


Hidden Data

David Lilburn Watson
Principal Consultant


Forensic Computing Ltd
Georgia House, 3, Nelson St, Ryde, IoW PO33 2EZ
01983 566 460 (v) 01983 811 603 (f)
www.forensic-computing.ltd.uk

13th April 2005 © Forensic Computing Ltd 2005 Page 1



So what is hidden data?

13th April 2005 © Forensic Computing Ltd 2005 Page 2



Dictionary – from the web!

hidden *A adjective*


1 buried, hidden
covered from view; "her face buried (or hidden) in her hands"; "a secret buried deep within herself"

2 hidden, obscure
difficult to find; "hidden valleys"; "a hidden cave"; "an obscure retreat"

3 hidden, secret
designed to elude detection; "a hidden room or place of concealment such as a priest hole"; "a secret passage"; "the secret compartment in the desk"

4 concealed, hidden, out of sight
not accessible to view; "concealed (or hidden) damage"; "in stormy weather the stars are out of sight"


13th April 2005 © Forensic Computing Ltd 2005 Page 3



Simple hiding

- Hiding a disk or computer where it cannot be seen/found;
- Hidden files in Windows and DOS;
- Burying text in the middle of a document;
- Deleting a document and later recovering it from the disk;
- Placing it on removable media;
- Etc.


13th April 2005 © Forensic Computing Ltd 2005 Page 4



Bit more complex

Rename the file and then change the suffix:
e.g.
Rename:
 bombmaking.doc
To
 railwaytrain.jpg


13th April 2005 © Forensic Computing Ltd 2005 Page 5



However


Using standard forensic tools we can see:

13th April 2005 © Forensic Computing Ltd 2005 Page 6



Getting better – or Bill is at it!


13th April 2005 © Forensic Computing Ltd 2005 Page 10



Metadata

A look under the bonnet of MS Office – well part of it – with thanx to Paul Birch of HMC&E who gave this at CIC 2005!


13th April 2005 © Forensic Computing Ltd 2005 Page 11



Have you ever wondered ...

- Small document.doc;
- Small document.txt;
- Both contain same text
- Different sizes
- Why???


13th April 2005 © Forensic Computing Ltd 2005 Page 12



Out of the bag... (1)

When I installed Windows 98 I filled in the registration process.
 === Microsoft Registration Wizard ===
 Default First Name = David
 Default Last Name = Lilburn Watson
 Mailing Address = Blah blah
 Daytime Phone = blah blah
 <snip>
 HWID = 1961c5cf6e7611d2bb50006008d31d03
 MSID = 63c896056a9f11d2bb50006008d31d03
 <snip>


13th April 2005 © Forensic Computing Ltd 2005 Page 13



Out of the bag... (2)

- Now my NIC ID was – you guessed it...
00 60 08 d3 1d 03
- If you registered on line this was transmitted to M\$ and the file was deleted after transmission;
- There was the option not to send this, but whatever you chose it was sent anyway!
- The M\$ RegBase holds all the information to link an NIC to an individual!
- This is not necessarily restricted only to M\$.

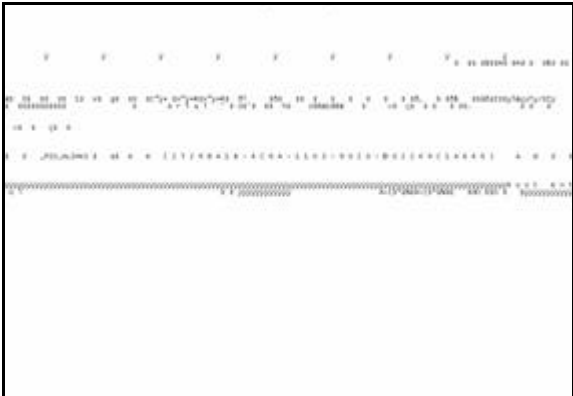
13th April 2005 © Forensic Computing Ltd 2005 Page 14




Out of the bag ... (3)

- So – if I open a M\$ Office file and know what I am doing I can identify the origin of a document;
- Chose a document;
- Open in Notepad;
- Search for _PID_GUID;
- Look what you find!


13th April 2005 © Forensic Computing Ltd 2005 Page 15



Out of the Bag ... (4) 

- Oh yes – and the NIC address is in cookies
- Is it in email?
- MS say that it is not possible to identify an originator of a document – but al you need is the process above;
- OK not the specific creator but the person who registered the software and the machine, check who sits there and whether they were in at the time

13th April 2005 © Forensic Computing Ltd 2005 Page 17

Metadata Proper 

Let's use Word as an Example


13th April 2005 © Forensic Computing Ltd 2005 Page 18

So to the Story!!

ABIG Plc

has received the following Word document and we have been asked to have a look at it.

13th April 2005 © Forensic Computing Ltd 2005 Page 19



ABIG PLC


To whom it may concern

I have got a copy of your product. If you don't pay me loads of wedge I will sell it to one of your competitors.


I will contact you with details of how to make the payment soon.

Pharaman


13th April 2005 © Forensic Computing Ltd 2005 Page 20




Using a hex viewer we can look below the document's surface and see some potential clues



13th April 2005 © Forensic Computing Ltd 2005 Page 21






Microsoft Word Time Stamps


- Word timestamps are 64-bit date and times, the 64 bits representing the number of nanoseconds since January 1, 1601.
- **Beware** Word takes its time stamps from the internal clock of the computer it is created on. If that computer's clock is set incorrectly then the document will reflect the incorrect time.

13th April 2005 © Forensic Computing Ltd 2005 Page 25



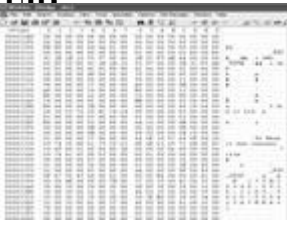
The _PID_GUID

13th April 2005 © Forensic Computing Ltd 2005 Page 26



A Hex view of part of Dodgy.doc

_PID_GUID




_PID_GUID {79B20940-5910-11D9-9965-000423A7EEA2}

The _PID_GUID is a VT_BLOB = DWORD count of bytes, followed by the same number of bytes of data. The byte count does not include the 4 bytes for the length of the count itself; an empty BLOB would have a count of 0 bytes. This is similar to VT_BSTR, but it does not guarantee a null byte at the end of the data.

13th April 2005 © Forensic Computing Ltd 2005 Page 27

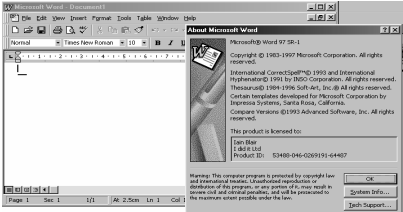
Which company manufactured the Network Card?



13th April 2005 © Forensic Computing Ltd 2005 Page 28


What are the licensing details of the Word application?

(Open the Word application and Select:- Help\About Microsoft Word)



13th April 2005 © Forensic Computing Ltd 2005 Page 29

MS Word settings can be found in the registry.



13th April 2005 © Forensic Computing Ltd 2005 Page 30

Some Microsoft resource documents that may be of assistance.



- WD97: Where Settings Are Stored in the Registry
<http://support.microsoft.com/kb/157464>
- Where settings are stored in the registry for Word 2000
<http://support.microsoft.com/kb/212242>


In Summary



- Dodgy.doc
- Word 97 document
- Born on 28th December 2004, 20:37:00
- Created on 28th December 2004, 20:38:50
- Signed by Pharaman but file properties show Author details as Iain Blair
- Company shown as 'I did it Ltd'
- MAC address of 000423A7EEA2, which shows that the NIC was manufactured by Intel Corporation

More hidden stuff without getting too complex






Same Colour Background and Text

- It is possible to bury a document or message in another file by using the same colour text as the background;
- An example is here:


13th April 2005 © Forensic Computing Ltd 2005 Page 34



How did we detect it?


<snip>
Comments:
No Comments
Font matching background:
Blocks of Font Matching Background: 1
Slide:Slide 3 Location: Text Box 4 Text box Rectangle
Small font (size 3 or smaller):
No text or shapes with small font
</snip>

13th April 2005 © Forensic Computing Ltd 2005 Page 35




Worryingly Clever

13th April 2005 © Forensic Computing Ltd 2005 Page 36

Hiding in a .wav file 


- Steganography – are of hidden writing;
- Use least significant bit – in this case a wav file;
- Can be used for all sorts of nasty things.

13th April 2005 © Forensic Computing Ltd 2005 Page 37

Getting more devious ... 

- Hiding text in a text file

13th April 2005 © Forensic Computing Ltd 2005 Page 38

Be Careful what you Leave Behind 

- Thumbs.db;
- Created by the system;
- Contains thumbnails of pictures in the folder;
- They may remain there after you have deleted the images;
- May not see thumbs.db – hidden file;
- Look what we find there!!!

13th April 2005 © Forensic Computing Ltd 2005 Page 39

