



A Methodology for Verification Testing of Data Evidence in Mobile Forensics

by

Lorie Hermesdorf

lorie.hermesdorf@mymail.champlain.edu

Master's Thesis

Master's Digital Forensic Science

Abstract

Digital forensics is a sub-discipline of forensic science. As such, the profession should follow the pillars of the scientific method to include hypotheses, testing, and error identification. The testing involves hardware and software. First, there is validation testing of forensic tools. Validation occurs at first use. Where forensic software is concerned, testing should occur again whenever there are significant updates or upgrades to the software. Hardware is tested when first placed in service, and then periodically thereafter or as policy dictates. Then, there is testing that verifies forensic tool output if there is a question about the validity of the output.

Where the courts are concerned, digital evidence must meet the *Daubert* standard for the evidence admittance. The *Daubert* standard presents what is required to meet the standard. One of those requirements involves tool testing. For many years now, there have been calls from digital forensic researchers regarding the need for testing of tools. Over the past few years,' critics have begun to doubt the science behind digital forensics. These critics point to the lack of testing as well as a failure to report errors (Erbacher, 2010. Beckett et al., 2011; Arshad et al., 2018). These issues have made some doubt whether digital forensics is a science at all. For the field of digital forensics to maintain a status in science, the testing must take priority.

This paper will deal with a branch of digital forensics called mobile forensics. Mobile forensics has overtaken the traditional computer forensics since the late 2000s, or around the time Apple introduced the iPhone. This device and other smartphone devices now on the market are handheld computers. In the past few years, the storage capabilities internally within the device have gone from 16GB to 256GB.

Introduction

Mobile devices or smartphones have been trendy since Apple introduced the iPhone back in 2007. According to Arne Holst (2019), there are approximately 269 million smartphone users in the U.S. or roughly 70% of the U.S. population (Holst, 2019). These devices have internet capabilities, and, over the years, the number of mobile applications has exploded. J. Clement (2020) recently published an article on [statista.com](https://www.statista.com), providing statistics on the number of apps available currently in the top app stores. The Apple App, 1.84 million apps, the most popular app store, is Google Play, which offers 2.57 million apps to its customers (Clement, 2020). There is no single mobile forensic tool on the market currently that can output all data stored either on the device or now in the cloud.

The Computer Forensic Tool Testing (CFTT) project is a joint effort of the U.S. Department of Homeland Security (DHS), the National Institute of Justice (NIJ), and the National Institute of Standards and Technology (NIST). The mobile forensic tool vendors submit their software for validation testing. The CFTT test reports can be available from the Department of Homeland Security, science, and technology section. Two popular mobile forensic tools are Cellebrite UFED and Oxygen Forensics Detective. In April 2019, a test report of Cellebrite UFED4PC v. 7.8.0.942 and Physical Analyzer v. 7.9.0.223 was published. The test results from iOS devices are represented in the tables below. Currently, mobile forensic examiners are utilizing version 7.32.0.16. The release should be taken into consideration upon reviewing the table of results. Further, it should be noted that while the iPhone models and iPad models are listed, there is no documentation on the iOS version. Also, there is no explanation in the report of what the criteria is for the table data labeled “as expected.”

A Methodology for Verification Testing of Data Evidence in Mobile Forensics

UFED 4PC v7.8.0.942/Physical Analyzer v7.9.0.223								
Test Cases – Internal Memory Acquisition		Mobile Device Platform: iOS						
		iPhone 4	iPhone 5S	iPhone 6S Plus	iPhone 7	iPhone 8	iPhone 8 Plus	iPhone X
Acquisition	Acquire All	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Disrupted	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Reporting	Preview-Pane	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Generated Reports	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Equipment/ User Data	IMEI	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	MEID/ESN	NA	NA	NA	NA	NA	NA	NA
	MSISDN	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
PIM Data	Contacts	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Calendar	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Memos/Notes	As Expected	As Expected	As Expected	Partial	As Expected	As Expected	As Expected
Call Logs	Incoming	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Outgoing	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Missed	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
SMS Messages	Incoming	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Outgoing	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
MMS Messages	Graphic	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Audio	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Video	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Stand-alone Files	Graphic	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Audio	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Video	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Application Data	Documents (txt, pdf files)	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Facebook	NA	Partial	Partial	Partial	Partial	Partial	Partial

UFED 4PC v7.8.0.942/Physical Analyzer v7.9.0.223								
Test Cases – Internal Memory Acquisition		Mobile Device Platform: iOS						
		iPhone 4	iPhone 5S	iPhone 6S Plus	iPhone 7	iPhone 8	iPhone 8 Plus	iPhone X
Social Media Data	Twitter	NA	As Expected	Partial	As Expected	Partial	Partial	Partial
	LinkedIn	NA	Partial	As Expected	As Expected	Partial	Partial	Partial
	Instagram	NA	NA	Partial	Partial	Partial	Partial	Partial
	Pinterest	NA	NA	NA	NA	Partial	Partial	Partial
	SnapChat	NA	NA	NA	NA	Partial	Partial	Partial
	WhatsApp	NA	NA	NA	NA	As Expected	As Expected	As Expected
Internet Data	Bookmarks	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	History	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Email	As Expected	NA	NA	NA	NA	NA	NA
GPS Data	Coordinates/Geo-tagged	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Non-Latin Character	Reported in native format	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Hashing	Case File/Individual Files	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Case File Data Protection	Modify Case Data	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected

Figure 1. Cellebrite UFED4PC and Physical Analyzer iOS test results. From NIST CFTT test report published April 20, 2019.

Next is the CFTT test report of the Oxygen Forensics mobile forensic tool. This report is the result of testing version 10.0.0.81. The current version of this tool is Oxygen Forensics Detective v. 12.3.0.16. Once again, the iPhone and iPad device models are listed, but there is no mention of the iOS version.

A Methodology for Verification Testing of Data Evidence in Mobile Forensics

Oxygen Forensics v10.0.0.81								
Test Cases – Internal Memory Acquisition		Mobile Device Platform: iOS						
		iPhone 4	iPhone 5S	iPhone 6S Plus	iPhone 7 Plus	iPad Mini	iPad Air	iPad Pro
Acquisition	Acquire All	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Disrupted	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Reporting	Preview-Pane	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Generated Reports	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Equipment/ User Data	IMEI	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	MEID/ESN	NA	NA	NA	NA	NA	NA	NA
	MSISDN	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
PIM Data	Contacts	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Calendar	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Memos/Notes	As Expected	As Expected	As Expected	Partial Expected	As Expected	Partial Expected	As Expected
Call Logs	Incoming	As Expected	Partial	As Expected	As Expected	NA	NA	NA
	Outgoing	As Expected	Partial	As Expected	As Expected	NA	NA	NA
	Missed	As Expected	Partial	As Expected	As Expected	NA	NA	NA
SMS Messages	Incoming	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Outgoing	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
MMS Messages	Graphic	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Audio	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Video	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Stand-alone Files	Graphic	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Audio	Not As Expected	Not As Expected	Not As Expected	Not As Expected	Not As Expected	Not As Expected	Not As Expected
	Video	Not As Expected	As Expected	As Expected	Partial Expected	As Expected	As Expected	As Expected
Application Data	Documents (txt, pdf files)	Not As Expected	Not As Expected	Not As Expected	Not As Expected	Not As Expected	Not As Expected	Not As Expected

Oxygen Forensics v10.0.0.81								
Test Cases – Internal Memory Acquisition		Mobile Device Platform: iOS						
		iPhone 4	iPhone 5S	iPhone 6S Plus	iPhone 7 Plus	iPad Mini	iPad Air	iPad Pro
Social Media Data	Facebook	NA	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Twitter	NA	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	LinkedIn	NA	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Instagram	NA	NA	As Expected	As Expected	As Expected	NA	As Expected
Internet Data	Bookmarks	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	History	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Email	As Expected	NA	NA	NA	NA	NA	NA
GPS Data	Coordinates/Geo-tagged	As Expected	Not As Expected	As Expected	Not As Expected	As Expected	As Expected	As Expected
Non-Latin Character	Reported in native format	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Hashing	Case File/Individual Files	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Case File Data Protection	Modify Case Data	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected

Figure 2. Oxygen Forensics v. 10.0.0.16 iOS devices test results. From NIST CFTT test report published April 15, 2018.

The digital forensic examination of mobile devices is critical to law enforcement as there is hardly a crime committed these days where a smartphone does not contain digital evidence of the crime. The digital evidence on these devices is also essential to civil litigation teams. Therefore, digital evidence must continue to be accepted by the courts.

Literature Review

This literature review is historical to demonstrate how long this topic has been calling out for attention. This researcher has selected research articles from 2010-2019. In 2010 researcher Robert F. Erbacher presented his research paper, *Validation for Digital Forensics*, to the seventh

International Conference on Information Technology. Immediately, in the introduction Erbacher (2010) posits that "no complete groundwork has been identified for the source of error in digital evidence" (Erbacher, 2010, p. 756). He follows this by delving into the legal admissibility issues of digital evidence as required by the Frye standard, which one of the requirements is the reporting of errors. Interestingly, he is in favor of the calculation of mean error rates and standard deviations.

Erbacher (2010) continues by explaining and providing definitions of "error- identifies the likelihood that the result is wrong," and "validation- identifies whether the actual solution is correct in terms of acceptance by the scientific community" (Erbacher, 2010, pg. 757). He then addresses the seven implications of validation throughout the forensic process. To demonstrate the seriousness of this issue, he lists a few failures of other forensic sciences, such as the Breathalyzer algorithm used to determine the amount of alcohol on the breath of a driver, was never scientifically validated. Next, the FBI ACE-V methodology for the latent fingerprint analysis system was never validated that it returned all potential matches. Thus, there existed the potential of singling out the wrong suspect.

Erbacher (2010) writes that validation is essential in the following steps of the forensic process,

- data generation
- data collection
- data storage
- system validation
- application validation
- algorithm applicability

- Algorithm implementation (Erbacher, 2010, p. 759).

While Erbacher demonstrates the need for error rates and standard deviations, he only presented one calculation for error in data storage. Erbacher (2010) concludes his research by commenting that as more attorneys become knowledgeable in digital forensic evidence, there will be more *Frye* challenges. There are currently two primary digital evidence admissibility standards, *Daubert* and *Frye*. It is unclear why this researcher only chooses to mention the *Frye* standard.

He identifies that more research is needed in the area of software errors as they are not well known (Erbacher, 2010). It would have been more beneficial if the researcher had presented specific instances where digital forensic errors caused a significant outcome in a criminal case. The failure of tool testing within digital forensics is an issue. The field risks becoming junk science.

Beckett and Slay (2011) write that the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) formally recognized digital forensics in 2003 as an accredited field. These researchers go on to present a short history of science and the scientific method. Next, they provide a quote from the U.S. Supreme Court in the *Daubert v. Merrell Dow Pharmaceutical* case, "science is not an encyclopedic body of knowledge about the universe. Instead, it represents a process for proposing and refining theoretical explanations about the world that are subject to further testing and refinement" (Beckett & Slay, 2011, pg.116).

Next, the researchers present the three main components of the modern scientific method, observation, hypothesis, and experimentation. The researchers assert that following a systematic process is what differentiates "sound science" from "junk science." They also call for standards

and errors in forensic science. Beckett & Slay (2011) provide criticism of forensic science by quoting Terrence Kiely, professor of Law at DePaul University. Kiely stated, "it is a significant problem that most forensic sciences that are used in the courts to adjudicate cases have never been tested" (Beckett & Slay, 2011, pg. 118).

Beckett and Slay (2011) continue with a review of ISO 17025 compliance process and documentation of the whole process of any lab analysis performed,

- validation of analytical methods and procedures
- equipment calibration testing and maintenance
- traceability
- control of non-conforming testing
- qualification of staff
- Written policies (Beckett & Slay, 2011, pg. 120).

The researchers write that the ISO 17025 lab compliance presents a challenge for digital forensics in two main areas, education and validation/verification testing of tools.

In the United States, the lab accreditation body, the American National Standards Institute (ANSI), now known as ANAB, and the digital forensics lab must meet the compliance standards within ISO/IEC 17025. The accreditation process is lengthy, and there is a fee. One of the members listed on the ANAB website is the Federal Bureau of Investigation-Quality Assurance Standards (FBI QAS) who conduct testing (ANAB Directory, n.d.).

The National Institute of Standards and Technology (NIST) (2014) published guidelines on mobile device forensics. The issue of tool testing is present within these guidelines. For instance, there is mention of tool errors such as, "inability to recover resident data, displayed data inconsistencies between workstation and tool report, and decoding/translation of recovered data"

(Ayers et al., 2014, pg. 25). NIST recommends that forensic tools be validated when updates or new versions of the tool are available. The tool validation process should include, "defining and identifying a comprehensive set of test data, following acquisition procedures to recover the test data, and assessment of results" (Ayers et al., 2014, pg. 25). This document acknowledges tool vendors' lack of providing detailed logs of data extraction, which would aid in assessing the tool validation. NIST specifically states that tool testing is necessary. Another recommendation regarding examiner up to date training on the tool they use is a method of dealing with human errors. The guidelines provide the examiner with a list of criteria to use when selecting a mobile forensic tool these are,

- Usability
- Comprehensive
- Accuracy
- Deterministic
- Verifiable
- And tested (Ayers et al., 2014).

The recommendation is that examiners use test devices to experiment with the tool's acquisition capabilities. Procedures for device acquisition should be tested and include documentation of validation. This validation process should consist of identification of possible solutions, testing on the same devices under known conditions, and documentation.

The examiner is directed to the NIST Computer Forensic Tool Testing (CFTT) program for test methods and reports. These test reports provide a mechanism for tool vendors to improve their product, and inform the examiner about potential anomalies, so they can make an informed choice on the tool they purchase (Ayers, et al, 2014).

The NIST publication is often cited and suggested for review by mobile device examiners. These guidelines attempt to place some standardization in the mobile device forensic process, which was still maturing at the time this document was published.

In 2017, researchers Grajeda et al. presented their research paper on the topic of data set availability for digital forensic research to the seventeenth annual DRFWS USA conference. They analyzed just over 700 peer-reviewed research papers spanning five years. Their focus was in three areas, (1) the origin of a dataset, (2) if researchers made their datasets publicly available, and (3) dataset types (Grajeda et al., 2017). These researchers posit that achievement of top-quality research, the datasets need to meet these three criteria,

1. quality of datasets
2. quantity of datasets
3. Availability of datasets (Grajeda et al., 2017).

They emphasize the fact that the scientific method requires the reproducibility of results. For this to occur, the tests require the same dataset, under the same conditions. Making datasets publicly available cannot be overstated. Grajeda et al. cite Abt & Baier (2014), who stated that "a lack of standards and available datasets presents three weaknesses in the digital forensic community. These weaknesses are "low reproducibility, comparability, and peer validated research" (Grajeda et al., 2017, pg. 595). The researchers located a little over 20 cellphone images distributed between two locations, CFReDs and Digital Corpora (Grajeda et al., 2017).

Since the publication of this research, Digital Corpora has recently added four new Android (smartphone) images of Android O.S. v. 7-10. Examiners have been making use of these Android images for testing, and instruction. However, there is a lack of iOS images. The two largest operating systems in current mobile devices are Android and iOS. As stated before,

mobile device forensics has outstripped what was commonly called "computer forensics" in the past 10-12 years. Yet, images related to mobile devices remain challenging to obtain.

Researchers Arshad et al. (2018) conducted a study focusing on issues in scientific validation of digital evidence. To begin with, they cite a recent amendment to the U.S. Federal Rule 902(14) that calls for the use of best practices in digital forensics. These researchers found that the "general view" is that digital evidence does not meet the scientific criteria required by the courts. They found that defense attorneys have a lack of trust in the digital forensic process, and have identified loopholes in the evidence collection process as well as comparison, which can introduce reasonable doubt in a case.

For digital forensic science to continue as sound science, the techniques used need to be verified and validated using a standard testing methodology. Once again, these researchers echo the fear of others before them that digital forensics is in peril of being considered a "junk science." Arshad et al. (2018) provide what they deem as the eleven characteristics of "good science,"

1. testable hypotheses
2. reproducible results
3. verifiable process
4. peer-review or publication
5. general acceptance by the community
6. standardization
7. experimentation
8. practicality
9. impartiality

10. realistic explanations

11. Use of precise methods (Arshad et al., 2018, pg. 349).

They write that the Daubert requirements are very similar to these characteristics. Arshad et al. (2018) once again sound the alarm bell in regards to the lack of verification and validation of the digital forensic process, and tools. They write this will reflect negatively on the field, especially where acceptance of digital evidence in court is concerned. These researchers have identified the following areas of concern,

- lack of sufficient datasets which contain current, in-depth data types
- creation of a dataset by an examiner could potentially introduce bias
- datasets for mobile forensics need to be from a current device, which can be costly
- The time to create mobile datasets can likely render the dataset obsolete by the time it is made available (Arshad et al., 2018).

According to these researchers, the absence of appropriate datasets makes it near impossible to conduct meaningful, in-depth testing in which to establish error rates to satisfy the Daubert requirements. These researchers agree with the newest Scientific Working Group on Digital Evidence (SWGDE) (2018) about most digital forensic errors being "systematic" rather than random. Further, they agree that statistical calculations of these types of errors are not possible due to the lack of population (static, unchanging), which is required.

Arshad, et al. (2018) reference the SWGDE (2018) *Error Mitigation Analysis* document. They focus on SWDGE's position that error mitigation methods should not focus solely on finding error rates. These researchers disagree with that position stating it is essential to calculate error rates where applicable. They note that the SWGDE (2018) document is useful in assisting examiners in understanding the fundamental validation issues associated with techniques

(processes), and explanation of the need for error mitigation for each process. The researchers close with commenting on weaknesses in the following areas, formal testing methods and development of sound scientific methods and best practices. They agree that these areas are difficult due to the rapid rate of change in technology.

Arshad et al. (2018) suggest the following areas for further research, creation of dataset with real-world data, development of new and formal testing methods, the establishment of matrices to quantify precision and accuracy of tools and practices, and identification of errors (Arshad et al., 2018).

These researchers present the fundamental building blocks of what constitutes "good science" very well. It was beneficial when they tied these characteristics to the Daubert requirements. Researchers could have listed the errors they thought could be calculated, and then suggest some calculation methods. They conducted an excellent review of current works in this area, especially the analysis of the SWDGE (2018) document on the issue of error mitigation in digital forensics.

Horsman (2019) identifies the problem of a lack of or inadequate tool testing. He wonders if the absence or poor quality of tool testing is related to the fact that the task is too difficult. He recommends the possible creation of a global regulatory body in the area of tool testing. Horsman (2019) cites that in the U.S., the NIST CFTT program has attempted to provide this service with forensic tool testing reports being made available. These reports are available through the Department of Homeland Security Science and Technology website. However, there remains a lack of research in the area of digital forensic tool testing. Horsman (2019) identifies three areas of tool testing that may have a significant effect on mobile digital investigations,

- data acquisition

- file system interpretation
- Artifact interpretation (Horsman, 2019).

The researcher is not suggesting that tool vendors are putting a sub-standard product on the market. Instead, the concern is that the vendors cannot test for every possible device, application, or potential error.

Again, the lack of publicly available datasets comes up. Horsman (2019) identifies the following issues related to this lack of datasets for mobile device testing,

- the time required to create the dataset
- proper documentation of the dataset created
- consideration of the cost/benefit analysis of the organization

Another area of concern is error testing. The researcher thinks there should be a differentiation between tool errors and user errors. Horsman (2019) cites researcher JR Lyle's paper published in 2010, where he listed what he considered to be the three most significant sources of errors, algorithm intended for the process, software implementation of the algorithm, and performance of the process by the user. In turn, these three sources are affected by the lack of standardized testing, organization accreditation, and differing levels of examiner training and experience (Horsman, 2019).

Horsman (2019) associates the cost/benefit analysis issues with contributing to more labs having taken to dual tool comparison testing. He has doubts about the soundness of this type of testing as both tools could erroneously interpret the data. This error could be due to the forensic software utilizing the same library for its code. For this reason, as well as others, this type of testing is questionable as a final solution for all digital forensic tool testing issues.

Horsman (2019) recognizes the following areas where tool testing, as well as data verification, are essential,

- System and application-specific parsing
- File system
- Image file
- Data acquisition
- Storage media (Horsman, 2019).

To gain a better understanding of the digital community's knowledge and concern in this area, he conducted a survey. A couple of items that stood out as concerning first that nearly $\frac{3}{4}$ of the respondents did have a concern over the current state of tool-testing. Of these, a little over 60% indicated they conduct their self-tests on forensic applications before their use. That means that a little over 30% do not test at all. Even more disturbing was nearly 80% of respondents indicated they use tools that they have never tested (Horsman, 2019).

So why is the need for tool testing and data testing so significant? Horsman (2019) identifies two main reasons, the number of forensic tools on the market, coupled with "endless functionality" (Horsman, pg. 173, 2019). He writes that the rapid changes in technology have driven the market to provide an endless number of tools, along with rapidly changing capabilities. Horsman (2019) cites work from Beckett and Slay (2007), whereby the researchers comment that the status of the digital forensics field calls for a continuous cycle of tool-testing that is being driven by technological advancements (Horsman, 2019). Further, he mentions that SWGDE (2017) writes in their document that "testing must be continuous and cannot be a one-time event" (Horsman, 2019, pg. 173). Horsman (2019) is correct in his assessment of the rapid rate of application updates. Which is especially true in mobile forensics. Further, he mentions the

lack of in-depth documentation associated with the application updates. Therefore, the examiner must conduct a revalidation since even simple changes to the underlying metadata within an application can affect a forensic tool's output (Horsman, 2019).

In closing, Horsman (2019) writes that while digital forensic tool testing is challenging, it does not mean that ignorance is acceptable. In his view, every valid attempt deserves support from the community to improve this situation. More importantly, he writes, "the field is under ethical and legal obligation to continue to strive to improve standards, so every step made in that direction should be taken" (Horsman, 2019, pg. 174).

The work by Horsman (2019) rightfully brings the most critical focus to the "ethical and legal" obligations the field of digital forensics has, to working on this issue. This issue has been beaconing from the past, and as yet has not established an answer to the problem. Horsman (2019) rightly addresses the issue with millions of applications being available to the user, especially in mobile application stores. Further, how the application updates may affect the forensic tool output. In mobile forensics, the examiner is not aware of the application updates or newer version availability unless they conduct this research on their own.

A few of the research papers mentioned have cited the SWDGE (2018) documents. Their documents titled *SWDGE Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis* as well as *SWDGE Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics* are in the next section.

Current Action

On November 20, 2018, the Scientific Working Group on Digital Evidence (SWGDE) published two documents, *Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics* and *Establishing Confidence in Digital and Multimedia Evidence Forensic*

Results by Error Mitigation. This paper will only address the recommendations for forensic tool testing. However, the courts consider the reporting of errors to be critical in the Daubert standard, so the reader should review the document on error mitigation.

The focus of this paper is on mobile forensics, and the SWDGE document on tool testing deals with mobile tool testing. In section 5.1.2.2, the testing of mobile device imagers is covered. There are two points of importance,

- The speed of change in both mobile devices and tools presents a real challenge.
- There is no one mobile forensic tool that can extract all data from all mobile devices (SWGDE, 2018).

In section 5.3.1, SWDGE recommends the following testing of what they call "search tools." These are tools that search for data, strings, data recovery, file identification, MAC times, and timeline analysis.

Testing, use a known dataset, or with manual verification. Known datasets must include relevant characteristics such as keyword searching, email, images, file types, and metadata.

Frequency, before the tool, is put in service, and after significant updates or revision.

In section 5.6, in-house developed tool issues are discussed. SWDGE notes that simple queries and scripts do not require testing. They describe the situations that require independent testing as,

- A tool or technique that is too complex to document in an examiner's notes.
- The amount of code is so large as not to fit into an examiner's notes.
- The results cannot be manually verified.
- Code not available to the digital forensic community.

Frequency, upon first use and after revisions (SWGDE, 2018, pg. 16).

Documentation of the testing is addressed in section 6 with the following recommendations of what information should be in the document,

- Purpose and scope (identify tool or technique)
- Who performed the test
- Date
- Testing procedures used or scenarios
- Datasets or other testing material used, including results
- Identify limitations (SWDGE, 2018, pg. 16).

One of the most significant issues in tool testing is the availability of community available mobile images. Just recently, Joshua Hickman, a digital forensic examiner, has made available Android O.S. versions 7-10, which include in-depth documentation. The Android O.S. versions 7-9 are available on the website Digital Corpora. The Android O.S. version 10 is available on Hickman's blog (Hickman, 2020). Hickman (2020) released two iOS images (versions 13.3.1 and 13.4.1) to the community in April 2020. These image files also contain in-depth documentation. Hickman (2020) writes that these images are free to use for education, research, and tool testing.

Digital Evidence Mobile Forensic Tool Issues

First, the iOS and Android operating systems are changing at a faster pace than in the past. This change includes how developers store user data within their applications such as SQLite databases, Realm databases, MongoDB, Knowledge-C, Google protocol buffers, and Google Room wrapper for SQL databases. Many of the commercial tools can deal with these databases and offer an SQLite editor within the tool itself. Some of the commercial tools offer a choice of different timestamp conversions to render the timestamp in human-readable format. In

contrast, others require an examiner to export the database file out and use a tool such as D.B. Browser for SQLite to navigate and query the database.

Sarah Edwards (2018) has conducted significant research in Knowledge-C databases, which are a type of SQL database, typically found in macOS and iOS. Edwards (2018) mentions in her blog that there is one main Knowledge-C database in iOS located in `/private/var/mobile/Library/CoreDuet/Knowledge/`, which is not in an iTunes backup. SQLite queries are interacting with the data. Some system files storing data in databases are, `/app/activity/`, `/app/inFocus/`, `/app/install/`, `/app/intents/`, `/device/batteryPercentage/`, and `/device/isLocked/` to name a few. Application usage on an iOS device can be in the `/app/inFocus/`. The timestamps within databases may require conversion to human-readable format. These timestamps formats are in seconds from UTC 2001, microseconds from UTC 2001, MAC Absolute time, and nanoseconds from UTC 2001. These databases may also include Binary Large Objects (BLOB), which can store images, videos, or even another database. Edwards (2018) suggests using the D.B. Browser for SQLite tool. If a BLOB is present, Edwards suggests double-clicking on the BLOB, and view the data in binary, text, or image (Edwards, 2018).

Speed and security are the main focuses of application developers. Where databases are concerned for some time now, SQLite databases were popular with iOS and Android apps for data storage. However, which database is chosen for data storage is a choice of the developer. For now, SQLite databases remain the top choice in mobile application databases. Some developers are choosing to use Realm databases such as MongoDB. According to Realm developers, their database platform offers the following improvements,

- Offline first database, this way if the user loses network connectivity they can still interact with their data

- Faster queries
- Safe threading reducing crashes
- Cross-platform
- Encryption (AES 256)
- Reactive architecture (Realm, n.d.)

Stefania Farrugia (2016) conducted an experiment with SQLite and NoSQL databases to compare their capabilities. What he found is that SQLite databases are designed to be less CPU intensive, memory constrained, and low energy (Farrugia, 2016). These factors make SQL a preferred choice by mobile application developers.

Beyond Commercial Tool Use for Testing

Another issue confronted by digital forensic labs when it comes to tool testing is the cost of commercial tools. Some smaller digital forensic labs and law enforcement labs simply do not have the budgets to cover two or more commercial mobile forensic tools. However, as was already stated by SWDGE (2018), "no one mobile forensic tool can extract all data from all mobile devices" (SWDGE, 2018, pg. 9).

The digital forensic examiner needs to be networking in the community, and this means attending local training, keeping up with experienced examiner blog posts, etc. It is the responsibility of the digital forensic examiner to keep their skills up to date. It is an error in and of itself to trust completely, without verification, what the commercial tool is reporting. Some of the brightest minds in the digital forensic community quote former President Ronald Reagan, "trust but verify!"

So, what are the options besides the use of another commercial tool to verify the commercial tool results? There are plenty of trusted GitHub repositories that contain python

scripts the digital examiner can download and utilize. Alexis Brignoni maintains one such repository. Brignoni (2019) developed a python tool that he calls iOS Logs, Events, and Properties Parser or iLEAPP. Alexis Brignoni (2019) writes in his blog that he built this tool for those smaller labs which do not have access to commercial tools due to funding (Brignoni, 2019). Additionally, he cites these other purposes for developing this tool,

- Create a central repository for iOS scripts written by himself
- Serve as an open-source tool for commercial tool testing
- Improve his python writing skills (Brignoni, 2019).

Brignoni did not stop there; he also developed the Android Logs, Events, and Protobuf Parser (ALEAPP). This tool is for the Android O.S. and is at Brignoni's GitHub repository. Both tools are continually being updated with new features added. Further, because they are open-source other digital forensic examiners are encouraged to contribute (Brignoni, 2020).

There are a few more open-source options for the Android O.S. than for iOS. Another no-cost option for Android O.S. is Autopsy developed and maintained by Brian Carrier (Carrier, 2020). There is another option for iOS, which is the Apple Pattern of Life Lazy Output'er (APOLLO) developed by Sarah Edwards. Sarah Edwards maintains this tool in her GitHub repository (Edwards, 2020). One more community resource is the website DFIR Training, managed by a digital forensic examiner, professor, and author Brett Shavers (DFIR Training, 2020).

A criticism of current academic research in mobile device forensics is the delay in getting the research papers published. Often, the issues specific to the study are already negated by the rapid changes not only in the mobile device O.S.'s, but hardware changes, and third party application changes. The peer-review process needs to be improved to provide up to date

research to the community. One non-profit organization, Digital Forensic Research Workshop (DFRWS), consisting of academia and practitioners, has been working on coming up with solutions to decrease the time it takes for practical research papers to be published such as DFIR Review (DFIR Review, 2020).

Methodology for Verification Testing of Data Evidence in Mobile Forensics

A mobile forensic examiner working either in a forensic lab or in a digital investigation unit lab should heed the advice of former President Ronald Reagan, "trust but verify." An examiner should verify what their commercial tool is representing either by use of another commercial tool, use of python scripts, or other open-source tools developed by experienced and trusted examiners.

The following hypotheses are tested in the development of this methodology, 1.) The commercial tools will process, parse, and display commonly observed third party iOS and Android applications, 2.) Not all commercial tools utilized in this test will parse all third party applications, databases or O.S. system files appropriately, 3.) Some files will require manual verification, and 4.) Commercial tool tests provided by the CFTT are out of date.

These are the recommended steps in this purposed methodology,

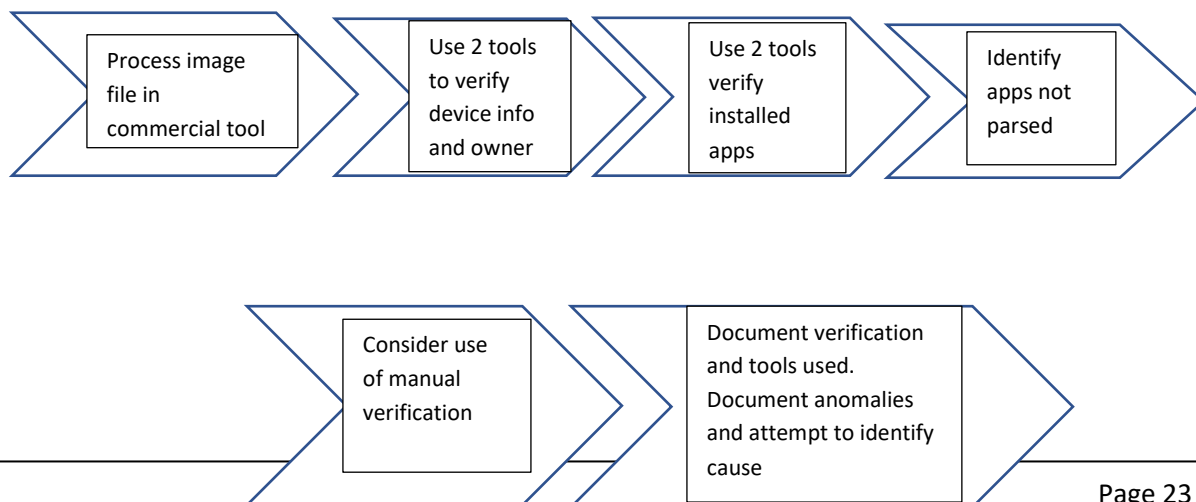


Figure 5. Methodology for Verification Testing of Data Evidence in Mobile Forensics.

The workstation utilized for the test of this process is an MSI Stealth laptop running Windows 10 Home version 1909, build 18363,720, 64 bit, an RAM 16GB, Intel Core I7 processor x64. Also utilizing VMware Workstation 15, and SANS SIFT Workstation running in a VMware virtual machine. Commercial tools within SIFT workstation are Cellebrite Physical Analyzer v. 7.32.0.16, Magnet Axion v. 3.11.0.1900, and Oxygen Forensic Detective v. 12.3.0.221. Open source tools used iLEAPP v. 1.0, and D.B. Browser for SQLite v. 3.11.2.

One of the most criticized issues from research in the past is the lack of mobile device images so that research could be replicated and verified. This issue will not affect this research as the image file used is the iOS 13.3.1 image file created by Josh Hickman. This image file is available in his blog on The Binary Hick.

The iOS 13.3.1 image data comes from an iPhone S.E., which is jailbroken using checkra1n. It was discovered that chipsets in the Apple iPhone model 5-X and other Apple devices contained a vulnerability allowing access to a full file system extraction. The following information is provided in a pdf file available within the image file download,

PHONE INFORMATION

Make: iPhone S.E. Model: A1662 (Rose Gold) Order Number: MLXL2LL/2 RAM: 2 G.B. Storage: 64 GB Carrier: Google Fi Phone Number: 919-579-4674 Serial: DX3T126VH2XV, Wi-Fi MAC: A0:D7:95:79:DD:A1 BT MAC: A0:D7:95:79:DD:A2. IOS VERSION

INFORMATION Version: 13.3.1 Build: 17D50, Passcode: 0731. As well as documentation of apps used on the device and data population within those applications. The iOS 13.3.1Extraction.zip

image file, size 9.0GB, MD5: d1456ce0aa836d6690fc9e13e55e3fd, SHA256: 496172037ae05c99878a8a8cb82bbd54ed8f56c98658acf59416310190af3d3, was downloaded from the Binary Hick website to MSI Stealth laptop, then copied to a SanDisk, 128GB exFAT formatted, USB 2.0 drive. The hashes were then verified using HashMyFiles. The files are extracted using 7zip. The file contained four folders, Extraction, Extraction Logs, iTunes Backup, and Sysdiagnose Logs. There is one .pdf file iOS-13-3-1-ImageCreation. The Extraction folder contains the image file, Apple iPhone S.E. (GSM) Full Image-13-3-1.tar.gz, size 15.6GB.

The USB was attached to the VMware SIFT virtual machine. The image file (**Apple iPhone S.E. (GSM) Full Image-13-3-1.tar.gz**) was first loaded into and processed by Oxygen Forensic Detective. Then the same file was loaded into and processed by Cellebrite Physical Analyzer. An issue was encountered while attempting to load the image file into the Magnet Axion tool. Axion did not see the file when pointed to it in the USB directory. Two database files (**/private/var/mobile/Library/CallHistoryDB/call-History.storedata**, and **/private/var/mobile/Library/CallHistoryDB/call-HistoryTemp.storedata**) were exported to the SIFT Windows 10 desktop, from the Cellebrite Physical Analyzer tool for analysis, and verification of timestamp conversions using the DB Browser for SQLite. Also, iLEAPP v. 1.0 was utilized from the command line using iLEAPP Master, ileappGUI.py.

Results

The iLEAPP tool parsed the iOS 13.3.1 image file with no problems. This tool creates HTML files that the examiner can use in their documentation. One of the HTML documents (Icon Positions) lays out how the applications are displayed on the screens of the iPhone S.E.,

A Methodology for Verification Testing of Data Evidence in Mobile Forensics

Icons screen #0			
com.apple.facetime	com.apple.mobilecal	com.apple.mobileslideshow	com.apple.camera
com.apple.Maps	com.apple.weather	com.apple.mobilenotes	com.apple.news
com.apple.AppStore	com.apple.podcasts	{'listUniqueIdentifiers': ['8AEA3798-8CC0-42A9-8C99-E2934FBE52C2'], 'iconLists': [['com.apple.Health', 'com.apple.Fitness', 'com.fitbit.FitbitMobile', 'com.redshiftdev.Fitbit-Health-Sync']], 'listType': 'folder', 'displayName': 'Health', 'uniqueIdentifier': '8A78AA4A-A95A-4505-A5FD-9E888F1C80FE'}	{'listUniqueIdentifiers': ['3D670AF9-B58B-46D1-A344-F1E89822E650'], 'iconLists': [['com.apple.Home', 'com.philips.lighting.hue2', 'com.belkin.plugin', 'com.signify.hue.blue']], 'listType': 'folder', 'displayName': 'Home', 'uniqueIdentifier': '61DBDB8B-2839-4DD8-B8F4-F27E681848FA'}
{'listUniqueIdentifiers': ['BEA36A80-25F7-4282-9873-C37066371A29'], 'iconLists': [['com.apple.Music', 'com.apple.MobileStore']], 'listType': 'folder', 'displayName': 'Music', 'uniqueIdentifier': '8C59A869-53F4-4A24-932A-3FA963721421'}	{'listUniqueIdentifiers': ['9A32331C-E35F-45A1-809F-F5518B8F65D0'], 'iconLists': [['com.apple.findmy', 'com.apple.Preferences', 'com.apple.Bridge', 'com.apple.DocumentsApp']], 'listType': 'folder', 'displayName': 'System', 'uniqueIdentifier': '63B1C5E3-ED74-4723-81B3-2741BF1A1868'}	{'listUniqueIdentifiers': ['EA1A8852-CEA3-432B-A52C-A982EFC0258B'], 'iconLists': [['com.apple.VoiceMemos', 'com.apple.compass', 'com.apple.measure', 'com.apple.calculator', 'com.apple.MobileAddressBook', 'com.apple.Passbook', 'com.apple.reminders', 'com.apple.mobiletimer', 'com.apple.stocks']], 'listType': 'folder', 'displayName': 'Default', 'uniqueIdentifier': '0537BCF6-112E-49F9-BE32-5598315C9949'}	
Icons screen #1			
com.hammerandchisel.discord	com.mentionmobile.cyberdust	com.facebook.Messenger	org.mozilla.ios.Focus
ingurmobile	co.babypenguin.imo	com.burtn.instagram	com.kik.chat
jp.naver.line	com.mewe	com.reddit.Reddit	org.whispersystems.signal
com.silencircle.SilentPhone	com.skout.SKOUT	com.skype.skype	com.toyopagroup.picaboo
com.spotify.client	ph.telegra.Telegraph	com.tinginteractive.usms	com.burtn.threads
Icons screen #2			
com.zhiliaapp.musically	com.miketigas.OnionBrowser	com.atebits.Tweetie2	net.kortina.labs.Venmo
com.viber	net.whatsapp.WhatsApp	com.mywickr.wickr	com.wearezeta.zclient.ios
ch.protonmail.protonmail	de.tutao.tutanota	com.adhoclabs.burner	com.herzick.houseparty
us.zoom.videomeetings	kjc.loader	com.saurik.Cydia	

Figure 6. Icon Position HTML report from iLEAPP.

```

14     <key>displayName</key>
15     <string>Folder</string>
16     <key>iconLists</key>
17     <array>
18     -   <array>
19         <string>com.apple.facetime</string>
20         <string>com.apple.mobilecal</string>
21         <string>com.apple.mobileslideshow</string>
22         <string>com.apple.camera</string>
23         <string>com.apple.Maps</string>
24         <string>com.apple.weather</string>
25         <string>com.apple.mobilenotes</string>
26         <string>com.apple.news</string>
27         <string>com.apple.AppStore</string>
28         <string>com.apple.podcasts</string>
29     -   <dict>
30         <key>displayName</key>
31         <string>Health</string>
32         <key>iconLists</key>
33     -   <array>
34     -   <array>
35         <string>com.apple.Health</string>
36         <string>com.apple.Fitness</string>
37         <string>com.fitbit.FitbitMobile</string>
38         <string>com.redshiftdev.Fitbit-Health-Sync</string>

```

```

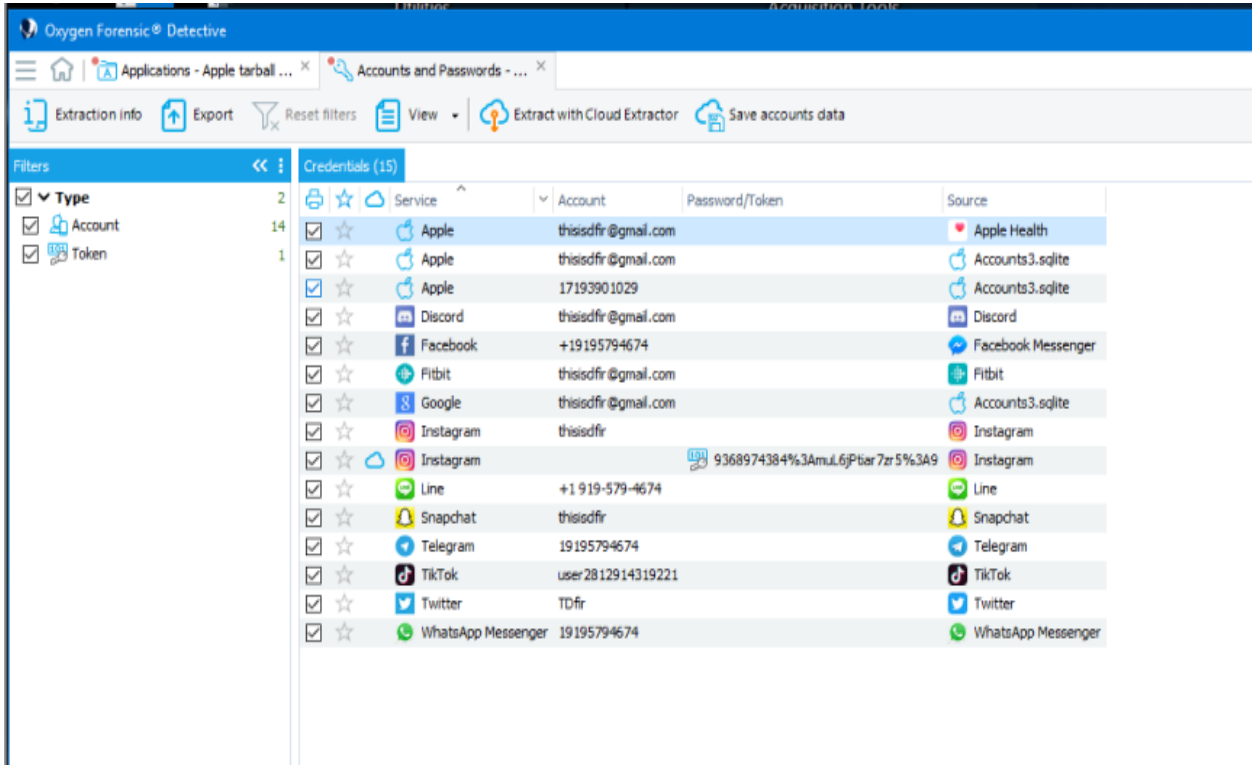
140     <string>com.mentionmobile.cyberdust</string>
141     <string>com.facebook.Messenger</string>
142     <string>org.mozilla.ios.Focus</string>
143     <string>imgurmobile</string>
144     <string>co.babypenguin.imo</string>
145     <string>com.burbn.instagram</string>
146     <string>com.kik.chat</string>
147     <string>jp.naver.line</string>
148     <string>com.mewe</string>
149     <string>com.reddit.Reddit</string>
150     <string>org.whispersystems.signal</string>
151     <string>com.silentcircle.SilentPhone</string>
152     <string>com.skout.SKOUT</string>
153     <string>com.skype.skype</string>
154     <string>com.toyopagroup.picaboo</string>
155     <string>com.spotify.client</string>
156     <string>ph.telegra.Telegraph</string>
157     <string>com.tinginteractive.usms</string>
158     <string>com.burbn.threads</string>
159 </array>
160 - <array>
161     <string>com.zhiliaapp.musically</string>
162     <string>com.miketigas.OnionBrowser</string>
163     <string>com.atebits.Tweetie2</string>
164     <string>net.kortina.labs.Venmo</string>
165     <string>com.viber</string>
166     <string>net.whatsapp.WhatsApp</string>
167     <string>com.mywickr.wickr</string>
168     <string>com.wearezeta.zclient.ios</string>
169     <string>ch.protonmail.protonmail</string>
170     <string>de.tutao.tutanota</string>
171     <string>com.adhoclabs.burner</string>
172     <string>com.herzick.houseparty</string>
173     <string>us.zoom.videomeetings</string>

```

Figure 7. Installed Apple stock apps and 3rd party apps, from iLEAPP report IconState.plist.

The report on the icon position of apps on the iPhone S.E. screens was verified by the images of the screens provided in the image file documentation file.

The Oxygen Forensic Detective tool did an excellent job of processing, parsing, and displaying the digital data. As observed in the snip below some applications were not parsed such as Wire, which is a secure message application,



Service	Account	Password/Token	Source
Apple	thisisdfr@gmail.com		Apple Health
Apple	thisisdfr@gmail.com		Accounts3.sqlite
Apple	17193901029		Accounts3.sqlite
Discord	thisisdfr@gmail.com		Discord
Facebook	+19195794674		Facebook Messenger
Fitbit	thisisdfr@gmail.com		Fitbit
Google	thisisdfr@gmail.com		Accounts3.sqlite
Instagram	thisisdfr		Instagram
Instagram		9368974384%3AmuL6jPtier7zr5%3A9	Instagram
Line	+1 919-579-4674		Line
Snapchat	thisisdfr		Snapchat
Telegram	19195794674		Telegram
TikTok	user2812914319221		TikTok
Twitter	TDfr		Twitter
WhatsApp Messenger	19195794674		WhatsApp Messenger

Figure 8. Oxygen Forensic Detective v. 12.3.0.221, Accounts, and Passwords.

Yet, the Cellebrite Physical Analyzer tool appeared to have some issues with the processing, parsing, and displaying the digital data,

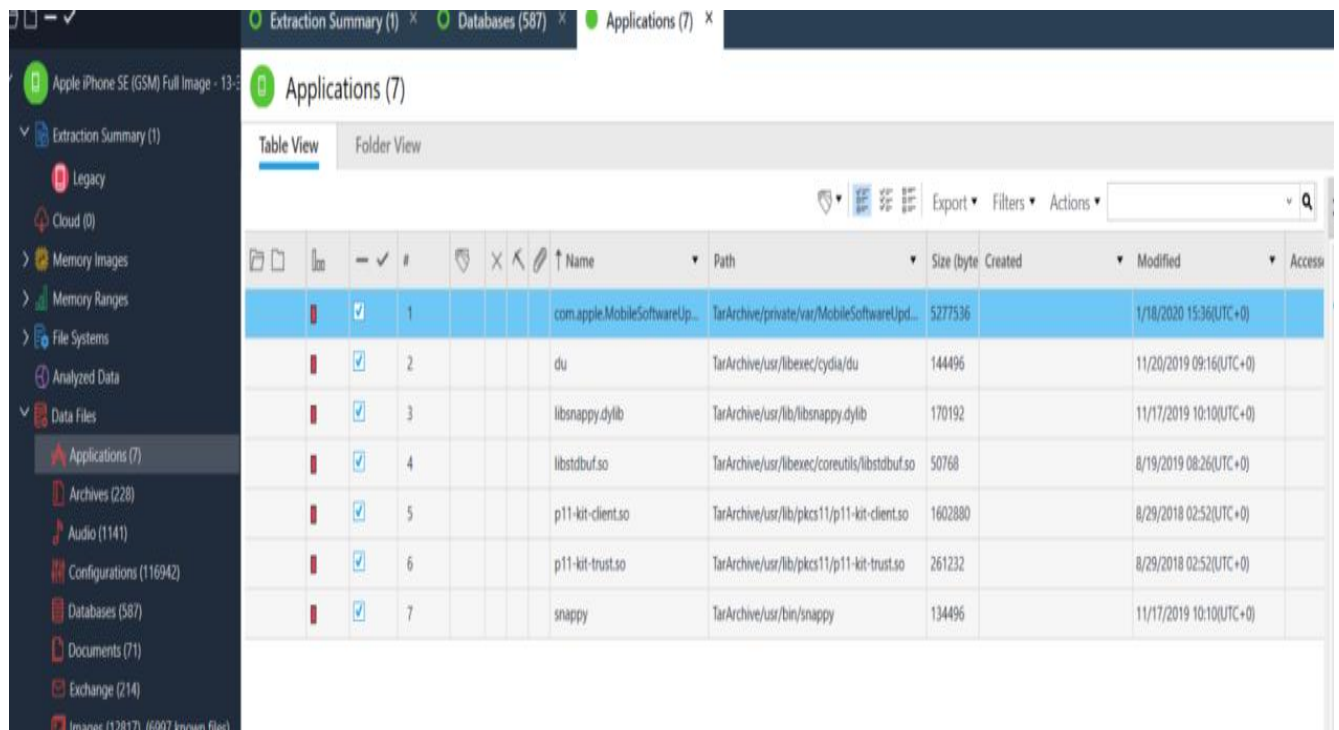


Figure 9. Cellebrite Physical Analyzer v. 7.32.0.16, Applications tab.

Still, iOS system apps, databases, and some third party applications were verified between these two tools. A manual keyword search for files was done within the Cellebrite Physical Analyzer tool. Even so, there was an anomaly noted within Cellebrite Physical Analyzer in that it did not parse any information about Wi-Fi connections from **/var/preferences/SystemConfiguration/com.apple.wifi.plist**. Yet, Oxygen Forensic Detective did the process and parsed this information. The displayed Wi-Fi connection name above was verified with the documentation provided with the iOS 13.3.1 Extraction.zip file.

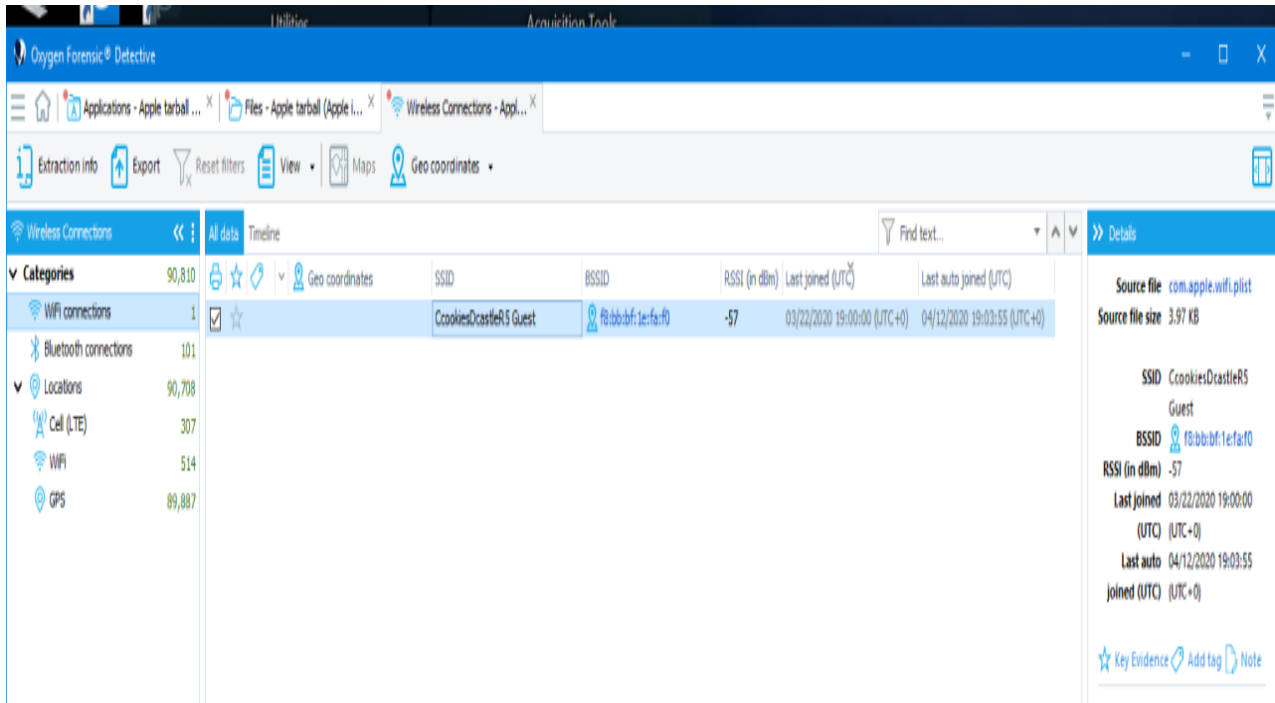


Figure 10. Oxygen Forensic Detective, display of Wi-Fi connections.

Next, the exported database files were opened **Read-only** in the D.B. Browser for SQLite.

There was an issue here. The database architecture was displayed correctly; however, there was no data in any of the tables. This tool was going to be utilized in confirming database timestamp conversions conducted using the SQL editor within the Oxygen Forensic Detective tool. Both exported database files from the Cellebrite Physical Analyzer tool presented the same issue when opened in D.B. Browser for SQLite. An unexpected anomaly presented here.

The iOS 13.3.1 creator Josh Hickman was contacted about the anomaly to determine if this was a "user error" or a "tool error." Hickman advised that the issue is with the underlying forensic workstation O.S., specifically Windows. The image file had no errors when used on a Macintosh or Linux O.S. Hickman stated that Windows presented iOS files that contained no data. That would explain why Cellebrite Physical Analyzer did not process, parse, or display the digital data well, and why there was no table data within the database files opened in D.B. Browser for SQLite tool.

Hickman stated that it appeared the error had to do with the extraction of the TAR file within Windows. Magnet Axiom also had issues processing, parsing, and displaying the image file as well. Hickman stated that a new image file had been made available on his website. The new iOS 13.3.1 image file was processed using the Cellebrite Physical Analyzer and Magnet Axiom with no reported errors. That is a clear demonstration of the importance of verification testing of data evidence.

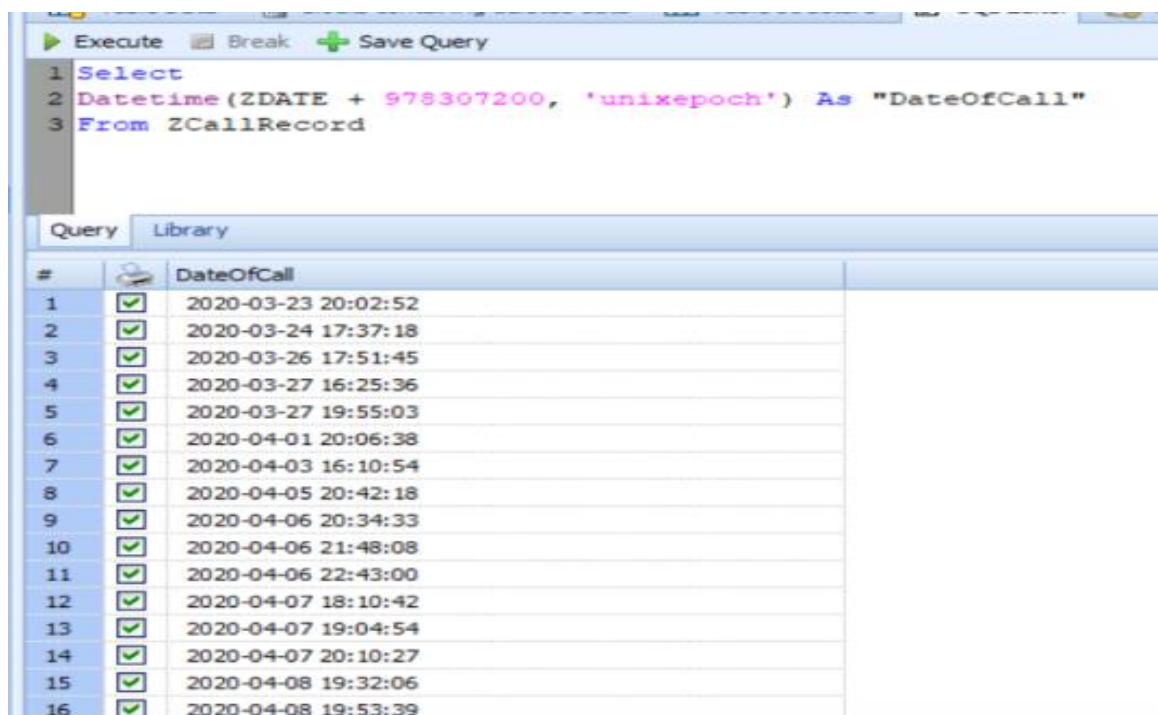
The third-party applications chosen for verification testing between Oxygen Forensic Detective and Cellebrite Physical Analyzer were, Wire, Proton-Mail, and Burner. The system application files data that was compared and verified was

/private/var/installid/Library/MobileInstallation/BackedUpState/System/AppInstallState.plist, and /private/var/mobile/Library/TCC/TCC.db. The chosen 3rd party applications presented data was verified between the two commercial tools. The system application files data was verified with both commercial tools and the use of iLEAPP.

Conclusion

While it is not appropriate or attainable to cross-verify every application on a mobile device, it is important to choose system applications and two or three third-party applications to conduct a verification test. The third-party applications would be those suspected of containing digital evidence of a crime. Choosing system application files is vital as that data should be available and should be verifiable either with another commercial tool, an open-source tool or manually on the device.

When parsing any application (stock or 3rd party) database, remember that timestamps will often need to be converted. Most of the commercial tools offer an SQLite editor within the tool. Cellebrite Physical Analyzer and Magnet Axiom provided suggested conversions in a drop-down menu. Oxygen Forensic Detective tool the timestamps can be converted by writing an SQL query,



```

1 Select
2 Datetime(ZDATE + 978307200, 'unixepoch') As "DateOfCall"
3 From ZCallRecord

```

#	DateOfCall
1	2020-03-23 20:02:52
2	2020-03-24 17:37:18
3	2020-03-26 17:51:45
4	2020-03-27 16:25:36
5	2020-03-27 19:55:03
6	2020-04-01 20:06:38
7	2020-04-03 16:10:54
8	2020-04-05 20:42:18
9	2020-04-06 20:34:33
10	2020-04-06 21:48:08
11	2020-04-06 22:43:00
12	2020-04-07 18:10:42
13	2020-04-07 19:04:54
14	2020-04-07 20:10:27
15	2020-04-08 19:32:06
16	2020-04-08 19:53:39

Figure 11. Call-History.sqlite timestamp conversion query within Oxygen Forensic Detective.

As was demonstrated in the testing of this methodology, it is the examiner's responsibility to attempt to determine the cause of anomalies or errors. It is also their responsibility to notify the tool vendors so they can check out the issue and correct it. Documentation of the application verification testing method and results should be in the examiner's notes. Any anomalies or errors encountered should be documented, as well.

Each of the hypotheses presented was proven correct. First, the commercial tools do process, parse, and display most common third-party applications; second, Cellebrite Physical Analyzer and Magnet Axion had issues processing, parsing, and displaying data from the iOS 13.3.1-Extraction.zip image file. Some third-party application files do require manual verification on the device. In this test, the data was verified using the documentation of the data population provided with the iOS13.3.1-Extraction.zip file. The commercial tool CFTT test reports from NIST are not current.

This methodology can be replicated and reviewed by using the community available dataset created by Josh Hickman. However, the same anomaly issue encountered in this test may not be reproduced as the issue is reportedly fixed.

Recommended future work is for this methodology to be tested by other researchers, checking the results for verification. It is also essential for the newer iOS 13.3.1 image file be tested to make sure the anomaly involving the Windows extraction of the TAR file is fixed. Lastly, there can be more in-depth research into the third-party applications not parsed by the different, popular commercial tools.

References

- Arshad, H., Jantan, A., & Abiodun, O. (2018). Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. *Journal of Information Processing Systems*, 14, 346 ~ 376.
<https://doi.org/10.3745/JIPS.03.0095>
- Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on mobile device forensics* (NIST SP 800-101r1; p. NIST SP 800-101r1). pp 25 National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.SP.800-101r1>
- Beckett, J., & Slay, J. (2011). Scientific underpinnings and background to standards and accreditation in digital forensics. pp. 115 & 118. *Digital Investigation*, 8(2), 114–121.
<https://doi.org/10.1016/j.diin.2011.08.001>
- Brignoni, A. (2019, December 24). Initialization vectors: ILEAPP: iOS Logs, Events, And Properties Parser. *Initialization Vectors*. <https://abrignoni.blogspot.com/2019/12/ileapp-ios-logs-events-and-properties.html>
- Carrier, B. (n.d.). *Autopsy*. Retrieved April 20, 2020, from <https://www.sleuthkit.org/autopsy/>
- Clement, J. (2020, January 15). *App stores: Number of apps in leading app stores 2019*. Statista.
<https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/>
- Edwards, S. (2020, January 14). Mac4n6.com. *Mac4n6.Com*. <http://www.mac4n6.com>
- Edwards, S. (2018, August 6), Knowledge is Power! Using the macOS/iOS knowledgeC.db Database to Determine Precise User and Application Usage. (2018, August 6). *Mac4n6.Com*.
<http://www.mac4n6.com/blog/2018/8/5/knowledge-is-power-using-the-knowledgedcdb-database-on-macos-and-ios-to-determine-precise-user-and-application-usage>

Erbacher, R. (2010). *Validation for Digital Forensics*. 756–761. pp. 757 & 759.

<https://doi.org/10.1109/ITNG.2010.18>

Farrugia, S. (2016). Mobile Cloud Computing Techniques for Extending Computation and Resources in Mobile Devices. *2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 1–10. <https://doi.org/10.1109/MobileCloud.2016.26>

Grajeda, C., Breitingner, F., & Baggili, I. (2017). Availability of datasets for digital forensics – And what is missing. *Digital Investigation*, 22, S94–S105. <https://doi.org/10.1016/j.diin.2017.06.004>

Hick, B. (2020, April 16). IOS 13 Images....ImageS...Now Available! *The Binary Hick*.

<https://thebinaryhick.blog/2020/04/16/ios-13-images-images-now-available/>

Holst, A. (2019, October 17). *Topic: U.S. smartphone market*. Wwww.Statista.Com.

<https://www.statista.com/topics/2711/us-smartphone-market/>

Horsman, G. (2019). Tool testing and reliability issues in the field of digital forensics. *Digital Investigation*, 28, 163–175. <https://doi.org/10.1016/j.diin.2019.01.009>

ANAB Directory of Accredited Organizations—ISO/IEC 17025—L-A-B. (n.d.). Retrieved April 4, 2020, from <http://search.anab.org/>

DFIR Training. (n.d.). Retrieved March 21, 2020, from

<https://www.dfir.training/resources/downloads/ctf-forensic-test-images/more-images>

DFIR Review. (n.d.). DFIR Review. Retrieved April 23, 2020, from <https://dfir.pubpub.org/>

Realm Database. (n.d.). Retrieved April 20, 2020, from <https://realm.io/products/realm-database/>

SWGDE Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis. (2018). 33.

SWGDE Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics. (2018). 20.

