

26th -27th
June 2021

eConference Proceedings

6th International
eConference-2021

Cyber & Digital Forensics



Supported by

linktr.ee/forensicscienceinstitute

6th International eConference-2021
Cyber & Digital Forensics

In Loving Memory

Neeraj Aarora



नैनं छिन्दन्ति शस्त्राणि नैनं दहति पावकः
न चैनं क्लेदयन्त्यापो न शोषयति मारुतः

The time where we were living with endurance, losing our pillars of strength does leave us shattered for the journey yet to be completed. Through the battle, which is yet to be won, we have lost one of our dearest, talented and kindest being Neeraj Aarora Sir. The personality we idolise has left us too soon to carry forward his legacy of excellence. Neeraj Sir has been rendering his expertise as a legal adviser and consultant of CyberImmersion Solutions. He was an Advocate-on-Record (AOR), arbitrator, and consultant on cyberlaw & digital forensics. His contribution to the field of cyber & digital forensics is remarkable and inspires his younger generations. He might have gone from our sight, but never from our hearts. We have lost a part of us.



GREETINGS FROM THE ORGANIZING DESK

The new era post the global pandemic has affected academics, establishments, and individuals' preparedness worldwide. Forensic Science has an interdisciplinary approach and its true essence can be proved meaningful with collaborative efforts of people present around the globe functioning together as a team. With a vision to bring all the academicians, students, and professionals and share their valuable contemplations, the International eConference are structured to lead the way through endeavors focused to take Forensic to greater heights. We welcome every science enthusiast to become a part of this revolutionizing effort and explore the technological advancements, scientific researches, and opportunities for everyone to flourish.



Dr. Ranjeet Kr. Singh
President
International Association
Of Scientists and Researchers



Phaneendar B N
Forensic Expert, CEO
Clue4 Evidence Foundation

THE ORGANIZER

INTERNATIONAL ASSOCIATION OF SCIENTISTS AND RESEARCHERS (IASR)

IASR is a non-profit organization focused to deliver the updated literature and research work to not only the global scientific and research society, but also to everyone. Providing open access to critically reviewed high-quality research papers and literature, it works with a mission of providing a user- friendly global platforms for researchers, scientists for sharing information, and dissemination of recent ground breaking researches and advancements in various fields working together for the betterment of the world.

About the eConference

Forensic Science has proffered techniques that have leveled up the competence of humankind and are staying up with the trend. At the outset, the International Association of Scientists and Researchers (IASR) in association with the Sherlock Institute of Forensic Science (SIFS) India organizing the 6th International eConference on “Cyber & Digital Forensics”, 2021. With utmost enthusiasm, the organizing committee invites the young minds and professionals of various disciplines of forensic science and become a part of the first-ever convention organized with the motto of bringing the unrecognized talents, present globally. The program would follow talks by eminent national and international experts accompanied by e-paper presentations, ePoster presentations, discussions, and scientific excellence awards.

Mission Statement

“Committing towards the fact of being a lead-follower of technology with a bold spirit of risk-taking, helping us make our presence noticeable worldwide”.

SPEAKER'S PROFILE

DR. GAURAV GUPTA

**Ministry of Electronics & Information Technology,
New Delhi, INDIA**



Dr. Gaurav Gupta is the first Indian to earn a doctorate in the field of digital forensics. He was bestowed with the Young Scientist Award by Indian Science Congress in 2010 and received it from the Man of Science, our beloved Dr A.P.J Abdul Kalam. He is on a mission to create awareness about technological fraud in society. He has been a mentor and guide to many research students and interns. He has a rich and varied experience (almost 20 years) of working in the private as well as the public sector spanning across: KPMG in the private domain (part of the Big 4); faculty member at Indraprastha Institute of Information Technology (IIIT) Delhi; and currently working as Additional Director with the Government of India. As an active researcher of this field, he has contributed to society by developing many state-of-the-art, efficient, and effective digital forensic solutions.

RAKSHIT TANDON

Hackdev Technology Pvt Ltd., New Delhi, INDIA



Rakshit Tandon, Cyber Security Evangelist has experience of more than a decade in Security Domain. He is Founder & Director of Hackdev Technology Pvt Ltd. He is Cyber Security Consultant to Internet and Mobile Association of India. Marked as Resource Person/Visiting Faculty for Cyber Crime Investigations at BPRD for Training Law Enforcement

Officers across the Country. He is a Chairman of India against Child Abuse, A National Outreach Program by Justice Mohan Children University and NCSST. He in personal capacity has sensitized more than 4.1 million students on the issue of Cyber Safety across the nation covering more than 25 states, 4 union territories. He has played an important role contributing to Child Online Protection in India Report by UNICEF. Speaker at "Talks at Google", "TEDx Talks "has been Non-European Expert at European Commission on Safer Internet in 2010. Awarded with Karamveer Jyoti Puruskar 2019, Gurugram Achievers Award 2019, and SKOTCH GOLD Governance Award to Gurugram Police for Cyber Security Summer Internship 2019 and also awarded with Karamveer Chakra by Rex Conclive 2015 and 2016 with Gold Karamveer Chakra, Cyber Guru of the Year Award in 2015 by Government of Maharashtra and Global Cyber Crime Helpline Award in December 2018. He has been invited nationally and International Conference on Cyber Security as Key Note Speaker and Panelist.

SPEAKER'S PROFILE

SAMIR DATT

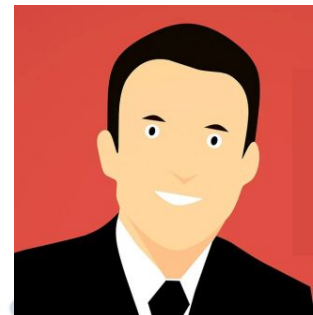
**Foundation Futuristic Technologies (P) Ltd (ForensicsGuru.com),
New Delhi, INDIA**



Samir Datt has been dabbling with digital investigations since 1988, which was around the time he solved his first case. He is the Founder CEO of Foundation Futuristic Technologies (P) Ltd, better known as ForensicsGuru.com. He is widely credited with evangelizing computer forensics in the Indian subcontinent and has personally trained thousands of law enforcement officers in the area. He has the distinction of starting the computer forensics industry in South Asia and setting up India's first computer forensics lab in the private sector. He is consulted by law enforcement agencies and private sector on various technology-related investigative issues. He has extensive experience in training thousands of investigators as well as examining a large number of digital sources of evidence in both private and government investigations. In addition, he is an author of the book "Learning Network Forensics" published by Packt Publishers, UK. He is also an Angel Investor for product start-ups in the Cyber Forensics/Investigations Field.

ABHISHEK KUMAR

Forensic Investigator, INDIA



Abhishek Kumar is an experienced fraud and cyber-crimes investigation leader with a strong Law Enforcement background. Over 10 years, he has worked with various Law Enforcement Agencies (LEAs) and Uber in India/APAC conducting complex investigations in financial frauds, internal misconduct, and cyber-crimes. He has a unique profile of working on large and varied datasets both from the perspective of law enforcement as well as a corporate investigator. This gives him the ability to think of crime/fraud detection and prevention from multiple angles and viewpoints. He has written and spoken extensively on cyber-crimes, Open Source Intelligence (OSINT), digital forensics, and cyber security. He has conducted multiple hands-on sessions for senior officers in National Police Academy, National Investigation Agency, Central Bureau of Investigation, National Customs Academy, Indian Institute of Public Administration and many state law enforcement academies. He is a visiting faculty in an International University conducting courses on cyber security and fraud detection analytics.

SPEAKER'S PROFILE

DR. RAJESH VERMA

**Regional Forensic Science Laboratory, Central Range,
Mandi, Himachal Pradesh, INDIA**



Dr. Rajesh Verma has about 30 years of experience in research and analytical work out of which more than 20 years in a Forensic Science Laboratory. He is currently working as the Deputy Director, Head of the Regional Forensic Science Laboratory, Central Range, Mandi, Himachal Pradesh supervising the work of different divisions in the laboratory. He has also served as the Assistant Director (2000-2011) in the State Forensic Science Laboratory, Head of the Physics and Ballistics Division. With this, he has also served as Project Associate in the State Council for Science, Technology, and Environment, H.P. Shimla under the Solar House Action Plan for Himachal Pradesh. He has a number of publications in renowned journals in his name. He has also been awarded the best paper presentation in numerous conferences. He has also given training to various professionals and students related to the arenas of forensic science and has been continuously contributing and sharing his pool of knowledge with others.

PROF. TRIVENI SINGH, IPS

Cyber Crime, Uttar Pradesh Police, INDIA



Prof. Triveni Singh, SP, Cyber Crime, Uttar Pradesh Police is India's first cyber cop. He has investigated more than 200 types of cybercrimes followed by arrests of thousands of criminals and solved cases involving over thousands of crores of fraudulent money. He is in charge of investigating cybercrime cases as well as providing administrative and technical supervision to 18 cybercrime police stations located at all commissionerates in the state of Uttar Pradesh. He is also the resource person for various central investigation agencies and judicial bodies such as Central Bureau of Investigation Academy (CBI), Ghaziabad, National Police Academy, Hyderabad and Institute of Chartered Accountants of India as well as different State Judicial training centres, Police Training Academies and Universities. Popular as a cybercrime investigation specialist with an intensive technical investigation process, he is known for his expertise in handling financial and banking frauds. He has shared his experiences of nabbing criminals and busting gangs in two of his books co-authored with Amit Dubey, a cyber-security expert and crime investigator – Hidden Files: Tales of Cyber Crime Investigation and Hidden Files – Unlock. He has been honoured with several distinctions, including President Medal for Gallantry by The President of India and Certificate of Honour by Director, CBI. He was also conferred with India Cyber Cop of the year award, 2012 by DSCI-NASSCOM.

SPEAKER'S PROFILE

SANTOSH KHADSARE

Digital Forensic & Incident Response Professional, INDIA

Santosh Khadsare is an InfoSec and DFIR professional who specializes in Digital Forensics and has headed the Digital Forensics Lab of CERT-India, Ministry of Electronics and IT for 2 years up to Feb 2021. He is the only person to head two different Govt. labs and notify them as Examiner of Electronic Evidence (EEE) under 79 A of IT Act. He is B.E (Electronics and Telecommunications) and possesses additional qualifications such as CHFI, CEH, RHCSA, IVTA (CMU, Pittsburgh, USA), Advance Cyber Forensic Course (CDAC), Cyber Crime Investigator (CCI), Cyber Crime Intervention Officer (CCIO) and Access Data Certified Professional. He was judged amongst top three scholars during the MDI-ISAC National Cyber Security Scholar Program for the year 2020 and was awarded for the best innovative paper titled "The Role of Digital Forensics in Industry 4.0". He has 20+ years plus of rich experience in the field of Digital Forensics, Cyber Laws, Information Security, Cyber Audit, and Incident Response. He is known in the digital forensics community for his experience, skillsets and mentorship qualities. He has been a speaker in various national and international conferences. He has authored various articles on information security and Digital Forensics in national and international publications.



DEEPAK KUMAR

Sr. Cyber Threat Intelligence & Digital Forensic Consultant, INDIA

Deepak Kumar (D3) is Sr. Cyber Threat Intelligence & Digital Forensic Consultant. He has been working on several consulting and investigating engagements with organisations such as Academia, Corporates, International Law Enforcement Organisations, Government sectors & PSUs. He is presently a member with Chair Member in National Cyber Safety and Security Standards, India; Active Member of the International Cyber Threat Task Force (ICTTF); Editorial Technical Committee Member in Digital 4n6 Journal; Technical Sr. Cyber Crime & Forensic Advisor/Investigator to various Law Enforcement Agencies-India/Kenya. He has been engaged with delivered talks/ guest-lectures /training on various domains like ethical-hacking, cyber-crimes/security, cyber threat intelligence & digital forensics. He has delivered workshops and corporate training to IT companies, esteemed academic institutions, Law enforcement and organizations; and also trained 25,000+ high-end professionals individually. Also, awarded with various industry-recognized certifications; received several appreciations from senior officials from law enforcement, academia, defence organizations and media as well. He is also a subject matter expert in the domain such as Digital Forensics, Cyber Crime, Cyber Security, Threat Intel, OSINT (Open Source Intelligence) & SOCMINT (Social Media Open Source Intelligence).



SPEAKER'S PROFILE

DUSAN KOZUSNIK

Compelson Labs, PRAGUE

Dusan co-founded Compelson Labs in 1991 while finishing his studies in computer science at Czech Technical University in Prague and has been a chief architect of software and hardware products since then. With his team, he created such software and hardware based products as PC security systems for advanced data and antivirus protection, encryption products used in banks, password management products and smart-card products for world brands. Since 1996 his effort has been concentrated on cell-phones. He designed the unique software system called MOBILedit, allowing further development of such products as phone management software, phone-copy solution, and a forensic tool for investigators, which set a global standard. He is leading the company while still working in research and development.



Chairing Panel Day 1



Chairperson
Omveer Singh

CERT-In, Ministry of Electronics &
Information Technology
New Delhi

Chairperson
Sanjay Gautam

CBI Academy
Ghaziabad



Chairperson

Dinesh O Bareja

Open Security Alliance / IndiaWatch



Chairing Panel Day 2

Chairperson

Aashish Sutar

Ministry of Defence
Govt. of India



Chairperson

Prince Boonlia

Digital 4n6 Journal
New Delhi



Chairperson

Dr. Ashish Badiye

Government Institute of
Forensic Science, Nagpur,



Chairperson for Scientific Presentations



Chairperson

Dr. Rajiv Pandey

Amity University
Lucknow

**PROFESSIONAL
CATEGORY**

PAPER PRESENTATION



Chairperson

Dr. Mukesh Sharma

State Forensic Science
Laboratory, Jaipur

**PROFESSIONAL
CATEGORY**

ePOSTER PRESENTATION

Chairperson for Scientific Presentations

Chairperson

Nitin Pandey

Police Headquarters
Lucknow



**STUDENT
CATEGORY**

PAPER PRESENTATION

Chairperson

Vinny Sharma

Galgotias University
Greater Noida,



**STUDENT
CATEGORY**

ePOSTER PRESENTATION

Professional Category

JURY MEMBERS FOR PAPER PRESENTATION



Narendra Kumar
Forensic Science Laboratory
Uttar Pradesh



Dr. Harsh Joshi
Information Security Group
HDFC Bank, Mumbai



Dr. Rakhi R. Wadhvani
Senior Assessor
Mumbai



Amrit Chhetri
IT Security, DFIR & AI Researcher
West Bengal

JURY MEMBERS FOR ePOSTER PRESENTATION



Nirali Bhatia
V4WEB Cyber Security &
Cyber B.A.A.P, Mumbai



Dr. Himanshu Khajuria
Amity Institute of Forensic Science
Noida



Dr. Gulshan Shrivastava
Sharda University
Gr. Noida



Shyam Chandel
Cyber Fraud Helpline
Udaipur

Student Category

JURY MEMBERS FOR PAPER PRESENTATION



Dr. Malvika Mehta

The Expert Witness
Pune



Mohit Yadav

Craw Cyber Security Pvt. Ltd.
India



Santosh Chaluvadi

Supraja Technologies
Vijayawada



Rohit Jain

Jain Associates
India

JURY MEMBERS FOR ePOSTER PRESENTATION



Shifa Cyclewala

Hacktify Community Virtually
Testing Foundation, United States



Rohit Gautam

Hacktify Community Virtually
Testing Foundation, United States



Shubham Gautam

Psyberbull & 3dayhack
Delhi



Vinay Singh

Forensic Science Laboratory
New Delhi

Advisory Board



Dr. HARSH SHARMA
State Forensic Science
Laboratory, M.P.



JOHN PAUL OSBORN
Forensic Document Examiner
Osborn & Son, USA



Dr. EDDY De VALCK
Academy of Forensic Medical
Sciences, Belgium



Dr. ROBERT GREEN
University Reader
University of Kent, UK



MICHAEL WAKSHULL
Forensic Document
Examiner Q9 Consulting, Inc.



Prof. EMILIO NUZZOLESE
University of Turin,
Italy



MICHAEL W. STREED
Forensic Facial Imaging Expert,
SketchCop, USA



Dr. RAJINDER SINGH
Former Director, CFSL, CBI
New Delhi



Dr. SANJEEV
Central Forensic Science
Laboratory, Chandigarh



Dr. RAKESH GOREA
Gian Sagar Medical College,
Patiala



Dr. G. K. GOSWAMY, IPS
Inspector General of Police,
Chief of ATS, Uttar Pradesh



HEIDI H. HARRALSON
Board Certified Document
Examiner Spectrum Forensic
International LLC. USA



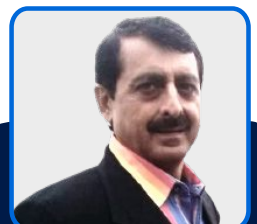
D. C. SAGAR, IPS
ADGP (PTRI) Bhopal,
M.P.



K. V. RAVIKUMAR
I/c Pro-Vice-Chancellor,
Rashtriya Raksha University Former
Dy. DIRECTOR at CFSL, DFSS, MHA



MOHINDER SINGH
Former Government Examiner
of Questioned Documents



DEEPAK HANDA
Former HOD & Principal
Scientific Officer CFSL CBI,
MHA, New Delhi



DEEPA VERMA
Forensic Science Laboratory
NCT of Delhi



Dr. RAJESH VERMA
Regional Forensic Science
Laboratory, Mandi, H.P.



JOHN PATRICK MOLONEY
Director and Co-Founder of
Forensic Comparison Software,
Australia



Dr. DANILO L. MAGTANONG
Dean, College of Dentistry,
Philippines

Advisory Board



Dr. G. S. SODHI
S.G.T.B. Khalsa College,
Delhi



Dr. SELINA LEOW
NSW Forensic Odontology Unit,
Australia



Dr. JOSEPH De LADURANTEY
The Vollmer Institute
California



Dr. MADHULIKA SHARMA
Forensic Science Laboratory
Govt. of N.C.T., Delhi, India



SANTOSH KHADSARE
Digital Forensics & Incident
Response, India



Dr. MUKESH YADAV
Government Allopathic Medical
College, India



Prof. JASON PAYNE JAMES
Sp. in Forensic & Legal
Medicine, U.K.



STEVEN DAVID LAMPLEY
The Oliphant Institute
USA



RAKSHIT TANDON
Hackdev Technology
New Delhi



Dr. V. V. PILLAY
AIMS, Kerala
India



Dr. T. B. SINGH
Central University of South
Bihar, India



Dr. VARUN KAPOOR (IPS)
ADGP, Rustamji Armed Police
Training College, India



**Dr. NILENDU BIKASH
BARDHAN**
CFSL CBI, New Delhi



**Dr. RUKMANI
KRISHNAMURTHY**
HELIK Advisory Ltd. India



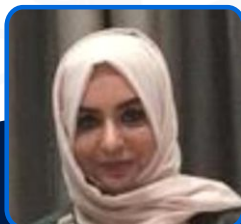
DINESH O BAREJA
Open Security Alliance
India Watch, India



BARRY A. J. FISHER (Retd.)
Los Angeles County Sheriff's
Crime Laboratory Director, USA



Dr. GHYASUDDIN KHAN
U.P. State Medico Legal Cell &
Forensic Medicine Expert, India



Dr. SAMEERA AL HAMMADI
Head of Forensic Medicine &
Pathology Section, Judicial Dept., UAE



Dr. ASHA SRIVASTAVA
CFSL, CBI, Delhi
India



Dr. S. L. VAYA
Rashtriya Raksha University
Gujarat, India

Advisory Board



NA VIJAYASHANKAR
Foundation of Data Protection
Professionals (FDPPI), India



Dr. WILLIAM R. BELCHER
University of Nebraska
Lincoln, USA



OMVEER SINGH
Ministry of Electronics &
Information Technology, N-Delhi



Dr. EVI UNTORO
Forensic Pathologist
Indonesia



CLOYD STEIGER
Author,
Criminal Justice



AI-SHARIF HASHEM MOGAHED
A Corresponding Member of the ASQDE & ASFDE,
Forensic Document Examiner
Forensic Medicine Authority, Ministry of Justice
Egypt



Dr. KAVITA SHARMA
Shri Vaishnav Vidyapeeth
Vishwavidyalaya, Indore



HEMANTA KUMAR PANDA
Retd. Fingerprint Expert,
Bhubaneswar, Odisha



Dr. AJAY SHARMA
State Forensic Science Laboratory,
Rajasthan



Prof. TRIVENI SINGH (IPS)
S. P., Cyber Crime
U. P. Police



Dr. GAGANDEEP SINGH
CRC Press, Taylor & Francis Group
Patiala



**Dr. MOHAMMED
NASIMUL ISLAM**
Forensic Pathologist, Malaysia



KEVIN M. SULLIVAN
Author, USA



RAJ SHRIVASTAVA
Forensic Science Laboratory
Sagar



Dr. SHALINI GUPTA
King George's Medical University
Lucknow



SHANE TURNIDGE
Fingerprint Expert,
Canada



ARUN SHARMA
Forensic Science Laboratory
Lucknow



Dr. AMAR JYOTI PATOWARY
Guwahati Medical College
Guwahati



Dr. RAAKESH KRIPLANI
Indian Cyber Psychology Association
Nagpur, India



Dr. CHANDNI SRINIVASAN
Psychotherapist & Counsellor
Chennai, India

Advisory Board



Dr. SONI KEWALRAMANI
Amity University
Lucknow



SAMIR DATT
Forensicguru.com
India



PRINCE BOONLIA
Digital 4n6 Journal
New Delhi, India



Dr. SANJAY GUPTA
Dept. of Forensic Medicine & Toxicology
Pramukhswami Medical College, Gujarat



Dr. SHUBHRA SANYAL
NGO,
New Delhi,



Dr. BHARTI MEHTA
Psychology Gym & CosmeClinic
Pune, India



AASHISH SUTAR
Digital Forensic Analyst and Instructor
Ministry of Defence, Govt. of India



Dr. A. NAGARATHNA
National Law School of India
University, Bengaluru



MOHAMMED ABO ELAZM
Alexandria Head of Forensic
Evidence, Egypt

Organising Committee

Convenor in Chief



Dr. RANJEET Kr. SINGH

President
International Association of
Scientists & Researchers

Convenor in Chief



PHANEENDAR B. N.

Chairman
Clue4 Evidence Foundation



Convenor

Mahesh Sharma

SIFS India



Convenor

Sheza Azeen

SIFS India



Convenor

Afreen Tarannum

SIFS India



Convenor

Vaishnavi Thakre

SIFS India



Convenor

Kratika Mishra

SIFS India



Convenor

Arti Varshney

SIFS India



Convenor

Saumya Solanki

SIFS India



Convenor

Preeti Kiran

SIFS India



Treasurer

Thomas T.O.

SIFS India



Organising Secretary

Madhuri Vagal



Organising Secretary

Dr. Pooja Chakraborty



Organising Secretary

Prerna Patel



Organising Secretary

Ruchika Dwivedi



Organising Secretary

Taniya Jaiswal



Organising Secretary

Priya Singh



Organising Secretary

Sudhakar Yadav



Organising Secretary

Falak Khan



Organising Secretary

Pallavi Mohanty



Organising Secretary

Aditi



Organising Secretary

Sheetal

Core Committee



Dr. ANKIT SRIVASTAVA
Dr. A.P.J. Abdul Kalam Institute of
Forensic Science & Criminology,
Bundelkhand University, Jhansi



Dr. RITESH SHUKLA
Ahmedabad University,
Gujarat



Dr. SUMIT CHOUDHARY
Rashtriya Raksha University,
Gujarat



Dr. HEMLATA PANDEY
Seth GS Medical College and KEM
Hospital, Mumbai, India



Dr. ASHISH BADIYE
Government Institute of Forensic
Science, Nagpur



Dr. RICHA ROHATGI
Amity University
Gurugram



NITIN PANDEY
Consultant Cyber,
Police Headquarters, Lucknow



Dr. KANCHANA KOHOMBANGE
International Hand Analyzing
Consultancy, Sri Lanka



Dr. NEETI KAPOOR
Government Institute of
Forensic Science, Nagpur



RAMANDEEP SINGH
Evolve Security, USA



MA TERESA G. de GUZMAN
University of the Philippines,
Manila



HANSI BANSAL
Government Institute of Forensic
Science, Nagpur

Scientific Committee



**Prof. MUKESH
Kr. THAKAR**
Dept. of Forensic Science,
Punjabi University
Patiala



ARVIND SUD
Senior Forensic Expert
Hoshiarpur



**Dr. RAJINDER SINGH
CHANDEL**
Dept. of Forensic Science,
Punjabi University
Patiala



**Dr. RACHEL
BOLTON-KING**
School of Law,
Policing & Forensics,
Staffordshire University, UK



**Prof. GYANESHWER
CHAUBEY**
Dept. of Zoology,
Banaras Hindu University,
Varanasi



TIFFANY ANN ROY
ForensicAid LLC,
United States



**Prof. (Dr.) GURMANJIT
RAI MAAN**
Forensic Medicine &
Toxicology, MMIMS Mullana,
Ambala



**Prof. (Dr.) BHARATH
Kr. GUNTHETI**
Dept. of Forensic
Medicine & Toxicology, Mamata
Medical College, Telangana



**BULENT
AYDOGMUS**
Sahtecilikgrafoloji
Uzmani, Turkey



Dr. S. K. PAL
State Forensic Science
Lab., DFS, Junga



**Dr. DENISE
GEMMELLARO**
Dept. of Biology,
Kean University, US



**Dr. AKHILESH
PATHAK**
Dept. of Forensic
Medicine & Toxicology,
AIIMS, Bathinda



Dr. KHALID KHALID
Dept. of Dentistry,
Nile University, Sudan



Prof. KOMAL SAINI
Dept. of Forensic Science,
Punjabi University
Patiala



Dr. PIYUSH KAPILA
Dept. of Forensic Medicine
IGM College & Hospital,
Shimla



**Prof. T. NATARAJA
MOORTHY**
Faculty of Health & Life
Sciences, Management &
Science University, Malaysia



**Dr. JAYASANKAR
P. PILLAI**
Dept. of Oral Pathology
Govt. Dental College
& Hospital, Ahmedabad



**E. SAI PRASAD
CHUNDURU**
Digital Forensic Division,
CFSL, DFS, Hyderabad



Dr. RAKHI KHANNA
State Forensic Science
Laboratory, Jaipur



**ANDREW
REITNAUER**
Delta Forensics, LLC,
United States



**Dr. VINDRESH
MISHRA**
Dept. of Toxicology,
CFSL, Kolkata



**Dr. CARLOS A.
GUTIERREZ**
True Forensic Science,
United States



**ANNA
BARBARO PhD**
Worldwide Association of
Women Forensic Experts,
Italy



**Dr. MUKESH
SHARMA**
Physics Division,
State Forensic Science
Laboratory, Jaipur



Dr. VIJAY ARORA
Dept. of Forensic Medicine,
Dr. R. P. Govt. Medical
College, Kangra



Dr. AMIT PATIL
Dept. of Forensic Medicine
& Toxicology, AIIMS,
Patna



Dr. INDERJIT SINGH
Senior Forensic Expert,
Patiala



VIJAY RUSTAGI
Senior Forensic Expert,
Gurugram

Scientific Committee



Dr. PRAVEEN JHA
State Forensic Science
Laboratory, Sagar



**Dr. ADEMIR
FRANCO**
School of Dentistry,
University of Dundee, UK



VIJAY VERMA
Central Forensic Science
Laboratory, CBI,
New Delhi



**Dr. KRISHNADUTT
H. CHAVALI**
Dept. of Forensic Medicine
& Toxicology, AIIMS,
Raipur



Dr. YADUKUL S.
Dept. of Forensic Medicine
& Toxicology, AIIMS,
Bibinagar



**Dr. PRATEEK
RASTOGI**
Kasturba Medical College,
Mangalore



**Dr. POOJA
RASTOGI**
Sharda University,
Greater Noida



Dr. NEERAJ TANEJA
Mobico Comodo Pvt Ltd.
Gurugram



Dr. ALOK PANDYA
Institute of Advanced
Research, Gandhinagar



Dr. JIJU PV
Central Forensic Science
Laboratory, DFSS, Pune



AMIR LIBERMAN
Nemesisco Limited,
Israel



**Dr. ADITYA
SHARMA**
IGM College & Hospital,
Shimla



Dr. NARESH KUMAR
Forensic Science
Laboratory, Delhi



**Dr. AMAR PAL
SINGH SHOKEEN**
Forensic Science
Laboratory, Delhi



**Dr. KAVERI
CHAUHAN**
MindSpark PsycCare,
Training and Development
Karnal



**Dr. PRATEEK
PANDYA**
Amity University
Noida, U. P.



**Dr. RAJESH
SINGH YADAV**
Dr. Harisingh Gour
Central University,
Sagar



**NEERAJ KUMAR
VARSHNEY**
Forensic Science
Laboratory, Patna



Dr. PREETI SINGH
National Post Graduate
Autonomous College
Lucknow



**Dr. PRIYANKA
KACKER**
National Forensic Science
University, Gujarat



Dr. PUNEET SETIA
AIIMS,
Jodhpur, Rajasthan



**Dr. DOMINGO
MAGLIOCCA**
Certified Geographic
Profiling Analyst, Italy



Dr. POOJA PURI
Amity University
Noida



**Dr. VIVEK
SAHAJPAL**
State Forensic Science
Laboratory, Shimla



ABY JOSEPH
Amity University,
Dubai



DR. KRITI NIGAM
Dr. A.P.J. Abdul Kalam Institute
of Forensic Science & Criminology,
Bundelkhand University,
Jhansi



**Dr. PARDEEP
SINGH**
Pt. J. L. Nehru Medical
College, Chamba, H. P.



V.B. KASHYAP
Fingerprint Expert,
Haryana

Scientific Committee



RAJVEER
State Forensic Science
Laboratory, Jaipur



Dr. ILA GAUTAM
Forensic Science
Laboratory, Sagar



**MOHAMMED
AL SUWAIDI**
Fingerprint Expert
Dubai Police, UAE



**Dr. BINAYA
KUMAR BASTIA**
AIIMS,
Rishikesh



**Dr. SHALOO
MALIK**
Regional Forensic
Science Lab., Jodhpur



**HANAN AHMAD
ALMULLA**
Forensic DNA Expert,
Police HQ, Dubai



Dr. ANU SINGLA
Dr. A.P.J. Abdul Kalam Institute
of Forensic Science & Criminology,
Bundelkhand University,
Jhansi



Dr. NIRAJ RAI
Ancient DNA Lab
Birbal Sahni Institute of
Palaeosciences, Lucknow



**DURGA PRASAD
GANGWAR**
Central Forensic Science
Laboratory, Chandigarh



**Dr. JONATHAN
ANDREW BROOKS**
King's College,
London, UK



Dr. UTSAV PAREKH
P S Medical College
Gujarat



**Dr. AMAN
CHOWDHRY**
Jamia Millia Islamia
New Delhi



Dr. PRADEEP JAIN
Regional Forensic
Science Lab. Bikaner



**Dr. PRASHANT
AGRAWAL**
College of Traffic
Management, IRTE,
Faridabad (MDU Affiliated)



R. SURESH
National Forensic Science
University, Gujarat



**Dr. VIKAS
MESHRAM**
Dept. of Forensic Medicine
& Toxicology, AIIMS,
Jodhpur



**Dr. MANOJ
PARSHAKE**
Dept. of Forensic Medicine,
Seth GS Medical College,
KEM Hospital, Mumbai



**Dr. VIJAY R.
CHOUREY**
Dept. of Forensic Science,
Govt. Holkar (Model Autonomous)
Science College, Indore



**Dr. INDRAJIT
KHANDEKAR**
Dept. Forensic Medicine
& Toxicology, MGIMS,
Sewagram



MANISH Kr. SAINI
Physics Division,
State Forensic Science Lab.,
MP



**KALPESH
SOLANKI**
SFSRM, Rashtriya Raksha
University, Gujarat



**Dr. MANOJ
KUMAR MOHANTY**
Dept. of Forensic
Medicine & Toxicology,
AIIMS, Bhubaneswar



**Dr. HIRAK
RANJAN DASH**
Forensic Science
Laboratory, Bhopal



**Dr. VISHAL
SHARMA**
Inst. of Forensic Science
& Criminology, Panjab
University, Chandigarh



**Dr. NADEEM
MUBARIK**
DNA Fingerprinting Unit,
State Forensic Science Lab.,
Srinagar



**Dr. PRAGNESH
PARMAR**
Dept. of Forensic Medicine
& Toxicology, AIIMS,
Bibinagar



**Dr. TREVILLE
PERIERA**
DY Patil University
School of Dentistry,
Navi Mumbai



R. APARNA
Jain
(Deemed-to-be University),
Bengaluru

Scientific Committee



PALLAVI MALIK CHOPRA
Forensic Science
Laboratory, Mohali



Dr. CRISTIANA PALMELA PERRIERA
University of Lisbon,
Portugal



Dr. NEELAM ARYA
Forensic Science
Laboratory, Haryana



ELENA FELDMAN
F_Lab, Chelyabinsk
State University,
Russia



Dr. ANUREKHA YADAV
Forensic Science
Laboratory, MP



Dr. NRASHANT SINGH
Amity University
Dubai



Dr. JEYASEELAN AUGUSTINE
Dept. of Oral Pathology,
Maulana Azad Institute of
Dental Sciences, New Delhi



Dr. MOHINESH CHANDRA
Forensic Science
Laboratory, New Delhi



Dr. ROHITASHVA MANI TRIPATHI
Central Forensic Science
Laboratory, Chandigarh



Dr. SUDHIR YADAV
Dept. of Forensic Science,
Guru Ghasidas University,
Bilaspur



Dr. SWATI SHRIVASTAVA
State Forensic Science
Laboratory, MP



Dr. DEEPIKA BABLANI POPLI
Faculty of Dentistry,
Jamia Millia Islamia,
New Delhi



Dr. MANOJ KUMAR VERMA
Chemistry Division,
Forensic Science Lab.,
U.P.



Dr. WASSIM MOHAMED RIHAWI
Syrian Forensic
Odontology Association,
Syria



Dr. MONICA MEHENDIRATTA
ITS Dental College,
Hospital & Research Centre,
Greater Noida



Dr. GAURAV MAHESHWARI
Quality Research &
Analytical Labs Pvt. Ltd,
New Delhi



VIJAY KUMAR YADAV
Dr. A.P.J. Abdul Kalam Institute
of Forensic Science & Criminology,
B.U., Jhansi



Dr. SUDHEER B. BALLA
Panineeya Institute of
Dental Science & Hospital,
Telangana



Dr. ROHIT SRIVASTAVA
College of Life Science,
CHRI Campus, Gwalior



Dr. GULSHAN SHRIVASTAVA
Dept. of Computer Science
& Eng., Sharda University,
Greater Noida



Dr. RAJEEV JAIN
Central Forensic Science
Laboratory, DFSS,
Chandigarh



Dr. HIMANSHU KHAJURIA
Amity Institute of Forensic
Sciences, Amity University
Noida



ABHISHEK VASHISTH
Forensic & Handwriting
Expert, Dehradun



MEBIN WILSON THOMAS
Jain (Deemed-to-be)
University, Bengaluru



Dr. RAJESH KUMAR
Dept. of Forensic Science,
Govt. Institute of Forensic
Science, Aurangabad



Dr. M. K. SUNIL
Dept. of Oral Medicine
& Radiology, TMU,
Moradabad



Dr. MANAVPREET KAUR
Wikimedia Foundation,
USA



Dr. LALIT PRATAP CHANDRAVANSHI
CTM, IRTE,
Faridabad

Scientific Committee



**Dr. MADHUSUDAN
ASTEKAR**
Institute of Dental
Sciences, Bareilly



**Dr. MALVIKA
MEHTA**
National Centre
for Handwriting Studies
Pune



**Dr. GUNVANTI
B. RATHOD**
Dept. of Forensic
Medicine & Toxicology,
AIIMS, Bibinagar



**Dr. KAMLESH
KAITHOLIA**
Forensic Science
Laboratory, MP



**Dr. JAGADISH
P. RAJGURU**
Hi-Tech Dental College &
Hospital, Utkal University,
Bhubaneswar



Dr. KAPIL KUMAR
Dept. of Biochemistry
& Forensic Science
Gujarat University,
Ahmedabad



**Dr. ASHUTOSH
TRIPATHI**
Institute of Sciences,
Sage University, Indore



Dr. NEETA SHARMA
Dept. of Oral Medicine
& Radiology, H.P. Govt.
Dental College & Hospital,
Shimla



RITESH BHATIA
V4WEB Cybersecurity,
Mumbai



Dr. HARSH JOSHI
Information Security
Group, HDFC Bank,
Mumbai



Dr. RAJIV PANDEY
AIIT, Amity University,
Lucknow



**Dr. MAHESH A.
TRIPATHI**
SFSRM, Rashtriya Raksha
University, Gujarat



Dr. ASHA PAHWA
Forensic Science
Laboratory, New Delhi



**Dr. ASTITVA
ANAND**
Forensic Science
Laboratory, Gujarat



**Dr. PANKAJ
KUMAR PANDEY**
State Forensic Science
Laboratory, Sagar



**Dr. RAKHI R.
WADHWANI**
Senior Assessor
Mumbai



**Dr. NEEHARIKA
SRIVASTAVA**
G.D. Goenka University,
Gurgaon



**Dr. KRITHIKA
RAJESH**
Forensic Science
Laboratory, Ahmedabad



**Dr. YMELDA WENDY
VELEZMORA MONTES**
SPOLFOC, Peru



**Dr. POONAM
SINGH**
Regional Forensic Science
Laboratory, Bhopal



**Dr. SWATI
DUBEY MISHRA**
SVIFS,
Shri Vaishnav Vidyapeeth
Vishwavidyalaya, Indore



**Dr. PARUL
KHARE SINHA**
Alpha Dental Clinic,
Shanghai



**Dr. FRENY
KARJODKAR**
Dept. of Oral Medicine &
Radiology, Nair Hospital
Dental College, Maharashtra



**Dr. HIMAKSHI
BHARDWAJ**
Forensic Science
Laboratory, New Delhi



AMRIT CHHETRI
IT Security, DFIR &
Web Researcher,
West Bengal



**Dr. RAJNISH
KUMAR SINGH**
Forensic Science
Laboratory, New Delhi



NARENDRA KUMAR
Forensic Science
Laboratory, U.P.



Dr. ARUNA MISHRA
Forensic Science
Laboratory, New Delhi

Scientific Committee



Dr. ALI RAZA
Arba Minch University,
Ethiopia



ZADIA-KAY SMITH
Jamaica Constabulary
Force, Jamaica



HEENA GOSWAMI
Gujarat National Law
University, Gandhinagar



**Dr. ABIRAMI
ARTHANARI**
Dept. of Oral Pathology,
Saveetha Dental College
& Hospital, Tamil Nadu



**Dr. KARPAGAVALLI
SHANMUGASUNDARAM**
Dept. Oral Medicine &
Radiology, Seema Dental
College & Hospital, Rishikesh



**Dr. UTTARA
DESHPANDE**
DentoUpanishad Dental
Clinic & Implant Center,
Pune



Dr. KUSUM SINGAL
Dept. of Neurology,
AIIMS, New Delhi



**Dr. ARUSHI
CHAWLA**
Dept. of Applied Sciences,
Parul University, Gujarat



**Dr. RANJEETA
KUMARI**
Central Forensic Science
Laboratory, CBI, New Delhi



**Dr. RISHA
JASMINE NATHAN**
Dept. Forensic Science,
Galgotias University,
Greater Noida



KAPIL DEV
Forensic Science
Laboratory, Moradabad



MAJID KHAN
Forensic Science
Laboratory, Muzaffarpur



Dr. RAJEEV KUMAR
Dept. of Forensic Science,
Galgotias University,
Greater Noida.



**MAYANK KR.
DUBEY**
Mody University,
Rajasthan



**Dr. SUDEENDRA
PRABHU**
Yenepoya Dental
College, Mangalore



**Dr. SOWJANYA
VASISTA**
Abyasa Educare Pvt. Ltd.,
Bangaluru



**PRASHANT
SHARMA**
Central Forensic Science
Laboratory, CBI,
New Delhi



**Dr. PRIYANKA
KAPOOR**
Faculty of Dentistry,
Jamia Millia Islamia,
New Delhi



**Dr. SHIVANI
BANSAL**
Nair Hospital Dental
College, Maharashtra



**SHYAM
CHANDEL**
Cyber Fraud Helpline,
Udaipur



VICHAR MISHRA
Jain (Deemed-to-be)
University, Bengaluru



**Dr. JASKARAN
SINGH**
Allied Health Sciences,
Sharda University,
Gr. Noida



**Dr. PRIYANKA
SINGH**
Amity Institute of
Forensic Sciences,
Amity University, Noida



VINNY SHARMA
Dept. of Forensic Science,
Galgotias University,
Greater Noida.



ABHIJEET SARKAR
Dept. of Forensic Science,
Govt. Institute of Forensic
Science, Aurangabad



Dr. AMBREEN KAUR
Luxmi Bai Institute of
Dental Sciences & Hospital,
Patiala



VEDIKA AGARWAL
Mental Health
Foundation, India



DIVYA DUBEY
Spire Solutions,
Dubai

Scientific Committee



PRACHI KATHANE
SFSRM,
Rashtriya Raksha
University, Gujarat



MELBA KURIAKOSE
Impress.ai,
Kochi



**Dr. DEEPIKA
BHANDARI**
State Forensic Science
Laboratory, DFS, Junga



REENA SHARMA
The Mind Practice,
Ahmedabad



NILESH B. WAGH
Central Forensic Science
Laboratory, CBI,
New Delhi



KRUPA NISHAR
Institute of Behavioural
Science, National Forensic
Sciences University, Gujarat



**SUBHASISH
SAHOO**
Forensic Science
Laboratory, Bhubaneswar



**Dr. HUNNY
MATIYANI**
LNJN National Institute
of Criminology & Forensic
Science, New Delhi



Dr. SWIKAR LAMA
Sardar Patel University of
Police, Security & Criminal
Justice, Jodhpur



**SUCHISMEETA
BEHERA**
Forensic Science
Laboratory, Odisha



**Dr. RUCHI
SHARMA**
Forensic Science
Laboratory, Rohini, Delhi



ANU SEBASTIAN
Div. Forensic Science
Laboratory, Bangalore



DEEPAK KUMAR
Digital Forensics & Cyber
Intelligence, Govt. of India



**NOUZIA
NOORDEEN**
SAFI Institute of Advanced
Study, SAFI College,
Kerala



**Dr. DAS
AMBIKA BHARTI**
Dept. of Psychological
Sciences, Central University
of South Bihar, Bihar



NIDHI PANDYA
Gujarat University
Ahmedabad



GEORGE DIXON
Jamaica Constabulary
Force, Jamaica



MOHIT YADAV
Craw Cyber Security
Pvt. Ltd., New Delhi



**SHIFA
CYCLEWALA**
Hacktify Community
Virtually Testing
Foundation, USA



ROHIT GAUTAM
Hacktify Community
Virtually Testing
Foundation, USA



**SHUBHAM
GAUTAM**
Psyberbull & 3dayhack
Delhi



**SUDHANSHU
SHEKHER TIWARI**
SFSRM, Rashtriya Raksha
University, Gujarat



RITU BHARTI
Govt. Holkar
(Model Autonomous) Science
College, Indore



**MANASHREE
AVINASH MANE**
Jain (Deemed-to-be)
University, Bengaluru



PAWAN DESAI
MitKat Advisory Services
Pvt. Ltd, Gurugram



SRI RAM
PrimeFort Pvt. Ltd.,
Puducherry



NAVEEN PAL
IT GRC
Compliance Audit



GOPIKA BAGHEL
Forensic Science
Education Society,
Raipur

Scientific Committee



DEEP SHANKAR YADAV
eSec Forte Technologies,
Gurugram



SANTOSH CHALUVADI
Supraja Technologies,
Andhra Pradesh



Dr. JYOTI SINGH
Amity Institute of Forensic
Sciences, Amity University,
Noida



RASHMI DILIP KADU
Jain (Deemed-to-be)
University, Bengaluru



DAVINDER SINGH
Cylos Consulting Private
Limited, New Delhi



GAURAV SHRAMA
Cyber Security
Professional, Gurugram



Dr. SHWETA SHARMA
SFSRM, Rashtriya Raksha
University, Gujarat



VINAY SINGH
Forensic Science
Laboratory, New Delhi



Dr. MAMTA PAL
Jain (Deemed-to-be)
University, Bengaluru
(Former)



SAURABH ATHAWALE
Kcyber Experts Pvt. Ltd.,
Nagpur



Dr. SWATHI KUMARESWAR
Dept. of Forensic
Odontology, JSS Dental
College & Hospital, Mysuru



JIN LEE
Independent
Lawyer, Delhi



ROHIT JAIN
Advocate
High Court, Indore



MADHURI VAGAL
SIFS INDIA
Mumbai

Call for Paper

GUIDELINES FOR STUDENT & PROFESSIONAL CATEGORY

Submission of Paper

- ◆ The paper should be **ORIGINAL** and **UNPUBLISHED** offering new insights, a new approach, or new knowledge to the body of literature.
- ◆ The abstract should be of a **maximum of 350 words** followed by a **minimum of 5 keywords** in the format given.
- ◆ All participants should email their respective abstracts before the mentioned deadline, **15th June 2021** at **iasrforensicconference@gmail.com**.

Criteria for Evaluation

- ◆ The evaluation depends upon the presentation skills, content, topic relevancy, and answers given to the jury.
- ◆ All abstracts submitted would be published in the **SOUVENIR of IASR**.
- ◆ The outstanding papers would be published in the **Academic Journal of Forensic Science, IASR** providing **FREE SCHOLARSHIP**.

Presentation of Paper

- ◆ The paper has to be presented in PowerPoint 2013/2010 or earlier in 16:9 ratio slides.
- ◆ A maximum of **10 slides** is allowed to present. The time limit for the presentation will be **8 minutes** followed by a **2-minutes** discussion with video 'ON'.
- ◆ The presentation should include an introduction, material, and methodology, information regarding collected data, major findings, conclusion, etc.
- ◆ In the case of multiple authors, only one author out of the two would be allowed to present the ePoster. All Co-authors would receive the participation eCertificate as co-authors.

Format of Paper: The manuscript should follow the format:

- ◆ Title of the paper, Name, Position with Institute name, Contact no. and Email Address.
- ◆ Approximately **300 words of abstract** followed by a **minimum of 5 keywords** along with the final paper.
- ◆ The paper should follow the font Times New Roman size 12 (Justify alignment) and heading size 14 (aligned centrally) in MS-Word Format.
- ◆ All references should follow the MLA (8th edition) style. All tables and figures should be appropriately numbered.

Guidelines for Paper and ePoster Submission

<https://youtu.be/mEqdhPXAmB8>

Call for ePoster

GUIDELINES FOR STUDENT & PROFESSIONAL CATEGORY

Submission of ePoster

- ◆ The ePoster should include completed or ongoing scientific research, proposing innovative ideas, interesting case study, etc.
- ◆ The abstract should be a **maximum of 350 words** followed by a **minimum of 5 keywords** in the format given.
- ◆ All participants should email their respective abstracts (approximate 350 words) and ePoster at **iasrforensicconference@gmail.com** before the mentioned deadline, **15th June 2021**.

Criteria for Evaluation

- ◆ The evaluation depends upon the presentation skills, content, topic relevancy, and answers given to the jury.
- ◆ All abstracts submitted would be published in the **SOUVENIR of IASR**.

Presentation of ePoster

- ◆ The ePoster has to be presented in the PowerPoint 2013/2010 or earlier in 16:9 ratio slides.
- ◆ The ePoster has to be made on a single (**ONE**) slide having information such as introduction, method and methodology, results, and conclusion.
- ◆ The time limit allotted for the presentation will be **5 minutes** followed by a **2-minutes discussion** with video '**ON**'.
- ◆ In the case of multiple authors, only one author out of the two would be allowed to present the ePoster. All Co-authors would receive the participation eCertificate as co-authors.
- ◆ Only the main Presenter would receive the Winning eCertificate of Achievement.
- ◆ The best ePoster in the two different categories (Student and Professional) will be duly acknowledged.

Guidelines for Paper and ePoster Submission

<https://youtu.be/mEqdhPXAmB8>

Awards

Awards for Best Scientific Paper & ePoster

The winners in both **STUDENT** and **PROFESSIONAL** category will receive:

Three outstanding Paper & ePoster would receive an **eCertificate of Excellence** with **Cash Prize** in each Category



STUDENT



PROFESSIONAL

**CASH PRIZE
OF Rs.2000/-**



**CASH PRIZE
OF Rs.1500/-**



**CASH PRIZE
OF Rs.1000/-**

The Best Paper will be published in Journal of IASR

Registration Details

NATIONAL & INTERNATIONAL PARTICIPANTS
FOR STUDENT AND PROFESSIONAL

Student

(Streamed on Zoom & YouTube
with Participation eCertificate)

₹100

Professional

(Streamed on Zoom & YouTube
with Participation eCertificate)

₹250

ePoster/Paper Presentation

(Streamed on Zoom & YouTube)

₹500









LAST DATE OF SUBMITTING ePOSTER/PAPER ABSTRACT

15th June 2021

Register On: www.forensicevents.com

*ePoster and Paper Participants will receive **Conference Participation** and **Competition Participation eCertificate** and Winners would also receive **Prize** along with **Certificate of Excellence**.*

Social media handle:

- | | | | |
|--|--|---|--|
|  | www.youtube.com/Forensic365 |  | Email : iasrforensicconference@gmail.com |
|  | www.facebook.com/iasrorg |  | Contact : +91-98188-77002 |
|  | www.linkedin.com/in/iasrorg/ |  | Website : www.forensicevents.com |
|  | www.instagram.com/Forensicscienceinstitut |  | linktr.ee/forensicscienceinstitut |

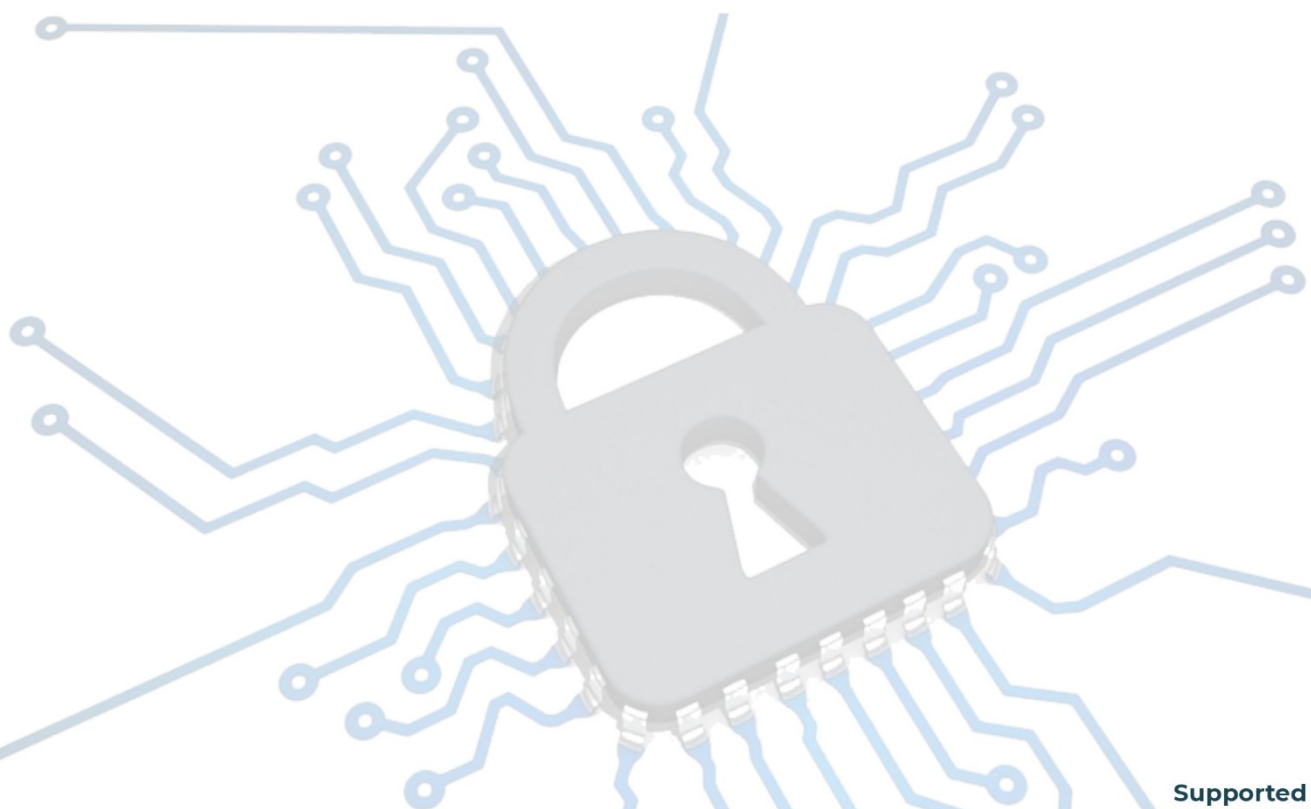
linktr.ee/forensicscienceinstitut, Contact us: +91 98188 77002

TABLE OF CONTENT

Paper Category

Paper Code	Authors and Co-authors	Title
PA 1	Navdha Bhardwaj Dr. Rajesh Verma Dr. Arnav Bhavsar	Application And Validation Of Likelihood Ratio Approach In Forensic Facial Recognition Using Morphometric Indices
PA 2	Vikas Razdan	Computer Forensics: Data Acquisition & Duplication
PA 3	Ashesh Sen B V Patel Kapil Kumar	Database Examination & Digital Forensics
PA 4	V. P. Selvapoornima	Unearthing Cyber Bullying Among College Students In Chennai City
PA 5	N. Ashwini Dr. Syed Umarhathab	A Study Of Digital Forensic Tools , Hacktivism Phenom And Challenges
PA 6	Riya Singh Shally Chauhan	Cyber Venting- A Healthy Tool For Mental Health
PA 7	Meenu Hariharan Dr. Rajesh Verma	Validation Of Automatic Voice Comparison Using Likelihood Ratios And Comparison With Traditional Approaches
PA 8	Gladwel Kubwalo Dr. Tejasvi Bhatia	Forensic Investigation of the Basic Digital Evidences in Mobile Devices
PA 9	Jagriti Khanna Anjali Jangra Yogita Saini Pankaj Kumar Naveen Saini	Online Crimes against Women and Children in Cyber Space- A Survey Based Research Report

PA 10	Shivani Rai	Cyber & Digital Forensics
PA 11	Preeti Ansari Ritika Sharma	Retrieved Data Comparison of WhatsApp and Signal Application



Eposter Category

Eposter Code	Author And Co-Authors	Title
EP 01	Preeti Kiran	Cyber Parenting: Need To Create Boundaries Around
EP 02	Ayushi Verma	Rise In Cyber Crime During Pandemic
EP 03	Arti Varshney	CyberPsychology
EP 04	Jessy Ayala	Using A Layered Approach For Graphical-Based Passwords
EP 05	Aastha Mahna	Law Merger: IT Act And IPC Laws Together In Sexual Harrassment Cases
EP 06	Vikas Razdan	Chip-Off Technique In Mobile Forensics
EP 07	Neelkamal Ganesh Battu	Cyber Terrorism: A Threat To National Security
EP 08	Aniruddhvaibhav Gupta	Cyber Relationships: Boon Or Bane

Paper Abstracts

APPLICATION AND VALIDATION OF LIKELIHOOD RATIO APPROACH IN FORENSIC FACIAL RECOGNITION USING MORPHOMETRIC INDICES

Navdha Bhardwaj¹, Dr. Rajesh Verma², Dr. Arnav Bhavsar³

¹Project Engineer, School of Computing & Electrical Engineering, Indian Institute of Technology, Mandi

²Deputy Director, RFSL Mandi, Himachal Pradesh

³Associate Professor, School of Computing & Electrical Engineering, Indian Institute of Technology, Mandi

Email address: navdhabhardwaj001@gmail.com

Abstract

We propose a novel approach aimed at facial comparison in the forensic context. We employed an automatic approach to detect facial landmarks and then selected independent facial indices extracted from a subset of these landmarks. It is difficult to compare the morphometric indices due to pose variations, so some statistically reliable method is required for face comparison. The present work demonstrates using the likelihood ratio (LR) approach to assess the grouping of facial images based on the morphometric indices, in a database of 40 persons, with 10 facial images each, in different poses, expressions, illumination, and background. We have calculated the performance metrics to assess the validation and reliability of the likelihood ratio (LR) approach. For the evaluation and validation of data, log-likelihood ratio cost (*c_{llr}*) is one of the metrics that gives better accuracy. Reliability is best expressed in terms of the true positive and false-positive rates, provided these are calculated by comparing the ground truth with the evaluation of LR (whether $LR < 1$ or > 1). As compared to more abstract face identification methods, the proposed approach is relevant in a forensic context, as it is based on interpretable morphometric features of faces. Furthermore, automated landmark identification significantly improves the efficiency as compared to manual landmark labelling. A likelihood ratio approach is a statistical approach, is reliable as it leverages the variations due to pose variations in the face images, offers good quality segregation of faces, and hence is a promising technique for forensic facial identification.

Keywords: likelihood ratio, facial identification, facial index, true positive, false negative.

COMPUTER FORENSICS: DATA ACQUISITION & DUPLICATION

Vikas Razdan¹

Abstract

Data acquisition is the first pro-active step in the computer forensic investigation process. The aim of the forensic data acquisition is to extract every bit of information present on the victim's hard disk and create forensic copy to use it as evidence in the court of law. Data acquisition in computer forensics encompasses all the procedures involved in gathering digital evidence including cloning and copying evidence from any electronic source. It involves producing a forensic image from digital devices including hard drive, removable hard drives, smartphones, and thumb drive. There are different types of data acquisition methods including logical disk-to-disk file, disk-to-disk copy, sparse data copy of a file or folder, and disk-to-image file. There are also different approaches used for data acquisition. The storage device is first connected to a "write blocking" device, which prevents any binary code from being altered or modified during the process. Then a mirror image or "clone" of the drive is created on a separate storage device to be examined later. After the initial acquisition, the original device is placed in a secure storage, and the forensic examiner conducts all forensic investigation only on the copy. The purpose of working on a copy of the evidence is to leave the original media intact, which allows to verify the evidence at a later date. Acquired media is often referred to as an "image" and is generally stored in one of several open or proprietary formats, the most common being EnCase, which employs a proprietary, compressible, EnCase Evidence File Format (EEDFF). During the acquisition process, such software creates a unique numerical code, called a verification "hash" of the media, which allows an analyst to later confirm that the image and its contents are accurate and unaltered. The EnCase Evidence File Format stores a hash for every 64K of data along with an appended MD5 hash of the entire media. Various hardware and softwares are used for carrying out the data acquisition.

Keywords: Computer Forensics, Data Acquisition, Live & Static Acquisition, Volatile Data, Imaging, Hash Values

DATABASE EXAMINATION & DIGITAL FORENSICS

Ashesh Sen¹, B V Patel², Kapil Kumar³

¹Dept. of Forensic Science, Gujarat University, Ahmedabad

²Dept. of Microbiology, Gujarat University, Ahmedabad

³Dept. of Forensic Science, Gujarat University, Ahmedabad

Email: asheshsen28@gmail.com; patelbaldev56@yahoo.in; kkforensic@gmail.com

Abstract

This research study sheds light on cyber security programs and digital forensic processes. Cyber security programs are different from digital forensic processes. Therefore, the number of cybercrimes is increasing nowadays and so cyber security programs are essential as it helps to protect systems from cyber-attack. The purpose of this particular research study is to analyse the importance of cyber security programs in software and android nowadays. Apart from that, the description of the significance of digital forensics in protecting data and fetching lost data back is another important purpose of this study. Therefore, the differences between cyber security and digital forensic as well as the relationship between cyber security and digital forensic is analysed in this research study properly. Cyber security helps to secure the data and digital forensic helps to fetch that data when cyber-crime of Forensic programs is essential and helpful for the protection of the data or information that people share through the internet on any digital platform. Database examination is crucial to gather some accurate breakthrough in a cybercrime giving a ground to the digital forensics wing to resolve a case. To conclude, it can be said that a strong cyber security is important to control changing cybercrime pattern. And so, digital forensics is equally essential as the team helps to fetch the lost data by investigation. Therefore, the relationship between database examination, cyber security and digital forensic is close knit in order to reduce digital criminal activities.

Keyword: Cyber security, Digital forensics, Cyber-crime, Cyber-attack, Investigation

UNEARTHING CYBER BULLYING AMONG COLLEGE STUDENTS IN CHENNAI CITY

V. P. Selvapoornima¹

¹Assistant Professor (T), Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Tirunelveli

Email id: purnima.eswar@gmail.com

Abstract

Crime follows opportunity; virtually every advance has been accompanied by a corresponding niche to be exploited for criminal purposes. Advancement in technology helps to develop and expand the modern communication network. It helps in faster communication and information exchange. With the increased usage of social media applications like Facebook, Whatsapp, Twitter, Instagram etc., and with a handy device like mobile phone there is a raise in cyber bullying. Now using social media has become a habit. With the increased use of social media, the crime related to it is frequent. One of these cyber crimes is cyber bullying. “Cyber bullying is abuse/ harassment by teasing or insulting the victims’ body shape, intellect, family background, dressing sense, mother tongue, place of origin, attitude, race, caste, or class using modern telecommunication networks such as mobile phones and Internet”. The respondents were college students from Chennai city in Tamil Nadu. Students were chosen from Arts, Science, and Law and Engineering background through convenient sampling method. Data was collected through 5- point scaled questionnaire. The aim of the study is to find the prevalence and victimization of cyber bullying among college students in Chennai city. Correlation value (0.923, $p < 0.05$) shows there is a strong positive relation between awareness and victimization. It is also found that cyber bullying doesn’t cause a significant effect on the victims.

Keywords: Cyber-crime, Cyber bullying, social media, online bullying, College students

A STUDY OF DIGITAL FORENSIC TOOLS, HACKTIVISM PHENOM AND CHALLENGES

Ms. N. Ashwini¹, Dr. Syed Umarhathab²

¹Ph.D. Research Fellow, Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Tirunelveli. E-mail: ashwiniachu43@gmail.com.

²Assistant Professor, Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Tirunelveli. E-mail: drsyedumar@gmail.com.

Abstract

Hactivism is the greatest test being looked by the Cyber world. Numerous advanced digital forensic tools are being created to manage this test however at a similar pace programmers are building up the counter procedures. This paper incorporates the advanced crime scene investigation fundamentals alongside the ongoing patterns of hactivism in long range informal communication locales, distributed computing, sites and phishing. The different devices of legal sciences with the stage bolstered, the ongoing variants and permitting subtleties are talked about. The paper stretches out with the present difficulties being faced by digital forensics,

Keywords: Hactivism, Memory legal sciences, Network legal sciences, Mobile Phone legal sciences, Database criminology, Anti advanced digital forensics (ADF)

CYBER VENTING- A HEALTHY TOOL FOR MENTAL HEALTH

Riya Singh¹, Shally Chauhan²

¹School of Basic and Applied Sciences, Galgotias University, Greater Noida, Uttar Pradesh, India

²School of Basic and Applied Sciences, Galgotias University, Greater Noida, Uttar Pradesh, India

Email: emilysingh.dav@gmail.com; shallychauhan1222000@gmail.com

Abstract

The phenomenal change in lifestyle influence the most delicate thing in our life i.e., our mental health. People doesn't give equal importance to mental health in respect to physical which enhances the level of stress, depression and heinously affects our capability of thinking, responding in circumstances and making choices or decisions. Senior executives of companies increased the work hours to cope up the work and also cancelled holidays. This brings up to frustration and anger level in employees which deliberately causes problems like anxiety, depression, short-temperedness, interpersonal and intrapersonal conflicts. All these negative emotions can effortlessly harm the person's productivity. All these activities force the employ to let off their steam which is called venting and as the growth of technologies is increasing day by day, people use social platforms to rant out their frustration, anger, irritation, backbiting etc., in every institution, organizations etc., which is called Cyber-venting. This is the root cause that the rate or need of Cyber-venting is increasing in day-to-day life. Recently there are many websites available which provide a platform to employees to rant and releasing their information which somehow enhance them to improve their mental health and make the virtuous and conflict free environment of office premises. In recent years, researchers have attempted to settle the contradiction by showing that venting doesn't reduce feeling of anger but has other benefits like improving people's mood, sense of fairness etc. This research paper includes random and controlled sample. Dependent sample are measured quantitatively in the form of a questionnaire.

Keywords: Venting, Mental Health, Depression, Backbiting, Conflicts, Cyber-venting

VALIDATION OF AUTOMATIC VOICE COMPARISON USING LIKELIHOOD RATIOS AND COMPARISON WITH TRADITIONAL APPROACHES

Ms. Meenu Hariharan¹, Dr. Rajesh Verma²

¹MSc Forensic Science Rashtriya Raksha University Gandhinagar, Gujarat

²Regional Forensic Science Laboratory, Mandi, Himachal Pradesh

Abstract

Forensic Scientists use voice comparison methods for evidence interpretation and to narrow down the suspects in a case like auditory method, spectrographic analysis and statistical analysis. Automatic speaker recognition is adopted in many non-forensic industries as biometrics and security features in mobile phone devices. This research addresses the void found between the two approaches by using the likelihood ratios as standard that is compatible with the requirements of the new paradigm as well as accounts the use of both the traditional acoustic phonetic and automatic methods. These approaches have been used on the voice recordings of a case received in the laboratory and reported as per the traditional approach and ABRE standard. Also, the same recordings were further examined in the automatic system. The comparison scores were converted into likelihood ratios and the strength of evidence in the traditional approach is compared with the strength of evidence in terms of likelihood ratio in the automatic approach obtained in the calibration of scores. To assess the similarity and typicality of the voice features, a database of same words was generated for 16 male volunteers after taking their informed consent. A transcript was prepared of the speech and 20 clearly spoken words were identified in the recording using Audacity software. Spectrographical analysis by matching the peaks and formant spectra comparison was performed by esection software. The likelihood ratio for each word was evaluated using the *dnorm* function in R or the *normdist* function in MS-Excel. Results obtained shows 13 words with 3 formant peak matches and rest having 2 peaks matching, ABRE standard of reporting the result corresponds to a “probable identification”. The likelihood ratios were greater than one for F1 in 15 words, F2 for 17 words, F3 for 17 words and F4 for 13 words which indicates high probability of the suspect being speaker of the words. The likelihood ratio of 470 and cost of log likelihood ratio (cllr) of .07 for the suspect highlights that its equivalent to moderately strong support for the prosecution hypothesis and the cllr of 0.07 means an excellent validation of the likelihood ratio.

Keywords: Forensic Speaker recognition, Voice Biometrics, Automatic Speaker recognition, Likelihood ratios, Forensic Voice comparison.

FORENSIC INVESTIGATION OF THE BASIC DIGITAL EVIDENCES IN MOBILE DEVICES

Gladwel Kubwalo¹

¹Lovely Professional University, Phagwara, Punjab

Abstract

Crimes have been happening since time in memorial. These crimes are committed differently and that is the reason why they have different names depending on the elements that constitute that offence. It is the core duty of investigators in law enforcement agencies as well as other relevant stake holders to crack down and identify the perpetrators of crimes. It is empirical to mention that the identification of perpetrators of crime depends on the evidence that has been collected. Evidence most of the times is collected at the scene of crime in physical form or from eye witnesses who are people that are present when a crime is being committed. Sometimes evidence is circumstantial depending on how the events surrounding the criminal act occurred. In the modern world, mobile devices are playing a very important part in our daily life. These days, mobile devices are being used by individuals of all classes as opposed to a distant past whereby usage of mobile devices was limited only to high class people. The wide usage of mobile phones provides vast availability of evidence. Potential evidence is collected from electronic devices such as mobile phone in digital form. It is advisable that all sorts of evidence that has been scientifically collected and analysed must be treated according to the legal standards in order to be admissible in court. Forensic investigators are mandated to ensure that they follow proper legal standards when handling forensic evidence. This paper will highlight some forensic evidences and the methodologies on how to collect them from mobile devices. It will also highlight some of the tools that are used to recover data or forensic evidences found in mobile devices.

Keywords: Offence, Law enforcement, Eye Witness, Electronic Device, Perpetrators

ONLINE CRIMES AGAINST WOMEN AND CHILDREN IN CYBER SPACE - A SURVEY BASED RESEARCH REPORT

Jagriti Khanna¹, Anjali Jangra², Yogita Saini, Pankaj Kumar, Naveen Saini

¹G.D.Goenka University

Email: jagriti.g16@gmail.com

Abstract

The advancement of technology has not only redefined the human life but it also has redefined cybercrimes. The rapid growth of internet users, speedy spread of mobile information and the use of social media has led to the emergence of cyber violence against women and children of all age groups which is impacting their security, dignity and psychological and social well-being as a whole. The digital space has a constructive reality in which the criminals commit crimes in a more complicated and complex way. Cyber violence against women and children is on a rise in all disciplines and the lack of awareness leads to the unstoppable commission of these crimes. The purpose of the paper is to understand and highlight the common cybercrimes experienced by individuals and to know about their opinions, knowledge and facts on the on-going cybercrimes against women and children and the level of awareness among the individuals. The paper discusses the common types of cybercrimes against women and children which are namely cyber stalking, cyber pornography, morphing, sending obscene messages, blackmailing or threatening, bullying and trafficking. It also highlights the major reasons for the growth of cyber violence, how it is impacting their social life. This paper analyses the cases and their judgments along with the cyber laws on this matter. This paper will also recommend the suggestions and solutions that are required to be taken up in order to curb cybercrime against women and children.

Keywords: Cybercrime, Cyber space, Women, Children, Information technology, Victim, Cyber laws, Security Awareness

CYBER & DIGITAL FORENSICSShivani Rai¹¹Mahatma Gandhi Central University, Bihar**Abstract**

The Cyber World, or cyberspace, is more than just the internet. It refers to an online environment where many participants are involved in social interactions and have the ability to affect and influence each other. In cyberspace people interact through the use of social media. Example of cyberspace interactions are: Create media, share media and consume media. Through Internet-based social networking sites such as Facebook, Twitter and Instagram, people can remain connected to their loved ones (e.g family and friends) and their larger community (e.g. distant relatives and ex-classmates), and even make new friends across the world. When people are online, most of them engage in activities that leaves a digital footprint. A digital footprint refers to all the credentials information about a person like name, date of birth, age, gender, & location etc. which are shared by user or someone else. These information can be misused by the hackers, the global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year. A report by Risk Based Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine month of 2019 alone. This number of record is more than double (112%) the number of records exposed in the same period in 2018. The threats countered by cyber- security are three-fold: Cybercrime, Cyber-attack, and Cyberterrorism. The people who collect, process, preserve and analyse computer-related evidence, they help identify network vulnerabilities and then develop ways to mitigate them. Sluethkit autopsy and Toolkit are the tools which are used to recover deleted data from a disk. These kind of tools are used help forensics team to investigate digital evidences.

Keywords: Cybercrime, Digital evidence, Cyber world, Cyberterrorism, Forensics.

RETRIEVED DATA COMPARISON OF WHATSAPP AND SIGNAL APPLICATION

Preeti Ansari¹, Ritika Sharma²

Abstract

Digital forensic is the science of identifying, extracting, analysing and presenting the digital evidence that has been stored in digital devices. WhatsApp and Signal are mobile applications which allows user to send messages, images, audios, videos, documents, user location and make audio and video calls. Forensic evidences are recovered from mobile phones by using different forensic tools so that data can be extracted, decoded, analysed and reported. The smart phones are merely used in criminal activities and can be used for digital evidence as a part of an investigation. In terms of investigation mobile phones play an important role as they are routinely found in crime scenes. There is a huge demand in extracting data from mobile phones today as crime rate in rapidly increasing. Many digital forensic tools used by investigator were not originally designed for forensic application. Data retrieval tools are generally used as the process of salvaging data partially or completely from damaged, failed, corrupted storage media. This paper focuses on retrieval of data and also comparison of extracted data from WhatsApp and Signal application by using MSAB XRY and Cellebrite UFED on the basis of different chipsets used in Android and Apple Smartphones namely Qualcomm's Snapdragon, Exynos, MediaTek, TSMC used in iPhone.

Keywords: Mobile forensic, WhatsApp, Signal, MSAB XRY, Cellebrite UFED, Data Extraction.

ePoster Abstracts

CYBER PARENTING: NEED TO CREATE BOUNDARIES

Preeti Kiran¹

¹Kurukshetra University, Kurukshetra, Haryana

Abstract

In affluent cultures, Internet access has become practically universal in homes with school-aged children. The Internet is both a fantastic social and educational tool and a minefield of potential threats. Children are more likely to be exposed to these threats if their parents do not provide adequate support and advice. However, this can lead to conflict and discord between parents and children. Because children are more knowledgeable and adept in the domain of technology than their parents, the situation is exacerbated. Parents are confronted with a new parenting dilemma regarding the use of the internet that previous generations of parents were not faced with. Although there are a variety of tactics and tools that parents may use to guide, protect, and oversee their children's internet use, many parents believe they are ill-equipped to do so. Because most youngsters use digital gadgets and the internet on a daily basis, cyber parenting is a hot topic these days. Almost every child of a certain age now utilises a digital device that is connected to the internet, which means that parents must deal with a whole new part of parenting known as "cyber parenting." They must choose what is good and harmful for their children when it comes to using digital gadgets, how much control is appropriate, and how to keep their children safe in the digital world. It's important to keep an eye on them and make sure they're acting appropriately and safely. This paper deals with the various case studies where creating a boundary at an early stage was very essential.

Keywords: Cyber-Parenting, Digital-Parenting, Digital Era, Gadgets, Cyber Pandemic, Internet.

RISE IN CYBER CRIME DURING PANDEMIC

Ayushi Verma¹

¹Kurukshetra University, Kurukshetra, Haryana

Abstract

Cybercrime is a criminal activity that either targets or uses a computer, computer network or a networked device. Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money or use the data as an anonymous person. Cybercrime is carried out by individuals or organizations. There was a significant spike in cyber-crimes in Delhi during the pandemic induced lockdown with as many as 135 such offences being reported every day on an average in May 2020. It is estimated that nearly 33,000 cases were registered until November, 2020. For instance, in January this year, 1,480 cyber-crimes -- or about 48 offences every day and so on. The spike in cyber-crimes during and after the lockdown is mainly due to unemployment, cash crunch, lots of spare time and easy availability of tools. The most common crimes observed during this era were Ransomware, Data Breach, Phishing, Scams and Online Stalking. With the help of this research paper an awareness can be provided among the people to get informed about cybercrimes that could happen in this pandemic and the ways for its prevention.

Keywords: Cybercrime, Pandemic, Data Breach, Forensic Science, Awareness, Cyber-Security.

CYBERPSYCHOLOGY

¹Arti Varshney

¹Sherlock Institute of Forensic Science, New Delhi

Abstract

CyberPsychology is the branch of Psychology that tells that how we interact with others using technology, how do we develop technology to best fit our requirements and desires and how our behavior and psychological states can be affected by technologies. As, with the advancing technology and in tough time of pandemic, people are bound to socialize through technology and as when surfing through the net, some of it describe it as 'Everywhere I do on internet, I find ME!', signifying people thoughts of seeming the technology an extension of themselves. To know how one interact with technology, we apply Eight Dimensions of Cyber psychology architecture. There are three major domain where cyberpsychology plays a vital role, namely cyber engineering, online privacy and cyber bullying. Cyber engineering leaves the culprit stressed and demotivated which accompanies other mental disorders and affecting the overall mental health. Online privacy on the other hand, exposes risks of cyber relationships, social media platforms etc. which affects the youth and the adults as well. Cyberbullying is taken as a matter of interest and to be addressed with strict actions as it harms people, mainly youth's mental health. To take a step ahead in prevention of the same and make your society a better place to live in, Identifying social situations, Finding malicious activity patterns, Fostering collaboration with lawmakers, Increasing public awareness and Understanding the effect of cybercrime.

Keywords: cyberpsychology, cyber awareness, socialize, cyber bullying, cyber engineering, online privacy, social media, spear-phishing, internet.

USING A LAYERED APPROACH FOR GRAPHICAL-BASED PASSWORDS

Jessy Ayala¹

¹Tandon School of Engineering, New York University, Brooklyn, New York, USA

Abstract

For as long as user-login techniques have existed, it is widely known that alphanumeric passwords have been the most popular type; however, graphical-based passwords are naturally harder to crack because problems are more computationally difficult for attackers to solve. In security, the concept of layering is one that is feasible for implementation. In the proposed method, Bluetooth Low-Energy (BLE) and the cued-click point method are layered together as an overall mechanism in effort to improve overall security of the log-in process. Furthermore, the scope of this mechanism is meant to be in the context of a corporate environment whose employees handle sensitive information. Previous literature go into how graphical passwords are easier to remember for the human mind, taking a visual approach as opposed to an alphanumeric one. In addition, a detailed description of how the cued-click point method works and previous graphical password implementations have also been explored. The proposed methodology adopted comes in two steps: the user has a physical device that utilizes BLE to upload an image to the computer; once successful, the user then proceeds to input their password via the cued-click point method for authentication. Data collection regarding computation power are done in comparison to historical graphical password methods and how they stand up towards common threats and vulnerabilities inherent to bypassing password interfaces. The evidence acquired implies the proposed method is more secure than using alphanumeric passwords and previously explored graphical-based password mechanisms for authentication from both quantitative and qualitative standpoints. In conclusion, layering a graphical password with physical security provides an extra boundary against attacks, making it more difficult to compromise accounts. Though in practice it may seem less feasible for the user to go through this process to log in their device, they can be assured that an adversary will have an insignificant chance of compromising personal information without having both the physical device containing the login image and the sequence of sub-images for a successful attack to occur.

Keywords: Authentication, Bluetooth, Graphical Password, Picture Password, Security.

LAW MERGER – A COMBINED VERSION OF IT ACT LAWS AND IPC LAWS IN SEXUAL HARASSMENT CASES

Aastha Mahna¹

¹B.Sc. (H) Forensic Science Second year, Amity University, Noida

Abstract

India does not have adequate laws related to sexual violence specifically in cyberspace. As the number of cases related to online sexual harassment are sky rocketing, we must be aware about some laws which have been described in the Indian Penal Code, 1860 and Information Technology Act, 2000 related to sexual violence. Only few aspects are dealt with these laws but, many of us are still unaware of this and we consider online sexual harassment only as bullying and ignore it majority of times which gives criminals the freedom to carry on with such crimes without getting into any serious trouble. The main objective of this poster is to highlight the laws and punishment related to them in order to make cyber environment a safe place. Legal aspects in the Indian Penal Code were amended recently in 2013 to directly report digital sexual violence. As a result of which 3 sections were updated in the IPC, 1860. There are listed sections i.e. Section 354A, Section 354C, Section 354D. Apart from these direct laws which came into being in 2013, there are other laws which also deals with cybercrimes and under these the crime can be reported and perpetrator can be imprisoned or fined. These are Section 499, Section 503, Section 507 and Section 509. The IT ACT, 2000 was also amended in 2008 in view of increasing cybercrimes and have resulted in the following sections related to sexual harassment are Section 66C, Section 66E, Section 67, Section 67B. Apart from these laws there are many bills which have been discussed in the Parliament related to crime against women. One bill which has been accepted is the Indecent Representation of Women Act, 2012. The Indecent Representation of Women (Prohibition) Act regulates and prohibits the indecent representation of women through the media of advertisements, publications etc. The Indecent Representation of Women (Prohibition) Amendment Bill, 2012 seeks to broaden the scope of the law to cover the audio-visual media and content in electronic form, and distribution of material will also include distribution on the Internet and the portrayal of women over the web.

Keywords: Sexual Violence, Indian Penal Code, Harassment, Bullying

CHIP-OFF TECHNIQUE IN MOBILE FORENSICS

Vikas Razdan¹

Abstract

With the advent of the digital age, one of the most important new areas of forensics is digital forensics — specifically the ability to extract data from a seized devices that are physically damaged, preventing investigators from using automated techniques to extract the data stored within the device that has suffered physical damage and is completely non-functional, the only way to obtain information from the device is to remove the device's flash memory chip. Chip-off forensics can be successful for devices that have received waterlogged and fire damage. Instead, investigators turn to chip-off analysis, where they use a thermal-based procedure to physically remove the memory chip from the device, and access the chip directly to extract the data stored on the chip. The technique is divided in six parts including opening the device using heat and air combination to remove its back and front covers, battery screws, other connections, etc. to retrieve the motherboard, the chip mustn't be overheated. It will delete all data. Usually it happens, because an examiner thinks that air isn't hot enough to melt soldering flux, and increases temperature too much. An examiner should remember, that chip is not only soldered to the board, but also glued with compound. That's why it should not only heat it, but also try to extract it carefully. Its recommend using IR station. Even the simplest IR station with automatic temperature regulator allows unsoldering BGA chips with safety. For standard chips unsoldering temperature is ~225-230 °C, for chips glued with compound – ~240-245 °C. To extract a chip from a smartphone board it's recommend heating it to 240 °C and then use a blade to extract it. NAND flash memory is located on the retrieved motherboard/circuit board, using appropriate heat (disordering) and chemicals (adhesive removal), and the memory chip is physically removed. The removed chip is cleaned and/or rebelled if necessary and the forensic image/dump of the chip is then acquired by using an imaging software and an adapter connecting it to the PC. The further analysis is conducted with the standard software's at the laboratory.

Keywords: Mobile Forensics, Damaged Mobile Phones, Chip off Method, Memory Chip, Rework Stations

CYBER TERRORISM: A THREAT TO NATIONAL SECURITY

Neelkamal Ganesh Battu¹

Abstract

Cyber-attacks, network security and information pose complex problems that reach into new areas for national security and public policy. This paper looks at one set of issues – those related to cyber-terrorism and cyber-attacks on critical infrastructure and their implications for national security. Cyber-terrorism is “the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population.” The premise of cyber terrorism is that as nations and critical infrastructure became more dependent on computer networks for their operation, new vulnerabilities are created – “a massive electronic Achilles' heel.” A hostile nation or group could exploit these vulnerabilities to penetrate a poorly secured computer network and disrupt or even shut down critical functions. Much of the literature on cyber-terrorism assumes that the vulnerability of computer networks and the vulnerability of critical infrastructures are the same, and that these vulnerabilities put national security at a significant risk. Given the newness of computer network technology and the rapidity with which it spread into economic activity, these assumptions are not surprising. A closer look at the relationships between computer networks and critical infrastructures, their vulnerability to attack, and the effect on national security, suggests that the assumption of vulnerability is wrong. A full reassessment is outside the scope of this paper, but a brief review suggests that while many computer networks remain very vulnerable to attack, few critical infrastructures are equally vulnerable. This poster aims to draw conclusion on the various methods to counter cyber terrorism and create safe environment for the civilians and protect the national integrity of the nation.

Keywords: Cyber Attacks, Cyber-terrorism, Vulnerability, National Integrity

CYBER RELATIONSHIPS: BOON or BANE

Anirudhvaibhav Gupta¹

¹B.Sc. (H) Forensic Science Second year, Amity University, Noida

Abstract

The Internet has made life a lot easier by making information more accessible to all and creating connections with different people around the world. However, it has also led a lot of people to spend too much time in front of the computer, and get affected by internet addiction. Internet addiction is of different types and in this pandemic situation; the cases of cyber relationship addiction are increasing with a huge number day by day. Cyber or online relationship addiction is deeply involved with finding and maintaining relationships online, which often leads to forgetting and neglecting real-life family and friends. The reason behind cyber relationships has to do sometimes with issues like self-disclosure, self-esteem, fear of physical relations, body image, and social interaction. The fact that most online relationships take place behind a computer screen can lead to issues like betrayal. Certain issues with cyber relationships are, (people lying on their profiles, a lot of individuals there are only looking for physical intimacy, and chances of lasting the relationship are very low). Certain points to be considered if one looking for a cyber relationship are, (don't engage solely in a cyber relationship, don't build a relationship with someone who lives in a different country, forget about people who are either committed or married). Hence, cyber relationships can be boon, creates room for introverts, more means of interaction, have features like auto compatibility match and showing its other sides of, lack of information, identity theft, unrealistic expectations, addiction, and mental trauma as a bane.

Keywords: Cyber Relationship, Addiction, Internet, Mental Trauma, Unrealistic



In Association with



SFSRM

