野生動物長期監測系統之優化與資料整合計畫 (4/4)

Optimization of the long-term wildlife monitoring system and data integration (4/4)

成果報告書

下冊：自動相機資訊系統開發

113農科-7.2.6-林-01

執行單位：國立屏東科技大學、國立嘉義大學、
中央研究院

計畫主持人：翁國精

共同主持人：劉建男、端木茂甯

計畫助理：古馥宇、李思賢、張俊怡、張筑竣、李金穎、
劉士豪、沈祥仁、周庭安、王人凱

中華民國113年12月

摘要

系統維運與開發部分，TaiBIF 團隊持續根據今年度所蒐集到之使用者回饋更新與優化程式。上傳程式介面調整內容包含連拍補齊功能可設定到秒數、編輯區塊提供使用者選擇字體大小功能、鳥類清單位置調整、新增同步上傳狀態功能、提供 csv 範例檔與物種清單 csv 檔供匯入功能參考使用、資料上傳時提醒尚未填寫物種欄位之資料有哪幾筆、上傳狀態通知調整為僅寄到當次資料夾上傳者與管理者之信箱等；線上系統調整部分則包含查看影像資料頁面版面及功能優化、新增受委託單位計畫成員權限、新增管理者刪除計畫功能、資料下載同時提供 csv 與 excel 類型的檔案、新增聯絡我們頁面的附加檔案類型等。針對更新、調整後的上傳程式介面與線上系統，本團隊辦理了四場教育訓練並完成對應的引導說明內容調整，另外線上系統今年度所有調整內容亦皆已進行資安檢測，確保無高風險資安問題。本年度亦完成上傳程式介面正式開放予第一線人員使用前所累積之自動相機舊資料清理並匯入至系統，雲端系統亦持續維持功能正常運作之狀態。除此之外，由於今年度確定不進行系統移轉作業，故未有相關之系統移轉計畫，但計畫團隊仍完成系統程式說明及資料標準文件撰寫，作為本四年期計畫之整體系統狀況參考。

目錄

一、 前言……..1
二、 計畫目標……5
三、 重要工作項目及實施方法……..5
1. 上傳介面功能優化……5
2. 線上系統功能優化……6
3. 系統維運及移轉準備……6
4. 教育訓練……7
四、 預期效益……..8
五、 期末評核標準……..8
六、 結果與討論……..9
1. 上傳介面功能優化……9
2. 線上系統功能優化……..13
3. 系統維運及移轉準備……..15
4. 教育訓練……..16

附錄1、資安檢測報告……26
附錄2、自2023年度期末報告撰寫完畢後至本期末報告撰寫完畢前所蒐集之意見回饋內容表單……45
附錄3、系統程式說明及資料標準內容……52
附錄4、臺灣自動相機資訊系統教育訓練計畫書……71
附錄5、上傳程式引導說明教學文件……74
附錄6、線上系統引導說明教學文件……..144

圖目錄

圖1、連拍補齊功能原本僅能設定到分鐘，調整為可設定到秒數...10
圖2、可於上傳程式介面的編輯區塊調整字體大小，目前提供三種尺寸供使用者選擇.....11
圖3、原鳥類清單中的鳥種移至物種下拉選單選項中.....11
圖 4、同步上傳狀態功能.....12
圖5、上傳介面程式資料夾中提供csv範例檔與物種清單csv檔.....12
圖6、資料上傳時出現彈出視窗提醒尚未填寫物種欄位之資料有哪幾筆.....12
圖7、查看影像頁面新增媒體類型及備註兩項篩選條件.....14
圖8、查看影像頁面的資料筆數每頁最多可呈現至1,000筆.....14
圖9、可在計畫管理-計畫成員頁面中進行受委託單位權限設定.....14
圖 10、計畫管理-基本資訊頁面中新增刪除計畫功能.....15
圖 11、四場教育訓練辦理情形.....17
圖12、教育訓練回饋問卷統計—操作流程介紹說明是否清楚明瞭..18
圖13、教育訓練回饋問卷統計—線上系統是否符合使用需求.....19
圖14、教育訓練回饋問卷統計—上傳程式介面是否符合使用需求..20

表目錄

表 1、自 2022 年 12 月 29 日系統正式上線截至今年度 11 月 5 日期間的上傳介面版本與對應之已上傳資料數量.....21
表 2、上傳程式介面中可供選擇之物種.....24
表 3、四場教育訓練各分署參與總人次.....25

一、前言

問題分析

過去國內自動相機資料欠缺整合的平台，也欠缺對相關調查計畫、拍攝影像及影片的管理機制，以致於難以整合不同計畫所收取的資料，也無法即時提供分析結果以支援及評估保育決策。隨著近幾年自動相機資料持續且快速地累積，對相關資料與資訊妥善地進行倉儲、管理與整合，便成為影響資料應用價值的重要關鍵。

為此，於民國107至108年，農業部生物多樣性研究所（前身為農委會特有生物研究保育中心）委託中央研究院生物多樣性研究中心的臺灣生物多樣性資訊機構（TaiBIF 團隊），建置完成「臺灣自動相機資訊系統」，提供一雲端資料整合及資訊管理平台，支援從自動相機影像檔案的倉儲、影像與計畫資訊的擷取及管理、計畫及資料的篩選與下載，到資料的分析及計畫的管考。此系統利用雲端服務降低開發跟維護的人力，成功地將過去自動相機資料生命週期中各階段的工作統整於單一平台、提供支援各項工作的線上工具，並確保相關資料與資訊得以在一致的結構與格式下進行倉儲及後續利用。自民國109年起，TaiBIF 團隊舉辦數次教育訓練，協助林業保育署各分署同仁使用該系統，並將歷年長期監測系統累積之照片上傳至臺灣自動相機資訊系統中，以利野生動物長期監測在照片資料倉儲、查詢、統計、管考等工作的執行。

然而經過一年的實務操作，雖然這套系統在一般網路環境下能使用無礙，但在林業保育署各分署及工作站的第一線人員操作這套系統時，卻受限於網路頻寬不佳，無法順暢於線上操作系統，或甚至無法完整上傳大量影像資料。因此，此段期間仍委由 TaiBIF 團隊由後端上傳歷年累積之照片至自動相機資訊系統上。此外，由於原先系統的設計支援整個資料生命週期中各階段參與人員的使用，提供的功能多樣，又加上當初設計時希望盡量擷取相關資訊，以致介面的操作相對複雜，所需填寫的內容相對繁複。雖已提供詳盡的操作說明手冊，並盡量減少必填資訊，但使用者仍多反映希望簡化操作介面。同時，相對完整

的資訊擷取也造成系統後端資料結構複雜，增加系統維運及後續功能優化上的困難。

最後，除了支持科學研究與決策的價值外，自動相機影像與資料在對一般民眾傳遞自然環境與生物多樣性的重要性上，以及對於學校教育的應用上，也具有極高的潛力，值得進一步探索此資訊系統支援相關應用的可能性。

擬解決問題重點

1. 解決目前系統在網路不佳之環境下的操作問題，以確實支援第一線工作人員的使用需求。
2. 優化系統前端的操作介面及簡化後端的資料結構，以提升系統操作及管理上的便利性。
3. 提升系統的應用，除強化資料分析與計畫管考功能外，並探索支援學校課程教學及科普教育推廣的應用性。

前人研究概況

中研院 TaiBIF 團隊所建置之「臺灣自動相機資訊系統」(https://camera-trap.tw/)，提供資料上傳、編輯、影像瀏覽與標註等工具與介面。使用者可以上傳照片及影片到系統中，在多數人所習慣使用的試算表介面進行物種辨識資料的登打及修訂；資料編輯同時，影像及影片可以自動播放，讓編輯工作可以流暢地進行。系統也提供資料篩選與基本的計算分析功能。使用者可以依照計畫名稱、資料收集時間與地點、標註的物種等資訊進行資料的搜尋與篩選。所篩選出的資料可以下載，也可以於系統上計算包括相機工作時數及各類 OI 值等數值，並以圖表顯示計算結果。

計畫管理與管考功能方面，系統提供計畫、樣區、相機位置、相機，以及資料收取行程的管理，使用者可以新增這些項目，並編輯各項目下的細項資訊。使用者在計畫總覽頁面可以瀏覽自己所屬的各計畫，以及所有於系統中開放瀏覽使用的計畫，或依照計畫名稱、計畫時間及計畫中標註的物種等資訊進行篩選。各計畫的首頁中顯示影像收取與物種標註的進度狀況，並可產生每月的資料繳交進度報表，協助計畫管考。

為了增加系統的可使用性，TaiBIF團隊於本計畫第一至第三年度(2021年-2023年)針對林業保育署各分署及工作站等第一線資料上傳人員開發完成上傳程式介面並優化線上系統，上傳程式介面功能包含了影像檔瀏覽與管理、影像資料的標註與上傳功能，資料上傳者可直接於離線的狀況下在電腦端匯入照片並編輯資料，等到上傳資料時才需要連線至系統，且提供資料續傳功能，不易受網路頻寬不足或連線不穩等問題影響，在2023年時亦開發完成文字資料（csv檔案）匯入功能，讓使用者除了匯入影像外，也可以匯入標註的文字資料至上傳程式介面進行資料的編輯與上傳；線上系統除優化現有功能外，亦新增計畫內的相機樣點運作及缺失比例頁面，以方便計畫管理者確認資料上傳狀況，並更新資料視覺化內容以及介面樣式，讓系統整體畫面呈現具有一致性。而為配合上傳介面的開發及因應篩選分析需求，另已調整系統的資料庫架構，將原本系統中的 MongoDB轉換成關聯式資料庫

系統 PostgreSQL，全部採用Python程式語言撰寫，提升系統的效能及維運的便利。

另外，2021年至2023年間已完成共十六場介紹本案系統操作的教育訓練，並已針對部分意見回饋調整系統功能。上傳程式介面及優化後的線上系統已於2023年1月1日上線至正式站供各分署與工作站上傳與管理影像資料使用，截至2023年12月，此系統中已包含從2009年至2023年共40個研究計畫、超過1,000萬筆資料與800萬筆多媒體檔案(影片或照片)，涵蓋全台296個樣區、2,705個相機位置。

二、計畫目標

全程計畫目標

1. 強化自動相機資訊管理系統的使用效能，優化操作介面並提升系統管理、計畫管考與資料分析功能，推廣系統的使用及擴展系統的應用層面。
2. 提供社會大眾、學者專家及管理單位公開的野生動物族群變動趨勢資訊，以利民間、學界、政府三方在野生動物保育及狩獵管理方面的溝通與政策依據。

本（113）年度目標

1. 維運並持續優化線上管理系統及資料上傳程式介面。
2. 研擬並進行系統程式與資料轉移的前置準備工作。

三、重要工作項目及實施方法

1. 上傳介面功能優化

上傳程式介面已於2023年1月1日正式上線供林業保育署及林業分署人員使用，目前資料上傳仍採新舊機制並行的方式進行，一方面由各工作站人員直接利用上傳程式介面輸入並上傳資料，一方面將影像及資料表按過去機制交由各林業分署承辦人員彙整後提供屏科大翁國精老師團隊。今年度計畫團隊持續針對使用者實際操作後提出的反饋調整系統與修復所發現之錯誤，並對新的資料上傳機制與流程進行檢討，依據需要進行調整與優化。上傳程式優先調整的項目包含：

- 根據不同尺寸的電腦螢幕對應調整上傳程式介面的版面呈現，並調整字體大小

- 新增鳥類清單的關鍵字搜尋功能
- 優化連拍補齊功能

2. 線上系統功能優化

目前線上系統前台的主要功能為資料的搜尋及下載,並有針對計畫成員設計的管考功能(即為後台),而為因應未來系統開放後的一般大眾使用需求,也已規劃不同的身份選項供使用者選擇,目前有教師、學生、研究人員、公家機關單位、一般大眾等五個選項,今年度可配合需求新增其他的使用者身份選項,並針對不同身份調整系統使用權限,如涉及敏感物種或相機架設確切點位的相關資料查看權限。在資料搜尋頁面,則針對現有資料欄位強化篩選功能,如影像及時間的相關篩選等,並提供包含csv與excel等至少兩種下載檔案類型。計畫團隊今年度亦持續依據系統使用狀況與問題回饋,調整、優化線上系統其他功能與資料視覺化呈現,以及於計畫結束前對前端及後端系統進行資安漏洞掃瞄,並針對發現之漏洞修補及更新程式碼。調整後的功能操作與使用流程持續補充進問題幫助頁面中,並對應更新操作說明文件內容。

3. 系統維運及移轉準備

計畫團隊今年度持續進行系統操作面相關問題回覆與線上系統錯誤修復,以使系統與相關操作流程能夠穩定運行,另外亦持續維運目前建置於雲端的系統,確保系統功能正常運作,並協助將2023年1月上傳程式介面正式使用前,林業保育署全島監測計畫所產生之自動相機影像與文字資料自後端匯入系統,或利用上傳介面的文字資料匯入功能將舊資料進行上傳。

而為配合後續的系統移轉,計畫團隊將與林業保育署討論系統架構與現有資料轉換至林業保育署內部或國網中心可能會遇到的問題,並協助排除移轉時出現的錯誤樣態。系統移轉作業準備工作預計將於2024年下

半年度開始進行，並將同時展開系統程式說明文件及資料標準文件的撰寫。

4. 教育訓練

本年度將針對林業保育署計畫管理者與執行者，辦理至少4場實體或線上系統操作教育訓練，如為實體辦理，則預計於林業保育署、林業分署或各工作站進行。實際規畫將於計畫執行期間持續與林業保育署討論。

四、預期效益

1. 建立野生動物資源之公開資訊平台。
2. 提升目前自動相機資訊管理系統的效能與功能。

五、期末評核標準

1. 完成系統移轉計畫
2. 完成系統程式說明文件及資料標準文件
3. 更新操作指引說明
4. 進行資安檢測
5. 完成至少 4 場教育訓練

六、結果與討論

1. 上傳介面功能優化

TaiBIF 團隊去年度已使用 python 語法及其內建的 Tkinter GUI 套件完成上傳程式介面的更新與功能優化，今年度 TaiBIF 團隊則針對使用者對於系統的回饋，持續更新與優化程式，以強化自動相機資訊管理系統的使用效能及易用性。目前上傳程式介面的使用者除了林業保育署各分署相關人員外，亦邀請雪霸國家公園執行自動相機業務的成員進行使用，至今本案系統中已有 575,083 筆資料是由雪霸國家公園提供。從 2022 年 12 月 29 日系統正式上線截至今年度 11 月 5 日期間的上傳程式介面版本與對應之已上傳資料數量則如表 1。

以下條列今年度上傳介面優化的主要項目：

- 連拍補齊功能原本僅能設定到分鐘，調整為可設定到秒數（圖 1）
- 調整上傳介面版面呈現使之能適用於各式尺寸的電腦螢幕，並可於編輯區塊調整字體大小，目前提供三種尺寸供使用者選擇（圖 2）
- 原鳥類清單中的鳥種移至物種下拉選單選項中（圖 3），可利用下拉選單的關鍵字搜尋功能選擇特定鳥種，目前可供選擇之物種可參考表 2
- 新增同步上傳狀態功能（圖 4），若使用者遇到資料實際上傳狀態與上傳紀錄不符時，可以使用此功能同步資料庫的上傳狀態
- 於上傳介面程式資料夾中提供 csv 範例檔與物種清單 csv 檔（圖 5），供使用者使用文字資料匯入功能時可參考使用
- 若有資料之物種欄位未填寫，點擊上傳資料夾功能時將跳出彈出視窗提醒尚有哪幾筆資料未填（圖 6）

- 相機上傳狀態通知信調整為僅寄到當次資料夾上傳者與管理者的信箱
- 因應防毒軟體阻擋問題更新相關程式碼，並在每次釋出新版本上傳介面時皆將程式提供給林業保育署，以確認程式碼是否有被誤判情形

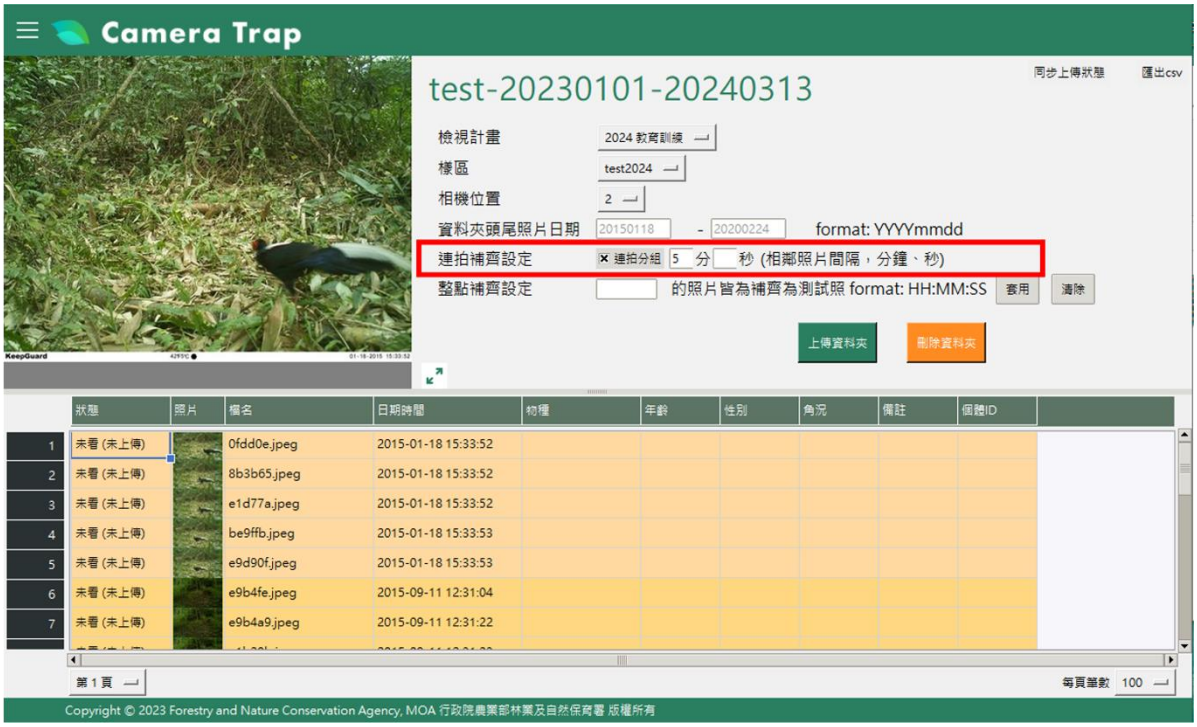


圖 1、連拍補齊功能原本僅能設定到分鐘，調整為可設定到秒數。

圖 2、可於上傳程式介面的編輯區塊調整字體大小，目前提供三種尺寸供使用者選擇。

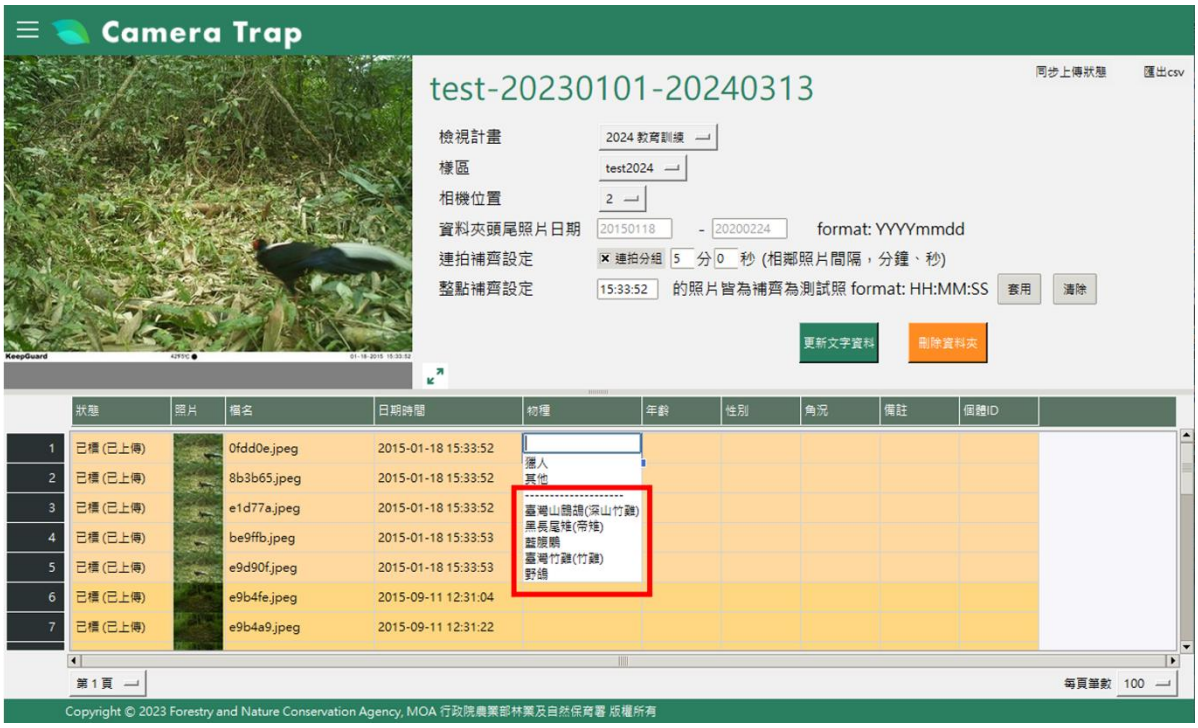


圖 3、原鳥類清單中的鳥種移至物種下拉選單選項中。

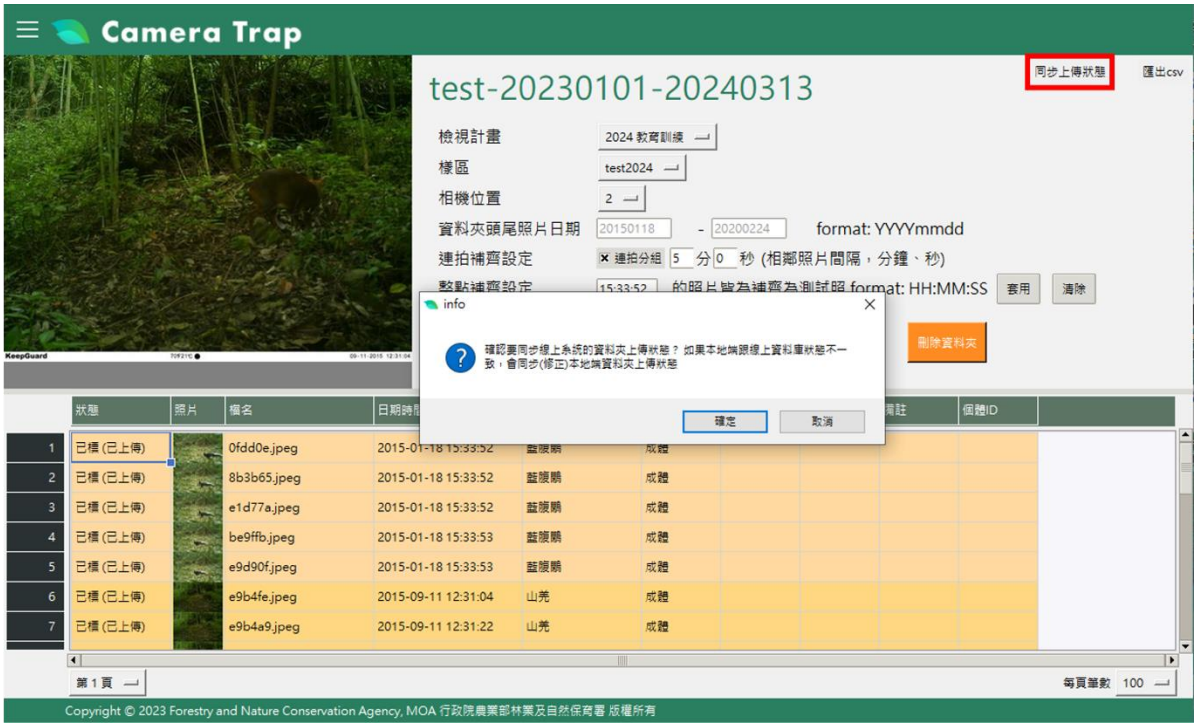


圖 4、同步上傳狀態功能。

圖 5、上傳介面程式資料夾中提供 csv 範例檔（檔名 import-example）與物種清單 csv 檔（檔名 import-example-species）。

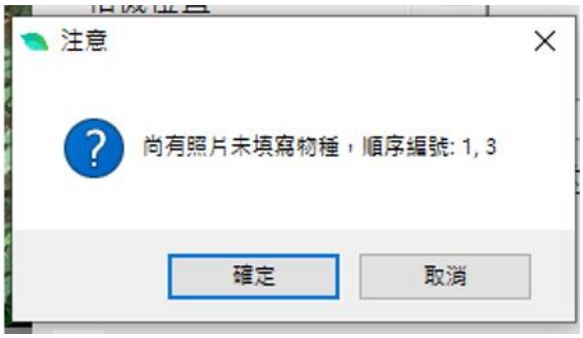


圖 6、資料上傳時出現彈出視窗提醒尚未填寫物種欄位之資料有哪幾筆

2. 線上系統功能優化

今年度上半年 TaiBIF 團隊針對使用者對於系統的回饋，持續更新與優化程式，所調整的項目如下：

- 查看影像頁面新增媒體類型及備註兩項篩選條件（圖 7），並調整時間及日期的篩選功能 bug
- 查看影像頁面篩選條件後顯示的照片自動依照相機位置名稱(A-Z)、日期時間(舊-新)、檔名(1-n)排序
- 查看影像頁面的資料筆數每頁最多可呈現至 1,000 筆（圖 8）
- 新增「受委託單位」權限，可在計畫成員中進行設定（圖 9），受委託單位僅能查看與下載所屬樣區的資訊，且與資料上傳者相同，不能使用包含檢視及編輯計畫管理頁面、編輯或刪除查看影像中的資料等功能
- 於計畫管理頁面中，新增刪除計畫功能（圖 10）
- 計畫管理頁面的計畫管理人與計畫成員依照信箱帳號首位數字與字母(1-n, A-Z)排序
- 資料下載同時提供 csv 與 excel 類型的檔案供使用者選擇
- 聯絡我們頁面的附加檔案功能新增可附加 db 檔及 zip 檔兩種檔案類型
- 其他細部調整，包含首頁及計畫資訊頁面的地圖呈現邏輯優化、查看影像頁面的版面優化、資料篩選與計算頁面的計算錯誤問題處理等

上述優化及調整內容皆已更新至正式站(https://camera-trap.tw/)，在經過 TaiBIF 團隊內部測試、並於教育訓練中供各分署學員實際操作確認無功能缺失後，現已通過資安檢測並確保無高風險資安問題（附錄 1）。

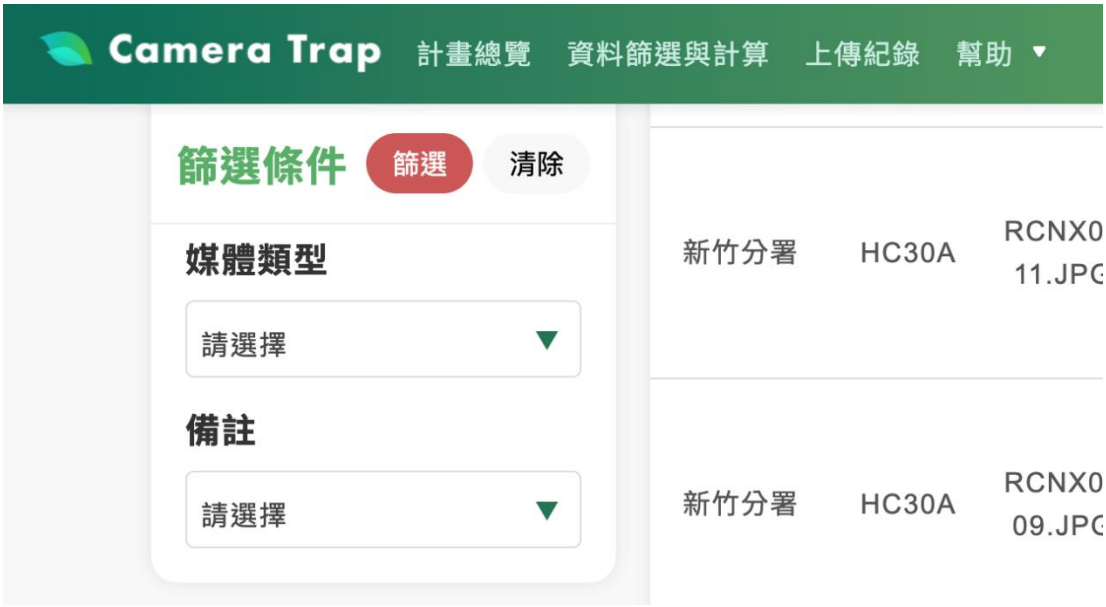


圖 7、查看影像頁面新增媒體類型及備註兩項篩選條件。

圖 8、查看影像頁面的資料筆數每頁最多可呈現至 1,000 筆。

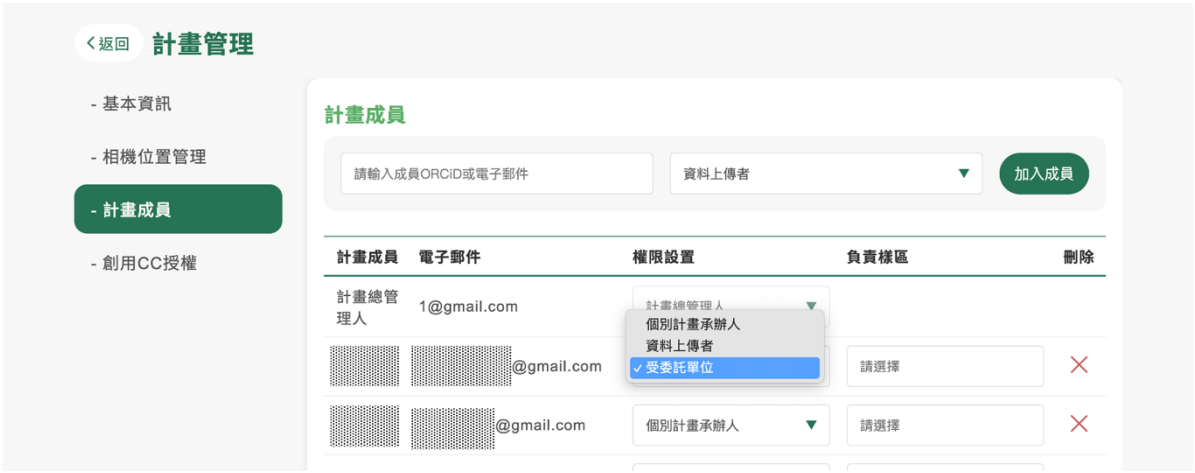


圖 9、可在計畫管理-計畫成員頁面中進行受委託單位權限設定。

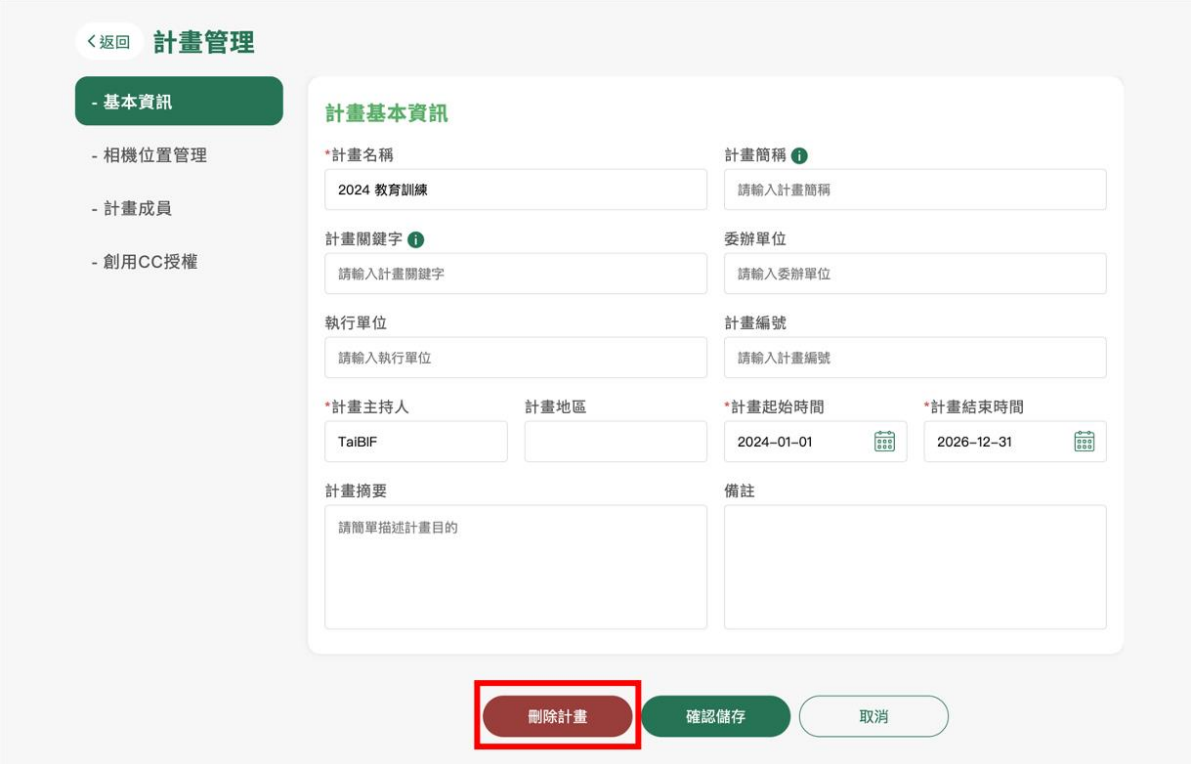


圖 10、計畫管理-基本資訊頁面中新增刪除計畫功能。

3. 系統維運及移轉準備

自 2023 年度起，林業保育署各分署及工作站人員開始透過本案系統上傳資料，TaiBIF 計畫團隊於此期間除了持續維持系統正常運作外，亦針對蒐集到之意見回饋調整與優化系統，自 2023 年度期末報告撰寫完畢後至本期末報告撰寫完畢前所蒐集到之相關意見回饋內容均整理成表單（附錄 2），以供查閱問題處理狀況。

過去由於各分署及工作站的第一線人員受限於網路頻寬不佳，無法順暢於線上操作系統，或甚至無法完整上傳大量影像資料，故於上傳程式介面正式開放予第一線人員使用之前，累積之自動相機舊資料由本團隊協助從雲端系統後台上傳。目前計畫團隊已將所有上述舊資料清理完畢（包括清點舊資料欄位及對應等）並匯入至新系統。

目前的雲端系統持續維持功能正常運作之狀態,所有資料仍繼續於 AWS 雲端服務託管，未受後端系統調整的影響。系統所使用的 AWS 雲端服務包含了 AWS EC2 運算單元（8G 記憶體、2 vCPU）及 AWS S3 物件儲存(Object Storage)服務，且目前已使用了大約 38 TB 的資料空間。

系統移轉工作部分於上半年度與林業保育署討論後,確認可採取以下四種可能形式：

- 使用國家高速網路與計算中心所提供之雲端服務
- 使用中華電信所提供之雲端服務
- 直接移轉至林業保育署之內部機房
- 繼續使用 AWS 雲端服務，但將系統搬遷至林業保育署之 AWS 帳號

後續在林業保育署之考量下,確定本計畫今年度不執行系統移轉工作,明年度系統亦將繼續透過本團隊 AWS 帳號下之雲端服務進行託管。但為了未來可能的移轉工作，我們仍完成系統程式說明及資料標準文件的撰寫，作為本四年期計畫之整體系統狀況參考，目前的系統程式說明及資料標準如附錄 3。

4. 教育訓練

為讓本案系統的使用能夠有效納入第一線人員自動相機資料收集、分析、管理的流程中，以建立資料完善發布機制，本團隊於今年度上半年 5 月 31 日及 6 月 14 日、與下半年 10 月 8 日及 10 月 14 日，在中央研究院辦理了共四場教育訓練，針對林業保育署各分署之自動相機相關業務執行者與管理者進行自動相機設置與系統操作之說明，共計 111 位相關人員參與（圖 11），各分署參與人次如表 3。課程除了提供自動相機設置的基本原則說明與物種辨識技巧外，亦透過實作練習方式，讓每位學員皆可使用電腦實際按步驟操作，將測試資料上傳至線

上系統中，並引導學員使用線上系統的其他功能。課後則邀請學員填寫線上問卷，提供操作上的回饋意見，四場教育訓練共蒐集到 78 份問卷，上半年場次及下半年場次各有 93.8 %與 100 %的學員認為操作流程介紹清楚明瞭（圖 12）、各有 85.4 %與 93.3 %的學員認為線上系統有符合使用需求（圖 13）、負責資料上傳工作的學員中則各有 86.4 %與 100 %認為上傳程式介面有符合使用需求（圖 14）。課程內容細節請見臺灣自動相機資訊系統教育訓練計畫書（附錄 4）。

在四場教育訓練皆完成後，本案系統提供的引導說明教學文件也進行了對應的內容調整（附錄 5 及附錄 6），並同步更新至上傳程式介面的教學說明頁面與線上系統的常見問題頁面中。

圖 11、四場教育訓練辦理情形。

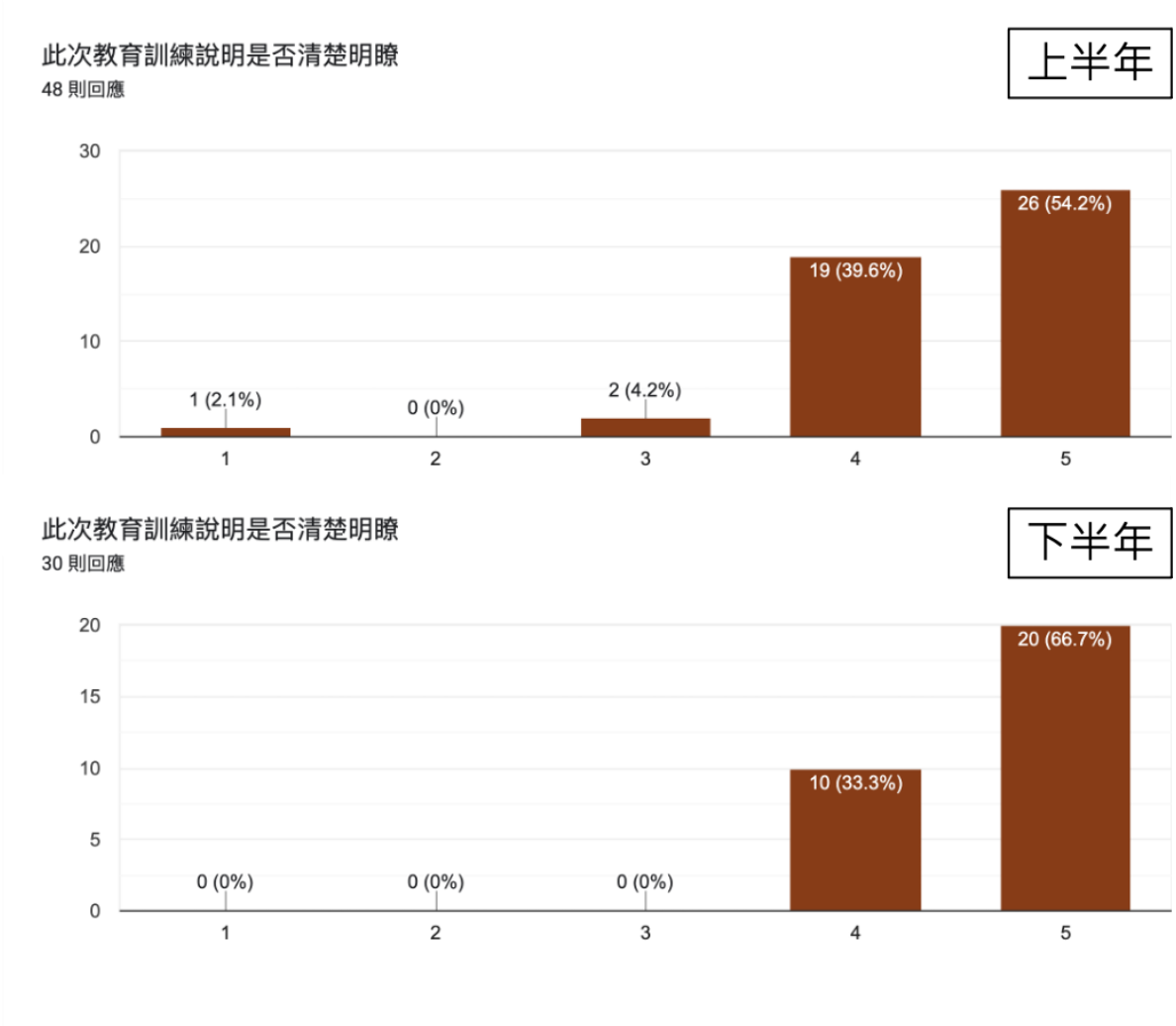


圖 12、教育訓練回饋問卷統計—操作流程介紹說明是否清楚明瞭（縱軸為回應數，橫軸 1 至 5 分別為非常不清楚至很簡單易懂）。

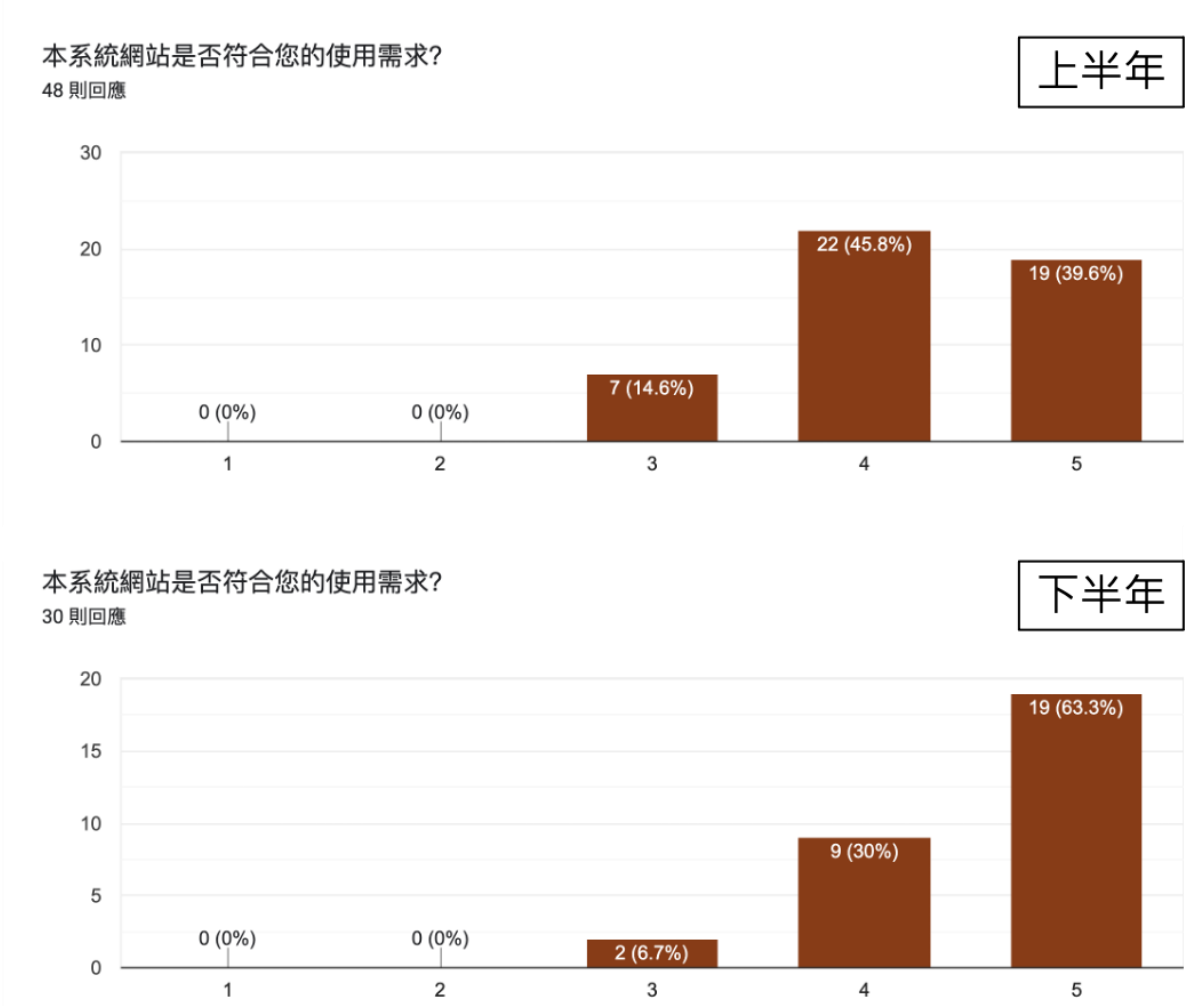


圖 13、教育訓練回饋問卷統計—線上系統是否符合使用需求（縱軸為回應數，橫軸 1 至 5 分別為非常不符合至非常符合）。

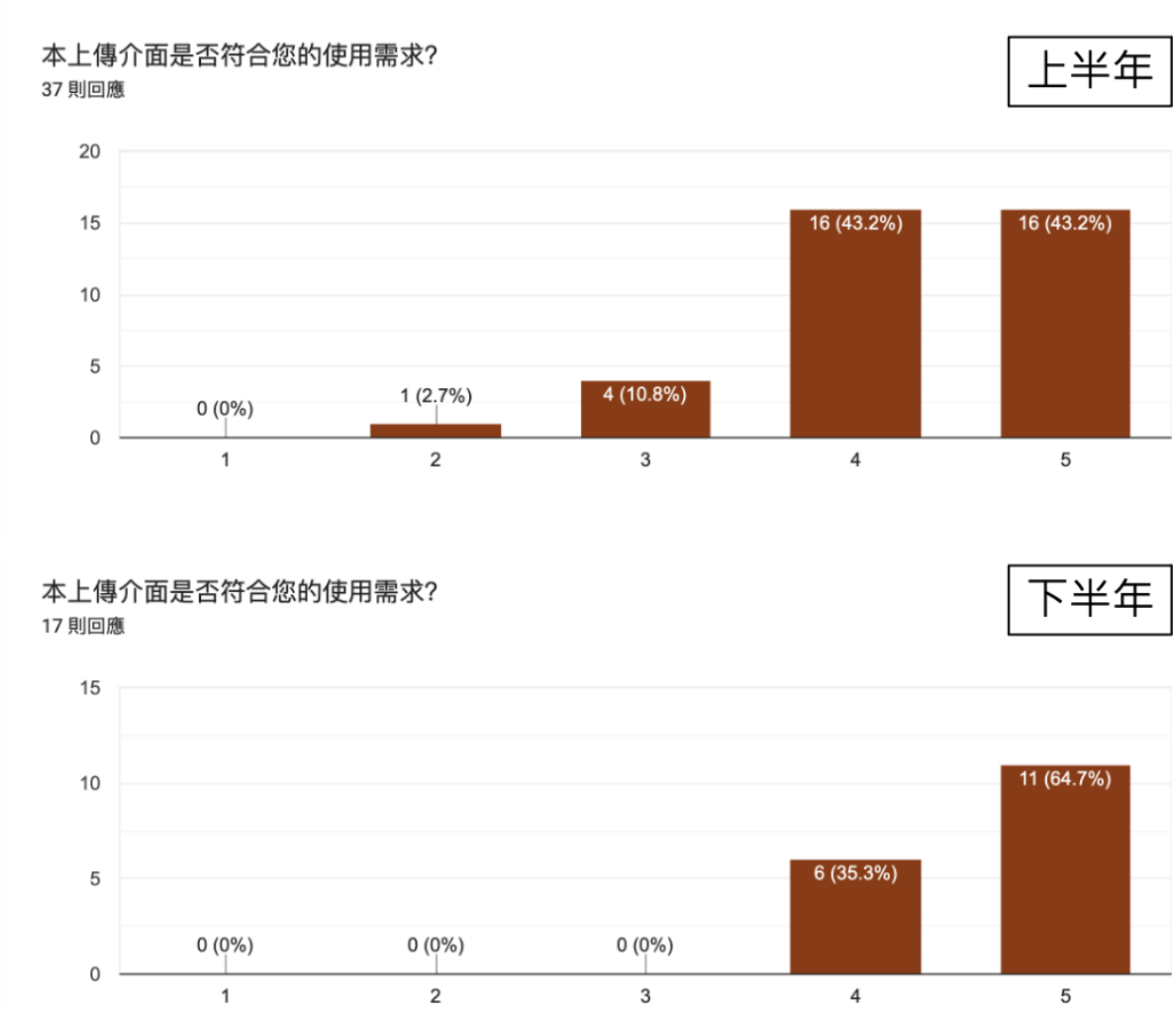


圖 14、教育訓練回饋問卷統計—上傳程式介面是否符合使用需求（縱軸為回應數，橫軸 1 至 5 分別為非常不符合至非常符合）。

表 1、自 2022 年 12 月 29 日系統正式上線截至今年度 11 月 5 日期間的上傳介面版本與對應之已上傳資料數量。

版本	釋出日期	更新內容	已上傳資料數量
v1.0.0	2022/12/29	正式上線的第一版	540,123
v1.1.0	2023/03/02	● 可選擇單頁呈現資料筆數 ● 匯出資料功能問題調整 ● 說明頁改為以彈出視窗顯示 ● 其他操作與上傳 bug 調整	781,323
v1.1.1	2023/05/10	● 新增「匯入資料夾時判斷資料夾名稱是否與已上傳之資料夾名稱重複」功能（此版本匯入資料夾時亦需連網） ● 新增「判斷上傳程式版本是否為最新版」功能 ● 資料夾匯入未完成時將無法關閉程式，避免後續影像匯入排程錯誤 ● 資料上傳時將不能進入資料夾編輯，避免後續資料上傳排程錯誤 ● 其他操作與上傳 bug 調整	43,047
v1.1.2	2023/06/21	● 新增資料編輯介面中的欄位拖曳下拉複製內容方式 ● 其他操作與上傳 bug 調整	559,261
v.1.1.6	2023/10/27	● 新增帳號登入功能：與線上系統相同，需使用 orcid 帳號登入，登入後即可選擇可上傳之計畫與對應樣區/相機位置 ● 新增文字資料與對應影像匯入功能：可匯入已標註欄位內容之 csv 文字檔與對應影像，csv 資料欄位需與現有上傳程式欄位相同，並需有影像檔名欄位 ● 連拍補齊功能調整為預設開啟 ● 物種選項調整：飛鼠改為「大赤鼯鼠」「白面鼯鼠」「小鼯	527,798

		鼠」，松鼠改為「赤腹松鼠」「條紋松鼠」「長吻松鼠」 ● 影像匯入錯誤時調整為可點擊進資料夾刪除此匯入錯誤資料夾 ● 其他操作與上傳 bug 調整	
v.1.1.7	2024/02/16	● 停止 v1.1.2(含)以前的上傳功能服務 ● 連拍補齊設定功能調整為可設定到秒數 ● 物種下拉選單選項與鳥類清單選項更新 ● 因應防毒軟體阻擋問題更新相關程式碼 ● 其他操作與上傳 bug 調整	218,083
v.1.1.8	2024/03/18	● 配合部分資料的上傳狀態混亂調整，設計「同步上傳狀態」功能 ● 其他操作與上傳 bug 調整	349,078
v.1.1.9	2024/04/30	● 編輯區塊提供不同的字體大小選項 ● 原鳥類清單中的鳥種移至物種下拉選單選項中，並移除原鳥類清單功能 ● 於上傳程式資料夾中提供 csv 範例檔供匯入功能參考使用 ● 其他操作與上傳 bug 調整	984,674
v.1.1.11	2024/07/22	● 上傳時提供哪幾筆資料尚未填寫「物種」欄位資訊的提醒文字 ● 更新教學說明內容 ● 其他操作與上傳功能優化及 bug 調整	391,609
v.1.1.12	2024/08/30	● 更新「同步上傳狀態」功能 ● 其他操作與上傳功能優化及 bug 調整	145,654

v.1.1.13	2024/09/27	● 更新物種下拉選單選項 a. 新增「灰鶯/褐鶯」、「山鷸鴴」、「灰頭黑臉鵐」、「臺灣/酒紅朱雀」4 種鳥類 b. 「山羊」更改為「野山羊」 c. 「柳鶯類」改為「柳鶯類(無法辨識)」 ● 上傳程式資料夾中新增物種清單檔案（檔案名稱 import-example-species.csv），使用文字資料與對應影像匯入功能時請統一物種寫法 ● 上傳通知調整為僅有上傳者會收到自己上傳資料完成與否的通知信件 ● 其他操作與上傳功能優化及 bug 調整	488,553

表 2、上傳程式介面中可供選擇之物種

通用物種	鳥類
工作照,測試,空拍,無法辨識,水鹿,山羌,獼猴,野山羊,野豬,鼬獾,白鼻心,食蟹獴,鳥類(無法辨識),鼠或鮑形目,赤腹松鼠,條紋松鼠,長吻松鼠,松鼠-無法辨識種類,飛鼠-無法辨識種類,大赤鼯鼠,白面鼯鼠,小鼯鼠,黃喉貂,黃鼠狼,小黃鼠狼,麝香貓,黑熊,石虎,穿山甲,狗,貓,梅花鹿,野兔,蝙蝠,人,獵人,其他	臺灣山鷓鴣(深山竹雞),黑長尾雉(帝雉),藍腹鷴,臺灣竹雞(竹雞),野鴿,灰林鴿,金背鳩,紅鳩,珠頸斑鳩,翠翼鳩,白腹秧雞(白胸秧雞),灰腳秧雞,山鷸,白鷺類(無法辨識),大/中白鷺,小白鷺,岩鷺,黃頭鷺,池鷺,夜鷺,黑冠麻鷺,大冠鷲,松雀鷹,鳳頭蒼鷹,黃嘴角鴞/領角鴞,蘭嶼角鴞,東方灰林鴞(灰林鴞),赤翡翠(紅翡翠),五色鳥,小啄木,大赤啄木,綠啄木,八色鳥,黑枕藍鶲,紅尾伯勞,棕背伯勞,松鴉,臺灣藍鵲,樹鵲,星鴉,巨嘴鴉(烏鴉、大嘴烏鴉),方尾鶲,青背山雀,臺灣鷦眉(鱗胸鷦鶯),白環鸚嘴鵯,烏頭翁,白頭翁,紅嘴黑鵯,棕耳鵯,柳鶯類(無法辨識),棕面鶯,紅頭山雀,斯氏/日菲繡眼(綠繡眼),低地繡眼,山紅頭,小彎嘴,大彎嘴,頭烏線,繡眼畫眉,臺灣噪眉(金翼白眉),白耳畫眉,紋翼畫眉,黃胸藪眉(黃痣藪眉、藪鳥),大陸畫眉(中國畫眉),臺灣畫眉,黑喉噪眉(黑喉笑鶇),臺灣白喉噪眉(白喉笑鶇),棕噪眉(竹鳥),鶇科(無法辨識),白氏/虎斑地鶇,白頭鶇,灰背鶇,白眉鶇,赤腹鶇,白腹鶇,斑點鶇,白腰鵲鴴,黃腹琉璃(黃腹仙鶲),白腹琉璃(白腹藍鶲、白腹姬鶲),小翼鶇,琉球歌鴝,臺灣紫嘯鶇(紫嘯鶇),白尾鴝,臺灣白眉林鴝(臺灣林鴝),栗背林鴝,黃胸青鶲,白腰文鳥,麻雀,山鶯鴝,灰鷺/褐鷺,灰頭黑臉鵐,臺灣/酒紅朱雀

表 3、四場教育訓練各分署參與總人次

單位名稱	參與總人次
林業保育署	7
南投分署	1
臺東分署	13
嘉義分署	7
屏東分署	14
新竹分署	10
臺中分署	15
宜蘭分署	17
花蓮分署	12
其他非林業保育署轄下單位	15

附錄 1、資安檢測報告

ZAP Scanning Report

Site: https://camera-trap.tw

Generated on Tue, 29 Oct 2024 09:42:45

ZAP Version: 2.14.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	8
Informational	8
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	2
CSP: Wildcard Directive	Medium	11
Sub Resource Integrity Attribute Missing	Medium	18
Cookie No HttpOnly Flag	Low	4
Cookie Without Secure Flag	Low	4
Cross-Domain JavaScript Source File Inclusion	Low	16
Permissions Policy Header Not Set	Low	11
Private IP Disclosure	Low	1
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	11
Strict-Transport-Security Header Not Set	Low	11
X-Content-Type-Options Header Missing	Low	12
Authentication Request Identified	Informational	1
Information Disclosure - Suspicious Comments	Informational	14
Modern Web Application	Informational	8
Non-Storable Content	Informational	1
Re-examine Cache-control Directives	Informational	10
Session Management Response Identified	Informational	3
Storable and Cacheable Content	Informational	10
User Controllable HTML Element Attribute (Potential XSS)	Informational	11

Alert Detail

Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://camera-trap.tw/search/
Method	GET
Parameter	
Attack	
Evidence	<form id="filter-form">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "altitude" "end_date" "keyword" "start_date"].
URL	https://camera-trap.tw/search/?altitude=ZAP&altitudeOperator=eq&end_date=ZAP&keyword=ZAP&start_date=2014-01-01
Method	GET
Parameter	
Attack	
Evidence	<form id="filter-form">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "altitude" "end_date" "keyword" "start_date"].

Instances	2
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium **CSP: Wildcard Directive**

Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://camera-trap.tw
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	font-src 'self' https://*.fontawesome.com https://fonts.googleapis.com https://fonts.gstatic.com; default-src 'self' https://www.google.com/recpatcha/ https://www.google.com/; style-src 'self' https://cdn.datatables.net https://*.fontawesome.com https://*.highcharts.com https://unpkg.com/ https://fonts.googleapis.com http://www.w3.org https://cdnjs.cloudflare.com; script-src 'self' https://cdnjs.cloudflare.com https://fonts.googleapis.com https://code.jquery.com https://cdn.datatables.net https://*.highcharts.com https://*.fontawesome.com https://unpkg.com/ data: http://www.w3.org https://www.google.com https://www.gstatic.com; media-src 'self' https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/; img-src 'self' https://*.highcharts.com https://*.fontawesome.com data: http://www.w3.org https://*.tile.osm.org/ https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/annotation-images/; connect-src 'self' https://*.fontawesome.com
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://camera-trap.tw/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	font-src 'self' https://*.fontawesome.com https://fonts.googleapis.com https://fonts.gstatic.com; default-src 'self' https://www.google.com/recpatcha/ https://www.google.com/; style-src 'self' https://cdn.datatables.net https://*.fontawesome.com https://*.highcharts.com https://unpkg.com/ https://fonts.googleapis.com http://www.w3.org https://cdnjs.cloudflare.com; script-src 'self' https://cdnjs.cloudflare.com https://fonts.googleapis.com https://code.jquery.com https://cdn.datatables.net https://*.highcharts.com https://*.fontawesome.com https://unpkg.com/ data: http://www.w3.org https://www.google.com https://www.gstatic.com; media-src 'self' https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/; img-src 'self' https://*.highcharts.com https://*.fontawesome.com data: http://www.w3.org https://*.tile.osm.org/ https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/annotation-images/; connect-src 'self' https://*.fontawesome.com
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://camera-trap.tw/admin/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	font-src 'self' https://*.fontawesome.com https://fonts.googleapis.com https://fonts.gstatic.com; default-src 'self' https://www.google.com/recpatcha/ https://www.google.com/; style-src 'self' https://cdn.datatables.net https://*.fontawesome.com https://*.highcharts.com https://unpkg.com/ https://fonts.googleapis.com http://www.w3.org https://cdnjs.cloudflare.com; script-src 'self' https://cdnjs.cloudflare.com https://fonts.googleapis.com https://code.jquery.com https://cdn.datatables.net https://*.highcharts.com https://*.fontawesome.com https://unpkg.com/ data: http://www.w3.org https://www.google.com https://www.gstatic.com; media-src 'self' https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/; img-src 'self' https://*.highcharts.com https://*.fontawesome.com data: http://www.w3.org https://*.tile.osm.org/ https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/annotation-images/; connect-src 'self' https://*.fontawesome.com
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://camera-trap.tw/admin/login/?next=/admin/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	font-src 'self' https://*.fontawesome.com https://fonts.googleapis.com https://fonts.gstatic.com; default-src 'self' https://www.google.com/recpatcha/ https://www.google.com/; style-src 'self' https://cdn.datatables.net https://*.fontawesome.com https://*.highcharts.com https://unpkg.com/ https://fonts.googleapis.com http://www.w3.org https://cdnjs.cloudflare.com; script-src 'self' https://cdnjs.cloudflare.com https://fonts.googleapis.com https://code.jquery.com https://cdn.datatables.net https://*.highcharts.com https://*.fontawesome.com https://unpkg.com/ data: http://www.w3.org https://www.google.com https://www.gstatic.com; media-src 'self' https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/; img-src 'self' https://*.highcharts.com https://*.fontawesome.com data: http://www.w3.org https://*.tile.osm.org/ https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/annotation-images/; connect-src 'self' https://*.fontawesome.com
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL	https://camera-trap.tw/contact-us
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	font-src 'self' https://*.fontawesome.com https://fonts.googleapis.com https://fonts.gstatic.com; default-src 'self' https://www.google.com/recpatcha/ https://www.google.com/; style-src 'self' https://cdn.datatables.net https://*.fontawesome.com https://*.highcharts.com https://unpkg.com/ https://fonts.googleapis.com http://www.w3.org https://cdnjs.cloudflare.com; script-src 'self' https://cdnjs.cloudflare.com https://fonts.googleapis.com https://code.jquery.com https://cdn.datatables.net https://*.highcharts.com https://*.fontawesome.com https://unpkg.com/ data: http://www.w3.org https://www.google.com https://www.gstatic.com; media-src 'self' https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/; img-src 'self' https://*.highcharts.com https://*.fontawesome.com data: http://www.w3.org https://*.tile.osm.org/ https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/annotation-images/; connect-src 'self' https://*.fontawesome.com
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://camera-trap.tw/faq
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	font-src 'self' https://*.fontawesome.com https://fonts.googleapis.com https://fonts.gstatic.com; default-src 'self' https://www.google.com/recpatcha/ https://www.google.com/; style-src 'self' https://cdn.datatables.net https://*.fontawesome.com https://*.highcharts.com https://unpkg.com/ https://fonts.googleapis.com http://www.w3.org https://cdnjs.cloudflare.com; script-src 'self' https://cdnjs.cloudflare.com https://fonts.googleapis.com https://code.jquery.com https://cdn.datatables.net https://*.highcharts.com https://*.fontawesome.com https://unpkg.com/ data: http://www.w3.org https://www.google.com https://www.gstatic.com; media-src 'self' https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/; img-src 'self' https://*.highcharts.com https://*.fontawesome.com data: http://www.w3.org https://*.tile.osm.org/ https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/annotation-images/; connect-src 'self' https://*.fontawesome.com
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://camera-trap.tw/policy
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	font-src 'self' https://*.fontawesome.com https://fonts.googleapis.com https://fonts.gstatic.com; default-src 'self' https://www.google.com/recpatcha/ https://www.google.com/; style-src 'self' https://cdn.datatables.net https://*.fontawesome.com https://*.highcharts.com https://unpkg.com/ https://fonts.googleapis.com http://www.w3.org https://cdnjs.cloudflare.com; script-src 'self' https://cdnjs.cloudflare.com https://fonts.googleapis.com https://code.jquery.com https://cdn.datatables.net https://*.highcharts.com https://*.fontawesome.com https://unpkg.com/ data: http://www.w3.org https://www.google.com https://www.gstatic.com; media-src 'self' https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/; img-src 'self' https://*.highcharts.com https://*.fontawesome.com data: http://www.w3.org https://*.tile.osm.org/ https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/annotation-images/; connect-src 'self' https://*.fontawesome.com
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://camera-trap.tw/project/overview
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	font-src 'self' https://*.fontawesome.com https://fonts.googleapis.com https://fonts.gstatic.com; default-src 'self' https://www.google.com/recpatcha/ https://www.google.com/; style-src 'self' https://cdn.datatables.net https://*.fontawesome.com https://*.highcharts.com https://unpkg.com/ https://fonts.googleapis.com http://www.w3.org https://cdnjs.cloudflare.com; script-src 'self' https://cdnjs.cloudflare.com https://fonts.googleapis.com https://code.jquery.com https://cdn.datatables.net https://*.highcharts.com https://*.fontawesome.com https://unpkg.com/ data: http://www.w3.org https://www.google.com https://www.gstatic.com; media-src 'self' https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/; img-src 'self' https://*.highcharts.com https://*.fontawesome.com data: http://www.w3.org https://*.tile.osm.org/ https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/annotation-images/; connect-src 'self' https://*.fontawesome.com
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://camera-trap.tw/search/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	font-src 'self' https://*.fontawesome.com https://fonts.googleapis.com https://fonts.gstatic.com; default-src 'self' https://www.google.com/recpatcha/ https://www.google.com/; style-src 'self' https://cdn.datatables.net https://*.fontawesome.com https://*.highcharts.com https://unpkg.com/ https://fonts.googleapis.com http://www.w3.org https://cdnjs.cloudflare.com; script-src 'self' https://cdnjs.cloudflare.com https://fonts.googleapis.com https://code.jquery.com https://cdn.datatables.net https://*.highcharts.com https://*.fontawesome.com https://unpkg.com/ data: http://www.w3.org https://www.google.com https://www.gstatic.com; media-src 'self' https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/; img-src 'self' https://*.highcharts.com https://*.fontawesome.com data: http://www.w3.org https://*.tile.osm.org/ https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/annotation-images/; connect-src 'self' https://*.fontawesome.com
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://camera-trap.tw/search/?altitude=ZAP&altitudeOperator=eq&end_date=ZAP&keyword=ZAP&start_date=2014-01-01
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	font-src 'self' https://*.fontawesome.com https://fonts.googleapis.com https://fonts.gstatic.com; default-src 'self' https://www.google.com/recpatcha/ https://www.google.com/; style-src 'self' https://cdn.datatables.net https://*.fontawesome.com https://*.highcharts.com https://unpkg.com/ https://fonts.googleapis.com http://www.w3.org https://cdnjs.cloudflare.com; script-src 'self' https://cdnjs.cloudflare.com https://fonts.googleapis.com https://code.jquery.com https://cdn.datatables.net https://*.highcharts.com https://*.fontawesome.com https://unpkg.com/ data: http://www.w3.org https://www.google.com https://www.gstatic.com; media-src 'self' https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/; img-src 'self' https://*.highcharts.com https://*.fontawesome.com data: http://www.w3.org https://*.tile.osm.org/ https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/annotation-images/; connect-src 'self' https://*.fontawesome.com
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://camera-trap.tw/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	font-src 'self' https://*.fontawesome.com https://fonts.googleapis.com https://fonts.gstatic.com; default-src 'self' https://www.google.com/recpatcha/ https://www.google.com/; style-src 'self' https://cdn.datatables.net https://*.fontawesome.com https://*.highcharts.com https://unpkg.com/ https://fonts.googleapis.com http://www.w3.org https://cdnjs.cloudflare.com; script-src 'self' https://cdnjs.cloudflare.com https://fonts.googleapis.com https://code.jquery.com https://cdn.datatables.net https://*.highcharts.com https://*.fontawesome.com https://unpkg.com/ data: http://www.w3.org https://www.google.com https://www.gstatic.com; media-src 'self' https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/; img-src 'self' https://*.highcharts.com https://*.fontawesome.com data: http://www.w3.org https://*.tile.osm.org/ https://*.s3.ap-northeast-1.amazonaws.com/ https://d3gg2vsgjlos1e.cloudfront.net/annotation-images/; connect-src 'self' https://*.fontawesome.com

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
Instances	11
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium **Sub Resource Integrity Attribute Missing**

Description	The integrity attribute is missing on a script or link tag served by an external server. The integrity tag prevents an attacker who have gained access to this server from injecting a malicious content.
URL	https://camera-trap.tw
Method	GET
Parameter	
Attack	
Evidence	<link href="https://cdn.datatables.net/1.13.1/css/jquery.dataTables.min.css" />
Other Info	
URL	https://camera-trap.tw
Method	GET
Parameter	
Attack	
Evidence	<script src="https://code.highcharts.com/highcharts.js"></script>
Other Info	
URL	https://camera-trap.tw
Method	GET
Parameter	
Attack	
Evidence	<script src="https://code.highcharts.com/modules/accessibility.js"></script>
Other Info	
URL	https://camera-trap.tw
Method	GET
Parameter	
Attack	
Evidence	<script src="https://code.highcharts.com/modules/export-data.js"></script>
Other Info	
URL	https://camera-trap.tw
Method	GET
Parameter	
Attack	
Evidence	<script src="https://code.highcharts.com/modules/exporting.js"></script>
Other Info	
URL	https://camera-trap.tw
Method	GET
Parameter	
Attack	
Evidence	<script src="https://code.highcharts.com/modules/series-label.js"></script>
Other Info	
URL	https://camera-trap.tw
Method	GET
Parameter	
Attack	
Evidence	<script src="https://code.jquery.com/jquery-3.6.1.js"></script>
Other Info	
URL	https://camera-trap.tw
Method	GET
Parameter	
Attack	
Evidence	<script type="text/javascript" src="https://cdn.datatables.net/1.13.1/js/dataTables.bootstrap5.min.js"></script>
Other Info	
URL	https://camera-trap.tw
Method	GET
Parameter	
Attack	
Evidence	<script type="text/javascript" src="https://cdn.datatables.net/1.13.1/js/jquery.dataTables.min.js"></script>
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	

Attack	
Evidence	<link href="https://cdn.datatables.net/1.13.1/css/jquery.dataTables.min.css" />
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	
Attack	
Evidence	<script src="https://code.highcharts.com/highcharts.js"></script>
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	
Attack	
Evidence	<script src="https://code.highcharts.com/modules/accessibility.js"></script>
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	
Attack	
Evidence	<script src="https://code.highcharts.com/modules/export-data.js"></script>
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	
Attack	
Evidence	<script src="https://code.highcharts.com/modules/exporting.js"></script>
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	
Attack	
Evidence	<script src="https://code.highcharts.com/modules/series-label.js"></script>
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	
Attack	
Evidence	<script src="https://code.jquery.com/jquery-3.6.1.js"></script>
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	
Attack	
Evidence	<script type="text/javascript" src="https://cdn.datatables.net/1.13.1/js/dataTables.bootstrap5.min.js"></script>
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	
Attack	
Evidence	<script type="text/javascript" src="https://cdn.datatables.net/1.13.1/js/jquery.dataTables.min.js"></script>
Other Info	
Instances	18
Solution	Provide a valid integrity attribute to the tag.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity
CWE Id	345
WASC Id	15
Plugin Id	90003

Low	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	https://camera-trap.tw/admin/login/?next=/admin/
Method	GET
Parameter	csrftoken
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://camera-trap.tw/contact-us
Method	GET
Parameter	csrftoken
Attack	

Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://camera-trap.tw/project/overview
Method	GET
Parameter	csrftoken
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://camera-trap.tw/admin/login/?next=/admin/
Method	POST
Parameter	csrftoken
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
Instances	4
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Low	**Cookie Without Secure Flag**
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://camera-trap.tw/admin/login/?next=/admin/
Method	GET
Parameter	csrftoken
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://camera-trap.tw/contact-us
Method	GET
Parameter	csrftoken
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://camera-trap.tw/project/overview
Method	GET
Parameter	csrftoken
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://camera-trap.tw/admin/login/?next=/admin/
Method	POST
Parameter	csrftoken
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
Instances	4
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html
CWE Id	614
WASC Id	13
Plugin Id	10011

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://camera-trap.tw
Method	GET
Parameter	https://cdn.datatables.net/1.13.1/js/dataTables.bootstrap5.min.js
Attack	
Evidence	<script type="text/javascript" src="https://cdn.datatables.net/1.13.1/js/dataTables.bootstrap5.min.js"></script>
Other Info	
URL	https://camera-trap.tw
Method	GET
Parameter	https://cdn.datatables.net/1.13.1/js/jquery.dataTables.min.js
Attack	
Evidence	<script type="text/javascript" src="https://cdn.datatables.net/1.13.1/js/jquery.dataTables.min.js"></script>
Other Info	
URL	https://camera-trap.tw
Method	GET

Parameter	https://code.highcharts.com/highcharts.js
Attack	
Evidence	<script src="https://code.highcharts.com/highcharts.js"></script>
Other Info	
URL	https://camera-trap.tw
Method	GET
Parameter	https://code.highcharts.com/modules/accessibility.js
Attack	
Evidence	<script src="https://code.highcharts.com/modules/accessibility.js"></script>
Other Info	
URL	https://camera-trap.tw
Method	GET
Parameter	https://code.highcharts.com/modules/export-data.js
Attack	
Evidence	<script src="https://code.highcharts.com/modules/export-data.js"></script>
Other Info	
URL	https://camera-trap.tw
Method	GET
Parameter	https://code.highcharts.com/modules/exporting.js
Attack	
Evidence	<script src="https://code.highcharts.com/modules/exporting.js"></script>
Other Info	
URL	https://camera-trap.tw
Method	GET
Parameter	https://code.highcharts.com/modules/series-label.js
Attack	
Evidence	<script src="https://code.highcharts.com/modules/series-label.js"></script>
Other Info	
URL	https://camera-trap.tw
Method	GET
Parameter	https://code.jquery.com/jquery-3.6.1.js
Attack	
Evidence	<script src="https://code.jquery.com/jquery-3.6.1.js"></script>
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	https://cdn.datatables.net/1.13.1/js/dataTables.bootstrap5.min.js
Attack	
Evidence	<script type="text/javascript" src="https://cdn.datatables.net/1.13.1/js/dataTables.bootstrap5.min.js"></script>
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	https://cdn.datatables.net/1.13.1/js/jquery.dataTables.min.js
Attack	
Evidence	<script type="text/javascript" src="https://cdn.datatables.net/1.13.1/js/jquery.dataTables.min.js"></script>
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	https://code.highcharts.com/highcharts.js
Attack	
Evidence	<script src="https://code.highcharts.com/highcharts.js"></script>
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	https://code.highcharts.com/modules/accessibility.js
Attack	
Evidence	<script src="https://code.highcharts.com/modules/accessibility.js"></script>
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	https://code.highcharts.com/modules/export-data.js
Attack	
Evidence	<script src="https://code.highcharts.com/modules/export-data.js"></script>
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	https://code.highcharts.com/modules/exporting.js
Attack	
Evidence	<script src="https://code.highcharts.com/modules/exporting.js"></script>

Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	https://code.highcharts.com/modules/series-label.js
Attack	
Evidence	<script src="https://code.highcharts.com/modules/series-label.js"></script>
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	https://code.jquery.com/jquery-3.6.1.js
Attack	
Evidence	<script src="https://code.jquery.com/jquery-3.6.1.js"></script>
Other Info	
Instances	16
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

Low **Permissions Policy Header Not Set**

Description	Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Permissions Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
URL	https://camera-trap.tw
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/contact-us
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/faq
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/policy
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/project/overview
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/search/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/sitemap.xml
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://camera-trap.tw/static/fontawesome-free-6.2.1/js/fontawesome.min.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/static/js/bootstrap.bundle.min.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/static/js/home.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	11
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy https://developer.chrome.com/blog/feature-policy/ https://scotthelme.co.uk/a-new-security-header-feature-policy/ https://w3c.github.io/webappsec-feature-policy/ https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	693
WASC Id	15
Plugin Id	10063

Low	**Private IP Disclosure**
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	https://camera-trap.tw/static/fontawesome-free-6.2.1/js/brands.min.js
Method	GET
Parameter	
Attack	
Evidence	10.1.9.34
Other Info	10.1.9.34 10.8.1.1 10.8.1.1
Instances	1
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP/PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Reference	https://tools.ietf.org/html/rfc1918
CWE Id	200
WASC Id	13
Plugin Id	2

Low	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	https://camera-trap.tw
Method	GET
Parameter	
Attack	
Evidence	nginx/1.25.3
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.25.3
Other Info	
URL	https://camera-trap.tw/admin/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.25.3
Other Info	
URL	https://camera-trap.tw/contact-us
Method	GET
Parameter	
Attack	
Evidence	nginx/1.25.3

Other Info	
URL	https://camera-trap.tw/faq
Method	GET
Parameter	
Attack	
Evidence	nginx/1.25.3
Other Info	
URL	https://camera-trap.tw/policy
Method	GET
Parameter	
Attack	
Evidence	nginx/1.25.3
Other Info	
URL	https://camera-trap.tw/project/overview
Method	GET
Parameter	
Attack	
Evidence	nginx/1.25.3
Other Info	
URL	https://camera-trap.tw/robots.txt
Method	GET
Parameter	
Attack	
Evidence	nginx/1.25.3
Other Info	
URL	https://camera-trap.tw/search/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.25.3
Other Info	
URL	https://camera-trap.tw/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	nginx/1.25.3
Other Info	
URL	https://camera-trap.tw/static/icon/logo%40leaf.png
Method	GET
Parameter	
Attack	
Evidence	nginx/1.25.3
Other Info	
Instances	11
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	200
WASC Id	13
Plugin Id	10036
Low	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://camera-trap.tw
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/contact-us
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://camera-trap.tw/faq
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/policy
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/project/overview
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/search/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/static/css/dataTables.bootstrap5.min.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/static/icon/logo%40leaf.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	11
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035
Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://camera-trap.tw/static/css/base.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://camera-trap.tw/static/css/dataTables.bootstrap5.min.css

Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://camera-trap.tw/static/css/home.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://camera-trap.tw/static/css/project_overview.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://camera-trap.tw/static/css/theme.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://camera-trap.tw/static/fontawesome-free-6.2.1/css/brands.min.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://camera-trap.tw/static/fontawesome-free-6.2.1/css/solid.min.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://camera-trap.tw/static/fontawesome-free-6.2.1/css/v5-font-face.min.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://camera-trap.tw/static/fontawesome-free-6.2.1/js/fontawesome.min.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://camera-trap.tw/static/icon/logo%40leaf.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://camera-trap.tw/static/jquery-ui-1.13.2/jquery-ui.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://camera-trap.tw/static/js/home.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	12
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational — **Authentication Request Identified**

Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	https://camera-trap.tw/admin/login/?next=/admin/
Method	POST
Parameter	username
Attack	
Evidence	password
Other Info	userParam=username userValue=ZAP passwordParam=password referer=https://camera-trap.tw/admin/login/?next=/admin/ csrfToken=csrfmiddlewaretoken
Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational — **Information Disclosure - Suspicious Comments**

Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	https://camera-trap.tw/static/fontawesome-free-6.2.1/js/fontawesome.min.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "!function(){"use strict";function n(a,t){var e,n=Object.keys(a);return Object.getOwnPropertySymbols&&(e=Object.getOwnPropertySym", see evidence field for the suspicious comment/snippet.
URL	https://camera-trap.tw/static/jquery-ui-1.13.2/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 7 times, the first in the element starting with: " // it causes a very odd bug in IE 8 (see #6720)", see evidence field for the suspicious comment/snippet.
URL	https://camera-trap.tw/static/jquery-ui-1.13.2/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected 6 times, the first in the element starting with: " // see: http://jsfiddle.net/JZSMt/3/ https://bugs.webkit.org/show_bug.cgi?id=107380", see evidence field for the suspicious comment/snippet.
URL	https://camera-trap.tw/static/jquery-ui-1.13.2/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 121 times, the first in the element starting with: " // Track widgets that inherit from this widget in case this widget is", see evidence field for the suspicious comment/snippet.
URL	https://camera-trap.tw/static/jquery-ui-1.13.2/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 7 times, the first in the element starting with: " // redefine the widget later", see evidence field for the suspicious comment/snippet.
URL	https://camera-trap.tw/static/jquery-ui-1.13.2/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	Select
Other Info	The following pattern was used: \bSELECT\b and was detected 39 times, the first in the element starting with: " // Select the wrapper - make it overflow: hidden and absolute positioned based on", see evidence field for the suspicious comment/snippet.
URL	https://camera-trap.tw/static/jquery-ui-1.13.2/jquery-ui.js
Method	GET

Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 24 times, the first in the element starting with: " // TODO: remove support for widgetEventPrefix", see evidence field for the suspicious comment/snippet.
URL	https://camera-trap.tw/static/jquery-ui-1.13.2/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 8 times, the first in the element starting with: "//>>description: Lists suggested words as the user is typing.", see evidence field for the suspicious comment/snippet.
URL	https://camera-trap.tw/static/jquery-ui-1.13.2/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 10 times, the first in the element starting with: " // this is the only case where we allow nulls for ALL properties.", see evidence field for the suspicious comment/snippet.
URL	https://camera-trap.tw/static/js/bootstrap.bundle.min.js
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():"function"==typeof define&&define.amd?def", see evidence field for the suspicious comment/snippet.
URL	https://camera-trap.tw/static/js/home.js
Method	GET
Parameter	
Attack	
Evidence	Select
Other Info	The following pattern was used: \bSELECT\b and was detected 3 times, the first in the element starting with: " // Select the top 10 species", see evidence field for the suspicious comment/snippet.
URL	https://camera-trap.tw/contact-us
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "<!-- Examples from desinger -->", see evidence field for the suspicious comment/snippet.
URL	https://camera-trap.tw/project/overview
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<!-- 起始年份 <div class="input-item", see evidence field for the suspicious comment/snippet.
URL	https://camera-trap.tw/search/
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<!-- <select name="box_1_studyareas" id="filter-project1-studyareas" multiple="multiple"> </s", see evidence field for the suspicious comment/snippet.
Instances	14
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10027

Informational **Modern Web Application**

Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://camera-trap.tw
Method	GET
Parameter	
Attack	
Evidence	 登入
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://camera-trap.tw/
Method	GET
Parameter	
Attack	

Evidence	 登入
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://camera-trap.tw/contact-us
Method	GET
Parameter	
Attack	
Evidence	 登入
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://camera-trap.tw/faq
Method	GET
Parameter	
Attack	
Evidence	 登入
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://camera-trap.tw/policy
Method	GET
Parameter	
Attack	
Evidence	 登入
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://camera-trap.tw/project/overview
Method	GET
Parameter	
Attack	
Evidence	 登入
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://camera-trap.tw/search/
Method	GET
Parameter	
Attack	
Evidence	 登入
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://camera-trap.tw/search/?altitude=ZAP&altitudeOperator=eq&end_date=ZAP&keyword=ZAP&start_date=2014-01-01
Method	GET
Parameter	
Attack	
Evidence	 登入
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
Instances	8
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational **Non-Storable Content**

Description	The response contents are not storable by caching components such as proxy servers. If the response does not contain sensitive, personal or user-specific information, it may benefit from being stored and cached, to improve performance.
URL	https://camera-trap.tw/admin/
Method	GET
Parameter	
Attack	
Evidence	no-store
Other Info	
Instances	1
Solution	The content may be marked as storable by ensuring that the following conditions are satisfied: The request method must be understood by the cache and defined as being cacheable ("GET", "HEAD", and "POST" are currently defined as cacheable) The response status code must be understood by the cache (one of the 1XX, 2XX, 3XX, 4XX, or 5XX response classes are generally understood) The "no-store" cache directive must not appear in the request or response header fields For caching by "shared" caches such as "proxy" caches, the "private" response directive must not appear in the response For caching by "shared" caches such as "proxy" caches, the "Authorization" header field must not appear in the request, unless the response explicitly allows it (using one of the "must-revalidate", "public", or "s-maxage" Cache-Control response directives) In addition to the conditions above, at least one of the following conditions must also be satisfied by the response: It must contain an "Expires" header field It must contain a "max-age" response directive For "shared" caches such as "proxy" caches, it must contain a "s-maxage" response directive It must contain a "Cache Control Extension" that allows it to be cached It must have a status code that is defined as cacheable by default (200, 203, 204, 206, 300, 301, 404, 405, 410, 414, 501).

Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524
WASC Id	13
Plugin Id	10049

Informational **Re-examine Cache-control Directives**

Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://camera-trap.tw
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/contact-us
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/faq
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/policy
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/project/overview
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/robots.txt
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/search/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/search/?altitude=ZAP&altitudeOperator=eq&end_date=ZAP&keyword=ZAP&start_date=2014-01-01
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://camera-trap.tw/feedback_request
Method	POST
Parameter	cache-control
Attack	
Evidence	
Other Info	
Instances	10

Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational — **Session Management Response Identified**

Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	https://camera-trap.tw/contact-us
Method	GET
Parameter	csrftoken
Attack	
Evidence	yn3YWgTUe8TWHkXtWfgFqPHHCjfOjd6n
Other Info	cookie:csrftoken
URL	https://camera-trap.tw/project/overview
Method	GET
Parameter	csrftoken
Attack	
Evidence	yn3YWgTUe8TWHkXtWfgFqPHHCjfOjd6n
Other Info	cookie:csrftoken
URL	https://camera-trap.tw/admin/login/?next=/admin/
Method	POST
Parameter	csrftoken
Attack	
Evidence	yn3YWgTUe8TWHkXtWfgFqPHHCjfOjd6n
Other Info	cookie:csrftoken
Instances	3
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112

Informational — **Storable and Cacheable Content**

Description	The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where "shared" caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://camera-trap.tw
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://camera-trap.tw/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://camera-trap.tw/contact-us
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://camera-trap.tw/faq
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://camera-trap.tw/policy
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.

URL	https://camera-trap.tw/project/overview
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://camera-trap.tw/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://camera-trap.tw/search/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://camera-trap.tw/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://camera-trap.tw/static/icon/logo%40leaf.png
Method	GET
Parameter	
Attack	
Evidence	max-age=604800
Other Info	
Instances	10
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524
WASC Id	13
Plugin Id	10049
Informational	User Controllable HTML Element Attribute (Potential XSS)
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	https://camera-trap.tw/admin/login/?next=/admin/
Method	GET
Parameter	next
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://camera-trap.tw/admin/login/?next=/admin/ appears to include user input in: a(n) [a] tag [href] attribute The user input found was: next=/admin/ The user-controlled value was: /admin/
URL	https://camera-trap.tw/admin/login/?next=/admin/
Method	GET
Parameter	next
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://camera-trap.tw/admin/login/?next=/admin/ appears to include user input in: a(n) [form] tag [action] attribute The user input found was: next=/admin/ The user-controlled value was: /admin/login/?next=/admin/
URL	https://camera-trap.tw/admin/login/?next=/admin/
Method	GET
Parameter	next
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://camera-trap.tw/admin/login/?next=/admin/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: next=/admin/ The user-controlled value was: /admin/
URL	https://camera-trap.tw/search/?altitude=ZAP&altitudeOperator=eq&end_date=ZAP&keyword=ZAP&start_date=2014-01-01
Method	GET

Parameter	altitudeOperator
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://camera-trap.tw/search/?altitude=ZAP&altitudeOperator=eq&end_date=ZAP&keyword=ZAP&start_date=2014-01-01 appears to include user input in: a(n) [option] tag [value] attribute The user input found was: altitudeOperator=eq The user-controlled value was: eq
URL	https://camera-trap.tw/search/?altitude=ZAP&altitudeOperator=eq&end_date=ZAP&keyword=ZAP&start_date=2014-01-01
Method	GET
Parameter	start_date
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://camera-trap.tw/search/?altitude=ZAP&altitudeOperator=eq&end_date=ZAP&keyword=ZAP&start_date=2014-01-01 appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: start_date=2014-01-01 The user-controlled value was: 2014-01-01
URL	https://camera-trap.tw/search/?altitude=ZAP&altitudeOperator=eq&end_date=ZAP&keyword=ZAP&start_date=2014-01-01
Method	GET
Parameter	start_date
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://camera-trap.tw/search/?altitude=ZAP&altitudeOperator=eq&end_date=ZAP&keyword=ZAP&start_date=2014-01-01 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: start_date=2014-01-01 The user-controlled value was: 2014-01-01
URL	https://camera-trap.tw/admin/login/?next=/admin/
Method	POST
Parameter	next
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://camera-trap.tw/admin/login/?next=/admin/ appears to include user input in: a(n) [a] tag [href] attribute The user input found was: next=/admin/ The user-controlled value was: /admin/
URL	https://camera-trap.tw/admin/login/?next=/admin/
Method	POST
Parameter	next
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://camera-trap.tw/admin/login/?next=/admin/ appears to include user input in: a(n) [form] tag [action] attribute The user input found was: next=/admin/ The user-controlled value was: /admin/login/?next=/admin/
URL	https://camera-trap.tw/admin/login/?next=/admin/
Method	POST
Parameter	next
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://camera-trap.tw/admin/login/?next=/admin/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: next=/admin/ The user-controlled value was: /admin/
URL	https://camera-trap.tw/admin/login/?next=/admin/
Method	POST
Parameter	password
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://camera-trap.tw/admin/login/?next=/admin/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: password=ZAP The user-controlled value was: zap
URL	https://camera-trap.tw/admin/login/?next=/admin/
Method	POST
Parameter	username
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://camera-trap.tw/admin/login/?next=/admin/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: username=ZAP The user-controlled value was: zap
Instances	11
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	10031

附錄 2、自 2023 年度期末報告撰寫完畢後至本期末報告撰寫完畢前所蒐集之意見回饋內容表單

回饋形式	回饋日期	上傳程式/線上系統	問題描述	TaiBIF 團隊修改評估
信箱回饋	20231207	上傳程式/線上系統	想取消"[臺灣自動相機資訊系統]上傳通知"此類的信件	已說明
信箱回饋	20231214	上傳程式	下載 1.6 版本會被防毒軟體偵測導致執行程式不見	已說明
信箱回饋	20231217	線上系統	請將我加入 [林務局哺乳動物監測網] 計畫成員	已說明
信箱回饋	20231218	上傳程式	檢視計畫沒有台東分署成功工作站	已說明
電話回饋	20231218	上傳程式	執行程式被防毒軟體檔直接被刪掉	已調整
信箱回饋	20231219	上傳程式	CSV 檔案上傳問題	已調整
電話回饋	20231219	上傳程式	匯入功能沒有反應，也沒有錯誤訊息	已解決
信箱回饋	20231225	上傳程式	因前幾天署內的防毒軟體將程式刪除好幾次,今日重新打開程式,結果之前判識完成的資料夾無法進行上傳,出現 TypeError: '>=' not supported between instances of 'NoneType' and 'int'	已調整
信箱回饋	20240102	上傳程式	上傳程式登入 ORCID 帳號提示視窗，上面有提示要「登入 ORCID」，但會以為是文字提示而不知道要點選該按鈕後才會出現驗證碼。 建議「登入 ORCID」按鈕可修改為「請按此處並登入 ORCID」	已調整
信箱回饋	20240102	上傳程式	系統的「檢視計畫」下拉沒有選項(如圖)	已說明
信箱回饋	20240110	上傳程式	林業保育署南投分署丹大工作站同仁，在更新使用 1.1.6 版本上傳程式軟體後，資料夾內之「檢視計畫」無「林務局哺乳動物監測網」可以選擇	已跟小古確認

信箱回饋	20240206	上傳程式	目前同仁下載 v1.1.6 版本，檢視計畫那欄無計畫可選以致新版上傳作業無法完成	待確認
信箱回饋	20240217	上傳程式	因發生有 3 張影像未成功上傳 能協助上傳並修改上傳結果狀態嗎	已調整
信箱回饋	20240217	上傳程式	新改版 1.1.7 會被防毒軟體擋下	待確認
信箱回饋	20240219	上傳程式	有部分資料夾中的照片未上傳成功或重複上傳	已調整
信箱回饋	20240307	上傳程式	想請問我昨天上傳 DS-LTMM-016-20240205-20240304 相片，用軟體上傳到一半就關掉了，今天要再上傳，但我按成更新文字資料，軟體顯示覆寫完成，沒辦法再上傳影像，請問要怎麼重新上傳? 上傳進度顯示上傳完畢，但有上傳成功的照片是 0 張，點進照片編輯的畫面，只有更新文字資料的按鈕，沒有上傳的按鈕。點進網頁看上傳紀錄，顯示影像未上傳成功。	已調整
信箱回饋	20240416	上傳程式/線上系統	下表是林業保育署宜蘭分署太平山工作站 上傳資料異常部分說明 詢問是否可協助註記	已說明
信箱回饋	20240416	上傳程式	上傳還是有問題	已調整
信箱回饋	20240418	線上系統	已申請 ORCID 帳號登入系統， 但尚未被加入計畫，需要貴單位的協助，以加入計畫進行上傳作業。 另外關於最新版本的程式，在網站上點擊更新公告後，即顯示權限不足的訊息，想請問該如何下載上傳程式軟體 v1.1.8 版?	已說明並跟小古確認
信箱回饋	20240423	線上系統	要進入線上系統下載自動相機監測上傳程式 v1.1.8 時，上面寫權限不足	已說明
電話回饋	20240423	上傳程式	不會操作新版的上傳程式，舊版的上傳程式也無法使用	已提供寄圖文操作手冊
信箱回饋	20240424	上傳程式/線上系統	近期有工作站巡視員反應， 該巡視員以自己的 Orcid 帳號登入後，下載的上傳軟體無法使用(會顯示	已說明

			權限不足，無法順利上傳照片)。 但是如果是職員(技士 OOO)以自己的 Orcid 帳號登入後下載的軟體，傳給該巡視員使用後，反而可以在該巡視員的電腦上正常使用。 因為工作站常常是巡視員須獨立作業，請協助排除此類差異。	
電話回饋	20240424	上傳程式	用自己 orcid 登入後看不到計畫	已說明
電話回饋	20240425	線上系統	分署承辦看不到計畫管理	已解決
信箱回饋	20240502	其他	一直無法註冊 orcid 帳號，所以無法設定相機記憶卡的資料上傳。無法辨識機關單位	已說明
信箱回饋	20240502	線上系統	如何下載相機上傳程式	已說明
電話回饋	20240502	上傳程式	臺東分署反應他們分署與工作站下載最新版單機程式，防毒軟體都還是會阻擋	已說明
信箱回饋	20240505	上傳程式	上傳錯誤，找不到刪除鍵	已說明
電話回饋	20240509	上傳程式	最新版上傳程式沒有上傳的鍵可以選	小古已寄信回覆
電話回饋	20240514	上傳程式	最新版上傳程式沒有上傳的鍵可以選(另外一個同事要上傳時，發生問題，問題同上)	已解決
信箱回饋	20240522	上傳程式	檢視計畫欄位無資料可選擇； 樣區欄位無資料可選擇	已說明
信箱回饋	20240523		目前看不到全站相機上傳情況，請協助處理	待確認
信箱回饋	20240523	線上系統	我無法更新 1.9，說權限不足	已說明
信箱回饋	20240524	上傳程式	台東分屬利嘉林道 TD106-03 相機之「20230101-20230214」檔案夾，最後一張水鹿圖檔拍攝呈像不全，導致 App 上傳資料夾時無法上傳、整個資料夾 Error。 由於嘗試數次整個資料夾無法上傳 App，故我也無法讀取全部圖檔，目前處置方式為刪除整個上傳的資料夾，先行跳過本資料夾。另外，我在想是否先將該圖檔移出資料夾，其他圖檔就可以完整上傳，等完整上傳後	待確認

			我再將該圖檔移回資料夾。 附檔為同時段的水鹿圖檔「RCNX1763~RCNX1773」，有問題圖檔為「RCNX1773」。	
電話回饋	20240524	上傳程式	利嘉林道 TD106-03 相機 20230101-20230214 的最後一張可能因為相機系統問題，拍的照片是不完整的，我在上傳資料夾就卡在那一張無法完成上傳資料夾	已回信
信箱回饋	20240526	上傳程式/線上系統	台東分屬在利嘉林道的 TD106-03 相機總共有五個資料夾，我透過 App 將其全部檢視完畢並上傳，App 顯示全部五個資料夾皆上傳完成了，但網頁的「上傳紀錄」只有四個資料夾，少一筆資料夾「TD106-03-20230416-20230609」	已調整
信箱回饋	20240528	上傳程式	上傳進度這裡沒辦法往下拉，看不到下面的資料夾，有資料夾上傳到一半，要按重啟上傳沒辦法按	已說明
信箱回饋	20240603	上傳程式	使用快捷鍵撰打物種名稱後，選擇框會跳到頁面的最左上角那欄位，變成要再用滑鼠手動拉回接續的欄位，對於只用鍵盤快速撰打的同仁較為不便，而前幾個版本無此問題	已調整
信箱回饋	20240603	線上系統	忘記帳號和密碼	待確認
信箱回饋	20240604	上傳程式	已建立帳號 ORCID 帳號，並加入計畫(林務局哺乳動物監測網)，下載上傳程式(v1.1.9)。新增資料夾後欲進行相片編輯，但"檢視計畫"、"樣區"和"相機位置" 無法選擇(點下去後沒東西可點選)	已說明
信箱回饋	20240604	上傳程式/線上系統	上傳資料同步有問題	已調整
電話回饋	20240605	上傳程式	上傳程式打開後出現警告，無法匯入以及上傳影像	已說明
電話回饋	20240605	上傳程式	1. 上傳程式看不到計畫、樣區、相機位置 2. 匯入資料夾失敗後卡住	已說明

電話回饋	20240605	上傳程式	想知道如果已經匯入資料到筆電，可以在另外一台桌電上編輯這些已匯入的資料嗎？	已說明
電話回饋	20240606	線上系統	確認相機樣點運作及缺失比例的頁面資訊邏輯	已說明
信箱回饋	20240606	上傳程式	介面無法放至最大，且文字完全重疊,看不到自己輸入的物種,造成使用上嚴重的困擾	已調整
信箱回饋	20240611	上傳程式	登入之後看不到我的現有資料夾我上週陸續上傳完成好幾個月的照片 上傳後再編輯 但還沒編輯完成我現在完全看不到可編輯的資料夾	待確認
信箱回饋	20240613	上傳程式	程式軟體更新(V1.1.9 版) 執行程式後檢視計畫和樣區和相機位置無法下拉式選單	已說明
電話回饋	20240617	上傳程式	資料夾中有照片沒有上傳完成，網頁也顯示錯誤，但按了上傳程式中的同步狀態之後還是錯誤	已說明
電話回饋	20240621	線上系統	相機壞掉，目前相機位址的照片還沒收回來，不能填缺失問題回報	已說明
信箱回饋	20240625	上傳程式/線上系統	上傳後系統網頁上顯示影像未成功上傳	已調整
信箱回饋	20240710	上傳程式	請問上傳資料除了照片以外，可以上傳影片嗎？	已說明
信箱回饋	20240710	上傳程式	1.最近常常明明已經上傳成功了但是網路系統出現未完成 2.上傳後出現綠色已完成,但是網路系統出現未完成 3.檔案可以刪除重傳嗎	待確認
信箱回饋	20240716	上傳程式	我是林業署台中分署雙崎工作站新任紅外線相機相片判釋人員，煩請新增我的帳號進入全台哺乳類監測計畫，感謝	已說明
信箱回饋	20240719	上傳程式	下載新版的上傳系統，但檢視計畫那邊沒有林業署哺乳動物監測網可以選	已說明
信箱回饋	20240722	上傳程式	在操作程式時會使用方向鍵操作圖片上下，然後會用快捷鍵輸入物種名稱 但在輸入物種後接著使用方	已說明

			向鍵往下，並不會接著往下張圖片而是跳到第一張圖片。應該是選取框在輸入完物種後，選取框會失去目標，因此如果再按下方向鍵就會跳回該頁第一張照片，所以建議在輸入完物種後自動往下一格跳	
信箱回饋	20240722	上傳程式	1.複製一列後再輸入物種，物種無法成功帶入進複製後的照片(會是空白)，因此會要在手動輸入複製照片的物種名稱。 2.若選取該頁第一張照片時，希望按上鍵能跳至該頁最後一張照片	第 1 點已說明 第 2 點待評估
信箱回饋	20240723	上傳程式	保育相機上傳成功時，其他非本人的信箱會收到上傳成功的信，非常干擾。(ex: A 相機照片上傳後，因該是管理 A 相機的甲收到上傳成功的信，而不是甲乙丙丁都收到) 若該項無法快速改善，乾脆直接不要信箱收到信件僅主管信箱能收到。	已調整
信箱回饋	20240723	上傳程式	v1.1.11 版本目前仍然會被防毒軟體封鎖，再麻煩協助解鎖	已調整
電話回饋	20240726	上傳程式	新版 1.1.11 的 key in 很慢	已說明
信箱回饋	20240726	上傳程式	最新版本的系統在批次填寫辨識物種後，按下一格時會跳回最坐上格（之前系統不會），無法用上下鍵逐一填寫物種，需用滑鼠點選，易出現漏填情形	已說明
信箱回饋	20240726	線上系統	在資料篩選與計算，篩選條件確定後，按右下角的「下載搜尋結果」，EMAIL 收到的 CSV 檔案，打開會是亂碼，請問可以怎麼處理	已調整
信箱回饋	20240801	上傳程式	同仁反映在上傳紀錄有一筆未完成，點選檢視錯誤後，顯示物種未填寫完整(同仁說他當時有填) 請問可以如何重新補填資料	已說明
信箱回饋	20240803	上傳程式/線上系統	LTMM-53 明明都 2369/2369 上傳完，但還是未完成	待確認

電話回饋	20240805	上傳程式	1. 不會取消連拍補齊 2. 一張照片有兩隻同樣的物種，要怎麼填寫	已說明
信箱回饋	20240813	上傳程式/線上系統	目前無法瀏覽資料，再麻煩幫忙開承辦權限	已說明
信箱回饋	20240905	上傳程式	再次建議，請不要將上傳成功通知信件群發給所有計畫同仁，可以將信件發至給該上傳人或僅群發給保育主辦	已調整
信箱回饋	20240906	上傳程式/線上系統	上傳還是有問題，已有試過很多次同步上傳狀態功能	已調整
信箱回饋	20240912	上傳程式/線上系統	林業保育署南投分署同仁帳號未被加入至林業署哺乳動物監測網，想麻煩協助設定	已說明
信箱回饋	20241001	線上系統	本人原任職林業及自然保育署宜蘭分署南澳工作站，由於本人業於今年 9 月初退休，相關業務已由其他同事辦理，爰相關業務訊息請勿再續傳此信箱	已說明
信箱回饋	20241024	上傳程式	可不可以將別人帳號內已辨識的資料直接移至另一人的帳號內 面臨此問題是因遇到業務交接的情況，方便未來管理資料。如可轉移 版本不同是否有影響	確認中

附錄 3、系統程式說明及資料標準內容

目前狀態

正式站: https://camera-trap.tw
正式站上傳計畫: 林務局哺乳動物監測網, id: 329

測試站: https://staging.camera-trap.tw/

開發

Source Code

- https://github.com/TaiBIF/camera-trap-tk/ 上傳程式
- https://github.com/TaiBIF/camera-trap-server/ 線上系統

Branch

- main - 目前廢用
- prod - 正式站
- dbtest - 測試站

測試

上傳程式

Release 前檢查

設定檔 (config.ini)

- Installation
  - `account_id=xxx`
- Server
  - `host = https://camera-trap.tw`
  - `project_option_list = 329::test` # default project ID
  - `ssl_verify = 0` # 0 for 林務局內部網路
- AWSConfig

- `bucket_name = camera-trap-21`
  - 測試站: camera-trap-21-dev
  - 正式站: camera-trap-21
- `mediaconvert_role` = arn:aws:iam::536600044933:role/MediaConvertRole-prod
  - 測試站: `arn:aws:iam::536600044933:role/MediaConvertRole-dev`
  - 正式站: `arn:aws:iam::536600044933:role/MediaConvertRole-prod`
- `mediaconvert_queue = camera-trap-prod_queue`
  - 測試站: `camera-trap-dbtest_queue`
  - 正式站: `camera-trap-prod_queue`
- `mediaconvert_job_template = camera-trap-prod_job_template`
  - 測試站: `camera-trap-dbtest_job_template`
  - 正式站: `camera-trap-prod_job_template`

Desktop App

- version 顯示正不正確
- 打包 zip 目錄正不正確 (小心弄錯資料夾)

單元測試

每個功能各自測試

主要參考: test-case.rst

測試匯入

正常情況

1. 加入資料夾方式:
    a. 按 "加入資料夾"
        i. 選擇資料夾, 可測試有以下狀況的資料夾
            1. 有影片
            2. 有錯誤影像
            3. 完全沒有影像
            4. 資料夾命名錯誤
            5. 資料夾命名與已上傳資料夾重複
        ii. 進入 "現有資料夾" 頁
        iii. 進度條每秒更新
        iv. 正在匯入時按"資料夾卡片"應該要不能進入編輯畫面(除非匯入錯誤)
        v. 正在匯入時關閉應用程式 (按視窗的 "X"), 會跳出"尚有資料夾正在匯入中..." 的錯誤訊息(對話框)
    b. 點選工具列匯入文字檔與影像
2. 完成後跳出 "匯入資料夾完成" 的訊息 (對話框)
3. 可以進入資料夾編輯畫面

測試錯誤處理 **(error handling)**

模擬匯入失敗 (匯一半當機...)

1. edit config.ini, set [Mode] force_quit = 1
2. 按 "加入資料夾"
3. 選擇資料夾
4. 進入 "現有資料夾" 頁
5. 進度條每秒更新
6. 離開程式
7. 重新開啟程式
8. 可以進入匯入錯誤的資料夾, 執行"刪除資料夾"

整合測試

App + Server 操作一起測試

測試項目:

- 上傳照片
  - 上傳時不可點擊進入資料夾內編輯
- 上傳影片
  - 影片副檔名 mp4
  - 影片副檔名 mov
- 上傳有 “複製” 的照片
- 上傳大量資料照片 (9999 張)
- 上傳後寄出 email 通知
- 上傳後有上傳記錄
- 月底會寄出缺失記錄通知

上傳測試站

1. 改config.ini的
   - [Server] host => 改成測試站domain: staging.camera-trap.tw
   - [AWSConfig] bucket_name => 改成camera-trap-21-dev
2. ct.db: sqlite的 state table, 修改 name=user_id, value=測試站上的taicat_contact.id, 如果sqlite3沒有的話表示沒有登入過, 再新增一筆 INSERT INTO state (name, value) VALUES (‘user_id’, ‘測試站上的taicat_contact.id’)

測試檔案

大照片數量 (9999張)
https://drive.proton.me/urls/Z2X68H7F10#eIsVC4V0QB1G

ct-9999-clean.db: 空白的9999張照片資料

測試 "日期時間" 的檔案
https://drive.proton.me/urls/50NAFP0278#B1fL70xXb5CP
1.1.4 以前的版本會抓到錯誤的, 1.1.5 後是正確的 (照片有浮水印對照)

匯入文字檔
https://drive.proton.me/urls/BBTACFKJ1C#zaQ9f3Uje8YX
- import-chaojin.csv 正常匯入
- import-clone.csv 有複製一列的資料
- import-not-controlled.csv 內容不是系統控制詞彙
- import-err.csv 各種錯誤格式
- import-err-header.csv 標題錯誤 (只檢查: 檔名,日期時間,物種)

特殊照片檔案

- 照片檔案壞掉 (連正常顯示都無法)
- 照片檔案壞掉 (可以開啟但是不能縮圖) (顯示一半灰)
- EXIF 日期格式壞掉
    - EXIF日期格式壞掉搭配其他沒問題的檔案 (測試用其他檔案的日期來填補)

伺服器部署/設定

正式站: https://camera-trap.tw
測試站: https://dbtest.camera-trap.tw/

Django 設定

Increase upload memory size, default is 2.5MB.

Each image annotation cost ~1KB, maximal number of images in a folder is 9999 (Camera SD card limit?), consider all image annotations are duplicated, double it, increase maximal number to: `1000*2*10000`

```
DATA_UPLOAD_MAX_MEMORY_SIZE = 20000000
```

時區

資料庫存 UTC 的 timezone

```
TIME_ZONE=='UTC'
USE_TZ= True
```

ex: image.id=12722790, PostgreSQL 存的 2022-12-11 22:13:22+00, 實際上照片是 06:13:22 AM (照片上的浮水印跟 exif 的時間都是 06:13:22)

Domain

- CSRF_TRUSTED_ORIGINS
- ALLOWED_HOSTS (.env)

Gunicorn 設定

前端 search 頁的 API 加了 verbose (給 download log 使用), 可能導致 query string 太長：出現 Request Line is too large 的錯誤。gunicorn 的預設是 4094
https://docs.gunicorn.org/en/stable/settings.html#limit-request-line

Data 設定

因為上次更新有更新到schema, 要麻煩幫忙修改`Species`這張表裡面的值
重新docker-compose down&up之後, 進到資料庫修改`Species`表, 把下面list裡的物種修改成 `is_default='t'`

```
DEFAULT_LIST = ['水鹿', '山羌', '獼猴', '山羊', '野豬', '鼬獾', '白鼻心', '食蟹獴', '松鼠',
                '飛鼠', '黃喉貂', '黃鼠狼', '小黃鼠狼', '麝香貓', '黑熊', '石虎', '穿山甲', '梅花鹿', '野兔', '蝙蝠']
```

Crontab 設定

```
0 16 * * * docker exec ct22-django-prod-container /code/cronjob.sh >> /tmp/stat.log 2>&1
0 16 * * * find /home/ec2-user/ct22-volumes/media/download/ -name *.xlsx -mtime +365 -delete >> /tmp/aaa.log 2>&1
0 16 * * * find /home/ec2-user/ct22-volumes/media/email-attachment/* -mtime +30 -delete >> /tmp/bbb.log 2>&1
0 0 1 * * docker exec ct22-django-prod-container /code/cronjob-every-month.sh >> /tmp/stat-every-month.log 2>&1
```

Docker Volumes 設定

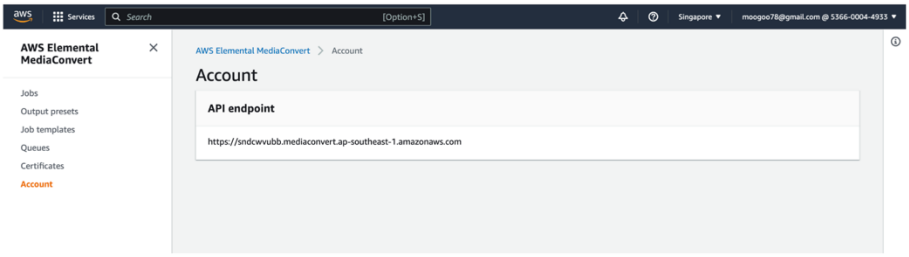
ct22-volumes/media/ 要新增一個download目錄, 否則task.py會找不到

AWS (Amazon Web Services) 設定

Video 轉檔設定

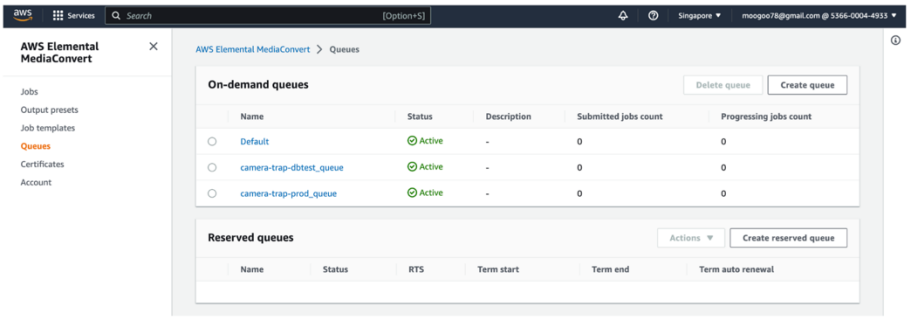
AWSMediaConvert 設定

1. AWS Elemental MediaConvert 側邊選項最下面: Acount 有 API endpoint



2. create Queue

取名字



3. create Job templates

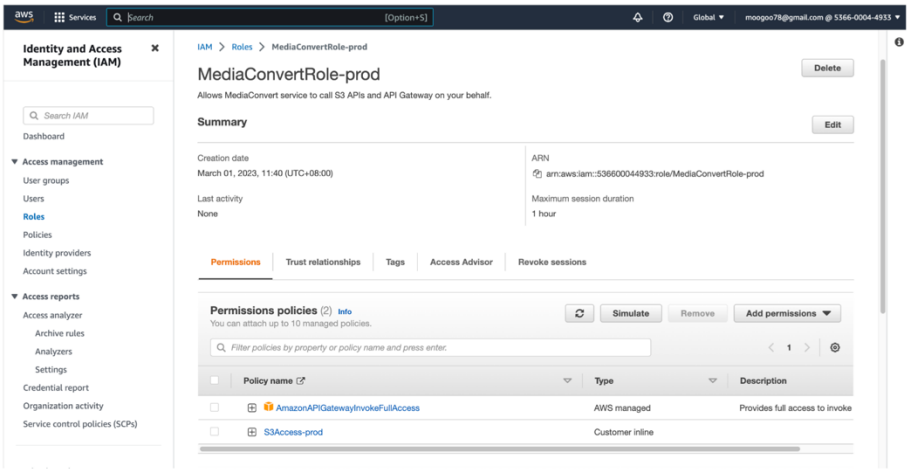
設定 Output groups

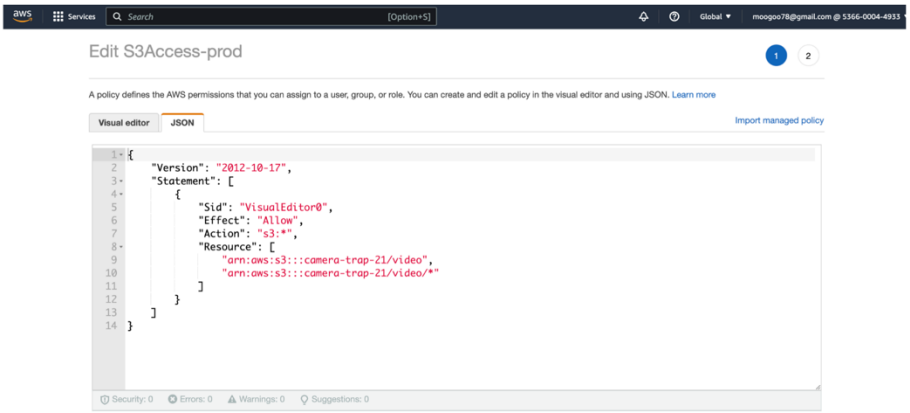
- File Group:
    - H.264 (1280 x 720), AAC
    - Max bitrate(bits/s): 6000000 一定要設定 ⚠️ 可以再研究最佳數值

AWS IAM 設定

1. create Role

增加一個 policy: 可以讀取 S3 bucket

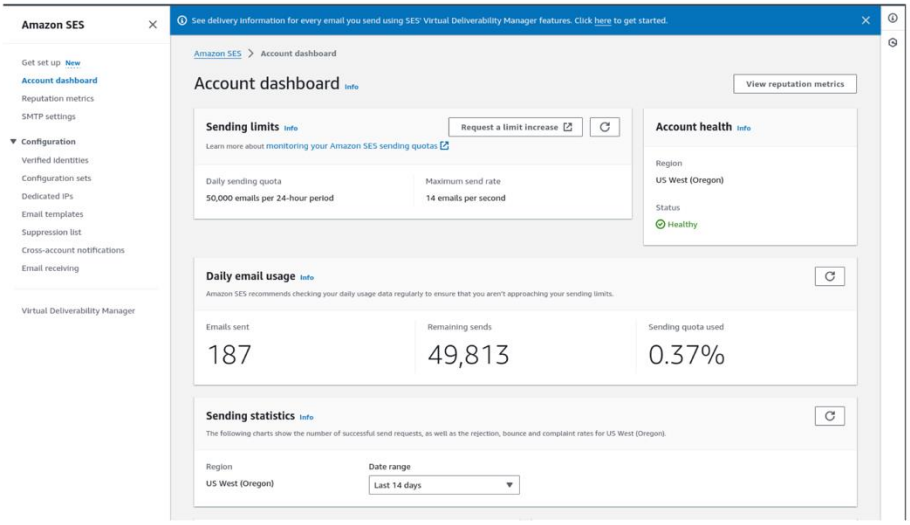




AWS SES (Simple Email Service)

預設 sending limits: 1 秒內14封，如果提高要送request表單說明原因。超過會造成email送不出去。

目前是用的AWS Region是Oregon (us-west-2)



AWS S3

TODO

系統設計

規格

照片縮圖 size (取較長的一邊匹配):

- q: 75
- m: 500
- l: 1024
- x: 2048
- o: 4096

時區

存db: 時間要 -8 hr (UTC timezone)
顯示: 要 db 時間 +8 hr
計算: 目前時間 -8 hr

計算

- 相機有效工作: 用行程來判定，這段時間都算相機正常工作 理想上，相機每天會拍測試照，有測試照的就算當天有工作，但實際上不是每台相機都有設定。
- 活動機率: ex: 五月有三十一天，其中有五天下午兩點到三點被拍攝到，則在下午兩點到三點的活動機率為 5/31
- 有效照片: 同一物種，隔__分鐘以上，第一張算有效照片
- 目擊事件: 在__分鐘內出現的照片都算同一事件
- 例如: 5小時中有7張照片，分別在 0、50、100、150、200、250、300分鐘各一張，如果有效照片設定為60分鐘，目擊事件間隔也是60分鐘 => 4張有效照片（0、100、200、300），1各目擊事件 (每張間隔都在60分鐘內)

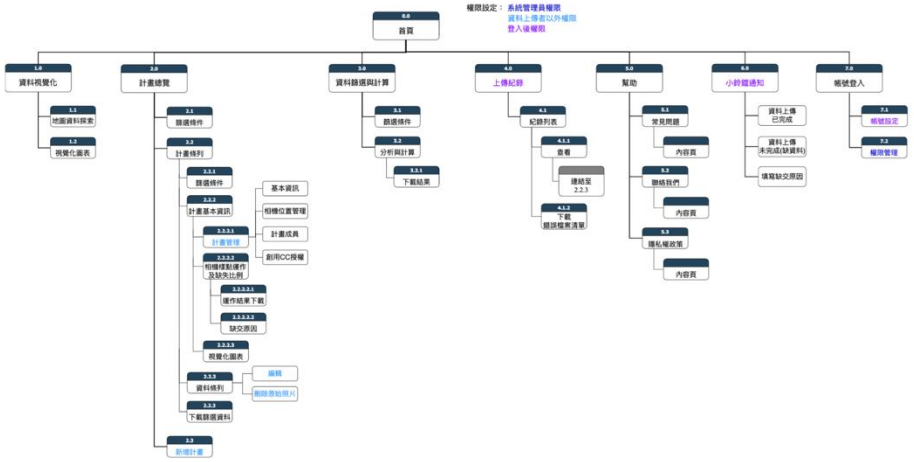
[實作細節]

上傳

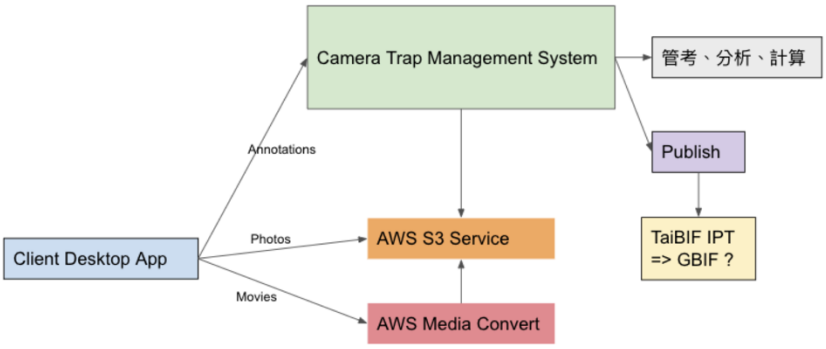
server判斷是否同一批上傳：deployment_id + folder_name + local_source_id

Sitemap

可以看使用者權限表



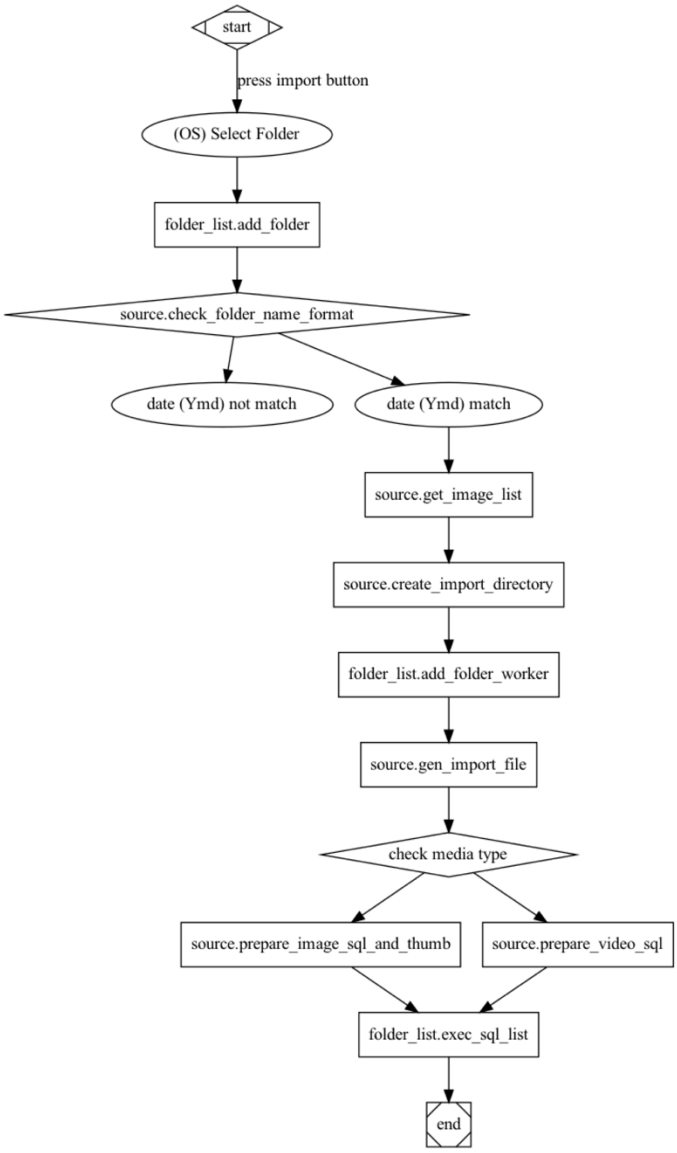
架構圖



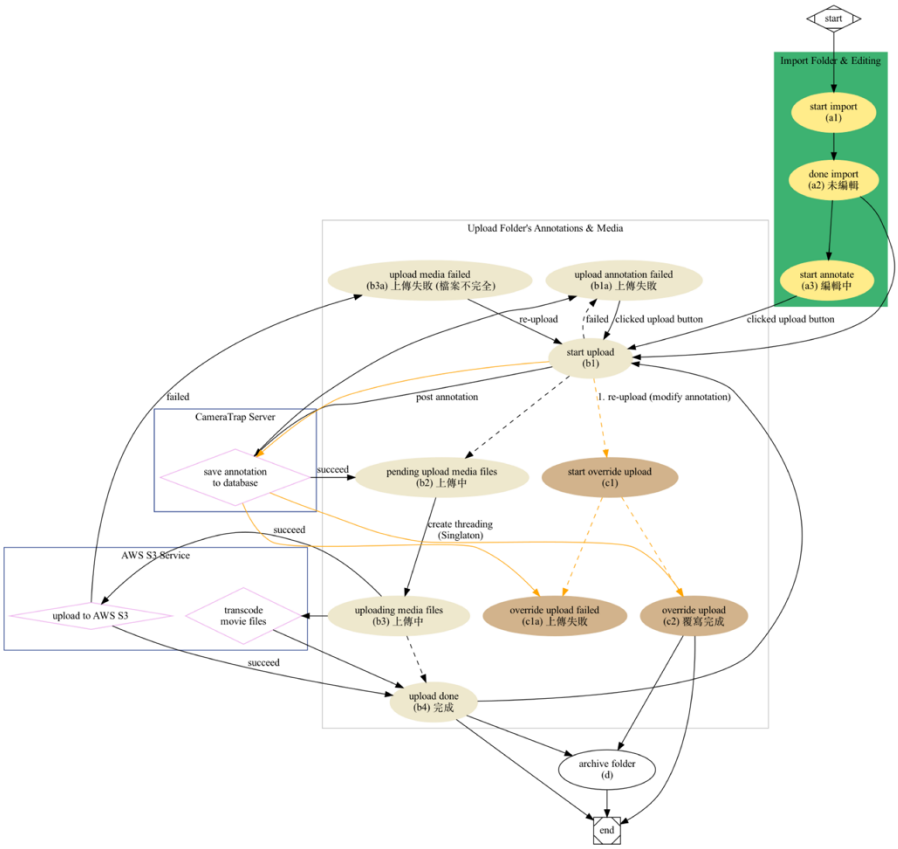
操作流程圖

source: https://github.com/TaiBIF/camera-trap-tk/blob/main/docs/workflow.md (Graphviz Dot 繪圖)

上傳程式:匯入資料夾


start
press import button
(OS) Select Folder
folder_list.add_folder
source.check_folder_name_format
date (Ymd) not match
date (Ymd) match
source.get_image_list
source.create_import_directory
folder_list.add_folder_worker
source.gen_import_file
check media type
source.prepare_image_sql_and_thumb
source.prepare_video_sql
folder_list.exec_sql_list
end

上傳程式：上傳流程



現有資料欄位標準設計

欄位名稱	說明	可填寫內容
檔名	系統自動抓取相關資訊	
日期時間	系統自動抓取相關資訊	
物種	下拉選單	參考本期末報告書之表2、上傳程式介面中可供選擇之物種
年齡	下拉選單	成體/亞成體/幼體/無法判定
性別	下拉選單	雄性/雌性/無法判定
角況	下拉選單	初茸/茸角一尖/茸角一岔二尖/茸角二岔三尖/茸角三岔四尖/硬角一尖/硬角一岔二尖/硬角二岔三尖/硬角三岔四尖/解角

備註	自由欄位	
個體ID	自由欄位	

UI 設計

- 2023 refresh layout Flow 1
- 2022 Figma CAMERA TRAP _OK – Figma (左邊選單有 guideline)
- Prototype (slides) ▸ camera case - CAMERA TRAP

上傳程式 Desktop App

功能

資料夾匯入

- 做完 thumbnails 後，就跟原圖脫鉤，如果 thumbnails 刪掉要再重做嗎? => 重新 import 比較實在
- 拍攝時間取得規則：先以照片的 EXIF 資訊 (DateTimeOriginal)為主，如果檔案沒有 EXIF 資訊，就抓檔案的創建時間 (st_ctime)。

照片編輯

- 設定測試照
- 狀態編輯, 相關 issues (https://trello.com/c/R7RH40lJ)
-

行程輸入

連拍補齊

標註為測試照的資料：「只有在連拍補齊時不被調整」，其他手動調整動作仍能進行

看大圖

Local Database

SQLite3

Schema

參考: https://github.com/TaiBIF/camera-trap-tk/blob/main/src/database.py

source

```
CREATE TABLE IF NOT EXISTS source (
 source_id INTEGER PRIMARY KEY AUTOINCREMENT,
 source_type TEXT,
 path TEXT,
 name TEXT,
 count INTEGER,
 created INTEGER,
 status TEXT,
 description TEXT,
 history TEXT,
 trip_start INTEGER,
 trip_end INTEGER,
 test_foto_time TEXT,
 deployment_journal_id INTEGER,
 upload_created INTEGER,
 upload_changed INTEGER
);
```

image

```
CREATE TABLE IF NOT EXISTS image (
 image_id INTEGER PRIMARY KEY AUTOINCREMENT,
 path TEXT,
 name TEXT,
 timestamp INTEGER,
 timestamp_via TEXT,
 status TEXT,
 hash TEXT,
 annotation TEXT,
 changed INTEGER,
 exif TEXT,
 source_id INTEGER,
 server_image_id TEXT,
 upload_status TEXT,
 sys_note TEXT,
 object_id TEXT,
 media_type TEXT,
 FOREIGN KEY (source_id) REFERENCES source(source_id)
);
```

Image Status Code

```
STATUS_START_IMPORT = 'a1'
STATUS_DONE_IMPORT = 'a2'                # 未編輯
STATUS_START_ANNOTATE = 'a3'             # 編輯中
STATUS_START_UPLOAD = 'b1'
```

```
STATUS_ANNOTATION_UPLOAD_FAILED = 'b1a'  # 上傳失敗
STATUS_MEDIA_UPLOAD_PENDING = 'b2'       # 上傳中
STATUS_MEDIA_UPLOADING = 'b2a'           # 上傳中
STATUS_MEDIA_UPLOAD_FAILED = 'b2b'       # 上傳失敗 (上傳不完全)
STATUS_DONE_UPLOAD = 'b2c'               # 完成
STATUS_START_OVERRIDE_UPLOAD = 'b3'      # 上傳覆寫
STATUS_OVERRIDE_ANNOTATION_UPLOAD_FAILED = 'b3a'  # 上傳失敗
STATUS_DONE_OVERRIDE_UPLOAD = 'b3b'      # 覆寫完成
STATUS_ARCHIVE = 'c'                     # 歸檔
```

Image Upload Status Code

- imported: 10
- start upload: 100
- annotation uploaded: 110
- media uploaded: 200

線上系統功能

公告

- OrcID 管理權限登入後，到網頁 https://camera-trap.tw/announcement
  可以在網頁上寄送公告email
- 網頁上那條黃黃bar的公告是寫死在HTML裡，要手動去修改
- 上傳程式app新版檢查：要去django admin (https://camera-trap.tw/admin) 後台的announcement新增一筆資料，主要是版本號要填最新，例如: v1.1.7 上傳程式app開啟會呼叫API: /api/client/v1/check_update/1.1.7/ ，server檢查**base_announcement** (django model) 找出最新的版本號，回傳結果，讓上傳程式app判斷開啟的app是不是最新公告的版本。

搜尋頁 (/search)

- 計畫|樣區|相機位置的篩選都是 OR

計畫管理 (/project/edit/basic/<project_id>)

相機位置管理/project/edit/deployment/<project_id>

刪除相機位置 API: GET /delete_dep_sa?type=dep&id=<deployment_id>

Crontab

每天:

- cronjob.sh: cron_scripts/update_stats.py

        - HompPageStat
        - ProjectStat
        - Species
        - ProjectSpecies
        - ImageFolder
        - GeoStat
        - StudyAreaStat (center of studyarea)
    - media/download: 刪除超過1年的 xlsx
    - media/email-attachment 刪除超過 30天的檔案

每月:

- cronjob-every-month.sh: cron_scripts/check_data_gap.py

實作: 線上系統 Web App, 伺服器

Software Stack

- Web App: Django, Celery
- Database: PostgreSQL, Redis
- Frontend: Javascript
    - jQuery
    - React (Material UI)

雲端照片網址編碼規則

- file_url 有值的話，檔案位置 (舊照片)
    - 規則: https://d3gg2vsgjlos1e.cloudfront.net/annotation-images/{file_url}
- image_uuid (新照片)
    - 規則:
      https://{bucket_name}.s3.ap-northeast-1.amazonaws.com/{image_uuid}-{size}.jpg
    - specific_bucket 空的
      bucket name 預設為: camera-trap-21-prod
    - specific_bucket 有值，就用這個值
      https://camera-trap-21-dev.s3.ap-northeast-1.amazonaws.com/63acef8771b7fe2017bf13e5-l.jpg
    - size:
        - q: 75
        - m: 500
        - l: 1024
        - x: 2048
        - o: 4096
    - ex: 有一筆紀錄的 image_uuid 是: 63acef8771b7fe2017bf13e5,
      specific_bucket 欄位的值是 camera-trap-21-dev, 照片的路徑就會是:
      https://camera-trap-21-dev.s3.ap-northeast-1.amazonaws.com/63acef8771b7fe2017bf13e5-l.jpg

- 新照片的 bucket_name 可能會有錯亂，所以要試試看: camera-trap-21, camera-trap-21-dev, camera-trap-21-prod

以上為舊資料，供日後修改參考

整合 **s3 bucket** 中的內容

目前有使用的 **s3 bucket** 列表

- **camrea-trap-21-prod:** 整合後的 destination bucket，檔案都在這裡面
- camera-trap-21-dev: 新照片上傳的位置。內容複製到 camera-trap-21-prod
- camera-trap-21: 新照片上傳的位置。內容複製到 camera-trap-21-prod
- camera-trap-api: 舊照片、影片上傳的位置。內容複製到 camera-trap-21-prod 後 annotation-original-images, annotation-original-videos的內容移出資料夾（較好統一 url 的寫法）

複製 bucket 的筆記：
https://angry-cayenne-e62.notion.site/Replicate-aws-s3-buckets-fa4be9c73ecd4f3d9bec4c3487ad7509?pvs=4

新照片、舊照片的差異

- 新照片：儲存不同解析度的照片
- 舊照片：僅儲存原解析度的照片，照片 url 會透過 cloudfront 產生（已經不以這種形式儲存）

新照片 URL 的寫法

https://{bucket_name}.s3.ap-northeast-1.amazonaws.com/{image_uuid}-{size}.jpg

- bucket_name: 照片儲存的 s3 bucket，預設為 **camrea-trap-21-prod**
- image_uuid: 每張照片的uuid
- size: 照片的解析度，預設為 x
    - q: 75
    - m: 500（網頁上縮圖呈現的尺寸）

    - l: 1024
    - x: 2048（下載影像的尺寸）
- 範例：送出 request 就會自動下載 https://camera-trap-21-prod.s3.ap-northeast-1.amazonaws.com/63e0a773ae43e99a4360d662-x.jpg

舊照片 URL 的寫法

`https://{bucket_name}.s3.ap-northeast-1.amazonaws.com/{file_url}.jpg`

- bucket_name: 照片儲存的 s3 bucket，預設為 **camrea-trap-21-prod**
- file_url: 好像是 cloudfront 產生的，還要再確定
- 範例：送出 request 就會自動下載 https://camera-trap-21-prod.s3.ap-northeast-1.amazonaws.com/5d57ae96e7641b9cfa1024f2.jpg

注意！ 舊照片 file_url 中的 uuid 和資料庫存的 image_uuid 不同

舊影片 URL 的寫法

`https://{bucket_name}.s3.ap-northeast-1.amazonaws.com/{file_url}.mp4`

- bucket_name: 影片儲存的 s3 bucket，預設為 **camrea-trap-21-prod**
- file_url: 好像是 cloudfront 產生的，還要再確定
- 範例：送出 request 就會自動下載 https://camera-trap-21-prod.s3.ap-northeast-1.amazonaws.com/5d319d63afe6c05f00896778.mp4

修改資料夾名稱

修改有 folder_name 欄位的資料表，一般來說共有 3 張資料表要改，image, imageFolder, deploymentJournal。如果有刪過照片的計畫，deletedImage 也要改。

修改物種名稱

上傳界面程式: 修改config.ini
網頁:

- cron_scripts/update_stat.py #175 species_list
- static/js/project_detail.js #948 species
- taicat/models.py #77 DEFAULT_LIST
- taicat/views.py #73 species_list
- HACK-SP

SQL:
update taicat_projectspecies set name = '野山羊' where name = '山羊';
update taicat_image set species = '野山羊' where project_id in (329,288,287) and species = '山羊';
update taicat_calculation set species = '野山羊' where species = '山羊';
UPDATE "taicat_species" SET name = '野山羊' WHERE name = '山羊';

update taicat_projectspecies set name = '柳鶯類(無法辨識)' where name = '柳鶯類';
update taicat_image set species = '柳鶯類(無法辨識)' where project_id in(329,288,287) and species = '柳鶯類';
update taicat_calculation set species = '柳鶯類(無法辨識)' where species = '柳鶯類';
UPDATE "taicat_species" SET name = '柳鶯類(無法辨識)' WHERE name = '柳鶯類';

教育訓練

- 使用正式站
- EC2 調整成 2xlarge (16G -> 32G), 30人同時使用有點慢, 但大致上還可以
- 2024-05-31 中研院C101 (wifi: IRBST, BRC_Guest), 學員同時上傳人數:23 (很順)
- 2024-10-08 中研院B208 (wifi: BRC_Guest), 學員15人, 沒有特別調整EC2 (xlarge 16G), 上傳順利, 但同時看網站有點慢

HACK

comment有放 HACK-* 的要記得修
- HACK-SP force更新物種名稱

Snippets

統計 APP 版本上傳數:
SELECT SPLIT_PART(memo, '/', 1) AS version, count(*) FROM taicat_image WHERE project_id = 329 GROUP BY version;

附錄 4、臺灣自動相機資訊系統教育訓練計畫書

（上下半年之計畫書內容相同，僅日期有差異，故此僅呈現上半年之計畫書）

臺灣野生動物自動相機資訊系統 TaiCaT
教育訓練計畫書

一、計畫背景：

過去國內自動相機資料欠缺整合的平台，也欠缺對相關調查計畫、拍攝影像及影片的管理機制，以致於難以整合不同計畫所收取的資料，也無法即時提供分析結果以支援及評估保育決策。隨著近幾年自動相機資料持續且快速地累積，對相關資料與資訊妥善地進行倉儲、管理與整合，便成為影響資料應用價值的重要關鍵。為此，於民國 107 至 108 年，農業部生物多樣性研究所（改制前農委會特生中心）委託中研院 TaiBIF 團隊，建置完成「臺灣自動相機資訊系統」，提供一雲端資料整合及資訊管理平台，支援從自動相機影像檔案的倉儲、影像與計畫資訊的擷取及管理、計畫及資料的篩選與下載，到資料的分析及計畫的管考。

本案經林業保育署於 107、108、110 年度三階段開發以及 111 年度的優化後，分別建置完成了資料庫網站及資料上傳介面，並優化了上傳及編輯的功能，加強資料的視覺化呈現，建立資料完善發布機制，以確保未來系統中的資料能成為生物多樣性開放資料的一部分，讓自動相機資料在鑑定和倉儲外，發揮更大的用處，展現資料管理系統的應用價值。本案系統已於 112 年度正式上線提供各林業保育署分署使用。

二、目的：

本教育訓練目的係為為傳達自動相機資訊系統設計理念及應用，輔助林業保育署及承辦自動相機業務的相關單位，運用資料上傳程式，導入系統操作至日常工作中，進而提升自動相機系統之效用及使用頻率。

三、辦理單位：

（一）主辦單位：農業部林業及自然保育署

（二）承辦單位：

國立屏東科技大學 野生動物保育研究所 翁國精教授團隊

中央研究院 生物多樣性研究中心 TaiBIF 團隊

四、實施對象：各林業分署、工作站等承辦自動相機業務相關人員（含委託研究、調查團隊）。

(請各分署邀請委託計畫之團隊派員參加，以利後續上傳照片)

五、實施日期及地點：(兩場次內容相同，請事先分配參加人員)

（一）113 年 5 月 31 日 (五)10-16 時：中央研究院跨領域大樓

（二）113 年 6 月 14 日 (五)10-16 時：中央研究院跨領域大樓

六、重要須知：

1. 每場次報名人數上限為 40 人，每分署每場次以 5 人為限。合作機關雪霸國家公園管理處每場

次 2 人。

2. 報名連結：https://reurl.cc/yL6nX8
3. 參與人員需自備筆電，電腦作業系統需求：Windows 7 以上。
4. 系統需用 orcid 帳號登入，請先至 orcid.org 註冊。
5. 5/31 場次請於 5/26 日前完成報名，6/14 場次請於 6/9 日前完成報名。

七、聯絡人：

(一)課程詢問:中研院 TaiBIF 團隊 張俊怡 產品經理

email: g11145590@gmail.com / 電話：02-27872220 分機 26

(二)報名詢問:林業及自然保育署保育管理組 王佳琪 視察

Email: m2557@forest.gov.tw / 電話：02-23515441 分機 679

八、活動流程：

讓學員了解相機設置事宜，並學習於自己的電腦端使用資料上傳介面編輯、上傳資料，以及於網頁中查閱資料。

時間	主題	授課目標	授課重點
09:40-10:00	報到		
10:00-10:10	計畫簡介	簡介本案規劃	計畫內容、執行目標與參與團隊
10:10-11:10	相機設置事宜說明	了解相機架設的規則	相機設置基本注意事項與上傳、辨識時常見的錯誤介紹
11:10-11:20	休息		
11:20-11:30	資料流程簡介	了解自動相機資料從上傳到系統上的流程，以及參與的角色	資料流程、系統角色及權限
11:30-12:00	上傳程式檔案安裝	學員安裝完畢上傳程式檔案以供後續課程使用	TaiBIF 團隊提供上傳程式安裝檔，引導學員安裝

12:00-13:00	午餐		
13:00-13:30	上傳程式介面功能說明	了解上傳程式介面現有功能	上傳程式介面現有功能介紹（匯入、檢視、編輯、上傳等）
13:30-14:30	實際操作	資料上傳實作練習	帶領學員運用實際檔案跟著步驟操作
14:30-14:40	休息		
14:40-14:50	上傳資料檢視	於線上系統查看資料是否成功上傳	引導學員至線上系統查看已上傳的資料
14:50-15:40	線上系統功能說明	了解線上系統現有功能	線上系統現有功能介紹（計畫建立、視覺化圖表、篩選與計算等）
15:40-16:00	學員回饋	系統使用意見回饋	疑難排解及提供回饋意見

報名 qr code:

附錄 5、上傳程式引導說明教學文件

資 料 流 程

2

計畫管理
系統網頁
權限設定
相機位置
由計畫總管理人
&
計畫承辦人設定
安裝上傳程式
安裝檔
下載
匯入檔案
上傳程式
開啟檔案
資料編輯
物種辨識
連拍補齊
複製列...
檔案上傳
計畫樣區選擇
上傳狀態提示
上傳進度條
系統登入
系統網頁
角色分流
檢視檔案
系統網頁
確認上傳檔案
3

計畫總管理人：
可管理、編輯及瀏覽所屬單位計畫及瀏覽所有公開計畫

計畫承辦人：
可管理、編輯及瀏覽個別承辦計畫及瀏覽所有公開計畫

資料上傳者：
可瀏覽所有公開計畫及個別所屬計畫，但沒有編輯權限

4

上傳介面檔案安裝

請先至系統網頁登入後下載安裝檔

5

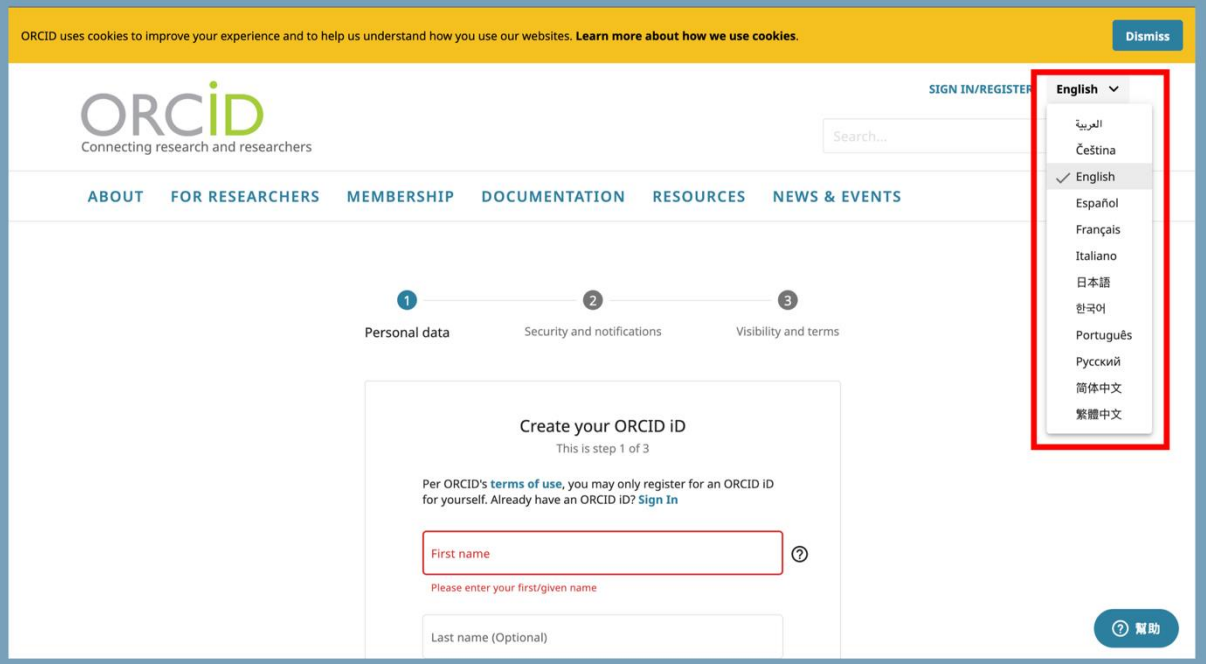
申 請 帳 號

ORCID
Connecting Research and Researchers

https://orcid.org/signin

6

註冊ORCID


ORCID uses cookies to improve your experience and to help us understand how you use our websites. Learn more about how we use cookies.
Dismiss
SIGN IN/REGISTER
English
ORCID
Connecting research and researchers
Search...
ABOUT
FOR RESEARCHERS
MEMBERSHIP
DOCUMENTATION
RESOURCES
NEWS & EVENTS
العربية
Čeština
English
Español
Français
Italiano
日本語
한국어
Português
Русский
简体中文
繁體中文
1 Personal data
2 Security and notifications
3 Visibility and terms
Create your ORCID iD
This is step 1 of 3
Per ORCID's terms of use, you may only register for an ORCID iD for yourself. Already have an ORCID iD? Sign In
First name
Please enter your first/given name
Last name (Optional)
幫助

7

註冊ORCID

創建您的ORCID iD
步驟 5 之 3 - 目前就業狀態
Adding a current employment affiliation helps distinguis
other researchers with a similar name.
目前就業情況
機構
輸入貴組織的名稱
部門 （選擇性）
學校、大專院校或科系
下一步
跳過此步驟，不新增附屬機構
前一步

8

登 入 系 統

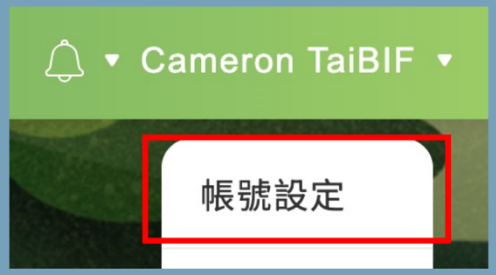
https://camera-trap.tw

9

設 定 資 料

編輯使用者名稱與個人資訊

填寫完整才能被搜尋到與下載資料



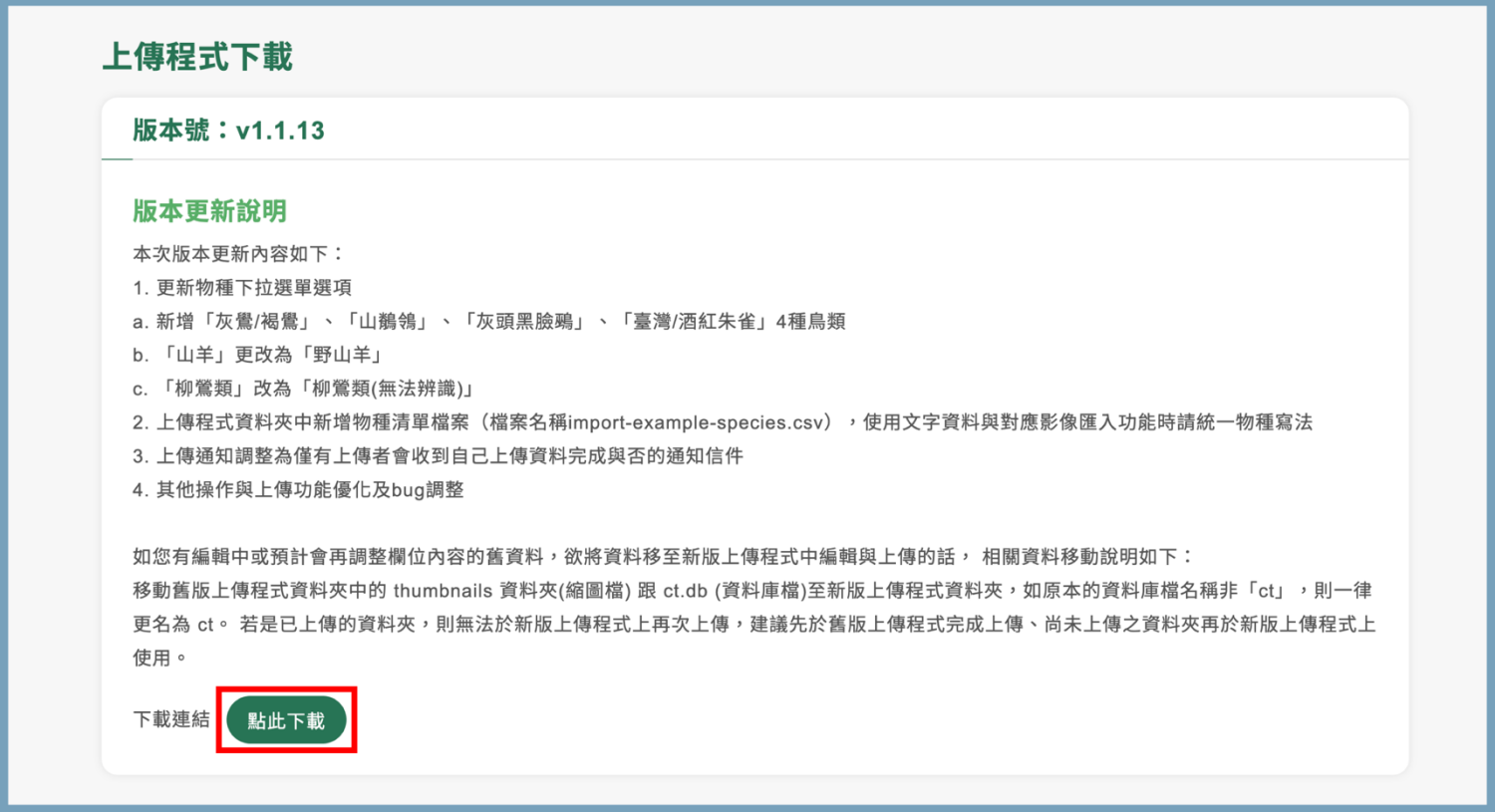
10

安裝檔下載

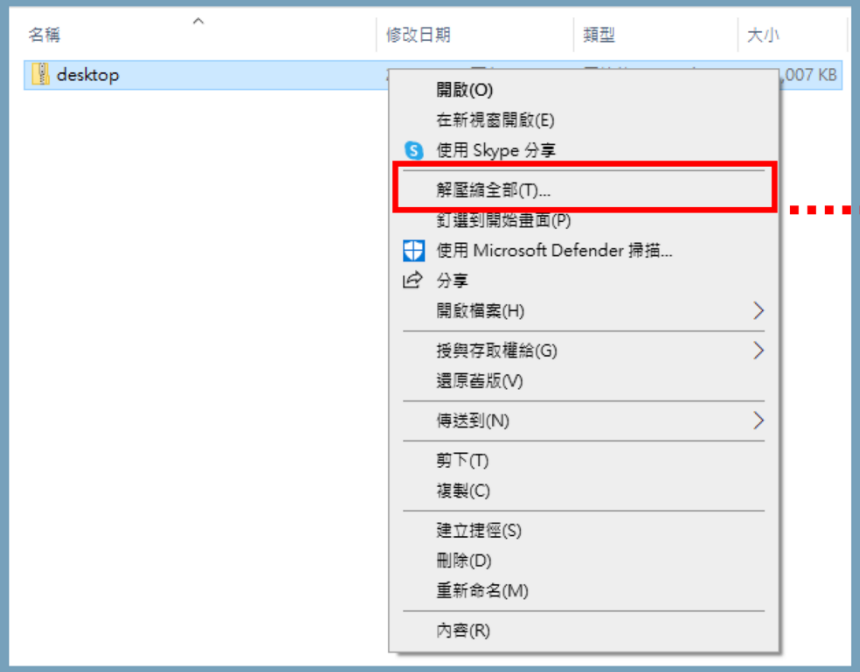
Camera Trap
計畫總覽
資料篩選與計算
上傳紀錄
幫助
Chun-I Chang
公告!
上傳程式軟體更新（v1.1.13版）
帳號設定
上傳程式下載
登出
臺灣自動相機資訊系統
Taiwan Camera Trap Information System
開始使用

11

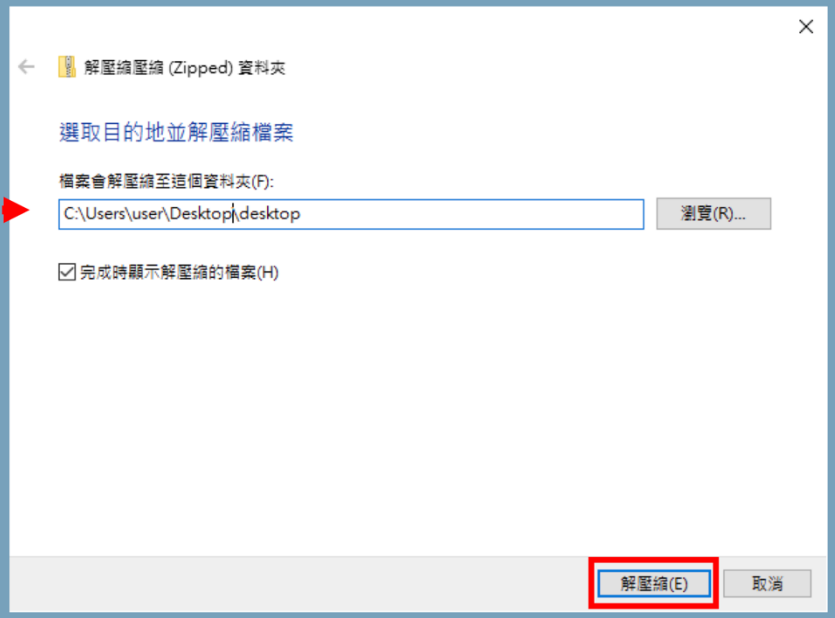
安裝檔下載


上傳程式下載
版本號：v1.1.13
版本更新說明
本次版本更新內容如下：
1. 更新物種下拉選單選項
a. 新增「灰鷺/褐鷺」、「山鷸鴴」、「灰頭黑臉鵐」、「臺灣/酒紅朱雀」4種鳥類
b. 「山羊」更改為「野山羊」
c. 「柳鶯類」改為「柳鶯類(無法辨識)」
2. 上傳程式資料夾中新增物種清單檔案（檔案名稱import-example-species.csv），使用文字資料與對應影像匯入功能時請統一物種寫法
3. 上傳通知調整為僅有上傳者會收到自己上傳資料完成與否的通知信件
4. 其他操作與上傳功能優化及bug調整
如您有編輯中或預計會再調整欄位內容的舊資料，欲將資料移至新版上傳程式中編輯與上傳的話， 相關資料移動說明如下：
移動舊版上傳程式資料夾中的 thumbnails 資料夾(縮圖檔) 跟 ct.db (資料庫檔)至新版上傳程式資料夾，如原本的資料庫檔名稱非「ct」，則一律更名為 ct。 若是已上傳的資料夾，則無法於新版上傳程式上再次上傳，建議先於舊版上傳程式完成上傳、尚未上傳之資料夾再於新版上傳程式上使用。
下載連結
點此下載
12

安裝檔開啟



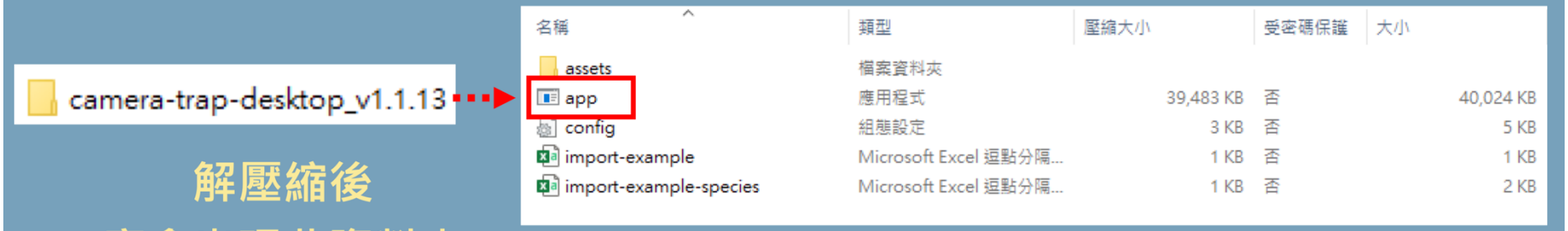
按右鍵>選取「解壓縮全部」



選取欲放置安裝檔的資料夾位置
點選「解壓縮」

13

安裝檔開啟

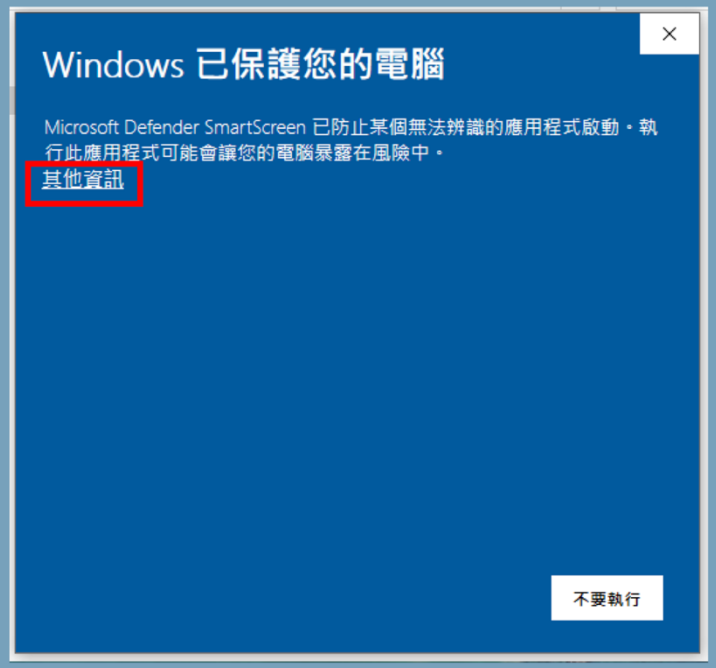


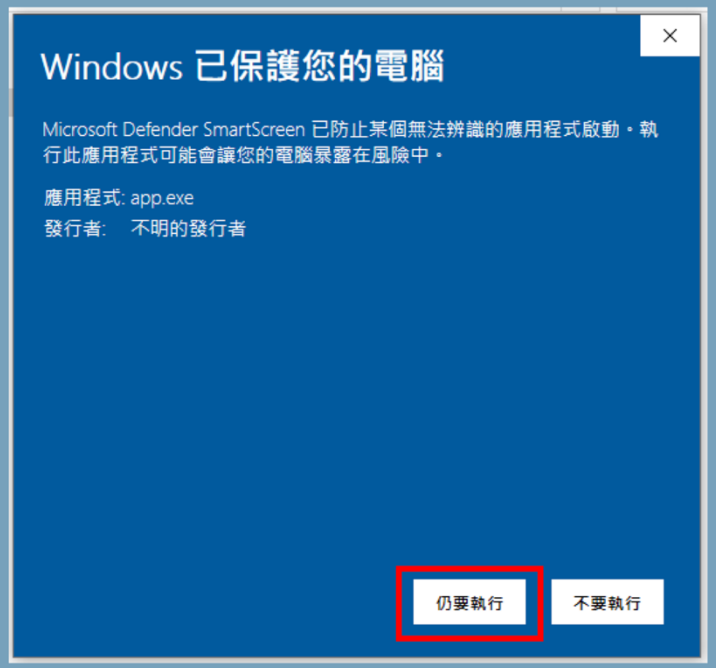
解壓縮後
應會出現此資料夾

請點選裡面的“app”檔案

14

安裝檔開啟





如開啟時跳出警告視窗，請點選「其他資訊」，再按「仍要執行」鍵

15

上傳介面功能說明

16

檔案匯入

login 工具 設定
Camera Trap
臺灣自動相機上傳系統
Taiwan Camera Trap System
現有資料夾
加入資料夾
選擇本機端的整個資料夾
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

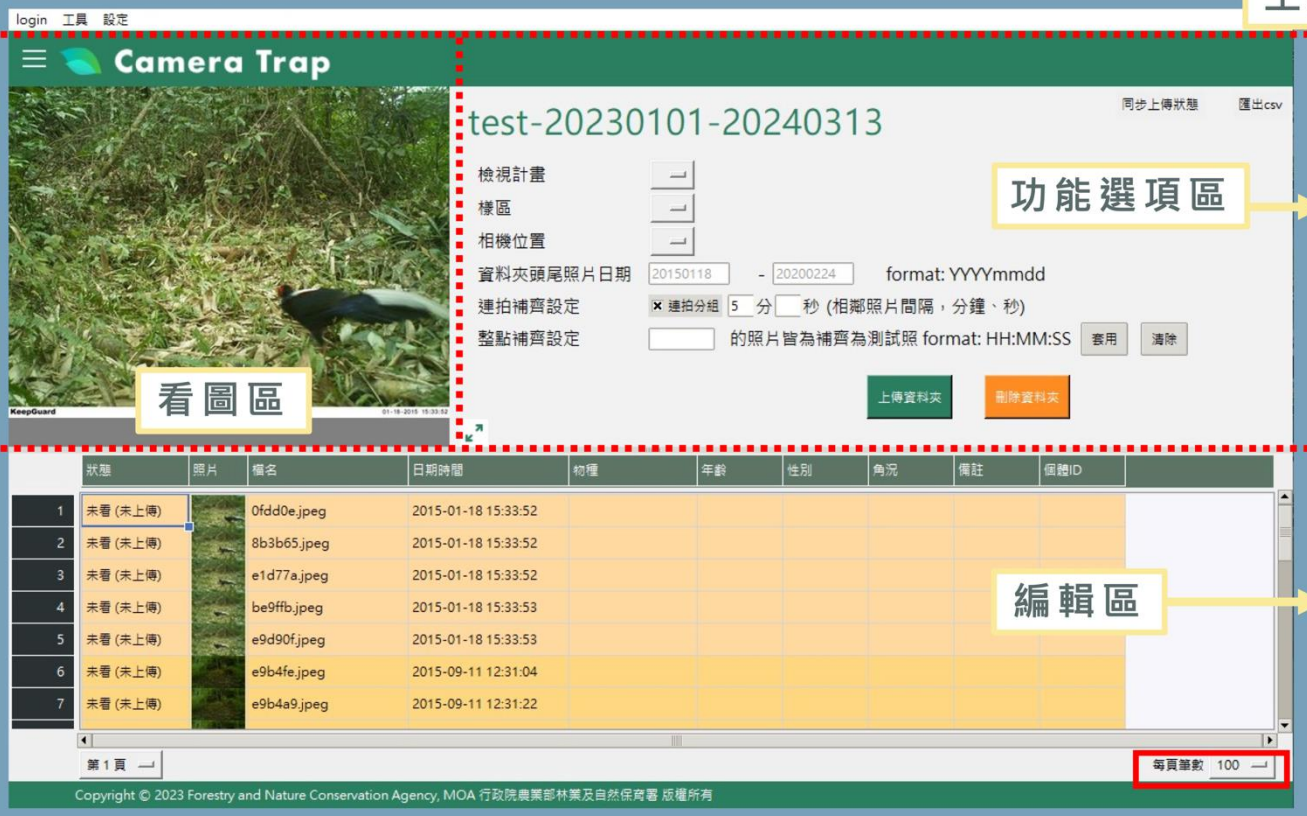
17

檔案匯入

login 工具 設定
Camera Trap
加入資料夾
現有資料夾
上傳進度
教學說明
選擇本機端的整個資料夾
臺灣自動相機上傳系統
Taiwan Camera Trap System
現有資料夾
加入資料夾
Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

18

檔案檢視 - 編輯介面



- 帳號登入
- 文字檔與影像匯入
- 設定快捷鍵
- 調整編輯區字體大小

- 選取計畫
- 連拍補齊設定
- 整點自動標註測試照
- 上傳資料
- 刪除資料夾
- 同步上傳狀態
- 匯出CSV檔

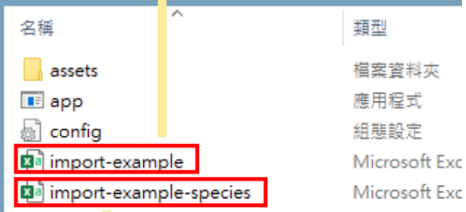
- 欄位內容編輯
- 複製/刪除一列
- 複製/貼上內容

19

檔案檢視 - 文字檔與影像匯入

可匯入已標註欄位內容之csv文字檔與對應影像
csv檔中之資料欄位需與現有上傳程式欄位相同，並需有影像檔名與日期時間欄位

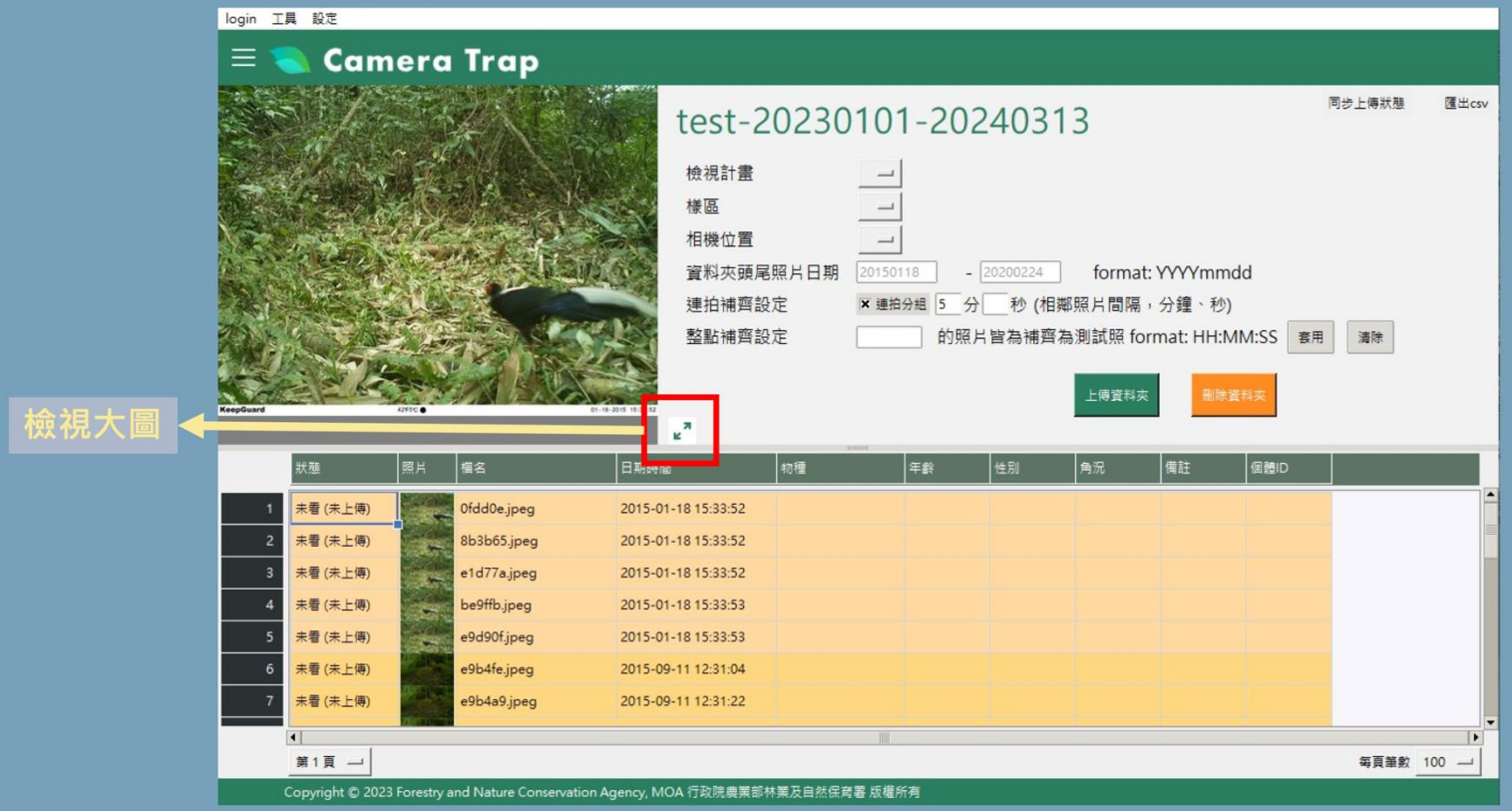
欄位範例檔



物種清單參考

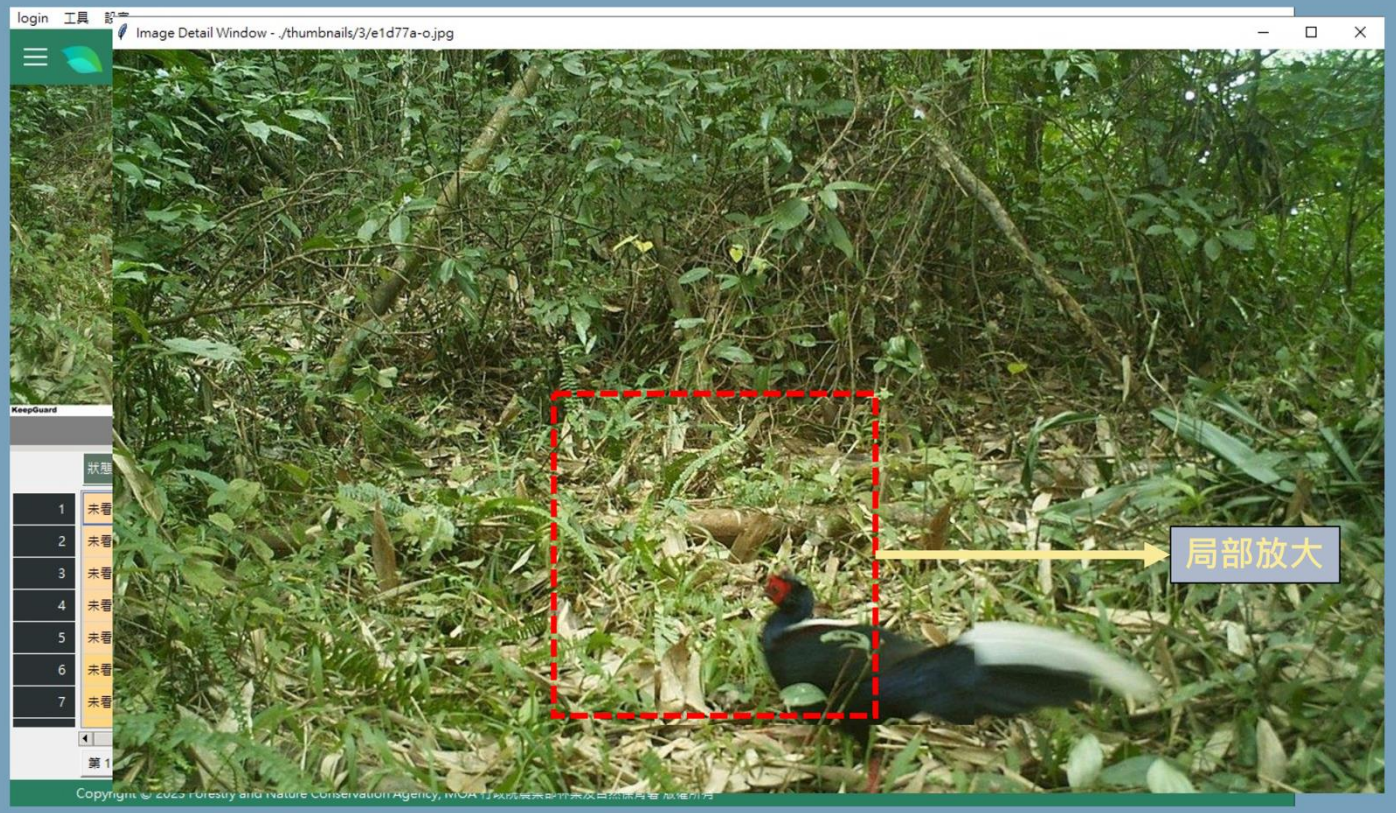
20

檔案檢視 - 檢視大圖


檢視大圖
login 工具 設定
Camera Trap
test-20230101-20240313
同步上傳狀態
匯出csv
檢視計畫
樣區
相機位置
資料夾頭尾照片日期
20150118
20200224
format: YYYYmmdd
連拍補齊設定
連拍分組
5
分
秒 (相鄰照片間隔，分鐘、秒)
整點補齊設定
的照片皆為補齊為測試照 format: HH:MM:SS
套用
清除
上傳資料夾
刪除資料夾
狀態
照片
檔名
日期時間
物種
年齡
性別
角況
備註
個體ID
1 未看 (未上傳) 0fdd0e.jpeg 2015-01-18 15:33:52
2 未看 (未上傳) 8b3b65.jpeg 2015-01-18 15:33:52
3 未看 (未上傳) e1d77a.jpeg 2015-01-18 15:33:52
4 未看 (未上傳) be9ffb.jpeg 2015-01-18 15:33:53
5 未看 (未上傳) e9d90f.jpeg 2015-01-18 15:33:53
6 未看 (未上傳) e9b4fe.jpeg 2015-09-11 12:31:04
7 未看 (未上傳) e9b4a9.jpeg 2015-09-11 12:31:22
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

檔案檢視 - 檢視大圖

可查看之前及之後的照片



22

上傳進度

檢視所有資料夾的上傳進度

現有資料夾

呈現本機所有已匯入之資料夾
與其編輯/上傳狀態

教學說明

使用說明、影像辨識與欄位填寫原則、常見問題

25

實際操作

跟著一步一步做

26

帳號登入

帳號
工具
設定
登入ORCID
登出
amera Trap
登入
ORCID登入
驗證碼(網頁登入後將顯示四碼數字)
送出
臺灣自動相機上傳系統
Taiwan Camera Trap System
現有資料夾
加入資料夾
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

27

帳號登入

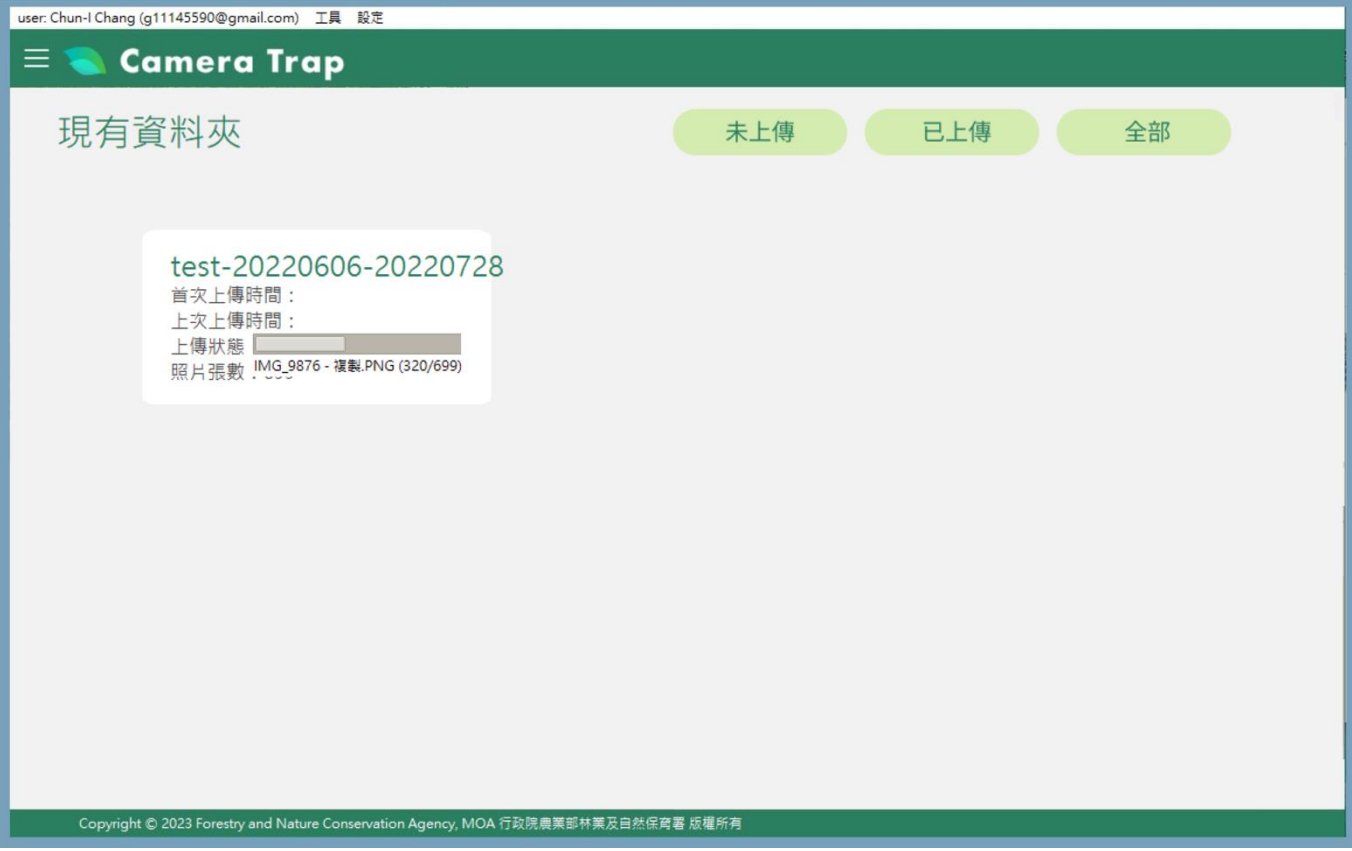
Camera Trap
計畫總覽
資料篩選與計算
上傳紀錄
幫助
Chun-I Chang
Camera Trap 桌機版登入
驗證碼: 7073
Camera Trap
行政院農業部
林業及自然保育署
行政院農業部
生物多樣性研究所
台灣生物多樣性
資訊入口網
國立屏東科技大學
隱私權政策 | Copyright © 2023 Forestry and Nature Conservation Agency 行政院行政院農業部林業及自然保育署 版權所有

檔案匯入

資料夾命名須符合格式：
名稱-行程開始日期-行程結束日期

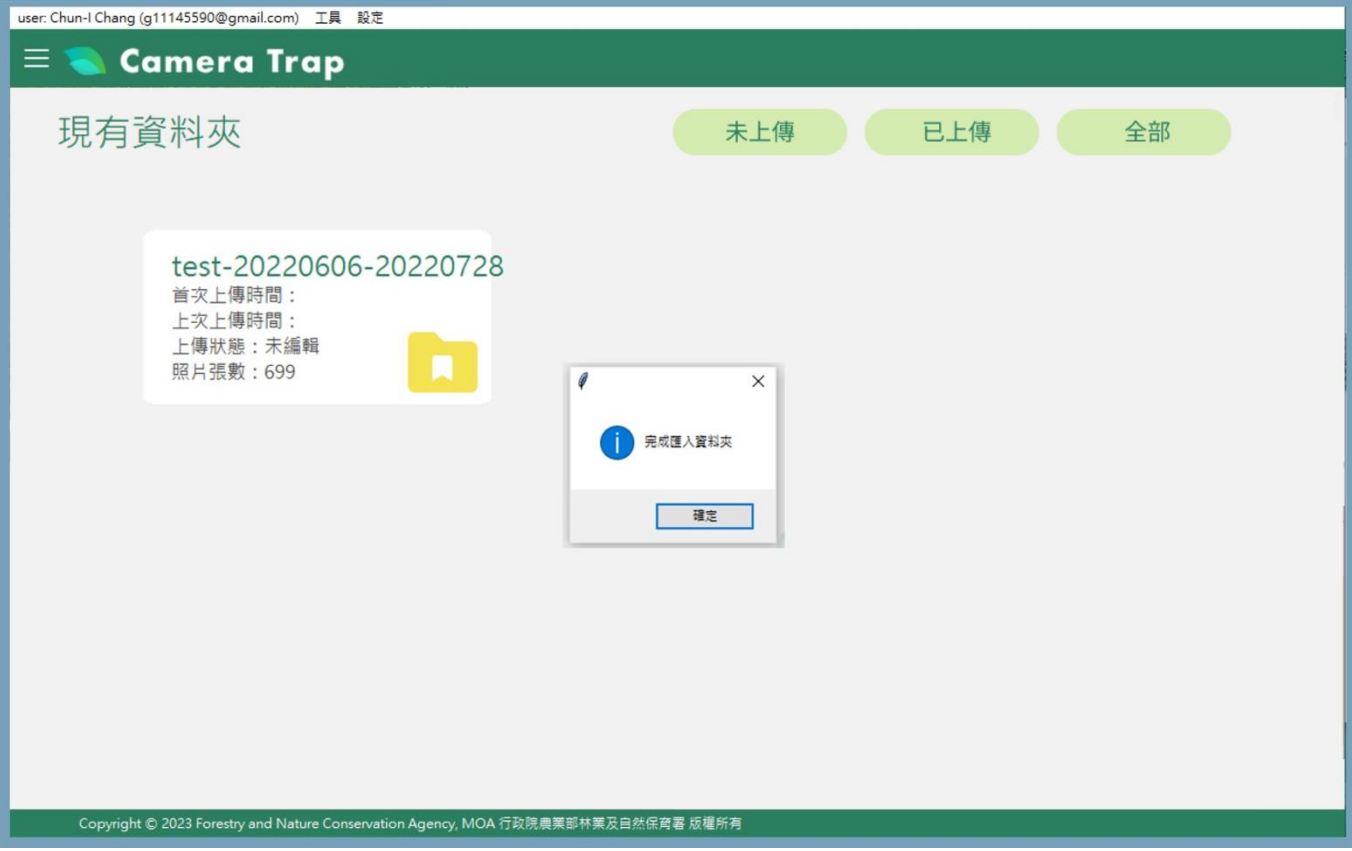
29

檔案匯入


user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
現有資料夾
未上傳
已上傳
全部
test-20220606-20220728
首次上傳時間：
上次上傳時間：
上傳狀態
照片張數
IMG_9876 - 複製.PNG (320/699)
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

30

檔案匯入


user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
現有資料夾
未上傳
已上傳
全部
test-20220606-20220728
首次上傳時間：
上次上傳時間：
上傳狀態：未編輯
照片張數：699
完成匯入資料夾
確定
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

31

選取計畫

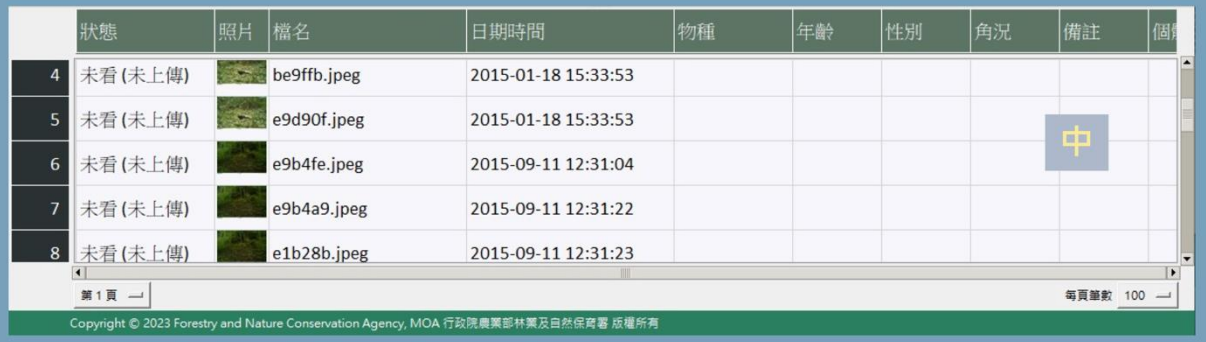
選取測試計畫、樣區與相機位置
test-20230101-20240313
同步上傳狀態
匯出csv
檢視計畫
2024 教育訓練
樣區
test2024
相機位置
2
資料夾頭尾照片日期
20150118
-
20200224
format: YYYYmmdd
連拍補齊設定
連拍分組
5
分
秒 (相鄰照片間隔，分鐘、秒)
整點補齊設定
的照片皆為補齊為測試照 format: HH:MM:SS
套用
清除
上傳資料夾
刪除資料夾
KeepGuard

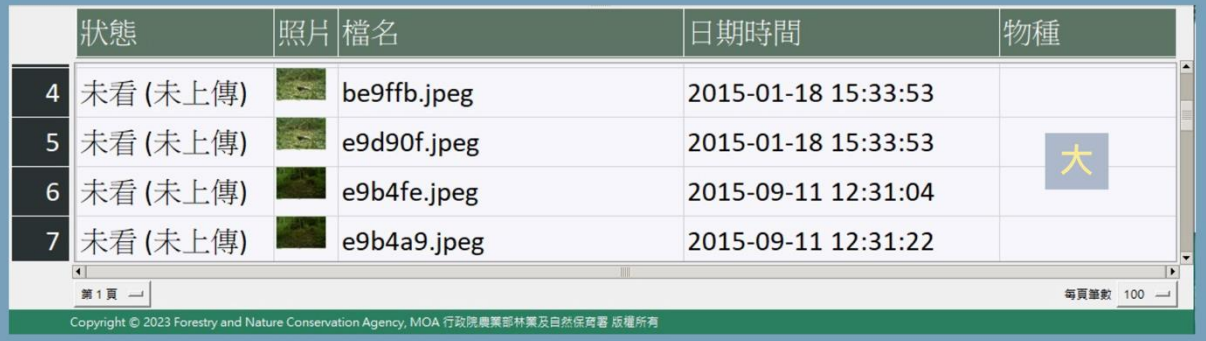
檔案編輯

工具
設定
設定快捷鍵
設定字體大小
可自行設定編輯區字體大小
user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
同步上傳狀態
匯出csv
Camera Trap Desktop - 設定字體大小
字體
編輯區字體大小
S
小
中
大
儲存設定
YYmmdd
秒)
t: HH:MM:SS
套用
清除
刪除資料夾
狀態
照片
檔名
個體ID
4 未看 (未上傳) be9ffb.jpeg
5 未看 (未上傳) e9d90f.jpeg
6 未看 (未上傳) e9b4fe.jpeg
7 未看 (未上傳) e9b4a9.jpeg 2015-09-11 12:31:22
8 未看 (未上傳) e1b28b.jpeg 2015-09-11 12:31:23
9 未看 (未上傳) e1b2a6.jpeg 2015-09-11 12:31:23
10 未看 (未上傳) e1b2b5.jpeg 2015-09-11 12:31:41
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

33

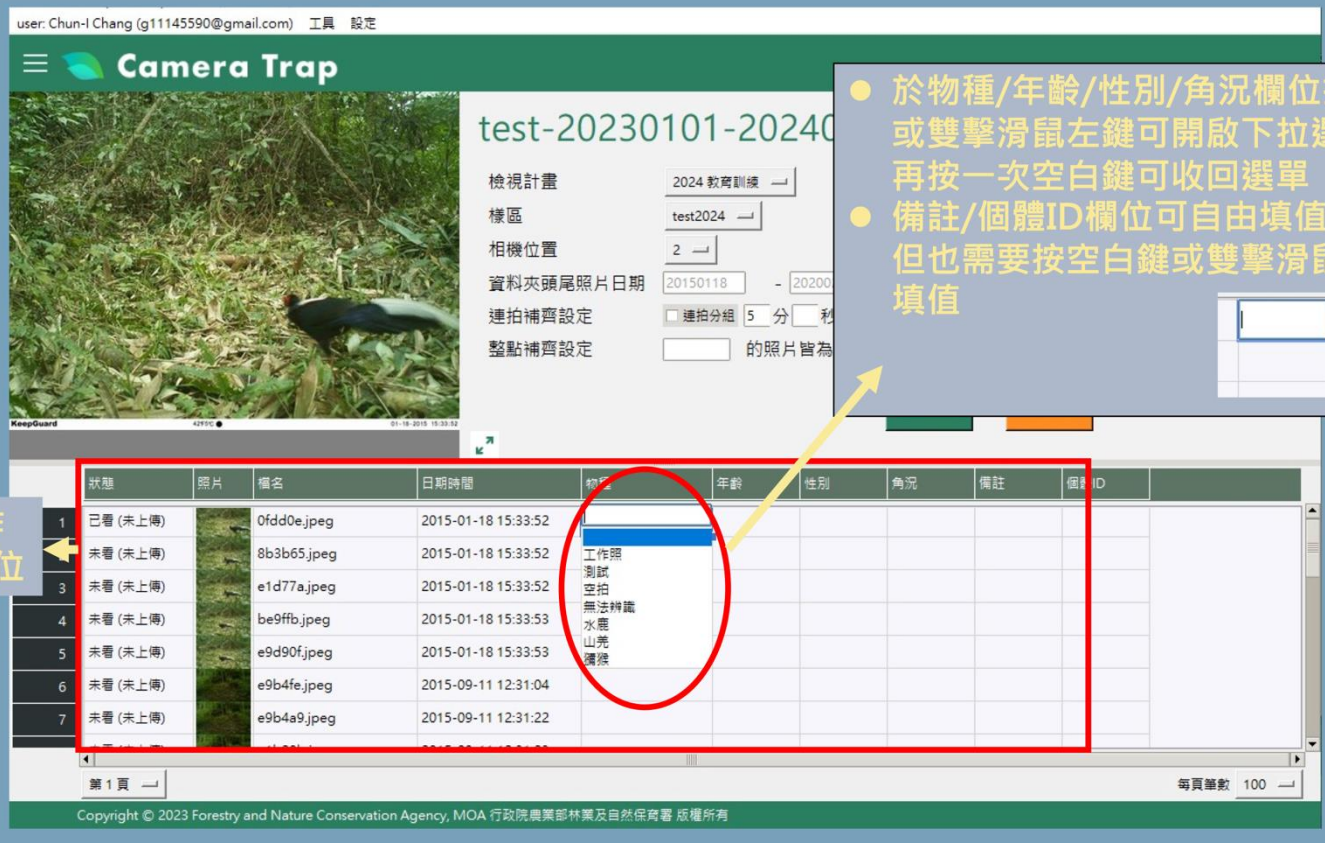
檔案編輯


狀態
照片
檔名
日期時間
物種
年齡
性別
角況
備註
4 未看 (未上傳) be9ffb.jpeg 2015-01-18 15:33:53
5 未看 (未上傳) e9d90f.jpeg 2015-01-18 15:33:53
6 未看 (未上傳) e9b4fe.jpeg 2015-09-11 12:31:04
7 未看 (未上傳) e9b4a9.jpeg 2015-09-11 12:31:22
8 未看 (未上傳) e1b28b.jpeg 2015-09-11 12:31:23
中
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有


狀態
照片
檔名
日期時間
物種
4 未看 (未上傳) be9ffb.jpeg 2015-01-18 15:33:53
5 未看 (未上傳) e9d90f.jpeg 2015-01-18 15:33:53
6 未看 (未上傳) e9b4fe.jpeg 2015-09-11 12:31:04
7 未看 (未上傳) e9b4a9.jpeg 2015-09-11 12:31:22
大
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

檔案編輯

物種為必填欄位，若未填上傳時會跳出提醒



- 於物種/年齡/性別/角況欄位按空白鍵或雙擊滑鼠左鍵可開啟下拉選單，再按一次空白鍵可收回選單
- 備註/個體ID欄位可自由填值，但也需要按空白鍵或雙擊滑鼠左鍵才可填值

Excel欄位可以操作
上下左右鍵選擇欄位

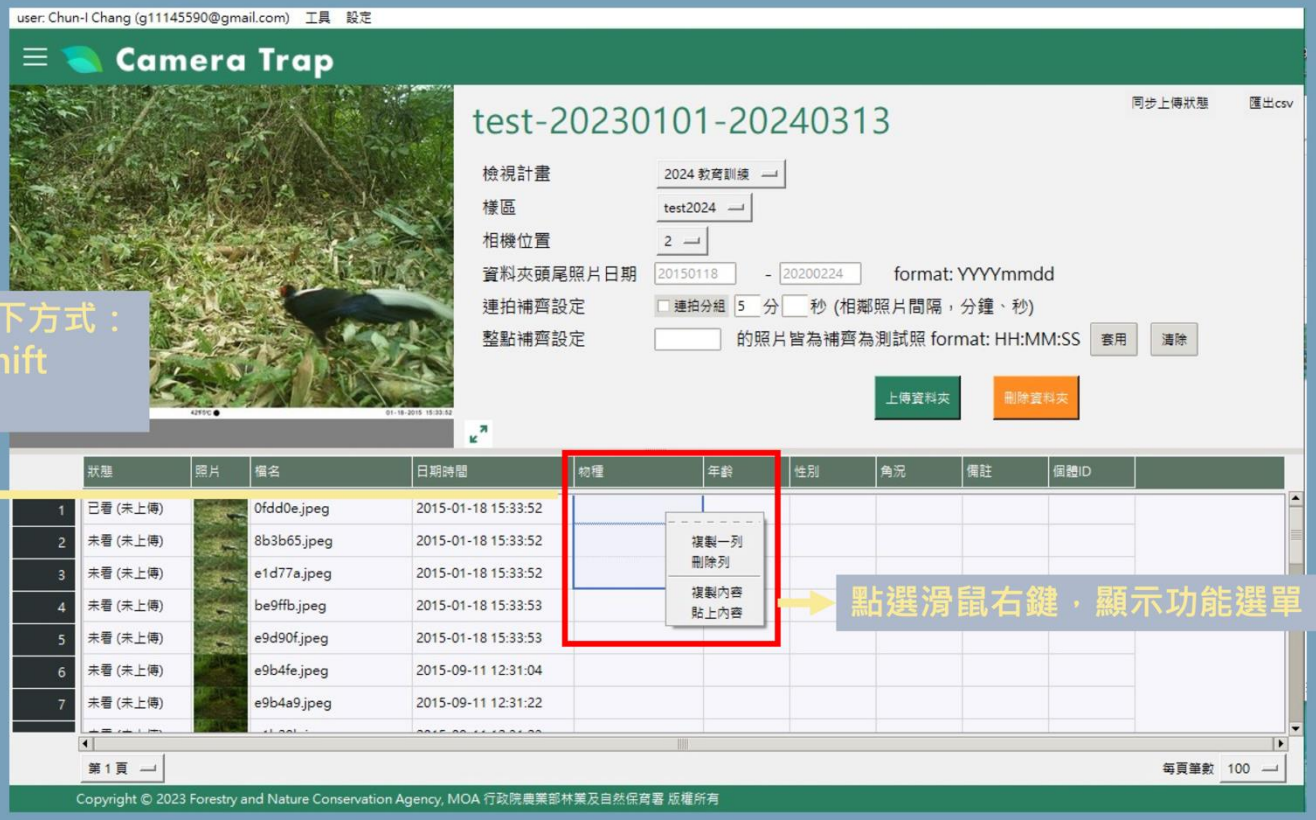
35

檔案編輯

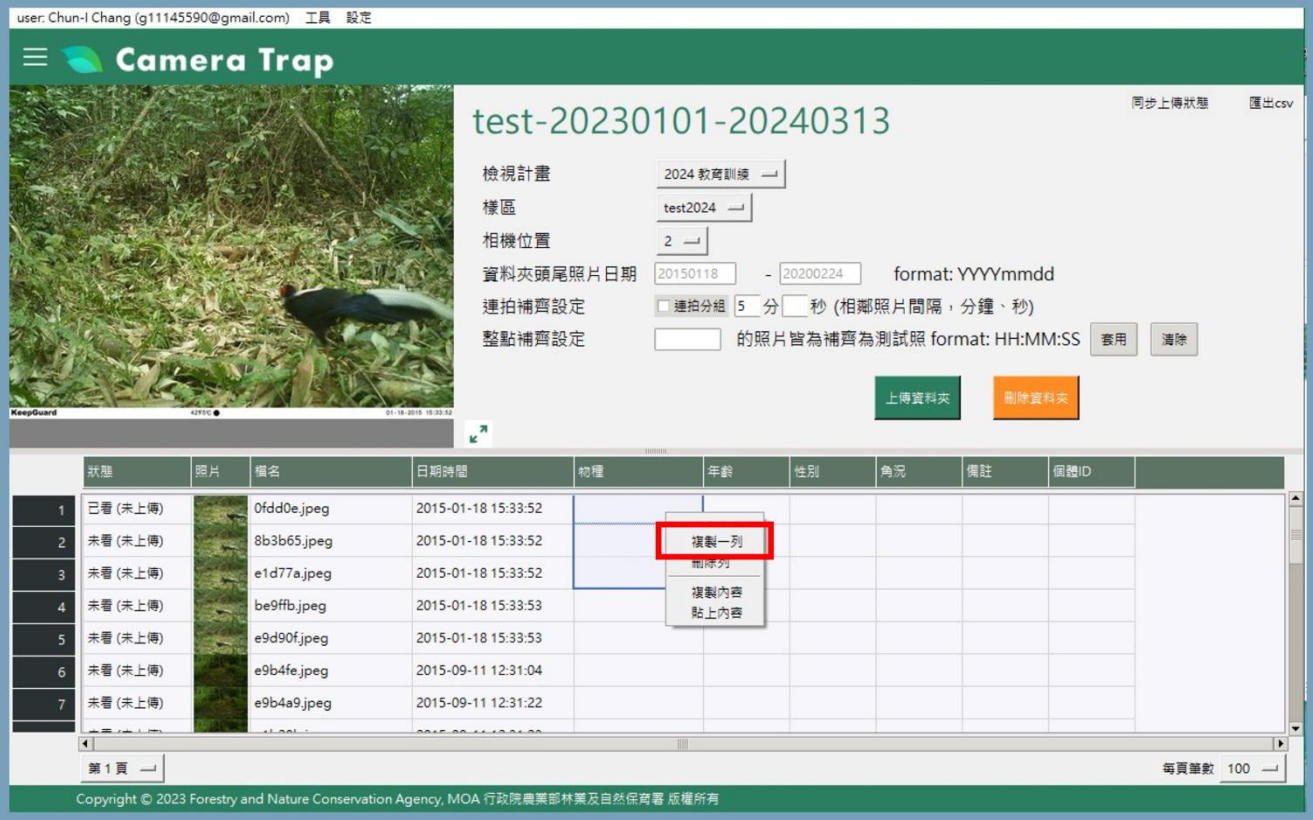
工具
設定
設定快捷鍵
設定字體大小
可自行設定物種常用快捷鍵
user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
同步上傳狀態
匯出csv
Camera Trap Desktop - 設定鍵盤快捷鍵
快捷鍵組合
Ctrl-1 測試
Ctrl-2 工作照
Ctrl-3 山羌
Ctrl-4 獼猴
Ctrl-5 野豬
Ctrl-6 鼬獾
Ctrl-7 白鼻心
Ctrl-8 食蟹獴
Ctrl-9 鳥
Ctrl-0 空拍
儲存設定
Ymmdd
秒)
HH:MM:SS
套用
清除
刪除資料夾
狀態
照片
檔名
個體ID
1 已看 (未上傳) 0fdd0e.jpeg
2 未看 (未上傳) 8b3b65.jpeg
3 未看 (未上傳) e1d77a.jpeg
4 未看 (未上傳) be9ffb.jpeg
5 未看 (未上傳) e9d90f.jpeg 2015-01-18 15:33:53
6 未看 (未上傳) e9b4fe.jpeg 2015-09-11 12:31:04
7 未看 (未上傳) e9b4a9.jpeg 2015-09-11 12:31:22
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

36

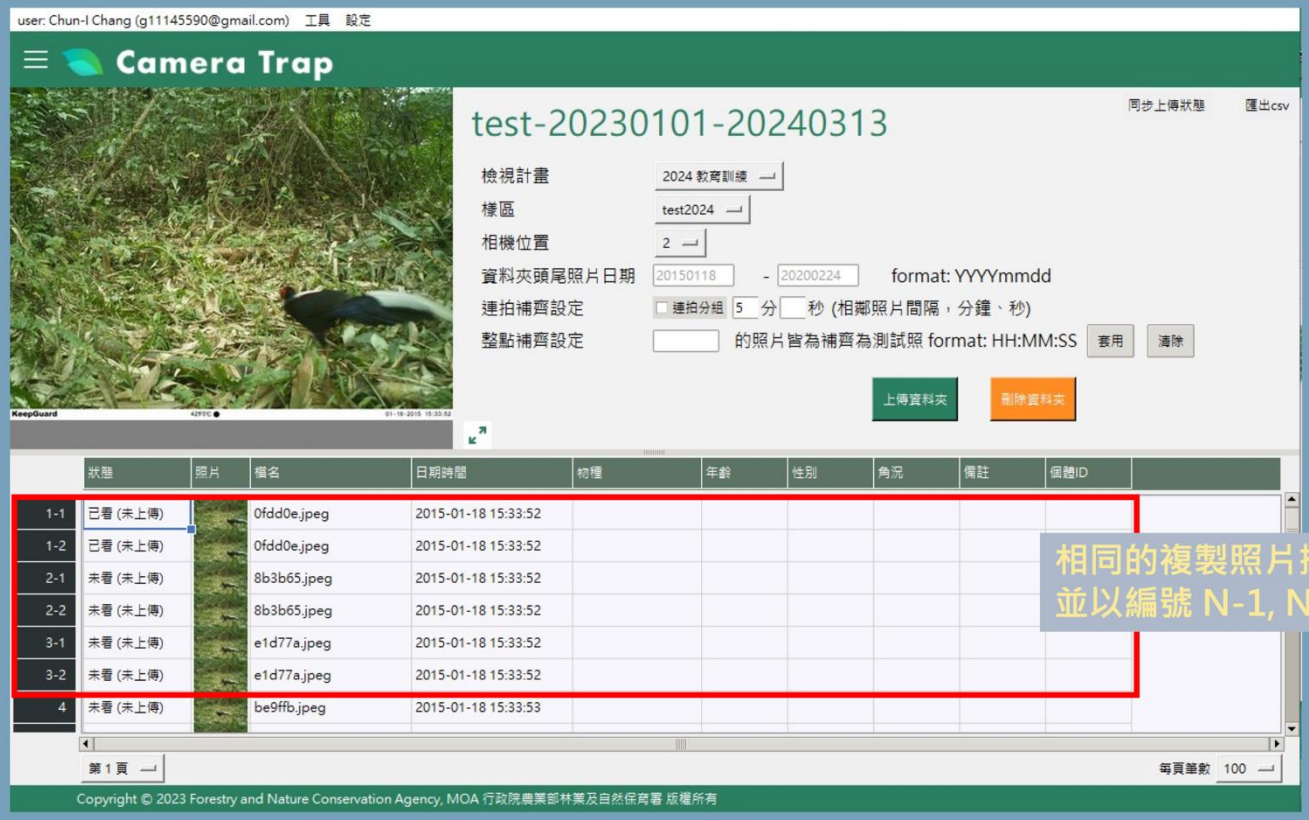
檔案編輯


user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
test-20230101-20240313
同步上傳狀態
匯出csv
檢視計畫 2024 教育訓練
樣區 test2024
相機位置 2
資料夾頭尾照片日期 20150118 - 20200224 format: YYYYmmdd
連拍補齊設定 連拍分組 5 分 秒 (相鄰照片間隔，分鐘、秒)
整點補齊設定 的照片皆為補齊為測試照 format: HH:MM:SS 套用 清除
上傳資料夾
刪除資料夾
狀態 照片 檔名 日期時間 物種 年齡 性別 角況 備註 個體ID
1 已看 (未上傳) 0fdd0e.jpeg 2015-01-18 15:33:52
2 未看 (未上傳) 8b3b65.jpeg 2015-01-18 15:33:52
3 未看 (未上傳) e1d77a.jpeg 2015-01-18 15:33:52
4 未看 (未上傳) be9ffb.jpeg 2015-01-18 15:33:53
5 未看 (未上傳) e9d90f.jpeg 2015-01-18 15:33:53
6 未看 (未上傳) e9b4fe.jpeg 2015-09-11 12:31:04
7 未看 (未上傳) e9b4a9.jpeg 2015-09-11 12:31:22
複製一列
刪除列
複製內容
貼上內容
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有
可以使用以下方式：
拖曳/ctrl/shift
選取多列
點選滑鼠右鍵，顯示功能選單

檔案編輯


user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
test-20230101-20240313
同步上傳狀態
匯出csv
檢視計畫
2024 教育訓練
樣區
test2024
相機位置
2
資料夾頭尾照片日期
20150118
20200224
format: YYYYmmdd
連拍補齊設定
連拍分組
5 分 秒 (相鄰照片間隔，分鐘、秒)
整點補齊設定
的照片皆為補齊為測試照 format: HH:MM:SS
套用
清除
上傳資料夾
刪除資料夾
狀態
照片
檔名
日期時間
物種
年齡
性別
角況
備註
個體ID
1 已看 (未上傳) 0fdd0e.jpeg 2015-01-18 15:33:52
2 未看 (未上傳) 8b3b65.jpeg 2015-01-18 15:33:52
3 未看 (未上傳) e1d77a.jpeg 2015-01-18 15:33:52
4 未看 (未上傳) be9ffb.jpeg 2015-01-18 15:33:53
5 未看 (未上傳) e9d90f.jpeg 2015-01-18 15:33:53
6 未看 (未上傳) e9b4fe.jpeg 2015-09-11 12:31:04
7 未看 (未上傳) e9b4a9.jpeg 2015-09-11 12:31:22
複製一列
刪除列
複製內容
貼上內容
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

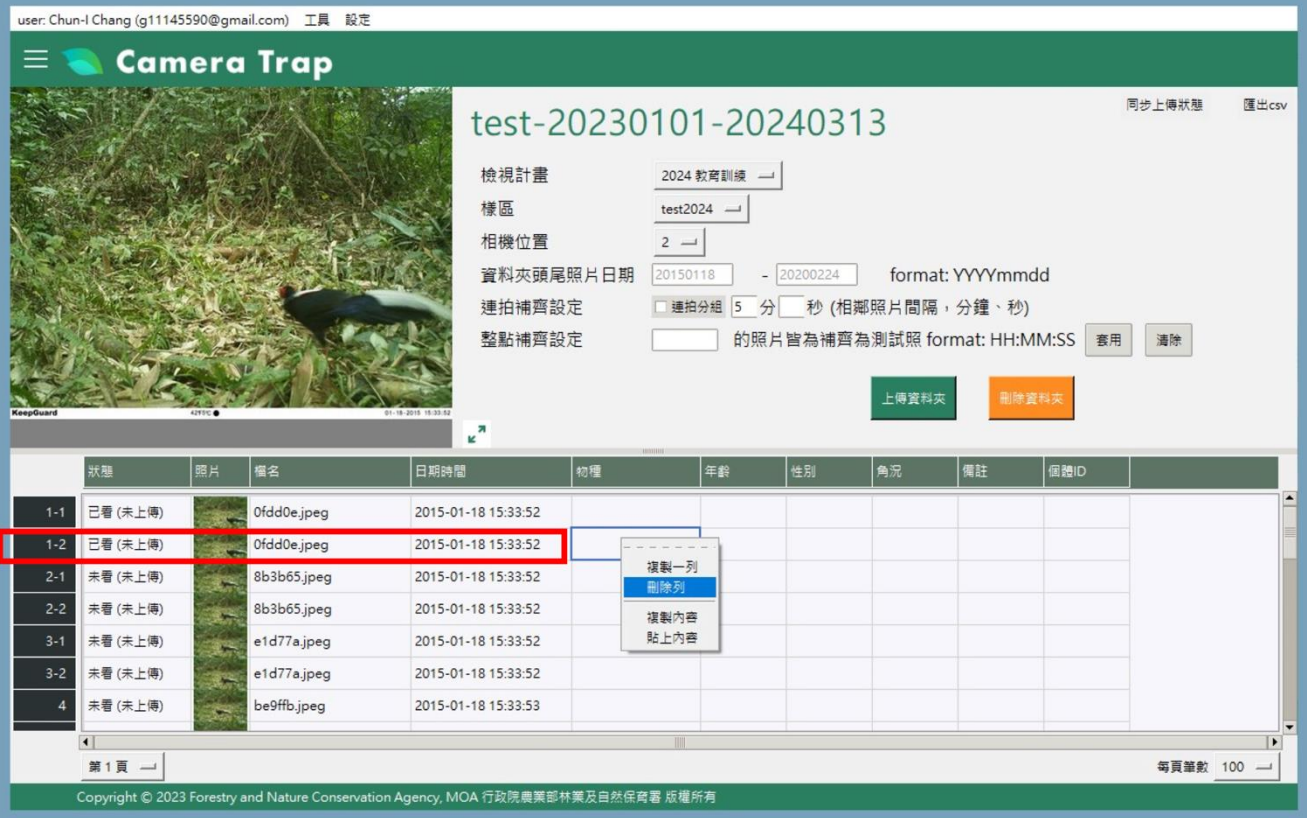
檔案編輯



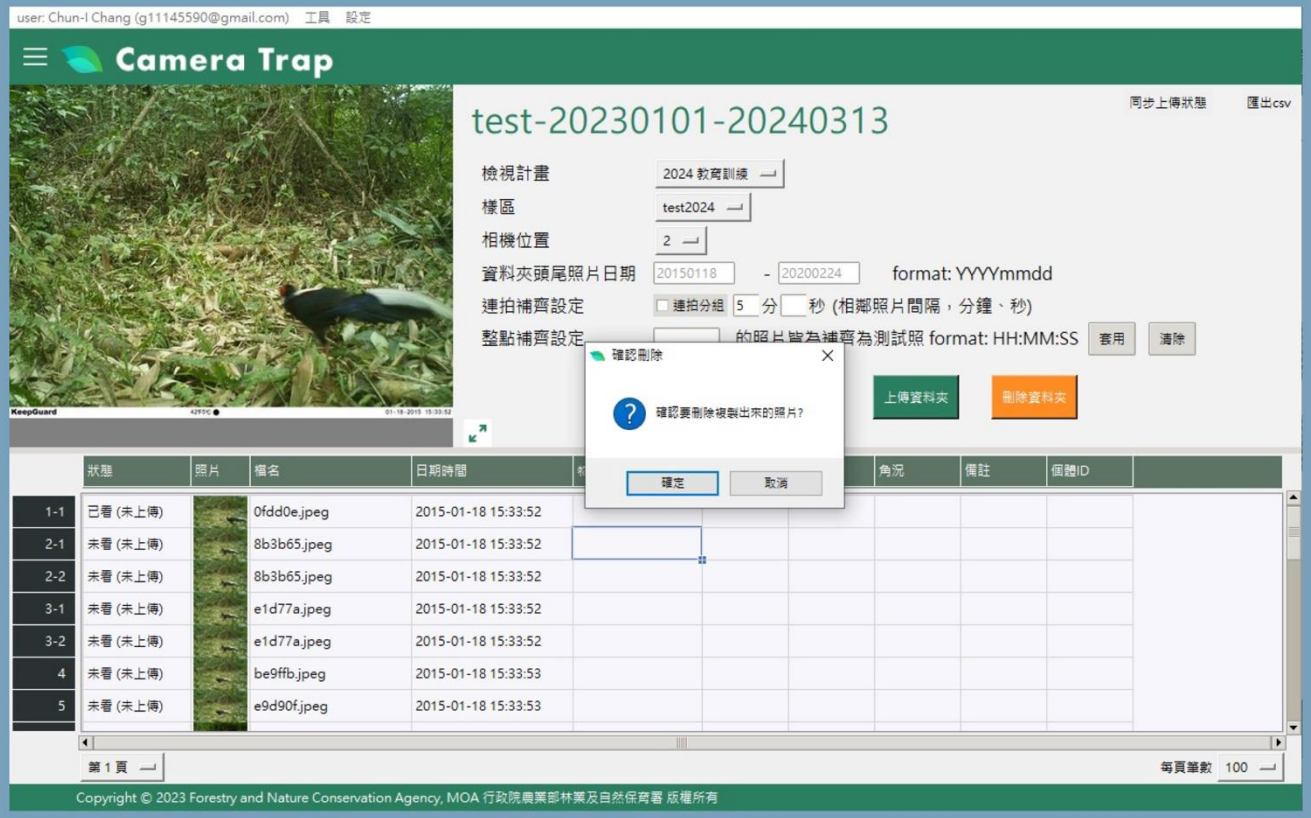
相同的複製照片排序在一起，
並以編號 N-1, N-2...顯示

檔案編輯

僅能刪除複製出來的照片

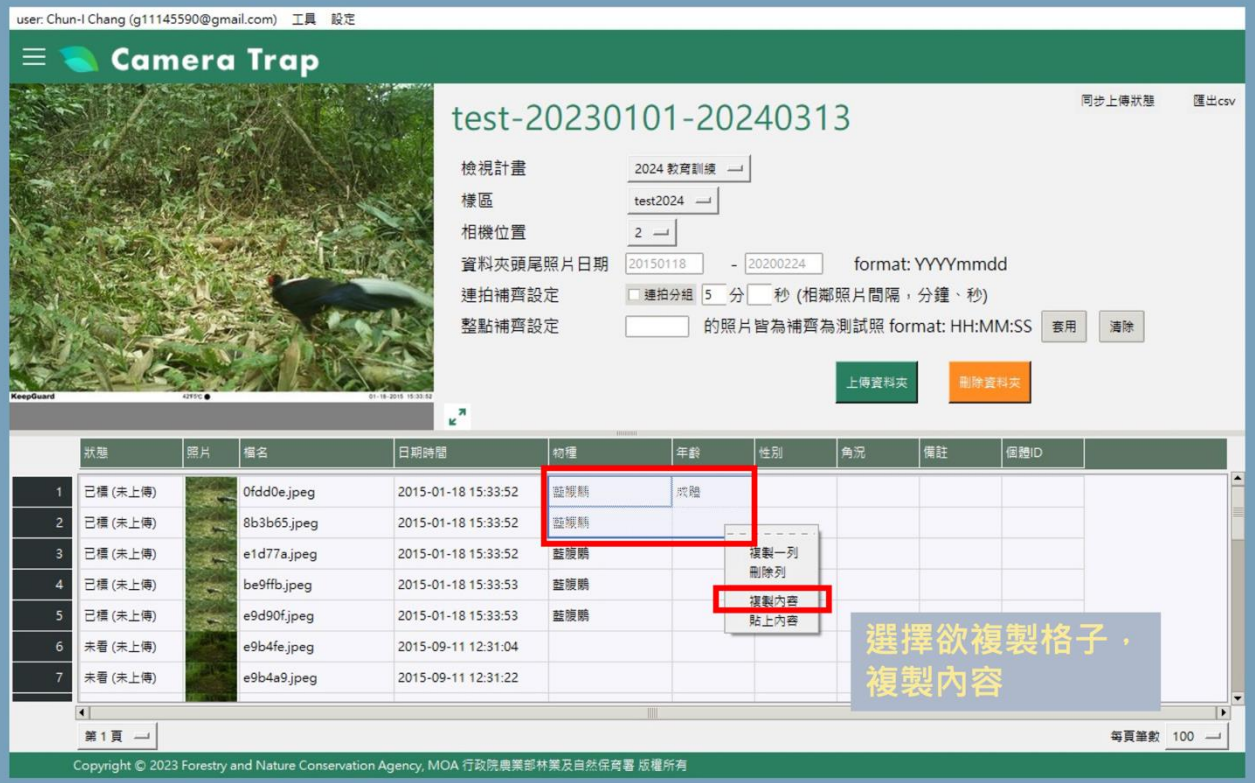


檔案編輯


user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
test-20230101-20240313
同步上傳狀態
匯出csv
檢視計畫
2024 教育訓練
樣區
test2024
相機位置
2
資料夾頭尾照片日期
20150118
20200224
format: YYYYmmdd
連拍補齊設定
連拍分組
5 分 秒 (相鄰照片間隔，分鐘、秒)
整點補齊設定
的照片皆為補齊為測試照 format: HH:MM:SS
套用
清除
上傳資料夾
刪除資料夾
確認刪除
確認要刪除複製出來的照片?
確定
取消
狀態
照片
檔名
日期時間
角況
備註
個體ID
1-1 已看 (未上傳) 0fdd0e.jpeg 2015-01-18 15:33:52
2-1 未看 (未上傳) 8b3b65.jpeg 2015-01-18 15:33:52
2-2 未看 (未上傳) 8b3b65.jpeg 2015-01-18 15:33:52
3-1 未看 (未上傳) e1d77a.jpeg 2015-01-18 15:33:52
3-2 未看 (未上傳) e1d77a.jpeg 2015-01-18 15:33:52
4 未看 (未上傳) be9ffb.jpeg 2015-01-18 15:33:53
5 未看 (未上傳) e9d90f.jpeg 2015-01-18 15:33:53
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

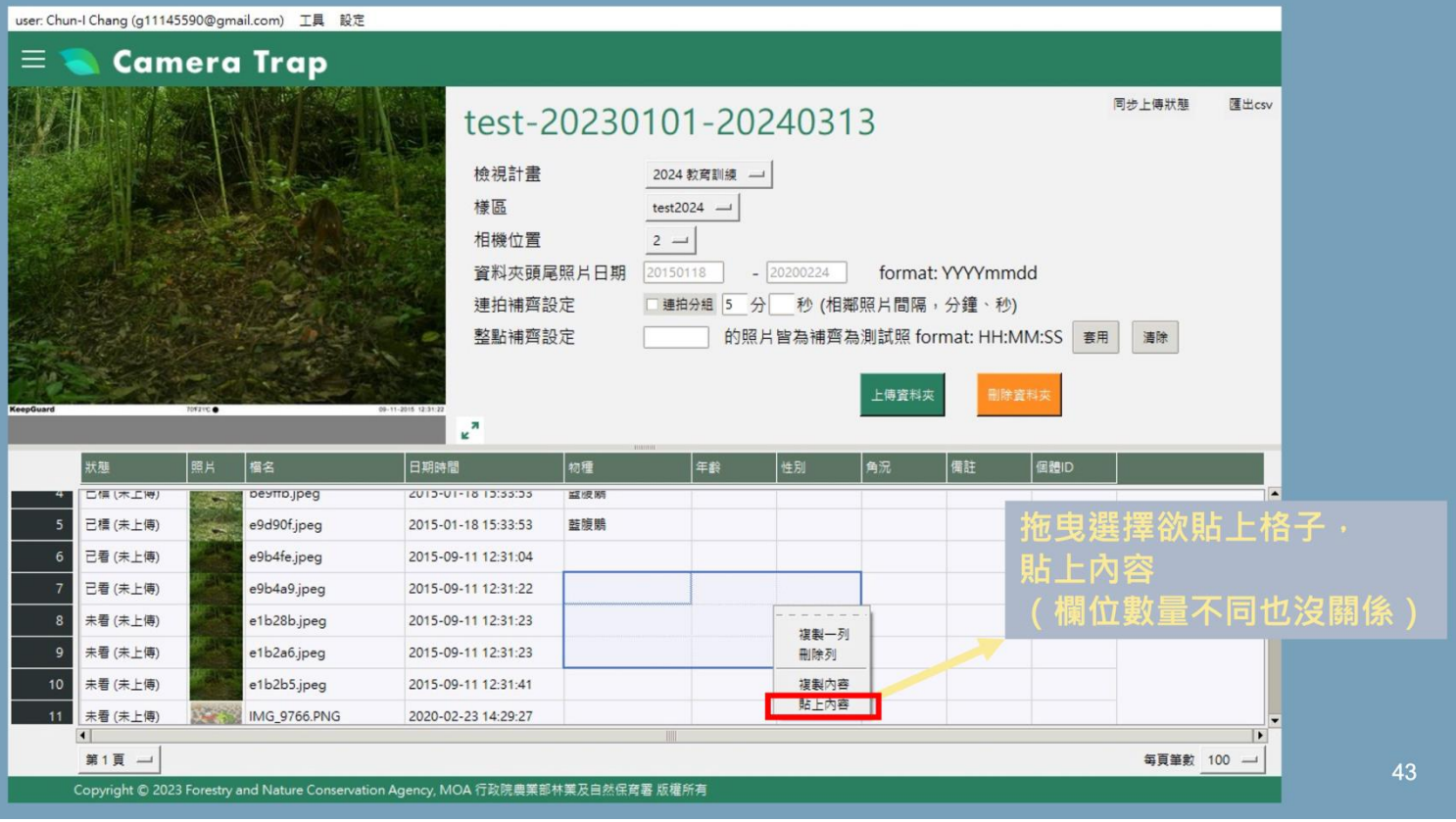
41

檔案編輯

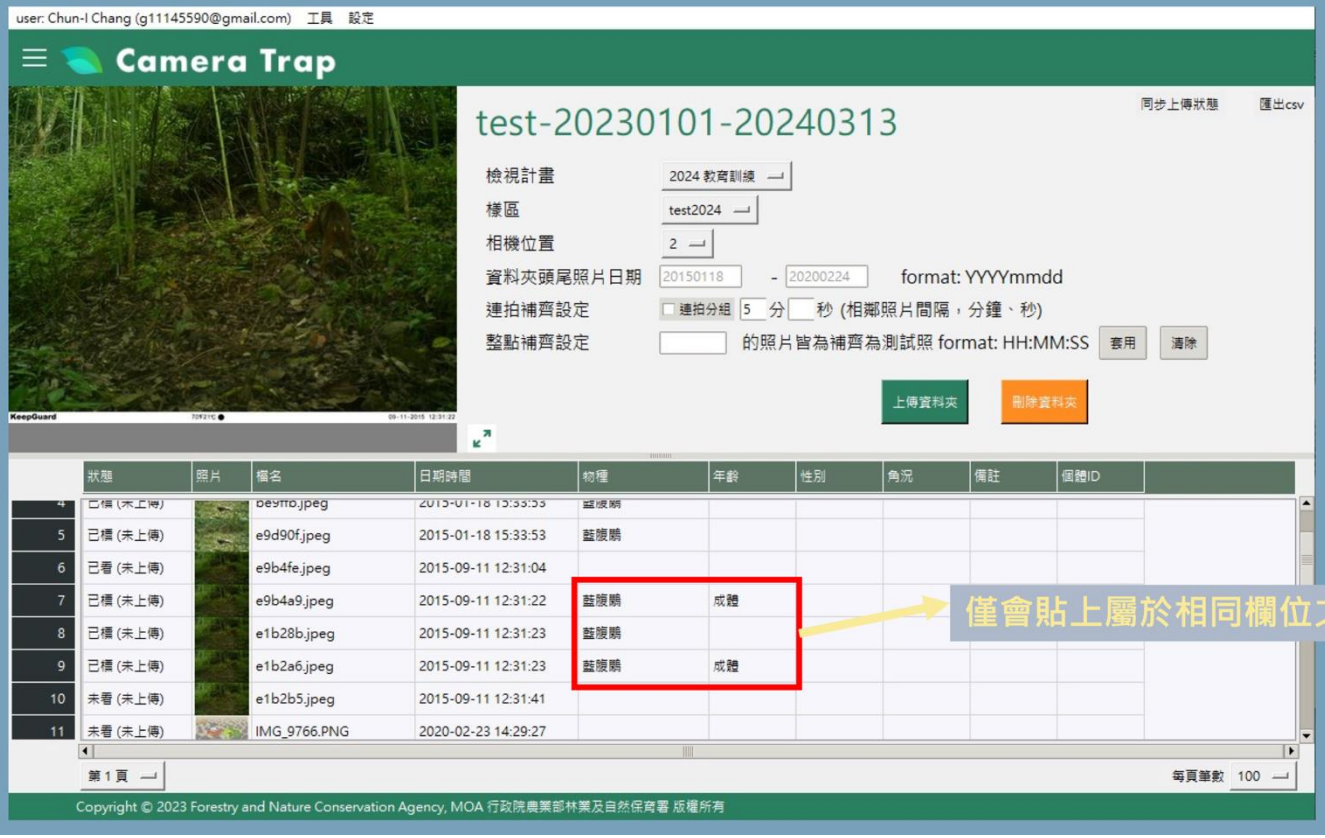


也可利用向下拖曳方式
直接複製內容

檔案編輯


user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
test-20230101-20240313
同步上傳狀態
匯出csv
檢視計畫
2024 教育訓練
樣區
test2024
相機位置
2
資料夾頭尾照片日期
20150118
20200224
format: YYYYmmdd
連拍補齊設定
連拍分組
5
分
秒 (相鄰照片間隔，分鐘、秒)
整點補齊設定
的照片皆為補齊為測試照 format: HH:MM:SS
套用
清除
上傳資料夾
刪除資料夾
狀態
照片
檔名
日期時間
物種
年齡
性別
角況
備註
個體ID
5 已標 (未上傳) e9d90f.jpeg 2015-01-18 15:33:53 藍腹鷴
6 已看 (未上傳) e9b4fe.jpeg 2015-09-11 12:31:04
7 已看 (未上傳) e9b4a9.jpeg 2015-09-11 12:31:22
8 未看 (未上傳) e1b28b.jpeg 2015-09-11 12:31:23
9 未看 (未上傳) e1b2a6.jpeg 2015-09-11 12:31:23
10 未看 (未上傳) e1b2b5.jpeg 2015-09-11 12:31:41
11 未看 (未上傳) IMG_9766.PNG 2020-02-23 14:29:27
複製一列
刪除列
複製內容
貼上內容
拖曳選擇欲貼上格子，
貼上內容
（欄位數量不同也沒關係）
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

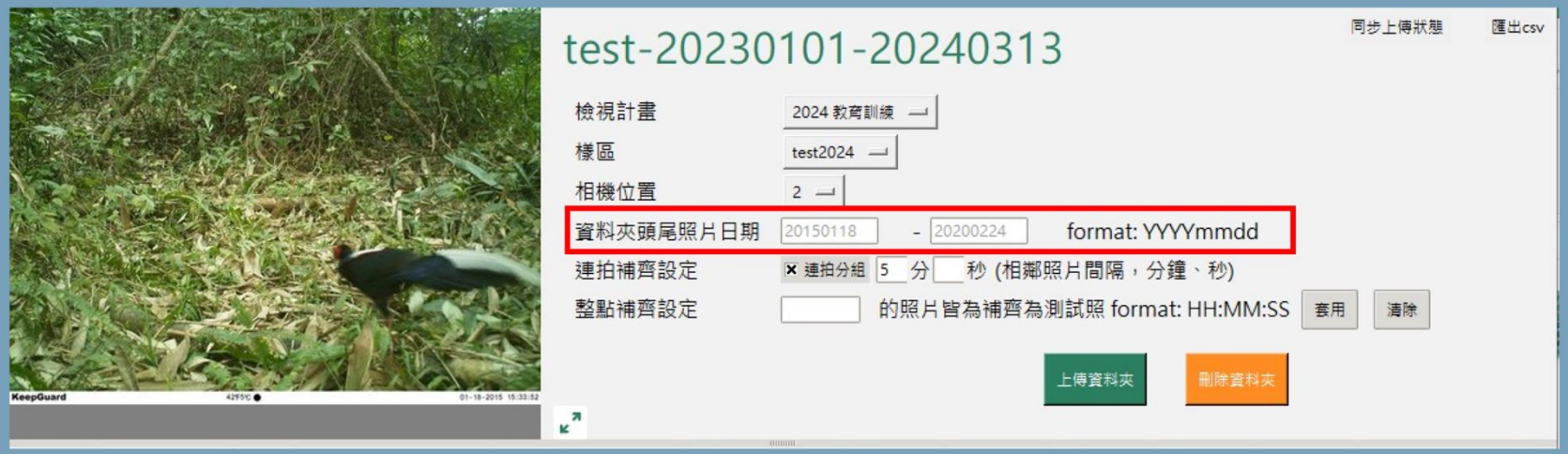
檔案編輯


user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
test-20230101-20240313
同步上傳狀態
匯出csv
檢視計畫
2024 教育訓練
樣區
test2024
相機位置
2
資料夾頭尾照片日期
20150118
-
20200224
format: YYYYmmdd
連拍補齊設定
連拍分組
5
分
秒 (相鄰照片間隔，分鐘、秒)
整點補齊設定
的照片皆為補齊為測試照 format: HH:MM:SS
套用
清除
上傳資料夾
刪除資料夾
狀態
照片
檔名
日期時間
物種
年齡
性別
角況
備註
個體ID
5 已標 (未上傳) e9d90f.jpeg 2015-01-18 15:33:53 藍腹鷴
6 已看 (未上傳) e9b4fe.jpeg 2015-09-11 12:31:04
7 已標 (未上傳) e9b4a9.jpeg 2015-09-11 12:31:22 藍腹鷴 成體
8 已標 (未上傳) e1b28b.jpeg 2015-09-11 12:31:23 藍腹鷴
9 已標 (未上傳) e1b2a6.jpeg 2015-09-11 12:31:23 藍腹鷴 成體
10 未看 (未上傳) e1b2b5.jpeg 2015-09-11 12:31:41
11 未看 (未上傳) IMG_9766.PNG 2020-02-23 14:29:27
僅會貼上屬於相同欄位之內容
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

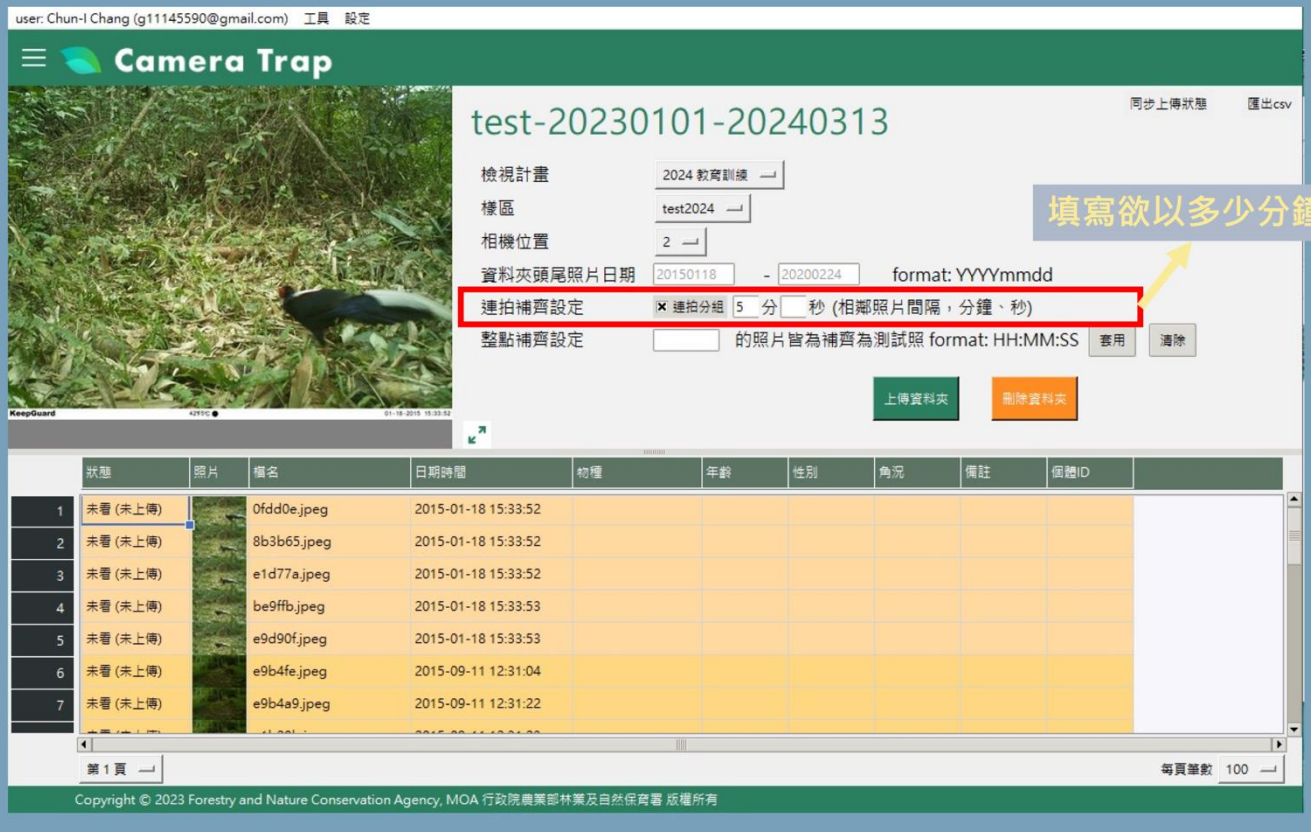
44

檔案編輯

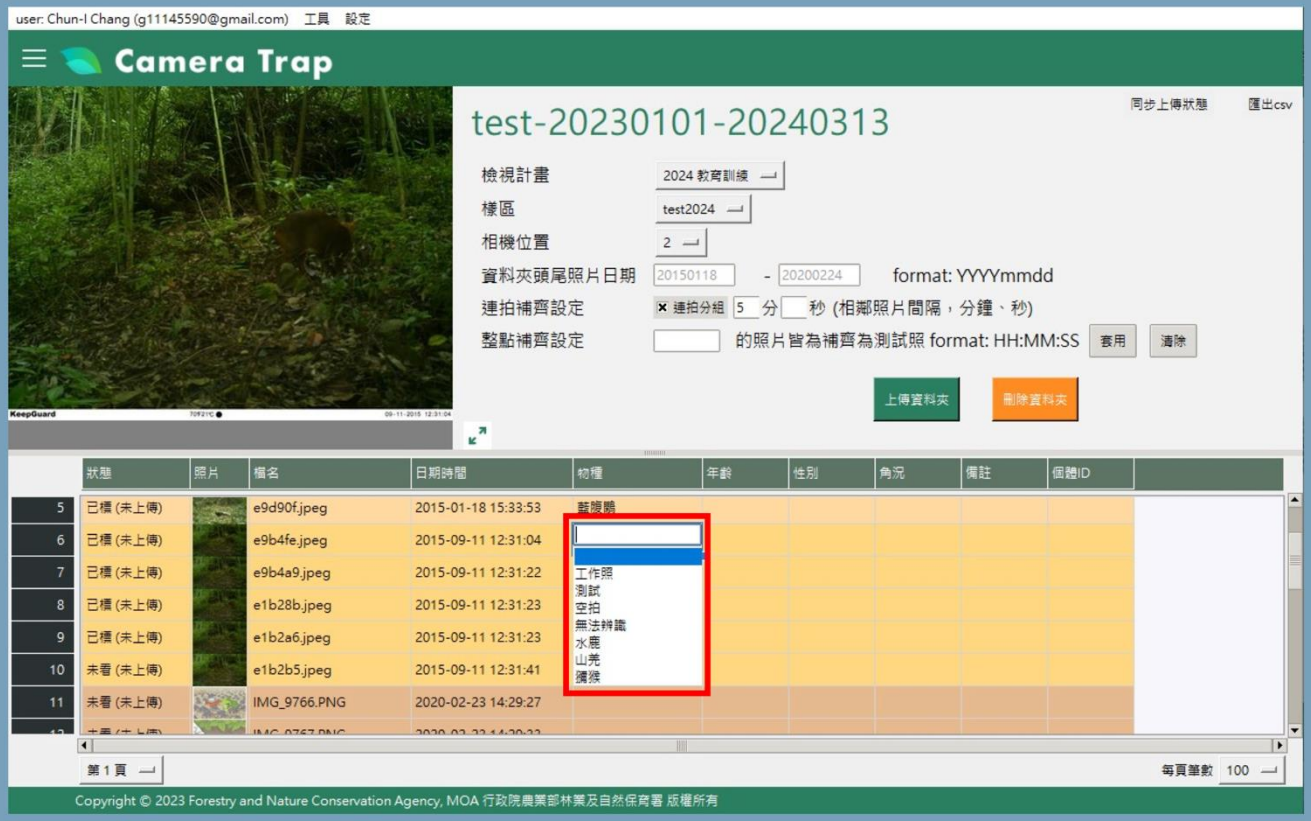
系統自動判斷行程起訖時間



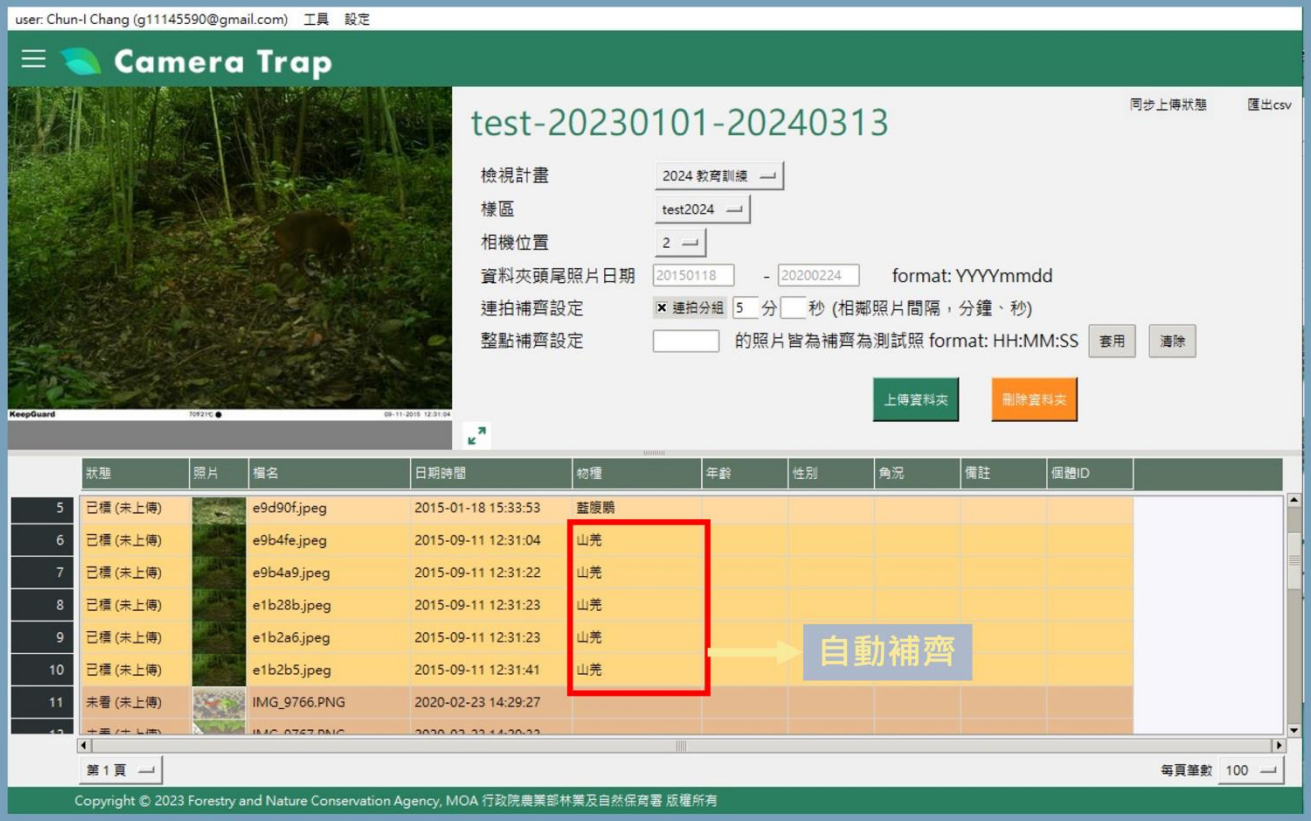
檔案編輯


user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
test-20230101-20240313
同步上傳狀態
匯出csv
檢視計畫
2024 教育訓練
樣區
test2024
相機位置
2
資料夾頭尾照片日期
20150118
-
20200224
format: YYYYmmdd
連拍補齊設定
連拍分組
5
分
秒 (相鄰照片間隔，分鐘、秒)
整點補齊設定
的照片皆為補齊為測試照 format: HH:MM:SS
套用
清除
上傳資料夾
刪除資料夾
填寫欲以多少分鐘、多少秒分組
狀態
照片
檔名
日期時間
物種
年齡
性別
角況
備註
個體ID
1 未看 (未上傳) 0fdd0e.jpeg 2015-01-18 15:33:52
2 未看 (未上傳) 8b3b65.jpeg 2015-01-18 15:33:52
3 未看 (未上傳) e1d77a.jpeg 2015-01-18 15:33:52
4 未看 (未上傳) be9ffb.jpeg 2015-01-18 15:33:53
5 未看 (未上傳) e9d90f.jpeg 2015-01-18 15:33:53
6 未看 (未上傳) e9b4fe.jpeg 2015-09-11 12:31:04
7 未看 (未上傳) e9b4a9.jpeg 2015-09-11 12:31:22
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

檔案編輯

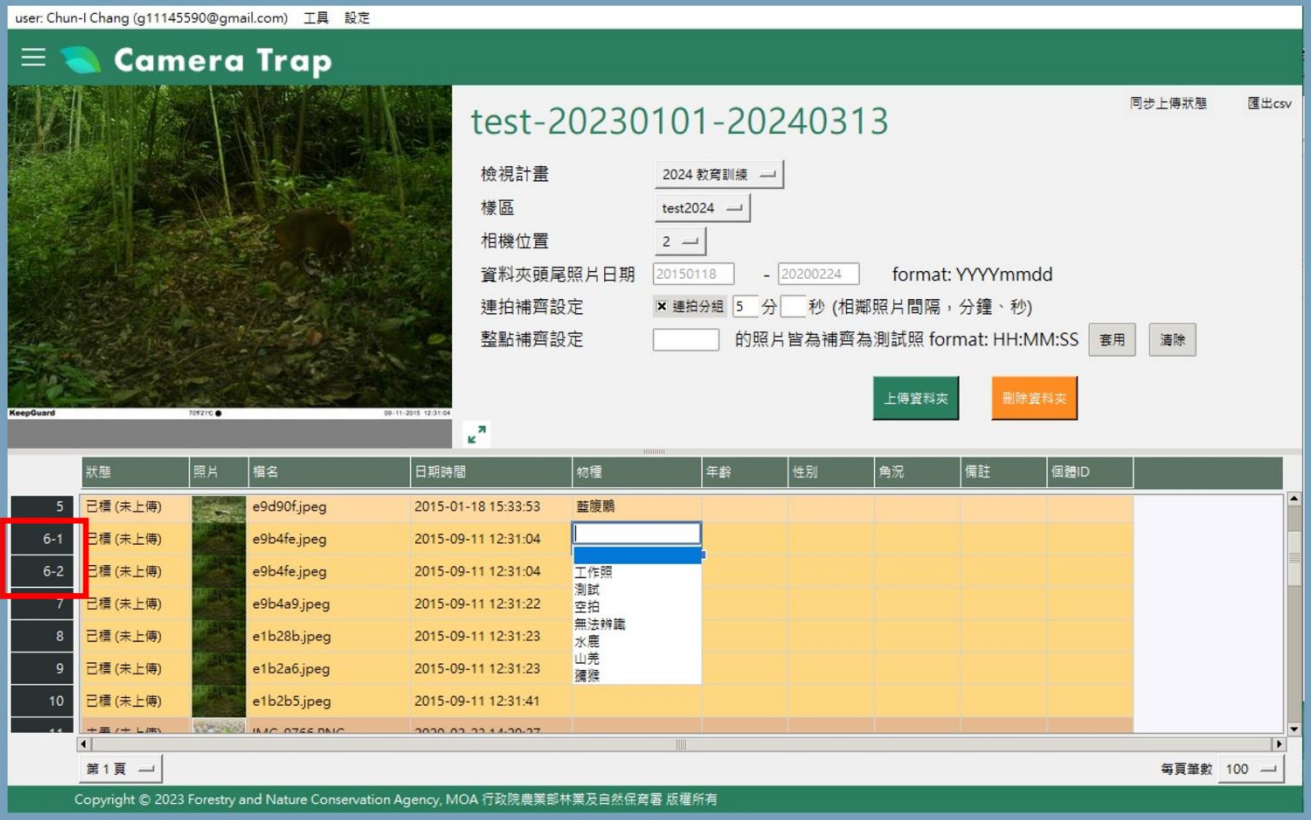

user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
test-20230101-20240313
同步上傳狀態
匯出csv
檢視計畫
2024 教育訓練
樣區
test2024
相機位置
2
資料夾頭尾照片日期
20150118
20200224
format: YYYYmmdd
連拍補齊設定
連拍分組
5
分
秒 (相鄰照片間隔，分鐘、秒)
整點補齊設定
的照片皆為補齊為測試照 format: HH:MM:SS
套用
清除
上傳資料夾
刪除資料夾
狀態
照片
檔名
日期時間
物種
年齡
性別
角況
備註
個體ID
5 已標 (未上傳) e9d90f.jpeg 2015-01-18 15:33:53 黃腹鼬
6 已標 (未上傳) e9b4fe.jpeg 2015-09-11 12:31:04
7 已標 (未上傳) e9b4a9.jpeg 2015-09-11 12:31:22
8 已標 (未上傳) e1b28b.jpeg 2015-09-11 12:31:23
9 已標 (未上傳) e1b2a6.jpeg 2015-09-11 12:31:23
10 未看 (未上傳) e1b2b5.jpeg 2015-09-11 12:31:41
11 未看 (未上傳) IMG_9766.PNG 2020-02-23 14:29:27
工作照
測試
空拍
無法辨識
水鹿
山羌
獼猴
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

檔案編輯

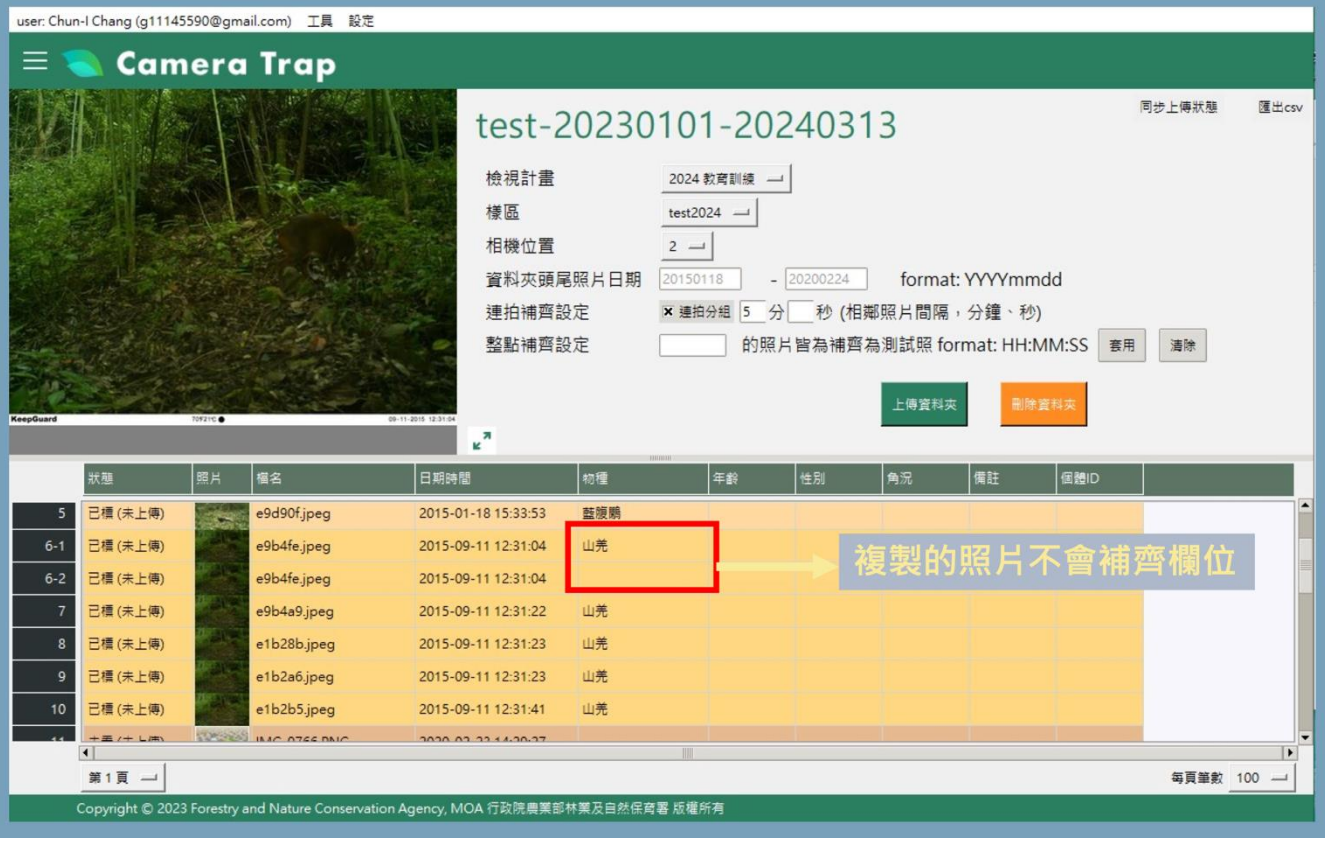

user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
test-20230101-20240313
同步上傳狀態
匯出csv
檢視計畫
2024 教育訓練
樣區
test2024
相機位置
2
資料夾頭尾照片日期
20150118
20200224
format: YYYYmmdd
連拍補齊設定
連拍分組
5
分
秒 (相鄰照片間隔，分鐘、秒)
整點補齊設定
的照片皆為補齊為測試照 format: HH:MM:SS
套用
清除
上傳資料夾
刪除資料夾
狀態
照片
檔名
日期時間
物種
年齡
性別
角況
備註
個體ID
5 已標 (未上傳) e9d90f.jpeg 2015-01-18 15:33:53 藍腹鷴
6 已標 (未上傳) e9b4fe.jpeg 2015-09-11 12:31:04 山羌
7 已標 (未上傳) e9b4a9.jpeg 2015-09-11 12:31:22 山羌
8 已標 (未上傳) e1b28b.jpeg 2015-09-11 12:31:23 山羌
9 已標 (未上傳) e1b2a6.jpeg 2015-09-11 12:31:23 山羌
10 已標 (未上傳) e1b2b5.jpeg 2015-09-11 12:31:41 山羌
11 未審 (未上傳) IMG_9766.PNG 2020-02-23 14:29:27
自動補齊
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

檔案編輯

如連拍分組遇到有複製照片的狀況

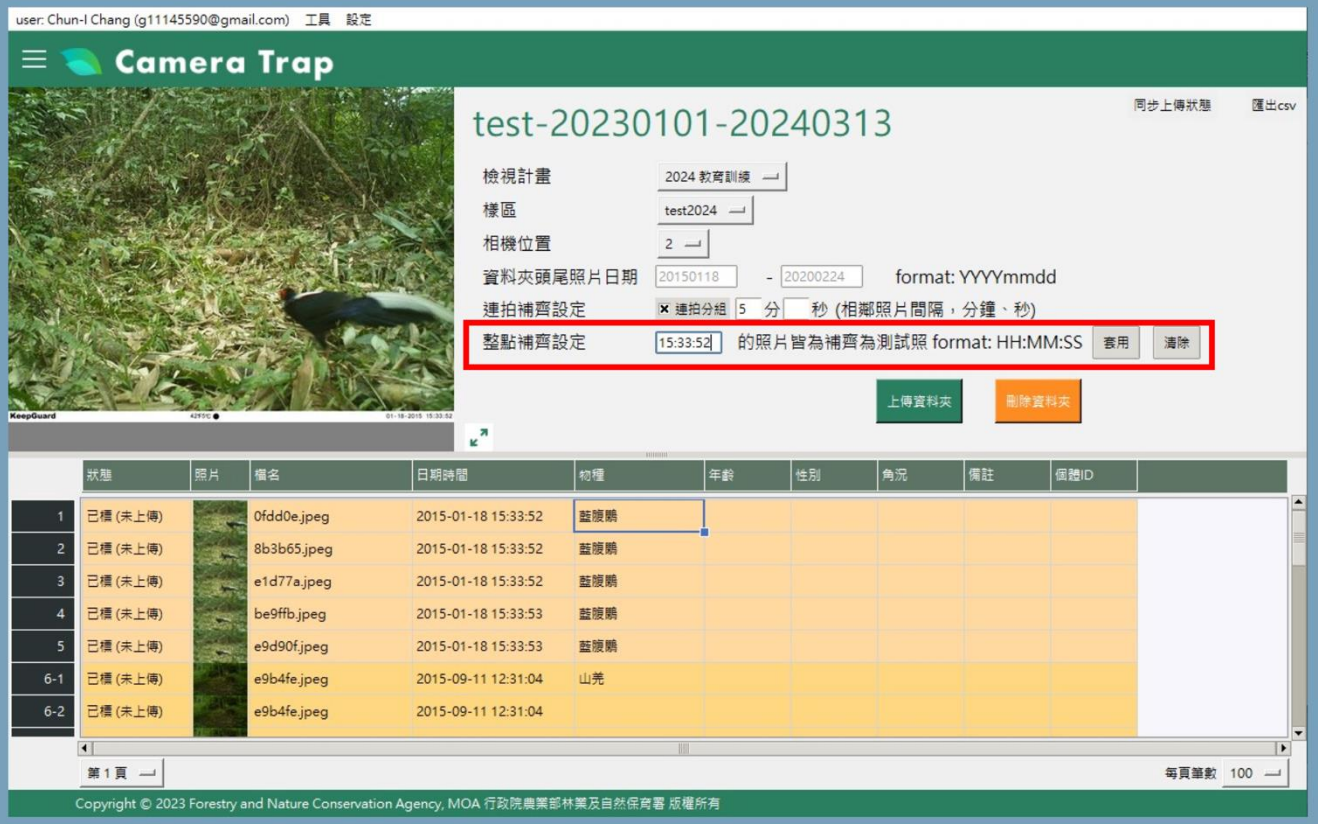


檔案編輯


user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
test-20230101-20240313
同步上傳狀態
匯出csv
檢視計畫 2024 教育訓練
樣區 test2024
相機位置 2
資料夾頭尾照片日期 20150118 - 20200224 format: YYYYmmdd
連拍補齊設定 連拍分組 5 分 秒 (相鄰照片間隔，分鐘、秒)
整點補齊設定 的照片皆為補齊為測試照 format: HH:MM:SS 套用 清除
上傳資料夾
刪除資料夾
狀態 照片 檔名 日期時間 物種 年齡 性別 角況 備註 個體ID
5 已標 (未上傳) e9d90f.jpeg 2015-01-18 15:33:53 藍腹鷴
6-1 已標 (未上傳) e9b4fe.jpeg 2015-09-11 12:31:04 山羌
6-2 已標 (未上傳) e9b4fe.jpeg 2015-09-11 12:31:04
7 已標 (未上傳) e9b4a9.jpeg 2015-09-11 12:31:22 山羌
8 已標 (未上傳) e1b28b.jpeg 2015-09-11 12:31:23 山羌
9 已標 (未上傳) e1b2a6.jpeg 2015-09-11 12:31:23 山羌
10 已標 (未上傳) e1b2b5.jpeg 2015-09-11 12:31:41 山羌
複製的照片不會補齊欄位
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

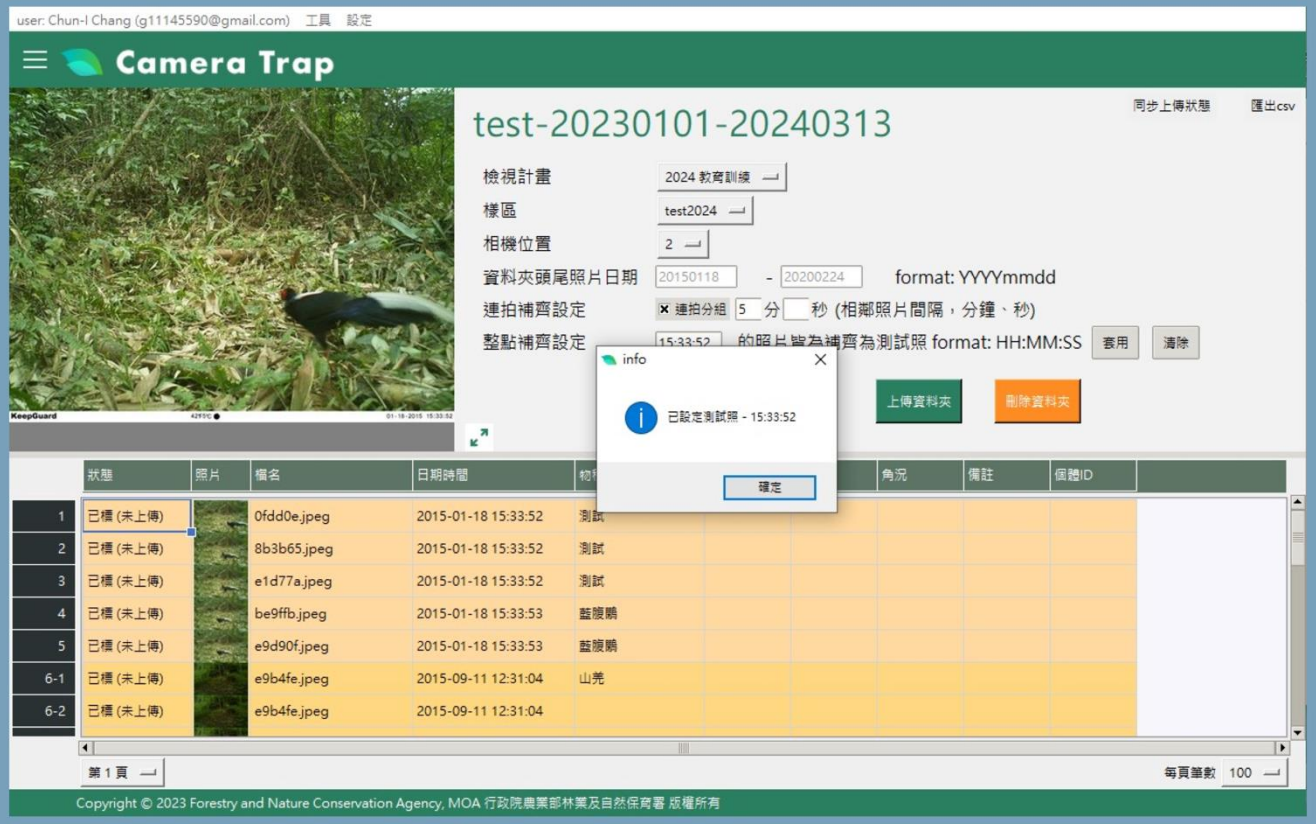
檔案編輯

整點自動標註測試照



檔案編輯

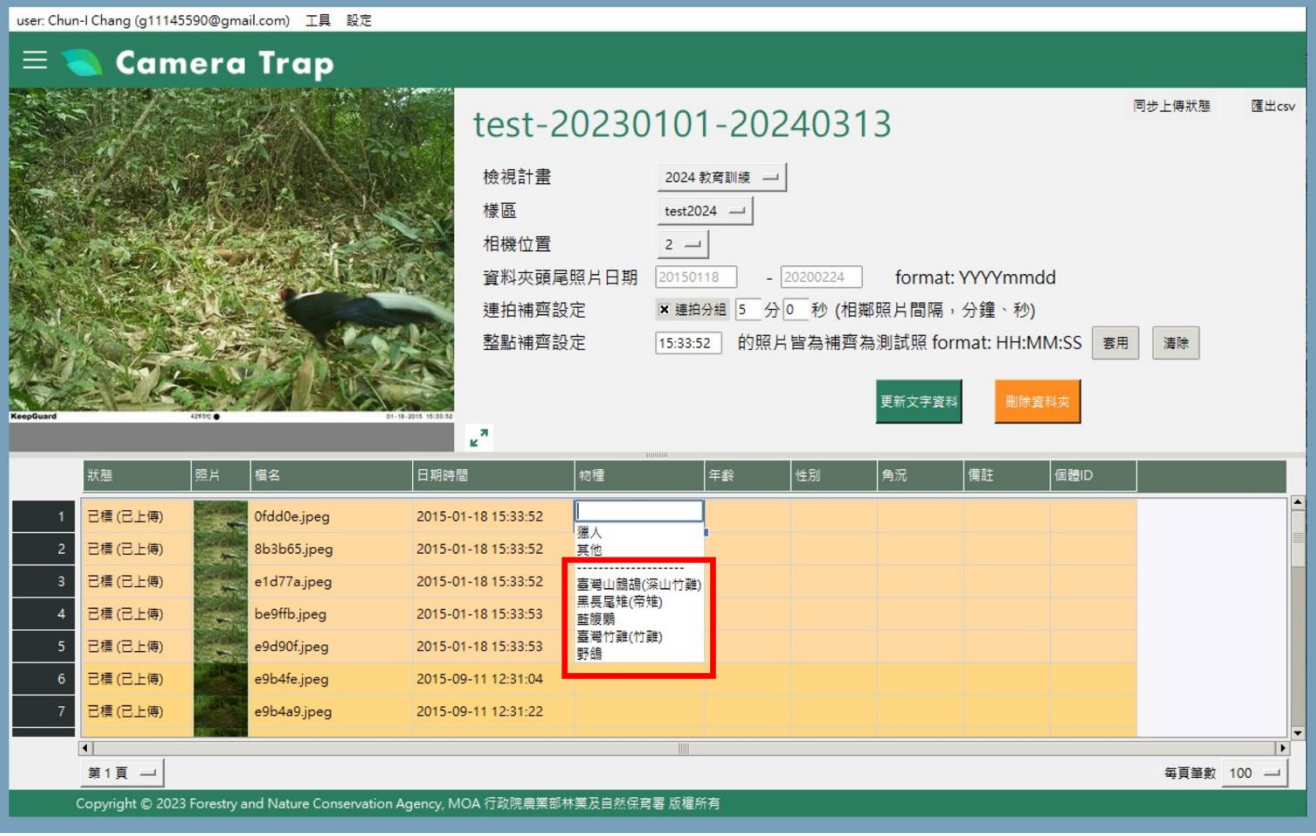
整點自動標註測試照



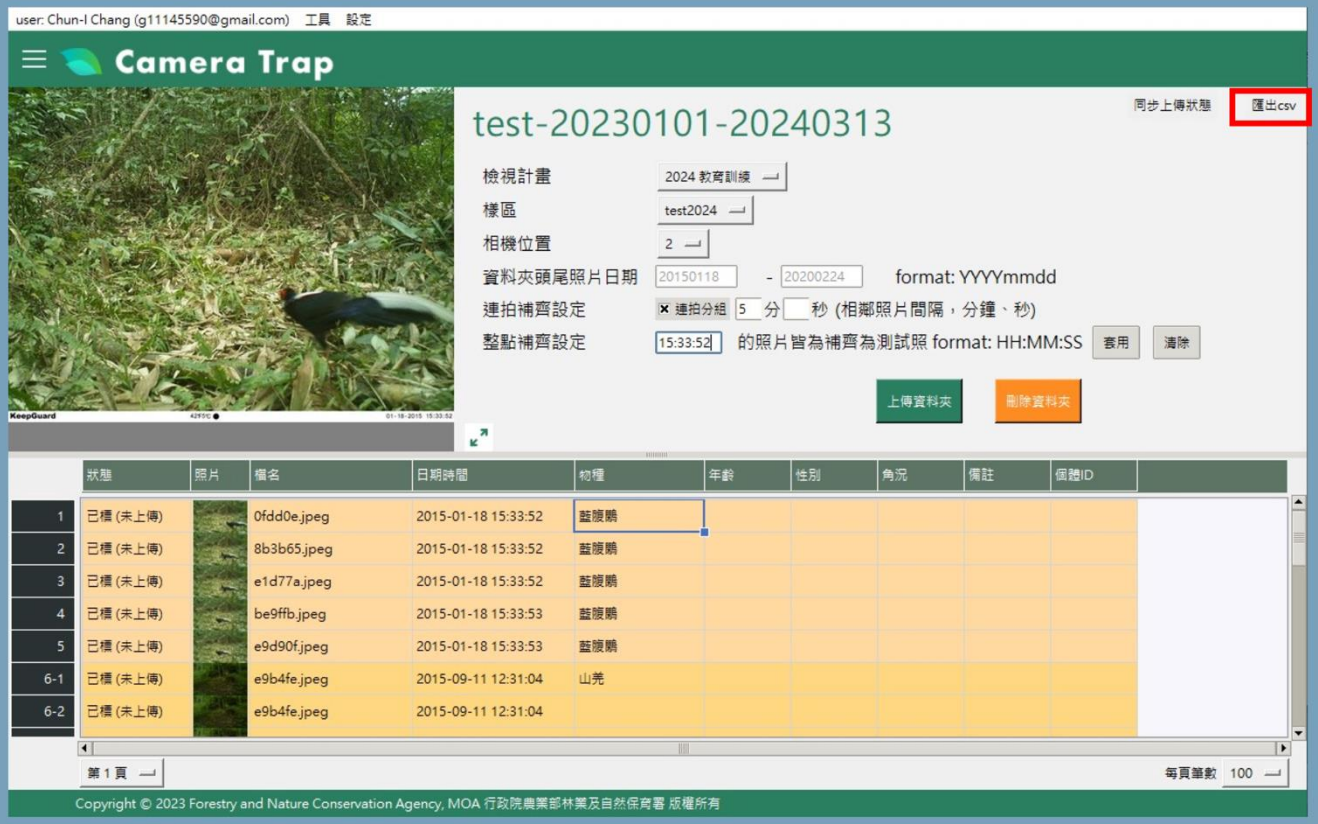
52

檔案編輯

原鳥類清單內容併入物種下拉選單選項



匯出檔案


user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
test-20230101-20240313
同步上傳狀態
匯出csv
檢視計畫 2024 教育訓練
樣區 test2024
相機位置 2
資料夾頭尾照片日期 20150118 - 20200224 format: YYYYmmdd
連拍補齊設定 連拍分組 5 分 秒 (相鄰照片間隔，分鐘、秒)
整點補齊設定 15:33:52 的照片皆為補齊為測試照 format: HH:MM:SS 套用 清除
上傳資料夾
刪除資料夾
狀態 照片 檔名 日期時間 物種 年齡 性別 角況 備註 個體ID
1 已標 (未上傳) 0fdd0e.jpeg 2015-01-18 15:33:52 藍腹鷴
2 已標 (未上傳) 8b3b65.jpeg 2015-01-18 15:33:52 藍腹鷴
3 已標 (未上傳) e1d77a.jpeg 2015-01-18 15:33:52 藍腹鷴
4 已標 (未上傳) be9ffb.jpeg 2015-01-18 15:33:53 藍腹鷴
5 已標 (未上傳) e9d90f.jpeg 2015-01-18 15:33:53 藍腹鷴
6-1 已標 (未上傳) e9b4fe.jpeg 2015-09-11 12:31:04 山羌
6-2 已標 (未上傳) e9b4fe.jpeg 2015-09-11 12:31:04
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

檔案上傳

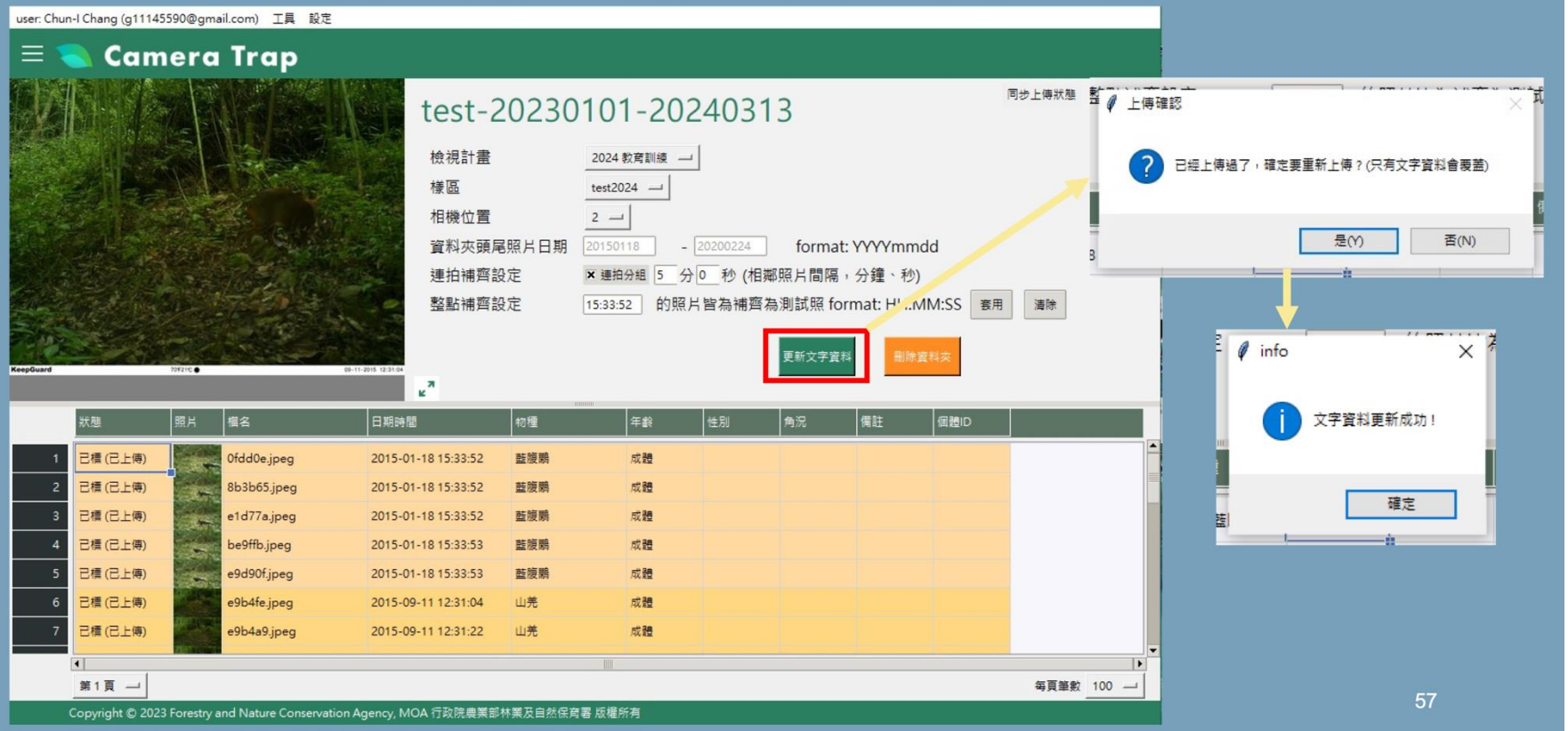
test-20230101-20240313
同步上傳狀態
匯出csv
檢視計畫
2024 教育訓練
樣區
test2024
相機位置
2
資料夾頭尾照片日期
20150118
-
20200224
format: YYYYmmdd
連拍補齊設定
連拍分組
5
分
秒 (相鄰照片間隔，分鐘、秒)
整點補齊設定
15:33:52
的照片皆為補齊為測試照 format: HH:MM:SS
套用
清除
上傳資料夾
刪除資料夾
確認計畫
請確認計畫、樣區、相機位置是否無誤？
確定
取消
注意
尚有照片未填寫物種，順序編號: 1, 3
確定
取消
serv...
上傳文字處理中...
關閉

55

檔案上傳

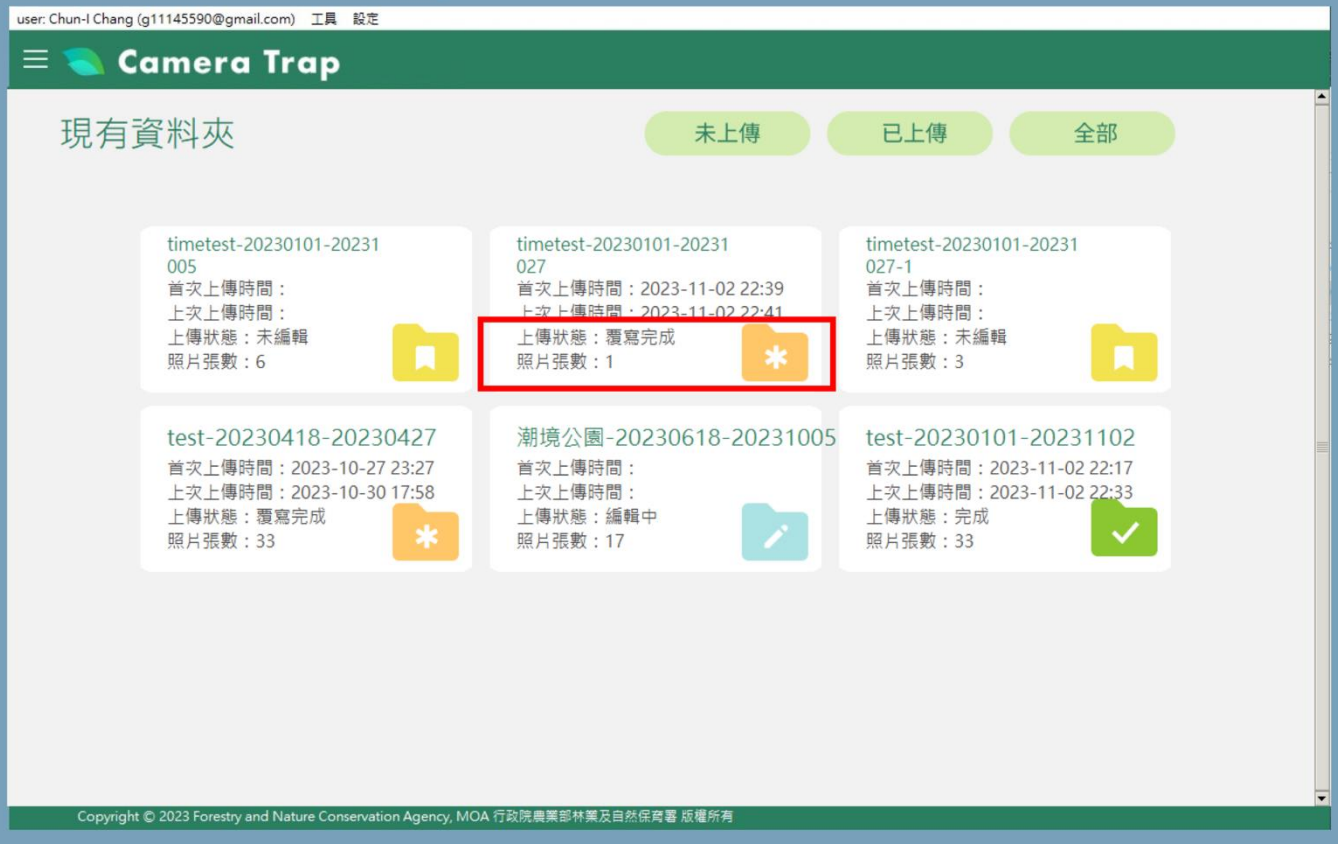
user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
上傳進度
test-20230418-20
資料夾上傳完畢
(33/33)
test-20230101-20231102
資料夾上傳中...
84.85%
(28/33)
暫停上傳
info
資料夾 test-20230101-20231102: 上傳成功
確定
同時間僅會上傳一資料夾內容，
其餘資料夾將依序上傳
開始上傳後所做的任何編輯動作都不會跟著上傳，
即使是還在等待排程上傳的照片也是一樣
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

檔案上傳

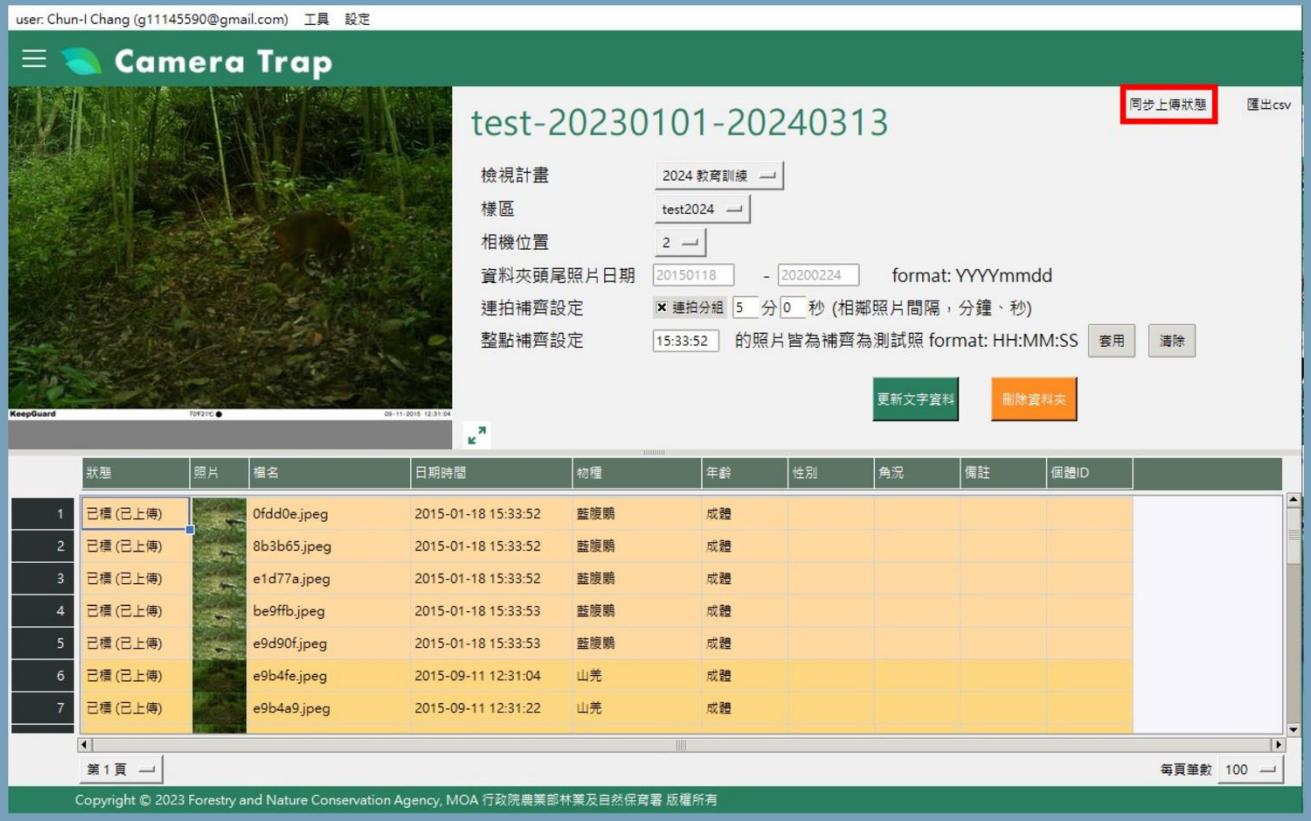

user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
test-20230101-20240313
同步上傳狀態
檢視計畫 2024 教育訓練
樣區 test2024
相機位置 2
資料夾頭尾照片日期 20150118 - 20200224 format: YYYYmmdd
連拍補齊設定 連拍分組 5 分 0 秒 (相鄰照片間隔，分鐘、秒)
整點補齊設定 15:33:52 的照片皆為補齊為測試照 format: HH:MM:SS 套用 清除
更新文字資料
刪除資料夾
狀態 照片 檔名 日期時間 物種 年齡 性別 角況 備註 個體ID
1 已標 (已上傳) 0fdd0e.jpeg 2015-01-18 15:33:52 藍腹鷴 成體
2 已標 (已上傳) 8b3b65.jpeg 2015-01-18 15:33:52 藍腹鷴 成體
3 已標 (已上傳) e1d77a.jpeg 2015-01-18 15:33:52 藍腹鷴 成體
4 已標 (已上傳) be9ffb.jpeg 2015-01-18 15:33:53 藍腹鷴 成體
5 已標 (已上傳) e9d90f.jpeg 2015-01-18 15:33:53 藍腹鷴 成體
6 已標 (已上傳) e9b4fe.jpeg 2015-09-11 12:31:04 山羌 成體
7 已標 (已上傳) e9b4a9.jpeg 2015-09-11 12:31:22 山羌 成體
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有
上傳確認
已經上傳過了，確定要重新上傳？(只有文字資料會覆蓋)
是(Y)
否(N)
info
文字資料更新成功！
確定

57

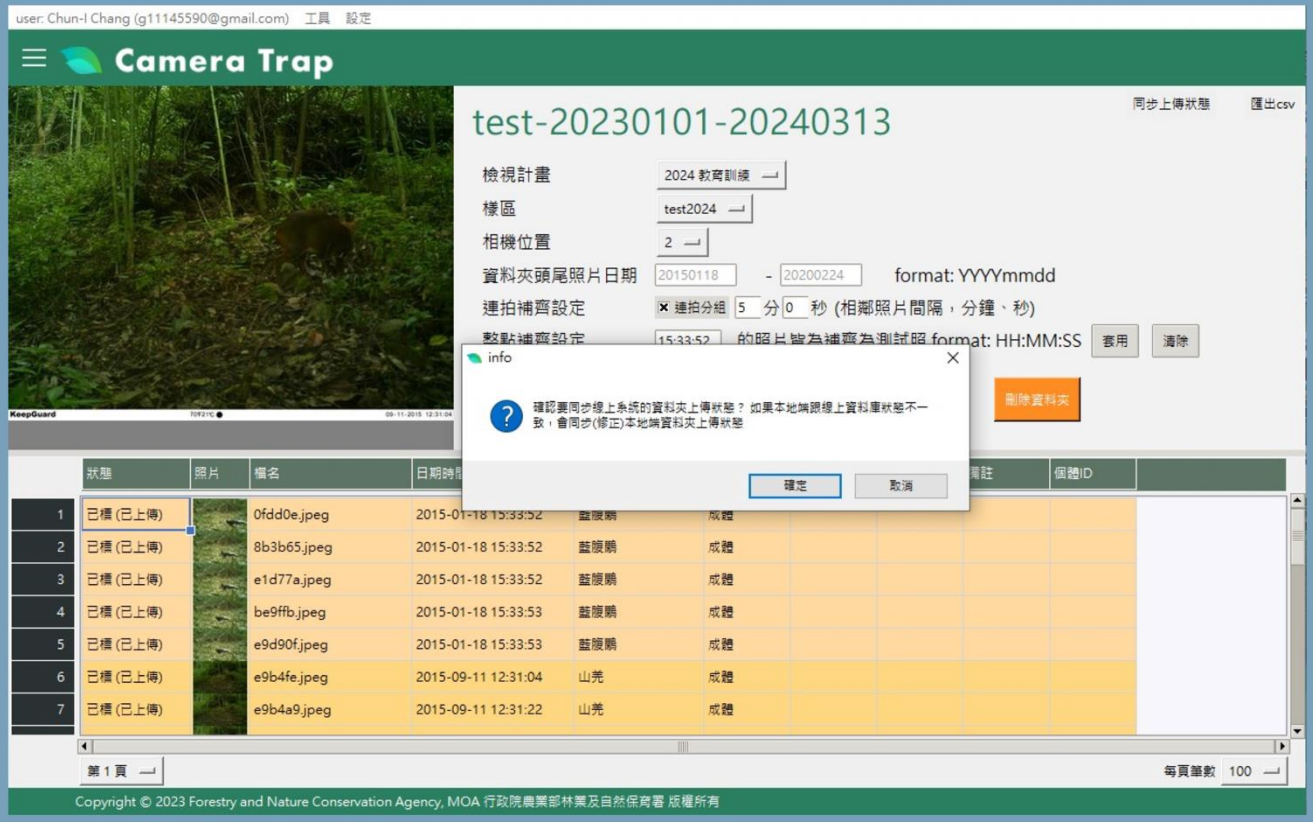
檔案上傳


user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
現有資料夾
未上傳
已上傳
全部
timetest-20230101-20231005
首次上傳時間：
上次上傳時間：
上傳狀態：未編輯
照片張數：6
timetest-20230101-20231027
首次上傳時間：2023-11-02 22:39
上傳狀態：覆寫完成
照片張數：1
timetest-20230101-20231027-1
首次上傳時間：
上次上傳時間：
上傳狀態：未編輯
照片張數：3
test-20230418-20230427
首次上傳時間：2023-10-27 23:27
上次上傳時間：2023-10-30 17:58
上傳狀態：覆寫完成
照片張數：33
潮境公園-20230618-20231005
首次上傳時間：
上次上傳時間：
上傳狀態：編輯中
照片張數：17
test-20230101-20231102
首次上傳時間：2023-11-02 22:17
上次上傳時間：2023-11-02 22:33
上傳狀態：完成
照片張數：33
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

檔案上傳


user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
test-20230101-20240313
同步上傳狀態
匯出csv
檢視計畫 2024 教育訓練
樣區 test2024
相機位置 2
資料夾頭尾照片日期 20150118 - 20200224 format: YYYYmmdd
連拍補齊設定 連拍分組 5 分 0 秒 (相鄰照片間隔，分鐘、秒)
整點補齊設定 15:33:52 的照片皆為補齊為測試照 format: HH:MM:SS 套用 清除
更新文字資料
刪除資料夾
狀態 照片 檔名 日期時間 物種 年齡 性別 角況 備註 個體ID
1 已標 (已上傳) 0fdd0e.jpeg 2015-01-18 15:33:52 藍腹鷴 成體
2 已標 (已上傳) 8b3b65.jpeg 2015-01-18 15:33:52 藍腹鷴 成體
3 已標 (已上傳) e1d77a.jpeg 2015-01-18 15:33:52 藍腹鷴 成體
4 已標 (已上傳) be9ffb.jpeg 2015-01-18 15:33:53 藍腹鷴 成體
5 已標 (已上傳) e9d90f.jpeg 2015-01-18 15:33:53 藍腹鷴 成體
6 已標 (已上傳) e9b4fe.jpeg 2015-09-11 12:31:04 山羌 成體
7 已標 (已上傳) e9b4a9.jpeg 2015-09-11 12:31:22 山羌 成體
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

檔案上傳


user: Chun-I Chang (g11145590@gmail.com) 工具 設定
Camera Trap
test-20230101-20240313
同步上傳狀態
匯出csv
檢視計畫
2024 教育訓練
樣區
test2024
相機位置
2
資料夾頭尾照片日期
20150118
20200224
format: YYYYmmdd
連拍補齊設定
連拍分組
5 分 0 秒 (相鄰照片間隔，分鐘、秒)
套用
清除
刪除資料夾
info
確認要同步線上系統的資料夾上傳狀態？ 如果本地端跟線上資料庫狀態不一致，會同步(修正)本地端資料夾上傳狀態
確定
取消
狀態
照片
檔名
日期時間
備註
個體ID
1 已標 (已上傳) 0fdd0e.jpeg 2015-01-18 15:33:52 藍腹鷴 成體
2 已標 (已上傳) 8b3b65.jpeg 2015-01-18 15:33:52 藍腹鷴 成體
3 已標 (已上傳) e1d77a.jpeg 2015-01-18 15:33:52 藍腹鷴 成體
4 已標 (已上傳) be9ffb.jpeg 2015-01-18 15:33:53 藍腹鷴 成體
5 已標 (已上傳) e9d90f.jpeg 2015-01-18 15:33:53 藍腹鷴 成體
6 已標 (已上傳) e9b4fe.jpeg 2015-09-11 12:31:04 山羌 成體
7 已標 (已上傳) e9b4a9.jpeg 2015-09-11 12:31:22 山羌 成體
第 1 頁
每頁筆數 100
Copyright © 2023 Forestry and Nature Conservation Agency, MOA 行政院農業部林業及自然保育署 版權所有

番外篇

操作小技巧教學

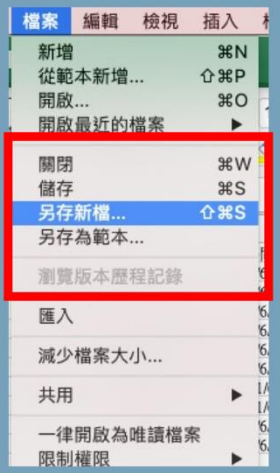
Excel轉存CSV

如何做呢？

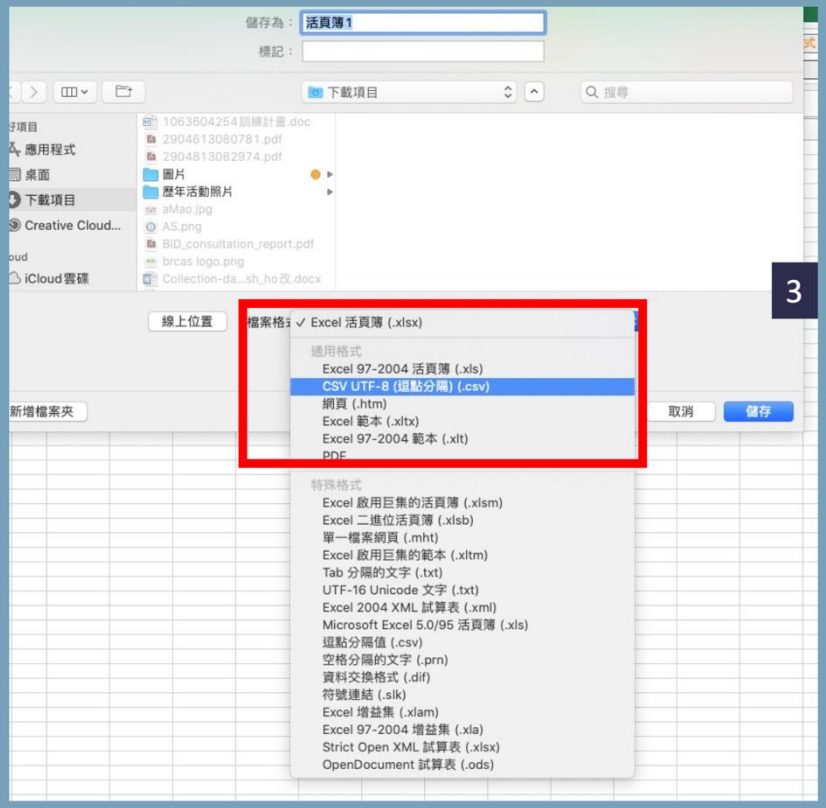
62

1 開啟要轉存的excel檔案

2



點選「檔案」→另存新檔



3 選好要儲存的位置，在檔案格式選擇 CSV UTF-8

然後儲存即可～

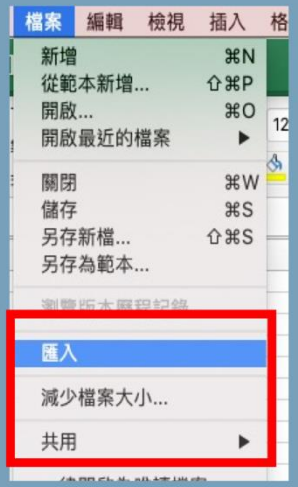
63

CSV匯入Excel

如何做呢？

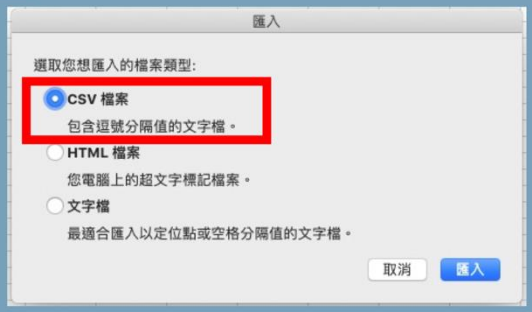
64

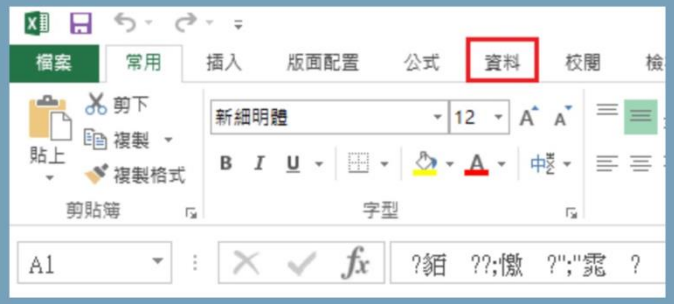
1 開啟excel



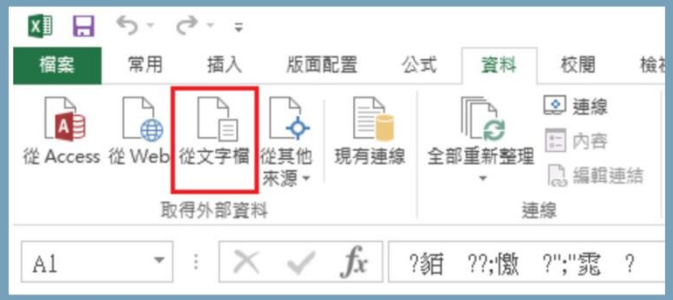
2 選擇匯入

3 選擇 CSV 檔案

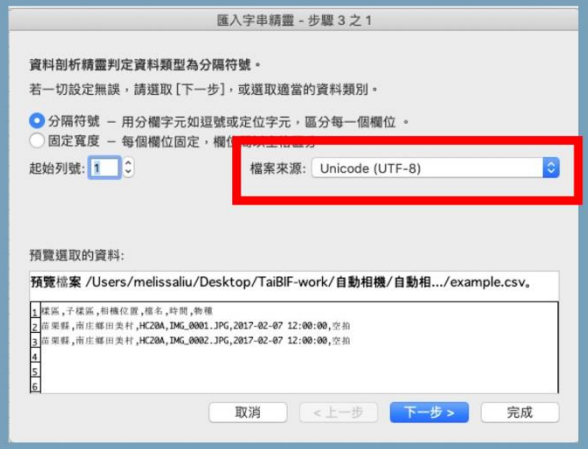




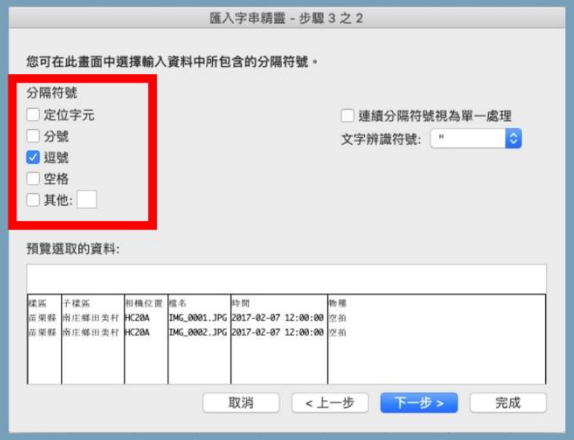
2 選擇「資料」功能



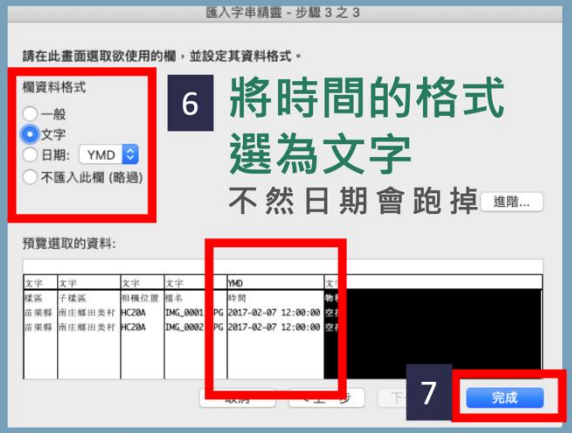
3 點選「從文字檔」，選擇 CSV 檔匯入



4 確認檔案來源為UTF-8



5 選擇逗號做為分隔符號



上傳資料檢視

跟著一步一步做

67

計畫選取

計畫總覽-我的計畫

68

計 畫 首 頁

點選查看影像按鍵

上 傳 結 果

找到您剛剛上傳的資料
完成！

70

附錄 6、線上系統引導說明教學文件

資 料 流 程

2

計畫管理
系統網頁
權限設定
相機位置
由計畫總管理人
&
計畫承辦人設定
安裝上傳程式
安裝檔
下載
匯入檔案
上傳程式
開啟檔案
資料編輯
物種辨識
連拍補齊
複製列...
檔案上傳
計畫樣區選擇
上傳狀態提示
上傳進度條
系統登入
系統網頁
角色分流
檢視檔案
系統網頁
確認上傳檔案
3

計畫總管理人：
可管理、編輯及瀏覽所屬單位計畫及瀏覽所有公開計畫

計畫承辦人：
可管理、編輯及瀏覽個別承辦計畫及瀏覽所有公開計畫

資料上傳者：
可瀏覽所有公開計畫及個別所屬計畫，但沒有編輯權限

4

線上系統功能說明

5

首 頁

https://camera-trap.tw

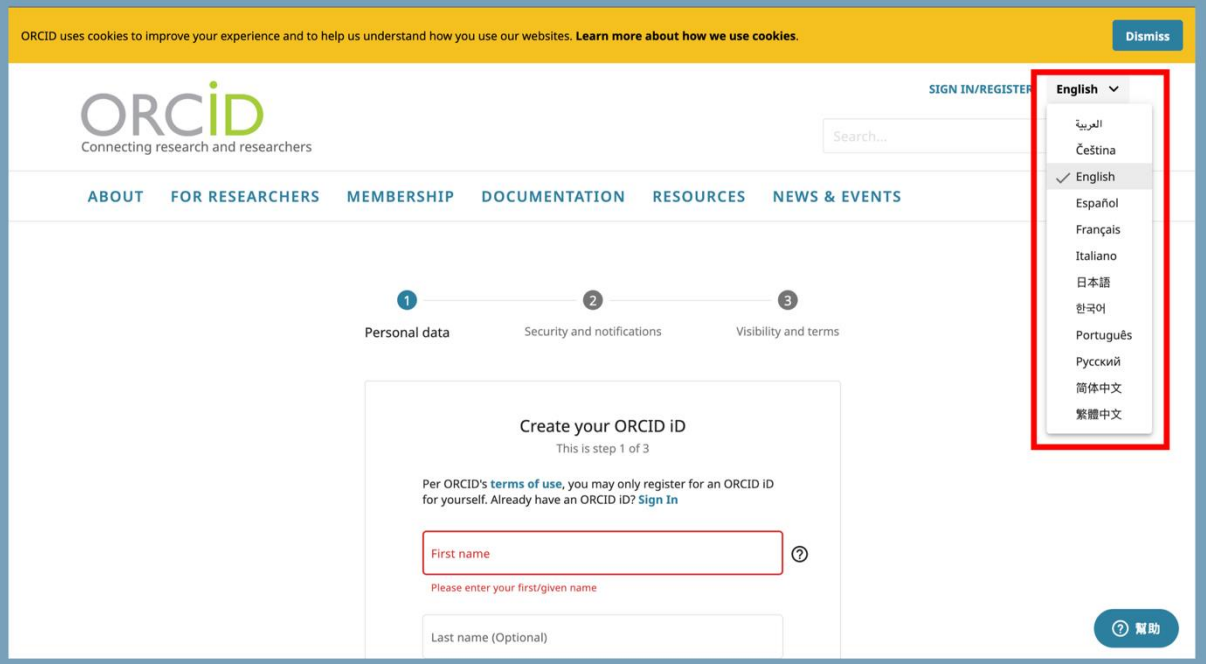
申 請 帳 號

ORCID
Connecting Research and Researchers

https://orcid.org/signin

7

註冊ORCID


ORCID uses cookies to improve your experience and to help us understand how you use our websites. Learn more about how we use cookies.
Dismiss
SIGN IN/REGISTER
English
ORCID
Connecting research and researchers
Search...
ABOUT
FOR RESEARCHERS
MEMBERSHIP
DOCUMENTATION
RESOURCES
NEWS & EVENTS
العربية
Čeština
English
Español
Français
Italiano
日本語
한국어
Português
Русский
简体中文
繁體中文
1 Personal data
2 Security and notifications
3 Visibility and terms
Create your ORCID iD
This is step 1 of 3
Per ORCID's terms of use, you may only register for an ORCID iD for yourself. Already have an ORCID iD? Sign In
First name
Please enter your first/given name
Last name (Optional)
幫助

8

註冊ORCID

創建您的ORCID iD
步驟 5 之 3 - 目前就業狀態
Adding a current employment affiliation helps distinguis
other researchers with a similar name.
目前就業情況
機構
輸入貴組織的名稱
部門 （選擇性）
學校、大專院校或科系
下一步
跳過此步驟，不新增附屬機構
前一步

9

登 入 系 統

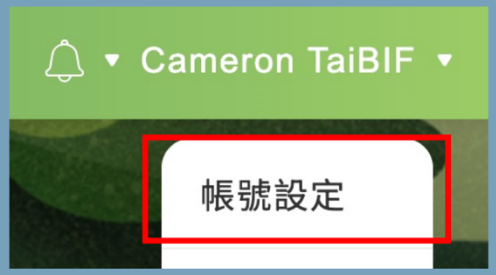
https://camera-trap.tw

10

設 定 資 料

編輯使用者名稱與個人資訊

填寫完整才能被搜尋到與下載資料



11

計畫總覽

我的計畫：
非公開
僅呈現自身有被加入成員的計畫

12

計畫首頁

林業署哺乳動物監測網
已辨識物種
樣區
全部
起始日期
YYYY-MM-DD
結束日期
YYYY-MM-DD
清除條件
委辦單位
計畫編號 112農科-7.2.6-務-e1
計畫主持人 翁國精
計畫時間 2015-09-01 至 2025-12-31
資料下載
查看影像
相機樣點運作及缺失比例
可互動視覺化圖表
Leaflet | © OpenStreetMap contributors
在地圖顯示林班地範圍
樣區 相機位置
全部樣區已辨識物種71種
最後更新時間：2023-11-02
山羌 45.88 %
空拍 20.35 %
測試 7.25 %
獼猴 6.39 %
工作照 4.36 %
水鹿 2.58 %
山羊 2.21 %
鼠或跑形目 1.63 %
其他物種 9.36 %
全部樣區已上傳照片1537844張
200k
150k
100k
50k
0
照片張數
2010-Jan
2015-Jan
2020-Jan

查看影像

樣區 / 相機位置
全部
TaiBIF測試
南投分署
嘉義分署
宜蘭分署
屏東分署
新竹分署
臺中分署
臺東分署
花蓮分署
雪霸國家公園
資料夾名稱
海拔
起（公尺）
11
訖（公尺）
3598
縣市
請選擇
保護留區
請選擇
拍攝時間
---:--:--
---:--:--
拍攝日期
2006-12-31
2024-05-03
媒體類型
請選擇
備註
請選擇
返回
林業署哺乳動物監測網
下載篩選資料
篩選條件
篩選
清除
物種
全部
(18647)
人 (11590)
大赤鼯鼠 (77)
大冠鷲 (159)
大彎嘴 (9)
小黃鼠狼 (106)
小彎嘴 (188)
山羊 (58459)
山羌 (1223759)
山鷸 (39)
工作照 (123589)
水鹿 (97421)
台灣山鷓鴣 (6657)
台灣白喉噪眉 (18)
台灣竹雞 (762)
台灣棕噪眉 (212)
台灣紫嘯鶇 (386)
台灣噪眉 (261)
台灣藍鵲 (488)
巨嘴鴉 (15)
巨嘴鴉(烏鴉、大嘴烏鴉) (3)
白氏/虎斑地鶇 (108)
白尾鴝 (387)
白眉鶇 (9)
白面鼯鼠 (114)
白腰鵲鴝 (315)
白腹鶇 (460)
白鼻心 (12094)
白頭鶇 (11)
石虎 (147)
樣區
相機位置
檔名
日期時間
物種
年齡
性別
角況
個體ID
備註
影像
臺中分署 DS-LTM M-024 RCNX2219.JPG 2024-05-03 07:52:55 工作照
臺中分署 DS-LTM M-024 RCNX2218.JPG 2024-05-03 07:52:54 工作照
臺中分署 DS-LTM M-024 RCNX2217.JPG 2024-05-03 07:52:52 工作照
臺中分署 DS-LTM M-024 RCNX2216.JPG 2024-05-03 07:52:51 工作照
臺中分署 DS-LTM M-024 RCNX2215.JPG 2024-05-03 07:52:50 工作照
臺中分署 DS-LTM M-024 RCNX2214.JPG 2024-05-03 07:52:49 工作照
臺中分署 DS-LTM M-024 RCNX2213.JPG 2024-05-03 07:52:47 工作照
臺中分署 DS-LTM M-024 RCNX2212.JPG 2024-05-03 07:52:46 工作照
臺中分署 DS-LTM M-024 RCNX2211.JPG 2024-05-03 07:52:44 工作照
臺中分署 DS-LTM M-024 RCNX2210.JPG 2024-05-03 07:52:43 工作照
正在檢視第 1 至 10 筆，總共 2648582 筆 每頁顯示 10 筆
1 上一頁 1 2 3 下一頁 264859

查看影像

返回
林業署哺乳動物監測網
下載篩選資料
篩選條件
篩選
清除
物種
全部
(18647)
人 (11590)
樣區
相機位置
檔名
日期時間
物種
年齡
性別
角況
個體ID
備註
影像
臺中分署
DS-LTM M-024
RCNX2219.JPG
2024-05-03 07:52:55
工作照
檔名
RCNX0023.JPG
日期
2023-08-19
時間
下午12:57:37
計畫
2024 教育訓練
樣區
test2024
相機位置
0429
物種
測試
年齡
性別
角況
個體ID
備註
下載影像
白鼻心 (12094)
白頭鶇 (11)
石虎 (147)
正在檢視第 1 至 10 筆，總共 2648582 筆
每頁顯示
10
筆
1
上一頁
1
2
3
下一頁
264859

計畫首頁

林業署哺乳動物監測網
已辨識物種
樣區
全部
起始日期
YYYY-MM-DD
結束日期
YYYY-MM-DD
清除條件
委辦單位
計畫編號 112農科-7.2.6-務-e1
計畫主持人 翁國精
計畫時間 2015-09-01 至 2025-12-31
資料下載
查看影像
相機樣點運作及缺失比例
Leaflet | © OpenStreetMap contributors
在地圖顯示林班地範圍
樣區 相機位置
全部樣區已辨識物種71種
最後更新時間：2023-11-02
山羌 45.88 %
空拍 20.35 %
測試 7.25 %
獼猴 6.39 %
工作照 4.36 %
水鹿 2.58 %
山羊 2.21 %
鼠或跑形目 1.63 %
其他物種 9.36 %
全部樣區已上傳照片1537844張
200k
150k
100k
50k
0
照片張數
2010-Jan
2015-Jan
2020-Jan

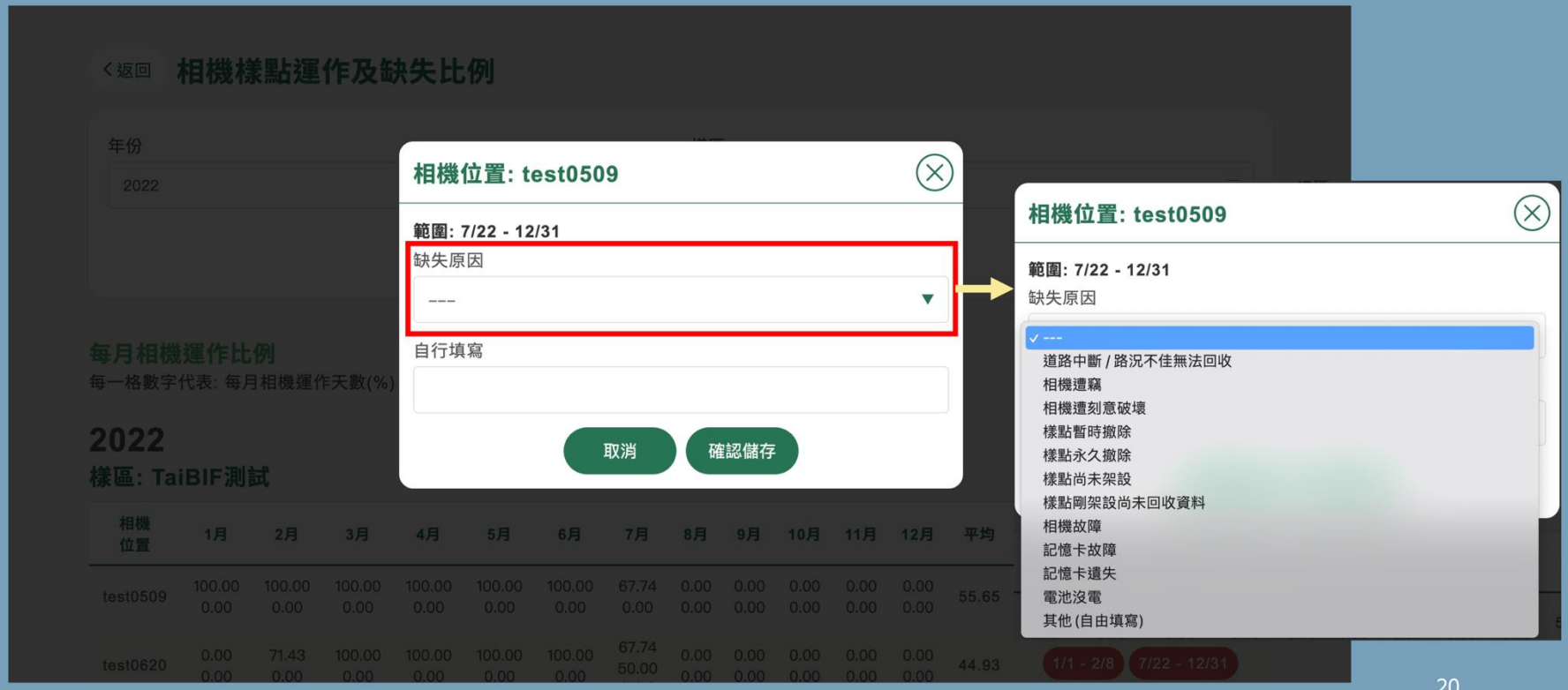
相機樣點運作及缺失比例

17

相機樣點運作及缺失比例

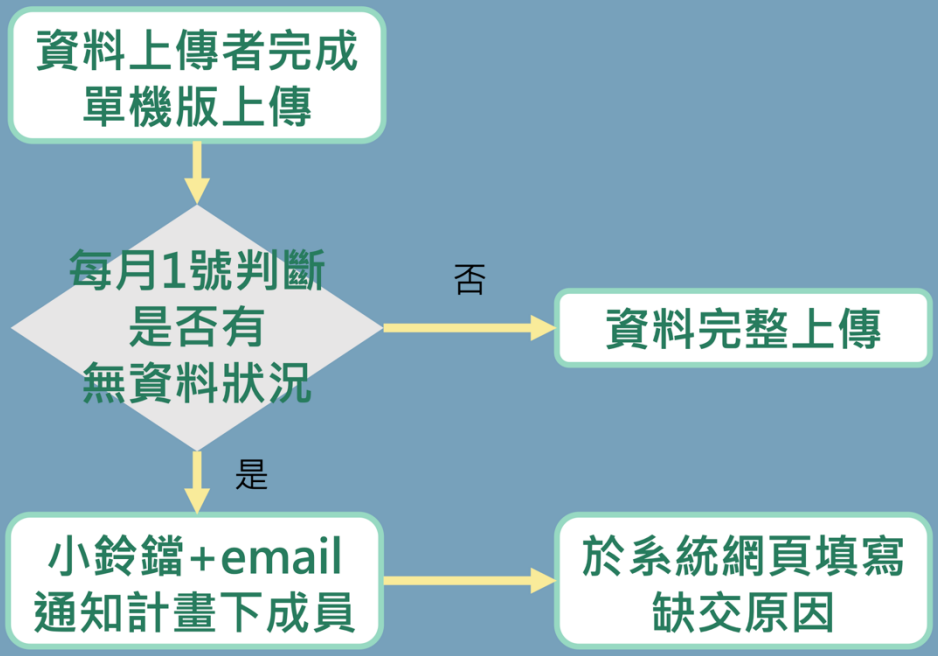
相機樣點運作及缺失比例

相機樣點運作及缺失比例



20

填寫缺失原因流程

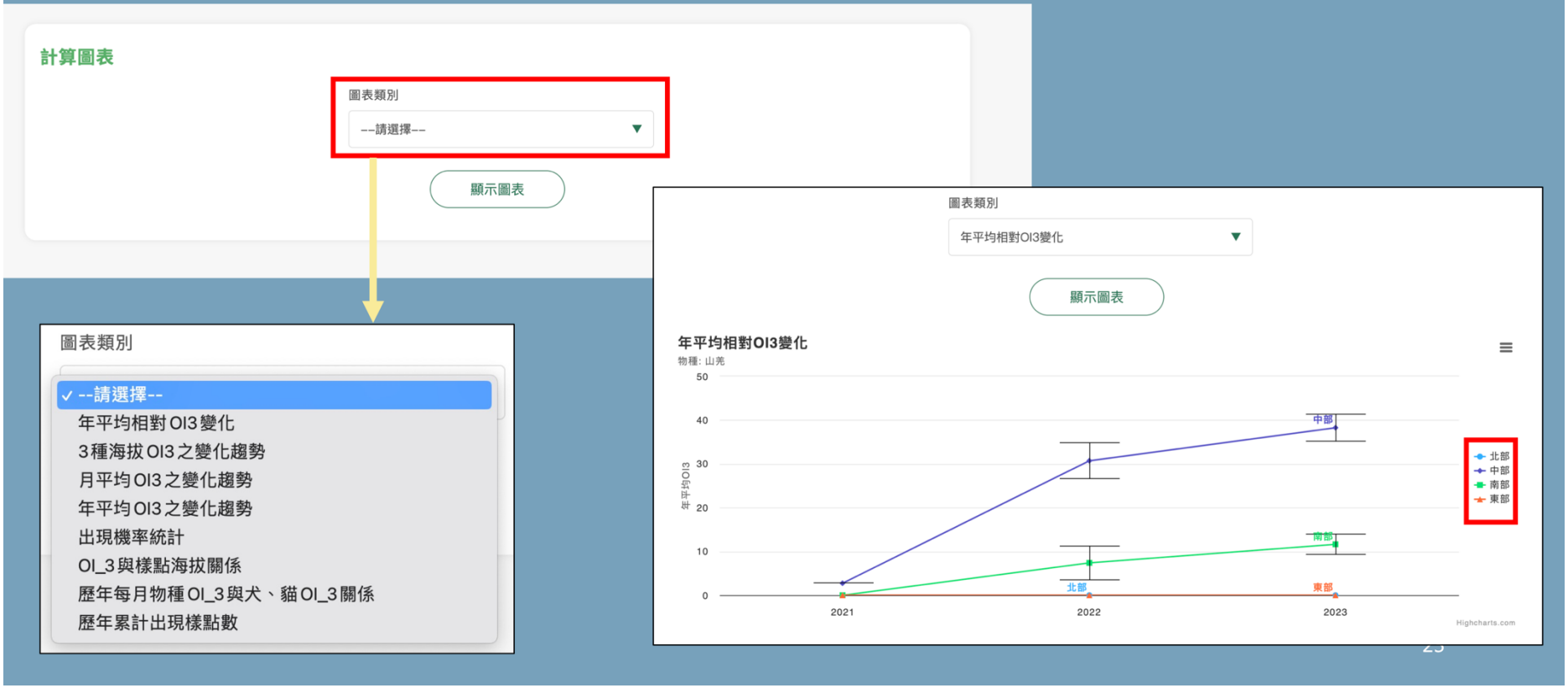

資料上傳者完成
單機版上傳
每月1號判斷
是否有
無資料狀況
否
資料完整上傳
是
小鈴鐺+email
通知計畫下成員
於系統網頁填寫
缺交原因

21

資料篩選與計算

★符號選項皆可多選

資料篩選與計算


計算圖表
圖表類別
--請選擇--
顯示圖表
圖表類別
--請選擇--
年平均相對OI3變化
3種海拔OI3之變化趨勢
月平均OI3之變化趨勢
年平均OI3之變化趨勢
出現機率統計
OI_3與樣點海拔關係
歷年每月物種OI_3與犬、貓OI_3關係
歷年累計出現樣點數
圖表類別
年平均相對OI3變化
顯示圖表
年平均相對OI3變化
物種: 山羌
年平均OI3
50
40
30
20
10
0
2021
2022
2023
中部
南部
北部
東部
北部
中部
南部
東部
Highcharts.com

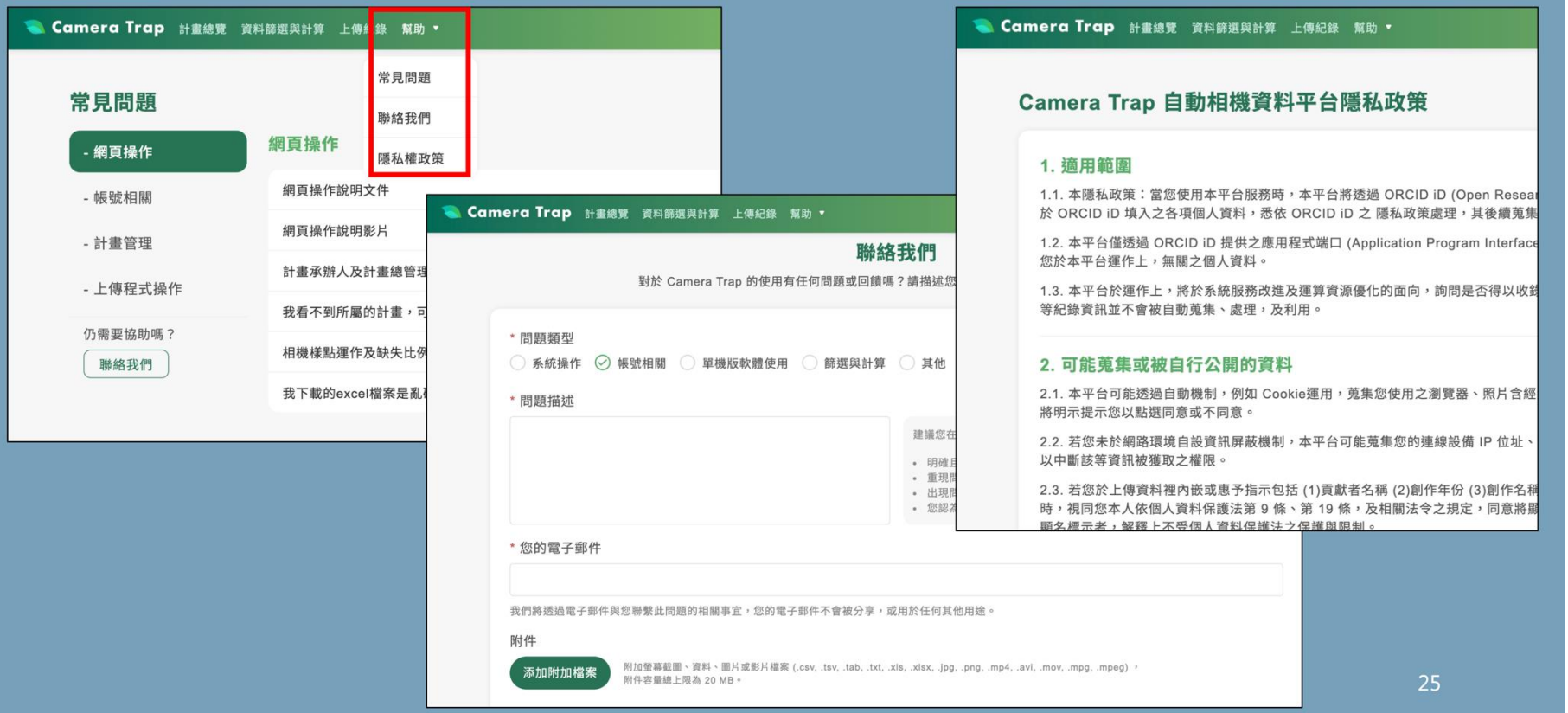
上傳紀錄

另外一個錯誤樣態為掉圖

點選後
可直接連到該資料夾所屬的查看影像頁面
查看上傳內容

24

幫助


Camera Trap 計畫總覽 資料篩選與計算 上傳紀錄 幫助
常見問題
聯絡我們
隱私權政策
常見問題
- 網頁操作
- 帳號相關
- 計畫管理
- 上傳程式操作
仍需要協助嗎？
聯絡我們
網頁操作
網頁操作說明文件
網頁操作說明影片
計畫承辦人及計畫總管理
我看不到所屬的計畫，可
相機樣點運作及缺失比例
我下載的excel檔案是亂
Camera Trap 計畫總覽 資料篩選與計算 上傳紀錄 幫助
聯絡我們
對於 Camera Trap 的使用有任何問題或回饋嗎？請描述您
* 問題類型
系統操作 帳號相關 單機版軟體使用 篩選與計算 其他
* 問題描述
建議您在
明確
重現
出現
您認
* 您的電子郵件
我們將透過電子郵件與您聯繫此問題的相關事宜，您的電子郵件不會被分享，或用於任何其他用途。
附件
添加附加檔案
附加螢幕截圖、資料、圖片或影片檔案 (.csv, .tsv, .tab, .txt, .xls, .xlsx, .jpg, .png, .mp4, .avi, .mov, .mpg, .mpeg)，
附件容量總上限為 20 MB。
Camera Trap 計畫總覽 資料篩選與計算 上傳紀錄 幫助
Camera Trap 自動相機資料平台隱私政策
1. 適用範圍
1.1. 本隱私政策：當您使用本平台服務時，本平台將透過 ORCID iD (Open Resea
於 ORCID iD 填入之各項個人資料，悉依 ORCID iD 之 隱私政策處理，其後續蒐集
1.2. 本平台僅透過 ORCID iD 提供之應用程式端口 (Application Program Interface
您於本平台運作上，無關之個人資料。
1.3. 本平台於運作上，將於系統服務改進及運算資源優化的面向，詢問是否得以收錄
等紀錄資訊並不會被自動蒐集、處理，及利用。
2. 可能蒐集或被自行公開的資料
2.1. 本平台可能透過自動機制，例如 Cookie運用，蒐集您使用之瀏覽器、照片含經
將明示提示您以點選同意或不同意。
2.2. 若您未於網路環境自設資訊屏蔽機制，本平台可能蒐集您的連線設備 IP 位址、
以中斷該等資訊被獲取之權限。
2.3. 若您於上傳資料裡內嵌或惠予指示包括 (1)貢獻者名稱 (2)創作年份 (3)創作名稱
時，視同您本人依個人資料保護法第 9 條、第 19 條，及相關法令之規定，同意將顯
顯名標示者，解釋上不受個人資料保護法之保護與限制。

如果您是
計畫總管理人
或
計畫承辦人

計畫總覽

資料上傳者與受委託單位無此功能

27

計畫總覽 - 新增計畫

資料上傳者與受委託單位無此權限

填寫計畫基本資訊
(*者為必填)

28

計畫總覽 - 新增計畫

資料上傳者與受委託單位無此權限

選擇資料授權方式：
參考創用CC授權說明
https://tw.creativecommons.net/home-page/

29

計畫首頁

資料上傳者與受委託單位無此功能

計畫管理

資料上傳者與受委託單位無此權限

31

資料上傳者與受委託單位無此權限

計畫管理 - 相機位置管理

勾選「棄用」還可在此頁面
找到此相機位置
只是無法於上傳介面中選取到

點選「刪除」即此相機位置
在此頁面也會被移除

計畫管理 - 計畫成員

資料上傳者與受委託單位無此權限

輸入參與此計畫成員之ORCiD帳號

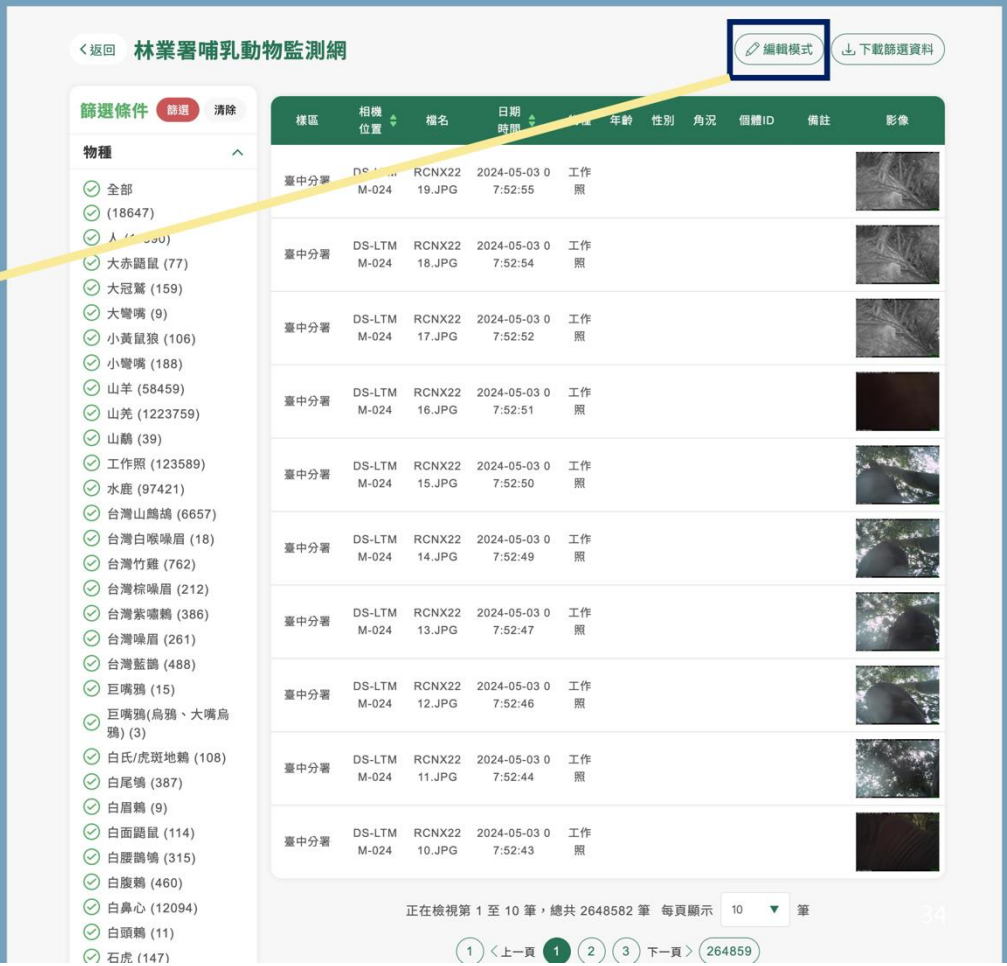
選擇該成員權限：
計個別計畫承辦人 / 資料上傳者 / 受委託單位

33

查看影像

資料上傳者與受委託單位無此功能

點選後，進入編輯模式



查看影像 - 編輯模式

資料上傳者與受委託單位無此權限

1 勾選特定資料，或全部勾選

2 點選編輯開啟編輯視窗，或刪除選取資料

3 結束編輯模式

35