CDI2.0

HANDBUCH

Inhalt

Was ist „C.D.I. – Den Daten auf der Spur“?

Das „CDI Forensik-System“ startet von DVD oder USB-Stick ein eigenständiges Betriebssystem, mit dem es Ihnen möglich ist – ohne Änderungen am installierten Betriebssystem vorzunehmen – verschiedene Aufgaben der Computerforensik durchzuführen und so auf Spurensuche zu gehen, wenn ein Computer beispielsweise von Unbefugten benutzt wurde.

- **Gelöschte Dateien finden:** Wurden Dateien versehentlich gelöscht oder ein Angreifer versucht, Spuren zu verwischen, können Sie gelöschte Dateien wieder herstellen. Hierfür stehen zwei Verfahren zur Verfügung.
- **Erstellung von Images:** Für die detaillierte Analyse können Sie Images von Festplatten erstellen und diese später in Ruhe analysieren. Beim Erstellen forensischer Images wird auch der Inhalt vermeintlich unbelegter Blöcke der Festplatte gesichert, was das spätere Auffinden gelöschter Daten erleichtert.
- **Caches und Verläufe finden:** Spüren Sie die Verläufe von Browserprofilen und den Inhalt von Caches auf. So erfahren Sie, wer welche Webseiten aufgesucht hat.
- **Mailboxen finden und öffnen:** Finden Sie Mailbox-Dateien von Outlook und Mozilla Firefox und öffnen Sie diese. Verschaffen Sie sich so einen Überblick über Kommunikationsinhalte und Metadaten.
- **Dateiverläufe öffnen:** Erkennen Sie anhand der Windows-Dateiverläufe, mit welchen Programmen und Daten ein Unbefugter an Ihrem Rechner gearbeitet oder was er gesucht hat.
- **Netzwerk-Schwachstellen-Scan:** Spüren Sie mit OpenVAS Rechner in Ihrem Heim- oder Büronetz auf, die verwundbar sind. OpenVAS findet auch unzureichend abgesicherte Smart-TVs oder verwundbare DSL-Router.
- **Netzwerk-Traffic-Analyse:** Schneiden Sie Netzwerkverkehr mit, um Rechnern im eigenen Netzwerk auf die Spur zu kommen, die beispielsweise zum Versand von Spam mißbraucht werden.
- **USB-Installation:** Besitzt der zu überprüfende Computer kein optisches Laufwerk (beispielsweise ein Netbook) oder ist dieses defekt?

Kein Problem. Erstellen Sie mithilfe des „CDI-Forensik-Systems“ einen startfähigen USB-Stick. So haben Sie Ihr persönliches Analyse-Kit immer dabei. Die Installation auf USB ist Voraussetzung für die Nutzung des Netzwerk-Schwachstellen-Scanners „OpenVAS“.

- **Fernwartung:** Sie wissen nicht so recht, wie die gefundenen Ergebnisse zu interpretieren sind? Geben Sie Ihren PC (Bildschirm, Maus und Tastatur) einfach für eine helfende Hand aus der Ferne frei - oder greifen Sie selbst tatkräftig einem Freund unter die Arme.
- **Arbeitsplatz:** Damit Sie eine Vielzahl von Dateien öffnen, im Internet recherchieren und auf Ihre Emails zugreifen können, sind eine Vielzahl gängiger Programme wie Bildbetrachter, VLC Media Player, ein kleines Office-Paket, sowie Mozilla Firefox und Thunderbird mit an Bord.

Bitte beachten Sie die Privatsphäre Dritter!
Das „CDI Forensik-System“ dient in erster Linie dazu, die Möglichkeiten der forensischen Analyse unverschlüsselter Festplatten und unverschlüsselter Netzwerkverbindungen, aber auch die leichte Überwindung von schwachen Passwörtern verständlich zu machen, beispielsweise wenn ein Computer gestohlen oder von Grenzbehörden konfisziert wird. Eine weitere Aufgabe besteht darin, Spuren auf Systemen zu suchen, die unbefugt von Dritten benutzt wurden (nach Diebstahl wiedererlangte Computer oder Computer, die gehackt wurden). Seien Sie bei darüber hinausgehenden Einsätzen vorsichtig: Der Mitschnitt fremden Netzwerkverkehrs kann eine Straftat darstellen! Ähnlich verhält es sich bei der Analyse von Mitarbeiter-PCs in Unternehmen, hier ist eine Analyse beispielsweise nur dann zulässig, wenn eine Betriebsvereinbarung die private Nutzung von Firmen-PCs ausdrücklich untersagt und nur die Verarbeitung geschäftlicher Daten erlaubt. Aus diesem Grund kann bereits die Analyse eines mit Schadsoftware befallenen Mitarbeiter-PCs in Unternehmen illegal sein. Kontaktieren Sie daher vor dem Einsatz auf anderen als ausschließlich selbst genutzten PCs einen Fachanwalt für Arbeits- oder IT-Recht. Um die illegale Nutzung der Brute-Force-Passwortknacker für Netzwerkdienste (SSH, FTP, CIFS...) zu verhindern, sind keine einfach zu nutzenden VPN-Konfigurationstools oder TOR-Wrapper enthalten.

Start-Vorgang

Das „CDI Forensik-System“ startet als eigenständiges Betriebssystem, ohne dass ein lokal installiertes Windows gestartet werden muss. Dies

erlaubt die Durchführung von Analyseaufgaben, ohne Spuren zu hinterlassen, Ergebnisse zu verfälschen oder Schadsoftware eine Chance zu geben, Spuren zu verwischen. Legen Sie die DVD ein und starten Sie den Rechner. Sollte kein DVD-Laufwerk zur Hand sein, erstellen Sie an einem anderen PC einen bootfähigen USB-Stick. Die Erstellung des USB-Sticks kann unter Windows erfolgen, das optische Laufwerk wird danach nicht mehr benötigt. Prinzipiell empfehlen wir die Nutzung vom USB-Stick, weil hier der Programmstart schneller ist, Auslagerungsspeicher zur Verfügung steht und Programme verwendet werden können, die viele temporäre Dateien schreiben (OpenVAS, Virenscanner).
Der Start des CDI-Forensik-Systems erfolgt in den meisten Fällen automatisch, wenn das System einen bootfähigen Datenträger erkennt. In einigen Fällen ist jedoch der Aufruf eines temporären Bootmenüs oder die dauerhafte Änderung der Bootreihenfolge notwendig.

Temporäres Bootmenü

Je nach Hersteller des Computers, beziehungsweise BIOS-Version kann unmittelbar nach dem Anschalten des Computers mit einer der Tasten >F8<, >F2<, >F9<, >F10<, >F11<, >F12<, >Alt<, >Esc< oder >Tab< eine Liste der angeschlossenen bootfähigen Datenträger ausgewählt werden. Wählen Sie hier mit den Pfeiltasten das DVD-Laufwerk oder den USB-Stick, der das CDI-Notfall-System enthält.

BIOS aufrufen

Ist kein Start über ein temporäres Bootmenü möglich, müssen Sie unmittelbar nach dem Anschalten des Computesr das Setup des BIOS aufrufen. Dies gelangt meist durch Drücken der Taste „Entf“ unmittelbar nach dem Einschalten des Rechners, in selteneren Fällen mit einer anderen Taste wie >F2<, >F8<, >F9<, >F10< oder >ESC<.

Im BIOS-Setup suchen Sie den Reiter „Boot“ oder „Startup“ und dort „Boot order“ oder „Startup priority“. Bei den meisten Computern können Sie in der Liste mit den Tasten >+< oder >-< (vorzugsweise des Zahlenblocks) ein Gerät in der Reihenfolge nach oben oder unten schieben. Nachfolgend finden Sie deshalb die häufigsten Verfahrensweisen um ins BIOS-Setup zu gelangen. Sollte keine davon zum Ziel führen, konsultieren Sie bitte das Handbuch zu Ihrem Rechner. Dort sollte die richtige Taste oder Tastenkombination ebenfalls vermerkt sein. Auch eine Google-

Suche mit dem Term ‚BIOS Zugang für <Ihr Board>' führt oft zum Ziel.

- Betätigen der Taste >Entf< nach Systemstart (allgemein üblich bei AMI- sowie verschiedenen Phoenix-BIOS)
- Betätigen der Taste >F2< nach Systemstart (allgemein üblich bei Phoenix-BIOS)
- Betätigen der Taste >F10< nach Systemstart (insbesondere COMPAQ-PCs)
- Betätigen der Taste >Esc< nach Systemstart
- Als Tastenkombinationen (oft auf Notebooks) kommen häufig ‚Strg+S', ‚Strg+Esc' und ‚Strg+Alt+Esc' vor.

Start auf UEFI PCs

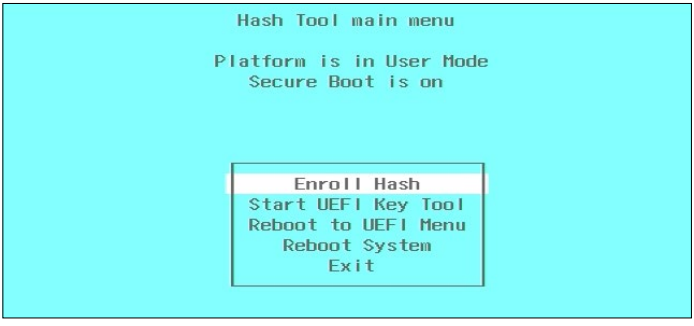
Computer, die mit Windows 8 oder neueren Windows-Versionen ausgeliefert wurden, nutzen in der Regel den BIOS-Nachfolger UEFI („Universal Extensible Firmware Interface"), in der Regel in der Kombination mit „Secure Boot", was nur den Start von signierten Bootloadern erlaubt. Das CDI-Forensik-System nutzt einen solchen signierten Loader, allerdings unterscheidet sich die Startprozedur etwas von der bei PCs mit klassischem BIOS.

Prinzipiell können Sie auf Rechnern mit UEFI auf dem gleichen Weg ins Setup wechseln wie bei BIOS, allerdings macht in vielen Fällen eine Voreinstellung, die der Beschleunigung des Startvorgangs dienen soll, einen Strich durch die Rechnung: Oft wird die Tastatur erst initialisiert, wenn das Bootmedium initialisiert und gestartet wurde. In diesem Fall können Sie den Start des CDI-Forensik-Systems aus Windows heraus anstoßen. Öffnen Sie hierfür in der „Modern UI" die PC-Einstellungen und klicken Sie dort unter „Allgemein" im Abschnitt erweiterter Start auf „Jetzt neu starten". Sie erhalten nun ein Startmenü, in dem Sie unter „Ein Gerät verwenden" den USB-Stick oder die DVD auswählen können.

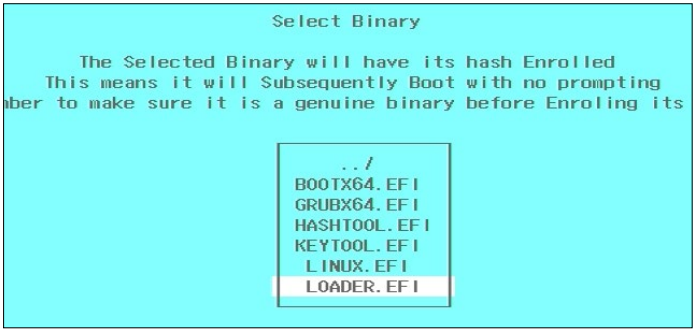
Secure Boot

Ist im UEFI „Secure Boot“ aktiviert, bringt der Bootloader beim ersten Start die folgende Warnung:

Bestätigen Sie „OK“ mit der Eingabetaste, es öffnet sich das „Hashtool“, wo Sie mit den Pfeiltasten auf „Enroll Hash“ gehen:



In der nun folgenden Liste „Select Binary“ wählen Sie die Datei „LOADER.EFI“ aus:



Sie werden nun gefragt, ob der Hashwert dieser Datei zu den zulässigen hinzugefügt werden soll. Wählen Sie „Yes“:

Verfahren Sie ebenso mit der Datei „LINUX.EFI“ und verlassen Sie anschließend das Hashtool über den Menüpunkt „Exit“. Sie befinden sich nun wieder im Bootmenü, wo Sie das „CDI Forensik-System“ starten können. Bei künftigen Starts ist dieser Schritt nicht mehr nötig, da zugelassene Hashwerte dauerhaft gespeichert werden.

FAQ: „CDI Forensik-System“ bootet nicht

Das „CDI Forensik-System“ baut auf dem Linux-System ‚LessLinux‘ auf, das eine große Bandbreite an Hardware erkennt und unterstützt. Nichtsdestotrotz wird es spezielle Einzelfälle und stark veraltete Systeme geben, in denen die Erkennung versagt und eine Verwendung nicht möglich sein wird. Wir bitten um Verständnis, falls dieses bei Ihnen der Fall ist. Unter Umständen helfen aber die folgenden Tipps:

- Deaktivieren Sie die Option ‚Secure Boot‘ in Ihrem BIOS zumindest zum Austesten, ob das „CDI Forensik-System“ dann funktioniert.
- Versuchen Sie, den PC im ‚Legacy only‘-Modus zu starten. Windows 8-Anwender achten bitte darauf, später vor dem Neustart wieder die Einstellung ‚UEFI only‘ zu aktivieren.
- Probieren Sie die verfügbaren Boot-Parameter aus, erreichbar über den Menüpunkt ‚Abgesicherter Start‘ im Bootmenü des „CDI Forensik-Systems“.

Boot-Menü des CDI Forensik-Systems

Das CDI-Forensik-System startet nach 10 Sekunden oder Betätigen der Eingabetaste mit automatischer Hardwareerkennung. Gerade auf älteren Computern kann es jedoch erforderlich sein, Startparameter abzuändern. Sie erreichen diese über den Menüpunkt „Abgesicherter Start“:

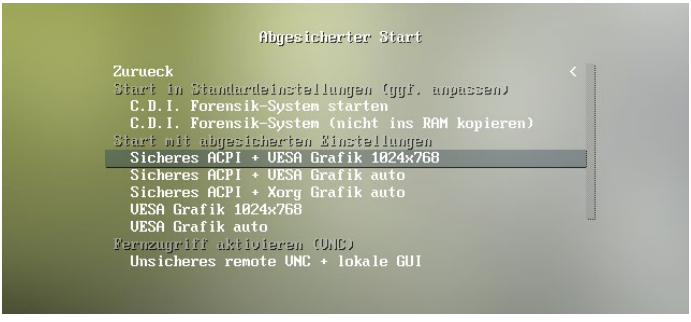
Bootmenü

- CDI-Forensik-System starten: Startet das Notfall-System direkt.
- Abgesicherter Start: Aufruf verschiedener Parameter zum Systemstart
- Von Festplatte starten: Verlässt das Bootmenü und startet den Rechner von Festplatte ins herkömmliche Betriebssystem

Abgesicherter Start

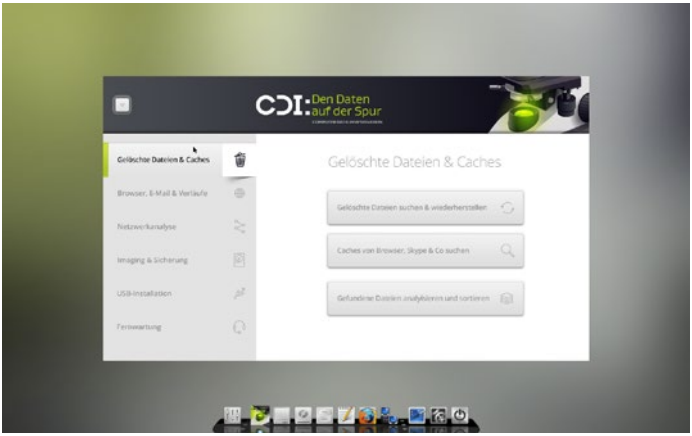
- **Zurück:** Zurück zum Bootmenü
- **Start in Standardeinstellungen:** Systemstart ohne Änderung der Voreinstellungen
  - CDI Forensik-System starten: Entspricht dem normalen Systemstart im Bootmenü
  - CDI Forensik-System (nicht ins RAM kopieren): Kopiert die DVD auch bei Systemen mit genügend Arbeitsspeicher nicht ins RAM, so können auch sehr speicherintensive Anwendungen genutzt werden
- **Start mit abgesicherten Einstellungen:** Ermöglicht den Start des „CDI Forensik-Systems" unter Berücksichtigung bekannter Probleme mit den Grafiktreibern und dem Energie-Management einiger Systeme. Diese Starteinstellungen werden vor allem auf älteren PCs mit nicht Standard konformem ACPI benötigt.
  - Sicheres ACPI + VESA Grafik 1024x768: Start mit weitgehend deaktiviertem ACPI und einer unveränderlichen Grafikauflösung von 1024 x 768 Pixel, die den VESA-Grafiktreiber nutzt. Probieren Sie diese Option, wenn der Computer in den Standardeinstellungen nicht startet oder sofort abstürzt.
  - Sicheres ACPI + VESA Grafik auto: Start mit weitgehend deaktiviertem ACPI und einer automatisch eingestellten Grafik, die den VESA-Grafiktreiber nutzt. Probieren Sie diese Option, wenn ein Notebook in den Standardeinstellungen nicht startet oder sofort abstürzt.
  - Sicheres ACPI + Xorg Grafik auto: Start mit weitgehend deaktiviertem ACPI und automatischer Auswahl der kompatibelsten Grafikauflösung. Als Grundlage dient der Xorg-Treiber. Probieren Sie diese Option, wenn zwar die Grafikanzeige in Standardeinstellungen korrekt ist, das System aber abstürzt oder einfriert.
  - VESA Grafik 1024x768: Start mit einer Grafikauflösung von 1024 x 768 Pixel auf VESA-Basis.
  - VESA Grafik auto: Start mit VESA-Anzeigeprotokoll. Der richtige VESA-Treiber wird selbsttätig ausgewählt.
- **Fernzugriff aktivieren (VNC):** Ermöglicht die Analyse eines Rechners via Fernzugriff, sollte auf Grund nicht vorhandener Verschlüsselung aber nur in absolut vertrauenswürdigen Umgebungen eingesetzt werden.
  - Unsicheres remote VNC + lokale GUI: Startet eine lokale grafische Oberfläche, auf die Sie per VNC-Viewer zugreifen können.

- Unsicheres remote VNC - ohne lokale GUI: Ermöglicht den Zugriff, ohne dass eine lokale grafische Oberfläche gestartet wird. Praktisch, wenn kein kompatibler Treiber für die Grafikkarte vorhanden ist.
- Reverse VNC + lokale GUI: Startet den VNC Server im „Push-Modus", erfordert, dass auf dem Rechner, der die Grafikausgabe anzeigen soll, ein VNC-Viewer im „Listening Mode" gestartet wurde. Drücken Sie vor dem Start mit dieser Option die Taste >Tab<, um die IP-Adresse des Zielrechners zu editieren.
- Reverse VNC - ohne lokale GUI: Wie der vorherige Punkt, allerdings ohne lokale Grafikausgabe. Sie können beliebige Auflösungen angeben und so eine komfortable Größe der Arbeitsfläche einstellen.

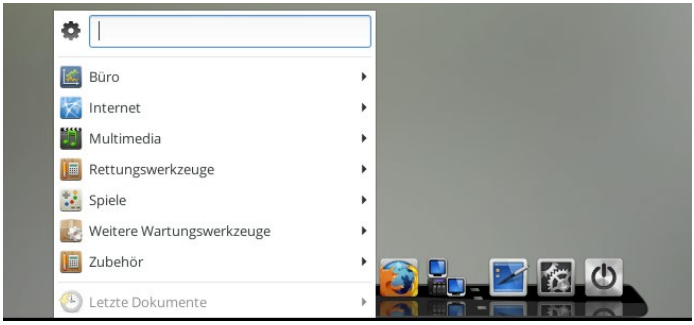


Arbeitsoberfläche

Nach dem Start des „CDI Forensik-Systems“ erscheint der Programm starter mit einer Auswahl der wichtigsten Werkzeuge zur Analyse und Spurensuche. In den Reitern links wählen Sie die gewünschte Kategorie aus, rechts können Sie dann die enthaltenen Programme starten. Am unteren Rand des Bildschirmes wird eine Menüleiste - das „Dock“ - angezeigt. Es enthält links ein Startmenü und bietet zudem Schnellzugriff auf wichtige Programme wie Firefox, den Dateimanager, Laufwerke und den Netzwerkverbindungsmanager.



Das Startmenü ist in Kategorien eingeteilt und enthält auch Werkzeuge zur Datenrettung und -sicherung, sowie eine Reihe von Anwendungen zum Öffnen gängiger Dateiformate. Dies erspart es Ihnen in vielen Fällen, gefundene Dateien zur genaueren Betrachtung auf einen Windows-Rechner kopieren zu müssen.



- **Anwendungsmenü[1]:** Hier können Sie verschiedene Büro-, Internet- und Multimediaprogramme sowie weitere wichtige Reparatur- und Systemtools direkt aufrufen, darunter:
  - Büro: PDF-Betrachter, Tabellenkalkulation und Textverarbeitung (AbiWord).
  - Internet: Ekiga-Softfon (VoIP, IP-Telefon (SIP, H.323), auch Videokonferenzen möglich), E-Mail-Client, InstantBird (Messenger), Web-Browser, Wicd Network Manager (Verwaltung der Netzwerkverbindungen).
  - Multimedia: Audacious (Audioplayer), Daten brennen (mit xfburn), Laustärkeregelung, VLC Media Player.
  - Rettungswerkzeuge: ClamAV (Virenscanner), Daten brennen, Daten retten, Festplatte nach VM Image, Kennwort neu, Partition retten, Platte klonen, Platte testen, QPhotoRec, Rettungs-Image erstellen, S.A.D.-Rettungsassistent, sicher löschen, Windows Shell zurücksetzen.
  - Spiele: Verschiedene Casual Games wie Mahjongg, Schach und Robots für Gelegenheitsspieler.
  - Weitere Wartungswerkzeuge: Bulk-Rename (Umbenennen von Dateien), Dateimanager als Root, Dateimanager Thunar, Festplattenbelegung analysieren, GHex, GParted Partitionierungswerkzeug, Grsync, Hardware anzeigen, Herunterfahren, PartImage, QPxTool, Root-Shell, SSHD (Fernzugriff), TeamViewer, VSS-Zugriff (Zugriff auf V-Shadow-Snapshots), Wireshark, Xfce Terminal, Zenmap.
  - Zubehör: Archivverwaltung, CIFS- oder WebDAV-Freigaben einbinden, Filezilla, Installation auf USB-Laufwerk, KeePassX, Laufwerke freigeben, Mousepad, Netzlaufwerke, Remmina, Software installieren, Taschenrechner, TrueCrypt, VNC-Server starten.

- **CDI-Assistent:** Aufruf der wichtigsten Tools des „CDI Forensik-Systems“.
- **Laufwerke:** Anzeige der im Rechner vorhandenen Laufwerke.
- **Dateimanager:** Aufruf des Thunar-Dateimanagers
- **Editor:** Aufruf eines Texteditors.
- **Webbrowser:** Aufruf des Firefox-Browsers.
- **Netzwerke einrichten:** Konfiguration Ihres WLANs oder drahtgebundenen Netzwerkes.
- **Desktop anzeigen:** Verkleinern aller offenen Fenster, um Zugriff zum Desktop zu erlangen.
- **Updates suchen:** Aktualisierung der Programmkomponenten. Hinweis: Auf DVD erfolgt die Aktualisierung mit jedem Start erneut, da das Medium keine permanente Speicherung der neuen Software erlaubt.
- Computer ausschalten: Fährt das System nach einer Abfrage herunter.

[1] Zur Bedienung der allgemein üblichen Programme wie Textverarbeitung, Medienplayer, Archivmanager, Browser usw. konsultieren Sie bitte die jeweilige digitale Online-Programmhilfe (vereinzelt funktionierende Internet-Verbindung notwendig).

Dateisystem-Besonderheiten

Das CDI-Forensik-System basiert auf einem Linux-Betriebssystem, das sich in vielerlei Hinsicht von Windows unterscheidet. Am auffälligsten ist dieser Unterschied bei der Organisation von Dateisystem und dem Zugriff auf Laufwerke. So verwendet Linux keine Laufwerksbuchstaben („“, „“ und so weiter), und als Pfadtrenner kommt der „Forwardslash“ (nicht der Backslash) zum Einsatz. Organisiert ist das Dateisystem wie folgt:

- /bin, /sbin, /usr/bin und /usr/sbin: Verzeichnisse mit Befehlen und Anwendungen, /sbin und /usr/sbin enthalten typischerweise Programme, die nur mit Administratorrechten ausgeführt werden können
- /boot, /lesslinux/boot: Zum Systemstart erforderliche Daten.
- /dev: Gerätedateien für die Hardware-Komponenten eines PC-Systems, darunter auch die verbauten Festplatten und anderen Laufwerke.

- /etc: Lokale Konfigurationsdateien.
- /home/Nutzername: Private Daten der normalen Nutzer eines PCs.
- /lib, /usr/lib: Programmbibliotheken.
- /media: Einhängepunkte für Wechselmedien wie CD/DVD/BD-Laufwerke und USB-Sticks, wird auch für interne Laufwerke genutzt.
- /opt: Reserviertes Verzeichnis für die nachträgliche lokale Installation zusätzlicher Software.
- /root: Heimatverzeichnis für persönliche Daten des Administrators (Benutzer ‚root') eines Systems.
- /tmp: Temporäre Dateien.
- /var: Enthält Daten, die während des Betriebs geschrieben werden, z.B. Protokolldateien oder Informationen über gestartete Dienste

Festplattenzugriff

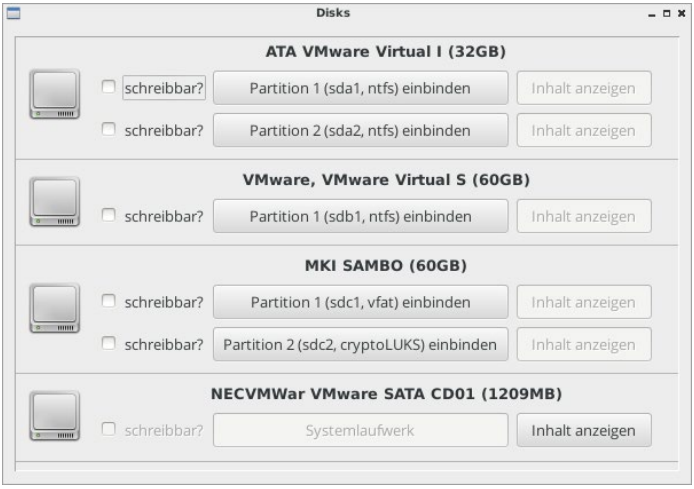
Festplatten und darauf vorhandene Partitionen werden unter Linux als sogenannte Gerätedateien verfügbar gemacht. SATA-, IDE-, SCSI- und USB-Laufwerke erscheinen in der Reihenfolge ihrer Erkennung als „/dev/sda", „/dev/sdb" und so weiter. Typischerweise werden interne Laufwerke zuerst erkannt, USB-Laufwerke anschließend. Partitionen auf Laufwerken werden durchnummeriert. Bei Festplatten mit MBR-Partitionsschema stehen die Partitionsnummern 1 bis 4 für primäre Partitionen, ab 5 für logische Partitionen, bei GPT partitionierten Platten gibt es diesen Unterschied nicht.

Beispiele:

- **/dev/sda** erste erkannte Festplatte, gesamtes Laufwerk incl. Bootsektor und nicht von Partitionen belegten Platzes
- **/dev/sdb1** erste (primäre) Partition der zweiten erkannten Festplatte
- **/dev/sdc5** erste logische Partition (BIOS/MBR) oder fünfte Partition (GPT) der dritten erkannten Festplatte

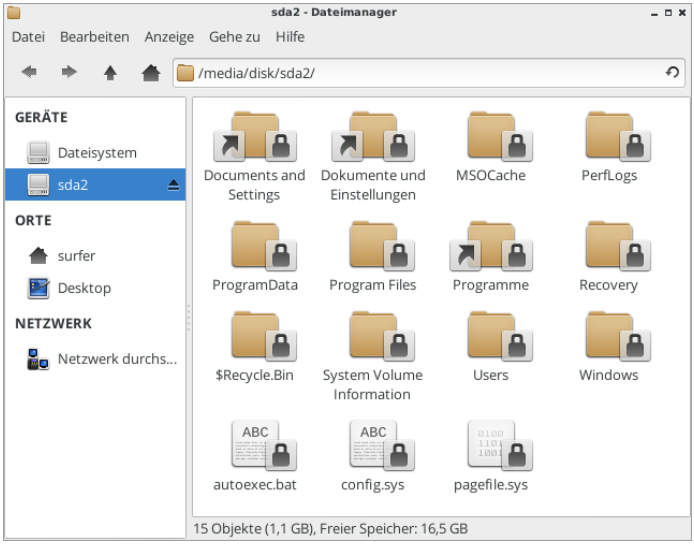
Der Laufwerkszugriff unter Linux funktioniert anders als unter Linux zweistufig: Die Gerätedateien unterhalb von „/dev" dienen lediglich dem rohen, blockweisen Zugriff. Ein Doppelklick auf diese Dateien bringt keine Laufwerksinhalte zum Vorschein. Tatsächlich werden Gerätedateien vor allem von Werkzeugen verwendet, die Daten von Laufwerken retten oder Images erstellen.

Um auf die in einem Laufwerk enthaltene Ordnerstuktur zugreifen zu können, muss das Laufwerk eingebunden (auch: „gemountet“) werden. Diese Laufwerkseinbindung erfolgt beim CDI Forensik-System nicht automatisch. So werden unnötige Schreibzugriffe vermieden, welche die Integrität der gespeicherten Daten gefährden könnten und Sie haben gleich nach dem Systemstart die Möglichkeit, Imaging-Werkzeuge zu nutzen, ohne vorher Laufwerkseinbindungen lösen zu müssen.
Das Mounten ist theoretisch per Kommandozeile möglich, dies setzt jedoch etwas Linux-Erfahrung voraus. Deutlich einfacher ist die Verwendung des Laufwerkemanagers im Dock. Der folgende Screenshot zeigt das Tool mit vier erkannten Laufwerken:

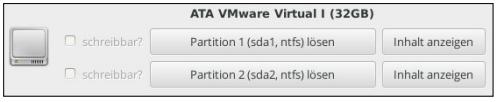


Die ersten beiden Einträge stehen für interne Festplatten. „/dev/sdc“ ist ein partitionierter USB-Stick und der letzte Eintrag gehört zum DVD-Laufwerk in dem die DVD des CDI Forensik-Systems liegt. Mit dem Klick auf „Partition . . . einbinden“ machen Sie den Inhalt dieser Partition übers Dateisystem verfügbar. Setzen Sie das Häkchen bei „schreibbar?“ nur dann, wenn der Schreibzugriff unbedingt erforderlich ist, beispielsweise bei einem USB-Laufwerk, auf dem Sie ein Image oder zu analysierende Daten speichern wollen! Nach dem Einbinden öffnet sich ein Dateima-

nager-Fenster. Haben Sie den Dateimanager versehentlich geschlossen, können Sie ihn mit dem Button „Inhalt anzeigen“ erneut öffnen.
Das Einbinden erfolgt unterhalb von „/media/disk“, der verwendete Ordner heisst wie die Gerätedatei, im Falle der Windows-Systempartition der ersten Festplatte also „/media/disk/sda2“. Unterhalb davon finden Sie die von Windows gewohnte Ordnerstruktur vor:



Um die Einbindung eines Laufwerkes zu lösen öffnen Sie ebenfalls das Werkzeug „Laufwerke“ und klicken Sie auf „Partition . . . lösen“.



Schlägt das Lösen der Laufwerkseinbindung fehl, ist noch ein Prozess aktiv, der auf Dateien dieses Laufwerkes zugreift. Gelingt es nicht, diesen Prozess ausfindig zu machen und zu beenden, hilft nur ein Neustart.

Beachten Sie bitte, dass viele Forensikwerkzeuge, beispielsweise zum

Aufspüren gelöschter Daten, Zugriff auf Blockebene benötigen, das betreffende Laufwerk sollte daher nicht eingebunden sein. Andere Werkzeuge wiederum wie das Werkzeug zum Aufspüren von Caches arbeiten auf Dateisystemebene und setzen daher eingebundene Laufwerke voraus. Als Faustregel gilt: Verwendet ein Werkzeug einen Auswahldialog, in dem Sie Festplatte oder Partition selektieren, dürfen die zu untersuchenden Laufwerke nicht eingebunden sein. Verwendet es dagegen einen Datei- oder Ordner-Auswahldialog, muss das zu untersuchende Laufwerk eingebunden sein. Achten Sie zudem bei der Angabe des Speicherortes für gefundene gelöschte Dateien, Images usw. darauf, dass das Ziellaufwerk schreibbar eingebunden ist.

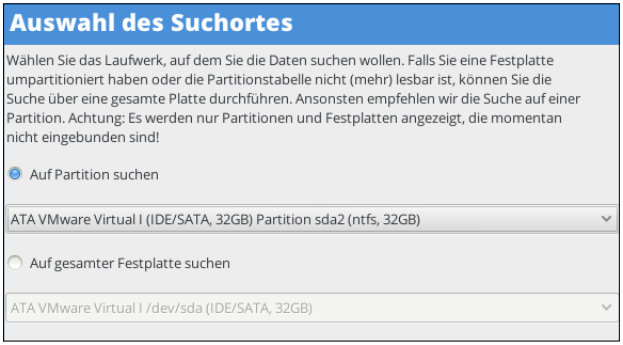
CDI Forensik-Assistent

Der Forensikassistent erlaubt den sofortigen Zugriff auf die wichtigsten Komponenten zur Analyse Ihres Computers. In den Reitern auf der linken Seite finden Sie die verfügbaren Kategorien:

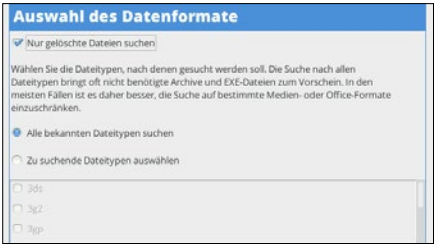
- Gelöschte Dateien und Caches: Suchen Sie in vermeintlich unbelegten Sektoren nach gelöschten Dateien und finden Sie die Cache-Verzeichnisse gängiger Webbrowser.
- Browser, Email und Verläufe: Finden Sie Email-Postfächer, konvertieren Sie diese und erhalten Sie Zugriff auf Browser- und Dateiverläufe.
- Netzwerkanalyse: Spüren Sie unsichere, veraltete und falsch konfigurierte Geräte in Ihrem Netzwerk auf
- Imaging und Sicherung: Komplettlöschung von internen und externen Datenträgern.
- USB-Installation: Installieren Sie Ihr „CDI Forensiksystem“ auf einen startfähigen USB-Stick. Neben dem schnelleren Programmstart können die Werkzeuge zur Netzwerkanalyse verwendet werden, zudem sind Updates möglich.
- Fernwartung: Erlangen Sie Zugriff auf fremde Rechner, bzw. ermöglichen Sie einen fremden Zugriff auf den zu untersuchenden Rechner via TeamViewer, VNC oder Remmina – beispielsweise um bequem von Ihrem Windows-Rechner aus eine Analyse zu überwachen.

Gelöschte Dateien suchen und wiederherstellen

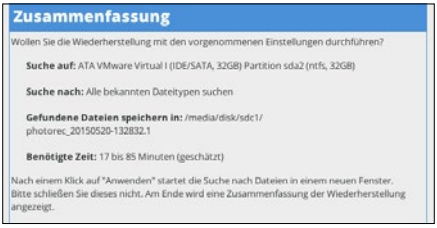
Bevor Sie die Datenwiederherstellung starten, binden Sie ein Ziellaufwerk ein, das über genügende freien Platz verfügt. Sie sind auf der sicheren Seite, wenn der freie Platz dem unbelegten Platz auf dem zu analysierenden Laufwerk entspricht.
Der erste Schritt nach dem Start des Assistenten ist die Auswahl des Suchortes: Gelöschte Dateien werden Sie in der Regel auf einer Partition suchen wollen. Nur wenn die Partitionstabelle beschädigt ist, werden Sie auf einer gesamten Festplatte suchen:



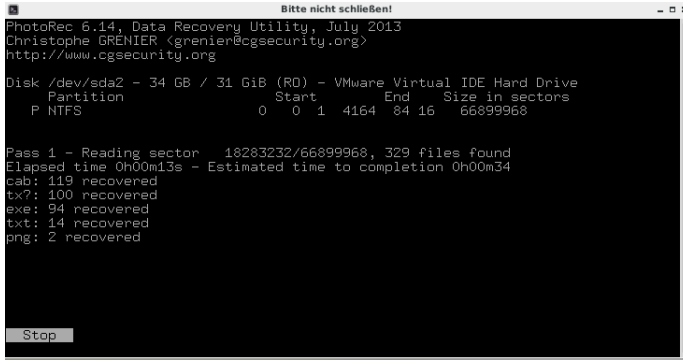
Es folgt die Auswahl der zu suchenden Datenformate und die Entscheidung, ob Sie nur gelöschte Dateien suchen wollen. Bei einem beschädigten Dateisystem sollten Sie das Häkchen bei „Nur gelöschte Dateien suchen“ entfernen, da möglicherweise nicht mehr alle Dateien über das Dateisystem zugänglich sind. Bei der Einschränkung der Dateitypen ist zu beachten, dass die Suche nach allen bekannten Dateitypen auch viele alte Installationsarchive von Windows-Updates findet. Sollten Sie nach den Spuren einer Schadsoftware suchen, die sich selbst gelöscht hat, ist diese Option zu belassen. In vielen anderen Fällen liefert sie jedoch nicht benötigte Dateien, die später aussortiert werden müssen. Beschränken Sie die Suche daher in den meisten Fällen auf die aufzuspürenden Office- oder Mediendateien.



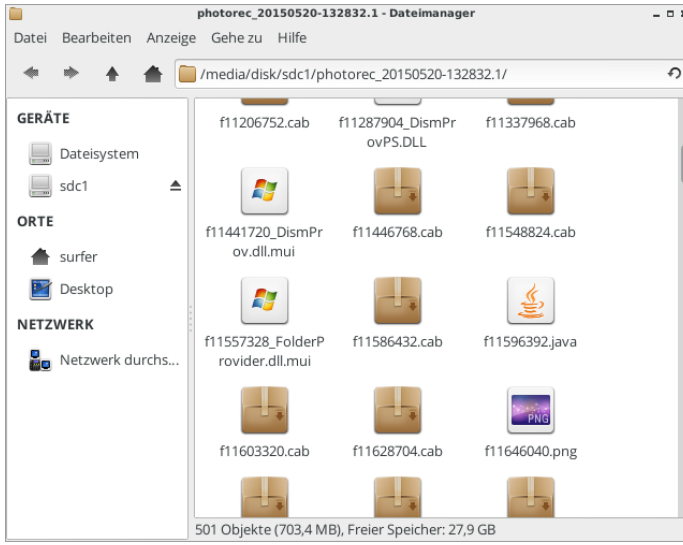
Es folgt die Auswahl des Zielverzeichnisses. Wählen Sie hier das Wurzelverzeichnis oder einen Unterordner eines schreibbar eingebundenen USB-Sticks oder einer USB-Festplatte. Lediglich bei der Spurensuche auf sehr kleinen Partitionen – beispielsweise der oft nur wenige hundert Megabyte großen Windows-Bootpartition können Sie das Zielverzeichnis im Arbeitsspeicher, beispielsweise unterhalb von „/tmp“ anlegen.



Nach der Bestätigung einer Zusammenfassung der vorgenommenen Einstellungen startet der Assistent die Dateisuche mit Hilfe von des Programmes „PhotoRec“. In diesem Fenster erhalten Sie auch Informationen über bereits gefundene Dateien und eine geschätzte Restzeit.



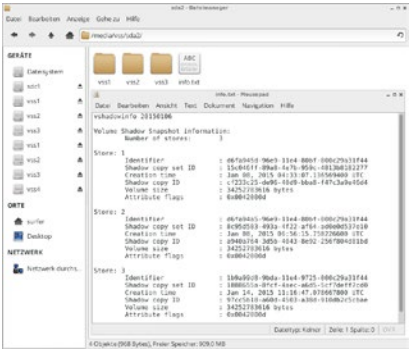
Nach Abschluss der Suche öffnet sich ein Dateimanager-Fenster mit dem angegebenen Zielverzeichnis.



Zugriff auf „Virtual Shadow Snapshots“ (VSS)

Das Dateisystem NTFS bietet einen Mechanismus namens „Virtual Shadow Snapshot“, der oft mit „Schattenkopien“ übersetzt wird. Schattenkopien werden unter anderem für die Erstellung von Systemwiederherstellungspunkten verwendet. Bei der Suche nach gelöschten Dateien ist es daher oft erfolgversprechend, vorhandene Schattenkopien zu suchen, zeitlich einzuordnen und gegebenenfalls darauf zuzugreifen. Für Linux existieren Werkzeuge zum Einbinden der Schattenkopien wie ein normales Laufwerk.

Das CDI Forensik-System bringt für diese Werkzeuge einen einfachen Assistenten mit. Sie finden Ihn unter „Anwendungsmenü > Weitere Wartungswerkzeuge > VSS-Zugriff“. Mit einem Klick binden Sie alle gefundenen Schattenkopieren als Laufwerke nur lesbar ein.



Nach dem Klick auf „Alle einbinden“ öffnet sich ein Dateimanager mit dem Ordner „/media/vss“. Hier finden Sie Unterordner für jede NTFS-Partition mit Schattenkopien vor, beispielsweise „/media/vss/sda2“. Diese Ordner wiederum enthalten enthalten für jede Schattenkopie einen Unterordner „vss1“, „vss2“ und so weiter. Eine Zuordnung dieser Ordner zu einem Datum finden Sie in der Textdatei „info.txt“.

Caches von Browser, Skype und Co. Suchen

Die Cache-Verzeichnisse des Webbrowsers aber auch von Messenger-Programmen wie Skype enthalten häufig unverschlüsselte temporäre Daten, die vielerlei Aufschlüsse darüber zulassen, welche Webseiten aufgesucht wurden und wann mit wem kommuniziert wurde.
Das CDI Forensik-System enthält ein Werkzeug zur Suche nach den Cache-Ordnern von Firefox, Internet Explorer, Google Chrome und Skype. Dieses Programm setzt voraus, dass die Partitionen eingebunden sind, auf denen gesucht werden soll.

Während der Suche erscheint immer dann ein neues Dateimanager-Fenster, wenn ein Cache-Verzeichnis gefunden wurde. Sie können die dort gefundenen Dateien per Doppelklick in den jeweils zugeordneten Anwendungen öffnen. Eine Übersicht über Bilddateien erhalten Sie, indem Sie Ordner mit Bilddateien über einem Fenster des Bildbetrachters Ristretto („Anwendungsmenü > Multimedia > Ristretto“) fallen lassen.

Gefundene Dateien analysieren und sortieren

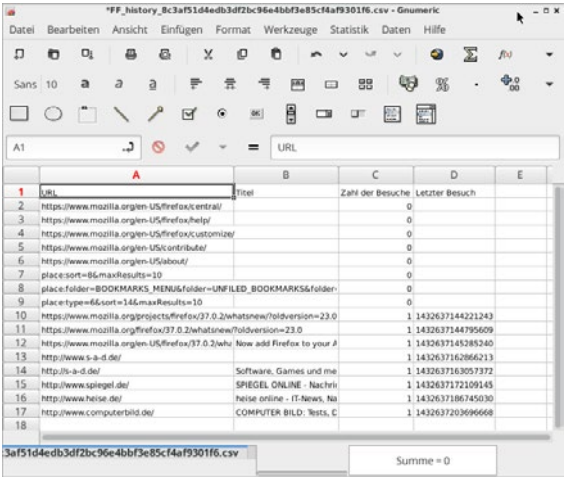
Egal, ob Cache-Ordner oder einst gelöschet und wiederhergestellte Dateien: Mit hunderten von Bildern, Audio- oder Videodateien lässt sich oft wenig anfangen, ohne einen Dateinamen zu kennen. Glücklicherweise enthalten JPEG-Dateien oft sogenannte EXIF-Tags, in denen Meta-Informationen wie Kamera, Aufnahmedatum und oft sogar Aufnahmeort gespeichert sind. Anhand dieser Daten ist es leicht möglich, gefundene Bildateien nach Kamera und Aufnahmedatum zu sortieren. Gleiches gilt für Musikdateien: MP3s enthalten in der Regel soganannte ID3-Tags, in denen Künstler, Album und Titel gespeichert sind. Umgekehrt kann man aus dem Fehlen von EXIF- und ID3-Tags ebenfalls Schlüsse ziehen: Aus vielen Bildbearbeitungsprogrammen erstellte JPEG-Dateien oder die MP3s von Diktiergeräten enthalten keine Tags. Mit der Schaltfläche „Gefundene Dateien analysieren und sortieren“ starten Sie die Sortierung gefundener Dateien.

Wählen Sie als Startverzeichnis einen Ordner, in den Sie gefundene Dateien oder Web-Caches kopiert haben. Für die Sortierung selbst haben Sie zwei Möglichkeiten: Dateien mit Tag zu kopieren oder zu verschieben. Während das Verschieben keinen zusätzlichen Speicherplatz benötigt, wird beim Kopieren schlimmstenfalls derselbe Speicherplatz zusätzlich benötigt. Nach Abschluss der Sortierung wird ein Dateimanangerfenster geöffnet, in dem Sie sich durch die entstandene Ordnerstruktur klicken können.

Browserverläufe finden und auslesen

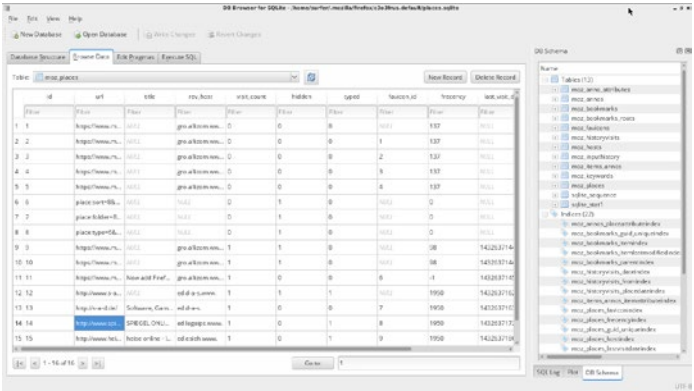
Wurden mit einem Rechner unerlaubte Aktionen durchgeführt, gibt oft der Verlauf des Webbrowsers Auskunft über die durchgeführten Aktionen. Gespeichert sind Browserverläufe zumeist in Datenbanken, die spezielle Werkzeuge zum Öffnen benötigen. Das „CDI Forensik-System“ verfügt über ein Werkzeug, welches die Verläufe von Firefox, Internet Explorer und Google Chrome findet und leicht zu durchsuchende Textdateien umwandelt.

Geben Sie als zu untersuchendes Verzeichnis den Einhängepunkt einer zu analysierenden Festplatte an oder – wenn ein bestimmtes Nutzerprofil durchsucht werden soll – den entsprechenden Unterordner in „Users“. Als Ausgabeverzeichnis können Sie das voreingestellte „/tmp“ belassen. Die gefundenen Daten sind selten größer als wenige hundert Megabyte und können daher im Arbeitsspeicher zwischengelagert werden. Nach abgeschlossener Suche öffnet sich das Ausgabeverzeichnis. Der Datei „history_index.csv“ entnehmen Sie, aus welcher History-Datei welche lesbare Datei erzeugt wurde. Daneben finden Sie CSV- und TXT-Dateien der jeweiligen Verläufe. Die CSV-Dateien von Chrome und Firefox sollten Sie in einer Tabellenkalkulation öffnen, hier bietet sich das mitgelieferte „Gnumeric Spreadsheet“ an:



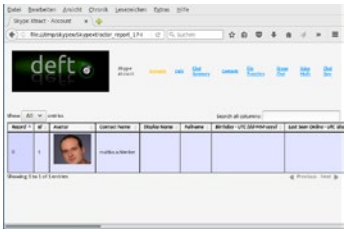
Tipp: SQLite Datenbank-Browser

Firefox und Google Chrome nutzen die Datenbank SQLite in Version 3.x. Eine Version 4 befindet sich lediglich in der Designphase. Dadurch ist sichergestellt, dass Chrome und Firefox in absehbarer Zeit weiterhin SQLite 3 nutzen. Allerdings sind Änderungen am Tabellenbau möglich, welche zur Folge haben, dass das zuletzt vorgestellte Tool nur teilweise oder gar nicht mehr arbeitet.
Das CDI Forensik-System enthält daher den SQLite Datenbank-Browser unter „Anwendungsmenü > Zubehör > DB Browser for SQLite“. In diesem können Sie die Datenbanken (Pfade unter „history_index.csv“) öffnen: Ziehen Sie einfach die SQLite-Datei in den geöffneten Datenbankbrowser.



Übrigens nutzen auch Skype und andere Programme SQLite3 zur tabellenartigen Datenablage: Skype oder Thunderbird beispielsweise für Adressbücher, Skype daneben für gespeicherte Chats und Dateiübertragungen. Sollten Sie nicht sicher sein, was für ein Format eine Datenbank nutzt, verwenden Sie den Shell-Befehl „file“, dem Sie als Argument den Pfad zu der zu analysierenden Datei übergeben.

Skype-Logs extrahieren

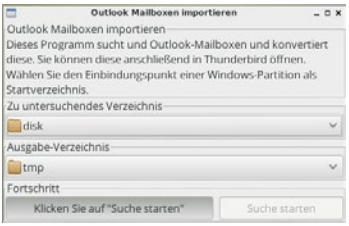


Skype speichert Adressbuch und Chatlogs in SQLite3-Datenbanken. Neben dem bereits erwähnten generischen Datenbank-Browser für SQLite3 steht in dieser Version des CDI Forensik Systems auch der „Skype Xtractor“ des Forensik-Linuxes DEFT bereit. Es handelt sich um ein klassisches Kommandozeilenwerkzeug. Um es aufzurufen, wechseln Sie in das Verzeichnis „/usr/share/skype_xtractor“ und starten einen Python-Prozess unter Angabe der Skype-Datenbank main.db und des Ausgabeverzeichnisses (unterhalb von „/tmp“ oder auf einem eingebundenen USB-Laufwerk):

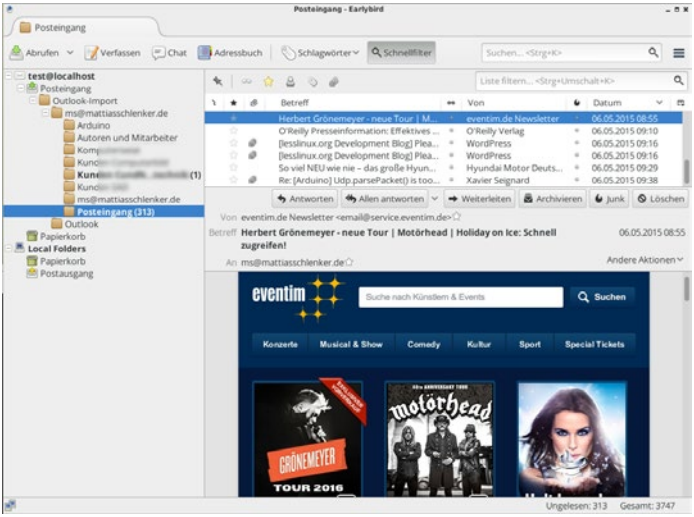
cd /usr/share/skype_xtractor
python skype.py -o /tmp/skype /pfad/zur/main.db

Mit dem zusätzlichen Parameter „-C“ werden auch die Chatsysnc-Dateien erstellt, hierfür muss die komplette Ordnerstruktur des Skype-Profils vorhanden sein. Sie können anschließend mit einem Webbrowser Adressbuch und Chatsync ansehen, Skype Xtractor legt dafür Ordner im Namensschema „Skypextractor_report_17-05-2016_09.08.24“ an, in denen eine „index.html“ Überblick und Zugriff auf die einzelnen Elemente gibt.

Mailboxen öffnen



Falls Sie Zugriff auf Outlook-Mailboxen erlangen möchten, ohne Änderungen an dem Postfach selbst durchzuführen, können Sie das Programm „Mailboxen öffnen“ verwenden. Es konvertiert die PST-Dateien von Outlook in das Mbox-Format, welches Mozilla Thunderbird aber auch viele IMAP-Server verwenden können. Wählen Sie als zu untersuchendes Verzeichnis den Einbindungspunkt einer Windows-Partition oder gegebenenfalls direkt den Ordner eines Nutzerprofils. Wenn bekannt ist, dass eine PST-Datei verhältnismäßig klein ist, können Sie das Ausgabeverzeichnis „/tmp“ belassen. Allerdings können vollständige Caches eines IMAP-Servers heutzutage mehrere Gigabyte groß sein. In diesem Fall müssen Sie als Ausgabeverzeichnis einen Ordner auf einem separaten Laufwerk (USB-Stick oder externe Festplatte) angeben. Dies hat zudem den Vorteil, dass die gesicherte Mailbox-Datei persistent ist. Achten Sie beim Start darauf, dass kein Mozilla Thunderbird läuft! Nach Abschluss der Suche öffnet sich ein Thunderbird-Fenster, in dem die konvertierten PST-Mailboxen bereits als Ordner verfügbar gemacht wurden.

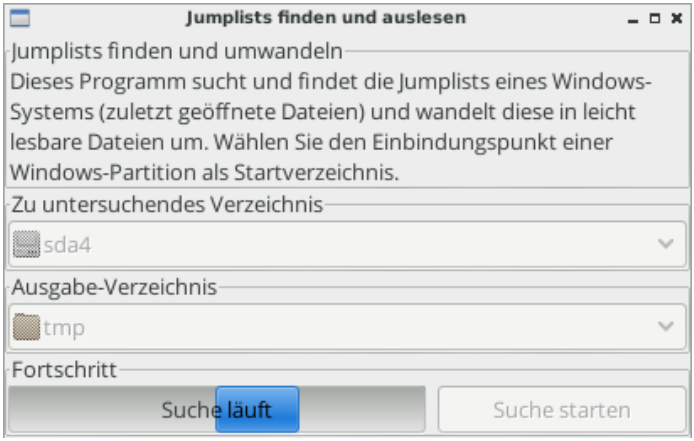


Mailboxen von Thunderbird unter Windows können Sie einfach verfügbar machen, indem Sie den Inhalt der Ordner „Mail“ beziehungsweise „ImapMail“ aus dem Thunderbird-Profil unter Windows in den entsprechenden Ordner im CDI Forensik-System kopieren. Nutzen Sie hierfür das Fake-Konto „test@localhost“, welches wir für das CDI Forensik-System zu diesem Zweck angelegt haben. Alternativ ist es möglich, die „profiles.ini“ des Thunderbird-Profiles des CDI Forensiksystemes mit dem absoluten Pfad zum Thunderbird-Profil von Windows zu versehen (und dort auch „IsRelative = 0“ zu setzen). Dies hat jedoch den Nachteil, dass je nach Einstellungen unter Umständen anstehende Emails heruntergeladen werden.
Das Programm „Mailboxen öffnen“ verwendet im Hintergrund das Kommandozeilenprogramm „readpst“.

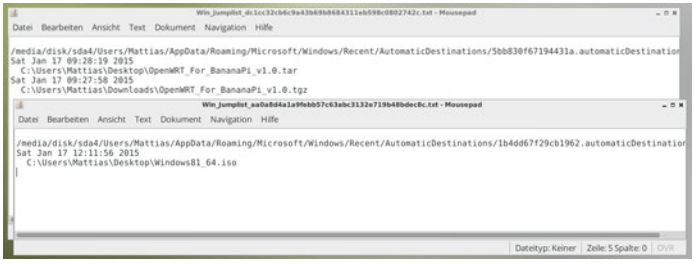
Dateiverläufe ermitteln

Windows nutzt seit Vista sogenannte Dateiverläufe oder Jumplists um einfach auf die letzten geöffneten Dateien zugreifen zu können. Jumplists können global oder Programm spezifisch erstellt werden. Zu-

dem gibt es selten benutzte systemweite Dateiverläufe, sowie häufiger verwendete Profil spezifische. Das Programm „Dateiverläufe ermitteln“ sucht Jumplists und wandelt diese in Textdateien um.



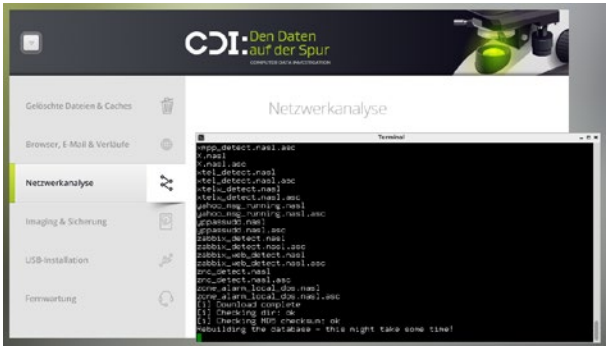
Als zu untersuchendes Verzeichnis geben Sie den Einhängepunkt einer Windows-Partition an, das Ausgabeverzeichnis können Sie auf „/tmp“ belassen, da selbst bei intensiv genutzten Rechnern selten mehr als einige hundert Kilobyte Daten anfallen. Nach Abschluss der Suche und Konvertierung wird das Ausgabeverzeichnis im Dateimananger geöffnet. Die Dateinamen lauten dabei „Win_Jumplist_Prüfsumme.txt“ und können im Texteditor geöffnet werden.



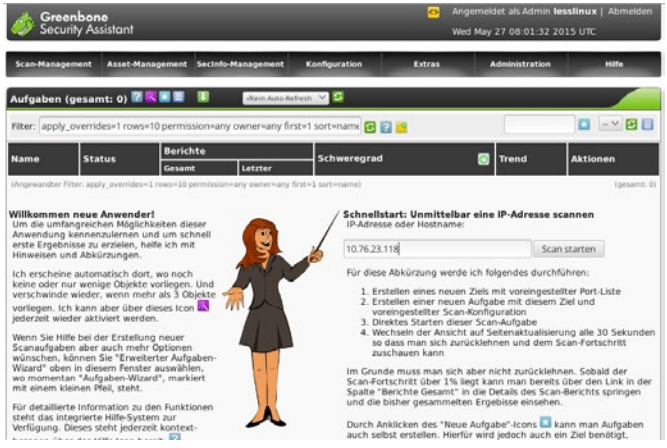
Netzwerkschwachstellen-Scan (OpenVAS)

OpenVAS („Open Vulnerability Assessment Scanner“) ist der freie Nachfolger des Schwachstellenscanners „Nessus“. OpenVAS dient dabei dem Aufspüren verwundbarer Rechner im Netz und eignet sich daher ideal zum Einsatz in Heim- und Firmennetzen. Da OpenVAS eine relativ große Schwachstellen- und Test-Sammlung herunterlädt (~300MB Download, ca. 1,5GB entpackt), sollte das CDI Forensik-System vor der Nutzung von OpenVAS auf einen wenigstens acht Gigabyte großen USB-Stick installiert und neu gestartet werden. Auf Rechnern mit vier Gigabyte RAM oder mehr ist die Nutzung von DVD möglich, wird aber nicht empfohlen.
Eine Nutzung per WLAN ist prinzipiell möglich. Um die Latenzen zu minimieren empfehlen wir jedoch, den Computer, mit dem der Schwachstellenscan durchgeführt wird, per Ethernet mit dem Router zu verbinden.
OpenVAS ermittelt laufende Dienste und deren Versionen und führt (zerstörungsfreie) Penetrationstests durch, prüft beispielsweise DSL-Router auf unsichere Webinterfaces, Smart-TVs auf verwundbare Versionen von Streaming-Protokollen oder Windows-Server auf fehlende Patches für Komponenten der Datei- und Verzeichnisfreigabe. Einzige Ausnahme sind Netzwerkdrucker, hier beschränkt sich OpenVAS auf die Identifizierung des Gerätes, weil einige Tests hohe Tinten- und Papierverbräuche zur Folge haben könnte.

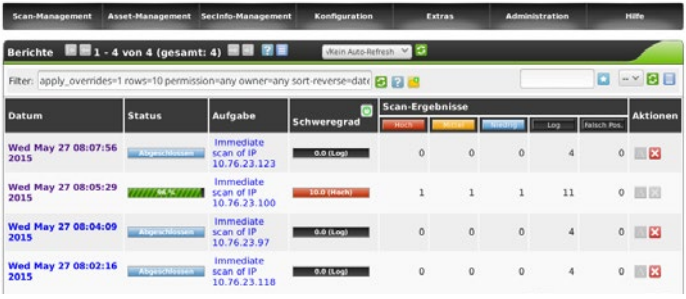
Beim ersten Start lädt OpenVAS eine Datenbank mit Penetrationstests herunter und konvertiert diese. Bei künftigen Tests werden nur neu hinzugekommene Tests heruntergeladen und importiert. Der erste Aufbau der Datenbank kann zwanzig Minuten oder länger dauern, dabei hängt die Geschwindigkeit auch stark vom verwendeten USB-Stick ab. Da viele kleine Dateien gelesen werden müssen, stellt der Prozessor selten den Flaschenhals dar. Sollte der erste Start länger als 30 Minuten dauern, schließen Sie das Terminalfenster und starten Sie OpenVAS erneut. Künftige Starts von OpenVAS liegen dann meist im Bereich von drei bis zehn Minuten.



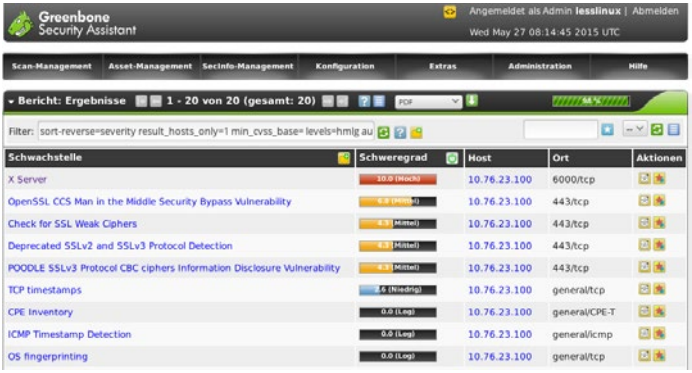
Nach dem Start von OpenVAS öffnet sich Firefox mit der OpenVAS Login-Maske. Verwenden Sie hier den Nutzernamen und das Passwort „lesslinux“ um sich anzumelden. Im OpenVAS-Administrations-Frontend „GSA“ können Sie nun direkt zum „Quickscan“ wechseln. Geben Sie dafür die IP-Adresse des zu scannenden Gerätes in das Eingabefeld neben „Scan starten“ ein. Die IP-Adresse ermitteln Sie in der Regeln aus den Netzwerkeinstellungen des zu scannenden Gerätes oder aus der Geräteübersicht des DSL-Routers.



Wechseln Sie nun zu „Scan-Management > Berichte“. Hier erhalten Sie einen Überblick über die Berichte laufender und abgeschlossener Scans. Sollten bereits Sicherheitslücken gefunden worden sein, wird dies angezeigt.



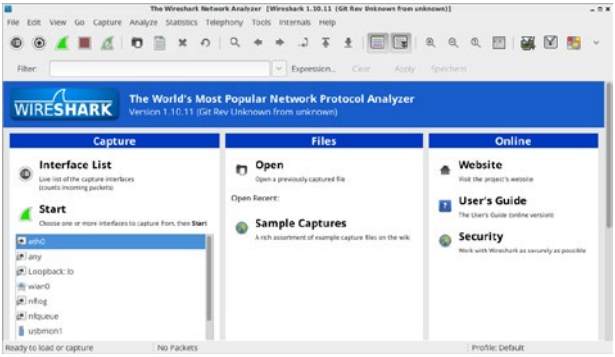
Mit einem Klick auf das angezeigte Datum gelangen Sie zum dem Bericht des Scans. Der hier rot markierte Rechner mit IP-Adresse 10.76.23.100 ist ein älterer Samsung Smart TV, der durch mehrere potentielle Schwachstellen beeindruckt. Ein Klick auf die Schchstelle zeigt Details zur Verwundbarkeit und deren Behebung. Im Falle unseres Samsung Smart TVs dürfte das größte Problem nicht der X-Server an erster Stelle sein, sondern die SSL-Verwundbarkeit an zweiter Stelle, die es ermöglicht, Updates zu kompromittieren oder Datenverkehr mitzulesen.



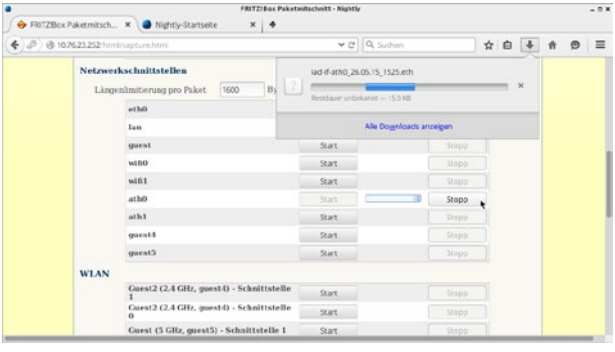
Ein sehr praktisches Werkzeug ist ein Assistent, mit dem Sie ein komplettes Netzwerk scannen können. Wechseln Sie daür zu „Scan-Management > Aufgaben“ und klicken Sie auf das Zauberstab-Symbol, um den „Wizard“ zu starten. Hier wechseln Sie zu „Aufgaben-Wizard > Erweiterter Aufgaben-Wizard“. In diesem Assistenten können Sie ein komplettes Netzwerk scannen, indem Sie die den zu scannenden Bereich als „192.168.1.1-192.168.1.254“ angeben. Zudem haben Sie die Möglichkeit als Scan-Konfiguration „Full and very deep“ oder gar „Full and very deep ultimate“ anzugeben. Der Sicherheitsscan dauert dann deutlich länger und kann Abstürze des Zielsystems verursachen, aber es sinkt das Risiko unentdeckter Sicherheitslücken.

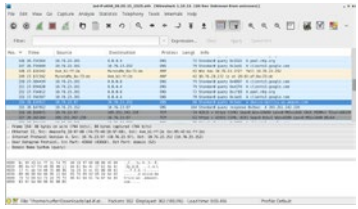
Traffic-Analyse (Wireshark)

Wireshark ist ist ein sogenannter Traffic-Sniffer, der Netzwerkverkehr „abschnüffeln“ und schließlich sortieren und anderweitig aufbereiten kann. Sie können Wireshark beispielsweise dazu benutzen, den Verkehr eines Smart TVs (der Werbung von den Servern des Herstellers nachlädt) zu analysieren oder mit Schadsoftware infizierte Windows-Rechner, die Spam verschicken zu identifizieren. Um den vollen Funktionsumfang von Wireshark nutzen zu können, sollten sowohl der zu analysierende Rechner als auch der PC, auf dem Sie das CDI Forensik-System gestartet haben, mit demselben Netzwerk-Switch verbunden sein. Ist dies nicht möglich (beispielsweise weil das zu analysierende Gerät nur über eine WLAN-Schnittstelle verfügt), können Sie – im Falle dass der WLAN-Accesspoint die Pakete nicht zum Forensik-Rechner durchreicht – den DSL-Router die Netzwerkpakete mitschneiden lassen und diese unter Wireshark analysieren.



Wireshark begrüßt Sie mit einer Liste der Netzwerkschnittstellen. Suchen Sie hier die Schnittstelle aus, von der Traffic mitgeschnitten werden soll, in der Regel ist dies „eth0“ oder „eth1“ (die erste und die zweite Ethernetschnittstelle). Klicken Sie dann auf die grüne Haifischflosse, die mit „Start“ beschriftet ist. Sie sehen nun die aktuell übers Netzwerk laufenden Pakete und deren Absender sowie Empfänger in Echtzeit. Mit dem Klick auf das rote Quadrat stoppen Sie den Mitschnitt wieder. Nach Abschluss des Mitschnittes können Sie die Tabelle nach Absender oder Empfänger sortierenb und den Inhalt der Pakete betrachten. Ist ein Mitschnitt interessant, speichern Sie diesen mittels „File > Save as...“ ab.





Analog laden Sie einen gespeicherten Mitschnitt. Dies gilt auch für Mitschnitte, welche Sie aus anderer Quelle beziehen, beispielsweise Ihren DSL-Router. Bei einer Fritzbox können Sie den Mitschnitt im Wireshark-Format unter der Adresse http://fritz.box/html/capture.html starten. Hier können Sie beispielsweise die Schnittstellen „ath0“ und „ath1“ auswählen, um WLAN-Traffic mitzuschneiden und direkt innerhalb des CDI Forensik-Systems zu speichern. Klicken Sie „Start“, um den Mitschnitt zu starten. Mit „Stop“ schließen Sie ihn ab. Die heruntergeladene Datei mit Endung „.eth“ können Sie nun über „File > Open“ in Wireshark öffnen und analysieren.

CDI als Accesspoint

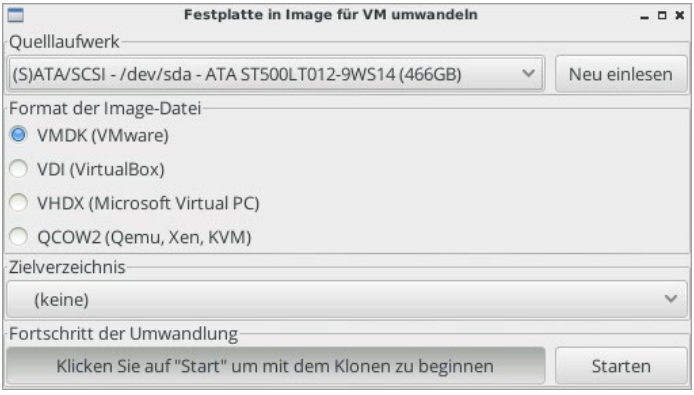
Steht kein DSL-Router mit Mitschnittfunktion bereit, können Sie CDI als Accesspoint konfigurieren. Hierfür wird eine WLAN-Karte benötigt, die sich im Accesspoint-Modus betreiben lässt und eine Ethernetverbindung zum DSL- oder Kabel-Router. WLAN-zu-WLAN-Brücken sind mit dem Assistenten noch nicht möglich, selbst wenn der Chipsatz dies unterstützt oder mehrere WLAN-Karten vorhanden sind. Linux versierte Nutzer können diese aber auf der Kommandozeile unter Verwendung der Programme „wpa_supplicant“, „brctl“ und „hostapd“ manuell konfigurieren. Gestartet wird der Accesspoint über den Menüeintrag „Zubehör > WLAN Accesspoint“. Wenn der Accesspoint erfolgreich gestartet wurde, können Sie mit Wireshark den gesamten Verkehr, der über den Accesspoint läuft (in beide Richtungen) über die Netzwerkschnittstelle „bridge0“ untersuchen.

Das Stoppen des Accessponts hat minunter zur Folge, dass gar keine Netzwerkkommunikation mehr möglich ist: Einige WLAN-Chips schalten zwar problemlos vom Modus STA („Station“) nach AP („Accesspoint“), aber nicht zurück. In diesem Fall hilft nur ein Neustart des gesamten Systems.

Achtung: Falls Sie einen unverschlüsselten Accesspoint mit generischem Namen wie „Hotel WLAN“ o.ä. aufsetzen um zu überprüfen, welche Daten ein Mobiltelefon oder Tablet ungesichert und damit leicht abfangbar überträgt, stellen Sie durch geeignete Maßnahmen (bspw. DHCP nur für bekannte Geräte) sicher, dass Sie nicht versehentlich die Kommunikation unbeteiligter Dritter abfangen!

Image erstellen

Die Funktion „Image erstellen“ hilft bei der Sicherung des kompletten Festplatteninhaltes in Form einer Datei. Das hier gestartete Programm erstellt Images, die auch von gängigen virtuellen Maschinen wie Vmware, VirtualBox oder Qemu verwendet werden können. So ist es möglich, das Image eines Rechners nach Zurücksetzen des Administratorpasswortes in einer virtuellen Maschine zu starten und so auch automatisch gestartete Anwendungen zu analysieren.



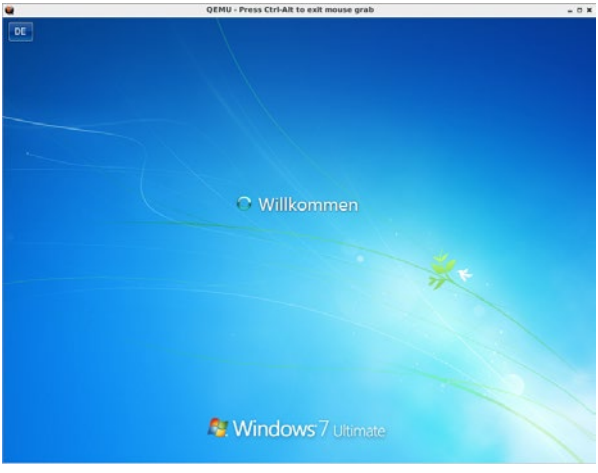
Achten Sie bei der Auswahl des Zielverzeichnisses darauf, dass sämliche Blöcke, die nicht mit Nullbytes beschrieben sind, mitgesichert werden, das Image demnach auch bei nicht vollständig belegter Festplatte fast die Größe der zu sichernden Festplatte erreichen kann.
Wählen Sie das Format nach dem späteren Einsatzzweck: Wollen Sie das Image primär in einer virtuellen Maschine unter Windows nutzen, wählen Sie „VMDK" (Vmware) oder „VDI" (VirtualBox). Bei der Verwendung von Qemu/KVM unter Linux ist Qcow2 am besten geeignet. Qcow2 kann unter Linux auch direkt eingebunden werden und hat sich hier als sehr flexibel erwiesen. Eine spätere Umwandlung in andere Formate ist jederzeit mit dem Programm „qemu-image" möglich.
Nach dem Klick auf „Starten" beginnt die Erstellung des Images. Die Dauer hängt dabei maßgeblich von der Geschwindigkeit von Quell- und Zielfestplatte ab. Typische Werte bei einem Ziel auf USB 2.0 liegen bei ca. 30 bis 40MB/s, die Erstellung eines Images einer 500GB-Platte dauert demnach drei bis vier Stunden.

Forensische Formate und defekte Festplatten

Image-Formate virtueller Maschinen sind praktisch, weil vielseitig. Doch auch sie stoßen an Grenzen. Weist eine Festplatte bereits Defekte auf, bricht die Erstellung des Images ab, selbst wenn nur wenige Blöcke nicht lesbar sind. Verwenden Sie in diesem Fall „Anwendungsmenü > Rettungswerkzeuge > Rettungs-Image erstellen", um ein Image im „rohen" Format zu erstellen. Sie können dieses Image auf Wunsch mit dem Programm „qemu-image" in die Formate virtueller Maschinen konvertieren.
Soll ein Image tatsächlich gegen Manipulationen geschützt sein, beispielsweise weil Sie den Verdacht haben, dass mit einem Rechner ernsthafte Straftaten begangen wurden und das Image daher möglicherweise Experten bereitgestellt werden, verwenden Sie das Programm „ewfacquire", um ein Image im „Expert Witness Format" („EWF") zu erstellen. Die Verwendung der EWF-Werkzeuge stellt mit Prüfsummen sicher, dass ein Image nicht manipuliert wird. Sie können das erstellte EWF-Image später mit „ewfexport" als „rohes" Image exportieren.

Image in VM ausführen

Im Qcow2-Format erstellte Images können Sie direkt als virtuelle Maschine starten. Hierfür kommt die Virtualisierungssoftware Qemu mit den KVM-Erweiterungen zum Einsatz. Um diese nutzen zu können, muss der PC auf dem Sie das Image in der virtuellen Maschine starten wollen, über Virtualisierungserweiterungen verfügen. Dies ist typischerweise bei ab 2009 eingeführten 64-Bit-Prozessoren der Fall. Bitte beachten Sie, dass die virtualisierte Hardware von Qemu möglicherweise stark von der im PC vorhandenen Hardware abweicht. Erfahrungsgemäß hat damit vor allem Windows XP Probleme, Vista und höher installieren in der Regel automatisch die benötigten Treiber. Eine sinnvolle Speichereinstellung liebt bei mindestens 512MB für Windows XP und einem Gigabyte oder höher für die Nachfolger.
Das Image startet nun in einem Qemu-Fenster. Der Mauszeiger bleibt in der Regel gefangen, bis Sie die Tastenkombination „Strg+Alt“ drücken.



Images unverändert lassen

Ein Problem beim Start von einem Image ist, das dieses dadurch verändert und möglicherweise verfälscht wird. Schlimmer noch: Es gibt Schadsoftware, die sich selbst löscht, wenn sie feststellt, dass sie in einer virtuellen Umgebung ausgeführt wird. Sie können dies verhindern, indem Sie ein „Schattenimage" oder „Overlay" erstellen, in das sie Schreibzugriffe umleiten. Ab CDI 2016 ist die Verwendung von Schattenimages Standard, Sie müssen lediglich den Ordner angeben, in dem das Schattenimage erstellt werden soll. Bei einem von DVD gestarteten System können Sie mit „/tmp" die Änderungen im Arbeitsspeicher belassen, wenn der PC über genügend RAM (6GB oder mehr) verfügt. Bei weniger RAM oder wenn Persistenz gewünscht ist sollten Sie das Schattenimage auf einer eingebundenen Partition, die entweder NTFS oder eines der Linux-Dateisysteme (ext4, btrfs...) nutzt ablegen. FAT ist nur bedingt geeignet, da die maximale Dateigröße dort etwas kleiner als vier Gigabyte ist.

Images mounten

Images in den meisten Formaten, die „qemu-img" bearbeiten kann, können unter Linux eingebunden oder gemountet werden. Der Weg dafür führt über ein sogenanntes „Network Block Device". Dafür wird zunächst der Treiber geladen und dann das Image einem Gerät zugeordnet - „-r" steht hier für „read only":

```
qemu-nbd -r -c /dev/nbd0 sda.qcow2
```

Nun werden die Partitionsmappings erstellt, Mountpoints angelegt und schließlich die benötigten Partitionen eingebunden:

```
kpartx -r -a -s /dev/nbd0
mkdir -p /media/nbd/nbd0p1
mkdir -p /media/nbd/nbd0p2
mount -o ro /media/nbd/nbd0p1
mount -o ro /dev/mapper/nbd0p2 /media/nbd/nbd0p2
```

Umgekehrt geben Sie das Image wieder frei: Zunächst hängen Sie die Partitionen aus, dann lösen Sie die Partitionsmappings und schließlich das Network Block Device:

```
umount /dev/mapper/nbd0p1
umount /dev/mapper/nbd0p2
dmsetup remove /dev/mapper/nbd0p1
dmsetup remove /dev/mapper/nbd0p2
qemu-nbd -d /dev/nbd0
```

USB-Installation

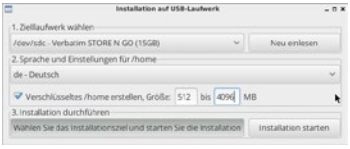
Der Programmstart von DVD ist mitunter recht langwierig, zudem entfallen hier die Möglichkeiten, Daten auf dem Startmedium abzuspeichern. Da OpenVAS sehr viel Speicher für seine Datenbanken benötigt, ist für die Nutzung dieses Programms die USB-Installation zwingend erforderlich. Zudem kann das auf USB installierte Forensik-System immer am Schlüsselbund dabei sein und Sie können auch Netbooks oder Ultrabooks mit dem Live-System starten.

Ihr Stick muss mindestens 4 Gigabyte Speicherkapazität besitzen und natürlich keine noch wichtige Daten enthalten, da diese vollständig überschrieben werden. Sticks mit mehr Speicherkapazität empfehlen sich für folgende Fälle:

- **Ab 8 Gigabyte (empfohlen):** Der Stick wird beim ersten Start partitioniert. Er erhält eine Auslagerungspartition und eine Partition für persistent gespeicherte Erweiterungen wie OpenVAS-Datenbanken oder Virensignaturen. Zudem wird Auslagerungsspeicher erstellt, der gerade bei Aufgaben, die viel RAM erfordern, das System entlastet.
- **Ab 16 Gigabyte:** Sie haben die Möglichkeit, zusätzlich ein verschlüsseltes Heimatverzeichnis zu erstellen und so Firefox-Lesezeichen, Firefox-Synchronisationseinstellungen oder ein E-Mail-Konto dauerhaft zu sichern. Das Heimatverzeichnis wird mit Linux' Standard-Verschlüsselungsmechanismus LUKS verschlüsselt und verhindert den Zugriff auf verlorene Sticks, wenn ein hinreichend sicheres Passwort benutzt wurde. Die empfohlene Größe beträgt 4096MB.

Die Verwendung größerer Sticks (typischerweise bis 64GB) hat den Vorteil, dass Sie ein noch größeres verschlüsseltes Heimatverzeichnis

(16384MB) erstellen können und zudem die unter Windows sichtbare erste Partition ernsthaft für den Datenaustausch genutzt werden kann. Von der Verwendung von Sticks mit 128GB oder externer Festplatten/SSDs dieser Größe raten wir ab, da viele BIOSe Bootprobleme mit derart großen USB-Datenträgern haben.
Hinweis: Soll das Forensik-System auf einem Computer mit weniger als vier Gigabyte RAM ausgeführt werden, ist der Start von einem USB-Stick ab 8GB dringend empfohlen, da sonst Programmabstürze auf Grund von Speichermangel auftreten können.



Wählen Sie jetzt das ‚Ziellaufwerk' (also den USB-Stick), bestimmen Sie die ‚Sprache' und aktivieren Sie die Option ‚Verschlüsseltes /home erstellen', wenn Sie möchten, dass auf dem Stick später auch permanent Daten abgelegt werden sollen, beispielsweise wichtige Dokumente. Die Größe des Home-Verzeichnisses richten Sie dabei an der verbliebenen Gesamtkapazität des Sticks aus.

Klicken Sie abschließend auf ‚Installation starten'.

Fernwartung

Für die Fernwartung eines PCs enthält das „CDI Forensik-System" drei unterschiedliche Programme:

- **Teamviewer:** Zur Fernwartung über das Internet oder innerhalb lokalen Netzwerken. Da Teamviewer Versionen für verschiedene Betriebssysteme anbietet, kann Windows auch während der Wartung aktiv sein. Mit Teamviewer können Sie Ihren Desktop für Dritte freigeben oder umgekehrt auf den freigegebenen Desktop eines anderen Rechners zugreifen. Sie erlangen dabei die gleichen Rechte wie der Anwender des Gastsystems.
- **VNC:** Mit VNC lassen sich Wartungsarbeiten innerhalb eines vertrauenswürdigen lokalen Netzes in Angriff nehmen - nicht jedoch über das Internet, da VNC keine Verschlüsselung verwendet und somit angreifbar ist.
- **Remmina:** Remmina kommt als Client zum Zugriff auf Computer zum Einsatz, die Zugang per RDP oder VNC anbieten.

Fernwartung mit Teamviewer

Die Fernwartung eines Rechners mit Teamviewer ist außerordentlich einfach. Klicken Sie im Assistenten auf ‚Fernwartung > Fernzugriff mit Teamviewer', und notieren Sie sich sowohl die ‚ID' als auch das ‚Kennwort', das Ihnen das Programm kurz darauf mitteilt. Diese beiden Daten übermitteln Sie der Person, die Sie beim Analysieren unterstützen soll. Sie stellt daraufhin Verbindung her und kann Ihnen über die Schulter blicken oder Tastatur und Maus übernehmen.

Weitere Werkzeuge

Netzwerk und Internet

Ihr CDI Forensik-System startet mehr oder weniger ‚eingekapselt' als autarkes System ohne Zugriff auf Festplatten und nur mit Zugriff auf ein kabelgebundenes Netzwerk. Da nicht überall drahtgebundenes Internet zugänglich ist, unterstützt das CDI Forensiksystem die gängigsten WLAN-Chipsätze und -Verschlüsselungsverfahren.
Zugriff auf den Verbindungsmanager erhalten über das Netzwerksymbol im Dock.

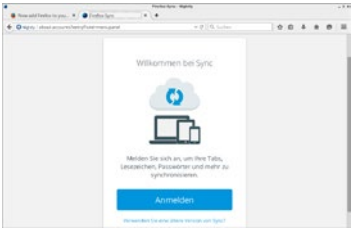
- Verfügen Sie über einen WLAN-Empfänger, beispielsweise einen USB-WLAN-Stick, listet Ihnen das „S.A.D. Notfall-System" alle erkannten Funknetzwerke auf. Wählen Sie Ihres aus und klicken Sie auf ‚Verbinden' oder ‚Properties' (‚Eigenschaften').
- Im nächsten Fenster wählen Sie die Art der Verschlüsselung aus, mit der Ihr WLAN abgesichert ist (in aller Regel WPA2) und geben Sie das Verbindungspasswort ein.
- Soll künftig automatisch eine Verbindung zu diesem Netz erstellt werden, klicken Sie auf „Automatically connect to this network" - diese Information und das Passwort wird bei Verwendung eines verschlüsselten Heimatverzeichnisses gespeichert
- Bestätigen Sie mit ‚OK'. Die Verbindung wird nun automatisch eingerichtet.

Netzlaufwerke verbinden

Über „Anwendungsmenü > Zubehör > CIFS- oder WebDAV-Freigaben einbinden“ können Sie Windows-Freigaben im lokalen Netz (beispielsweise vom Samba-Server einer NAS) oder WebDAV-Speicher im Internet (beispielsweise T-Online- oder GMX-Mediacenter) als Laufwerk einbinden. So umgehen Sie mögliche Platzbeschränkungen lokaler Laufwerke.
Um Zugriff auf Netzlaufwerke zu erhalten, müssen Sie deren Adresse im Netz wie beispielsweise ‚‘ kennen sowie die Benutzerdaten für den Zugriff (Name und Passwort) zur Hand haben. Windows-Freigaben einer NAS im lokalen Netz werden in der Form ‚cifs://12.34.56.78/share‘ geschrieben.

Haben Sie diese Daten nicht parat, fragen Sie Ihren Systemadministratoren oder rufen Sie die Supportseiten Ihres Providers auf, die in aller Regel ebenfalls die notwendigen Angaben bereithalten. Unterstützt werden neben WebDAV-Freigaben von der Telekom auch 1und1 und GMX. Viele weitere Anbieter unterstützen WebDAV, informieren Sie sich auf den Webseiten Ihres Speicheranbieters über Servernamen und Aufbau der Zugangsdaten.

Im Netz surfen und Mails lesen



Mit Firefox ist ein vollwertiger Webbrowser installiert, der jedoch aus Lizenzgründen keinen Flash-Player und eine etwas reduzierte Codec-Unterstützung für HTML5-Videos enthält. Prinzipiell empfehlen wir die Nutzung eines verschlüsselten Heimatverzeichnisses und die Nutzung von „Firefox Sync“ zum automatischen Abgleich von Lesezeichen mit Ihrem desktop-Firefox.

Gleiches gilt für Mozilla Thunderbird als Email-Client: Richten Sie Thunderbird für den IMAP-Zugang zu Ihren Mailkonten ein, achten Sie aber darauf, dass nur Nachrichten, die kleiner als 50kB sind, automatisch heruntergeladen werden. So verhindern Sie, dass Nachrichten mit großen Anhängen lokal zwischengespeichert werden und dadurch den knappen Speicherplatz einschränken. Beim Doppelklick auf eine Nachricht wird diese dennoch vollständig heruntergeladen.

Virenscan

In vielen Fällen verursacht Schadsoftware „anormales" Verhalten eines PCs. Die Suche nach Viren und Trojanern beziehungsweise die Möglichkeit, eine Infektion weitgehend auszuschließen sind daher ein sinnvoller Analyseschritt.
Verwenden Sie „Anwendungsmenü > Zubehör > Software installieren", um den Virenscanner „AVG AntiVirus free" herunterzuladen und zu installieren. Das System sollte hierfür bereits auf USB installiert und von dort gestartet worden sein.

Öffnen Sie nach der Installation ein Root-Terminal und führen Sie dort den Befehl „avgupdate“ aus. Nach der erfolgreichen Aktualisierung der Virensignaturen können Sie mit dem Kommando
avgscan /media/disk/sda2
den Inhalt der zweiten Partition der ersten Platte scannen. Verwenden Sie „avgscan –help“, um Hinweise zu den Scan-Einstellungen wie Scan von Archiven oder Heuristiken zu erhalten.

Hinweis: AVG überschreitet keine Mountpoints! Wenn Sie als Scan-Ordner „/media/disk“ angeben, wird keiner der darunter eingebundenen Ordner gescannt. Führen Sie stattdessen einzelne Scans auf jedem Mountpoint durch!

FRED Forensic Registry Editor

Mitunter finden sich die Spuren von Schadsoftware beziehungsweise deren Aktionen in der Registrierungsdatenbank von Windows. Gelegentlich tauchen gar Schädlinge auf, die sich komplett in der Registry verstecken. Bei der Analyse der Registry helfen Registry-Editoren mit Zugriff auf Binärschlüssel. Mit FRED enthält das CDI Forensik-System einen derartigen Registry-Editor. Sie starten ihn über „Anwendungsmenü > Weitere Wartungswerkzeuge > FRED Registry Editor“. 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

„Hackers Delight“

Verwenden Sie Passwörter, die sicher genug sind? Finden Sie es heraus: CDI bringt Passwortknacker für unterschiedliche Typen von Passwort-Datenbanken und Netzwerkprotokolle mit. Deren typischer Einsatz-

zweck 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.

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 oder LUKS zu knacken.

Ophcrack

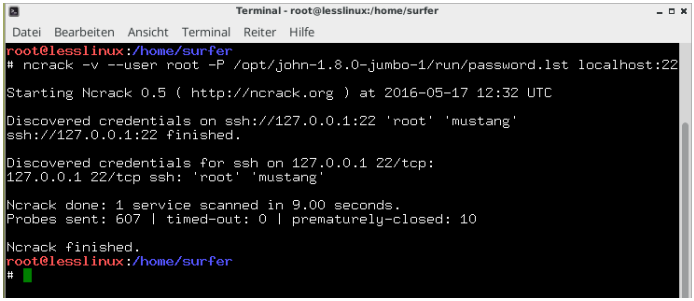
Anders als John arbeitet „ophcrack" mit Regenbogentabellen, also Tabellen vorberechneter Hashes aus praktisch beliebigen Zeichenkombinationen. Diese Hashtabellen sind in Versionen mit verschiedenen Längen und unterschiedlich umfangreichen Zeichensätzen erhältlich und typischerweise einigen Gigabyte bis mehrere Terabyte (!) groß. Für die praktikable Nutzung sollten die Hashtabellen daher auf eine hinreichend schnell angebundene Festplatte oder SSD abgelegt werden. 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.

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.

Aircrack-ng

Die Programmsuite „aircrack-ng“ kann zum Überwachen unverschlüsselter Funknetze und zum Knacken von WEP-/WPA-/WPA2-Schlüsseln verwendet werden. „aircrack-ng“ bietet zudem die Möglichkeit, manipulierte Pakete zu senden, wofür aber oft spezielle Treiber notwendig sind. Da „aircrack-ng“ bereits bei der Hardwareauswahl viel Aufmerksamkeit erfordert und die Verwendung viel Hintergrundwissen über verwendete Protokolle erfordert, möchten wir an die Webseite des Projektes verweisen, wo Sie viele Tutorials zum Einsatz des Programms finden: http://www.aircrack-ng.org/

Copyright | Support

Aktualisierte Versionen des Handbuchs werden über die Update-Funktion des CDI-Forensik-Systems bereitgestellt, sofern dies durch künftige Entwicklungen erforderlich sein sollte.

Hinweise und Verbesserungsvorschläge bitte an

support@s-a-d.de

oder

ms@mattiasschlenker.de.

Unseren Support erreichen Sie kostenlos per E-Mail

support@s-a-d.de

oder auf

www.sad-support.com

C.D.I. – Den Daten auf der Spur
NUTERZERHANDBUCH