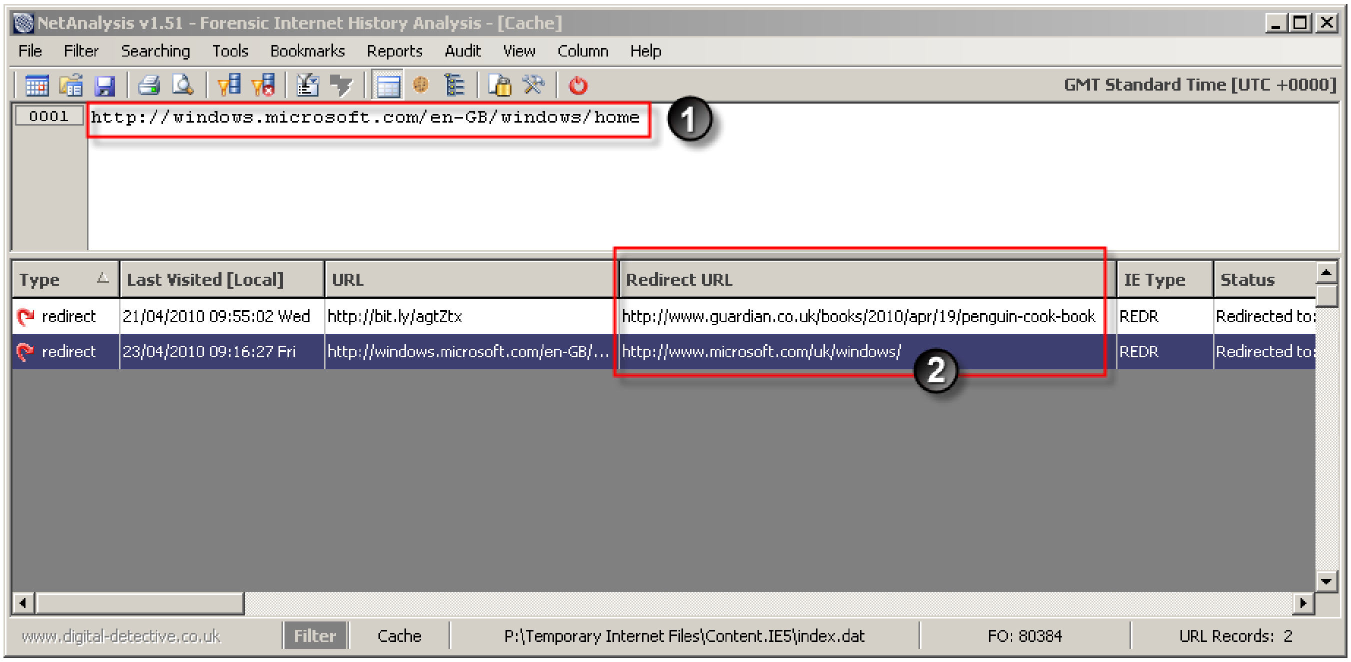
Redirects

Redirects in Microsoft Internet Explorer

Embedded within the CACHE INDEX.DAT file are numerous Internet records that have REDR as the record header. This header is a REDIRECT entry and is evidence of a SERVER-SIDE redirect. Client Side redirects are NOT recorded within the INDEX.DAT files as REDR records. The REDR entry is a URL that has been visited and the server has responded with an HTTP 300 response which tells the browser the page is in a different location. This entry reflects the URL which caused the redirection. the entries are marked as Type: Redirect with the entry shown below.

redirect

In previous versions of NetAnalysis, we were not able to show where the user was redirected to. Following research and testing, we identified a methodology for resolving redirect entries. However, it is only possible to show the resulting redirected URL if the data still exists within the INDEX.DAT record. There is a marker to indicate whether the entry is live or deleted. It is also only possible to show resulting redirect entries from live INDEX.DAT files. It is not possible to do this with the data recovered by HstEx. This is a significant development in the analysis of Internet browser artefacts as previously, the investigator did not have this information. At the time of writing this Article, NetAnalysis v1.50+ is the only software available to extract this important evidence. In addition to identifying the URL where the user was redirected to, it is also possible to identify the date/time this action occurred. This also was not previously possible. The status column informs the examiner whether the redirect entry is intact or not. If it is intact and from a live INDEX.DAT file, there will be date/time information. As mentioned previously, this data is not available for overwritten or deleted redirect entries.


NetAnalysis v1.51 - Forensic Internet History Analysis - [Cache]
File
Filter
Searching
Tools
Bookmarks
Reports
Audit
View
Column
Help
GMT Standard Time [UTC +0000]
1
2

```
0001  http://windows.microsoft.com/en-GB/windows/home
```

Type	Last Visited [Local]	URL	Redirect URL	IE Type	Status
redirect	21/04/2010 09:55:02 Wed	http://bit.ly/agtZtx	http://www.guardian.co.uk/books/2010/apr/19/penguin-cook-book	REDR	Redirected to:
redirect	23/04/2010 09:16:27 Fri	http://windows.microsoft.com/en-GB/...	http://www.microsoft.com/uk/windows/	REDR	Redirected to:

www.digital-detective.co.uk | Filter | Cache | P:\Temporary Internet Files\Content.IE5\index.dat | FO: 80384 | URL Records: 2

Figure 4

Figure 4 shows NetAnalysis and two Server Side Redirect entries. In this case, item number one is the original URL which caused the server to respond with a server side redirect HTPP response. This is the standard URL record which is shown in the URL column. In addition, as this is a REDR record which is intact, NetAnalysis has the Redirect URL (item number two) in the corresponding column. The Type column reflects the fact it is a redirect entry, as does the IE Type column (Internet Explorer Record Type). As this Redirect entry is intact, the Last Visited time stamp can be extracted.