eConference Proceedings

IASR
INTERNATIONAL ASSOCIATION
OF SCIENTISTS & RESEARCHERS

11th INTERNATIONAL
eCONFERENCE-2021

Cyber Security

Supported by

Sherlock Institute of Forensic Science India

linktr.ee/forensicscienceinstitute

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 eConferences 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 11th International eConference on "Cyber Security", 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".

Keynote Speakers

Sanjay Sahay

Navigating the Future of Data Protection & Privacy

Dr. Varun Kapoor (IPS)

The Key Role of Citizen Awareness in Ensuring Cyber Security

Elena Feldman

Problems of Investigation Across Cyberspace

Na. Vijayashankar

Role of Forensics in Personal Data Protection

Prof. Prasad B. Honnavalli

Cyber Security Ignorance can be Disastrous

Aashish Sutar

Cyber Security Organisations in India and Reporting of Cyber Crimes

E. Sai Prasad Chunduru

Digital Forensics-Trends

Nitin Pandey

Cyber Threat Intelligence

Amrit Chhetri

Role Of Forensic Triage in Cyber Security Trends 2022

11th INTERNATIONAL eCONFERENCE-2021

Cyber Security

Supported by

Sherlock Institute of Forensic Science India

linktr.ee/forensicscienceinstitute,Contactus:+919818877002

SPEAKER'S PROFILE

SANJAY SAHAY

Police Computer Wing, Govt. of Karnataka, INDIA

Sh. Sanjay Sahay is an IPS officer of the 1989 batch, Karnataka Cadre, who took the Voluntary Retirement Scheme in March-2020 and is an alumnus of Delhi's prestigious St. Stephen's College. With 31 years of distinguished service as Police Chiefs of three dist. and Additional Commissioner of Police in Bangalore City Police has also headed the investigation wing of Lokayukta, Police Welfare, Public Grievances & Human Rights, State Police Communication and State Crime Records Bureau as ADGP. He led the UN, Recruitment & Selection for Kosovo Police Service at Pristina, Kosovo, erstwhile Yugoslavia and was a Regional Commander in the UN Peacekeeping Mission in Sudan. Since his first indulgence in Cyber Security in 2013, today, he happens to be India's most sought-after practitioner and speaker in this area. He is a Complete Technocrat with 20 years of hands-on experience in governance and technology. Post-retirement, in his new role as a Tech Entrepreneur, he is now the Founder Director of TechConPro Pvt. Ltd – World's first Technology Consultancy Aggregator.

DR. VARUN KAPOOR (IPS)

Rustamji Armed Police Training College, Indore, INDIA

Dr. Varun Kapoor is a senior IPS officer. He has done his BE (Honours) Mechanical Engineering – NIT Trichy (Tamil Nadu). He joined India Police Service in 1991 and was allotted Madhya Pradesh Cadre. He is currently ADGP, Rustamji Armed Police Training College, Indore. He has served as SP in three districts – Dhar, Sehore & Ratlam. He was DIG in three ranges – Chhatarpur, Ratlam & Ujjain and ADG in one zone – Indore. His other posting includes IGP, Police Radio Training School, Indore; ADGP, Narcotics, Indore. He started Black Ribbon Initiative for cybersecurity awareness among community members. He has conducted 453 sessions across India in schools, colleges, institutions, organizations, departments etc. Over 3,00,000 citizens were made aware in 2 hour long highly interactive sessions. Out of these, 109 have been webinar-based sessions during the COVID-19 times. This pan India effort in 28 states is also a record in itself as lakhs of citizens have been reached and made cyber security aware and equipped. He holds a World Book of Records London – Maximum Number of cybersecurity awareness workshops by anyone anywhere in the world (2018). He started police training under the initiative – THE BLUE PALM. Over 5000 cutting edge level officers (SI-SP) of 20 state police forces; 6 different paramilitary troops, and the Indian Army trained in the specialized course in 12 modules. To date, 136 such practices have been organized. He has conducted special training workshops across the country to use cyber technology for improving wildlife protection and solving wildlife crime being done under a campaign designated as ROARING TIGER INITIATIVE. Presently a unique project is being delivered across the country in 6 leading tiger reserves. This project is called "CYBER CLAW" and is being coordinated by the National Tiger Conservation Authority of the Ministry of Environment & Forests of the GOI. He is also a regular faculty at premier training institutions of the country. He is the first police officer in Asia to be awarded an Honorary Doctorate in Cyber Security (Indore University).

SPEAKER'S PROFILE

ELENA FELDMAN

F-Lab, RUSSIA

Elena Feldman is a senior trainer in network security and advanced networking. She has 10-years of experience in Telecom core networking and operational departments. Since 2011, she has been the head of the CSIRT operational department at Ural Federal Region, private cybercrime investigator and forensic expert in law. She is currently a Professor at the Department of Computer Security and Applied Algebra, Chelyabinsk State University, Russia. She is the founder of Forensic Laboratory F-Lab, Cyber Security Center Ltd. (law and technical support operations for business and government).

NA VIJAYASHANKAR

Foundation of Data Protection Professionals in India, Bangaluru, INDIA

Na. Vijayashankar (Vijayashankar Nagaraja Rao), more popularly known as Naavi, has been a pioneer in Cyber Law in India and a pioneer in Data Protection and Data Governance. A professional based in Bangalore, he is a Data Governance Consultant developing jurisprudence in Cyber Law and Data Protection Law. As a thought leader, he has pioneered several activities in India around Cyber Laws and Data Protection. He is the founder of the Naavi organization and Cyber Law College. He is the Chairman of the Foundation of Data Protection Professionals in India (FDPPI), the premier organization in India dedicated to data protection. He has pioneered many Cyber Law related technology services such as Cyber Evidence Archival Center and Online Dispute Resolution. In the field of Data protection, he has pioneered through FDPPI, new Certification programs for "Certified Data Protection Professional" which are designed to provide more value for money for the Indian Data Protection Professional than the other international certification programs and has also introduced an exclusive framework Personal Data Protection Standard of India (PDPSI) for the implementation and Certification of organizations for compliance of Data Protection laws. He is a visiting faculty in several educational institutions, including NLSUI Bangalore, NALSAR, Hyderabad, BMS Law College, Bangalore, NLUI, Raipur etc. He is also a guest faculty in NPA and several other organizations. He is an author of many books, including "Personal Data Protection Act of India (PDPA 2020)" and the concept of "Theory of Data". He has expertise in the multiple domains of banking and Finance, Advertising and Marketing, Education, Cyber Law, Information Security, Data Protection and Data Governance.

SPEAKER'S PROFILE

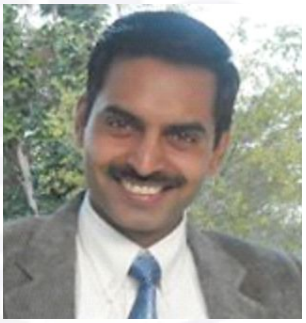
Prof. PRASAD B. HONNAVALLI

PES University, Bengaluru, INDIA

Prof. Prasad B. Honnavali is currently working as a Professor in Computer Science and Engineering at PES University, focusing on all aspects of Information Security. He leads the Teaching, Research, Executive Education and Industry Consultancy in this domain. He is the Director for PESU Centre for Information Security, Forensics and Cyber Resilience and the Director for the PESU Centre for Internet of Things, focusing on Security. Before academia, he worked for many years in various industries & corporate leadership roles such as an end to end program management/delivery of multiple, large, complex System Integration programs encompassing IT Technology Transformation, IT Infrastructure, complex Cloud engagements – IaaS, PaaS & SaaS, Software Development, Automation, IT Security, and Managed Services.

AASHISH SUTAR

Ministry of Defence, Govt. of India, INDIA



Aashish Bhagwan Sutar is Geographic Information System (GIS) and Digital Forensics aficionado. He is also a National Cyber Security Scholar. Apart from Masters in IT, he holds several certifications in GIS and the Cyber Security field. He has more than 20 years of experience in GIS, Cyber Security, Cyber Security Audits and Digital Forensics. He also has vast experience in executing GIS projects, setting up Cyber Forensic Laboratory, preparing Quality manuals for the Forensic Lab and conducting surveillance audits. He has also appeared as an Expert Witness in several Courts of Law on numerous occasions. After holding the charge of Cyber Forensic Laboratory at Delhi for more than three years, he is now pursuing further studies in GIS.

SPEAKER'S PROFILE

E. SAI PRASAD CHUDURU

Central Forensic Science Laboratory, Hyderabad, DFSS, MHA, Govt. of India, INDIA

Eswara Sai Prasad Chunduru is currently working as Assistant Director and Scientist C with the Directorate of Forensic Science Services, Ministry of Home Affairs, Government of India. He is an experienced senior professional and subject matter expert in digital forensics. He has actively contributed to framing the policy documents I4C (Indian Cyber Crime Co-ordination centre) and CCPWC (Centre of Cybercrime Prevention against Women and Children) of MHA (Ministry of Home Affairs) Government of India. He has also contributed to establishing NSFL (National Cyber Forensic Laboratory for Evidentiary Purposes) at CFSL Hyderabad. He has numerous professional and technical certifications under his name. He was appreciated by Director General Police, Telangana Police, for his contribution in compiling the book 'Handbook on Cyber Crime Investigation'. He has numerous national and international publications under his name. He has actively conducted critical professional training, lectures, and workshops. He has delivered more than 1500 lectures and was a guest and visiting faculty in various National premier academies/training institutes/professional bodies in Incident Response Management, Cyber Forensics, and investigation of Digital evidence.

NITIN PANDEY

Police Headquarters, Lucknow, INDIA

Nitin Pandey is a National Cyber Security Expert, Researcher, Penetration Tester, International Speaker, Author, Trainer, Blogger, and has experience of more than 13+ years in the Cyber Security Domain. His expertise in Ethical Hacking, Information Security and Compliance, Dark Web, Counter & Cyber Terrorism, Cyber Crime Investigations, Cyber Threat Intelligence, Cyber Safety, Social Engineering Techniques, Financial Frauds, CyberPsychology, and the Latest Cyber Threats is widely recognized in India and abroad. He has been invited by the Government of Russia and Sri Lanka to deliver talks and train professionals in cybersecurity. He is Chairman of the National Information Security Council. He is also a Founding member and lead consultant of the Cyber Research and Analysis Foundation (CR&AF) and Founder of Hackers Day. He was Chapter Leader of DEF CO and has also led OWASP & OWASP India. He has been invited to various National & International Cyber Security conferences as Chief Guest, Keynote & Technical Speaker. He has trained over 20,000 students, corporate people, police, cybercops, government officials by giving workshop training & sessions. He has also been acknowledged & listed in the Hall of Fame by Tech giants such as Google, Microsoft, Dell, Intel, Belkin, Avira Antivirus, Adaware, etc., for finding Security bugs/loopholes in their Websites & databases.

AMRIT CHHETRI

DFIR Expert, AI and Cyber Security Researcher, West Bengal, INDIA

Amrit Chhetri has 17 years of experience in IT/ICT. He has worked in the Business Intelligence Industry for nine years, gaining experience in System Requirement Analysis, Software System Design, Testing, Quality Assurance and User Manual Development. During nine years in BI Industry, he has received opportunities to work across all significant Business Sectors, including Manufacturing, Pharmaceutical, Banking and Finance/Insurance, Fashion, Shipping, Aviation and E-Commerce. He has provided BI Consultancy in some of the great organizations, including APL, Disney World, Fidelity, HSBC, Infosys, NIIT, Kean India (NTT Data), and LG/CNS India. After this, he worked in the IT Solution Domain. He received pride in giving consulting as an energetic Functional Consultant, Social Media Strategist and Software Solution Architect to design and deliver Architecture Concepts to clients such as Crowdsource Community. Currently, he is into Cyber Security, Computer Forensics, Data Science and Machine Learning related domains and conducting Training, Workshops, Seminars, Penetration Testing and Security Auditing for the last six years to clients of Rosefinch/RCS, Siliguri. He has acquired technological expertise in Cyber Security/Forensic Programming- with Python, J2EE, C++, Scala, etc. He has published a Computer Forensic Book titled "Computer Forensics Practical Guide Investigating Computer Attacks". He has learnt Machine Learning using Google Tensor Flow-for Cyber Security, Computer Forensics, Incident Management, CSOC and CII (Cyber Counter Intelligence). To acquire and contribute to IT Ecosystem, I'm also engaged with different Business, IT, Cyber Security and Machine Learning Communities/Forms. Some of them are NASSCOM Community, DSCI, IEEE, DevOps, Human Brain Project and Internet Security Society.

Chairing Panel 27th Nov. 2021

Chairperson

Lt. Gen. Arun Sahani PVSM,UYSM,SM,VSM

Former General Officer
Commanding in Chief, Indian Army

Chairperson

Prince Boonlia

Digital 4n6 Journal
Udaipur

Chairperson

Dr. A. Nagarathna

National Law School of India
University, Bengaluru

Chairing Panel 28th Nov. 2021

Chairperson

Santosh Khadsare

Cyber Security Professional
Senior Cyber Forensic Expert

Chairperson

Pawan Desai

MitKat Advisory Services Pvt. Ltd
Gurugram

Chairperson

Rakhi R. Wadhwani

Senior Assessor
Mumbai

11th INTERNATIONAL eCONFERENCE-2021

Cyber Security

Supported by

Sherlock Institute of Forensic Science India

linktr.ee/forensicscienceinstitute,Contactus:+919818877002

Hon'ble Jury Members

PROFESSIONAL CATEGORY

JURY MEMBERS FOR PAPER PRESENTATION

Ritesh Bhatia
Founder
V4WEB Cybersecurity, Mumbai

Deepak Kumar
Digital Forensics & Cyber Intelligence, India

Amol Desmukh
Nodal Officer Mantralya Govt. Institute, Mumbai

Dr. Harsh Joshi
Information Security Group HDFC Bank, Mumbai

JURY MEMBERS FOR ePOSTER PRESENTATION

Mohit Yadav
Craw Cyber Security Pvt. Ltd.
New Delhi

Amar Thakare
Lumiverse Solutions Pvt Ltd.
Nashik

Amrit Chhetri
Digital Forensics Analyst, Cyber Security Evangelist, DFIR Researcher (Edge AI & QML), Siliguri, West Bengal

Davinder Singh
Cylos Consulting Pvt. Ltd.
New Delhi

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

11th INTERNATIONAL eCONFERENCE-2021

Cyber Security

Supported by
Sherlock Institute of Forensic Science India

Hon'ble Jury Members

STUDENT CATEGORY

JURY MEMBERS FOR PAPER PRESENTATION

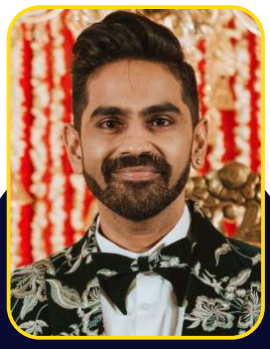
Sri Ram
PrimeFort Pvt. Ltd.
India

Deep Shankar Yadav
eSec Forte Technologies
Gurugram

Gaurav Sharma
Cyber Security Professional,
Gurugram

Sailaja Vadlamudi
SAP Labs India Pvt Ltd
Bengaluru

JURY MEMBERS FOR ePOSTER PRESENTATION



Saurabh Athawale
Kcyber Experts Pvt. Ltd.,
Nagpur

Mrinal Kanti Biswas
EY Global Delivery Services
India

Naveen Pal
Capgemini,
India

Gopika Baghel
Forensic Science Education
Society, Raipur

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

11th INTERNATIONAL eCONFERENCE-2021

Cyber Security

Supported by
Sherlock Institute of Forensic Science India

IASR Advisory Board

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

JOHN PAUL OSBORN
Osborn & Son
New Jersey

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

Dr. ROBERT GREEN
University of Kent
England

MICHAEL WAKSHULL
Q9 Consulting, Inc.
California

Prof. EMILIO NUZZOLESE
University of Turin,
Italy

MICHAEL W. STREED
SketchCop Solutions Inc.
California

Dr. RAJINDER SINGH
(Former) Central Forensic Science Laboratory, CBI, New Delhi

Dr. SANJEEV
Central Forensic Science Laboratory, Chandigarh

Dr. RAKESH Kr. GOREA
Gian Sagar Medical College
Patiala

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

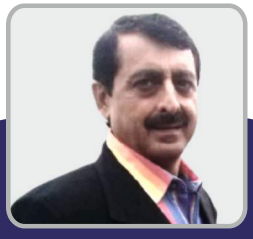
HEIDI H. HARRALSON
Spectrum Forensic International LLC., Arizona

D. C. SAGAR (IPS)
ADGP Police Training & Research, Bhopal, M.P.

K. V. RAVIKUMAR
Rashtriya Raksha University
Gujarat

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

MOHINDER SINGH
Former GEQD,
Shimla & Hyderabad



DEEPAK HANDA
(Former) Central Forensic Science Laboratory, CBI, New Delhi

DEEPA VERMA
Forensic Science Laboratory
NCT of Delhi

Dr. RAJESH VERMA
Forensic Science Laboratory
Mandi

JOHN PATRICK MOLONEY
Forensic Comparison Software, Gr. Melbourne

IASR Advisory Board

Dr. G. S. SODHI
Forensic Science Unit, S.G.T.B. Khalsa College, DU, New Delhi

Dr. RUKMANI KRISHNAMURTHY
Helik Advisory Ltd., Academic Council Member, NFSU, Gujarat

Dr. SELINA LEOW
NSW Dept. of Oral Health, Westmead Centre for Oral Health

Dr. JOSEPH De LADURANTEY
The Vollmer Institute California

Dr. MADHULIKA SHARMA
(Former) Forensic Science Laboratory, NCT of Delhi

Dr. S. L. VAYA
Pioneer of Forensic Psychology In India

Dr. MUKESH YADAV
Government Allopathic Medical College, Banda

Prof. JASON PAYNE JAMES
William Harvey Research Institute, London

STEVEN DAVID LAMPLEY
The Oliphant Institute of Forensics, USA

RAKSHIT TANDON
Hackdev Technology Pvt. Ltd. Noida

Dr. V. V. PILLAY
Amrita Institute of Medical Sciences & Research Center, Kerela

Prof. TEJ BAHADUR SINGH
Centre for Psychological Sciences, Central University of South Bihar, Gaya

Dr. DANILO L. MAGTANONG
College of Dentistry, University of the Philippines, Manila

Sh. NILENDU BIKASH BARDHAN
(Former Director) CFSL, CBI, New Delhi

DINESH O BAREJA
Open Security Alliance India Watch, Mumbai

Dr. GHYASUDDIN KHAN
U.P. State Medico Legal Cell Lucknow

Dr. SAMEERA AL HAMMADI
Dept. Forensic Medicine & Pathology Justice Dept., Emirate, Abu Dhabi

Dr. ASHA SRIVASTAVA
Forensic Psychology, CFSL, CBI, New Delhi

SANTOSH KHADSARE
Cyber Security Professional Senior Cyber Forensic Expert

NA VIJAYASHANKAR
Foundation of Data Protection Professionals in India, Karnataka

IASR Advisory Board

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

OMVEER SINGH
Ministry of Electronics & Information Technology, New Delhi

Dr. EVI UNTORO
Faculty of Medicine, University of Trisakti, Indonesia

CLOYD STEIGER
Author & The American Investigative Society of Cold Cases, Washington

Al-SHARIF HASHEM MOGAHED
Forensic Medicine Administration, Ministry of Justice, Egypt

Dr. KAVITA SHARMA
Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore

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

Dr. AJAY SHARMA
State Forensic Science Laboratory, Jaipur

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

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

Dr. MOHAMMED NASIMUL ISLAM
Faculty of Medicine, Universiti Teknologi MARA (UiTM), Malaysia

KEVIN M. SULLIVAN
Author, USA

RAJ SHRIVASTAVA
Forensic Science Laboratory Sagar

Dr. SHUBHRA SANYAL
Counsellor (OHBII) Sewa Kuthir, New Delhi, Former Senior Reader (NICFS)

SHANE TURNIDGE
SST Forensics, Canada

ARUN SHARMA
State Forensic Science Laboratory Lucknow

Dr. GAURAV GUPTA
Ministry of Electronics & Information Technology, New Delhi

Prof. (Dr.) RAAKESH KRIPLANI
RK Psychotherapy, CIIPS Nagpur

Dr. CHANDNI SRINIVASAN
Psychotherapist & Counsellor Chennai

Dr. SONI KEWALRAMANI
Amity University, Uttar Pradesh Lucknow Campus

IASR Advisory Board

SAMIR DATT
Fellow - Indian Police Foundation

PRINCE BOONLIA
Digital 4n6 Journal
Udaipur

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

Dr. BHARATI MEHTA
Psychology Gym & CosmeClinic
Pune

AASHISH SUTAR
Ministry of Defence, Govt. of India
New Delhi

HEMANTA KUMAR PANDA
Retd. Fingerprint Expert
Bhubaneswar

Dr. AMAR JYOTI PATOWARY
Dept. Forensic Medicine & Toxicology, NEIGRIHMS, Shillong

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

Dr. SHALINI GUPTA
King George's Medical University
Lucknow

MOHAMMED ABO ELAZM
Alexandria Head of Forensic Evidence, Egypt

IASR 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

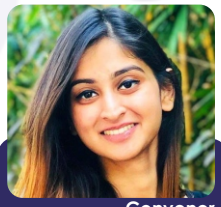
Convenor
Afreen Tarannum
SIFS India

Convenor
Kratika Mishra
SIFS India

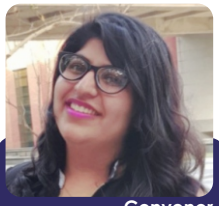
Convenor
Arti Varshney
SIFS India

Convenor
Saumya Solanki
SIFS India

Convenor
Preeti Kiran
SIFS India



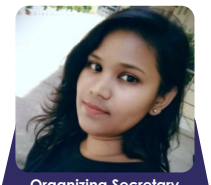
Convenor
Ashi Yadav
SIFS India



Convenor
Vanshika
SIFS India

Treasurer
Thomas T.O.
SIFS India

Organizing Secretary
Madhuri Vagal



Organizing Secretary
Pratima Kumari

Organizing Secretary
Swetang Patel

Organizing Secretary
Ruchika Dwivedi

IASR 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

IASR Scientific Committee

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

ARVIND SUD
Senior Forensic Expert Hoshiarpur

Prof. 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, MMIMSR 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

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

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

Dr. INDERJIT SINGH
Senior Forensic Expert, Patiala

VIJAY RUSTAGI
Senior Forensic Expert, Gurugram

Dr. ADITYA SHARMA
Dept. of Forensic Medicine, IGM College Shimla

E. SAI PRASAD CHUNDURU
CFSL Hyderabad, DFSS, MHA, Govt. of India

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

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

Dr. NARESH KUMAR
Forensic Science Laboratory, Delhi

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

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

Dr. SHALOO MALIK
Regional Forensic Science Lab., Jodhpur

Dr. ARUNA MISHRA
Forensic Science Laboratory, New Delhi

Dr. RAKHI KHANNA
State Forensic Science Laboratory, Jaipur

IASR Scientific Committee

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

Dr. PRATEEK RASTOGI
Dept. Forensic Medicine & Toxicology, Kasturba Medical College, Mangalore

Dr. VINDRESH MISHRA
CFSL, Kolkata DFSS, MHA Govt. of India

SANJEEV Kr. GUPTA
Forensic Science Laboratory, New Delhi

Dr. CARLOS A. GUTIERREZ
True Forensic Science United States

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

ANDREW REITNAUER
Delta Forensics, LLC, United States

Dr. KRITHIKA RAJESH
Forensic Science Laboratory, Ahmedabad

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

Dr. RAJIV PANDEY
AIIT, Amity University, Lucknow

Dr. POOJA RASTOGI
SMS&R, Sharda University, Greater Noida

Dr. RAJNISH KUMAR SINGH
Forensic Science Laboratory, New Delhi

NARENDRA KUMAR
Forensic Science Laboratory,U.P.

Dr. PREETI SINGH
National Post Graduate Autonomous College Lucknow

AMIR LIBERMAN
Nemesysco Limited, Israel

VIJAY VERMA
Central Forensic Science Laboratory,CBI, New Delhi

Dr. SWATI SHRIVASTAVA
State Forensic Science Laboratory, MP

Dr. PARDEEP SINGH
Pt. Jawahar Lal Nehru Govt. Medical College and Hospital, Chamba

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

ABY JOSEPH
Amity University, Dubai

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

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

Dr.REENA SHARMA
The Mind Practice, Ahmedabad

Dr. GUNVANTI B. RATHOD
Pathology & Lab Medicine Department, AIIMS, Bibinagar

Dr. CRISTIANA PALMELA PEREIRA
University of Lisbon, Portugal

Dr. UTSAV PAREKH
Dept. of Forensic Medicine & Toxicology, PS Medical College, Karamsad

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

Dr. POOJA PURI
Amity Institute of Forensic Sciences, Amity University Noida

IASR Scientific Committee

Dr. VIVEK SAHAJPAL
State Forensic Science Laboratory, Shimla

Dr. PRIYANKA KACKER
School of Behavioral Science of NFSU, Gandhinagar

Dr. AMAR PAL SINGH SHOKEEN
Forensic Science Laboratory, Delhi

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

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

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

NEERAJ KUMAR VARSHNEY
Forensic Science Laboratory, Patna

NILESH B. WAGH
Central Forensic Science Laboratory, CBI, Navi Mumbai

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

Dr. PRAVEEN JHA
State Forensic Science Laboratory, Sagar

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

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

Dr. ALOK PANDYA
Institute of Advanced Research, Gandhinagar

Dr. JIJU PV
CFSL Pune, DFSS, MHA, Govt. of India

Dr. NEERAJ TANEJA
Mobico Comodo Pvt Ltd. Gurugram

Dr. PRATEEK PANDYA
Amity Institute of Forensic Sciences, Amity University Noida

Dr. RAJESH SINGH YADAV
Dept. of Criminology & Forensic Science, Dr. Harisingh Gour Vishwavidyalaya, Sagar

Dr. PUNEET SETIA
Dept. of Forensic Medicine & Toxicology, AIIMS, Jodhpur

RAJVEER
State Forensic Science Laboratory, Jaipur

MOHAMMED AL SUWAIDI
Fingerprint Expert Dubai Police, UAE

Dr. BINAYA KUMAR BASTIA
Dept. of Forensic Medicine & Toxicology, AIIMS, Rishikesh

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

DURGA PRASAD GANGWAR
CFSL Chandigarh, DFSS, MHA, Govt. of India

Dr. AMAN CHOWDHRY
Faculty of Dentistry, Jamia Millia Islamia, New Delhi

Dr. LALIT PRATAP CHANDRAVANSHI
CTM, IRTE, Faridabad

Dr. PRADEEP JAIN
State Forensic Science Laboratory, Jaipur

Dr. PRASHANT AGRAWAL
School of Allied Health Sciences, Sharda University, Greater Noida

R. SURESH
CFSL Assam, DFSS, MHA, Govt. of India

IASR Scientific Committee

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

HANAN AHMAD ALMULLA
Forensic DNA Expert, Police HQ, Dubai

V.B. KASHYAP
Fingerprint Expert, Haryana

Dr. ILA GAUTAM
Forensic Science Laboratory, Sagar

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

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

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

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

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

PRASHANT SHARMA
Central Forensic Science Laboratory, CBI, New Delhi

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

Dr. DOMINGO MAGLIOCCA
Judicial Police Section Italy

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

PAWAN DESAI
MitKat Advisory Services Pvt. Ltd, Gurugram

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

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

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

IASR Scientific Committee

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

Dr. RAJEEV JAIN
CFSL Chandigarh, DFSS, MHA, Govt. of India

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. MANAVPREET KAUR
Wikimedia Foundation, USA

KALPESH SOLANKI
SFSRM, Rashtriya Raksha University, Gujarat

RAKHI R. WADHWANI
Senior Assessor Mumbai

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

Dr. MADHUSUDAN ASTEKAR
Institute of Dental Sciences, Bareilly International University Bareilly

Dr. MALVIKA MEHTA
National Centre for Handwriting Studies Pune

SAILAJA VADLAMUDI
SAP Labs India Bengaluru

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

RITESH BHATIA
Founder, V4WEB Cybersecurity, Mumbai

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

MAHESH 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. NEEHARIKA SRIVASTAVA
G.D. Goenka University, Gurgaon

ANNA BARBARO PhD
Worldwide Association of Women Forensic Experts, Italy

Dr. YMELDA WENDY VELEZMORA MONTES
Instit. Legal Medicine & Forensic Sciences, SPOLFOC, Peru

Dr. POONAM SINGH
Regional Forensic Science Laboratory, Bhopal

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

Dr. MOHINEESH CHANDRA
Forensic Science Laboratory, New Delhi

IASR Scientific Committee

Dr. PARUL KHARE SINHA
Alpha Dental Clinic, Shanghai

Dr. HIMAKSHI BHARDWAJ
Forensic Science Laboratory, New Delhi

AMRIT CHHETRI
Digital Forensics Analyst, Cyber Security Evangelist, DFIR Researcher (Edge AI & QML), Siliguri, (West Bengal)

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

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

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. UTTARA DESHPANDE
DentoUpanishad Dental Clinic & Implant Center, Pune

Dr. KUSUM SINGAL
PGIMER, Chandigarh

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

Dr. RISHA JASMINE NATHAN
School of Basic & Applied Sciences, Galgotias University, Gr. Noida

KAPIL DEV
Forensic Science Laboratory, Moradabad

MAJID KHAN
Forensic Science Laboratory, Muzzafarpur

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

MAYANK KR. DUBEY
Mody University, Rajasthan

Dr. SUDEENDRA PRABHU
Centre for Foresnic Odontology, Yenepoya Dental College, Mangalore

Dr. SOWJANYA VASISTA
Abyaas Educare Pvt. Ltd., Bengaluru

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

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

Dr. KAVERI CHAUHAN
MindSpark PsycCare, Training and Development Karnal

Dr. SHIVANI BANSAL
Nair Hospital Dental College, Maharashtra

SHYAM CHANDEL
Cyber Fraud Helpline, Udaipur

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

Dr. JASKARAN SINGH
Dept. of Forensic Science, Sharda University, Greater Noida

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

Dr. MANOJ KUMAR VERMA
Chemistry Division, Forensic Science Lab., Lucknow

IASR Scientific Committee

PALLAVI MALIK CHOPRA
Forensic Science Laboratory, Mohali

VINNY SHARMA
Div. 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

PRACHI KATHANE
SFSRM, Rashtriya Raksha University, Gujarat

MELBA KURIAKOSE
Impress.ai, Kochi

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

KRUPA NISHAR
School of Forensic Psychology, National Forensic Sciences University, Gujarat

SUBHASISH SAHOO
Forensic Science Laboratory, Odisha

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

SUCHISMEETA BEHERA
Forensic Science Laboratory, Odisha

Dr. RUCHI SHARMA
Forensic Science Laboratory, Delhi

DEEPAK KUMAR
Digital Forensics & Cyber Intelligence, India

NOUZIA NOORDEEN
SAFI Institute of Advanced Study, SAFI College, Kerela

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

NIDHI PANDYA
Dept. of Forensic Science Gujarat University Ahmedabad

GEORGE DIXON
Jamaica Constabulary Force, Jamaica

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

SHIFA CYCLEWALA
Hacktify Cyber Security, Mumbai

ROHIT GAUTAM
Hacktify Cyber Security, Mumbai

SHUBHAM GAUTAM
Psyberbull Pvt. Ltd. Delhi

SUDHANSHU SHEKHER TIWARI
SFSRM, Rashtriya Raksha University, Gujarat

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

MANASHREE MANE
Jain (Deemed-to-be-University) Bangalore

SRI RAM
PrimeFort Pvt. Ltd., India

NAVEEN PAL
Capgemini India

IASR Scientific Committee

NIRALI BHATIA
V4WEB Cyber Security & Cyber B.A.A.P, Mumbai

GOPIKA BAGHEL
Forensic Science Education Society, Raipur

DEEP SHANKAR YADAV
eSec Forte Technologies, Gurugram

SANTOSH CHALUVADI
Supraja Technologies, Andhra Pradesh

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

DAVINDER SINGH
Cylos Consulting Private Limited, New Delhi

GAURAV SHARMA
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

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 November 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

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

11th INTERNATIONAL eCONFERENCE-2021

Cyber Security

Supported by

Sherlock Institute of Forensic Science India

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 November 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

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

11th INTERNATIONAL eCONFERENCE-2021

Cyber Security

Supported by

Sherlock Institute of Forensic Science India

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

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

11th INTERNATIONAL eCONFERENCE-2021

Cyber Security

Supported by

Sherlock Institute of Forensic Science India

Registration Details

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

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 November 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

www.facebook.com/iasrorg

www.linkedin.com/in/iasrorg/

www.instagram.com/Forensicscienceinstitue

Email : iasrforensicconference@gmail.com

Contact : +91-98188-77002

Website : www.forensicevents.com

linktr.ee/forensicscienceinstitue

11th INTERNATIONAL eCONFERENCE-2021

Cyber Security

Supported by

Sherlock Institute of Forensic Science India

TABLE OF CONTENT

Paper Category

ePoster Category

ePoster Code	Author and Co-author	Title
EP 01	**Saurabh Kumar**	*Cyberbullying*
EP 02	**Ruchika Dwivedi**	*Bring Your Own Device*
EP 03	**Janki Nitin Gavandalkar**	*Cyber Security Awareness*
EP 04	**Dr. Monika Goyal Dr. Shrabana Kumar Naik**	*Medico-Legal Importance Of Skin And Its Role In Cyber Security*
EP 05	**Arti Varshney**	*Social Media Network: Jeopardizing Privacy and Security*
EP 06	**Vandana Ravat**	*Cyber Criminals And Their Targets*
EP 07	**Aarti Rajapurkar**	*Cyber Defamation Under The Preview Of The Current Statutory Provisions*
EP 08	**Shivangi Gupta**	*Cyberbullying Through Videogaming*
EP 09	**Tanu Sindhvani**	*Causes Of Cyber Crime*
EP 10	**Aastha Mahna**	*Hackers & Public WI-FI*
EP 11	**Surbhi Kawatra**	*Cyber Bullying And Its Various Impacts*
EP 12	**Mansi Seewal**	*Cyberstalking: A Bane Arising With The Progressing Technology*

EP 13	**Anuraj Khandelwal**	*India's New National Cyber Security Strategy*
EP 14	**Sumit Kumar**	*Phishing Attacks And How To Protect Yourself From Phishing Attack*

Paper Presentations

ALARMING THREAT OF CYBER CRIMES AND NEED FOR CYBER HYGIENE AMID COVID-19 PANDEMIC

Dr. Atul S. Jaybhaye[1]

[1]Assistant Professor (Law) & Warden (Boys Hostel), Hidayatullah National Law University

Atal Nagar, Raipur, Chhattisgarh,

Abstract

The entire world was fighting to overcome and spreading of COVID- 19 pandemic and on the other hand, cyber criminals started taking undue advantage of helplessness of public and deceived countless netizens by adopting newest trends and techniques of cyber-attacks. The enormous threat of COVID-19 pandemic compelled India as well to impose lockdown during March 2020 as a preventive measure to fight against corona virus. The impact of the lockdown resulted in massive use of technology and internet for netizens due to which victimisation of cyber frauds also increased automatically. Phishing attack, Hacking, ATM Skimmer Fraud, Ransomware attack, Denial of service attack, Sim swap fraud, QR Code fraud on OLX, Data Breaches, Dissemination of fake news, Cloning of Social media accounts, Cloning of Govt websites and fingerprints, Cyber bullying, Pegasus software controversy, Juice jacking are few examples of cyber-attacks which took place worldwide. Most of the netizens are unaware about the cyber hygiene and netiquettes which has to be strictly followed while browsing or carrying out online transactions in cyberspace. There is a high need to sensitise general public about emerging cyber-crimes in the digital age and appropriate preventive measures to combat with the same.

Keywords: Covid-19 pandemic, Cyber Crimes, Phishing, Dissemination of fake news, Cyber hygiene.

CYBER INVESTIGATION USING INTERNET PROTOCOL DETAIL RECORD (IPDR)

Vikas Razdan[1]

Abstract

Cyber Criminals are increasingly using virtual platform and mobile based communication applications having end-to-end encryption to connect to each other. This makes traditional analysis of call graphs or traffic analysis virtually impossible and so is a hindrance for law enforcement agencies. Governments in various countries have expressed concerns that not only the use of encrypted messaging services but also web based services including VPN's over the virtual platforms can be a threat to national security as it can be used by terrorists and other criminals to harm the society. Internet Protocol Detail Record (IPDR) plays a vital role in Cyber Investigation, as it provides information about Internet Protocol (IP)-based service usage. IPDR provides superior network intelligence that can be applied to tasks such as monitoring subscriber usage. IPDR datasets helps to generate a profile of the mobile user as it helps to track details of a telecommunication call or message generated by a phone device. These logs contain metadata that describe details of a specific call, like calling phone number, destination port, start date/time, end date/time etc. IPDR analysis also provides information such as which websites and social media used by the suspect committing cybercrime. An IPDR is composed of multiple fields. Examples of fields include Landline/MSISDN for Internet Access (calling party), Source IP Address (calling party IP Address), Source Port (calling party Port), Public IP Address, Public IP Port, Destination IP Address, Destination Port, Start Date & Time of IP allocation (date and time), End Date & Time of IP allocation (date and time), Static/Dynamic IP Address Allocation, IMEI (International Mobile Equipment Identity) , IMSI (International Mobile Subscriber Identity), Cell ID IPDR consists of logs of potential criminals being tracked by the law enforcement agencies. It correlates the IPDR'S of the suspects who are using the same service at the same time, and potentially assuming that they are connected to each other helps the cyber investigators to reach to any conclusion that can help the investigating agencies in analyzing the logs containing metadata to help in knowing the platforms/services/mobile based applications used.

Keywords: IPDR, Cyber Criminals, Virtual Platform, Cyber Investigation, Metadata,

CORRELATION BETWEEN INTERNET USE, AGGRESSION AND PROBLEMATIC PORNOGRAPHY CONSUMPTION AMONG INDIAN COLLEGE STUDENTS

Abel Anil Thomas[1]

[1]National Forensic Sciences University

Abstract

The study aimed to find out the contribution of internet use in daily life to deviancy among college students in India. The deviancy being focused in the study is problematic pornographic consumption and aggression. The results are meant to throw light on the fact that the internet, something our lives revolve around, has its adverse effects on the human psyche and the possibility that using the internet on a regular basis might cause individuals to behave more aggressively than usual or indulge in possible problematic pornography consumption. The objectives of the study were to assess the severity of Internet Use, Aggression and Problematic Pornography Consumption and to further find out the correlation between Internet Use and Aggression, Internet Use and Problematic Pornography Consumption and between Aggression and Problematic Pornography Consumption. We further find out and compare the differences in the mean scores for each variable between the male (N=59) and female (N=56) participants out of the total 115 participants. No statistically significant correlation was found between Internet Use and Aggression or between Internet Use and Problematic Pornography Consumption. However a mildly significant ($p \leq 0.05$) positive correlation was found between Aggression and Problematic Pornography Consumption and furthermore a moderately significant ($p \leq 0.01$) positive correlation was found between Physical Aggression (Subscale of Aggression) and Salience, Tolerance and Withdrawal (Subscales of Problematic Pornography Consumption). There was no statistically significant difference in the mean Internet Use and Problematic Pornography Consumption scores among the male and female participants although males scored, on average, 8 points more than females on the Buss-Perry Aggression Scale.

Keywords: Internet Use, Aggression, Problematic Pornography Consumption.

IDENTITY THEFT ON THE INTERNET AND ITS DIFFERENT CONSEQUENCES

Aneeta Jaison[1]

[1]Adikavi Nannaya University, Andhra Pradesh

Abstract

Identity theft is often perceived as major upcoming threats in crime. Even normal browsing activities like clicking on an enticing ad or filling out a for downloadable content can lead to online Identity theft when users don't know what to do for Key loggers can be overlaid on seemingly legitimate banking or investment programmers, and intrusive tracking methods can be turned off. Obtaining data or applications via download, clicking on pop-ups o opening email attachments, going to shady websites .When a thief steals someone else's personal information and passes it off as its own , he creates a new identity for that individual. Cyber criminals uses our personal information for unlawful or illegal purposes. Once the hacker who installed spyware on our computer has your personal information, they can steel money and open credit card and bank account in our name, it will be sold to others who would utilize it for nefarious an unlawful purpose. Identity theft is not something that happens by chance. Cyber criminals employ strategic cyber assault strategies that focus on social engineering to persuade victims to provide personal information that they should not share with strangers. When a cybercriminal uses our personal information for any kind of abuse like blackmailing, fake social media relationship from that financial dealings and those will be based on our personal information; as social media becomes increasingly integrated into daily life, identity theft on the platform is becoming more common. Simple error can lead to the theft of our social security number, as well as damage to your credits. This study focus on various theft using our personal identity and consequences of identity theft and also about prevention of identical theft and also how it affect in different category of people in different ways and the goal of designing this poster is to raise an awareness about identity theft among people who use the internet frequently.

Keywords: Identity Theft, Online Identity Theft, Detection of Online Theft, Prevention of Online Theft, Key Loggers.

SYNOPSIS ON RANSOMWARE

Manubhav Sharma[1]

[1]B.Tech, 2nd year, SRM Institute of Science and Technology

Abstract

Ransomware is one the leading threats facing organizations today. With volumes of malicious inbound emails and already infected devices within your environment, regaining control over ransomware can be tedious and time consuming. Some Prevention Tips For An Organization: Every computer connected to the organization's network, security updates of the operating system, and/or application software, must be kept current (patched and updated). Firewall software shall be installed to aid in the prevention of malicious code attacks/infections. Email attachments and shared files of unknown integrity shall be scanned and send to sandbox for malicious code before they are opened or accessed. Storage devices should be scanned for malicious code before accessing any data on the media. Always keep a hard copy of backup data at some other center/place. What If You Are Attacked? How To Response and Recover You're Data - Gather the incident response team. Make sure IT staff, management, PR and legal teams are aware of the issue and ready to tackle their roles in the response efforts, Disconnect/Isolate the infected system from outside world i.e network to prevent further possible propagation of the malicious code or other harmful impact, Any removable writeable media recently used on an infected machine shall be scanned prior to opening and/or executing any files contained therein, Perform a thorough investigation. Try to identify which ransomware strain has been used, its potential risks and recovery options. Some ransomware varieties use weak encryption that has a publicly available decryption mechanism provided by a security vendor or researcher, Eradicate malware, and recover from the incident. This involves wiping infected systems and restoring lost data from backups. Be sure to change all account, network and system passwords after removing a device or system from the network. Change passwords again once the malware is removed completely from the network. Some Tools/Techniques/Tips: Go to www.nomoreransom.org to check whether the decryptor of your ransomware is present in their database. If yes, download and run it on the infected system. The No More Ransom initiative, a partnership between law enforcement and IT security companies, aims to help ransomware victims recover files where plausible. Do a full network and system scan at regular intervals? Most Important Tip is to always keep a hard copy of backup data at some other center/place. What Experts Are Doing Wrong? Experts after facing a ransomware attack don't perform analysis and learn from the attack. During this step, organizations can discover and analyze why the attack happened and apply appropriate actions to ensure the same vulnerability is not compromised in the future. But a lot of organizations ignore this step and try to move on with their previous vulnerable security implementations and policies. For example, if the ransomware was the result of an employee clicking a malicious link, the company should perform additional security awareness training. Organizations should revise security policies if necessary. Security teams should also analyze how the ransomware incident response plan performed. If certain steps did not go as planned, review the plan, and update where needed to improve efficiency.

Keywords: Ransomware, Firewall software, Encryption, Malware, Malicious.

THE EMERGENCY ACTIONS AFTER HACKING

Denita.V[1]

[1]GIET Degree College, Andhra Pradesh

Abstract

The importance of the internet and social media to our everyday lives and to the growth of a company or business now indicate that we need to take cyber security more seriously, especially since hacking is now becoming more prominent on the internet. Today businesses are facing the biggest threats from hackers. Any successful computer hacking attack can create a disaster to networks and important secret information stored in the various computer within the network. IT sector demands professional having ethical hacking skills to work for them and provide security to their computers and networks. White hat hackers or ethical hackers, the professionals are expert in the area of anti-hacking techniques. They work for preventing the motives of malevolent hackers from stealing or damaging important data and ensure the safety and protection of computer systems and networks. Situation where top secret information, plans of companies are suddenly found in public domain, information concerning national security falls in wrong hands or someone unauthorized accesses and takes control of a bank's customer data, a greedy BPO worker decides to draw off customer data for financial satisfaction. These are real-life cases, which happens regularly and feature as newspaper headlines. One of the greatest threats to corporate information system lies within the network. People are often the weakest links in the security chain. Hacking is the serious issue to be taken care of by the government, private sector with legislations.

Keywords: Hacking, Cybersecurity, Attack, Malevolent Hacking, Network, Unauthorized Accesses, BPO, Legislation.

AWARENESS OF CREDIT CARD FRAUDS

Christy Susan Thomson[1]

[1]Government Institute of Forensic Science

Abstract

Credit cards are an essential financial tool that helps the holder to make payment transaction. It is issued to the holder by the banks and financial institutions for the easy usage of short-term financial needs. The two types of credit cards are consumer credit cards and business credit cards. The composition of the cards may differ like plastic cards, metals (stainless steel, gold, platinum) cards or even gemstone metal cards. The card will have the name of the owner, logo of the company, card number, expiration date, EMV chips and contactless chip.
The purpose of this paper is to create awareness to the credit card users about the frauds encountered with the credit cards. The types of credit card frauds include false application frauds, lost or stolen frauds, email scams, trapping, operational frauds, account takeover etc. Credit card fraud is the most growing types of fraud in the developing countries. According to the recent reports, the United States has the highest peak being victim to credit card frauds. Credit card fraud affects consumer, merchants and the issuer alike. Credit card frauds usually occurs either due to card owner's negligence or violation in a website's security. There are different key measures used for detecting and preventing the credit card frauds. These techniques includes Address Verification Service (AVS), Credit Verification Values (CVV), negative databases, fraud rates, relocation, 3-D secure, chip and pin, biometrics etc. For the detection of payment frauds using credit cards it is necessary to obtain the sufficient amount of structured, unbiased and quality historical data. The fraud can be detected with the help of set of activities followed by systematic investigation. The most common kind of credit card fraud detection is with Machine Learning. This technique gives accurate results and information regarding the transactions, date, user zone, amount etc. Credit card frauds can be prevented by keeping credit cards on safe location, avoid sharing card information to unknown persons, using credit cards safely on the Internet and checking for inconsistent charges or transactions.

Keywords: Credit Card, Frauds Related To Credit Cards, Detection Of Frauds, Detection Using ML, Prevention Of Frauds.

SOCIAL ENGINEERING

Anushka Tiwari[1], Sharon Jolly[2]

[1]Department of Engineering and Technology, Amity University Noida, UP

[2]Department of Computer Science and Technology, Rajagiri School of Engineering and Technology Kochi, Kerala

Abstract

In the recent global pandemic, there was an 11.8% rise in cybercrime as reported by NCB in the year 2020. The basis of most of these crimes was social engineering. Social engineering includes manipulating people into giving their personal details, it's used to lure users into giving out their personal data, spreading malware infections, and giving access to restricted systems. In today's technologically advanced world, data privacy and protection are very important. Now, there is a hefty amount of software to protect the information stored in the devices, but what about the information stored in the human brain? Can it be hacked? The answer is yes! With the rapid growth and use of social networking sites, it has become very easy to dig out the personal and sensitive information of the users, indirectly or directly. Such social engineering attacks are increasing day by day due to a lack of awareness and proper knowledge. In this paper, we will discuss the different ways in which a hacker collects bits of personal information from a human being and use it for their own benefits and also the psychology used behind it. Emphasis is placed on the study of social engineering techniques in the system of human-machine interaction used to implement the illegal (malicious) manipulation of human behavior patterns. We will also analyze a survey and try to find out the main reason people easily give out personal information. The actual major threat occurs when social engineering is paired with other different types of attacks like phishing. We will also discuss the direct and indirect attacks of social engineering and also the defense mechanism for these attacks. These defense mechanisms include spreading awareness among users and installing antivirus software, we will discuss these in detail in the paper.

Keywords: NCB, Crimes, Social Engineering, Phishing, a Defense Mechanism.

PREVENTION OF ONLINE TRANSACTION FRAUDS USING OTP

Femina.S.P[1]

[1]Bharathiyar University, Coimbatore, Tamil Nadu

Abstract

The OTP (One Time Password) also known as one time pin, is valid for only one transaction. The criminals trying to steal money from your bank account through online transaction. There has been a large number of cases in which criminals duped bank customers into revealing OTP or accessed it by hacking the smartphone. With the developing technology online shopping of goods and various other products has increased to a great extent. With this service people tend to use their debit cards and credit cards for the online payment and this has been a common practice. The purpose of this paper is to say how we can prevent the OTP frauds. The types of OTP fraud include COVID fraud, digital wallet scam**,** fraud on used product selling apps, phishing or email scams, credit card reward point fraud, unverified mobile apps, UPI fraud etc. Security is provided by the generation of OTP (One Time Password) providing a dual layer security mechanism which includes cookie based OTP generation and location based OTP generation. The key points of OTP generation, cookies, location parameters, dual layer security mechanism have been discussed in this paper considering user satisfaction and comfort with implementing the best possible security measures. The precaution for OTP frauds include never disclose your OTP and PIN to any person. No bank or other institution will ask for credentials like OTP, PIN, CVV number or other credentials. The preventive measures for OTP fraud, you must not share your OTPs over the phone banks or any service provider never ask for your passwords or OTPs. App pin, UPI pin, CVV number, expiry date of debit card and 16 digit debit card is for personal use.

Keywords: OTP frauds, Online Shopping, Cookies, Types, Security, Online Fraud, Transaction Frauds, Precaution, Prevention.

VISHING: THE CALL OF DECEPTION

Anirudhvaibhav Gupta[1]

[1]B.Sc. (H) Forensic Science, Second Year (Batch 2019-22)

Amity University, Noida Uttar Pradesh

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, for many people, having access to this information is no longer just an advantage, it is essential. Connecting a private network to the Internet can expose critical or confidential data to malicious attack from anywhere in the world. This paper will discuss about an emerging threat which is the combination of social engineering and technology. This paper gives a brief information about the term voice phishing what exactly it is, describes the modus operandi that is used by these fraudsters nowadays. Voice Phishing also known as vishing is a type of cyber fraud in which a fraudster uses social engineering techniques to steal the personal and sensitive information of a person over telephone lines. Vishing frequently involves a criminal who masquerade as a trusted institution, company, bank official, or government agency. You may be asked to buy an extended warranty, offered a "free" vacation or a lottery, or they may tell you that your credit card is expired or in locked stated and asked you to confirm your personal detail. As the security threats are constantly evolving, and wearing new shapes to avoid detection, the cyber securities must evolve to avoid such attacks. An increased awareness about these attacks will provide an effective means for overcoming the security issues. We need to continue to raise awareness for these lurking threats, and ensure that our peers, colleagues, friends, and family understand the risks and avoid sharing their sensitive information.

Keywords: Vishing, Social engineering, Cyber fraud, Modus operandi, Cyber security.

ePoster Presentations

CYBERBULLYING

Saurabh Kumar[1]

[1]Master of Science in Chemistry, Mahatma Gandhi Kashi Vidyapith, Varanasi, Uttar Pradesh

Abstract

Cyberbullying is a bullying with the use of digital technologies. It can take place on social media, messaging platforms (such as text messages, WhatsApp, Facebook etc.) through mobile phones and other devices. It is a repeated-behaviours, aimed at scaring, angering, shaming or humiliating those who are targeted. Spreading lies about or posting embarrassing photos of someone on social media, Sending hurtful messages or threats via messaging platforms, impersonating someone and sending mean messages to others on their behalf. Face-to-face bullying and cyberbullying can often happen alongside each other. But cyberbullying leaves a digital footprint. A record that can prove useful and provide evidence to help stop the abuse (verbal and non-verbal). Case Study: Vishaka & Ors. Vs the state of Rajasthan & Ors. (1997) - Cyberbullying was the first time dealt as an issue by the supreme court of India in the landmark case of Vishaka vs the State of Rajasthan. In this while dealing with the issue of bullying guidelines to protect women from sexual harassment was laid down by the Supreme Court. Cyberbullying can harm the online reputations of everyone involved- not just the person being bullied but those doing bullying or participating it. The case study's abstract should mention the relevant facts and other major landmark judgments or opinions to be presented to the audience. Action: Superseded by the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 (known as "SEXUAL HARRASMENT ACT")

Keywords: Cyberbullying, Harassment, Digital technology, Supreme Court.

BRING YOUR OWN DEVICE

Ruchika Dwivedi[1]

[1]SIFS, India

Abstract

Using modern technologies such as smartphones and tablets has many benefits, which has made them increasingly popular as consumer devices in private life. It is also common to use them at work. Who, on the other hand, wants to carry and manage two devices: one for personal usage and the other for work-related tasks? As a result, & dual use, & or using a single device for both personal and professional purposes, may be a viable option. As a result, & Bring Your Own Device, & or BYOD, has emerged as a term to characterise the situation in which employees make their personal gadgets available for corporate usage. This presents both opportunities and threats for businesses. This poster presentation will discuss the beneficial use of Bring Your Own Device Policy in Organizational and well as educational purpose along with the related risk, Challenges and their solution are also described and discussed.

Keywords: BYOD, BYOT, Challenges Device. Technology, Educational, Organizational, Policy,

CYBER SECURITY AWARENESS

Janki Nitin Gavandalkar[1]

[1]MBA Education Management Alagappa University, Tamil Nadu

Cyber Law Mumbai University, Maharashtra

Abstract

Cyber security plays an important role in the field of information technology. Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that to come to our mind is "cybercrimes". Which are increasing immensely day by day.Various Government & Companies are taking many measures in order to prevent these cybercrimes. Besides various measures cyber security is still a very big concern to many.These paper mainly focus on challenges faced by cyber security on the latest technologies. It also focuses on latest about the security techniques ethic and the trends the changing the face of the cyber security.

Keywords: Cyber Security, Cyber Crime, Cyber Ethics, Social Media, Cloud Computing, Android Apps.

MEDICO-LEGAL IMPORTANCE OF SKIN AND ITS ROLE IN CYBER SECURITY

Dr. Monika Goyal [1], Dr. Shrabana Kumar Naik[2]

[1]Junior Resident, Department of Forensic Medicine,
Lady Hardinge Medical College & Associated Hospitals, New Delhi

[2]Director Professor, Department of Forensic Medicine,
Lady Hardinge Medical College & Associated Hospitals, New Delhi

Abstract

Skin is the largest organ of human body'. 'Beauty is only skin deep'. Every dermatologist feels proud of the above statements. Scientifically, skin is the main barrier and protector of human body from invisible micro-organisms. Even hand hygiene has been ascribed as a tool to fight against the ongoing pandemic Covid-19. Skin forms the sole basis of identification of individual as well as racial discrimination. It is well known that every part of the human body has its own medico-legal importance. Medico-legal significance of some of the human structures / parts like that of hairs, teeth, bones etc. have been described in detail in most of forensic medicine text books by various authors. As a lot of medico-legal information can be gathered from examination of any single part or organ of the human body, the present authors have made an attempt to highlight the medico-legal importance of skin in detail to widen the thought while conducting medico-legal examination of any part of human body from top of the head to tips of the toes. The usefulness of skin in relation to different chapters in Forensic Medicine and Toxicology, starting from identification of the individual up to clinical diagnosis of poisoning is discussed. Recognition of skin (finger print) has become a functionality standard in all modern devices like smart phones, tablets laptops for better cyber security. In most organisations, fingerprint has now almost replaced passwords, ID cards and door entry codes having advantages like improvement in security, ease of use, non-transferable, accountability and cost effective security solution. Thus role of skin in cyber security is also discussed.

Keywords: Skin; Forensic Medicine, Toxicology, Medico-legal Importance, Fingerprint, Cyber Security.

SOCIAL MEDIA NETWORK: JEOPARDIZING PRIVACY AND SECURITY

Arti Varshney[1]

[1]SIFS, India

Abstract

Social media network has allowed us to connect around the world. In these virtual worlds, individuals interact with each other both socially and professionally. Though, social media has given a new avenue of communication for millions of people but, it also tricks our privacy by handing over sensitive information, stealing personal data. The information posted on social media sites can lead to security risks such as identity theft, online stalking, and cyber harassment. One type of serious privacy violation that occurs in social networks involves photos. A conscientious user might have placed appropriate controls on his/her settings concerning the ability to view photos posted on his/her wall. When a friend posts a photo on his/her wall without putting it in context and invites all mutual friends to view the photos, it could jeopardize the carefully crafted privacy settings of the first user. This kind of privacy violation is all too common in social networks.

Keywords: Social Media, Privacy and Security, Cyber Security, Cyber Crimes, Online Crimes.

CYBER CRIMINALS AND THEIR TARGETS

Vandana Ravat[1]

[1]M.Sc. Forensic Science, Lucknow University, U.P

Abstract

Cybercrimes are a new class of crimes to India rapidly expanding due to extensive use of Internet. Dishonest and greedy people take advantage of easy and free access to Internet and perform any acts to satisfy their needs. The need could be physiological or psychological in nature. Too much online shopping and wide use of “social media” are root cause of cybercrimes. Much awareness created for cybercrimes and users were educated. But still people do not complain it to authorities. Even somebody do it then also police or crime branch unable to clear such complains in reasonable time period. Delay in justice will lead to no registration of complain. This is not healthy situation in free democratic INDIA. The law IT (Information Technology) Act 2000 and several sections of the IPC are in place but in large population country like China and India, it is very difficult to control crime caused by cyber world. We need to have self-control for better society. We shall evaluate impact of social media, trends towards shopping online and punishment for cyber attackers in this paper. We shall also try to prepare road map for Indian and recommend approach suitable for young generation of India.

Keywords: Cybercrime, Information Technology, IT Law, Internet.

CYBER DEFAMATION UNDER THE PREVIEW OF THE CURRENT STATUTORY PROVISIONS

Aarti Rajapurkar [1]

Des Shri Navalmal Firodia Law College, Pune

Abstract

The enormous scope of cyberspace has expanded after the Digital Revolution. Accessing and transmitting information through the World Wide Web has become a significant part of contemporary lifestyle. This exposes us to social experiences, where the individuals show up through a 'username' with an identity of their own choice to find, develop and exploit their own "parallel reality". The widespread internet has a strong grip over every aspect of our life and criminal activities are no exception to this. India has marked constant growth in Cyber offenses over a decade. The ePoster talks about one such offense of defamation in cyberspace. Cyber defamation is an offense of publishing defamatory material against an individual, institution or a community in the cyber domain. It is one of the worst forms of cybercrime which engulfs all walks of life into its fold and endangers and causes damages upon the individual and institution's name and fame, to a larger extent. The researcher has relied upon the secondary sources of data such as books, journals, e-sources, articles, newspapers and relevant provisions with case laws. Right to reputation or right against defamation is recognized as a basic human right in international legal instruments. As per article 12 of UDHR, the reputation of an individual should be protected from arbitrary attack on reputation and article 10 of the European Convention on Human Rights also recognizes the right to reputation as a basic human right by way of imposing restrictions on freedom of speech and expression. The poster highlights the misdemeanor of Cyber defamation in accordance with the provisions laid down under the Indian Penal Code and the Information Technology act, 2000 along with landmark judgments. The key objective of this poster is to analyze the Indian statutory provisions of the offense and to draw conclusions from it.

Keywords: Cyber Defamation, Information Technology Act, 2000, Indian Penal Code, Statutory provisions, Judgments.

CYBERBULLYING THROUGH VIDEOGAMING

Shivangi Gupta[1]

[1]Galgotias University, Greater Noida, Uttar Pradesh

Abstract

Cyberbullying is the use of electronic communication to bully a person typically by sending messages of an intimidating or threatening nature. Cyberbullying through online gaming such as video gaming includes multiplayer gaming, avatar gaming, player genders. Cyberbullying do have pros and cons in online gaming. Online gaming can be played on computer, tabs, game console, handheld system which allow users to play with known players as well as to the unknown players. Gaming has the positive effects on players but on the other hand it also has the negative remarks that turns into cyberbullying. While there are many types of cyberbullying crimes that are recorded and are researched in the recent years, one of them is online gaming of video games. Children are more likely towards online gaming like shooter gaming, action gaming, role player games. People use different tactics like DOXING, FALSE IDENTITY PROFILE, also referred as SOCKPUPPET for cyberbullying and also they leak the personal information and through posting, texting and instant messaging hurtful things. The online communities make their team and they post the links that appear to game related but are truly computer viruses or malware through which they gain the access to disrupt, damage to a computer and also to their gaming success history. Children are not aware about the security so they become the victim for cyberbullying. Cyber security provides the information about how to secure the account and block the fake accounts who use the avatar gender and try to bully children and send them life threats. Reporting the game developer or the company and blocking the player who is bullying or de-friend the player from the social media in gaming communities.

Keywords: Cyberbullying, Tactics, Avatar gender, Player genders, Causes and prevention.

CAUSES OF CYBER CRIME

Tanu Sindhvani[1]

[1]Amity University Noida (Uttar Pradesh)

Abstract

Cyber-crime is an illegal crime which is done by a person who is expert in playing with technologies, networking and computer system. Cyber-crime is the most widespread crime performing a distressing role in Current time. Now a days, we all are familiar with computer and internet system. Mostly people use system work for their knowledge purposes or playing games, net surfing but many of them use their mind for criminal activities like frauds, blackmailing, stealing identities, bullying, threatening, ATM fraud, spam messaging, E-mail hacking etc. Passwords are easily hacked by the criminals because most of the people write their password in terms of numbers like 1, 2, 3, 4, 5, and 6 which is easily idealized by the criminals. There are various crimes related to cyber such as hacking, pornography, cyber bullying, phishing, harassment, cyber stalking, intellectual property theft, Credit card fraud. In present time, Crypto-market is a new form of cyber-crime in which criminal maintain a website to keep them anonymous for drug dealing. This paper will give you some facts about the major causes of cybercrime. So that all of you can be careful regarding these types of crime. We all have to maintain a strong password for personal and professional accounts or use an updated version of the system and keep your social account private. So, no one can follow us without our permission.

Keywords: Crypto market, E-mail, Bullying, Intellectual, Harassment.

HACKERS & PUBLIC WI-FI

Aastha Mahna[1]

[1]Amity Institute of Forensic Science, Amity University, Noida, Uttar Pradesh

Abstract

Nowadays free Wi-Fi is available everywhere such as at restaurants, hotels, airports, book stores and even random outlets of retail products. Everyone can have access to these Wi-Fi is and can serve the internet from these free access point easily. But this free access comes at a price, though, and only a few people understand the Wi-Fi risks associated with these connections. The features which attract the consumers to use free Wi-Fi hotspots also attracts the hackers to use the same, for example, these access points does not require any authentication to establish the network connection. This also creates an amazing opportunity for the hacker to get an authenticated access to devices which are unsecured on the same network. The biggest threat to the consumers who use free Wi-Fi is that the hackers position himself between the consumer and the connection point. So instead of directly using the Wi-Fi hotspot which is provided the consumer unknowingly sends his or her information to the hacker and who then release it on. The hacker has access to every piece of information which the consumer is sending out on the internet, for example important emails, their credit card or debit card information and even their security credentials. Once the hacker has all this information, he can at his own comfort access the consumers systems as and whenever he wants. Hackers also use an unsecured Wi-Fi connection to transfer malware. If any consumer allows file sharing across a network, the hacker can easily infect the software on his or her computer. Some hackers even managed to hack the connection point itself, causing pop-ups to appear during the process of connection offering an update to a popular software. And clicking on the window installed the malware which was distributed by the hacker. There are certain precautions which consumers must take to keep the information safe such as: 1. Use a VPN 2. Consumers should use SSL connections 3. Sharing should be avoided while using a public network. 4. Wi-Fi should be turned off when not in use.

Keywords: Hackers, WIFI, Risks, Malware, Software, Precautions

CYBER BULLYING AND ITS VARIOUS IMPACTS

Surbhi Kawatra[1]

[1]Institute of Road Traffic Education, Faridabad

Abstract

Cyber Bullying also known as online bullying, it is a term used when any person is bullied by the means of internet using any electronic means over any social media or any game platform by another person. The bullying behaviour may include posting threats, any personal information, rumours, sexual remarks or any hate speech which may lead the victim to have suicidal thoughts, lower self-esteem and various other negative emotions such as anger, depression, frustration, etc. which is done repeatedly with an intent of causing harm to the victim. This can be of various types such as Harassment, Cyber Stalking, Flaming, Trolling, Masquerading and Fraping. This is committed by using various platforms such as through social media which includes Instagram, Facebook, Snapchat, etc., through online games or in search engines as information spreads very fast on internet which is hard to stop. There are no specific laws for regulation of cyber bullying in India but various section under Information Technology Act such as Section 66A for punishment of sending annoying, offensive and insulting communication digitally, 67 for publishing or transmitting obscene material, 67A sexually explicit material in electronic form, etc. and various sections under Indian Penal Code such as Section 499 for sending defamatory messages by email, 507 for Criminal Intimidation by anonymous communication, etc. consists of certain punishments for offences that are linked with Cyber Bullying. In this e-poster presentation, I will briefly conclude the various harmful effects which had cause a great impact on the victim where victim could be a teenager or youth and also discuss the need of a specific law or particular section dedicated only for cyber bullying.

Keywords: Cyber Bullying, Masquerading, Frapping, Threats, Sexual Remarks, Self-esteem.

CYBERSTALKING: A BANE ARISING WITH THE PROGRESSING TECHNOLOGY

Mansi Seewal[1]

[1]Banaras Hindu University, Varanasi, Uttar Pradesh

Abstract

Universally, there has been a rapid rise in the use of computers and electronic gadgets. These developments have led to significant growth in criminality, especially in cyberspace. Cybercrimes have continued to rise alarmingly across the world. Cybercrimes have grown progressively with perpetrators developing newer and sophisticated techniques every day. Cyber-crimes mainly involves the activity that use internet and computers as a tool to extract private information of an individual either directly or indirectly and disclosing it on online platforms without the persons consent or illegally with the aim of degrading the reputation or causing mental or physical harm. With the increase of dependency on cyber-crimes committed against women have also increased. Thus cybercrime has emerged as a major challenge for the law enforcement agencies of different countries in order to protect the women and children who are harassed an abused for voyeuristic pleasures. Women are commonly targeted for cyber stalking, cyber pornography, impersonation, etc. India is one of such country which has enacted the IT Act 2000 to deal with the issues pertaining to cybercrimes in order to protect the women from exploitation by vicious predators. Cyber Stalking is the use of the Internet or other electronic means to stalk or harass a person. The utilization of technology allows stalkers to harass their target from any part of the world. As such, the Internet has literally become a fertile breeding ground for an entirely new and unique type of criminal offender hereafter known as the cyber stalker – an offender who uses the Internet as a tool or weapon of sorts to prey upon, harass, threaten, and generate immense fear and trepidation in its victims through sophisticated stalking tactics. Although there are many preventions through which cyber stalking can be prevented. And there are Acts too to take legal actions on the persons who did such crimes.

Keywords: Cyber-crimes, Internet, Women, Cyber-stalking, IT Act, Stalkers, Preventions.

INDIA'S NEW NATIONAL CYBER SECURITY STRATEGY

Anuraj Khandelwal[1]

[1]Government Institute of Forensic Science, Aurangabad

Abstract

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks and unauthorized access. The National Cyber Security Policy (NCSP) released by the Government of India in 2013, had laid down several strategies to counter security threats from cyberspace. The lack of a comprehensive cyber security strategy/policy is conspicuous and increasing vulnerability. Before we embark into 2022, India would have been presented with a National Strategy on Cyber security by the Department of Electronics and Information Technology. This puts a premium on ensuring the security of the national cyberspace an ultimate necessity in the coming years. Additionally, the lockdown due to COVID-19 pandemic has further increased the dependency on digital platforms, which has further expanded the span of usage of the country's cyberspace. Central Government's push for its scheme of "Digital India," has created a culture of dependency on virtual communications and transactions in the minds of the people of the country. Whilst eight years have passed, limited implementation has taken place, and our country remains amongst the most targeted nations. There seems to be a light at the end of the tunnel for India. It is a potential activity by which information and other communication systems are protected from and/or defended against the unauthorized use or modification or exploitation or even theft.

Keywords: Cyber security, Information technology, threats, digital platforms, National Cyber Security Strategy.

PHISHING ATTACKS AND HOW TO PROTECT YOURSELF FROM PHISHING ATTACK

Sumit Kumar[1]

[1]Sherlock Institute of Forensic Science, A-14, First Floor, Stadium Rd, Mahendru Enclave, Chhatrasal, New Delhi

Abstract

The most common form of social engineering attack is phishing. Phishing attacks exploit human error to harvest credentials or spread malware, usually via infected email attachments or links to malicious websites. The phishing is also called psychological trick crime. Phishing is the act of sending fraudulent messages via e-mail, telephone/voice or text messages which appears to be from legitimate sources like a bank, a recruiter, a credit card company etc. The phishing scam is of different types like deceptive phishing, vishing, smishing, spear phishing and whaling. Now a days, this attack or scam is very common. The attackers can exploit the victim by either stealing money or stealing sensitive personal information (name, Aadhaar details, bank account details etc.) or harm the victim in any other way. Phishing starts with a fraudulent email or other communication that is designed to lure a victim. The message is made to look as though it comes from a trusted sender. If it fools the victim, he or she is coaxed into providing confidential information, often on a scam website. Sometimes malware is also downloaded onto the target's computer. Once trapped, the attackers can exploit the victim by either stealing money or stealing sensitive personal information (name, Aadhaar details, bank account details etc.) or harm the victim in any other way. These criminals create such kind of emergency that user has to take decisions rapidly, he becomes nervous and act impulsively which makes them follow the instructions given by the attacker and makes him/her infected with these crimes. The entire basis of this kind of attack is to make the victim fall into their trap by sending fake emails/website (Phishing), calls (Vishing) or SMS (Smishing).

Keywords: Phishing, Scam, Fraud, theft, personal information.