JOHANNES KEPLER
UNIVERSITÄT LINZ
Netzwerk für Forschung, Lehre und Praxis

TNF

Forensische Analyse von Web-Browsern, deren Spuren und Werkzeugen zur Spurenlöschung

Praktikum

aus

Netzwerke und Sicherheit

Angefertigt am *Institut für Informationsverarbeitung und Mikroprozessortechnik*

Betreuung:

Assoz.Prof. Priv.-Doz. Mag. Dipl.-Ing. Dr. Michael Sonntag

Eingereicht von:

Markus Jäger BSc, k0657537

Linz, April 2013

Zusammenfassung

Mit diesem Projekt soll untersucht werden, welche Spuren auf einem Computer hinterlassen werden, wenn mit einem Browser das World Wide Web gesurft wird und in weiterer Folge, wie effizient ausgewählte Werkzeuge zum Entfernen dieser Spuren arbeiten.

Allgemein bekannt ist, dass Spuren wie ein Verlauf, temporäre Internetdateien, Cache und gespeicherte Zertifikate im System erhalten bleiben, die auf das Browsingverhalten des Nutzers rückschließen lassen können. Es soll untersucht werden, welche, neben den bekannten soeben erwähnten, Spuren tatsächlich im System nachvollziehbar sind.

Kapitel 1 beinhaltet eine kurze Einführung in die Thematik bzw. die Motivation für diese Arbeit und eine zusammengefasste Aufgabenstellung, die einen Überblick über das Projekt geben soll.

Kapitel 2 beschreibt die Arbeitsumgebung näher. Hierzu zählen die verwendete Virtualisierungssoftware und das Betriebssystem, auf dem die Untersuchungen und Versuche durchgeführt werden. Weiters werden die verwendeten Browser beschrieben und die ausgewählten Löschwerkzeuge erläutert.

Den relevanten Untersuchungsobjekten wird, da hier sehr detaillierte Informationen über die jeweiligen Browser und die Objekte gelistet werden, ein eigenes Kapitel gewidmet. In Kapitel 3 werden alle verfügbaren Informationen über gespeicherte Objekte und Informationen sowie deren Speicherorte und Speicherarten, auch browserspezifische Informationen darüber, soweit die Recherchen ergeben haben, erläutert.

In Kapitel 4, dem Ablauf, wird die genaue Vorgehensweise erläutert. Dies erfüllt den Zweck der späteren Nachvollziehbarkeit der gefundenen und dokumentierten Spuren.

In der Versuchsdurchführung in Kapitel 5 wird gezeigt, welche Spuren, für jeden verwendeten Browser, erzeugt wurden, wo sie gefunden wurden und, für jedes Werkzeug, wie effizient und gründlich die Spuren entfernt wurden.

In Kapitel 6 werden basierend auf den Ergebnissen in Kapitel 5 die Löschwerkzeuge miteinander verglichen und die Ergebnisse ausgewertet.

Kapitel 7 gibt abschließend eine kurze Zusammenfassung und ein Resümee über den Inhalt des Projekts und stellt weitere Versuche in diesem Gebiet in Aussicht.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung

1.1 Motivation

Beim Masterstudium "Netzwerke und Sicherheit" an der Johannes Kepler Unversität Linz wird neben den klassischen Netzwerkthemen auch ein Schwerpunkt auf sicherheitsrelevante Themen gelegt, worunter auch die Forensik, im Speziellen die Computerforensik, fällt. Ich möchte mit diesem Projekt unter anderem die forensischen Aspekte in diesem Studium etwas intensiver bearbeiten und mir dadurch mehr Erfahrung in diesem Bereich aneignen.

Im Zuge der Computerforensik werden auch oft Spuren der Benutzung von Webbrowsern eines Users untersucht. Allgemein bekannt ist, dass beim Surfen des World Wide Webs vom Browser Spuren im System hinterlassen werden. Zu den bekannten Spuren zählen unter anderem die Chronik bzw. der Verlauf, der Cache und temporäre Internetdateien.

Einige dieser Spuren werden von allen Browsern global an einer Stelle im System gespeichert, andere Spuren werden von jedem Browser individuell und auf unterschiedliche Weise abgespeichert. Weiters wird vermutet, dass ausser den bekannten Spuren noch weitere nachvollziehbare Informationen im System erhalten bleiben, von denen der Nutzer nichts weiß. Beispielsweise sind in der Registrierung die letzten zehn eingegeben Link-Adressen (typed URLs) vom Internet Explorer zu finden. Ein Umstand, der nur den wenigsten Nutzern bekannt ist. Mit ziemlicher Sicherheit sind auch Spuren in der jeweiligen Auslagerungsdatei vom Betriebssystem Microsoft Windows zu finden.

Die Motivation hinter diesem Projekt ist, über diese Themen möglichst viel herauszufinden und die tatsächlichen Veränderungen, die im System verursacht werden wenn ein Benutzer im Internet surft, soweit wie möglich zu dokumentieren. In weiterer Folge sollen auch Werkzeuge bzw. Programme, die ein Beseitigen dieser Spuren versprechen, getestet werden: Wie effizient und gründlich diese wirklich arbeiten. Ein anschließender Vergleich zwischen den Programmen soll eine fundierte Entscheidungshilfe bringen.

1.2 Aufgabenstellung

(353.000) PR: Praktikum aus Netzwerke und Sicherheit [INMNPPRNESI]
Betreuung: Assoz.Prof. Priv.-Doz. Mag. Dipl.-Ing. Dr. Michael Sonntag
Institut für Informationsverarbeitung und Mikroprozessortechnik
Johannes Kepler Universität Linz

Thema

Forensische Analyse von Web-Browsern, deren Spuren und Werkzeugen zur Spurenlöscung

Arbeitsplattform: Oracle VM VirtualBox 4.2.6

Betriebssystem: Microsoft Windows XP Professional

Browser: Mozilla Firefox 17.0, Google Chrome 23, Internet Explorer 8, Opera 12.11

Untersuchungsobjekte: Verlauf bzw. Chronik, Zertifikate, Cookies, eingegebene Adressen, Konfigurationseinstellungen, Auslagerungsdatei

Löschwerkzeuge: CCleaner, ClearProg, One-Click-Privacy, TraXEx, Wipe

Vorgehensweise: Es soll mit Hilfe von datei- bzw. sektorweiser Analyse der virtuellen Festplatten versucht werden, die Veränderungen zu dokumentieren, welche beim Surfen im Internet am Computer bzw. in der virtuellen Maschine entstehen. Darauf aufbauend sollen die oben genannten Werkzeuge zur Spurenlöschung für jeden Browser separat eingesetzt und überprüft werden, wie effektiv und gründlich die ausgewählten Werkzeuge zur Löschung bzw. Verschleierung der entstandenen Veränderungen arbeiten. Dies soll jeweils für jeden Browser und für jedes Werkzeug untersucht werden, woraus sich aus vier Browsern und fünf Werkzeugen insgesamt 20 Szenarien ergeben.

2 Arbeitsumgebung

2.1 Oracle VM VirtualBox

Hierbei handelt es sich um eine mehrere Plattformen unterstützende Virtualisierungsapplikation [VMW]. Sie läuft auf Windows, Mac, Linux und Solaris. Als virtuelle Maschinen ausführbar sind 32- und 64-Bit Systeme. Die von Oracle genannten möglichen Szenarien, für die die Anwendung von virtuellen Maschinen nützlich sind, sind wie folgt:

- **Gleichzeitiges Ausführen mehrerer Betriebssysteme.** Der größte Vorteil liegt wohl in der gleichzeitigen Anwendung mehrerer Betriebssysteme. Zum einen ermöglicht es das Ausführen von Software, die beispielsweise nur für ein bestimmtes Betriebssystem entwickelt wurde, ohne neu starten zu müssen, zum anderen hat man die Möglichkeit der Konfiguration von virtueller Hardware (wenn man beispielsweise das Betriebssystem MS-DOS ausführen möchte, wird spezielle Hardware verlangt, welche von heutigen Betriebssystemen nicht mehr unterstützt wird).
- **Einfachere Installation von Software.** Wird häufig bei der Anwendung von großen Softwarepaketen und deren (meist komplexen) Konfigurationsmöglichkeiten verwendet.
- **Testen und Wiederherstellen von Systemzuständen.** Wurde eine virtuelle Maschine installiert, so befinden sich alle Festplattendaten in einer großen Containerdatei. Diese Containerdateien können eingefroren, wieder aktiviert, gesichert, kopiert und zwischen verschiedenen Hostsystemen ausgetauscht werden. Weiters ist eine inkrementelle Veränderungsdokumentation mittels so genannten "Snapshots" möglich. Dies hat den Vorteil, dass man beispielsweise auch mal mit Schadsoftware experimentieren kann.
- **Infrastruktur-Konsolidierung.** Da die meisten Rechner nur einen Bruchteil ihrer tatsächlichen Leistung nutzen, wird mit dem Kauf mehrerer Geräte oftmals Strom, Hardware und Leistung vergeudet. Mit virtuellen Maschinen lassen sich die Ressourcen gezielter nutzen, in dem einfach ein Rechner für mehrere Virtualisierungen verwendet wird.

Weiters wurden die VirtualBox Guest Additions aktiviert, um einen problemlosen Austausch von Daten zwischen der virtuellen Maschine und dem Hostsystem zu ermöglichen. Grund für die Verwendung dieser Erweiterung ist, dass das zu untersuchende System browsing-technisch möglichst unberührt bleiben soll, damit die weiteren Untersuchungsergebnisse nicht verfälscht werden. Das Herunterladen eines Browsers hinterlässt immerhin auch Spuren, was nicht im Sinne der Aufgabenstellung ist. Darum werden die Browser-Installationsfiles auf dem Host-Rechner heruntergeladen und dem Gastsystem (Image A) zur Verfügung gestellt.

Festplattenformate In den neueren Versionen von VirtualBox werden die folgenden Festplattenformate unterstützt:

- **Virtual Disk Image (VDI)** ist das eigene Containerformat von VirtualBox, welches standardmäßig verwendet wird.
- **VM Ware Virtual Disk File (VMDK)** wird von VirtualBox vollständig unterstützt.
- **Microsoft Virtual Hard Disk (VHD)** wurde ursprünglich für Virtual PC und Virtual Server entwickelt und wird heute neben den meisten Virtualisierungsprogrammen auch von Betriebssystemen wie Windows 7 und Windows Server 2008 unterstützt.
- **Parallels Format 2 HDD** wird in alten Ausführungen ebenfalls unterstützt, es ist allerdings möglich, die neueren Formate in Version 3 und 4 mit Programmen, welche von Parallels angeboten werden, in Version 2 zu konvertieren.
- **QEMU enhanced disk (QED)** bietet etwas weniger Funktionalitäten wie QCOW, ermöglicht aber einen schnelleren Zugriff und sorgt für bessere Datenintegrität. [Qem13]
- **QEMU Copy-on-Write (QCOW)** ist das klassische QEMU Festplattenformat - damit erzeugte Festplatten sind immer dynamisch in der Größe.

Da das VHD und VDI Format auch von Programmen wie dem Komprimierungsprogramm 7-Zip gelesen werden können und sich somit weitere Analysemöglichkeiten ergeben, werden diese Formate verwendet.

Weiters kann beim Anlegen einer neuen virtuellen Maschine noch zwischen einer dynamisch allozierten Festplatte oder einer mit fester Größe gewählt werden. Generell wird eine Festplatte mit dynamischer Allokation empfohlen, da diese auch im Nachhinein leichter modifziert werden kann. Hierfür gibt es im VirtualBox Konsolenmanager "VBoxManage" den Befehl "modifyHD", der hier nicht weiter behandelt wird.

2.2 Microsoft Windows XP Professional (x86)

Das gewählte Betriebssystem wurde von Microsoft 2001 veröffentlicht. Zu den großen Neuerungen gegenüber Windows 98 und Windows 2000 gehörten ein Ausbau der Funktionalität des Startmenüs, ein verbesserter Windows-Explorer, die Möglichkeit, ältere Applikationen mittels Kompatibilitätsemulation auszuführen und die Verfügbarkeit des NTFS (New Technology File System) Dateisystems ausserhalb von Windows 2000. Eine weitere große Neuerung war die Einführung der Systemwiederherstellung. Die letzte Aktualisierung erfolgte mit der Veröffentlichung des Service Packs 3 im April 2008, dessen Supportende mit April 2014 angekündigt ist. [Win12]

In der virtuellen Umgebung wurden die nötigsten Updates ausgeführt und für zusätzliche Sicherheit sorgt das microsofteigene Virenschutzprogramm "Microsoft Security Essentials".

2.3 Verwendete Browser

Die Wahl der benutzten Browser wurde aufgrund der Häufigkeit ihrer Nutzung und ihrer Bekanntheit getroffen: Microsoft Internet Explorer als integrierter Bestandteil von Microsoft Windows, Mozilla Firefox als stärkste Alternative, Google Chrome als zweitstärkste Alternative und Opera. Die aktuellen Marktanteile der genutzten Browser lassen sich unter [Bro12] einsehen (Stand: 19.12.2012). In Abbildung 1 sind die Logos der verwendeten Browser abgebildet.

- **Firefox** 42.0%
- **Internet Explorer** 24.0%
- **Chrome** 12.6%
- **Mobile Safari** 7,7%
- **Safari** 6,0%
- **Android Browser** 4,5%
- **Opera** 2.2%

Abbildung 1: Logos der verwendeten Browser

2.3.1 Mozilla Firefox 17

Dieses Programm wird seit 2002 als freier Webbrowser angeboten. Da er eine breite Palette an persönlich anpassbaren Features und Erweiterungen bereitstellt, hat er sich allmählich gegen den stark verbreiteten Internet Explorer durchgesetzt. Ursprünglich sollte das Produkt Webbrowser, Emailverwaltung, Adressbuch und HTML-Editor in einem anbieten, die einzelnen Funktionen wurden aber nach der Übernahme 2004 als eigene Komponenten veröffentlicht. Aktuell ist der

Browser in der Version 17.0 verfügbar (Stand: 20.11.2012). Zu den erweiterten Konfigurationseinstellungen von Firefox gelangt man, wenn man in der Linkleiste "about:config" aufruft. [Fir13]

2.3.2 Google Chrome 23

Dieser Browser wurde von Google entwickelt und ist seit Ende 2008 verfügbar. Er ist hauptsächlich integraler Bestandteil des Betriebssystems Google Chrome OS, einem Betriebssystem das speziell für NetBooks entwickelt wurde. [Wik12] Die aktuelle Version ist 23 (Stand: 06.11.2012). Eine Liste von internen Chrome-URLs, was in etwa den erweiterten Konfigurationseinstellungen bei den anderen Browsern entspricht, erhält man, wenn man in der Linkleiste "chrome://about" aufruft.

2.3.3 Microsoft Internet Explorer 8

Der Internet Explorer ist seit dem Betriebssystem Windows 95 ein fixer Bestandteil aller darauf folgenden Betriebssysteme, die von Microsoft entwickelt wurden. Version 8 ist die letzte Version, die für Windows XP verfügbar ist. Version 9 wird von Windows Vista ab Service Pack 2, Windows 7 und den Windows Server Editionen 2008, 2008 R2 und 2012 unterstützt. Dieser Browser unterstützt keine Manipulation der erweiterten Konfigurationseinstellungen über eine Inhaltsseite selbst - man muss alle Einstellungen über die Optionen vornehmen. [IE809]

2.3.4 Opera 12.11

Dieser Browser ist seit 1994 verfügbar, aber erst seit 2000 kostenlos, allerdings mit integrierter Werbung. Seit 2005 ist der Browser komplett kostenlos und werbefrei. Wie ursprünglich der Mozilla Firefox, besteht Opera aus drei Komponenten: dem Browser selbst, einem e-Mail- und RSS-Reader-Programm, genannt Opera-Mail, und den Entwicklerwerkzeugen, genannt Dragonfly. [Wik12] Aktuell ist dieser Browser in der Version 12.11 verfügbar (Stand: 20.11.2012). Zu den erweiterten Konfigurationseinstellungen von Opera gelangt man, wenn man in der Linkleiste "opera:config" aufruft. [Ope13]

2.4 Werkzeuge zum Löschen von Spuren

Auf den nun folgenden Seiten werden die ausgewählten Löschwerkzeuge für diesen Versuch kurz vorgestellt, Bezugs- und Versionsinformationen bereitgestellt und ihre eigenen Angaben, welche Bereiche gelöscht werden (sollen), aufgelistet. Der Vergleich der Arbeitsweise bzw. Zuverlässigkeit der einzelnen Werkzeuge erfolgt nach der Versuchsdurchführung in Kapitel 6, dem Vergleich der Löschwerkzeuge und der Interpretation.

2.4.1 CCleaner

Freeware von der Firma Piriform, kostenpflichtige Erweiterungsmöglichkeiten verfügbar. Löscht nach eigenen Angaben alle Bereiche des Computers, welche auf Nutzerverhalten schließen lassen, inkl. aller Browser-Spuren und aller Spuren in der Registrierung. Das kostenlose Programm ist erhältlich unter[1]. Beim Versuch werden natürlich nur die relevanten Bereiche zum Löschen ausgewählt, also der jeweils benutzte Browser. In Abbildung 2 ist die Oberfläche des Programmes abgebildet. Interessant ist die Aufteilung bzw. Zuordnung der Browser: der Internet-Explorer findet sich in der Kategorie "Windows", alle anderen Browser in der Kategorie "Anwendungen".

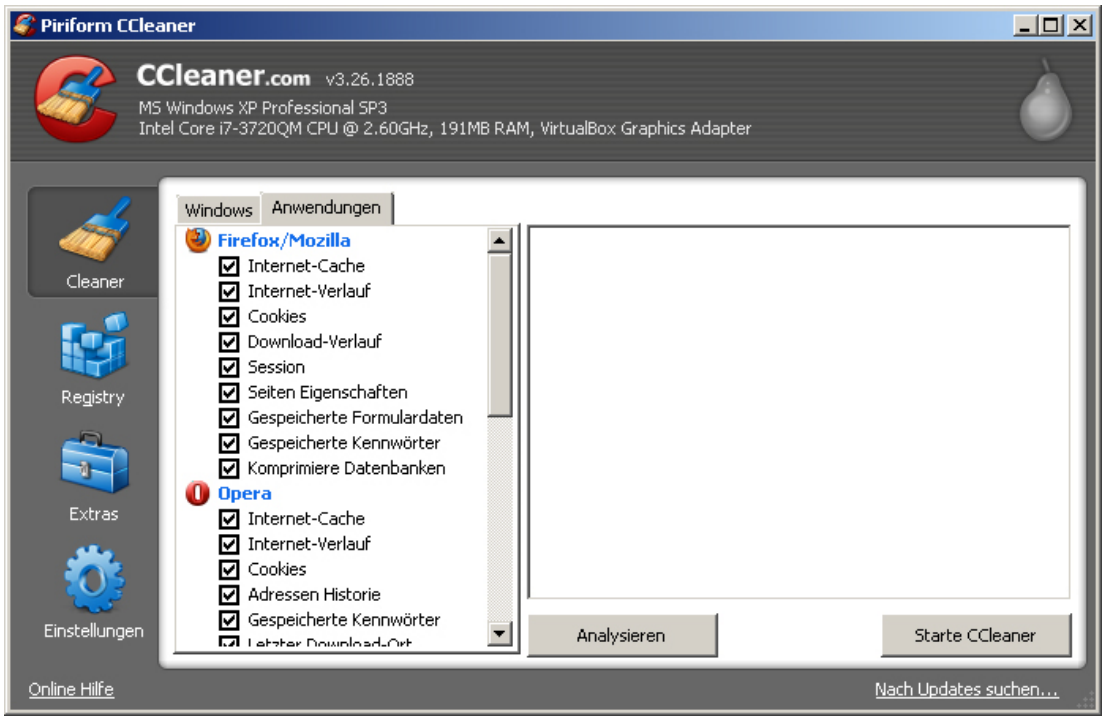

Abbildung 2: Piriform CCleaner, Version 3.26.1888

[1] `http://www.piriform.com/ccleaner`

2.4.2 ClearProg

Dieses Programm, ebenfalls Freeware, wird von SHTools angeboten und gilt als gute Alternative für den CCleaner. Laut Hersteller werden folgende Daten entfernt: Cookies, Verlauf, Cache, eingegebene Adressen und Autovervollständigung. Es können weitere Optionen, welche Spuren der Benutzung des Betriebssystems ebenfalls entfernen, angegeben werden. Lt. Herstellerangabe werden Internet Explorer, Netscape, Firefox und Opera unterstützt, Google Chrome aber nicht[2]. In Abbildung 3 ist die Oberfläche des Programmes abgebildet.

Abbildung 3: ClearProg, Version 1.6.0 Final

2.4.3 One-Click-Privacy

Hier handelt es sich um eine Testversion, die 30 Tage lang mit eingeschränktem Funktionsumfang von der Firma LAB1.de (jetzt "Tools & More") zur Verfügung gestellt wird, wobei das genannte Programm nicht mehr im Produktangebot des Unternehmens aufgelistet ist. Laut Hersteller soll es mit diesem Programm ganz einfach möglich sein (eben nur mit einem Klick), alle Spuren zu entfernen. Aufgelistet sind ua. zuletzt geöffnete Dokumente, zuletzt abgespielte Multimediadateien und bei Browsern Cache, AutoVervollständigung, Cookies und History[3]. Tatsächlich interessant

[2] `http://www.shtools.de/downloads.php`
[3] `http://www.pcwelt.de/downloads/One-Click-Privacy-558089.html`

sind hier die Auswahlmöglichkeiten, die sich auf Internet Explorer und Netscape beziehen. Firefox und Chrome werden nicht unterstützt. Ebensowenig gibt es eine Auswahl für Opera. In Abbildung 4 ist die Oberfläche des Programmes abgebildet.

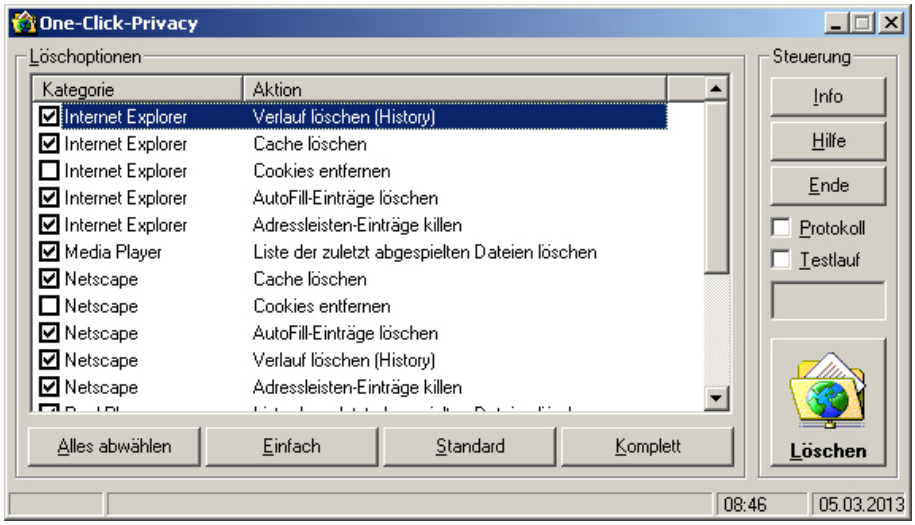

Abbildung 4: One-Click-Privacy, Version 1.5.3

2.4.4 TraXEx

Der von Almisoft angebotene TraXEx Spurenverwischer verspricht Ähnliches wie die oben genannten Programme und wurde bei einer Computerbild-Testreihe in den Jahren 2009 und 2010 Testsieger[4]. Wird das Programm gestartet, nachdem ein neuer Browser installiert wurde, so wird diese Installation automatisch erkannt und der Browser zur Liste der Auswahlmöglichkeiten der Löschoptionen hinzugefügt. Jeder Browser kann in der Liste erweitert werden und die genauen Angaben, welche Inhalte gelöscht werden, sind ersichtlich. In Abbildung 5 ist die Oberfläche des Programmes abgebildet.

2.4.5 Wipe

Diese Freeware ist von privacyroot und löscht System- und Internetspuren wie Cookies, History, Internetcache und automatisches Vervollständigen[5]. Ähnlich wie bei TraXEx hat man hier wieder die Möglichkeit, die gewünschten Spuren einzeln auszuwählen. In Abbildung 7 ist die Oberfläche des Programmes abgebildet.

[4] `http://www.almisoft.de/?cont=download`
[5] `http://www.chip.de/downloads/Wipe_38236462.html`

Abbildung 5: TraXEx, Version 3.3.5.0.7.5

2.5 Unterstützung beim Vergleich

7-Zip & QEMU Da die generierten Festplattenimages auch verglichen werden müssen, sind weitere Schritte notwendig: neben einer "händischen Dateianalyse" mit dem Programm 7-Zip ist eine genaue Analyse der Festplatte notwendig. Hierzu wird vom Programm QEMU Version 1.0.1 [Qem13] der Befehl "qemu-img convert" verwendet, der die Festplattendateien in reine Datendateien (RAW Dateien) umwandelt.

Diese RAW Dateien lassen sich dann sektorweise vergleichen und bei Unterscheidungen können dann die genauen Stellen festgestellt werden, an denen sich Daten befinden. Details dazu aber in den Kapiteln 4 und 5.

Abbildung 6: Logo QEMU

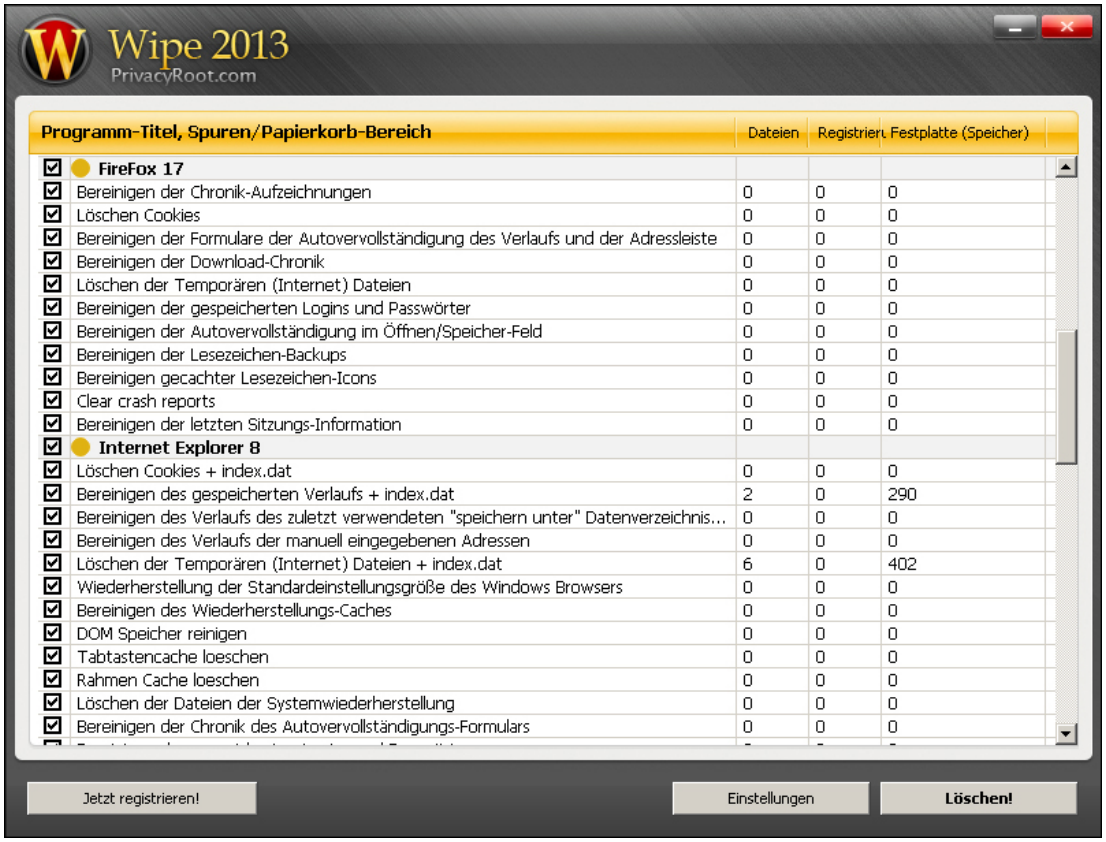

Abbildung 7: Wipe 2013, Version 13.01

X-Ways Forensics Um eine genauere Zuordnung der gefundenen Daten bzw. Datenfragmente möglich zu machen, wird das Programm "X-Ways Forensics 16.8" der Firma "X-Ways Software Technology AG"[6] für ein Szenario verwendet, da man mit diesem Programm die genaue Zugehörigkeit von Inhalten und Dateien herausfinden kann.

[6] http://www.x-ways.net/

3 Untersuchungsobjekte

Im Folgenden werden Informationen darüber gegeben, welche Untersuchungsobjekte bzw. relevanten Bereiche auf dem Rechner in welcher Form und an welchem Ort gespeichert werden. Es wird dabei auch auf browserspezifische Vorgehensweisen des Speicherns eingegangen, soweit die Recherchen brauchbare Ergebnisse geliefert haben.

3.1 Verlauf

Andere Bezeichnungen für den Verlauf eines Browsers können auch Chronik, Geschichte oder History sein. Mit dem Verlauf geht meist auch die Speicherung eines Browsercache mit einher. Unter dem Verlauf eines Webbrowsers versteht man im Wesentlichen die Speicherung der vom Benutzer besuchten Webseiten. Neben der besuchten Adresse werden meist auch Inhalte wie Bilder lokal am Rechner abgelegt (gecached). Diese Daten ermöglichen zum einen das Nachverfolgen besuchter Seiten, zum anderen kann damit die Surfgeschwindigkeit im Internet erhöht werden, da bereits vorhandene Daten nicht ein weiteres Mal geladen werden müssen sondern aus dem Cache geholt werden. Der Verlauf wird meist von jedem Browser unterschiedlich gesichert:

- **Firefox:** Der Verlauf ist im lokal abgelegten Profilordner unter C:\Dokumente und Einstellungen\USER\Anwendungsdaten\Mozilla\Firefox\Profiles\PROFIL.default gespeichert.

  Firefox ermöglicht das User-basierte Löschen des Verlaufs in den Einstellungen unter der Rubrik Datenschutz. Hier kann man die kürzlich angelegte Chronik oder einzelne Cookies löschen. Beim Löschen der Chronik kann man den Zeitraum auswählen und einstellen, welche Daten gelöscht werden sollen (Besuchte Seiten und Download Chronik, eingegebene Suchbegriffe und Formulardaten, Cookies, Cache, Aktive Logins, Offline Webseiten Daten und Webseiten Einstellungen).

- **Chrome:** Die Verlaufsdaten werden ebenfalls lokal unter C:\Dokumente und Einstellungen\USER\Lokale Einstellungen\Anwendungsdaten\Google\Chrome\User Data\Default abgespeichert.

  Chrome unterstützt eine In-Browser-Funktion mit dem Namen "Browserdaten löschen", wo neben der Auswahl des Zeitraumes, für den die Daten gelöscht werden sollen (von der letzten Stunde bis gesamter Zeitraum), auch ausgewählt werden kann, welche weiteren Browserdaten gelöscht werden sollen (Browserverlauf, Downloadverlauf, Cache, Cookies und andere Website- und Plug-in-Daten, gespeicherte Passwörter, gespeicherte AutoFill-Formulardaten, Daten aus gehosteten Anwendungen und die Autorisierung von Inhaltslizenzen).

- **Internet Explorer:** IE8 speichert den Verlauf ebenfalls lokal unter C:\Dokumente und Einstellungen\USER\Lokale Einstellungen\. Hier gibt es die Ordner Temporary Internet Files (für gecachte Inhalte) und Verlauf.

  Beim Anwenden der Erweiterung "Browserverlauf löschen" werden beim Internet Explorer alle Daten im Verlauf gelöscht, ausgenommen der gespeicherten Favoritenseiten und man kann im erscheinenden Dialogfeld auch angeben, dass der Verlauf von häufig besuchten Webseiten beibehalten werden sollen. Weitere Auswahlmöglichkeiten zum Löschen hat man von Temporären Internetdateien, Cookies, Verlauf, Formulardaten, Kennwörtern und InPrivate-Filterungsdaten, was dem Privaten-Surf-Modus vom IE entspricht.

- **Opera:** Den Verlauf von Opera findet man in einer History-Datei unter C:\Dokumente und Einstellungen\USER\Anwendungsdaten\Opera\Opera\global_history.dat

  Hier gibt es für den User die Möglichkeit, die erzeugten Spuren selbst zu löschen, in dem man unter den Opera-Einstellungen die Option "Internetspuren löschen" auswählt. Man kommt ebenfalls zu einer Auswahl von Inhalten, die gelöscht werden sollen (Sitzungs-Cookies, alle Cookies (wobei man hier die Cookies einzeln verwalten kann), Logins für passwortgeschützte Seiten, Cache, Plug-in-Daten, Geolocation-Daten, Kamera-Berechtigungen, Verlaufsliste der aufgerufenen Webseiten, Downloads, Favouriten Icons und Zeitpunkt der Lesezeichen Aufrufe, Passwörter von E-Mail Konten, Passwörter im Passwortmanager (hier können auch die Passwörter einzeln verwaltet werden), dauerhaften Speicherplatz und das Beenden aller aktuell geöffneten Tabs).

3.2 Zertifikate

Unter einem Zertifikat versteht man einen Datensatz, der die Zugehörigkeit einer Person, eines Unternehmens oder eines Objektes zu einem Schlüssel auf digitalem Wege überprüfen kann. Am verbreitetsten sind Zertifikate, die nach dem Public-Key-Verfahren die Integrität eines Zertifikatinhabers verifizieren. Die behandelten Browser speichern die bei ihnen aufgerufenen, bzw. installierten Zertifikate in den lokalen Profilordnern, meist in der Nähe des Verlaufs. Lediglich der Internet Explorer legt die Zertifikate in einem allgemeinen Ordner ab.

- **Firefox:** Die Zertifikate werden auch im lokalen Profil unter C:\Dokumente und Einstellungen\USER\Anwendungsdaten\Mozilla\Firefox\Profiles\PROFIL.default in der Datei "cert8.db" abgelegt.

- **Chrome:** Google Chrome verwendet den Zertifikatsspeicher von Microsoft bzw. den des Internet Explorers, diese liegen also im selben Verzeichnis.

- **Internet Explorer:** Die Zertifikate werden unter C:\Dokumente und Einstellungen\All

Users\Anwendungsdaten\Microsoft\Crypto\RSA\MachineKeys bzw. \DSS\MachineKeys gesichert.

- **Opera:** Die Zertifikate werden lokal abgelegt im Verzeichnis C:\Dokumente und Einstellungen\USER\Anwendungsdaten\Opera\Opera. Hier gibt es die Dateien opcacrt6.dat für bekannte Zeritifizierungsstellen, opcert6.dat für eigene Zertifikate und opicacrt6.dat für Zwischenzertifikate der Zertifizierungsstellen.

3.3 Cookies

Als Cookies bezeichnet man auf dem lokalen Rechner gespeicherte kurze Textdateien, welche Daten über die besuchten Webseiten enthalten. Beim Internetsurfen werden eigentlich nur HTTP- und Flash-Cookies gespeichert. Sinn von Cookies ist das (zeitlich beschränkte) Archivieren von Daten bzw. Informationen über den letzten Besuch auf einer Seite. Beispielsweise wird auf einem Rechner lokal gespeichert, wann und ob sich ein Benutzer auf einer (verschlüsselten) Seite das letzte Mal eingeloggt hat. Wird die Seite ein weiteres Mal aufgerufen, wird der Benutzer automatisch eingeloggt. Das Cookie hat dem lokalen Rechner bzw. Webbrowser also mitgeteilt, dass die Logindaten vom letzten Login wiederverwendet werden sollen, damit der Benutzer sich nicht noch einmal einloggen muss. Cookies werden wie folgt browserspezifisch abgelegt:

- **Firefox:** Cookies werden im lokalen Benutzerverzeichnis unter C:\Dokumente und Einstellungen\USER\Anwendungsdaten\Mozilla\Firefox\Profiles\PROFILE.default in der Datei cookies.sqlite abgelegt.
- **Chrome:** Die lokal abgelegten Cookies von Chrome findet man unter C:\Dokumente und Einstellungen\USER\Lokale Einstellungen\Anwendungsdaten\Google\Chrome\User Data.
- **Internet Explorer:** Der Internet Explorer handhabt die Ablage von Cookies etwas einfacher bzw. in einem weniger tief verschachtelten Verzeichnis und weniger schwer auffindbar unter C:\Dokumente und Einstellungen\USER\Cookies.
- **Opera:** Hier werden Cookies ebenfalls im Profilverzeichnis unter C:\Dokumente und Einstellungen\USER\Anwendungsdaten\Opera\cookies4.dat abgelegt.

Speicherung bzw. Pfadangaben in der Registrierung findet man in Bezug auf das Benutzerprofil unter HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User-Shell Folders\Cookies sowie mit absoluter Pfadangabe unter HKEY_CURRENT_USER\Software \Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies.

3.4 Eingegebene Adressen

Unter eingegebenen Adressen (typed URLs) versteht man jene Daten bzw. Adressen, welche der Nutzer in der Adresszeile seines Browsers manuell eingegeben hat. Diese Adressen erleichtern einem Nutzer das Navigieren im Webbrowser, da er Adressen, welche er schon einmal besucht hat, nicht mehr vollständig eingeben muss, da ihm bereits nach der Eingabe der Anfangsbuchstaben der Adresse der gesamte Link vorgeschlagen wird. Diese Informationen zur Auto-Vervollständigung werden sowohl von den typed URLs als auch von der History und dem Cache herangezogen.

Beispiel: Ist ein Nutzer oft auf der Seite des KUSSS Systems (`http://www.kusss.jku.at`), so wird diese Adresse unter den typedURLs abgespeichert und dafür genutzt, dass der Nutzer, sobald er die Buchstaben "ku" in der Adresszeile eingibt, die gesamte URL vorgeschlagen bekommt und diese nur noch auswählen muss, anstatt sie selbst komplett eintippen zu müssen.

- **Firefox:** Die Liste der eingegebenen Adressen wird bei Firefox ebenfalls im lokalen Profil unter C:\Dokumente und Einstellungen\USER\Anwendungsdaten\Mozilla\Firefox\Profiles\PROFILE.default in der Datei formhistory.sqlite gespeichert.
- **Chrome:** Bei Chrome ebenfalls im lokalen Profilverzeichnis unter C:\Dokumente und Einstellungen\USER\Lokale Einstellungen\Anwendungsdaten\Google\Chrome\User Data abgelegt.
- **Internet Explorer:** Es werden die letzten 10 eingegebenen Adressen in der Registrierung unter dem Schlüssel HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs sowie für jeden User bzw. jede User-ID separat unter HKEY_USERS\[User-ID]\Software\Microsoft\Internet Explorer\TypedURLs hinterlegt.
- **Opera:** Ebenfalls im Opera-Verzeichnis zu finden unter C:\Dokumente und Einstellungen\USER\Anwendungsdaten\Opera\Opera\typed_history.xml bzw. places.sqlite.

3.5 Konfigurationseinstellungen

Bei den verwendeten Browsern gibt es keine dedizierten Hinweise darauf, wo die getätigten Konfigurationseinstellungen des jeweiligen Browsers tatsächlich abgelegt werden. Auch die Speicherform der Einstellungen bleibt verborgen, es wird aber eine XML-ähnliche Form vermutet. Grund dafür sind vermutlich Sicherheitsbedenken, da das Offenlegen der programminternen Einstellungen durchaus die Möglichkeit bieten würde, sensible Konfigurationen zu manipulieren und evtl. sogar zur Schaffung von Sicherheitslücken beitragen kann. Es wird vermutet, dass die Konfigurationseinstellungen der einzelnen Browser jeweils lokal im oder "in der Nähe" der Profildateien

abgelegt werden, da dies der Organisation und Zusammengehörigkeit der Daten dienen würde. Firefox speichert seine Konfigurationen beispielsweise in einer SQLite Datenbank ab.

3.6 Auslagerungsdatei

Die Auslagerungsdatei von Windows XP stellt eine Erweiterung des physischen Hauptspeichers dar. Diese Datei enthält ausgelagerte Seiten des Arbeitsspeichers, welche unter Umständen sehr lange gespeichert bleiben. Da beim Herunterfahren des Systems die Auslagerungsdatei in der Regel nicht gelöscht wird, braucht man, wenn man die Datei nachträglich untersuchen möchte, das System nicht einfach vom Netz nehmen, sondern kann diese direkt von der Festplatte heraus untersuchen. Es gibt eine Registry-Einstellung, mit der bewirkt wird, dass die Auslagerungsdatei beim Systemherunterfahren durchgehend mit ”0” überschrieben wird, diese Einstellung ist jedoch bei den meisten Rechnern bzw. Installationen nicht eingestellt. Eine Möglichkeit in diesem Zusammenhang wäre noch, das System in Ruhezustand zu schicken, da hier der gesamte Inhalt des Hauptspeichers in das ”Hibernation-File” geschrieben wird. Da aber für dieses Projekt nur die Auslagerungsdatei von Bedeutung ist, wird auf die Untersuchung des ”Hibernation-Files” nicht näher eingegangen. [Son09]

4 Ablauf

Vorbereitungen:

- Formatieren der Festplatte mit dem NTFS Dateisystem, laut Windows-Installation. Installieren bzw. Aufsetzen des Testbetriebssystems in der virtuellen Umgebung, samt (aller notwendigen) Betriebssystem-Updates und eines Virenschutzes, wie in den vorherigen Kapiteln beschrieben. Benötigt wird zumindest Service Pack 2, damit der Internet Explorer 8 und weitere Programme installiert werden können. Um die Installationsdateien der Browser und Löschwerkzeuge ohne Internetzugriff auf der Maschine installieren zu können, werden die VirtualBox Guest Additions benötigt, damit "Gemeinsamer Ordner" zwischen Hostbetriebssystem und VM hergestellt werden kann. Weiters muss die Kopie des Betriebssystems aktiviert werden um ein einwandfreies Arbeiten zu gewährleisten. Spezifikation: Windows XP Professional 2002 Service Pack 3, 2 GB Festplattenspeicher, 192 MB Arbeitsspeicher, 128-256 MB Auslagerungsdatei, Computername "PraktikumNWS".
- Installation der ausgewählten Browser und Werkzeuge - es ist wichtig, dass die Programme vor der eigentlichen Versuchsdurchführung installiert werden, da eine Installation direkt vor dem Vergleich der Festplattendateien nur noch mehr Veränderungen verursachen würde, was zum einen die Versuchsdurchführung verkomplizieren und zum anderen die Ergebnisse verfälschen würde. Es entsteht eine Grundinstallation, im Folgenden bezeichnet als Ausgangs-Image "A".

Ablauf:

- Bestimmen bzw. Festlegen einer genauen Vorschrift, welche Seiten und Inhalte im Internet besucht werden sollen, damit bei der darauf folgenden Untersuchung auch genau nachvollzogen werden kann, welche Veränderungen im System welchen Inhalten zuzuordnen sind. Als zu besuchende Seiten wurden die folgenden ausgewählt:
  - `www.gmx.at` (Global Mail Exchange): viel besuchte und sehr bekannte Seite, Möglichkeit zur Anlegung von gratis Mailaccounts.
  - `www.informatiker.at.tf` (inoffizielles Forum für Studierende der Informatik an der JKU Linz): bei dieser Seite muss vom User bestätigt werden, dass ein Zertifikat installiert wird um die Seite besuchen zu können, weiters besteht eine Loginmöglichkeit, bei der auch Cookies gespeichert werden. Es muss zuerst `https://davinci.khg.jku.at/users/gue/main.php` aufgerufen werden, wo die Möglichkeit besteht, eine Sicherheits-Ausnahmeregel hinzuzufügen, bzw. das Zertifikat herunterzuladen. Erst danach lässt sich die Seite mittels Direct-Link besuchen. Auf dieser Seite wird ein Login getätigt, mit aktivierten Cookies und anschließendem Speichern des Passworts.

- Nun werden die unterschiedlichen Festplattenimages erzeugt, also jeweils ein Image für einen Browser, mit dem laut oben angegebener Vorschrift gesurft wurde. Es entstehen vier Images welche die Veränderungen, jeweils für jeden Browser, beinhalten, im Folgenden bezeichnet als die "Browser-Images" FF (Firefox), IE (Internet Explorer), GC (Google Chrome) und OP (Opera).
- Die einzelnen erzeugten Images werden mit Hilfe des Programmes "QEMU Disk Images Utility" in binäre Datendateien umgewandelt damit, der spätere sektorweise Vergleich der Festplattendateien ermöglicht wird.
- Vergleich des Ausgangsimages mit jeweils einem Browser-Image, damit gezeigt wird, in welchen Sektoren Daten über den Surf-Vorgang zu finden sind.
- Für jedes der im letzten Schritt erzeugten Browser-Images werden die Löschprogramme eingesetzt. Jeweils alle fünf Löschwerkzeuge einzeln für jeden Browser, woraus aus jedem Browser-Image fünf zu untersuchende bzw. zu vergleichende "Compare-Images" entstehen. Diese Images werden wie folgt bezeichnet:
  - Ausgehend aus dem Image FF (Firefox) entstehen die Images FF-CC (CCleaner), FF-CP (ClearProg), FF-OC (One-Click-Privacy), FF-TX (TraXEx) und FF-WI (Wipe).
  - Ausgehend aus dem Image IE (Internet Explorer) entstehen die Images IE-CC (CCleaner), IE-CP (ClearProg), IE-OC (One-Click-Privacy), IE-TX (TraXEx) und IE-WI (Wipe).
  - Ausgehend aus dem Image GC (Google Chrome) entstehen die Images GC-CC (CCleaner), GC-CP (ClearProg), GC-OC (One-Click-Privacy), GC-TX (TraXEx) und GC-WI (Wipe).
  - Ausgehend aus dem Image OP (Opera) entstehen die Images OP-CC (CCleaner), OP-CP (ClearProg), OP-OC (One-Click-Privacy), OP-TX (TraXEx) und OP-WI (Wipe).
- Auswertung der Compare-Images, also genaue Analyse der Festplattenimages, ob noch die Werte "a4g", "gmx", "jag" "jku" oder "khg" zu finden sind. "a4g" ist ein Teil des Login-Passwortes, "jag" ein Teil des Login-Benutzernamens des Forums. "gmx" bezieht sich natürlich auf die besuchte GMX-Seite, "khg" und "jku" sind Teile der besuchten Foren-Seite. Der Textbereich "ike", welcher von www.informatiker.at herausgenommen wurde ist offensichtlich ein Text, der auch bei anderen Betriebssystemsektoren vorkommt, weshalb die hohe Anzahl an Vorkommnissen nicht repräsentativ ist. Dieser String wurde bei der ersten fehlerhaften Firefox-Versuchsreihe verwendet.
- Gegenüberstellung der Ergebnisse und Vergleich der Zuverlässigkeit der Löschwerkzeuge.

In Abbildung 8 ist der Ablauf schematisch dargestellt.

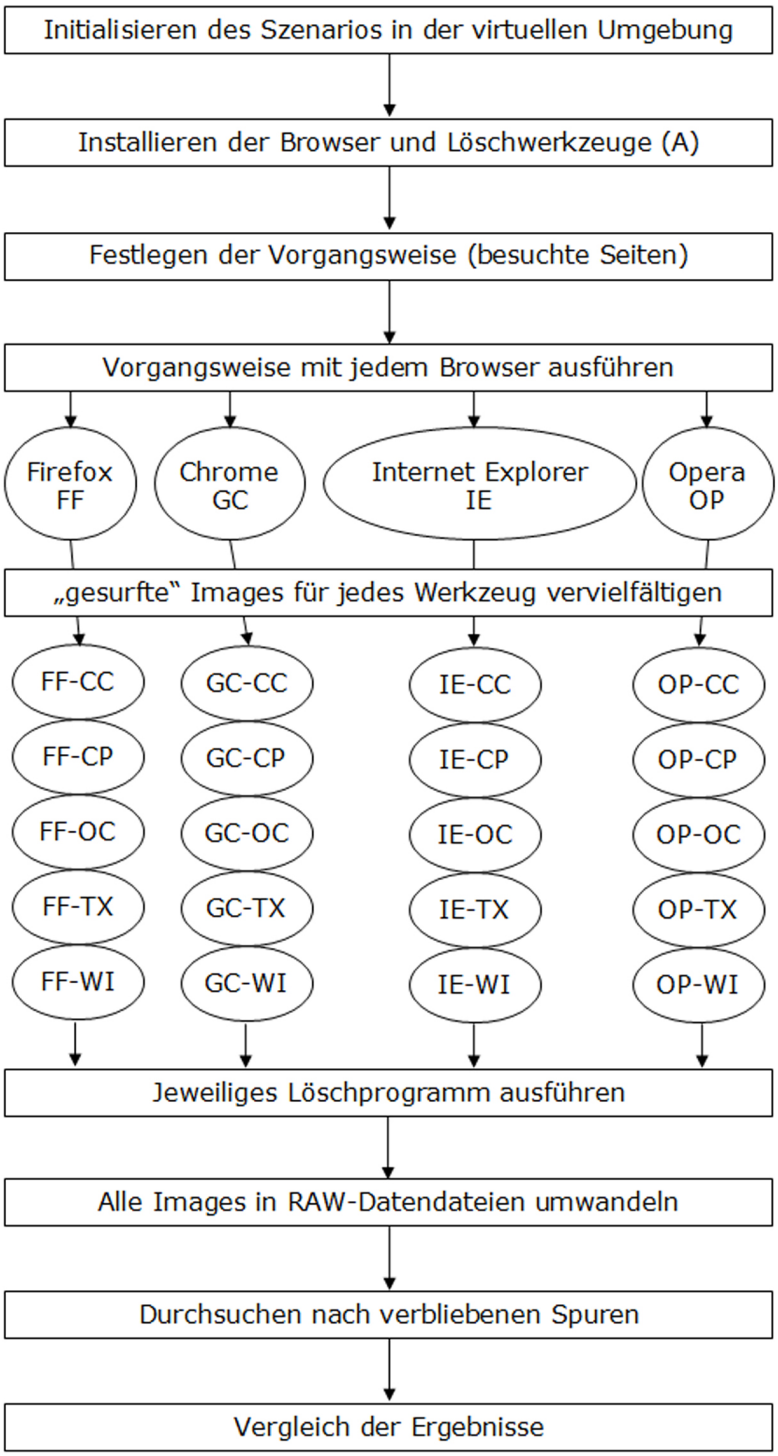

Abbildung 8: Ablauf

5 Versuchsdurchführung

5.1 Vorinformationen

Präambel: Es wurden alle Versuchsreihen durchgeführt, allerdings kam es zu einer Verfälschung der Ergebnisse. Bei den Automatischen Updates von Microsoft Windows XP wurde die Option "Benachrichtigen, aber nicht herunterladen oder installieren" gewählt, damit keine unnötigen Bewegungen auf der Festplatte zustande kommen. Offensichtlich werden aber dennoch Updates heruntergeladen, da bei deaktivierter Netzwerkverbindung bei Anwendung der Löschprogramme, die danach generierten Vergleichsdateien wesentlich kleiner ausfallen (Tabelle 1). Dieser Umstand fiel bei der Durchführung der Versuchsreihe Opera auf, da hier die Vorgehensweise mit deaktivierter Netzwerkverbindung gewählt wurde. Auch der Unterschied der Images von A und OP war unrealistisch groß, wie aus der Tabelle zu entnehmen ist. Aus diesem Grund wurde die gesamte Versuchsreihe noch einmal durchgeführt, allerdings wird schon beim Image A die Option "Automatische Updates deaktivieren" gewählt (Tabelle 2).

Es wurden drei verschiedene Arten von Vergleichsprogrammen implementiert bzw. verwendet, welche sich auf der CD/DVD im Anhang wiederfinden:

- **compareImages:** Mit dem Vergleichsprogramm wurden jeweils sektorweise (je 512 Byte) zwei Images miteinander verglichen. Sich unterscheidende Sektoren wurden als Text in Textdateien exportiert, wo jeweils die Nummer des betroffenen Sektors sowie der Inhalt des Sektors beider Images ersichtlich ist.
- **searchStrings:** Es werden sektorweise alle Bytes des Images nach den Strings a4g, gmx, jag, jku und khg durchsucht und die Sektornummern, in denen die Strings gefunden werden sowie die Gesamtsumme der Funde in eine Textdatei exportiert.
- **compareSearch:** Eine Mischung aus den ersten beiden Programmen - sich unterscheidende Sektoren werden nach den Strings durchsucht und die Sektornummern der Fundorte sowie die Anzahl der Funde exportiert.

Diese Textdateien können mitunter sehr groß werden, da ja das Betriebssystem unheimlich viele Operationen durchführt, vor allem beim Starten, und unter Umständen auch große Datenbereiche verschoben werden, auch wenn der Inhalt gleich ist. Hier bleibt eine händische Analyse nicht aus, aber aufgrund der genauen "Surf-Vorschrift" (siehe Kapitel 4), ist ja bekannt, wonach gesucht werden muss. Aus diesem Grund wird bei der folgenden Darstellung der Ergebnisse jeweils eine händische Auswertung vorgenommen, basierend auf den in Kapitel 3 recherchierten bekannten Speicherorten.

Situation	Firefox	Chrome	IE	Opera
Gesurft	729 MB	1.580 MB	720 MB	2.130 MB
CCleaner	612 MB	716 MB	1.360 MB	484 MB
Clear-Prog	503 MB	923 MB	833 MB	526 MB
One-Click-Privacy	792 MB	916 MB	1.220 MB	519 MB
TraXEx	826 MB	959 MB	1.100 MB	520 MB
Wipe	873 MB	957 MB	1.000 MB	504 MB

Tabelle 1: Größe der Vergleichsdateien (verfälschte Version)

Die Größe der Textdatei, die nach dem Surfen mit dem jeweiligen Browser, durch den Vergleich mit dem Ausgangsimage entsteht beläuft sich auf ca. 600 - 2.200 MB, was vor allem bei der Nutzung von Opera besonders auffällt, da die Größe des Images selbst nur knapp über 3 GB groß ist. Da besonders große Textdateien betrachtet werden und dies mit den üblichen Programmen "Editor" bzw. "Notepad++" nicht möglich ist, wird der Editor "gVim 7.3" verwendet.

Nach dem Anwenden der Löschwerkzeuge wird nur das neue Image auf verbliebene Spuren untersucht, sowohl händisch als auch mit einer sektorweisen Analyse der Festplattendatei.

Situation	Firefox	Chrome	IE	Opera
Gesurft	536 MB	533 MB	533 MB	532 MB
CCleaner	495 MB	515 MB	452 MB	447 MB
Clear-Prog	492 MB	495 MB	463 MB	426 MB
One-Click-Privacy	517 MB	540 MB	430 MB	466 MB
TraXEx	528 MB	514 MB	518 MB	477 MB
Wipe	509 MB	523 MB	543 MB	463 MB

Tabelle 2: Größe der Vergleichsdateien (korrekte Version)

Betrachtet man die Werte aus Tabelle 2, so sieht man an der Zeile "Gesurft", dass der Unterschied der Datenveränderungen nach dem Surfen bei allen vier Browsern nahezu ident ist. Auch die Größe der Unterscheidungsdateien nach der Anwendung der Löschwerkzeuge bewegt sich in nicht allzu großen Bereichen. Es wurde vor dem Besuchen der ausgewählten Seiten das Ausgangsimage A nach den Schlüsselwörtern durchsucht, das Ergebnis ist in Tabelle 3 abgebildet. Diese Vorab-Suche soll die späteren Suchergebnisse nicht verfälschen, da hier bereits ersichtlich ist, dass die gesuchten Schlüsselwörter in ihren Fragmenten auch schon vor dem Besuchen der ausgewählten Webseiten auf der Festplatte vorhanden sind.

GMX	JKU	KHG	A4G	JAG
90	96	137	231	215

Tabelle 3: Gefundene Schlüsselwörter im Ausgangsimage A

Bei den Versuchsreihen wird bei der abschließenden Gegenüberstellung jeweils die Anzahl der gefundenen Schlüsselwörter vom Ausgangsimage, vom Vergleich Ausgangsimage mit dem gesurften Image, und vom gesurften Image allein noch aufgelistet, um einen übersichtlicheren Vergleich machen zu können.

5.2 Vorabsuche mit X-Ways Forensics

Wie in Kapitel 2.5 bereits beschrieben, kann mit diesem Programm festgestellt werden, in welchen Dateien sich gewisse Objekte und Daten befinden. Es wurde das gesurfte Image FF durchsucht und folgende Ergebnisse ermittelt:

Suche nach dem Passwort: Es wurden auf der gesamten Festplatte keine Klartextdarstellungen gefunden. Die Funde mit dem Textfragment "a4g", welches aus dem Passwort stammt, sind somit in anderen Zusammenhängen auf der Festplatte abgelegt.

Suche nach dem Loginnamen "daJaga": Case-sensitive Übereinstimmung in den folgenden Dateien: C:\Programme\Google\Chrome\Application\25.0.1364.172\Locales\et.pak sowie ...Mozilla\Firefox\Profiles\9k3xqkbi.default\formhistory.sqlite und C:\Programme\Google\Chrome\Application\25.0.1364.172\Installer\chrome.7z. Dieses Suchergebnis ist äußerst seltsam, da der Browser Google Chrome in diesem Szenario lediglich installiert und noch nicht benutzt wurde.

Suche nach "www.gmx.at": C:\Dokumente und Einstellungen\Markus\Anwendungsdaten\Mozilla\Firefox\Profiles\9k3xqkbi.default\places.sqlite, cookies.sqlite und sessionstore.js. Weiters in Bereichen, die früher sessionstore.js und places.sqlite-wal zugeordnet waren, jetzt zwar gelöscht, aber auf der Festplatte noch lesbar sind und einige Male in Sektoren, die mittlerweile als freier Speicherplatz deklariert sind.

Suche nach "davinci.khg.jku.at": C:\Dokumente und Einstellungen\Markus\Lokale Einstellungen\Anwendungsdaten\Mozilla\Firefox\Profiles\9k3xqkbi.default\Cache_CACHE_003_.

Weiters in den bereits bekannten Dateien C:\Dokumente und Einstellungen\Markus\Anwendungsdaten\Mozilla\Firefox\Profiles\9k3xqkbi.default\places.sqlite, sessionstore.js, cert8.db, signons.sqlite und cookies.sqlite. Auch in der Datei C:\$LogFile lässt sich der Link finden. Weiters, wie bereits bei dem vorigen Suchdurchlauf, in Bereichen, die früher sessionstore.js und places.sqlite-wal zugeordnet waren, jetzt zwar gelöscht, aber auf der Festplatte noch lesbar sind und einige Male in Sektoren, die mittlerweile als freier Speicherplatz deklariert sind.

5.3 Versuchsreihe Firefox

Im Folgenden werden die Folgen der Anwendung der Löschwerkzeuge für den Browser Firefox analysiert, am Ende erfolgt eine Gegenüberstellung der Ergebnisse und ein Resümee.

5.3.1 Gesurft

Händische Auswertung

- **Verlauf:** In den Dateien signons.sqlite, cert_override.txt und sessionstore.bak finden sich Verweise auf die eingegebenen URLs in Klartext.
- **Zertifikate:** Im Profilordner finden sich etliche Verweise auf "davinci.khg.jku.at" in der Datei cert8.db - kein Vorkommen von GMX.
- **Cookies:** Im Profilordner in der Datei cookies.sqlite sind Verweise auf die beiden besuchten Seiten zu finden.
- **Eingegebene Adresse:** In formhistory.sqlite finden sich der Loginname und Teile des Passworts unverschlüsselt, Vorkommen der eingegebenen Adressen lassen sich jedoch nicht finden. In places.sqlite findet man die Adressen.

Extrahierte Unterschiede In den extrahierten Unterschieden der Images A und FF wurde nach den Schlüsselwörtern gesucht: 340x "gmx", 131x "jku", 105x "khg", 8x "a4g" und 10x "jag"

Durchsuchung von nur FF ergab folgende Vorkommnisse: 429x "gmx", 221x "jku", 224x "khg", 231x "a4g" und 212x "jag".

5.3.2 CCleaner

Anwendung Es wurden insgesamt 43 Spuren mit einer Gesamtgröße von 3,12 MB vom CCleaner gefunden.

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten, wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** In cookies.sqlite finden sich noch Reste von URLs, die Dateien sessionstore.bak und signons.sqlite wurden gelöscht.

- **Zertifikate:** Die Zertifikatsdatei cert8.db existiert nicht mehr, dafür ist in cert_override.txt noch ein Verweis auf die Zertifikatseite zu finden.
- **Cookies:** In der Datei cookies.sqlite sind noch Verweise auf die eingegebenen Adressen zu finden, aber keine Informationen über GMX.
- **Eingegebene Adresse:** Die Datei formhistory.sqlite wurde entfernt, somit sind keine Verweise mehr zu finden, in places.sqlite gibt es noch URL-Reste.

Extrahierte Unterschiede Im Image FF-CC wurde nach den Schlüsselwörtern gesucht: 454x "gmx", 226x "jku", 227x "khg", 229x "a4g" und 212x "jag".

5.3.3 Clear-Prog

Anwendung Es wurden insgesamt 26 Spuren mit einer Gesamtgröße von 2,34 MB vom Clear-Prog gefunden.

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten, wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** Die Datei signons.sqlite wurde entfernt, in cert_override.txt sind noch Informationen vorhanden.
- **Zertifikate:** cert8.db enthält nachwievor Informationen über die besuchte Seite und über das Zertifikat, keine Informationen über GMX.
- **Cookies:** In cookies.sqlite sind nachwievor alle Informationen zu finden.
- **Eingegebene Adresse:** In formhistory.sqlite finden sich noch immer der Loginname und Teile des Passworts unverschlüsselt. Auch in places.sqlite sind noch Links zu finden.

Extrahierte Unterschiede Im Image FF-CP wurde nach den Schlüsselwörtern gesucht: 321x "gmx", 212x "jku", 220x "khg", 230x "a4g" und 216x "jag".

5.3.4 One-Click-Privacy

Anwendung Es wurden keine Spuren gefunden.

Händische Auswertung Dieses Programm unterstützt das Entfernen von Spuren, welche von Firefox verursacht wurden, nicht. Aus diesem Grund wurden auch die Dateien nicht mehr durchsucht. Das Betriebssystem wurde hochgefahren und das Programm gestartet, weshalb sich evtl. Veränderungen auf der Festplatte ergeben können.

Extrahierte Unterschiede Im Image FF-OC wurde nach den Schlüsselwörtern gesucht: 428x "gmx", 218x "jku", 220x "khg", 230x "a4g" und 213x "jag".

5.3.5 TraXEx

Anwendung Es wurden insgesamt 105 Spuren mit einer Gesamtgröße von 4,28 MB von TraXEx gefunden.

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten, wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** Die Datei signons.sqlite wurde gelöscht. Die Datei cert_override.txt enthält noch Spuren vom Forums-Link, aber nichts von GMX.
- **Zertifikate:** cert8.db enthält nachwievor Informationen über die besuchte Seite und über das Zertifikat, aber keine Informationen über GMX.
- **Cookies:** Die Datei cookies.sqlite wurde gelöscht.
- **Eingegebene Adresse:** Die Datei formhistory.sqlite wurde gelöscht. In places.sqlite sind noch Reste von beiden Adressen zu finden.

Extrahierte Unterschiede Im Image FF-TX wurde nach den Schlüsselwörtern gesucht: 627x "gmx", 294x "jku", 270x "khg", 229x "a4g" und 212x "jag".

5.3.6 Wipe

Anwendung Es wurden insgesamt 36 Spuren mit einer Gesamtgröße von 3,5 MB von Wipe gefunden.

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten, wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** In signons.sqlite wurde gelöscht. Die Datei cert_override.txt enthält noch Spuren vom Forums-Link, aber nichts von GMX.
- **Zertifikate:** cert8.db enthält nachwievor Informationen über die besuchte Seite und über das Zertifikat, aber keine Informationen über GMX.
- **Cookies:** Die Datei cookies.sqlite wurde gelöscht.
- **Eingegebene Adresse:** Die Datei formhistory.sqlite wurde gelöscht. Auch in places.sqlite sind noch Reste von beiden Adressen zu finden.

Extrahierte Unterschiede Im Image FF-WI wurde nach den Schlüsselwörtern gesucht: 417x "GMX", 211x "JKU", 216x "KHG", 229x "a4g" und 213x "jag".

5.3.7 Gegenüberstellung

Firefox	GMX	JKU	KHG	A4G	JAG
A	90	96	137	231	215
A-FF	340	131	105	8	10
FF	429	221	224	231	212
CCleaner	454	226	227	229	214
Clear-Prog	321	212	220	230	216
~~**One-Click-Privacy**~~	~~428~~	~~218~~	~~220~~	~~230~~	~~213~~
TraXEx	627	294	270	229	212
Wipe	417	211	216	229	213

Tabelle 4: Versuchsreihe Firefox: Anzahl Vorkommnisse

Wenn man die Ausgangswerte von der Zeile "FF" verwendet sieht man zwar, dass ein Großteil der Programme im Dateisystem viele der Spuren löscht (Details in vorangegangenen Bereichen), auf der Festplatte selbst aber die übriggebliebenen Spuren nicht überschrieben werden.

5.4 Versuchsreihe Google Chrome

Im Folgenden werden die Folgen der Anwendung der Löschwerkzeuge für den Browser Google Chrome analysiert, am Ende erfolgt eine Gegenüberstellung der Ergebnisse und ein Resümee.

5.4.1 Gesurft

Händische Auswertung

- **Verlauf:** In den folgenden Dateien im lokalen Profilordner finden sich Spuren der besuchten Seiten: Current Session, Current Tabs, Favicons, Favicons-journal, History, History Index 2013-03, History Provider Cache, Network Action Predictor, Network Action Predictor-journal, Preferences (die Bereiche dns_prefetching und startup_list beinhalten auch umliegende URLs), Shortcuts, Web Data. Im Unterordner Cache finden sich in den Datendateien ebenfalls die URLs.
- **Zertifikate:** Eine Zertifikatsdatei findet man wie angegeben im Zertifikatsspeicher von Microsoft. Hier ist unter \RSA\S-1-5-18 eine Datei abgelegt, welche aber keine genaueren Informationen auslesen lässt.
- **Cookies:** In der Datei Cookies im Profilordner findet man Verweise auf beide besuchte Seiten, in der Datei "Login Data" findet sich auch der Loginname vom Forum und das verschlüsselte Passwort
- **Eingegebene Adresse:** In welcher Datei genau die eingegebenen Adressen hinterlegt wurden ist nicht bekannt - naheliegend wäre die Datei "Visited Links", diese enthält jedoch keine Informationen.

Google Chrome ist der einzige Browser, bei dem bisher eine Form von "Einstellungsdatei" (Preferences) direkt im Dateisystem unverschlüsselt gelesen werden kann.

Extrahierte Unterschiede In den extrahierten Unterschieden der Images A und GC wurde nach den Schlüsselwörtern gesucht: 341x "gmx", 80x "jku", 81x "khg", 8x "a4g" und 12x "jag".

Durchsuchung von nur GC ergab folgende Vorkommnisse: 430x "gmx", 169x "jku, 199x "khg", 231x "a4g" und 213x "jag".

5.4.2 CCleaner

Anwendung Es wurden insgesamt 78 Spuren mit einer Gesamtgröße von 18,7 MB vom CCleaner gefunden.

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten, wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** Von den Dateien, die Spuren enthielten, wurde ein Großteil gelöscht. Vorhanden sind noch die Dateien Favicons, History, Preferences, Shortcuts und Webdata. In den Dateien Shortcuts, Favicons, History und Web Data (nur GMX) finden sich noch Reste der URLs.
- **Zertifikate:** Die Zertifikatsdatei ist noch vorhanden und wurde nicht verändert.
- **Cookies:** Die Spuren in der Datei Cookies wurden entfernt, die Datei "Login Data" wurde gänzlich gelöscht.
- **Eingegebene Adresse:** Hier kann nur auf die verbliebenen Spuren in den oben genannten Dateien verwiesen werden.

Extrahierte Unterschiede Im Image GC-CC wurde nach den Schlüsselwörtern gesucht: 446x "gmx", 181x "jku", 210x "khg", 228x "a4g" und 215x "jag".

5.4.3 Clear-Prog

Anwendung Es wurden keine Spuren gefunden.

Händische Auswertung Dieses Programm unterstützt das Entfernen von Spuren, welche von Google Chrome verursacht wurden, nicht. Aus diesem Grund wurden auch die Dateien nicht mehr durchsucht. Das Betriebssystem wurde hochgefahren und das Programm gestartet, weshalb sich evtl. Veränderungen auf der Festplatte ergeben können.

Extrahierte Unterschiede Im Image GC-CP wurde nach den Schlüsselwörtern gesucht: 429x "gmx", 170x "jku", 200x "khg", 225x "a4g" und 211x "jag".

5.4.4 One-Click-Privacy

Anwendung Es wurden keine Spuren gefunden.

Händische Auswertung Dieses Programm unterstützt das Entfernen von Spuren, welche von Google Chrome verursacht wurden, nicht. Aus diesem Grund wurden auch die Dateien nicht mehr durchsucht. Das Betriebssystem wurde hochgefahren und das Programm gestartet, weshalb sich evtl. Veränderungen auf der Festplatte ergeben können.

Extrahierte Unterschiede Im Image GC-OC wurde nach den Schlüsselwörtern gesucht: 429x ”gmx”, 171x ”jku”, 200x ”khg”, 225x ”a4g” und 213x ”jag”.

5.4.5 TraXEx

Anwendung Es wurden insgesamt 103 Spuren mit einer Gesamtgröße von 18,57 MB von TraXEx gefunden.

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten, wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** Vorhanden sind noch die Dateien Favicons, Favicons-journal, History, History Provider Cache, Network Action Predictor, Network Action Predictor-journal, Preferences, Shortcuts und Web Data. Die Datei History enthält keine Spuren mehr, bei den anderen sind noch Reste zu finden.
- **Zertifikate:** Die Zertifikatsdatei ist noch vorhanden und wurde nicht verändert.
- **Cookies:** Die Datei Cookies und ”Login Data” wurde entfernt.
- **Eingegebene Adresse:** Hier kann nur auf die verbliebenen Spuren in den oben genannten Dateien verwiesen werden.

Extrahierte Unterschiede Im Image GC-TX wurde nach den Schlüsselwörtern gesucht: 609x ”gmx”, 247x ”jku”, 276x ”khg”, 225x ”a4g” und 216x ”jag”.

5.4.6 Wipe

Anwendung Es wurden insgesamt 64 Spuren mit einer Gesamtgröße von 18,81 MB von Wipe gefunden.

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** Der Ordner Cache wurde gänzlich entfernt. in den verbliebenen Dateien Faviconsjournal (kein GMX), Network Action Predictor (kein GMX), Network Action Predictorjournal und Preferences im Profilverzeichnis finden sich noch Spuren der URLs.
- **Zertifikate:** Die Zertifikatsdatei ist noch vorhanden und wurde nicht verändert.
- **Cookies:** Die Datei Cookies wurde gelöscht, in "Login Data" findet man noch die Logindaten vom Forum.
- **Eingegebene Adresse:** Hier kann nur auf die verbliebenen Spuren in den oben genannten Dateien verwiesen werden.

Extrahierte Unterschiede Im Image GC-WI wurde nach den Schlüsselwörtern gesucht: 415x "gmx", 149x "jku", 178x "khg", 225x "a4g" und 212x "jag".

5.4.7 Gegenüberstellung

Google Chrome	GMX	JKU	KHG	A4G	JAG
A	90	96	137	231	215
A-GC	341	80	81	8	12
GC	430	169	199	231	213
CCleaner	446	181	210	228	215
~~**Clear-Prog**~~	~~429~~	~~170~~	~~200~~	~~225~~	~~211~~
~~**One-Click-Privacy**~~	~~429~~	~~171~~	~~200~~	~~225~~	~~213~~
TraXEx	609	247	276	225	216
Wipe	415	149	178	225	212

Tabelle 5: Versuchsreihe Google Chrome: Anzahl Vorkommnisse

Auch bei dieser Versuchsreihe sieht man, dass ein Großteil der Spuren im Dateisystem entfernt wurde, auf der Festplatte selbst aber viele Sektoren noch vorhanden sind, in denen auf die Daten rückgeschlossen werden kann. Besonders hingewiesen werden soll auf die Größe der gefunden Spuren, die weit über dem Durchschnitt im Vergleich zu den anderen Browsern liegt.

5.5 Versuchsreihe Internet Explorer

Im Folgenden werden die Folgen der Anwendung der Löschwerkzeuge für den Browser Internet Explorer analysiert, am Ende erfolgt eine Gegenüberstellung der Ergebnisse und ein Resümee.

5.5.1 Gesurft

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten, wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** Im Unterordner "Temporary Internet Files" findet sich der Ordner Content.IE5, in dem die gecachten Inhalte liegen. Im Unterordner "Verlauf" liegt der Ordner History.IE5, wo sich in der Datei index.dat Informationen über die besuchten Seiten befinden.
- **Zertifikate:** Im Ordner \RSA\S-1-5-18 findet sich eine Datei, in der keine weiteren Informationen über das Zertifikat selbst nachvollziehbar sind.
- **Cookies:** Im Cookies-Ordner findet sich eine ganze Liste von Dateien, welche Informationen enthalten - nicht nur über die besuchten Seiten, sondern auch über alle möglichen Seiten, welche auf den besuchten Seiten nur verlinkt waren.
- **Eingegebene Adresse:** Im angegebenen Verzeichnis in der Registrierung finden sich die eingegebenen Links. Seltsam ist hier, dass nur GMX gefunden wird, vom anderen Link ist nichts zu finden, was auch nach einer Durchsicht mit X-Ways Forensics nicht erklärbar ist.

Extrahierte Unterschiede In den extrahierten Unterschieden der Images A und IE wurde nach den Schlüsselwörtern gesucht: 1.448x "gmx", 86x "jku", 50x "khg", 8x "a4g" und 21x "jag".

Durchsuchung von nur IE ergab folgende Vorkommnisse: 1537x "gmx", 175x "jku", 170x "khg", 233x "a4g" und 225x "jag".

5.5.2 CCleaner

Anwendung Es wurden insgesamt 180 Spuren mit einer Gesamtgröße von 1,6 MB vom CCleaner gefunden.

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten, wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** Alle Rückstände wurden entfernt, lediglich im Ordner Verlauf\History.IE5 findet sich in der Datei index.dat noch ein Verweis auf die besuchten Seiten.
- **Zertifikate:** Die Zertifikatsdatei wurde nicht entfernt.
- **Cookies:** Der Cookiesordner ist leer und in der Datei index.dat finden sich keine URL-Reste mehr.
- **Eingegebene Adresse:** Die Registrierungsschlüssel wurden entfernt.

Extrahierte Unterschiede Im Image IE-CC wurde nach den Schlüsselwörtern gesucht: 1220x "gmx", 128x "jku", 144x "khg", 230x "a4g" und 217x "jag".

5.5.3 Clear-Prog

Anwendung Es wurden insgesamt 200 Spuren mit einer Gesamtgröße von 1,64 MB vom Clear-Prog gefunden.

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten, wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** Die Inhalte der Ordner "Verlauf" und "Temporary Internet Files" wurden gelöscht, in den zugehörigen index.dat Dateien sind aber noch Reste zu finden.
- **Zertifikate:** Die Zertifikatsdatei wurde nicht entfernt.
- **Cookies:** Der Cookiesordner ist zwar leer, aber in der Datei index.dat finden sich noch URL-Reste.
- **Eingegebene Adresse:** Die Registrierungsschlüssel wurden entfernt.

Extrahierte Unterschiede Im Image IE-CP wurde nach den Schlüsselwörtern gesucht: 1536x "gmx", 141x "jku", 169x "khg", 230x "a4g" und 213x "jag".

5.5.4 One-Click-Privacy

Anwendung Es wurden insgesamt 176 Spuren mit einer Gesamtgröße von 1,58 MB von One-Click-Privacy gefunden.

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten, wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** Unterordner im Cache-Verzeichnis sind noch zu finden, allerdings ohne Inhalte. Die jeweiligen index.dat Dateien enthalten Reste der URLs.
- **Zertifikate:** Die Zertifikatsdatei wurde nicht entfernt.
- **Cookies:** Der Cookiesordner ist zwar leer, aber in der Datei index.dat finden sich noch URL-Reste.
- **Eingegebene Adresse:** Die Registrierungsschlüssel wurden entfernt.

Extrahierte Unterschiede Im Image IE-OC wurde nach den Schlüsselwörtern gesucht: 1438x ”gmx”, 169x ”jku”, 167x ”khg”, 227x ”a4g” und 215x ”jag”.

5.5.5 TraXEx

Anwendung Es wurden insgesamt 489 Spuren mit einer Gesamtgröße von 4,93 MB von TraXEx gefunden.

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten, wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** Inhalte und Unterordner wurden gelöscht, aber in den index.dat Dateien sind noch Spuren der URLs zu finden.
- **Zertifikate:** Die Zertifikatsdatei wurde nicht entfernt.
- **Cookies:** Cookies wurden gelöscht, aber in der index.dat finden sich noch Reste.
- **Eingegebene Adresse:** Die Registrierungsschlüssel wurden entfernt.

Extrahierte Unterschiede Im Image IE-TX wurde nach den Schlüsselwörtern gesucht: 1237x ”gmx”, 158x ”jku”, 169x ”khg”, 229x ”a4g” und 221x ”jag”.

5.5.6 Wipe

Anwendung Es wurden insgesamt 210 Spuren mit einer Gesamtgröße von 1,6 MB von Wipe gefunden.

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten, wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** Alle Unterordner und Inhalte sind gelöscht, in den index.dat Dateien findet sich auch nichts mehr.
- **Zertifikate:** Die Zertifikatsdatei wurde nicht entfernt.
- **Cookies:** Alle Cookies wurden entfernt und in der index.dat finden sich auch keine Hinweise mehr.
- **Eingegebene Adresse:** Die Registrierungsschlüssel wurden entfernt.

Extrahierte Unterschiede Im Image IE-WI wurde nach den Schlüsselwörtern gesucht: 1192x "gmx", 139x "jku", 138x "khg", 229x "a4g" und 220x "jag".

5.5.7 Gegenüberstellung

Internet Explorer	GMX	JKU	KHG	A4G	JAG
A	90	96	137	231	215
A-IE	1.448	86	50	8	21
IE	1.537	175	170	233	225
CCleaner	1.220	128	144	230	217
Clear-Prog	1.536	141	169	230	213
One-Click-Privacy	1.438	169	167	227	215
TraXEx	1.237	158	169	229	221
Wipe	1.192	139	138	229	220

Tabelle 6: Versuchsreihe IE: Anzahl Vorkommnisse

Internet Explorer ist der einzige Browser, der von allen Löschwerkzeugen unterstützt wird. Wie bei den beiden vorangegangenen Versuchsreihen werden auch hier vermehrt die meisten Spuren entfernt, auf der Festplatte bleiben aber die Daten erhalten.

5.6 Versuchsreihe Opera

Im Folgenden werden die Folgen der Anwendung der Löschwerkzeuge für den Browser Opera analysiert, am Ende erfolgt eine Gegenüberstellung der Ergebnisse und ein Resümee.

5.6.1 Gesurft

Händische Auswertung

- **Verlauf:** Der Verlauf in global_history.dat enthält die Informationen der URLs. Ebenso sind die Links in vlink4.dat enthalten. Im Unterordner sessions finden sich ebenfalls Dateien mit Linkinformationen.
- **Zertifikate:** Die Datei opcacrt6.dat enthält keine Informationen, ebensowenig opcert6.dat und opicacrt6.dat.
- **Cookies:** cookies4.dat enthält Informationen zu den besuchten Seiten, über Loginname und Passwort gibt es aber nichts.
- **Eingegebene Adresse:** In der Datei typed_history.xml finden sich die beiden eingegebenen Adressen.

Extrahierte Unterschiede In den extrahierten Unterschiede der Images A und OP wurde nach den Schlüsselwörtern gesucht: 249x ”gmx”, 54x ”jku”, 58x ”khg”, 9x ”a4g” und 14x ”jag”.

Durchsuchung von nur OP ergab folgende Vorkommnisse: 338x ”gmx”, 144x ”jku”, 178x ”khg”, 236x ”a4g” und 217x ”jag”.

5.6.2 CCleaner

Anwendung Es wurden insgesamt 63 Spuren mit einer Gesamtgröße von 1,55 MB vom CCleaner gefunden.

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten, wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** Die Dateien global_history.dat und vlink4.dat wurden gelöscht, ebenso die Dateien im Unterordner sessions.

- **Zertifikate:** In den betroffenen Dateien finden sich keine Informationen zum Zertifikat.
- **Cookies:** Der Inhalt der Datei cookies4.dat wurde gelöscht, somit sind die Spuren entfernt.
- **Eingegebene Adresse:** Die Datei typed_history.xml wurde gelöscht.

Extrahierte Unterschiede Im Image OP-CC wurde nach den Schlüsselwörtern gesucht: 338x "gmx", 138x "jku", 171x "khg", 231x "a4g" und 215x "jag".

5.6.3 Clear-Prog

Anwendung Es wurden keine Spuren gefunden, obwohl das Programm explizit "Opera" zur Auswahl anbietet. Es wurden auch keine Spuren gelöscht, somit fällt dieses Programm bei Opera ebenfalls aus der Wertung.

Händische Auswertung Dieses Programm unterstützt das Entfernen von Spuren, welche von Opera verursacht wurden, nicht. Aus diesem Grund wurden auch die Dateien nicht mehr durchsucht. Das Betriebssystem wurde hochgefahren und das Programm gestartet, weshalb sich evtl. Veränderungen auf der Festplatte ergeben können.

Extrahierte Unterschiede Im Image OP-CP wurde nach den Schlüsselwörtern gesucht: 338x "gmx", 137x "jku", 179x "khg", 240x "a4g" und 224x "jag".

5.6.4 One-Click-Privacy

Anwendung Es wurden keine Spuren gefunden.

Händische Auswertung Dieses Programm unterstützt das Entfernen von Spuren, welche von Opera verursacht wurden, nicht. Aus diesem Grund wurden auch die Dateien nicht mehr durchsucht. Das Betriebssystem wurde hochgefahren und das Programm gestartet, weshalb sich evtl. Veränderungen auf der Festplatte ergeben können.

Extrahierte Unterschiede Im Image OP-OC wurde nach den Schlüsselwörtern gesucht: 338x "gmx", 138x "jku", 168x "khg", 233x "a4g" und 218x "jag".

5.6.5 TraXEx

Anwendung Es wurden insgesamt 62 Spuren mit einer Gesamtgröße von 1,44 MB von TraXEx gefunden.

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten, wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** Die betroffenen Dateien wurden gelöscht.
- **Zertifikate:** Die Zertifikatsdateien sind nachwievor ohne Information zu den besuchten Seiten, weshalb auch keine Löschung nachvollzogen werden konnte.
- **Cookies:** cookies4.dat enthält keine Informationen mehr zu den besuchten Seiten.
- **Eingegebene Adresse:** Die Datei typed_history.xml wurde gelöscht.

Extrahierte Unterschiede Im Image OP-TX wurde nach den Schlüsselwörtern gesucht: 341x ”gmx”, 140x ”jku”, 173x ”khg”, 234x ”a4g” und 218x ”jag”.

5.6.6 Wipe

Anwendung Es wurden insgesamt 107 Spuren mit einer Gesamtgröße von 1,6 MB von Wipe gefunden.

Händische Auswertung Die Dateien, welche nach dem Surfen Spuren enthielten, wurden nach dem Löschvorgang nochmals durchsucht.

- **Verlauf:** Die betroffenen Dateien wurden gelöscht, im Dateisystem sind diesbezüglich keine Informationen mehr zu finden.
- **Zertifikate:** Die Zertifikatsdateien sind nachwievor ohne Information zu den besuchten Seiten, weshalb auch keine Löschung nachvollzogen werden konnte.
- **Cookies:** cookies4.dat enthält keine Informationen mehr zu den besuchten Seiten.
- **Eingegebene Adresse:** Die Datei typed_history.xml wurde gelöscht.

Extrahierte Unterschiede Im Image OP-WI wurde nach den Schlüsselwörtern gesucht: 343x ”gmx”, 144x ”jku”, 174x ”khg”, 233x ”a4g” und 218x ”jag”.

5.6.7 Gegenüberstellung

Opera	GMX	JKU	KHG	A4G	JAG
A	90	96	137	231	215
A-OP	249	54	58	9	14
OP	338	144	178	236	217
CCleaner	338	138	171	231	215
~~**Clear-Prog**~~	~~338~~	~~137~~	~~179~~	~~240~~	~~224~~
~~**One-Click-Privacy**~~	~~338~~	~~138~~	~~168~~	~~233~~	~~218~~
TraXEx	341	140	173	234	218
Wipe	343	144	174	233	218

Tabelle 7: Versuchsreihe Opera: Anzahl Vorkommnisse

Auch bei dieser Versuchsreihe arbeiten die Werkzeuge, die auch wirklich Spuren löschen, sehr zuverlässig, die tatsächlichen Spuren auf der Festplatte bleiben aber, wie bei den anderen Szenarien auch, erhalten.

6 Vergleich der Löschwerkzeuge und Interpretation

Basierend auf den Ergebnissen der Durchführung der Versuchsreihen Firefox 5.3, Google Chrome 5.4, Internet Explorer 5.5 und Opera 5.6 wird nun ein Vergleich der Zuverlässigkeit der verwendeten Löschwerkzeuge vorgenommen. Es wird jeweils die Effizienz bzw. Zuverlässigkeit bezogen auf die getesteten Kategorien mit klassischen österreichischen Schulnoten (1 = Sehr Gut, 2 = Gut, 3 = Befriedigend, 4 = Genügend, 5 = Nicht genügend) bewertet und gegenübergestellt.

6.1 Gegenüberstellung der gefundenen Spuren

Vorab werden die gefundenen Spuren bzw. deren Größe bezogen auf den jeweiligen Browser bzw. das verwendete Werkzeug gegenübergestellt:

Gefundene Spuren	**Firefox**	**Chrome**	**IE**	**Opera**	**Schnitt**
CCleaner	43	78	180	63	91
Größe in MB	3,12	18,7	1,6	1,55	6,24
Clear-Prog	24	0	200	0	124
Größe in MB	2,34	0	1,64	0	1,99
One-Click-Privacy	0	0	176	0	176
Größe in MB	0	0	1,58	0	1,58
TraXEx	105	103	489	62	190
Größe in MB	4,28	18,57	4,93	1,44	7,3
Wipe	36	64	210	107	104
Größe in MB	3,5	18,81	1,6	1,6	6,38
Schnitt	52	82	251	77	-
Schnitt Größe in MB	3,31	18,7	2,27	1,53	-

Tabelle 8: Gefundene Spuren

Die meisten Spuren werden vom Internet Explorer erzeugt, was sich vermutlich dadurch begründen lässt, dass diese Programm integraler Bestandteil des Betriebssystems ist. Bei den restlichen Browsern halten sich die Anzahl der Funde in der Waage, ”0-Funde” wurden nicht in die Wertung mit aufgenommen. Die meisten Spuren werden im Schnitt vom Programm TraXEx gefunden. Die größte Menge an Spuren, gemessen am Speicherplatz, verursacht der Browser Google Chrome. Clear-Prog arbeitet nicht bei Google Chrome und Opera, obwohl der Browser Opera explizit zum Spurenlöschen gewählt werden kann.

One-Click-Privacy unterstützt lediglich Internet Explorer, Netscape steht als Browser noch zur Auswahl. Der Nachfolger des Netscape Navigator kommt zwar aus der Produktsparte Mozilla, womit Firefox ein möglich zu unterstützendes Programm wäre, es werden aber keine Ergebnisse erzielt. Vermutlich ist das Alter des Programmes ein Grund für dessen ”Unbrauchbarkeit”, weshalb es auch nicht mehr auf der Herstellerseite angeboten wird.

6.2 Ergebnis CCleaner

CCleaner	Firefox	Chrome	IE	Opera	Schnitt
gefundene Spuren	43	78	180	63	91
Größe der Spuren in MB	3,12	18,7	1,6	1,55	6,24
Verlauf	3	3	2	1	2,25
Zertifikate	2	5	5	1	3,25
Cookies	2	1	1	1	1,25
typedURLs	5	3	1	1	1,5
Schnitt	3	3	2,25	1	-

Tabelle 9: Ergebnis CCleaner

Der CCleaner ist für die Spurenlöschung eines der bekanntesten Programme und arbeitet "im Großen und Ganzen" eigentlich sehr zuverlässig. Vor allem die Ergebnisse bzw. Zuverlässigkeit bei Firefox und insbesondere Opera lassen dieses Programm durchaus weiterempfehlen. Das etwas schlechtere Ergebnis von Chrome fällt bei der Auswertung auf, hält sich aber im Vergleich mit den anderen Programmen trotzdem im oberen Bereich. Die einzelnen Bereiche werden großteils verborgen, nur mit einer genaueren Recherche in den Speicherorten der Daten im Dateisystem lassen sich noch Spuren finden, lediglich bei der Löschung von Zertifikaten und den typedURLs hat der CCleaner unterdurchschnittliche Ergebnisse geliefert. **Gesamtnote: 2**

6.3 Ergebnis Clear-Prog

Clear-Prog	Firefox	Chrome	IE	Opera	Schnitt
gefundene Spuren	24	-	200	-	124
Größe der Spuren in MB	2,34	-	1,64	-	1,99
Verlauf	3	-	2	-	2,5
Zertifikate	3	-	5	-	4
Cookies	5	-	2	-	3,5
typedURLs	5	-	1	-	3
Schnitt	4	-	2,5	-	-

Tabelle 10: Ergebnis Clear-Prog

Bei diesem Werkzeug fällt nachwievor auf, dass es Opera explizit auflistet, aber keine Informationen oder Spuren findet. Dass bei Firefox Cookies und typed URLs gar nicht entfernt werden, wirkt etwas enttäuschend, umso überraschender sind die durchwegs guten Ergebnisse beim Löschen der Spuren, die vom Internet Explorer erzeugt wurden (ausgenommen Zertifikate). Besonders wenn man auf die Einfachheit abzielt, die gegeben ist um eine Datei zu löschen (typed URLs bei Firefox), verglichen mit dem gezielten Löschen von Registrierungsschlüsseln. **Gesamtnote: 3**

6.4 Ergebnis One-Click-Privacy

One-Click-Privacy	Firefox	Chrome	IE	Opera	Schnitt
gefundene Spuren	-	-	176	-	176
Größe der Spuren in MB	-	-	1,58	-	1,58
Verlauf	-	-	2	-	2
Zertifikate	-	-	5	-	5
Cookies	-	-	2	-	2
typedURLs	-	-	1	-	1
Schnitt	-	-	2,5	-	-

Tabelle 11: Ergebnis One-Click-Privacy

Dieses Programm findet mäßig viele Spuren, leider kommt es nur bei der Verwendung des Internet Explorers zur Anwendung und lässt auch beim Zertifikatsspeicher mit seinen Versprechungen aus. Die eingegebenen Adressen werden vollständig entfernt, beim Verlauf und den Cookies wird auch gut gearbeitet. Da der Internet Explorer nicht mehr so stark genutzt wird wie in früheren Zeiten und One-Click-Privacy nur diesen Browser unterstützt, wird von der Benutzung dieses Programms zur Spurenlöschung, vor allem aber auch wegen des Alters des Programms, abgeraten. **Gesamtnote: 4**

6.5 Ergebnis TraXEx

TraXEx	Firefox	Chrome	IE	Opera	Schnitt
gefundene Spuren	105	103	489	62	190
Größe der Spuren in MB	4,28	18,57	4,93	1,44	6,24
Verlauf	3	4	2	1	2,5
Zertifikate	3	5	5	5	4,5
Cookies	1	1	2	1	1,25
typedURLs	5	4	1	1	1,75
Schnitt	3	3,5	2,5	2	-

Tabelle 12: Ergebnis TraXEx

Dieses Programm liefert auch durchgängig gute Ergebnisse, vor allem die Spuren bei Opera und Firefox (bis auf die typedURLs) werden sehr zufriedenstellend entfernt. Lediglich beim Zertifikatsspeicher von Chrome, IE und Opera können keine Löschungen verfolgt werden, was vor allem bei Opera verwunderlich ist, da hier ebenfalls nur Dateien gelöscht bzw. Inhalte von Dateien verändert werden müssten. Bei Chrome liefert das Programm generell schlechte Ergebnisse, da sowohl Verlauf als auch die typed URLs nicht entfernt werden. **Gesamtnote: 2,5**

6.6 Ergebnis Wipe

Wipe	Firefox	Chrome	IE	Opera	Schnitt
gefundene Spuren	36	64	210	107	104
Größe der Spuren in MB	3,5	18,81	1,6	1,6	6,38
Verlauf	3	4	1	1	2,25
Zertifikate	3	5	5	5	4,5
Cookies	1	3	1	1	1,5
typedURLs	5	4	1	1	1,75
Schnitt	3	4	2	2	-

Tabelle 13: Ergebnis Wipe

Obwohl das Programm sehr neu wirkt, findet es nur durchschnittlich wenig Spuren im Vergleich zu den anderen Löschprogrammen, dafür schneidet es bei allen Browsern gut ab. Bemängeln lässt sich nur das Löschen der Zertifikate, was bei 3 von 4 Browsern nicht funktioniert, ebenso das Entfernen der typedURLs bei Firefox. Umso besser die Zuverlässigkeit bei Internet Explorer und Opera, da hier wirklich alle Spuren restlos entfernt werden. **Gesamtnote: 2,5**

7 Zusammenfassung und Resümee

Dieses Projekt hat mir einige neue Bereiche der Computerforensik eröffnet und mir die Gelegenheit gegeben, mich tiefer in diese Materie einzuarbeiten. Über diesen Aspekt bin ich sehr froh, denn im Bereich der Computerforensik gibt es mit Sicherheit unbegrenzte Möglichkeiten.

Die meisten Recherchen bzw. Vorbereitungsarbeiten für die Durchführung der Versuche erforderte das Herausfinden der Informationen, wo welcher Browser welche Informationen in welcher Form abspeichert. Ich möchte aber darauf hinweisen, dass diese Informationen vermutlich bereits wieder veraltet sind, da mit jeder neuen Browserversion die Möglichkeit besteht, dass die Speicherorte für die relevanten Informationen geändert werden.

Das Anwenden der Löschwerkzeuge war lediglich mit viel Speicher- und Rechenaufwand verbunden ebenso das nachherige Exportieren der Festplattendateien, die jeweils eine Größe von 3 GB hatten. Entsprechende Hardware und Rechenleistung erleichtert hier das Arbeiten immens und verringert die Wartezeiten auf ein Minimum.

Zeitintensiv war das Vergleichen der Festplattenimages miteinander und das sektorweise Durchsuchen nach Schlüsselwörtern. In diesem Bereich fällt besonders auf, dass man, egal wie viele Informationen man im Dateisystem entfernt, man immer noch Spuren und Informationen in den Sektoren der Festplatte findet - man muss nur wissen wonach man suchen muss, dann lässt sich der Besuch von Webseiten sehr einfach nachweisen.

In diesem Kontext muss aber auch erwähnt werden, dass es für die Entwicklung von Löschprogrammen bestimmt schwer ist, gewisse Daten direkt auf der Festplatte zu löschen bzw. zu überschreiben, da hier auch genaue Informationen darüber bekannt sein müssen, welche Sektoren von der aktuellen Datei belegt werden. Ein Löschen des Dateiinhaltes, dass dieser nicht mehr angezeigt wird, ist eine Sache, aber die Daten tatsächlich gänzlich von der Festplatte zu entfernen ist ein anderes Thema der Computerforensik und Datenträgerbehandlung.

Fazit: Wenn man ein wirklich zuverlässiges Programm zum Löschen von Spuren haben möchte, konzipiert und implementiert man es am besten selbst, weil man nur dann auf Nummer sicher gehen kann, dass alle Spuren wirklich restlos entfernt werden. Natürlich nur, wenn man auch entsprechende Überschreibung bzw. Löschung der Inhalte auf den jeweiligen Sektoren der Festplatte berücksichtigt.

Literatur

[Bro12] Webanalyse - aktuelle browser-marktanteile, 2012.

[Fir13] *Firefox Wiki*, 2013.

[IE809] *Internet Explorer 8 - Übersicht über die Technologie für Unternehmens- und IT-Fachleute*, 2009.

[Ope13] *Opera Wiki*, 2013.

[Qem13] *QEMU Buch*, 2013.

[Son09] Assoz.Prof. Priv.-Doz. Mag. Dipl.-Ing. Dr. Michael Sonntag. Vorlesungsfolien it-recht und computerforensik, 2009.

[VMW] *Oracle VM Virtualbox User Manual*.

[Wik12] Wikipedia, die freie enzyklopädie, 2012.

[Win12] *Microsoft Windows XP Professional*, 2012.

A Source Code

Die verwendeten Programme sind auf einer CD/DVD beigelegt.