Computer Forensics

Catching and Convicting The Electronic Criminal

By

Dc Paul Tew Bsc(Hons) MBCS
Nottinghamshire Police (UK)
and
The Open University

The Role of Forensics in Computing

What is forensic computing?

Quite simply, the combination of

- Science
- Law

Computer Forensics – Where does it fit in?

Determining the nature and extent of incidents

Identifying and securing any evidence

Analysis of any evidence collected

Presentation of the evidence in court (if necessary)

Types of Incident

Disciplinary proceedings

Civil claims (as claimant or respondent)

Public accountability or reassurance

Criminal matters:

- Murder
- Serious sexual assault

Criminal matters (cont'd):

- Fraud
- Theft
- Child abuse photos/movies
- Bullying
- Stalking

A Case Exercise

Information:

Intelligence has been received from the Norwegian police that they have raided the premises of a server which was supplying unlawful pictures of teddy bears to the Internet. A recovered log file shows that on 2008-04-12 14:15:03 a picture was sent to the IP address 217.155.193.97 which is registered by Zen Internet in the UK.

What are the potential pitfalls?

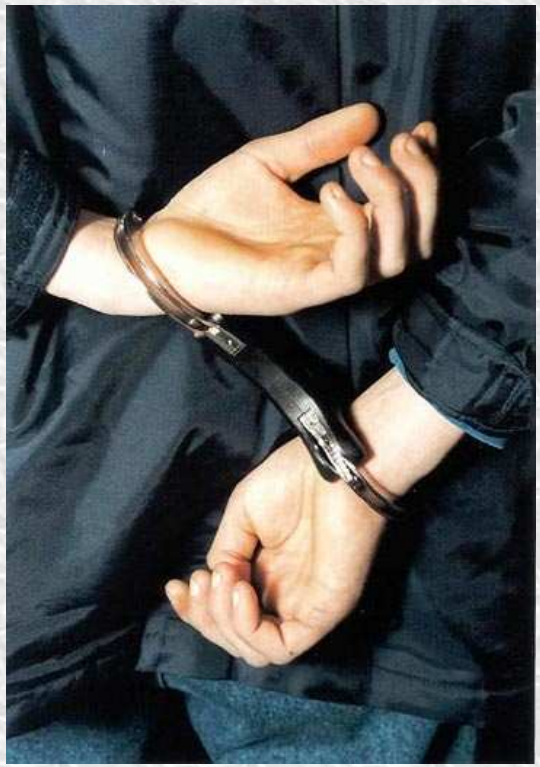
Is there enough information for the UK police to start an enquiry?

The Next Step

A police raid is organised to visit the address:

The Evidence

The suspect is arrested and a computer and ADSL wireless router are seized.



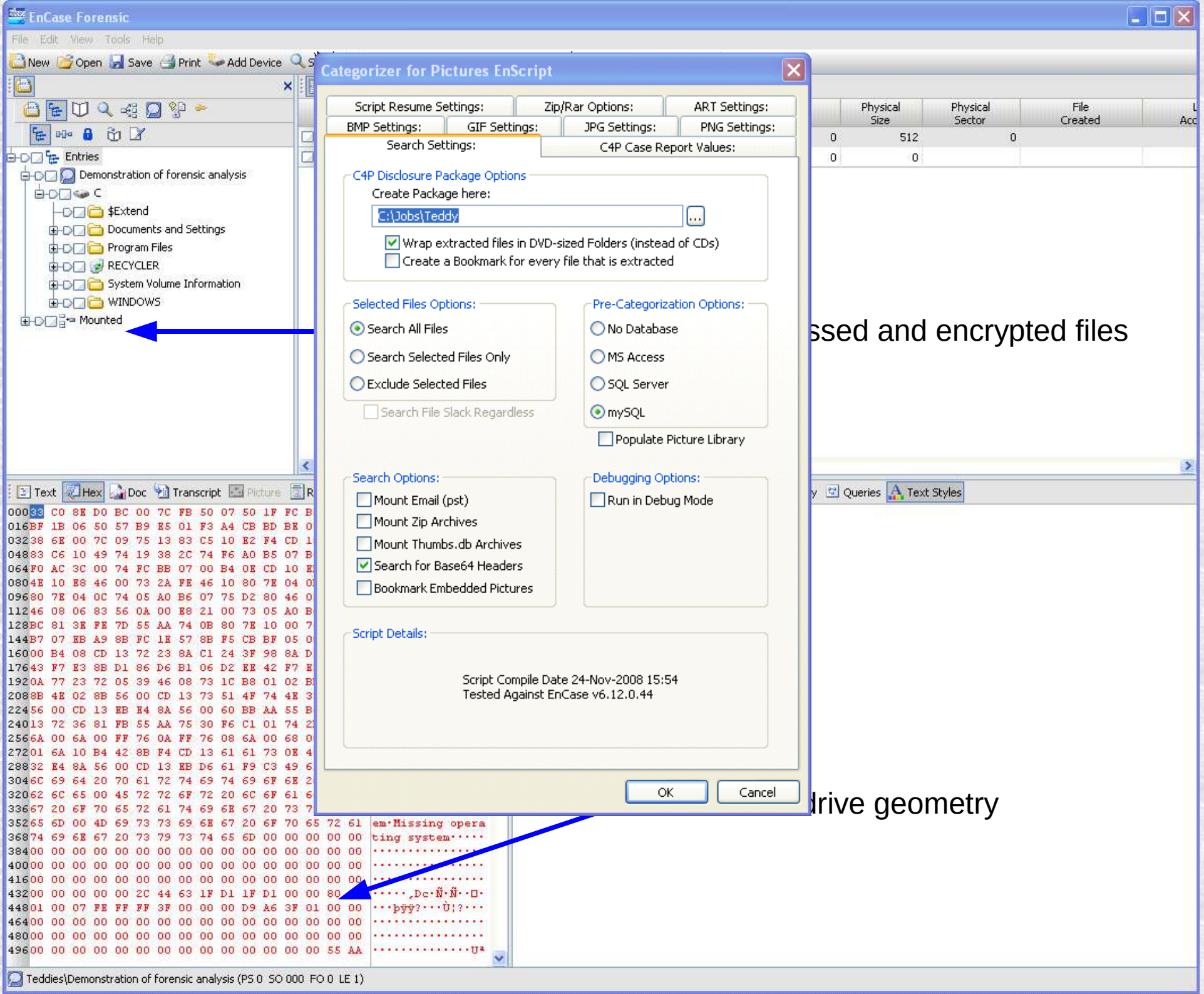
Data Acqusition

The data is extracted from the computer.

- The hard drive is removed
- The hard drive is attached to a forensic workstation via a write blocker

The computer BIOS is examined and the time is compared with the actual time.

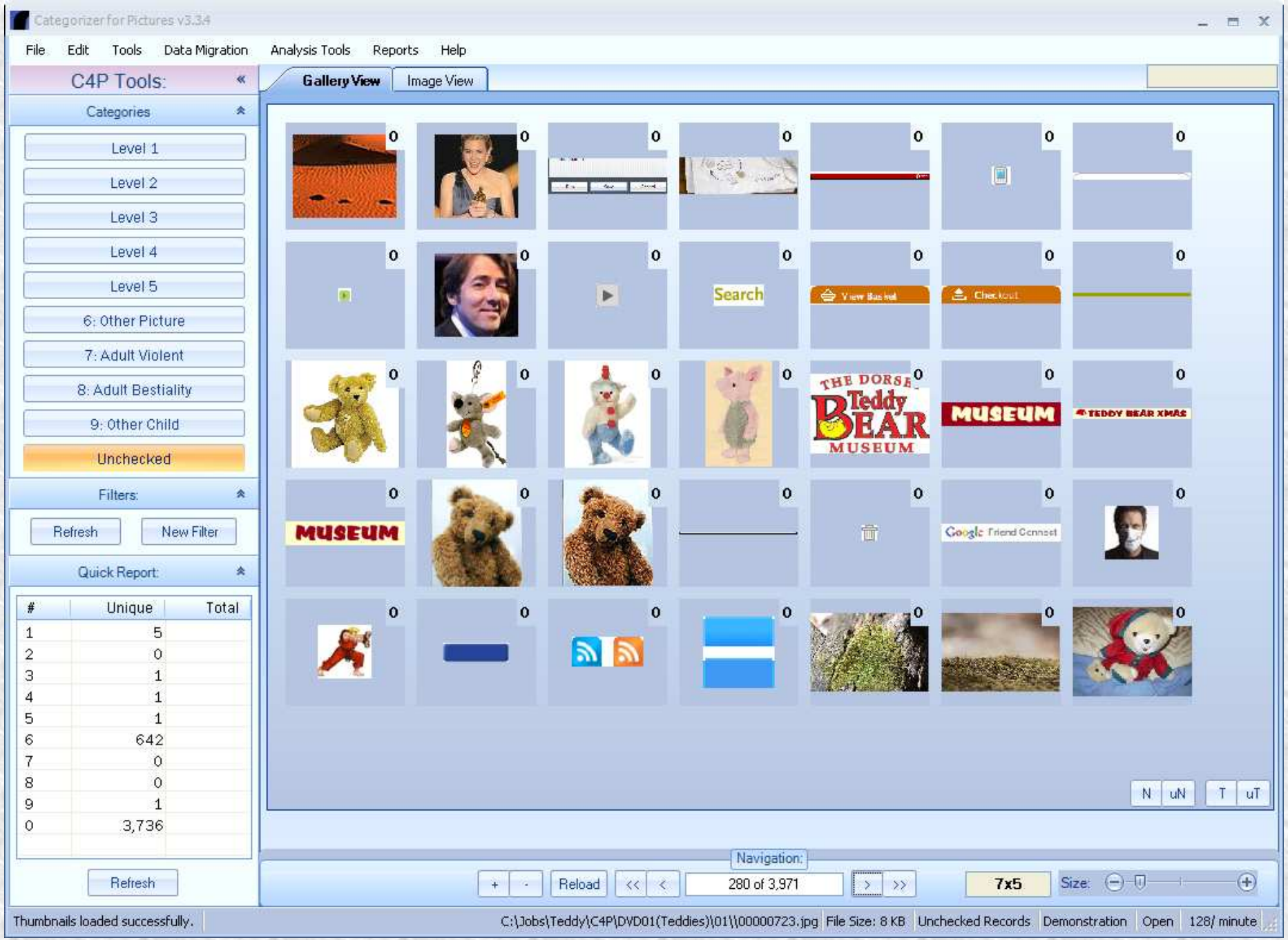
The settings on the router are examined.



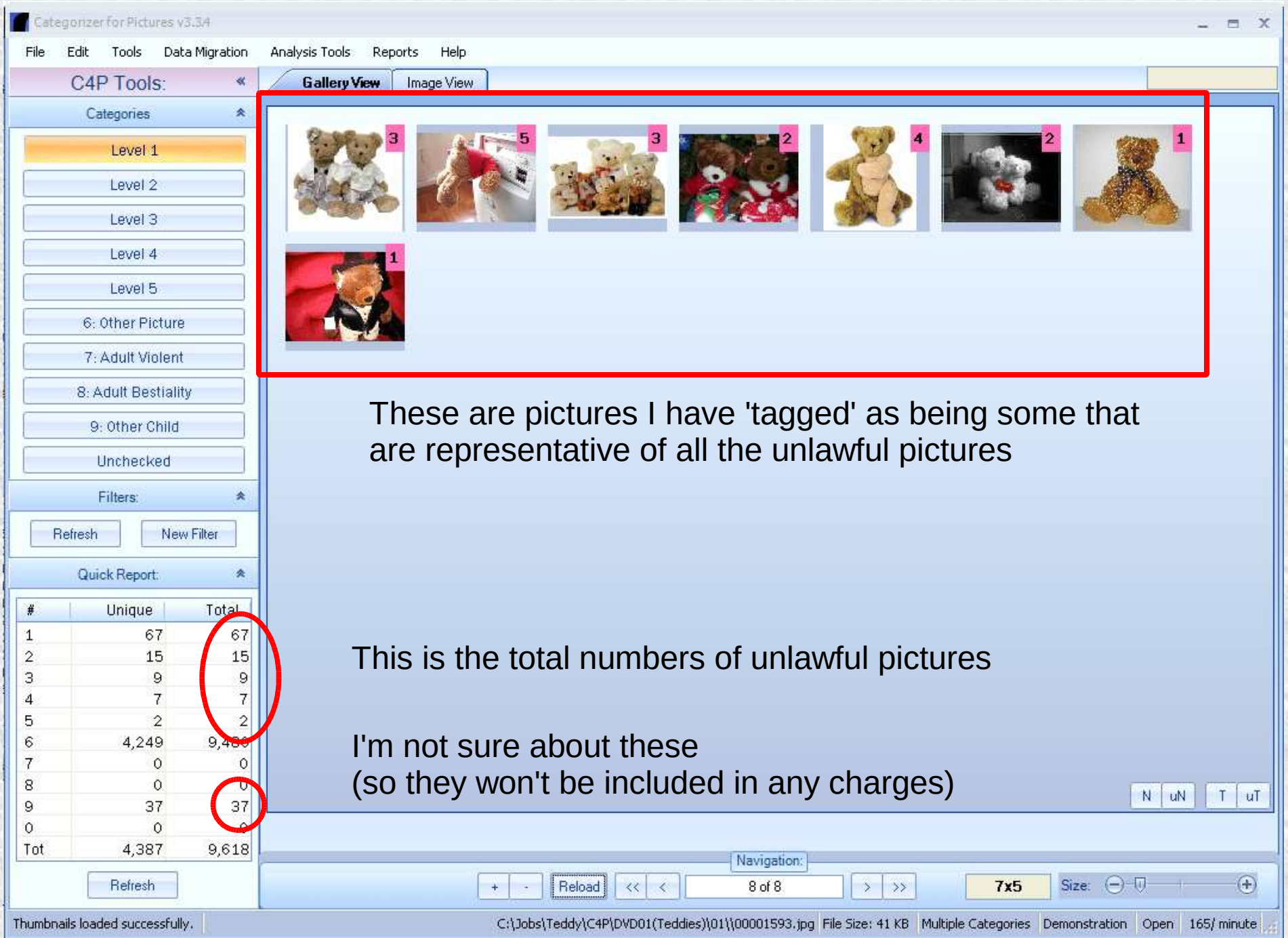
ssed and encrypted files

drive geometry

C4P – The Application



Refining the results



Working On Proof

Having selected some sample images we can now work on trying to prove how they came to be there.

The following slides are taken from an investigation using Brian Carrier's Sleuthkit and Autopsy tools (both open source). These are available from http://www.sleuthkit.org/

FILE ANALYSIS | KEYWORD SEARCH | FILE TYPE | IMAGE DETAILS | META DATA | DATA UNIT | HELP | CLOSE

Directory Seek

Enter the name of a directory that you want to view.
C: /

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

Current Directory: C:/ /Documents and Settings/ /Paul/ /My Documents/ /LimeWire/ /Saved/

ADD NOTE | GENERATE MD5 LIST OF FILES

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	S
	d / d	../	2009-03-24 08:44:32 (GMT)	2009-03-24 11:59:57 (GMT)	2009-03-24 08:44:32 (GMT)	2009-03-24 08:44:06 (GMT)	5
	d / d	./	2009-03-24 12:02:51 (GMT)	2009-03-24 12:02:51 (GMT)	2009-03-24 12:02:51 (GMT)	2009-03-24 08:44:32 (GMT)	5
	r / r	lovee_teddy_bears_by_MaggotEye.jpg	2009-03-24 11:59:52 (GMT)	2009-03-24 12:02:51 (GMT)	2009-03-24 12:00:52 (GMT)	2009-03-24 11:59:48 (GMT)	4
	r / r	Thumbs.db	2009-03-24 12:02:14 (GMT)	2009-03-24 12:02:12 (GMT)	2009-03-24 12:02:14 (GMT)	2009-03-24 12:02:12 (GMT)	1
	r / r	Thumbs.db:encryptable	2009-03-24 12:02:14 (GMT)	2009-03-24 12:02:12 (GMT)	2009-03-24 12:02:14 (GMT)	2009-03-24 12:02:12 (GMT)	(

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note
File Type: JPEG image data, JFIF standard 1.01

C:/Documents and Settings/Paul/My Documents/LimeWire/Saved/lovee_teddy_bears_by_MaggotEye.jpg

Thumbnail: View Full Size Image

This is the image I have chosen to investigate

This is the date it was created (on this partition)

And the full path is:

C:\Documents and Settings\Paul\My Documents\LimeWire\Saved\lovee_teddy_bears_by_MaggotEye.jpg

Working On Proof (continued)

The photographwas created on this machine on 2009-03-24 11:59:48 and is located at C:\Documents and Settings\Paul\My Documents\Limewire\Saved.
It is named lovee_teddy_bears_by_MaggotEye.jpg

- What hypotheses can we make about the origin of this photo from just this information?
- What enquiries and investigations do we now need to make?
  - What artifacts does Limewire leave behind in normal use and are they present on this machine?
  - What other references are there on this machine to this particular photo?

Working On Proof (continued) Investigating LimeWire

What version?

How are you going to investigate?

Virtual machine

Clone drive

What tools?

Sysinternals

Process Monitor

Process Explorer

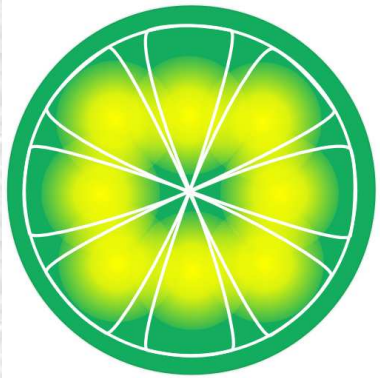
Wireshark

What artifacts are you looking for?

Settings

User generated material

Why does this need to be done?

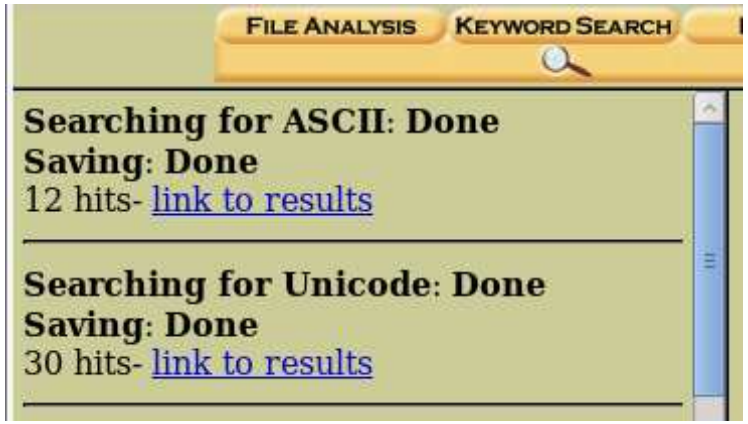


Working On Proof (continued)
The Photo

Now we know how LimeWire works, how do we investigate the photo?

Remember the name is:
lovee_teddy_bears_by_MaggotEye.jpg

Working On Proof (continued)
A Text Search

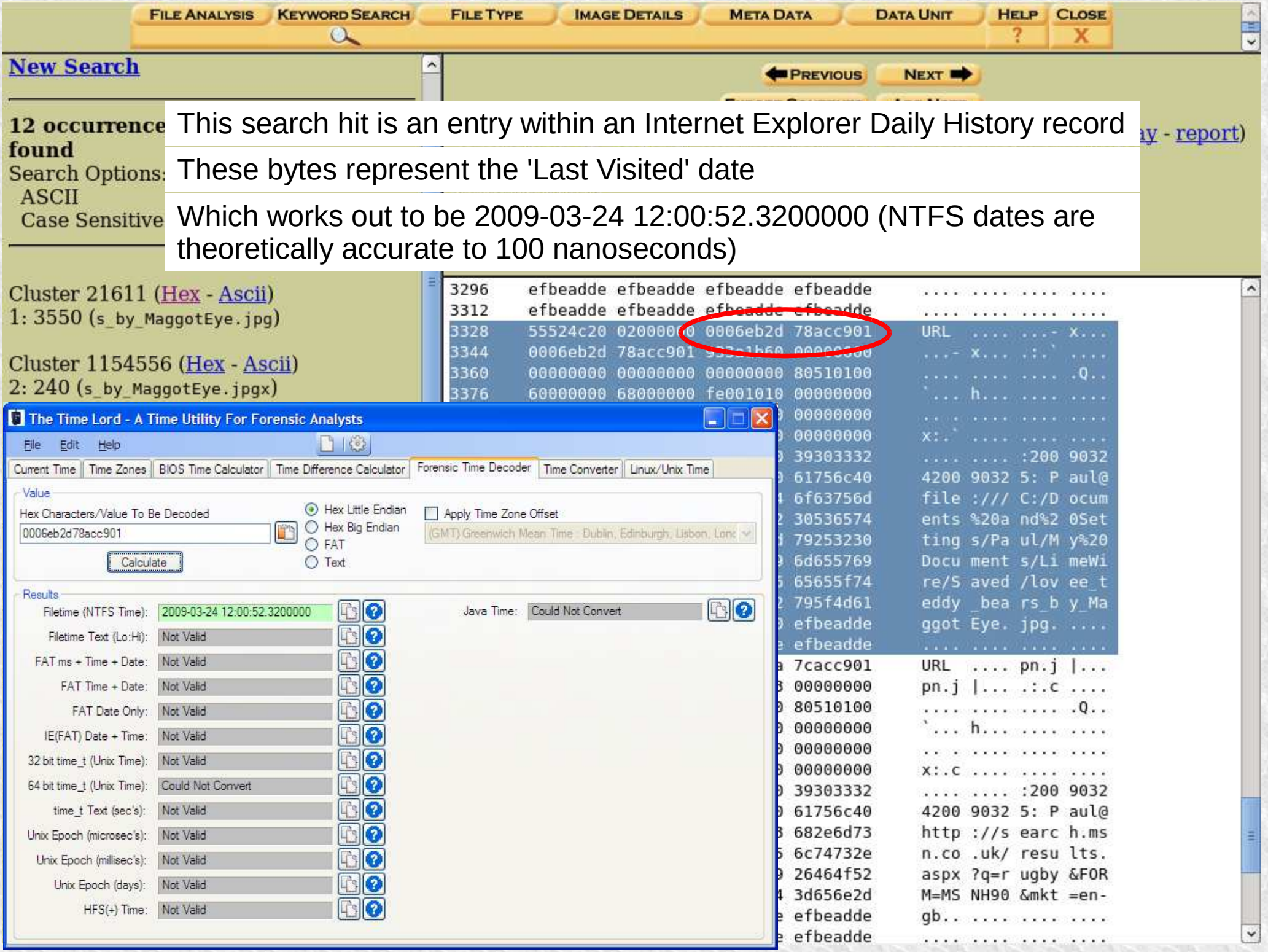


Working On Proof (continued)
Text Search Results

The results of the text search in this case were within:

- Internet Explorer history records (x 2)
- Registry files (1 active and 2 deleted registry hives)
- A link (shortcut) file in the ...\Paul\Recent folder
- 3 x Limewire files (a download database, a library and a properties file)
- $MFT entries for the photo and the link file
- INDX entries for the photo and the link file

Lets examine a couple of these hits in more detail:


FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
New Search
PREVIOUS
NEXT
12 occurrence
found
Search Options:
ASCII
Case Sensitive
ay - report)
This search hit is an entry within an Internet Explorer Daily History record
These bytes represent the 'Last Visited' date
Which works out to be 2009-03-24 12:00:52.3200000 (NTFS dates are theoretically accurate to 100 nanoseconds)
Cluster 21611 (Hex - Ascii)
1: 3550 (s_by_MaggotEye.jpg)
Cluster 1154556 (Hex - Ascii)
2: 240 (s_by_MaggotEye.jpgx)
3296 efbeadde efbeadde efbeadde efbeadde
3312 efbeadde efbeadde efbeadde efbeadde
3328 55524c20 02000000 0006eb2d 78acc901
3344 0006eb2d 78acc901
3360 00000000 00000000 00000000 80510100
3376 60000000 68000000 fe001010 00000000
URL
The Time Lord - A Time Utility For Forensic Analysts
File Edit Help
Current Time
Time Zones
BIOS Time Calculator
Time Difference Calculator
Forensic Time Decoder
Time Converter
Linux/Unix Time
Value
Hex Characters/Value To Be Decoded
0006eb2d78acc901
Calculate
Hex Little Endian
Hex Big Endian
FAT
Text
Apply Time Zone Offset
(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, Lond
Results
Filetime (NTFS Time): 2009-03-24 12:00:52.3200000
Java Time: Could Not Convert
Filetime Text (Lo:Hi): Not Valid
FAT ms + Time + Date: Not Valid
FAT Time + Date: Not Valid
FAT Date Only: Not Valid
IE(FAT) Date + Time: Not Valid
32 bit time_t (Unix Time): Not Valid
64 bit time_t (Unix Time): Could Not Convert
time_t Text (sec's): Not Valid
Unix Epoch (microsec's): Not Valid
Unix Epoch (millisec's): Not Valid
Unix Epoch (days): Not Valid
HFS(+) Time: Not Valid

Searching for ASCII: Done
Saving: Done
12 hits- link to results

Searching for Unicode: Done
Saving: Done
30 hits- link to results

New Search

12 occurrences of MaggotEye were found
Search Options:
ASCII
Case Sensitive

Cluster 21611 (Hex - Ascii)
1: 3550 (s_by_MaggotEye.jpg)

Cluster 1154556 (Hex - Ascii)
2: 240 (s_by_MaggotEye.jpgx)

Cluster 1154557 (Hex - Ascii)
3: 747 (s_by_MaggotEye.jpgw)

Cluster 1160701 (Hex - Ascii)
4: 463 (s_by_MaggotEye.jpg)

Cluster 1162574 (Hex - Ascii)
5: 179 (s_by_MaggotEye.jpg;)

Cluster 1352195 (Hex - Ascii)
6: 141 (s_by_MaggotEye.lnk)
7: 1589 (s_by_MaggotEye.lnk)

Cluster 1428728 (Hex - Ascii)
8: 1669 (s_by_MaggotEye.lnk)
9: 1925 (s_by_MaggotEye.lnk)

Cluster 1433112 (Hex - Ascii)
10: 1876 (s_by_MaggotEye.jpg)

Cluster 1494512 (Hex - Ascii)
11: 2693 (s_by_MaggotEye.lnk)
12: 2949 (s_by_MaggotEye.lnk)

PREVIOUS | NEXT
EXPORT CONTENTS | ADD NOTE

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)
File Type: ASCII English text, with very long lines, with CRLF line terminators

Cluster: 1162574
Status: Allocated
Hide Meta Data Address
Pointed to by MFT Entry: 16392-128-4
Pointed to by file: C:/Documents and Settings/Paul/Application Data/LimeWire/limewire.props

ASCII Contents of Cluster 1162574 in Teddy-63-20948759

```
#LimeWire properties file
#Tue Mar 24 12:01:41 GMT 2009
MAX_SKIP_ACKS=2
RECENT_DOWNLOADS=C\:\\Documents and Settings\\Paul\\My Documents\\LimeWire\\Saved\\lovee_teddy_bears_by_MaggotEye.jpg;C\:\\Docu
ENABLE_DHT_ALT_LOC_QUERIES=true
LAST_ACCEPTABLE_BUG_VERSION=4.17.6
INSPECTOR_IPS=76.8.67.27
ENABLE_PUSH_PROXY_QUERIES=true
WINDOW_X_V5=290
GEO_LOCATION=\#props\r\n\#Tue Mar 24 11\:55\:13 GMT 2009\r\nAreaCode\=0\r\nDmaCode\=0\r\nLatitude\=51.200001\r\nCity\=Farnham\
LIBRARY_VERSION=FIVE_0_0
MIN_ACTIVE_DHT_AVERAGE_UPTIME=1800000
UPDATE_DOWNLOAD_DELAY=14400001
UPDATE_RETRY_DELAY=1800001
UPDATE_GIVEUP_FACTOR=49
AVERAGE_CONNECTION_TIME=506045
SESSIONS=2
LAST_FILECHOOSER_DIR=C\:\\Documents and Settings\\Paul
BUCKET_ID_MODULUS=40000
MANAGE_OTHER_FILES=false
POSITIONS_SET=true
MAX_UPLOAD_BYTES_PER_SEC=6
FRACTIONAL_UPTIME=8.6602184E-4
FILTER_HASH_QUERIES=true
LAST_EXPIRE_TIME=1237884208027
WINDOW_Y_V5=50
MIN_PASSIVE_LEAF_DHT_INITIAL_UPTIME=300000
MIN_PASSIVE_LEAF_DHT_AVERAGE_UPTIME=60000
SEARCH_VIEW_TYPE_ID=0
TOTAL_CONNECTIONS=1
PORT=18531
LIME_QRP_ENTRIES=lime;wire;limewire;pro;limewirepro
CONTENT_AUTHORITIES=fserv1.limewire.com\:10000
UPDATE_STYLE=1
CRAWLER_IPS=76.8.67.27;
PUBLISH_ALT_LOCS=true
```

Working On Proof (continued)
Search Results Revisited

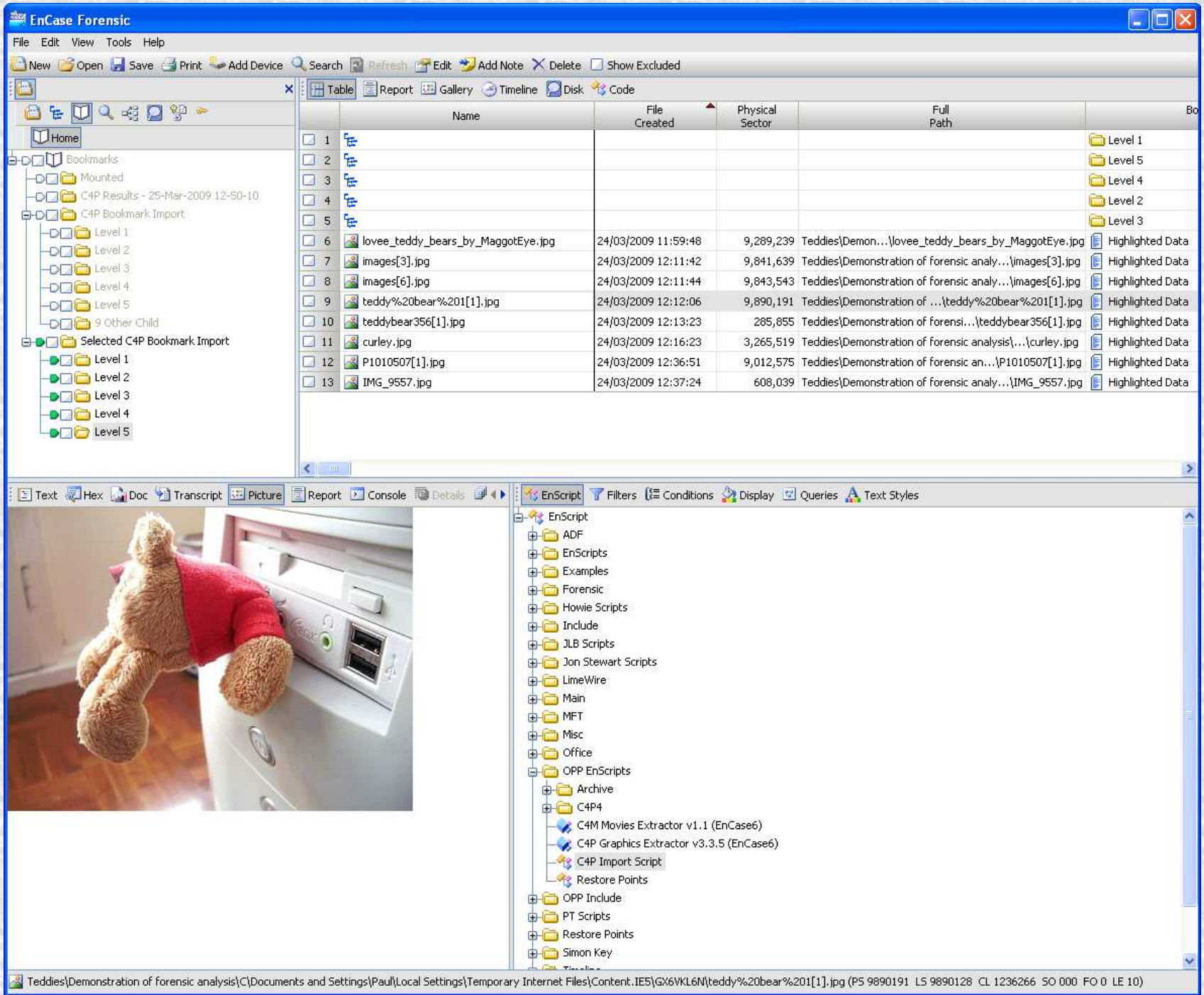
In this case all the hits for 'MaggotEye' are consistent with LimeWire having downloaded the file into it's current location.

What if any of the findings were inconsistent, what do we do with these?

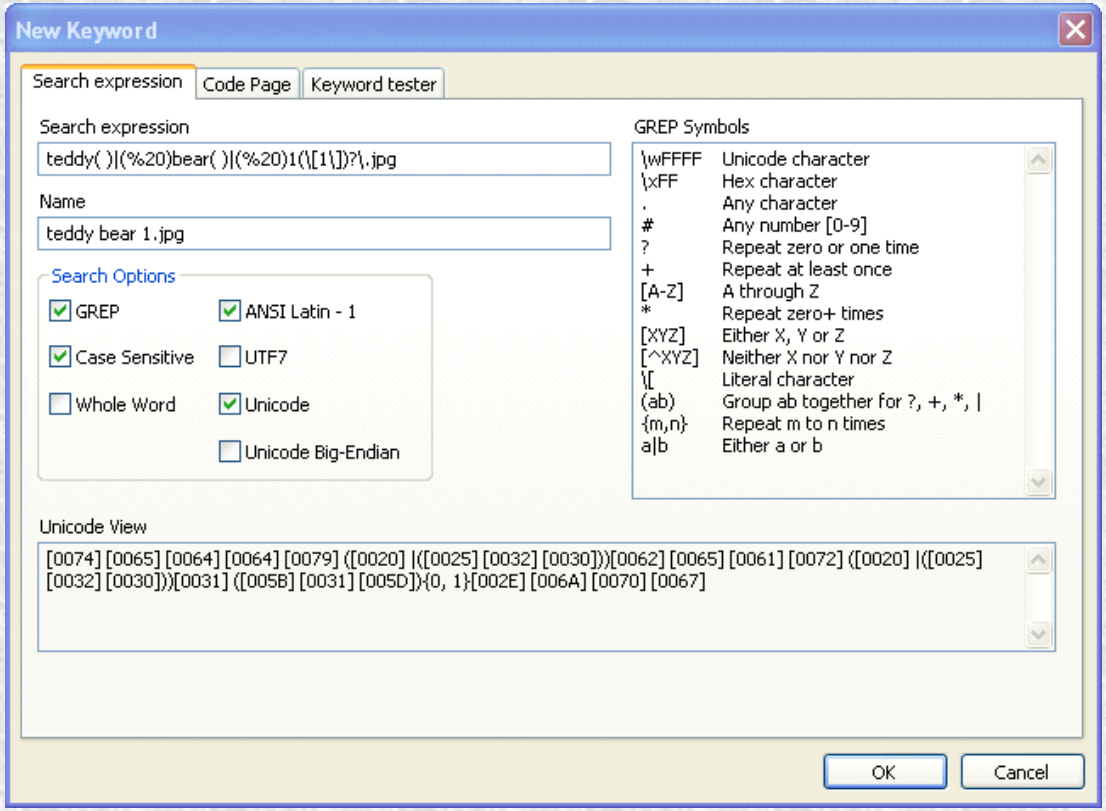
Working On Proof (continued) Another Photo

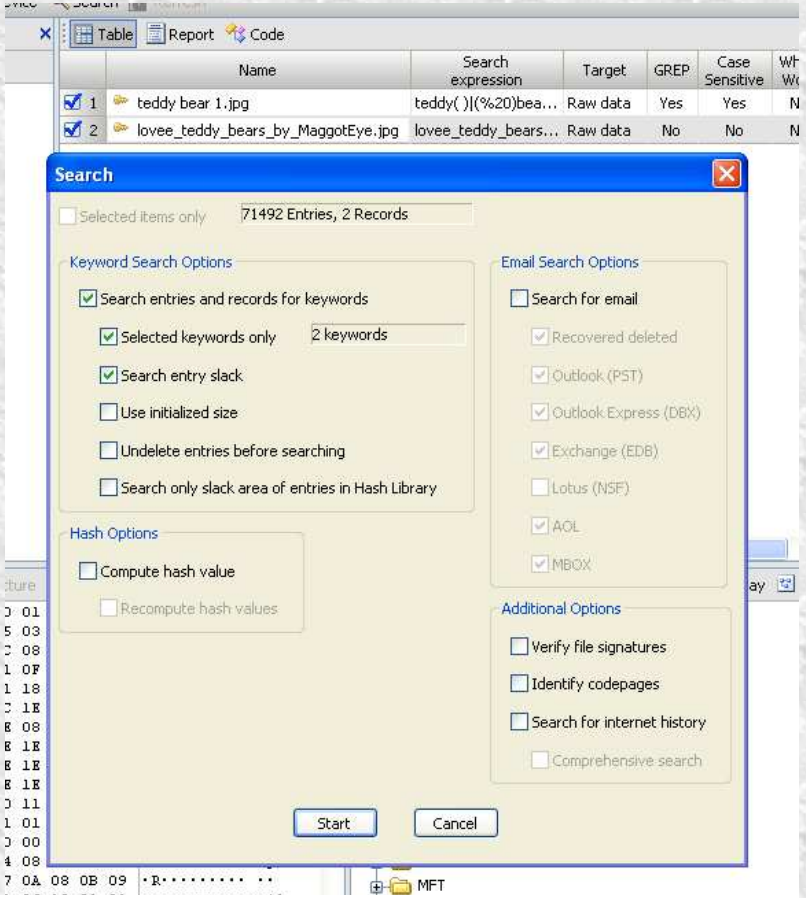
- Lets (very quickly) have a look at investigating an image from a web page.
- The following slides are taken from an investigation using EnCase® from Guidance Software

Working On Proof (continued)



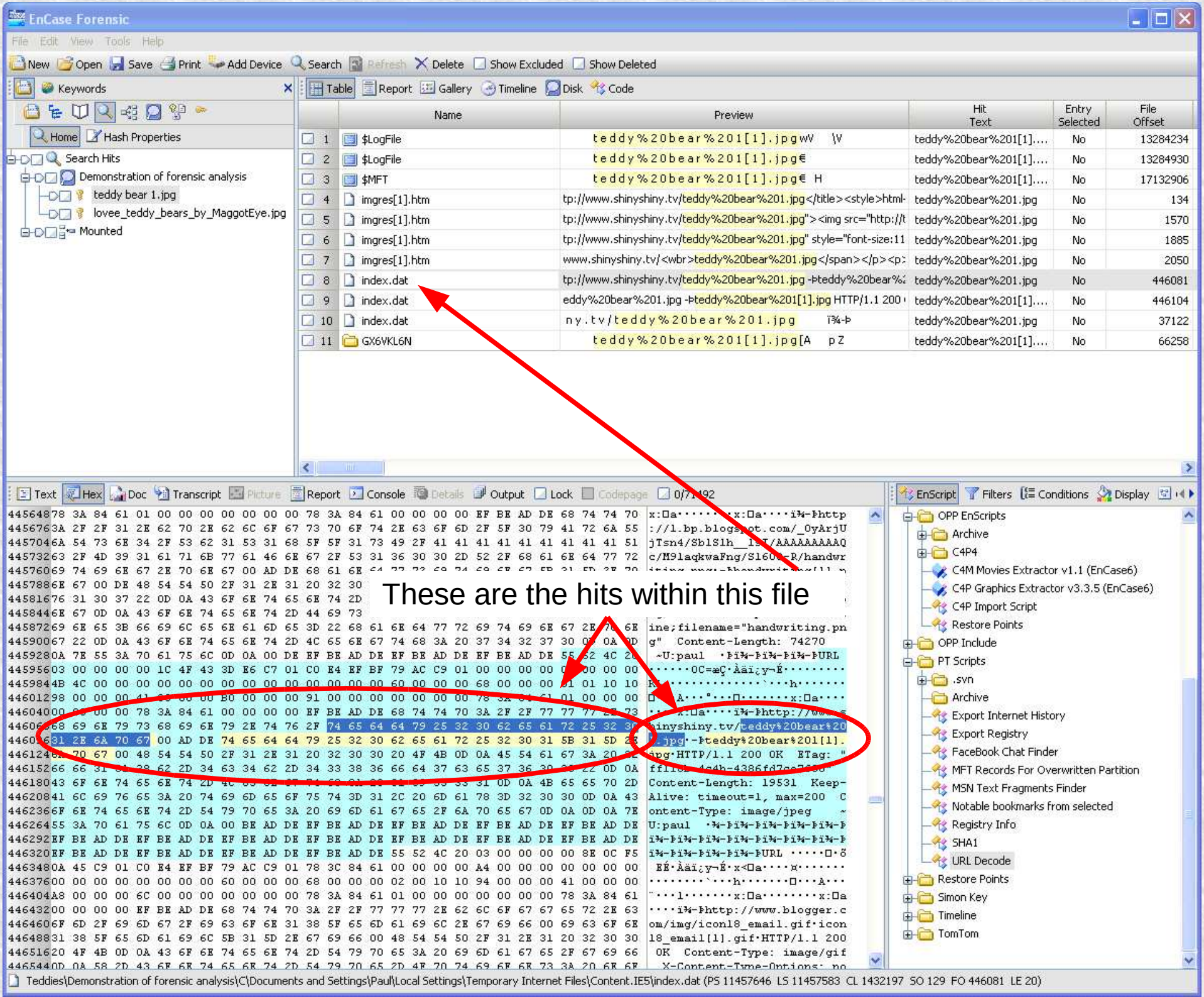
Working On Proof (continued)
EnCase Text Search





Search Summary

Hits	First Searched	Last Searched	Search Text
11	25/03/2009 14:38:26	25/03/2009 14:38:26	teddy( )|(%20)bear( )|(%20)1(\[1\])?\.jpg
6	25/03/2009 14:38:26	25/03/2009 14:38:26	lovee_teddy_bears_by_MaggotEye.jpg

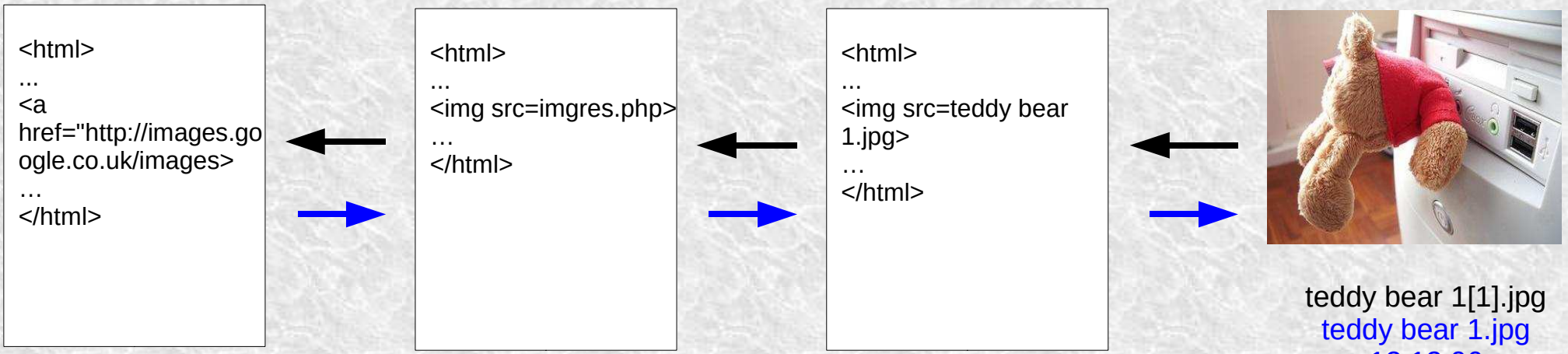

EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Delete Show Excluded Show Deleted
Keywords
Home Hash Properties
Search Hits
Demonstration of forensic analysis
teddy bear 1.jpg
lovee_teddy_bears_by_MaggotEye.jpg
Mounted
Table Report Gallery Timeline Disk Code
Name Preview Hit Text Entry Selected File Offset
1 $LogFile teddy%20bear%201[1].jpg teddy%20bear%201[1].... No 13284234
2 $LogFile teddy%20bear%201[1].jpg teddy%20bear%201[1].... No 13284930
3 $MFT teddy%20bear%201[1].jpg teddy%20bear%201[1].... No 17132906
4 imgres[1].htm tp://www.shinyshiny.tv/teddy%20bear%201.jpg</title><style>html- teddy%20bear%201.jpg No 134
5 imgres[1].htm tp://www.shinyshiny.tv/teddy%20bear%201.jpg"><img src="http://t teddy%20bear%201.jpg No 1570
6 imgres[1].htm tp://www.shinyshiny.tv/teddy%20bear%201.jpg" style="font-size:11 teddy%20bear%201.jpg No 1885
7 imgres[1].htm www.shinyshiny.tv/<wbr>teddy%20bear%201.jpg</p><p: teddy%20bear%201.jpg No 2050
8 index.dat tp://www.shinyshiny.tv/teddy%20bear%201.jpg -Þteddy%20bear%2 teddy%20bear%201.jpg No 446081
9 index.dat eddy%20bear%201.jpg -Þteddy%20bear%201[1].jpg HTTP/1.1 200 teddy%20bear%201[1].... No 446104
10 index.dat ny.tv/teddy%20bear%201.jpg ï¾-Þ teddy%20bear%201.jpg No 37122
11 GX6VKL6N teddy%20bear%201[1].jpg[A pZ teddy%20bear%201[1].... No 66258
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/71492
These are the hits within this file
EnScript Filters Conditions Display
OPP EnScripts
Archive
C4P4
C4M Movies Extractor v1.1 (EnCase6)
C4P Graphics Extractor v3.3.5 (EnCase6)
C4P Import Script
Restore Points
OPP Include
PT Scripts
.svn
Archive
Export Internet History
Export Registry
FaceBook Chat Finder
MFT Records For Overwritten Partition
MSN Text Fragments Finder
Notable bookmarks from selected
Registry Info
SHA1
URL Decode
Restore Points
Simon Key
Timeline
TomTom
Teddies\Demonstration of forensic analysis\C\Documents and Settings\Paul\Local Settings\Temporary Internet Files\Content.IE5\index.dat (PS 11457646 LS 11457583 CL 1432197 SO 129 FO 446081 LE 20)

Working on Proof (continued) EnCase Search Hit

```
Internet Explorer URL Cache Record

Located in:
Demonstration of forensic analysis\C\Documents and Settings\Paul\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
At offset: 445952

Web server last modified time:     24/08/2007 10:55:20 (UTC)
Local machine last modified time:  24/03/2009 12:12:06 (UTC)
File size:                         19531 bytes
Cache folder number:               1
Cache folder name:                 GX6VKL6N
File last accessed:                24/03/2009 12:12:08 (UTC) (rounded up)
Hits:                              1
File created:                      24/03/2009 12:12:08 (UTC) (rounded up)
URL:
http://www.shinyshiny.tv/teddy%20bear%201.jpg

Cache filename:
teddy%20bear%201[1].jpg

HTTP GET response:
--------Start---------

HTTP/1.1 200 OK
ETag: "ff118b-4c4b-4386fd7ce7600"
Content-Length: 19531
Keep-Alive: timeout=1, max=200
Content-Type: image/jpeg

---------End---------

Username:                          paul
```

	A	B	C
1	**Last access (UTC)**	**Entry type**	**Address (URL)**
791	24/03/2009 12:11:14	Cache / URL	http://www.teddybearhouse.co.uk/images/dtbm.gif
792	24/03/2009 12:11:14	Cache / URL	http://www.teddybearhouse.co.uk/images/menu/xmas_up.gif
793	24/03/2009 12:11:14	Cache / URL	http://www.teddybearhouse.co.uk/images/menu/home_up.gif
794	24/03/2009 12:11:14	Cache / URL	http://www.teddybearhouse.co.uk/images/menu/buy_up.gif
795	24/03/2009 12:11:15	Cache / URL	http://www.teddybearhouse.co.uk/images/menu/museum_over.gif
796	24/03/2009 12:11:15	History	http://www.teddybearhouse.co.uk
797	24/03/2009 12:11:15	Cache / URL	http://www.teddybearhouse.co.uk/images/menu/house_over.gif
798	24/03/2009 12:11:15	Cache / URL	http://www.teddybearhouse.co.uk/images/menu/buy_over.gif
799	24/03/2009 12:11:15	Cache / URL	http://www.teddybearhouse.co.uk/images/menu/home_over.gif
800	24/03/2009 12:11:15	Cache / URL	http://www.teddybearhouse.co.uk/images/menu/xmas_over.gif
801	24/03/2009 12:11:15	Cache / URL	http://www.teddybearhouse.co.uk/images/menu/shop_over.gif
802	24/03/2009 12:11:21	Cache / URL	http://www.google.co.uk/search?hl=en&q=teddy bear&start=10&sa=N
803	24/03/2009 12:11:28	History	http://www.google.co.uk/search?hl=en&q=teddy bear&start=10&sa=N
804	24/03/2009 12:11:33	History	http://www.google.co.uk/search?hl=en&q=teddy bear&start=10&sa=N
805	24/03/2009 12:11:46	History	:Host: images.google.co.uk
806	24/03/2009 12:11:47	Cache / URL	http://images.google.co.uk/favicon.ico
807	24/03/2009 12:12:03	Cache / URL	http://images.google.co.uk/imgres?imgurl=http://www.shinyshiny.tv/teddy%20bear%201.jpg&imgref
808	24/03/2009 12:12:05	Cache / URL	http://www.blogger.com/dyn-css/authorization.css?targetBlogID=30096512275057616?&zx=02fa9c
809	24/03/2009 12:12:05	Cache / URL	http://www.blogger.com/widgets/2300090209-widget_css_bundle.css
810	24/03/2009 12:12:05	Cache / URL	http://www.blogger.com/v-css/3727950723-blog_controls.css
811	24/03/2009 12:12:06	Cache / URL	http://tbn0.google.com/images?q=tbn:nC7mzSUf8lqspM:http://www.collectibleteddybearsonline.com
812	24/03/2009 12:12:06	Cache / URL	http://www.blogger.com/img/icon18_email.gif
813	24/03/2009 12:12:06	Cache / URL	http://www.blogblog.com/rounders2/corners_cap_bot.gif
814	24/03/2009 12:12:06	Cache / URL	http://www.shinyshiny.tv/teddy bear 1.jpg
815	24/03/2009 12:12:06	Cache / URL	http://www.blogger.com/img/icon18_edit_allbkg.gif
816	24/03/2009 12:12:06	Cache / URL	http://1.bp.blogspot.com/_0yArjUjTsn4/Sb1S1h__1sI/AAAAAAAAAQc/M91aqkwaFng/S1600-R/han
817	24/03/2009 12:12:06	Cache / URL	http://www2.blogblog.com/rounders2/corners_cap_top.gif
818	24/03/2009 12:12:07	Cache / URL	http://www1.blogblog.com/rounders2/corners_main_top.gif
819	24/03/2009 12:12:07	Cache / URL	http://www1.blogblog.com/rounders2/corners_main_bot.gif
820	24/03/2009 12:12:07	Cache / URL	http://www.blogblog.com/rounders2/rails_main.gif
821	24/03/2009 12:12:07	Cache / URL	http://www.blogger.com/jsbin/1164304776-iframe_colorizer.js
822	24/03/2009 12:12:07	Cache / URL	http://www.blogger.com/img/icon_delete13.gif
823	24/03/2009 12:12:07	Cache / URL	http://www2.blogblog.com/rounders2/icon_arrow.gif
824	24/03/2009 12:12:08	Cache / URL	http://i146.photobucket.com/albums/r251/sergio1984/Picture069.jpg
825	24/03/2009 12:12:09	Cache / URL	http://img1.blogblog.com/img/icon18_wrench_allbkg.png
826	24/03/2009 12:12:09	Cache / URL	http://farm4.static.flickr.com/3407/3180648050_0f265f06d2.jpg?v=0

Working on Proof (continued)
The Evidence Chain



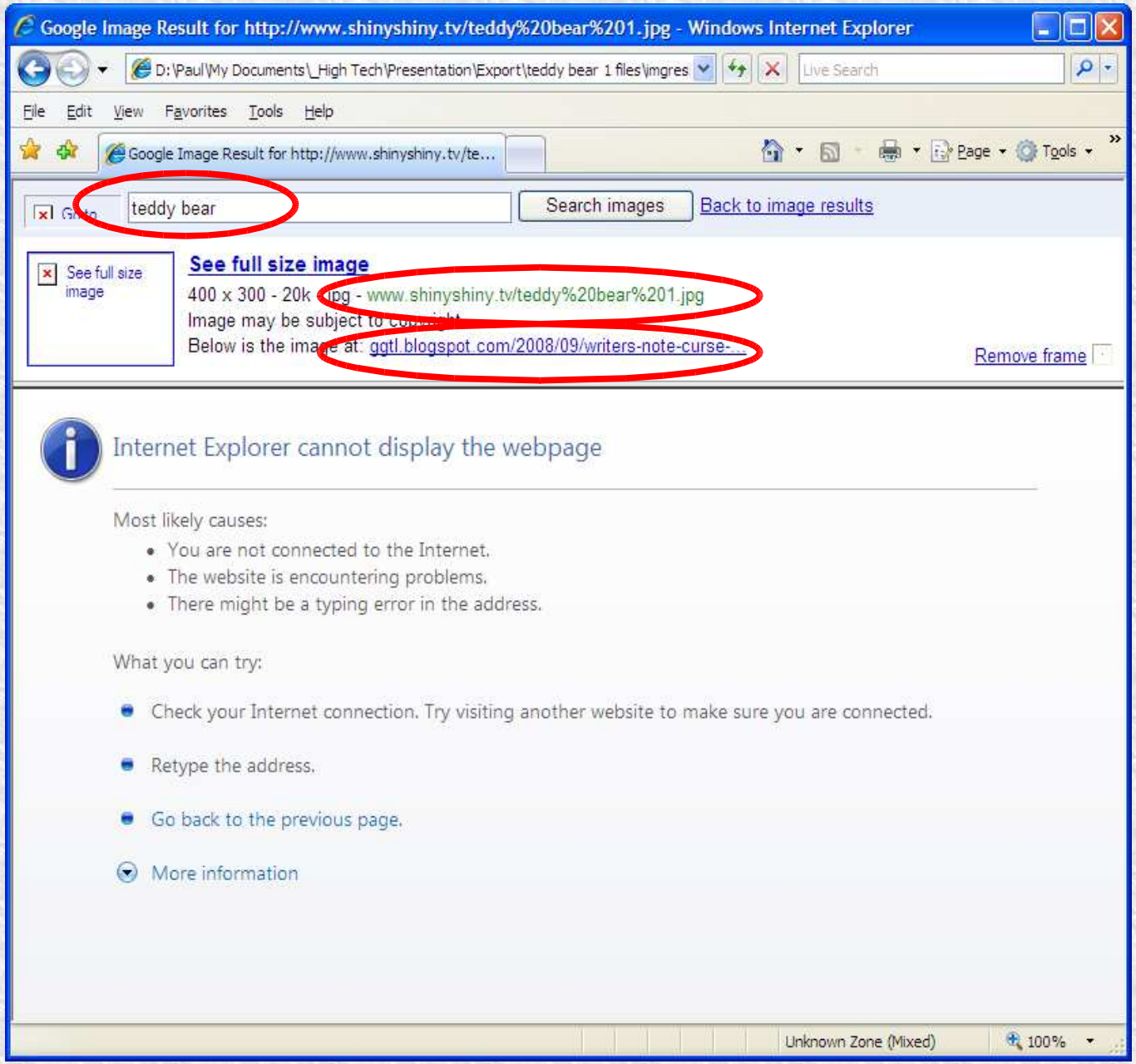
search[3].htm
search.php
12:11:21

images[1].htm
images.php
12:11:46

imgres[1].htm
imgres.php
12:12:03

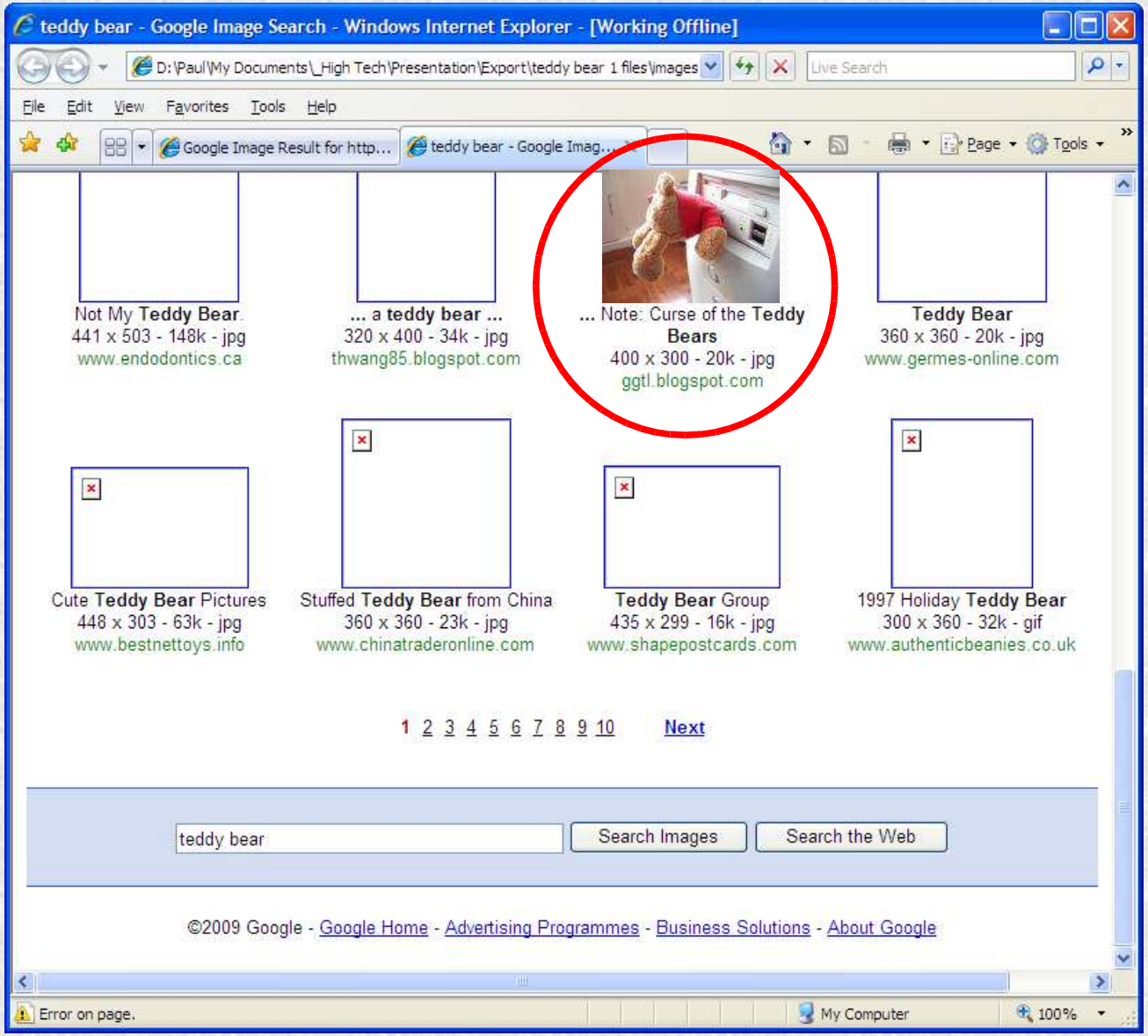
teddy bear 1[1].jpg
teddy bear 1.jpg
12:12:06

Working On Proof (continued)



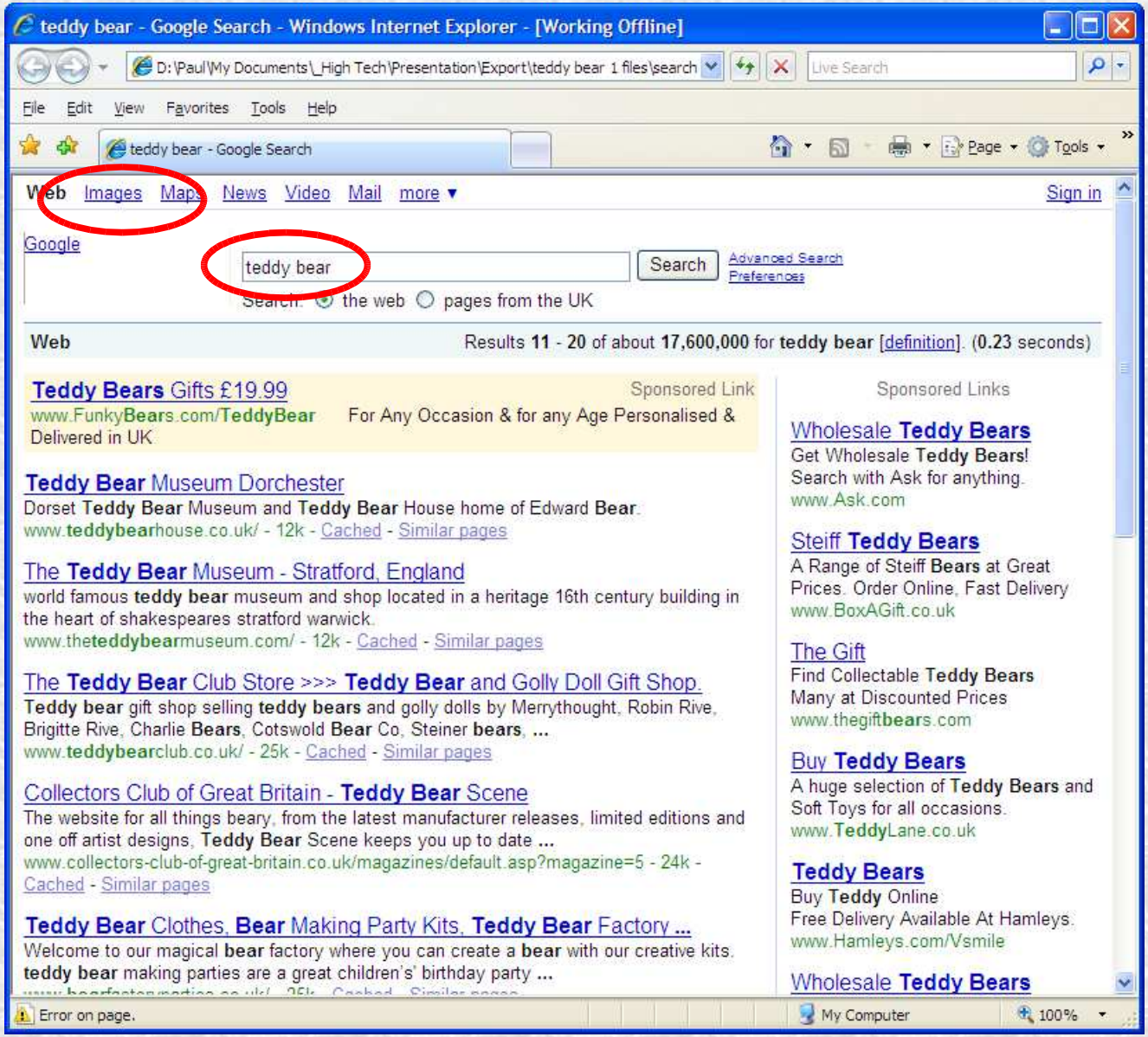
imgres[1].htm

Working On Proof (continued)



images[1].htm

Working On Proof (continued)



search[4].htm

Working On Proof (continued) Summing Up

Two photos

- 1 apparently downloaded using LimeWire
- 1 Apparently browsed to by following a Google search

All the other chosen pictures are the same (Limewire or Web photos)

All the times and dates are consistent with each other and with the user having initiated the actions

Is there enough evidence to prosecute?

After The Analysis

You may think that the work of a computer forensic analyst stops there, in fact there is much yet to be done:

- A technical report (which can be quite large)
- Assist the officer in the case to interview the suspect
- Assist in the prosecution case
- Assist the CPS to understand the technical aspects
- Liase with the prosecution team prior to a court case
- Liase with the defence expert

Computer Forensics

Catching and Convicting The Electronic Criminal

By

Dc Paul Tew Bsc(Hons) MBCS
Nottinghamshire Police (UK)
and
The Open University