Zertifikatsprogramm - Z202

Python 1 - Programmierung und Forensik

- Einführung in Python
- Forensische Analyse mit Python: Datenbanken und Anwendungen
- Forensische Analyse mit Python: Windows

Prof. Dr. Martin Rieger
Patrick Eisoldt, M.Eng.
David Schlichtenberger, M.Sc.

Open C³S
Open Competence Center for Cyber Security

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Python 1 – Programmieren im IT-Security-Umfeld

Studienbrief 1: Einführung in Python

Studienbrief 2: Forensische Analyse mit Python: Datenbanken und Anwendungen

Studienbrief 3: Forensische Analyse mit Python: Windows

Autoren:

Prof. Dr. Martin Rieger

Patrick Eisoldt, M.Eng.

David Schlichtenberger, M.Sc.

2. Auflage

Hochschule Albstadt-Sigmaringen

Institut für wissenschaftliche Weiterbildung
Open C^{3}S | Zertifikatsprogramm
Steinachstraße 11
72336 Balingen

2. Auflage (2017-01-25)

Um die Lesbarkeit zu vereinfachen, wird auf die zusätzliche Formulierung der weiblichen Form bei Personenbezeichnungen verzichtet. Wir weisen deshalb darauf hin, dass die Verwendung der männlichen Form explizit als geschlechtsunabhängig verstanden werden soll.

Inhaltsverzeichnis

Einleitung zu den Studienbriefen

I. Abkürzungen der Randsymbole und Farbkodierungen

Beispiel	B
Definition	D
Exkurs	E
Merksatz	M
Quelltext	Q
Übung	Ü

II. Zu den Autoren

Prof. Dr. Martin Rieger studierte Elektro- und Informationstechnik an der Technischen Universität München und schloss an derselben Hochschule die Promotion mit Auszeichnung ab. Ein Schwerpunkt seiner Forschungsarbeit lag in der Erstellung von Methoden und Werkzeugen zur Modellierung sowie Analyse und Optimierung elektrischer Schaltungen. Er war fünf Jahre Leiter des Labors für schnelle Analog-ICs in der IC-Entwicklungsabteilung des Forschungs- und Entwicklungszentrums der Firma Thomson Multimedia in Villingen. In der Zeit bei Thomson Multimedia war er Erfinder bzw. Miterfinder an 15 deutschen, 12 europäischen und 8 weltweiten Patenten.

Seit 1993 ist er als Professor an der Fakultät Engineering der Hochschule Albstadt-Sigmaringen auf den Gebieten Informatik und Informationstechnik tätig. Im Labor für Eingebettete Systeme und IT-Sicherheit betreibt er anwendungsnahe Forschung auf den Gebieten Embedded Systems und IT-Sicherheit. Er hatte über viele Jahre an der Hochschule Albstadt-Sigmaringen Positionen als Studiendekan, Prodekan, Prorektor und Rechenzentrumsleiter inne.

Prof. Dr. Rieger ist Initiator und Gründungs-Studiendekan des Master-Studiengangs Digitale Forensik, der in Kooperation mit der Friedrich-Alexander Universität Erlangen-Nürnberg und der Ludwig-Maximilians-Universität München betrieben wird.

Er leitet das vom BMBF geförderte Zertifikatsprogramm Open-C^{3}S, das 35 Hochschul-Zertifikatsmodule auf dem Gebiet Cybersicherheit anbietet und das kooperativ von der Hochschule Albstadt-Sigmaringen, der Friedrich-Alexander-Universität Erlangen-Nürnberg, der Freien Universität Berlin, und der Ludwig-Maximilians-Universität München, getragen wird.

Patrick Eisoldt, M. Eng. hat an der Hochschule Albstadt-Sigmaringen und der Glyndŵr University in Wales studiert. 2012 schloss er erfolgreich sein Masterstudium Systems Engineering ab. Im Rahmen seiner Master-Thesis konzipierte und realisierte er einen prototypischen Editor zur Projektierung von Prozessleitsystemen der Firma Siemens nach dem Ursache-Wirkung-Prinzip. Von November 2010 bis August 2011 unterstützte er das Institut für Wissenschaftliche Weiterbildung bei der Erstellung von Studienbriefen für den Studiengang Digitale Forensik.

Seit 2012 ist er für das Open Competence Center for Cyber Security als Modulentwickler tätig.

David Schlichtenberger studierte Medien- und Kommunikationsinformatik an der Hochschule Reutlingen. Nach seinem Masterstudium arbeitete er einige Jahre als Webentwickler und Kundenberater für Internetservices. Seit November 2014 ist er als akademischer Mitarbeiter an der Hochschule Albstadt-Sigmaringen am Institut für Wissenschaftliche Weiterbildung beschäftigt.

III. Modullehrziele

Ziel dieses Moduls ist es, Aufgabenstellungen aus dem Umfeld der IT-Sicherheit mit Hilfe von Python-Programmen schnell und effektiv lösen zu können. In diesem Modul lernen Sie die Programmiersprache Python anhand von praktischen Übungen kennen. Ziel dieses Moduls ist es nicht, Vorgehensmodelle zur Softwareentwicklung zu vermitteln, wie sie bei komplexer Software benötigt werden. Mit Python sollen Sie viel mehr in der Lage sein, kleinere überschaubare Programme zu schreiben, die schnell zu Ergebnissen führen.

Python liegt in zwei Versionen vor, die beide aktiv von Programmierern verwendet werden. Die Version 3 ist mit Python 2 nicht mehr kompatibel und ist die einzige Version, die aktiv weiterentwickelt wird. In diesem Modul wird weitestgehend die aktuelle Version von Python verwendet. In einigen Abschnitten wird aber auf die Vorgängerversion zurückgegriffen, da die verwendeten Module noch nicht von den Entwicklern portiert wurden.

Neben der Programmiersprache Python wird auch das Erstellen und Verwenden von Datenbanken grundlegend erklärt. Hierfür wird das Hilfsmodul SQLite verwendet, das ein wartungsfreies Datenbanksystem enthält und Teil der Python-Umgebung ist.

Der Studienbrief 1 beschäftigt sich mit den Grundlagen der Python-Programmierung, Studienbrief 2 mit Datenbanken. Studienbrief 2 schließt mit der Untersuchung von Anwendungsartefakten an den Beispielen Skype und Firefox ab.

Der Studienbrief 3 befasst sich mit dem Thema Informationsgewinnung unter forensischen Aspekten. Die vorgestellten Beispiele sollen dabei die universellen Einsatzmöglichkeiten von Python aufzeigen und zum Experimentieren einladen.

Auf dieses Modul wird mit einem Folgemodul „Python 2 – Programmieren im IT-Security-Umfeld“ aufgebaut, bei dem der Fokus auf Penetrationstests und Netzwerkforensik liegt.

Hinweise zur Typographie

Dieses Modul enthält zahlreiche Programmbeispiele, die stets in einer `Monospace Schriftart` gehalten sind. Zusätzlich wird zwischen Beispielen ohne gelbe Kästen und Quelltext in gelben Kästen unterschieden. Die Beispiele ohne gelbe Kästen sollen in der Python-Shell der IDLE-Umgebung (siehe Abs. 1.5) realisiert werden, Quelltexte in gelben Kästen in einer Skriptdatei (siehe Abs. 1.10). Zusätzlich können die Beispiele für die Shell an der sogenannten Prompt (>>>) erkannt werden. An einigen Stellen sind die Codezeilen zu lang, weshalb sie mit einem Backslash (\) umgebrochen wurden. Der Quellcode ist somit korrekt und kann wie abgebildet ausgeführt werden.

Warum Python?

Python ist eine interpretierte höhere Programmiersprache. Es handelt sich um eine leicht zu erlernende Programmiersprache, die sich durch ihren übersichtlichen und gut zu lesenden Quellcode auszeichnet. In der Python-Shell können Befehle und deren Wirkung direkt beobachtet werden. Dies erleichtert den Einstieg in das Programmieren und ermöglicht das „schnelle Ausprobieren“, ohne das Programm gleich vollständig implementieren zu müssen. Python wird oft als Skriptsprache verwendet, es unterstützt aber unterschiedliche, fundamentale Programmierstile (Programmierparadigma) und kann auch für größere Projekte eingesetzt werden. Einer der größten Stärken von Python ist die große Sammlung an standardisierten Programmkonstrukten (Funktionen innerhalb der Standardbibliothek), wodurch sich Python für viele Anwendungsbereiche eignet. Die meisten Funktionen sind zudem plattformunabhängig und sind somit auf unterschiedlichen Betriebssystemen lauffähig. Die Community von Python erweitert das Einsatzgebiet zusätzlich durch die unzähligen Open-Source-Projekte.

Ende 2013 erreichte Python Spitzenwerte bei der Softwarequalität und zeichnete sich durch einen äußerst hohen Reifegrad aus.[1]

Im Gegensatz zu den meisten verbreiteten Programmiersprachen verzichtet Python bei der Strukturierung auf eine Klammerung und begrenzt die Blöcke stattdessen durch gleiche Einrückung. Python unterstützt sowohl objektorientierte Programmierung als auch aspektorientierte oder funktionale Programmierung. Im Gegensatz zu Java, bei dem die Grunddatentypen keine Objekte sind, ist in Python alles ein Objekt, egal ob Klasse, Typ, Methode, Modul etc. Der Datentyp einer Variable wird dynamisch vergeben uns ist an das Objekt gebunden. Die verhältnismäßig wenigen Schlüsselwörter in Kombination mit der reduzierten Syntax tragen zu einem übersichtlichen Gesamtbild des Quellcodes bei. Ein Python-Programm ist oftmals kürzer als eine Implementierung in einer anderen Sprache wie C++ oder Java[2], was sich positiv auf die Entwicklungszeit auswirken kann.

Das Zen von Python

Ein offizieller Beitrag zu den Python-Verbesserungsvorschlägen (engl. Python Enhaucement Proposals, kurz PEPs) beinhaltet die Philosophie von Python und verdeutlicht anhand von 20 Aphorismen, von denen nur 19 niedergeschrieben wurden, welches Konzept sich hinter der Programmiersprache verbirgt.[3]

Diese Leitgedanken werden auch als „das Zen von Python“ bezeichnet:

Schön ist besser als hässlich.
Explizit ist besser als implizit.
Einfach ist besser als kompliziert.
Kompliziert ist besser als undurchschaubar.
Flach ist besser als verschachelt.
Spärlich ist besser als beschränkt.
Lesbarkeit zählt.
Spezialfälle sind nicht spezial genug, als dass sie die Regeln sprengen dürften.
Obwohl die praktische Anwendbarkeit die Reinheit übertrifft.
Fehler sollten nie schweigend verlaufen.
Außer man hat sie explizit zum Schweigen gebracht.
Im Angesicht der Mehrdeutigkeit, widersage der Versuchung zu raten.
Es sollten einen — und bevorzugt genau einen — offensichtlichen Weg geben, es zu tun.
Obwohl dieser Weg auf den ersten Blick nicht offensichtlich erscheinen mag, außer man ist Holländer.
Jetzt ist besser als nie.
Obwohl nie oft besser ist als JETZT SOFORT.
Wenn die Implementierung schwer zu erklären ist, ist es eine schlechte Idee.
Wenn die Implementierung einfach zu erklären ist, könnte es eine gute Idee sein.
Namensräume sind eine glänzende Idee — lasst uns mehr davon tun!

Obwohl die Formulierung scherzhaft ist und sich die Aufzählung als Easter Egg in der Python-Umgebung wiederfindet (`import this`), sind diese Aphorismen durchaus ernst gemeint und spiegeln sich bereits bei den einfachsten Programmen wieder. Hierfür werden in den Programmiersprachen Python, C++ und Java die Quelltexte für ein Hallo-Welt-Programm verglichen. Hierbei handelt es sich um ein Computerprogramm, dass auf einfachste Weise veranschaulicht, welche Bestandteile für ein lauffähiges Programm in einer Programmiersprache benötigt werden.

Quelltext 1: Hallo-Welt in Python

```
1 print("Hallo Welt!")
```

[1] `http://heise.de/-1948541` [Stand: 25.1.2017]
[2] `http://www.python.org/doc/essays/comparisons/` [Stand: 25.1.2017]
[3] `https://www.python.org/dev/peps/pep-0020/` [Stand: 25.1.2017]

Quelltext 2: Hallo-Welt in C++

```cpp
#include <iostream>

int main () {
  std::cout << "Hallo Welt!\n";
}
```

Quelltext 3: Hallo-Welt in Java

```java
public class HalloWelt
{
 public static void main(String[] args)
 {
  System.out.println("Hallo Welt!");
 }
}
```

Alle drei Programme würden beim Ausführen den gleichen Text an die Standardausgabe senden. Folglich würde der Text „Hallo Welt!“ auf dem Bildschirm erscheinen. Python benötigt hierfür, im Gegensatz zu den anderen Programmiersprachen, nur eine Zeile und verdeutlicht bereits damit eine Vielzahl der Leitgedanken. Das Programm ist auf das Wesentliche reduziert und enthält keine unnötigen und verwirrenden Bestandteile. Selbst ohne Programmierkenntnisse kann man verstehen, dass etwas ausgedruckt oder ausgegeben wird (`print`) und die Worte „Hallo Welt“ in irgend einem Verhältnis `()` zu `print` stehen.

Studienbrief 1 Einführung in Python

1.1 Lernergebnisse

Nach Abschluss dieses Studienbriefes sind Sie mit der Python-Shell vertraut und können mit Hilfe von Modulen aus der Standardbibliothek einfache Programme erstellen. Sie können die Begrifflichkeiten der objektorientierten Programmierung einordnen und können die wichtigsten Konzepte aufzählen. Mit dem Wissen über das Erstellen von eigenen Funktionen können Sie nicht nur auf die Funktionen von Modulen zurückgreifen, sondern darüber hinaus auch Ihr Programm besser strukturieren. Sie sind mit den Standarddatentypen in Python vertraut und können differenzieren, wann Sie welchen Datentyp verwenden sollen und wie sie eine Typumwandlung vornehmen. Zudem können Sie Skriptdateien erstellen und mithilfe von Kontrollstrukturen auch komplexere Programme erstellen. Hierbei unterstützt Sie auch das Wissen, wie ein Textmenü erstellt werden kann und Kommandozeilenparameter entgegengenommen werden. Innerhalb der Sortieralgorithmen sind Ihnen Bubblesort und Timsort bekannt, wobei Sie mit Bubblesort einen Sortieralgorithmus im Detail verstanden haben und mit Timsort einen effektiven Sortieralgorithmus kennen und zudem Aussagen zur Effizienz treffen können.

1.2 Advance Organizer

Skriptsprachen eignen sich besonders gut für schnelle Ad-hoc-Lösungen. Durch die Kenntnisse im Umgang mit Python ist es somit beispielsweise möglich, Aufgaben mit sich wiederholendem Ablauf zu automatisieren. Sie können zudem viele Programmierkonstrukte von Python auf andere Programmiersprachen übertragen, was das Verstehen und Erlernen von weiteren Programmiersprachen erheblich fördert.

1.3 Grundlagen

Das Modul ist sehr praxisorientiert und soll einen schnellen Einstieg in die Programmierung bieten. Dennoch werden in diesem Abschnitt einige Grundlagen vermittelt, die für das Verständnis des Moduls bzw. Programmieren im Allgemeinen unerlässlich sind.

1.3.1 Programmieren

Beim Programmieren geht es um das Formulieren eines Algorithmus' in einer Programmiersprache. Somit kann die Programmiersprache als Schnittstelle zwischen dem Menschen und einem Computer verstanden werden.

Definition 1.1: Algorithmus

Ein Algorithmus ist eine eindeutige, ausführbare Folge von Anweisungen endlicher Länge zur Lösung eines Problems. Ein Algorithmus besteht aus einem Deklarationsteil, der definiert was benötigt wird, und einem Anweisungsteil, der beschreibt wie das Problem gelöst wird.

D

Entscheidend für das Erlernen einer Programmiersprache ist das Denken in Strukturen und Algorithmen. Eine komplexe Aufgabenstellung muss in kleinere Teilprobleme aufgeteilt und diese wiederum durch Algorithmen gelöst werden.

Studienbrief 2 Forensische Analyse mit Python: Datenbanken und Anwendungen

2.1 Lernergebnisse

Sie können Informationen als Datensatz abbilden und diese logisch in Tabellen unterteilen. Sie sind imstande, einfache Datenbanken zu entwerfen und dabei die Regel der 1. Normalform zu beachten. Hierfür verwenden Sie das Ihnen bekannte ER-Modell nach der Chan-Notation. Da Sie mit der Datenbanksprache SQL vertraut sind, sind Sie nach kurzer Einarbeitungszeit in der Lage die Datenbank mit einer beliebigen Datenbank-Software umzusetzen. Durch diesen Studienbrief sind Sie im speziellen mit der Programmbibliothek „sqlite3“ vertraut. Mit der Untersuchung von Anwendungs-Artefakten in Python haben Sie den Aufbau der Skype-, Chrome- und Firefox-Datenbank verstanden und können hier gezielt Informationen extrahieren.

2.2 Advance Organizer

Bei der alltäglichen Arbeit am Rechner kommt man unbewusst vielfach mit Datenbanken in Berührung. Viele Anwendungen, wie Internet-Browser oder Chatprogramme, verwenden Datenbanken. Auch Webseiten, die mit einem Inhaltsverwaltungssystem (z. B. Joomla, TYPO3 oder WordPress) arbeiten, verwenden diese, um den eigentlichen Inhalt zu speichern. Diese Datenbanken können vor allem bei Anwendungen mit geringem Arbeitsaufwand ausgelesen werden und zum Beispiel nach konkreten Inhalten untersucht werden.

2.3 Datenbanksystem

Ein Datenbanksystem (DBS) ist ein System zum Speichern und Verwalten von meist großen Datenmengen. Ein DBS besteht aus einer Verwaltungssoftware, dem Datenbankmanagementsystem (DBMS) und den zu verwaltenden Daten, die als Datenbank bezeichnet werden.

Die Art und Weise, wie ein Datenbanksystem abgebildet wird, bezeichnet man als Datenbankmodell. Ein etablierter Standard ist hierbei die relationale Datenbank. Dabei handelt es sich um eine Sammlung von logisch zusammenhängenden Tabellen. Jede Zeile (Tupel) einer Tabelle ist ein Datensatz (record), wobei die Spalten die Eigenschaften (Attribute) der Tupel beschreiben.

Beispiel 2.1: Relation „Buch“

B

Ein Buch in einer Bibliothek soll durch einen Datensatz beschrieben werden. Der Datensatz besteht aus folgenden Attributen:

- Buch-ID
- Autor
- Titel
- Verlag
- Verlagsjahr

Um einen Datensatz **eindeutig** identifizieren zu können, wird ein (oder mehrere) Schlüssel (key) benötigt. Ein Schlüssel hat eine unveränderliche

Studienbrief 3 Forensische Analyse mit Python: Windows

3.1 Lernergebnisse

Sie können den Aufbau der Windows-Registry beschreiben und den Registry-Schlüssel zu gesuchten Informationen bestimmen und auswerten. Die Hauptschlüssel der Registry und deren Inhalt können Sie erläutern. Sie können die Aufgabe von SIDs, SAMs und GUIDs beschreiben und damit verbundene Informationen zuordnen. Bei einem Live System können Sie die Werte der Registry über das Python-Modul `winreg` extrahieren. Zudem ist es Ihnen möglich aus sichergestellten Hive-Dateien Informationen mit dem Modul `python-registry` zu gewinnen. Sie sind mit Python in der Lage gelöschte Dateien aus dem Papierkorb wiederherzustellen und gespeicherte WLAN-Kennwörter zu entschlüsseln. Ihr Wissen über die Windows-Forensik umfasst zudem das Parsen von Metadaten bei PDFs, Bilddateien, Word-Dokumenten und Torrent-Dateien sowie dateiformatsunabhängigen Metadaten.

3.2 Advance Organizer

Die Registry wird als „Goldgrube“ für forensisch interessante Spuren in Windows-Clients bezeichnet, weil sie von vielen Nutzeraktivitäten umfassende Spuren enthält. Dieser Studienbrief soll Ihnen als Leitfaden für die forensische Nutzung der Windows-Registry dienen und Ihnen einen Einblick in die Struktur und deren Besonderheiten verschaffen.

3.3 Windows Registry

Die Registry gibt es seit der Betriebssystemversion Windows 95. Sie ist als zentrale, hierarchisch organisierte Datenbank angelegt. Ihre binäre Form ermöglicht einen schnelle konvertierungsfreie Verarbeitung, die durch die Transaktionsüberstützung ganz oder gar nicht durchgeführt werden. Die Registry ist eine unverzichtbare Quelle für Forensiker, denn sie enthält wichtige Informationen über die Systemkonfigurationen, die Benutzerprofile und -aktivitäten, die installierten Programme und deren Ausführungen sowie über Hard- und Software-Komponenten des Rechnersystems.

3.3.1 Einführung

Die Registry bildet ein baumartiges, hierarchisch aufgebautes System, ähnlich wie Dateien und Ordner. In der Registry werden die Informationsbehälter als „Schlüssel“ (HKEY) bezeichnet. Diese sind den Dateiordnern ähnlich. Schlüssel können Unterschlüssel (KEY) haben, genau wie Ordner Unterordner haben können (vgl. Abb. 3.1). Die Daten, die in einem Schlüssel enthalten sind, werden als „Wert“ bezeichnet und sind vergleichbar zu Dateinamen. Die eigentlichen Daten können unterschiedliche Formate (z. B. Zeile, Zahl oder Zahlenfolge) haben.

selbst erst am 11. März 2015 auf dem Datenträger kopiert wurde. Seit Erstellung folgten keine Änderungen an der Datei. Das Änderungsdatum wurde von der Datei selbst übernommen.

K

Kontrollaufgabe 3.17

Gegeben sei ein Computer mit Windows 7 und zwei Datenträger. Diese sind jeweils mit dem NTFS-Dateisystem formatiert.

Welche der untenstehenden Ereignisse wirken sich auf welche Zeitstempel aus?

- Eine Datei wird von Datenträger 1 auf Datenträger 2 kopiert.
- Eine Datei wird von Datenträger 1 auf Datenträger 2 verschoben.
- Eine Textdatei mit dem Inhalt „Hallo“ wird mit dem selben Inhalt überschrieben.
- Eine ausführbare Datei wird mittels Doppelklick ausgeführt.

3.8 Zusammenfassung

Die Windows-Registry ist eine hierarchische Datenbank und dient als zentrale Instanz aller Konfigurationen. In der Registry sind zum Beispiel die physikalischen Adressen hinterlegt, mit denen sich der Rechner über WLAN verbunden hat. Als weiteres Beispiel für die Einträge in der Registry können die Windows-Benutzernamen genannt werden. Mit dem Modul `winreg` lassen sich diese Informationen auslesen.

Metadaten sind optionale Informationen, die für den Anwender nicht direkt sichtbar sind. Die Metadaten eines PDFs enthalten zum Beispiel Informationen über den Autor. Exif ist ein Standard für Metadaten von JPEG- und TIFF-Bildern. Der Umfang der Exif-Daten variiert stark und hat abhängig von der verwendeten Hardware und den Einstellungen einen hohen Informationsgehalt. So verfügen die meisten Smartphones über die Möglichkeit, bei Bildern die GPS-Koordinaten als Metadaten zu hinterlegen. Die Metadaten können über externe Module der Python-Community ausgelesen werden.

Beautiful Soup ermöglicht das Parsen von HTML- und XML-Dokumenten. In diesem Studienbrief wurde gezeigt, wie alle Bilder einer Seite mit *Beautiful Soup* herausgefiltert und heruntergeladen werden können und wie diese Bilder anschließend auf GPS-Koordinaten untersucht werden können.

3.9 Übungen

Ü

Übung 3.1

Xpdf[29] stellt unter anderem das Programm `pdftotext.exe` bereit, das eine PDF-Datei in eine Textdatei umwandeln kann. Es gibt auch Python-Module, die das Umwandeln von PDFs in Textdateien beherrschen, diese sind aber laut Entwickler um das 20-fache langsamer[30]. Erstellen Sie ein Python-Skript, das unter Verwendung von `pdftotext` eine PDF-Datei konvertiert.

Ü

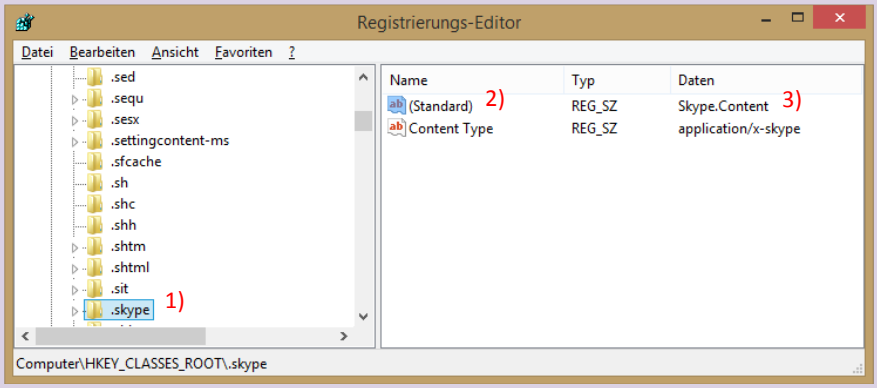
Übung 3.2

Ergänzen Sie das Skript aus Übung 3.1. Das Skript soll ein Durchsuchen der erstellten TXT-Datei nach einem bestimmten Suchbegriff ermöglichen. Versuchen Sie eine Lösung zu realisieren, die die Zeilen ausgibt, in der sich der Suchbegriff befindet. Alternativ genügt eine Meldung über die Anzahl der gefundenen Treffer. Der Name der zu konvertierenden PDF-Datei sowie der Suchbegriff sollen als Parameter an das Skript übergeben werden.

Ü

Übung 3.3: Registry

Erstellen sie ein Python-Skript, dass vollständig durch die Baumstruktur einer sichergestellten Hive-Datei (Post-Mortem-Analyse) iteriert und dabei die (Unter-)Schlüssel (1) sowie die Bezeichner (2) und die Daten (3) der Schlüsselwerte nach einem String durchsucht, der dem Skript als Argument übergeben wird.



Ü

Übung 3.4: WLAN-Schlüssel

Erstellen Sie ein Python-Skript, dass alle Dateien in den Verzeichnissen C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces\[GUID] analysiert und die SSIDs sowie Kennwörter in Klartext auf der Konsole ausgibt.

[29] `http://www.foolabs.com/xpdf/download.html` [Stand: 25.1.2017]
[30] `http://www.unixuser.org/~euske/python/pdfminer/` [Stand: 25.1.2017]

Liste der Lösungen zu den Kontrollaufgaben

Lösung zu Kontrollaufgabe 1.1 auf Seite 19

```
>>> 1 + \
... 2
3
```

Lösung zu Kontrollaufgabe 1.2 auf Seite 19

```
>>> 1+2
3
>>> 1-2
-1
>>> 1*2
2
>>> 1/2
0.5
>>> 5%2
1
>>> 5//2
2
>>> 2**3
8
>>> +1
1
>>> -1
-1
```

Lösung zu Kontrollaufgabe 1.3 auf Seite 23

```
>>> import math
>>> def kugel_volumen(radius):
        volumen = 4/3*math.pi*radius**3
        return volumen

>>> volumen = kugel_volumen(5)
>>> volumen
523.5987755982989
```

Lösung zu Kontrollaufgabe 1.4 auf Seite 24

Bei der Variable `a` handelt es sich um die Ganzzahl 1 und bei `c` um die Gleitkommazahl 1. Der Vergleichsoperator == liefert als Ergebnis `True` da die Variablen dennoch den gleich Wert haben (ähnlich wie 1 Euro entspricht 1,00 Euro). Dennoch handelt es sich bei den Variablen um unterschiedliche Objekte, da sonst die Information um welchen Datentyp es sich jeweils handelt verloren gehen würde.

Lösung zu Kontrollaufgabe 1.5 auf Seite 25

Gültige Variablennamen sind: __init__, x, bäm, var2
Ungültige Variablennamen sind: 1_variable, None

```
>>> 1_variable = 1
  File "<stdin>", line 1
    1_variable = 1
             ^
SyntaxError: invalid syntax
>>> __init__ = 2
>>> __init__
2
>>> None = 4
  File "<stdin>", line 1
SyntaxError: assignment to keyword
>>> x = 4
>>> x
4
>>> bäm = 3
>>> bäm
3
>>> var2 = 2
>>> 2
2
>>>
```

Lösung zu Kontrollaufgabe 1.6 auf Seite 27

Das vollständige Importieren eines Moduls trägt zu einem schlecht lesbaren Code bei, da nicht ersichtlich ist, welche Teile des Moduls für das Programm relevant sind. Das vollständige Importieren erleichtert vor allem im interaktiven Modus die Arbeit.

Lösung zu Kontrollaufgabe 1.7 auf Seite 28

```
>>> pi = 3.14
>>> from math import *
>>> pi
3.141592653589793
```

Lösung zu Kontrollaufgabe 1.8 auf Seite 29

```
def funktion(x = 1, y = 10):
    print(x)
    print()
```

Lösung zu Kontrollaufgabe 1.9 auf Seite 31

```
>>> funktion(x)
x hat den Wert 2
```

Lösung zu Kontrollaufgabe 1.10 auf Seite 38

```
>>> 'Hallo Welt'[2]
'l'
>>> 'hallo'+' welt'
```

```
'hallo welt'
>>> 3*'hallo'
'hallohallohallo'
>>> len('hallo')
5
```

Lösung zu Kontrollaufgabe 1.11 auf Seite 40

```
>>> (1, 2, 3)[1]
2
>>> (1, 2, 3)+(4, 5)
(1, 2, 3, 4, 5)
>>> 2*(1, 2, 3)
(1, 2, 3, 1, 2, 3)
>>> len((0, 1, 2))
3
```

Lösung zu Kontrollaufgabe 1.12 auf Seite 41

```
>>> ['Musterman','Max','Hauptstr. 6',12345,43]
['Musterman', 'Max', 'Hauptstr. 6', 12345, 43]
>>> 2*['Musterman','Max','Hauptstr. 6',12345,43]
['Musterman', 'Max', 'Hauptstr. 6', 12345, 43,
'Musterman', 'Max', 'Hauptstr. 6', 12345, 43]
>>> ['Musterman','Max','Hauptstr. 6',12345,43][2]
'Hauptstr. 6'
>>> len(['Musterman','Max','Hauptstr. 6',12345,43])
5
```

Lösung zu Kontrollaufgabe 1.13 auf Seite 41

```
>>> liste = ['a', 'b', 'b', 2, 3, 1, '1a']
>>> liste.count('a')
1
>>> liste.pop()
'1a'
>>> liste.remove(2)
>>> liste[3] = None
>>> liste
['a', 'b', 'b', None, 1]
>>> del liste[3:4]
>>> liste.reverse()
>>> liste
[1, 'b', 'b', 'a']
```

Lösung zu Kontrollaufgabe 1.14 auf Seite 42

```
>>> menge = set("cba")
>>> menge.add("d")
>>> menge
{'c', 'a', 'd', 'b'}
```

Lösung zu Kontrollaufgabe 1.15 auf Seite 42

```
>>> {"Deutsch": "deutsch", "Schweiz": "deutsch", "Spanien":"spanisch"}
{'Spanien': 'spanisch', 'Schweiz': 'deutsch', 'Deutsch': 'deutsch'}
>>> {"Apfel":"apple", "Tisch":"table"}
{'Apfel': 'apple', 'Tisch': 'table'}
>>> {"Balingen":[48.26652, 8.84941], "Albstadt":[48.26652, 8.84941]}
{'Albstadt': [48.26652, 8.84941], 'Balingen': [48.26652, 8.84941]}
```

Lösung zu Kontrollaufgabe 1.16 auf Seite 45

```
from math import pi

def quader_volumen(kanten):
    if kanten[0] == kanten [1] == kanten[2]:
        print("Hierbei handelt es sich um einen Würfel")
    v = kanten[0]*kanten[1]*kanten[2]
    return v

def kugel_volumen(radius):
    volumen = 4/3*math.pi*radius**3
    return volumen
```

Lösung zu Kontrollaufgabe 1.17 auf Seite 46

```
eingabe = input('Geben Sie eine Zahl ein: ')
zahl1 = int(eingabe)
print('Die Quadratzahl von '+eingabe+' lautet: '+str(zahl1**2))
```

Lösung zu Kontrollaufgabe 1.18 auf Seite 50

Quelltext 3.18

```
alter = int(input("Alter: "))

a16 = ["AM", "A1"]
a17 = ["B", "BE"]
a18 = ["A2", "B1", "C1", "C1E", "CE"]
a20 = ["A"]
a21 = ["C", "D1", "D1E"]
a24 = ["D", "DE"]

if alter >= 24:
    print(a16+a17+a18+a20+a21+a24)

elif alter >= 21:
    print(a16+a17+a18+a20+a21)

elif alter >=20:
    print(a16+a17+a18+a20)

elif alter >= 18:
    print(a16+a17+a18)

elif alter >=  17:
    print(a16+a17)

elif alter >= 16:
    print(a16)

else:
    print("Fahrrad")
```

Lösung zu Kontrollaufgabe 1.19 auf Seite 52

```
>>> for i in range(1600,2015,4):
if i % 100 != 0 or i % 400 == 0:
print(i)
```

Lösung zu Kontrollaufgabe 1.20 auf Seite 52

Quelltext 3.19

```
eingabe = input('Geben Sie eine Zahl ein: ')
try:
    zahl1 = int(eingabe)
except ValueError:
    print("Hierbei handelt es sich um keine Zahl")
except:
    print("Unbekannter Fehler")
```

Lösung zu Kontrollaufgabe 1.21 auf Seite 57

```
import math

kanten = [3,3,3]
radius = 3

def quader_volumen():
    if kanten[0] == kanten [1] == kanten[2]:
        print("Hierbei handelt es sich um einen Würfel")
    v = kanten[0]*kanten[1]*kanten[2]
    return v

def kugel_volumen():
    volumen = 4/3*math.pi*radius**3
    return volumen

def quit():
    print("Beende das Programm")
    raise SystemExit

def handle_menu(menu):
    while True:
        for index, item in enumerate(menu, 1):
            print("{}  {}".format(index, item[0]))
        choice = int(input("Ihre Wahl? ")) - 1
        if 0 <= choice < len(menu):
            print(menu[choice][1]())
        else:
            print("Bitte nur Zahlen im Bereich 1 - {}\
             eingeben".format(len(menu)))

menu = [["Quadervolumen", quader_volumen],
    ["Kugelvolumen", kugel_volumen],
    ["Beenden", quit]]

handle_menu(menu)
```

Eine vollständige Lösung:

```
import math

def quader_masse():
    kanten = []
    for i in range(3):
        kanten.append(int(input("Kantenlaenge eingeben: ")))
    print(quader_volumen(kanten))

def quader_volumen(kanten):
    if kanten[0] == kanten [1] == kanten[2]:
        print("Hierbei handelt es sich um einen Würfel")
    v = kanten[0]*kanten[1]*kanten[2]
    return v

def kugel_masse():
```

```
    radius = int(input("Radius eingeben: "))
    print(kugel_volumen(radius))

def kugel_volumen(radius):
    volumen = 4/3*math.pi*radius**3
    return volumen

def quit():
    print("Beende das Programm")
    raise SystemExit

def handle_menu(menu):
    while True:
        for index, item in enumerate(menu, 1):
            print("{}  {}".format(index, item[0]))
        choice = int(input("Ihre Wahl? ")) - 1
        if 0 <= choice < len(menu):
            menu[choice][1]()
        else:
            print("Bitte nur Zahlen im Bereich 1 - {}
             eingeben".format(len(menu)))

menu = [["Quadervolumen", quader_masse],
    ["Kugelvolumen", kugel_masse],
    ["Beenden", quit]]

handle_menu(menu)
```

Lösung zu Kontrollaufgabe 1.22 auf Seite 61

```
Max [a-zA-Z. ]*Mustermann;
\d{5};
\d{3}.\d{3}.\d{3}.\d{3};
[\dA-Fa-f][\dA-Fa-f]([-: ]?[[0-9]A-Fa-f]{2}){5};
([01]?[0-9]|2[0-3]):([0-5]?[0-9])
```

Lösung zu Kontrollaufgabe 1.23 auf Seite 65

Die Variante (.*?) findet möglichst wenig Text, während (.*) möglichst lange Fundstellen findet.

Lösung zu Kontrollaufgabe 1.24 auf Seite 68

```
import argparse
from math import sqrt

parser = argparse.ArgumentParser()
parser.add_argument("sqrt",
"Berechnet die Wurzel der übergebenen Zahl", type=int)
args = parser.parse_args()
print(sqrt(args.sqrt))
```

Lösung zu Kontrollaufgabe 1.25 auf Seite 71

```
print("i\n=====")
```

```
for i in range(1,10,2):
    print(i)

print("j\n=====")
j=0
while j < 100:
    j+=1

    if j%5 == 0:
        print(j)
    else:
        pass
```

Lösung zu Kontrollaufgabe 1.26 auf Seite 73

Nein.

```
>>> keyword.iskeyword("other")
False
>>> keyword.iskeyword("self")
False
```

Lösung zu Kontrollaufgabe 1.27 auf Seite 73

```
    def __ne__(self, other):
        return self.checksum != other.checksum
```

Lösung zu Kontrollaufgabe 1.28 auf Seite 75

Die Entropie liegt in der Regel mit einem Wert von größer 8 sehr hoch. Bei Bildern mit einem Wert zwischen 8 und 10 ist eine Unterscheidung nur schwer möglich. Mit der Entropie lassen sich aber problemlos Bilder mit wenigen Farben (z. B. Webseitenelemente) von Fotografien unterscheiden. Eine Staffelung der Bilder anhand der Entropie wäre sinnvoll.

Lösung zu Kontrollaufgabe 1.29 auf Seite 82

Ohne Darstellung

Lösung zu Kontrollaufgabe 1.30 auf Seite 82

Ohne Darstellung.

Lösung zu Kontrollaufgabe 1.31 auf Seite 83

```
#https://pypi.python.org/pypi/hsaudiotag3k#downloads
from hsaudiotag import auto

class Audio(File):

    def __init__(self, filename, filepath):
        File.__init__(self, filename, filepath)
        self.audio = auto.File(self.filepath+'\\'+self.filename)
        self.artist = self.audio.artist
```

```
        self.album = self.audio.album

    def getall(self):
        return
```

Lösung zu Kontrollaufgabe 1.32 auf Seite 86

```
def bubblesort(a):
    for j in range(len(a) - 1):
        swapped = False
        for i in range(len(a) - j - 1):
            if a[i] > a[i+1]:
                a[i], a[i+1] = a[i+1], a[i]
                swapped = True
        if swapped == False:
            break
    return a

a = [9,3,0,6,2,1,8,7,4,5]
print("Unsortiert: ", a)

result = bubblesort(a)
print("Sortiert  : ", result)
```

Lösung zu Kontrollaufgabe 2.1 auf Seite 96

Relation „Buch“

ID	Autor	Titel	Verlags-ID	Verlagsjahr
1	Michael Weigend	Objektorientierte Programmierung mit Python 3	1	2010
2	Johannes Ernesti & Peter Kaiser	Python 3 - Das umfassende Handbuch	2	2012
3	Ronny Ritschel	Langzeitbelichtung und Nachtfotografie	1	2012

Relation „Verlag“

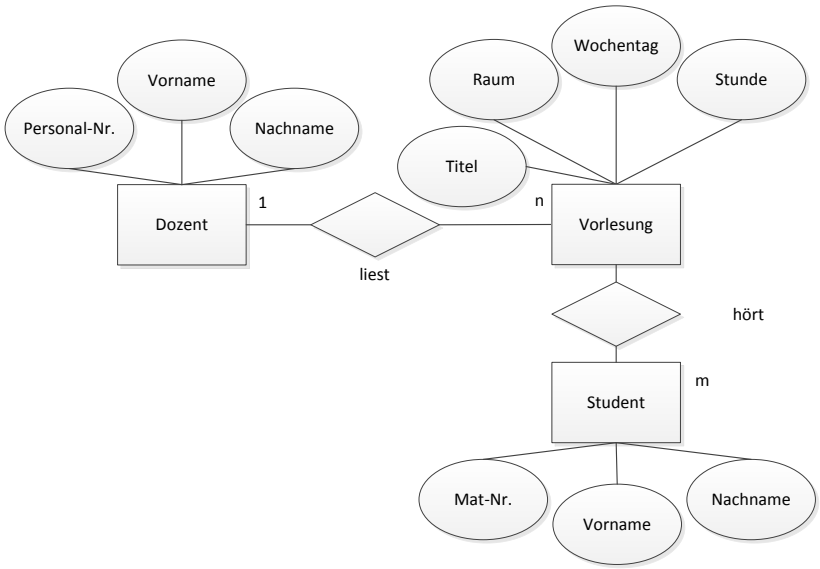
ID	Verlag
1	mitp
2	Galileo Computing

Lösung zu Kontrollaufgabe 2.2 auf Seite 97

„Kunde entleiht eBook“ kann als n:m-Beziehung realisiert werden. Wenn man Kunden unterschiedlich einstuft, wäre „Kunde ist Premium-Kunde“ eine 1:1-Beziehung.

Voraussetzung hierfür wäre natürlich, dass die Angaben für Premium-Kunden (z. B. Umfang der Leistung) in einer gesonderten Tabelle erfasst werden und nicht Teil der Tabelle „Kunde“ sind.

Lösung zu Kontrollaufgabe 2.3 auf Seite 97



Lösung zu Kontrollaufgabe 2.4 auf Seite 100

Tom O’’’Neill

Lösung zu Kontrollaufgabe 2.5 auf Seite 101

Dazu muss die `sqlite3.exe` mittels Doppelklick geöffnet werden und im Anschluss der Befehl `.open hellodatabase.db` eingegeben werden. Im Verzeichnis der `sqlite3.exe` sollte sich nun eine Datei namens `hellodatabase.db` befinden.

Zur Speicherungen von Datenbanken im Arbeitsspeicher kann der `.save`-Befehl verwendet werden.

Lösung zu Kontrollaufgabe 2.6 auf Seite 103

Erstellen der Tabelle „user“ und Erzeugung des Index:

```
sqlite> CREATE TABLE user (id integer PRIMARY KEY, surname TEXT,
lastname TEXT, yearofbirth NUMERIC);

sqlite> CREATE INDEX lastname ON user(lastname)
```

Die Spalte „id“ ist gleichzeitig der Primärschlüssel um einen Datensatz eindeutig zu identifizieren. Datentypen haben in SQLite eine eher untergeordnete Rolle, da jedes Feld prinzipiell den Inhalt jedes Datentyps annehmen kann. Dennoch ist empfohlen Datentypen für die Felder zu defineiren, da je nach Datentyp eine spezifische Speicherklasse verwendet wird. Beispielsweise wird eine Zahl in Text konvertiert, wenn diese in ein Feld vom Datentyp „TEXT“ eingefügt wird.

Zudem gibt es im Vergleich zu anderen DBMS (z.B. MySQL) auch nicht die Notwendigkeit Längenangaben für Felder zu definieren. Prinzipiell kann eine Feld jeglichen verfügbaren Speicherplatz ausnutzen.

Eine gute Hilfestellung zu den Datentypen und deren Verwendung bietet die SQLite-Referenz[31]

Als `INDEX` wurde „lastname“ gewählt. Prinzipiell sind jedoch auch noch weitere Indizes sinnvoll.

Lösung zu Kontrollaufgabe 2.7 auf Seite 103

```
sqlite> ALTER TABLE user ADD COLUMN password TEXT;
```

Lösung zu Kontrollaufgabe 2.8 auf Seite 104

```
sqlite> insert into buch (id,autor,titel,verlag,verlagsjahr) values
(1,'Michael Weigend', 'Objektorientierte Programmierung mit Python 3',
 'mitp', 2010);
sqlite> insert into buch (id,autor,titel,verlag,verlagsjahr) values(2,
'Johannes Ernesti & Peter Kaiser',
'Python 3 - Das umfassende Handbuch', 'Galileo Computing', 2012);
sqlite> insert into buch (id,autor,titel,verlag,verlagsjahr) values(3,
'Ronny Ritschel', 'Langzeitbelichtung und Nachtfotografie', 'mitp',
2012);
```

Lösung zu Kontrollaufgabe 2.9 auf Seite 104

Wie bereits erwähnt, kann über den primären Schlüssel ein Datensatz eindeutig identifiziert werden. Folglich könnte die Änderung wie folgt durchgeführt werden:
`update kunde set nachname='Schmid' where nachname='Schmidt' and id=10;`

Lösung zu Kontrollaufgabe 2.10 auf Seite 105

```
sqlite> create view asdf as select * from kunde;
sqlite> select * from asdf;
10|Otto|Schmidt
11|Tim|Tintin
```

Lösung zu Kontrollaufgabe 2.11 auf Seite 107

```
sqlite> select * from buch where titel like '%python%';
1|Michael Weigend|Objektorientierte Programmierung mit Python 3...
2|Johannes Ernesti & Peter Kaiser|Python 3 - Das umfassende Han...
```

Lösung zu Kontrollaufgabe 2.12 auf Seite 109

Lösung siehe Kapitel 2.6.

[31] `http://www.sqlite.org/datatype3.html` [Stand: 25.1.2017]

Lösung zu Kontrollaufgabe 2.13 auf Seite 111

```
import sqlite3

conn = sqlite3.connect('bib.db')
c = conn.cursor()

buecher = [(1,'Michael Weigend',
    'Objektorientierte Programmierung mit Python 3', 'mitp', 2010),
    (2,'Johannes Ernesti & Peter Kaiser',
    'Python 3 - Das umfassende Handbuch', 'Galileo Computing', 2012),
    (3,'Ronny Ritschel', 'Langzeitbelichtung und Nachtfotografie',
    'mitp', 2012)]

kunden = [(10, 'Otto', 'Schmidt'),
          (11, 'Tim', 'Tintin')]

entliehen = [(11, 1, '2014-01-31')]

print_all =
("SELECT * FROM buch","SELECT * FROM kunde","SELECT * FROM entliehen")

def insert_into(sql, tupel_liste):
    for i in range(len(tupel_liste)):
        c.execute(sql,tupel_liste[i])

try:
    c.execute('''CREATE TABLE buch (buchid integer primary key,\
        autor text, titel text, verlag text, verlagsjahr text);''')
    c.execute('''CREATE TABLE kunde(kundennr integer primary key,\
        vorname text, nachname text);''')
    c.execute('''CREATE TABLE entliehen(kundennr integer, buchid integer,\
        abgabedatum text, PRIMARY KEY(kundennr, buchid))''')
    insert_into("INSERT INTO buch VALUES (?,?,?,?,?)", buecher)
    insert_into("INSERT INTO kunde VALUES (?,?,?)", kunden)
    insert_into("INSERT INTO entliehen VALUES (?,?,?)", entliehen)


    for j in range(len(print_all)):
        c.execute(print_all[j])
        print(c.fetchall())

finally:
    conn.commit()
    conn.close()
```

Lösung zu Kontrollaufgabe 2.14 auf Seite 115

Lösungen siehe untenstehend:

```
1. SELECT skypename,fullname FROM Accounts;
2. SELECT author,body_xml FROM Messages WHERE body_xml IS NOT
NULL LIMIT 0,100;
3. SELECT IDENTITY,dispname,strftime('%d.%m.%Y %H:%M:%S',creation_timestamp,
 'unixepoch', 'localtime') as "Startzeit" FROM CallMembers;
```

Lösung zu Kontrollaufgabe 2.15 auf Seite 117

Ja, hierbei handelt es sich um einen impliziten Join.

Lösung zu Kontrollaufgabe 2.16 auf Seite 117

Aus der Skype-Datenbank werden aus der Tabelle „Transfers“ alle Datensätze ausgelesen, deren Feld Dateiname (filename) gefüllt ist. Falls ein Dateipfad (filepath) vorhanden ist, handelt es sich dabei um eine gesendete Datei. Anhand des Dateipfads kann mittels Python (z.B. `os.path.exists(file_path)`) überprüft werden, ob diese Datei auf dem Rechner existiert. Mittels der gesammelten Informationen kann in Python nun eine Liste mit den Dateinamen erstellt werden und den Attributen „sendOrReceived“ bzw. „existsOnDisk“.

Lösung zu Kontrollaufgabe 2.17 auf Seite 121

In aktuellen Firefox-Versionen befindet sich die Download-History in der SQLite-Datenbank „places.sqlite“ und der Tabelle „moz_annos“. Die wichtigsten Informationen sind in Abbildung 12 markiert.

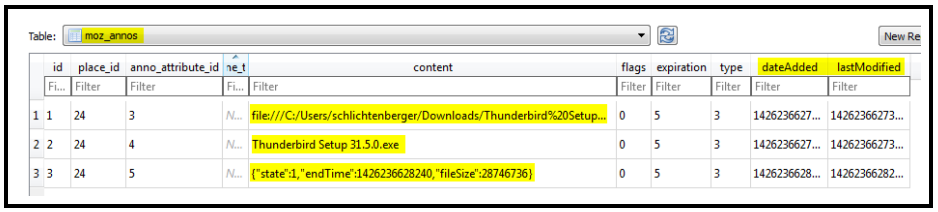


Abb. 12: Felder der Tabelle „moz_annos“

Lösung zu Kontrollaufgabe 2.18 auf Seite 121

Eine gesicherte SSL-Verbindung sichert die vollständige TCP-Datenverbindung. Die URL selbst (inkl. aller vorhandenen Parameter) werden weiterhin verschlüsselt übertragen. Sensitive Informationen sollten dennoch nicht in der URL übertragen werden, da diese i.d.R. z.B. im Klartext in den Logdateien der Betreiber gespeichert werden. Jedoch hat eine Besucher auf die Verfahrensweise keinen Einfluss, sondern lediglich der Betreiber der Webanwendung.

Fakt ist, dass der GET-Parameter im Browserverlauf (mit oder ohne SSL-Verschlüsselung) zumindest auf dem PC des Benutzers gespeichert wird.

Lösung zu Kontrollaufgabe 2.19 auf Seite 126

- `args_parser`: Definiert verfügbare Argumente und nimmt eine Ablaufsteuerung vor.
- `main`: Stellt die Verbindung zur SQLite-Datenbank her und liest die Zugangsdaten aus. Falls Zugangsdaten vorhanden sind werden diese mittels der Funktion `CryptUnprotectData` entschlüsselt.
- `csv`: Schreibt / exportiert die Zugangsdaten in eine CSV-Datei namens `chromepass.csv`.

Das Programm kann ohne Argumente aufgerufen werden. In diesem Fall wird eine Liste mit den Zugangsdaten direkt ausgegeben. Falls das Programm mit `-output` aufgerufen wird, werden die Zugangsdaten in eine CSV-Datei exportiert.

Lösung zu Kontrollaufgabe 3.1 auf Seite 134

Die Windows Registry wird in einem binären Format gespeichert. Die Registrierungsdatenbank ist seit Vista in fünf Hauptgruppen unterteilt:

HKEY_CLASSES_ROOT Informationen über unterstützte Dateitypen und zugehöriges Programm (Verweist auf HKEY_LOCAL_MACHINE\Software\Classes).

HKEY_LOCAL_MACHINE Optionen und Einstellungen aller Benutzer des Systems.

HKEY_USERS Optionen und Einstellungen, die nur auf einen einzigen Nutzer zutreffen.

HKEY_CURRENT_USER Das Profil des aktuell angemeldeten Benutzers (Verweist auf HKEY_USERS).

HKEY_CURRENT_CONFIG Verweist auf HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current.

Nachfolgend wird der Registry-Schlüssel mit den Informationen zu den WLAN-SSIDs erklärt. Da es sich hierbei um allgemeine Einstellungen handelt, befinden sich die Informationen im Hauptschlüssel HKEY_LOCAL_MACHINE. Da es sich hierbei um Einstellungen von Windows selbst handeln, befinden sich die Einträge unter SOFTWARE\Microsoft\Windows NT\CurrentVersion\. Hier gibt es den Subkey NetworkList, der wiederum die Profiles enthält. Die relevanten Werte innerhalb des Schlüssels sind die SSID (ProfileName), Beschreibung (Description), Zeitpunkt der Erstellung (DateCreated) und Zeitpunkt des letzten Verbindungsaufbaus (DateLastConnected).

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\NetworkList\Profiles\
{C87BD789-00CD-4DC5-B6DA-A4B6E8F09685}

Lösung zu Kontrollaufgabe 3.2 auf Seite 135

In dem Registry Schlüssel befinden sich folgende Subkeys:

- HKEY_USERS\.DEFAULT
- HKEY_USERS\S-1-5-18
- HKEY_USERS\S-1-5-19
- HKEY_USERS\S-1-5-20
- HKEY_USERS\S-1-5-21...
- HKEY_USERS\S-1-5-21..._Classes

Die ersten vier Subkeys (.DEFAULT, S-1-5-18, S-1-5-19, and S-1-5-20) sind integrierte Systemaccounts, die von Windows erstellt werden. Die Subkeys, beginnend mit S-1-5-21, beziehen sich auf „reale Accouns“.

Lösung zu Kontrollaufgabe 3.3 auf Seite 136

Im Schlüssel befinden sich bspw. die drei Werte „PATH=C:\Program Files (x86)\Nmap“, „TEMP=TMP=%USERPROFILE%\AppData\Local\Temp“

Lösung zu Kontrollaufgabe 3.4 auf Seite 138

In dem Registry-Schlüssel befinden sich bspw. die folgenden Werte:

```
Schlüsselname:          HKEY_LOCAL_MACHINE\HARDWARE\...
Klassenname:            <KEINE KLASSE>
Letzter Schreibzugriff: 13.02.2015 - 11:05
Wert 0
  Name:            BiosMajorRelease
  Typ:             REG_DWORD
  Daten:           0x2

Wert 1
  Name:            BiosMinorRelease
  Typ:             REG_DWORD
  Daten:           0x3d

Wert 2
  Name:            ECFirmwareMajorRelease
  Typ:             REG_DWORD
  Daten:           0x1

Wert 3
  Name:            ECFirmwareMinorRelease
  Typ:             REG_DWORD
  Daten:           0xd

Wert 4
  Name:            BaseBoardManufacturer
  Typ:             REG_SZ
  Daten:           LENOVO

Wert 5
  Name:            BaseBoardProduct
  Typ:             REG_SZ
  Daten:           24298K1

Wert 6
  Name:            BaseBoardVersion
  Typ:             REG_SZ
  Daten:           Not Defined

Wert 7
  Name:            BIOSReleaseDate
  Typ:             REG_SZ
  Daten:           05/07/2014

Wert 8
  Name:            BIOSVendor
  Typ:             REG_SZ
  Daten:           LENOVO

Wert 9
  Name:            BIOSVersion
  Typ:             REG_SZ
  Daten:           G4ETA1WW (2.61 )
```

```
Wert 10
  Name:            SystemFamily
  Typ:             REG_SZ
  Daten:           ThinkPad T530

Wert 11
  Name:            SystemManufacturer
  Typ:             REG_SZ
  Daten:           LENOVO

Wert 12
  Name:            SystemProductName
  Typ:             REG_SZ
  Daten:           24298K1

Wert 13
  Name:            SystemSKU
  Typ:             REG_SZ
  Daten:           LENOVO_MT_2429

Wert 14
  Name:            SystemVersion
  Typ:             REG_SZ
  Daten:           ThinkPad T530
```

Interessante Informationen sind u. a. der Hersteller, Versionsnummer, Erscheinungsdatum der BIOS-Version und Informationen zum Produkt selbst.

Lösung zu Kontrollaufgabe 3.5 auf Seite 141

Hive (engl.: Bienenstock) ist ein elementarer Bestandteil in der Windows-Registry. Ein Hive ist der oberste Knoten eines Hauptschlüssels. Die Hive-Files sind die dazugehörigen Binärdateien, die die Informationen der Registry enthalten.

Die folgenden Hive-Files sind in dem Verzeichnis %SystemRoot%\System32\Config\ gespeichert:

- Sam – HKEY_LOCAL_MACHINE\SAM
- Security – HKEY_LOCAL_MACHINE\SECURITY
- Software – HKEY_LOCAL_MACHINE\SOFTWARE
- System – HKEY_LOCAL_MACHINE\SYSTEM
- Default – HKEY_USERS\.DEFAULT
- Userdiff – Nicht mit einem Hive verbunden. Wird nur beim Systemupdate verwendet.

Die folgende Datei ist in jedem Benutzerverzeichnis gespeichert:
%USERPROFILE%\Ntuser.dat – HKEY_USERS\<User SID>
(verweist auf HKEY_CURRENT_USER)

Bei älteren Windows-Versionen gibt es zusätzlich folgende Datei:
%USERPROFILE%\Local Settings\Application Data\Microsoft\Windows\Usrclass.dat
(lokalisierter Pfad) – HKEY_USERS\<User SID>_Classes
(HKEY_CURRENT_USER\Software\Classes)

Unter Windows Vista und neuer wurde der Pfad geändert:
%USERPROFILE%\AppData\Local\Microsoft\Windows\Usrclass.dat (Pfad ist nicht lokalisiert) alias %LocalAppData%\Microsoft\Windows\Usrclass.dat – HKEY_USERS\<User SID>_Classes (HKEY_CURRENT_USER\Software\Classes)

Lösung zu Kontrollaufgabe 3.6 auf Seite 141

Beim Öffnen des Verzeichnisses %SystemRoot%\System32\Config unter Windows Vista und neuer erscheint ein Dialogfenster. Es werden höhere Berechtigungen für den Zugriff benötigt. Diese erhält man mit einem Klick auf „Fortsetzen“.

Das Öffnen oder Kopieren der Dateien ist nicht möglich.

Lösung zu Kontrollaufgabe 3.7 auf Seite 142

Bei einer GUID handelt sich um eine 16-Byte-Zahl (128-Bit), die aus einer Menge von Informationen gebildet wird, um Objekte eindeutig zu identifizieren. So wird unter anderem die MAC-Adresse der Netzwerkkarte bei der Erstellung einer GUID verwendet um sicherzustellen, dass die GUID weltweit eindeutig ist. Die SID ist ähnlich aufgebaut, kann aber nur einen Benutzer oder eine Gruppe innerhalb einer Domäne eindeutig identifizieren.

Lösung zu Kontrollaufgabe 3.8 auf Seite 144

```
import winreg

def main():
    explorer = 'Software\\Microsoft\\Windows\\Current'+\
        'Version\\Explorer'

    with winreg.OpenKey(winreg.HKEY_CURRENT_USER, explorer) as key:
        try:
            i = 0
            while True:
                print(winreg.EnumKey(key, i))
                i += 1
        except WindowsError:
            pass

if __name__ == "__main__":
    main()
```

Lösung zu Kontrollaufgabe 3.10 auf Seite 149

Q

Quelltext 3.20

```
1 import argparse
2 from Registry import Registry
3
4 def rec(key, depth=0):
5     for subkey in key.subkeys():
6         if subkey.name() == "skype":
7             print(subkey.path())
8         rec(subkey, depth+1)
9
10 def main():
11
12     reg = Registry.Registry("software")
13     key = reg.root()
14
15     rec(key)
16
17 if __name__ == "__main__":
18     main()
```

Lösung zu Kontrollaufgabe 3.11 auf Seite 150

```
import platform
version = platform.release()

if version == '7':
...
```

Lösung zu Kontrollaufgabe 3.12 auf Seite 152

```
#I. A. a. Violent Python
import os
from winreg import *
def sid2user(sid):
    try:
        key = OpenKey(HKEY_LOCAL_MACHINE,
        "SOFTWARE\Microsoft\Windows NT\CurrentVersion"+\
            "\ProfileList"+ '\\' + sid)
        (value, type) = QueryValueEx(key,\
            'ProfileImagePath')
        user = value.split('\\')[-1]
        return user
    except:
        return sid
def returnDir():
    dirs=['C:\\Recycler\\','C:\\Recycled\\',\
        'C:\\$Recycle.Bin\\']
    for recycleDir in dirs:
        if os.path.isdir(recycleDir):
            return recycleDir
    return None
```

```
def findRecycled(recycleDir):
    dirList = os.listdir(recycleDir)
    for sid in dirList:
        files = os.listdir(recycleDir + sid)
        user = sid2user(sid)
        with open('test.txt', 'a') as f:
            f.write('\n[*] Listing Files For User: ' +\
            str(user))
            for file in files:
                f.write('[+] Found File: ' + str(file)+
                    '\n')
def main():
    recycledDir = returnDir()
    findRecycled(recycledDir)
if __name__ == '__main__':
    main()
```

Lösung zu Kontrollaufgabe 3.15 auf Seite 160

Über den Parameter `r` können rekursiv alle Dateien bearbeitet werden. Selbstverständlich ist auch eine Lösung mittels Python möglich, aber da exiftool diesen Parameter bereits anbietet, hier die bessere Wahl.

Quelltext 3.21

```
1 import os
2
3 os.system("exiftool -r -all= C:/Bilder/*.jpg")
```

Q

Lösung zu Kontrollaufgabe 3.16 auf Seite 161

```
exiftool -ThumbnailImage= -PreviewImage= image.jpg
```

Bitte beachten Sie, dass es neben dem ThumbnailImage u.U. auch PreviewImages gibt, welche nicht Teil des Exif-Standards ist.

Lösung zu Kontrollaufgabe 3.17 auf Seite 170

- Eine Datei wird von Datenträger 1 auf Datenträger 2 kopiert:
  Änderung des Erstellungs- und Zugriffszeitstempels.
- Eine Datei wird von Datenträger 1 auf Datenträger 2 verschoben:
  Es findet keine Änderung statt.
- Eine Textdatei mit dem Inhalt „Hallo“ wird mit dem selben Inhalt überschrieben.
  Änderung des Änderungszeitstempels.
- Eine ausführbare Datei wird mittels Doppelklick ausgeführt.
  Änderung des Zugriffszeitstempels, sofern in der Registry entsprechender Wert zu Aktualisierung gesetzt. Ansonsten keine Änderung.

Verzeichnisse

I. Abbildungen

II. Beispiele

III. Definitionen

IV. Exkurse

V. Tabellen

VI. Literatur

Grant Allen and Mike Owens. *The Definitive Guide to SQLite*. Apress, New York, 2nd edition, 2010. ISBN 978-1-430-23225-4.

Johannes Ernesti and Peter Kaiser. *Python 3 - Das umfassende Handbuch*. Galileo Press, 3. Auflage, Bonn, 2012. ISBN 978-3-836-21925-9.

F. Hajji. *Das Python-Praxisbuch: Der große Profi-Leitfaden für Programmierer*. Open source library. Pearson Deutschland, 2008. ISBN 9783827325433. URL `https://books.google.de/books?id=vfzazxfQScYC`.

D. Richard Hipp. Syntax diagrams for sqlite. Website, 2015. `http://www.sqlite.org/syntaxdiagrams.html#select-stmt`.

J. Honeycutt. *Microsoft® Windows® Registry Guide*. Microsoft Press, 2009. ISBN 9780735637351.

Jay A. Kreibich. *Using SQLite*. O'Reilly Media, Inc., Sebastopol, CA, 2010. ISBN 978-0-596-52118-9.

TJ O'Connor. *Violent Python - A Cookbook for Hackers, Forensic Analysts, Penetration Testers, and Security Engineers*. Newnes, London, 1st edition, 2012. ISBN 978-1-597-49957-6.

A.S. Tanenbaum. *Moderne Betriebssysteme*. Pearson Studium - IT. Pearson Deutschland, 2009. ISBN 9783827373427.

tutorialspoint. Sqlite - SQL Database Engine. Website, 2010. `http://www.tutorialspoint.com/sqlite/sqlite_using_joins.htm`.

Michael Unterstein and Günter Matthiessen. *Relationale Datenbanken und SQL in Theorie und Praxis*. Springer DE, 5. Auflage, Berlin, 2012. ISBN 978-3-642-28986-6.

Michael Weigend. *Objektorientierte Programmierung mit Python 3 - Einstieg, Praxis, professionelle Anwendung*. Hüthig Jehle Rehm, 4. Auflage, München, 2010. ISBN 978-3-826-61750-8.

Wikipedia. Office open xml. Website, 2015a. `http://de.wikipedia.org/wiki/Office_Open_XML`.

Wikipedia. Iptc-iim-standard. Website, 2015b. `http://de.wikipedia.org/wiki/IPTC-IIM-Standard`.

Anhang

A. Schlüsselwörter

```
False      class      finally    is         return
None       continue   for        lambda     try
True       def        from       nonlocal   while
and        del        global     not        with
as         elif       if         or         yield
assert     else       import     pass
break      except     in         raise
```

Stichwörter

Open C³S
Open Competence Center for Cyber Security

Fort- und Weiterbildung

Neue Bedrohungszenarien stellen Sicherheitsexperten und IT-Verantwortliche in Unternehmen und einschlägigen Behörden vor immer größere Herausforderungen. Neue Technologien und Anwendungen erfordern zusätzliches Know-how und personelle Ressourcen.

Zur Erhöhung des Fachkräftepools und um neues Forschungswissen schnell in die Praxis zu integrieren, haben sich die im Bereich lehrenden und forschenden Verbundpartner zum Ziel gesetzt, ein hochschuloffenes transdisziplinäres Weiterbildungsprogramm im Sektor Cyber Security zu entwickeln. Auf der Grundlage kooperativer Strukturen werden wissenschaftliche Weiterbildungsmodule im Verbund zu hochschulübergreifenden Modulpaketen und abschlussorientierten Ausbildungslinien konzipiert und im laufenden Studienbetrieb empirisch getestet.

Die Initiative soll High Potentials mit und ohne formale Hochschulzugangsberechtigung über innovative Weiterbildungsangebote (vom Zertifikat bis zum Masterprogramm) zu Sicherheitsexperten aus- und fortbilden. Hierzu werden innovative sektorale Lösungen zur Optimierung der Durchlässigkeit von berulicher und hoch- schulischer Bildung entwickelt und für eine erfolgreiche Implementierung vorbereitet. Unter prominenter Beteiligung einschlägiger Verbände, der Industrie sowie Sicherheits und Ermittlungsbehörden verfolgt die Initiative das Ziel, im deutschsprachigen Raum eine Generation von Fachkräften wissenschaftlich aus- und weiterzubilden, die unser Internet schützen kann.

Open Competence Center for Cyber Security

Open C³S ist aus dem Verbundvorhabens Open Competence Center for Cyber Security entstanden. Das Gesamtziel des Programms war die Entwicklung eines hochschuloffenen transdisziplinären Programms wissenschaftlicher Weiterbildung im Sektor Cyber Security. Das Bundesministerium für Bildung und Forschung (BMBF) fördert das Großprojekt im Rahmen des Wettbewerbs „Aufstieg durch Bildung: offene Hochschulen“, der aus BMBF-Mitteln und dem Europäischen Sozialfonds finanziert wird.

Neun in Forschung und Lehre renommierte Hochschulen und Universitäten aus dem gesamten Bundesgebiet haben sich zum Ziel gesetzt, Online-Studiengänge auf dem Gebiet der Cybersicherheit zu entwickeln. Dieses Konzept soll den Studierenden ermöglichen, sich berufsbegleitend auf hohem Niveau wissenschaftliche Qualifikationen anzueignen und akademische Abschlüsse zu erlangen. Beruflich erworbene Kompetenzen können eingebracht werden. Die Bezeichnung „Open“ steht auch für die Öffnung des Zugangs zu akademischer Bildung ohne klassischen Hochschulzugang.

Mission der Initiative ist es, dringend benötigte Sicherheitsexperten aus- und fortzubilden, um mit einer sicheren IT-Infrastruktur die Informationsgesellschaft in Deutschland und darüber hinaus zu stärken.

Umsetzungsnahes Wissen ist ein wesentlicher Schlüssel um der wachsenden digitalen Bedrohung zu begegnen. Solange wir nicht in der Lage sind, Systeme hinreichend zu härten, Netzwerke sicher zu designen und Software sicher zu entwickeln, bleiben wir anfällig für kriminelle Aktivitäten. Unser Ziel ist es, die Mitarbeiter von heute zu Sicherheitsexperten und Führungskräften von morgen auszubilden und dafür zu sorgen, dass sich die Zahl und die Fertigkeiten dieser Experten nachhaltig erhöht.

Weitere Informationen zu Open C³S: https://open-c3s.de

Z202 Python 1 - Programmierung und Forensik

Ziel dieses Moduls ist es, Aufgabenstellungen aus dem Umfeld der IT-Sicherheit mit Hilfe von Python-Programmen schnell und effektiv lösen zu können. In diesem Modul lernen Sie die Programmiersprache Python anhand von praktischen Übungen kennen. Ziel dieses Moduls ist es nicht, Vorgehensmodelle zur Softwareentwicklung zu vermitteln, wie sie bei komplexer Software benötigt werden. Mit Python sollen Sie viel mehr in der Lage sein, kleinere überschaubare Programme zu schreiben, die schnell zu Ergebnissen

führen.

Python liegt in zwei Versionen vor, die beide aktiv von Programmierern verwendet werden. Die Version 3 ist mit Python 2 nicht mehr kompatibel und ist die einzige Version, die aktiv weiterentwickelt wird. In diesem Modul wird weitestgehend die aktuelle Version von Python verwendet. In einigen Abschnitten wird aber auf die Vorgängerversion zurückgegriffen, da die verwendeten Module noch nicht von den Entwicklern portiert wurden.

Neben der Programmiersprache Python wird auch das Erstellen und Verwenden von Datenbanken grundlegend erklärt. Hierfür wird das Hilfsmodul SQLite verwendet, das ein wartungsfreies Datenbanksystem enthält und Teil der Python-Umgebung ist.

Der Studienbrief 1 beschäftigt sich mit den Grundlagen der Python-Programmierung, Studienbrief 2 mit Datenbanken. Studienbrief 2 schließt mit der Untersuchung von Anwendungsartefakten an den Beispielen Skype und Firefox ab.

Der Studienbrief 3 befasst sich mit dem Thema Informationsgewinnung unter forensischen Aspekten. Die vorgestellten Beispiele sollen dabei die universellen Einsatzmöglichkeiten von Python aufzeigen und zum Experimentieren einladen.

Auf dieses Modul wird mit einem Folgemodul „Python 2 – Programmieren im IT-Security-Umfeld“ aufgebaut, bei dem der Fokus auf Penetrationstests und Netzwerkforensik liegt.

Zertifikatsprogramm

Die Zertifikatsmodule auf wissenschaftlichem Niveau und mit hohem Praxisbezug bilden ein passgenaues Angebot an Qualifikation und Spezialisierung in der nebenberuflichen Weiterbildung. Damit können einzelne Module nebenberuflich studiert werden. Durch die Vergabe von ECTS-Punkten können sie auf ein Studium angerechnet werden.

https://zertifikatsprogramm.de