Abstract:

This paper focused on the manual forensics examination of mobile devices that followed the Platform Independent Forensics Process Model for Smartphones (PIFPM). There were eight mobile devices and several mobile device operating systems' (Android, Apple iOS, Blackberry (RIM), and Windows 10) that were on a network and analyzed with Experiment One: MSAB XRY®8.0 and Experiment Two: DiffMerge®4.2. Experiment One involved securing the mobile device file structure at the byte level by examination based on the projected probability of the user from test state one to test state two. Experiment Two determined the path with the nominal possibility of contagion when examining a device manually by test state one versus test state two. The least amount to the most amount of contagions were realized for the manual examination of PIFPM for most of all mobile devices. Further research is evident in order for the manual analysis to be statistically accurate.

*Keywords- Mobile device forensics, Platform Independent Forensic Process Model (PIFPM) for Smartphones*

## Introduction

It is well known in academia that computer forensics students have been taught that one of the most important elements of digital forensic is to have a working copy of the original device. Though this concept flourishes with desktops, laptops, notebooks, and other computing devices, it does not with mobile devices. Any action taken on a smartphone is logged and furthermore, attempting to create a copy would change the state of the device and in essence, making the use of hashes null and void. What is unperceived is how to combat these challenges for mobile devices. Additionally, criminal justice officers and other bureaus centered in petite populations do not have the means to examine automated evidence on a mobile device due to

limited resources. In Mississippi, there are only four examiners who are located in Jackson that specialize in mobile devices (Office of the Attorney General State of Mississippi, 2013). Out of the eighty-two counties in this state, these examiners are the only ones available to conduct mobile device forensics examinations. Agents staffed in the Attorney General's Cyber Crime Division provide critical training in computer forensics to nearly 276 police and sheriff departments across the state. The Cyber Crime Division operates the only statewide digital forensics laboratory, which has been used to obtain, analyze, and report thousands of electronic items related to criminal cases statewide (Office of the Attorney General State of Mississippi, 2013). This is exemplary for computing, but it is a continuous process for mobile devices. Given the number of mobile devices on the network for users in Mississippi versus the number of mobile device forensics examiners in the state, it is crucial to improve the manual examination techniques regardless of make, model, functionality, portability, and ease of use for mobile devices (Dancer and Dampier, 2013; Dancer and Skelton, 2013; Dancer, 2016; Dancer, 2017). Examining mobile devices manually would allow guidance without an automated examination, and moreover, without financial and personnel restrictions by the agencies.

## Methodology

The researcher can predict what happens to mobile devices that have been activated through one carrier to contrast the functionality of each eight devices in the PIFPM, shown in Figure 1, using the Manual Analysis Phase. The approach will be the same as experiment one and experiment two in (Dancer and Dampier, 2013; Dancer and Skelton, 2013; Dancer, 2016; Dancer, 2017), with the addition of activated mobile devices, a mobile tool called MSAB Office: XRY® 8.0 and DiffMerge ® 4.2. This manual path is determined by computing the percentage

of change with respect to file size and the number of files that change between states, thus which category alters memory the most.

The network that the researcher had selected is AT&T®. This carrier is on the Global System for Mobiles communication (GSM), unlike networks that have Code Division Multiple

*The following figure and note are adapted from A Platform Independent Forensic Process Model for Smartphones*. Scholars Press (2013).

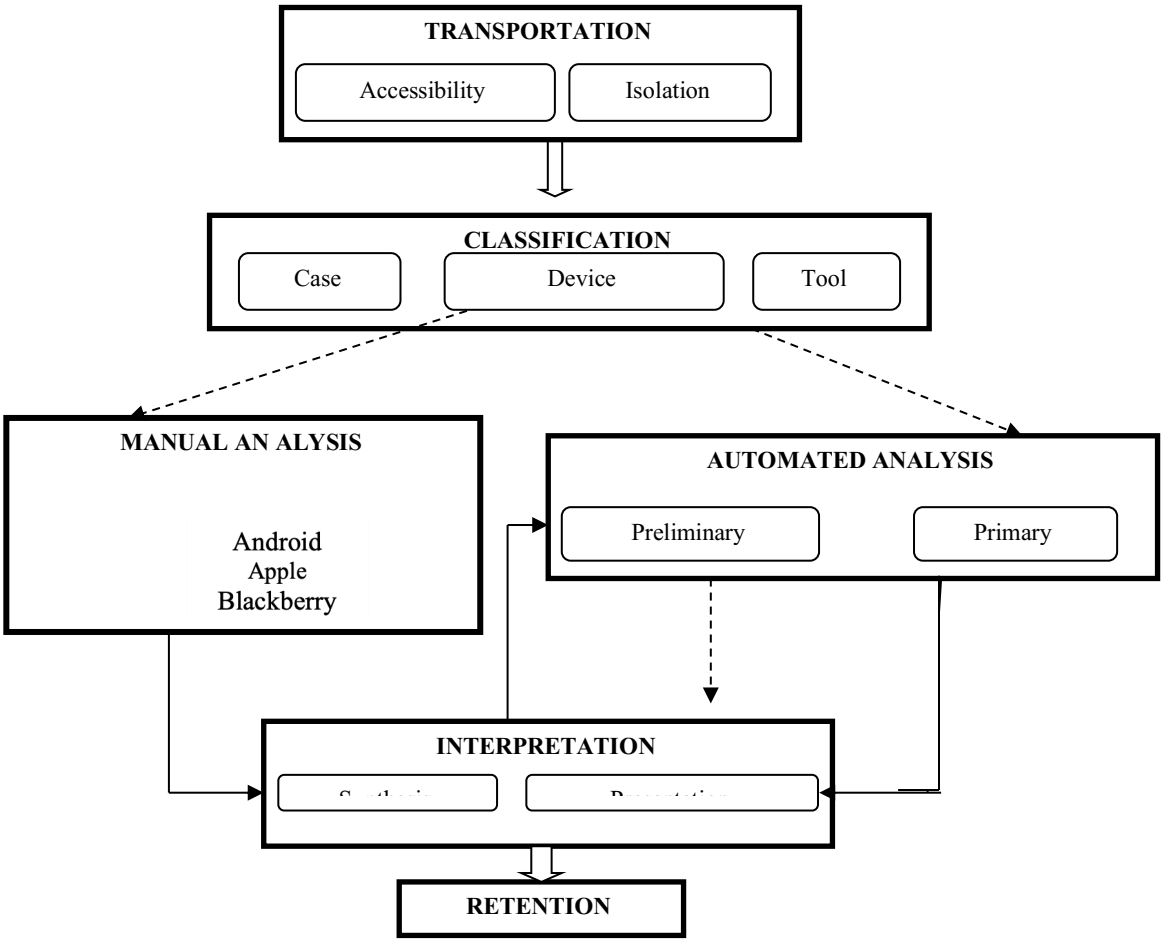


Figure 1: Platform Independent Forensics Process Model

Access (CDMA). CDMA uses a physical channel and a dedicated code for every device, so it is handset specific whereas GSM has network towers in each cell, or large area, to serve a mobile phone in that area, so it is SIM specific (Venkatesan, (2013). The full operation of each mobile device has not been realized for twenty years because mobile devices contain proprietary software. Two experiments were designed to reveal how the kernel arranges file stores, edits, and deletes after a particular process.

**Experiment 1 Design**

Experiment 1 involved securing the files generated by XRY® 8.0 and capturing the size of each at the byte level. The files are compared to others in thirty-four separate tests within that particular smartphone category with respect to the size of the other experiments, but with one difference. There are categories termed Email and Call with one Call Unique ID, V-IDTA, that was absent initially as can be seen in (Dancer and Dampier, 2013; Dancer and Skelton, 2013; Dancer, 2016; Dancer, 2017). This affords us the knowledge of discovering which categories offer the least and most file size change. When dealing with the changes in file size, either the size will increase, decrease, or have no change on a network instead of not on a network, as seen in (Dancer and Dampier, 2013; Dancer and Skelton, 2013).

The researcher had gathered and compared all calls, (received, missed), texts, pictures, SMS, MMS, browser functions plus two novel approaches, email and declined to answer, of seven mobile devices that were on a network. The eight smartphones used in this experiment had varying levels of operation. No devices had to be hard reset as in (Dancer, 2017), and there were no limitations of the experiments in every test as the smartphones were all activated except one, Windows Lumia 650. This device is not jailbroken and not on the AT&T® network.

Apple iPhone X TD-LTE is a part of the Apple iOS operating system for mobile phones

manufactured by Apple Inc., but several items should have been shielded prior to acquiring the XRY system. When the investigator required the smartphone and connected it, the password was not necessary for these experiments, and it was also not encrypted. The user has to trust the computer and allow the device to select USB Debugging. The user created a backup on this mobile device and would be able to fully connect to the device and examine the root directories (Burgess, 2012).

Blackberry KEYone (1) and Blackberry KEYone (2) are Blackberry Mobile's new Android7.1.1 Nougat operating system instead of RIM in 2017. The system of RIM was outdated as far as users are concerned. Manufactured by Telephone Communication Limited (TCL) Corporation, it is mainly Google® software on the device. Unlike the Apple iPhone X, the Blackberry KEYone (1) attained three categories of evidence; Files, Device, and Contacts, Blackberry KEYone (2) attained two categories of evidence; whereas the Apple iPhone X has four categories of evidence; Files, Device, Organizer, and Web.

Samsung Galaxy 10e, Samsung Galaxy S9, and Samsung Galaxy Note 8 are a part of the Android Pie 9 operating system manufactured by Samsung Electronics with its custom user interface pre-installed and Google® software. Unlike the Apple iPhone X or the Blackberry KEYone (1), the Samsung Galaxy Note 8 had two categories of evidence; Files, and Device like Blackberry KEYone (2) and Samsung Galaxy S9. The Samsung Galaxy 10e had four categories of evidence like the Apple iPhone X but with two differences. Whereas Apple iPhone X had the Organizer and Web categories, Samsung Galaxy 10e had the Locations and Messages categories.

Windows Lumia 950 and Windows Lumia 650 are Windows Mobile Devices (WMDs) which manages the Windows 10 operating systems manufactured by Microsoft Mobile. Windows Mobile Device (WMD) has been increasingly rare in the last few years, and due to

this, WMD Lumia software has concluded after this research and will be taken out of the manual analysis of PIFPM (Warren, 2017). Windows Lumia 950 and Windows Lumia 650 had the same number of evidence files as the Samsung Galaxy Note 8 and Blackberry KEYone (2); Files and Device. Maybe because automatic detection is not supported in either case, so as a result, the user only had the file system support on the media partition of the phone.

**Experiment 2 Design**

Experiment 2's goal is to determine the path with the nominal possibility of contagion when examining a device manually. This manual path is determined by computing the percent of change with respect to file size and the number of files that change between states, thus, which category alters memory most significantly. Each category is ranked with respect to the percent difference from least to greatest. In order to compute the difference in the number of files where the content differs, each folder structure representing each test was inputted into the DiffMerge version 4.2.0 software along with its comparison test folder structure. DiffMerge returned the number of identical and different files, the number of files without peers, and the number of folders. The percent difference in the number of files where the content changed was computed by adding the number of different files and files without peers and dividing by the total number of files within the folder structure. This number is then divided by 100 (Dancer, 2017).

## RESULTS

**Experiment 1 Results**

Before experimentation began, the author coded each test using a unique ID and developed projections regarding the outcome of each test shown in Table 1. Of the 34 tests conducted, at least one or more of the devices conform to 19% of the projected results. Because there were eight smartphones this experiment instead of three smartphones using the same

protocol as the last experiment, the numbers are extremely different. 12% of the tests are not predicted due to uncertainty by the author, and therefore, the projected resulted is coded as undecided (U). There are four other codes in the table, I, D, NC, and N/A, which are acronyms for the following: increased in file size, decreased in file size, no change in file size, and not applicable. Some of the entries in the table have a red font. These are the actual results that

Table 1: Experiment 1 - Projected Results vs. Actual Results

| | | Actual Result | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Test ID | Projected Result | Apple iPhone X | Samsung Galaxy10e | Samsung Galaxy S9 Plus | Samsung Galaxy 8 | Blackberry KEYone (1) | Blackberry KEYone (2) | Microsoft Lumina 950 | Microsoft Lumina 650 |
| B-IO | I | I | NC | NC | NC | I | NC | I | NC |
| B-OG | I | I | I | NC | NC | D | NC | NC | NC |
| B-GC | D | I | NC | NC | NC | D | NC | NC | NC |
| B-OC | U | D | NC | NC | NC | I | NC | NC | NC |
| B-GD | D | I | I | NC | NC | NC | NC | NC | NC |
| B-CD | D | D | NC | NC | NC | NC | NC | NC | NC |
| C-IN | I | I | NC | NC | NC | I | NC | NC | NC |
| C-NA | U | I | NC | NC | NC | NC | NC | NC | NC |
| C-AD | D | NC | NC | NC | NC | NC | NC | NC | NC |
| M-IR | I | D | I | I | NC | I | NC | NC | N/A |
| M-IS | I | I | NC | D | NC | NC | NC | NC | N/A |
| M-RO | U | I | NC | I | D | NC | NC | NC | N/A |
| M-RD | D | D | D | I | I | D | NC | NC | N/A |
| M-SD | D | D | I | I | I | NC | NC | NC | N/A |
| P-IN | I | I | D | I | D | I | I | NC | I |
| P-ND | D | D | I | D | D | D | D | NC | D |
| S-IR | I | D | D | I | I | I | NC | NC | N/A |
| S-IS | I | D | D | D | D | NC | NC | NC | N/A |
| S-RO | U | I | I | I | D | NC | NC | NC | N/A |
| S-OD | D | D | NC | NC | I | D | NC | NC | N/A |
| S-SD | D | NC | D | NC | I | NC | NC | NC | N/A |
| V-IP | I | I | I | NC | I | I | D | NC | N/A |
| V-IRA | I | D | I | NC | NC | NC | I | NC | N/A |
| V-IRU | I | I | D | NC | NC | NC | NC | NC | N/A |
| V-IDC | I | D | I | NC | NC | D | NC | NC | N/A |
| V-PDC | I | NC | NC | NC | NC | NC | NC | NC | N/A |
| V- | D | D | D | NC | NC | NC | NC | NC | N/A |
| V- | I | I | NC | NC | D | I | NC | NC | N/A |
| E-IO | I | D | I | D | I | NC | NC | NC | NC |
| E- | I | NC | I | NC | NC | NC | NC | NC | NC |
| E-OS | I | I | NC | NC | NC | NC | NC | NC | NC |
| E-OD | D | I | NC | NC | NC | NC | NC | NC | NC |
| E-OT | D | D | D | NC | NC | NC | NC | NC | NC |
| E-IT | I | I | NC | NC | NC | NC | NC | NC | NC |

*Note: The table is adapted from A Platform Independent Forensic Process Model for Smartphones*. Scholars Press (2013).

contradict the projected results.

The actual results show the relationship between devices based on how similar or dissimilar they perform. Across the battery of tests, the Apple iPhone X performed 62% of the projected results, and Samsung Galaxy 10e performed 41% of the time. Samsung Galaxy S9 Plus performed 21% of the time, as did Samsung Galaxy 8. Like Samsung Galaxy 10e, Blackberry KEYone (1) performed 41% of the time. Blackberry KEYone (2) performed 9% of the time, Microsoft Lumina 950 performed 3% of the time, and Microsoft Lumina performed 6% of the time. One thing is curious. Test C-AD had decreased in file size for the projected result, but all smartphones had no change in file size, even Files.txt, which is a log file. Also, Test V-PDC had increased in file size for the projected result, but all smartphones had no change in file size but one. Because it is the Windows Lumina 650, it could have no change in file size, but it was non-measurable.

**Experiment 2 Results**

The Apple iPhone X is the device where the total number of folders per test fluctuated between 118 and 172. Samsung Galaxy 10e is the device where the total number of folders per test fluctuated between 700 and 711. Because the Apple iPhone X is not jailbroken as was done in the Apple iPhone 3G (Dancer, 2017), XRY would not reveal the 99% of post-jailbroken state; thus, the investigator is left with what is realized. Blackberry KEYone (1) investigation had left the user with a total number of folders fluctuating between 78 and 79. The number of folders throughout all other tests for every other device fluctuates between 6 and 21 folders. Given the limitations of extraction by XRY 8.0, it is not surprising that Windows Lumina 950, Windows Lumina 650, and Blackberry KEYone (2) contained 0 different files for all thirty-four tests as it was different for Blackberry KEYone (1).

Since Windows Lumina 950, Windows Lumina 650, and Blackberry KEYone (1) and (2) are not listed as a supported device, not much data was extracted from the device except Blackberry KEYone (1). Blackberry KEYone (1) contained 78 folders, but the same device and a different model contained 6 folders. The investigator is unsure of why this happened to the same device. Further experiments will be discussed during a later date comparing and contrasting two smartphones of the same make and model.

Due to the amount of data retrieved from the Apple iPhone X, the Samsung Galaxy 10e, and the Blackberry KEYone (1) tests, it is infeasible to discuss each. Therefore, only the most interesting tests will be mentioned in the text but Table 2 is the Categorical Percent Difference of all the smartphones. Apple iPhone X categories coupled with the average amount of change per category from least amount of change to most: Contacts – 56%, Picture – 64%, SMS – 66%, MMS – 67%, Browser – 68%, Email – 69%, and Call – 70%. Samsung Galaxy 10e categories coupled with the average amount of change per category from least amount of change to most: Browser – .04%, Contacts - .08%, Picture – .1%, SMS/MMS/Email/Call – .2%. Blackberry KEYone (1) categories coupled with the average amount of change per category from least amount of change to most: Contacts – 70%, Picture – 71%, SMS – 72.16%, MMS – 72.1%, Browser – 67%, Email – 72%, and Call – 73%.

The Windows Lumina 950 and Windows Lumina 650 report 8 files as identical, 0 files as different, and at the most, 3 files as being without peers. The percentage is the same for the Windows Lumina 950 with smartphone categories of Contacts, Picture, SMS, MMS, Call, Email, and Browser – 0%. Windows Lumina 650 had the same percentage of 0 for the following categories: Browser and Contact. N/A is the answer for SMS, MMS, and Call as there was no

SIM card in this device. The only categories that have responses are Email – 20% and Picture – 24%.

Table 2: Experiment 2-Categorical Percent Difference

| Test ID | Apple iPhone 10 | | Samsung Galaxy10e | | Samsung Galaxy S9 Plus | | Samsung Galaxy 8 | | Blackberry KEYone (1) | | Blackberry KEYone (2) | | Microsoft Lumina 950 | | Microsoft Lumia 650 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | %Δ | Avg | %Δ | Avg. | %Δ | Avg | %Δ | Avg | %Δ | Avg. | %Δ | Avg | %Δ | Avg | %Δ | Avg. |
| B-IO | 67.5 | | 0 | | 0 | | 0 | | 66.67 | | 0 | | 0 | | 0 | |
| B-OG | 67.8 | | 0 | | 0 | | 10 | | 65.52 | | 0 | | 0 | | 0 | |
| B-GC | 68 | .679 | .05 | .0004 | 0 | 0 | 10 | .08 | 68.96 | .67 | 0 | 0 | 0 | 0 | 0 | 0 |
| B-OC | 68 | | .05 | | 0 | | 10 | | 65.52 | | 0 | | 0 | | 0 | |
| B-GD | 68.2 | | .08 | | 0 | | 10 | | 68.96 | | 0 | | 0 | | 0 | |
| B-CD | 68.2 | | .08 | | 0 | | 10 | | 68.96 | | 0 | | 0 | | 0 | |
| C-IN | 55.9 | | .08 | | 0 | | 10 | | 70.79 | | 0 | | 0 | | 0 | |
| C-NA | 56 | .559 | .08 | .0008 | 0 | 0 | 10 | .10 | 70.79 | .70 | 0 | 0 | 0 | 0 | 0 | 0 |
| C-AD | 56 | | .08 | | 0 | | 10 | | 70.79 | | 0 | | 0 | | 0 | |
| M-IR | 67.5 | | 0.2 | | 30 | | 10 | | 72.22 | | 100 | | 0 | | N/A | |
| M-IS | 65.2 | | 0.2 | | 70 | | 10 | | 72.22 | | 0 | | 0 | | N/A | |
| M-RO | 69.2 | .677 | 0.2 | .002 | 50 | .66 | 30 | .28 | 72.22 | .721 | 100 | .4 | 0 | 0 | N/A | N/A |
| M-RD | 69.3 | | 0.2 | | 88.9 | | 80 | | 71.91 | | 0 | | 0 | | N/A | |
| M-SD | 67.5 | | 0.2 | | 88.9 | | 10 | | 71.91 | | 0 | | 0 | | N/A | |
| P-IN | 59.1 | .642 | 0.1 | .0015 | 10 | .05 | 70 | .85 | 70.79 | .71 | 50 | .25 | 0 | 0 | 27.3 | .237 |
| P-ND | 69.4 | | 0.2 | | 0 | | 100 | | 71.91 | | 0 | | 0 | | 20 | |
| S-IR | 66.6 | | 0.2 | | 36.4 | | 30 | | 72.22 | | 0 | | 0 | | N/A | |
| S-IS | 65.2 | | 0.2 | | 30 | | 50 | | 72.22 | | 0 | | 0 | | N/A | |
| S-RO | 66.6 | .663 | 0.2 | .002 | 30 | .31 | 30 | .48 | 72.22 | .7216 | 0 | .4 | 0 | 0 | N/A | N/A |
| S-RD | 66.6 | | 0.2 | | 30 | | 70 | | 72.22 | | 100 | | 0 | | N/A | |
| S-SD | 66.6 | | 0.2 | | 30 | | 60 | | 71.91 | | 100 | | 0 | | N/A | |
| V-IP | 69.6 | | 0.2 | | 30 | | 10 | | 73.03 | | 0 | | 0 | | N/A | |
| V-IRA | 69.8 | | 0.2 | | 30 | | 100 | | 73.03 | | 100 | | 0 | | N/A | |
| V-IRU | 69.6 | | 0.2 | | 30 | | 100 | | 73.03 | | 0 | | 0 | | N/A | |
| V-IDC | 69.5 | | 0.2 | | 30 | | 10 | | 73.03 | | 0 | | 0 | | N/A | |
| V-PDC | 69.5 | .696 | 0.2 | .002 | 30 | .3 | 100 | .61 | 73.03 | .73 | 100 | .286 | 0 | 0 | N/A | N/A |
| V-RUD | 69.8 | | 0.2 | | 30 | | 10 | | 73.03 | | 0 | | 0 | | N/A | |
| V-IDTA | 69.9 | | 0.2 | | 30 | | 100 | | 73.03 | | 0 | | 0 | | N/A | |
| E-IO | 68.7 | | 0.2 | | 0 | | 0 | | 72.22 | | 0 | | 0 | | 20 | |
| E- | 68.7 | | 0.2 | | 0 | | 10 | | 72.22 | | 0 | | 0 | | 20 | |
| E-OS | 68.7 | | 0.2 | | 0 | | 0 | | 72.22 | | 0 | | 0 | | 20 | |
| E-OD | 68.7 | .687 | 0.2 | .002 | 0 | 0 | 0 | .01 | 72.22 | .72 | 0 | 0 | 0 | 0 | 20 | .2 |
| E-OT | 68.7 | | 0.2 | | 0 | | 0 | | 72.22 | | 0 | | 0 | | 20 | |
| E-IT | 68.7 | | 0.2 | | 0 | | 0 | | 72.22 | | 0 | | 0 | | 20 | |

*Note: Δ is percent difference. The table is adapted from A Platform Independent Forensic Process Model for Smartphones*. Scholars Press (2013).

Samsung Galaxy S9 Plus and Blackberry KEYone (2) are deemed enthralling because they had the same categories with a 0 percentage; Browser, Contacts, and Email. The investigator is perplexed about this situation, but Calls, SMS/MMS, and Picture Categories are different. In the Samsung Galaxy S9 Plus, the categories are as follows: Picture – 5%, Call – 30%, SMS – 31%, and MMS – 66%. In the Blackberry KEYone (2), the categories are as follows: SM/ MMS – 4%, Picture – 25%, and Call – 28.6%.

Samsung Galaxy Note 8 is significant as well. Of all thirty-four tests, the Picture and Calls Categories piqued curiosity. Everywhere there is a 0 in identical files, there is also a 0 in different files. It ranges from 10 – 20 files with no peers, so the categorical difference is more for the Call and the Picture Categories than any of the other categories. In the Samsung Galaxy Note 8, the categories are as follows: Email – 1%, Browser – 8%, Contacts – 10%, MMS – 28%, SMS – 48%, Call – 61% and Picture – 85%.

## DISCUSSION

Files are the principal fragment of the structure of a smartphone. Of the eight smartphones being examined, only two, maybe three, of the devices were worthy of being forensically examined based of file structure. RIM, which are Android based systems as of this year, WMD, which are Windows based systems, and selected Android systems lack some file systems due to automatic detection. Thus, pictures, text messages, contacts, and call logs cannot be achieved using the XRY tool. iOS systems have an enhanced result based on file structure, thus, the XRY tool extracts data based on the number of files it receives from the device using DiffMerge.

The PIFPM extendable framework will provide examiners with a process model for the purpose of inspecting any model smartphone conscious of the unique qualities belonging to each.

After reviewing the models already established, it was discovered that no such model existed. After its development, the researcher conducted several quantitative studies in an effort to reveal any new information about the different smartphones. The researcher modified the design of PIFPM to include a path for manual examination based on the information discerned in the File Size Difference and the Average Change in Content experiments.

An order of examination can be deduced based on eight smartphones. Windows Lumina 950 has the same amount of categorical change, and therefore, this experiment does not assist in devising an order of examination for this device. Windows Lumina 650 and Windows Lumina 950 shall be opted out after these experiments due to limited popularity. However, this order can be realized for the remaining devices in the next two years. The researcher plans to conduct future studies that will result in statistical significance.

## Acknowledgments

F. Chevonne Dancer thanks the National Science Foundation (NSF) for sponsoring this research, Grant# 182709 Historically Black Colleges and Universities Undergraduate Program (HBCU-UP).

# References

Allen, S., Graupera, V., & Lundrigan, L. (2010). *Pro smartphone cross-platform development: iPhone, blackberry, windows mobile and android development and distribution*. Apress.

Burgess, J. (2012). The iPhone moment, the Apple brand, and the creative consumer: From "hackability and usability" to cultural generativity. In *Studying mobile media* (pp. 36-50). Routledge.

Dancer, F. C. T. (2016, December). Analyzing and Comparing Android HTC Aria, Apple iPhone 3G, and Windows Mobile HTC TouchPro 6850. In *2016 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 1037-1042). IEEE.

Dancer, F. C. T. (2017). Manual Analysis Phase for (PIFPM): Platform Independent Forensics Process Model for Smartphones. *International Journal of Cyber-Security and Digital Forensics*, *6*(3), 101-109.

Dancer, F. C., & Dampier, D. A. (2013). *A Platform Independent Forensic Process Model for Smartphones*. Scholars Press.

Dancer, F. C. T., & Skelton, G. W. (2013, November). To change or not to change: That is the question. In *2013 IEEE International Conference on Technologies for Homeland Security (HST)* (pp. 212-216). IEEE.

Office of the Attorney General State of Mississippi. (2013). Cyber Crime Unit, Retrieved from http://www.ago.state.ms.us/divisions/cyber-crime/.

Stellmach, R. N. (1995). *U.S. Patent No. 5,423,083*. Washington, DC: U.S. Patent and Trademark Office.

Warren, T. (2017). “Microsoft finally admits Windows Phone is Dead” Retrived from https://www.theverge.com/2017/10/9/16446280/microsoft-finally-admits-windows-phone-is-dead.

Venkatesan, K. G. S. (2013). Comparison of CDMA & GSM Mobile Technology. *Middle-East Journal of Scientific Research*, *13*(12), 1590-1594.