ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

ANALYSIS OF WHETHER DIGITAL EVIDENCE CAN BE RELIED UPON IN LEGAL PROCEDURES, AND DETERMINATION OF THE IDEAL DF MODEL

Arhan Kamdar Pande
Prabhavati Padmashi Soni International Junior College
953@ppsijc.com

Abstract

The broad objectives of this research paper are to review the efficiency of existing Digital Forensics modelsin identification and collection of digital evidence, whilst analyzing whether the discoverable information on digital media is suitable for use in court. Research has been conducted using a mixed approach: both an experimental and a theoretical one. The theoretical sector of the paper is focused on determining the most well suited DF model. The experiment aims to investigate the ease of fabrication of digital evidences and whether individuals can tell apart a genuine evidence from a fake one. Since the results indicate that most people cannot identify fake evidences, it is deemed that the reliability of digital evidence is, currently, low. Further analysis is carried out to arrive at the major conclusion that using the IDIP model increases the reliability of digital evidence in court.

Keywords:*Digital Forensics, Cybercrime, Digital Evidence, DF Models, Investigation*

Introduction

With the advent of social media and the advancements in technology in recent times, the number of people who are active online has increased exponentially. Whilst the technology and the services on the Internet (such as email, chatrooms, social media sites and streaming platforms) can be put to efficient and positive use in numerous ways, it can very well provide a facade for those with malicious intent, and by doing so, increase their temptation to harass other people within the digital space. This unfortunate yet clearly evident rise in cybercrime levels has led to the popularisation of a new field in criminal investigations : Digital Forensics.

Digital Forensics is popularly defined as the process of preserving, identifying, extracting and documentingdigital evidence which can be used by the court of law [2].The importance of Digital evidence in criminal cases of today's world is severely undermined. According to Randy Hillman, Director of the DA association and Office Of Prosecution Services, Digital Evidence is prevalent in 90% of their cases, while DNA analysis is in a very small percentage of them [7]. Considering the previous statistic, it is irrefutably crucial for Digital Forensic investigations to yield accurate and reliable digital evidence. While criminal investigators have been using

Forensics since the past numerous decades, Digital Forensics is a new introduction to the investigation process and is still being developed to be used to its whole potential. Given that, it is undeniable that a DF investigator may face a considerable amount of challenges while collecting and presenting digital evidences. The vulnerability of digital evidence to sheer fabrication and manipulation leads to professional investigators not being able to solely consider what they have discovered online (or on other digital media) as proof to base their conclusion on. This is further supported by Hewling and Sant [1]with a quotation in their paper in the same field –"Digital evidence can be reproduced and manipulated by personnel involved with the investigation, maliciously or accidentally".Physical evidence is widely considered to be "primary" evidence, and rightly so- due to its higher accuracy. This point can be very well summarized with a statement by David Chaikin [3]-"Digital objects bear less evidence of authorship, provenance, originality and other commonly accepted attributes than do analogue objects".

Various digital forensic models have been developed and implemented by firms and law-enforcement personnel. The sole fact that this large a number of models exist and that there is no standardized process followed in digital forensic investigation goes to show, according to Hewling and Stan[1], that "there are some inconsistencies in the field". These models will be discussed in greater detail later in the paper.

This paper will analyze the reliability of making use of digital evidence in favor of or against an individual accused of a cybercrime. It will provide a balanced and evaluated view on the subject by considering the accuracy and legitimacy of the digital evidence obtained by digital forensics. The paper will also focus on the evaluation of the numerous existing DF models. It will aim to identify the prime DF model to collect relevant evidence.

Existing Digital Forensics Models (Theorotical)

Over the years, numerous authors have put forward their own optimized DF model, to be potentially used by professional investigators in the acquisition and analysis of digital evidence. The work of various individuals/organizations in this field with their invented framework is thoroughly discussed in this section.In this section, the focus will mainly be on the explanations of the working and functioning of each of the models. A comparison of these models will be included in the *Discussionand conclusion*section of this paper.

(I) Kruse and Heiser Model

This model was put forward by Kruse et al in their book titled "Computer Forensics: Indicent Response Essentials", published in 2001. The model was designed to be relatively simple use and understand, with a total of a merethree steps that needed to be followed:

Step 1 – Acquisition of the evidence.

According to Dr. Sudesh Rani [8], it was essential for this evidence to be acquired "without alteration or damage to the original evidence". This is important because any accidental or intentional tampering of the original data would lead to the collected evidence not being considered genuine, *potentially* changing the outcome of the case altogether.

Step 2 – Authentication of the collected evidence by comparing it to the data originally obtained.

After the collection of digital evidence, professionals compare it to the data it was collected from, to check its consistency and (to some extent) its reliability.

Step 3 – Analysis of the data

Once the digital evidence is confirmed to be authentic and consistent with the original "mother" data, It is handed over to DF investigators for thorough analysis. This is arguably the most important step of the three, for what majorly matters from a practical point of view is the magnitude of advancement

further in the case yielded by the DF process. And this advancement indefinitely requires an efficient analysis and evaluation of the secured evidence.

Because the three stages of the Kruse and Heiser Model are "Acquisition", "Authentication" and "Analysis", it is popularly recognized as the "3As".

This model is briefed with**Fig.1** below:

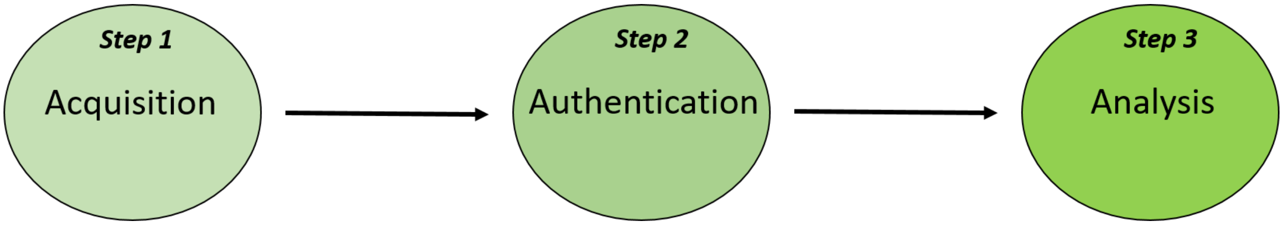


Fig.1 The three stages of the Kruse and Heiser Model for DF.

(II) USDOJ (US Department Of Justice) Model

The USDOJ Model in DF follows four key stages :

Step 1 –Collection of the evidence

The collection phase involves searching for relevant data, identifying if it is applicable to the case, and then collecting this evidence. It is important for the individual carrying out this step to document every step taken in the process [9], so that it can be referred to in the future by other personnel working on the case.

Step 2 **-**Examination

The second stage deals with using methods such as advanced data mining in order to uncover and reveal other meaningful evidences of hidden and "obscure" nature [9]. This would include the information that is not explicitly available or visible, but canbe extracted by a professional. The importance of the examination step is large to say the least, because the "hidden" data often proves to be the most useful type, when it comes to making advancements in the case.

Step 3-Analysis

Prior to the thorough examination of the collected digital evidence, it must be analyzed. The analysis stage deals with interpreting the data in relation to the questions under investigation to reach a convincing solution. It is at this stage when investigators really begin to link the examined evidence with the actual case. Again, like with the collection stage, every step taken in the Analysis stage is compulsorily documented.

Step 4 – Report

For the evidence to have any effect on any kind of legal procedure, it must be presented before the court of law. In step 4, the examined and analyzed evidence is presented in form of a report, to ensure its usability in court. The report will document the whole process, from the first stage.

The USDOJ Model for DF is graphically summarized in **Fig.2**below:

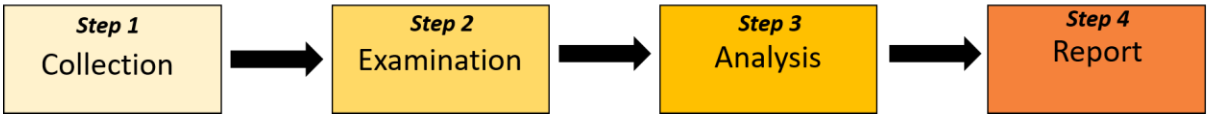


Fig.2 The four key stages of the USDOJ Model

(III)Integrated Digital Investigation Process (IDIP)

In 2003, Carrier and Spaford designed a Digital Forensics model that considers the "dual investigative nature" (as worded by Dr. Sudesh Rani [8]) of the DF process. This model was known as the "Integrated Digital Investigation Process".Both, the physical as well as digital aspects of a hypothetical case have been incorporated into this model. The model is divided into five different groups of phases (stages), with 17 phases in total between them:

Group 1 -Readiness phases

This group of phasesis aimed towards ensuring that the professional team is able to fully support the investigation. The two phases under Group 1 are *operations readiness* and *infrastructure readiness*. The operation readiness phase has an objective of providing adequate training and equipment for the investigators. The infrastructure readiness phase focuses majorly on confirming that data relevant to the case exists.

Group 2 – Deployment phases

Prior to the Readiness phases, the Deployment phases are carried out. In the deployment phases, a set of fixed mechanisms is used in order to detect and confirm an incident. Group 2 consists of the *Detection & Notification*, *Confirmation* and *Authorization* phases, which are carried out in the same order.

Group 3 – Physical Crime Scene Investigation phases

As mentioned before in the paper, IDIP considers both, the physical as well as the digital perspective of a given investigation. Group 3 aims to, as its name suggests explicitly, collect and analyze physical evidence relevant to the case. Group 3 consists of the following phases:

Preservation of physical scene, Survey for Physical Evidence, Document Evidence and Scene, Search for Physical Evidence, Physical crime scene reconstruction, and Presentation of complete theory

Group 4 – Digital Crime Scene Investigation phases:

In this group, every digital device may be considered as a separate "crime scene". The main purpose of this group of phasesis to ensure the collection of maximum electronic (or "digital") evidence. Group 4 consists of phases "identical" to Group 3, but in context of digital forensics rather than its physical counterpart:

Preservation of Digital scene, Survey for Digital Evidence, Document Evidence and Scene, Search for Digital Evidence, Digital crime scene reconstruction, and Presentation of complete theory.

Refer to **Fig.3** and **Fig.4** for the working sequence of the respective phases in Group 3 and Group 4.

Group 5 – Review

The final group is Review, in which the entirety of the process is reviewed to finds points of potential improvement, while identifying new procedures or new training requirements. Despite the fact that there are no seperate phases within this group, the importance of reviewing one's work is undeniable (it is the only way the model can be made more optimum and foolproof, as time progresses.)

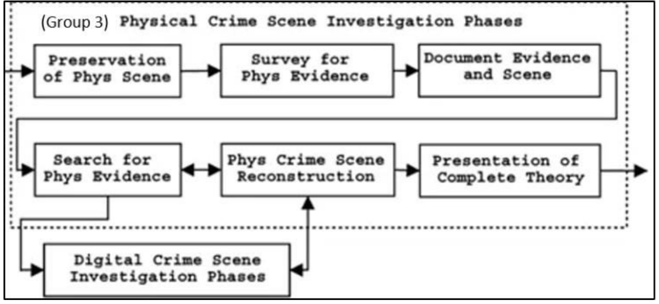

(Group 3) Physical Crime Scene Investigation Phases
Preservation of Phys Scene
Survey for Phys Evidence
Document Evidence and Scene
Search for Phys Evidence
Phys Crime Scene Reconstruction
Presentation of Complete Theory
Digital Crime Scene Investigation Phases

Fig.3 Phases and their order in Group 3

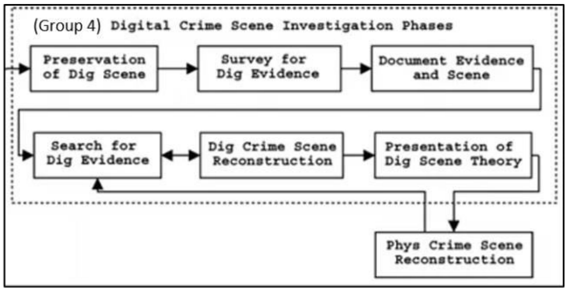

(Group 4) Digital Crime Scene Investigation Phases
Preservation of Dig Scene
Survey for Dig Evidence
Document Evidence and Scene
Search for Dig Evidence
Dig Crime Scene Reconstruction
Presentation of Dig Scene Theory
Phys Crime Scene Reconstruction

Fig.4 Phases and their order in Group 4

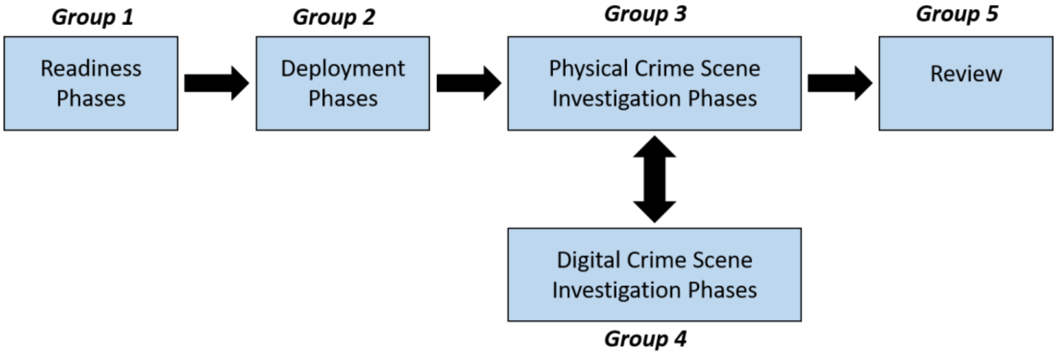

Group 1
Group 2
Group 3
Group 5
Readiness Phases
Deployment Phases
Physical Crime Scene Investigation Phases
Review
Digital Crime Scene Investigation Phases
Group 4

Fig.5 Summary of IDIP model structure (without inclusion of phases in individual groups)

Experimental

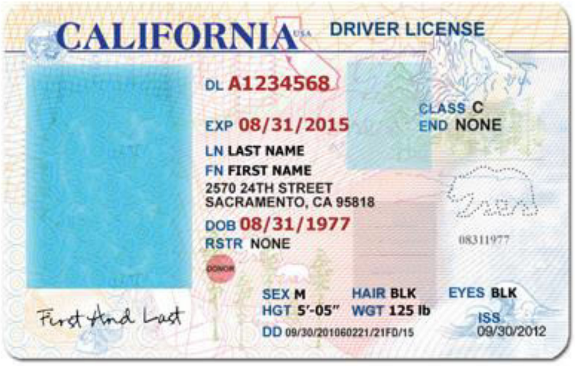
In this paper, a single experiment was conducted with an aim to identify how difficult it is for one to fabricate evidence, and to analyze whether people can differentiate between fake and genuine digital evidence.

Procedure-

In the first stage of the experiment, three evidences were fabricated using different applications and platforms. Along with these, three genuine evidences were obtained from the internet. In the second stage of the experiment, an online survey was conducted, in which people were asked to identify the fake and real evidences from a list of evidences that contained both.The purpose of the second stage was to analyze how accurate the faked evidence can be portrayed to be.

Stage 1 of experiment–In stage 1, a driver's license, a tweet and a chat were fabricated.

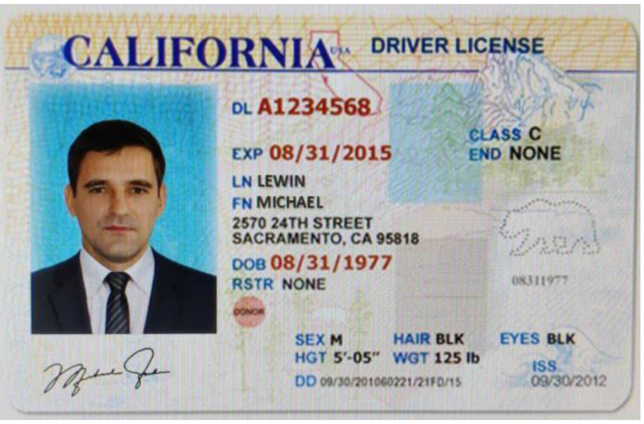
(i) Driver's License: In order to create a driver's license that seemed genuine, a free template was downloaded from the web. **Fig.6**below is the template that was used.



CALIFORNIA USA DRIVER LICENSE
DL A1234568
EXP 08/31/2015
CLASS C
END NONE
LN LAST NAME
FN FIRST NAME
2570 24TH STREET
SACRAMENTO, CA 95818
DOB 08/31/1977
RSTR NONE
DONOR
08311977
First And Last
SEX M HAIR BLK EYES BLK
HGT 5'-05" WGT 125 lb
DD 09/30/201060221/21FD/15
ISS 09/30/2012

Fig.6 Driver's License Template

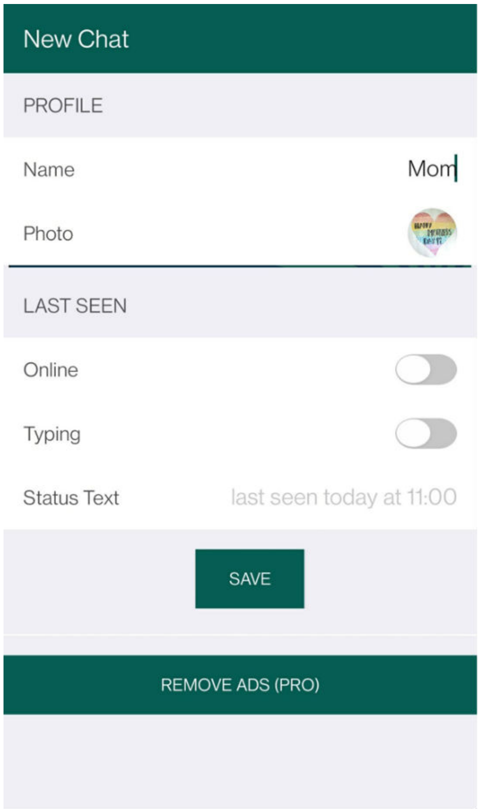
A shutterstock image of an individual (Fig.7) was obtained from the internet and edited along with the License template to create the final fake license. The standard version of *Microsoft Powerpoint 2007* was used for all editing purposes. To make the license seem as genuine as possible, a signature (also found online) was included in the finished license.



CALIFORNIA USA DRIVER LICENSE
DL A1234568
EXP 08/31/2015
CLASS C
END NONE
LN LEWIN
FN MICHAEL
2570 24TH STREET
SACRAMENTO, CA 95818
DOB 08/31/1977
RSTR NONE
DONOR
08311977
SEX M HAIR BLK EYES BLK
HGT 5'-05" WGT 125 lb
DD 09/30/201060221/21FD/15
ISS 09/30/2012

Fig.7 Shutterstock photo **Fig.8**Finished License

(ii) Fake Chat: To create a fabricated WhatsApp chat, a free mobile application with the name of "Whatsmessage" was made use of. The application allows the user to create what can be best described as a "simulation" of a chat. The user can alter all aspects of the chat – such as the time the message was sent, the profile picture of the recipient, or the background of the chat.It should be noted that the chat that was created is naturally not something controversial or one that would be used in real cases, but a person with malicious intent could definitely use this technology to fabricate something of a more grave nature, which could be of actual relevance to a hypothetical case.**Fig.9**shows the interface of the app that enables the user to create a new chat. **Fig.10** is the final chat that was created. (Figures on the next page)



New Chat

PROFILE

Name: Mom

Photo

LAST SEEN

Online

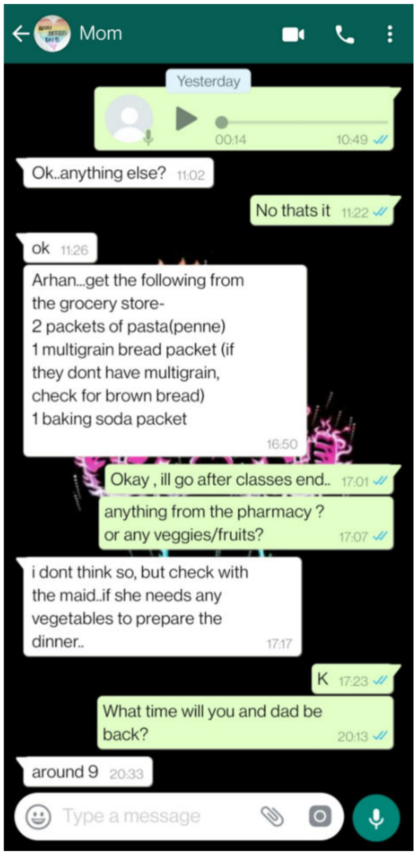
Typing

Status Text: last seen today at 11:00

SAVE

REMOVE ADS (PRO)

Fig.9 App Interface



Mom

Yesterday

00:14 10:49

Ok..anything else? 11:02

No thats it 11:22

ok 11:26

Arhan...get the following from the grocery store-
2 packets of pasta(penne)
1 multigrain bread packet (if they dont have multigrain, check for brown bread)
1 baking soda packet 16:50

Okay , ill go after classes end.. 17:01

anything from the pharmacy ? or any veggies/fruits? 17:07

i dont think so, but check with the maid..if she needs any vegetables to prepare the dinner.. 17:17

K 17:23

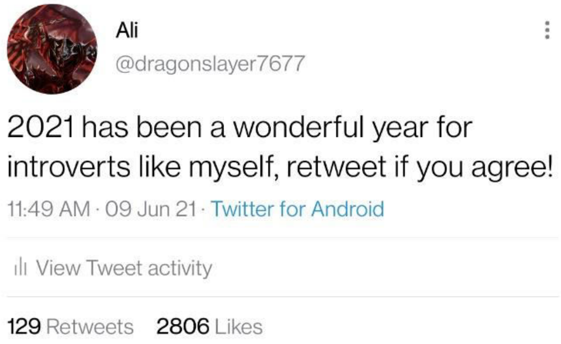
What time will you and dad be back? 20:13

around 9 20:33

Fig.10 Final chat

(iii) Fake tweet: With the rise of social media, it becomes increasingly crucial for one to be aware of their statements and/or opinions that they put out on the web. The website “Twitter” is known to allow individuals to freely voice their opinions. The posts that a person makes on the platform are known as “tweets”. The app “tweet creator” was used in order to fabricate the tweets. While in this case a simplistic tweet was created, this service could easily be put to unethical use. For instance- a person could fabricate offensive tweets under someone else’s name, to defame them. Even if the victim defends themselves by proving the absence of this particular tweet in their feed, It is easy for the accuser to claim that the victim simply deleted the post. Such a scenario is an example of how digital evidence, if inaccurate, could steer the case towards the wrong direction.

Fig.11 below shows the tweet that was created



Ali
@dragonslayer7677

2021 has been a wonderful year for introverts like myself, retweet if you agree!

11:49 AM · 09 Jun 21 · Twitter for Android

View Tweet activity

129 Retweets 2806 Likes

Fig.11 Fabricated tweet

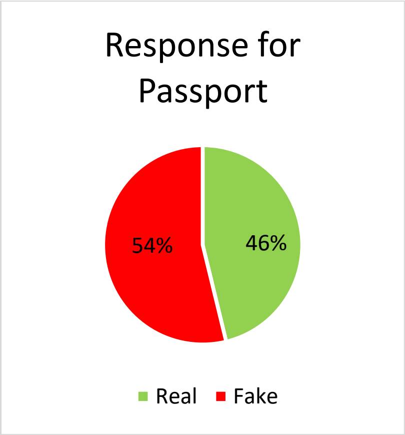
Stage 2 of the experiment– Survey

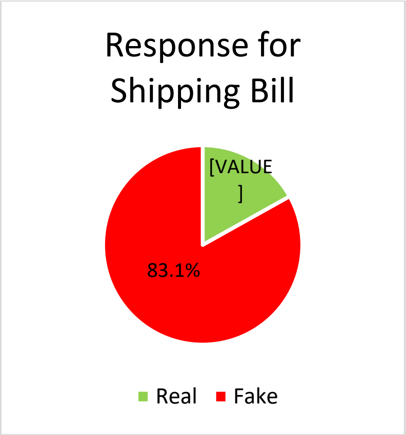
The purpose of conducting the survey was to answer the question- "How genuine can the fabricated evidence be made to look?". For the survey, three genuine evidences were downloaded from the internet. They consisted of a digital certificate, a shipping bill and a passport. Putting the three fake and three real evidences together, a total of six evidences were obtained. In the survey, which was conducted via Google Docs, subjects were asked to identify whether each of the six evidences was genuine or not.

Results of the Survey

A total of 78 people took part in the survey. No personal information was asked for in the survey, because it wasn't relevant to the research.

Results for genuine evidences- 53.8% of people incorrectly guessed the real passport to be faked, 83.1% of people incorrectly guessed the real shipping bill to be fake, and 51.3% of people incorrectly guessed the real digital certificate to be fake. These results are graphically presented in Figures 12 to 14 (next page):





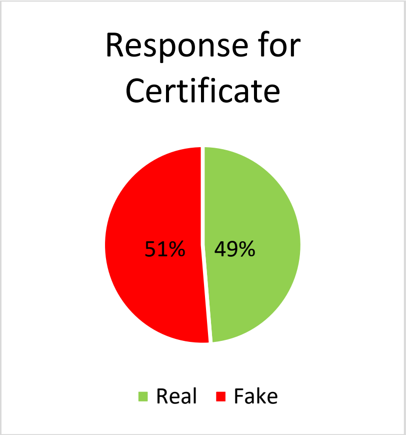
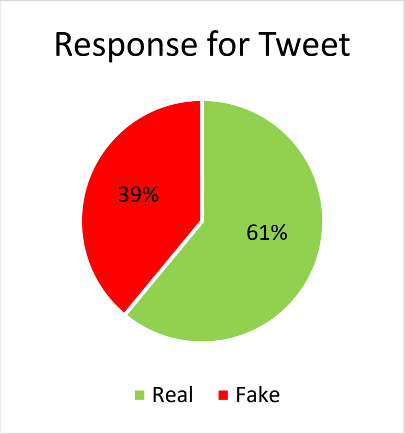
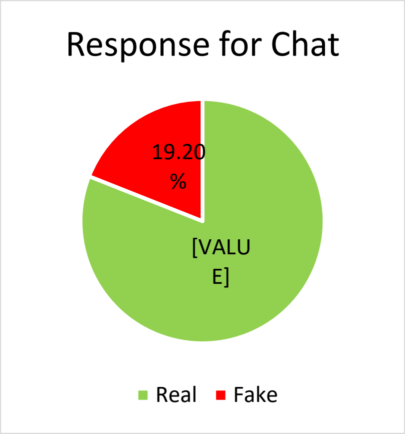


Fig.12 Response for Passport **Fig.13** Response for Bill **Fig.14** Response for Certificate





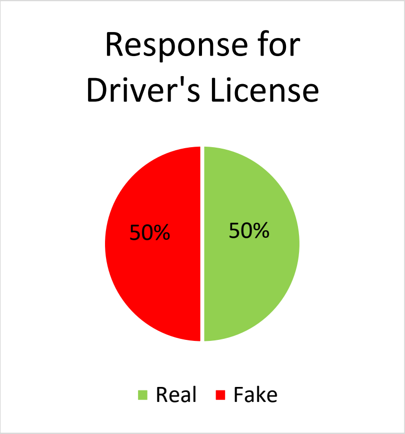


Fig.15 Response for Tweet **Fig.16** Response for Chat **Fig.16** Response for LicenDiscussion and Conclusion

Results for fabricated evidences- 39% of people correctly guessed that the tweet was fake, 19.2% of people correctly guessed that the chat was fake, and 50% of people correctly guessed that the license was fake. These results are displayed graphically in figures 15 to 17 below.
The discussion sector will be divided into two sections: The interpretation of the experimental results, and the discussion of the theoretical aspect to this paper.

Section I – Experimental results
It is found that only 36.07% of all people were able to successfully guess that the fabricated evidences were, indeed, fake. Also, according to the results of the survey, 62.73%of individuals incorrectly guessed the genuine evidences to be fake. The latter statistic was especially alarming, because it wasn't expected that the real evidences would be voted to be fake more frequently than the fabricated evidences themselves. A fairly unbiased sample of subjects was taken in this survey, so it is safe to say that the majority of people are unable to differentiate between genuine and fabricated evidences.

All the fake evidences were fabricated by the use of basic and free software, and without the help of an expert. If data can be made to seem so genuine with such ease, it is a definite area of concern for cyber-crime authorities. If such evidence could be created using basic software and little equipment, one fabricated by someone with superior editing skills and/or more advanced equipment could potentially pass through the authorities undetected as a fake. One might argue that the DF authorities could hire ethical hackers to hack into the fabricator's system, but it is easier said than done. With facilities that allow offenders to hide their IP address and browse the internet without leaving any footprints whatsoever, a hacker's job has become more difficult than ever. The advancement of technology has skyrocketed to say the least, and it favors the offenders much more than it does the legal authorities. It can, hence, be concluded that the reliability of digital evidence in court is fairly low, and it is best if digital evidence is used as more of a supporting material than a key factor in deciding the outcome of the case.

To increase the reliability of the digital evidence, it is vital for it to somehow be linked to a more solid physical evidence (more about this in Section II).

Section II – DF Models

Three models were discussed previously in the theoretical section of the paper– The Kruse and Heiser Model, USDOJ Model and the IDIP Model.

The major advantage of using the Krus and Heiser model is that it is easier, less time consuming and cheaper to implement than the other two models. However, the efficiency of the authentication process can be questioned, because it involves only "checking whether the recovered evidence is consistent with the data originally seized" [8]. In technical terms, this is a verification process (i.e, checking whether the data stored in two different locations are consistent with one another) rather than the equally essential validation process, which involves determining whether the data is factually correct. In other words, If the data from which the evidence had been collected was fabricated or tampered with in the first place, there is no way to identify the same.

The advantage of the USDOJ model over Krus and Heiser model is that it has the "Examination" step in the process, which involves digging deep into the evidence and attempting to find implicit details. Also, USDOJ accommodates a stage (Report) which involves presentation of the results before the court of law. This was absent in the Kruse and Heiser model. However, USDOJ does not attempt to correlate the digital evidence with physical evidence of any kind. As mentioned in Section I of the discussion, it is vital for the digital evidence to be interpreted in relevance of some physical evidence, for it to be of greater reliability. This aspect is present in none of the two models discussed above.

The third model, IDIP, does take the physical evidence into consideration. Linking the Physical Evidence with the Digital Evidence provides a stronger link between two possibly related scenario and proves to be more helpful in the court of law. Even though it is undoubtedly the most time consuming and expensive (due to equipment and training costs) to implement of the three, Government-funded investigative authorities already equipped with fairly advanced technology can comfortably afford to make use of this model. Keeping in mind also the fact that relating digital and physical evidences will be key to improving the reliability of the digital proof, it is conclusive that IDIP is the most optimum model to use in modern day DF investigations.

References

[1] Moniphia Hewling, Paul Sant "Digital Forensics: An integrated approach" presented at CFET, Canterbury, United Kingdom , September 20th 2012.

[2]EC-Council "How Well Do You Know Digital Forensics"eccouncil.org. https://www.eccouncil.org/what-is-digital-forensics/ (accessed May 26 2021)

[3] David Chaikin , "Network Investigations of Cyber Attacks : The Limits of Digital Evidence" in *Crime, Law and Social Change*5th ed. FL , USA , Springer.

[4] Xiaoyu Du , Nhien-An Le-Khac , Mark Scanlon " Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service" presented at ECCWS 2017 , Dublin , Ireland

[5] Dan Manson, Anna Carlin, Steve Ramos, Alain Gyger, Matthew Kaufman, Jeremy Treichelt "Is the Open Way a Better Way? Digital Forensics using Open Source Tools" presented at the 40th Hawaii International Conference on System Sciences – 2007, Pomona, California, USA

[6] Khuram Mushtaque , Kamran Ahsan , Ahmer Umer "Digital Forensic Investigation Models : An Evolution Study" (Not Presented), August 2015, Karachi, Pakistan

[7] Andrew J. Yawn "In crime investigations, digital evidence 'outweighs' DNA" montogomeryadvertiser.com
https://www.montgomeryadvertiser.com/story/news/2015/09/30/digital-evidence-outweighs-dna/73082266/

[8] Dr. Sudesh Rani "Digital Forensic Models: A comparative analysis" published in "International Journal of Management, IT & Engineering" Vol.8 Issue 6, June 2018.

[9] Michael Kohn, J.H.P Eloff, MS Olivier "UML Modelling Of Digital Forensic Process Models (DFPMs)" (Presentation details not available), University of Pretoria, South Africa.