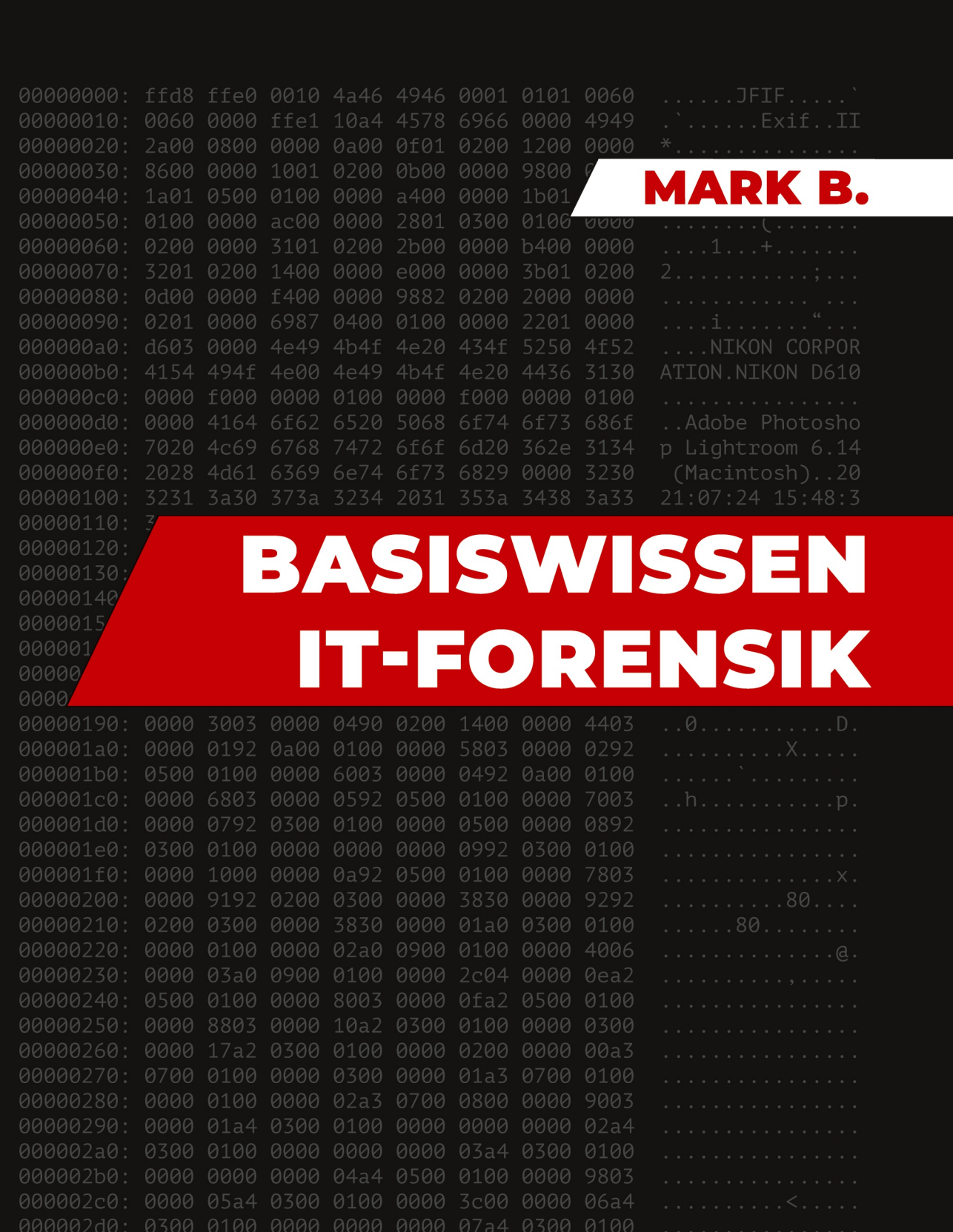

MARK B.
BASISWISSEN
IT-FORENSIK

MARK B.

BASISWISSEN IT-FORENSIK

EINFACH ERKLÄRT

IMPRESSUM

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

© 2020-2022 Mark B.

Herstellung und Verlag:
BoD – Books on Demand, Norderstedt

ISBN:
978-3-7562-7015-6

INHALTSVERZEICHNIS

VORWORT

IT-Forensik ist ein sehr spannendes und immer wichtiger werdendes Betätigungsfeld. Die Anzahl der Geräte, auf denen sich Daten befinden, wächst stetig und heute tragen wir Datenspeicher in der Hand- oder Hosentasche und am Handgelenk außerdem haben wir Dutzende weitere Datenspeicher am Arbeitsplatz und zu Hause.

Es gibt kaum noch Ermittlungen im strafrechtlichen und im gewerblichen Umfeld, an dem keine IT-Forensiker beteiligt sind. Daher ist dieses Arbeitsfeld auch eine gute Karrieremöglichkeit.

Ich will Ihnen mit diesem Buch einen Überblick über die einzelnen Teilbereiche und Techniken geben und Ihnen auch gleichzeitig die nötigsten Grundlagen vermitteln, um die ersten Schritte erfolgreich zu meistern.

Wenn Sie Fragen, Anregungen oder Kritik loswerden wollen, schreiben Sie mir bitte an: mark.b@seznam.cz

In diesem Sinne wünsche ich Ihnen viel Spaß beim Lesen, Lernen und Experimentieren,

Ihr

WAS IST IT-FORENSIK

In der IT-Forensik geht es darum, durch Ermittlungs- und Analysetechniken Beweise auf einem bestimmten IT-System so zu erfassen und zu sichern, dass sie bei einer Gerichtsverhandlung verwertbar sind.

Das Ziel dieses auch als Computer- oder digitale Forensik bezeichneten Fachgebiets besteht darin, eine strukturierte Untersuchung durchzuführen und diese zu dokumentieren, damit sich genau feststellen lässt, welche Vorgänge auf einem IT-System stattgefunden haben und wer dafür verantwortlich war.

Die Welt wird immer vernetzter und Computer oder mobile Endgeräte sind wie selbstverständlich in unseren Alltag integriert. Daher werden diese Geräte auch für Straftaten verwendet. Hierbei kann eine Tat direkt mit dem Computer begangen werden (*zB Hackerangriffe oder Warenbetrug*) oder nur durch den Einsatz von IT-Geräten unterstützt werden (*zB eine Lösegeldforderung per E-Mail*).

Dabei kommt die IT-Forensik in vielen Bereichen vom privaten Sektor über Behörden bis hin zu Militär, Geheimdiensten und Strafverfolgungsbehörden zum Einsatz.

Auch wenn der Begriff Computer-Forensik nach wie vor gebräuchlich ist, impliziert dieser aber einen wesentlich kleineren Bereich, der heutzutage nicht mehr wirklich stimmt. Wir haben es in der IT-Forensik mit allen möglichen Geräten von IoT-Geräten über Telefone, Tablets, Laptops und Standcomputer bis zu digitalen Kameras, Speichermedien, Netzwerkgeräten, Navigationssystemen, uvm. zu tun.

Nicht jede forensische Untersuchung endet zwangsläufig vor Gericht, aber dennoch muss man als IT-Forensiker immer davon ausgehen, dass dies passieren wird. Da dann eine forensische Untersuchung immer von der Gegenseite infrage gestellt werden wird, muss die Auswahl der Methoden und Tools sowie das Vorgehen bei der Beweissicherung und Untersuchung, die Dokumentation und Analyse den Standards des Gerichts genügen.

Das gilt vor allem für die forensisch korrekte Vorgehensweise bei der Beweissicherung und die lückenlose Dokumentation der Beweismittelkette und der einzelnen Untersuchungsschritte.

Eine der größten Herausforderungen in der IT-Forensik ist die Tatsache, dass Gesetzgeber und Gerichte nicht wirklich mit den rasanten Entwicklungen in der IT-Welt mithalten können. Erschwerend kommt hinzu, dass Straftaten im

Internet oft grenzüberschreitend stattfinden, was es für die Strafverfolgungsbehörden oftmals deutlich erschwert.

Dabei sind die wichtigsten Aufgaben:

1. Das Finden von Beweisen auf IT-Geräten
2. Das Sichern und Bewahren von digitalen Beweisen
3. Das Zuordnen von Handlungen und Vorgängen zu einem Verursacher
4. Datenlecks identifizieren
5. Das Klären von Schäden die durch ein Datenleck oder einen Angriff entstanden sind
6. Das Erstellen eines Untersuchungsberichts
7. Eine Zeugenaussage vor Gericht und/oder das Briefing für eine Zeugenvernehmung

Dabei kann man IT-Forensik nach der Art der untersuchten Geräte einteilen:

- Computer-Forensik
- Mobile-Forensik
- Netzwerk-Forensik
- usw.

Im größeren Zusammenhang ist die IT-Forensik ein Teil des Incident Response Prozess Models. Oft sind IT-Forensiker auch Teil eines CSIRT (*Computer Security Incident Response Team*). Zumindest muss es im CSIRT forensisch geschulte Mitglieder geben, die eine korrekte Beweissicherung durchführen können.

Die generelle Vorgehensweise bei einer Untersuchung ist im ISO Standard `ISO/IEC 27037:2012` (`https://www.iso.org/standard/44381.html`) festgehalten. Ihr Vorgehen sollte zumindest diesem Standard entsprechen.

Cyberkriminalität

Dies sind Verbrechen, die mit IT-Geräten und/oder in Netzwerken wie dem Internet begangen werden. Hierbei gibt es einige Unterscheidungen, nach denen man diese Verbrechen klassifizieren kann.

Nach der Herkunft:

- Insider Angriffe, die meistens gefährlicher sind, da aktuelle und ehemalige Mitarbeiter oft genau wissen wo die Schwachstellen liegen oder welche Datenlecks den maximalen Schaden verursachen.
- Angriffe von Fremden, die aus Eigennutz, Geltungssucht oder im Auftrag eines Dritten durchgeführt werden.

Nach der Art der Beteiligung des IT-Gerätes:

- Das Gerät ist das Ziel eines Angriffs (*zB unautorisierter Zugriff*)
- Das Gerät wurde für den Angriff eingesetzt (*zB DoS-Angriff*)
- Das Gerät wurde unterstützend eingesetzt (*zB: Telefonat mit Komplizen*)

Nach der Art des Verbrechens:

- Verbreitung von Schadware (*auch Malware genannt*)
- Ransomware und andere Erpressungsversuche wie Scaremails
- Hackingangriffe (*zB SQL-Injection, Session Hijacking, etc.*)
- Phishing und Pharming
- Identitätsdiebstahl
- Spamversand
- Verkauf illegaler Dienste und Waren (*zB im Darknet oder Deepweb*)
- DoS- und DDoS-Angriffe
- Social Engineering
- Illegale Verbreitung urheberrechtlich geschützter Werke (*Musik, Filme, ...*)
- Cybermobbing
- etc.

Cyberkriminelle werden immer besser darin Angriffe zu verschleiern und auch Schadware wird immer fortschrittlicher und komplexer. Oftmals forscht man den vermeintlichen Urheber eines Angriffs aus, nur um dann bei der Untersuchung der sichergestellten Beweise zu merken, dass der vermeintliche Täter selbst ein Opfer ist, dessen Computer fremdgesteuert wurde.

ABLAUF EINER FORENSISCHEN UNTERSUCHUNG

Bei einer forensischen Untersuchung durchlaufen wir in der genannten Reihenfolge sechs Schritte. Hierbei gibt es keine Abkürzungen und in der Regel sollten die Schritte auch in der genannten Abfolge ausgeführt werden.

Es kann in bestimmten Situationen durchaus vorkommen, dass man von der genannten Reihenfolge abweicht oder Schritte überspringt - dies sollte man im Zweifelsfall aber hinreichend und logisch vor Gericht begründen können.

1. Identifikation

Hierbei müssen wir bedenken, dass wenn sich in der realen Welt zwei Objekte berühren, dann hinterlassen diese am jeweils anderen Spuren - das nennt man das Locard'sche Prinzip. Das gleiche gilt auch für die digitale Welt!

Hier haben wir allerdings das Problem, dass es im digitalen Umfeld oftmals einfacher ist diese Spuren zu verschleiern oder zu fälschen. Darum sollten wir bei der digitalen Forensik auch jede Aussage durch mindestens zwei unabhängige Spuren und/oder Tools bestätigen lassen.

2. Sicherstellen von Medien

Beim Sicherstellen muss verhindert werden, dass eine Manipulation vorgenommen wird. Dies können Snapshots von virtuellen Maschinen sein oder das physische Bewachen von Systemen bis zum Eintreffen einer forensisch ausgebildeten Person für die Beweissicherung.

Außerdem muss sichergestellt werden, dass die Geräte vom Netzwerk bzw. dem Internet getrennt werden. Ein Komplize könnte über das Internet zB Beweise von einem Mobiltelefon oder Tablet löschen. Dazu muss das Gerät aber den entsprechenden Befehl bekommen und dazu muss es mit dem Internet verbunden sein. Genau darum müssen wir die Internetverbindung trennen!

3. Sicherung der Spuren

Hier muss einerseits der Zustand dokumentiert werden (*zB waren die Geräte eingeschalten, mit dem Internet verbunden, ...*) und auch der Vorgang der Beweissicherung (*eingesetzte Programme, Geräte, etc.*) und das Handling (*zB wurde ein PC heruntergefahren oder einfach der Stecker gezogen, wurden Telefone in Faraday-Beutel verpackt, etc.*).

Computer enthalten volatile und nicht volatile Daten. Der volatile RAM-Speicher geht verloren, sobald ein PC abgeschaltet wird. Durch die Dokumentation des Zustandes der Geräte beim Eintreffen lässt sich im Nachhinein eindeutig nachweisen, dass zB eine Sicherung des RAM-Speichers nicht möglich war.

Der RAM-Speicher kann wichtige Beweise enthalten und sollte, falls möglich, gesichert werden.

Beim Herunterfahren eines Rechners werden einige Aufräumvorgänge durchgeführt, die Beweise vernichten könnten - daher ist es besser, den Stecker zu ziehen bzw. den Akku zu entfernen. Dinge wie ARP-Cache, Routing-Tabellen oder temporäre Dateien können wichtige Beweise enthalten.

Außerdem muss bei der Sicherung der Daten dafür gesorgt werden, dass eventuelle nachträgliche Manipulation nicht möglich ist.

Bedenken Sie hierbei, dass manche der Vorgänge wie zB das Erstellen eines RAM-Dumps selber Spuren hinterlassen - so wird das entsprechende Programm selber einen Fußabdruck im Speicher hinterlassen.

Der Vorgang muss also klar und nachvollziehbar sein - nicht nur für Sie, sondern auch für einen IT-Forensiker der Gegenseite, der Ihre Ergebnisse überprüft.

Andere Einflussnahme auf die Beweise muss verhindert werden - so kann das Anschließen einer Platte an einen Rechner dazu führen, dass das Betriebssystem diese einbindet und Zeitstempel, Thumbnail-Cache und manches andere verändert. Daher muss so etwas mit einem Writeblocker verhindert werden.

Ein solcher Hardware-Writeblocker sorgt dafür, dass keinerlei Schreibvorgänge mehr an den Datenträger gesendet werden. Die Geräte gibt es mit allen möglichen Anschlüssen von IDE über SATA und SAS bis zu USB.

Wie Sie sehen, gibt es bereits bei der Spurensicherung viele Möglichkeiten, einen Fall zu ruinieren, bevor wir überhaupt mit der Untersuchung begonnen haben. Daher muss diese auch von entsprechend geschultem Personal durchgeführt und im Idealfall mit Fotos dokumentiert werden.

Ein wichtiger Teil der Dokumentation ist die schriftliche Aufzeichnung der Beweismittelkette. Hier muss vermerkt werden wie Beweise gefunden, gesichert, transportiert, analysiert, gelagert und ausgewertet werden. Außerdem wird hierauf auch vermerkt wer die genannten Arbeiten, wann durchgeführt hat.

Ohne die ordentliche Dokumentation der Beweismittelkette sind die gewonnenen Informationen nicht verwertbar.
Die entsprechende schriftliche Dokumentation muss also folgende Fragen beantworten können:

- Was sind die Beweise?
- Wo wurden diese gefunden?
- Wie war der Zustand der Geräte zum Zeitpunkt der Beweissicherung? (*ein- oder ausgeschaltet, mit dem Internet verbunden, war ein User eingeloggt oder war das System mit einem Passwort vor Zugriff geschützt, usw.*)
- Wie wurden die Beweise gesichert und transportiert?
- Wie wurden die Beweise untersucht? (*Programme, Programmversionen, Techniken, etc.*)
- Wann hatten welche Personen Zugang zu den Beweisen und aus welchem Grund?
- Wie wurden die Beweise im weiteren Verlauf der Untersuchung benutzt?

4. Untersuchung

In der digitalen Forensik arbeiten wir nicht auf den originalen Beweisen. Wir erstellen eine Kopie, dann eine Kopie der Kopie als Backup und dann untersuchen wir die Kopie.

Es sollte jederzeit eine Kopie der ursprünglichen Originaldaten vorgehalten werden für den Fall, dass Daten bei der Untersuchung oder Analyse versehentlich konterminiert werden. Außerdem müssen wir davon ausgehen, dass ein erneutes Sichern der Beweise nicht mehr möglich ist.

RAM-Speicher geht verloren, Festplatten können beschädigt werden oder geflippte Bits aufweisen und sind dann nicht mehr verifizierbar.

Bedenken Sie, dass magnetische Ladungen in Festplatten genau wie elektrische Ladungen in Flash-Speichern mit der Zeit verblassen. In der IT-Forensik

haben wir oft mit den Mühlen des Gesetzes zu tun und diese mahlen bekanntlich langsam.

Also müssen wir bedenken, dass Beweise auch noch in einigen Jahren für eine erneute Überprüfung verifizierbar sein müssen.

Die Verifizierung ist in der Regel das erneute Berechnen eines Hash-Wertes und das Vergleichen mit dem Ergebnis der gleichen Berechnung, die bei der Beweissicherung auf den Originaldaten durchgeführt wurde.

Ändert sich nur ein einziges Bit in den Daten, dann resultiert dies in einer Änderung des errechneten Hashs und die Beweise sind nicht mehr vertrauenswürdig. Vor allem SSDs verblassen je nach verwendetem Speichertyp relativ schnell, jedenfalls viel schneller als magnetische Festplatten.

Daher sollte auch immer ein zusätzliches Backup der geklonten Datenträger existieren, falls wir aus Versehen an einer Kopie etwas verändern. Außerdem trennen wir in diesem Schritt Beweise von irrelevanten Daten.

5. Analyse

Bei der Analyse arbeiten wir die Beweise durch auf der Suche nach neuen Informationen oder Beweisen, die Annahmen stützen. Hierbei versuchen wir bei jedem Durchgang immer nur eine Frage zu beantworten, um uns auf diese vollumfänglich zu konzentrieren.

Wir versuchen, mit Gegenproben alle gefundenen Daten zu verifizieren. Gleiches gilt für automatische Filter die Forensik-Software anbieten. Eine permanente Eigenkontrolle und Kontrolle der verwendeten Tools sorgt für entsprechende Sicherheit, wenn wir die Resultate vor Gericht oder vor einem Auftraggeber
präsentieren.

6. Präsentation

Spätestens zu Beginn dieser Phase werden das Ergebnis der Untersuchung und die gefundenen Antworten auf die Fragen der Auftraggeber verschriftlicht. Voreingenommenheit oder die eigene Meinung haben in diesem Bericht aber nichts zu suchen!

Ein solcher Bericht muss klar strukturiert und auch für Laien verständlich formuliert sein und trotzdem alle wichtigen technischen Details enthalten damit ein anderer IT-Forensiker die Arbeitsschritte die zu den Ergebnissen führten und die Ergebnisse selber nachvollziehen kann.

Außerdem ist diese auch für uns selbst wichtig. Wenn wir uns in eine Sackgasse verrannt haben, müssen wir in der Lage sein unsere Schritte zurückzuverfolgen um dann herauszufinden, wo unser Fehler lag.

Daher beginnt das Erstellen des Reports nicht erst am Ende der Untersuchung, sondern bereits bei der Beweissicherung, Untersuchung und Analyse müssen wir entsprechende Notizen anfertigen, um später beim Schreiben des Berichts keine Details zu vergessen. Noch besser wäre es, den Bericht direkt parallel mit der Untersuchung zu erstellen und jede ausgeführte Aktion und jeden Fund sofort im Bericht zu ergänzen.

Oftmals kommt es dann vor, dass wie die Ergebnisse dann auch vor Gericht präsentieren müssen und dort als Zeuge oder Sachverständiger auftreten.

DAS FORENSISCHE LABOR

Im Idealfall ist ein forensisches Labor ein eigens abgesperrter und abgeschlossener Bereich. Sie brauchen auch die entsprechende Privatsphäre, um Beweise zu sichten und zu extrahieren.

Zumindest muss der Zugang aber auf ausgesuchte Personen beschränkt werden. Keine Person sollte sich im Labor ohne Grund aufhalten dürfen.

Dazu kann man beispielsweise ein Zugangskontrollsystem, Monitoring, Alarmanlagen, etc. verwenden.

Wenn nicht an den Beweismitteln gearbeitet wird, haben diese sicher versperrt gelagert zu werden. Dazu muss es einen Tresor oder zumindest einen versperrbaren Schrank geben, zu dem nur diejenigen einen Schlüssel haben, die auch eine Untersuchung durchführen.

Zu der Mindestausstattung gehören meiner Meinung nach Faraday-Beutel, die Tablets, Laptops und Mobiltelefone vom Mobilfunknetz abschneiden und Hardware-Writeblocker. Diese relativ günstigen Geräte gibt es zB von den Firmen `CRU` bzw. `WiebeTech`, `Tableau`, `Epos`, `DeepSpar`, usw. Hier kann man mit einem USB-Writeblocker beginnen denn so gut wie alle Speichermedien kann man auf USB adaptieren. Im Idealfall hat das Labor Writeblocker für die verschiedenen Anschlüsse.

Als Computer würde ich einen PC mit ausreichend Speicher, schnellem Mehrkernprozessor (*mindestens 8 Kerne*) und mindestens 32GB RAM empfehlen. Für das knacken von Passwörtern sollte die Forensik-Workstation auch noch über eine gute Grafikkarte verfügen. Hierbei haben Mittelklasse Gaming-Grafikkarten das beste Preis-/Leistungsverhältnis.

Aus Sicherheitsgründen sollte die Forensik-Workstation nicht mit dem Firmennetzwerk oder Internet verbunden sein währen deiner Untersuchung. Einerseits kann ein Windows-Update einen laufenden Prozess wie das Knacken eines Passwortes oder das Klonen eines Datenträgers abbrechen und andererseits wollen Sie auch nicht riskieren, dass Sie Schadware in ihr Firmennetzwerk entlassen oder das diese eine Backdoor öffnen kann und so eine Untersuchung kompromittiert.

Aus dem gleichen Grund sollten auch keine forensischen Berichte auf der Workstation geschrieben werden.

Große Labore, die viele Datenträger Klonen, haben meist auch einen eigenständigen forensischen Imager wie zB von CRU, Tableau, Atola, JogiCube, ZXi-Forensic und einigen anderen.

Im Gegensatz zu günstigen HDD Docks mit Klone-Funktion, die man ab 40 EUR finden kann, garantieren diese Produkte korrektes forensisches Klonen. Für den Aufpreis von mindestens 1.500 EUR erkauft man sich meiner Meinung nach nur die entsprechende Anerkennung aber die IT-Forensik ist kein Feld, in dem man mit ungetesteten Tools experimentiert.

Wenn Sie nicht Dutzende Platten pro Woche klonen müssen, dann benötigen Sie auch keinen forensischen Duplikator. Verwenden Sie einfach einen Writeblocker und das kostenlose Tool FTK Imager mit dem wir in einem der nächsten Kapitel arbeiten werden. Bringen Sie aber keinesfalls die ganze Untersuchung in Gefahr, indem Sie irgendwelche alternativen und nicht erprobten Tools, Programme, etc. verwenden!

Ein weiteres sehr günstiges, aber auch sehr praktisches Produkt ist ein Mouse-Jiggler. Dieses kleine USB-Gimmick gibt sich als Computermaus aus und bewegt den Cursor alle paar Sekunden damit der PC nicht in den Schlafmodus geht.

Die gängigsten Programme für IT-Forensiker sind EnCase, FTK, OSForensics, Oxygen Forensics, Autopsy, Belkasoft und X-Ways Forensics. Wir werden in diesem Buch mit OSForensics arbeiten, da dieses Tool relativ günstig ist und für die gelegentliche Nutzung sogar eine Monatslizenz anbietet.

Im Bereich der Mobile-Forensik haben wir Cellebrite, MASB XRY, Oxygen Forensics und MobilEdit. Wobei ich hier für eine gelegentliche Nutzung MobilEdit empfehlen kann, dass eine Single-Phone Lizenz hat.

Es gibt aber auch einige kostenlose Linux-Distributionen die für IT-Forensik zusammengestellt wurden. Hier wären DEFT, CAINE, SANS SIFT und als spezielles System zur Malwareanalyse auch REMnux zu nennen.

BEWEISSICHERUNG IM NETZWERK

In einem kompromittierten Netzwerk ist das Netzwerk selbst ein guter Ausgangspunkt für eine Untersuchung, vor allem wenn nicht klar ist, welche der Systeme kompromittiert sind, lässt die Kommunikation im Netzwerk darauf schließen, welche Systeme man sich näher ansehen sollte.

Aber nicht nur der Netzwerkverkehr an sich, sondern auch diverse Logdateien von Routern, Firewalls, IDS/IPS-Systemen, etc. liefern wertvolle Hinweise. Daher müssen diese ebenfalls gesichert und ausgewertet werden!

In bestimmten Fällen sind wir aber rechtlich dazu verpflichtet, Mitarbeiter davon in Kenntnis zu setzen, dass Ihre Aktivitäten überwacht werden, um rechtlichen Schwierigkeiten vorzubeugen falls sich auch private Daten in den aufgezeichneten Datenverkehr befinden. Wann dies verlangt ist, müssen Sie mit dem Auftraggeber bzw. deren Rechtsvertretern klären.

Als IT-Forensiker sind wir keine Rechtsexperten und sollten uns im Zweifelsfall Rückversichern und sei es nur, um der eigenen Sorgfaltspflicht Genüge zu tun.

Im Idealfall haben wir bei einer derartigen Untersuchung ein Netzwerkdiagramm zur Verfügung um Router, Gateways, Subnets und wie diese zusammenhängen schnell und einfach zu überblicken. Leider ist die Welt nicht immer perfekt und nicht in jeder Situation sind wir willkommen und können auf die Mitarbeit oder Informationen der Personen vor Ort bauen.

Selbst wenn sind diese oftmals falsch oder unvollständig. Daher muss jede Information überprüft werden. Gleiches gilt für Netzwerkgeräte - diesen sollten Sie auch nicht zu 100% vertrauen da Beweise manipuliert oder die Konfiguration mittlerweile verändert sein könnte.

Allein dies zu erkennen kann für sich allein schon eine ziemliche Herausforderung sein. Daher ist das Zusammenführen von Informationen aus verschiedensten Quellen so wichtig. Nur wenn alle Informationen sich gegenseitig verifizieren und ein stimmiges Bild ergeben ist mit großer Wahrscheinlichkeit davon auszugehen, dass diese korrekt sind.

Aber logging bringt auch wieder rechtliche Probleme mit sich und ist darum oftmals nicht so ausführlich, wie man sich das als IT-Forensiker wünschen würde.

Unterschiedliche Logformate von unterschiedlichen Geräten machen eine Analyse der Logs auch oftmals aufwendiger als nötig.

Ein SIEM (*Security Information Management System*) wäre die Lösung für solche Probleme. Dies führt Logs aus den unterschiedlichen Quellen zusammen und speichert diese an einem zentralen Ort in einem einheitlichen Format. Allerdings sind diese Systeme kosten- und zeitintensiv bei der Anschaffung, Einrichtung und im Betrieb. Daher sind diese oft nicht vorhanden.

Ein Opensource Projekt namens `Security Onion` will diese Lücken ausfüllen. Dieses System stellt eine Linux-Distribution mit verschiedensten Opensource-Tools dar und ist auch nicht wirklich trivial zu implementieren.

Es gibt eine ganze Reihe von Tools um Netzwerkverkehr abzufangen und zu analysieren, aber bevor wir uns die Tools ansehen, will ich Sie noch auf eine Limitierung hinweisen. Ist der Netzwerkverkehr verschlüsselt, dann können wir zwar feststellen, welche Systeme miteinander kommunizieren aber nicht was da an Daten übertragen wird.

Grundsätzlich kann man das Aufzeichnen des Netzwerkverkehrs auf drei mögliche Arten realisieren:

- Spezielle Geräte, die zwischen den Rechner und das Netzwerk gesetzt werden wie zB ein PacketSquirrel von Hak5.
- Mit Port-Mirroring / SPANs (*Switch Port Ananlyzer*), die auf vielen gemanagten Switchen über das Managementinterface aktiviert werden können
- Mit Software, die dann auf dem Gateway für das Netzwerksegment oder dem Client, den wir untersuchen wollen, läuft.

Als Softwarelösungen wären folgende Tools zu nennen:

- TCPdump
- WinPcap
- Wireshark

Hier ist die Dokumentation besonders wichtig sowie das Hashing der Daten, um später bei der Analyse eine Manipulation auszuschließen.

BEWEISSICHERUNG VON COMPUTERSYSTEMEN

Beachten Sie, dass Tools zur Sicherung von Beweisen in der Regel Admin-Rechte benötigen, um die Daten zu sichern.

Wie bereits erwähnt müssen wir beim Eintreffen zuerst den Zustand der Geräte feststellen und schriftlich dokumentieren und dann entscheiden welche Schritte wir vornehmen.

Ist das System in Betrieb, dann sollten wir zur Sicherheit die volatilen Daten aus dem RAM-Speicher sichern auch wenn wir im Moment noch nicht sicher wissen, ob wir diese brauchen, haben wir nach dem ausschalten keine Chance mehr diese Daten zu sichern. So können wir auch vorbeugen, dass ein Sachverständiger der Gegenseite in den Raum stellt, dass wir eventuelle Beweise im RAM nicht gesichert haben.

Danach würde ich im Regelfall den Stecker ziehen oder den Akku entfernen, um das System abzuschalten. So vermeide ich, dass ein ordnungsgemäßes Herunterfahren Cleanup-Routinen ausführt und damit Beweise vernichtet.

Das Klonen der Datenträger mache ich in der Regel nicht am laufenden System. Ich entnehme die Datenträger, schließe diese an einem Writeblocker an und Klone sie auf einem meiner Systeme. Dafür brauchen wir keine besonders große Systemleistung und daher verwende ich für diese Aufgabe ein paar alte Laptops, auf denen Windows und `FTK Imager` laufen.

Damit das Klonen nicht ewig dauert, sollten die Laptops zumindest zwei USB 3.x Ports haben (*einen für das Quell- und einen für das Zielmedium*).

Aber nicht in allen Fällen können wir ein System offline nehmen - wenn es sich um ein wichtiges System handelt, dass nicht heruntergefahren werden darf, bleibt uns nichts anderes übrig als die Daten im laufenden Betrieb zu sichern.

Ein weiteres Szenario ist die partielle Extraktion von Daten, die zB bei Cloud-Diensten angewandt wird. Hier werden zB nur die Daten eines Useraccounts gesichert und nicht das ganze System.

Es gibt sogar die Möglichkeit, eine Remote-Beweissicherung durchzuführen. Ein relativ einfaches System, das das anbietet, wäre `Belkasoft R`.

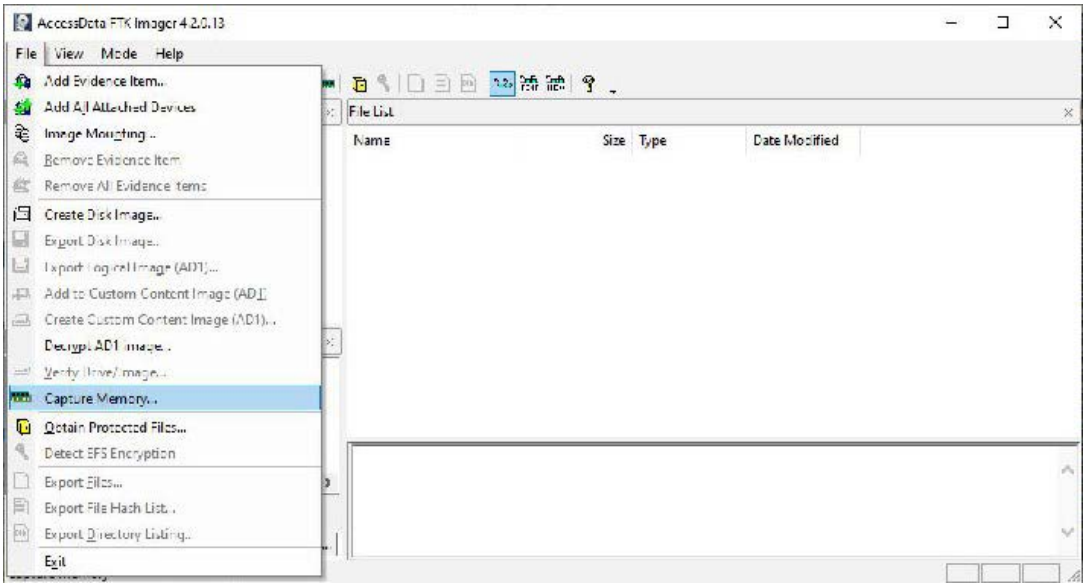
Checkliste für die Beweissicherung

1. **Fotografieren der vorgefundenen Situation**
   Hierbei sollten Fundort, Zustand (*an oder aus, Netzwerkkabel angeschlossen oder nicht,* ...) erkennbar sein. Dies dient auch der eigenen Sicherheit - nicht selten wird man beschuldigt einen Schaden verursacht oder etwas verlegt zu haben.
2. **Sofortmaßnahmen**
   Stellt ein System eventuell ein Risiko für andere Systeme dar, dann trennen Sie die Netzwerkverbindung oder wenn Sie fürchten, dass Schadware Beweise vernichten könnte, sobald der Kontakt zum Command- und Controll-Server abbricht, fahren Sie mit Punkt 3 fort und schalten Sie dann das System aus.
3. **Sichern Sie den volatilen Speichern**
   Dieser enthält aktive Netzwerkverbindungen, geladene Programme, DLLs und viele weitere Informationen. Auch wenn Sie meinen, diese Informationen im aktuellen Fall nicht zu brauchen, machen Sie es zu Sicherheit.
4. **Schalten Sie das System "hart" ab (***Stecker ziehen, Akku entfernen,* ...**)**
5. **Fotografieren Sie alle Label des PC**
   Vor allem Seriennummern sind wichtig, um später sicherzustellen, dass es dieser PC ist. Bedenken Sie Geräte werden auch weitergereicht und wir wollen auf jeden Fall Verwechselungen ausschließen.
6. **Entfernen Sie alle Datenträger und Fotografieren Sie die Label**
   Hier gilt das Gleiche wie für den PC selbst.
7. **Klonen Sie die Datenträger falls nötig vor Ort oder verpacken Sie diese für den Transport stoßsicher und in Antistatik-Beuteln**
   Es kann auch nicht schaden die Beutel oder Transportbehälter zu versiegeln, um sicherzustellen, dass diese nicht geöffnet wurden. Ein einfacher weißer Aufkleber mit Ihrer Unterschrift, der sich nicht zerstörungsfrei entfernen lässt, reicht vollauf.
8. **Machen Sie Notizen oder zusätzliche Fotos**
   Es kann eine lange Zeit zwischen dem Sichern der Beweise und dem Schreiben des Berichts vergehen. Sie werden sich Details wie Programmversionen, Uhrzeit, genaue Abfolge, etc. nicht alles so lange merken - daher schreiben Sie es auf, diktieren Sie es oder Fotografieren Sie jeden Schritt!

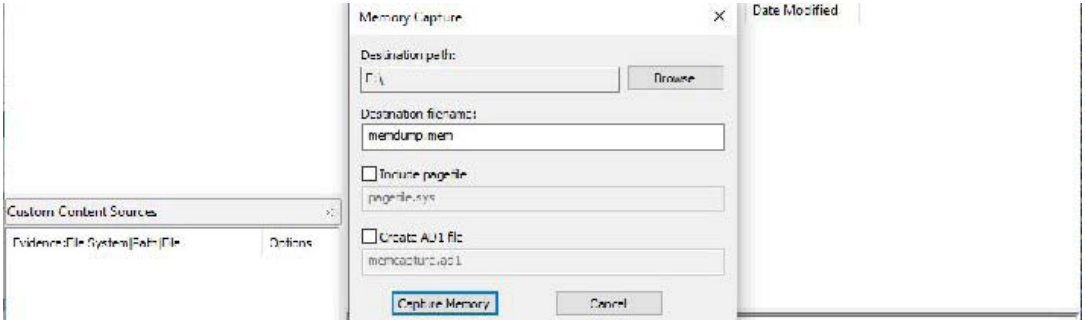
RAM-Speicher mit FTK Imager sichern (Windows)

In Windows ist das kostenlose Programm `FTK Imager` eine der einfachsten Möglichkeiten den RAM-Speicher zu sichern.

Dieses Tool können wir von `https://accessdata.com/product-download/FTK-Imager-version-4-5` herunterladen. Alternativ dazu gibt es auch ein kostenloses Tool von Belkasoft.



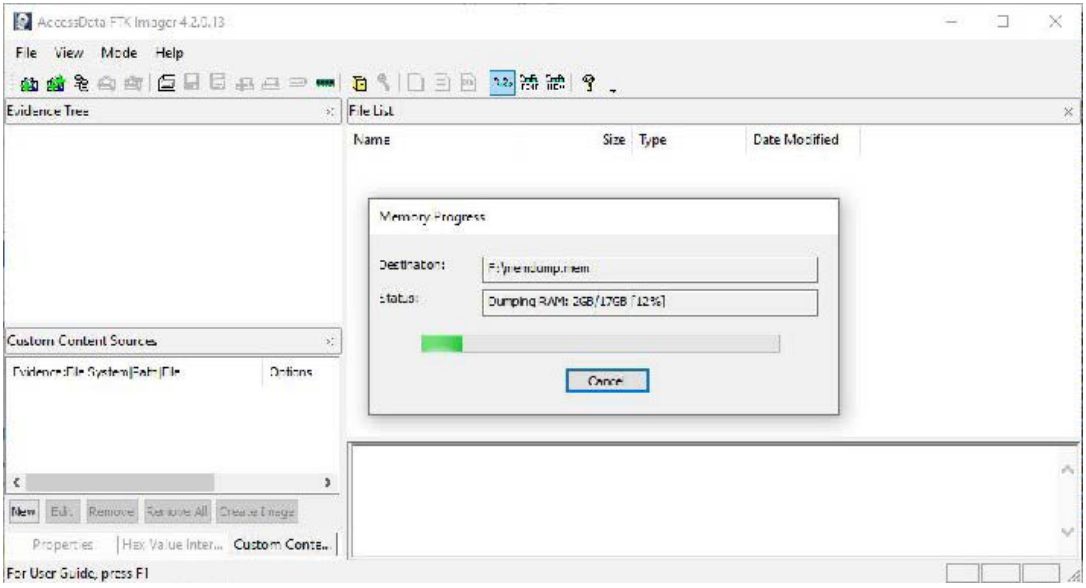
Nachdem wir das Programm gestartet haben, wählen Sie `File` -> `Capture Memory` aus und Sie sehen dann den folgenden Dialog:



Hier haben Sie die Möglichkeit den Pfad und den Dateinamen für den RAM-Dump festzulegen und gleich auch den virtuellen Speicher (`pagefile.sys`) zu kopieren und eine AccessData-Datei (`AD1`) anzulegen.

Wir brauchen in diesem Fall beides nicht. Die Datei `pagefile.sys` sichern wir nach dem Ausschalten des Rechners mit dem Klonen der Platte.

Klicken Sie auf `Capture Memory` und warten Sie, bis der Vorgang abgeschlossen ist:



Im Vergleich zu dem Tool von `Belkasoft` bietet uns `FTK Imager` aber eine ganze Menge weiterer Funktionen. Daher werden wir dieses Tool für einige weitere Aufgaben einsetzen und alternative Tools werde ich nur am Rande erwähnen.

Um schon vorab die Registry untersuchen zu können gibt es die Funktion `File -> Obtain protected files`. Hierbei haben Sie die Auswahl nur die Daten zum Knacken der Login-Passwörter zu sichern oder die gesamte Registry.

Da das Klonen einer Platte einige Stunden dauern kann, können wir so schon mit dem Untersuchen der Registry anfangen, während die Platte geklont wird.

RAM-Speicher mit AVML sichern (Linux)

Unter Linux können wir AVML von Microsoft verwenden. Dieses Tool können wir von `https://github.com/microsoft/avml/releases` als Binärdatei herunterladen.

Eigentlich sollte das Tool auf den meisten Linux-Distributionen lauffähig sein, aber sollte dies einmal nicht der Fall sein, können Sie den Quellcode von GitHub laden und das Programm selber kompilieren.

Danach brauchen Sie der Datei nur die entsprechenden Rechte mit `chmod` zuweisen und sie ausführen:

```
mark@ubuntu:~$ chmod 755 avml
mark@ubuntu:~$ sudo ./avml memory.img
```

Hierzu brauchen wir natürlich `root`-Rechte. Dem Programm übergeben wir nur den Dateinamen bzw. den Pfad mit dem Dateinamen und wir erhalten einen RAW-Dump des volatilen Speichers.

RAM-Speicher von OS X Systemen sichern

Für diese Aufgabe gibt es zwei Tools, die in Frage kommen:

```
https://sumuri.com/software/recon-itr/
https://www.cellebrite.com/en/digital-collector/
```

Diese grafischen Tools sollten selbsterklärend sein. Daher verzichte ich aus Platzgründen darauf sie mit den entsprechenden Screenshots dazustellen...

RAM-Speicher von virtuellen Maschinen sichern

Virtualisierung wird immer beliebter und daher werden wir als IT-Forensiker früher oder später darauf stoßen. Natürlich könnte man den RAM-Speicher wie bereits gezeigt einfach mit den entsprechenden Tools sichern aber virtuelle Maschinen haben virtuellen RAM und wenn wir diese Maschinen anhalten, dann wird er virtuelle RAM-Speicher auf die Festplatte des Host-Systems geschrieben damit die VM später den RAM-Inhalt wiederherstellen kann.

Das liefert uns, je nachdem, welche Technologie zur Virtualisierung eingesetzt wird, einen perfekten RAM-Dump.

Tipps für die Beweissicherung

Vergessen Sie nicht, die so gewonnenen Daten in der Dokumentation zu vermerken und auch die verwendeten Programme und deren Versionen.

Außerdem müssen Sie mit einem geeigneten Tool einen Hash für diese Dateien errechnen und vermerken.

Bedenken Sie auch, wenn Sie einen Hash in einer Textdatei speichern, kann dieser genau wie die Datei manipuliert werden. Darum mache ich zusätzlich ein Foto von der geöffneten Textdatei mit meiner Kamera.

Ich nutze hierfür eine günstige Spiegelreflexkamera aus drei Gründen:

1. Diese Kamera erlaubt mir Aufnahmen im RAW-Format zu machen und der viel größere Sensor im Vergleich zu Point-and-Shoot Kameras bietet mehr Details.
2. Das RAW-Format bietet bei der Entwicklung viel mehr Spielraum und so kann man aus dunklen Ecken oft noch einiges an Details gewinnen. Außerdem erschwert es Bildmanipulationen.
3. Größere Sensoren rauschen deutlich weniger - das ist vor allem bei Innenaufnahmen hilfreich.

Natürlich kann man mit dem entsprechenden Wissen sicherlich auch RAW-Daten bearbeiten aber die ganzen RAW-Entwickler arbeiten anders und speichern Veränderungen nur in einem Protokoll, das bei der Umwandlung in JPG auf die Datei angewendet wird. Somit hat man immer ein unverändertes Originalbild für den Fall der Fälle.

Klonen von Datenträgern

Kopieren wir Dateien von einem auf einen anderen Datenträger, dann erhalten wir lediglich die aktuell am System verfügbaren Daten. Abgesehen davon müssten wir darauf achten, dass das Programm mit dem wir die Daten kopieren auch die Zeitstempel sauber übernimmt und das Betriebssystem nicht auf Dinge wie zB Thumbnail-Datenbanken zugreift und diese zB aktualisiert.

Wir haben also relativ viel, dass wir beachten müssen für eine lückenhafte Sicherung der Daten. Beim Klonen kopieren wir Byte für Byte den gesamten Speicher des Datenträgers (*egal ob belegter oder freier Speicher*) und erhalten damit ein vollständiges Abbild mit allen gelöschten Dateien oder zumindest Dateifragmenten davon.

Hierbei können wir die Datenträger auf einen anderen Datenträger klonen oder in eine Datei. Ich bevorzuge Letzteres, da wir so in der Lage sind diese Datei direkt in einem Analysetool zu öffnen.

Wir können beim Klonen eines Datenträgers bestimmen ob wir den gesamten Datenträger mit MBR (*Master Boot Record*), Partitionstabelle, etc. und allen Partitionen klonen wollen oder nur eine spezifische logische Partition.

Ich persönlich würde immer die gesamte Platte klonen, außer es gäbe zB rechtliche Gründe, die dagegensprechen. In der Regel werden wir die Datenträger entnehmen und an einem unserer PCs klonen (*Dead Imaging*) aber sollte dies nicht möglich sein, ist es auch möglich einen Datenträger im laufenden Betrieb zu klonen (*Live Imaging*).

Vorbereiten der Ziel-Datenträger

Auch wenn wir unser Image in eine Datei speichern, sollten wir dennoch unsere Datenträger vorbereiten und sicherstellen, dass alle vorher darauf befindlichen Daten sicher gelöscht wurden.

Sollte mir die Frage gestellt werden, ob die Datenträger vor dem Einsatz von alten Daten bereinigt wurde, möchte ich nicht lange erklären müssen, warum dies nicht nötig ist in dem Fall und darauf hoffen, dass ein Richter diese Antwort auch richtig versteht, sondern ich erwidere lieber: "*Sehen Sie sich bitte Anlage 12 meines Gutachtens an, dort sehen Sie, dass der Datenträger sicher gelöscht und der Löschvorgang erfolgreich verifiziert wurde*".

Das bringt uns gleich zum nächsten Punkt - es ist immer besser derartige Aussagen auch gleich belegen zu können. Sie können natürlich auch ein kostenloses Tool wie zB Eraser (https://sourceforge.net/projects/eraser/) verwenden und dann einen Screenshot erstellen oder sie nutzen zB den Drive eRazer Ultra von CRU (https://wiebetech.com/products/wiebetech_drive_erazer_ultra/).

Dieses Tool gibt einen Löschbericht über die serielle Schnittstelle aus. Um diesem auf modernen Computern zu Empfangen gibt es ein seriell auf USB-Adapterkabel und die passende Software von CRU.

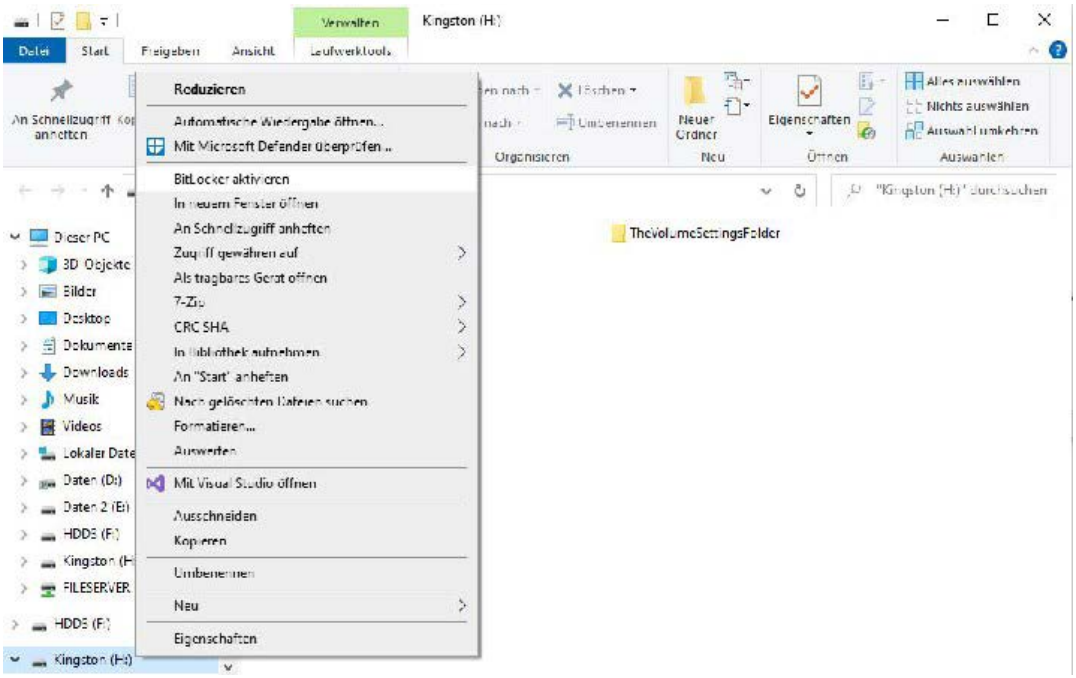
Abgesehen vom Bericht den Sie erhalten, belegen Sie so keinen Arbeitsplatz für Stunden mit den Löschvorgängen, können auch IDE-Platten löschen und das Gerät ist relativ günstig. Außer für die einzelnen forensischen Berichte sind die Löschberichte auch für Ihre Datenschutzdokumentation von Vorteil.

Verschlüsselung der Ziel-Datenträger

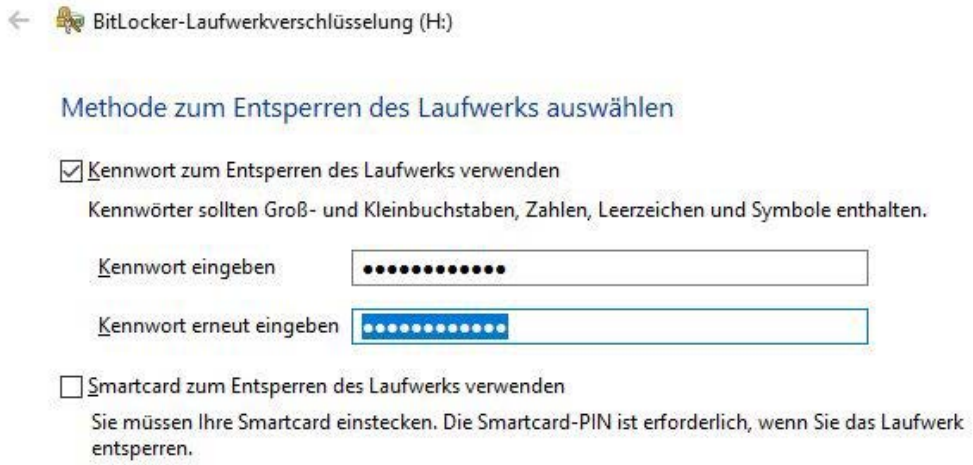
Um Daten vor unbefugten Zugriff zu schützen, ist es eine gute Idee, die Laufwerke auf denen Beweismittel gesichert werden zu verschlüsseln. Hierzu können wir `Bitlocker` oder auch `VeraCrypt` verwenden.

`VeraCrypt` gibt es nicht nur für Windows, sondern auch für Linux und Mac OS X.

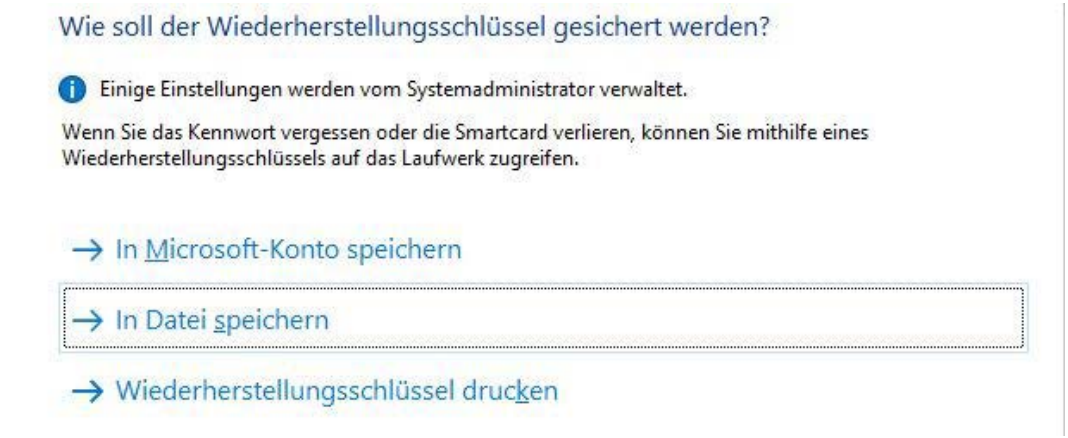
Sehen wir uns zuerst Bitlocker an:



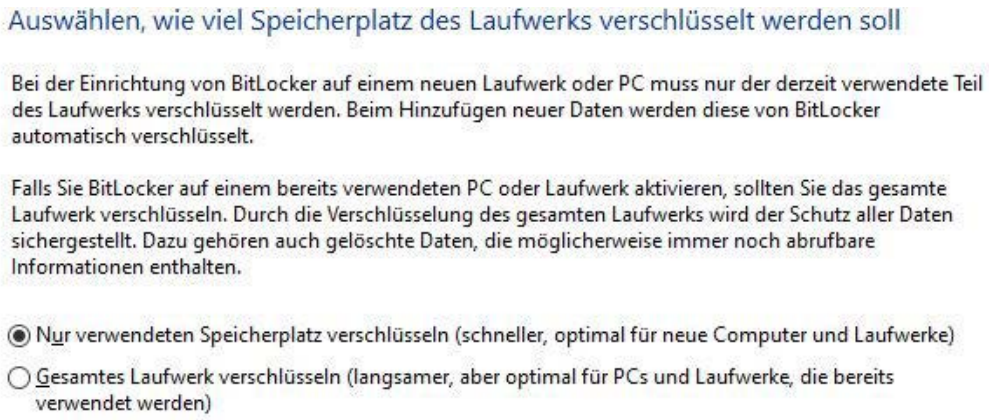
Mit einem Rechtsklick auf das Laufwerk im Explorer können wir `Bitlocker` aktivieren. Danach wird uns folgender Dialog angezeigt:



Geben Sie ein Passwort ein oder verwenden Sie eine Smartkarte.

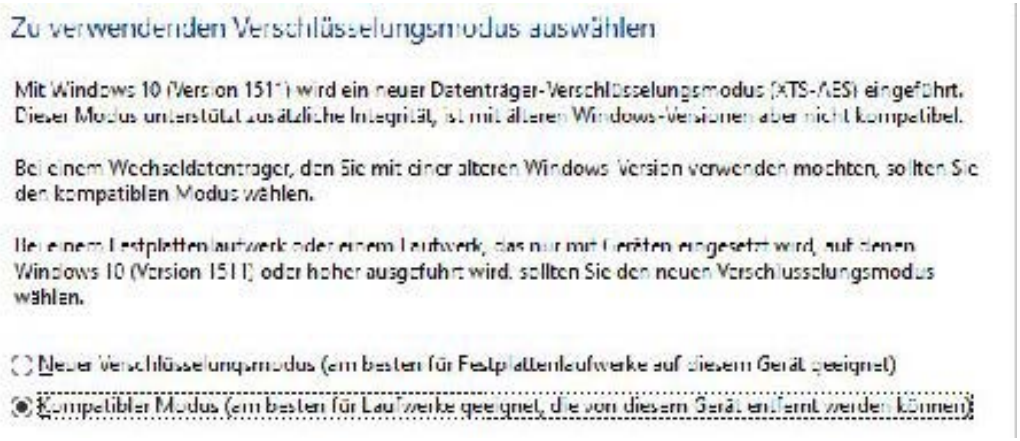


Ich würde vorschlagen, dass Sie den Wiederherstellungsschlüssel in eine Datei speichern oder ausdrucken. In der Regel brauchen Sie diesen nur, wenn Sie das Passwort vergessen.



Da wir dies in der Regel am Beginn einer Ermittlung machen und nicht irgendwann mittendrin oder am Ende und einen sicher gelöschten Datenträger nutzen brauchen wir nur den verwendeten Speicherplatz verschlüsseln.

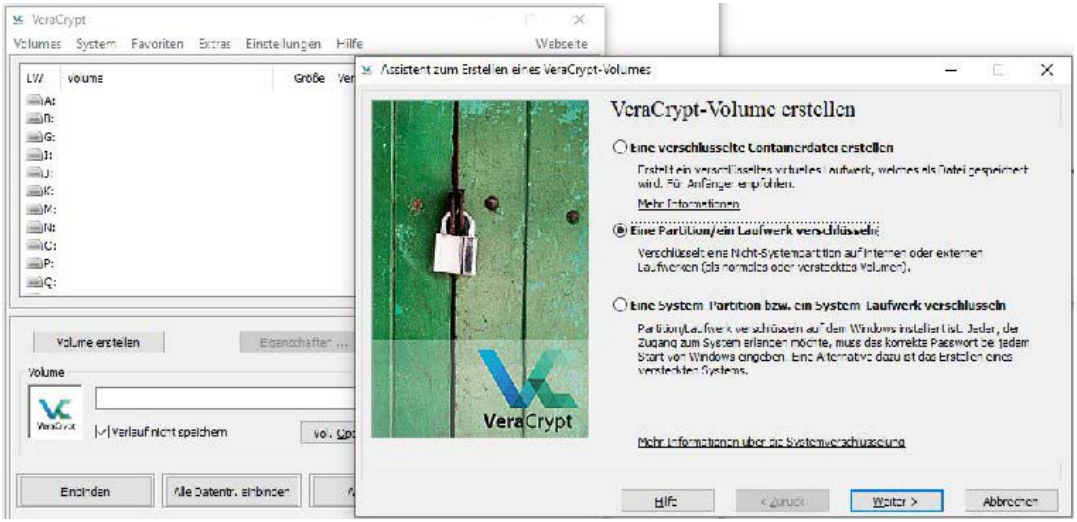
Das spart Zeit, denn je nach Größe des Laufwerks kann die Verschlüsselung des ganzen Datenträgers recht lange dauern!



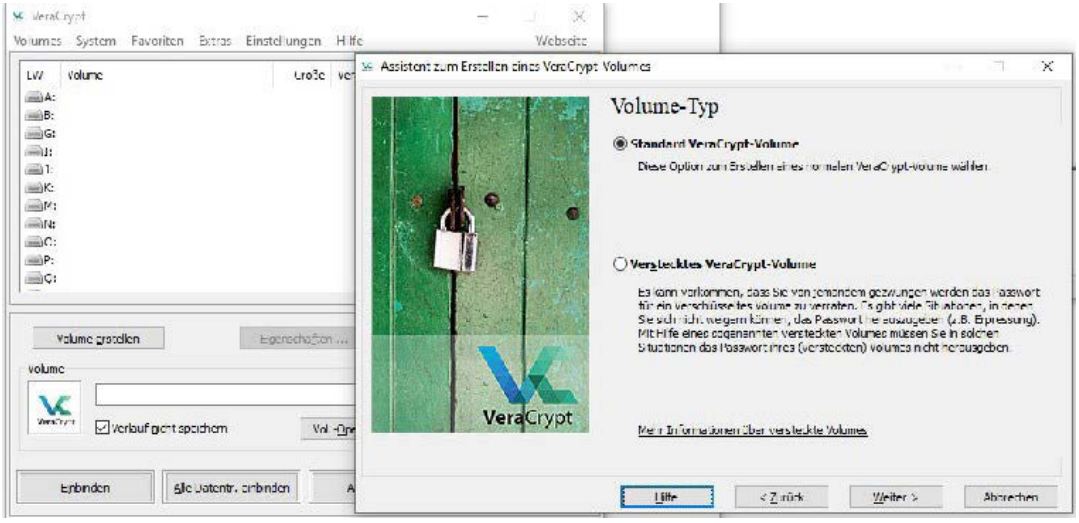
Ich nutze zur Sicherheit immer den Kompatiblen Modus, da ich für spezielle Aufgaben auch ein altes Windows 7 System nutze, dass alte Tools beheimatet die auch Windows 10 nicht mehr laufen. Im Bereich der Datenrettung nutze ich für einige Spezialfälle sogar noch ein altes System mit Windows XP auf dem ältere Tools laufen, die nur bis Windows XP einwandfrei funktionierten.

Die Einrichtung von `VeraCrypt` ist ähnlich einfach. Nachdem Sie `VeraCrypt` von `https://www.veracrypt.fr/en/Downloads.html` heruntergeladen und installiert

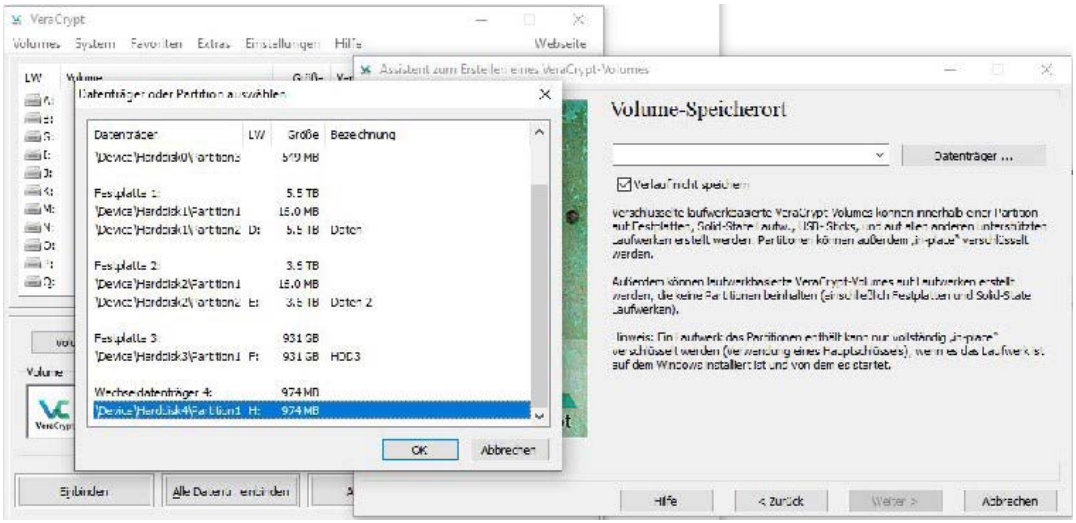
haben, können Sie das Programm starten und auf "Volume erstellen" klicken:



Hier wählen wir dann "Eine Partition / ein Laufwerk verschlüsseln" aus und klicken auf "weiter".

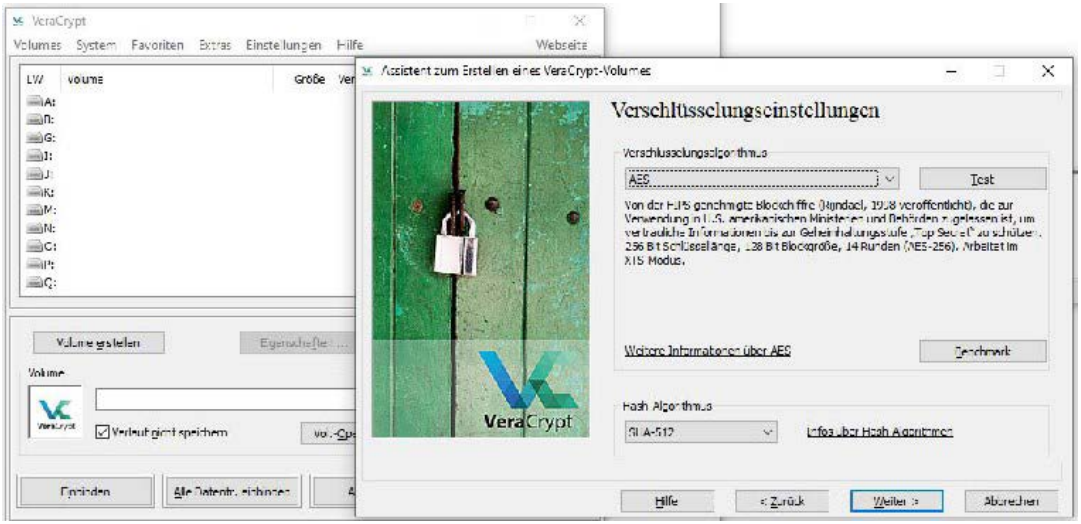


Dann haben wir die Auswahl zwischen einem Standard- und einem versteckten Volumen.

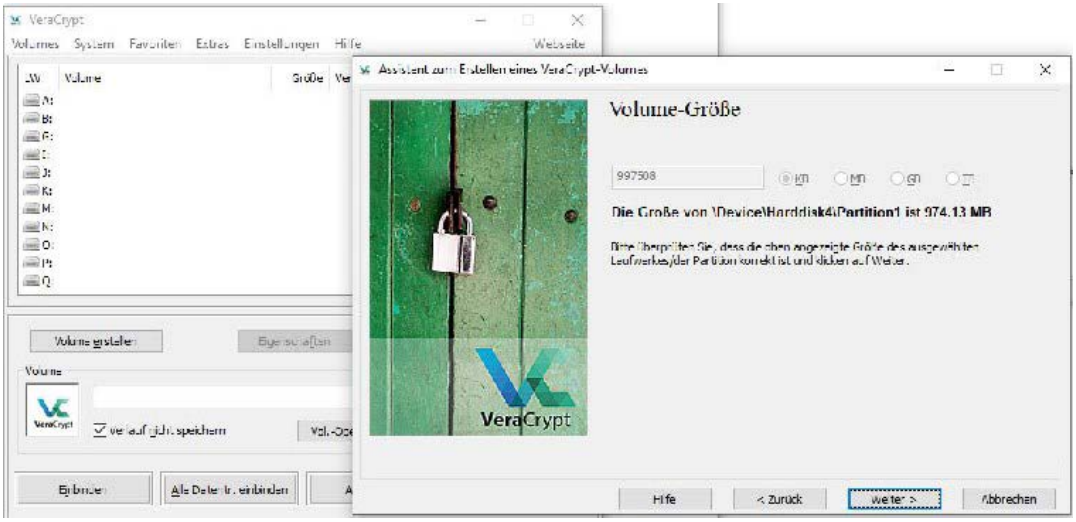


Nachdem wir auf "Datenträger" geklickt haben, öffnet sich ein weiteres Fenster in dem wir den Datenträger auswählen können. Wenn wir die Auswahl mit "OK" bestätigt haben, kommen wir mit einem Klick auf "weiter" zu folgendem Fenster:

Da die Platte ohnehin leer sein sollte, können wir "Verschlüsseln und Formatieren" wählen.



Dann können wir die Verschlüsselungsmethode auswählen. Wenn nichts anderes verlangt wird, würde ich den Standard mit AES und SHA-512 als Hash-Algorithmus so übernehmen.



Falls Sie eine verschlüsselte Containerdatei erstellen, können Sie nun die Datei- bzw. Containergröße auswählen.