Quest Journals
Journal of Software Engineering and Simulation
Volume 7 ~ Issue 7 (2021) pp: 20-29
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Adoption of Digital Forensic Tools Based On Perceived Usefulness (PU) To Mitigate the Risks in Criminal Investigation

Engr. Tahir Bashir
Al-Madinah International University, Kuala Lumpur, Malaysia
Supervisor: Assoc. Prof. Dr. Najeeb Abbas Al-Sammarraie, PhD

ABSTRACT : *Digital forensics has gained much attention, with the advancements in the technology, to maintain and assess the legal and regulatory requirements. At the same time, Government and Private regulators unable to formulate a procedure for adoption of most suitable digital forensic tools as per operational requirements. Moreover, hundreds of expensive digital forensic tools have arrived in the markets which generates the challenges for regulators upon their selection. The objectives of this research are, to identify the most suitable digital forensic investigation tool using perceived usefulness (PU), identification of correlation between considered features (independent variables) and suitable tool adoption (dependent variable) and study the procedure and technique for adopting the most appropriate digital forensic tool. Both elements (PU, PEOU) of Technology Acceptance Model (TAM) have used to gather the validate information from the digital forensic experts while performing quantitative survey. The research design of this thesis is correlational in nature with positivist research approach and quantitative research technique is adopted. Digital Forensic investigators and experts are considered in population selection along with purpose (EXP > 6 years) based sampling. Google forms and IBM-SPSS software are used to perform quantitative survey and statistical calculations respectively. Descriptive statistical calculations are used to achieve the first objective, i.e. most suitable digital forensic tool, Pearson correlation analysis are performed to achieve the second objective, i.e. correlation between variables and third objective achieved via formulating the complete procedure in the research.*

KEYWORDS: *Digital Forensics, Mobile Forensics, Cellebrite, XRY, OXYGEN Forensic.*

Received 10 July, 2021; Revised: 24 July, 2021; Accepted 26 July, 2021

I. INTRODUCTION

Digital forensics can be defined as a "process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable" (McKemmish et al, 2015). A more detailed definition of digital forensics is stated by (US-CERT, 2020) suggesting that "The discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law". There are other definitions exists though most of these are built within the same concept where extraction of the data is performed on various devices for the purpose of analysis and identification of a specific criminal act that can be considered valid as a legal evidence in the judiciary system. Most of the digital forensic investigation take place after the identification of a criminal or illegal incident that needs assistance as a proof to be justified in the legal system which may include damage to someone's property, theft of patents, inventions and trade secret, illegal financial crimes like money laundering and credit card theft or misuse (Al-Murjan & Xynos, 2016). Moreover, the investigations are also conducted in the case of blackmailing, child pornography and human trafficking. At corporate level, digital forensic investigations are also conducted to enhance the security of system and avoid the entry of the external hackers into the systems.

The main aim of digital forensics is to extract the needful information from specific devices, networks and cloud storage to answer the 5Ws (Why, When, Where, What, and Who) (Sachdev & Wimmer, 2018). By answering these questions, the goal of data extraction can be clearly established, and further strategies can be formulated to establish proper forensic processes within a controlled environment. The process helps the teams of digital forensics to create synergy as well as reduces the risks and challenges that may arise. In an environment, where each digital forensic scientist follows his own technical abilities and uses wide varieties of

*Corresponding Author: Abdalftah Elbori
MODES Department Atilim University Turkey

tools can cause a disruption in generating the evidence for investigation purpose that may not be needful for law enforcement agents. The investigators.

The current research particularly focuses on the mobile devices which are wide in varieties, however, broadly can be categorized on the operating systems basis: iOS based, and Android based. Such platforms within have extensively detailed information and technicalities that make them profoundly different base on version of software, model of the device, application used and adoption of an authentically passcode by the user.

II. SELECTION OF A SUITABLE SOFTWARE FOR DIGITAL FORENSIC INVESTIGATION

There is various software obtainable for digital forensic investigations with a petite or wide variable difference. Most of the disparity among software are related to functional capacity to perform precise tasks as well as the complexity of the system. A software that delivers comprehensive understanding of the dissimilar functionalities as well as easier to operate is typically considered to be well fit for the investigators. However, the acceptance of perceived usefulness and perceived easiness of use on personal basis is not a valid choice) (Sachdev & Wimmer, 2018). This is due to the reasons that personal experiences and choices will create differentiations among team members and also validity of the results can be compromised. The complexities within a software can be design related where interface provides limited user experience. Another problem that may arise while selecting a particular software from management perspective is costing of the software. Since the tools are highly sophisticated, the pricing is spiked as well (Swain, 2020). There is some free software available, however, in proper organizations which are involved in judiciary investigations, adoption of such software is not recommended for the dearth of legal acceptance. Three criteria for selecting a specific software are recommended:

- **Proper acquisition and preservation of evidence**

Considering the fact that electronic information is very sensitive in nature, it can easily be altered or erased from the system if not handled well with proper techniques and tools. For instance, booting a computer with MS Windows tends to alter specific information in the subject tool like important date stamps, replacement of temporary data as well as unessential write up on the disk for the system requirements (Quick, 2016). Therefore, it is important that adoption of tool should be carefully selected to avoid any problems in the preservation of the data on the subject system, mobile or device under investigation.

- **Authentication of collected data**

Another important element of consideration while selecting the tool is the authentication of the data it provides. By authentication of the data means that the retrieved evidence has to be valid and accepted in the legal system based on the legitimacy of the tool used for investigation purpose (Quick, 2016). In many cases, legal system can verify the provided data for the purpose of verifying if the digital forensic investigation is processed through a meaningful and correct manner without tampering or changing the evidence. Therefore, selecting the authentic and valid tools is extremely important along with other variables of selection.

- **Recovery of all available data**

Another important element of consideration is the capacity of the tool to perform various recovery tasks. Recovery of the files can be extensively different, which merely means deleted files from a system's hard disk or specifically from software being used like WhatsApp, social media applications or other third-party suppliers. In most of the cases, third party supplied software are encrypted like in the case of WhatsApp and difficult to be decrypted if the software is not technically sound to do so (Quick, 2016). There are various instances where deleted files are completely overwritten, and such data becomes more sensitive to be erased without proper handling of the sophisticated software.

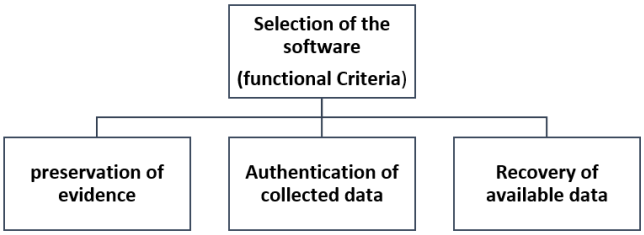

Figure 1: Attributes of Tool selection for Digital Forensic Investigation

III. AIM OF THE PAPER

This paper helps to achieve the following two aims;

a. The aim of the current project is to suggests tools and techniques to be adopted for the identified needful technicalities for digital forensic process among private and public organizations.
b. The alignment of the tasks and identification of specific tools will help to create SOPs and regulations within the corporation and reduce the risk of data loss or disruption of the digital forensic investigation.

IV. HYPOTHESIS OF THE STUDY

H01: Recovery of WhatsApp messages is significantly related to the adoption of a specific tool for digital forensic investigation in the organization.
H02: Digital Call Logs is significantly related to the adoption of a specific tool for digital forensic investigation in the organization.
H03: Phone profile support is significantly related to the adoption of a specific tool for digital forensic investigation in the organization.
H04: Decryption support is significantly related to the adoption of a specific tool for digital forensic investigation in the organization.
The mentioned hypothesis is presented in the below Conceptual framework;

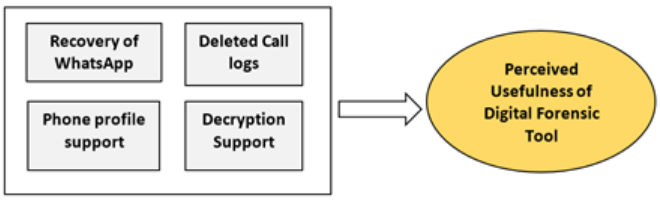

Figure 2: Conceptual Framework

V. IMPORTANCE OF THE RESEARCH

The process of digital forensic is highly sensitive and involves various technicalities that needs understanding of different tools and techniques along with the proper implementation of a framework to meet the needs of legal procedures. Deficiencies in understanding of the available tools, adequate knowledge and lack of implementation skills can hamper the process and meet the required legal standards. One of the core problems that occur while conducting the digital investigation is the lack of understanding of the proper tools for investigation as well unalignment among teams to reach to a specific goal (Ahmad et al., 2009). Unavailability of regulatory framework and standard operating procedures in the corporate organization can limit extraction of the data in a complete manner and lead to poor proof. Further, proper assessment of the capacity of different tools and techniques is vital for digital forensic process as incorrect selection of a tool may erase the needful data and extraction process can be impossible.

Top-notch corporate agencies related to digital forensics create specific protocols and standard operating procedures demonstrate clear processes, selection of tools and techniques and implementation progression by identifying clear goals and aims of the data extraction. These best practices create checklists for proper planning and execution of the tasks in a clear fashion. Unfortunately, the digital forensics investigation is not fully equipped in the developing nations. The investigators use their own intuition, experience and skills to solve a particular problem and extract the data for criminal investigational purposes. Such approach poses a huge risk as the information extracted may not be fully attained and cause disruption in the process of criminal investigation. Therefore, there is a need to identify the need for specific tools and techniques for specific purpose by identification of the problems digital forensic scientists face to enhance the overall process.
Thus, the current research is highly important for the digital forensic companies as well as future research in the area of digital forensics.

VI. RESEARCH DESIGN

The research design for the current research is correlational in nature that intends to determine the cause and effect of specific attributes of the model (Bell et al, 2016). The correlational study intends to identify the relationship of different independent variables in the current case (Recovery of WhatsApp messages, Digital Call Logs, Phone profile support, Decryption support) to the dependent variable (adoption of digital forensic tool). The study is objective in nature and based on the idea that reality of an issue can be understood realistic manner.

In the present research design, the relationship between identified variables is correlational in nature. In this situation, the correlation design seeks to show the association of the identified variables mentioned earlier.

The design is objective in nature based on the philosophical idea that reality can be understood through measurable data. Another approach of research is qualitative in nature where interviews are conducted to determine the impact and explore the phenomenon of the results. However, the qualitative research is not used in the current research because the aim is to test the hypothesis in accordance with the technology acceptance model.

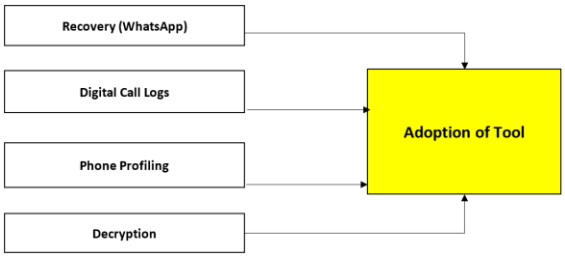

Figure 3: Forensic software adoption framework

VII. RESEARCH APPROACH

Creswell (2003) Determines four decision making model which are important to be considered while approaching a particular research design in any study. This conceptualization is based on the framework of Crotty's (1998) four research design elements that determines a particular opposed to be adopted be it quantitative, qualitative or mixed. further the approach is adopted based on the idea and primarily dependent on the philosophy stance of the researcher and the way he looked into the knowledge precisely. such ideological stances can be objectivism or subjectivism. Objectivism is more concerned with the reality to be considered as it is and not to be looked through critical analysis rather more analytical approach is adopted the concept is also called as positivist approach where the researcher intends to take up the data through analytical findings and therefore quantitative research is more appropriate in this regard (Punch, 2005). On the other hand, subjectivism is a philosophical stance where critically analysis is adopted and focus is to understand the reality through different perspective. in this regard a qualitative analysis through interviews or case studies are adopted. such kind of methodology's are inclined towards exploratory analysis where the knowledge is created two appropriate techniques. considering the fact that the current research is positivist approach based on the ideology of the researcher a quantitative research is adopted and particularly the hypothesis related to the adoption of the particular software within the field of digital forensics, the approach seems to be fit well in the context of the objective of the research. the quantitative research will help to identify the problems in a cause and effect as well as relationship manner through the statistical tests which will be adopted and discussed further in the analysis of the research. quantitative research is beneficial in many ways (Creswell, 2003). the data can be gathered through an easy approach of questionnaire survey where lot of participants can be included in the research. the data is prepared in the form of structured questionnaire and only intended answers are asked based on the specification of the study.

VIII. RESEARCH INSTRUMENT

Survey is the research tool used in this study. Survey method is a commonly used approach in correlation research where data are gathered and various questions examined according to the research objective are posed.

Scale	Range	Interpretation	Descriptions
5	4.21-5.00	Strongly agree	The respondents are highly inclined towards the question
4	3.41-4.20	Agree	The respondents are Somewhat inclined towards the question
3	2.61-3.40	Moderately agree	The respondents are neutral towards the question
2	1.81-260	Disagree	The respondents are Somewhat inclined towards the question
1	1.00-1.80	Strongly disagree	The respondents are Not at all inclined towards the question

Figure 3: Measurement of Likert Type Scale

IX. RESEARCH TOOLS

- **Reliability**

For reliability of the research Cronbach Alpha test was used, which refers to the degree to which the results obtained by a measurement and procedure can be replicated (Bell & Bryan, 2016). The test will measure the

internal consistency (homogeneity) of the questions and determine if they are reliable to be used in the current study. The Cronbach's alpha coefficient was evaluated using the guidelines suggested by George and Mallery (2016) where > .9 excellent, > .8 good, > .7 acceptable, > .6 questionable, > .5 poor, and ≤ .5 unacceptable.

Scale	No. of Items	α	Lower Bound	Upper Bound
WhatsApp Recovery	13	0.82	0.76	0.88
Call Records	12	0.79	0.72	0.86
Phone profile	12	0.84	0.79	0.89
decryption	12	0.95	0.93	0.97
software adoption	5	0.68	0.55	0.8

Figure 4: Suggestion guidelines of variables

- **Validity**

Face Validity was performed from the professional in the field of forensic science. In psychometrics, validity refers to the extent to which a measure represents all facets of a given construct. The current research performed "face validity" to demonstrate the validity of the questionnaire which is an extent to which a test is subjectively viewed as covering the concepts it expects to measure. The face validity has been done by a research expert or organization who can show that the topics used are relevant in order to achieve the aim of current research.

- **Software use**

Two main tools were used to perform the research:

a. Google Forms: google forms is used to create the survey.
b. IMB SPSS Software: the software is used to conduct the statistical tests

- **Data Collection and Analysis**

The researcher sent the survey through email to his colleagues at workplace and other companies along within hand filled surveys. The total number of returned surveys were 65 in number that is an appropriate target population for the research. The analysis of the current research will be performed through SPSS analysis where two kinds of data will be gathered. Descriptive and Inferential.

a. Descriptive statistics will be conducted based on demographic questions where Age, experience, gender and years of experience of the respondents will be presented through frequency distribution, percentile as well as mean median and mode.
b. Inferential statistics will be used to conduct perform the statistical tests for testing the hypothesis test. For this reason, regression analysis and Pearson correlation will be used that would demonstrate the relation of each independent variable with adoption of usefulness of the technology (Render & Stair, 2016).

Objective	Methodology	Technique	Sampling	Analysis
1. Identification of need of different features	Correlational research	Survey method – each feature testing through Likert type Scale	Digital forensic scientist in private companies	Regression analysis Pearson Correlation Testing
2. Identification of tools	Descriptive research	Survey method – ranking of software based on each software	Digital forensic scientist in private companies	Mean, Median, Frequency, percentile

Figure 5: Summary of Research methodology

X. OPERATIONAL FRAMEWORK

- **List of variables**

In order to predict the required digital forensic software, it is mandatory to list the requirement of features that must be or nearly present in the digital forensics' software. So, the enlisted features can be considered as independent variables as well. Furthermore, Adoption of digital forensic tool can be considered as dependent variable which would be predicted using independent variables. Following are the list the independent and depend variables.

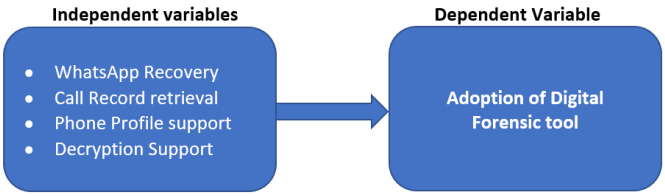

Figure 6: List of variables

Mentioned variables has opted based on practical experience in the relevant field. These independent variables play a vital role in the digital forensic processes which includes extraction, preservation & analysis of data. These independent variables help to adopt the nearly relevant digital forensic tool using TAM model.

- **Diagram of connections**

It is important to show the visual representation of how the independent and dependent variables are connected together, within the framework because flowchart and diagrams are the best possible ways to illustrate these connections. Theses connections and variables are well defined in the literature review as well.

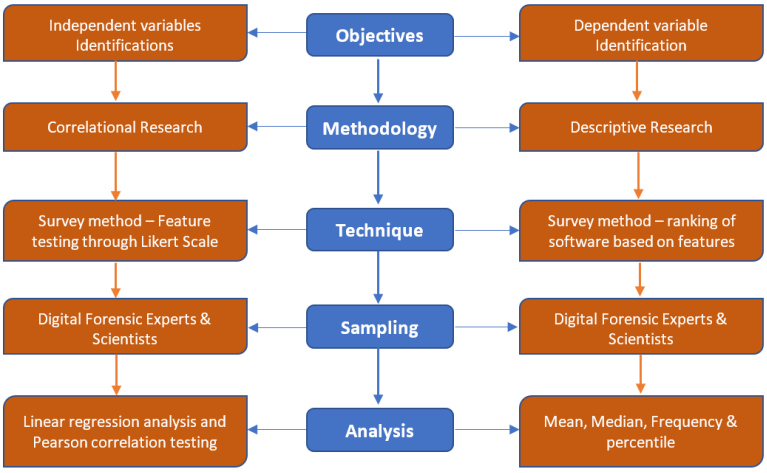

Figure 7: Diagram of connections

- **Connection details**

With the reference to operational framework, Research objectives has been identified on the initial stage which includes the identifications of built-in features (independent variables) in digital forensic tools to adopt the required digital forensic tool (dependent variable) from the list of available tools in the market.

In the methodology, it is necessary to find the correlation between the built-in features of digital forensic tool and adoption or selection of digital forensic tool (dependent variable). In order to find the relationship between independent and dependent variable, Pearson correlation research analysis will perform to find the statistical results. Moreover, Pearson correlation research analysis will also help to find the importance of each independent variable to adopt the digital forensic software. So, Pearson correlation will perform in between each independent variable and dependent variable.

Survey is used as a technique to collect or gather data from the digital forensic experts or digital forensic investigators. Furthermore, importance of surveyor's experience will also be calculated by ANOVA method which helps to analyze the variance to determine whether there were significant differences between software adoption and Total years of experience in digital forensic field of expert or investigator. Quantitative survey is used to analyze the features of digital forensic tool with the help of Likert scale. Descriptive research will perform to find the best available digital forensic tool in the market. Moreover, Descriptive statistics of software and descriptive statistics of variables will also help to find the impact of independent variable in selection procedure of dependent variable.

In last stage, analysis will be performed on the gathered data using linear regression analysis and Pearson correlation methods. This stage will help us to move forward toward conclusion.

XI. DATA ANALYSIS

- **Demographic Data Analysis**

Frequencies and percentages were calculated for Nationality, Age, Total years of experience in Digital Forensics, Highest Level of study, and Gender.

Variable	*n*	*%*
Nationality		
Asian	35	53.03
GCC Countries	10	15.15
American	10	15.15
European	10	15.15
Missing	1	1.52
Age		
36 - 40	40	60.61
26-30	20	30.30
Above 40	5	7.58
Missing	1	1.52
Total years of experience in Digital Forensics		
6 - 1-0 years	20	30.30
2- 5 years	35	53.03
10+	10	15.15
Missing	1	1.52
Highest Level of study		
Bachelor	55	83.33
Masters	10	15.15
Missing	1	1.52
Gender		
Male	50	75.76
Female	15	22.73
Missing	1	1.52

- **Descriptive Statistics of Software usage**

Frequencies and percentages were calculated to Select the Software which use for Data recovery in mobile forensics. The most frequently observed category of Select the Software you use for Data recovery in mobile forensics was Cellebrite Forensics Tools (n = 26, 39%). Frequencies and percentages are presented in table;

Variable	*n*	*%*
Select the Software you use for Data recovery in mobile forensics		
Cellebrite Forensics Tools	26	39.39
Oxygen Forensics Tools	10	15.15
MSAB XRY Forensics Tools	10	15.15
FTK Forensics	10	15.15

Belkasoft Forensics	5	7.58
Belkasoft Evidence	5	7.58
Missing	0	0.00

- **Linear Regression Analysis**

A linear regression analysis was conducted to assess whether Call Records, Phone Profile, Decryption, and WhatsApp Recovery significantly predicted Software Adoption.

The results of the linear regression model were significant, F (4,60) = 18.93, p < .001, R2 = 0.56, indicating that approximately 56% of the variance in Software Adoption is explainable by Call Records, Phone Profile, Decryption, and WhatsApp Recovery. Call Records did not significantly predict Software Adoption, B = 0.22, t (60) = 1.65, p = .105. Based on this sample, a one-unit increase in Call Records does not have a significant effect on Software Adoption. Phone Profile significantly predicted Software Adoption, B = 0.55, t (60) = 4.37, p < .001. This indicates that on average, a one-unit increase of Phone Profile will increase the value of Software Adoption by 0.55 units. Decryption significantly predicted Software Adoption, B = 0.20, t (60) = 3.30, p = .002. This indicates that on average, a one-unit increase of Decryption will increase the value of Software Adoption by 0.20 units. WhatsApp Recovery did not significantly predict Software Adoption, B = 0.08, t (60) = 0.35, p = .726. Based on this sample, a one-unit increase in WhatsApp Recovery does not have a significant effect on Software Adoption. Table 10 summarizes the results of the regression model.

Variable	*B*	*SE*	95% CI	β	*t*	*p*
(Intercept)	0.39	0.51	[-0.63, 1.41]	0.00	0.76	.451
Call Records	0.22	0.13	[-0.05, 0.49]	0.22	1.65	.105
Phone Profile	0.55	0.13	[0.30, 0.80]	0.50	4.37	< .001
Decryption	0.20	0.06	[0.08, 0.32]	0.32	3.30	.002
WhatsApp Recovery	0.08	0.21	[-0.35, 0.50]	0.05	0.35	.726

Figure 7: Results for Linear Regression with Independent predicting Software adoption

- **Pearson Correlation Analysis**

A Pearson correlation analysis was conducted between WhatsApp Recovery and Software Adoption. Cohen's standard was used to evaluate the strength of the relationship, where coefficients between .10 and .29 represent a small effect size, coefficients between .30 and .49 represent a moderate effect size, and coefficients above .50 indicate a large effect size (Cohen, 1988).

Correlations

Correlations

		Whatsapp_Recovery	Call_Records	Phone_Profile	Decryption	Software_Adoption
Whatsapp_Recovery	Pearson Correlation	1	.687**	.420**	.359**	.526**
	Sig. (2-tailed)		.000	.000	.003	.000
	N	65	65	65	65	65
Call_Records	Pearson Correlation	.687**	1	.613**	.127	.603**
	Sig. (2-tailed)	.000		.000	.313	.000
	N	65	65	65	65	65
Phone_Profile	Pearson Correlation	.420**	.613**	1	-.155	.607**
	Sig. (2-tailed)	.000	.000		.219	.000
	N	65	65	65	65	65
Decryption	Pearson Correlation	.359**	.127	-.155	1	.292*
	Sig. (2-tailed)	.003	.313	.219		.018
	N	65	65	65	65	65
Software_Adoption	Pearson Correlation	.526**	.603**	.607**	.292*	1
	Sig. (2-tailed)	.000	.000	.000	.018	
	N	65	65	65	65	65

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Figure 8: Pearson correlation analysis

XII. CONCLUSION

The result of the correlation was examined based on an alpha value of 0.05. A significant positive correlation was observed between WhatsApp Recovery and Software Adoption (rp = 0.53, p < .001, 95% CI [0.32, 0.68]). The correlation coefficient between WhatsApp Recovery and Software Adoption was 0.53, indicating a large effect size. This correlation indicates that as WhatsApp Recovery increases, Software Adoption tends to increase. Table 11 presents the results of the correlation. The findings of the results in agreement to Yoo, (2019) suggesting that Technologies like cloud data storage has caused much wider problem in adoption of toolkits along with the adoption of applications which are totally encrypted like WhatsApp. There are wide legal challenges in accessing information present on such information due to privacy laws and therefore limit the automation of forensic automation. Since WhatsApp continuously upgrade the application to fix the bugs or adding advancements through new features, investigation is widely dependent on the tool selected which must be compatible with the used version of the application.

The result of the correlation was examined based on an alpha value of 0.05. A significant positive correlation was observed between Call Records and Software Adoption (rp = 0.60, p < .001, 95% CI [0.42, 0.74]). The correlation coefficient between Call Records and Software Adoption was 0.60, indicating a large effect size. This correlation indicates that as Call Records increases, Software Adoption tends to increase.

The result of the correlation was examined based on an alpha value of 0.05. A significant positive correlation was observed between Phone Profile and Software Adoption (rp = 0.61, p < .001, 95% CI [0.43, 0.74]). The correlation coefficient between Phone Profile and Software Adoption was 0.61, indicating a large effect size. This correlation indicates that as Phone Profile increases, Software Adoption tends to increase. Studies like Osho et al (2016) demonstrated that selection of the specific tool is widely dependent on the model, type, version and software of the application which may include the use of specific phone profiles. The authors claim that it is almost infeasible to use one tool to perform all the functionalities of retrieving data in a comprehensive manner across all smart full devices.

The result of the correlation was examined based on an alpha value of 0.05. A significant positive correlation was observed between Decryption and Software Adoption (rp = 0.29, p = .018, 95% CI [0.05, 0.50]). The correlation coefficient between Decryption and Software Adoption was 0.29, indicating a small effect size. This correlation indicates that as Decryption increases, Software Adoption tends to increase. Table 14 presents the results of the correlation.

The ANOVA was examined based on an alpha value of 0.05. The results of the ANOVA were not significant, F (2, 62) = 0.50, p = .609, indicating the differences in Software Adoption among the levels of Total years of experience in Digital Forensics were all similar (Table 15). The main effect, Total years of experience in Digital Forensics was not significant, F (2, 62) = 0.50, p = .609, indicating there were no significant differences of Software Adoption by Total years of experience in Digital Forensics levels.

Overall the study provided insights about the various functionalities. One of the major issues with most of the software is that they do not provide a full-functional method where complete automation can be achieved. This is due to the reason that changes in the technologies in the mobile industry are much faster that the upgradation of the toolkits and processing.

REFERENCES

[1]. Ayers R. P., "Smart Phone Tool Specification | NIST.", (2018, Apr), Internet: https://www.nist.gov/publications/smart-phone-tool-specification, [March 18, 2020].

[2]. Bell, E., Bryman, A., & Harley, B. (2018). Business research methods. Oxford university press.

[3]. de Braekt, R. I., Le-Khac, N. A., Farina, J., Scanlon, M., & Kechadi, T. (2016, April). Increasing digital investigator availability through efficient workflow management and automation. In 2016 4th International Symposium on Digital Forensic and Security (ISDFS) (pp. 68-73). IEEE

[4]. Epifani, M., & Stirparo, P. (2016). Learning iOS forensics. Packet Publishing Ltd.

[5]. Geetha, S., & Phamila, A. (2019). Countering cyber-attacks and preserving the integrity and availability of critical systems (1st ed.). IGI Global.

[6]. George, D. & Mallery, P. (2016). SPSS for Windows step by step: A simple guide and reference, 11.0 update (14th ed.). Allyn and Bacon.

[7]. Ghosh R. K. (2017), "Mobile OS and Application Protocols," in Wireless Networking and Mobile Data Management, Singapore: Springer Singapore, [On-line], pp. 217–261. Internet: http://link.springer.com/10.1007/978-981-10-3941-6_8

[8]. Heidelberg, [On-line], pp. 264–282, Available: http://link.springer.com/10.1007/978-3-642-39891-9_17 (March 18, 2020]

[9]. Homem, Irvin. "Towards automation in digital investigations: Seeking efficiency in digital forensics in mobile and cloud environments." PhD diss., Department of Computer and Systems Sciences, Stockholm University, 2016.

[10]. Iqbal, A., Ekstedt, M., & Alobaidli, H. (2017, October). Digital Forensic Readiness in Critical Infrastructures: A case of substation automation in the power sector. In International Conference on Digital Forensics and Cyber Crime (pp. 117-129). Springer, Cham.

[11]. Jones, G. M., & Winster, S. G. (2017). Forensics analysis on smart phones using mobile forensics tools. International Journal of Computational Intelligence Research, 13(8), 1859-1869.

[12]. Karpisek, F., Baggili, I., & Breitinger, F. (2015). WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages. Digital Investigation, 15, 110-118.

[13]. Krishnan, S., & Chen, L. (2019). Legal Concerns and Challenges in Cloud Computing. arXiv preprint arXiv:1905.10868.

[14]. Lohiya R., John P., and Shah P. (2015, May), "Survey on Mobile Forensics," Int. J. Comput. Appl., vol. 118, no. 16: pp 6–11

[15]. Lwin, H. H., Aung, W. P., & Lin, K. K. (2020, February). Comparative Analysis of Android Mobile Forensics Tools. In 2020 IEEE Conference on Computer Applications (ICCA) (pp. 1-6). IEEE.
[16]. McKemmish, R. What Is Forensic Computing? Australian Institute of Criminology: Canberra, Australia, 1999.
[17]. Osho, O., & Ohida, S. O. (2016), "Comparative evaluation of mobile forensic tools," mecs-press.net, Available: http://www.mecs-press.net/ijitcs/ijitcs-v8-n1/IJITCS-V8-N1-9.pdf
[18]. Patzakis, J. (2004) 'Computer forensics as an integral component of the information security enterprise', Guidance Software White Paper, www.guidancesoftware.com/corporate/ whitepapers
[19]. Quick, D.; Choo, K.-K.R. Big forensic data reduction: Digital forensic images and electronic evidence. SIGMOD Rec. 2001, 30, 55–64.
[20]. Render, B., & Stair Jr, R. M. (2016). Quantitative Analysis for Management, 12e. Pearson Education India.
[21]. Sathe, S. C., & Dongre, N. M. (2018, January). Data acquisition techniques in mobile forensics. In 2018 2nd International Conference on Inventive Systems and Control (ICISC) (pp. 280-286). IEEE.
[22]. Spivak, B. L., & Shepherd, S. M. (2020). Machine learning and forensic risk assessment: new frontiers. The Journal of Forensic Psychiatry & Psychology, 1-11.
[23]. Teel Technologies, Internet: http://www.teeltech.com/mobile-device-forensic-software/up-828-programmer/ [March 18, 2020]