Digitale Forensik

Eine Einführung

Gerhard Klostermeier

Hochschule für Technik und Wirtschaft Aalen

18. Juli 2013

Kurzbeschreibung. Diese Einführung zum Thema *Digitale Forensik* entstand im Rahmen der Vorlesung *Netzwerksicherheit* an der Hochschule für Technik und Wirtschaft in Aalen. Sie beinhaltet grundlegendes Wissen und Übungen, um einen Überblick über die Vielfalt der digitalen Forensik zu bekommen.

Inhaltsverzeichnis

1 Einleitung

Unter dem Begriff *Forensik* im klassischen Sinne, können sich viele Menschen etwas vorstellen. Durch Kriminalfilme und Romanfiguren wie Sherlock Holmes, dessen reales Vorbild, Joseph Bell, tatsächlich ein Pionier der Forensik war[1], haben die meisten ein Bild vor sich, um was es bei Forensik geht.

1.1 Definition

„Unter dem Begriff Forensik werden die wissenschaftlichen Arbeitsgebiete zusammengefasst, in denen kriminelle Handlungen systematisch identifiziert beziehungsweise ausgeschlossen sowie analysiert oder rekonstruiert werden.“[2]

1.2 Ziele

Die Ziele der Forensik sind fast unmittelbar aus der Definition ableitbar:

- Identifizieren
- Analysieren
- Rekonstruieren/Auswerten

Mit diesen Zielen vor Augen und mit einer sauberen, systematischen Arbeitsweise, welche bei Forensik eine zwingende Voraussetzung ist, können folgende Fragen beantwortet werden:

- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie ist es passiert?

Eventuell auch:

- Wer hat es getan?
- Was kann dagegen getan werden?

2 Digitale Forensik

Die digitale Forensik (auch *IT-Forensik* oder *Computer-Forensik*) ist ein Teilgebiet der Forensik. Sie beschränkt sich auf die Untersuchung von Vorfällen auf IT-Systemen.

2.1 Definition

„IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems.“[3]

2.2 Bestandteile

Die digitale Forensik unterteilt sich in einzelne Fachbereiche. Beispiele sind:

- Network Forensics
- Multimedia Forensics
- Image Forensics
- Mobile Device Forensics
- etc.

Viele der Teilgebiete unterscheiden sich stark voneinander, weswegen es viel Zeit und Arbeit braucht um alle Fachbereiche zu meistern. Dies ist auch ein Problem welches in dem folgenden Kapitel angesprochen wird.

2.3 Probleme der digitalen Forensik

Obwohl sich die digitale Forensik nicht grundlegend in der Vorgehensweise von der klassischen Forensik unterscheidet, bleiben im Detail Probleme die die klassische Forensik nicht hat.

2.3.1 Gerichtliche Verwertbarkeit

Einer der wichtigsten Unterschiede zwischen der klassischen Forensik und der Computer-Forensik ist, dass die Beweise (Artefakte, Spuren) rein virtuell sind. Sie können manipuliert werden ohne Spuren zu hinterlassen. Dies wird zum Problem wenn der Forensiker durch fahrlässiges Verhalten Beweise verfälscht oder schlimmer, bewusst gefälschte Beweise hinterlegt.

Um dieses Problem in den Griff zu bekommen gibt es mehrere Lösungsansätze die kombiniert werden sollten, um fahrlässiges oder bewusstes Fehlverhalten zu unterbinden.

- **Write Blocker**
  Ein *Write Blocker* ist ein Gerät an welches Datenträger (z.B. Festplatten) zum auslesen angeschlossen werden können, ohne dass auf diese geschrieben werden kann. Zusätzlich sollte der *Write Blocker* zertifiziert sein, damit sichergestellt ist, dass das Gerät korrekt funktioniert und nicht manipuliert ist. Es ist natürlich auch möglich durch Software das Schreiben auf Datenträger zu verhindern, nur ist hier das Ausschließen von Manipulationen und das Sicherstellen der korrekten Arbeitsweise sehr viel schwieriger.
- **Imager/Dupplicator**
  Ein *Dupplicator* ist ein Gerät, dass das exakte Kopieren von Datenträgern ermöglicht. Die Kopie gleicht in jedem Bit ihrem Original. Eine Kopie ist in der Praxis oft nötig, da nach einem zu untersuchenden Vorfall die betroffene Anlage schnell wieder in den Betrieb genommen werden soll. Diese Inbetriebnahme würde die Daten verfälschen, weswegen zur Untersuchung eine Kopie angefertigt wird.

  Auch hier gilt wie beim *Write Blocker*, dass das Gerät zertifiziert sein sollte.
- **Sicherheitsüberprüfung**
  „Das Sicherheitsüberprüfungsgesetz des Bundes regelt die Voraussetzungen und das Verfahren zur Sicherheitsüberprüfung von Personen, die mit bestimmten sicherheitsempfindlichen Tätigkeiten betraut werden sollen [...] oder bereits betraut worden sind [...]." [4]

  Das Sicherheitsüberprüfungsgesetz (SÜG) sieht drei Sicherheitsstufen vor:
  - Einfache Sicherheitsüberprüfung (Ü1)
  - Erweiterte Sicherheitsüberprüfung (Ü2)
  - Erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen (Ü3)

  Die Maßnahmen zur Sicherheitsüberprüfung steigen im Verhältnis zur Sicherheitsstufe. So wird beispielsweise für die Ü1 der Fragenkatalog der Sicherheitserklärung für die zu überprüfende Person abgearbeitet. Bei einer Ü2 wird die Überprüfung bereits auf den/die Ehegatten/in oder Lebenspartner/in ausgeweitet.

  Typischerweise stehen Sicherheitsüberprüfungen an, wenn eine Person Zugriff auf Dokumente haben möchte, die als *STRENG GEHEIM*, *GEHEIM* oder *VS-VERTRAULICH* eingestuft sind, oder in einer sicherheitskritischen Einrichtung arbeitet (lebens- oder verteidigungswichtig). [4, vgl.] [5, vgl.]
- **Zeugen**
  Allgemein ist es nicht falsch, kritische Prozesse (z.B. das Kopieren einer Festplatte) unter Aufsicht von fachkundigen Zeugen durchzuführen. Falls eine Aussage vor Gericht nötig wird, kann sich auf diese Zeugen berufen werden.

2.3.2 Vielfalt

Obwohl sich die digitale Forensik nur auf die forensische Analyse von IT-Systemen beschränkt, leidet sie doch unter dem Phänomen, dass es in diesem Umfeld sehr viele unterschiedliche Installationen gibt. So unterscheidet sich beispielsweise ein Image einer Festplatte mit Windows grundsätzlich von einem Image einer Festplatte mit Linux. Aber auch zwischen Teilgebieten (z.B. Network Forensics und Mobile Device Forensics), Versionen (z.B. Windows XP zu Windows 7), Distributionen (z.B. Ubuntu zu Arch-Linux), usw. sind die Unterschiede so groß, dass jedes Wissen um diese einzeln perfektioniert werden muss.

2.4 Werkzeuge

Auch hier hat die IT-Forensik wieder viel gemein mit der klassischen Forensik. Gute Werkzeuge sind für die Untersuchung eines Voralls in jedem Fall nötig. Bei einem Computer-Forensiker sind dies oftmals viele verschiedene Programme - aber auch Geräte wie ein *Dupplicator* dürfen nicht fehlen.

2.4.1 Hardware

In der Computer-Forensik werden selbstverständlich hauptsächlich Computer als physikalische Werkzeuge eingesetzt. Häufig handelt es sich dabei um einen Laptop mit möglichst schnellen externen Datenschnittstellen (S-ATA, USB3.0, FireWire, etc.). Aber auch Geräte wie ein *Write Blocker*, *Dupplicator* und mehrere schnelle Festplatten (SSD) hat ein IT-Forensiker bei sich, um vor Ort seine Arbeit ausführen zu können.

Abbildung 1: IT-Forensik Koffer von Dell für den mobilen Einsatz

2.4.2 Software

Software für IT-forensische Analysen gibt es viele. Die Kunst ist viel mehr das „richtige“ Werkzeug zu kennen und bedienen zu können, wobei die Wahl des „richtigen“ Werkzeugs vom Betrachtungswinkel abhängt. Wird der Vorfall den es zu analysieren gilt beispielsweise auf Dateisystemebene betrachtet, so sind Programme die aus Dateisystemen die Metainformationen extrahieren (z.B. ein NTFS INDX Slack Parser) eine sinnvolle Wahl, während Software zur Netzwerkanalyse für diese Aufgabe nicht von Nutzen ist.
Typische Betrachtungswinkel für Computer-Forensik Probleme sind:

- Betriebssystemebene
- Dateisystemebene
- Dateiebene
- Netzwerkebene
- etc.

Es gibt einige große IT-Forensik Suits die mit vielen Tools ausgestattet sind und kommerziell vertrieben werden. Aber auch die *Open Source*-Szene bietet eine Vielzahl an Programmen, mit denen computerforensische Untersuchungen durchgeführt werden können.

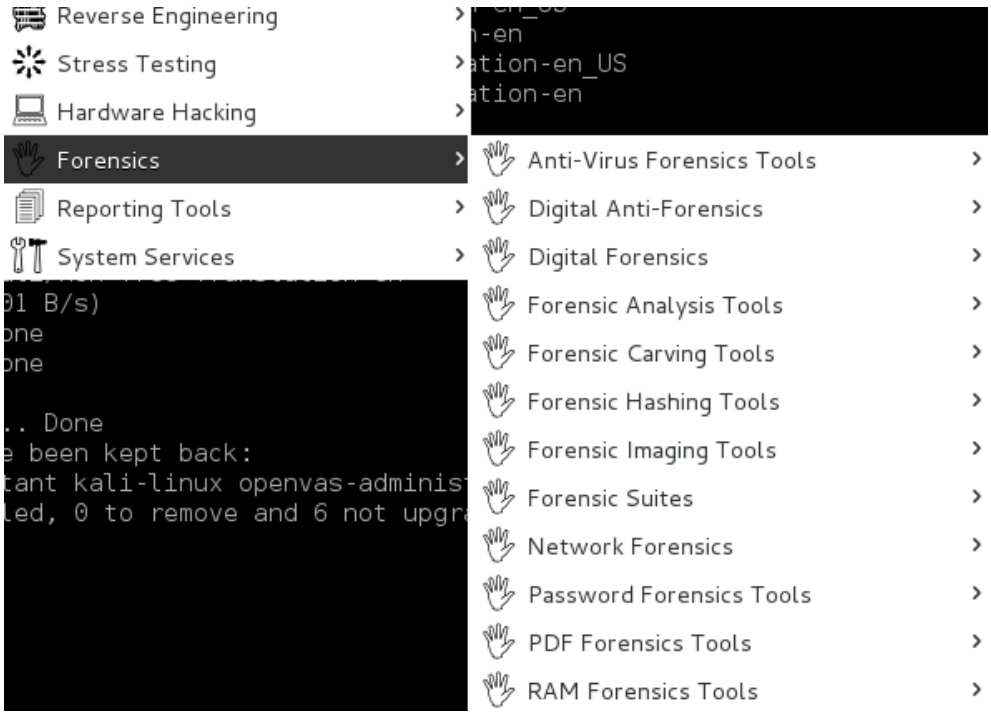

Abbildung 2: Übersicht über die Sammlung von kostenlosen Forensik-Tools die in Kali-Linux[1] enthalten sind

[1] Webpräsenz von Kali-Linux: http://www.kali.org/

3 Übungen

Diese Übungen (in der IT-Forensik oftmals auch *Challenge* genannt) sollen einen einfachen, praktischen Einstig in Thematik ermöglichen. Falls danach das Interesse geweckt worden ist, können unter folgenden Links weiter Herausforderungen gefunden werden:

- http://www.honeynet.org/challenges
- http://www.forensicfocus.com/images-and-challenges

3.1 Exif-Datenanalyse

In dieser Übung werden die Exif-Daten von Dateien (PDFs und Bilder) analysiert. Dazu wird das in Perl geschriebene *ExifTool* von Phil Harvey eingesetzt. Das Programm kann auf einem Ubuntu-Linux einfach aus den Quellen installiert werden.

```
> sudo apt-get install libimage-exiftool-perl
```

Alternativ kann die neuste Version direkt von der Webseite heruntergeladen werden: http://www.sno.phy.queensu.ca/~phil/exiftool/

Das Programm kann wie folgt verwendet werden.

```
> exiftool Dateiname
```

3.1.1 Aufgabenstellung

In dem beigelegten Ordner „Übung-1“ sind mehrere Dateien zu finden die mit dem ExifTool analysiert werden sollen. Dabei geht es nicht darum einen Fragenkatalog präzise abzuarbeiten, sondern vielmehr darum sich mit Exif-Daten vertraut zu machen, Querbezüge herzustellen und Inkonsistenzen zu erkennen.

Alle Dateien stammen von der Homepage der Hochschule Aalen.

3.1.2 Auflösung

In dieser Auflösung werden ein paar Auffälligkeiten an den Dateien genannt. Die Erkenntnisse haben kein Anspruch auf Vollständigkeit.

- **4952_Sammelbogen_Studium_Generale_CC.pdf**
  Autor: mjooss. Nach einer kurzen Internetrecherche kann festgestellt werden, dass es sich um Margit Jooß, eine Mitarbeiterin des Sekretariats an der Hochschule Aaalen, handelt.
  Umgebung: Das Dokument wurde auf einem Windows-PC mit Microsoft Excel verarbeitet und durch den Acrobat PDFMaker 8.1 als PDF exportiert.
  Sonstiges: Das Dokument wird mit dem Google Documents Cloud-Dienst abgeglichen. Dass das nötige Plugin für Microsoft Office installiert ist, ist der *Google Documents Plugin Version* und der *Google Documents Document Id* Exif-Information zu entnehmen.
- **ABCD_Flyer_2012.pdf**
  Autor: Patricia Müller. Auch hier kann über eine Internetrecherche festgestellt werden, dass es sich um eine Mitarbeiterin an der Hochschule Aalen handelt.
  Umgebung: Das Dokument wurde auf einem Windows-PC mit Microsoft Powerpoint unter Verwendung einer Postervorlage erstellt und durch den Acrobat PDFMaker 7.0.5 als PDF exportiert.
  Sonstiges: Obwohl die Autorin Mitarbeiterin der Hochschule Aalen ist, hat das Dokument „Pandora“ und nicht „HTW-Aalen“ als Firmennamen vermerkt.
- **Anleitung_Bericht_14032012.pdf**
  Autor: Volker Knoblauch. Wie bei den vorigen Dateien auch, handelt es sich um einen Mitarbeiter der Hochschule Aalen.
  Umgebung: Das Dokument wurde auf einem Windows-PC mit Microsoft Word 2010 unter Verwendung einer Briefvorlage erstellt und exportiert.
  Sonstiges: Das Dokument hat eine Inkonsistenz in der Datumsangabe. In dem PDF ist der 14.03.2012 als Datum angegeben. Die Exif-Daten besagen jedoch, dass der Brief am 16.07.2012 erstellt wurde. (Dies ist typisch wenn im Nachhinein etwas korrigiert wurde.)
- **gallery_130426_TagUndNacht__1271_.JPG**
  Autor: Unbekannt.
  Umgebung: Geschossen mit einer „Canon EOS 600D“ Kamera (ohne Blitz, Firmware Version: 1.0.2, Objektiv: EF-S18-135mm f/3.5-5.6 IS STM, etc.)
  Sonstiges: Das Bild besitzt keine geographischen Informationen. Mache Kameras die mit einem GPS-Empfänger ausgestattet sind und typischerweise Smartphones, fügen den geschossenen Bildern die aktuellen GPS-Koordinaten als Exif-Daten an. So kann festgestellt werden, wo das Bild aufgenommen wurde.

3.2 Windows Forensik

In dieser Übung soll ein Windows XP Image untersucht werden. Dazu kommen mehrere frei erhältliche Programme zum Einsatz.

Die folgenden Installationshinweise beziehen sich auf ein Ubuntu-Linux in der Version 12.10.

- **xmount**
  Da das zu untersuchende Image in dem Format „.E01“ vorliegt, muss es mit xmount erst eingebunden werden, um ein „mountbares dd Image“ zu erhalten.
  Installation:

```
> sudo apt-get install xmount
```

  Nutzung:
  Zunächst müssen zwei Mountpoints (Ordner) erstellt werden.

```
> mkdir mp1 mp2
```

  Nun kann das E01-Image eingebunden werden.

```
> sudo xmount --in ewf path/to/image.E01 path/to/mp1
```

  Im `mp1` Verzeichnis ist jetzt das Image im gängigen „dd“-Format. Um dieses mit `mount` Einbinden zu können, muss erst der Offset berechnet werden.

```
> sudo fdisk -l path/to/mp1/WinXP.dd
```

  Berechnung: $Start \cdot UnitSize = Offset$
  Für das in der Übung genutzte Image: $63 \cdot 512 = 32256$
  Daraus ergibt sich dann folgender `mount`-Befehl:

```
> sudo mount -t ntfs -o loop,ro,noexec,offset=32256 \
  path/to/mp1/WinXP.dd path/to/mp2
```

  Durch die `mount`-Optionen „ro“ und „noexec“ kann die Windowsfestplatte sorglos untersucht werden, da Schreibzugriffe und das Ausführen von Programmen nicht möglich sind.

- **RegRipper**
  Dieses Programm parst einen Teil (*Hive File*) der Windows-Registry und gibt die Daten in einer aufbereiteten Textform aus.
  Installation:
  RegRipper ist ein Windows-Programm. Deswegen wird zur Ausführung unter Linux `wine` benötigt.

```
> sudo apt-get install wine
```

  Das Programm selbst und die zwingend benötigten Plugins werden direkt von der Webseite des Herausgebers heruntergeladen.

http://regripper.wordpress.com/
Die Plugins müssen im Unterverzeichnis „plugins“ im selben Ordner liegen in dem auch das Programm „rr.exe“ liegt.
Nutzung:

```
> cd path/to/RegRipper
> wine rr.exe
```

In der nun erscheinenden Windows-Oberfläche muss zunächst ein *Hive File* gewählt werden. Ein typisches Beispiel mit vielen wichtigen Informationen ist „NTUSER.DAT“. Diese Datei befindet sich unter `path/to/mp2/Documents\ and\ Setting /Username/NTUSER.DAT`. Weitere nützliche *Hive Files* können dem beigelegtem *SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf* [6] entnommen werden. In dem Feld *Report File* wird lediglich ein frei wählbarer Pfad zu einer (nicht existenten) Text-Datei angegeben, in der die Programmausgabe gespeichert werden soll. Das Profil sollte anhand des gewählten *Hive Files* eingestellt werden. Wenn also die „NTUSER.DAT“ untersucht wird, sollte das Profil „ntuser“ zum Einsatz kommen.

- **log2timeline**
  `log2timeline` ist ein Programm, welches möglichst viele Ereignisse aus verschiedenen Quellen auf einen Zeitstrahl abbildet. Quellen sind beispielsweise Apache Logs, Browser History, PCAP Dateien, Windows 2k/XP Event Log, PDF Metadaten, Papierkorb, etc. Die Programmausgabe kann in verschiedenen Formaten erfolgen. Für diese Übung reicht jedoch CSV (*Comma-separated values*) welches mit *LibreOffice Calc* betrachtet und verarbeitet werden kann.
  Installation:
  Das Programm kann von der Google Code Projektseite heruntergeladen werden.
  https://code.google.com/p/log2timeline/downloads/list
  `log2timeline` hat mehrere Abhängigkeiten (Perl-Module) die ebenfalls installiert werden müssen. Um zu sehen welche auf dem Zielsystem fehlen kann wie folgt vorgegangen werden.

```
> cd path/to/log2timeline
> perl Makefile.PL
```

Die noch fehlenden Abhängigkeiten können über passende Pakete aus den Quellen der Linux-Distribution geladen werden (`apt-get`), oder direkt mit dem perl-internen *Packet Manager* installiert werden.

```
> sudo perl -MCPAN -e 'install Date::Manip, \
  DateTime::Format::Strptime, ...'
```

Wenn alle Abhängigkeiten erfüllt sind, kann `log2timeline` installiert werden.

```
> perl Makefile.PL
> make
> sudo make install
```

Nutzung:

```
> log2timeline -p -r -f winxp -z timezone path/to/mp2 -w timeline.csv
```

Wie die korrekte Zeitzone (*timezone*) des Zielsystems ermittelt wird, kann dem SANS Poster[6] entnommen werden.

Um die Ausgabe von `log2timeline` etwas zu optimieren, kann das Skript `l2t_process_old` verwendet werden. Es sortiert die CSV-Datei und entfernt Doppeleinträge.

```
> l2t_process_old -b timeline.csv > clean-timeline.csv
```

Die CSV-Datei kann mit `libreoffice` betrachtet werden. Sinnvolle Einstellungen um die Ansicht zu verbessern, können über das Menü getätigt werden.
Data → *Filter* → *Autofilter* → *OK*
Data → *Sort* → *Sort key 1 = date, Sort key 2 = time* → *OK*

- **wisp**
  `wisp` ist ein Windows INDX Slack Parser. Mit ihm können NTFS-Metadaten eingesehen werden. Für die Computer-Forensik besonders interessant sind die als gelöscht markierten Dateien.
  Installation:
  Das Programm kann für die gängigen Betriebssysteme wie Windows, Mac und Linux auf der Herstellerseite in 32Bit oder 64Bit heruntergeladen werden.
  https://tzworks.net/prototype_page.php?proto_id=21
  `wisp` bedarf keiner Installation und kann direkt verwendet werden.
  Nutzung:

```
> cd path/to/wisp
> ./wisp32 -image path/to/mp1/WinXP.dd -offset 0x7e00 \
  -path "path\to\some\windows\folder" -level 5 -all -csv > out.cvs
```

  Die Ausgabedatei kann wieder mit `libreoffice` betrachtet werden.

3.2.1 Aufgabenstellung

In dem beigelegtem Ordner „Übung-2“ ist ein Link zum Download eines Windows-Images enthalten. Nach Erhalt des Images soll dieses mit den im vorigen Kapitel vorgestellten Werkzeugen untersucht werden.

Szenario
Der Angestellte Castor Troy verlässt unerwartet die Software Firma für die er arbeitete. Mitarbeiter berichten, dass er am letzten Arbeitstag sehr früh kam und sich seltsam verhalten habe. Castor Troy hatte Zugriff auf kritische Unternehmensdaten, weswegen nach seinem plötzlichen Gehen sein Computer kurz untersucht wurde. Dabei wurden verdächtige .zip-Dateien gefunden.

Sie haben nun den Auftrag herauszufinden, was es damit auf sich hat. Wurden Daten gestohlen? Wenn ja, wie? Was können Sie noch (heraus)finden?

3.2.2 Auflösung

Im folgenden werden Erkenntinisse vorgestellt die nahe legen, dass der ehemalige Mitarbeiter, Castor Troy, Daten gestohlen hat. Die Erkenntnisse haben kein Anspruch auf Vollständigkeit.

- **Zeitzone:** PST8PDT.
- **30.01.2008 - 06:08:** Winzip wurde installiert (und ein Systemwiederherstellungspunkt erstellt).
- **30.01.2008 - 06:18:** Mehrere „secret$X$.zip"-Dateien wurden erstellt.
- **30.01.2008 - 06:26 und später:** Geheime („secret$X$.zip") Dateien wurden von „My Documents" nach Laufwerk „E:" kopiert. Dieses Laufwerk ist laut *System Hive File* ein USB-Stick.
- **30.01.2008 - 06:28:** „secret5.zip" wurde geöffnet.
- ... Und vieles mehr!

Um die Spuren zu verwischen wurden die .zip-Dateien gelöscht. Auch der „Recent"-Ordner der unter Windows Verknüpfungen zu zuletzt verwendeten Dateien enthält, wurde geleert. Wenn jedoch das Programm `wisp` auf diesen Ordner ansetzt wird, kann festgestellt werden, dass sich in dem Ordner vor kurzem noch die Dateien „secret2.ink" und „secret5.ink" befunden haben.

All diese Funde und die Tatsache dass versucht wurde die Spuren zu verwischen deuten darauf hin, dass Castor Troy Daten des Unternehmens gestohlen hat.

Das Windows-Image birgt noch weitere Spuren (z.B. Hinweise auf „supersecret" unter `Software\Microsoft\Windows\CurrentVersion\Explorer\Streams\0\ViewView2` des „NTUSER.DAT" *Hive Files*). Manche davon können mit den vorgestellten Werkzeugen gefunden werden, andere benötigen Techniken die über diese Einstiegsübung hinausgehen.

Quellen

[1] Wikipedia.de. (2013). Joseph Bell, Adresse: https://de.wikipedia.org/w/index.php?title=Joseph_Bell&oldid=118074802.

[2] ——, (2013). Forensik, Adresse: https://de.wikipedia.org/w/index.php?title=Forensik&oldid=117655935.

[3] Bundesamt für Sicherheit in der Informationstechnik. (2011). Leitfaden it-forensik, Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Leitfaden_IT-Forensik_pdf.pdf?__blob=publicationFile.

[4] Wikipedia.de. (2013). Sicherheitsüberprüfungsgesetz, Adresse: https://de.wikipedia.org/w/index.php?title=Sicherheits%C3%BCberpr%C3%BCfungsgesetz&oldid=116228436.

[5] Bundesministerium der Justiz. (2013). Gesetz über die voraussetzungen und das verfahren von sicherheitsüberprüfungen des bundes, Adresse: http://www.gesetze-im-internet.de/s_g/index.html.

[6] SANS. (2012). Digital forensics and incident response poster, Adresse: http://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf.