以3GP/MP4多媒體視訊檔內嵌元資料鑑別視訊檔案來源之研究

鄧思源 / 法務部調查局資通安全處資安鑑識實驗室調查官

摘要

目前常見的手持式行動數位裝置大部分都具有錄製視訊影片的功能，而所拍攝的影片格式大部分為壓縮的3GP及MP4(H.264/AVC)的視訊檔案格式，這些行動數位裝置也可能會記錄著與犯罪案件有關的視訊檔影片資料，當這些視訊影片因案扣押成為重要物證時，數位鑑識人員可否快速鑑別行動數位裝置儲存媒體中所存放的3GP/MP4視訊檔有無經過某些多媒體視訊編輯或轉檔軟體處理及修改，實為多媒體視訊影片內容鑑識作業的一大挑戰。目前市面上有許多3GP/MP4(H.263/H.264)視訊編輯或視訊轉檔軟體可對手持式行動數位裝置所拍攝的MP4或3GP的多媒體視訊影片來直接進行增、刪、連結及格式轉換等後製處理，對於這些經過加工處理之3GP/MP4檔案，目前並無簡單及可供鑑別的數位鑑識方法，本研究嘗試提出在多媒體數位鑑識實務作業

中，應用MP4及3GP視訊影片檔案中所內嵌的特定Atoms元資料欄位內容來鑑別檔案是否為原件及鑑別多媒體視訊影片是否曾使用特定軟體竄改及編修檔案內容。本研究嘗試個化出可用於偽變造視訊影片內容之3GP/MP4視訊編輯軟體的特徵項目或軟體工具痕，並歸納出可列為反電腦鑑識(Anti-Computer Forensics)工具之編輯或轉換軟體。實驗結果顯示某些3GP/MP4視訊影片編輯及轉換軟體可鑑別出不同之特徵項目或軟體工具痕，可作為數位鑑識人員在鑑識手持式行動裝置所拍攝之3GP/MP4多媒體視訊影片是否為原件或檔案內容是否遭偽變之參考。

關鍵字 數位證據、反鑑識、反鑑識偵測技術、數位鑑識、多媒體檔案鑑識。

一、前言

根據國際電信聯盟統計全球手機用戶數量在2013年已突破68億而全球人口目前有71億，另外聯合國報告顯示2014年底全世界的手機用戶數量就會超過全球人口總數，目前台灣的手機普及率已經超過100%，以上種種資訊顯示，目前常見之手持式行動數位裝置，每年都以驚人的數量不斷增長。這些手持式行動數位裝置大部分都具備拍攝視訊影片之功能，且目前全世界各家廠牌所生產之手持式行動數位裝置，約有95%皆預設使用副檔名為MP4(H.264/AVC)或3GP之視訊檔案格式來存放所拍攝之影片內容。由於這些影片的內容很有可能因某些原因紀錄到某些犯罪案件的發生經過與犯罪事實成為相當有力之佐證或直接犯罪證據。當這些視訊影片檔案不論是因證人主動提供或是因案被扣押而成為重要物證時，有無簡易的數位鑑識方法與工具軟體可提供數位鑑識人員來鑑別這些多媒體視訊影片檔為原始未編修之檔案，抑或為已使用某些多媒體視訊編輯或轉檔軟體所處理過之後製視訊影片檔，實為多媒體視訊影片檔案來源鑑別作業的一大挑戰。例如民眾以匿名向司法機關檢舉並提供某件犯罪案件的3GP/MP4(H.263/H.264)多媒體視訊影片檔，要求偵辦追查視訊影片中的犯罪行為人，同時檢舉人在匿名檢舉信中可能提及該多媒體檔案之拍攝時間及係利用某行動數位裝置所拍攝，且宣稱該3GP/MP4多媒體視訊影片檔係在2012年6月12日下午13時02分在新北市某地點，以Nokia N95手機所拍攝。當司法機關收到這些視訊影片檔的檢舉資料，首先要確認的是影片中之犯罪事實為真抑或為假，由於檢舉之影片內容有可能係以視訊編輯、剪接或轉換軟體加工處理及偽變之後製品，而不是原先所檢舉之犯罪內容。影片內容真假之鑑別方法最基本的步驟為先確認影片之來源是否為原始檔案且未經任何軟體加工處理，如果確認該影片為已經視訊軟體處理過，則有必要再對影片內容進行

真偽鑑定作業，例如透過畫格(Frame)之分析，找出可能遭偽變之視訊內容。又如在犯罪嫌疑人的電腦硬碟或其他儲存媒體如拇指碟及記憶卡中發現某些疑似與犯罪事實或可揭露其他犯行有關之多媒體視訊影片，如能透過數位鑑識方法來確認該視訊影片之行動數位裝置來源，則對於案件之後續偵查作業，必有相當之助益，以上所舉的多媒體視訊影片偽變造犯罪手法，我們尚可舉出許多其他以視訊影片編輯工具軟體加工偽造犯罪物證的其他案例，目前我國司法機關對於手持式行動數位裝置所拍攝之3GP/MP4 多媒體視訊檔案的來源鑑別及影片內容是否係原件並無相關研究，本研究嘗試藉由多媒體內嵌之Atom元資料資訊分析，並以簡易的數位鑑識方法來鑑別視訊檔案之來源及判讀是否經特定視訊編輯或轉換軟體處理。

在3GP或MP4(H.264/AVC)的多媒體視訊檔案中的視訊軌資料有內嵌所謂的元資料(亦可稱為詮釋資料或後設資料)，元資料在MP4檔案中通常保存在所謂Moov的原子容器(Atom Container)中，所謂原子(Atom)資料就是3GP/MP4(H.263/H.264)視訊檔案用來定義及組織檔案中所有資料的一種物件格式。基本上所有原子都是個別容器物件(Container)，具有大小及各種類型，另外原子資料也可以包含其他原子的資料，例如所有媒體資料通常會保存在所謂的Mdat原子容器中，而trak原子容器中則定義一些與軌道有關的輔助資訊，透過3GP或MP4檔案中某些特定的元資料內容的分析與解讀，將可用於鑑別視訊檔案的來源。

目前在網際網路上有許多可用於編輯或轉換3GP/MP4(H.263/H.264)多媒體視訊影片檔的免費或是商用工具軟體，這些軟體設計主要目的為提供使用者可直接對以行動數位裝置所拍攝的3GP/MP4多媒體視訊影片檔進行視訊內容的剪接、編輯與轉檔等作業。編輯作業包括可將不同格式的視訊內容加以合併與剪接、加入文字、聲音及特效等等。而轉檔作業則提供將不同之多媒體視訊影片檔或影像檔等不同之檔案格式轉換為可支援它種作業系統環境下可播放之多媒體視訊影片檔案格式，或者可產生在不同廠牌或型號的手持式行動數位裝置上可播放之各類解析度多媒體視訊影片檔格式。這些多媒體視訊影片檔編輯或轉檔工具軟體，大部分只能在微軟視窗作業系統下作業，但也有少數編輯工具軟體可在Linux及MAC作業系統上運作，甚至有跨越以上三種不同作業平台的版本。

以多媒體視訊影片檔內容偽變造鑑識及反電腦鑑識工具偵測與鑑別的角度及觀點來看，這些常見的3GP/MP4(H.263/H.264)視訊編輯與轉檔工具軟體，無疑可提供有心犯罪的不法份子作為規避多媒體視訊影片檔案來源鑑別的一種反鑑識工具。因此本研究將藉由觀察3GP/MP4多媒體視訊影片檔案在經由視訊編輯及轉換工具軟體編修時，檔案內嵌之特定原子欄位資料內容的變化情形，嘗試歸納出多媒體視訊影片檔遭此類工具軟體竄改時所顯現之特徵項目或軟體工具痕。並以特定之原子欄位資料內容作為鑑別多媒體視訊影片檔案來源是否為原件，作為判定多媒體視訊影片檔案做為證據能力可信賴性之參考，及作為多媒體視訊影片檔案鑑定的初步分析結果。

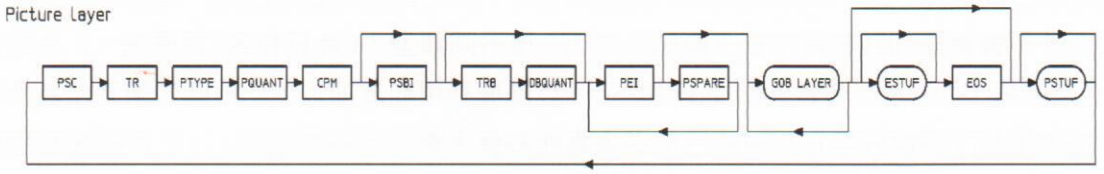
二、相關文獻與背景知識

以行動裝置來拍攝視訊影片相當流行，這些視訊影片大部分以MP4或3GP的多媒體檔案格式存在。如何透過該等視訊影片資料物件內嵌之Moov原子容器元資料內容來確認行動裝置之機型，以及如何判讀該視訊影片是否係裝置所拍攝之原件亦或已遭3GP/MP4(H.263/H.264)視訊編輯及轉換軟體編修過，目前並無相關文獻與研究可供參考。本篇研究嘗試提出以觀察MP4(H.264)及3GP檔案物件內嵌之Moov原子容器中之特定元資料欄位資訊是否為特定數值、Atom內嵌之檔案建立時間及修改時間等元資料是否為固定之時間參數、I-PICTURE在視訊檔中所出現之位置參數是否為特定數值等資訊，作為鑑別該多媒體視訊影片檔案之來源及判斷是否遭視訊軟體編輯及轉檔等後製之依據。並嘗試歸納出可用於從事影片後製之各種3GP/MP4(H.263/H.264)視訊編輯及轉換軟體之特徵項目或軟體工具痕。

2.1 H.263標準

1995 年，ITU-T制定 H.263 標準，適用於64 Kbps以下的低編碼率視訊傳輸。H.263標準主要分為以下5點:(1)採用畫格內(IntraFrame)和畫隔間(InterFrame)兩種編碼方法，(2)運動補償採用半像素精確度，(3)傳輸碼採用變動長度編碼，(4)無限制的運動向量以及基於語法的算術編碼，(5)事先預測方法採用和MPEG中的P-B畫格(Frame)一樣的畫格預測方法。

H.263標準採用分層的方法進行管理，可以分為圖片層(Picture Layer)、群組區塊層(Group of Blocks Layer)、巨區塊層(Macroblock Layer)、區塊層(Block Layer)等層級。每個圖片資料包含一個圖片頭，並緊跟著群組區塊資料，最後是一個序列結束碼和填塞位。圖片層啟始碼(Picture Start Code)是一個22位元的字，它的值是0000 0000 0000 0000 1 00000。所有的圖片啟始碼都應該以字組對齊，並以在啟始碼之前插入PSTUF來完成，因此啟始碼的第一個位元是一個字組中的第一個位元（也是最重要的一個位元）。接下來為時間域參照(TR) (8 Bits)、類型資訊(PTYPE) (13 Bits)[1]，量化器資訊(PQUANT) (5Bits)、連續出現的多點(CPM) (1 bit)、圖片子位元串流指標(PSBI) (2 Bits)、額外插入資訊(PEI) (1 bit)、填塞 (ESTUF) (變長)及序列結束(EOS) (22 Bits)[2]。以軟體觀察H.263相關資訊如圖一所示：



圖一、H.263標準之檔頭資訊(引用自ITU-T H.263(04/2005)文件)

[1]其中PTYPE13Bits之第9位元表示圖片編碼類型，「0」表示INTRA (I-Picture)，「1」表示 INTER (P-Picture)最為重要。

[2]這個碼字由22個位元。它的值為0000 0000 0000 0000 1 11111。由編碼器來決定是否插入這個碼字。EOS可以是字組對齊的。

H.263標準提出了具體的格式與編碼技術，分別為採用CIF格式(Common Intermediate Format)，H.263支持的影像格式主要有SQCIF、QCIF、CIF、4CIF和16CIF，這些影像格式保存的是YUV色彩值，而沒有保存RGB全彩色彩值，影像解析度如圖二所示。

Picture format	Number of pixels for luminance (dx)	Number of lines for luminance (dy)	Number of pixels for chrominance (dx/2)	Number of lines for chrominance (dy/2)
sub-QCIF	128	96	64	48
QCIF	176	144	88	72
CIF	352	288	176	144
4CIF	704	576	352	288
16CIF	1408	1152	704	576

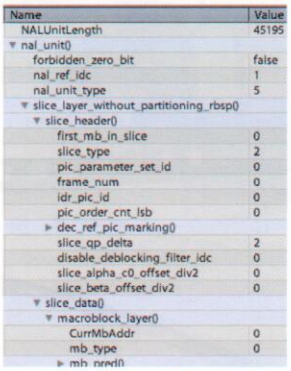
圖二、不同格式支援的解析度像素值(引用自ITU-T H.263(04/2005)文件)

2.2 H.264標準：

H.264標準是由JVT(Joint Video Team)組織提出的新一代數位視訊編碼標準。H.264標準作為MPEG-4標準的一個新的部分(MPEG-4 part.10)，H.264標準的主要特點有：(1)更高的編碼效率，(2)高質量的視訊畫面，(3)提高網路適應能力，(4)採用混合編碼結構，(5)H.264的編碼選項較少，(6)H.264提供錯誤復原功能，(7)有較高的複雜度。H.264 的功能可分為兩層，即視訊編碼層(VCL，Video Coding Layer)和網路抽象層(NAL，NetworkAbstraction Layer)。VCL用於完成對視訊序列的高效率壓縮，VCL資料即編碼處理的輸出，它表示被壓縮編碼後的視訊資料序列。在VCL資料傳輸或存儲之前，這些編碼的VCL資料，先被映射或封裝進NAL單元中，NAL則是對具體的網路傳輸環境把壓縮資料進行傳輸封裝，每個NAL單元(如圖三所示)包括一個原始字組序列負荷(RBSP，Raw ByteSequence Payload)、一組對應於視訊編碼資料的NAL頭信息。一個視訊圖片可編碼成一個或更多個片(Slice)，每片包含整數個巨區塊（Macro Block），即每片至少含有一個MB，最多時則每片包含整個圖片的巨區塊，亦即圖片中每片的巨區塊數量不是固定值。一個巨區塊是由一個16×16 亮度像素和附加的一個8×8Cb和一個8×8 Cr的彩色像素塊所組成。每個圖片中，若干巨區塊被排列成片的形式。設片的目的是為了限制錯誤編碼的擴散和傳輸，使編碼片相互間是獨立的，某片的預測不能以其它片中的巨區塊為參考圖片，這樣某一片中的預測誤差才不會傳播到其它片中去。編碼片共有5 種不同類型，I 片只包含I 巨區塊，P 片可包含P 和I 巨區塊，而B 片可包含B 和I 巨區塊。。I 巨區塊利用從當前片中已解碼的像素作為參考進行畫格內預測（不能取其它片中的已解碼像素作為參考進行畫格內預測）。P 巨區塊利用前面已編碼影像作為參考影像進行畫格內預測，一5個畫格內編碼的巨區塊可進一步作巨區塊的分割為：16×16、16×8、8×16 或8×8 亮度像素塊（以及附帶的彩色像素）。如果選了8×8 的子巨區塊，則可再分成各種子巨區塊的分割，其尺寸為8×8、8×4、4×8 或4×4 亮度像素塊（以及附帶的彩色像素）。B 巨區塊則利用雙向的參考圖片（當前和未來的已編碼圖片畫格）

進行畫格內預測。除了 I 片、P 片、B 片外，還有SP 片和SI 片。其中SP（切換P）是用於不同編碼串流之間的切換，包含P 和/或I 巨區塊，它是擴展設定中必須具有的切換。SI為一種特殊類型的編碼巨區塊， 也是擴展設定中的必備功能。

H.264影片資料串流結構可分為五層：視訊序列層，影像圖片層，片(Slice)層，巨塊(Macro Block)層，區塊(Block)層。H.264標準中指明在每個NAL單元前添加起始碼：0x000001。當檢測到0x000000時也可以表徵當前NAL 的結束。H.264標準另外一種叫做「防止競爭」的編碼機制為在編碼器編碼完一個NAL 時，應該檢測是否出現0x000000、0x000001、0x000002及0x000003等四個字組序列，以防止它們和起始碼競爭。如果檢測到這些序列存在，編碼器將在最後一個字組前插入一個新的字組：0x03。當解碼器在NAL內部檢測到有0x000003 的序列時，將把0x03 拋棄，恢復原始資料。

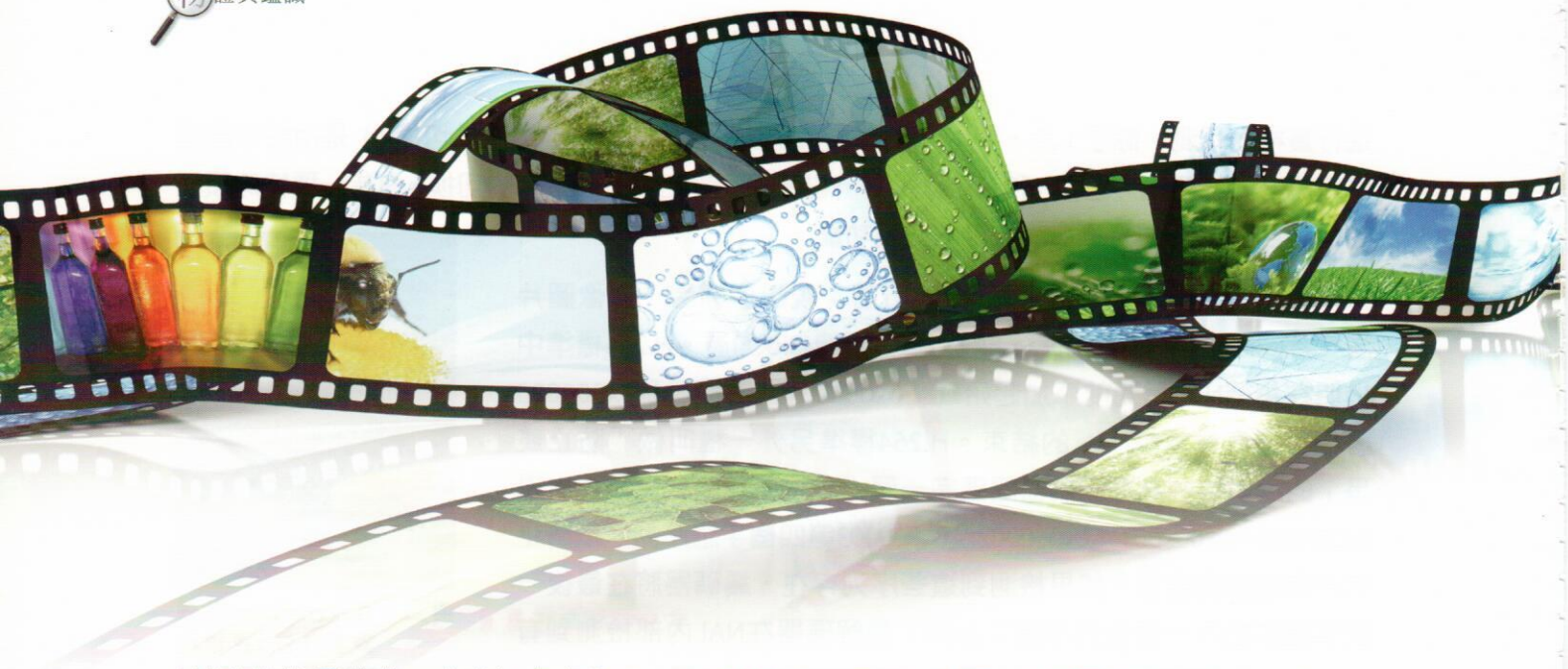


圖三、在SceneScope軟體觀察H.264視訊檔NAL單元資訊

2.3 MPEG-4標準(ISO/IEC 14496)標準

MPEG-4 提供自然和合成的聲音、影片以及基於物件的影像編碼工具。MPEG-4編碼串流主要包括基本編碼串流和系統串流。基本編碼串流包括音視訊和場景描述的編碼串流表示，每個基本編碼串流只包含一種資料類型，並通過各自的解碼器解碼。系統串流則指定根據編碼視聽資訊和相關場景描述資訊產生交互方式的方法，並描述其交互通信系統。MPEG-4標準為新一代的影像壓縮編碼技術，係基於視訊物件(VO，Video Object)進行壓縮編碼。通過VO來達到區域分層，可把視訊串流中的每一個畫格分割成任意的視訊物件平面(VOP，Video Object Plane)，視訊及聲音物件(AVO，Audio/Video Objects)是MPEG-4為支持基於影片內容編碼而提出的重要概念。MPEG-4視訊串流可為分為視訊物件平面(VOP，Video Object Plane)、視訊物件平面層(GOV，Group Of Video ObjectPlanes)、視訊物件層(VOL，Video Object Layer)、視訊物件(VO)及視訊會話(VS，Visual Session) 等5層。其中VOP可視為VO 在某一時刻的表示，即某一畫格(Frame)。GOV提供視訊串流的標記點，標記VOP 單獨解碼的時間區域位置，亦即對視訊串流任意訪問的標記。VOL用於擴展VO 的時間區域和空間區域分辨率，包含VO 的三種屬性信息。VO為場景中的某個物體，有生命週期，由時間上連續的許多畫格構成。一個完整的視訊物件序列(VOS)是由多個VS 組成。每個VS 由一個或多個VO 構成，每個VO 可能有一個或多個VOL 層，如基本層、增強層等，每個層是VO 的某一分辨率表示。每個層中都有時間連續的GOV，每個GOV 又由一系列的VOP 構成。檔頭資訊如表一所示。

類似於MPEG-1及H.263 等壓縮標準的三種畫格格式I、P、B，MPEG-4標準的VOP 也有I-VOP(節點編碼，Intra-Coded-VOP)、P-VOP(預測編碼，Predictive-Coded-VOP)、B-VOP(前後預測編碼，Bidirectionally Predictive-Coded) 等三種相應的畫格格式。在MPEG-4標準中所有視訊串流資



料都是以視覺化位元串流語法來表示，每個視訊串流資料都會有一組特定的啟始碼(Start Codes)位元參數，由一組前置字串及數值所組成，前置字串的二進位值通常以‘0000 0000 0000 0000 0000 0001’來表示，如果以16進位表示則為「00 00 01」。

表一：視覺化字串常見起始碼值(引用自ISO/IEC 14496-2(1998))

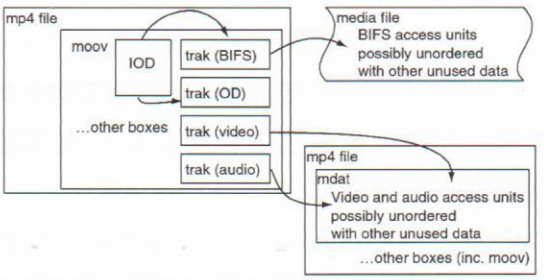
名稱	起始碼值 (16進位表示)
video_object_start_code	00 到 1F
video_object_Layer_start_code	20 到 2F
visual_object_sequence__start_code	B0
visual_object_sequence_end_code	B1
user_Data_start_code	B2
group_of_VOP_start_code	B3
video_session_error_code	B4
visual_object_start_code	B5
VOP_start_code	B6
face_object_start_code	BA
face_object_plane_start_code	BB
mesh_object_start_code	BC
mesh_object_plane_start_code	BD
still_texture_object_start_code	BE
texture_spatial_Layer_start_code	BF
texture_snr_Layer_start_code	C0
System start codes (see note)	C6 到 FF

2.4 MP4 (MPEG-4 Part 14) 檔案格式

MP4是由MPEG-4標準所定義的多媒體容器格式，這種容器格式的完整名稱為「MPEG-4 Part 14」，完整的定義在ISO/IEC 14496-14標準中，通常用於儲存視訊及聲音流媒體資料。而MPEG-4 Part 14 標準的基礎則建立在ISO/IEC14496-12:2004(MPEG-4Part 12: ISO Base Media File Format) 標準之上(如圖四所示)。此標準制定的基礎主要基於Apple公司的QuickTime 多媒體容器格式規格之上，但MP4尚支持所謂的起始物件描述(IOD，Initial Object Descriptors)的特性。基於ISO 基本媒體檔案格式，MP4檔案格式定義某些額外項，用以支持MPEG-4視訊/聲音編解碼及不同的MPEG-4系統特色，例如物件描述以及場景描述等等。

標準中制定的正式副檔名為「.MP4」，副檔名命名可分為以下3種狀況：(1)MPEG-4檔案包含視訊及聲音資料，通常會使用標準的「.MP4」副檔名，(2)原始的MPEG-4視訊位元流資料，通常會以「.M4V」作為副檔名，但有時候也會使用此種副檔名作為MP4檔案容器格式，(3)行動電話通常使用3GP檔案，此種檔案係基於MPEG-4 Part 12標準，類似MP4，它使用「.3GP」及「.3G2」副檔名，這些檔案也會儲存非MPEG-4標準視訊及聲音資料(例如H.263及AMR等等)。

MP4檔案格式最大的特色在於將元資料(Meta Data)與媒體資料(Media Data)區分開來。元資料內容包括視訊/聲音的時間資訊、視訊/聲音資料所佔用的容量以及此段視訊在整個檔案的位置等多媒體資訊的重要參數。媒體資料內容為數張影像/聲音編碼出來的資料流，它可以和元資料存放在同一個檔案，也可以是存放在另一個檔案中。MP4檔案把每個位元流資訊存放在一個單軌裡，一個單軌記載著一連串的影像/聲音的時間資訊以及資料型態，每個單軌會有自己的單軌識別符號，一個單軌內有許多樣本(Samples)，以影像資料為例，一個樣本代表一個VOP。MP4的檔案格式會儲存每個樣本之間的時間差值(Duration)，而相對應單軌出現時間以及內部每個樣本時間間隔的資料結構則存在編輯列表(Edit List)中。



圖四、交換檔格式-ISO/IEC 14496-PART 14(引用自ISO/IEC 14496-14(2003))

2.5 3GP (3GPP TS 26.244) 檔案格式

3GP檔案格式是由第三世代夥伴計畫(The Third Generation Partnership Project，3GPP)組織所定義。該組織是由歐洲的ETSI、日本的ARIB和TTC、韓國的TTA以及美國的T1在1998年底發起成立的。旨在研究制定並推廣基於演進的GSM核心網絡的3G標準，即WCDMA、TD-SCDMA、EDGE等。3GP檔案格式在3GPP TS 26.244(在2011年4月已發行到第10版)中定義，其中規定了3GP多媒體檔案的封裝格式、聲音編碼格式、視訊編碼格式以及串流化的擴展等幾個方面。3GP檔案格式

是MP4檔案格式在手機上的簡化版。MP4檔案的標準編碼組合最普通的設定為MPEG-4視訊加上AAC聲音。而3GP檔案的編碼組合則按版本演進可分為3GPP R5(H.263/MPEG-4 + AMR-NB/AMR WB)及 3GPP R6(增加H.264 視訊和AAC+ 聲音支持)。3G2(又稱3GPP2檔案格式)是由3GGP2組織針對3GCDMA2000多媒體裝置所開發的一種多媒體容器格式。這種檔案格式非常類似3GP檔案格式，但與3GP檔案格式做一比較，仍可發現格式有一些延伸與限制。3GP定義在ETSI的3GPP技術規範中，3G2檔案格式則定義在3GPP2的技術規範中。

3GP及3G2的檔案格式結構都是基於ISO/IEC 14496-12標準所定義的ISO基礎媒體檔案格式。3GP檔案格式中有關視訊串流媒體的儲存，主要是以MPEG-4 Part14或H.263或8MPEG-4 Part 10(亦即AVC/H.264)等視訊標準為主，另外3GPP還可使用AMR及H.263的作為編碼格式。

三、多媒體視訊檔內容偽變鑑識原理

數位鑑識人員在鑑識3GP/MP4多媒體視訊檔案內容是否係原件之鑑識作業前，必須

先瞭解3GP/MP4多媒體視訊檔之Atom元資料概念以及可能有哪些軟體可用於修改Atom元資料的內容，以下分為二部份討論：

3.1 MPEG-4/3GP Atom元資料結構分析

在鑑識MPEG-4/3GP視訊檔案內嵌之Atom(或稱為Box)元資料前，必須先瞭解Atom元資料的相關結構與內容。Atom是MP4/3GP檔案的最基本的元資料單元，所有的視訊及控制資料都是由Atom所包覆與組成。每個Atom都包含大小及型態欄位資訊，Atom的型態通常是以一組四字元的ASCII碼來表示。Atom本質上就是階層式架構，也就是說一個Atom可能為一個容器(Container Atom)，Atom內部還可以存放其他Atom資訊，也可以當作實際儲存資料的欄位(例如Leaf Atom)。

在MP4/3GP檔案中，最上層的Atom分別是Ftyp，Mdat、Moov以及Free等四種，這些

Atom都可個別再包覆其他類型Atom或資料欄位。所有的Meta Data都定義在Moov Atom中，影像/聲音、BIFS或Object Description(OD)的資料放在Mdat Atom內，Free Atom則是為了加入新資料。

檔案型別元資料 (Ftyp Atom)則是用來識別檔案型態，例如MPEG-4檔案及JPEG-2000檔案的區別。比較重要的欄位包括「Major_Brand 」、「Minor_Version 」以及「Compatible_Brands」等三個欄位，其中MPEG-4檔案的「Major_Brand」的值通常表示為「MP42」，3GP檔案的「Major_Brand」的值通常表示為「3GP4」或「Isom」等等。

影片樣本資料 (Mdat Atom)用於區別視訊畫格以及聲音樣本組等媒體樣本資料。影片樣本資料(Moov Atom)大部分皆由一個影片標頭元資料(Mvhd Atom)和一個或多個Trak Atom(單軌資料)所組合而成，影片標頭內容包括此影片資料最初建立的日期/時間、最後被更改的日期/時間、時間比例尺、總長度以及此影片的播放速率。Track Atom用於

定義影片，一部影片有可能是由一個或多個單軌所組成，每個單軌彼此獨立並各自擁有所屬的時間與使用空間資訊，單軌元資料(Track Atom)也有標頭記載其相對應的媒體資料最初被建立以及最後被更新的日期、總長度以及元資料。單軌元資料與數位鑑識有重要關係的其他Atom資料分別為單軌標頭元資料(Tkhd Atom)及媒體元資料(Mdia Atom)，單軌標頭元資料說明影片中單軌所有的特性，重要內容包括版本、旗標狀態、單軌標頭的建立日期時間(通常以UTC時間顯示)、修改日期時間(通常以UTC時間顯示)、單軌識別符號(Track ID)、單軌的總長度、寬度及高度[3]。媒體元資料(Mdia Atom)用於描述及定義一個影片軌的媒體形態(視訊或聲音)、樣本資料(如時間比例及軌道長度)及媒體與軌道的特定資訊(如聲音大小與圖形模式)，媒體元資料也包含了媒體資料的參考資訊，亦即說明樣本資料是存放在哪個檔案中，另外提供樣本表元資料詳細說明樣本描述、長度以及每個媒體樣本的資料參考位元組偏移值等重要屬性。

[3]單軌標頭元資料(Trak Header Atom)中的width及height欄位值皆以像素為單位。

媒體元資料下又包含媒體標頭元資料(Mdhd Atom)及媒體資訊元資料(Minf Atom)等元資料資訊，其中媒體標頭元資料係用於說明媒體的相關特性，包括媒體資料的建立及修改時間、時間比例及影片時間週期等資訊。媒體資訊元資料則包括影片媒體檔頭資訊(Video Media Header)、資料資訊容器(Data Information Container)及樣本表元資料(Sample Table Atom)等重要元資料內容。

在單軌元資料中還有另外四種很重要的Atom，分別為(1)編輯列表元資料(Edit list Atom)，Atom欄位名稱為「Elst」，內部存放能明確相對應的單軌出現時間以及內部每個樣本時間間隔的資料結構，使得MP4檔案內影像藉由讀寫這些編輯列表元資料就可以達到播放樣本的功能。(2)處理程序參考元資料(Handler Reference Atom)，Atom欄位名稱為「Hdlr」，說明用於解譯媒體資料的媒體處理程序元件的資訊，重要資料包括處理程序的型態(例如「Vide」就是定義視訊資料，「Soun」則用於定義聲音資料)。(3)資料參考元資料(Data Reference Atom)，Atom欄位名稱為「Dref」。提供如何存取單軌的媒體資料，以及指出媒體資料是否存在於目前的MP4檔案或在其他檔案中。(4)樣本表元資料(Sample Table Atom)，Atom欄位名稱為「Stbl」。提供有關每個樣本詳細的資訊，樣本表是由一群元資料所組成，而這些元資料是以表格的型態呈現，表格中定義了每個樣本實體位置的資訊，以及時間資訊，藉由把時間資訊轉成樣本的號碼及樣本的位置，藉此可查出每個樣本位在單軌中的實際存放位址。而樣本表元資料內部又包含6種具有重要數位鑑識價值的元資料，分述如下：

(1)樣本描述元資料(Sample Description Atom)：Atom欄位名稱為「Stsd」，會根據媒體資料類型的差異而有所不同。對於媒體單軌而言，其含有MPEG-4 基本串流媒體描述資料(Elementary Stream Descriptions)。

(2)時間對樣本元資料(Time-to-Sample Atom)：Atom欄位名稱為「Stts」，其內部

存著每筆樣本的週期資訊，藉由此元資料的資料可以查出各個樣本的顯示時間為何。

(3)同步樣本元資料(Sync Sample Atom)：Atom欄位名稱為「Stss」，此元資料定義了媒體資料中的主鍵畫面資料，在此主鍵畫面資料的定義為沒有經過動態預測/補償所編出來的影像，因此失真度不會從上一張影像累積下來，進而提供一串影像重新同步化的功能。

(4)樣本對資訊塊元資料(Sample-to-Chunk Atom)：Atom欄位名稱為「Stsc」，內部存著資訊塊的資訊，讓使用者可以藉由查表得知各個樣本位於那一個資訊塊以及資訊塊中的那個位置。

(5)樣本大小元資料(Sample Size Atom)：Atom欄位名稱為「Stsz」，其內容記載了各個樣本的大小，如果只有一個樣本，則此Atom的「size」欄位只有一個，如果有多個樣本，則此欄位以向量形式呈現。

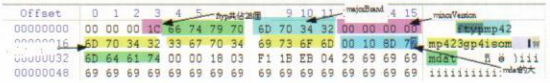
(6)資訊塊偏移值元資料(Chunk Offset Atom)：Atom欄位名稱為「Stco」，此元資料內容記載了從MP4檔案開頭到每個資訊塊的偏移值，單位以位元組為單位，可以32位元或64位元數字來表示。

MPEG-4視訊檔使用「MP4v」的資料格式，並使用所謂的基本流媒體描述符元資料(Esds，Elementary Stream Description)來增強媒體樣本的描述，以補充標準視訊樣本描述的不足。MPEG-4基本流媒體描述符元資料所包含的Atom皆完整定義於MPEG-4標準10中 (ISO/IEC FDIS 14496-1) 。

此元資料重要且最具鑑識價值的元資料欄位就是「DecConfigDescr」下層欄位的「DecSpecificInfo」的「Info」元資料欄位值，該數值就是提供MPEG-4串流媒體的特定資訊，亦是提供MPEG-4解碼的重要資訊。MP4(H.264)視訊檔係使用所謂的AVC視覺串流組態元資料(AVC Visual Stream Configuration，‘avcC’)來增強媒體樣本的描述。此元資料最重要且具鑑識價值的欄位值就是「SequenceEntries」下層欄位的「SequenceParameterSetNALUnit」元資料欄位值，該值就是提供MPEG-4(H.264)串流媒體的特定資訊，亦是提供MPEG-4(H.264)解碼的重要資訊。

3.2 MP4/3GP ATOM元資料解讀範例

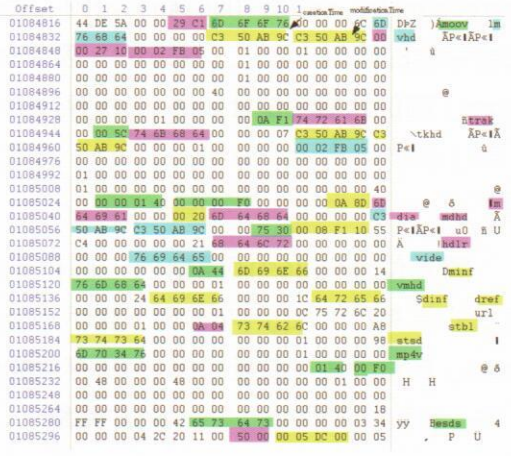
以下使用Nokia E51手機之02112007.MP4檔說明MPEG-4流媒體所內嵌之Atom資料(如圖五所示)，由檔頭部分開始解譯，這些位元組所代表的意義解釋如下：



圖五、以WinHex檢視MP4 檔頭資訊

圖五位址3存放的2個字元組為‘0x1C’，換算為十進位表示為”28”，亦即表示「Ftype Atom」起始位置為0在位址28結束。位址4-7表示「Ftyp」識別字。位址8-11表示「Major Brand」，在此為「MP42」。位址12-15表示「Minor Version」，在此值為「0」。位址16-27表示「Compatible Brands」，在此為「MP423GP4isom」。位址28-31所表示之

「00108D77」十六進位值，經換算為十進位的值為「1084783」，此值表示整個Mdat Atom在檔案中所佔用的位元組。



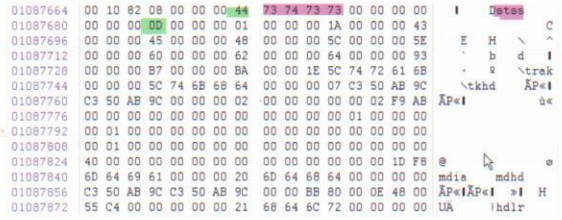
圖六、WinHex檢視MP4檔案Atom結構

圖六位址1084821開始的二個位元組存放的值為「29C1」(1068110)，表示「Moov Atom」的所使用的容量，起始位置為108481910，結束位置為109550810。位址1084830所存放的值「6C」表示「Mvhd Atom」的所佔用的位元組。位址1084839-1084842表示建立時間，值為「327684393210，Fri Nov 02 18:25:32 2007 UTC」。位址1084843-1084846表示修改時間，值為「327684393210，Fri Nov 02 18:25:32 2007 UTC」。位址1084847-1084850表示時間比例尺，在此值為「2710」(1000010)。位址1084851-1084854表示時間週期(單位為千分之一秒)，在此值為「02FB05」(19533310)，將該值乘以千分之一秒則為195.333秒，表示影片時間長度為195.333秒。

位址1084937開始的二個位元組存放的值為「0AF1」(279310)，表示「Trak Atom」的大小。位址1084946存放的值為「005C」(8410)，表示「Tkhd Atom」的大小，位址1084955-1084958表示建立時間，值為「327684393210，Fri Nov 02 18:25:32 2007 UTC」。位址1084959 -1084962表示修改時間，值為「327684393210，Fri Nov 02 18:25:32 2007 UTC」。位址1084971 -1084974表示時間週期， 在此值為「02FB05 」(19533310) 。位址1085025-1085028表示寬度，在此為「0140」(32010)，位址1085029-1085032表示高度，在此為「00F0」(24010)。位址1085037開始的二個位元組存放的值為「0A8D」(269310)，表示「Mdia Atom」的大小。位址1085046所存放的值「20」表示「Mdhd Atom」的大小。

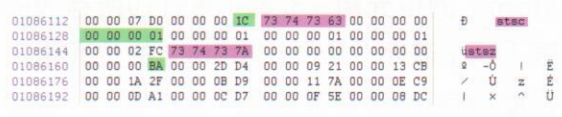
位址1085055-1085058表示建立時間，值為「327684393210，Fri Nov 02 18:25:32 2007UTC」。位址1085059-1085062表示修改時間，值為「327684393210，Fri Nov 02 18:25:322007 UTC」。位址1085063-1085066表示時間比例尺，在此值為「7530」(3000010)。位址1085067-1085070表示duration，在此值為「0008F110」(58600010)。位址1085078所存放的值「21」表示「Hdlr Atom」的位元組。位址1085063-1085066表示「HandlerType」，在此顯示為「vide」。位址1085110開始的二個位元組存放的值為「0A44」(262010)，表示「Minf Atom」的位元組。位址1085119所存放的值「14」表示「Vmhd Atom」的位元組。位址1085139所存放的值「24」表示「Dinf Atom」的位元組。位址1085147所存放的

值「1C」表示「Dref Atom」的位元組。位址1085174開始的二個位元組存放的值為「0A44」(255610)，表示「Stbl Atom」的位元組。位址1085183所存放的值「A8」表示「Stsd Atom」的位元組。位址1085199所存放的值「98」表示「MP4v Atom」的位元組。位址1085228-1085229表示寬度，在此為「0140」(32010)，位址1085230-1085231表示高度，在此為「00F0」(24010)。位址1085285所存放的值「42」表示「Esds Atom」的位元組。



圖七、以WhinHex檢視Stts Atom結構

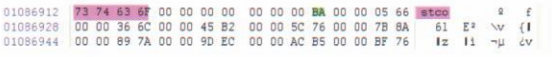
圖七位址1085315所存放的值「1D」(2910)表示「decSpecificInfo descriptor」的位元組，該描述符下的「info」欄位值以十六進位表示為「000001B002000001B50ECF0000010000000120086C5D4C285020F0A31」，該值所佔用之位元組及內容可能依廠牌及型號之差異而有所不同。位址1085350開始的二個位元組存放的值為「0300」(76010)，表示「Stts Atom」的位元組。位址1085363所存放的值「5E」(9410)表示「EntryCount」的位元組。



圖八、以WinHex檢視 stsc Atom結構

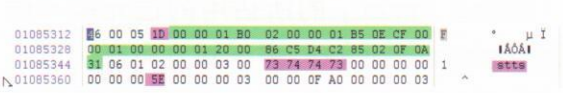
圖八位址1086119所存放的值「1C」表示「Stsc Atom」的位元組。位址1086128-1086131所存放的值為「1」，表示entryCount為1。位址1086146開始的二個位元組存放的值為「02FC」(75610)，表「Stsz Atom」的位元組。位址1086163所存放的值「BA」(18610)表示「SampleCount」的位元組。

圖九位址1086910開始的二個位元組存放的值為「02F8」(76010)，表示「Stco Atom」的位元組。位址1086163所存放的值「BA」(18610)表示entryCount的位元組。



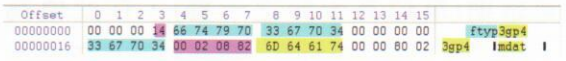
圖九、以WinHex檢視 Stco Atom結構

圖十位址1087671開始的二個位元組存放的值為「0044」(6810)，表示「Stss Atom」的位元組。位址1087683所存放的值「0D」(1310)表示entryCount的位元組。



圖十、以WinHex檢視Stss Atom結構

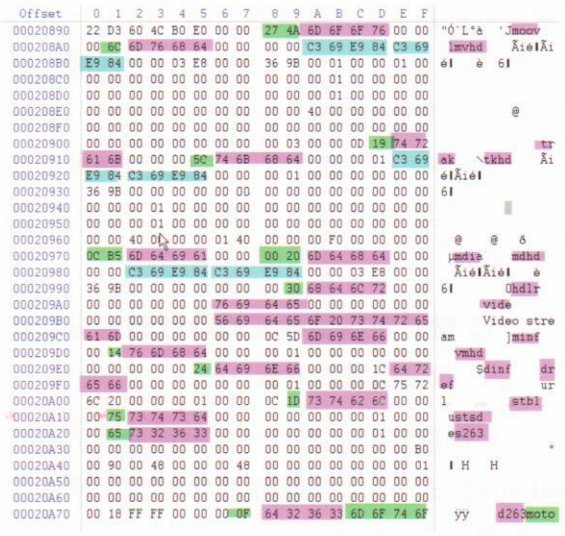
以下使用Motorola U9手機之moto1.3GP檔說明3GP(H.263)流媒體所內嵌之Atom資料(如圖十一所示)，由檔頭部分開始解譯，這些位元組所代表的意義解釋如下：



圖十一、3GP檔頭階層結構

圖十一位址3存放的2個字元組為0x14，換算為十進位表示為20，亦即表示「Ftype

Atom」起始位置為0在位址20結束，位址4-7表示「Ftyp Atom」識別字，位址8-11表示「MajorBrand」，在此為「3GP4」，位址12-15表示「MinorVersion」，在此值為「0」，位址16-27表示「Compatible Brands」，在此為「3GP4」，位址28-31所表示之「00020882」十六進位值，在此換算為十進位的值為「133242」，此值表示整個Mdat Atom在檔案中所佔用的位元組。



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00020890	22	D3	6D	4C	B0	E0	00	00	27	4A	6D	6F	6F	76	00	00	"ÓmL°à 'Jmoov
000208A0	00	6C	6D	76	68	64	00	00	00	00	C3	69	E9	84	C3	69	lmvhd Ãié„Ãi
000208B0	E9	84	00	00	03	E8	00	00	36	9B	00	01	00	00	01	00	é„ è 6l
000208C0	00	00	00	00	00	00	00	00	00	00	00	01	00	00	00	00	
000208D0	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00	
000208E0	00	00	00	00	00	00	00	00	00	00	40	00	00	00	00	00	@
000208F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00020900	00	00	00	00	00	00	00	00	00	03	00	00	0D	19	74	72	tr
00020910	61	6B	00	00	00	5C	74	6B	68	64	00	00	00	01	C3	69	ak \tkhd Ãi
00020920	E9	84	C3	69	E9	84	00	00	00	01	00	00	00	00	00	00	é„Ãié„
00020930	36	9B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	6l
00020940	00	00	00	01	00	00	00	00	00	00	00	00	00	00	00	00	
00020950	00	00	00	01	00	00	00	00	00	00	00	00	00	00	00	00	
00020960	00	00	40	00	00	00	01	40	00	00	00	F0	00	00	00	00	@ @ ð
00020970	0C	B5	6D	64	69	61	00	00	00	20	6D	64	68	64	00	00	µmdia mdhd
00020980	00	00	C3	69	E9	84	C3	69	E9	84	00	00	03	E8	00	00	Ãié„Ãié„ è
00020990	36	9B	00	00	00	00	00	00	00	30	68	64	6C	72	00	00	6l 0hdlr
000209A0	00	00	00	00	00	00	76	69	64	65	00	00	00	00	00	00	vide
000209B0	00	00	00	00	00	00	56	69	64	65	6F	20	73	74	72	65	Video stre
000209C0	61	6D	00	00	00	00	00	00	0C	5D	6D	69	6E	66	00	00	am]minf
000209D0	00	14	76	6D	68	64	00	00	00	01	00	00	00	00	00	00	vmhd
000209E0	00	00	00	00	00	24	64	69	6E	66	00	00	00	1C	64	72	$dinf dr
000209F0	65	66	00	00	00	00	00	00	00	01	00	00	00	0C	75	72	ef ur
00020A00	6C	20	00	00	00	01	00	00	0C	1D	73	74	62	6C	00	00	l stbl
00020A10	00	75	73	74	73	64	00	00	00	00	00	00	00	01	00	00	ustsd
00020A20	00	65	73	32	36	33	00	00	00	00	00	00	00	01	00	00	es263
00020A30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	B0	°
00020A40	00	90	00	48	00	00	00	48	00	00	00	00	00	00	00	01	‖ H H
00020A50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00020A60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00020A70	00	18	FF	FF	00	00	00	0F	64	32	36	33	6D	6F	74	6F	ÿÿ d263moto

圖十二、3GP Moov Atom階層結構

圖十二位址20898開始的二個位元組存放的值為「274A」(1005010)，表示「Moov Atom」的位元組，起始位置為13327010，結束位置為14332810。位址208A1所存放的值「6C」表示「Mvhd Atom」的位元組。位址208AA-208AD表示建立時間，值為「327849818010，Wed Nov 21 21:56:20 2007 UTC」208A1-208B1表示修改時間，值為「327849818010，Wed Nov 21 21:56:20 2007 UTC」。位址208B4-208B5表示時間比例尺，在此值為「03E8」(100010)。位址208B8-208B9表示時間週期，表示時間週期(單位為千分之一秒)，在此值為「369B」(1397910)，將該值乘以千分之一秒則為139.79秒，表示影片時間長度為139.79秒。

位址2090C開始的二個位元組存放的值為「0D19」(334510)，表示「Trak Atom」的位元組。位址20915存放的值為「5C」(8410)，表示「Tkhd Atom」的位元組，位址2091E-20921表示建立時間，值為「327849818010，Wed Nov 21 21:56:20 2007 UTC」位址20922-20925表示修改時間，值為「327849818010，Wed Nov 21 21:56:20 2007 UTC」。位址20930開始的二個位元組表示時間週期，在此值為「369B」(1397910)。位址20964-20967表示寬度，在此為「0140」(32010)，位址20968-2096B表示高度，在此為「00F0」(24010)。

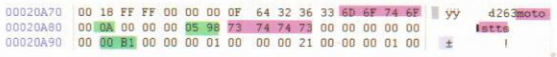
位址20970開始的二個位元組存放的值為「0CB5」(324510)，表示「Mdia Atom」的位元組。位址20979所存放的值「20」表示「Mdhd Atom」的位元組。位址20982-20985表示建立時間，值為「327849818010，Wed Nov 21 21:56:20 2007 UTC」位址20986-20989表示修改時間，值為「327849818010，Wed Nov 21 21:56:20 2007 UTC」。位址2098C-2098D表示時間比例尺，在此值為「03E8」(100010)。位址20990-20991表示時間週期，在此值為「369B」(1397910)。

位址20999所存放的值「30」表示「Hdlr Atom」的位元組。位址209A6-209A9表示「HandlerType」，在此顯示為

「Vide」，位址209B6-209C1表示「Handler name」，在此值顯示為「Video stream」。位址209C8開始的二個位元組存放的值為「0C5D」(315710)，表示「Minf Atom」的位元組。位址209D1所存放的值「14」表示「Vmhd Atom」的位元組。位址209E5所存放的值「24」表示「Dinf Atom」的位元組。位址209ED所存放的值「1C」表示「Dref Atom」的位元組。

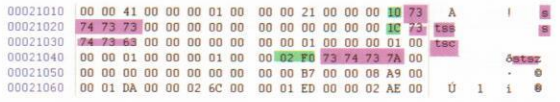
位址20A08開始的二個位元組存放的值為「0C1D」(309310)，表示「Stbl Atom」的位元組。位址20A12所存放的值「75」表示「Stsd Atom」的位元組。位址20A21所存放的值「65」表示「s263 Atom」的位元組(s263表示H263 Sample Description)。位址

20A3E-20A3F表示樣本之寬度，在此為「00B0」(17610)，單位為像素。位址20A40-20A41表示樣本之高度，在此為「0090」(14410)，其意義為每個樣本之高度，單位為像素。位址20A77所存放的值「0F」表示「d263 Atom」的位元組。



圖十三、3GP d263及Stts Atom結構

圖十三位址20A7C-20A7F表示「Vendor」，在此顯示為「moto」(1836020847 10)，位址20A81表示「h263Level」，在此顯示為「0A」(1010)。位址20A85開始的二個位元組存放的值為「0598」(142410)，表示「Stts Atom」的位元組。位址20A92所存放的值「B1」(17710)表示「EntryCount」的位元組。



圖十四、3GP stss等Atom階層結構

圖十四位址2101E存放的值為「10」(1610)，表示「Stss Atom」的位元組。位址21027-2102A所存放的值「00000000」表示EntryCount的位元組為0。位址2102E所存放的值「1C」表示「Stsc Atom」的位元組。位址2103A所存放的值為「01」，表示「EntryCount」為1。位址21049開始的二個位元組存放的值為「02F0」(75210)，表示「Stsz Atom」的位元組。位址2105A所存放的值「B7」(18310)表示「SampleCount」的位元組。

3.3 常見視訊編輯或轉換軟體的分類與數位鑑識的價值

目前在網路上有許多免費或商用的3GP/MP4(H.263/H.264)多媒體視訊編輯及轉換工具軟體可供下載試用，並可讓使用者直接編輯與轉檔由行動數位裝置所拍攝的3GP/MP4視訊檔案內容。這些視訊檔案編輯或轉檔工具軟體在常見的WINDOWS/MAC/LINUX等三大作業系統都提供有不同的版本，本研究僅針對微軟視窗作業系統平台上的視訊編輯或轉檔軟體進行相關鑑識實驗，嘗試以數位鑑識的角度來觀察及檢驗這些視訊檔案編輯與轉檔工具軟體所產生的結果，是否可做為某些有心人士用來規避多媒體視訊影片檔案來源鑑別及視訊檔案內容偽變的一種反電腦鑑識工具。為了使數位鑑識人員對這些軟體有更多瞭解，本研究共列出45種市面上常見之

3GP/MP4(H.263/H.264)多媒體視訊編輯及轉換工具軟體名稱、版本、可接受之輸入視訊格式、支援之功能以及具數位鑑識價值之多媒體視訊檔案格式等資訊。上述軟體依視訊檔案編輯與轉檔等處理功能可概分為3類，如表二所示。第1類為提供視訊檔案編輯及轉檔功能，如OpellVideo to 3GP Converter軟體。第2類為提供合併視訊檔案與轉檔功能，如Intertech 3GP Converter等軟體。第3類為僅提供轉檔功能，如ABC 3GP/MP4 Converter等軟體。這些編輯或轉檔工具軟體絕大部分都可匯入各種視訊或影像檔案格式使用，僅有少部分只能匯入3GP/MP4等特定之視訊檔案格式，而不支援其他類型多媒體視訊檔案格式匯入。

表二： 3GP/MP4(H.263/H.264)視訊編輯/轉換軟體表

軟體分類	軟體名稱	編輯/轉檔 功能	軟體所產生之具數位鑑識價值的視訊檔案格式
提供視訊檔案編輯及轉檔功能	OpellVideo to 3GP Converter等3種	編輯及轉檔	3GP(H.263),MP4(H.264)、3G2,特定手持式行動機型3GP
提供合併視訊檔案與轉檔功能	Intertech 3GP Converter等3種	合併與轉檔	3GP(H.263),MP4(H.264)
提供轉檔功能	ABC 3GP/MP4 Converter等36種	轉檔	3GP(H.263),3G2,MP4(H.264),Mortola,Nokia,Samsung,SonyEricsson

四、多媒體視訊檔內容來源鑑別及檔案內容是否偽變之數位鑑識流程與方法

本研究使用之多媒體視訊檔案來源，選定為使用行動電話(Mobile)及個人數位助理(PDA)等手持式行動數位裝置所拍攝之多媒體視訊影片做為實驗觀察之標的。所有實驗之行動數位裝置機型至少取得3筆以上3GP/MP4(H.263/H.264)多媒體視訊檔以做為鑑識基準樣本。另上述每種機型之基準樣本視訊檔再以FTK Imager鑑識軟體複製3份，以供檢驗不同之3GP/MP4(H.263/H.264)多媒體視訊編輯或轉檔軟體進行內容編輯竄改及轉檔等動作之實驗對照組。

有關鑑別3GP/MP4(H.263/H.264)多媒體視訊檔是否係原件及檔案內容有無遭偽變竄改之數位鑑識方法可分為以下9個步驟：

步驟1：取得3GP/MP4(H.263/H.264)多媒體視訊編輯或轉檔工具軟體，並紀錄有關該軟體之版本及功能等相關資訊。

步驟2：針對欲鑑識之行動數位裝置機型，儘可能取得相關視訊影片檔案格式資料，以供比對相關Atoms元資料相關資訊。

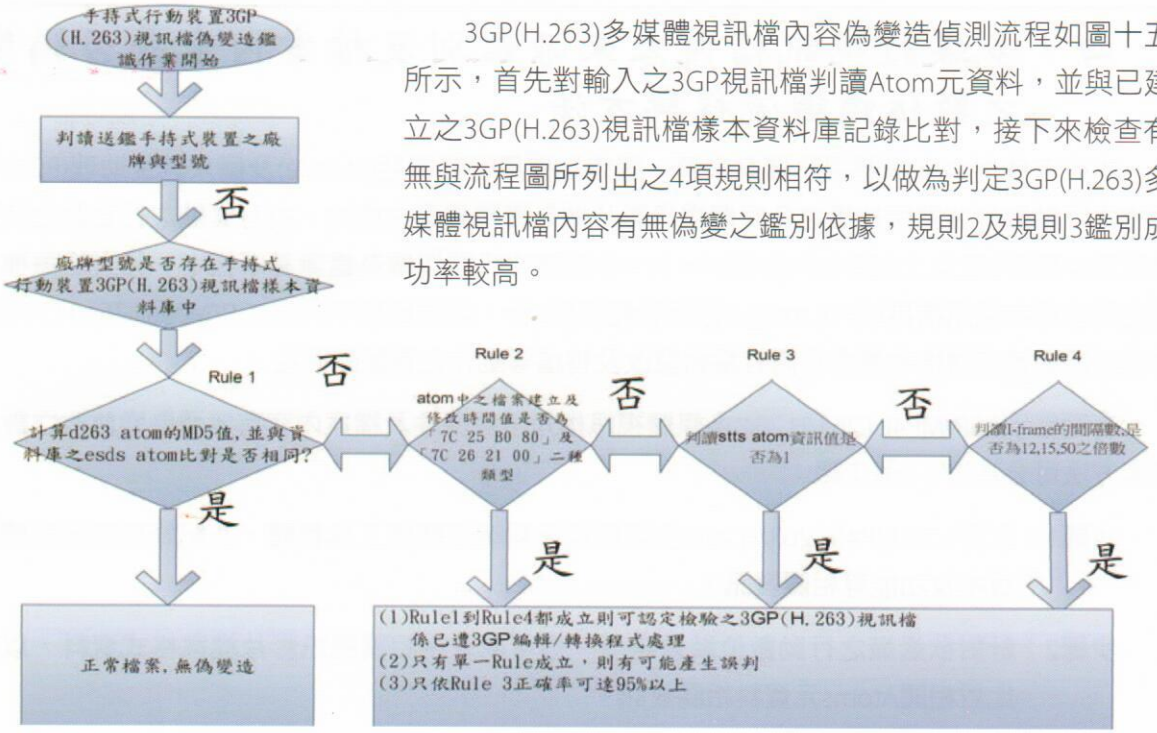
步驟3：取得上述行動數位裝置所拍攝之3筆3GP/MP4(H.263/H.264)多媒體視訊影片檔案樣

本，以此作為判讀之基準樣本檔，並複製3份，作為實驗修改對照組樣本。

步驟4：使用WinHex等鑑識軟體判讀及檢驗基準3GP/MP4(H.263/H.264)多媒體視訊影片檔中之esds Atom、d263 Atom、avcC Atom、tkhd Atom及mdhd Atom之建立時間及修改時間欄位資訊、stts Atom、stsz Atom、stco Atom及I-Frame出現的間隔數目等資料。此步驟需判讀多筆多媒體視訊影片檔，以確認相關檢驗資訊，esds Atom、d263 Atom及avcC Atom資訊另以MD5演算法計算雜湊值(Hash Value)，並匯入行動數位裝置3GP/MP4(H.263/H.264)多媒體視訊檔實驗資料表中以供比對。

步驟5：依序啟動45種3GP/MP4(H.263/H.264)視訊編輯或轉檔工具軟體，並以實驗修改對照組視訊檔樣本做為視訊編輯或轉檔軟體編輯之標的， 並檢查對照組中3GP/MP4(H.263/H.264)多媒體視訊影片檔內嵌之Atom元資料中有關Esds、d263、Stts、Stsz、Stco及時間等欄位資訊。

步驟6：使用WinHex等鑑識軟體判讀及檢驗實驗修改對照組3GP/MP4(H.263/H.264)多媒體視訊影片檔樣本與步驟4檢驗之相同資料，Esds Atom、d263 Atom及avcC Atom等資訊另以MD5演算法計算雜湊值。



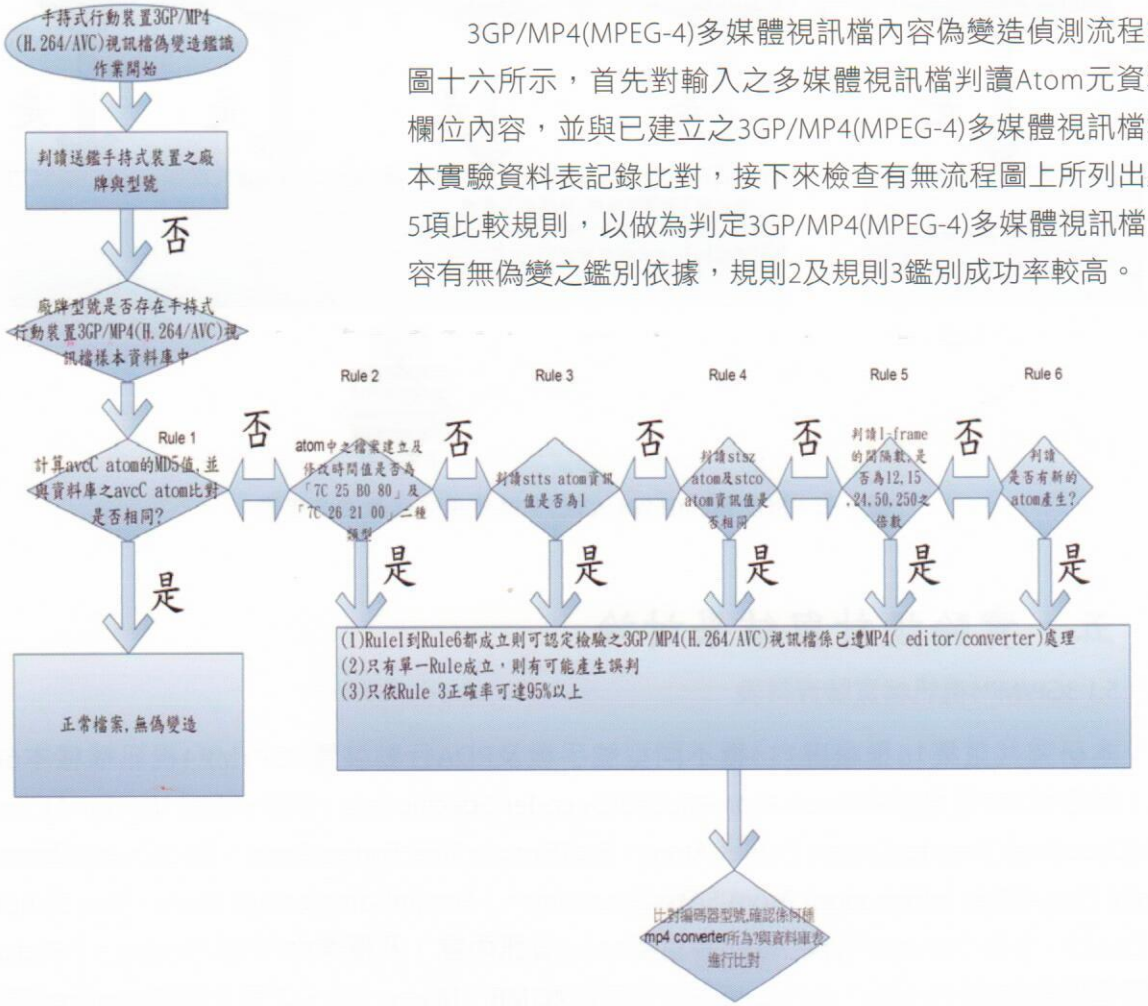
3GP(H.263)多媒體視訊檔內容偽變造偵測流程如圖十五所示，首先對輸入之3GP視訊檔判讀Atom元資料，並與已建立之3GP(H.263)視訊檔樣本資料庫記錄比對，接下來檢查有無與流程圖所列出之4項規則相符，以做為判定3GP(H.263)多媒體視訊檔內容有無偽變之鑑別依據，規則2及規則3鑑別成功率較高。

圖十五、3GP(H.263)多媒體視訊檔鑑識流程圖

步驟7：將步驟6產生之Esds Atom、d263 Atom及avcC Atom之MD5雜湊值與步驟4產生之行動數位裝置3GP/MP4(H.263/H.264)多媒體視訊檔資料表進行比對，其他結果之變化則以UltraCompare Professional檔案內容比較分析軟體分析比對。

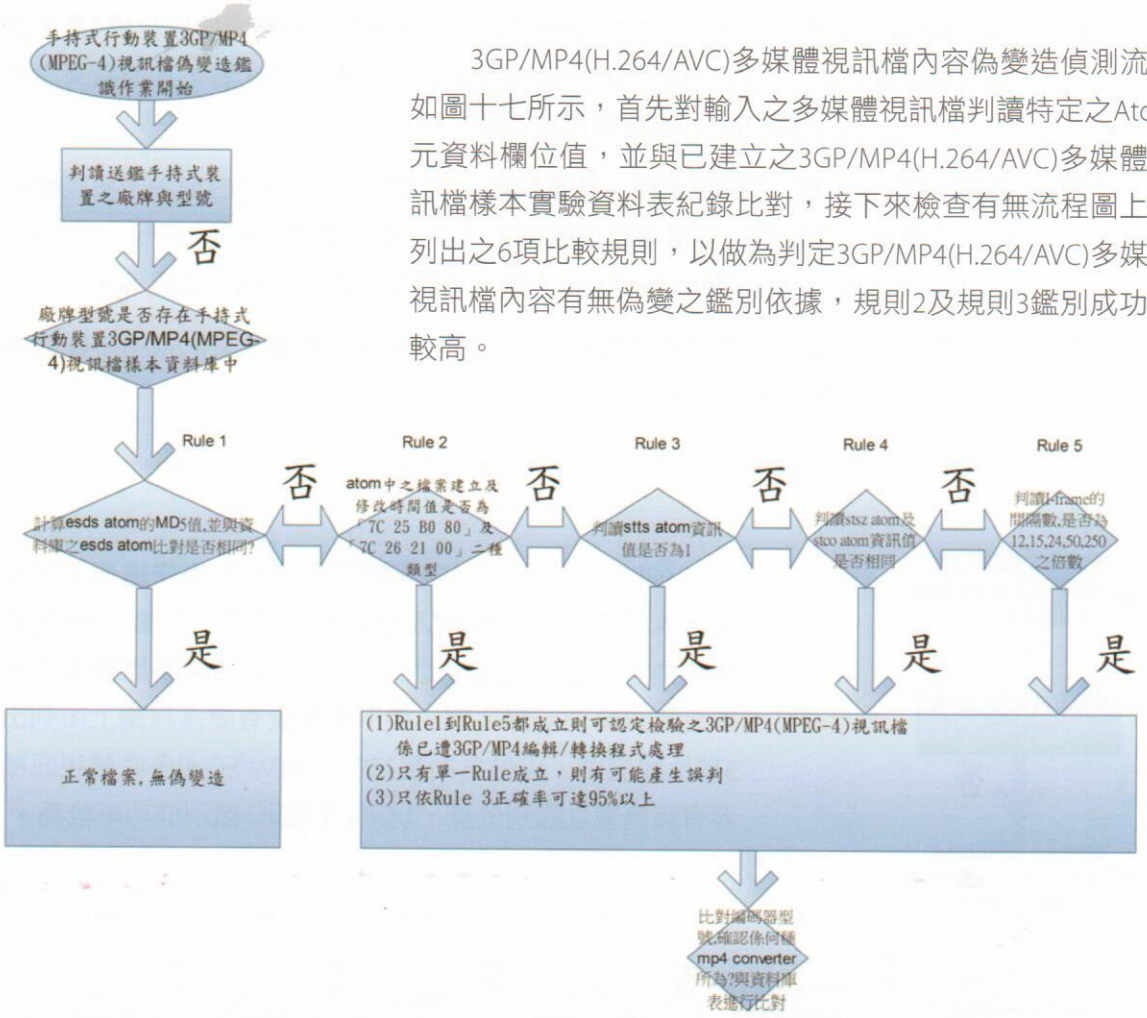
步驟8：重複步驟1至步驟7之檢驗步驟，並嘗試個化特定3GP/MP4(H.263/H.264)多媒體視訊編輯或轉檔工具軟體之特徵項目或軟體工具痕，如特定之Esds Atom、d263Atom、avcC Atom及Tkhd Atom及Mdhd Atom之建立時間及修改時間欄位資訊等。

步驟9：針對實驗結果進行軟體特徵比對及分類，歸納出所有檢驗之3GP/MP4多媒體視訊編輯或轉檔工具軟體之特性。



3GP/MP4(MPEG-4)多媒體視訊檔內容偽變造偵測流程如圖十六所示，首先對輸入之多媒體視訊檔判讀Atom元資料欄位內容，並與已建立之3GP/MP4(MPEG-4)多媒體視訊檔樣本實驗資料表記錄比對，接下來檢查有無流程圖上所列出之5項比較規則，以做為判定3GP/MP4(MPEG-4)多媒體視訊檔內容有無偽變之鑑別依據，規則2及規則3鑑別成功率較高。

圖十六、3GP/MP4(MPEG-4)多媒體視訊檔鑑識流程圖



圖十七、3GP/MP4(H.264/AVC)多媒體視訊檔鑑識流程圖

3GP/MP4(H.264/AVC)多媒體視訊檔內容偽變造偵測流程如圖十七所示，首先對輸入之多媒體視訊檔判讀特定之Atom元資料欄位值，並與已建立之3GP/MP4(H.264/AVC)多媒體視訊檔樣本實驗資料表紀錄比對，接下來檢查有無流程圖上所列出之6項比較規則，以做為判定3GP/MP4(H.264/AVC)多媒體視訊檔內容有無偽變之鑑別依據，規則2及規則3鑑別成功率較高。

五、實驗設計與結果討論

5.1 3GP/MP4視訊檔實驗資料表

本研究共蒐集16種廠牌114種不同型號手機及PDA行動裝置3GP/MP4視訊檔樣本640筆，並分析3GP視訊檔中Moov Atom如d263(Decoder Specific Info H263 Video) Vendor Atom、Stts(Decoding) Time-to-Sample Entries Atom、Stsz(Sample Size) Entries Atom、Stco(Chunk Offset，Partial Data-Offset Information) Atom、Stss(Sync (Key， I-Picture)Samplemap) Atom、Stsc Sample-to Chunk、Hdlr Handler Type Atom等重要Atom資訊內容，及檔案中所有I-Picture、P-Picture間隔情形與每個I-Picture、P-Picture內所有巨區塊(MB，Macro Block)之量化值(Quantizer)變化情形，經過濾分析確認以MP4視訊影片檔內嵌之Esds Atom Decspecificinfo 項目及avcC Atom

SequenceParameterSetNALUnit 項目MD5值可個 化出63種手機型號裝置，另以3GP視訊影片檔內嵌之d263(Decoder Specific Info H263 video) Vendor Atom可個化出12種手機型號裝置。

5.2 實驗設計

本實驗主要在驗證由本研究所提出之45種3GP/MP4視訊編輯或轉檔軟體對行動裝置3GP/MP4視訊檔進行視訊檔案編輯、剪接、合併及轉檔等作業後，透過分析相同廠牌機型之已編修及轉檔之視訊檔及正常之樣本視訊檔之檔案內容及Atom元資料變化情形，整理及歸納出具判斷價值之特徵，並驗證偵測這些特徵的正確率及錯誤率資料，以做為送鑑3GP/MP4視訊檔來源判讀是否為可信賴及正確。在3GP/MP4視訊檔編輯或轉換軟體方面，目前所歸納及整理出可供判斷比對之特徵分別有：視訊檔所內嵌Tkhd Atom 的建立及修改時間，內嵌之Stts Atom Entry Count值，內嵌之Stsz Atom Entry Count值是否相等於stco Atom之Entry Count 值，視訊檔中I-Picture出現之位置是否為12、15、20、50、250之倍數，3GP/MP4檔案之Esds Atom Decspecificinfo值是否與資料之相同機型之值相同，及3GP(h.263)檔案之d263 Vendor Atom是否與資料庫相同機型之值相同等特徵。

5.3 實驗結果

由本研究所提出之45 種3GP/MP4(H.263/H.264)多媒體視訊編輯或轉檔軟體對3GP/MP4(H.263/H.264)多媒體視訊檔進行視訊檔案編輯、剪接、合併及轉檔等實驗後，發現共有5種Atom元資料特徵項目(如表三所示)及1種視訊畫格(Frame)位置參數可供鑑別，不同軟體所符合之特徵項目及位置參數均有所不同，但特徵項目數字愈高者，表示視訊檔案曾以某些編輯或轉換軟體進行視訊內容編修之機率越高，亦即檢驗之視訊檔案鑑別為非原件之結果較為可能。特徵項目數字愈低者，表示可供鑑別之特徵項目極少，視訊檔案內容不易鑑別為原件或是否曾使用軟體編修。實驗結果顯示特徵項目值在5以上者計有4U MP4 VIDEO CONVERTER等22種視訊編輯或轉換軟體，特徵項目值在4者計有Aimersoft Video Editor 等11種視訊編輯或轉換軟體，特徵項目值在4者

計有Agogo Video to iPod/Cellphone/MP4等6種視訊編輯或轉換軟體，其他視訊編輯或轉換軟體則為特徵項目值為2以下。

特徵項目1之鑑別正確率最高，高達100%。原因在於樣本視訊檔經由視訊編輯或轉檔軟體所編修及轉檔處理過後，所產生之新的視訊檔案中之Tkhd Atom及Mdhd Atom的「Created Time」及「Modified Time」將可能會固定至某一特定時間值。實驗結果發現共有29種3GP/MP4編輯或轉換軟體會將所編修的視訊檔中所內嵌Tkhd Atom及mdhd Atom之「Created Time」及「Modified Time」的欄位值變更至「7C 25 B0 80」及「7C 26 21 00」，其中「7C 25 B0 80」解譯出之時間資訊為「Thu Jan 01 08:00:00 1970 UTC」，「7C 26 21 00」解譯出之時間資訊為「Thu Jan 01 16:00:00 1970 UTC」，但以此特徵項並無法個化到特定之單一特定之視訊編輯或轉檔軟體。

另外特徵項目3之鑑別正確率也可達95%以上，原因在於樣本視訊檔經由視訊編輯或轉檔軟體所編修及轉檔處理過後，所產生之新的視訊檔案中之stts Atom值幾乎都會為「1」。

其他特徵項目之錯誤率原因在於檢測之樣本部分資訊內容與特徵項目相同，導致錯誤率產生。部分3GP/MP4多媒體視訊編輯或轉檔軟體實驗結果如表三所示。

表三：3GP/MP4編輯或轉換軟體實驗結果

可供參考特徵 ＼ 軟體名稱		FREE 3GP VIDEO CONVETER	ImTOO. Video. Editor	VideoPad Video Editor
項目1	Tkhd Atom 及Mdhd 之 Created Time及Modified Time有無變化	YES	NO	YES
項目2	Stts Atom Entry Count值是否為1	YES	YES	YES
項目3	Stsz 與Stco Atom之Entry Count 值是否相等	YES	YES	YES
項目4	I-Picture出現之位置是否為12等數值之倍數	YES (12的倍數)	YES (12的倍數)	NO
項目5	3GP/MP4 Esds Atom Decspecificinfo 項目值及avcC Atom SequenceParameterSetNA L Unit項目值	Lavc52.10.0	avc2.0.11.111	Lavc52.11.0
項目6	3GP d263 Vendor Atom		FFMP	
可供參考特徵總計		5	4	4

六、結論與未來研究方向

本研究提出藉由觀察及檢驗行動裝置中之3GP/MP4(H.263/H.264)視訊影像檔案所內嵌之Atoms 元資料， 來判讀3GP/MP4(H.263/H.264) 多媒體視訊檔是否遭3GP/MP4(H.263/H.264)編輯及轉換等具反鑑識功能軟體剪接編輯、切割、合併、轉檔等偽變處理。並透過Atoms元資料檢視輔助工具的協助及提供數位鑑識人員需注意此類具反鑑識功能之3GP/MP4(H.263/H.264) 視訊編輯或轉換軟體之特徵項目， 例如由3GP/MP4(H.263/H.264)視訊檔所內嵌之Tkhd Atom及Mdhd Atom之建立時間及修改時間值是否改變，stts的值是否固定為「1」，Esds Atom Decspecificinfo值是否與原機型有所不同、視訊檔中之I-PICTURE(畫格)由隨機出現的狀態改變為出現規律之間隔性(位置參數)等特徵項目之變化，可充分鑑別3GP/MP4視訊檔是否為原件或檔案內容是否遭遭軟體編修。

有關3GP/MP4視訊檔內容偽變分析，本研究所提出以多媒體視訊檔內嵌之Atom 內容變化並找出特徵項作為比對之方法正確率高，但是僅止於可用於確認檔案來源是否為原件。至於能否找出視訊檔中剪輯或合成畫面的部分，本研究目前的方法並不適用，亦無法用於判讀視訊內容遭偽變之部分。如何應用本研究方法再拓展有關視訊檔案內容偽變部分的研究將可成為未來可進一步深入研究之方向。FACT

參考文獻

[1] 鄧少華、李栩洋，“多媒體視訊檔案鑑識研究”，2009第十二屆資訊管理學術暨警政資訊實務研討會論文集，2009。

[2] James Luck and Mark Stokes、“An Integrated Approach to Recovering Deleted Files from NANDFlash Data”，SMALL SCALE DIGITAL DEVICE FORENSICS VOL.2(1),2008.

[3] Karel Rijkse ，“H.263:Video coding for low bit rate communication”, Communication Magazine,IEEE，VOL.34(12),1996.

[4] ISO/IEC，” Information technology - Coding of audio-visual objects - Pt.12: ISO base media format”，Ref. No. ISO/IEC 14496-12:2005/Cor.1:2005(E),2005.

[5] ISO/IEC “Information technology - Coding of audio-visual objects - Pt.14: MP4 file format”, Ref. No. ISO/IEC 14496-14:2003(E),2003.

[6] F. Pereira and T. Ebrahimi , “The MPEG-4 Book, Prentice Hall IMSC multimedia series”，Prentice Hall,2002.

[7] B. Carrier, “File System Forensic Analysis”，Addison-Wesley,2005.

[8] Iain E and G Richardson, “Video Codec Design”, John Wiley and Sons, 2002.