International Journal of Engineering Innovation & Research
Volume 4, Issue 6, ISSN: 2277 – 5668

Digital Forensics in Kingdom of Saudi Arabia

Dr. Abdullah Aljumah
Email: aljumah88@hotmail.com

Dr. Mohammad GulamAhamad
Email: mg.ahmad@psau.edu.sa

Mohammed Yousuf Uddin
Email: m.yousuf@psau.edu.sa

***Abstract* – Digital forensics is growing field of technology which encompasses various fields such as computer forensics, network forensics, and cloud forensics. In the present investigation a brief survey of the global scenario and in particular status of digital forensics in Kingdom of Saudi Arabia (KSA) were outlined. No significant work is carried out in KSA in academics, research and development of digital forensics. King Fahad Security College is offering a diploma course and Naif Arab University of security science offering Master's Program in network security. A brief account of Information Communication Technology report of 2014 has been discussed. It is observed that the population of the kingdom using smart phones and other digital devices at a very proportion. Therefore it is observed that a defined way of forensic framework is yet to be setup to curb the illegal activities and help law enforcement agencies.**

***Keywords* – Digital Forensics, Digital Evidence, E-Discovery, Anti-Cybercrime Law.**

I. INTRODUCTION

With the advent of internet the illegal hacking of bank account credit card fraud and theft of computer files data, and many more crime waves leading to e-frauds is order of the day. To combat this, an endeavor is made in the form of digital forensics to knock door of law enforcing institutions. Digital forensics is the science of identifying, colleting, preserving, documenting, examining, analyzing, and presenting evidence from computers, networks, and other electronic devices [1]. The evidence is mainly called digital investigation or computer investigation or electronic investigation of technical truth meant for the civil, criminal and corporate proceedings in the form of legal acceptance of virtual truth. The electronic forensics is well applied to detect rapture of copy rights and intellectual rights, fraud detection and law enforcement agencies.

The forensics can be broadly categorized as two disciplines as digital forensics and cyber forensics. The former further categorized into audio and video devices. The audio devices include iPod voice recognize devices, MP3 devices and audio surveillance devices. The latter includes the video surveillance devices digital cameras, scanners, facsimile devices plotters and photo copiers. The third category may include the combination of both audio and video devices such as CDs, DVDs, USB drives cell phones, iPhones and Blackberry and other communication devices

The process of Digital investigation is playing a vital role in combating crime in different arenas. Digital forensics investigation is now a more matured professional and academic discipline. Many universities and institution offer specialized training and courses in the field of digital forensics investigation. The rapid evolution of digital technologies like smartphones, tablet computers, laptops and smart watches etc., are compelled us towards digital forensic development. These advancements lead to establishment of the digital forensics investigation as special branch in crime investigation. Digital evidence is playing a significant role in not only crimes committed in information communication technologies settings, but also crimes committed on the ground where digital objects are partially involved, and this leads to the involvement of digital evidence in court proceedings, and proved to be effective in solving the mysterious criminal cases around the world. Thus digital forensics investigation is required in cases where crime is committed using digital objects in digital world and also where crime committed on the ground where digital objects are partial involved. There exist challenges with digital evidences as they can be reproduced and manipulated intentionally or by accident. To overcome these challenges and appreciate its contribution many research centers and security institutions have developed digital forensics as more matured and developed sector. Since the year 2005, digital forensic has achieved significant development. The US courts have adopted the digital evidence as part of proceedings and this new evidence is termed as electronic discovery (e-discovery). The Computer Analysis and Response Team (CART) of FBI has contributed significantly in crime investigation [15].The CART has nearly 500 highly trained certified digital forensics agents. The statistics shows that during fiscal year 2012 CART supported nearly 10400 investigations, and conducted more than 13300 digital forensic examinations involving 10500 terabytes of data (https://www.fbi.gov). Thus the Digital Forensics is vital tool in combating crimes and at the same time it faces challenges which are introduced because of changes in Information and communication technology. The storage devices are continuously increasing in size and, solid state drives and file format with more complexity became difficult for analysis [2]. In the cloud computing platforms where data is split into elements recovery process has become even more difficult. The cell phones and other mobile computing platforms are big challenge for forensic examiner, as cell phones models are in thousands and have become important tool for criminals. Lastly a variety of legal challenges makes the computer forensics more complicated, time consuming, and expensive. When it comes to research and development, many universities are funding digital forensic research and several journals and conferences exist, despite these challenges. There are relatively few cases of academic research being delivered as end-user products. There is need for new detection algorithms, tools and techniques to work in real world data-rich environment. [10].

The Digital Forensics enable us to look in to past and uncover hidden data in computer and other electronic media, Many criminal cases were solved and the real criminals are proven guilty. On October 17, 2000 year, Mr. John Diamond had shot and killed the air force captain Mr. Marty Theer, and his wife was implicated in crime and her computer with 88000 emails and instant messages was the only evidence. Mr. Dennis Rader the serial killer was caught and proved as guilty after 30 years with evidence from floppy disk. During the year 2002 Mr. Scott Tyree had kidnapped and imprisoned a 13 year old girl. He was caught by FBI with the help of instant message sent by him to another man [5].

II. Current Structure of Digital Forensics in Kingdom of Saudi Arabia

There is no significant research done to understand the importance of digital forensics infrastructure in Saudi Arabia. There are no specially designed law enforcement procedures or guidelines which governs the digital forensics investigation.

There exists only one anti-cyber Crime law of Royal Decree No M/17 8 Rabi 1 1428 / 26 March 2007 First Edition 2009 [7].It deals with crimes committed on computers and other digital devices, As per this law any type of unlawful access and unauthorized interception of data, hacking of websites and defamation using information technology will be punishable for not more than one year with fine of hundred thousand riyals [7]. Crimes with more severity, like banking fraud, stealing of credit card details are subject to higher penalties. Bureau of Investigation and public prosecution carry out investigation and the communication and information technology commission will provide the technical support. The E-Transaction Act with Royal Decree No M/8 deals with electronic transactions and signatures and provides the guidelines for acceptability of any document or information stored in electronic form, where accuracy and integrity of information should be preserved, information should be accessible for future, original source, author and time stamps of the documents should be available. If above criteria is fulfilled these information and documents shall be admissible as evidence [8]. Law of criminal procedure Royal Decree No M/39 describes the procedure of collection of information and evidence necessary for investigation and it should be done by criminal investigation officer and other personal having powers of criminal investigation[9]. With above analysis we understood that there are no specific guidelines for digital evidence and digital forensic investigations.

2.1 Academics and Research

The study of Digital forensics, as it applies to digital evidence recovery, forensic laboratory analysis, and legal and ethical issues regarding seizure of computer evidence will have to be explored in-depth. Computer network security, protocols, and intrusions detection will have to be provided to the students with skills required to protect against threats and vulnerabilities. A hands-on approach will be used to reinforce the concepts of the subject.

The King Fahad Security College established its first digital forensics investigation lab and offering a diploma course in Digital forensics investigation (www.kfsc.edu.sa). The college of computer and information security Naif Arab University of security sciences offers a Master's Degree in Computer Security and Master's Degree in Network Security. And very few research articles have been published in the area of digital forensics investigation in Saudi Arabia. It is far behind the current requirements(http://www.nauss.edu.sa)

2.2 Current Structure of Digital forensics Infrastructure around the Globe

The developed nations which have concrete and well established digital forensics infrastructure suchas United States of America had started its Computer Forensics departments in 1990s.The Computer Analysis and Response Team CART, and Scientific Working Group Digital Evidence (SWGDE) to develop the standards for forensic science in USA. The National Institution of Standards Technology (NIST) established standards for forensic science by forming Overseas Security Advisory Committee (OSAC) which is part of an initiative by NIST and the Department of Justice to strengthen forensic science in the United States. The OSAC has formed a digital multimedia scientific area committee (DMSAC).Under this committee there are sub committees like digital evidence subcommittee [12]. International Organization on Computer Evidence (IOCE) is formed to develop principles upon which standards would be built. The IOCE worked with American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) to accredit digital evidence laboratories. Till the year 2013 it has accredited 73 digital evidence laboratories. Many of the universities started offering undergraduate and post graduate programs in digital forensics and cyber forensics, such as Boston University, University of Maryland, Marshall University and California State University and many others. Some of these Universities offer e-learning programs. Digital Forensics Science programs were accredited by Technical Working Group on education digital evidence (TWGE-DE) and American Academy of Forensic Science then formed forensic science education program Accreditation Commission (FEPAC) in 2004. The FEPAC has accredited Marshall University's Master in Forensics Science Concentration Digital Evidence program [14]. Further the Department of Defense formed Center of Digital Forensics Academic Excellence (CDFAE)

2.3 The Digital Forensic Tools

The DF tools are ready made third party soft wares available in the commercial market which are used for digital forensic synthesis and analysis:

Forensic tool kit (FTK): This tool kit is meant for detailed computer forensic examination and popular in corporate world as e-mail analysis tool. It has other facilities as password dictionary creation, book marking and report generation.

Encase tool kit: Guidance software Encase forensic tool kit is popular tool kit. It has specific functionalities such as acquisition, automation tools, analysis features, viewers, searching, reporting bookmarking, email and internet investigation.

Sleuth kit: This is invented by Brain carrier, which is UNIX based free command line file system with media management.

Autopsy: It is open source tool kit. The software is developed by perl. It is HTML based GUI browser for Sleuth kit. Running this software is simple.

FIT4D (Forensic Investigation Toolkit 4 Developing countries): This is an extension to Sleuth kit. This is low cost software meant for developing countries. This tool kit operated on virtual private networks (VPN).

III. Current ICT Infrastructure in Kingdom of Saudi Arabia

The Kingdom of Saudi Arabia is one of the most tech savvy nations. The population of the county had adopted the new technologies especially in the information and communication sector instantly. The Government departments are offering its e-services with more efficiency and reliability. The usage of e devices has dramatically risen in the kingdom. Saudi is ranked 36th out of 193 nations in United Nations E-government survey 2014, Saudi has shown growing trend It was 41st rank in 2012 survey and jumped 5 ranks up. The Saudi ranked as 3rd in Gulf Cooperation Council. The Saudi is among top 20 countries listed for online service delivery [4].

The Technology Indicator of 2014 reported that the steep enhancement of mobile subscriptions. There are 51 million mobile subscriptions, 169.3 percent of penetration. Table 1 indicates the ICT status of Saudi Arabia as per CICT report of 2014[6].

Table 1: ICT Report 2014

Service	Number of Users	Penetration
Mobile Subscriptions	51 million	169.3%
Fixed Broadband	3.18 millions	48.4%
Mobile Broadband	20.7 millions	68%
Internet	18.3 millions	60%
Smartphone users	24 million	72.8%

The Ministry of Communication and Information Technology estimates $37 million spending in ICT sector in year 2015, with local and regional bodies moving towards smart city strategies, and hybrid cloud models would gain the market. It is expected that there will be a huge increase in Smartphone users and 28% increase in 4GLTE (Fourth Generation Long Term Evolution) devices [11].

Global web index indicated that 91%of users of internet in Kingdom of Saudi Arabia are between age group of 16 to 64 years. Thus it is very clear how widespread is the use of technology among all age groups. Internet is accessed through many devices and a report from Ministry of communication and Information Technology indicated in table 2 [11].

Table 2: Internet User's devices ownership.

Type of Device	Internet Access
PC / Laptop	91%
Smart Phone	80%
Tablet	47%
Game Console	37%
Smart TV	34%
Smart Watch	9%
Smart Wristband	7%
None of the above	2%

The Communication and Information Technology Commission report 2015 shows the ICT spending in Saudi Arabia. The ICT sector of Saudi has grown significantly in past 10 years. In year 2012, the ICT spending was 94 billion SAR and in year 2013, it grown to 102 billion SAR, recording 14% growth and it is expected Compound Annual Growth Rate will be approximately 8.1% and by year 2017 ITC and spending may reach 138 billion SAR. The Key technology markets and their contribution to ICT spending for 2012 are given in table 3[2]

Table 3: ICT spending for year 2012.

Technology Market	Contribution	Estimated CAGR
Telecommunication	64.9%	5.8
ICT Hardware	23.1%	9.4%
IT Services	8.4%	16.2%
Packaged Software	3.6%	15.1%

IV. Conclusion

After analyzing the facts and figures of technological advancements done by Saudi it is evident that Digital Forensic needs an urgent push, more research and development should be initiated and legal system of sharia law of Saudi should address the challenges and more advanced laboratories should be established and graduates should be encouraged to pursue digital forensics as the specialization in higher studies.

Acknowledgment

This work has been carried out under the project titled "Digital Forensics in Kingdom of Saudi Arabia" sponsored by deanship of scientific research Prince Sattam bin Abdulaziz University Saudi Arabia.

References

[1] Anthony Lang, Masooda Bashir, Roy Campbell and LizanneDeStefanoDeveloping a new digital forensics curriculum. TheJournal of Digital Investigation Volume 11 2014

[2] Li Zhang, Shen-gang Hao, Jun Zheng, Uu-an-Tan,Quan-xin Zhang and Yuan-zhang Li Descrambling data on solid-state disks by reverse engineering the firmware. The Journal of Digital Investigation Volume 12. 2015

[3] Communication and Information Commission Saudi Arabia (2015) ICT Report Mobility in Saudi Arabia. Retrieved from www.citc.gov.sa
[4] United Nations e-government survey. Available: www.unpan.org/e-government2014
[5] Simson L.Garfinkel. American Scientist, Volume 101. 2013
[6] Communication and Information Commission Saudi Arabia ICT Indicators Report Q2 Available: www.citc.gov.sa. 2014
[7] Communication and Information Commission Saudi Arabia Anti-Cyber Crime Law Royal Decree No. M/17. Available: www.citc.gov.sa 2009
[8] Communication and Information Commission Saudi Arabia (2007) Electronic Transactions Law Royal Decree No. M/8. Available: www.citc.gov.sa.
[9] Communication and Information Commission Saudi Arabia Law of Criminal Procedure Royal Decree No. M/39. Available: www.citc.gov.sa. 2001
[10] Simson L.Garfinkel Digital forensics research: The next 10 years. Journal of Digital Investigation Volume 7. 2010.
[11] Communication and Information Commission Saudi Arabia Report on Internet user's device ownership. Available: www.mcit.gov.sa. 2015
[12] Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang Guide to Integrating Forensics Techniques into Incident Response. Retrieved from csrc.nist.gov 2006
[13] Brian D Carrier, Eugene H. Spafford (2004) Digital Forensics Research Workshop.
[14] Available : http://fepac-edu.org/accredited-universities
[15] https://www.fbi.gov/news/stories/2013/january/piecing-together-digital-evidence

AUTHOR'S PROFILE

Dr. Abdullah Aljumah
Associate Professor in College of Computer Engineering, department of Computer Engineering. Prince Sattam bin Abdulaziz University, Saudi Arabia. Completed PhD from Cardiff University of Wales (UK) and he had published many papers in different areas like Artificial intelligence, neural networks, Data mining, Digital forensics, Network Security.
Email: aljumah88@hotmail.com

Dr. Mohammad Gulam Ahamad
Professor in College of Computer Engineering, department of Computer Engineering. Prince Sattam bin Abdulaziz University, Saudi Arabia. Completed PhD from Osmania University India. He had published many papers in different areas like Data mining, Digital forensics.
Email: prof.gulam@gmail.com

Mohammad Yousuf Uddin
Lecturer in College of Computer Engineering, department of Computer Engineering. Prince Sattam bin Abdulaziz University, Saudi Arabia. Completed MSc IS from Osmania University India.
Email: m.yousuf@sau.edu.sa