Pre-Release OSIRT iii Version 2.0

OSIRT iii Digital Casebook User Guide

OSIRT Ltd
MAY 2025

Contents

🛠️ Installation (Windows)

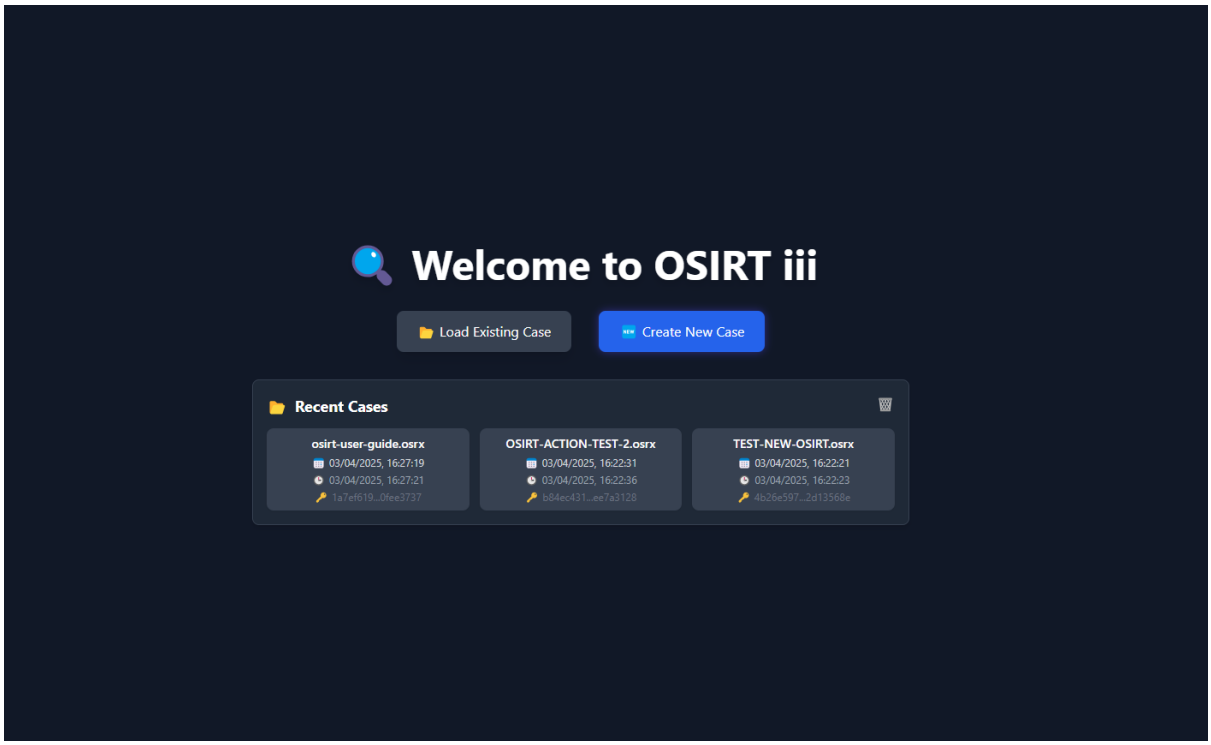
1. **Download the Installer**
    - See details in e-mail for download location
2. **Run the Installer**
    - Locate the downloaded .exe file and double-click it.
    - If prompted by Windows SmartScreen, click **More info** → **Run anyway**.
    - Follow the installation wizard prompts to complete setup:
        - Choose an installation location (default is fine for most users).
        - Click **Install** and wait for the process to complete.
3. **Finish Installation**
    - Once installation is complete, you may launch OSIRT iii immediately by checking **"Launch OSIRT iii"** or using the desktop/start menu shortcut.

🚀 First Run

1. **Allow Localhost Connection**
    - On first launch, OSIRT iii will start a local server (localhost) to enable its link to the browser extension.
    - **Windows Defender Firewall** or other antivirus software may prompt you to allow the connection.
        - Make sure to **Allow access** when prompted (usually a Windows Security dialog).
        - This is required for full functionality—blocking it will prevent the extension from working correctly.

Note: The first run of OSIRT iii after installation can take a short while (up to 30 seconds) to load up.

🏠 OSIRT iii Home Screen



When you first launch OSIRT iii, you'll see the **Home Screen**, which acts as your starting point for any digital investigation.

It provides two main options:

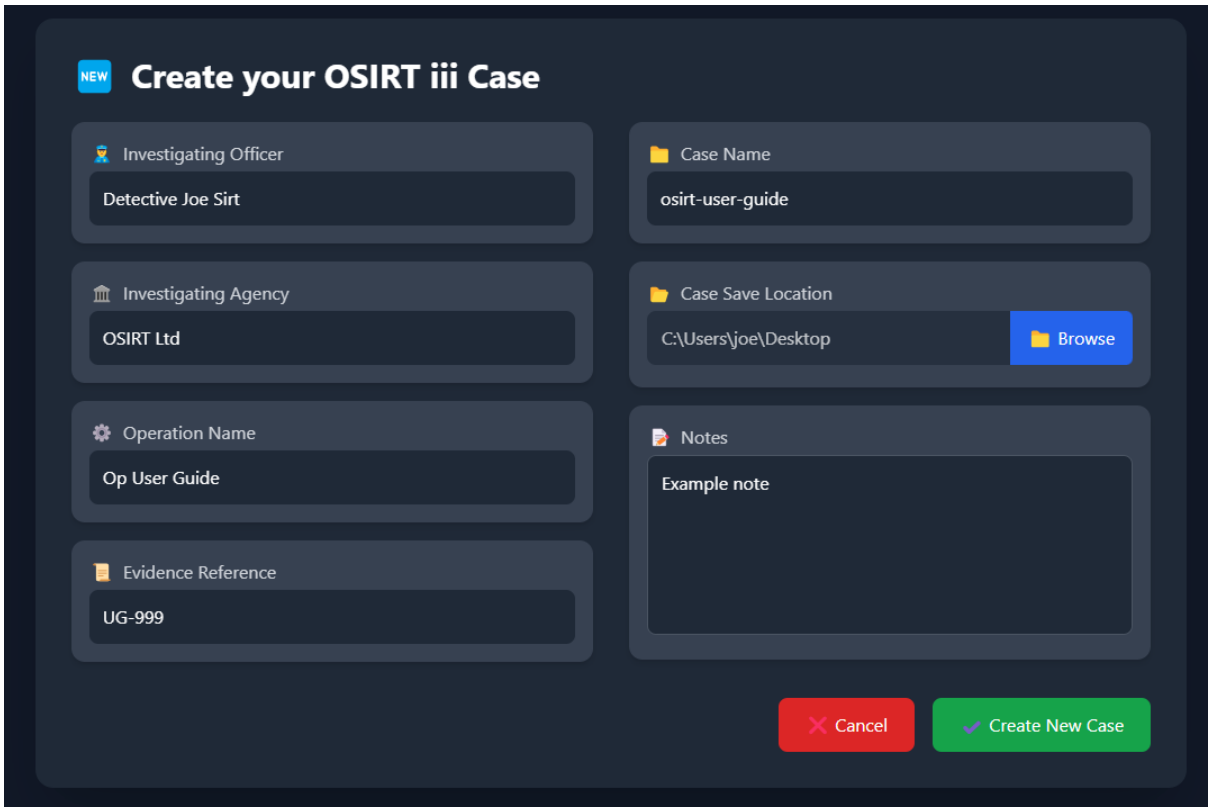
1. Create New Case

Clicking this button allows you to begin a fresh case. You'll be asked to provide case details such as the name, location, officer and agency names, and any relevant notes. This ensures all artefacts you collect later are properly attributed and organised from the outset.

2. Load Existing Case

If you've already worked on a case and want to continue, use this button to open a previously saved .osrx case file. OSIRT iii will extract and restore all associated artefacts, logs, and metadata, allowing you to pick up right where you left off.

🗁 Creating a New Case



To begin a new investigation, click **"Create New Case"**.

This opens a secure form where you can fill out important case metadata, including:

- **Case Name**: A unique name for your case
- **Case Location**: Choose where the case folder should be stored on your device.
- **Officer Name**: Your name or the investigator's name.
- **Agency Name**: The department or agency overseeing the case.
- **Operation Name**: Optional field for naming the operation.
- **Evidence Ref**: Any reference ID related to the evidence or legal tracking.
- **Hash**: Currently pre-filled as sha512 – this is used for data integrity checks.
- **Notes**: Any initial notes about the case.

🟢 When you're ready, hit **"Create Case"**.

🛠️ Behind the scenes, OSIRT iii:

- Creates a structured folder layout for artefacts.
- Initialises a secure SQLite database for storing captured evidence.
- Prepares the dashboard so you can start collecting and reviewing data.

After creation, the app transitions smoothly into the **main dashboard** where you can begin collecting digital artefacts like screenshots, text grabs, and web captures.

🗂 Case Folder Structure

When you create a new case in OSIRT iii, it automatically generates a dedicated folder with a standardized internal structure and a custom icon.

🕵️ Folder Appearance

- **Custom Icon**: Each case folder uses a distinctive icon featuring "Detective Joe Sirt" to make your case files instantly recognisable in Windows Explorer.

- The icon is defined by a folderIcon.ico file inside each case folder. You'll see this icon automatically applied when browsing folders in File Explorer (Windows).

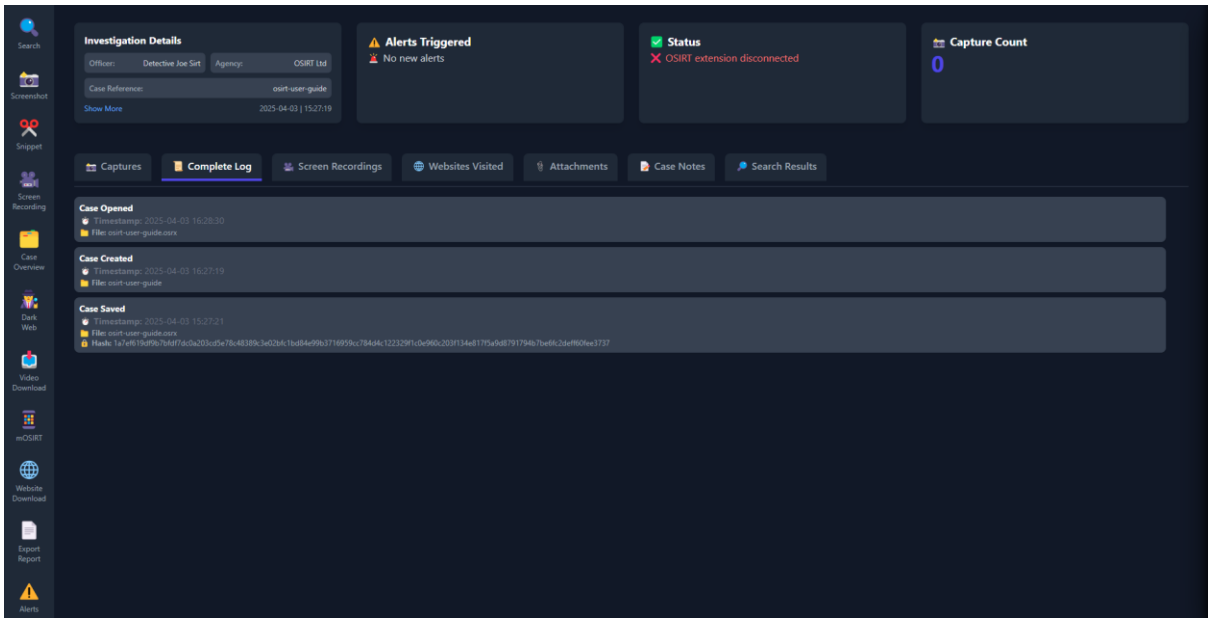
🗂 Folder Structure Overview

Each case folder includes the following subdirectories and files:

🗂 Item	Description
attachments/	Stores any external files you import or drag-and-drop into the case
downloads/	Contains files captured through the download feature
images/	Holds screenshots, snips, and full-page captures
reports/	Where reports and printed artefacts are generated and stored
videos/	Contains screen recordings or captured video evidence
case.db	The SQLite database that stores all structured case data
folderIcon.ico	The custom icon file applied to the case folder (Detective Joe Sirt)

This structure is created automatically when you make a new case and ensures all evidence is neatly organised and properly linked in the application.

Main Dashboard Overview



Once a case is created or loaded, OSIRT iii transitions you into the **Main Dashboard** — this is your digital casebook, where all investigative work is centralised and easily accessible.

The dashboard is neatly laid out into the following key sections:

Investigation Details (Top Left)

Displays high-level case metadata:

- **Officer & Agency**: The assigned investigator and their organisation.
- **Case Reference**: A unique identifier for the case.
- **Timestamp**: When the case was created or loaded.
- Click **"Show More"** to expand additional case fields like operation name, evidence reference, hash type, and any notes you've entered.

Alerts Triggered

This area will display any alert flags or notifications related to suspicious or notable content collected during your investigation.
If there are no alerts, it will simply show **"No new alerts"**.

Status Indicator

Shows whether the **OSIRT browser extension** is connected.

- ✅ Green means connected and ready to receive data from the web.
- ❌ Red means disconnected — which may prevent live captures from functioning.

Capture Count

Displays a running total of all artefacts captured during the case (screenshots, downloads, logs, etc.). This counter increases automatically as you work.

Artefact Tabs (Just Below the Top Panel)

These tabs organise the core artefacts of your case:

- **Captures** – Screenshots, mhtml files, full-page grabs, and other webpage artefacts.
- **Complete Log** – A chronological log of all actions taken, including when the case was created, saved, opened, and each artefact added.
- **Screen Recordings** – Any screen activity you've recorded using the built-in recorder.
- **Websites Visited** – Logs and cards for every website recorded during the session.
- **Attachments** – Manually imported files or evidence attachments.
- **Case Notes** – Typed notes and observations linked to specific points in the investigation.
- **Search Results** – Will populate with any captured web search result pages.

Each tab is interactive and displays artefacts as "cards" — which you can click for more information or export later.

Left-Hand Toolbar (Navigation Panel)

This vertical menu gives you fast access to OSIRT iii's tools:

- **Search**, **Screenshot**, **Snippet**, **Screen Recording**
- **Dark Web Capture**, **Video Download**, **Website Download**
- **mOSIRT** (mobile tools), **Export Report**, and more.

This means you're never more than one click away from capturing or importing evidence.

This dashboard is designed to give you a complete view of the investigation — from administrative details to real-time evidence collection — all in one secure interface.

Navigation Panel Breakdown

Taking a Screenshot

The **Screenshot** tool is one of the most frequently used features in OSIRT iii, allowing you to quickly capture visual evidence from any screen connected to your system.

To access it, simply click the **camera icon** on the left-hand navigation bar labelled **"Screenshot"**. This opens a slide-out panel on the right-hand side of the screen with the following options:

Select a Screen

Use the dropdown menu to choose which monitor or screen you want to capture. If you have more than one screen connected, they'll appear as "Screen 1", "Screen 2", etc. A small **live preview thumbnail** will appear below to help confirm the correct screen is selected.

Delay Before Screenshot

Use the slider to set a **delay timer** (in seconds) before the screenshot is taken. This is especially helpful if you need to arrange your desktop or hover over a menu before capturing.

Take Screenshot Button

When ready, press the **"Take Screenshot"** button. OSIRT iii will:

Capture the full visible screen

Automatically store the image within your active case folder

Calculate a **SHA-512 hash** to ensure authenticity

Log the capture time and metadata in the case log

Captured screenshots will then appear in the **"Captures"** tab, clearly marked and timestamped.

Region Snippet Tool

The **Snippet** feature lets you capture a specific rectangular portion of your screen — perfect for isolating relevant parts of a webpage, chat, image, or video without saving the full screen.

To access the tool, click the red **scissors icon** on the left navigation bar labelled **"Snippet"**.

When activated, your screen will dim and a **red dashed selection box** appears, which you can move and resize to highlight the area you want to capture.

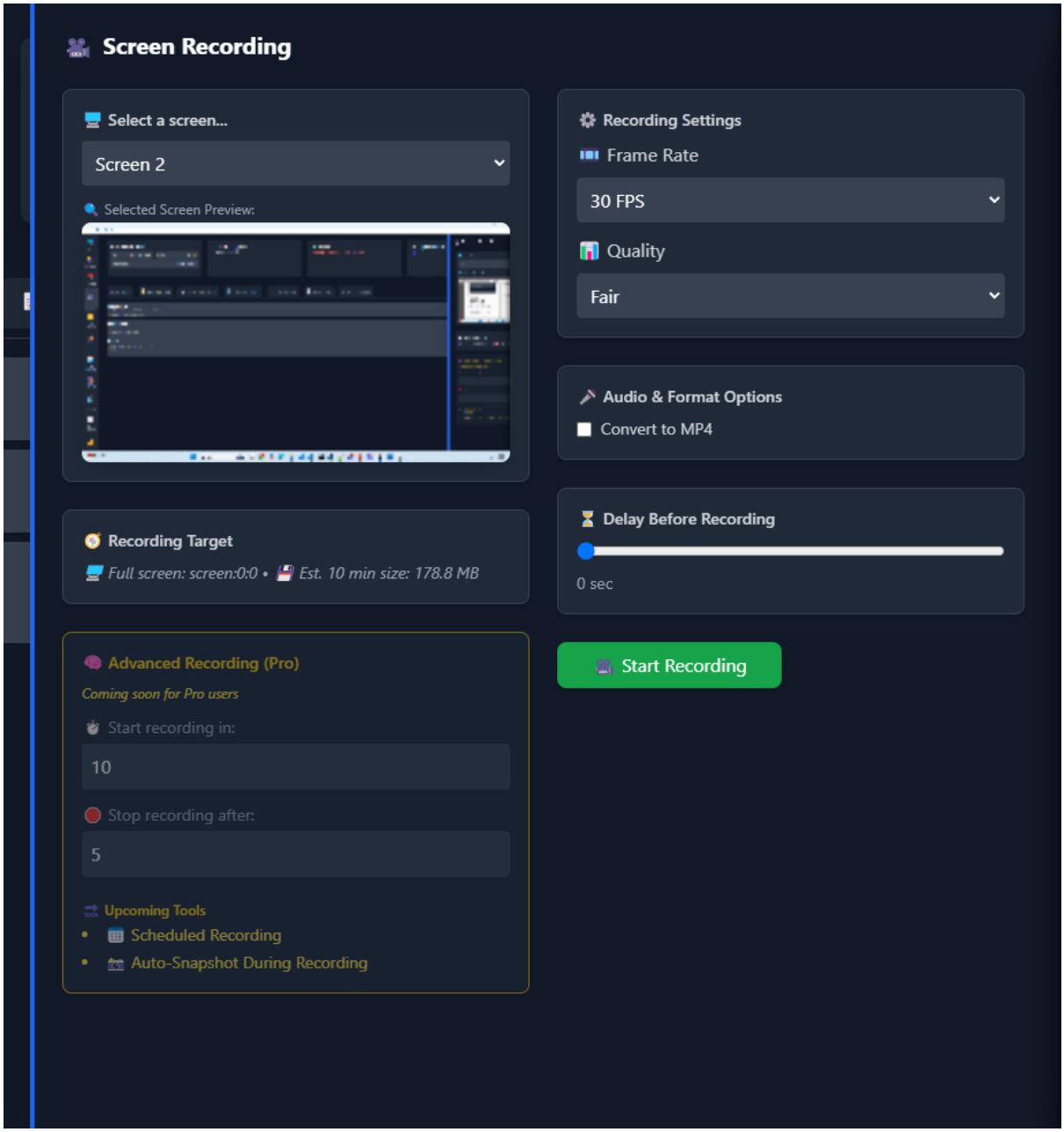
At the bottom of the screen, you'll see a small control bar with the following options:

- **Capture**: Click this to take the screenshot of the selected area. The image will be automatically saved into your case and recorded in the log.
- **Cancel**: Exits the tool without capturing anything.
- **Enable Click-Through**: Allows you to interact with content (e.g., open dropdowns or right-click menus) beneath the selection box before capturing.
- **Delay**: Set a timer (in seconds) before the capture is taken. This gives you time to prepare the area, such as opening tooltips or hovering over content.

Captured snippets are treated the same as full screenshots — complete with hash validation, timestamp, and file logging.

This tool is ideal for focused evidence gathering when only a part of the screen is relevant.

Screen Recording



The **Screen Recording** tool in OSIRT iii lets you record visual activity across your screen — including **sound**, and optionally, **a specific region** of the screen rather than the full display. It's ideal for capturing dynamic interactions, social media scrolling, live chats, or evidence that unfolds over time.

Click the **purple camera icon** labelled **“Screen Recording”** from the left navigation panel to open the recording interface.

Select a Screen

Choose which display you want to record from the dropdown menu. A live thumbnail helps confirm you’ve selected the right one.

Region Selection

Although the default is full-screen capture, you can also record a **custom region** of the screen. This is particularly useful when you want to isolate a specific window, chat box, or browser pane while ignoring the rest.

Recording Target

The interface will indicate whether you're recording the full screen or a region. It also estimates the file size for a 10-minute recording based on your settings.

Recording Settings

- **Frame Rate**: Choose the smoothness of playback (e.g. 30 FPS for standard quality).
- **Quality**: Adjust recording quality — higher quality means clearer video but larger file size.

Convert to MP4 ⭐ (Pro feature)

Tick this to automatically convert the recording from .webm to .mp4 format when it's done. MP4 is a more portable and compatible format, especially for exporting evidence.

Delay Before Recording

Set a short countdown (e.g. 5 or 10 seconds) before the recording begins. This gives you time to prepare content or open necessary tabs.

Start Recording

Click the **green "Start Recording"** button to begin. A clear interface will allow you to stop the recording at any time. Once stopped:

- The file is saved directly to your case folder.
- It's logged in your case record with a **timestamp** and **SHA-512 hash**.
- It appears under the **Screen Recordings** tab in the dashboard.

⤓ Video Downloading

The **Video Download** tool allows you to collect online video evidence directly from platforms like YouTube, providing a forensic copy of visual content that might otherwise change or be removed. It's a crucial tool for investigations involving user-generated content, misinformation, or social media activity.

Click the **blue-and-pink download icon** labelled **"Video Download"** in the left-hand navigation bar to open this tool.

Video URL

Paste a valid video link (e.g. from YouTube) into the **Video URL** field. Supported URLs typically include public, non-password protected videos.

Check URL

Click **"Check URL"** to validate the link. If successful, OSIRT iii will:

- Connect to the platform
- Extract video metadata
- Display a **thumbnail preview**
- Show the **video title** underneath

This lets you visually confirm you're about to download the correct content.

Download Video

Once the video is verified, click the green **“Download Video”** button. OSIRT iii will:

- Download the video directly to your active case folder
- Assign a **SHA-512 hash** for authenticity
- Log the action with a **timestamp** and full metadata
- Display the video under the **Captures** tab in your case

The file is stored in its original resolution and format to preserve evidential quality.

Version Check

The **Video Downloader** section at the bottom allows you to check for updates to the underlying download engine — ensuring it stays compatible with evolving video platforms.

This tool gives you a way to **secure online video content before it’s altered or removed**, preserving it as evidence that can be reviewed or included in reports.

mOSIRT Capture (Mobile Evidence Collection) ☆ (Pro feature)

The **mOSIRT** tool lets you capture screenshots, recordings, and logs from an Android device connected to your computer. It's designed for mobile evidence collection in live investigations and works through USB using Android’s debugging capabilities.

To open it, click the **mOSIRT icon** from the left-hand navigation menu.

Setting Up Your Android Device

Before mOSIRT can detect your phone, you’ll need to prepare the device:

1. **Enable Developer Mode**
   Go to *Settings* > *About Phone* and tap **Build Number** several times until you're told developer options are enabled.
2. **Enable USB Debugging**
   In *Settings* > *Developer Options*, switch on **USB Debugging**.
3. **Connect the Device**
   Use a USB cable to plug your phone into the computer. When prompted on the phone, **authorise** the connection and tick "Always allow from this computer".

Once connected, your device will appear in the dropdown menu, and the status will show as connected.

Capture Options

Once your device is detected, you can perform the following actions:

- **Take Screenshot**
  Captures a still image of the mobile screen, saved directly to your case with a timestamp and hash.
- **Start Recording**
  Begins a live screen recording. You can interact with the device through the mirrored window while recording. Close the window to end the capture.
- **Timed Screenshot**
  Set a delay and take a screenshot after a countdown.
- **Interval Screenshot**
  Automatically take a series of screenshots at set intervals over a chosen duration.

All captures are logged and added to the case file securely.

Mirror Screen

Click **Start Mirroring** to view and interact with the phone's screen from your computer. This lets you navigate apps and content as part of your investigation.

Logcat Console

You can also collect background logs from the device by clicking **Start Logcat**. These logs can reveal technical events, errors, or hidden app activity. You can clear the log, or pop it out into its own window for easier review.

mOSIRT makes it easy to document activity on a mobile device in a structured, tamper-evident way.

🌐 Website Download ☆ (Pro feature)

The **Website Download** tool is designed to collect entire webpages or dynamic websites in a structured, verifiable way. It captures the visible content, background data, and optionally, a full-page screenshot. This is especially useful for preserving online articles, social media threads, and pages that load content as you scroll.

Click the **globe icon** labelled **Website Download** in the left-hand navigation menu to open the capture panel.

Website URL

Enter the full URL of the webpage you want to download. Make sure the page is publicly accessible.

Save Location

Choose where the downloaded content will be stored inside your case folder. Click **Browse** to select or create a subfolder.

Capture Options

- **Capture Images**: Ensures all embedded images on the webpage are downloaded.

- **Take Full Page Screenshot**: Captures a full-length visual image of the webpage from top to bottom, not just what's visible in the browser window.

XHR/Fetch Capture (Optional)

If the page loads content dynamically (e.g. social feeds, comment sections), you can enable **Capture XHR/Fetch**:

- **Poll Interval**: How often OSIRT should check for new content (in seconds).
- **Max Wait Time**: How long OSIRT should keep checking before ending the session.

This is useful for collecting live updates or data that appears as the user scrolls or interacts with the page.

Behaviour Options

- **Max Scrolls**: Defines how far OSIRT should scroll down the page to trigger new content. Increasing this can help capture pages with long feeds or infinite scroll.
- **User Agent**: Lets you specify how OSIRT identifies itself to the website. Default is Desktop, but you can switch to Mobile if needed.

Output Options

- **Generate Index Report**: Produces a summary of all captured content for easy reference.
- **Zip Captured Files**: Automatically compresses the results into a zip file — handy for archiving or sharing.

Once all options are configured, click the **Start Download** button. The entire session will be captured, saved to the case, and logged in your case timeline with hash validation.

📄 Report Exporting

The **Report Exporting** tool allows you to generate a professionally structured report of all evidence and actions taken in a case. This is ideal for internal documentation, briefing materials, or presenting findings in legal or investigative contexts.

Click the **Report Export** icon in the left-hand navigation panel to open the export configuration screen.

Folder Name and Report Name

Enter a name for the report folder and the title of the report file. These fields define how the exported report is labelled and organised.

Save Location

Choose where the report will be saved. Use the **Browse** button to select or create a destination folder.

Upload Logo

You can personalise the report by uploading your organisation's logo, which will appear on the cover page.

Select Data to Include

Tick which case elements you want to include in the report:

- Webpage Log
- Webpage Artefacts
- Videos
- Attachments
- OSIRT Actions
- Case Notes

These will be compiled into a structured, timestamped format with all artefacts linked to their associated hashes and metadata.

Additional Options

- **Export Artefact Notes**: Includes any notes you've made on individual evidence items.
- **Open Report Folder After Creation**: Automatically opens the folder where the report was saved.
- **Save Copy to Case**: Keeps a copy of the generated report in your active case folder.

Date Range

You can optionally filter the report by a date range. Tick **Enable Date Range** to only include actions or evidence captured between specific dates.

Append to Report ⭐ (Pro Feature)

Upload an existing PDF or Word document (e.g. an external statement or summary) and have it automatically added to the start or end of the report. This is available to Pro users.

Insert Blank Pages ⭐ (Pro Feature)

You can choose to insert blank pages at the start or end of the document, useful for printed reports that need separation between sections.

Report Customisation

Add a **protective marking** label, such as “OFFICIAL – SENSITIVE” or your organisation’s internal classification, which will be shown in the header of the report.

Export Report

When ready, click **Export Report** to generate the document. OSIRT iii will compile all selected data into a clean, well-organised PDF with case details, artefact evidence, and audit logs.

The exported report serves as a tamper-evident, court-ready output that mirrors the integrity of your case folder.

⚠ Alerts

The **Alerts** feature lets OSIRT iii automatically watch for specific keywords in the data you collect. If a match is found, the system will trigger an alert — helping you catch important terms, names, or phrases in real time, even across large investigations.

Click the **Alerts icon** in the left-hand toolbar to open this panel.

Enable Alerts

Tick this to turn alerts on. When enabled, OSIRT will monitor incoming artefacts and flag any that contain your specified alert tags.

Add Alert Tag

Type in a keyword you want the system to monitor (e.g. a suspect name, alias, or operation code). Click **Add** to activate it.

Example:
If you enter joe, OSIRT will alert you if that name appears in any supported content.

Active Alert Tags

All active tags are listed here. You can remove any by clicking the red ❌ icon.

Search for Tags In:

Choose the types of data OSIRT should scan for alert tags:

- **URLs** – Flags if a tag appears in a captured link.
- **Plain Text Files** – Includes scraped website text, logs, and notes.
- **Image Files** ⭐ (Pro feature) – Enables scanning for visible text within images using OCR.
- **Documents (PDFs, etc.)** ⭐ (Pro feature) – Enables scanning inside document contents.

This tool is ideal for tracking priority subjects or identifiers without manually reviewing every artefact. Alerts also appear in the top dashboard panel so they're never missed.

🔍 Search

The **Search** tool allows you to quickly find specific words, phrases, or references across all evidence in your case. Whether you're looking for a person's name, a domain, or a keyword, this feature helps you zero in on where it appears across visited websites, artefacts, notes, and more.

Click the **Search icon** in the left-hand menu to open the panel.

Enter Search Term

Type in the word or phrase you want to search for, then click **Start Search**. Matching results will be shown instantly, with highlights showing where each instance was found.

Date Range (Optional)

You can narrow your search by selecting a **start and end date**. This is useful for large cases or when focusing on specific time periods.

Search In

Tick the areas you want to include in the search:

- **Websites Visited**: URLs and metadata from the browsing history.
- **Artefacts**: Screenshots, captures, and files gathered during the case.
- **Videos**: Search filenames and metadata.
- **Attachments**: Files manually added to the case.
- **Notes**: Text from your written observations.

Pro Features ⭐

If you're using OSIRT Pro, additional options become available:

- **Search Text in Documents**: Enables scanning inside file contents like PDFs, Word docs, and spreadsheets.
- **Search Text in Images (OCR)**: Allows OSIRT to read and search for visible text inside images and screenshots.

Results

Search results are grouped by type and shown directly in the **Search Results** tab. Each result includes:

- A link to the original artefact or URL
- A visual preview (where applicable)
- Timestamps, browser used, and file hash

If OCR is enabled and a match is found inside an image, the result will be marked as an **OCR Match** so you know it came from visual content.

This tool is especially valuable when tracking the spread of terms or verifying whether key information has appeared throughout the case.

🖼️ Screenshot Capture Card

When you capture a screenshot in OSIRT iii, it appears as a **visual card** inside the **Captures** tab. Each card provides a detailed, tamper-evident summary of the artefact, combining both visual and technical metadata in one place.

Here’s what each section of a screenshot capture card includes:

Screenshot Preview

A thumbnail of the captured image is shown at the top of the card. This lets you quickly recognise the content at a glance without opening the file.

Hash

Beneath the preview, two hash values are shown:

- The **raw SHA-512 hash** of the file, proving the file's integrity.
- A **shortened display hash** that still uniquely identifies the file, useful for referencing or quick matching.

Timestamp

Displays the exact date and time when the screenshot was taken.

URL

If the screenshot was taken from a webpage using the OSIRT browser extension, the URL is automatically recorded and displayed here.

Browser

Lists the browser used to take the screenshot — helpful for establishing context or verifying how the content appeared.

Export to Report

Ticking this box ensures the screenshot is included in the final report when it's exported. You can untick it if you prefer to exclude this particular capture.

Action Buttons

- **View**: Opens the full image in a separate viewer.
- **Extract Text** ⭐: (Pro feature) Runs OCR on the image to extract any visible text — useful for analysing screenshots of messages or documents.
- **Save a Copy**: Lets you export a separate copy of the screenshot to a location of your choice.
- **Note**: Allows you to attach a comment or observation directly to the capture, which will be included in the case log and final report.

These cards give you a complete, evidence-ready record of every screenshot you capture, combining image, metadata, and user input in a single place.

Image Viewer

Clicking **View** on any screenshot capture card opens the **OSIRT iii Image Viewer**, a dedicated window for examining, exporting, and annotating visual evidence. It's built to give investigators an easy way to review full-resolution images while also preparing them for presentation or inclusion in reports.

Here's what you can do in the viewer:

Zoom and Navigation

Use the **+ / – / Fit to screen / 1:1** controls at the bottom to zoom in and out or reset the image to its actual size. This makes it easy to inspect small details, such as chat messages, timestamps, or embedded links.

Save Annotated

Click **Save Annotated** to export a copy of the image with a **timestamp and the source URL** overlaid directly onto the screenshot. This provides clear, visible context and traceability — ideal for courtroom evidence or case summaries.

The annotation is automatically formatted and positioned for legibility, ensuring no critical content is obscured.

Save as Printable PDF

This option allows you to export the screenshot as an A4 PDF version, preserving the full image at high quality. This is useful for hard-copy printing or when submitting digital bundles that require PDF-only formats.

The viewer makes it easy to transition from raw capture to presentable, context-rich evidence in just a couple of clicks — all while maintaining forensic integrity.

📄 Text-Based Capture Card (e.g. Page Source)

When you capture a text-based artefact — such as a webpage's **HTML source**, a JSON response, or any structured text — OSIRT iii generates a detailed **text artefact card** within the **Captures** tab.

These cards ensure every detail of the captured content is stored safely, hash-verified, and available for export.

File Type

The card clearly identifies the type of capture, such as **Page Source Captured**, and includes a link to preview the content in plain text format. Clicking **Preview** allows you to quickly check the contents without opening an external editor.

Hash

Every captured file includes:

- A unique identifier for the capture
- A **SHA-512 hash** to verify the integrity of the file

This ensures the evidence hasn't been altered since it was captured.

URL

Shows the exact webpage address from which the page source was taken — critical for verifying the origin of the content.

Timestamp

Displays the exact date and time the source was captured, recorded to the second.

Browser

Indicates which browser version was used during the capture — helpful when reviewing differences in how sites behave across browsers.

Export to Report

Tick this box to include the artefact in your final report. If left unticked, it will remain in the case file but be excluded from the export.

Action Buttons

- **View File**: Opens the full source code or text content in a clean, readable format.
- **Save Copy**: Saves a duplicate of the file outside the case, if needed.
- **Add Note**: Lets you attach context or observations to the artefact.

Text artefacts are especially valuable for verifying background code, form content, embedded scripts, or timestamps that aren't visible in a regular screenshot. OSIRT ensures this data is captured and preserved in its original form for later analysis or courtroom use.

🗃 MHTML Capture Card

When you capture an **MHTML** file in OSIRT iii, the entire webpage — including layout, styling, images, and text — is preserved in a single, self-contained format. This is especially valuable for storing live pages exactly as they appeared at the time of investigation, without relying on an internet connection to view them later.

Captured MHTML artefacts are displayed as dedicated cards in the **Captures** tab.

Preview and Metadata

Each card provides:

- A **Preview** link for quickly checking the content.
- The **original URL** of the captured webpage.
- A **timestamp** indicating the exact moment the page was saved.
- The **browser version** used during capture.

View File

Clicking **View File** opens the MHTML in OSIRT's built-in **offline viewer**. This ensures:

- The page renders safely and accurately without making a live network connection.
- No scripts, redirects, or live content are reloaded — preserving the forensic integrity of the capture.

This is particularly useful when reviewing pages that could contain dynamic or potentially harmful elements, as the offline viewer neutralises active content.

Other Options

- **Save Copy**: Allows you to save an additional copy elsewhere if needed.
- **Add Note**: Attach your own commentary, findings, or observations.
- **Export to Report**: Toggle to include or exclude this artefact in the final exported case report.

MHTML captures offer a reliable, verifiable way to preserve how a webpage looked at a specific point in time, with full visual fidelity and zero risk of altering or reloading live content.

Case Notes

The **Case Notes** tab in OSIRT iii provides a secure, timestamped space to document observations, actions, and investigative decisions throughout the life of a case. It functions as your digital notebook — perfect for recording context that isn't tied to a specific artefact.

You can access it any time by clicking the **Case Notes** tab at the top of the interface.

Writing Notes

Simply type your note in the large text field. You can enter up to **5,000 characters** per note, giving you plenty of space for detail.

Notes might include:

- Observations about evidence
- Summaries of investigative steps
- Reminders or next actions
- Interview snippets or leads

Saving Notes

Click **Save Note** to store it. Once saved:

- The note is locked in with a **timestamp**
- It's added to your case log for full traceability
- The note becomes available for inclusion in your **exported report** if selected

Each saved note is preserved in the order it was entered, helping maintain a clear narrative of your investigative process.

Notes are not linked to specific artefacts — if you want to annotate an individual screenshot, file, or recording, use the **Add Note** button found directly on that item's capture card instead.

The Case Notes tab is designed for general-purpose recording — perfect for staying organised and ensuring that your thought process is documented alongside the evidence.

🧩 Customising Layout: Swapping Icons, Tabs and Cards

OSIRT iii gives you flexibility to arrange your workspace the way you prefer. Many parts of the interface — including sidebar icons, dashboard tabs, and evidence cards — are **swappable**, meaning you can change their order by simply dragging them.

Sidebar Icons

The icons on the left-hand side (like Screenshot, mOSIRT, Dark Web, etc.) can be rearranged to suit your workflow. Just click and drag an icon up or down to move it to a different spot.

Dashboard Tabs

Tabs such as **Captures**, **Complete Log**, **Screen Recordings**, and others can also be reordered. Want "Attachments" to appear first? Just drag it to the left. The order will stay how you leave it, making it easier to prioritise the sections you use most often.

Dashboard Cards (Top Row)

- Investigation Details
- Alerts Triggered
- Status
- Capture Count

can be **dragged and dropped** into a different order. Simply click and hold on a card, then drag it left or right to reposition it. This is useful if, for example, you want the Status card to always appear first or want Alerts to be more visible during active monitoring.