Synopsis on

A PRIVACY AND INTEGRITY PRESERVING FRAMEWORK FOR INCORPORATING INTELLIGENCE IN DIGITAL FORENSICS

Submitted for registration in the degree of

Doctor of Philosophy

JULY-2020

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CHITKARA UNIVERSITY

HIMACHAL PRADESH

Submitted by

PRIYA RAINA

PHDENG18054

Under the supervision of

Dr. Neha Kishore

Associate Professor

Department of Computer Science & Engineering, Chitkara University, Himachal Pradesh

Dr. Sistla Srinivas Murthy

Assistant Director

CFSL, Hyderabad

Synopsis on

A PRIVACY AND INTEGRITY PRESERVING FRAMEWORK FOR INCORPORATING INTELLIGENCE IN DIGITAL FORENSICS

Submitted for registration in the degree of

Doctor of Philosophy

JULY-2020

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CHITKARA UNIVERSITY

HIMACHAL PRADESH

Submitted by

PRIYA RAINA

PHDENG18054

Under the supervision of

Dr. Neha Kishore

Associate Professor

Department of Computer Science & Engineering, Chitkara University, Himachal Pradesh

Dr. Sistla Srinivas Murthy

Assistant Director

CFSL, Hyderabad

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ABBREVIATED FORM	FULL FORM
ADFM	Abstract Digital Forensics Model
AI	Artificial Intelligence
ALS	Alternating Least Squares
ANN	Artificial Neural Network
AR	Automated Reasoning
ASP	Answer Set Programming
CBR	Case Based Reasoners
CFFTP	The Computer Forensic Field Triage Process Model
CTANS	Center for Telecommunications and Network Security (CTANS) at Oklahoma State University
CTI	Cyber Threat Intelligence
DC3	Defense Cyber Crimes Center
DF	Digital Forensics
DFR	Digital Forensic Readiness
DFRWS	Digital Forensic Research Workshop
DFT	Digital Forensic Tools
DSS	Decision Support System
DST	Department of Science and Technology
EEDI	End-To-End Digital Investigation
IDIP	Integrated Digital Investigation Process
ISA	Intelligent Software Agents
JADE	Java Agent Development Framework
JRF	Junior Research Fellow
KR	Knowledge Representation
LEA	Law Enforcement Agency
MADIK	Multi- Agent Digital Investigation Tool Kit
ML	Machine Learning
NIJ	National Institute of Justice
OSINT	Open Source Intelligence
SIFT	Sans Investigative Forensics Toolkit
UNODC	United Nations Office on Drugs and Crime

1. Introduction

Digital forensics (DF) is a practical science of relatively recent origin that has been rapidly evolving in order to adapt to the fast paced technological changes. According to (Zatyko 2007), digital forensics can be defined as "The application of computer science and investigative procedures for a legal purpose, involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation." Initially restricted to computer forensics, it has diversified to include network forensics, mobile forensics, cloud forensics, multimedia forensics, IoT forensics and so on. There are many commercial and open source digital forensic tools that are available today and are used by computer forensic examiners and analysts during their investigations. Yet, none of this is sufficient to handle the recent data explosion that has resulted into increased processing times for evidence and consequently compounding of case backlogs (Justice 2016). On the flipside, the data challenge presents an opportunity for intelligence analysis in digital forensics.

While establishing the proof in court requires focus on evidence itself, intelligence is the information extracted and processed into knowledge designed for action (UNODC 2011). There are three types of criminal intelligence viz. Tactical, Operational, and Strategic (UNODC 2011). Tactical Intelligence consists of short-term activities, primarily focussed on arrests or gathering evidence and supports the front line staff. Operational Intelligence provides a broader organizational level to support mid-level management in crime reduction, like terrorism and organised crime. It assists in prioritisation for optimum resource allocation. Strategic Intelligence provides insights into patterns of criminal behaviour and environment for planning future activities in the long term. It supports the high-level decision making authorities (Ratcliffe 2007) (UNODC 2011). Intelligence-led policing (Ratcliffe 2007) uses criminal intelligence and data

analysis to reduce, disrupt, and prevent crime and digital forensics, with its treasure trove of data, has the potential to be the enabler and enforcer of this idea. However, without a proper framework, crucial linkages may remain undiscovered. Using the advances in data analytics and use of intelligence analysis techniques like OSINT, it is expected that a large volume of disparate data could be collated to draw valuable inferences. Data across historical cases can provide valuable information and intelligence to assist other current and future investigations.

Use of intelligence in digital forensics is a promising area that has been neglected for too long. However, this should be done in a manner that is sensitive towards the privacy of citizens, because we do not want to create a police state.

This work seeks to explore how intelligence analysis can be incorporated into the digital forensic process while preserving integrity and privacy. Section 2 presents the literature survey, which covers a study of digital forensic frameworks, the state of the art in intelligence analysis in digital forensics and useful tools and techniques. Section 3 presents the justification for research followed by the problem statement, objectives and methodology outlined in Section 4. Section 5 and 6 present the expected outcomes and proposed work plan, respectively, followed by conclusion in Section 7.

2. Literature Review

2.1 Digital Forensics Frameworks

DF refers to the application of Computer Science and investigative procedures for a legal purpose involving the use of digital evidence (Zatyko 2007)(Sammons 2012). It is an umbrella term that has expanded to include within its fold Network Forensics, Mobile Device Forensics, Database Forensics, Cloud Forensics, Social Media Forensics and so on. It deals with the identification, collection, organi- zation, preservation, and presentation of evidence data which is permissible in

the courtroom (Casey 2011). Registry keys, log files, digital fingerprints etc. can provide crucial clues and serve as key evidence. The subsections of this section presents a short background of some of the DF Frameworks proposed in the literature.

2.1.1 Early Models

Pollitt (1995) gave one of the first generalized models for mapping the forensic process with four distinct steps - Acquisition, Identification, Evaluation and Admission as evidence. The U.S. Department of Justice (NIJ 2001) defined an abstract process for collection, examination, analysis, and reporting. The framework by DFRWS (Palmer 2001), a first by the academic community, proposes the steps as identification, preservation, collection, examination, analysis, and presentation. This framework, shown in Fig.1. is by far the most popular and has served as a base for many models like:

- The Abstract Digital Forensics Model (ADFM; Reith, Carr & Gunsch 2002) useful for categorization of incidents
- The Integrated Digital Investigation Model (IDIP; Carrier & Spafford 2003) proposing DF-readiness and investigation of both the physical as well as digital crime scenes
- The End-to-End Digital Investigation Process (EEDI; Stephenson 2003) focusing on the analysis part and integration of spatially diffused events.

The framework by Ciardhuáin (2004), perhaps the most exhaustive framework till date, is the culmination of previous attempts with crisp steps for DF investigation including awareness, authorization, planning, notification, search and identify, collection, transport, storage, examination, hypotheses, presentation, proof, defence and dissemination - useful for development of tools and techniques. Concepts like Event Reconstruction (Carrier & Spafford 2004), knowledge reuse and case relevance (Ruibin, Yun & Gaertner 2005) were added subsequently.

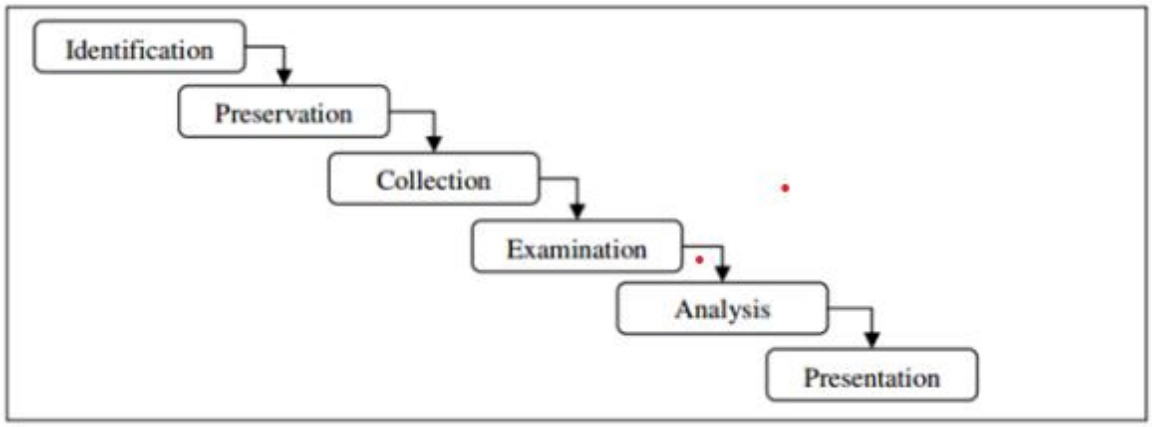

Fig. 1.: The DFRWS model

2.1.2 Tiered Frameworks

Beebe & Clark (2005) proposed the hierarchical objectives based framework for the digital investigations process, a multi-tiered model as against the previously adopted single-tier approach. The first tier comprises the phases dealing with preparation, incident response, data collection, data analysis, presentation and incident closure. The second tier consists of survey phase, extract phase and examine phase. Objective-based tasks are used for analysis. Later, Ademu, Chris & David (2011) presented a generalization of the DF process as a four-tier iterative framework. The first tier involves preparation, identification, authorization, and communication and the second tier handles collection, preservation, and documentation. The third tier handles the analytical part with examination, exploratory testing, and analysis while the fourth tier deals with presentation through result, review and report.

2.1.3 Frameworks for Live Acquisition

Derived from the IDIP Framework (Carrier & Spafford 2003), The Computer Forensic Field Triage Process Model (CFFTP; Rogers et. al 2006) closely relates to the real world investigative methods. As identification, analysis, and interpretation of digital evidence are done on-site rather than in a forensic lab. The phases of the framework include planning, triage, usage/user profiles,

chronology/timeline, internet activity and case-specific evidence. Perumal (2009) proposed a model based on Malaysian Investigation Process for handling fragile evidence.

2.1.4 Integrated Frameworks

Kohn, Eloff, and Oliver (2013) tried to synchronize the existing frameworks by iden- tifying functional similarities in steps/phases across different frameworks suggesting a highly abstract model with three stages viz. Preparation, Investigation, and Presentation. Freiling and Schwittay (2007) proposed the Common Process Model for Incident and Computer Forensics combining incident response and computer forensics with phases including incident preparation, pre-analysis, analysis, and post-analysis. Valjarevic and Venter (2012) attempted to merge existing models, also offering flexibility with respect to placement of various phases and introducing parallel actions in the framework.

2.2 State of the art : Intelligence in Digital Forensics

(Author, Year) Title	Source	Summary	Gaps
(Qadir and Adam 2020) The Role of Machine Learning in Digital Forensics	IEEE Xplore	It presents the predicition based applications of various ML techniques in DF(ML forensics). It suggests that ML techniques like link analysis, self-organising maps, etc. be used for prediction of attacks and crimes and fraud detection.	It is largely a survey paper. It does not discuss the challenges of ML forensics.

(Evangelista et. al 2020) Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence	TnF	It analyses almost 244 publications related to OSINT over the past decade. It traces the growth of OSINT+AI as a research area with increasing applications in cyber security and military intelligence. It leads to a list of interesting papers on OSINT+AI.	Although it's a review paper, it does not present technical insights into the domain, but rather explores the organisation of literature in the domain based on various factors. Also, the paper is not directly related to DF, but is included since OSINT+AI is getting attention from DF researchers.
(Raaijmakers 2019) Artificial Intelligence (AI) for Law Enforcement: Challenges and Opportunities	IEEE Security and Privacy	Machine and deep learning for analysis of evidence: Challenges like Bias, difficulties in model explanation/auditing, Technical Skill for personnel for retraining models and handling AI based solutions (AutoML) are hindering the growth of AI in DF.	Survey paper, primarily discussing operational and legal issues surrounding the AI based solutions for automating steps in DF. Technical details are sparingly discussed. Also, does not highlight the role of AI in extracting intelligence.

(Serketzis et. al 2019) Improving Forensic Triage Efficiency through Cyber Threat Intelligence(CTI)	Future Internet	Builds upon and extends a DFR model that utilises actionable CTI to improve the maturity levels of DFR. Experiments are performed by simulating real-world attack scenarios on malware-related network data. The model identifies the root causes of information security incidents with high accuracy (90.73%), precision (96.17%) and recall (93.61%). Significantly reduces the volume of data requiring manual examination.	The proposed model seems to be useful for internal monitoring in an organisation. It is centred around malware based network attacks. It is not clear how this model will be applicable for LEAs.
(Costantini, Gasperis & Olivieri 2019a) Digital forensics and investigations meet artificial intelligence	Annals of Mathe-matics and Artifici-	Demonstrates the potential of ASP, a logic-based AI technique, in developing DSS for evidence analysis phase. The work involves	Dependent on the investigators' skills for drawing parallels with computational problem(s). Proof of correctness of the

	al Intellig-ence, Springer	reducing fragments of investigative cases into known computational problems and mapping their elements. This is followed by using a suitable ASP solver (existing or custom-designed). Results after execution of ASP solvers are interpreted and integrated to form hypotheses.	reduction can not be presented formally.
(Costantini, Gasperis & Olivieri 2019b) DigForASP: A European Cooperation Network for Logic-based AI in Digital Forensics	Confere-nce paper	AI techniques like exploration of big data and use of ML are suited for the phase of crime identification or detection in DF. But due to their black box nature, they can not be employed for the analysis phase due to inadmissibility as legal evidence. Here Logic-	Presents only the preliminary ideas on the proposal. To the best of knowledge, no details are available yet.

		based AI is more relevant. Proposes DigForASP based upon KR and AR for the evidence analysis phase.	
(Krivchenkov, Misnevs & Pavlyuk, 2018) Intelligent Methods in Digital Forensics: State of the Art	Springer confere-nce	Main areas for application of intelligent methods: (1) rule extraction (2) anomaly detection, (3)intrusion classification. large volume of heterogeneous data with multiple characteristics lead to a classical problem of machine learning—feature selection and extraction. Recommended methods were artificial neural networks, association rule learning, decision trees, probabilistic graphical models, classical clustering methods and	survey paper focussed on intrusion detection systems rather than the entire domain of DF

		classifiers, ensemble learning, and evolutionary algorithms.	
(Quick & Choo 2018) Digital Forensic Data and Intelligence	springer briefs	Discusses criminal intelligence as defined by (UNODC,2011), including types of intelligence (tactical, operational and strategic) and intelligence analysis process. Further discusses how applying the same to digital investigation, in conjuction with other approaches like criminal profiling and cross-referencing can give useful insights. Role of Big digital forensic data from mobile and IoT devices and cloud services in extracting intelligence is also examined and how data reduction is key to	The role of computational intelligence techniques in extracting intelligence from high volume, disparate digital forensic evidence is not studied. Its major focus is on data reduction.

		achieve the same in a reasonable time-frame	
(Vidalis, Angelopoulou & Jones 2016) Extracting Intelligence from Digital Forensic Artefacts	Conference paper	Presents a conceptual architecture for a distributed system that will allow forensic analysts to forensically fuse and semantically analyse digital evidence for the extraction of intelligence that could lead to the accumulation of knowledge necessary for a successful prosecution. Proposes semantic analysis using crime specific ontologies, demonstrated with the examples of identity theft.	Crime specific modules, how integration across these modules and communication between nodes will be secured, is not explicitly mentioned. The techniques used for extracting intelligence have not been listed; there is only a vague reference to big-data like analytics. The conceptual model presented seems to lack clarity.
(Quick & Choo 2014) Data reduction and	Springer Briefs	Modifies existing DF frameworks to add support for data reduction by selective imaging. This process is done in addition	While the results for data reduction are tabulated, details about

data mining framework		to the ususal processing of evidence. This can have multiple applications, like triaging, creating archives/repository of case data, analysis of remotely located data and portable devices etc. Further, reviewing the data-subset so achieved using data mining can assist the investigators in the analysis phase.	implementation of data mining is not given in the case studies.
O'Malley 2015 Forensic informatics enabling forensic intelligence	AJFS, TnF	Presents a case study of Queensland police department, which demostrates the benefits of creating a forensics information register for information sharing developed using agile methodology, It helped in creating useful linkages, leading to rapid forensic	Although not specifically related to DF evidence/artefacts, the paper provides useful insights into the need of a unified system for investigations, digital as well as real.

		analysis, providing significant savings for investigations and ultimately making the community safer by resolving crimes in a timely manner and reducing recidivism. By reducing end-to-end timeframes, the true intelligence value of forensic evidence can be realised.	
Legrand & Vogel 2014 The landscape of forensic intelligence research	AJFS, TnF	Is not related to DF, but use of intelligence for forensics in general. identifies the opportunities and challenges in the implementation of intelligent forensics viz: 1)standardization problems for creating an indexed database for cross referencing.	survey paper

		2)Forensic and investigative independence/divide 3)communication barrier. Further it identifies that intelligent forensics should be used for proactive and preventive policing and prosecution should only be regarded as a by-product.	
(Mitchell 2010) The use of artificial intelligence in digital forensics: an introduction	Confere-nce paper	Identifies two types of applications for automating low level functions and to assist at a higher level in the overall process: some of the possible applications of AI in DF: 1) Expert systems for assisting the investigators for decision making in higher order situations. Case based reasoners can	Data visualisation, applications of SVM are not covered.

		be used for helping the investigators with previously unencountered situations, based on previous cases, also taking care of the reasoning part. Both expert systems and CBRs are, however, ill suited to automate low level activities. 2)Pattern recognition and knowledge discovery with machine learning and data mining. 3) Adaptable tools and techniques using ML based learners and refiners.like decision trees, ANN, ALS etc. 4)knowledge representation and standardisation of ontologies, which would also lead to development	

		of reusable repository consisting of sanitised cases. This would be useful as training data. This should be the first step in order to achieve maximum benefits of using AI.	
(Hoelz Ralha & Geeverghese 2009)\ Artificial Intelligence Applied to Computer Forensics	ACM confere-nce	Presents the architecture of a toolkit, MADIK (MultiAgent Digital Investigation toolKit), which uses AI for (i) reduction of routine and repetitive analysis while also reducing the amount of evidence that must be personally reviewed by the expert, (ii) correlation of evidences (iii) distribution of processes. The system is composed	Details of how correlation is achieved in practical terms are not provided. MADIK is not part of any existing tool.

		of a set of ISAs (Intelligent Software Agents) that perform different analysis on the digital evidence related to a case on a distributed manner using CBRs (Case Based Reasoners). For achieving coordination, agents follow a layered hierarchy (tactical, operational and strategic) and note the observations on a blackboard managed by the operational manager. The toolkit is Implemented using JADE framework. It pre-processes the evidence and marks the evidence as "ignore, inform or alert), These labels are reviewed by human examiner, which is used to determine	

		the confidence level of the agent for similar cases in future.	
(Weiser, Biros & Mosier 2006) Development of a National Repository of Digital Forensic Intelligence	Confere-nce paper	CTANS and DC3 partnered to develop a national repository for sharing digital forensic information among security and law enforcement agencies in the USA. The components of the proposed system included a forensic knowledge base, the expert system, and best practices for forensic investigations, the certified/available tool index, and forensic case index. . The aim was to gather better insights by cross-referencing data across cases. fusion based search and data mining.	The latest publicly available information about the system so developed (DFILink) dates back to 2014, to the best of my knowledge.

		They also identified the reason for failure of such attempts in the past, the primary reason being the reluctance of departments to share/exchange knowledge.	
(Ruibin & Gaertner 2005) Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework	International Journal of Digital Evidence	Proposes application of AI in existing digital forensic frameworks by means of an expert system based on "Case Relevance Information" and text mining and information retrieval. It uses 3 sub-phases, namely, the survey, the extraction, and the examination for the extraction of digital evidence. During the survey, the human investigator develops a profile for the reported case, which is sent to the	Case relevance is an abstract concept. They have not talked about any methods/metrics to implement this concept. Another problem is scalability of the system in practical implementations.

		expert system. Based on the previous cases, the expert system recommends some keywords as seed search information for the input case profile. These keywords are used by the extraction sub-phase to iteratively fetch information until all relevant information is extracted. The findings of the extraction stage are reviewed by the human investigator. The study demonstrated the benefits of incorporating artificial intelligence in the automation of digital investigation.	

2.3 Tools and Technologies

Various tools and technologies will be used in developing and testing the framework for intelligent digital forensics:

1. DF Tools: Triaging tools like EnCase portable and Triage investigator, write blocking and imaging tools like Tableau, open source tools like linux utilities (dd, dcfldd) and autopsy, tools for live memory forensics, OSINT and so on.
2. Kali linux OS
3. Oracle Virtual box
4. Python with Jupyter notebooks or R for implementation.

3. Justification for Research

3.1 Motivation

Digital forensics as a research area is interesting due to two reasons. Firstly, the fact that it is an evergreen area which can never really become irrelevant. Another reason is the existence of a wide pool of challenging problems that still need the attention of the researchers. One such problem that requires attention is digital forensic intelligence.

Intelligence analysis has been often discussed in forensic sciences literature since the early 2000s, but most of the work is more didactic in nature, with suggestions as to what should/can be done, without any followup on the practical front. The same is true for digital forensics intelligence too, which requires a multi-disciplinary approach. Given the volume of data that needs to be analysed in a single case, intelligence analysis may help in extracting useful insights in a shorter time frame. More broadly, it may even help in preventing and deterring crimes.

As JRF in the DST sponsored project “Study the Effects of Parallel Hashing Algorithms and the Use of Digital Footprints for Security and Fast Digital Forensic Investigations”, the study of digital footprints led me to digital forensics intelligence.

3.2 Research Gaps

Based on the study of relevant literature, following gaps were identified:

a) Distinction between acquisition and analysis tools: A majority of the currently available DFTs, like Tableau, EnCase, SIFT, FTK etc.,are either hardware or software. Hardware tools are used in the initial stages, primarily for acquisition of evidence, imaging and hashing. Software tools dominate the analysis phase of the investigation. The two classes of tools complement each other and yet are almost mutually exclusive. Thus, there is a clear demarcation between hardware and software tools, the number of alternatives being very few in the former as compared to the latter. In modern computing, like IoT and cyber-physical systems- the boundary between hardware and software is blurred. Digital forensic tools will have to evolve along similar lines. Thus, hardware tools can no longer be ignored. Of late, some triaging tools have emerged, which are a cross between hardware and software tools but there still is a need to work on the edges (Carrier & Spafford 2003; Casey 2011;Sammons 2012).

b) Despite there being much discussion regarding the data volume challenge and many calls for research into the applications of data mining and other techniques to address the problem, there has been very little published work in relation to a method or framework to apply data mining techniques or other methods to reduce and analyse the increasing volume of data (Quick & Choo 2018).

c) In addition, the value of extracting or using intelligence from digital forensic data has barely been discussed, nor there is research regarding the use of open, closed and confidential source information during digital forensic analysis (Quick & Choo 2018).

d) Use of AI in DF is still restricted to classification and assistance in decision making. Its utility in predictive analysis is a less explored area (Costantini, Gasperis & Olivieri 2019b).

4. Problem Statement

To propose and implement a privacy and integrity preserving framework for incorporating intelligence in digital forensics.

4.1 Objectives

- To propose a practical model for intelligence analysis in digital forensics investigation, that may leverage the advances in big data analytics for predictions.
- To verify and validate the model using publicly-available data.
- To present a privacy and integrity-preserving digital forensic framework that supports the proposed model.
- To demonstrate the applications of the framework on different types of storage devices.

4.2 Methodology

The flowchart in Fig. 2 outlines the methodology that is likely to be followed, mapping the activities to the objectives stated above.

5. Expected outcomes

The proposed work is likely to enhance the existing digital forensic process by adding the ability to collate data and draw meaningful inferences and associations in a shorter time-frame. At the same time, the resulting framework would be sensitive towards privacy. This approach would be particularly useful in processing the evidence in modern computing environments, like cloud, mobile, IoT etc. It may also have implications for areas where predictive analysis can be useful, like financial forensics and preventive policing.

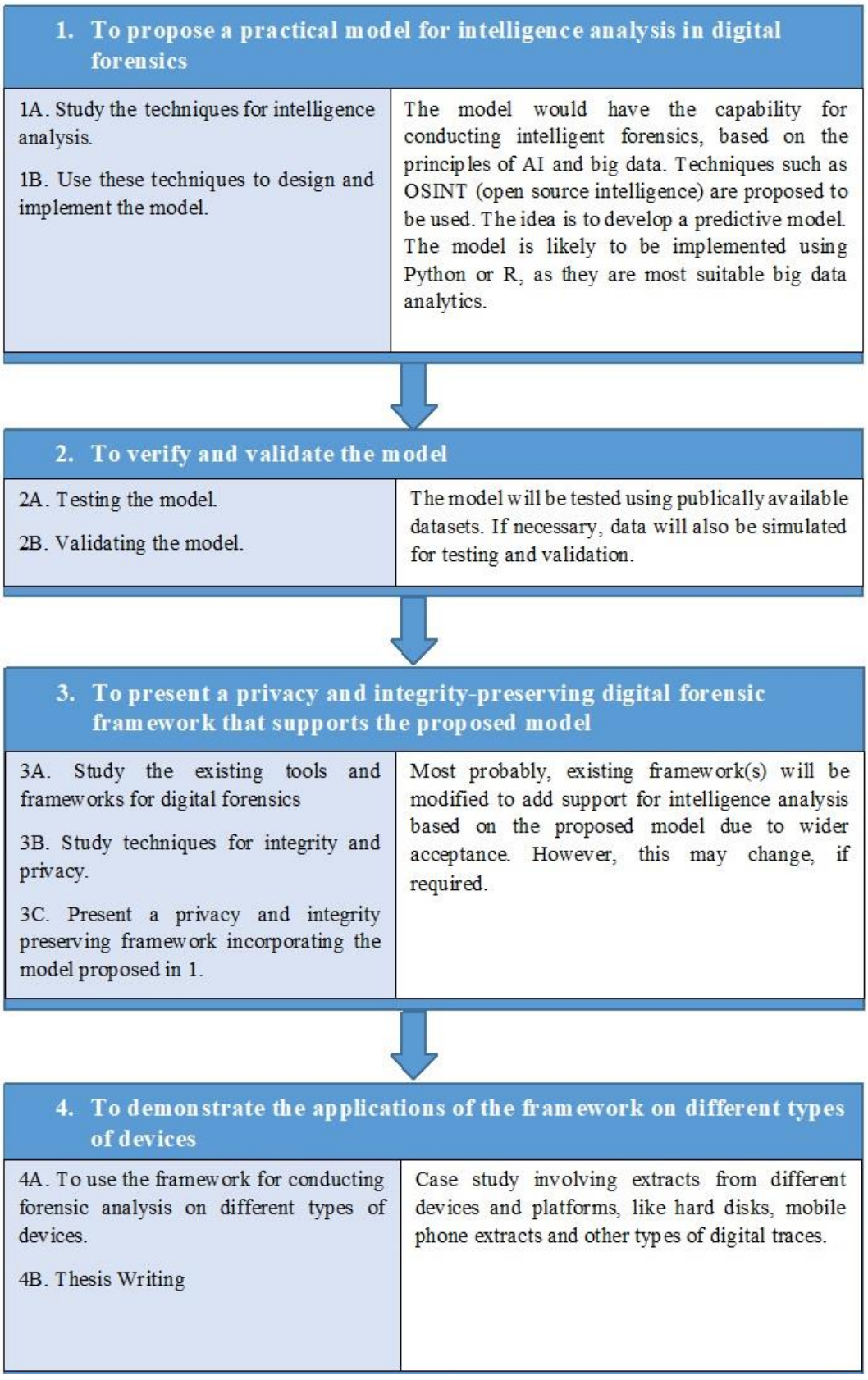

Fig.2: Methodology

6. Workplan

Fig.3 depicts the tentative timeline for conducting the research.

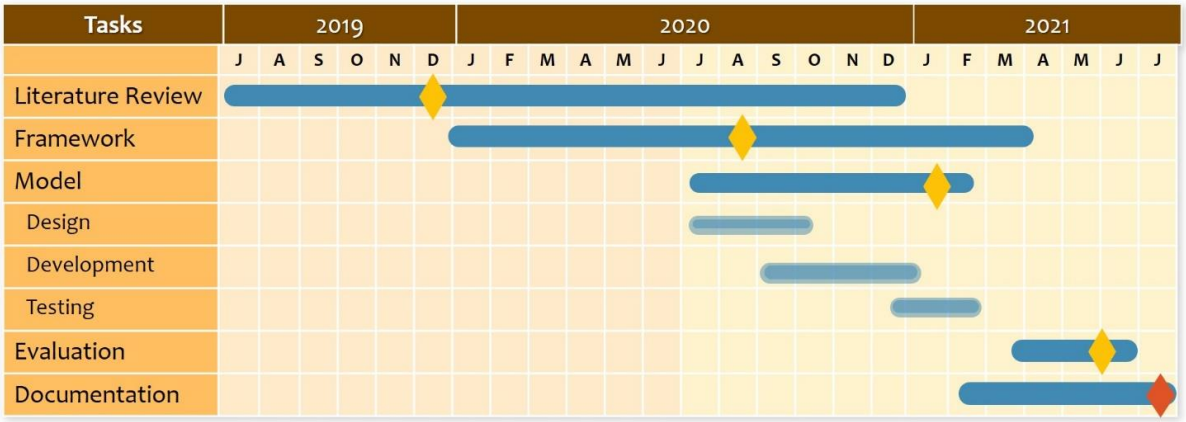

Fig. 3 Gantt Chart

7. Conclusion

Digital forensics faces challenges due to the 3Vs of data- volume, variety and velocity. This has led to an increase in the processing times of evidence, accumulating backlogs. If this data challenge is viewed as an opportunity rather than a problem (talking about glass being half full), digital forensics is a treasure trove of data, which if processed using latest developments in data analytics, can help in deriving various levels of intelligence. This can be the key to reducing crime in near future. However, caution must be observed that this intelligence does not come at the cost of serious damages to individual rights, like privacy. Therefore, a privacy-preserving intelligent and proactive framework is the next giant leap for digital forensics.

References

Ademu, I.O., Imafidon, C.O. and Preston, D.S., 2011. A new approach of digital forensic model for digital forensic investigation. International Journal of Advanced Computer Science and Applications, 2(12), pp.175-178.

Beebe, N.L. and Clark, J.G., 2005. A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, 2(2), pp.147-167.

Carrier, B. and Spafford, E., 2004. An event-based digital forensic investigation framework. In Proceedings of DFRWS 2004. *https://dfrws.org/wp-content/uploads/2019/06/2004_USA_paper-an_event-based_digital_forensic_investigation_framework.pdf .Last accessed on 10 August 2020*

Carrier, B. and Spafford, E.H., 2003. Getting physical with the digital investigation process. International Journal of digital evidence, 2(2), pp.1-20.

Casey, E., 2011. Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.

Ciardhuáin, S.Ó., 2004. An extended model of cybercrime investigations. International Journal of Digital Evidence, 3(1), pp.1-22.

Costantini, S., De Gasperis, G. and Olivieri, R., 2019. Digital forensics and investigations meet artificial intelligence. Annals of Mathematics and Artificial Intelligence, 86(1-3), pp.193-229.

Costantini, S., Lisi, F.A. and Olivieri, R., 2019. DigForASP: A European Cooperation Network for Logic-based AI in Digital Forensics. In Casagrande, A. and Omodeo, E.(Eds.) proceedings of the 34th Italian Conference on Computational Logic (CILC 2019; pp. 138-146).

Evangelista, J.R.G., Sassi, R.J., Romero, M. and Napolitano, D., 2020. Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence. Journal of Applied Security Research, pp.1-25.

Freiling, F. C. & Schwittay, B., 2007. A common process model for incident response and computer forensics. In: Göbel, O., Günther, D., Hase, H. G., Nedon, J., Schadt, D., Brömme, A. & Frings, S. (Eds.), IMF 2007: IT-Incident Management & IT-Forensics. Bonn: Gesellschaft für Informatik e. V.. (pp. 19-39).

Hoelz, B.W., Ralha, C.G. and Geeverghese, R., 2009, March. Artificial intelligence applied to computer forensics. In Proceedings of the 2009 ACM symposium on Applied Computing (pp. 883-888).

Justice, UDo (2016). Office of the Inspector General. Audit of the federal bureau of investigation's New Jersey regional computer forensic laboratory, <https://oig.justice.gov/reports/2016/a1611.pdf>. *Last accessed on 10 August 2020*

Kohn, M.D., Eloff, M.M. and Eloff, J.H., 2013. Integrated digital forensic process model. Computers & Security, 38, pp.103-115.

Krivchenkov, A., Misnevs, B. and Pavlyuk, D., 2018, October. Intelligent Methods in Digital Forensics: State of the Art. In International Conference on Reliability and Statistics in Transportation and Communication (pp. 274-284). Springer, Cham.

Legrand, T. and Vogel, L., 2015. The landscape of forensic intelligence research. Australian Journal of Forensic Sciences, 47(1), pp.16-26.

Mitchell, F., 2010. The use of Artificial Intelligence in digital forensics: An introduction. Digital Evidence & Electronic Signature Law Review, 7, p.35.

National Institute of Justice (US). Technical Working Group for Electronic Crime Scene Investigation, 2001. Electronic crime scene investigation: A guide for first responders. US Department of Justice, Office of Justice Programs, National Institute of Justice.

O'Malley, T., 2015. Forensic informatics enabling forensic intelligence. Australian Journal of Forensic Sciences, 47(1), pp.27-35.

Palmer, G., 2001. A road map for digital forensics research-report from the first Digital Forensics Research Workshop (DFRWS). Utica, New York.

Perumal, S., 2009. Digital forensic model based on Malaysian investigation process. International Journal of Computer Science and Network Security, 9(8), pp.38-44.

Pollitt, M., 1995, October. Computer forensics: An approach to evidence in cyberspace. In Proceedings of the National Information Systems Security Conference (Vol. 2, pp. 487-491).

Qadir, A.M. and Varol, A., 2020. The Role of Machine Learning in Digital Forensics. In 2020 8th International Symposium on Digital Forensics and Security (ISDFS), (pp. 1-5). IEEE. doi: 10.1109/ISDFS49300.2020.9116298.

Quick, D. and Choo, K.K.R., 2014. Data reduction and data mining framework for digital forensic evidence: storage, intelligence, review and archive. Trends & issues in crime and criminal justice, 480, pp.1-11.

Quick, D. and Choo, K.K.R., 2018. Digital Forensic Data and Intelligence. In Big Digital Forensic Data (pp. 29-47). Springer, Singapore.

Raaijmakers, S., 2019. Artificial intelligence for law enforcement: challenges and opportunities. IEEE Security & Privacy, 17(5), pp.74-77.

Ratcliffe, J. (2007). Integrated intelligence and crime analysis: Enhanced information management for law enforcement leaders (2nd ed.). Washington, DC: Police Foundation.

Reith, M., Carr, C. and Gunsch, G., 2002. An examination of digital forensic models. International Journal of Digital Evidence, 1(3), pp.1-12.

Rogers, M.K., Goldman, J., Mislan, R., Wedge, T. and Debrota, S., 2006. Computer forensics field triage process model. Journal of Digital Forensics, Security and Law, 1(2), p.2.

Ruibin, G., Yun, T. and Gaertner, M., 2005. Case-relevance information investigation: binding computer intelligence to the current computer forensic framework. International Journal of Digital Evidence, 4(1), pp.1-13.

Sammons, J., 2012. The basics of digital forensics: the primer for getting started in digital forensics. Elsevier.

Serketzis, N., Katos, V., Ilioudis, C., Baltatzis, D. and Pangalos, G., 2019. Improving Forensic Triage Efficiency through Cyber Threat Intelligence. Future Internet, 11(7), p.162.

Stephenson, P., 2003. A comprehensive approach to digital incident investigation. Information Security Technical Report, 8(2), pp.42-54.

UNODC 2011. United nations office on drugs and crime—Criminal intelligence manual for analysts, United Nations, New York, Vienna, Austria.

Valjarevic, A. and Venter, H.S., 2012. Harmonised digital forensic investigation process model. In 2012 Information Security for South Africa (pp. 1-10). IEEE.

Vidalis, S., Angelopoulou, O. and Jones, A., 2016. Extracting intelligence from digital Forensic artefacts. In European Conference on Cyber Warfare and Security (p. 282). Academic Conferences International Limited.

Weiser, M., Biros, D.P. and Mosier, G., 2006. Development of a National Repository of Digital Forensic Intelligence. In Proceedings of the Conference on Digital Forensics, Security and Law (p. 17). Association of Digital Forensics, Security and Law.

Zatyko, K., 2007. Commentary: Defining digital forensics. Forensic Magazine.