行政院及所屬各機關出國報告
(出國類別：出國研習)

數位影像處理在刑事鑑識上的應用

服務機關： 臺北市政府警察局
出國人
職　稱： 技士
姓　名： 周俊銘
出國地區： 美國
出國期間： 93.03.20~93.06.25
報告日期： 93.09.25

行政院及所屬各機關出國報告提要

出國報告名稱：數位影像處理在刑事鑑識上的應用

頁數：168 含附件：■是□否

出國計畫主辦機關／聯絡人／電話：人事行政局

出國人員姓名：周俊銘
服務機關：臺北市政府警察局
單位：刑事鑑識中心
職稱：技士
電話：02-23366777

出國類別：□1考察□2進修■3研究□4實習□5其他

出國期間：九十八日
出國地區：美國

報告日期：93.09.25

分類號／目

關鍵詞：刑事鑑識、影像處理、交互詰問

內容摘要：（二百至三百字）

數位影像有傳輸容易、儲存方便、安定性佳、及容易處理等優點，因此不論是在任何領域之中，例如：醫學、刑事鑑識等方面都已利用數位影像來儲存或作處理，更由於數位相機、掃描器及CCD 等輸入設備之進步，所取得之影像已由黑白二色之灰階影像（gray-level）進步到可擷取全彩影像（true-color）。

利用數位影像科技，國內的執法人員可以截取、處理、存檔、列印影像而無需暗房的協助，數位影像的鑑識應用係於所取得的影像需要強化以使其能和已知的人或物比對，但在數位影像可能有被逐一改變像素而形成偽造或變造的疑慮之

下，實施法庭交互詰問的美國透過法庭上及公聽會的辯論聽證程序，對數位影像可否做為呈堂證據雖仍在辯論中，但已接受數位影像可成為呈堂證據的佛羅里達州而言，該州刑事實驗室對數位影像的處理及標準作業程序，無疑是使該州法官及陪審團接受數位影像的重要關鍵。

本文電子檔已上傳至出國報告資訊網
(http://report.gsn.gov.tw)

目次

內容　　　　　　　　　　　　　　　　　　　　　　　　頁數

壹、目的：數位影像處理在刑事鑑識上的應用

貳、過程：

一、啟程：人事行政局在行前說明會中一再強調，出國計畫的原意是要求所有錄取的人員，以一個學校為主要研究地點，配合為二個星期的觀摩實習，故為符合計畫要求且已獲聯絡單位同意前往，選擇以下行程：

（一）康州紐海芬大學李昌鈺刑事鑑識訓練機構刑事鑑識課程，以了解康州刑事實驗室在應用數位影像於刑事鑑識方面的進展，並有機會和來自全美各地的警察同仁交換心得及詢問各地對數位影像應用於刑事鑑識上的做法。

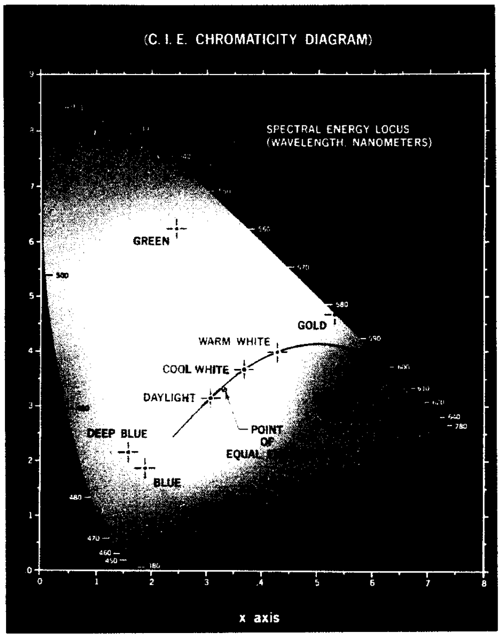
（二）佛羅里達州邁阿密戴德郡（Miami-Dade）警察局訓練中心，數位影像強化處理訓練班：學習佛羅里達州在接受處理後之數位影像證據為呈堂證供，其處理方法技巧及法庭接受的原因，該課程在簡述課程內容中刻意強調，課程的第五日為法庭交互詰問實地演練。

（三）及國際光電學會（SPIE）安全與防衛國際研討會（Security and Defense Symposium)：

二、佛羅里達州邁阿密戴德郡（Miami-Dade）警察局訓練中心，數位影像強化處理訓練班（Digital Image Enhancement Workshop)：主要內容有：

（一）介紹影像的基礎理論：自然界的光線投射於物體，物體吸收部份色光，反射部份色光，投射於人類的視網膜上，於是形成視覺，所以視覺上所獲得顏色的資訊，是經由物體表面反射而來，若無反射，則是呈現黑色，白色物體則是其表面反射所有的光所形成，在此所描述的黑色和白色並未經過其三原色的比例的檢驗，而只是觀察者在觀察時所得的經驗，可見光的頻率範圍佔自然界中自然波動的頻

率範圍很小的一部份，僅可見光和其波長的對應關係如圖一所示，色光本身具有連續性質，同時也構築我們生活週遭的美麗色彩組合。

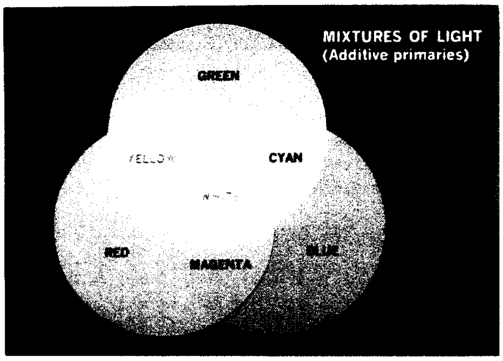


圖一：光波波長與顏色的關係（資料來源：奇異電器）。

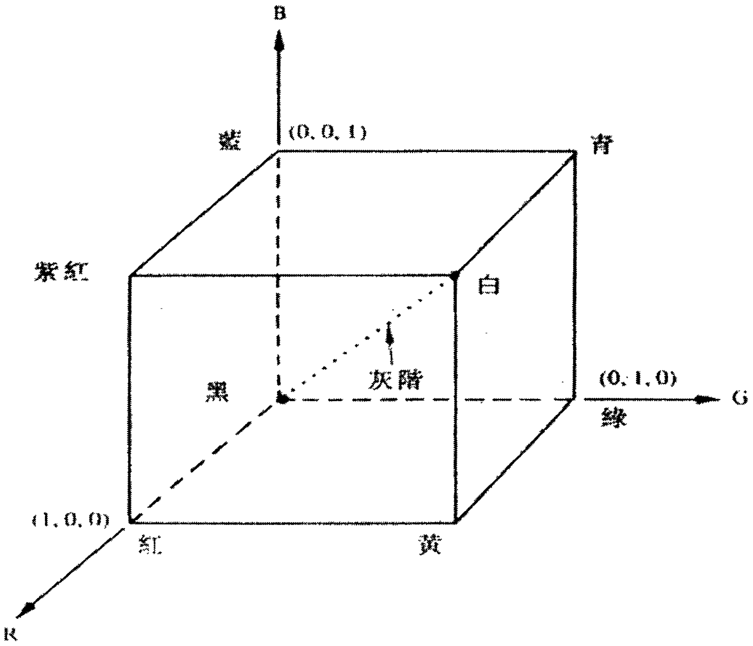
基於顏色的基本原理及應用，對顏色的定義隨著其應用範圍的不而不同，國際照明委員會（Commission International del'Eclairage ；CIE)便針對不同應用的需要，制定許多種不同的色彩規格或是色彩模型，利用彩色模型提供某種標準來指定顏色，一種彩色模型給定一個三度空間的座標，而三度空間座標中的一個點即代表一種顏色，目前常用的彩色模型有RGB、YIQ、HSI、CMY、CIE L*a*b、I1_I2_I3，各在不同的領域中應用：

L*a*b、I1_I2_I3，各在不同的領域中應用：

1、舉例來說R(紅)、G(綠)、B(藍)三原色（如圖二），在可見光譜中是利用不同的紅.綠.藍的基譜分量來表示彩色，三種色光以不同的比率和強度混合後就會產生不同的顏色，若加以一般化（normalize）後，取R.G.B.的值都在(0,1)之間,則可得到由R.G.B.三平面所組成之立方體（如圖三），從原點(0,0,0)到點(1,1,1)這條主對角線則為灰階（gray level）影像。

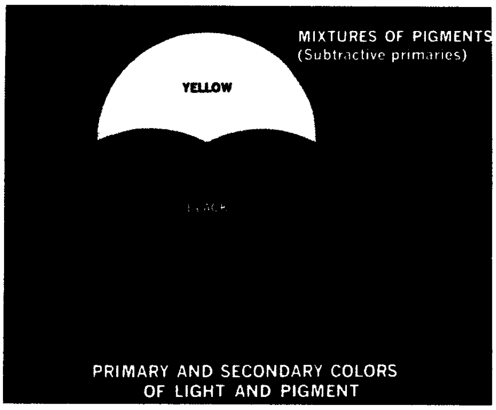


圖二：RGB三原色的組成。



圖三：三原色立體示意圖。

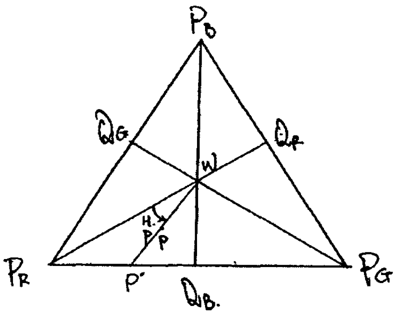
2、CYM彩色模型係由RGB三原色所組合而成的白光，分別減去紅光(R)、綠光(G)、藍光(B)，產生C(青)、M(洋紅)、Y(黃)三補色所致，應用於印刷方面色色輸出設備，如印表機（如圖四所示）。



圖四：CYM色彩模型

3、YIQ彩色模型是利用人類的視覺特性來設計的，應用在彩色電視訊號傳送的標準模型，其中Y表示亮度資訊(luminance)、I及Q表示彩色分量，因為人類的視覺系統對於亮度資訊的靈敏度大於彩色資訊的靈敏度，而且YIQ的優點是亮度(Y)和彩色資訊(I和Q)是分離的，所以一張彩色影像的亮度是可以單獨處理，而不受到它彩色分量的影響。

4、HSI亦是一種針對人類視覺所開發的彩色模型，其中I表亮度(Intensity)、H為色調(Hue)就是代表彩色純度的度量(例如純黃、純藍、純紅)、S為飽和度(Saturation)就是顏色滲入白色的程度，高飽和度的顏色代表此顏色滲入的白色愈少，而且HSI彩色模型有兩個特性，第一，亮度I和彩色資訊H、S是分離的；第二，色調和飽和度與人類的視覺感受有關，如圖五所示。



圖五：HIS 色彩模型

5、I1_I2_I3 彩色模型也是一種模擬人類視覺感受所制定的彩色模型，其中 I1 是表示亮度，I2 與 I3 表色彩資訊,當 I2 值為正值時表示色彩偏紅，I2 值為負值,表示色彩偏綠，當 I3 值為正值時表示色彩偏黃，I3 值為負值，表示色彩偏藍。

6、L*a*b 彩色模型為 Commission International del'Eclairage (CIE) 於 1931 年所提出，作為國際色彩測量標準的基礎。1976 年，這個模型經過重訂並命名為 CIE L*a*b。其中由亮度 (L) 成分；以及兩個彩色資訊成分：a 成分(由綠到紅)和 b 成分(由藍到黃)所組成。

(二)介紹數位影像在佛羅里達州司法部門的應用情形：佛羅里達州是美國第一個接受數位影像做為呈庭證據的州，但截至目前為止，該州對數位影像的處理方法僅止於對於影像的強化，影像放大的部分則未涉及，處理案件類型百分之九十五為指紋強化案件，但在國內則是百分之九十為車牌號碼的辨識，致使該州法庭接受數位指紋強化後之影像起源，起因：

1、1996 年 9 月 18 日，佛羅里達州 Pompano Beach 的一

條上，男子 Henry Guzman 的屍體在一條小路上被發現，死者的身體被以毛毯包裹，頭部則套上塑膠袋及用水管膠帶綑綁，主要死因為頭部遭到槍擊，當地警方利用雷射科技在水管膠帶上找到六枚指紋，六枚指紋送往指紋單位被鑑定為無法比對。

２、2001 年 6 月 18 日偵查員恩格斯（Engels）選擇其中三枚指紋的底片，送往布洛瓦郡州警辦公室的數位影像實驗室（Broward County Sherriff's Office Crime Scene Unit Digital Imaging Lab），由分析者 David Knoerlein 在 MoreHits 影像處理監控處理軟體監控之下，用 Adobe 公司出產的 Photoshop 軟體，以色階、型態移除、深色化及淺色化等強化影像方法後，再送往指紋部門，該三枚指紋反成為具有比對價值的指紋，並成功的比對到嫌犯 Victor Reyes。

３、因為原本無法鑑定的指紋因數位影像處理後成為可以比對，被告要律師要求法院進行符合 Frey 法則的公聽會，Frey 法則為美國證據法上對依據科學方法所提出的證據，法院可接受的原則，由法院召集該項證據相關領域的專家進行公聽會，以了解該項科技是否為普遍被接受的技術，若被法官接受方可提交陪審團進行交互詰問的法庭辯證程序，最後該三枚指紋被法官接受其具有普遍可接受的性質。

４、本案上訴期間，被告律師一再以 Photoshop 軟體可以將數位影像加入非常多的特效，使數位影像失去原來的型態來攻擊警方的證據，但是警方所提出的文件中則顯示，進行影像強化中的每一個步驟，均由該局所使用的影像監控軟體進行紀錄，且該紀錄亦已一併提

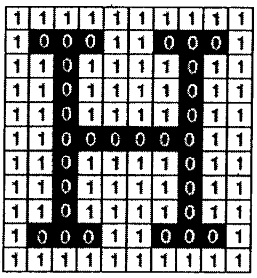
交法院，故於地方法院的判決中，被告被判有罪。

5、被告進行上訴期間，上訴法院另外進行公聽會，檢視佛羅里達州警所提出的數位影像指紋是否符合聯邦證據法中 Frey 法則及 Daubert 法則，佛羅里達州警提出數位影像運用於指紋已被美國聯邦調查局、食品藥物管理局等單位所接受使用，且數位錄影及照相已被法院接受使用有十年之久，另外，國際鑑定協會亦在 1997 年 Resolution & Legislative Committee 中承認電子數位影像在紀錄、強化及列印上與傳統底片相同經過證明是符合科學的，且被專業影像大廠、執法單位及刑事鑑識社群所接受。另外所使用的影像處理監控軟體亦已被美國聯邦調查局、食品藥物管理局等單位所接受使用，上訴法庭法官接受警方說法，同意該案指紋得列為符合證據法之證據，本案的詳細法院資料及報導，詳參附件。

三）介紹數位影像的鑑識問題及限制：

1、數位影像是拍攝景物、物體，或來自文件、照片、原稿及藝術作品的掃描所形成的電子式相片，利用方格點（或稱為像素）的標示，每一個像素的亮度值是由一串以二進位方式表示的值做為代表亮度值，每一串二進位數值的長度則代表亮度（顏色）的深度，彩色影像則是三個維度的亮度表示，各個維度各代表著紅、藍、綠三個原色，每一個像素的二進位的訊號值被電腦依序儲存成為一個以數學形態表示的影像，這些訊號值可由電腦透過檔頭的解譯成為另一種形態以展示及列印，即是我們在電腦螢幕上所見的影像組成，圖一所舉例每一個像素的深度只有 2（以一個位

元代表一個像素的值)，一為白一為黑，通常一個標準的數位照相機中每一個像素的深度都是 8（用八個二進位的符號表示一個亮度值)，用 256 階來描述黑到白色中的差異。圖六中的實例表示一個二階色階的影像，類似於經過傳真機的影像。



1	1	1	1	1	1	1	1	1	1
1	0	0	0	1	1	0	0	0	1
1	1	0	1	1	1	1	0	1	1
1	1	0	1	1	1	1	0	1	1
1	1	0	1	1	1	1	0	1	1
1	1	0	0	0	0	0	0	1	1
1	1	0	1	1	1	1	0	1	1
1	1	0	1	1	1	1	0	1	1
1	1	0	1	1	1	1	0	1	1
1	0	0	0	1	1	0	0	0	1
1	1	1	1	1	1	1	1	1	1

圖六：數位影像的概念表示圖。

2、數位化（Digitalization）這個名詞，在一般人的觀念中似乎是進步、高科技、新潮的代表，和數位系統相對的類比系統，似乎就成了守舊、退步的代名詞，但在實際上，數位化所代表的是一個對類比系統妥協及簡化處理程序的結果，因為在自然界的現象並不是以數位的方式呈現，要完整的處理一個自然界的現象必需取得其最小單位的定義，但是自然界的現象中幾乎是以實數的狀態呈現，由圖二說明數位化的情形，數位化是對時間軸上的取樣值，既是取樣，則不可能包括全部，式一中 Nyquest 取樣原理告訴我們，取樣的密度愈高，數位的結果會愈接近於真實，以一個數學的例子說明，實數系有一個重要的性質，就是稠密性，我們可以由式二中輕易的證明，在相鄰二個實數

中必定還有其他的實數存在，近代物理中最小粒子及醫學中最小的分子生物的發現也是如此，從最早期被認最小的元素，到原子、質子、電子，再到夸克粒子的發現過程中，沒有人有辦法保證再也不會有更小的粒子會出現，只是很難發現而已（或是說以目前的科技水準無法偵測），同樣地，從被認為最小的細菌，到病毒的發現，再到去氧核醣酸酸的發現，是否會是無窮無盡的發現，在現今科技水準之下，沒有人可以陳述完整，所以，既然最小的單位不可得，採用目前所知的最小單位或是大家均可以接受的單位便是一項不得不然的選擇，數位化便由此產生，所以，我們可以用另一個數系說明數位系統，那就是整數系，整數系可以用下列式三表示，在整數的點之外，均不賦予意義，同時，二個整數間所經歷的時間的倒數即為取樣原理中的取樣頻率。

３、數位化雖是較為不精密的作業方式，但是，它提供了一種簡單、快速的處理模式，可迅速地幫助我們得到結果，但僅僅是『得到結果』，是不是『理想的結果』，或是『我們希望的結果』則是另外一回事，因為後二者則和我們所採用的取樣頻率有關，以鑑別率的例子來說明，若是二個物體之間的距離小於是在我們取樣的距離（密度）以內，也可說是取樣的解析度大於標的物，則經取樣後我們並無法分辨二者，天文望遠鏡是另外一個實例，放大倍率不足的天文望遠鏡，無法使遠處的星系在我們的眼睛視覺上形成可分辨該星系中二個星球，則我們即無法分辨該二個星球存在的事實，而會認為是僅有一個星球，甚至於無法分辨整

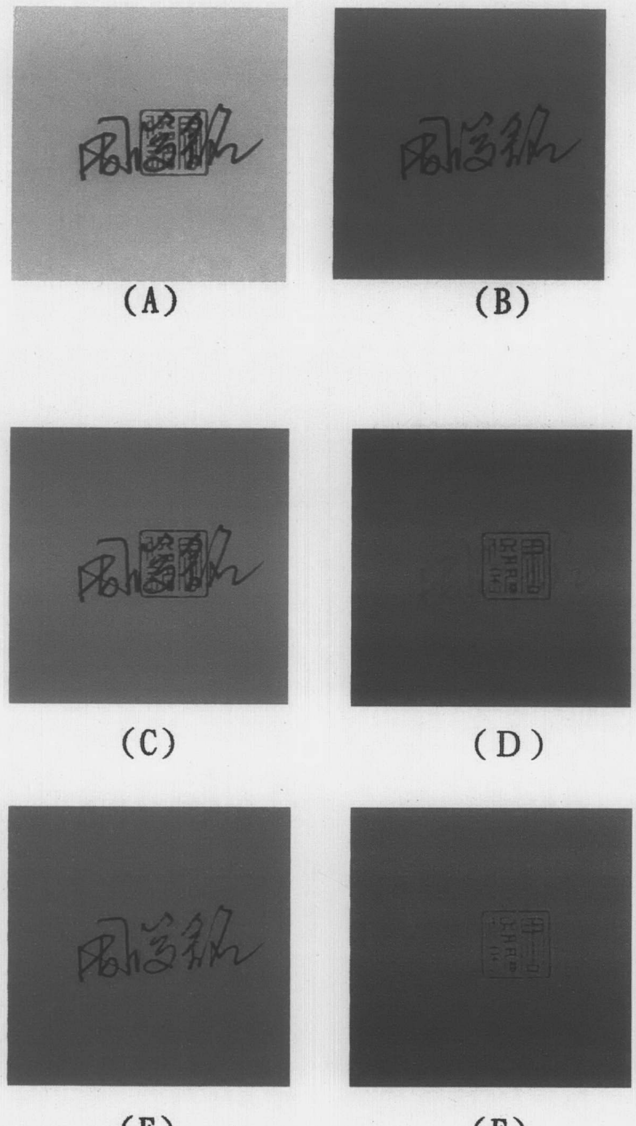
個星系到底有多少顆星球，所以在要能達到『我們希望的結果』必需依照希望取得鑑別的程度，來設計所需要的取樣頻率或是器材的精密程度，才有可能得到『理想的結果』。。

（四）傳統類比式錄音帶及錄影帶與數位影像與影像強化工具的介紹及實作—Adobe Photoshop CS 與影像監控及資料庫軟體—MoreHits 介紹：

1、佛羅里達州刑事實驗室對影像處理並不涉及放大（Rescaling）的問題，放大影像的過程中須加入內插法的運算，例如在放大四倍的影像，其中有高達四分之三的像素是經『內插』而來，也即是經過運算而得到，無法知道其原始是否與吾人內插所得之值相同，既然無法得出其為真實，則會涉及有改造變造的潛在問題，所以美國聯邦調查局在其特殊照相組中將加入內插的影像結果，稱之為分析影像（Analytical Image）。

2、強化方法：

（1）一般而言：利用 color channel 選擇一個可以使背景單純化的影像使指紋部份強調出來，再改變其色彩模式，成為灰階影像，以便進一步處理，例如以寧海得林處理過的指紋，在強化作業時僅挑選綠色的 color channel 可有效凸顯指紋的紋線，用在硃墨分離更經證明具有良好的效果，如圖七所示。



(A) (B)

(C) (D)

(E) (F)

圖七：色層分離效果。(A) 原始影像；(B) 紅色層影像；(C) 綠色層影像；(D) 藍色層影像；(E) 紅色層影像強化後結果；(F) 藍色層影像強化後結果。

（２）灰階影像模式中的指紋影像，利用黑白影像中的明亮濃度、階數（Level）的調整進一步凸顯指紋的紋線，其中反向選擇、高反差效果、亮度對比的調整需搭配使用，以求得最佳效果。

（３）區域化工具（Localize）lasso tool 對部份區域的強化具有良好的效果，而不影響其他未選擇的區域。

（４）取代顏色選項，在開始影像強化的時侯便要加以選擇，讓整體指紋的強化免除顏色的干擾，尤其在不同的平面性質上我們會採取不同的指紋採取方法，如鋁製飲料罐外表最佳採取方法為三秒膠法，但指紋採取的方法考慮因素上並不包括背景顏色，所以在濾除飲料罐上複雜的背景顏色，取代顏色便是首要處理的問題。

（５）加深顏色及顏色淡出（dodge and burn）：可對一定區域內的影像像素平均加上數階亮度值或是平均減去數階亮度值，作用在於使原本噪訊比較小較不明顯的指紋紋線，以得到良好的強化效果，但需注意，所使用 dodge and burn 的直徑，需要大於五條以上的指紋紋線距離，因為在加深顏色時若使用較小的直徑，有可能製造出不必要的指紋特徵，而使用顏色淡出的功能在使用過小直徑，則有可消滅原有指紋特徵點的疑慮。

（６）所有數位影像在輸入、處理到結束，均需在影像監控軟體的監視之下，該軟體會記載所有對數位影像的處理步驟，該州的標準作業程序中明確的

強調這項作業內，且該監控軟體More Hits本身設計上亦採用plug in的方式，在直接點選使用Adobe Photoshop時即可自動進入More Hits的監控之下。

（五）文書鑑定、鞋印、咬痕、血跡型態數位影像的應用：

1、在各項刑事鑑識相關項目的強化上，使用高像素的數位單眼相機，Nikon d100，以取得較佳品質的影像，證物照相中需使用可更換鏡頭型式的數位相機，使該相機可以同時拍攝全景及近攝的影像，康州刑事實驗室建議在拍攝近攝影像時，需同一位置及角度需拍攝二張，一張包含有比例尺，另一張則否。

2、三角架對鏡頭及相機的平衡具有助益，亦可協助取得垂直的拍攝角度。

3、拍攝鞋印影像時除前述二點以外，對形成的鞋印上的任何雜物，均不要予以移除。

4、拍攝鞋印時除了證物編號、比例尺外，建議加上地理上的方向，以利於日後的重建。

（六）法庭交互詰問詢答的表現方式及實地演練：

1、本課程由MIAMI-DADE地區檢察署二位檢察官，安排所有上課學員於上課期間所進行的指紋強化，，二位檢察官一位代表律師，一位代表檢察官，進行實地交互詰問，使學員於上課中即可得知實際於法庭論罪時，律師檢察官所關心及所問問題的方向。

2、每一個步驟的影像包括選取的範圍均以單張影像簡報方式呈現，且每一張均採相同尺寸，以方便說服陪審團，建議最後二張簡報使用完全強化結束後影像及原始影像，可更增加說服力。

3、除了使用的方法、流程的呈現，律師所問問題還包含：

（1）是否在監控之下所做的強化動作。

（2）是否有應迴避的事由，例如與嫌犯是否認識等。

二、國際光電學會（SPIE）安全與防衛國際研討會（Security and Defense Symposium）。主要內容有：

（一）各項有關安全與防衛的器材展示：最大宗者為紅外線熱影像器，紅外線熱影像器(Infrared Thermography or Infrared Imager)又稱紅外線攝影機(Infrared Camera)，乃利用紅外線感測器，配合光學鏡頭和電子電路所組成的一種設備。紅外線(Infrared) 為電磁波之一種，因源於熱效應又稱為熱輻射(Thermal Radiation)，波長範圍大致介於0.75μm~100μm 之間， 0.75~ 15μm之範圍是較常用到的紅外線光譜區。由於人類的視覺感應光譜範圍是由0.45μm 至0.75μm 之間，因此超過這個區域以外往長波長的方向，即所謂的紅外光，人類視覺並無法察覺。而因為許多訊息都是以紅外光的波段輻射出能量，要看到這些訊息，必須借助紅外線熱影像器將之轉換成電訊，再以可見光的訊號顯現出來，紅外線熱影像器應用方面，基本以軍事用途為主，紅外線熱影像器商用市場主要應用，目前大致以保養維護、監視控制、研究開發、醫療等用途為主；應用產業別則以石化、電子、能源、造紙等產業之使用為多，汞鎘碲紅外線熱影像器由於價格昂貴限制其在商用市場之發展，目前商用領域主要有警政單位之監控、海上警備、搜尋救難、保全系統等。

（二）論文發表內容涵蓋以下領域：

1、多重生物測量與融合（Multi-Biometric/Fusion）：利用紅外線、2D、3D影像中做電腦人臉的識別。

２、指紋（Fingerprint）：包括指掌紋更精確辨識的演算法、特徵的截取、更有效率的比對方式、部份指紋的比對等等。

３、人臉（Face）：包括五官的偵測、定義、分類、除錯、及在動態影像中臉部的追蹤，虹膜偵測辨別方式。

４、隱私權、安全性與效能評估（Privacy, Security, and Performance Evaluation）：包括虹膜偵測辨別方式耳朵的生物測量方式應用於門禁、出入管理等方面的方法與建議。

５、行為生物量測（Behavioral Biometrics）：包括語言的特性、簽名的特徵截取與定義、編碼。

６、生命偵測（Liveness Detection）如手部幾何形狀掃描及光學血液流動偵測以加強安全防護、手汗者指紋辨識上的加強辨識演算法、小波轉換（wevelet）偵測活體指紋掃描器。

７、3D 臉部（3D Face）：包括利用傅利葉頻譜協助偵測活人臉部、臉型固定特徵量測的 3D 模型、臉部形狀顏色的比較與組合協助臉部辨識、影像壓縮與個別變異對臉部辨識的影響評估等

８、其他生物量測：包括牙齒Ｘ光影像鑑別、虹膜組識定位方法、簽名識別、生物量測浮水印防偽等人別鑑定方法。

（三）訓練課程：參加電子影像處理課程，主要介紹：

１、影像格式、量化取樣及影像系統的介紹，包括：視覺的形成與影響因素、取樣、差異的定義與影像檔案定義及差異。

２、影像轉換：傅利葉、WALSH、HADAMARD、COSINE、HOUGH、

HOTELLING 轉換的介紹、性質、數位上的運用。

３、影像強化及還原：對比、亮度、色階、色階分布圖等影像強化方法介紹與運用，空間性質，高頻、低頻濾波器方法介紹與應用，傅利葉轉換、傅利葉轉換圓形對稱濾波器等頻譜影像濾波器的應用驗 INVERSE、WEINER 濾波器的應用，另介紹非線性濾波器如幾何平均法、YP 平均法。

４、影像識別：影像識別是指使電腦能辨識且形成判斷特定物體存在與否，最常用者為 MORPHOLOGY 的方法取得特定物體的幾何形狀，如外觀或骨架，並可小規模修補影像，再搭配閥值形成資料庫中物體的辨識。

三、紐海芬大學（University of New Haven）李昌鈺博士刑事鑑識訓練機構（Dr. Henry Lee’s Institute of Forensic Science）：參與各項刑事鑑識課程，主要內容有：

（一）槍擊案件重建：康州實驗室與佛蒙州的刑事實驗室均同樣引進與國內內政部警政署刑警察局相同的 IBIS 子彈自動比對系統，協助彈底紋的自動比對，該系統所採用的方式為影像自動比對，自動紀錄彈底特徵，但在取得數位影像時採取了下列的方式，以避免可能產生的誤差：

１、固定式子彈底座。

２、固定角度及色溫的光源。

３、前述二個因素配合固定倍率的鏡頭，使獲得的彈底影像能有一致的影像品質，且可避免因子彈彈底不夠平整，受不同角度光照射後可能產生陰影，以致產生特徵的誤認。

（二）指紋與 AFIS 特徵影像比對：指紋比對在進入電腦化後就已開始使用數位影像儲存掃描的指紋影像，針對此項，

美國聯邦調查局也規定了認可的儲存影像的格式、認可的油墨成份及使用紙張的品質等，予以標準化。

（三）刑案現場照相：

1、令人印象深刻的是美國各州的刑事實驗室仍保留自有的沖印設備，經實驗室人員解釋起因於1986年間，於科羅拉多州曾發生一起綁架案，當時的監控照片也是外送沖洗照片，但照相館員工發現所沖洗的照片可能和綁架案有關時，私自將照片賣給記者，經媒體披露，三日後便發現了小女孩的屍體，歹徒亦放棄本案，至今尚未破案。

2、利用數位影像科技，國內的執法人員可以截取、處理、存檔、列印影像而無需暗房的協助，數位影像的鑑識應用係於所取得的影像需要強化以使其能和已知的人或物比對，在美期間與來自各州刑事人員交換心得結果，美國部分州的執法單位如奥勒岡州，業已將數位相機的使用引進於所有的警察工作之中，以減少底片的積存，及暗房維持的花費。

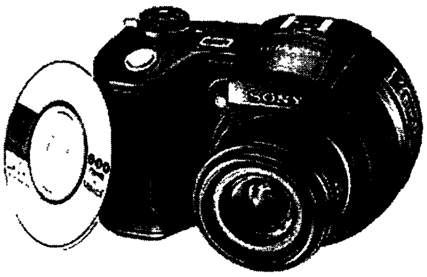
3、康州刑事實驗室仍未全面引進數位影像取代傳統的照相技術，主因是康州的司法系統尚未經過完整的討論以數位影像成為證據，故目前仍以個案討論。

（四）現場勘查技術：

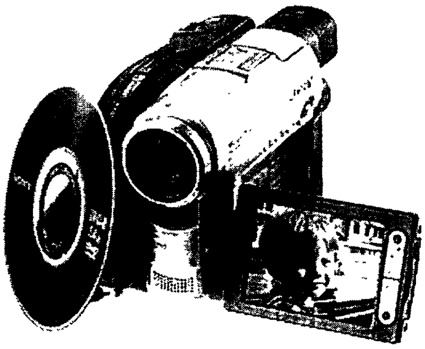
1、雖然康州的司法系統尚未經過完整的討論以數位影像成為證據，但商業公司已進一步推出著眼於證物監督鍊的數位相機及攝影機。

2、筆者於康州紐海芬大學時，正逢該學校與康州刑實驗室合作測試一款數位相機與攝影機，均由新力公司所出品，以CD-R為儲存媒體的數位相機，及以DVDR為

儲存媒體的攝影機，鑑於CDR及DVDR光碟的特性為僅能寫入一次且無法更改，可符合證物監督鍊的要求，五百萬畫素亦可符合5"*7"的沖片要求，如圖八斤示。



圖：以CDR為儲存媒體的數位像機（資料來源：新力公司）



圖：以DVDR為儲存媒體的攝影機（資料來源：新力公司）

參、心得：

一、數位化（Digitalization）這個名詞，在一般人的觀念中似乎是進步、高科技、新潮的代表，和數位系統相對的類比系統，似乎就成了守舊、退步的代名詞，但在實際上，數位化

所代表的是一個對類比系統妥協及簡化處理程序的結果，因為在自然界的現象並不是以數位的方式呈現，要完整的處理一個自然界的現象必需取得其最小單位的定義，但是自然界的現象中幾乎是以實數的狀態呈現，由圖二說明數位化的情形，數位化是對時間軸上的取樣值，既是取樣，則不可能包括全部，式一中 nyquest 取樣原理告訴我們，取樣的密度愈高，數位的結果會愈接近於真實，以一個數學的例子說明，實數系有一個重要的性質，就是稠密性，我們可以由式二中輕易的證明，在相鄰二個實數中必定還有其他的實數存在，近代物理中最小粒子及醫學中最小的分子生物的發現也是如此，從最早期被認最小的元素，到原子、質子、電子，再到夸克粒子的發現過程中，沒有人有辦法保證再也不會有更小的粒子會出現，只是很難發現而已（或是說以目前的科技水準無法偵測)，同樣地，從被認為最小的細菌，到病毒的發現，再到去氧核醣酸酸的發現，是否會是無窮無盡的發現，在現今科技水準之下，沒有人可以陳述完整，所以，既然最小的單位不可得，採用目前所知的最小單位或是大家均可以接受的單位便是一項不得不然的選擇，數位化便由此產生，所以，我們可以用另一個數系說明數位系統，那就是整數系，整數系可以用下列式三表示，在整數的點之外，均不賦予意義，同時，二個整數間所經歷的時間的倒數即為取樣原理中的取樣頻率。

二、數位化雖是較為不精密的作業方式，但是，它提供了一種簡單、快速的處理模式，可迅速地幫助我們得到結果，但僅僅是『得到結果』，是不是『理想的結果』，或是『我們希望的結果』則是另外一回事，因為後二者則和我們所採用的取樣頻率有關，以鑑別率的例子來說明，若是二個物體之間的距

離小於是在我們取樣的距離（密度）以內，也可說是取樣的解析度大於標的物，則經取樣後我們並無法分辨二者，天文望遠鏡是另外一個實例，放大倍率不足的天文望遠鏡，無法使遠處的星系在我們的眼睛視覺上形成可分辨該星系中二個星球，則我們即無法分辨該二個星球存在的事實，而會認為是僅有一個星球，甚至於無法分辨整個星系到底有多少顆星球，所以在要能達到『我們希望的結果』必需依照希望取得鑑別的程度，來設計所需要的取樣頻率或是器材的精密程度，才有可能得到『理想的結果』。

三、利用數位影像科技，國內的執法人員可以截取、處理、存檔、列印影像而無需暗房的協助，數位影像的鑑識應用係於所取得的影像需要強化以使其能和已知的人或物比對，在美期間與來自各州刑事人員交換心得結果，美國部分州的執法單位如奧勒岡州，業已將數位相機的使用引進於所有的警察工作之中，以減少底片的積存，及暗房維持的花費，故在部分州數位影像被運用於刑事鑑識各方面，例如指紋、成型紋、鞋印、輪胎印、文書鑑定、工具痕跡、破碎痕跡、血跡型態分析及咬痕，。

四、Dr. Russ 在他的數位影像的鑑識用途（Forensic Use of Digital Imaging）中便提到，一般人總會被『旭日東升（Rising Sun）』這種電影所影響，認為數位影像可以經過不斷放大，而且可以掀開影像中的阻擋物及去除被覆蓋的像素，還原原有的影像內容，這是不可能的，在每一個數位後的結果，即已將該取樣範圍內的顏色亮度值確定，小於取樣密度內的資訊被排除及統一，稱之為量化（Quantization），而無法回復，故強化是改變原有影像在視覺上的效果，讓『原本就有而不明顯』的資訊揭露，並無法憑空創造原先即沒有

的資訊，當然，若是利用其他數學的計算方式或是內插（Interpolation）的方法執行影像的放大，則僅是就其內插方法去填補放大後空缺的像素值，例如一個 100*100 像素的影像，在每邊放大二倍後成為 200*200 像素的影像，則放大後的影像像素中有四分之三是借由內插的方式來完成，但是這四分之三的像素值是否與數位照相時被量化而消失的值相同，則不無疑問，故原像素位置改變後的影像所得的結果，僅能以分析後的結果視之，無法評論其正確與否。

五、在美國期間無意中發現，美國並沒有路口測速照相的設備，使警方可以依據設備所拍得的照片來告發民眾違規的事實，經人解釋：依據美國憲法第六修正案的規定，每一個被指控的嫌犯有權與舉發他的人當面對質，另外，很多人駕駛相同型式的車子，只有超速當時駕駛超速的車子的人才能被處罰，美國法庭交互詰問制度實施已久，所有案件，包括交通警察開立罰單亦需經過法庭裁定，實施無人測速照相並無法使該照相機到庭接受交互詰問，測速照相的照片並無法明確指出在該車輛在超速的時候是誰在開車，使法庭不支持單靠照相的結果任意處罰，且警察不得隨時開啟雷達測速器，欲使用雷射測速器，需先以目測評估行駛中的車輛是否超速，如果該名警察的專業認知認為車輛以超速，則才能開啟雷達測速器的電源，測得超速後需攔下該車，不得以照片逕行舉發，直接處罰車主，但遭攔停的車輛駕駛人則必需出示身份證件及駕照及車輛保險證，若無證件，則警察有權將駕駛人上手銬帶回查證及開立罰單，與國內交通當局處置狀況十分不同。

六、國內有關影像的案件型態則不同，以筆者所服務單位，所接受的影像處理案件百分之九十五以上是路口攝影機所拍攝得

到的畫面，要求鑑識所拍得的車輛牌照號碼，但攝影機所處位置、鏡頭角度、光線、背景光線強弱等種種因素都會嚴重影響攝影機拍攝影像品質，以台北市為例，多數街口監視攝影機多數為警察局及各村里長所設置，但如何設置、影像品質如何、錄影效果如何則全權交由投標廠商處理，設立之後的鏡頭的保養、儲存媒體的更換，則未見重視，另外重複使用的儲存媒介，尤其是類比式的錄影帶，重複使用及磁頭未保養的結果則是常見磁頭的滯磁現象，使錄製的錄影帶上帶有高亮度的雜訊，有關此部份的說明，在美國聯邦調查局及及國際鑑定協會歷經數次會議，由其下的科技事務委員會所針對案件偵辦需要所草擬的設備器材的建議事項，內容多可參考，中譯說明如伍附錄一，原文則附於文末，茲就閉路電視監視系統設計上需注意事項摘要如下：

（一）所錄得影像需能分辨人身上的個別特徵。

（二）具有可檢視 NTSC 全螢幕訊號的功能。

（三）攝影機的視野不應被堵塞，也不應直接面對強光。

（四）攝影機鏡頭焦距的深度應該保持於攝影機前三呎到十呎的距離。

（五）內部或外部全景影像的攝影機所錄得的影像對調查很有幫助，但不能指望此類影像可用來提供鑑定之用。

（六）在攝影機的拍攝範圍內，足量且平均的燈光是必要的，且（燈光的）變動範圍不能超過攝影機所能紀錄的能力。

（七）系統需保持至少 30 分鐘的備用電力直到電力恢復或是關閉系統，以確保錄影內容在電力不足的狀況下不致毀損。

（八）系統的電力應為獨立迴路且適當的接地以防止外來干擾及訊號減弱。

（九）攝影機的訊號頻寬至少需 7 百萬赫茲（MHz)。

（十）文字資料的錄製對整體畫面資料的影響需降到最低。

（十一）各攝影機的訊號經過遠距離的傳輸可能會時間上的誤差應序校正。

（十二）類比式錄影系統的錄製解析度至少應具有 240 掃描線以上。

（十三）以硬碟或光碟為儲存媒介的數位影像錄影機則需以 640 像素的水平解析度及 480 像素的垂直解析度錄製每一個圖框。

（十四）建議使用不失真模式錄製啟動後的影像,製造商會使用其獨特的壓縮格式應可於原統內解為一般性的資料格式。

（十五）系統每秒每一攝影機應至少截取一個圖框。

（十六）系統不得使用多重影像顯示的模式下錄製影像(錄製分割畫面)。

（十七）系統必須能夠精確輸出影像檔案至可移動式的儲存媒體，若系統是使用所有者自行開發的儲存格式，則必須確保可使執法人員於有取得影態影像必要時,可以精確地取得以.TIFF 或是.BMP 格式的影像檔案輸出。

（十八）類比系統至少必須具備有四百條以上輸出的水平掃描線的解析度,數位錄影機必須具備有四百八十條以上輸出的水平掃描線的解析度。

（十九）系統必需一定程度的保養,使其使用壽命過程中中均能發揮一定的功效。

（二十）錄影媒介均有一定的壽命,必須在錄影媒介壽命結束之前予以更新。

（二十一）類比式匣式錄影帶建議在重覆使用前保留期限為

31 天；數位錄影內容的保存必須在無壓縮的狀態下至少足以保存十天的錄影內容。

七、佛羅里達州是美國第一個接受數位影像做為呈庭證據的州，但截至目前為止，男子 Henry Guzman 命案嫌犯 Victor Reyes 在上訴法庭，陪審團雖同意警方於膠帶上所採取之指紋強化後證明為嫌犯所有，但是指紋是位於膠帶上，僅能證明嫌犯曾觸摸膠帶，或許可參與綑綁被害人，並無法證明嫌犯殺人之事實，因此嫌犯並不觸犯檢察官所起訴的一級謀殺罪，故謀殺罪部份無罪，也因為檢察官僅就此一部份起訴，故當庭釋放，此案與我國辦案人員的思維並不相同，採取了保守的思維，但是案發現場發現的指紋與嫌犯之間仍具有時間前後不同的邏輯問題，且死者身上物品的指紋，其留存的時間，與死者死亡的時刻並不一定相同，如不相同，則指紋所有人留存指紋與死者死亡的事實並不必然相關，此間邏輯值得司法偵審人員省思。

八、93.05.17 曾向李博士詢問有關數位影像在康州州警與法院的應用情形，及對從事影像處理流程的建議，李博士講解摘要為：

（一）各地方法院接受與否情況不一，通常如果有 law challenge 的情形下，法官必需召開公聽會（public hearing），傾聽各方代表意見後，由法官決定是否接受數位處理後之證據。

（二）數位影像是否可被接受為證據，在監督鍊（chain of custody）的方面，必須保有原始的檔案，針對每一個處理的步驟，所使用的方法，設定的參數均需翔實且完整的予以紀錄，並對每一步驟所產生的結果予以另外儲存，並予以展現，俾使得以追蹤影像證物轉變的情形，可供公開

驗證。

（三）另紐海芬大學Dr. Harper解釋美國憲法第六修正案時表示：針對科學性的證據所召開公聽會，由法官決定其是否具備證據能力，再由法庭陪審團決定其可信度。

九、依據佛羅里達州布洛瓦郡及Pinella郡的標準作業程序的規定，具有下列特點：

（一）所有數位影像的儲存、傳送、備份、處理均需在監控軟體的監控之下始能為之，但實地操作時，該監控軟體在任何啟動影像編輯軟體時，必會先啟動監控軟體，以紀錄每一張影像所經歷的過程。

（二）所有儲存、備份的作為均只能使用一次燒錄的光碟，不得使用可重覆使用的光碟，以確保其原始狀態。

（三）所有的處理程序僅能在複本檔案上執行，原始檔案僅能收為保存及控制樣本之用。

（四）標準作業程序中對每一項器材的操作，採取一個口令一個動作的方式，不論硬體設備的架設、軟體作業均對每一個步驟明確的敘明。

（五）單位內人員的權限、系統維護的頻率、項目做明確的界定。

（六）附錄陸及附錄柒為該二郡標準作業程序譯文，原文參照文末附件資料。

十、2003年新力公司發表了拍攝時直接燒入CDR光碟的數位相機及拍攝時直接燒成DVD的攝影機，提供另一種符合證物監督鍊的選擇，配備140MB的CDR或是1.8GB的DVDR可以使拍攝後即燒錄成光碟型式，筆者九十三年五月造訪康州刑事實驗室時，該實驗室影像組正在評估該二型器材的適用性，一方面透過不可重覆使用的光碟特性保持數位影像本身的忠實

性，惟目前尚不了解經過該二類型機器所拍攝的光碟上，是否連同照相機或攝影機的機器碼一併燒錄在光碟上，另外，針對悪意重製的光碟是否可紀錄重製機器的序號，亦未見原製造商說明，近年來國內各執法單位漸漸有接受數位相機的趨勢，甚至在刑案現場採證及證物處理上亦有逐漸以數位相機取代，但在數位化可在軟體之中改變的特性，證物監督的完整性將更加重要，最原始影像的保留及其原始性的證明將會是一大挑戰。

十一、有關數位相機所使用之感光元件，目前使用上約可分為二類，一為光電耦合元件 CCD(Charge Coupled Device)、另一種為互補式金屬氧化半導體 CMOS(Complementary Metal Oxide Semiconductor)、CCD/CMOS Hybrid、CID(Charge Injection Device)等，其中以 CCD 的技術最為成熟、應用也最廣泛，其穩定的品質是中高階數位相機、數位攝影機的最佳選擇。CMOS 的技術近幾年才逐漸進入應用期，主因是其低耗電、低成本及高整合性的優點，廣泛應用在低階的數位相機、PC 相機、行動電話等產品，CMOS 與 CCD 最大的不同在於使用的設備與製程。CCD 的訊號必須一行一行的讀出，電荷經過多次傳遞才被讀出，其中過程須完整無缺。因此 CCD 雖然也是以矽晶片為材料，但發展出的是特殊的製程，目前所有的研發、製造技術及專利仍掌握在日系廠商手中。CMOS 感測器製程上則與隨機存取記憶體（DRAM）類似，使用一般的半導體製程、設備即可，設計業者將開發線路交由晶圓代工廠製造即可，非常適合半導體產業架構完整的台灣廠商發展。CMOS 與 CCD 二者應用於數位相機各有其優缺點，CCD 的優點為低雜訊、高感度、線路設計及製程單純、技術成熟，缺點則為 高耗電量、畫素無法隨機讀取、電荷傳遞須接近完

美無缺。CMOS優點為低價位、低耗電量、畫素可隨機讀取、相機功能可整合在單一晶片上，缺點則為雜訊度較高、感度較差、晶片線路複雜、技術尚未完全成熟，實際使用於刑事鑑識上，考量CMOS感測元件在設計上隨機與內插的應用，較可能出現失真的現象，故以求真求實的刑事鑑識運用，器材採購上，應以使用CCD為感測元件的數位相機為宜。

十二、大部分的數位相機紀錄檔案是以JPEG格式。不過是一種特殊的JPEG表示，稱之為EXIF。EXIF標準格式是由日本電器工業研發協會所(JEIDA)研發並適用於大部分機型的數位相機。這種標準格式能讓相機將其他的資訊紀錄到影像檔案內。目前所研發的最新版本為2.2。影像檔案的附加資訊包括照相時的模式，相機的設定，色彩解碼資訊，照相時的聲音紀錄及全球定位系統(GPS)資訊。紀錄的內容完全取決於數位相機的品牌和機型。通常相機製造商所附的觀圖軟體均有可以看到關於這個檔案的詳細資訊的功能。若將數位相機的檔案直接傳輸到個人電腦上(不使用TWAIN)，則您會發現新增一個名為"相機資訊(Exif)"的標籤群組。在這個群組中您可以看到拍照情況的相關資訊，像是拍照日期，快門速度，孔徑大小及其他內容。這些資訊會包含在JPG檔中，就算將數位相片複製到光碟片或其他的電腦中資訊還是會保存。不過這類資訊常會因為影像編輯工具或其他軟體進行儲存的動作而流失，對送驗影像初步檢視其EXIF檔案是否存在，可以了解是否為原始檔案，另外亦可使用一些免費軟體如BR’s EXIFextracter檢視EXIF檔案內容。

肆、建議：

一、據報載交通部預定於九十四年起全面更換車輛牌照，按我國

車牌的設計，底色多為白色之淺色，文字及數字部分為黑色或紅色，黑色的物體因為反射的色光甚少，無法在攝影機感測元件上引發電流而錄記，同時容易因為背景淺色的物體所反射光的擴散反而造成深色或黑色字體的特徵被掩蓋，人類的視覺感應亦是以較亮的部份較早引起視覺反應，以目前我國治安單位倚重各路口攝影機所拍攝的影像內容來偵辦刑案的情形，建議未來於設計車輛所使用之車牌能考慮使用深色背景，淺色字體，並加大其對比效果，以收易於辨認之效。

二、台北市政府各區建設經費使用於路口監控設備應加強使用之稽核，超廣角的鏡頭僅能收監視之效，攝影機錄製影像受限於 NTSC 的標準，截取畫面最多僅能達到 720*486 畫素，如以四分割或九分割等分割影像方式錄製，各分格畫面畫素甚少，除非能做到派人全程監控即時反應外對犯罪偵防並無實益，犯罪事件發生後對歹徒的辨識困難，徒然浪費納稅人的金錢，此外，設置系統後的保養，尤以拍攝鏡頭設置於街頭，最易因天氣或人為的影響而受損，如未能考量養護條件而一味裝設，不如不裝，另外，以錄影帶以儲存媒介者，系統維護上另需考量錄影帶的重覆使用次數不得過多，以數位方式錄製者其存檔的型式不得過度壓縮等情形，在詳細規格的制定上應參照一定標準。

三、刑案偵辦單位及鑑識單位對於數位影像設備之引進與使用，應對數位影像可能引起遭到竄改可能性的疑慮，訂定嚴謹而周密的標準作業程序，排除每一階段的空窗期，使數位影像證據在傳送、轉接均有一定的規範可循，落實證物監督鍊的管制。

四、刑事訴訟法的大幅修正後，我國司法體系改革為『改良式當事人進行主義』，檢察官必須蒞庭論罪，傳訊證人成為論罪的

重要手段，偵查或鑑識人員對於成為證人或鑑定人在提出不利於被告或原告的證詞後，常面對不利的一方提出證人或鑑定人『適格與否』的問題，相關單位亦提出相關人應通過認證的說詞，但是，如何認證？誰來實施認證？法務部？還是內政部？還是司法院？何種項目需經認證？認證程序為何？認證的效力為何？實施認證的單位有無能力進行認證？取得公務員資格的國家考試算不算認證？等問題，均未見再進一步論述與執行，建議應就此一部份儘速確定與執行，使執法人員得以取得執法專業能力之證明，增進執法之品質。

五、附錄二至附錄五為 Broward Sheriff's Office 標準作業程序及 Pinellas County 影像標準作業程序中英文對照，內容方式認具相當參考價值，提供相關單位於建立相關程序文件時參考。

伍、附錄一商業使用閉路電視（CCTV）保全監視系統建議（草案）

國際鑑定協會影像科技科學事務委員會

一、目的

（一）本文件目的的主要目的在於提供使用之系統建議給予使用閉路電視（CCTV）保全監視系統之商業機構如銀行、便利商店或其他相類機構。本文件的目的在於說明靜態獨立照相機及固定式錄影設備。本網領適用於任何使用照相機及錄影機的設備系統，同時適用於類比及數位系統，本網領內容可使錄影的影像品質在鑑定物體或個人時變得容易。

（二）儘管本文件部份內容可用於員工監守自盜等內部管理安全項目，但本文並不特別加以說明，相同的，本文亦不說明對人員的監視系統，有關這部份的說明，請參照六、附錄A。

（三）再者，本網領並不意圖變更或接管將實行本網領的特定司法機構對管理上之規定。

二、影像科技科學事務委員會（SWGIT）在商業機構應用閉路電視（CCTV）保全監視系統的角色扮演

１、閉路電視（CCTV）保全監視系統的使用及保安影像的錄製，在銀行等商業機構，已是一種被接受的習慣，為了嚇阻犯罪，這項習慣通常可容易的證明涉入犯罪個人及抒緩對犯罪的憂慮。使這些系統可以有效的進行即是影像科技科學事務委員會（SWGIT）的角色，使這些系統可以有效的進行必需符合下列原則：

（１）錄到犯罪的過程的錄影紀錄必需保存，且應提供執法機關取得正本原始影像並紀錄以符合證物監督。

（２）攝影機的數量、位置及型式應能提供監視區域內足夠的覆蓋（監視的範圍涵蓋全部監視的範圍）。

（３）監視區域內應維持有足量的燈光亮度。

（４）系統說明書及保養手冊應建立，且應依照保養手冊內規定做日常保養。

（５）系統說明書需以文件方式提出，使員工能了解於發生犯罪事件時該如何處理。

三、介紹

（一）閉路電視（CCTV）保全監視系統可能包含一個或數個攝影機，涵蓋範圍可能包括，結帳臺、通道、車道、提款機（ATM），公共團體建物的服務區域，住宅的進出口、工作場所、內部走廊、玄關、內部或外部的停車場。

（二）攝影系統包含一個攝影機、一個用來觀看影像的螢光幕，一個錄製影像機器用來錄製所挑選的影像，及一個軟體或是開關用來控制選取影像的方法，其於位置及情形的不同，攝影系統可能使用類比卡式錄影機（VCR）或是數位錄影機（DVR）或是以個人電腦為基礎的數位錄影截取工作站來紀錄來自攝影機的影像，最後，重新取得及儲存影像需併入該系統中。

（三）這份文件稱呼閉路電視（CCTV）保全監視系統主要在七個領域，分別為：

１、系統設計（五）

２、錄影系統（六）

３、攝影機（七）

４、介面（八）

５、系統維護（九）

６、資料保存（十）

７、證物的處理及提交程序（十一）

四、功能需求

（一）以下這些要求的目的在於增加執法單位於錄影資料中取出影像後可用於鑑別錄影當時的個人或物件。

（二）為了鑑別個人，則所錄得影像需能分辨人身上的個別特徵（解析度需高於分辨所需資料的解析度），例如眼睛、鼻子、嘴巴、下巴的詳細外觀、如果可以分辨更小的特徵如痣、疤痕、刺青或雀斑的型態，則將使鑑定更加容易，而且可以得到測量的結果，同樣地，對車輛的鑑定則要求需能客觀地讀出車牌的號碼，或其他可分辨的特徵。

（三）如附圖一，左側的影像較右側的影像容易做人別的鑑定，下方的影像表示上方影像目標物的頭部影像強化後的結果比較。

五、系統設計

１、閉路電視（CCTV）保全監視系統要能夠提供執法單位最大的協助助需有數個因素所配合，包含了攝影機、鏡頭、錄影機、儲存空間、壓縮格式，而這些因素之間亦不是獨立因子，而是互相作用與配合的，例如，若要在現有系統中加入更多的攝影機，則必需調整錄影來源的總和或是增加選取影像的比例。

２、系統建置前必須對每一個設計過程的環節做相當詳細的調查，包括每一個攝影機選取設置的位置及其所拍攝的角度均需作書面說明且列入調查內容的一部份。設置完成的最後，必需測試系統中所得到影像的輸出結果，具有足夠的品質以提高執法單位於鑑定影像中人或物的可能性。

（二）系統元件

1、閉路電視（CCTV）保全監視系統需包以的元件，最少一個或數個固定式或是活動式的攝影機，一個監視螢幕及一個錄影設備（包含自此錄影設備截取出來的資料的儲存設備），需要將聲音與影像同時紀錄的攝影機及其適法性的問題均需列入考慮，錄影設備的指導事項將在以下及第六點中說明，攝影機的指導事項將在以下及第七點中說明。

2、監視螢幕需包含於每一個閉路電視（CCTV）保全監視系統中，使每位操作人員能進于每日的例行性檢查（詳本文八），監視螢幕強烈建議應具有可檢視NTSC全螢幕訊號的功能（Underscan的模式），這種模式可以讓操作者檢視紀錄影像時所有視野所見內容。

（三）攝影機的數量與建置位置

1、任一假定的機構所需的攝影機的數量因各項因素的影響而不同，包括機構特別的安全需要和監視區域，應考慮確保攝影機勿設在容易被破壞或被意外調整到的位置，要將攝影機無法使用降至最低可考慮利用其他元件與攝影機結合使攝影機免於天氣和（或）機體損壞。

2、攝影機的視野不應被堵塞，也不應直接面對強光，如窗戶或亮光，如果無法避免瞄準亮光處，則應考慮於攝影機後方加光源照明或用具有背光補償的機種，使所得影像最佳化。

3、在最少的限度下，每一個出口均需至少有一具攝影機，該攝影機應瞄準向監視場所內部，每一個攝影機所設置的位置均應至少可以得到自該場所出來的個

人的頭及肩，攝影機鏡頭焦距的深度應該保持於攝影機前三呎到十呎的距離，使自該場所外出的個人可以得到良好的影像，焦距的深度保持於攝影機前三呎到十呎距離的攝影機的另外的好處是可以提供整個走廊的全景及自該場所進入或外出的個人的全身影像。

4、攝影機所設置位置應使每一個交易窗口均在鏡頭視野內無任何阻擋的情形下錄影，例如辦理窗口、自動櫃員機、免下車車道、收銀機等每一處均需至少有一台攝影機紀錄顧客交易的情形，且攝影機需聚焦於顧客可能站立的位置上，如果視野中有發現可能阻礙物如窗戶等，則攝影機的位置必需考慮儘量避免反射、強光及其他會造成無法使錄影標的的人或物清楚的阻礙物。

5、附圖一a中的人像，清楚顯示頭或肩膀較適合於出口或交易處顧客的攝影機取景之用，有關攝影機的鏡頭所需達到的視野，我們將在第七點中討論。

6、閉路電視（CCTV）保全監視系統中可提供內部或外部全景影像的攝影機所錄得的影像對調查很有幫助，但不能指望此類影像可用來提供鑑定之用，在本文中，此類攝影機的重要性會降低（不列入討論），但在系統中若是出口處及交易處的攝影機無法提供全景錄影，則可考慮另外加攝影機以達成此項目的。

7、如果必要，戶外攝影機的設置以拍攝車輛的攝影機，則攝影機必需裝置於可以直接拍攝車輛後面的位置上，且車牌號碼需清楚可讀，室外的全景攝影機的設置則可以提供其他有關車輛的資訊。

8、最後，在某些商業機構的例子，人們發現包含監視攝

影機成為安全監控策略的其中一環是有效的，這些攝影機中所見並不是為錄製影像，而是提供員工觀察其他在員工視線以外的區域，圓頂型、平底型或是傾斜型的可移動式的攝影機可以透過預設的警報裝置提供額外空間的被覆，動作偵測器或門戶接觸探測可以用來啟動攝影機，使警報時得到高解析度的影像，這項功能提供在免手動的情況下其他物體的被覆，且在一定預設的時間過後，該攝影機可以回到待命的狀態或是由固定設備進行區域的掃描錄影。

９、如果系統包含一個由控制桿控制的矩陣式開關，警衛或觀察者可以透過控制桿的操作，手動式的追蹤並將近鏡頭拉近以得到可疑人物的高解析度影像，該攝影機建議應具備有可變速度及自動對焦的功能，使追蹤可疑人物的功能更可以發揮，而在前項功能未啟的狀態下，該攝影機可以做為一個固定式的攝影機來使用。

１０、監視攝影機及鏡頭的其他資訊將在後面資料中提供。

（四）燈光

１、不足的燈光是降低錄影品質的最常見原因，在攝影機的拍攝範圍內，足量且平均的燈光是必要的，且（燈光的）變動範圍不能超過攝影機所能紀錄的能力。

２、強烈的背光及高對比的光線會使被攝影的人臉部輪廓在陰影中變得朦朧甚至消失，這將使對該人的鑑定變得困難或是不可能，同樣的，聚光燈會在臉上同時造成陰影及強調某一部份，這會造成臉上特徵色調的改變難以察覺甚至消失，例如發現臉上的毛髮結果僅是

燈光造成的效果，使用低照度且容許性高的非紅外線攝影機，通常可以考慮用來幫助改善影像品質。

3、例如架設於天花板上的日光燈會比可追蹤物體的聚光燈效果來得佳。

4、不同的光源會有不同的色溫會影響被攝物的表現顏色，鎢絲燈的光源會給被攝物表面增加紅色的色調，同樣的鈉燈會給被照謝物較多的黃色色調，大部份的彩色攝影機可對此類情形做補償，而且多是自動的。

5、在正常的光線下（日光），當一張自然的白色參照卡片放在彩色攝影機的拍攝範圍內時，彩色攝影機可以對這個特殊的白色參照物進行色彩平衡，使在這個白色的狀態下，紅、藍、綠三種原色調整到相同的輸出色階，所以室內彩色攝影機在設置之初即應做白平衡，且在燈光改變時重新做白平衡，但是，注意到部份商業機構內部燈光視不同情況下是可變的，所以白平衡也就並非隨時可以進行（市面上現在可以找到可自動白平衡的機種）。

6、紅外線光源可低亮度的情形下提供單色攝影機（黑白、夜間攝影模式 night-shot）改善品質的影像，彩色攝影機並不支援紅外線光源，因為他們會過濾紅外線的光譜，如果使用紅外線攝影機，執法人員會發現，在紅外線下照射的衣服所才到的顏色和在正常光線下所拍攝的衣服在顏色上會有相當的不同。

7、有關光源設立的技巧及建議，在附錄B中有進一步的提供。

（五）電源

1、閉路電視（CCTV）保全監視系統需要有足夠的電力以

維持，備用電源及電壓陡升防護裝備必需考慮，以確保錄影內容在電力不足的狀況下不致毀損，系統需保持至少 30 分鐘的備用電力直到電力恢復或是關閉系統，以保存錄製內容，錄影功能如 DVR 在重新獲得電力後需能回復原先操作模式而毋需人力介入，然而，在具此種功能之下，必需於卡式錄影機或數位錄影機前方面板上清楚標示在啟動設備前應先開啟或關閉此項功能（回復原先操作模式），此種自動回復啟動錄影的功能是發生先前錄影內容遭洗除或覆蓋的主要原因。

２、閉路電視（CCTV）保全監視系統的電力應為獨立迴路且適當的接地以防止外來干擾及訊號減弱，如果系統是在室外、長距離輸送電力或是易於遭受雷擊的位置，強烈建議適當的保護裝置以防止電力陡升及附近應有適度的照明。

（六）頻寬：傳送視訊的頻寬需相容、足夠、適合於下列各項錄影設備的需求，雖然最小頻寬的需求並不保證影像品質即可接受，但它扮演一定程度的重要性，為改善影像品質的可接受度，攝影機的訊號頻寬至少需 7 百萬赫茲(MHz)。

１、 噪訊比（s/n ratio）：和影像清晰度程度相關的一個主要問題就是雜訊，某些電子雜訊表現上會涵蓋整個訊號，表現有如雪花或木紋覆蓋住整個螢幕，隨後並被紀錄到錄影帶上，雜訊的來源有下列數端：不良的線路設計、熱、訊號的過度放大、外來因素干擾、自動增益控制及傳輸系統等，某些影像訊號的雜訊並無法以合理的方式解決，然而為了改進獲得可接受影像訊號的可能性，攝影機必需有 52dB 以上的噪訊比，

更進一步，在攝影機與分工器或錄影機之珀掃描線漏失的比率則不得超過 45dB。

（七）錄影的安全：系統錄影設備的機身安全及忠誠必需採行一定步驟加以確保，錄影機身所放置位置應不是一般人可自由進出之處，建議設置於上鎖的櫥櫃或房間，並依照製造規範施以週遭環境的控制。使用說明必需放在適當的地方，以備執法人員必要時得儘快取得已錄製好的影像資料。

（八）相關文字資料料的錄製：

1、類比及數位的閉路電視（CCTV）保全監視系統均有在錄製時同時加入和影像內容資料相關的文字資料的功能，如時間日期或攝影機的編號，在某些實例中，業務和個人資料有可能和影像資料一起錄製，這項功能的達成常是利用文字直接重疊於影像之上（覆蓋該處影像資料）。

2、時間日期或攝影機的編號對偵查工作而言，是十分重要的應予以保存，然而前述的文字資料存在於畫面中可能擋住標的人物的臉或車牌則反而妨害偵查工作的進行，所以文字資料的錄製對整體畫面資料的影響需降到最低，需進行試錄以了解此部份是否合於需求及錄製的文字資料內容是否正確。

3、影像科技科學事務委員會（SWGIT）建議數位閉路電視（CCTV）保全監視系統的數字資料與相對應的影像資料聯結在一起，且應無法改變，但應有指示使執法人員能從影像資料中將文字與純影像加以分離。

4、對於類比式的閉路電視（CCTV）保全監視系統，所錄製的畫面中的文字資料並無法加以抽離，則在錄製時

可將時間等錄製文字資料以一秒錄製一次（或更少），如果文字資料是在螢幕上直接可見，則其所佔螢幕的面積應在可清楚讀出的前提下愈小愈好，以減小其所可能帶來的影響。

5、每一個個體（攝影機）的影像資料均應有時間的標記，如果僅是單一攝影機直接連結到單一錄影機，則直接使用錄影機上的時間即可，但若是攝影機架設距離較遠或是透過廣域網路（Wide Area Network, WAN）來錄製，則各攝影機的訊號經過遠距離的傳輸可能會時間上的誤差，此時以影像來源（攝影機）的時間來做為時間標記是較合適的，使含有時間標記的影像檔案透過廣域網路傳輸到錄影機，趨於使用網際網路通訊協定（Internet Protocol, IP）的攝影機具有接受時間同步輸入的功能使前述同步的流程變得容易。

6、使多部電腦和數位設備時間同步化的的工業標準是網路時間協定（Network Time Protocol, NTP），這項公開標準是由網際網路工程任務編組（Internet Engineering Task Force, IETF）所發起，並以美國國家高等研究計畫署（Advanced Research Project Agency，ARPA）RFC1305號所定義的網際網路標準，這份標準明確定義時間同步化設備的精確層級，隨著基於時間安排的全球位置測定系統的進步，這類設備價格逐漸普及化。

六、錄影系統：使用於閉路電視（CCTV）保全監視系統的錄影子系統應至少符合下述最低標準：

1、類比式錄影系統的錄製解析度：類比式錄影系統的錄製解析度至少應具有240掃描線，鼓勵採用更高的解

析度。

２、數位影像錄影機（DVRs）的錄製解析度：

（１）使用數位影像錄影機最小錄製解析度隨使用的媒體的不同而不同，某些製造商採用類比系統中的掃描線數來代替數位解析度（像素），大略來說，至少 450 條的解析度可用於使用數錄影帶的數位影像錄影機，以硬碟或光碟為儲存媒介的數位影像錄影機則需以 640 像素的水平解析度及 480 像素的垂直解析度錄製每一個圖框，另外，全景錄製至少需 640*240 的解析度；影像科技科學事務委員會（SWGIT）建議儘可能使用更高的解析度來錄製影像（使用不同單位說明解析度係因製造商使用不同的工業標準）。

３、壓縮：

（１）壓縮是使數位檔案空間降低的過程，因為錄影影像每秒鐘即具有龐大的資料量，故所有的數位影像錄影設備均會以壓縮的手段來減低儲存及傳輸的需求。

（２）壓縮可分為失真及不失真，不失真的方式是指壓縮時僅有多餘的資訊被移除，壓縮後的影像可完全回復原始影像，失真的壓縮方式則是除了多餘的資訊被移除外，不恰當的資訊亦一併被移除，故壓縮後的影像無法回復成原始影像。

（３）在”警報啟動”的模式下（見），如果可能，建議使用不失真模式錄製啟動後的影像，如果系統無法以不失真模式錄製啟動後的影像，為了使執法人員在有需要時能取得最大資料量，建議在錄影

時使用最小的被壓縮量（最小壓縮比）。

（４）某些製造商會使用其獨特的壓縮格式，而必須以其獨特的流灠程式才能觀看所錄得的影像，使用這些程式會阻礙執法人員取得及處理這些影像，如果使用此類模式必須採行必要的措施以利執法人員可以順利取得影像內容。

４、長時間錄影：

（１）符合美國國家電視標準委員會（NTSC）標準的錄影機每約錄製 30 個圖框的影像，每一個圖框包含二個影像，所以實際上每秒錄製 60 個影像。

（２）類比式錄影帶通常以以下三種速度之一錄製影像：標準播放模式（Standard Play/ SP）、長時間播放模式（Long Play/ LP）及超長時間播放模式（Extended Play/Super Long Play, EP/SLP），AT-120 標準錄影帶在 SP 模式下可錄製二小時，在 LP 的模式下可錄製四小時，SLP 模式下則為六小時。

（３）長時間錄影機具有每秒鐘錄影遠少於 60 個影像，所以可以錄製一段相當長的時間，例如以 AT-120 標準錄影帶，在 SP 模式下可以每秒 60 個影像錄製二小時，在以 24 小時設定下的長時間錄影機可以錄下 12 小時的影像，每秒錄下小於五個影像，附表一表示長時間錄影機在不同的錄影模式下每秒所錄製的圖框數目。

（４）某些特製專用於閉路電視（CCTV）保全監視系統的長時間錄影機是以加大錄製圖框數量的方式加長錄影時間，與表一所示的長時間錄影機不

同，例如某些高密度的錄影帶在24小時的模式下每秒仍可錄製高達20個圖框，同樣的，數位錄影機仍可以有錄製較高圖框數量的能力。

（５）在符合影像科技科學事務委員會（SWGIT）的規範，閉路電視（CCTV）保全監視系統每秒每一攝影機應至少截取一個圖框。

５、切換開關與多路傳輸器（分割器）：

（１）超過一個攝影機以上的系統通常會採用一種設備使錄影設備可以在同一時間同時錄下來自不同攝影機的影像，這種設備可分為二種，其一是切換器，另一種是分割器。

（２）切換器就如其名，在不同的攝影機間切換，使切換器的輸出在任何時間均為來自單一個攝影機的單一畫面影像，以切換器的輸出作為錄影設備的輸入，將使錄影所得的影像為各個攝影機的輪流畫面，所有的攝影機均輪流截取影像一次所需的時間稱為"攝影機間隔"（camera interval），這個時間的倒數又稱為"攝影機更新速率"，因此一個攝影機間隔為1/2秒的系統，其攝影機更新頻率為每秒二次。

（３）多路傳輸器使用來自數個攝影機的影像且加以編碼成為一個的訊號，以使錄影設備可以連續地錄製各個攝影機的影像，編碼的方式幾乎都是各家的私人財產而沒有一定的標準可言，如此一來，透過多路傳輸器錄得的影像幾乎無法找到適用的硬體或軟體以解析回原始影像。

（４）切換器、多路傳輸器和類似的設備經常產生多重影像顯示，多重影像顯示是將螢幕區域分割使同時可以同一螢幕上觀看數個攝影機的影像，然而以此種分割畫面模式下所錄製的影像將會明顯地降低各個攝影機的影像尺寸和影像品質。

（５）因此，若為符合影像科技科學事務委員會（SWGIT）的規範，閉路電視（CCTV）保全監視系統不得使用多重影像顯示的模式下錄製影像（許多廠牌的雙工多路傳輸器可容許使用者同時觀看數個螢幕的影像，但仍是錄製全螢幕的影像）。

（６）在六、４、（５）中錄影設備需每一秒至少截取一個完整圖框，這將會限制僅有一個錄影設備的系統中攝影機的更新速率，表二即表示在不同速率的長時間錄影機中每秒每架攝影機可錄製的影像數目的對照。

（７）表二中的攝影機的數量，係假設即時錄影速率在每秒60個圖框的狀況，某些專門針對長時間錄影的特殊設計儲存設備，可能具有超過前述能力的功能，則在符合影像科技科學事務委員會（SWGIT）的規範下，該錄影設備可容許同時錄製來自更多攝影機的影像。

（二）掣動錄影機

１、某些情況下，系統可能包含掣動器，使系統可於不同於平常錄影模式一定速度或程序錄製影像，例如系統可由平時長時間錄影模式轉變為即時錄影或是由平

常並未而錄影而於鏡頭景觀區偵測動作而啟動錄影動作。

２、諸如此類的設備的運用不應違反本文六、４、(5) 中所揭示的準則，如每具攝影機每秒至少紀錄一個完整圖框。

３、測試必需完整以確保掣動系統及隨後的錄影動作可以確實運作，而不致於危及所紀錄的影像品質。

（三）遙控影像

１、某些閉路電視（CCTV）保全監視系統的紀錄及錄影主機和攝影鏡頭有一段距離，在種情形下，通常為了傳送影像資料而對影像進行一定程度的壓縮，以符合頻寬的限制，但如同本章第六節所述，過度的壓縮將會降低影像的品質。

２、這種情形在遙控監視最為常見，影像科技科學事務委員會(SWGIT)建議錄影設備應設置於每一個監視點，如此一來所錄製的影像可以使用最少量的壓縮程度。

３、在某些例子中，可由數個外來位置訊號遙控錄影設備，可能也同樣具有遙控外在位置上的攝影機的功能，這些能力應在系統日常基礎保養上確實測試，且必須建立在某一個外在位置上的設備有意外事件時人員的反應程序，遙控功能和外在位置的錄影內容二者皆能確保所應採行的步驟。

（四）警報掣動數位緩衝

１、在警報啟動的事件中，執法人員將會尋求獲致最高可能的影像品質，這包含了影像使用不失真的壓縮型式，因此，為了符合影像科技科學事務委員會(SWGIT)所宣示的準則，使用失真壓縮模式錄製影像的閉路電

視（CCTV）保全監視系統，在其系統內必須納入警報系統，並於警報模啟動後，以不失真的壓縮模式錄製影像，並盡可能使用即時模式。

２、更進一步，在警報掣動的狀況下，應要求以下所列的系統設定的警報次序，以符合影像科技科學事務委員會（SWGIT）所宣示的準則：

（１）無失真壓縮。

（２）錄影設備須至少有在警報掣動前五分鐘的備份容量，以容納無失真壓縮狀態下的影像資料。

（３）系統錄影須每秒六十個圖框，於系統切換攝影機時仍應保持此效率（亦即在長時間錄影時每具攝影機有更多的圖框）。

（４）一旦警報啟動，系統應保持無失真壓縮模式錄影直到操作人員經已建立的標準作業程序步驟以手動解除回復原先錄影模式，錄影時間至少需經歷五分鐘，直到犯罪結束或引發警報的事件結束，錄影設備至少需有在無失真錄影模式下三十分鐘以上容量空間。

（５）所有警報引發的錄影影像可以以黑白模式儲存。

（五）數位錄影機輸出設備

１、未使用可移動式儲存媒介設備（如 CDR、DVDR）以儲存每日錄影內容的數位錄影系統必需可以外接一般商用的可移動式儲存媒介設備，以備份錄影內容的副本，這對執法人員而言是必要的，執法人員於必要時可以以位元對位元的方式精確地取得某個時段的錄影內容。

２、為符合影像科技科學事務委員會（SWGIT）所宣示的準

則，閉路電視（CCTV）保全監視系統，必須裝備有含可一次寫入光碟設備（Compact Disk, CD-R)，更佳的狀況是裝配有 DVD-R（Digital Versatile Disk, DVD）的光碟輸出設備，這項較新的建議是因為警報啟動的錄影內容至少十分鐘以上（五分鐘前置時間，事件發生經過及另外增加的五分鐘)，使用 DVD-R 的設備可有效減少儲存所須的光碟片數量，所使用的 DVD-R 輸出設備應避免使用一般商用軟體的標準壓縮而應使用位元對位元拷貝的複製。

（六）輸出檔案型態

１、數位錄影系統必須能夠精確輸出影像檔案至可移動式的儲存媒體，若系統是使用所有者自行開發的儲存格式，則必須確保可使執法人員於有取得影態影像必要時，可以精確地取得以.TIFF 或是.BMP 格式的影像檔案輸出。

２、更進一步，為了讓執法人員可以於事件發生後最短時間內取得有關事件發生時的靜態影像，數位錄影系統須具備有立即以高品質數位靜態影像輸出的能力，輸出格式最好是.TIFF、.JPG 或是.BMP 格式的影像檔案，另外可輸出無壓縮動態影像檔.AVI 也是一樣重要，所有的輸出格式均須具有和原始錄影內容相同精確的能力。

七、攝影機：閉路電視（CCTV）保全監視系統所使用的攝影機須符合以下的準則

（一）黑白攝影機與彩色攝影機：雖然黑白攝影機比彩色攝影機可提供更佳的色調解析度，但彩色攝影機可提供的顏色資訊，在犯罪偵查上具有重大意義，所以攝影機的選用取

決於錄影的內容。

（二）攝影機感光元件尺寸：數位或非數位攝影機所使用感光元件（CCD感光晶片）有種型式，一般而言有四分之一吋、三分之一吋及二分之一吋，感光元件的尺寸會直接影響鏡頭所使用的焦距，更進一步的資訊將在本章第五節中說明。

（三）攝影機解析度：為符合影像科技科學事務委員會（SWGIT）所宣示的準則，閉路電視（CCTV）保全監視系統所使用的攝影機，類比系統至少必須具備有四百條以上輸出的水平掃描線的解析度，數位錄影機必須具備有四百八十條以上輸出的水平掃描線的解析度，愈高解析度的攝影機愈好。

（四）攝影機的紅外線特性：

１、某一些使用於黑白攝影機的感光元件對部份紅外線光譜具有感光能力，雖然此部份的光譜在人類視覺可感受範圍之外，但在低照度的狀況下，可提供較佳的拍攝效果。

２、自紅外線光譜所拍得影像具有使較暗衣物或物體可顯示較光亮的情況，所以具有紅外紿感光攝影功能的攝影機，不建議設置於照明良好的地方，一般而言，黑白攝影機均以外接濾光鏡解決此部份的問題，但外接濾光鏡並不適用於彩色攝影機，因為彩色攝影機內已裝設有阻礙紅外線進入的柵欄。

（五）鏡頭、焦距及鏡頭視野

１、鏡頭的選擇受到每支攝影機所覆蓋視野大小的影響，而且受到攝影機感光元件大小的支配。

２、對於想紀錄的區域（如人的臉、車牌）需佔鏡頭視野

的15%以上，對於人的臉寬度約六吋，所以鏡頭的焦距內視野約需三英呎。

3、焦距長度欲達到三呎寬的視野時，感光元件的尺寸與攝影機到物體的距離的關係如後附表三所表示，物體的位置在鏡頭內必須是清楚的。

4、提供內外全景的攝影機的焦點長度需選擇以符合視野的要求，對於出口處的攝影機須要求於三呎深的清楚距離，且在物體進出時可以清楚。

（六）曝光控制：攝影機須能在不同亮度的狀況下自動調整，以取得適光的曝光， 此類機制包，但不限於自動增益、日夜環境偵測變換及鏡頭自動光圈設計。

（七）攝影機外罩：攝影機或許需要外罩以防止不當的破壞或是自然環境的損壞，注意明亮的覆蓋物位於鏡頭前將減低影像的品質，因此，除非是特殊環境或是案全上的考量而須採用攝影機外罩，否則，不建議使用。

八、媒介：媒介包含有類比錄影帶、光碟、數位錄影帶及DVD，媒介必需是高品質及符合產品製造規格，低品質的媒介可能會損壞器材及低品質的影像。

九、系統維護：閉路電視（CCTV）保全監視系統必需一定程度的保養，使其使用壽命過程中中均能發揮一定的功效，因此以下建議事項須遵從：

（一）系統文件：機構應就所有的閉路電視（CCTV）保全監視系統保存紀錄，且文件應至少含有下列內容：

1、所有系統元件的廠牌及型號，例如：錄影機、攝影機、鏡頭、切換開關與多路傳輸器等，若是數位系統，另應包含使用的軟體名稱及版本、硬體等，附錄C即為一例，如果可能，在維護保養的紀錄表內應有一份複

本。

2、書明系統設置機構及（或）負責保養機構名稱及聯絡方式，至少包含二個絡人的姓名及電話。

3、保全監視範圍內所有器材機件設置平面圖，且應包含攝影機設置位置，而且標示每一具攝影機拍攝角度及範圍。

4、此份文件應每月更新並於事件發生後執法人員到達現場時提交給執法人員。

（二）系統確認與維護：

1、在使用之前，必須確認系統符第四章中的要求，也就是系統可以提供執法人員足以辨認人員的影像，此步驟必於每次警報過後重新確認。

2、在不同的時間進行各種的系統測試是必要的，若在測試的過程中發現有錯誤訊息產生，調整回復的步驟應確實完成。

3、維修過程及維護所進行的動作均須書面紀錄。

4、附表四即為維護的計畫表及維護內容。

（三）錄製媒體的維持

1、設置機構須明定錄影媒介內的內容的保存期限。

2、由於錄影媒介均有一定的壽命，必須在錄影媒介壽命結束之前予以更新。

3、例如錄影帶一般而言重複錄影的次數上限是十二次，超過十二次錄影帶表面會有無法預期的雜訊及影像品質降低等問題，使用長時間錄影機更是會大幅降低錄影帶的使用壽命。

4、數位錄影設備，製造商所建議的器服役時限應該要注意，對於可重覆寫入或使用的硬碟應定期的掃描硬碟

結構，避免壞軌的出現以確保錄影像的品質，另外可重覆使用的錄影媒介應在廠商保證使用次數以內即予以更換。

5、使用可重覆使用讀寫的機構應建立規範使最近錄製的內予以明文紀錄之。

十、錄影的保存

（一）類比式匣式錄影帶建議在重覆使用前保留期限為31天，這和每捲錄影帶重覆使用12次的建議相一致，每次的重覆使用均需於錄影帶的標籤上註明錄明的日期、時間及重覆的次數。

（二）由於數位錄影的本質（受限於存空間的大小），影像科技科學事務委員會（SWGIT）建議錄影內容的保存必須在無壓縮的狀態下至少足以保存十天的錄影內容。

十一、證物處理程序：本章意在提出一些當執法機關對案件有所反應時的處理程序，執法機關有反應的案件可能是搶劫或是其他的犯罪案件調查。

（一）交付執法機關的文件：系統文件，如第九章第一節中所提的，監視範圍平面圖、系統設備、聯絡資訊、保養維修紀錄均應讓執法機關可以取得，其他部份有用的資訊如錄影模式、錄影機時與實際時間的差異，亦是非常有效的資訊，附錄C提供此類資訊的紀錄範例。

（二）證據的錄影內容的處理：隨著事件的發生伴隨著執法機關的反應（偵查作為），確保執法機關可以得錄影的內容是必須的，除非錄影內容有被覆蓋的可能性，否則錄影的作為不應該被停止，直到執法人員到達為止。

1、匣式錄影帶系統：

（1）錄影停止後，錄影帶應隨即取出，在執法人員到

達前不應再被播放，更新錄影帶標籤上的日期及時間，錄影帶外包裝盒上的資料亦應一併更新。

（２）在遞交錄影帶給執法機關人員前，確保錄影帶並未錯交或損毀的動作需先執行，這包括使錄影帶遠離電視、收音機及喇叭等帶有磁性的物體，另外錄影帶本身應放置於室溫中非由陽光直接照射之處，亦不可放置於汽車中以避免高溫。

（３）在執法人員到達之前，前來協助取得影像的合格技術人員應出示身份及工具。

２、數位錄影系統：須遵照以下程序：

（１）錄影停止後，前來協助取得影像的合格技術人員應出示身份及提供有效的技術協助，出示身份可透過電話或親身前往達成。

（２）執法機關會調節人力，在人員離開犯罪現場前派遣人員檢視錄影內容並取得最佳品質影像，若是，影像有自現場立即傳遞的必要時，它們應可借由網路、電子信件、光碟或其他方法，故系統影像應可提供成 TIFF、BMP 或 JPEG 之格式，如果錄影內容儲存於較遠之處，應可提供電子信箱可供執法人員寄送影像至特定的電子信箱位址。

（３）機構的安全人員應製作二份相關的影像及錄影動畫內容於 CD 或是 DVD 上，且光碟及 DVD 應為不可重覆寫入型式，格式應為非系統所有者的獨特規格。

（４）本文六中提及的警報啟動的事件中，執法機關需要在警報啟動前五分鐘所錄得之影像，整起事件發生過程的影像及事件發生後五分鐘的影像，或

者是要求其他環境的錄影影像。

（５）如果所錄得內容是經過令狀授權，執法人員可能會通知系統所有機構保全約十天的硬碟及其錄影內容，意即執法人員可以檢視事件發生十天前的錄影內容。

（６）一旦相關的錄影帶內容及影像被拷貝，執行拷貝機關名稱、執行人員名稱、日期及時間均應標示於錄影帶標籤上加以更新，這項資訊不應寫入錄影內容中，較佳的方式為標示在錄影帶的保存器具外。

表一：長時間錄影機在不同的錄影模式下每秒所錄製的圖框數目（與正常速度每秒 60 個影像相比較）。

長時間錄影機模式（小時）	2	12	24	48	72	120	240
每秒圖框數	60	10	5	2.5（2秒5個圖框）	1.67（3秒5個圖框）	1	0.5（2秒1個圖框）

表二：不同的長時間錄影模式下，每台攝影機每秒錄製的影像數量。

每具攝影機每秒錄製的圖框數							
		長時間錄影機模式（小時）					
		2	12	24	48	72	120
相機數量	1	60	10	5	2.5	1.67	1*
	2	30	5	2.5	1.75	ˆ	ˆ
	4	15	2.5	1.25	ˆ	ˆ	ˆ
	8	7.5	1.25	ˆ	ˆ	ˆ	ˆ
	16	3.75	ˆ	ˆ	ˆ	ˆ	ˆ
	32	1.875	ˆ	ˆ	ˆ	ˆ	ˆ
	60	1*	ˆ	ˆ	ˆ	ˆ	ˆ

表三：三呎寬視野所需的焦距

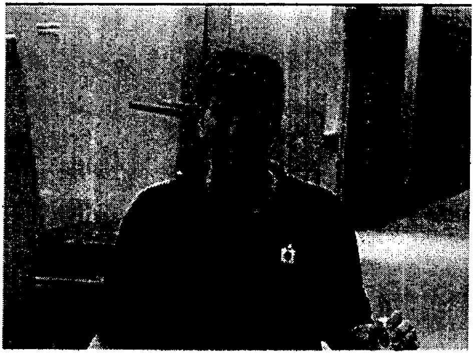
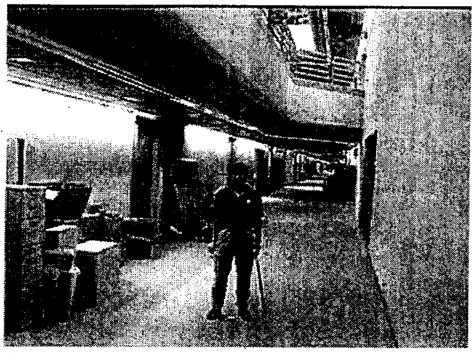
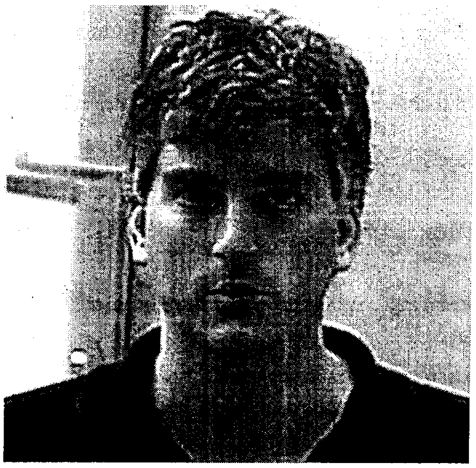
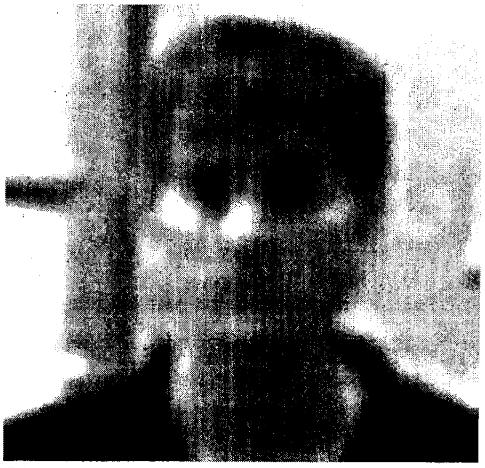
	焦距長度(mm)						
	到物體距離(f)	2’	5’	10’	15’	20’	30’
感光元件尺寸(inch)	¼”	2.3	5.9	11.7	17.6	23.5	35.2
	1/3”	3.1	7.8	15.7	23.5	31.3	47.0
	½”	4	10.1	20.2	30.3	40.4	60.7

表四：系統檢查與維護計畫表

		檢查項目	檢查步驟
檢查頻率	每日檢查內容	系統是否正常運作？	倒帶三十秒檢視所有攝影機所得影像均已錄製。
		攝影機影像是否清晰？對焦是否正確？攝影機視野內是否有阻擋物？	檢視來自各攝機的即時影像以確定之。
		時間與日期是否正確？	如何執行此項檢查依系統設計而定
		錄影媒介（如錄影帶）是否裝置妥當且在正確的模式下錄影？	檢查錄影指示燈是否亮起，且錄影計數器是否前進？
		系統保全狀態是否妥當？	檢查設備裝置外包裝及門口鎖頭狀況？
	每月檢查內容	清理攝影機外保護殼及鏡頭(視環境條件決定增加清理次數，避免機件損壞)	依製造商的說明書為之。
		使用可更換媒介（錄影帶）系統的錄影機件清理	依製造商的說明書為之。
		檢查環境條件（溫度及濕度）確定符合製造商說明書內所設定的工作環境條件	依製造商的說明書為之。
	年度檢查內容	全系統預防檢查	以合格的閉路電視監視系統技術人員進行此項檢查

		利用硬碟儲存錄影內容應進行磁碟掃描確保寫入內容正確，並確保操作系統更新	參照製造商操作指南及使用說明書
		確保寫入步驟及操作系統更新	檢視現有規定必要時予以更新
		確保工作人員勝任系統操作，尤其是警報模式下的反應	操作人員施予訓練
		確保系統輸出影像符合執法人員所需	擇一影像寫入可移置媒介（如光碟）並在另一台電腦檢視
		確保可重覆寫媒介已更換	由系統操作人員執行

附圖一

	
圖一(a) 一個可能適合作人別鑑定的閉路電視監視系統所錄得的影像	圖一(b) 一個可能不適合作人別鑑定的閉路電視監視系統所錄得的影像
	
圖一(c) 上圖 1(a)中影像經裁切、放大及強化後的結果	圖一(d) 上圖 1(b)中影像經裁切 、放大及強化後的結果

註：用做人臉自動比對系統的閉路電視監視系統其標準和本文內所建議的標準可能不同。

十二、附錄 A－閉路電視（CCTV）保全監視系統參考文獻

（一）USDOJ, Office of Justice Programs (OJP), National Institute of Justice (NIJ)
www.ojp.usdoj.gov/nij

（二）The Appropriate and Effective Use of Security Technologies in U.S. Schools, A Guide for Practical School Security Applications by Mary W. Green, September, 1999
http://www.ojp.usdoj.gov/nij/pubs-sum/178265.htm

（三）Law Enforcement and Corrections Standards and Testing Program, Video Surveillance Equipment Selection and Application Guide, NIJ Guide 201-99 by D.J. Atkinson, V.J. Pietrasiewicz, and K.E. Junker, February 2000
http://www.ojp.usdoj.gov/nij/pubs-sum/179545.htm

（四）Police Scientific Development Branch, UK Home Office
Digital Imaging Procedure Version 1.0
© CROWN COPYRIGHT 1998 FIRST PUBLISHED 2002 PSDB
Publication number 02/2002
http://www.homeoffice.gov.uk/pcrg/psdb/publications/digimpro.pdf

（五）Assessment of the ADVIS, IMPRESS, VIEW Video

Enhancement System for the UK Police Service
J Rason, T Kent, I Sall, P Gugenheim, S Walker
© CROWN COPYRIGHT 2000 FIRST PUBLISHED 2000 PSDB
Publication number 1/2000

（六）CCTV: Making it Work. Guidance on Recruitment and Selection Practice for CCTV E Wallace, C Diffley
© CROWN COPYRIGHT 1998 FIRST PUBLISHED 1998 PSDB
Publication number 8/98

（七）CCTV: Making it Work. Training Practices for CCTV Operators C Diffley, E Wallace
© CROWN COPYRIGHT (1998) ISBN: 1 84082 045 4 PSDB No: 9/98
http://www.homeoffice.gov.uk/pcrg/psdb/publications/cctv-9_98.pdf

（八）CCTV: Making It Work. Time and Date Displays A Griffiths © CROWN COPYRIGHT 1998 FIRST PUBLISHED 1998 PSDB Publication number 13/98

（九）CCTV: Making it Work. CCTV Control Room Ergonomics E Wallace, C Diffley© CROWN COPYRIGHT 1998 FIRST PUBLISHED 1998 PSDB Publication number 14/98

（十）Guidelines for the Handling of Video Tape P

Mather © CROWN COPYRIGHT 1998 FIRST PUBLISHED 1998 PSDB Publication number 21/98

(十一) Performance Testing CCTV Perimeter Surveillance Systems J Aldridge, C Gilbert © CROWN COPYRIGHT 1995 FIRST PUBLISHED 1995 PSDB Publication number 14/95

(十二) CCTV Operational Requirements Manual Version 3.0 J Aldridge © CROWN COPYRIGHT 1994 FIRST PUBLISHED 1994 PSDB Publication number 17/94 ISBN 1 85893 335 8 http://www.homeoffice.gov.uk/pcrg/psdb/publications/or_manual.pdf

(十三) UK Home Office Crime Reduction Programme http://www.crimereduction.gov.uk/cctvminisite4.htm

(十四) Crime Reduction: Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness Closed Circuit Television In Public Places: Its Acceptability And Perceived Effectiveness reports on results of an examination of public attitudes to CCTV issues. http://www.crimereduction.gov.uk/cctv3.htm 19/7/2001

（十五）Crime Reduction: Understanding Public Car Parks, Crime and CCTV: Evaluation Lessons from Safer Cities Police Research Group – Crime Prevention Unit Series Paper No. 42 (1993) by Nick Tilley
http://www.crimereduction.gov.uk/cctv2.htm
19/7/2001

（十六）Crime Reduction: Closed Circuit Television in Town Centres: Three Case Studies Police Research Group - Crime Detection and Prevention Series Paper 68 (1995) by Ben Brown
http://www.crimereduction.gov.uk/cctv1.htm
19/7/001

（十七）Crime Reduction: Transmission Guidance Guidance issued by the Home Office on the transmission of CCTV image data.
http://www.crimereduction.gov.uk/cctv25.htm
15/6/2001

（十八）Crime Reduction: A Consistent Approach to Gathering Evidence Guidelines on how police may interact tactfully with CCTV operators when gathering CCTV tapes for evidence of criminal activity.http://www.crimereduction.gov.uk/cctv24.htm 9/7/2001

(十九) Crime Reduction: CCTV Initiative: Round Two Schemes that intend to use Digital Recording Information on the operational requirements and best value for using digital recording.
http://www.crimereduction.gov.uk/cctv23.htm
16/5/2001

(二十) Crime Reduction: CCTV and the Human Rights Act The implications for the use of public space surveillance of the European Convention on Human Rights
http://www.crimereduction.gov.uk/cctv13.htm
19/7/2001

(二十一) Crime Reduction: Digital Images as Evidence Information and advice on the use of digital images as evidence.
http://www.crimereduction.gov.uk/cctv27.htm
15/6/2001

(二十二) International Association of Chiefs of Police (IACP) www.theiacp.org

(二十三) Use of CCTV/Video Cameras in Law Enforcement http://www.theiacp.org/documents/pdfs/Publications/UseofCCTV.pdf Uses and interests of over 200 responding law enforcement agencies using CCTV today.

It also highlights some of the practical considerations and policy issues police executives must consider when employing this technology.

（二十四）Police In-Car Video Camera Evaluation http://www.theiacp.org/research/index.htm The IACP will be conducting a comprehensive evaluation on the installation, use and impact of police in-car video cameras in 47 state police and highway patrol agencies. This 18-month project, commencing in June 2002, will examine and ascertain the impact of in-car cameras in four critical areas: police officer safety, agency liability, community perceptions of police, and police professionalism.

（二十五）Security Industry Association (SIA) www.siaonline.org

（二十六）SIA CCTV Surveys Survey on Evidence of Digital Images http://www.siaonline.org/page.asp?c=ig_cctv_srvy_intro Recently, the SIA CCTV Industry Advisory Board formed a sub-committee to investigate the issues around digital evidence and the impact it has on the court systems both here in the United States and globally.

(二十七) The Focus - CCTV Newsletter
http://www.siaonline.org/page.asp?c=ig_cctv_news
The CCTV Industry Group quarterly newsletter, Focus.

(二十八) 2001 Closed Circuit TV Market Report
http://www.siaonline.org/page.asp?c=storeproduct_19 MR-CCTV-2001 "Cameras everywhere" may well be the best motto for this growth industry. It is becoming a favorite tool in law enforcement; municipal infrastructure, education, retailing, medicine, commercial monitoring, residential monitoring, and a host of other market applications now made possible by video and communications technology.

(二十九) 1998-1999 CCTV for Public Safety Report
http://www.siaonline.org/page.asp?c=storeproduct_59 PSR-CCTV-1998 This third in a three volume series details CCTV for public safety application in an additional 37 U.S. cities. The 1998 report, designed to assist law enforcement and public safety officials in understanding how CCTV technology is being used and defined in the public sector, is designed to offer real-world examples of CCTV application successes and failures. Each example outlines why a program succeeded or was sent back to the drawing board. The 1998 report also provides and

summarizes examples of how state and federal legislation is defining the public sector use of CCTV technology. (355 pages) The 1998 report comes with a Privacy Supplement that details the legal and civil-rights issues associated with CCTV application in the public sector. This comprehensive resource document not only details CCTV privacy issues in the U.S., but also around the world. (75 pages)

十三、附錄 B –燈光的技術要則

（一）在本文件中有關照度的單位是流明（lux），有些較舊的文章或參考文獻可能會提到呎燭光（foot candle）的照度單位，1 呎燭光約等 11 流明（lux）。

（二）為了使攝影機提供較佳品質的影像，在攝影機視野所覆蓋的範圍內應保持在 275~333 流明（lux）的照度。

（三）對於在外部的自助式機具，如自動提款機的門廳及出車道，每天二十四小時均應提供 110 流明（lux）以上的照度。

（四）外部區域如走道、入口、夜間保險箱在攝影機視野所覆蓋的範圍內至少應保持在 55 流明（lux）的照度。

（五）停車場在攝影機視野所覆蓋的範圍的地面至少應保持在 11 流明（lux）的照度。

（六）自動提款機或是其他自助式區域以附加的燈光提供使用者臉部的照度是必須的。

十四、附錄 C – 系統文件及設置場所平面圖範例

系該設備資料:

錄影機廠牌及型號

多路傳輸器廠牌及型號

攝影機廠牌及型號

錄影型式（圈選） VHS SVHS DVR（數位錄機） 電腦 其他

若是數位錄影機或是電腦者:

硬體製造商 軟體名稱及版本

是否附有最近維修紀錄影本?（圈選） 是 否

系統錄製多部攝影機?（圈選） 是 否

如果是，有幾部?

聯絡資訊

錄影系統的聯絡資料:

姓名 電話:

系統所有機構聯絡資料:

姓名 電話:

如果系統錄製多支攝影機影像，標示各攝影機位置及視野範圍（範例如下頁）

其他事項

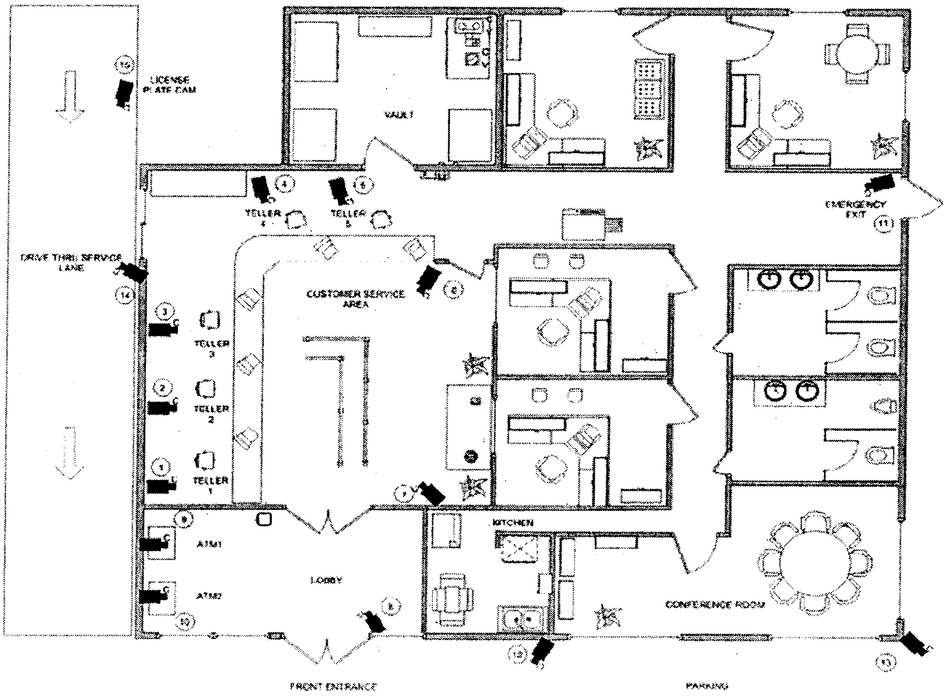
系統使用何種錄影模式（小時）?（圈選）

2 6 12 24 48 72 其他 未知

錄影機時間和實際時間是否相同?(圈選)　是　　否

事件發生日期/時間
錄影帶上事件發生日期/時間
錄影帶自系統取出日期/時間
其他:

EXAMPLE OF SITE PLAN FOR
SMALL BANK



攝影機 1 : 朝東第一位交易員

攝影機 2: 朝東第二位交易員

攝影機 3: 朝東第三位交易員

攝影機 4: 朝東第四位交易員

攝影機 5: 朝東第五位交易員

攝影機 6: 朝西南顧客服務區

攝影機 7: 朝東北顧客服務區

攝影機 8: 朝西南大廳

攝影機 9: 大廳一號自動提款機

攝影機 10: 大廳二號自動提款機

攝影機 11: 朝西緊急出口

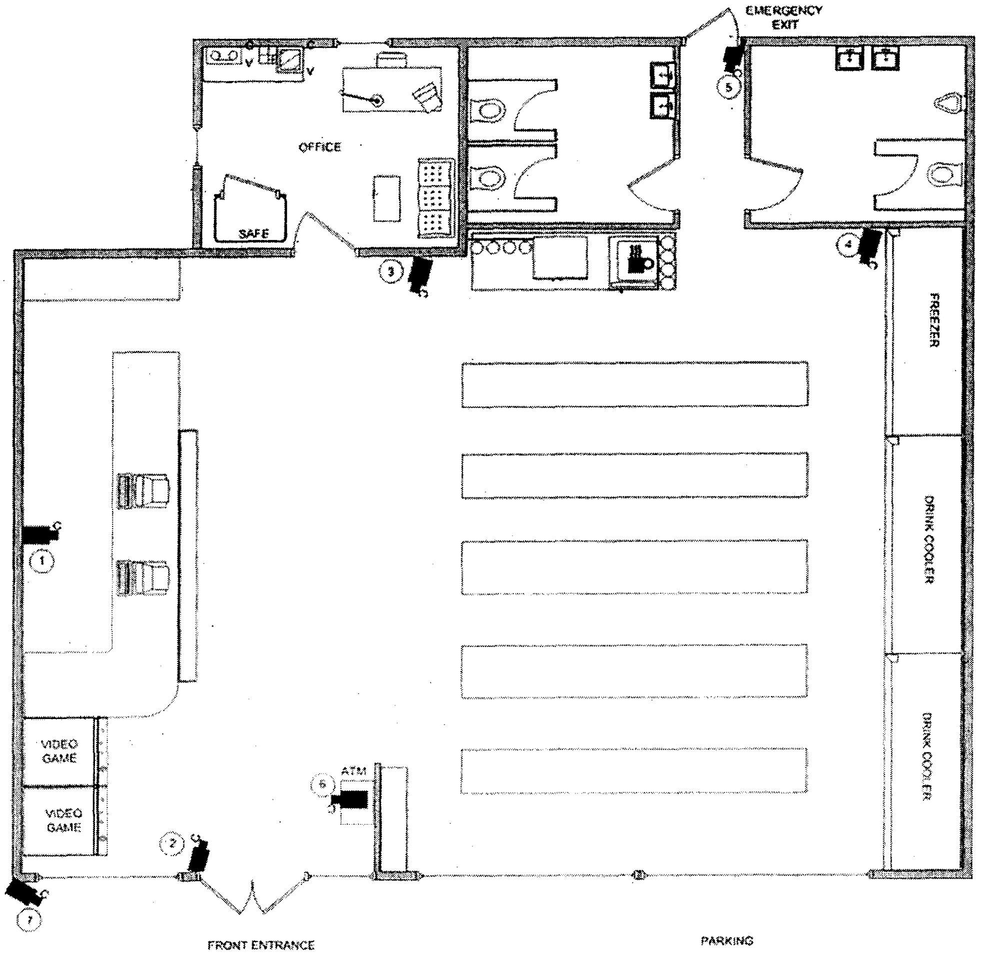
攝影機 12: 外部停車場

攝影機 13：大樓西南角停車場

攝影機 14：朝西免下車服務區車道

攝影機 15：朝南免下車服務區車道

EXAMPLE OF SITE PLAN FOR
CONVENIENCE STORE



攝影機 1 :	朝東櫃檯
攝影機 2:	朝北前門入口
攝影機 3:	朝南辦公室外
攝影機 4:	朝南冰箱區
攝影機 5:	朝南緊急出口
攝影機 6:	朝西自動提款機
攝影機 7:	朝東南停車場

陸、附錄二：布洛瓦州警辦公室刑事現場部門（Broward Sheriff’s Office Crime Scene Unit）標準作業程序—數位影像截取與處理

一、背景

（一）布洛瓦郡州警辦公室刑事現場部門（Broward Sheriff’s Office Crime Scene Unit）業已購置影像截取裝置及個人電腦基礎的影像強化設備，且相關人員業已歷經相關訓練，習得使用本設備的相關技巧。

（二）本影像系統包含三個部份，第一部份是移動式截取設備，第二部份是固定式截取設備，第三部份則是實驗室部份，移動式截取設備係提供予布洛瓦郡州警辦公室刑事現場調查部門於犯罪現場勘查時，拍攝現場採取所得指紋，固定式截取設備則是供布洛瓦郡州警辦公室刑事現場調查部門與指紋室人員於證物處理顯示指紋後，拍攝數位化指紋以評估及鑑驗之用，實驗室部份係為管整套系統及處理、列印處理過後的數位影像。

（三）本系統的使用與管理係依據布洛瓦郡州警辦公室刑事現場部門標準作業程序操作手冊，僅有熟悉標準作業程序與受過良好訓練的部門人員可以獲准操作系統截取及處理指紋。

（四）操作人員除應具備前述能力外，另在系統部份針對每一位可操作系統人員執行密碼管控，分級管制。

（五）本系統管理者係由布洛瓦郡州警辦公室刑事現場部門監督者指派。

（六）本系統的使用及標準作業程序的訂定係參照聯邦證據法則及現行有關電磁紀錄證據的判例。

（七）使用本係統不應排除任何員工依標準方法以取得指紋影像，但使用不同的方法則需布洛瓦郡州警辦公室批准。

二、任務

主要係利用本系統的器材以取得指紋影像後並加以強化，文書血跡、咬痕、鞋印、輪胎印影像的取得則為本系統的邊際效應。使原始或強化的影像均符合法令上的要求。針對影像截取到儲存及處理及處理結果的一步驟，準備庭證所需的文書資料。

三、目標

（一）布洛瓦郡州警辦公室刑事現場部門（Broward Sheriff's Office Crime Scene Unit）和指紋室於必要時得以如同往常一般拍照方法進行，取得指紋的數位化照片。

（二）每一個布洛瓦郡州警辦公室刑事現場部門（Broward Sheriff's Office Crime Scene Unit）和指紋室的員工均需熟練標準作業程序及訓練手冊內的要求有關指紋數位影像的處理。

（三）每一個布洛瓦郡州警辦公室刑事現場部門（Broward Sheriff's Office Crime Scene Unit）和指紋室的員工強化，文書血跡、咬痕、鞋印、輪胎印影像的取得的器材僅限於布洛瓦郡州警辦公室所核可者為限。

（四）針對調查中的案件是否決定使用數位影像技術取決於案件的複雜度，原始指紋影證物的品質、依傳統方法重新取得完整印痕的能力及藉由數位影像處理改善品質的潛而定。

（五）依據布洛瓦郡州警辦公室的要求、標準作業程序及訓練

手冊以維持最高標準的工作產出。

四、訊息傳遞

（一）所有在刑事現場部門及刑案分析部門的監督者間的訊息傳遞均需清楚及明確。

（二）為使數位影像部份及指紋室間訊息傳遞方便容易，刑案分析者應經常與該部門的成員溝通，以確保所截取及強化後的數位影像能達到預期可比對。

（三）刑案分析者應和監督者溝通以獲致同步的更新訊息。

五、品質管控

（一）犯罪實驗室品保協調員應管理數位影像實驗室的品質管控事宜。

（二）於數位影像單位工作的每一個人均有責任隨時反應有關品質控制的問題給品保協調員，以便採取必要步驟。

（三）刑案分析員負責所有文書資料品質管控，品保協調員及（或）刑案現場監督者將更新及檢查這些紀錄。

（四）每一個指派至數位影像單位工作的員工，依照品質管控計畫，將被要求必需通過數位影像處理熟練度測驗及年度測驗。

（五）數位影像器材有任何不尋常的問題應立刻報告該單位主管。

六、安全性

（一）所有數位影像工作單位的人員均需遵守由布洛瓦郡政府、布洛瓦郡州警辦公室及現場部門所建立的安全規則。

（二）人員於處理具有生物性危害或以指紋粉末或化學藥劑

處理過的證物，在使用數位影像單位的器材時均應穿戴單位發放適當的防護裝備。

（三）急救藥箱應放置於人員隨手可取得之處。

七、人員配置

（一）系統管理者（刑案分析者）應負責全部系統元件的維護，並於系統出現超過管理者維護能的問題時，聯絡適當廠商進行處理。

（二）僅有刑案分析者、犯罪現場監督者所指派的人員及受過良好訓練的人員可以從事位影像強化的工作。

（三）犯罪現場監督者具有管理及調派數位影像單位人員的權力。

八、系統及影像保安

（一）通往州警辦公室，刑案現場組數位影像部門的門於無使用時應上鎖。

（二）進入數位影像部門的權力系由 Johnson 門禁管制系統所控管，且此項管控非重大緊急案件不得被推翻。

（三）州警辦公室，刑案現場組數位影像部門應利用 More Hits 鑑識影像追蹤軟體於存檔、追蹤、處理及輸出數位指紋影像。

（四）只有受過More Hits鑑識影像追蹤軟體使用訓練的人員能操作、進入 More Hits 鑑識影像追蹤軟體系統電腦及檔案，受過 More Hits 鑑識影像追蹤軟體使用訓練的人員將可獲得一組獨立的密碼，取得操作電腦的權力。

（五）州警辦公室，刑案現場組監督者指派一位系統管理者，負責維護 More Hits 鑑識影像追蹤軟體系統，此管理者在

其他子輔助系統之管理者之外為惟一具有全部系統的管理及操作維護權。

（六）員工對 More Hits 鑑識影像追蹤軟體系統操作權限，係由系統管理者依據該員對系統的熟悉及受訓程度而定。

（七）系統管理者需維護系統操作、檔案存檔、系統備份、輸出影像檔案及由其他 More Hits 系統操作的工作紀錄。

（八）所有用以比對的數位指紋影像均需於 PC Pros 電腦上的 More Hits 系統下操作，以便透過系統軟體追蹤完整的操作處理過程。

（九）所有在 PC Pros 電腦上的 More Hits 系統下操作調整的影像，均須進入歷程追蹤，以便操作者可重複操作步驟，這項安排用於指定所有人員操作步驟統一化。

（十）存檔或是檔案輸出的文書資料均應保存於州警辦公室刑案現場組數位影像部門的工作紀錄上。

（十一）鑑識影像處理須由提出處理要求的人員填寫州警辦公室刑案現場組數位影像部門影像追蹤表格後始為之。

（十二）連結於 More Hits 系統上的數據機僅指定用於 PC Pros 電腦的技術支援進行遠距系統診斷之用，禁止使用於一般網路，且數據機需保持關機狀態，除非技術人員於檢修期間要求遠距系統斷方得開。

（十三）More Hits 系統配備有不斷電系統，以避免於突發性斷電時造成資料遺失，More Hits 系統的操作任何時間均需在已連接不斷電系統的情形始得為之。

（十四）數位鑑識影像系統的元件（或）軟體，為刑案分析者或系統管理者所單獨保管，任何非經授權使用該系統的員工均需得到現場組長官的許可

九、器材

（一）現場工具組：用於現場人員在現場截取數位影像可能包下列器材，但不限於以下所列內容：

１、Fuji S1 數位相機

２、Nikon D1 數位相機

３、Nikon D1X 數位相機

４、Nikon 鏡頭

（１） 28-85 mm macro zoom

（２） 60 mm micro

５、1 GB micro drive 記憶卡

６、PCMCIA Type II compact flash 記憶卡

７、攜帶式電源

８、交直流電源轉換線

９、手提電腦（Dell Inspiron）

１０、三角架

１１、三角架配件

１２、電子閃光燈

１３、LCD 螢幕

１４、攜帶式LCD 螢幕電源

（二）截取工作站：用於刑案現場組截取數位影像可能包下列器材，但不限於以下所列內容：

１、Kodak DCS 420 數位相機

２、Nikon D1X 數位相機

３、Nikon D1 數位相機

４、Fuji S1 數位相機

５、Nikon 鏡頭

（１） 24-50 mm zoom 鏡頭

（２） 28-85 mm macro zoom 鏡頭

（３） 35-105 mm zoom 鏡頭

（４） 60 mm micro 鏡頭

（５） 50 mm 鏡頭

６、PCMCIA Type II compact flash 記憶卡

７、可攜帶式 PCMCIA 讀卡機

８、SCSI 介面電腦連接線

９、Evolution 5000 PC 電腦

１０、連接至 Digital Lab之乙太網路

１１、17” 彩色螢幕

１２、具可調式燈源的翻拍架

１３、多波域光源

１４、雷射

１５、平台式掃描器

（三）數位處理實驗室：用於數位實驗室截取數位影像可能包下列器材，但不限於以下所列內容：

１、“PC Pros” 牌電腦 PC based Pentium 4, 2.00 Ghz tower computer ，windows XP 作業平台

２、Lacie 80 GB 外接式硬碟

３、連接至截取工作站的乙太網路

４、“Viewsonic” P815 21” 彩色螢幕

５、“Seagate”內接式磁帶驅動設備

６、“Microtech” 內接式 PCMCIA 讀卡機

７、“Toshiba” 內接式 compact disc (CD-ROM)

８、“Plexwriter” 內接式 CD 燒錄器

９、“Agfa Duoscan” T1200 平台掃描器

１０、“Kodak” Model 8650 熱昇華印表機

１１、“Kodak” Model 8660 熱昇華印表機

１２、“Lexmark” Model Optra S 1855 雷射印表機

１３、“HP” Deskjet 952c 噴墨印表機

１４、“US Robotics” 56K 外接式數據機

１５、“Polaroid” SprintScan 35 Plus 底片掃描器

１６、“Smart Pro” Triplite 不斷電系統

十、各單位架構

（一） 現場工具組

現場工具組主要用在刑案現場直接截取影像之用，利用一個5英吋的LCD直接觀察截取時的時像，所有在現場截取的影像立即進入建置於刑案現場勘查車內的膝上型電腦內的More Hits影像追蹤資料庫，截取影像者負有取得最佳影像品質的責任，另外，在該現場所有影像均截取完成後，需將所有截取的影像燒錄成CD-ROM光碟存檔。

（二） 截取工作站

截取工作站設置於刑案現場組辦公室裡的雷射室內，用來截取潛伏指紋的影像及潛伏證物的數位影像進入More Hits影像資料庫，一架NIKON D1X數位相機架設於翻拍架上，並直接電纜連接至電腦，它容許操作人員於每截取一張影像後並顯示在螢幕上，在此可直接調整亮度、濾鏡或使用化學藥劑增顯指紋，以取得最高品質的證物影像。工作站並有另一台平台式掃描器

連接至電腦，以便取得文書或其他二維的證物的影像進入資料庫。每一位刑案現場組的員工都有二個密碼，第一個用來啟動工作站的作業平台，第二個則用來啟動More Hits影像追蹤資料庫軟體，現場工具組所取得的影像亦利用此工作站取出再利用乙太網路將影像檔案存入位於數位處理實驗室的伺服器內，規定所有員工於處理完畢後，需將系統登出並關機。

（三） 數位處理實驗室

所有截取或儲存的影像均存入More Hits影像資料庫伺服器中，分析者或路其他指定人員將會分析存入的所有影像，決定何者需要強化，何者僅需檔存，所有影像的處理包括強化，均僅能由分析者予以紀錄及執行，影像強化的歷程及其他和該影像相關的資訊均會被存入資料中，當同一案中所有影像均通過強化等處理程序後，每一張強化後影像和原始影像會列印1比1的輸出，一份複本會傳遞回原送驗單位承辦人，當同一案所有影像均處理完畢或工作單填記紀錄連同處理的影像會燒在一張CD-ROM內以備存檔，每一張光碟會指定一個流水序號存放於數位處理實驗室內的保險內。僅有分析者和刑事鑑識主管擁有保險箱的鑰匙，數位處理實驗室透過乙太網路和富士網路列表機相連，該列表機是以密碼保護，僅分析者和刑事鑑識部門主管可使用。

十一、各單元操作方法

（一）現場工具組：配件有：

１、Fiji S1 camera body

２、60mm macro lens

３、24-50mm zoom lens

４、128mb “Flash Cards”

５、1 GB. Micro drives

６、AA batteries

７、S1 AC power adapter

８、Remote release cord

９、Monitor patch cable

１０、62mm Orange filter

１１、Nikon SB28DX flash unit

１２、Flash extension cable

１３、Monitor Kit

１４、Laptop Kit

１５、Portable Video Light

１６、Fiji S1 架設程序

（１）插入空白紀憶卡

（２）選鏡頭 Micro 適合指紋拍攝

（３）光圈優先

（４）手動對焦

（５）光圈值調到最大

（６）張單拍攝

（７）影像品質無壓縮 RGB/TIFF 每張約 17mb

（８）自動白平衡

（９）ISO 200

（１０） 相機架在三腳架上

（１１） 連結快門線

（１２） 連結螢幕接通螢幕電源

（１３） 連結螢幕及相機

１７、影像截取程序

（１）CLOSE UP

（２）比例尺和指紋同時攝入

（３）用適當光源

（４）拍攝

（５）記錄拍攝位置

（６）IF 紀憶卡滿關電源後才取出

（７）紀憶卡遠離電場磁場高熱

（８）取得影像燒錄 CD

（９）全部影像燒 CD

（１０）放入保護套貼上證物膠帶，油性筆簽日期及燒錄人姓名

（１１）使用 EXIF 軟體選擇所需影像進入 More Hits

１８、現場匯影像進入 more hits

（１）先登入 More Hits

（２）建立案號

（３）選取要匯入記憶卡上的影像

（４）正規化（取影像上 1 公分距離）

（５）刪除暫存影像及記憶卡上影像

（６）填寫影像追蹤單，送驗單

（二）現場影像實驗室的做法

１、 開啟登入 More Hits(lab 的 laptop)

２、 匯入原始cd於暫存區

３、 燒錄cd光碟

４、 刪除暫存檔案

５、 該cd放入實驗室電腦，匯入檔案

６、 確認資料無誤

７、 取出cd 封存

（三） 影像截取工作站

１、證物處理：注意生物性證物可能引起的污染問題

２、工作站器材

（１）Nikon D1x digital camera

（２）Nikon Lenses

24-50 mm zoom
28-85 mm macro zoom
35-105 mm zoom
60 mm micro
50 mm

（３）PCMCIA Type II compact flash storage card

（４）Firewire cable connection to computer

（５）Evolution 5000 PC computer

（６）Ethernet connection to Digital Lab

（７）17" color monitor

（８）Copy stand w/adjustable lights

（９）Alternate light sources

（１０）Laser

（１１）Flatbed Scanner

3、Nikon D1x 架設程序

（1）翻拍架，焦距約等鏡頭數值的1.5倍

（2）Nikon 24-50mm zoom = approximately 36-75mm

（3）和螢幕及電腦連

（4）相機用 ac 電源

4、影像截取

（1）基礎相機設定

光圈優先模式

光圈值11或更大

不曝光補償

含比例尺攝入畫面

儘可能使指紋最大

建議階層曝光（增益值+較亮，-較暗），使曝光分階段

階層（級）曝光時光圈值應仍保持在11以上，曝光時間會加長，但可拍得景深會較長

（2）監控軟體

雙按 More Hits 按鈕

選擇自己名字

輸入自己的密碼

選擇”image”

滑鼠移到”acquire”

選擇”twain setup”

Select DCS camera

Click on (Image)

Move cursor to (Acquire)

Click (Twain)

輸入案件編號

建立新案名後會自動啟動 kodak 驅動介面

....

（３）取得影像

自 kodak driver intrerface 取得影像

利用影像內比例尺正規化

輸入案名

儲存並登出

*可一次輸入多張影像

5、 日誌資訊

（１）日誌資訊係由由影像實驗內的分析者所管控，包含送驗偵查員所輸入的案件的基本資料，及分析者處理進度所加註的訊息，例如已列印、已處理等，日誌本身可做為分析者的參考及偵查員的進度追蹤之用。

（２）以下資料由送驗偵查員輸入：

影像取得日期

案 類

案件編號

取得影像人員

鑑識組帶隊官名字

鑑識組實驗室編號

機構代碼

機構案號

機構帶隊官

處理資訊

截取位置

截取方法

附註

（３）影像分析者需輸入資料：

強化日期

核對無誤勾選欄

列印無誤勾選欄

列印日期

列印數量

發送對象

附註

歸檔日期

歸檔卷冊編號

十二、數位影像處理實驗室　分析者及管理者標準作業程序

（一）一般原則

１、儘可能的提供最高品質的指紋證物影像是布洛瓦州警辦公室刑案現場部門影像組的目標，同時維持最高的影像程序正當性，利用科技標準電腦化的影像設備及技術，應用於清晰度不佳的指紋影像時，能改善其可見度、正確性及較少的時間的浪費。

２、自現場及各勘查組所有截取的影像，均以數位化的型式透過網路儲存於影像實驗室的伺服器中，現場勘查人員於影像截取工作站中利用數位相機或讀卡機截取影像，同時，截取工作站可透過網路登入位於影像

實驗室中的MoreHits資料庫，一旦影像進入資料庫，分析者有責任予以強化，每一個步驟均需仔細予以紀錄，所有強化的動作均僅能在複本上中執行，原始檔案則不得有任何刪除或改變，強化動作完成於對影像中每一個像素均完成調整後，強後影像和原始影像的差異僅在於像素上數值的不同，將此二影像相減即可得到二者的差異，亦即強化後的影像是可由原始影像加以複製的（鑑驗結果具有重現性），紀錄強化後的結果，使經過本局刑事鑑識科現場調查部門影像組的影像可以由分析者複製。

（二） 影像強化

１、原始影像不得改變，強化前須先複製一複本，所有的強化動作均在複本上執行，原始影像做為後來每一階段的控制項。

２、在MoreHits的軟體在影像強化功能被執行時，即可自動產生影像複本，且該複本影像自動在Adobe Photoshop中開啟，並且同時開啟Adobe Photoshop的強化歷程紀錄對話框。

３、分析者將實施任何強化方法至他認為影像細節最清楚為止，每一個強化方法執行的過程均被紀錄到強化歷程紀錄對話框中，甚至連顏色模式的替換均加以紀錄。

４、 影像強化處理結束，強化後影像及歷程紀錄均可回到MoreHits的資料庫軟體之下。

５、 個案中的所有影像均處理結束後，該個案之所有影像均將被存檔，所有影像、案件資訊、處理歷程紀錄均

將永久被燒錄到光碟上。

6、被選取存檔的影像，在存檔完成時原電腦上影像即被刪除。

7、存檔的光碟上將標記上包含案件資料、日期、案件號碼的記號。

8、一片光碟上將不限僅一件案子，端視個案強化的影像數量而定。

9、檔存光碟儲存於影像 實驗室內上鎖的保險箱內，僅有分析者與刑案現場部門主管可取得該處光碟。

（三） 影像分送

1、影像實驗室可分製成以下數種型態的輸出媒體：

（1）熱升華彩色列印

（2）熱升華黑白列印

（3）富士牌彩色黑白數位印表機

（4）惠普 950C 彩色噴墨印表機

（5）黑白雷射印表機

（6）CD-R 光碟片

（7）3.5 吋磁片

（四）指紋影像

1、所有指紋影像均送往指紋室作 1:1 的列印輸出。

2、所有指紋影像送往指紋室在影像室以熱升華彩色印表機列印。

3、所有送往指紋室的指紋影像均會回到該案現場勘查人員處。

（五）其他影像

1、分析者將依據影像品質選擇印表機。

2、 檢驗品質將使用黑白雷射印表機、 惠普 950C 彩色噴墨印表機或富士牌彩色黑白數位印表機列印。

3、 照片品質的影像則利用熱升華彩色列印或富士牌彩色黑白數位印表機列印。

4、 若送驗單位有要求光碟或磁片，分析者將在光碟或磁片外註記，且該光碟內將附有 More Hits 影像觀賞程式，允許送驗人員於無 More Hits 軟體的電腦上亦可流灠光碟內影像。

5、 刑案現場部門管理者必需核准使用網路傳送影像。

（六）影像品質控制

1、分析者必需監控所取或獲得的全部份影像，以確保刑案現場部門人員適切使用器材。

2、分析者將直接告知送驗承辦人需配合事項。

3、新器材或新程序實施，分析者應教導刑案現場人員。

（七）影像存檔

More Hits 影像追蹤軟體一個特殊的功能即是可將影像在軟體的監控下予以備份存檔，在存檔的過程中，系統將原始及強化後影像傳送到一個暫存的資料夾中，俟存檔的動作完成，暫存的資料夾中的檔案即被燒錄到 CDR 光碟中，光碟的燒錄必需使用”單次燒錄”（single session burn），而不能以多次燒錄的功能（multi-session burn），以避免資料的可能毀損，另外主系統並用一磁帶定期做備份，以避免尚未存檔的資料遺失。

十三、其他單位要求的影像處理（適用對象：分析者及刑事鑑識

管理者）

（一） 證物處理

1、證物收集、包裝、監管程序請參閱 BROWARD COUNTY SHERIFF'S OFFICE, CRIME SCENE UNIT, STANDARD OPERATIONAL PROCEEDURES 手冊

2、證物請影像組鑑驗需附二件文書：證物收據及送驗單

3、分析者需作工作底稿

4、分析者需留意防護手套，證物上可能含有血跡及體液而有生物性危害的可能，故證物不得與影像實驗室的器材有直接接觸。

5、證物在影像實驗室內仍需保持證物監管鍊的關係。

（二） 影像截取裝置（數位影像實驗室內使用於證物處理）

1、平台式掃描器

（1）平台式掃描器以取得反射式的真實本質

（2）平台式掃描器掃描成 1:1 或真實比例的影像

2、Agfa Duoscan T1200 平台式掃描器，預設以 1200DPI 解析度掃描。

3、Agfa Duoscan T1200 平台式掃描器使用逐步解釋 step by step （仍是在 More Hits 軟體下取得掃描影像及加以正規化）

4、Polaroid SprintScan 35 Plus 底片掃描器

（三）影像強化

1、原始影像不得改變，強化前須先複製一複本，所有的強化動作均在複本上執行，原始影像做為後來每一階

段的控制項。

２、在 MoreHits 的軟體在影像強化功能被執行時，即可自動產生影像複本，且該複本影像自動在 Adobe Photoshop 中開啟，並且同時開啟 Adobe Photoshop 的強化歷程紀錄對話框。

３、分析者將實施任何強化方法至他認為影像細節最清楚為止，每一個強化方法執行的過程均被紀錄到強化歷程紀錄對話框中，甚至連顏色模式的替換均加以紀錄。

４、影像強化處理結束，強化後影像及歷程紀錄均可回到 MoreHits 的資料庫軟體之下。

５、個案中的所有影像均處理結束後，該個案之所有影像均將被存檔，所有影像、案件資訊、處理歷程紀錄均將永久被燒錄到光碟上。

６、被選取存檔的影像，在存檔完成時原電腦上影像即被刪除。

７、存檔的光碟上將標記上包含案件資料、日期、案件號碼的記號。

８、一片光碟上將不限僅一件案子，端視個案強化的影像數量而定。

９、檔存光碟儲存於影像 實驗室內上鎖的保險箱內，僅有分析者與刑案現場部門主管可取得該處光碟。

（四）影像分送

１、 影像實驗室可分製成以下數種型態的輸出媒體：

（１）熱升華彩色列印

（２）熱升華黑白列印

（３）富士牌彩色黑白數位印表機

（４）惠普 950C 彩色噴墨印表機

（５）黑白雷射印表機

（６）CD-R 光碟片

（７）3.5 吋磁片

（五）影像存檔

More Hits 影像追蹤軟體一個特殊的功能即是可將影像在軟體的監控下予以備份存檔，在存檔的過程中，系統將原始及強化後影像傳送到一個暫存的資料夾中，俟存檔的動作完成，暫存的資料夾中的檔案即被燒錄到 CDR 光碟中，光碟的燒錄必需使用”單次燒錄”（single session burn），而不能以多次燒錄的功能（multi-session burn），以避免資料的可能毀損，另外主系統並用一磁帶定期做備份，以避免尚未存檔的資料遺失。

十四、數位實驗室系統維護

（一）系統維護：維修紀錄

１、軟硬體保證書及操作手冊需填寫及保存於影像實驗室

２、器材維護及修理紀錄保留於影像實驗室

３、MoreHits 的資料庫由原廠商負責保養

（二）每日保養內容

１、截取工作站及數位影像實驗室的每日保養，可由分析者透過網路對截取工作站及數位影像實驗室的電腦檢查。

２、截取工作站數位相機內的影像每日更新刪除

３、系統管理者可取得電腦內登入及登出的資料。

（三）每週保養養內容

磁帶系統備份

（四）每月保養內容

１、所有器材清潔

２、螢幕與印表機顏色模式應相同

（五）每年保養內容

１、一年至少二次執行系統執行診斷

２、More　Hits 軟體設定、硬體裝設及系統更新均應由原廠保固

十五、日誌與紀錄

（一）日誌保存於影像實驗室

（二）日誌可供所有現場人員查閱其所送的案子的進度

（三）MoreHits 會主動追蹤登入及登出人員與其所送驗案件資料，且會紀錄登入的時間、人員等資料。

（四）僅有分析者或管理員能流灠或列印日誌

十六、統計數字

分析者每月依據以下資料製作統計資料：

１、取得影像的數目

２、強化影像的數目

３、比中指紋的數目

４、本郡案件處理數目

５、其他單位案件處理數目

６、非犯罪數位計畫數目

７、参與訓練時數

8、指導訓練時數

9、出庭作證時數

十七、訓練

（一）任何數位影像或將影像數位化的工作人員至少需接受以下性質的訓練：單位作業程序、基礎數位影像技巧、影像截取程序、若需利用影像處理，則另加MoreHits影像追蹤軟體。

（二）每一位現場勘查人員及指紋單位人員需熟悉標準作業程序及訓練手冊，了解作用於指紋的數位影像處理。

（三）所需受訓的等級及種類由刑案現場組主管基於人員介入案件程度而決定。

（四）使用處理數位影像的工作人員需熟悉由刑案現場組所公布用以追蹤影像處理的內部紀錄單

十八、精確度的試驗

（一）使用數位影像系統的現場組人員都必需接受標準作業程序熟練度的訓練及測驗，分析者負責提供使用數位影像系統的現場組人員的訓練計畫，當軟硬體改變時或現場組長官要求時得再舉行測驗。

十九、展示

分析者需對現場組主管所指定其他人或團體作系統簡報或展示。

二十、法庭

原始影像及強化後影像及強化影像的資料的副本將被視為呈堂證物，或是作成簡報型式在法庭解釋影像強化過程。

柒、附錄三：Pinellas County Sheriff’s Office 標準作業程序

生效日：

處罰日：

一、目的：

建立使影像組人員不論底片或是數位型式的影像均能收集、處理、儲存、保存影像標準作業程序

二、討論：

紀錄現場的影像應該比照證物保存，隨著影像科技的進步，全盤考慮證物監督關係是更重要的，儘快提交影像給偵查單位或檢察署

三、定義：

（一）影像股長：影像組主管

（二）影像技士：影像組工作人員

（三）影像組：刑事鑑識部門內的單位，負責錄影帶驗影像處理

四、步驟：

（一）系統保全

１、刑事影像科技的應用需保持證物監督鍊關係，一接到證物立刻填上送驗單位提供的案件编號

２、僅限影像組人員及直屬長官可使用影像組的器材，做影像像的紀錄、管理、儲存與處理

３、進入電腦、網路連結、軟體使用均須密碼管控

４、可攜帶式的儲存工具（floopy, CD, DVD,ZIP……..）

均需儲存於保險箱中，且僅限影像組人員及直屬長官可取得。

5、底片及原始檔案出影像組二要件：法律程序、主官核可，二者須同時成立。

6、影像組人員不在，送驗證物放置於門外固定盒內，盒須上鎖，僅影像組人員及直屬長官可開啟該固定盒。

五、數位影像檔案

（一）影像收到其他單送驗影像，先儲存原始檔案於安全的電腦上，並立刻轉燒於永久非揮發性的媒介上（不可複寫或重複讀寫，或稱為電子負片），及編定一永久流水號，原始檔案不得刪除或更改

（二）影像可由流水號及案名索引

（三）影像處理僅可由影像檔副本為之，影像強化工具僅限使用傳統暗房可達到效果的工具：

（１）校正對比和明暗度。

（２）校正色彩平衡

（３）放大或縮小

（四）不得以強化後之檔案取代原始檔案，須另存新檔且存於永久非揮發性的媒介上。

六、底片

（一）本鑑識單位所拍攝底片會保留於影像組，外單外送來需處理之底片，先送資材部門列財產，處理完後，再還資材課。

（二）州警其他成員或簽約商送來底儲於影像組

（三）其他州執法單位送來底片處理後歸還原單位，除非送驗

單位或鑑識主管同意才存放影像組

（四）偵查員送底片需附底片清單，註明日期、報告書文號、報告型式、拍攝人

（五）外單位偵查員送驗（洗）底片需附送驗單，且註明必要資訊。

（六）外單位偵查員送洗底片後，影像組負責沖片、印相，如有要求放在網路上，然後切底片存檔

（七）前述切完後底片存於影像組內有安全防護櫃子內鎖

（八）前述切完後底片儲存依報告單號碼及年份編碼儲存

（九）底片上影像將在列印之前以平台式掃描器掃描

（十）要求以數位列印的底片，將送到外面本鑑識單位主官認可的相館列印，底片的強化與數位影像強化相同的程序

七、影像的散布

（一）原始底片或影像有要求時，24小時內複本會被放在影像組網路伺服器上，以便檢察官或偵查察取得。

（二）因操作原因，下列案件非經特別要求不會放置於內部網路上：

1、偵查中的凶殺案

2、性犯罪

3、兒童被虐待案

4、家暴案件

5、車禍案件

6、縱火案件

7、毒品案件

（三）進入內部網路僅限執法人員且在本局防火牆內

（四）獲授權進入網站流灠照片者僅限流灠其目的照片，且不

得更動照片內容，安全層級依需要及單位而定，例夜盜小組不會被授權流覽凶殺組的照片。

（五）照片列印需求可填寫下列表格傳送至影像組即可

（六）當公設辯護人或律師要求處理且被接受，首先需確認州檢察官辦公室的交辦單是否在CJIS終端系統上有存檔。

（七）影像基於審判與調查中才會列印，任何時候均應強調安全的電子傳送在。

（八）代私人律師、保險公司、市民列印相片或製作影像檔收費，費用逐案認定且向請求者收取

（九）至影像組領取影像者需出示身份證明

（十）本局除案件承辦人為應付調查或起訴所需外，調閱照片應取得鑑識主官同意或承辦人授權。

（十一）提供照片給公開調查案件的本單位成員或非本單位成員，或是本單位員工涉訟調閱照片，事先應得到法律顧問室的許可。

八、器材管理

（一）影像組負責移撥給現場部門的照相器材的保養。

（二）現場部門應建立刑事鑑識主官授權給偵查員照相器材的紀錄

（三）非授權的照相器材應在刑事鑑識部門主管的指導下良好保存於科技服務大樓內。

（四）影像組組員、刑事鑑識股長或其指定人員可發配未受指定的器材，一份日誌將會被建立如同這些器材已被分配給偵查員，以下的資料可能包含但不限於日誌內：

１、35mm照相機組

２、120mm空中照相機組

３、留存的數位相機

４、錄影機組

５、留存的記憶體載台

６、錄影機組

九、影像組需和後勤組合作及時維修無法操作或損壞的照相設備，維修必需經過刑事鑑識主管的核可。

（一）影像組技術人員在刑事鑑識主管指導下，將協助獲取新資訊，研究、科技或器材計畫，以提供足夠且最新的操作。

（二）影像組技術人員需對所有的器材依製造廠商所建議事項執行必要的維護，且維護內容需紀錄於維修日誌上，維護需包含但不限於：

１、小型暗房

（１）每次輪值操作控制帶

（２）執行每日檢查事項

執行月例行性維護，包含清理底片架或清理、更換顯影液濾網

２、底片掃描器

（１）每月清理空氣濾網

（２）必要時更換燈泡

３、印表機／螢幕

（１）依製造商建議事項校正

捌、Broward Sheriff's Office 標準作業程序（英文）

BACKGROUND

The Digital Capture and Computer Enhancement of Developed Latent Fingerprint Evidence

The Broward Sheriff's Office Crime Scene Unit has acquired the equipment to provide for the digital capture and computerized enhancement of latent fingerprint evidence. In addition, members of the Broward Sheriff's Office Crime Scene Unit and Latent Fingerprint Section have been trained in the technology to take advantage of this equipment in a laboratory environment.

The imaging system shall consist of three platforms, one portable, one capture station, and one laboratory based. The portable system shall be utilized by members of the Broward Sheriff's Office Crime Scene Unit to capture latent fingerprint evidence during an investigation at a crime scene. The capture station shall be utilized by members of both the Broward Sheriff's Office Crime Scene Unit and Latent Fingerprint Section for the capture of latent fingerprint evidence for the purpose of fingerprint evaluation and/or examination. The digital lab will be utilized to manage the entire imaging system, and enhance and print digitally captured images.

The use of this equipment shall be governed by the Broward Sheriff's Office, Crime Scene Unit Standard Operating Procedures Technical Manual. Only those employees familiar with the Standard Operating Procedures (SOP) Technical Manual and having completed training in the operation of the system's, shall utilize this equipment for the capture and or processing of latent fingerprint evidence.

In addition to each employee being properly trained and being familiar with the Standard Operating Procedures, each system shall be password protected. The computer systems will have security levels established in addition to the individual passwords issued, which will be overseen by a System Administrator(s) who will have total access to the system.

The assignment of the System Administrator will be at the discretion of the

Broward Sheriff's Office Crime Scene Unit Supervisors.

The utilization of this equipment and the development of the (SOP) Technical Manual shall be guided by established Federal Rules of Evidence and existing Court Case Law in regard to electronically recorded evidence, and the use of digitally captured and processed latent fingerprint evidence.

The use of this technology shall not preclude any employee from utilizing standard methods for the purpose of recovering latent fingerprint evidence, but should be utilized as any other tool currently in use by the Broward Sheriff's Office Crime Scene Unit to recover latent fingerprint evidence.

MISSION STATEMENT

To capture high quality images of latent fingerprint evidence using digital imaging equipment, thereby providing the ability to digitally enhance those images of latent evidence, documents, blood spatter, bite marks, footwear impression, and tire impressions that may be of marginal value..To be able to validate the integrity of both the original and enhanced versions of each and every image that is captured and acquired into the Digital Imaging System. To prepare testimony and documentation for courtroom proceedings for every step involved in the capture and enhancement of digital images taken and processed by the Broward Sheriff's Office, Crime Scene Unit, Digital Lab.

OBJECTIVE

The BSO Crime Scene Unit and the Latent Fingerprint Section shall utilize forensic imaging for the capture of latent fingerprint evidence when necessary, in the same way as conventional photographic techniques are currently used.

Every Crime Scene Unit and Latent Fingerprint Section employee will familiarize themselves with the Standard Operational Procedures (SOP) and Training Manuals concerning the handling of digital images to be used as latent fingerprint evidence.

The equipment used by BSO personnel to digitally capture and enhance latent fingerprint evidence, documents, blood spatter, bite marks, footwear impression, and tire impressions shall include only those items approved by the Broward Sheriff's Office Crime Scene Unit.

The decision to utilize forensic imaging technology during an investigation shall be guided by the type of case involved, the quality of the original latent fingerprint evidence, the ability to recover the impression intact using conventional methods, and the potential for improved quality through the use of forensic image processing.

Maintain the highest standard of work product as dictated by the Sheriff's Office. Policies and Procedures Manual as well as the Crime Scene Unit Standard Operating Procedures Manual.

COMMUNICATION

1. All communications between the supervisor of the Crime Scene Unit and the Forensic Analyst shall be clear and concise.
2. To facilitate open dialog and information dissemination between Digital Imaging personnel and members of the Latent Fingerprint Section, the Forensic Analyst will meet regularly with individuals from that unit to ensure the quality of the images being digitally captured and enhanced are expectable for comparisons.
3. The Forensic Analyst shall communicate with supervisors keeping them abreast of upgrades.

QUALITY ASSURANCE/QUALITY CONTROL

1. The Crime Lab QA Coordinator will oversee the Quality Assurance and the Quality Control of the Digital Imaging Lab.
2. It is the responsibility of anyone working in or for the Digital Imaging

Unit to report any quality control problem to the QA coordinator immediately so that the appropriate action can be taken.

3. The Forensic Analyst will have the responsibility for maintaining all quality control documents. The QA coordinator and/or the Crime Scene supervisor will handle updating and reviewing these records.
4. As part of the Quality Assurance Program each person designated to do digital imaging will be required to satisfactorily complete a digital imaging competency test and an annual proficiency test.
5. All irregularities or problems associated with the digital imaging components will be immediately reported to the supervisor of the unit.

SAFETY

1. All safety procedures established by the Broward County Government, the Broward County Sheriff's Office, and the Crime Scene Section, which includes State and Federal regulations will be followed by the Digital Imaging Staff.
2. When handling evidence, which poses a potential biohazard, or evidence, which has been treated with fingerprint powders and/or chemicals, personnel using digital imaging equipment will wear the appropriate personal protection equipment provided by the unit.
3. A First Aid Kit shall be maintained within easy access to all unit personnel.

STAFFING

1. A System Administrator/Forensic Analyst will be responsible for the maintenance of all the components of the system, and will contact the appropriate vendor when maintenance / repairs are required which are beyond the administrator's knowledge and ability level.
2. Only the Forensic Analyst and those individuals that have been assigned by the Crime Scene Supervisor, and have been properly trained as an imaging specialist will be allowed to perform image enhancements to original images.
3. The Crime Scene Supervisor will have authority over all digital imaging personnel and will be responsible for staffing of the Digital Imaging Unit.

SYSTEM AND IMAGE SECURITY

1. The door to the Broward Sheriff's Office, Crime Scene Unit Forensic Imaging Section shall be closed and locked when not occupied.
2. Access to the Forensic Imaging Section shall be controlled via the Johnson Controls Card Key Access device only, and the standard door lock access shall not be overridden except in a case of emergency.
3. The Broward Sheriff's Office, Crime Scene Unit Forensic Imaging Section shall utilize the PC Pros "More Hits" Forensic Image Tracking System for archiving, tracking, processing and output of latent fingerprint images.
4. Only those employees trained in the PC Pros "More Hits" system will operate or have access to computer components and files within the "More Hits" system. Those employees shall then be issued an individual password to gain access and utilize the "More Hits" system
5. The PC Pros "More Hits" Forensic Image Tracking System shall have a System Administrator assigned by the Broward Sheriff's Office, Crime Scene Unit Supervisor. That individual along with any designated Assistant System Administrator(s) shall be the only employee with total control over the system access and maintenance.
6. An employee's level of system access will be determined by the System Administrator(s), based upon the employee's level of training and involvement within the system.
7. The System Administrator(s) shall maintain Control Logs in regard to system access, archiving of system files, system back up and exportation of image files for viewing and or processing by another "More Hits" system.
8. All images utilized for latent fingerprint comparison purposes shall be processed only within the PC Pros "More Hits" Forensic Image Tracking System, so as to provide tracking and integrity of the processed images through the system software.
9. All image adjustments utilized within the PC Pros "More Hits" Forensic Image Tracking System shall be entered within the tracking history, so as to allow.the repeatability of the individual processes used

by the operator. The terms and format used to designate the adjustments shall be standardized throughout the agency.

10. All documentation for archived files and exported files shall be retained within the Broward Sheriff's Office Crime Scene Unit Forensic Imaging Section Logs.
11. Forensic image processing shall only be performed after proper written request is made via a Broward Sheriff's Office Crime Scene Unit Forensic Image Tracking Form, by the employee requesting the processing.
12. The modem attached to the "More Hits" system is designated for use by "PC Pros" Technical Support personnel for remote system diagnostics, and will not be utilized for internet use. The modem shall remain turned off unless requested by support personnel for those periods required for remote system diagnostics.
13. The "More Hits" system is equipped with an auxiliary power back-up system to prevent power surges and loss of data in the event of a power outage. The "More Hits" system will not be utilized at any time with the unit disconnected.
14. The Forensic Digital Imaging System's components and or software will be operated exclusively by the Forensic Analyst or the System administrator. Any request by unauthorized employees to utilize any part of the system, must be approved by the Crime Scene Supervisor.

EQUIPMENT

Field Kit

(1) The equipment utilized for the capture of digital images by Crime Scene personnel in the field may include, but not be limited to the following items:

- Fuji S1 digital camera
- Nikon D1 digital camera
- Nikon D1X digital camera
- Nikon Lenses
  28-85 mm macro zoom
  60 mm micro

- 1 GB micro drive
- PCMCIA Type II compact flash storage cards
- Portable battery power supply
- AC to DC power adapter
- Laptop computer (Dell Inspiron)
- Tripod
- Tripod Accessories
- Electronic flash equipment
- LCD monitor
- Portable battery power supply for monitor

Capture Station

The equipment utilized for the capture of digital images in the Capture Station by Crime Scene personnel may include, but not be limited to the following items:

- Kodak DCS 420 digital camera
- Nikon D1X digital camera
- Nikon D1 digital camera
- Fuji S1 digital camera
- Nikon Lenses
  24-50 mm zoom
  28-85 mm macro zoom
  35-105 mm zoom
  60 mm micro
  50 mm
- PCMCIA Type II compact flash storage card
- Portable PCMCIA card reader
- SCSI interface cable connection to computer
- Evolution 5000 PC computer
- Ethernet connection to Digital Lab
- 17" color monitor
- Copy stand w/adjustable lights
- Alternate light sources
- Laser

- Flatbed Scanner

Digital Processing Lab

The equipment used by the Forensic Analyst to capture, enhance, and archive images in the Digital Processing Lab will include but not be limited to the following items:

- "PC Pros" brand PC based Pentium 4, 2.00 Ghz tower computer running a windows XP operating system
- Lacie 80 GB external hard drive.
- Ethernet connection to Workstation
- "Viewsonic" P815 21" color monitor
- "Seagate" internal tape drive
- "Microtech" internal PCMCIA card reader
- "Toshiba" internal compact disc (CD-ROM)
- "Plexwriter" internal compact disc writer
- "Agfa Duoscan" T1200 flatbed scanner
- "Kodak" Model 8650 dye-sublimation printer
- "Kodak" Model 8660 dye-sublimation printer
- "Lexmark" Model Optra S 1855 laser printer
- "HP" Deskjet 952c Inkjet printer
- "US Robotics" 56K external modem
- "Polaroid" SprintScan 35 Plus film and negative scanner
- "Smart Pro" Triplite UPS (Uninterruptible Power Supply)

BASIC UNIT STRUCTURE

The Digital Imaging System will consist of three basic components.

The Field Kit will be used to capture digital images of latent evidence at crime scenes. A 5 inch LCD monitor will be available to view images at the time of capture. All images that are captured in the field will be immediately acquired into the MoreHits Forensic Image Tracking database, located on the Digital Imaging laptop, in the Mobile Crime Scene Response Vehicle. The individual that captured the original images will be responsible for acquiring the best quality images into the MoreHits database. In addition an archive "CD" will be burned at the scene of all the images captured.

The **Capture Station** will be located in the Crime Scene Unit laser room and used to capture and acquire images of latent fingerprints and other latent evidence into the MoreHits database. A Nikon D1x digital camera will be mounted on a copy stand and tethered directly to a computer. Each time the shutter is fired the captured image appears on the monitor. This technique allows the Crime Scene personnel to adjust lighting, filters, or perform other chemical processes in order to capture the best possible image of the evidence.
Also attached to the computer will be a flatbed scanner allowing Crime Scene personnel to acquire documents and other two dimensional objects into the image database. This workstation will be configured so that each Crime Scene investigator will have their own password to start Windows 2000, and a second password to gain access into the MoreHits Forensic Image Tracking software. After the Crime Scene investigators have finished capturing images, they will acquire them into the MoreHits Database from the same workstation. The acquired image will be automatically sent to the Main Digital Processing Lab server via an Ethernet connection between the two computers. Once the Crime Scene personnel have finished acquiring their images they will log off the workstation.

The **Digital Processing Lab** is where all of the images that have been captured are stored in the MoreHits Forensic Image Tracking System server. The Forensic Analyst or other designated imaging personnel will analyze all of the captured images and determine which images are in need of enhancement and which images just need to be archived. All image processing, including image enhancement will be performed and documented by the Forensic Analyst or designated imaging personnel only. The image enhancement history and all other data associated with each image are stored in the database. After all of the images in a case have gone through the enhancement process a 1to1 (life-size) print is produced of each enhanced image and a copy is forwarded back to the Crime Scene personnel that are working the case. As cases are completed or as workload dictates all images (original and enhanced) and the data associated with those images are archived onto a CD. Each CD is assigned a volume number and is filed in locked safe in the Digital Lab. The Forensic Analyst and the Crime Scene supervisor are the only personnel assigned keys to the safe. The Digital Lab is also connected to the Fuji print station via Ethernet. This connection is password protected and can only be activated from the Digital Lab, and by the Forensic Analyst.

Field Kit Equipment

The equipment utilized for the capture of digital images by Crime Scene personnel in the field may include, but not be limited to the following items:

(1)	Fiji S1 camera body
(1)	60mm macro lens
(1)	24-50mm zoom lens
(3)	128mb “Flash Cards”
(2)	1 GB. Micro drives
(8)	AA batteries
(1)	S1 AC power adapter
(1)	Remote release cord
(1)	Monitor patch cable
(1)	62mm Orange filter
(1)	Nikon SB28DX flash unit
(1)	Flash extension cable
(1)	Monitor Kit
(1)	Laptop Kit
(1)	Portable Video Light

Fuji SI Camera Setup at Crime Scenes

- Choose and attach the appropriate lens to the S1 camera body. (The 60mm macro is the lens of choice for fingerprint images)
- Set the exposure MODE to Aperture Priority.
- Set the FOCUS control switch to M for manual focus.
- Set the APERTURE to the smallest setting on the lens.
- Set the FRAME ADVANCE control switch to S for single frame advances.
- Set the IMAGE QUALITY (or compression setting) to RGB/TIFF. Each image will be approximately a 17mb,

uncompressed, TIFF file.

- Set the WHITE BALANCE to A for auto white balancing.
- Set the ISO sensitivity to 200
  (higher settings introduce noise into the image, and should be avoided).
- Insert a blank FLASH CARD or a blank MICRO DRIVE media into the camera *(THE CAMERA MUST BE TURNED OFF.)*
- Secure the camera to the TRIPOD.
- Attach the REMOTE RELEASE to the S1 camera body.
- Secure the MONITOR to the tripod and attach the monitor battery.
- Attach one end of the MONITOR CABLE to the S1 camera body, and the other end to the monitor's Video-In jack.

Image Capture at Crime Scenes

- Position the tripod for close-up photography.
- Frame the image in the camera's viewfinder to include the fingerprint and a portion of the scale. (metric scale recommended) (This may require moving the camera in and out, in order to fill the frame properly)
- Illuminate the fingerprint with the appropriate light source.
- Using the remote release, take a test shot.
- To save this image, press the (FUNC) button. The word (REC) will flash in the rear display panel as the image is recorded onto the Flash card or micro drive media. No other camera functions are operable during this process.
- Using the Exposure compensation control on the S1, increase or decrease the exposure when taking addition shots.
- Notes should be taken after each image is captured, of its location and any other necessary information.
- When the Flash card or Micro drive media is full, turn the camera off and remove the card.

(WARNING: Care should be taken in the storage and handling of the cards. They are small, fragile, and an electronic recording media. And as such they should never be stored in or exposed to extreme heat, near a magnetic field, or subject to a static electrical charge)

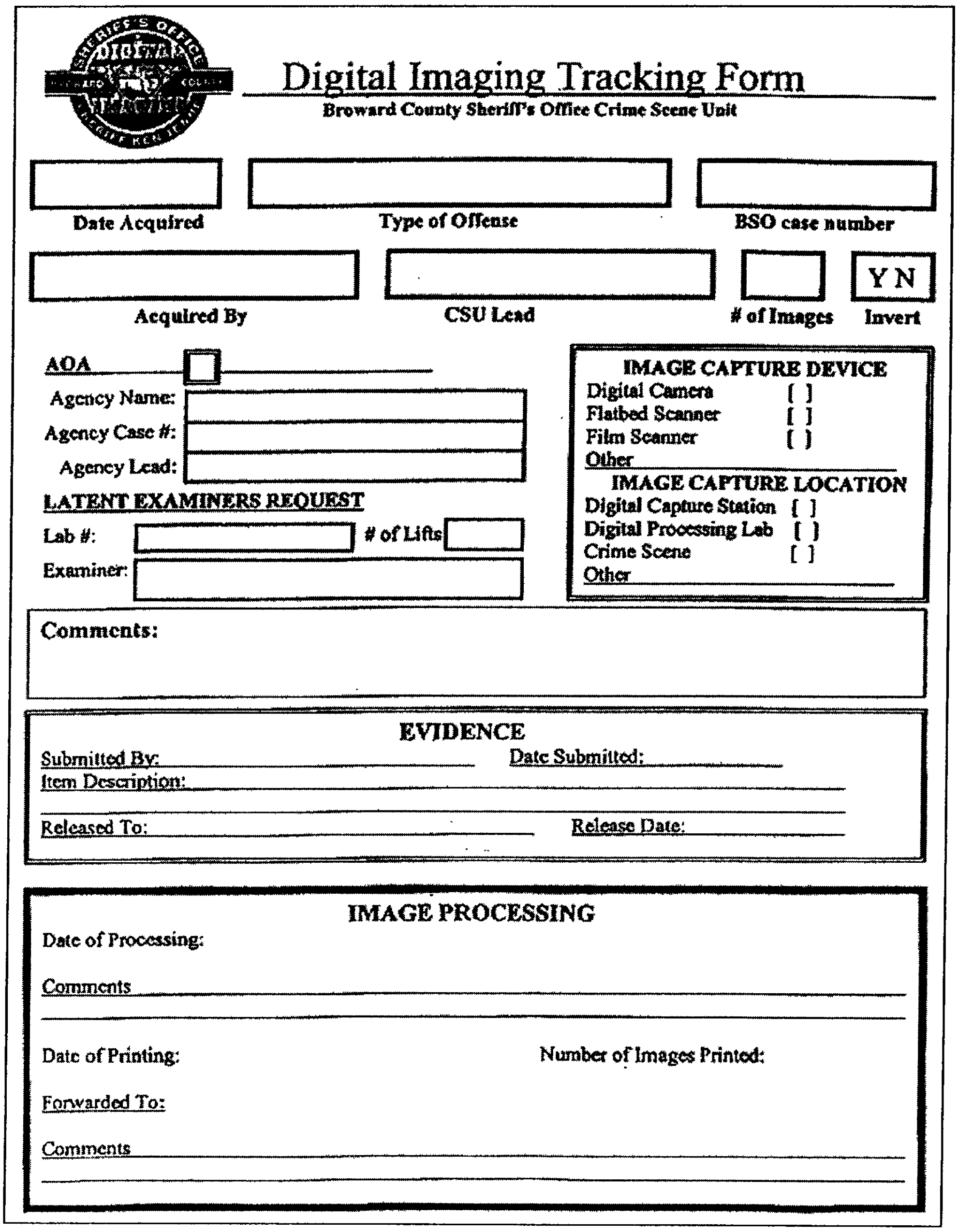
Acquiring Captured Images at Crime Scenes

- Insert the Flash card or Micro drive media into card slot 1 on the MoreHits Forensic Image System Laptop computer, located on the Mobile Crime Scene Response Vehicle.
- Utilizing the "Easy CD Creator" software on the laptop, burn a CD of all images contained on the Flash card or Micro drive media.
- Remove the CD (date & initial) the top of the CD with a permanent ink marker. Mark the CD as "Card Archive"
- Package the CD in a protective sleeve, seal with evidence tape, (date & initial) the tape.
- Maintain custody of CD until it can be forwarded to the Forensic Analyst for permanent storage.
- Activate the Fuji "EXIF" viewer software by *double clicking* the "EXIF" icon. All of the images on the Flash card or Micro drive media will be displayed.
- From the "EXIF" viewer display, select the images to be acquired into the MoreHits Forensic Image Tracking System database.

Acquiring Images into MoreHits at Crime Scenes

- *Log On* to MoreHits.
- *Click* on (IMAGE) *Select* (ACQUIRE) *Click* on (FILE).
- At this point an "Import File" window will appear.
- *Click* on the (MoreHits Images) icon
- *Double Click* the Image number that is to be acquired.
- The image that you have selected will now appear in the "MoreHits Forensic Image Tracking Systems" image-acquiring screen.
- Once the image is loaded into "MoreHits," the (Enter Case Number) dialog appears. The default value is the last entered case number. If this is a new case, type over the number and click (OK.) The case number entry shall follow standard Broward Sheriff's Office protocol (XX*##-##-####*).
- The (Create Case) dialog window will then appear.
- Click (YES) when prompted to create the new case.
- Select (Category Type) and highlight the appropriate selection.
- The (Image Source) will automatically read (Existing File).
- Click on (Calibrate Image).
- Click on (two markings 1cm. Apart)
- In the (Select Distance) enter (1)
- Click on (CM)
- Click on (OK) and (Close).
- Click on (Display Fingerprint Info)
- Select the appropriate variables that apply to that image. Some are chosen by scrolling down a list of choices and clicking on your choice, and others are chosen by clicking and dragging a choice to the appropriate box. After all selections have been made click on (OK).
- In (Image Description) indicate the item of evidence #, the location the print came from, and/or any other note to yourself, as if documenting the back of a print lift.
- In (Case Title) scroll and click on (the appropriate title.)
- Click on (Save)
- After all of the images have been acquired, *Log Off* of MoreHits.
- From the desktop screen *Click* on the (MoreHits Images) icon.
- *Select all* of the images in this file and *delete* them.

- From the desktop screen *Click* on the (EXIF) viewer icon.
- *Select all* of the images in this file and *delete* them.
- Remove the Flash card or Micro drive media from card slot 1.
- Place blank Flash card or Micro drive media in the Digital Field Kit case.
- Fill out the Forensic Digital Imaging Tracking Form and forward it to the Forensic Analyst for further action.



Digital Imaging Tracking Form

Broward County Sheriff's Office Crime Scene Unit

Date Acquired	Type of Offense	BSO case number	
Acquired By	CSU Lead	# of Images	Y N Invert

AOA □

Agency Name:

Agency Case #:

Agency Lead:

LATENT EXAMINERS REQUEST

Lab #: # of Lifts

Examiner:

IMAGE CAPTURE DEVICE

Digital Camera [ ]

Flatbed Scanner [ ]

Film Scanner [ ]

Other

IMAGE CAPTURE LOCATION

Digital Capture Station [ ]

Digital Processing Lab [ ]

Crime Scene [ ]

Other

Comments:

EVIDENCE

Submitted By: Date Submitted:

Item Description:

Released To: Release Date:

IMAGE PROCESSING

Date of Processing:

Comments

Date of Printing: Number of Images Printed:

Forwarded To:

Comments

Importing Cases Acquired at Crime Scenes

Upon receiving the Card Archive CD containing all of the original captured images from a crime scene, and the Forensic Image Tracking Form, The Forensic Analyst will be responsible for performing the following task:

- On the MoreHits Forensic Image System Laptop computer, Start and log onto MoreHits
- *Click* on the *Image* Tab.
- *Select* from the drop down menu (*Export MoreHits Case*).
- *Select* from the (Export case window) the case number to be exported, and *click the arrow* to move the case number into the *To be copied* window.
- *Click OK.*
- Close the MoreHits program.
- Start the Easy CD Creator software by *double clicking* it's icon on the desktop.
- Burn a CD of the (*C:\Morehits\export)* folder.
- Delete the contents of the (*C:\Morehits\export)* folder.
- Shut down the laptop.
- Place the CD containing the exported case into the CD reader of the Digital Imaging Lab computer.
- Start and log onto MoreHits.
- *Click* on the *Image* Tab.
- *Select* from the drop down menu (*Import MoreHits Case*).
- From the *Import File* menu locate the CD containing the exported case.
- *Highlight* the case number and *click* Open.
- Verify that all images and case information has been acquired into the data base.
- Verify the Authenticity of each image.
- Close the MoreHits Program.
- Remove the CD containing the exported case and place it into a protective sleeve.
- Package the CD in a protective sleeve, seal with evidence tape, (date& initial) across the tape.

DIGITAL CAPTURE STATION

Evidence Handling

- The collection, packaging, and custody procedures for the handling of evidence collected at a crime scene are documented in the.

BROWARD COUNTY SHERIFF'S OFFICE, CRIME SCENE UNIT, STANDARD OPERATIONAL PROCEEDURES manual.

- When handling evidence all Biohazard procedures will be followed.

Capture Station Equipment

The equipment utilized for the capture of digital images in the capture station by Crime Scene personnel may include, but not be limited to the following items:

- Nikon D1x digital camera
- Nikon Lenses
  24-50 mm zoom
  28-85 mm macro zoom
  35-105 mm zoom
  60 mm micro
  50 mm
- PCMCIA Type II compact flash storage card
- Firewire cable connection to computer
- Evolution 5000 PC computer
- Ethernet connection to Digital Lab
- 17" color monitor
- Copy stand w/adjustable lights
- Alternate light sources

- Laser
- Flatbed Scanner

Nikon D1x Digital Camera and Computer Setup

- Mount the appropriate lens on the camera body, keeping in mind that the focal length is approximately 1.5 times as long as the marked focal length of the lens selected. (Example 35mm = 52.2mm approximately a "normal" lens for a 35mm format). It should be noted that the f-stop is not affected in the same way.

- The lenses that are in use by the Broward Sheriff's Office Crime Scene Unit are listed as follows:
  - Nikon 24-50mm zoom = approximately 36-75mm
  - Nikon 28-85mm macro zoom = approximately 42-127.5mm
  - Nikon 35-105mm zoom = approximately 52.2-157.5mm
  - Nikon 60mm Micro = approximately 90mm
  - Nikon 50mm = approximately 75mm

- The Nikon D1x digital camera is mounted onto a copy stand.
- An AC power cord is attached to the back of the camera.
- A tethered connection between the Nikon D1x digital camera and the workstation computer is made with a (Firewire interface cable) which transmits data between the two units. As images are captured with the digital camera they can be visualized on the computers monitor.

Image Capture

Basic Camera Settings

- The exposure "Mode" should be set on "Aperture Priority"
- The lens should be set on "f-11" or a small aperture if needed
- The "Exposure Compensation" setting should be on "O"
- Position the evidence and a scale in the field of view. (metric measurement preferred)
- Move the camera up or down to fill the field of view with the fingerprint and scale, limiting excess background.
- To "Bracket Exposures" it is recommended that the "Exposure Compensation" be set in the (+) direction to (LIGHTEN) the image, and in the (-) direction to (DARKEN) the image.

Note: By using the "Exposure Compensation" settings to bracket the exposure, the aperture can remain small resulting in a greater depth of field.

- Click on the "MoreHits" Icon
- Select (Your name)
- Enter (Your Password)
- Click (OK)
- After MoreHits starts click on (Image)
- Move cursor to (Acquire)
- Select (Twain Setup)
- Select DCS camera
- Click on (Image)
- Move cursor to (Acquire)
- Click (Twain)
- The (Enter Case Number) dialog appears. The default value is the last entered case number. If this is a new case, type over the number and click (OK.) The case number entry shall follow standard Broward Sheriff's Office protocol

(XX##-##-####).

- The (Create Case) dialog window will then appear.
- Click (YES) when prompted to create the new case.
- This will activate the "Kodak Driver Interface". The screen will now have a (Contact Sheet) displayed of all the images that are on the "Compact Flashcard" in the DCS420 digital camera.
- To take a picture move the cursor overtop of the (Camera Icon) and click
- The image will appear as the next in-line "Contact"
- To see an enlarged version of this image click on the arrow next to word (View), then click on (Preview)
- To return to the contact view click on the word (View), then click on (Contact Sheet)
- The camera settings data is displayed on the right side of the screen for the selected image.

Image Acquisition

Acquiring Individual Images

- Click on the image. The selected image will have red outline.
- Click on (Acquire)
- Click on (Done) This will close the "Kodak Driver Interface" and open the selected image in MoreHits.
- Select (Category Type) and highlight the appropriate selection.
- The (Image Source) will automatically read (Existing File).
- Click on (Calibrate Image).
- Click on (two markings 1cm. apart)
- In the (Select Distance) enter (1)
- Click on (CM)
- Click on (OK) and (Close).
- Click on (Display Fingerprint Info)
- Select the appropriate variables that apply to that image. Some are chosen by scrOlling down a list of choices and clicking on your choice, and others are chosen by clicking and dragging a (choice) to the appropriate box. After all selections have been made click on (OK).

- In (Image Description) indicate the item of evidence #, the location the print came from, and/or any other note to yourself, as if documenting the back of a print lift.
- In (Case Title) scroll and click on the appropriate title.
- Click on (Save)
- Click on (Utilities), then click on (Authenticate)
- To acquire another individual image return to (Image) (Acquire) (Twain) and repeat the above steps.
- When finished log out of MoreHits

Acquiring Multiple Images (Same Case#)

- Hold down the (CTRL) key and click on the images that you want to acquire. The selected images will have red outline around them.
- Click on (Acquire)
- Click on (Done) this will close the "Kodak Driver Interface" and open "MoreHits" displaying the first image in-sequence that you selected.
- Select (Category Type) and highlight the appropriate selection.
- The (Image Source) will automatically read (Existing File).
- Click on (Calibrate Image).
- Click on two markings 1cm. apart
- In the (Select Distance) enter (1)
- Click on (CM)
- Click on (OK) and (Close).
- Click on (Display Fingerprint Info)
- Select the appropriate variables that apply to that image. Some are chosen by scrolling down a list of choices and clicking on your choice, and others are chosen by clicking and dragging a (choice) to the appropriate box. After all selections have been made click on (OK).
- In (Image Description) indicate the item of evidence #, the location the print came from, and/or any other note to yourself, as if documenting the back of a print lift.
- In (Case Title) scroll and click on the appropriate title.
- ·Click on (Save) The next image in sequence will now be

displayed.

- Repeat the above steps starting with (Category Type).
- After all of the selected images have been acquired, Click on (Utilities), then click on (Authenticate)
- Log out of MoreHits

Log Information

A Log will be maintained in the Digital Lab by the Forensic Analyst detailing case status throughout the imaging process. The Forensic Analyst will add additional information to the log entries, as individual cases have been enhanced, printed, and archived. This log information will act as a reference for the Forensic Analyst and the Crime Scene investigators to track the progress of cases that have been entered into the MoreHits Database.

Below is a list of the information that will be entered into the Log Book:

Info Entered By Crime Scene Personnel:

- **Date images were acquired**
- **Type of Crime**
- **BSO case number**
- **Name of Investigator acquiring images**
- **BSO CSU lead investigator**
- **Lab number**
- **AOA case number**
- **Agency Name**
- **Agency case number**
- **Agency lead investigator**
- **Processing information**
- **Capture location**

- **Capture method**
- **Comments**

Info entered by Forensic Analyst:

- **Date of enhancement**
- **Enhanced check-off box**
- **Printed check-off box**
- **Date of printing**
- **Number of prints**
- **Distribution (who were the prints forwarded to)**
- **Comments**
- **Archive date (when was the case archive to CD)**
- **Volume # (the number assigned to the CD containing the case)**

IMAGE PROCESSING DIGITAL LAB
(Forensic Analyst/Systems Manager)

General Guidelines

It shall be the goal of the Broward Sheriff's Office, Crime Scene Unit, Forensic Imaging Section to provide latent fingerprint evidence imaging at the highest quality possible, while maintaining the highest level of image integrity, utilizing industry standard computerized photographic equipment and techniques. When applied to latent fingerprint evidence of poor visibility, these techniques can offer enhancements to improve the visual quality of an image with, greater accuracy, repeatability and less time expended

All images that are captured digitally either in the field or in the workstation will be stored in the Digital Lab computer. This is accomplished by having the **Capture Station** computer and the **Digital Lab** computer networked together. Crime Scene Personnel can capture images at the **Capture Station** using the digital camera or the card reader. At the same **Capture Station** Crime Scene Personnel can acquire the images into the MoreHits database, which is located in the **Digital Lab** via the network. Once the images have been acquired into the MoreHits database it will be the responsibility of the Forensic Analyst to digitally process those images. Each step of the process must be carefully documented. All enhancements are performed on exact copies of the original images. At no time during the enhancement process will any area of an image be (Deleted or Altered) in any way. All enhancement processes are accomplished by adjusting the (Values) of each pixel (picture element) that make up the total image. As each adjustment is made to an image, the difference between the adjustment and the original image is recorded as a numeric value. If all of the recorded numeric values were applied to another identical copy of the original image the enhancement can be duplicated. The process of recording the enhancements will allow the Forensic Analyst to duplicate the enhanced version of any image that has gone threw the Broward Sheriff's Office, Crime Scene Unit, Forensic Imaging Section.

Image Enhancement

- No original images will be enhanced, a copy of the original will be made and enhancements shall be performed on that copy. The "Original" will serve as a "Control" for any subsequent processed image(s).
- The copy is generated automatically when the enhancement tab is selected in MoreHits.
- The copy is opened in Adobe Photoshop software, by MoreHits automatically when the enhancement tab is selected.
- Along with a copy of the original image, the MoreHits **(Image Enhancement History)** dialog box is displayed.
- The Forensic Analyst will apply whatever enhancement he feels will show the most detail in the image.
- After applying the enhancement to the image, the (Values) are recorded into the **(Image Enhancement History)** dialog box.
- Some images may only need to be converted from a color (RGB) format into a (Grayscale) format. This single step is also recorded in the **(Image Enhancement History)** dialog box.
- When all of the enhancements have been completed and documented, the enhanced image and the enhancement history for that image are returned to the MoreHits database.
- After each image associated with a single case goes through the enhancement and documentation process, the case can be archived.
- The case is then archived for permanent storage. All of the images (originals and enhanced), case information, and the enhancement history are permanently burned onto a CD.
- During the archive procedure the images that are selected to be archived are removed from the computers hard drive.
- A marker indicating that the images and data associated

with that case number have been archived to CD volume # (----), is displayed instead of the images.

- Archived CD's may contain several cases depending on how many images are acquired for each case.
- Archived CD's are stored in a locked safe located in the **Digital Lab**. Access to the CD's are limited to the Forensic Analyst and the Crime Scene Unit Supervisor.

Image Distribution

The Digital Lab is equipped with the ability to produce various types of output media. Below is a list of the output media currently available from the **Digital Lab**:

- Dye Sublimation (Color prints)
- Dye Sublimation (B&W prints)
- Fuji Digital Printer (Color and B&W)
- HP950C Inkjet (Color prints)
- Laser (Black & White Proof prints)
- CDR compact disc
- 3 ½" floppy diskette

Fingerprint Images

- All fingerprint images that are to be forwarded to the Latent Unit, will be printed (1to1) scale.
- All fingerprint images that are to be forwarded to the Latent Unit, will be printed using the Dye Sublimation Printer.

- All fingerprint images that are to be forwarded to the Latent Unit, will be returned to the Crime Scene Personnel working the case.

All other Images

- Printer selection will be determined by the Forensic Analyst depending on the quality requirements of the printed images.
- Proof quality prints will be produced by using the laser printer, the inkjet printer, or the Fuji digital printer.
- Photo quality prints will be produced using the Dye Sub or the Fuji digital printer.
- If a CD or floppy disc is requested, the Forensic Analyst will record the serial number of that disc.
- All case images recorded on CD media for the purpose of viewing will include a copy of the MoreHits Forensic Image Viewer. (The Viewer allows agencies that don't have MoreHits to view MoreHits images and case information)
- The Crime Scene Supervisor must approve all email transmissions of images.

Image Quality Control

- The Forensic Analyst will monitor the quality of the images that are captured and acquired to ensure that Crime Scene Personnel are using the imaging system to its fullest potential.
- The Forensic Analyst will report any problems directly to the individual that may need assistance.
- The Forensic Analyst will provide individual training to Crime Scene Personnel on any new techniques and/or procedures.

Image Archiving

One of the most important functions of the MoreHits Forensic Image Tracking System is archiving. During the archive process, image data is written to a CD. The Archiving procedure transfers original and enhanced images (from the **before** and **enhanced** folders) to the temporary archive folder. Once the archive function is complete, images are transferred to CD using "Easy CD Creator" software and a CD writer.

The Forensic Analyst will perform the archiving procedure as caseload and/or hard drive storage space dictates. CD burns for the purpose of archiving will always be performed as a "single session burn". This is done to eliminate the possibility of data corruption that may occur if CD's are written to in "multi session burns". After a burn session the CD is labeled using a permanent marker with a volume number. The Forensic Analyst will maintain an archive CD log. A consistent Backup program (using tape storage media that are rotated and replaced on a regular basis) will be conducted to prevent the loss of any data that has not been archived to CD.

IMAGE PROCESSING for OTHER AGENCIES

(For Forensic Analyst/Systems Manager)

Evidence Handling

- The collection, packaging, and custody procedures for the handling of evidence are documented in the BROWARD COUNTY SHERIFF'S OFFICE, CRIME SCENE UNIT, STANDARD OPERATIONAL PROCEEDURES manual.
- All evidence received for processing in the Digital Lab will have the following forms completed:
    1. Property Receipt Form BSO RP#54
    2. Submission Of Evidence Form BSO CL#15
- The Forensic Analyst will fill out a Digital Imaging Worksheet.
- When handling evidence in the Digital Lab the Forensic Analyst will ware the provided protective gloves.
- Whenever evidence may pose a biohazard because of the presence of blood or body fluids the protective gloves must be removed prior to entering case information using the computer keyboard.
- Whenever evidence may pose a biohazard because of the presence of blood or body fluids, it will not come in physical contact with any of the Digital Lab equipment.
- When applicable the agencies representative should remain in the Digital Lab maintaining custody of the evidence.

Image Capture Devices

Flatbed Scanner

- When acquiring large images of a reflective nature, the flatbed scanner should be used to capture the image.
- Generally images that are scanned on a flatbed scanner are at true-life size or a 1:1 ratio due to the fact that the flatbed scanner utilizes a linear array to capture the data, rather than an area array.
- The Agfa Duoscan T1200 flatbed scanner interface has predefined scanning resolutions, which include a setting at 1200 pixels per inch (PPI) but not 1000 (PPI). Images scanned on this device should therefore be captured at the 1200 (PPI) resolution.
- When placing a reflective original to be scanned, open the top cover of the scanner revealing the reflective glass surface. Place the original face down on the reflective glass plate with the top side against the middle of the front ruler. Then close the cover before scanning.
- When placing a transparent original for scanning, pull out the Universal Transparency Plate from the front of the scanner. Place the original, emulsion side down, into an appropriate sized slide holder and center the holder on the universal transparency plate so that its topside is directed towards the calibration slit. (The calibration slit is an approximately 1/2 inch wide window nearest the front of the universal transparency plate)
- Make sure to press the slide holder against the Universal Transparency Plate to guarantee that the original is flat. Then replace the Universal Transparency Plate into the scanner with the "AGFA" logo facing up

Note: Optical performance of a (CCD) scanner is always best near the middle of the scan area. However, the specified scan quality is guaranteed for the entire scan area.

Agfa Duoscan T1200 Twain Driver Selection

- Start the (More Hits) program from the desktop icon and wait until the (More Hits) Forensic Image Tracking System program window opens.
- Click on (Image) inside the (More Hits) Forensic Image Tracking System menu bar, Select (Acquire,) (Twain Select) if this is the first use of the scanner for the work session.
- The (Twain Select Source) dialog box will open with the Twain Drivers that are available for use. Select the Fotolook 32 Twain Driver from the list, and click (Set-Up.)

Twain Select and Scanning

- Click on (Image) inside the (More Hits) Forensic Image Tracking System menu bar, Select –(Acquire)-(Twain) and the (Agfa'Fotolook Preview) interface will open.
- Set the input (Pull-down) menus in the interface to the appropriate Original: (Reflective) Mode: (Color RGB), Input: 1200 PPI, Scale to: 100%, Range: Automatic
- Load the reflective or transparent original per the aforementioned procedures
- Click (Preview) to scan a low-resolution image to judge orientation and position. Cropping extraneous image data can be performed at this time. The less extraneous data, the smaller the file size and the more efficient it is to work with.
- If the image is in the proper orientation / position, click (Scan) to capture the image.

- Close the Fotolook interface, the image will appear in the (More Hits) Forensic Image Tracking System (New) image window.

"New" Image Data Entry

a. On the "New Tab," enter the following required information. Your entries are used for several different reports, including the 1:1 lift card.

  - Image category and source
  - Fingerprint information
  - Image description
  - Outside agency information (if appropriate)
  - Crime category

b. Once the image descriptors have been completed, images of fingerprints, and palm prints must be calibrated for size. On the "New Tab, click the "Calibrate Image" button to display the "Image Sizing Dialog."

c. Once the dialog box opens, click the mouse in the image to define the first calibration point (pick a point on the scale in the image) Note that the image can be calibrated in either inches or centimeters.

d. After marking the first point, finish the operation by clicking on an end point along the ruler. Once the end point is defined, the "Enter Actual Distance Dialog" box appears. Type the actual distance (for Example .75 for 3/4") and click "OK."

e. At this point you may rotate the image for proper orientation, however, the rotations are limited to 90° and 180° movements

f. Prior to saving the image, double-check all your information on the "New Tab" for accuracy. Information can be changed at this point but not after saving the image.

g. Click "Save" to save the scanned image and complete the image acquisition process.

Polaroid SprintScan 35 Plus Film Scanner

When acquiring an image from standard 35 mm film stock into the "More Hits" System, the Polaroid SprintScan 35 Plus film scanner may be utilized. The Polaroid SprintScan 35 Plus film scanner is designed primarily for 35 mm slide scanning, however, the unit has the option to scan from a negative strip of no more then six, 35 mm frames that are held in a specially designed carrier. When loading the slide or the negative carrier, the emulsion side of the film stock should be placed facing the back of the unit, away from the operator, and up side down

Twain Driver Selection

a. Start the "More Hits" program from the desktop icon and wait until the "More Hits" Forensic Image Tracking System program window opens.

b. Click on (Image) inside the "More Hits" Forensic Image Tracking System menu bar, Select (Acquire,) (Twain Select) if this is the first use of the scanner for the work session.

c. The (Twain Select Source) dialog box will open with the Twain Drivers that are available for use. Select the (SprintScan 35 32bit) Twain Driver from the list and click (Set-Up.)

Twain Select and Scanning

a. Click on (Image) inside the "More Hits" Forensic Image Tracking System menu bar, Select –(Acquire) –(Twain) and the Polaroid SprintScan 35 Plus Control panel and Preview window will open.

b. Set the input (Pull-down) menus in the control panel to the appropriate Film: (Slide / Negative), Image Type: (Color / B&W), Media: (Landscape (Horizontal)/ Portrait (Vertical)).

c. Next set the resolution to a minimum of 1000 pixels per inch (PPI), and Scale: to 100%.

d. Load the slide and or filmstrip carrier to match the set-up parameters.

e. Click (Preview) to scan a low-level resolution image to judge orientation and position.

f. If the image is in the proper orientation for the set-up parameters, click (Scan) to capture the image.

g. Once captured, the Polaroid SprintScan 35 Plus interface will close and the image will appear in the "More Hits" Forensic Image Tracking System (New) image window.

"New" Image Data Entry

a. On the "New Tab," enter the following required information. Your entries are used for several different reports, including the 1:1 lift card.

- Image category and source
- Fingerprint information
- Image description
- Outside agency information (if appropriate)
- Crime category

b. Once the image descriptors have been completed, images of fingerprints, and palm prints must be calibrated for size. On the "New Tab, click the "Calibrate Image" button to display the "Image Sizing Dialog."

c. Once the dialog box opens, click the mouse in the image to define the first calibration point (pick a point on the scale in the image) Note that the image can be calibrated in either inches or centimeters.

d. After marking the first point, finish the operation by clicking on an end point along the ruler. (Metric Preferred) Once the end point is defined, the "Enter Actual Distance Dialog" box appears. Type the actual distance and click "OK."

e. At this point you may rotate the image for proper orientation; however, the rotations are limited to 90° and 180° movements

f. Prior to saving the image, double-check all your information on the "New Tab" for accuracy. Information can be changed at this point but not after saving the image.

g. Click "Save" to save the scanned image and complete the image acquisition process.

Image Enhancement

- No original images will be enhanced, a copy of the original will be made and enhancements shall be performed on that copy. The "Original" will serve as a "Control" for any subsequent processed image(s).
- The copy is generated automatically when the enhancement tab is selected in MoreHits.
- The copy is placed into Adobe Photoshop software, which also starts automatically when the enhancement tab is selected in MoreHits.
- Along with a copy of the original image, the MoreHits (**Image Enhancement History**) dialog box is displayed.
- The Forensic Analyst will apply whatever enhancement he feels will show the most detail in the image.
- After applying the enhancement to the image, the (Values) are recorded into the (**Image Enhancement History**) dialog box.
- Some images may only need to be converted from a color (RGB) format into a (Grayscale) format. This single step is also recorded in the (**Image Enhancement History**)

dialog box.

- When all of the enhancements have been completed and documented, the enhanced image and the enhancement history for that image are returned to the MoreHits database.
- After each image associated with a single case goes through the enhancement and documentation process, the case can be archived.
- The case is then archived for permanent storage. All of the images (originals and enhanced), case information, and the enhancement history are permanently burned onto a CD.
- During the archive procedure the images that are selected to be archived are removed from the computers hard drive.
- A marker indicating that the images and data associated with that case number have been archived to CD volume # (----), is displayed instead of the images.
- Archived CD's may contain several cases depending on how many images are acquired for each case.
- Archived CD's are stored in a locked safe located in the **Digital Lab**. Access to the CD's are limited to the Forensic Analyst and the Crime Scene Unit Supervisor.

Image/Evidence Distribution

The Forensic Analyst and the requesting officer will determine the appropriate media for image distribution depending on the final usage of the images.

At the time of completion the Forensic Analyst will make arrangements via telephone with the requesting agency/individual to pickup the images and to transfer custody of the original evidence.

Image Archiving

All images captured utilizing the film or flatbed scanner will be archived following the archive guidelines outlined in page #22.

SYSTEMS MANAGEMENT DIGITAL LAB
(Forensic Analyst/Systems Manager)

System Maintenance
Service and Repair Records

- Warranty information and operating manuals for all of the hardware and software associated with the Digital Imaging System will be filed in the Digital Lab.
- An equipment repair and maintenance log will be maintained in the Digital Lab.
- Only PC Pros, Inc., personnel or their designee will perform service to the "More Hits" Computer System.

Daily Maintenance

- A systems check will be performed daily of both the Capture Station and the Digital Lab. This will be conducted by the Forensic Analyst in the Digital Lab via the network connection between the two computers.
- Any images remaining on the compact flash card in the Capture Stations digital camera will be deleted.
- A (Logon Logoff) log is automatically recorded by MoreHits and could be accessed by the Systems Administrator, should the need arise to document such events.

Weekly Maintenance

- The Forensic Analyst will perform a weekly Tape Backup of major systems file.
- The tapes used to record the files will be recorded over after a ten-week rotation of tapes.

Monthly Maintenance

- All of the computer equipment will be cleaned and checked.
- Color calibrations to the monitor and printers will be performed to ensure consistent results.

Annual Maintenance

- At least two times per year, unless otherwise needed, the system will undergo a period of remote system diagnostics.
- Only PC Pros, Inc., personnel or their designee will perform system hardware and software installations, or upgrades on the "More Hits" Computer System.

Logs and Records

- A log will be maintained in the Digital Lab.
- The log will available to all Crime Scene Personnel to check the current status of their cases.
- The MoreHits Forensic Image Tracking software automatically tracks the identity of those individuals that (log-on/log-off) to the system. The date and time of each (log-on/log-off) is also recorded.
- Only the Forensic Analyst or other personnel with administrative access to the system can view or print the log.

Statistics

The Forensic Analyst will formulate the monthly/annual statistics based on the following data:

- Number of images Acquired
- Number of images Enhanced
- Number of fingerprint (Hits)
- Number of B.S.O. cases processed
- Number of A.O.A. cases processed

- Number of Digital Projects (non-criminal)
- Number of hours (attending) training
- Number of hours (giving) training
- Number of hours attending court

Training

1. Any employees working with images that are digital or will be digitized, will first participate in training in the following areas - unit procedures, basic digital imaging technology, image capture procedures, and if image processing will be utilized, the "PC Pros" "More Hits" Image Tracking System.
2. Every Crime Scene Unit and Latent Fingerprint Section employee will familiarize themselves with the Standard Operating Procedures (SOP) / Training Manual concerning the handling of digital images to be used as latent fingerprint evidence.
3. The level and type of training required by individual employees utilizing forensic imaging techniques shall be determined by the Broward Sheriff's Office Crime Scene Unit Supervisors, based upon the employee's individual level of involvement.
4. Those employees utilizing forensic imaging will familiarize themselves with the internal tracking form utilized by the Broward Sheriff's Office Crime Scene Unit for requesting and tracking image processing (enhancement).

Proficiency Testing

All Crime Scene Personnel utilizing the digital imaging system shall be trained and tested for competency and proficiency in the standard operation of the relevant imaging technology. The Forensic Analyst will provide a formal training program for those personnel utilizing the imaging system. This training will be repeated as necessary when significant changes to hardware and/or software are made, or when instructed by the Crime Scene Supervisor.

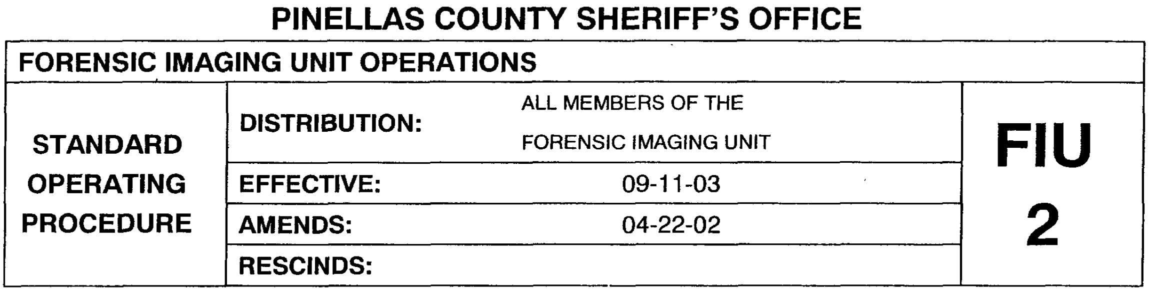
Demonstrations/Presentations

It will be the responsibility of the Forensic Analyst or designee to demonstrate the Digital Imaging System's capabilities to those individuals and or groups that have been approved by the Crime Scene Supervisor.

Court

A copy of all original and enhanced images along with the enhancement history information will be made available as evidence for court. If requested a PowerPoint presentation will be made and presented in court to explain the process of digital image enhancement.

玖、Pinellas County 影像標準作業程序



PINELLAS COUNTY SHERIFF'S OFFICE

FORENSIC IMAGING UNIT OPERATIONS			
STANDARD OPERATING PROCEDURE	DISTRIBUTION:	ALL MEMBERS OF THE FORENSIC IMAGING UNIT	FIU 2
	EFFECTIVE:	09-11-03	
	AMENDS:	04-22-02	
	RESCINDS:		

PURPOSE

The purpose of the Standard Operating Procedure is to establish guidelines for the proper collection, handling, processing, storage, and preservation of images, either film based or digital based, by the Forensic Imaging Unit.

DISCUSSION

It is of the utmost importance that images documenting crime scenes be preserved to maintain their integrity as evidence. With the advent of digital technology, it is even more imperative that all measures be taken to preserve the chain of evidence, and to provide images to investigators and prosecutors in as timely a manner as possible.

DEFINITIONS

A.Forensic Imaging Supervisor – The supervisor of the Forensic Imaging Unit.

B.Forensic Imaging Technologist - Members serving in the Forensic Imaging Unit.

C.Forensic Imaging Unit – A Unit within the Forensic Science Section, which handles all the video and photographic needs of the Section.

PROCEDURES

A. System Security

1.Forensic Imaging Technologists will maintain a Chain of Custody log of film or memory cards received, by entering the case information provided by the submitting member. This information will included the report / case number, the date, and the photographer.

2.Access to all hardware and software utilized by the Forensic Imaging Unit to record, manage, store, and process images will be restricted to the Forensic Imaging Unit Technologists, the Forensic Imaging Unit Supervisor, the Forensic Science Section Manager, and the Division Commander.

3.Passwords will be required on all computers, to gain entry / access, for network connections, and sensitive software applications.

4.All portable storage medium, including, but not limited to, floppy disks, compact disks (CD-ROM), zip disks, Digital Versatile Discs (DVD), or any other such medium, will be secured in locked storage, with access restricted to Forensic Imaging Technologists, the Forensic Imaging Supervisor, the Forensic Science Section Manager or his designee, and the Division Commander.

5.No original negatives or digital images will leave the Imaging Unit without due process of law, and with the expressed authorization of the Forensic Science Section Manager or designee.

6.When Forensic Imaging Technologists are not present in the Forensic Imaging Unit, any and all film or portable digital storage mediums to be submitted to the Forensic Imaging Unit, will be placed in the lock box, located outside the entrance to the Forensic Imaging Unit. Case information will accompany the submission of film or images. Access to the lock box will be limited to the Forensic Imaging Technologists, the Forensic Imaging Supervisor, the Forensic Science Section Manager, or the Division Commander.

B. Digital Image Files

1. Upon receipt of a portable storage medium containing original digital image files from Forensic Science Specialists, Pinellas County Sheriff's Office (PCSO) personnel, or outside law enforcement agencies (i.e. contract

cities), Forensic Imaging Technologists will transfer said images to a secure terminal and, when sufficient in number, they will be recorded on to permanent, non-volatile medium (such as compact disks that are not re-writable), in their original form. This becomes the "electronic negative" that all copies are made from. No alteration or deletion of original images will be allowed.

2. Images will be stored and indexed under the respective report / case number or event title.

3. Images taken as part of a follow-up investigation will be indexed under the report number and given an ascending letter character to show it is an addition to the original case file of images.

4.Enhancements will only be applied to copies of the original image. Enhancements to crime scene images will be limited to those processes which would be applied in traditional film dark rooms.

A.Correct contrast / brightness

B.Correct color balance

C.Enlarge or reduce image size, or a part of it

5. Under NO circumstances will an enhanced image be substituted for the original. All enhanced images will be saved as a separate file. They may be permanently stored on Compact Disk (CD) with the original image, but will be given an individual file name and specified as a copy.

C. Film Files

1. Any and all film taken by a Forensic Science Section Specialist will be maintained and secured by the Forensic Imaging Unit.

2. Any items collected as evidence from a crime scene or citizen that requires processing by the Forensic Imaging Unit will first be turned into the Property and Evidence Division. The requested process will be documented on the Evidence Label. The Property and Evidence Division will notify the Forensic Imaging Unit of the evidence, at which time a Forensic Imaging Technologist will check the item out of Property for processing. Once the item has been processed, the item will be returned to the Property and Evidence Division.

3.Film submitted by PCSO members other than the Forensic Science Section members, or from law enforcement agencies that contract with the Pinellas County Sheriff's Office, will be maintained in the Forensic Imaging Unit.

4.Film submitted by other law enforcement agencies for processing will be returned to the submitting agency upon completion, unless the Forensic Science Manager or designee approves storage within the Forensic Imaging Unit.

5. All film submitted to the Forensic Imaging Unit by Specialists, will be accompanied by a "Film Slip" listing the date, report number(s), report type(s), and photographer's name.

6. All film submitted to the Forensic Imaging Unit by an outside agency, will; be accompanied by a Forensic Imaging Unit Request Form, where all pertinent information requested must be supplied.

7. When a Specialist submits film to the Forensic Imaging Unit, it will become the responsibility of the Forensic Imaging Unit. The film will be developed, printed, or put on the website when required, and then cut and filed.

8. The cut negatives will be maintained in secured cabinets in the Forensic Imaging Unit, or within the secured archive storage area, within the Forensic Science Section, Technical Services

Building, or as designated by the Division Commander.

9.Negatives will be stored by report number and by the year of the report. (i.e., all 2001 report negatives together, all 2002 report negatives together, etc.)

10.Images on film will be scanned with a digital scanner prior to being printed by the Forensic Imaging Unit. Film that is requested to be printed without being digitized, will be sent to an outside photo lab that is approved by the Forensic Science Manger for printing. Enhancement of film will be restricted to the same enhancement 'processes as with digital images.

D. Distribution of Images

1. When requested from the original film or digital images, copies will be loaded to the Imaging Unit web server, so they will be available to investigators, and prosecutors, within twenty-four hours, when possible.

2. As a matter of operation, all submitted cases, which pertain to the following types of criminal investigations will, without request, be copied and placed on the Intra-Net website:

Active Homicide Investigations.

Sexual Battery Investigations.

Child Abuse Investigations.

Cases involving Domestic Violence.

Fire / Arson Investigations.

Traffic Investigations involving the Major Accident Investigation Team.

Narcotics Investigations.

3. Access to the Intra-Net website is limited to Law Enforcement / Government Agencies that can hardware connect to the Sheriff's Office Local Area Network (LAN), which is inside the county security "firewall."

4. All persons who are authorized to view images will have a security file which allows limited access to the website for viewing purposes only.

5 No alteration of the images is allowed by way of this access. Security Levels are assigned based on the individuals or Units need for access, (i.e., a burglary detective will not have authorization to view the active homicide cases of a homicide detective).

6. Requests for prints can be made by completing the form at the bottom of the secure web page, which is then transmitted to the Forensic Imaging Unit, where the requested images will be printed.

7. When a request from the Public Defender's Office or private attorneys for images is received, it must first be verified that an "Answer to Demand for Discovery" from the State Attorney's Office is on file in the CJIS computer terminal system.

8. All requests for images from attorneys, insurance companies, private citizens, or other organizations must be approved by the case agent or State Attorney's Office, and verified by the Forensic Science Manager or his designee.

9. Images will be printed on an as needed basis for trial and ongoing investigations. Emphasis will be placed on secure electronic transfer whenever possible.

10.A fee for photographic prints or digital image files created for private attorneys, citizens, insurance companies, and any others determined on a case by case basis, will be charged to the requester, at a rate established by command, to cover production cost.

11. Persons receiving images, in any form, from the Forensic Imaging Unit, must present proof of identity, unless that person is

known to the Forensic Imaging Unit Technologist releasing the images.

12. Release of photographs and / or images to PCSO members, other than to the assigned case agent for the purpose of ongoing investigation or prosecution, shall be approved by the Forensic Science Manager or designee prior to the release.

13. Release of photographs to members and / or non-members who are the subject of an open investigation, or matters where the Pinellas County Sheriff's Office may be involved in civil litigations (i.e. member involved departmental vehicle crash), must be approved by General Counsel's Office.

E. Equipment Management

1. The Forensic Imaging Unit will be responsible for the photographic equipment assigned to the Forensic Science Section.

2. The Forensic Imaging Unit will maintain a record of all photographic equipment that is assigned to Specialists as authorized by the Forensic Science Manager.

3. All non-assigned photographic equipment will be stored, at the direction of the Forensic Science Manager, within the Technical Services Building.

4.Forensic Imaging Unit Technologists, Forensic Science Shift Supervisors, or their designee, will issue all non-assigned equipment. A log will be maintained as to the Specialists who were issued the equipment. This may include, but is not limited to:

35mm camera kits.

120mm aerial cameras.

Spare digital cameras.

Spare compact flash portable storage mediums.

Video camera kits.

5. Forensic Imaging Technologists will work with the Purchasing Division, to coordinate the timely repair of any photographic equipment, which becomes inoperable or damaged through the course of use. Said repairs to be approved by the Forensic Science Manager.

6. Forensic Imaging Unit Technologists, when directed by the Forensic Science Manager, will assist in the gathering.of information for research and planning of technologies and / or equipment to provide the most efficient and up-to-date operation possible.

7.Forensic Imaging Unit Technologists will perform required maintenance and calibration on all equipment as recommended by the manufacturers and the maintenance will be documented in a logbook. Maintenance will include but is not limited to:

Film Developing Mini-lab

Running control strips at the beginning of each shift.

Performing daily pre-check.

8.Performing monthly maintenance to include cleaning processing racks and cleaning or replacing replenisher filters.

Film Scanner

Clean air filter weekly.

Replace light bulb when necessary.

Printers\Monitors

Calibrate according to manufacturers recommendations.

附件

IN THE CIRCUIT COURT

OF THE 17 th JUDICIAL CIRCUIT
IN AND FOR BROWARD COUNTY,
FLORIDA

CASE NO: 99-11535CF10A
JUDGE: STANTON S. KAPLAN

STATE OF FLORIDA,
Plaintiff,

v

VICTOR REYES,
Defendant.

OPINION AND ORDER
ON DEFENDANT'S MOTION IN LIMINE
RE: LATENT FINGERPRINT ANALYSIS

THIS CAUSE having come on to be heard on Defendant's Motion in Limine Re: Fingerprint Analysis and the response thereto of the State of Florida filed November 27, 2001, and the Court having held a full Frye Hearing.thereon, this Court finds as follows:

The defense has asked this Court to grant a motion in limine prohibiting the admission of fingerprint evidence in this case. The motion is based upon the premise that the digital enhancement of the latent print captured on negative print film in this case constitutes a new and unverified science that does not meet Frye Standards. The Defendant asserts that digital enhancement of the fingerprint process utilized in this case is untested and its reliability has not been established.

The digital enhancement of the fingerprint in this case was accomplished by use of the PC Pros MORE 14ITS program which incorporates and uses the ADOBE PHOTO SHOP software. The Defendant called only one expert witness, Debra Myers, an expert in the use of ADOBE PHOTO SHOP to discredit the use of digital enhancement process.

(1) To demonstrate that the use of digital imaging to enhance a latent print is not new or novel and that it is accepted within the relevant forensic community, the State presented the testimony of three expert witnesses, i.e., Mr. Erik Berg, Mr. David Witzke, and Mr. David Knoerlein.

(2) Mr. Berg, developer of the PC Pros MORE HITS program, testified that while digital enhancement of fingerprints is a relatively new procedure, it has received **widespread acceptance in the forensic scientific community in its application to enhancement of fingerprints.. Digital enhancement of video tapes and photographs** has been in use and used in courts for more than a decade.

More specifically, the International Association for Identification (IAI) passed Resolution 97-9, which states:

... *the International Association for Identification recognizes that electronic digital imaging is a scientifically valid and proven technology for recording, enhancing, and printing images and like conventional silver-halide based photography, it is accepted by professional commercial photographers, law enforcement photographers, and the identification community.*

This has offered legitimacy to the technology and has encouraged its adoption among the members of the [Al. Since that time, digital imaging technology has spread to nearly every major law enforcement agency in the United States.

(3) This Court also heard testimony from Mr. Witzke, a sales executive for PC Pros MORE HITS, who is considered to be an expert in forensic digital imaging, and is internationally renowned for his training programs in forensic image processing. In his testimony, Mr. Witzke described the standard image enhancement processes and procedures that are taught and followed throughout the United States, Canada and England.

Mr. Witzke also testified that he had trained and had cause to review the proficiency of the person who performed the procedures used in this digital enhancement process, Mr. Knoerlein.

Mr. Knoerlein testified that he is a forensic analyst with more than 18 years of experience, and is well trained and proficient in the use of the digital image enhancement system, and that he has more than five years of experience in digital imaging. During that time, he has enhanced more than 10,000 images, most of which are latent prints.

(4) Mr. Knoerlein testified that the procedures used by the Broward County Sheriff's Office in no way changes the basic fingerprint image, but only makes the image clearer. He further testified that he follows the standard operating procedures and guidelines established by the Broward County Sheriffs Office for digital image processing. All enhancements are performed on exact copies of the original image, and that during the enhancement process no areas of an image are deleted or altered in any way. All enhancement processes are accomplished by adjusting the values of each pixel that make up the total image. Each of these processes are recorded for purposes of authenticating the image enhancement process.

Mr. **Knoerlein further testified that these procedures follow the Scientific Working** Group on Imaging Technologies' (SWGIT) recommendations and guidelines for the use of digital image processing in the criminal justice system. The stated purpose of the SWGIT guidelines is to ensure the successful introduction of forensic imagery as evidence in a court of law.

(5) Both Messrs Witzke and Knoerlein demonstrated to the satisfaction of this Court that the enhancement procedure does not change the basic image. This Court concurs with the reasoning stated by the Washington Court of Appeals in State of Washington v Hayden, 950 Pa2d 1024 (Court of Appeals 1998) that digital enhancement methodology does not involve new scientific principals and should not require a Frye Hearing, but nevertheless the methodology does satisfy the Frye requirements. Two Florida appellate decisions dealing with digital enhancement of video tapes support this position that digital imaging enhancement is not new scientific and untested evidence, ie: State of Florida versus Veleka Bryant, a First

District case cited at 810 So.2d 532 (Fla. V DCA 2002); and State of Florida versus Roger Dolan, a Fourth District case cited at 743 So.2d 544, 546 (Fla. 4th DCA 1999). In a recent first degree murder case in this Circuit, the Court allowed similar digital enhancement of fingerprint evidence performed with the same procedure by the same expert ie: David Knoerlein, admitted ie: State of Florida versus Lucious Boyd, Case No. 99-5809CF10A, Circuit Court 17th Judicial Circuit, Broward County, Florida.

(6) Mr. Witzke testified and demonstrated for this Court that the PC Pros MORE HITS image enhancement process is simply an automation process that is intended to improve the visual appearance of a duplicate of an original image. He demonstrated in this Court that neither the scanning nor the image enhancement process alters the physical appearance or the contents of the original image captured from the negative.

Furthermore, the fundamental, principal requirements for admitting a photograph into evidence - whether it is digital or film-based - are relevance and authentication. Mr. Knoerlein testified that the digital photograph was an accurate representation of the image captured on the negative, and Mr. Witzke demonstrated for this Court that the MORE HITS program could successfully authenticate the image.

(7) In State v Bryant, the Appellate Court upheld the trial court's finding that the original time lapse videotapes were authentic based upon testimony by the State's expert about the nature of the original time-lapse videotape and the enhancements made to a duplicate of the original, time-lapse videotapes. The court went on to define a duplicate as:

> *A counterpart produced by the same impression as the original ... by means of photography, including enlargements and miniatures; by mechanical or electronic rerecording, by chemical reproduction; or by equivalent technique that accurately reproduces the original FS 90.951 (3) ...*

In *United States v. Beeler, 62 F Supp. 2d 136, 148 (D. Me.* **1999), the Court found that "Rerecordings** that are enhanced so that the images are clearer to depict [sic] are also 'duplicates' so long as the tapes accurately reproduce the original images on the tape."

(8) The enhancement of the latent image in this case was not extensive and this Court is satisfied that at least two experienced latent fingerprint comparison experts, Messrs Robert Holbrook and James DelValle, have stated in their opinions that a positive identification was made of both the enhanced digital fingerprint image as well as the original digital image with that of the Defendant's rolled print. Their opinions were contradicted in part by the testimony of two other latent fingerprint examiners, namely Ms. **Rena Barry and Ms.** Eva **Souder, neither of whom claimed** that it was a wrong identification, but only that they could not make the identification themselves.

Further, this Court recognizes that fingerprint comparison is a technical field that is subject to the experience and proficiency of the examiner, and in any event that the testimony of Ms. Barry and Ms. Souder goes only to the weight to be given the testimony of Mr. Holbrook and Mr. DelValle.

Therefore, this Court finds that all four of the above named latent print examiners are qualified to give their opinions.

(9) This Court heard testimony that the process of digital enhancement of fingerprints used in this case, i.e., the "MORE HITS software program" is currently being used by the Federal Bureau of Federal Bureau of Investigation (FBI), US Department of Justice Drug Enforcement Agency (DEA), US Department of Treasury Inspector General for Tax Administration (TIGTA) (Formerly the IRS), US Postal Inspection Services United States Air Force Office of Special Investigations (USAF OSI), United States Army Crime Lab, United States Customs, the United States Secret Service as well as more than 150 different state and municipal law enforcement agencies throughout the United States, and it is also being used in Canada

and England. This Court finds that the process of digital imaging enhancement of fingerprints is widely used and accepted as reliable in the forensic community.

(10) (10) This Court finds that the testimony of Simon H. Cole, PhD., would not be helpful to the jury in this case and would only tend to confuse the jury. Dr. Cole's testimony can be summarized as his opinion based on his unspecified readings and unsubstantiated studies that the current methodology used in making fingerprint comparisons is unreliable, subject to error, and has not been scientifically tested.

This Court takes note that Dr. Cole has no personal experience or training in fingerprint comparison methodology. This Court draws the comparison that his testimony would be similar to expert testimony as to the unreliability of eyewitness testimony which has been disallowed. This Court rules at this time that Dr. Cole's testimony is not admissible without prejudice to renew the proffer at trial..

(11) Notwithstanding the attack on fingerprint evidence in general by the defense, this Court finds that there is no reason to depart from the accepted law in Florida and in all other States and Federal Courts in the United States of allowing into evidence the opinion of duly qualified experts as to the identification of a latent fingerprint with that of a known rolled fingerprint.

(12) This Court finds that Automated Fingerprint Identification Systems (AFIS), which is based on digital imaging technologies, have been used successfully throughout the United States and Canada to digitally record, enhance, store and manage fingerprints for more than 30 years.

(13) This Court finds that there are specific rules and standards that govern the use of digital images for fingerprints, including but not limited to the minimum accepted resolution of digital images. These standards are published as the FBI's guidelines regarding digital image quality standards, and have been accepted within the fingerprint community for more than two decades.

ACCORDINGLY, it is hereby,

ORDERED AND ADJUDGED that the said Defense Motion in Limine is denied.

DONE AND ORDERED in chambers in Broward County, Fort Lauderdale this 21 day
of October 2002.

STANTON S. KAPLAN

STANTON S. KAPLAN
CIRCUIT COURT JUDGE

A TRUE COPY

cc: Thomas F. Kern, A.S.A.
Barbara A. Heyer, Esq.

Sun Sentinel Newspaper Article

Fingerprint technology faces test in court

By Paula McMahon
Staff Writer
Posted December 15 2002

When detectives were investigating the 1996 shooting death of a Pompano Beach man, they found faint handprints on duct tape wrapped around the body. But, at the time, the prints were useless to identify the killer.

That changed last year, when the Broward County Sheriff's Office turned one of the smudges into valuable evidence by using two controversial forensic techniques that prosecutors say reveal hidden clues. Using digital photography and computer software, technicians uncovered a print that was almost invisible to the naked eye. Some experts say the print implicates Victor Reyes, 33, who already had been charged in 1999 with the first-degree murder of Henry Guzman, based on other evidence.

But defense attorneys say the fingerprint technology crosses the line between uncovering evidence and creating it.

Both methods are on the cutting edge of new forensic tools that are just beginning to be tested in the nation's courts. They are so new that only two appellate courts, in Ohio and Washington State, have ruled that one of them -- digitally enhancing fingerprints -- is scientifically reliable enough to meet legal standards.

The other method, "dodge and burn," which is used to lighten or darken images digitally, has not yet been tested in the courts.

At Reyes' first-degree murder trial early next year in Broward Circuit Court, both new technologies will get their first serious challenge in Florida. Reyes' Fort Lauderdale attorney, Barbara Heyer, has launched the most aggressive attack yet, calling it "junk science." The trial judge has ruled it can be used.

"I think it's very suspicious that you have something that is of no value and suddenly you enhance it and it becomes of value," said Heyer. "It is very clear that this type of thing can be manipulated."

The software used to enhance the print is the same that some tabloid newspapers use to create seamless "photographs" of space aliens hanging out with celebrities. Time magazine used a similar program to alter a police mug shot of O.J. Simpson and make his complexion appear darker on its front page in 1994.

Heyer said that shows the software is not a scientific tool, but an unreliable art form that could be used to misrepresent reality or simply create things.

Added to the mix in the Reyes case is that the print on the duct tape has disappeared. It wore off the tape because it was processed and examined so many times.

The partial print from the duct tape, which experts say matched Reyes' palm, went from being useless, to a match for Reyes, to nothing but a digitally captured image.

"It's nonexistent because it's gone now," said Heyer.

Two FBI experts and one Broward examiner say the palm print matches Reyes'. Another Broward examiner says she will not identify it.

BSO forensic analyst David Knoerlein, who enhanced the print, was not allowed by his supervisors to discuss the specifics of the Reyes' case. But Knoerlein says that enhancement and "dodge and burn" are phenomenal forensic tools.

"There is a big difference between altering and enhancing," said Knoerlein, adding that BSO has strict rules about what can be done to an image. Only certain staff members can access the system and it automatically logs the user and length of use.

Starting with a digital image of a barely visible fingerprint on a check, the software creates a copy and then saves the original image and gives it an encryption code that Knoerlein says would detect if he made alterations.

He goes to work on the copy, which is saved in a separate computer folder and assigned its own encryption code when Knoerlein finishes his work. He uses Adobe Photoshop, a computer program for graphic artists and photographers, and another program, More Hits, developed for law enforcement by a forensic analyst in Tacoma, Wash.

Knoerlein says what he does is like adjusting the contrast on a TV set and trying to make the picture clearer.

The new methods have come in most useful in lifting fingerprints from surfaces such as bed sheets, duct tape and plastic garbage bags that, in the past, could not be dusted with powder. Using a digital camera, a crime scene technician can take a digital photograph of the print. Then Knoerlein uses the software to remove repetitive patterns like the weave of a fabric and make the print more visible.

Using "dodge and burn," Knoerlein can take parts of the image and make the ridges and valleys of a fingerprint appear darker in places where they are too light, or lighter in places where they are too dark. As if by magic, print details appear and can be used by a fingerprint expert to compare against a suspect's prints to see if they match.

Some agencies, including the Broward Sheriff's Office, have guidelines on how the software can be used. Knoerlein says he never uses some of the program tools like the eraser, which he calls "a no-no, because that would be considered an alteration, not an enhancement."

The software has some safeguards to identify if someone tampers with images. But Knoerlein and Erik Berg, who developed the More Hits program, acknowledge that just having procedures on the books is not enough to guarantee the system is not abused.

Like many aspects of law enforcement, it comes down to the integrity of the individuals involved, said Knoerlein. He only enhances the prints that are then sent on to a print examiner, who is qualified to decide if the print matches the suspect.

One of the biggest questions about the new technology is: Could a skillful technician create or copy a suspect's fingerprint and frame someone by making it look like that fingerprint was at a crime scene?

"I don't think I could recreate a fingerprint," said Knoerlein, pointing out that he never sees the suspect's fingerprints. The system might be more vulnerable where print examiners have both sets of prints and also are responsible for enhancing the prints, he said.

"Could it be done? Probably," said Knoerlein. "But it would take a lot of skill and a lot of time."

Berg says a person could be framed if someone in law enforcement took a legitimate fingerprint and claimed to have found it somewhere linked to a suspect.

But it was also possible to do that in the "old-fashioned" system, when police used powder, tape and Super Glue to capture fingerprints.

Technicians did similar things in the darkroom when they used black-and-white film, said Knoerlein. In fact, the term "dodge and burn" comes from the old days of darkroom developing when photographers would use their hands or a piece of paper to cast shadows on parts of a print and expose other areas of it to more light.

That was done under much less controlled circumstances, said Knoerlein. In the computer program, analysts note the changes they make and that documentation is saved with the evidence.

But Reyes' attorney, Heyer, says that's not good enough.

Because the dodge-and-burn process is so subjective -- like sweeping a paintbrush across a canvas -- no technician can exactly replicate the work of another technician, Heyer said.

"There are no proficiency tests, there are no independent studies to say that this works or that it's reliable," Heyer said.

Dr. Jim Ongley, a Broward assistant public defender and former assistant medical examiner, calls it pseudo-science.

"They call it science, but the hallmark of science is the ability to reproduce the same result. If a scientist in Fort Lauderdale and a scientist in California can get the same outcome from the same raw material, that is science," said Ongley. "This is cosmetic fraud."

Broward Circuit Judge Stanton Kaplan has ruled the evidence can be used in Reyes' trial, so it will be up to a jury to decide whether it can be used to send Reyes to prison for life. If convicted, Reyes will appeal the use of those techniques to Florida's appellate courts.

Prosecutors Deborah Zimet and Tom Kern have other evidence -- the motive appears to be drug-related, the victim's blood was found at Reyes' home and a convicted criminal initially gave a statement that he saw the shooting. That witness, now serving a federal prison sentence, has stopped cooperating with prosecutors. The victim also told his girlfriend during a cell phone call shortly before he died that he was going to Miami with Reyes, an acquaintance, Guzman's girlfriend said.

As forensic experts work to make the system invulnerable to attack, Knoerlein said he hopes that it will soon be standard to have software automatically record everything done to a print. He also wants crime scene technicians to use encrypted cameras that record when an image was captured and whether any alterations were made to it.

In Tacoma, Berg is enthusiastic about the strides made in digital enhancement of prints and how much time it saves law enforcement. It has cut processing time from six hours to 10 minutes, he said.

But in his day-to-day work for the Tacoma Police Department, Berg said he prefers to use the old-fashioned methods unless he's faced with a difficult surface for lifting a print.

"It's like my toolbox got bigger," said Berg. "If I come up with a fingerprint with powder and it's clear -- there's nothing better."

Posted on Sun, Nov. 09, 2003

COURTROOM STRATEGY

Cops gain new fingerprint tool

An appellate court has approved new methods of enhancing hard-to-read fingerprints. Software helps separate the print from a distracting background.

By WANDA J. DeMARZO

wdemarzo@herald.com

When Fort Lauderdale crime scene investigators scoured the apartment of murder victim Michael Sortal, they could harvest only a bloody footprint on the floor and a partial palm print on a blood-soaked comforter.

In the old days, that would have been insufficient to make an ID. Not anymore.

A new computer program called More Hits allows investigators to make prints that in the past would have been unreadable. Using More Hits, Sortal case investigators were able to photograph and duplicate the prints, feed them into a computer, then clean the image -- removing background patterns and extraneous squiggles -- until they could be compared with clear prints of a suspect or suspects.

They had a match. Two suspects were arrested.

Defense attorneys have attacked this process as "junk science," but the court system doesn't think so. In September, the Fourth District Court of Appeal upheld fingerprint "enhancements" used in the Sortal case as valid.

The Sortal case marked only the second time Broward prosecutors have used enhanced digital imaging in court. Having it upheld by the court of appeals was a relief for the Crime Scene Unit of Fort Lauderdale police.

Fort Lauderdale was the first agency in the Southeastern United States to have successfully admitted digitally enhanced images into evidence at a criminal trial.

= [100.0] standards."

The new software allows police to pull a partial or smudged print or even one on patterned material so it can be enhanced and possibly matched to a suspect.

The software is used by Fort Lauderdale police, the Broward Sheriff's Office and Miami-Dade police.

MIAMI RAPE CASE

The enhancement program is not utilized by the Miami Police Department and might have been a useful tool for police investigating the seven rapes and four attempted rapes now attributed to the Shenandoah rapist.

During their investigation of the serial rapist, Miami police later acknowledged having partial prints from a crime scene, but said they could not find enough identifying markers to match them to a suspect.

The suspect was caught not through forensics but when police staking out another suspect spotted him driving a car that matched the description of the rapist's vehicle.

Miami police officials did not respond to four e-mailed requests for comment.

DIGITAL SOFTWARE

Partial prints, enhanced with the digital software, can yield unique characteristics or "points," such as arches, loops and rolls not visible to the naked eye, said David Witzke, vice president of PC Pros, the company that manufactures More Hits.

Every time someone touches something -- a screwdriver, a knife handle, he leaves a print. The visibility of the print depends on the pressure the person used when he touched the object, the type of object -- was it porous, how much was the person perspiring when he touched the item? -- Witzke said.

LIGHT OR DARK PRINTS

"The pressure exerted by the person determines if the print is light, faint or dark enough to be seen by the naked eye," he said. ``One usually finds partial prints at crime scenes because people don't roll their fingertips in black ink before they commit a crime."

And, although a person can't see the print in its entirety, it doesn't mean it's not there, Witzke said.

"With the More Hits program, we're finding more and more prints and matching them to suspects than ever before," Witzke said. ``Just because we can't seen the print doesn't mean it's not there. Miami could have used the program. It could have helped them."

The computer software was developed in 1995 by Erik Berg, a forensic supervisor with the Tacoma police in Washington, who testified at a hearing in the Sortal murder case.

Berg said his system is no different from changing the contrast on a TV set.

"I've changed what you see, but I'm not altering the image. I'm clarifying it," Berg said. ``It's like when you have a closet with three bulbs and there are shadows in the closet you want to get rid of. You remove one of the bulbs."

THREE IN NATION

The Sortal case is one of only three in the country that have resulted in a guilty verdict.

Two other state appellate courts, in Ohio and Washington, have ruled that the digital enhancement of prints is reliable and meets legal standards.

The system was used in a landmark 1996 Washington murder trial that hinged on bloody palm prints on a bedsheet.

The prints were obscured by the fabric's pattern, but Berg's software was able to bring them up more clearly. A suspect was convicted of rape and murder.

The Ohio Supreme Court ruled that digital enhancement of prints found on the bedspread of an Ohio woman raped and murdered in 1997 could be used in court. A suspect was convicted and sentenced to death.

AFTER SLAYING

Fort Lauderdale installed its system in April 2001, a month after the slaying of Michael Sortal, a warehouse manager found dead in his apartment.

He was naked, with a plastic bag over his head and a belt around his neck. Police collected genetic material from his body.

The evidence led them to two Fort Lauderdale suspects, Geoffrey Kennedy, 28, and Kevin Hoffman, 27.

AT LOCAL BAR

Police said the two met Sortal, 47, at a local bar. Detectives think the two Fort Lauderdale roommates preyed on gay men.

Using the enhanced method, investigators working in Sortal's apartment were able to lift prints matching those of Kennedy and Hoffman.

Kennedy, convicted in January 2002, was sentenced to life in prison. His appeal was denied.

Hoffman's trial is expected to start soon.

BSO installed the program three years ago. Investigators used it in an attempt to make a case against Victor Reyes, a suspect in a 1996 Pompano Beach homicide.

FAINT HANDPRINTS

Detectives investigating the shooting death of a Pompano Beach man said they found faint handprints on duct tape wrapped around the body. At the time, the prints were useless.

That changed when BSO enhanced a smudged print that was almost invisible to the naked eye. A technician changed the tone of the print and came up with a design matching that of Reyes.

Reyes' attorney, Barbara Heyer, argued the technique was "junk science," unreliable and easily manipulated.

Reyes was acquitted.

Jurors didn't question the enhancement method, rather they were concerned about when and how the fingerprint came to be on the tape.

BSO says there's nothing fake about the evidence. The print itself is not altered during the enhancing, the agency says.

APPEAL EXPECTED

"We anticipated that if [Reyes] had been found guilty, Heyer would have appealed the case on the fingerprint enhancement," said BSO crime scene Sgt. Jim Kammerer.

So, when the Kennedy case came up on appeal, "this is ultimately what we have been all waiting for," he said. ``Essentially, if it passes the court of appeals, then it's pretty solid evidence."

Posted 2/7/2004 6:09 PM

Digital photography poses thorny issues for justice system

By Brian Bergstein, Associated Press

When Victor Reyes went on trial for murder last year, the technology that fingered him was supposed to be a star witness.

Police in Florida had used software known as More Hits to determine that a smudged handprint they had found on duct tape wrapped around a body — but originally couldn't decipher — implicated Reyes in the 1996 killing.

The judge let prosecutors introduce More Hits' digital enhancement. But the defense called it "junk science," and had an art professor testify that the process resembled how Adobe Photoshop can be used to make trick-photo illustrations.

Reyes was acquitted.

Jurors said they based their decision mainly on the notion that the print didn't prove Reyes was the killer — not on the legitimacy of More Hits' method. And a Florida appeals court later ruled that More Hits' technology — used by 215 U.S. police departments — is acceptable.

Still, some defense attorneys learned a lesson: Get more aggressive about challenging digitally generated evidence.

"Now whenever you hear the word enhancement, an antenna goes up," said Hilliard Moldof, a Florida defense attorney who is questioning digitally enhanced fingerprints in two cases.

Or in the words of Mary DeFusco, head of training for the Philadelphia public defender's office: "I thought digital was better, but apparently it's not. We're definitely going to take a look at it."

As more police departments abandon chemically processed film in favor of digital photography, the technology could be confounding for the justice system.

Film images are subject to darkroom tricks, but because digital pictures are merely bits of data, manipulating them is much easier.

And although willful evidence manipulation is rare, forensic specialists acknowledge that a poorly trained examiner incorrectly using computer enhancement programs can unwittingly introduce errors.

"What you can do in a darkroom is 2% of what Photoshop is capable of doing," said Larry Meyer, former head of photography for State Farm Insurance Co.

Courts have consistently allowed digital photographs and enhancement techniques. But some observers say such methods should endure a more thorough examination, as have technologies such as DNA analysis.

"There have been relatively few challenges to the use of digital technology as evidence and in most of them the courts have looked at them in a fairly superficial way," said Edwin Imwinkelried, an evidence expert at the University of California-Davis law school.

Concerns about the impeachability of digital photographs are one reason many police departments have been hesitant to ditch film for crime scene photographs and forensic analysis.

In fact, some people who train law enforcement agencies in photography estimate that only 25 to 30% of U.S. police departments have gone digital — despite the huge cost benefits of no longer having to buy film and the ease with which digital pictures can be captured and disseminated.

The police department in Santa Clara, Calif., bought 30 digital cameras recently but is holding off on giving them to detectives and technicians until the department specifies ways to lock away the original photos as evidence "so there can be no question that anything was changed," said Sharon Hoehn, an analyst for the department.

George Pearl, who runs a civil-case evidence service in Atlanta and is a past president of the Evidence Photographers International Council, sticks with film partly because he doesn't want to explain on a witness stand if he used a computer to adjust the contrast and other settings of a digital image.

"Even if it was honest adjustments," Pearl said. "Juries, they're all skeptical and they're all sitting there waiting to jump on something that's wrong."

Some law enforcement officials also worry about the limitations that still plague digital photography.

Digital pictures can't be blown up as clearly for courtroom displays as well as film photos. Or the compression needed to store a digital file on disk can make the image blurry or blocky, potentially obscuring key details.

"Digital imaging for the most part has a long way to go to meet the quality of film," said Richard Vorder-Bruegge, an FBI forensic expert who chaired a panel that wrote guidelines for law enforcement use of digital imaging.

For example, he said, a negative shot on traditional 200-speed film can produce the equivalent of 18 megapixels of resolution. Only highly specialized, expensive digital cameras approach that now; most that consumers buy are less than 5 megapixels.

Vorder-Bruegge concedes that a top-notch photographer with plenty of time "could do an outstanding job" with a 1-megapixel camera. But such skills are in short supply in many police departments, especially smaller ones.

Consequently, he believes cops should stay with film for capturing close-up details of footprints and tire tracks.

Many people in law enforcement believe Vorder-Bruegge's assessments are too conservative. They say that with proper training and stringent procedures, digital photos should not be problematic.

For one thing, blurriness or other errors in digital imaging are nowhere near severe enough to "fool an examiner into misidentifying a fingerprint," said George Reis, a crime scene investigator in Newport Beach, Calif., where police began converting to digital a decade ago, saving more than $6,000 a month in Polaroid costs. Reis helps other police agencies make the digital conversion through a business he runs, Imaging Forensics.

In Oregon State Police's forensic laboratory, which has been all digital for about five years, original pictures of fingerprints and other evidence are encrypted so they can't be changed, and burned onto a CD, giving the lab the equivalent of a film negative to reference later.

Any enhancement, such as lightening or darkening elements of the picture — something traditionally done in film darkrooms as well — is performed on a copy of the image, not the original, said Mike Heintzman, the lab director.

Erik Berg, a forensic supervisor in Tacoma, Wash., and the developer of More Hits, said digital photos can allow for even more security than traditional means of stowing film negatives in a drawer.

"I have the ability to lock down one or more digital files to a point where I can ensure not only who can or cannot look at it, but for how long, whether or not they can print it or distribute it," he said. "I can also prove whether or not it has been tampered with since it was created."

Perhaps most importantly, software such as More Hits or Adobe Photoshop now can automatically log changes made to an image, so the alterations can be reproduced by other people. The function was not deployed during the Reyes investigation in Florida.

Barbara Heyer, who defended Reyes, concedes that if used properly, the logging function can improve the acceptability of digital evidence.

"Until there's a history of (what was done and when), not only will I attack it, it should be attacked," Heyer said. Otherwise, "you are relying solely on the word of the person doing the work. That's not something I would like to do when someone's facing life in prison or death."

CNN.com

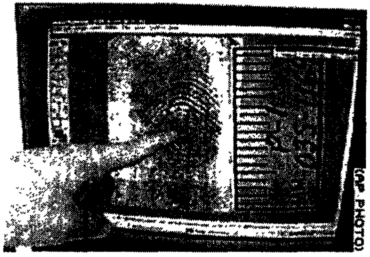
International Edition | Netscape

MAKE CNN.com YOUR HOME PAGE

TECHNOLOGY

Tuesday, February 10, 2004 Posted: 10:39 AM EST (1539 GMT)

(AP) -- When Victor Reyes went on trial for murder last year, the technology that fingered him was supposed to be a star witness.



(AP PHOTO)

Police in Florida had used software known as More Hits to determine that a smudged handprint they had found on duct tape wrapped around a body -- but originally couldn't decipher -- implicated Reyes in the 1996 killing.

The judge let prosecutors introduce More Hits' digital enhancement. But the defense called it "junk science," and had an art professor testify that the process resembled how Adobe Photoshop can be used to make trick-photo illustrations.

Reyes was acquitted.

Jurors said they based their decision mainly on the notion that the print didn't prove Reyes was the killer -- not on the legitimacy of More Hits' method And a Florida appeals court later ruled that More Hits' technology -- used by 215 U.S. police departments -- is acceptable.

Still, some defense attorneys learned a lesson: Get more aggressive about challenging digitally generated evidence

"Now whenever you hear the word enhancement, an antenna goes up," said Hilliard Moldof, a Florida defense attorney who is questioning digitally enhanced fingerprints in two cases.

Or in the words of Mary DeFusco, head of training for the Philadelphia public defender's office: "I thought digital was better, but apparently it's not. We're definitely going to take a look at it "

As more police departments abandon chemically processed film in favor of digital photography, the technology could be confounding for the justice system.

Film images are subject to darkroom tricks, but because digital pictures are merely bits of data, manipulating them is much easier.

And although willful evidence manipulation is rare, forensic specialists acknowledge that a poorly trained examiner incorrectly using computer enhancement programs can unwittingly introduce errors

"What you can do in a darkroom is 2 percent of what Photoshop is capable of doing," said Larry Meyer, former head of photography for State Farm Insurance Co

Courts have consistently allowed digital photographs and enhancement techniques But some observers say such methods should endure a more thorough examination, as have technologies such as DNA analysis

"There have been relatively few challenges to the use of digital technology as evidence and in most of them the courts have looked at them in a fairly superficial way," said Edward Imwinkelried, an evidence expert at the University of California-Davis law school

Concerns about the impeachability of digital photographs are one reason many police departments have been hesitant to ditch film for crime scene photographs and forensic analysis.

AP PHOTO

Oregon State Police latent print examiner Hector Hernandez views a digital image of a fingerprint on a soda can at the forensics lab in Salem, Oregon.

In fact, some people who train law enforcement agencies in photography estimate that only 25 to 30 percent of U.S. police departments have gone digital -- despite the huge cost benefits of no longer having to buy film and the ease with which digital pictures can be captured and disseminated.

The police department in Santa Clara, California, bought 30 digital cameras recently but is holding off on giving them to detectives and technicians until the department specifies ways to lock away the original photos as evidence "so there can be no question that anything was changed," said Sharon Hoehn, an analyst for the department.

George Pearl, who runs a civil-case evidence service in Atlanta and is a past president of the Evidence Photographers International Council, sticks with film partly because he doesn't want to explain on a witness stand if he used a computer to adjust the contrast and other settings of a digital image.

"Even if it was honest adjustments," Pearl said. "Juries, they're all skeptical and they're all sitting there waiting to jump on something that's wrong."

Some law enforcement officials also worry about the limitations that still plague digital photography.

Digital pictures can't be blown up as clearly for courtroom displays as well as film photos. Or the compression needed to store a digital file on disk can make the image blurry or blocky, potentially obscuring key details.

"Digital imaging for the most part has a long way to go to meet the quality of film," said Richard Vorder-Bruegge, an FBI forensic expert who chaired a panel that wrote guidelines for law enforcement use of digital imaging.

For example, he said, a negative shot on traditional 200-speed film can produce the equivalent of 18 mega pixels of resolution. Only highly specialized, expensive digital cameras approach that now; most that consumers buy are less than 5 mega pixels.

Vorder-Bruegge concedes that a top-notch photographer with plenty of time "could do an outstanding job" with a 1-megapixel camera. But such skills are in short supply in many police departments, especially smaller ones.

Consequently, he believes cops should stay with film for capturing close-up details of footprints and tire tracks.

Many people in law enforcement believe Vorder-Bruegge assessments are too conservative. They say that with proper training and stringent procedures, digital photos should not be problematic.

For one thing, blurriness or other errors in digital imaging are nowhere near severe enough to "fool an examiner into misidentifying a fingerprint," said George Reis, a crime scene investigator in Newport Beach, California, where police began converting to digital a decade ago, saving more than $6,000 a month in Polaroid costs. Reis helps other police agencies make the digital conversion through a business he runs, Imaging Forensics.

In Oregon State Police's forensic laboratory, which has been all digital for about five years, original pictures of fingerprints and other evidence are encrypted so they can't be changed, and burned onto a CD, giving the lab the equivalent of a film negative to reference later.

Any enhancement, such as lightening or darkening elements of the picture -- something traditionally done in film darkrooms as well -- is performed on a copy of the image, not the original, said Mike Heintzman, the lab director.

International Association for Identification
1997 Resolutions & Legislative Committee

James Gettemy, Chairperson

RESOLUTION 97-9

WHEREAS the members of the International Association for Identification assembled at their 82nd Annual Training Conference in Danvers, Massachusetts on August 1, 1997, wish to formally recognize that just as color film was a normal progression of the technological evolution of imaging from black and white film, electronic/digital imaging is a normal progression of the technological evolution of imaging from silver-halide based film, therefore be it

RESOLVED, that the International Association for Identification recognizes that electronic/digital imaging is a scientifically valid and proven technology for recording, enhancing, and printing images and like conventional silver halide based photography, it is accepted by professional commercial photographers, law enforcement photographers, and the identification community.

Further, like silver-halide based photography, the quality and reliability of an electronic/digital image is dependant upon the technical specifications of the equipment, the quality control procedures, and the training, experience and ability of the photographer or imaging specialist.
And be it further

RESOLVED, that a copy of this resolution be published in the Association's official publication.

Robert C. Sanders

Robert C. Sanders
Recording Secretary