

	ELECTRONIC EVIDENCE	DIGITAL FORENSICS	CYBER SECURITY
Breakout Rooms	London & Madrid	Oslo & Paris	Prague & Rome
09.00 - 10.00 (1 hour)	<p>KEYNOTE SPEECH BY:</p> <p>Karl Hennessee SVP of Litigation & Investigations, Airbus Group</p> <p>Development And Use of Electronic Evidence in International Arbitration</p> <p>Chill Out Zone</p>		

Current Sponsors of INsig2 LTEC 2016

TITLE SPONSOR



EXCLUSIVE PARTNER - Encrypted Communications



DINNER SPONSOR



PLATINUM SPONSORS



KEYNOTE SPONSORS



GOLD SPONSORS



SILVER SPONSORS



LANYARD SPONSOR



BAG SPONSOR



INsig2 LTEC 2016 Agenda - Tuesday, 8th November

Breakout Rooms	London & Madrid	Oslo & Paris	Prague & Rome
10.00 - 10.30	COFFEE BREAK		
10.30 - 11.20 (50 min)	<p>EE 7</p> <p>Technology, Data, And Regulation at a Crossroad: Key Trends in Our Industry</p> <p>The volume of emerging technologies is increasing, as are the ways those technologies are being used in the business world and specifically in the legal industry. Business communications now reside in myriad electronic locations and on multiple devices, increasing the complexity of data privacy and eDisclosure concerns. National lawmakers try to match the speed of these developments, but the regulatory framework is constantly moving. This session will explore the key corporate and industry trends that are impacting the eDisclosure industry.</p> <p>Presenter: Adi Elliott, Epiq Systems</p>	<p>DF 7</p> <p>Digital Forensics 101 – The Basic Forensics Process And Framework From Start to Finish</p> <p>New to Digital Forensics? This is the session for you! During this session, the panelists will discuss the forensics process of planning, information acquisition, analysing, and reporting. Investigators essentially recover and analyse digital evidence to support or disprove a hypothesis in civil and criminal proceedings. Within the context of an investigation, forensic specialists and the tools for acquisition and analysis are selected based on the specific circumstances of the case. At the completion of an investigation, a report laying out the findings is prepared. Join us for a basic but detailed discussion of the process and framework from start to finish.</p> <p>Presenter: Michal Koczwar, ASOS</p>	<p>CS 7</p> <p>Is It All About The Money? – What Are The Motivations Behind Recent Attacks And How Resilient Are Your Internal Controls?</p> <p>Money is arguably the prime motivator for cyber-attacks as it is estimated that they will become a \$2.1 trillion “industry” by 2019. However, believing that an attack is motivated only by profit could result in a false sense of security for organisations that are small private entities or the like. Thus, it is important to know that other compelling motivators are equally as appealing and include industrial espionage, sabotage, revenge, envy, political ideology, recognition, and the list goes on. Join this panel session for a more in-depth discussion of the motivations behind cyber-attacks and the internal controls that should be in place to prevent them.</p> <p>Moderator: Anca Plovie, Nokia</p> <p>Panelists: William De Riemaeker, Buyle Legal Sergey Martynov, MS Business Security Consulting Oy Ton van Gessel, SYBER Ina Kroi, EASE S.A.</p>
11.30 - 12.20 (50 min)	<p>EE 8</p> <p>Semantic Analysis for eDiscovery</p> <p>Robust early case assessment and search term identification have been critical competencies within eDiscovery for a long time. However, the volume of analysed text data grows rapidly and multi-language litigations are becoming more and more common. Therefore, traditional approaches are getting costly and less practical. To discover patterns and trends in the data, it is no longer possible to rely on manual analysis only. This session introduces the state-of-the-art methods for both automated unstructured content analysis and search term identification in large document sets. We will show advanced approaches to text data processing, including very complex languages, and explain how to employ these methods, e.g., in an effective search term expansion. Also, we will give examples illustrating the time and cost savings gained when combining the latest results of academic research with their real-life applications.</p> <p>Presenter(s): Jan Balatka, Deloitte Kateřina Veselovská, Deloitte</p>	<p>DF 8</p> <p>Anatomy of a Security Breach</p> <p>Attorneys around the world are being targeted. This presentation will contain a case study on a recent breach. It will address weaknesses in the environment and how not to become the next Panama Papers.</p> <p>Presenter: Robert Moody, Forensic Data Services</p>	<p>CS 8</p> <p>Cyber Insurance – Advantages And Disadvantages</p> <p>In a world where cyber risks are ever-increasing, interest in cyber insurance has risen dramatically. But do the benefits really outweigh the costs? Do the policies provide adequate coverage? What are the exclusions? Is the claims process straightforward or complicated? This panel discusses the advantages and disadvantages of cyber insurance.</p> <p>Moderator: Cameron Brown, Independent Cyber Defence Advisor</p> <p>Panelist: Sebastian Hess, Isabel Group Özkan Demiröz, Demiroz Consultancy Stéphanie De Smedt, LOYENS & LOEFF James Tuplin, QBE European Operations</p>
12.30 - 13.30	LUNCH BREAK		

INsig2 LTEC 2016 Agenda - Tuesday, 8th November

Breakout Rooms	London & Madrid	Oslo & Paris	Prague & Rome
	EE 9	DF 9	CS 9
13.30 - 14.20 (50 min)	<p>Law Firm Management of Electronic Evidence in Relation to Client Information, Confidentiality, Integrity, And Availability</p> <p>In addition to protecting clients' personal information, law firms must protect electronically stored confidential client information and attorney-client privilege in electronic communications. To prevent non-authorised public disclosure, law firms should utilise available electronic tools, best practices, and internal control measures. Various law bar associations have dedicated resources to preserving the safety, integrity, and availability of electronic correspondence between law firms and their clients. The impact on law firms can be devastating as evidenced in the recent Panama Papers case, LuxLeaks, and other similar cases. The acceptance of electronic correspondence as legitimate evidence, the common practice of public courts and alternative dispute resolution cases, also provides a challenge for law firms. Join this panel session for a discussion of the challenges associated with the management of electronic evidence as related to sensitive client information.</p> <p>Moderator: Vitaly Bondar, ChristmannSchmitt</p> <p>Panelist: Andrew Rice, Hitachi Capital (UK) PLC Satya Staes Polet, Freshfields Bruckhaus Deringer</p>	<p>Image, Video, And Sound Forensics – Advanced Techniques Used in Separating Authentic Evidence From What is Not</p> <p>Within video, image, and audio forensics, sometimes the question is asked if the recordings are authentic or not. There are several tools available to determine the authenticity of the multimedia stored. For a forensic case it is advised to analyze features of the multimedia material if there have been manipulations of the evidence. Check lists can be used for this. A replay of the recording is much harder to prove, and also one should consider the time and expertise needed to make a good manipulation.</p> <p>Moderator: Zeno Geradts, Netherlands Forensic Institute</p> <p>Panelist: Stefan Petrushevski, UL Nick Rich, Stroz Friedberg Adam Stogdale, Deloitte</p>	<p>ISO 27001 And PCI DSS Compliance – Banks, Merchants, And Service Providers - Security Policies For The Modern IT Landscape</p> <p>Navigating the expanding landscape of information security standards like ISO 27001 and PCI DSS can be a challenge as computing and communication devices, technologies, and trends change. Very few organisations are now immune to vulnerabilities, as well as threats and risks, such as disruption to business, fines, and reputational damage. Join the panel session to learn how to assess your options, get strong, quick wins, identify the standards and certifications that might best meet your needs, and form the basis for any necessary action that, depending on the nature of the organisation, can go well beyond the needs of the standard itself.</p> <p>Moderator: David Carvalho, OCS Group</p> <p>Panelist: James Mckinlay, Independent Security Consultant Sudaman Thoppan, BNP Paribas Fortis Mubarak Dirie, Simply Business</p>
14.30 - 15.20 (50 min)		DF 10	CS 10
		<p>Exploring Advanced Visual Analytics And Artificial Intelligence in Forensic Examinations</p> <p>During a forensic investigation it is critical that examiners process data as quickly and efficiently as possible. Without advanced visual analytics (AVA) and artificial intelligence (AI), this would be virtually impossible as it would take an enormous amount of time to investigate complex data sets from multiple sources. With AVA and AI, examiners can quickly find areas of concern and detect corruption, noncompliance, and fraud. Join this panel session for a thorough discussion of how forensic examiners use AVA and AI during an investigation.</p> <p>Moderator: Adrianus Warmenhoven, RedSocks</p> <p>Panelists: Steve Couling, kCura Mattias Aggeler, Swiss FTS Sudaman Thoppan, BNP Paribas Fortis Cécile De Barys, Kurt Salmon Luxembourg</p>	<p>Mobile Device Security – Nightmares And Solutions For The CIO in The Era of “Always Connected” And Cloud Applications</p> <p>Today's CIO's are faced with the challenge of integrating effective security and privacy in mobile devices. The never-ending release of new devices AND new malware, means ongoing vigilance including monitoring, cooperation, testing, education, policy updates, and keeping abreast of the new technologies that exist to combat attacks. Join this panel session for a discussion of the issues CIO's face and the possible solutions.</p> <p>Moderator: Guy Kindermans, Belgian IT Journalist</p> <p>Panelist: David Carvalho, OCS Group Andrew Rice, Hitachi Capital (UK) PLC João Torres Barreiro, HCL Technologies Michael Meixner, Computerforensic & more GmbH Stefan Petrushevski, UL</p>
15.20 - 16.00	COFFEE BREAK and EVENT CLOSE		