

RipRS will check each offset, determine the total length of the compound file, and attempt to determine if it is an Automatic Crash Recovery file created by Internet Explorer or another type of compound file. If RipRS determines that the file is an Automatic Crash Recovery file, it will attempt to determine if the file is a recovery store file or a tab data file based on the files contents.

Each file will be written to the specified output directory individually. If RipRS determines the file is a recovery store file, it will use the naming convention 'recoverstore.{offset<offset>}.dat'. If RipRS determines the file is a tab data file, it will use the naming convention '{offset<offset>}.dat'.

The output from RipRS will appear as follows:

```
Examining offset 0...
  Not an ACR file
-----
Examining offset 151552...
  Tab data file detected
  Written to: c:\output2\{Offset151552}.dat
  File size: 17408 bytes
-----
Examining offset 172032...
  Tab data file detected
  Written to: c:\output2\{Offset172032}.dat
  File size: 3584 bytes
-----
Examining offset 176128...
  Tab data file detected
  Written to: c:\output2\{Offset176128}.dat
  File size: 4096 bytes
-----
Examining offset 14864384...
  Not an ACR file
-----
Examining offset 18288640...
  Not an ACR file
-----
Examining offset 87642112...
  Tab data file detected
  Written to: c:\output2\{Offset87642112}.dat
  File size: 10240 bytes
-----
Examining offset 87654400...
  Recovery store file detected
  Written to: c:\output2\RecoveryStore.{Offset87654400}.dat
  File size: 4608 bytes
-----
Examining offset 87662592...
  Tab data file detected
  Written to: c:\output2\{Offset87662592}.dat
  File size: 39424 bytes
-----
Examining offset 87703552...
  Not an ACR file
-----
Examining offset 87883776...
  Tab data file detected
  Written to: c:\output2\{Offset87883776}.dat
  File size: 3584 bytes
-----
```

The diagram illustrates the RipRS output with several callouts in red boxes and arrows pointing to specific parts of the text:

- File offset:** Points to the offset value '0' in the first line.
- Tab data file detected:** Points to the text 'Tab data file detected' in the second block.
- File output location:** Points to the file path 'c:\output2\{Offset176128}.dat' in the third block.
- Compound file is not an ACR file:** Points to the text 'Not an ACR file' in the fourth block.
- Recovery Store file detected:** Points to the text 'Recovery store file detected' in the fifth block.
- Output file size:** Points to the file size '3584 bytes' in the final block.

ParseRS

ParseRS will extract browsing information from recovery store and tab data files created by Internet Explorer 8 and 9.* Automatic Crash Recovery files are created by Internet Explorer to recover tabs and frames in the event of a non-recoverable error and contain various pieces of browsing information.

* At the time this version was developed, Internet Explorer 9 was still in beta form, however there appeared to be no change in the format of the Automatic Crash files.

Tab data files are created for each tab opened in Internet Explorer and contain information about the current page as well as the tab's page history.

Recovery store files contain information about the currently active tab and are used as a reference to link individual tab data files to a single browsing session.

Both tab data files and recovery store files are named using GUIDs, which are used to link individual files to single browsing sessions; therefore, if these files are recovered from unallocated space using RipRS or any other tool, while the files will still contain browsing information, it will be impossible to link them to their browsing sessions.

ParseRS can be used with three switches:

`/d` takes one argument, a directory path. Using the `/d` switch, ParseRS will examine each recovery store file in the specified directory, then attempt to match each tab data file with its corresponding recovery store file.

For example:

```
> ParseRS /d C:\ACR
```

The output using the `/d` switch is grouped by recovery store file will appear as follows:

```
Reading Automatic Crash Recovery files in C:\ACR...
-----
RecoveryStore.{6C8DA475-42A3-11E0-B638-E12886E2DCED}.dat
    Opened: 2/27/2011 6:56:05 PM
    Closed: 2/27/2011 6:57:29 PM
    Frame 0:
    Open Tabs:
        6C8DA476-42A3-11E0-B638-E12886E2DCED
        Created : 2/27/2011 6:57:29 PM
        Page 0 URL : http://www.google.com/
        Page 0 Title: Google
        Page 1 URL : http://www.wcsh6.com/
        Page 1 Title: Maine News, Weather, Sports Channel 6 NBC
        Portland | WCSH6.com | Portland
    Current Page: 1
```

Recovery store file name

Frame open And close times

Tab GUID

Tab created time

Tab history

Current URL: http://www.wcsh6.com/

6C8DA477-42A3-11E0-B638-E12886E2DCED

Created : 2/27/2011 6:57:29 PM

Page 0 URL : http://www.ebay.com/
Page 0 Title: eBay - New & used electronics, cars, apparel,
collectibles, sporting goods & more at low price

Referring page

Referred from: http://www.google.com/

Page 1 URL : http://www.msn.com/

Page 1 Title: craigslist: MSN.com

Current page

Current Page: 1

Current URL

Current URL: http://www.msn.com/

RecoveryStore.{72D8C367-2B46-11E0-AEE8-005056C00008}.dat

InPrivate browsing detected!

InPrivate Browsing
detected

Opened: 1/29/2011 1:24:00 AM

Closed:

Frame 0:

Frame number

Open Tabs:

72D8C368-2B46-11E0-AEE8-005056C00008

Created : 1/29/2011 1:24:00 AM

Page 0 URL : http://www.ebay.com/
Page 0 Title: eBay - New & used electronics, cars, apparel,
collectibles, sporting goods & more at low price

Current Page: 0

Current URL: http://www.ebay.com/

Open tabs

Closed Tabs:

797B9F17-2B46-11E0-AEE8-005056C00008

Created : 1/29/2011 1:24:11 AM

Page 0 URL : http://www.wcsh6.com/
Page 0 Title: Maine News, Weather, Sports Channel 6 NBC
Portland | WCSH6.com | Portland

Current Page: 0

Current URL: http://www.wcsh6.com/

Closed tabs

If ParseRS is unable to locate a tab data file that should be associated with a recovery store file, the GUID of the tab data file will still be displayed along with a message stating 'Unable to locate file!'.

As mentioned previously, if these files are recovered from unallocated space using RipRS or any other tool, it will not be possible to link individual files to their browsing sessions, so the it will be best to examine the files individually using the next two switches.

The /r switch takes one argument, a recovery store file name. Using the /r switch, ParseRS will examine only a single recovery store file then attempt to match any tab data files in the same directory with the recovery store file.

For example:

```
> ParseRS /r RecoveryStore.{03E774A5-2B47-11E0-AEE8-005056C00008}.dat
```

The output using the /r switch will appear in the same format as the /d switch:

```
Reading RecoveryStore.{03E774A5-2B47-11E0-AEE8-005056C00008}.dat...
```

```
-----  
RecoveryStore.{03E774A5-2B47-11E0-AEE8-005056C00008}.dat
```

```
Opened: 1/29/2011 1:28:03 AM  
Closed:
```

```
Frame 0:
```

```
Open Tabs:
```

```
03E774A6-2B47-11E0-AEE8-005056C00008
```

```
Created : 1/29/2011 1:28:03 AM
```

```
Page 0 URL : http://www.wcsh6.com/  
Page 0 Title: Maine News, Weather, Sports Channel 6 NBC  
Portland | WCSH6.com | Portland,
```

```
Current Page: 0
```

```
Current URL: http://www.wcsh6.com/
```

```
03E774A7-2B47-11E0-AEE8-005056C00008
```

```
Created : 1/29/2011 1:28:03 AM
```

```
Page 0 URL : http://www.ebay.com/  
Page 0 Title: eBay - New & used electronics, cars, apparel,  
collectibles, sporting goods & more at low price
```

```
Current Page: 0
```

```
Current URL: http://www.ebay.com/
```

The /t switch takes one argument, a tab data file name. Using the /t switch, ParseRS will examine only a tab data file and extract its browsing information.

For example:

```
> ParseRS /t C:\{03E774A6-2B47-11E0-AEE8-005056C00008}.dat
```

The output using the /t switch will appear in the same format as the /d switch:

```
Reading {03E774A6-2B47-11E0-AEE8-005056C00008}.dat...
```

```
-----
```

```
{03E774A6-2B47-11E0-AEE8-005056C00008}.dat
```

```
Created : 1/29/2011 1:28:03 AM
```

```
Page 0 URL : http://www.ebay.com/
```

```
Page 0 Title: eBay - New & used electronics, cars, apparel,  
collectibles, sporting goods & more at low price
```

```
Current Page: 0
```

```
Current URL: http://www.ebay.com/
```