Python Forensics

Duur: 4 dagen Prijs: € 2650

Open Rooster

Python Forensics

Doelgroep voor de Cursus Python Forensics

De cursus Python Forensics is bedoeld voor developers en analisten die Python willen leren gebruiken voor opsporings onderzoek ter ondersteuning van het juridische proces.

Voorkennis voor de Training Python Forensics

Ervaring met Python programmeren is niet strikt noodzakelijk om deel te nemen aan deze cursus. Ervaring in Python programmeren is wel bevorderlijk voor een goede begripsvorming.

Uitvoering Training Python Forensics

De theorie in de cursus Python Forensics wordt behandeld aan de hand van presentatie slides. Illustratieve demo's verduidelijken de concepten. De theorie wordt afgewisseld met oefeningen. De cursustijden zijn van 9.30 tot 16.30.

Certificaat Python Forensics

De deelnemers krijgen na het goed doorlopen van de cursus een officieel certificaat Python Forensics.

Inhoud Cursus Python Forensics

In de cursus **Python** Forensics leren de deelnemers de programmeer taal Python te gebruiken voor het onderzoek van data op desktop computers en mobile devices en de analyse van het berichten verkeer ter ondersteuning van opsporingsonderzoek.

Device Data Analysis

De cursus is gericht op het onderzoek en de analyse van de data die op devices aanwezig zijn in file systemen, browsers, log files en andere data bronnen.

Python Fundamentals en Libraries

In de eerste plaats wordt ingegaan op de fundamentals van de Python programmeer taal waarbij data types, control flow, classes, modules, packages en comprehensions aan de orde komen.
Ook diverse Python Libraries die van belang zijn bij opsporingsonderzoek worden daarbij besproken zoals de Regular Expression pattern matching library, de log library en de library Date en Time library.

File en Database Analysis

Vervolgens wordt uitgebreid aandacht besteed aan de benadering van het file systeem en de analyse van files. Speciale onderwerpen daarbij zijn de creatie van Artifact Reports en de hashing van Data Streams. Ook de analyse van databases zoals SQLite, het identificeren van gaps daarin en data recovery zijn onderdeel van het cursus programma. Voorts wordt besproken hoe uit Wi-Fi berichten locatie gegevens kunnen worden achterhaald en wordt de analyse van web server logs besproken.

Audio en Video Analysis

Aan de orde komt ook de analyse van audio en video data en de mining van PDF en Office Metadata. De registry kan eveneens belangrijke informatie verschaffen en de analyze daarvan wordt besproken.

Mail Box Analysis

Tenslotte wordt ingegaan op de analyse van PST and OST mail boxes, het lezen en analyseren van EML files en de opsporing en het gebruik van Key Loggers.

Modules Cursus Python Forensics

Module 1 : Python Essentials	Module 2 : Classes and Objects	Module 3 : Python Libraries
Python 2 versus Python 3 Lines and Indentation Python Data Types Numbers and Strings Lists and Tuples Sets and Dictionaries Python Flow Control Comprehensions Functions Modules and Packages Exception Handling	Python Object Orientation Creating Classes Class Members Creating and Using Objects Property Syntax Static Methods Encapsulation Inheritance and Polymorphism Constructor Chaining Overriding Methods Abstract Classes	Regular Expressions Logging Log Configuration Generators Unit Testing Dates and Times JSON Access XML Access Numpy Library Pandas Library Plotting
Module 4 : File Analysis	**Module 5 : DB and Mobile Data**	**Module 6 : Extracting Metadata**
File I/O Iterating over Files Recording File Attributes Copying Files Attributes and Timestamps Hashing Data Streams Creating Artifact Reports Working with CSVs Visualizing Events with Excel Parsing PLIST Files	Database Access Python DB API Handling SQLite Databases Identifying Gaps in SQLite Logging Results Putting Wi-Fi on the map Recover Messages Log-Based Artifact Recipes Parsing IIS Web Logs Interpreting daily.out Log	Audio and Video Metadata Mining for PDF Metadata Review Executable Metadata Office Document Metadata Metadata Extractor with EnCase Networking Analysis Compromise Recipes Jump start with IEF Taking Names Recipes Viewing MSG Files
Module 7 : Forensic Artifacts Recipes	**Module 8 : Parsing PST Containers**	**Module 9 : Key Loggers**
Forensic Evidence Recipes Opening Acquisitions Gathering Media Information Processing Container Files Searching for Hashes Searching High and Low Reading the Registry Gathering User Activity Parsing Prefetch Files Indexing Internet History Dissecting the SRUM database	Personal Storage Table PST and OST Mailboxes libpff and pypff Reading Emails Parsing EML files Traversing Folders Summarizing Data Using HTML Templates Heat Map Word Statistics pffexport and pffinfo	Detecting Malicious Processes Hardware Keyloggers Software Keyloggers Monitoring Keyboard Events Capturing Screenshots Capturing Clipboard Monitoring Processes Multi Processing Keylogger Controllers Special Keys Non-English Keyboards