Vancouver Police Department

Forensic Video Audit

Simon Demers, Audit Manager

Vancouver Police Department

June 2009

Vancouver Police Department
312 Main Street
Vancouver, British Columbia
V6A 2T2

PR2009-1002 Forensic Video Audit
June 2009

8hr94jq589h048fqd67h85

Table of Contents

1 Executive Summary

1.1 The Audit Unit conducted a Forensic Video Audit. The review was initiated by the Audit Unit in March 2009 and was endorsed by the Inspector in charge of the Emergency & Operational Planning Section (EOPS). The primary objective of the audit was to confirm that forensic video evidence is collected, processed and analyzed in a timely manner and in accordance with all applicable policies, procedures and standards.

1.2 The following table summarizes the main findings and recommendations of the Audit Unit.

Table 1-1 Main Findings and Recommendations

Observations	Recommendations
FINDING 1: The forensic video analysis process appears to be consistent with most of the best operating practices documented in the literature.	RECOMMENDATION 1: Update the Forensic Video SOP manual.
FINDING 2: Several video exhibits are never analyzed or are not analyzed in a timely manner.	RECOMMENDATION 2: Create a two-tier forensic video analysis stream.
FINDING 3: Several processed video exhibits are never picked up or are not picked up in a timely manner by investigators.	RECOMMENDATION 3: Manage video submissions using the Versadex Workflow environment.
FINDING 4: Video exhibits are not stored in an optimal environment.	RECOMMENDATION 4: Improve the storage conditions of video exhibits.

1.3 The Audit Unit is confident that the implementation of these recommendations would strengthen forensic video analysis at the VPD.

2 Introduction

2.1 The Audit Unit conducted a Forensic Video Audit. The audit was initiated in March 2009 and was endorsed by the Inspector in charge of the Emergency & Operational Planning Section (EOPS).

2.2 The primary objective of the audit was to confirm that forensic video evidence is collected, processed and analyzed in a timely manner and in accordance with all applicable policies, procedures and standards.

2.3 The Audit Unit would like to thank all the audit stakeholders for their assistance. The assistance of the Forensic Video Unit was particularly valuable. The contribution of the practicum student Darlene Lau is also gratefully acknowledged.

3 Audit Scope and Methodology

3.1 The Audit Unit assembled a large volume of background documentation from the forensic video literature. Using this documentation, the Audit Unit compiled a list of best operating practices and compared the forensic video analysis process with these best practices.

3.2 The Audit Unit reviewed the submission, intake, analysis and archival processes associated with video exhibits with an emphasis on management controls, quality assurance and risk management.

3.3 The Audit Manager interviewed the Forensic Video Officer and visited the Forensic Video Unit's work and storage areas.

3.4 The Forensic Video Officer provided a copy of the Forensic Video Standard Operating Procedures (SOP) manual and a copy of the Forensic Video database. The Forensic Video Unit also compiled the list of processed video exhibits that had not been picked up as of May 2009.

4 Audit Background

4.1 With the proliferation of commercial video surveillance and personal video recording tools, many people and events are increasingly likely to be captured on video. Surveillance cameras and closed circuit television (CCTV) systems can be found in and around airports, banks, automated teller machines (ATMs), convenience stores, gas stations, schools, hospitals, government buildings, office buildings, apartment buildings, shopping malls, parking lots, public roadways, public transit, taxicabs as well as various other private and public, indoor and outdoor locations. Most new cell phones come equipped with video recording capabilities.

4.2 The prevalence of video surveillance and other video recording tools provides substantial investigative opportunities for police.

Video Evidence

4.3 In the context of a criminal investigation, video evidence typically consists of visual facts about a crime or an individual that have been recorded on video and stored on a magnetic medium (e.g. VHS tape) or an electronic device (e.g. hard drive).

4.4 At trial, video evidence can be presented in court on television sets or computer monitors. Still images can be either printed as hardcopy or presented on computer monitors. Slideshow presentations and/or expert reports can also be used to present the forensic video analysis results.

INVESTIGATIVE VALUE

4.1 Video evidence is a valuable component of many police investigations and prosecutions. In accordance with the RPM, seizing relevant video evidence is a key investigative strategy [redacted]

S.15

S.15

S.15

S.15, S.15

S.15
---------- ----------

4.2 As stated in the 2002 Major Case Management Manual by the Canadian Police College, the swift identification of a suspect or witness through video can make an important difference in all criminal investigations. Several very high-profile investigations have relied on video evidence, including the 1994 Stanley Cup riot, the 1995 Oklahoma City bombing, the 2001 terrorist attacks in the United States, and the 2005 London bombings. It is now routine for investigators to consider the possibility that the victim or the suspect may have been captured on video at the crime scene, nearby, or travelling to/from the scene. This is supported by the 2000 Homicide Investigation Checklist by the BC Ministry of Attorney General, the 2000 Murder Investigation Manual from the United Kingdom Association of Chief Police Officers (ACPO), the 2005 Hate Crime Good Practice and Tactical Guidance from ACPO, the 2007 Road Death Investigation Manual from ACPO and the 2007 Intelligence-Led Policing Practice Advice from ACPO.

4.3 Video evidence can be very compelling. Video evidence can provide reliable information about the location of the incident, the subjects involved (e.g. suspect, victim, witness), the travel path and actions of the subjects involved, the vehicles involved, the timeline of events, the weapon used, the physical layout of the scene, etc. Video evidence can be used to decisively confirm or refute alibis, eliminate or identify suspects and identify forensic opportunities that would otherwise remain hidden. Video evidence can uncover illicit activities that would otherwise remain concealed (e.g. Bakker investigation, child pornography, home video showing criminal act or criminal activity) or information that would not be available otherwise (e.g. Bernardo investigation, terrorist before the explosion, robber before he enters the bank). According to the 2004 Handbook on Criminal Harassment produced by the Department of Justice Canada, investigators in criminal harassment cases should consider searching for video or audio tapes that might contain surveillance footage or other information recorded by the stalker himself.

S.15

4.4 Video evidence is a very desirable type of forensic evidence because it can be more easily scrutinized by the court and is typically more objective than witness statements. Video evidence cannot be prejudiced or intimidated. Like other physical forensic evidence, video evidence can be weighed by the court according to objective scientific criteria.

LEGAL FOUNDATIONS

4.5 Seminal legal decisions in Canada related to the use of forensic video evidence include R. v. Nikolovski (1996) and HMTQ v. Cooper (2000). The legal tests usually applied to expert testimony by forensic video analysts are described in R. v. Mohan (1994).

4.6 In R. v. Mohan (1994), the Supreme Court of Canada ruled that opinion evidence is admissible in criminal proceedings only when it is relevant, necessary to allow the judge or jury to appreciate all the facts of the case (e.g. probative value outweighs prejudicial effect), not subject to any exclusionary rule, and presented by a properly qualified expert.

4.7 In R. v. Nikolovski (1996), the Supreme Court of Canada ruled that a video exhibit depicting the scene of a crime can be admissible as evidence as long as it is not altered or changed. It also established that video evidence can and should speak for itself, with no need for independent corroborating evidence or witness testimony (i.e. silent witness).

4.8 In HMTQ v. Cooper (2000), the BC Supreme Court held that video analysis and enhancement processes such as digitization or contrast adjustment do not amount to changing, altering or tampering the video. This was later reiterated by the BC Court of Appeal in R. v. Gill (2004) and a *voir dire* decision for R. v. Pasqua (2008).

4.9 Fundamentally, a video exhibit is more likely to be admitted as evidence when the Crown can demonstrate it is the best evidence available and fairly and accurately displays the events it claims to represent.

Forensic Video Analysis

4.10 Unfortunately, video evidence is often produced by and acquired from privately-operated recording systems. The overall quality of the evidence is therefore largely outside the control of the police. Video recordings obtained by law enforcement consist primarily of digital surveillance video or analog security tapes which are often multiplexed, interlaced, time-lapsed, recorded in a proprietary format, compressed using lossy compression algorithms, compatible only with specific platforms, improperly time-coded, and/or of relatively poor quality. In many cases, very specialized forensic video analysis is required before a video exhibit or video footage can be used as part of a police investigation or in a court setting.

4.11 Forensic video analysis is the scientific examination, comparison, and evaluation of video evidence in legal matters. Forensic video is officially recognized by the International Association for Identification (IAI) as a sub-specialty within the scientific discipline of forensic imaging.

4.12 Forensic video analysis can be used to recover previously recorded material, duplicate video recordings, enhance recordings, and authenticate recordings. The primary objective of forensic video analysis is to provide to investigators and the court the best possible evidence and a product that accurately and fairly represents the visual content of the original evidence. In general, this is achieved by formatting information from the input image into details discernible to the human eye (e.g. restoring/enhancing/optimizing/analyzing the image).

4.13 The following table summarizes some of the techniques typically used by forensic video analysts and technicians.

Table 4-1 Common Forensic Video Techniques

Technique	Primary Goal	Basic Approach
Color Correction or Grading	Recover the colors of the original scene by compensating for varying filming conditions (e.g. poor lighting).	Calibrate video camera using a known standard and adjust color mode, brightness, contrast, luminance, saturation and hue.
Contrast Adjustment or Histogram Equalization	Intensify contrasts.	Change the color palette by equalizing the tonal distribution of the image.

Technique	Primary Goal	Basic Approach
De-Interlacing or Motion Compensation	Isolate and analyze separately each interlaced field (with only half the horizontal lines).*	Combine fields or interpolate missing lines to display full frames.*
De-Multiplexing	Isolate and analyze separately individual camera views (scenes) that have been recorded sequentially.	Reorder the frames by connecting the ones that appear to be similar in content.
Edge Enhancement or Sharpening	Enhance the apparent sharpness or definition of the video by creating crisp, high-contrast edges.	Identify sharp edge boundaries in the frame (e.g. contours between subject and background) and increase the image contrast in the area immediately around the edges.
Frame Averaging	Reduce noise and video graininess.	Average each individual pixel from multiple sequential frames.
Homomorphic Filtering	Highlight details obscured by shadows (e.g. licence plate in the dark).	Simultaneously normalize the brightness and increase contrast.
Image Segmentation	Locate or isolate elements and boundaries within the frame (e.g. face recognition, plate recognition).	Identify edge boundaries and label every pixel within the frame such that pixels with the same label share certain visual characteristics.
Image Stabilization or Tracking	Counteract the visible frame-to-frame jitter caused by subtle camera movements or the motion blur caused by high-speed movement.	Distract horizontal and vertical movement or track the target object by slightly shifting the image within each frame.
Image Subtraction or Differencing	Isolate patterns or isolate changes between two frames.	Capture lightfield (reference) image and subtract from the input image.
Inverse Filtering	Recover the original frame from a frame that has been enhanced, degraded or corrupted.	Reverse the transformation process applied to the degraded frame.
Masking or Blurring	Obscure an area to hide sensitive information (e.g. face, licence plate).	Apply a mosaic or blur on the relevant area within the frame.
Noise Reduction	See image or frame averaging.	See image or frame averaging.
Photogrammetric or Geometric Correction	Remove shading artifacts and distortions caused by the mapping of non-planar (e.g. 3D) geometric shapes into a two-dimensional frame.	Derive the required spatial transformation by analyzing known reference points.
Photogrammetric or Reverse Projection	Derive reliable geometric measurements from a frame (e.g. height, distance, speed).	Obtain reference measurements and use a calibrated measurement standard to extrapolate real-world measures.

* Interlaced video is divided into two sets of horizontal scanning lines (odd and even) that are displayed sequentially. Each set of lines is called a field. A frame consists of two interlaced fields, each containing half the image information. The playback and recording rate for National Television Standards Committee (NTSC) video is 29.97 frames or 59.94 fields per second.

4.14 Prior internal VPD studies have concluded that forensic video analysis can be extremely cost-effective because it represents an opportunity to quickly and decisively identify suspects and key witnesses, therefore shortening the investigation, freeing up traditional investigative resources, increasing the likelihood of a guilty plea, and reducing police and court costs.

Forensic Video Unit

4.15 At the VPD, forensic video analysis is conducted primarily by the Forensic Video Unit within the Emergency & Operational Planning Section (EOPS). The mandate of the Forensic Video Unit is to process video evidence for court purposes.

4.16 The Forensic Video Unit was officially created in 1998, after the investigation surrounding the 1994 Stanley Cup riot highlighted the value of and the need for forensic video analysis. One Forensic Video Officer was originally assigned to the Forensic Video Unit. A second sworn position was temporarily added in 1999 but was returned to the Forensic Identification Unit in 2000. Subsequent staffing adjustments have left the Forensic Video Unit with a total of one sworn Forensic Video Officer, two Forensic Video Analysts and one Forensic Video Administrative Assistant. The Forensic Video Officer acts as the Forensic Video Coordinator.

4.17 The following table summarizes the main staffing changes in the Forensic Video Unit since it was created in 1998.

Table 4-2 Staffing in the Forensic Video Unit

Date	Staffing Change	Business Rationale
1998	Creation of Forensic Video Unit using one existing sworn position	1994 Stanley Cup Riot
November 2002	New civilian Forensic Video Analyst position	2000 Workload Changes Report 2002 Police Sworn and Civilian Support Staffing Request
December 2005	New civilian Forensic Video Administrative Assistant position	2004 Staffing Report 2005 Review of the VPD's Staffing Requirements
April 2008	Additional civilian Forensic Video Analyst position	2007 Operational Review
TOTAL	**1 SWORN AND 3 CIVILIAN POSITIONS**	

4.18 Other major forensic video units include the RCMP Technical Operations Branch, the FBI Forensic Audio, Video, and Image Analysis Unit (FAVIAU) and the London Metropolitan Police Service Video, Audio and Imaging Laboratory.

Internal Policies and Processes

4.19 The RPM section 1.9.17 describes the policies and procedures for handling and processing video evidence. The RPM section 1.9.16 describes the appropriate procedures for handling taxicab camera evidence. Like other video evidence, taxicab camera evidence is normally processed and analysed by the Forensic Video Unit.

4.20 The Forensic Video Unit also actively maintains a Standard Operating Procedures (SOP) manual describing in detail various internal procedures and business processes.

Submission Process

4.21 In accordance with the RPM sections 1.9.16 and 1.9.17, officers who require the services of the Forensic Video Unit must place the video exhibit in a sealed envelope. The video exhibit and the related documentation must then be deposited in the Forensic

S. 15

4.22 Each exhibit must be accompanied by a completed VPD1322 Forensic Video Work Request Form and a Property Tag. The VPD1322 Forensic Video Work Request Form is used to capture information about the submitting officer, the incident being investigated and the video exhibit.

Intake Process

4.23 In accordance with the Forensic Video SOP manual, all forensic video analysis requests deposited in the Forensic Video drop box are collected twice daily by the Forensic Video Administrative Assistant and electronically logged into the Forensic Video database using the incident number from PRIME as the reference number.

4.24 The Forensic Video Administrative Assistant is responsible for sorting submissions in accordance with various prioritization criteria, including crime type and the purpose or nature of the request.

S. 15

4.25 The most serious cases like homicides, serious assaults and sexual assaults are usually handled by the sworn Forensic Video Officer, the most experienced Forensic Video Unit member. Routine cases are assigned to the civilian Forensic Video Analysts.

ANALYTICAL PROCESS

4.26 Digitized video files are normally stored on the Forensic Video server S. 15 or on a portable hard drive.

4.27 In accordance with the SOP manual, a Forensic Video Expert Report is used to document the work done and the methodology used. The Expert Report outlines the analytical process, the observations of the analyst and the conclusions of the analyst.

4.28 Once the video evidence has been analyzed, the Forensic Video Administrative Assistant is responsible for advising the investigator by email, placing the processed evidence in the Forensic Video pick-up bin and updating the database. The Forensic Video database is used to document who returned the video exhibit to whom and when. Each database record is then printed and archived in the Forensic Video log book.

4.29 The bottom section of the VPD1322 Forensic Video Work Request Form is used to summarize the analysis performed. The Forensic Video database, the Forensic Video Expert Report and the VPD1322 Forensic Video Work Request Form combine to form the audit trail.

S. 15

5 Findings

5.1 The findings of the Audit Unit are summarized below.

FINDING 1: The forensic video analysis process appears to be consistent with most of the best operating practices documented in the literature.

5.2 Based on the information obtained by the Audit Unit, the forensic video analysis process appears to be consistent with most of the best operating practices documented in the scientific literature and summarized in the appendix.

5.3 The RPM and the Forensic Video SOP manual both describe various record keeping standards, evidence handling procedures, examination procedures and archiving procedures (BEST PRACTICE 1). These procedures are designed to maintain the evidentiary value of video exhibits and avoid the accidental destruction or degradation of the video image (BEST PRACTICE 7). For example, officers investigating serious crimes (including homicides, robberies and sexual assaults) are warned that they should not attempt to rewind or view the video before seizing it. Immediately after seizing a video tape, officers are asked to remove the recording tab on the spine of the cassette (BEST PRACTICE 8) and document any date or time discrepancies (BEST PRACTICE 9). Requests for video analysis are triaged based on the seriousness of the offence and the potential value of the video evidence (BEST PRACTICE 3). All video evidence is also labelled and catalogued.

5.4 In accordance with the SOP manual, the following information is recorded in the Forensic Video database: summary of the analysis request, description of the work conducted by the analyst, description of the procedures and equipment used, summary of the incident, apparent defects or damages on the recording, findings and observations of the analyst and identity of the analyst who performed the work. This forms the audit trail (BEST PRACTICE 2).

5.5 The hardware and software used by the Forensic Video Unit as part of the examination process appear to meet the technical standards generally accepted by the

forensic video community (BEST PRACTICE 5). Avid Systems is the main equipment provider for the Forensic Video Unit.

5.6 The Forensic Video Officer confirmed that the aspect ratio of digital video recordings is calibrated in accordance with scientific standards and the SOP manual (BEST PRACTICE 12). Although hash verifications or checksum tests are not usually performed, other IT-based security measures are designed to protect the integrity of the digital video data (BEST PRACTICE 11).

FINDING 2: Many video exhibits are never analyzed or are not analyzed in a timely manner.

5.7 According to the Forensic Video database, the Forensic Video Unit would have received approximately 1,400 video exhibits in 2008. Up to 600 of these were still not processed or analyzed as of April 2009.

5.8 Most of the video exhibits waiting to be processed are associated with relatively minor property crimes like store thefts but a few relate to serious cases like store robberies and break & enters. Some of the seemingly more serious pending cases include a possible shooting 22(3)(b) ---------- and an impaired driving incident (VA2008-142333).

5.9 Overall, the criteria used by the Forensic Video Unit to prioritize video analysis requests appear to be reasonable. The Forensic Video Unit seems to be able to process and analyze video exhibits related to the most serious investigations but lower priority cases are almost unavoidably dropped. Dropped video exhibits may represent lost or overlooked investigative opportunities.

5.10 Public safety and the reputation of the VPD could be seriously jeopardized if significant forensic video evidence was missed or overlooked. The VPD could also face substantial civil liabilities.

22(3)(b)

FINDING 3: Several processed video exhibits are never picked up or are not picked up in a timely manner by investigators.

5.11 As of May 2009, almost 370 processed video exhibits were waiting to be picked up by an investigator. More than half of these have been waiting in the Forensic Video room since at least 2007, 81 have been waiting since 2008 and 76 were processed in the first quarter of 2009.

5.12 The normal practice within the Forensic Video Unit is to contact the investigator by email as soon as the video evidence is processed. According to the Forensic Video database, most investigators would have been contacted just after the video was processed and analyzed. In 56 cases, however, there is no database entry confirming that the investigator was contacted after the video evidence was processed.

5.13 The following table shows how many video exhibits were associated with each type of case. Exhibits processed after the first quarter of 2009 are excluded.

Table 5-1 Processed Video Exhibits Waiting to be Picked Up

S.15		
TOTAL	**351**	**368**

5.14 If processed video exhibits and evidence packages are not picked up and reviewed in a timely manner by investigators, there is a risk investigative opportunities could be lost or overlooked. As a result, suspects may not be charged even when there is sufficiently compelling video evidence to support a possible conviction.

S.15

FINDING 4: Video exhibits are not stored in an optimal environment.

5.15 Although critical video exhibits related to ongoing major cases are usually held in a secure office S.15 [redacted]

S. 15 [redacted]

S. 15 [redacted]

S. 15, S. 15 , S.15

6 Recommendations

6.1 The following recommendations are presented for consideration.

RECOMMENDATION 1: Update the Forensic Video SOP manual.

6.2 The Forensic Video SOP manual should be updated to include references to the following:

- Maintenance and calibration process or schedule for the video equipment and software (BEST PRACTICE 5).
- Quality management system involving technical inspections and administrative peer reviews (BEST PRACTICE 6).
- Disaster response procedures in case of fire or flood (BEST PRACTICE 10).
- Hash verification procedures for important digital video files (BEST PRACTICE 11).

6.3 This would make the Forensic Video SOP manual consistent with the best operating practices documented in the forensic video literature.

RECOMMENDATION 2: Create a two-tier forensic video analysis stream.

6.4 The Forensic Video Unit is currently the only unit within the VPD with the mandate to duplicate, review and analyze forensic video evidence. To reduce workload pressures on the Forensic Video Unit, a two-tier forensic video analysis stream should be implemented.

ANALYSIS STREAM

6.5 The objective of the secondary video analysis stream would be to leverage video evidence that is associated with less serious crimes but is also more readily available.

6.6 The secondary video analysis stream could contribute to reduce the backlog in the Forensic Video Unit and would provide a shorter average turnaround time by

concentrating on quick hits and low-hanging fruits such as store videos showing prolific shoplifters and/or suspected theft or break & enter suspects. However, compared to the Forensic Video Unit, the secondary video analysis stream would offer fewer analysis options and would not provide any expert opinion or positive identification through comparative analysis. When advanced analysis is required and the case appears significant enough, the Forensic Video Unit would take over the case.

VIDEO ANALYSIS UNIT

6.7 The second tier of the two-tier forensic video analysis stream could take the form of a secondary Video Analysis Unit.

6.8 The Video Analysis Unit would play a role similar to the Crime Scene Investigation Unit (compared to Forensic Identification Unit) and the Street Crime Enforcement Units (compared to Strike Force). The mandate of the new Unit would be to assist investigators by preparing video evidence so that they can view and use it in a user-friendly manner. The staff assigned to the Video Analysis Unit should benefit from the same specialized training provided to Forensic Video Analysts but would not normally use any advanced tools or complicated enhancement techniques and would only work with common video formats (e.g. VHS and some common digital formats).

6.9 Based on its mandate, the Video Analysis Unit could be located within the Operations Investigative Section. This would put the Video Analysis Unit closer (both physically and organizationally) to patrol operations and the General Investigation Unit, two important consumers of forensic video analysis services in terms of volume. If the Video Analysis Unit is not created as a standalone Unit with a separate supervisor, it could become a component (sub-unit) of the Crime Analysis Unit, General Investigation Unit or Crime Scene Investigation Unit. Alternatively, it could also become a component of the Forensic Video Unit.

RECOMMENDATION 3: Manage forensic video submissions using the Versadex Workflow environment.

6.10 The Forensic Video Unit should rely on the Versadex Workflow environment to manage analysis requests and video submissions.

6.11 The Versadex Workflow environment is a component of the PRIME Records Management System (RMS) that enables the automated and semi-automated movement of cases and follow-up assignments between officers and organizational units. Workflow is designed to give any employee the ability to electronically route cases or investigative assignments anywhere within the VPD. When new information is added to a case file or a follow-up assignment is completed, an update is immediately generated by Workflow to notify the people involved, ensuring that they are kept up to date as the case evolves. Work-to-do queues keep supervisors and staff informed of all the follow-up work they are directly responsible for. Workflow establishes accountability by making it possible for supervisors and managers to electronically track follow-up assignments from initial entry to final disposition.

6.12 When video evidence needs to be processed or analyzed, the investigator should electronically route the case to the Forensic Video Unit handle for notification purposes (e.g. with Notify status) and forward the physical video recording to the Forensic Video Unit in accordance with the RPM policy. The Forensic Video Coordinator should then be responsible to assign the appropriate follow-up request to a Forensic Video Analyst. When the analysis is complete, the Forensic Video Analyst would notify the Forensic Video Coordinator by concluding the follow-up request. When the processed evidence package becomes ready to be picked up, the Forensic Video Coordinator should notify the investigator by submitting a new follow-up request to the lead investigator, asking the investigator to pick up the processed evidence package. When the investigator picks up the evidence package, the follow-up request could be concluded.

6.13 Using Workflow to manage Forensic Video Unit follow-up assignments and analysis requests would reduce the risk that critical evidence or analysis will be overlooked, not performed in a timely manner or not performed to an acceptable

standard. As a by-product, the Workflow system could also generate statistical data useful for workload or staffing analysis and performance benchmarking.

RECOMMENDATION 4: Improve the storage conditions of video exhibits.

6.14 The storage room used to physically store and archive video exhibits should be upgraded or replaced in order to meet the standards recommended in the forensic video literature and prevent the loss of video evidence.

6.15 Analog tapes, digital tapes, CDs and DVDs should be locked in a clean, dry room or cabinet where temperature fluctuations and relative humidity are monitored and controlled (e.g. between 15°C and 25°C and relative humidity of 15% to 50%). The room should not contain combustible materials. Access to the room should be restricted, monitored and documented appropriately.

6.16 Exhibits should be protected in case of flooding, fire or earthquake. Cardboard sleeves, paper envelopes and cardboard boxes should be replaced with plastic storage compartments (or something similar). Storage media should be kept away from smoke, dust, strong magnetic fields, electrical hazards, intense light, intense heat, fluids and chemical products. Video tapes should be stored vertically in their individual case to minimize the warping effects of gravity. Because they are subject to degradation, digital files stored on short to medium term removable media (e.g. CDs, DVDs, digital tapes) should be transferred regularly to new media or to professionally managed data management archive systems.

6.17 These criteria would ensure that video exhibits remain securely stored (BEST PRACTICE 4).

7 Conclusion

7.1 Overall, the forensic video analysis process appears to be consistent with the best operating practices documented in the forensic video literature. Unfortunately, some investigative opportunities may be missed because several video exhibits are never analyzed, are not analyzed in a timely manner or are not picked up in a timely manner even after they have been analyzed by the Forensic Video Unit.

7.2 The Audit Unit is proposing the creation of a two-tier forensic video analysis stream. The objective would be to leverage video evidence that is associated with less serious crimes but is also more readily available (i.e. low-hanging fruits or quick hits).

7.3 To facilitate supervisory and managerial oversight, the Forensic Video Unit should manage analysis requests and video submissions using the Versadex Workflow environment. Among others, this would ensure that processed video exhibits and evidence packages are picked up and reviewed in a timely manner by investigators.

7.4 The following table summarizes the main findings and recommendations of the Audit Unit.

Table 7-1 Main Findings and Recommendations

Observations	Recommendations
FINDING 1: The forensic video analysis process appears to be consistent with most of the best operating practices documented in the literature.	RECOMMENDATION 1: Update the Forensic Video SOP manual.
FINDING 2: Several video exhibits are never analyzed or are not analyzed in a timely manner.	RECOMMENDATION 2: Create a two-tier forensic video analysis stream.
FINDING 3: Several processed video exhibits are never picked up or are not picked up in a timely manner by investigators.	RECOMMENDATION 3: Manage video submissions using the Versadex Workflow environment.
FINDING 4: Video exhibits are not stored in an optimal environment.	RECOMMENDATION 4: Improve the storage conditions of video exhibits.

7.5 The Audit Unit is confident that the implementation of these recommendations would strengthen forensic video analysis at the VPD.

8 Appendix – Forensic Video Best Practices

8.1 This section summarizes good operating practices or "best practices" documented in the forensic video analysis literature. These practices are generally accepted by field practitioners and industry representatives as good operating practices and are based on common sense, experience and testing.

8.2 The best practices in the following table apply to both analog and digital video evidence.

Table 8-1 Best Practices in the Field of Forensic Video Analysis

Best Practice	Summary
BEST PRACTICE 1: Maintain a Standard Operating Procedures (SOP) manual.	Policies and procedures should ensure the integrity of the video exhibits, before, during and after court proceedings.
BEST PRACTICE 2: Record an audit trail for each video exhibit.	An audit trail should be initiated at the earliest possible stage of the capture process to log information about the use or movement of the master evidence and any significant use, enhancement or distribution of working copies.
BEST PRACTICE 3: Triage new video analysis requests.	New video exhibits should be triaged and assessed to determine whether or not the request for analysis is reasonable. All video evidence should be labelled adequately and catalogued.
BEST PRACTICE 4: Store video exhibits in a secure location.	Video exhibits should be protected from physical damage or contamination and stored securely.
BEST PRACTICE 5: Use suitable equipment.	All equipment used for forensic video analysis should be properly calibrated, maintained in a fully operational condition and meet the standards generally accepted within the scientific community.
BEST PRACTICE 6: Implement a quality assurance program.	All forensic video analysis work should be subject to regular technical and administrative reviews as part of a quality assurance program.
BEST PRACTICE 7: Preserve the master evidence.	The master evidence or master copy should only be viewed to establish the integrity or authenticity of the evidence. All the analysis should be conducted using a working copy.
BEST PRACTICE 8: Protect video exhibits using write-protect mechanisms.	Video exhibits should be protected as soon as possible to prevent tampering and maintain evidential integrity.
BEST PRACTICE 9: Validate date and time information.	Video exhibits should be reviewed as soon as possible to confirm that time and date settings are correct. Any time and date inconsistencies should be documented in the audit trail and taken into account during the analysis.
BEST PRACTICE 10: Prepare a business continuity plan.	Disaster response procedures should be documented in a business continuity plan specific to the Forensic Video Unit. These procedures should include key information about the equipment room and storage facility and the disaster response procedures in case of fire or flood.

8.3 The following additional best practices apply specifically to digital video recordings.

Table 8-2 Best Practices for Digital Video Recordings

Best Practice	Summary
BEST PRACTICE 10: Confirm the integrity of digital video recordings.	Steps should be taken as early as possible to ensure that each digital video recording can be verified before it is presented as evidence in court.
BEST PRACTICE 11: Correct the aspect ratio of digital video recordings.	The aspect ratio of digital video recordings should be validated and corrected if necessary.

8.4 The following table lists the sources consulted to compile the best practices.

Table 8-3 Sources of Best Practices in the Field of Forensic Video Analysis

Organization	Publication
Association of Moving Image Archivists (AMIA)	Videotape Preservation Handbook
Federal Bureau of Investigation (FBI)	Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems
Home Office Scientific Development Branch	Digital Imaging Procedure
	Guidelines for the Handling of Video Tape
	Storage, Replay and Disposal of Digital Evidential Images
International Organization on Computer Evidence (IOCE)	International Principles for Computer Evidence
Law Enforcement and Emergency Services Video Association (LEVA)	Best Practices for the Acquisition of Digital Multimedia Evidence
	Guidelines for the Best Practice in the Forensic Analysis of Video Evidence
Scientific Working Group on Digital Evidence (SWGDE)	Best Practices for Forensic Audio
	Data Archiving
	Data Integrity Within Computer Forensics
	Proficiency Test Program Guidelines
	Proposed Standards for the Exchange of Digital Evidence
	Recommended Guidelines for Developing Standard Operating Procedures
	Recommended Guidelines for Developing a Quality Management System
	Recommended Guidelines for Validation Testing
Scientific Working Group on Imaging Technology (SWGIT)	Best Practices for Archiving Digital and Multimedia Evidence in the Criminal Justice System
	Best Practices for Documenting Image Enhancement
	Best Practices for Forensic Image Analysis
	Best Practices for Forensic Video Analysis
	Best Practices for Maintaining the Integrity of Digital Images and Digital Video

Organization	Publication
	Considerations for Managers Migrating to Digital Imaging Technology
	Digital Imaging Technology Issues for the Courts
Senior Managers Australian and New Zealand Forensic Laboratories (SMANZFL)	Australasian Guidelines for Digital Imaging Processes

8.5 Each suggested best practice is reviewed in more details below.

BEST PRACTICE 1: Maintain a Standard Operating Procedures (SOP) manual.

8.6 To ensure that forensic video analysis is approached in a methodical and structured manner, Standard Operating Procedures (SOPs) should be documented and implemented. SOPs are internal written documents outlining baseline requirements, general concepts, standards, principles, policies, procedures, methods, tasks, steps, instructions and processes expected to reinforce the quality of the analysis. SOPs are essential to the acceptance of forensic video analysis by the courts.

8.7 The SOPs should encourage consistency in the analytical process and help maintain the scientific rigour required by the forensic examination of video evidence. The SOPs should be compatible with generally accepted scientific principles and legal standards. They should also reflect the procedures generally accepted in the field of forensic video analysis.

8.8 The SOPs should include written policies and procedures designed to ensure the integrity of the video exhibits, before, during and after court proceedings. Such policies should include record keeping standards, evidence handling procedures, examination procedures, archiving procedures, disclosure policies and retention guidelines. Policies and procedures should describe the appropriate mechanisms for the disposal of images and video exhibits once the retention period has expired. Policies and procedures should detail the circumstances when the original recording or master evidence can be used and the process involved in the copying and distribution of working copies.

Policies and procedures must ensure that original recordings are not altered or erased. Submission guidelines should describe the appropriate format to report findings and analysis results. Findings reports should be written clearly in non-technical terms and copied on commonly accepted portable media.

8.9 The SOPs should be reviewed and updated periodically to ensure that they remain suitable and effective. Controversial techniques or procedures should be validated through an external peer review. Additional assurance and legal advice could be obtained through the Audit Unit, the Legal Advisor or prosecutors.

8.10 The SOPs should not discourage creativity and experimentation. Instead, they should be used to formalize, standardize and validate business and forensic processes. Forensic video analysts should still be able to exercise their professional judgement and discretion.

BEST PRACTICE 2: Record an audit trail.

8.11 An audit trail should be initiated at the earliest possible stage of the capture process (e.g. when the video becomes the possession of the police) to maintain the integrity of the video evidence.

8.12 Robust audit trails are required in order to safeguard or demonstrate the authenticity and integrity of the evidence. It is imperative that technicians and analysts be able to articulate what was done to recover the original recording and how the evidence before the court came to be. Audit trails can be used to show that the data is unaltered and provides an accurate representation of what it is supposed to show. The aim is to support the presentation of forensic video evidence through legal proceedings.

8.13 All key actions performed during the retrieval, processing and analysis stages should be documented or logged in the appropriate written case records or audit trail. The audit trail should describe the procedures followed, instruments used, tests performed and findings of each technician, analyst or support staff. The audit trail should be used to log all actions related to the master evidence and document

significant actions related to working copies that may be produced as evidence. This includes creating, storing, moving, accessing, viewing, copying, enhancing, exporting, distributing or destroying working copies. Any unused or unviewed material should be documented as part of the audit trail as well.

8.14 The level of detail provided in the audit trail would depend on the intended use for the evidence and the complexity of the analysis. All tasks should be documented in sufficient detail to allow a comparatively trained individual to retrace the steps and independently replicate or evaluate the results of the technician or analyst.

8.15 The following processes should be documented in a comprehensive audit trail: retrieval/seizure process, transfer process, image processing/enhancement process, disclosure process, retention/archival/disposal process. The audit trail should also include (or at least refer to) the relevant submission forms, maintenance logs, viewing logs, disclosure schedules and authentication reports. An auto-generated electronic audit trail can augment or replace the written audit trail but all records should be of a permanent nature and made available to the court when requested.

8.16 When the conclusions of the analyst are supported by a statistical test, the margin of error or level of precision should be reflected using the appropriate probability and all underlying assumptions should be reported as part of the audit trail.

8.17 Proprietary video formats may be associated with specific software or hardware requirements. Without the appropriate configuration, the images may remain inaccessible. The appropriate hardware configuration should be documented in the audit trail and the required replay software should be made available with the video recording (if possible).

BEST PRACTICE 3: Triage video analysis requests.

8.18 A standard submission form should be completed for each video exhibit submitted for analysis. The following information should be supplied on or attached with the submission form to assist with later replay, analysis and court disclosure:

- case file number and other relevant details about the case;
- date of submission;
- identity of the primary investigator;
- identity of the analyst or technician;
- owner and source of the video (e.g. location of the originating camera and/or video recorder, camera views);
- technical information about the system and capture equipment (e.g. make and model, serial number, number of cameras, multiplexer, time-lapse, recording format, system settings, event logs, user manuals, required software and/or hardware);
- information about the point of transfer (identity of the operators, third parties who loaded or ejected the tape);
- time period covered by the video including any error in display time or date;
- description of the events on the video;
- special handling instructions (if relevant);
- physical condition of the evidence (e.g. apparent defects or damages, write-protect mechanism).

8.19 All video evidence should be labelled adequately and catalogued. Each digital file should be given a unique and sensible name to facilitate retrieval. When applicable, both the media and its casing should be labelled. Appropriate labels and/or pens should be used. Care should be taken to ensure that any label attached to a video exhibit is suitable for the intended purpose. To prevent jamming, labels should sit flush in the recess moulded into video tapes.

8.20 The submission form associated with each video exhibit should be reviewed and all discrepancies should be resolved. In some cases, the technician or analyst may need to contact the investigating officer to obtain additional information. If the submitted exhibit is a copy of the original recording, the investigating officer may be asked to obtain the original (assuming it still exists). Tapes should be visually inspected to ensure that the housing case and tape are both intact. Mechanical write-protect mechanisms

should be enabled if they were not already. Information regarding the recording format, time and date should be verified.

8.21 New video exhibits should be triaged and assessed to determine whether or not the request for analysis is reasonable and all the required material has been submitted by the investigating officer. This preliminary assessment should be documented in the case file and the audit trail. The preliminary assessment should compare the required resources and expected financial cost against the seriousness of the incident and the potential investigative value, taking into account the amount of work required, the equipment available, and the time available. An upper limit on caseload should be established for every category of tasks. In some cases, only a subset of the submitted material might be analyzed. If the request is deemed unreasonable, alternatives and other options should be presented to the investigating officer.

BEST PRACTICE 4: Store video exhibits in a secure location.

8.22 A comprehensive archiving plan should ensure that archived video exhibits can be located and retrieved as required. The archiving plan should apply to both physical exhibits and digital evidence. Archived video exhibits should be catalogued or indexed and disposed of in accordance with the applicable statutory requirements and departmental policies.

8.23 Careless handling and poor storage conditions can damage video exhibits and cause the accidental loss of video evidence. Video exhibits should be protected from physical damage or contamination and stored securely. In order to prevent the loss of evidence, analog tapes, digital tapes, CDs and DVDs should be locked in a clean, dry room or cabinet where temperature fluctuations and relative humidity are monitored and controlled (e.g. between 15°C and 25°C and relative humidity of 15% to 50%). Tapes exposed to temperatures above 25°C or relative humidity levels above 50% should be acclimatized before playback. Video tapes should be stored vertically in their individual case to minimize the warping effects of gravity. Cardboard sleeves are not recommended for long-term storage of VHS tapes. Storage media should be kept away from smoke, dust, strong magnetic fields, electrical hazards, intense light, intense heat,

fluids and chemical products. Because they are subject to degradation, digital files stored on short to medium term removable media (e.g. CDs, DVDs, digital tapes) should be transferred regularly to new media or to professionally managed data management archive systems. The storage room containing the master copies should be well-insulated (e.g. of fireproof construction) and should not contain wooden boxes, cardboard boxes, wooden shelving or other easily combustible materials. If an overhead water sprinkler system is installed, the shelving should be designed so that sprinkler water will not contact the tapes. Access to the room should be restricted, monitored and documented appropriately.

8.24 When a server is used to store video files, access to the server should be restricted to individuals with the appropriate clearance and a need-to-know. Access to individual digital files could be further controlled using an electronic password and/or encryption. The server should be backed up as a matter of course but, depending on the risk assessment, further redundancy may be required to prevent the loss of data. Critical high-priority applications (e.g. terrorism investigations) may require a dedicated storage area in order to ensure the confidentiality and availability of the evidence.

BEST PRACTICE 5: Use suitable equipment.

8.25 The correct operation and maintenance of all forensic video equipment is essential to safeguard the evidence from adverse criticism. All equipment used for forensic video analysis should be tested, properly calibrated and maintained in a fully operational condition. All hardware and software used as part of the examination process should meet the technical standards generally accepted by the forensic video community.

8.26 Forensic video analysts should have the ability to digitize the entire NTSC signal in an uncompressed manner. Standard consumer televisions typically only show 480 horizontal lines but each video frame based on the National Television Standards Committee (NTSC) standard carries a total of 525 scan lines of information, with approximately 486 lines containing picture information. The lines that are not displayed represent the underscan area of the analog video signal. The underscan area contains visual information that is not usually displayed on consumer televisions but may be

pivotal in a police investigation. Without the proper analog video monitor or computer software, the analyst will be unable to analyze the underscan area during the video examination process.

8.27 Forensic video analysts should have the ability to export and print high-quality images from video evidence. Printed images should remain faithful to the original video frame. Water-soluble ink is unsuitable for forensic work because prints can be spoiled by any contact with water. Digital images should remain uncompressed or saved in a lossless compression format.

8.28 Forensic video analysts should also have the ability to import uncompressed digital video recordings, view and analyze video at the field level, digitally isolate camera angles from multiplexed video and digitize video using lossless compression algorithms. The analysis software should be able or be programmed to automatically track and record system settings and analysis histories.

8.29 All forensic video equipment should be maintained in accordance with the practices recommended by the manufacturer in the user guide, operating manual or servicing manual. Maintenance should be performed by an authorized technician when required. Regular equipment checks should be performed to make sure that everything is properly powered, the latest software updates have been applied, adjustable settings are appropriate, time and date settings are correct and any visible damage is accounted for. Any equipment or tool requiring calibration should be calibrated at least annually according to the manufacturer's specifications. All equipment verifications, system checks, maintenance activities and corrective actions should be documented in maintenance records. The temperature and relative humidity in the equipment room should remain consistent with the manufacturer's specifications. Electrical surge protection should be employed to protect the electronic equipment.

8.30 A formal replacement schedule should be established to ensure that the forensic video equipment does not become obsolete and to prevent large unexpected financial expenditures. The annual budget should take into account the recurring costs

associated with maintaining, upgrading and replacing the forensic video equipment. Capital costs should be properly amortized and factored in financial projections.

BEST PRACTICE 6: Implement a quality assurance program.

8.31 All forensic video analysis work should be subject to quality control guidelines, regular technical inspections and administrative peer reviews as part of a quality assurance program or quality management system. The quality management system should be supported by proper case records and documented as part of the SOP manual.

8.32 A qualified assessor should be asked to conduct regular technical inspections on a sample of cases. Technical inspections should consider the integrity of all processes used and the validity of all critical findings. Technical inspections should be documented as part of the case management system and the audit trail.

8.33 An administrative peer review should also be performed on each completed case. Administrative reviews should be used to confirm the consistent application of and adherence to SOPs. Among other things, court testimony by forensic video analysts should be monitored and reviewed with an emphasis on impartiality and effectiveness.

8.34 Proficiency tests should be administered periodically by an independent assessor to verify that the technical procedures used are valid and the quality of the work is maintained. The proficiency tests should demonstrate that each forensic video analyst can complete routine activities competently.

8.35 Any gap highlighted by a technical inspection, an administrative review or a proficiency test should be addressed through policy amendments, remedial training or corrective actions. All performance checks and corrective actions should be documented. Regular audits could complement the quality assurance program.

BEST PRACTICE 7: Preserve the master evidence.

8.36 For evidentiary purposes, it must be possible to demonstrate that the images presented in court are authentic and originate from the video captured by the camera and recorded by the recording system. All images should be presented so that evidential content is not compromised. Where possible, images should be stored in an unaltered state and presented in their native or original format. The original evidence should not be subjected to processes that cause permanent alterations.

8.37 The original recording is the video data as it is stored on the CCTV system or other medium. The master evidence or master copy or is the first copy of the data saved on a removable media or a secure server. The master evidence should be defined, labelled, stored, documented and protected as such. It should be stored securely pending its production as an exhibit in court. The master evidence should be secured and sealed as soon as possible to reduce the risk that the evidence will be accidentally or maliciously altered or destroyed. The master evidence should only be viewed to establish the integrity or authenticity of the evidence. All the analysis should be conducted using a working copy.

8.38 A working copy is a version of the master evidence used to conduct the analysis, support the investigation and prepare the prosecution file. A working copy is typically produced simultaneously or immediately after the master evidence is defined, preferably during the first and only replay. A working copy of the video can be made from the original recording or the master evidence. The working copy may or may not be in the same format as the master evidence but any format conversion is likely to adversely impact image quality. The working copy can be viewed, analyzed, duplicated and disseminated as needed.

8.39 In the case of digital video recordings (e.g. digital CCTV), the master evidence should be an exact binary copy of the original video recording when possible. With analog video (e.g. VHS tape), the original tape is sealed and becomes the master evidence once a working copy has been made by either digitizing the video or copying the video on a separate tape. The working copy is typically a slightly degraded version

of the master evidence because additional image noise is generated by the physical wear and tear of the analog tape each time it is played, paused or copied. Poorly maintained VCRs accelerate the degradation of the video. The advantage of digital video recordings is that identical bit-for-bit copies can be produced from the original digital file or the master evidence.

BEST PRACTICE 8: Protect video exhibits using write-protect mechanisms.

8.40 To reduce the opportunities for legal challenges, evidential integrity needs to be protected at the earliest stages of the investigation. Video exhibits should be protected as soon as possible to prevent tampering and maintain evidential integrity. Write-protect mechanisms can prevent accidental erasure, alteration or over-recording.

8.41 As soon as an evidential analog tape is removed from its recording device, the mechanical write-protect mechanism should be activated where available. This is usually in the form of a switch with two positions (e.g. MiniDV cassettes) or a tab that can be removed to prevent the device from switching to record mode (e.g. VHS tapes). Digital video evidence should be designated read-only or stored on write-only removable media as soon as possible after it is captured.

BEST PRACTICE 9: Validate date and time information.

8.42 The images produced by CCTV security systems are often recorded with time and date information to help operators create accurate logs, establish a reliable timeline of events, quickly locate relevant images, and track movements between cameras/systems. Surveys and pilot studies have demonstrated that most CCTV time and date displays are not regularly checked, resulting in many systems displaying incorrect times. Time and date information is more likely to be inaccurate during leap years (on or around February 29th), after the transition from or to Daylight Savings Time (second Sunday in March and first Sunday in November) and after power failures or maintenance work. If the time and date information displayed is incorrect and a time log has not been kept, the value of the recorded evidence may be reduced or questioned.

8.43 First responders and investigators should be encouraged to document and validate the time and date settings every time they seize CCTV video footage. Video exhibits should be reviewed as soon as possible to confirm that time and date settings are correct. The accuracy of the recording system's clock can be established by comparing it to a reliable source (e.g. Computer-Aided Dispatch system or U.S. Naval Observatory Master Clock). All time and date inconsistencies should be documented on the submission form or in the audit trail, should be reconciled as part of the analysis and should be disclosed and explained the court.

BEST PRACTICE 10: Prepare a business continuity plan.

8.44 Video evidence in general and magnetic tapes in particular are highly susceptible to damage in the event of a disaster, such as a fire, flood or earthquake. When exposed to intense heat, tape will melt or burn. Smoke will also affect tapes by leaving an oily film on the tape surface. Water exposure or other liquids can seriously weaken the structural integrity of magnetic tapes. In the event of an earthquake, tapes can fall from the storage shelves or be crushed by falling objects. Physical deformation, chemical decay and surface contamination can cause the loss of evidence.

8.45 In case of fire or flooding, no attempt should be made to play or repair damaged tapes without expert advice. The tensions encountered during playback may result in the permanent deformation of wet tapes. Deformation or chemical decay can also occur if the tape is not allowed to dry properly. If possible, the handling and decontamination should be performed by specialists with a success record in salvaging damaged tapes. If tapes must be disassembled from their original cartridge or hub during the decontamination process, careful notes should be maintained to document the relationship between each tape and the associated information on the box.

8.46 Disaster response procedures should be documented in the Forensic Video Unit's SOP manual and business continuity plan. These procedures should include key information about the equipment room and storage facility (e.g. temperature and humidity control mechanisms, fire alarm system, sprinkler system, location of circuit breaker boxes and shut-off valves, etc.) and the disaster response procedures in case

of fire or flood (e.g. key contact information of recovery service providers and professional experts or labs). Although fire extinguishers and emergency supplies such as gloves and plastic sheeting should be kept in or near tape storage areas, burning video tape produces noxious fumes so staff should be instructed to evacuate immediately in case of fire.

8.47 The Forensic Video Unit business continuity plan could mirror the business continuity plan for the Evidence Room, the Forensic Identification Unit and the Technological Crime Unit (if available).

BEST PRACTICE 11: Confirm the integrity of digital video recordings.

8.48 Digital evidence submitted for forensic examination should be handled and stored in a way that will preserve the integrity of the data. Data integrity ensures that the information presented in court is complete and unaltered.

8.49 Steps should be taken as early as possible to ensure that the integrity of each digital video recording can be verified before it is presented as evidence in court. The verification process should establish the integrity of the recording by confirming that the acquired data (e.g. working copies) reflects the master evidence or even the original data (e.g. on the digital CCTV recorder).

8.50 Integrity verification can be achieved using hash verifications or checksum tests. Hash functions rely on mathematical algorithms to confirm that a digital file was copied properly without any undesirable changes such as conversion or compression artifacts. Any minute difference between the original recording and the copy would cause the hash comparison to fail. The integrity of the recording is assured when the identifier of the original recording matches exactly with the identifier computed for the copied data.

8.51 Hash verifications should be initiated before the original data is copied (“acquisition hash”) and before a working copy is analyzed (“verification hash”). This will ensure that the integrity of the data is not compromised and will authenticate the video file as a true and accurate copy of the original evidence.

BEST PRACTICE 12: Correct the aspect ratio of digital video recordings.

8.52 Most CCTV video cameras currently in use produce an analog signal. When the signal is sampled/converted and encoded by a digital video recording system, the video can become distorted. These distortions are caused by the cross-conversion of the analog signal based on a non-square pixel matrix into a square-pixel digital environment. These conversion errors lead to horizontal stretching in NTSC images and vertical compression in Phase-Alternation Line (PAL) images.

8.53 In order to recognize and correct the distortions introduced during the conversion of the analog signal, the aspect ratio of digital video recordings should be validated and corrected if necessary. Aspect ratio calibration is especially important for photogrammetric applications and comparison analysis (e.g. suspect identification).

8.54 Calibrating the aspect ratio of a digital video recording would involve the use of a calibration chart (e.g. SMPTE chart) to obtain a control image (e.g. live camera feed recorded using an analog VHS tape) that can be compared to the digital recording using specialized software. The entire calibration process should be documented in the audit trail, along with all the relevant calibration settings.