Scientific Working Group on Digital Evidence

Position on Timely Preservation via Digital Acquisition

25-F-001-1.0

Disclaimer Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish standards, requirements, best practices, guidelines, technical notes, positions, and considerations in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

SWGDE requests notification by email before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in such proceeding. The notification should include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be submitted via the SWGDE Notice of Use/Redistribution Form or sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, deprecated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

Redistribution Policy

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain this SWGDE cover page containing the Disclaimer Regarding Use.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or creation date) of the document and also indicate if the document is in a draft status.

Requests for Modification

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be submitted via the SWGDE Request for Modification Form or forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address

d) Telephone number and email address
e) SWGDE Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for suggested modification

Intellectual Property

All images, tables, and figures in SWGDE documents are developed and owned by SWGDE, unless otherwise credited.

Unauthorized use of the SWGDE logo or document content, including images, tables, and figures, without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Scientific Working Group on Digital Evidence

Position on Timely Preservation via Digital Acquisition

Table of Contents

1. Purpose

The purpose of this document is to define the SWGDE position regarding the digital acquisition of data being used as a preservation technique. This document will also clarify caveats, outline parameters to determine acceptable use of preservation by digital acquisition, and demystify the process of acquiring data, while counteracting misinformation or misunderstanding of the technique.

2. Scope and Limitations

This paper references the necessary preservation of ephemeral data stored within modern digital devices. It is not meant to be extrapolated to digital devices that do not risk having their data becoming unrecoverable. The continued evolution of digital devices requires regular updates with regard to legal understanding.

3. Definitions

- **Acquisition**: In digital forensics, the process of using an access interface to read digital data from a digital source and to create a destination object.
- **Seizure**: When an individual with the legal authority removes property from an individual's possession following unlawful activity or to satisfy a judgment entered by the court.
- **Preservation**: The intentional act to prevent damage, contamination, alteration, or deterioration of anything contained within a scene.
- **Unrecoverable**: Data that has been rendered inaccessible and can no longer be acquired.

4. Background

Software and hardware manufacturers have implemented automated processes that render certain data unrecoverable, causing investigators to lose access to crucial evidence before they can acquire and analyze it. Network isolation alone cannot prevent automated processes on the device from irreversibly altering data into a non-recoverable format, making prompt digital acquisition critical to preserving crucial evidence. Time-sensitive data, such as logs, pictures, messages, or location history, often plays a critical role in reconstructing events or establishing evidence.

In digital forensics, preservation is the process undertaken to maintain the integrity of potential digital evidence. The process of preserving digital data may necessitate immediate exfiltration or other techniques that circumvent processes that render data otherwise inaccessible. Preservation prevents automated, unintentional, or malicious triggering of irreversible data-removal processes, preserving ephemeral evidence that would otherwise be rendered permanently unrecoverable. Digital acquisition involves the technical process of extracting or copying digital information from a device without interpreting, analyzing, or reviewing the data. However, current tool methodologies sometimes involve presentation of interpretation upon acquisition. Tools should allow the option to acquire without providing interpreted data. Multiple methods of preservation

exist to include triggering local device storage (e.g., diagnostic and crash logs) and digital acquisition of data to external media. By preserving data, investigators have the opportunity to review potentially vital evidence both exculpatory and inculpatory.

The need for preserving modern digital devices by digital acquisition techniques ensures the evidence data set contains the most accurate representation of the activity at the time of seizure. The resultant file or files generated from the extraction should now be considered a preserved copy of acquired data. This ensures that crucial evidence is not permanently lost.

Modern digital devices cause data to become unrecoverable over time. A contemporaneous digital acquisition of a device allows for the most equitable and just outcome of inquiry. This dataset will include both inculpatory and exculpatory data. Allowing this data to spoliate may deprive any party from providing their best explanation of an event. Loss of power or a simple reboot of the system can render data permanently unavailable with current technology. For this reason, urgency exists to preserve data while it's still accessible.

5. Examples of Unrecoverable Data

Examples of current unrecoverable data due to specific automated timelines include, but are not limited to, chat messages, media files, locations, log files that track both user and system activity, operating system artifacts, and internet activity. Additionally, certain manufacturers have implemented an automated reboot feature for mobile phones after a certain period, which can result in data encryption, making all data unrecoverable without the access credentials. Applications exist that allow users to delete all of their data with no physical interaction given a preconfigured stimulus or timeframe. Some digital devices need to remain powered on, attached to charging power, which may result in hardware destruction. Technological advancements are inevitable and will undoubtedly drive further changes, impacting even more data types that could become unrecoverable.

6. Analogous Preservation

Digital devices continue to present new legal challenges in the courts. While these devices will never be completely analogous to tangible evidence items, we must find acceptable similarities in our reach for a balance of privacy and justice. The courts have long held that there are acceptable reasons to preserve evidence that would otherwise be destroyed.

6.1 California v. Trombetta, 467 U.S. 479 (1984)

In *California v. Trombetta*, the Court opined, “We have long interpreted [this] standard of fairness to require that criminal defendants be afforded a meaningful opportunity to present a complete defense” [1]. The risk exists whereby automatic security functions of the device may destroy or otherwise render evidence, exculpatory or inculpatory, permanently inaccessible while outside the possession of the owner/operator. With this understanding, best practice dictates the

practitioner must perform the necessary operations required to preserve evidence in their possession.

6.2 New Jersey v. Hempele, 120 N.J. 182 (1990)

In *New Jersey v. Hempele*, the State Supreme Court addressed the constitutionality of warrantless searches of trash left at the curb for collection. They determined that trash is protected due to personal and sensitive contents, same with digital devices [2]. *State v. Pasanen*, 229 N.J. Super. (1989) was reviewed simultaneously. The court determined the officer did not require a warrant to seize the trash bags due to their reasonable suspicion and a warrant was required to go through the contents of the bag [3]. This reasoning applies to digital data as during the extraction process examiners are using a forensic tool to preserve a copy of the data, and not reviewing the data (e.g., the digital trash bag can be preserved pending a warrant).

6.3 New Jersey v. DeLuca, 168 N.J. 626 (2001)

In *New Jersey v. DeLuca*, a detective seized a pager from a suspect of a robbery. Being familiar with the volatile nature and limited memory of data on a pager, the detective recognized that new incoming data would overwrite the stored data on the device. The officer read through and recorded the numbers currently on the pager, preserving that data. The court ruled that the detective did not need a warrant due to the probability that this data would disappear and become nonrecoverable. A digital acquisition of a modern digital device is less intrusive than in DeLuca, as the detective viewed the contents of the pager whereas data preserved via modern digital acquisition can be obtained in a form that maintains the privacy rights of the owner/operator of the device [4].

6.4 Illinois v. McArthur, 531 U.S. 326 (2001)

In *Illinois v. McArthur*, police officers responding to a domestic dispute suspected that the defendant was hiding marijuana inside his home. In order to prevent the evidence from being destroyed, they temporarily restricted him from entering the house alone while they obtained a search warrant. The Court ruled that the officer's actions were reasonable under these circumstances [5]. Conducting a digital acquisition for preservation can prevent the loss of data, not only from automated processes, but also malicious intent attempts, such as manual deletion of data (e.g., a user/owner deleting pictures). The aforementioned data examples are both susceptible to being unrecoverable due to passage of time alone. For example, deleted pictures, on some devices, are still recoverable with forensic tools if data was acquired and memorialized in a timely fashion.

6.5 Holmes v. South Carolina, 547 U.S. 319 (2006)

In *Holmes v. South Carolin*a, the Court found that the defendant had been denied the opportunity to present a legal defense by being barred from introducing evidence that indicated the guilt of a different party [6]. A legitimate defense could include evidence of malicious software having

been responsible for a criminal act; it is necessary for examiners to preserve indicators of this activity. Research has shown that this activity can be found in device system logs. These logs are often of a fixed size that overwrite themselves in a matter of hours or days and become unrecoverable.

7. SWGDE Position

Timely preservation of data on a digital device is crucial for forensic investigations because it ensures the integrity and completeness of the evidence. By safeguarding data, investigators maintain the reliability, admissibility, and evidentiary value of the information, ensuring a thorough and just investigative process. Data is nonrecoverable if not captured during its window of availability. It is essential to continuously update our understanding and methodologies to deal with digital evidence.

8. References

[1] California v. Trombetta, 467 U.S. 479 (1984).

[2] New Jersey v. Hempele. 120 N.J. 182 (Supreme Court of New Jersey 1990).

[3] State v. Pasanen, 229 N.J. Super. 553 (New Jersey Superior Court 1989).

[4] New Jersey v. DeLuca, 168 N.J. 626 (2001).

[5] Illinois v. McArthur, 531 U.S. 326 (2001).

[6] Holmes v. South Carolina, 547 U.S. 319 (2006).

9. Additional Resources

- Apple. "Apple Platform Security Guide." *Apple Platform Security*. Accessed 15 Jan. 2025.
- Apple. "Data Protection Classes." *Apple Platform Security*. Accessed 15 Jan. 2025.
- Apple. “Delete or Hide Photos and Videos on iPhone.” *iPhone User Guide.* https://support.apple.com/guide/iphone/delete-or-hide-photos-and-videos-iphb4defbde9/18.0/ios/18.0. Accessed 15 Jan. 2025.
- Apple. “Recover Deleted Messages in Message on iPhone.” *iPhone User Guide*. https://support.apple.com/guide/iphone/recover-deleted-messages-iph16ecebf48/ios. Accessed 15 Jan. 2025.
- Awad, Yusuf M., et al. "Proposed Methodology for Battery Aging and Drainage Mitigation." *International Journal of Intelligent Computing and Information Sciences*, vol 24, no. 1, 2024, pp. 42-54.

- Epstein, Brandon, et al. " Analysis of Sysdiagnose in iOS 15 to Identify the Sending Phone Number of AirDrop Data." *Journal of Forensics Sciences*, vol. 67, no. 4, 2022, pp. 1704-1707.
- Google. “Restore Recently Deleted Photos & Videos.” *Google Photos Help.* https://support.google.com/photos/answer/9343482?hl=en-GB&co=GENIE.Platform%3DDesktop&sjid=2066554013321820896-NA. Accessed 15 Jan. 2025.
- Heath, Howard, et al. "Forensic Investigations of Popular Ephemeral Messaging Applications on Android and iOS Platforms." *International Journal on Advances in Security*, vol. 13, no. 1-2, 2020, pp. 41-53.
- Heinrich, Alexander, et al. "AirGuard-Protecting Android Users from Stalking Attacks by Apple Find My Devices." *WiSec ’22: Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, San Antonio, TX, US, 2022, pp. 16-38.
- JISKA. "Reverse Engineering iOS 18 Inactivity Reboot." *Naehrdine*, 17 Nov. 2024, https://naehrdine.blogspot.com/2024/11/reverse-engineering-ios-18-inactivity.html. Accessed 15 Jan. 2025.
- Kelkar, Soham P. *Detecting Information Leakage in Android Malware Using Static Taint Analysis*. Wright State University, Master of Science in Cyber Security, MA Thesis, 2017.
- Khan, Shujahat Ali, et al. "An Android Applications Vulnerability Analysis Using MobSF." *2024 International Conference on Engineering & Computing Technologies (ICECT)*, Islamabad, Pakistan, 2024, pp. 1-7.
- Lucky [x13a]. “x13a/Wasted: Lock and Wipe on Emergency: Source Code and Read Me.” *Github,* 2022, https://github.com/x13a/Wasted. Accessed 15 Jan. 2025
- Lyons, Allan. *Be Careful What You Write, Someone Might Read It: Logging Personally Identifiable Information on Android*. University of Calgary, MA of Computer Science, MA Thesis, 2023.
- Moser, Katherine. "Database Forensics for Analyzing Data Loss in Delayed Extraction Cases." *A Practical Hands-on Approach to Database Forensics*. Springer, 2022, pp. 175-232.
- Toby. "GrapheneOS Review." *Gear-Report*. https://gear-report.com/grapheneos-review/. Accessed 15 Jan. 2025.
- Whiffin, Ian. “Location, Location, Location.” *DFIR Review*, 29 Aug. 2024, https://dfir.pubpub.org/pub/4fkeiv34/release/1. Accessed 15 Jan. 2025.

10. History

Revision	Issue Date	History
1.0	1/16/2025	Initial draft created. SWGDE voted to approve as a Final Approved Document.
1.0	2/18/2025	Formatted for release as a Final Approved Document.