Cybercrimes and Digital Forensics Forum

Naif Arab University for Security Sciences, Riyadh, Kingdom of Saudi Arabia.

19-21/11/2019
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Overview</td>
<td>4</td>
</tr>
<tr>
<td>Forum Program</td>
<td>9</td>
</tr>
<tr>
<td>Speakers Abstracts</td>
<td>29</td>
</tr>
<tr>
<td>Workshops</td>
<td>45</td>
</tr>
<tr>
<td>Institutions and Companies Profiles</td>
<td>53</td>
</tr>
</tbody>
</table>
Cybercrimes and Digital Forensics Forum

Forum Aims:

- Looking at modern issues, experience, and practices in fields related to cybercrimes and digital forensics.
- Looking at laws and regulations and principles of investigation in fields related to digital forensics and cybercrimes.
- Looking at trends in education and training in the field of cybercrimes and digital forensics, and presenting the experience of Naif Arab University for Security Sciences (The Digital Forensics Laboratories).
- Exchanging experiences and looking at the latest developments in research and technology and defensive strategies in fields related to digital forensics and cybercrimes.

Main Topics of the Forum:

- The latest developments in academic research related to cybercrimes and digital forensics.
- Efforts and developments in laws and legislations that systematize cybercrimes and digital forensics on an Arab and international scale.
- Education and training in fields related to cybercrimes and digital forensics on an Arab and international scale.
- The present state and future of modern technologies and standard practices in fields related to cybercrimes and digital forensics on an Arab and international scale.

Organizers:

Naif Arab University for Security Sciences represented by:

- The Arab Society for Forensic Sciences and Forensic Medicine (ASFSFM)
- Events Management / General Directorate of External Relations
Scientific Committee:

Dr. Fahad Mohammed Alharby
Naif Arab University for Security Sciences

Dr. Hasan Ahmed Alshehri
Naif Arab University for Security Sciences

Dr. Abdulsallam Bakdash
Naif Arab University for Security Sciences

Dr. Abdulrazaq Abdulaziz Almarjan
King Abdullah University of Science and Technology (KAUST)

Dr. Fatimah Yousef Alakeel
King Saud University

Dr. Moudhi Mohammed Aljamea
Saudi Telecom Company (STC)

Dr. Hamad Mansoor Alawar
Dubai Police

Colonel Dr. Rashed Awadh Al-adheelah
Department of Criminal Evidence in Riyadh

Dr. Meryem Abdulqader Ammi
Naif Arab University for Security Sciences
DAY - 1

Tuesday  19.11.2019

08.30-10.00 AM  Registration
10.00-10.30 AM  Opening
10.30-12.00 PM  Plenary Session (Hall A)

- Open Panel discussion
- Cybercrimes and Digital Forensics: Challenges and Opportunities

12.00-13.00 PM  Break
13.00-14.30 PM  Session 1 (Hall A)

- Education and training in fields related to cybercrimes and digital forensics
- Oral Presentations OP1 - OP4

14.30-14.45 PM  Break
14.45-16.30 PM  Exhibition, Laboratories Tour

- Cypercrimes and Digital Forensics Exhibition
- NAUSS Digital Forensics Laboratories Tour

Workshops

<table>
<thead>
<tr>
<th>Lab. 4</th>
<th>Lab. 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.30-14.30 PM</td>
<td>Workshop 1</td>
</tr>
<tr>
<td>14.45-16.15 PM</td>
<td>Workshop 3</td>
</tr>
</tbody>
</table>
### DAY - 2

**Wednesday 20.11.2019**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session 2 (Hall A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>08.30-09.00 AM</td>
<td>Registration</td>
</tr>
<tr>
<td>09.00-10.30 AM</td>
<td>Latest Developments in Cybercrimes and Digital Forensics</td>
</tr>
<tr>
<td></td>
<td>Oral Presentations OP 5 - 8</td>
</tr>
<tr>
<td>10.30-10.45 AM</td>
<td>Break</td>
</tr>
<tr>
<td>10.45-12.15 PM</td>
<td>The Present State and Future of Modern Technologies and Standard Practices in</td>
</tr>
<tr>
<td></td>
<td>Fields Related to Cybercrimes and Digital Forensics</td>
</tr>
<tr>
<td></td>
<td>Oral Presentations OP 9 - 12</td>
</tr>
<tr>
<td>12.15-13.15 PM</td>
<td>Break</td>
</tr>
<tr>
<td>13.15-14.45 PM</td>
<td>Open Panel Discussion</td>
</tr>
<tr>
<td></td>
<td>Cybercrimes and Digital Forensics: Updates and Solutions</td>
</tr>
</tbody>
</table>

**Workshops**

<table>
<thead>
<tr>
<th>Time</th>
<th>Lab. 4</th>
<th>Lab. 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.45-12.15 PM</td>
<td>Workshop 4</td>
<td>Workshop 5- Part1</td>
</tr>
<tr>
<td>13.15-14.45 PM</td>
<td>Workshop 6</td>
<td>Workshop 5- Part2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lab. 1</td>
</tr>
<tr>
<td>13.15-14.45 PM</td>
<td>Repeated Workshop 2</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Session</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>09.00-10.30 AM</td>
<td>Session 5 (Hall A)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Developments in Laws and Legislations Related to Cybercrimes and Digital Forensics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Oral Presentations OP 13 - 16</td>
<td></td>
</tr>
<tr>
<td>10.30-10.45 AM</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>10.45-12.15 PM</td>
<td>Session 6 (Hall A)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Open Panel Discussion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Legal Frameworks for Combatting Cybercrimes</td>
<td></td>
</tr>
<tr>
<td>12.15-13.00 PM</td>
<td>Closing Ceremony, Recommendations (Hall A)</td>
<td></td>
</tr>
</tbody>
</table>
Day One
19 November 2019

Forum Program
DAY - 1

Tuesday 19.11.2019

Registration : 08.30 - 10.00 AM
Opening Ceremony : 10.00 - 10.30 AM

10.30-12.00 PM : Plenary Session (Hall A), Cybercrimes and Digital Forensics: Challenges and Opportunities

Moderator : Dr. Abdulrazaq Abdulaziz Almarjan
Manager of Security Systems, King Abdullah University of Science and Technology (KAUST), Saudi Arabia.

Topics

- Cyber Laws and Digital Forensics.
- Education in Cybercrimes and Digital Forensics: Challenges and Opportunities.
- Role of ITU in Cyber Security
- Combating Cross-border Organized Crime and Strategies to deal with Cybercrimes.
- The Employing of Technology in Traditional Crimes and how to Qualify Specialists to Deal with the Rapid Development of Cybercrimes.

**Panelists**

**His Excellency Dr. Khalid Al-Luhaidan**  
Member of the Supreme Court, Saudi Arabia

**Mr. Ebrahim Al-Haddad**  
Regional Director, Arab States, International Telecommunication Union (ITU).

**Dr. Saleh Ibrahim Almotairi**  
General Director, National Cybersecurity Center (NCS), Saudi Arabia

**Dr. Danil Zakoldaev**  
Dean of Faculty of Information Security and Computer Technologies of ITMO University, St. Petersburg, Russia.

**Col. Saeed M. Al Hajri**  
Director, Cybercrime Department, Criminal Investigation Department, Dubai Police, UAE
13.00-14.30 PM: **Session 1 (Hall A), Education and training in fields related to cybercrimes and digital forensics**

**Chairperson:** Dr. Fatimah Yousef Alakeel
Director of Training Center, Faculty of Applied Studies and Community Service, KSU

**OP 1**

**Title:** How will Naif Arab University for Security Sciences Contribute to Reducing Cyber and Conventional Crimes?

Author: Dr. Abdulrazaq Abdulaziz Almarjan

Affiliation: Director of Security Technology Department, King Abdullah University of Science and Technology (KAUST), Saudi Arabia.

**OP 2**

**Title:** Addressing Cybercrime Challenges: Strategies for Capacity & Capability Building.

Author: Prof. Dr. Muhammad Khurram Khan

Affiliation: Center of Excellence in Information Assurance, King Saud University, Saudi Arabia
OP 3

**Title:**
Education and Training in Fields Related to Cybercrimes and Digital Forensics on an Arab and International Scale.

**Author:**
Dr. Moudhi Mohammed Aljamea

**Affiliation:**
General Manager of Digital Technology at STC Academy, Saudi Arabia

OP 4

**Title:**
Threats Landscape and the Role of Education and Training in Cybersecurity.

**Author:**
Mr. Rasheed Al-Odah

**Affiliation:**
Trend Micro, Japan
WORKSHOPS

13:30 - 14:30 : Workshop 1, (Lab 1)

Title
Connected Threat Defense

Presenter
Mr. Ali Zubayd

Affiliation
Cybersecurity Consultant, Trend Micro, KSA

13:30 - 14:30 / 14:45 - 16:15 : Workshop 2, (Lab 4)

Title
Voice and Face Biometrics: How to Find and Verify People

Presenters
Mr. Konstantin Danilov ¹, Mr. Kais Boughanmi ²

Affiliation
¹ Product Manager, Speech Technology Center, Russia
² Business Development Manager, Speech Technology Center, Russia

14:45 - 16:15 : Workshop 3, (Lab 1)

Title
How to build Efficiency and Reduce Time around Managing Cases and Forensic Tasks

Presenters
Dr. James Kent ¹, Mr. John Nassif ²

Affiliation
¹ CEO & Co-Founder Black Rainbow Ltd, United Kingdom
² Region Head META-APAC, Black Rainbow Ltd, Dubai, UAE
Day Two
20 November 2019

Forum Program
Wednesday 20.11.2019

Registration: 08.30 - 09.00 AM

09.00-10.30 AM: Session 2 (Hall A)
Latest Developments in Cybercrimes and Digital Forensics

Chairperson: Dr. Hasan Ahmed Alshehri
Forensic Sciences Dep., College of Criminal Justice, NAUSS

Title: The Need for a Holistic Approach to Cyber Safety

Author: Prof. Elhadj Benkhelifa
Affiliation: Staffordshire University, UK

Title: Challenges and Techniques in Drone Forensics.

Author: Dr. M A Hannan Bin Azhar
Affiliation: Canterbury Christ Church University, UK.
Title: Decoding the Minds of Hackers: The Intersection of Research and Reality.

Author: Prof. Christopher E. Pogue

Affiliation: Head of Nuix Partner Connect / Adjunct Professor, Southern Utah University, USA

Title: The Future of Forensic evidence and 3D Printing.

Author: Major. Dr. Hamad M Alawar

Affiliation: Biometrics & Forensic Gait Analysis Expert, Dubai Police, UAE.
10.45-12.15 PM: **Session 3 (Hall A), The Present State and Future of Modern Technologies and Standard Practices in Fields Related to Cybercrimes and Digital Forensics**

**Chairperson**: Colonel Dr. Rashed Awadh Al-Adheelah
Director of Crime Investigation Division, Department of Criminal Evidence in Riyadh, Saudi Arabia

**OP 9**

**Title**: Digital Sensor and Media Forensics: A Practical Approach.

**Author**: Prof. Ahmed Bouridane

**Affiliation**: Northumbria University Newcastle, UK.

**OP 10**

**Title**: Cloud Forensics Investigation (Challenges and Solutions).

**Author**: Dr. Saad Alqahtany

**Affiliation**: Head of Video Forensics, Forensic and Criminology Department, MOI, KSA.

**OP 11**

**Title**: Cybercrimes and Methods to Dealing with Digital Evidence
Author: 

Affiliation: 
Director of Digital Forensics Department, General Directorate of Criminal Evidence, Saudi Arabia.

Title: 
When Cyber Attacks Meet Financial Crimes.

Author: 
Mr. Yueng-Tien Lo.

Affiliation: 
Ministry of Justice Investigation Bureau, Taiwan.

13.15-14.45 PM: Session 4 (Hall A), Open Discussion 
Cybercrimes and Digital Forensics: Updates and Solutions

Chairperson: Dr. Fahad Muhammed Alharby
Supervisor-General of Administrative Financial Affairs, NAUSS

Speech 1

Title: 
What are the challenges / obstacles for Digital forensics in telecoms industry?

Speaker: 
Mr. Mazen Dakhil Al Ahmadi

Affiliation: 
STC, Saudia Arabia
Speech 2
Title: Strategies to Combat Cybercrimes.
Speaker: Col. Saeed M. Al Hajri
Affiliation: Director, Cybercrime Department, Criminal Investigation Department, Dubai Police, UAE

Speech 3
Title: Experience of Digital Forensic Labs in Dubai Police.
Speaker: Major. Hamad J Alajmi
Affiliation: Deputy Director of Electronic Evidence Department, Dubai Police, UAE.

Speech 4
Title: Utilizing Information Security Techniques as Digital Evidence for Cybercrime Activities
Speaker: Prof. Dr. Adnan Gutub
Affiliation: Professor of Computer Engineering, Umm Al- Qura University, KSA.
WORKSHOPS

10:45 - 12:15 : Workshop 4, (Lab 1)

Title
Next Generation Digital Forensics: Challenges and Future Paradigm

Presenter
Eng. Pratap Kumar

Affiliation
Cyberforensics Specialist, Infratech, Saudi Arabia

10:45 - 12:15 / 13:15 - 14:45 : Workshop 5, (Lab 2)

Title
Humanizing Digital Forensics

Presenter
Eng. Khaled Hegazy

Affiliation
Solution Consultant EMEA, Nuix, Australia

13:15 - 14:45 : Workshop 6, (Lab 1)

Title
Drone Forensics

Presenter
1st Lt. Khalifa Mohammad AlRoom

Affiliation
Dubai Police, UAE
Call for Papers

The Journal of Information Security and Cybercrimes Research (JISCR) is a peer-reviewed, refereed journal, published by Naif Arab University for Security Sciences (NAUSS). It publishes specialized research work on Information Security and its pertinent topics in order to disseminate the modern and comprehensive concepts of security policies and mechanisms in the cyberspace. The JISCR contributes also to the advancement of knowledge related to the regulations and laws for ensuring cybersecurity.

Focus and Scope:

The topics covered in the JISCR include, but not limited to:

- Computer and Networks security
- Cryptography and Foundations of Computer Security
- Authentication/Authorization and access control
- Privacy and Security in cyberspace issues
- Wireless Access Security
- Biometric applications security
- Data science security
- E-commerce security
- Developing cyber safety policies
- Cybercrimes laws
- Physical Computer Security
- Copyright and Intellectual property Law
- Intrusion detection systems and Firewall
- Blockchain and smart contracts
- Incident response and Digital forensics
- IT governance and risk management
- IoT security and privacy
- Multimedia and mobile security
- Human factors in cybersecurity

The JISCR publishes original contributions in English that fall under any of the following manuscript categories: Original research papers, Case reports, Review articles, Book Reviews and Conferences / Symposia Proceedings.

The Journal of Information Security and Cybercrimes Research (JISCR) is pleased to announce the publication of its volume3, 1st issue in March 2019. The Journal welcomes the submission of scientific articles in all disciplines of Information Security and cybercrimes research.

For submission and more information, please contact:

Journal’s Website: https://journals.nauss.edu.sa/index.php/JISCR
Journal’s e-mail: jiscr@nauss.edu.sa
Day Three
21 November 2019

Forum Program
DAY - 3
Thursday 21.11.2019

09.00-10.30 AM : Session 5 (Hall A)
Developments in Laws and Legislations Related to Cybercrimes and Digital Forensics

Chairperson : Prof. Tajuldeen Madani
Department of Criminal Law, College of Criminal Justice, Naif Arab University for Security Sciences

OP 13
Title:
Mechanisms for Combating Cybercrimes, A Study in Algerian Legislation

Author:
Prof. Tekarri Haifa Rachida

Affiliation:
Faculty of Law and Political Science University Ali Lounici Blida 02, Algeria

OP 14
Title:
Cybercrimes and The Difficulty of Implementing their Provisions

Author:
Prof. Amara El Mokhtar

Affiliation:
Faculty of Law, Mohammed V University of Rabat, Morocco
OP 15

Title:
Identify Laws, Legislations and Investigative Principles in the Fields of Cybercrime and Digital Evidence

Author:
Dr. Ahmed Saleh Alzahrani

Affiliation:
Public Prosecution, Saudi Arabia

OP 16

Title:
Criminal Responsibility for Cyber Terrorism Crimes

Author:
Dr. Khaled hamed moustafa

Affiliation:
Department of Criminal Law, College of Criminal Justice, Naif Arab University for Security Sciences
10.45-12.15 PM: Session 6 (Hall A), Open Discussion
Legal Frameworks for Combating Cybercrime

**Chairperson:** His Excellency Dr. Khalid Al-Luhaidan
Member of the Supreme Court, Saudi Arabia

**Speech 1**

**Title:**
Cybercrime Investigation Procedures.

**Speaker:**
Dr. Ahmed Salih Alzahrani

**Affiliation:**
Public Prosecution, Saudi Arabia

**Speech 2**

**Title:**
Cybercrime and Digital Evidence Laws and Legislations.

**Speaker:**
Mr. Fahad Abdulrahman Alduraibi

**Affiliation:**
CITC, Communications and Information Technology Commission.
Speech 3

Title: The Evidential weight of Digital Evidence

Speaker: Dr. Zaki Shannak

Affiliation: Department of Criminal Law, College of Criminal Justice, Naif Arab University for Security Sciences

Speech 4

Title: Mechanisms of International Cooperation in the Fight against Cybercrimes

Speaker: Prof. Amara El Mokhtar

Affiliation: Faculty of Law, Mohammed V University of Rabat, Morocco

12.15 - 13.00 : Closing Session, (Hall A)

Chairperson: Dr. Abdulsallam Bakdash
Secretary General, The Arab Society for Forensic Sciences and Forensic Medicine
The Arab Journal of Forensic Sciences and Forensic Medicine (AJFSFM) is pleased to welcome the submission of scientific articles in all disciplines of forensic science and forensic medicine. The AJFSFM is a peer-reviewed, open access (CC BY-NC), international journal dedicated to the development and application of forensic sciences and forensic medicine knowledge and research for the purpose of law and justice across the globe.

The AJFSFM is an official publication of the Arab Society for Forensic Sciences and Forensic Medicine (ASFSFM) and is published twice a year.

**Focus and Scope:**
The topics covered in the AJFSFM include, but not limited to:

- Forensic Pathology
- Odontology
- Histochemistry
- Toxicology (drugs, alcohol, etc.)
- Psychiatry and Hypnotics
- Forensic Anthropology and Archeology
- Fingerprints and Impressions
- Firearms and Toolmarks
- Digital forensics and Cyber crimes
- Criminal justice
- Crime scene
- Investigations of value to public health
- Forensic chemistry (Inks, Paints, Dyes, Explosives, Fire accelerants)
- Forensic Biology (Serology, Human DNA profiling, Entomology, population Genetics, Anthropology)
- White collar crimes (Counterfeiting and Forgery; Questioned documents)

The AJFSFM publishes original contributions that fall under any of the following manuscript categories: Original research papers, Case reports, Review articles, Book Reviews and Conferences / Symposia Proceedings.

Papers can be written in English or Arabic. Articles received are sent for blind peer review, with a review procedure completed within 4-6 weeks of submission. Authors can also submit their manuscripts online or send them via e-mail: ajfsfm@nauss.edu.sa

For more information, please contact:

Journal’s Website: https://journals.nauss.edu.sa/index.php/AJFSFM/index
Journal’s Mail: ajfsfm@nauss.edu.sa
Focus and Scope:
The topics covered in the AJFSFM include, but not limited to:

- Forensic Pathology
- Odontology
- Histochemistry
- Toxicology (drugs, alcohol, etc.)
- Psychiatry and Hypnotics
- Forensic Anthropology and Archeology
- Fingerprints and Impressions
- Firearms and Toolmarks
- Digital forensics and Cyber crimes
- Criminal justice
- Crime scene
- Investigations of value to public health
- Forensic chemistry (Inks, Paints, Dyes, Explosives, Fire accelerants)
- Forensic Biology (Serology, Human DNA profiling, Entomology, population Genetics, Anthropology)
- White collar crimes (Counterfeiting and Forgery; Questioned documents)

Arab Journal of Forensic Sciences and Forensic Medicine (AJFSFM)
The Arab Journal of Forensic Sciences and Forensic Medicine (AJFSFM) is pleased to welcome the submission of scientific articles in all disciplines of forensic science and forensic medicine. The AJFSFM is a peer-reviewed, open access (CC BY -NC), international journal dedicated to the development and application of forensic sciences and forensic medicine knowledge and research for the purpose of law and justice across the globe.

The AJFSFM is an official publication of the Arab Society for Forensic Sciences and Forensic Medicine (ASFSFM) and is published twice a year.

CALL FOR PAPERS

For more information, please contact:
Journal's Website: https://journals.nauss.edu.sa/index.php/AJFSFM/index
Journal's Mail: ajfsfm@nauss.edu.sa
**Title:**
How will Naif Arab University for Security Sciences Contribute to Reducing Cybercrimes and Conventional Crimes?

**Authors:**
Dr. Abdulrazaq Abdulaziz Almarjan

**Affiliation:**
Director of Security Technology Department, King Abdullah University of Science and Technology (KAUST), Saudi Arabia.

**Abstract:**

تشير التقارير الدولية إلى ارتفاع جرائم الإنترنت، وذكرت إحصاءات مركز IC3 لشكاي جرائم الإنترنت أن عدد شكاوى منذ عام 2014م، حيث استقبل في عام 2014م 269.422 شكوى وفي عام 2018م قفزت الشكاوى إلى 351.936 شكوى بمعدل يزيد على 900 شكوى يومياً، وسجلت جرائم الاحتيال والسرقة والاستغلال الإلكتروني خسائر مالية كبيرة قدرت بـ 2.7 مليار دولار أمريكي لعام 2018م مقارنة بـ 800 مليون دولار أمريكي لعام 2014م.

أصبحت هذه الجرائم تهدد الأمن الوطني للدول ولم تقتصر مواجهتها على المنظومات العدلية الجنائية لوحدها بل مسؤولية جميع القطاعات. ومن أهم هذه القطاعات القطاع التعليمي من حيث تأسيس وتأهيل الخبراء والمختصين لمواجهة هذه المخاطر الحديثة.

وتعد جامعة نايف العربية للعلوم الأمنية من الجامعات الرائدة والمتميزة في إعداد القادة والخبراء الأمنيين في مجالات أمنية متعددة. واستُكشِفاً بدورها في المساهمة والمشاركة بتحليل التحديات الحديثة التي تواجه المنظمات العدلية الجنائية في الدول العربية، أطلق الجامعة استراتيجيتها الجديدة في عام 2019م ورؤيتها لتكون المؤسسة الأولى في إعداد القادة والخبراء العرب في المجالات الأمنية.

ستتناول المحاضرة الأليات التي اتبعتها الجامعة في ترجمة هذه الرؤية على أرض الواقع لمواجهة الجرائم الحديثة، ومن أهم المحاور التي سيتم مناقشتها: هما استراتيجيتها الجامعية لتكون رائدة في مواجهة الجرائم السيبرانية والتقليدية؟ كيف سيتم إعداد القادة والخبراء العرب في مجالات مكافحة الجرائم السيبرانية والأدلة الرقمية الجنائية؟ كيف سيتم الاستجابة من البيانات الضخمة؟ ومن هم المستفيدون من برامج مكافحة الجرائم السيبرانية والأدلة الجنائية الرقمية؟.
OP 2

**Title:**
Addressing Cybercrime Challenges: Strategies for Capacity & Capability Building

**Authors:**
Prof. Dr. Muhammad Khurram Khan

**Affiliation:**
Center of Excellence in Information Assurance, King Saud University, Saudi Arabia

**Abstract:**

Cybercrime is an offensive or illegal act that is undertaken with a criminal motive to intentionally acquire financial gains, cause physical or mental harm, and defame the victim. Such activities exploit vulnerabilities in use of the internet and computing systems to illicitly access or attack information and services. It is well-understood that crime follows money and due to the heavy global investments, online financial transactions, and monetary scale of cyberspace, it has also become a great treasure for illicit criminal activities.

Cybercrimes are becoming increasingly pervasive and sophisticated and have more severe economic impact than most conventional crimes happened in the physical world. Furthermore, the modus operandi of cybercriminals is going to be more complex and persistent due to the use of offensive artificial intelligence (AI) and machine learning (ML) driven state-of-the-art hacking tools, which are quite hard to identify, protect, detect, respond and recover. It is estimated that cybercrime damages could cost the world around USD 6 trillion by 2021, which is more profitable than the global trade of illegal drugs and higher than the GDP of many developed countries. On the other hand, to defend cyberspace from crimes, hacking, extortions, and intrusions, USD 1 trillion is expected to be spent globally between 2017 and 2021.

Hence, to confront cybercrimes of new-age, state-of-the-art strategies are needed to build capacity and capability. In this speech, we would discuss some insights from the intersecting dimensions of policy, research and practice to fight against cybercrimes for a resilient, safe, and peaceful cyberspace.
**Title:**
Education and Training in Fields Related to Cybercrimes and Digital Forensics on an Arab and International Scale

**Authors:**
Dr. Moudhi Mohammed Aljamea

**Affiliation:**
General Manager of Digital Technology at STC Academy, Saudi Arabia

**Abstract:**
The rise of cybercrime continues to accelerate as it is expected it will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015 and that shows us how cybercrimes is increasing and cyber forensic is becoming more important for cybersecurity policy and management nowadays. An effective fight against cybercrime is an important priority globally for many countries through building strong national strategies focusing on developing capabilities. In fact, in 2016 an international skills gap analysis estimated a global shortage of 2 million skilled cybersecurity professionals by 2019, with the number of unfilled cyber security jobs predicted to reach 3.5 million by 2021.

We will be having and an overview on the current state of the developing capabilities in the field of cybercrimes and digital forensics, what are the national strategies for different countries on developing capabilities to fight cybercrimes globally and the kingdom of Saudi Arabia as a case study.

**Title:**
Threat Landscape and the Role of Education and Training in Cybersecurity.

**Authors:**
Mr. Rasheed Al-Odah

**Affiliation:**
Trend Micro, Japan
Abstract:
A recent Trend Micro roundup report revealed a surge in fileless attacks designed to disguise malicious activity. In Middle East and North Africa (MENA), the Kingdom of Saudi Arabia blocked the highest numbers of email threats (65,175,007) and malware threats (976,508). In this session, the latest threats landscape in Saudi Arabia will be presented, as well as the role of education and training in protecting individuals, families, and businesses.

Title:
The Need for a Holistic Approach to Cyber Safety.

Authors:
Prof. Elhadj Benkhelifa

Affiliation:
Staffordshire University, UK

Abstract:
With the ever evolving cyber space, it is necessary to keep upskilling our workforce in order to keep up with these changes and meet new security requirements. The Digital Economy and the information age we are living create new generations of cyber attacks, which elevates business risk to a new level. Cybersecurity has become the cornerstone of our digital economy; securing everything from connected devices (IoT) to payments online. Cybersecurity has indeed become a so diverse discipline with numerous sub domains and specializations.

On another hand, One of the main reasons that impedes the wider adoption of new technology paradigms, such as cloud computing, have been linked primarily to aspects related to data governance. While security is one of the most cited challenges to cloud adoption, 41% of the security problems are related to governance and legal issues.

Forward thinking organizations believe that the only way to solve the data problem will be the implementation of an effective data governance. Up to very recently governance is mostly informal with very ambiguous and generic regulations, in silos around specific enterprise repositories, lacking structure and the wider support of the organization. Despite its highly recognized importance, the area of data governance is still under developed and under researched.
This talk will present an analysis of the current and predicted future cyber space and what skills will the next generation of professionals need to tackle emerging threats. The analysis will show that future Cyber workforce will be highly complex and heterogenous and will have to go beyond the technical skills to combine domain specific knowledge, data governance strategy, and social intelligence to be able to reduce business risks.

**Title:** Challenges and Techniques in Drone Forensics

**Authors:**
Dr. M A Hannan Bin Azhar

**Affiliation:**
Canterbury Christ Church University, UK

**Abstract:**
Carrying capabilities of drones and their easy accessibility to public have led to an increase in crimes committed using drones in recent years. For this reason, the need for forensic analysis of drones captured from the crime scenes and the devices used for these drones is also paramount. After capturing the drone, a forensic analysis can provide a lot of information about the potential suspect of a crime based on the data gathered from on-board sensors and other electronics that assist with flight and navigation, as well as the camera and digital storage.

Interpreting the flight data and tackling the multi-platform nature of drones are the major challenges in forensic analysis of drones. This talk presents the challenges and techniques in extraction and identification of important artefacts from the recorded flight data as well as the associated mobile devices to aid the analysis of two popular drone systems - the DJI Phantom 3 Professional and Parrot AR Drone 2.0. Although different drones vary in their operations, this talk discuss the extraction and analysis of the data from the drones and associated devices using some generic methods which are forensically sound adhering to the Drone forensics Frame work and the guidelines of the Association of Chief Police Officers (ACPO).
Title:
Decoding the Minds of Hackers: The Intersection of Research and Reality

Authors:
Prof. Christopher E. Pogue

Affiliation:
Nuix / Southern Utah University, USA

Abstract:
Over the past few years, we’ve examined the reality that cybersecurity professionals and today’s organizations face in The Black Report. This presentation will uncover some of the key learnings from our research including the typical profile of hackers, their motivations, and how easy it is for them to infiltrate an organization. We’ll then move into a real-world example with Pat Hogan of the United States Secret Service, who will discuss how these specific areas pertain to the recent arrest of an international hacker responsible for the theft and monetization of more than 160 million credit card numbers.

In this session you will learn: What our research uncovered about how organizations can defend themselves against hackers, and Defensive techniques and tools that can help you become more resilient in the face of a nimble and increasingly resourceful adversary.

Title:
The Future of Forensic Evidence and 3d Printing

Authors:
Major. Dr. Hamad M Alawar

Affiliation:
Biometrics & Forensic Gait Analysis Expert, Dubai Police, UAE
Abstract:
3D printing is regarded as one of the main technologies that form the propeller for the current 4th industrial revolution. The technology holds great promise to humanity, yet as with any technology there is potential to use it in a criminal manner. 3D printing technology will influence various aspects of police forensic work, specifically firearms, fingerprint, forensic engineering and biometrics. Therefore it should be a mandate on all police forces to proactively find solutions and forensic techniques to use.

Title:
Digital Sensors and Media Forensics: A Practical Approach

Authors:
Prof. Ahmed Bouridane

Affiliation:
Northumbria University Newcastle, UK

Abstract:
In recent years, the field of digital imaging has seen significant advances to the point that every smartphone now has a built-in video camera for recording high quality videos at no cost and without any constraints.

This seminar aims to discuss a practical approach to process smartphone media (image and video) in order to extract evidential information about video content authenticity as well as the source smartphone camera and its model and make. The detection and location of forgery in maliciously manipulated videos is an important forensic tool at the disposal of forensic scientists and investigators in police forces.

In the applications of source smartphone identification, video authentication and forgery detection, the analyst is assumed to have access to multiple smartphone camera devices including the genuine one or a set of smartphone videos including the ones recorded by the same smartphone. The goal is then to analyse an input video whose origin is unknown in order to identify/verify the source device and authenticate the video content.

In the seminar the concept of sensor pattern noise (SPN) for sensor and source media identification will be introduced and discussed especially for forensic investigation.
Title:
Cloud Forensics Investigation (Challenges and Solutions)

Authors:
Dr. Saad Alqahtany

Affiliation:
Head of Video Forensics, Forensic and Criminology Department, MOI, Saudi Arabia

Abstract:
Cloud computing is a promising next generation computing paradigm which offers significant economic benefits to both commercial and public entities. Due to the unique combination of characteristics that cloud computing introduce, including: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service, digital investigations face various technical, legal and organizational challenges to keep up with current developments in the field of cloud computing. There are plenty of issues that need to be resolved in order to perform a proper digital investigation in the cloud environment. This paper examines the challenges in cloud forensics that are identified in the current research literature.

Furthermore, it explores the current research proposals and technical solutions addressed in the respective research. Ultimately, it highlights the open problems in digital investigation that need further efforts to be tackled.

Title:
Cybercrimes and Methods of Dealing with Digital Evidence

Authors:
Lt. Col. Jalal bin Khalifa Al-Hashel
Affiliation:
Director of the Digital Forensics Department, General Directorate of Criminal Evidence, Saudi Arabia

Abstract:
When cyber attacks meet financial crimes

Title:
When cyber attacks meet financial crimes

Authors:
Mr. Yueng-Tien Lo

Affiliation:
Ministry of Justice Investigation Bureau, Taiwan

Abstract:
Financial institutions are likely main cybercrime targets. In the past years, several cybercrime occurred in Taiwan. For example, a few domestic securities and futures firms had experienced cyber attacks which caused Taiwan bank ATMs spew out millions after hack.

How did the hackers get access to ATMs in Taiwan, and steal a total amount of over $2.5 million from the Bank without using cash cards?

This talk will review the cyber attacks and discuss how it happened and what we have learned. Cybercrime continues evolving into a holistic transnational activities. Collaboration is the key solution to fight cybercrime.
Title:
Mechanisms for Combating Cybercrimes: A Study of Algerian Legislation

Authors:
Prof. Tekarri Haifa Rachida

Affiliation:
Faculty of Law and Political Science, University Ali Lounici Blida 02, Algeria

Abstract:

إن جرائم الكمبيوتر والإنترنت، أو جرائم التكنولوجيا العالية، أو الجريمة الإلكترونية، ظاهرة إجرامية مستجدة نسبياً بحيث تتكبّل المجتمعات في الأزمة الأخيرة من انتهاك الحقوق والخصوصيات الإلكترونية، وبقاء تطور هذا النوع من الجرائم المتزايد مع التطورات التي تطرأ على التقنيات والاتصالات، التي يسرّب سبل التواصل وانتقال المعلومات بين مختلف الشعوب والحضارات وسهلة حركة الأعمال، إلا أن هذا التقدم المذهل والمميز لا يخلو من عيب، لأن استخدامه لا يقتصر على الإنسان الخيّل بل الإنسان الشرير الذي قد يوصف كمجرم سهيل سعيه وراء أطماعه وانتصافه الفرص لتحقيق أغراضه غير المشروعة، فإن يتواجد عند التقدم التكنولوجي لتطوير قدراته الإجرامية باستخدام شبكة المعلوماتية كوسيلة سهلة لتنفيذ العمليات الإجرامية، مما يلقي ضرراً بالآخرين.

وتعتبر أهمية موضوع الجرائم الإلكترونية فيانتشار الواسع لهذا النوع من الجرائم والذي رافق الاستخدام الواسع للمعاملات الإلكترونية على الصعيد الدولي والإقليمي والوطني هذا من جهة، ومن جهة أخرى فقد أصبحت الجريمة الإلكترونية متأصلة مع التطور السريع والهائل في مجال تكنولوجيا الاتصالات والعلومات، فاتجاه Developers للتقدم الكبير في استخدامات الشبكة العنكبوتية "الإنترنت"، نظم الجرائم الإلكترونية بصورة مختلفة، وأصبحت تهدد الأمن المعلوماتي للأفراد، المؤسسات والحكومات.

وبعد أن وصلت مستويات قياسية في الأعوام الأخيرة، فشلت السلطات الأمنية مجابهة الجرائم الإلكترونية على اختلاف أنواعها بقانون يعزز آليات التصدي لها، من خلال مما سبق تبرز اشكالية الربط لهذه الورقة العلمية، والتمثيلية، ما هي الجريمة الإلكترونية وما هي آليات التصدي لها؟ وتعتبر هذه الورقة آليات مكافحة الجريمة الإلكترونية كدراسة في التشريع الجزائري.
Title: Cybercrimes and the Difficulty of Implementing their Provisions

Authors: Prof. Amara El Mokhtar

Affiliation: Faculty of Law, Mohammed V University of Rabat, Morocco

Abstract: 

The advent of cybercrimes has led to the need for the development and adoption of new laws and regulations. The difficulty in implementing such provisions is evident. Cybercrimes are characterized by their ability to transcend national borders, making it challenging to adapt existing legal frameworks. This imposes a significant challenge on legal systems, particularly in the context of international law. Cybercrimes are often committed through international networks, utilizing the ease of access and capabilities provided by the internet. This makes it imperative to develop comprehensive frameworks that can be universally adopted to combat cybercrimes. The abstract delves into the challenges faced in defining and addressing the complexities of cybercrimes, emphasizing the need for a unified legal approach that can effectively respond to this emergent threat.
Title:
Identifying Laws, Legislations and Investigative Principles in the Fields of Cybercrime and Digital Evidence

Abstract:

The paper discusses the need for laws and regulations in the fields of cybercrime and digital evidence. It highlights the importance of establishing a comprehensive legal framework to address the challenges posed by cybercrime. The authors argue that existing legal frameworks are inadequate to address the complexities of modern digital crimes. They emphasize the need for international cooperation and the development of new legal principles to effectively combat cybercrime.

Authors:
Dr. Ahmed Saleh Alzahrani

Affiliation:
Public Prosecution, Saudi Arabia
Title: Criminal Responsibility for Cyber Terrorism Crimes

Authors: Dr. Khaled Hamed Moustafa

Affiliation: Department of Criminal Law, College of Criminal Justice, Naif Arab University for Security Sciences

Abstract: جرائم الإرهاب السيبراني بأنها "الأعمال غير المشروعة والتهديدات والهجمات الإلكترونية ضد جهاز الكمبيوتر والشبكات والعلومات المعززة، أو البنية التحتية الحيوية، أو الخدمات الأساسية: يتصدح أطراف الدولة أو شعوبها وإرغامها على عمل معين أو الامتثال من عملي ل لتحقيق أهداف سياسية أو إعلامية، أو إتفاق الملكية الرقمية أو الممتلكات المادية للدولة أو الأفراد. أو الاعتداء على الأشخاص عبر شبكة الإنترنت لغرض إرهابي". ومن أجل ذلك تصاحب الشبكات المعلوماتية الاتخاذية والواقعية الإلكترونية إما أسلوب تستخدمها التنظيمات الإرهابية في ارتقاء الجريمة، أو غير تؤكد فيها ما دام الهدف من الاعتداء تحقيق أغراض إرهابية، ومتناوب شروط متضرر من الجريمة ينبغي إجرائها.

كما يلعب الفضاء السيبراني دورًا بارزاً في الجريمة من خلال تقارب الفضاء السيبراني فضفاضة وسيلة يتم فيها استخدام الشبكة الاتخاذية عبر الفضاء الإلكتروني، وجعل الأخير ساحة معركة بدلاً من القتال المباشر، ومن حيث السلاح فبشرة الدعاية الإرهابية، والتطرف.
Cybercrime and Digital Forensics Forum
19-21 November 2019

Scientific Session

Wojciech Toryn, and the training to add the ideological dimension to their ideas, and to deepen the thinking of a large number of

Forum Program Scientific Session

Cybercrime and Digital Forensics Forum

Wojciech Toryn, and the training to add the ideological dimension to their ideas, and to deepen the thinking of a large number of

Forum Program Scientific Session

Cybercrime and Digital Forensics Forum

Wojciech Toryn, and the training to add the ideological dimension to their ideas, and to deepen the thinking of a large number of

Forum Program Scientific Session

Cybercrime and Digital Forensics Forum

Wojciech Toryn, and the training to add the ideological dimension to their ideas, and to deepen the thinking of a large number of

Forum Program Scientific Session

Cybercrime and Digital Forensics Forum

Wojciech Toryn, and the training to add the ideological dimension to their ideas, and to deepen the thinking of a large number of

Forum Program Scientific Session

Cybercrime and Digital Forensics Forum

Wojciech Toryn, and the training to add the ideological dimension to their ideas, and to deepen the thinking of a large number of
الجمعية العربية لعلوم الأدلة الجنائية والطب الشرعي

مجموعات العمل العلمية العربية

لتخصصات علوم الأدلة الجنائية والطب الشرعي

الأهداف:
1) توفير ونشر معايير وممارسات متطورة ومعتمدة بما يرقى بالمؤسسات العاملة في مجالات علوم الأدلة الجنائية والطب الشرعي.
2) توحيد معايير وممارسات العمل في مجالات علوم الأدلة الجنائية والطب الشرعي على المستوى العربي.
3) تنظيم الفعاليات العلمية والعملية في مجالات علوم الأدلة الجنائية والطب الشرعي.
4) المساهمة في تطوير التعليم والتدريب والبحث في مجالات علوم الأدلة الجنائية والطب الشرعي.

لتسجيل الرسوم من المعلومات:
https://asfsfm.nauus.edu.sa

nauss.edu.sa   nauus.sa   nauss_sah   info@nauss.edu.sa
Workshops
19-21 November 2019
Workshop 1
Connected Threat Defense
ورشة عمل
الدفاع المتصل ضد التهديدات

**Presenter:**
Mr. Ali Zubayd

**Affiliation:**
Cybersecurity Consultant, Trend Micro, KSA

**Workshop Purpose:**
Demonstration of how the Trend Micro Connected Threat Defense (CTD) technologies works by using End-point detection & response (EDR) to investigate the detection.

**Workshop Goals:**
To have a Proactive approach, how the malicious unknown object is detected and how intelligence is shared among different systems.

**Target Audience:**
Cybersecurity professionals are especially targeted for this content, but other professionals with IT background will find it useful.

---

**Fees:**
100 SR

**Pre Registration:**
Limited seats available

**Duration:**
1 Hour

**Date:**
19/11/2019

**Time:**
13:30-14:30
Workshop 2
Voice and Face Biometrics: How to Find and Verify People

Presenter(s):
1. Mr. Konstantin Danilov  2. Mr. Kais Boughanmi

Affiliation(s):
1. Product Manager, Speech Technology Center, Russia
2. Business Development Manager, Speech Technology Center, Russia

Workshop Purpose:
This workshop presents general information about different types of biometrics. Voice and face biometrics will be discussed in detail. Biometrics from practical perspective: why and where voice and face biometrics can be used and what values it gives to customers and users. The audience will be provided with live demo sessions where everyone will be able to create their voiceprint and faceprint and check how biometrics works in real.

Workshop Goals:
- To introduce general biometric concepts and accuracy metrics.
- To introduce key voice and face biometric characteristics and use-cases.
- To provide the audience with live demo and ability to try voice and face biometrics themselves.

Target Audience:
Anyone interested in voice and face biometrics.

Fees: 200 SR
Pre Registration: Limited seats available
Duration: Part1: 1 Hour
Part2: 1 Hour, 30 min. Discussion
Time: 13:30-14:30
14:45-16:15
Date: 19/11/2019
Workshop 3
How to build Efficiency and Reduce Time around Managing Cases and Forensic Tasks
ورشة عمل
كيفية زيادة الكفاءة وتنقيل الوقت في إدارة القضايا والمهام الجنائية

Presenter(s):
1. Dr. James Kent
2. Mr. John Nassif

Affiliation(s):
1. CEO & Co-Founder Black Rainbow Ltd, United Kingdom
2. Region Head META-APAC, Black Rainbow Ltd, Dubai, UAE

Workshop Purpose:
This workshop presents how to set up a flexible and robust approach to manage and complete cases by automating forensic applications with dynamic workflows and procedures to reduce the time to complete cases.

Workshop Goals:
- To educate investigators on the importance of having a well-established workflow and system in place for case management.
- To support the case from start to finish and provide a report.
- To summarize the key actions that have occurred in an investigation.

Target Audience:
Digital forensics investigators, technologist, digital forensics practitioner.

Fees:
100 SR

Pre Registration:
Limited seats available

Duration:
1 Hour, 30 min. Discussion

Date:
19/11/2019

Time:
14:45-16:15
Workshop 4
Next Generation Digital Forensics: Challenges and Future Paradigm

Workshop Purpose:
This workshop is intended to discuss about future trends of digital forensics and incident response with case studies and videos.

Workshop Goals:
To provide insight on how to deal with cyber incidents and address technical challenges involved in forensic cases.

Target Audience:
Cybercrime investigators, digital forensics practitioners, information security professionals and incident responders.

Presenter:
Eng. Pratap Kumar

Affiliation:
Cyberforensics Specialist, Infratech, Saudi Arabia

Fees:
100 SR

Pre Registration:
Limited seats available

Duration:
1 Hour, 30 min. Discussion

Date:
20/11/2019

Time:
10:45-12:15
Workshop 5

Humanizing Digital Forensics

ورشة عمل محاكاة الطابع البشري في الفحص الجنائي الرقمي

Presenter:
Eng. Khaled Hegazy

Affiliation:
Solution Consultant EMEA, Nuix, Australia

Workshop Purpose:
Sharing the latest techniques and methodologies for big data analysis and digital investigation.

Workshop Goals:
Attendees will understand how to link the digital forensics artifacts.

Target Audience:
Cybercrime investigators, digital forensics practitioners and incident responders.

Fees: 200 SR
Pre Registration: Limited seats available
Duration: Part1: 1 Hour, 30 min. Discussion
Part2: 1 Hour, 30 min. Discussion
Time: 10:45-12:15
13:15-14:45
Date: 20/11/2019
**Workshop 6**

**Drone Forensics**

**Workshop Purpose:**
The workshop explains how drone forensics is vital for the digital forensics and set up the process for extracting data from commercial drones and how to analyze them in a beneficial way for the course of investigation.

**Workshop Goals:**
To educate digital forensic practitioners on ways of extracting forensics artifacts from commercial drones and how to link them to suspects device. Moreover, understanding what vital data could be extracted from commercial drones and how it could be beneficial for the process of investigation.

**Target Audience:**
Digital Forensics practitioners looking into exploring the drone forensics area.

**Presenter:**
1st Lt. Khalifa Mohammad AlRoom

**Affiliation:**
Dubai Police, UAE

**Fees:** 100 SR

**Pre Registration:** Limited seats available

**Date:** 20/11/2019

**Time:** 13:15-14:45

**Duration:** 1 Hour, 30 min. Discussion
Vision
To be a leader in developing a high standard of excellence in forensic science and forensic medicine in the Arab world.

Mission
To create a scientific platform for all specialists in forensic sciences and forensic medicine who can lead scientific work in specialist areas.

ASFSFM Objectives:
The ASFSFM seeks to achieve the following:
1. Forming a distinct merge of all scientific and intellectual concepts and similarities among members of the ASFSFM.
2. Sharing knowledge and expertise in various disciplines of forensic sciences between the ASFSFM and forensic experts, institutions and bodies through academic and professional activities (meetings, conferences, symposia and workshops).
3. Offering academic and professional assistance to institutes, colleges, universities, law enforcement/planning agencies and other professional bodies to develop and improve programs and curricula related to forensic sciences, forensic medicine and security.

http://asfsfm.nauss.edu.sa  
e-mail: asfsfm@nauss.edu.sa

الرؤية
تحقيق القيادة والتميز في علوم الأدلة الجنائية والطب الشرعي.

الرسالة
إيجاد حاضنة علمية لجميع المختصين في علوم الأدلة الجنائية والطب الشرعي، تستطيع قيادة العمل العلمي المشترك في هذه التخصصات.

أهداف الجمعية
تسعى الجمعية إلى تحقيق الأهداف التالية:
1- تطوير العمل الجنائي وتعزيز الكفاءة المهنية للعاملين في مجالات علوم الأدلة الجنائية والطب الشرعي في الدول العربية.
2- تبادل التجارب والخبرات بين الجمعية والأفراد والمؤسسات المعنية بعلوم الأدلة الجنائية والطب الشرعي، لتعزيز الاستفادة من نتائج تلك التجارب والخبرات.
3- توطيد الصلات العلمية والفكرية بين أعضاء الجمعية.
Vision
To be a leader in developing a high standard of excellence in forensic science and forensic medicine in the Arab world.

Mission
To create a scientific platform for all specialists in forensic sciences and forensic medicine who can lead scientific work in specialist areas.

ASFSFM Objectives:
The ASFSFM seeks to achieve the following:
1. Forming a distinct merge of all scientific and intellectual concepts and similarities among members of the ASFSFM.
2. Sharing knowledge and expertise in various disciplines of forensic sciences between the ASFSFM and forensic experts, institutions and bodies through academic and professional activities (meetings, conferences, symposia and workshops).
3. Offering academic and professional assistance to institutes, colleges, universities, law enforcement/planning agencies and other professional bodies to develop and improve programs and curricula related to forensic sciences, forensic medicine and security.

- تطوير العمل الجنائي وتعزيز الكفاءة المهنية
1/دالة الجنائية
- تبادل التجارب والخبرات بين الجمعية وداتلية الجنائية
2/دالة الجنائية
- تعميم استفادة النتائج تلك التجارب والخبرات.
- تطوير المجلات العلمية والفكرية بين أعضاء الجمعية
3.
الإدارة العامة للأدلة الجنائية – إدارة فحص الجرائم المعلوماتية

هي الهيئة المكلفة بفحص وتحليل المحتوى الرقمي للأجهزة الإلكترونية مثل أجهزة الهواتف وأجهزة الملاحظة فيديو والصور وأجهزة المراقبة التلفزيونية المختلفة (GPS، DVR، NVR) ووسائط التخزين المختلفة المرفوعة من مسرح الجريمة أو المضبوطة من قبل جهات الضبط المختلفة والجهات الحكومية الأخرى، بالإضافة إلى مراقبة وتحليل مرور البيانات الشبكية من خلال القنوات المختلفة من الخوادم والأجهزة الطرفية ووسائل الربط الشبيك وذلك لجمع المعلومات واستخراج الأدلة القانونية بها من الدخول الف익 مصرف بـ تلك الشبكات أو الاختراق لتسجيل البيانات أو تغييرها أو تدميرها وذلك عبر برامج فحص جنائي رقمية معتمدة دولياً وأدوات أخرى مساعدة لإجراء التقارير الجنائية وفق العواقب المعمول بها دولياً، لتوصل لكل ما من شأنه خدمة الجهاد الأمني والعدالة وكذلك اقتراح الأسس والمعايير الفنية الخاصة بالجرائم الرقمية والتأكد من تطبيقها.

+966 112467777
+966 112464260

الإدارة العامة للأدلة الجنائية، الرياض، المملكة العربية السعودية
الإدارة العامة للأدلة الجنائية
إدارة فحص الجرائم المعلوماتية
Saudi Telecom Company (STC)

With its headquarter in Riyadh, STC Group is the largest in the Middle East and North Africa based on market cap. STC’s revenue for 2018 amounted to 51,963 million SAR (13,857 million US dollars) and the net profit amounted to 10,780 million SAR (2,875 million US dollars). STC was established in 1998 and currently has customers around the globe. It focuses on providing services to customers through a fiber-optic network that spans 158,000 kilometers across Asia, the Middle East and Europe. In Saudi Arabia (the group’s main operation site) STC operates the largest modern mobile network in the Middle East as it covers more than 99% of the country’s populated areas in addition to providing 4G mobile broadband to about 90% of the population across the Kingdom of Saudi Arabia. STC group was among the first in MENA region to launch 5G networks and was considered one of the fastest globally in deploying 5G network, where 196 sites in the holy regions of Makka and Madinah enabled Pilgrims to connect to the first 5G services for the first time during Hajj season 1440. Besides its main operation in Saudi Arabia, STC’s investments include 100% ownership in Viva Bahrain, 51.8% stake in Viva Kuwait, 25% stake in Binariang GSM Holding in Malaysia which owns 62% of Maxis in Malaysia. In addition to the above-mentioned, STC has a wide range of underlying investments in local companies in information technology, content, distribution, contact centers, real estate and Fintech where it supports their telecom operations and provide them with innovative services.

+966114527000  info@stc.com.sa
+966114525580  www.stc.com.sa

King Abdulaziz Complex, Mursalat, Riyadh P.O. Box 87912 Riyadh 11652
STC Cybersecurity GUARD Strategy

**VISION**
We are leaders in Cybersecurity and the MENA Center of Excellence, inspiring trust in STC and keeping the Kingdom safe.

**MISSION**
We deliver effective Cybersecurity to make STC strong and resilient.

---

**G**
- **Governance**
  - to ensure agile Cybersecurity in STC, fit for purpose and aligned to digital ways of working

**U**
- **Unification**
  - Cybersecurity approach to holistically secure the STC Group and National Telecom Infrastructure

**A**
- **Assurance**
  - to customers, shareholders and employees of the security & resilience of STC's digital footprint

---

**R**
- **Resilience**
  - of the business to disruptions caused by cyber threats and attacks

**D**
- **Defense**
  - mechanisms to proactively repel attacks and protect STC's digital perimeter
Cisco Saudi Arabia

Cisco Systems, Inc. designs and sells broad lines of products, provides services and delivers integrated solutions to develop and connect networks around the world, building the Internet. Over the last 30 plus years, we have been the world’s leader in connecting people, things and technologies—to each other and to the Internet—realizing our vision of changing the way the world works, lives, plays and learns. We have expanded to new markets that are a natural extension of our core networking business, as the network has become the platform for automating, orchestrating, integrating, and delivering an ever-increasing array of information technology (IT)–based products and services. We are focused on helping our customers achieve their desired business outcomes. Cisco customers include businesses of all sizes, public institutions, governments, and communications service providers. They look to us as a strategic partner to help them use IT to enable, differentiate, or fundamentally define their business strategy and drive growth, improve productivity, reduce costs, mitigate risk, and gain a competitive advantage in an increasingly digital world.

+966 11 813 6000

+966 11 813 6001  www.cisco.com

Cisco (Saudi Arabia) Support Limited, ITCC - Building IT01, An Nakhil 6708, Unit No 11, Ar Riyadh
Riyadh, Ar Riyadh 12382-3610, Saudi Arabia
Go From Under Siege To In Control.

Cisco. Security above everything.

The bridge to possible
TREND MICRO

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints.

All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With over 6,000 employees in over 50 countries and the world’s most advanced global threat intelligence, Trend Micro secures your connected world.

+966 11-225-3646
www.trendmicro.com
Trend Micro Saudi Arabia, Building C1, Unit 3 Ground Floor, The Business Gate, East Ring Airport Road, PO Box 33554, Riyadh 11458, Saudi Arabia
Keeping up with today’s unprecedented speed of business is a challenge. Add the onslaught of sophisticated, targeted attacks using fileless malware, ransomware, phishing, business email compromise, and cryptomining, and one thing remains clear - you need the resilience to stay ahead.

With our smart, optimized, and connected technology you can see the big picture and prepare for, withstand, and rapidly recover from threats.

That's The Art of Cybersecurity.

www.trendmicro.com
Speech Technology Center

Speech Technology Center (STC) is an international leader in speech technology and multimodal biometrics. It has over 29 years of research, development and implementation experience in Russia and internationally.

STC is leading global provider of innovative systems in high-quality recording, audio and video processing and analysis, noise cancellation, speech synthesis and recognition, and real-time, high-accuracy voice and facial biometrics solutions. STC innovations are used in both public and commercial sectors, from small expert laboratories, to large, distributed contact centers, to nation-wide security systems. STC is ISO-9001: 2008 certified.

+7 812 331 0665 stc-spb@speechpro.com
+7 812 327 9297 www.speechpro.com

Russia, 4 Krasutskogo street, St. Petersburg, 196084
Speech Technology Center – innovative solutions for audio world
Infratech

Infratech prides itself on providing the best IT Infrastructure, IT Security, and Digital Transformation services in Saudi Arabia, working with prestigious governmental and private B2B organizations including defence, security, health, finance, education and banking sectors. Infratech provides its esteemed clients with unparalleled solutions that can help streamline their business processes, secure their infrastructure, and transform them to be ready for Vision 2030.

**Mission:** Empowering the market with Revolutionary Integrated Solutions in IT Infrastructure, IT Security and Digital Transformation.

**Vision:** To be the Top IT solutions provider in the MENA Region.

92 000 9988  marketing@infratech.com.sa
+966 114449944  www.infratech.com.sa
Kingdom of Saudi Arabia, Riyadh – 12476 Uthman Ibn Affan Rd, At Taawun First floor office # 08
Protection Against Cybercrimes

Infratech is fully focused on delivering the best solutions to protect against cybercrimes.

Digital Forensics

Infratech is a leading professional forensics service provider in Saudi Arabia with vast experience in forensic technologies.

Forensics Training

Infratech offers a combination of both Computer and Digital Forensics Training covering techniques such as identifying, preserving, extracting, analyzing and reporting forensics evidence on computers and mobile devices.
MTVision

WHO WE?
MTVision is 100% Saudi company specialized in providing hi-tech, advanced and reliable security solutions from inception to completion (E2ES). In addition to preparation, rehabilitation and knowledge transfer for national cadres. Serving both public and private sectors.

WHY M ARE TVision?
We are committed to provide the required guidance to whom needed a niche capability to understand and solve these problems or requirements by delivering a competent and innovative solution through our professionals and exclusive worldwide resources.

@ info@mtvision.com.sa

🌐 www.mtvision.com.sa

📍 Saudi Arabia | Riyadh
نموذج طلب تسجيل العضوية

المعلومات الشخصية

<table>
<thead>
<tr>
<th>الاسم الكامل:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>الاسم باللغة الإنجليزية:</td>
<td></td>
</tr>
<tr>
<td>تاريخ الميلاد:</td>
<td></td>
</tr>
<tr>
<td>الجنس:</td>
<td>ذكر □ أنثى □</td>
</tr>
<tr>
<td>لقب المهني:</td>
<td></td>
</tr>
<tr>
<td>الوظيفة:</td>
<td></td>
</tr>
<tr>
<td>التخصص العام:</td>
<td></td>
</tr>
<tr>
<td>التخصص الدقيق:</td>
<td></td>
</tr>
<tr>
<td>مقر الإقامة:</td>
<td></td>
</tr>
<tr>
<td>الجنسية:</td>
<td></td>
</tr>
</tbody>
</table>

العنوان

<table>
<thead>
<tr>
<th>مقر العمل:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>صندوق البريد:</td>
<td>P.O.Box</td>
</tr>
<tr>
<td>الرمز البريدي:</td>
<td></td>
</tr>
<tr>
<td>المدينة:</td>
<td></td>
</tr>
<tr>
<td>الدولة:</td>
<td></td>
</tr>
<tr>
<td>المحمل:</td>
<td></td>
</tr>
<tr>
<td>البريد الإلكتروني:</td>
<td></td>
</tr>
<tr>
<td>الفاكس:</td>
<td></td>
</tr>
<tr>
<td>المحمول:</td>
<td></td>
</tr>
<tr>
<td>التاريخ:</td>
<td></td>
</tr>
<tr>
<td>التوقيع:</td>
<td></td>
</tr>
</tbody>
</table>

يرجى إرفاق صورة بالبريد الإلكتروني لما يلي:

- السيرة الذاتية
- خطاب من جهة العمل
- صور من الشهادات العلمية

Society Website: asfsfm.nauss.edu.sa
Society E-mail: asfsfm@nauss.edu.sa

ناجح في التقدم إلى الجمعية العربية لعلوم الأدلة الجنائية والطب الشرعي (ASFSFM)

Society E-mail: asfsfm@nauss.edu.sa
Society Website: asfsfm.nauss.edu.sa