**Technische Berichte in Digitaler Forensik**

**Herausgegeben vom Lehrstuhl für Informatik 1 der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) in Kooperation mit dem Masterstudiengang Digitale Forensik (Hochschule Albstadt-Sigmaringen, FAU, Goethe-Universität Frankfurt am Main)**

# Forensische Analyse persistenter Spuren des Bildbearbeitungsprogramms PhotoScape

Michael Terörde

09.05.2018

Technischer Bericht Nr. 15

## Zusammenfassung

Das Bildbearbeitungsprogramm PhotoScape ist ein beliebtes kostenfreies Werkzeug für Manipulationen von Fotos. Damit können auch böswillige Manipulationen durchgeführt werden indem Informationen in Fotos entfernt, verändert oder eingefügt werden. Die entstehenden Fälschungen können zum Beispiel zum Versicherungsbetrug oder zur Wahlbeeinflussung genutzt werden. Dieser technische Bericht untersucht erstmals das Programm PhotoScape nach einer forensischen Spurenmenge. Die gefundenen Spuren können eine Verwendung von PhotoScape sowie frühere Installationen die wieder deinstalliert wurden, nachweisen.

Dieses Paper ist im Rahmen des Moduls Browser- und Anwendungsforensik des Studiengangs Digitale Forensik unter der Anleitung von Holger Morgenstern entstanden.

# Inhaltsverzeichnis

# 1 Aufgabe

## 1.1 Aufgabenstellung

Dieser Bericht beschreibt die forensische Anwendungsanalyse der Software PhotoScape in der Version 3.7. Dabei wird die Anwendung auf ihre Spurenmenge untersucht und eine detaillierte Dokumentation der Spuren erstellt. Es sollen konkret die Fragen beantwortet werden, wo man die Spuren finden und wie man diese auslesen kann. Die Anwendung wird auf einem Windows 7 Betriebssystem installiert und betrieben. Die Analyse der Spurenmenge kann in realen forensischen Untersuchungen helfen die persistenten Spuren von PhotoScape zu identifizieren und zu interpretieren.

Eine frühere forensische Analyse von PhotoScape ist dem Autor auch nach ausgiebiger Recherche nicht bekannt. Diese Arbeit soll die folgenden zentralen Fragen beantworten:

1. Welche Spuren in Bildern deuten auf eine Verwendung von PhotoScape hin?
2. Welche Informationen über Modifikationen an Bildern lassen sich aus den Bildern herauslesen?
3. Ist oder war das Programm installiert?

## 1.2 Beschreibung der Anwendung und der forensischen Relevanz

Das Programm PhotoScape ist ein kostenloses und frei verfügbares Bildverarbeitungs-programm[1] (siehe **Bild 1.1**). Mit dem Programm können Bilder betrachtet und manipuliert werden. Dazu gehören typische Modifikationen wie zuschneiden, aufhellen, abdunkeln, schärfen und weichzeichnen. Das Programm gilt als einsteigerfreundlich und als Alternative zum kostenpflichtigen Photoshop. Es ist für alle gängigen Windows-Versionen sowie für Mac OS X erhältlich. Das Programm finanziert sich über Werbung und Adware.

Die forensische Relevanz ergibt sich aus der Tatsache, dass dieses Programm für böswillige Manipulationen an Bildern genutzt werden kann. So können Informationen in Fotos entfernt, verändert oder eingefügt werden. Bekannte Beispiele solcher Manipulationen ist der iranische

[1] Weitere Informationen zum Programm: http://help.photoscape.org/help.php?id=intro

Raketentest im Jahr 2008, bei dem eine zusätzliche Rakete[2] eingefügt wurde, und die Bildmanipulation des Sportlers Martin Szwed aus dem Jahr 2015, die ihn angeblich beim Südpol zeigen soll[3]. Weiterhin können z.B. Fotos von Rechnungen für Versicherungsbetrug manipuliert werden.

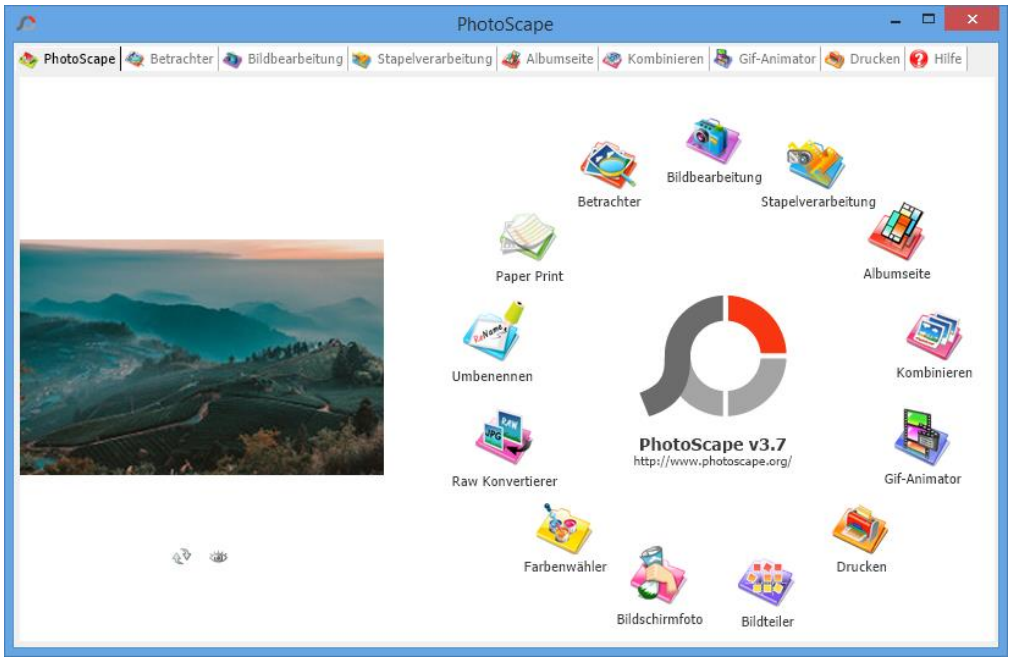



**Bild 1.1** Start-Benutzeroberfläche von PhotoScape

2 Quelle: http://www.spiegel.de/wissenschaft/mensch/bildmanipulationen-forscher-a-1158472.html, abgerufen am 21.12.2017

3 Quelle: http://www.spiegel.de/reise/aktuell/zweifel-an-suedpol-rekord-szwed-raeumt-fotomanipulation-ein-a-1020695.html, abgerufen am 21.12.2017

# 2 Untersuchungsmethoden

Für die Analyse von PhotoScape werden die Zustandsmethode und die Ereignismethode verwendet. Zusätzlich werden Fotos mit forensischen Bilduntersuchungs-Programmen untersucht. Alle Untersuchungen wurden auf einem HP Envy Laptop unter zu Hilfenahme von Virtualbox durchgeführt.

## 2.1 Arbeitsumgebung

### 2.1.1 Verwendete Hardware

Die Anwendungs-Analyse von PhotoScape wurde mit folgendem PC-System durchgeführt:

- Notebook HP Envy 17 mit dem 64-Bit Betriebssystem Windows 8.1, 2,40 GHz Intel Core i7-4700MQ, 4 Kerne und 12 GB Arbeitsspeicher

Vor Beginn der Arbeit wurde mittels dem Anti-Viren-Programm *Symantec Endpoint Protection* sichergestellt, dass die Systeme virenfrei sind.

### 2.1.2 Verwendete Software

Auf dem Notebook (Host) wurde mittels Oracle Virtualbox eine Virtuelle Maschine mit dem Betriebssystem Windows 7 32-Bit (Gastsystem) errichtet. Diese virtuelle Maschine wird genutzt um zu untersuchen, welche persistenten Spuren PhotoScape erzeugt. Diese virtuelle Maschine hat keinen Zugang zum Internet, damit Updates während der Analyse die Spurenmenge nicht verfälschen. Der Datenaustausch zwischen dem Host und dem Gastsystem erfolgt über einen gemeinsamen Ordner. Über diesen gemeinsamen Ordner wurden dem Gastsystem zu manipulierende Fotos und die Installationsdatei von PhotoScape und die Ausführungsdatei von RegShot zur Verfügung gestellt. Der Process Monitor (ProcMon) von Sysinternals in der Version 3.10 wird zur Aufzeichnung von Events des Betriebssystems eingesetzt und ist bereits auf der virtuellen Maschine enthalten[4]. ProcMon nutzt die Hookingtechnik zur Ermittlung der Events[5].

[4] Die virtuelle Maschine stammt aus dem Modul M105 Grundlagen der Digitalen Forensik

[5] Simon Jansen: Analyse der Spurenmenge der Anwendung OpenVPN Client Version 2.3.9 in Microsoft Windows. Technischer Bericht Nr. 1 vom 15.2.2016.

Eine weitere virtuelle Maschine mit dem Betriebssystem Ubuntu 14.04 LTS 32-Bit wird für den Vergleich von zwei Datenträgerabbildern mittels des Python-Programms idifference2.py verwendet. Alle weiteren verwendeten Programme sind in **Tabelle 1** zusammengefasst.

**Tabelle 1 Verwendete Programme und deren Einsatzzweck**

| **Software** | **Verwendet für** |
|---|---|
| Oracle Virtualbox Version 5.1.14 | Virtuelle Maschinen mit Windows 7 und Ubuntu 10.04 LTS |
| Process Monitor Version 3.10 | Spurenakquise mittels Ereignismethode |
| PowerGui Script Editor v3.8.0.129 | Für PowerShell-Skript zur Erstellung von Snapshots |
| Idifference2.py | Vergleich zweier Datenträgerabbilder (Zustandsmethode) |
| JPGsnoop v1.7.3 | Zur Auswertung der Meta-Daten von JPGs |
| EXIFtool v5.16.0.0 | Zur Auswertung der Meta-Daten von JPGs |
| PhotoScape v.3.7 | Das zu analysierende Bildbearbeitungs-Programm |
| WinPrefetchView v1.35[6] | Zur Analyse der Prefetch-Dateien |
| RegShot 1.9.0 x64 | Zur Analyse der Registry-Änderungen |
| Registrierungs-Editor (Regedit) v6.1 | Zur Untersuchung der Registry |

## 2.2 Ablauf der forensischen Untersuchungen

Das Vorgehen bei der Analyse der Anwendung PhotoScape ist an der Abfolge einer typischen Verwendung von PhotoScape orientiert. Dazu wird der Ablauf in drei Phasen unterteilt, wie in **Tabelle 2** beschrieben.

**Tabelle 2 Übersicht der zu untersuchenden Phasen**

| **Lfd. Nr.** | **Aktion/Phase** | **Beschreibung** |
|---|---|---|
| 1 | Installation von PhotoScape | Installation von PhotoScape mittels des Installationsprogramms photoscape-3-7-multi-win.exe. Es werden die Standardeinstellungen verwendet, außer die Installation von Google Chrome als Standardbrowser. |
| 2 | Bildmanipulationen | Starten des Programms durch Doppelklick auf das Desktop-Symbol von PhotoScape. Einlesen eines Bildes. Durchführung der Bildmanipulationen, Speichern der Änderungen und beenden von PhotoScape |
| 3 | Deinstallation von PhotoScape | Deinstallation von PhotoScape mittels der Windows-Funktion *Programme deinstallieren* in der Systemsteuerung |

6 Quelle: http://www.nirsoft.net/utils/win_prefetch_view.html

Vor jeder der vorgestellten Phasen wird ein Snapshot zur Sicherung des Status der virtuellen Maschine erstellt. So kann später zu den einzelnen Phasen zurückgekehrt werden. Jede Phase wird mehrfach untersucht: einmal mit Procmon, mit idifference2 und mit RegShot. Bei einer Analyse mit Procmon und Verwendung des zugehörigen Snapshots für eine Analyse mittels idifference2.py wären irrelevante Spuren, die durch Procmon verursacht worden wären, in der Auswertung enthalten. Damit sich die Akquisemethoden nicht gegenseitig beeinflussen, aber dennoch derselbe Ausgangspunkt genutzt wird, wird der Snapshot jeweils auf die entsprechende Phase zurückgesetzt. Der Ablauf der Spurenakquise am Beispiel der Phase PhotoScape-*Installation* ist somit:

1. VM Win 7 starten
2. Snapshot $S_0$ erzeugen
    a. ProcMon starten
    b. Photoscape installieren
    c. ProcMon-Report abspeichern
3. Snapshot $S_0$ wiederherstellen
    a. Registry-Abbild 1 mittels RegShot
    b. Photoscape installieren
    c. Registry-Abbild 2 mittels RegShot
4. Snapshot $S_0$ wiederherstellen
    a. Photoscape installieren
    b. Snapshot $S_1$ als Ausgangspunkt für nächste Phase generieren
5. Idifference2 auf $S_0$ und $S_1$ anwenden

Damit typische betriebssystembedingte Änderungen aus der Spurenmenge entfernt werden, wird ein weiteres Abbild $S_2$ erzeugt, bei dem keine Aktion ausgeführt wird. Dadurch erhält man nur „Spuren“, die vom Betriebssystem selbst erzeugt wurden. Solch ein Leerlauf-Abbild wird für die Registry- und die idifference2-Analyse erstellt.

Zusätzlich zur Anwendung der Zustandsmethode und Ereignismethode für die definierten Phasen, werden die Prefetch-Dateien explizit betrachtet, sowie Modifikationen der Metadaten in bearbeiteten jpg-Bildern untersucht.

## 2.3 Zustandsmethode

Das Programm wird auf einer virtuellen Maschine mit Windows 7 verwendet. Vor und nach den zu untersuchenden Aktionen wird ein Snapshot der VM erstellt. Beide Snapshots werden

auf Unterschiede untersucht durch das Programm idifference2.py aus dem Projekt DFXML, welches auf der Ubuntu-VM verfügbar ist. Neben idifference2 wird auch RegShot als Zustandsmethode verwendet, um Veränderungen in der Registry zu erkennen.

## 2.4 Ereignismethode

Mittels des Programmes Procmon aus der Sysinternals-Suite wird das Programm untersucht. Da bei jeder PhotoScape-Aktion eine Vielzahl von Events auftreten, wird die Analyse auf relevante Spuren begrenzt, wie das Erstellen, Schreiben und Lesen von Dateien, um die persistente Spurenmenge zu erhalten. Dazu wird ein entsprechender Filter in Procmon gesetzt:

*Process Name begins with photoscape* (siehe **Bild 2.1**)

Procmon wird vor der jeweiligen Phase mit dem Filter aktiviert und am Ende der Phase wird die Event-Aufzeichnung gestoppt. Die Ergebnisse werden in Form einer CSV-Datei gespeichert.

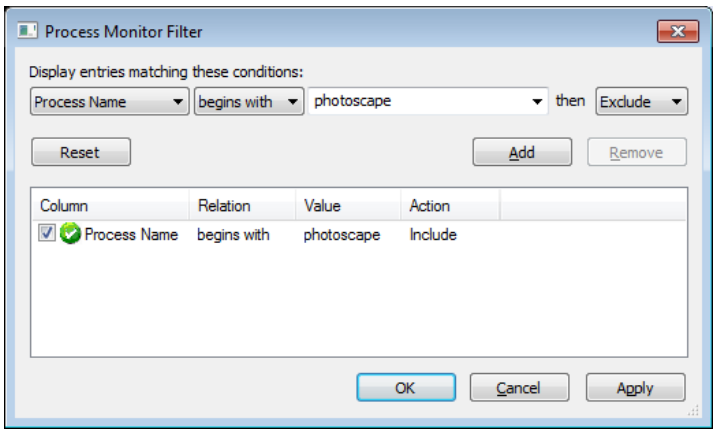



**Bild 2.1** Filtereinstellungen beim Process Monitor

## 2.5 Klassifizierung von Spuren

Digitale Spuren können entsprechend ihrer Flüchtigkeit in persistente, semi-persistente und flüchtige Spuren im engeren Sinne eingeteilt werden[7]. Flüchtige Spuren im engeren Sinne sind trotz Stromzufuhr nur temporär vorhanden, wie z.B. Netzwerkdaten oder Prozessorregister-

[7] Dewald, A.: Formalisierung digitaler Spuren und ihre Einbettung in die Forensische Informatik, Dissertation, Universität Erlangen-Nürnberg, 2012

inhalte. Semi-persistente Spuren sind nur bei ständiger Stromzufuhr permanent vorhanden, wie z.B. Daten im Hauptspeicher. Dieses Gutachten untersucht nur persistente Spuren, also Spuren die auch ohne Stromzufuhr dauerhaft erhalten bleiben, weil sie z.B. auf der Festplatte gespeichert sind.

Die persistenten Spuren werden im Rahmen des Gutachtens in technisch vermeidbare und technisch unvermeidbare Spuren unterteilt. Dabei sind technisch vermeidbare Spuren nicht kritisch für fehlerfreie Systemverhalten und können in der Regel einfach beseitigt werden. Technisch unvermeidbare Spuren fallen unweigerlich an und können nicht durch Änderungen an der Konfiguration eines Systems vermieden werden[8]. Zur Vermeidung oder Beseitigung von technisch unvermeidbaren Spuren sind spezielle Programme nötig, da die Bordmittel von Betriebssystemen dazu nicht ausreichen.

Weiterhin werden in diesem Gutachten digitale Spuren als robust bezeichnet, wenn das Entfernen oder Detektieren Detailkenntnisse voraussetzt und somit einem typischen Benutzer verborgen bleibt.

8 Dewald, A.: Formalisierung digitaler Spuren und ihre Einbettung in die Forensische Informatik, Dissertation, Universität Erlangen-Nürnberg, 2012

# 3 Ergebniszusammenfassung

Wie in Abschnitt 2.2 beschrieben werden die Spuren von PhotoScape mittels der Zustandsmethode durch die Programme idifference2.py sowie RegShot und durch die Ereignismethode mit der Software ProcMon akquiriert und im Anschluss analysiert. Zusätzlich werden forensische Tools wie JPGsnoop und Exiftool zur Untersuchung von Bearbeitungsspuren in Fotos verwendet. In diesem Kapitel werden die Untersuchungsergebnisse und die technisch vermeidbare sowie technisch unvermeidbare Spurenmenge vorgestellt.

## 3.1 Spuren im Dateisystem

Der Vergleich der Festplattenabbilder mittels idifference2.py erzeugt eine Textdatei mit vier Kategorien:

- New files (neu erstellte Dateien)
- Deleted files (gelöschte Dateien)
- Renamed files (umbenannte Dateien)
- Files with changed properties (Dateien mit geänderten Eigenschaften)

Das PowerShell-Skript zur Erzeugung der Festplattenabbilder (RAW-Datei) ist in **Anhang 5.1** zu finden. Das Bash-Skript zur Erzeugung der Spuren mittels der Zustandsmethode ist in **Anhang 5.2** zu finden.

### 3.1.1 Installation

Die Ausführung der Installation mit den Standardeinstellungen (Google Chrome wird nicht mit installiert) führt zu persistenten Spuren im Dateisystem. Nach der Standard-Installation von PhotoScape befindet sich das Verzeichnis *c:\Program Files\PhotoScape* auf dem Dateisystem (siehe **Bild 3.1**). Hier sind alle für die Anwendung relevanten Daten enthalten.

New files:
====

| | | |
|---|---|---|
| 2003-11-05T16:05:42Z | Program Files/Windows Media Player/Skins/modern-header.bmp | 9744 |
| 2003-12-09T07:23:48Z | Program Files/PhotoScape/riched20.dll | 431888 |
| 2005-07-07T04:33:24Z | Program Files/PhotoScape/frame/blackline01.bmp | 92 |
| 2005-08-17T12:03:14Z | Program Files/PhotoScape/texture/paper/noise_hard_03.jpg | 31152 |
| 2005-08-20T03:43:08Z | Program Files/PhotoScape/texture/paper/flower_01.jpg | 31018 |
| 2005-08-20T03:44:14Z | Program Files/PhotoScape/texture/paper/noise_hard_01.jpg | 22665 |
| 2005-08-20T03:45:34Z | Program Files/PhotoScape/texture/paper/noise_02.jpg | 28510 |
| 2005-08-20T03:46:32Z | Program Files/PhotoScape/texture/paper/line_vertical.jpg | 15362 |

**Bild 3.1** Beispiele neu erstellter Dateien im Verzeichnis c:\Program Files\PhotoScape[9]

Zusätzlich zum Installationsverzeichnis werden Einträge im Startmenü von Windows erzeugt und eine Verknüpfung auf dem Desktop angelegt. Auch die Prefetch-Datei wird als neu erstellte Datei erkannt. Die weiteren erzeugten Dateien und Verzeichnisse sowie deren Zweck sind in **Tabelle 3** aufgeführt. Weitere Dateizugriffe abgesehen von Zugriffen auf Standardbibliotheken des Windowsbetriebssystems und temporären Dateien erfolgen seitens des PhotoScape Installationsprozesses nicht.

**Tabelle 3 Verzeichnisse und Dateien bei der Installation**

| **Lfd. Nr.** | **Verzeichnis/Datei** | **Beschreibung** |
|---|---|---|
| 1 | C:\Program Files\PhotoScape | Installationsverzeichnis von PhotoScape |
| 2 | C:/ ProgramData/Microsoft/Windows/Start Menu/Programs/PhotoScape/ | Eintrag in der Start-Menüleiste von Windows |
| 3 | Users/Benutzername/AppData/Roaming/Microsoft/Internet Explorer/Quick Launch/PhotoScape.lnk | Windows-Verknüpfung |
| 4 | Users/Benutzername/Desktop/PhotoScape.lnk | Verknüpfung auf dem Desktop |
| 5 | Windows/Prefetch/PHOTOSCAPE-3-7-MULTI-WIN.EXE-6C74BAB0.pf | Prefetch-Datei des Installers |

Direkt im Anschluss an die Installation ruft der Installer die Internetseite *http://photoscape.org/link/link.php?version=installer&topic=afterinstall&v=3.7* auf. Eine Untersuchung der Browser-History nach dieser Internetseite liefert Hinweise über den Installationszeitpunkt. Die URL verweist durch ihre Bezeichnung *afterinstall* (siehe **Bild 3.2**) auf eine vorherige Installation und liefert einen Hinweis auf die Version (hier 3.7).

9 Der erste Eintrag *program files\windows media player* gehört nicht zur Spurenmenge von Photoscape

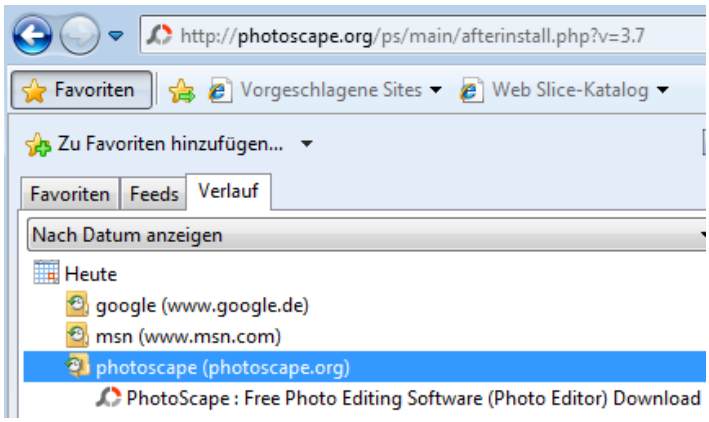



**Bild 3.2** Eintrag im Browser-Verlauf

### 3.1.2 Bildbearbeitung

Die Phase Bildbearbeitung erzeugt unter Verwendung von *Speichern* und *Speichern in…* standardmäßig den Ordner *C:\output* und legt dort das bearbeitete Bild ab (siehe **Bild 3.3**). Dieser Ordner sowie die Prefetch-Datei (bei erstmaliger Ausführung) werden neu angelegt (siehe **Bild 3.4**).

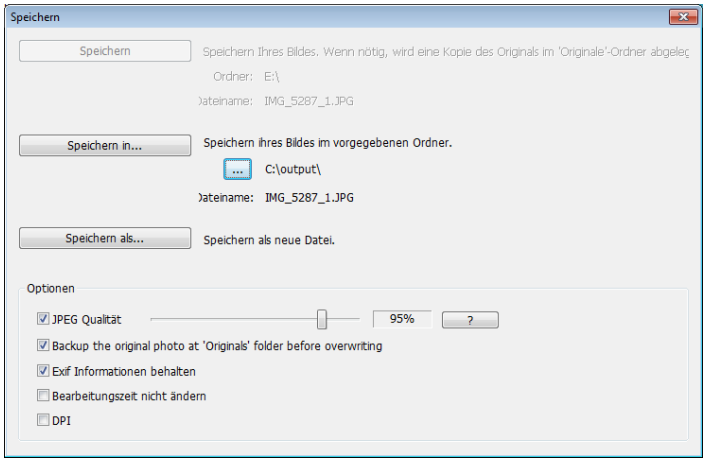



**Bild 3.3** Speichern eines Bildes

```
2012-12-26T14:17:58Z    Program Files/PhotoScape/frame/antique_photo01.psi    208
2018-01-05T16:45:35Z    Users/Benutzername/AppData/Roaming/PhotoScape         48
2018-01-05T16:45:44Z    Windows/Prefetch/PHOTOSCAPE.EXE-11B7AA72.pf           196840
2018-01-05T16:45:50Z    output                                4096
n/a                     Program Files/PhotoScape/balloon/b_08.emf
```

**Bild 3.4** Neu erstellte Dateien durch Bildbearbeitung

Nicht durch die Installation, aber durch die Programmausführung wird der Ordner *c:\Users\Benutzername\AppData\Roaming\PhotoScape* mit drei cfg-Dateien erzeugt (siehe **Bild 3.5**). Dabei ist es unerheblich, ob ein Bild eingelesen wurde. Bei cfg-Dateien handelt es sich um Konfigurationsdateien im Textformat, die von vielen Programmen genutzt werden. Das Verzeichnis und die cfg-Dateien bleiben auch nach der Deinstallation erhalten und sind ein Nachweis für die Ausführung von PhotoScape.

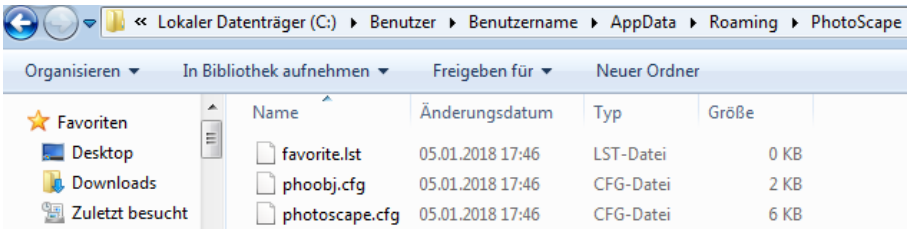



**Bild 3.5** cfg-Dateien, die durch die Programmausführung erstellt werden ohne dass es zu einer Bildbearbeitung kam

### 3.1.3 Deinstallation

Da die Anwendung während der Deinstallation vom System entfernt wird, werden in dieser Phase hauptsächlich Löschoperationen durchgeführt. Diese Phase erzeugt keine neuen Dateien. Aus forensischer Sicht von Interesse sind dabei Dateien, die beim Installieren und Anwenden der Software entstehen, aber nicht durch die Deinstallation entfernt werden. Solche persistenten Spuren können als Nachweis dienen, dass die Software auf dem aktuellen Betriebssystem des zu untersuchenden Rechners installiert war. Die in **Tabelle 3** genannten Dateien, werden bei der Deinstallation ausnahmslos entfernt. Der Ordner *c:\output* wird bei Deinstallation nicht entfernt, da dieser Ordner vom Benutzer gespeicherte Bilder enthalten kann. Aufgrund der weit verbreiteten Bezeichnung des Ordners ohne Bezug zu PhotoScape, ist es jedoch nur ein schwacher Hinweis auf eine vorherige PhotoScape-Nutzung. Aufgrund der einfachen Löschung des Ordners, handelt es sich um eine technisch vermeidbare und nicht-robuste Spur. Eine robuste Spur ist wie in Unterabschnitt 3.1.2 beschrieben, dass vorhanden sein des Ordners *c:\Users\Benutzername\AppData\ Roaming\PhotoScape.*

## 3.2 Spuren in der Registrierungsdatenbank

Mittels der Software Regshot Version 1.9.0 kann ein Abbild der Windows-Registrierungsdatenbank (kurz: Registry) vorgenommen werden. Die Registry ist die zentrale hierarchische Konfigurationsdatenbank von Windows und enthält Informationen zu Windows selbst und zu Programmen. Das Programm RegShot berechnet alle Änderungen von zwei Registry-Abbildern und speichert diese (siehe **Bild 3.6**). Damit Registry-Änderungen, die vom Betriebssystem erzeugt wurden, nicht in der Spurenmenge von PhotoScape erfasst werden, wird ein RegShot-Differenzbild erstellt bei dem keine Aktion ausgeführt wurde. Die durch dieses Leerlauf-Bild erkannten Spuren, werden aus der Spurenmenge von PhotoScape herausgenommen.

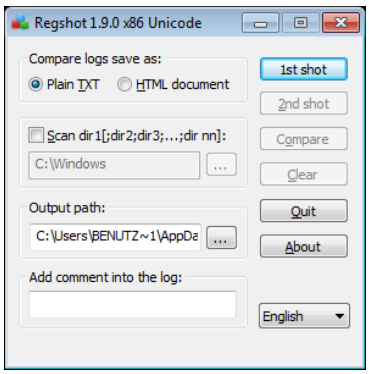



**Bild 3.6** Benutzeroberfläche von Regshot

### 3.2.1 Installation

Die Installation von PhotoScape erzeugt persistente Spuren in der Registry. Das Programm Regshot erkennt 11 zusätzliche Schlüssel (siehe **Bild 3.7**). Aufgrund der Bezeichnungen mit *photoscape* und *Mooii* (Hersteller des Programmes) ist eine eindeutige Zuordnung der Schlüssel zu PhotoScape möglich. Die Eintragungen mit Google (HKLM\SOFTWARE\Google) werden ebenfalls von der Installationsdatei erzeugt, da diese anbietet Google Chrome als Browser zu installieren. Zusätzlich wurden 25 Werte in der Registry hinzugefügt (siehe **Anhang 5.3**). Es wurden keine Schlüssel entfernt.

```
Keys added: 11
----------------------------------
HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASAPI32
HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASMANCS
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\PhotoScape.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\PhotoScape
HKLM\SOFTWARE\Google
HKLM\SOFTWARE\Google\No Chrome Offer Until
HKLM\SOFTWARE\Google\No Toolbar Offer Until
HKLM\SOFTWARE\Mooii
HKLM\SOFTWARE\Mooii\PhotoScape
HKU\S-1-5-21-2862746655-870442873-1674630423-1000\Software\Mooii
HKU\S-1-5-21-2862746655-870442873-1674630423-1000\Software\Mooii\PhotoScape
```

**Bild 3.7** Ausschnitt des Analyseergebnisses von Regshot bei der Installation

### 3.2.2 Bildbearbeitung

Das Starten der Anwendung, das Einlesen eines Fotos, sowie die Bildmanipulation, das anschließende Speichern und das Beenden der Anwendung erzeugen keine Spuren in der Registry, da keine Schlüssel erzeugt und keine neuen Werte eingetragen wurden.

### 3.2.3 Deinstallation

Nach der Phase Bildbearbeitung wird ein Registry-Snapshot erstellt und anschließend wird PhotoScape über die Systemsteuerung deinstalliert, wonach das zweite Registry-Snapshot entsteht (siehe **Anhang 5.4**). Es werden vier Schlüssel und elf Werte entfernt (siehe **Bild 3.8**). Diese Untersuchung zeigt, welche Registry-Änderungen die Deinstallation konkret vornimmt.

```
----------------------------------
Keys deleted: 4
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\PhotoScape.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\PhotoScape
HKLM\SOFTWARE\Mooii\PhotoScape
HKU\S-1-5-21-2862746655-870442873-1674630423-1000\Software\Mooii\PhotoScape

----------------------------------
Values deleted: 11
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\PhotoScape.exe\: ""C:\Program Files\PhotoScape\PhotoScape.exe""
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\PhotoScape.exe\Path: ""C:\Program Files\PhotoScape\PhotoScape.exe""
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\PhotoScape\DisplayName: "PhotoScape"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\PhotoScape\UninstallString: ""C:\Program Files\PhotoScape\uninstall.exe""
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\PhotoScape\DisplayIcon: ""C:\Program Files\PhotoScape\PhotoScape.exe""
HKLM\SOFTWARE\Mooii\PhotoScape\ProgramFolder: "C:\Program Files\PhotoScape"
HKLM\SOFTWARE\Mooii\PhotoScape\ProgramPath: "C:\Program Files\PhotoScape\PhotoScape.exe"
HKU\S-1-5-21-2862746655-870442873-1674630423-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\C:\
        Users\Benutzername\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\PhotoScape\PhotoScape.lnk: 0x00000001
HKU\S-1-5-21-2862746655-870442873-1674630423-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\C:\
        ProgramData\Microsoft\Windows\Start Menu\Programs\PhotoScape\PhotoScape.lnk: 0x00000001
HKU\S-1-5-21-2862746655-870442873-1674630423-1000\Software\Mooii\PhotoScape\ProgramFolder: "C:\Program Files\PhotoScape"
HKU\S-1-5-21-2862746655-870442873-1674630423-1000\Software\Mooii\PhotoScape\ProgramPath: "C:\Program Files\PhotoScape\PhotoScape.exe"
```

**Bild 3.8** Ausschnitt des Analyseergebnisses von Regshot bei der Deinstallation

Um die persistenten Spuren zu erhalten, die nachweisen, dass das Programm PhotoScape auf einem Rechner installiert und wieder deinstalliert wurde, muss ein Registry-Abbild vor der Installation und nach der Deinstallation erstellt werden.

Ausgehend vom selben Snapshot wie bei der Installation wird PhotoScape installiert und direkt wieder über die Systemsteuerung deinstalliert. Der Regshot macht dabei vor der Installation und nach der Deinstallation jeweils ein Registry-Abbild und vergleicht dies. Die Analyse zeigt, dass sieben Registry-Keys (**Bild 3.9**), die bei der Installation erstellt werden auch nach der Deinstallation erhalten bleiben. Liegt z.B. der Registry-Key *HKLM\SOFTWARE\Microsoft\Tracing\ photoscape-3-7-multi-win_RASAPI32* vor (siehe **Bild 3.10** links), hat man eine robuste Spur für eine PhotoScape-Deinstallation. Eine weitere eindeutige Spur ist der Registry-Schlüssel *HKLM\SOFTWARE\Mooii* (siehe **Bild 3.10** rechts). Es bleiben 14 Registry-Werte als robuste Spuren bestehen (siehe 5.4).

```
Keys added: 7
----------------------------------
HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASAPI32
HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASMANCS
HKLM\SOFTWARE\Google
HKLM\SOFTWARE\Google\No Chrome Offer Until
HKLM\SOFTWARE\Google\No Toolbar Offer Until
HKLM\SOFTWARE\Mooii
HKU\S-1-5-21-2862746655-870442873-1674630423-1000\Software\Mooii
```

**Bild 3.9** Robuste Spuren in Form von Registry-Keys durch PhotoScape

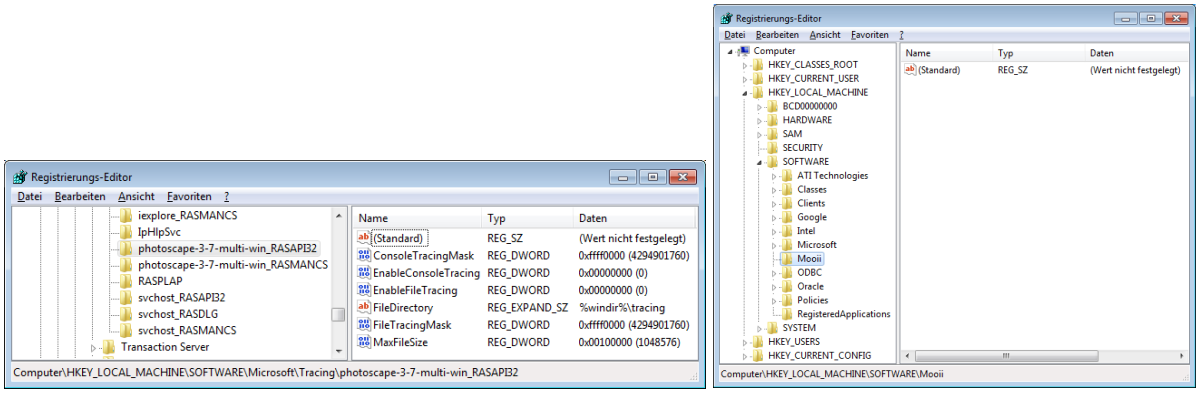



**Bild 3.10** Spuren einer Deinstallation von PhotoScape

## 3.3 Spuren im Prefetch-Verzeichnis

Prefetch-Dateien sind Systemdateien, die von Windows zur Startoptimierung von Anwendungen genutzt werden. Die Prefetch-Funktion lädt häufig genutzte Programme und Bibliotheken bereits beim Systemstart in den Arbeitsspeicher[10]. Sie stellen einen Indikator für die Existenz oder ehemalige Existenz von ausführbaren Dateien auf einem System dar. Solche Prefetch-Dateien sind robuste Spuren, da Anwender selten von solchen Dateien Kenntnisse haben[11].

Beim Durchlaufen der verschiedenen Phasen werden aufgrund des Aufrufs von ausführbaren Dateien mehrere Prefetch-Dateien erzeugt und im Verzeichnis *c:\Windows\Prefetch* mit einer Bezeichnung, die mit PHOTOSCAPE beginnt, abgelegt. Beim Aufruf des Installers wird direkt eine Prefetch-Datei mit der Bezeichnung PHOTOSCAPE-3-7-MULTI-WIN.EXE-B085E55EC.pf angelegt, wobei die Kennung nach dem letzten Bindestrich variabel ist. Liegt diese Datei im Ordner *c:\windows\prefetch* vor, ist es eine Spur für eine Installation von PhotoScape. Anhand des letzten MAC-Zeitpunktes kann auf den wahrscheinlichen Zeitpunkt der Installation geschlossen werden.

Wird PhotoScape erstmalig gestartet, wird eine weitere Prefetch-Datei mit der Bezeichnung PHOTOSCAPE.EXE-CCF544F.pf erstellt, wobei auch hier die Kennung nach dem letzten Bindestrich variabel ist. Das Vorhandensein dieser Datei ist also eine Spur für die Verwendung von PhotoScape und der letzte MAC-Zeitpunkt zeigt die letztmalige Verwendung des Programmes. Die Bearbeitung von Bilder erzeugt keine weiteren Einträge im Prefetch-Verzeichnis. Die Deinstallation entfernt keine Dateien aus dem Prefetch-Ordner, womit diese zwei Prefetch-Dateien robuste Spuren auf Verwendung von PhotoScape sind.

Das Programm WinPrefechView zeigt die Anzahl der Programmaufrufe (Run Counter) und die Zeitstempel der Aufrufe (Last Run Time) an (siehe **Bild 3.11**). Damit kann ausgesagt werden, wann das Programm installiert (Created Time) und ausgeführt wurde.

---

10 Internetquelle: http://www.pctipp.ch/tipps-tricks/kummerkasten/windows-xp/artikel/wozu-ist-der-prefetch-ordner-da-33023/, abgerufen am 20.12.2017

11 Simon Jansen: Analyse der Spurenmenge der Anwendung OpenVPN Client Version 2.3.9 in Microsoft Windows. Technischer Bericht in digitaler Forensik Nr. 1 vom 15.2.2016. Abrufbar unter: https://www1.cs.fau.de/content/technische-berichte-digitaler-forensik

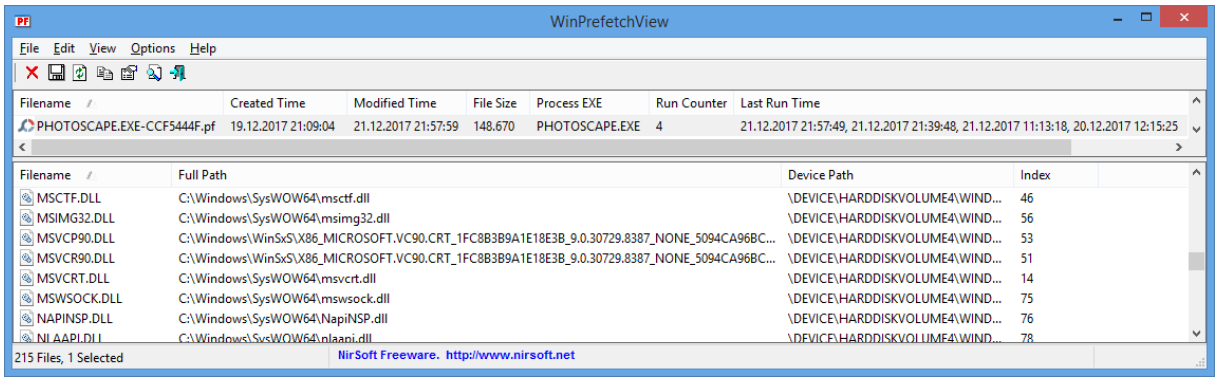



**Bild 3.11** Ausschnitt für die Prefetch-Datei zur Ausführungsdatei von PhotoScape

## 3.4 Ereignismethode mit Procmon

Das Analysetool Procmon wird wie im Abschnitt 2.4 beschrieben mit dem Filter *Process Name begins with photoScape* eingesetzt.

### 3.4.1 Installation und Deinstallation

Die Installation kann durch Procmon nachvollzogen werden[12]. Das Starten des Installers, der Eintrag der Prefetch-Datei, das Erstellen der Desktop-Verknüpfung sowie die Registry-Einträge sind erkennbar (siehe **Bild 3.12**). Es wurden dieselben Spuren gefunden wie bereits in den vorherigen Kapiteln beschrieben. Durch Ansicht des Process Tree in Procmon erkennt man, dass zum Installer auch der Aufruf einer Internetseite (im vorliegenden Fall mit dem Standard-Browser Internet Explorer) gehört (siehe **Bild 3.13**)[13].

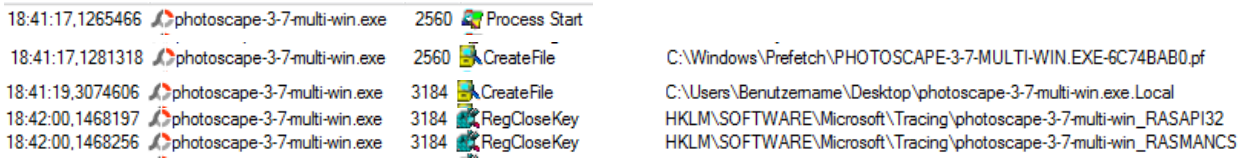



**Bild 3.12** Ausschnitte des Analyseergebnisses von Procmon

12 Nur die Installation erzeugt bereits 25.658 Ereignisse mit dem gesetzten Filter und insgesamt erfasst Procmon in dieser Zeit 204.233 Ereignisse.

13 GTGCAPI ist eine Art von Windows-Datei mit Windows Betriebssystem von Mooii. Quelle: https://www.afixtoz.com/german/1597279/gtgcapi-exe-fehler-beheben-gtgcapi-exe-detaillierte-informationen.html

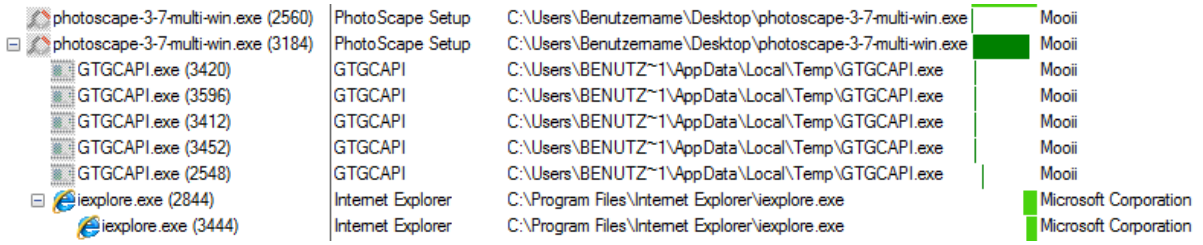



**Bild 3.13** Ausschnitte des Process Trees

Die Ereignismethode angewandt auf die Phase Deinstallation liefert keine nennenswerten zusätzlichen Resultate.

### 3.4.2 Bildbearbeitung

Die Phase Bildbearbeitung zeigt auch in der Ereignismethode die bereits bekannten Spuren, wie das Erstellen der Prefetch-Datei für die Ausführungsdatei, sowie das Anlegen des Ordners Output und die Speicherung des Bildes (siehe **Bild 3.14**).

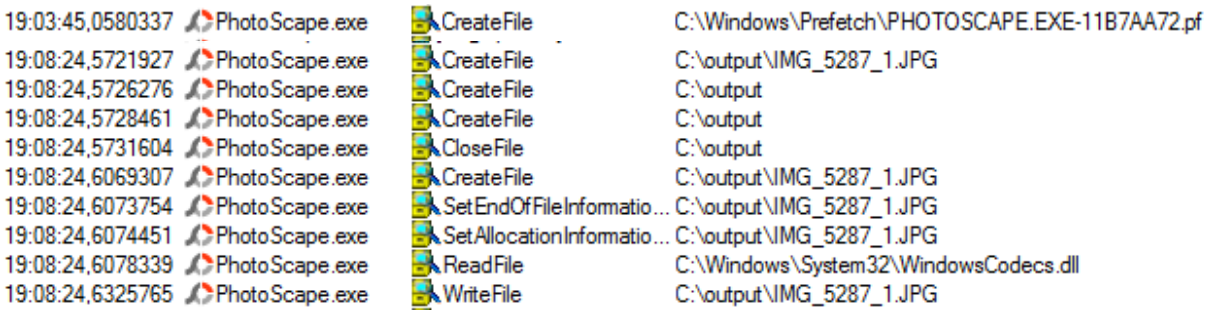



**Bild 3.14** Phase Bildbearbeitung

## 3.5 Spuren in JPG-Bildern

Im Folgenden wird untersucht, ob in Bildern Spuren existieren, die auf eine Bildbearbeitung durch PhotoScape hindeuten. Dazu werden die zwei frei verfügbaren Tools exiftool und JPGsnoop zur Analyse der Metadaten verwendet. Da die meisten Fotos im JPG-Format vorliegen, wird ein solches untersucht. Das zu untersuchende Foto zeigt mehrere Quallen und wurde mit einer Canon PowerShot SX230 HS Kamera aufgenommen. Die durchgeführten Bildmanipulationen sind die Duplizierung mehrerer Quallen mittels des Kopierstempels (Clone Stamp) von PhotoScape (siehe **Bild 3.15**).

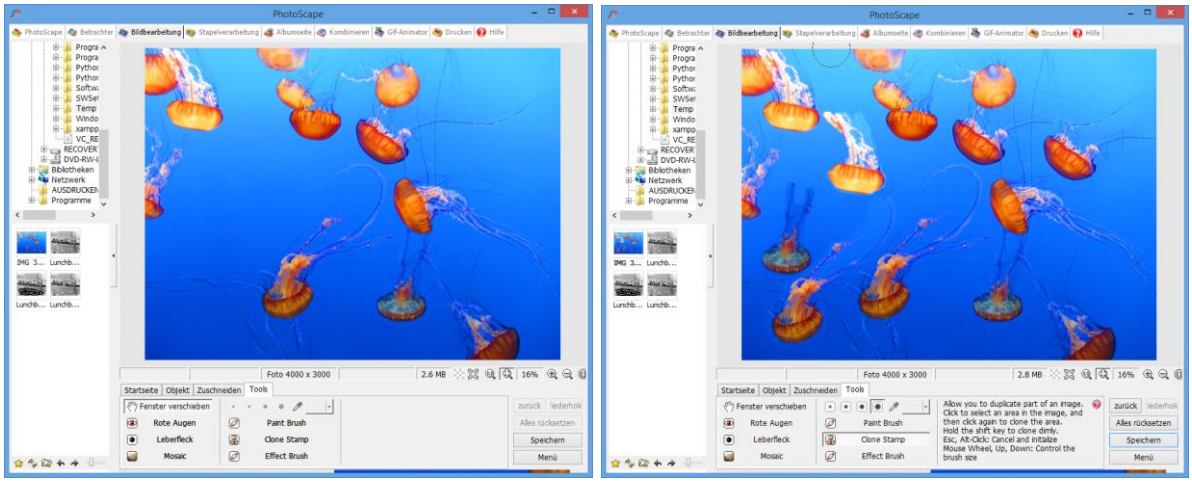


**Bild 3.15** Originalbild (links) und modifiziertes Bild (rechts)

Durch die Bildmanipulation hat sich neben der Dateigröße, die leicht von 2,6 auf 2,8 MB vergrößert wurde, der Zeitstempel FileModifyDate und FileAccessDate verändert. Eine robuste Spur ist der Metadateneintrag beim Marker IFD0 *Software PhotoScape* (siehe **Bild 3.16** rechts). Dieser Eintrag deutet direkt auf eine Verwendung von PhotoScape hin.

| | ---- System ---- |
|---|---|
| FileName | IMG_3227.JPG |
| Directory | . |
| FileSize | 2.6 MB |
| FileModifyDate | 2015:02:17 20:58:12+01:00 |
| FileAccessDate | 2015:03:02 20:12:28+01:00 |
| FileCreateDate | 2015:03:02 20:12:28+01:00 |

| | ---- IFD0 ---- |
|---|---|
| ImageDescription | |
| Make | Canon |
| Model | Canon PowerShot SX230 HS |
| Orientation | Horizontal (normal) |
| XResolution | 180 |
| YResolution | 180 |
| ResolutionUnit | inches |
| ModifyDate | 2015:02:17 20:58:13 |
| YCbCrPositioning | Co-sited |

| | ---- System ---- |
|---|---|
| FileName | IMG_3227.JPG |
| Directory | . |
| FileSize | 2.8 MB |
| FileModifyDate | 2018:01:08 21:23:23+01:00 |
| FileAccessDate | 2018:01:08 21:23:23+01:00 |
| FileCreateDate | 2015:03:02 20:12:28+01:00 |

| | ---- IFD0 ---- |
|---|---|
| ImageDescription | |
| Make | Canon |
| Model | Canon PowerShot SX230 HS |
| XResolution | 180 |
| YResolution | 180 |
| ResolutionUnit | inches |
| Software | PhotoScape |
| ModifyDate | 2015:02:17 20:58:13 |
| YCbCrPositioning | Co-sited |

**Bild 3.16** Metadaten des Originalfotos (links) und Metadaten des modifizierten Fotos (rechts)

## 3.6 Übersicht und Klassifizierung der Spuren

Es konnten in jeder der definierten Phasen digitale Spuren gefunden werden. Die **Tabelle 4** zeigt eine Übersicht über die Spuren und in welcher Phase sie gefunden wurden. Die Spur im Prefetch-Verzeichnis in der Phase Bildbearbeitung, wird durch das Starten von PhotoScape und nicht durch die eigentliche Bildmanipulation erzeugt.

**Tabelle 4 Übersicht, ob Spuren existieren**

| **Phasen** | **Spuren** | | | |
|---|---|---|---|---|
| | **Dateisystem** | **Registry** | **Prefetch** | **Metadaten** |
| Installation | ja | ja | ja | keine |
| Bildbearbeitung | ja | keine | ja | ja |
| Deinstallation | ja | ja | keine | keine |

Die **Tabelle 5** zeigt eine Übersicht von Beispielen der konkreten Spuren in den jeweiligen Phasen. Nach der Klassifizierung von Spuren im **Abschnitt 2.5** handelt es sich bei den Spuren im Dateisystem, der Registry und im Prefetch-Ordner um technisch vermeidbare Spuren, da diese mit den Bordmitteln von Windows entfernt werden können ohne das Funktionieren des Systems zu gefährden. Der Eintrag in den Metadaten des Fotos ist eine technisch nicht vermeidbare Spur und kann nicht mit den Bordmitteln von Windows entfernt werden.

Nach der Definition von Robustheit (siehe **Abschnitt 2.5**) handelt es sich bei dem Installationsverzeichnis und dem Verzeichnis c:\output im Dateisystem um nicht-robuste Spuren, da diese Ordner einfach zu detektieren und entfernen sind. Die URL-Spur im Browser-Verlauf, die Einträge in der Registry, die Dateien im Prefetch-Ordner und die Veränderung der Metadaten sind robuste Spuren, da sie Detailkenntnisse voraussetzen. Das Verzeichnis für die cfg-Dateien wird ebenfalls als robuste Spur klassifiziert, da es nicht durch die Installation erzeugt wird und die Entfernung Kenntnis von Konfigurationsdateien voraussetzt.

**Tabelle 5 Konkrete Spuren der jeweiligen Phasen (robuste Spuren sind fett hervorgehoben)**

| **Phasen** | **Spuren** | | | |
|---|---|---|---|---|
| | **Dateisystem** | **Registry** | **Prefetch** | **Metadaten des Fotos** |
| Installation | • C:\Program Files\PhotoScape<br>• **Browserverlauf: http://photoscape.org...** | • **HKLM\SOFTWARE\ Mooii\PhotoScape** | • **PHOTOSCAPE-3-7-MULTI I-WIN-B085E55EC.EXE-.pf** | • keine |
| Bildbe-arbeitung | • C:\output<br>• **C:\Users\Benutzername\AppData\Roaming\PhotoScape** | • keine | • **PHOTOSCAPE.EXE-CCF544F.pf** | • **Software: PhotoScape** |
| Deinstal-lation | • C:\output<br>• **C:\Users\Benutzername\AppData\Roaming\PhotoScape** | • **HKLM\SOFTWARE\Microsoft\ Tracing\ photoscape-3-7-multi-win_RASAPI32** | • keine | • keine |

# 4 Fazit und Wertung

Die beschriebenen Ergebnisse der Anwendungsanalyse zeigen persistente Spuren von PhotoScape im Dateisystem, in der Registry und in dem Windows-Prefetch-Ordner. Es können somit Rückschlüsse gezogen werden, ob die Anwendung auf einem Rechner installiert war und ob Fotos mit der Software manipuliert wurden.

Die Deinstallation vernichtet den Großteil der persistenten Spuren einer früheren Installation im Dateisystem. Ein vorhandenes Verzeichnis *c:\output* kann als ein Hinweis auf eine frühere Installation und Bildbearbeitung interpretiert werden, jedoch nicht als robuste Spur. Eine robuste Spur einer Deinstallation ist das Vorhandensein des Verzeichnisses mit den Konfigurationsdateien sowie der Browserverlauf-Eintrag, der durch die Installation erstellt wird.

Durch die bei der Deinstallation nicht entfernten Werte und Schlüssel sowie den hinzugefügten Werten in der Registry, lässt sich nachweisen, dass PhotoScape installiert war. Eine Bildmanipulation erzeugt keine Veränderungen in der Registry.

Insbesondere die von Windows erzeugten Prefetch-Dateien zu PhotoScape sind robuste Spuren, die eine vorherige Existenz der Anwendung beweisen. Anhand der Datei PHOTOSCAPE-3-7-MULTI-WIN.EXE-B085E55EC.pf lässt sich der wahrscheinliche Zeitpunkt der Installation ermitteln, und anhand der Datei PHOTOSCAPE.EXE-CCF544F.pf die Zeitpunkte der Verwendungen des Programmes.

Eine aus forensischer Sicht interessante Spur, die eine Bildbearbeitung mittels PhotoScape in einem Bild vom Typ jpg nachweist, kann in den Metadaten des Bildes als Eintrag bei Software vorhanden sein.

# 5 Anhang

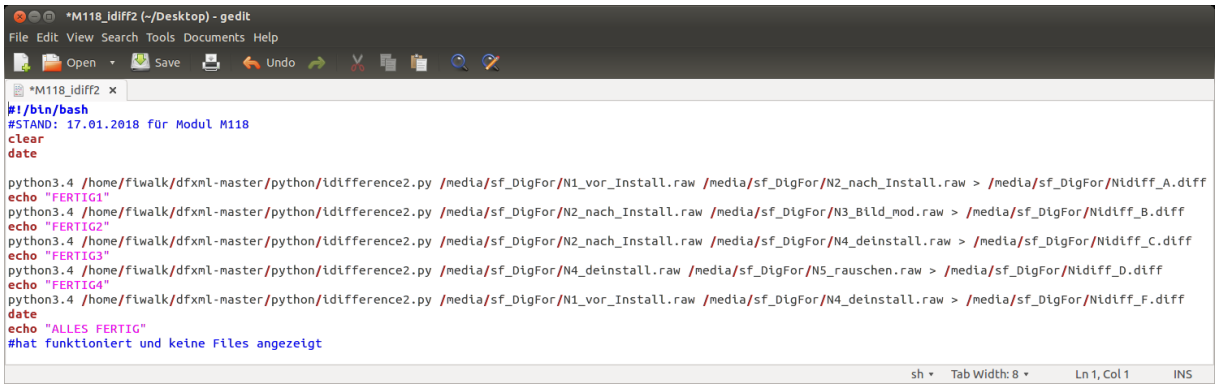
## 5.1 PowerShell-Skript zur Erstellung der Festplattenabbilder

```
#Stand 09.01.2018
#Dies ist ein PowerShell-Skript!
##Skript zur Erstellung der raw-Dateien aus den VMs zur späteren Analyse mittels
idifference2 und Python
clear
Write-Host "----Start----"
$starttime = date

#######1. RAW-Datei erstellen
c:\programme\oracle\virtualbox\vboxmanage.exe list hdds
C:\programme\Oracle\VirtualBox\vboxmanage clonehd 552e26ca-2a57-4539-8bf3-
9eed13c9a365 --format RAW C:\temp\Snapshots_RAW\N1_vor_Install.raw
Write-Host "----Beendet1----"
C:\programme\Oracle\VirtualBox\vboxmanage clonehd 449cdfc6-98a9-4602-a000-
6388a19fa656 --format RAW C:\temp\Snapshots_RAW\N2_nach_Install.raw
Write-Host "----Beendet2----"
C:\programme\Oracle\VirtualBox\vboxmanage clonehd 2bb4ff2f-b069-4c2c-9c8c-
d7fe10a93da1 --format RAW C:\temp\Snapshots_RAW\N3_Bild_mod.raw
Write-Host "----Beendet3----"
C:\programme\Oracle\VirtualBox\vboxmanage clonehd 3d474634-cd8e-4a17-b041-
b39f33abcec6 --format RAW C:\temp\Snapshots_RAW\N4_deinstall.raw
Write-Host "----Beendet3----"
C:\programme\Oracle\VirtualBox\vboxmanage clonehd 17ad932c-d10d-42b9-8cfb-
da18a1a5d18b --format RAW C:\temp\Snapshots_RAW\N5_rauschen.raw
####hier wird der Snapshot in das RAW-Format umgewandelt; Dauer: 5 Min. bei 6 GB

$endtime = date
$time = $endtime - $starttime
Write-Host
"$($time.Hours)h:$($time.Minutes)m:$($time.Seconds)s:$($time.Milliseconds)ms"
Write-Host "----Beendet----"
```

## 5.2 Bash-Skript zur Erstellung von Spuren mittels Zustandsmethode



## 5.3 Zusätzliche Werte in der Registry durch Installation

- Values added: 25
- ----------
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASAPI32\EnableFileTracing: 0x00000000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASAPI32\EnableConsoleTracing: 0x00000000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASAPI32\FileTracingMask: 0xFFFF0000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASAPI32\ConsoleTracingMask: 0xFFFF0000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASAPI32\MaxFileSize: 0x00100000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASAPI32\FileDirectory: "%windir%\tracing"
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASMANCS\EnableFileTracing: 0x00000000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASMANCS\EnableConsoleTracing: 0x00000000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASMANCS\FileTracingMask: 0xFFFF0000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASMANCS\ConsoleTracingMask: 0xFFFF0000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASMANCS\MaxFileSize: 0x00100000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASMANCS\FileDirectory: "%windir%\tracing"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\PhotoScape.exe\: ""C:\Program Files\PhotoScape\PhotoScape.exe""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\PhotoScape.exe\Path: ""C:\Program Files\PhotoScape\PhotoScape.exe""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\PhotoScape\DisplayName: "PhotoScape"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\PhotoScape\UninstallString: ""C:\Program Files\PhotoScape\uninstall.exe""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\PhotoScape\DisplayIcon: ""C:\Program Files\PhotoScape\PhotoScape.exe""
- HKLM\SOFTWARE\Google\No Chrome Offer Until\Mooii: 0x0133EEE0
- HKLM\SOFTWARE\Mooii\PhotoScape\ProgramFolder: "C:\Program Files\PhotoScape"
- HKLM\SOFTWARE\Mooii\PhotoScape\ProgramPath: "C:\Program Files\PhotoScape\PhotoScape.exe"
- HKU\S-1-5-21-2862746655-870442873-1674630423-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\C:\Users\Benutzername\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\PhotoScape\PhotoScape.lnk: 0x00000001
- HKU\S-1-5-21-2862746655-870442873-1674630423-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\C:\ProgramData\Microsoft\Windows\Start Menu\Programs\PhotoScape\PhotoScape.lnk: 0x00000001
- HKU\S-1-5-21-2862746655-870442873-1674630423-1000\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Persisted\C:\Users\Benutzername\Desktop\photoscape-3-7-multi-win.exe: 0x00000001
- HKU\S-1-5-21-2862746655-870442873-1674630423-1000\Software\Mooii\PhotoScape\ProgramFolder: "C:\Program Files\PhotoScape"
- HKU\S-1-5-21-2862746655-870442873-1674630423-1000\Software\Mooii\PhotoScape\ProgramPath: "C:\Program Files\PhotoScape\PhotoScape.exe"

## 5.4 Spuren als Registry-Werte nach Deinstallation

- Values added: 14
- ----------
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASAPI32\EnableFileTracing: 0x00000000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASAPI32\EnableConsoleTracing: 0x00000000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASAPI32\FileTracingMask: 0xFFFF0000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASAPI32\ConsoleTracingMask: 0xFFFF0000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASAPI32\MaxFileSize: 0x00100000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASAPI32\FileDirectory: "%windir%\tracing"
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASMANCS\EnableFileTracing: 0x00000000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASMANCS\EnableConsoleTracing: 0x00000000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASMANCS\FileTracingMask: 0xFFFF0000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASMANCS\ConsoleTracingMask: 0xFFFF0000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASMANCS\MaxFileSize: 0x00100000
- HKLM\SOFTWARE\Microsoft\Tracing\photoscape-3-7-multi-win_RASMANCS\FileDirectory: "%windir%\tracing"
- HKLM\SOFTWARE\Google\No Chrome Offer Until\Mooii: 0x0133EEE0
- HKU\S-1-5-21-2862746655-870442873-1674630423-1000\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Persisted\C:\Users\Benutzername\Desktop\photoscape-3-7-multi-win.exe: 0x00000001