SECUPERTS
THE SECURITY EXPERTS

FORENSIC SYSTEM

Inhaltsverzeichnis

1 Was ist das SecuPerts-Forensik-System?

Das SecuPerts-Forensik-System ist ein eigenständiges Betriebssystem, das von DVD oder USB-Stick gestartet wird, also keine Änderungen an dem auf Festplatte installierten Betriebssystem vornimmt. Das erlaubt einerseits die unbemerkte Spurensuche, andererseits können Sie auch bei einem nicht startenden Windows herausfinden, ob die Ursache ein Manipulationsversuch, Schadsoftware oder ein einfacher Hardwarefehler ist. Neben der Spurensuche auf lokalen Laufwerken hilft das SecuPerts-Forensik-System bei der Analyse von Netzwerk-Traffic und beim Aufspüren von gehackten oder infizierten Netzwerkgeräten. Zudem können Sie Geräte im Netzwerk identifizieren und aktiv auf Schwachstellen untersuchen.

1.1 Was ist es nicht?

Es ist kein "Hacking-Tool", sondern dient in erster Linie der Analyse eigener Systeme und von Geräten im eigenen Netzwerk. Der Funktionsumfang von Passwort-Knackern ist daher bewusst gering gehalten und auf legalen Einsatz optimiert. So können Sie beispielsweise das SecuPerts-Forensik-System verwenden, um sehr schwache Passwörter von Mitarbeitern aufzuspüren (um diese zur Verwendung stärkerer aufzufordern), die Möglichkeiten, echter tiefer "Brute-Force-Attacken" sind jedoch eingeschränkt.

1.2 Welche rechtlichen Aspekte sind zu beachten?

Das SecuPerts-Forensik-System dient in erster Linie der Analyse Ihrer eigenen Rechner und Ihres eigenen Netzwerkes. Bei der Verwendung in Firmennetzwerken sind arbeitsrechtliche und IT-rechtliche Aspekte zu beachten und ggf. der Betriebsrat zu informieren. Ein weiterer Einsatzzweck ist die Verwendung als Schulungswerkzeug, beispielsweise um auf die Problematik unverschlüsselter mobiler Datenträger oder schnell formatierter Festplatten hinzuweisen.

Das SecuPerts-Forensik-System ist entwickelt zur Prüfung der Sicherheit und Auslastung des eigenen Datennetzes des Nutzers (siehe dazu Bundestagsdrucksache 16/5449 zu § 202c StGB). Mit Akzeptieren der Nutzungs- und Haftungsbedingungen verpflichtet sich der Nutzer, das Programm ausschließlich gesetzeskonform, insbesondere auch im Sinne der datenschutzrechtlichen Bestimmungen, einzusetzen. Das heißt u.a., dass die Erlaubnis jedes einzelnen Netzwerkteilnehmers bei einer Netzwerkprüfung eingeholt werden muss.

2 Der Startvorgang

Das SecuPerts-Forensik-System startet als eigenes Betriebssystem, in der Regel muss sein Start bereits erfolgen, bevor der Windows-Bootloader in Aktion tritt. Erhalten haben Sie das SecuPerts-Forensik-System entweder DVD oder als USB-Stick. Falls Sie die DVD gekauft haben, können Sie mit dieser an einem anderen Computer einen startfähigen USB-Stick erstellen. Hierfür liegt im Wurzelverzeichnis der DVD eine EXE-Datei. Im Idealfall hat der Hersteller des Computers das BIOS oder UEFI so konfiguriert, dass bei Erkennung eines bootfähigen Datenträgers dieser automatisch als Startmedium ausgewählt wird.

Falls dies nicht der Fall sein sollte, müssen Sie eventuell die Boot-Reihenfolge Ihres Systems ändern. Drücken Sie dazu, je nach verwendetem Gerät, beim Starten auf eine der folgenden Tasten (wird meistens beim Startvorgang angezeigt): F2, F8, F9, F10, F11, F12, Alt, Esc, oder Tab. Anschließend wählen sie das von Ihnen verwendete Medium (DVD oder USB-Stick) im Menü aus. Sollte das nicht

funktionieren müssen Sie eventuell die Boot-Reihenfolge im BIOS manuell ändern.

2.1 BIOS aufrufen

Starten Sie gleich nach dem Hochfahren des Rechners das BIOS. Die Methode zum Starten unterscheidet sich dabei je nach Modell des Mainboards. Welche Tastenkombination benötigt wird, wird Ihnen in der Regel während des Startvorgangs angezeigt. Häufige Tastenkombinationen, die direkt nach dem Systemstart zu drücken sind: Entf, F2, F10, und Esc. Bei Netbooks müssen Sie oft zusätzlich noch Strg und Alt betätigen, also zum Beispiel 'Strg + Alt + Esc'. Sollte keine dieser Kombinationen funktionieren sollten Sie eine Google-Suche mit dem Term 'BIOS Zugang für Ihr Mainboard' starten.

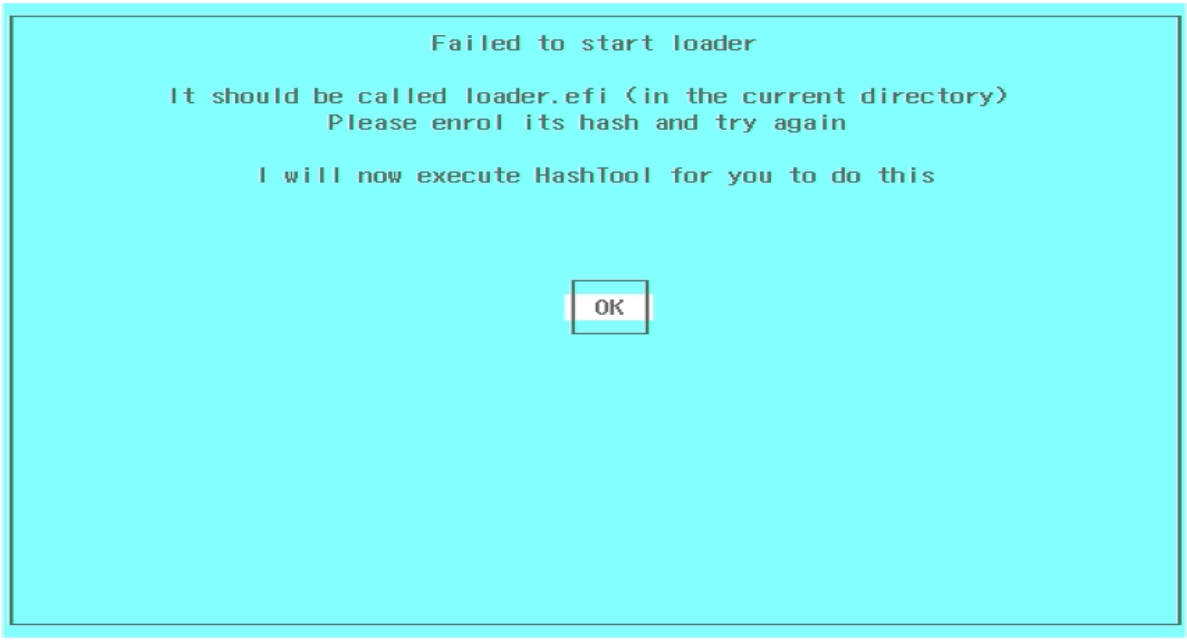
2.2 Boot-Reihenfolge ändern

BIOS-Oberflächen besitzen in der Regel ein Register mit einer Bezeichnung wie 'Boot', 'Boot Settings' oder auch 'Boot Options'. Es kann auch sein, dass die Einstellung unter einem Reiter namens 'Advanced' zu finden ist. Haben Sie die richtige Einstellung gefunden, wählen Sie Ihr DVD- oder USB-Laufwerk als erstes Boot-Laufwerk aus. Bei der Auswahl der Laufwerke wird oft das Plus-Zeichen auf dem Zahlenblock verwendet.

2.3 Start auf UEFI PCs

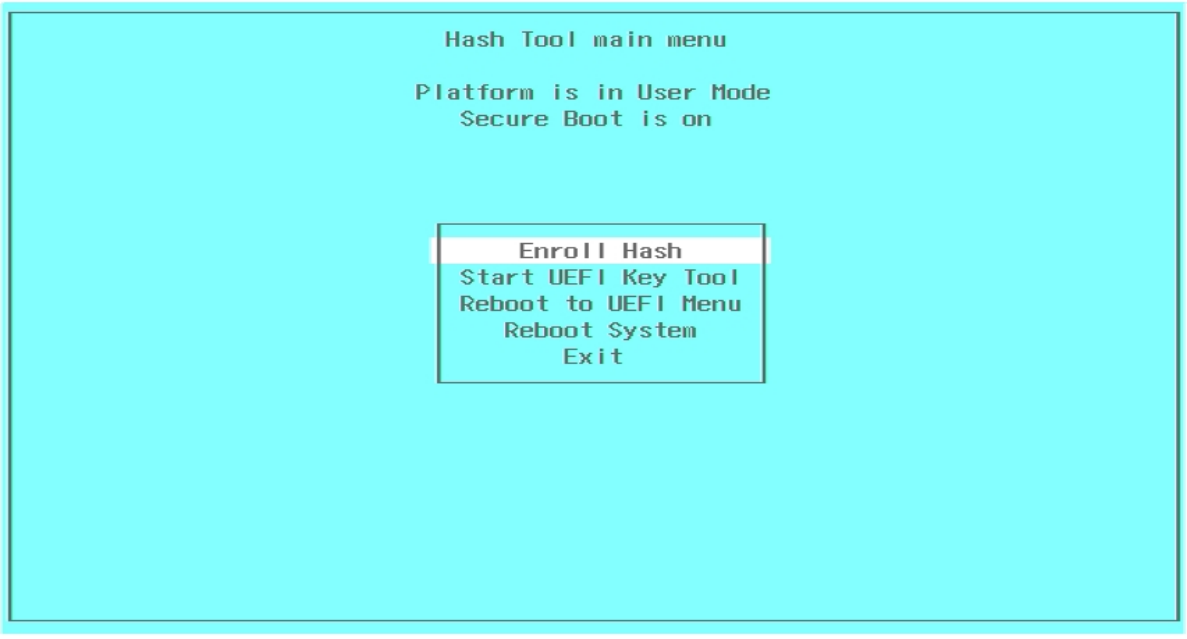
Neuere Windows-Versionen (Windows 8 und höher) nutzen in der Regel den BIOS-Nachfolger UEFI ("Universal Extensible Firmware Interface") in Kombination mit "Secure Boot". Auch das SecuPerts-Forensik-System verwendet solch einen signierten Loader, wobei sich die Startprozedur von einem klassischen BIOS unterscheidet. Wenn das Bootmenü nicht automatisch startet, können Sie es auch aus Windows heraus anstoßen. Öffnen Sie hierfür in der "Modern UI" die PC-Einstellungen. Anschließend klicken Sie auf "Allgemein" und "Jetzt neu starten". In dem nun erscheinenden Menü können Sie unter "Ein Gerät verwenden" ihr Start-Medium auswählen.

Dies startet den Bootloader Gummiboot, in dem Sie den Start des Forensik-Systems auswählen können (der meist angezeigte Eintrag "UEFI Default Loader" startet Windows). Bei aktiviertem "Secure Boot" erhalten Sie beim ersten Start die folgende Warnung:



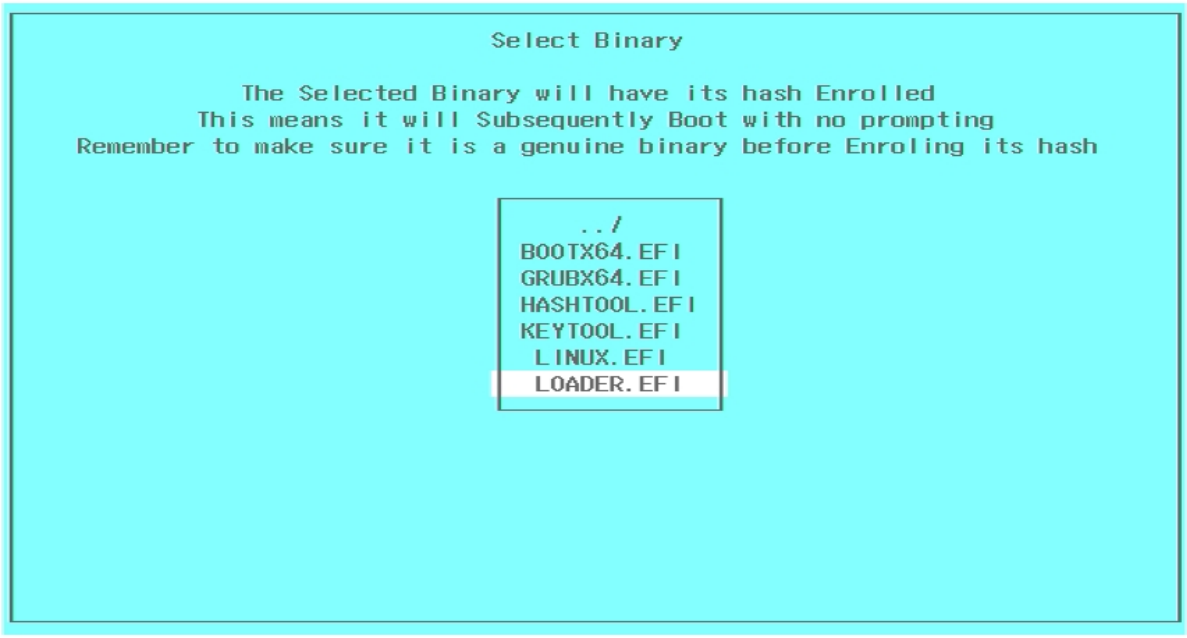
Bestätigen Sie "OK" um ins Hashtool zu gelangen

Bestätigen Sie mit "OK", was Sie zum "Hashtool" führt. Wählen Sie "Enroll Hash aus":



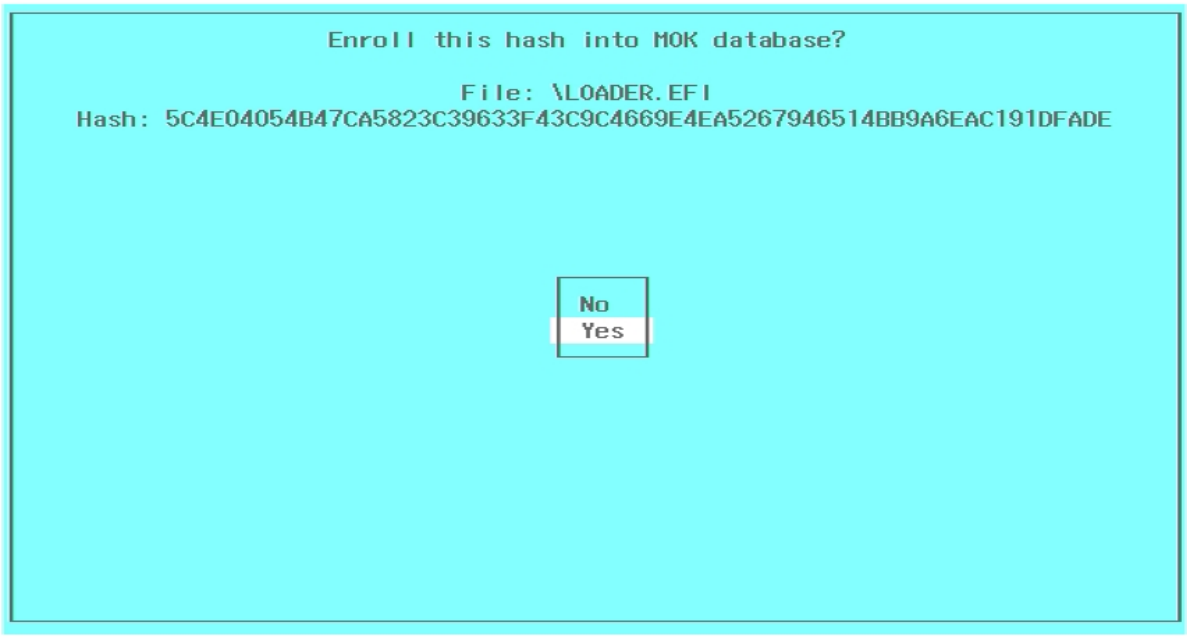
Wählen Sie "Enroll Hash"

In der folgenden Liste "Select Binary" wählen Sie die Datei "LOADER.EFI" aus:



Wählen Sie zuerst LADER.EFI, später LINUX.EFI

Jetzt werden Sie gefragt, ob der Hashwert der Liste der zulässigen zugefügt werden soll:



Bestätigen Sie jeweils mit Yes

Beantworten Sie mit "YES" und wiederholen Sie den Vorgang mit der Datei "LINUX.EFI". Verlassen Sie dann das Hashtool mit "EXIT" und wählen Sie im Bootmenü den Starteintrag für das SecuPerts-Forensik-System.

2.4 SecuPerts-Forensik-System bootet nicht

Das SecuPerts-Forensik-System baut auf dem linuxbasierten System 'LessLinux' auf. Dieses unterstützt eine Vielzahl von Hardwarekonfigurationen. In Einzelfällen kann es aber vorkommen, dass gerade Ihr System nicht unterstützt wird. Wir bitten um Verständnis, falls Sie davon betroffen sind. Eventuell hilft Ihnen einer der folgenden Tipps:

- Starten Sie Ihren PC im 'Legacy only'-Modus. Nutzer mit Windows 8 oder höher sollten darauf achten vor dem Neustart wieder 'UEFI only' zu aktivieren.
- Versuchen Sie die verfügbaren Boot-Parameter, welche Sie über den Menüpunkt 'Abgesicherter Start' im Bootmenü des SecuPerts-Forensik-Systems erreichen können.
- Schlägt der Start von USB-Stick fehl, können Sie von der Datei "boot.iso" auf dem Stick eine Start-CD/DVD erstellen, mit der sich der Start bei angeschlossenem Stick anstoßen lässt

3 Bootmenü des Forensik-Systems

Das SecuPerts-Forensik-System startet meistens direkt vom Bootmenü-Bildschirm, entweder nach Betätigen der Enter-Taste oder nach automatisch nach Ablauf von 30 Sekunden. Teilweise müssen noch einige Parameter geändert werden. Diese erreichen Sie über den Menüpunkt 'Abgesicherter Start'.

Bootmenü auf BIOS-Systemen

3.1 Aufteilung des Boot-Menüs

- **Starte SecuPerts-Forensik-System:** Startet direkt das Forensik -System.
- **Abgesicherter Start:** Anpassen von verschiedenen Parametern zum Systemstart.
- **Von Festplatte starten:** Verlässt das Boot-Menü und startet Ihr normales Betriebssystem.

Daneben haben Sie die Möglichkeit, mit der Tab-Taste (BIOS) oder der Taste "E" (UEFI) in den Editiermodus der Boot-Kommandozeile zu gelangen. Hier können Sie Bootparameter ändern oder ergänzen, gestartet wird die geänderte Boot-Kommandozeile mit der Eingabetaste. Diese Option wird gelegentlich benötigt, wenn Sie mit unserem Support Kontakt hatten.

3.2 Abgesicherter Start

- **Zurück:** Schließt die Parameterauswahl und wechselt zurück zum Boot-Menü
- **Start in Standardeinstellungen:** Systemstart ohne jegliche Änderungen.
- **SecuPerts-Forensik-System starten:** Entspricht dem Systemstart aus dem Boot-Menü.
- **SecuPerts-Forensik-System (nicht ins RAM kopieren):** Wenn Ihr System wenig Arbeitsspeicher besitzt oder Sie OpenVAS beim von DVD gestarteten System verwenden wollen, nutzen Sie bitte diese Option. So bleibt genug RAM zum Aufruf von Programmen verfügbar.
- **Start mit abgesicherten Einstellungen:** Startet das System unter Berücksichtigung von Problemen mit Grafiktreibern oder dem Energie-Management einiger Systeme.
- **Sicheres ACPI + VESA Grafik 1024x768:** Startet das System mit einer festen Auflösung von 1024x768 und kontrollierten Energie-Management. Nutzen Sie diese Option, wenn es Probleme mit Ihren Grafiktreibern gibt.
- **Sicheres ACPI + VESA Grafik auto:** Startet das System mit automatischer Auswahl der kompatibelsten Auflösung auf Grundlage des VESA-Anzeigeprotokolls und kontrollierten Energie-Management.
- **Sicheres ACPI + XORG Grafik auto:** Startet das System mit automatischer Auswahl der kompatibelsten Auflösung auf Grundlage des Xorg-Anzeigeprotokolls und kontrollierten Energie-Management.
- **VESA Grafik 1024x768:** das System mit einer festen Auflösung von 1024x768
- **VESA Grafik auto:** Startet das System mit automatischer Auswahl der kompatibelsten Auflösung auf Grundlage des VESA-Anzeigeprotokolls.
- **Fernzugriff aktivieren (VNC):** Hiermit können Sie Ihren Rechner per Fernzugriff warten. Diese Funktion sollte allerdings nur in einer absolut vertrauenswürdigen Umgebung eingesetzt werden.
- **Unsicheres Remote VNC + lokale GUI:** Ermöglicht die Verfolgung der Arbeiten, die am PC durchgeführt werden mit einem VNC-Viewer ohne Passworteingabe.
- **Unsicheres Remote VNC + ohne lokale GUI:** Ermöglicht die Verfolgung der Arbeiten, die am PC durchgeführt werden ohne visuelle Überprüfung, Sie können diese Option als Workaround verwenden, wenn Ihre Grafikkarte gar nicht angesprochen werden kann.
- **Reverse VNC + lokale GUI:** Ermöglicht die Fernwartung innerhalb eines eigenen Fensters auf dem Bildschirm. Der Zielrechner muss dafür vorher mit einem VNC-Viewer im "Listening Mode" eingerichtet werden.
- **Reverse VNC - ohne lokale GUI:** Ermöglicht die Fernwartung innerhalb eines eigenen Fensters auf dem Bildschirm. Der Zielrechner muss dafür vorher eingerichtet werden. Auch hier gibt es keine lokale visuelle Überprüfung.

Bei den VNC-Fernzugriffs-Modi können Sie mit der Tabulatortaste in den Editiermodus der Boot-Kommandozeile gelangen und hier Änderungen an Grafikauflösung, Passwort und Zielrechner (Reverse VNC) vornehmen.

4 Der Start-Bildschirm

Nach erfolgreichem Systemstart müssen Sie zunächst die Nutzungs- und Haftungsbedingungen akzeptieren. Ist dies geschehen, sehen Sie die Kategoriekacheln des Assistenten, zudem wird ein Desktop und eine Taskleiste angezeigt. Die Taskleiste wird sichtbar, wenn Sie mit dem Mauszeiger an den unteren Bildschirmrand fahren. Sie enthält ein Startmenü, einige Programm-Icons und Schaltflächen zum Aus- und Einblenden geöffneter Fenster, sowie einen Tray-Bereich rechts. Den Desktop können Sie wie unter Windows gewohnt zur Ablage von Dateien oder Programmstartern verwenden. Die Programme im Startmenü sind oft zur Kontrolle laufender Aktionen und natürlich zum Starten von nicht über den Assistenten angebotenen Funktionen nützlich.

Der Assistent des Forensik-Systems

4.1 Die obere Assistentenleiste

Die obere Leiste mit kleinen Icons dient dem Schnellzugriff auf häufig benötigte Funktionen:

- **Hilfe öffnen:** Öffnet dieses Handbuch
- **Webbrowser starten:** Recherchieren Sie im Internet
- **Netzwerkeinstellungen:** Verbinden Sie mit einem WLAN oder legen Sie Einstellungen
- **USB-Installation:** Installieren Sie das Forensik-System auf einen USB-Stick, hier können Sie auch eine Neuinstallation mit anderen Einstellungen (verschlüsseltes persistentes Heimatverzeichnis) auf einen größeren Stick vornehmen
- **Assistent minimieren:** Schafft Platz auf dem Desktop, in dem es den Assistenten ausblendet. Über die Taskleiste können Sie ihn wieder in den Vordergrund bringen.

4.2 Die Kategorien im Assistenten

Der Assistent teilt die Programme in vier Kategorien ein:

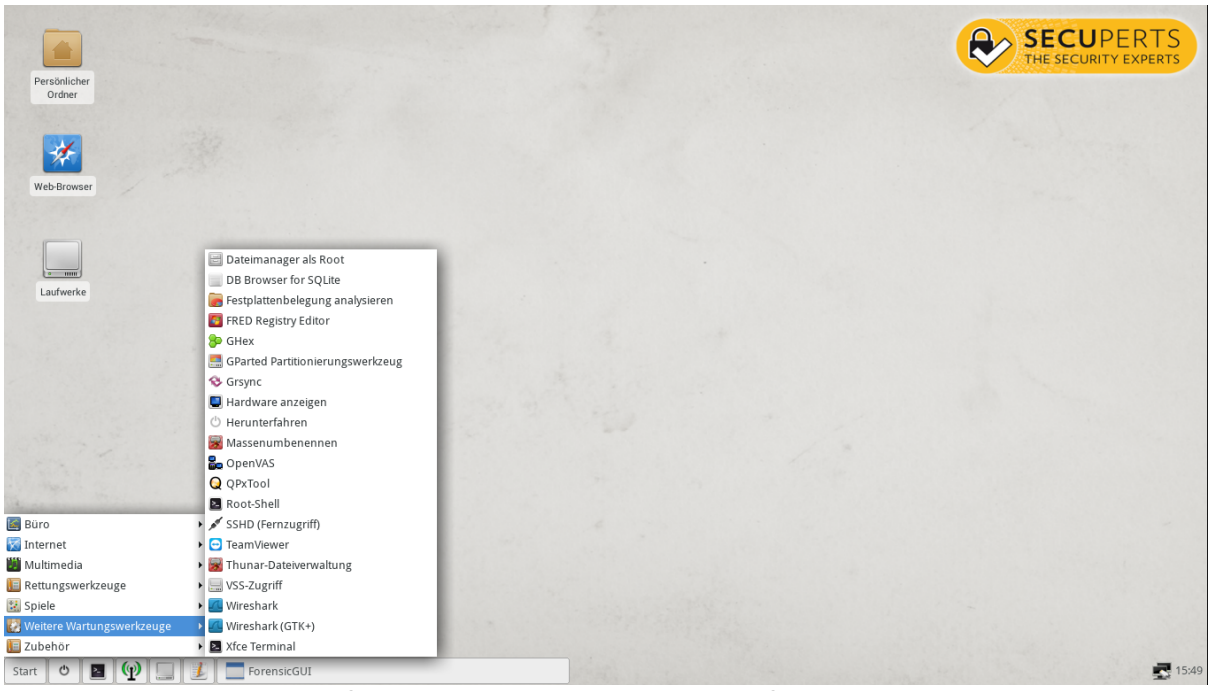
- **Festplattenforensik:** In dieser Kategorie finden Sie Programme für die Arbeit mit Festplatten, die

Datei- und Verzeichnis-Operationen einschließen. Dazu gehören die Wiederherstellung gelöschter Daten, der Zugriff auf Volumenschattenkopien, das Aufspüren von Schadsoftware und die Sortierung wiederhergestellter Dateien anhand ihrer Metadaten.

- **Zugriff auf Caches und History:** Hier erhalten Sie Zugriff auf die Zwischenspeicher vieler Programme wie diverser Webbrowser, auf die Email-Datenbanken von Outlook und die Datei- und Programmverläufe von Windows.
- **Netzwerk-Forensik:** Schneiden Sie Netzwerkverkehr mit, prüfen Sie, welche Rechner im Netz welche Dienste anbieten und spüren Sie verwundbare Geräte mit OpenVAS auf. Schließlich können Sie noch einen WLAN-Accesspoint aufspannen um beispielsweise den Netzwerkverkehr von Smartphones analysieren zu können.
- **Block-Geräte-Operation:** Hier finden Sie Werkzeuge für die Arbeit mit Festplatten auf Blockebene, die Dateisysteme und den Typ gespeicherter Daten ignorieren. So können Sie Festplatten bitgetreu klonen, Images von Festplatten oder einzelnen Partitionen erstellen (auch von beschädigten Datenträgern) oder vorhandene Images bootfähiger Windows-Installationen (ohne Veränderungen) in der virtuellen Maschine Qemu starten. Die Funktion "Sicheres Löschen" stellt sicher, dass eine weitergegebene Festplatte keine sensiblen Daten mehr enthält

4.3 Programme im Startmenü

Im Startmenü der Taskleiste finden Sie weitere Programme für Alltagsaufgaben, Datenrettung, Datensicherung und einige Spiele zum Zeitvertreib während langwieriger Operationen. Teilweise stellen diese dieselbe oder eine ähnliche Funktionalität bereit wie die Programme im Assistenten. In solch einem Fall sollten Sie zunächst die Funktion im Assistenten nutzen, da hier die Funktionsweise meist besser erläutert wird.



Startmenü und Desktop des Forensik-Systems

- Büro: Textbetrachter (Abi-Word), PDF-Betrachter und Tabellenkalkulation.
- Internet: E-Mail-Client, InstantBird (Messenger), Web-Browser, Wicd Network Manager (Verwaltung der Netzwerkverbindungen).
- Multimedia: Audacious (Audioplayer), Daten brennen (mit Brasero oder xfburn),

Lautstärkeregelung, Ristretto-Bildbetrachter, VLC Media Player für Videos.
- Rettungswerkzeuge: Daten brennen, Daten retten, Festplatte nach VM Image, Kennwort neu, Partition retten, Platte klonen, Platte testen, QPhotoRec (Bilder retten), Rettungs-Image erstellen, sicher löschen Windows Shell zurücksetzen.
- Weitere Wartungswerkzeuge: Dateimanager als Root, DB Browser for SQLite, Festplattenbelegung analysieren, FRED Registry Editor, GHex, GParted Partitionierungswerkzeug, Grsync, Hardware anzeigen, Herunterfahren, Massenumbenennen, PartImage, Root-Shell, SSHD (Fernzugriff), TeamViewer, Thunar-Dateiverwaltung, VSS-Zugriff, Xfce-Terminal.
- Zubehör: Archivverwaltung, Bildschirmfoto, Bildschirmtastatur, CIFS- oder WebDAV-Freigaben einbinden, Dateiverwaltung, FileZilla, Installation auf USB-Laufwerk, KeePassX, Laufwerke freigeben, Midnight Commander, Mousepad, Netzlaufwerke, Taschenrechner, Terminal, VeraCrypt, VNC-Server starten, WLAN access point.

4.4 Updates

Das SecuPerts-Forensik-System prüft unmittelbar nach dem Start der grafischen Oberfläche und noch einmal zehn Minuten später, ob Aktualisierungen vorhanden sind. Wenn Sie in dieser Zeit keine Internetverbindung hergestellt haben, können Sie über den Menüpunkt "Zubehör > Suche nach Systemupdates" prüfen, ob Aktualisierungen vorhanden sind. Kleinere Kompatibilitäts- und Stabilitätsupdates werden in einer Form ausgeliefert, die im Arbeitsspeicher des laufenden Systems installiert wird und in der Regel weniger als eine Minute Downloadzeit benötigt. Größere Sicherheits- und Treiberupdates erfordern ein auf USB-Stick installiertes Forensik-System und einen Neustart zum Abschluss der Aktualisierungen. In jedem Fall werden Sie per Assistent durch den Update-Prozess geführt.

5 Die Werkzeuge des Forensik-Systems

5.1 Festplattenforensik

In dieser Kategorie finden Sie Programme für die Arbeit mit Festplatten, die Datei- und Verzeichnis-Operationen einschließen. Dazu gehören die Wiederherstellung gelöschter Daten, der Zugriff auf Volumenschattenkopien, das Aufspüren von Schadsoftware und die Sortierung wiederhergestellter Dateien anhand ihrer Metadaten.

5.1.1 Dateien wiederherstellen

Diese Funktion stellt Dateien her, auch wenn der Papierkorb des Laufwerkes geleert, eine Partition formatiert oder bei einer Festplatte die Partitionstabelle gelöscht wurde. Sie können die Suche auf einer Partition oder einer kompletten Festplatte durchführen. Grundsätzlich arbeitet die Funktion Dateisystem ignorant, das heißt sie findet vorhandene Dateien egal, ob diese im Dateisystem referenziert oder nach Löschen übrig geblieben sind. Auf lange Zeit im Einsatz befindlichen Festplatten kann die Menge der gefundenen Daten daher beinahe so groß werden, wie das ausgewählte Quelllaufwerk. Verwenden Sie in solchen Fällen immer ein Ziellaufwerk, welches größer als das Quelllaufwerk ist.

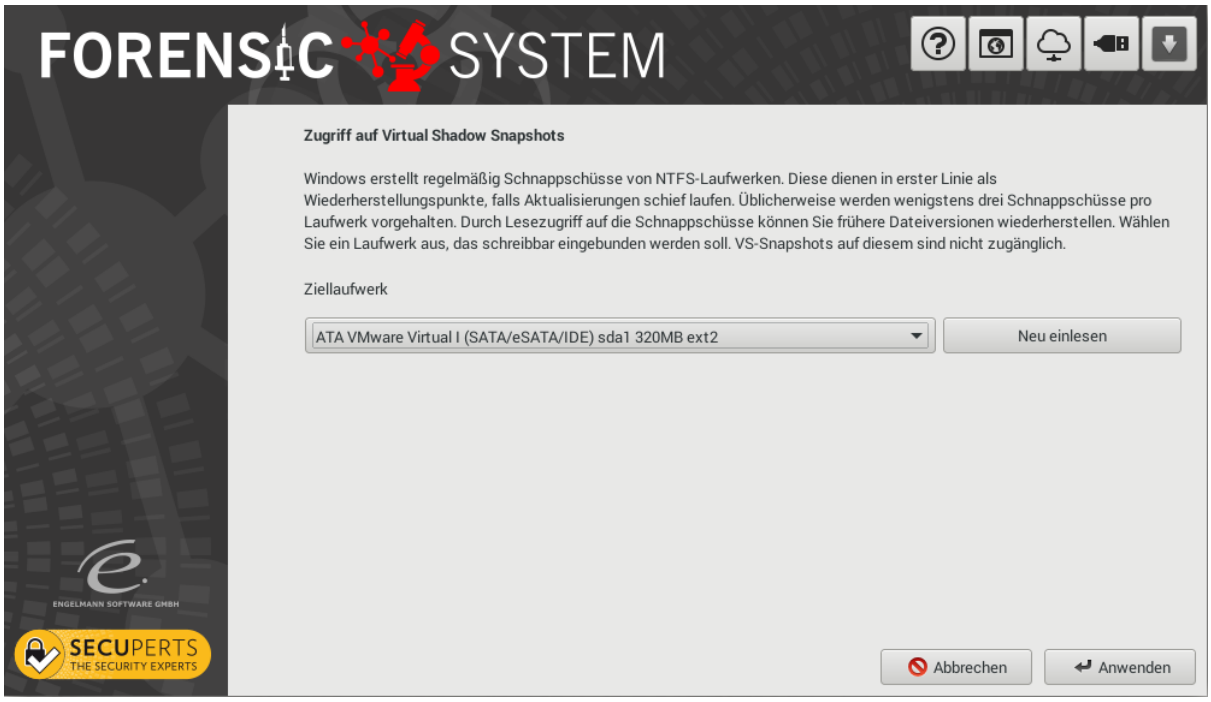
Dateien können auch bei beschädigten Dateisystemen wiederhergestellt werden

Soll lediglich auf Partitionen gesucht werden, kann das Ziellaufwerk auf derselben Festplatte liegen, allerdings raten wir aus Gründen der Performance hiervon ab. Bei der Suche auf kompletten Festplatten ist zwingend die Angabe eines Ziellaufwerkes auf einer anderen Festplatte (beispielsweise USB-Festplatte) möglich. Ist der zu untersuchende Datenträger beschädigt, empfehlen wir, diesen vorher auf einen unbeschädigten Datenträger zu klonen. Die Zeit für die Analyse hängt stark von Transferrate der Festplatte, aber auch der Geschwindigkeit Ihres Prozessors ab. Gehen Sie bei einst stark befüllten Laufwerken von etwa 10MByte/s aus - die Datenwiederherstellung einer Terabyte-Platte kann also mehr als einen vollen Tag in Anspruch nehmen.

Bei der Wiederherstellung selbst findet keine Sortierung statt, Dateien werden stur nach ihrer einstigen Blockadresse benannt. Sie können jedoch nach der Wiederherstellung die Funktion "Wiederhergestellte Dateien sortieren" verwenden, um Dateien anhand ihrer Metadaten zu sortieren.

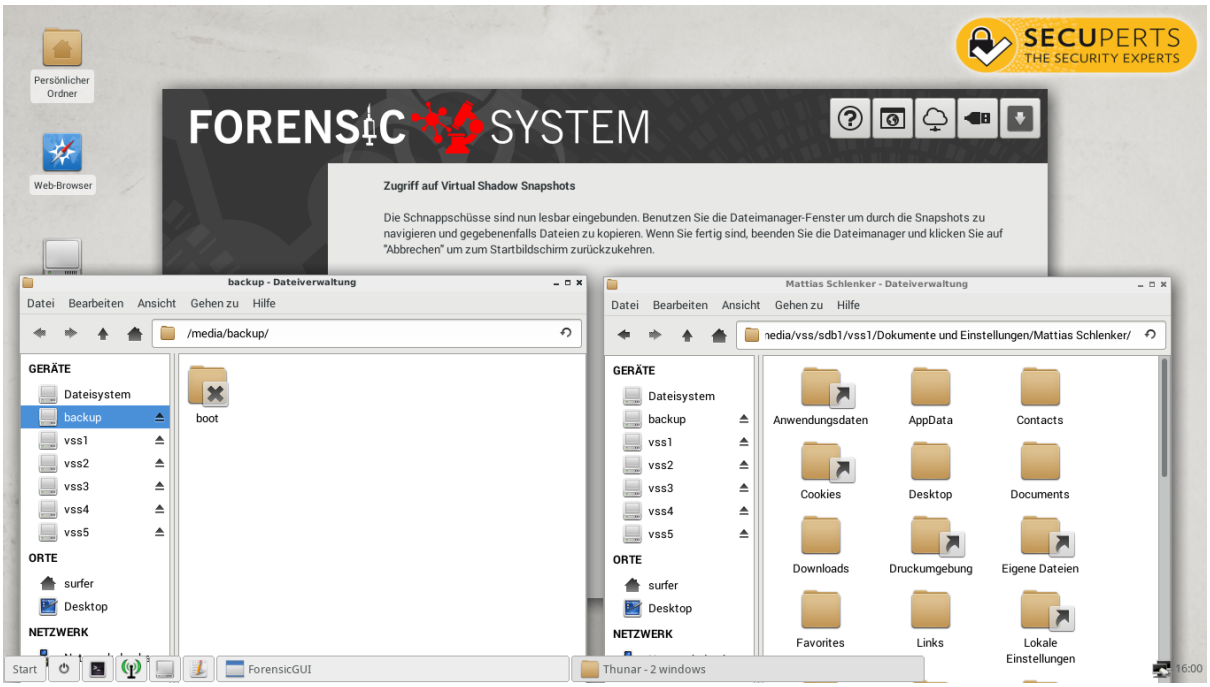
5.1.2 Zugriff auf Schattenkopien

Das NTFS-Dateisystem erlaubt die Erstellung sogenannter Schattenkopien. Dies sind Schnappschüsse des Dateisysteminhaltes im Moment der Erstellung der Schattenkopie. Üblicherweise werden Schattenkopien vor größeren Änderungen am System beispielsweise der Installation von Updates erstellt. Sie können diese jedoch auch manuell mit dem Befehl "vssadmin" aus der Windows-Kommandozeile erstellen. Wenn Sie regelmäßig Windows-Updates durchführen, erstellt Windows diese Schattenkopien typischerweise im Abstand von ungefähr einem Monat und hält wenigstens die letzten drei vor.



Vor dem Einbinden von Schattenkopien wählen Sie ein Laufwerk als Sicherungslaufwerk

Mit der Funktion "Zugriff auf Schattenkopien" geben Sie zunächst ein Laufwerk an, das als schreibbar eingebundenes Laufwerk für gerettete Daten dienen soll. Bei allen anderen (NTFS-) Laufwerken werden vorhandene Schattenkopien automatisch eingebunden. Falls Sie Dateien und Verzeichnisse mit dem aktuellen Stand vergleichen wollen, binden Sie die entsprechenden Laufwerke über das Werkzeug "Laufwerke" in der Taskleiste lesbar ein. Sie können nun in den Schattenkopien wie in jedem anderen eingebundenen Laufwerk stöbern und haben so die Möglichkeit, Dateien, die zwischen zwei Windows-Updates gelöscht oder geändert wurden in ihrer ursprünglichen Form wieder herzustellen.



Laufwerke mit Schattenkopien werden nur-lesbar eingebunden

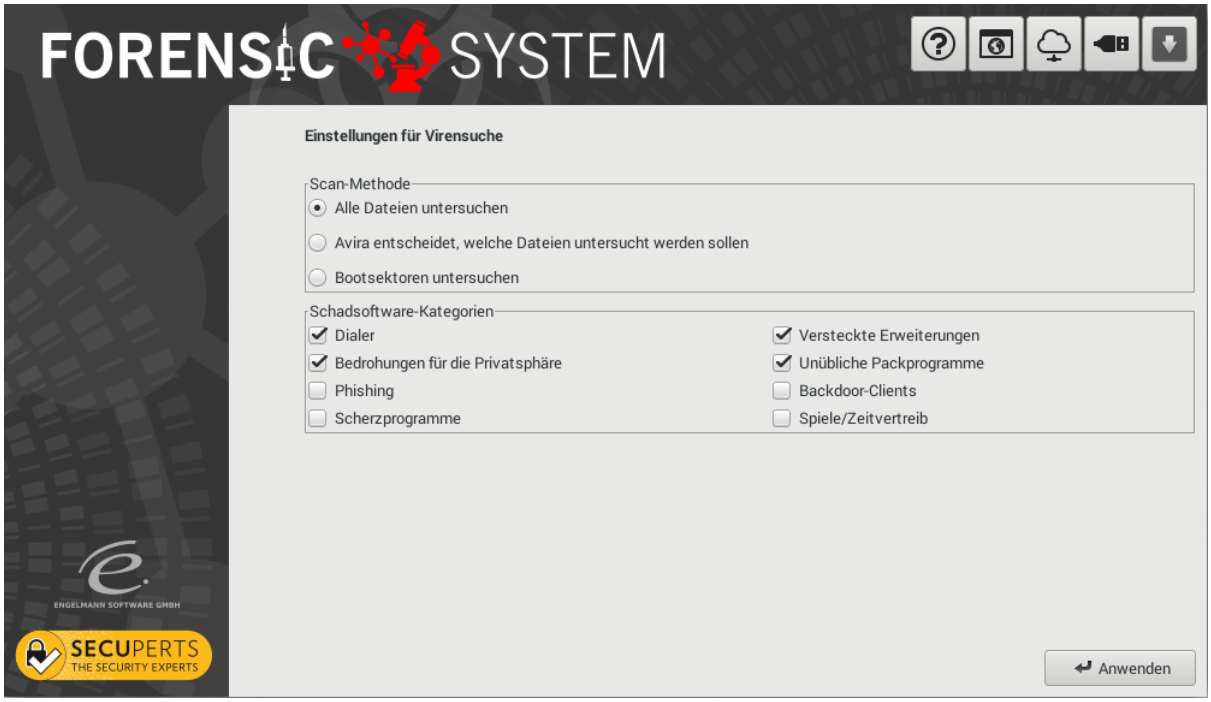
Sind Sie mit der Suche in den Schattenkopien fertig, klicken Sie auf "Abbrechen". Dies löst die Einbindung der Schattenkopien. Eventuell über das Programm "Laufwerke" eingebundene Partitionen müssen Sie manuell lösen. Dateimanager-Fenster, die Sie nicht mehr benötigen, schließen oder minimieren Sie selbst.

5.1.3 Schadsoftware aufspüren

Ein Problem für Antivirensoftware unter Windows ist, dass es Schadsoftware teilweise gelingt, die Antivirensoftware auszuschalten. Zudem finden viele Antivirenprogramme versteckte Fernwartungssoftware oder Spionageprogramme nicht zwingend, wenn diese in vielen Ländern beispielsweise zur Mitarbeiterüberwachung eingesetzt werden kann. Wenn Sie beispielsweise den Verdacht haben, dass ein Kollege Ihnen Spionagesoftware untergeschoben haben könnte, nutzen Sie diese Funktion.

Wählen Sie die auf Schadsoftware zu untersuchenden Laufwerke

Im ersten Bildschirm wählen Sie die zu untersuchenden Laufwerke aus, ein Klick auf "Einstellungen" bringt Sie zur Möglichkeit, die Suche einzuschränken oder zu erweitern. Die Kategorie "Scherzprogramme" enthält beispielsweise Signaturen von Programmen, die gerne von Kollegen benutzt werden, um Windows-Anwender in den Wahnsinn zu treiben.



In den Einstellungen können Sie die Suche auf weitere Programmtypen ausdehnen

Eine Löschung von Schadsoftware ist nicht möglich. Dies entspricht dem Wesen des

Forensiksystemes, das versucht, ohne Änderungen am untersuchten System zu arbeiten. Um Schadsoftware zu löschen, nutzen Sie bitte das Live-System eines Herstellers von Antivirensoftware oder das

5.1.4 Wiederhergestellte Dateien sortieren

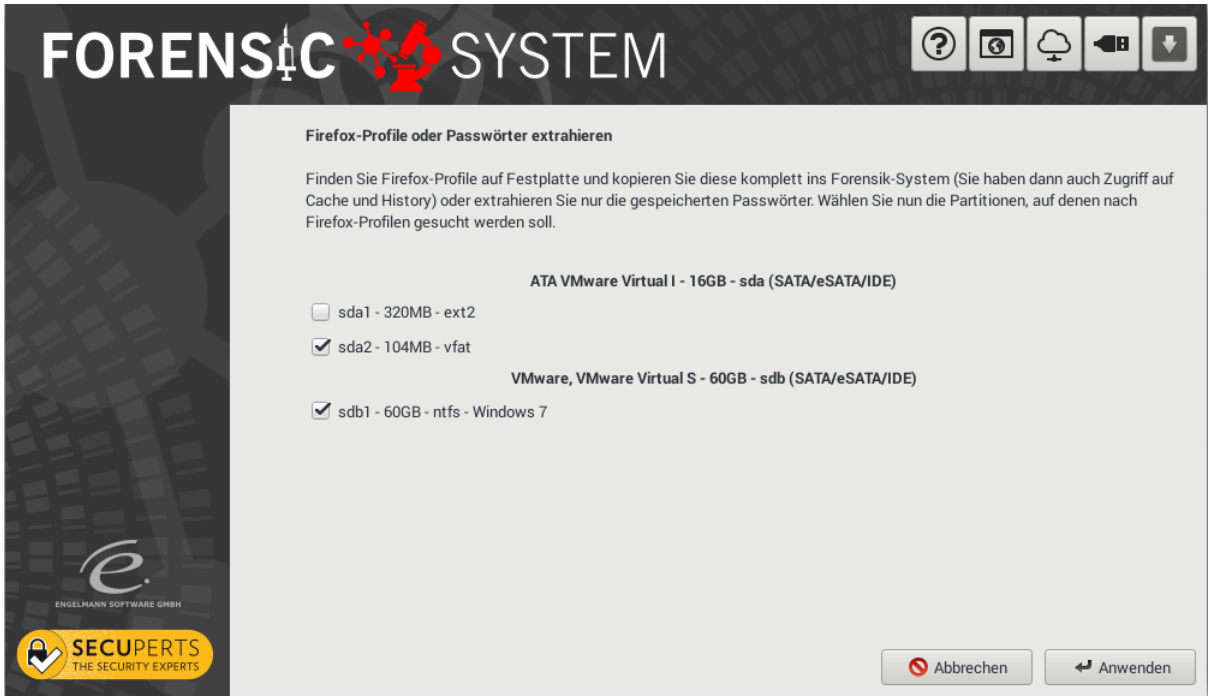
Nutzen Sie diese Funktion beispielsweise nach der Datenrettung, wenn Dateinamen verloren gegangen sind oder bei der Analyse von Cache-Ordnern, bei denen Dateinamen nicht auf Dateiinhalte hinweisen. Die Sortierfunktion nutzt in den Dateien enthaltene Metadaten.

5.2 Zugriff auf Cache-Speicher und History

Viele Programme legen Verläufe und temporäre Dateien in Datenbanken und Ordnern auf der Festplatte ab. Mit dieser Programmkategorie erhalten Sie Zugriff auf die Zwischenspeicher vieler Programme wie diverser Webbrowser, auf die Email-Datenbanken von Outlook und die Datei- und Programmverläufe von Windows.

5.2.1 Zugriff auf Firefox-Profile

Firefox speichert seine Einstellungen in Javascript-Dateien, SQLite-Datenbanken und Cache-Ordnern. Der einfachste Weg, auf ein Firefox-Profil zuzugreifen ist das Kopieren des gesamten Profils oder einiger Datenbanken in das Firefox-Profil des Live-Systems. Dieses Werkzeug automatisiert den Vorgang, indem es nach Firefox-Profilen sucht und auch das Kopieren automatisiert. Nach abgeschlossener Suche und Auswahl des Profils können Sie entscheiden, entweder nur die Passwortliste oder das komplette Profil - inclusive Such-Historie, Surf-Historie und Lesezeichen ins laufende Forensiksystem zu kopieren.



Das Forensik-System automatisiert die Suche nach Firefox-Profilen

Sollen anschließend Passwörter wiederhergestellt werden, können Sie unter "Einstellungen > Sicherheit

> Gespeicherte Zugangsdaten" Einblick in die Passwortliste nehmen. Wollen Sie lange Listen von Passwörtern exportieren (beispielweise für den Umzug auf einen anderen Computer), installieren Sie das Firefox-Add-On "Password Exporter".

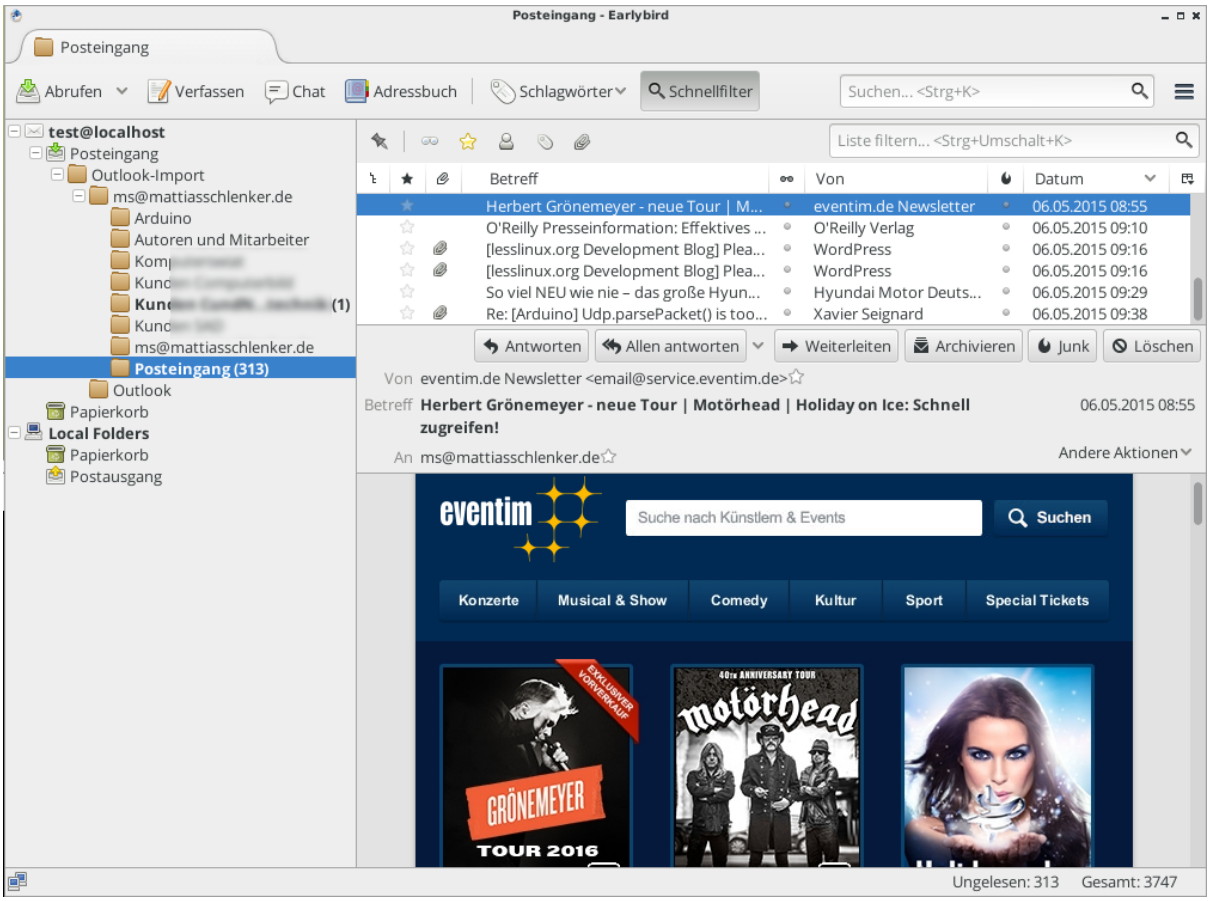
5.2.2 Windows-Jumplists

Ab Windows Vista führt das Betriebssystem aus Redmond Listen von Datei- und Programmzugriffen in sogenannten Jumplists. Diese Jumplists können Sie mit dem SecuPerts-Forensik-System auslesen und bringen so in Erfahrung, mit welchen Programmen und Dateien jemand gearbeitet hat, der unbefugt Ihren Rechner benutzt und so potentiellen Zugriff auf private Dateien erlangt hat.

Die erstellten Listen sind in einem einfachen textbasierten Tabellenformat und können außerhalb des Forensiksystems mit jeder beliebigen Tabellenkalkulation geöffnet werden. Beachten Sie bitte, dass es je nachdem, ob die Windows-Systemzeit auf lokale Zeit oder UTC (universelle Weltzeit) eingestellt ist, zu Zeitdifferenzen kommen kann. Nehmen Sie daher eine kleine Folge von Dateien, bei denen Sie den Zugriffszeitpunkt recht genau kennen als Anhaltspunkt, um eventuelle Abweichungen festzustellen.

5.2.3 Outlook-Mailboxen wiederherstellen

Outlook speichert seine Mailboxen in proprietären Datenbankformaten, die prinzipiell nur mit Outlook geöffnet werden können. Glücklicherweise haben Forensiker das verwendete Datenbankformat analysiert und eine Möglichkeit geschaffen, Outlook-Mailboxen in das gängigere Mbox-Format zu konvertieren, welches beispielsweise auch Mozilla Thunderbird verwendet. So können Sie auf die Inhalte von Outlook-Mailboxen zugreifen, ohne ein Outlook-Profil anlegen und Dateien umkopieren zu müssen.



Outlook-Mailboxen werden konvertiert und in Thunderbird geöffnet

Bitte beachten Sie, dass mitunter der temporäre Speicherplatzbedarf recht hoch ist. In diesem Fall warnt das Forensik-System vor Platzmangen. Installieren Sie das Forensiksystem dann auf einen (größeren) USB-Stick und wiederholen Sie den Vorgang nach einem Neustart. Wenn nur Titel gefunden werden und Emails selbst nur teilweise oder gar nicht angezeigt werden, dann liegt das an der Einstellung, dass nur zum Lesen angeklickte Emails vollständig heruntergeladen wurden. Diese Einstellung nehmen besonders Nutzer mobiler Geräte wie Notebooks oder Tablets gerne vor, um das Downloadvolumen bei teuren Mobilfunk oder langsamen WLAN-Verbindungen gering zu halten. Da die Emails in diesem Fall noch auf dem Server lagern ist keine weitere Analyse lokaler Dateien mehr möglich.

5.2.4 Browser und Chatverläufe

Wenn Browser und Chatprogramme ihre Verläufe in Datenbankdateien speichern, finden und analysieren Sie diese mit diesem Werkzeug. Gegenwärtig unterstützt es die Verläufe von Firefox, Chrome und Internet Explorer, sowie die Chat-Verläufe von Skype. Aufbereitet werden die Daten in Formaten, die gängige Tabellenkalkulationen lesen können. Da sich die Formate mit neuen Versionen ändern, sollten Sie von Zeit zu Zeit auf Aktualisierungen des Forensik-Systems prüfen.

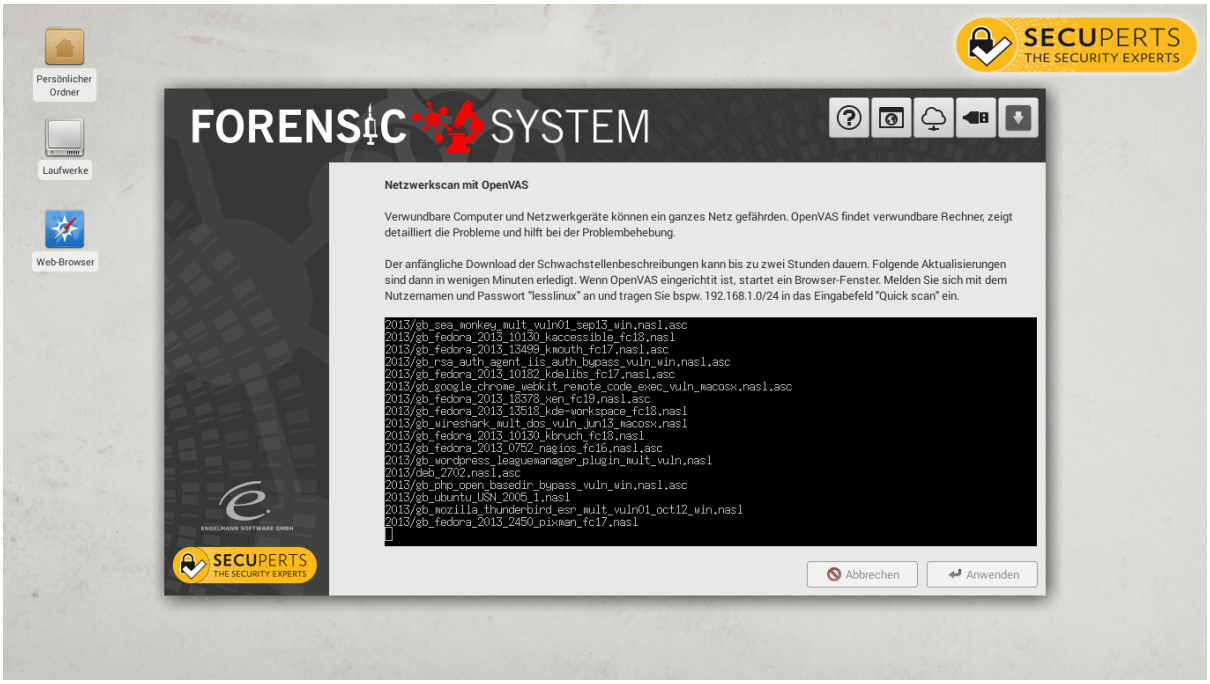
Sollten sich Formate dramatisch geändert haben, können Sie im Profilordner der jeweiligen Anwendung nach großen Dateien suchen und mit dem Kommandozeilenbefehl "file" überprüfen, ob es sich um eine SQLite-Datenbank handelt. Ist dies der Fall, können Sie die Tabellen der Datenbank mit dem "SQLite DB Browser" (im Startmenü unter "Zubehör") analysieren.

5.3 Netzwerkforensik

Wissen Sie, was Ihr Netzwerk so treibt? Vielleicht ist die IP-Webcam ja Teil eines DDoS-Botnetzes oder der Fernseher versucht Server zu knacken? Seit Botnetze wie Mirai auch Windows-PCs als Sprungbrett zu IoT-Geräten nutzen, ist es wichtig, den Überblick im Netzwerk zu behalten, Schwachstellen zu kennen und verwundbare Geräte zu identifizieren.

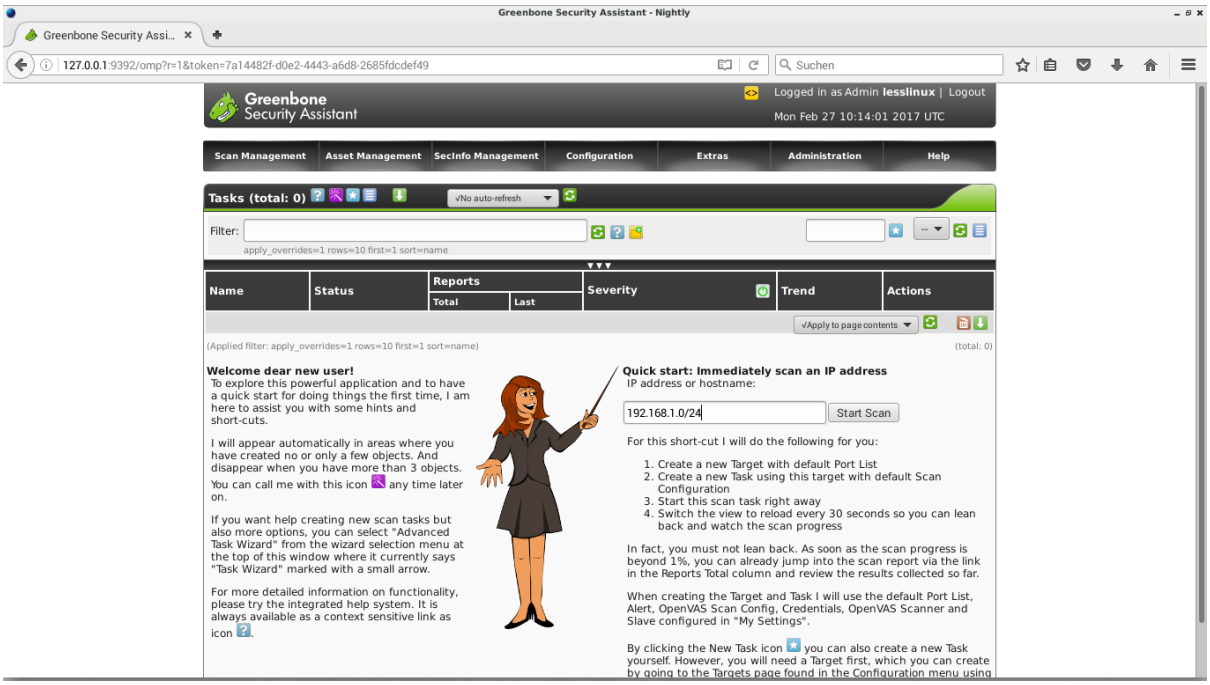
5.3.1 OpenVAS

Mit dem "Open Vulnerability Assessment Scanner" inventarisieren Sie Ihr Netzwerk und spüren Sie verwundbare Geräte im Heimnetzwerk auf. OpenVAS sucht zunächst nach Geräten im Netzwerk, führt dort einen Portscan durch und prüft dann anhand von Datenbanken, ob die Dienste verwundbar sind. Der Grad der Prüfungen kann unterschiedlich eingestellt werden, so sind beispielsweise echte Penetrationstests möglich. OpenVAS ist relativ aufwendig zu konfigurieren, doch diese Arbeit erledigen beim Forensik-System spezielle Skripte.



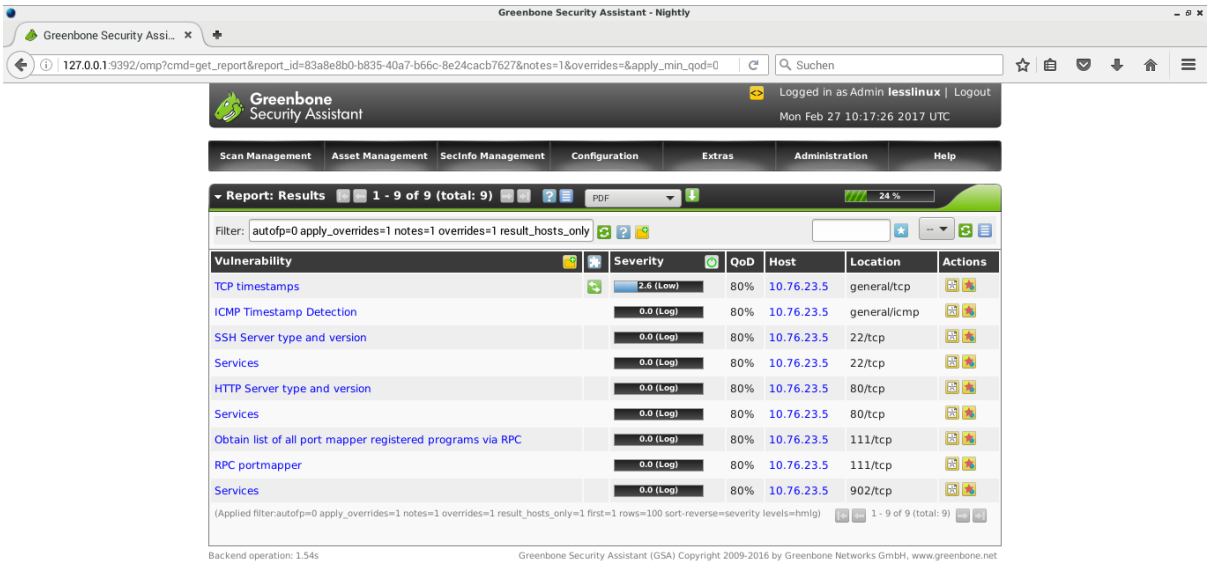
Die Ersteinrichtung von OpenVAS kann mehrere Stunden dauern

Die Systemanforderungen von OpenVAS sind verhältnismäßig hoch: Die Installation aus USB-Stick ist Voraussetzung. Da beim ersten Start rund 1,5 Gigabyte Schwachstellendefinitionen heruntergeladen werden und in eine Datenbank eingepflegt werden, sollte ein schneller USB-Stick mit Schreibraten von 15MB/s oder höher verwendet werden. Beim ersten Start ist Geduld angesagt: Der initiale Aufbau der Schwachstellendatenbanken kann mehrere Stunden dauern. Bei künftigen Starts sind für die Aktualisierung der Schachstellendatenbanken typischerweise zehn bis 30 Minuten einzuplanen.



Starten Sie zunächst einen "Quick scan" über einen Rechner oder das gesamte Netzwerk

Ist OpenVAS fertig konfiguriert und die Datenbanken aufgebaut, startet Firefox mit dem Webfrontend von OpenVAS. Melden Sie sich hier mit dem Nutzernamen "lesslinux" und dem Passwort "lesslinux" an. Sie können dann im Feld "Quick Scan" rechts entweder einen einzelnen Rechner oder ein komplettes Subnetz scannen. Für den ersten Scan empfehlen wir, das komplette Subnetz zu verwenden. Wenn Ihr Router die IP-Adresse "192.168.1.1" verwendet, ist als Subnetz beispielsweise in der Regel "192.168.1.0/24" einzutragen. Ist das Subnetz unbekannt, können Sie im Terminal den Befehl "ifconfig" verwenden, um Ihre aktuelle IP-Adresse zu ermitteln. Selbstverständlich ist sicherzustellen, dass Ihre Geräte mit dem Netzwerk verbunden sind, schalten Sie Smart-TVs also ein und spielen Sie beispielsweise auf Tablets YouTube-Videos ab.

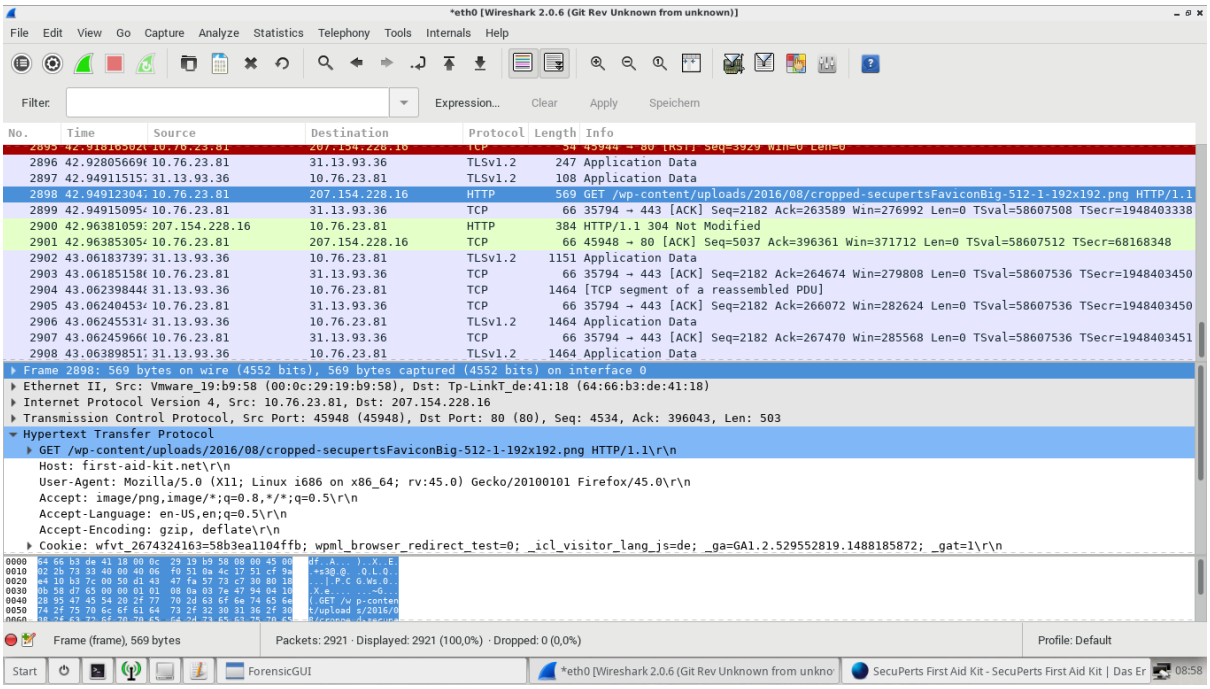


Gefundene Schwachstellen sortiert OpenVAS nach Grad der Bedrohung

Bereits während des Scans können Sie über die Tasktabelle auf die teilweise vorhandenen Protokolle zugreifen, die nach Risikograd sortiert sind. Bei den gefundenen Schwachstellen handelt es sich teilweise um "False Positives", denn in Standardeinstellungen versucht OpenVAS keine "echten" Angriffe. Wenn Sie sicherstellen können, dass Abstürze des kompletten Systems oder einzelner Dienste zu verschmerzen sind, starten Sie einen neuen Scan und wählen Sie bei der Taskangabe "Full and very deep ultimate". Häufig kommt es vor, dass der vermeintlich verwundbare Dienst bereits gepatcht wurde, allerdings kann der "echte Angriff" eben auch Abstürze zur Folge haben, wenn dies nicht geschehen ist.

5.3.2 Wireshark

Verwenden Sie Wireshark, um den Netzwerkverkehr einzelner Geräte oder des gesamten Netzwerkes mitzuschneiden, beispielsweise um herauszufinden, welche Daten der Smart TV so verschickt und empfängt. Das Mitschneiden von Netzwerkverkehr sollte über die Ethernetkarte stattfinden, zudem müssen Ethernetkarte und Switch beim Umschalten in den Promiscous Mode zusammenspielen und eventuell vorhandene Accesspoints dürfen WLAN-Verkehr nicht separat filtern. Gelingt dies nicht, gehen Sie zum vierten Programm in diesem Abschnitt, wo erklärt wird, wie Sie einen WLAN-Accesspoint aufspannen, der als Brücke zwischen Ethernet- und WLAN-Schnittstelle dient.



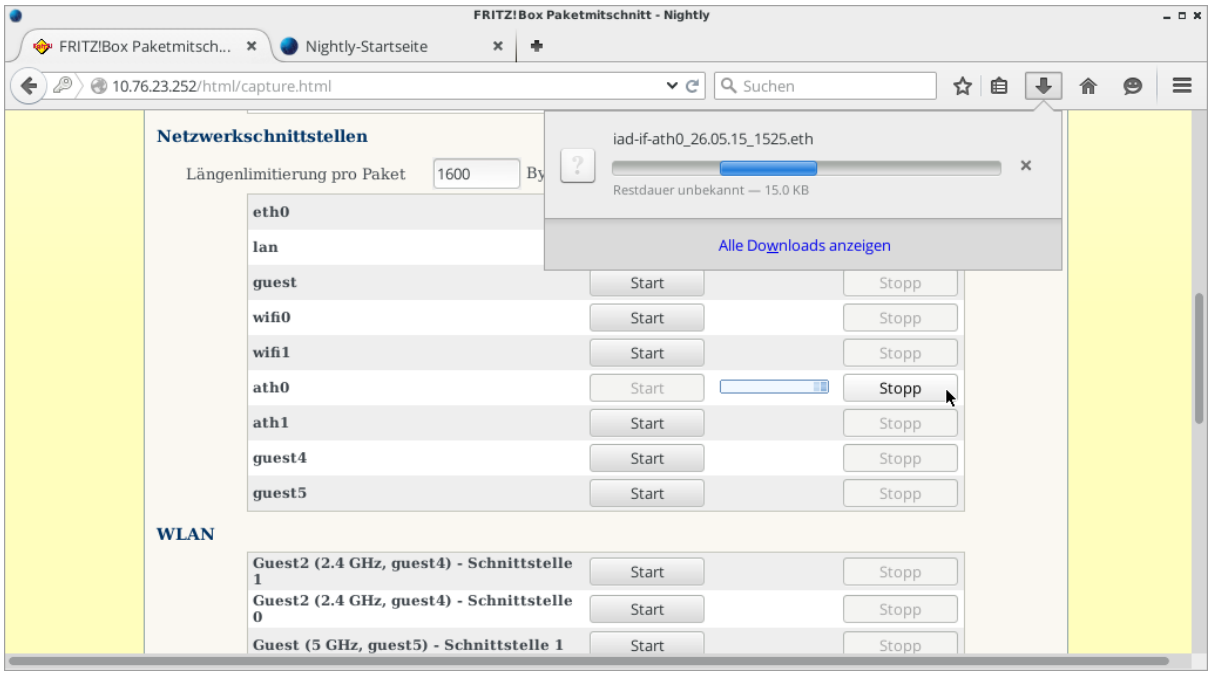
Verwenden Sie Wireshark um Netzwerkverkehr mitzuschneiden oder auszuwerten

Um einen Live-Paketmitschnitt zu starten, klicken Sie auf die grüne Haifischflosse. Während des Mitschneidens können Sie einzelne Netzwerkpakete anzeigen lassen, nach Quelle, Ziel oder verwendeten Protokollen filtern lassen. Nach abgeschlossener Arbeit haben Sie die Möglichkeit, den gesamten Mitschnitt oder gefilterte Teile davon zu speichern.

Längere Paketmitschnitte empfehlen wir, nicht in Wireshark vorzunehmen. Nutzen Sie dafür das Programm tcpdump, beispielsweise mit

tcpdump -i eth0 -w /tmp/dump.pcap

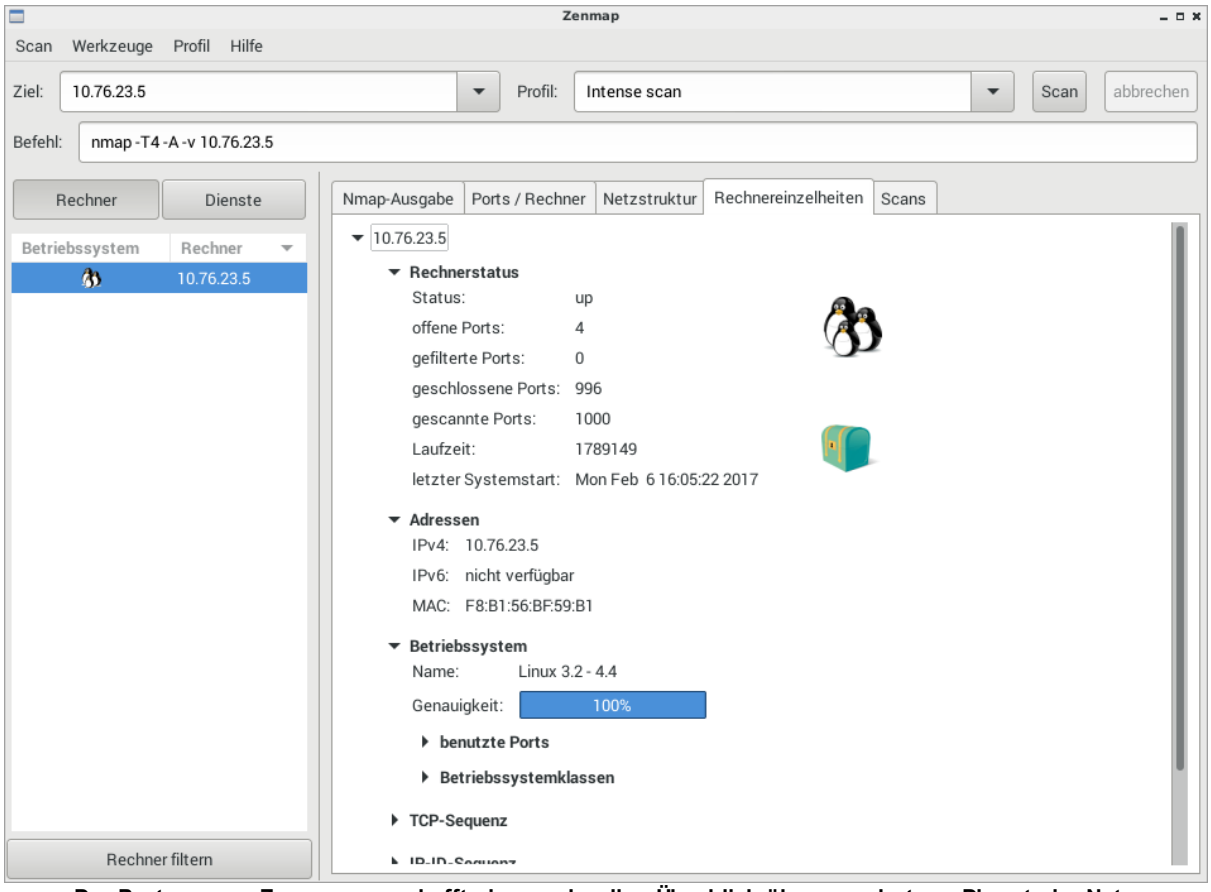
um eine Binärdatei mit dem Netzwerkverkehr zu erstellen. Auch viele DSL-Router wie AVMs Fritzbox und sämtliche OpenWRT basierte Router haben tcpdump bereits an Bord und bringen teils Webinterfaces mit, um Mitschnitte auf einzelne Hosts oder ein bestimmtes WLAN-Interface einzuschränken. Die damit erstellten Mitschnitte können Sie anschließend in Wireshark laden und dort analysieren.



Viele DSL-Router bieten eigene Werkzeuge für längere Traffic-Mitschnitte

5.3.3 Zenmap

Praktisch der kleinere Bruder von OpenVAS ist Zenmap, ein grafisches Frontend für den Portscanner Nmap. Größter Vorteil von Zenmap ist, dass dieses Programm sofort einsatzbereit ist und kein langwieriges Herunterladen von Schachstellendatenbanken erfordert. Dafür scannt Zenmap nur auf offene Ports und angebotene Dienste und kann keine Penetration Tests durchführen. Dennoch gibt Zenmap einen guten Überblick über im Netz anwesende Rechner und bereitgestellte Dienste.

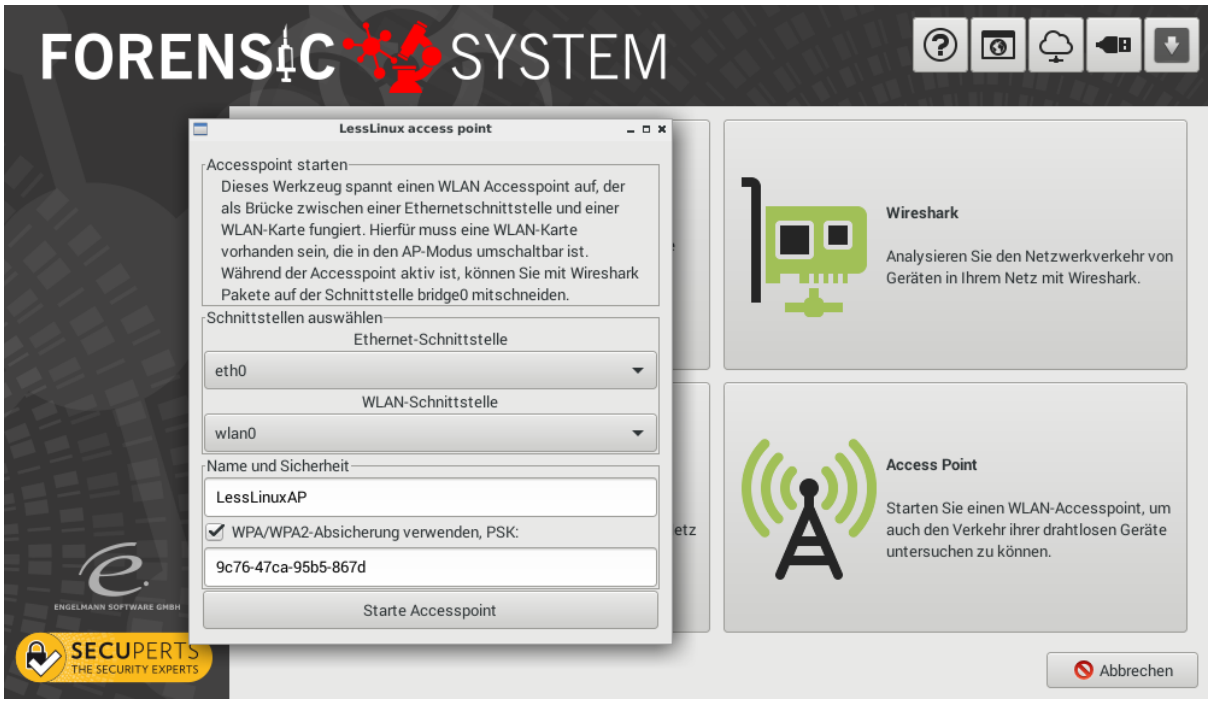


Der Portscanner Zenmap verschafft einen schnellen Überblick über angebotene Dienste im Netz

Starten Sie einen Scan, indem Sie in das Feld "Ziel" entweder eine IP-Adresse wie "192.168.1.1" oder ein Subnetz "192.168.1.0/24" eintragen. Lassen Sie die weiteren Einstellungen für den ersten Scan unverändert und klicken Sie auf "Scan". Scans über ganze Netze dauern in der Regel fünf bis zehn Minuten, Scans einzelner Hosts sind in weniger als 30 Sekunden abgeschlossen. Nach abgeschlossenem Scan können Sie links in der Leiste auf "Rechner" klicken, um sich die gefundenen Geräte anzeigen zu lassen. Klicken Sie einen Rechner an und lassen Sie mit dem Reiter "Rechnereinzelheiten" die Details dieses Netzwerkgerätes anzeigen.

5.3.4 Accesspoint

Ist aus technischen Gründen kein Mitschnitt mit Wireshark möglich, können Sie der Funktion "WLAN Accesspoint" einen Accesspoint aufspannen, der als passive Brücke zwischen Ethernet und WLAN dient und das Auslesen des Traffics verbundener Geräte an der Schnittstelle "bridge0" ermöglicht. Um den Accesspoint aufspannen zu können, sollte Ihr Computer in dieser Sitzung noch nicht als Client mit einem Funknetzwerk verbunden gewesen sein, war er das, starten Sie einfach neu. Steht die Verbindung über das Ethernetkabel, können Sie den Accesspoint anschalten.



Mit dem integrierten Accesspint scannen Sie auch Netzwerkverkehr von Rechnern im WLAN

Klappt die Verbindung des Endgerätes mit dem Accesspoint nicht, probieren Sie es erneut ohne Verschlüsselung: Nicht jeder WLAN-Chipsatz für Endgeräte unterstützt im Accesspoint-Modus Verschlüsselung. Ist der Accesspoint nicht sichtbar, kann es an einem Chipsatz liegen, der gar keine Accesspoint-Funktionalität bietet. In solch einem Fall sollten Sie ein anderes Notebook oder einen USB-WLAN-Stick ausprobieren.

5.4 Blockgeräte-Operationen

In dieser Programmkategorie finden Sie Operationen auf "rohen" Blockgeräten, also Festplattenpartitionen oder ganzen Festplatten. Die hier vorgestellten Funktionen interessieren sich nicht für Partitionierung oder Dateisysteme, sie können demnach auch dazu genutzt werden, bei beschädigten Datenträgern Images oder Klone für eine weitere Analyse zu erstellen.

5.4.1 Datenträger-Abbild erstellen

Diese Funktion erstellt ein bitgetreues Abbild einer Partition oder einer kompletten Festplatte. Da defekte Blockbereiche intelligent ermittelt und nach Abschluss des Kopierens unbeschädigter Blöcke erneut probiert werden, ist auch die Erstellung von Images beschädigter Laufwerke möglich. Achten Sie beim Einbinden des Ziellaufwerkes darauf, dieses schreibbar einzubinden. Zudem sollte großzügig freier Speicher vorhanden sein, da die bitgetreuen Images nur Blöcke aussparen, die Nullbytes enthalten. Das Laufwerk, von dem ein Image erstellt werden soll, darf nur-lesbar eingebundene Partitionen enthalten. Dies ist zwar für die Geschwindigkeit beim Kopieren etwas ungünstig, gefährdet aber nicht die Integrität des Ergebnisses.

Die Abbild-Funktion erstellt Images von Partitionen oder kompletten Laufwerken

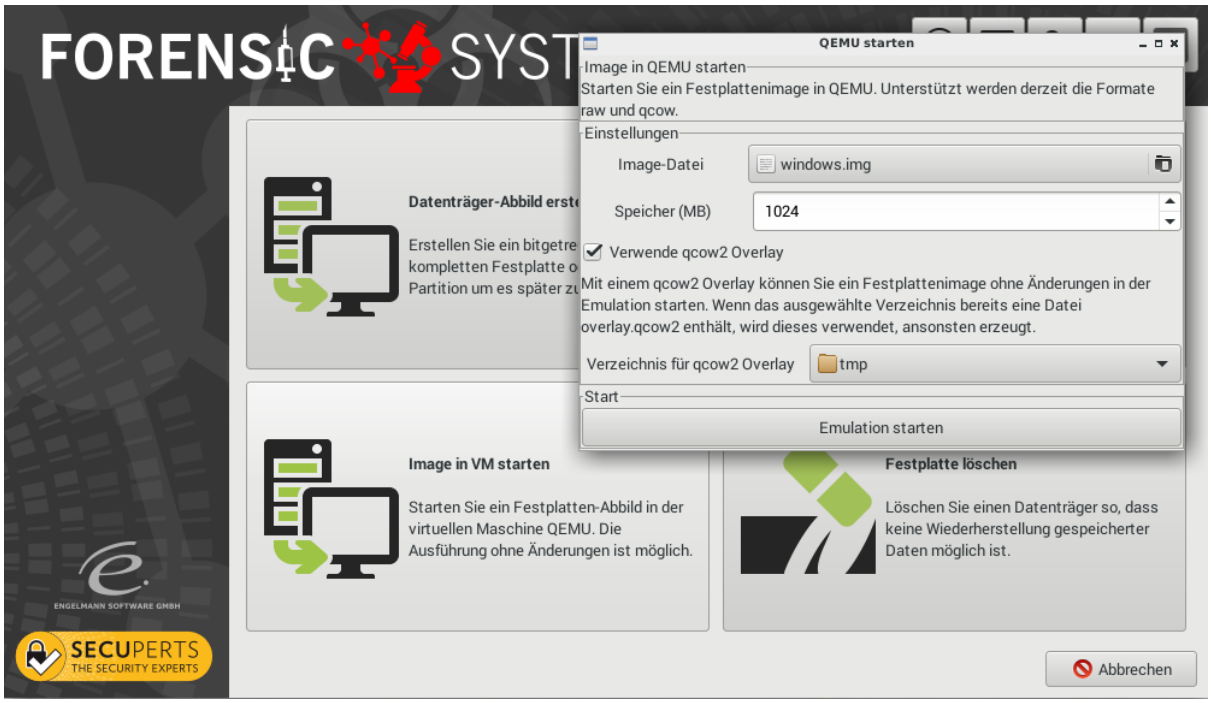
Erstellen Sie das Abbild einer einzelnen Partition, wenn Sie später mittels Qphotorec Daten von dieser retten wollen oder Sie das Image einbinden wollen, um per Dateisystem auf gespeicherte Daten zuzugreifen. Erstellen Sie ein Image einer kompletten Festplatte, wenn das Image später bootfähig sein soll, beispielsweise in einer virtuellen Maschine oder Sie planen, das Image einer beschädigten Festplatte auf eine neue Festplatte zu übertragen.

5.4.2 Festplatte klonen

Mit diesem Programm klonen Sie ein Festplatte eins zu ein auf eine andere Festplatte. Für beschädigte Blöcke gilt dasselbe wie bei der Erstellung eines Abbildes. Die Zielplatte muss gleich groß oder größer als die Quellplatte sein. Nach dem Klonen einer kleineren auf die größere Festplatte können Sie mit Werkzeugen wie Gparted Partitionen verschieben oder strecken.

5.4.3 Image in VM starten

Starten Sie das Abbild einer kompletten Festplatte in der virtuellen Maschine Qemu. Hierbei kann ein Overlay-Abbild verwendet werden, in dem Schreibzugriffe abgefangen werden. Dies bedeutet, dass die Integrität des unterliegenden Abbildes gewahrt bleibt. Bitte beachten Sie, dass das Netzwerk aktiviert ist. Wollen Sie ohne Netzwerk starten, verwenden Sie bitte qemu in der Kommandozeile.



Festplattenimages mit Bootsektor können Sie in Qemu direkt starten

Da die Hardware der virtuellen Maschine mitunter erheblich von der Hardware des Computers abweicht, startet nicht jedes Betriebssystem einwandfrei. Problematisch ist der Start von Windows XP und Server 2003. Windows Vista sowie Windows Server 2008 oder höher starten ohne Probleme. Die meisten Linux-Systeme ebenfalls, allerdings mitunter mit Grafik- oder Netzwerkproblemen.

5.4.4 Festplatte löschen

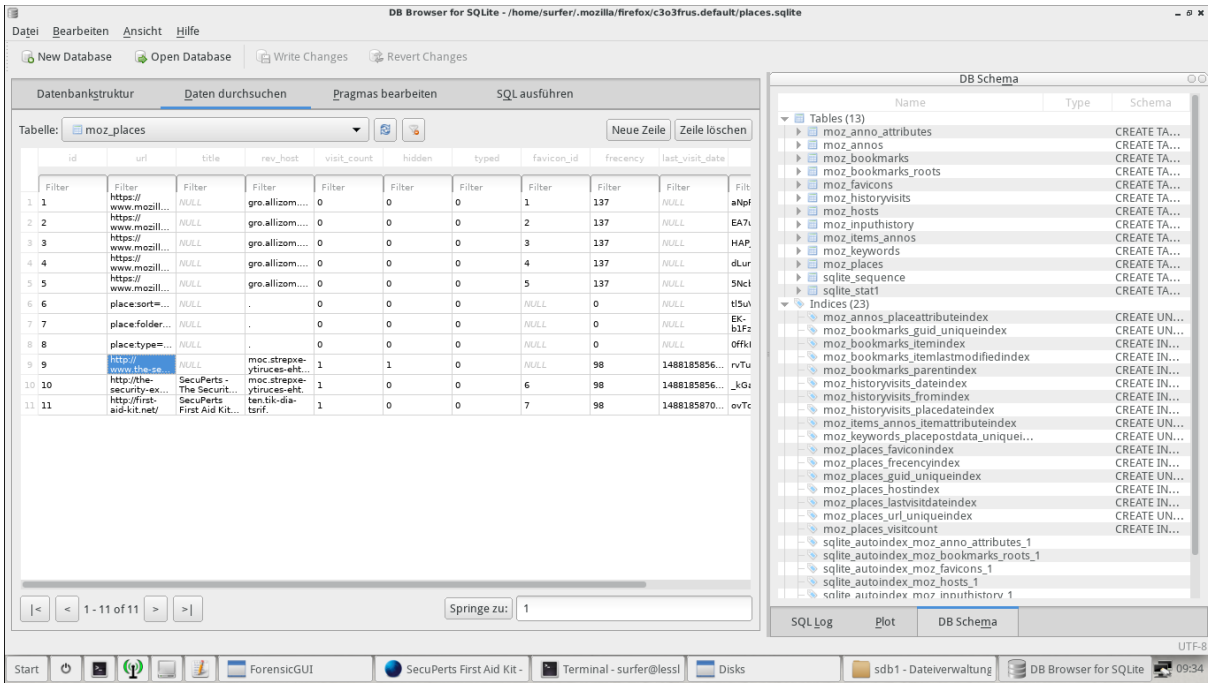
Wenn Sie eine Festplatte weitergeben oder einen Computer verkaufen wollen, ist es sinnvoll, vor der Formatierung oder Neuinstallation die Festplatte komplett zu säubern. Das gilt auch für Datenträger, die bei nach Forensikinstrumenten viele sensible Daten enthalten: Gerade Copy-on-Write-Dateisysteme wie NTFS behalten Daten auch, wenn man einzelne Dateien zuerst überschreibt. Bei der Löschung von SSDs wird nach dem einfachen Überschreiben mit Nullbytes ein TRIM vorgenommen, was künftige Schreibvorgänge erheblich beschleunigt.

6 Nützliche Tools in Menü und Kommandozeile

Nicht jedes hilfreiche Werkzeug kann im Assistenten gestartet werden. Ein Blick in das Startmenü zeigt einige Perlen. Weitere Tools verstecken sich auf der Kommandozeile.

6.1 SQLite Datenbank-Browser

Verläufe und Passwort-Datenbanken speichern viele Programme in der freien SQLite-Datenbank, meist in Version 3.x. Datenbanken dieses Formates können Sie mit dem SQLite Datenbank-Browser öffnen. Sie finden ihn im Anwendungsmenü unter "Zubehör > DB Browser for SQLite". Datenbanken können Sie entweder über "Datei öffnen" anzeigen oder per Drag&Drop ins Fenster des Programms.



Der SQLite-Browser zeigt das weit verbreitete SQLite-Datenbankformat übersichtlich an

6.2 Skype-Logs

Auch Skype speichert Adressbuch und Chatlogs in SQLite3-Datenbanken. Komfortabler als die Zusammenführung der Tabellen oder der Suche im generischen Datenbankbrowser ist die Verwendung eines speziell entwickelten Programmes, das die Daten aufbereitet. Hierfür ist Skype Xtractor des Forensik-Systems DEFT an Bord, das als klassisches Kommandozeilenwerkzeug unter Angabe des Pfades der Datei "main.db" aufgerufen wird.

```
cd /usr/share/skype_xtractor
python skype.py -o /tmp/skype /pfad/zur/main.db
```

Geben Sie den zusätzlichen Parameter "-C" an, um auch Chatsyncs zu erstellen. Im Ordner "/tmp/skype" können Sie anschließend über HTML-Dateien auf die Skype-Verläufe zugreifen.

6.3 Netzlaufwerke verbinden

Mit dem Programm "Zubehör > CIFS- und WebDAV-Freigaben einbinden" können Sie CIFS-/SMB-Shares (Windows-Freigaben) oder WebDAV-Laufwerke (Internetlaufwerke) einbinden. So können Sie auch, wenn lokal zu wenig Speicher bereitsteht, Daten auf NAS oder Onlinespeicher sichern. Geben Sie die Share-Bezeichnungen im Format

https://webdav.provider/pfad/

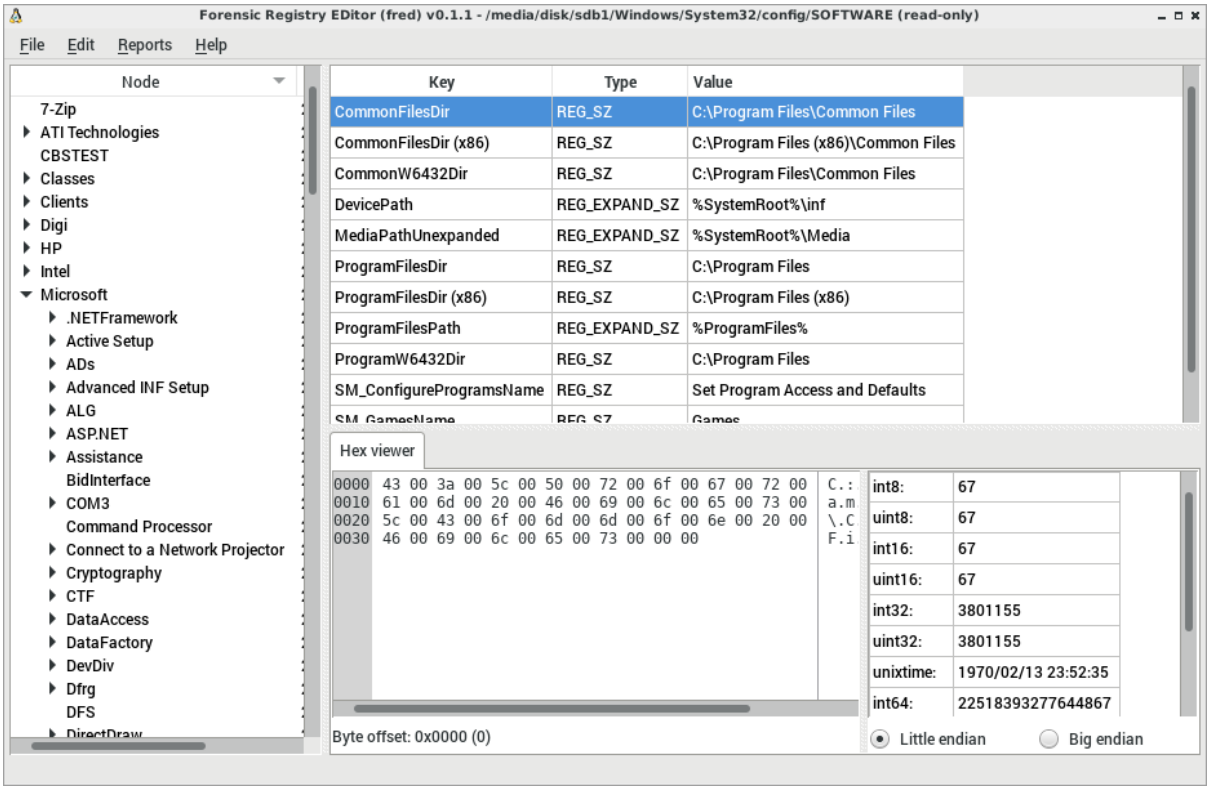
oder

cifs://192.168.0.24/sharename

an.

6.4 Fred Forensic Registry Editor

Unter "Weitere Wartungswerkzeuge > FRED Registry Editor" finden Sie einen weit fortgeschrittenen Registry-Editor, der bei der Analyse der Registry hilft. Im FRED-Fenster müssen Sie über den Menüpunkt "File > Open Hive" eine Registrierungsdatenbank auswählen. Sie finden diese unter "Windows/System32/config". Die Dateien "SOFTWARE" und "SYSTEM" enthalten dabei die gleichnamigen Zweige. "USERS" ist in den Heimatverzeichnissen der Nutzer abgelegt. Wie im Registry-Editor von Windows können Sie sich links durch die Struktur durchklicken und rechts Werte einsehen. Eine Schreibunterstützung ist aus Sicherheitsgründen nicht aktiv. Sie können diese jedoch über "Edit > Enable write support" einschalten und so auch Änderungen vornehmen



Mit dem forensischen Registry-Editor FRED analysieren Sie Windows-Registrierungen

7 Passwort-Werkzeuge

Verwenden Sie Passwörter, die nicht sicher genug sind? Die Antwort darauf bringt das Forensik-System mit Passwortknackern für Passwortdatenbanken und Netzwerkdienste mit. Deren typischer Einsatzzweck ist die Nutzung in Firmenumgebungen, wo Administratoren die Passwortsicherheit erhöhen wollen. Als Proben kommen Wörterbücher, Listen bekannt gewordener Passwörter (https://wiki.skullsecurity.org/ Passwords) und das Durchprobieren aller Zeichenkombinationen zum Einsatz. Hintergrund ist der, dass selbst ein „gutes“ Passwort, das durch Phishing abgegriffen wird, oft in anderen Kontexten verwendet wird. Administratoren können dann bei Treffern das Passwort sperren und die Vergabe eines sichereren erzwingen. Bitte beachten Sie, dass einige der enthaltenen Passwort-Knacker auf angepassten Linux-Systemen mit Unterstützung durch die Grafikkarte deutlich mehr Zeichenkombinationen pro Zeit ausprobieren können, es für den ernsthaften Einsatz in Firmenumgebungen demnach sinnvoll sein kann, eine separate Maschine mit leistungsstarker Grafikkarte nur zur Passwortprüfung aufzusetzen.

Achtung: Selbstverständlich dürfen Sie nur eigene Systeme untersuchen. Der Angriff auf Passwörter und Authentifizierungssysteme Dritter stellt einen Straftatbestand dar.

7.1 John the Ripper

Dieses Programm arbeitet mit Wortlisten und Brute-Force-Angriffen. Die Standardwortliste von John ("password.lst") enthält geleakte und gephishte Passwörter, sowie viele häufig im Englischen verwendete Worte. Sie können die Liste mit einem deutschen Wörterbuch oder den oben verlinkten weiteren Passwortlisten erweitern.

Der einfachste Einsatz von John ist möglich, wenn eine Passwortdatenbank die Passwort-Hashes im Klartext enthält. Öffnen Sie eine Rootshell und setzen Sie in dieser das Passwort des Administrators "root" mit dem Befehl "passwd". Verwenden Sie ein einfaches Passwort wie "test1" und starten Sie nun John:

```
cd /opt/john-1.8.0-jumbo-1/run
./john /etc/shadow
```

Ein wenig aufwendiger ist das Knacken von Windows-Passwörtern. Zunächst muss die SAM-Datei gefunden und ausgelesen werden. Hierfür dient das Programm "samdump2", der folgende Befehl extrahiert die Hashes in die Datei "/tmp/sam.txt"

```
samdump2 /media/disk/sda2/WINDOWS/system32/config/SAM /tmp/sam.txt
```

Anschließend ist John an der Reihe, in diesem Fall geben Sie ihm den Typ der Hashes an:

```
john -format=LM /tmp/sam.txt
```

Weitere Hinweise zur Verwendung von John finden Sie unter http://www.openwall.com/john/doc/EXAMPLES.shtml. Unter anderen kann John dafür verwendet werden, Passwörter von verschlüsselten Containern wie Truecrypt/Veracrypt oder LUKS zu knacken.

7.2 Ophcrack

Im Gegensatz zu John arbeitet Ophcrack mit sogenannten Regenbogentabellen, welche die Berechnung von Hashwerten abkürzen und letztlich durch die Suche in Datenbanken ersetzen. Diese Hashtabellen können je nach abgedeckten Passwortlängen und Zeichensätzen mehrere Terabyte groß sein. Die Hashtabellen sollten Sie auf einer schnellen Festplatte oder besser SSD ablegen. Besuchen Sie die Seite http://ophcrack.sourceforge.net/tables.php um Regenbogentabellen für bestimmte Zwecke herunterzuladen.

Rufen Sie anschließend

```
ophcrack --help
```

auf um angezeigt zu bekommen, wie Sie ophcrack den Speicherort und die zu verwendenden Tabellen mitteilen.

7.3 Ncrack

Das Programm „ncrack“ knackt Passwörter, die zur Netzwerkauthentifizierung verwendet werden, darunter FTP, SSH, HTTP, SMB, RDP, VNC oder MySQL. Wieder bietet sich ein lokaler Test an. „ncrack“ arbeitet mit Passwortlisten, die entweder Komma getrennt oder unter Angabe eines Dateinamens übergeben werden. Starten Sie zunächst in einer Root-Shell den SSH-Dienst:

/etc/rc.d/0600-openssh.sh start

Vergeben Sie anschließend mit dem Befehl „passwd“ ein leicht zu erratendes Passwort für „root“. Nun können Sie unter Angabe der Wortliste
von John the Ripper einen simulierten Angriff starten:

ncrack -v --user root -P /opt/john-1.8.0-jumbo-1/run/password.lst localhost:22

Verwenden Sie den Befehl "ncrack --help" um detailliert alle Optionen des Programms angezeigt zu bekommen. Soll ein echter Brute-Force-Angriff mit ncrack durchgeführt werden, müssen Sie Wortlisten (beispielsweise per Perl- oder Ruby-Script) erzeugen und dann diese verwenden.

8 Das Linux-System

Das SecuPerts-Forensik-System ist ein linuxbasiertes System. Dieses unterscheidet sich in vielen Aspekten von Windows-Systemen.

8.1 Das Dateisystem

Der größte Unterschied liegt in der Organisation des Dateisystems. Unter Windows werden zum Beispiel Laufwerke mit einem Buchstaben belegt, worauf dann weitere Verzeichnisse und Dateien gespeichert werden. Linux verwendet ein Wurzelverzeichnis (Root) und ordnet diesem alle Festplatten, Partitionen und Laufwerke als Gerätedateien im Verzeichnis "/dev" unter. Dabei beinhaltet das Root-Verzeichnis die folgende Standardverzeichnisstruktur:

- /bin, /sbin: Verzeichnis mit grundlegenden Shell-Befehlen, typischerweise minimale Befehle, die für den Systemstart notwendig sind
- /dev: Gerätedateien für Hardware-Komponenten eines PCs, wie zum Beispiel verbaute Festplatten.
- /etc: Systemweite Konfigurationsdateien und Startskripte.
- /home/Nutzername: Private Dateien der normalen Nutzer eines Rechners.
- /lib, /usr/lib: Programmbibliotheken.
- /media: Verzeichnis für Wechselmedien wie CD/DVD/BD-Laufwerke und USB-Sticks. Auch interne Laufwerke verwenden dieses Verzeichnis.
- /opt: Verzeichnis für nachträglich installierte Software.
- /root: Verzeichnis für persönliche Daten des Administrators.
- /tmp: Temporäre Daten.
- /usr: "Unix System Ressources" Systemdateien und Anwendungsprogramme
- /var: Daten, die während des Betriebs geschrieben werden.

8.2 Laufwerke einbinden

Vorhandene Laufwerke werden nicht automatisch beim Starten des SecuPerts-Forensik-Systems eingebunden. Sie müssen erst, im Gegensatz zu Windows, manuell eingelesen werden. Unter Linux sind Laufwerke nicht durch Buchstaben, sondern durch Gerätedateien unter "/dev" gekennzeichnet. Die

erste Festplatte hat zum Beispiel die Bezeichnung "sda", die erste Partition auf dieser Festplatte "sda1". Das Anklicken dieser Datei führt jedoch nicht zu den gespeicherten Daten. Zunächst muss die Gerätedatei "/dev/sda1" ein einen Ordner (diesen nennt man "Mountpoint") eingebunden werden. Der Mountpoint kann sich an beliebiger Stelle des Dateisystems befinden, üblicherweise verwendet man Ordner unter "/media/disk", beispielsweise "/media/disk/sda1". Am einfachsten mounten Sie Laufwerke über das Tool "Disks", wo Sie mit einem Häkchen entscheiden, ob das Laufwerk schreibbar sein soll und anschließend mit dem Klick auf "Partition X (sdaX, ntfs) einbinden" das Laufwerk mounten und gleich einen Dateimanager öffnen. Das Laufwerk bleibt gemountet, bis entweder das System heruntergefahren wird oder Sie die Laufwerkseinbindung manuell lösen.