X-Ways Software Technology AG • Agrippastr. 37-39 • D-50676 Köln
Web: http://www.x-ways.com • E-Mail: mail@x-ways.com • Tel.: +49-221-420 486 5 • Fax: +49-721-151 322 561

X-Ways Capture

Kurzbeschreibung

X-Ways Capture ist ein spezialisiertes Computerforensik-Tool für die elektronische Beweismittelsicherung unter Windows und Linux. Es sucht in einem laufenden System mit unterschiedlichen Methoden nach Anzeichen von laufender Verschlüsselungssoftware, und es erkennt aktiven ATA-Festplatten-Passwortschutz. Es sichert den Arbeitsspeicher und angeschlossene Datenträger des laufenden Systems auf einen vom Benutzer anzugebenden Zieldatenträger, z. B. eine externe USB-Festplatte. Dadurch stehen nach dem Ausschalten des Computers auch solche Daten noch für eine forensische Untersuchung zur Verfügung, die einer Verschlüsselung oder anderem Zugriffsschutz unterworfen, aber zum Zeitpunkt der Sicherung gerade per Passwort freigeschaltet waren. So vermeiden Sie, wie nach dem Abschalten des Computers und einer konventionellen Sicherung mit leeren Händen dazustehen, wenn Sie feststellen, dass die relevanten Dateien verschlüsselt sind. Etwaige Passwörter lassen sich u. U. zudem später im gesicherten Arbeitsspeicher finden. Alle Arbeitsschritte und Einstellungen sind weitgehend vom Benutzer im voraus konfigurierbar und werden mitprotokolliert.

Funktionsweise

X-Ways Capture besteht aus zwei Modulen, eines für Windows 2000/XP, das andere für Linux (jeweils auf Intel-x86-Architektur, egal ob Workstation oder Server). Das Ausführen des jeweils falschen Moduls ist normalerweise unmöglich, wird andernfalls erkannt und abgefangen.

Dem Benutzer muss bewusst sein, dass durch das Anschließen eines weiteren Datenträgers und das Ausführen von X-Ways Capture das laufende System (zumindest ein kleiner Teil des Arbeitsspeichers) geringfügig verändert wird. Um X-Ways Capture möglichst klein und sparsam an Ressourcen zu halten, wurde es als reines Kommandozeilenprogramm entwickelt, ohne graphische Oberfläche. Dadurch wird beim Laden des Programms so wenig Arbeitspeicher wie möglich verändert und die Wahrscheinlichkeit sehr gering gehalten, dass das Betriebssystem Arbeitspeicher auf die Festplatte auslagert, bevor gesichert wird. *Um geschützte Daten im unverschlüsselten Zustand sichern zu können, bleibt Ihnen in vielen Fällen keine andere Wahl, als eine solche geringfügige Änderung in Kauf zu nehmen.*

Beachten Sie außerdem, dass im laufenden Betrieb vorgenommene physische Sicherungen aus Betriebssystemsicht ggf. keinen *konsistenten* Zustand abbilden, weil sich z. B. gerade bestimmte temporäre Dateien im Zugriff befanden.

Das Programm führt folgende Schritte aus, wenn nicht in der Konfigurationsdatei etwas anderes festgelegt wurde:

- Sichern des physischen Arbeitsspeichers und (unter Windows) des Speichers aller laufenden Prozesse
- Erkennen von aktivem ATA-Passwortschutz, Erkennen von Host-Protected Areas (HPAs)
- Erkennen von aktiver Verschlüsselungssoftware
- physisches Sichern angeschlossener Datenträger (sektorweise)

- logisches Sichern (Kopieren) von Dateien

Die Sicherung des Arbeitsspeichers wird standardmäßig als erstes durchgeführt, damit der Speicher soweit wie möglich im Originalzustand gesichert wird. Anschließend wird der Rechner auf Einstellungen und Programme untersucht, die den Zugriff auf die Daten nach einer evtl. Abschaltung erschweren. Dies sind ATA-Passwortschutz sowie Verschlüsselungssoftware. Dann werden je nach Befund die angeschlossenen Datenträger ggf. physisch gesichert. Diese Sicherung wird in der Voreinstellung vor der logischen Sicherung durchgeführt, um ein möglichst unverfälschtes Abbild der Festplatten zu erhalten. Erst im Anschluss hieran findet ggf. die logische Sicherung statt.

Falls die Images und die zu logisch zu kopierenden Dateien nicht auf einen Datenträger passen, fragt das Programm neue Datenträger an. Auch die Protokolldatei wird dann auf diesem Datenträger fortgesetzt. Um das Protokoll später wieder richtig zusammensetzen zu können, werden die Teildateien fortlaufend nummeriert.

Alle Dateien werden im Zielpfad der Sicherung mit einem Präfix benannt, das sich aus Datum und Uhrzeit des Beginns der Programmausführung ergibt. Die Protokolldatei hat z. B. den Namen <*Präfix*>-log-<*fortlaufende Nummer*>.txt.

Die Konfigurationsdatei steuert im Abschnitt [steps] die genaue Abfolge der Schritte. Jeder auszuführende Schritt wird im [steps]-Abschnitt erwähnt. Die Schritte sind im einzelnen:

0. Programmstart, Erkennung des Betriebssystems

a) Das Windows-Modul erkennt die exakte Windows-Version und verhindert einen Start unter Linux mittels Wine. Das Linux-Modul erkennt die exakte Linux-Version und ist nicht unter Windows ausführbar.

b) Die Aufrufparameter werden geparst. Hier kann der Zielpfad angegeben werden, oder mit –i <*Dateiname*> kann eine andere Konfigurationsdatei als capture.ini verwendet werden.

c) X-Ways Capture fragt den Benutzer nach dem Zielpfad für die Ausgabe der Protokolldatei und Sicherungen, wenn beim Programmstart kein Pfad als Parameter angegeben wurde. Dieser Pfad wird im folgenden als Ziel bezeichnet. Der angegebene Pfadname muss absolut sein.

d) Aus der aktuellen Uhrzeit wird ein Zeitstempel der Form JJJJ-MM-TT, HH-MM-SS erzeugt. Der Vorteil dieses Formats besteht darin, dass alle Dateibrowser so benannte Dateien chronologisch sortiert auflisten. Optional kann durch die Befehle GetUserDate, GetUserTime die tatsächliche Uhrzeit protokolliert werden, damit später nachvollzogen werden kann, ob die Systemzeit verstellt war.

e) Damit die Konfiguration von X-Ways Capture später nachvollzogen werden kann, wird capture.ini ins Protokoll kopiert. [steps]-Name: AppendIni

f) Optional können weitere Daten durch den Ask-Befehl protokolliert werden:
Ask "Text eingeben"
gibt „Text eingeben“ auf dem Bildschirm aus und wartet auf eine Eingabe. Alternativ kann Ask in der Form
Ask "IP Addresse eingeben" ???.???.???.???

verwendet werden, wobei ???.???.???.??? zur Validation herangezogen wird, und für ein ? ein beliebiges Zeichen eingegeben werden darf.

1. RAM-Sicherung

a) Der physische Arbeitsspeicher wird als Roh-Image-Datei auf das Ziel gesichert, sofern der Zugriff nicht durch fehlende Administrator- bzw. Root-Rechte oder sog. Linux Security Enhancements behindert wird. [steps]-Name: DumpPhysicalMemory. Es ist normal, dass Windows den Zugriff auf mehrere kleine Bereiche des Speichers verhindert und X-Ways Capture daraufhin Warnungen ausgibt.

b) Nur unter Windows: Der Speicher der einzelnen Prozesse wird in je eine Datei gesichert. Als Dateiname wird an den Prozessnamen die Nummer des Prozesses angehängt. [steps]-Name: DumpProcessMemory

c) Die Liste der laufenden Prozesse wird protokolliert. [steps]-Name: DumpProcessList

d) Die Liste der Treibernamen wird protokolliert (Windows: DumpDriverList, Linux: AppendToLog /proc/modules)

2. Prüfung von ATA-Festplatten

a) Unter Windows generell, unter Linux nur mit Root-Rechten: Die Modellbezeichnung von ATA-Festplatten und ihre Security-Einstellungen (Passwortschutz) werden ermittelt. [steps]-Name: ATACheck

- Unterstützung des Security Mode Feature Set j/n
- Security Mode aktiv j/n
- Platte gesperrt j/n
- Security Freeze Lock j/n
- Sicherheitslevel hoch/maximum

Für *S*-ATA-Platten kann das Funktionieren nicht garantiert werden. Etwaige gemeldete Resultate für Nicht-ATA-Platten (insbes. Hardware-RAID-Verbunde) sind undefiniert.

b) Nur unter Windows, sofern Zugriff nicht behindert durch fehlende Administratorrechte: Prüfung auf aktive HPA (Host-Protected Area) und entsprechende Mitteilung. [steps]-Name: HPACheck

c) Festplatten und Partitionen protokollieren
Hier wird protokolliert, welche Partition auf welcher Festplatte liegt und wo sie beginnt. Für Festplatten versucht Capture die Modellbezeichnung, die vom Hersteller vergebene Seriennummer (nur unter Windows), Größe und Bustyp zu ermitteln sowie ob es sich um eine „dynamisch“ partitionierte Platte handelt (nur für Windows). Unter Windows gibt es hierfür den Schritt ListMountedVolumes, die Linux-Version der .ini-Datei erreicht dasselbe durch zwei Aufrufe von AppendToLog.

3. Prüfung auf aktive Verschlüsselungssoftware

Dieser Schritt besteht aus mehreren Teilschritten, die zudem vom Betriebssystem abhängen.

Unter Windows wird an folgenden Stellen nach Anzeichen für eine aktive Verschlüsselung

gesucht, wobei der erste Fund die weiteren Teilschritte abbricht, wenn sie nicht durch die Konfigurationsdatei erzwungen werden:

a) EncryptionCheckProcessList:
   Die Namen der aktiven Prozesse werden mit einer Liste bekannter Windows-Verschlüsselungsprogramme im Abschnitt [SearchProcessesForEncryption] abgeglichen. Z. B. ist der Name des residenten Dienstes/Prozesses von PGP Desktop 9.02 „PGPserv.exe“.
b) CheckDriverListForEncryption
   Durchsucht die im Schritt DumpDriverList erzeugte Datei nach Namen, die aus dem Abschnitt [SearchDriverListForEncryption] gelesen werden. Bei Bedarf wird hierfür die Treiberliste erstellt, falls dies nicht bereits geschehen ist.
c) EncryptionCheckProcessMemory:
   In den geladenen .exe-Dateien laufender Prozesse wird nach den Schlüsselwörtern aus dem Abschnitt [SearchProcessMemory] der Konfigurationsdatei gesucht, sowohl im ASCII- als auch im Unicode-Zeichensatz. Dadurch kann ein bekanntes Verschlüsselungsprogramm selbst dann erkannt werden, wenn dessen .exe-Datei umbenannt wurde und damit auch der laufende Prozeß einen unerwarteten Namen hat. Als Schlüsselwörter eignen sich z. B. interne Programmnamen oder Copyright-Hinweise, wie sie in den Versionsinformationen von .exe-Dateien enthalten sind. Z. B. ist „PGPsdkService“ der interne Name des Services „PGPserv.exe“.
d) EncryptionCheckDiskSectors
   Sofern Zugriff nicht behindert durch fehlende Administratorrechte: Mit zwei verschiedenen Methoden werden bestimmte Sektoren jeder Festplatte gelesen und die Ergebnisse verglichen. Unterschiedliche Ergebnisse deuten auf eine Verschlüsselung der betreffenden Festplatte durch ein residentes Programm wie „SecureDoc“ oder „CompuSec“ hin.
e) EncryptionCheckAllFiles
   Alle Dateien auf NTFS-Laufwerken werden auf EFS-Verschlüsselung hin überprüft. Dieser Teilschritt ist je nach Anzahl von Dateien auf NTFS-Laufwerken die zeitintensivste aller Prüfungen in diesem Abschnitt. Der Ausgabedatenträger und das Laufwerk, von dem Capture gestartet wurde, sind von dieser Prüfung ausgeschlossen. Dieser Schritt ist nur dann sinnvoll, wenn LogicalBackup übersprungen wird, da LogicalBackup immer nach EFS-verschlüsselten Dateien sucht und diese gleich sichert. Über den Parameter network kann bestimmt werden, ob Netzlaufwerke von der Suche betroffen sind: +network aktiviert die Suche auf Netzlaufwerken, -network deaktiviert sie. -network ist die Voreinstellung.
f) CheckForBitLockerVolumes
   Sofern Zugriff nicht behindert durch fehlende Administratorrechte: Alle gemounteten Volumes werden auf die BitLocker-Signatur geprüft.

Linux:

a) Die Durchsuchung bestimmter Dateien kann über das EncryptionCheckFile-Kommando im [steps]-Abschnitt gesteuert werden. Für jedes derartige Kommando gibt es einen [EncryptionCheckFile]-Abschnitt. Hinter dem Kommando muss die zu durchsuchende Datei stehen, ebenso in der ersten Zeile des entsprechenden [EncryptionCheckFile]-Abschnitts. Im Rest des entsprechenden [EncryptionCheck File]-Abschnitts stehen die zu suchenden Schlüsselwörter. Sinnvollerweise sollten die Dateien /proc/mounts und /proc/modules durchsucht werden.

b) Die Namen der aktiven Prozesse werden mit einer Liste bekannter Linux-Verschlüsselungsprogramme im Abschnitt [EncryptionCheckProcessList] abgeglichen.

4. **Physische Sicherung** ([steps]-Name: PhysicalImaging)

In diesem Schritt erzeugt Capture physische Sicherungen (Images) von Festplatten, wenn es dies für notwendig erachtet oder wenn der Schritt erzwungen wird. Eine physische Sicherung einer Festplatte funktioniert sektorweise, nicht dateiweise.

a) Falls eine Festplattenverschlüsselung im Schritt EncryptionCheckDiskSectors erkannt wurde oder ein evtl. ATA-Passwortschutz gerade entriegelt ist, wird ein Image der Platte erzeugt.
b) Falls ATA-Passwortschutz für eine Festplatte aktiv ist, aber Capture nicht eindeutig die betroffene Platte erkennen kann, werden alle Platten gesichert.
c) Falls dieser Schritt erzwungen wird, werden ebenfalls alle Festplatten gesichert. Ausnahmen können in der Konfigurationsdatei definiert werden (s. u.).

Von der physischen Sicherung auszunehmende Festplatten können in Form von Modellbezeichnungen in der Konfigurationsdatei angegeben werden (s. u.). Der physische Datenträger, von dem X-Ways Capture aus gestartet wurde, sowie der Zieldatenträger sind automatisch ausgeschlossen. Unter Windows 2000 funktioniert der Ausschluß nur mit festen Datenträgern (Festplatten), nicht mit physischen Wechseldatenträgern wie USB-Sticks.

Bedingung für eine erfolgreiche Sicherung, die mit Zugriff auf Sektorebene arbeitet, ist, dass der im System angemeldete Benutzer dafür ausreichende Rechte hat.

Im Fall einer durch Software verschlüsselten, aber gerade lesbar geschalteten Festplatte werden die durch die Verschlüsselungssoftware entschlüsselten Daten gesichert. Die Sicherungen können als Roh-Images (dd-Images) oder Evidence-Files (.e01-Dateien) erstellt werden. Die Größe der Segmente kann im Abschnitt [settings] konfiguriert werden. Evidence-Files können optional komprimiert werden. Unter Linux wird die Liste vorhandener physischer Datenträger /proc/partitions entnommen. Netzlaufwerke, optische Datenträger oder bestimmte Dateisysteme können über die Konfigurationsdatei von der Sicherung ausgeschlossen werden.

Während der Sicherung kann ein Hash-Wert des gesicherten Datenträgers berechnet und in das Evidence-File bzw. im Fall eines Roh-Image in eine separate Datei geschrieben werden. Wenn während oder nach der Sicherung noch auf den Datenträger geschrieben wird, ist der Hash-Wert nur noch für das Image charakteristisch, nicht mehr für den Datenträger.

5. **Volume-Sicherung** ([steps]-Name: LogicalImaging)

Verschlüsselte Volumes (z. B. erstellt mit Bitlocker oder TrueCrypt) mit können u. a. daran erkannt werden, dass ihr 1. Sektor, wenn von dem Volume gelesen, andere Daten liefert als der entsprechende Sektor auf der Festplatte, wenn von dort gelesen. Ein anderes Kriterium ist, wenn einem Volume keiner Partition auf einer Festplatte zuzuordnen ist (was bedeutet, dass es wahrscheinlich in einer geladenen Container-Datei gespeichert ist). Dieser Schritt prüft alle in Form von Laufwerksbuchstaben geladenen Volumes auf diese Kriterien und fertigt ggf. ein *sektorweises* Image des jeweiligen Volumes an. Im Gegensatz zum bloßen Kopieren der *Dateien* des Volumes werden so auch freier Speicher, Schlupfspeicher, etwaige

gelöschte Dateien, alle Metadaten usw. in verschlüsselten Partitionen und Containern gesichert werden. Der Schritt wird unabhängig von anderen Analyseergebnissen durchgeführt, beeinflusst keine anderen Schritte, und betrifft nur Windows.

6. **Logische Sicherung** ([steps]-Name: LogicalBackup)

   Falls in Schritt 3 zuvor Anzeichen einer Verschlüsselung gefunden worden sind (außer EncryptionCheckDiskSectors) oder dieser Schritt durch die Konfigurationsdatei erzwungen wird, werden alle lesbaren Dateien zusätzlich logisch gesichert, d. h. kopiert. Damit wird sichergestellt, dass alle zum Zeitpunkt der Sicherung lesbaren Dateien auch bei der späteren Untersuchung unverschlüsselt vorliegen, selbst wenn der Quelldatenträger verschlüsselt ist oder die Dateien sich in einem verschlüsselten Container befinden oder eine ATA-Festplatte mit einem Passwortschutz versehen (zum Zeitpunkt der Sicherung aber freigeschaltet) ist. Bei der Sicherung werden, soweit möglich, die Dateinamen und Pfade im Ziel beibehalten. Unter Umständen müssen aber Änderungen an Pfad und/oder Name einer Datei vorgenommen werden, damit der Name und der Pfad der Datei auf allen unterstützten Dateisystemen erlaubt ist. Daher werden bei Bedarf Pfade und/oder Namen gekürzt, damit sie eine Länge von weniger als 256 Zeichen haben. Gekürzte Pfade werden in einem Unterverzeichnis „overlong“ des Ziels gesammelt. Unzulässige Zeichen in Dateinamen werden ersetzt. Wenn dadurch geänderte Dateinamen doppelt auftreten, wird eine fortlaufende Nummer direkt vor der Dateiendung eingefügt. Bei den Änderungen bleibt die Endung erhalten. Die Änderungen werden protokolliert.

   Vor dem Kopieren werden für jede Datei Datum und Uhrzeit des letzten Lesezugriffs gesichert und nach dem Kopieren wiederhergestellt, da diese beim Kopieren verloren gehen. Auf Linux-Dateisystemen und auf NTFS geht unvermeidlicherweise das ursprüngliche Datum der letzten Änderung der Inode bzw. des FILE-Records jeder einzelnen Datei (nicht das Datum der letzten Änderung der Datei selbst) verloren. Darauf wird im Protokoll einmalig hingewiesen. Aus diesem Grund sollte dieser Schritt erst nach der physischen Sicherung stattfinden.

   Unter Windows sind das Startlaufwerk und das Ziellaufwerk von X-Ways Capture von der logischen Sicherung ausgeschlossen, unter Linux alle Verzeichnisse unterhalb der Mountpoints des Start- und Zielverzeichnisses. Da je nach Quell- und Zieldateisystem ausgeschlossen ist, dass sämtliche Meta-Informationen über eine Datei auch in der Kopie erhalten werden können, werden Dateinamen, Größe, Datumsangaben, Attribute, Linux-Berechtigungen, Eigentümer und Gruppenname (jeweils sofern verfügbar) in einer separaten Dateiliste festgehalten. Die Dateiliste hat den Namen <*Präfix*>-files-<*fortlaufende Nummer*>.txt.Wenn überlange Pfade auftreten, werden die Originalpfade in einer Warnmeldung ausgegeben.

   Unter Windows durchsucht Capture alle NTFS-Laufwerke nach EFS-verschlüsselten Dateien und kopiert sie, unabhängig von den Resultaten vorhergegangener Suchschritte. Wurde keine Verschlüsselung gefunden, werden Verzeichnisse und Log-Dateien nur für EFS-verschlüsselte Dateien erzeugt, um die Pfade zu den EFS-Dateien zu erhalten. Im Falle von EFS-verschlüsselten Dateien kann die übliche Kopiermethode, die ADS erhält, nicht angewandt werden.

Auch hier kann der Parameter network verwendet werden, um zu bestimmen, ob Netzlaufwerke von der Sicherung betroffen sind. +network aktiviert die Sicherung von Netzlaufwerken, -network deaktiviert sie. –network ist wieder Standard

Aufbau der Konfigurationsdatei „capture.ini“

Die Konfigurationsdatei capture.ini kann wesentliche Aspekte von X-Ways Capture ändern. Dazu gehört die Reihenfolge der Verarbeitungschritte, auszuschließende Datenträger, Verzeichnisse, Sprache, zu suchende Schlüsselwörter, Namen bekannter Verschlüsselungssoftware und vieles mehr. Die Datei ist eine reine ASCII-Datei und kann daher leicht mit einem geeigneten Texteditor an die eigenen Bedürfnisse angepasst werden. Die Konfigurationsdatei für Linux enthält Linux-Zeilenendezeichen, die Konfigurationsdatei für Windows enthält Windows-Zeilenendezeichen. Sie besteht aus einzelnen Abschnitten, deren Namen jeweils in eckigen Klammern stehen, wie z. B. [steps]. Die Reihenfolge der Abschnitte ist beliebig. Jede Zeile kann durch ein vorangestelltes „#“ als Kommentar gekennzeichnet bzw. unwirksam gemacht werden. Die Bedeutung der einzelnen Abschnitte wird im folgenden erklärt.

Der Abschnitt [steps] regelt die Reihenfolge der Arbeitsschritte. Ein Beispiel für einen solchen Abschnitt ist:

AppendIni
DumpPhysicalMemory
DumpProcessMemory
DumpProcessList
ATACheck
HPACheck
EncryptionCheckProcessList
+EncryptionCheckProcessMemory
+EncryptionCheckDiskSectors
#EncryptionCheckAllFiles
PhysicalImaging
LogicalImaging
+LogicalBackup

Die Bedeutung der einzelnen Schritte wird im Kapitel „Funktionsweise“ erklärt. Durch ein vorangestelltes Minuszeichen (-) kann die Ausführung eines Schrittes unterdrückt werden; ein vorangestelltes Pluszeichen (+) *erzwingt* die Ausführung des entsprechenden Schrittes. „+“ kann insbesondere verwendet werden, um eine logische Sicherung aller Dateien zu erzwingen, auch wenn X-Ways Capture keine Anzeichen für Verschlüsselung gefunden hat, oder um weitere Tests auf Verschlüsselung zu prüfen, auch wenn ein solches Programm bereits gefunden wurde.

Der Abschnitt [ListProcessesCommand] führt für Linux das Kommando auf, mit dessen Hilfe die Liste der laufenden Prozesse angezeigt wird. In der Voreinstellung ist dies „ps -A“.

Die Abschnitte [SearchFileForEncryption] stehen nur unter Linux zur Verfügung. Die jeweils erste Zeile in einem solchen Abschnitt definiert die zu durchsuchende Datei, alle weiteren Zeilen geben die Suchbegriffe für diese Datei an. Da es mehrere Abschnitte dieses Typs geben darf, können verschiedene Dateien durchsucht werden. In der Voreinstellung wird „/proc/mounts“ durchsucht

nach „/dev/loop“, und „/proc/modules“ wird durchsucht nach Begriffen wir „aes“, „blowfish“, „twofish“ usw.

Der Abschnitt [SearchProcessListForEncryption] enthält Prozeßnamen bekannter Verschlüsselungsprogramme, die in der Prozeßliste gesucht werden. Wird ein Prozeß gefunden, der in diesem Abschnitt aufgeführt ist, wird das als Hinweis auf eine aktive Verschlüsselung gewertet.

[SearchProcessMemoryForEncryption] enthält Schlüsselwörter, nach denen unter Windows in geladenen .exe-Dateien gesucht wird.

[ExcludeDevicesFromPhysicalImaging] gibt die Bezeichnung der Datenträger an, die von der physischen Sicherung ausgeschlossen werden sollen. Unter Linux muss die /dev/-Bezeichnung, ohne /dev/, eingetragen werden, z. B. hdb für /dev/hdb. Für Windows werden die Hersteller-Modellbezeichnungen der auszuschließenden Datenträger aufgelistet, z. B. „SAMSUNG SP1614C“. Der Zieldatenträger ist automatisch ausgeschlossen. Die unter Windows anzugebende Modellbezeichnung von Festplatten kann man z. B. vorher in WinHex oder X-Ways Forensics ermitteln.

[ExcludeFromLogicalBackup] gibt die Verzeichnisse, Laufwerke oder Medien an, die von der logischen Sicherung auszuschließen sind. Hier angegebene Pfade müssen absolut sein, d. h. unter Windows mit einem Laufwerksbuchstaben beginnen und unter Linux mit /. Alle Dateien und Verzeichnisse, die mit einem der hier angegebenen Teilpfade beginnen, werden von der Sicherung ausgeschlossen. Daher schließt bspw. c:\win auch c:\windows aus. Unter Linux wird in der Voreinstellung z. B. das Geräteverzeichnis „/dev“ ausgeschlossen. Unter Linux wird anhand des angegebenen Ausgabepfades der Zieldatenträger und die Startpartition von Capture automatisch von der logischen und physischen Sicherung ausgeschlossen.

[LinuxExcludeFS] listet die Dateisysteme auf, die unter Linux von der Sicherung ausgeschlossen sind. Die Standardkonfiguration listet optische und Netzlaufwerke auf.

Für diverse Einstellungen dient der Abschnitt [settings], der z. B. wie folgt aussehen kann:

```
[settings]
#language=English
language=German
PromptForOutputPath
#UserShouldAcknowledge
#DateFormat=dd/mm/yyyy
DateFormat=dd.mm.yyyy
LogInfoMsgs
LogHints
LogWarnings
LogErrors
LogResults
PrintInfoMsgs
PrintHints
PrintWarnings
PrintErrors
PrintResults
ImageSegmentSize=2000
#PhysicalImageFormat=raw
```

#PhysicalImageFormat=e01-compressed
PhysicalImageFormat=e01-uncompressed
#PhysicalImageCalcHash=md5
#PhysicalImageCalcHash=sha-1
#PhysicalImageCalcHash=sha-256
#PhysicalImageCalcHash=none

„ImageSegmentSize“ gibt die gewünschte Größe der Segmente für die physische Sicherung an. Wenn diese Einstellung auskommentiert wird, werden .e01-Evidence-Files auf etwa 2 GB begrenzt, während die Größe von Roh-Images nur durch das darunterliegende Dateisystem begrenzt wird. „PhysicalImageFormat“ bestimmt das Format eines so erzeugten Images: „raw“ erzeugt eine Roh-Image-Datei, „e01-compressed“ erzeugt ein komprimiertes Evidence-File, „e01-uncompressed“ ein unkomprimiertes. Die Einstellung kann über Kommentarzeichen (#) einfach ausgetauscht werden. „PhysicalImageCalcHash“ gibt den bei der physischen Sicherung zu berechnenden Hash an („md5“, „sha-1“, „sha-256“ oder „none“ = keinen). Bitte beachten Sie, dass die Hash-Berechnung merklich Zeit kosten kann, insbes. unter Linux. „Language“ schaltet zwischen deutscher und englischer Sprache um. „FileSplitSize“ wird bei der logischen Sicherung unter Linux verwendet: Dateien, die größer als das darin angegebene Limit sind, werden aufgeteilt (gesplittet).

Die Einstellungen LogInfoMsgs, LogHints, LogWarnings, LogErrors, LogResults, PrintInfoMsgs, PrintHints, PrintWarnings, PrintErrors, PrintResults steuern, ob und wie Nachrichten ausgegeben werden. Alle Nachrichten in Capture gehören einer der Kategorien Info, Hinweis, Warnung, Fehler, oder Resultat an. Diese Einstellungen steuern, ob die Nachrichten ins Protokoll geschrieben werden oder auf dem Bildschirm erscheinen (Print).

„UserShouldAcknowledge“ steuert, ob der Benutzer folgende Funde durch Drücken der Enter-Taste bestätigen muss: Wenn Capture auf einem Laufwerk ATA-Paßwortschutz findet, wenn eine HPA gefunden wird, wenn ein unter [SearchProcessListForEncryption] gelisteter Prozeß gefunden wird, wenn ein Prozeß einen unter [SearchProcessMemory] gelisteten Suchbegriff enthält, wenn ein verschlüsselter Sektor gefunden wird (Windows), wenn eine EFS-verschlüsselte Datei gefunden wird oder wenn in einer Datei ein unter [SearchFileForEncryption] gelisteter Begriff gefunden wird.

Mit Hilfe der Option „PromptForOutputPath“ kann die Frage nach dem Zielpfad verhindert werden. Dann verwendet X-Ways Capture unter Windows das Stammverzeichnis der Partition zur Sicherung, von der aus es gestartet wurde. Unter Linux wird der Mountpoint verwendet, der zum Pfad gehört, aus dem Capture gestartet wurde. Ohne diese Option muss bei Programmstart der Zielpfad eingegeben werden, wenn dieser nicht als Parameter von der Kommandozeile übergeben wurde.

Tipps & Hinweise

Unter Linux kann eine FAT-Partition zur Sicherung eines Systems verwendet werden, wenn das entsprechende Kernel-Modul geladen wurde. Unter Windows bietet sich eher NTFS an, damit auch alternative Datenströme bei der logischen Sicherung nicht verloren gehen.

Um herauszufinden, welchen Pfad man unter Linux als Sicherungspfad angeben muss, helfen vielleicht folgende Hinweise. Unter Linux werden Medien häufig automatisch in den Verzeichnisbaum eingebunden, meist unter /mnt/ oder /media/. Man kann sich mit „mount“ eine Liste der eingebundenen Dateisysteme anzeigen lassen. U. U. hilft auch die Ausgabe von „df“ weiter. Wurde

der Datenträger vorab mit einer Datei owner.txt präpariert, die z. B. die Adresse des Inhabers enthält, kann man ganz sicher gehen, dass es sich um den eigenen Datenträger handelt.

Es darf immer nur ein Sicherungsdatenträger gleichzeitig an das System angeschlossen sein. Da capture.ini nur bei Programmstart gelesen wird, bleiben Änderungen während der Ausführung unberücksichtigt.

Die Ausführung des Programms kann jederzeit durch Drücken von Strg+C abgebrochen werden.

Wichtig: Natürlich darf X-Ways Capture nicht auf einen der zum laufenden System gehörigen Originaldatenträger kopiert und dort ausgeführt werden. X-Ways Capture sollte von einer mitgebrachten CD oder sonstigem externen Datenträger gestartet werden. Dies kann auch gleichzeitig der Sicherungsdatenträger sein.