Python Forensics

Audience Course Python Forensics

The course Python Forensics is designed for developers and analysts who want to learn how to use Python for criminal investigation to support the legal process.

Prerequisites Training Python Forensics

Knowledge and experience with Python programming is not strictly necessary to participate in this course. Experience in Python programming is beneficial to good understanding.

Realization Training Python Forensics

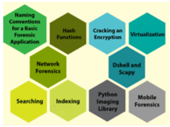
The theory in the course Python Forensics is discussed on the basis of presentation slides. Illustrative demos clarify the concepts. The theory is interchanged with exercises. Course times are from 9:30 to 16:30.

Certificate Python Forensics

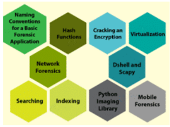
After successful completion of the course the participants receive an official certificate Python Forensics.

Duration: 4 days **Price: € 2450**

Open Schedule



Python Forensics



Content Course Python Forensics

In the course Python Forensics the participants learn to use the Python programming language for the investigation of data on desktop computers and mobile devices and the analysis of message traffic to support investigative research.

Device Data Analysis

The course targets the research and analysis of the data present on devices in file systems, browsers, log files and other data sources.

Python Fundamentals and Libraries

In the first place the fundamentals of the Python programming language are discussed in which data types, control flow, classes, modules, packages and comprehensions are discussed. Various Python Libraries that are important in criminal investigations are also discussed, such as the Regular Expression pattern matching library, the log library and the Date and Time library.

File and Database Analysis

Subsequently extensive attention is paid to the approach to the file system and the analysis of files. Special topics are the creation of Artifact Reports and the hashing of Data Streams.

The analysis of databases such as SQLite, identifying gaps in them and data recovery are also part of the course program. Furthermore it is discussed how location data can be retrieved from Wi-Fi messages and the analysis of web server logs is treated.

Audio and Video Analysis

The analysis of audio and video data and the mining of PDF and Office Metadata are also part of the course schedule. The registry can also provide important information and its analysis is discussed.

Mail Box Analysis

Finally attention is paid to the analysis of PST and OST mail boxes, the reading and analysis of EML files and the detection and use of Key Loggers.

Modules Course Python Forensics

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