行政院所屬各機關因公出國人員出國報告書

（出國類別：國際會議）

參加 2011 年「聯合國教科文組織下之國際數位鑑識組織（IFIP）會議」心得報告

服務機關 ： 法務部調查局資通安全處

出國人姓名 ： 陳受湛科長

出國地點 ： 美國佛羅里達州奧蘭多市

出國期間 ： 中華民國 100 年 1 月 28 日至 2 月 3 日

報告日期 ： 中華民國 100 年 3 月 29 日

報告大綱

壹、 行程記述……3

貳、 2011 IFIP 國際鑑識會議簡介……3

參、 參與 2010 IFIP 國際會議活動記要……4

肆、 心得與建議……15

附件：附表及相關會議照片……18

壹、行程記述

此次行程主要是參加由美國佛羅里達州奧蘭多之中央佛羅里達大學舉辦之第7屆聯合國教科文組織國際資訊處理協會11.9數位鑑識工作群組(IFIP，International Federation for Information Processing WG 11.9)舉辦之數位鑑識國際會議，並維持本局與國際鑑識專家學者之交流。本次會議時間自2011年1月30日起至2011年2月2日止共計4天，在中央佛羅里達大學國家鑑識科學中心會議廳舉行，此次會議共有15個國家，50多位來賓與會。

貳、IFIP WG11.9 國際數位鑑識組織會議簡介

國際資訊處理協會(IFIP)為一非官方及非營利的組織，協助各國相關協會在資訊處理領域的研究發展工作，IFIP是在1960年由聯合國教育科學文化組織(UNESCO)經費贊助下所建立的，目前該協會下共有56個國家或區域的資訊科技協會，分佈全球五大洲共約50萬的會員，IFIP依資訊處理之不同需求將組織架構分工為14個技術委員會(TC，Technical Committees)，每個委員會(TC)依需求再細分為不同的工作群組(WG，Working Group)，本次所參與的數位鑑識國際會議即由資訊處理系統之安全與防禦技術委員會(TC11，第11個委員會)下轄之11.9數位鑑識工作群組(WG 11.9)所舉辦，該工作群組主要任務為結合國際間從事數位鑑識的科學家、工程師及執法人員以推動數位鑑識科技研究領域發展。現任主席為美國籍的Mark Pollitt先生，他目前為中央佛羅里達大學國家鑑識科學中心教授，亦曾為美國FBI CART部門主管，負責處理電腦犯罪案件之數位證據擷取，在數位鑑識技術與研究方面頗為專精。此次由IFIP WG 11.9所舉辦之數位鑑識國際會議

為第七屆（自2005年至2011年），也是按照往例於美國佛羅里達州該校舉行(前三屆均在美國佛羅里達州奧蘭多市國家鑑識科學中心舉辦，第四屆在日本，第五屆又回到奧蘭多市，第六屆則在香港舉辦)。本次研討會議主題，除介紹手機內儲存媒體的數位鑑識技術及趨勢外，亦介紹了巴西警方在電腦鑑識領域的發展情形，另有其他議題如：雲端鑑識、數位證據檢驗之科學理論基礎、數位鑑識在商業上的應用、鑑識與調查、網路鑑識、釣魚網站與惡意程式分析、鑑識技術與工具、數位證據的可信賴保護及未來鑑識技術之發展。

參、參與 2011 國際數位鑑識組織會議活動記要

一、本次會議報到時間為 1 月 30 日（星期日）晚上 17:30 在住宿之 Radisson 旅館一樓大廳辦理報到手續，主辦單位並在 18:00 帶領各國與會人員驅車前往餐廳舉行歡迎晚宴，在主持人簡短的致詞後，即由與會之各國學者專家自行點菜用餐，這實在是一大進步，可以點些自己喜歡的口味。席間除自我介紹外並藉互相交換名片能多認識此次與會的貴賓，以便將來做進一步之交流聯繫。此次見到多位老朋友，包括 Mark Pollitt 主席夫婦，香港大學的鄒錦沛教授及英國 Dr Stephen Wolthusen 教授等。晚宴於 21:30 結束，主辦單位並作了會議時程的說明與報告；會議場地在中央佛羅里達大學，距離住宿之旅館只有 15 分鐘車程，又因許多貴賓有租車，所以大會希望大家可利用搭便車方式一同從旅館往返學校會議室，原則是上午 8:00

及下午 16:30 往返於會議場地及住宿飯店，如此也藉搭別人便車可以多認識與會的貴賓。

二、1 月 31 日上午 7:00 在旅館使用早餐後搭車前往學校，並於 8:20 由此次大會主席 Pollitt 先生開幕致詞後，隨即由美國秘勤局 James Darnell 先生作專題報告「U.S. Secret Service Efforts in Cell Phone and Embedded Device Forensics」，介紹該局電腦鑑識實驗室在手機鑑識方面有四類。第一是邏輯資料鑑定，第二是邏輯檔案系統鑑定，第三是實體非侵入性鑑定及最後是實體侵入性鑑定。會中亦提及手機鑑定所使用的一些工具，甚至使用越獄程式(jailbreak)作為鑑識取得證物內資料的工具。接著進行：

Session 1：Themes and Issues 議題，包括「The State of the Science of Digital Evidence Examination」和「Cloud Forensics」兩篇學術論文，探討有關數位鑑識與鑑識科學之關係，包括鑑識與科學是否有一致性及文學與科學之現行狀態。另外有關雲端鑑識方面，因著雲端運算將成為目前最新演進的技術，這些雲端的服務公司與使用者亦需建立雲端的鑑識能量。當然雲端鑑識是網路鑑識的一部分，從 3 大方向來看，第一是技術面，包括鑑識資料的蒐集，非常大的靜態與動態鑑識範圍，鑑識資料分散於多處及在不同的司法管轄地及鑑識前之

資料蒐集等。第二是組織面，雲端的鑑識調查應包含兩大部分，一是 CSP 雲端服務業者及雲端用戶，且 CSP 將部分外包時，其組織面則更擴大，鑑識之難度亦相對增加，所以鑑識人員需明瞭所需鑑識的範圍。第三在法律面，會面臨多重司法管轄及多重委託或租賃主機情況，還有 CSP 與顧客間的法律協議(SLA)。因著雲端犯罪所面臨的雲端鑑識需要對多重司法及多重資料中心作調查，以及涉案對象的系統、操作及資料交換等，還有事件的追縱與重建都是需要的。而雲端鑑識主要的內容包括 1.問題確認，如確認所涉資料存於雲端實體與虛擬環境的位置，以及確認雲端服務的功能與系統作業的情況。2.記錄監控，就是在雲端跨系統中針對記錄資料，來蒐集、分析及建立關聯性，以協助稽核與檢查應有的管理作為。3.資料及系統復原，將在雲端已被有意或無意刪除或更改的資料復原，以及被入侵而造成損壞的系統復原，還有是雲端資料的獲取與保全。

在 Session 2：Business Applications 議題，包括「Leak Detection Analysis of Business Processes」及「Detecting Collusion in ERP Systems」兩篇論文，主要介紹在商業處理上常使用的稽核與認證模式的檢測軟體，檢測其漏洞並作分析，特別是資訊流(IF)分析，包括集中在正常管道及政策下及不能完全保證之隔離與限制使用之資料處理系統。另一篇介紹

ERP 系統的偵測結果，藉設計一些詐欺模式及檢視系統，來偵測在使用 ERP 系統之內部共謀詐欺行為，包括從不同來源與可攜式媒體中，取得公司重要資料。經其測試發現目前的 ERP 系統中，仍舊有許多內部人員之詐欺問題存在，且無法偵測。

中餐過後 13:30 開始進行

Session3: Investigative Frameworks 議題，介紹「A Framework for Investigative Questioning in Incident Analysis and Response」，特別介紹如何建置一個以系統化模組來作電腦犯罪或事件關聯性調查之數位鑑識的架構。它是三層式架構來協助數位鑑識調查工作，1.社會層包括人、組織及其目的與意圖 2.邏輯層包括電腦、網路與軟體等，3.實體層，包括所有可接觸的實體，如設施、紙張文件等等。而且社會層與邏輯層活動的結果產生實體層，而最後調查目標是所有事件需聯於犯罪行為人，故在程序導向之事件分析中，藉結構性架構整合而產生完整的鑑識架構。另外「A Case-Based Reasoning Framework for Live Forensics」，此篇報告是巴西警方建置了一個作業方法來協助同仁在現場取得開機時之數位證據，它的好處包括：可以將先前案件之專業技術作為知識庫分享，採納最佳程序來確保證據收集，減少開機狀況下之鑑識分析時間及可建構一個持續成長知識庫，且均為已被證實且成功的實作案例。此

作業流程分為:1.查詢－以目前所遇到的問題去知識庫查閱之前完成的案件並瞭解其解決方式。2.照作－將所查成功案件所建議之方式作作看。3.修正－藉專家評估其結果並提出調整方式。在其過程中如何將現有案件對應到之前所存於知識庫案件？他們提出自我組織式對應方式,首先使用人工神經網路系統來作自我學習，再作相似度計算，最後找出最高相似度及其相鄰之案件作一些調整去符合此案件需求。之後就可從其中取得一整套的鑑識程序並且合適於此案件之鑑識作業方式與程序了。當然所有案件之鑑識程序都可以在知識庫中被查閱，這知識庫是可以不斷新增、修改並進步的。此知識庫可分成 6 種屬性：密碼破解，網頁郵件服務，網路即時通，網路銀行，P2P 應用，社交網站等。而所鑑識的案件亦可分為：兒童色情，釣魚網站詐欺，盜版軟體，毒品犯罪，經濟犯罪及資料外洩等。如此的比對出類似案件的鑑識方法就能提供鑑定人員最佳的解決方案。另外香港大學的教授報告「Sensitivity Analysis of Digital Forensic Reasoning Using Bayesian Networks」指出利用貝式網路模型作數位鑑識之敏感分析,特別說到先假設各種情況，如由事件 A 所涉及的證物與事件 B 所涉及的證物，再假設如果在案件偵辦中所發生的事件，找出各事件間的關聯性，就可假設可能會存在某些特定的證物。因為數位鑑識

是事後的處理，若是能反向考量，藉著所取得的證物，觀察其內容而得知發生的事件，又從所發生的事件可推斷合理的鑑識作為。故此其分析方式是一種學習程序，藉著不斷的觀察而一再更新其結果。

在 Session 4: Network Forensics I 議題，發表了「Deterministic Router and Interface Marking for Network Forensics」及「Extracting Digital Evidence from VoIP Applications」兩篇論文，第一篇說到利用網路 IP 位址作追縱，可以追查到入侵來源，但其問題是如何確認其來源的實際位置，若能則可對入侵者繩之以法，這就是網路鑑識。目前網路鑑識從目的分有廣義網路鑑識及狹意網路鑑識，從封包側錄分有全側錄系統及停看聽系統，從分析時間上分有即時分析與事後分析，從資料來源分有資料流系統及封包串系統。故為了能對入侵者所送之封包作記號以便於追蹤及對所經過之路由設備作標記，為其論述之主要內容。第二篇主要是介紹從網路電話環境中擷取數位證據之鑑識工具。因著所有 VoIP 的使用者均只需有一名稱及有效的電子郵件，故追查不易。又因其聲音資料是作壓縮加密，所以此鑑識工具包括了 1.資料封包順序的重建 2.具功能性之相互查詢技術並自動記錄 3.藉解密及路由協定作聲音檔分析，如藉 FFT 數位訊號處理確認其開始與

結束位置及定義其為何種語言 4.藉跟蹤與追蹤，取得 VoIP 使用者資訊。該工具並作成圖形化介面方便鑑識人員操作。

三、2 月 1 日上午哈佛大學教授發表「Gathering Evidence of Large-Scale Internet Frauds」演講，說到如何從大範圍的網路詐欺案件中取得證據，這些案件如網路釣魚與地下經濟，廣告詐欺與仿冒及非法線上藥品販售等，作為其研究對象。該演說中強調如何掃描釣魚網站，如何防止其攻擊並縮短其生存時程。廣告詐欺部份，特別利用我們無法查覺的錯誤名稱所誤導而遭受損失。查覺的方式有收集常用的網域名稱，測量比較字串，肥大指頭距離計算等。因有以下的網站攻擊方式，一是其網頁已被感染，一是被導向到惡意網站，一是線上賣藥網站卻是販售一般物品，我們亦可使用搜尋引擎來發覺。一些搜尋引擎公司提供了此方面的服務。接著

Session 5: Phishing and Malware Analysis 議題，有二篇論文：「What is So Smart about Mr. Brain?」及「Cross Evidence Malware Identification Using deLink」主要是介紹釣魚網站及惡意程式的分析技術，因著釣魚網站攻擊是個嚴重問題，最常見的是偷取個人資料，且是有組織的行為。其分析手法包括蒐集惡意檔案如 ZIP 檔、RAR 檔或 TAR 檔就是 Phishing Kit，而這些都是後門程式。從這些程式中可以發現一些小動作而且

因利用技巧來模糊它，包括陣列、並置、隱藏、設定值、16進位加密、64位元加密等，如何將其作成鑑識工具是未來努力之方向。

Session 6: Network Forensics II 議題，有二篇論文，「A Network Forensic Implementation for Detecting Mobile Botnets using Artificial Immune Systems」及」「An FPGA-Based System for Detecting Malicious DNS Network Traffic」，第一篇主要說到利用人工免疫系統作為偵測行動殭屍之網路鑑識應用。因著殭屍電腦之惡意程式開始在行動裝置上活動而造成新的威脅，且使偵測上分辨電腦或行動裝置變為模糊及垃圾 SMS 也開始像垃圾郵件一樣漫延。故此希望建置一套人工免疫系統(AIS)，利用樣本辨識原型，從正常中區隔出不正常者，也能明確區別正常的 SMS 或垃圾 SMS。該系統可利用明確實例自我訓練而產生唯一的特徵值作為其樣本，使其有能力偵測不正常發送 SMS 的行為，就可提供給服務業者。第二篇是探討如何利用 FPGA 電路合成系統偵測惡意 DNS 網路活動。因著發現有 DNS 協定不正常的使用，導致一些重要資訊被駭客所偷。故利用點對點的追縱分析系統(TRAPP)及快速的處理器與網路卡來審查每一封包，並過濾其 DNS 的 UDP 及 port 53，讀出其 DNS 網域且產生 sdbm 雜湊值，作為白名單，若比

對不在白名單者即作成記錄。如此即可偵測不正常的 DNS 攻擊行為。此系統經測試確實有效。中午還是在學校用餐，餐後 Session 7: Forensic Techniques and Tools 議題，有 3 篇論文，「Fast Content-Based File Type Identification」，「lightgrep: A Multipattern Regular Expression Search Tool for Digital Forensics」及「Assembling the Metadata for a Database Forensic Examination」，主要是能針對檔案內容作檔案格式的辨認，因著所有的檔案都是一連續的字元所組成，而每一個字元有 256 種表示方式，我們可利用計算這 256 個字元出現的模式產生字元分佈的頻率。再利用統計及資料探勘技術作檔案身份確認。按此原理－不同的檔案型態就有不同高頻率態樣，作為特徵選項技術，並統合所有檔案的特徵作為檔案交叉比對的態樣。至於有關資料庫系統(DBMS)包含中介資料(metadata)及資料(data)，若是我們在資料庫中能查覺中介資料放更改，就有方法查覺資料被更改。其方法主要是從資料庫的四個層面來作其主要的鑑識作為：資料模組，資料字典，應用模式及應用資料。將這四個層面的資料及中介資料作組合並檢視其是否”乾淨”，若以此方式就可查覺資料庫是否有被更動。

四、2 月 2 日上午 08:30 至 10:00 進入 Session 8: Novel

Techniques，有三篇的論文，「Stylometric Approaches to Author Obfuscation: An Empirical Study」「SWF Steganography: Techniques for Hiding Data in SWF Files」及「Resolving Conflicts between Access Control and IT Forensics」。主要是談到資料隱藏及著作權模糊之鑑識問題，因著網路上著者身份辨識上的困難造成鑑識問題，又因著網路上的文章多以 SWF 檔格式呈現，所以如何利用 SWF 檔案中之資料隱藏技術來證明其資料為真，而非是用來隱藏。例如檔案以 web 格式存在，它包含影像、聲音、影片，字型及指令，而通常是在網際網路的應用上。它的結構中有檔頭及資料標記等等，而其中有些資料是隱藏的，若是能在一般正常的資料外加入使用者自己的標示，而不會被注意，當有爭議時能成功取出其所隱藏資料。

Session 9: Forensic Analysis Techniques，有二篇的論文「Investigating Forensic Processes for the Apple iPad」及「Forensic Analysis of Plug Computers」主要介紹蘋果 iPad 的鑑識技術及即插式電腦之鑑識分析。因著這一年平版電腦的發達，尤其是 iPad 的流行，而面臨鑑識上的需求。因著硬體的改變，鑑識方法亦需要持續的更新。目前的鑑識方式有：1.商業工具軟體分析，包括 Lantern，Mobilyze 及 Oxygen

Forensics Suite 等。其各有其優點如為 Mac 或 Windows 介面，並在手動還原下作資料備份。2.但亦有使用破解工具如 jailbreak 者，目前可以針對 4.2.1 版作資料備份與讀取。3.使用 iTunes 備份方式，利用其所提供的同步功能，但無法對加密備份資料作鑑識。在資料分析方面，它有潛在證據如文件、各種聲音影像，應用程式及其它各種檔案如電子郵件，通訊錄(Contacts)，瀏覽網頁(Safari)，YouTube，Maps，行事曆等。當然亦會面臨內部系統安全功能包括清除、通行碼及資料加密等，但因著行動設備不斷增多，故鑑識分析亦越為重要。另外即插式電腦(Plug Computers)的介紹，它非常的小，像智慧型手機，卻有電腦之功能。它於 2009 年開始出現於市場(名叫 SheevaPlug)，cpu 為 Marvell 88F600 有 1.2GHz，RAM 有 512MB DDR2 及 512MB 的 flash memory。此報告亦介紹該機器的鑑識方法，非常特殊，增加了此方面的瞭解。

五、此次會議於 2 月 2 日中午結束，中午用餐後，主席 Mark Pollitt 先生為盡地主之誼，邀請我們參觀佛羅里達州非常有名的奧蘭多溼地公園，它涵蓋了 1650 英畝土地，可以藉回歸自然，放鬆心情，欣賞美麗的夕陽。溼地有許多的湖泊與沼澤，遊客多來此賞鳥、攝影、慢跑及騎自行車，據他所知道的有超過 220 種的鳥類在此被發現。我們很幸運看到了美國老鷹，還有許多野

生鱷魚，難得有了一趟知性之旅。

肆、心得與建議

一、心得：

(一)此次會議因在美國舉行，所以從歐美國家來的與會者較多，反而亞洲地區來的較少，好像只有一位是從日本來的，四位是從香港來的。此次的論文多以新型態的鑑識為主，如手機、流行之行動裝置等。還有雲端鑑識亦為目前全球各國鑑識單位所著重的項目。雖不是很成熟但卻走出一步。執法單位亦有許多的論文發表，包括美國秘勤局，巴西聯邦警察，香港警察，美國空軍等，有比較實務上的經驗分享。

(二)會議中亦就本實驗室所遇見的一些技術問題與與會者多有私下的討論，包括搜索現場之查扣數位證物，一些國家亦十分注重現場鑑識作業，不像以往只要看到電腦設備就全部扣押，而是如何利用工具針對開機電腦按一定之程序作初步過濾，並且將存在記憶體內資料擷取檢視，而將扣押物縮小範圍，使後續鑑識作業更有效率。另外亦討論有關網路鑑識方面之技術，如何檢視過濾惡意之遠端控制程式及 IP 位址的追查。還有討論到未來有可能許多目前電腦所使用之資料處理軟體會因著不斷更新版本而造成版本不相容，甚至無法開啟多年前大家所熟悉的檔案資料，該有如何之因應與對策，使

得在任何年代的鑑識報告及所取得的證物，均能完整、完全且正確的還原出來。

(三)此次會議中，亦注重利用鑑識的觀念作著作權的確認，或是利用與資料相關的中介資料，作為判定有否被修改之鑑定方法，都已經將傳統鑑識之概念，應用到資料的安全，文獻的正確保存及著作權的保護等需求上。

(四)因著國內在數位鑑識這領域多為公領域範圍，在面臨個人資料保護法實施後，勢必會有許多相關的訴訟與官司產生，在國外有許多數位鑑識與顧問公司可以處理一部分屬民事的案件，但目前國內還未開放，若能作局部的開放，將可帶動數位鑑識技術與認知大幅提昇。

(五)因著去年亦參加此國際會議，今年又有機會前往，覺得此會議內容能一直不斷的創新，又能考量資安實務上的需要，還見到多位好朋友，實在感到萬分難得。

二、建議事項

(一)持續於國內推動舉辦國際性之數位鑑識研討會，並能透過學術單位，結合國內數位鑑識之人才為基本會員，共同推動國內數位鑑識之基本認知。

(二)數位鑑識是無國界之鑑識技術與科學，如何藉助國際上的組織，接觸國際上此方面的專家，是提昇國內鑑識能量，然這

需要政府大力的支持，尤其在經費上能多有協助。此次有許多國家如巴西、南非等在數位鑑識上都很有發展，實在需要派員前往學習。

(三)可規劃允許民間成立相類似的數位鑑識顧問公司，藉政府之審核並認證管理，利用民間之專業能力，來處理有關民事訴訟案件中相關的數位證據的採證及辨證，以減輕政府鑑識部門之負擔，並推動數位鑑識產業在國內之發展。

(四)持續提升本局外勤人員數位證據蒐集能力，尤其是針對目前所流行的 iPhone 及 iPad 等行動裝置之鑑識技術與工具，以繼續發展本局外勤所需之整合性的工具。

附錄：附表及相關會議照片

一、大會議程

Seventh Annual IFIP WG 11.9 International Conference on Digital Forensics
National Center for Forensic Science
University of Central Florida
Orlando, Florida
January 30 – February 2, 2011
January 30, 2011 (Sunday)
06:30pm - 08:30pm: Dinner (High Tide Harry's, 4645 S. Semoran Boulevard; Tel: (407) 273-4422)
Meet in Hotel Lobby @ 05:30pm for Car Pooling
January 31, 2011 (Monday)
06:30am - 08:00am: Breakfast (Hotel Radisson University)
08:20am - 08:30am: Welcoming Remarks and Logistics
08:30am - 09:30am: Keynote Lecture
U.S. Secret Service Efforts in Cell Phone and Embedded Device Forensics
Special Agent James Darnell, U.S. Secret Service, Washington, DC
09:30am - 10:30am: Session 1: Themes and Issues
Chair: Mark Pollitt, Daytona State College, Daytona, Florida
The State of the Science of Digital Evidence Examination
F. Cohen, J. Lowrie and C. Preston
California Sciences Institute, Livermore, California
Cloud Forensics
K. Ruan, J. Carthy, T. Kechadi and M. Crosbie
University College Dublin, Dublin, Ireland
IBM, Dublin Ireland
10:30am - 10:45am: Break
10:45am - 11:45am: Session 2: Business Applications
Chair: Hein Venter, University of Pretoria, Pretoria, South Africa
Leak Detection Analysis of Business Processes
R. Accorsi and C. Wonnemann
University of Freiburg, Freiburg, Germany
Detecting Collusion in ERP Systems
A. Islam, M. Corney, G. Mohay, A. Clark, S. Bracher, T. Raub and U. Flegel
Queensland University of Technology, Brisbane, Australia
SAP Research Center, Brisbane, Australia
11:45am - 01:00pm: Lunch (Marketplace@UCF Campus – Shuttle Transportation Provided)

01:30pm - 03:00pm: Session 3: Investigative Frameworks

Chair: Jill Slay, University of South Australia, Mawson Lakes, Australia

A Framework for Investigative Questioning in Incident Analysis and Response

C. Blackwell

Oxford Brookes University, Oxford, United Kingdom

A Case-Based Reasoning Framework for Live Forensics

B. Hoelz, C. Ralha and F. Mesquita

National Institute of Criminalistics, Brazilian Federal Police, Brasilia, Brazil

University of Brasilia, Brasilia, Brazil

January 31, 2011 (Monday) (continued)

Sensitivity Analysis of Digital Forensic Reasoning Using Bayesian Networks

M. Kwan, K.-P. Chow, H. Tse, F. Law and P. Lai

University of Hong Kong, Hong Kong, China

03:00pm - 03:30pm: Break

03:30pm - 04:30pm: Session 4: Network Forensics I

Chair: Rafael Accorsi, University of Freiburg, Freiburg, Germany

Deterministic Router and Interface Marking for Network Forensics

E. Pilli, R. Joshi and R. Niyogi

Indian Institute of Technology – Roorkee, Roorkee, India

Extracting Digital Evidence from VoIP Applications

D. Irwin and J. Slay

University of South Australia, Mawson Lakes, Australia

06:30pm - 08:00pm: Dinner (Smoky Bones, 303 N. Alafaya Trail; Tel: (407) 249-2009)

Meet in Hotel Lobby @ 06:15pm for Car Pooling

February 1, 2011 (Tuesday)

06:30am - 08:00am: Breakfast (Hotel Radisson University)

08:30am - 09:30am: Keynote Lecture

Gathering Evidence of Large-Scale Internet Frauds

Tyler Moore, Center for Research on Computation and Society, Harvard University, Cambridge, Massachusetts

09:30am - 10:30am: Session 5: Phishing and Malware Analysis

Chair: Kam-Pui Chow, University of Hong Kong, Hong Kong, China

What's So Smart about Mr. Brain?

H. McCalley, B. Wardman and G. Warner

University of Alabama at Birmingham, Birmingham, Alabama

Cross Evidence Malware Identification Using deLink

A. Flaglien, K. Franke and A. Arnes

Gjovik University College, Gjovik, Norway

10:30am - 10:45am: Break

10:45am - 11:45am: Session 6: Network Forensics II

Chair: Martin Olivier, University of Pretoria, Pretoria, South Africa

A Network Forensic Implementation for Detecting Mobile Botnets using Artificial Immune Systems

I. Vural and H. Venter

University of Pretoria, Pretoria, South Africa

An FPGA-Based System for Detecting Malicious DNS Network Traffic

B. Thomas, B. Mullins, G. Peterson and R. Mills

Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio

11:45am - 01:00pm: Lunch (Marketplace@UCF Campus – Shuttle Transportation Provided)

01:30pm - 03:00pm: Session 7: Forensic Techniques and Tools

Chair: Gilbert Peterson, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio

Fast Content-Based File Type Identification

I. Ahmed, K. Lhee, H. Shin and M. Hong

Queensland University of Technology, Brisbane, Australia

Ajou University, Suwon, South Korea

`lightgrep`*: A Multipattern Regular Expression Search Tool for Digital Forensics*

J. Stewart and J. Uckelman

Lightbox Technologies, Arlington, Virginia

University of Amsterdam, Amsterdam, The Netherlands

Assembling the Metadata for a Database Forensic Examination

H. Beyers and M. Olivier

University of Pretoria, Pretoria, South Africa

03:30pm - 03:30pm: Break

03:30pm - 04:45pm: Panel: Preserving the Authenticity of Digital Evidence

Chair: Barbara Endicott-Popovsky, University of Washington, Seattle, Washington

Panelists

B. Endicott-Popovsky, University of Washington, Seattle, Washington

F. Cohen, California Sciences Institute, Livermore, California

L. Duranti, University of British Columbia, Vancouver, Canada

A. Jansen, University of British Columbia, Vancouver, Canada

February 1, 2011 (Tuesday) (continued)

06:30pm - 08:30pm: Dinner (Miller's Ale House, 641 N. Alafaya Trail; Tel: (407) 736-0333)

Meet in Hotel Lobby @ 06:15pm for Car Pooling

February 2, 2011 (Wednesday)

06:30am - 08:00am: Breakfast (Hotel Radisson University)

08:30am - 10:00am: Session 8: Novel Techniques

Chair: Philip Craiger, Daytona State College, Daytona, Florida

Stylometric Approaches to Author Obfuscation: An Empirical Study

P. Juola and D. Vescovi
Duquesne University, Pittsburgh, Pennsylvania
SWF Steganography: Techniques for Hiding Data in SWF Files
M.-A. Fouche and M. Olivier
University of Pretoria, Pretoria, South Africa
Resolving Conflicts between Access Control and IT Forensics
C. Winter, M. Schneider and Y. Yannikos
Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany

10:00am - 10:15am: Break

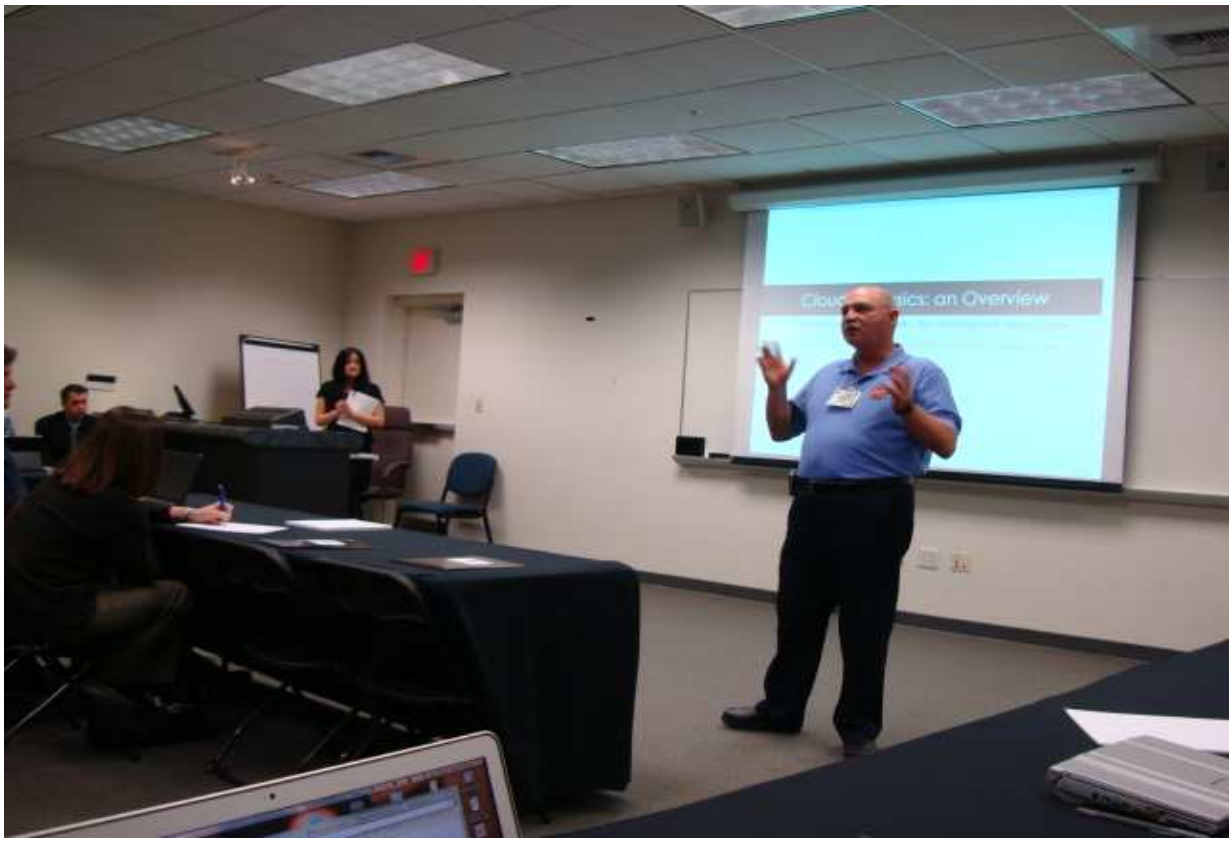
10:15am - 11:15am: Session 9: Forensic Analysis Techniques

Chair: Mason Rice, University of Tulsa, Tulsa, Oklahoma
Investigating Forensic Processes for the Apple iPad
A. Hay, D. Krill, B. Kuhar and G. Peterson
Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio
Forensic Analysis of Plug Computers
S. Conrad, G. Dorn and P. Craiger
National Center for Forensic Science and University of Central Florida, Orlando, Florida
Daytona State College, Daytona, Florida and National Center for Forensic Science, Orlando, Florida

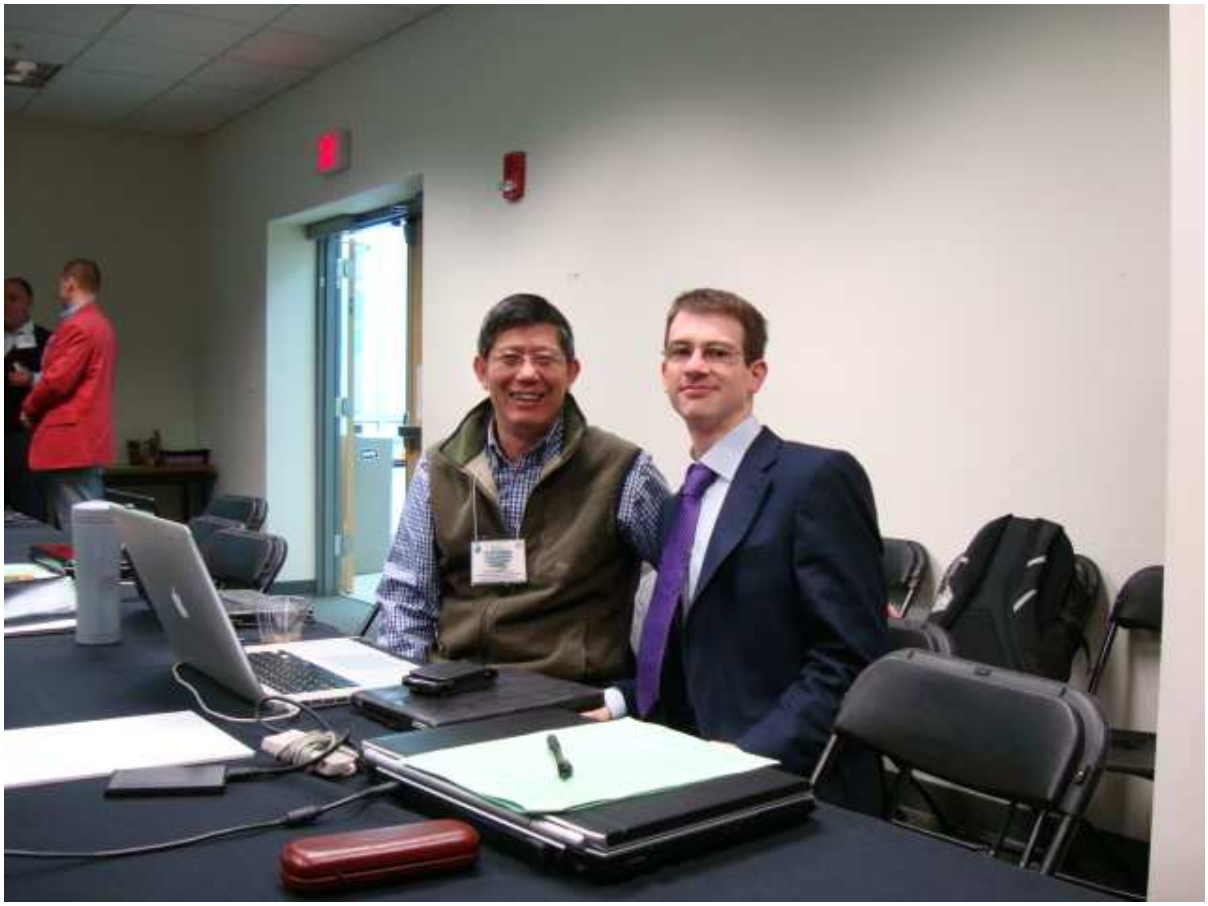
11:15am - 12:30pm: Lunch (Marketplace@UCF Campus – Shuttle Transportation Provided

會議照片：

現任協會主席及此次大會主席 Mark Pollitt 先生 參加歡迎晚宴

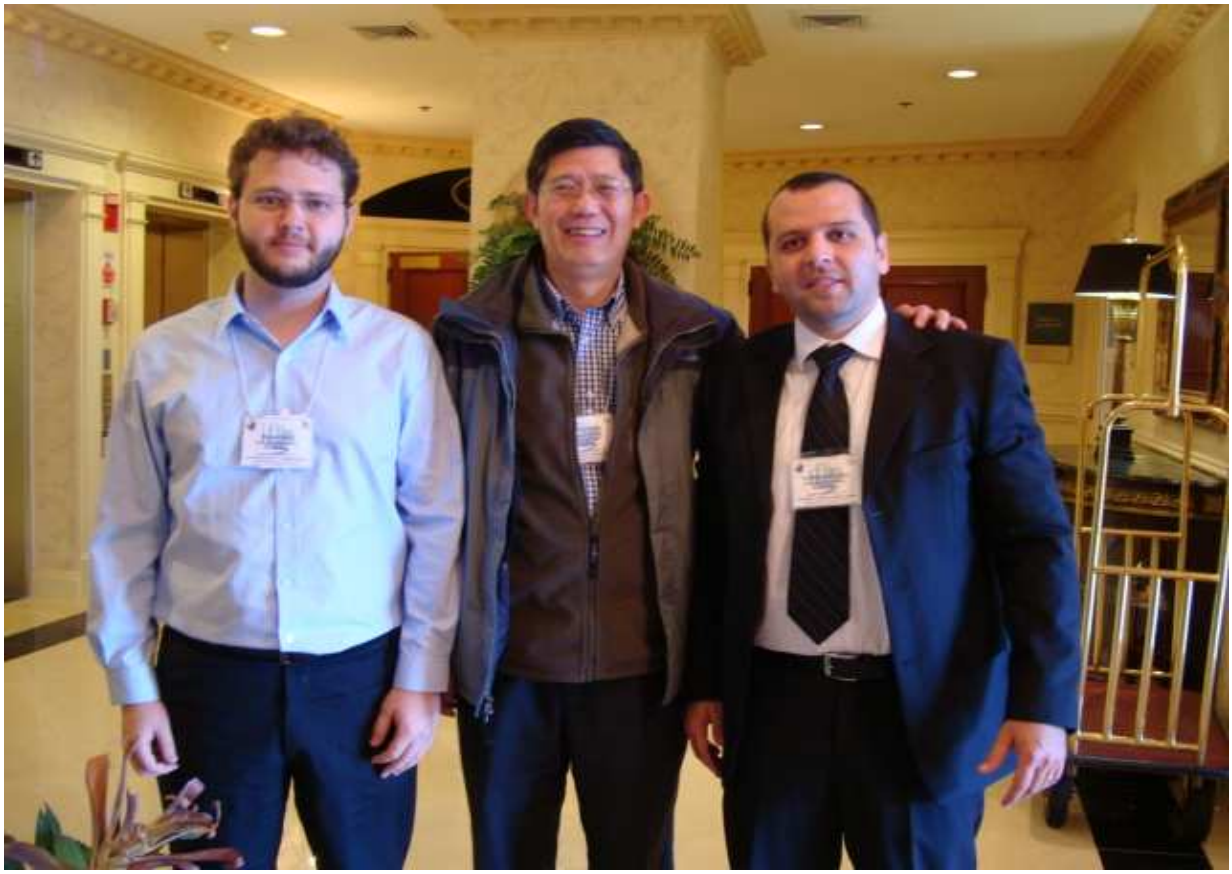


開會現場一

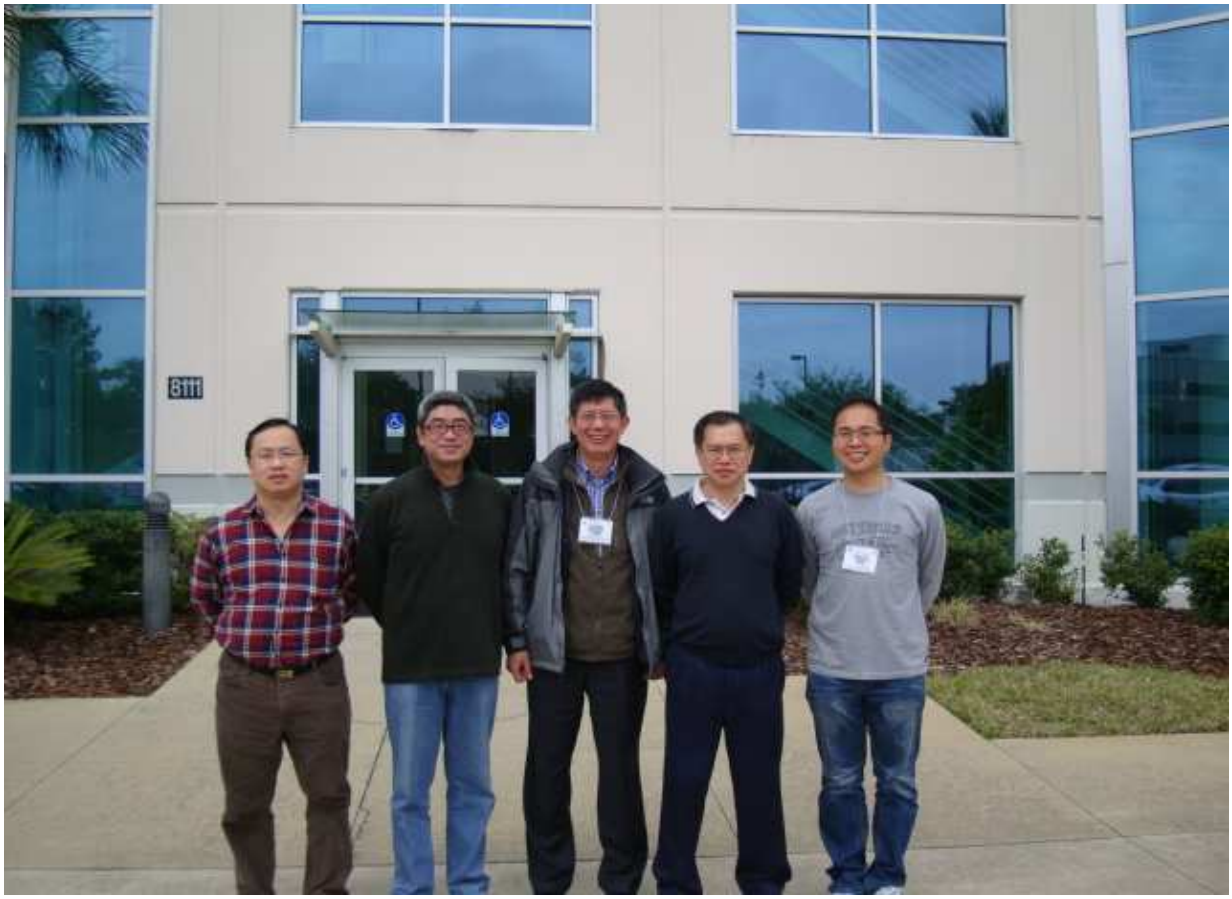


開會現場二，皇家哈洛威大學數學系 Dr Stephen D Wolthusen 教授

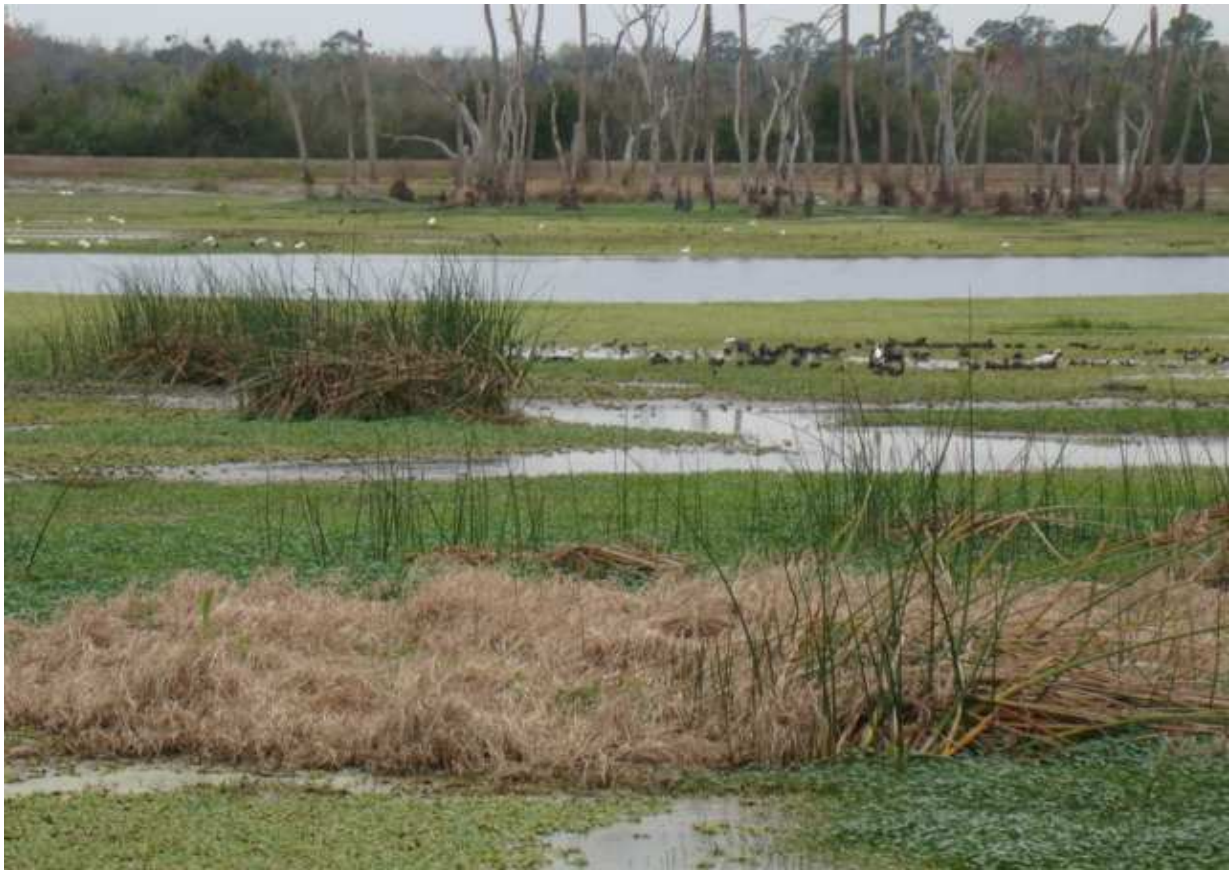
會議論文發表情況



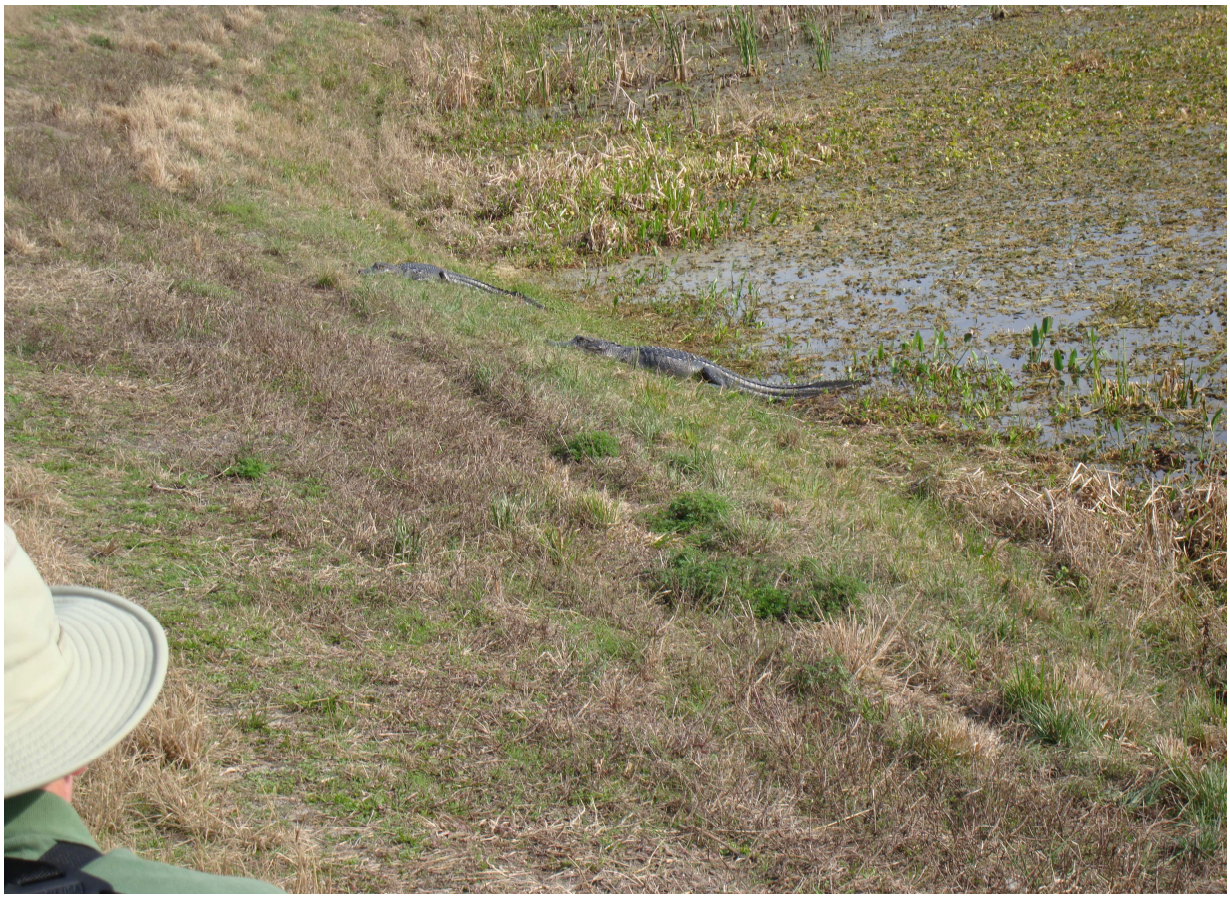
巴西首都巴西里亞聯邦警察局二位警官。



香港大學及香港警察人員



奧蘭多溼地公園一



奧蘭多溼地公園二