行政院所屬各機關因公出國人員出國報告書
（出國類別：實習）

參加「澳洲數位鑑識會議專案及南澳警察鑑識工具研習營」心得報告

服務機關 ： 法務部調查局

姓名職稱 ： 鄭健行調查官，蔡詩彥調查官

派赴國家 ： 澳洲 阿德雷德市及伯斯市

出國期間 ： 中華民國 101 年 11 月 29 日至 12 月 7 日

報告日期 ： 中華民國 101 年 12 月 13 日

摘要

第 10 屆澳洲數位鑑識會議係由澳洲 ECU 大學安全研究協會(ECU Security Research Institute)主辦，澳洲電腦社群協會、澳洲安全網站公司及思科公司等協辦，於 2012 年 12 月 3 日至 5 日在澳洲伯斯市的伯斯蘭利諾富特飯店（Novotel Perth Langley）會議中心舉行，主要參與者來自澳洲學、警及資訊業界，其他還有美、亞等近百名之各國資訊安全與數位鑑識組織人員、企業實務界代表以及學術界研究人員與會。本次會議舉行同時，大會亦在同地點其他會議室舉辦其他主題研討會，包含第 13 屆「澳洲資訊戰研討會」、第 10 屆「資訊安全管理研討會」及第五屆「澳洲安全與情報研討會」等，可提供電腦鑑識與資訊安全相關領域之參考。藉由參與澳洲電腦鑑識科學國際會議，瞭解澳洲目前在電腦鑑識科學之學術研究方向，分享實務經驗並建立國際交流管道。亦瞭解澳洲電腦鑑識科學實務應用之最新發展趨勢，供本局數位鑑識人員參考。

南澳警察鑑識工具研習營由南澳警察局（SAPOL）所主辦，於 2012 年 11 月 30 日至 12 月 1 日在澳洲阿德雷德市南澳警察局偵查科技犯罪部門舉行，因該部門人員曾參訪本局資安鑑識實驗室，並介紹實務上南澳警察在第一線所使用之工具及流程，後持續保持聯繫，近來因澳洲使用之數位鑑識工具已不同，願提供本局數位鑑識工具與流程之研習課程，因南澳警方在數位鑑識領域之現場數位證據採證技術發展較早，前其使用之 zero tech 工具設計亦提供本局於發展第一線人員數位證據採證工具時許多具有價值之參考，藉由此次學習交流，對於本局將來數位鑑識之架構分工、整體流程及工具技術的發展，皆極有幫助。

報告大綱

壹、會議目的

此行赴澳洲參加「2012 年第 10 屆澳洲數位鑑識會議」及「南澳警察鑑識工具研習營」之主要目的可分為以下 2 點：

一、 藉由參與澳洲電腦鑑識科學國際會議，吸取澳洲及各國在網路、資訊安全及電腦鑑識之心得；同時瞭解澳洲目前在電腦鑑識科學之學術研究方向，分享實務經驗並建立國際交流管道。

二、 參加南澳警察鑑識工具研習營以瞭解南澳警察現行工作之架構分工、鑑識流程及數位證據採證工具，以提供本局數位鑑識未來發展之參考方向。

貳、南澳警察科技犯罪偵查部門及澳洲數位鑑識研討會簡介

南澳警察科技犯罪偵查部門負責偵查有關網路犯罪、線上交易詐欺及數位證物蒐證鑑識，成員包含警探及鑑識人員，於2006年該單位與南澳大學合作，研發第一線人員zero tech數位證據蒐證軟體，並運用於實案上，在現場數位證據採證流程、工具運用等實務經驗非常豐富。

第10屆「澳洲數位鑑識會議」（The 10th Australian Digital Forensics Conference of 2012 secau Security Congress）為澳洲ECU大學安全研究機構（ECU：Edith Cowan University）所主辦， 此次大會同時舉辦之研討會還包含第13屆「澳洲資訊戰研討會」、第10屆「資訊安全管理研討會」及第五屆「澳洲安全與情報研討會」等，澳洲ECU大學在資訊安全、電腦鑑識、情報及醫療數位化等，皆已投入研究多年，會議議程如附件2。

參、活動記要

一、 2012 年 11 月 30 日到達後，即至南澳警察局科技犯罪防制部門參加課程，由該部門主管Mr. Barry 熱情接待，並親自介紹其部門成員，包含負責偵辦網路犯罪之警探及電腦鑑識分析人員，在稍作休息後，由Mr. Barry 先親自授課，課程先介紹 Computer Forensic Triage Tool 的概念及使用時機，再由鑑識專業人員講授操作說明，此套工具可同時運用在第一線現場採證及初步過濾分析。

此套工具僅須具備基本電腦概念，輔以短期訓練即能順利使用，圖形化的介面，讓使用者易於操作及了解，使用階段分為 Scan、Analyze 及 Act 三階段，迅速取得並分類目標電腦內之資訊，亦適合第一線數位證據蒐證使用，尤其是偵辦難度不高的案子如：兒童色情照片或網站，找出檔案後即可移送，若遇現場無法分析則

後送鑑識單位鑑定，該工具如要運用於國內環境尚有 2 點待克服，其一為英文介面較難上手，另外就是工具以套數計算版權費用，若要推廣所費不貲。

二、 12 月 1 日上午由南澳警方辦案警探介紹美國聯邦調查局（FBI）提供予執法人員使用之工具 osTriage，此工具須向 FBI 提出申請，說明為執法人員身份，就可以獲得授權使用，該工具亦為圖形化介面易於操作，使用方式類似本局現行工具 liveDetector，只是蒐集之項目不同；由於此項工具只要是各國執法單位向美國聯邦調查局提出申請，皆能免費使用，因此在警探說明操作方法之後，即提供一套工具供本局帶回試用，有相當之實際參考價值。

下午由鑑識專家 Lin,Yi-Chi 博士協助，介紹南澳警方的電腦鑑識實驗室及所使用的工具、收件的流程及鑑識報告格式範例（提供 2 份實案之鑑定報告供本局參考，如附件 3）。

現今數位證據的種類及數量皆以倍數成長，南澳洲在 2 年前，一個非急要之普通數位鑑定案件，須等待 4-6 個月時間方能排入鑑定時程，但今日已須等待 18-24 個月，為了能解決此積案問題，南澳警方已預備在分局設立數位鑑識組，由經過訓練之合格人員先行檢視過濾數位證據。

三、 12 月 2 日為週日，搭乘澳洲國內航線，前往澳洲西部伯斯市。

四、 12 月 3 日上午 9:00 前往伯斯市伯斯蘭利諾富特飯店（Novotel Perth Langley）會議廳簽到參加研討會，會場共區分為 4 個會議廳，除了此次計劃參加之第 10 屆「澳洲數位鑑識會議」外，大會又同時舉辦了相關研討會還包括第 13 屆「澳洲資訊戰研討會」、第 10 屆「資訊安全管理研討會」、第 5 屆「澳洲安全與情報研討會」、第 3 屆「澳洲反恐研討會」及第 1 屆「澳洲健康網資訊安全研討會」等 5 個研討會（13th Australian Information Warfare Conference、10th Australian Information Security Management Conference、 5th Australian Security and Intelligence Conference、3nd Australian Counter Terrorism Conference、1st Australian eHealth Informatics and Security Conference），大會首先由思科公司 Mr Gavin Reid 演講「Where automation ends and people begin」，內容講述資訊安全有許多自動化工具做協助，但有關使用者的正確作為，亦是重要的關鍵。

緊接著即由各廳分由不同研討會之講者發表其主題，我們二人參加的場次以數位鑑識及資訊安全的議題為主，為能更有效的吸收新知，如同時有 2 場相關領域之研討主題，即分開參加，本日參加之場次有「The 2012 Analysis of Information Remaining on

Computer Hard Disks offered for Sale on the Second Hand Market in the UAE」、「The 2012 investigation into remnant data on second hand memory cards sold in Australia」、「What is the proper forensics approach on trojan banking malware incidents?」、「Ethical Issues in Benevolent Hacking」、「Forensic readiness for wireless medical systems」、「Evidence examination tools for social network」及「Cloud security: A case study in telemedicine」等，內容包含市場二手硬碟及隨身碟內容資料的分析、數位網路鑑識工具、無線醫療系統、惡意程式鑑識及雲端安全，議題之範圍相當廣泛，也有許多值得本局參考之處，以二手硬碟內含資訊分析為例，有不少屬於內部機敏資料，進而思考國內民間企業乃至於公務機關廢棄儲存媒體的處理，是否已建立一套標準機制，以避免機敏資料或個人資料外洩，實有待全面檢討；至於雲端化及虛擬化課題，也是近來很熱門的話題，為響應政府節能減碳政策，降低日益龐大的資訊設備維護成本，本局近來積極導入主機虛擬化，其虛擬主機系統、網路的安全亦是本次參加場次重點之一，虛擬化的安全議題大致可分為 3 個面向：Hypervisor 弱點、虛擬網路層的弱點及 GuestOS 本身弱點，經由歸納出這 3 個弱點再設計出相對應之安全機制或設備，即可大幅提升虛擬主機的安全，本局雖於傳統資訊環境建置了相關完整的資安防護體系，但面對新型態的虛擬化平台，還須持續探討其安全防護機制之有效性。

五、 12 月 4 日上午 9:30 由 Ulster 大學 Rosemary Craig 先生演講「Getting away with murder」開始大會的議程，此議題近於刑事偵查部分，與數位鑑識較無直接關聯，接著的課程我們選擇了與資訊安全及數位鑑識近年來所面臨的一些挑戰，較相關的課程，包含「Eavesdropping on the Smart Grid」、「The security challenges and countermeasures of virtual cloud」、「Implementing a secure academic grid system」、「Does the android permission system provide adequate information privacy protection for end-users of mobile apps?」、「A proposed formula for comparing kill password effectiveness in single password RFID systems」及「The mobile execution environment: A secure and non-intrusive approach to implement a bring your own device policy for laptops」等，尤其是近來熱門的雲端運算，在資訊安全領域，如何去維持雲端服務的可用性、完整性及機密性，是政府機關和民間企業所共同重視的議題，而雲端化所帶來 BYOD (Bring Your Own Device)的趨勢，這對機關及企業亦產生了另一波更大的風險，對 BYOD 實施前資安政策制定以及使用控管之管理軟體可將風險降到最低，如何確保攜帶方便並含有敏感資料的移動裝置安全無虞，這將成為資安部門在制定移動裝置的資安政策上面臨極大的挑戰，本次會議學者僅提出 3 個導入建議：選擇安全可靠的移動裝置、部署安全軟體

及日誌送到 SOC 分析，根據以前經驗，使用者的管理才是最大成敗關鍵，尤其政府部門資料外洩事件層出不窮，往往因為使用者習慣不佳未遵守 SOP 所致，這有賴教育訓練落實及管理階層的支持；數位鑑識領域已不同於以往，過去在現場將電腦及相關儲存媒體包裝運回，即能完整蒐證，而今很多的數位證據潛藏於雲端的伺服器中，該如何去取證、保存及驗證，為今日執法機關的一大挑戰，此次研討會課程雖在此議題上著墨不多，但會間與其他國家之與會專家討論亦有收獲。

六、 12 月 5 日為研討會之最後一天，早上 9:45 會議議程在大會頒發最佳論文獎後，即由英國 Plymouth 大學 Steven Furnell 教授演講「Infosec: Lots of safeguards and no protection?」，許多資訊環境我們都安裝了防駭、防入侵的工具，但是否就真的有效果？我們須要更多費心去瞭解其效用及目的，才能真正發揮效果；接著參加之研討會課程包含「Hierarchical Attack Representation Models for Network Security Analysis」及「1st Australian e-Health Informatics and Security Conference - Special presentation」，皆是有關資訊安全的議題，演講者提出了一個演算法去計算當企業發生資安事件時，可以歸納出攻擊來源與受影響範圍，但本局轄下單位遍及各縣市且設備數量眾多，是否適用值得討論。

七、 12 月 6 日彙整此次研討會之資料，並與澳洲及香港與會者會談，交換此次研討會內容的心得，雙方介紹彼此國內資訊安全與數位鑑識現況，香港警方目前採用之工具與我們相近，但他亦提及中國大陸目前在數位鑑識領域的法規、規範及制度上，皆已十分成熟，例如可由通過認證之數位鑑識機構對數位電子媒體進行鑑識而被法院認可，而此工作的推展，實已包含對鑑識機構認證制度的建立、鑑識人員資格審核及法律面的教育及認可；另外中國大陸對於數位鑑識工具的開發及商業化，亦不遺餘力，近年來在數位鑑識之工具軟體及設備的開發及整合，已能與歐、美產品在市場上較勁，加上價格具備競爭力，對於整個數位鑑識產業未來發展十分樂觀。

八、 12 月 7 日返國。

肆、心得與建議

一、 此次赴南澳警察局參加「南澳警察鑑識工具研習營」，不僅僅在工具的使用上有很大的助益，在組織架構及案件鑑定流程上，亦有許多值得借鏡之處：

(一) 此次介紹之 2 種工具：Computer Forensic Triage Tool 及 osTriage，其一是商業公司的產品，另一種是 FBI 所免費提供之工具，二者的功能差異不大，但前者商業軟體又多具備了進階分析的功能，若要提供給很多使用者使用，例如本局各外勤人員，即需要考量成本以後者為佳；但若使用者不多，例如僅提供鑑識實驗室人員使用，考量到工具功能及未來因應新電腦系統之更新速度，以前者為佳。

而目前本局所使用之現場數位證據採證工具，因計劃推廣於外勤及中文化之考量，採委外開發而全局授權之方式，如此可降低成本，亦能具商業軟體更新之需求，此次藉由工具的學習獲得很大助益，可以提供本局未來現場工具開發時，在操作介面及功能上之參考，。

(二) 經與南澳警察局鑑識專家 Lin,Yi-Chi 博士討論，近年來數位產品更新速度快，所以案件有關的數位證據，不論是種類及數量皆大幅成長，也造成了積案問題，以南澳警方為例，2 年前普通案件約須等待 6 個月時間，而今可能需要等待 2 年方能處理，為解決這問題，南澳警方已著手進行在分局設置附屬數位鑑識中心，因澳洲幅員廣大，若能於主要城市設置數位鑑識中心，除可省去證物傳遞所造成的風險，及更能貼近辦案需求，亦能紓解案件處理速度之問題。

(三) 南澳警方科技犯罪防制部門，其下人員有警探、鑑識專家及制服警員三類人員，警探及鑑識專家皆具資訊技術背景，警探負責部門內科技犯罪偵辦業務，鑑識專家除了部門內案件外，亦須接受其他部門數位證據之鑑識工作，制服警員則負責現場蒐證之工作，亦有能力使用現場數位證據採證工具；此種分工方式與本局相近，差別在於其已建立一組制服警員，具備有基本資訊背景，藉由提供圖形化介面的一線數位證據蒐證工具，能於現場進行 Scan、Analyze 及 Act，迅速取得並作目標電腦內之資訊分類，有效協助辦理各種案件。

(四) 第 10 屆「澳洲數位鑑識會議」（The 10th Australian Digital Forensics Conference of 2012 secau Security Congress）3 天之內容包含：針對二手儲存媒體內含資訊之分析、移動裝置與網路安全、雲端資訊安全研討及手機作業系統之防

駭工具等，都有研究報告提出。在現今網路已完全融入人類生活，運用此電腦及通訊技術，提供人們學習知識、社群交流、購物等功能，而提升生活品質與效能之際；亦有違法者利用網路犯罪不易發覺真實身分之特性，使用詐騙、恐嚇、入侵、竊取資訊的方法以獲取不法所得，近年來利用網路漏洞之不法者（駭客）由單一的初學者、玩家，逐漸轉變成組織性的專家，其動機從好奇心、成就感轉換成營利、詐財等，甚者由國家、組織培養出具有特定政治目的之網路駭客組織。對此威脅，各國司法機關皆急於尋求因應之道。而本局已投入相當人力、物力，在因應高科技之網路犯罪，例如成立電腦偵辦科及資安鑑識科等單位，配置專業人力，從事網路犯罪調查及數位證據鑑識，已有相當成效；但因現今經濟犯罪、肅貪及緝毒等傳統案件類型，犯罪者皆已利用高科技產品，幾乎所有案件都與數位證據有關，造成網路調查及數位鑑識需求大量增加，如何能更有效率提升案件處理能力，實為當務之急。

藉由與香港警方李總督察的意見交流，得知許多中國大陸數位鑑識的現況，在法律、規範、認證制度及鑑識工具上，皆已相當成熟，再視台灣現況，對於數位證據的蒐證、保存、分析及報告，尚未建立法律層面的共識，司法人員及律師之法律見解不一，造成實務上做法也各行其道，所以應儘快建立國內數位鑑識之法律規範，並司法審理及判決案件中，對數位證據蒐證及鑑識程序上取得共識。

二、 策進作為：

(一) 加強工具更新：資訊產品日新月異，蒐證工具亦需不斷的進步，更要適合不同執法人員角色提供不同的工具，配合不同角色使用不同之工具，進而建立適當的教育訓練配套作為。

(二) 強化執法人員之數位證據蒐集及科技偵查能力：犯罪者今日已善於利用網路、科技犯罪，因此一般執法人員對於現代科技的瞭解，至少要有基本使用者程度，進而在外勤成立區域性之具專業技能團隊，以利協助案件偵查及數位證據初階鑑識，亦能紓解目前鑑識案件積案的問題。

(三) 藉與司法人員交流，建立其對數位鑑識之基本觀念：以中國大陸對於數位鑑識所建立的法律規範為例，我們法律對於數位鑑識的法規命令著墨太少，國內應多舉辦相關之研討會，邀請司法官及律師等法界人士參與，藉

以建立國內司法界對數位證據及數位鑑識之基本觀念。

(四) 國際合作：科技犯罪往往都有跨國之情形，為共同追查打擊犯罪，國際合作為日後必然之趨勢，此次會議與澳洲、香港之專業人士交流，皆認為網路無國界，例如網路 IP 的追查，協助追查潛逃罪犯等，須從彼此的互信及交流開始；要能有效打擊跨國犯罪，惟有加強彼此的合作。

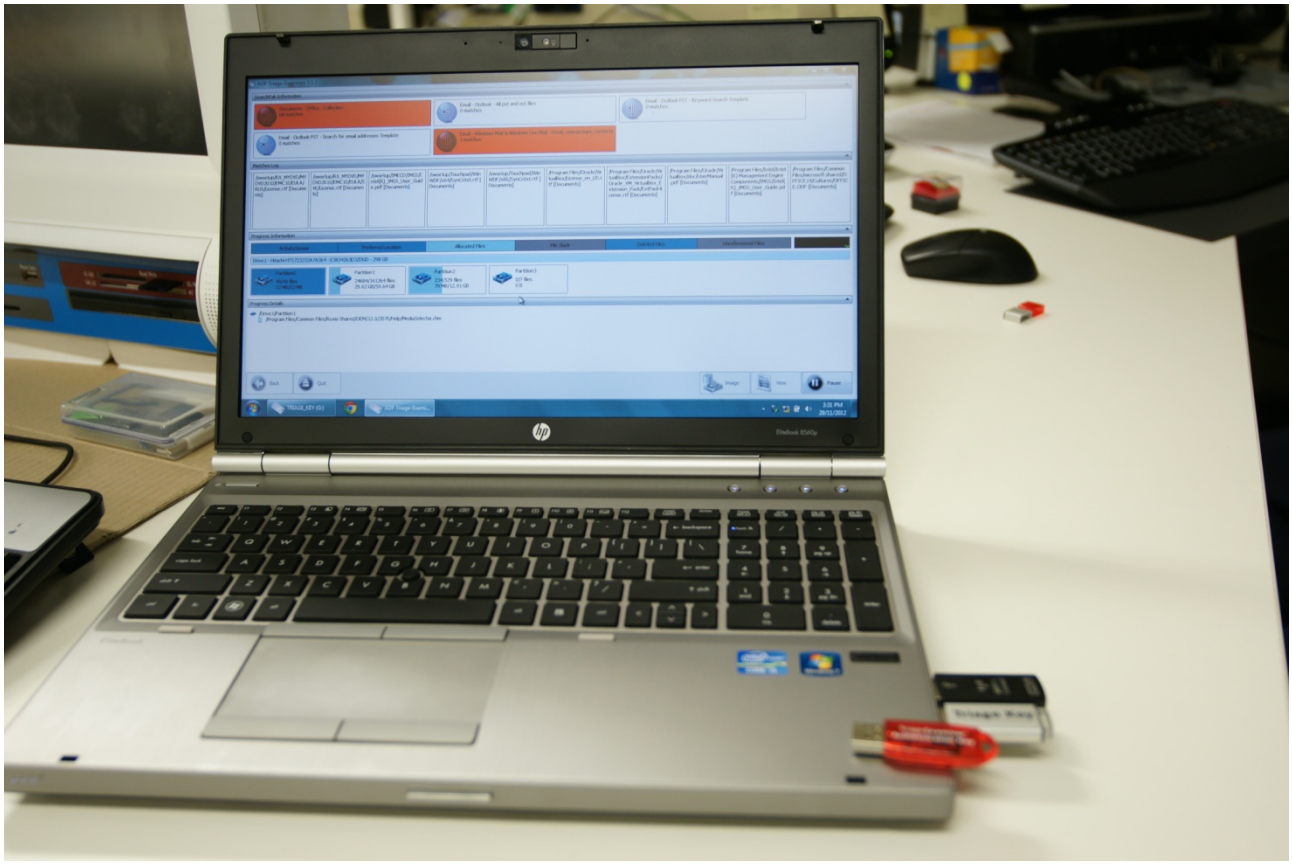
伍、附件：訓練照片、議程表及南澳警方的電腦鑑識實驗室鑑定報告 2 份

附件 1

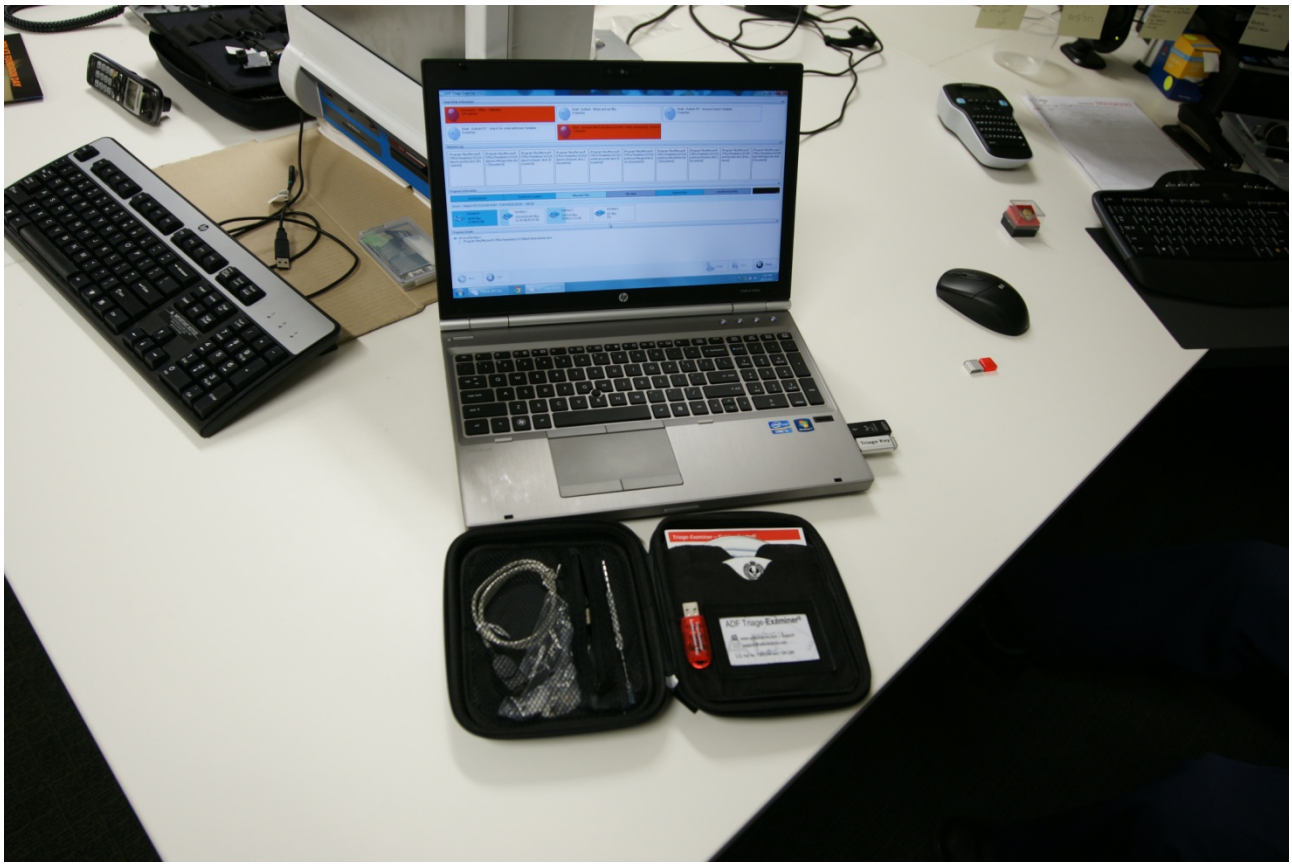
照片一：Mr. Barry 親自授課 Computer Forensic Triage Tool 的概念及使用時機

照片二：南澳警警察介紹美國聯邦調查局提供執法人員使用之工具 osTriage

照片三：osTriage 工具軟體

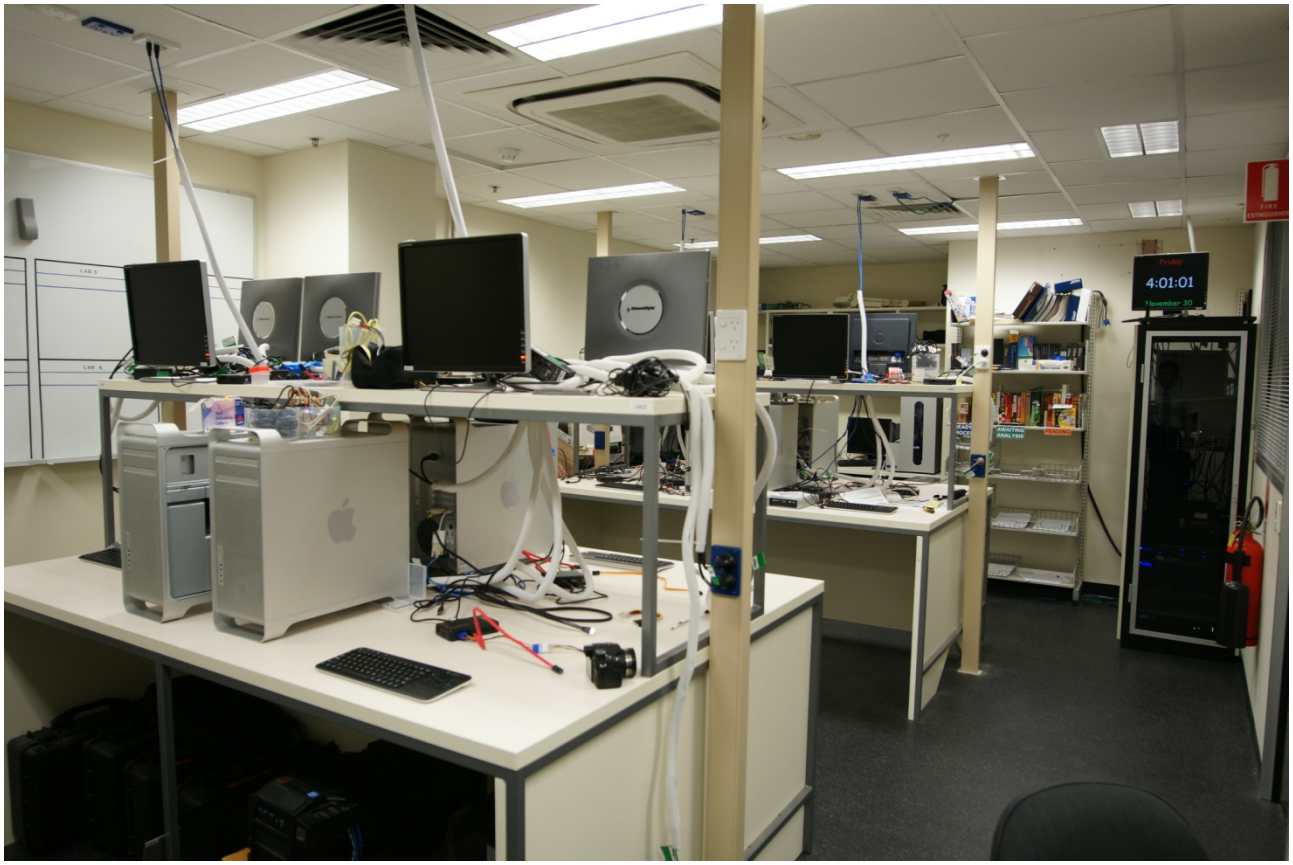


照片四：osTriage 軟體工具包



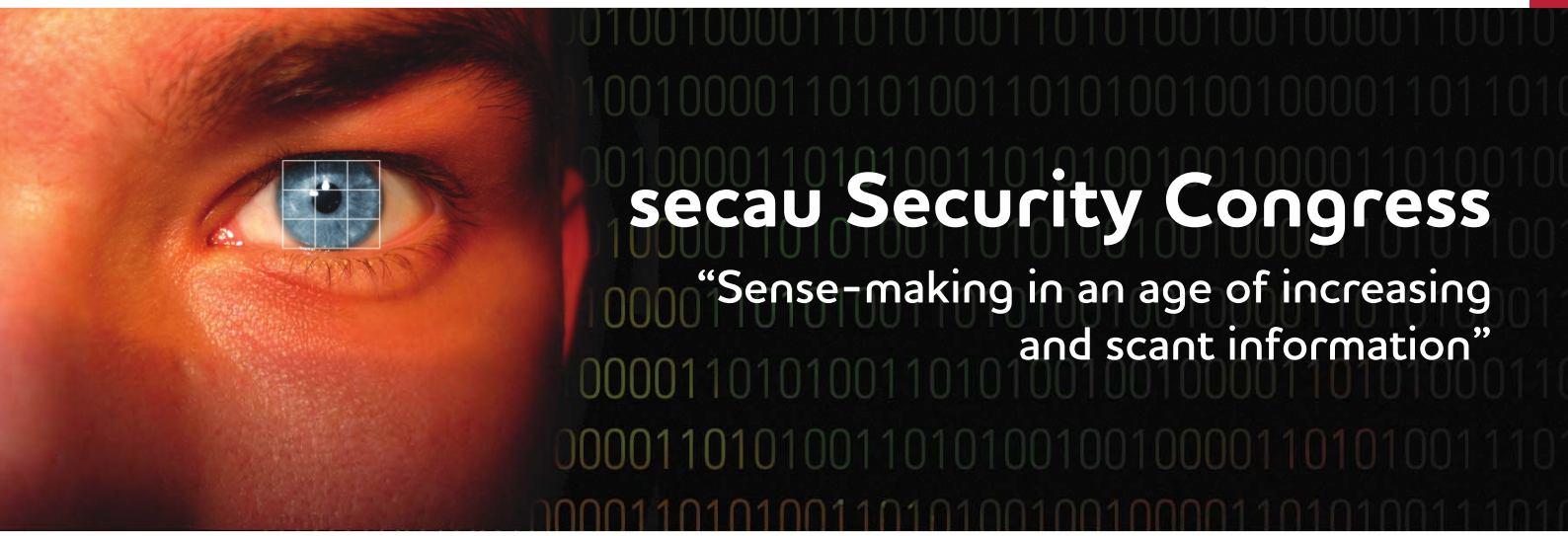
照片五：與南澳警局警探及鑑識專家 Lin,Yi-Chi 博士合照

照片六：南澳警局鑑識實驗室



照片七：澳洲數位鑑識研討會

Edith Cowan University
Security Research Institute



Program and Abstract Book

3-5 December, 2012

Novotel Langley Hotel, Perth, Western Australia

conferences.secau.org

SECAU
Securing Australia's Future

Sponsors

Emirates
Group Security
Centre of Aviation & Security Studies

woodside

Woodside is Australia's largest independent oil and gas company, with a proud history of safe and reliable operations spanning decades. We have been operating our landmark Australian project, the North West Shelf, for 28 years and it remains one of the world's premier liquefied natural gas (LNG) facilities.With the successful start-up of the Pluto LNG Plant in 2012, Woodside now operates six of the seven LNG processing trains in Australia. We strive for excellence in our safety and environmental performance and continue to strengthen our relationships with customers, co-venturers, governments and communities to ensure we are a partner of choice.

CISCO

Cisco is the worldwide leader in networking for the internet & for the cyber market is the #1 company for total Security product sales. Cisco will invest over $5.6B in R&D this year to drive innovation for our customers, with security one of our top priorities. Cisco recognizes the challenges organizations face as they seek to unleash the power of information sharing and collaboration, with the need to simultaneously safeguard your very infrastructure and resources these services depend on, through the introduction of cyber security initiatives.

SECAU
Securing Australia's Future

AUSTRALIA
ECU
EDITH COWAN
UNIVERSITY

Supporters


acs
AUSTRALIAN
COMPUTER
SOCIETY


fsm


Australia's Security Portal
MySecurity
.com.au


MSIA


hisa


ROUTLEDGE
Routledge
Taylor & Francis Group


Congress on Engineering and Technology
cet
CET


THE AUSTRALIAN AND NEW ZEALAND
FORENSIC SCIENCE SOCIETY INC.
WEST AUSTRALIAN BRANCH


APSM
ASIA PACIFIC
SECURITY
MAGAZINE


SECAU
Securing Australia's Future


AUSTRALIA
ECU
EDITH COWAN
UNIVERSITY

About the Congress

The 2012 secau Security Congress incorporates a continuum of new ideas and research ranging from digital to physical security and from highly technological solutions to human factors using scientific and socially embedded frameworks. The Congress aims to draw together competing and complementing areas of security as part of a holistic engagement with the wider security discourse.

The secau Security Congress incorporates the following conferences:

- 13th Australian Information Warfare Conference
- 10th Australian Information Security Management Conference
- 10th Australian Digital Forensics Conference
- 5th Australian Security and Intelligence Conference
- 3nd Australian Counter Terrorism Conference
- 1st Australian eHealth Informatics and Security Conference

Congress Organising Committee

Congress Chair:	Professor Craig Valli
Conference Chair (IWAR):	Dr Christopher Bolan
	Professor Matt Warren
Conference Chair (ASIC):	Mr Jeff Corkill
	Mr Michael Coole
Conference Chair (ACTC):	Mr David Cook
	Mr Michael Crowley
Conference Chair (AISM):	Dr Trish Williams
	Dr Mike Johnston
Conference Chair (ADF):	Dr Andrew Woodward
Conference Chair (AeIS)	Dr Trish Williams
	Dr Lizzie Coles-Kemp
Committee Member:	Associate Professor Ken Fowle
Committee Member:	Mr Patryk Szewczyk
Congress Organiser:	Ms Emma Burke

Keynote Speakers

Ms Rosemary Craig

Rosemary Craig spent 15 years in the private sector at senior management level in advertising, marketing and public relations. A graduate in psychology (and mature student) she relinquished her lucrative career to realise her life time passion – to read law at Queen's University Belfast. She was quickly head hunted by the Anderson McAuley retail group where her past experience in retailing coupled with her legal expertise added a further dimension to her talents. A specialist in employment law she undertook a confidential role for the Goodyear Tyre & Rubber Company Northern Ireland (NI) prior to the Company ceasing to trade in NI. As graduate from Sandhurst Military College she spent ten years, part time as an Officer in the British Army. She saw Service in some of the worst times of the NI Troubles while holding down her full time employment roles.

In the public sector she was Director & Legal Adviser to the Green Park Health Care Trust where she introduced business techniques to the Medical Profession. She graduated from the University of Leicester with a Masters Degree in International Industrial Relations and Employment Law. Her Dissertation entitled *"An Equal Force?"* focused on the role of women in management within the Royal Ulster Constabulary as espoused by the equality legislation of 1976 and mirrored the Patten Commission recommendations of its time.

The call and indeed love of the law, in tandem with academia brought her full circle back to university life. She is a law lecturer with the University of Ulster and delivers all post graduate modules. Today she tempers academia with her work in the legal profession in a continuing career. She was requested by the Office of the First and Deputy First Minister to appoint the new Northern Ireland Police Ombudsman. It is testament to her reputation for fairness and justice in the legal profession and her dealings with people that led to this prestigious appointment. She has served on the Bench of the Youth and Family Courts in the County Court Division of Belfast for the past 29 years. She was recently appointed as a European Adviser on the SMART and RESPECT European Projects due to her experience with the Security Forces and knowledge of the law.

Professor Steven Furnell

Professor Steven Furnell is the head of the Centre for Security, Communications & Network Research at Plymouth University in the United Kingdom, and an Adjunct Professor with Edith Cowan University in Western Australia. His interests include security management and culture, computer crime, user authentication, and security usability. Professor Furnell is active within three working groups of the International Federation for Information Processing (IFIP) - namely Information Security Management, Information Security Education, and Human Aspects of Information Security & Assurance. He is the author of over 220 papers in refereed international journals and conference proceedings, as well as books including Cybercrime: Vandalizing the Information Society (2001) and Computer Insecurity: Risking the System (2005). He is also the editor-in-chief of Information Management & Computer Security, and the co-chair of the Human Aspects of Information Security & Assurance (HAISA) symposium (www.haisa.org). Further details can be found at www.plymouth.ac.uk/cscan, with a variety of security podcasts also available via www.cscan.org/podcasts. Steve can also be followed on Twitter (@smfurnell).

Keynote Speakers

Mr Colin Honey

Colin Honey is an applied ethicist. For more than 20 years he was a head of College at the University of Western Australia. He was founding Director of the Kingswood Centre for Applied Ethics and taught ethics in the professions to accountants, police, nurses and doctors, dentists and media students. From Perth he went to Cambridge and he continues
there for a term every year as a member of a research team specialising in applied ethics. Otherwise he lives and works in Melbourne.
Trained in philosophy in Melbourne, theology in Cambridge, and bioethics in Edinburgh, Colin has been a visiting fellow in New York, Cambridge, and in several other centres in America. He has designed medical ethics decision-making processes which are now used in some of these centres.
Colin says that he does not aim to give answers. He says that he likes to clarify issues and stimulate others to apply their ethical principles and values consistently, coherently and inclusively.
Public policy and legislation have occupied much of his time both here and in Britain. He has given hundreds of radio broadcasts and has appeared on television on the ABC, and the Seven, Ten and Nine Networks.
He likes to see participation in decision-making; and he likes to see people making intelligent and informed decisions.
He says that his diversions include joke-telling, restoring old cars, learning Italian (and visiting Italy), learning to play the pipe-organ, and cross-cultural involvement in the community.

Mr Gavin Reid

As a computer security specialist with more than two decades of experience, Gavin Reid works with some very interesting people – from leaders in the vanguard of information security, to hackers in the computer underground. Gavin leads the Computer Security Incident Response Team at Cisco Systems – a global team of information security professionals responsible for the 24/7 monitoring, investigation and response to cyber security incidents. With annual revenue of $44 Billion and the bulk of transactions conducted over the Internet, Cisco is a prime target for cyber attack and exploitation. As an active member of the computer security community, he also supports FIRST and chairs the working group responsible for the Common Vulnerability Scoring System.
Gavin joined Cisco in 1999 from the National Aeronautics & Space Administration where he oversaw IT Security at the Johnston Space Centre. He lives in North Carolina (USA).

ABSTRACTS

Technical Difficulty: 🛠 - Low 🛠🛠 - Medium 🛠🛠🛠 - High
Unrated abstracts should be accessible to all Congress delegates

Day 1 – December 3, 2012

9:30 - 10:30

Room - Silver Room - Keynote Presentation
🛠 - Low

Mr Gavin Reid
Cisco Systems

Where automation ends and people begin

We all want a magic button that fixes our network security problems. Automated tools can improve a weak computer security posture by preventing new infections and disrupting command and control channels. In reality, though, the scope of these tools will always be limited to the most basic of attacks. A strong security posture requires not only automated equipment, but people to program the equipment and to act on its output. Cisco CSIRT (Cisco Security Incidents & Response Team) has taken a pragmatic approach where automated equipment better serves the purpose of providing intelligence to highly-trained IT staff, rather than attempting to replace the security staff.

10:30 – Morning Tea

11:00 - 11:30

Room - Ballroom North

Creating a counter-insurgency plan: elements required based upon a comparative analysis of research findings

W. J Bailey
Security Research Institute, Edith Cowan University

The development of a counter-insurgency doctrine is an evolutionary process: no two insurgencies are the same. However, certain fundamental principals remain consistent and these can be applied to meet the required circumstances. The creation of an overarching plan encompassing a combination of military, political and social actions under the strong control of a single authority is central. Therefore, understanding the basics allows for the development of a tactical strategy based upon a structured plan. Compiling the 'Plan' should be based upon the lessons learnt from the past. To this end, the methodology used is supported by a literature review and interviews from participants in a limited assessment of the two historical conflicts: Malaya and Kenya.

Based upon the findings, a condensed table is presented to aid analysis, using a French doctrinal approach as a tool for interpretation. In addition, this is supported by quotes from the respondents involved in the research process. These findings are the preliminary results of a research study looking at what was effective during the prosecution of the selected insurgencies. Outcomes indicate that the fundamental principals are pertinent today and are therefore generally applicable.

Room - Boardroom
🛠 - Low

The 2012 Analysis of Information Remaining on Computer Hard Disks offered for Sale on the Second Hand Market in the UAE

Andrew Jones, Thomas Martin, Mohammed Al Zaabi
Khalifa University

The growth in the use of computers has continued to increase to the point where desktop, laptop, netbook or tablet computers are now almost essential in the way that we communicate and work. As a result of this, and the fact that these devices have a limited lifespan, enormous numbers of computers are being disposed of at the end of their useful life by individuals or/and organisations. If not properly cleansed of data when they are released into the public domain they may contain data that is sensitive to the organisation or the individual and which may be relatively up to date. This research describes the first survey of data remaining on computer hard disks sold on the second hand market in the United Arab Emirates (UAE). It was undertaken to gain insight into the volumes and sensitivity of data found on disks purchased in the UAE and to gain an understanding of the relative level of the problem of residual data in the UAE. Disks were purchased

anonymously from shops, on-line auctions and personal advertisements, then analysed to determine whether any data could be recovered and if so, whether it could be used to determine the previous owner.

Room - Langley Room

Developing governance capability to improve information security resilience in healthcare

Rachel Mahncke, PIBT
Patricia Williams, School of Computer and Security Science, Security Research Institute
Edith Cowan University

General medical practices' in Australia are vulnerable to information security threats and insecure practices. It is becoming well accepted in the healthcare environment that information security is both a technical and a human endeavour, and that the human behaviours, particularly around integration with healthcare workflow, are key barriers to good information security practice. This paper develops a holistic capability approach to information security by completing a preliminary iteration of mapping operational capabilities to governance capabilities. Using an operational backup capability matrix exemplar, the approach is analysed against the governance policy capability matrix. The resultant mapping between the operational and governance capability frameworks demonstrates that resilience can be promoted through sound governance. This implies that improved security performance and compliance contributes to measurement and oversight of the governance processes thereby making the organisations demonstrably more resilient to security threats. This paper proposes the need for a holistic capability approach to information security.

Room - Silver Room

A Survey of Computer and Network Security Support from Computer Retailers to Consumers in Australia

Patryk Szewczyk, School of Computer and Security Science, Security Research Institute
Edith Cowan University

Previously undertaken research suggests that novice end-users rely on computer retailers for security advice and support during and after a sale has occurred. This paper documents the survey results of computer and network security support provided to consumers by retailers in Perth, Western Australia between 2011 and 2012. The conducted survey shows that in the majority of cases, computers retailers were favourable in providing support and recommendations. However, these views were found to be flawed, confusing and do little to ensure that end-users are not victimized by cyber crime.

11:30 - 12:00

Room - Ballroom North

Defence in Depth, Protection in Depth and Security in Depth: A comparative analysis towards a common usage language

Jeff Corkill, Michael Coole, Andrew Woodward
School of Computer and Security Science, Security Research Institute, Edith Cowan University

A common language with consistency of meaning is a critical step in the evolution of a profession. Whilst the debate as to whether or not security should be considered a profession is ongoing, there is no doubt that the wider community of professionals operating in the security domain are working towards achieving recognition of security as a profession. The concepts of defence in depth, protection in depth and security in depth have been used synonymously by different groups across the domain. These concepts represent the very foundation of effective security architecture are hierarchical in nature and have specific meaning. This paper through comparative analysis clearly defines the difference between and establishes the hierarchy such that a common understanding can be achieved.

Room - Boardroom

🛠 - Low

The 2012 investigation into remnant data on second hand memory cards sold in Australia

Patryk Szewczyk, Krishnun Sansurooah
School of Computer and Security Science, Security Research Institute, Edith Cowan University

This study investigates the remnant data on memory cards that were purchased through Australian second hand auctions sites in 2012. Memory cards are increasing in capacity and are commonly used amongst many consumer orientated electronic devices including mobile phones, tablet computers, cameras and multimedia devices. This study examined 78 second hand memory cards. The investigation shows that confidential data is present on many of the memory cards and that in many instances there is no evidence to suggest that the seller attempted to erase data. In many instances the sellers are asking the buyer the erase the data on the memory card. It is evident through this research that consumers are not appropriately informed of the dangers of disposing of personal media through second hand auction sites. Subsequently consumers do not take the appropriate actions to remove data.

Room - Langley Room

Building patient trust in electronic health records

Helen Cripps, Craig Standing
The Centre for Innovative Practice, Edith Cowan University

While electronic medical records have the potential to vastly improve a patient's health care, their introduction also raises new and complex security and privacy issues. The challenge of preserving what patients' believe as their privacy in the context of the introduction of the Personally Controlled Electronic Health Record (PCEHR), into the multi-layered and decentralised Australian health system is discussed. Based on a number of European case studies the paper outlines the institutional measures for privacy and security that have been put in place, and compares them with the current status in Australia. The implementation of the PCEHR has not been as straight forward, holistic or as uniform as in the European countries' studied. This has meant that issues around personal privacy and security have not been addressed in an effective and functional manner. Surprisingly, the researchers found that the patient is absent in the PCEHR privacy and security discussion; and their perceptions of, and requirements for privacy and secure management of their medical information is absent. The concept of personal privacy and security has yet to be fully explored from the patient's perspective, despite it being a Personally Controlled Health Record.

Room - Silver Room

🛠 - Low

Web-based risk analysis for home users

R.T. Magaya[1] & N.L.Clarke[1,2,] [1]Centre for Security, Communications & Network Research (CSCAN), Plymouth University, UK, [1,2]School of Computer and Security Science, Edith Cowan University, Western Australia

The advancement of the Internet has provided access to a wide variety of online services such as banking, e-commerce, social networking and entertainment. The wide availability and popularity of the Internet has also led to the rise in risks and threats to users, as criminals have taken an increasingly active role in abusing innocent users. Current risk analysis tools, techniques and methods available do not cater for home users but are tailored for large organisations. The tools require expertise to use them and they are expensive to purchase. What is available for home users are generic information portals that provide a whole-host of awareness raising information, much of which will have varying degrees of usefulness depending upon the particular individual, their technology usage and prior knowledge. As such a tool is required that can bridge the gap between bespoke risk assessment approaches that provide tailored information and broad-spectrum approaches that simply provide all information regardless of its relevance. The paper proposes a web-based risk analysis tool for home users that is simple to use, requires no prior knowledge or expertise of security and can provide bespoke and tailored guidance on improving a user's security posture. The tool follows a simple step procedure for gathering key asset and behavioural information to inform the risk profiling process. A prototype was developed and evaluated by a sample of home users and 93% of the participants found the tool to be helpful and very informative.

12:00 - 12:30

Room - Ballroom North

The intelligence game:
Assessing delphi groups and structured question formats

Bonnie Wintle[1], Steven Mascaro[2], Fiona Fidler[1], Marissa McBride[1], Mark Burgman[1]Louisa Flander[3], Geoff Saw[4], Charles Twardy[5], Aidan Lyon[6] & Brian Manning[1], [2] Bayesian Intelligence,Melbourne[3] ACERA, School, Population Health, University of Melbourne,[4] School of Psychological Sciences, University of Melbourne, [5] C4I Center, George Mason University, USA[6] Department of Philosophy, University of Maryland, USA

In 2010, the US Intelligence Advanced Research Projects Activity (IARPA) announced a 4-year forecasting "tournament". Five collaborative research teams are attempting to outperform a baseline opinion pool in predicting hundreds of geopolitical, economic and military events. We are contributing to one of these teams by eliciting forecasts from Delphi-style groups in the US and Australia. We elicit probabilities of outcomes for 3-5 monthly questions, such as "will Australia formally transfer uranium to India by 1 June 2012"? Participants submit probabilities in a 3-step interval format, view those of others in their group, share, rate and discuss information, and then make a second private judgement. Performance is assessed using Brier scores.

After Year 1, we ranked second of five teams in the competition. The Brier scores from the US Delphi groups improved on the baseline scores by 10%, the prediction market operated by our team in the US beat the baseline by 47%, and the Australian Delphi groups outperformed the baseline by 51% (answering different, matched questions to the US groups). The Australian groups were more socially and demographically diverse than the US groups. Group diversity may be an important factor determining the forecasting performance of the aggregated predictions.

Room - Boardroom
🛠🛠 - Medium

What is the proper forensics approach on trojan banking malware incidents?

Andri P Heriyanto
School of Computer and Security Science, Edith Cowan University

Digital forensics procedures should be developed to obtain digital evidence with regard to legal requirements such as admissibility, authenticity, completeness, reliability and believability. On the other hand, Trojan banking malware incident has grown significantly and creates a great threat to online banking users globally. This type of malware is known to use anti-forensic techniques to avoid forensic detection. Moreover, there are numerous works and researches that impose the drawbacks on post-mortem forensics approach in dealing with evidence that only resided on non-persistence memory or non-volatile memory. There are works that reveal the disadvantage of live-response approach on incident response that might compromise the evidence as well. For the last four years, there has been notable development of memory forensic approaches that focus on malware incidents. This paper demonstrates the procedures that use three different forensics approaches on three different Trojan banking malware samples: Cridex, ZeuS and SpyEye. The aim of this work is to obtain the proper forensics approach on Trojan banking malware incidents. The paper also uses a network forensics approach to gather and analyse the network-based evidence.

Room - Langley Room

A holistic approach to ehealth security in Australia: developing a national ehealth security and access framework (nesaf)

Yvette Lejins, John Leitch, National E-Health Transition Authority (NEHTA)

The Australian ehealth landscape is confronted with new challenges for healthcare providers in appropriately managing and protecting personal health information. The vision of the National eHealth Security and Access Framework (NESAF) is to adopt a consistent approach to the application of health information security standards and provide better practice guidance in relation to eHealth specific security and access practices. The eHealth information security landscape has a number of unique attributes, many that are faced by other business that provide a service or products – but we see that there is no industry in Australia where such widespread changes in the access to, the creation and delivery of information is transpiring. As the significant investment in Australian eHealth unfolds the emerging threat and risk assessment for information security and access is more prominent. There is an increasing volume of information being exchanged and accessed, and that this will occur in novel ways supporting emerging clinical models and to meet patient needs and growing expectations from the information age. One key area that must be examined is data provenance, ensuring that all electronic health information is traceable from its creation at a verifiable trusted source, and through its transition and possible augmentation enroute to its destination for immediate and potential futures uses. This will support better health outcomes for patients, and also the use of the information to support tertiary and secondary uses. For example, Clinical Research may generate personal health content in the context of a clinical trial and its context of use bound to the research environment in which it was generated. The goals and principles of the NESAF are intended to guide in the design and implementation of secure eHealth systems to manage and protect healthcare information. This paper presents a description and discussion of the NESAF framework, and the work that has driven its formulation.

Room - Silver Room
🛠 - Low

An information security awareness capability model (isacm)

Robert Poepjes and Michael Lane
School of Information Systems, University of Southern Queensland

A lack of information security awareness within some parts of society as well as some organisations continues to exist today. Whilst we have emerged from the threats of late 1990s of virus such as Code Red and Melissa, through to the phishing emails of the mid 2000's and the financial damage some such as the Nigerian scam caused, we continue to react poorly to new threats such as demanding money via SMS with a promise of death to those that won't pay. So is this lack of awareness translating into problems within the workforce? There is often a lack of knowledge as to what is an appropriate level of awareness for information security controls across an organisation. This paper presents the development of a theoretical framework and model that combines aspects of information security best practice standards as presented in ISO/IEC 27002 with theories of Situation Awareness. The resultant model is an information security awareness capability model (ISACM). A preliminary survey is being used to develop the Awareness Importance element of the model and will leverage the opinions of information security professionals. A subsequent survey is also being developed to measure the Awareness Capability element of the model. This will present scenarios that test Level 1 situation awareness (perception), Level 2 situation awareness (comprehension) and finally Level 3 situation awareness (projection). Is it time for awareness of information security to now hit the mainstream of society, governments and organisations?

12:30 Lunch

1:30 - 2:30

Room - Silver Room - Keynote Presentation

Mr Colin Honey
University of Cambridge
Hacktivism: Ethical Issues in Benevolent Hacking

2:30 - 3:00

Room - Ballroom North
🛠🛠 - Medium

Understanding the vulnerabilities in Wi-Fi and the impact on its use in CCTV systems

Craig Valli, Andrew Woodward, Michael Coole
Security Research Institute, Edith Cowan University

Modern surveillance devices are increasingly being taken off private networks and placed onto networks connected via gateway to the Internet or into Wi-Fi based local area wireless networks (LAWN). The devices are also increasingly using IPv4 and IPv6 network stacks and some form of embedded processing or compute built in. Additionally, some specialist devices are using assistive technologies such as GPS or A-GPS. This paper explored the issues with use of the technologies in a networked environment, both wireless and internetworked. Analysis of these systems shows that the use of IP based CCTV systems carries greater risk than traditional CCTV systems, primarily due to the exposure to IP based vulnerabilities. Furthermore, Wi-Fi based IP CCTV systems are additionally susceptible to remote, physical denial of service attacks due to the broadcast nature of wireless communication systems. Interception of traffic is possible with IP based systems, and again, Wi-Fi IP based CCTV systems are more susceptible due to protocol vulnerabilities and lack of processing power. The paper concludes that more research is needed in this area to identify and classify generic vulnerabilities that these systems are vulnerable to, and to present a framework which can be used to mitigate the risk of adopting these systems.

Room - Boardroom
🛠🛠 - Medium

Forensic readiness for wireless medical systems

Brian Cusack; Ar Kar Kyaw
AUT University, Auckland New Zealand

Wireless medical devices and related information systems are vulnerable to use and abuse by unauthorized users. Medical systems are designed for a range of end users in different professional skill groups and also people who carry the devices in and on their bodies. Open, accurate and efficient communication is the priority for medical systems and as a consequence strong protection costs are traded against the utility benefits for open systems. Flexible security provisions are required and strong forensic capabilities built into the systems to treat the risk. In this paper we elaborate the problem area and discuss potential solutions to ready a medical system for the trade-off of open and secure services.

Room - Langley Room
🛠 - Low

Mobile Device Management for Personally Controlled Electronic Health Records: Effective Selection of Evaluation Criteria

Murray Brand, Patricia A. H. Williams,
School of Computer and Security Science, Security Research Institute
Edith Cowan University

Enterprises are faced with the task of managing a plethora of mobile computing devices in the workplace that are employed for both business purposes and private use. This integration can contribute to the demands of security protection and add significant threats to the enterprise. The introduction of the Personally Controlled Electronic Health Record (PCEHR) system is a significant step in e-health for Australia and will likely result in sensitive information being accessed from mobile computing devices. Mobile Device Management (MDM) offers a potential solution to manage these devices, however there is a variety of vendors with a range of solutions. This paper presents preliminary research into a generic methodology that could be used to assist the enterprise in the MDM selection process particularly when mobile devices will eventually integrate with the Australia's PCEHR.

Room - Silver Room
🛠🛠🛠 - High

Human-readable Real-time Classifications of Malicious Executables

Anselm Teh, Arran Stewart
Defence Science and Technology Organisation

Shafiq et al. (2009a) propose a non–signature-based technique for detecting malware which applies data mining techniques to features extracted from executable files. Their technique has a high level of accuracy, a low false positive rate, and a speed on par with commercial anti-virus products. One portion of their technique uses a multi-layer perceptron as a classifier, which provides little insight into the reasons for classification. Our experience is that network security analysts prefer tools which provide human-comprehensible reasons for a classification, rather than operating as "black boxes". We therefore build on the results of Shafiq et al. by demonstrating a technique which uses decision trees to distinguish packed from non-packed files, producing a classification diagram which can be understood by analysts. We show that the resulting detector still provides high accuracy and classifies files rapidly.

3:00 - 3:30

Room - Ballroom North - *No presentation*

Room - Boardroom
🛠🛠 - Medium

Secure key deployment and exchange protocol for manet information management

Brian Cusack; Alastair Nisbet, AUT University, Auckland New Zealand

Secure Key Deployment and Exchange Protocol (SKYE) is an innovative encryption Key Management Scheme (KMS) based on a combination of features from recent protocols combined with new features for Mobile Ad Hoc Networks (MANETs). The design focuses on a truly ad hoc networking environment where geographical size of the network, numbers of network members and mobility of the members is all unknown before deployment. This paper describes the process of development of the protocol and the application to system design to assure information security and potential evidential retention for forensic purposes. Threshold encryption key management is utilized and simulation results show that security within the network can be increased by requiring more servers to collaborate to produce a certificate for a new member, or by requiring a higher trust threshold along the certificate request chain. The cost of information management (eg. time, processor use and battery use in mobile devices) is also a consideration.

Room - Langley Room

Accountable-EHealth Systems: The next step forward for privacy

Randike Gajanayake[1], Renato Iannella[1, 2], Bill Lane[3, 4] and Tony Sahama[1,5], [1]Science and Engineering Faculty, Queensland University of Technology, [2]NEHTA, [3]Faculty of Law, Queensland University of Technology, [4]Clayton Utz

EHealth systems promise enviable benefits and capabilities for healthcare, yet the technologies that make these capabilities possible brings with them undesirable drawback such as information security related threats which need to be appropriately addressed. Lurking in these threats are patient privacy concerns. Resolving these privacy concerns have proven to be difficult since they often conflict with information requirements of healthcare providers. It is important to achieve a proper balance between these requirements. We believe that information accountability can achieve this balance. In this paper we introduce accountable-eHealth systems. We will discuss how our designed protocols can successfully address the aforementioned requirement. We will also compare characteristics of AeH systems with Australia's PCEHR system and identify similarities and highlight the differences and the impact those differences would have to the eHealth domain.

Room - Silver Room
🛠🛠 - Medium

An investigation into the wi-fi protected setup pin of the linksys wrt160n v2

Symon Aked[1], Christopher Bolan[1,2], Murray Brand[1,2]
[1]School of Computer and Security Science, [2]ECU Security Research Institute, Edith Cowan University

Wi-Fi Protected Setup (WPS) is a method of allowing a consumer to set up a secure wireless network in a user friendly way. However, in December 2011 it was discovered that a brute force attack exists that reduces the WPS key space from 10^8 to 10^4+10^3. This resulted in a proof of concept tool that was able to search all possible combinations of PINs within a few days.

This research presents a methodology to test wireless devices to determine their susceptibility to the external registrar PIN authentication design vulnerability. A number of devices were audited, and the Linksys WRT160N v2 router was selected to be examined in detail. The results demonstrate that the router is highly susceptible to having its WPS PIN brute forced. It also details that even with WPS disabled in the router configuration, WPS was still active and the PIN was equally vulnerable.

3:30 – Afternoon Tea

4:00 -4:30

Room - Ballroom North

Representing Variable Source Credibility in Intelligence Analysis with Bayesian Networks

Ken McNaught, Cranfield University

Assessing the credibility of an evidential source is an important part of intelligence analysis, particularly where human intelligence is concerned. Furthermore, it is frequently necessary to combine multiple items of evidence with varying source credibilities. Bayesian networks provide a powerful probabilistic approach to the fusion of information and are increasingly being applied in a wide variety of settings. In this paper we explore their application to intelligence analysis and provide a simple example concerning a potential attack on an infrastructure target. Our main focus is on the representation of source credibility. While we do not advocate the routine use of quantitative Bayesian networks for intelligence analysis, we do believe that their qualitative structure offers a useful framework for evidence marshalling. Furthermore, we believe that quantified Bayesian networks can also play a part in providing auxiliary models to explore particular situations within a coherent probabilistic framework. This process can generate fresh insights and help to stimulate new hypotheses and avenues of enquiry.

Room – Boardroom

🛠🛠 - Medium

Evidence examination tools for social networks

Brian Cusack; Jung Son, AUT University, Auckland New Zealand

Social networking (SNS) involves computer networks and billions of users who interact for a multiplicity of purposes. The web based services allow people to communicate using many media sources and to build relationship networks that have personalized meanings. Businesses and Governments also exploit the opportunity for economical consumer interaction. With the valued use of SNS services also comes the potential for misuse and legal liability. In this paper three software tools are tested in the laboratory to assess the capability of the tools to extract files from the four most popular web browsers while browsers are being used to surf the three most popular SNS sites, Facebook, Twitter, and LinkedIn. The results showed that the capability for evidence extraction differed markedly between tools indicating that the use of a particular tool has a material impact if the files are being extracted for evidential purpose.

Room - Langley Room

eHealth in Australia and elsewhere: A comparison and lessons for the near future

Randike Gajanayake[1], Tony Sahama[1,] and Renato Iannella[1, 2]
[1]Science and Engineering Faculty, Queensland University of Technology [2]NEHTA

Meticulous planning and preparation do not always guarantee that eHealth programs unfold as predicted. Ehealth entails interdependent social interactions which are difficult to predict without past experience or reference to lessons learned. Judicious insight into past case studies and eventualities, therefore, is essential towards building a successful eHealth solution. Australia's eHealth program is at a crucial stage where appropriate policy considerations and operational changes are in order. In this paper, we present an initial exploration of prominent eHealth initiatives of other countries to identify similarities, differences and to seek lessons towards making Australia's eHealth initiative a better journey.

Room - Silver Room
🛠🛠 - Medium

Experimenting with Anomaly Detection by Mining Large-Scale Information Networks

A.Taleb-Bendiab, School of Computer and Security Science
Edith Cowan University

Social networks have formed the basis of many studies into large networks analysis. Whilst much is already known regarding efficient algorithms for large networks analysis, data mining, knowledge diffusion, anomaly detection, viral marketing, to mention. More recent research is focussing on new classes of efficient approximate algorithms that can scale to billion nodes and edges. To this end, this paper presents an extension of an algorithm developed originally to analyse large scale-free autonomic networks called – the Global Observer Model. In this paper, the algorithm is studied in the context of monitoring large-scale information networks. Hence, taking into account the size of such networks, the proposed algorithm starts by partitioning the graph using structural network metrics. This is followed by a calculation of the graph nodes' metrics, which are used in the selection from the original graph a subset of nodes to be monitored. The paper is organised as follows: it will outline the problem definition and algorithm, then will proceed to a brief description of an event and signature based model used to instrument monitored nodes. Finally, the paper will conclude with an evaluation using an infection detection scenario, which will be followed by a general discussion and proposed further works.

4:30 - 5:00

Room - Ballroom North - *No presentation*

Room - Boardroom

Protective Emblems in Cyber Warfare

Iain Sutherland[1,2,3] , Konstantinos Xynos[1], Andrew Jones[1,3,4], Andrew Blyth[1],
[1]University of Glamorgan, Treforest, UK., [2] Noroff University College, Kristiansand, Norway, [3]Edith Cowan University, Australia., [4]Khalifa University of Science, Technology & Research, UAE

The Tallinn Manual will be released in February 2013 and makes a significant step towards defining the concepts of cyber warfare. The early draft of the manual is available and the expert working party has interpreted the existing international agreements, instruments and conventions and applied them to the field of cyber warfare. The Manual makes a number of interpretations on the legal position of civilians and other parties that should be viewed as non-combatants during a cyber conflict. The manual makes it clear that the existing conventions are applicable and that civilian / religious and medical systems should be viewed as non-combatants in a cyber conflict. In the kinetic warfare environment non-combatants are indicated with recognized international symbols such as the Red Cross, Red Diamond and the Red Crescent. This paper proposes a simple method in which these and other symbols for protected sites could be replicated in the cyber world with a form of a digital marker to ensure that systems and traffic are recognized as being clearly protected under the Geneva Conventions.

Room - Langley Room

Cloud security: A case study in telemedicine

Michael N. Johnstone
School of Computer and Security Science, Security Research Institute
Edith Cowan University

Security as part of requirements engineering is now seen as an essential part of systems development in several modern methodologies. Unfortunately, medical systems are one domain where security is seen as an impediment to patient care and not as an essential part of a system. Cloud computing may offer a seamless way to allow medical data to be transferred from patient to medical practitioners, whilst maintaining security requirements. This paper uses a case study to investigate the use of cloud computing in a mobile application for Parkinson Disease. It was found that functionality took precedence over security requirements and standards.

Room - Silver Room
🛠🛠 - Medium

A quantitative survivability test method in the large scale network based on SD pairs

Ming Liang, Tang Jian
Beijing Institute of System Engineering, China

Survivability is a necessary property of network system in disturbed environment. A survivable network always experiences five phases, i.e., normal phase, resistance phase, destroyed phase, recovery phase, and adaptation and evolution phase, in

its survivable process. This paper concludes the network survivability into a novel composite metric—Network Recovery Time. In order to measure this metric in quantity, a concept of Source-Destination Pair, i.e. SD Pair, is created to abstract an end-to-end activity in the network, and the quality of SD Pair is also used to describe the network performance, such as connectivity, quality of service, link degree, and so on. After that, a test method based on SD Pair for calculating the Network Recovery Time is provided. Analysis shows that the method can be used to test and evaluate quantitative survivability of a large scale network.

5:30 - 7:30

Please join us at the Senses -South Lounge on the entrance level of the Novotel Langley Hotel for the secau Security Congress welcome reception

Day 2 – December 4, 2012

9:30-10:30

Room - Silver Room - Keynote Presentation

Rosemary Craig
University of Ulster

Getting away with murder

In 2009 the news that the renowned Northern Ireland dentist Dr Colin Howell and his former lover Hazel Buchanan had murdered their respective spouses in 1991 was something of a sensation. The fact that lies, intrigue, sex and Christianity were all bound up in a web of deceit rocked the Province. Colin Howell had confessed to police and pleaded guilty in his subsequent Court Hearing.

In 1991 two bodies were found in a car in a garage. Police were satisfied that the pair, a serving Police Officer and father to two young children, *(the husband of Hazel Buchanan)* and the wife of a local dentist and mum to four children under the age of five (*Lesley Howell*) had committed suicide. This conclusion by police was despite the fact that it was known that it was their respective spouses who were *'having an extra marital affair.'* Had the *'lovers'* got away with *'the perfect murder?'* It was only some 18 years later when Colin Howell confessed to these murders that the shock waves were felt in every quarter.

The investigation by the Police Service of Northern Ireland in 2009 into the murders led to a guilty plea from Colin Howell. His former lover Hazel Buchanan, *(now Stewart)* remarried at this time to a retired police Superintendent pleaded *'not guilty.'* During the most sensational criminal trial ever seen in Northern Ireland, Howell gave evidence against Hazel Stewart for the Crown and she exercised her *'right to silence'*. A jury unanimously found Stewart guilty of the double murders. She intends to appeal her conviction. How did they get away with murder for so long? Why did the original police investigation get it so wrong? What did the police ombudsman for Northern Ireland conclude?

All of these questions will be addressed by Rosemary in her keynote address. Rosemary will set the scene by discussing how the dentist and his young lover felt they were *"Waltzing in Time"* as they plotted to kill their spouses in what appeared to be the *'perfect murder'*. Why did Colin Howell confess? Rosemary will deliver some incredible facts about this case during her presentation.

10:30 - Morning Tea

11:00 - 11.30

Room - Ballroom North

A model of psychological disengagement

Kira J. Harris, Edith Cowan University

This paper presents the preliminary findings of research into the disengagement from highly entitative and ideological social groups, such as one percent motorcycle clubs, military Special Forces and fundamental ideological groups. Using a grounded theory approach, the discourse of 25 former members identified the discrepancy between group membership and the self-concept as the core theme in the disengagement experience. This model presents the process of experiencing a threat, self-concept discrepancy and management, physical disengagement and the post-exit identity. The findings indicate a consistent experience of disengagement and allow further understanding to the factors influencing membership appraisal.

Room - Boardroom
🛠🛠 - Medium

Eavesdropping on the Smart Grid

Craig Valli, Andrew Woodward, Peter Hannay, Murray Brand, Clinton Carpene, Chris Holme & Reino Karvinen
Security Research Institute, Edith Cowan University

An *in situ* deployment of smart grid technology, from meters through to realise through to access points and wider grid connectivity, was examined. The aim of the research was to determine what vulnerabilities were inherent in this deployment, and what other consideration issues may have led to further vulnerability in the system. It was determined that there were numerous vulnerabilities embedded in both hardware and software and that consideration issues further compounded these vulnerabilities. He cyber threat against critical infrastructure has been public knowledge for several years, and with increasing awareness attention and resource being devoted to protecting critical in the structure, it is concerning that a technology with the potential to create additional attack vectors is apparently insecure.

Room - Langley Room

Legal issues related to Accountable-eHealth systems in Australia

Randike Gajanayake[1], Bill Lane[1, 2], Renato Iannella[1, 3] and Tony Sahama[1,4]
[1]Science and Engineering Faculty, Queensland University of Technology
[2]Clayton Utz, [3]NEHTA

Information privacy requirements of patients and information requirements of healthcare providers (HCP) are competing concerns. Reaching a balance between these requirements have proven difficult but is crucial for the success of eHealth systems. The traditional approaches to information management have been preventive measures which either allow or deny access to information. We believe that this approach is inappropriate for a domain such as healthcare. We contend that introducing information accountability (IA) to eHealth systems can reach the aforementioned balance without the need for rigid information control. IA is a fairly new concept to computer science, hence, there are no unambiguously accepted principles as yet. However, the concept delivers promising advantages to information management in a robust manner. Accountable-eHealth (AeH) systems are eHealth systems which use IA principles as the measure for privacy and information management. AeH systems face three main impediments; technological, social and ethical and legal. In this paper, we present the AeH model and focus on the legal aspects of AeH systems in Australia. We investigate current legislation available in Australia regarding health information management and identify future legal requirements if AeH systems are to be implemented in Australia.

Room - Silver Room
🛠🛠 - Medium

A novel network survivability analysis and evaluation model

Wang Chunlei
Beijing Institute of System Engineering, China

With the increase of network complexity and continuous development of network attack techniques, network survivability technologies are becoming more and more important in the network security domain. Network survivability has the characteristics of complexity, dynamic evolution and uncertainty, which has become one of the most important factors for analysing and evaluating network performance. Network survivability analysis and evaluation is a process of analysing and quantifying the degree to which network systems can survive in network threats. This paper proposes a novel network survivability analysis and evaluation model. Firstly, network survivability is abstracted as a dynamic game process among network attacker, network defender and normal user, thereafter network survivability evolutionary game model is established and network survivability analysis algorithm is proposed based on the game model. Secondly, the survivability characteristics of the network can be measured and evaluated based on the analysed information and based on the proposed immune evolutionary algorithm for network survivability metric weight solving and network survivability evaluation method using multiple criteria decision making. Finally, the proposed network survivability analysis and evaluation model is experimented in a typical network environment and the correctness and effectiveness of the model is validated through experimental analysis.

11:30 - 12:00

Room - Ballroom North

The Deradicalisation of Terrorists

Jason-Leigh Striegher, Doctoral Candidate

Governments today tend to grapple with the development and implementation of deradicalisation programs; and as such, the results of such programs have led to varying degrees of success. The programs of three nation states — Yemen, Saudi Arabia and Indonesia have been selected for discussion due to the diversity of programs used in these Islamic states. This paper focuses on the distinction between disengagement and deradicalisation; and identifying and understanding the affects that push and pull factors potentially have to extricate identified terrorists from violent extremism. It also highlights Jack Roche as an example of someone that in general deradicalised himself as a result of push and pull factors.

"If the development of terrorism is a product of its own time and place, it follows that issues of disengagement (and all that that implies) will also be context-specific and necessarily nuanced … in terms of how the programmes are constructed, implemented, and promoted …"

Room - Boardroom - *No presentation*

Room - Langley Room

Security specialists are from Mars; healthcare practitioners are from Venus: the case for a community-of-practice approach to security architectures for healthcare

Lizzie Coles-Kemp[1] and Patricia A H Williams[2]
[1]. Information Security Group, Royal Holloway University of London, [1,2]School of Computer and Security Science [2]Security Research Institute, Edith Cowan university

Information security is a necessary requirement of information sharing in the healthcare environment. Research shows that the application of security in this setting is sometimes subject to work-arounds where healthcare practitioners feel forced to incorporate practices that they have not had an input into and with which they have not engaged with. This can result in a sense of security practitioners and healthcare practitioners being culturally very different in their approach to information systems. As a result such practices do not constitute part of their community of practice nor their identity. In order to respond to this, systems designers typically deploy user-centred, participatory approaches to design using various forms of consultation and engagement in order to ensure that the needs of users are responded to within the design. Learning from international implementations of e-health, the development of the Australian electronic health records (EHR) system has been a participatory process. However, the more participatory approach has not been used as part of the technical security design of the e-health system and the functionality of the security governance architecture was not included in the process of consultation. Such exclusions result in a design-reality gap in so far as the healthcare systems as envisioned by designers are not easily related to by "front-line" clinical staff. Despite repeated design-reality issues in healthcare systems design, there is no fundamental change in the development paradigm to address the socio-technical security aspects of such systems. Indeed, the security perspective of system designers seems to originate from a very different perspective to that of front-line clinical staff. This discussion paper characterises the problem, uses examples from both the UK and Australian EHR experience, and proposes an alternative start-point to healthcare systems design.

Room - Silver Room

🛠🛠 - Medium

Exposing Potential Privacy Issues with IPv6 Address Construction

Clinton Carpene, Andrew Woodward
Security Research Institute, Edith Cowan University

The usage of 128 bit addresses with hexadecimal representation in IPv6 poses significant potential privacy issues. This paper discusses the means of allocating IPv6 addresses, along with the implications each method may have upon privacy in different usage scenarios. The division of address space amongst the global registries in a hierarchal fashion can provide geographical information about the location of an address, and its originating device. Many IPv6 address configuration methods are available, including DHCPv6, SLAAC (with or without privacy extensions), and Manual assignment. These assignment techniques are dissected to expose the identifying characteristics of each technique. It is seen that use of the modified EUI-64 in SLAAC can allow agents to simply decipher an interface's MAC address over layer 3 communications, whilst discernable patterns can be used to identify the presence of DHCPv6 or manual address assignment. Additionally, the frequency and lifetime of unique addresses originating from a single network prefix may allude to privacy addresses in use within the network. Together these issues pose a risk to the privacy of IPv6 users, as it may allow for tracking of users of portable network devices.

12:00 - 12:30

Room - Ballroom North

Cyberterrorism: addressing the challenges for establishing an international legal framework

Krishna Prasad
School of Law and Justice, Edith Cowan University

The increase of international cyberterrorism in recent years has resulted in computer-based criminal activities that generate worldwide fear, destruction and disruption. National laws and policies that address cyberterrorism are mainly limited to developed nations and are not cohesive in managing 21st century cyberterrorism. Given the absence of an international legal framework to address cyberterrorism, authorities and governments around the world face extreme challenges in finding and prosecuting those responsible for cyberterrorism. This article argues for the need for a cohesive international legal framework; highlights key elements to establish an effective international legal framework; and identifies existing international treaties and cross-border agreements that could be expanded to provide legislative guidelines for prosecution.

Room - Boardroom - *No presentation*

Room - Langley Room - *No presentation*

Room - Silver Room

🛠🛠 - Medium

The security challenges and countermeasures of virtual cloud

Bhupesh Mansukhani, Tanveer A Zia
School of Computing and Mathematics, Charles Sturt University

The adaption of cloud computing is on a rise these days, due to the various effects that it has on enterprise. As it allows the users to have scalable infrastructure and economical benefits which indeed a way to boost any enterprise mind in opting for such service. Cloud Computing offers a whole new paradigm to allow the users to have high-end and scalable infrastructure at an affordable cost and without even the need of managing the inventory. The interesting part of cloud computing is it offer three platforms to choose from IaaS, PaaS, and SaaS, these three platforms together, form cloud computing, out of these three platforms the interesting one is IaaS (infrastructure as a service) that allows the users to have on the fly infrastructure. Although IaaS offers great benefits to the users but the complexity in its structure, open doors to unseen and forcible threats to security of the data and cloud computing. In this paper, the authors have proposed countermeasures to secure cloud computing IaaS virtual platform by High Trust Zone. The solution proposed would minimize the threats to the virtualized infrastructure of the cloud by binding the VMs (Virtual Machines) in one trusted zone, irrespective of the Users applications and security policy, this zone will provide utmost protection to the other running VMs and devices of the physical host such as memory, hardware etc. The authors believe that by using the proposed solution (High Trust Zone), it can offer pre-emptive protection words complex and dynamic cloud virtual infrastructure.

12:30 Lunch

1:30 - 2:00

Room - Ballroom North

Boko Haram: Terrorist organisation, freedom fighters or religious fanatics? An analysis of Boko Haram within Nigeria, an Australian perspective and the need for counter terrorism responses that involves proscribing them as a terrorist organisation

Gabrielle Blanquart
School of Computer and Security Science, Edith Cowan University

The adoption of Sharia law and the creation of an Islamic government are prominent motivations for religious terrorism within the current climate. Throughout history, Nigeria has been exposed to ethno religious violence and political discontent and has recently seen an escalation in associated violence threatening its sovereignty, territorial integrity, peace and stability. This paper explores Boko Haram, a Nigerian Islamist sect, responsible for numerous attacks in northern and central Nigeria on infrastructure and people. The origins and ideological motivations of this group are examined and compared to the current wave of religious terrorism in relation to tactics, leadership and objectives. Parallels and relationships are drawn between Boko Haram and other proscribed terrorist organisations such as al-Qa'ida, al-Qa'ida in

the Islamic Maghreb (AQIM) and the Somalian al Shabaab. This paper defines Boko Haram as a terrorist organisation, as opposed to religious fanatics or freedom fighters, other common views about this group. This paper takes an Australian legislative approach to defining terrorism and terrorist organisations and examines Boko Haram against a terrorist organisation proscribed by the Australian Government, AQIM, to substantiate claims that this organisation demonstrates features common among terrorist organisations. Future prospects of this group, including potential expansion and listing them as a terrorist organisation by the Australian government for national security, are presented.

Room - Boardroom - *No presentation*

Room - Langley Room - *No presentation*

Room - Silver Room

🛠🛠 - Medium

Implementing a secure academic grid system – a Malaysian case

Mohd Samsu Sajat, Suhaidi Hassan, Adi Affandi Ahmad, Ali Yusny Daud, Amran Ahmad, Mohamed Firdhous, InterNetWorks Research Lab, School of Computing, UUM CAS, University Utara Malaysia

Computational grids have become very popular in the recent times due to their capabilities and flexibility in handling large computationally intensive jobs. When it comes to the implementation of practical grid systems, security plays a major role due to the confidentiality of the information handled and the nature of the resources employed. Also due to the complex nature of the grid operations, grid systems face unique security threats compared to other distributed systems. This paper describes how to implement a secure grid system with special emphasis on the steps to be followed in obtaining, implementing and testing PKI certificates.

2:00 - 2:30

Room - Ballroom North

The emergence of Boko Haram: An analysis of terrorist characteristics

Peter L. Lacey, Edith Cowan University

Boko Haram (BH) is a Nigerian extremist group which emerged only in the last decade, but has rapidly established a reputation for violence. This paper reviews the development and behaviour of BH in recent years, concluding that the group's activities meet the definition of terrorism as systematic use of fear-evoking violence against civilians to achieve political goals. This characterisation is justified in terms of four definitional elements of terrorism, and further supported by comparison of BH with contemporary terrorist groups such as Abu Sayyaf Group and Caucasus Emirate, which espouse an ostensibly similar ideology. BH should not be mistaken for a gang of criminals, freedom fighters or religious fanatics. The group is capable, driven, and should be understood as a modern terrorist organisation.

Room - Boardroom - *No presentation*

Room - Langley Room

Cyber resilience in Australian critical infrastructure: Securing critical infrastructure industrial control systems in the face of emerging advanced persistent threats

Nicholas Jenzen-Jones, Marc Loney, Edward Baxter, Alan Davies

The past twenty years have seen rapid advances in the IT sector, and the increasing digitisation of the industrial sector. Protection of critical infrastructure Industrial Control Systems has long focused on security by obfuscation and segregation. With the increasingly digitised nature of critical infrastructure, and the dominant trend towards externally networked ICS, there is a need to adjust models to reflect changes in technology, and to adjust to modern Advanced Persistent Threats and the possibility of High-Impact, Low-Frequency events. At present, there are no mandatory Australian standards relating to the protection of such systems. This paper will outline current ICS vulnerabilities and precautionary measures in place, examine challenges to implementing the latter effectively, look at existing standards and policies, and seek to explore the ways in which these could be supplemented in order to buttress the security of Australia's critical infrastructure ICS.

Room - Silver Room

🛠🛠 - Medium

Does the android permission system provide adequate information privacy protection for end-users of mobile apps?

Michael Lane, School of Information Systems
University of Southern Queensland

This paper investigates the Android permission system and its adequacy in alerting end-users of potential information privacy risks in an app. When an end-user seeks to install an app, they are presented with the required permissions and make a supposedly informed decision as to whether to install that app based on the permissions presented. The results from an analysis of ten popular apps indicate a number of permissions that pose potential information privacy risks of which most end-users are likely to be unaware. The Android permission system is complex and difficult for end-users to comprehend and effectively evaluate the potential information privacy and security risks in an app. Most end-users will install the app without evaluating the list of required permissions presented to them. Furthermore there is an inconsistent approach to informing end-users about the privacy policy and terms of use for Android apps. The findings of this paper indicate a need for better decision support apps so end-users can more easily make better decisions regarding privacy and security protection provided by apps. Future research should also examine the free market failure of mobile application market places to provide adequate privacy protection and the need for stronger privacy protection laws.

2:30 - 3:00

Room - Ballroom North

Commitment and the 1% motorcycle club: threats to the brotherhood

Kira J. Harris, Edith Cowan University

The brotherhood ethos is the founding principle of the 1% motorcycle clubs community. Interviews with former members and partners show how threatening this social bond can reduce satisfaction and lead to doubts over involvement with the club.

Room - Boardroom - *No presentation*

Room - Langley Room

🛠🛠 - Medium

Applying Feature Selection to Reduce Variability in Keystroke Dynamics Data for Authentication Systems

Mark Abernethy and Shri M. Rai
Murdoch University, Perth, Western Australia

Authentication systems enable the verification of claimed identity. Password-based authentication systems are ubiquitous even though such systems are vulnerable to numerous attack vectors and are therefore responsible for a large number of security breaches. Biometrics has been increasingly researched and used as an alternative to password-based systems. There are a number of alternative biometric characteristics that can be used for authentication purposes, each with different positive and negative implementation factors. Achieving a successful authentication performance requires effective data processing. This study investigated the use of keystroke dynamics for authentication purposes, by applying a feature selection process (based on normality statistics) to reduce the variability associated with keystroke dynamics raw data. Artificial Neural Networks were used for classification, and results were calculated as the false acceptance rate (FAR) and the false rejection rate (FRR). Experimental results returned an average FAR of 0.02766 and an average FRR of 0.0862, which were at least comparable with other research efforts in this field.

Room - Silver Room

🛠 - Low

A proposed formula for comparing kill password effectiveness in single password RFID systems

Christopher Bolan, School of Computer and Security Science
Security Research Institute, Edith Cowan University

The Electronic Product Code standard for RFID systems plays a significant role in worldwide RFID implementations. A feature of the RFID standards has been the RFID Kill command which allows for the 'permanent' destruction of an RFID tag through the issuing of a simple command. Whilst the inclusion of this command may be vital for user privacy it also opens up significant avenues for attack. Whilst such attacks may be well documented there has been little to no discussion of the efficacy of the differing mitigation approaches taken. A simple formula to calculate the full timing of such

an attack on differing RFID setups is presented. The formula allows for users to model the effect that altering such aspects as timeout or transmission response time will have on RFID security.

3:00 - Afternoon Tea

3:30 -4.00

Room - Ballroom North

🛠 - Low

A study of remnant data Found on USB storage devices offered for sale on the Australian second hand market in 2011.

Krishnun Sansurooah, Patryk Szewczyk
School of Computer and Security Science, Security Research Institute
Edith Cowan University

The uptake of USB storage has mainly replaced previous portable media. With the evolution of USB storage devices, increased importance is placed on this technology in both the private and commercial worlds. USB storage capacity has increased tremendously in recent decades, with capacities of 16 megabytes in early models expanding to as much as 256 gigabytes today. The relative low cost of these devices, together with their robustness, low power consumption, excellent response rates, non-volatility and easy of transport, have increased their accessibility and revolutionised the potential uses of the device. The study obtained second hand USB storage devices to determine whether there were traces of information or data and if whether or not they had been effectively wiped. If fragments of data on the USB storage devices were present, the study further scrutinised whether the data retained was of significant volume or of enough sensitivity to the previous owner to be of significant value to anyone with a malicious intent. The research found that in the majority of the cases, the USB storage devices retained a significant amount of identifiable information. As with the outcomes from the previous study carried out in 2009, the USB storage devices, owned by both individuals and organisations, failed to meet their regulatory or legal obligations in wiping their USB storage devices.

Room - Boardroom - *No presentation*

Room - Langley Room

Exterminating the cyber flea: irregular warfare lessons for cyber defence

Ben Whitham
University of New South Wales

Traditional approaches to tactical Computer Network Defence (CND), drawn from lessons and doctrine of conventional warfare, are based on a team of deployed security professionals countering the adversary's cyber forces. The concept of the adversary in cyberspace does not fit neatly into conventional military paradigms. Rather than fighting an identifiable foe, cyber adversaries are clandestine, indistinguishable from legitimate users or external services, operate across state boundaries, and from safe havens that provide sanctuary from prosecution. The defender also faces imbalances with rules of engagement and a severe disparity between the cost of delivering the defence and the attacker's ability to deliver an effect. These operational conditions are more akin with Irregular Warfare (IW) than a conventional conflict.
This paper proposes a new approach to CND, based on a review of literature on IW. Rather than fight the battle alone, the CND team should concentrate efforts to persuade and empower network users to take responsibility for protecting the organisation's critical data. This approach seeks to apply the lessons learnt from IW, where the resistance to the adoption of security best practices, intentional or otherwise, is the real adversary. This approach appears more likely to deliver long-term protection from current cyber threats than a dedicated monitoring team to track adversaries that are invisible and employ attacks that are constantly evolving.

Room - Silver Room

🛠🛠 - Medium

The mobile execution environment: A secure and non-intrusive approach to implement a bring your own device policy for laptops

Peter James, School of Computer and Security Science, Edith Cowan University
Don Griffiths, School of Information Systems, Curtin Business School, Curtin University

Bring Your Own Device (BYOD) has moved primarily from a knowledge worker's use of a personally owned laptop in the workplace, usually due to the superior capabilities of the laptop compared to the employer furnished laptop/PC, to the adoption of the BYOD concept as a mainstream work practice to both attract staff and reduce information technology expenditure. Organisations that are using telework and/or activity based work methodologies are also increasingly

adopting the BYOD paradigm for laptops, as it supports the flexible and agile nature of the professional and private life of the modern knowledge worker. However, the BYOD approach can increase an organisation's information security risks. The security risks can be mitigated or managed through the selection of an appropriate secure laptop software configuration. This paper considers how one specific laptop software configuration, known as the Mobile Execution Environment (MEE) can be used to minimise information security risks when a BYOD policy for laptops is implemented. The MEE is one of a number of laptop software configurations that can be used to achieve a secure BYOD policy for laptops. In this paper the security and business risks associated with the implementation of such a policy are identified and discussed before giving an overview of a range of laptop software configuration options suitable for the implementation of a secure BYOD policy. The design requirements of the MEE are enumerated and its key features described. For each identified security/business risk, the MEE features that mitigate or manage the risk are presented. The paper concludes by considering the type of work for which the MEE is most suited and also how the security features of the MEE can be enhanced when the MEE is installed on a secure portable execution and storage environment.

6:30 - 10:30

secau Security Congress Dinner
Chanterelle at Jessicas Restaurant, **The Fortescue Centre, Terrace Road, East Perth**

Day 3 – December 5, 2012

9:45 – 10:00

Room - Silver Room - **Best Paper awards will be presented by Congress Chair, Professor Craig Valli**

10:00 - 11:00

Room - Silver Room - Keynote Presentation

Professor Steven Furnell
Plymouth University, United Kingdom
Infosec: Lots of safeguards and no protection?

It is hard to escape IT security, with related safeguards to be found on most of the devices, applications and services that we use. The average user is faced with a plethora of threats that they are warned to ignore at their peril, and many will consequently devote significant time to security-related tasks and interactions. In spite of this, they can still face the risk of attacks and exploitation against their systems, and so may arguably feel that they have gained a tangible security overhead, but have relatively little to show for it. This presentation will consider the extent of the burden that security can place upon users (including the time, difficulty and constraints involved), and the extent to which these can be offset through better attention to the technology itself and through changing the culture of those that must use it.

11:00 - Morning Tea

11:30

Room - Ballroom North

Al-jihad fi sabilillah: In the heart of green birds

Robyn Torok
Security Research Institute, Edith Cowan University

With an increasing focus on lone-wolf operations, al-Qaeda is becoming increasingly focussed on its internet discourses and propaganda. One of its most significant discourses is the importance of jihad and martyrdom in carrying out a terrorist attack. This study looks at Facebook pages and profiles and examines the discourses presented in relation to jihad and martyrdom. Three important concepts including their justification are considered: Al-Jihad fi Sabilillah (just fight for the sake of Allah), Istishhad (operational heroism of loving death more than the West love life) and Shaheed (becoming a martyr). Results supported previous studies indicating the strong seductive nature of such discourses. Although many discourses were similar to previous studies, several key differences were noted; namely, different emphasises within the concept of Shaheed as well as a strong focus on green bird imagery which became prominent during the Bosnia conflict.

Understanding such discourses will be critical in not only preventing terrorism, but also in the developing better deradicalisation strategies.

Room - Boardroom

HARMs: Hierarchical Attack Representation Models for Network Security Analysis

Jin Hong, Dong-Seong Kim, Department of Computer Science and Software Engineering, University of Canterbury, Christchurch, New Zealand

Attack models can be used to assess network security. Purely graph based attack representation models (e.g., attack graphs) have a state-space explosion problem. Purely tree-based models (e.g., attack trees) cannot capture the path information explicitly. Moreover, the complex relationship between the host and the vulnerability information in attack models create difficulty in adjusting to changes in the network, which is impractical for modern large and dynamic network systems. To deal with these issues, we propose hierarchical attack representation models (HARMs). The main idea is to use two-layer hierarchy to separate the network topology information (in the upper layer) from the vulnerability information of each host (in the lower layer). We compare the HARMs with existing attack models (including attack graph and attack tree) in model complexity in the phase of construction, evaluation and modification.

Room - Langley Room

The regulation of space and cyberspace: One coin, two sides

Brett Biddington, Adjunct Professor, Security Research Institute, Edith Cowan University

In the 1960s, during some very tense days in the Cold War the United States of America (USA) and the Union of Socialist Soviet Republics (USSR) brokered a deal in the United Nations for a treaty regime to govern human activities in outer space. This regime has served well enough for almost 50 years. In recent years, however, fears of space weaponisation, the proliferation of space debris in the Low Earth Orbits (LEO) and increasing demands on the electromagnetic spectrum (EMS) have led to demands for regulatory reform. Some nations now consider space to be the fourth domain of modern warfare.

Meanwhile, the cyber domain continues to develop apace. The world is struggling to determine whether, and if so how, to regulate the cyberspace. The United States now considers cyberspace to be the fifth domain of warfare and has announced that it reserves the right to meet cyber attacks, on interests it considers vital, with conventional kinetic responses.

The space and cyberspace domains overlap and have mutual dependencies which demand a degree of coherence and integration in legislative, policy, and regulatory responses. There are also some important differences and distinctions. This paper explores some of the dilemmas that are faced by decision-makers who seek to make both the space and cyberspace domains safe and secure places which will deliver benefit to humans across the planet long into the future.

Room - Silver Room

Security of user-centric session in mobile and heterogeneous environment

Ali Hammami, Noémie Simoni
Telecom ParisTech, France

Next Generation Networks (NGN) have become increasingly heterogeneous and mobile. Moreover, Next Generation Services (NGS) are evolving towards user-centric approach; it consists of offering dynamic and personalized service session according to user preferences and context with respect of continuity and quality of service. In such context, security issues, such as authenticity, confidentiality, integrity and availability, represent a major concern.

To overcome these challenges, we have contributed, in previous work, to propose an extension of Session Initiation Protocol (SIP), called SIP+, that permits to establish a personalized and mobile service session. It is based on QoS (Quality of Service) negotiation to maintain the required end-to-end QoS and it conveys a Security Token to ensure a unique user authentication in a cross-organizational environment. This leadss to provide a unique, seamless and user-centric service session. These objectives have been achieved and it remains to achieve security requirements. Thus, we aim in this work to secure the proposed SIP+ protocol against the potential attacks and vulnerabilities in order to provide a secure service session while respecting our user-centric requirements.

12:00 - Lunch

1:00 -1:30

Room - Silver Room

1st Australian e-Health Informatics and Security Conference - Special presentation

Dr Mike Civil

General Practitioner, Stirk Medical Group, WA

Video Consultation in your General Practice: A WA experience

Dr Mike Civil is a leading telehealth advocate and user. Given the enormous cost reductions, in addition to the improvements in access to healthcare services that telehealth can provide, it is not surprising that this is a fast growing area of healthcare service delivery world wide. Australia has embraced this with Government incentives for its adoption particularly for the general practitioner-patient-specialist triangle of healthcare delivery. With over 350 tele-consultations to date, Dr Mike Civil from Stirk Medical Group will present the practical experience of using this as a method of patient care. He will outline how certain factors such as patient safety and security should be foremost in mind when conducting such consultations, and present the challenges associated with these.

1:30 -2:00

Room - Silver Room

1st Australian e-Health Informatics and Security Conference - Special presentation

Dr Vincent McCauley

National eHealth Implementation Coordinator Medical Software Industry Association

E-health conformance testing: A tool of clinical benefit

The development of a national e-health system is a highly complex and involved process. In Australia this has seen a service oriented architecture (SOA) approach adopted. The medical software industry in Australia has highlighted the complexity with which conformance in an SOA environment needs to be addressed to ensure, not only, patient safety but also the many and varied workflows and implementations related to the use of health software. The success and lessons learned from this are presented in light of the personally controlled electronic health record (PCEHR) introduction in July 2012 and the multiple security issues raised in regard to this initiative.

2:00 -2:30

Room - Silver Room

1st Australian e-Health Informatics and Security Conference -Special presentation

Gil Carter

Business Aspect

Supporting BYOD in a complex eHealth security environment

Portable devices are revolutionising the way that health professionals can work with health information, opening exciting new possibilities and helping to improve care delivery for health consumers. The model of allowing users to 'bring your own device' has been widely embraced in corporate ICT environments, but has created challenges for information security and device management practices. In a health environment already managing sensitive patient information that may come from source systems both internal and external to the organisation, the security challenges around a BYOD model for portable devices create an additional layer of complexity to be managed. In this complex environment, how can clinical users and ICT security administrators work together to get the benefits of portable devices in secure but useful ways? This presentation will discuss some of the challenges in this area, and explore some options for taking the right forward steps for your organisation.

2:30 -3:00

Room - Silver Room

1st Australian e-Health Informatics and Security Conference

Panel Discussion

3:00 -3:30 Afternoon Tea

P.D. 166

STATEMENT OF WITNESS

Statement of: Age: **Over 18 years**

This statement, consisting of 8 page(s) signed by me is true to the best of my knowledge and belief. I know that this statement is to be used for the purpose of a prosecution and that if it contains material which I know to be false or misleading, I will be guilty of an offence.

Dated the ..... of ....., ...

Signed: .....

Witnessed by (name): .....

of (address): 60 Wakefield Street

Adelaide SA 5000

Signature of Witness: .....

I am an Electronic Evidence Support Officer with the Electronic Crime Section of the South Australia Police (SAPOL), a role which I have undertaken since September 2008. I commenced this statement on Monday 22 March 2010 in the ECS office.

I hold a Bachelor degree of Computer Science from the National Taiwan Ocean University, a Master degree of Information Management (Computer Science) from the Providence University in Taiwan, and a PhD in Computer Science (Computer Forensics) from the University of South Australia. In addition, I have undertaken training in mobile telephone analysis using .XRY from Micro Systemation. I have also

completed the EnCase Computer Forensics II course provided by Guidance Software.

The responsibility of the Electronic Evidence Support Officer is to provide specialist support to investigations where there are issues involving, or possibly involving, electronically based evidence. This support involves the provision of specialist expertise to analyse the contents of electronic devices. The analysis process is performed in a non-invasive manner utilising industry standard forensic procedures.

On **Monday 15 June 2009** a request was received at the Electronic Crime Section to assist in a police enquiry involving the following property items:

Exhibit Property Item	**Item Type**	**Make/Model**
09/A61859-9	1*External Hard Disk Drive, 2*USB devices	External HD (Western Digital), USB devices (N/A)
09/A61859-10	Laptop Computer	Toshiba
09/A61859-13	Desktop Computer	Dell/Precision 340
09/A61859-15	Desktop Computer	Dell/Optiplex 745
09/A61859-16	USB Memory Storage Device	Lexar

This request was given the internal reference of: **ECS 2009/634**

On **Tuesday 29 December 2009**, I commenced the examination of the forensically sound copy, 09-A61859-9 HD. On **Thursday 18 March 2010**, I assisted investigator Anthony BRAIN in reviewing its contents, and identified the following:

- A report of this exhibit was produced and called "***Report of Exhibit 09-A61859-9 HD***". This report is located in the folder with the following path ***\Reports\09-A61859-9 HD***.

- A folder named **holy roman bible**, including files and sub-folders, was extracted, and stored in ***\Extracts\09-A61859-9 HD.*** The corresponding report was produced and called "***Report of holy roman bible***". This report is located in the folder with the following path ***\Reports\09-A61859-9 HD***.

- A folder named **KARINA**, including files and sub-folders, was extracted, and stored in ***\Extracts\09-A61859-9 HD.*** The corresponding report was produced and called "***Report of KARINA***". This report is located in the folder with the following path ***\Reports\09-A61859-9 HD***.

- 10 entries from Internet History (Bookmarks) were extracted. The corresponding report for the above 10 entries (including *Name, Url Name, Url Host, and Last Accessed*) was produced and called "***Internet History IE (Bookmarks)***". This report is located in the folder with the following path ***\Extracts\09-A61859-9 HD***.

- 109 entries from Internet History Mozilla (Bookamrks) were extracted. The corresponding report for the above 109 entries (including *Url Name, Url Host, and Last Accessed*) was produced and called "***Internet History Mozilla (Bookmarks)***". This report is located in the folder with the following path ***\Extracts\09-A61859-9 HD***.

On **Wednesday 30 December 2009**, I commenced the examination of the forensically sound copy, 09-A61859-9 USB1. On **Monday 17 March 2010**, I assisted investigator Anthony BRAIN in reviewing its contents, and identified the following:

- No relevant information found in this item.

On **Wednesday 30 December 2009**, I commenced the examination of the forensically sound copy, 09-A61859-9 USB2. On **Thursday 18 March 2010**, I assisted investigator Anthony BRAIN in reviewing its contents, and identified the following:

- A report of this exhibit was produced and called "***Report of Exhibit 09-A61859-9 USB2***". This report is located in the folder with the following path ***\Reports\09-A61859-9 USB2***.

- A folder named **holy roman bible**, including files and sub-folders, was extracted, and stored in ***\Extracts\09-A61859-9 USB2.*** The corresponding report was produced and called "***Report of holy roman bible***". This report is located in the folder with the following path ***\Reports\09-A61859-9 USB2***.

On **Tuesday 29 December 2009**, I commenced the examination of the forensically sound copy, 09-A61859-10 LT HD. On **Thursday 18 March 2010**, I assisted investigator Anthony BRAIN in reviewing its contents, and identified the following:

- 9 files of possible evidentiary value, and they appear to be picture files. These files were extracted and stored in the folder with the following path **\Extracts\09-A61859-10 LT HD\Picture Files.**

  The corresponding report for the above 9 files (including *Name, Full Path, Description, Is Deleted, Last Accessed, File Created, Last Written, Entry Modified, and Logical Size*) was produced and called "***Report of Picture Files***". This report is located in the folder with the following path **\Reports\09-A61859-10 LT HD.**

- 150 files of possible evidentiary value, and they appear to be link files. These files were extracted and stored in the folder with the following path **\Extracts\09-A61859-10 LT HD\Link Files (BRANDO-Recent).**

  The corresponding report for the above 150 files was produced and called "***Report of Link Files (BRANDO-Recent)***". This report is located in the folder with the following path **\Reports\09-A61859-10 LT HD.**

- 35 entries from Internet History (Bookmarks) were extracted. The corresponding report for the above 35 entries (including *Name, Url Name, Url Host, Profile Name, and Last Accessed*) was produced and called "***Internet History IE (Bookmarks)***". This report is located in the folder with the following path ***\Extracts\09-A61859-10 LT HD***.

- 5 entries from Internet History (Daily) were extracted. The corresponding report for the above 5 entries (including *Url Name, Url Host, Profile Name, Visit Count, and Last Accessed*) was produced and called "***Internet History IE (Daily)***". This report is located in the folder with the following path ***\Extracts\09-A61859-10 LT HD***.

- 93 entries from Internet History (Typed URL) were extracted. The corresponding report for the above 93 entries (including *Url Name, and Url Host*) was produced and called "***Internet History IE (Typed URL)***". This report is located in the folder with the following path ***\Extracts\09-A61859-10 LT HD***.

- 28 entries from Internet History (Visited Link) were extracted. The corresponding report for the above 28 entries (including *Url Name, and Url Host, Profile Name, Visit Count, and Last Accessed*) was produced and called "***Internet History IE (Visited Link)***". This report is located in the folder with the following path ***\Extracts\09-A61859-10 LT HD***.

- 109 entries from Internet History Mozilla (Bookamrks) were extracted. The corresponding report for the above 109 entries (including *Url Name, Url Host, Profile Name, and Last Accessed*) was produced and called "***Internet History Mozilla (Bookmarks)***". This report is located in the folder with the following path ***Extracts\09-A61859-10 LT HD***.

On **Tuesday 29 December 2009**, I commenced the examination of the forensically sound copy, 09-A61859-13 PC HD. On **Monday 17 March 2010**, I assisted investigator Anthony BRAIN in reviewing its contents, and identified the following:

- No relevant information found in this item.

On **Tuesday 29 December 2009**, I commenced the examination of the forensically sound copy, 09-A61859-15 PC HD. On **Thursday 18 March 2010**, I assisted investigator Anthony BRAIN in reviewing its contents, and identified the following:

- 76 entries from Internet History (Bookmarks) were extracted. The corresponding report for the above 76 entries (including *Name, Url Name, Url Host, Profile Name, and Last Accessed*) was produced and called "***Internet History IE (Bookmarks)***". This report is located in the folder with the following path ***\Extracts\09-A61859-15 PC HD***.

- 256 entries from Internet History (Daily) were extracted. The corresponding report for the above 256 entries (including *Url Name, Url Host, Profile Name, Visit Count, and Last Accessed*) was produced and called "***Internet History IE (Daily)***". This report is located in the folder with the following path ***\Extracts\09-A61859-15 PC HD***.

- 299 entries from Internet History (Visited Link) were extracted. The corresponding report for the above 299 entries (including *Url Name, and Url Host, Profile Name, Visit Count, and Last Accessed*) was produced and called "***Internet History IE (Visited Link)***". This report is located in the folder with the following path ***\Extracts\09-A61859-15 PC HD***.

- 109 entries from Internet History Mozilla (Bookamrks) were extracted. The corresponding report for the above 109 entries (including *Url Name, Url Host, and Profile Name*) was produced and called "***Internet History Mozilla (Bookmarks)***". This report is located in the folder with the following path ***Extracts\09-A61859-15 PC HD***.

- 49 entries from Internet History Safari (Bookamrks) were extracted. The corresponding report for the above 49 entries (including *Url Name, Url Host, and Profile Name*) was produced and called "***Internet History Safari (Bookmarks)***". This report is located in the folder with the following path ***Extracts\09-A61859-15 PC HD***.

On **Tuesday 29 December 2009**, I identified no forensically sound copy of exhibit 09/A61859-16 was created. Nil analysis proceed.

The extracted files were copied onto a CD disk, marked **ECS 2009/634 YL1**.

STATEMENT OF WITNESS

Statement of: Age: **Over 18 years**

This statement, consisting of 13 page(s) signed by me is true to the best of my knowledge and belief. I know that this statement is to be used for the purpose of a prosecution and that if it contains material which I know to be false or misleading, I will be guilty of an offence.

Dated the ..... of ....., ...

Signed: .....

Witnessed by (name): .....

of (address): 60 Wakefield Street

Adelaide SA 5000

Signature of Witness: .....

I am an Electronic Evidence Support Officer with the Electronic Crime Section of the South Australia Police (SAPOL), a role which I have undertaken since September 2008. I commenced this **addendum** statement on Wednesday 14 April 2010 in the ECS office.

I hold a Bachelor degree of Computer Science from the National Taiwan Ocean University, a Master degree of Information Management (Computer Science) from the Providence University in Taiwan, and a PhD in Computer Science (Computer Forensics) from the University of South Australia. In addition, I have undertaken

training in mobile telephone analysis using .XRY from Micro Systemation. I have also completed the EnCase Computer Forensics II course provided by Guidance Software.

The responsibility of the Electronic Evidence Support Officer is to provide specialist support to investigations where there are issues involving, or possibly involving, electronically based evidence. This support involves the provision of specialist expertise to analyse the contents of electronic devices. The analysis process is performed in a non-invasive manner utilising industry standard forensic procedures.

On **Friday 20 March 2009,** a request was received at the Electronic Crime Section to assist in a police enquiry including the following property items:

Exhibit Property Item	Item Type	Make/Model
09/A76636-2	Laptop	Toshiba Satellite A200

This request was given the internal reference of: **ECS 2009/466**

On **Friday 19 March 2010,** I provided Mr. Brian JARMAN with access to a forensically sound copy of 09/A76636-2 to allow him to conduct analysis of this item.

I was later provided with a report prepared by Mr. Brian JARMAN, named **"Forensic Report for Iles Selley Lawyers, In the matter of Porch"**. I have read this report and provided the following observations of this report.

Page 4 of the report provides a table which details URLs (web addresses) and associated times. This table provides an edited version of the internet history from exhibit 09/A76636-2. I checked each entry in the table against the full internet history and identified an error in the representation provided in the table. I note that the last entry in this table with the access time of 03/01/2009 11:53:32 is out of sequence. As this is an A.M. time reference and the rest are P.M. time references. I am unable to comment as how Mr. Brian JARMAN made this error. I have provided a full copy of the Internet History for reference, named ***Entire Internet History***, and this file is located at ***Reports\09-A76636-2\Internet History***.

Starting on page 4 of the report concluding on page 5 is a description of the characteristics of **virusremover2008**. At page 5 the report lists 13 characteristics of the virus with a reference provided, "http://safeweb.norton.com/report/show?url=powerfulvirusremover2008.com". I checked this reference and was unable to locate the characteristics as provided. I reviewed reports from other anti virus companies including Symantec and McAfee. I was not able to identify the characteristics as described. For reference I have provided copies of the websites visited and the information detailed relating to virusremover2008 (Files stored in the folder with path: ***Reports/09-A76636-2/Anti Virus Site Screenshots***).

On page 5 of Mr. Brian JARMAN report in the last paragraph above the heading Para 5 a statement is made "*Consequently it appears that (at least from 3 Jan) the PC was severely compromised.*" This statement does not equate with the information located on the previously mentioned web sites which refers to virusremover2008 as not being serious but as an annoyance.

On page 6 of the report, a table is used to explain the actions mentioned at point 6 of "Introduction and brief" on page 3 which provides a reason for use of the key word *pedopics*. In order to provide a better understanding of the Internet use I reviewed the full Internet History, and identified the following URLs (containing words commonly associated with child exploitation material) Due to the large amount of Internet History entries, I provide an example of some of the entries:

- http://www.sexprowler.com/Feed/Rss/Latest/category/45
  (Last Accessed: 16/09/2008 23:11:37)
- http://www.bestialityhost.com/zooaccess/freemovies/008/?id=43
  (Last Accessed: 16/09/2008 23:22:41)
- http://zoo-cum.com/dtr/link.php?link=horizban&gr=2&id=aec9c8&url=http://www.bestialitymodels.com/43
  (Last Accessed: 16/09/2008 23:23:23)
- http://www.barnyardfuckfest.com/43
  (Last Accessed: 16/09/2008 23:23:50)

- http://www.yourbeastgirls.com

  (Last Accessed: 16/09/2008 23:27:17)

- http://www.google.com.au/search?hl=en&q=tits+and+tats&btnG=Google+Search&meta=

  (Last Accessed: 23/09/2008 12:52:12)

- http://www.bebaretoo.com/free_pages/naked-mom-kids.html

  (Last Accessed: 23/09/2008 13:01:09)

- http://www.youngpornmovies.com

  (Last Accessed: 21/10/2008 14:19:12)

- http://www.teenspantyhose.com/2007/guysformatures/0119m/pichunter_files/pichunter_files/fhg_guysformatures_g008_clip05.wmv

  (Last Accessed: 21/10/2008 14:33:35)

- http://www.bebaretoo.com/young-nudism-photos.html

  (Last Accessed: 21/10/2008 19:02:20)

- http://www.bebaretoo.com/nude-teen-pictures.html

  (Last Accessed: 21/10/2008 19:02:20)

- www.beastialitylove.com

  (Last Accessed: 18/11/2008 16:16:21)

- http://private-x-x-x.com/out.php?l=toplist&t=teenie-models.net

  (Last Accessed: 18/12/2008 23:57:25)

- http://www.teenie-models.net/favicon.ico

  (Last Accessed: 18/12/2008 23:57:32)

- http://www.teenie-models.net/go.php?link=top&ref=69xxxfreehostpagecom

  (Last Accessed: 18/12/2008 23:58:53)

- http://www.xxx-channels.com/free_sites.php

  (Last Accessed: 19/12/2008 00:15:03)

- http://offteens.com/index.html?7793

  (Last Accessed: 19/12/2008 00:17:09)

- http://virginscrazy.com

  (Last Accessed: 19/12/2008 00:18:14)

- http://young-vaginas.com

  (Last Accessed: 19/12/2008 00:39:11)

- http://nakedgirlsss.com

  (Last Accessed: 19/12/2008 00:39:57)

- http://www.youngteenz.name/index.html

  (Last Accessed: 19/12/2008 01:26:11)

- http://teenysexx.com/?id=youngfairygirlscom

  (Last Accessed: 19/12/2008 01:27:13)

- http://www.google.com.au/search?hl=en&q=nymphet+nude+pics&btnG=Google+Search&meta=

  (Last Accessed: 23/12/2008 00:06:26)

- http://www.google.com.au/search?hl=en&q=exposing+girls+underwear&btnG=Google+Search&meta=cr=countryAU

  (Last Accessed: 02/01/2009 17:34:50)

- http://www.google.com.au/search?hl=en&q=women+thongs+pics&btnG=Google+Search&meta=

  (Last Accessed: 03/01/2009 08:51:54)

- http://www.nymphets.net

  (Last Accessed: 03/01/2009 08:57:43)

- http://1st.nymphteen.com/alfateen/?ft=nymphets.net

  (Last Accessed: 03/01/2009 08:58:23)

- http://www.nymphets.net/cgi-bin/out.cgi?n=julibbs&id=930&url=http://bbs.juliapics.com/&p=2

  (Last Accessed: 03/01/2009 08:59:41)

- http://nude-teengirls.com

  (Last Accessed: 03/01/2009 09:39:51)

- http://littles-raped.com/index.html?275

  (Last Accessed: 03/01/2009 09:44:46)

- http://little-young.com/cgi-bin/out.cgi?ses=QJC3bCJ3el&id=209&url=http://youngestfreephotos.freeyounggphotos.com/

  (Last Accessed: 03/01/2009 09:51:59)

- http://groups.google.co.zm/group/free-little-lolita-fbl/feed/atom_v1_0_msgs.xml

  (Last Accessed: 03/01/2009 10:52:46)

- http://www.young-pussy.org/index.htm

  (Last Accessed: 16/02/2009 22:57:49)

- http://www.teen3somes.net/feed/atom

  (Last Accessed: 16/02/2009 23:15:02)

- galleries.teens3some.com

  (Last Accessed: 16/02/2009 23:15:52)

- http://www.littleuncensored.com/pictures/school4.shtml

  (Last Accessed: 19/02/2009 15:42:52)

- http://www.littlegirluncensored.com

  (Last Accessed: 19/02/2009 15:43:04)

- http://www.google.com.au/search?hl=en&q=paris+hilton+sex+tapes&btnG=Google+Search&meta=

  (Last Accessed: 19/02/2009 21:04:39)

- http://www.google.com.au/search?hl=en&q=father+fucking+daughter&meta=

  (Last Accessed: 21/02/2009 22:42:42)

- http://www.google.com.au/search?hl=en&q=young+virgins+pop+their+cherry&btnG=Search&meta=

  (Last Accessed: 21/02/2009 22:47:42)

- http://youngestnudist.com

  (Last Accessed: 21/02/2009 22:59:42)

- http://www.youngestlist.com/in.php

  (Last Accessed: 21/02/2009 23:00:10)

- http://www.youngestever.net

  (Last Accessed: 21/02/2009 23:13:36)

- http://www.young-bodies.net

  (Last Accessed: 21/02/2009 23:19:11)

- http://www.littlewhiteteens.com

  (Last Accessed: 21/02/2009 23:20:26)

- http://www.google.com.au/search?hl=en&q=illegal+preteen+nude+pics&start=10&sa=N

  (Last Accessed: 21/02/2009 23:35:38)
- http://www.google.com.au/search?hl=en&q=illegal+11+yr+old+preteen+nude+pics&btnG=Search&meta=

  (Last Accessed: 21/02/2009 23:38:31)
- http://www.google.com.au/search?hl=en&q=nude+kiddy+pics&meta=

  (Last Accessed: 21/02/2009 23:46:45)
- http://www.google.com.au/search?hl=en&q=kiddy+porn&meta=

  (Last Accessed: 21/02/2009 23:46:48)
- http://www.google.com.au/search?hl=en&q=illegal+tiny+nymphet+pics&btnG=Search&meta=

  (Last Accessed: 21/02/2009 23:48:25)
- http://illegal-incest.com

  (Last Accessed: 21/02/2009 23:52:08)
- http://www.google.com.au/search?hl=en&q=illegal+lolita+kiddy+pics&meta=

  (Last Accessed: 21/02/2009 23:52:21)
- http://www.google.com.au/search?hl=en&q=illegal+lolita+9+year+old++pics&btnG=Search&meta=

  (Last Accessed: 22/02/2009 00:54:45)
- http://groups.google.com.au/group/misc.kids.breastfeeding/feed/atom_v1_0_msgs.xml

  (Last Accessed: 22/02/2009 00:55:40)

- http://groups.google.com.au/group/comp.lang.c/browse_thread/thread/6cf9eb3479bab85a?hl=en&ie=UTF-8&q=illegal+lolita+9+year+old++pics
  (Last Accessed: 22/02/2009 00:56:28)
- http://groups.google.com.au/group/IT-Jobs-In-NY-and-NJ/browse_thread/thread/41a033f1dd91993a?hl=en&ie=UTF-8&q=lolita+pedo+stars
  (Last Accessed: 22/02/2009 00:59:49)
- http://groups.google.com.au/groups/search?hl=en&ie=UTF-8&q=lolita+pedo+stars&sitesearch=
  (Last Accessed: 22/02/2009 01:01:34)
- http://groups.google.com.au/groups/search?hl=en&ie=UTF-8&q=young+9+year+old+nymphet+nude+pics&btnG=Search&sitesearch=
  (Last Accessed: 22/02/2009 01:04:42)
- http://pics.greatincest.com/favicon.ico
  (Last Accessed: 03/03/2009 23:04:24)
- http://family-incest-pics.com
  (Last Accessed: 03/03/2009 23:07:13)
- http://www.google.com.au/search?hl=en&q=family+group+sex+pics&start=10&sa=N
  (Last Accessed: 03/03/2009 23:19:39)
- http://brutalhome.com/?from=sexinfamily.com&x=3845.
  (Last Accessed: 05/03/2009 00:12:15)
- gallery.purefamilysex.com
  (Last Accessed: 05/03/2009 00:13:46)

I reviewed the entire Internet History by keywords commonly associated with child exploitation material (google, incest, lolita, nymphet, pedo, powerfulvirus, preteen, pthc, underage, and young), and produced the corresponding excel reports named: ***Internet History (google)***, ***Internet History (incest)***, ***Internet History (lolita)***, ***Internet History (nymphet)***, ***Internet History (pedo)***, ***Internet History (powerfulvirus)***, ***Internet History (preteen)***, ***Internet History (pthc)***, ***Internet History (underage)***, and ***Internet History (young)***. I also extracted all Internet History and produced the report called ***Entire Internet History***. The above files are stored in the folder with path: ***Reports/09-A76636-2/Internet History.*** I reviewed the extracted Internet History, and identified the following:

- I located entries relating to websites including:
  www.fullfamilyincest.com,
  www.youngfairygirls.com,
  sexinfamily.com,
  zetincest.com,
  www.yourincestpics.com,
  galleries.incestcash.com,
  www.extremeyoungest.com were visited.

- Websites containing the keyword "nymphet" in their URL were accessed with visits to these websites on five particular dates (19/12/2008, 23/12/2008, 03/01/2009, 21/02/2009, and 22/02/2009).

- Websites containing the keyword "young" in their URL were accessed with visits to these websites on eight particular dates (21/10/2008, 19/12/2008, 03/01/2009, 23/01/2009, 19/02/2009, 21/02/2009, 22/02/2009, and 04/03/2009)

- Websites containing the keyword "pedo" in their URL show on four particular dates (23/12/2008, 03/01/2009, 21/02/2009, and 22/02/2009).

- Websites containing the keyword "lolita" in their URL show on four particular dates (23/12/2008, 03/01/2009, 21/02/2009, and 22/02/2009).

- Websites containing the keyword "pthc" in their URL show on two particular dates (03/01/2009, and 21/02/2009).

- Websites containing the keyword "preteen" in their URL show on three particular dates (23/12/2008, 03/01/2009, and 21/02/2009).

On page 7 of the report, a table depicting security events is included, after which is an opinion that "*These security activities appear to largely coincide with the end of 'interesting' activity - one possibility is that one or other of these updated programs removed the malware that was causing issues*". No evidence has been provided that supports the relationship between the malware and this matter. Further to this no explanation has been provided as to what is "*interesting activity*".

Counter examples show that Internet activities with keywords including pedo, lolita, preteen, in their URL occurred earlier than 03/01/2009, which is the date Mr. JARMAN believed the exhibit 09/A76636-2 was severely compromised. Secondly there is no similar Internet activities during 03/01/2009 and 21/02/2009, while the malware was still active within this period (based on the information in Mr. JARMAN's report).

I performed a virus scan using McAfee (Engine Version: 5400.1158, AntiVirus DAT Version: 5924.0) on 19/03/2010. Five trojans (in seven different locations) and one remote admin tool were still detected. The names of the trojans are ***DNSChanger.r***, ***FakeAlert-AB.gen.e***, ***generic!bg.cjo***, ***Generic Dropper.cx***, and ***Fakealert!bmp***. The name of the remote admin tool is ***RemAdm-VNC***. The McAfee report, named **09-A76636-2 LT HD P2**, was produced and stored in the folder with path: ***Reports/09-A76636-2/Virus Report.*** I reviewed the McAfee website, and identified the above six detections are mainly recognized as low risk assessments. None are recorded as being associated with sites containing child exploitation materials.

I subsequently copied abovementioned reports to a CD disk marked ***ECS 2009/466 YL2***.