DIGITAL FORENSICS-

IMPLEMENTATION AND CHALLENGES

NAVEEN DAYAKAR VELPUR
RUID- 176004603

ABSTRACT

Digital forensics is not an item of definition, rather it is a process. The topic of digital forensics is very wide and has many sub-divisions within it with respect to the technology and the industry it is associated with.

The process of forensics in the digital world is complicated by the laws and the technical challenges put forth. The paper discusses the need for a proper model, that devices a way of right approach to the forensic investigation, irrespective of the technology or the organization where the crime is being investigated.

The challenges faced by the digital forensic experts in terms of legal issues, technical issues and also the difficulties faced while collecting the data are discussed. The challenges discussed under these above-mentioned categories are ever existing irrespective of the technological changes that could happen in the future.

Comparison of the current day digital forensic models were discussed, proposed by various organizations according to their needs. The comparison will be in terms of procedure proposed, the feasibility of it in almost all common scenarios in E-crimes, and the probable direction for the future research work to propose an interoperable framework.

The high volume of data that is being stored, along with the advantages and disadvantages of it are discussed in the paper. Since there are emerging technologies and new file formats on a daily basis, is it practically impossible for the tools and techniques developed to solve digital crimes to cope up.

With the invention of new technologies, it should not be forgotten that there are new vulnerabilities that are yet to be found and fixed. There is a tradeoff between the cost required to find the weaknesses in a network and the cost required in the process to make it more secure.

The possibilities of using current day digital forensic models and why they would not be so useful in the future can be explained by observing the changes in both the quantity and how much these devices are involved in day-to-day life.

Additionally, methods to avoid and solve the challenges are provided. The emphasis is on the possible changes to digital forensics that may happen in the future, and also the ways the digital forensics industry must be prepared to overcome those challenges in the future.

1.INTRODUCTION

These days, E-crimes are more unknown, expanding in number and harder to recognize. The issue is that an understudy programmer who cuts down a server only for the sake of entertainment is similarly a criminal with a programmer who takes data from a server. Since the cybercriminals don't share a typical profile, police work turns out to be more troublesome. With a specific end goal to examine such violations, innovative skill and instruments are required. This prompted the advancement of the new time of crime scene investigation called Digital Forensics.

Computerized crime scene investigation is a procedure. There are more than several examination systems everywhere throughout the world and each varies from each other as for the association that created it. Some of them center around the innovative parts of information securing, while some emphasis is on the information examination part of the investigation.

A good model for investigations is a necessity for the investigators and computer experts, as it will provide an abstract reference framework, that will be independent of the technology or organization. It benefits not only law enforcers, it also helps security practitioners, IT managers etc., as breaches and inappropriate use of internet in a company is a violation of company policy.

As we quicken towards a more advanced world, the probability that a data relating to a wrongdoing can be found in computerized shape is high. This can moderately anticipate violations all in all. The upgrades in the advanced world have prompted the high rate of creation of computerized data. A forensic agent needs the best devices for extracting and analyzing information that has an impact on a crime. Once the data is acquired, the challenge is to preserve it long enough till it is required to be presented lawfully as an evidence. Data storage has become easy due to cloud services, but the differences in the way data are stored in the cloud and the organizational structure may have an impact on the data collected as evidence from the cloud.

Though the present-day technologies are used to collect and store information, there are some challenges that the field of digital forensics meets legally, ethically and technologically. Technical difficulties arise during the data acquisition stage, where the forensic investigator must look for possible evidence and in the process, huge amounts of data must be logged and collected. The volatility of data and unavailability of a forensic tool-kit that can solve all issues are major technical problems. There is very little consistency between the forensic industry and the court of law, as digital forensics is a relatively new topic with technological advancements on a daily basis. This has given a way for the lack of a standardized procedure or framework. A unified law concerning computer-related crime between governments is the solution to legal problems faced in this industry.

The paper aims to identify and analyze the problems faced during forensic activity and also the procedure of storing and reserving the information after the acquisition phase. The technical, ethical and resource challenges are discussed elaborately and thoroughly analyzed. The paper proposes extended models of cybercrime investigations, compares the models against each other, discusses the potential for future research work.

2.RESOURCE CHALLENGES

Each year, with the invention of new technologies, new digital crimes come along with it. Since the technology changes and improves at a fast rate, the digital crimes are also becoming complex and hard to avoid. As more devices become digitized, the tools to identify the threats must also evolve at the same rate. In this section, we discuss the challenges that have to be faced to collect, efficiently store and analyze digital evidence.

The volume of data that could serve as potential evidence in investigations is increasing rapidly. The increasing proliferation in the number of IOT and mobile devices, the increase in storage capacities are the major factors that demand new technologies and tools that are capable of handling huge amounts of data for investigations.

In addition, the already existing backlog of cases for investigation will blow in size due to the increase of the gadgets and their daily use. The already existing backlog was created because of the high volume of logs that was acquired, stored and difficulty in making certain that the collected data is admissible in the court as an acceptable evidence.

The increase in backlog cases pending investigation are subject to the increase in [Lillis, David et al., (2016)]:

- Number of devices
  The increase in the number of devices that are collected as digital evidence for a single case keeps increasing, this is a result of an increase in the number of digital devices on a daily basis.
- Number of cases
  The number of E-crimes where digital evidence is a key factor are more in number.
- Storage size
  The data logged by each device is more frequent and huge in volume.

The backlog and pending cases due to these issues are responsible for the long durations of legal processing and created delays in courts.
Improvements in the form of digital forensics is always seen as a technological advancement in improving the tools to solve crimes and investigate with ease, but the real problem arises if the data is not stored properly and there is struggle in data retrieval and acquisition. Since digital forensics is a process, the most important part of the investigation is collecting the appropriate evidence as quickly and accurately as possible and storing it securely till it is presented in court. To expedite the process, the below infrastructural improvements are explored.

Below are some of the most common resource challenges faced by digital forensic experts [Lillis, David et al., (2016)].

- Need for data reduction techniques, since there is a complexity problem arising from the data being collected at the lowest level with increasing volume and heterogeneity.
- The lack of standardization of digital evidence causes a plurality of operating systems, file formats etc. It also adds to the complexity of sharing digital evidence between national and international law enforcement agencies.
- Also, due to the lack of standardization, the tools which are designed to find fragments of evidence are not able to be of advantage for every investigation. Different tools must be used for different types of investigation.

- There is lack of sufficient automation for analysis, which is a result of increased storage capacities and also the increasing number of digital devices.
- The time-zone differences and time stamp interpretations may differ between the different sources obtained as evidence. This creates a unified time-lining problem.

Resource challenges in Cloud Environments

Data in a cloud is distributed to nodes instead of storing it in a single system like traditional forensic scenarios. This amplifies the cost, and also the time needed for a digital forensic procedure. The fact that the data is split into blocks and stored in different blocks that may be separated geologically adds complexity to the forensic scenarios in cloud environments.

The willingness of the CSP (Cloud Service Provider) and the user base must be taken into account before proceeding with the acquisition and reproduction of data.
Since it is an easy process to even buy a cloud service with almost no input required from the clients end, any criminal could sign-up and can be anonymous once an E-crime is committed.

Encryption and other anti-forensic techniques are used in solving the crimes, but also the fact that the cloud systems and continuously running and data can be over-written at any time poses an issue. The time acquisition required for tools to identify the culprit is difficult in cloud environments due to the above-mentioned reasons.

Most of the investigations do not cross the point where the suspect's devices are checked, so investigators do not usually go through the process of accessing the cloud storage for proper evidence. But the rise of the number of devices, can change this process. Due to cheap and easily accessible cloud services on the rise, adequate tools to investigate the stored information in cloud environments may be necessary.

Resource challenges in IoT Environments

IoT can overtake the world with the rise of interdependency and communication between devices. But, the IoT has its own security issues and it also paves way for a person who does an E-crime to go unnoticed because of the limited ways to trace information origin or destination. There is no certainty as to where the data is stored and where it originated from.

The data can be stored in an in-network hub if it is stored for long periods or it may be sent to the cloud for persistent storage. It is very evident that the challenges are similar for IoT just like the cloud environment.
Since the IoT devices can consist of different brands, interfaces, etc,. the lack of similarity between the interconnected IoT devices can cause hurdles to digital forensic investigators.

To prevent E-crimes, the security can be tightened in devices that have a CPU at least. But IoT has devices that are small and battery-operated.
Nowadays, our daily life is dependent on devices that can be carried with us, and they are expected to increase in number and also the associated complexity of them increases as the devices are no capable of communicating with each other. In digital forensics, we can expect that these devices will be involved in almost all of the digital forensic investigations in the future.

3.TECHNICAL CHALLENGES

It is very important to address the fact that, all the participating entities in a digital forensic investigation must be aware of the technical difficulties that may arise. The technology has been improving so fast and at an unexpected pace, that the tools required to investigate the cases are not able to cope up. It is necessary for the research to continue to improve the tools and techniques in the best way possible.

The technicians working on a case must constantly update themselves on the latest technological improvements, their disadvantages and weaknesses. The investigators must be as technologically sound as the hackers themselves, and must be aware of all the viruses and their functions. This session discussed the most common technical challenges that occur and also speaks about the possible ways to avoid them.

Ubiquitous availability of data:

Since the use of devices on a daily basis and almost a complete dependency of humans on them, the devices in the current day scenario log huge amounts of data on a regular basis. The devices are even capable of listening and talking with each other and they can even limit or increase the scope of another device that is running in its control.

The data that is being logged by even small hand-held devices to battery operated ICs, is of tremendous amounts and the extraction and acquisition of the relevant data for a particular set of events that may act as a potential evidence is a big investment of time and money.
It is impossible in the future to avoid using big datasets to scrape a small piece of information, so technical experts in the field must adapt to data mining techniques.

Data Volatility:

The data that has been deemed to be a possible evidence cannot be discarded or altered till it has been produced in court. Data sometimes can be collected in the most unstable forms, and the technicians have to deal with the protection and preservation techniques to make sure the data is not damaged till it is accepted by law as an evidence [Miranda Lopez et al., (2016)]. Special tools like handle must be used to capture the volatile memory [Xrysanthou et al., (2006)], since they can give insights about the instance being investigated.

Technical challenges in cloud environments:

As seen before the cloud service provider and the investigators must go hand-in-hand to tackle some of the technical challenges involved in digital forensics in cloud environments. Sometimes, there may be no physical access to the location where a particular data is stored, since the cloud does not have a proper storage location for all the networks. The provider must cooperate with the investigator to perform the necessary steps to retrieve the data.

Also, the same information may fall under the jurisdiction of two or more countries with different laws, the cloud service provider must solve the legal issues and also implement resource sharing techniques between multiple investigators working on a same case.

The interoperability of the investigators is not a possible option if more than one cloud service is involved in the investigation process. There may be no correlation between the networks and the technology used in the different cloud services. Even if they were the same, cooperation between two or more cloud service providers is a rare scenario.

Forensic Tool-Kit:

The investigators and technicians working on digital forensics must device an appropriate tool-kit for every particular case. This would be of use since the tool must be compatible with the network, or the interface from where the evidence is to be extracted.

It is depressing that there is not a single solution such as a universal tool-kit. Each case is different since digital forensics is a wide topic that has many branches such as network forensics, mobile forensics etc. Each E-crime can be form any of these branches or at the worst case can involve all of them.

Cryptographic Techniques:

With the growing need to access any network easily and ease of retrieval of information of this fast pace world, even signing up for cloud service does not take much time. But this luxury comes with its own disadvantages. The security issues are on the rise and almost all of the data communications are not end-to-end encrypted.

The encryption techniques are done so that hackers do not get their hands on important information or any private data of a person. When investigations are carried out even in these secure environments, the technicians are forced to reverse engineer attacks and it is a painstaking process. The technicians must be aware of the cryptographic techniques [Miranda Lopez et al., (2016)] and require cooperation from the government to obtain legal permission to use decryption techniques.

Recovering lost or deleted data:

All evidence in the form of information is not readily available. The data that acts as a potential evidence may be very difficult to retrieve or track. Most of the data, due to the enormous amounts of it, can be discarded or lost if not backed up regularly. Sometimes, forensic experts are expected to perform live forensics. This means that the data is continuously tracked and involves traffic capture [Xrysanthou et al., (2006)]. During this process, the appropriate tools to recover data from backups, and even from repositories are necessary [Miranda Lopez et al., (2016)].

This is even more difficult in cloud environments where the data is continuously rewritten over already recorded data. Any information that is not backed up in these environments is lost forever.

The forensic examiner must usually have a lot of coding experience, as coding will be necessary to alter the exiting tools to comply with the network or the interface the particular case is dealing with. Also, for the evidence to be accepted, the tools used to retrieve the information must also be accepted. The tools used for the investigation must be checked under normal conditions, with well-organized situation similar to the investigation case [Xrysanthou et al., (2006)]. This is very important as the data collected may be incomplete and leads to a wrong assumption and ultimately a wrong judgement.

4.ETHICAL CHALLENGES

Since computer data is vulnerable to tampering, forging, and deletion, in order to make it acceptable as evidence, it must be made sure that during the generation, storage and maintenance of the data, the originality of the data must remain unaltered. In order to meet these requirements, a set of steps have to be followed by the digital forensic experts.

- The harmed PCs, the original state, the investigation carried out, the result of the examination must be legitimately recorded.
- The information must be backed up on a timely basis during the investigation.
- The gathered confirmation must be preserved properly to keep it from getting damaged or altered.
- The investigation must not be done on the information specifically
- The programming for breaking down the information must be sheltered and secure.
- There must be a signature done before breaking down the information.

Because of these requirements, the legal entity of the investigation must have some computer knowledge and the technical experts must have a knowledge of the legal aspects of the investigation.

Digital forensics is a wide area and it is exponentially expanding. This creates a huge gap between technical experts and legal advisors.

The legal entity in an investigation process will know the legal practices, the importance of knowing the technical aspects of the evidence that has been found and the procedures necessary to get the evidence. However, it is very impractical to expect a complete knowledge of the technical issues related to gaining evidence in an investigation.

For example, electronics evidence is difficult to store and preserve for a long time and also it can be affected by viruses, hacker attacks and can also be damaged or altered. Also, electronic evidence cannot be transferred normally, it cannot be read directly and its access to transportation depends on the availability of appropriate technology. This must be understood by both the technical and legal entities before proceeding with an investigation.

Developing security and information assurance controls crosswise over topographies and developing administrative definitions/requirements may add to the complexity of gathering evidence.

For example, data accessible on the suspect's machine (given by the organization) may contain certain private, non-delicate data, which might be valuable in investigations. Be that as it may, access to this data might be viewed as an infringement in specific nations.

Thus, with the period of "bring your own particular device" (BYOD), organizations enabling work-force to utilize individual cell phones for getting to official correspondence may add to the difficulties of gathering evidence. For example, access to an email from webmail through a cell phone and the download of connections might be a source of information theft. Be that as it may, particular data on the gadget on which such data was downloaded and points of interest on which records were downloaded might be hard to follow in the present condition.

Privacy laws:

According to the privacy laws, they are set up to provide protection to each citizen of a country. A digital forensic investigator can connect an attack to a person's IP address and can access the suspect's computer or device in order to do so. If the investigator is not able to prove to the court that the information collected is not sufficient for a warrant, the suspicions may not be proved in court [Xrysanthou et al., (2006)].
Also, sometimes the investigator has to compel the ISP's to collect and retrieve data from them for investigations, which the IPS does not will to give because of the cost and time involved.
The European laws state that the ISP's can hold on to a private data of a suspicious act for no more than 90 days and it will be a privacy invasion otherwise [2].
These are some of the difficulties that all the entities involved in an investigation must be aware of.

Jurisdiction:

Since investigators have to collect huge amounts of data as evidence, they may even have to travel to several countries and get on-site to retrieve the evidence [Xrysanthou et al., (2006)]. It is difficult for the investigation to proceed at the fast pace due to these differences in jurisdiction and laws in different parts of the world. There are places where even creating computer viruses is not a crime.

FORZA framework:

To incorporate all legal issues, a digital forensics framework was introduced called the FORZA framework.
According to Ricci Ieong [3], the roles can be further classified and they would fall into 8 categories as mentioned below.
"They are classified into Case leader, System/business owner, Legal advisor, Security/ system- architect/ auditor, Digital forensics specialist, Digital forensics investigator/system administrator/operator, Digital forensics analyst and Legal prosecutor [3]".

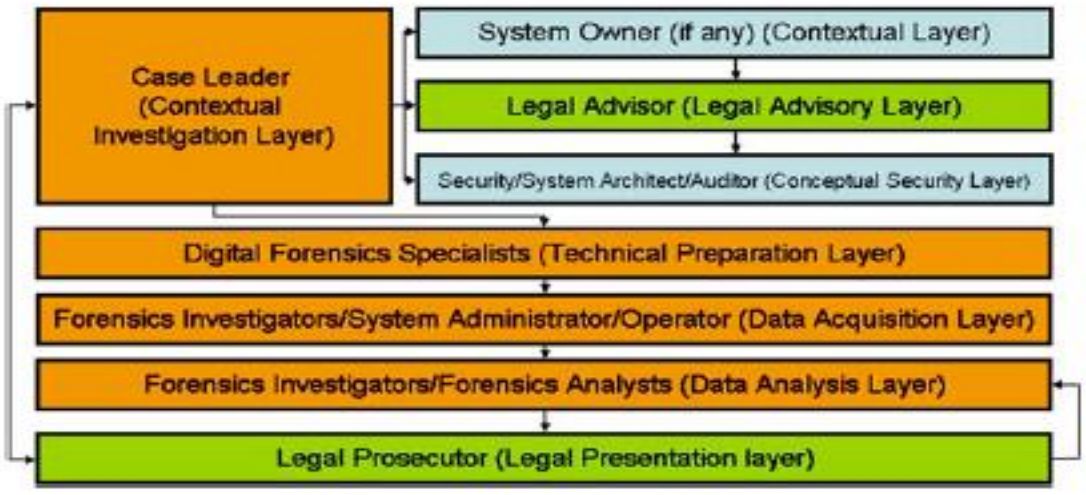

Figure 1: Source- Ieong, Ricci. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. Digital Investigation. 3. 29-36. 10.1016/j.diin.2006.06.004.

The flow chart depicted above shows the holistic approach of how the various entities that are interdependent in a digital forensic investigation must come together for ease of process. The process of investigation was always seen from a technical and technological point of view, but the business end must coincide with the legal and technical aspects of the investigation team. The framework will act as a guideline for the procedure.

The framework clearly lists out the procedures to be carried out by the legal advisors and thus eliminating the confusion that may be caused due to the interference of other entities in the investigation. Ricci Ieong [3] states the set of questions like what, why, who, how, where and when that have to be answered by a legal entity.

It is the duty of the legal advisor to focus on the objectives (why), the background issues (what), procedures for further investigation (how), geography (where), entity and participants (who) and the legal timeframe (when).

5.CURRENT FORENSIC MODELS

To overcome all of the mentioned challenges, in whatever form they may be, it is evident that the guidance of frameworks and standardization of procedures is necessary for the smooth functioning of investigations. The rise of devices in use will increase multifold and the technologies and tools to investigate should evolve along with them. To support this, there are a number of standardized forensic models being used commonly. The session discusses the models, their advantages and downsides and compares them against each other.

A good model is important as it provides a framework that is independent of organizations, their procedures and also is independent of technologies. To understand the direction of future research of models that will be used for cyber-crime investigations, it is necessary to discuss about the current models in use.

Lee's Model:

The lee's model is supposed to have a design to guide crime scene investigation and not the full investigative process (Lee et al., (2001), cited in [Ó Ciardhuáin, Séamus., (2004)]).

- Recognition is the first step in this process, where there is a search for potential evidence. All the items are to be seen as a lead to the investigation. The recognition is followed by preservation and documentation.
- Identification of the evidence, which means that the item must be classified. The property of the item like the physical and biological aspects etc. must be noted down in this stage.
- Individualization refers to identifying whether a particular item is linked to another item or an event.
- Reconstruction, as the name suggests is the process of collecting all the useful evidence right from the beginning and framing a series of events and actions in a crime scene.

Lee et al., (2001), thus described a model that would define a series of steps to identify a list of events or possible series of actions in a crime scene, but it fails to address the same issue

for a digital crime scene investigation. Though the steps are almost similar for both digital and normal crime scene investigations, the specific procedures where the difficulties in transporting and means of communicating with digital evidence with other investigators are not explored in this model.

Casey's Model:

The Casey's model is designed to address the procedures for processing and examining digital evidence (Casey.E, 2000), cited in [Ó Ciardhuáin, Séamus. (2004)]. The steps in the model are almost similar to the Lee's model.

- Recognition
- Preservation, collection and documentation
- Classification, comparison and individualization
- Reconstruction.

The last steps as mentioned in [Ó Ciardhuáin, Séamus. (2004)], will refer to the phase where the analysis takes place. Casey points out that the evidence processing in this model is a cycle since the reconstruction may lead to the first step of the model again.

The advantage of this model is that it is defined in terms of standalone systems and also can be extended to computer networks. Since it is flexible it is applied to both the network and standalone device environments.

DFRWS Model:

According to (Palmer, 2001), cited in [Ó Ciardhuáin, Séamus. (2004)], a new model was proposed by the Digital Forensics Research Workshop. The steps are as below:

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation
- Decision

The DFRWS model appears normal and with no specification to the technology that it supports, but it is feasible for a prospective expansion. It has a set of steps defined for each stage of the process and takes feedback from one stage to another.

Reith, Carr and Gunsh Model:

The model is derived from the DFRWS model and in (Reith, Carr and Gunsh, 2002), cited in [Ó Ciardhuáin, Séamus. (2004)], the steps in the model include:

- Identification
- Preparation
- Approach Strategy
- Preservation
- Collection
- Examination

- Analysis
- Presentation
- Returning Evidence

The advantage of this model is that it is deemed to serve any particular technology or any technology that has to be used. Also, the approach strategy stage sets the platform for the model to fit right in whether evidence is extracted from a floppy disk or even a high-tech hand-held device.

Activity in new model	***MODEL***			
	Lee et al.	Casey	DFRWS	Reith et al.
Awareness				✓
Authorisation				
Planning				✓
Notification				
Search/Identification	✓	✓	✓	✓
Collection	✓	✓	✓	✓
Transport				
Storage				
Examination	✓	✓	✓	✓
Hypothesis	✓		✓	✓
Presentation	✓		✓	✓
Proof/Defence			✓	
Dissemination				

Figure 2: Source- Ó Ciardhuáin, Séamus. (2004). An Extended Model of Cybercrime Investigations. IJDE. 3

The table above compares the stages in each of the model, together it gives a better idea how the steps have been improved in recent years. This shows the need for a better fit to the investigations and each organization sculpting the model in their own way to make it a better one. There are numerous models available, but the reason of discussion of the above ones because they are most commonly used as standard procedures.

The discussion about a proposed model to suit the needs of the current day scenario and the future, where even the basics like storage of data, jurisdictional laws are completely different than what was a decade ago. ad

6.FUTURE RESEARCH

Majority of the tools and techniques available are not suitable for identifying anomalies in an unattended way [Miranda Lopez et al., (2016)]. The future research should aim in the creation of such tools that analyze bulk data and report possible clues including proper visualization to the forensic investigator. Some of the possibilities of promising future research work are discussed below.

Distributed Processing

As it was already discussed, the probability that the processing power and other delays during the acquisition of evidence are responsible for the large number of pending cases in the digital forensic department is high.

As in (Roussev et al., 2016) cited in [Ó Ciardhuáin, Séamus. (2004)], specifies that there are two reasons why the distributed processing is still not an important part of investigations. It is because the developers did not consider processing speeds of the tools as a priority, and the users also did not mention the importance of performance. Roussev et al., (2016) cited that with the current processing speed and scenarios, coping up with a commodity SATA HDD at 120MB/s will take 120 to 200 cores. So, the future research should head in a direction to improve the processing speeds of the core forensic functions.

HPC and Parallel Processing

As discussed above, the bottleneck scenario of the digital forensic investigation is not only caused by the processing power of tools. Since the analysis phase takes a lot of time by humans and computers, the high-performance computing techniques must be used wherever necessary to expedite the process. The HPC and parallel processing can be employed after the acquisition phase for pre-processing, storage and analysis of data [Lillis, David et al., (2016)].

Digital Forensics as a service(DFaaS)

The lack of standardized procedures in the field is what is responsible for the backlog of pending cases in this industry. The steps associated with each entity in the forensic investigation coupled with the lack of knowledge of one entity about another one, (for example the legal advisor does not fully understand the technical procedures of the investigation and vice versa) is another reason. The development of a framework has always been a solution for this issue, but each organization has come up with its own framework and this has worsened the standardization process.

DFaaS is an enlarged model that appears as an extension of the conventional model [Lillis, David et al., (2016)]. The model is a solution to take care of aspects like the acquisition, storage and analysis of information and it is an automatic process. Though DFaaS has a lot of advantages, there is a lot of room for future improvement. Though the service is cloud-based, there is another potential bottleneck situation if there is an upper bound for uploading information after the evidence is collected [Lillis, David et al., (2016)].

The future work in this DFaaS could be a process that facilitates easy retrieval of the associated unique files in the cloud, resulting in the faster acquisition phase. Also, there must be research work to reduce the non-pertinent and benign files during the acquisition of relevant data. According to Van Baar et al., (2014), improvements in the system can be in the form of indexing capabilities, increasing the functionality available to the case detectives etc.

Field programmable gate arrays

With the use of IoT devices in everyday life, it is possible to record all the information and store the data in a cloud service. Local storage of information is also possible but limited. In a crime scene, it is necessary to reconstruct the series of events by accessing the recorded information on the IoT devices. This could be aided by using visual analytic tools to reconstruct the series of physical events along with time stamping to follow the right order of the events [Lillis, David et al., (2016)].

In order to facilitate the use of devices to suit the need of the investigation, FPGA's can be used. FPGA's are like ICs that are reprogrammable to user's needs. They are more beneficial

than traditional CPUs in the digital forensic scenarios. They can achieve results in fewer logical operations than a CPU and can be integrated into IoT devices that are structurally small. Since FPGA's are increasingly used in cryptography and visual computing etc., they are demonstrating useful traits to digital forensic experts. While SSDs and other technologies are used to each the bottleneck issue of the forensics, the FPGAs can be used in the analysis phase of the forensic industry.

Cost-Benefit Analysis

In many scenarios, the investigators face challenges due to the placement of devices in a crime scene. There is a stage of confusion due to the location of the device.
In recent scenarios, as discussed under the legal challenges, the device that needs to be accessed for the investigation can be located in a difficult place to reach [Caviglione, Luca et al., (2017)]. The difficulty can be in terms of geographic location or in terms of jurisdictional borders.

The solution would be to conduct a cost-benefit analysis, to find the optimal decision. This would give a clear idea whether the device is worth accessing in spite of all the risks and costs.

Unified Meta-interface for IoT

In the near future IoT and CPS frameworks will account for most of optimization and revenue maximization of many processes, but at the same time they give way to new ad-hoc attacks. IoT devices will have several devices with controllers and pieces of monitoring equipment manufactured by different vendors [Caviglione, Luca et al., (2017)]. The devices may follow or be a part of any low-level interface even if they are connected as a single network.

Due to the interface in which a device is bound in, the forensic investigator has to sacrifice the retrieval of information from that device. Some interfaces may not allow the retrieval of information and thus a development of a unified meta-interface for IoT devices is necessary since all the IoT devices can be from different vendors and can support different interfaces. The solution is to develop a Meta-interface that should cover a large spectrum of devices and low-level interface [Caviglione, Luca et al., (2017)].

The future work should not only aim at easier ways to recover or track evidence, it should also aim at presenting the data in a visual manner that gives a holistic view of the crime, the cause and effect of it. Improved visualization techniques and ways to transport large amounts of data without any damage or alterations to it, is an area yet to be explored with potential room for improvement [Garfinkel, Simson. (2010)].

Autonomous is the key word. Since all the devices that are self-sufficient in the current day scenario, with minimal involvement or inputs required for its functioning, the forensic process must also be automated to automatically detect outliers and report the concerned department. The system must have the capacity to track the hacker, or even shut down the vulnerable systems to protect further damage.

Digital forensic experts and practitioners can survive the challenges exhibited by the new inventions and new vulnerabilities associated with them is by developing faster data acquisition and processing methods.

7.CONCLUSION

The paper aimed to predict the possible changes that the digital forensic industry can expect, as that would allow the people working in the industry to know what are the possible changes even a small technological invention can bring to the world.

The challenges discussed in the paper were collated from the possible legal and technical consequences a digital forensics team could face if the procedure is not executed in the proposed manner. Thus, the procedure was regarded as one of the most ideal and practical approach to a proper digital forensic activity. However, it was seen that the frameworks were not compatible cross platform, and even the tools and techniques required for an investigation has to be altered for ease of operation.

The most commonly used frameworks or models were compared and it was observed that over time, there were slight improvements to the models over one another. But, though the steps were expanded with the models over time, the base structure remained almost the same. But still, the models were chosen according to the compatibility with the investigation. It is now clear that, no matter what challenges exist now, in future the challenges may become more complicated due to the changes in technology. However, a procedure for the forensic process defines the guidelines and allows the different entities to interact and inter-operate with each other with minimal knowledge of a branch that is outside of their scope.

The future research work section also suggests ways to ease the inter-operability between the participants in a forensic investigation. With the introduction of IoT and other revolutionary inventions, where human interaction is rarely necessary, devices along with their integrity and security are of utmost importance. More attention must be given to the standardization of protocols, platform independent development, and increasing the research quality to make the devices completely secure.

REFERENCES:

1. Lillis, David; Becker, Brett A.; O'Sullivan, Tadhg; and Scanlon, Mark, "Current Challenges and Future Research Areas for Digital Forensic Investigation" (2016). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 6.

2. Xrysanthou, Anargyros & Apostolakis, Ioannis. (2006). Network Forensics: Problems and Solutions.

3. Ieong, Ricci. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. Digital Investigation. 3. 29-36. 10.1016/j.diin.2006.06.004.

4. Reith, Mark & Carr, Clint & Gunsch, Gregg. (2003). An Examination of Digital Forensic Models. 1.

5. Ó Ciardhuáin, Séamus. (2004). An Extended Model of Cybercrime Investigations. IJDE. 3.

6. Garfinkel, Simson. (2010). Digital forensics research: The next 10 years. DFRWS 2010 Annual Conference. 7. S64-S73.

7. Caviglione, Luca & Wendzel, Steffen & Mazurczyk, Wojciech. (2017). The Future of Digital Forensics: Challenges and the Road Ahead. IEEE Security and Privacy Magazine. 15. 10.1109/MSP.2017.4251117.

8. Miranda Lopez, Erik & Moon, Seo & Park, Jong. (2016). Scenario-Based Digital Forensics Challenges in Cloud Computing. Symmetry. 8. 107. 10.3390/sym8100107.

9. Casey, E. (2000) Digital Evidence and Computer Crime. San Diego: Academic Press

10. Lee, H.C., Palmbach, T.M ., & Miller, M.T. (2001), Henry Lee's Crime Scene Handbook. San Diego : Academic Press