手持式行動數位裝置之3GP/MP4多媒體視訊影片檔內容僞變偵測的研究

鄧思源
法務部調查局資通安全處資安鑑識實驗室 調查官
Buyer92@mjib.gov.tw

摘要

目前常見的行動數位裝置大部分都具有攝影的功能，而所拍攝的影片格式大部分爲壓縮的3GP及MP4的視訊格式，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爲重要物證時，數位鑑識人員如何快速鑑別所鑑定行動數位裝置不論是內嵌或外接之儲存媒體裝置中所存放之3GP/MP4視訊檔有無經過任何多媒體視訊編輯或轉檔軟體處理及修改?實爲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，數位鑑識人員該如何鑑別?本研究嘗試提出如何在多媒體數位鑑識實務作業中，以MP4及3GP視訊影片檔案中所內嵌特定之atoms元資料欄位內容來進行鑑別，以鑑定多媒體視訊影片是否已遭軟體竄改及編修，並嘗試個化出可用於僞變造視訊影片內容之3GP/MP4視訊編輯軟體的特徵項或軟體工具痕，並歸納出可列爲反電腦鑑識(Anti-Computer Forensics)工具之軟體。由實驗結果得知，本研究用於實驗的某些3GP/MP4視訊影片編輯及轉換軟體可鑑別出不同之特徵項或軟體工具痕，可滿足數位鑑識人員在鑑驗手持式裝置3GP/MP4多媒體視訊影片內容僞變偵測之鑑識需求。

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在2010年底已突破53億，另DIGITIMES Reasearch網站有關2010年全球手機市場規模調查資料顯示，2010年全球手機規模共約爲14.54億支，而2011年手機市場規模預測將可達15.54億支，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，而這些行動數位裝置大部分都具有攝錄視訊影片之功能，目前各廠牌所生產之手持式行動數位裝置，用來存放之多媒體視訊影片檔格式，約有95%皆預設副檔名爲MP4或3GP之多媒體視訊檔案格式，而透過Google搜尋引擎的搜尋功能，我們也可以在網際網路上發現許多免費或是商用可編輯或轉換3GP/MP4多媒體視訊影片檔之工具軟體，這些軟體設計主要目的爲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、音訊及特效等等，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爲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，大部分皆都是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僞變造鑑識及反鑑識工具偵測與判別的角度及觀點來看，這些常見的3GP/MP4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爲規避多媒體視訊影片檔案來源鑑別的一種反鑑識工具，我們來設想一些可能的犯罪場景，例如某人以匿名向司法機關檢舉並提供某件犯罪案件的多媒體視訊影片檔，要求偵辦追查視訊影片中的犯罪行爲人，同時檢舉人意在匿名檢舉信中可能提及該多媒體檔案之拍攝時間及系利用何種行動數位裝置所拍攝，例如宣稱該多媒體視訊影片檔係在2010年9月21日下午10時20分在台北市某地點，以Nokia 6300手機所拍攝。當司法機關收到這些多媒體視訊影片檔檢舉資料，要如何確認影片中之犯罪事實爲真?亦即該多媒體視訊影片確由Nokia 6300手機所拍攝之犯罪事實爲真，亦或爲假?因爲該多媒體視訊檔案有可能已經過上述視訊檔案編輯或轉換工具軟體之加工處理，多媒體視訊影片的內容實際上是已經過僞變造，而不是原先所檢舉之犯罪內容；以上所舉的多媒體視訊影片僞變造犯罪手法，我們尙可舉出許多其他以視訊影片編輯工具軟體加工僞造犯罪物證的其他案例，而目前司法機關對於手持式行動數位裝置所拍攝之多媒體視訊檔案的來源鑑別並無相關研究，也就是如何鑑別送鑑之3GP/MP4多媒體視訊影片檔案是否係由手持式行動數位裝置所拍攝之原件，而未經視訊編輯及轉換軟體處理之鑑定案件。

目前市面上有許多可用於編修3GP/MP4視訊檔案內容之多媒體視訊影片編輯或轉換軟體，該軟體可提供如影片合成、剪輯及轉檔等功能，因此本研究將透過藉由觀察3GP/MP4多媒體視訊影片檔案經3GP/MP4編輯及轉換工具軟體編修時，檔案所內嵌之atoms欄位資料內容變化情形，以歸納出多媒體視訊影片檔遭此類工具竄改時所顯現之特徵項目或軟體工具痕，並作爲判斷多媒體視訊影片是否爲原件以判定其證據能力之可信賴性，作爲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皆以MP4或3GP的多媒體檔案格式存在，如何透過視訊影片所內嵌之atoms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及3GP檔案格式所內嵌之atoms元資料資訊、I-VOP及P-VOP等影像之量化值(Quantizer)、I-PICTURE出現之位置等資訊之變化，作爲判讀視訊影片內容有無僞變之依據，並嘗試個化出各種3GP/MP4視訊編輯及轉換軟體之特徵或工具痕。

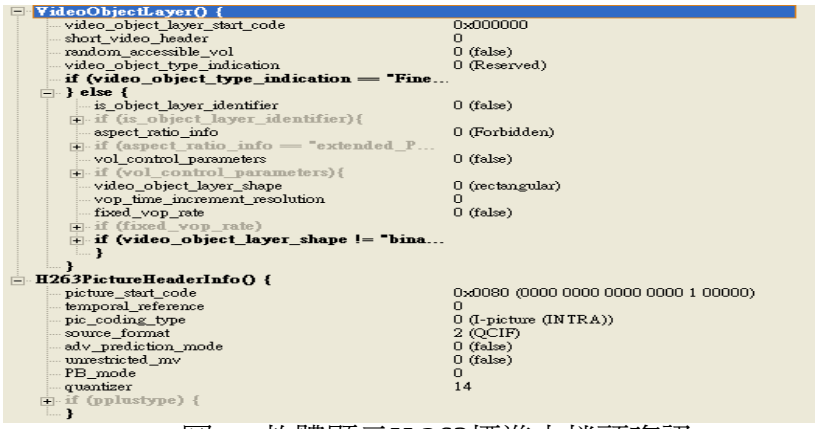
數位鑑識人員在從事3GP/MP4多媒體視訊影片檔之鑑驗作業前，必須對這些多媒體檔案標準與儲存檔案格式有相當之認識與了解，才能研究出如何判讀多媒體檔案內容是否僞變的鑑識方法及鑑驗程序，本篇研究將只針對涉及3GP與MP4多媒體檔案有關的標準與檔案格式介紹，以作爲多媒體檔內容僞變鑑識之基礎認識。

2.1 H.263標準

H.263是國際電信聯盟ITU-T的一個標準草案，是爲低碼流通信而設計的，標準的主要特定分爲以下5點:(1)採用圖片內（Intraframe)和圖片間(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圖片一樣的圖片預測方法。

H.263標準採用分層的方法來進行管理，可以分爲圖片序列、圖片組、圖片、區塊組層、巨塊層、區塊層等層級。在圖片層內包含輸入圖片順序的參數，表示圖片類型爲圖片內編碼還是像前預測編碼或雙向預測編碼的參數。圖片條的解碼包含圖片塊內的DCT係數解碼、運動向量解碼等等。巨區塊則是由巨區塊標投訊息和區塊資料組成，其中Quantizer Information(DQUANT，量化器訊息)，用於改變量化係數，共有-1，-2，1，2四種增量，如果相加超過了[1，31]的範圍，就將結構設定在邊界值，以軟體觀察H.263相關資訊如圖一所示：



圖一: 軟體顯示H.263標準之檔頭資訊

H.263標準提出了具體的格式與編碼技術，分別爲採用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。在編碼方面採用VLC編碼，該編碼是在霍夫曼編碼基礎上提出的新編碼方法，分別使用在MCBPC區塊、CBPY區塊、TCOEF區塊、INTRA模式DC係數、運動向量等可產生VLC編碼的地方。

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

2.2 H.264標準：

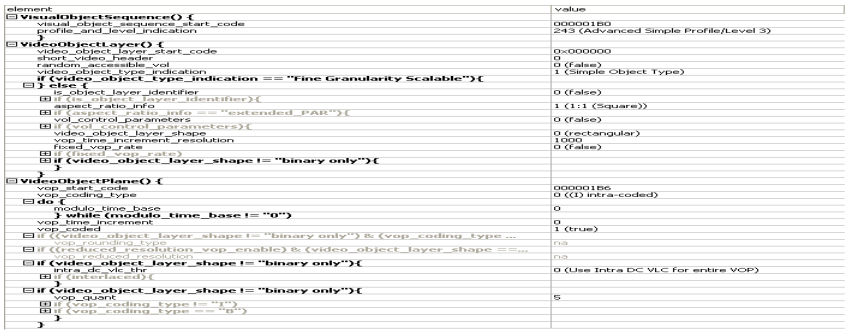
H.264標準是由JVT組織提出的新一代數位視訊編碼標準。H.264標準作爲MPEG-4標準的一個新的部分(MPEG-4 part.10)，H.264標準的主要特點有：(1)更高的編碼效率(2)高質量的視訊畫面(3)提高網路適應能力(4)採用混合編碼結構(5)H.264的編碼選項較少(6)H.264提供錯誤復原功能(7)有較高的複雜度。H.264設計上的理念是將視訊編碼與視訊傳輸分開來看，因此在語法的概念上區分爲視訊編碼層(VCL，Video Coding Layer)與網

路抽象層(NAL，Network Abstraction Layer)，VCL用於完成對視訊序列的高效率壓縮，NAL則是對具體的網路傳輸環境把壓縮資料進行傳輸封裝。H.264影片資料串流結構可分爲五層：視訊序列層，影像圖片層，片(Slice)層，巨塊(Macro Block)層，區塊(Block)層。

圖三: 視訊軟體顯示H.264標準檔頭資訊

2.3 MPEG-4標準(ISO/IEC 14496)標準

MPEG-4標準爲新一代的圖片壓縮編碼技術，它支持MPEG-1、MPEG-2中的多數功能，MPEG-4係基於視訊物件(VO，Video Objecr)進行壓縮編碼，具有可交互性以及寬碼率範圍的特性。通過VO來達到區域分層，可把視訊串流中的每一個圖框分割成任意的視訊物件平面(VOP，Video Object Plane)，視訊及音訊物件(AVO，Audio/Video Objects)是MPEG-4爲支持基於影片內容編碼而提出的重要概念，MPEG-4視訊串流可爲分爲5層，分別爲視訊物件序列(VS，Visual Object Sequence)、視訊物件(VO)，視訊物件層(VOL，Video Object Layer)、視訊物件平面層(GOV，Group Of Video Object Planes)、視訊物件平面(VOP)，檔頭資訊如下圖所示。



圖四：MPEG-4標準之檔頭資訊

2.4 MP4 (MPEG-4 Part 14) 檔案格式

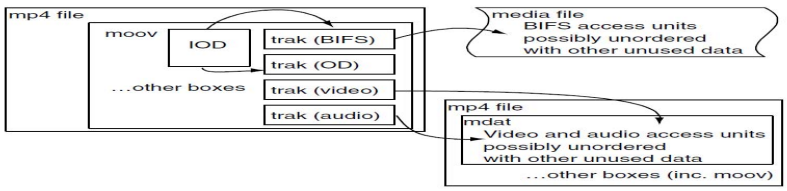
MP4是由MPEG-4標準所定義的多媒體容器格式，這種容器格式的完整名稱爲「MPEG-4 Part 14」，完整的定義在ISO/IEC 14496-14標準中，通常用於儲存視訊及音訊流媒體資料。而MPEG-4 Part 14 標準的基礎則建立在ISO/IEC14496-12:2004(MPEG-4 Part 12: ISO base media file format)標準之上，此標準制定的基礎主要基於Apple公司的QuickTime 多媒體容器格式規格之上，將MPEG-4 Part 14 (MP4)與MOV等二種檔案格式加以比較可以發現，此二種多媒體容器格式，主要架構內容大部分皆相同，但MP4尚支持所謂的起始物件描述(IOD，Initial Object Descriptors)的特性，MP4檔案格式可一般化

成ISO 基本媒體檔案格式(ISO/IEC 14496-12:2004)，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/音訊編解碼及不同的MPEG-4系統特色，例如物件描述以及場景描述等等。

在標準中制定的正式副檔名爲「.MP4」，副檔名命名可分爲以下3種狀況：(1)MPEG-4檔案包含視訊及音訊資料，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」作爲副檔名，但有時候也會使用此種副檔名作爲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資料(例如H.263及AMR等等)。

MP4所支援的編碼及額外資料流媒體大致可分爲視訊、音訊及字幕三類，本研究僅專注於視訊部分，視訊常用編碼格式如MPEG-4 Part 10 (亦即H.264/MPEG-4 AVC)、MPEG-4 Part 2等，其他較少使用的壓縮格式如MPEG-2及MPEG-1等標準。

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)分離開來，元資料包括了影像/聲音的時間資訊、影像/聲音資料所佔用的位元數以及此段影像在整個檔案的位置等多媒體資訊的重要參數，媒體資料內容爲數張影像/聲音編碼出來的資料流，它可以和元資料位在同一個檔案，也可以是位於另一個檔案中。MP4檔案把每個位元流資訊存放在一個Track裡，一個Track記載著一連串的影像/聲音的時間資訊以及資料型態，每個Track會有自己的Track Identifier，一個Track內有許多Samples，以影像資料爲例，一個Sample代表一個VOP。MP4的檔案格式會儲存每個Sample之間的時間差值，稱爲Duration，而相對應Track出現時間以及內部每個Sample時間間隔的資料結構則存在Edit List中，



圖五:交換檔格式-ISO 14494-PART 12

2.3 3GP (3GPP TS 26.244) 檔案格式

3GP(又稱3GPP檔案格式)是由第三世代夥伴計劃(The Third GenerationPartnership Project (3GPP))針對3G UMTS多媒體裝置所制定的一種多媒體容器格式，這種檔案格式通常用於3G行動電話，但亦可在2G的手機上播放。3G2(又稱3GPP2檔案格式)是由3GGP2針對3G CDMA2000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技術規格中，3G2檔案格式則定義在3GPP2的技術規範中。

3GP及3G2檔案格式二者的結構都是基於在ISO/IEC 14496-12(MPEG-4 Part 12)標準所定義的ISO基礎媒體檔案格式，規格方面大致可分爲以下兩項，分別爲(1)3GPP檔案格式係針對GSM爲主的手機來設計，通常會使用.3GP副檔名。(2) 3GPP2檔案格式係針對CDMA爲主的手機來設計，通常會使用.3G2副檔名。

3GP檔案格式中有關視訊流媒體的儲存，主要是以MPEG-4 Part2或H.263或MPEG-4 Part 10(亦即AVC/H.264)等視訊標準爲主，3GPP允許在ISO基礎多媒體檔案格式中使用

AMR及H.263的編碼格式，因爲3GPP在ISO基礎多媒體檔案格式中定義了樣本項目(Sample Entry)及模板欄位的用法，同時也定義了新容器(box，或稱爲atom)以對應所參用的編碼器。

三、多媒體視訊檔內容僞變鑑識原理

數位鑑識人員在鑑識有關3GP/MP4多媒體視訊檔案內容是否係原件或已經編輯或轉換軟體僞變造之處理，必須先瞭解3GP/MP4多媒體視訊檔之atom元資料概念以及可能會更改到這些元資料的相關軟體，以下分爲二部份討論：

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(或稱爲box)元資料前，必須先瞭解atom元資料的相關檔案結構與內容，atom也是MP4/3GP檔案的最基本的資料單元，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，atom的型態通常是以一組四字元的ASCII碼來表示，atom在本質上就是一個階層式的架構，也就是說一個atom可能爲一個容器(Container atom)，atom內部可以存放其他atom，也可以當作實際儲存資料的欄位(例如Leaf atom)，atom內部定義了資料結構的型別、長度等資訊。

在MP4/3GP檔案中，最上層的atom分別是ftyp，mdat、moov以及free等四種，此四種atom內部都可以個別再裝進其他種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則是空的、沒有用到的空間，其存在的原因是爲了預留給以後要再編輯、加入新資料使用的。

ftyp atom(File type compatibility)是用來識別檔案型態以及從類似的檔案型態加以區別，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」的值通常表示爲「MP42」，3GP檔案的「Major_Brand」的值通常表示爲「3GP4」或「isom」等等。Mdat atom(Movie sample data)用於區別如視訊框以及音訊樣本組等媒體樣本，通常這個atom資料僅用來解譯電影資源檔。Moov atom (Movie sample data)大部分皆由一個Movie Header(atom型態爲mvhd)和一個至多個track atom(atom型態爲trak)所組合而成，Movie Header內容包括此Movie data最初備建立的日期/時間、最後被更改的日期/時間、此Movie data的Time Scale、 Movie data的總長度以及此電影的播放速率(值通常設定爲1，表示正常速率)。

Track atom用於定義電影的single track，一部電影有可能是由一個或多個track所組成，每個track彼此之間都是獨立的有擁有自己的時間與空間資訊，跟moov atom一樣，track atom有Header記載其相對應的Media data最初被建立以及最後被更新的日期、此Track的總長度以及Meata data。Track atom中與元資料鑑識有較重要關係的atom分別爲tkhd atom (Track Header atoms)及mdia atom (Media atoms)，tkhd atom詳細說明電影中單軌所有的特性，重要內容包括版本、旗標狀態(通常設定值爲1)、track header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)、Track ID(如果顯示爲0，則表示無track可用)、track的總長度、track的寬度及高度(單位爲像素)。

mdia atom用於描述及定義一個電影軌的媒體形態(視訊或音訊)、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)，media atom也包含了

媒體資料的參考，亦即說明樣本資料存放在哪個檔案中，另外提供樣本表 atom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，media atom(‘mdia’)內容必須包含Media header atom(‘mdhd’)，mdhd atom也包含了’hdlr’atom (a handler reference atom)、’minf’atom (media information atom)及’udta’ atom(user data atom)。

Media header atoms詳細說明媒體的特性，包括media atom的建立及修改時間、時間比例及長度等資訊。Handler reference atom說明用於解譯媒體資料的媒體處理器元件的資訊，重要資料包括處理者型態，例如’vide’就是定義視訊資料’soun’則用於定義音訊資料，元件名稱則說明用於處理媒體的媒體處理器名稱。Media information atom中存放有關軌道媒體資料的處理器特定資訊，媒體處理器使用這個資訊來對映媒體時間與資料。

視訊媒體資訊 atoms(Video media information atoms)是視訊媒體的最高層atom，這些atom包含其他用來說明視訊媒體資料特性的atom。在track atom中還有另外四種很重要的atom的種類，以下分別爲(1)Edit list atom：此atom類型爲”elst”，內部存放能明確相對應的Track出現時間以及內部每個Sample時間間隔的資料結構，使得MP4檔案內影像藉由讀寫這些edit list就可以達到播放Sample的功能。(2)Handler reference atom：此atom的類型爲”hdlr”，定義了要播放Media data的重要資訊，如Media data type等等所需的不同資訊。(3)Data reference atom：此atom的類型爲”dref”，提供了如何對此Track的Media data 作存取；以及指出Media data是否在和目前的MP4檔案同一個檔案中或者在其他檔案。(4)Sample table atom：此atom的類型爲”stbl”提供有關每個Sample詳細的資訊，Sample table是由一群atom所組成，而這些atom是以查表的型態呈現，定義了每個Sample實體位置資訊，以及時間資訊，藉由把時間資訊轉成Sample的號碼，再轉成Sample的位置可查出每個Sample位在Track中的位址。

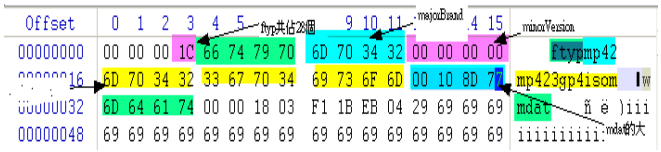
而Sample table atom內部又包含六種具重要鑑識價值的atom，分別爲(1)Sample description atom：此atom的類型爲”stsd”，內部含有Sample Description Table，其擁有的table會根據Media data類型的不同而有所不同；對於Media track而言，其含有MPEG-4 ESDs(Elementary Stream Descriptions)。而對於Hint track來說，其含有通訊協定的名稱與控制參數。(2)Time-to-sample atom：此atom的類型爲”stts”，其內部存著每筆Sample的Duration資訊，藉由此atom的資料可以查出各個Sample的顯示時間爲何。(3)Sync sample atom：此atom的類型爲”stss”，此atom定義了Media data中的key Picture，在此key Picture的定義爲沒有經過動態預測/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)Sample-to-chunk atom：此atom的類型爲”stsc”，內部存著Chunk的資訊，讓使用者可以藉由查表得知各個Sample位於那一個Chunk以及Chunk中的那個位置。Sample-to-chunk table的結構。(5)Sample size atom：此atom的類型爲”stsz”，其內容記載了各個Sample的大小，其中size欄位爲32-bit的整數，如果只有一種大小的Sample，則此atom的size欄位只有一個，如果有多種大小的Sample，則此欄位以向量形式呈現。(6)Chunk offset atom：此atom的類型爲”stco”，此atom內容記載了從MP4檔案開頭到每個Chunk的offset值，單位以bytes爲單位，可以32-bit或64-bit數字來表示。

MPEG-4視訊使用’MP4v’的資料格式，並使用所謂的基本流媒體描述符(‘esds’) atom來增強媒體樣本的描述，以補標準視訊樣本描述的不足， MPEG-4 Elementary Stream Descriptor Atom ('esds')所包含的atom皆完整定義於MPEG-4規格(ISO/IEC FDIS 14496-1)

中，此atom最重要的且具鑑識價值的欄位就是「decConfigDescr」描述符下層「decSpecificInfo」描述符中「info」欄位值，該值就是提供MPEG-4流媒體的特定資訊，該資訊亦是提供MPEG-4解碼的重要資訊，ESD(Elementary Descriptor)。

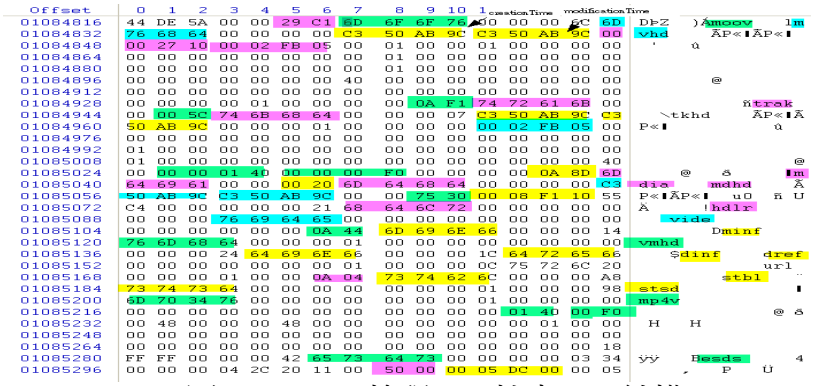
3.2 MP4/3GP ATOM元資料解讀範例

以下使用Nokia E51手機之02112007.MP4檔說明MPEG-4流媒體所內嵌之atom資料該如何解讀，如圖4.10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：



圖六:以WinHex檢視MP4 檔頭資訊

圖六位址3存放的2個字元組爲‘0x1C’，換算爲十進位表示爲”28”，亦即表示ftype atom起始位置爲0在位址28結束，位址4-7表示ftyp atom 識別字，位址8-11表示majorBrand，在此爲「MP42」，位址12-15表示minorVersion，在此值爲「0」，位址16-27表示compatibleBrands，在此爲「MP423GP4isom」，位址28-31表示mdat atom(media data container)的大小，在此換算爲十進位的值爲「1084783」。



圖七:WinHex檢視MP4檔案atom結構

圖七位址1084821開始的二個位元組存放的值爲「29C1」(10681_{10})，表示moov atom(container for all the meta-data)的大小，起始位置爲1084819_{10}，結束位置爲1095508_{10}。位址1084830所存放的值「6C」表示mvhd atom(movie header)的大小；位址1084839-1084842表示建立時間(creationTime)，值爲「3276843932_{10}，Fri Nov 02 18:25:32 2007 UTC」1084843-1084846表示修改時間(modificationTime)，值爲「3276843932_{10}，Fri Nov 02 18:25:32 2007 UTC」；位址1084847-1084850表示timescale，在此值爲「2710」(10000_{10})；位址1084851-1084854表示duration，在此值爲「02FB05」(195333_{10})。

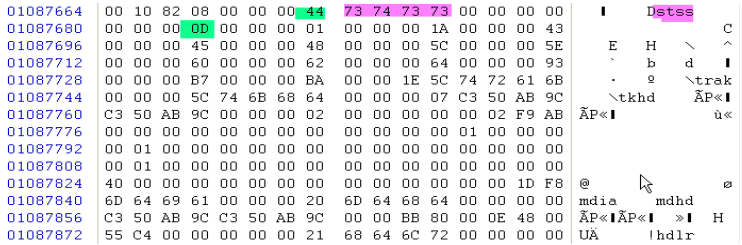
位址1084937開始的二個位元組存放的值爲「0AF1」(2793_{10})，表示trak atom(container for an individual track or stream)的大小；位址1084946存放的值爲「005C」(84_{10})，表示tkhd atom(track header)的大小，位址1084955 -1084958表示建立時間(creationTime)，值爲「3276843932_{10}，Fri Nov 02 18:25:32 2007 UTC」1084959 -1084962表示修改時間

(modificationTime)，值爲「3276843932_{10}，Fri Nov 02 18:25:32 2007 UTC」；位址1084971-1084974表示duration，在此值爲「02FB05」(195333_{10})；位址1085025-1085028表示寬度，在此爲「0140」(320_{10})，位址1085029-1085032表示高度，在此爲「00F0」(240_{10})。

位址1085037開始的二個位元組存放的值爲「0A8D」(2693_{10})，表示mdia atom(container for media information in a trak)的大小；位址1085046所存放的值「20」表示mdhd atom(media header)的大小；位址1085055-1085058表示建立時間(creationTime)，值爲「3276843932_{10}，Fri Nov 02 18:25:32 2007 UTC」1085059-1085062表示修改時間(modificationTime)，值爲「3276843932_{10}，Fri Nov 02 18:25:32 2007 UTC」；位址1085063-1085066表示timescale，在此值爲「7530」(30000_{10})；位址1085067-1085070表示duration，在此值爲「0008F110」(586000_{10})。

位址1085078所存放的值「21」表示hdlr atom(handler type)的大小；位址1085063-1085066表示handlerType，在此顯示爲「vide」；位址1085110開始的二個位元組存放的值爲「0A44」(2620_{10})，表示minf atom(media information container)的大小；位址1085119所存放的值「14」表示vmhd atom(video media header)的大小；位址1085139所存放的值「24」表示dinf atom(data information box)的大小；位址1085147所存放的值「1C」表示dref atom(data reference atom)的大小

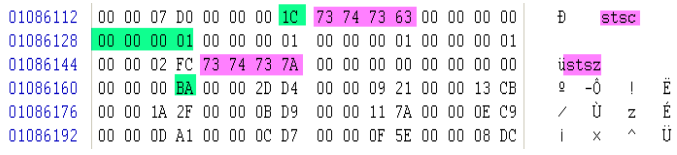
位址1085174開始的二個位元組存放的值爲「0A44」(2556_{10})，表示stbl atom(sample table atom)的大小；位址1085183所存放的值「A8」表示stsd atom(sample descriptions)的大小；位址1085199所存放的值「98」表示MP4v atom(visual sample description) 的大小；位址1085228-1085229表示寬度，在此爲「0140」(320_{10})，位址1085230-1085231表示高度，在此爲「00F0」(240_{10})；位址1085285所存放的值「42」表示esds atom(elementary stream description)的大小。



01087664	00 10 82 08 00 00 00 44	73 74 73 73 00 00 00 00
01087680	00 00 00 0D 00 00 00 01	00 00 00 1A 00 00 00 43
01087696	00 00 00 45 00 00 00 48	00 00 00 5C 00 00 00 5E
01087712	00 00 00 60 00 00 00 62	00 00 00 64 00 00 00 93
01087728	00 00 00 B7 00 00 00 BA	00 00 1E 5C 74 72 61 6B
01087744	00 00 00 5C 74 6B 68 64	00 00 00 07 C3 50 AB 9C
01087760	C3 50 AB 9C 00 00 00 02	00 00 00 00 00 02 F9 AB
01087776	00 00 00 00 00 00 00 00	00 00 00 00 01 00 00 00
01087792	00 01 00 00 00 00 00 00	00 00 00 00 00 00 00 00
01087808	00 01 00 00 00 00 00 00	00 00 00 00 00 00 00 00
01087824	40 00 00 00 00 00 00 00	00 00 00 00 00 00 1D F8
01087840	6D 64 69 61 00 00 00 20	6D 64 68 64 00 00 00 00
01087856	C3 50 AB 9C C3 50 AB 9C	00 00 BB 80 00 0E 48 00
01087872	55 C4 00 00 00 00 00 21	68 64 6C 72 00 00 00 00

圖八: 以WhinHex檢視stts atom結構

圖八位址1085315所存放的值「1D」(29_{10})表示decSpecificInfo descriptor的大小，該描述符下的info欄位值以十六進位表示爲「000001B002000001B50ECF0000010000000001200086C5D4C285020F0A31」。位址1085350開始的二個位元組存放的值爲「0300」(760_{10})，表示stts atom(time-to-sample)的大小；位址1085363所存放的值「5E」(94_{10})表示entryCount的大小。

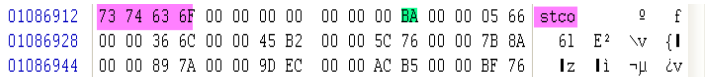


01086112	00 00 07 D0 00 00 00 1C	73 74 73 63 00 00 00 00
01086128	00 00 00 01 00 00 00 01	00 00 00 01 00 00 00 01
01086144	00 00 02 FC 73 74 73 7A	00 00 00 00 00 00 00 00
01086160	00 00 00 BA 00 00 2D D4	00 00 09 21 00 00 13 CB
01086176	00 00 1A 2F 00 00 0B D9	00 00 11 7A 00 00 0E C9
01086192	00 00 0D A1 00 00 0C D7	00 00 0F 5E 00 00 08 DC

圖九: 以WinHex檢視 stsc atom結構

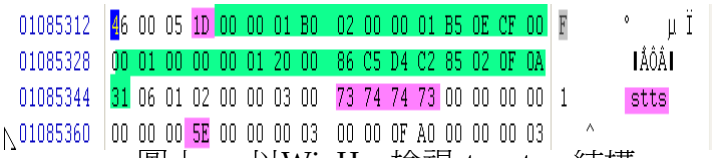
圖九位址1086119所存放的值「1C」表示stsc atom(sample-to-chunk)的大小；位址1086128-1086131所存放的值爲「1」，表示entryCount爲1。位址1086146開始的二個位元組存放的值爲「02FC」(756_{10})，表示stsz atom(sample sizes)的大小；位址1086163所存放的值「BA」(186_{10})表示sampleCount的大小。

圖十位址1086910開始的二個位元組存放的值爲「02F8」(760_{10})，表示stco atom(chunk offset)的大小；位址1086163所存放的值「BA」(186_{10})表示entryCount的大小。



圖十: 以WinHex檢視 stco atom結構

圖十一位址1087671開始的二個位元組存放的值爲「0044」(68_{10})，表示stss atom(sync (key， I-Picture) sample map)的大小；位址1087683所存放的值「0D」(13_{10})表示entryCount的大小。



圖十一: 以WinHex檢視stss atom結構

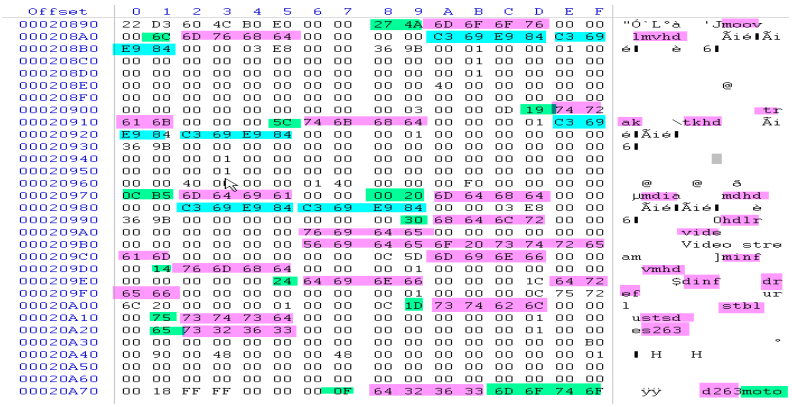
以下使用Motorola U9手機之moto1.3GP檔說明3GP(H.263)流媒體所內嵌之atom資料該如何解讀，如圖4.16所示，由檔頭部分開始解譯，這些位元組所代表的意義解釋如下：

圖十二: 3GP檔頭階層結構

圖十二位址3存放的2個字元組爲‘0x14’，換算爲十進位表示爲”20”，亦即表示ftype atom起始位置爲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，在此爲「3GP4」，位址12-15表示minorVersion，在此值爲「0」，位址16-27表示compatibleBrands，在此爲「3GP4」，位址28-31表示mdat atom(media data container)的大小，在此換算爲十進位的值爲「133242」。

圖十三位址20898開始的二個位元組存放的值爲「274A」(10050_{10})，表示moov atom(container for all the meta-data)的大小，起始位置爲133270_{10}，結束位置爲143328_{10}。位址208A1所存放的值「6C」表示mvhd atom(movie header)的大小；位址208AA-208AD表示建立時間(creationTime)，值爲「3278498180_{10}，Wed Nov 21 21:56:20 2007 UTC」208A1-208B1表示修改時間(modificationTime)，值爲「3278498180_{10}，Wed Nov 21 21:56:20

2007 UTC」;位址208B4-208B5表示timescale,在此值爲「03E8」(1000_{10});位址208B8-208B9表示duration，在此值爲「369B」(13979_{10})。



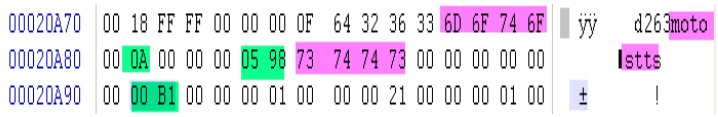
圖十三: 3GP moov atom階層結構

位址2090C開始的二個位元組存放的值爲「0D19」(3345_{10})，表示trak atom(container for an individual track or stream)的大小；位址20915存放的值爲「5C」(84_{10})，表示tkhd atom(track header)的大小，位址2091E-20921表示建立時間(creationTime)，值爲「3278498180_{10}，Wed Nov 21 21:56:20 2007 UTC」位址20922-20925表示修改時間(modificationTime)，值爲「3278498180_{10}，Wed Nov 21 21:56:20 2007 UTC」；位址20930開始的二個位元組表示duration，在此值爲「369B」(13979_{10})；位址20964-20967表示寬度，在此爲「0140」(320_{10})，位址20968-2096B表示高度，在此爲「00F0」(240_{10})。

位址20970開始的二個位元組存放的值爲「0CB5」(3245_{10})，表示mdia atom(container for media information in a trak)的大小；位址20979所存放的值「20」表示mdhd atom(media header)的大小；位址20982-20985表示建立時間(creationTime)，值爲「3278498180_{10}，Wed Nov 21 21:56:20 2007 UTC」位址20986-20989表示修改時間(modificationTime)，值爲「3278498180_{10}，Wed Nov 21 21:56:20 2007 UTC」；位址2098C-2098D表示timescale，在此值爲「03E8」(1000_{10})；位址20990-20991表示duration，在此值爲「369B」(13979_{10})。

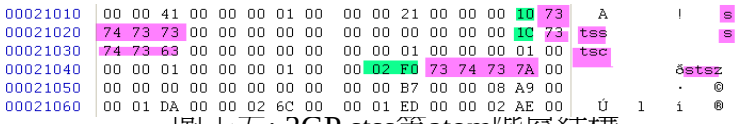
位址20999所存放的值「30」表示hdlr atom(handler type)的大小；位址209A6-209A9表示handlerType，在此顯示爲「vide」，位址209B6-209C1表示handler name，在此值顯示爲「Video stream」；位址209C8開始的二個位元組存放的值爲「0C5D」(3157_{10})，表示minf atom(media information container)的大小；位址209D1所存放的值「14」表示vmhd atom(video media header)的大小；位址209E5所存放的值「24」表示dinf atom(data information box)的大小；位址209ED所存放的值「1C」表示dref atom(data reference atom)的大小

位址20A08開始的二個位元組存放的值爲「0C1D」(3093_{10})，表示stbl atom(sample table atom)的大小；位址20A12所存放的值「75」表示stsd atom(sample descriptions)的大小；位址20A21所存放的值「65」表示s263 atom(H263 sample description)的大小；位址20A3E-20A3F表示寬度，在此爲「00B0」(176_{10})，位址20A40-20A41表示高度，在此爲「0090」(144_{10})；位址20A77所存放的值「0F」表示d263 atom(decoder specific info H263 video)的大小。



圖十四: 3GP d263及stts atom結構

圖十四位址20A7C-20A7F表示vendor，在此顯示爲「moto」(1836020847_{10})，位址20A81表示h263Level，在此顯示爲「0A」(10_{10})。位址20A85開始的二個位元組存放的值爲「0598」(1424_{10})，表示stts atom(time-to-sample)的大小；位址20A92所存放的值「B1」(177_{10})表示entryCount的大小。



圖十五: 3GP stss等atom階層結構

圖十五位址2101E存放的值爲「10」(16_{10})，表示stss atom(sync (key， I-Picture) sample map)的大小；位址21027-2102A所存放的值「00000000」表示entryCount的大小爲0；位址2102E所存放的值「1C」表示stsc atom(sample-to-chunk)的大小；位址2103A所存放的值爲「01」，表示entryCount爲1；位址21049開始的二個位元組存放的值爲「02F0」(752_{10})，表示stsz atom(sample sizes)的大小；位址2105A所存放的值「B7」(183_{10})表示sampleCount的大小。

表一: 3GP/MP4視訊編輯/轉換軟體表

軟體分類	軟體名稱	編輯/轉檔功能	具鑑識價值之輸出視訊檔案格式
提供視訊檔案編輯及轉檔功能	Aimersoft Video Editor等3種	編輯及轉檔	3GP,MP4、3G2,特定手持式行動機型3GP
提供合併視訊檔案與轉檔功能	AVS Video Editor 4.1等3種	合併與轉檔	3GP,MP4
提供轉檔功能	FREE 3GP VIDEO CONVETER、等36種	轉檔	3GP,3G2,MP4,Mortola,Nokia,Samsung,SonyEricsson

3.3 視訊編輯轉換軟體的分類與鑑識價值

目前在網路上有許多免費或商用的3GP/MP4多媒體視訊編輯及轉換工具軟體可供下載試用，這些軟體可讓使用者對所拍攝的3GP/MP4視訊檔案進行視訊內容編輯與轉檔作業。這些視訊檔案編輯或轉檔工具軟體各種作業系統平台都有提供，本研究僅針對微軟

Windows作業系統平台上的軟體進行相關實驗；以多媒體視訊檔案內容僞變造鑑識的觀點來看的話，這些視訊編輯與轉檔工具軟體可提供有心人士用來規避多媒體視訊影片檔案來源鑑別鑑識的一種反鑑識工具，爲了使數位鑑識人員對這些軟體有更多瞭解，本研究特列出45種市面上常見之3GP/MP4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、支援之功能與具鑑識價值之輸出多媒體視訊檔案格式等資訊，依視訊檔案編輯與轉檔的處理功能可概分爲3大類，第1類爲提供視訊檔案編輯及轉檔功能，如Aimersoft Video Editor軟體，第2類爲提供合併視訊檔案與轉檔功能，如Apecsoft AVI 3GP Joiner等軟體，第3類爲僅提供轉檔功能，如4U MP4 VIDEO CONVERTER等軟體。這些編輯或轉檔工具軟體大部分都接受各種視訊或影像檔案格式，僅少部分只能接受3GP/MP4之視訊檔案格式，其他種多媒體視訊檔案格式則無法匯入使用。

四、多媒體視訊檔內容僞變鑑識流程與方法

本研究使用之數位相片來源，選定爲由行動電話(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作爲實驗觀察之標的，每種行動數位裝置機種都取得三筆以上3GP/MP4多媒體視訊檔以做爲檢驗標的之基準樣本。另將上述每台機種之多媒體視訊檔複製多份，以供檢驗不同之3GP/MP4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。

有關鑑識3GP/MP4多媒體視訊影片檔有無遭內容竄改或鑑別是否係原件之鑑驗方法可概分爲以下9個步驟：

步驟1：取得3GP/MP4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：針對欲鑑驗之行動數位裝置機型，儘可能取得相關規格資料，以供比對相關ATOM元資料資訊。

步驟3：取得上述行動數位裝置所拍攝之3GP/MP4多媒體視訊影片檔案樣本，以此作爲判讀之基準多媒體視訊影片檔，並複製多份，作爲實驗修改對照組樣本。

步驟4：使用WinHex等鑑識軟體判讀及鑑驗基準3GP/MP4多媒體視訊影片檔中之esds atom、d263 atom、建立時間及修改時間 atom、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，以確認相關鑑驗資訊，esds atom及d263 atom資訊另以MD5演算法計算，並匯入行動數位裝置3GP/MP4多媒體視訊檔實驗資料表中已供比對。

步驟5：依序啓動45種3GP/MP4視訊編輯或轉檔工具軟體，並以實驗修改對照組數位影像樣本做爲編輯之標的，更改對照組中3GP/MP4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。

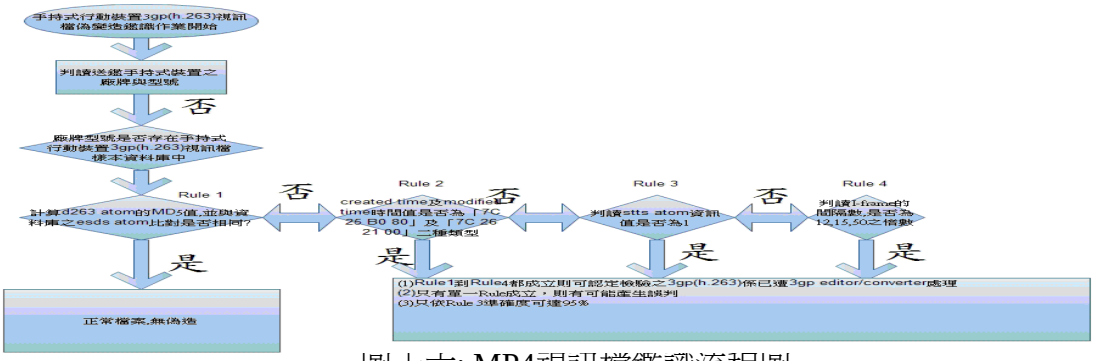
步驟6：使用WinHex等鑑識軟體判讀及鑑驗實驗修改對照組3GP/MP4多媒體視訊影片檔樣本與步驟4檢驗之相同資料，esds atom及d263 atom等資訊另以MD5演算法計算。

步驟7：將步驟6產生之esds atom及d263 atom MD5訊息摘要值與步驟4產生之行動數位裝置JPEG影像資料表進行比對，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、d263 atom及時間等。

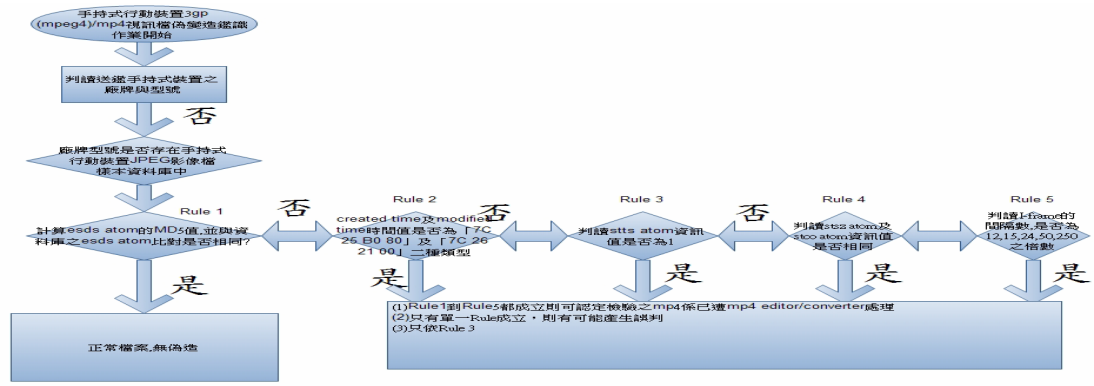
步驟9：針對實驗結果進行軟體特徵比對及分類，歸納出所有鑑驗之3GP/MP4多媒體視訊編輯或轉檔工具軟體之特性。

MP4多媒體視訊檔內容僞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，並與已建立之MP4多媒體視訊檔樣本實驗資料庫記錄比對，接下來檢查有無流程圖上所列出之5項比較規則，以做爲判定MP4多媒體視訊檔內容有無僞變之鑑別依據。



圖十六: MP4視訊檔鑑識流程圖

3GP多媒體視訊檔內容僞變造偵測流程如圖十七所示，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，以做爲判定3GP多媒體視訊檔內容有無僞變之鑑別依據。



圖十七:3GP多媒體視訊檔鑑識流程圖

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) sample map) atom、stsc sample-to-chunk， partial data-offset information atom、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 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。在此依實驗需求共建立二種樣本資料表，分別爲3GP視訊檔 d263 atom樣本資料表、MP4視訊檔esds atom樣本資料表。

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數據，以做爲送鑑3GP/MP4視訊檔來源判讀是否爲可信賴及正確。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出現之位置是否爲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；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多媒體視訊編輯或轉檔軟體對3GP/MP4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，發現共有六項可供辨識之特徵項目，不同軟體所符合之特徵項目均有所不同，但統計數字愈高者，表示僞變結果容易以本論文所開發之簡易鑑識工具偵測，統計數字愈低者，表示可供識別之特徵項目極少，僞變內容不易偵測；實驗結果顯示統計數字在5以上者計有4U MP4 VIDEO CONVERTER等22種，統計數字在4者計有Aimersoft Video Editor 等11種，統計數字在4者計有Agogo Video to ipod/cellphone/MP4等6種，其他爲數字總計爲2以下。特徵一項目正確率最高，高達100%，原因在於由軟體所編修及轉檔過後之視訊檔Tkhd atom之created time及modified time有無變化，結果發現共有29種3GP/MP4編輯或轉換軟體會使所編修之視訊檔所內嵌Tkhd atom之created time及modified time之欄位值會取代原來視訊檔之時間值，但以此特徵項並無法個化到特定之單一軟體。

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所示。

五、結論與未來研究方向

本研究提出如何由觀察及檢驗行動裝置中之3GP/MP4視訊影像檔案所內嵌之atoms元資料，來判讀3GP/MP4多媒體視訊檔是否遭3GP/MP4編輯及轉換等具反鑑識功能軟體剪接編輯、切割、合併、轉檔等僞變處理，藉由atoms元資料檢視輔助工具的協助，提供鑑識人員可能需注意此類具反鑑識功能之3GP/MP4視訊編輯或轉換軟體之特徵，由3GP/MP4視訊檔所內嵌之mdhd atom之creationTime及ModificationTime值是否改變、stts的值是否固定爲1、esds atom decspecificinfo值是否與原機型有所不同、視訊檔中之I-PICTURE(frame)由隨機出現的狀態改變爲出現規律之間隔性、I-picture quantizer及

P-picture quantizer量化係數的改變等特徵項目之變化，可鑑別3GP/MP4視訊檔是否遭偽變。

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爲比對之方法錯誤率低，正確率高，但是僅止於可用於確認檔案來源是否爲原件，至於能否找出視訊檔中剪輯或合成畫面的部分，本研究目前的方法仍無法判讀，此部分的研究亦可成爲日後之研究方向。

表二:MP4編輯或轉換軟體鑑驗之特徵項

軟體名稱 / 可供參考特徵	4U MP4 VIDEO CONVERTER	ABC 3GP/MP4 Converter	ACALA 3GP movies FREE
Tkhd atom 之 created time 及 modified time有無變化	YES	YES	YES
Stts atom entry count值是否爲1	YES	YES	YES
stsz 與stco atom之entry count 值是否相等	YES	YES	YES
I-Picture出現之位置是否爲12等數值之倍數	YES(12的倍數)	YES(12 的 倍數)	YES(12的倍數)
3GP/MP4 Esds atom decspecificinfo text值	Lavc51.25.0	Lavc51.57.0	
3GP d263 vendor atom		FFMP	FFMP
可供參考特徵總計	5	5	5

六、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 NAND Flash 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.