Digital Experience België, 5 oktober 2020 – Brussel

Registratie

08.30 - 09.00 Ontvangst & registratie

Opening & Keynote

09.00 - 09.15 u Opening Digital Experience België

09.15 - 10.45 u **Keynote: Frank van de Goot, Forensisch Patholoog; TUNNELVISIE in de opsporing**

Forensisch Patholoog Frank van de Goot is een zeer gerenommeerd deskundige in het forensisch vakgebied. Met name wanneer het gaat om moord- of zelfmoorddossiers waarbij sectie verricht moet worden, wordt er met grote regelmaat een beroep op hem gedaan. Hierdoor is hij zeer geregeld betrokken bij spraakmakende onderzoeken, waarbij de situatie niet altijd is wat het lijkt. In deze enerverende keynote neemt Frank u mee aan de hand van een aantal treffende voorbeelden uit de praktijk, waarbij het risico van aannames en tunnelvisie aanwezig zijn. Juist door deze unieke inkijk in de wereld van forensisch medisch onderzoek wordt u op een prettige en onderhoudende wijze meegenomen in een boeiende zoektocht naar de waarheid.

Koffie pauze

10.45 - 11.15 u ***Netwerk pauze - Bezoek de stands van onze partners!***

Sessies	Diamond	Emerald - Ruby	Jade - Sapphire	Aquamarine
11.15 - 12.00 u	*Financiële criminaliteit bestrijden - DataExpert*	*Messenger Forensics. Evidence Hide-and-Seek – Oxygen Forensics*	*Win de race tegen cybercrime voor door middel van educatie - DataExpert*	*LEAP - Automated Analysis and Reporting of Large Amounts of Data – T3K*

Lunch

12.00 - 13.00 u ***Netwerk Lunch - Bezoek de stands van onze partners!***

Sessies	Diamond	Emerald - Ruby	Jade - Sapphire
13.00 - 13.45 u	*GEOINT – DataExpert*	*Physical acquisition from iOS devices. New approaches and possibilities - Elcomsoft*	*Current trends in European eDiscovery Technology and approaches - Forcyd*
	Diamond	**Emerald - Ruby**	**Jade - Sapphire**
14.00 - 14.45 u	*Multi fusion and Multi Source intelligence - IBM*	*Check out the latest updates of EnCase Forensic and Tableau - OpenText*	*CyberRange simulatie, breng uw cybercrime kennis in de praktijk - DataExpert*

Pauze

14.45 - 15.15 u ***Netwerk pauze - Bezoek de stands van onze partners!***

Sessies	Diamond	Emerald - Ruby	Jade - Sapphire
15.15 - 16.00 u	*How successfully implementing Triage to your forensic workflow can help minimize your digital exhibit backlog – Evidence Talks*	*Recovering Mac Data 'live' in 2020 – BlackBag Technologies*	*macOS: Forensic Artifacts and Techniques that are Essential for Mac Investigations - Magnet Forensics*

Afsluiting & borrel

16.00 u **Afsluiting / borrel**

Workshops:

11.15 – 12.00 u

Diamond

Financiële criminaliteit bestrijden met IBM I2 – Karlijn Cox, Senior Consultant, DataExpert

Ontdek hoe de technologie van IBM i2 kan helpen bij onderzoek naar fraude en andere vormen van financiële criminaliteit. Met deze krachtige analyse tooling kunnen verschillende typen data gecombineerd worden ten behoeve van detectie van frauduleuze transacties en preventie van toekomstige frauduleuze handelingen.
Tijdens deze sessie laten we zien hoe veel voorkomende vragen met betrekking tot financieel onderzoek kunnen worden opgelost door het gebruik van IBM i2. ***Deze sessie is in het Nederlands****.*

Emerald - Ruby

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. ***This session is in English****.*

Jade - Sapphire

Win de race tegen cybercrime voor door middel van educatie! – Sjoerd van der Meulen, Cybersecurity Specialist, DataExpert

Als we de strijd tegen cybercrime vergelijken met het winnen van een race, moeten we ons realiseren dat we vaak net een stap achter de boeven aanlopen. De winst blijft steeds buiten bereik en zelfs wanneer we de criminelen een keer inhalen, vinden ze wel weer een nieuwe manier om vals te spelen.
Bij de DataExpert Academy geloven we sterk in de kracht van onderwijzen om de cybercrime race te winnen. Niet alleen bereiden we de studenten voor op de race, we zorgen ervoor dat ze de race volhouden en op lange termijn zullen winnen!
Tijdens deze sessie ziet u hoe DataExpert u de juiste kennis kan leren om cybercrime tegen te gaan. ***Deze sessie is in het Nederlands****.*

Aquamarine

T3K LEAP - Automated Analysis and Reporting of Large Amounts of Data – Rob de Loenen, 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. ***This session is in English***

13.00 – 13.45 u

Diamond	**GEOINT –** GEO Intelligence Specialist, DataExpert
	Netwerkvisualisaties, tijdlijn analyses, trendinzichten.. U gebruikt ze waarschijnlijk in uw analyse werk meer dan eens. Veel van deze informatie bevat ongebruikte locatiegegevens. Wat doet u met deze gegevens? Vaak herbergen deze locatiegegevens een schat van informatie en de mogelijkheid om data extra te duiden. Denk aan heatmaps, plaats delict visualisatie, (mobiele) telefoon analyse, verplaatsingen etc. Bent u nog niet bekend met de GEOINT toepassingen in IBM i2 Analyst's Notebook? Ontdek de mogelijkheden in deze GEO gerichte sessie! ***Deze sessie is in het Nederlands****.*
Emerald-Ruby	**Physical acquisition from iOS devices. New approaches and possibilities –** Alexey Shtol, Elcomsoft
	Physical acquisition is an essential part of mobile forensics. Some data on mobile devices is device-encrypted, and can be extracted with physical acquisition only. A jailbreak is required to access and decrypt hardware-protected data. The jailbreaking is a complex procedure with multiple implications. Jailbreaks tamper the system's security features, and may leave traces behind even after they are removed. I will discuss the two innovative jailbreak types: the rootless jailbreak and the newest generation of jailbreaks based on the unpatchable bootrom exploit. Both of these jailbreak types have their share of pros and contras. ***This session is in English***
Jade - Sapphire	**Current trends in European eDiscovery Technology and approaches -** Forcyd
	From internal investigations to white collar crime, cartels and regulatory enforcement. ***Deze sessie kan in het Nederlands of Engels worden gegeven.****.*

14.00 – 14.45 u

Diamond	**Multi fusion and Multi source intelligence –** Raf Verhoogen, Solution Specialist, IBM
	Together with partners IBM has created an implementation where data is coming from different sources that are fused for analysis. The session will cover the architecture of the solution. A demo of a concrete case will show this solution in action. We will investigate the disappearance of 20 students in Columbia. ***This session is in English***
Emerald-Ruby	**Check out the latest updates of EnCase Forensic and Tableau** – Stephen Gregory, Principal Forensic Solutions Consultant, OpenText
	This session discusses the latest updates to OpenText forensic products and a hint of what's to come. ***This session is in English***
Jade - Sapphire	**CyberRange simulatie, breng uw cybercrime kennis in de praktijk** – Joost Gijzel, Cybersecurity Specialist, DataExpert
	Vanaf 2020 biedt de DataExpert CyberRange u de mogelijkheid om uw cyberkennis in een veilige omgeving in de praktijk te brengen. Met CyberRange kunt u aan den lijven ervaren hoe cyberaanvallen worden uitgevoerd, en hierop uw Response en onderzoekstechnieken toepassen. Ook biedt CyberRange de mogelijkheid om juist aanvalstechnieken en Red-Blue teaming te trainen. CyberRange is modulair opgebouwd en biedt de mogelijkheid om specifieke (ook OT) omgevingen in na te bouwen, waardoor het uitermate geschikt is voor maatwerk binnen opsporing. *In deze sessie zal worden ingegaan op de technische mogelijkheden en op wat simulatie training in de praktijk toevoegt aan uw huidige trainingen/opleiding.* *Er wordt een korte showcase gegeven van het simulatieplatform, de beschikbare scenario's, modules en programma's worden doorlopen, en u we bieden u de mogelijkheid om feedback te geven op het belang/ontwikkeling voor opsporing.* ***Deze sessie is in het Nederlands****.*

15.15 – 16.00 u

Diamond

How successfully implementing Triage to your forensic workflow can help minimize your digital exhibit backlog – Andrew Sheldon & James Buckland, Evidence Talks

DataExpert is delighted to host Andrew Sheldon, an International expert on the topic of triage for a session to run through best practice, the benefits and risks of triage, and why he 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*

This session is in English

Emerald-Ruby

Recovering Mac Data 'live' in 2020 – Tim Thorne, BlackBag Technologies

MacQuisition continues to evolve at pace and remains the most comprehensive forensic imaging and triage tool for Macs. MacQuisition is the only tool to provide examiners with Physical Decrypted Images from T2 Macs, thereby ensuring that you do not miss out on thousands of files that will not be collected by our competitors who can still only give you 'logical data' from T2 and Fusion Drive Macs. ***This session is in English***

Jade - Sapphire

macOS: Forensic Artifacts and Techniques that are Essential for Mac Investigations – Marco Klockenkämper, Solution Consultant, Magnet Forensics

Mac investigations can be challenging for a number of reasons. Learn about the Apple File System (APFS) and the changes made as part of the update from HFS+, while discussing the best techniques for successfully completing macOS investigations in Magnet AXIOM. In this lab we will not only discuss changes made with the latest macOS 10.15 (Catalina) update, but also investigate operating system artifacts and files such as: KnowledgeC.db, FSEvents, Volume Mount Points, Quarantined Files, AirDrop and bash history, providing context on how these artifacts will help connect the dots in your investigations.