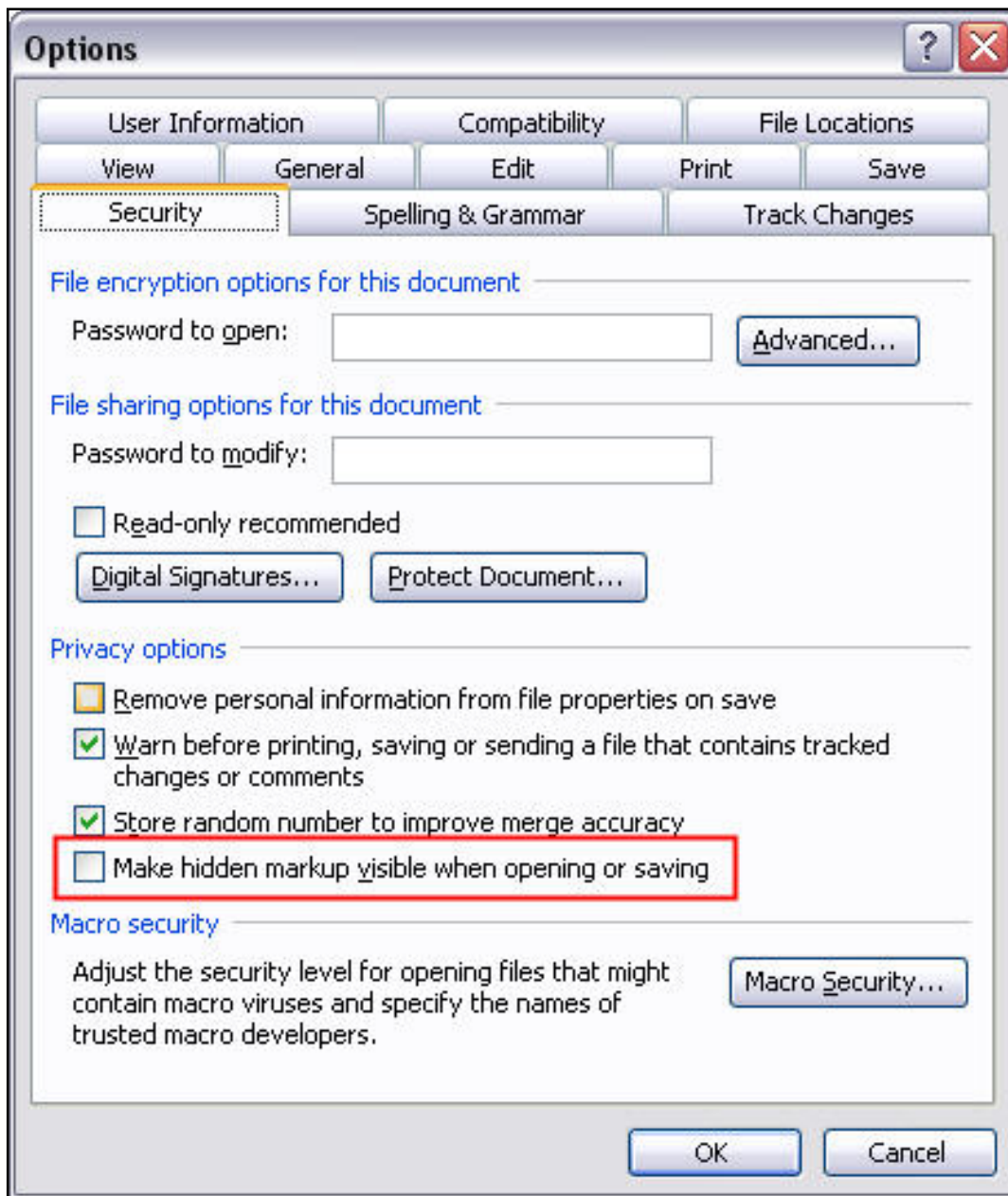


Figure 6. Making hidden markups visible in MS Office 2003.

Note: by default, the 'Make hidden markup visible when opening or saving' option is enabled to refrain the user from accidentally distributing the document with any sensitive information.

This was the procedure for disabling the feature in Word 2003. However, in Word 2002, the markup text can be hidden through the reviewing toolbar as shown in Figures 7 and 8, and it will not show up on opening or saving the file.

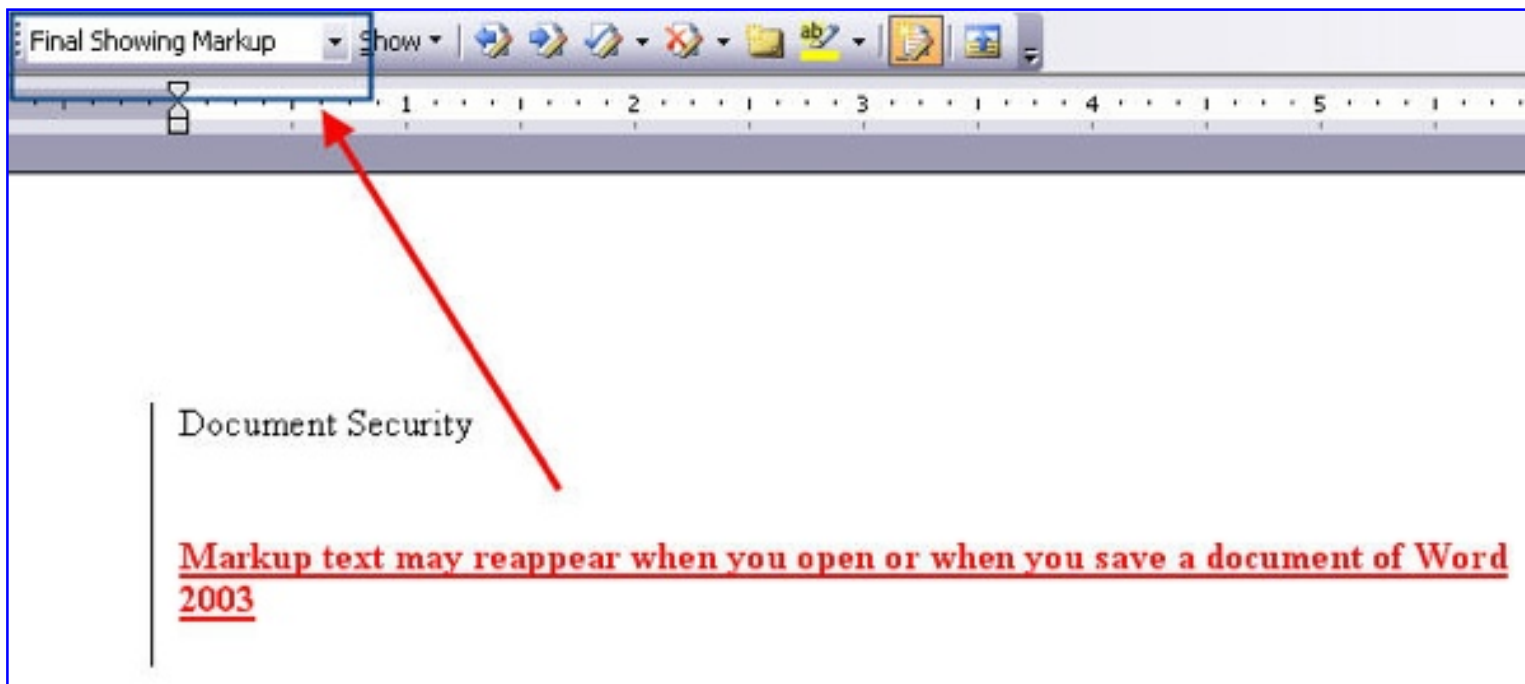


Figure 7. Making hidden markups visible in MS Office 2002.

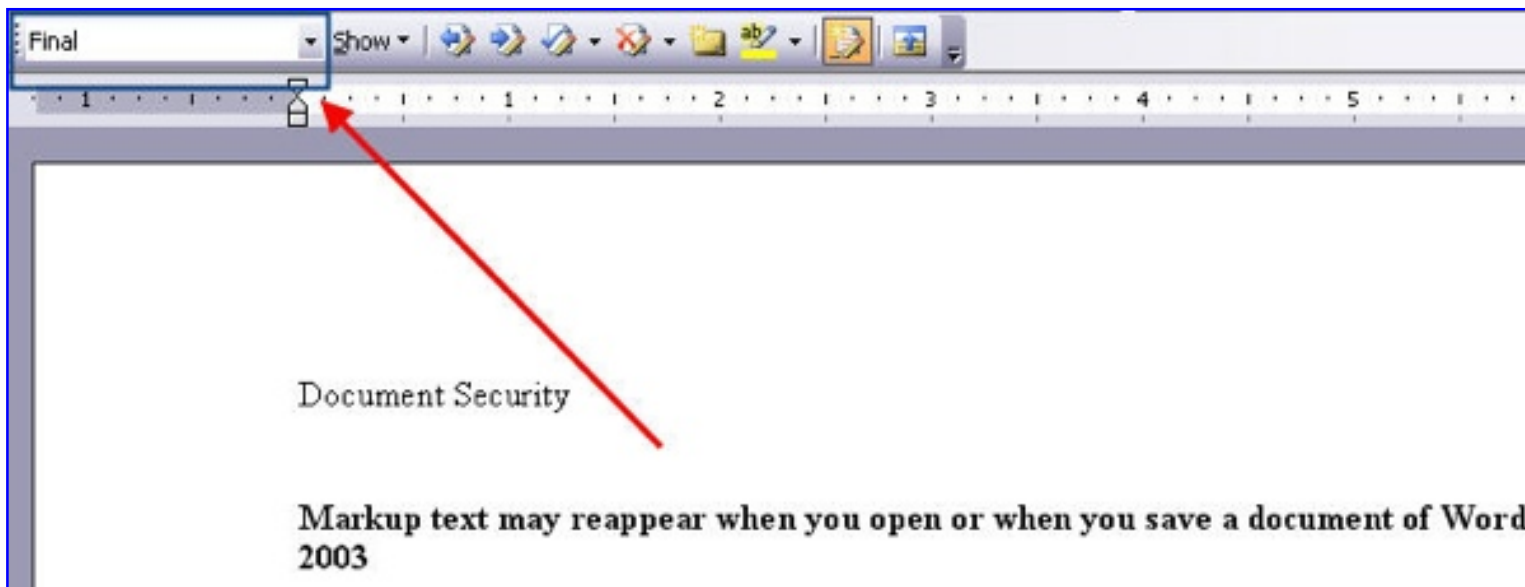
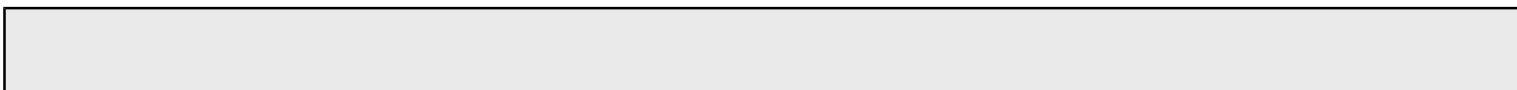


Figure 8. Making hidden markups visible in MS Office 2002.

2.1.2 Deleting a large number of comments in a document

Sometimes, even the comments show up 'as is' when the document is re-opened. These can be hidden as shown above. However, a technique exists for deleting a large number of comments in a document. This can work for MS Word and MS Excel documents. A simple macro can do the trick and rid you from the painful task of deleting each comment manually.

Macro for deleting comments from MS Word: add the following macro to the desired document or document template:



```
'Function to delete and confirm the deletion of comments
Sub DeleteAllCommentsAndConfirm( )

'Variable Initialization
Dim i As Integer

Dim iNumberOfComments As Integer

If MsgBox( _"Are you sure you want to delete
  ALL comments in this document?", _vbYesNo) = vbYes Then

  iNumberOfComments = ActiveDocument.Comments.Count

  For i = iNumberOfComments To 1 Step -1

    ActiveDocument.Comments(i).Delete

  Next i

MsgBox iNumberOfComments & " Comment(s) Deleted", vbInformation

End If

End Sub
```

2.2 Document sent for review through MS Office applications

Feature: 'Send to Mail Recipient for Review' allows documents to be sent to the default e-mail application. It should be used very carefully as it has the details of the entire document. This is shown below in Figure 9.

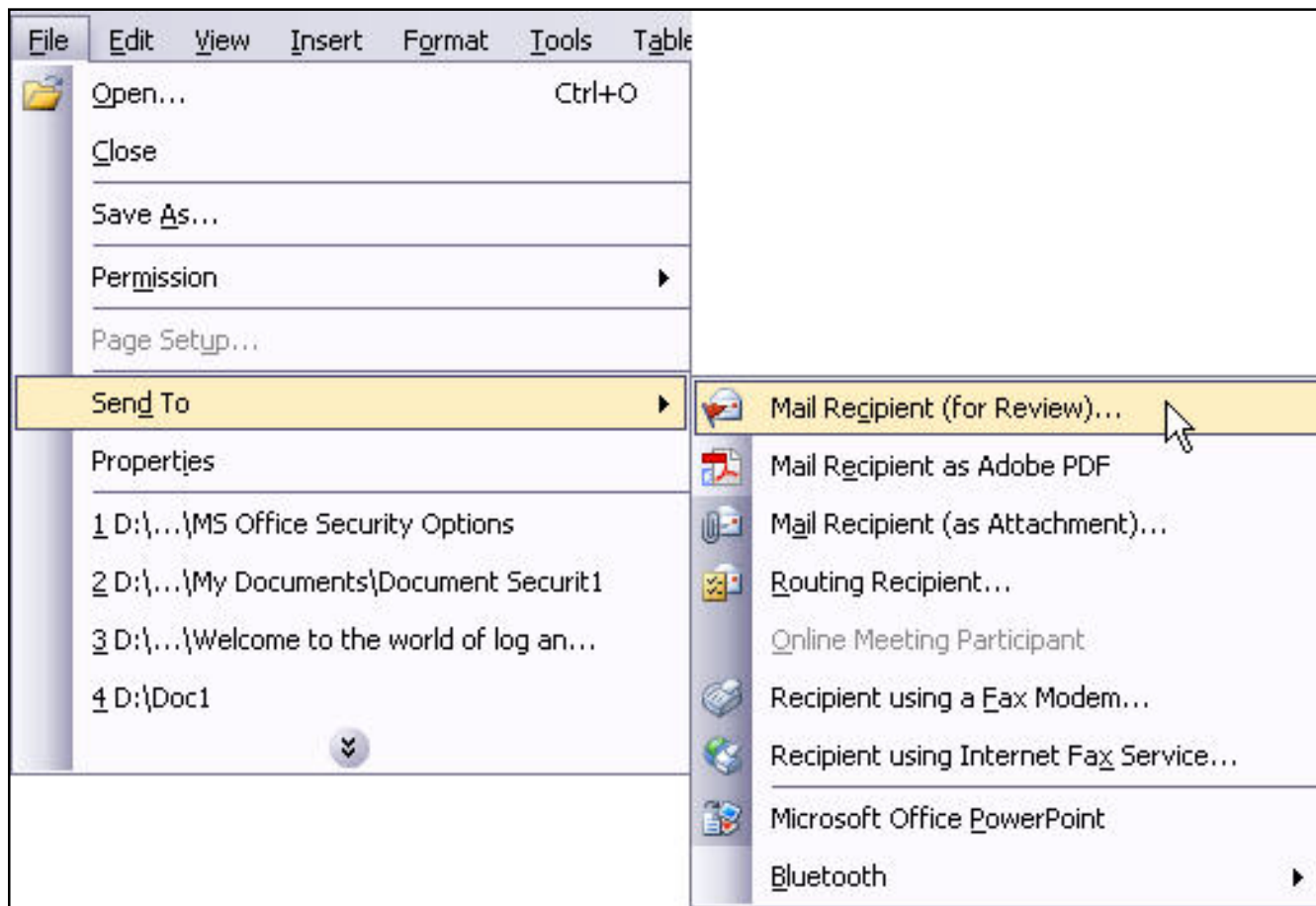


Figure 9. Mail recipient option (for review).

Investigator's Interest: If the document is sent through Outlook, when the recipient opens the document and views the file properties (Files > Properties > Custom), entries such as `_TentativeReviewCycleID` and `_ReviewCycleID`, `_EmailSubject`, `_AuthorEmail`, and `_AuthorEmailDisplayName` are shown.

The details of this 'Custom' tab are also stored on the recipient's system in a file called 'Adhoc.rcd' or 'Review.rcd' (depending upon the version of MS Office used; it's 'Review.rcd' in the case of Office 2003). They are usually found in the following location:
 System_Drive>User's_Documents_and_Settings>\Application Data\Microsoft\Office.

The Adhoc.rcd or Review.rcd file typically contains the same information as shown in the Custom Properties tab. The entry reveals the following:

- Machine from which the document was sent
- Username of the logged in user
- E-mail Address
- E-mail Subject

For any reason, if the investigator needs to access the email message, he/she can route back to it via the Exchange server or any other convenient technique.

You can avoid this by:

- Manually attaching the document to an email
- Using any email application other than Outlook

2.3 Recover unseen metadata

Feature: The 'Recover Text From Any File (*.*)' File Open option. This option rips the formatting off the document and displays all the text along with the exhaustive file properties. This is shown below in Figures 10, 11, and 12.

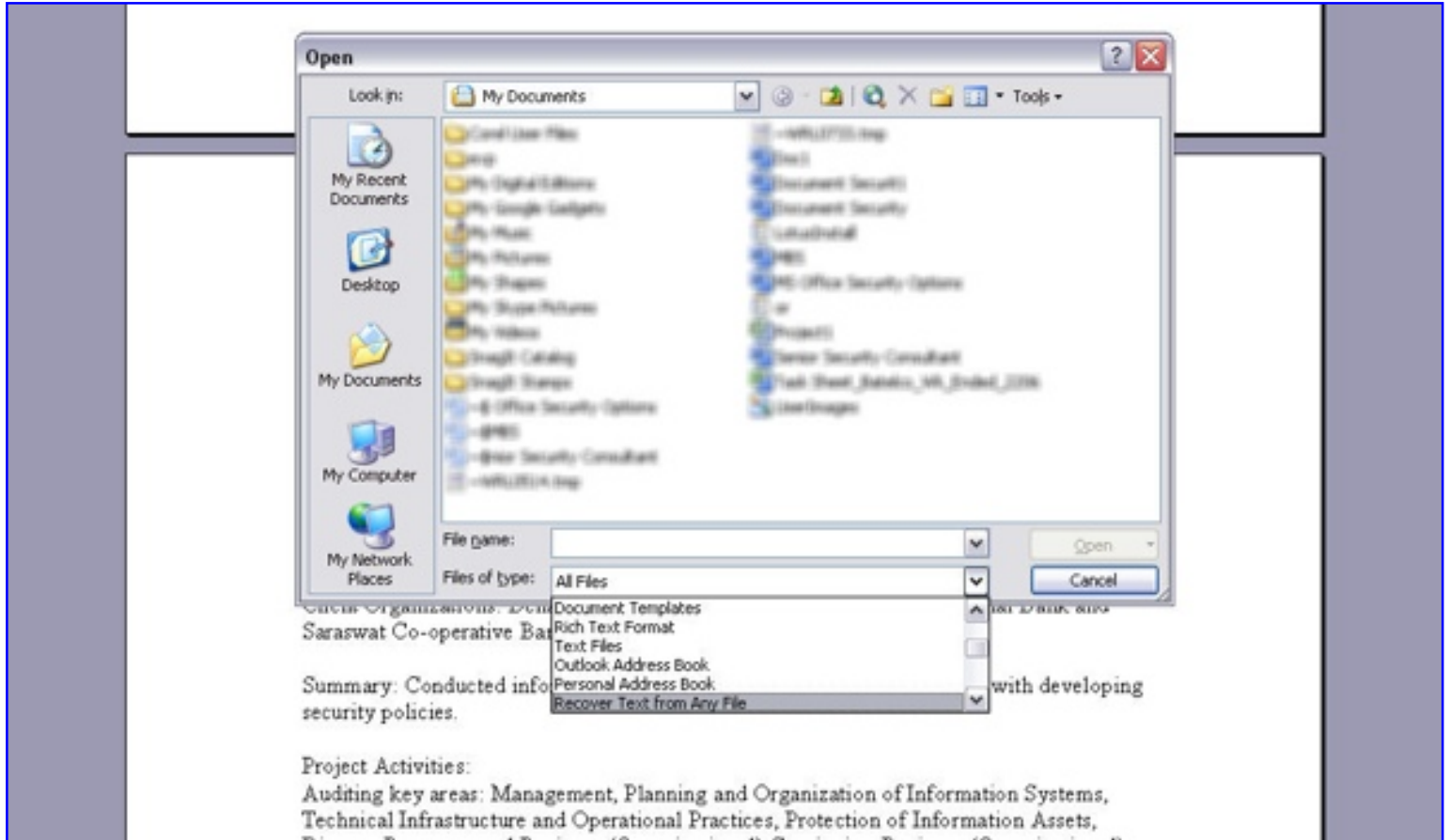


Figure 10. 'Recover Text From Any File (*.*) Option.

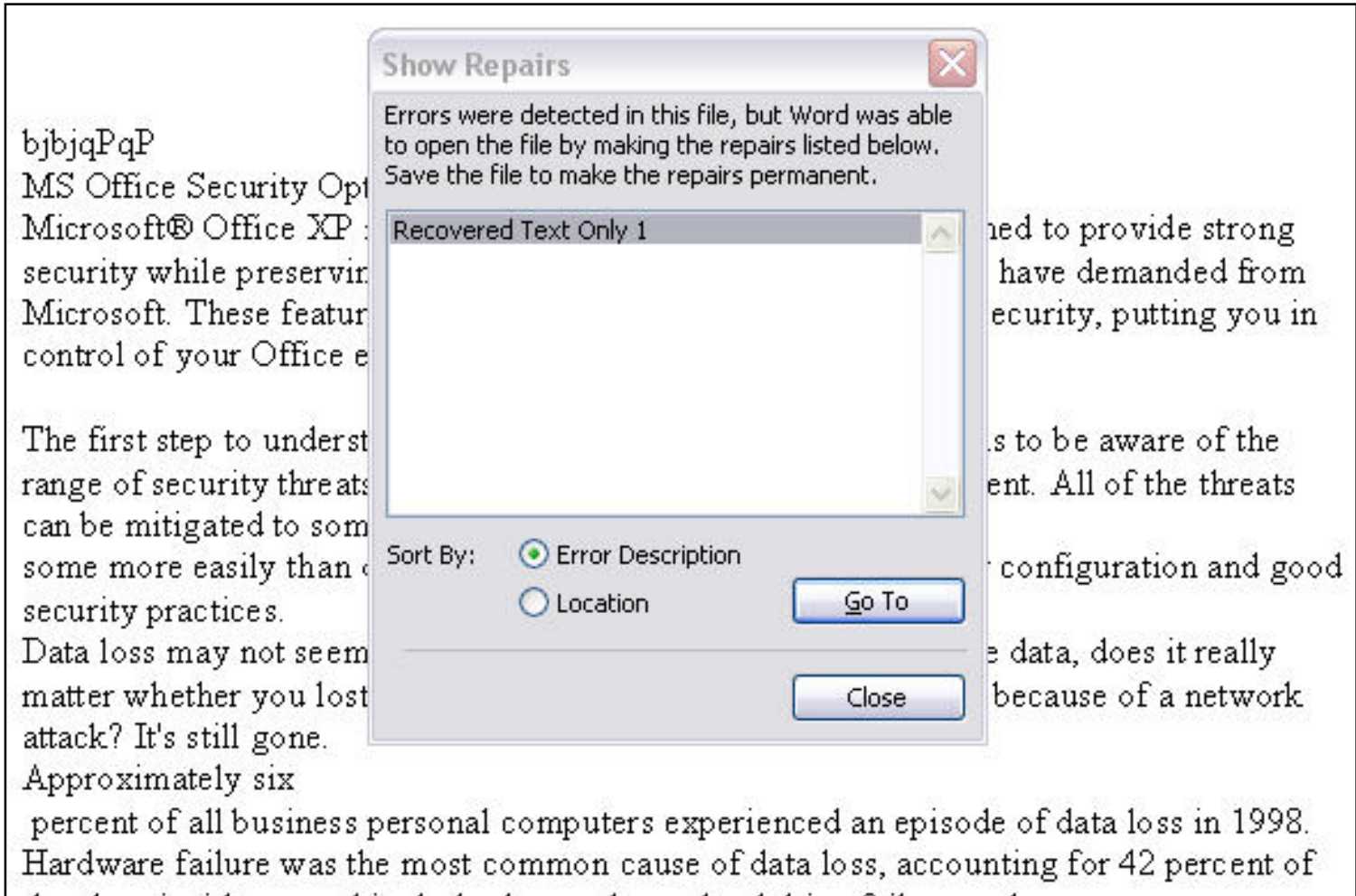


Figure 11. Dialogue when file recovered (Select Close).

```
Times New Roman
Symbol
Symbol
Tahoma
Tahoma
MS Office Security Options
MS Office Security Options
User 2
User 2
MS Office Security Options
User 2
Normal
Microsoft Office Word
MS Office Security Options
Root Entry
1Table
1Table
WordDocument
WordDocument
SummaryInformation
SummaryInformation
DocumentSummaryInformation
DocumentSummaryInformation
CompObj
CompObj
Microsoft Office Word Document
MSWordDoc
Word.Document.8
```

Figure 12. Sample contents of the recovered file.

Investigator's Interest: An exhaustive listing of the file properties reveals information which may turn out to be crucial evidence, may help build a timeline, or may help make certain deductions during the analysis phase of the forensic investigation.

No known workaround or solution exists to stop an MS Office application from being recovered. We cannot stop MS Office from recording metadata but we can definitely take measures to hide it. Thus when sending any files, one can:

1. Convert the file to PDF format and retain only necessary information.
2. Convert the file into Rich Text Format (.rtf) and send it or reconvert it to (.doc) format. Converting to (.rtf) removes all the metadata from the file and retains the formatting.

An important note to be made is that this conversion does not remove the revision history of the document.

2.4 'Recently Opened Files' Listing

Feature: This is feature which displays the list of recently opened files. A maximum of nine entries can be displayed:

1. The listing is shown in the 'File' menu as the last set of entries, or
2. The listing is shown through the 'Startup Task Pane'

Investigator's Interest: Such a listing undoubtedly serves as a quick reference as to where to begin from and saves the investigator the trouble of going through the metadata of several Office files individually.

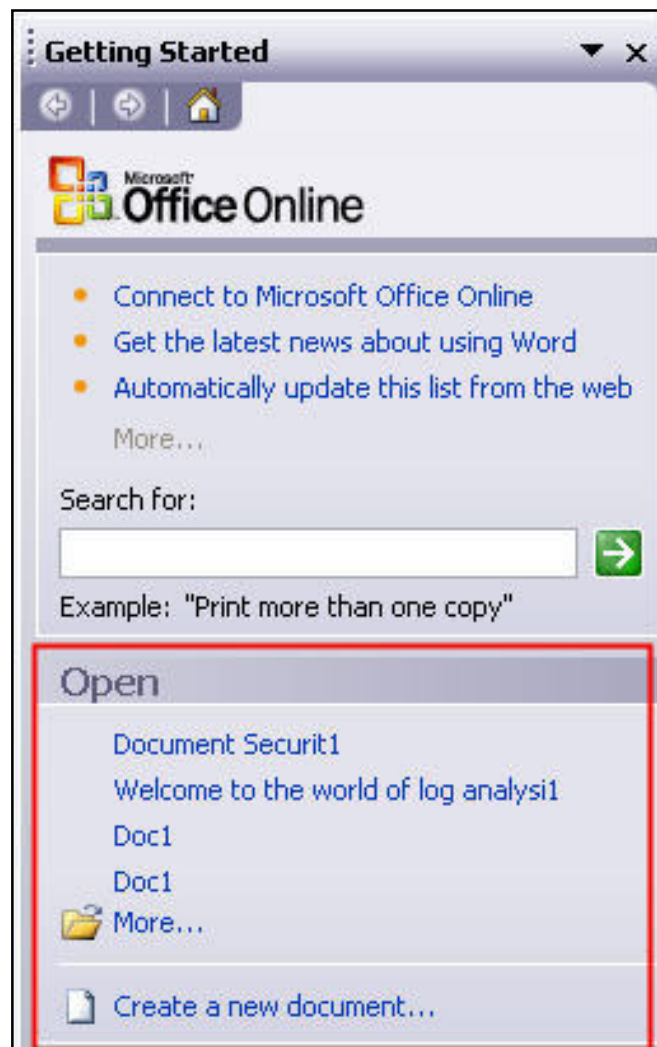


Figure 13. Recently opened files listing.

The number of entries in the 'Recently Opened Files' option can be set to 0, as shown below in Figure 14.

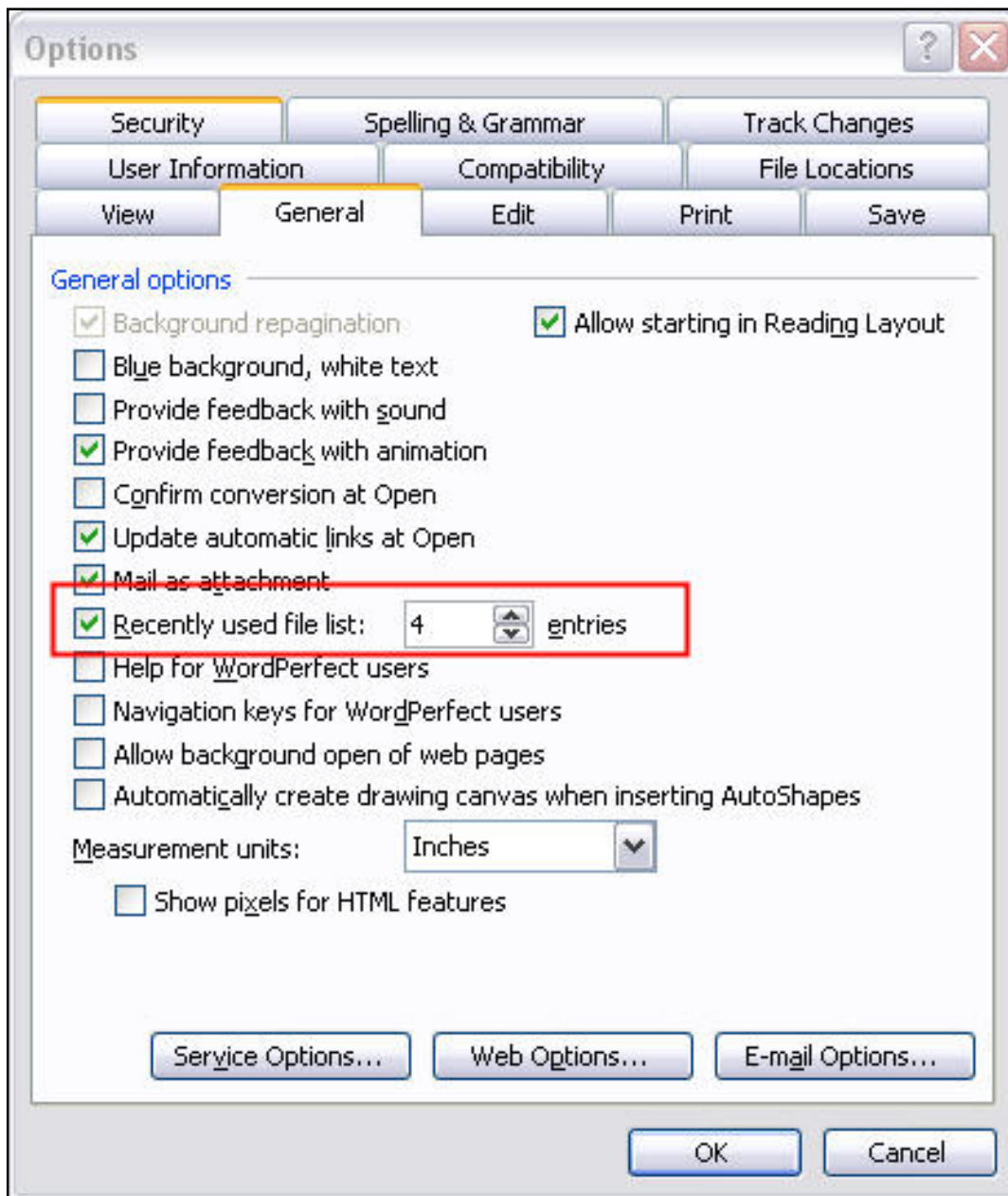


Figure 14. Highlighted Entry to be set to '0'.

One can avoid the Task Bar from showing up each time an Office application is opened as well. This is shown below in Figure 15.

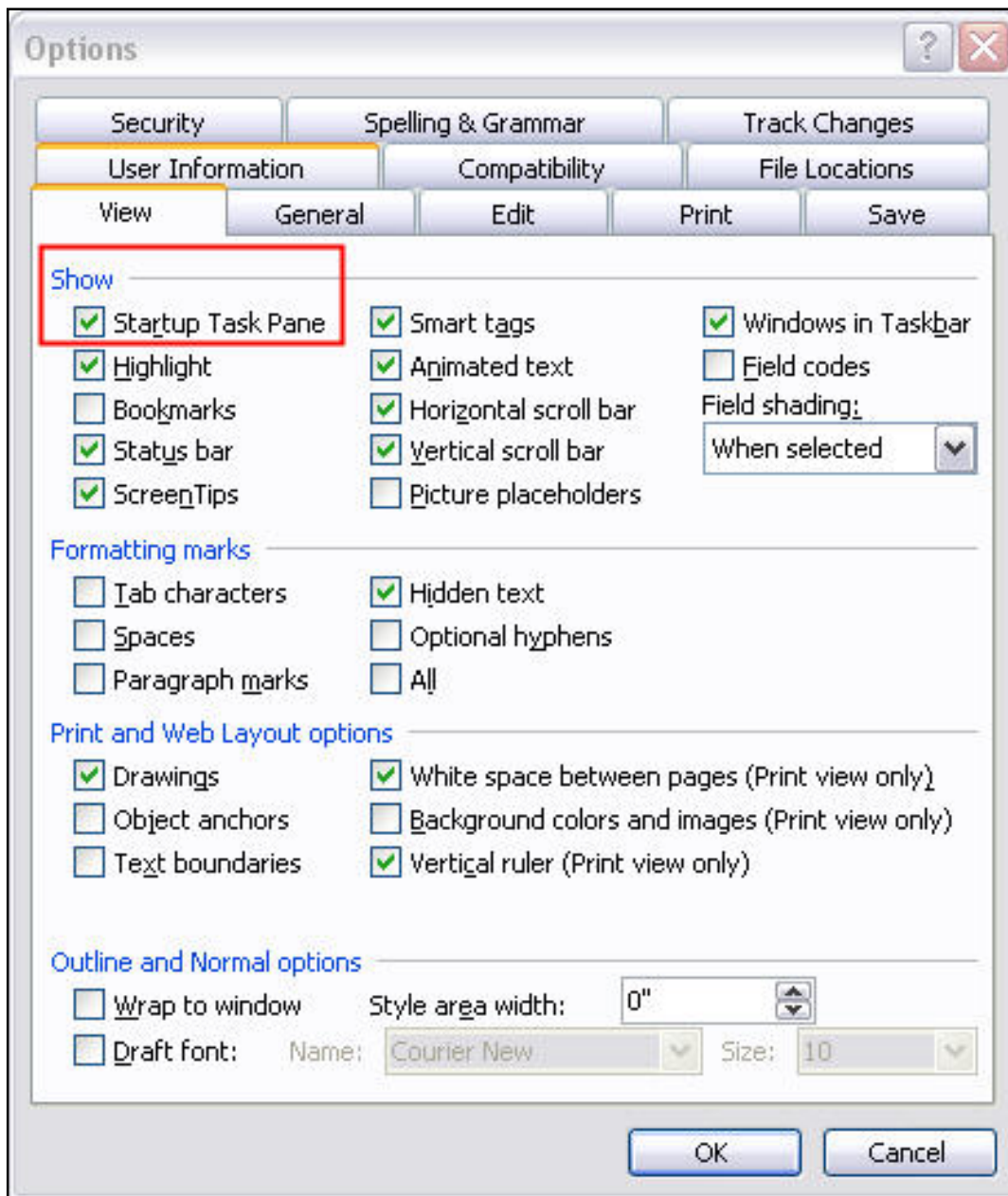


Figure 15. 'Startup Task Pane' viewing option to be unchecked.

2.5 MS Office 'Summary Information'

The 'Privacy Options' feature is used to secure the document primarily against information disclosure.

The first feature is that it helps secure personal information associated with any document. Personal Information refers to the document details which are written and archived across users and authors of the same document. It's important to understand that 'Personal Information' is not the 'User Information' included in the file as shown in Figure 16:

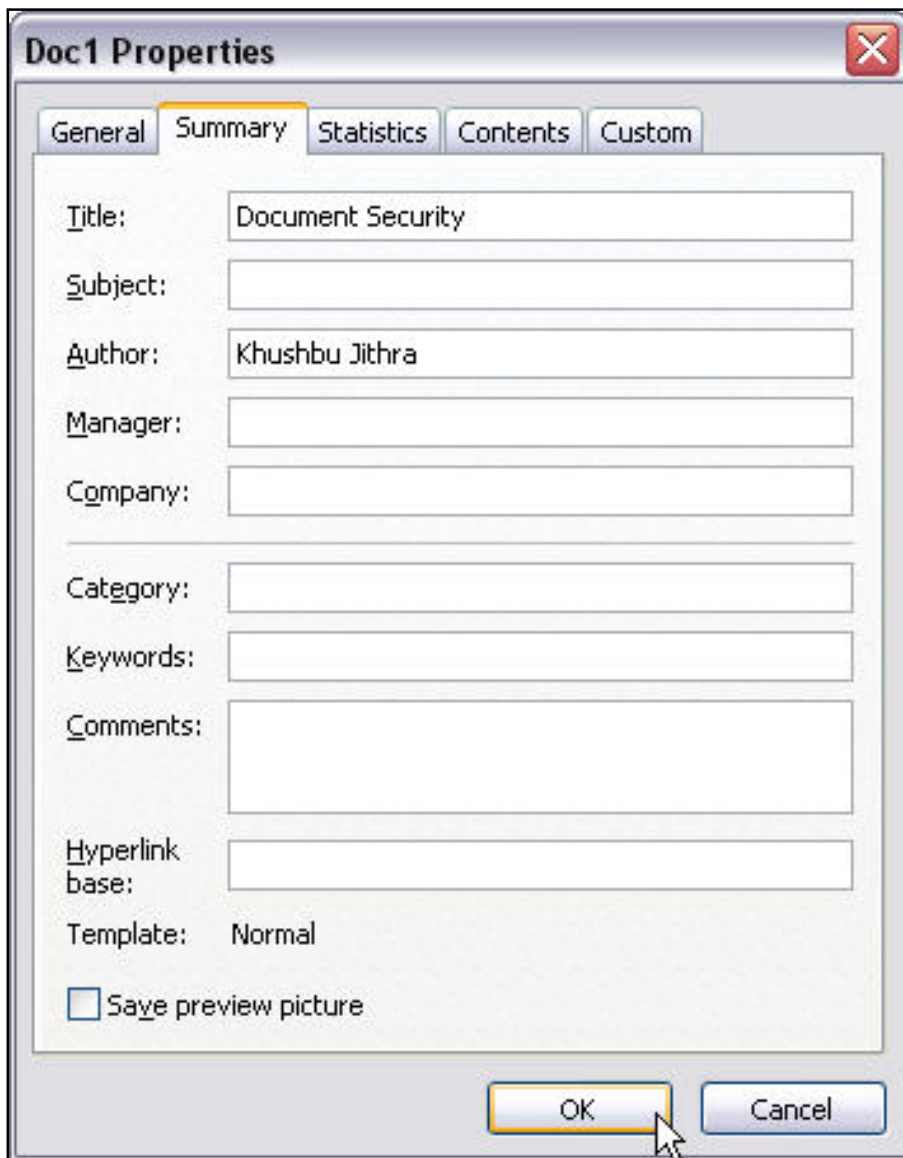


Figure 16. Sample 'User Information'.

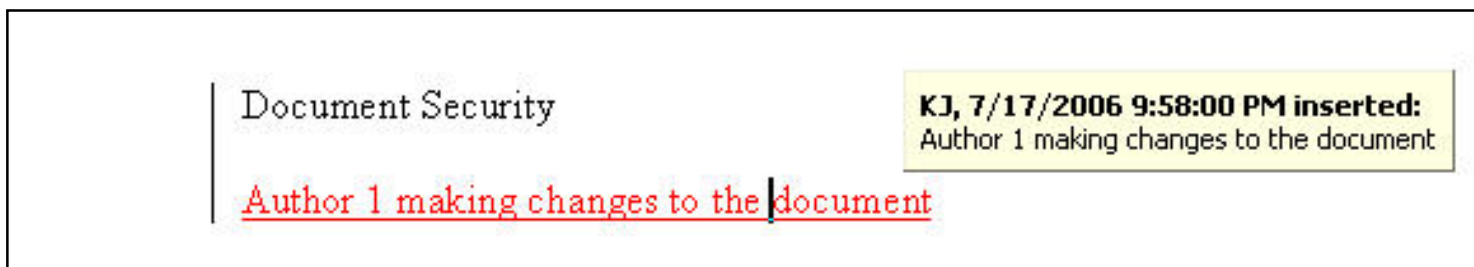


Figure 17. Personal Information: Different author details with 'Track Changes' turned on.

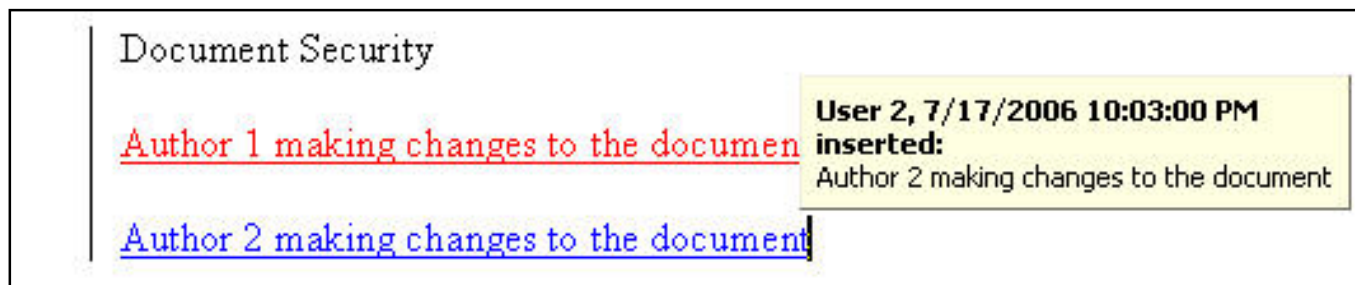


Figure 18. Personal Information: Different author details with 'Track Changes' turned on.

This kind of personal information may be confidential. No one would (even accidentally) like their prospective employer to know who helped them make changes/revisions to their resume nor would anyone like to disclose this to their potential client. Consider the number of revisions made to a price quote before sending the final proposal, as well as knowing who all made the revisions! The following option can save the reader from embarrassment and ensure the security of the document.

Tools > Options

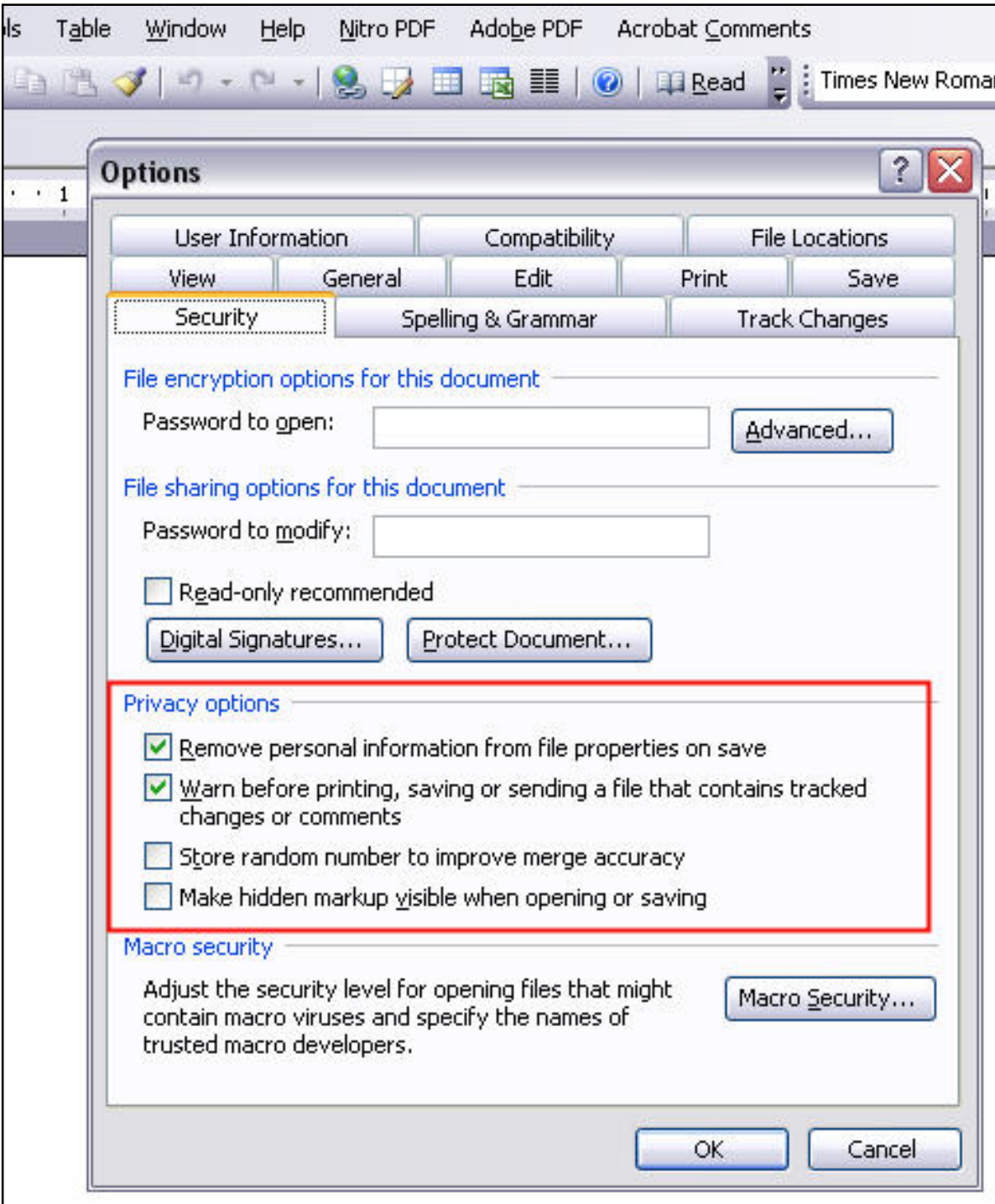


Figure 19. Removing 'Personal Information' from file properties.

There are times when you would like to keep the names of the authors confidential but show

the comments and modifications through Track Changes. There is a somewhat tedious way to change the name of the authors/reviewers of the document as shown below:

Step 1: Save the file in rich text format (.rtf) using the 'Save As' option.

Step 2: Open the document in any rich text editor or even Notepad.

Step 3: Look for the string '{*\revtbl'.

Step 4: The content of the braces following this string has the list of authors/reviewers.

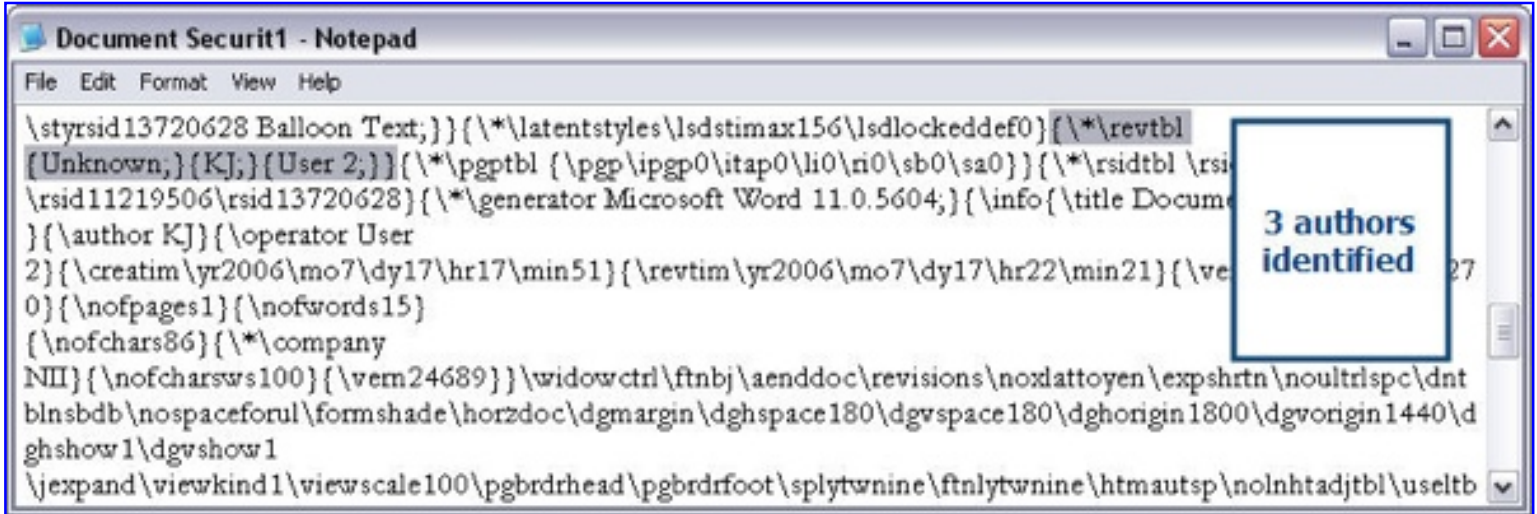


Figure 20. Author Identification with '{*\revtbl' string.

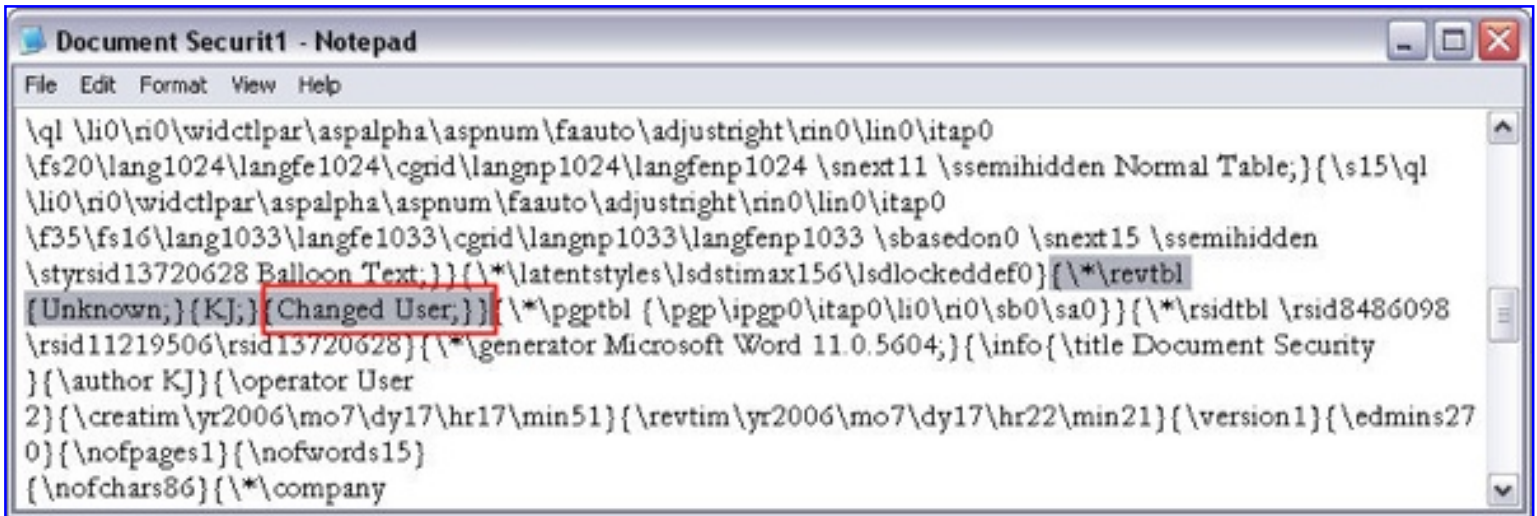


Figure 21. Entry modification.

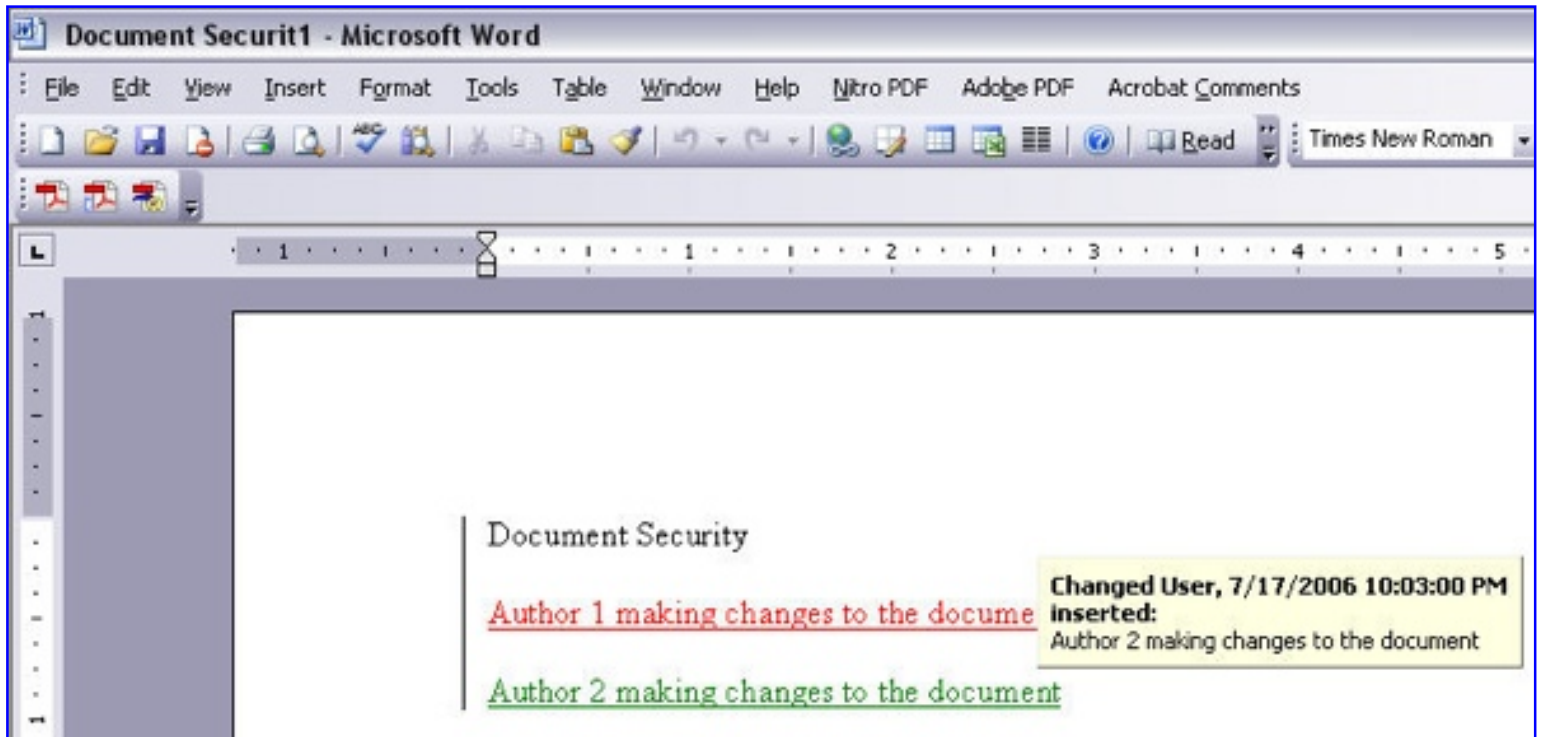


Figure 22. Changed entry in MS Word.

The above method shows the list of authors of the document. There are other ways of accessing this information and investigating much more with the help of a file viewing utility called the DocFile View. This utility provides the property set IDs of the OLE Structured Storage and its corresponding values saved in the document's SummaryInformation stream.

The screenshot shows the 'DocFile View - 0.1' application window. On the left, a tree view displays the file structure for 'C:\k\HUSHBU on NII (192.168.0.88)'. The selected item is 'WordDocument', which is expanded to show 'SummaryInformation'. The main pane on the right displays a table of properties for this SummaryInformation block.

PropID	Type	Value
1	I2	1252
2	LPSTR	Alls well that ends well
3	LPSTR	
4	LPSTR	New User
5	LPSTR	
6	LPSTR	
7	LPSTR	Normal
8	LPSTR	Last User
9	LPSTR	5
18	LPSTR	Microsoft Office Word
10	FileTime	01-Jan-1601 00:07:00
12	FileTime	06-Aug-2006 09:48:00
13	FileTime	06-Aug-2006 09:56:00
14	I4	1
15	I4	57
16	I4	278
19	I4	0

Figure 23. SummaryInformation viewed through DocFile View.

Name	Property ID string	Property ID	VT type
Title	PIDSI_TITLE	0x00000002	VT_LPSTR
Subject	PIDSI_SUBJECT	0x00000003	VT_LPSTR
Author	PIDSI_AUTHOR	0x00000004	VT_LPSTR
Keywords	PIDSI_KEYWORDS	0x00000005	VT_LPSTR
Comments	PIDSI_COMMENTS	0x00000006	VT_LPSTR
Template	PIDSI_TEMPLATE	0x00000007	VT_LPSTR
Last Saved By	PIDSI_LASTAUTHOR	0x00000008	VT_LPSTR
Revision Number	PIDSI_REVNUMBER	0x00000009	VT_LPSTR
Total Editing Time	PIDSI_EDITTIME	0x0000000A	VT_FILETIME (UTC)
Last Printed	PIDSI_LASTPRINTED	0x0000000B	VT_FILETIME (UTC)
Create Time/Date(*)	PIDSI_CREATE_DTM	0x0000000C	VT_FILETIME (UTC)
Last saved Time/Date(*)	PIDSI_LASTSAVE_DTM	0x0000000D	VT_FILETIME (UTC)
Number of Pages	PIDSI_PAGECOUNT	0x0000000E	VT_I4
Number of Words	PIDSI_WORDCOUNT	0x0000000F	VT_I4
Number of Characters	PIDSI_CHARCOUNT	0x00000010	VT_I4
Thumbnail	PIDSI_THUMBNAIL	0x00000011	VT_CF
Name of Creating Application	PIDSI_APPNAME	0x00000012	VT_LPSTR
Security	PIDSI_SECURITY	0x00000013	VT_I4
* Some methods of file transfer, such as a download from a BBS, do not maintain the file system version of this information correctly.			

Figure 24. Property ID Strings corresponding to PropIDs (courtesy [MSDN Website](#)).

The PropID shown in Figure 23 should be mapped with the Property ID hexadecimal value (column 3) in Figure 24. As seen from the screenshots, a forensics investigator may quickly collect important document information like the Author, User and so on who saved the document last, the time and date of the last save, revision number, and more. One may wonder why this procedure is needed when one can simply open the file and visit the 'Properties' sub-menu to access all of the above information. The answer is quite simple. Such tools help the forensic investigator to retrieve all the information without actually opening the file. He can scan a large number of files one after the other to get any evidence.

Note: This method will not prove helpful if the file is in the 'Read Only' mode or if it has been encrypted.

The best way to remove all personal information before sending any document is by using an [Add-in from Microsoft](#) which can permanently remove hidden data and collaboration data, such as change tracking and comments, from Microsoft Word, Microsoft Excel, and Microsoft PowerPoint files.

3. Conclusion

Part one of this article looked primarily at the OLE Structured Storage of Microsoft Office documents. Part two looked at forensic avenues that can be used by investigators, post-compromise. Some of the features shown in part two are more appropriate for a proactive approach towards incident response. Usually, forensic investigators do not start the application on the compromised system, they make an image of the disk and begin to investigate the contents using sophisticated tools and techniques.

MS Office overall provides very good security features and recovery options. Some are well-known while others are not. The suggested techniques in this article could be implemented to secure one's written communication. The forensic investigator's perspective was shown to highlight the areas of possible forensic interest. The features highlighted do not play against the user but guide the user to be careful with the documents and set the security options after deciding the confidentiality and sensitivity of the document.

4. References

4.1 Web references

1. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/stg/stg/storage_vs__stream_for_a_property_set.asp
2. http://msdn2.microsoft.com/dede/library/microsoft.office.interop.word.oleformat_members.aspx
3. <http://blogs.msdn.com/erikaehrli/archive/2005/11/30/dsofileproperties.aspx>
4. <http://windowssdk.msdn.microsoft.com/en-us/library/ms725799.aspx>
5. <http://en.wikipedia.org/wiki/Dropper>
6. <http://desaware.com/tech/persist.aspx>
7. <http://www.microsoft.com/technet/security/bulletin/MS06-027.msp>

4.2 Selected book references

1. Andrew Savikas, Word Hacks. O'Reilly, November 2004.
2. Chris Davis, Aaron Philipp, David Cowen, Hacking Exposed Computer Forensics. McGraw-Hill Professional, November 2004.

5. About the author

Khushbu Jithra, is an Information Developer and Security Researcher at [NII Consulting](#), an Information Security Consulting firm based out of India. She writes at [iScribe](#) on her main interest - [Information Security Documentation](#)

6. Comments?

The comments section of this article is to be used for technical clarification and discussion only. Submitted comments must have technical merit in order to be approved.

7. Copyright

This article is © Copyright 2006, SecurityFocus. Reproduction without prior authorization is prohibited.

[Privacy Statement](#)

Copyright 2006, SecurityFocus