FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Analyse von Browserdaten im RAM

Frederik Rausch
Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

Gliederung

Motivation + Ziele

Vorgehen

Plugins

Datenbank-Erweiterung

Fazit

Motivation

- Kriminelle Aktionen mit Browsern
- Aktionen hinterlassen Spuren

- Anonymes Surfen
- Daten wurden gelöscht oder versteckt

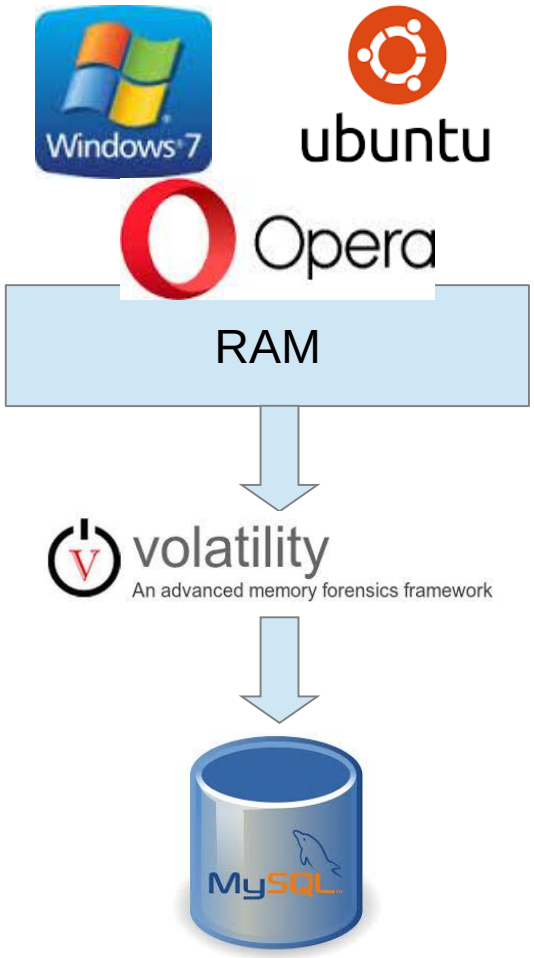
Volatility

- Sammlung von IT-Tools
- Untersucht RAM-Abbilder
- Wird zur Aufklärung von Straftaten verwendet

- Plugin Internet Explorer
  - Volatility Foundation
  - History
- Plugin Firefox und Chrome
  - Dave Lassalle
  - History, Downloads, Cookies

Ziele

- Schreiben Browser interessante Daten in den RAM?
- Daten im RAM auffindbar?
- Falls ja:
  - Daten Analysieren
  - Programm schreiben um diese Daten auszugeben
- Verwendeter Browser Opera
- Zuerst Fokus auf Windows 7, später für Linux erweitert.
- Daten in Datenbank schreiben



Vorgehen bei Opera

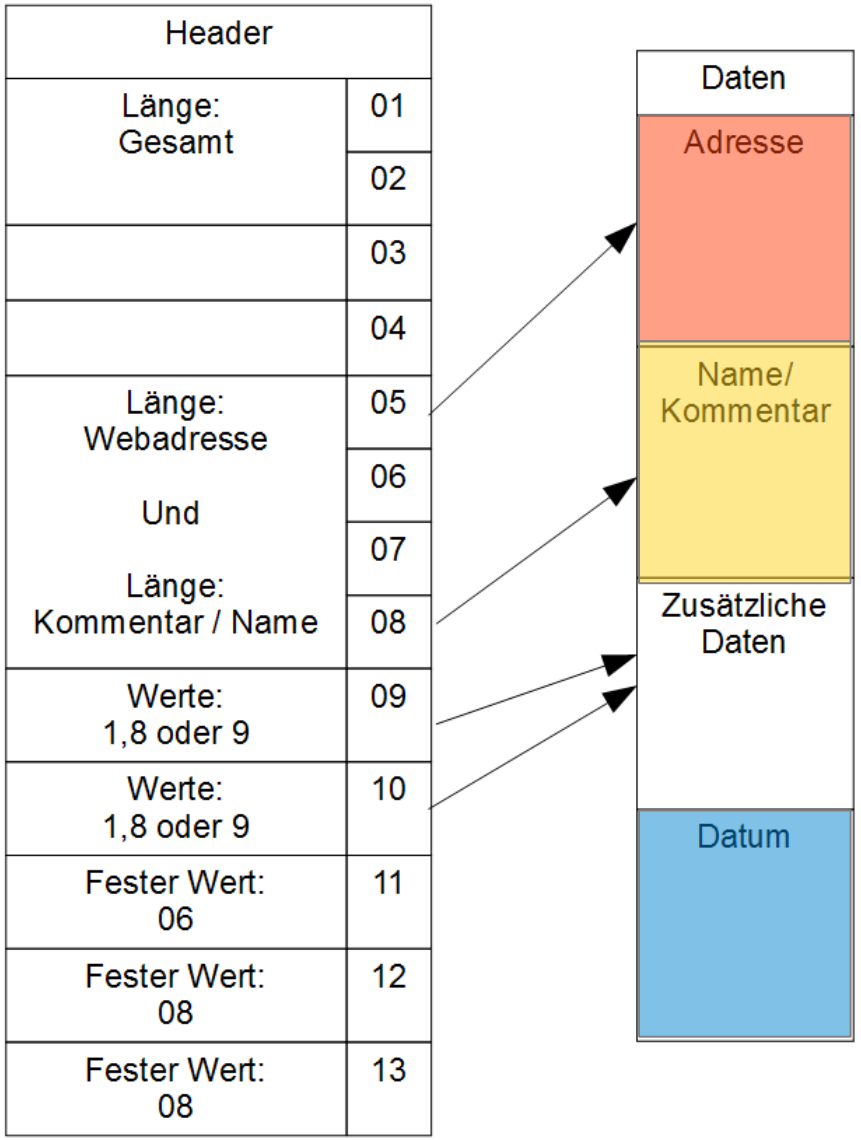
- Virtuelle Maschinen erzeugt
- Nachstellen eines Benutzers(Browsen im Netz)
- RAM-Abbilder der VM erstellt
- Analyse des RAM
- Datenstrukturen gefunden
  - History, Downloads und Cookies

Beispiel RAM-Struktur

- Gleicher Aufbau
  - Header und Daten
- Header
  - Längenangaben
  - Flags

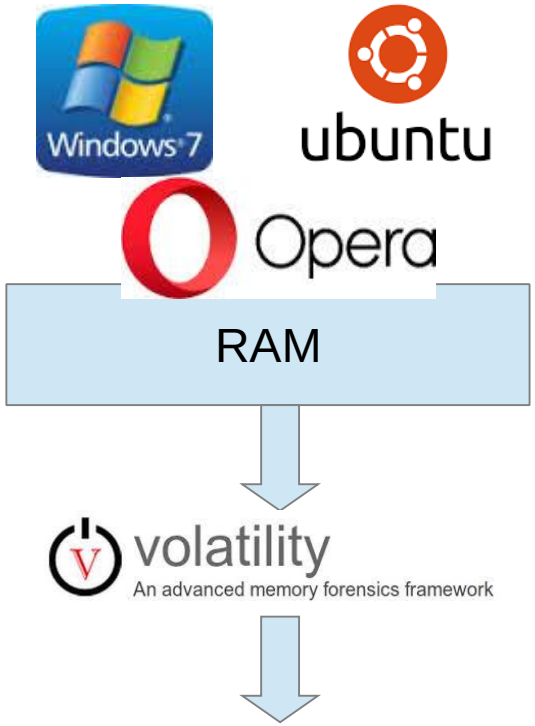
```
C9 45 05 09 00 39 45 01 01 06 08 08 68 74 74 70
3A 2F 2F 77 77 77 2E 73 70 69 65 67 65 6C 2E 64
65 2F 4E 61 63 68 72 69 63 68 74 65 6E 20 2D 20
53 50 49 45 47 45 4C 20 4F 4E 4C 49 4E 45 02 02
00 2E 79 1B 1A D8 53
```

```
ÉE...9E.....http
://www.spiegel.d
e/Nachrichten -
SPIEGEL ONLINE..
..y..ØS
```



Plugins

- Mehrere Plugins für Volatility entwickelt
- Für Windows
  - operahistory
  - operacookies
  - operadownloads
- Für Linux
  - linux_operahistory
  - linux_operacookies
  - linux_operadownloads



History Plugin

- operahistory bzw. linux_operahistory
- Wird auch angelegt wenn Benutzer Speicherung deaktiviert hat

Beispiel Output des Plugins:

```
C:\...\volatility-2.4>vol.py -f C:\...\test.vmem operahistory
Volatility Foundation Volatility Framework 2.4

Location: http://www.google.de/
Comment : Google
Date    : 2015-08-02 07:52:33

Location: http://www.spiegel.de/
Comment : Nachrichten - SPIEGEL ONLINE
Date    : 2015-07-10 14:50:50

Location: http://heise.de/
Comment : heise online - IT-News, Nachrichten und Hintergr├╝nde
Date    : 2015-07-01 09:15:50
```

Downloads Plugin

- operadownloads bzw. linux_operadownloads
- Werden immer in den Speicher geladen
- Quellpfad nicht immer angegeben

Beispiel Output des Plugins

```
C:\...\volatility-2.4>vol.py operadownloads -f C:\...\test.vmem
Volatility Foundation Volatility Framework 2.4

----------------------------------
path        : C:\Users\test\Downloads\winrar-x64-521d.exe
Start date  : 2015-08-02 07:56:28
End date    : 2015-08-02 07:56:31
Source      : http://www.winrar.de/downld.php

----------------------------------
path        : C:\Users\test\Downloads\npp.6.8.Installer.exe
Start date  : 2015-08-02 07:55:04
End date    : 2015-08-02 07:55:43
Source      :
http://www.chip.de/downloads/c1_downloads_hs_getfile_v1_16084909.html?t=1438494869&v
=3600&s=ab8673556e3b7aefa034e73d270aea58
```

Cookie Plugin

- operacookies bzw. linux_operacookies
- Werden nicht alle in Speicher geladen
- Nur wenn Speichern Aktiviert

Beispiel Output des Plugins:

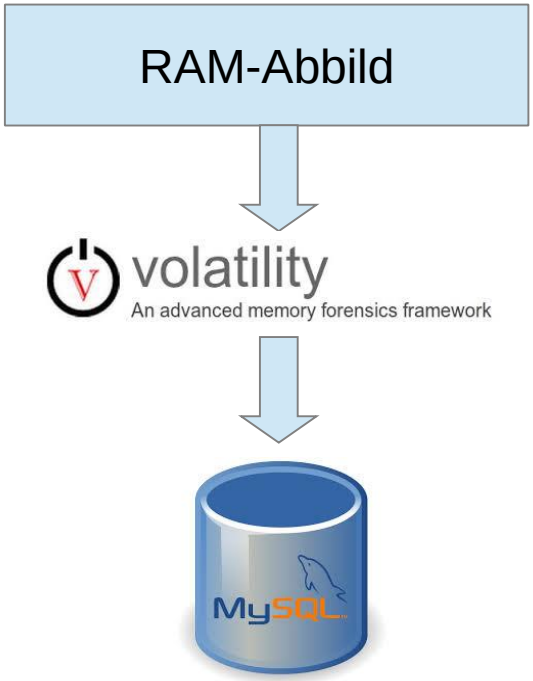
```
C:\...\volatility-2.4>vol.py -f C:\...\ubuntu.vmem linux_operacookies --
profile=LinuxUbuntux86
Volatility Foundation Volatility Framework 2.4

----------------------------------
cookie name    : __utmc
adress         : www.golem.de
date start     : 2016-01-07 09:51:39
date end       : temp

----------------------------------
cookie name    : iS
adress         : www.golem.de
date start     : 2016-01-07 09:51:42
date end       : temp
```

MySQL-Ausgabe

- Zusätzlich MySQL-Ausgabe für alle Plugins
- INSERT-Befehle




```
C:\...\volatility-2.4>vol.py -f C:\...\test.vmem operahistory --output=mysql
Volatility Foundation Volatility Framework 2.4

INSERT INTO `operahistory` (`HistoryAddress`, `HistoryComment`, `HistoryDate`)
VALUES ('http://www.google.de/','Google','2015-08-02 07:52:33');
INSERT INTO `operahistory` (`HistoryAddress`, `HistoryComment`, `HistoryDate`)
VALUES ('http://www.spiegel.de/','Nachrichten - SPIEGEL ONLINE','2015-07-10
14:50:50');
INSERT INTO `operahistory` (`HistoryAddress`, `HistoryComment`, `HistoryDate`)
VALUES ('http://heise.de/','heise online - IT-News, Nachrichten und
Hintergr├╝nde','2015-07-01 09:15:50');
```

Datenbank Programm

- Ruft ein Volatility Plugin mit MySQL Ausgabe auf
- Schreibt gefundene Daten in MySQL-Datenbank
- Datenbanktabellen brauchen festgelegtes Format
- Parameter
  - Host, Datenbankname, Benutzer und Passwort
  - Volatility-Pfad, RAM-Abbild und Pluginname

```
C:\...>db_insert_opera_plugins.py --host=127.0.0.1 --database=testdatenbank --
user=test --pass=test --vol=C:\...\volatility-2.4\ --ram=C:\...\test.vmem --
operaplugin=operahistory
```

Fazit

- Es sind interessante Daten im RAM
- Neue Volatility Plugins finden Daten von Opera
- Daten können in Datenbank geschrieben werden
- Ausblick:
  - Änderungen durch Updates
  - Plugins für weitere Betriebssysteme testen
  - Weitere Volatility-Plugins für MySQL

Ende

Vielen Dank für Ihre Aufmerksamkeit