# Contents

About OSIRT and Author ........................................................................................................... 4
Downloading OSIRT ................................................................................................................ 4
System Requirements .............................................................................................................. 4
Extracting OSIRT – Portable Version .................................................................................... 4
Installing and running OSIRT – Installable Version ............................................................... 4
Running OSIRT - Portable ..................................................................................................... 5
OSIRT’s First Load Screen ..................................................................................................... 5
  First Load Screen Options .................................................................................................. 6
Creating a New Case ................................................................................................................ 6
  Hash Functions .................................................................................................................. 7
  Opened Case ...................................................................................................................... 7
Loading an Existing Case ...................................................................................................... 7
Main Browser ........................................................................................................................ 8
  Features ............................................................................................................................ 9
  Installing Flash Plugin ....................................................................................................... 10
  Webpage Logging ............................................................................................................. 10
Saving Images from Website ................................................................................................. 10
Opening a Link in New Tab .................................................................................................. 10
Viewing and Saving Page Source Code ............................................................................... 11
Viewing Exif data .................................................................................................................. 11
Show Facebook Profile ID ................................................................................................... 12
Reverse Image Searching ...................................................................................................... 12
Copy Image Location to Clipboard ....................................................................................... 13
Extracting links from webpage ............................................................................................. 13
Downloading .......................................................................................................................... 13
Browser Engine .................................................................................................................... 13
Taking Screenshots ............................................................................................................... 13
  Full Page Screenshot ........................................................................................................ 13
  Current View Screenshot .................................................................................................. 13
  Timed Current View Screenshot ....................................................................................... 14
Snippets .................................................................................................................................. 14
Image Previewer ..................................................................................................................... 14
Video Capture ......................................................................................................................... 15
  Start Capture .................................................................................................................... 15
  Stop Capture ...................................................................................................................... 15
Preamble........................................................................................................................................31
Step 1 ...........................................................................................................................................32
Step 2 ...........................................................................................................................................32
Step 3 ...........................................................................................................................................34
Step 4 ...........................................................................................................................................34
Author’s Comments .....................................................................................................................34
A required library is missing that OSIRT needs........................................................................34
Possible Solution 1 .....................................................................................................................34
Possible Solution 2 .....................................................................................................................34
You require the .NET framework 4.6 or later............................................................................35
About OSIRT and Author

OSIRT (Open Source Internet Research Tool) is a WinForms application written in C# by Joseph Williams, a University Instructor and PhD candidate from Canterbury Christ Church University. OSIRT is in continuous development, and many of the features integrated into OSIRT have been requested by law enforcement officials across the UK.

If you wish to make a feature request, report a bug, send an amendment for this user guide or any other queries please feel free to contact me: joseph.williams@canterbury.ac.uk

Downloading OSIRT

OSIRT does not automatically update, so ensure you obtain the latest version of OSIRT from http://osirtbrowser.com/.

System Requirements

OSIRT works on both 32 and 64 bit versions of Windows 7, 8, 8.1 and 10. However, you will also have to install two additional pieces of software for OSIRT to work correctly if they are not already present on the system. These are:

- .NET Framework 4.6.1 (or above)
  - Press download and select vcredist_x86.exe

**IMPORTANT:** You must restart your computer after the installation of these programs. OSIRT will not work until after a restart.

Extracting OSIRT – Portable Version

OSIRT, and its required libraries, are bundled in a Zip file. This Zip file must be fully extracted before attempting to run OSIRT, otherwise OSIRT cannot run correctly.

For this example, the file downloaded from http://osirtbrowser.com/is called osirt-example.zip

- Right click on osirt-example.zip
- Click “Extract All..” and wait for the contents to be fully extracted
- The folder will now be extracted. For this example, the folder is called osirt-example
- Double click osirt-example

Installing and running OSIRT – Installable Version

For this example, the file downloaded from http://osirtbrowser.com/is called osirt-example.msi

- Double click on osirt-example.msi
- Following the installing instructions by confirming you’re happy to install
- Installation is complete once the installation wizard finishes
- An OSIRT icon is placed on the Desktop
- Double click the OSIRT icon to launch OSIRT
Running OSIRT - Portable

Once you have opened the extracted folder, double click on OSIRT.exe, or OSIRT if the system does not have file extension turned on.

![Folder contents]

**Figure 1 OSIRT's containing folder**

**IMPORTANT:** Do not run OSIRT.exe outside of this folder. The files within this folder are necessary for OSIRT to function.

**OSIRT’s First Load Screen**

When OSIRT first loads, you are presented with three main options (Figure 2)
First Load Screen Options

Create New Case – Creates a brand new OSIRT case to work on.

Load Case – Load an existing an existing OSR case file into OSIRT

View Case Audit Log – View a cases’ audit log by loading an existing OSR case.

Creating a New Case

1. Select “Create New Case” from the first load screen
2. Fill out the case details
   a. All fields must have a text entered. Not filling all the fields out will result in an error.
   b. OPTIONAL: A password may be entered to protect the case.
3. Press “Next”
4. The case will be saved at the location entered in the “Case Location” field.

**Note:** The Case Reference field becomes the name of the case container file. For example, a Case Reference with the name “example-case” will generate an example-case.osr file once the case has closed.

**Note:** The Case Reference field may only contain letters, numbers, underscores and hyphens. This is to, largely, conform with Windows file name conventions.

**Hash Functions**

OSIRT provides various hashing algorithms hash artefacts taken or attached to OSIRT. These algorithms are MD5, SHA1, SHA256, SHA384 and SHA512. It’s recommended to use a SHA variant over MD5.

**Opened Case**

When a case is open in OSIRT, it’s in its **extracted state**; its extracted state is a series of directories. Figure 3 is a tree of an extracted OSIRT case (this case has no evidential artefacts).

![Figure 3 Tree representation of an extracted OSIRT case](image)

**IMPORTANT:** When a case is in its extracted state do not manipulate it outside of OSIRT.

**Loading an Existing Case**

1. Select “Load Case” from the first load screen.
2. Browse to the location of the .osr case file you wish to load.
3. Select “Open Case” from the existing case details screen (Figure 4)
The open existing case screen displays:

- The name of the case being opened
- The SHA512 hash of the case being opened
- The date and time stamp the case was last modified according to Windows.

**IMPORTANT:** You cannot double click on the .osr to open it within OSIRT, it has to be loaded via the Load Case option on the opening screen.

**Main Browser**

OSIRT has been designed to replicate the look and feel of a standard web browser (Figure 5), but with additional features for law enforcement. The browser has multiple tab capabilities, clicking the “new tab” button next to the last open tab will create a new tab which loads the default homepage.
Figure 5 OSIRT’s main browser

Features

Home – Go to the homepage (default: http://google.co.uk)

Back – Go back one page (if can go back)

Forward – Go forward one page (if can go forward)

Full page Screenshot – Takes a screenshot of the entire page

Video capture – Records the screen

Attachment – Add item to the current OSIRT case

Audit Log – View the current cases audit log and export report options.

Tools – Additional tools for the investigator

Options – OSIRT options menu
Installing Flash Plugin

1. Close down OSIRT if opened
2. Visit https://get.adobe.com/flashplayer/otherversions/ on a browser other than OSIRT
3. Step 1: Select your Operating System (this example has selected Windows 10/Windows 8)
   a. Note: You may have a different Operating System. Check with your system administrator if unsure.
4. Step 2: Select FP 23 for Opera and Chromium – PPAPI
   a. FP 23 is the version; this may be a higher number when you look. Make sure to select a version with Opera and Chromium – PPAPI
5. Uncheck the “Optional offers” boxes (unless you want the optional offers).
6. Press “Download now”.
7. Find the download, and double click on it to install Flash.
8. Once the installation has completed, you may open OSIRT.
9. If Flash still isn’t working, restart the PC.

Webpage Logging
Any webpage visited is automatically logged with a date and time stamp and placed in the audit log.

Saving Images from Website
1. Right click on the image to save
2. Select “Save image” from the menu that pops-up
3. Wait for the Image Previewer to display (see Image Previewer section)

Opening a Link in New Tab
1. Right click on the link to open
2. Select “Open link in new tab”
3. A new tab will load and open the website in the link

**Viewing and Saving Page Source Code**
1. Right click anywhere on the webpage
2. Select “View Page Source”
3. Wait for the page source code window to open
4. To save the page source code, press the icon

**Viewing Exif data**
Exif (Exchangeable image file format) data may be found in some Jpeg/Jpg images. The information found in Exif data (if available) can be useful. For example, the Exif data may contain the date and time the picture was taken, the location and what camera was used.

1. Right click on an image
2. If the image has a Jpg/Jpeg extension, the “View image EXIF data” option will display
3. Click “View image EXIF data”
4. If the image contains Exif data, a new Window will pop up containing the Exif data.
5. To save the Exif data to the audit log, press the “Log exif data” button.

**Note:** Some websites or image processing tools remove Exif data when images are uploaded or saved. So not all Jpegs will have associated Exif data, or may only have limited Exif data.

**Show Facebook Profile ID**
If the Facebook profile being looked at uses a vanity tag, for example, [https://www.facebook.com/joe.bloggs99](https://www.facebook.com/joe.bloggs99) then it’s possible to obtain the numerical profile ID the following way:

1. Right click anywhere on the Facebook profile
2. Press “Show Facebook Profile ID”
3. A window will pop-up displaying the profile ID.

**Reverse Image Searching**
1. Right click on any image on the webpage
2. Select “Reverse image search using TinEye”
Copy Image Location to Clipboard
1. Right click on any image on the webpage
2. Select “Copy image location to clipboard”
3. The image location will now be on the clipboard

Extracting links from webpage
1. Right click on any image on the webpage
2. Select “Extract all links on page”
3. A window will appear containing all the link on the page
4. To save the page link, press the icon

Downloading
Downloads are automatically triggered when a downloadable item is requested. The download is saved to the requested location, then copied over to the OSIRT case container where it is logged as usual.

1. Click “Save” when the Save File dialog appear is it recommended that you do not change the recommended file name
   a. You may save anywhere you wish.
2. A green progress bar will appear at the bottom right hand side, and when this is full, a “Download Complete” pop-up message will appear.

Browser Engine
OSIRT’s browser uses CefSharp, it’s a “lightweight .NET wrapper around the Chromium Embedded Framework (CEF)”. For simplicity, think of it like Google Chrome.

Taking Screenshots
Full Page Screenshot
1. Press the icon in the toolbar
2. The toolbar will be disabled (grey out) while capturing is in process
3. The page will automatically scroll and take a screenshot
   a. Depending upon the size of the page, this can take 30 seconds or so.
   b. IMPORTANT: Do not touch the webpage while it is scrolling and capturing.
4. Wait for the screenshot to build.
   a. Depending upon the size of the page, this can take 30 seconds or so.
5. Wait for the Image Previewer to display (see next section)

Current View Screenshot
This will take a screenshot of what you are currently looking at in the Main Browser.

1 https://github.com/cefsharp/CefSharp
1. Press the arrow next to the icon

2. Press Current View Screenshot
3. Wait for the Image Previewer to display (see next section)

Timed Current View Screenshot
This will take a screenshot of what you are currently looking at in the Main Browser after a specified time. This is particularly useful for capturing webpage elements that only display when the mouse cursor is hovered over them.

1. Press the arrow next to the icon
2. Press Current View Timed Screenshot
3. Enter a time in seconds. A screenshot will be taken after this time.
4. Wait for the Image Previewer to display (see next section)

Snippets
Snippets allow you to select a portion of the screen as a rectangle.

1. Press the arrow next to the icon
2. Press Snippet
3. Click and drag the left mouse button over what you would like to capture. A red box will be drawn around the area as you drag.
   a. If you do not wish to capture a snippet, press the Esc key.
4. Let go of the left mouse button when complete
5. Wait for the Image Previewer to display (see next section)

Image Previewer
The Image Previewer (Figure 6) displays when a screen capture has been taken. This image is displayed on the right hand side, and further details about the image on the left are displayed, such as the date and time the image was taken, the hash value and the URL where the image was taken.

1. A filename is provided by default, but you may overwrite this if required
2. Save as either PNG, PDF or JPG. The default is PNG.
a. **Note:** PDF save only works for smaller images. If OSIRT cannot save as PDF, it will revert to saving as PNG. There isn’t a way to determine if saving as PDF will fail before trying it.

3. Enter a note about the image.
   a. **Note:** A note is required.

4. Press “Log” to log this image in the audit log

5. If this image is no longer required to be logged, press “Cancel” or close the previewer.

---

**Video Capture**

The video capture library uses the H.264 codec, which is capable of recording in 1080p. The default setting records at 30FPS, but this can be adjusted in the options menu.

**Start Capture**

1. To start screen recording, press
2. Continue to work on the case as usual

**Stop Capture**

1. To stop screen recording, press
2. Wait for the Video Previewer will display (see next section)

**Marker Window**

To record a particular section of the screen, use the Marker Window option.

1. Press the arrow next to the icon
2. Press **Marker Window**
3. A new window will now be displayed (Figure 7)
4. Resize and place this new window where you’d like OSIRT to record. OSIRT will only record content within the Marker Window.

5. Press to start capturing where the Marker Window is placed
   a. IMPORTANT: Resizing this Marker Window while recording will not be reflected in the recording.

Error: The maximum resolution for H.264 video is 1920x1080
If you receive an error message that reads “The maximum resolution for H.264 video is 1920x1080” resize the OSIRT window and try capturing again.

Video Previewer
The Video Previewer (Figure 8) displays when a video screen capture has been taken. This video is displayed on the right hand side, and further details about the video on the left are displayed; such as the date and time the video was taken and the hash value.

1. A filename is provided by default, but you may overwrite this if required.
2. Enter a note about the video.
a. **Note:** A note is required.
3. Press “Log” to log this video in the audit log
4. If this video is no longer required to be logged, press “Cancel” or close the previewer.

![Video Previewer](image)

**Figure 8 Video Previewer**

**Attachments**

If a piece of evidence or an artefact has been received into relation of the case, but wasn’t directly obtained using OSIRT, then the Attachment functionality provides a way to add this item to the case by hashing, date and time stamping, and logging it to the audit log.

1. Press the ![Attachment](attachment) icon
2. The Attachment window will pop-up (Figure 9)
3. Select “Browse...” and locate the file to attach
4. File details such as name and size are displayed.
5. Add a note about this attachment
   a. **Note**: A note is required.
6. Press “Attach File” to attach this item to the case and log it
7. To attach another file, start from step 3 otherwise close the attachment window.

![Attach File to Case](image)

**Figure 9 Attaching a file to an OSIRT case**

---

**Case Notes**

While OSIRT maintains an audit trail of all actions taken, you may wish to keep your own log to maintain any thought processes throughout the case. The case notes option provides a way to do this.

**Entering a Case Note**

1. Press the ![CASE icon](image) icon
2. The Case Notes will pop-up (Figure 10)
3. Enter your note in the bottom white box
4. Press Enter, or “Add Note” to append the note.
   a. The note is date and time stamped automatically.

![Case Notes window](image)

**Figure 10 Case Notes window**

**Exporting Case Notes**

1. Press the icon
2. Enter a name for the case notes and select a location where to save them
3. Click “OK”
4. The case notes will automatically open when saved.
5. Saving case notes will automatically place this action in the audit log along with a date and time stamp, and the file hash value.

**Audit Log**

The Audit Log shows all actions that have been taken when conducting Open Source Research.

1. Press the icon
2. The Audit Log (Figure 11) will open
The Audit Log is split into tabs and is paginated (25 records show per page). These tabs are split as follows:

- **Websites Loaded** – All websites that have been visited when using OSIRT.
- **Website Actions** – All actions taken on a website. This may be screenshots, downloads, downloading page source code, etc.
- **OSIRT Actions** – All OSIRT actions, such as when the case was opened and closed, reports exported, etc.
- **Attachments** – Any attachments to this OSIRT case.
- **Videos** – All videos taken within OSIRT.
- **Complete** – A combined log of all actions in chronological order.

### Row Details and File Previewer

On the left hand side of the Audit Log window are row details, these are changed when a particular row is selected. If a row contains a file, then the File Previewer will display an icon for that file type. Clicking on the icon will open the file in the system’s default application for that file type.

**IMPORTANT**: Ensure to close the application that has the file opened via the File Previewer.

### Searching

The Audit Log contains search functionality situated on the top right (Figure 12).
1. Enter a term to search in the textbox
2. Select which tab you would like to search. If you require to search the entire log, select “All Tables”
3. Press the Enter key or press the “Search” button
4. The Audit Log will now populate with all the records that match the search term (Figure 13).
5. To return back to the regular Audit Log press the icon situated in the top left of the Audit Log, this will close the search results.

![Figure 13 Audit Log search for term “2016-08-20”](image)

**Loggable Actions**
The following is a list of actions that can be logged in OSIRT. Actions can be logged through direct user input, and others are automatically logged by OSIRT.

- Screenshot
- Scraped
- Snippet
- Batchsnap
- Saved
- Attachment
- Video
- Download
- Source
- Whois
- Report
- Loaded
- CaseLoaded
- CaseClosed
- CaseNotes
Exporting the Report

1. Press the **LOG** icon
2. The Audit Log (Figure 11) will open
3. Press the **File** icon on the top left
4. The report panel (Figure 14) will replace the Row Details panel

![Figure 14 Report exporting options](image)

**Report Selection**
Ability to omit tables by unchecking the box. If there are no rows within a particular table, then the checkbox is disabled (Figure 15 shows Attachment checkbox disabled as there are no attachments added to this case).
Report Options

Report options provide a way to tailor the report (Figure 16).

- **Link images in report** – Provides a hyperlink to any images in the report. If the report is HTML, then hovering over a link will display a thumbnail of the image.
- **Link videos in report** - Provides a hyperlink to any videos in the report. If the report is HTML, then a video will be visible in the report.
- **Open report once created** – Opens the report in the system’s default application for that file type.
- **Print audit notes** – Adds the notes associated with an artefact. For example, notes added in the Image Previewer when taking a screenshot.
- **Merge case notes** – Adds the case note to the report.
- **GSCP Stamp** - Protectively mark the report with the following stamps
  - Not Protectively Marked
  - Top Secret
  - Secret
  - Official

Export Report

1. Press “Browse...” and choose a location where you would like the report to be saved
2. Select the type of report to export, there are three options
   a. **HTML** – HTML is the language of the web and this file type can be opened in any web browser. It provides a richer reporting experience to the recipient.
   b. **PDF** – PDF provides a simple way to view the report, it’s simple to send over e-mail and if you don’t need the bells and whistles PDF provides that.
c. – Comma Separated Value (CSV) file provides a spreadsheet friendly file of the Audit Log. **The CSV file option only exports the audit log and no artefacts.**

d. – eXtensible Markup Language (XML) provides an XML formatted audit log ready to be stylised by XSLT.

3. Wait for the report to export, you will receive a confirmation it has reported successfully.

4. The report will be saved to the location in a folder with the following name report_[case-name]_[date-and-time] with “case-name” being the name of the case and “date-and-time” being the date and the report was exported.

**Report Folder**

The exported folder will contain the report in either HTML or PDF, depending upon what was selected, and a folder called “artefacts”. This artefacts folder contains all the evidential artefacts obtained via OSIRT. Figure 17 shows a tree of the report folder exported as an HTML report. Note that the artefact folder contains sub folders for particular artefact types.
Viewing the Report
1. Open the report containing folder
2. If PDF report double-click on report.pdf
3. If HTML report double-click on combined.html
4. The report will open in the system’s default application for that file type.
   a. If HTML, then that’s usually a web browser
   b. If PDF, then that’s usually Adobe Acrobat Reader (or another PDF viewer if installed)

Additional Tools
1. Press the icon
2. A menu will pop-up with additional tools
a. WhoIs? – Displays a window with WhoIs information in regards to the domain you are presently on. (Figure 18)

b. What’s the IP? – Displays all the IP addresses associated with this particular domain.

c. Force Cache Refresh – Refreshes the current web page but ignores the cache when doing so.

WhoIs?
To save WhoIs information to the audit log, press the icon

Options Menu
1. To access the options menu, press the icon
2. The options menu will pop-up (Figure 19)
The options menu is split into three sub menus:

- **Browser**
- **Video Recording**
- **General**

**Figure 19 OSIRT Options menu**

### Browser Options

**Setting Homepage**

You are able to set the homepage here. The default homepage is google.co.uk

### Video Recording Options

**Setting Audio Source**

You can set the audio source to record from either a microphone or record what the speaker output is (Stereo Mix).

**Showing Cursor When Recording**

If you need to show the cursor and/or cursor clicks, select the options under “Capture”.

### General Options

**Setting Constabulary or Agency Icon for Report**

1. Select “Browse…”
2. Find your icon. Square images make better icons
   - **Note:** OSIRT will resize your icon to 250px by 250px
3. When OSIRT has resized your icon, it will be displayed.
Exporting Hash on Close
To export a hash to a text file when you close OSIRT, perform the following:

1. Tick “Export Hash on Close?” (This is ticked by default)
2. Select a location where to save the hash.
   a. Desktop is the default location

Advanced Browser Options
Tor (The Onion Router)
OSIRT contains Tor functionality in order to browse the deep web.

1. On the OSIRT first load screen, press the icon on the bottom right
2. The advanced browser options menu will open (Figure 20)
3. Tick “Connect via the Tor network”
4. Press the OK button
5. You may now load or create a new OSIRT case, and you will be connected to the Tor network
6. The address bar in OSIRT will now be purple to signify you are in Tor mode (Figure 21)
7. To disconnect to the Tor network, close down OSIRT.

![Advanced Browser Options](image)

Figure 20 Advanced browser options to connect to Tor

IMPORTANT: You will only be connected to the Tor network in OSIRT, not in any other browser.

Note: You will need to check this box every time OSIRT loads and you require Tor.

Note: Tor can be slow, you may have to wait up to 60 seconds for a page to load.
Spoofing User Agent
Your browser will tell a website about itself when you visit. The user agent typically contains what operating system and web browser you’re using. This information is useful as it allows a website to adjust itself to suit your browser and device. For example, if you’re on a mobile phone you do not necessarily want to be directed to the desktop site as it’s hard to navigate.

The user agent string that is sent to the web server for the page you are requesting while running OSIRT on a Windows 10 machine looks like this:
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36

The pertinent bits are Windows NT 10.0 (using Windows 10) and Chrome/51.0.2704.103 (using a version of the Chrome browser).

You may wish to fool a webserver by hiding (better known as spoofing) your user agent. You may wish to do this to see a different version of the website, or to simply hide yourself.

How to Spoof Your User Agent

1. On the OSIRT first load screen, press the icon on the bottom right
2. The advanced browser options menu will open (Figure 22)
3. In the Spoof User Agent box, enter a user agent to use. If it’s left empty, OSIRT will use the default user agent.
   a. A link is provided to a list of over 5 million possible user agents. Although it is recommended not to choose a really esoteric one.
4. In this example, I searched for “Iceweasel debian” to obtain a user agent string for the Iceweasel browser on a Debian GNU/Linux machine.
a. Mozilla/5.0 (X11; U; Linux i686 (x86_64); en-GB; rv:1.9.1.3) Gecko/20090101 Iceweasel/3.5.3 (Debian-3.5.3-2)

5. Paste this user agent string into the textbox (Figure 22)
6. Click “OK”
7. Load or create an OSIRT case.
8. You will now be using the spoofed user agent (Figure 23)

![Advanced Browser Options](image)

*Figure 22 Setting a different user agent*

![User Agent Information](image)

*Figure 23 How my user agent looks to a website*

**Note:** You will need to check this box every time OSIRT loads and you require a spoofed user agent.
Closing OSIRT

1. Press the X in the top right of the window.
2. Press “Yes” at the prompt confirming if you would like to close the current case.

3. OSIRT will close after performing some important clean-up operations.

Troubleshooting

Recovering an OSIRT case
If your case is in its extracted state after you have closed OSIRT, this guide will help you turn your case back into an .osr file for OSIRT to load.

It’s important that OSIRT is closed before you attempt to recover a case.

Preamble
For the purposes of this documentation, an example case called example_case has been created and OSIRT has been unable to re-archive it to its .osr format. This leaves the case in its extracted state, which is a normal Windows file structure at the location where the case was saved. In this example, the case has been saved to the user’s desktop.

Looking at the desktop, we have this folder:

This folder is the extracted case we want to change back into an .osr file.

We can verify this is an extracted OSIRT case by looking in this folder, it should have the following contents. Do not modify these contents, however.
Step 1
Open OSIRT, and click on the silver icon with the yellow triangle on the bottom left of the screen.

![Image](image.png)

This will open the case recovery tool, seen below.

![Image](image2.png)

Click this icon

Step 2
Click the “Browse...” button and browse to the extracted case. In this example, we’ll be browsing to C:\Users\Joe\Desktop\example_case
The case recovery tool will then display the location of where the extracted case is:

Select the parent folder. In this example, the example_case folder.
Step 3
Click the “Recover” button. Depending on the size of the case, the re-archiving may take a short while, but it is quite quick for smaller cases. There is a scrolling progress bar that is displayed to let you know OSIRT is working on recovering the case.

If you do not receive an error, the case has been successfully recovered.

Step 4
Check the location of the case. In this example, we are checking the desktop. There should now be a file called \example_case.osr

Close the case recovery tool, and proceed to load this case into OSIRT.

Author’s Comments
This section contains a semi-technical explanation of how OSIRT case containers work.

An .osr file is simply a zip file that has had its file extension renamed to .osr.

A case in its opened state is fully extracted, this is so OSIRT can write to the directories (e.g. save screenshots) and the case database. Once a case has closed, OSIRT re-archives this extracted case back to an .osr file. However, there can be occasions where OSIRT is unable to re-archive the case, examples being a system crash, or OSIRT not closing correctly for whatever reason. This is why a case can be left in its ‘open’ state.

OSIRT does attempt recover these extracted cases automatically when re-opened, but it may not always work. Hence the need for the case recovery tool.

Knowing that an .osr is only a zip file, and if you have an understanding of how zip files work, you can simply create your own .zip file, ensuring that you give the zip file the exact same name as the parent directory of the extracted case. Then you can just drag the entire extracted case into the zip file, and rename the file extension from .zip to .osr. You’ll need to turn on file extensions to do this correctly.

A required library is missing that OSIRT needs...

Possible Solution 1
Ensure that OSIRT is running from within the extracted folder. See the ‘Running OSIRT’ section.

Possible Solution 2
Ensure that all the required dependencies are installed (.NET Framework and VC++). See the ‘System Requirements’ section. Remember to restart after installing these dependencies.
You require the .NET framework 4.6 or later...
Ensure that .NET Framework 4.6 or later is installed. See the ‘System Requirements’ section. Remember to restart after installing these dependencies.