NIST Interagency Report
NIST IR 8387

Digital Evidence Preservation

Considerations for Evidence Handlers

Barbara Guttman
Douglas R. White
Tracy Walraven

This publication is available free of charge from
https://doi.org/10.6028/NIST.IR.8387

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Interagency Report
NIST IR 8387

Digital Evidence Preservation

Considerations for Evidence Handlers

Barbara Guttman
Douglas R. White
Software & Systems Division
Associate Director for Laboratory Programs

Tracy Walraven

This publication is available free of charge from
https://doi.org/10.6028/NIST.IR.8387

September 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST IR 8387
September 2022

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

NIST Technical Series Policies
Copyright, Fair Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2021-08-01

How to Cite this NIST Technical Series Publication
Guttman B, White DR, Walraven T (2022) Digital Evidence Preservation: Considerations for Evidence Handlers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8387. https://doi.org/10.6028/NIST.IR.8387

NIST Author ORCID iDs
Barbara Guttman: 0000-0001-9706-389X
Douglas R White: 0000-0001-5872-3963
Tracy Walraven: 0000-0003-2732-3785

Contact Information
Barbara Guttman Barbara.Guttman@nist.gov

Abstract

The preservation of digital evidence (DE) presents unique problems beyond traditional evidence preservation. This document addresses considerations related to the preservation of digital evidence. This document is part of a series on evidence management and its primary audience is evidence management professionals. The document discusses traditional sources of digital evidence including physical storage media and digital objects and also addresses law enforcement generated digital evidence. The document further discusses key considerations related to digital evidence preservation and the difference from the preservation of other evidence types. Related considerations, such as acquisition of digital evidence are only addressed when there is overlap with preservation.

Keywords

Digital evidence; computer forensics; chain of custody; evidence preservation.

Table of Contents

Acknowledgments

The authors of this report thank members of the Digital and Evidence Management communities who walked us through their procedures and commented on the draft. In particular, we want to thank Sergeant Maryann Magnelli, Evidence Unit Manager and Sergeant Michael Yu, Electronic Crimes Unit, of the Montgomery County Police; Daren Ford, Director of the Northern Colorado Regional Laboratory; Brandon Epstein of the Middlesex County Prosecutor's Office, Jesse Lindmar, Digital & Multimedia Evidence Section Supervisor, Virginia Department of Forensic Science and members of the Evidence Management Steering Committee for their contributions to the development and review of this report.

Evidence Management Steering Committee Membership
Suzi Doerff, CEO, Police Evidence Audits, LLC

Rachell Ekroos, Assistant Professor, University of Nevada, Las Vegas (UNLV), School of Nursing

Sarah Hawkins, Chief Deputy Public Defender, Clark County, Nevada Public Defender's Office

Melisse Huffmaster, Evidence Vault Director, Las Vegas Metropolitan Police Department

Jennifer Johnson, Program Coordinator, Forensic Assessment Consultation and Treatment Program, Shawnee Mission Health

Joseph Latta, Executive Director, International Association for Property and Evidence, Inc.

Robert Martin, Evidence Manager, Volusia County Sheriff's Office
Nancy McKay-Hills, Evidence Superintendent, Tucson Police Department, Property and Evidence Section

Stacey Mitchell, Clinical Associate Professor, Texas A&M University

Marcela Najarro, Research Chemist, National Institute of Standards and Technology

Phil Pulaski, Retired Former Chief of Detectives, New York City Police Department

Brian Russell, Lieutenant/Manager, Charlotte Mecklenberg Police Department, Property and Evidence Division

Elizabeth Small, Supervisory Physical Scientist, Evidence Management Unit, FBI Laboratory

Lindsey Smith, Executive Director, North Carolina Innocence Inquiry Commission

Ellen Spain, Forensic Evidence Manager, Virginia Department of Forensic Science

Patricia Speck, Professor/Coordinator, University of Alabama at Birmingham, MSN Advanced Nursing Program

Robert Thompson, Senior Research Manager, NIST Special Programs Office

Erin Trujillo, Assistant Director, Los Angeles Sheriff's Department, Scientific Services Bureau
Raymond Valerio, Director, Forensic Sciences, Office of the Queens County District Attorney

Sponsorship

NIJ is the research, development, and evaluation agency of the U.S. Department of Justice and is dedicated to researching crime control and justice issues. NIJ provides objective, independent, evidence-based knowledge and tools to meet the challenges of the nation's criminal justice community. NIJ's OIFS is the federal government's lead agency for forensic science research and development and administers programs that provide direct support to crime laboratories and law enforcement agencies. OIFS forensic science programs and initiatives provide resources for the creation of new, innovative, and emerging technologies through the integration of research and development, laboratory efficiency and capacity enhancement, and technology transition, which will increase the capacity of crime laboratories to process growing amounts of evidence effectively and expeditiously.

The NIST mission is to advance measurement science, standards, and technology. It accomplishes these actions for the forensic science community through its Special Programs Office's Forensic Science Research Program (FSRP). The FSRP directs research efforts to develop performance standards, measurement tools, operating procedures, guidelines, and reports that will advance the field of forensic science. The Special Programs Office also manages the Organization of Scientific Area Committees for Forensic Science (OSAC) and the Scientific Foundation Reviews.

1. Introduction

The preservation of digital evidence (DE) presents unique problems beyond traditional evidence preservation. Digital evidence includes any information in binary form that can be useful in criminal or other legal investigations and proceedings. By its nature, digital evidence resides on physical media, but it is the content and related information, rather than the media, that are most often important. Often only the digital content is available to evidence examiners; its physical form could be on law enforcement (LE) provided media or in the cloud, and it may be unclear where the data are actually stored.

Digital storage can contain an exceptionally large amount of information in a small physical footprint. It is present in a growing number of cases, owing to the ubiquitous presence of cell phones, social media use, and the vast array of digital helpers often called the Internet of Things (IoT). Digital data can be easy to change but there are powerful techniques for preventing and detecting change.

This document addresses considerations related to the preservation of digital evidence. Related considerations, such as acquisition of digital evidence or transport of devices and media are only addressed when there is overlap with preservation. The primary intended audience of this document is evidence management professionals.

The document is organized according to the four major types of digital evidence that evidence managers frequently encounter. The types of evidence are described and then preservation considerations related to this type of evidence are discussed. A references section follows.

1.1. Evidence Sources

This document describes four types of digital evidence: physical media, digital images/files, other digital objects, and law enforcement (LE)-generated evidence.

- Physical media includes hard drives in computers and mobile devices, and external storage such as USB drives, CDs and DVDs. There are many types of physical media.
- Digital images and files are produced when digital evidence is copied from physical media or other systems. These may be copied from remote (cloud-based) systems, from physical systems that remain in the field or from physical systems that are seized and brought into an evidence system.
- Other digital objects include a wide variety of digital material that does not exist as an image or file, such as an online account.
- Law enforcement also generates potential digital evidence, especially through body worn camera (BWC) programs, in car video, and other electronic records. It consists of both a physical device and digital data.

Each of these evidence types is discussed below along with the prevalent issues evidence handling professionals should consider when preserving the data. Figure 1 shows the basic relationship among the evidence types.

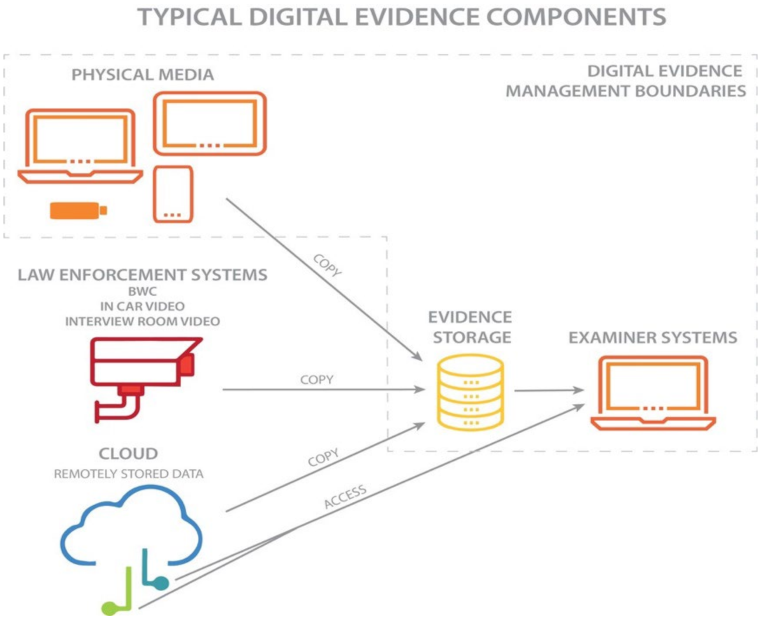

Figure 1. Typical Digital Evidence Components.

1.2. Evidence Management Projects at NIST

The management and preservation of evidence are often overlooked, but are crucial aspects of the criminal justice system. Since 2011, the National Institute of Standards and Technology (NIST) has worked in partnership with the National Institute of Justice (NIJ) and a host of other stakeholders representing various facets of the criminal justice system to provide best practices and guidance for the preservation of evidence. This report is the first in a series of reports geared toward evidence professionals, or people or organizations engaged in the preservation of evidence. Law enforcement organizations play the largest role in evidence preservation, but evidence handlers in public and private forensic laboratories, hospitals, or courts will also find this guidance useful and applicable.

To find out more about other related Evidence Management Projects at NIST, visit the NIST Evidence Management website.

2. Physical Media and Devices

2.1. Background

Computers store data for long periods of time in multiple ways on multiple media types. Physical media refers to a long-term type of computer storage. These storage types are integrated into many everyday items such as PCs, phones, drones, and watches.

Computers also keep data in computer memory, which is used for short-term storage. The difference is that long-term storage keeps a copy of data when it is powered off and memory requires power to maintain the data. Because of this, most physical evidence that is collected is kept as a copy in long-term storage, rather than in memory.

There are three major types of storage:

1) Magnetic Media (spinning). This is what standard hard drives are, and it is present in multiple types of devices such as hard disk drives (HDDs) in PCs; storage for large computer systems such as RAIDs, and game consoles. Tapes and floppy diskettes are also in this category.

2) Solid State Drives (SSD). These drives do not have moving parts, are faster, and are less prone to failure. SSDs are becoming more common and are replacing spinning magnetic media in laptops, phones, DVRs and many PCs. SSDs are also found in smaller external storage such as flash drives, SD cards, and other removable digital storage.

3) Optical Storage. This class is primarily composed of DVDs and CDs.

Evidence management systems are required to be able to track physical items. In this regard, digital evidence management is similar to standard evidence management.

2.2. Physical Media and Device Storage Considerations

1.) Temperature/Humidity. Standard office temperature and humidity are sufficient for storing physical devices and media. High temperature or humidity can decrease the lifespan for some media types. See Media Longevity Table 1.

2.) Magnetism/Electricity. Magnetic media, such as hard disks, can be erased by powerful magnets. In the unlikely event that a large magnet (e.g., one with over 45 kilograms or 100 pounds of pull) enters the evidence storage area, it needs to be kept away from magnetic media. (Kingsley-Hughes, 2012)

3.) Media vs. Device Preservation. Many digital devices are large and bulky. It is not necessary to keep the devices if they do not contain data unless they are needed for retrieval or p45layback of the data or contain other relevant evidence. Items such as monitors generally do not need to be retained unless they are standalone devices with physical data storage capability. Since computing changes frequently, it is best to check with the Digital or Multimedia Evidence Unit to see what devices need to be retained and which ones can be released. This will become more important for larger and more valuable items.

a. Vehicles. Cars and other vehicles contain multiple computers including the infotainment unit and operational systems.

b. Large IoT devices. Computers are being incorporated into many large objects such as appliances that will present challenges to Evidence Units. Most of these devices will store their data remotely in the cloud and they do not need to be physically kept or preserved in order for their related data to be accessible. Refer to your Digital and Multimedia Evidence Unit for further guidance.

4.) Radio Frequency Isolation. Many computers and other devices can connect to various networks such as Wi-Fi, cellular, and Bluetooth. This fact can present a security issue for the Evidence Unit and may be an opportunity for outsiders to change digital evidence before it is collected. Many computers and other devices in an Evidence Unit will be powered off, but some units may lack a method to be powered off or may power off into a standby mode that can be accessed remotely. See SWGDE Best Practice for Mobile Device Evidence Collection and

Preservation, Handling, and Acquisition (Scientific Working Group on Digital Evidence, 2019) for information on radio isolation for powered-on devices. The guidance on how to perform radio isolation changes over time. Best practices should be reviewed and updated every 2-3 years.

5.) Accessories. Computers often require multiple accessories (e.g., connector cables, or adapters). Accessories should be stored with the devices.

6.) Transfers to Digital Evidence Units. As with other types of evidence, the physical unit may need to be transferred between a central evidence unit and the specialized unit analyzing it. Standard check in and out processes are sufficient for preserving the chain of evidence. Best practice is to make a copy of evidence to create digital files. (See Digital Images/Files below.) When a piece of evidence is imaged, the digital file will typically be stored in the Digital Evidence Unit. There are now at least two copies of the evidence.

7.) Long term storage of physical media. Some cases may necessitate holding onto media for a long time. It is possible that the media may degrade or that there will not be players capable of reading the media when it is required. It is acceptable to use off-line media such as CD-Rs, DVD-Rs, tape or hard disks. SSDs are not appropriate for long term storage as they require occasional (in some cases, monthly) power to ensure data retention. (Veaux, 2018) If the copy is stored on CD, DVD, tape or hard disks, it should be copied to new media every 20 years. The data can also be archived using cloud-based services. Many services offer security commensurate with the needs of law enforcement. Note that the cost of storage can become expensive. Off-line media storage is generally less expensive over time. See Media Longevity Table 1.

8.) Contamination. As with other types of physical objects, digital evidence can have chemical or biological contamination. Processes employed for safe handling of other evidence types (e.g., personal protective equipment) should be used. Digital media does not present additional risks. However, Digital Evidence Units may not be accustomed to working with potentially contaminated devices and may not be aware of the issue or the processes that need to be in place to mitigate it.

9.) Return to Owner. After media has been imaged or when the media or device is no longer needed, it may be returned to the owner.

10.) Reuse, Disposal or Sale. Computer media must be erased using either a full disk wiping program or via secure erase if that is supported by the drive. See NIST Special Publication SP 800-88, Guidelines for 56 Media Sanitization (Kissel, 2014). Simple erase commands are not sufficient since they normally only erase the directory, not the contents.

Table 1. Media Longevity.

Type of Storage	Media Type	Longevity*	Archival Use	Notes and Primary References See also References Section
Optical	Pre-recorded (CD/DVD-ROM)	<10 years	Not recommended for archival use	Provided here for clarity since there are many references describing their failure rates (Library of Congress CD-ROM)
	CD-R and DVD-R Blu-ray	<30 years	Acceptable for archival use	30 years is a conservative minimum longevity. There are reputable claims of 50 or 100 years. Gold disks last longer than silver. CDs last longer than DVDs. Blanks should be used within 5 years. Consider future availability of readers. (Library of Congress CD-R & DVD-R); (Council on Library and Information Resources) (Coughlin, 2014) Industry assessments
	M-DISC (DVD & Blu-ray)	At least 100 years	Acceptable for archival use	Introduced in 2009; requires M-DISC writer. (Naval Air Warfare Center Weapons Division, Life Cycle and Environmental Engineering Branch, 2009) Laboratoire National de Metrologie et d'Essals (Perdereau, 2012)
	CD/DVD-RW	<20 years	Use CD-R and DVD-R	(US Digital Media CDROM2GO)
Magnetic	Solid State Drives (SSD)	<1 year	Not recommended for archival use	(Coughlin, 2014)
	Hard Disk Drives (HDD)	<2 years	Not recommended for archival use	(Coughlin, 2014)
	Tape	20 years	Acceptable for archival use	Consider future availability of readers. (Coughlin, 2014)

*Longevity. This is the amount of time an unused (no power supplied) media can be expected to be readable with very high confidence. Most media will last longer than the duration indicated in this table. From an archive perspective, this information provides the maximum amount of time the media should sit before the data are copied to new media.

3. Digital Images/Files

3.1. Background

There are multiple types of digital data. It is helpful to categorize them by how they are acquired. Note that the process of copying digital data is called acquisition or imaging. A discussion of acquisition is beyond the scope of this document. See documents from the Scientific Working Group on Digital Evidence, www.swgde.org.

Digital Images and Files Acquired via Forensic Tools. In a typical case, physical devices or media are seized and taken to a digital forensics lab to be imaged. The physical items are logged into the evidence management system and the digital forensics lab uses various tools to make a copy (digital image) of the data on the device or media. The image is then stored in a case management system or other computer system that is often not a part of the Evidence Unit. Data may also be acquired via a forensic tool in the field, rather than in the lab. It is common for data to be acquired directly from a device or media without taking possession of the physical item. This is often the case for data acquired from multi-user servers, cloud-based storage, or other devices that are impractical to bring to the lab or take offline.

What is an Image? *The term image means two things in forensics. The first meaning is similar to its use in regular English; that is, an image is a picture or graphic. The second meaning is a specialized term in computing. It is a bit for bit copy. In computing, there are many ways to copy something. A bit for bit copy is an exact copy including part of the data that is not visible to a user. For example, a printout of a document is a copy of that document, but the internal formatting commands are not visible. An image copy will encompass everything in the file including formatting, deleted text, date created and other details. It is the "gold standard" of copying. The resulting copy is called an image file.*

Digital Images and Files Acquired Directly. Digital images may also be acquired from 3rd party organizations via requests made to the organization; copied without the use of a forensic tool; provided by government or private surveillance systems; or by the public who have witnessed a potential crime, especially in the form of cell phone videos.

Other Digital Objects. Some digital data will not be in the form of files or images. Cryptocurrencies are obtained via passwords or other keys. They are acquired into evidence via a law enforcement (LE) account. They are neither images nor files. See the section below for a fuller explanation of digital objects.

What is a File? *A computer file is fairly similar to its meaning in the physical world. It is a self-contained set of data. In a computer, the operating system sees a file as data to be managed as a single unit. Computer operating systems have file systems for keeping track of data. Files can be tiny or extremely large. Image files, because they can contain the entirety of a hard disk, tend to be large.*

3.2. Digital Image and File Storage Considerations

1.) Chain of Custody. Digital files are very easy to change, so maintaining the integrity of the data is a critical concern. (See also Section 9 Technologies to Assist with Digital Evidence Management.)

a. Documentation of the original source of the image or file and how it was created by or transferred to law enforcement.

b. Hashes and digital signatures. It is best practice to hash digital images and other objects using a NIST approved hashing algorithm and the resulting hashes should be stored separately from the image or file in a secure location. Case management systems normally provide this functionality. If not available, the hash data must be transmitted to either a computer system not under the control of the digital forensics practitioner or printed and stored beyond the control of the practitioner.

What is a Hash? *A hash is a digital checksum. Secure hashes, such as NIST's Secure Hash Algorithm (SHA) are a form of cryptography. A file can be uniquely identified by its hash. Any change to a file will result in a different hash.*

- It is acceptable to use an older hashing algorithm (e.g., MD5 or SHA-1) if needed but newer algorithms are preferred. See SWGDE Position on the Use of MD5 and SHA1 Hash Algorithms in Digital and Multimedia Forensics (Scientific Working Group on Digital Evidence, 2019). Example algorithms may be found in Federal Information Processing Standards Publication 180-4, Secure Hash Standard.

c. What to do when hash comparisons fail. Secure digital hashes are very sensitive. The change of even one bit will cause the hash to be completely different. Changes to files can occur in several ways that do not change the evidence itself. If a hash comparison fails, it is possible to still verify the integrity of the file. See also the National Digital Stewardship Alliances, Checking Your Digital Content. (Paula De Stefano et al, 2014)

- The primary approach is to save more than one copy of digital files, so a corrupted file can be replaced with its backup.

- Block hashes (hashes made of multiple smaller parts of a file) can be used to limit the amount of data that is suspect.

- If there is not a backup copy, the chain of evidence and security of the sole copy would need to be assessed by the practitioner to determine if the change was intentional or accidental.

d. Alternatives to hashing. If a hash is not made, a copy of the data - created early in the collection process and preferably before any investigative procedures have begun - should be stored on physical media, and all of the transfers should be documented. This physical copy should be kept in the Evidence Unit.

e. Securing the files.

- Evidence files should be kept in a system that is not connected to the internet and that has strong security including individual authentication, access controls, and logging. If the organization uses a cloud-based system, appropriate security is needed. Techniques such as VPNs can be used to protect forensic evidence even while using the internet. NIST (NIST CSRC) and other organizations such as the Multi-State Information Sharing and Analysis Center (MS-ISAC) provide advice about securing systems. See csrc.nist.gov and https://www.cisecurity.org/ms-isac/. Note that government systems are often targeted for attacks including ransomware.

- Directly Acquired Digital Evidence. Digital evidence may be received directly, such as those from 3rd party organizations such as cloud service providers. In these cases, there may be no record of the item in an Evidence Management system. Digital Evidence Units will need to have a method for recording evidence that enters the unit directly.

f. A special case is direct public submission of material. An example of this is videos from a witness's cell phone. Occasionally, law enforcement issues a public request for material and may receive large volumes of cell phone, video, or other material.

2.) Multiple Copies and Best Evidence. It is possible to make multiple copies of digital evidence. By verifying hashes or digital signatures, it is accurate to state that the copies are identical to the original. The concept of "best evidence" is not applicable since the copy is identical to the original. This applies even to a digital image made from a physical device. (Daniel J. Ryan, 2010)

3.) Storage of Digital Images and Files. Digital images and files will normally be preserved locally on some form of media or stored in a remote (cloud-based) system. The amount of digital evidence can be large. If an organization has significant amounts of data, it makes sense to pick different storage strategies based on length of time that the case's evidence needs to be preserved, the cost of the storage and, for cloud-based storage, the likelihood that the data will need to be retrieved.

a. Considerations for local storage:

- Since digital information can remain on media if it is not fully erased, the receiving media must be wiped before use. (See Physical Media Considerations Paragraph 10.)

- Backups. All digital evidence should be backed up to a location unlikely to be impacted by an event (e.g., fire) at the primary site.

- Long term storage. Best practice for long term storage of digital material is to transfer the material from old technology to new technology. When a technology used for storing evidence is becoming obsolete, it should be re-written to a more modern technology. Data stored on optical media, such as CDs and DVDs, should be re-written within 30 years since the media can degrade. Table 1 shows the archival properties for various types of storage media. Cloud-based long-term storage should provide the refresh needed for preservation.

b. Considerations for cloud-based storage. There are several cloud-based systems that offer archival storage and have robust security. A discussion of various types of cloud services and security is beyond the scope of this document. The considerations addressed here are those specifically addressing the storage of digital evidence rather than other uses of the cloud-based resources.

- Security. Storing and transferring data to the cloud introduces security vulnerabilities. Transfer issues are generally mitigated with VPNs and encryption of data. Access to cloud-based storage of digital evidence should be protected with strong security, including two-factor authentication.

- Encryption. If data is encrypted prior to cloud storage, it is essential that the keys can be retrieved at future dates. The Evidence Unit may be in a good position to store encryption keys long term given the nature of their mission.

- Transition. It is possible that the host agency contract with the provider may end prior to the retention period or that the provider could go out of business or change their services. A strategy for moving the data to a different provider will be needed. Current costing models require a fee when data is retrieved from archival storage.

4.) Retention. In the absence of statute or a retention policy from the relevant jurisdiction, best practice is to retain digital evidence for a time frame defined by the organization for consistency (e.g., five years, 6 months) after the case has been adjudicated. The adjudication process may include criminal and civil proceedings and the appeal process. See Media Longevity Table 1.

5.) Disclosure of evidence. Despite security measures put in place, it is possible for digital evidence to be accidentally or maliciously disclosed by insiders or to be disclosed as part of a security breach. Encrypting data when it is being stored (also known as data at rest) is the strongest protection against this. Agencies should address the disclosure of digital evidence in their general disclosure and incident management policies.

6.) Formats. When a computer or phone is imaged, or a surveillance video is acquired, the resulting file may be in a format that is proprietary to the acquisition tool or surveillance system or it may be in an open format. Many proprietary formats require proprietary playback equipment or software. Proprietary formats can cause issues for both long term retrieval of information and can be an impediment to the sharing of evidence. Evidence should generally be saved in the format that contains the most data. If this format is proprietary, it may be necessary to also preserve the data in an open format. The Library of Congress publishes a Recommended Formats Statement (Library of Congress Formats).

What is a Format? *Digital information is normally stored in a file. Each file has a file type or format. For a computer to be able to interpret the data in the file, it needs to have the instructions that go with that file. Common examples of file formats include Word or PDF. For a computer to display a PDF file, it needs to have an application such as an Adobe reader. Some formats are containers and their contents include multiple files, such as Zip files. Some formats are owned by a company and that company restricts access to paying customers. Some are made freely available and some are completely open. Without the instructions to open a file, the data can be fully or partially unreadable.*

As technology systems mature, there is a tendency to move to more open formats, but it is not universal. Considerations related to formats are discussed by technology type.

a. Computers. The common formats for most files in use now are well known and adequate for long term storage. Even proprietary formats, such as Microsoft and Apple and digital acquisition tools are well known and understood and are likely to be usable in timeframes appropriate for law enforcement needs. Software to read the formats is available at a reasonable cost. Proprietary image files created by acquisition tools, e.g., such as Encase (E01 files), are likely to be usable for the next 5 to 10 years. If a case is likely to be needed beyond that and the image file is in a proprietary format, the Evidence Unit should also preserve a copy of the acquisition software. The raw image format (e.g., produced by Unix/Linux "dd") is an open format and can be used for long term storage.

b. Mobile Devices. Like computers, the file formats used on mobile devices are generally well known and are likely to be readable in the future. The tools used to create images of mobile devices are rapidly evolving and may not produce images that will be readable in the future without a copy of the system that created the image.

c. Surveillance Video. Many surveillance systems can output either a proprietary format or an open format that often contains significantly less data. The business model for surveillance system vendors is dependent on selling playback systems as well as surveillance systems. If law enforcement does not own the surveillance system, the evidence should be collected in both the native proprietary format and the open format if possible. LE will need a means to playback the video which may entail purchasing playback systems. Other users of the evidence (courts, defense) will also need playback systems.

d. Law Enforcement Systems (BWC, in-car video). LE-generated data such as body worn camera, car video and monitoring, and interview room video presents similar challenges as surveillance video. Many vendors sell closed systems at a lower price than open systems. LE purchasers of these systems need to weigh the potential downstream costs across the justice system of needing proprietary playback systems when purchasing these types of technology.

e. Emerging Systems. As new technology changes, it will result in new format types. The general principle of saving both the highest quality format and an open format should be followed when possible.

7.) Removal of Data. There are situations where it is desirable to remove information from already collected digital evidence. These situations can arise when more information was collected than a warrant specified or when material is identified as belonging to someone who is not a part of the investigation. There are currently no available tools for digital evidence managers to use to remove some material from a digital image. While in some situations it may be technically possible, it is generally infeasible to do. If material needs to be removed from digital evidence, digital evidence managers will need to exclude that material from processing by digital evidence analysis tools. Given that there are multiple copies of most digital evidence, any notes about excluding material will need to be placed at all entry points to obtaining the digital image.

8.) Sharing of Digital Data. Digital data is very easy to share. Sharing data can allow for many benefits for linking similar cases, developing proactive policing strategies, and other higher-level analyses. Policies for sharing data are beyond the scope of this document, but if a decision is made to share evidence data, it needs to be tracked so that any removal order can be shared as well. Data sharing raises many privacy and other control issues. It is very difficult to remove data from digital information. Privacy techniques such as anonymization are beyond the scope of this document, but evidence managers should be skeptical of these techniques. Many can be reversed or there may be other information in the content that can still link data to individuals.

9.) Technologies to Assist with Digital Evidence Management. It is important to store hashes or digital signatures of digital evidence in a manner that supports showing that they have not been tampered with. The following types of weaknesses in the chain of custody are possible.

a. Change the evidence before it is hashed

b. Change the evidence, re-hash it and overwrite a stored hash

c. Manipulate the evidence and use an MD-5/SHA-1 to create two versions of the evidence with the same hash value.

d. Accidental changes to the evidence or hashes.

To prevent or detect these attacks, it is best practice to hash evidence as close to collection as possible. Many systems that are designed for collecting evidence, such as surveillance systems, may hash files before collection by law enforcement. LE should hash all evidence at collection. It is possible that the hash is either forged or that the hash algorithm was generated using a slightly different version of the file (e.g., with or without header information).

a. Digital storage. Hashes need to be stored in a secure location where they cannot be changed or overwritten.

- Case Management Software. Law enforcement developed and commercial case management systems may provide a mechanism for storing hashes and digital signatures.
- Other secure digital storage. Hashes can be sent via email or other technique. The key factor is that there is a record of the hash that cannot be altered by people with access to the evidence.
- Hash chains, in which hashes of files are appended to each other are a useful technology for securing hashes.

b. Manual. It is possible to manually record and store the hashes.

c. Blockchain. Blockchain is a distributed database technology that underlies several cryptocurrencies but can be used for many other applications. For a digital evidence management scheme, it provides the ability to store hashes in a secure and transparent way, but there is significant overhead in managing the blockchain including implementation of a distributed ledger. For most evidence units, the overhead associated with using blockchain technology will be too large to justify its use.

4. Other Digital Objects

4.1. Background

There are other types of digital objects that may become evidence in addition to files and images. Common types of digital object include accounts held by banks and other financial institutions, digital or cryptocurrency, such as Bitcoin, and other non-currency assets, such as contracts, objects held in video games, airline miles or other points held by a vendor. The key similarity among these assets is that access to them is controlled by an authentication mechanism (such as a username, password or cryptographic key). A major distinction is whether the asset is held by an organization that is capable of "freezing" or otherwise securing the asset and those that are not. This section addresses only assets that enter the Evidence system, that is, assets that can't be secured in place by the holding organization. (Note: this section does not address warrants or other authorities to seize data.)

To seize the asset that can't be secured by an organization, law enforcement must log on using seized credentials and transfer the asset or change the authentication information to something possessed only by law enforcement. In many cases just changing the password will not be sufficient as there may be a password reset option that uses other credentials. This section primarily addresses cryptocurrencies, but there are other types of digital assets. Large online video games may have their own virtual currency or other objects that are bought and sold within the game. Private companies develop various forms of points which can be redeemed for company products. These can become quite valuable e.g., airline miles. Since these digital asset types and the companies that control them can change rapidly, it may be necessary to research the asset before determining how to safeguard it.

4.2. Digital Object Storage Considerations

1.) Establishing accounts and accountability.

a. To seize digital currency, the Evidence Unit will need to set up an account and the asset will need to be transferred to it. Evidence Units will need multiple accounts for any type of digital currency that is seized.

b. Since most cryptocurrencies are designed to be anonymous, access is controlled solely by a password or other credential. If the access is through a password, it will be difficult to prevent Evidence Unit employees from being able to have unsupervised access to the asset. All an Evidence Unit employee would need to do is to memorize or take photo of the password when it is created. (Some people are able to memorize long strings of characters.) It may be difficult to protect Evidence Unit employees from accusations of theft if the asset is kept as a cryptocurrency.

- To safeguard the asset and protect Evidence Unit employees, it may be necessary to transfer it to conventional currency and secure it using existing safeguards in place for cash and other valuable assets.
- Use of a split key. There are many cryptographic systems that split a key into two or more parts so that there can be dual-party control over the key.

- It may be possible to transfer the cryptocurrency to a larger department or Federal agency that specializes in cryptocurrency and can provide split key control.

2.) Value Fluctuation. Cryptocurrencies, like other assets such as gold, fluctuate in value. A record will need to be maintained of the asset when it was seized, and the department should establish a policy whether to hold the asset in its current form or transfer it to regular currency. Since it is possible that the asset will change in value, it is preferable to store it in its original form unless the Evidence Unit is unable to provide multi-party control of the key.

5. LE- Generated Digital Evidence

5.1. Background

Most evidence arrives at the Evidence Unit through traditional means having been acquired by police or other authorities from suspects or witnesses. However, other evidence is generated by the police. Body worn camera (BWC), in-car video, and technology designed to record police activity can become evidence either of a police-involved incident or as a witness to an event.

When a video is identified as having potential value as a piece of evidence, a copy should be sent as soon as possible to the Evidence Unit or other system for collecting directly acquired digital evidence. This will minimize the possibility of it being overwritten.

5.2. LE-Generated Digital Evidence Storage Considerations

1.) Sanitization of Physical Media. The devices that record LE-general evidence are used in the field and may be lost or stolen and it may be possible to retrieve data from them, including data from previous uses. These devices should be periodically sanitized (have the storage overwritten or wiped) and again before disposal. See NIST Special Publication SP 800-88, Guidelines for 56 Media Sanitization (Kissel, 2014).

2.) Security of Systems for Chain of Custody. If the system produces a hash, that should be transferred with the evidence. A record of the transfer should be made in keeping with general chain of custody procedures.

3.) Formats. Many LE owned systems are closed proprietary systems. This restricts to the ability to share the file with others in the justice system who need to see it. See Format section above.

6. References

National Center for State Courts. (2016). *Managing Digital Evidence in Courts.* NCSC Joint Technology Committee.

Anders O. Flaglien, A. M. (2011). Storage and exchange formats for digital evidence. *Digital Investigation*, 122-128.

Byers, F. (2003). *Care and Handling of CDs and DVDs: A Guide for Librarians and Archivists.* Council on Library and Inforamtion Resources & National Institute of Standards and Technology. Retrieved from https://clir.wordpress.clir.org/wp-content/uploads/sites/6/2016/09/pub121.pdf

CDOM2GO.COM by USDIgitalMedia. (n.d.). *Media Longevity*. Retrieved from https://www.cdrom2go.com/media-longevity

Coughlin, T. (2014, June 29). *Keeping Data For A Long Time*. Retrieved from Forbes: https://www.forbes.com/sites/tomcoughlin/2014/06/29/keeping-data-for-a-long-time/#31dd723715e2

Council on Library and Information Resources. (2020, January 28). *How Long Can You Store CDs and DVDs and Use Them Again?* Retrieved from Council on Library and Information Resources: https://www.clir.org/pubs/reports/pub121/sec4/

Daniel J. Ryan, G. S. (2010). *Legal Aspects of Digital Forensics.* http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf.

Dylan Yaga, P. M. (2018). *Blockchain Technology Overview.* NIST. doi:https://doi.org/10.6028/NIST.IR.8202

Epstein, B. (2018, August). Seargant, New Brunswick (NJ) Department of Police.

Ford, D. (2018, August). DME Lab Manager, Northern Colorado Forensic Lab, Weld County (CO) Sheriff's Office.

International Association for Property and Evidence, Inc. (2018, May). *Manuals and Guides*. Retrieved from http://home.iape.org/evidence-resources/guides-and-manuals.html

Jacobi, J. L. (2015). *PCWorld*. Retrieved from https://www.pcworld.com/article/2933478/m-disc-optical-media-reviewed-your-data-good-for-a-thousand-years.html

Joseph T. Latta, R. E. (n.d.). *IAPE Professional Standards.* International Association for Property and Evidence, Inc.

Kingsley-Hughes, A. (2012, November 28). Can A Magnet Destroy A PC? *Forbes*, pp. https://www.forbes.com/sites/adriankingsleyhughes/2012/11/28/can-a-magnet-destroy-a-pc/#eb684f97de0f.

Kissel, R. (2014). *Guidelines for Media Sanitization.* https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final: National Institute of Standards and Technology.

Library of Congress CD-R & DVD-R . (2020). *CD-R and DVD-R RW Longevity Research* . Retrieved from https://www.loc.gov/preservation/scientists/projects/cd-r_dvd-r_rw_longevity.html

Library of Congress CD-ROM. (2020, January 28). *Library of Congress* . Retrieved from CD-ROM Longevity Research: https://www.loc.gov/preservation/scientists/projects/cd_longevity.html

Library of Congress Formats. (2020, January 27). *Recommended Formats Statement*. Retrieved from Library Of Congress: http://www.loc.gov/preservation/resources/rfs/

Magnelli, M. (2018, February). Sergeant, Evidence Unit Manager, Montgomery County (MD) Department of Police.

Molina Granja, F. a. (2017). The preservation of digital evidence and its admissibility in the court. *Int. J. Electronic Security and Digital Forensics*, Vol. 9, No. 1, pp.1–18.

MS-ISAC. (2020). Retrieved from https://www.cisecurity.org/ms-isac/

National Institute of Justice. (2008). *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition.* NIJ.

Naval Air Warfare Center Weapons Division, Life Cycle and Environmental Engineering Branch. (2009). *Accelerated Life Cycle Comparison of Millenniata.* China Lake, CA: US Navy.

NDSA. (n.d.). *Checking Your Digital Content*. Retrieved from Digital Preservation: http://hdl.loc.gov/loc.gdc/lcpub.2013655117.1

NIST CSRC. (2020). *csrc*. Retrieved from Computer Security Resource Center: csrc.nist.gov

Oliver Slattery, R. L. (2004). Stability Comparison of Recordable Optical Discs--A study of Error Rates in Harsh Conditions. *Journal of Research of the National Institue of Standards and Technology, [J. Res. Natl. Inst. Stand. Technol. 109, 517-524 (2004)*. Retrieved from https://www.loc.gov/preservation/scientists/projects/j95sla.pdf

Optical Storage Technology. (2004). *Understanding Recordable & Rewritable DVD*. Retrieved from http://www.osta.org/technology/dvdqa/dvdqa11.htm

Paula De Stefano et al, C. F. (2014). *Checking Your Digital Content.* http://www.digitalpreservation.gov/documents/NDSA-Fixity-Guidance-Report-final100214.pdf: NDSA.

Perdereau, J. (2012). *https://www.lne.fr/sites/default/files/inline-files/syylex-glass-dvd-accelerated-aging-report.pdf.* Laboratoire National de Metrologie et D'Essais - Laboratoires de Trappes. Retrieved from https://www.lne.fr/sites/default/files/inline-files/syylex-glass-dvd-accelerated-aging-report.pdf

Scientific Working Group on Digital Evidence. (n.d.). Retrieved from Scientific Working Group on Digital Evidence: https://swgde.org

Scientific Working Group on Digital Evidence. (2018). *SWGDE Best Practices for Mobile Device Evidence Collection, Preservation, and Acquisition.* SWGDE. Retrieved from https://www.swgde.org/documents/Released%20For%20Public%20Comment/SWGDE%20Best%20Practices%20for%20Mobile%20Device%20Evidence%20Collection,%20Preservation,%20and%20Acquisition

Scientific Working Group on Digital Evidence. (2019). *SWGDE Best Practices for Mobile Device Evidence Collection and Preservation, Handling, and Acquisition.* https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Mobile%20Device%20Evidence%20Collection%20and%20Preservation,%20Handling,%20and%20Acquisition.

Scientific Working Group on Digital Evidence. (2019). *SWGDE Position on the Use of MD5 and SHA1 Hash Algorithms in Digital.* www.swgde.org.

Szejnmann, C. (2008). *How long should a DVD last?* Retrieved from The Guardian: https://www.theguardian.com/technology/askjack/2008/may/08/howlongshouldadvdlast

Veaux, F. (2018, September 18). Why are solid-state drive (SSD) not suited for archival purposes? *Quora*, pp. https://www.quora.com/Why-are-solid-state-drive-SSD-not-suited-for-archival-purposes.

Virginia Department of Forensic Science. (2018). *DIGITAL & MULTIMEDIA EVIDENCE SECTIOI PROCEDURES MANUAL.* Virginia Department of Forensic Science.

Walraven, T. (2018, August). DC Department of Forensic Sciences.

Yu, M. (2018, February). Sergeant, Montgomery County (MD) Department of Police.