Qualitative Analysis for Platform Independent Forensics Process Model (PIFPM) for Smartphones

F. Chevonne Thomas Dancer(✉)

Department of Electrical Engineering, Computer Engineering, and Computer Science, Jackson State University, Jackson, MS 39217, USA
frances.c.dancer@jsums.edu

Abstract. This paper details how forensic examiners determine the mobile device process and if the Platform Independent Forensics Process Model for Smartphones (PIFPM) helps them in achieving the goal of examining a smartphone. The researcher conducted interviews, presented the PIFPM process to the examiners, and supplied surveys that the examiners were exposed to. Using convenience sampling, the frequency and percent distribution of each examiner is given as well as strengths and weaknesses of PIFPM as it relates to the examiner. Based on the hypotheses given by the researcher, the results were either refuted or supported through sampling from the forensic examiners. The goal of this paper is to uncover interesting details that the researcher overlooked when examining a smartphone.

Keywords: Platform Independent Forensics Process Model (PIFPM) Digital forensics · Interviews · Mobile device forensics

1 Introduction

The Platform Independent Process Model (PIFPM) for Smartphones introduces a novel approach of examining mobile device forensics. The author presents a way of examining smartphones regardless of make, model, or device as seen in Fig. 1. The PIFPM is explained in more detail in [1].

Smartphone devices were used to analyze data in the Primary Stage of the Analysis Phase that averages the percent of change by category in Experiment 1. The first experiment involves securing the files generated by XRY 6.1 and capturing the size of each at the byte level. The files were compared to files in 40 separate tests within their particular smartphone category concerning the size, carrier, OS, and device. Doing so enabled the author to compute the differences in size by test as well as by category. This affords us the knowledge of discovering which categories offer the least and most file in size change. When dealing with the changes in file size, the results can take one of three options: Either the size will increase, decrease, or have no change. Given these options, the researcher was able to provide projections of how each XRY file would be affected by each test [2–4]. To assist with folders that change in content, the researcher has designed a lookup tables with unique IDs that tells the status from test state 1 to test

K. Arai et al. (Eds.): FICC 2018, AISC 887, pp. 74–89, 2019.
https://doi.org/10.1007/978-3-030-03405-4_6

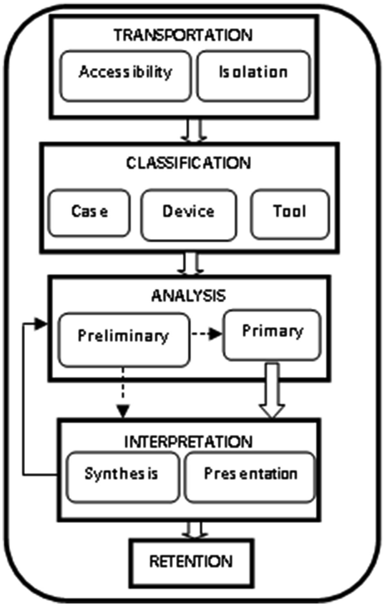

Fig. 1. Platform independent process model for smartphones (PIFPM).

state 2 in Table 1 [2–4]. For example, B-OC is the unique ID for the Browser Category. The researcher opens a browser window on HTC Pro 6850 and saves the folder size of the smartphone, and closes the browser window and saves the folder size of the smartphone. Table 2 shows an example file size change of six devices in Experiment 1.

In the second experiment, the XRY files from the first experiment were exported to the hard drive as a hierarchical folder containing all the files and folders extracted from each device. The number of files within the folder structure that differed from one state to the next was compared by inputting the two folders into SourceForge DiffMerge version 3.3.2 software DiffMerge returned the number of identical, "Iden," and different files, "Diff," the number of files without peers, "W/P," and the number of folders, "# Folds". The percent difference, "% Δ," 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. "Num of Diff" is the number of differences from test state 1 to state 2 and "Cat%Δ" is the number that is categorically different [2–4]. An example of the Apple iPhone 3G A1241 is below in Table 3 [2]. From these experiments, each test within each category was ranked from least to the greatest amount of change with respect to the percentage of change reported. It compared the files with their smartphone category concerning the size, carrier, and platform. Those same smartphones were used to generate the average change in file content by device while applying XRYv6.1 and DiffMerge 3.3.2 in Experiment 2. The manual analyses of smartphones were obtained by comparing Experiment 1 with Experiment 2 [1–6].

Table 1. Unique ID lookup table

	Unique ID	Test state 1 to Test state 2
Browser	B-IO	Initial to Open Browser Window
	B-OG	Open Browser Window to Google Search
	B-GC	Google Search to Close Browser Window
	B-OC	Open Browser Window to Close Browser Window
	B-GD	Google Search to Delete History and Bookmarks
	B-CD	Close Browser Window to Delete History
Contact	C-IN	Initial to New Contact
	C-NA	New Contact to Altered Contact
	C-AD	Altered Contact to Deleted Contact
MMS	M-IR	Initial to Received MMS message
	M-IS	Initial to Sent MMS message
	M-RO	Received MMS message to Opened MMS message
	M-RD	Received MMS message to Deleted MMS message
	M-SD	Sent MMS message to Deleted MMS message
Pic	P-IN	Initial to New Picture
	P-ND	New Picture to Deleted Picture
SMS	S-IR	Initial to Received SMS message
	S-IS	Initial to Sent SMS message
	S-RO	Received SMS message to Opened SMS message
	S-OD	Received SMS message to Deleted SMS message
	S-SD	Sent SMS message to Deleted SMS message
Call	V-IP	Initial to Placed Call
	V-IRA	Initial to Received Answered Call
	V-IRU	Initial to Received Unanswered Call
	V-IDC	Initial to Deleted Call log
	V-PDC	Placed Call to Deleted Call log
	V-RUDM	Received Unanswered Call to Deleted Missed Call
Miscellaneous	A-ISA	Initial to Stop All Apps (TouchPro 6850 only)
	J-IJB	Initial to Jailbreak (iPhone only)
	J-JBDM	Jailbreak to Delete SMS (iPhone only)
	L-IL	Initial to Passcode Enabled (iPhone only)
	L-LnS	Passcode Enabled to no SIM (iPhone only)
	Vmail-IR	Initial to Received Voicemail (iPhone only)
	Vmail-RL	Received Voicemail to Listened to Voicemail (iPhone only)
	Vmail-LD	Listened to Voicemail to Deleted Voicemail (iPhone only)

This research involves collecting data from two case studies to determine the feasibility and usefulness of PIFPM. After the data is gathered in the qualitative design, the hypotheses (1–5) are either negated or supported depending on the answers from the forensics examiners. Those answers are shown in the Frequency/Percent Distribution by Group in Tables 4, 5, 6, 7, 8, 9, 10 and 11.

Table 2. Projected results vs. actual results

Test ID	Projected result	Apple iPhone 3G	HTC Touch Pro 6850	HTC Aria	RIM BB 8530	RIM BB8703	Nokia 5230
B-IO	I	D	I	NC	I	N/A	N/A
B-OG	I	D	I	I	NC	N/A	N/A
B-GC	D	I	I	D	NC	N/A	N/A
B-OC	U	I	I	NC	NC	N/A	N/A
B-GD	D	I	I	D	NC	N/A	N/A
B-CD	D	I	D	D	NC	N/A	N/A
C-IN	I	I	D	I	I	I	I
C-NA	U	I	NC	D	I	I	D
C-AD	D	I	D	D	D	D	I
M-IR	I	I	NA	NA	N/A	N/A	N/A
M-IS	I	D	I	NA	I	N/A	D
M-RO	U	I	NA	NA	N/A	N/A	N/A
M-RD	D	I	NA	NA	N/A	N/A	N/A
M-SD	D	I	NA	NA	D	N/A	N/A
P-IN	I	I	I	NA	NC	N/A	I
P-ND	D	I	I	NA	NC	N/A	D
S-IR	I	I	NA	NA	D	NC	N/A
S-IS	I	I	I	I	I	I	D
S-RO	U	I	NA	NA	NC	NC	N/A
S-OD	D	I	NA	NA	NC	NC	N/A
S-SD	D	I	I	D	D	D	N/A
V-IP	I	I	I	I	I	I	N/A
V-IRA	I	D	NA	NA	N/A	N/A	N/A
V-IRU	I	I	NA	NA	N/A	N/A	N/A
V-IDC	D	I	D	NC	D	D	N/A
V-PDC	D	I	D	D	D	D	N/A
V-RUDM	D	I	NA	NA	N/A	N/A	N/A
A-ISA	D	NA	I	NA	N/A	N/A	N/A
J-IJB	I	I	NA	NA	N/A	NC	N/A
J-JBDM	D	D	NA	NA	N/A	NC	N/A
L-IL	U	D	NA	NA	NC	N/A	N/A
E-IE	I	N/A	N/A	N/A	N/A	NC	N/A
E-ELAN	U	N/A	N/A	N/A	N/A	NC	N/A
N-IDN	D	N/A	N/A	N/A	NC	N/A	N/A
W-ILAN	I	N/A	N/A	N/A	I	NC	N/A

Table 3. Apple Iphone: % change in folder content by device and category

Test ID	Iden	Num of Diff		# Folds	% Δ	Cat.% Δ
		Diff	W/P			
J-IJB	1	9	71023	4430	99.999%	62.7%
J-JBDM	54784	6410	14645	4355	27.763%	
M-IS	55041	16484	19345	4743	39.429%	34.0%
M-SR	64563	7626	17901	4833	28.335%	
M-RO	64394	8101	17354	4800	28.331%	
M-OD	54869	16644	19404	4774	39.649%	
S-IS	66276	7096	15628	4731	25.533%	25.3%
S-SR	65933	7407	15714	4728	25.963%	
S-RO	66815	6679	15464	4769	24.892%	
S-OD	66750	6802	15431	4743	24.986%	
Vmail-IR	55774	7520	14409	2590	28.222%	27.9%
Vmail-RL	56215	7557	13601	2550	27.345%	
Vmail-LD	55599	8125	13581	2611	28.078%	
V-RUDM	55796	7770	13636	2648	27.727%	28.2%
V-DMR	55745	7630	14054	2648	28.005%	
V-IP	56133	7553	13620	2587	27.389%	
V-PDC	56496	7168	13596	2637	26.875%	
P-IN	56298	7332	13772	2644	27.265%	27.3%
P-ND	56257	7539	13609	2614	27.321%	
B-DBO	39193	23142	16021	2686	49.981%	46.6%
B-OG	37100	24862	17000	2656	53.015%	
B-GC	53427	9142	16024	2577	32.021%	
B-CD	38285	24222	16124	2679	51.311%	
C-IN	38529	24032	16044	2679	50.984%	61.1%
C-NA	53619	9008	15976	2679	31.785%	
C-AD	1	61678	18030	2680	99.999%	
L-IL	1	61942	17607	2637	99.999%	75.0%
L-LnS	39531	23567	15284	2637	49.566%	

Table 4. Question 2 frequency/percent distribution by group

Q2. How difficult is PIFPM to understand?		
Option	SE	ME
a. Not difficult	1/100%	1/50%
b. Slightly difficult	0/0%	0/0%
c. Somewhat difficult	0/0%	1/50%
d. Very difficult	0/0%	0/0%
e. Extremely difficult	0/0%	0/0%

Table 5. Question 3 frequency/percent distribution by group

Q3. Rate how feasible PIFPM would be in its application to the forensic processing of smartphones?		
Option	SE	ME
a. Not at all feasible	0/0%	0/0%
b. Slightly feasible	0/0%	0/0%
c. Somewhat feasible	0/0%	1/50%
d. Very feasible	0/0%	0/0%
e. Extremely feasible	1/100%	1/50%

Table 6. Question 4 frequency/percent distribution by group

Q4. How likely would you be to incorporate PIFPM into your forensic examination process?		
Option	SE	ME
a. Not likely	0/0%	0/0%
b. Slightly likely	0/0%	0/0%
c. Somewhat likely	0/0%	1/50%
d. Very likely	0/0%	1/50%
e. Extremely likely	1/100%	0/0%

Table 7. Question 5 frequency/percent distribution by group

Q5. Of the phases listed below, which one(s) do not fit the logical progression of a forensic examination?		
Option	SE	ME
a. Transportation	0/0%	0/0%
b. Classification	0/0%	0/0%
c. Analysis	0/0%	0/0%
d. Interpretation	0/0%	0/0%
e. All seem logical	1/100%	2/100%

Table 8. Question 6 frequency/percent distribution by group

Q6. How useful is PIFPM in a smartphone examination?		
Option	SE	ME
a. Not useful at all	0/0%	0/0%
b. Slightly useful	0/0%	0/0%
c. Somewhat useful	0/0%	1/50%
d. Very useful	0/0%	1/50%
e. Extremely useful	1/100%	0/0%

Table 9. Question 8 frequency/percent distribution by group

Q8. Is it logical for smartphones to use the same forensic process model as computers?		
Option	SE	ME
a. Not logical	0/0%	0/0%
b. Slightly logical	0/0%	0/0%
c. Somewhat logical	1/100%	1/50%
d. Very logical	0/0%	1/50%
e. Extremely logical	0/0%	0/0%

Table 10. Question 9 frequency/percent distribution by group

Q9. How often do you manipulate the process you frequently use to examine smartphones, whether intentionally or unintentionally?		
Option	SE	ME
a. Not often	0/0%	1/50%
b. Slightly often	0/0%	1/50%
c. Somewhat often	1/100%	0/0%
d. Very often	0/0%	0/0%
e. Extremely often	0/0%	0/0%

Table 11. Question 14 frequency/percent distribution by group

Q14. Do you believe that incorporating PIFPM into phone examinations will change the confidence level of the investigator?		
Option	SE	ME
a. Yes, it will lower the confidence level greatly	0/0%	0/0%
b. Yes, it will lower the confidence level slightly	0/0%	0/0%
c. No, the confidence level will not change	0/0%	0/0%
d. Yes, it will elevate the confidence level slightly	0/0%	2/100%
e. Yes, it will elevate the confidence level greatly	1/100%	0/0%

2 Qualitative Design Study

The observable population consists of three professional forensic examiners with varying years of experience exploring many different devices including smartphones. Eight forensic examiners were sought after for this study, and four agreed to have interviews. Only three forensic examiners were dialogued because one examiner was in court at that time. The researcher traveled to each participant in his/her perspective locations. The participants were interviewed concerning their current process when examining mobile devices as well as the usage of any equipment. Then, the participants examined the proposed model while a presentation was given about PIFPM. After the presentation was completed, the participants were allowed to ask any questions they had about the model. A follow-up survey was given that captured qualitative data regarding usefulness and feasibility of PIFPM.

Each participant was interviewed separately to maintain an unbiased environment. Each person was asked the same four questions in an attempt for uniformity, but each examiner was also asked one or more follow-up questions. The answers to the interview questions allowed the researcher to discover a theme that could be verified through interviews with a larger population set.

Examiners ME-A and ME-B, from the same organization, almost follow the same process from beginning to end. They also used the same tool, almost never deviating. On the other hand, Examiner SE-A uses a more ad-hoc process where he adapts to his environment depending on the type of OS being dealt with. ME-A and SE-A were both asked the same follow-up question after the researcher inquired about their specific process which was, “What happens if [your process] does not work?” ME-A said that they return the phone to its owner without trying any other tool other than Cellebrite. When asked about XRY in particular, he said that anything XRY could read, Cellebrite could read and if Cellebrite cannot read the device, XRY cannot read the device either. On the other hand, SE-A said that they go on to the other tools in their arsenal to see if any of those can extract the data. If none of the other tools comply, the examiner returns the phone to the user. He also added that if the client still wants the information to be extracted without the use of tools, they usually return the phone to them and instruct them to look for the information manually.

While mapping the interviewees with their particular responses, it was discovered that each examiner had once before manually examined a device. In every case, with each examiner, the process used in these instances was the same. They take photographs of every action taken by the examiner on the device. SE-A was then asked another follow-up question concerning whether or not he has ever examined a device manually for a reason other than to be used in a court of law. His answer was, “Sure.”

The next question was purely a question that stemmed from curiosity. The researcher asked them whether or not they ever examined two phones of the same make/model and compared them to see what effect their actions had on the OS. The answers from each examiner were that they had not done so either because they had not had the opportunity or that they never had a reason to.

Next, the examiners were asked whether or not there was a particular model smartphone that they feel more confident in examining over others. SE-A and ME-A both said no, but ME-B said that he likes examining anything but a Samsung Galaxy or an iPhone. When inquiring why, the examiner mentioned that no tool in his organization could break into the phone if it were passcode protected. The only thing they would be able to do is extract the SIM card and get whatever information is available there or ask a federal agency for the tool that can break into the phones.

3 Qualitative Analysis Results

All participants were males with two having 3 to 4 years of experience and the other having 2 to 3 years. Given this information, the researcher created two categories about experience since some of the research questions deal with that in particular. The categories are More Experience (ME) and Some Experience (SE). Using this information, eight frequency/percent tables were created outlining each question that deals with the hypotheses as well as a Rankings and Medians Table. To follow is a discussion of the responses to the questions found on the post-survey. The hypotheses are:

(1) How useful is PIFPM in a smartphone examination?
(2) Is it feasible to include PIFPM in the current process for examining smartphones?
(3) Does PIFPM offer anything to a smartphone investigation that other models do not?
(4) Is it logical to suggest that every category of a technological device should assume a unique forensic process model?
(5) Do examiners, whether intentional manually manipulate current process models to suit specific model smartphones?

In this study, the sampling method used was convenience sampling. In using this method, there is a possibility of bias, but this method was selected due to ease of collection and the nature of the careers of the participants. This resulted in a sample size insufficient to support this work with great confidence. In determining the confidence interval of the survey data given here, it can be stated with 95% confidence that if the same population is sampled on numerous occasions and interval estimates are made on each occasion, the resulting intervals would bracket the true population in approximately 56.58% of the cases [7]. Tables 4, 5, 6, 7, 8, 9, 10 and 11 are reported based on this data.

Given this, the margin of error is well beyond what is acceptable by the researchers. To alleviate this, the study will have to be repeated to obtain a sample size of at least 24. Then the researcher will be able to state that the margin of error is 20% and that the answers will represent those reported 95% of the time. To absolve all doubt, as part of future work, the researchers plan to survey a total of 384 forensic examiners to obtain a confidence interval of 5% [7].

As far as results, some questions are discussed at length, and some are not. Question 1 asked the forensic examiners about the years of experience they acquired; question 7 is a discussion question and will be discussed later in this paper; question 10 states, “Have you ever manually examined a device with no external equipment” and the answer to all was yes; question 11 was a follow-up question if they answered yes in question 10, and questions 12 & 13 are discussion questions and will be discussed later.

Question 2 asked the participants how difficult PIFPM was to understand. The response frequency and percents are broken down by groups and mapped to each response given on the survey as seen in Table 4. The SE Group and 50% of the ME Group feel that PIFPM is not at all difficult to understand and the other half of the ME Group feel that it was somewhat difficult to understand.

Question 3 asked the participants to rate how feasible PIFPM would be in its application to the forensic processing of smartphones. Table 5 show that the SE group and 50% of the ME Group feel that it is extremely feasible. The remaining 50% of the ME Group feel that PIFPM is somewhat feasible.

Question 4 asked each participant how likely he would be to incorporate PIFPM into his forensic examination process and Table 6 shows the frequency and percentage of the responses from each group. The SE Group reported that it would be extremely likely to incorporate PIFPM into their forensic process. The ME Group is split. Half of the group reported that they would very likely to incorporate the model whereas the other half reported that it would be somewhat likely to use PIFPM in their examination process.

Question 5 asked the examiners which phases do not fit the logical progression of a forensic examination out of the following: Transportation, Classification, Analysis, and Interpretation. If they felt that all of the phases are logical, they had the opportunity to circle that choice as well. 100% of both groups feel that all of these phases seem logical as shown in Table 7.

Question 6, as seen in Table 8, asked each participant how useful PIFPM would be in a smartphone examination. The SE Group feels that PIFPM would be extremely useful. The ME Group is split. 50% of the group feels that PIFPM would be very useful, whereas the other half thinks that the model would be somewhat useful.

Table 9 shows the frequency and percent of the responses given for Question 8. This question asked the participants whether it is logical for smartphones to use the same forensic process model as computers. The SE Group and half of the ME Group feel that it is somewhat logical to use the same forensic process model as computers. The remainder of the group thinks that it is very logical.

Question 9 asked each participant how often he manipulates the process when he examines a smartphone. Table 10 shows that the SE Group changes the process somewhat often. Half of the ME Group reported that its process does not often change when examining smartphones and the remainder of the group reported that change occurs slightly often.

Table 11 reports the frequency and percent of the responses for Question 14 on the survey. Each examiner was asked whether he believes that incorporating PIFPM into smartphone examinations would change the confidence level of the investigator. The SE Group feels that using PIFPM would elevate the confidence level of the investigator greatly and the ME Group feels that using the model would elevate the confidence level of the investigator slightly.

The survey also contained two questions that asked each examiner to list any strength and weaknesses they could discern from evaluating the model during the presentation. Table 12 reports the number of weaknesses and strengths outlined by the examiners. The SE Group reported one weakness and one strength. The ME Group reported one weakness and three strengths.

Table 12. Number of reported PIFPM weaknesses vs. strengths group distribution frequency

	SE	ME
Strengths	1	3
Weaknesses	1	1

The first discussion question asked the examiners what strengths PIFPM offers to the examination of a smartphone. One examiner reported that it offers good guidelines on the next step to take in most situations. Another examiner reported that it gives them an orderly process to follow and it also ensures the same process is followed each time. The last examiner reported that the model offers them diversity.

The second discussion question asked the examiners what weaknesses PIFPM offers to a forensic examiner in a smartphone investigation. One examiner reported that it would need to adapt as [smartphone] OS's change. Another examiner reported that given the amount and frequency of updates on phones, inconsistency would be an issue. The last examiner had no weaknesses to report.

Table 13 shows the three discussion questions asked to the examiners as shown on the survey; two discussions questions were already discussed above. The final discussion question asked each participant whether PIFPM offered anything to an examination that other models do not. One examiner had no response because he said that he could not answer it. Another examiner reported that he had no model for comparison, and the last examiner reported, "Not that I am aware of."

Table 13. Post survey discussion questions

Q7	Does PIFPM offer anything to an examination that other models do not?
Q12	What strengths does PIFPM offer to a forensic examiner in a smartphone investigation?
Q13	What weaknesses does PIFPM offer to a forensic examiner in a smartphone investigation?

Table 14 contains the responses for each question that relates to our hypotheses and ranks the answers from 1 to 5 using a mapping created from the available responses labeled a to e in Tables 4, 5, 6, 7, 8, 9, 10 and 11. The median values are the values used to either support or refute our hypotheses. Table 15 shows a mapping of the research questions to the premises and the survey questions.

Table 14. Post survey response rankings and medians

	Q2	Q3	Q4	Q5	Q6	Q8	Q9	Q14
A	3	5	4	5	3	4	1	4
B	1	3	3	5	4	3	2	4
C	1	5	5	5	5	3	3	5
Median	1	5	4	5	4	3	2	4

Table 15. Research questions, hypotheses, and survey questions mapping

Research questions	Hypothesis	Y or N	Post survey Q
R1. How useful is PIFPM in a smartphone examination?	H1a. Examiners with less experience will find PIFPM to be at least somewhat useful	Y	Q6
	H1b. Examiners with more experience will find PIFPM to be at least slightly useful	N	
	H1c. Examiners with less experience will be more likely to incorporate PIFPM into their forensic examination process than examiners with more experience	Y	Q4
	H1d. Examiners with more experience will be less likely to incorporate PIFPM into their forensic examination process than examiners with less experience	Y	
R2. Is it feasible to include PIFPM in the current process for examining smartphones?	H2a. Most examiners will find PIFPM to be at least somewhat feasible	Y	Q3
	H2b. Most examiners will find that all the proposed phases fit the logical progression of a smartphone forensic examination	Y	Q5
	H2c. Examiners, regardless of experience, will find that PIFPM is not difficult	Y	Q2
R3. Does PIFPM offer anything to a smartphone investigation that other models do not?	H3a. Examiners with less experience will find that PIFPM has more strengths than weaknesses	N/A	Q12, Q13, Q7
	H3b. Examiners with more experience will find that PIFPM has more weaknesses than strengths	N/A	
R4. Is it logical to suggest that every category of a technological device should assume a unique forensic process model?	H4. Examiners, regardless of experience, will not find that it is very logical to use the same process model to examine smartphones and computers	Y	Q8
R5. Do examiners, whether intentional or not, manually manipulate current process models to suit specific model smartphones?	H5a. Examiners with less experience do not manipulate current process models often	N	Q9
	H5b. Examiners with more experience do manipulate current process models often	N	

To support or refute Research Questions 1 to 5, the researcher has to refer back to the frequency and percent tables. Research Question 1 (R1) maps to Hypothesis 1a (H1a), Hypothesis 1b (H1b), Hypothesis 1c (H1c), and Hypothesis 1d (H1d). H1a states that "Examiners with less experience will find PIFPM to be at least somewhat useful." Table 8 shows that the SE Group reported finding PIFPM very useful. Since the SE Group is the group with less experience than the ME Group, H1a is supported by the qualitative data. H1b states that "Examiners with more experience will find PIFPM to be at least slightly useful." Table 14 shows that the median response maps between "Somewhat useful" and "Very useful." The researcher believed that a more experienced examiner might not be as open to change as a less experienced examiner, but this was not the case in this instance. As a result, H1b is not supported by the qualitative data. H1c states that "Examiners with less experience will be more likely to incorporate PIFPM into their forensic examination process." H1d states that "Examiners with more experience will be less likely to incorporate PIFPM into their forensic examination process." Table 4 shows that the SE Group reported finding that it is extremely likely that they would incorporate PIFPM into their examination whereas the ME Group reported that their likelihood of incorporating PIFPM into their examination would be the median of "Very likely" and "Somewhat likely." Given our mapping scale, the data shows that the group with the least amount of experience would be more likely to incorporate the model into the daily examination than the group with the most experience. As a result, both H1c and H1d are supported by the qualitative data. Given that three of the four hypotheses derived from Research Question 1 is supported by the qualitative data, that Table 14 reports the median response of the usefulness of PIFPM as being "very useful", and the likelihood of the examiner incorporating the model into the daily routine as being "very likely", it is reasonable to believe that PIFPM would be at least somewhat useful in a smartphone examination.

Research Question 2 (R2) maps to Hypothesis 2a (H2a), Hypothesis 2b (H2b), and Hypothesis 2c (H2c). H2a states that "Most examiners will find PIFPM to be at least somewhat feasible." Table 14 shows that the median answer for survey Q3 is "Extremely feasible." As a result, the qualitative data is shown to support H2a. H2b states that "Most examiners will find that all the proposed phases fit the logical progression of a smartphone forensic examination." Table 14 shows that the median answer for survey Q5 is "All seem logical." As a result, the qualitative data is shown to support H2b. H2c states that "Examiners regardless of experience will find that PIFPM is not difficult." Table 14 shows that the median answer for Q2 is "Not difficult." As a result, the qualitative data is shown to support H2c. Given that all the hypotheses derived for Research Question 2 are supported by the qualitative data, it is reasonable to believe that it is feasible to include PIFPM in the current process to examine smartphones.

Research Question 3 (R3) was answered by using the frequencies reported in Table 12. R3 maps to Hypothesis 3a (H3a) and Hypothesis 3b (H3b). H3a states that "Examiners with less experience will find that PIFPM has more strengths than weaknesses." H3b states that "Examiners with more experience will find that PIFPM has more weaknesses than strengths." Table 12 shows that the SE Group reported the same amount of weaknesses and strengths, and the ME Group reported more strengths than weaknesses. Given this, the qualitative data refutes both H3a and H3b.

This question was also asked the participants verbatim in Question 7 on the survey. As mentioned previously, the participants had no answer for this question for various reasons. Therefore, the researcher is not able to answer R3 which asks whether PIFPM offers anything to a smartphone investigation that other models do not based on the qualitative data in this study.

Research Question 4 (R4) maps to Hypothesis 4 (H4). H4 states that "Examiners, regardless of experience, will not find that it is very logical to use the same process model to examine smartphones and computers." Table 14 shows that the median answer for survey Q8 is "Somewhat logical." As a result, the qualitative data is shown to support H4. Given that the hypothesis derived for Research Question 4 is supported by the qualitative data, it is reasonable to suggest that every category of a technological device should assume a unique forensic process model.

Research Question 5 (R5) maps to Hypothesis 5a (H5a) and Hypothesis 5b (H5b). H5a states that "Examiners with less experience do not manipulate current process models often" and H5b states that "Examiners with more experience do manipulate current process models often." Table 10 shows that the SE Group reported that it manipulates its process somewhat often whereas the ME Group reported that its frequency of manipulation would be the median of "Not often" and "Slightly often." As a result, both H5a and H5b are not supported by the qualitative data. In deriving these hypotheses, the researcher believed that the less experienced examiner would be less likely to change their routine and skew from the norm. It was also the belief of the researcher that the more experienced examiner would be more likely to change their process mainly due to lessons learned. Even though the hypotheses are not supported by the data, Table 14 shows that the median response for all participants is that they manipulate their process slightly often, which answers R5.

Although the results given in the surveys are not statistically significant, there were several lessons that can be taken away from the qualitative portion of the study based on whether or not they would actually apply PIFPM, instances in which they would or would not use the model, what they would change about PIFPM, and their overall opinion of the model.

The author asked the participants, after they experienced the model and its uses, if and how they would incorporate PIFPM into their examinations and the response was unanimously positive. No participant reported that they would decline to incorporate it into their work. For example, Participant A reported that he would be very open to incorporating it into his normal process because the model is not difficult to understand and it seems logical. He would first test the model out by using it after using his normal process to compare procedures several times. If he felt comfortable with the process and results, he would then begin to incorporate it into his normal processes. Alternatively, Participant B also feels that the model is not difficult to understand, and he would feel more comfortable incorporating PIFPM if a workshop was conducted that will assist in directing examiners on how to approach each phase and sub-phase in the model.

When asked of any instance they could think of that they would not feel comfortable incorporating PIFPM, Participant C stated that because he does not feel comfortable examining Android and Apple mobile devices, he would more than likely not use the model on these devices. Participant B felt that he may not feel comfortable testifying in a court of law based on this model without some experience.

The participants were asked what aspects of PIFPM they would change given the fact that they are practicing examiners, Participant A would change the order of manual examination. Given that the browser of most smartphones reloads all the windows last used, he would change this category to the last category viewed on an Android device. After further thought, he also decided that this should probably be the case for every OS smartphone. Participant C also mentioned that the browser information for the Android and Apple mobile devices should be listed last. Other than that, he said that he would not change anything from this initial introduction. Participant B felt that he could not decide what he would change in theory, but after he has been able to apply the practices of the model, he could give a more accurate response to this question.

The researcher inquired how the participants felt about the model overall. Participant A felt that the model was "cool" and that it would be great because there would be something out there to follow. Participant B did not have any negative feedback of the model itself. He questioned the use of the word 'forensics' when referring to the examination of a smartphone since smartphone examinations always change the state of the device and forensic examinations are not supposed to make changes. This is true in general, but there is no method in general that is guaranteed to preserve the state of a smartphone or any cell phone during an examination. This is accepted practice and can be explained in court. Participant C felt that the model seemed to be an overall logical one and that he would have more of an opinion after being able to apply the model.

4 Conclusions and Future Work

The difficulty for the examiner lies in the lack of a methodology for smartphones. Neither ad-hoc methods nor methods for computer examination are well suited for the examination of a smartphone due to their distinct issues [8–10]. These methods do not take into consideration the uniqueness of smartphones and therefore could lead to a loss or non-discovery of any information with evidentiary value. In this study, forensic examiners had the PIFPM presented to them, and they answered questions based on feasibility. These questions were given based on a survey to answer the hypotheses. Frequency/Percent Distributions, Tables 4, 5, 6, 7, 8, 9, 10 and 11, were split into groups based on experience. Based on the survey response medians, the researcher could tell whether the hypotheses were negated, supported, or not applicable.

For future work, the researcher will be able to state with a confidence interval of 5% of 384 forensic examiners state that PIFPM is secure to examine the devices in mobile device forensics. Also, the researcher will continue the PIFPM for smartphones using ad-hoc and non-ad-hoc methods to further support or negate the hypotheses with confidence. With enough participants, the researcher can state whether PIFPM is easy but reliable when it comes to examining smartphones regardless of make, model, or OS.

Acknowledgments. I would like to thank Dr. David A. Dampier, Professor and Interim Chair of Information Systems and Cyber Security at the University of Texas at San Antonio, Texas, the forensic examiners at the National Center for Forensics at Mississippi State University, Mississippi and the forensic examiners at the Attorney General's Office in Jackson, Mississippi.

References

1. Chevonne Thomas Dancer, F., Dampier, D.A., Jackson, J.M., Meghanathan, N.V.: A theoretical process model for smartphones. In: Proceedings of 2012 Second International Conference on Artificial Intelligence, Soft Computing and Applications, Chennai, India, 13–15 July 2012
2. Chevonne Thomas Dancer, F.: Analyzing and comparing android HTC Aria, Apple iPhone 3G, and Windows Mobile HTC TouchPro 6850. In: The 2016 IEEE International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, USA, 15–17 December 2016
3. Chevonne Thomas Dancer, F.: Manual analysis phase for (PIFPM): Platform Independent Forensics Process Model for smartphones. Int. J. Cyber Secur. Digit. Forensics **6**(3), 101–108 (2017)
4. Dancer, F.C.T., Skelton, G.W.: To change or not to change: that is the question. In: 2013 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, pp. 212–216 (2013)
5. Chevonne Thomas Dancer, F., Dampier, D.A.: Refining the digital device hierarchy. J. Acad. Sci. **55**(4), 8 (2010)
6. Chevonne Thomas Dancer, F., Dampier, D.A.: A platform independent process model for smartphones based on invariants. In: SADFE 2010: IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, pp. 56–60. https://doi.org/10.1109/SADFE.2010.15
7. Graziano, A.: Research Methods: A Process of Inquiry. Pearson, London (1993)
8. Patil, D.N., Meshram, B.B.: Digital forensic analysis of ubuntu file system. Int. J. Cyber Secur. Digit. Forensics **4**(5), 175–186 (2016)
9. Jansen, W., Delaitre, A., Moenner, L.: Overcoming impediments to cell phone forensics (2008)
10. Punja, S.G., Mislan, R.P.: Mobile device analysis. Small Scale Digit. Forensics J. **2**(1), 1–16 (2008)