

Spring 2021

A Policy Examination of Digital Multimedia Evidence in Police Department Standard Operating Procedures (SOPs)

Timothy P. Larmon

Follow this and additional works at: https://via.library.depaul.edu/soe_etd



Part of the [Educational Leadership Commons](#)

Recommended Citation

Larmon, Timothy P., "A Policy Examination of Digital Multimedia Evidence in Police Department Standard Operating Procedures (SOPs)" (2021). *College of Education Theses and Dissertations*. 214.
https://via.library.depaul.edu/soe_etd/214

This Capstone is brought to you for free and open access by the College of Education at Via Sapientiae. It has been accepted for inclusion in College of Education Theses and Dissertations by an authorized administrator of Via Sapientiae. For more information, please contact digitalservices@depaul.edu.

DePaul University
College of Education

**A Policy Examination of Digital Multimedia Evidence in Police
Department Standard Operating Procedures (SOPs)**

A Capstone in Education with A Concentration in Educational Leadership

By: Timothy P. Larmon

© 2021 Timothy P. Larmon

Submitted in Partial Fulfillment of the Requirements for the
Degree of Doctor of Education

June 2021

I approve the capstone of Timothy P. Larmon.

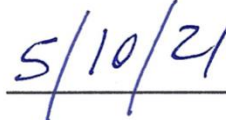
A handwritten signature in blue ink, reading "Andrea Kayne", written over a horizontal line.

Andrea Kayne

Program Director &
Associate Professor in Educational Leadership

DePaul University

Capstone Advisor

A handwritten date "5/10/21" in blue ink, written over a horizontal line.

Date

Certification of Authorship

I certify that I am the sole author of this capstone. Any assistance received in the preparation of this capstone has been acknowledged and disclosed within it. Any sources utilized, including the use of data, ideas and words, those quoted directly or paraphrased, have been cited. I certify that I have prepared this capstone according to program guidelines as directed.

Author Signature  _____ Date 10/21/21

Executive Summary

2020 will be a year forever marked by the Covid-19 pandemic. The year will also be remembered for the death of George Floyd at the hands of police officer Derek Chauvin. The death was recorded by a bystander's cell phone and broadcast all over the world to see. This video proved pivotal in the prosecution and conviction of Chauvin for Floyd's death. The video provided powerful evidence highlighting the importance of incorporating video evidence into the investigation and prosecution of crime.

Today, police use a variety of video evidence to assist in their investigations. In some cases, it may be a small part of the case whereas in others it may provide vital evidence. There has been an explosion in the number of video sources where police can now gather evidence. Cellphone videos, private security cameras on homes or businesses, social media postings, and police body cameras all provide possible evidence that must be collected, extracted and analyzed. In 2019, there were 40 million professionally installed video recording systems and 224 million smartphones in the U.S. alone. Along with the approximately 400,000 body cameras worldwide, there is a numerous amount of video available to investigators.

It is important for police departments to acquire this video evidence according to legal requirements and best practices according to industry leaders to avoid any future legal challenges to the evidence. This study will analyze how police departments around the country are handling video evidence through their Standing Operating Procedures (SOPs) using legal requirements and industry best practices as a guideline. The author chose to concentrate on two of the main legal challenges facing law enforcement today while working with digital evidence: authentication and integrity. Despite sometimes being used interchangeably, authentication and integrity present two different challenges when working with digital evidence. Authentication is when the evidence put forth in a trial is what the party admitting it into evidence claims it to be. Integrity is ensuring the evidence has not been changed or altered since its original form. In this study, the author chose to concentrate on the issues of authentication and integrity specifically in relation to Digital Multimedia Evidence (DME). DME is information of probative value stored in binary form including but not limited to tape, film, magnetic, optical media, and/or the information contained therein.

The author created a rubric utilizing best practices identified by industry leaders along with legal guidelines set forth by the Federal Rules of Evidence, court cases, and law reviews. The rubric evaluated the Department's SOPs on three phases: Training, Process, and Documentation.

Table of Contents

List of Figures	vii
INTRODUCTION.....	1
LITERATURE REVIEW	5
Authentication and the Federal Rules of Evidence	5
Authentication and the Supreme Court	8
Authentication and Federal Appeals Court Cases	9
Authentication and State Cases.....	14
Law Reviews.....	18
Best Practices	21
METHODOLOGY	23
Data Analysis.....	31
Overview of the Sample.....	32
Limitations.....	32
RESULTS.....	34
Above Average Digital Multimedia Evidence SOPs.....	34
Average Digital Multimedia Evidence SOPs.....	37
Below Average Digital Multimedia Evidence SOPs.....	40
DISCUSSION.....	43
Digital Multimedia Evidence – Training.....	43
Digital Multimedia Evidence – Process.....	45
Digital Multimedia Evidence – Documentation.....	47
Other Considerations.....	48
RECOMMENDATIONS	51
CONCLUSION.....	55
REFERENCES	56
APPENDICES	60

Appendix A – Evaluation Rubrics	60
Appendix B – Documentation Form Examples	67
Appendix C – Workflow Examples	76

List of Figures

Figure A: Growth in Video.....	2
Figure B: SWGDE Image Integrity Workflow.....	29
Figure C: SWGDE Sample Field Note Form	30
Figure D: Department A Equipment List.....	34
Figure E: Department A Documentation Form.....	35
Figure F: Department B Retrieval Form	37
Figure G: Department Evaluation Results.....	42
Figure H: SWGDE Workflow Example	46

INTRODUCTION

The death of George Floyd brought to public light many issues in policing today. One problem the case shined a light on is the importance of video evidence in police investigations. The most crucial witness in the case was the cellphone video taken by a bystander. This evidence was pivotal in bringing charges against officer Derek Chauvin. What would have happened to the case if the lead investigator not recover the bystander video? What if that video came from the building's surveillance system and was overwritten before investigating units could retrieve it? The recovery and handling of video surveillance or digital multimedia evidence (DME) is a crucial component of police investigations today. Without it we might have never fully understood the George Floyd case. There was video surveillance footage, Body Worn Camera video, and In-Car Camera video, along with the cellphone video. All of these methods of capturing an incident were utilized by the prosecution in the case against Chauvin.

The prevalence of security camera systems across the country has exploded in recent years. Including the number of cellphones, body cameras, and in-car cameras, most aspects of our daily lives are being recorded by some sort form of video. Around the world, approximately 6 billion hours of video are recorded every hour (Friese, 2019). According to data presented by the International Association of Chiefs of Police (IACP) 2019 conference, in 2019 there were:

- 40 million professionally installed video recording systems in the U.S.
- 224 million smartphones in the U.S.
- 98 million network surveillance cameras in the world
- 29 million CCTV surveillance cameras in the world
- 400,000 body cameras worldwide (Friese, 2019)

In addition to all the surveillance and cellphone footage available, the Scientific Working Group on Digital Evidence (SWGDE) provides additional resources that could aid in investigations:

- Municipal surveillance systems (downtown cameras, pole cameras)
- Public Transportation
- Freeway and Toll Road Cameras
- Rideshare, Taxi, or private dash recording systems
- Commercial unmanned aerial vehicles (drones)
- Video gaming consoles
- Social media platforms
- News media outlet websites
- Game and wildlife cameras
- Cloud-based video storage solutions (Scientific Working Group on Digital Evidence, 2021, p. 5)

A digital forensic detective who has worked with video evidence for the past ten years has seen first-hand the dramatic increase in available video. The detective provided the amount

of growth in video retrieval for his agency which covers a municipal jurisdiction of approximately 100,000 residents:

- 2013: 331 videos, 19.76 GBs
- 2014: 6595 videos, 279.81 GBs
- 2015: 13,013 videos, 540.97 GBs
- 2016: 17,154 videos, 788.65 GBs
- 2017: 19,801 videos, 1092.47 GBs
- 2018: 43,870 videos, 1752.45 GBs
- 2019: 34,590 videos, 2474.04 GBs (Paxton, 2020)

The need for law enforcement personnel to utilize this evidence has also increased dramatically. All of this video is possible evidence that can be utilized to solve crimes and prosecute offenders. It is important to recover this evidence and ensure that the evidence is being recovered in the right way to verify the right person is being charged with a crime. It is also important to properly handle this massive amount of evidence and ensure integrity in investigations. In discussing the importance of digital evidence in homicide investigations, the Police Executive Research Forum (PERF) identified the challenges of handling digital evidence compared to traditional forms of physical evidence such as fingerprints or DNA. Digital evidence contains a wider array

of source material, can sometimes contain personally sensitive information and requires specialized training and equipment (Police Executive Research Forum, 2018). The National Institute of Justice (2020) further explains proper seizure of technological devices must be done correctly due to the volatile nature of the data to preserve the integrity of the data and ensure the evidentiary value in legal proceedings.

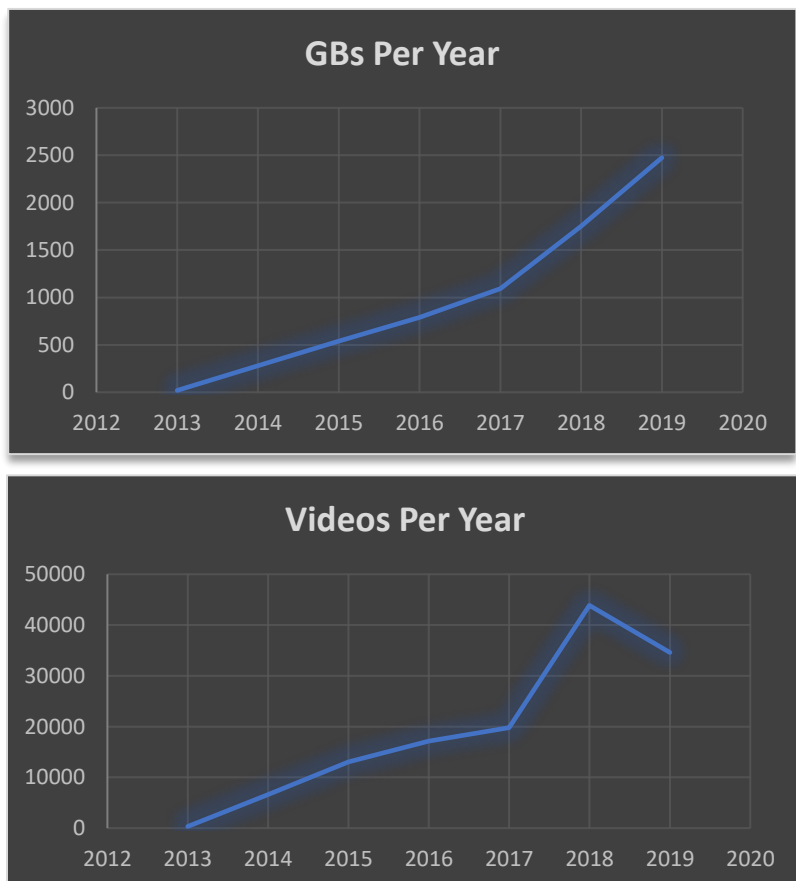


Figure A. Growth in video retrieval for a police department covering a municipal jurisdiction of 100,000 residents. (Paxton, 2020)

Police departments will need a thorough and comprehensive network of procedures to properly handle the challenges they face with collecting, extracting, and analyzing digital evidence. This report will look at how departments train their members in the best practices in handling digital multimedia evidence (DME) by evaluating their Standard Operating Procedures (SOPs). In discussing the importance of a policy and procedure manual, (Orrick, n.d.) states when a policy and procedure manual is adequately developed and implemented, it provides staff with information to act decisively, consistently, and legally. It also ensures department personnel are prepared for any unusual circumstances and identifies the correct course of action.

The following definitions will be used as key terms throughout this report. The author includes the definitions for Digital Evidence and Digital Multimedia Evidence. The author chose to concentrate specifically on Digital Multimedia Evidence for this research but utilized sources and materials that do not distinguish between the two.

Digital Multimedia Evidence (DME): information of probative value stored or transmitted in binary form including, but not limited to, tape, film, magnetic and optical media, and/or the information contained therein. (Law Enforcement and Emergency Services Video Association, UNK, p. 4)

Digital Evidence: Information of probative value that is stored or transmitted in binary form (Scientific Working Group on Digital Evidence, 2016, p. 7).

Digital Video Recorders (DVR): primarily found in residential, commercial, or governmental institutions and include these major types:

- Stand-Alone Embedded Digital Video Recorder
 - Stand-Alone Embedded Network Video Recorder
 - Hybrid Digital Recorder
 - Dedicated Computer
 - Personal Computer
 - Serve-Based (only accessible by client station)
-

(Scientific Working Group on Digital Evidence, 2018)

The following definitions are provided to assist in the reading of this report. They are taken directly from SWGDE's Digital & Multimedia Evidence Glossary (2016, pp.4-19):

- CD/DVD: Optical Disc formats designed to function as digital storage media.
- Chain of Custody: The chronological documentation of the movement, location and possession of evidence.
- Copy: An accurate reproduction of information.
- Data: Information in analog or digital form that can be transmitted or processed.

- **Data Extraction:** A process that identifies and recovers information that may not be immediately apparent.
- **Digital Evidence:** Information of probative value that is stored or transmitted in binary form.
- **Downloading/Exporting:** The process of retrieving audio, video, and still images and transactional data from a DVR system. Can be in either the native/proprietary format or an open format.
- **DVR (Digital Video Recorder):** a stand-alone embedded system or a computer-based system used to record video and/or audio data.
- **Integrity Verification:** The process of confirming that the data presented is complete and unaltered since time of acquisition.
- **Media:** Objects on which data can be stored.
- **Metadata:** Data, frequently embedded within a file, that describes a file or directory, which can include the locations where the content is stored, dates and times, application specific information, and permissions.
- **Multimedia Evidence:** Analog or digital media, including, but not limited to, film, tape, magnetic and optical media, and/or the information contained therein.
- **Original Image:** An accurate and complete replica of the primary image, irrespective of media. For film and analog video, the primary image is the original image.
- **Physical Copy:** An accurate reproduction of information contained on the physical device.
- **Proprietary File Format:** Any file format that is unique to a specific manufacturer or product.
- **Triage:** The process by which items considered for collection or analysis are prioritized to determine the order in which they should be collected and/or analyzed, if at all.
- **Verification:** 1) The process of confirming the accuracy of an item to its original. 2) Confirmation that a tool, technique or procedure performs as expected.
- **Video:** The electronic representation of a sequence of images, depicting either stationary or moving scenes. It may include audio.
- **Video Analysis:** The scientific examination, comparison, and/or evaluation of video in legal matters.
- **Video Security Recording System:** One of more cameras connected to a recording device capable of storing analog or digital video information.
- **Work Copy:** A copy or duplicate of a recording or data that can be used for subsequent processing and/or analysis.

LITERATURE REVIEW

The 6th Amendment of the U.S. Constitution guarantees the right to a speedy and public trial, the right to an impartial jury, to confront the witnesses against the accused, and the right to have an attorney present. While this is not a complete list of the rights guaranteed by the 6th Amendment, it highlights the point made by the founding fathers of a fair and impartial jury (Sixth Amendment, n.d.). When conducting investigations, police departments should make every attempt to ensure they are collecting and presenting evidence that abides by the principles of the 6th Amendment. To guarantee the evidence they put forth results in every citizen receiving a fair and impartial trial, police departments need to ensure the evidence they produce in court is what they, in fact, say it is. Goodison et al. (2015) identified the issue of authentication and chain of custody as one of the leading legal challenges facing law enforcement when working with digital evidence. They define authentication as the “process of establishing that the evidence is actually what its proponents claim it to be,” meaning the party introducing the evidence at court is required to show the evidence is genuine. Part of the authentication process is chain of custody, which assures the evidence was preserved in its original form (Goodison et al., 2015, p. 11). Similarly, the terms “Integrity” and “Authentication” are sometimes interchanged. Integrity Verification looks to answer if the evidence has been changed or altered; Authentication seeks to answer if the evidence accurately represents what it purports to be (Law Enforcement and Emergency Services Video Association, 2010). By addressing these legal challenges and understanding what the courts are ruling regarding digital evidence, police departments will be better equipped to establish best practices in their policies and procedures.

Authentication and the Federal Rules of Evidence

Digital evidence that is recovered during an investigation may go through “authentication” during trial. Authentication is “the process by which a party attempting to have some sort of evidence admitted at trial must provide sufficient evidence so that a reasonable juror can conclude that the evidence the party seeks to admit is what that party claims it to be” (Rule 901.Authenticating or Identifying Evidence, n.d., para. 1). In the Federal court system, authentication of evidence is guided by the Federal Rules of Evidence. Under the Federal Rules of Evidence, several rules help provide guidance on digital evidence. One of those rules, Rule 901.Authenticating or Identifying Evidence (n.d.), states the following:

- (a) In General, to satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient enough to support a finding that the item is what the proponent claims it is.
- (b) Examples. The following are examples only – not a complete list – of evidence that satisfies the requirement:
 - (1) Testimony of a Witness with Knowledge
 - (2) Nonexpert Opinion about Handwriting
 - (3) Comparison by an Expert Witness of the Trier of Fact
 - (4) Distinctive Characteristics and the Like
 - (5) Opinion About a Voice

- (6) Evidence about a Telephone Conversation
- (7) Evidence about Public Records
- (8) Evidence about Ancient Documents or Data Compilations
- (9) Evidence about a Process or System
- (10) Methods Provided by a Statute or Rule (para. 1)

Concerning digital evidence, the most important examples in Rule 901 are examples (b)(1) and (9). Example (b)(1) states, “testimony that an item is what it is claimed to be” (Rule 901. Authenticating or Identifying Evidence, n.d., para. 1). Example (b)(1) would pertain to homeowners testifying to footage collected from their surveillance system or law enforcement personnel testifying to digital evidence they recovered, processed, or produced in the course of their investigation. Example (b)(9) states: “evidence describing a process or system and showing it produces an accurate result” (Cornell Law School, n.d., para. 1). Example (b)(9) helps guide the systems that produce digital evidence such as computers, cameras, video recorders, DVR’s, NVR’s or other surveillance systems. Rule (b)(9) is designed for situations where the accuracy of a result depends on the process that produces that result. In following up Rule 901, Rule 902-Evidence that is Self-Authenticating (n.d.) states the following:

The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:

- (1) Domestic Public Documents That Are Sealed and Signed
- (2) Domestic Public Documents That Are Not Sealed but Are Signed and Certified
- (3) Foreign Public Documents
- (4) Certified Copies of Public Records
- (5) Official Publications
- (6) Newspapers and Periodicals
- (7) Trade Inscriptions and the Like
- (8) Acknowledged Documents
- (9) Commercial Paper and Related Documents
- (10) Presumptions Under a Federal Statute
- (11) Certified Domestic Records of a Regularly Conducted Activity
- (12) Certified Foreign Records of a Regularly Conducted Activity
- (13) Certified Records Generated by an Electronic Process or System
- (14) Certified Data Copied from an Electronic Device, Storage Medium, or File
(para. 1)

Similar to Rule 901, there are certain sections of Rule 902 that can be applied directly to digital evidence. 902(13) states:

A record generated by an electronic process or system that produces an accurate result as shown by a certification of a qualified person that complies with the certification requirements of Rule 902 (11) and (12). The proponent of the evidence must also meet the notice requirements of Rule 902 (11) (para. 1).

This amendment provides a procedure where authenticating specific electronic evidence can be done without utilizing the testimony of a foundation witness. This amendment was established to alleviate the expense and inconvenience of producing a witness to authenticate an item of electronic evidence. Under this Rule, a proponent seeking to establish authenticity must present a certification containing the same information that would be sufficient to establish authenticity from information provided by a witness at trial. The new rule allows the authenticity foundation that satisfies Rule 901(b)(9) to be established by certification instead of testimony from a witness (Rule 902. Evidence that is Self-Authenticating, n.d.). Rule 902 (14) states: “data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902 (11) or (12)” (Rule 902. Evidence that is Self Authenticating, n.d., para. 1). The proponent also must meet the notice requirements of Rule 902 (11). Similar to (13), this establishes a procedure that allows parties to authenticate data copied from an electronic device, storage medium, or an electronic file without having to produce testimony from a foundation witness (Rule 902. Evidence that is Self-Authenticating, n.d.). This data can be authenticated by what is called the “hash value.”

Hash Value is a unique number that contains: “a series of letters and numbers, what some courts have called a ‘digital fingerprint’ assigned to a particular input” (Martin, 2018, p. 3). Because a hash value is a unique identifier produced by an algorithm, any change in a file will change the hash value. An unedited copy of a file will have the same hash value as the original. If a copy has a different hash value, then that copy will not be an exact replica. Rule 902(14) allows for self-authentication from certification of a qualified person that they checked the hash value of the proffered item and that it is identical to the original (Rule 902. Evidence that is Self-Authenticating, n.d.). Dennis Martin’s (2018) *Demystifying Hash Searches* describes a “hash search” as: “a very accurate, very computationally efficient type of search that can be used not just for legitimate purposes but also to identify evidence of crimes outside the scope of a search warrant” (p. 2). He further breaks down the terms “hash function” and “hash set.” A hash function is described as “a mathematical process that takes some input, like a text file or an image, and outputs a hash value” (p. 3). A hash set is described as “a collection of inputs that are stored according to their hash values” (p. 3). The use of hashing and hash values can be used to preserve evidence for trial. For example, when a copy is made of a hard drive or surveillance video, each file generates a unique hash value. Any minor change in that file will cause a significant difference in the hash value, therefore causing a digital chain of custody. This way, the evidence presented at trial can be proven to be the same evidence seized initially. The Scientific Working Group on Digital Evidence (SWGDE) identifies the following as the four most common hash algorithm families in current use: MD5, SHA1, SHA2, and SHA3 (Scientific Working Group on Digital Evidence, 2019).

Hash values can help determine that a copy is the same as an original. When dealing with digital evidence, the “original” is defined by the Federal Rules of Evidence 1001 (d), which states: the “ ‘original’ means any printout—or other output readable by sight—if it accurately reflects the information. An ‘original’ photograph includes the negative or a print from it” (Rule 1001. Definitions That Apply to This Article, n.d. para. 1). Rule 1001 (e) defines a “duplicate” as “a counterpart produced by a mechanical, photographic, chemical, electronic, or other equivalent

process or technique that accurately reproduces the original” (Rule 1001, n.d. para. 1). Rule 1003 Admissibility of Duplicates (n.d.) further explains: “a duplicate is admissible to the same extent as the original unless a genuine question is raised about the original’s authenticity or circumstances make it unfair to admit the duplicate” (para. 1). In essence, the Federal Rules of Evidence is stating there is not a single “original” when it comes to digital evidence. Anything that is an exact copy or replica of the original is then considered an original. Therefore, by using hash values, a copy can be introduced and proven to be the same as the “original” in trial. By producing a hash value when acquiring digital evidence, a member will be able to check any future copies against the original to maintain the integrity of the evidence.

FRE 702, Testimony by Expert Witnesses (n.d.), may be necessary when handling digital evidence if a member collects, extracts, or analyzes the evidence. FRE 702 states,

A witness who is qualified as an expert by knowledge, skill, experience, training or education may testify in the form of opinion or otherwise if:

- (a) The expert’s scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
- (b) The testimony is based on sufficient facts or data;
- (c) The testimony is the product of reliable principles and methods; and
- (d) The expert has reliably applied the principles and methods to facts of the case. (para. 1)

Authentication and the Supreme Court

The United States Supreme Court is the foremost authority in our legal system. The Supreme Court has yet to decide any landmark cases dealing with the authentication of digital evidence; however, we can look at several past decisions to help guide us. In *Frye v. United States* (1923), the District of Columbia Court of Appeals came up with what is now known as the *Frye* Test. In their decision, the court noted that “the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs” (*Frye v. United States*, 1923, para. 6). In essence, the court said a “test” without an established place in science is between experimental and demonstrated science and therefore not “sufficiently established.” So for a “process” or “test” to be admitted into evidence, it has to be “sufficiently established” and accepted within the scientific community (*Frye* Case Brief, n.d.). The Supreme Court articulated a similar threshold standard dealing with the admissibility of expert evidence in 1993 in *Daubert v. Merrell Dow Pharmaceuticals Inc* (1993). *Daubert* is the standard by which a trial judge assesses whether an “expert witness’s scientific testimony is based on scientifically valid reasoning that which can properly be applied to the facts at issue” (*Daubert*, n.d., para.1). The Supreme Court further identified the following factors to determine admissibility:

- (1) Whether the theory or technique in question can be and has been tested
- (2) Whether it has been subjected to peer review and publication
- (3) Its known or potential error rate
- (4) The existence and maintenance of standards controlling its operation; and

- (5) Whether it has attracted widespread acceptance within a relevant scientific community (Daubert, n.d., para. 2)

Authentication and Federal Appeals Court Cases

The state of Illinois falls under the 7th Circuit Court of Appeals jurisdiction, which means their decisions have mandatory authority over the state and any police department within it. Mandatory authority is any case, statute, or regulations the court must follow because it is binding on the court. Therefore, lower courts must follow the decisions handed down by the higher courts. Persuasive authority are any cases, statutes, regulations, or secondary sources that a court may elect to follow but is not mandated to do so (When and How to Use Secondary Sources and Persuasive Authority to Research and Write Legal Documents, 2004). The 7th Circuit of Court of Appeals has yet to decide any cases dealing with video evidence; however other circuit Court of Appeals decisions can help give guidance through their persuasive authority. The following are additional circuits Court of Appeals cases dealing with authentication and digital evidence:

US v. Taylor (1976)

A jury convicted Taylor and Hicks for Armed Robbery of a federally insured state bank. On the morning of February 10th, 1975, the Havana State Bank in Florida was robbed by two men wearing masks. The robbers ordered everyone inside into a bank vault where they were locked inside. As the robbers fled, a bank camera was tripped, which took pictures of the robbers. Taylor and Hicks were stopped about an hour later in Georgia but were released after two bank tellers from the Havana State Bank could not identify them. They were re-arrested the next day by the FBI due to the strength of the bank photographs taken at the time of the robbery. Hicks argued in his appeal that the district court erred in admitting into evidence the contact prints made from the bank cameras. Hicks argued the government did not lay the proper foundation for admission because none of the eyewitnesses could testify the prints accurately represented the inside of the bank when they were taken because they were locked in the vault. The 8th circuit agreed with the notion the eyewitnesses would not be able to testify to the accuracy of the prints. However, the only testimony offered as to the foundation was the government witnesses who were not present at the time of the incident. The government witnesses only testified to the “manner in which the film was installed in the camera, how the camera was activated, the fact that the film was removed immediately after the robbery, the chain of its possession, and the fact that it was properly developed and contact prints made from it.” The 5th Circuit found this testimony was enough for sufficient authentication for admission of the prints (*US v. Taylor*, 1976).

US v. Rembert (1988)

In *Rembert*, the appellant Rembert was identified by eyewitnesses as well as a witness who made an identification after viewing a series of photographs from a closed-circuit surveillance video camera. The photographs from the eyewitness identification were entered into evidence during the trial, with the sole authenticating witness being the supervisor of the loss-control division of a bank. The supervisor testified how the cameras were set up, how they

recorded, how the cameras took a picture every three seconds, and how the process imprinted the date and time on each picture. The supervisor testified that she did not have any personal knowledge of the events that took place but testified the photographs presented in court accurately depict what she viewed on the original videotape. Rembert argued the photographs were admitted under two theories of authentication, illustrative or “pictorial testimony” and the “silent witness” model. He further argued the foundation offered by the prosecution did not satisfy either of those two theories. The court found that he was correct in claiming the foundation by the prosecution did not meet either of those two theories. However, they followed the precedent set in an earlier ruling under *United States v. Blackwell* (1982) in that when dealing with photographic evidence, “authentication and identification are specialized aspects of relevancy that are necessary conditions precedent to admissibility” (para. 16). In *Blackwell*, photographs of the defendant holding a firearm were seized in a search warrant. The picture of the firearms was discovered in the same room as the recovered firearms. No witnesses were able to testify to when, where, or by what process the photographs were made.

Additionally, there were no witnesses to testify the photographs accurately and fairly depicted any particular scene on any specific date. A detective who conducted the search warrant was able to testify to the detail of the pictured weapon. The detective also testified the interior background was similar to the details of the firearm and room in question. The court required “only that the proponent of documentary evidence make a showing sufficient to permit a reasonable juror to find that the evidence is what its proponent claims” (para. 16). The court also cited a previous case in the 9th Circuit, *United States v. Stearns* (1977) where Judge Kennedy wrote: “Even if direct testimony as to foundation matters is absent...the contents of a photograph itself, together with such other circumstantial or indirect evidence as bears upon the issue, may serve to explain and authenticate a photograph sufficiently to justify its admission into evidence” (paras. 12-21). To be consistent with their decision in *Blackwell* and other sister circuit courts, the court stated: “we conclude that the contents of photographic evidence to be admitted into evidence need not be merely illustrative, but can be admitted as evidence independent of the testimony of any witness as to the events depicted, upon a foundation sufficient to meet the requirements of Federal Rule of Evidence 901(a)” (*US v. Rembert*, 1988, para. 14). The court also noted “the role of photography in technology and society at large is a changing one, and the courts must change with it” (*US v. Rembert*, 1988, para. 16). The court ruled the District Court judgment was without error in ruling the evidence was correctly admitted and affirmed (*US v. Rembert*, 1988).

US v. Munoz (2003)

In another 8th Circuit case, part of Rodriguez argues a videotape recording of his post-Miranda statements was wrongly admitted into evidence by the district court. Munoz and Rodriguez were arrested after a narcotic investigation in South Dakota. After being advised of his Miranda Rights, Rodriguez consented to an interview when he admitted to selling and purchasing methamphetamine. An edited version of this videotape confession was shown at the trial. Rodriguez argued the videotape confession should not have been admitted into evidence due to the poor quality. The 8th Circuit first noted the seven foundational requirements discussed

in *McMillan* (1974) were satisfied to allow the tape into evidence. In *McMillan* (1974), the court provided seven requirements for introducing evidence obtained through electronic monitoring:

- 1) That the recording device was capable of taping the conversation now offered in evidence.
- 2) That the operator of the device was competent to operate the device
- 3) That the recording is authentic and correct
- 4) That changes, addition, or deletions have not been made in the recording
- 5) That the recording has been preserved in a manner that is shown to the court
- 6) That the speakers are identified
- 7) That the conversation elicited was made voluntarily and in good faith, without any kind of inducement (para. 8)

These requirements having been satisfied, the court ruled, “the quality of the recording did not call into question its trustworthiness, and because the evidence indicates that the recording was audible and intelligible, we conclude that the district court did not abuse in admitting it into evidence” (*US v. Munoz*, 2003, para. 14).

The following Federal Appeals court cases concern issues with hash values and functions. They provide guidance on the importance and reliability of hash values.

US v. Glassgow (2012)

Robert Glassgow was convicted of receipt of child pornography after the seizure of his computer, which contained 88 images of child pornography on his hard drive. Glassgow admitted to investigators that he viewed the images, which he accessed through a peer-to-peer program called “Frostwire.” After the images were downloaded, they were modified, accessed, and then attempted to be deleted but remained on unallocated space on his hard drive. Glassgow argued the government’s exhibit 1, a DVD compilation of three video clips from a law enforcement database, were only “similar” to the images found on his computer. The government’s witness testified the SHA1 values of the law enforcement videos matched the SHA1 values of the files on Glassgow’s computer. According to the government witness, the SHA1 values matching meant there was a 99.9999% probability that Exhibit 1 contained the same video clips found on Glassgow’s computer. The court also defined SHA-1 as “stands for Secure Hash Algorithm Version 2- a digital fingerprint of a computer file. It is a 32-digit number that is calculated for a file and unique to it” (para. 4). The Eighth Circuit found the district court did not abuse its discretion in admitting their video exhibits. This case is also an excellent example of why Rule 902 (13) and (14) were enacted. This case was settled in 2012, before 902 (13) and (14). However, in this case, the prosecution could have produced a certified document showing the SHA1 values for Glassgow’s files compared to the SHA1 values of the law enforcement database files. This certified document may have alleviated the need to bring in the government witness to testify to the match (*US v. Glassgow*, 2012).

US v. Miknevich (2011)

Miknevich argued in this case that the warrant issued for his home did not have sufficient probable cause from the affidavit prepared by law enforcement. Investigators with the Delaware State Police were investigating child pornography using P2P file-sharing networks. During the investigation, a file known to law enforcement to be child pornography was discovered along with its SHA1 hash value. From experience, investigators knew this hash value to be child pornography. The network used by investigators returned a list of users and their IP addresses who had this same file or a portion of it. One of those IP addresses belonged to Miknevich. Due to these facts, a warrant was obtained to seize Miknevich's computer. The court upheld the District Court's order affirming the search warrant was valid in part due to the "significance of the SHA1 value as a 'digital fingerprint' and avers that the investigating officers were familiar with the SHA1 value associated with the file on Miknevich's computer" (para. 21). Despite the court recognizing that computer file names do not always represent what is contained in the file, the court found that the descriptive file name and the SHA1 value had sufficient facts for probable cause (*US v. Miknevich, 2011*).

US v. Wellman (2011)

The Wellman case is another child pornography case where the validity of the search warrant was challenged. Like Miknevich, West Virginia State Police investigators received a spreadsheet from another local law enforcement agency that identified instances where child pornography was transmitted over a computer file-sharing network. Although the files were not identified by name, type, or description, as was the case in Miknevich, their hash value identified them. The investigators received a spreadsheet that "contained a hash value for a digital file, the Internet Protocol (IP) address of the computer offering the file for download, the locality in which that computer operated, the time and date the file was observed, and the officer from the Task Force who identified the file, as well as his or her law enforcement agency" (para. 2). Further investigation revealed one IP address belonging to Wellman alleged to have hosted five different digital files of suspected child pornography. The court ruled that the district court did not err in denying Wellman's motion to suppress because of the totality of the information provided in the search warrant. The affiant in the search warrant provided his background as an investigator, which established his experience in child pornography cases. A thorough explanation of the technology used in the investigation and the additional effort that resulted in a six-week investigation provided enough probable cause for the search warrant (*US v. Wellman, 2011*).

The following case deals with chain of custody issues that can provide guidance on the importance of handling evidence and chain of custody.

Gallego v. United States (1960)

Gallego was a case decided in the 9th Circuit where the court looked at the issue of chain of custody with evidence. Gallego was stopped crossing the border into the US from Mexico by an immigration inspector and a customs inspector. The immigration inspector discovered a paper sack containing marijuana in the trunk of Gallego's vehicle, who then handed the sack to the customs inspector. The customs inspector then immediately gave the paper sack to Fred

Valenzuela, the Deputy Collector of Customs, who took the sack to his office and placed it in his desk at the Customs House. Immediately afterward, Gallego was searched at the Customs house where a tobacco can containing marijuana cigarettes was discovered on his person, which was also placed in Valenzuela's desk. Both items were in the desk for about an hour, with Valenzuela in the vicinity the entire time. Valenzuela then put the items in a safe for the night.

The next day, Valenzuela retrieved the two items, brought them to a hearing, and returned them to the safe after the hearing. Ten days later, the items were removed from the safe and sent by registered mail to a customs laboratory in Los Angeles. After testing, they were then returned by registered mail and put back in the safe, where they were kept until the day of the trial. At trial, the immigration inspector identified the paper sack and its contents with his initials and testified that it was the same one he had discovered in Gallego's vehicle. He was handed the can with his initials on it and testified it appeared to be the same can that was found but was unable to testify the contents were the same. Valenzuela also examined both items and testified the sack as the same one turned over to him and the can as the same one he discovered on the appellant's person. He further testified the contents of the can appeared to be "very much" the same as when he discovered the can. The chemist who analyzed the two containers testified they were the same ones that reached him by registered mail that, by his analysis, both containers tested for marijuana. The safe where the contents were kept had a combination where the only two individuals with the combination were Valenzuela and the acting deputy collector of customs, who took the place of Valenzuela when he was away. Gallego challenged the admissibility of the evidence for failing to show the government had exclusive control and possession of the articles during the ten days they were in the safe. Gallego further argued that it was incumbent on the government to prove that the chain of custody was complete and the items were not tampered with or altered during the ten-day period. The 9th Circuit stated that a physical object connected with the commission of a crime must be shown to be in "substantially the same condition as when the crime was committed" to be admitted into evidence. The only person allowed to make this determination is the trial judge. The jury is then allowed to disregard the evidence if the article was not correctly identified or change in its nature. The court determined the following factors to be considered by the judge: "the nature of the article, the circumstances surrounding the preservation and custody of it, and the likelihood of intermeddlers tampering with it. If upon the consideration of such factors the trial judge is satisfied that in reasonable probability the article has not been changed in important aspects, he may permit its introduction into evidence." The court further noted the jury is then free to disregard evidence if it finds the evidence was not adequately identified or a change in its nature. The court also cited *Pasadena Research Laboratories v. United States* (1948), absence of evidence to the contrary, "the presumption of regularity supports the official acts of public officers, and courts presume that they have properly discharged their official duties" (para. Presumption of Regularity). They further state: "there is no rule requiring the prosecution to produce as witnesses all person who were in a position to come into contact with the article sought to be introduced in evidence" (para. 15). The court ruled the trial court did not err in allowing the two items into evidence (*Gallego v. United States*, 1960).

Authentication and State Cases

In the state system, the rules of evidence are guided by each states' rules of evidence statutes. For example, in Illinois, the rules of evidence are guided by the Illinois Rules of Evidence. Most states model their rules of evidence after the Federal Rules of Evidence (FRE). In Illinois, authentication and identification are covered in Article IX of the rules of evidence. Like the FRE, Rule 901 is the Requirement of Authentication or Identification and Rule 902 covers Self-Authentication (Illinois Rules of Evidence, n.d.). In Illinois, Rule 902 (12) Certified Records Generated by an Electronic Process or System and (13) Certified Data Copied from an Electronic Device, Storage Medium, or File are similar to FRE Rule 902 (13) and (14) (Illinois Rules of Evidence, n.d.). Just as we can look at Supreme Court and Federal Court of Appeals decisions to provide us guidance, we can also look to the state court system to provide guidance on dealing with authentication. In Illinois, *People v. Taylor* (2011) is the standard regarding video evidence.

Illinois and the *People v. Taylor*

In the state of Illinois, the Illinois Supreme Court provided guidance on admitting video evidence in *People v. Taylor* (2011). In case a hidden motion-activated surveillance camera caught a night watchman stealing from a desk in a locked office. The camera was set up by a detective, who then copied footage from the hard drive of the digital video recorder (DVR) to a VHS tape. The night watchman was identified by several co-workers and subsequently prosecuted for theft after admitting to stealing money in a police interview. During the trial, the detective testified to setting up the camera and making sure it was in proper working order. He also testified that he tested the equipment after the incident and found it to still be in proper working order. The detective further explained the motion activation feature of the camera and how the motion produced two video clips, one being twelve seconds and the other being eight seconds. The detective testified the thirty-second gap between the two recordings was due to the settings on the camera system that stops recording when it no longer senses motion. It was further explained the first video clip was of the defendant entering the office and squatting in front of the desk. The camera's motion sensors did not pick up any motion while the defendant was squatting down in front of the desk. The second clip caught the defendant standing back up and exiting the room.

After being found guilty of misdemeanor theft by the trial court, the defendant filed a motion to reconsider a new trial on the basis the State had failed to lay a proper foundation for the admission of the VHS tape. After citing *People v. Vaden* (2003), where "the appellate court noted that under the 'silent witness' theory, photographic or videotape evidence may be admitted without an eyewitness to establish the accuracy of the images depicted if there is sufficient proof of the reliability of the process that produced the photograph or videotape," the appellate court reversed and remanded. The Court ruled the State failed to lay a proper foundation for admission of the VHS tape because it was unable to establish reliability of the process that produced the tape. The State also failed to show proper chain of custody; the camera was working correctly, the original DVR recording was preserved, and it was unable to explain the process of copying the recording from the DVR to VHS tape. The Supreme Court reversed under the grounds the appellate court's reasoning was overly restrictive. The Illinois Supreme Court held the State did, in fact, lay a proper foundation for admission of the tape. The

Supreme Court noted most jurisdictions allow photographic and video evidence to be introduced as substantive evidence under the “silent witness” theory. Each case will present varying circumstances and foundation requirements for guaranteeing the genuineness of the evidence (*People v. Taylor*, 2011).

If we look closer at the decision by the Illinois Supreme Court, in this case, the court provided a lot of guidance for digital evidence. In providing analysis on the standard of review dispute, the court offered several cases that help understand how the court views video evidence. In *Cisarik v. Palos Community Hospital* (1991), the court pointed out videotapes were admissible on the same basis as photographs. In *People v. Smith* (1992), the court found that the admission of photographs was at the trial court's discretion. In *People ex rel. Sherman v. Cryns* (2003), the court noted that videotapes could be admitted into evidence when properly authenticated and expressly stated: “the admission of a videotape into evidence is within the sound discretion of the circuit court and will not be disturbed absent an abuse of discretion. Addressing chain of custody in *People v. Woods* (2005), the court noted: “chain of custody is used to lay a proper foundation for the admission of evidence...and a challenge to the chain of custody is an evidentiary issue.”

In reviewing the admissibility of videotape, the court provided a definition for the “silent witness” theory. When the photographs and videotapes are introduced as substantive evidence under the “silent witness” theory, they do so after a proper foundation has been laid out. A witness does not need to necessarily testify to the accuracy of a photograph or video footage as long as the accuracy of the process that produced that material is established with the proper foundation. In *People v. Taylor* (2011), the court admitted that they had not yet addressed foundational issues for establishing the accuracy of a process that produces surveillance camera recording evidence. They further note that other jurisdictions have set forth various relevant factors to consider. For example, in *State v. Harris* (2001), the court noted three factors for laying a foundation of authentication of photos taken by automated camera: “(1) system was reliable, (2) system was in working order when the photo was taken, and (3) film was handled and safeguarded properly from time it was removed from the camera until time of trial.” In *Washington v. State* (2008) the court found surveillance footage and photographs produced from surveillance equipment which was automatically operated admissible when “a witness testifies to the type of equipment or camera used, its general reliability, the quality of the recorded product, the process by which it was focused, or the general reliability of the entire system.”

The court understood the circumstances of each case, and the “requirements to guarantee the genuineness of the evidence will always differ” (*People v. Taylor*, 2011, para. 34). So even though the courts may set forth various factors in assessing the process that produces surveillance footage, those factors are not necessarily exclusive foundation requirements. The

PEOPLE V. TAYLOR (2011)

Several factors in determining whether a proper foundation had been laid:

- 1) the device's capability for recording and general reliability
- 2) competency of the operator
- 3) proper operation of the device
- 4) showing the manner in which the recording was preserved (chain of custody)
- 5) identification of the persons, locale, or objects depicted
- 6) explanation of any copying or duplication process (para. 35)

appellate court in *People v. Taylor* (2011) looked at several factors in determining whether a proper foundation had been laid:

- 1) the device's capability for recording and general reliability
- 2) competency of the operator
- 3) proper operation of the device
- 4) showing the manner in which the recording was preserved (chain of custody)
- 5) identification of the persons, locale, or objects depicted
- 6) explanation of any copying or duplication process (para. 35)

The court agreed with the appellate court's factors, however as they noted with other jurisdictions, they emphasized that the list of factors was nonexclusive. They wanted each case evaluated on its own, depending on the facts of the case. In some cases, some of those factors may not be relevant; in other cases, there may be a need to consider more factors (*People v. Taylor*, 2011).

State v. Sassarini (2019) - Oregon

This case involved a confrontation between neighbors that resulted in one neighbor recording part of the confrontation with a video camera. The neighbor then provided the police with a copy of the confrontation on a DVD which contained three files the day after the incident. The files would not play at the police station, so the neighbor provided another copy four days later. Sassarini filed a motion to exclude the evidence because it could not be authenticity of the chain of custody. During a hearing for an *in limine* motion, the neighbor identified the camera and the DVD that was booked into evidence. After the DVD was played in court, Sassarini argued the video she received in discovery was not the same video as the one played in court. The court discovered Sassarini's copy included the in-car camera footage that the police department had added to provide one single DVD containing all the

video footage. The neighbor further testified that the video footage played in court was the same footage as the original recordings on his camera. The neighbor further testified he had initially brought the camera's memory card to a third party to produce the copy for the police but did not alter the footage in any way. The police officer who responded to the scene and took custody of the DVD testified the video played in court was the same video that he observed at the neighbor's home. The officer also was unable to testify to what happened to the recordings between the time he watched the footage and the time he took custody of the DVD. The court ruled the state had presented a sufficient showing of authenticity and sent the footage to the jury. The Oregon Court of Appeals concluded the trial court correctly admitted the video into evidence under OEC 901 with sufficient evidence to authenticate the video.

Washington v. State (2008) - Maryland

Washington got into a verbal argument with another patron at a bar. After leaving the bar and returning, Washington asked the victim to step outside. Upon stepping outside, the victim was immediately shot, resulting in a spinal injury. Washington was subsequently arrested. At trial, the State introduced a videotape recording of the bar's surveillance cameras from inside and outside the bar. The bar owner testified to the number and placement of cameras and the operational setup of the camera. After the police requested to see the video, the owner testified he had a technician make a copy for the police. The officer investigating the case testified at trial as to what he observed in the video. Two other witnesses who were in the bar testified to the events they observed in the bar. The State did not call the technician who made the copy of the video from the system. The Court of Appeals ruled the video was inadmissible because the State failed to lay an adequate foundation as to the process that produced the copy of the video. The court further stated:

Because of the lack of extrinsic evidence showing under what circumstances the surveillance footage was transferred to a compact disc, the trier of fact could not reasonably infer the subject matter is what the State claims it to be and, thus, the videotape was not sufficiently authenticated. (*Washington v. State*, 2008, para. 19)

The State failed to authenticate the video because it was derived from an eight-camera system, was created by an unknown person, and from an unknown process without any testimony to how that occurred or to any chain of custody. This Court of Appeals remanded the case back to trial court for a new trial.

State v. Nieves (2013) – New Jersey

A resident called 9-1-1 after hearing gunshots and observing an individual lying on the ground. An officer from the Prosecutor's Office Crime Scene Technical Services Unit met the resident, reviewed the surveillance system, and copied footage to a disc of two people walking. The video shows light flashes from the shooting, and then a subject walk away. Detectives then meet with an owner of a bar where the bar's four exterior cameras were working. A detective viewed the footage taken during the time of the incident that the bar owner provided. The Detective was not aware of how the footage was extracted from the system, who extracted it, or

if any changes were made to it. A third set of recordings were recovered from another bar in the area. The video showed the victim and defendant talking inside the bar at an unknown date/time. The State's expert then created a composite video utilizing the three sources of video that had been recovered. The composite video was shown to the Grand Jury, which ended up indicting Nieves. The Defense expert argued the videos could not be authenticated because of the lack of the originals and lack of time stamps on the video. The judge granted the defense motion to bar admission of the tapes because they lacked probative value and didn't meet the fundamental requirements of admissibility under NJRE 901. The Appellate Division of The Superior Court agreed with the trial judge because the composite video was created from copies from several cameras that were not correctly time-stamped. Authentication would be impossible without an accurate timeline, without specifically eliciting a chain of custody because the originals were not taken, and without reliable identification as to "time, place, date, individuals and activities."

Commonwealth v. Connolly (2017) - Massachusetts

Connolly was arrested for assault and battery stemming from an altercation in an apartment building hallway. Connolly didn't deny the confrontation but argued it was self-defense. The State only produced one witness, a police officer who viewed surveillance footage of the incident that was recorded from inside the building. Unfortunately, the video was accidentally deleted before the defense had an opportunity to view the footage. The defense objected to the officer's testimony about the footage, but it was allowed at trial by the judge. The Appeals court found the State did not lay a proper foundation for authentication because it did not present evidence to show the video's date, time, or location. Further, the State did not call in the building manager to testify to the nature of the camera system, such as the placement of the cameras, the type of equipment, or how he came to view the footage. Therefore, the State did not establish a sufficient foundation for the jury to determine the video was what the officer claimed it to be. The Court found the Commonwealth would have to establish authenticity of the video with testimony from another individual in any retrial.

Law Reviews

Just as we look to the courts to provide guidance on how to deal with authenticating digital evidence in the everchanging world of technology, the discussions and ideas put forth in law reviews can also provide guidance. In *Law of the Foal: Careful Steps Towards Digital Competence in Proposed Rules 902(13) and 902(14)*, Facciola and Barrett (2016) discuss the difficulty the courts have in applying the Federal Rules of Evidence in modern times. The Federal Rules of Evidence was established to provide guidance on every evidentiary problem that may arise during a trial. However, they were initially established to deal with physical evidence such as DNA and fingerprints. 902(13) and 902(14) were established to help the courts deal with the virtual world of digital evidence. The Committee purposefully made 902(13) narrow to allow authentication of electronically stored information to avoid having to call in a witness. The committee provides an example of a photograph introduced in trial. Instead of calling in a witness to testify to taking the picture, the phone software captures metadata of things like the date, time, and GPS coordinates. This information is automatically generated due to a system that produces the same results every time. A party would only need to produce certification on

how the electronically stored information was created, transmitted, or stored to establish authenticity. In 902(14), the Committee made the rule on the premise that every piece of electronically stored information has a unique “hash value.” The “hash value” is a unique and random identifier that is compared to a digital fingerprint. Checking “hash values” allows for authentication of copies of evidence to the original to prove the evidence is what the proponent says it is. However, Facciola and Barret are concerned that courts may not further adjust rules to keep up with technology. They worry that the courts will accept certification and move on without challenging the process that produced the certification. For example, a breathalyzer produces a report that can be authenticated. However, the question of whether that process worked correctly or produced an accurate result should be evaluated (Facciola & Barret, 2016).

In their article, *Authenticating Digital Evidence*, Grimm et al. (2017) discuss how the new amendments 902(13) and 903(14) will change the way the courts authenticate digital evidence. They begin by emphasizing that authenticating digital evidence is the “same mild standard” as traditional forms of evidence. Before understanding digital evidence authentication, they first discuss FRE 104(a), which states: “the court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege” (p. 5). In essence, for most decisions about the admissibility of evidence, either digital or not, the decision must be made by the judge alone. The judge will be the sole decision-maker if the evidence is relevant, constitutes hearsay, is excessively prejudicial compared to probative value, the qualification of experts, and the extent of their opinion testimony, etc. The judge decides what evidence the jury may hear, and then it is up to the jury to weigh the evidence as they see fit. FRE Rule 104(b) qualifies 104(a) by providing the court with guidance on when the relevance of evidence depends on when a fact exists that must be proved later (Grimm et al., 2017). With the new self-authentication rules in 902(13) and 902(14), the burden of authenticity questions shifts to the opponent of the evidence. The opponent is still afforded the opportunity to challenge the certificate of authenticity, not the burden of proof. 902(13) and 902(14) provides the proponent of the evidence a more straightforward method to authenticate without reducing the standards for authentication. A certification under 902(13) and 902(14) establishes only that the proffered item has satisfied the admissibility requirements for authenticity (Grimm et al., 2017).

In recent times, some of the digital evidence being introduced at trial comes from police body-worn cameras (BWC’s) and private citizen footage from cell phones. One of the challenges arising in today’s climate is how do we authenticate digital evidence from these sources. In *Democratizing Proof: Pooling Public and Police Body-Camera Videos*, Fan (2018) discusses the importance of pooling public and police videos in an effort to solve crime. One of the issues with this concept is that only police videos are currently uploaded securely to the cloud, ensuring video integrity, chain of custody, and inclusion into the official record. On the other hand, public videos are often uploaded on the internet to places like YouTube, Facebook, Instagram, and other social media outlets. According to Fan, this presents challenges in authentication. Fan identifies

Fan identifies the following relevant factors from *McEntyre v. State* and *United States v. Munoz* which help in determining authentication of videos:

- 1) there have been no changes, additions, or deletions to the recording
- 2) the recording was preserved in a way that ensures its own integrity
- 3) the recording is correct and authentic
- 4) the device used to record was capable of capturing the relevant events
- 5) the person who recorded was competent to do so
- 6) the recording was made in good faith
- 7) participants on the recording are identified (Fan, 2018, p. 6)

the following relevant factors from *McEntyre v. State* and *United States v. Munoz* which help in determining authentication of videos:

- 1) there have been no changes, additions, or deletions to the recording
- 2) the recording was preserved in a way that ensures its own integrity
- 3) the recording is correct and authentic
- 4) the device used to record was capable of capturing the relevant events
- 5) the person who recorded was competent to do so
- 6) the recording was made in good faith
- 7) participants on the recording are identified (Fan, 2018, p. 6)

Also discussing the importance of body camera footage, Pike (2018) argues in her article, *When Discretion to Record Becomes Assertive: Body Camera Footage as Hearsay*, that evidence deriving from officer's body-worn camera should be evaluated differently from ordinary digital evidence due to the human element associated with body-worn cameras. Pike argues that even computers and forensic machines should be subject to more rigorous admissibility standards due to human coding and thus have a human element attached to them. She also believes there is a case for heightened standards for police body-worn cameras. She writes: "courts have repeatedly held that cameras- both manually and automatic- may be authenticated as a silent witness, body cameras represent a unique challenge to authentication that is distinguishable from cameras of the past" (Pike, 2018, p. 5). Body cameras are controlled by the officer, therefore relaying on direct human manipulation to work. They are also meant to provide an "officer perspective" of the incident. Security cameras result from computer coding that results in the camera either constantly recording or being activated by a specific automated process such

as motion. Body-worn cameras are triggered by a human response to human-recognized triggering events. Pike argues that body camera footage should then be viewed as hearsay evidence instead of demonstrative evidence (Pike, 2018). The above-listed articles identify that not all video evidence in the trial will come from surveillance cameras. Trials may have video evidence from surveillance cameras, body-worn cameras, or cell phone videos uploaded to social media. As the courts have attempted to keep up with technology with rules like 902 (13) and (14), the courts will have to continually monitor and evaluate technology and advances in video to ensure the rules of evidence stay relevant.

Best Practices

After utilizing the court decisions at the federal and state level and law reviews discussing current issues in digital evidence authentication, the experts can provide guidance in procedures and policy to help law enforcement stay up to date. The National Institute of Justice provides guidance for law enforcement when dealing with authentication of digital evidence in their report, *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors* (National Institute of Justice, 2007). The NIJ advises that key issues when dealing with authentication deal with showing that the evidence has not undergone significant changes. This can be done by providing chain of custody or through a witness with knowledge testimony to show the evidence is what it claims to be. The witness with knowledge who will testify must have personal knowledge of the facts they will testify to, but the witness “need not have been the programmer of the computer in question, have knowledge of its maintenance and technical operation, or have seen the data entered” (National Institute of Justice, 2007, p. 30). The NIJ provides an example of a computer seized from a defendant. The evidence could be authenticated by the investigating officer that seized the computer, who would show the computer was in the defendant’s possession and the examiner who recovered the files to show they were found on the same computer (National Institute of Justice, 2007).

In 2015, the NIJ put out another report titled: *Digital Evidence and the U.S. Criminal Justice System, Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence* by Goodison et al. This report looks at current trends in digital evidence recovery, legal issues, research, case discussion, and recommendations that help law enforcement navigate working with digital evidence. In October of 2016, the Bureau of Justice Assistance (BJA), in a collaborative effort with the Global Justice Information Sharing Initiative, issued a report, *Video Evidence: A Primer for Prosecutors*, acknowledged the change in video evidence in the court room over the last ten years. The report identified challenges using video evidence in prosecutions, the video-evidence process, and preparation tips for trial (Global Justice Information Sharing Initiative, 2016).

The Scientific Working Group on Digital Evidence (SWGDE) consists of members approved and voted in from all across law enforcement, the legal community, private industry, and academia. Members are involved in the digital and multimedia forensic profession and make up six committees that develop guidance documents and three administrative committees. The SWGDE releases documents that provide guidance, best practices, recommendations, and tech notes. Some of the documents produced by the SWGDE that may be beneficial to law enforcement in digital evidence include:

- Training Guidelines for Video Analysis, Image Analysis, and Photography
- Best Practices for Data Acquisition from Digital Video Recorders
- Best Practices for Digital & Multimedia Evidence Video Acquisition from Cloud Storage
- Best Practices for Archiving Digital and Multimedia Evidence
- Best Practices for Digital Forensic Video Analysis
- Guidelines & Recommendations for Training in Digital & Multimedia Evidence
- Best Practices for Maintaining the Integrity of Imagery

By keeping updated on the most recent court decisions, legal opinions, and industry standards, law enforcement can attempt to minimize future legal challenges to their investigations. The above listed material provides law enforcement agencies guidance in how to set up their policies and procedures to do that.

METHODOLOGY

To evaluate how various departments across the country follow best practice in the field of digital multimedia evidence (DME), the author created an evaluation rubric from multiple sources such as the organization Law Enforcement and Emergency Services Video Association International (LEVA) and the Scientific Working Group on Digital Evidence (SWGDE). The author also used best practices from other groups such as the National Institute of Justice (NIJ), Bureau of Justice Administration (BJA), and the Police Executive Research Forum (PERF). The author also relied on his professional experience working with digital evidence in his capacity as a Detective in a large urban police department located in the Midwest. The author is currently assigned to a technology unit tasked with provided technology support primarily in homicide investigations and shootings, robberies, burglaries, etc. Although the author is responsible for performing many job functions while assigned to the unit, the main emphasis is on collecting, extracting, and analyzing DME. In his current position, the author has received some of the training listed in the rubric and performs many of the functions and tasks listed in the rubric. Although this rubric may not address every possible best practice suggested by professional organizations, the author believes it covers most of them by using the premier organizations and authorities in digital evidence as guidance.

The primary source for the rubric came from LEVA and SWGDE because they are considered the preeminent authorities on digital evidence. LEVA was founded in 1989 and “serves as a key resource to the global public safety community by focusing on the needs of digital multimedia evidence disciplines by providing opportunities for professional development through quality training and informational exchange” (Law Enforcement & Emergency Services Video Association, n.d.). LEVA members come from all over the world and include international, federal, state, and local law enforcement, public safety, prosecutors’ offices, and private analysis. LEVA training consists of lecture and hands-on practical exercises that allow students to work with equipment and tools that are widely used in the field (Law Enforcement & Emergency Services Video Association, n.d.). LEVA also provides training that exposes students to the theory and principles considered best practices in Digital Multimedia Evidence (DME). A student who has completed and passed LEVA’s level 1 and 2 training courses can become a Certified Forensic Video Technician CFVT). Students who have completed and passed LEVA’s levels 1 through 4 training can become Certified Forensic Video Analysts (CFVA). Both a CFVT and CFVA require specialized training, but there are differences in handling digital evidence. Generally, a person who employs a Technical Function in processing DME, such as a CFVT, will follow a step-by-step process or procedure. A few examples of Technical Functions are:

- copy digital media
- convert digital media from one format to another
- print images from digital media
- archive data
- output data to an analog or digital medium
- resize digital images

- perform basic image adjustments
- time reference adjustments/calibrations (Law Enforcement and Emergency Services Video Association, UNK, p. 5)

Someone who performs Analytical Functions similar to the CFVA will require additional skills, education, experience, and training. This training allows them to exhibit a significant amount of judgment or opinion based on the product they produced from specific processes. A person who performs Analytical Functions can perform the tasks listed in Technical Functions but can also include:

- image Comparison or Photographic/Video Comparison such as comparing and contrasting known objects or persons to questioned objects or persons
- conduct image aspect ratio calibration
- color correction
- reverse projection
- photogrammetry
- motion tracking
- image stabilization
- media alignment
- audio/video alignment (Law Enforcement and Emergency Services Video Association, UNK, p. 5)

SWGDE also describes different job categories of responding personnel who may come across DME. Each job category may have a different name or responsibility from organization to organization depending on how they are defined and their involvement in handling digital evidence. However, SGWEDE identifies that these job categories often overlap. Training programs should be designed specifically for the tasks to be performed but may contain several job categories. The SWGDE job categories are:

- First Responder: Includes personnel who are the first to secure, preserve, and/or collect video, image, and photographic evidence at a crime scene. These personnel often have general crime scene evidence collection responsibilities.
- Field Photographer/Videographer: includes personnel who document and preserve conditions and evidence through photography or videography outside the laboratory.
- Technician: includes personnel whose primary responsibility is to collect and/or prepare video, image, and photographic evidence for examination and analysis.
- Laboratory Photographer: includes personnel whose primary responsibility is to document and preserve evidence through photography within the laboratory
- Examiner/Analyst: includes personnel for whom examination, analysis, and/or recovery of video, image, and photographic evidence is a major component of their routine duties. (Scientific Working Group on Digital Evidence, 2016, p. 6)

For this study, the author has chosen to analyze and evaluate police departments on their best practices under the job categories and duties of the First Responder and Technician.

Although departments may have separate job titles or defined roles for recovering DME, one specific job title will often be responsible for other tasks that do not fall under their primary responsibility. For example, a technician may be the First Responder while conducting their duties and, therefore, must have a basic understanding of the primary responsibilities of the First Responder. Vice versa, a First Responder, may find themselves being tasked to perform Technician duties due to circumstances outside their control. Well-written policy and procedure that provides officers with a proper, easy to follow guideline to follow best practices identified in the policy. The author chose to evaluate under the scope of these two categories because they most envelop the job description and duties the author encounters in his current position and, therefore, know those categories. The author also feels well-defined standard operating procedures can be the most useful to these two positions. They cover the broadest and general job descriptions of handling digital multimedia evidence.

LEVA follows guidelines and best practices identified and provided by the Scientific Working Group on Digital Evidence (SWGDE). On its website, SWGDE identifies itself as "bringing together organizations actively engaged in the field of digital multimedia evidence to foster communication and cooperation as well as to ensure quality and consistency within the forensic community" (Scientific Working Group on Digital Evidence, n.d.). SWGDE consists of six main committees "that develop guidance documents on the sub-disciplines within digital evidence." These six committees are the Audio Committee, Forensic Committee, Imaging Committee, Photography Committee, Quality Standards Committee, and the Video Committee. SWGDE's member organizations are a combination of public and private organizations such as various federal, state, and local law enforcement, prosecutor's offices, private tech firms, and even retail stores. SWGDE's members compose of individuals who have been approved and voted in from all levels of government, the legal community, private industry, and academia involved in the digital and multimedia forensic profession (Scientific Working Group on Digital Evidence, n.d.). In their bylaws, SWGDE states their purpose as: "to support and promote the advancement of the application of digital and multimedia forensics through the development and dissemination of consensus-based standards, guidelines, best practices, and recommendations. The Scientific Working Group on Digital Evidence brings together organizations actively engaged in the field of digital and multimedia evidence to foster communication and cooperation as well as to ensure quality and consistency in the forensic community" (Scientific Working Group on Digital Evidence, n.d.). SWGDE's objectives state they shall at a minimum:

- Define the scope and practice areas of the discipline of digital and multimedia evidence
- Recommend standard practices, protocols, reports, and terminology
- Recommend standards for data interpretation and wording of conclusions
- Recommend education, training, and continuing education requirements
- Promulgate and disseminate research and development priorities to the community
- Collect and distribute discipline-specific information on scientific foundation

- Seek international recognition and harmonization of appropriate SWGDE work products (Scientific Working Group on Digital Evidence, n.d.)

Along with the recommendations and best practices provided by LEVA and SWGDE, the author also chose to utilize best practices by agencies such as the Bureau of Justice Assistance (BJA), National Institute of Justice (NIJ), and Police Executive Research Forum (PERF). These reports consist of knowledge and input from law enforcement professionals from the federal, state, and local levels and prosecutors and private sector employees similar to LEVA and SWGDE.

Utilizing these various resources and rulings from the courts and discussions brought forth in the Law Reviews, the author has developed a rubric (See Appendix A) to evaluate how police departments follow current best practices when dealing with their digital evidence. The main focus of the rubric will be concentrated on how the departments' policies and procedures address the issue of authenticity of the evidence they handle. The author would like to identify where these policies and procedures either follow best practice to mitigate future challenges to authenticity or are not following best practice thereby creating an opportunity for future challenges to the evidence.

The author chose to evaluate police departments in three pivotal phases: Training, Methods, and Documentation. The author will evaluate how these departments' Standard Operation Procedure's (SOPs) and policies address the best practices identified by LEVA, SWGDE, etc., concerning these three areas. In looking at how departments prepare to handle digital evidence in the Preparation section, four key areas were identified: Outside Training, Internal Training, Continuing Education, and Equipment. For police departments that want to ensure their members are following the most current and common procedures in the forensic community, SWGDE recommends they follow the following training recommendations:

- Define and employ a quality assurance program for the implementation of a training program for the valid and reliable use of appropriate procedures.
- Training should include only the use of validated technologies and methods. Training should include awareness of and/or methods used for validating technologies.
- Commit to continuous learning in video, image, and photographic technologies and stay abreast of new findings, equipment, techniques, legal developments, and technological advances.
- Implement a program for continual assessment of employees' skills.
- Pursue professional development certificates (Scientific Working Group on Digital Evidence, 2016, p. 5).

SWGDE further identifies the different categories of training relevant to those individuals who deal with digital evidence or who supervise it as the following:

- Awareness: Training designed to provide the student with a general knowledge of the major elements of digital and multimedia evidence (e.g., video analysis, forensic audio, image analysis and computer forensics), including the capabilities and limitations of hardware and software.

- Skills and Techniques: Training designed to provide the student with the ability to competently use specific tools and procedures.
- Knowledge of Processes: Training designed to provide the student with an understanding of digital and multimedia evidence procedures and how to apply that understanding given various situations and sub-disciplines.
- Skills Development for Legal Proceedings:
 - Witness Testimony: Training designed to provide the student with the ability to present clear and non-technical digital and multimedia evidence-based testimony in court.
 - Forensic Results Preparation: Training designed to provide the student with the ability to prepare accurate and reliable documentation and/or visual aids (e.g., notes, reports, printouts, audio recordings).
- Continuing Education: Training designed to provide personnel with the ability to obtain the skills and knowledge of evolving technology in digital and multimedia evidence.
- Specialized Applications and Technologies: Training in specific sub-disciplines or in specialized areas (e.g., cell phones, image comparison, audio authentication, video optimization) (Scientific Working Groups on Digital Evidence and Imaging Technology, 2010, p. 5).

A digital evidence processing workshop completed in a joint effort by the Rand Corporation and PERF found clear support among the participants in the need to train investigators and all levels of staff, including patrol, detectives, and command staff. For example, training on handling and preserving digital evidence "at the academy level and as part of investigator training would promote better evidence preservation and limit seizing devices not relevant to an investigation (Goodison et al., 2015).

The author has separated training into three distinct areas: Outside Training, Internal Training, and Continuing Education. Outside Training would be training from outside agencies such as LEVA, other Federal, State, and local agencies, or private companies such as tech or software companies. SWGDE identifies this training to be beneficial in exposing officers to "new innovations and techniques, and assist with ensuring organizations are continuing to use best practices" (Scientific Working Group on Digital Evidence, 2016, p. 7). SWGDE further identifies other avenues to obtain outside training to encompass "conferences, trade shows, professional organizational memberships, professional publications, current literature, and specialized courses or workshops" (Scientific Working Group on Digital Evidence, 2016, p. 7). "Internal Training" is training within the department that is either available to all members or training specifically designed for units or members that deal specifically with digital evidence. According to SWGDE, this training provides personnel with the relevant knowledge necessary to perform job-related tasks" (Scientific Working Group on Digital Evidence, 2016, p. 6). SWGDE also identifies the importance of training under an experienced and competent practitioner to gain knowledge, experience, and improved skills (Scientific Working Group on Digital Evidence, 2016, pp. 6-7). Finally, the "Continuing Education" section will evaluate how departments provide further educational opportunities to keep up to date with the most current techniques and

procedures. SWGDE defines Continuing Education as "training designed to provide personnel with the ability to obtain the skills and knowledge of evolving technology in digital and multimedia evidence" (Scientific Working Groups on Digital Evidence and Imaging Technology, 2010, p. 5). Continuing Education can also be acquired annually from sources such as conferences, trade shows, professional organizational memberships, professional publications, current literature, and specialized courses (Scientific Working Groups on Digital Evidence and Imaging Technology, 2010).

The second section of Training will evaluate the equipment provided to members. This section will look at the equipment provided to members to help perform their duties, such as laptops, processing equipment, storage devices (USBs, DVDs), and digital cameras. SWGDE and the Organization of Scientific Area Committees for Forensic Science (OSAC) lists equipment they recommend that will assist in the acquisition of video from DVRs, such as portable computers, USB ports, extra monitors, and keyboards (Scientific Working Group on Digital Evidence, 2018, pp. 6-7) (Organization of Scientific Area Committees for Forensic Science, 2020, pp. 29-30).

TRAINING Phase				
	Outside Training	Internal Training	Continuing Education	Equipment
Notes:				
Other Observations:				
Score:				
Total Score:				

The next phase in the rubric will be the Process phase which will be broken into the following sections: Preparation, Methods of Extraction, and Chain of Custody. The Preservation section will evaluate steps taken before the actual physical extraction of evidence. Actions such as anticipating physical and logical barriers to the evidence, ensuring access to the system, removing bystanders, isolating the evidence from remote sources, and obtaining legal authority to recover the evidence will help ensure evidentiary integrity and the ability to review data (Organization of Scientific Area Committees for Forensic Science, 2020, pp. 7-9). The author will also evaluate if the departments identify the need to locate and preserve DME in crime scenes or provide procedures after discovering DME in crime scenes.

In the Method of Extraction section, how departments utilize the most effective extraction methods and steps taken to verify the integrity of the video will be analyzed. Ensuring their members are utilizing the most current and generally accepted extraction methods will ensure evidence satisfies any Frye or Daubert challenge. LEVA recognizes there is currently not an extraction or acquisition standard within the industry. The lack of standard results in the absence of a single best process for recovering DME (Law Enforcement and Emergency Services

Video Association, UNK). However, the SOPs will be evaluated on the information they provide their members in assisting them in this process.

Further factors to be evaluated will consist of steps taken during the extraction process to ensure the authenticity of the evidence, such as comparing the extracted data from the original data, verifying the correct date/time were recovered and the recovered evidence is playable (Organization of Scientific Area Committees for Forensic Science, 2020, pp. 8-21; Scientific Working Group on Digital Evidence, 2018, pp. 8-11). The author understands this may be the most challenging phase to evaluate due to departments not wanting to publish to the public investigative practices and procedures. The author will also be assessing if the SOPs provide direction or guidance to its members where they would be able to find more descriptive policies or procedures.

The final section to be evaluated under the Process phase is Chain of Custody. Once the evidence has been obtained, OSAC and SWGDE advise in initiating chain of custody according to the departments Standard Operating Procedures (Organization of Scientific Area Committees for Forensic Science, 2020, p. 22; Scientific Working Group on Digital Evidence, 2018, p. 11). Proper documentation and following SOPs on chain of custody will keep the authenticity and integrity of the evidence intact and begin during the extraction phase. The *Gallego* (1960) case provides guidance on the importance of maintaining a proper chain of custody. Like the Methods of Extraction, the author understands that every evidence handling procedure will be publicly available. The author will also evaluate how departments provide guidance on where to find a more descriptive chain of custody procedures. (See Figure B.)

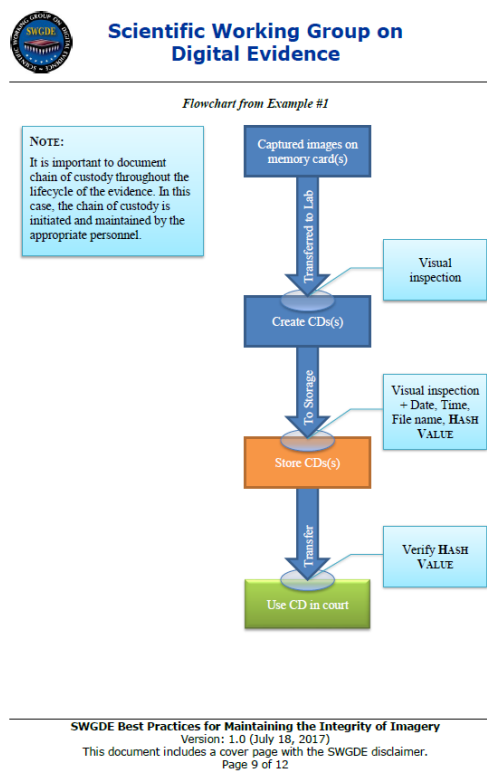


Figure B. SWGDE Image Integrity Workflow

PROCESS Phase			
	Preparation Steps	Method of Extraction	Chain of Custody
Notes:			
Other Observations:			
Score:			
Total Score:			

The final phase that will be evaluated in the rubric will be the Documentation phase. This phase will evaluate how departments document the steps taken during the Preparation and Process phase. This section will also assess how departments document the final disposition of the evidence, such as storage and report writing. The first section of the Documentation phase to be evaluated will be the Field Notes section. Proper field notes will help document important information such as location, points of contact, DVR make and model, serial numbers, date/time offset, number of cameras, and system settings. SWGDE also recommends taking photographs of the DVR system, cameras, and setup (Scientific Working Group on Digital Evidence, 2018, pp. 6-7). (See Figure C.)

The next section to be evaluated will evaluate the Final Reports produced from both the previous phases. Most of this information can be obtained through proper field notes. Along with information derived from the field notes, proper documentation of the chain of custody will also verify the authenticity of the DME. This can be accomplished by documenting when and where the evidence was collected, who owned the device, and had access to it. The report should address the chain of custody and document facts such as who had access to the evidence, who handled the evidence, and how it was stored (Goodison, Davis, & Jackson, 2015). Finally, the report should document any further evidence that was derived from the recovered DME. Final reports should also document any analytical techniques performed and should be thorough enough to allow a similarly trained person the ability the

Appendix A

Appendix A Sample Audio/Video Field Retrieval Worksheet

AUDIO/VIDEO FIELD RETRIEVAL FORM

Incident #: _____ Offense Type: _____

Location (Address): _____

Scene Point of Contact: _____

Scene Point of Contact Telephone Number: _____

Date & Time of Offense: _____

Date & Time of Acquisition: _____

Date & Time- Actual: _____ Date & Time- DVR: _____

DVR Recording Date & Time Difference to Actual (Time Offset): _____

DVR Type & Manufacturer: _____

DVR Model #: _____ DVR Serial #: _____

DVR Username: _____ DVR Password: _____

ADDITIONAL INFORMATION (IF AVAILABLE):

Earliest Recorded Date/Time: _____ Manual for DVR available? Y N

Storage Capacity: _____ Overwrite Enabled: Y N Firmware Version: _____

of Cameras Possible: _____ # of Cameras Attached to the DVR: _____ Cameras Exported: _____

Camera Resolution: _____ Camera Frame Rate: _____ Logs Present: Y N Logs Exported: Y N

Image Quality: High Medium Low Other _____ Camera Settings (e.g. alarm or motion triggered): _____

Starting Date & Time of Selection: _____ Ending Date & Time of Selection: _____

Media Backup Format: _____ Media Copied to: DVD CD Flash Drive Other _____

Notes:

• Native/proprietary video files should be the highest priority. • Verify video exported on a separate PC prior to leaving scene if possible. • Create a hash value for any video retrieved. • Begin Chain of Custody immediately. • Properly label and protect all electronic evidence. • Do not use ball point pens or stickers on CDs, DVDs, or other disc-based media. • Fill out as much information as you have available on this form. • Retain this form as part of the case file.

SWGDE Best Practices for Data Acquisition from Digital Video Recorders
Version: 1.0 (April 25, 2018)

This document includes a cover page with the SWGDE disclaimer.
Page 12 of 13

Figure C. SWGDE Sample Field Note Form

replicate the techniques and reach the same conclusion (Scientific Working Group on Digital Evidence, 2018).

The final evaluation will look at the final disposition of the evidence. SWGDE identifies the need to transfer any evidence stored on a temporary storage device to a permanent storage device (Scientific Working Group on Digital Evidence, 2018). It is best practice to have a policy that defines what data is to be archived and how long it will be retained. There should also be a system to identify how the department will store the evidence, such as using optical media or external hard drives. According to SWGDE (2020, p.5):

Management of a digital evidence archive is an active, ongoing process involving a set of policies, practices, procedures and tools that collectively ensure archived information is preserved, safeguarded and remains accessible and usable for its entire lifecycle, from acquisition to final disposition.

The author understands the policy of storing and accessing evidence typically is under the job duties of an “evidence section,” the author is looking for basic procedures in the SOPs such as storage options and documentation of storage along with evidence procedures.

DOCUMENTATION Phase			
	Field Notes	Final Reports	Evidence Disposition
Notes:			
Other Observations			
Score:			
Total Score:			

Data Analysis

The author will compare the different departments' results to evaluate where they measure in relation to the best practices identified by the above-mentioned organizations. The author chose to utilize a Likert scale from 1-5 to score how the departments' SOPs compare to best practices, with (1) being below average to (5) being above average. Having a continuum of responses, Likert-type scales assume the responses are linear and can be measured (McLeod, 2019). In this study, the author will score the evaluations by how above or below average the department's SOPs compare to the identified best practices.

Scoring Table				
1	2	3	4	5
Below Average	Slightly Below Average	Average	Slightly Above Average	Above Average

Overview of the Sample

The author utilized both purposive and convenience sampling to gather data for this analysis. The author utilized web searches on the internet to obtain various police department manuals, Standard Operating Procedures (SOPs), or policies. The web searches allowed the author to access the most easily accessible policies saving time and effort (Gray, 2014). The primary web source utilized in acquiring this information came from a webpage titled "Police Manuals" (Ciaramella, n.d.). This website contains various policies and procedures from 38 police departments across the country. Most entries have a hyperlink next to the city's name that re-directs the user to a department's website with their policies and procedures. A Google search for "police department policy and procedures" or "police department manuals" will return a listing for the "Police Manuals" website utilized in this report. All policies and procedures used in this report were open to the public. The author also utilized purposeful sampling to locate manuals that contained varying levels of thoroughness concerning DME in their policies. Gray (2014) identifies using purposive sampling when settings are chosen because they are known to provide important information. In choosing samples that varied in DME content, the author's goal was to identify disparity among police departments from their DME policy.

Six total departments were chosen based on their policy and procedures concerning Digital Evidence. 2 departments were selected to exhibit a Below Average level of thoroughness, 2 showed an Average level of thoroughness, and 2 revealed an Above Average level of thoroughness. The departments came from all over the country and vary in size of department members and size of the population they serve. All departments evaluated in this report had policies and procedures that were open to the public and accessible on the internet and through the "Police Manuals" website. The following departments were utilized in this study:

- Department A: a large urban department in the Mid-Atlantic region
- Department B: a large urban department in the Northeast
- Department C: a medium urban department located in the West
- Department D: a medium to large urban department located in the Southwest
- Department E: a large urban department located in the Northwest
- Department F: a large urban department located in the Southeast

Limitations

One of the limitations of this study is the small sample size. The author only chose to evaluate six departments from across the country, which does not accurately reflect every department throughout the country. There are numerous factors to consider when evaluating departments, such as the number of officers, size of the population it serves, size of the geographical area it covers, geographical location of the department, and many others that may be taken into consideration. A large, urban police department in the northeast may not operate the same way as a small, rural department in the southwest. Departments will have varying levels of resources available to them, affecting the staffing and equipment they can designate for items such as DME. Also, there are different types of departments such as municipal departments, sheriff's offices, state patrol or investigative agencies, and federal law

enforcement. This report does not account for differences among the various law enforcement agencies throughout the United States.

Another limitation in this study only evaluated open source policies and procedures that could be accessed through the internet. This allowed for convenience but did not result in a full and thorough evaluation of all policies, procedures, training bulletins, guidelines, or material available to the various members of the departments. Materials not open to the author may be more thorough and precise concerning digital evidence within the departments. The author also understands the need for departments to keep some policy and procedure accessible to only department members. While the lack of access to some materials may have hindered some of the research conducted in this study, the author utilized this opportunity to evaluate the accessibility of SOPs. A police officer who may find themselves in the middle of a crime scene with potential DME should have the ability to access SOPs regarding DME while on scene easily. This will help the officer follow best practices or give the officer the information to contact someone to provide guidance. A more thorough examination of all materials pertaining to policy, procedure, and digital evidence may have produced a different result.

A final limitation of this study was the subjective nature of the evaluation by the author. The author did not utilize a published or industry standard for evaluating the departments and their policies concerning Digital Evidence/DME. The author's evaluation method was based on the author's interpretation of based practices identified by industry leaders and the author's personal experiences handling Digital Evidence/DME. The findings in this report are the author's interpretations and evaluations of the policies and procedures. Due to the small sample size, not having access to all available materials, and the author's subjective review, this report lacks external validity and should not be generalized to all departments.

RESULTS

In looking at police department policies and procedures or Standard Operating Procedures (SOPs), the author began by looking for sections designated explicitly for Digital Multimedia Evidence or Video Evidence. If the author could not find specific DME SOPs or related SOPs, the author expanded the search to include anything Digital Evidence related. If there were no resources associated with Digital Evidence, the author then researched other SOPs involving evidence handling, forensics, crime scene duties, or follow-up procedures. Frequently when there were no stand-alone DME or Digital Evidence SOP, DME or Digital Evidence information could be found in one or some of these other SOPs.

Above Average Digital Multimedia Evidence SOPs

Having a stand-alone SOP on Digital Evidence provides easy access for department members to find information about Digital Evidence. Department A and Department B both had stand-alone SOPs specific to digital evidence. Department A has a Special Order titled “Digital Video Evidence Recovery (DIVRT) Kits,” S.O. XX-XX, while Department B has a “Digital Evidence” SOP listed under Directive X.XX. Both orders are specific to Digital Evidence and specifically to Digital Multimedia Evidence. Department A also has a special order titled “Requesting Video Evidence” S.O. XX-XX, but the order focuses more on requesting video footage from their CCTV system but still may provide some crossover with the DIVRT order.

Department A

Department A has many similarities to Department B when it comes to Digital Evidence SOPs. Department B has provided certain members of their department with Digital Video Evidence Recovery (DIVRT) Kits and has an SOP specifically for using those kits. Although there is beneficial information in the SOP, most of the information concerning Digital Evidence has to be gathered from other SOPs in their directives system. For example, they have separate SOPs specifically for Outside Training and In-Service training. The SOPs provide procedures for requesting training, procedures for records keeping after training, and duties for supervisors when outside training is requested. The outside training SOP also provides documents to request training as an attachment and

Digital Video Evidence Recovery (DIVRT) Kit Inventory

- Black Pelican 1500 Storage Case
 - Hard molded foam insert
- Software CD – Techsmith Camtasia Version 8.6.0 CD
 - License key, please specify: _____
- Resolution Video – Retrieval Kit Guide Book
- LawMate Personal Video Recorder (PVR) with battery and charger
 - Serial Number (located in battery compartment), please specify: _____
- Case Logic soft case containing
 - 512 MB Zip Drive
 - 2 GB Zip Drive
 - 8 GB Zip Drive
- Flashlight – Cree Hausbell
- Camera, please specify the model: _____
 - Serial Number, please specify: _____
- StarTech VGA to S-Video and Composite Video Converter
 - Serial Number, please specify: _____
- DVDs + RW
- CD-RW
- DVD+R
- CD-R
- Soft green carrying case containing
 - Blue – Network cable
 - Red – Network cable
 - USB small computer mouse
 - USB cable

 (DIVRT Kits)
 Attachment A
 DIVRT Kit Inventory

Figure D. Department A Equipment List

instructions for their members. The internal training SOP also provides procedures for requesting training, procedures for developing training, supervisor duties, and identifies mandatory 40-hour training yearly for sworn department members. The internal training SOP does not include any forms for actions such as requesting training or developing training. The training SOPs and the DIVRT SOP do not address Digital Evidence training specifically, which may be addressed in other directives that are not open source. Department is the only department evaluated for this report that had an SOP specifically for equipment related to Digital Evidence. The DIVRT SOP contains an inventory form as an attachment that lists all equipment associated with the kit. This equipment inventory list includes the cases, cables and connectors, USBs and DVD/CDs, a camera, flashlight, laptop, a LawMate Personal Video Recorder (PVR), and guide books. (See Figure D.)

Few preparation steps were dealing with digital evidence within the department's SOPs. The preparation steps in the DIVRT SOP identified steps in making sure the DIVRT kits were functional and operational before digital evidence retrieval. All other SOPs dealing with crime scene response, evidence collection, and criminal investigation provided general procedures with nothing specific to DME. When it comes to extracting DME, there is generic information in the DIVRT SOP, such as filling out forms and uploading recovered evidence. The retrieval documentation form does identify important information from the system that should be addressed during extraction: DVR make and model, number of cameras, and DVR offset. Similarly, when it comes to managing Chain of Custody, the DIVRT SOP does not contain specific sections concerning Chain of Custody. Still, the retrieval documentation form contains an entire "Audit Trail" section for documentation. The author was able to locate other SOPs detail the proper collection and handling of evidence that included a "general property record" form to document chain of custody.

Department A provides its members with a retrieval documentation form that is ideal for use as field notes. (See Figure E.) The form is a very descriptive 4-page document that includes all the relevant information needed in digital multimedia evidence recovery: make, model, serial number, date/time offset, number of cameras, passwords, etc. The DIVRT SOP does not detail procedures for final reporting, but there are other SOPs within the directives that detail procedures

DIGITAL VIDEO EVIDENCE RECOVERY KITS
RETRIEVAL DOCUMENTATION FORM

Name of Member _____
 Rank _____
 CAD _____
 Badge _____

Equipment Information:
 Make _____ Model _____
 Serial Number _____
 Number of Connected Cameras _____ Number of Connected Microphones _____

Type of Cameras Connected Analog Digital IP
 Display Connections BNC Composite RCA Composite HDMI
 VGA DVI
 Data Connections USB e-SATA Network
 Internal Devices Optical Disc Drive SD/ CF Card Slot Floppy Disk

System Settings:
 Current Date _____ Current Time _____
 System Date _____ System Time _____
 Calculated Offset _____
 User Name(s) _____
 Password(s) _____

Page 1

Figure E. Department A Documentation Form

for final documentation. These SOP's define procedures for documenting the uploading of video or who is responsible for final case files; however, they do not specifically mention procedures for final reporting on DME. Similar to final reporting SOPs, the DIVRT SOP identifies for its members related general evidence SOPs for proper inventorying procedures. These are general SOPs and do not contain specific information about digital evidence. Department A's numerous SOPs accessible to the public are very detailed; however, the author found that some were very outdated. There seemed to be a lot of information across numerous SOPs. It would be helpful to have more of the various details on digital evidence in one SOP.


Department B

Department B Directive X.XX scored very well in most sections of the Rubric created by the author. Department B had the most extensive training information in their SOP with a dedicated section titled "Required and Accepted Training" within Directive X.XX. The training section lists approved outside agencies for training in Digital Evidence and identified training that might come from interdepartmental sources. Although the directive does not list actual training courses, the directive specifies the need for training. It outlines the responsibility for Department B's Office of Forensic Science to keep up with industry standards and best practices. When it comes to the Equipment section, Department B was average in relation to the other departments. Directive X.XX didn't specifically itemize equipment available to members but did notate within the order, "All 'Department B' issued tools and equipment have been removed and collected." The directive advises "personnel that they will not exceed the scope of their training (i.e., DIVRT training covers the extraction of video from DVRs, not cell phones)," which tells the author that Department B personnel have access to equipment.

Department B Directive X.XX was very advanced compared to the other departments in relation to the Process section of the evaluation. Department B once again had a section titled "Preparing to Recover Digital Evidence." The directive identifies the need for personnel to obtain permission to access the device or have legal authority before recovering digital evidence. A "DE Recovery Form" (xx-xxx) and a "Recovery Log" (xx-xxx) are identified in the preparation section of X.XX. Throughout the entire directive, Department B identifies the need to canvas for digital evidence, the procedure for notifying the correct responding personnel, and who is authorized to recover digital evidence. When it comes to the extraction process in Directive X.XX, the directive also has a section titled "Recovery of Digital Evidence." Although most of this section appeared to the author to be more in line with computer-related evidence, the directive provides other valuable procedures such as photographing equipment before recovering, moving, or disturbing electronic devices. Department B identifies the need to follow the most current SOPs when recovering evidence due to the rapidly changing and evolving pace of technology. Department B also identifies the need to recover evidence in their "native, unaltered format" and document all procedures and actions taken when that is not possible. The directive then identifies procedures for requesting forensic examinations and the responsibilities of those conducting forensic examinations. Department B does a nice job of addressing Chain of Custody issues with digital evidence. All digital evidence is stored in their Digital Evidence Management System (DEMS), described as a virtual evidence room. It is a secure location for digital evidence with only authorized access. All user actions are logged and audited; all evidence has an audit

trail as well as receiving a hash value upon entry into the system. According to the directive, all data will be stored redundantly in case of a catastrophic system failure. The directive refers to “the most current SOPs for complete user information on DEMS” but did not give a directive/SOP number or a hyperlink to the SOP; therefore, the author could not access it.

Directive X.XX provides personnel with two Digital Evidence Recovery Forms, Form xx-xxx-Digital Evidence Recovery Form and Form xx-xxx-Digital Evidence Recovery Form (Digital Video). (See Figure F.) Form xx-xxx is the more generic form used on all digital evidence, while Form xx-xxx is more specific to Digital Multimedia Evidence. Form xx-xxx covers many of the vital information needed to recover Digital Evidence, such as make, model, serial number, username/password, DVR offset, number of cameras, and retention time. Along with providing the forms, the directive also provides instructions within the SOP on what information should be filled out by recovering personnel. The directive does not address final reporting procedures; however, with the information obtained in the field notes and recovery forms, most of the pertinent information needed for a final report will be easily accessible from these forms. Finally, along with the chain of custody information provided throughout the directive, there is a section titled “Retention and Purging.” This section assigns evidence disposition responsibilities to a “Digital Evidence Custodian” who will safeguard and manage “digital evidence created, collected, or otherwise utilized by the XXXXXX Police Department.” The section also identifies the need to conduct periodic audits and reviews of their DEMS system to ensure digital evidence is submitted, stored, and purged responsibly.



Digital Evidence Recovery Form
Appendix A (Digital Video)

DC#: _____ Recovering Party: _____

Make: _____ Model: _____ Serial Number: _____

User Name: _____ Password: _____

DVR System Date: ___/___/___ Time: _____

Official Date: ___/___/___ Time: _____

Reference Time Source: _____ Offset: + / - _____ days _____ hrs _____ min

Software / Firmware Version: _____ Retention Time: _____

Pixel Resolution: _____ Image Quality Setting: _____

Frames Per Second (FPS) _____ Motion Activated Recording: Yes / No

Network IP Address: _____ Subnet Mask: _____

Gateway: _____ Infrared (IR) Enabled: Yes / No

Number of Inputs / Cameras: ___/___ Player / Version: _____

Files Recovered: _____

Time	Actions Taken
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____


DIRECTIVE 

Figure F. Department B Retrieval Form

Average Digital Multimedia Evidence SOPs

Department C

In the previous two departments, we have seen strong examples of having well-written SOPs addressing Digital Multimedia Evidence. The following two departments demonstrate average SOPs where they are above average in some areas and below average in other areas. Department C has a specific digital evidence order titled “Recovering Digital Media Evidence.” This SOP touches upon a few of the essential topics related to digital multimedia evidence but is not as detailed as the previously analyzed departments. The order does not contain a training

section or define any training specific to digital evidence. The department does have a training SOP that contains standard training information. It defines inside and outside training, responsibilities for members seeking training, and responsibilities for training personnel. The SOP identifies forms to be filled out for actions such as requesting training. However, it does not provide an example of the form within the SOP or a hyperlink to the form. Regarding identifying equipment for digital evidence, the digital media evidence SOP does not have anything specific to digital evidence. The SOP identifies members from a criminal analysis unit to convert recovered video in a playable format that would require some equipment but does not explicitly mention which or what type of equipment.

In evaluating Department C's SOPs to the Process phase of the rubric, Department C's SOPs contain general procedures with few pertaining specifically to DME. In identifying preparation steps for recovering digital evidence, the digital media evidence SOP outlines the need for an investigator to accompany recovering personnel to the location of recovery. The investigator is also responsible for providing the date, time, and location of digital media evidence. The SOP also identifies the need for recovery personnel to recover digital media evidence in accordance with their training and best practices but does not provide any more information. The department has other SOPs that cover general crime scene and investigator responsibilities, chain of custody, and evidence handling procedures, but these SOPs do not contain information or policies specific to DME. According to the digital media evidence SOP, the Crime Analysis Unit is responsible for recovering digital evidence. Still, the author could not locate any SOPs pertaining to this unit in Department C's policy system. From the information provided from the various SOPs, the author could not find any procedure information concerning the extraction or chain of custody of DME.

When it comes to documenting field notes and final reporting, Department C's SOPs provide general information and do not provide a lot of detail. For example, the SOP identifies a recovery request form and a digital evidence recovery form but does not provide a copy as an attachment or a hyperlink. The author was unable to view these forms to evaluate their content. The SOP also identifies the need to document the recovery of digital evidence in police reports but does not provide specifics such as a format, required content, responsible personnel, etc. The SOP also identifies another specific SOP for a forensic report for computers and other digital evidence. Still, the link to view the SOP within the policy system was inactive. According to the digital media evidence SOP, the final disposition of evidence procedures can be found in a separate SOP which covers general evidence handling procedures. The forms identified in the digital evidence SOP may be comprehensive and contain good information that will allow recovery personnel to document the recovery in a very detailed manner. For having an entire SOP specific to digital multimedia evidence, the author felt it was too generic and not specific enough to DME.

Department D

Department D does not have an SOP specific to digital evidence or DME from what was available to the general public in their online policies and procedures webpage. An SOP that contained digital evidence information can be found in their SOP titled "Crime Scene Duties." Although it would be easier to have a stand-alone SOP specific to digital evidence, the SOP does

have specific sections related to the recovery of digital evidence. Similar to other departments, Department D has a separate SOP that covers all training within the department. Besides the initial training to be a licensed law enforcement member, Department D also identifies in-service training, roll-call training, specialized training, and career development. Most training is provided within the department but does allow for officers to seek training outside the department when it is beneficial to the member and not available through Department D. Department D has a Training Academy Online web portal, along with a Career Development Program through the portal which was restricted to members of the department. The author was unable to locate any information specific to training and equipment within the SOPs. The online training academy and Career Development Program may provide much more information to members that are not accessible to the public.

The Crime Scene Duties SOP contains two specific sections covering digital evidence: "Crime Scenes Where Video Recordings Are Made" and "Preservation of Digital Evidence." The "Preservation of Digital Evidence" section is more associated with recovering computers and computer-related equipment. Still, it does provide some reasonable preparation steps for dealing with all digital evidence, including digital multimedia evidence. The measures include having tech personnel on scene prior to executing a search warrant, guidelines for when officers first encounter digital storage devices, and documenting all actions taken when members manipulate devices. The "Crime Scenes Where Video Recordings Are Made" section provides some preparation steps before extracting evidence, such as contacting whoever is in charge of recording location and notifying a supervisor when denied access. The SOP offers very little information about the extraction process of digital evidence and reminds officers to maintain chain of custody when recovering video recordings. The latest update to the SOP was in 2014, but the author noticed the SOP repeatedly referred to VHS tapes throughout the SOP.

The Crime Scene Duties SOP lists referenced documentation forms but does not provide examples or hyperlinks. All other processes for documentation are generic and do not specifically mention DME. The only information the author was able to locate concerning documentation and digital evidence was in an SOP about digital photography. This SOP dealt with Department D's members documenting physical evidence or observable crime scene detail with the department's equipment. The SOP had some practical procedures for digital multimedia evidence such as documenting name and badge number of the person producing the evidence, the date and time it was put onto a storage device and distinguishing between the "master" copy and copies. However, this SOP was strictly related to Department D self-documenting crime scenes or other important circumstances of a case and not directly with digital evidence. Finally, when detailing the final disposition of evidence, the crime scene duty SOP describes the procedure for delivering master video recordings along with reports to a specific location within the headquarters building. For any other information concerning evidence handling, Department D members can look to other SOPs that supply generic evidence handling procedures but nothing specific to digital evidence. Department D did create a section within their crime scene duty SOP to provide information on recovering and handling digital evidence. Still, the information contained within the SOP was not very thorough. The SOP could use updating with its vocabulary, procedures, and documentation to be more effective.

Below Average Digital Multimedia Evidence SOPs

Department E

The last group of departments evaluated did not have any specific digital evidence SOPs or digital evidence sections within other SOPs similar to Department D's crime scene duty SOP. Department E did not have any specific SOPs or sections within an SOP that dealt directly with digital evidence. The author evaluated various SOPs within Department E's policy system for any SOPs that might contain any information concerning digital evidence. The author began by evaluating Department E's training SOP to check for any information that may be useful to training and digital evidence or DME. Department E's training SOP contained generic training information with nothing specific to digital evidence. The training SOP was similar to the other departments' SOPs, with general information provided about outside training, internal training, and continuing education. In looking at Department E's directive system, the author could not find any information that identified equipment in relation to digital evidence. There was one SOP within their system related to equipment, but the SOP was more specific to returning department-issued equipment upon separation from the department.

Continuing to look within Department E's SOP system, the author was also unable to find anything specific to digital evidence and the Process phase of the rubric. Since there was no SOPs specific to digital evidence, the author searched other SOPs such as crime scene investigation and homicide/investigation units for information that may be relevant to the process of handling digital evidence. Those SOPs identified steps for conducting investigations and procedures to follow were nothing concerning preparing, extraction, or handling digital evidence. The department had very detailed evidence handling SOP that provided procedures for maintaining chain of custody but did not include anything relative to digital evidence in the SOP.

While looking through the other SOPs within Department E's system, the author found various forms identified within those SOPs that are to be used by members when documenting investigations. These forms included basic incident reports to a summary of investigation reports. The author was unable to locate the content of these forms through the SOP system, a hyperlink was not included, and the forms were not provided as an attachment to the SOP. The author was able to find one mention of DME in an SOP detailing homicide investigation procedure. In that SOP, members were advised which items of the investigation file should be included. This identified items such as lab reports, interviews, crime scene sketches, autopsy reports, and "digital media." A definition of "digital media" was not provided, and the author was unable to locate any other sections within the SOP that mentioned "digital media." Just as in the chain of custody section, the author found very detailed SOPs concerning evidence handling and disposition, but nothing that specific to digital evidence.

The author found one SOP that had a promising title but was quick to find out that it did not provide the information relevant to this report. The SOP was about the department's video center, which is the city and department's CCTV system in public areas. This is the city and department run CCTV program and all the information provided was procedure in handling the CCTV system with no information about third-party digital evidence. The department also has an 11-page SOP for cybercrime. This SOP provides excellent information with the investigation,

recovery, handling, and storage of computer equipment. This SOP provides a lot of the information being sought for digital multimedia evidence acquisition but is almost entirely about computer-related equipment and does not provide information on video-related computer equipment such as DVRs. It would be easy for Department E to add information pertaining to DME to this SOP.

Department F

The evaluation of the final department's manual produced one SOP about photo evidence. The SOP states the policy applies to the creation and preservation of photographic evidence but does not define photographic evidence. From evaluating the SOP, the author felt the SOP was defining procedure for taking and handling photographs produced by department members. The beginning of the SOP states the policy addresses when members obtain digital photographic and video evidence from a third party; however, the information provided is highly minimal.

The only training brought up in the photo evidence SOP is the training employees will receive on Digital Single-lens Reflex (DSLR) camera systems and investigative photography techniques. Although this training may provide some beneficial information regarding digital evidence, this training appears to be designed to train members in the use of DSLR cameras to document crime scenes and evidence. The author looked at other training SOPs within the system, which provided information on external and internal training and continuing education. The author could not locate any training specific to the recovery or handling of digital evidence within the department's policies. For equipment provided to members to help with digital evidence, the photo evidence SOP identifies the DSLR cameras and smartphones, "department-supplied devices," and media cards. The SOP does not identify or further describe the department-supplied devices but states employees will use them to capture photographic evidence. Members are also provided with imaging processing software to help document crime scenes, but the SOPs do not identify the software.

When it comes to preparing for digital evidence, there is nothing in the department's SOPs to guide their members in preparation for digital evidence. There is also nothing in the SOPs when it comes to extracting or obtaining digital evidence. In the photo evidence SOP, there is a section for dealing with the collection of third-party photographs. However, this section only identifies that these photos can be uploaded to the Digital Evidence Management System (DEMS) and provides procedures for doing that. The photo evidence SOP does not address the issue of chain of custody when dealing with digital evidence. The author looked to evidence procedures within the department system and found the department's SOPs provide a link to the state patrol forensics services guide for proper evidence collection procedures. The state patrol guide provided detailed chain of custody procedures but nothing specific to digital evidence.

The photo evidence SOP does not provide any information in the documentation of photo evidence or procedures for final reporting on the evidence. The only form mentioned in the SOP was a photo media envelope used when submitting evidence from a media card when the DEMS system is not functioning. Looking through the SOPs for final reporting procedures revealed procedure stating case files must follow standards set forth by the States Attorney office with

nothing specific to digital evidence. The photo evidence SWOP primarily contains procedures for how members upload or enter their photo evidence in either their DEMS system, a DEMS web kiosk, or a third-party storage provider. The entire SOP primarily refers to photos or photographic evidence and does not mention video or any other digital multimedia evidence.

Further, the state patrol forensic services guide provides evidence submission and general guidelines for collecting, preserving, and packaging physical evidence. Still, it does not offer any specific procedure for digital evidence. The author was also able to find a state patrol “high tech crimes unit” section within the forensic services guide. Still, the unit only assisted departments with support and training in cell phones, computers, cameras, SD cards, and other digital storage devices. This unit within the state or other units with the department could provide digital evidence support, but the author was unable to find anything in the materials available online.

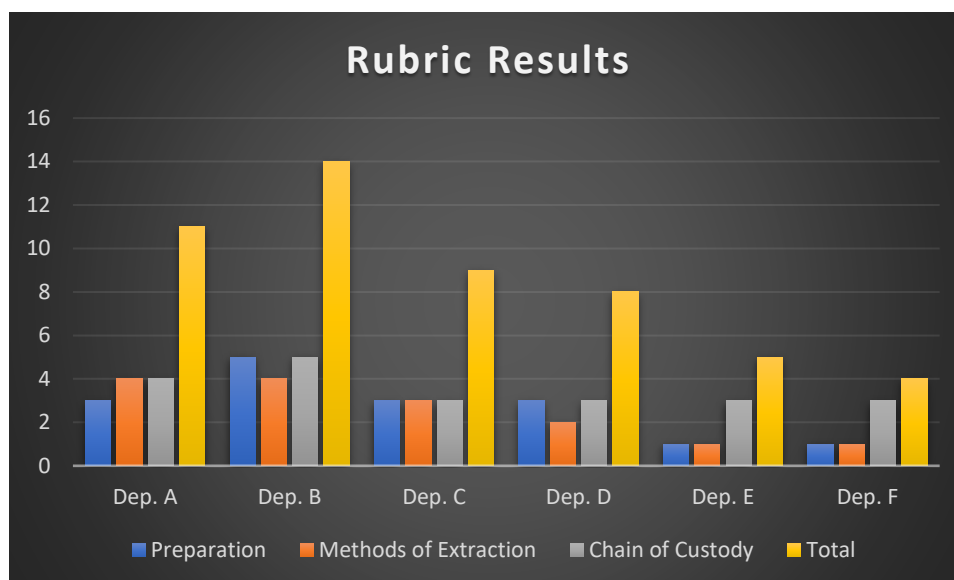


Figure G. Department Evaluation Results

DISCUSSION

This report aimed to identify best practices for handling digital multimedia evidence using federal and state rules of evidence, legal opinions, and industry leaders as a guideline. By comparing the best practices established by industry leaders with the guidelines put forth by the courts and legal opinions, the author will utilize the data from the evaluations to come up with recommendations. These recommendations will concentrate on best practices within police departments when creating SOPs for digital multimedia evidence. The author purposefully chose SOPs with varying degrees of thoroughness in their procedures for digital evidence to develop areas where SOPs need improvement and areas where SOPs are strong and can be used as an example for other departments. By having solid SOPs that comply with industry best practices, current legal requirements will allow departments to conduct better investigations, minimize court challenges, and stay up to date with technology that is constantly changing.

Digital Multimedia Evidence – Training

Evaluating the training procedures outlined in the department's SOPs, which are accessible to the public, was challenging. Understandably, departments may not list all training requirements, topics, or methods in general SOPs. Specific training material may be kept within a training unit. For example, DME training may be located in the Forensics Unit or in another unit responsible for handling digital multimedia evidence. In evaluating the six departments, Department A and Department B both included a fair amount of information about training in either their DME-specific SOP or general training SOP. Department B listed for their members outside agencies that the department approves for DME training. Department A has SOPs explicitly designated for outside training and internal training that provide information. The Department A outside training SOP even included forms for requesting outside training in the SOP. Department A and Department B both identified the need to continue education by stating the need to keep up with technological changes and stating the number of yearly training hours members are to receive. The department's commitment to putting these training requirements and information in writing shows they understand the importance of utilizing best practices identified by SWGDE.

Departments need to ensure their members are using validated technologies and methods and have an understanding of any new findings, equipment, techniques, and legal developments (Scientific Working Group on Digital Evidence, 2016). By having the training information listed in general training SOPs or the DME SOP, every member in the department can find information that may help them obtain the training needed to handle DME. As Goodison, Davis, and Jackson (2015) discovered in their workshop, all levels of staff need to be trained in DME. Good training information within either a DME-specific or training SOP will help provide all members the information needed to acquire such training. The other departments all had similar training SOPs that provided training information such as methods for requesting additional training, forms for requesting training, yearly training hours required, and even online training academy portals. These departments did not provide any training guidelines specific to

DME, so they were given a lower evaluation. However, if the author had more access to the training materials and SOPs, the departments' evaluations might be rated higher.

Training is significant in handling DME because the member handling the evidence may be called on to authenticate the evidence at some point during legal proceedings. The methods and techniques utilized by the member must be able to pass a *Frye* or *Daubert* challenge. Showing the court the training received by the member provided the member with up-to-date methods and techniques will help satisfy any *Frye* or *Daubert* challenge. In *Munoz*, one of the seven requirements for introducing evidence was the fact the operator was competent in the operation of the device. The court in *People v. Taylor* provided a similar requirement by looking at the operator's competency in deciding factors for a proper foundation. Training according to best practices in the operation of recording devices will show the members competency in handling the device and the evidence it produces. Further, the member may be called to trial to provide testimony as an expert witness under FRE 702. Proper training is the first step that will allow the member to prove they are qualified by their knowledge, skill, experience, training, or education (Cornell Law School, n.d.).

Just as training is essential to show the member is utilizing current best practices and techniques, the proper equipment utilized by the member is a critical component of handling digital evidence. Like training, it is understandable that departments might not list all equipment available to members in SOPs accessible to the public. Equipment may be further defined and detailed in unit-specific SOPs. Looking at the evaluations of the departments, some of the SOPs still provide helpful information that departments should utilize. Department A provides trained members with the Digital Video Evidence Recovery (DIVRT) kits and an inventory form with all equipment in the kit listed. This allows members to easily use a "grab n go" kit containing all the necessary equipment needed to handle DME. Along with an inventory checklist where members can visually confirm the equipment, the members will be fully equipped to handle DME in the field.

While analyzing the other departments' SOPs, the author was able to identify other equipment available to those departments' members that is beneficial in DME. Items such as stand-alone laptops and digital cameras to document crime scenes can be highly beneficial when working with DME. Laptops with admin privileges allow members the ability to download proprietary software to play videos. Digital cameras allow members to document the area where the video systems are located, the video system, and any identifying markings, date/time offset, and the display screen with the number of cameras and camera views. From personal experience, documenting these factors is very important. It allows a member the ability to check information such as date/time offset and camera view to make sure the evidence recovered is what was being sought after. Taking pictures allows the member, along with good field notes, to make sure the evidence they are acquiring is what they say it is to avoid any authentication challenges.

Digital Multimedia Evidence – Process

The Process phase begins with evaluating the preparation taken before the actual recovery of the evidence. It is essential to prepare to handle evidence by understanding what evidence is being sought, where the evidence is located, legal authority, and the timeframe to be recovered. SWGDE identified the need to obtain proper legal authority before seizing or acquiring video evidence and specifically mentions referring to organizational policy regarding requirements for obtaining authority (Scientific Working Group on Digital Evidence, 2018). Department B had an entire section within their digital evidence SOP directed at the preparation of digital evidence. It outlined the importance of identifying legal authority, evaluating the system, and determining the data to be recovered. Department C's SOP also identified the need for members to be provided the date, time, and recovery location. Proper preparation and understanding of what is to be recovered will provide the member with the information needed to ensure they minimize authentication issues in the future.

Other steps for preparation identified in the SO's that were not specific to digital evidence were the need to properly canvas crime scenes for evidence. Expressly, members should be advised in their SOPs the need to identify DME similar to the way they are trained to identify other forms of evidence such as fingerprints or DNA when responding to crime scenes. SWGDE recognized the importance of determining the physical location of the recording device, the date(s) and time(s) of interest, and any expected storage media needs before any acquisition (Scientific Working Group on Digital Evidence, 2018) (Scientific Working Group on Digital Evidence, 2021). By identifying locations of DME along with the necessary information about the location of the DME such as owner, availability for access, system info will provide responding personnel responsible for recovering the evidence the information needed to perform their duties. SWGDE (2021) also recommends being proactive by contacting businesses and citizens in high-volume call areas to build community relationships to expedite video recovery. In most of the SOPs detailing crime scene duties, the author observed that the SOPs did not specifically identify DME when looking for or protecting evidence in a crime scene.

The extraction phase of recovering DME is the first time members begin handling the evidence. The departments did not have very descriptive extraction procedures listed in their SOPs. Department A and Department B provided the best procedure by identifying the need to photograph the equipment, providing documentation forms to fill out during the extraction process, and identifying the need to extract the evidence using best practices and in the native format when possible. LEVA (n.d.) recognizes the need for SOPs to be sufficiently detailed but

not be so rigid that members are not allowed any flexibility. As we have seen from court cases such as *People v. Taylor* (proper operation of the device, explanation of the copying or duplication process), *State of Maryland v. Washington* (evidence not authenticated because an unknown person derived it by an unknown process), *State of New Jersey v. Nieves* (authentication not possible due to a lack of timeline and without reliable identification as to time, place, date, individuals and activities) and *Commonwealth v. Connolly* (did not lay a proper foundation for authentication because it did not present evidence to show the date, time, or location of the video), the extraction process is vital to proving the authenticity of the evidence.

Identifying basic procedures and best practices for extracting the DME will provide the member sufficient guidance to get the job done and allow them the flexibility to deal with any issue that may arise during the process. Members should have already received training to have the skills and techniques, and knowledge of processes that have been identified from best practices to effectively extract the evidence (Scientific Working Groups on Digital Evidence and Imaging Technology, 2010). A flow chart may be helpful in the SOP to allow members that do not have as much training as technicians to complete basic extraction methods when situations do not allow more trained personnel to do the extraction. A flowchart provides a visual aid providing members easy-to-follow procedure. (See Figure H.)

All departments contained Chain of Custody information within their SOP system, either in their DME SOP or in their general evidence handling SOPs. Department A had an audit trail section within their retrieval documentation form to document chain of custody. Department B's evidence storage system also contained an audit trail and logged user actions to help maintain the integrity of the video. *US v. Taylor and Hicks* (chain of possession), *US v. Gallego* (court does not have to produce all witnesses who were in a position to come into contact with evidence), *People v. Taylor* (showing the manner the recording was preserved), *State of Maryland v. Washington* (lack of testimony to chain of custody), and *State of New Jersey v. Nieves* (authentication not possible without explicitly eliciting a chain of custody) demonstrate the importance of establishing and documenting Chain of Custody.

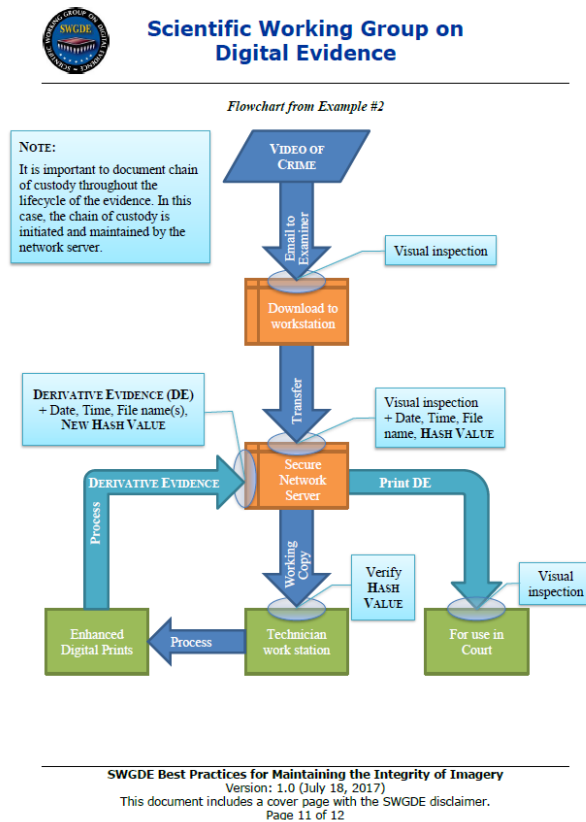


Figure H. SWGDE Workflow Example

Department B's SOP also assigned a hash value to all DME. Department B is creating the digital chain of custody by assigning a hash value that will help with any future challenges to authentication and integrity. The courts have recognized the accuracy and reliability of using Hash values in cases such as *Glassgow, Mikenvich, and Wellman*. Furthermore, SWGDE (2019) identifies the importance of integrity verification for maintaining chain of custody and recommends hashes be made as early as possible in the collection of evidence. By creating the hash value and starting the chain of custody, departments can verify any copies of the evidence and identify any changes made to the evidence.

Digital Multimedia Evidence - Documentation

Documentation is a crucial component to proper DME handling and recovery. Documentation connects all the other phases and processes and is essential for providing details that may be needed in the future. Good documentation in the form of field notes is also an integral part of completing any final reporting procedures. The SOPs that received the highest scores in the evaluations all provided a documentation form within the SOP. The documentation forms contained important information such as time offset, DVR make/model and serial number, number of cameras, retention time, general notes, and audit trail information. This aligns with the suggested items to be documented from SWGDE (Scientific Working Group on Digital Evidence, 2018) and OSAC (Organization of Scientific Area Committees for Forensic Science, 2020). Descriptive field notes allow for easier final report writing. The author has had to write numerous final reports where he relied on extensive field notes to complete the final report. Some reports consisted of multiple locations of recovery with DME produced from various sources. The ability to refer to well-documented field notes and also utilize pictures of the systems was beneficial. Most SOPs that were evaluated did not have specific final reporting procedures but mostly identified the need to document the facts of the case. Final reporting procedures may be covered in more detail in unit-specific SOPs so the author was not surprised to see very little information concerning final reporting.

Finally, when it came to the evidence disposition section of the Documentation phase, the highest-rated SOPs contained detailed policy on the responsibilities of evidence disposition. Department B's SOP identified a digital evidence custodian responsible for retaining, auditing, and purging the evidence. The SOP also identified the need to ensure all pertinent and viable evidence is adequately safeguarded. The other departments all had general evidence SOPs that discussed evidence disposition along with chain of custody. Due to the unique nature of digital multimedia evidence, such as the different ways it can be stored: optical disc, USB, hard drives, or cloud service, as well as issues such as the ability to access the evidence, it will be necessary for departments to have strong DME policies in evidence disposition and storage. SWGDE (2020, p.6) provides a summary of best practices for archiving DME:

1. Define in policy what data the organization requires to be archived for how long it must be retained
2. Have a system to keep track of what is in the archive, where it is stored, and for validating its integrity
3. Choose storage that appropriately meets the organization's needs
4. Have redundancy, preferably geographically dispersed

5. Have policy, plans, and procedures for:
 - a. Identifying personnel responsible for managing the archive
 - b. Adding data to the archive
 - c. Retrieving data from the archive
 - d. Ensuring archived content will be accessible when needed for full retention period
 - e. Removing data from the archive when no longer needed

One of the limitations of this report was the inability to access every SOP or policy manual from the departments evaluated. Only SOPs accessible through the internet, which didn't require any permission or special clearance, were used. It is understandable if departments do not want to make all investigative SOPs publicly available. Departments should consider identifying in their general SOPs where members can find all pertinent procedure information within department resources. During the evaluations, the author could not access specific procedures and forms because the hyperlink directed the author to a department login web. This would provide members direct access to material and would also ensure security for the materials.

Other Considerations

Following SWGDE, LEVA, government reports, and other industry leaders for best practices provides detailed guidance for handling DME. It is advisable to follow these guidelines; however, law enforcement personnel will have to balance the need to follow best practices and outside factors that are situationally dependent. Every case and every location where DME may be recovered is different. The members handling DME will have to balance the need to follow best practices along with the needs of home and business owners who may be providing access to their systems. Not every home or business owner will understand DME best practices and the actions taken by law enforcement personnel. It may appear to them that law enforcement personnel are damaging or changing their system in the process of recovery. They may not like their system info and/or personal info being documented and possibly photographed.

Business owners have to balance the need to run a business as well as assist law enforcement. The author has recovered DME in numerous businesses where the recording system was behind the counter or in public view of the customers. Anyone in the store could observe the author or any other law enforcement personnel while they were in the process of extracting DME. To avoid this, members can close the store or prevent access to certain areas of the store. But this may cause the business to lose customers or draw more attention to the store's assistance with law enforcement. Law enforcement personnel need to balance the need of the business owners with procedures for handling DME. In certain high crime areas, the business owners are more than willing to assist with law enforcement and balance the perception of helping the police from the community. Some businesses keep their video systems in the ceiling or other hard-to-reach areas to deter any equipment tampering. Sometimes the video systems are located in an office with other computer equipment or merchandise on top of it. Personnel should always attempt to leave the systems in the exact condition they found it. Therefore, it may be hard to take pictures of the information on the box without risking the possibility of moving and damaging equipment. The more extended law enforcement personnel are in a business, the longer they may be drawing attention to that business.

Similarly, homeowners may be worried about retribution from gangs or criminals for helping law enforcement. This may cause them to be hesitant to provide personal information or allow access to their system. The author has experienced situations where the offender(s) have lived on the block or next door to locations with video cameras. The author has had to recover DME from buildings where possible offenders were residing. Homeowners have requested the author come at certain times and take a particular path to get to the house. Proper preparation can sometimes alleviate some of these issues. Knowing what evidence is needed, such as date and time of occurrence and camera angles or numbers of cameras, can expedite the extraction process. Contacting businesses or homeowners if their information is known beforehand will provide them the opportunity to help when it is convenient for them. This also avoids wasting the members' time by heading to a location to discover they cannot get access to a system. The goal should be for law enforcement personnel to work with home and business owners on recovery procedures to maintain a positive relationship, so they continue to assist in future investigations.

Caseload may be another factor that affects the ability of members to collect, extract or analyze DME. Most departments evaluated in this report came from medium to large size departments from urban areas. Departments in large metropolitan areas with high crime rates will have different caseloads than small rural departments with low crime rates. Staffing and the number of members either trained or tasked with handling DME will vary from department to department. A department with a small amount of trained personnel that serves an area with high crime rates may have a different caseload than the smaller rural department with the same number of trained personnel. This is why it is important to have easily accessible and understandable SOPs to help when personnel that may not have a lot of training or experience with DME are given the task due to various situations. It is another reason why the SOPs should be "sufficiently detailed but not be so rigid as to not allow for flexibility" per LEVA (Law Enforcement and Emergency Services Video Association, n.d., p. 4).

The author works in a large urban department in an area with high crime rates. The author's location will often have nights when multiple homicides require a response. The members in the author's unit have to balance the need to respond to these crime scenes with the existing follow-up work for other homicide and violent crime cases. The author's unit may have to triage the amount of work due to caseload and staffing. We may not be able to recover DME and complete a full report all in one shift. A homicide investigation may contain numerous locations or multiple crime scenes that may take weeks to follow up. Various forms of DME may need to be recovered and compiled, such as surveillance video, Body Worn Cameras, red light/speed cameras, and third-party videos such as YouTube or video posted on social media. These situations present different challenges than responding to a burglary scene with a two-camera video system in a rural area. On the other hand, where the author has numerous members in his unit, there are officers in rural departments who are the only individual tasked with handling DME in either the entire town, city, county, or region. Allowing flexibility in SOPs will enable members to follow best practices and make decisions that best handle each case's different scenarios.

This report only looked at department SOPs concerning general handling of DME but did not go into the numerous types of DME or the nuances of handling each type. When creating or updating SOPs, it will be beneficial to consider all kinds of video recording systems and video sources in the world today. With the explosion in the use of social media, platforms such as Facebook, Instagram, and YouTube can provide information of evidentiary value. Newer surveillance systems targeting homeowners that utilize cloud technology have also seen a dramatic increase. Cloud-based systems such as Ring are providing homeowners with the ability to share video directly with law enforcement through email, text, or their applications like the Ring Neighbors App.

Additionally, SOPs should address other areas where DME can be obtained and provide material of evidentiary value. Red-light cameras, speed cameras, ATM cameras, and cellphone cameras all can capture evidence. These methods of capturing video must be addressed along with traditional forms such as DVRs.

One of the significant obstacles in properly handling DME within police departments comes down to money. It costs a lot of money to receive training, procure equipment, and keep up with all of the technological advances. It may be necessary for departments to obtain outside funding to help with all the costs associated with adequately handling DME if they do not already have systems in place. The Police Executive Research Forum (PERF) recommends pooling resources such as joining federal task forces and creating regional computer forensic labs or fusion centers to help smaller or rural departments that may not have the resources available to them (Police Executive Research Forum, 2018).

RECOMMENDATIONS

After reviewing the literature and evaluating the various departments' SOPs, the author offers the following recommendations to assist police departments in establishing best practices for the acquisition and handling of digital multimedia evidence in their SOPs. It is the author's recommendation to have a stand-alone SOP to deal specifically with digital evidence or DME; however, these recommendations should be taken into consideration for a stand-alone SOP or a specific DME section within another SOP.

Recommendation #1: Establish a training protocol to teach and maintain DME best practices

To keep up with the constantly changing world of technology, law enforcement personnel must understand the various technologies they will be working on. This begins with training and continues while working with DME to stay on top of the latest techniques and tools. The training should contain the categories identified by SWGDE's (2010, p.5) recommendations for personnel who collect, preserve, analyze, and/or examine digital evidence:

- Awareness
- Skills and Techniques
- Knowledge of Processes
- Skills Development for Legal Proceedings (Witness Testimony & Forensic Results Preparation)
- Continuing Education
- Specialized Applications and Technologies

By developing SOPs along these guidelines will help establish the competency of the members working with DME. This will help satisfy any questions as to the skills and abilities of the personnel handling DME. In cases where members may be called in as an expert witness, proper training help satisfy the standards outlined in FRE 702. Being trained and the ability to show certificates in current technologies will also help address any future *Frye* or *Daubert* challenges that may be brought up. Certifications of training and knowledge in currently accepted best practices by the member will go towards the admissibility of the evidence for either of these challenges.

The SOP should also address any procedure for members who may want to request future training. This may include attaching "request forms" for training, procedures for requesting training and having a list of approved training vendors or providers. Department B identified approved outside training vendors such as the International Association (IAI), LEVA, National Technical Investigators Association (NATIA), and the FBI Forensic Audio, Video and Image Analysis Unit (FAVIAU). In addition to these organizations, there are numerous others such as the Regional Computer Forensics Laboratory (RCFL), run by the Federal Bureau of Investigation; the National Domestic Communications Assistance Center (NDCAC), the National White Collar Crime Center (NW3C), the National Cyber Crime Conference and the National Computer Forensics Institute (NCFI,) run by the United States Secret Service. For a list of searchable training opportunities, departments can utilize The Law Enforcement Cyber Center, managed by the U.S.

Bureau of Justice Assistance (International Association of Chiefs of Police, n.d.). In addition to these organizations, private technology vendors also provide training and certificates in their technology to handle DME.

The SOP should not need to address every training aspect of working with DME but should be an available resource for any member who may have questions about DME training procedures. Goodison et al. (2015) identified the need to expand training to all department members and beyond the introductory level. This may avoid excess requests for evidence recovery and increase efficiency, improve evidence preservation and help manage expectations on how quickly evidence can be obtained. More formal training DME policy and procedure for work in a forensic lab or unit specifically tasked with working with DME should contain more detailed training SOPs. If we look at Department B's digital evidence SOP as a guide, the SOP identified an approved list for outside training vendors and identified who was responsible for keeping up with policy and procedures to be current with best practices. It also identified procedures for managing and recording any certifications/training received by members.

Recommendation #2: Provide easily accessible basic DME acquisition SOPs available to all members of the department

Not every item of DME will have the ability to be recovered or handled by a member who has been trained in the proper procedures in DME acquisition. Staffing, caseload, situational circumstances may require members who have minimal to no training in DME to be responsible to recover that evidence. It will be essential to have easy-to-follow general DME handling procedures for situations when trained personnel cannot respond. This should allow for a first responder who comes across evidence the ability to identify DME, document the essential information relative to the DME, attempt an extraction of the DME, understand any urgency of DME recovery such as retention time, as well as understanding the proper procedure for notifying the follow-up units. Some important areas to address:

- Retention time
- DVR make, model, serial number
- Number of cameras/camera angles
- Date/time offset
- Owner info
- Usernames/passwords

Identifying important extraction information will benefit the untrained members and assist them in getting information that will help responding follow-up personnel who have training. For the author, it is vital to get the evidence while the opportunity is available instead of waiting for follow-up personnel to make a recovery. Depending on circumstances, waiting may result in the loss of the evidence through data retention issues or human interference (deletion). Therefore, the SOP should provide basic procedures to allow for minimally trained personnel to identify DME and attempt an extraction or make notification to extract. The workflows provided in Appendix C provides a framework used as a template to help illustrate basic extraction procedures.

One issue that connects training and extraction methods is equipment. Department members should have the proper equipment to handle DME and be adequately trained in any specialized equipment they use. For General SOP guidance, the SOP should address everyday equipment needs for the extraction of DME. Items such as storage media (USB drives, optical disks), felt tip markers, extra mouse and keyboard, flashlight, and a department-issued smartphone to document DME equipment, could all be identified in SOPs. The SOP should also specify how the equipment can be utilized to collect, extract, and preserve DME. For departments, writing digital evidence unit-specific SOPs, more advanced equipment such as laptops, extra connection cables, keyboards, and monitors may be addressed. Any unit tasked with handling digital evidence will also require equipment for processing the digital evidence/DME, such as specialized computers, monitors, software with licenses, and storage solutions.

Recommendation #3: Provide documentation forms along with procedure for properly documenting DME acquisition

Proper documentation is a vital component in the collection, extraction, and preservation of DME. Documentation provides a record of the equipment the DME was extracted from, what methods were used, inventory procedures, etc. Proper documentation can also help with issues related to the ability to playback the video, chain of custody, and any future forensic analysis performed on the recovered material. Good documentation can address any issues as to the integrity or authentication of the video.

Documentation forms such as field notes or retrieval forms should be provided directly in the SOP as either an attachment or through a hyperlink. This will allow members easy access to forms and enable members to bring them into the field to utilize while working with DME. This allows the member to document in real-time and provides a guide on what information should be collected. The forms should contain all relevant information needed for extraction, such as make and model, retention time, username and passwords, date/time offset, and any other pertinent information deemed necessary by the department. These documentation forms will also assist in any future final reporting required of members working with DME.

Properly documenting chain of custody and providing a hash value to any recovered DME will speak to the integrity of the evidence. This is valuable in proving that a particular piece of evidence is the original and has not been altered in any way. There are times when evidence does need to be shortened, resized, or brightened for many reasons. Providing proper documentation to any changes made to the original evidence to allow a third party the ability to complete the same steps and get the same result will show the reliability of the data. Good documentation can provide important information as to the authenticity of the evidence. By documenting specific aspects of the acquisition like date/time offset, camera angles, and including pictures of the camera views and device information, will help show the data is what it purports to be. Utilizing hash values at the time of acquisition will help document the authenticity of the evidence and keep the integrity intact.

Recommendation #4: Secure funding to pay for training, equipment, and other operational needs.

The recommendations made in this report will not be cheap to implement. Training and equipment cost money. With municipalities tightening their budgets and other areas in the police department competing for budget money, additional funding sources will be needed. For example, LEVA's website lists its level 1 training costs at \$1,100.00 for law enforcement personnel and \$2,000.00 for private-sector employees (Law Enforcement & Emergency Services Video Association International, Inc., n.d.). Some organizations provide free training, such as NCFI and NW3C, but free training should not be the sole source.

Equipment is another significant expense with proper DME handling. Computer equipment built to handle the high volume of data processing will be required, and laptops for any fieldwork. Other equipment such as storage media, extra cables, monitors, keyboards, and other previously mentioned equipment will have to be supplied to members. Licensing will for any processing programs or equipment will also have to be accounted for. Members will also have to receive training to use any of these processing programs. It is also advisable to have a secure lab and workspace for members handling DME. This space will have to include features such as internet connection and security features to ensure the integrity of the evidence. Another option is to join partnerships with other agencies or tasks such as regional task forces to lower costs.

Archiving evidence can also be costly. SWGDE recommends utilizing online servers for large data volumes as well as third-party hosted storage. Online servers or networked storage require hardware, maintenance, and electrical/climate control costs to become very expensive. Hosted storage options have recently seen their prices reduced. However, the amount of redundancy and speed, and frequency of retrieval will involve recurring costs that will increase with the volume of the stored data (Scientific Working Group on Digital Evidence, 2020). Departments will also have to factor in these costs that may annually increase if the volume of data continues to grow.

CONCLUSION

The video of the death of George Floyd provided a powerful account of the incidents from May in 2020. Along with the other available video from that night, the evidence against Derek Chauvin was overwhelming. This case highlights the importance of identifying and recovering video evidence from crime scenes. It can be such an essential part of the evidence that police departments should be handling video or Digital Multimedia Evidence (DME) with techniques and procedures with best practices that industry leaders recognize.

The constant changing of technology presents a challenge for the courts and legal system to keep up. When the technology that produces the evidence is changing rapidly, how do departments prepare their members for these changes? Having strong, flexible Standard Operating Procedures (SOPs) helps address the change that is constantly occurring with technology. This study identified several important areas in collecting and handling DME by evaluating industry best practices along with current legal guidelines. Several recommendations were made to guide police departments in developing SOPs to address those issues. While the recommendations are a beginning to the proper handling of DME, the author feels further research is needed to keep up with the constantly evolving world of technology.

REFERENCES

- Authentication*. (n.d.). Cornell Law School - Legal Information Institute:
<https://www.law.cornell.edu/wex/authentication>
- Ciaramella, C. (n.d.). *Police Manuals*. <https://policemanuals.neocities.org/>
- Cisarik v. Palos Community Hospital*, 144 Ill 2d 339 (1991)
- Commonwealth v. Connolly*, 78 N.E.3d 116 (Mass. App. Ct. 2017)
- Daubert Standard*. (n.d.). Cornell Law School - Legal Information Institute:
https://www.law.cornell.edu/wex/daubert_standard
- Facciola, H. J., & Barret, L. (2016). Law of the foal: Careful steps towards digital competence in proposed rules 902(13) and 902(14). *Geo. L. Tech. Rev.* 6(2016), 6-16.
- Fan, M. D. (2018, June). Democratizing proof: Pooling public and police body-camera videos. *North Carolina Law Review*, 1-18.
- Fourth Amendment*. (n.d.). Cornell Law School - Legal Information Institute:
https://www.law.cornell.edu/constitution/fourth_amendment
- Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923).
- Frye v. United States-Case Brief For Law Students*. (n.d.). Case Briefs:
<https://www.casebriefs.com/blog/law/evidence/evidence-keyed-to-fisher/lay-opinions-and-expert-testimony/frye-v-u-s/>
- Gallego v. United States*, 276 F.2d 914 (9th Cir. 1960)
- Global Justice Information Sharing Initiative. (2016, October). *Video Evidence: A Primer For Prosecutors*. Retrieved from Bureau of Justice Assistance:
<https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/final-video-evidence-primer-for-prosecutors.pdf>
- Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. Rand Corporation.
- Gray, D. E. (2014). *Doing Research in the Real World*. Sage Publications.
- Grimm, P. W., Capra, D. J., & Joseph, G. P. (2017, Winter). *Authenticating Digital Evidence*. *Baylor Law Review*, 1-55.

Illinois Rules of Evidence. (n.d.).

<http://www.illinoiscourts.gov/SupremeCourt/Evidence/Evidence.htm#901>

International Association of Chiefs of Police. (n.d.). *Training and Conferences*. IACP Law

Enforcement Cyber Center. <https://www.iacpcybercenter.org/training-and-conferences/>

Law Enforcement & Emergency Services Video Association International, Inc. (n.d.).

<https://www.leva.org/>

Law Enforcement and Emergency Services Video Association. (2010, April 14). *Best Practices for the Acquisition of Digital Multimedia Evidence*.

<https://legaltekix.com/images/LEVA%20Best%20Practices%20for%20the%20Acquisition%20of%20Digital%20Multimedia%20Evidence%20.pdf>

Martin, D. (2018, Feb). Demystifying Hash Searches. *Stanford Law Review*, 70(2), 1-35.

McEntyre v. State, 717 S.W.2d 140 (Tex. App. 1986)

McLeod, S. (2019, August 3). *Likert Scale*. Simply Psychology.

<https://www.simplypsychology.org/likert-scale.html>

National Institute of Justice. (2007). *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors*. Washington D.C.: National Institute of Justice.

Organization of Scientific Area Committees for Forensic Science. (2020, June). *Standard Practice for Digital Retrieval from Digital CCTV Systems*.

Orrick, W. D. (n.d.). *Best Practices Guide: Developing a Police Department Policy-Procedure Manual*. International Association of Chiefs of Police.

<https://www.theiacp.org/sites/default/files/2018-08/BP-PolicyProcedures.pdf>

Pasadena Research Laboratories v. United States, 169 F.2d 375, 381-382 (9th Cir. 1948)

People ex rel. Sherman v. Cryns, 203 Ill 2d 264, 284 (2003)

People v. Smith, 152 Ill. 2d 229, 263 (1992)

People v. Taylor, 2011 IL 110067 (2011)

People v. Taylor, 398 Ill. App. 3d 74

People v. Vaden, 336 Ill. App. 3d 893 (2003)

People v. Woods, 214 Ill. 2d 455, 471 (2005)

Police Executive Research Forum. (2018). *New national commitment required: The changing nature of crime and criminal investigations*. PERF.

Pike, N. F. (2018, Summer). When discretion to record becomes assertive: Body camera footage as hearsay. *Vanderbilt Journal of Entertainment and Technology Law*, 1-19.

Rule 702-Testimony by an expert witness. (n.d.). Cornell Law School - Legal Information Institute. https://www.law.cornell.edu/rules/fre/rule_702

Rule 901. Authenticating or identifying evidence. (n.d.). Cornell Law School - Legal Information Institute. https://www.law.cornell.edu/rules/fre/rule_901

Rule 902. Evidence that is self-authenticating. (n.d.). Cornell Law School - Legal Information Institute. https://www.law.cornell.edu/rules/fre/rule_902

Rule 1001. Definitions that apply to this article. (n.d.). Cornell Law School - Legal Information Institute. https://www.law.cornell.edu/rules/fre/rule_1001

Rule 1003. Admissibility of duplicates. (n.d.). Cornell Law School - Legal Information Institute. https://www.law.cornell.edu/rules/fre/rule_1003

Scientific Working Group on Digital Evidence. (n.d.). <https://www.swgde.org/>

Scientific Working Group on Digital Evidence. (2021, January 14). *SWGDE Guidelines for Video Evidence Canvassing and Collection.* <https://www.swgde.org/documents/published>

Scientific Working Group on Digital Evidence. (2020, September 17). *SWGDE Best Practices for Archiving Digital and Multimedia Evidence.* <https://www.swgde.org/documents/published>

Scientific Working Group on Digital Evidence. (2019, September 29). *SWGDE Position on the Use of MD5 and SHA1 Hash Algorithms in Digital and Multimedia Forensics.* <https://www.swgde.org/documents/published>

Scientific Working Group on Digital Evidence. (2018, April 25). *SWGDE Best Practices for Data Acquisition from Digital Video Recorders.* <https://www.swgde.org/documents/published>

Scientific Working Group on Digital Evidence. (2018, November 20). *SWGDE Best Practices for Digital Forensic Video Analysis.* <https://www.swgde.org/documents/published>

Scientific Working Group on Digital Evidence. (2017, July 18). *SWGDE Best Practices for Maintaining the Integrity of Imagery.* <https://www.swgde.org/documents/published>

Scientific Working Group on Digital Evidence. (2016, February 8). *Training Guidelines for Video Analysis, Image Analysis and Photography.* SWGDE. <https://www.swgde.org/documents/published>

Scientific Working Group on Digital Evidence and Imaging Technology. (2010, January 15). *SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence.* <https://www.swgde.org/documents/published>

Sixth Amendment. (n.d.). Cornell Law School - Legal Information Institute.
https://www.law.cornell.edu/constitution/sixth_amendment

State v. Harris, 55 M.J. 433, 439-40 (C.A.A.F. 2001)

State v. Nieves, DOCKET NO. A-2034-12T3 (N.J. Super. Aug. 15, 2013)

State v. Sassarini, 452 P.3d 457, 300 Or. App. 106 (Or. Ct. App. 2019)

U.S. v. Munoz, 324 F.3d 987 (8th Cir. 2003)

U.S. v. Rembert, 863 F.2d 1023 (D.C. Cir. 1988)

United States v. Blackwell, 694 F.2d 1325 (D.C. Cir. 1982)

United States v. Glassgow, 682 F.3d 1107 (8th Cir. 2012)

United States v. McMillan, 508 F.2d 101 (8th Cir. 1974)

United States v. Miknevich, 638 F.3d 178 (3rd Cir. 2011)

United States v. Stearns, 550 F.2d 1167 (9th Cir. 1977)

United States v. Taylor, 530 F.2d 639 (5th Cir. 1976)

United States v. Wellman, 663 F.3d 224 (4th Cir. 2011)

Washington v. State, 406 Md. 642, 961 A.2d 1110 (Md. 2008)

When and How to Use Secondary Sources and Persuasive Authority to Research and Write Legal Documents. (2004). The Writing Center at Georgetown University Law Center.

<https://www.law.georgetown.edu/wpcontent/uploads/2018/02/secondarysources.pdf/>
2

APPENDICES

Appendix A – Evaluation Rubrics

Methodology Form: _____

TRAINING Phase

	Outside Training	Internal Training	Continuing Education	Equipment
Notes:				
Other Observations:				
Score:				
Total Score:				

PROCESS Phase

	Preparation Steps	Method of Extraction	Chain of Custody
Notes:			
Other Observations:			
Score:			
Total Score:			

DOCUMENTATION Phase

	Field Notes	Final Reports	Evidence Disposition
Notes:			
Other Observations			
Score:			
Total Score:			

Final Score: _____

Methodology Form: Department F

Training Phase				
	Outside Training	Internal Training	Continuing Education	Equipment
Notes:	-Have a training SOP that defines outside or external training -identifies request procedure outside training -nothing specific to DME	-Training SOP also identifies internal training -nothing specific to DME	-Training SOP (nothing specific to DME) -defines "Roll Call" and "In-Service" Training	-nothing specific in SOPs in relation to DME
Other Observations:	-Training SOP is detailed but generic, no specific mention of DME			
Score:	3	3	3	1
Total Score:	10			

PROCESS Phase			
	Preparation Steps	Method of Extraction	Chain of Custody
Notes:	-Nothing DME specific in SOPs	-Nothing in SOPs about DME	Very good detailed description of Chain of Custody in SOP but nothing specific for DME
Other Observations:	-SOP about Crime Scene Investigation discusses developing an investigative plan, outlining specific responsibilities for processing crime scene but nothing DME specific		
Score:	1	1	3
Total Score:	5		

DOCUMENTATION Phase			
	Field Notes	Final Reports	Evidence Disposition
Notes:	-nothing about field notes and nothing specific to DME	-SOP identifies need to list evidence -identifies what should be in report but nothing specific to DME	-General evidence SOP but nothing specific to DME -detailed description of Chain of Custody
Other Observations	-Crime Scene Investigation APD.SOP .3081 has an entire section about Photographs and Videotape Information but it only discusses photo/video taken by APD personnel of crime scenes -should add hyperlinks to forms		
Score:	1	2	3
Total Score:	6		

Final Score: 21

Methodology Form: Department A

TRAINING Phase				
	Outside Training	Internal Training	Continuing Education	Equipment
Notes:	-Entire SOP on requesting outside training -includes forms for requests -not DME specific	-Whole SOP on in-service training -not DME specific	-SOP states members should receive at least 40 hrs of training yearly	-Dept issues DIVRT kits to members -kit includes a large amount of equipment -also have stand-alone laptops -DIVRT kit inventory form
Other Observations:	-DIVRT (Digital Video Evidence Recovery) Kit -Also have a LawMate PVR (Personal Video Recorder) to obtain DME			
Score:	4	3	3	5
Total Score:	15			

PROCESS Phase			
	Preparation Steps	Method of Extraction	Chain of Custody
Notes:	-a few preparation steps -mostly deals with getting DIVRT kits ready -SOP dealing with the management of Criminal Investigations is outdated (1987)	-Documentation form identifies Make, Model, # of cameras, DVR offset which is consistent with best practices -No written process in policy	-have a "Audit Trail" section in the Retrieval Documentation Form
Other Observations:	-SOP provides officers with location of forms to request video		
Score:	3	4	4
Total Score:	11		

DOCUMENTATION Phase			
	Field Notes	Final Reports	Evidence Disposition
Notes:	-DIVRT SOP provides officers with the Retrieval Documentation Form -very descriptive, 4 pages -also a PD81 form, Property Record Form	-SOP identifies process of uploading video and how to document -Identifies a "Crime Scene Examination Case File" that would have all relevant reports included -No specific mention of DME	-DIVRT SOP directs reader to Evidence SOP for proper inventory procedures -General Evidence SOP, nothing else specific to DME
Other Observations	-A lot of information across numerous SOPs, would be nice to have DME pertinent information located in one SOP.		
Score:	5	4	4
Total Score:	13		

Final Score: 39

Methodology Form: Department C

TRAINING Phase				
	Outside Training	Internal Training	Continuing Education	Equipment
Notes:	-Have a training SOP that defines outside or external training -identifies dept form to request outside training -nothing specific to DME	-Training SOP also identifies internal training -nothing specific to DME	-Training SOP (nothing specific to DME) -defines "Roll Call Training"	-nothing specific in SOPs in relation to DME -Recovering Digital Media Evidence SOP discusses Criminal Analysis Unit (CAU) having ability to convert video, must have some equipment/programs
Other Observations:	-Recovering Digital Media Evidence SOP states CAU members who have been trained are allowed to convert. Only mention of DME/training together in SOPs			
Score:	3	3	3	2
Total Score:	11			

PROCESS Phase			
	Preparation Steps	Method of Extraction	Chain of Custody
Notes:	-SOP outlines role of Investigator to provide info to recovery personnel -SOP identifies need to provide date, time, location of DME recovery -SOPs cover general crime scene/investigator responsibilities, nothing DME specific	-SOP identifies the need to recover DME per training and best practices -nothing specific to what training is or best practices	-SOP covers general Chain of Custody procedures -nothing specific to DME
Other Observations:	-HPD has an entire SOP called "Recovering Digital Media Evidence" (SOP 1.17) but not as thorough for being an entire SOP specific to DME, could add more info -Have a Crime Analysis Unit but unable to locate SOP or info about it -Have a SOP 8.13-Handling of Evidence but unable to gain access		
Score:	3	3	3
Total Score:	9		

DOCUMENTATION Phase			
	Field Notes	Final Reports	Evidence Disposition
Notes:	-SOP identifies Digital Multimedia Evidence Recovery Form HPD-503 but unable to access -should add hyperlinks directly to SOPs for forms	-SOP identifies need for documenting recovery of DME in police report but not specific	-General evidence SOP but nothing specific to DME
Other Observations	-Does identify "Crime Analysis Request Form" HPD-107B and Computer & Digital Forensic Report SOP 8.18 but unable to access, should add hyperlinks to forms		
Score:	4	3	2
Total Score:	9		

Final Score: 29

Methodology Form: Department B

TRAINING Phase				
	Outside Training	Internal Training	Continuing Education	Equipment
Notes:	-Identifies outside agencies approved for training in DME	-Digital Evidence SOP repeatedly mentions training -identifies that some training will be done through inter-departmental channels	-SOP identifies the importance of keep up with technology with changes at a rapid pace	-SOP mentions "PPD issued tools and equipment" in regard to recovering DME but does not list specific equipment
Other Observations:	-SOP identifies DME as possible evidence at crime scene -SOP identifies procedure for managing and recording certifications and training related to DME -SOP identifies responsibility of Office of Forensic Science (OFS) to keep policies and procedures up to date and compliant with current best practices -Ensures will keep an "Approved Training List" -SOP mentions DIVRT technicians and FVA's but does not mention specific training or equipment they may have			
Score:	5	5	5	3
Total Score:	18			

PROCESS Phase			
	Preparation Steps	Method of Extraction	Chain of Custody
Notes:	-SOP identifies need for legal authority before recovering DME -identifies procedure for "responding personnel" to canvas crime scene for Digital Evidence and look specially for digital surveillance systems -identifies only trained personnel are authorized to recover DME -has entire section titled (Preparing to Recover Digital Evidence)	-entire section titled "Recovery of Digital Evidence" -section geared a little more towards computers but a lot of crossover with DME -identifies need to photograph DME equipment -identifies need to recover using best practices and in native format if possible	-All digital evidence is stored in their Digital Evidence Management System (DEMS) -DEMS is secure storage with its own SOP -authorized access only -all user actions logged and periodically audited -audit trail for chain of custody -all digital evidence receives a hash value
Other Observations:	-SOP identifies outside agencies that may be helpful in assisting in recovery or examination of digital evidence -SOP identifies methods for requesting further examination of DME by OFS and OFS responsibilities		
Score:	5	4	5
Total Score:	14		

DOCUMENTATION Phase			
	Field Notes	Final Reports	Evidence Disposition
Notes:	-SOP identifies a DE Recovery Form, 75-665 -attaches a copy of form to SOP -provides a process for filling it out -specific section on surveillance video -Have a DE Recovery Form (Digital Video), 75-656 that identifies DVR make, model, offset, # of cameras, retention time, notes, etc	-SOP does not specifically mention final reporting -recovery forms and SOP section covering recovery form identifies important information need to be notated	-SOP has an entire section titled "Retention and Purging" -identifies a "Digital Evidence Custodian" -identifies periodic audits and reviews -identifies need to ensure pertinent and viable evidence is safeguarded
Other Observations	-would be nice to have a hyperlink to DEMS		
Score:	5	3	5
Total Score:	13		

Final Score: 45

Methodology Form: Department D

TRAINING Phase				
	Outside Training	Internal Training	Continuing Education	Equipment
Notes:	-SOPs allows for officers to apply for outside training -No SOPs in relation to outside training and DME.	-Have a SAPD "Training Academy" that is online through SAPD web -appears to be a good resource for additional training -Nothing specific to DME	-SAPD Training Academy online -SOP identifies 40hrs of training to be done yearly for officers -Nothing specific to DME	-nothing specific in SOPs in relation to DME
Other Observations:	-SOPs do have small paragraphs that define "Specialized Training" and "Career Development" but nothing specific to training and DME -SAPD has a "Career Development Program" offered through to dept to officers. Access through SAPD web portal (unable to access)			
Score:	3	3	3	1
Total Score:	10			

PROCESS Phase			
	Preparation Steps	Method of Extraction	Chain of Custody
Notes:	-SOPs identify actions for officers in "Crime Scene Duties" SOP. -very narrow duties	-SOP gives process for handling some DME but appears to be more geared towards VHS -not very specific -seems outdated	-SOPs cover general procedures for documenting chain of custody -identifies basic chain of custody procedures -nothing specific for DME
Other Observations:	-have an entire section titled: "Crime Scenes Where Video Recordings are Made" -entire section seems out of date, numerous mentions of VHS -needs to be updated		
Score:	3	2	3
Total Score:	8		

DOCUMENTATION Phase			
	Field Notes	Final Reports	Evidence Disposition
Notes:	-Have numerous forms listed but unable to access -all processes of documenting are generic, no DME	-entire SOP about reporting: offense/incident/ supplemental -nothing specific to DME -identifies where reports can be found but unable to access	-Describes a "Videotape Receptacle in Headquarters Building where final master copy is to be dropped off -all other SOPs are generic to evidence handling, nothing DME specific
Other Observations:	-evidence disposition seems out of date with "Videotape Receptacle" -might need to update along with updating verbiage		
Score:	3	3	3
Total Score:	9		

Final Score: 27

Methodology Form: Department E

TRAINING Phase				
	Outside Training	Internal Training	Continuing Education	Equipment
Notes:	-Have a training SOP that encourages further training -states officers SHOULD be provided with 30hrs of training a year -nothing specific to DME	-Training SOP also identifies In-service training as standard training -classes provided to update training -nothing specific to DME	-Training SOP (nothing specific to DME)	-SOPs identify smartphones for taking pics and media cards but used to document crime scenes -nothing specific to DME
Other Observations:	-SOP titled Photographic Evidence 7.090 states employees will receive training but it is only in regard to dept. DSLR cameras to document crime scene -also provided with image processing software for documenting crime scene but nothing specific to DME			
Score:	1	1	1	2
Total Score:	5			

PROCESS Phase			
	Preparation Steps	Method of Extraction	Chain of Custody
Notes:	-Nothing DME specific in SOPs -minor description of drop-off procedure of computers to Forensic Lab, not DME related	-SOP has a good process description for submitting photos for evidence, not DME related	-SOP provides info about documenting chain of custody but not DME related -Washington State Patrol Forensic Services Guide has paragraph detailing chain of custody but not DME related
Other Observations:	-Washington State Patrol Forensic Laboratory Services Bureau has a "High Tech Crimes Unit" but only specifically mentions Cell Phones -WSP Forensic Laboratory Services Bureau also does processing of Firearms, DNA, prints, etc but no mention of DME		
Score:	1	1	3
Total Score:	5		

DOCUMENTATION Phase			
	Field Notes	Final Reports	Evidence Disposition
Notes:	-only mention is a "Canvass Card" for documenting witness information	-only mention is that Case Files should satisfy standards set forth by States Attorney office and published by Criminal Investigations Bureau	-General evidence SOP but nothing specific to DME -detailed description of dealing with photos produced for documenting crime scene
Other Observations:	-SPD has a very detailed SOP titled Photographic Evidence but it only deals with photographic evidence produced from SPD members documenting crime scenes. Could easily add DME information to this SOP		
Score:	1	1	3
Total Score:	5		

Final Score: 15

Appendix B – Documentation Form Examples



Standard Practice for Data Retrieval from Digital CCTV Systems

602

APPENDIX

603

(Non-mandatory Information)

604

XI. CCTV SYSTEM INFORMATION FORM

605

CCTV System Information Form

606 **Scene Contact Information:**

607 Scene Address: _____

608 Hours of Operation: _____

609 Scene Point of Contact: _____

610 Email: _____

611 Phone: _____ Phone: _____

612 CCTV System Point of Contact: _____

613 Phone: _____ Phone: _____

614 Email: _____

615 **Equipment Information:**

616 Digital Video Recorder Analog Video Recorder

617 Make/Model: _____

618 Serial Number: _____

619 Stand-Alone Personal Computer Network Video Recorder Manual

620 Available

621 Multiplexor Make/Model: _____

622 Standard User Name and Password: _____

623 Administrative/Engineer User Name and Password: _____

624 Date/Time Display: _____ Actual Date/Time: _____

625 Date/Time Offset: _____ Loss Prevention Steps Taken (See Notes)

626 **Other System Information and Settings:**

627 Number of Recording Units: _____ Number of Hard Drives: _____

628 Storage Capacity: _____



Standard Practice for Data Retrieval from Digital CCTV Systems

- 629 Network Connection (See Notes) IP Address: _____
- 630 System Firmware Version: _____ Applicable Event/Service Log(s) (See Notes)
- 631 Total Cameras (See Notes for associated names): _____ Total Active Cameras: _____
- 632 Alarm/Motion Triggered (See Notes) Infrared (See Notes)
- 633 Make/Model: _____
- 634 Transmission Method: _____ Camera Resolution: _____
- 635 Record Mode (Analog) (e.g. 2, 6, 12, 24, 48, 72 hour): _____
- 636 Image Quality (Digital): High Medium Low
- 637 Image/Frame Size (e.g. 320x240): _____ Frames/Images per Second (FPS / IPS): _____
- 638 Total Audio Inputs: _____ Audio Sampling Rate: _____
- 639 Location(s) of Microphones: _____
- 640 Changes Made to System (See Notes) Photographs Taken
- 641 Export Options (Hardware): _____
- 642 File Format Export Options: _____
- 643 Playback Software: _____ Version: _____
- 644 Playback Software User Name and Password: _____
- 645 Media Collected (e.g. tape, CD/DVD, USB Device, etc.): _____
- 646
- 647
- 648
- 649
- 650
- 651
- 652
- 653

Department B Recovery Forms



Digital Evidence Recovery Form
Appendix A (Digital Video)

DC#: _____ - _____ - _____ Recovering Party: _____

Make: _____ Model: _____ Serial Number: _____

User Name: _____ Password: _____

DVR System Date: ____/____/____ Time: ____:____:____

Official Date: ____/____/____ Time: ____:____:____

Reference Time Source: _____ Offset: + / - ____ days ____ hrs ____ min

Software / Firmware Version: _____ Retention Time: _____

Pixel Resolution: _____ Image Quality Setting: _____

Frames Per Second (FPS) _____ Motion Activated Recording: Yes / No

Network IP Address: _____ Subnet Mask: _____

Gateway: _____ Infrared (IR) Enabled: Yes / No

Number of Inputs / Cameras: ____ / ____ Player / Version: _____


Files Recovered: _____

Time

Actions Taken

<u>Time</u>	<u>Actions Taken</u>
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____



DIRECTIVE 



Digital Evidence Recovery Form

DC#: ____ - ____ - _____ Location of Occurrence: _____

Unit Control #: ____ - _____ Date of Occurrence: ____ / ____ / _____

Time of Occurrence: ____ : ____ Assigned Investigator: _____

Recovery Date: ____ / ____ / _____ Location of Recovery: _____

Recovery Time: ____ : ____ Recovering Unit: _____

Owner: _____ Owner Address: _____

Owner Phone: () ____ - _____ Search Warrant Number: _____

Property Receipt: Yes ____ No ____ Prop Receipt Number: _____


Device Type: DVR ____ Smart Device ____ PC / Server ____ Other (list) _____

* If the item(s) were not placed on a property receipt complete the below information fields *

Make: _____ Model: _____

Color: _____ Serial Number: _____



DIRECTIVE 

Department A Retrieval Documentation Forms



DIGITAL VIDEO EVIDENCE RECOVERY KITS

RETRIEVAL DOCUMENTATION FORM

Name of Member

Rank

CAD

Badge

Equipment Information:

Make Model

Serial Number

Number of Connected Cameras Number of Connected Microphones

Type of Cameras Connected Analog Digital IP

Display Connections BNC Composite RCA Composite HDMI

VGA DVI

Data Connections USB e-SATA Network

Internal Devices Optical Disc Drive SD/ CF Card Slot Floppy Disk

System Settings:

Current Date Current Time

System Date System Time

Calculated Offset

User Name(s)

Password(s)





RETRIEVAL DOCUMENTATION FORM

Software Version _____

Total Number of Hard Drives _____ Capacity vs. Amount Full _____

Earliest Recorded Date _____

Settings	Camera	Camera	Camera	Camera
Resolution				
Frames Per Second				
Quality / Compression				
Event / Motion				

Network Settings:

IP Address _____

Subnet Mask _____

Gateway _____

DHCP enabled? Yes No





RETRIEVAL DOCUMENTATION FORM

Video Information of Interest:

Camera	Date	Time Start	Time End

Date and Time to be Retrieved:

Methods of Recovery Available:

ORDER FOR RECOVERY:

- CD/DVD Writer
- CF/SD Card Writer
- USB Connection
- Floppy Disk Drive
- Network Connection
- BNC or RCA Composite Monitor Connection
- VGA or DVI Computer Monitor Connection
- Other



(DIVRT Kits)

Attachment B





RETRIEVAL DOCUMENTATION FORM

Audit Trail:

A large, empty rectangular area with a light blue background and a thin black border, intended for recording the audit trail.

(DIVRT Kits)

Attachment B



Department A Equipment List



Digital Video Evidence Recovery (DIVIRT) Kit Inventory

- Inspection Mirror
- Black sharpie marker
- Power supply for PVR
- Soft blue carrying case containing
 - DVI to VGA Adapter
 - Scan converter power supply
 - Composite video cables x2
 - BNC T Connector
 - RCA adapters x2
 - Power Supply for PVR
 - PVR Cables x2
 - Micro USB to USB cable
 - Headphones
 - Mini remote control for PVR
 - Stylus Black pic
 - Micro SD Adapter

- Yellow envelope containing
 - PVR Operation Manual
 - StarTech Operation Manual
 - CD Rom for Fuji Camera

- Laptop
 - Dell Laptop Latitude E5450 with soft case and charger
 - Serial Number MPD, please specify:
 - Serial Number, please specify:
 - DVD Burner
 - Model Number GP61NB60



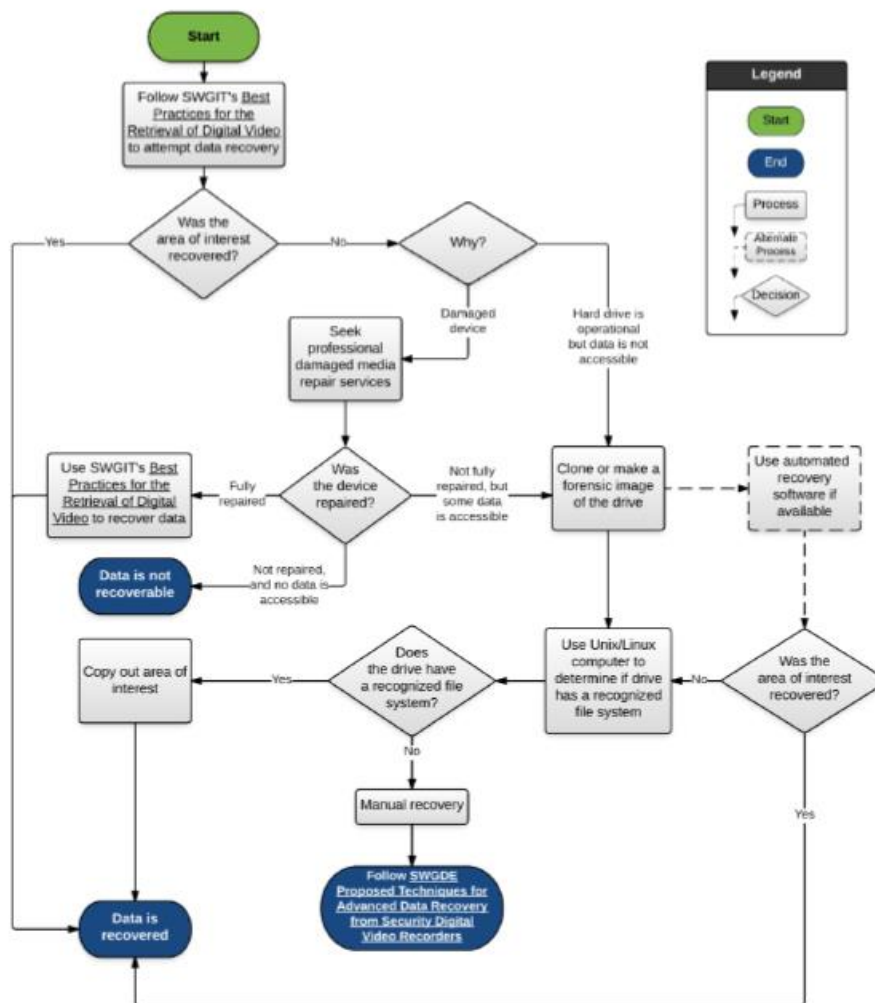
(DIVIRT Kits)
Attachment A
DIVIRT Kit Inventory

Appendix C – Workflow Examples



Scientific Working Group on Digital Evidence

Appendix A – Decision-Making Process for DVR Recovery Methods



SWGDE Best Practices for the Recovery of Data from Security Digital Video Recorders Containing H.264 Data – Appendix A

Version: 1.2 (June 23, 2016)

This document includes a cover page with the SWGDE disclaimer.

Page 17 of 19

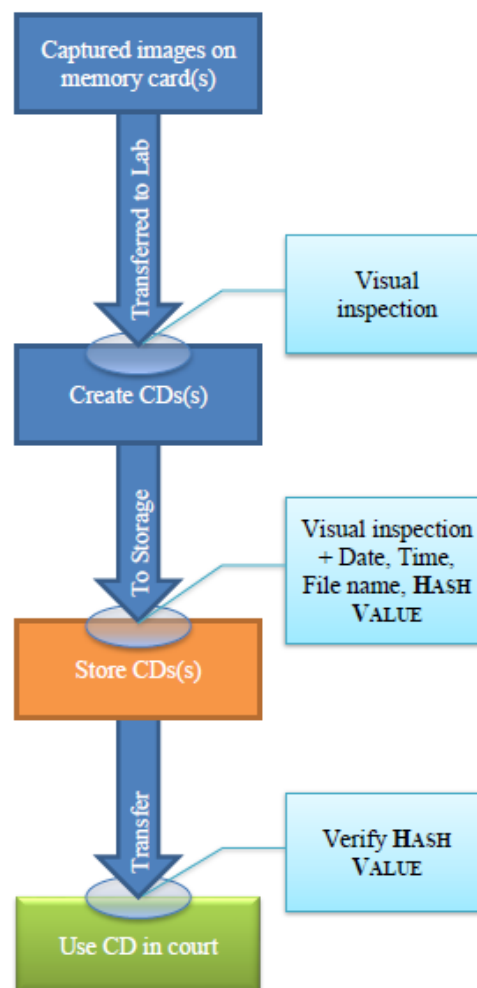


Scientific Working Group on Digital Evidence

Flowchart from Example #1

NOTE:

It is important to document chain of custody throughout the lifecycle of the evidence. In this case, the chain of custody is initiated and maintained by the appropriate personnel.



SWGDE Best Practices for Maintaining the Integrity of Imagery

Version: 1.0 (July 18, 2017)

This document includes a cover page with the SWGDE disclaimer.

Page 9 of 12

Collecting Digital Evidence Flow Chart

