July-Sep 2023

CDTI, HYDERABAD Bulletin

HORIZON

Our Motto "*ज्ञानं सम्यग् वेक्षणम्*" which means
"WISDOM LIES IN PROPER PERSPECTIVE"

CENTRAL DETECTIVE TRAINING INSTITUTE
HYDERABAD BPR&D, MHA

A Quarterly Bulletin of Central Detective Training Institute, Hyderabad

MESSAGE OF THE DIRECTOR

It gives me immense pleasure that the Central Detective Training Institute, Hyderabad is going to launch its quarterly year news magazine "HORIZON" for the period Jul to Sept, 2023.

CDTI, Hyderabad is declared as Centre of Excellence for “Police Information Technology and Cybercrime” and coupled with the establishment of “National Cyber Research, Innovation and Capacity Building Centre (NCRI&CB)” under the Indian Cyber Crime Coordination Centre (I4C), MHA, enabled CDTI-Hyderabad to hone the investigative skills of police officers in the field of cybercrimes. In 2021-22, four courses have been successfully conducted at NCRI&CB Lab on “Cyber Crime Investigation & Digital Forensics” in which 94 Police Officers trained. In 2022-23, Six courses have been conducted at NCRI&CB Lab in which 184 Police Officers were trained. In this Year, so far Eight courses have been conducted at NCRI&CB Lab in which 235 Police Officers were trained. I am sure that the training in the NCRI&CB Lab will give a great amount of confidence and success to the LEAs in the investigation of cyber crime cases.

I am glad to inform you that CDTI - Hyderabad is accredited as “उत्तम” under the Capacity Building Commission’s National Standards as assessed by National Accreditation Board of Education and Training (NABET).

It has been our continuous endeavor to improve the investigative skills of the Law Enforcement Officers and I am proud to say that we are moving in the right direction.

KRANTHI KUMAR GADIDESI, IPS
DIG/ DIRECTOR

CONTENTS

ABOUT TRAINING

Central Detective Training Institute, Hyderabad imparts training to the client state police officers of Andhra Pradesh, Telangana, Karnataka, Tamil Nadu, Kerala, Maharashtra, Puducherry, Delhi, Gujarat and Lakshadweep. It also imparts training to Police Officers of other States/ UTs and CRPF, BSF, CISF, SSB, RPF on the courses related to cyber crime cases. Armed Personnel from Army, Navy and Air Force are also given training on their request. Each state/ organization is allotted 02 seats in each course and if a particular state requests for more number of seats, the same is catered to.

This year (2023-24), CDTI, Hyderabad got approval from the BPR&D Hqrs for conducting 82 courses which includes Workshops, Webinars, Conferences, ITEC courses and Awareness Programmes. Based on the duration of course, some of the courses of duration one day are conducting in 'Online' and remaining courses in 'Offline' mode.

The Institute conducts long term as well as short term courses which deal mostly with investigation and various aspects of policing. The Institute conducts two long term courses in every academic year. "Advanced Course on Investigation & Detection of Crime" of 10 weeks duration were scheduled to conduct from 03.07.2023 to 08.09.2023 and 30.10.2023 to 05.01.2023. It is the flagship course of the institute. Conducted "138th Advanced Course on Investigation & Detection of Crime" of 10 weeks duration from 03.07.2023 to 08.09.2023 and trained 11 officers from State/ UT/ CPMFs.

The institute also conducts short-term courses of 1 day, 5 days and 10 days duration on various topics of contemporary interest concerning modern day policing, besides various Webinars & Workshops', and Awareness Programmes.

COURSES CONDUCTED FROM JULY – SEPTEMBER, 2023

From 01st July to 30th September, 2023 a total of 21 Courses (including 01 Flagship course, 03 Workshops, 02 Webinars, 01 Conference and 05 Courses related to NCRI&CB) were conducted in which 513 Officers were trained from State/UT and CPMFs.

S.NO.	Name of the Course	Date		No. of Participants
		From	To	
1	Intermediate Course on "Cyber Crime Investigation & Digital Forensics"	03.07.23	07.07.23	29
2	Dark Web, Crypto Currency & Block Chain Technology	03.07.23	07.07.23	17
3	138th Advanced course on Investigation & Detection of Crime	03.07.23	08.09.23	11
4	Workshop on Deep and Darkweb & Block Chain Forensics	06.07.23	06.07.23	31
5	Webinar on AI and Block Chain based cyber crime investigation	07.07.23	07.07.23	23
6	Course on Drones Investigation	10.07.23	14.07.23	18
7	Conference on Cyber Crime Investigation SOPs	14.07.23	14.07.23	23
8	Cyber security & incident response	24.07.23	28.07.23	19
9	Open Source Intelligence Gathering Techniques (OSINT)	31.07.23	04.08.23	17
10	Basic Course on "Cyber Crime Investigation & Digital Forensics"	31.07.23	04.08.23	28
11	Intermediate Course on "Cyber Crime Investigation & Digital Forensics"	07.08.23	11.08.23	28
12	Latest trends in Cyber Crimes - case studies with SOPs	07.08.23	11.08.23	25
13	Basic Course on "Cyber Crime Investigation & Digital Forensics"	14.08.23	18.08.23	29
14	Intermediate Course on "Cyber Crime Investigation & Digital Forensics"	21.08.23	25.08.23	28
15	Workshop on CCTV investigation	17.08.23	17.08.23	48
16	Webinar on Ethical and legal implications of AI in Cyber Crime Investigation	18.08.23	18.08.23	39
17	Negotiation	28.08.23	01.09.23	19
18	Soft Skills, Communication skills and public dealing	04.09.23	08.09.23	15
19	Emerging trends in Forensic Science/ Contemporary forensics for Ios	11.09.23	15.09.23	12
20	Workshop on latest trends in cyber crimes	21.09.23	21.09.23	61
21	Workshop on Investigating cloud based cyber crime	26.09.23	26.09.23	36
TOTAL				**556**

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on"Drones Investigation"

10-07-2023 to 14-07-2023

tting (L to R) S/Sri :- Rushikesh Aghav, Digital Forensic Expert. NCR & IC,BPRD, R.S.Jaya Kumar, Vice Principal, CDTI,Ms.Kavitha Sharma, Inspr(Rajasthan), Sh.Kranthi Kumar Gadidesi, IPS, DIG/Director,CDTI, Nagendra Prasad K.V, PI(Kar), D.Srinivasa Rao, RI(AP), Anasuya Baral, Dy.SP, CDTI.

anding 1 (L to R) S/Sri :- Ch.Jeevan, RSI(TS),Akula Srinivas, SI(TS),Amrendra Kumar, SI(Jharkhand),Dev Raj, SI/Tele, ITBP, M.Prashanth, SI(TS), Smt.Gunna Shruthi, SI(TS), Laxmzn Kumar Ram, SI(Jharkhand), B.Naresh, SI(TS), D.Anjaneyulu, SI(TS), Shaga Sai Krishna, RSI(TS), Ravi Kant Prasad, Sub-Inspr(Bihar).

anding 2 (L to R) S/Sri :- Nalla Venkata Ramana, SI(TS), Sreedasan M.V, SI(Ker), N.Vasanth Kumar, Inspr(TS), Raju, PSI(Kar).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Basic and Intermediate Course on"Cyber Crime Investgation and Digital Forensics"

26-06-2023 to 07-07-2023

Sitting (L to R) S/Sri :- Rushikesh Aghav, Digital Forensic Expert, NCR & IC,BPRD, S.Jaya Kumar, Vice Principal, CDTI, B.Rajendran, Addl.SP(TN), Sh.Kranthi Kumar - Gadidesi, IPS, DIG/Director,CDTI, Selvasekar, Dy.SP(TN), Devendhiran C, Inspr(TN), M.S.Venugopal, Dy.SP, CDTI.

Standing 1 (L to R) S/Sri :- Bishwajit Thakur, SI(Jharkhand), Sivasakthi D, SI(TN),Vijay Kumar Mishra, Inspr, SSB, T.Venugopal, RSI(AP),M.Selvam, Inspr(TN),T.Selvi, SI(TN), Kavitha Periyanayagam, Inspr(TN), Ms.Siva Meena A, SI(TN), Anu Raj.R, SI(Ker), Alagupandi.P, SI(TN), Rahul Kumar, SI, SSB, Damodar Prasad Mishra, Inspr(Chhattisgarh).

Standing 2 (L to R) S/Sri :- Arvind Kumar, SI(Bihar), Sachin Arjun Limkar, PSI(Mah), Prasanth CP, SI(Ker), Rakesh Kumar Suryakant Thakar, PI(Guj), Manjur Alam, - - SI(Kolkata Police), Kishore Sathwara, SI(Guj), Prince George, SI(Ker), Subash P A, SI(Ker).

Standing 3(L to R): S/Sri :- A.M.Dara, Inspr(Ker), Deepak Ravindra Desale, PSI(Mah), Digambar Hiraman Thorat, SI(Mah), Thiyagarajan G, SI(TN), Debabrat Phukon, - - SI(Assam), Sarvjeet Kumar, SI(Jharkhand).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on"Dark Web, Crypto Currency & Block Chain Technology"
03-07-2023 to 07-07-2023

Sitting (L to R) S/Sri :- Surinder S.Chahal, Inspr(DP), R.S.Jaya Kumar, Vice Principal, CDTI, Dharmender Kumar, ACP(DP), Sh.Kranthi Kumar Gadidesi, IPS, - - DIG/Director,CDTI, Ashish Singh, AC/GD, ITBP, Akhilesh Rao Kanduri, Cyber Crime Investigator, P.Ayub Khan, Dy.SP, CDTI.

Standing 1 (L to R) S/Sri :- Vampu Vijay Kumar, Inspr(TS),Kumar Kunal Saurav,SI(Bihar),Robert Anthony Dkhar, Inspr(Meghalaya),Kyrshan Khardewsaw,SI(Meghalaya),- Tejinder Singh, SI(Ladakh), Narasimha Murthy. N, PI(Kar), Sushil Kumar Marandi, SI(Jharkhand), Nirabhay Kumar, SI(Bihar), Sandra - - Veeraiah, Inspr(TS), D.Venkat Reddy, SI(TS), Rajesh Kumar Meena, Inspr(Rajasthan).

Standing 2 (L to R) S/Sri :- Kontham Sujith, RSI(TS), Shivayogi Lohar, PI(Kar), ch.Ankuraj, SI(TS).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on "Cyber Security & Incident Response"
24-07-2023 to 28-07-2023

Sitting (L to R) S/Sri :- Rushikesh Aghav, Digital Forensic Expert, NCR & IC,BPRD, Anand C.S, Dy.SP(Kar), S.Jaya Kumar, Vice Principal,CDTI, Ashish Kumar,A.C,ITBP, Sh.Kranthi Kumar Gadidesi, IPS, DIG/Director,CDTI, Kuncham Ramesh, Dy.SP(TS), Anasuya Baral, Dy.SP, K.Nagaraja Rao, Dy.SP(Law), Ms.Divya A.K, Cyber Trainer.

Standing 1 (L to R) S/Sri :- Sharath Kumar H.P, PI(Kar), Ram Kishore Joshi, SI(MP), Gopa Kumar G, Inspr, ITBP, Anup Kumar Thakur, SI(Bihar), Ms..R.Shobha, SI(TS), Manoj Kumar, SI(Jharkhand), Vikas Channaveer Dindure, PI(Mah), Purushottam Maheria, CI(Rajasthan Police), Chittari Ajay, Inspr(TS), Kodityala Sharath Chandra, SI(TS).

Standing 2 (L to R) S/Sri :- Vijay Abbas Waghmare, API(Mah), P.Stalin, RSI(AP), Manoj Kumar Mahato, SI(Kolkata Police), B.Anjaneyulu, RSI(AP), Sushil Kumar, SI, BSF, Azhar Nasir Shaikh, PSI(Mah).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on "Open Sourse Intelligence (OSINT) Gathering Techniques"
31-07-2023 to 04-08-2023

Sitting (L to R) S/Sri :- Rushikesh Aghav, Digital Forensic Expert, NCR & IC,BPRD, Akhilesh Rao Kanduri, Cyber Crime Investigator, Ashish Kumar, A.C, ITBP, Sh.Kranthi Kumar Gadidesi, IPS, DIG/Director,CDTI, Rakesh Kumar Chhari, Dy.SP(MP), P.Ayubkhan, Dy.SP, CDTI, Anasuya Baral, Dy.SP.

Standing 1 (L to R) S/Sri :- S.Hari Krishna, Inspr(TS), Uddhav Sadashiv Bhutekar, API(Mah),Kande Ravinder, Inspr(TS),Akula Srinivas, SI(TS),Manesh Rangnath Jadhav,- - PSI(Mah), Ms.Nasreen Begum, SI(TS), A.M.Dara, Inspr(Ker), Feesto T.D, SI(Ker), Manuraj G.P, Inspr(Ker), Gokul R, SI(Ker).

Standing 2 (L to R) S/Sri :- A.Satyanarayana, Inspr(TS), Kadali Venu Gopal, SI(AP), Shrikant Kumar, SI(Jharkhand), M.Suresh Kumar Reddy, SI(AP), Pradeep Kumar, - - SI(Bihar).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" Latest Trends in Cyber Crimes, Case Studies and SOP's "
07-08-2023 to 11-08-2023

Sitting (L to R) S/Sri :- R.S.Jaya Kumar, Vice Principal, CDTI, Rahul Kumar Uyake, Dy.SP(Chhattisgarh), Yakshvender Pundir, Asst.Commandant, CISF, Sh.Kranthi Kumar Gadidesi,IPS,DIG/Director,CDTI,Kothuri Sunil Kumar, Asst. Commandant,CRPF,Ms.Anasuya Baral,Dy.SP, CDTI, M.S.Veugopal Rao, Dy.SP, CDTI.

Standing 1 (L to R) S/Sri :- Nighil S, SI(Ker), Jeetendra Kaushle, Inspr(Chhattisgarh), Pramendra Singh, Inspr.(Del), Devendra Kumar Meena, Inspr. CRPF, Smt.Smita - - Shankar Sutar, PI(Mah), Smt.Parvin Tarachand Yadav, PI(Mah), Ms.Hardi Jayantibhai Patel, PI(Guj), Amit Kumar, SI(Del), Anurag Harsh, - - SI(Bihar), Kannan, SP,SI(Ker), Nidhin Raj S, SI(Ker), Ajay Chouhan, SI/EXE, CISF.

Standing 2 (L to R) S/Sri :- G.Shanmukharao, RSI(AP), Chaudhari Kamlesh Kavjibhai, PSI(Guj), Manish Singh Charan, Inspr(Rajasthan), Paramesha D.G, PSI(Kar), Ravi Kumar Meena, SI, RPF, M.Prasanna Kumar, SI(TS), D.Naresh Kumar, Inspr(TS), Kadari Vinod, Inspr(TS), Binoj S, Inspr(Ker), Sajesh C.Jose, SI(Ker).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on"Cyber Crime Investigation & Digital Forensics(Basic & Intermediate)"
31-07-2023 to 11-08-2023

Sitting (L to R) S/Sri :- Riyaz Sarvaiya,ACP(Guj),R.Muthamilselvan, ADSP(TN),R.S.Jaya Kumar, Vice Principal,CDTI,D.Kumar, ADSP(TN),Sh.Kranthi Kumar Gadidesi, -IPS, DIG/Director, CDTI, K.Nagaraja Rao, Dy.SP(Law), N.K.Selvaraj, ADSP(TN), Vishwas K.M, AC,SSB, Sandeep Mudalkar, Cyber Crime - - Investigator.

Standing 1 (L to R) S/Sri :-Rajaram M, SI(Technical)(TN), Anoop A, Inspr(Ker), Sreejesh P.S, Inspr(Ker), Ms.Vasanthi P, Inspr(TN), Ms.Uvapriya.P, Dy.SP(TN), Ms.Gaddam - -Vasavadatta, SI(TS), Ms.V.Rama, Inspr(TN), Ms.Jakkula Manjula, Inspr(TS), Suresh Sayaji Korabu, API(Mah),Jangili Ramesh,SI(TS),Rakesh- - Kumar Mahto, SI(Jharkhand), Raguvaran R, SI(TN).

Standing 2 (L to R) S/Sri :- Anoob Kumar E, Inspr(Ker), Amal K.S, Inspr(Ker), Kolimi Subhash, SI(TS),Nikhil K.K, Inspr(Ker),T.S.Kailasam, Inspr(TN), Rajesh Kumar Hazra- - SI(Jharkhand), Raj Kumar A, Inspr(TN),Mansinh Nurjibhai Vasava, PSI(Guj), Raghubansh Kumar Singh, SI(Jharkhand), Baidyanath - - Nayak, SI(Odisha), Rajesh Kumar Yadav, SI(Commn)SSB.

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" Cyber Crime Investigation & Digital Forensics (Basic & Intermediate)
14-08-2023 to 25-08-2023

Sitting (L to R) S/Sri :- Rushikesh Aghav, Digital Forensic Expert, NCR & IC, BPRD, Akhilesh Rao Kanduri, Cyber Crime Investigator, R.S.Jaya Kumar, Vice Principal, - CDTI, Dharmana Ravi Teja, AC, SSB, Sh.Kranthi Kumar Gadidesi,IPS,DIG/Director,CDTI, Tapas Chandra Pradhan, ACP(Odisha), Ishvarbhai - - Narsinhbhai Parmar, ACP(Guj), Ms.Priyadharshini R, Dy.SP(TN), P.Ayubkhan, Dy.SP, CDTI.

Standing 1 (L to R) S/Sri :- Palvannanathan A, SI(Tluk)(TN), Anoop P.G, SI(Ker), Velmurugan K, SI(Taluk)(TN), N.Thirukumaran, SI(Taluk)(TN), Ms.Tamannaben Ashok - - Bhai Desai, PI(Guj), Ms.Uma Reddaboina, SI(TS), Ms.Vethapravi P, Inspr(TN), Avinash Hembrom, SI(Jharkhand), Gajanan Ramdas Tamte - - PI(Mah), Rakesh S.V, SI(Ker), Sudhi K.Sathyapalan, SI(Ker).

Standing 2 (L to R) S/Sri :- Shankar Ram, SI(Jharkhand), B.Dhanasekaran, SI(Taluk)(TN), Ram Kishore, SI(Comnd), SSB, Dwijesh S, Inspr(Ker), Kumaran T.K, Inspr(TN), Avinash A, Nalegaonkar, PSI(Mah), Vinoj A, SI(Ker).

Standing 3 (L to R): S/Sri :- N.Kottieswaran, ADSP(TN), R.Kishore, RSI(TS), Satish L, SI(Taluk)(TN), Jees Mathew, SI(Ker), Sanjeev Kumar, SI(Jharkhand), Kutla Srinivas, - SI(TS), Abdul Jaleel K, SI(Ker).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" Soft Skills, Communication Skills and Public Dealing"
04-09-2023 to 08-09-2023

Sitting (L to R) S/Sri :- P.Ayubkhan, Dy.SP, CDTI, R.S.Jaya Kumar, Vice Principal,CDTI, Dharmendra singh, AC, CRPF, Sh.Kranthi Kumar Gadidesi, IPS,DIG/Director, CDTI, Dr.B.Vijaya Raghu Rama Raju,Director Prastav Solutions Motivational Speaker, Ms.Divya A.K, Cyber Trainer,Ms.Anusuya Baral,Dy.SP, CDTI.
Standing 1 (L to R) S/Sri :- Rohit, SI/Exe, CISF, Gunjan Kumar, SI(Jharkhand), Ch.Pitchi Reddy, RI(TS), Sonal Ashish Kujur, SI(Jhakhand), Ravi Kant Dariya, Inspr(Raj), Mrs.Sushma,SI(Del), Balaji Macchindra Maske, PSI(Mah), P.Prabhakar, SI(TS), Sabir Hossain, SI(WB),Uttam Singh, SI, CISF.
Standing 2 (L to R S/Sri :- Razak Madar, RSI(Kar), Niladri Mali, PSI(WB), R.Chandra Kumar, SI(TN), Manmohan Sharan, PSI(Bihar).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

138th Advanced Course on" Investigation and Detection of Crime"
03-07-2023 to 08-09-2023

Sitting (L to R) S/Sri :- Susheel Kumar, Insp(GD) SSB, R.S.Jaya Kumar, Vice Principal,CDTI, Sh.Kranthi Kumar Gadidesi, IPS,DIG/Director, CDTI,S.Sai Krishna, Dy.SP,CDTI, Ms.Anusuya Baral, Dy.SP, CDTI.
Standing 1 (L to R) S/Sri :- Gannamaneni Sravan Kumar, SI(TS), Mahesh Jagannath Karche, PSI(Mah), Sadanand, SI(Jharkhand), Amit Kumar Gupta, SI(Jharkhand), Ms.Pushpa, DSI(Kar), Medhulkumar Sindhav, PSI(Guj), Kanhiya Ram, Sub/GD, Assam rifles, Lalchand Mahato, SI(Jharkhand), Pushpendra - - Rajput, SI, SSB, Anil Kumar, Insp(GD) SSB.

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" Emerging Trends in Forensic Science / Contemporary Forensics For IOs"
11-09-2023 to 15-09-2023

Sitting (L to R) S/Sri :- Ms.Anusuya Baral, Dy.SP, CDTI, Anurag Dangi, Asst.Commandant, CRPF, R.S.Jaya Kumar, Vice Principal,CDTI, S.Desigan, Dy.SP(TN), M.S.Venugopal Rao, Dy.SP, CDTI.
Standing 1 (L to R) S/Sri :- Sanal S, Inspr(Ker), S.Deepak, SI(TS), Sundhara Moorthy. N, SI(TN), Virendra Kumar Choren, SI(Jharkhand), Smt.S.Padma, SI(TS), Suman Mallick, SI(WB), Joy P.P, Inspr(Ker), S.K.Rahamat, SI(WB), Md.Maqsud Ahmed, SI(Jharkhand), Debi Prasad Sahoo, SI(Odisha).

ACTIVITIES AT CDTI, HYDERABAD

1. 97 Intermediate students of Deeksha Junior Colleges, Hyderabad visited CDTI, Hyderabad on 13.07.2023. They have been briefed about the various training modules/ activities conducted at the Institute as well as visited NCRI&CB Lab and the premises.

2. Sh. Sriram Taranikanti, IAS, Addl. Secretary, MHA visited CDTI, Hyd on 02-08-2023. He interacted with the officers of CDTI-Hyd about its functioning and training being imparted. He went around the CDTI-buildings, observed the training sessions. Thereafter, he visited CFSL, Hyd.

3. The 77th Independence Day was celebrated at CDTI, Hyderabad. All the staff participated in the celebration along with their families. Director, in his speech, honoured the freedom fighters leaders who sacrificed their lives for India's freedom

4. The Officers, staff and trainee officers of CDTI-Hyderabad watching the LIVE telecast of Chandrayaan-3 landing on moon on 23-08-2023.

5. The 138 Advance Course on Investigation and Detection of Crime was conducted at CDTI, Hyderabad from 03.07.2023 to 08.09.2023. 11 Officers from various States/CPMFs attended the Course.

6. On 12.09.2023, 72 Officers (67 SIs & 05 Inspectors) and On 14.09.2023, 70 Officers (61 SIs & 09 Inspectors) of CRPF, Barkas, Chandrayangutta, Hyderabad visited CDTI, Hyderabad on Study tour. They have been briefed about the various training modules/activities conducted at the Institute as well as visited NCRI&CB Lab and the premises.

7. 14.09.2023 को सीडीटीआई, हैदराबाद में हिंदी दिवस मनाया गया। अध्ययन दौरे पर आए सभी कर्मचारी/अधिकारी और 70 सीआरपीएफ प्रशिक्षु एसआई ने भाग लिया।

8. Conducted an awareness programme on 'Cyber Stalking/ Cyber Bullying and Cyber Crime Against Women' on 26.09.2023 at the Seminar Hall of CDTI, Hyderabad. 80 students and 04 lecturers of MLR College, Hyderabad participated.

Cybercrimes against women & children - SOPs for investigating them

Sh. M S Venugopal Rao
Dy. SP, CDTI, Hyderabad
SP (Retd), Telangana)

Types of Cybercrimes Against Women and Children:

Cyber bullying: This includes online harassment, threats, and the spread of harmful or defamatory content through social media, email, or other digital platforms.

Online Grooming: Predators may target children and adolescents online to build trust and manipulate them into engaging in inappropriate or illegal activities.

Online Harassment and Stalking: Perpetrators may continually harass, threaten, or stalk victims using various online means, causing emotional distress and fear.

Non-consensual Sharing of Intimate Content (Revenge Porn): Sharing explicit images or videos without the consent of the person involved is a serious violation of privacy and can have severe emotional and psychological consequences.

Child Exploitation: This involves the creation, distribution, or possession of explicit images or videos of children, often referred to as child pornography.

Sexting: Involves the sending or receiving of sexually explicit messages, images, or videos, typically between teenagers.

Online Scams and Fraud: Women and children can be targeted by scams and fraudulent schemes, such as phishing, cat fishing, or online dating scams.

Standard Operating Procedures (SOPs) for Investigating Cybercrimes Against Women and Children:

Immediate Response:

Report the incident to the appropriate authorities, such as local law enforcement or a specialized cybercrime unit.
Preserve digital evidence by taking screenshots, recording URLs, and documenting relevant details.
Encourage victims to seek emotional support and counseling.
Forensic Analysis:

Employ digital forensics experts to collect and analyze digital evidence from devices, servers, or online platforms.
Maintain a chain of custody for evidence to ensure its admissibility in court.
Victim Support and Protection:

Ensure the safety and privacy of the victim throughout the investigation.
Connect victims with support services, including counseling and legal assistance.
Legal Considerations:

Determine applicable laws and jurisdiction for the specific cybercrime.
Prepare search warrants or subpoenas for relevant digital records and user information.

Collaboration:
Collaborate with internet service providers, social media platforms, and technology companies to access user data and cooperation in the investigation.

Training:
Train law enforcement personnel and digital forensics experts to handle cybercrime cases involving women and children sensitively and effectively.

Prosecution:
Build a strong case with the evidence collected and ensure that the perpetrators are appropriately charged and brought to justice.
Prevention and Awareness:
Conduct awareness campaigns to educate women, children, and parents about online safety and the risks of cybercrimes.
Promote responsible digital behavior and reporting mechanisms.
It's essential to approach these cases with sensitivity, empathy, and a focus on the well-being of the victims. Additionally, laws and procedures may vary by jurisdiction, so it's crucial to work within the legal framework of your region when investigating cybercrimes against women and children.

Deepfakes: A New Tool for Propaganda and Disinformation

Rushikesh Aghav,
Digital Forensic Expert
NCRI&CB Lab, I4C, MHA.

In the ever-evolving realm of technology, deepfakes have emerged as a powerful tool with the potential to manipulate and deceive. These synthetic media creations, often in the form of videos, audios, or images, can seamlessly replace a person's face, voice, or body with that of another, making it increasingly difficult to discern reality from artifice. This ability to seamlessly fabricate content has raised serious concerns about the potential misuse of deepfakes for propaganda and disinformation purposes.

The Power of Deepfakes

Deepfakes leverage artificial intelligence (AI) and machine learning techniques to create remarkably realistic and convincing media. By analyzing vast amounts of source data, these algorithms can learn the facial expressions, vocal intonations, and physical mannerisms of target individuals, enabling them to create synthetic content that appears authentic. This ability to mimic reality poses a significant threat, as it allows malicious actors to create deepfakes that can be used to spread misinformation, damage reputations, and sow discord.

Propaganda and Disinformation in the Digital Age

The rise of social media and the proliferation of online platforms have created an unprecedented opportunity for the dissemination of information, both genuine and fabricated. Deepfakes, with their ability to bypass traditional gatekeepers and spread rapidly through social networks, have become a potent weapon in the hands of those seeking to influence public opinion and manipulate perceptions.

The Impact on Society

The potential impact of deepfakes on society is far-reaching and multifaceted. The erosion of trust in information sources, the spread of misinformation, and the manipulation of public opinion can have profound consequences for individuals, communities, and nations.

Deepfakes can be used to damage reputations, harm businesses, and sow discord among social groups. They can also be employed to manipulate elections, undermine democratic processes, and incite violence. The ability to fabricate content that appears authentic can have a chilling effect on free speech and the pursuit of truth.

Addressing the Challenge

Technological Countermeasures: Developing techniques to detect and debunk deepfakes, such as analyzing video artifacts and identifying inconsistencies in facial expressions or lip movements.

Public Awareness: Educating the public about deepfakes, how to spot them, and the dangers they pose.

Legal Frameworks: Establishing legal frameworks to hold those responsible for creating and disseminating malicious deepfakes accountable.

Responsible AI Development: Promoting ethical guidelines and standards for the development and use of AI technologies, including deepfakes.

How to Spot a Deepfake?

Deepfakes, synthetic media that use artificial intelligence to create realistic videos or audio recordings of people saying or doing things they never actually said or did, have become increasingly sophisticated, making it more challenging to distinguish them from real media. However, there are still some signs that can help you identify a deepfake.

- **Unnatural Facial Expressions and Movements**

  Deepfakes often exhibit subtle imperfections in facial expressions and movements. Look for inconsistencies in the way the person's mouth forms words, their blinking patterns, and the synchronicity between facial expressions and the audio. In deepfakes, these elements may appear unnatural or slightly off-sync.

- **Skin Tone and Texture Anomalies**

  Pay close attention to the person's skin tone and texture. Deepfakes may struggle to accurately replicate skin imperfections, such as moles, wrinkles, or blemishes. The skin may appear too smooth or lack the natural variations in tone and texture that are characteristic of real skin.

- **Lighting and Shadow Incoherencies**

  Examine the lighting and shadows in the video. Deepfakes may exhibit inconsistencies in lighting and shadow patterns, particularly around the edges of the person's face or hair. The shadows may appear too dark or too light, or they may not align correctly with the surrounding environment.

- **Audio Quality and Lip-Syncing**

  Assess the audio quality and lip-syncing in the video. Deepfakes may have slightly distorted audio or noticeable mismatches between the person's mouth movements and the audio. The audio may sound artificial or robotic, and the lip-syncing may appear unnatural or out of sync with the words being spoken.

- **Background Inconsistencies**

  Observe the background of the video. Deepfakes may exhibit inconsistencies in the background, such as blurry or poorly rendered objects, or inconsistencies in lighting or shadows. The background may appear too static or lack the subtle movements that are characteristic of a real environment.

- **Metadata and Source Information**

  Check the metadata and source information associated with the video. Deepfakes may have inconsistent or misleading metadata, such as the wrong file creation date or discrepancies in the location or camera information. Be cautious of videos shared from unverified sources or websites.

- **Rely on Reputable Sources**

  When consuming online content, prioritize reputable sources and established news organizations. These sources have editorial processes in place to verify the authenticity of content and are less likely to disseminate deepfakes.

- **Utilize Fact-Checking Tools**

  Employ fact-checking tools and websites to verify the authenticity of videos or audio recordings. These tools can analyze the content, identify potential inconsistencies, and provide additional information or context.

- **Seek Expert Opinion**

  If you have concerns about the authenticity of a video or audio recording, consider seeking the opinion of experts in deepfake detection or digital forensics. They can provide a more in-depth analysis and assess the likelihood of the content being a deepfake.

- **Stay Informed and Alert**

  Stay updated on the most recent advancements in deepfake technology and the methodologies employed to produce and identify them. As deepfake technology continues to evolve, it is crucial to stay informed and maintain a critical eye when evaluating online content.

Unveiling the Truth: Deception Detection with EDS

Ms. Divya,
Guest Faculty
CFSL, Hyderabad

In the realm of security and investigative procedures, the ability to distinguish truth from deception is of paramount importance. Traditional methods of lie detection have often relied on polygraph tests, which measure physiological responses such as heart rate and sweating. However, these methods can be intrusive and, at times, unreliable. The Eye Detection System (EDS) is a groundbreaking technology that offers a promising alternative for deception detection.

The Power of EDS in Deception Detection

Understanding Deception

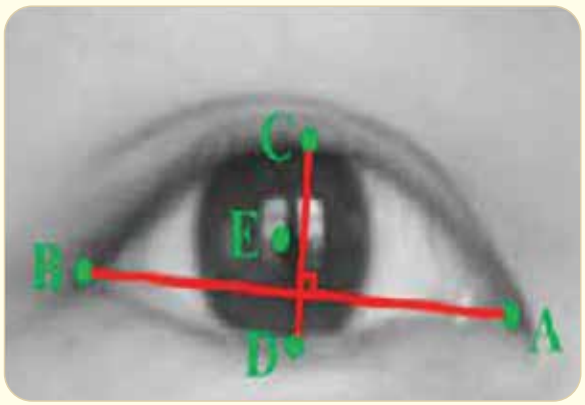
Deception detection involves identifying when an individual is not truthful or is attempting to conceal information. It plays a pivotal role in various domains, including law enforcement, border security, and even corporate investigations. The ability to accurately detect deception can mean the difference between uncovering critical information and being misled.

How EDS Detects Deception

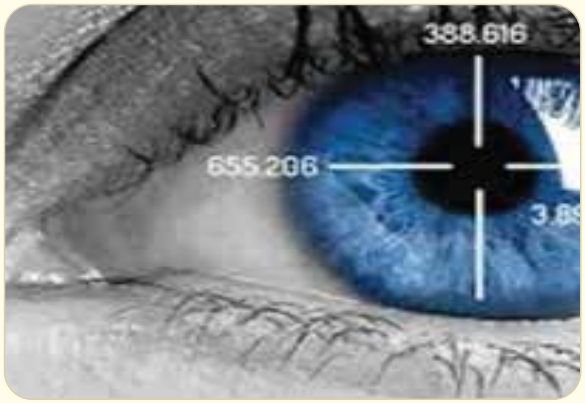
Deception detection involves identifying when an individual is not truthful or is attempting to conceal information. It plays a pivotal role in various domains, including law enforcement, border security, and even corporate investigations. The ability to accurately detect deception can mean the difference between uncovering critical information and being misled.

Firstly, a baseline has to be established in order to understand every individual's response to truth and deception. There are various ways to establish a baseline, here is an example. The subject is asked to sit comfortably and interact with the EDS system. The subject is instructed to pick a number between say, 1 and 12. Then the subject is asked to try and deceive the EDS by giving wrong answers to questions like "Did you pick the number 4?" This way, the system registers cues to determine the "tells" of this individual and establishes a baseline for comparison. When the real questions are asked in the interview, the EDS compares the subject's reaction to the baseline to comprehensively determine anomalies and flag them.

EDS employs a unique approach to deception detection by analysing specific eye-related physiological and behavioural patterns. Here's how it works:



1. Eye Movement Analysis: EDS tracks an individual's eye movements using high-resolution cameras.When people are being deceptive or anxious, they may exhibit unusual or rapid eye movements, such as excessive blinking, darting eyes, or avoiding eye contact. EDS algorithms capture and analyse these patterns to identify anomalies that could suggest deception.



2. Pupil Dilation: The size of the pupil can change in response to emotional arousal, including anxiety or stress. When a person is being deceptive, their pupils may dilate or constrict involuntarily. EDS tracks these changes in real-time during conversations or interactions, flagging potential deception based on variations in pupil size. When a person is deceptive or anxious, their pupils may dilate or constrict. EDS monitors changes in pupil size during conversations or interactions to flag potential deception.

3. Gaze Direction: The direction in which a person looks while speaking can provide insights into their thought processes. Individuals avert their gaze when discussing sensitive or deceptive topics. Shifting eye gaze away from the listener during dishonesty or deception can be a revealing indicator which can be flagged by the EDS.

4. Micro expressions: EDS can capture microexpressions – fleeting, involuntary facial expressions that reveal concealed emotions. When a person is deceptive, micro expressions may betray their true feelings despite their efforts to maintain a composed facade.

5. Baseline Comparison: EDS establishes a baseline for an individual's eye-related behaviour during a neutral or non-deceptive state. Subsequent interactions are compared to this baseline to identify deviations or anomalies that may signal deception.Since human subjects are involved, each baseline is unique to that individual. For example, some people may have a high blink-rate even under normal circumstances. The system relies on deviations from the individual's normal eye behaviour to raise suspicion.

6. Pattern Recognition Algorithms: The core of EDS lies in the sophisticated pattern recognition algorithms that process the data collected from eye-related behaviours. These algorithms analyse multiple facets of eye behaviour simultaneously, considering factors like blink rate, gaze direction, and pupil size. The system then applies statistical and machine learning techniques to assess the likelihood of deception.

7. Data Integration: EDS integrates data from various sources, including eye tracking cameras and facial recognition technology. By combining information from different sensors and data points, EDS provides a holistic view of an individual's behaviour during an interaction. Since multiple factors are taken into consideration holistically, the results and interpretations are highly accurate.

Advantages of Using EDS for Deception Detection

The EDS software and hardware can be integrated with a wide range of set-ups and workstations. The EDS can prove helpful in entry and exit points at airports, bus stations, railway stations, government offices and other places of importance where suspects can easily be screened without alerting them and creating a possibly threatening situation. The integration of EDS into deception detection processes offers several notable advantages:

1. Non-Intrusive and Non-Contact: Unlike traditional lie detection methods, which may involve physical sensors and invasive procedures, EDS is non-intrusive and non-contact. Individuals being assessed for deception need only engage in a conversation or interaction with an EDS-equipped system, eliminating the discomfort associated with traditional methods. The software and system are easy to integrate anywhere.

2. High Accuracy: The intricate analysis of eye-related patterns by EDS provides a high level of accuracy in deception detection. The analytical aspects of eye changes are measured with very high accuracy, which may not be detected by investigators. By scrutinizing multiple facets of eye behaviour simultaneously, EDS can provide a comprehensive assessment of an individual's truthfulness.

3. Objective Assessment: EDS offers an objective assessment of deception. Unlike human interrogators who may be influenced by personal biases or subjective judgment, EDS relies on data-driven algorithms and does not make assumptions based on appearance or stereotypes. While emotions may be faked, eye movements cannot be controlled.

4. Real-Time Analysis: EDS can analyse eye-related data in real-time, allowing for immediate feedback during interviews or interactions. This feature enables investigators to adjust their approach based on the detected patterns of deception, potentially enhancing the effectiveness of their questioning.

5. Consistency: EDS provides consistent results across multiple interactions. Human operators may experience fatigue or variability in their judgment, but EDS maintains its analytical rigor throughout the assessment process.

6. Comprehensive Data Storage: EDS can store and archive data from deception detection sessions. This feature is valuable for reviewing and comparing results over time, as well as for maintaining a detailed record of interactions for investigative or legal purposes. It is also useful to detect repeat offenders.

7. Potential for Integration: EDS can be integrated with existing security and investigative systems, providing an additional layer of deception detection without requiring a complete overhaul of current practices. It can comprehensively be used during interrogations, to enhance security in places like airports, railway stations and entry points of other public places.

8. Applicability: EDS can be used for any subject and circumstance as it is independent of language, race, etc. The instructions and questions provided by the EDS can be translated by the system into any global language for a wide range of applicability. It also requires minimal human interference.

Conclusion

The Eye Detection System's application in deception detection represents a significant step forward in the quest for accurate and non-intrusive truth verification. By focusing on the subtle yet revealing behaviours of the eyes, EDS offers an objective, high-accuracy means of assessing an individual's honesty.

While EDS is a promising technology, it is essential to recognize that no single method of deception detection is infallible. EDS should be considered as a valuable tool to complement other investigative techniques and human judgment. It serves as a powerful resource for identifying potential areas of deception, prompting further inquiry and potentially leading to a more comprehensive understanding of the truth.

In many countries, the EDS is also being used during recruitment for sensitive posts. The most commonly posed questions during the screening process are “Have you ever taken drugs?” or “Have you ever stolen money?” etc. It is also deployed in airports during the security checks to detect smugglers and other suspects.

As EDS continues to advance and its integration into various industries expands, we can anticipate even greater strides in the realm of deception detection. The synergy between this cutting-edge biometric technology and the timeless quest for truth promises to uncover hidden insights and enhance the effectiveness of investigative processes world.

CENTRAL DETECTIVE TRAINING INSTITUTE HYDERABAD

BPRD
CENTRAL DETECTIVE TRAINING INSTITUTE
HYDERABAD

cdtshyderabad@nic.in
cdtihyd@gov.in
040-27038182, 27036865
@bprdcdtihyd
facebook.com/bprdcdtihyd

Address:
CDTI, Ramanthapur,
Hyderabad,Telangana,
Pin-500013