DataExpert Academy

Training Courses

Digital Forensics
Data Analytics
OSINT
Cryptocurrency
Cybercrime
Cyber Security

As an expert in the field of data analytics & visualisation, digital forensics, incident response, and cyber security, DataExpert also offers up-to-date specialised training courses. DataExpert provides training at product level, but also in the areas of cybercrime, cryptocurrency, cyber security, and OSINT. Custom training and training on the job are also possible. Our teachers have years of experience in the field and as trainers and bring in practical knowledge.

To get the best result from yourself and the tools you work with on a daily basis, training is essential. The DataExpert training courses ensure that you can work with confidence. At our modern training centre in Veenendaal we host our training courses, but we also offer training courses including laptops and other training materials on location. A number of trainings can also be hosted online. DataExpert's e-learning platform supports our training courses.

Would you like to receive more information, don't hesitate to get in touch with us

Meaning symbols

- Classroom training
- Online training
- SPEN accredited

Table of Contents

DataExpert

Analytics

The diversity, volume, and speed at which data and crime are evolving significantly increase the complexity of data analysis in crime fighting. Not only exploring, storing and interpreting data but also finding connections and patterns in data are becoming increasingly difficult and time consuming. Performing in-depth analysis, as well as adding information from various offline or online digital data sources, such as Dark/ DeepWeb and Social Media, are essential steps in the (data) analytics process.

The Analytics training courses provide insight and skills in the field of data analytics, using different technologies. The aim of the training courses is to be able to extract as much relevant intelligence as possible from data sourced from OSINT-, telecom-, cyber- , and financial- investigations with the right skills, knowledge and technology.

Analytics

i2 Analyst's Notebook

During this four-day training course, you will learn how to use i2 Analyst's Notebook as a tool in answering complex questions such as 'Find out if there is a connection between a series of burglaries and a series of telephone conversations'. The examples and issues are derived from law enforcement cases (car theft, drug transport, and robbery) and from the financial sector cases(fraud, money laundering, skimming, money laundering). You need to be using i2 Analyst's Notebook in your work to register.

For whom is this training intended?

The training is intended for researchers and analysts who are (or will be) involved in visualizing and (in-depth) analyzing research data (for tactical, strategic, or operational analysis). i2 Analyst's Notebook is mainly used (usually in combination with iBase User) by analysts from the police, army, large private or government organizations, banks, non-profits, and insurance companies.

What do you learn during the training?

- Build timelines manually or by importing data from structured data format files.
- Build network charts manually or by importing data from structured data format files.
- Import large amounts of data such as telephone calls and financial transactions from Excel and text files.
- Apply several layout options to charts, such as Peacock Layout, Grouped by Time Layout, and Minimise Crossed Links Layout.
- Use several search options, such as customized Visual Search, List Items, and the Search Function.
- Use advanced Barcharts and Histograms functionalities to analyze complex charts and discover trends and anomalies. e.g. the HeatMatrix Analysis and Time Wheel are powerful ways to gain new insights.
- Search for duplicate entities with Smart Matching and solve entity conflicts by using Merge Entities.
- Recognize the most important players in a complex scheme with Social Network Analysis.
- Gain insight into the chart by using list items and analysis attributes.
- Apply Conditional Formatting rules (standard and custom) to reveal important information in the right context and to (automatically) outline relevant information.

Please note: We advise you to do this training before starting iBase User training.

DataExpert

i2 iBase User

In this training, you will learn to use relational databases in which all data relevant to your research can be entered, both manually and via import. You will also learn to search and analyze the data using Browse, Find, Queries, Search 360, Scored Matching, Create Sets, and export data (to Analyst's Notebook).

i2 iBase is an intuitive relational database that allows you to store, visualize, and explore data imported from a variety of sources in a structured format. In combination with i2 Analyst's Notebook, you are equipped with powerful technology for solving difficult crime cases, faster. In this four-day training course, you will learn how i2 iBase can be used as a tool for answering questions such as 'Find out if the people who meet the individual's profile may know each other'. The examples and exercises are derived from law enforcement cases (car theft an drug transport) and the financial sector (fraud and money laundering). The training takes 3 days of training and a refresher day a few weeks later. This allows you to bring in a use case, learn tricks, and get tips that apply to your daily activities.

For whom is this training intended?

Investigators and analysts who are or will be importing, analysing, and relationally visualising data (for example, operational analysis). i2 iBase User is used (usually in combination with i2 Analyst's Notebook) by investigators and analysts, defense, and larger commercial and government institutions.

What do you learn during the training?

- Create new records by entering data manually in the fields of entities and links.
- Perform extensive data searches, including Browse, Visual Queries, 360 Search, and Scored Matching.
- Display records, compare, sort, and search for duplicate data, etc.
- Display data in an i2 iBase Link Chart and i2 Analyst's Notebook.
- Integrate the data into i2 Analyst's Notebook and create charts from i2 iBase.
- Set labels to entities in i2 Analyst's Notebook by using Labelling schemes.
- Perform basic calculations with the data.
- Enter data with data sheets, making data entry more efficient and less error-prone.
- Import records from a text file or another application such as MS Excel.
- Edit or delete large numbers of records.
- Generate reports.
- Export records.

Additional information

We advise you to do this training following the i2 Analyst's Notebook training.

i2 iBase Designer

With i2 iBase Designer, you can design relational databases to store all data relevant to your investigation into and to enable analysis tools. During this four-day training, you will learn how to design databases in i2 iBase that meet analysts' needs. This involves designing the database to match the data, enabling and indexing settings and tools and managing the rights to the data(base).

The examples and issues come from a variety of fields with various types and forms of data, including financial data, telecoms data, ICT data, forensic data, and personal data.

The training takes 3 days of training and a refresher day a few weeks later. This allows for you to bring in a use case learn tricks and get tips that apply to your daily activities.

For whom is this training intended?

The course is designed for database designers and analysts who are or will be involved in designing, creating, and managing a relational database. In practice, i2 iBase Designer is mainly used (usually in combination with i2 Analyst's Notebook) by analysts from the police, defense, large private or government organisations, banks, non-profits, and insurance companies.

What do you learn during the training?

- Designing a relational data model.
- Designing an iBase database, including multiple options for Security and Audit Levels.
- Creating the iBase database based on this design.
- Creating entities and links with associated semantic meanings.
- Creating different types of fields, including calculation fields, discriminator fields, index fields, and standard fields.
- Adding attachments and degrees of certainty to fields.
- Indexing word search and search 360.
- Labelling schemes and creating chart attributes.
- Designing data sheets making input more efficient and less prone to error.
- Import records from structured data formats. Building, scheduling, and storing these import specifications for reuse.
- Creating a template from a database.
- Repairing, compressing, managing, and controlling a database.
- Managing and securing a database.

Additional information

This training has been modified and now only covers database design and not usage. i2 iBase User knowledge is expected as prior knowledge for participation in this training.

DataExpert

Application Management for i2 iBase and i2 Analyst's Notebook

The questions that Functional Managers encounter when setting up and managing the i2 iBase and i2 Analyst's Notebook products transformed DataExpert into a one-day training course in which frequently asked questions are answered and the technical aspects of i2 iBase and i2 Analyst's Notebook are highlighted.

For whom is this training intended?

Functional Managers who want to gain insight into:

- how do I configure i2 iBase & i2 Analyst's Notebook for the network?
- which functions are available?
- how do I deal with backups?

What do you learn during the training?

i2 iBase:

- Security files and databases, Access and SQL Server databases, file extensions, SQL Server clients and network servers, user profile information, optional paths for users.
- Authorisation management: rights to the database, security files, users and groups, the use of SCC codes.
- Databases: creating databases via templates, creating a case-controlled database, using subsets. Soft delete, batch delete, SQL Server connection settings, move SQL Server databases. Which files require a backup, update database scheme, scheme and link integrity check, plug-ins and Bluebase.
- Setup and use of extra functions: alerting, search 360, installation on SQL Server and Client, SQL Server Agent, auditing, iBase Scheduler for batch imports and exports, bulk import.

i2 Analyst's Notebook:

- Installation structure.
- Optional paths for users.
- Plug-ins.
- Own icons and templates.
- Import specifications and batch imports.
- Spelling checker and timeline in Dutch date format.

Additional information

The course is taught in English and can be offered online or in classroom setup.

Maltego Fundamentals

Maltego is one of the most widely used OSINT tools worldwide for collecting, connecting and analysing online public information. The software is characterised by its graphical link analysis interface and the many transforms that allow the integration of other tooling through API access, including Virus Total, PiPl, ShadowDragon, Att&ck and more. Additionally, exported data from i2 Analyst's Notebook can be enriched using Maltego and further analysis can then take place in i2 Analyst's Notebook based on data obtained from Maltego.

During the one-day Maltego Fundamentals training course, participants are provided with the necessary tips, tricks and hands-on experience, so that they learn to use the software effectively during investigations in the field of OSINT, due diligence or Cyber Threat Intelligence (CTI).

The training is given in an interactive way, in which theory and practice are alternated. Topics are explained, after which the participants practice them independently or in pairs by means of assignments or cases.

For whom is this training intended?

This training is intended for users who have little or no experience with the use of Maltego software or who want to refresh their knowledge.

What do you learn during the training?

- The operation and installation of Maltego.
- OpSec (Operational Security) & Maltego.
- Working with the Maltego user interface.
- The effective collection of data with Maltego (entities & collections).
- The operation of (and working with) machines and transforms.
- Gaining insight between standard hubs/transforms versus commercial hubs/transforms and the impact on the investigation.
- Import and export data with Maltego.
- How to conduct a targeted investigation with Maltego.

Additional information

The course is taught in English and has a frontal-teaching format. It is also possible to apply customisation, please contact us for more information.

Mercure

Mercure is a unique software solution, already the standard in several countries in the field of complex telecom analysis. It offers you the possibility to store CDRs, mast data, effortlessly merge forensic mobile extractions in various formats and iOS versions using tap and beacon data, in which the data is duplicated. Within seconds

you can also quickly search online communication data such as WhatsApp and Snapchat, where everything can be converted geographically and/or in a timeline automatically. Follow this two-day training course and learn all the ins and outs of Mercure.

For whom is this training intended?

The Mercure training is intended for (forensic) investigators, telecom investigators and operational analysts.

What do you learn during the training?

DataExpert offers this product training to teach users all parts of Mercure. It deals with reading data but also with the large number of built-in searches, timelines, specialised queries, and graphical displays. Through practical cases, the user is introduced to all the possibilities that Mercure has to offer.

Additional information

The course is taught in English.

SINTELIX User Training for i2 Analyst's Notebook

During this training, participants learn extensive analysis and visualisation techniques for large volumes of unstructured data using SINTELIX. SINTELIX extracts, analyses and visualises entities, relationships and other important information from large amounts of text data. Accuracy and high performance are two reasons why investigative agencies worldwide have chosen SINTELIX.

For whom is this training intended?

This five-day training is suitable for operational/case analysts, digital investigators and strategic/tactical analysts who use i2 software during their investigations.

What do you learn during the training?

- Link, entity and metadata extraction with SINTELIX.
- Network semantic, geographic and temporal analysis using SINTELIX.
- Using extensive search filters, including clustering of search results according to different criteria.
- Interactively accessing and linking the extracted data.
- Enriching data and analysis investigation in i2 Analyst's Notebook with new insights from unstructured data.
- Interactively access and link all extracted data.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

Social Network Harvester

During this two-day training course, you will learn how to use Social Network Harvester (SNH) as a tool for collecting and analysing social network data during your investigation. Within the user-friendly interface of SNH, you can use extensive analysis and visualisation functionalities in the field of connections, messages, images, videos, comments and likes. This allows you to quickly and efficiently identify important network elements and previously unknown groups and connections. In addition, during the training you will learn to export the network or parts thereof and to secure them for further processing.

The training course is given in an interactive way, in which theory and practice are alternated. Topics are explained, after which the participants practice them independently or in pairs by means of assignments or cases.

For whom is this training intended?

For official investigation authorities, business consultancies, law firms or investigative agencies that want to gain more insight into social networks from a formal investigation and want to visualise and analyse mutual connections. There is a need to collect data for further analysis purposes.

What do you learn during the training?

- Efficiently investigate Social Networks like Facebook, Twitter, Instagram, VKontakte, Odnoklassniki, YouTube, Telegram, TikTok and GETTR.
- Work with the Profile Manager in combination with the investigation accounts.
- Collect/scrape data and secure friend lists, group members, photo albums and posts on a timeline including comments and likes.
- Optimal use of all dashboard functionalities.
- Analyse the collected data, by establishing a user ID, identifying relevant profiles, providing insight into shared contacts, groups and activities, and preparing the data for export and further analysis.
- Visualise network parts and secure relevant network data.
- Work with the reporting tool.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

DataExpert

Voyager Darknet Intelligence

During this training, participants will learn how to search for data and relevant information in Darknet, Darknet Markets and Telegram, without risk of damage, using the Voyager platform by Web-IQ. This platform features a fully web-browser user interface and provides users with functionality for querying, alerts, categorisation, filtering, case management, visualisations and more! It is also possible to search the history of the Darknet.

For whom is this training intended?

This two-day training is suitable for operational/case analysts, digital investigators and strategic/tactical analysts who want to enrich their investigation data with information from sources such as the Darknet, the Darknet Markets and Telegram.

What do you learn during the training?

- Create data snapshots of raw data and derived datasets.
- Set up alerts so that a notification is immediately issued when a specific person, ad or event is mentioned or active on specific ad sites or forums.
- Interpret and analyse the smart dashboards.
- Use of the Voyager Realtime Scan. This functionality provides automated insights into informal online relationships that are difficult for investigators to find. The scan shows whether people, companies and/or addresses have an online connection by scanning and providing insight into hundreds of websites, social media accounts and forums within seconds.
- Create network visualisations and interact with data within this platform.
- Use the extensive search and filter functionalities.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

Refresher Training

The knowledge and skills acquired during a course ebb away when the student is unable to get started with the program immediately after the training. Refresher training is an excellent opportunity to retrieve knowledge and skills in a short time and possibly get acquainted with new versions of the same solutions.

Refresher Training i2 Analyst's Notebook and i2 iBase

Freshen up the important points from the i2 Analyst's Notebook and/or i2 iBase training courses and use this knowledge and software for solving investigation and operational analysis issues.

Notes

Cryptocurrency

Blockchain and cryptocurrencies are gaining prominence in society. Bitcoin, Ethereum, Binance Smart Chains, are just some of the digital offerings. The different types of blockchain technologies offer the possibility of unprecedented developments; fast cross-border transactions, sale of digital art, decentralised supercomputing and more. With the right analytics, you can gain insight into the world of blockchains and track and visualise cryptocurrency transactions.

DataExpert offers various training courses to train investigators and detectives to become cryptocurrency investigators. DataExpert is a Gold Partner of Chainalysis. This allows us to provide you with all Chainalysis training in addition to our own.

Cryptocurrency

Cryptocurrency Investigations

Cryptocurrency and the blockchain are developing at lightning speed. Therefore, investigating this comes with many opportunities and challenges. But how does this process work? During the “Cryptocurrency Investigations” training, the participants will learn all ins & outs about cryptocurrency and the blockchain. They will learn to conduct investigations from multiple perspectives and with various open source and paid tools. After the training, they can trace a Bitcoin transaction, de-anonymise users and more. They will also be able to report their findings.

For whom is this training intended?

This four-day training is suitable for anyone who does investigations into the blockchain and cryptocurrency. The training is suitable for investigators with the police and other investigation and security services, thematic analysts, financial institutions (CDD, KYC, AML), private investigators, etc.

What do you learn during the training?

At the end of this training, the participants will have gained insight into the possibilities and challenges of cryptocurrency and the blockchain. The participants have obtained knowledge on all aspects (both technical and social) of cryptocurrency and the blockchain. After completing the training, they can also investigate and analyse this using open source tools and Virtual Machines.

Additional information

The course is taught in English and can be offered in both online or in classroom setup. Furthermore, the training courses are modular, making it possible to compose a customized training with matching casuistry.

Cryptocurrency Investigations - Expert (custom)

While conducting an investigation on blockchains and cryptocurrencies, there are advanced methods to apply with or without analysis tooling in addition to conventional investigation methods. In addition to our standard training courses, DataExpert also offers custom Cryptocurrency Investigations Expert training courses. Together with investigation teams, we look at the wishes and needs and the training is tailored to the field of the participants.

Since the level of this training is expert, participants should have knowledge of the basic investigation methods of blockchain technology and cryptocurrencies. In addition, participants are required to have at least three months of investigation experience in the field of blockchains and cryptocurrencies.

The duration of the training depends on the needs discussed in advance and the number of participants.

DataExpert

Ethereum Basics

The cryptocurrencies and blockchain have developed rapidly. The Ethereum blockchain has undeniably grown alongside Bitcoin to become one of the most frequently used. Research on the Ethereum blockchain therefore offers many opportunities for investigators, but also new challenges. How can the investigator deal with this?

During the “Ethereum Basics” training, participants learn all ins & outs of the Ethereum Blockchain. Students learn to investigate using multiple angles and with various open source tools. After the training, they can track Ethereum transactions, swaps and staking and lending and de-anonymize users. They are also able to report their findings.

For whom is this training intended?

This two-day training is for anyone who conducts (investigative) research in the blockchain and cryptocurrency. The training is suitable for, among others, police detectives and other investigation and security services, theme investigators, financial institutions (CDD, KYC, AML), private investigators, etc.

What do you learn during the training?

At the end of this training, participants will have insight into the possibilities and challenges of the Ethereum blockchain. The participants have gained knowledge about the most important basic aspects (both technical and social aspects) of this blockchain as well as the operation and implementation of smart contracts. After completing the training, they can also investigate and analyze this using open source tools.

Other information

The training can be provided in Dutch or English; both classroom or online. Furthermore, the training is modular, making it possible to put together a tailor-made training with matching case studies.

Ethereum Advanced

The Ethereum blockchain has boosted adoption, spawning multiple protocols and EVM-compatible chains. How can the researcher deal with the many opportunities and challenges?

During the “Ethereum Advanced” training, participants learn all the ins & outs of Ethereum protocols and EVM-compatible blockchains such as chain hopping, privacy protocols and more. Students learn to conduct research from multiple perspectives and with various open source tools. After the training, they will be able to track cross-chain transactions, recognize the possibilities in tracing privacy transactions and investigate NFT transactions. They are also able to report their findings.

For whom is this training intended?

This two-day training is for anyone who conducts (investigative) research in the blockchain and cryptocurrency.

The training is suitable for, among others, detectives at the police and other investigation and security services, theme researchers, financial institutions (CDD, KYC, AML), private investigators, etc.

What do you learn during the training?

At the end of this training, participants will have insight into the possibilities and challenges of the various advanced aspects of Ethereum and other EVM-compatible blockchains. The participants have built up knowledge about all aspects (both technical and social aspects) of these blockchains and have developed the cryptocurrencies on them. After completing the training, they can also research and analyze this using open source tools.

Other information

The training can be provided in Dutch or English; both classroom or online. Furthermore, the training is modular, making it possible to put together a tailor-made training with matching case studies.

Chainalysis Cryptocurrency Fundamentals (CCFC)

During the “Chainalysis Cryptocurrency Fundamentals (CCFC)” training, the participants learn the fundamental knowledge about blockchain technology and cryptocurrency. Then, using this knowledge, participants will learn to utilise blockchain explorers while investigating Bitcoin transactions.

For whom is this training intended?

The Chainalysis Cryptocurrency Fundamentals Certification (CCFC) training is suitable for anyone without basic knowledge of cryptocurrency and blockchain technology. Participants may come from the police and other investigative and security services, financial institutions (CDD, KYC, AML), private investigators and more.

What do you learn during the training?

At the end of this four-day training (four half-day sessions), the participant will be able to recognise the value and context of cryptocurrencies in relation to the traditional financial system. The participant has learned the underlying technique of blockchain technology on which cryptocurrencies operate. After the training, he/she will know how Bitcoin works and will have gained knowledge about the most commonly used Altcoins. In addition, he/she can evaluate the ecosystem, identify key actors and is aware of regulatory and privacy developments. With the acquired knowledge, the participant is able to perform basic blockchain analyses.

Exam

The participant must take an exam and obtain a score of at least 75%. The exam will be taken at the end of day four. This training offers all the knowledge needed to successfully complete the exam. The training includes one retake.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

DataExpert

Cryptocurrency Investigations Basics & Chainalysis Reactor Certification

In order to be able to investigate transactions involving the use of cryptocurrencies, a solid basic knowledge of their operation is required. In addition, it is important to be able to use a tool that can monitor and analyse these transactions. During the “Cryptocurrency Investigations Basics & Chainalysis Reactor Certification” training, the participants acquire basic knowledge about cryptocurrency and the blockchain. They also learn to investigate using Chainalysis Reactor, the world’s leading tool for blockchain investigation.

For whom is this training intended?

This four-day training is suitable for anyone who does investigation into the blockchain and cryptocurrency and is a user of Chainalysis Reactor. Think of the police and other investigation and security services, thematic analysts, financial institutions (CDD, KYC, AML), private investigators, etc.

What do you learn during the training?

At the end of this training, the participants will have gained insight into the possibilities and challenges of cryptocurrency and the blockchain. The participants have obtained knowledge about the “core-concepts”, mining, wallets, ledger etc. After the training, the participants will also be able to use the Chainalysis Reactor tool for their investigations and analyses.

Exam

For Chainalysis Reactor Certification (CRC), participants must pass an exam and obtain a score of at least 75%. The exam will be taken at the end of day four. This training offers all the knowledge needed to successfully complete the exam. If necessary, one resit is included in the training.

Additional information

The course is taught in English and can be offered in both online or in classroom setup. Furthermore, the training courses are modular, making it possible to compose a customized training with matching casuistry.

Chainalysis Reactor Certification (CRC)

Cryptocurrency and the blockchain are developing at lightning speed. The Chainalysis Reactor analysis tool offers the possibility to analyse and examine the blockchain and cryptocurrency.

For whom is this training intended?

This two-day training is suitable for users of Chainalysis Reactor. Fundamental knowledge of cryptocurrency and transactions in the blockchain is required.

What do you learn during the training?

At the end of this training, participants will be able to use the Chainalysis Reactor tool to investigate and analyse the blockchain and Bitcoin transactions. They will have gained the experience to be able to successfully

complete the Chainalysis Reactor Certification (CRC) exam.

Exam

For Chainalysis Reactor Certification, participants must pass an exam and obtain a score of at least 75%. The exam will be taken at the end of day two. This training offers all the knowledge needed to successfully complete the exam. If necessary, one resit is included in the training.

Additional information

The course is taught in English and can be offered in both online or in classroom setup..

Chainalysis Reactor Certification: Recertify

After obtaining Chainalysis Reactor Certification, you will be able to apply proper practices and analysis methods in investigations of cryptocurrencies and blockchains. The field is dynamic, so the investigation methods change regularly. Chainalysis Reactor responds to these changes through product updates. The annual Chainalysis Reactor Certification: Recertify training ensures that you stay abreast of the latest developments and trends. This allows you to continue to make optimal use of Chainalysis Reactor.

For whom is this training intended?

The Chainalysis Reactor Certification: Recertify is intended for Chainalysis Reactor users who have already completed Chainalysis Reactor Certification.

What do you learn during the training?

At the end of the one-day training, the participant will have gained knowledge about the basic functionalities of Chainalysis Reactor so that he/she can use them to their full potential. The participant also learned to work with the latest functionalities of Chainalysis Reactor.

Exam

The participant must take an exam and obtain a score of at least 75%. The exam will be taken at the end of the day. The training includes one retake.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

DataExpert

Chainalysis Risk and Regulation Training (CRRT)

With the advent of cryptocurrency, traditional Anti-Money Laundering (AML) assessment frameworks need to be expanded. By applying a risk-based approach (RBA) to cryptocurrencies, effective AML/compliance policies can be implemented that comply with applicable laws and regulations. During the Chainalysis Risk and Regulation training, participants learn to apply a risk-based approach and analyse off-chain and on-chain data.

Who is this training for?

The training is suitable for analysts, investigators and those who oversee cryptocurrencies or monitor and/or report cryptocurrency activities/companies.

What do you learn during the training?

- Distinguish cryptocurrencies from each other (privacy coins, stable coins etc.), recognise and mitigate risks.
- The operation of DeFi (Decentralised Finance) and the effective application of transaction monitoring.
- What geographical considerations should be made in transaction monitoring.
- Blockchain analytics.
- Recognise and mitigate risks from Virtual Asset Service Providers (VASPs). In the form of both on-chain and off-chain data.
- Detect red flags from cryptocurrency exchanges through a secure mock cryptocurrency exchange built by Chainalysis.
- Requirements in reporting in relation to unusual activities.
- Identify and place important developments in international and regional regulations. Evaluate compliance decisions and draw conclusions through a risk-based approach.
- Knowledge Check
- To obtain the Chainalysis Risk and Regulation Certification, participants must complete a knowledge check within two weeks of the start of the training.

Chainalysis Investigation Specialist Certification (CISC)

Due to the growing popularity of cryptocurrency and the increasing use of privacy techniques such as CoinJoin mixing, advanced investigation techniques are needed. During the two-day Chainalysis Investigation Specialist Certification training, participants learn these advanced investigation methodologies and workflows. They use the Chainalysis Reactor software for this. The training course expands on the methodologies learned from the CRC training. The CISC training is a practical training course in which the participants learn to apply the techniques on the basis of case studies.

For whom is this training intended?

The Chainalysis Investigation Specialist Certification training is suitable for “power users” who have at least three months of experience in Chainalysis Reactor and have obtained the CRC certificate.

What do you learn during the training?

- Take advantage of the advanced capabilities in Chainalysis Reactor.
- Apply comprehensive transaction analysis using “all-source” information.
- Identify which specific wallets have been used.
- Apply advanced workflows to analyse more deeply than with traditional blockchain analysis.
- Investigate transactions that use privacy techniques such as CoinJoin mixing and chain hopping.

Exam

For the Chainalysis Investigation Specialist Certification, participants must pass an exam and achieve a minimum score of 75%. The exam takes place within two weeks after the training. This training course offers all the knowledge needed to successfully complete the exam. If necessary, one resit is included with the training.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

Chainalysis Ethereum Investigations Certification (CEIC)

Of all the blockchains that have been developed, Ethereum is still one of the most widely used blockchains. The Chainalysis Reactor analysis tool offers the possibility to investigate this blockchain and the smart contracts that have settled on it. During the two-day Ethereum Investigations Certification training course, participants will learn the necessary knowledge and practices to track transactions on the Ethereum blockchain using Chainalysis Reactor.

For whom is this training intended?

The Chainalysis Ethereum Investigations Certification training course is suitable for Chainalysis Reactor users who have obtained the CRC certificate.

What do you learn during the training?

- Distinguish between ether transactions and smart contract transactions in Chainalysis Reactor.
- Identify centralised services and smart contracts on Ethereum.
- Analyse smart contracts using OSINT (Open Source Intelligence).
- The most important principles in the field of Decentralised Finance (DeFi).
- Trace transaction traces through commonly used DeFi protocols.

Exam

For the Chainalysis Ethereum Investigations Certification, participants must pass an exam and achieve a minimum score of 75%. The exam takes place within two weeks after the training. This training course offers all the knowledge needed to successfully complete the exam. If necessary, one resit is included with the training.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

DataExpert

TRM Crypto Fundamentals

In this training, you gain insight and practical methods needed to familiarize yourself with block-chain related concepts and cryptocurrency. It is a comprehensive orientation to the crypto ecosystem and related key concepts necessary to understand, analyse, and engage with cryptocurrency and track entities and transactions across blockchains.

For whom is this training intended?

This training is designed for those new to cryptocurrency and the blockchain.

What do you learn during this training?

- Explain how blockchains and cryptocurrencies work
- Find data related to blockchain-based entity or transaction addresses
- Follow a transaction across blockchains
- Track attribution in relation to service providers, actors and entities
- Identify and use open source methods of attribution
- Understand smart contracts and tokens
- Explain Non-Fungible Tokens (NFTs) and how they relate to blockchain

TRM Certified Investigator

In addition to the fundamentals of blockchain technology, cryptocurrencies and emerging use cases, students learn on-chain investigative techniques using TRM Lab's industry-leading forensics tools to trace the flow of funds, linking suspicious activity to real world entities.

For whom is this training intended?

The training is for anyone with some blockchain investigation experience who needs to trace crypto transactions across multiple blockchains

What do you learn during this training?

- Identify and explain crypto-crime typologies
- Leverage off-chain open-source intelligence (OSINT) sources
- Identify transaction data types
- Understand blockchain intelligence sources
- Identify attribution on UTXO and account-based blockchains
- Understand behavioral patterns of blockchain activity by an entity
- Trace transactions at both the address level and the entity level across multiple blockchains
- Document on-chain transactional activity
- Understand the general components of crypto compliance

TRM Advanced Crypto Investigator

TRM-ACI is ideal for power users who want to leverage blockchain intelligence to the fullest extent during investigations and provides practitioners with advanced knowledge and skills for a variety of investigative blockchain activities.

For whom is this training intended?

The TRM Advanced Crypto Investigator is an advanced certification course designed for those with existing crypto forensics experience.

What do you learn during this training?

- Understand the threat landscape and vectors that lead to crypto crime
- Explain manual demixing via services such as Wasabi and Tornado Cash
- Understand derivation paths
- Read contracts and identify contract spoofing
- Apply signatures, both manual and those available in TRM Labs
- Apply advanced forensics methods such as multi-signature confirmation in hex

DataExpert

TRM Crypto Compliance Specialist

TRM-CCS provides the knowledge necessary to implement on-chain compliance workflows, understand third-party risk in relation to crypto transactions, and gain an understanding of current trends, typologies, and tooling.

For whom is this training intended?

Compliance and due diligence practitioners requiring the skills to protect against abuse, money laundering, and financial crime.

What do you learn during this training?

- Understand the global regulatory and compliance landscape surrounding cryptocurrencies
- Identify risky activity on the blockchain and understand how it informs organizational risk appetite
- Analyze addresses via transaction monitoring and wallet screening
- Identify third-party custodians (3PC) and crypto on- and off-ramps and determine how they operate
- Write effective Suspicious Activity Reports (SAR)

TRM Digital Forensics & Cryptocurrencies

This training provides an understanding of the intricacies of blockchain technology and recognizing cryptocurrency artifacts left behind in digital evidence, equipping learners to tackle the increasing amount of investigations with a cryptocurrency nexus.

For whom is this training intended?

Digital forensic examiners and their teams who need to close the gap between traditional digital forensics investigations and cryptocurrency investigations.

What do you learn during this training?

- Understanding the intricacies of blockchain technology
- Identify individual and entity cryptocurrency usage
- Recognize and preserve cryptocurrency artifacts in digital evidence
- Understand the differences in popular types of cryptocurrency wallets
- Use open-source tools for analyzing memory images
- Deconstruct blockchain data, including block and transaction structures

Notes

Cybercrime

Digitisation has become an inextricable part of our society. Both privately and professionally, we are more and more connected and an increasing amount of data is stored and shared online.
A gold mine for cybercriminals who are able to carry out their criminal acts more and more easily. For instance, DDoS attacks, ransomware and other forms of malware distribution can easily be ordered as a service via the Internet.

However, what is not as easy for cybercriminals is to remain anonymous and not leave traces. And that is where the chance to track down a cybercriminal is found. During the cybercrime training sessions, we provide participants with more insight into how cybercrime works, what traces a cybercriminal can leave behind and how these traces can be used in an investigation.

Cybercrime

Cybercrime, the (cyber)crime report

Employees from the Intake and Service department of police are the first point of contact when filing a report and lay the foundation for an investigation. The (cyber)crime report training is aimed specifically towards these employees. They learn to properly document reports of cybercrime. Collecting the right information and recognising the sometimes fleeting traces are important during this process. These subjects are therefore extensively discussed during training. We'll also discuss how to properly translate cybercrime to the Penal Code.

For whom is this training intended?

This two-day training is extremely suitable for employees of the police's Intake and Service department.

What will you learn during the training?

At the end of this training, the participants are aware of the trends, developments, opportunities and threats surrounding cybercrime and digitalisation. Additionally, they are capable of documenting cybercrime reports. They have also learned how to safely do a small search query online. They will also know how to have a better password policy and recognise phishing.

Additional information

The course is taught in English and can be offered in both online or in classroom setup. Furthermore, the training courses are modular, making it possible to compose a customized training with matching casuistry.

Cybercrime & Teams Training Trajectory

A significant rise in cybercrime has led to an increased demand in specialised investigators. In order to better counter this form of crime, it is important to equip detectives and investigators with the right mix of competences and skills.

The Cybercrime & Teams training trajectory comprise three separate courses, with each course further increasing knowledge levels and expanding on competences. It covers all aspects of investigating cybercrime and digitised crime.

The training trajectory comprises the following courses:

- Cybercrime Investigations – 4 days
- Cybercrime Advanced – 3 days
- Cybercrime Professional – 3 days

Courses are consecutive but are scheduled individually to allow participants to process the material and reflect between courses. This process of reflection can be facilitated with the information on the e-learning platform, or

by applying the knowledge from the courses to practice. In addition, it is also possible to complete one or two of the courses in the trajectory if this is adequate for the participant's job description.

For whom is this training intended?

This training trajectory is suitable for investigators who are structurally involved with both simple and complex cybercrime investigations, such as (new) investigators on a cybercrime unit. This trajectory does not have any basic skill or knowledge requirements.

What do you learn during this training trajectory?

After completing the Investigations, Advanced and Professional Cybercrime training sessions, investigators are able to chart and investigate simple and (more) complex cybercrime processes. They are able to focus on potential harm risks and on their own safety. Investigators are also knowledgeable on how to construct and support a file. For additional information on training session contents, please refer to the individual courses.

Additional information

The courses in this trajectory are supported through the DataExpert e-learning platform, where participants can learn the theory through both text and short videos. In addition, the courses can be offered in both online or in classroom setup.

Cybercrime & Teams 2024 update

This two-day training has been developed for people who have completed the Cybercrime Learning Trajectory. We focus on the latest trends and developments within the domain of cybercrime and also reflect on the skills and knowledge gained during the Cybercrime & Teams training. The teacher assesses the extent to which the learning objectives have been maintained and which topics require extra attention. During this training, we will also review a specific case from reporting to resolving, focusing on effectively searching and interpreting evidence.

For whom is this training intended?

The world of cybercrime is undergoing rapid changes, which is why an annual update is needed. This review session is intended for participants who deal with cybercrime investigations daily or who have completed the Cybercrime & Teams training.

Cybercrime Investigations

Cybercrime and digitised crime are topics that everyone performing investigations will eventually come to face. Social digitisation has led to a vast increase in investigations into cybercrime and digitised crime in recent years. Other investigations are starting to include ever-increasing cyber components. As such, knowledge of the digital world can be of exceptional added value for any investigation.

For whom is this training intended?

This course is suitable for anyone in investigations aiming to deepen their understanding of the world of cybercrime, including investigators tasked with simple cybercrime investigations or digital community officers.

What do you learn during the training?

After completing this course, participants will have gained insight into current trends, developments, opportunities, and threats from cybercrime and digitisation. During the course, participants follow the process from reporting a cybercrime to a case submitted to the Justice department. Topics covered as part of this process include:

- Basic knowledge of internet and computer technology through e-learning.
- National legal frameworks with regard to cybercrime and authorities.
- Preparing and performing a cybercrime-related search.
- Restricting harm risk during an investigation.
- Interpreting and investigating data secured from a smartphone.
- Interpreting mail headers during a phishing investigation.
- Performing a brief online investigation to benefit one's investigation.
- Creating and interview/interrogation plan and report.

Additional information

This course is part of the Cybercrime & Teams trajectory that also includes the Advanced and Professional courses. The training is supported through DataExpert's e-learning platform, where participants can learn the theory through both text and short videos. The course is taught in English and can be offered in both online or in classroom setup.

Cybercrime Advanced

The fight against cybercrime calls for a coordinated investigative approach. The Cybercrime Advanced course covers how to make even better use of opportunities for internet and computer technology in (cyber) investigations. Whereas anyone in investigations will, at some point, come into contact with cybercrime or digitised crime, there are those investigators and specialists who deal with these issues in their investigations daily. The Cybercrime Advanced course allows these investigators and specialists to expand the knowledge, competences, and tools needed to perform these investigations with (even) greater efficiency.

For whom is this training intended?

This course is intended for anyone in investigations who actively deals with cybercrime or digitised crime investigations. Examples are investigators whose tasks emphasise cybercrime, team leads directing cybercrime specialists, and investigators intending to function as points for cybercrime contact in investigations teams. Participants are recommended to complete the Cybercrime Investigations successfully before taking part in this course.

What do you learn during the training?

After completing this course, participants will be able to complete cybercrime investigations into secured data,

and to consult others in cybercrime investigations. Topics covered as part of this process include:

- Current cybercrime trends and developments.
- National/European authorities and legal frameworks with regard to cybercrime.
- Investigating the front-ends of, for example, phishing websites or online stores.
- Investigating complex mail headers and DNS-records.
- Read-outs, investigations, and interpretations of data from secured data carriers.
- Conducting basic investigations on the darknet.
- Investigating and mapping IoT and connected devices.

Additional information

This course is part of the Cybercrime & Teams training trajectory that also includes the Investigations and Professional courses. The training is supported through DataExpert's e-learning platform, where participants can learn the theory through both text and short videos. The course is taught in English and can be offered in both online or in classroom setup.

Cybercrime Professional

The rise in cybercrime has been substantial in recent years. This rise is part of the reason for the Dutch Public Prosecutions and police departments increase dedication to combating this type of crime. The police have established various "cybercrime" teams, as well as a "hacking" and "dark web" team. The investigators working in a cybercrime team deal with complex cybercrime investigations. This course focusses on providing investigators with the knowledge needed with regard to complex cybercrime investigations.

For whom is this training intended?

This course is intended for investigators who structurally deal/come into contact with both simple and complex cybercrime investigations. Participants are recommended to complete the Cybercrime Investigations and Cybercrime Advanced courses successfully before taking part in this course.

What do you learn during the training?

After completing this course, participants will be able to chart and investigate (more) complex cybercrime processes. In addition to tracking cybercriminals, the disruption of a cybercrime process may also be a desired outcome. Therefore, this training also covers Public-Private Collaborations and out of the box-thinking. Topics covered as part of this course include:

- Current cybercrime trends and developments.
- International authorities and legal frameworks with regard to cybercrime.
- Investigating the back-ends of, for example, phishing websites or online stores.
- Conducting digital forensic investigations of an impounded server.
- Conducting basic investigations into a cryptocurrency trail using a ransomware casus.
- Charting and disrupting a cybercrime process.
- Working with virtualisation, using tools like Linux Command Line and KALI Linux.

Additional information

This course is part of the Cybercrime & Teams Training Trajectory that also includes the Investigations and Advanced courses. The training is supported through DataExpert's e-learning platform where participants can learn the theory through both text and short videos. The course is taught in English and can be offered in both online or in classroom setup.

Digitally Proficient Investigator (DPI)

In this customised Digitally Proficient Investigator training course, participants are given a complete picture of everything that involves policing in relation with digital aspects and cybercrime. After the training, the participants will be able to use modern investigative techniques. They can also recognise opportunities within the digital domain from their role as an investigator.

In addition, they will improve their general understanding of 'cyber' and digital investigation. The participants know how to assess digital traces and know how to avoid hazards to lose information. They are also able to responsibly investigate telephone data and take the first measures at a digital crime scene.

For whom is this training intended?

This training is suitable for detectives/investigators working within investigation teams associated with major crime, organized crime, thematic enforcement, etc.

What do you learn during the training?

- Conducting a simple data investigation.
- Using common investigation programmes.
- Basic concepts around digital investigation and cyber.
- What the world of cryptocurrency and the dark web looks like.
- Minimising harm risks in Internet and on-site investigation.
- The basic concepts of interception.
- Handling of digital traces.
- Entering a digital crime scene responsibly.

Additional information

The training is a combination of e-learning and classroom training.

Cyber Security

The digital world is developing rapidly. This development presents new opportunities, but also new threats. Cybercriminals, including hackers, unfortunately need less and less technical knowledge to harm a country, business or person online. As such, securing data against cybercriminals through cyber security is becoming increasingly important.

During our Cyber Security training sessions, participants become more aware of the possibilities and dangers of cybercrime. This allows the participants to better recognise cybercrime, take action themselves and take the appropriate measures.

Cyber Security

Cybercrime and Cyber Security Awareness

Ransomware, data breaches and phishing are commonplace. The question is not if you will be affected, but when. A data breach at another organisation does not mean that your organisation can sit back and relax. An important step in preventing victimisation by cybercrime is making employees aware of how to act.

For whom is this training intended?

The Cybercrime and Cyber Security Awareness workshop consists of one day of three training sessions, each lasting two hours, in order to make the various groups of employees within an organisation aware or more aware of cybercrime. The emphasis is shifted per session, depending on the function/job group of the participants.

What do you learn during the training?

Each training session looks at the trends of cybercrime, but also at relevant legislation including the GDPR. The goal of the workshop is to make the participants more resilient, to give them insight in how to act, but also to make them aware of their responsibilities and how this relates to other parts of the organisation. There is also plenty of room for interaction; participants can ask questions, and statements and/or dilemmas are used.

The topics covered in the training sessions include:

- Cybercrime (actors, motivation, objectives).
- Risks to the organisation/employee.
- (Practical) Measures.
- Relevant legislation (GDPR and more).

The intention is to make the individual employee aware of his/her position in the defence and fight against cybercrime within the organisation.

Additional information

A maximum of 25 participants can register per session. It should be taken into account here that groups are homogeneous in terms of work. The course is taught in English and can be offered in both online or in classroom setup.

Incident Response Readiness

If you are affected by a cyber incident, your organisation must be prepared to act quickly and appropriately. This can significantly limit (financial) damage. To prepare your organisation for such a situation, DE-CERT offers the Incident Response Readiness workshop.During this two-hour workshop, an Incident Supervisor from DataExpert will guide you and your colleagues through the world of Incident Response.

DataExpert

For whom is this training intended?

This workshop course is intended for all organisations that want to prepare for a possible cyber incident.

What dol you learn during the training?

- The course of a cyber attack.
- What Incident Response entails.
- What a forensic investigation entails and what it delivers.
- Everything surrounding ransomware payments.
- The role of the Police and the Dutch Data Protection Authority.
- The internal and external impact of a cyber crisis.
- The short-term and long-term implications.

Using practical examples, we will give you insight into the working methods of our Incident Responders. We show how a thorough Incident Response preparation can contribute to getting your organisation back in business faster. We discuss how we would proceed in the event of a cyber incident in your organisation and also address non-technical topics such as leadership, communication and risk management. You will also receive practical tips to prepare your organisation for a possible incident, we provide you the tools to take action regarding insight and risks, and together we will draw up an incident roadmap for how to act in the event of a cyber attack in your organisation.

Additional information

This workshop is taught in English and can be offered in both online or in classroom setup.

Security Discovery

If you are affected by a cyber incident, your organisation must be prepared to act quickly and appropriately. This can significantly limit (financial) damage. But where do you stand today, both technically and in terms of process? What is your baseline? During this three-hour workshop, a specialist from DataExpert will guide you and your colleagues through the world of Cyber Security.

For whom is this training intended?

This training course is intended for (IT) technical team members and management who want to determine their baseline and want to know where their cyber risks are.

What do you learn during the training?

- Course of a cyber attack.
- Technical and process measures.
- Working with security frameworks (e.g. NIST, CIS, GDPR, ISO27001).
- Measures to be implemented immediately.

Based on the attack methodology of cyber criminals, we provide you with insight into the techniques and processes that you can use to realise quick wins. Here we answer questions such as: Where does your organisation stand at the moment, what is the benchmark, which actions have (and haven't) you already defined? What is business-critical and for which department?

We also discuss what possibilities and impossibilities security frameworks offer your organisations and we provide direct pragmatic advice in the field of people, process and technology. This results in an interview report with short and long-term guidance for your organisation and immediately executable actions.

Additional information

This workshop is taught in English. For a successful workshop, it is important that it can take place physically and the organisation is requested to share information with us prior to the session.

Digital Forensics

Laptops, PCs, mobile devices, smart home devices, and even cars contain an enormous amount of information. The challenge for digital investigators is to filter relevant data from these devices in a forensically correct way and critically analyse it, so that the retrieved data can be used as evidence.

During DataExpert's Digital Forensics training sessions, participants obtain insight into and skills in effectively using technology in the field of mobile, digital, and cloud forensics. This way investigations into digital crime become more thorough.

Digital Forensics

Amped FIVE Forensic Image and Video Enhancement

Amped is the world's leading company in terms of image processing of digital photos and videos. FIVE is especially designed for forensic and safety applications. During this four-day training, you'll learn how to work with this unique and complete solution in a simple, fast and thorough way.

For whom is this training intended?

This training is intended for users who just started using the FIVE programme. This is the beginner's course for investigators that are involved in multimedia investigation.

What do you learn during the training?

Participants in this course learn the basics of image and video analysis and also how to handle the digital multimedia evidence. The trainees acquire the right knowledge and skills to process and analyse photo and video material in a forensically correct manner.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

Amped FIVE Additions

During this three-day training, participants learn to work with this unique and complete solution in a simple, fast and thorough way.

For whom is this training intended?

This training is meant for investigators who have already followed the Forensic Image and Video Enhancement with Amped FIVE course. This is a refreshment course that enables participants to learn about the newest filters and features and to properly interpret the data so the tool can be used optimally. The Additions training is built up modularly and can partially be personally customised.

What do you learn during the training?

The trainees learn to process and restore image material in a forensically responsible way. Additionally, the participants learn to refine image material and to analyse it using Amped Five software.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

DataExpert

Amped Authenticate

Amped Authenticate is a software application for forensic image authentication, tampering detection, and camera ballistics on digital images. This product offers a complete suite of powerful tools to exploit the data behind digital images, allowing for the analysis of image integrity, authenticity, metadata, source, history and more! During this hands-on three-day training course students will obtain the knowledge and skills required to properly analyze digital images with Amped Authenticate.

For whom is this training intended?

This is an intermediate and expert-level course designed for users who are seeking to use Amped Authenticate for their investigations.

What do you learn during the training?

Participants will learn the techniques necessary to perform authentication analysis on digital images in a forensic science setting as well as to package, deliver, and present those findings in court.

Additional information

This training course is taught in English and can be offered in both online or in classroom setup.

Amped Replay

Amped Replay is an enhanced video player that allows investigators, frontline officers, first responders, security personnel and CCTV operators to conduct a quick first-level analysis of their videos, with easy conversion, quick corrections, redaction, and annotation functions, as well as a report. During this two-day training course participants will obtain the knowledge and skills required to properly examine and process image and video evidence with practical or simulated cases using Amped Replay.

For whom is this training intended?

This is an entry-level course designed for investigators and first responders.

What do you learn during the training?

- How to implement a firm legal process for using and reporting image and video evidence in daily investigations.
- What the basics of image and video analysis are.
- How to convert proprietary video files.
- How to apply basic corrections to an image.
- How to prepare the evidence for presentations with redactions and annotations.
- What the challenges and pitfalls are when using digital multimedia evidence in investigations.

Additional information

This training course is taught in English and can be offered in both online or in classroom setup.

Berla iVe Vehicle System Forensics

Berla is a supplier of solutions in the field of vehicle systems. Based on the found vehicle data, investigators can quickly and efficiently determine what happened, where it happened and who was involved. During this five-day hands-on training you will learn how to interact with vehicle data using the iVe program. You will learn how to work with this powerful software and efficiently find information about recent destinations, favorite locations, phone calls, etcetera.

For whom is this training intended?

This training is for Digital Investigators working at government institutions or corporate businesses.

What will you learn during the training?

After a brief theoretical introduction, there will soon be a switch to practical exercises such as the removal of infotainment systems from vehicles and reading out of data. Participants learn how to copy and analyze data from various infotainment systems such as Microsoft Sync, MyFord Touch, OnStar, Uconnect and Entune.

Additional information

The course is taught in English and has a classroom setup.

Cellebrite Apple Forensics Fundamentals (CAFF)

This four-day Apple Mac training is intended for digital investigators already familiar with forensics based on the Windows platform. During the Cellebrite Apple Forensic Fundamentals (CAFF) training, participants will learn, among other things, how to use Cellebrite Digital Collector and Inspector to analyse specific data points within operating systems and file system artefacts. This is a practical training that works on the basis of a case.

Who is this training for?

This training is intended for digital investigators who already have experience with digital investigations in general and want to expand their knowledge to include investigating Apple devices. This is the basic course for all other Cellebrite Apple Forensics training courses.

What do you learn during the training?

- Different start-up procedures of Apple devices.
- Establishing a plan for successful triage and imaging.
- MacOS structures and their limitations.
- Key HFS+ and APFS file system artifacts.
- Impact of changes in APFS and macOS structure on forensic analysis.
- Handling macOS with property-list (PLIST) data.
- Identifying user preferences and system preferences.
- Influence of date/time and time zone on data analysis.
- Recognising the different disk images encountered on a macOS.

- Saving, viewing and sharing encountered media files on macOS and iOS.
- Analysing Apple metadata attributes.
- Analysing mounted volumes, device connections and network connections in macOS.
- Investigating artifacts from web browsers such as Safari.
- Interpreting encountered log files on macOS and iOS devices.

Cellebrite Apple Intermediate Forensics (CAIF)

This three-day training will include a deeper look at analysing macOS and iOS devices. In the course, participants work on a case using the Cellebrite Inspector software.

Who is this training for?

This training is designed for digital investigators with a basic knowledge of macOS and iOS devices who want to expand their knowledge and reach a higher level of proficiency. It is recommended to take the Cellebrite Apple Forensics Fundamentals training first before starting this course.

What do you learn during the training?

- Analysing mounted volumes, device connections and network connections in macOS.
- Interpret encountered log files on macOS and iOS devices to analyse Apple Mail. including its structure, e-mail messages and related files.
- Identifying evidence around the use of Terminal.
- Recognising the GUID Partition Table and understanding its structure.
- Understanding the Hierarchical File System (HFS+).
- Distinguishing and interpreting APFS disk structures from different macOS versions.
- Creating, investigating and analysing an APFS disk.
- Recognising and understanding the differences between link files, APFS clones and APFS farm links in macOS.
- Creating and analysing Time Machine backups and APFS Snapshots.

Cellebrite Apple Advanced Forensics (CAAF)

Operating systems leave complex traces in both allocated space and unallocated free space on a data carrier. This three-day training will cover, among other things, the more complex concepts, such as recovery points found in an iOS and macOS investigation. The Cellebrite Apple Advanced Forensics training is led by an instructor who provides comprehensive explanations of the subject matter, but the participants also do many practical exercises themselves.

Who is this training for?

This training is for advanced digital investigators with good knowledge of Computer Forensics and extensive knowledge of Mac forensics obtained in e.g. the Cellebrite Apple Intermediate Forensics training.

What do you learn during the training?

- Distinguishing between handling deleted APFS and HFS+ files.
- Recovering artefacts in both allocated and unallocated spaces.
- Recognising hardware and software RAID systems.
- Understanding advanced iOS analytics practices.
- Using log files to reconstruct usage history and create timelines.
- Understanding and exploring Extended Attributes, Spotlight evidence and file sharing artefacts.
- Identifying and using passwords stored on macOS.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

Cellebrite Mobile Forensics Fundamentals (CMFF)

The four-day course provides attendees with compulsory digital forensics core knowledge (fundamentals) including: mobile device communication networks, explorations of Android and iOS file systems, extraction methodologies and memory (NAND) functions. Attendees will learn reasoning and strategies (concepts) used by creditable practitioners and organisations to form the future of digital forensic best practices.

For whom is this training intended?

The training is intended for Digital Investigators starting their careers. Basic knowledge of computer systems would be an advantage.

What will you learn during the training?

- Compare and contrast different mobile devices and operating systems.
- Identify the phases or digital forensic processes.
- Recognise best practice for on-scene identification, collection, packaging, transport, examination and storage or digital evidence data and devices.
- Interpret extracted digital evidence device data using the UFED Reader.
- Analyse the constructs of auto-generated reports generated using the UFED Touch and 4PC.
- Examine the use of the UFED Reader software.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

DataExpert

Cellebrite Certified Operator (CCO)

This two-day course is designed for participants tasked with extracting data in a forensically sound manner using UFED Touch or UFED 4PC. The CCO training builds upon the concept from the CMFF course with the focus on operational factors. Furthermore, it is explained and demonstrated how extractions can be imaged and analysed with Physical Analyzer.

For whom is this training intended?

The training course is meant for investigators with some experience in digital investigation. Having completed the CMFF training course would be an advantage.

What will you learn during the training?

- Install and configure UFED Touch, UFED Touch 2 or UFED 4PC and Physical Analyzer software.
- Explain the best practices for on-scene identification, collection, packaging, transport, examination and storage or digital evidence data and devices.
- Display best practice when conducting cell phone extractions.
- Identify functions used within UFED Touch, UFED Touch 2 or UFED 4PC to perform supported data extractions.
- Exhibit how to open extractions using Physical Analyzer.
- Summary how to conduct basic searches using Cellebrite Physical Analyzer.
- Outline how to create reports using Cellebrite Physical Analyzer.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

Cellebrite Certified Physical Analyst (CCPA)

This three-day course is based on data analysis and advanced search techniques using Physical Analyzer Software. During the training no extractions are made, but the available data will be examined in detail. Especially the different search methods are discussed.

For whom is this training intended?

This course is an advanced level program designed for technically savvy investigators, digital evidence analysts and forensic practitioners. Having completed the CCO training would be an advantage.

What will you learn during the training?

- Conduct advanced mobile device forensic analysis using the UFED Physical Analyzer software.
- Recall techniques used for authentication and validation or data parsed and collected as evidence.
- Identify functions within Physical Analyzer software which allow examination of various types of data.
- Recognise Physical Analyzer's capabilities to generate custom reports in an organised manner.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

Cellebrite Advanced Smartphone Analysis (CASA)

This five-day course takes a hands-on, in-depth look into forensic recovery or application data found in today's smartphones. The participants in this course will learn how to decode information which is not decoded by forensic tools. They will also utilise third party software and Python scripts for analysis, verify and validate findings.

For whom is this training intended?

This class is recommended for those familiar with UFED Physical Analyzer or who have completed the CCPA course.

What will you learn during the training?

- Decoding and data recovery of smartphones.
- Working with Python and other so-called 3rd party tools.
- Analysis of the decoded data.
- Validation of data and reporting.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

In this interactive training, participants learn how to dismantle and reassemble mobile phones with the aim of performing a data extraction in a forensically correct manner.

For whom is this training intended?

This five-day training course is intended for (digital) investigators who deal with damaged mobile devices that require repair before data extraction is possible.

What do you learn during the training?

- Properly replacing key components of mobile phones and USB drives.
- Forensically recovering data from damaged mobile devices.
- Replacing parts such as charging ports, LCD screens and certain buttons of a mobile phone.
- Importing, analysing and reporting UFDR files in Cellebrite Reader.
- Heat and soldering techniques.

DataExpert

Exam

At the end of this training, the participants take a practical exam in which they use UFED technology. Upon successful completion, participants will receive the Certified Evidence Repair Technician Forensic certification.

Additional information

The course is taught in English and is in a classroom setup.

Digital Investigation for Tactical Investigators

Society is now highly digitised. People are connected 24/7 to their network, work and in many other ways. Within the investigation world, this creates enormous opportunities to find traces and provide evidence. Tactical investigators are increasingly dealing with the results of digital forensic investigations. One of the tools used in digital investigation is AXIOM. During this training, participants learn to work with data that has been obtained with this tool during an investigation.

For whom is this training intended?

Tactical investigators who in their daily work are confronted with all kinds of data that have been analysed with the tool AXIOM.

What do you learn during the training?

- AXIOM and obtaining data as a digital investigator.
- Reading data within an AXIOM Portable Case.
- Artifacts (e.g. registry entries).
- Reviewing different types of documents and metadata.
- Setting filters and applying tags in relevant data.
- Viewing e-mails and analysis of the e-mail header.
- Analysis of a browser, Internet history, favourites and bookmarks.
- Cloud possibilities.
- Timeline investigation.

Additional information

Prior to the training, the participant will acquire basic knowledge of AXIOM through e-learning. The course is taught in English and can be offered in both online or in classroom setup.

Elastic - Data Analysis with Kibana

A powerful search and analysis engine needs an equally powerful user interface to create advanced visualisations and perform deeper analysis. This is the central theme of this practice-oriented training. Participants will learn to analyse data in Elasticsearch using the software Kibana.

For whom is this training intended?

This three-day training is suitable for operational/case analysts, digital investigators and strategic/tactical analysts who want to analyse data in Elasticsearch using Kibana software.

What do you learn during the training?

- The core concepts of data analysis with Kibana and Elastic Stack. These include simple aggregation-based graphs, but also complex geo-based visualisations and complex time series visualisations.
- How to get search hits with Kibana search.
- How to create visualisations and dashboards for different data sets.
- How to manage Kibana.
- How to find answers and anomalies in your Elasticsearch data sets using Kibana.

Exam

After completing the training, you can take an exam to earn your certification as an Elastic Certified Analyst.

Additional information

The course is taught in English and has a classroom setup.

Elastic - Elastic Observability Engineer

Insight into data structures is achieved when you bring together your logs, statistics and APM traces to get a complete picture of the health and activity of your infrastructure. This course provides participants with a strong foundation for using the Elastic Stack. This way, they learn to implement a unified observation with a single-stack solution.

For whom is this training intended?

This three-day training is suitable for operational/case analysts, digital investigators and strategic/tactical analysts who want to create insight into their IT infrastructure.

What do you learn during the training?

- How to collect logs, metrics and APM data and then send it to one datastore: Elasticsearch.
- How to make uniform observation data actionable through machine learning and alerting.
- How data can be correlated more easily across different data sources.
- How to visualise your observability data through the intuitive user interface of Kibana.

Exam

After completing the training, you can take an exam to earn your certification as an Elastic Certified Observability Engineer.

Additional information

The course is taught in English and has a classroom setup

DataExpert

Elastic - Elasticsearch Engineer

During this hands-on training, participants will learn the basics to get started with Elasticsearch and Elastic Stack. This is followed by a deeper dive into various topics such as data modelling, data management, data processing, cluster management, developing search applications and shards.

For whom is this training intended?

This three-day training is suitable for operational/case analysts, digital investigators and strategic/tactical analysts for both beginners and experienced users.

What do you learn during the training?

- How Elasticsearch and the components of Elastic Stack work together.
- Where and when to use what search language.
- What the different ways of importing and processing data are.
- How to build complex queries and process search results from them.
- How to scale up and down your clusters.
- How to manage indices in large and multiple clusters.
- The ins and outs of data & cluster management.
- Recommendations for problem solving.
- How to build your own custom search applications that use Elasticsearch in the background.

Exam

After completing the training, you can take an exam to earn your certification as an Elastic Certified Engineer.

Additional information

The course is taught in English and has a classroom setup.

Elastic - Threat Hunting with Kibana

During this training, participants learn through assignments how to detect threats and how this differs from other security analysis processes. Then they learn how to use Elastic Stack and its powerful tools to support this process.

For whom is this training intended?

This two-day training is suitable for security analysts interested in using Kibana to investigate potential threats to their data and systems.

What do you learn during the training?

- The essential Kibana functionalities for analysing security data.
- How network and host data sources can be enriched.

- The philosophy, workflow, models and techniques that can be applied in the hunt for (cyber) threats.
- How Threat Hunting helps improve the effectiveness of the Security Operations Center.

Additional information

The course is taught in English and has a classroom setup.

Elastic - Networking Security Monitoring Cyber Operator

During this five-day training, participants will learn to work with a suite of cybersecurity tools. Although it features open-source security tools, the Networking Security Monitoring Cyber Operator does not involve tool training. The objective of the training is to teach Cybersecurity Operators to detect and track cyber threats using Elastic Stack and tools such as Zeek and Suricata.

To conclude the training, participants work on a case with multiple scenarios, using the skills they have learned to find the 'enemy' in network traffic.

For whom is this training intended?

This training is suitable for Cybersecurity Operators who need to analyse data to detect bad actors in their network as part of a machine-assisted, human-driven approach.

We recommend attending this training only if you are familiar with Linux, networking and network security concepts.

What do you learn during the training?

- Basics of Packet analysis
- Intrusion detection systems (IDS) with Suricata
- Network Metadata Analyses with Zeek
- Kibana UI for Security
- Threat hunting Capstone

Additional information

The course is taught in English and has a classroom setup.

Elastic - Network Security Monitoring Engineer

This 10-day training focuses on deploying Elastic Stack in a security context. The focus will be on implementing the various components of the Elastic Stack (Elasticsearch, Kibana, Beats and Logstash) and optimising the performance of these components.

DataExpert

During the training, participants will learn all about the Elastic Stack and its core components and use this knowledge to build Network Security Monitoring (NSM) sensors in different configurations. At the end of the training, participants will be able to build with the Elastic Stack in such a way that they can analyse data sources in their network and systems. This is to create a more complete security overview.

For whom is this training intended?

This training is suitable for Security Engineers responsible for installing, using and maintaining the Elastic Stack and network monitoring platforms.

What do you learn during the training?

- Ansible
- Installing, using, maintaining and optimising Zeek
- Installing, using and maintaining Kafka
- Passive operations and tapping
- Installing, using and maintaining CAPES
- Installing, using and maintaining Elastic Stack
- Suricata rule management and tuning
- Sensor troubleshooting
- Engineer capstone event

Additional information

The course is taught in English and has a classroom setup.

EnCase DF120

EnCase offers advanced options for investigation of computer data. During this four-day practice-oriented training with practical example cases, you'll get to know the features of this software.

For whom is this training intended?

This training is intended for digital investigators and IT security experts. The training is suitable for investigators who don't have any or little experience when it comes to digital forensic investigation.

What will you learn during the training?

- What digital evidence is and how a computer works.
- An overview of the EnCase Computer Forensic methodology.
- Insight into the structure of Fat and NTFS file systems.
- How you create a case.
- 'Previewing' and 'acquiring' data carriers.
- How to carry out basic 'keyword searches'.

- How to analyse digital footprints and view files.
- How to restore suspicious data.
- How to store the results of the investigation.
- How to prepare and present evidence in court.
- How to verify evidence.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

EnCase DF210

This practice-oriented four-day training is meant for experienced computer users, who also already have some experience with EnCase. This training picks up where the EnCase DF120 training left off. This training enables the digital investigator to optimally use the unique features of EnCase.

For whom is this training intended?

This training is intended for experienced digital investigators and IT security experts who have completed the EnCase DF120 training.

What will you learn during the training?

- How to create and use 'logical evidence files'.
- How to recover removed partitions and folders.
- How to carry out advanced search query using GREP.
- How the Windows Register works.
- How to use composite files.
- How to export files, directories and the complete contents from a drive.
- How to work with hash libraries and file identification.
- How Windows parts like links, user folders and trash within EnCase.
- How to recover printed pages.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

DataExpert

EnCase DF220

This four-day hands-on training offers practical demonstrations and case studies to better understand the EnCase Forensic Version 8 methodology. This training is not a replacement of the EnCase DF120 and EnCase DF210 training.

For whom is this training intended?

This training is intended for experienced digital investigators that want to make the step to using EnCase version 8. For example, EnCase version 6 users that have undergone the EnCase DF210 training or users with an ENCE certification. This training can also be applied as a refreshment course for users of version 7.

What will you learn during the training?

- The structural differences between EnCase version 8 and previous versions.
- Operation of the modules.
- The new file structure of the 'evidence files' and the transition from previous versions.
- The new search feature.
- How to use external viewing tools.
- How to carry out hash analyses.
- Creating reports using the new templates.
- The archiving capabilities.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

EnCase DF320

This four-day training goes further into the subject matter that has been addressed in the EnCase DF210 training and emphasises the investigation of operating systems.

For whom is this training intended?

This training is intended for experienced digital investigators and IT security experts that have completed the EnCase DF210 training. Basic knowledge of computer forensics is required.

What will you learn during the training?

- How Windows NT File Systems (NTFS) operate.
- NTFS data recovery.
- Investigation of Windows Register Files.
- Analysis and recovery of the Windows event log files.
- Hard-end Software RAID technology, acquisition and investigation.

- The principles of Encrypted Data Recovery.
- Understanding and writing investigation to Windows BitLocker.
- Linux and UNIX operating systems and file information.
- Linux partition recovery.
- Forensic investigation of Macintosh computers.
- The Macintosh operating system.
- In-depth look at the EnCase computer forensic methodology.
- Introduction of EnScript programming.

Additional information

The course is taught in English and can be offered in both online or in classroom setup..

EnCase DF410-NTFS

During this four-day training, the participants learn to handle the technical challenges of the Windows NTFS file system and additionally, how to subject the Master File Table to an in-depth analysis. This is an intensive, practice-oriented training with practical case studies.

For whom is this training intended?

The hands-on training is intended for experienced digital investigators, network administrators and the IT security administrators that want more insight into NTFS and Windows networks in relation to cybercrime. The participants in this training are required to be familiar with EnCase. Additionally, they must have ample experience when it comes to computer investigation.

What will you learn during the training?

- Thoroughly analyse the Master File Table (MFT).
- Gain a thorough understanding of the NTFS file system.
- Investigate Windows artefacts and assess their value as evidence.
- Recover erased NTFS partitions.
- Comprehending register information like the NTUSER.DAT and the SAM-file.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

EnCase DFIR350

The training enables the digital investigator to interpret evidence found on the computer of a suspect or victim using EnCase and, among others, goes into the operation of Bit-Torrent P2P networks, the operation of Trojan viruses and the operation of several types of email clients.

DataExpert

For whom is this training intended?

The practice-oriented training is meant for experienced computer users (digital investigators and IT security experts), who already have some experience with EnCase and is part of the 'Expert series' by OpenText. In almost all computer investigation email and internet traffic will be found. This underlines the necessity to understand its relevance in a digital investigation.

What will you learn during the training?

- Backgrounds of PTP and BitTorrent.
- The operation of BitTorrent and the BitTorrent protocol.
- The operation of the Gnutella P2P network.
- The operation of the LimeWire and Bearshare programmes.
- The background and operation of Trojan Viruses.
- The use of VFS and PDE to identify and analyse Trojans.
- How to detect and analyse Keyloggers.
- The operation and use of Windows LIVE messenger.
- The operation of Internet History and WebCache.
- Goal, content and indexing of Internet cookie files.
- Reconstruction of web pages.
- Construction and analysis of Outlook PST files.
- The use of Mozilla Firefox.
- Lotus Notes analysis with EnCase.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

Forensic Toolkit 101

Want to conduct computer investigations thoroughly and effectively? The four-day Forensic Toolkit 101 course introduces participants to the key capabilities and processes of Forensic Toolkit (FTK).

For whom is this training intended?

The Forensic Toolkit 101 course is intended for digital detectives/investigators. FTK and other Exterro products are used mainly by forensic specialists and fraud investigators.

What will you learn during the training?

- Building and managing an FTK case.
- Using the FTK Interface.
- Search options.
- Filter options.
- Using the Manage Menu.

- Exporting items in FTK.
- Installing and applying the Know File Filter (KFF).
- Performing a Disk Level Analysis.
- Using the FTK Python Scripter.
- Visualising data in FTK.
- Creating reports.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

Forensic Toolkit 201

Want to conduct computer investigations thoroughly and effectively? The four-day Forensic Toolkit 201 course goes beyond the Forensic Toolkit 101 course and takes a more in-dept approach to the analysis of forensic artefacts with FTK. Exterro's recent QView tool is also covered in this course.

For whom is this training intended?

The Forensic Toolkit 201 course is intended for digital investigators. Participant are recommended to complete the Forensic Toolkit 101 course before attending this course.

What will you learn during the training?

- Existing general data structures.
- Analysing graphic images and video.
- Analysing the Windows registry.
- Analysing Windows event logs.
- Analysing the Windows operating system.
- Analysing Apple MacOS.
- Analysing internet browsers.
- Interpreting cloud-data.
- Using QView.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

DataExpert

Griffeye Analyze DI Certification

While more digital images potentially bring with them more digital evidence, it's nearly impossible to uncover valuable information without the right tools. Griffeye's Analyze DI Pro can offer digital forensic investigators excellently support in this. During this training, the most important functionalities of the Analyze DI Pro tool are discussed.

For whom is this training intended?

This four-day training is specifically for digital forensics teams who deal specifically with so-called CSAM cases, which stands for Child Sexual Abuse Material.

What do you learn during the training?

- Which features Analyse DI Pro has. Think of functionalities such as: grouping and searching metadata, face recognition and image and video hashing.
- How to use the tooling during your investigation.

Additional information

After the successful completion of this training, participants receive the Griffeye Analyze DI Pro certificate. The course is taught in English and can be offered in both online or in classroom setup.

Hansken Advanced

Hansken is a forensic data analysis platform widely used within the criminal investigation community. The platform supports analysts and digital investigators in accessing digital evidence, quickly searching and creating insights into the data encountered and mapping possible traces.

During the hands-on Hansken Advanced training, digital investigators and analysts learn to work with Hansken's advanced functionalities. They do this using a case study with real-life examples. The focus of the training is on the technical user interface (Hansken Expert UI).

Who is this training for?

This three-day training is suitable for analysts and digital forensics experts who want to expand their knowledge around Hansken to include its more advanced functionalities. It is recommended that participants in this training have completed the Hansken Intermediate training or have already gained considerable experience with Hansken during their work.

What do you learn during the training?

- How Hansken extracts traces from digital evidence
- Further examining and interpreting identified traces
- Performing complex searches and advanced queries with the trace model and query language
- Processing evidence (chain of evidence) and recording the process (chain of custody)

- Available tools and statistics
- Working with the case operator
- Visualisation options
- Reporting options
- Basic scripting and extraction plug-ins

Additional information

This training is given in a classroom form and can be given in Dutch or English. Given the hands-on nature of the training, participants will have access to the Hansken practice environment.

Incident Response in the Microsoft Cloud

In this two-day hands-on training, you'll learn everything you need to know about forensics and incident response in the Microsoft cloud. This training covers both Microsoft 365 and Microsoft Azure, you'll get hands-on experience with investigating attacks and digging through the relevant log artifacts. Everything you learn is related to real-life threats observed against the Microsoft cloud.

The trainer has real-life experience with incident response and forensic investigations in the cloud, knowledge will be shared that's not available on any website. Once you've completed this training you will feel comfortable investigating any threat in the Microsoft cloud. The training is very hands-on and concludes with two full attack scenarios in both Azure & M365 and you're tasked in the CTF to solve as many pieces of the puzzle as you can.

Pre knowledge

The required pre-knowledge will be provided through OnDemand videos that can be watched before the course starts. The topics include:

- Azure platform basics such as hierarchy and terminology.
- Azure Active Directory/Entra ID components such as users, groups and service principals
- Audit logging in a Microsoft Azure environment.

Once you've completed this training you will feel comfortable investigating any threat in the Microsoft cloud. The training is very hands-on and concludes with two full attack scenarios in both Azure & M365 and you're tasked

Magnet Forensic Fundamentals (AX100)

During this Forensic Fundamentals (AX100) training, participants will learn the basic skills for conducting digital forensic investigations. The most important terminology and working procedures are discussed, but also the type of data carriers and what the investigator should take into account when securing evidence.

DataExpert

For whom is this training intended?

This four-day training is designed for beginning digital investigators who are not yet familiar with the basics of Digital Forensics.

What do you learn during the training?

- What Magnet AXIOM is.
- How digital evidence is collected and stored. Think of the procedures and frameworks the investigator has to deal with.
- Disk geometry such as defining and articulating certain parts of hard drives and similar media and what basic components they contain, how the capacity of a disk is calculated, and the difference between CHS and LBA sector numbering.
- The basics of data storage (bits, bytes and hex). This includes the associated number systems and how the basic process works from pressing a key to storing it on a hard drive.
- Everything about partitioning, formatting and file systems including the differences, the structuring and the processes involved.
- What a boot process and drive letter assignments means and how it works.
- What the principles of data storage are and how sectors on a data carrier are affected when files are stored, moved and deleted.
- What information the Windows Registry contains and where the most common artifacts are located.
- How images can be created from computer media and mobile devices and how Magnet can support AXIOM in this.
- How to gain insight into iPhone and Android mobile devices and how to use rooting and jailbreaking to gain access to suspicious devices.

Additional information

This training is modular. Each module uses scenarios and hands-on exercises to reinforce the learning objectives. Furthermore the course is taught in English and can be offered in both online or in classroom setup.

Magnet AXIOM Examinations (AX200)

In this hands-on course, the participant learns in an interactive manner how to handle digital evidence that is found on computers and mobile phones. In this course, the focus is on the traces that are found after internet use, use of Social Media and apps on mobile phones. Magnet AXIOM goes beyond looking for and processing artefacts because deep analysis using tools that enable you to look at the evidence in new ways. After the AXIOM installation, the participants will get to work with searching and analysing the data, after which the findings are documented in a report.

For whom is this training intended?

This four-day training is designed for digital investigators of investigative services from the forensics community

like police, defense, special task forces but also private investigation institutes. The course is suited for both new digital investigators as well as ones who have already been using AXIOM for a while but haven't yet undergone training.

What will you learn during the training?

After the training, the participants are able to:

- To configure Magnet AXIOM.
- To get the most important evidence (image material) from the computer and smartphones.
- How to recover the most relevant information.
- To explore the evidence in a more in-depth way.
- Simplifying the analysis activities of intuitive linking of facts and data.
- Preparing the most important artefacts for collaboration with other stakeholders.

Additional information

This training is modular. Every module uses an extensive base of scenarios and hands on exercises in Magnet AXIOM, to strengthen the learning goals and provide further insight to the participant into the Magnet AXIOM feature and its application in the forensic workflow. Furthermore the course is taught in English and can be offered in both online and frontal-teaching formats.

Magnet AXIOM Advanced Computer Forensics (AX250)

This is the continuation of the AX200 training. In this hands-on course, participants interactively learn how to deal with digital evidence found on computers. The focus is on the traces found after Internet use, use of social media and apps. Magnet AXIOM goes beyond finding and processing of artifacts by enabling deep analysis using these tools to look at evidence in new ways. This course covers the following topics: advanced search methods in RAM memory, encryption, decrypting Windows passwords and searching for missing information in cache files.

For whom is this training intended?

This four-day training course is designed for digital investigators from the forensics community such as police, defence, special task forces but also private investigative agencies. The course is suitable for advanced digital investigators, as well as those who have already completed the AX200 training.

What do you learn during the training?

After the training, the participants will be able to:

- Configure Magnet AXIOM.
- Understand the operation of Windows 10 and its forensic implications.
- Use register locations and track volume serial numbers.
- Filter and search for relevant artifacts.
- Further investigate app data.

DataExpert

- Further investigate prefetch files.
- Determine the use of an encrypted container.
- Investigate iOS backups and use the AXIOM Wordlist Generator.
- Identify cloud data and further investigate a Gmail account.

Additional information

This training is modular. Each module makes use of an extensive basis of scenarios and hands-on exercises, in order to strengthen the learning objectives and give the participant further insight into the functionality of Magnet AXIOM and its application within the forensic workflow. Furthermore the course is taught in English and can be offered in both online and frontal-teaching formats.

Magnet AXIOM Advanced Mobile Forensics (AX300)

This is the continuation of the AX200 training. In this hands-on course, participants interactively learn how to deal with digital evidence found on mobile phones. The focus is on the traces found after Internet use, use of social media and apps on mobile devices. Magnet AXIOM goes beyond finding and processing of artifacts by enabling deep analysis using these tools to look at evidence in new ways. During this training, the following topics will be discussed: advanced techniques such as Chip-Off, JTAG and ISP, and the operation of iOS and Android operating systems.

For whom is this training intended?

This four-day training course is designed for digital investigators from the forensics community such as police, defence, special task forces but also private investigative agencies. The course is suitable for advanced digital investigators, as well as those who have already completed the AXIOM AX200 training.

What do you learn during the training?

After the training, the participants will be able to:

- Configure Magnet AXIOM.
- Distinguish the different acquisition methods such as Chip-Off, JTAG and ISP.
- Understand the iOS operating system and how to image Apple devices.
- Understand the Android operating system and how to image Android devices.
- Apply the Media Transfer Protocol (MTP).
- Use the Dynamic App Finder.
- Determine the use of an encrypted container.
- Create XML artifacts and carve data from SQLite databases.

Additional information

This training is modular. Each module makes use of an extensive basis of scenarios and hands-on exercises, in order to strengthen the learning objectives and give the participant further insight into the functionality of Magnet AXIOM and its application within the forensic workflow. Furthermore the course is taught in English and can be offered in both online or in classroom setup.

Magnet GK200 GRAYKEY Examinations (AX301)

In this hands-on course, participants interactively learn how to deal with digital evidence found on iOS devices combined with Graykey. Magnet AXIOM goes beyond finding and processing of artifacts by enabling deep analysis using these tools to look at evidence in new ways. During this training, the following topic will be discussed: AXIOM in combination with the GRAYKEY unit.

For whom is this training intended?

This four-day training course is designed for digital investigators from the forensics community such as police, defence and special task forces. The course is suitable for the advanced digital investigator, as well as for those who have been using AXIOM for some time but have not yet completed the training. Only for government agencies after acceptance of Grayshift!

What do you learn during the training?

After the training, the participants will be able to:

- Configure Magnet AXIOM.
- Use the GRAYKEY unit in combination with AXIOM.
- Compare different types of data extraction.
- Understand the iOS operating system and Apple security.
- Use the Dynamic App Finder and other functions such as 'Search for Custom Files by type'.
- Further investigate artifacts found.

Additional information

This training is modular. Each module makes use of an extensive basis of scenarios and hands-on exercises, in order to strengthen the learning objectives and give the participants further insight into the functionality of Magnet AXIOM and GRAYKEY and its application within the forensic workflow. Furthermore the course is taught in English and can be offered in both online or in classroom setup.

Magnet AXIOM Incident Response Examinations (AX310)

During the AXIOM Incident Response Examinations (AX310) training, participants learn how to conduct a digital forensic investigation of a malware incident using a hands-on case. For this they use Magnet AXIOM and the associated Incident Response Toolkit.

For whom is this training intended?

This four-day training is designed for digital investigators who are familiar with the principles of digital forensics and want to expand their knowledge with advanced forensic and incident response techniques. It is recommended that participants complete the Magnet AXIOM Examinations (AX200) training first.

DataExpert

What do you learn during the training?

- Which functionalities Magnet AXIOM has.
- What malware is, what traces it leaves behind, how it behaves and how it can be stopped.
- How malware can penetrate and move through network traffic and how network traffic can be captured, filtered, and analysed during a malware forensic investigation.
- How WireShark works.
- How to use the Incident Response Toolkit to collect volatile data from a computer and create output using AXIOM to locate the malware.
- How to analyse the RAM memory of a computer involved in a malware incident and map which programs were running at the time and from which location.
- How PCAP files can be processed from RAM memory to support a forensic investigation.
- How a static analysis of malware can be performed using a virtual machine.
- How to create a dynamic analysis of malware.
- How to create a report of a malware investigation using AXIOM's artifact-first approach.
- How all the separate elements of a study can be extracted and correlated with each other.

Additional information

This training is modular. Each module uses scenarios and hands-on exercises to reinforce the learning objectives. Furthermore the course is taught in English and can be offered in both online or in classroom setup.

Magnet AXIOM Internet and Cloud Investigations (AX320)

This is expert training. It is strongly recommended to complete the AX200 training first. In this hands-on course, participants interactively learn how to deal with digital traces found on the Internet and in the cloud. The focus is on the traces found after Internet use, use of social media and apps. Magnet AXIOM goes beyond finding and processing of artifacts by enabling deep analysis using these tools to look at evidence in new ways. This course focuses on the acquisition and investigation of cloud data using AXIOM and open-source tools and techniques.

For whom is this training intended?

This four-day training course is designed for digital investigators from the forensics community such as police, defence, special task forces but also private investigative agencies. The course is suitable for advanced digital investigators who want to expand their knowledge in the field of cloud investigation and social media forensics.

What do you learn during the training?

Topics that will be discussed during the training are:

- Investigation methods for cloud data.
- The cloud aspects of Apple, Google, Microsoft, Twitter, Facebook, Instagram, Dropbox, Box and E-mail.
- Repetition of what has been learnt incl. final exercise.

Additional information

Each module makes use of an extensive basis of scenarios and hands-on exercises, in order to strengthen the learning objectives and give the participant further insight into the functionality of Magnet AXIOM and its application within the forensic workflow. Furthermore the course is taught in English and can be offered in both online or in classroom setup.

Magnet AXIOM macOS Examinations (AX350)

During the AXIOM macOS Examinations (AX350) training, participants learn how to examine devices that run on the macOS operating system.

For whom is this training intended?

This four-day training is designed for digital investigators who are familiar with the principles of digital forensics and who wish to expand their knowledge in the areas of macOS and device forensic analysis based on the APFS file system and AXIOM. We recommend that participants first complete the AXIOM Examinations (AX200) training before starting this training.

What do you learn during the training?

- The basics of the macOS operating system and the APFS file system including the changes in the security of macOS devices and what the main components of the macOS operating system are.
- What encryption challenges exist and how they can be investigated using Passware.
- What different macOS logs there are and what log artifacts can be found.
- What the KnowledgeC database and powerlog database mean that are stored on macOS.
- What internet artifacts there are.
- What specific details of a user account may be of interest to a forensic investigation.
- How to recover artifacts and attachments from the standard mail application Mail.App.
- What useful information can be found on a desktop. For example, which items are stored in the mac Dock, the application of the menu bar, recently used items and thumbnails.
- What the Time Machine and Snapshot features of MacOS and the APFS file system mean.
- How macOS cloud services are used and which databases control the data flows between the cloud services and the host computer.

Additional information

This training is modular. Each module uses scenarios and hands-on exercises to reinforce the learning objectives. Furthermore the course is taught in English and can be offered in both online or in classroom setup.

DataExpert

Oxygen Forensic Bootcamp (OFBC)

The focus of this three-day training is on analysing the data and creating a report with Oxygen Forensic Detective. Data extraction from a mobile device is only dealt with globally in this training. Participants will learn how to import and analyse extractions from Android, Apple and other data types.

For whom is this training intended?

This practical three-day training is intended for participants who already have basic knowledge of acquiring and analysing mobile devices such as smartphones and iPads.

What do you learn during the training?

This training is a mix of theoretical and practical sessions and concludes with an exercise in which a major case is examined. This involves the following aspects:

- Installation and configuration of the Oxygen Forensic Detective software.
- Interpretation of the user interface.
- Extraction and import options of the software.
- How to interpret the data.
- Investigation of categories such as calls, contacts and accounts.
- Analysis of the timeline, social media and photos.
- Understanding the 'Key Evidence Manager'.
- Categorisation of faces (Facial recognition)
- Other Oxygen tooling such as Oxygen Maps., Oxygen Cloud Extractor etc.
- Keyword Search.
- Searching for Wi-Fi connections and locations.
- Searching for passwords and tokens.
- How to deal with backups.
- Data export and reporting functionality.

At the end of this training the participants will have insight into the possibilities of the Oxygen Forensic Detective platform. The participants have acquired knowledge about extracting data from devices (iOS, Android and KaiOS).

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

Oxygen Forensic Advanced Analysis (OFAA)

This hands-on training is a continuation of the Oxygen Forensic Bootcamp Training (OFBC) and delves deeper into the functionalities of Oxygen Forensic Detective. The goal of the training is to gain in-depth knowledge of mobile forensics using this tool.

For whom is this training intended?

This three-day training is suitable for digital investigators who want to further specialise in collecting and analysing mobile data from smartphones and iPads. It is a requirement to attend the Oxygen Forensic Bootcamp Training (OFBC) prior to this training.

What do you learn during the training?

After completing this training, participants are aware of the functionalities Oxygen Forensics has to offer. Among other things, they know how to analyse, parse and recover data using this technology. They also learned to work with advanced tools like Call Data Record expert, SQLite, Property list viewer and Oxygen Maps. Furthermore, participants will learn to investigate IoT devices and merge and correlate data from multiple sources for their investigation.

Additional information

The course is taught in English and can be offered in both online or in classroom setup.

Oxygen Forensic Cloud Extraction (OFCE)

The focus of this training is on collecting data from the cloud using Oxygen Forensic KeyScout. A number of different platforms will be covered during the training, including Apple and Google.

For whom is this training intended?

This one-day training is suitable for digital investigators who are already familiar with Oxygen Forensic Detective and who want to learn how to conduct an investigation in the cloud with KeyScout.

What do you learn during the training?

- Extracting cloud-based repositories using Oxygen Forensic KeyScout and Oxygen Forensic Detective with the goal of obtaining login credentials and tokens to access cloud platforms.
- What problems can arise with two-factor authentication.
- How to restore a WhatsApp database.
- What type of data can be collected on platforms such as Amazon, Google, WhatsApp and Apple services using the Oxygen Forensic Cloud Extractor.
- How a dead box recovery from hard drives taken from computers, forensic images and live machines can be performed using Oxygen Forensic KeyScout.
- How search paths and search profiles can be tailored and how these results can then be stored for further analysis with Oxygen Forensic Detective.

Additional information

The course is taught in English and has an online format.

DataExpert

Oxygen Forensic Extraction in a Box (XiB)

This three-day hands-on training focuses on extracting data from mobile phones. The focus is on data extraction from Android, Apple and KaiOS devices, but Drones, SD cards and SIM cards are also investigated.

Each participant will be given a plastic box containing 10 different phones as a base at the start of the course, hence the title of the training. The Oxygen Forensic Extractor, part of Oxygen Forensic Detective, is used for this.

Who is this training for?

This course is suitable for participants with a basic knowledge of mobile forensics.

What do you learn during the training?

- Logical, physical and OxyAgent extraction methods
- Basics of Full Disk encryption and File-based encryption
- Decryption, bypass, Emergency Download (EDL) and ADB techniques

Additional information

The course is taught in English and has a classroom setup.

Teel Technologies Advanced Flasher Box & Bootloader Forensics

During this five-day hands-on training, investigators will learn how to decrypt and read the memory of mobile devices using the most common Flasher Box and Bootloader tools. This technique is particularly useful where standard tooling is not sufficient. This method can be used on high-end Android devices such as Samsung smartphones, as well as on simple mobile phones with MediaTek or Chinese chipsets.

Flasher Box

During this part of the training, the students get an overview of the most common Flasher Box tools. In addition, the students will start installing and using these tools themselves. This involves the use of various models that may be kept after the end of the training.

Bootloader

During this part of the training, students will learn how to access partitions on mobile devices for unlocking or bypass purposes. You will learn how to apply ADB Commands, how to identify and bypass FRP locks on a mobile phone, how to use CWM and TWRP to unlock a mobile device and to access or copy the memory.

For whom is this training intended?

This training is intended for investigators who have experience in the field of Mobile Forensics and want to increase their knowledge in the field of analysis of mobile devices.

What do you learn during the training?

At the end of this training, participants will be able to independently access and decrypt mobile devices using advanced techniques. After completion, each student will receive a complete Flasher and Unlock kit consisting of an NCK dongle, an XTC clip with Y-cable and an EFT dongle.

Additional information

The course is taught in English and has a classroom setup.

Teel Technologies Board Level Repair for the Digital Forensic Examiner

There is a wide variety of tooling available for reading and analysing mobile devices. While much is possible, there are also limitations. Faulty smartphones can often only be read at board level. Data extraction then takes place directly on the chip. This does mean that the device in question must be dismantled. During this hands-on training, participants learn diagnostic skills, troubleshooting and the latest repair techniques with state-of-the-art equipment.

For whom is this training intended?

This five-day training course is suitable for digital investigators and specialists who have to deal with damaged data carriers during their forensic investigations.

What do you learn during the training?

- Restore data present on a damaged data carrier (e.g. water damage).
- Which tools can be used to repair defective devices.
- Recognise when data is irretrievable.
- The operation of circuit boards.
- The operation of Surface Mount Components (SMCs).
- Precise soldering techniques, repair and so-called reballing.
- Read diagrams.
- And so much more!

Additional information

The course is taught in English and has a classroom setup.

DataExpert

Teel Technologies Chip-Off 2.0 Forensics

During the five-day Teel Tech Chip-Off Forensics training, participants learn how to remove memory chips from mobile devices like smartphones, prepare them and read them to acquire data using specialist equipment.
In the first half of the training, the focus is on comprehending the construction of the devices and how to best remove the chip without damaging it. Additionally, the participants get insight into the different memory structures of mobile devices (mobile phones, tablets, SSD hard drive etc.) and how the Chip-Off can be used to collect data. In the second half of the training, participants learn the basic principles of the memory structure and how they can use available tools to read the chip's memory. Participants can put the acquired knowledge to practice by practising on a BlackBerry device containing data.

For whom is this training intended?

This Chip-Off training is intended for participants who are familiar with the concept of raw data, have ample experience in analysing it and want to increase their knowledge of chip-off methodologies.

What will you learn during the training?

After following this training, the participants will have the following competencies:

- Removing a BGA chip from a device the proper way.
- Treatment and preparation of the chip for reading.
- Reading the chip to gain data.
- Applying tools and techniques to decode the information found.
- Practical knowledge about the Chip-Off process of a blocked, unlocked BlackBerry and then the use of forensic software to create and analyse the data dump.

Additional information

The course is taught in English and has a classroom setup.

Teel Technologies Embedded Hardware Acquisition & Analysis

During this hands-on training, the focus is on processes that can be used to access digital data at the physical level of data carriers. These sources include:

- IOT devices
- Smart TVs
- Vehicle systems
- Drones
- Skimmers/Shimmers

For whom is this training intended?

This five-day training course is intended for digital investigators and specialists who have to deal with digital data on physical data carriers during an investigation.

What do you learn during the training?

- Basic knowledge of how electronics work in relation to techniques used in this training.
- Which (open source) sources and commercial tools can be used.
- How to adapt techniques like JTAG, ISP and Chip-Off to collect data from sources like embedded code and the flash memory of controller chips.
- How to analyse the acquired data looking for evidence and traces of malware.

Additional information

The course is taught in English and has a classroom setup.

Teel Technologies ISP Forensic

During this five-day training, investigators learn how to carry out extractions using so-called In-System Programming (ISP). This method enables investigators to gain direct access to the eMMC memory of a mobile device. eMMC is the most common type of memory that's applied to chips of current smartphones. During the ISP process, the chip doesn't have to be removed, leaving the original evidence intact. At the beginning of the training, the participants are handed a number of phones to practise Chip-Off extractions on, to learn about back-tracing and connection points and to carry out data-extractions.

For whom is this training intended?

This ISP training is intended for investigators that are experienced in Chip-Off and soldering techniques and want to broaden their knowledge regarding analysis of mobile devices.

What will you learn during the training?

At the end of this five-day training, participants are able to carry out ISP extractions independently and compare the results of the different extractions. Although a basic knowledge of soldering PCBs is assumed, there'll be plenty of practice in soldering resistors and capacitors on and off the circuit board.

Additional information

The course is taught in English and has a classroom setup.

Teel Technologies JTAG Forensic

During this five-day training, investigators will learn how to unlock the information of locked mobile phones using the JTAG process. In this, the device is completely taken apart and approached on a physical level. After the data has been copied, the participant learns how to recover the password to then decode the found information. The device is then brought back to its original state and can be unlocked using the found password. The JTAG process can be applied in the following situations:

- Locked Android devices with the USB debugging turned off.

DataExpert

- Locked Windows devices.
- Locked devices with uncommon operating systems.
- Access to the physical memory of a device if this can't be supported by tooling.
- Damaged or destroyed devices.

For whom is this training intended?

This advanced JTAG training is intended for digital investigators with proper knowledge of Computer Forensics and ample experience with investigation of mobile devices who want to broad their technical knowledge.

What will you learn during the training?

At the end of this training, participants are able to completely dismantle a working phone, read the relevant information and then reassemble the device in a non-destructive manner. Additionally, you'll be taught how to identify several Mac copy files and copies made with other tools or operating systems. The location in the file system, how to gather information in a forensically correct way and how to crack passwords will also be addressed.

Additional information

The course is taught in English and has a classroom setup.

Teel Technologies SQLite Forensics

Both Google's Android OS and Apple's iOS are dominant players in today's mobile phone market. Although these two companies are rivals, with vastly different file systems, they have one thing in common; both use SQLite as storage for user data. SQLite is a library that implements an independent, serverless, zero-configuration SQL database engine. During this training, participants will learn how to analyse and restore SQLite databases at a basic data level. Upon completion of this training, investigators with this knowledge will be able to analyse over 99% of the data they encounter on mobile devices.

For whom is this training intended?

This training is designed for digital investigators and specialists who will be dealing with mobile devices during their forensic investigations.

What do you learn during the training?

- How SQLite works at the byte level.
- What the five most common locations to recover SQLite data are.
- How to validate report data.
- What the different types of SQLite data component types are.
- Reverse engineering a SQLite database.
- Easily convert and identify virtually any data format.
- Displaying SQLite BLOB data in a forensic program.
- Recovering data from .WAL and .journal files.

- Quickly generating reports from a SQLite database with externally linked images.
- SQLite Record recovery.
- Manually parsing Write-Ahead Logs and Journal files.
- SQLite Payload investigation/SQLite Data Construct parsing.
- Manually recovering SQLite data.
- SQLite encryption.
- Using simulations to test/verify/decode data.

Additional information

The course is taught in English and has a classroom setup.

Notes

Open Source Intelligence

The Internet contains an unfathomable amount of data. This data can be of added value in investigations. By using Open Source Intelligence (OSINT), investigators can retrieve data that is important to the investigation. For example, it can be used to map social networks, collect and analyse news messages and provide insight into forum publications.

During the OSINT training sessions, investigators are taught the right skills to collect and interpret data from the public Internet. What information is true, what data is reliable and how can the found results be properly recorded? These questions are all answered during the training.

Open Source Intelligence

OSINT Training Trajectory

In recent years, OSINT has become an important tool for information and data acquisition. However, it applies to more than just the internet, and goes beyond a simple search engine query. This training trajectory offers participants a broad range of competences. It teaches them to plan and perform a complete OSINT investigation from beginning to end, to interpret the information obtained in the correct context, and to report on the findings– independent of tools and using their own skillset.

The OSINT training trajector comprises three individual courses with each course further increasing knowledge levels and expanding on competences. It covers all aspects of OSINT, both in terms of methodology and technique.

The content of this trajectory comprises the following courses:

- OSINT Basic – 3 days
- OSINT Advanced – 3 days
- OSINT Technical – 3 days

Courses are consecutive, but are scheduled individually to allow participants to process the material and reflect between courses. This process of reflection can be facilitated with the information on the e-learning platform, or by applying the knowledge from the courses to practice. In addition, it is also possible to complete one or two of the courses in the trajectory if this is adequate for the participant's job description. Each course is individually accredited by SPEN/CPION. This means that, upon successful completion of one of these courses, the participant will obtain the associated recognised title and diploma.

For whom is this training intended?

This trajectory is suitable for anyone using the internet for investigations, including police and other investigations and safety services, thematic reviewers, bank analysts (CDD, KYC, AML) and private investigators.

What do you learn during this training trajectory?

After completing the OSINT Basic, Advanced and Technical courses, participants will be able to plan, conduct, and report in simple and (more) complex OSINT investigations, while keeping an eye on potential harm risks and their own safety. Participants will also be able to construct their tools to perform investigations based using their own skillset. For more detailed course contents, please refer to the individual courses.

Additional information

The courses in this trajectory are supported through the DataExpert e-learning platform, where participants can learn the theory through both text and short videos. In addition, the courses are in English and can be offered in both online or in classroom setup.

DataExpert

OSINT Basic - Registered OSINT Practitioner ®

By using Open Source Intelligence, also known as Internet investigation, it is possible to find relevant data from digital open sources during fraud, cybercrime and/or criminal investigations.

During the “OSINT Basic” training, the participants learn the basic skills needed to conduct a good investigation on the Internet. After completing this training, the participants can conduct an investigation on the Internet, interpret the information found and then verbalise/report it in the correct context.

This training is an accredited SPEN-register training. If you take and successfully complete a final test, you will receive a diploma from the Stichting Permanente Educatie Nederland (SPEN) and you may use the title “Registered OSINT Practitioner ®” (in short: ROP). This also means that you will be registered in the graduate register of the Centrum voor Post Initieel Onderwijs Nederland (CPION) and will receive Personal Education (PE) points.

For whom is this training intended?

This three-day training course is suitable for anyone who uses the Internet for investigations, including police and other investigative and security services, thematic analysts, analysts at banks (CDD, KYC, AML), private investigators and more.

What do you learn during the training?

At the end of this training, the participant has insight into the possibilities of the Internet and digitisation in the world of investigation. The participant has learnt to make effective use of search engines, investigate images, e-mail headers and has taken the first steps in investigating on social media (SOCMINT). The participant also knows how to search within websites, where data can be claimed (if authorised) and what techniques are available to operate anonymously.

Additional information

This course is part of the OSINT training trajectory that also includes the Advanced and Technical courses. The training is supported through DataExpert’s e-learning platform, where participants can learn the theory through both text and short videos. In addition, the courses are in English and can be offered in both online or in classroom setup.

OSINT Advanced - Registered OSINT Specialist ®

By using Open Source Intelligence, also known as Internet investigation, it is possible to find relevant data from digital open sources during fraud, cybercrime and/or criminal investigations.

During the “OSINT Advanced” follow-up training, the participants learn additional skills required to conduct an in-depth investigation on the Internet. After completing this training, the participants can conduct an extensive investigation on the Internet and the dark web. They can interpret the information they encounter and then verbalise/report it in the right context.

This training is an accredited SPEN-register training. If you take and successfully complete a final test, you will receive a diploma from the Stichting Permanente Educatie Nederland (SPEN) and you may use the title "Registered OSINT Specialist ®" (in short: ROS). This also means that you will be registered in the graduate register of the Centrum voor Post Initieel Onderwijs Nederland (CPION) and will receive Personal Education (PE) points.

For whom is this training intended?

This three-day training course is suitable for anyone who uses the Internet for investigations, including police and other investigative and security services, thematic analysts, analysts at banks (CDD, KYC, AML), private investigators and more. However, we do advise the participant to first complete the OSINT Basic training successfully.

What do you learn during the training?

At the end of this training, the participant has insight into the possibilities of deeper investigation on the Internet and the dark web. The participant has learnt to make effective use of advanced search techniques, geolocation investigation and has taken advanced steps in investigating on social media (SOCMINT). The participant is also able to set up virtual investigation environments and initiate investigations into cryptocurrencies, including Bitcoin.

Additional information

This course is part of the OSINT training trajectory that also includes the Basic and Technical courses. The training is supported through DataExpert's e-learning platform, where participants can learn the theory through both text and short videos. The course is taught in English, and can be offered in both onlin or in classroom setup.

OSINT Technical - Registered OSINT Technical Specialist ®

By using Open Source Intelligence, also known as Internet investigation, it is possible to find relevant data from digital open sources during fraud, cybercrime and/or criminal investigations. During the "OSINT Technical" follow-up training, the participants learn the 'technical' skills needed to conduct an in-depth investigation on the Internet using Linux, scraping and other tools. After completing this training, the participants can conduct a partially automated investigation on the Internet using tools, virtual machines and Python.

This training is an accredited SPEN-register training. If you take and successfully complete a final test, you will receive a diploma from the Stichting Permanente Educatie Nederland (SPEN) and you may use the title "Registered OSINT Technical Specialist ®" (in short: ROTS). This also means that you will be registered in the Education (PE) points.

For whom is this training intended?

This three-day training course is suitable for anyone who uses the Internet for investigations, including police and other investigative and security services, thematic analysts, analysts at banks (CDD, KYC, AML), private in-

vestigators and more. We advise participants to successfully complete the OSINT Basic and OSINT Advanced training courses befo¬re participating in this training.

What do you learn during the training?

At the end of this training, the participant has insight into the possibilities of deeper (technical) investigation on the Internet. The participant has an understanding of ports and protocols and knows how to make effective use of the Linux command line. The participant can also use Python scripts and scrapers to perform automated investigations using, among other things, APIs.

Additional information

This course is part of the OSINT training trajectory that also includes the Basic and Advanced courses. The training is supported through DataExpert's e-learning platform, where participants can learn the theory through both text and short videos. The course is taught in English, and can be offered in both online r in classroom setup.

OSINT Onl1ne G4ming

The online gaming community is growing faster than ever. There are more than 715 million gamers in Europe alone. As a result, more and more platforms have emerged or evolved in recent years to support these online communities. However, these platforms are also increasingly used by (cyber) criminals to support criminal activities, such as exploitation, money laundering, fraud, or hacking. Unnoticed, millions of euros are circulating in this relatively invisible world.

For many investigators, this is a new (virtual) world in which investigative opportunities arise, provided they know how to use them. During the training, topics such as terminology, online communities such as Reddit, underground (gaming) markets, and platforms such as Twitch are covered.

So, whether you're an online gaming n00b or a pro with serious skills, this training led by one of our dungeon masters will have you safely farm your XP to take OSINT skills to the next level.

For whom is this training intended?

This two-day training is suitable for anyone who uses the internet in (criminal) investigations, including the police, defense, and other investigative and security services, thematic investigators, analysts at banks (CDD, KYC, AML), insurers, private investigators, and more.

We advise participants to complete the OSINT Basic and OSINT Advanced training before attending this training.

What do you learn during the training?

At the end of the OSINT Online Gaming training, the participants have gained insight into the most popular online gaming platforms and the associated communities and social media platforms. The participant recognizes the detection opportunities and challenges that such an investigation entails and knows how to use them if

possible. In addition, the participant is able to conduct research on various online gaming platforms and report the findings.

Python

During the training the participants will learn how to programme in Python. This dynamic programming language is 'easy to learn and hard to master'. Because of its simple set-up Python is the go-to programming language for beginners. With Python it is possible to relatively simple carry out tasks and analyses, run web servers, apply artificial intelligence and more! As a beginning Python programmer the participants will learn the intricacies of this programme language in a five-day training.

For whom is this training intended?

The training is for participants who have some technical experience of computers and want to upgrade their skill-set.

What will you learn during the training?

- The Python Interpreter.
- The basis of the Python language.
- The basic principles of reading and writing files.
- Working with 'packages'.
- To manage various programming environments.
- Analysing an extended logfile.
- Making a web crawler.

Additional information

The course is taught in English, and can be offered in both online or in classroom setup.

Refresher Training

The knowledge and skills attained during a course usually fade over time. In addition, there are always new developments within the OSINT and digital field which are of added value to address. Training is an excellent possibility to recover knowledge and skills within a short period.

Freshen up the most important highlights from our OSINT course(s) and apply this knowledge and software to solve issues.

DataExpert

Private Training

Aside from our standard training, we also offer customised training. We view the wishes and needs together of your organisation together and tailor the course material if needed. We'd love to contribute if you have specific wishes.

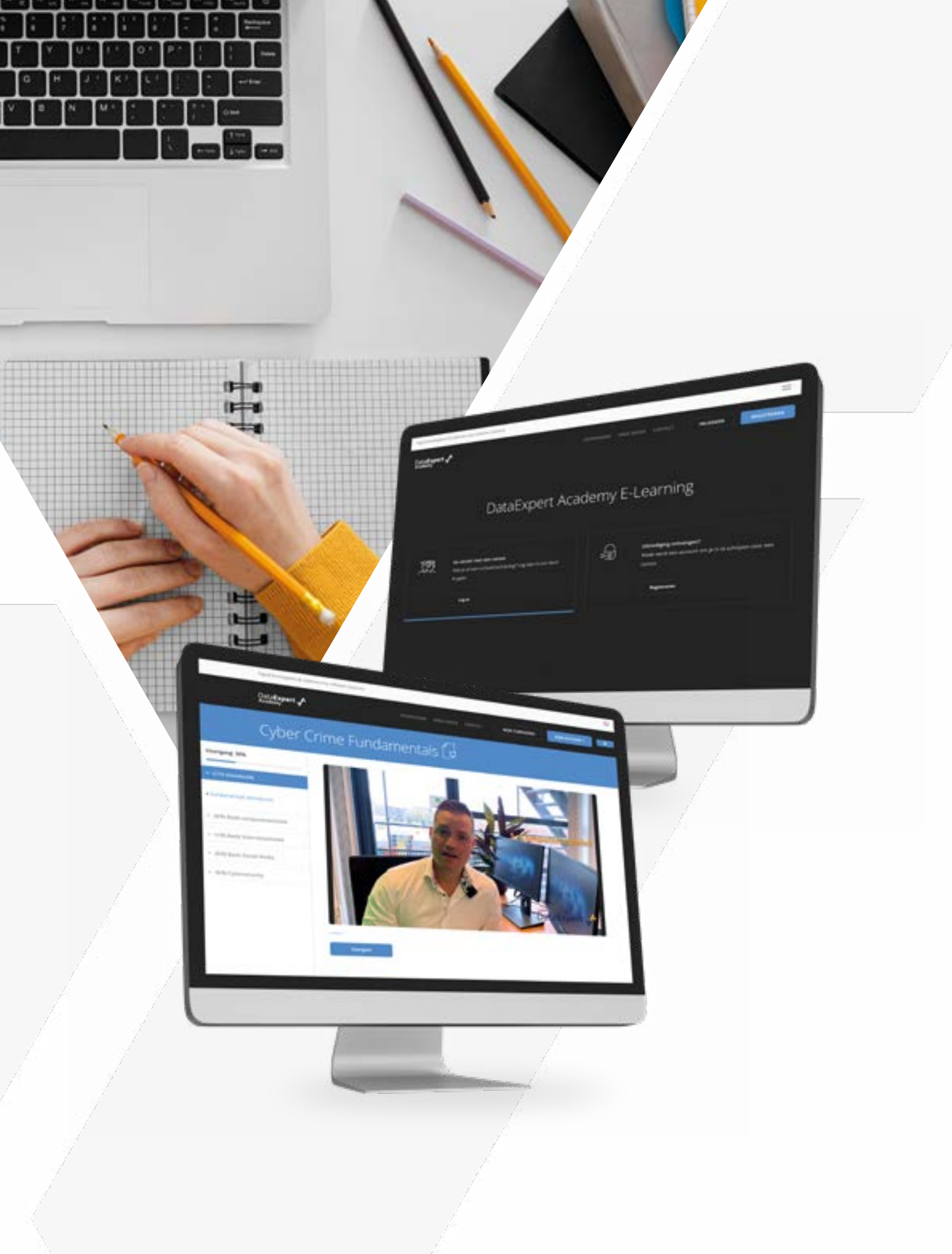
A customised training can be defined as:

- Training for 1 or more participants from the same organisation.
- Training is completely tailored to the wants of the trainees or organisation.
- Training can take place at your location or at DataExpert in Veenendaal.
- Contents of the training can be tailored in advance and in agreement with the trainer.
- Your own data or example data can be used during the training (if GDPR proof).
- The duration of the training is determined in advance with the training and is partially dependent of the amount of material and the number of trainees.

Please contact us for information about the various possibilities!

> THE GREAT AIM OF EDUCATION IS NOT KNOWLEDGE BUT ACTION.
>
> HERBERT SPENCER

> DEVELOP A PASSION FOR LEARNING. IF YOU DO, YOU WILL NEVER CEASE TO GROW.
>
> ANTHONY J. D'ANGELO


DataExpert Academy E-Learning
Cyber Crime Fundamentals

The DataExpert e-learning platform

At DataExpert, we value clear and transparent knowledge transfer. We do this by offering a combination of learning methods.

Pre-learning

A number of training courses in our portfolio are supplemented with one or more pre-learning modules. These are self-paced, online classes that can be followed in the e-learning platform. These modules allow the course participant to gain knowledge in their own time before participating in a classroom training.

Self paced training

We also offer e-learning-only training through our e-learning platform. These are training courses which the participant can follow at his/her own time and pace. In this training, the participant will find a series of instructions and assignments in our platform.

Video materiaal

Many of our training courses include written material as well as videos. These videos complete the blended learning experience. For a select number of training courses, for example in the field of cybercrime, all modules include both text and video material.

Knowledge base

We offer various training courses in a classroom setting. These are part of a scheduled programme and are led by a professional trainer. Our e-learning platform fulfils the role of knowledge base in this setup; all the training material can be consulted here.

Tests

If applicable, the participant concludes the lessons in the e-learning platform with a test. These tests are multiple choice or open assignments. The result of a multiple choice test is immediately known and recorded with one's progress. In case of an assignment, the instructions for it can be found in the platform.

DataExpert

Digital Badges

A training course requires time, effort, and attention. You will have acquired new skills and methodologies that you can immediately apply in your investigation. Besides receiving a diploma or certificate, we at DataExpert believe that this should be rewarded and shown. DataExpert therefore offers participants for a large part of our courses a Digital Badge. Each training course has its own learning objectives and therefore its own badge.

Cybercrime

Analytics

Digital Forensics

Open Source Intelligence

Notes

More information:

DataExpert BV – The Netherlands
+31 (0)318 543173
info@dataexpert.nl

DataExpert ApS – Denmark
+45 5350 6959
info@dataexpert.dk

DataExpert Nordic AB - Sweden
+46 735 000644
info@dataexpert-se.se