2014 李昌鈺鑑識暨參訪心得

科學學院研習

林建隆／刑事警察局股長
陳建源／中央警察大學鑑識科學研究所博士生
林育梨／法務部調查局調查員
林益弘／屏東縣警察局巡官

壹、前言

今年「李昌鈺博士物證科學教育基金會」選派研習人員為法務部調查局調查員林育梨、警政署刑事警察局股長林建隆、中央警察大學鑑識科學所陳建源及屏東縣警察局巡官林益弘等四人，全額補助至國外研習。2014年初秋來到美國東岸，開始為期兩週的參訪與研習，參加「數位鑑識與網路犯罪國際研討會」及「李昌鈺鑑識科學學院」之指紋鑑定課程。

貳、參訪行程

參訪行程由「駐紐約臺北經濟文化辦事處」的秘書陳希傑協助安排下，我們參訪了三個不同屬性的地方，分別是科技公司：「Google紐約辦公室」，教育機構：「John Jay 刑事司法學院」及執法機關：「聯邦調查局紐約辦公室」。




一、Google紐約辦公室

在得知我們要參訪Google時，大家都非常的興奮。不管是從新聞報導、網路文章亦或「實習大叔（The Internship）」這部電影，都可以知道Google的辦公環境非常的活潑，不但有遊戲間、健身房、咖啡廳，還有吃不完的食物。我們除了參觀他們的辦公環境外，最重要的就是跟Google公司的網路安全部門人員互相交流。

圖1：參訪人員於Google紐約辦公室

在出發前我們就被告知，希望可以準備幾個討論議題或報告。既然是參訪Google，所以議題當然要跟Google相關。我們準備了Android智慧型手機的數位鑑識案例及利用手機惡意程式進行小額付款的詐騙案件，報告的題目為「Android Smartphone Forensics－Real Case Study in Taiwan」。

Android是Google以Linux核心所開發的作業系統，是目前市占率最高的智慧型手機，也因此在刑案偵查過程中最常收到的送鑑證物就是Android智慧型手機。像是八里雙屍命案中，媽媽嘴老闆呂〇〇的手機即為Android智慧型手機。在鑑識分析的過程發現，該手機中曾存有呂〇〇與謝〇〇的關鍵對話錄音檔案，但檔案已被刪除。若要將被刪除的重要檔案復原，首先必須取得該手機的最高權限（root），檔案復原後，即可提供專案小組釐清案情。過程中亦分享最近在臺灣非常嚴重的手機小額付款詐騙手法，及分析手機惡意程式的方法與成果。Google朋友對於我們分享的案例覺得好奇，詢問這些惡意程式是否在Google Play所下載安裝的？因為Google Play對於上架的程式會做檢測，所以這些惡意程式都是放在網路空間，由使用者自行下載安裝的。在會談的同時，Google朋友也分享他們的工作內容，例如：分析是否有人利用Google所提供的服務散布惡意程式或是釣魚網站，亦不斷地研發Google帳號的安全機制，提供使用者更安全的網路環境。

二、John Jay 刑事司法學院

紐約市立大學John Jay 刑事司法學院，為美國著名的刑事司法學院之一，李昌鈺博士為該校校友。參訪當天，在Adam Wandt教授的帶領下，我們參觀了緊急應變管理模擬系統（Emergency Management Simulator）、數位鑑識實驗室（digital forensics laboratory）及模擬法庭（Moot Court Room）。

緊急應變管理模擬系統類似臺灣的警察機關勤務指揮中心或情資整合中心，映入眼簾的就是多個螢幕所組合而成的超大螢幕牆，每個螢幕可以獨立顯示亦可以整合成一個大畫面，操作人員可以利用網路把想要觀看的影像（例如某個路口的監視器）投射在螢幕上。由於此為一間教學模擬教室，故每個座位上的電腦畫面皆可以投射在前方的大螢幕上，讓每位學生可以看到其他同學的操作畫面。

數位鑑識實驗室裡面有各種鑑識軟硬體設備，Adam Wandt教授主要研究領域為網路犯罪及惡意程式分析，實驗室所使用的鑑識工具與臺灣執法機關大致相同。另外，我們亦參觀Moot Court Room，裡面的環境及設施就跟一般法院相同，可以讓學生模擬法庭上的情境。

三、聯邦調查局紐約辦公室

聯邦調查局紐約辦公室設立於紐約市聯邦聯合辦公室大樓內，此次安排參訪的是電腦犯罪與數位鑑識部門。在會議開始前，由該部門主管介紹其工作內容，主要負責網路犯罪偵查，包含網路反恐、駭客入侵、重大網路詐欺等案件，會議中，我們亦報告目前臺灣非常嚴重的智慧型手機小額付款詐騙案件，其手法係利用社交工程方式，傳送有惡意程式連結之網址，然後再藉由惡意程式詐騙民眾之小額付款。與會人員對此犯罪手法均感到非常有趣，也詢問相關犯罪數字，依據我們事前準備的資料，這類犯罪在103年1至5月份共有2千6百多件，損失高達1千7百萬美元。FBI的成員表示，美國地區發生像這種重大的案件，就會由他們來偵辦。

由於網路犯罪大多是跨境犯罪，因此，國際合作顯得份外重要，我們也討論到幾年前，由FBI所偵辦的Ghost Click行動，與愛沙尼亞共同逮捕DNS Changer集團成員。該案件為駭客利用綁架電腦DNS設定，運用廣告詐欺獲利高達1千4百萬美元。FBI在破獲DNS Changer集團之後，以正常的DNS伺服器取代駭客集團的伺服器，讓感染DNS Changer的電腦可以正常運作。惟該正常的DNS伺服器即將關閉之際，仍有許多受感染的電腦並未處理，為使受感染電腦能正常運作，FBI即請各國執法部門協助處理，其中發現計逾3千多筆係屬於我國內註冊之網路服務提供者「ISP」之可能受感染IP資料。此案件當時即由刑事警察局協助處理，並撰寫中文化程式提供我國民眾檢測與清除。

希望藉由此次參訪，雙方能夠建立合作管道，不管在技術上的交流，或是案件合作都能夠更為順暢。

參、數位鑑識與網路犯罪國際研討會

第6屆數位鑑識與網路犯罪國際研討會（ICDF2C）暨數位鑑識系統理論與實務國際研討會（SADFE），於美國康乃狄克州紐海芬市之OMNI飯店舉辦，為期3日，會議主題涵蓋數位鑑識、網路犯罪、軟體侵權犯罪、資訊安全、隱私權保護等學術討論及實務分享。由於行動裝置的普及，使得它已成為人們日常生活中不可或缺的工具，再加上手機上所搭載的儲存空間愈來愈多，手機成為犯罪活動的媒介、工具或場所，已屢見不鮮。在此次研討會中，邀請行動裝置鑑識工具兩大廠商：美國Cellebrite公司及瑞典MicroSystemation公司，分別於2個場次介紹該公司之產品UFED及XRY，在會場上亦設置展示攤位，供與會人員體驗該公司之產品。

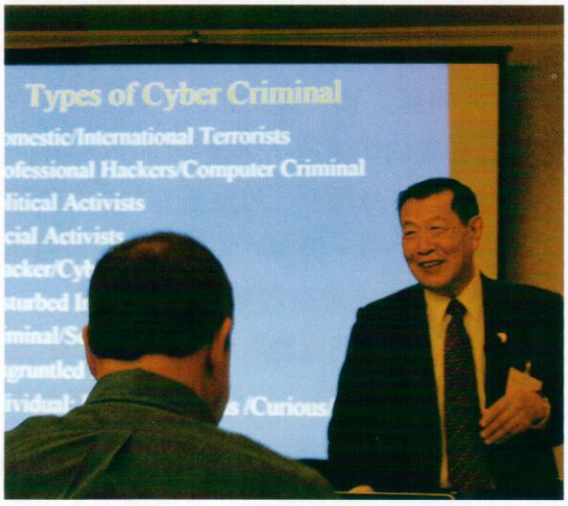


圖2：李昌鈺博士於研討會開幕演講

本次研討會與數位鑑識相關論文如下：

一、Understanding computer forensics requirements in China via the "Panda burning incense" virus case

此篇論文主要講述中國大陸的數位鑑識、數位證據發展歷程以及分析目前司法現況。中國大陸的司法制是非常獨特，並且與西方國家的司法制度迥然不同。雖然中國大陸已從2000年就開始發展數位鑑識，但司法制度開始考量到數位證據的合法性以及接受它為法律上證據的一種是在2013年3月1日。為使數位證據在法庭上成功呈現，其所需要的作業程序與西方司法系統是不同的，故必須更了解數位鑑識的發展與中國大陸有關於數位證據使用的法律要求。

中華人民共和國公安部是第一個建立數位鑑識的技術研究能力的單位，並長期投入中國大陸的數位鑑識發展。在2005年11月，中國大陸於北京舉辦第一場國內數位鑑識研究研討會，該研討會聚集中國科學院（簡稱中科院）、中國人民大學法學院、國內相關企業及公安部等專家學者，共同檢視一些常見的數位鑑識模型，以此為基礎，進而制定出中國數位鑑識模式的雛型。這些專家學者亦開始規劃數位鑑識人才的培育計畫及討論其能力建立的重要性。

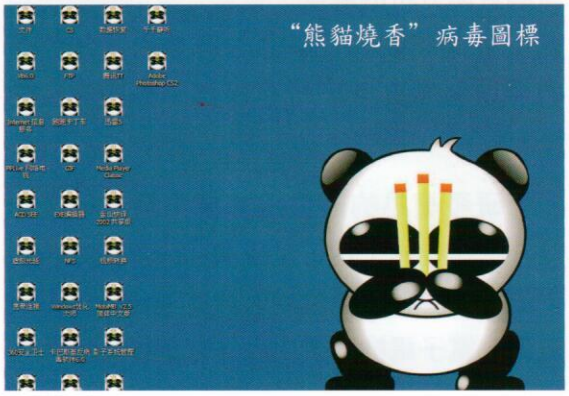
從2005年到2012年，每年舉辦的中國大陸數位鑑識研討會都在不斷的倡導數位鑑識的標準及促進這個領域人員的訊息交流。再者，自2009年到2012年，中國國家檢察官學院安排數門數位證據識別課程，用以保證這些檢察官具備有理解及可將數位證據完整呈

現於法庭的能力。

2009年，國家認證委員會與司法部成立一個符合國際標準的數位鑑識實驗室，並使數位鑑識人員的認可與認證正式化。於2012年1月，司法部公布數位證據訓練教材，並透過在武漢舉辦的國家數位鑑識研討會進行培訓工作。以上為中國境內對於數位鑑識發展的顯著里程碑。

中國大陸將數位鑑識分析分為4個層級，分別為取證層（evidence level）、應用層（application level）、技術層（technical level）及基本層（fundamental level）。取證層即分析與擷取數位證據的程序以支持刑事、民事及行政訴訟；應用層即透過分析應用軟體與設備以了解使用者行為；技術層即因犯罪所涉及的設備與各種活動進行檢視分析；基本層即在擷取及分析前，首先必須判斷該案件是否違反法律，並且了解數位鑑識基本原則及標準程序。

作者以熊貓燒香（Panda Burning Incense Virus）病毒案件為例，套用中國大陸所訂定的數位鑑識分析4個層級，以說明數位鑑識作業過程，及每一步驟應注意及檢視的重點為何。



二、AUDIT: Automated disk investigation toolkit

本篇論文主要介紹適用於非專家及調查人員的一套自動化磁碟調查工具包，簡稱AUDIT。磁碟分析軟體工具在數位鑑識調查方面扮演很重要的角色，但這些數位鑑識工具往往難以使用、通常為任務導向且需要有專業及被訓練過的人員才會使用。有鑑於此，作者提出一個在專家系統內整合開放式數位鑑識工具，調查人員只要有少許的磁碟結構及檔案系統結構知識，即可操作此工具；分析人員可利用內建之圖片搜尋功能、文件搜尋功能、電子郵件搜尋功能、及特殊搜尋功能（例如：信用卡資料、社會安全碼）以找尋目標資料。

AUDIT系統設計理念是含有一個靜態資料庫，此資料庫存有數位鑑識工具及調查工作的相關知識。這些知識的來源是來自對於數位鑑識工具有相當了解的專家。AUDIT系統就如同智慧型助理，點選或輸入欲查詢的目標，即可自動化的產生出結果。

AUDIT系統根據調查人員輸入的條件選出的工具，可以清楚的提供成為報告的一部分。並且可提供技術的說明，例如使用何種工具及為何使用它。再者，AUDIT系統亦可詳細地闡述資料是從磁碟的何處取得，這些過程對於調查人員在出庭作證時是非常有用的。作者設計這一套AUDIT系統亦包含一種理念，即想要將一些專業的用語或名詞，使用簡單的描述，呈現給非專業的人員了解。

三、Effects of the factory reset on mobile devices

本篇論文主要研究在執行“回復原廠模式“功能後，行動裝置的儲存空間內的使用者資料，是否會被清空。選擇9支Apple iPhone手機、10支Android系統手機及2支BlackBerry手機作為回復原廠模式後的系統評估實驗機種。使用美國Cellebrite公司之UFED physical analyzer、開放來源的Bulk Extractor工具及作者自行開發程式來擷取metadata、將檔案路徑分類及比較各個映像檔之間的差異。

為更清楚的了解及看出手機回復原廠模式前後之間的差異，作者使用Apple iPhone 4S及Samsung Galaxy SIII兩支手機進行實驗，首先將回復前與回復後，手機狀態製作副本。在這個實驗中，作者加入數個特定的檔案，這些特定的檔案被假設在回復原廠模式後，會被系統從手機內部刪除。

實驗後發現，大多數資料經回復原廠模式後會被移除，但有一些使用者特定配置的資料仍然留存。Android手機在移除使用者資料及媒體方面表現很差，常可意外發現一些留存在手機內的資料，例如：照片、影音、文件、電話號碼、電子郵件地址、定位資料、系統設定資料及金鑰。對於數位鑑識分析人員而言，回復原廠模式後的行動裝置，還是有可能提供一些有助於案件調查的資訊。

此次參加ICDF2C及SADFE研討會，我們深感數位鑑識的推廣及簡易數位證據分析工具的重要性，分析如下：

數位鑑識領域知識的推廣：參與研討會讓我們瞭解目前學術與實務單位，對於數位鑑識程序、法律、工具的發展。令人印象深刻的是，香港大學鄒錦沛教授所發表的論文，主要是說明中國大陸發展數位鑑識的過程，以及其定義的四個階層，並使用案例以說明每個階層必須完成的事情。看似簡單的定義，但中國大陸長期投入時間的蒐集資料、研討、不斷地修正及推廣、培訓，最後提出一套適用於中國大陸的數位鑑識程序。令人值得學習的是，他們不只是培訓數位鑑識調查與分析的專家，更進一步的訓練檢察官，讓他們能夠了解數位證據所代表的意義，以利需要時，可將事實原貌呈現於法庭。

研發簡易的數位證據蒐集及擷取工具包：這類型的工具正是目前國內執法單位需要的。由於執法單位的人員並非每一位都是資訊、電子電機背景出身，在偵辦案件的各

階段（例如：現場搜索、過濾、初步檢視），遇到各類型的數位證物時，要如何正確且快速地找到所需資料，的確是一大考驗。若能研發出簡易的工具包，以一步一步的詢問方式（例如：使用選項方式點選），將欲擷取的資料複製到目的硬碟，如此一來，使用者可不必具備相關技術與知識，只要了解“要甚麼資料”即可。

肆、李昌鈺鑑識科學學院研習

本次在美國康州紐海芬大學（University of New Haven）之研習為期5天，由李昌鈺博士及Mr. Kenneth B. Zercie講授課程。除我國籍學員外，並有來自中國大陸之訪問學者，以及美國籍、卡達籍等學員。本次研習課程涵蓋以下主題：

「指紋鑑定研習課程」、「現場重建基礎概念」、「案例研究」及「參訪李昌鈺鑑識科學學院（The Henrry C. Lee Institute of Forensic Science）」。

一、指紋鑑定研習課程（Fingerprint Classification and Comparison）：

本課程由Mr. Kenneth B. Zercie講授，由於學員們各來自不同領域與專業，故本課程從指紋基礎理論開始逐一介紹，包括：指紋如何發現、指紋之特性、指紋之紋型分類及比對、指紋之應用、指紋鑑識未來發展趨勢、自動指紋辨識系統（AFIS）操作方法等主題。

值得一提的是，美國現行採用「NCIC分析法」來進行指紋卡上之十指紋分析，與我國現行採用的「亨利氏（四步、六步）分析法」原理相近，但有數部計算公式的定義及結果呈現方式略有不同。「NCIC分析法」之表格及分析資料填寫方式如下所示：

NCIC

CLASS · FPC

1	6	0	8	A	A	d	I	P	O	S	R	6	2	T	T	C	I	X	M
↑		↑		↑		↑		↑		↑		↑		↑		↑		↑	
右拇指		右食指		右中指		右環指		右小指		左拇指		左食指		左中指		左環指		左小指	

介紹完指紋基礎知識後，Mr. Kenneth B. Zercie每日提供題目讓學員們反覆練習，累積指紋比對經驗。課堂中亦提供數組「同卵雙胞胎」指紋卡，讓學員們觀察，結果發現同卵雙胞胎各相對應手指之紋型雖極近似，但仍存在差異，再度驗證指紋具有「人各不同」的重要特性，故能作為人別鑑定的依據。

二、現場重建基礎概念：

本課程由李博士親自講授，首先介紹各種證物的分類，依證物特性可分為：

（一）暫時性物證（Transient Evidence）：

短暫存在，易隨時間、環境、氣候而變化、消失。例如：氣味、溫度、顏色、印（凹）

痕、臨時標記、煙霧、昆蟲、植物、乾溼……。

（二）情況性物證（Conditional Evidence）：

當時情況到底如何？由某一事件、行為產生，若無適時觀察、記錄，此資訊將永久消失。例如：燈光、火、屍體狀態、窗戶位置、瓦斯開啟或關閉。

（三）型態性物證（Pattern Evidence）：

由於「人－人」、「人－物」間物體接觸所產生。例如：物體損壞；身體姿勢、傷勢；犯罪手法（MO）；衣服、物品散布；輪胎、煞車痕跡；血跡噴濺痕；玻璃碎裂；火燒態樣；家具擺設；射擊彈道、殘跡；追逐腳印、拖拉痕跡。

圖3：李昌鈺博士與學員於教室合影

（四）移轉性物證（Transfer Evidence）：

微量證物；依「路卡交換原理」，兩表面間，只要有接觸，無時不刻都會有物質，在接觸範圍內產生交換轉移。例如：毛髮、血跡、體液、灰塵印痕、花粉、纖維、油漆。

（五）關連性物證（Associative Evidence）：

犯罪現場採集、發現的特定物品，可與被害者、嫌犯相互連結。例如：指紋、DNA等生物性跡證、犯嫌皮夾遺落現場、證明犯罪事實物證、犯罪工具、犯罪結果、違禁品、對照檢體、現場不合理物品。

（六）數位（電子）物證（E-Evidence）：

於電腦及相關各類型犯罪中所使用之物項均屬之，證據資料不只實體證據，還包括各種無形的數位化資料。例如：錄音、錄影到電腦、網路上之數位證據。

三、案例研究：

本課程由李博士及Mr. Kenneth B. Zercie共同講授。課前已分別講教授現場重建基礎概念及介紹指紋於現場之重要性，李博士及Mr. Kenneth B. Zercie以數個美國案例，引導學員們應用所學，共同研究，進行互動式討論。

（1）Consetta Serra Case：

Penny Serra於1973年7月16日New Haven市區遭到謀殺，該案當時懸而未破。案發26年後，當時現場之盒子證物，經以最新採證方法進行指紋增顯，成功顯現1枚潛伏指紋，比中犯嫌因而破案。透過此案例，可了解美國警政單位對現場重要證物保存之重視與嚴謹程度，以及陳舊

指紋增顯之時間極限，同時了解許多當代懸案，其重要證物若能妥善保存，待日後採證技術益愈進步時可再作嘗試，即使冷案亦可能有破案的機會。

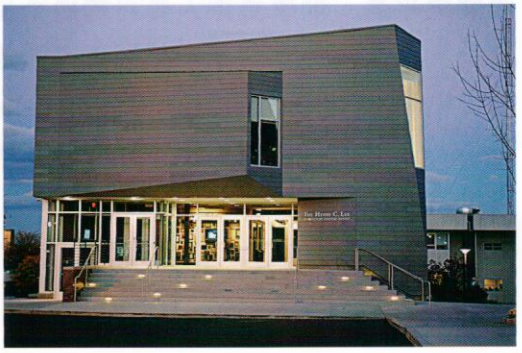
（2）Hartford Homicide Case、Bridgeport Homicide Case：

針對現場可疑的血跡印痕、指紋，先使用多波域光源（ALS）進行非破壞性檢視，搜尋可疑斑跡或印痕的位置，再使用化學試劑（如：TMB等）使之呈色增顯。「屍體」可視為一處現場，其中蘊藏許多重要線索與資訊，尤其重大暴力案件（如命案或涉及性犯罪之姦殺案），兇嫌可能會在犯罪或移屍過程中接觸被害者的皮膚，若能運用技術於被害者皮膚上採獲潛伏指紋，將能強而有力連結犯罪，直接證明嫌犯身分。

（3）其他：

包括「Karen Mount Case」案例、「孩童性侵案件調查」（Child Sex Investigation）、「電腦虛擬犯罪現場之保全」（Secure the Virtual Crime Scene）等主題，均有詳盡介紹與精闢分析。

四、參訪紐海芬大學李昌鈺鑑識科學學院（The Henrry C. Lee Institute of Forensic Science）：



在李博士特別安排下，其助理帶領學員們參觀校內聞名遐邇的「李昌鈺鑑識科學學院」。李昌鈺博士為享譽國際之刑事鑑識專家，自1975年開始便在紐海芬大學任教，任教期間更將刑事鑑識課程成為該校最著名的課程之一。李博士目前為該校終身教授，亦為鑑識科學學院之創辦人，透過這所學院的設立，將各國刑事鑑識相關的優秀學者、學生、科學家、法律機構及各領域專家連結整合。學院涵蓋教育、諮商、研究及公共訓練等層面，提供全世界刑事鑑識及刑事司法系統所面對問題的解決之道。

這所學院自2010年10月15日啟用，結合先進的教學教室與最新科技的實驗室設計，將紐海芬大學提升成為全球領導鑑識科學與刑事司法領域研究的學府。學院主要分為以下數個部門：

（一）鑑識科學研習中心：

包括先進的鑑識實驗室、現場模擬教室、研習教室等，藉由主題性模組化課程的設計，提供警察、律師、偵查人員、鑑識人員及在校學生研習鑑識與偵查相關之最新知識與實務經驗。中心內建置有透地雷達（Ground Penetrating Radar，簡稱GPR）、彈道重建高強度雷射、「SICAR系統」鞋印資料庫及鑑識衛星網路系統等。

（二）鑑識危機管理與調查中心：

圖4：李昌鈺博士與學員於學院正門合影

此中心集合不同專業領域的學者、專家，並整合相關可用之資料，建立可提供辦案所需資訊的資料庫。此中心亦為一橫向聯繫之平臺，刑事偵查人員可透過衛星與執法人員、國土安全部聯邦緊急事務管理局（FEMA，Federal Emergency Management Agency）及其他政府單位，共同研商解決複雜的犯罪問題。

（三）一般性學習中心：

中心內有許多互動式展示資料，包括虛擬教室、觸控式螢幕資訊桌、小型播映室等，可看到過去歷史名案，並能認識鑑識科學的專業領域，提高參觀者閱覽的興趣；另透過歷史名案偵辦的展覽介紹，讓參觀者對鑑識科學應用於案件調查能有更具體、深刻的認識。

（四）冷案調查中心：

當調查人員不再接收到新的線索資訊，案情無法突破的案件，終將成為「冷案」（Cold case）。部分懸而未破的「冷案」，其相關證物或資料被送至此中心，由各領域專家運用當代最新科技，重新鑑驗與審視，並提供專業意見，成立至今至少已有25件懸案獲得解決。

伍、研習心得

李昌鈺博士為第6屆數位鑑識與網路犯罪國際研討會開幕演講者，主題就是數位鑑識與網路犯罪，顯見數位鑑識已經成為刑事鑑識的重要一環，網路犯罪更是目前全世界所共同面臨的問題。藉由此次研習活動，我們深知鑑識工作也要與時俱進，不論是指紋、DNA亦或數位鑑識，都是利用科學方法與技術，對於犯罪相關跡證進行蒐集、分析與辨別，例如將現場採獲之指紋，輸入先前已建立之資料庫進行比對，以期調查犯罪者或被害者的身分；或針對屍體殘骸、牙齒、毛髮進行採驗，藉由分析DNA型別進行身分比對；其他尚包括槍彈、毒物、微物、文書等多種證物，均屬鑑定、

圖5：學員們與中心內展示設備進行互動教學

分析比對之範疇。隨著科技的演進，數位產品融入於日常生活，犯罪者的一舉一動可能都會在電腦、智慧型手機中留下物證，數位鑑識也成為鑑識科學中不可缺少的重要環結。

在了解各種證物於現場（Scene）的型態與分布後，運用科學原理與技術，快速有效尋找與蒐集，並送至實驗室（Lab）進行鑑定、比對，證物蒐集均合乎法律要求，移轉間亦有完善監管過程，期能將鑑定結果為司法偵審機關（Court）提供有力支持，這也是李博士於課堂中一再強調的「鑑識證據之利用——從現場、實驗室、法庭」（Utilization of Forensic Evidence — Scene, Lab, Court）。

在鑑識科技日新月異、科學證據愈為審判之重要依據的時代，「現場重建」程序與「證物監管鍊」是否完善，尤為法庭所重視。現場有各種不同型態，重建的方式則需視物證種類及待證事實而定，妥善運用科學知識與勘察工具，採取不同的步驟。如何從一個刑案現場中解讀跡證所透露出的各種訊息，是為現場勘察之鑑識人員所需要的重要能力。現場往往只有一次處理的機會，須完善勘察現場、進行重建，並精緻證物處理品質，「讓證據說話」，還原真相、辨冤白謗，方能辟弭爭議，彰顯正義公理，並實現人權保障之普世價值。FACT