Forensic Experts

Digital Experience Nordics March 24th, 2020 – Stockholm

Registration

| 09.30 - | 10.00 | Registration |

Opening & Keynote

| 10.00 - | 10.15 | Opening Digital Experience Nordics – **Christian Almstedt - Forensic Experts Scandinavia** |

| 10.15 - | 11.15 | Keynote: ***Towards Predictive Threat Intelligence - Staffan Truvé, Recorded Future***
Having actionable threat intelligence knowledge across threat prevention, third-party risk management, and brand protection strategies can be a most effective way for every security function to save time, money, and effort — and ultimately, accelerate risk reduction. This talk describes how to produce descriptive threat intelligence - what threats are present today - and how to move towards predictive threat intelligence - to know what will be important to prepare to defend against tomorrow. |

Break

| **11.15 -** | **11.45** | ***Networking break***
Please visit the booths of our partners at the exhibition floor! |

Sessions		Room 4	Room 5	Room 6
11.45 -	12.30	*Financial Crime Analysis with IBM i2 - DataExpert*	*Messenger Forensics. Evidence Hide-and-Seek – Oxygen Forensics*	*Keeping up with cybercrime evolution through education - DataExpert*

Lunch

| **12.30 -** | **13.15** | ***Networking break***
Please visit the booths of our partners at the exhibition floor! |

Sessions		Room 4	Room 5	Room 6
13.15 -	14.00	*GEOINT – Point Duty*	*T3K LEAP - Automated Analysis and Reporting of Large Amounts of Data – T3K*	*Security Intelligence. Applied Cyber Threat Intelligence – Recorded Future*

		Room 4	Room 5	Room 6	Room 7
14.00 -	14.45	*What's new in Digital Forensics? - DataExpert*	*Password trends, Passware news and Decryptum - Passware*	*CyberRange Simulation, put your cybercrime knowledge to the test! – DataExpert & Cyberbit*	*Mapping the European network associated with the Islamic Revolutionary Guard Corps (IRGC) – Qods Force - Paliscope*

Break

| **14.45 -** | **15.15** | ***Networking break***
Please visit the booths of our partners at the exhibition floor! |

Sessions		Room 4	Room 5	Room 6	Room 7
15.15 -	16.00	*How successfully implementing Triage to your forensic workflow can help minimize your digital exhibit backlog – Evidence Talks*	*Magnet Forensics*	*Video Forensics Casework: Issues, Solution, Trends – Amped Software*	*Darknet Intelligence - Explore Web-IQ's DarkCloud – Web-IQ*

Refreshments

| **16.00** | | **Networking drinks** |

Workshops:

11.45 – 12.30

Room 4	**Financial Crime Analysis with IBM i2 –** Karlijn Cox, Senior Consultant Analytics, DataExpert

Find out how IBM i2 technology helps financial crime investigators to solve and prevent (attempted) fraud while building a strong case against past fraudulent activity and improper transactions. During this demonstration we will showcase how frequent financial crime investigation questions can be answered using IBM i2 technology.

Room 5	**Messenger Forensics. Evidence Hide-and-Seek.**- Tanya Pankova, Oxygen Forensics

Messengers nowadays are without doubt a primary source of digital evidence storing a tremendous amount of user data including chats, shared files, geo locations, contacts, and many other artifacts. Due to the limitation of the current mobile device extraction methods, sophisticated app encryption and app features that include self-destruct messages and hidden chats getting this valuable evidence has already become a great challenge for investigators.

In this session we will talk a wide range of messengers, like WhatsApp, Viber, Telegram, Facebook, Signal, Wickr Me, Threema, etc. that are popular not only with law-abiding users but also with drug dealers, terrorists, and people sharing sexual abuse images. We will examine their encryption algorithms, secret and hidden chats, and alternative extraction methods from computer and cloud including some methods exclusively available in Oxygen Forensic® Detective software.

Room 6	**Keeping up with cybercrime evolution through education** – Niels Hilderink, Cybersecurity & Digital Forensic Specialist, DataExpert

Comparing the fight against cybercrime to winning a race, you might realise that most of the time we are lagging behind the bad guys. Victory remains unreachable and even when you manage to get ahead of the criminals, they will surely find a new way to get ahead again.

At the DataExpert Academy we firmly believe in teaching to win the cybercrime race. Not only do we prepare students for the race, we make sure they can keep up with the race and successfully win it in the long run: either as an investigator or from any other thinkable role. During this session you will learn how DataExpert can supply the right knowledge to combat cybercrime.

13.15 – 14.00

Room 4	**GEOINT** – Jordan Summerfield, Point Duty

Network visualisations, timeline analysis, trend insights.. You probably use them in your analysis more than often. Many of these essential pieces of information hold unused location intelligence. What do you do to make these pieces of information actionable? In most occurrences this location-data withhold viable information and the possibility to interpret your case data even better. Think of heatmaps, crime scene visualisation, (mobile) phone analysis, movements etc. Are you not yet aware of the GEOINT applications possible in IBM i2 Analyst's Notebook? Discover these possibilities during this session!

Room 5	**T3K LEAP - Automated Analysis and Reporting of Large Amounts of Data –** Martina Tschapka, Project Management, T3K

With the advance of technical development, smartphones contain more and more data, so the focused search for evidence in mobile forensic investigations become increasingly difficult.

The manual inspection of seized data binds ever more resources, leading to shortages in staff and consequently backlogs. With the development of LEAP, T3K set out to revolutionize the analysis of big amounts of data, by automating time-consuming work through the usage of an artificial intelligence. Whether it is locations and routes, contacts, languages, links between persons, or the photos and videos found on a person's phone, LEAP will produce a standardized PDF and HTML report, enabling investigators and even case workers to decide whether a phone needs to be inspected more closely, thus minimizing the time a mobile forensic expert needs to spend with devices that don't indicate criminally relevant data. LEAP lets the user help identify a person for immigration purposes, but also detect criminal activities, such as Human trafficking or Drug-related crime, and a big focus also lies on detecting Crimes against Children.

Room 6	**Security Intelligence - Applied Cyber Threat Intelligence –** Magnus Lundgren, Recorded Future

In today's rapidly changing and stealthy threat environment, knowing what's happening inside your organization is not enough. Recorded Future arms every department with relevant security intelligence to lower risk.

14.00 – 14.45

Room 4 | **What's new in Digital Forensics?** – Erik Boerboom & Helmi van den Brink, DataExpert

This session is perfect if you want to learn more about the latest tools and trends in Digital Forensics. In this non-technical session DataExpert's Forensic Expert Erik Boerboom and Forensic Consultant Helmi van den Brink will discuss the challenges and the latest solutions on the market. Topics that will be presented are around Mobile Forensics, Triage and Video Analysis.

Room 5 | **Password trends, Passware news and Decryptum -** Toni Pärn, Passware

We will go over the findings of our analysis of leaked passwords. We will do live examples on how to decrypt certain files, share Passware product updates and training. Introduce Decryptum – liquid cooled GPU accelerated devices for password recovery.

Room 6 | **CyberRange Simulation, put your cybercrime knowledge to the test!** – Joost Gijzel, Cyber Security Specialist, DataExpert

With CyberRange you can experience how cyberattacks are done and practice your own (Incident) Response and research techniques. CyberRange also provides the possibility to specific train attacks and Red-Blue teaming. CyberRange is a modular system and provides the possibility to recreate specific (also OT) settings which makes it extremely suitable for tailored investigations or offensive trainings.
During this session we will show you the technical possibilities of CyberRange and how it can help you within your current daily investigations and trainings.
We will give a short showcase of the simulation platform, available scenario's, modules, student programs and we ask you for feedback to keep developing this product/services to suit your needs!

Room 7 | **Mapping the European network associated with the Islamic Revolutionary Guard Corps (IRGC) – Qods Force -** Paliscope

The rise in terrorism has resulted in an increased need to map terrorist and state-linked espionage networks with expert precision and efficiency. At the same time, there's a need for an easier way to identify and catalogue individuals associated with malign groups. This demonstration will show you how Paliscope's products were used to build a picture of Qods Force.

15.15 – 16.00

Room 4 | **How successfully implementing Triage to your forensic workflow can help minimize your digital exhibit backlog -** James Buckland & Shane Barnes, Evidence Talks

DataExpert is delighted to host James Buckland and Shane Barnes from Evidence Talks, on the topic of triage for a 1 day hands on session to run through best practice, the benefits and risks of triage, and why Evidence Talks developed SPEKTOR for his investigations.
Around the world Digital Forensic labs are overwhelmed with submissions and the traditional process of full forensics on everything no longer scales to match the demands put on the forensic examiners. Triage is a widely adopted process in the UK & US to enable law enforcement to quickly check if there is something of importance or interest on a device. The triage process can be undertaken in the field or back in the lab by other teams, freeing up the forensic examiners time to focus on the most important exhibits.
At this session:
- *You will learn the principles of adopting a triage process into your workflow.*
- *Types of examinations and circumstances where triage is particularly beneficial*
- *How using SPEKTOR you can lockdown the triage process to minimize risk and avoid human error*
- *How SPEKTOR can enable the triage of multiple exhibits at one time.*

Room 5 | **Magnet Forensics**

More information will follow

Room 6 | **Video Forensics Casework: Issues, Solution, Trends** – Martino Jerian, Amped Software

In this presentation, Amped Software shares the results of an internal study covering casework received over the years by their support team.
Key questions analysed include:
- *What are the most common requests for video analysis?*
- *What are the most common scenarios and sources of image and video data during investigations?*
- *What are the most problematic video formats?*
- *What are the biggest quality issues and the rate of success?*
- *How are technology trends evolving over the years?*

This will help stakeholders to better understand scenarios, issues, and chances of success for image and video forensics activities. It will also help the research community to understand today's challenges and, possibly, focus efforts on solving them.

Room 7   **Darknet Intelligence - Explore Web-IQ's DarkCloud -** Annemarie Brockmöller, Program manager CSE & intel analyst, Web IQ

Do you know what happened on the Darknet today? Are you aware of potential perpetrators threatening your country, city or organization? Get notified by DarkCloud service and drill down to threats.
We are continuously monitoring thousands of Darknet sources and have a clear overview of the darknet markets and other trends and threats. We harvest and structure the data into actionable intelligence that is made available via a user friendly search interface and via API for integration with other monitoring services.
We call it Darknet Intelligence as a Service.