REPORT

02 DAYS TRAINING ON CYBER CRIME

02-03 NOV 2017

CONTENTS

With the collaboration of UNDP-SRLP and financial assistance from SDC, the Judicial Academy has successfully rolled out 02 days training on 'Cyber Crimes'. Crime as such is not an isolated phenomenon that can be examined, analyzed and described in one piece. It affects every part of the country and almost every level of society. The offenders and its victims are people of all ages, income and backgrounds.[1] Its trend are difficult to ascertain. Its causes are multitude. Its cures are speculative and controversial. Computer related crimes, popularly termed as 'Cyber Crimes', are latest among all the crimes. Cyber crime, in a general sense, is an act that covers the entire range of crimes which involves computer, computer network, cell phones, etc., either as its target or as an instrumentality or associate. Thus any kind of criminal activity that takes place with the help of or against such electronic equipments and in the cyber space, comes under the purview of the word cyber crimes. Like other criminal activities, the motive or intention to cause an injury is one of the ingredients and the same is not limited to any specific type. Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world. Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyber laws are a very technical field and that it does not have any bearing to

---

[1] Dr. Pramod Singh "Laws on Cyber Crime" p.6

most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives. Pakistan too has a legal framework in place to address cyber crimes. The Electronic Transaction Ordinance 2002 was passed by the government of Pakistan with the objective to recognize and facilitate documents, records, information, communications and transactions in electronic form and to provide for the accredition and certification service providers. With this legal framework we do have legal backing for electronic information and communication as any written and signed document. With this law in place Pakistan has joined an exclusive band of countries that provide necessary framework and an impetus for growth of electronic commerce in Pakistan. The ordinance has laid down clauses for offences related to electronic transactions namely provision of false information, issue of false certificate and damage to information system. Furthermore, the electronic crime Bill, 2004 was drawn up with the electronic Transaction Ordinance 2002 as the basis, but the bill lapsed and subsequently an ordinance under the name of Prevention of Electronic Crimes Ordinance# 72 of 2007 was promulgated which law addressed and laid down legislative terms for the cyber crimes namely; criminal access, criminal data access, data damage, system damage, electronic fraud, electronic forgery, misuse of devices, malicious code, cyber stalking, spamming, spoofing, unauthorized interception and attempt and aiding or abetting. The Ordinance, however, expired by efflux of time and then another Ordinance with the same name was promulgated in 2008 which also expired by efflux of time. Until now there is no legislation in Pakistan on the subject. Recently the parliament has passed a bill namely prevention of electronic crimes bill 2015 which declares cyber terrorism, electronic fraud and forgery, glorification of an offense and hate-speeches, child pornography and hacking as punishable offenses. The federal government will establish or designate a law enforcement

agency for the investigation of offences under this Act. This Act of the Parliament is, however, is pending with the President of Pakistan for his assent.

It is essential to educate and empower youth to safely and responsively take control of their internet experience. Cyber crimes may be introduced in schools and adding it to curriculum will create the required awareness amongst the youth. Information for consumers and businessmen may be disseminated on computer security and safeguarding personal information. Along with this contact numbers of authorities, the process etc should be explicitly stated. It is not possible to eliminate cyber crime from the cyber space in its entirety. However, it is quite possible to check it. Any legislation in its entirety might be less successful in totally eliminating crime from the globe. The primary step is to make people aware of their rights and duties, report crime as the collective duty towards the society and further, making the application of the laws more stringent to check crimes.

This course has been designed initially for sensitization of judicial officers regarding cyber laws. Conscious, knowledgeable and intelligent judges can play more effective role in all such cases particularly cyber crimes because these cases are very delicate and have profound impact on the society. Training always become very helpful to enhance one`s caliber, knowledge and comprehension about the issues which one has to deal with. It is expected that this training will be immensely beneficial to the participants in the relevant field and will provide them the unique opportunity to gain diverse and abundant knowledge and experience in cyber space.

1. KP Judicial Academy has designed this course specifically for a non-technical audience who wish to gain an understanding of Cyber Crime. The course will provide an understanding of Cyber Crime, how it occurs, the effects it has on society and how it is investigated and tried.

2. There is a growing tendency of criminal & civil cases in one way or the other related to information and communication technologies. Thus judges are confronted with cyber-crime and electronic evidence matters. It necessitates a continual education of cyber-crime and electronic evidence. As a start the Judicial Magistrates needs to obtain at least basic training in matters related to cyber-crime and electronic evidence. At the same time, these are highly technical and constantly evolving issues and it cannot be expected that judges in general are able to keep up with technological developments at all times. It is therefore necessary to provide advanced knowledge to a sufficient number of judges who become specialized in cyber-crime and electronic evidence.

3. A *fortiori,* in 2011, at least 2.3 billion people, the equivalent of more than one third of the world's total population, had access to the internet. Over 60 per cent of all internet users are in developing countries, with 45 per cent of all internet users below the age of 25 years. By the year 2017, it is estimated that mobile broadband subscriptions will approach 70 per cent of the world's total population. By the year 2020, the number of networked devices will outnumber people by six to one, transforming current conceptions of the internet. In the hyper connected world of tomorrow, it will become hard to imagine a 'computer crime', and perhaps any crime, that does not involve

electronic evidence linked with internet protocol (IP) connectivity [2]. Thus this formulation of the crashed course is the need of the hour.

The **objectives** of this training course are:

- Computer and Networks: How do they work, basic notions of the functioning of the internet, role of Service providers, particular challenges to Judges.

- Cybercrime: How information and communication technologies are used to commit crime.

- Cybercrime legislation: Domestic legislation (including case law) and international standards.

- Jurisdiction and territorial competencies.

- Electronic evidence: Technical procedures and legal consideration.

Outcomes:

As a result of the basic training judges should be in a position to:

- ✓ Relate criminal conduct to provisions in domestic legislation.

- ✓ Approve investigative techniques.

- ✓ Order the search and seizure of computer systems and the production of electronic evidence.

- ✓ Expedite international cooperation

- ✓ Question witnesses and experts

- ✓ Present/ Validate electronic evidence.

Modules

---

[2] UNITED NATIONS OFFICE ON DRUGS AND CRIME, Vienna. Comprehensive Study on Cybercrime Draft February 2013

This specialized course on consumer law constitutes of four modules. As this is a 02 day short course thus an endeavor is made to cover it in three lectures with each of 90 minutes duration.

01	Basic orientation -- Hardware, Networking & World Wide Web

Focus

- Introduction to the Personal Computer

- Identify and describe the various components that make up a personal computer and define information technology

- Computer Assembly Step-by-Step

- Fundamental Operating Systems

- Describe operating system capabilities, the installation process, navigation, basic preventive maintenance, and troubleshooting

- Fundamental Laptops and Portable Devices

- Identify and describe the main components of laptops and portable devices, basic preventive maintenance, and troubleshooting

- Fundamental Printers and Scanners and other related devices

- Fundamental of Networks

- Identify and describe basic network components, technologies, basic preventive maintenance, and troubleshooting

- Fundamental of Information / Data Security

- Introduction to WWW and History

- Internet features

- Connecting to the Internet

- Internet etiquette

- Internet protocols

- Web browsers, Search engines, Searching the Web

- E-mail, Effective use, Sending e-mail, Receiving e-mail

- Web Services

- Blogs, Micro Blogs

- Portal/CMS

  - Forums

  - Image Galleries

  - Wikis

  - Social Networking

  - Ad Management

  - Calendars

  - Gaming

  - Mails, mailing lists

  - Polls and Surveys

  - Project Management

  - E-Commerce

  - ERP

  - Guest books

  - Customer Support

  - Development Frameworks

  - Educational Systems

  - Music and Video Sharing

  - File Management

  - Online Libraries

  - Online communication (Email, IM, Video Call, Webcast)

Suggested Readings

i. *Fundamentals of Computers, https://en.wikibooks.org/wiki/A-level_Computing/AQA/Computer_Components,_The_Stored_Program_Concept_and _the_Internet/Fundamentals_of_Computer_Systems*

ii. *Computer Fundamentals, https://www.cl.cam.ac.uk/teaching/1011/CompFunds/CompFunds.pdf*

iii. *Information Security, Wikipedia, https://en.wikipedia.org/wiki/Information_security*

iv. *Internet Basics, http://www.gcflearnfree.org/internet101*

v. *Internet Basics, http://www.internetbasics.gov.au/*

vi. *Internet, Webopedia, http://www.webopedia.com/TERM/I/Internet.html*

vii. *How Stuff Works, http://computer.howstuffworks.com/internet/basics*

viii. *Internet World Stats, http://www.internetworldstats.com/*

02	What is Cyber crime and how it is committed

Focus

- What is Cyber crime, History & how committed

- Legal Challenges

- Cyber Crime v/s Conventional Crime

- Types of Cyber Crimes

- Financial crimes, Cyber pornography, Sale of illegal articles, Online gambling, Intellectual Property crimes, Email spoofing, Forgery, Cyber Defamations, Cyber stalking, Unauthorized access to computer systems or networks, Theft of information contained in electronic form, Email bombing, Data diddling, Salami attacks, Denial of Service attack, Virus / worm attacks, Logic bombs, Trojan attacks, Internet time theft, Web jacking, Theft /damaging of computer system, Unauthorized Access,

- Targets of Cyber Crimes (Individual property, Organization and Society at large)

- What is Hacking, Cyber Attacks, Vulnerabilities, Malware, Spying, Cyber War, Surveillance etc.

Suggested Reading:

    i.   NR3C, FIA, http://www.nr3c.gov.pk/

    ii.   Federal Investigation Agency, http://www.fia.gov.pk/

    iii.   http://www.ncfta.net/

    iv.   https://www.cybercrimeinvestigators.com/

    v.   The Hackers News, https://thehackernews.com/

03	History & development of Cyber Law in Pakistan

Focus

- Pre-partition legislations in respect of electronic communication devices.
- Post independence legislations
- The proposed laws on cyber crime prevention

Suggested Readings:

    i.   The Electronic Transaction (Re-organization) Act, 1996,

    ii.   The Wireless Telegraph Act, 1933,

    iii. The Telegraph Act, 1885,

    iv. Electronic Transaction Ordinance 2002,

    v.   The Payment Systems and Electronic Fund Transfers Act, 2007,

    vi. Prevention of Electronic Crimes Ordinance, Pakistan 2007,

    vii. Prevention of Electronic Crimes Ordinance, Pakistan 2008

04	**National and International Case laws on Cyber crime**

FOCUS

- Salient international pronouncements on cyber laws

- Pakistani case laws

Suggested Readings:

i. United States of America vs David Nosal case. http://cdn.ca9.uscourts.gov/datastore/opinions/2012/04/10/10-10038.pdf

ii. United States of America vs SUIBIN ZHANG, http://www.insideprivacy.com/United%20States%20v.%20Zhang.pdf

iii. REGINA v.BOW STREET MAGISTRATES COURT AND ALLISON (A.P.*).* http://www.publications.parliament.uk/pa/ld199899/ldjudgmt/jd990805/bow.htm

05	**Electronic Evidence**

Focus

- Meaning & definition of Electronic Evidence.

- Status of Electronic Evidence under the Quanon-e-Shahdit Order, 1984

- Modes of Electronic evidence

- Evidentiary value of the electronic evidence.

Suggested Readings:

i. Electronic Evidence, 2nd Edition 2012 by Joshi

ii. Evidence Law, Edition 2012 by Sohoni

Chaudary Ayaz, Deputy Director FIA delivered the first lecture of the training on "An overview of existing legislation on Cyber Crime around the Globe-International Perspective". The lecture was delivered in two sessions. The first session mainly focused on the thematic areas of 1) what is cyber operation? Defining Cyber Attack, The role of Law, Categorization of Cyber Threats, Cyber Operation amounting to Use of Force under Art 2 (4) of UN Charter, Cyber terrorism, States and Cyberspace etc. The second lecture will be in continuation of the first session where group discussion and Q&A were held. The lecture was descriptive as it focused on various concepts and themes. The holding of plenary sessions at the end shaped the lecture as participatory one.

At the end of the session, the participants were able to know the importance of the subject as well as the participant's idea on existing legislation on Cyber crime around the globe in International perspective.

AN OVERVIEW OF EXISTING LEGISLATION ON CYBER CRIME AROUND THE GLOBE-INTERNATIONAL PERSPECTIVE
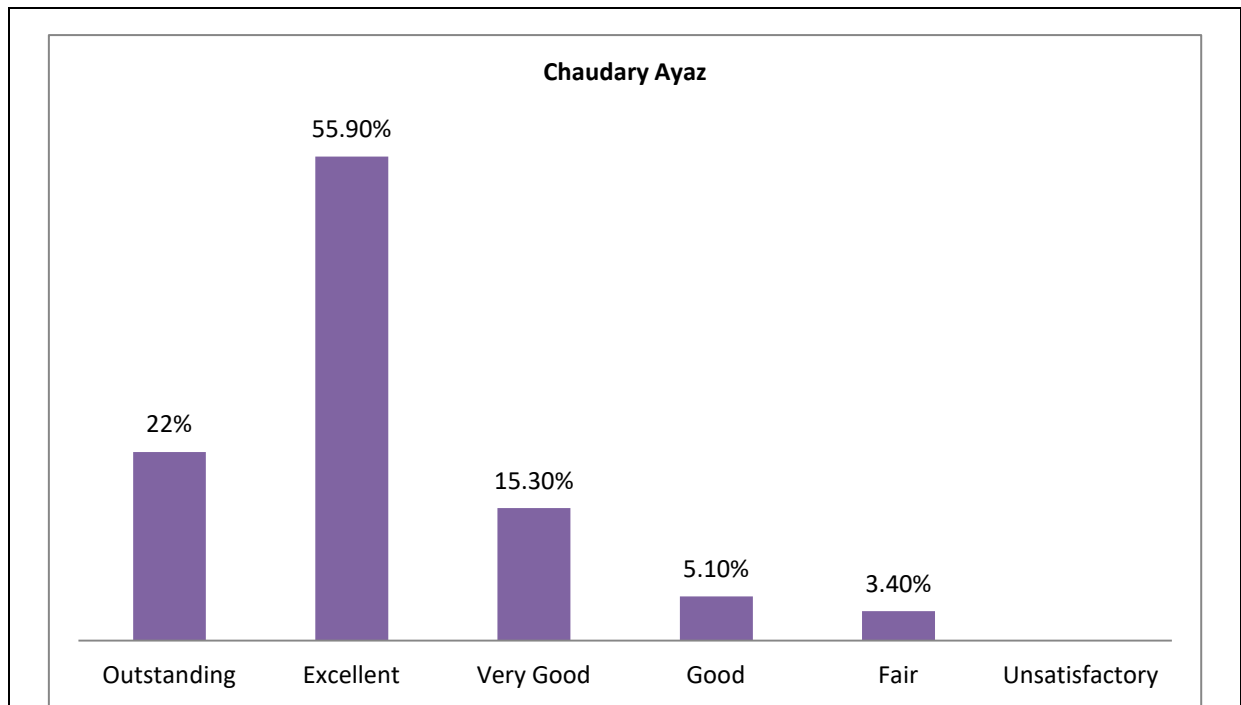
Introduction

One of the most important distinctive features of cyber crime is that its impact is much wider than the traditional crime. A criminal act committed in one part of the world may cause impact at some other part of the world. In view of reach of the cyber crime, entire world has virtually turned into a small village. Another feature is that the criminalization and increase in the cyber crime is uniform all around the world. It may happen that an act is a crime in one country, but may not be in another country. But if a person commits a crime, although it may not be crime in his country, he still may be liable to prosecution under the provision of law of

another country. The legal response to the cyber crimes of various countries of the world is varied. Such laws are still under its gestation period. There is not even a single law that can be stated to contain all the necessary attributes of modern cyber legislation. To meet the challenge posed by new kinds of crime made possible by computer technology including telecommunication, many countries have also reviewed their respective domestic criminal laws so as to prevent computer related crimes. Some of these countries are USA, Austria, Denmark, France Germany, Greece, Finland, Italy, Turkey, Sweden, Switzerland, Australia, Canada, India, Japan, Spain, Portugal, UK, Malaysia and Singapore.

Basic approaches for creation of Cyber Laws

Following are the basic approaches for creation of Cyber Laws, which will ensure the smooth governance of Internet globally:

a) Formulation of new laws and amendment of existing laws by nations within their present territorial boundaries thereby attempting to regulate all actions on the Internet that have any impact on their own population.

b) Nations may enter into multi-lateral international agreements to establish new and uniform rules specifically applicable to conduct on the Internet.

c) Creation of an entirely new international organization, which can establish new rules and new means of enforcing those rules.

d) Guidelines and rules may naturally emerge from individual decisions like domain name and IP address registrations and by websites and users deciding about whom will they patronize.

Chaudary Ayaz

	Outstanding	Excellent	Very Good	Good	Fair	Unsatisfactory
	22%	55.90%	15.30%	5.10%	3.40%	

Mr. Khuram Siddique Director Legal PTA delivered a extensive lecture on "Cyber Laws and Cyber crime in Pakistan". Cyber crime has grown in importance. The Resource person gave a detailed account of the different legislations and explained the salient feature of legislations of cyber crimes. It also includes traditional crimes in which computers or networks are used to enable the illicit activity.

The lecture mainly focused on the following thematic areas: Cyber Laws, Cyber Laws in Pakistan (Conventional), and Conflict of Laws. The lecture was descriptive as it focused on various concepts and themes in the presentation on the subject. The holding of plenary sessions at the end shaped the lecture as participatory one. At the end of the session, the participants were able to know the importance of the subject and had clear idea on cyber crimes and cyber laws in Pakistan.

CYBER LAWS AND CYBER CRIME IN PAKISTAN

Overview

In this lecture there will be discussion about cyber law and cyber crime ordinance in Pakistan. Cyber law is a generic term that encapsulates the legal issues and activities regarding communicative, transaction and distributive features of the computer, the internet and the World Wide Web. Cyber crime is a sin having its line of descent in the rising dependence on computers in advanced life. In a modern age, when everything from microwaves and refrigerators to nuclear power plants are being lead on computer cyber crime has assumed rather threatening implications. Thus, according to the generalized definition cyber crimes are; unlawful acts in which any electronic device is either a tool or an objective or both.

Pakistan while daring and initiating to further step from any advance countries, has introduced, enacted and amended various statutes namely;

(i) Electronic Transaction Ordinance 2002.

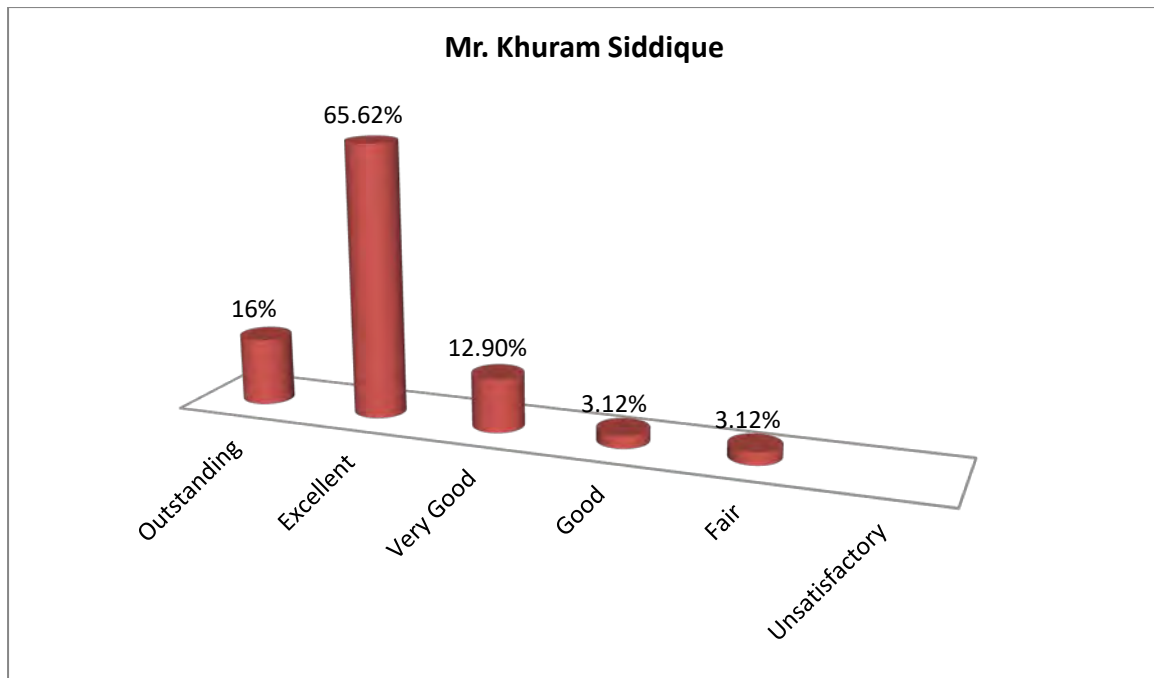(ii) Prevention of Electronic Ordinance 2008.

(iii) Amended Article 2 (e) of Qanon-e-Shahdat 1984.

(iv) Payment System Electronic funds Transfer Act 2007.

(v) Anti Money Laundering Act 2010.

(vi) Investigation for Fair Trial Act 2013.

Mr. Khuram Siddique

Mr. Imran Haider Senior Investigator FIA, Cyber Crime Circle shared a talk on the "Cyber Forensics & Data Protection".

CYBER FORENSICS & DATA PROTECTION

Overview

Lecture will start with an introduction about the Digital Forensics and Computer Crime. Crimes in past and crimes with advanced technology will be explained. Various ways in which computers can be used as a tool for crime such as cyber theft, identity theft, cyber fraud, and internet gambling etc. will be discussed. Computers can be used as a target for crime with the example of e-mail bombing, multilevel marketing. Classification of crimes will also be explained. Inputs for digital forensics are data from computer, mobile, database, live, and network. Forensic science is a set of scientific methods used to find the truth.
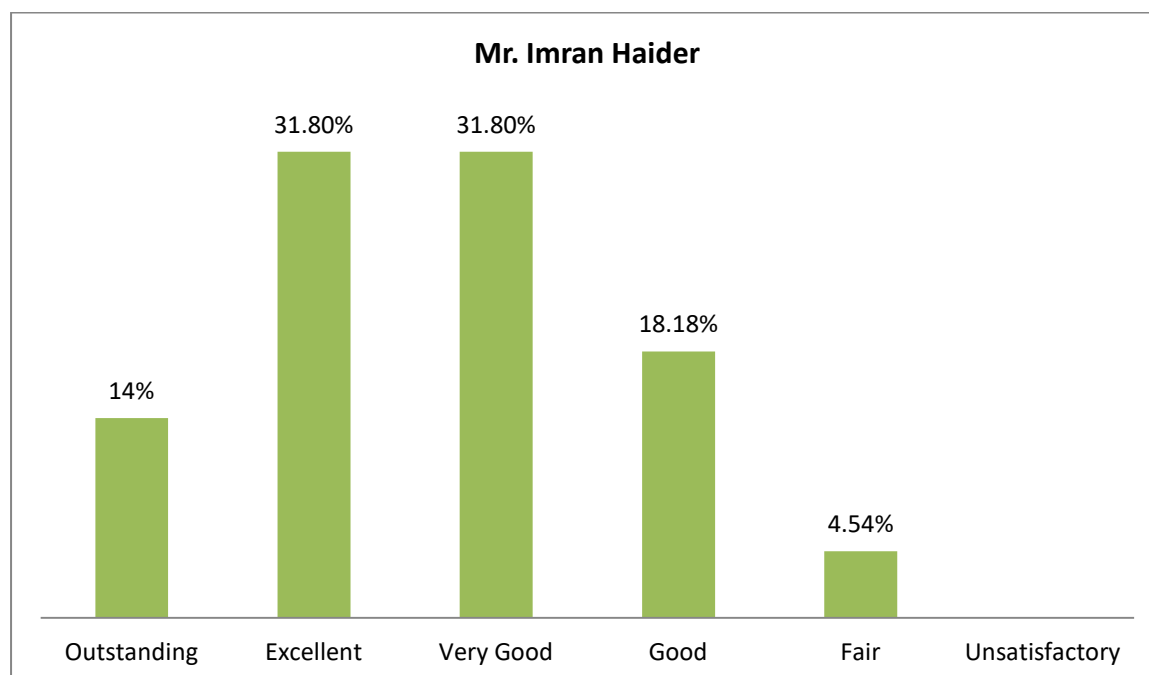
Digital Forensics:

This concept involves

i) Detection and documentation of crimes through disciplined method.

ii) Prevent the occurrence of cyber-crime in vulnerable institutions like Government, Organizations, Airlines and other institutions enquiring security from loss, pilferage and

mishandling by accidental or intentional manipulation. Some real time cases handled were discussed and related videos were shown. Awareness about data protection and privacy will be given to the participants.

This lecture will be very useful for the trainees to know about the current leading trends in Industry.

Mr. Imran Haider

Outstanding	Excellent	Very Good	Good	Fair	Unsatisfactory
14%	31.80%	31.80%	18.18%	4.54%	

Mr. Shahid Hussain Deputy Director FIA Cyber Crime Wing, deliberated on the topic "Importance of Cyber Crimes and Preventive measures and on the Privacy issues"
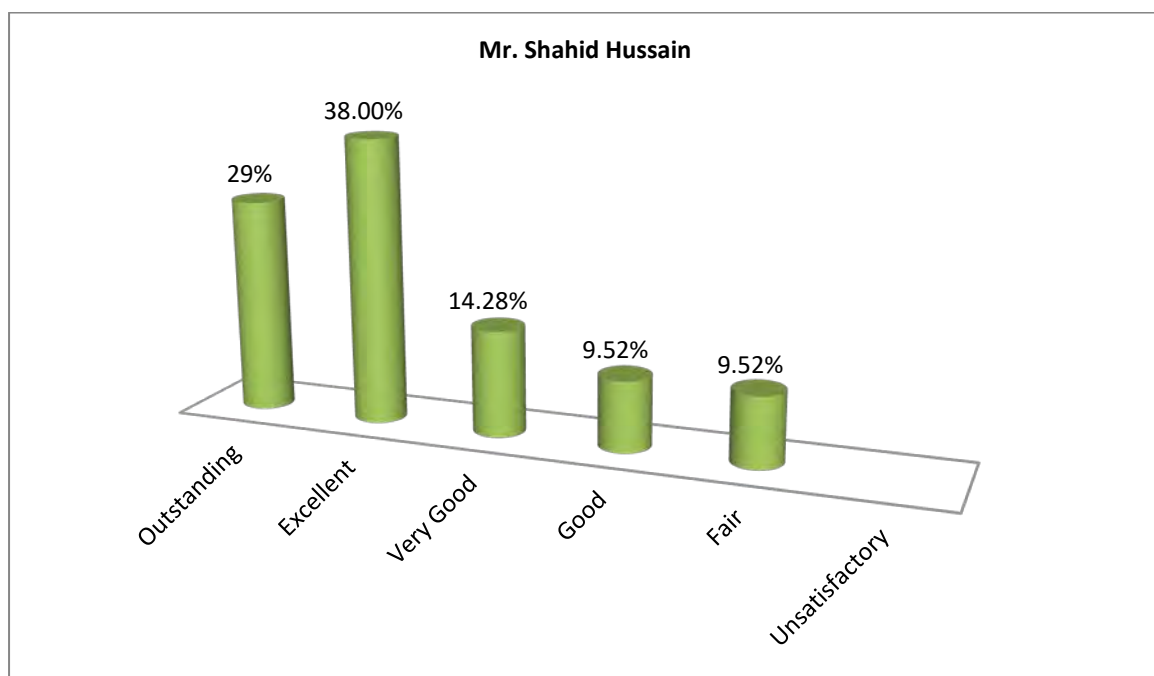
THE PRIVACY ISSUES

Overview

All the related practicalities in the matter will be covered in this session. Practical demonstration of different type of cyber crime will be given. The privacy issues involved will be discussed. In this lecture, how devastating these crimes will be discussed. The nature of digital evidence; Types of digital evidence; its admissibility in the court of law; relevant amendments in the Evidence Law, Information Technology perspective, cyber crimes, cyber

crime scenarios, cyber criminal activities, establishment of nr3c & its capabilities and current laws and challenges & way forward will be discussed.

The lecture will also focused on: The reservations of the civil society on the cyber laws, the Budapest convention, ISO standards and the need of MLATS. The lecture will be purely practical.

Outcome

At the end of the session, the participants will be able to know the importance of the subject and had idea on types of cyber crimes.

Mr. Shahid Hussain

Outstanding 29%
Excellent 38.00%
Very Good 14.28%
Good 9.52%
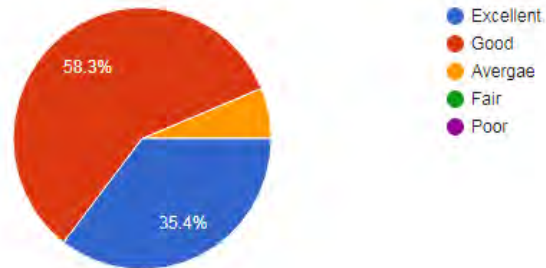Fair 9.52%
Unsatisfactory

REACTION SURVEY (PRE-TRAINING)

Program Administration

What was the level of information provided to you about the training program by KPJA? Please choose the appropriate level for each attribute given below.
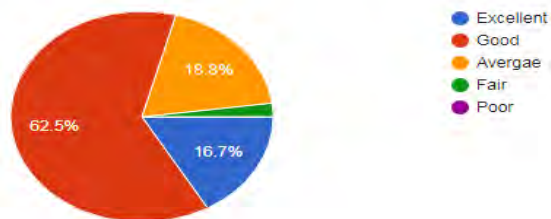
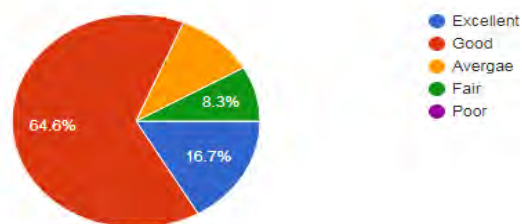## a. About the schedule of training program.

48 responses

Legend:
- Excellent
- Good
- Avergae
- Fair
- Poor

58.3%
35.4%

b. Sharing of pre requisites material for training.

48 responses

Legend:
- Excellent
- Good
- Avergae
- Fair
- Poor

62.5%
18.8%
16.7%

c. Relevance of the pre requisite material to the training program.

48 responses

Legend:
- Excellent
- Good
- Avergae
- Fair
- Poor

64.6%
8.3%
16.7%

d. About the location of training program.

48 responses

- Excellent
- Good
- Avergae
- Fair
- Poor

45.8%
12.5%
39.6%
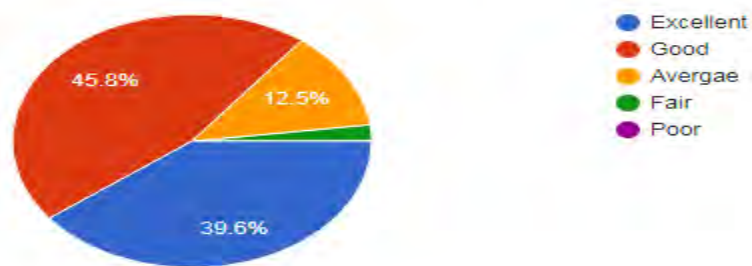
Schedule

8. What do you think what should be the appropriate schedule for training program?

48 responses

- Single long session on single topic with no breaks
- Single long session on single topic with single break
- Short lectures on different topics each day with breaks

62.5%
35.4%

---

9. Which teaching methodology you would suggest to be followed during the training program?

47 responses

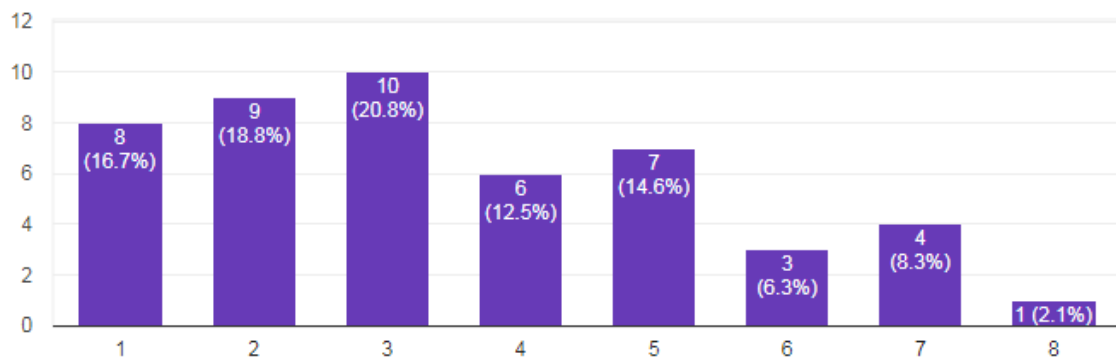|		
Purely lecture b…		7 (14.9%)
Case study met…		29 (61.7%)
Prior lecture han…		22 (46.8%)

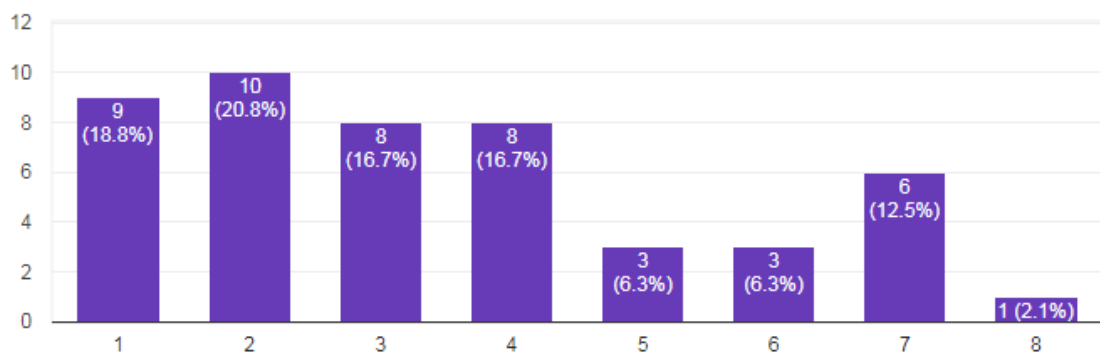0   5   10   15   20   25   30
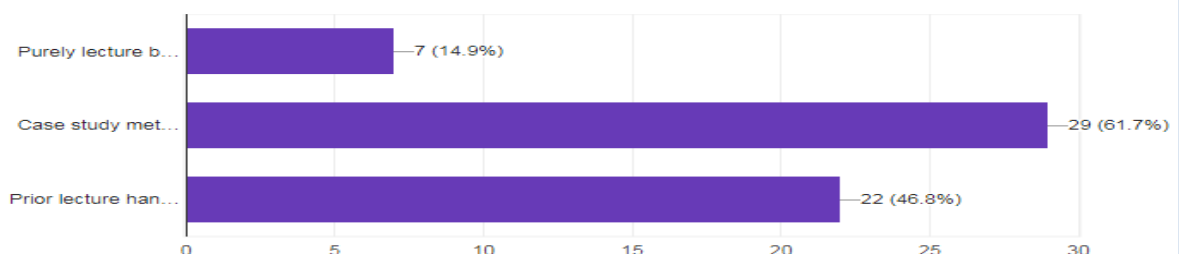
a) Communication

48 responses
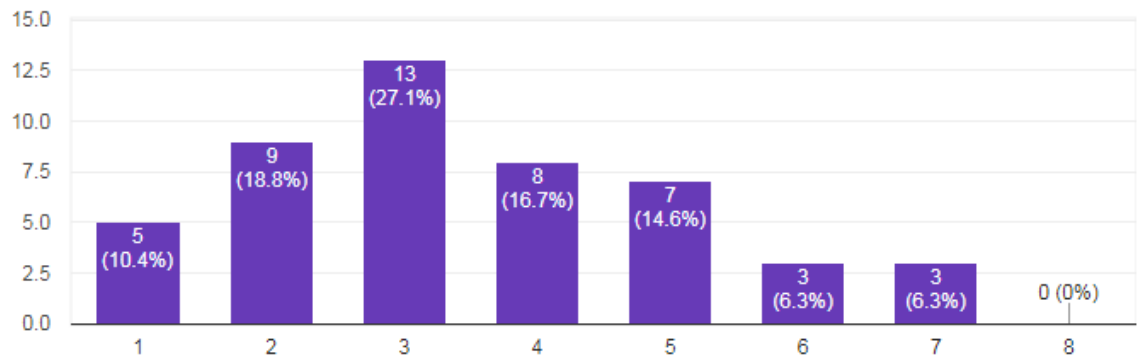
b) Analytical

48 responses

c) Strategic

48 responses

d) Decision making

48 responses
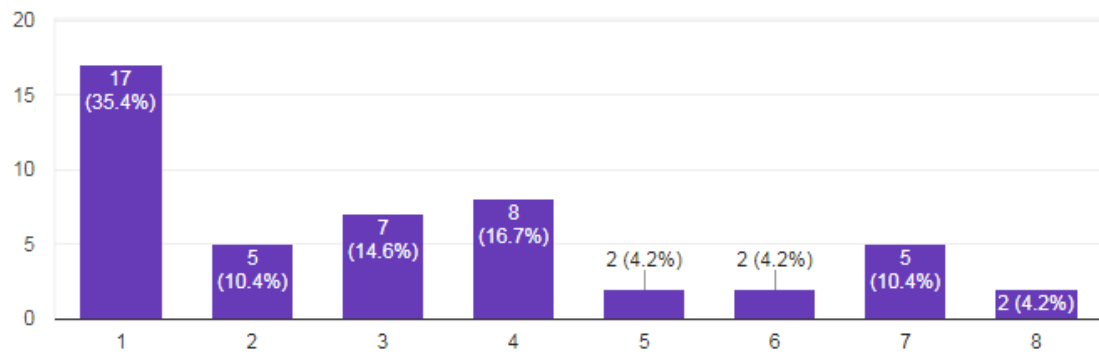
e) Networking

46 responses
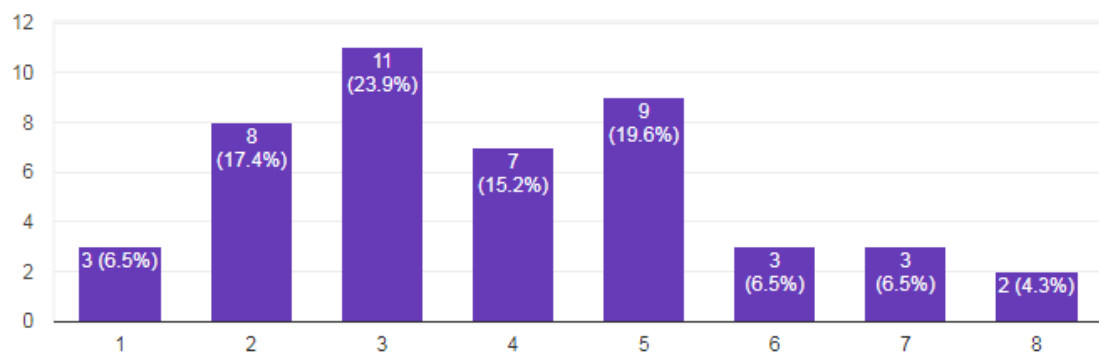
f) Interpersonal

48 responses
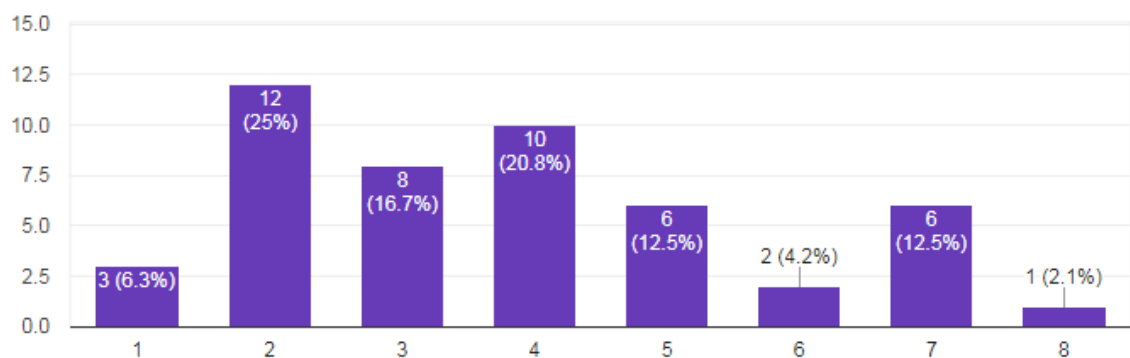
g) Leadership

48 responses
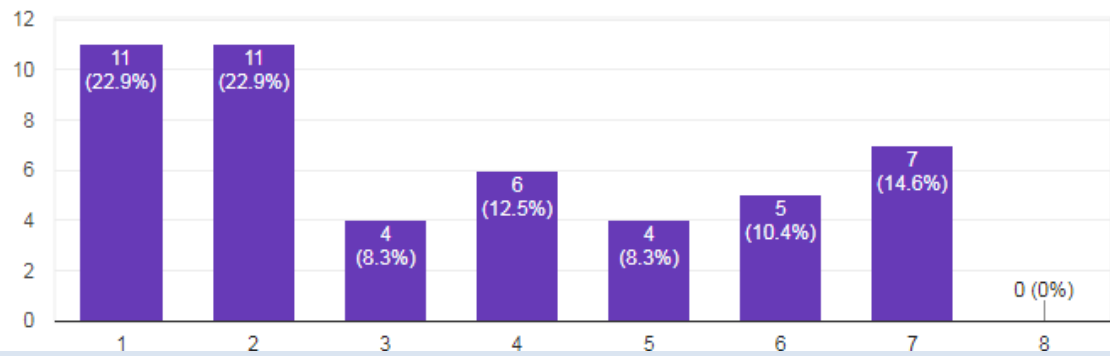
h) Management

48 responses
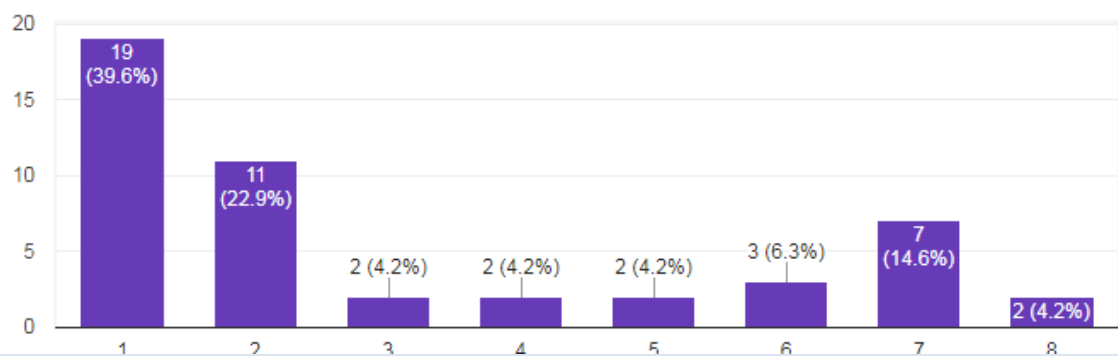
REACTION SURVEY (POST-TRAINING)

Reaction Survey (Post-Training)

1. Express your opinion about the attributes of training course you attended

i. Overall course objectives were met.
44 responses

- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

20.5%
68.2%
9.1%

ii. Concepts were clearly conveyed.

44 responses
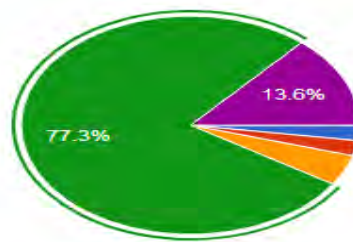
- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

13.6%

77.3%

iii. The sequence of course was logical.

44 responses
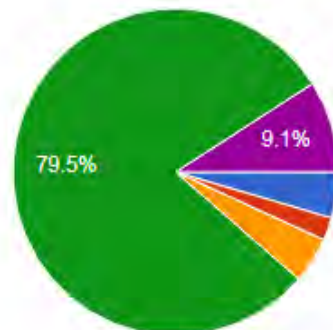
- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

79.5%

9.1%

i. I felt comfortable asking questions.

44 responses

- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

31.8%
59.1%

ii. I was given the opportunity to contribute during class discussions.

44 responses

- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

22.7%
70.5%
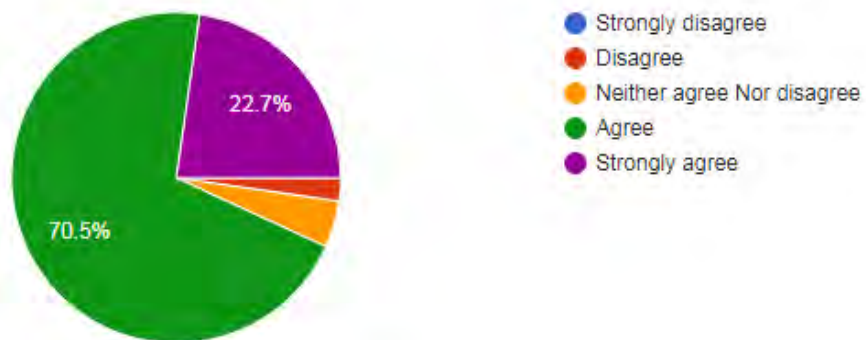
iii. I was provided opportunities to network with other participants.

44 responses

- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

63.6%
9.1%
13.6%
13.6%
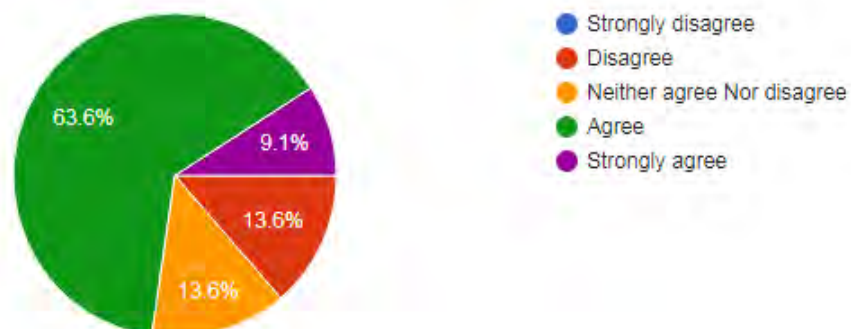
i. Instructor/s had lot of personal experience.
44 responses

- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

25%
70.5%

ii. Instructor/s had good understanding and knowledge of topics he was teaching.
44 responses

- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

13.6%
79.5%

Agree
35 (79.5%)
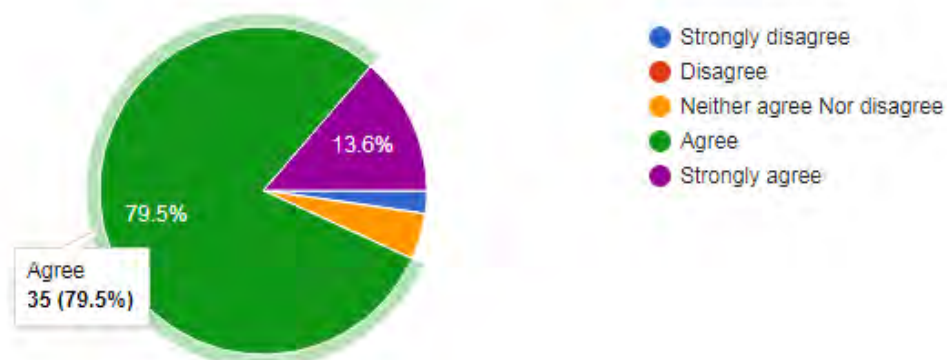
iii. Instructor/s was great at taking questions further into Law Enforcement aspects.
44 responses

- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

13.6%
79.5%

iv. He/she was dynamic and excellent speaker.

44 responses

Legend:
- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

Agree: 81.8%
Strongly agree: 11.4%
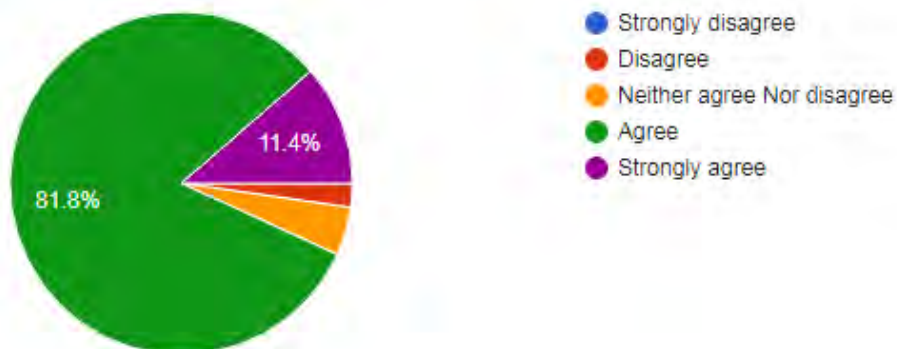
v. Instructor was comfortable with self and subject matter.

44 responses

Legend:
- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

Agree: 90.9%
Strongly agree: 9.1%
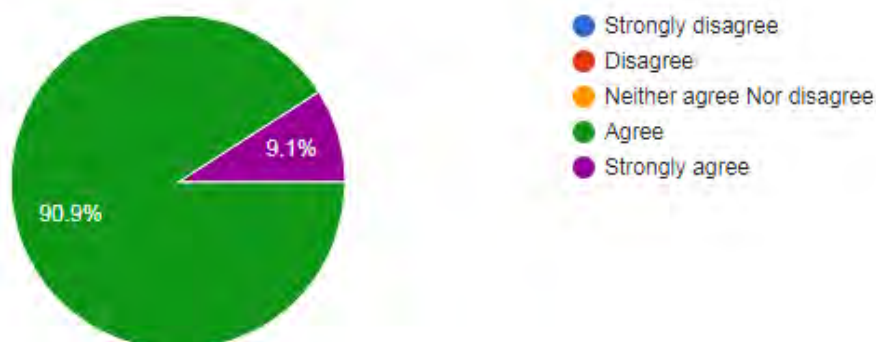
vi. Knowledge and communication skills of instructor were exceptional.

44 responses

Legend:
- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

Agree: 72.7%
Strongly agree: 9.1%
Neither agree Nor disagree: 18.2%

i. I was using the knowledge and/or skills presented in the training courses prior to attending a training course.

44 responses

- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

34.1%
29.5%
31.8%
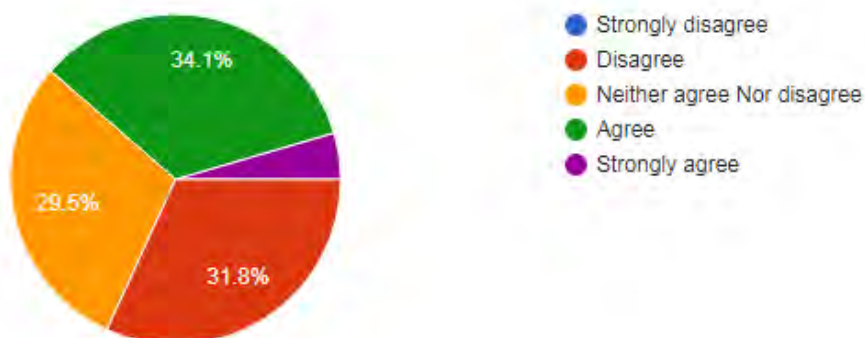
ii. The concepts and/or skills learned at the training courses were related to my work situation.

44 responses

- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

34.1%
61.4%

iii. I assume that training courses have offered me the required elements for the demands of my job.

44 responses

- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

31.8%
65.9%

iv. The content of the training courses were appropriate for achieving the course objectives.

44 responses

- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

18.2%

72.7%

5. Expectations of the training course

i. I believe that the training courses create a sense of group cohesiveness among participants.

44 responses

- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

15.9%

65.9%

15.9%

ii. I believe I have made a significant impact on my personal growth, as a participant in a training course. (e.g. new opportunities for learning, broadening of the intellectual level)

44 responses

- Strongly disagree
- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

25%

70.5%

iii. I assume that training courses have offered me the required elements for the demands of my job.

44 responses

- ● Strongly disagree
- ● Disagree
- ● Neither agree Nor disagree
- ● Agree
- ● Strongly agree

31.8%

65.9%

iv. The content of the training courses were appropriate for achieving the course objectives.

44 responses

- ● Strongly disagree
- ● Disagree
- ● Neither agree Nor disagree
- ● Agree
- ● Strongly agree

18.2%

72.7%

i. I believe that the training courses create a sense of group cohesiveness among participants.

44 responses

- Strongly disagree
- Disagree
- Neither agree Nor disagree
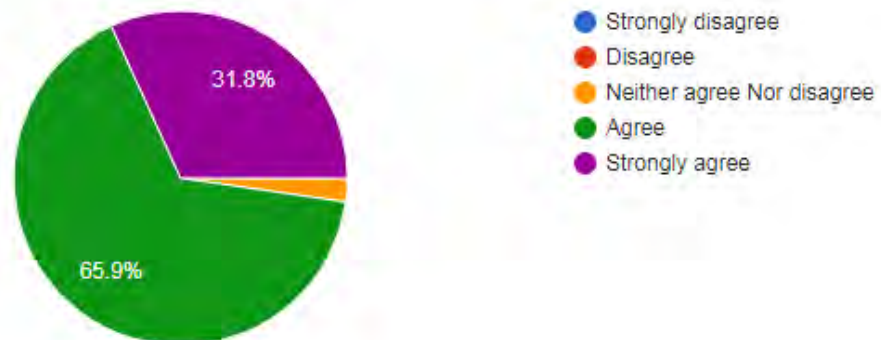- Agree
- Strongly agree

65.9%
15.9%
15.9%

ii. I believe I have made a significant impact on my personal growth, as a participant in a training course. (e.g. new opportunities for learning, broadening of the intellectual level)
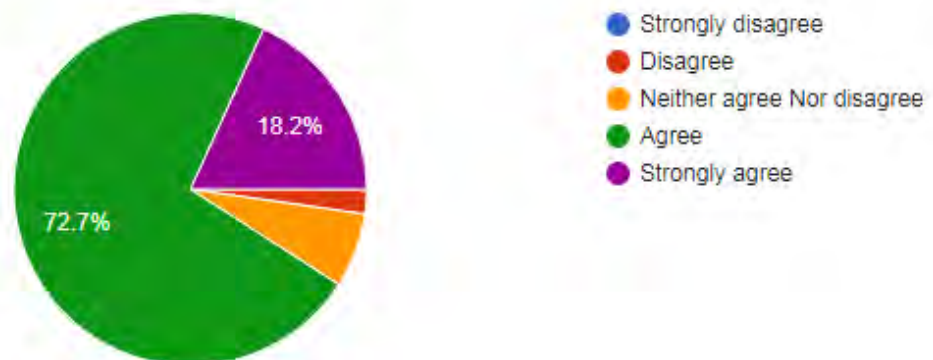
44 responses

- Strongly disagree
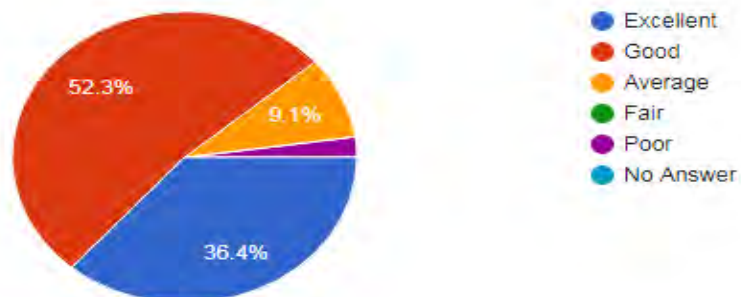- Disagree
- Neither agree Nor disagree
- Agree
- Strongly agree

25%
70.5%

Over all feedback

7. Please rate overall quality of the training.

44 responses

- Excellent
- Good
- Average
- Fair
- Poor
- No Answer

52.3%
9.1%
36.4%

ANNEXURE

Schedule of Activities of 02 days training on Cyber Crime
02-03,Nov 2017

Day - 1 Thursday (02 November, 2017)

S.No	Topic	Resource Person	Duration
1.1	Registration & Pre-Evaluations		08:30-8:35
	Recitation from the Holy Quran		
1.2	Introductory Remarks	Director General	8:35-8:40
1.3	Orientation and Ice Breaking	Dean Faculty	8:40-9:00
1.4	An overview of existing legislation on Cyber Crime around the Globe-International Perspective	Chaudary Ayaz Deputy Director FIA	9:00-10:30

Tea Break 10:30 – 11:00

S.No	Topic	Resource Person	Duration
1.5	Cyber Laws & Cyber Crimes in Pakistan	Mr. Khuram Siddique Director Legal PTA	11:00-12:30

Prayer & Lunch Break 12:30 - 1:30

S.No	Topic	Resource Person	Duration
1.6	Cyber Forensics & Data Protection	Mr. Imran Haider Senior Investigator FIA, Cyber Crime Circle	1:30-3:00

Day – 2 Friday (03 November, 2017)

S.No	Topic	Resource Person	Duration
2.1	Recitation from the Holy Qur'an		8:30-8:35
2.2	Importance of Cyber Crimes and Preventive measures	Mr. Shahid Hussain Deputy Director FIA, Cyber Crime Wing	9:00-10:30

Working Tea

10:30 – 11:00

S.No	Topic	Resource Person	Duration
2.3	Investigation & Prosecution mechanism in Cyber Crimes	Chaudary Ayaz Deputy Director FIA	11:00 – 12:30

Prayer & Lunch Break

12:30 - 01:30

2.4	The Privacy Issues	1:30-3:00
	• The reservations of the civil society on the Cyber Laws • An overview of Electronic Crime Act, 2016	Mr. Shahid Hussain Deputy Director FIA, Cyber Crime Wing

Post training Evaluations

3:10 - 3:20

Concluding Ceremony

2.4	Class Representative remarks.	03:20 –
2.5	Concluding address of the Director General	

Group photograph

S.No	Name	Designation	Posting
1	Mr. Azhar Khan	Judge on Special Task	Mardan
2	Syed Kamal Hussain Shah	Judge, Anti-Corruption (Central)	Peshawar
3	Mr. Mohammad Tariq	Chairman, Drug Court	Peshawar
4	Mr. Muhammad Hamid Mughal	Member, Khyber Pakhtunkhwa Service Tribunal	Peshawar
5	Mr. Safi ullah Jan	ADJ- Additional District & Sessions Judge	Lakki
6	Mr. Mamriz Khalil	Additional District & Sessions Judge	Kabal (Swat)
7	Mr. Fazal Sattar	ADJ- Additional District & Sessions Judge	Paharpur (D.I.Khan)
8	Ms. Shahnaz Hameed Khattak	ADJ- Additional District & Sessions Judge	Abbottabad
9	Mr. Hayat Gul	ADJ- Additional District & Sessions Judge,	D.I.Khan
10	Ms. Sumbal Naseer	ADJ- Additional District & Sessions Judge,	Dargai (Malakand)
11	Mr. Ghulam Abbas	ADJ- Additional District & Sessions Judge,	Mansehra
12	Mr. Ahmed Iftikhar	ADJ- Additional District & Sessions Judge,	Chitral
13	Mr. Fareed Khan Alizai	ADJ- Additional District & Sessions Judge,	Buner
14	Ms. Alia Sadia Lodhi	ADJ- Additional District & Sessions Judge,	Peshawar

ANNEX-B LIST OF PARTICIPANTS

15	Mr. Jamal Shah Mehsud	ADJ- Additional District & Sessions Judge,	Kohat
16	Mr. Shakir Ullah	ADJ- Additional District & Sessions Judge	Peshawar
17	Mr. Kashif Dilawar	ADJ- Additional District & Sessions Judge,	Mardan
18	Mr. Sultan Hussain	Senior Civil Judge,	Shangla
19	Mr.Tariq Abbas	Civil Judge/JM,	Charsadda
20	Mirza Muhammad Kashif	Civil Judge/JM,	Banda Daud Shah (Karak)
21	Mr. Ihsan ul Haq	Civil Judge/JM,	Bannu
22	Mr. Muhammad Mushtaq khan	Civil Judge/JM,	Kohat
23	Mr. Abdul Hassan Mohmand	Civil Judge/JM,	Matta (Swat)
24	Syed Hassan Raza Shah	Civil Judge/JM,	Balakot (Mansehra)
25	Mr. Junaid Alam	Civil Judge/JM,	Swat

KHYBER PAKHTUNKHWA JUDICIAL ACADEMY

02-days training course on "Cyber Crimes" for Judicial Officers,

2nd & 3rd November, 2017

Sitting L to R   Ms. Alia Sadia Lodhi, Mr. Namriz Khalil, Mr. Muhammad Hamid Mughal, Mr. Choudhry Ayaz, Mr. Muhammad Asif Khan (SDA), Syed Kamal Hussain Shah, Mr. Azhar Khan, Mr. Mohammad Tariq, Mr. Sohail Sheraz Noor Sani(SDR&P), Ms. Aisha Rasool(DR&P), Ms. Hajira Rahman(DJ-I), Ms. Shahnaz Hameed Khattak, Ms. Sumbal Naseer.

Standing L to R   Mr. Zia Ur Rahman (DJ-II), Mr. Ahmed Iftikhar, Mirza Muhammad Kashif, Mr. Sultan Hussain, Mr. Junaid Alam, Mr.Tariq Abbas, Mr. Fazal Sattar, Mr. Fareed Khan Afizak, Mr. Safi ullah Jan, Mr. Shakir Ullah, Syed Hassan Raza Shah, Mr. Ghulam Abbas, Mr. Muhammad Mushtaq khan, Mr. Abdul Hassan Mohmand, Mr. Jamal Shah Mehsud, Mr. - Ihsan ul Haq, Mr. Hayat Gul, Mr. Kashif Dilawar.