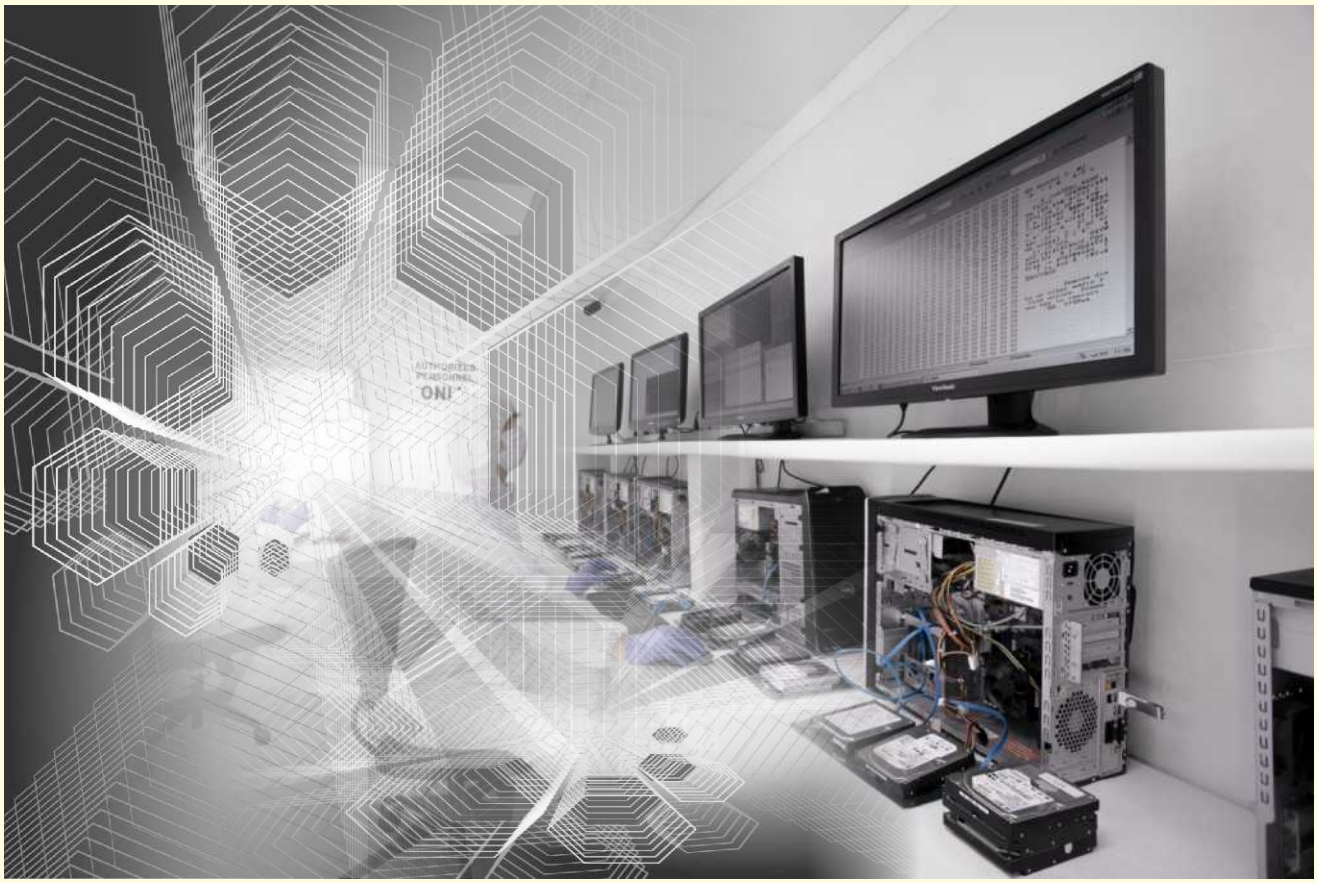
ISSN: 2522-3429 (Print)
ISSN 2616-6003 (Online)

International Journal for Electronic Crime Investigation (IJECI)



Vol. 3 Issue: 2
ISSUE: April - June 2019

Email ID: ijeci@lgu.edu.pk

Digital Forensics Research and Services Center
Lahore Garrison University Lahore, Pakistan.

LGU International Journal for Electronic Crime Investigation
Volume 3(2) April - June (2019)

CONTENTS

LGU International Journal for Electronic Crime Investigation
Volume 3(2) April - June (2019)

Shahzad et al LGURJCSIT 2019

LGU International Journal for
Electronic Crime Investigation

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

Research Article

Vol. 3 Issue 2, April - June 2019

Cyber-Terrorism Law, Implementation and Ways Forward

Amir Shahzad
DDPP Sargodha
7th Batch specialized Training of Counter Terrorism Prosecution
aamirshahzad510@yahoo.com

Abstract:
This research paper is concerned with focused critical analysis of cyber terrorism laws in Pakistan. Cyberspace is now becoming a battlefield where terrorists are active on dark net and using digital tunnel for which every country of the world has to take necessary steps for global peace, in the same way Pakistan needs an effective legislation and its efficient implementation. We explore here some crucial questions regarding cyberterrorism threats, cyber terrorism laws, implementation challenges and some recommendations based on current situation as well as a slight glance on future perspective of the topic Cyber terrorism law, implementation and the ways forward.

Keywords:

1. Introduction

Before the promulgation of prevention and electronic crime act (PECA) in 2016, there was a law namely Electronic transaction Ordinance 2002 (ETO) to deal with the unauthorized and unlawful access to information system. However, ETO was an incapable law to cope the multidimensional nature of cybercrime. An increasing use of internet at one click is at the same time a phase of new challenge for the globe as well as in Pakistan which enforced legislature to draft a legal framework to protect the legitimate digital media users as the modern school of thought now tells that "digital rights are basically human rights in the internet era". Accordingly elaborating 25 new offences and their punishments, Prevention of Electronic Crime Act 201 6 was passed on August 11, 2016 in Pakistan, first comprehensive law in our history to encounter cybercrime as well as cyber terrorism. Much has been said on the issue of "Electronic Pearl Harbor" before and after Washington and New York attacks of September 11, 2001 but thereafter apprehensions raised a bitter question to the whole world as alarming notion that "what would be the probabilities and trepidations of terrorist attacks in cyberspace in future"? As reported by Carnegie-Mellon Computer Emergency Response Team Coordination Center, about 200000 cyber security incidents took place within the first three quarters of 2003 by nasty programmers? Hackers? Or script kiddies? The answer is not so simple. The person behind cyber-attacks could belong to any terrorist organization, intending to cause widespread damage to the peace and prosperity of the world. So here we are with a law Prevention of Electronic Crime Act 2016 in Pakistan to deal with this modern challenge of digital era i.e. Cybercrime & Cyber terrorism.

Obviously, implementation of PECA,2016 in letter and spirit would remain a challenge for Pakistan, as we are a country victimized most by terrorism and unfortunately, we are now placed in the grey list of Financial Action Task Force (FATF) with allegation of terrorism financing. So, to curtail our victimization, to get out from the grey list and to protect our future we need to protect our country from cyber terrorism. Accordingly, we need an efficient comprehensive moderate legal framework and

its effective implementation, hence this study aims to review this law in this perspective.
This law is multifaceted in nature dealing with the cybercrime in general, cyber terrorism and with other legal and procedural aspects. This review only focusses on provisions related to the cyber terrorism and its implementation issues. Firstly, sections related to cyber terrorism are analyzed. Secondly investigation, procedure and related issues are critically reviewed. Thirdly, legal, investigative, administrative, and technical challenges to implement this law, particularly to encounter cyber terrorism. Lastly, ways forward to these challenges are proposed.

2. Research Methodology

Research methodology for this paper is a combination of primary and secondary research. Interviews have been conducted of the legal, computer sciences and digital forensics experts from the different practical fields. As a secondary source, benefits have been obtained from different research articles, thesis, different statutes and other sources from all over the world. Proper references have been made accordingly.

3. What is Cyber Terrorism?

Before going to discuss the concept of cyber terrorism we need to pass the bridge of complexity i.e. the definition "terrorism" which is not only different among the different countries but also an absolute clarity in the definition is still needed. Pakistan has longest definition of terrorism under section 6 of Anti-Terrorism Act 1997. Accordingly, for a general understanding it can be inferred that if an act is terrorism for a country and if the same is done by using any information system, the offence would be cyber terrorism. Let's have a look on few important definitions of cyberterrorism to understand its scope.
Dorothy E. Denning, defined cyberterrorism in year as: "Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives".
Websites hacked by terrorist organization are often political or social and are used as tactics of cyber terrorists. In the word of J.T Caruso:
"Cyberterrorism – meaning the use of cyber tools to shut down critical national infrastructures (such as energy, transportation or government operations) for the purpose of coercing or intimidating a government or civilian population".
In the advent of 21st century, there remained a debate to define the cyber terrorism between the thinktanks around the world. Media used to derive the definition of cyber terrorism from the above notion e.g. in 2001 Business World Report publish a list of cyber terrorism attack, two of which given below:

a. Dutch hackers made theft of information from the U.S. Department of Defense computers about U.S. troop movements during the 1990-91 Persian Gulf War and tried to sell the information to the Iraqis but the Iraqis thought it was a trick.

b. Disfigurement of U.S. Web sites after the April 1, 2001 crash between a Chinese jet fighter and a U.S. investigation plane.
However, these examples remained failed to qualify Denning's definition: "Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not"
As observed above, media reporting was cited misleading and arguments were offered that there was no specific example of cyberterrorism which qualified Denning's prerequisites till that time. So, there are various concepts on this issue considering cyber-terror, cyberterrorist and cyberterrorism. While PECA 2016, reveals the definition of cyberterrorism in the following words under section 10
"Cyber terrorism. Whoever commits or threatens to commit the offences under sections 6. 7, 8 or 9, where the commission or threat is with intent to-

"(a) coerce, intimidate, create a sense of fear, panic or insecurity in the Government or in the public or a section of the public or community or sect or create a sense of fear or insecurity in

society; or

b) advance interfaith, sectarian or ethnic hatred

c) advance the objectives of organizations or individuals or groups proscribed under the law"

While the corresponding provisions referred above, section 6 deals with offence "Unauthorized access to critical infrastructure information system or data". Section 7 deals with offence "Unauthorized copying to critical infrastructure information system or data". section 8 deals with offence "Unauthorized interference to critical infrastructure information system or data". section 9 deals with offence "glorification of an offence".

So mainly offences are defined in section 6,7,8,9 but if these offences are committed or threaten to commit with the Mens rea as revealed in section 10 above, would amount to cyberterrorism under the perspective of PECA, 2016. However, it extends its perspective in section 10A & 10B in the following manner:

Section 10A reveals the concept of Hate Speech, "whoever prepare or disseminate information through any information system or device that advances or likely to advance inter-faith, sectarian or racial hatred"

Section 10B divulges the offence of that recruitment, funding and planning of terrorism, preparing or disseminating information, through any information system or device, that invites or motivates to fund, or recruits people for terrorism or plans for terrorism.

So, a wider scope definition we have now under PECA but still there is much to say about it. Some of the critics considered it as a law full of vagueness and the scope of cyber terrorism is contradictory with the fundamental human rights guaranteed by Constitution of Pakistan. Concept of terrorism entailed by section 10 of PECA is criticized for its too much broader scope which makes it unclear. It's a general principle to test the unclear legislation on the basis of vagueness doctrine. The essence of this doctrine is based on clarity of criminal law. It requires an explicit clarity that a criminal legislation must answer clearly that what type of conduct is punishable?

The mindset correlated to terrorism, hate, cyber terrorism, cyber hate is sightseen as well as scrutiny of wider theories which relate to cybercrimes such as "social influence", "social identity theory" and "social identity model of individualism", belongings and discriminatory moral disentanglements. An efficient implementation of any law is always a slave of its given scope and definition. It's now universal reality that cyber space in a parallel universe within the human world which is much wider and bigger indeed. Terrorist are part of this world and they do have complementary opportunity to use cyberspace for their ulterior causes which is much easier to do as compare to physical actions and may be more fatal than ever before. Anti-terrorism legislation always adversely affects the human fundamental rights. Peace and prosperity of a state is more valuable then freedom of speech or freedom of using digital media.

After facing almost two decades of worst terrorism, we are forced to have such wider scope definition of cyber terrorism with vast powers of investigation agencies. However, probability of political misuse of any criminal law cannot be ruled out. More the wider scope definition more chances of its misapplication.

4. Historical Review of Cyber-Terrorism

The importance of cyberspace can be well adjudged that almost each of the frontline terrorist organization has Web site(s). These sites even cannot be forced off because these terrorist groups are genius enough that they use to operate their web sites from the countries with wide scope freedom of speech laws e.g. alneda.com of Al-Qaeda group used at first Malaysia as its host country then Taxas and thereafter Michigan. It was forced off in 2002.

Web sites were used by terrorist groups for various causes. Few examples from the history are listed below:

a. hizbullah.org was used by Hizballah as its central press office.

b. moqawama.org was used to present the details of its attacks on Israel

c. Jehad.net, aloswa.org were established by supporters of Al Qaeda to support Osama bin Laden.

d. Al-Farouq website was used by Osama bin Laden to publish 39 principles of jehad

e. 7hj.7hj.com was used to impart the skills of hacking for Jehad purpose.

f. Alneda.com notable most with reference to its multi-features i.e. cyber-planning through use of internet via publication of terrorist cause and propaganda, recruitment, information gathering, internet techniques to hide identities, fund raising, control and mobilization etc.
Talking about 9/11 attacks, Muhammad Atta placed his final instruction via email, as reported:

"the semester begins in three more weeks. We have obtained 19 confirmations for the studies in the faculty of law, the faculty of urban planning, the faculty of arts, and the faculty of engineering"

The code words used, encapsulated, it is said that four targets or four airplanes to be used for attacks

Obviously, it's a natural progression for terrorist groups to target /use cyber space for their attacks. Hence cybersecurity is a global issue, it must be treated globally. Not only every state is required to have an efficient and moderate anti cyberterrorism legislation but there is also a crucial need to have a global legislation with mutual integration of all countries of the world for global peace and prosperity. PECA ,2016 by Pakistan is first-rate step, in line with this mutual global mission.

5. Cyber Terrorism Laws in Pakistan:

As said earlier sections 6,7,8,9,10,10A,10B of Prevention of Electronic Crime Act, 2016 with section 11W of Anti-Terrorism Act 1997 are the direct provisions to encounter cyberterrorism in Pakistan. Let's have a gist of understanding of these provisions:

5.1 Section 2(c) of PECA, 2016:

The basic prerequisite of sections 6,7,8 is "critical infrastructure" which is broadly defined in section 2(c). It encapsulates all those processes, networks, assets, systems, facilities, if they got loss or their integrity is compromised, the consequences would might be in all or any of the followings:

1. Substantial causalities or loss of life
2. Substantial adverse impact(s) on economic or social situation
3. Substantial adverse impact(s) on national security
4. Substantial adverse impact(s) on national defense
5. Substantial adverse impact(s) on functioning of the of the state

Its scope has been made wider by proviso of this subsection where its provided that it is authority of the Government to declare any private or Government infrastructure as critical infrastructure based on its objectivity in purview of above-mentioned criteria.

5.2 Section 2(k) of PECA 2016:

It further extends and specify this concept by giving the gist of critical infrastructure information system and critical infrastructure data. These terms are specifically used in penalizing sections this Act.

5.3 Section 6 of PECA:

Incriminates the unauthorize access to critical infrastructure system or data and provides punishment of imprisonment up to 3 years or fine up to one million rupees.

5.4 Section 7 of PECA

Section 7 incriminates the unauthorize copying or transmission of critical infrastructure data and provides punishment of imprisonment up to 5 years or fine up to 5 million rupees.

5.5 Section 8 of PECA

Section 8 incriminate the interference with the critical infrastructure system or data and provides punishment of imprisonment up to 7 years or fine up to 10 million rupees. These three sections penalize a cybercrime without its node with any kind of cyberterrorism.

5.6 Section 9 of PECA

Section 9 is directly related to terrorism activity and incriminate a pet activity of terrorist i.e. glorification of an offence. From all the history of terrorism it is evident that every terrorist group needs its glorification to flourish and to fascinate the attentions. This section reveals in the following way:

- Whoever prepares or disseminates information,
- Through any information system or

device,

- With the intent to glorify an offence related to terrorism or
- With the intent to glorify any convicted terrorist who is convicted for terrorism charge
- With the intent to glorify activities of proscribed organization
- With the intent to glorify activities of proscribed individual
- With the intent to glorify activities of proscribed group

It further explains the word "Glorification" as praise or celebration in any form of description. The punishment provided under this section is an imprisonment up to 7 years or fine up to 10 million rupees. This section in fact is very important with reference cyber terrorism as history tells us that terrorist groups used their web pages for their glorifications

5.6 Section 10 of PECA

Then section 10 comes with the proper term of "cyber terrorism" and encapsulates the scope of the offence of cyber terrorism. It focuses on "intent" or we may say "Mens rea" to create nexus of offences under sections 6,7,8,9 particularly with cyber terrorism. It covers both commission of offence or threat to commit which makes this section wider in scope in term of its implementation. A cybercrime under the aforementioned sections becomes cyber terrorism under this section mainly because of the intention of the offender. It elaborates in clause (a) that intention of offender is:

- Creation of coercion
- Creation of intimidation
- Creation of sense of fear
- Creation of sense of panic
- Creation of sense of insecurity

For:

- The Government
- The public
- Any section of public
- The community
- Any sect
- The society

So, in clause (a) of section 10, clear details come across, what terrorist groups usually aim to do ever. Clause (b) specifically emphases sectarianism, like intention to evolve hate or to spread hate between the sects or ethnic groups. It is pertinent to mention here that; this focus is one of the prerequisites provided in the preamble of Anti-Terrorism Act 1997 to encounter the intense abuse of sectarianism in Pakistan.

Every terrorist organization or group has its objectives for which terrorists strive for. They need to spread their objective notion at its maximum to achieve them. Clause (c) speaks about such objectives. It relates Mens rea of offender to advance the objective of proscribed individuals or proscribed groups or proscribed organizations. So, to stop the advancement of objectives of terrorist, this clause is emerged wisely. Punishment provided under section 10 is imprisonment up to 14 years or with 50 million rupees.

5.9 Section 10-B of PECA

The section deals with the offence of recruitment of people for their terrorist group, generation of funds for their terrorist activities and terrorism planning vide using information system. As said earlier, now it easier for the terrorist groups to motivate people to join their cause and to invite their financial support by interacting with them through internet devices as everyone have now this source in his hand round the clock in the shape of cell phones. At the same time, it has become an effective way then ever before, for their planning. This section provides 7 years or fine as punishments for the offenders.

5.10 Section 11W of Anti-Terrorism Act 1997

Section 11W of Anti-Terrorism Act 1997 was emerged to encounter the projection of any kind of terrorism or terrorist or proscribed organization or even organization under observation due its suspicious activities or funding etc. via publication, dissemination or any other such like sources. As mentioned above, facing new wave of terrorism in the leadership of Maulvi Fazlullah in Sawat, who used FM radio channel to motivate people in the name of jehad against the Government of Pakistan by declaring this country as Darul Harrab etc, Government emerged specifically the word FM radio by amending this section in 2009 but thereafter it was repealed in 2010. The scope of this section is very broad by including about all types of source of communication and about all types of possible acts to use these sources with the multi-motive(s) behind related to terrorism behind.

Actions:

1. Glorification of terrorist
2. Glorification of terrorist activities
3. Projection of any convicted terrorist who is convicted under the charge of terrorism
4. Projection of any proscribed organization
5. Projection of any proscribed person
6. Projection of any organization which is under the observation

Methods or Source of Communication:

a. Printing
b. Publishing
c. dissemination
d. Audio cassettes
e. Video cassettes
f. Any form of data device
g. Any form of storage device
h. Any kind of visible sign
i. Written photographic
j. Electronic
k. Digital
l. Wall chalking
m. Any other source or method

The punishment provided under the charge 11W ATA is 5 years imprisonment with fine. News report is exception of this law provided in this section but with the condition of "good faith". So, all the news channels and newspapers etc. are exempted from this penalized section when they are reporting to the general public. However, on the part of reporting agency would be observed in any adverse circumstances46.

5.11 Section 24 & 25 of PECA, 2016

All the offences under this Act may be read in the light of above both the sections of PECA. Scheme of this law reflects that substantive offences like terrorism would be tried along with sections of this law if the information system was also used for commission of terrorism. Offences of terrorism, for example glorification, hate speech are tried under the Anti-Terrorism Act 1997, if the mode of committing does fall under the ambit of ATA,1997 and would be punished under the same Act only, but if any information system is used or any other mode provided in PECA 2016 is used the offender shall additionally be punished under this PECA 2016 as well.

5.12 Sections 26 (3)(4), 28 & 37 of PECA, 2016

Collection, preservation and production of digital forensic evidence is a significant subject of any cyber law as well as cyber terrorism law. Sub-section 3 & 4 of Section 26 of PECA, 2016 caters to the requirement of scientific standards for admissibility of forensic evidence. Even preservation of data under Section-28 is also an enabling provision along with successive sections. Section 37 also help in this context which authorizes the government for establishment of forensic Laboratory.

So as afore discussed there are bunch of sections to face the challenges of cyber terrorism. This law provides much more but, for an effective delivery of any law, it has to pass through its implementation challenges.

6. Implementation of Cyber Laws in Pakistan – Problems

Talking about cybercrime and cyber terrorism, our country does have its history without any combatable law in hand. PECA, 2016. A late legislation is now a comprehensive law to cope this modern scientific contest. Obviously, there are series of hurdles and glitches on the way of its effective implementation:

6.1 Legal Complications

1. Chap-V speaks about all offence are non-cognizable, compoundable and bailable, except offences u/s 10, 19 & 19-A; this chapter is somewhat defective as does not talk about application of code of criminal Procedure expressly; though an attempt has ben made to highlight it in section 47 but it does not serve the purpose. Even who would compound the offence is a big question,offences which are non-cognizable obviously would be investigated if they are annexed with any offence under PPC or any other law which are cognizable. Question of jurisdictions would arise if the offence is added by any other law; section 41 would be a great hurdle in this respect. Unnecessary litigation would reduce the efficacy of this law.

2. No appointment of prosecutor is highlighted as it is mentioned in ATA & CNSA;

which would open a debate for prosecution of offences.

3. Trend of investment, use and speculations in "digital currency" is increasing day by day which is an offence on one side but it has other worst faces like it is being used for money laundering as well as it can be used for terrorism financing. No specific provision, definition or penalized section has been emerged in this regard. More over in the current era, money laundering and cybercrime should be seen together. These offences, in this cyber dependent modern world, should be understood together and dealt accordingly. Unfortunately, Anti-Money Laundering, 2010 is also silent on this issue.

4. Section 27 of PECA, 2016 reveals "power to investigate" and start with the word "only an authorized officer of the investigation agency shall have power to investigate under this Act". This might be problematic. In the current scenario FIA has power to investigate offence under this Act. For instance, if any terrorist attack is happened in any area of the country and CTD is dealing with that, according to this section if that terrorist activity is also related with some cyber terrorism activity then CTD is unable to investigate or collect evidence up to that extent?? Obviously, this would amount to loss of evidence and other procedural complications. In the same way concept of joint investigation team under this section is also unclear. It becomes more confused once again with the compulsion of authorized person.

5. Preservation of Data etc. is being regulated through the intervention of court under section 30, as its give power to authorized officer to dispense with such warrant if he apprehends destruction of data. Seeking permission from court in such like cases would be a futile exercise because destruction of data is one click away in the system; until the warrant is obtained, data would be no more in the system. It should be the prerogative of Investigating officer to directly approach the unit for data where ever it may be. We have seen the misuse of section 94 & 95 of Cr. P.C which is not being effectively applied and accused gets the benefit.

6. Sub-section 3 & 4 of Section 26 of PECA, 2016 provides the requirement of scientific standards for admissibility of forensic evidence. Conservation of data under Section-28 is also an enabling provision. Section 37 also helps in this context which authorizes the government for establishment of forensic Laboratory. Here it's important to understand that digital evidence is not tangible. By taking into possession any kind of device vide recovery memo is not a digital evidence preservation. Digital evidence is intangible content, it cannot be dealt under police rules or any other such like law for the time being enforced rather it needs customized rules and regulations. Its admissibility would remain in question. This law is silent and there are no such framed rules about the stander of admissibility of evidence i.e. Procedure of preservation of digital evidence and its production before the court of law etc..

7. According to the IT experts, terrorist groups uses or can use digital tunnel or dark net to be remained untraceable. PECA 2016 does not define even these terms. This would remain a complicated issue unless properly legislated.

8. There are voices which considered that cyber terrorism clauses under PECA 2016, as against the fundamental human rights, ensured by the Constitution of Pakistan 1973 like freedom of speech etc. the broader powers of investigation agency or authorized officer are also criticized from the same house accordingly.

6.2 Issues Related to Investigation

1. Contrary to the provisions of PECA, 2016, power to investigate is devolved to Federal Investigation Agency (FIA) rather establishment of an independent investigation agency as required by this law. A wing namely NR3C is established within FIA to investigate cybercrime. It's astonishing fact that a proximately thirty thousand application pertaining to cybercrime are pending with FIA while there are only 10 investigation officers to deal with cybercrime. Accordingly, the question arises about investigation of cyber terrorism cases and how can cyber laws implemented in letter and spirit?

2. History tells us that terrorists groups operate wisely and now they are very keen to use cyberspace for their all types of activities like planning, recruiting, fund raising, training, and glorifying etc. While we do have an old wine in a new bottle. FIA has no capacity, skills and infrastructure to combat this challenge. Moreover, the human resource working as

Authorized officer is unqualified, unskilled and untrained. So, FIA is lacking not only quantitatively but also qualitatively.

3. As discussed earlier, collection of digital evidence, its preservation, transmission, its forensic analysis and its presentation to the court need a complete package of legal and technical skills so that it can be admitted by the court of law is completely a scientific process. Neither we do have any trained force to do so nor have any set of rules for this purpose. So even FIA arrests an offender, there is minimum chance of his conviction. Worries becomes more bitter when we see our capacity with reference to the giant of cyber terrorism.

By virtue of subsection 3 of section 26, PECA requires the establishment of an independent digital forensic lab which is yet to be established. We are depending on PFSA Lahore for digital forensic analysis which is already overburdened. Moreover, it has no complete digital forensic infrastructure and compatible capacity. So, there is dire need of an independent digital forensic lab for effective implementation cyber terrorism laws.

7. Ways Forward – Future Perspective

At first, we must realize the significance of cyberspace, cyber evidence in connection with the terrorism. Even now and onward we need digital evidence or we can use cyber evidence to prove petty offences in the court of law. To stop the cyber based terrorism, we need to a proactive approach by all means. We can't wait for the incidences. More over its an easy way to drag the culprits into the prison and save the innocent people from fake accusations. Followings are the endorsements in the light of aforementioned issues:-

a. PECA is a law, based on technology, not easily understandable by the investigating officers, prosecutor and the judges. Frequent meetings of these three, combined trainings with respect to understanding of protocols applied for arriving at the results and calling of experts in the courts only in critical cases. The most important area for presentation of evidence be focused in such efforts.

b. As aforesaid, this is a technology-based law, hence cannot be implemented without relevant infrastructure for possible monitoring of cyberspace with proactive approach, effective investigation, collection, preservation and presentation of digital evidence.

c. The necessity of digital evidence will increase day by day with high pace in the upcoming times. We were late in legislating proper cyber law and now we must not get late in establishing an efficient well equipped digital forensic lab. Without such lab cyber laws or cyber terrorism laws would remain dreams to be implemented.

d. Legislation flaws as aforementioned, need a dire attention of Government. A body consisting technical experts, legal experts and others may be constituted to work on these legal complications and framing of the proposal of solutions.

e. As required by the Act, an independent investigation agency may be established with skilled and qualified sufficient strength of work force.

For effective implementation of cyber terrorism laws, a customized special wing comprising technical experts and counter terrorism trained personnel may be established within CTD so that terrorism activities may be deal efficiently.

8. Conclusion

Pakistan is a frontline country fighting with the 21st century monster i.e. terrorism, at the same time we are a Nation victim most in war against terrorism as we have lost more than 80000 lives and much more. Lacking of infrastructure and an expert team, incidents of cyberterrorism are not properly reported or even screened and understood in Pakistan. Terrorist has an open opportunity in the shape of cyber world for their all types of activities e.g. recruiting, training, fund raising, funds transferring, planning, and operations etc.

We are having legal, infrastructure and investigation issues along with other systematic problems due to which we remained unable to take effective steps to counter cyber terrorism. We do not have a proper investigation agency to investigate and to properly implement cyber-terrorism laws. What we need to do is to create infrastructure with sophisticated tools to

monitor cyberspace at maximum, to detect and to prevent cybercrime as well as cyber terrorism. We also need an efficient legal framework compatible to the future cyber terrorist attacks. Our general public and institutions may also be sensitized regarding the understanding, sensitivity and apprehensions of cyberterrorism.

9. References

[1] Electronic Transaction Act 2002

[2] Hutt, Rosamund. 2015. "digital Rights Are Basically Human Rights In The Internet Era." World Economic Forum.

[3] National Assembly Secretariat. (2016). "prevention Of Electronic Crime Act" May 2016. Islamabad. Available At: http://www.na.gov.pk/uploads/documenTs/1472635250_246.pdf

[4] Tan, Kheng Lee Gregory. 2003. Confronting Cyberterrorism With Cyber Deception . Monterey, California .

[5] Karim, Shahid. 2019. Www.dawn.com. Jun 10.

[6] Anti-terrorism Act 1997 Of Pakistan.s.6

[7] http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[8] Forno, Richard. 2002. "Shredding The Paper Tiger Of Cyberterrorism ."

[9] Tan, Kheng Lee Gregory. 2003. Confronting Cyberterrorism With Cyber Deception . Monterey, California

[10] Ibid

[11] Http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[12] National Assembly Secretariat. (2016). "prevention Of Electronic Crime Act" May 2016. Islamabad. Available At: Http://www.na.gov.pk/uploads/documen Ts/1472635250_246.pdf

[13] Prevention Of Electronic Crime Act 2016, S.6

[14] IBID, S. 7

[15] IBID, S. 8

[16] IBID, S. 9

[17] IBID, S. 10A

[18] IBID, S. 10B

[19] Khan, Eesha Arshad. N.d. "the Prevention Of Electronic Crimes Act 2016: An Analysis." 1-10.

[20] Faisal Daudpota, 'an Examination Of Pakistan's Cybercrime Law' (2016) Ssrn 14 <http://dx.doi.org/10.2139/ssrn.2860954> Accessed 16 May 2018.

[21] Blakmore, Brain. 2016. Policing Cyber Hate, Cyber Threat And Cyber Terrorism. New York: Routledge.

[22] Timothy L. Thomas. Al Qaeda And The Internet: The Danger Of "cyberplanning". Parameters. Spring 2003.

[23] Dorothy E. Denning. Cyberterrorism. Testimony Before The Special Oversight Panel On Terrorism, Committee On Armed Services, Us House Of Representatives, May 23, 2000. Http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html, Accessed July 2003.

[24] IBID

[25] IBID

[26] Joel Leyden. Al-qaeda : The 39 Principles Of Holy War. Israel News Agency. 4 September 2003

[27] Ibid

[28] Bradley K. Ashley, Lt. Col, Usaf. Anatomy Of Cyberterrorism: Is America Vulnerable? Research Paper, Air War College, Air University, Maxwell Afb, Al. 27 February 2003.

[29] Timothy L. Thomas. Al Qaeda And The Internet: The Danger Of "cyberplanning". Parameters. Spring 2003

[30] Timothy L. Thomas. Al Qaeda And The Internet: The Danger Of "cyberplanning". Parameters. Spring 2003.

[31] Prevention Of Electronic Crime Act 2016, S. 2(c)

[32] IBID, S. 2(K)

[33] IBID, S. 6

[34] IBID, S 7

[35] Prevention Of Electronic Crime Act 2016, S. 8

[36] IBID, S 9

[37] [Denning1, 2000] Dorothy E. Denning. Cyberterrorism. Global Dialogue, Autumn 2000. http://www.cs.georgetown.edu/~denning/infosec/cyberterror-gd.doc, Accessed July 2003.

[38] Prevention Of Electronic Crime Act 2016, S. 10

[39] Anti-terrorism Act 1997

[40] Zuberi, Kokab Jamal. 2018. "use Of Cyber Space By Terrorist Organization." Electronic Crime Investigation.

[41] Prevention Of Electronic Crime Act 2016, S. 10a

[42] IBID, S. 10B

[43] Zuberi, Kokab Jamal. 2018. "use Of Cyber Space By Terrorist Organization."

Electronic Crime Investigation.
[44] Khan, Yousaf Ali & Ijaz. Winter 2018. "uses And Abuses Of Fm Radiaos By Mreasiitants In Former Federally Administered Tribal Areas (fata) Ans Provincially Administered Areas (pata), Pakistan." Central Asia Journal No. 83.
[45] 2003 P.cr.l.j 277
[46] Anti-terrorism Act 1997, S. 11w
[47] Prevention Of Electronic Crime Act 2016, S. 24
[48] IBID, S. 25
[49] Rafiq, Amjad. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 10)
[50] Prevention Of Electronic Crime Act 2016, S. 26
[51] IBID, S.28
[52] IBID, S.37
[53] Rafiq, Amjad. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 10)
[54] Rafiq, Amjad. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 10)
[55] Ibid.
[56] Zuberi, Kokab Jamal. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 7).
[57] Anti-money Laundering Act 2010
[58] Zuberi, Kokab Jamal. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 7).
[59] Prevention Of Electronic Crime Act 2016, S. 30
[60] Code Of Criminal Procedure 1898, S. 94
[61] Ibid S. 95
[62] Zuberi, Kokab Jamal. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 7)
[63] IBID
[64] Khan, Eesha Arshad. N.d. "the Prevention Of Electronic Crimes Act 2016: An Analysis." 1-10.
[65] Zuberi, Kokab Jamal. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 7)
[66] Zuberi, Kokab Jamal. 2018. "use Of Cyber Space By Terrorist Organization." Electronic Crime Investigation.
[67] Rafiq, Amjad. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 10)
[68] Malik, Muhammad Baqir. N.d. "pakistan And India Cyber Security Strategy." 1-5
[69] Zuberi, Kokab Jamal. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 7)
[70] 2018. International Journal For Electronic Crime Investigation Vol.2. Lahore: Lgu International Journal For Electronic Crime Investigation .
[71] Mr. Muhammad Usman Akram, Mr. Tahir Abdullah. 2011. "effective Enforcement Of Cyber Laws In Pakistan ." International Journal Of Science And Technology 1-15.
[72] Zuberi, Kokab Jamal. 2018. "use Of Cyber Space By Terrorist Organization." Electronic Crime Investigation.
[73] Sue, Siman Shecliff. 2012. "the Use Internet For Terrorist Purpose." United Nations, Unodc 7-12.

Malik et al LGURJCSIT 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 2, April - June 2019

Electronic Devices to Investigate Offences of Torturing, Abusing, Molesting, Assaulting or Killing the Innocent Children

Aftab Ahmad Malik[1], Mujtaba Asad[2], Waqar Azeem[3]

[1] Professor Department of Computer Science,
[2] PhD Scholar, School of Electronics Information & Electrical Engineering, Shanghai Jiao Tong
[3]Assistant Professor, Department of Computer Science
Lahore Garrison University (LGU), Pakistan[1]
University Shanghai China[2]
Lahore Garrison University (LGU), Pakistan[3]
dr_aftab_malik@yahoo.com[1], asadmujtaba@sjtu.edu.cn [2], waqar.azeem@lgu.edu.pk [3]

Abstract:
The offences of torturing, abusing, molesting, assaulting, physical torturing or killing the innocent children are increasing day by day in our society. Mostly such offences are practiced on the young learners studying in various institutions ranging from lower primary, primary and middle level. Irrespective of the privately managed or public institution, the heinous offences occur in the schools. The torture ratio is comparatively high in village schools and also where the learners are sent exclusively for religious education. In such schools mostly the poor and orphan learners are admitted and may be the whole time resident of the schools. Another common aspect is the torture extended to innocent young female or male, who are resident servants. There are also periodical reports of inflicting torture sometime accompanied by killing. Another category of offenders is that who choose the innocent children from local neighbouring localities rape, molest, sodomise and then kill them. They either commit the offences alone or with their gang or allies. In case of killing the dead body is thrown in the locality or nearby canal. The procedure or steps taken by offender for committing an offence is "Modus Operandi". On most of the occasions the forensic evidence left and available by means of which the criminals can be traced, while in certain other cases, it is not adequate for the purpose of prosecution. A few case study are revealed. In this paper, we focus on some effective digital and electronic devices to facilitate the investigation to collect effective evidence usable in the court of law. The relevant tools for retrieving the forensic data are also introduced..

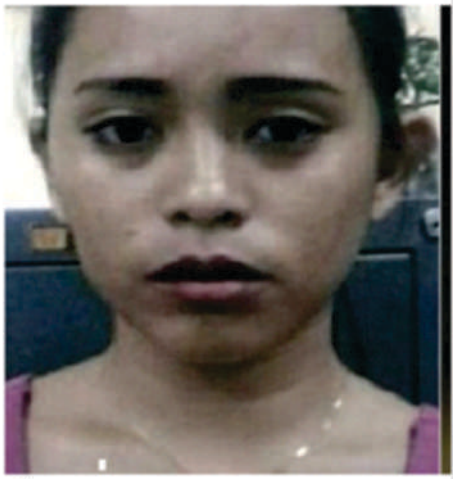
Keywords: Mobile communication equipment, Criminal data storage and retrieval, Databases and Data Ware houses, Data Mining

1. Introduction

The victims of the offences of abusing, molesting, assaulting, physical torturing or killing the innocent children inflict high degree of torture. Every day, we hear of police brutality and cruelty [3], [5-6]. It happens as and when a police officer exceeds his limits of power and becomes inhumane, atrocious, terrible and cruel. At that time he uses more force than required in performance of his duty. This is called use force quantum. The criminals reacting with the society, in a similar fashion inflict torture to innocent women and children, especially teen agers. The sequence of their modus operandi may be abduction, rape and then killing.

According to [1] creating harassment and intimidating innocent children under 18 through internet and displaying their pornographic videos is serious cyber crime. The motive behind these offences comes from animated cartoon, films sand rubbish material polluting the minds

of offenders. The dark web also provides them difference ways to inflict torture to the innocent creation- the children. The offender involved in such offences have serious psycho and psychiatric disorders such as exhibition of sexual organs in public, sexual instability, masturbation and barbarity. In the initial stages the offenders arrange meetings with the children and capture their photographs and video for black mail. Sometimes they arrange the outstation tours with innocent children. The computers, cameras and other electronic equipment are used to accomplish the crime. According to [2], the pornography has reached to high limits even on internet, films and videos. That sort of material creates intent to commit other offences being discussed in this paper. The subject of child abuse is not recent one. Tremendous amount of legislation exists in this field. On the other hand [1] the darkweb or darknet or deep web is a magnet for the criminal of child abuse. It is separate world of criminals and their heinous, terrible and dreadful activities. There are millions of such accounts on deepweb where video and pictures of innocent children can be observed while being abused and tortured from high to very high degree of injuries. The offences against children are spreading like terrorist activities in various countries specially Pakistan. We know one little Zainab of city Kasur Pakistan, but there are millions of such little girls round the world, who have been abducted, tortured, raped and killed.



Picture 1: Photograph of Margallo

According to [7], a Philippine girl Liezyl Margallo aged 23 years (Picture 1), was caught by NBI National Bureau of Investigation as a child trafficker. Apart from this, her modus operandi was also to abduct torture and kill innocent young children. Moreover, she liked torturing little girls to death on Camera. She was also managing international cyber-pornography business. There is long list of offences against humanity, but two of them are relevant to our work i.e. crimes against public morals and children.

It is perhaps unknown to the rest of the world that how the learners (particularly poor and orphans) are living in school boarding to get religious education; their life is extremely miserable because of the harsh, intimidating and cruel attitude of the teacher. All such schools are privately managed and no fee is charged from students. These schools are run on donations. According to [11], all the offences such as victimisation, sodomy, torture, harsh punishments and sometimes killing are practised on innocent children. Heavy sticks, rubber pipes and punches are used to punish the students in such schools. The picture [2] is that of 5-years boy, who was killed and hanged after sodomy inside the place of learning.

Picture 2: Ashraf Javed age 5, Killed

2. Major Reasons for Child Abuse

Due to the impact of various types of warfare in the societies such as economic warfare, cultural warfare, warfare based of religious differentiation, poverty and unemployment which are nurturing the elements of criminality are nurturing. The marriages of young males are considerably delayed. In the absence of any effective deterrent force like that of religion, fear

of God and law, the individual and groups of criminal are becoming stronger, particularly when Police is silent spectator. The preparation and display of pornographic films, Cartoons, magazines and other available material increase the elements criminality rapidly. A portion of social media is constantly projecting shameful stories of men having intercourse and sexual activities with a real sister, wife of the brother and nearest relatives ("Mehramats") or neighbours and also of acts sodomy, molestation, torture or killing of innocent children. It is duty of the society, academia, law enforcement agencies and government to take seriously on war footing to eliminate such trends. The publication or broadcast or telecast of such material and its distribution or propagation in any form must be banned. The parents do not have time to observe the children while they are outside home. According to [4], the children are born innocent and should be loved cared. It is the duty of the parents to make them useful citizens and apply utmost vigilance almost until they are out of teen age. The parents must keep an eye of how they are treated outside home while receiving school or religious education.

It is usual practice that children are inflicted with heavy beating using hard things resulting damages, wounds and punishment-prints, which are visible. The body of the child is delicate like flowers. The wounds so caused to innocent children become permanent memories in their soul, heat and mind, really not erasable.

3. Law Related to Offences against Children

The most comprehensive and self contained law [9] was promulgated by British parliament for entire United Kingdom in 1978. The Act defines almost all aspects such as indecency, mens rea, pseudo-photograph and role of computer files connected with offences against children. The Protection of Children from Sexual Offences Act [10], was promulgated in 2012 in India, which covers all the aspects of offences committed and their modus operandi. The sexual intimidation, penetrative-sexual-assault and sexual harassment are the major issues for which punishments were prescribed. The Act also deals with [10] punishments for child pornography, abetment for commission of the offence and most impotently the role of media and photographer. The detailed procedure for recoding the evidence is also provided in this Act.

According to [12], an amendment in PPC was made regarding Child Abuse in 2016. The section 82 of PPC is relevant in this case. In Pakistan apart from abusing the children, the elimination of children is another hot issue. According to [13], the lagal setup in Pakistan in not adequate to fight with child sexual abuse. The law alone cannot make rapid changes in the society. Most of the cases are reported in Britain, United States, Pakistan and India. Pakistani children require [14] strong protection system against abduction, rape, sodomy, molestation and killing. This is needed due to tremendous increase in the rate of crime. The Law alone cannot provide protection [14] to Pakistani Children.

Our children are facer dangers outside home from abusers groups of offenders. The use narcotics, keep knives or guns; they move freely in society. Sometimes, police employees of lower rank may be their alias. According to [15], the crimes of " sexual abuse" and "molestation" are related to child abuse while the terminology of sexual abuse is prevalent for persons of all ages.

4. Harsh Beating and Punishing Children in Islam is Prohibited

The Prophet of Islam being "Rahmatan lil 'alamin", extended mercy and blessing for all.

He was very kind, affectionate and gracious for the children. He prohibited the people not kill their young little daughters and not to beat their children harshly with full emotions. Further, the children should not be beaten on their faces. This is the morality and ethics of Islam in this context, not to be harsh and hard with children.

5. Tortures by Teachers in Schools

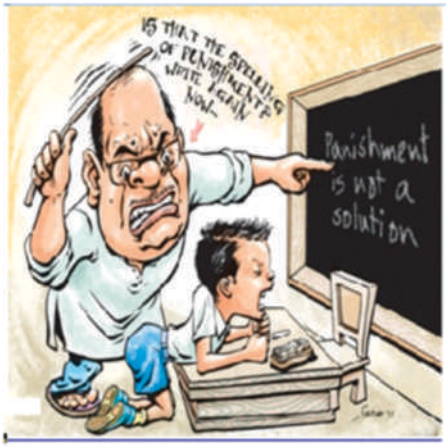
The school teachers extend torture using different methods, [16] elaborates some of these methods. These are slapping on the face, calling the students in Principal office and beating harshly, complaints with parents and calling them, locking up in solitude (Picture 4) , humiliation, kicking out of class, harsh physical punishment with stick, kneeling down (Picture 5) , withdrawal of students privileges and

imposing fine.

Picture 3: Slap on the Face

Picture 4: An innocent baby in lock up

Picture 5: Kneeling down for longer times



Picture 6: Use of Stick

Picture 7: Girls victims of teacher

Picture 8: Self explanatory

6. Tools used by Criminals

Apart from weapons and torturing equipment the criminal use the following electronic devices to communicate to their alias and keep record of their sinful activities:

- Mobile Phones
- Video recording Camera
- Computer and internet

The reason for using the Video recording Camera, Computer and internet is to communicate or sell the tapes of victims. The mobile phones are dynamically, frequently and actively used because the modern cell phones possess the potential of other electronic devices. The information of mobile phones of the criminals provides best forensic evidence and can be used in the investigation. We know that Data saved in computer file being in binary system is not readable. A screen image photograph [9]. It is called a derived image. It is actually another form of the original photograph. According to the Act, this is an offence to take obscene and indecent photographs of a child. Downloading such objectionable matter on disk is also an offence.

Picture 9: Mobile Devices

7. Facilities in the Modern Mobile

The criminals and terrorists frequently use their mobiles for communication with their alia. The present day mobile phones possess most facilities of a computer such as chargeable battery, camera and torch, advanced multimedia, Google, colour display unit, Bluetooth, central processing unit, strong wifi, Networking and communication system, File handling, a database of user's contacts, calculator, TV, Radio audio-video recording and display systems, Email and messaging. It keeps records of movies for future display as it is provided with adequate memory. There are several other applications, capabilities and services available to the user. The mobile hand set phones have become need of the day and luxury in leisure and free time. It also possesses additional functions and computing facilities with a built in operating system. The android operating system has been preferred by various companies due to its compatibility with mobile hardware. There is a race and competition amongst the manufacturing companies to present most innovative mobile phones. Every mobile set iDEN, GSM or WCDMA, is allocated a unique identity called IMEI "International Mobile Equipment Identity ". The SIM card allows the user to enter money for mobile calls and messages. One mobile can interact with mobiles of other companies. Further the roaming facility, fax, calendar, clock and games are also important features of user's interest.

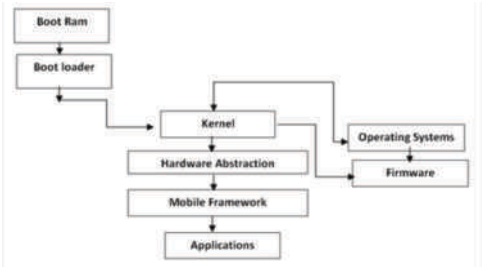


Figure : Internal System of Mobile Device

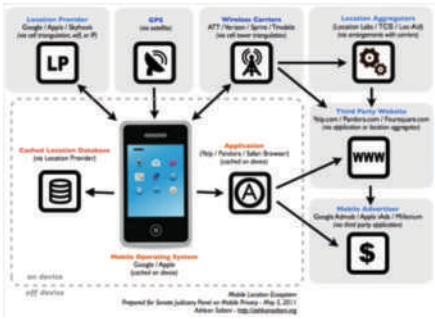


Figure 2: Modes of Tracking Information from Mobile

8. Accessing and Tracking the Information of a Mobile

The purpose of this section is to know the procedure for recovering information of criminals from their mobiles regarding past transactions. The internal software System of the mobile shows how it works and provides service to the users. On one hand the mobile data is stored in the mobile and on the other important data is stored in the repository of the mobile company, the service providers. The mobile service providers can access to the information such as location, messages, call logs, phone numbers of the Call/messages of the user and the recipients. The entire data of the user can be accesses such as stored images, audios, video and other documents and tables. According to [17], using the software "Remote Display Control", provided free, information on the mobile can be displayed. According to [18], widows 10 Windows 10 Mobile has a built-in text message backup option. When messages from mobile are deleted, they are not removed permanently. They are tagged in the mobiles memory and the phone's operating system write new information over that same storage space. A wireless backup service is available.
such as iTunes, Samsung Smart Switch, or LG Bridge to create a backup of mobile computer and can be tracked.

Figure 1 shows the internal mechanism of the mobile, how the applications are run on the internal system. Kernel is actually chief executive to manage memory and processes. Figure 2 explains modes of tracking information from mobile devices using various techniques: such as by accessing location coordinates of mobiles GPS. However, if mobile don't have GPS sensor installed, the location can also be tracked by other modes of accessing. For example

- Accessing Information through Service Provider.
- Through installed applications on the criminal's mobile device.
- Through browser and third party logins, which are store information on the device and subsequent locations in sequence.

9. Conclusions:

The criminals involved in offences of torturing, abusing, molesting, assaulting, physical torturing or killing the innocent children can be arrested using information in their mobiles and computer directly from these device or with the help of service providers. The locations pf the moving criminals can also be found invoking roaming information stored on the mobile and service provider end. Mobile Messages can be recovered using existing technology for forensic evidence. Other data on the mobiles and computers of the criminals such as photographs, videos, SD cards and phone log can be easily tracked..

Acknowledgement: The authors acknowledge the guidance of Mr Kaukab Jamal Zuberi, the Chief Editor and Director DFRSC, Lahore Garrison University, extended during this research work.

10. References

[1] S Mariyum Nizami: "Causes, Prevention and Law Concerned with Cyber Child Pornography", LGU International Journal for Electronic Crime Investigation Volume 2(4)) October-December (2018).

[2] Brutality | Definition of Brutality at Dictionary.com www.dictionary.com/browse/brutality

[3] What Is Police Brutality? - The Law Dictionary; thelawdictionary.org/.../what-is-police-brutality

[4] Sam Harris (2011),"In Defence of Torture", The Blog, http://adinfo.aol.com

[5] Ryan General (2017) "Filipino Woman Who Loved Torturing Little Girls to Death on Camera Finally Arrested".

[6] The Protection of Children Act 1978, legislation.gov.uk

[7] Protection of Children from Sexual Offences Act, 2012; www.advocatekhoj.com/library/bareacts . indiacode.nic.in/.../123456789/2079/4/A2012-32.pdf

[8] M. Nasir (2012): http://islamvs.blogspot.com/2012/11/.html

[9] Pakistan Penal Code Child Abuse Amendment 2016 www.lawsofpakistan.com/pakistan-penal-code-child- abuse...

[10] "Child Abuse Elimination in Pakistan Law General Essay", www.uniassignment.com/essay-samples/law/child...

[11] Legislation Alone Cannot Protect Pakistan's Children asiafoundation.org/2018/01/17/legislation-alone.

[12] Is There a Difference Between Molestation and Sexual Abuse ... brettpodolsky.com/child-abuse/is-there-a...

[13]: Tanvi Sharma(2013); "10 Most Common Ways in which Teachers Punish Students"; listdose.co/10-common-ways-in-which-teachers-punish..

[14]: How can retrieve a data from a mobile phone https://www.techyv.com/questions/how-can-retrieve-data-mobile-phone/

[15]: Andrew Border :Technical Writer, Trainer for Apple Inc; "How to Get Old Text Messages from Cell Phones", cellphones.lovetoknow.com/innovation-technology/...

Fatima et al LGURJCSIT 2019

LGU International Journal for
Electronic Crime Investigation

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

Research Article

Vol. 3 Issue 2, April - June 2019

Forensic Photography: A Visual and Legal Record of Crime Scene

Fatima Fatima
fatima.dfrsc@lgu.edu.pk
Lahore Garrison University

Abstract:
Based on priority forensic photography is a source of documenting crime scenes. Currently it enables to signify a crime scene with every significant pieces of location and evidences. Adding to forensic investigation, crime scene photography provides a true and precise record of original scene and evidences relevant to surroundings. Crime scene photograph can illustrate a crime scene easily than verbal description by an investigator as it freezes time and records the evidences. It records all type of crime scenes such as fingerprints, impressions, injuries or bruises on skin in assault cases, human identification, bloodied body and knife in murder case etc. Scientific photography skills and techniques such as UV, IR and Fluorescence light filters are practiced to discover and preserve the hidden information during investigation. It is an integral part of criminal investigation by providing proper documented focused photographs to present actual story of the scene in the courtroom.

Keywords:

1. Introduction

"A picture depicts thousands of words especially true in crime scene or forensic photography."

Photography has demonstrated and preserved history for past 200 years from landscapes to historic events (3). Forensic photography is as old as the camera itself (7). It was familiarized in 1851 when a forged document photograph was allowed to present it as court room evidence in Belgium. It was born as forensic investigative tool and became an advanced technology in 1870s for forensic identification and scene analysis. It provides a permanent visual proof of the scene to the forensic investigators which later can be analyzed for further investigation. Photography is of value measuring an item's accurate site and position with respect to other items which is missing with sketches. Forensic photographs were able to provide the preferred description for many cases (1, 2, 3 and 4).

With the passage of time criminologists realized the value of forensic photography as it could freeze time by producing an evidently definite record of evidence or even victim's at scene of crime (7). Forensic photographs are not only used as a source of providing evidence but also as a blueprint for reconstructing a scene for further processing if required. These reconstructive events can be used to recall the memories of the witness who might saw the culprit without recognizing they had (6). Alphonse Bertillon was first French photographer to record a crime scene with organized investigating systems by capturing images at several distances including ground level and aerial shots. Forensic photographs become an important part of investigation and accusing a crime scene as most of the evidence is temporary. With reference to this statement, it is essential to lift the Fingerprints, take the victim bodies for autopsy and life should return to its normal state. Where the Forensic photographs preserve most of transitory evidences such as blood stain's shapes which is swabbed up, it also signifies the position of evidences placed at scene of crime and their relation to its surrounding area. These types of photographs later can be vibrant to investigating team when

the crime scene is vanished (7, 4).

Despite of videotaping does record everything, still photographs are very important at every crime scene as these can be used for direct comparison. Objective application of the photographs can provide permanent and easily controlled proofs that are capable to bring conviction. Therefore forensic photography can be applied to fix an object for future reference as the camera can sees further that human eye cannot such as scratches or bruises on the victim body, ante-mortem defense injuries and secret writings etc. Similarly forensic photographs give solution for the continuation of a crime by providing an initial appearance of the crime i.e. victim's body and weapon position, shape and size of injury marks. Lastly, to photograph the phase of crime that will not be available in its initial state like those of skid marks (3, 4).

Soon after the discovery of the photography, judicial authorities realized its value as central part of all legal departments and police services. Forensic photographs are authoritative for court hearing and trails if they relevant to the case and provide an enduring visual record of the crime scenes with collected evidence from scene to the judge and jurors (3, 7). This evidence presented into court can be termed as physical evidence. For the proper documentation of the evidence in the court of law, the forensic photographer should have sufficient understanding of mechanics and technical skills (2, 4). Documentation should include information like camera brand, model with serial number, manual setting and photograph's time/date when captured. Doing so can detect any modification tried to be done on photographs. This can be achieved if the referred agency control the chain of custody of all photographs and maintain its integrity and validity (3, 4).

2. Principle of Forensic Photography

Forensic photography introduced a new way to the early detectives with their crime scene sketches by producing photographs that are more real and sound to life than drawings. These photographs can record and document the primary state of a crime scene and technically modest enough to be manipulated as they are drastically deviate from reality (7, 4). It does not take a prescribed time to document a crime scene by capturing photographs. It is influenced by size and condition of crime scene with certain complications including environmental factors such as weather and threat to investigating team. It could have thousands of photographs and hours of work (1). A good photograph of scene should be with precise coverage, sharp focus free from distortion and concerned depth of field (7). To yield proper photographs, following certain rules are followed;

2.1. Secure the Scene

Secure the crime scene as it is after it has been established, as any rearrangement will act as wrong evidence in scene photographed.

2.2. Evaluate Conditions

The scene conditions such as light and weather should be evaluated by adjusting camera settings accordingly.

2.3. Shot the Scene

The entire scene should be captured by using wide range shots and the close up shots to visualize the relationship of scene with over all scene and evidence as follows;

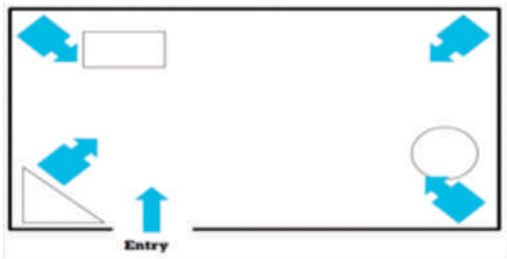


Figure 1: An overview of a crime scene captured with relation to evidences and other objects (1)

2.4. Victims Photograph

Photographs of victims should be highlighted with location, condition and injuries.

2.5. Evidence Photograph

Photographs of evidence should be taken directly at right angles by removing distance distortion for clear vision. Evidence with each part should be photographed with and without scale to show size and relationship with overall scene respectively as in following figure;

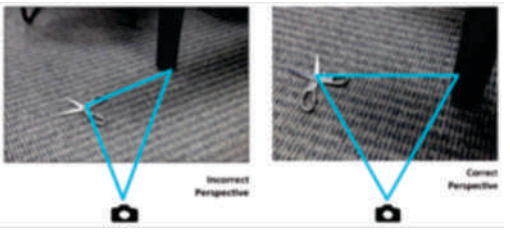


Figure 2: Evidence photography using scale and angles positions for clear visualization (1).

2.6. Mark the Evidence

Crime scene should be captured with and without evidence markers so that to confirm if the scene has been altered, therefore the first shot of entire scene is very essential.

2.7 Reshot for New Evidence

The entire scene including all evidence should be reshot if any new evidence is marked by the investigator. These photographs should have the entire scaled piece of evidence with sizes (1, 2, 3, and 4).

2.8 Use of Special imaging techniques

Distinct techniques and lighting are used for capturing objects like fingerprints, indentations, vehicle identification numbers, shoe print, tire track impressions and tiny parts of evidences as follows;

- **Alternate Light Source (ALS)**

Alternate light source or ALS includes lasers, blue or green lights and colored filters. Colored filters help to detect and illuminate latent fingerprints for photography as in following photograph;

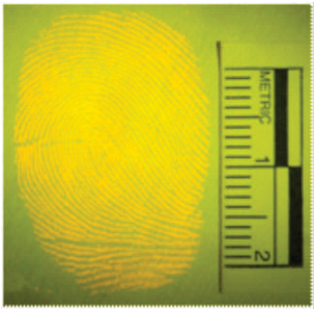
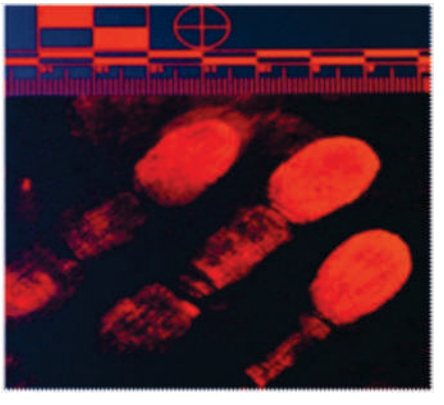


Figure 3: Use of Green Light to illuminate a latent fingerprint (1).

Ultraviolet, Infrared and florescence are used for capturing latent fingerprints go hand in hand forensically. Where the visible fingerprints are photographed without lifting, the latent prints are firstly developed by powder dusting or suspension method and then photographed. Thus reducing the chances of forgery by being invisible genuine for match (3, 8). Fluorescence powders and chemicals are used to photograph the latent fingerprints by enhancing them. Chemical which are naturally fluorescent such as riboflavin present in fingerprint residues, can be noticed earlier to any treatment. However, UV lights and fluorescence powders or liquid dye stains are used for most of fingerprints to fluoresce (8) as shown in the following figure;

(a)



(b)

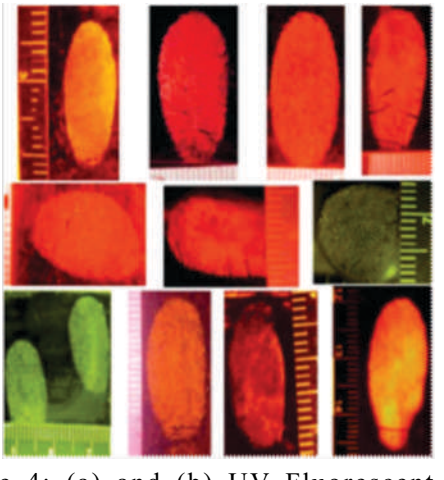


Figure 4: (a) and (b) UV Fluorescent fingerprints (8).

- **Oblique Light**

Flashlights, camera lights and ALS are used at a low angle to produce a shadow that would allow the impressions or fingerprint for photography as shown in following figure (1, 2, 3, and 11);

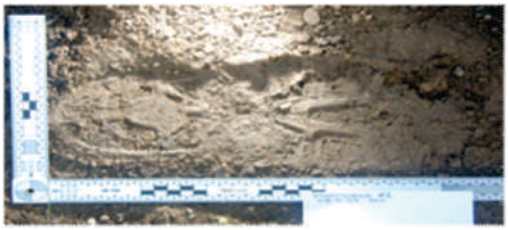
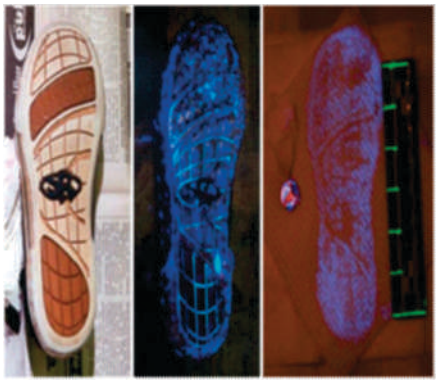


Figure 5: Oblique light used to create a contrast to a footprint (1).

To photograph an impression, the first and foremost step is orientation of impression in the scene. Close-up shots are made by placing a scale on same plane as the impression. Strong colored filters of UV and fluorescence lights are used from different angles to show the finest details of an impression as shown in the following figure (2, 8 and 11);

(a)



(b)

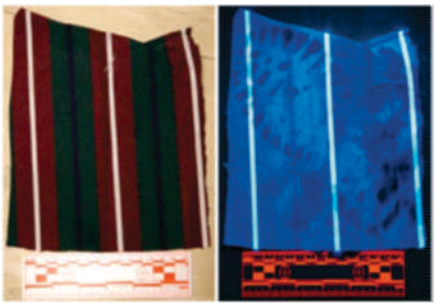


Figure 6: (a) Luminol fluorescing a "cleaned" shoe, (b) UV absorbed by blood (8).

Oblique light with an adequate cross light followed brightness with flashlight can photograph different fingerprint subjects such as dust, wax and clay grease. Low oblique light is used to capture fingerprints on glass and mirrors by placing white card or cloth behind them. Transmitted light or back lightening is used with diffusion screen to capture the fingerprint from perspiration prints left on glass (2, 11).

- **Macro Lenses**

Macro lenses are used for close up photographs of small objects including tool marks, trace evidence and fingerprints as shown cartridge case in figure 7. At the scene, the documents should be photographed accurately with lighting conditions provided. Photographers can add artificial light such as flash light to the photographs after capturing them so that any sort of camera limitation should be avoided (1, 2, 3, and 4).

Figure 7: Cartridge case details photographed with macro lens (1).

Fingerprints are photographed by using macro or close-up lens with gray card for proper exposures. A well detailed fingerprint can be obtained using black and white films which are more contrast (2).

3. Basic Equipment of Forensic Photography

A forensic photography kit might vary based on crime scene or laboratory protocols. Most of the kits have basic camera or even several cameras, electronic flashes, different light source filters, numerous lenses for close up shots, midrange and wide range angles, a tripod, cable release, ruler, gray/index card and protective measurements from rain, cold and heat exposure (1, 2, 4, and 7).

4. Types of Forensic Photographs

Crime scene photographs are of three types mainly overview, midrange and close-ups as follows;

4.1. Overview Photographs

Each and every item of evidence at crime scene is photographed. It is important for individual item to be relevant to the crime scene in order to make a sense to the viewers. Similarly the crime scene also should be relevant to its general surroundings. In such way, the whole view of crime scene questioned is documented by overview photographs. The overview photograph is capture of scene where the photographer stands at possible higher height. This presumes the position of the photographer when the photographs were taken. It is done so to relationship of scene with surroundings. An aerial photography can be done from balcony, a rooftop, using fire ladder truck or an aircraft depending on the nature and location of scene. Often overview photograph is not taken by bending or standing on support to get high but if done then note of this fact should be documented. Also if particular point of view is photographed then it must be documented as note. Adequate photographs can return the judge and jury to the crime scene which is not possible in some cases (4, 8 and 20).

Overview photographs include exterior and interior overviews in both cases of indoor and outdoor crime scene. Exterior view photographs relate to the general surrounding area in relation to crime scene as shown in following figure;

Figure 8: Exterior overview of burglary scene(8).

Interior overview not only includes photographs of scenes that took place inside like a room or car but also the exterior overview including entrance and exits as shown in following figure 9. Photographs of the audiences present at the scene of crime can be used in future to detect witnesses or perpetrators.

Figure 9: Interior overview from corner to corner (8).

4.2. Midrange Photographs

Where the overview photographs deal with documenting the crime scene, midrange photographs record individual items by linking them to the scene before close-ups. Midrange photographs as compared to the close-ups, locates the position of evidence with reference to crime scene like a gun's relation to a door frame, blood stains or to the rest of the scene area as in the following figure;

Figure 10: Midrange photographs of a gun and door frame (8).

4.3 Close-up Photographs

Finally the evidence is documented with close-up shots with marks identifying scares on victim's body or a serial number on tool of crime like knife as shown in figure 11. While capturing close-up images, the photographer needs to take a shot of evidence as it is found in the scene before movement of anything. Then the photographer will capture a duplicate image by using ruler to establish scale (4, 7 and 8).

Figure 11: Close-up series of bloodied knife (8).

5. Photographic Documentation

Using photography in recording crime scene has become a dedicated part of the forensic investigation processing (6). Therefore forensic photography is crucial for the proper documentation of physical evidence in an accurate way for further court proceedings. Following are necessary steps for proper documentation;

- **Lighting;** crimes scene photograph should be taken in day light or using background light.
- **Scale and date;** the injuries photographs should be taken with and without evidence ruler, and must be dated.
- **Body identification;** while photographing, the identification of person/body is important to prove it in court of law therefore the face should be captured properly.
- **Authenticity;** authenticity of photographs should be maintained by recording every process from capturing to presentation in court of law and protecting the captured image by giving trademark.
- **Chain of Evidence (COE);** during the chain of evidence, photograph's origin, usage, storage and evidence processing with its integrity should be clearly documented.
- **Images Storage;** the captured photographs should be transferred to CD-R in any case by storing in locker with limited access.
- **Protection;** computers preserving photographs should be protected with password with limited access. For this purpose special hard disks are used for storage (2, 4, 5 and 8).

6. Photographing Specific Crime Scenes

6.1. Forensic Medical Photography

The aim and objective of medical photography is different. Images taken are primarily used for legal purpose, consequently outcomes should be precise and complete for court use. The photographer should have not only the technical skills of photography but also medical and legal requirements. As the photographs are not repeatable in autopsy cases so forensic autopsy photography should be extremely reliable and followed with minimal delay. A good photograph with clear demonstration and without misleading information can be achieved by using equipment which are easily portable with supplementary mechanical maintenance. For this purpose, factors considered are identification of the body, orientation, background, body color with injuries or spots, lighting, scale and cropping (8, 14) as shown in following figure;

(a)

(b)

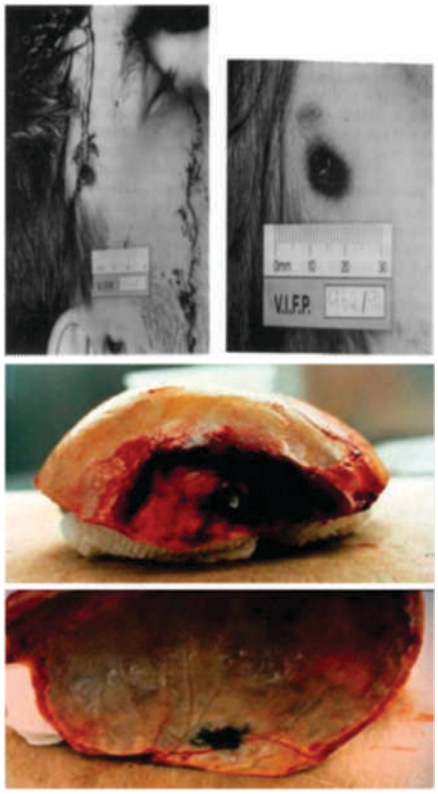


Figure 12: (a) gunshot orientation to the temple (14), (b) Contact gunshot wound to skull (8).

Forensic medical photography has a significant role in preserving injury patterns, bite marks,

bruises and wounds in skin of sexually abused victims as physical evidence as shown in figure 13. It is important for odontologist, pathologist and legal system to accurately photograph these injury patterns. Photographs are the only visual and permanent proof of injuries and wounds on the victim body as there is vast time interval between the crime event and court trials. Therefore proper photographing of injuries as a source of recording and preserving evidence, is imperative for crime scene investigators (13, 14 and 15).

(a)

(b)

Figure 13: (a) and (b) Injuries to rape victim (8).

There is dramatic increase in referrals to physician for medical evaluation including forensic photography as a result of increase in reports of sexual abuse in different age groups of victim. Photographs of significant lesions and injuries with high quality clos-ups can be an imperative part of this assessment. Colposcopes and instant camera systems are required. Medical doctor examining the sexually abused cases should know basics of operating camera, film procedure and medical legal approach to sufficient photography system. Case studies and discussions are carried out by physicians to photograph the victims (8, 13 and 15).

6.2. Forensic Dental Photography

Human identification is now possible by understanding the mechanism of dental identification which is solely based on comparisons between antemortem and postmortem data of the victim. This can be achieved only when modern tech devices used for the prime management of postmortem data and if the victims do have the dental treatment records. In most of the situation the victims do not have such records so antemortem data is approached from personal belongings. One of the antemortem data detected from personal belonging is smile photographs which are considered as common record for dental identification. Such a forensic case in 2011 of an airplane crash has been reported in present study (19) where the antemortm smile photographs were compared with the postmortem dental photographs of the burnt victim. Both of these two data were of discrete physical characteristics and identified the burnt body by the application of the forensic photography using image superimposition technique as illustrated (19) in following figure;

(a)

(b)

Figure 14: Technique of direct comparison between (a) AM and (b) PM photographs, (c) Technique of image superimposition between AM and PM photographs (19).

Similarly, the forensic photography technically digitized termed as forensic digital photography also aids to forensic dental investigation for the record, crime and medical legal purposes. This technical modification assists and improves forensic dentistry practice involving cases of identification, human abuse and considerably the bite mark cases. Photographs of these cases are analyzed by using ALS filters including UV, IR and fluorescent lights as shown in figure 15. Forensic digital photography plays a vital role in forensic investigation mostly collecting and preserving evidences in identification of alive and departed persons. Forensic identification is mainly achieved by the organization and collaboration of multidisciplinary team including forensic odontologists, anthropologists, pathologists and criminalists (12, 16 and 17).

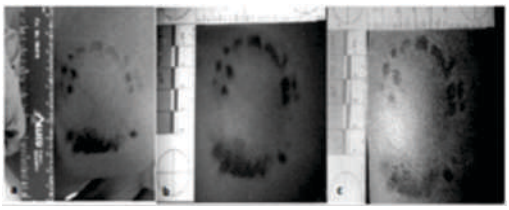


Figure 15: (a) Color image of bite mark on shoulder of black homicide victim, (b) fluorescent image, (c) UV image (16).

6.3. Forensic Facial Photography

With an increase use of the photographs on individual genuine papers of identity including ID cards, passports, security cards, credit cards and driving license, has increased the fabrication of such documents with perpetrator's photographs for the purpose of committing crimes. These altered photographs are used as valued physical evidence for the comparison of the known photographs of the suspects with some individual characteristics left on the evidence. These individual characteristics include facial features such as size, shape (nose, eyebrows, mouth, ears, forehead creases), scars, moles, dimples etc. With the ease and enhanced technology of forensic photography and anatomical morphology, now it is possible to compare facial symmetry and anthropometric measurements for shortlisting the suspects (21) as shown in following figure;

(a)

(b)

(c)

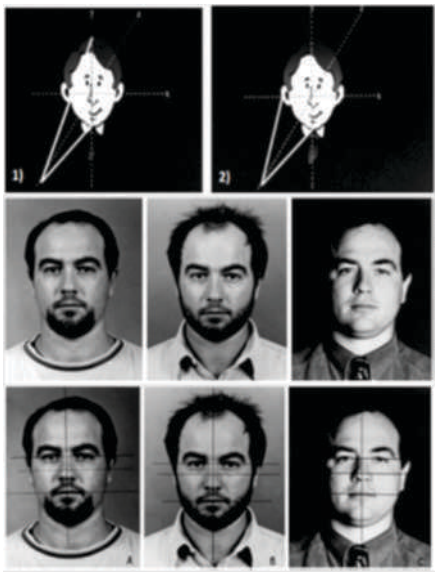
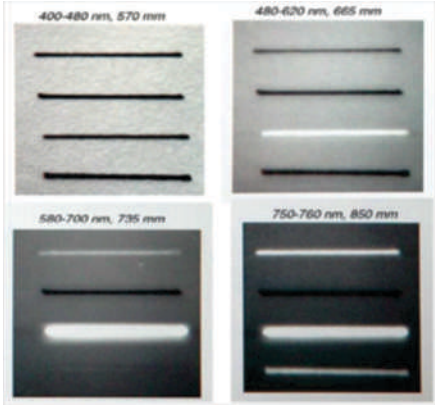


Figure 16: (a) Distance relationships from a camera viewpoint to two points on (1) the vertical axis (2) the horizontal axis, (b) three photographs of one of the authors used as the case study to demonstrate the examination technique, (c) Photographs displaying anthropometric orientation lines (21)

6.4. Forensic Handwriting Photography

Forensic photography also adds to the handwriting examination by detecting various kind of ink in solving a forgery or simulation. Different light sources such as Infrared and Ink Fluorescent are used to visualize the handwriting photographs with simulation, alteration and obliteration etc. The dyes and pigments present in ink react to these lights by showing numerous special effects even similar shades of ink that appear black, shows drastic changes as shown in following figure (3, 8);

(a)



(b)

Figure 17: (a) Inks reacting to various lights, (b) Ink fluorescing and transmitting IR in altered check (8).

6.5. Forensic Photogrammetry

Forensic photogrammetry is the application of photogrammetry in the field of forensic sciences. It involves the extraction of measurements from the crime scene photographs. It has been used not only in all disciplines of forensics but also other industries. It has been a practical tool to provide better information to the investigators, lawyers and insurance adjusters. Forensic photogrammetry is applied to obtain an accurate 3D reconstruction of the crime scene or an accident that would determine later the suspect's dimension (position and distance) with respect to scene (22, 23). All photographs after the application of photogrammetry are useful to recover or preserve data that can discover new piece of crucial evidence for measurements to an investigator even after several years.

Forensic photogrammetry can be used for several forensic applications such as measurement of crime scene mapping, crush on damaged vehicle, skid mark, bullet trajectory, blood spatter, suspect height, shoe and tire print as shown height measurement in figure 18 (8, 22 and 23). Two types of photogrammetry are used in forensic photography including close-range and aerial photogrammetry. Close-range photogrammetry uses everyday cameras to create 3D image and recover the lost items and locations for archeological, architectural, engineering and forensic purposes. The aerial photogrammetry is used for topographic maps such as terrain-mapping from an air craft. Tools required for forensic photogrammetry of crime scene are six or twelve inch ruler, ABFO scales for bite marks or fingerprints, bureau scale for foot prints, and twenty five and one hundred foot tape measure for drawing and drafting (22, 23).

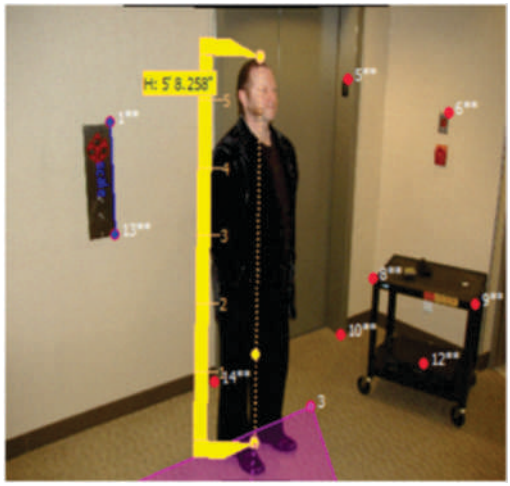


Figure 18: Height measurement with respect to surrounding area from scene photograph (23).

7. Conclusion

Forensic photography plays enormous role throughout the entire investigation by creating a stable visual proof of the crime scene and evidence found in original state. It reconstructs the event of the scene that took place by giving a clear image to the jurors in the court room. Earlier photographs were not considered as evidence but a source to give a visual record of crime scene and evidence location within the scene. Forensic photographs gives not only overall view of the crime scene and the relevant evidence but also the surrounding details such as weather, timing either day or night time. Such photographs include fingerprint, footprint or tire track impressions, bloodied body or assaults injuries, burglary scenes, homicide or murder scene and any tools committing crime such as a knife or gun etc. These photographs can be best captured if the photographer has a sufficient skill and training of using camera. Special techniques such as UV, IR and Fluorescence filters are used in order to capture the undetectable evidences. Proper documentation of the photographs with every signal details from case name to location and maintained chain of custody make them admissible in court room.

8. References

[1] National Forensic Science Technology Center (NFSTC), "A Simplified Guide to Crime Scene Photography," Bureau of Justice Assistance (BJA), award #2009--➥D1--➥BX--➥K028. Available: info@nfstc.org.

[2] S. Gouse, S. Karnam, H. C. Girish and S. Murgod, "Forensic photography: Prospect through the lens," Journal of Forensic Dental Sciences, vol. 10(1), January-April 2018. Available: www.jfds.org.

[3] R. Rohatgi and A.K. Kapoor, "Importance of Still Photography at Scene of Crime: A Forensic Vs Judicial Perspective," Journal of Harmonized Research, vol. 2(4), pp. 271-274, 2014. Available: www.johronline.com.

[4] Forensic Science Training Unit FBI Laboratory, "Fundamental Principles and Theory of Crime Scene Photography," National Criminal Justice Reference Service, Feb, 1995. Available: NCJRS.gov.

[5] K. Mancini, "Forensic Photography," Westchester.gov.com. Available: www.westchestergov.com.

[6] J. Claridge, "Forensic Photography," Forensic Explorer.com, 1 Jan, 2017. Available: www.exploreforensics.co.uk.

[7] S. Dowdey, "How Crime Scene Photography Works," Science.howstuffworks.com, 2019. Available: https://science.howstuffworks.com/crime-scene-photography.htm.

[8] M.R. Edward, "Crime Scene Photography," Elsevier Inc. 2nd Ed, pp 1-685, 2010. Available: http://www.elsevierdirect.com/companions/9780123757289.

[9] A. Wittmann, "Overview of the Forensic Photography," J Forensic Science & Criminal Investigation, vol. 2(2), 2017. Available: DOI: 10.19080/JFSCI.2017.02.555581.

[10] A. Bell, "Crime Scene Photography in England, 1895–1960," Journal of British Studies, vol. 57, pp. 53–78, January 2018. Available: https://www.cambridge.org/core.

[11] N. Marin and J. Buszka, "Forensic Photography Techniques," eBook, 1st Ed. Pp. 92, September 2014.

[12] G.M. Gordon and M. Steyn, "An investigation into accuracy and reliability of skull-photo superimposition in a South African sample," Forensic Science International, vol. (216), pp. 1–6, 2012. Available:www.elsevier.com/locate/forsciint

[13] E. Vogeley, M. Clyde and G. Bertocci, "Experience with wood lamp illumination and Digital Photography in the documentation of Bruises on Human Skin," Arch Pediatric Adolescent Med, vol. 156, pp. 265-268, 2002. Available: https://archpedi.jamanetwork.com.

[14] A.P. Henham and K.A.P. Lee, "Photography in forensic medicine," Journal of Audiovisual Media in Medicine, vol. 17, pp. 15-20, 1994.

[15] L.R. Ricci, "Medical Forensic Photography of the Sexually Abused Child." Child Abuse & Neglect, Vol. 12, pp. 305-310, 1988.

[16] S.G. Gregory, "Forensic Photography," Research Gate, 201-242, 1997. Available: https://www.researchgate.net/publication/285100083.

[17] N. Balaji, S. Senapati and M.K. Sumathi, "Forensic Digital Photography," A Review. Int. J Dent Med Res, vol. 1(3), pp. 132-135, 2014. Available: www.ijdmr.com.

[18] J.H. Wagner and G.M. Miskelly, "Photography of blood," Journal of Forensic Sciences, vol. 48(3), pp. 593-603, 2003.

[19] R.F. Silva, A. Franco and J.B. Souza, "Human Identification through the Analysis of Smile Photographs," Am J Forensic Med Pathol, vol. 36, pp. 71–74, 2015. Available: www.amjforensicmedicine.com.

[20] H.J. Kim, S. Lim and J. Moon, "A photographic forensic case study: Myths, principles and techniques," Mathematical and Computer Modelling, vol. 55, pp. 3–11, 2012. Available: doi:10.1016/j.mcm.2011.01.001.

[21] G. Porter and G. Doran, "An anatomical and photographic technique for forensic facial identification," Forensic Science International, vol. 114, pp. 97-105, 2000. Available: www.elsevier.com/locate/forsciint.

[22] M. Mayda, "Forensic Photogrammetry." Available Int. J Dent Med Res, vol. 1(3), pp. 132-135, 2014. Available: www.ijdmr.com.

[23] "Forensic Photogrammetry," DCM Technical services Inc. Available: http://www.dcmtechservices.com

Tariq et al LGURJCSIT 2019

LGU International Journal for
Electronic Crime Investigation

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

Research Article

Vol. 3 Issue 2, April - June 2019

Advanced Password Stealers

Muhammad Arslan Tariq[1], Wahid Qayyum[2], Rehmatullah[3]
Email: arslan.tariq@lgu.edu.pk[1], wahidqayyum@lgu.edu.pk[2],rehmatullah@lgu.edu.pk[3]
Lahore Garrison University Lahore, Pakistan

Abstract:
People have access to everything available online and uses services given by others that also brings a great amount of risks. Everyone has something which is valuable to him, he wants to keep it private from others and uses password to protect it. A Password may be of any kind. But there are also some people who are intruders and wants to steal others passwords for different purposes. This research paper is regarding the study of password hackers/stealers. Let's discuss about the passwords Stealers types malicious persistent programs and key loggers. some embedded drivers with these programs and some case scenarios where hackers have been successful in stealing information, even now a days where modern world has done tremendous achievement regarding information security issue why these hackers have been so successful? In this paper, we will also share some tips to save ourselves from such hackers and in this paper, we will try to clarify the difference between spyware key loggers and other password stealers.

Keywords: Ransomware, Advance Malicious Software, Ransom amounts, Ransomware types

1. Introduction

People use to steal password for their own benefit. For instance, some are having psychological disorders, they steal password to tease others and blackmail them. Some steals passwords or hack someone's account to get money. Although there are different ways by which we can overcome them and protect our accounts and data [1].

The word password stealer means any code i.e. software program or technique to steal someone's private information. Such as username, passwords etc. in normal life we don't save are passwords in computer or in any other database because we don't have a lot of passwords to keep in mind. so, we use to take some of our password in our mind just. But sometimes business Mans and other people used to save their passwords or private information in some highly encrypted databases. Stealer don't only steal user's password they can also perform some malicious activities. Which are discussed below it can also Steal user's private information. Example keystrokes pictures access point names but if we have threats then on the other hand also have ways to minimize them. now a day's main password stealer are spywares browser hijacker commercial spywares route kids remote access tools rat key loggers dictionary attacks brute force attacks [2-3].

2. Password Stealing Methods

There are different types of password attacks performed by someone to steal password. One can easily find someone's password by dictionary attack. If a user has set alphanumeric password than it can easily be broken by this attack.

Password stealer may also threat physically the user to get his password. Now people use to put an extra Scanner (reader) on your ATM machines so they can easily get access to your pin and do whatever with your account.

Wi-Fi router can also be used to get passwords of users. One can access the router and have all the passwords and activities that you are performing.

Viruses and software are also used to steal

password nowadays. Key logger is installed on someone's system that keeps on recording the passwords from that system. One can also create a virus of specified target which can be an image or any file. If you open that file it disappears and goes into the root of system and does its work (Password Stealing). Different types of cyber-attacks are performed to steal password country to country. Fingerprints can also be easily stolen by different ways. Brute Force attack is also famous in password stealing techniques. It can discover credentials [4].

3. Fundamentals of Password-Stealers

A. Dictionary attack:

In this type of attack still try to login by applying combination of common words as compared to brute force attack where large number of keys are searched automatically the dictionary attack applies only possibilities those are likely to succeed typically choose from list of words in simple words we can say that dictionary attack deals with dictionary words example, (Run) (rain) (road) etc. these are easily predictable words [5].

B. Key logger:

To track the keystrokes of user a hacker uses the special program so everything the user types including login IDs passwords etc. will be recorded to that program it's different as compared to dictionary attack or brute force attack because the key login program can be a Malware or a virus that first hacker have to throw in the users device and hacker has to trig the user to download it then it's ready to work a logo attacks are very harmful and Unstoppable sometimes because even strong password don't provide protection against them [6].

C. John The Ripper:

It is the modern password cracking tool used for UNIX Linux and Mac yes it's Windows version is also ready to use now it can find week password but its upgraded version provides better performance you can download John the ripper from the link below in reference.

D. The Hydra:

The fastest password cracking tool as compared to other similar tools is hydra, one can add module easily in it it's available for Windows OS x Linux this tool can perform its task on certain networks protocols.

E. Key logger

Is basically we can say that a type of program or a software that hacker first have to enter in the victims device once the victim has installed a keylogger in his device then victim is totally hacked by the hacker because now anything that a vector can perform in his device is visible to the hacker and hacker can do any malicious task with the victims information or personal data [7].

F. Osx Linux

This is basically a tool that can perform its task on different network protocol example: CVs, HTTP form, Oracle listener and many more [15].

G. Brute force attack

With the help of script awesome computer programs, I have tries to get into someone's personal information with the possible combination of different type of logins and password such type of attack is known as the brute force attack [13].

H. Brutus

Brutus it is one of the most famous online crackers available in Google it is easiest to find and the thing which Rises 8 in the list of hacking tools is that it claims that it is the fastest online password cracking software/ tool. This tool is free of cost means you have to pay nothing to download it and use it but the fall in this tool is that it's available only for the windows version means if you are using Linux or any other operating system then you cannot use this tool [8].

4. Protection against Attacks

Privacy can be attained for securing your data and accounts by making a complex password. If password is lengthy, it will be difficult for intruder to guess it. Let me tell you one thing that, no one can say my password is unbreakable or can be stolen, It's just the matter of time [10].

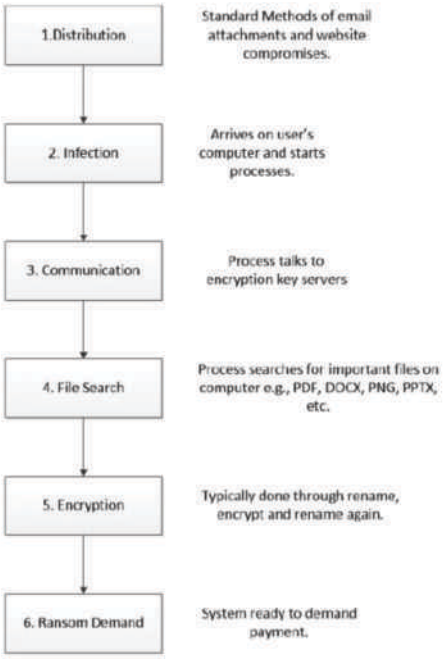


Fig.1. Ransomware Execution Steps

5. Creating Secure Password

Use special characters (! &%@), capital letters (ANSM) for password. Here are few examples of a secure enough passwords " x$5WT_@! nk4G ", "O=VbK$by_l! (". If your password is lengthy enough like more than 20 characters than it will take years to break it. Keep on changing your password every third week depending upon the sensitivity of your data. Do not share your password with anyone. Not only accounts but keep track of your Wi-Fi router password too. Do not use passwords resembling names, cities and streets. In case you want to send password to someone you can send it in a sentence like: "I am going to Eva Street#4 at 11 o clock in Morning". Here password is "EvaS#411M" [9].

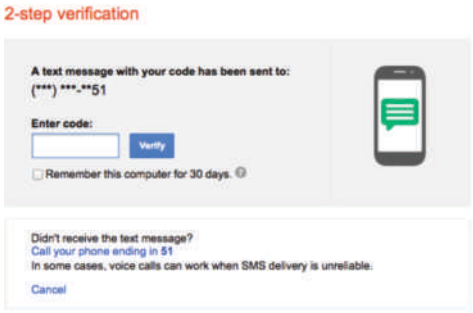
6. Graphical Password

Matching different points in an image is known as graphical password. This type off passwords are not very often.

Fig.2. Percentage of New Families of crypto ransomware, Lockers, Misleading Apps & Fake AV between 2005 and 2015

7. Second Step Verification

Everyone should enable second step verification for their emails and other accounts. If someone gets your password and tries to login, he will fail at this step because you are having your phone number registered at site on which you will receive pin for verification [11].



8. Conclusion

Now a day's hackers are advanced as compared to past and have more functions example as pivot Steels all the history of users search but there are a lot of ways to remain safe from such attacks one have to look the background services with the passage of time and look for the open port if found then close them and make sure that they were not opened by any hackers attack especially for programmers and Developers there are some patterns and procedure by which they can protect them from these attacks memory scans are also helpful to remain secured [12].

Today in the modern world as hackers and Thieves are more moderate and have more skills to catch and get someone's personal data or

personal information, it's a great threat to all the human beings but the good thing is that if we have some threads then we have a lot of ways to save ourselves from such kind of attacks one have to look towards its open ports in the background with the passage of time and if found some ports which are open then close them instantly and try to make it sure that the ports were not open by any malicious attack or any hackers attack [14].

9. References

[1] Ronny Richardson and Max North, “Ransomware: Evolution, Mitigation and Prevention,” Information State Department. Kennesaw State University, GA USA, vol. 13 No. 1, 2017.

[2] Hirra Sultan, Aeel Khalique, Shah Imran Alam and Safdar Tanweer, “A Servey on Ransomware: Evolutiobn, Growth, And Impact,” in Department of Computer Scince, School of Engineering Sciences &Technology Jamia Hamdard: vol 9, No. 2, March-April 2018.

[3] G. O’ Gorman, G. McDonald, “Ransomware: a growing me-nace”, White Paper, 8th November 2012, Symantec.

[4] J. Crowe, “Ransomware growth by the numbers: ransomware statistics 2017”, June 2017, Barkley.

[5] Nilesh Chakraborty Samrat Mondal "Towards Improving Storage Cost and Security Features of Honeyword Based Approaches" 6th International Conference On Advances In Computing & Communications ICACC 2016 pp. 6-8 September 2016.

[6] Manisha Jagannath Bhole "Honeywords: A New Approach For Enhancing Security" International Research Journal of Engineering and Technology (IRJET) vol. 02 no. 08.

[7] S Venkadesh K. Palanivel "A Survey on Password Stealing Attacks and Its Protecting Mechanism" International Journal of Engineering Trends and Technology (IJETT) vol. 19 no. 4 Jan 2015.

[8] Juels Ari L. Rivest Ronald "Honeywords:Making Password-Cracking Detectable" International Conference on Science and Technology 2015 RMUTT ACM SIGSAC Conf. Comput.Commun. Security 2013.

[9] Imran Erguler "Achieving Flatness: Selecting the Honeywords from Existing User Passwords" IEEE TRANSACTIONS ONDEPENDABLE AND SECURE COMPUTING vol. 13 no. 2 MARCH/APRIL 2016.

[10] Kelly Brown "The Dangers of Weak Hashes" SANS InstituteInfoSec Reading Room.

[11] Joseph Jaegery Thomas Ristenpartz Qiang Tangx Honey Encryption Beyond Message Recovery Security February 2016.

[12] Ari Juels Thomas Ristenpart Honey Encryption: Security Beyond Brute Force Bound January 2014.

[13] A. Juels T. Ristenpart "Honey Encryption: Encryption beyond the Brute-Force Barrier" Security Privacy IEEE vol. 12 no. 4 pp. 59 July-Aug. 2014.

[14] A. Vance "If Your Password is 123456 Just Make It Hackme" The New York Times vol. 20 2010.

[15] Prashant Dhas Ismail Mohammed "Efficient Approach for High Level Security Using Honeywords" IJARCSSE vol. 5 no. 11 2015.

[16] Nirvan Tyagi Jessica Wang Kevin Wen Daniel Zuo "Honey Encryption Applications" in 6.857 Computer &Network Security Massachusetts Institute of Technology Spring 2015.

Malik et al LGURJCSIT 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 2, April - June 2019

Ransomware Detection and Defense

Muhammad Shairoze Malik
Lahore Garrison University, Lahore.
shairozemalik@lgu.edu.pk

Abstract:
Like other criminals in world, cyber-criminals are using different illegal and unethical ways to gain their mischievous purposes. Malware known as Ransomware is a new threat to world used by cyber hackers to blackmail individuals and organizations and has been identified as a major threat to network and computer security across the world [1]. Ransomware lock victim's computer by encrypting user files and demands payment often in crypto currency i.e. Bitcoins to give access to files. Research showed that 19,750 victims paid over $16 million as ransom payment in two years [2]. Due to increasing amount of ransomware attacks, different software and hardware level techniques are proposed to detect and mitigate ransomware attacks and to recover user files without ransom payment. Pay Break is a proactive defense mechanism on software level against ransomware that allow victim to recover files without any ransom payment. Furthermore, ransomware variants could get kernel privilege, that let them to shutdown software-based system defense. Considering this, first hardware level defense system is proposed named Flash Guard which is resistant against ransomware that use kernel vulnerabilities.

Keywords: Security, Privacy, Ransomware, Ransomware Detection, Cyber-Defense, Malware, Pay Break, Flash Guard

1. Introduction

Cyber-criminals are using new approaches to make money illegally. Malware known as Ransomware is a new threat to world used by cyber hackers to blackmail individuals and organizations and has been identified as a major threat to network and computer security across the world [1]. Ransomware is a modern approach adopted by cyber hackers to enhance their profit. Ransomware is the most visible growing threat to all users. It comes in different forms and shapes. It holds user files "hostage" until it is paid by victim. Ransomware variants were introduced in late 1980s but modern age of ransomware started in 2013 with Crypto Locker. Ransomware is a malware that attacks user machine by using system vulnerabilities and available methods. It silently encrypts user documents and media and then demands for ransom payment to recover data. Young and Yung were the first to give the idea of file encrypting ransomware in 1996. Their explanation is a perfect picture of current most successful crypto based ransomware families that use encryption to threaten users into paying ransom. Attackers are now more sophisticated and business minded. In start, initial victims were individual systems (regular people) but now they target business sector as ransomware attacks are successful against businesses and they can get more profit from them by halting their productivity. This situation is very torturing for both individuals and businesses. Some of the dangerous forms of ransomware include Crypto locker, Crypto wall, CTB Locker, Tesla Crypt or WanaCry. Digital extortion has increased significantly in last couple of years as the number of online application and smart devices continue to grow [2]. The impact of ransomware is so huge that it is now rated as the biggest cyber threat that hit the market [3].

These attacks are shifting focus to organizations. For example, the Hollywood Presbyterian

Medical Centre in the United States was attacked in February 2016. They were hit by Crypto Ransomware and were forced to shut down. The ransomware encrypted the files, denying hospital access to health records [4].

According to FBI (Federal Bureau of Investigation), due to ransomware attacks estimated losses of about $1 billion US Dollars was incurred in the year 2016. Out the people affected by the attack, nearly 40% of victims paid the ransom. Unfortunately, current preventive methods are not adequate enough to handle the effects of such attacks [7] [10].

Ransomware payloads and malicious binary codes use techniques that make it difficult to detect or analyze. In response to ransomware attacks, it is important to develop tools or techniques that can extract ransomware behavior and improve detection systems. Malwares use almost common evasion methods to evade known detection techniques to attack end user. Techniques to detect, analyze and mitigate ransomware attacks are not different from other methods of identifying malicious attacks. Ransomware use similar approach like other attacks for example opening email attachment or clicking on advertisement can be the cause of attack on user side. Security research groups are working to investigate what particular problems in exposing ransomware attack are similar to other malicious attacks and which are independent in characteristics and need more attention [5]. Several detection and defense systems have been proposed by researchers that use cryptographic algorithms and file access features or patterns to identify and mitigate ransomware attacks.

2. Background:

WanaCry hit thousands of users. Many public and private sectors become victim of this ransom attack. This attack utilize kernel vulnerability, encrypts user data and asked for bitcoin payment to unlock files. So concerned increased after large number of high profile ransomware attacks that how to fight against them [5].

PC Cyborg was first ransomware variant reported in 1989. The encryption algorithm used was symmetric cryptography and was easily decrypted [11]. Another ransomware GpCode also employed custom symmetric encryption, first discovered in 2005, and improved over time to become more and more sophisticated [12-13]. Reveton, also known as Police Ransomware, spread through pornographic websites, it changes extensions in win/system32 folder and display notification pages to victims [14][15].

Ransomware authors usually choose between symmetric and asymmetric cryptography. Old ransom versions were based on symmetric encryption, which were quickly reversed by malware engineering and provided decryption instruments. So ransomware attacks were defeated because of their weak cryptology. Malware authors decided to ignore the popular adage “don't roll your own crypto” [8]. Malware authors learned from their past mistakes and started implementing strong hybrid crypto algorithms in their attacks. Besides this, some modern forms of ransomware use kernel privileges for attack. To deal with ransomware attacks and to achieve data recovery capability, it is important to study the behavior of ransomware and its interaction with user data. Research showed that malware locks user data speedily and size of encrypted data is comparatively small. They try to remove any means through which victims could recover from the attack without paying [9]. Proactive detection and defense mechanism is required and for this security research community proposed different tools and techniques like UNVEIL uses the kernel as the module to search for file system activities. CryptoHunt identifies malicious binary code cryptographic functions when attacks use custom cryptographic functions [5]. CryptoDrop detects ransom through the inspection of programs, their activities and user data changes. Redemption implements abstract model that contains behavior or characterization of a large dataset of ransomware attacks to identify malicious process [5]. Pay Break is a new mechanism of protection. It stores cryptographic encryption-keys securely in the key vault and allow victims to recover their ransomed files without paying [8]. Flash Guard, a SSD (Solid-State Drive) has a firmware-level recovery system through which fast, efficient recovery from ransomware encryption can be done without relying on backups [9]. In this paper we will focus on detection and defense techniques particularly Pay Break and Flash Guard.

3. Detection and Defense Techniques:

During the year of 2016 just, a large scale of crypto-ransomware attack occurred on north

American universities, which impacted the university computers & services. Systems were taken offline, as university did not pay the ransom of amount $38000 to release the encrypted file. Recovery took many days to normal the services. Ransomware focuses on controlling system resource's, encrypting data files and holding the decryption keys to demand the ransom. Malware is first distributed to victim`s machine. Once its executed, it encrypts files and notify user by altering that contents are encrypted and they will be lost unless they pay ransom. Ransom note either have unique ransom address or a link on that note for payments to be done against ransomware. They choice Bit coin as their payment method as its decentralized and unregulated. Ransom also includes how to purchase bitcoins and from which exchange [9]. Researchers tracked ransomware end to end by combining multiple data-sources including ransomware binary, victim telemetry, seed ransom payments, and bit coin addresses. Over $16 million US Dollar ransom payments made by 19,750 victims in span of 2 years [9]. Ransomware usually target those users who do not follow good practices [6]. In this response, users are instructed to backups their important data [9]. Back up is reliable defense against ransomware but back up devices had only those data which had last time backup, so this can be prevented by educating people, by proper communication and by upgrading to new technologies in terms of software and Hardware upgrade. To fight against ransomware, it is important to develop methods that can increase evasion costs, upgrade malware detection systems, and help malware analysts to unmask the internal functioning of malicious code [5].

3.1 Enhancing Detection / Monitoring Techniques:

Dynamic analysis technique is good in analyzing malicious binary code and extracting behaviors or functionalities of malware sample [5]. Bare-metal automated analysis known as Bare Cloud technique is proposed by Kirat and colleagues. It doesn't have any in-guest monitoring component which makes this solution more robust against current bypass techniques [5]. Bare-Cloud extracts the behavioral profile of the malware from its network level and disk level activity. The disk level activity is obtained by comparing the system's state after each execution of malware with the initial clean state. With the understanding of the OS of the analysis host, Bare-Cloud also obtain operating-system-level changes, such as changes to system files and registry keys. Network-level activities are captured as a stream of network packets. For valid monitoring, it is important to know how malware author use cryptosystems, how encryption keys are generated and how attack make user data unreachable. UNVEIL technique use kernel as module to look for system activities [16]. It monitors user processes that have interaction with file system. File monitoring system in UNVEIL gives full view of all file system modifications as it has access to buffers that deals with I/O calls [5]. Another technique named CryptoHunt is introduced by Xu and colleagues. It identifies cryptographic functions in malicious binary code as attacks use customized cryptography functions to bypass detection instead of known crypto functions. Research showed that customized crypto functions are not coded well so recovering encrypted data is easy [5].

3.2. End-Point Protection Systems:

End point solutions are proposed to monitor operating system resource usage to stop attacks once data starts encrypted by ransomware.
Software Level Support
CryptoDrop is an early warning system for ransomware attack [17]. It detects ransomware by inspection of programs, activities and changes to user data. It alerts user and suspends suspicious process. 3 primary (File Types Changes, Similarity Measurement and Shannon Entropy) and 2 secondary indicators (Deletion and File type Funneling) are identified to create strong detector to mitigate ransomware. Hence parameters are set in system for quick detection with low false-positives. This way ransomware can be prevented from completely encrypting a victim`s files and mitigates the amount of victim data loss.

3.3. Pay Break

It is protection tool against hybrid crypto ransomware attacks. In hybrid crypto system, attacker use symmetric key to encrypt each file. This symmetric key is termed as Session Key. The session key is then encrypted with public key of attacker and saved it together with encrypted file contents. So in this case attacker is

generating a symmetric key pair on his command and controlling whole game [8]. Malware authors use cryptography into their malware codes by dynamically linking against system provided crypto libraries or statically linking libraries that are embedded into executable application code. It is observed that two famous ransomware families CryptoWall and CryptoLocker are using the same APIs that windows are using for cryptographic functionality and is guaranteed to be present on every windows installation. Practically encryption is doneon the victim`s machine in ransom attack. This characteristic of attack helps in designing Pay Break to fight against modern ransomware. Pay Break consists of three components (Hooking, Key Vault and File recovery) that together make cohesive system to recover encrypted files [8]

4. Hooking Crypto Function:

Pay Break support both linking libraries. It looks for procedures in dynamically linked libraries by their name and address and statically linked procedures by Fuzzy Byte Signature. Pay Break use hooking scheme that helps to export session keys, algorithms and its parameters used for symmetric encryption [8].
Dynamically Linked Libraries Hooking.
In Microsoft, encryption through Crypto API is performed by using Crypt Encrypt Function. Ransomware based on CrytoAPI uses Crypt Encrypt function to do encryption of files. Hooking is done in Crypt Encrypt function to securely export the keys. Moreover, pay break hooks the CryptAcquireContext and CryptSetKeyParam functions to know about the algorithm used for encryption and to obtain cipher mode, initialization vector parameters. Base material that is used to generate session keys and which is used by ransomware by linking libraries dynamically or statically is stored by Pay Break via hooking scheme [8].

4.1. Statically Linked Libraries Hooking:

Statically Linked libraries are placed into the executable code of the application. Pay Break use a slightly different approach when ransomware statically links a cryptographic library. Cryptographic procedures are identified and hooked by Pay Break at runtime in process memory. Pay Break rely on signatures to identify statically linked crypto libraries. Pay Break Prototype is compatible with signatures for Crypto++ statically linked library. Pay Break scans memory of all executed processes for function signatures. Hook is placed when signature is identified at its address. Hook then securely exports the Crypto++ session keys and algorithm details [8].

4.2. Key Vault

Key vault stores symmetric session keys and algorithm details with its parameters (i.e. IV and block cipher mode) that are extracted from hook to recover encrypted data. User public key is used to encrypt and export session keys securely to key vault and key vault itself is secured by user`s private key. Public and private keys of user are generated during installation of pay break. Pay Break uses 2040-bit RSA keys for secure encryption of data [8].

4.3. File Recovery

Last component of Pay Break is Recovery of files that are encrypted during ransomware attack. File recovery works in 3 phases.

1. Key vault is decrypted with user`s private key.
2. Data in vault i.e (symmetric keys and their corresponding encryption algorithms with parameters of block cipher mode and IV are analyzed minutely.
3. Finally, victim`s encrypted files are recovered by retrieved session keys.

Each file encrypted with ransomware have meta data such as file length, encryption date, encryption key. Because of this metadata, actual encrypted file data is offset in files held for ransom. Pay Break decrypt file with each possible key and offset until decryption state is reached [8]. See figure below [18]

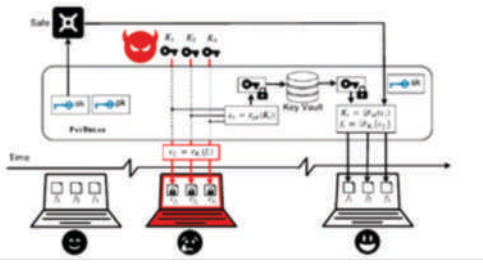


Figure 1: Overview of Pay Break

Research showed that Pay Break defeated 12 of 20 active ransomware families. Files are successfully recovered that are encrypted by CryptoWall and Locky. Locky encrypted 982 files which were recovered in 40s and CryptoWall encrypted 204 files and were recovered in 86s. Pay Break gives the ability to fight against ransomware by using multiple cryptographic libraries including Microsoft Crypto API and Crypto++. To eliminate remaining, respective static / dynamically linked encryption libraries & functions can be hooked with Pay Break [7]. See figure below:

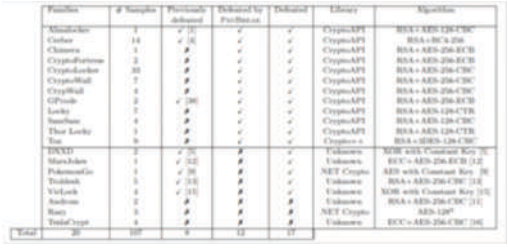


Table 1: Active Ransomware Samples

Redemption another ransomware protection tool is introduced besides PayBreak and Cryptodrop. This detection technique is based on abstract model that holds behavior or characterization of large class of ransomware attacks is implemented. A process is marked as malicious if its behavior matches with the behavior recorded in abstract model [5].

5. Hardware Level Support:

5.1. Flash Guard:

Modern ransomware now using approach to run with administration privilege to load kernel code and carry out attacks on kernel level. They obtain kernel privileges to terminate software-based defense systems such as anti-virus or to destroy backups. To defend ransomware without depending on software-based solutions and backups, idea of Flash Guard-Solid State Drive (SSD) is proposed which has light weight hardware-assisted data recovery system and is resistant against ransomware. It has firm-level recovery system that provides efficient recovery from encryption ransomware without relying on backups. It is based on the out-of-place characteristic of an SSD. SSD keeps old copies of pages that are updated or deleted until they are reclaimed by the garbage collection process [9].

5.2. Design and Implementation:

Flash Translation layer (FTL) in new SSDs consists of four data structures. Flash Guard technique is based on Solid State Drive data structure. It modifies garbage collection process of SSD to keep copies of data encrypted by ransomware and to ensure data recovery. It consists of two major components, a tool for data recovery and (RFTL) Ransomware Flash Transition layer. SSD data structure works with other components of Flash Guard. It is very hard to track the pages that are encrypted. RFTL is proposed to track invalid pages resulted from ransomware attack.

RFTL use existing FTL structure with additional Data Structure RTT (Read Tracker Table). Ransomware encrypt data by reading from disk and then overwrite/delete original copy. RTT is used to track pages that has been read and to check if it is valid or not. Each entry is a read bit map indexed by a block address [9].

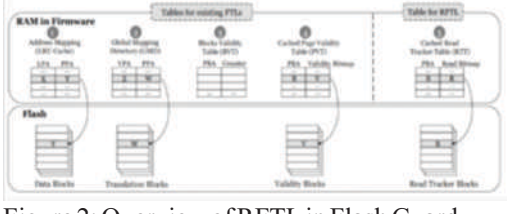


Figure 2: Overview of RFTL in Flash Guard.

5.3. Garbage-Collection in Flash Guard:

Garbage-collection is key component in SSDs, it provides free blocks for future use. It plays important role in keeping invalid pages (old copies) of the data exploited. A new garbage collection (GC) scheme in RFTL is proposed to make Solid State Drive capable of keeping data for recovery. Traditional GC looks for number of valid pages in each block by using Block Validity table (BVT) and to ensure whether block is garbage-collected or not. Once block is highlighted as GC candidate, PVT (Page Validity table) is accessed to verify which pages are valid and should be moved to new free block.

The GC in RFTL follows the basic procedures of FTL including block selection and valid page movement. Invalid pages whose RIP bit is not set, and has been read as indicated by RTT, are treated as pages to be kept. RFTL copy retained invalid pages kept in flash device for a certain time or all encrypted writes which means all invalid pages that have been read will be kept in

SSD. It will keep retained invalid page until it is expired. Old copies (invalid pages) are collected by garbage collector (GC). RFTL takes retained invalid pages as valid pages and the blocks carrying these retained invalid pages will have their GC delayed. RFTL will delete those that have never been read and garbage collect it. The idea behind this is that before encryption data is read by ransomware from SSD, so pages that have never been read are not damaged data [9].

5.4. Data Recovery:

Flash Guard use its OOB meta data to reconstruct user files. It uses previous physical page address stored in metadata to reverse invalid page to its previous version. Recovery tool in Flash guard sort invalid pages with their LPAs and time stamp to recover original file. Flash guard keep all versions of invalid pages in flash device which helps recovery tool to reverse invalid pages and allow users to verify content [9].

5.6. Performance:

Flash Guard efficiently recovers encrypted user data. The execution time to restore encrypted data is from 4.2 to 49.6 seconds. According to statistically studies, flash guard have impact on storage performance. Only small portion of storage operations have similar I/O patterns. So flash guard will keep small amount of invalid pages for regular applications. Second, RFTL retained invalid pages by counting them as valid pages which delays GC execution on flash blocks. Third, FTL allows GC to run during idle time of flash controller which reduces performance. Finally, when all pages on flash block are invalid, flash block will be erased without any additional page movement. This gives boost to performance [9].

7. Discussions:

Pay Break is a system that hold keys on user behalf. Government mandated key escrow systems but this approach is criticized. Pay Break if different from Government proposed Key escrow system as only one entity is involved to access keys-user herself. To bypass ransomware approach, malware authors are considering to implement their own cryptographic libraries or to use secure third-party libraries but Pay Break working experience with different libraries shows that it is supportive against other libraries as well. For this, malware analyst needs to identify encryption scheme once and add it to Pay Break to add support [8]. Malware authors can use another strategy to bypass Pay Break by detecting that Pay Break is running on user machine and accordingly jump over the hooks. This approach of malware authors can be mitigated by inserting hooks at arbitrary points in the function [8]. Ransomware that have knowledge of Pay Break mechanism can bypass Pay Break by using denial of service attack either by corrupting the public key that is used to encrypt vault data or by putting garbage values into vault. Pay Break can be modified to have a dedicated process that appends to vault to protect public key. The privileged process mentioned above alerts user of ongoing attack and terminate malicious process. So Pay Break is a strong defense mechanism in fighting against modern ransomware and in recovering encrypted user files without paying ransom [8]. Considering SSD characteristics, few encryption ransomwares was developed. Flash gives support to data recovery by holding data encrypted by ransomware and prevents it from being removed by garbage collector [9]. Institutions suggest that attacker can exploit storage capacity by writing content to occupy available space in SSD which in turn forcing flash guard to leave control. Second attack would be that ransomware keep reading and overwriting data to SSD so that flash guard retains large amount of garbage data. Such attacks are not useful. Flash guard do not release data hold until data is expired, even though SSD is full. In this case, flash guard will stop taking I/O requests that result into failure of OS file system [9]. The longer the flash guard contains old data, the more overhead it imposes to I/O operations so time factor is important for both security and performance of flash Guard. For this, user needs to set expiry of holding data relatively short. Flash guard have negligible overhead to I/O operations even life span of data is set to 20 days [9]. Flash Guard can protect user against encryption ransomware on multiple platforms. Its approach can be applied to any kind of flash-based storage devices. Flash devices are used on mobiles as well. This idea can be deployed on mobiles to protect them from ransomware attack [9].

8. Conclusion:

Ransomware is new threat to modern world especially to small business owners and organizations. Cyber criminals attack user system, encrypts user data files and demand for ransom for files access. They are increasingly using bitcoins for their payments as Bit coin crypto currency is unregulated. Security research community proposed different tools and techniques by analyzing ransomware behavior and techniques that malware authors are using to by pass defense mechanism. Successful ransomware families are using hybrid crypto approach or exploiting kernel privileges. Pay Break is a protection tool that defeats threat of hybrid crypto ransomware by using key vault technique. It is very efficient in recovering encrypted files. Moreover, researchers explored possibility of using hardware to provide security against ransomware attack. They introduce flash guard as first firmware solution that is resistant against ransomware. This hardware level anti ransomware technique helps in providing resistance against kernel level ransomware attacks.

9. References

[1] A. Gazet, “Comparative analysis of various ransomware virii,” Journal in Computer Virology, vol. 6, pp. 77-90, 2010.

[2] A. Bhardwaj, “Ransomware: A rising threat of new age digital extortion,” in Online Banking Security Measures and Data Protection, ed: IGI Global, 2016, pp. 189-221.

[3] R. Brewer, "Ransomware attacks: detection, prevention and cure, "Network Security, vol. 2016, pp. 5-9, 2016.

[4] C. Everett, "Ransomware: To pay or not to pay?," Computer Fraud and Security, vol. 2016, pp. 8-12, 2016.

[5] A. Kharraz, W. Robertson and E. Kirda, "Protecting against Ransomware: A New Line of Research or Restating Classic Ideas?," in IEEE Security & Privacy, 2018.

[6] L. Zhang-Kennedy and J. R. R. M. K. B. a. S. C. Hala Assal, "The aftermath of a crypto-ransomware attack at a large academic institution," in 27th USENIX Security Symposium, 2018.

[7] D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, A. C. Snoeren and D. McCoy, "Tracking ransomware end-to-end," in IEEE Symposium on Security and Privacy, 2018.

[8] E. Kolodenker, W. Koch, G. Stringhini and M. Egele, "PayBreak: Defense Against Cryptographic Ransomware," in Conference on Computer and Communications Security, 2017

[9] J. Huang, J. Xu, X. Xing, P. Liu and M. K. Qureshi, "FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware," in Conference on Computer and Communications Security, 2017.

[10] A. Continella, A. Guagnelli, G. Zingaro, G. De Pasquale, A. Barenghi, S. Zanero, et al., "ShieldFS: A self-healing, ransomware-aware file system," in 32nd Annual Computer Security Applications Conference, ACSAC 2016, 2016, pp. 336-347.

[11] D. Kansagra, M. Kuhmar, and D. Jha, "Ransomware: A threat to Cyber-Security," CS Journals, vol. 7, 2016.

[12] R. Richardson and M. North, "Ransomware: Evolution, Mitigation and Prevention," International Management Review, vol. 13, p. 10, 2017.

[13] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the gordian knot: A look under the hood of ransomware attacks," in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 2015, pp. 3-24.

[14] D. P. Pathak and Y. M. Nanded, "A dangerous trend of cybercrime: ransomware growing challenge," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume, vol. 5, 2016.

[15] P. Zavarsky and D. Lindskog, "Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization," Procedia Computer

Science, vol. 94, pp. 465-472,2016.

[16] KHARRAZ, A., ARSHAD, S., MULLINER, C., ROBERTSON, W. K., AND KIRDA, E. Unveil: A large-scale, automated approach to detecting ransomware. In USENIX Security Symposium (2016), pp. 757–772.

[17] SCAIFE, N., CARTER, H., TRAYNOR, P., AND BUTLER, K. Cryptolock (and drop it): stopping ransomware attacks on user data. In 36th International Conference on Distributed Computing Systems (ICDCS) (2016), IEEE, pp. 303–312.

[18] Eugene Kolodenker, William Koch, Gianluca Stringhini, and Manuel Egele, "PayBreak : Defense Against Cryptographic Ransomware" Conference Paper 2017 ACM.

LAHORE GARRISON UNIVERSITY

Lahore Garrison University has been established to achieve the goal of excellence and quality education in minimum possible time. Lahore Garrison University in the Punjab metropolis city of Lahore is an important milestone in the history of higher education in Pakistan. In order to meet the global challenges, it is necessary to touch the highest literacy rates while producing skillful and productive graduates in all fields of knowledge.

VISION

Our vision is to prepare a generation that can take the lead and put this nation on the path to progress and prosperity through applying their knowledge, skills and dedication. We are committed to help individuals and organizations in discovering their God-gifted potentials to achieve ultimate success actualizing the highest standards of efficiency, effectiveness, excellence, equity, trusteeship and sustainable development of global human society.

MISSION

At present, LGU is running Undergraduate, Graduate, Masters, M.Phil. and Ph.D. programs in various disciplines. Our mission is to serve the society by equipping the upcoming generations with valuable knowledge and latest professional skills through education and research. We also aim to evolve new realities and foresight by unfolding new possibilities. We intend to promote the ethical, cultural and human values in our participants to make them educated and civilized members of society.

Contact: For all inquiries, regarding call for papers, submission of research articles and correspondence, kindly contact at this address:
Sector C, DHA Phase-VI Lahore, Pakistan

Phone: +92- 042-37181823
ijeci@lgu.edu.pk

Published by: Digital Forensics Research and Service Center, Lahore Garrison University