[redacted]

[redacted]

Untersuchung TrueCrypt

Arbeitspaket 6

Ressourcen-Analyse

[redacted]

[redacted]

Historie

Version	Autor	Kommentar	Datum
0.1	[redacted]	Initale Dokumentenversion erstellt	16.09.10
0.2	[redacted]	Annahmen aktualisiert, erste Ergebnisse eingefügt	24.09.10
0.3	[redacted]	Annahmen aktualisiert, Windows Tests und TrueCrypt-interne Tests	04.10.10
0.4	[redacted]	Tests finalisiert, Analyse der Ergebnisse	21.10.10
0.5	[redacted]	Korrekturen nach BSI-Review, Executive Summary, Kurzergebnisse weiter ausgeführt	04.11.10
0.6	[redacted]	Review von Version 0.5	05.11.10
1.0	[redacted]	Finale Version 1.0	15.11.10

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1 Vorbetrachtung

1.1 Zielsetzung

Für den Einsatz einer Festplattenverschlüsselung ist es von Interesse, eine Abschätzung zu bekommen, wie stark sich der Einsatz von Verschlüsselung und der damit einhergehende Verlust von DMA auf die Systemperformance auswirkt.

Gerade im Hinblick auf den Einsatz zur „Full-Disc-Encryption“ können signifikante Ressourceneinbußen zu verzeichnen sein, je nachdem wie leistungsstark die zugrundeliegende Plattform ist.

Das Ziel dieses Arbeitspaketes ist es daher zunächst, basierend auf den in Kapitel 2.1 beschriebenen Testszenarien, für verschiedene Hardwareplattformen Messungen durchzuführen, die eine nominale Abschätzung der minimalen und maximalen Ressourceneinbußen durch den Einsatz von Verschlüsselung ermöglichen.

Darüber hinaus soll getestet werden, inwiefern der Einsatz einer Festplattenverschlüsselung für einen Benutzer in unterschiedlichen Szenarien zu einer Beeinträchtigung seiner Arbeit führen kann. Die Ergebnisse dieses Arbeitspaketes sollen letztlich dazu genutzt werden, Hardwareanforderungen abzuleiten, die ein System unter den spezifizierten Einsatzszenarien aus AP2 erfüllen muss, um trotz des Einsatzes von einer Verschlüsselungssoftware noch performant genug zu sein.

1.2 Messgrößen

Folgende Fragestellungen sind im Rahmen der Ressourcenanalyse hinsichtlich der entsprechenden Messgrößen zu beantworten:

1.2.1 CPU Auslastung

- *Minimum*
  Was ist der minimale Overhead, den TrueCrypt im entsprechenden Testszenario erzeugt?
- *Durchschnittlich*
  Wie groß ist der Einfluss von TrueCrypt in einem regulären Arbeitseinsatz, bei dem die Rechenleistung der ausführenden Plattform nur zu x% verwendet wird?
- *Maximum*
  Wie hoch sind die Performance-Einbußen durch den Einsatz der Verschlüsselungssoftware TrueCrypt maximal?

1.2.2 CPU Laufzeit

- Welche Laufzeit haben die kryptographischen Algorithmen?
- Gibt es signifikante Laufzeit-Unterschiede bei unterschiedlichen Algorithmen

und Kombinationen?

1.2.3 Speicherbedarf

- Wie groß ist der zusätzliche Speicherbedarf beim Einsatz von TrueCrypt?
- Wie skaliert der Speicherbedarf in Abhängigkeit der Anzahl der verschlüsselten Volumes?

1.2.4 Latenzzeit

- Wie groß ist die durch TrueCrypt verursachte Latenzzeit?

1.3 Laufzeitumgebung

TrueCrypt wird im Rahmen dieses Arbeitspaketes auf zwei unterschiedlichen Betriebssystemen untersucht:

- Microsoft Windows 7 (64-Bit)
- Microsoft Windows Vista (64-Bit)
- Ubuntu 10.04 LTS (mit Linux Kernel 2.6.32.24 bzw. 2.6.32.25)
  - 32-Bit (Netbook Edition)
  - 32-Bit (Desktop Edition)
  - 64-Bit (Desktop Edition)

Hierzu werden keine sich im aktiven Betrieb befindlichen Systeme genommen, sondern die Betriebssysteme werden neu installiert. Dies soll zum einen die Reproduzierbarkeit der Testergebnisse sicherstellen, zum anderen sollen die Testergebnisse nicht durch den Einsatz von Dritt-Software verfremdet werden.

Die genau verwendete Betriebssystemsoftware inkl. aktuellem Patchstand wird jeweils im Testbericht hinzugefügt.

1.4 Untersuchte Hardware

Die folgenden Hardwareplattformen werden für die Untersuchung verwendet. Je nach eingesetzter CPU stehen die folgenden Betriebsmodi, CPU-Kerne und Taktraten zur Verfügung. Geeignete, repräsentative Kombinationen werden in den Testszenarien ausgewählt.

1.4.1 Acer Aspire one D250-1Bk

- *CPU:* Intel Atom N280
- *CPU-Architektur:* 32-Bit
- *Anzahl CPU-Kerne:* 2 (DualCore)
- *Taktraten:* 1666 Mhz

- *RAM:* 1 GB DDR-2, 667 Mhz
- *Speicherbandbreite:* PC2-5300
- *Festplatte:* WD Scorpio 160GB SATA-2

1.4.2 Lenovo x61s

- *CPU:* Intel Core2Duo
- *CPU-Architektur:* 64-Bit
- *Anzahl CPU-Kerne:* 2 (DualCore)
- *Taktraten:* 800 Mhz, 1200 Mhz, 1600 Mhz
- *RAM:* 3GB (1x2GB+1x1GB) DDR-2, 667 Mhz
- *Speicherbandbreite:* PC2-5300
- *Festplatte:* Samsung 500GB SATA-2

1.4.3 HP EliteBook 8540p

- *CPU:* Intel Core i7-620M mit Hardware-AES Beschleunigung
- *CPU-Architektur:* 64-Bit
- *Anzahl CPU-Kerne:* 2 (mit Hyperthreading: 4 (QuadCore))
- *Taktraten:* 1200 Mhz, 1333 Mhz, 2666 Mhz
- *RAM:* 4GB (1x4GB) DDR-3, 1333 Mhz
- *Speicherbandbreite:* PC3-10600
- *Festplatte:* Seagate Momentum 320GB SATA-2

1.4.4 xPC Shuttle-PC G2

- *CPU:* AMD Athlon X2 7750
- *CPU-Architektur:* 64-Bit
- *Anzahl CPU-Kerne:* 2 (DualCore)
- *Taktraten:* 1350 Mhz, 2700 Mhz
- *RAM:* 4GB (2x2GB) DDR-2, 800Mhz
- *Speicherbandbreite:* PC2-6400
- *Festplatte:* WD SATA-2

2 Vorgehensbeschreibung

Durch die vielen verschiedenen Parameter der Ausführungsumgebung und der sehr großen Anzahl an möglichen Kombinationen von Hardware, Betriebssystemen, Festplatten, Taktfrequenzen und dergleichen, ist eine vollständige Testabdeckung nicht realisierbar. Vielmehr ist daher hier zu untersuchen, welche Auswirkungen die entsprechenden Faktoren auf die Performance des Systems haben und wie TrueCrypt diese in den entsprechenden Einsatzszenarien beeinflusst.

Um einen eindeutige Aussage treffen zu können, wird zuerst der Ist-Zustand der Messgrößen aus Abschnitt 1.2 ohne den Einsatz einer Verschlüsselungssoftware ermittelt. Im Anschluss daran werden die Testszenarien aus Abschnitt 2.2 mit Einsatz von TrueCrypt getestet.

2.1 Test-Anforderungen

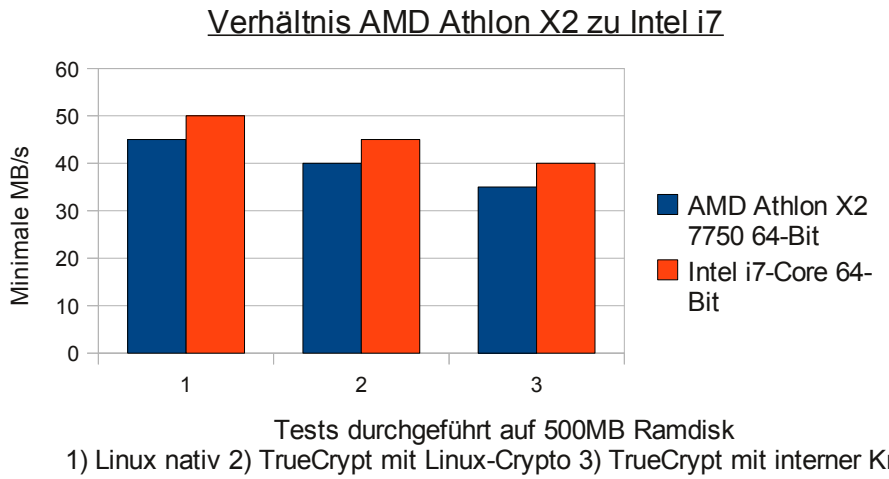
- Zur Reproduzierbarkeit der Testergebnisse und zur Minimierung der Einflussfaktoren durch Drittsoftware werden nur neu installierte Maschinen mit einem stabilen Betriebssystem geprüft.
- Die Testergebnisse sollen losgelöst von festplattenspezifischen Parametern sein. Hierzu wird eine Ramdisk mit einer Größe von 500 MB verwendet.
- Um bei einem Programmstart realistische Zeitmessungen zu erhalten, werden die Programme nach der Installation zunächst einmal ohne Messung gestartet, damit ggf. notwendige Konfigurationen beim ersten Start durchgeführt werden können. Im Anschluss daran muss der Testrechner neu gestartet werden, um die Messwerte nicht durch Programmreste im Speicher bzw. im Cache zu verfremden.
- Bei Tests im Umgang mit Dateien (z.B. Dateien packen / entpacken, kompilieren von Quelltext) muss nach jedem Testdurchlauf ein Neustart des Testrechners erfolgen, um die Messwerte nicht durch Datenreste im Speicher bzw. im Cache zu verfremden.

2.2 Test-Annahmen

2.2.1 AMD CPU versus Intel CPU

Es besteht kein signifikanter Unterschied zwischen dem Einsatz einer AMD-CPU im Vergleich zu einer Intel-CPU mit gleichen Leistungsmerkmalen (DualCore, 64-Bit, gleiche Taktrate). Im direkten Vergleich war die etwas modernere Intel-CPU zwar marginal schneller, das Verhältnis zwischen den beiden CPUs ist jedoch konstant. Daher kann im weiteren Testverlauf auf einen extra Testlauf mit einer AMD-CPU verzichtet werden:

- *Intel i7, 64-Bit, mit 2,67 Ghz* (QuadCore, aber nur 2 Kerne in Verwendung)
- *AMD Athlon, 64-Bit, mit 2,7 Ghz* (DualCore)



2.2.2 MultiCore versus SingleCore

Moderne CPUs bestehen heutzutage aus mehreren Kernen (z.B. DualCore, QuadCore). Diese können vom Betriebssystem einzeln angesteuert werden, sodass es möglich ist, einzelne Prozesse auf dedizierten CPU-Kernen auszuführen. Dies ist dann besonders von Vorteil, wenn Anwendungen auf einem „*thread*"-Modell basieren und Teile parallel ausgeführt werden können. Der Mehraufwand durch das zusätzliche „*thread*"-Management ist in der Regel vernachlässigbar, sodass die Annahme getroffen werden kann, dass MultiCore-CPUs schneller sind als SingleCore-CPUs.

Betrachtet man z.B. die Ergebnisse des TrueCrypt-internen Benchmarks (siehe Kapitel 4.2) unter Windows im Höchstleistungsmodus und vergleicht die effektiven Geschwindigkeiten bei MultiCore-Systemen, so erkennt man, dass diese Annahme für den reinen Algorithmusablauf zu stimmen scheint.

Acer Aspire One	
DualCore	27,1 MB/s
SingleCore	14,8 MB/s
Lenovo X61s	
DualCore	113 MB/s
SingleCore	64,9 MB/s
HP EliteBook 8540p	
QuadCore	234 MB/s
SingleCore	105 MB/s

Tabelle 1: Vergleich TrueCrypt-interner Benchmark für MultiCore vs. SingleCore

Der Geschwindigkeitsvorteil beim Einsatz von MultiCore-Systemen liegt im Schnitt bei 80-120%.

Es gibt allerdings Ausnahmen, in denen der Overhead durch den Einsatz von MultiCore zu einer langsameren Performance führt. Dies ist immer dann der Fall,

wenn auf Daten zugegriffen wird, die kleiner sind als eine Kernelseite (in der Regel 4096 Byte = 4 kB). So sind automatisch Dateisysteme mit einer Blockgröße in Höhe einer Sektorgröße (512 Byte) für den Einsatz bei MultiCore-Systemen inperformanter als bei SingleCore-Systemen. Die folgende Tabelle veranschaulicht die Geschwindigkeitsunterschiede bei unterschiedlichen Blockgrößen:

Name:	***Acer Aspire One***	***Acer Aspire One***
32-Bit / 64-Bit:	32-Bit	32-Bit
Anzahl Kerne:	DualCore	SingleCore
Linux-Crypto-Geschwindigkeit	**in MB/s**	**in MB/s**
512 Byte	9,8	10,1
1024 Byte	10,3	10,6
2048 Byte	10,5	8,7
4096 Byte	24,0	20,0
8192 Byte	23,9	22,2
16384 Byte	24,0	22,5
32768 Byte	24,0	22,1

Name:	***HP EliteBook 8540***	***HP EliteBook 8540***
32-Bit / 64-Bit:	64-Bit	64-Bit
Anzahl Kerne:	QuadCore	SingleCore
Linux-Crypto-Geschwindigkeit	**in MB/s**	**in MB/s**
512 Byte	56,4	59,3
1024 Byte	59,7	59,8
2048 Byte	57,3	63,5
4096 Byte	148,0	127,0
8192 Byte	148,0	128,0
16384 Byte	134,0	128,0
32768 Byte	149,0	129,0

Name:	***HP EliteBook 8540***	***HP EliteBook 8540***
32-Bit / 64-Bit:	32-Bit	32-Bit
Anzahl Kerne:	QuadCore	SingleCore
Linux-Crypto-Geschwindigkeit	**in MB/s**	**in MB/s**
512 Byte	51,2	52,4
1024 Byte	53,4	53,9
2048 Byte	52,0	55,2
4096 Byte	127,0	110,0
8192 Byte	127,0	111,0
16384 Byte	127,0	111,0
32768 Byte	127,0	111,0

Tabelle 2: Geschwindigkeitsunterschiede in Abhängigkeit der Blockgröße und der Kernanzahl

Gleichzeitig zeigt sich aber auch, dass der ursprünglich reine Geschwindigkeitsvorteil der reinen CPU-Zeit beim Einsatz auf Dateisystemen nicht mehr so groß ist. Jedoch bietet der Einsatz von MultiCore-CPUs den Vorteil, dass mehrere Aufgaben gleichzeitig ausgeführt werden können, sodass eine zu hohe Betriebslast durch den Einsatz von Verschlüsselung besser verteilt werden kann. Tests auf SingleCore-CPUs zeigen, dass die CPU-Auslastung bei 100% liegt, sodass während der reinen Kryptooperation keine weiteren Dienste parallel ausgeführt werden, sodass das System in dieser Zeit hängt. In der Regel ist dies je nach System mehr oder weniger bemerkbar, da hier auch die Festplattenzugriffszeit eine Rolle spielt.

Im MultiCore-Betrieb liegt die Auslastung des einzelnen Core, welcher gerade die Kryptooperation durchführt, ebenfalls bei 100%, jedoch stehen weitere Cores für den regulären Betriebsablauf zur Verfügung, sodass das System nicht hängt.

2.2.3 CPU-Taktfrequenz

Das Verhältnis des Datendurchsatzes in Abhängigkeit von der CPU-Taktrate ist nahezu linear.

- *Intel i7, 64-Bit*: Es wurde die Taktraten 1333 Mhz sowie die maximale Taktrate von 2666 Mhz gewählt. Die erreichten Messwerte verdoppelten sich bei einer Verdopplung der Taktrate (25,28 MB/s versus 56,5 MB/s).
- *Intel Core2Duo, 64-Bit*: Es wurde die Taktrate 800 Mhz sowie die maximale Taktrate von 1600 Mhz gewählt. Hier haben sich die Messwerte zwar nicht verdoppelt, sie stiegen lediglich um 43% (13,8 MB/s versus 24,5 MB/s). Dies kann unter anderem mit der langsameren Speicherbandbreite zusammenhängen.
  Zur Vereinfachung der weiteren Tests reicht es dennoch aus, sich die minimalen und maximalen Frequenzen der jeweiligen CPUs anzusehen. Die Performance bei den Zwischen-Taktfrequenzen verhält sich nahezu linear.

2.2.4 Lesevorgang versus Schreibvorgang

Das Lesen von (verschlüsselten) Daten ist schneller als das Schreiben von (verschlüsselten) Daten. Daher werden im Folgenden lediglich die Geschwindigkeiten von Schreibvorgängen gemessen.

2.2.5 64-Bit CPUs versus 32-Bit CPUs

64-Bit CPUs sind schneller als 32-Bit CPUs. Daher werden zur Bestimmung von maximaler Performance die Messwerte unter einer 64-Bit Architektur gemessen.

2.2.6 Einsatz von AES-Hardwarebeschleunigern

Der Einsatz von Hardware-Beschleunigern, wie z.B. die neuen *AES-NI*-Instruktionen in Intel's Core-i7-CPU erhöhen signifikant den Kryptodurchsatz beim Einsatz von AES. Allerdings setzt dies den Einsatz von AES als Algorithmus zwingend voraus. Um eine realistische Abschätzung der minimalen Hardwarekonfiguration für den Einsatz einer Festplattenverschlüsselung zu erzielen und um nicht auf AES als Kryptoalgorithmus festgelegt zu sein, werden im Folgenden zunächst der Geschwindigkeitsvorteil beim Einsatz von Hardwarebeschleunigern bestimmt, im

Anschluss daran allerdings sämtliche Tests ohne Hardwarebeschleuniger durchgeführt. Dies hat den Vorteil, dass man auch die Geschwindigkeit von anderen in Software implementierten Algorithmen realistischer abschätzen kann.

HP EliteBook 8540p unter Linux			
	mit AESNI	***ohne AESNI***	***Faktor***
QuadCore 64-Bit	1,5 GB/s	242 MB/s	ca. 6x
SingleCore 64-Bit	563 MB/s	117 MB/s	ca. 5x
QuadCore 32-Bit	995 MB/s	200 MB/s	ca. 5x
TrueCrypt-Benchmark der reinen Algorithmen			
512 Byte Blöcke	***mit AESNI***	***ohne AESNI***	***Faktor***
QuadCore 64-Bit	90 MB/s	55 MB/s	ca. 1,6x
SingleCore 64-Bit	105 MB/s	60 MB/s	ca. 1,75x
4096 Byte Blöcke	***mit AESNI***	***ohne AESNI***	***Faktor***
QuadCore 64-Bit	270 MB/s	150 MB/s	ca. 1,8x
SingleCore 64-Bit	230 MB/s	130 MB/s	ca. 1,75x
Einsatz von AES-NI auf realen Blockdevices (RAMDisk)			

Tabelle 3: Vergleich der Geschwindigkeiten bei Einsatz von Intel's Hardwarebeschleunigung AES-NI

Die Tabelle zeigt, dass die reine Ausführungszeit der Algorithmen durch TrueCrypt ca. 5-6x schneller beim Einsatz der AES-Hardwarebeschleunigung ist, als bei reinen Software-Operationen ohne Hardwareunterstützung. Jedoch zeigt sich, dass sich im echten Einsatz auf einem Blockgerät dieser Geschwindigkeitsvorteil auf ca. 70-80% reduziert.

2.3 Testszenarien

Dieser Abschnitt beschreibt die Testszenarien, die im Rahmen der Arbeiten von AP6 durchgeführt werden. Ein Verweis auf die erzielten Testergebnisse der einzelnen Szenarien wird jeweils in Klammern referenziert.

2.3.1 Ist-Zustand

Feststellen des Ist-Zustandes (Bestimmung der Messgrößen) ohne den Einsatz von Verschlüsselung. (siehe 4.3)

2.3.2 Performance der Krypto-Algorithmen

Die folgenden Tests werden zunächst losgelöst von einem physischen Medium nur innerhalb einer virtuellen Festplatte im RAM ausgeführt. Als Ramdisk-Größe wurde 500MB gewählt:

- Geschwindigkeitsmessung der
  - TrueCrypt-internen Krypto-Implementierung unter Windows (siehe 4.2, 4.4.2, 5.2, 5.4)
  - TrueCrypt-internen Krypto-Implementierung unter Linux (siehe 4.2, 4.4.1, 5.2, 5.3)
- Vergleich der
  - TrueCrypt-internen Krypto-Implementierung mit den Implementierungen innerhalb des Linuxkernels (siehe 4.4.1)
  - Geschwindigkeit bei Einsatz von Hardware-Beschleunigung (z.B. AES-NI bei Intel i7 CPU, siehe 2.2.6, 5.2.3, 5.3.3, 5.4.3)

2.3.3 Auswirkungen auf die Performance durch das verwendete Dateisystem

- Dateisysteme unter Windows:
  - FAT32
  - NTFS

  (siehe 4.5.3, 5.4)
- Dateisysteme unter Linux
  - EXT3
  - REISERFS
  - VFAT
  - XFS

  (siehe 4.5.1, 4.8, 5.6)

2.3.4 Auswirkungen auf die Performance in Abhängigkeit von der Blockgröße

- Nativer Blockzugriff mit unterschiedlichen Blockgrößen unter Linux
  - 512 Byte
  - 1024 Byte
  - 2048 Byte
  - 4096 Byte (Kernel page)
- (siehe 4.8, 5.3, 5.6.2)

2.3.5 Erstellen eines TrueCrypt-Volumes

Durchführung der folgenden Tests und Messungen innerhalb des verschlüsselten TrueCrypt-Volumes:

Auswirkungen auf die Performance durch die Größe der zu öffnenden Dateien

- Kleinste Dateigröße (Sektorgröße)
- Kleine Dateigröße (Kernel page)
- Mittlere Dateigröße (wenige KB)
- Große Dateigröße (wenige MB)
- Riesige Dateigröße (>500MB – 1GB)

  (siehe 5.6)

Auswirkungen auf die Performance durch die Anzahl der zu öffnenden Dateien

- Packen / Entpacken von vielen kleinen Dateien (siehe 4.5)
- Compilieren von Sourcecode mit vielen kleinen Dateien (siehe 4.6)

2.3.6 Full-Disc-Encryption

- Komplett-Verschlüsselung der Systempartition unter Windows
- Vergleich der Systemstart-Zeiten
- Vergleich der Programm-Startzeiten

  (siehe 4.7, 5.5)

3 Testvoraussetzungen und Vorgehensweise

3.1 Installation benötigter Software

Folgende Testwerkzeuge werden für die nachfolgenden Tests – neben TrueCrypt – verwendet:

3.1.1 Testwerkzeuge für Linux

- cryptsetup[1]
- dd
- Bonnie++[2]
- iozone[3]
- valgrind[4]
- Systemmonitor

Diese werden wie folgt installiert:

```
# apt-get install cryptsetup bonnie++ iozone3 valgrind
```

Zusätzlich werden noch für Dateisystemtests die folgenden Pakete benötigt:

```
# apt-get install reiserfsprogs xfsprogs
```

3.1.2 Vorgehensweise unter Linux

Um Performancemessungen unter Linux durchzuführen, werden die folgenden 3 Werkzeuge verwendet[5], die erzielten Messwerte resultieren jeweils aus sequentiellen d.h. linearen Schreibzugriffen:

- **dd** Mittels `dd` können Datenblöcke direkt auf Blockgeräte geschrieben werden. `dd` benötigt kein zugrundeliegendes Dateisystem, die zu verwendende Blockgröße kann direkt mit angegeben werden. Im Anschluss an jeden Schreibvorgang gibt `dd` die benötigte Zeit sowie die durchschnittliche Leistung in MB/s aus. Folgende Befehle werden verwendet, um die Geschwindigkeit bei unterschiedlichen Blockgrößen zu messen:
  - *512 Byte:* `dd if=/dev/zero of=$TESTBLOCKFILE bs=512 count=1000000`
  - *1024 Byte:* `dd if=/dev/zero of=$TESTBLOCKFILE bs=1024 count=500000`
  - *2048 Byte:* `dd if=/dev/zero of=$TESTBLOCKFILE bs=2048 count=250000`
  - *4096 Byte:* `dd if=/dev/zero of=$TESTBLOCKFILE bs=4096 count=125000`
  - *8192 Byte:* `dd if=/dev/zero of=$TESTBLOCKFILE bs=8192 count=62500`
  - *16 kByte:* `dd if=/dev/zero of=$TESTBLOCKFILE bs=16k  count=31250`

1 http://code.google.com/p/cryptsetup/
2 http://www.coker.com.au/bonnie++/
3 http://www.iozone.org/
4 http://www.valgrind.org
5 Zur Automatisierung der folgenden Tests sind Skripte verfügbar.

- *32 kByte:* `dd if=/dev/zero of=$TESTBLOCKFILE bs=32k count=15625`

Bei den folgenden Messungen variiert für die einzelnen Tests lediglich das Zielblockgerät (hier identifiziert via `$TESTBLOCKFILE`). Um die einzelnen Testziele zu erzeugen, wird wie folgt vorgegangen:

1. Anlegen einer 500MB-großen Ramdisk (*tmpfs*):

   ```
   #    mount -t tmpfs none -o size=500m $TESTPATH
   ```

2. Schreiben von 500MB in eine Datei, dabei Messen der Speichergeschwindigkeit via `dd` bei unterschiedlichen Blockgrößen.

   ```
   #    dd if=/dev/zero of=$TESTBLOCKFILE bs=<512-32k>
   ```

3. Erzeugen eines Blockgerätes mittels `losetup`.

   ```
   #    losetup /dev/loop0 $TESTPATH/$TESTBLOCKFILE
   ```

4. Nach Erzeugen des Blockgerätes `/dev/loop0` kann der Performanceverlust durch den Device-Mapper des Linuxkernels gemessen werden.

   ```
   #    dd if=/dev/zero of=/dev/loop0 bs=<512-32k>
   ```

5. Dieses Blockgerät wird nun mittels der Linuxkernel-Krypto verschlüsselt:

   ```
   #    cryptsetup create test /dev/loop0 -c aes-xts-plain
   ```

6. Anschließend folgt die Bestimmung der Performance der Linuxkernel-Krypto:

   ```
   #    dd if=/dev/zero of=/dev/mapper/test bs=<512-32k>
   ```

7. Das Krypto-Mapping wird nun wieder entfernt und das Blockgerät `/dev/loop0` mittels TrueCrypt verschlüsselt und die Performancetests via `dd` wiederholt.

   ```
   #    cryptsetup remove test
   #    truecrypt -t --create --volume-type=Normal /dev/loop0
        --encryption=AES --hash=SHA-512 –filesystem=None \
        -p="no-password" --random-source=/dev/urandom \
        --non-interactive
   #    truecrypt -t --mount /dev/loop0 -p="no-password" \
        --filesystem=none –non-interactive \
        --slot=5
   #    dd if=/dev/zero of=/dev/mapper/truecrypt5 bs=<512-32k>
   ```

8. Die obigen Tests haben jeweils die linuxinternen Krypto-Algorithmen verwendet. Nun wird Punkt 7) wiederholt, jedoch nicht über die Kommandozeile, sondern über die grafische Benutzeroberfläche von TrueCrypt. TrueCrypt muss dazu jedoch zunächst wie in Abschnitt 3.4.2 beschrieben auf die Verwendung der internen Krypto-API umgestellt werden.
9. Zuletzt werden Tests 1-8) in unterschiedlichen Konfigurationen (QuadCore, DualCore, SingleCore – siehe Abschnitt 3.2.2) und Energiemodi (Performance, Powersave – siehe Abschnitt 3.3.2) wiederholt.

- **Bonnie++** Mittels `Bonnie++` lässt sich die Performance von Blockgeräten mit Hilfe von unterschiedlichen Tests untersuchen, unter anderem das Lesen, Schreiben von Dateien mit unterschiedlichen Datei- und Blockgrößen.

  1. Um diese Tests durchzuführen, ist es zunächst nötig, die Punkte 1)2)3) und 7) bzw. 8) der dd-Tests auf Seite 17 zu wiederholen, um ein verschlüsseltes Blockgerät zu erzeugen.
  2. Danach wird auf dem Blockgerät ein Dateisystem erzeugt und dieses in das Dateisystem eingehängt.

     - **EXT3**: `# mkfs.ext3 /dev/mapper/truecrypt5`
     - **ReiserFS**: `# mkfs.reiserfs -b 4096 /dev/mapper/truecrypt5`
     - **VFAT**: `# mkfs.vfat /dev/mapper/truecrypt5`
     - **XFS**: `# mkfs.xfs -f /dev/mapper/truecrypt5`

     ```
     # mount /dev/mapper/truecrypt5 $MOUNTTARGET
     ```

  3. Anschließend können die Tests mit `Bonnie++` durchgeführt werden

     ```
     # bonnie++ -u root -d $MOUNTTARGET -s 200 -r 100 -b
     ```

     Der Parameter „-s“ legt hierbei die Dateigröße in MB fest, „-r“ stellt hierbei die zu verwendende Menge an Arbeitsspeicher ein.

- **Iozone:** Iozone ist ebenfalls ein Dateisystem-Benchmarking-Werkzeug, welches eine Vielzahl an Tests durchführen kann, u.a. unterschiedliche Dateioperationen (read, write). Idealerweise führt man die Tests mit Iozone direkt im Anschluss an Punkt 3) der `Bonnie++` Tests durch, da das entsprechende Dateisystem dann bereits erstellt und eingehängt ist.

  # iozone -a -o -n 512 -g 16m -y 512 -q 16m -f $MOUNTTARGET/iozone.test

  Die Parameter bedeuten:

  - „-a“: automatischer Modus
  - „-o“: automatisches synchronisieren mit dem Blockdevice, um Einflüsse durch Caches zu verhindern
  - „-n“: minimale Dateigröße in kB
  - „-g“: maximale Dateigröße in MB
  - „-y“: minimale Blockgröße in kB
  - „-q“: maximale Blockgröße in MB

3.1.3 Testwerkzeuge für Windows

- Dataram RAMDisk[6] Version 3.5.130RC14
- CrystalDiskMark Version 3.0 x64 (Release 2010/3/21)[7]
- Windows Power Shell[8] Version 2.0
  - *Measure-Command* zur Zeitmessung
- Ressourcenmonitor

3.1.4 Vorgehensweise unter Windows

Unter Windows sind die notwendigen Testschritte um einiges einfacher als unter Linux, da es für TrueCrypt nicht zwei unterschiedliche Krypto-Algorithmen gibt, sodass grundsätzlich die internen Funktionen verwendet werden. Um unter Windows die gleichen Tests nachzuvollziehen, wird wie folgt vorgegangen:

- **Dataram RAMDisk:** Zunächst wird mittels dieser Software eine RAMDisk mit 500 MB angelegt.

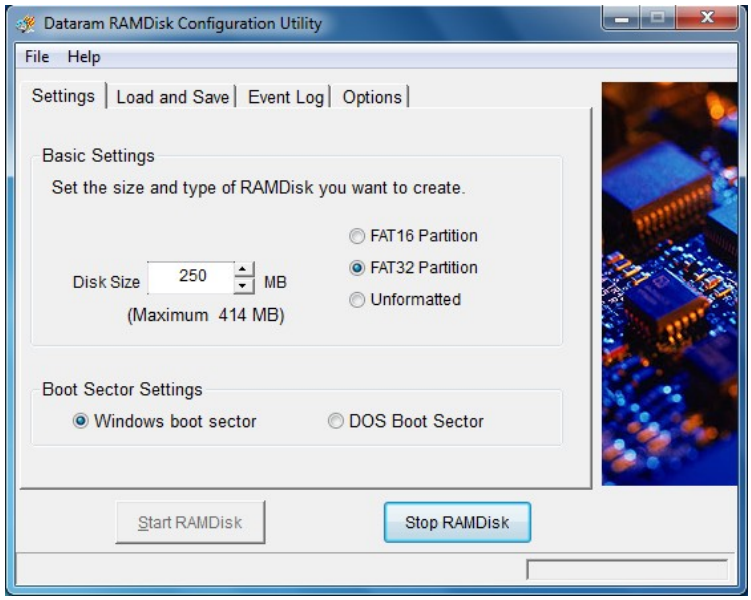


Abbildung 1: Bildschirmfoto des Dataram RAMDisk Konfigurationswerkzeug

  - Dazu wird die „Disk Size“ entsprechend eingestellt und auf „Start RAMDisk“ geklickt.
  - Nun steht unter Windows ein neues Laufwerk „D:\“ zur Verfügung, welches rein aus Arbeitsspeicher besteht.

6 http://memory.dataram.com/products-and-services/software/ramdisk
7 http://crystalmark.info/software/CrystalDiskMark/index-e.html
8 Integraler Bestandteil von Windows 7

CrystalDiskMark: Mittels CrystalDiskMark kann man nun die Zugriffszeiten bestimmen. Relevant für die Testauswertung sind, wie in Abschnitt 2.2.4 beschrieben, lediglich die Schreibvorgänge der rechten Spalte. Um Vergleichbarkeit mit den Linuxtests herzustellen, werden die sequentiellen Ergebnisse aus der ersten Zeile verwendet.

- Bestimmung der RAMDisk-Geschwindigkeit

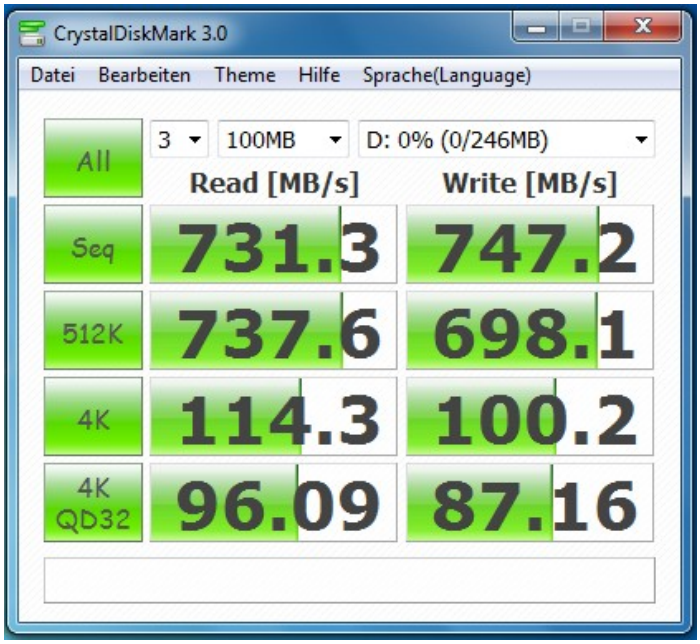


Abbildung 2: Bildschirmfoto über die Geschwindigkeitsmessungen von CrystalDiskMark

- Starten von TrueCrypt und Erzeugen eines verschlüsselten Blockdevices auf dem Laufwerk D: zugeordneten Device.
- Einhängen des verschlüsselten Gerätes auf ein neues Laufwerk (z.B. E:\)
- Dann die Benchmarks mit CrystalDiskMark auf dem neu eingehängten Laufwerk E:\ wiederholen. Die Ergebnisse spiegeln nun die Performance beim Einsatz von Verschlüsselung auf einem Blockgerät wider.
- Obige Tests werden sowohl für den Höchstleistungs- als auch den Energiesparmodus (siehe Abschnitt 3.3) durchgeführt und zwar sowohl für den QuadCore / DualCore-Betrieb als auch für den SingleCore-Betrieb (siehe Abschnitt 3.2).

- **Zeitmessungen:** Um im weiteren Testverlauf den Einfluss einer Full-Disc-Encryption auf die Gesamtsystemleistung zu ermitteln, werden zunächst einige Zeitmessungen durchgeführt, um im Nachhinein die für einen Benutzer merklichen Unterschiede herauszufinden. Hierzu werden folgende Daten manuell mittels einer Stoppuhr ermittelt und in Sekunden notiert, ebenfalls für den QuadCore / DualCore-Betrieb als auch für den SingleCore-Betrieb (siehe Abschnitt 3.2).
  - Starten von Windows
  - Herunterfahren von Windows
  - Starten von Mozilla Firefox
  - Starten von OpenOffice
  - Extrahieren von Eclipse

    (1.251 kleine und große Dateien mit Archivgröße >100MB)
  - Starten von Eclipse IDE

    (Jedoch erst nach Neustart des Systems, um ggf. im Cache befindliche Daten zu eliminieren)

- **Full-Disc-Encryption:** Je nach Einsatzszenario von TrueCrypt ist es nötig, das gesamte System zu verschlüsseln. Diese Full-Disc-Encryption kann unter Umständen die Systemperformance erheblich beeinflussen, da der durch DMA gewonnene Geschwindigkeitsverlust durch die Ver- und Entschlüsselung der Daten in der CPU wieder aufgehoben wird. Um den für den Benutzer merklichen Einfluss auf die Performance zu messen, wird das System mit TrueCrypt Full-Disc-verschlüsselt und im Anschluss daran die obigen Zeitmessungen wiederholt. Darüber hinaus wird die Zeit, welche zum Umschlüsseln benötigt wird, ebenfalls gemessen.

3.2 Umschalten zwischen MultiCore auf SingleCore Betrieb

3.2.1 Windows

Unter Windows stehen in der Standardkonfiguration dem Benutzer immer sämtliche verfügbaren CPUs zur Verfügung. Um jedoch die Anzahl der verwendeten CPUs zu reduzieren und so weitere Tests durchzuführen, kann man die Anzahl der CPUs wie folgt konfigurieren:

Start → Systemkonfiguration → Start → Erweiterte Optionen →

Prozessoranzahl = 1 (für SingleCore oder 2 für DualCore) →

Übernehmen → OK → Neustart

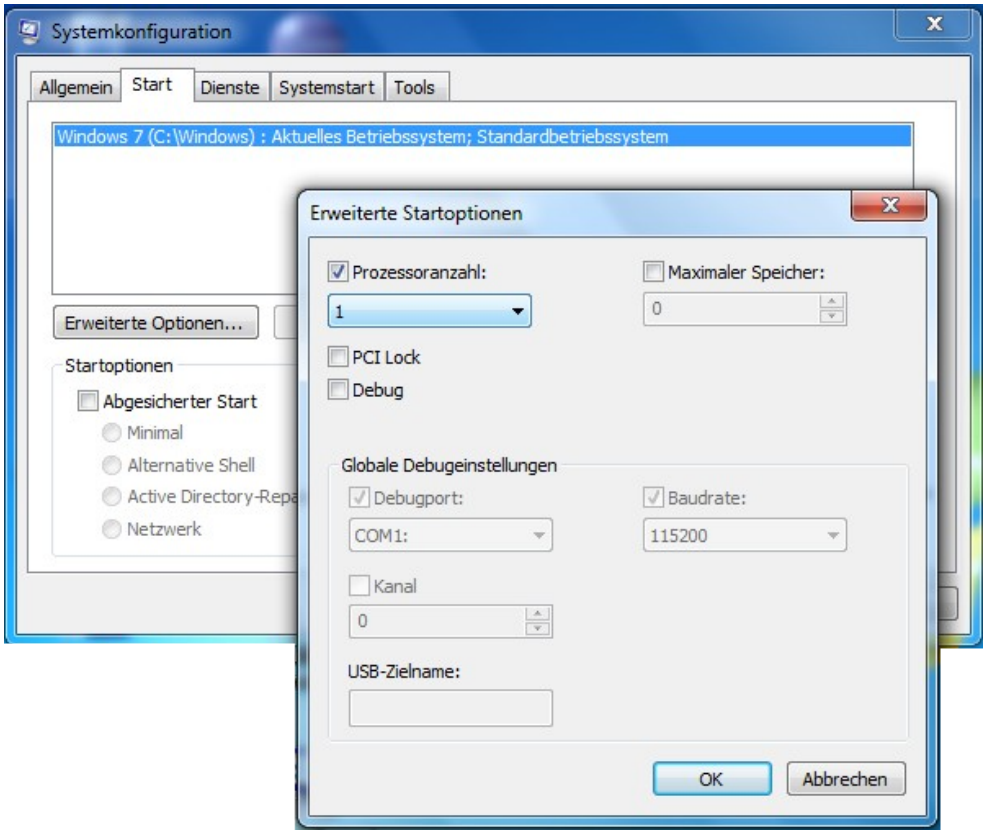


Abbildung 3: Bildschirmfoto der Systemkonfiguration zum Umschalten auf SingleCore unter Windows

3.2.2 Linux

Wenn unter Linux ein SMP-fähiger Kernel installiert ist, stehen hier ebenfalls standardmäßig sämtliche verfügbaren CPUs zur Verfügung. Um die Anzahl der Kerne zu reduzieren, muss der Kernel-Konfigurationszeile (in der Regel in der Bootloader-Konfiguration „grub.cfg“ oder „menu.lst“ in der Zeile „kernel“) folgender Parameter hinzugefügt werden:

für SingleCore: `kernel= … nosmp maxcpus=1`

für DualCore: `kernel= … maxcpus=2`

3.3 Umschalten zwischen verschiedenen Taktfrequenzen und Energieprofilen

3.3.1 Windows

Unter Windows besteht die Möglichkeit, über verschiedene Energieprofile die Taktfrequenzen und die Leistung von Windows zu regulieren. In den folgenden Untersuchungen kommen zwei Profile zum Einsatz:

- Energiesparmodus
- Höchstleistungsmodus

Zum Einstellen des jeweiligen Modus muss wie folgt vorgegangen werden:

Start → Systemsteuerung → System und Wartung → Energieoptionen

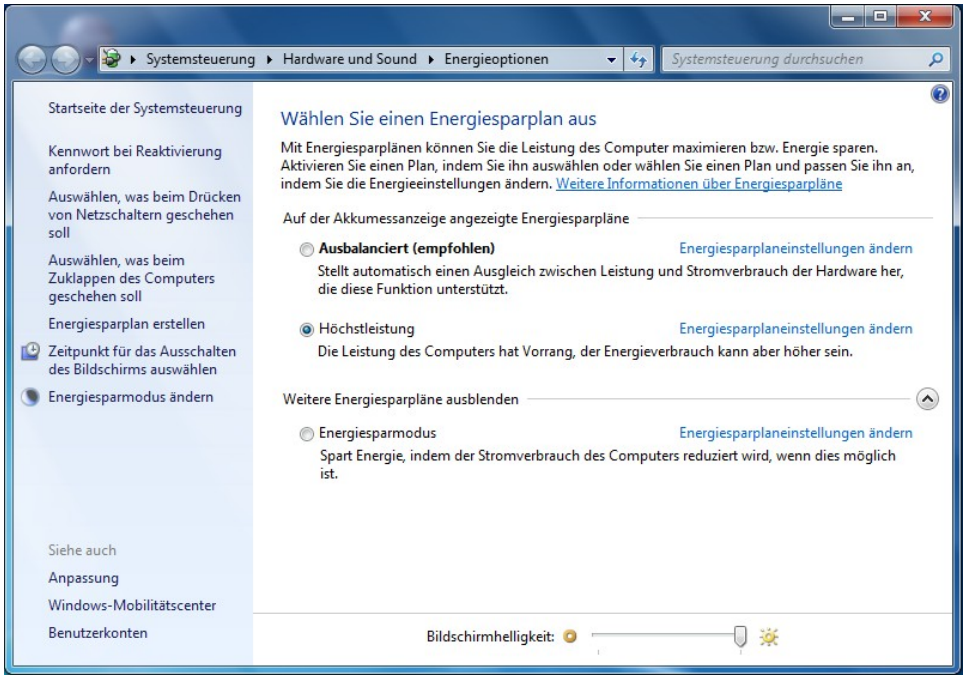


Abbildung 4: Bildschirmfoto der Windows Energieoptionen

3.3.2 Linux

Unter Linux wird die CPU-Geschwindigkeit über sogenannte „Governor“ reguliert. Hier stehen in der Regel die folgenden zur Verfügung:

- conservative
- ondemand
- userspace
- powersave
- performance

Für die folgenden Untersuchungen sind nur die folgenden beiden Governor von Interesse, da sie die minimale und maximale Taktfrequenz auswählen:

- powersave
- performance

Um den entsprechenden Governor einzustellen, kann man dazu entweder über die KDE-Energieverwaltung den Modus „*Aggressive Powersave*“ bzw. „*Performance*“ auswählen, oder manuell in einem Terminal über:

- powersave

```
echo   powersave   >   /sys/devices/system/cpu/cpu0/cpufreq/scaling_governor
echo   powersave   >   /sys/devices/system/cpu/cpu1/cpufreq/scaling_governor
echo   powersave   >   /sys/devices/system/cpu/cpu2/cpufreq/scaling_governor
echo   powersave   >   /sys/devices/system/cpu/cpu3/cpufreq/scaling_governor
```

- performance

```
echo   performance   >   /sys/devices/system/cpu/cpu0/cpufreq/scaling_governor
echo   performance   >   /sys/devices/system/cpu/cpu1/cpufreq/scaling_governor
echo   performance   >   /sys/devices/system/cpu/cpu2/cpufreq/scaling_governor
echo   performance   >   /sys/devices/system/cpu/cpu3/cpufreq/scaling_governor
```

3.4 AES-Hardwarebeschleunigung bei Intel Core-i7 CPUs

3.4.1 Windows

Unter Windows stellt man die Verwendung von der *AES-NI*-Beschleunigung neuerer Intel Core-i7 CPUs direkt in TrueCrypt ein. Hierzu setzt oder löscht man den Haken bei:

- TrueCrypt starten → Settings → Performance → „Accelerate AES encryption/decryption by using the AES instructions of the processor“

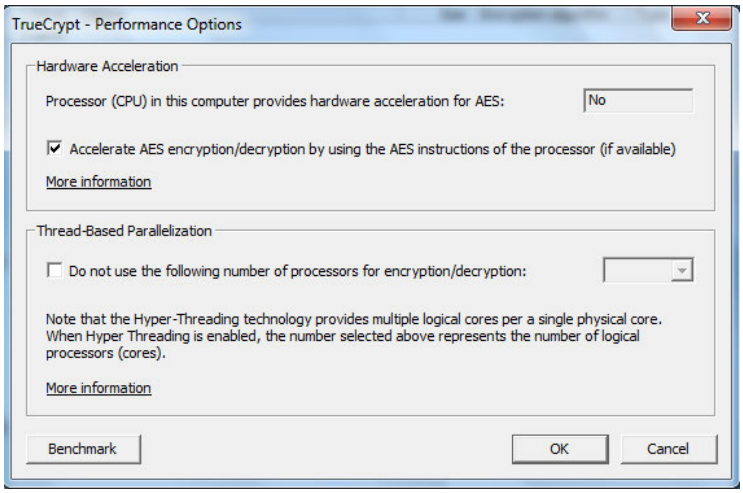


Abbildung 5: Bildschirmfoto von TrueCrypt unter Windows zum Aktivieren der AES-NI Beschleunigung

3.4.2 Linux

Unter Linux bestehen grundsätzlich zwei Möglichkeiten, Kryptooperationen auszuführen. Zum einen kann man die TrueCrypt-internen Implementierungen verwenden, für die TrueCrypt auch Unterstützung für die AES-Beschleunigung in neueren Intel-Prozessoren mitbringt. Um diese auszuwählen, geht man wie folgt vor:

- Kernel-Kryptographie abschalten, Haken setzen bei:
  - TrueCrypt starten → Settings → Preferences → System Integration → „Do not use kernel cryptographic services“

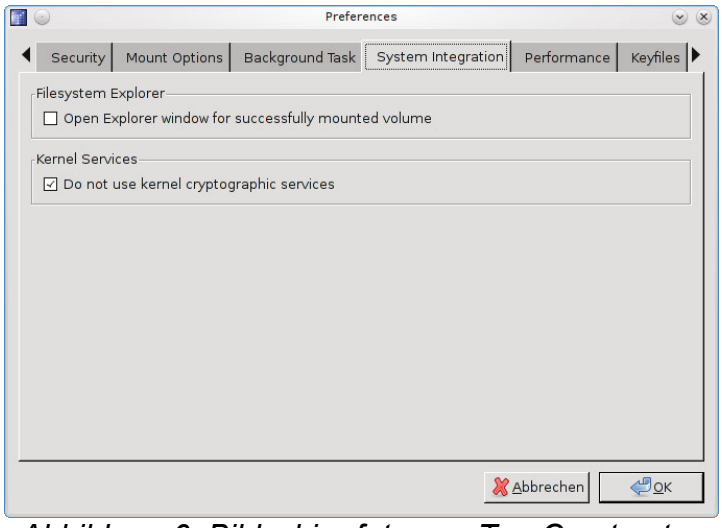


Abbildung 6: Bildschirmfoto von TrueCrypt unter Linux zum Abschalten der Linux-Krypto

- AES-NI einschalten, Haken entfernen bei:
  - TrueCrypt starten → Settings → Preferences → Performance → „Do not accelerate AES encryption/decryption by using the AES instructions of the processor“

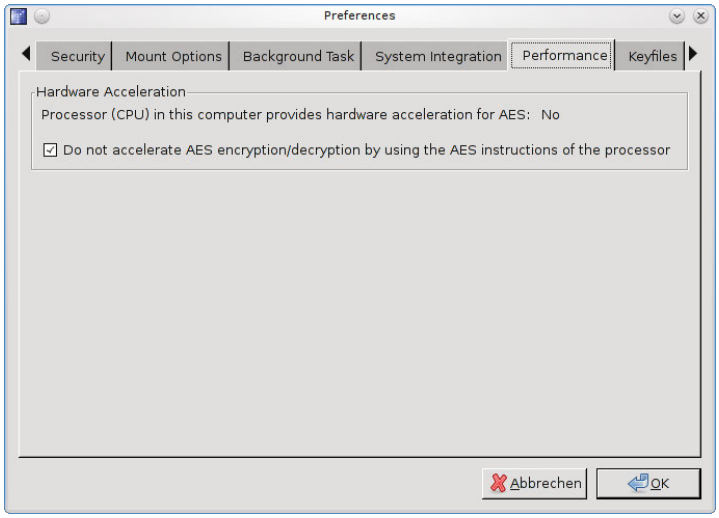


Abbildung 7: Bildschirmfoto von TrueCrypt unter Linux zum Aktivieren der AES-NI Beschleunigung

Möchte man nicht die TrueCrypt-interne Kryptoimplementierung verwenden, sondern auf die von Linux mitgebrachten und meist optimierten Implementierungen zurückgreifen, müssen die entsprechenden Kernelmodule geladen sein. Ein

- `# cat /proc/crypto`

zeigt die bereits im Linuxkern verfügbaren Algorithmen an.

Um nun die AES-NI Beschleunigung zu aktivieren, lädt man das folgende Modul:

- `# modprobe aesni_intel`

Um die Verwendung zu unterbinden, entfernt man es aus dem Kernel:

- `# rmmod aesni_intel`

3.5 Löschen von Caches (nur Linux)

Unter Linux besteht ab Kernel Version 2.6.16 die Möglichkeit, den Cache sowie nicht mehr verwendeten Speicher zu löschen. Dies ist für die folgenden Tests von Interesse, da ggf. noch im Cache befindliche Daten das Timing-Verhalten (z.B. beim Entpacken von Archiven) verändert. Um von der bereitgestellten Möglichkeit Gebrauch zu machen, stellt der Kernel im `proc`-Dateisystem – konkret: `/proc/sys/vm/drop_caches` - ein Interface zur Verfügung, in welches man eine der folgenden Nummern schreiben kann:

- Um Seitenspeicher (*page cache*) zu löschen:

  ```
  # echo 1 > /proc/sys/vm/drop_caches
  ```

- Um D-Einträge und inodes zu löschen:

  ```
  # echo 2 > /proc/sys/vm/drop_caches
  ```

- Um Seitenspeicher, D-Einträge und inodes zu löschen (also 1+2):

  ```
  # echo 3 > /proc/sys/vm/drop_caches
  ```

Die obigen Aktionen sind alle nicht-destruktiv und löschen lediglich nicht-verwendete Objekte aus dem Speicher und den Cache-Tabellen.

4 Testergebnisse (Kurzzusammenfassung) und Analyse

4.1 Speicherbedarf von TrueCrypt

TrueCrypt benötigt den folgenden Speicherplatz auf Festplatte:

	Linux	Windows
Anwendung nur Konsole	2,1 MB	n/a
Anwendung mit GUI	4,5 – 4,7 MB	6,5 MB
Gemeinsame Bibliotheken	16 MB	20,9 MB
Gesamt	**18,1 – 20,7 MB**	**27,4 MB**

TrueCrypt benötigt zur Laufzeit wie folgt Arbeitsspeicher:

	Linux
Anwendung (GUI)	4,9 MB – 5,8 MB
Gemeinsame Bibliotheken	14,4 MB- 15,6 MB
Zzgl. je Volume	4,1 MB
Gesamt (bei 1 Volume)	**ca. 25,5 MB**
Gesamt (z.B. bei 3 Volumes)	**ca. 32,7 MB**

	Windows
Hintergrundprozess	5 MB
Anwendung (GUI)	2 MB
Ab Einhängen von Volume	13 MB
Gesamt (bei 1 Volume)	**ca. 20 MB**
Gesamt (z.B. bei 8 Volumes)	**ca. 20 MB**

4.1.1 Analyse

Der Speicherplatzbedarf von TrueCrypt ist unter Linux abhängig von der eingesetzten Variante (z.B. reine Konsolenanwendung 2 MB vs. GUI 4 MB). Da die Anwendungen dynamisch gelinkt sind, kommen noch ca. 16 MB an gemeinsamen Bibliotheken hinzu. Unter Windows ist der Speicherplatzbedarf leicht höher, die reine Anwendung benötigt 6 MB Festplattenspeicher zzgl. 20 MB an gemeinsamen Bibliotheken.
Auf heutigen Systemen sind in der Regel große Festplatten (in der Größenordnung Gigabyte bis Terabyte) verbaut, sodass der Speicherplatz keine nennenswerte Rolle spielt. Anders stellt sich dies dar, wenn man TrueCrypt z.B. unter Linux in einer Initrd einsetzen möchte, da die Größe und damit der RAM-Verbrauch durch den Einsatz

von dynamischen Bibliotheken signifikant steigt. Hier empfiehlt sich daher, TrueCrypt manuell statisch zu kompilieren und ggf. Abhängigkeiten zu der GUI zu entfernen.

Hinsichtlich der Arbeitsspeicherverwendung zur Laufzeit benötigt TrueCrypt unter Linux bei einem Volume 25 MB. Für jedes weitere Volume kommen hier ca. 4 MB hinzu.
Unter Windows liegt der Arbeitsspeicherbedarf konstant bei ca. 20 MB, er erhöht sich auch nicht durch das Hinzufügen von weiteren Volumes.

4.2 TrueCrypt-interner Benchmark

Die folgende Tabelle zeigt die Ergebnisse des TrueCrypt-internen Benchmarks für den AES-Verschlüsselungsalgorithmus. Betrachtet wurden hier jeweils die Betriebssysteme Windows und Linux, sowohl im Höchstleistungsmodus als auch im Stromsparmodus. Darüberhinaus wurde bei MultiCore-CPUs auch der SingleCore-Fall betrachtet.

	Windows		**Linux**	
	Höchsteistungs-modus	*Energie-sparmodus*	*Performance*	*Powersave*
Acer Aspire One				
DualCore	27,1 MB/s	26,9 MB/s	26 MB/s	15 MB/s
SingleCore	14,8 MB/s	14,5 MB/s	15 MB/s	9 MB/s
Lenovo X61s				
DualCore	113 MB/s	47,6 MB/s	114 MB/s	52 MB/s
SingleCore	64,9 MB/s	58,9 MB/s	-	-
HP EliteBook 8540p				
QuadCore 64-Bit				
mit AESNI	1,3 GB/s	923 MB/s	1,5 GB/s	638 MB/s
ohne AESNI	234 MB/s	246 MB/s	242 MB/s	103 MB/s
SingleCore 64-Bit				
mit AESNI	467 MB/s	458 MB/s	563 MB/s	586 MB/s
ohne AESNI	105 MB/s	105 MB/s	117 MB/s	119 MB/s
QuadCore 32-Bit				
mit AESNI	-	-	995 MB/s	455 MB/s
ohne AESNI	-	-	200 MB/s	84 MB/s
xPC Shuttle				
DualCore	-	-	245 MB/s	125 MB/s
SingleCore	-	-	-	-

Tabelle 4: TrueCrypt-interner Benchmark - Vergleich der unterschiedlichen Plattformen, Betriebssysteme und Modi

4.2.1 Analyse

Die Benchmark-Ergebnisse zeigen, dass der Datendurchsatz bei Computern mit modernen CPUs (wie bei HP EliteBook oder xPC Shuttle) groß genug ist, um eine Festplattenverschlüsselung einzusetzen, da hier jeweils der Datendurchsatz über dem der jeweiligen Festplatte liegt, sodass kaum Performanceeinbußen vor allem beim Einsatz einer Full-Disc-Encryption zu erwarten sind. Auf der anderen Seite zeigt sich aber auch, dass bei langsamen Systemen wie Netbooks (Acer Aspire One) der Einsatz von Verschlüsselung das System extrem ausbremsen kann, vor allem wenn das System batterieschonend betrieben wird.

Acer Aspire One	65 MB/s
Lenovo X61s	65 MB/s
HP EliteBook 8540p	95 MB/s
xPC Shuttle	110 MB/s

Tabelle 5: Festplattendurchsatz der Plattformen

4.3 Unverschlüsselter Speicherdurchsatz

In diesem Abschnitt werden die Messungen des Speicherdurchsatzes dargestellt. Somit lässt sich der Verlust durch den Einsatz von Verschlüsselung besser vergleichen.

4.3.1 Linux

	Linux: 512 Byte Blöcke		Linux: 4096 Byte Blöcke	
	Performance	*Powersave*	*Performance*	*Powersave*
Acer Aspire One				
DualCore	98,90 MB/s	59,70 MB/s	317,00 MB/s	207,00 MB/s
SingleCore	87,70 MB/s	60,00 MB/s	314,00 MB/s	208,00 MB/s
Lenovo X61s				
DualCore	326,00 MB/s	159,00 MB/s	864,00 MB/s	443,00 MB/s
HP EliteBook 8540p				
QuadCore 64-Bit	760,00 MB/s	317,00 MB/s	1843,20 MB/s	886,00 MB/s
SingleCore 64-Bit	740,00 MB/s	717,00 MB/s	1638,40 MB/s	1843,20 MB/s
QuadCore 32-Bit	569,00 MB/s	241,00 MB/s	1638,40 MB/s	780,00 MB/s
SingleCore 32-Bit	569,00 MB/s	593,00 MB/s	1228,80 MB/s	1126,40 MB/s
xPC Shuttle				
DualCore	450,00 MB/s	287,00 MB/s	1331,20 MB/s	792,00 MB/s

Tabelle 6: Speicherdurchsatz unter Linux (RAMDisk)

4.3.2 Windows

	Windows: 512k Blöcke	
	Höchstleis-tungsmodus	*Energiespar-modus*
Acer Aspire One		
DualCore	700,00 MB/s	700,00 MB/s
SingleCore	720,00 MB/s	750,00 MB/s
Lenovo X61s		
DualCore	1331,20 MB/s	700,00 MB/s
SingleCore	1331,20 MB/s	1331,20 MB/s
HP EliteBook 8540p		
QuadCore 64-Bit	2764,80 MB/s	2560,00 MB/s
SingleCore 64-Bit	2969,60 MB/s	2969,60 MB/s

Tabelle 7: Speicherdurchsatz unter Windows (RAMDisk)

4.3.3 Analyse

Dieser Abschnitt ist rein informativ und wird nicht analysiert.

4.4 Speicherdurchsatz einer verschlüsselten Ramdisk

4.4.1 Linux

Die folgenden beiden Abschnitte zeigen den Durchsatz auf einer verschlüsselten Ramdisk. Hierbei werden sowohl die interne Krypto-Implementierung in Linux als auch die TrueCrypt-Implementierung gemessen. Im Anschluss werden diese Werte mit dem regulären Speicherdurchsatz aus Kapitel 4.3 verglichen und der Performanceverlust ausgewertet.

Krypto-API von Linux

	Linux: 512 Byte Blöcke		Linux: 4096 Byte Blöcke	
	Performance	*Powersave*	*Performance*	*Powersave*
Acer Aspire One				
DualCore	9,80 MB/s	6,00 MB/s	24,00 MB/s	14,60 MB/s
SingleCore	10,10 MB/s	6,00 MB/s	20,00 MB/s	13,30 MB/s
Lenovo X61s				
DualCore	24,90 MB/s	13,80 MB/s	77,30 MB/s	11,60 MB/s
HP EliteBook 8540p				
QuadCore 64-Bit	56,40 MB/s	22,90 MB/s	148,00 MB/s	58,60 MB/s
SingleCore 64-Bit	59,30 MB/s	58,70 MB/s	127,00 MB/s	127,00 MB/s
QuadCore 32-Bit	51,20 MB/s	19,70 MB/s	127,00 MB/s	48,10 MB/s
SingleCore 32-Bit	52,40 MB/s	52,40 MB/s	110,00 MB/s	110,00 MB/s
xPC Shuttle				
DualCore	49,60 MB/s	27,00 MB/s	117,00 MB/s	69,20 MB/s

Tabelle 8: Krypto-Durchsatz unter Linux mit Linux-Krypto

	Linux: 512 Byte Blöcke		Linux: 4096 Byte Blöcke	
	Performance	*Powersave*	*Performance*	*Powersave*
Acer Aspire One				
DualCore	90,09%	89,95%	92,43%	92,95%
SingleCore	88,48%	90,00%	93,63%	93,61%
Lenovo X61s				
DualCore	92,36%	91,32%	91,05%	97,38%
HP EliteBook 8540p				
QuadCore 64-Bit	92,58%	92,78%	91,97%	93,39%
SingleCore 64-Bit	91,99%	91,81%	92,25%	93,11%
QuadCore 32-Bit	91,00%	91,83%	92,25%	93,83%
SingleCore 32-Bit	90,79%	91,16%	91,05%	90,23%
xPC Shuttle				
DualCore	88,98%	90,59%	91,21%	91,26%

Tabelle 9: Verluste durch den Einsatz der Linux-Krypto

interne Krypto-API von TrueCrypt

	Linux: 512 Byte Blöcke		Linux: 4096 Byte Blöcke	
	Performance	*Powersave*	*Performance*	*Powersave*
Acer Aspire One				
DualCore	8,20 MB/s	4,90 MB/s	19,00 MB/s	11,30 MB/s
SingleCore	8,20 MB/s	4,90 MB/s	17,70 MB/s	11,30 MB/s
Lenovo X61s				
DualCore	18,30 MB/s	11,60 MB/s	62,20 MB/s	32,10 MB/s
HP EliteBook 8540p				
QuadCore 64-Bit	46,00 MB/s	18,20 MB/s	115,00 MB/s	45,10 MB/s
SingleCore 64-Bit	48,90 MB/s	49,10 MB/s	103,00 MB/s	103,00 MB/s
QuadCore 32-Bit	42,40 MB/s	15,90 MB/s	99,70 MB/s	39,30 MB/s
SingleCore 32-Bit	42,80 MB/s	42,80 MB/s	88,60 MB/s	88,60 MB/s
xPC Shuttle				
DualCore	40,80 MB/s	23,40 MB/s	103,00 MB/s	57,20 MB/s

Tabelle 10: Krypto-Durchsatz mit TrueCrypt unter Linux

	Linux: 512 Byte Blöcke		Linux: 4096 Byte Blöcke	
	Performance	*Powersave*	*Performance*	*Powersave*
Acer Aspire One				
DualCore	91,71%	91,79%	94,01%	94,54%
SingleCore	90,65%	91,83%	94,36%	94,57%
Lenovo X61s				
DualCore	94,39%	92,70%	92,80%	92,75%
HP EliteBook 8540p				
QuadCore 64-Bit	93,95%	94,26%	93,76%	94,91%
SingleCore 64-Bit	93,39%	93,15%	93,71%	94,41%
QuadCore 32-Bit	92,55%	93,40%	93,91%	94,96%
SingleCore 32-Bit	92,48%	92,78%	92,79%	92,13%
xPC Shuttle				
DualCore	90,93%	91,85%	92,26%	92,78%

Tabelle 11: Verluste durch den Einsatz von TrueCrypt unter Linux

4.4.2 Windows

	Windows: 512k Blöcke	
	Höchstleis-tungsmodus	*Energiespar-modus*
Acer Aspire One		
DualCore	25,00 MB/s	25,00 MB/s
SingleCore	15,00 MB/s	15,00 MB/s
Lenovo X61s		
DualCore	110,00 MB/s	55,00 MB/s
SingleCore	70,00 MB/s	70,00 MB/s
HP EliteBook 8540p		
QuadCore 64-Bit	235,00 MB/s	235,00 MB/s
SingleCore 64-Bit	115,00 MB/s	115,00 MB/s

Tabelle 12: Krypto-Durchsatz mit TrueCrypt unter Windows

	Windows: 512k Blöcke	
	Höchstleis-tungsmodus	*Energiespar-modus*
Acer Aspire One		
DualCore	96,43%	96,43%
SingleCore	97,92%	98,00%
Lenovo X61s		
DualCore	91,74%	92,14%
SingleCore	94,74%	94,74%
HP EliteBook 8540p		
QuadCore 64-Bit	91,50%	90,82%
SingleCore 64-Bit	96,13%	96,13%

Tabelle 13: Verluste durch den Einsatz von TrueCrypt unter Windows

4.4.3 Analyse

Es zeigt sich, dass mit dem Einsatz von Verschlüsselung und dem damit einhergehenden Verlust von DMA (da alle Daten durch die CPU verarbeitet werden müssen) ein erheblicher Performanceverlust in Höhe von >90% bei reinem sequentiellen Speicherzugriff einhergeht. Dies gilt für beide Betriebssysteme Windows und Linux in allen Variationen. Solange die effektive Geschwindigkeit durch den Einsatz von Verschlüsselung dennoch höher ist als die Geschwindigkeit der verwendeten Festplatte, ist der Einsatz einer Verschlüsselung ohne merkbare Verluste für den Benutzer möglich. Sobald allerdings die Datenrate unter die mögliche Festplattenleistung sinkt, ist der Einsatz von Verschlüsselung merkbar.

4.5 Zugriffszeiten beim Entpacken von Dateien

4.5.1 Linux

Performance-Modus unter Linux

	Plain EXT3	TrueCrypt EXT3	Plain REISERFS	TrueCrypt REISERFS	Plain VFAT	TrueCrypt VFAT	Plain XFS	TrueCrypt XFS
Acer Aspire One								
DualCore	6,07	11,9	5,21	9,23	5,12	10,4	4,66	9,67
Lenovo X61s								
DualCore	4,09	6,36	3,99	10,44	4,65	6,45	3,27	10
HP EliteBook 8540p								
QuadCore 64-Bit	1,87	2,18	1,84	2,19	1,84	2,12	1,73	2,03
QuadCore 32-Bit	1,66	2,7	1,71	2,53	1,59	2,67	1,67	2,7
xPC Shuttle								
DualCore 64-Bit	2,12	3,3	1,95	2,95	1,91	2,71	1,76	2,61

(Zeiten in Sekunden)

Tabelle 14: Auspacken eines Archivs unter Linux

4.5.2 Analyse

Vergleicht man die Zeit, die zum Entpacken eines großen Archivs mit vielen kleinen Dateien benötigt wird, so stellt man fest, dass etwa 70-100% mehr Zeit aufgewandt werden muss (siehe Tabelle 14). Je nach Plattform ist dies unwesentlich, z.B. ist es für den Benutzer des HP EliteBook in der Regel egal, ob er 1,6 oder 2,7 Sekunden warten muss. Auf langsameren Systemen hingegen (z.B. Lenovo x61s) ist der Unterschied durchaus merkbar, z.B. 3,99 Sekunden versus 10,44 Sekunden.

4.5.3 Windows

	Höchstleistungsm.			Energiesparm.		
	Plain FAT32	*TrueCrypt FAT32*	*TrueCrypt NTFS*	*Plain FAT32*	*TrueCrypt FAT32*	*TrueCrypt NTFS*
Acer Aspire One						
DualCore	150	150	150	200	180	180
SingleCore	150	215	215	200	215	215
Lenovo X61s						
DualCore	50	55	45	95	90	85
SingleCore	70	75	65	85	80	70
HP EliteBook 8540p						
QuadCore 64-Bit	12	25	26	21	59	63
SingleCore 64-Bit	31	28	29	30	28	30

(Zeiten in Sekunden)

Tabelle 15: Auspacken eines Archivs unter Windows

4.5.4 Analyse

Erstaunlicherweise scheint es hier einen signifikanten Flaschenhals in dem von Haus aus mitgelieferten Entpackprogramm zu geben. Die Entpackdauer ist – verglichen mit Linux – viel langsamer. Die Geschwindigkeitsprobleme überwiegen dabei so stark, dass der Einsatz von Verschlüsselung nahezu unbemerkt bleibt. Einzige Ausnahme stellt hier die QuadCore-Variante des HP EliteBook dar. Diese Abweichung kann ggf. mit dem Overhead durch das Management der einzelnen Threads erklärt werden

4.6 Kompilieren von Quelltext

Ein interessanter Anwendungsfall ist das Kompilieren von Quelltext. Um die Geschwindigkeitsunterschiede festzustellen, wurde in diesem Test der Linuxkernel kompiliert und die benötigte Zeit gemessen. Das Kompilieren erfolgte unter Linux im *performance*-Modus, sowohl nativ auf der Festplatte als auch in einem mit TrueCrypt verschlüsselten Container, jeweils mit ext3-Dateisystem.

Folgende Ergebnisse wurden dabei gemessen:

	Lenovo x61s		**HP EliteBook 8540p**	
	nativ	*TrueCrypt Container*	*nativ*	*TrueCrypt Container*
Entpacken des Linuxkerns: `tar -xjf linux-2.6.34.tar.bz2`	30s	65s	19s	115s

Kompilieren mit MAKEOPTS:
`make allnoconfig`
`make -j3 / make -j5`
	123s	128s	48s	64s

(Zeit in Sekunden)				

Tabelle 16: Zeiten bei Kompilieren von Quelltext

4.6.1 Analyse

Die Messungen zeigen, dass sich der Einsatz der Verschlüsselung hier ebenfalls, wie bereits in Kapitel 4.5.1 gesehen, negativ auf die Entpackzeit (von ca. 34000 Dateien) auswirken. Erstaunlicherweise ist der Kompiliervorgang durch den Einsatz des TrueCrypt-Containers auf beiden Plattformen nicht bedeutend langsamer geworden.

4.7 Full-Disc-Encryption Tests (nur Windows)

Ohne FDE					Mit FDE				
Starten von Windows	Herunterfahren von Windows	Starten von Firefox	Starten von OpenOffice	Starten von Eclipse	Starten von Windows	Herunterfahren von Windows	Starten von Firefox	Starten von OpenOffice	Starten von Eclipse
Acer Aspire One – DualCore									
40	15	14	8	30	30	18	10	11	40
Lenovo X61s – DualCore									
25	20	8	8	22	30	20	8	8	50
HP EliteBook 8540p – QuadCore									
25	10	4	5	22	25	11	7	8	30

(Zeiten in Sekunden)

Tabelle 17: System- und Programmstartzeiten unter Windows

4.7.1 Analyse

Im Rahmen dieser Tests wurden gängige Benutzeraktionen sowohl mit als auch ohne Full-Disc-Encryption durchgeführt. Hierbei zeigt sich, dass z.B. das Hoch- und Herunterfahren von Windows nahezu unabhängig von dem Einsatz einer Verschlüsselung sind.

Anders sieht es beim Starten von Anwendungen im Benutzerkontext aus. Hier wird beim Einsatz von FDE etwas mehr Zeit zum Starten der Anwendungen benötigt als ohne FDE, der konkrete Verlust hängt anscheinend mit der Anzahl der zu öffnenden Dateien zusammen. Der zeitliche Mehraufwand wurde in der Größenordnung von 30-50% gemessen.

4.8 Dateisystem-Benchmarks (nur Linux)

Name:	Acer Aspire One		Lenovo X61s		HP EliteBook 8540p 64		xPC Shuttle	
Bit:	32-Bit		64-Bit		64-Bit		64-Bit	
Blockgröße:	plain	True-Crypt	plain	True-Crypt	plain	True-Crypt	plain	True-Crypt
	EXT3							
512	60,41	12,91	110,92	36,44	272,25	135,12	150,17	56,31
4096	62,21	13,22	113,51	39,83	253,06	134,19	145,11	58,62
16386	64,11	12,76	111,23	41,27	247,24	137,35	172,50	58,51
	REISERFS							
512	62,52	13,60	158,47	44,80	45,72	47,05	50,01	49,99
4096	97,62	16,60	214,89	48,69	403,48	123,23	201,42	80,14
16386	108,74	16,75	218,12	52,78	453,71	152,18	325,10	80,31
	VFAT							
512	155,86	18,20	302,82	58,08	709,28	225,62	456,74	101,57
4096	165,64	18,54	285,01	59,78	612,77	227,48	450,11	101,65
16386	175,35	18,64	277,56	55,59	616,71	230,55	415,54	100,59
	XFS							
512	142,22	17,57	370,06	59,52	879,32	241,99	474,10	96,27
4096	162,09	17,33	351,38	60,91	710,07	217,27	511,03	100,94
16386	196,00	18,28	338,19	61,72	693,17	246,27	504,70	94,38
(Angaben in MB/s pro 16k-Datei)								

Tabelle 18: Dateisystem-Benchmarks unter Linux

4.8.1 Analyse

Tabelle 18 zeigt eine Benchmark-Übersicht über verschiedene Plattformen, Blockgrößen und Dateisysteme. Diese Werte sind insofern interessant, da sie nicht die linearen Zugriffszeiten auf den Arbeitsspeicher messen, sondern auch Dateisystem-spezifische Eigenschaften, wie sie im alltäglichen Einsatz zum Tragen kommen, widerspiegelt. Es zeigt sich, dass die effektiven Verluste nicht mehr auf >90% belaufen, sondern sich auf 50-80% reduzieren. Eine exakte Analyse der Verluste ist in Kapitel 5.6.2 zu sehen.

5 Testergebnisse (ausführlich)

5.1 Speicherbedarf von TrueCrypt

In diesem Abschnitt wird der Speicherbedarf von TrueCrypt analysiert. Hierzu zählen sowohl der auf der Festplatte verwendete Speicherplatz (inkl. Abhängigkeiten) als auch der dynamische Arbeitsspeicherverbrauch – jeweils getrennt für Windows und Linux.

5.1.1 Linux

Festplattenspeicherbedarf

Die TrueCrypt-Binaries werden auf der TrueCrypt-Homepage in 2 Varianten angeboten, einmal mit grafischer Benutzeroberfläche und einmal nur für die Kommandozeile. Beide Varianten gibt es darüberhinaus in 32-Bit und 64-Bit.

- **TrueCrypt nur für die Kommandozeile:**

32-Bit

```
$ file truecrypt

ELF 32-bit LSB executable
Intel 80386
version 1 (SYSV)
dynamically linked (uses shared libs)
stripped

$ ls -l truecrypt
2113504 Bytes = 2,1 MB
```

64-Bit

```
$ file truecrypt

ELF 64-bit LSB executable
x86-64
version 1 (SYSV)
dynamically linked (uses shared libs)
stripped

$ ls -l truecrypt
2101296 Bytes = 2,1 MB
```

Beide Versionen sind dynamisch gelinkt und hängen von folgenden Bibliotheken ab:

32-Bit + 64-Bit
/lib/ld-linux.so.2
libc.so.6
libdl.so.2
libfuse.so.2
libgcc_s.so.1
libm.so.6
libpthread.so.0
librt.so.1
libstdc++.so.6
linux-gate.so.1

- **TrueCrypt mit grafischer Oberfläche:**

32-Bit

```
$ file truecrypt

ELF 32-bit LSB executable
Intel 80386
version 1 (SYSV)
dynamically linked (uses shared libs)
stripped

$ ls -l truecrypt
4717328 Bytes = 4,5 MB
```

64-Bit

```
$ file truecrypt

ELF 64-bit LSB executable
x86-64
version 1 (SYSV)
dynamically linked (uses shared libs)
stripped

$ ls -l truecrypt
4873392 Bytes = 4,7 MB
```

Diese Binaries sind ebenfalls dynamisch gelinkt und hängen neben den bereits oben erwähnten Bibliotheken von den folgenden weiteren ab, die zusammen ca. 16 MB belegen (Ausgaben von *ldd*):

32-Bit	64-Bit
/lib/ld-linux.so.2	/lib64/ld-linux-x86-64.so.2
libatk-1.0.so.0	libatk-1.0.so.0
libcairo.so.2	libcairo.so.2
libc.so.6	libc.so.6
	libdirect-1.4.so.0
	libdirectfb-1.4.so.0
libdl.so.2	libdl.so.2
	libdrm.so.2
libexpat.so.1	libexpat.so.1
libfontconfig.so.1	libfontconfig.so.1
libfreetype.so.6	libfreetype.so.6
libfuse.so.2	libfuse.so.2
	libfusion-1.4.so.0
libgcc_s.so.1	libgcc_s.so.1
libgdk_pixbuf-2.0.so.0	libgdk_pixbuf-2.0.so.0
libgdk-x11-2.0.so.0	libgdk-x11-2.0.so.0
libgio-2.0.so.0	libgio-2.0.so.0
libglib-2.0.so.0	libglib-2.0.so.0
	libglitz-glx.so.1
	libglitz.so.1
	libGL.so.1
libgmodule-2.0.so.0	libgmodule-2.0.so.0
libgobject-2.0.so.0	libgobject-2.0.so.0
libgthread-2.0.so.0	libgthread-2.0.so.0
libgtk-x11-2.0.so.0	libgtk-x11-2.0.so.0
libICE.so.6	libICE.so.6
libm.so.6	libm.so.6
libpango-1.0.so.0	libpango-1.0.so.0
libpangocairo-1.0.so.0	libpangocairo-1.0.so.0

libpangoft2-1.0.so.0	libpangoft2-1.0.so.0
libpixman-1.so.0	libpixman-1.so.0
libpng14.so.14	libpng14.so.14
libpthread.so.0	libpthread.so.0
libresolv.so.2	libresolv.so.2
librt.so.1	librt.so.1
libSM.so.6	libSM.so.6
libstdc++.so.6	libstdc++.so.6
libuuid.so.1	libuuid.so.1
libX11.so.6	libX11.so.6
	libX11-xcb.so.1
libXau.so.6	libXau.so.6
	libxcb-glx.so.0
	libxcb-render.so.0
	libxcb-render-util.so.0
libxcb.so.1	libxcb.so.1
libXcomposite.so.1	libXcomposite.so.1
libXcursor.so.1	libXcursor.so.1
libXdamage.so.1	libXdamage.so.1
libXdmcp.so.6	libXdmcp.so.6
libXext.so.6	libXext.so.6
libXfixes.so.3	libXfixes.so.3
libXinerama.so.1	libXinerama.so.1
libXi.so.6	libXi.so.6
libXrandr.so.2	libXrandr.so.2
libXrender.so.1	libXrender.so.1
	libXxf86vm.so.1
libz.so.1	libz.so.1
linux-gate.so.1	linux-vdso.so.1

Arbeitsspeicherbedarf

Startet man die Hauptanwendung von TrueCrypt mit grafischer Oberfläche, so werden unmittelbar 2 Prozesse im Kontext des Benutzers erzeugt:

Prozess	Arbeitsspeicher	Gemeinsamer Speicher
1)	4,9 MB – 5,8 MB	14,4 MB – 15,6 MB
2)	1,7 MB – 1,8 MB	0,4 MB – 1,0 MB

Bei der Aufteilung des Speicherverbrauchs gilt folgende Unterscheidung:

- **Arbeitsspeicher** ist der durch TrueCrypt selbst angeforderte Speicher.
- **Gemeinsamer Speicher** ist die Speichernutzung durch die Verwendung von gemeinsamen Bibliotheken (*shared libraries*)

Dies erklärt auch die Verwendung von zwei unterschiedlichen Prozessen: Der erste Prozess stellt die grafische Benutzeroberfläche dar und verwendet viele Funktionen aus den gemeinsamen Grafikbibliotheken.

Der zweite Prozess hingegen beinhaltet den *CoreService* von TrueCrypt. Dieser wartet auf Eingaben aus der GUI.

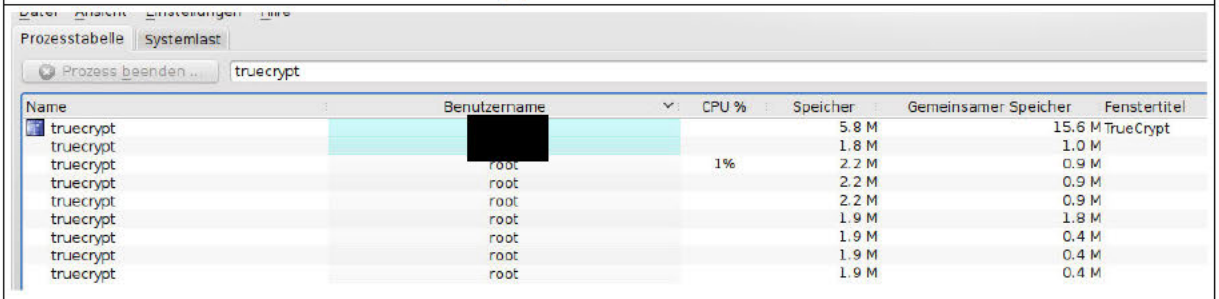
Für jedes Volume, welches mit TrueCrypt geöffnet wird, werden zwei weitere Prozesse erzeugt, welche im Hintergrund ausgeführt werden. Dies sind ebenfalls Instanzen des *CoreService* und laufen mit privilegierten *root*-Rechten.

Startet man beispielsweise die GUI und hängt einen TrueCrypt-Container ein, so werden insgesamt 4 Prozesse erzeugt::

Prozess	Arbeitsspeicher	Gemeinsamer Speicher
1)	4,9 MB – 5,8 MB	14,4 MB – 15,6 MB
2)	1,7 MB – 1,8 MB	0,4 MB – 1,0 MB
3)	2,2 MB	0,9 MB
4)	1,9 MB	0,4 MB

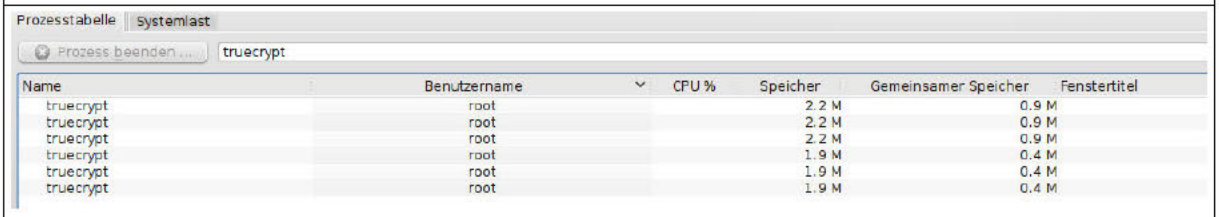
Für jedes weitere Volume, welches zusätzlich geöffnet wird, kommen jeweils weitere 2 Prozesse mit konstantem Speicherbedarf von insgesamt (2,2 MB + 1,9 MB =) 4,1 MB hinzu. Beendet man die GUI, so laufen diese Prozesse im Hintergrund weiter. Die folgenden Bilder zeigt die Prozesse bei 3 gemounteten Container mit und ohne GUI:

TrueCrypt-Prozesse mit GUI




```
~ $ ps -ef | grep truecrypt
[redacted] 19015  4155  4 10:53 pts/1    00:00:10 truecrypt
[redacted] 19016 19015  0 10:53 pts/1    00:00:00 truecrypt
root      19900     1  0 10:54 pts/1    00:00:00 /usr/local/bin/truecrypt --core-service
root      19902     1  0 10:54 ?        00:00:00 /usr/local/bin/truecrypt --core-service
root      19904     1  0 10:54 ?        00:00:01 /usr/local/bin/truecrypt --core-service
root      20850     1  0 10:56 ?        00:00:00 /usr/local/bin/truecrypt --core-service
root      20852     1  0 10:56 ?        00:00:00 /usr/local/bin/truecrypt --core-service
root      21847     1  0 10:57 ?        00:00:00 /usr/local/bin/truecrypt --core-service
root      21849     1  0 10:57 ?        00:00:00 /usr/local/bin/truecrypt --core-service
```

TrueCrypt-Prozesse ohne GUI




```
~ $ ps -ef | grep truecrypt
root      19902     1  0 10:54 ?        00:00:00 /usr/local/bin/truecrypt --core-service
root      19904     1  0 10:54 ?        00:00:01 /usr/local/bin/truecrypt --core-service
root      20850     1  0 10:56 ?        00:00:00 /usr/local/bin/truecrypt --core-service
root      20852     1  0 10:56 ?        00:00:00 /usr/local/bin/truecrypt --core-service
root      21847     1  0 10:57 ?        00:00:00 /usr/local/bin/truecrypt --core-service
root      21849     1  0 10:57 ?        00:00:00 /usr/local/bin/truecrypt --core-service
```

Die *CoreService-Prozesse* werden unabhängig von dem verwendeten Krypto-Modus erzeugt, d.h. es spielt keine Rolle, ob die Linux-interne Krypto-API verwendet wird oder die internen Implementierungen zum Einsatz kommen. Im ersten Falle werden von TrueCrypt noch die folgenden *Mappings* im Linuxkern angelegt, welche jedoch noch wenige Kilobyte Speicher im *Kernelspace* benötigen:

```
# dmsetup table
truecrypt1: 0 204288 crypt aes-xts-plain64 <key not shown> 256 7:0 256
truecrypt2: 0 204288 crypt aes-xts-plain64 <key not shown> 256 7:1 256
truecrypt3: 0 204288 crypt aes-xts-plain64 <key not shown> 256 7:2 256

# dmsetup status | grep truecrypt
truecrypt1: 0 204288 crypt
truecrypt2: 0 204288 crypt
truecrypt3: 0 204288 crypt
```

5.1.2 Windows

Festplattenspeicherbedarf

Unter Windows besteht TrueCrypt aus mehreren separaten Anwendungen und Bibliotheken:

Programm	Größe
TrueCrypt	1.462 KB
TrueCrypt Format	1.555 KB
TrueCrypt Setup	3.407 KB
truecrypt.sys	226 KB
truecrypt-x64.sys	225 KB

Darüber hinaus verwendet TrueCrypt noch die folgenden Bibliotheken von Windows:

Bibliothek	Größe
advapi32.dll	625 KB
comctl32.dll	518 KB
comdlg32.dll	475 KB
dbghelp.dll	834 KB
fmifs.dll	23 KB
gdi32.dll	297 KB
kernel32.dll	837 KB
ole32.dll	1.379 KB
oleaut32.dll	558 KB
riched20.dll	462 KB
setupapi.dll	1.629 KB
shell32.dll	12.565 KB
shlwapi.dll	342 KB
srclient.dll	42 KB
user32.dll	792 KB
version.dll	21 KB
	21.399 KB =20,9 MB

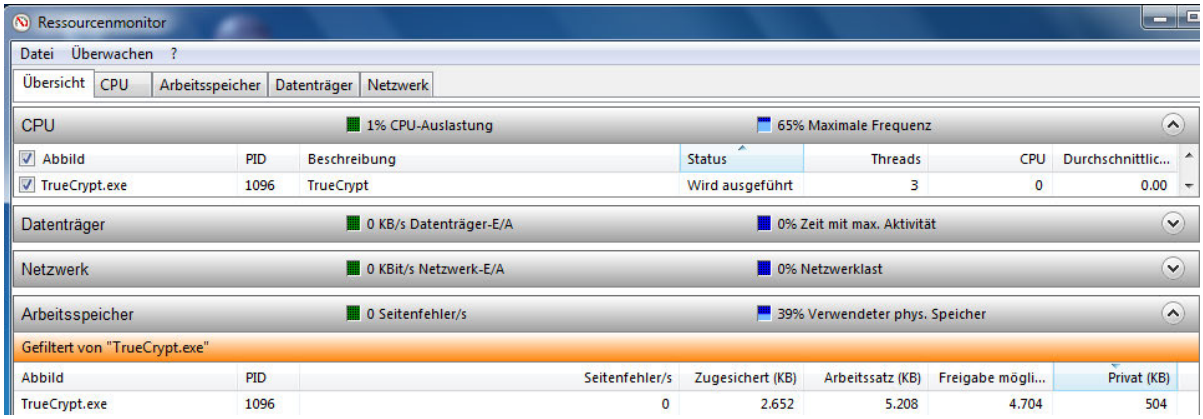
Arbeitsspeicherbedarf

Unter Windows kann mittels der Anwendung „*Ressourcenmonitor*“ die Menge des von einer Anwendung belegten Arbeitsspeicher angezeigt werden. Die Anzeige des Speichers ist hierbei wie folgt unterteilt[9]:

- **Arbeitsspeicher** (*Arbeitssatz*): Menge von Arbeitsspeicher im privaten Arbeitssatz plus der Menge von Arbeitsspeicher, die vom Prozess verwendet wird und nicht mit anderen Prozessen gemeinsam genutzt werden kann.
- **Privat** (*Privater Arbeitssatz*): Dieser technische Begriff beschreibt die Menge von Arbeitsspeicher, die von jedem einzelnen Prozess verwendet wird. Der private Arbeitssatz beschreibt speziell die Menge von Arbeitsspeicher, die von einem Prozess verwendet wird und nicht mit anderen Prozessen gemeinsam genutzt werden kann. *Privater Arbeitssatz* ist eine Teilmenge von *Arbeitssatz*.
- **Zugesicherte Größe:** Menge von virtuellem Arbeitsspeicher, die für die Verwendung durch einen Prozess reserviert ist.

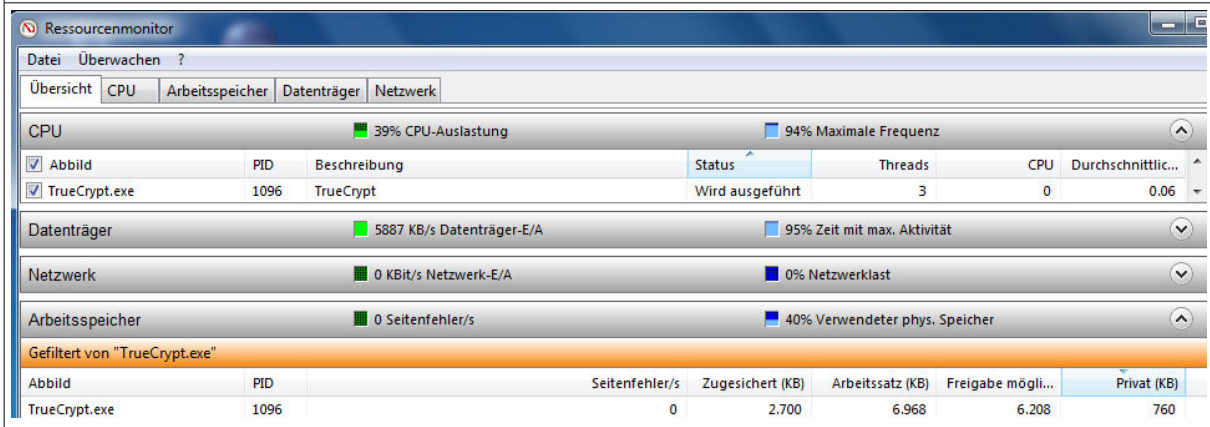
Es stellt sich heraus, dass der Hintergrundprozess von TrueCrypt 3 Prozesse erzeugt und ca. 500 KB Speicher pro Prozess benötigt, insgesamt belegt es ca. 5 MB RAM. Startet man die grafische Oberfläche, so erhöht sich die benötigte Arbeitsspeichermenge auf 7 MB. Sobald man nun ein Volume einhängt, werden von TrueCrypt ca. 20 MB Arbeitsspeicher belegt. Diese Zahl bleibt konstant und hat sich auch nach dem 8. zeitgleich geöffneten Container nicht weiter erhöht.

TrueCrypt-Hintergrundprozesse ohne GUI

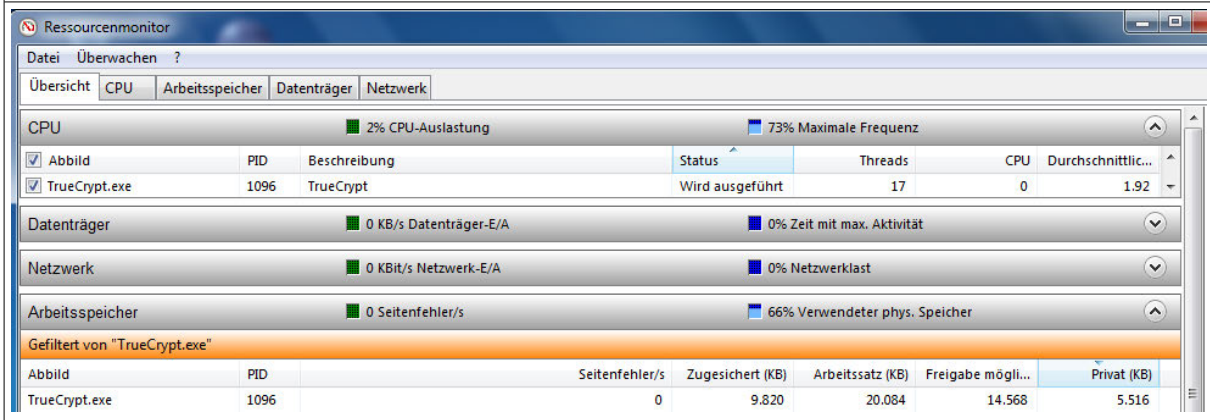


9 http://windows.microsoft.com/de-DE/windows-vista/See-details-about-your-computers-performance-using-Task-Manager

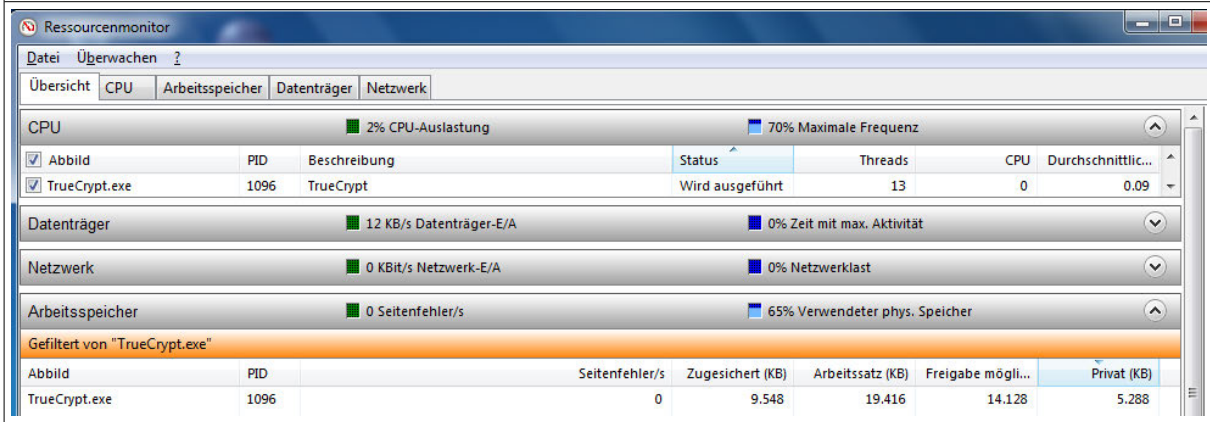
TrueCrypt mit GUI



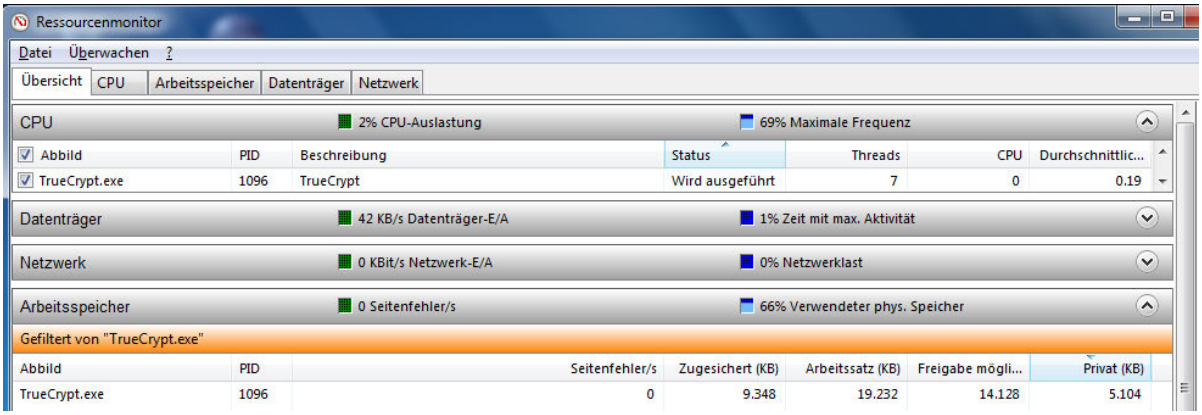
TrueCrypt mit GUI und 1 Volume



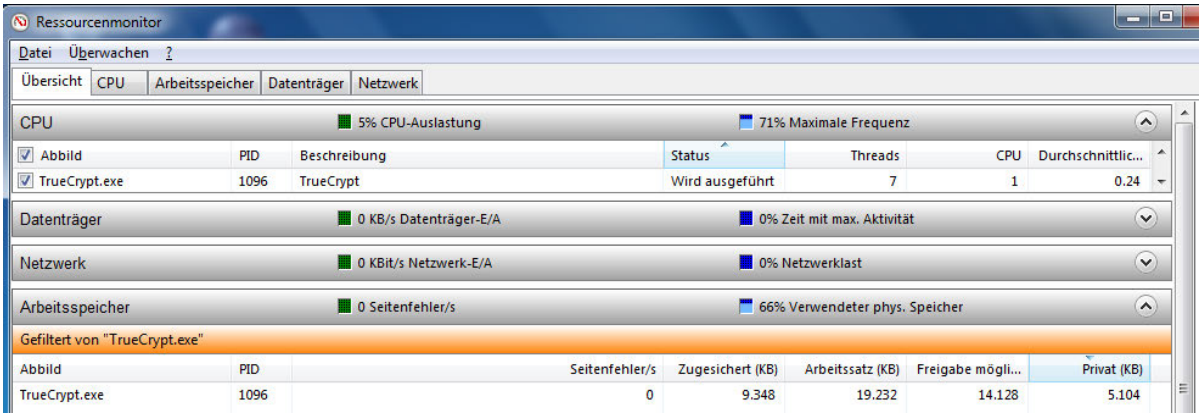
TrueCrypt mit GUI und 2 Volumes



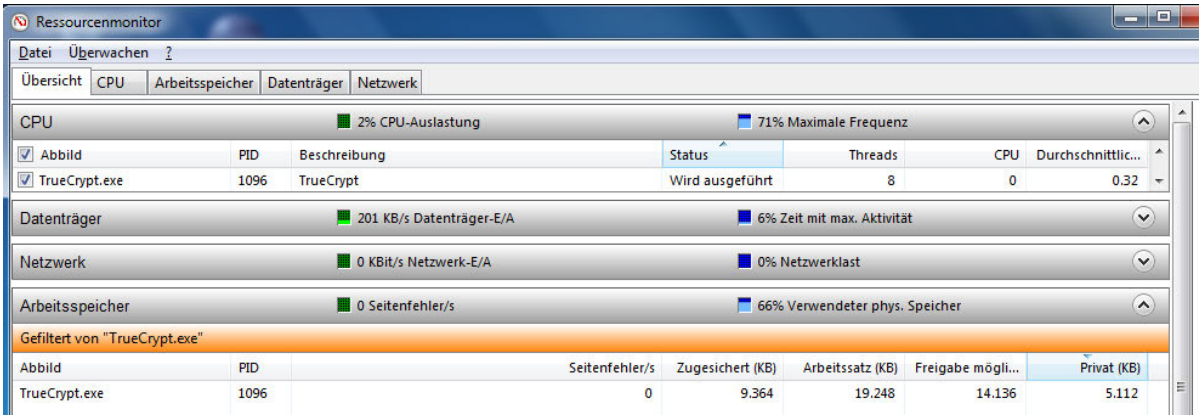
TrueCrypt mit GUI und 3 Volumes



TrueCrypt mit GUI und 4 Volumes



TrueCrypt mit GUI und 5 Volumes

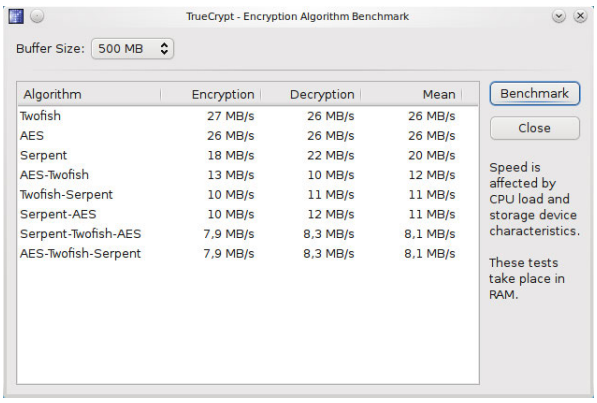


5.2 TrueCrypt-interner Benchmark

5.2.1 Acer Aspire one D250-1Bk

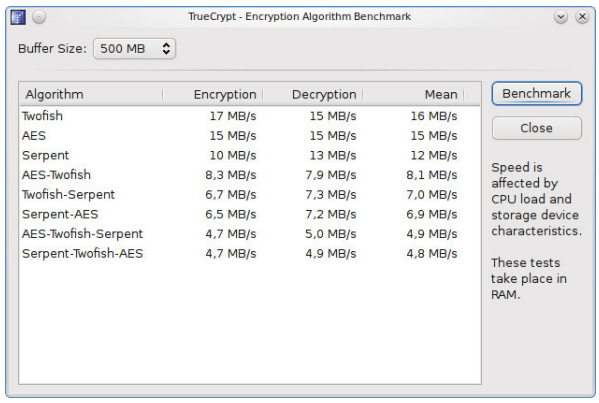
Linux DualCore 32-Bit

Performance



Algorithm	Encryption	Decryption	Mean
Twofish	27 MB/s	26 MB/s	26 MB/s
AES	26 MB/s	26 MB/s	26 MB/s
Serpent	18 MB/s	22 MB/s	20 MB/s
AES-Twofish	13 MB/s	10 MB/s	12 MB/s
Twofish-Serpent	10 MB/s	11 MB/s	11 MB/s
Serpent-AES	10 MB/s	12 MB/s	11 MB/s
Serpent-Twofish-AES	7,9 MB/s	8,3 MB/s	8,1 MB/s
AES-Twofish-Serpent	7,9 MB/s	8,3 MB/s	8,1 MB/s

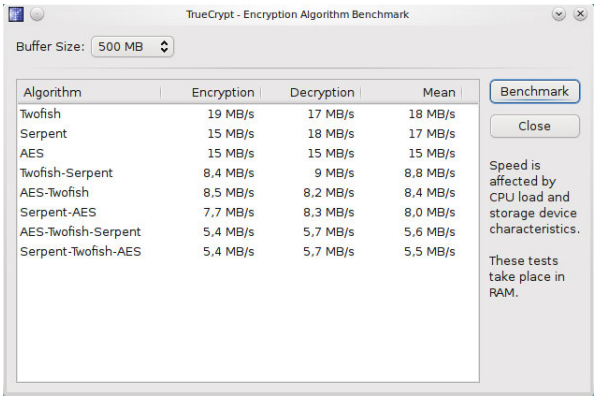
Powersave



Algorithm	Encryption	Decryption	Mean
Twofish	17 MB/s	15 MB/s	16 MB/s
AES	15 MB/s	15 MB/s	15 MB/s
Serpent	10 MB/s	13 MB/s	12 MB/s
AES-Twofish	8,3 MB/s	7,9 MB/s	8,1 MB/s
Twofish-Serpent	6,7 MB/s	7,3 MB/s	7,0 MB/s
Serpent-AES	6,5 MB/s	7,2 MB/s	6,9 MB/s
AES-Twofish-Serpent	4,7 MB/s	5,0 MB/s	4,9 MB/s
Serpent-Twofish-AES	4,7 MB/s	4,9 MB/s	4,8 MB/s

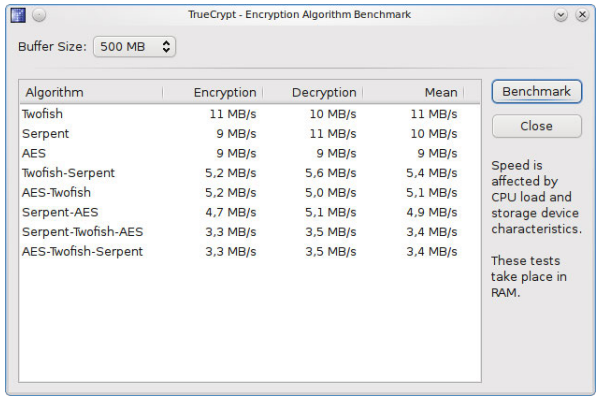
Linux SingleCore 32-Bit

Performance



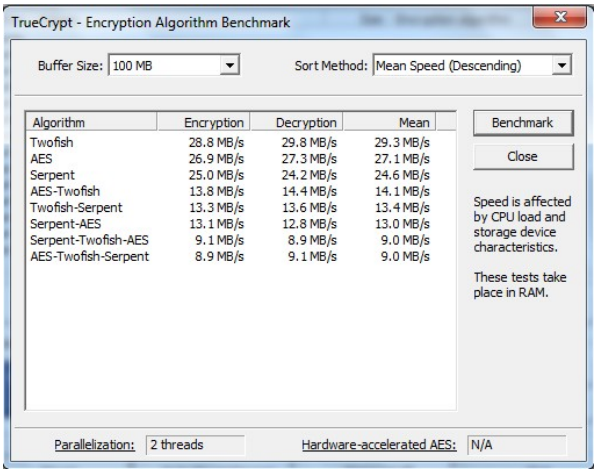
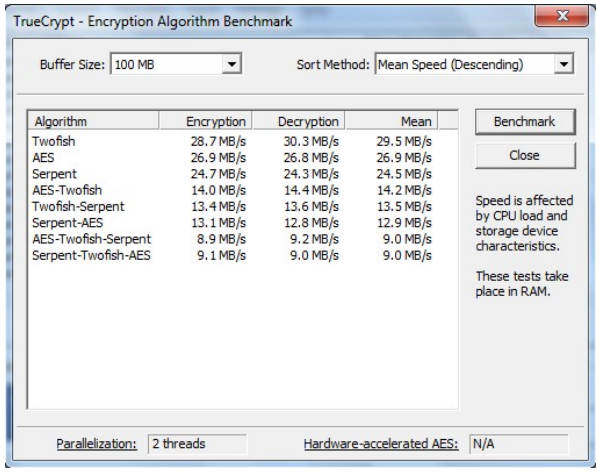
Algorithm	Encryption	Decryption	Mean
Twofish	19 MB/s	17 MB/s	18 MB/s
Serpent	15 MB/s	18 MB/s	17 MB/s
AES	15 MB/s	15 MB/s	15 MB/s
Twofish-Serpent	8,4 MB/s	9 MB/s	8,8 MB/s
AES-Twofish	8,5 MB/s	8,2 MB/s	8,4 MB/s
Serpent-AES	7,7 MB/s	8,3 MB/s	8,0 MB/s
AES-Twofish-Serpent	5,4 MB/s	5,7 MB/s	5,6 MB/s
Serpent-Twofish-AES	5,4 MB/s	5,7 MB/s	5,5 MB/s

Powersave

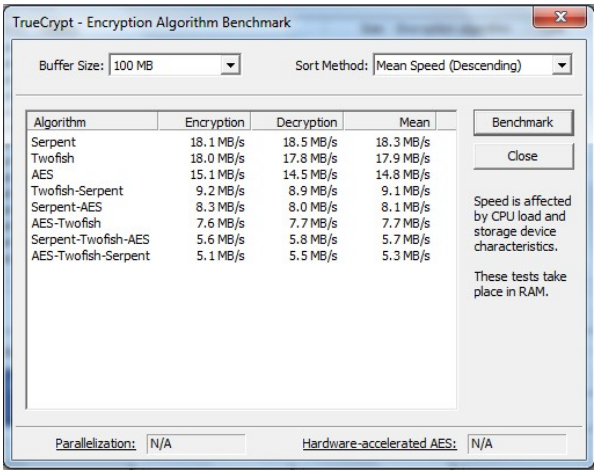
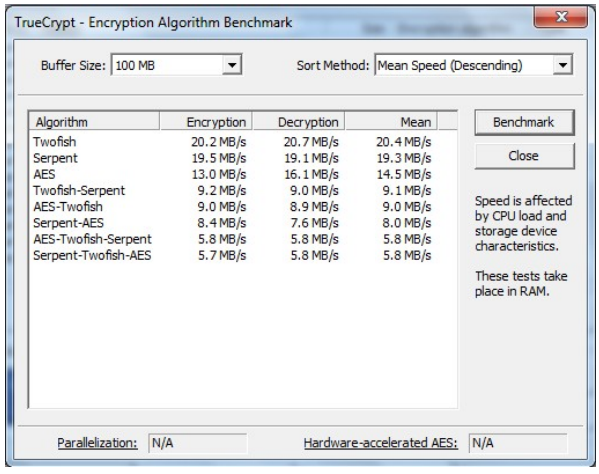


Algorithm	Encryption	Decryption	Mean
Twofish	11 MB/s	10 MB/s	11 MB/s
Serpent	9 MB/s	11 MB/s	10 MB/s
AES	9 MB/s	9 MB/s	9 MB/s
Twofish-Serpent	5,2 MB/s	5,6 MB/s	5,4 MB/s
AES-Twofish	5,2 MB/s	5,0 MB/s	5,1 MB/s
Serpent-AES	4,7 MB/s	5,1 MB/s	4,9 MB/s
Serpent-Twofish-AES	3,3 MB/s	3,5 MB/s	3,4 MB/s
AES-Twofish-Serpent	3,3 MB/s	3,5 MB/s	3,4 MB/s

Windows DualCore 32-Bit

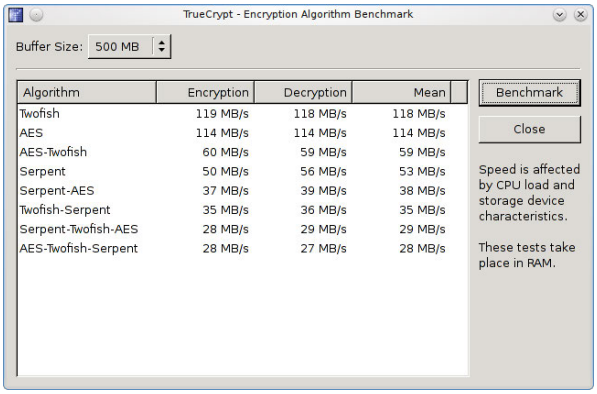
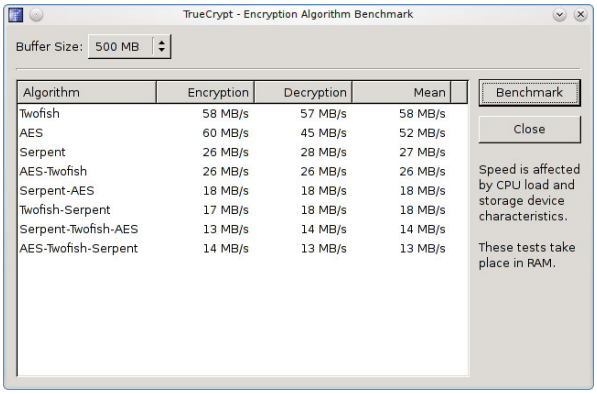
Höchstleistungsmodus	Energiesparmodus
	

Windows SingleCore 32-Bit

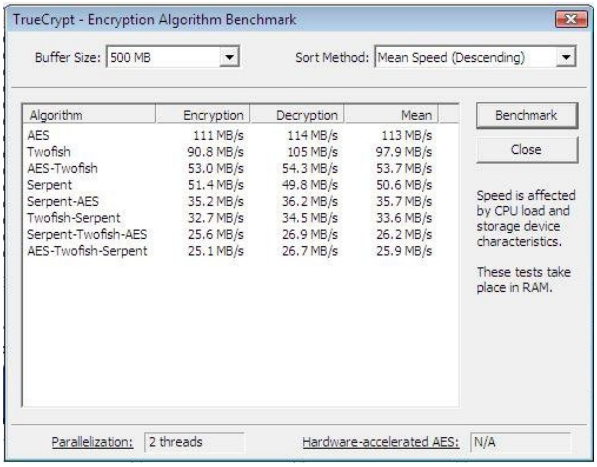
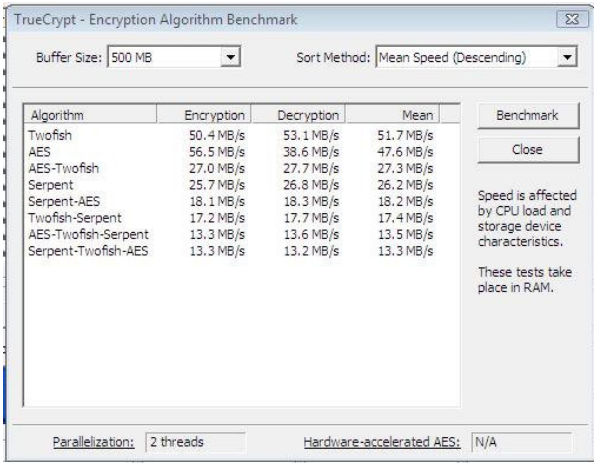
Höchstleistungsmodus	Energiesparmodus
	

5.2.2 Lenovo x61s

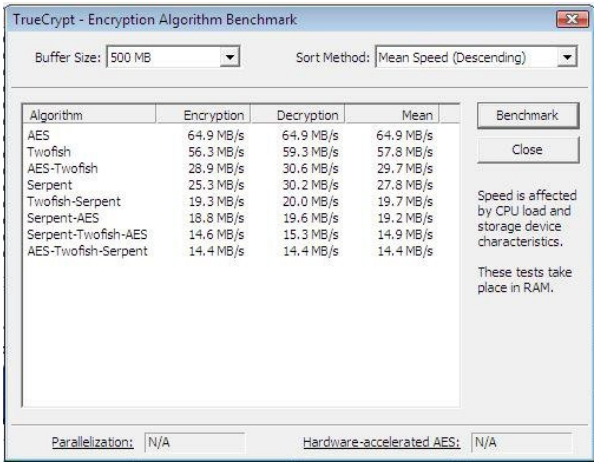
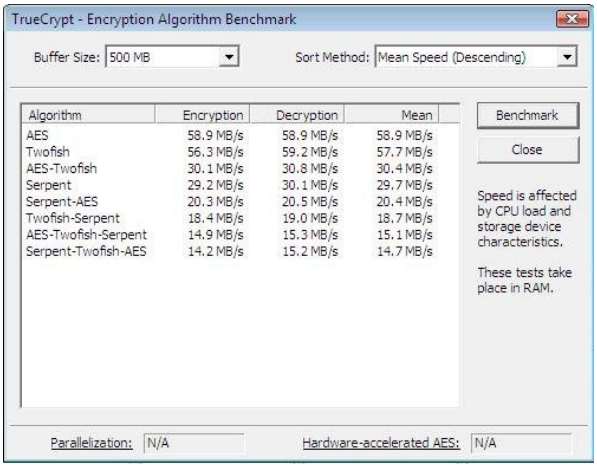
Linux DualCore 64-Bit

Performance	Powersave
	

Windows DualCore 64-Bit

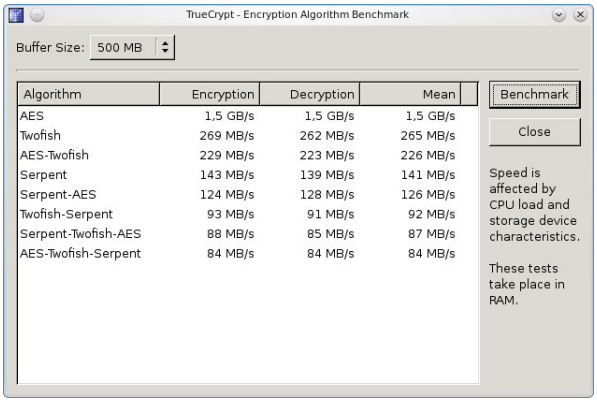
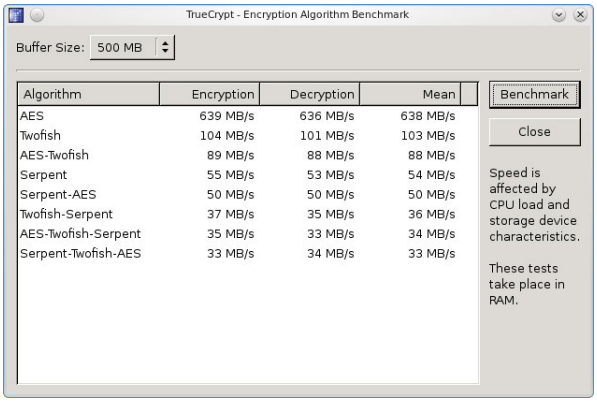
Höchstleistungsmodus	Energiesparmodus
	

Windows SingleCore 64-Bit

Höchstleistungsmodus	Energiesparmodus
	

5.2.3 HP EliteBook 8540p

Linux QuadCore 64-Bit mit AES-NI

Performance	Powersave
	

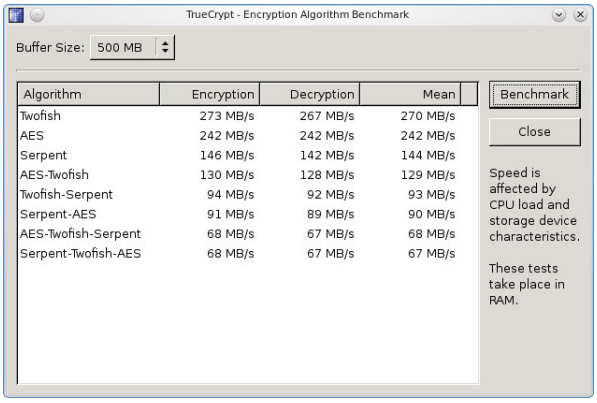
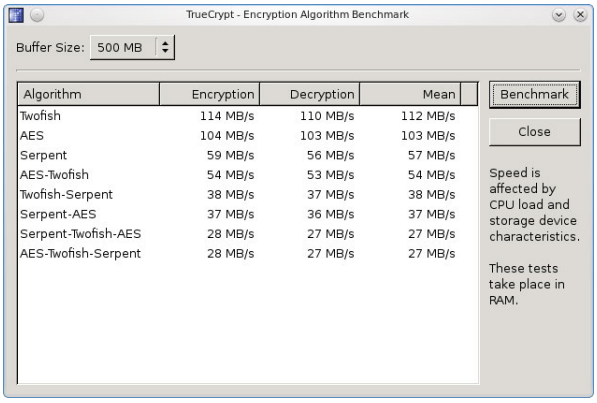
Performance:

Algorithm	Encryption	Decryption	Mean
AES	1,5 GB/s	1,5 GB/s	1,5 GB/s
Twofish	269 MB/s	262 MB/s	265 MB/s
AES-Twofish	229 MB/s	223 MB/s	226 MB/s
Serpent	143 MB/s	139 MB/s	141 MB/s
Serpent-AES	124 MB/s	128 MB/s	126 MB/s
Twofish-Serpent	93 MB/s	91 MB/s	92 MB/s
Serpent-Twofish-AES	88 MB/s	85 MB/s	87 MB/s
AES-Twofish-Serpent	84 MB/s	84 MB/s	84 MB/s

Powersave:

Algorithm	Encryption	Decryption	Mean
AES	639 MB/s	636 MB/s	638 MB/s
Twofish	104 MB/s	101 MB/s	103 MB/s
AES-Twofish	89 MB/s	88 MB/s	88 MB/s
Serpent	55 MB/s	53 MB/s	54 MB/s
Serpent-AES	50 MB/s	50 MB/s	50 MB/s
Twofish-Serpent	37 MB/s	35 MB/s	36 MB/s
AES-Twofish-Serpent	35 MB/s	33 MB/s	34 MB/s
Serpent-Twofish-AES	33 MB/s	34 MB/s	33 MB/s

Linux QuadCore 64-Bit ohne AES-NI

Performance	Powersave
	

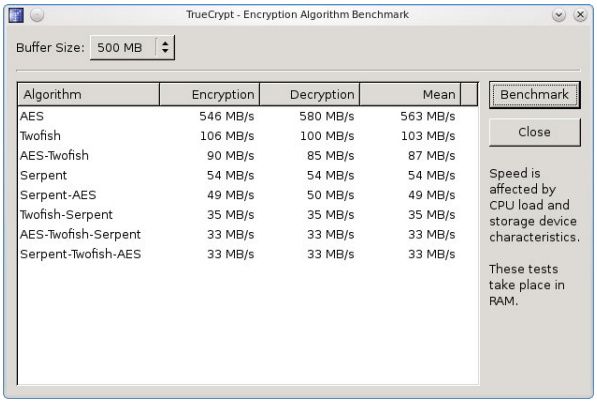
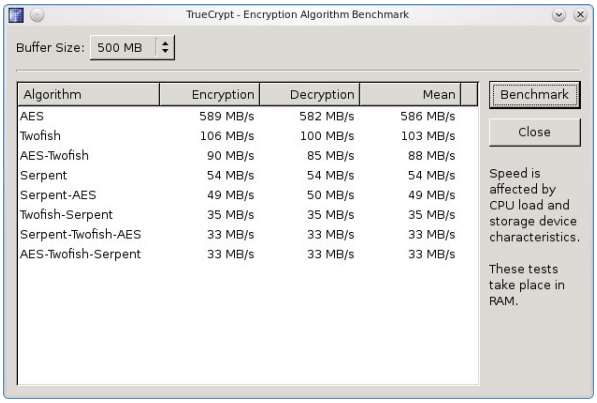
Performance:

Algorithm	Encryption	Decryption	Mean
Twofish	273 MB/s	267 MB/s	270 MB/s
AES	242 MB/s	242 MB/s	242 MB/s
Serpent	146 MB/s	142 MB/s	144 MB/s
AES-Twofish	130 MB/s	128 MB/s	129 MB/s
Twofish-Serpent	94 MB/s	92 MB/s	93 MB/s
Serpent-AES	91 MB/s	89 MB/s	90 MB/s
AES-Twofish-Serpent	68 MB/s	67 MB/s	68 MB/s
Serpent-Twofish-AES	68 MB/s	67 MB/s	67 MB/s

Powersave:

Algorithm	Encryption	Decryption	Mean
Twofish	114 MB/s	110 MB/s	112 MB/s
AES	104 MB/s	103 MB/s	103 MB/s
Serpent	59 MB/s	56 MB/s	57 MB/s
AES-Twofish	54 MB/s	53 MB/s	54 MB/s
Twofish-Serpent	38 MB/s	37 MB/s	38 MB/s
Serpent-AES	37 MB/s	36 MB/s	37 MB/s
Serpent-Twofish-AES	28 MB/s	27 MB/s	27 MB/s
AES-Twofish-Serpent	28 MB/s	27 MB/s	27 MB/s

Linux SingleCore 64-Bit mit AES-NI

Performance	Powersave
	

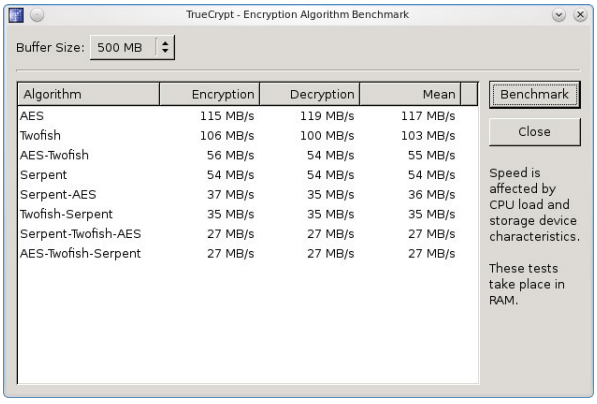
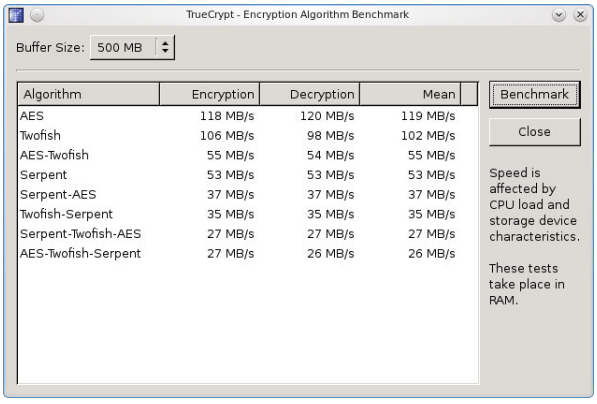
Performance

Algorithm	Encryption	Decryption	Mean
AES	546 MB/s	580 MB/s	563 MB/s
Twofish	106 MB/s	100 MB/s	103 MB/s
AES-Twofish	90 MB/s	85 MB/s	87 MB/s
Serpent	54 MB/s	54 MB/s	54 MB/s
Serpent-AES	49 MB/s	50 MB/s	49 MB/s
Twofish-Serpent	35 MB/s	35 MB/s	35 MB/s
AES-Twofish-Serpent	33 MB/s	33 MB/s	33 MB/s
Serpent-Twofish-AES	33 MB/s	33 MB/s	33 MB/s

Powersave

Algorithm	Encryption	Decryption	Mean
AES	589 MB/s	582 MB/s	586 MB/s
Twofish	106 MB/s	100 MB/s	103 MB/s
AES-Twofish	90 MB/s	85 MB/s	88 MB/s
Serpent	54 MB/s	54 MB/s	54 MB/s
Serpent-AES	49 MB/s	50 MB/s	49 MB/s
Twofish-Serpent	35 MB/s	35 MB/s	35 MB/s
Serpent-Twofish-AES	33 MB/s	33 MB/s	33 MB/s
AES-Twofish-Serpent	33 MB/s	33 MB/s	33 MB/s

Linux SingleCore 64-Bit ohne AES-NI

Performance	Powersave
	

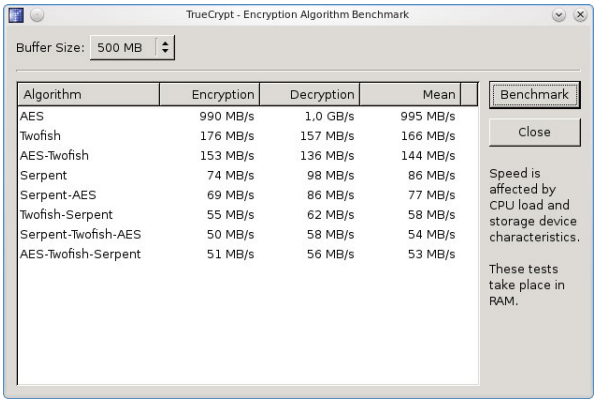
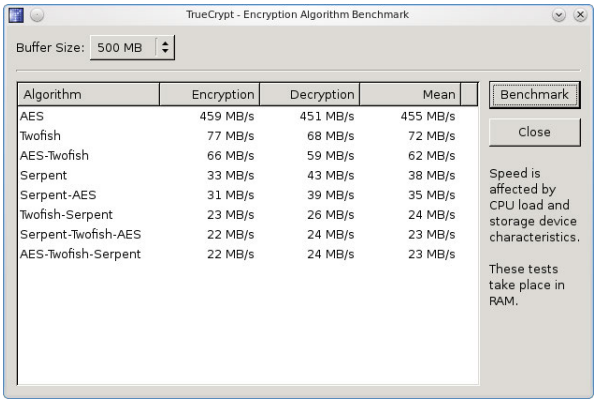
Performance

Algorithm	Encryption	Decryption	Mean
AES	115 MB/s	119 MB/s	117 MB/s
Twofish	106 MB/s	100 MB/s	103 MB/s
AES-Twofish	56 MB/s	54 MB/s	55 MB/s
Serpent	54 MB/s	54 MB/s	54 MB/s
Serpent-AES	37 MB/s	35 MB/s	36 MB/s
Twofish-Serpent	35 MB/s	35 MB/s	35 MB/s
Serpent-Twofish-AES	27 MB/s	27 MB/s	27 MB/s
AES-Twofish-Serpent	27 MB/s	27 MB/s	27 MB/s

Powersave

Algorithm	Encryption	Decryption	Mean
AES	118 MB/s	120 MB/s	119 MB/s
Twofish	106 MB/s	98 MB/s	102 MB/s
AES-Twofish	55 MB/s	54 MB/s	55 MB/s
Serpent	53 MB/s	53 MB/s	53 MB/s
Serpent-AES	37 MB/s	37 MB/s	37 MB/s
Twofish-Serpent	35 MB/s	35 MB/s	35 MB/s
Serpent-Twofish-AES	27 MB/s	27 MB/s	27 MB/s
AES-Twofish-Serpent	27 MB/s	26 MB/s	26 MB/s

Linux QuadCore 32-Bit mit AES-NI

Performance	Powersave
	

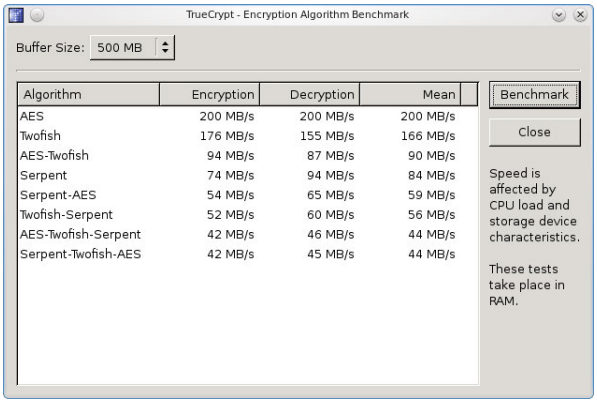
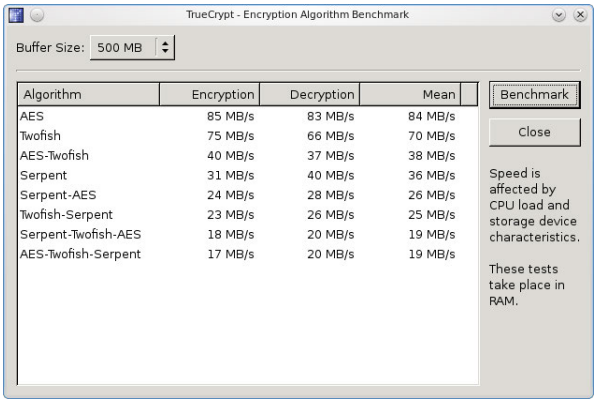
Performance

Algorithm	Encryption	Decryption	Mean
AES	990 MB/s	1,0 GB/s	995 MB/s
Twofish	176 MB/s	157 MB/s	166 MB/s
AES-Twofish	153 MB/s	136 MB/s	144 MB/s
Serpent	74 MB/s	98 MB/s	86 MB/s
Serpent-AES	69 MB/s	86 MB/s	77 MB/s
Twofish-Serpent	55 MB/s	62 MB/s	58 MB/s
Serpent-Twofish-AES	50 MB/s	58 MB/s	54 MB/s
AES-Twofish-Serpent	51 MB/s	56 MB/s	53 MB/s

Powersave

Algorithm	Encryption	Decryption	Mean
AES	459 MB/s	451 MB/s	455 MB/s
Twofish	77 MB/s	68 MB/s	72 MB/s
AES-Twofish	66 MB/s	59 MB/s	62 MB/s
Serpent	33 MB/s	43 MB/s	38 MB/s
Serpent-AES	31 MB/s	39 MB/s	35 MB/s
Twofish-Serpent	23 MB/s	26 MB/s	24 MB/s
Serpent-Twofish-AES	22 MB/s	24 MB/s	23 MB/s
AES-Twofish-Serpent	22 MB/s	24 MB/s	23 MB/s

Linux QuadCore 32-Bit ohne AES-NI

Performance	Powersave
	

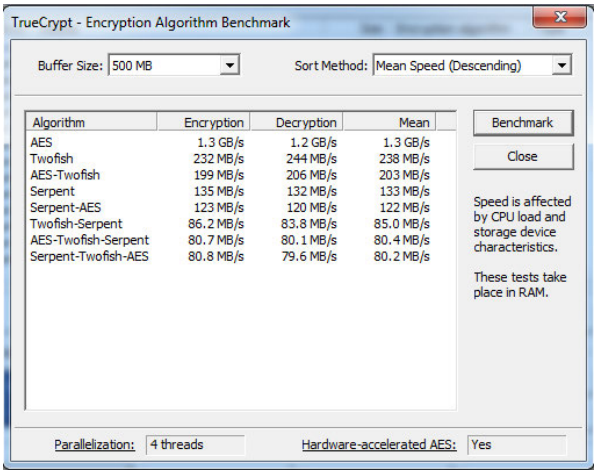
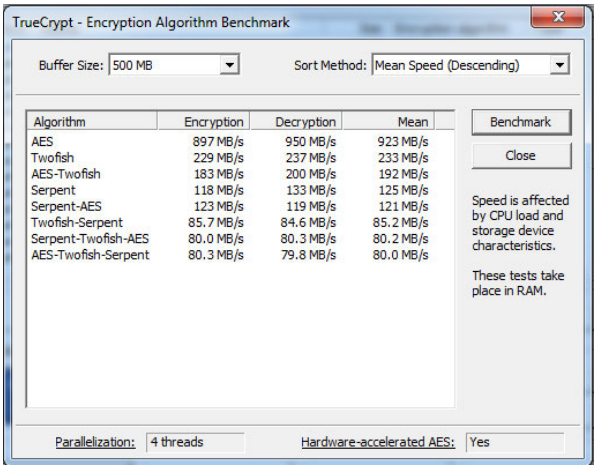
Performance

Algorithm	Encryption	Decryption	Mean
AES	200 MB/s	200 MB/s	200 MB/s
Twofish	176 MB/s	155 MB/s	166 MB/s
AES-Twofish	94 MB/s	87 MB/s	90 MB/s
Serpent	74 MB/s	94 MB/s	84 MB/s
Serpent-AES	54 MB/s	65 MB/s	59 MB/s
Twofish-Serpent	52 MB/s	60 MB/s	56 MB/s
AES-Twofish-Serpent	42 MB/s	46 MB/s	44 MB/s
Serpent-Twofish-AES	42 MB/s	45 MB/s	44 MB/s

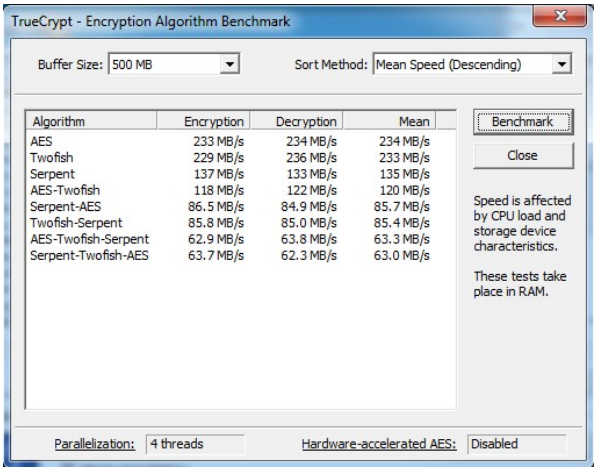
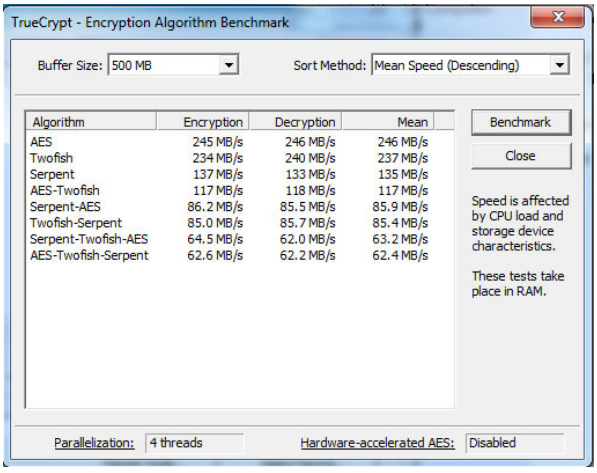
Powersave

Algorithm	Encryption	Decryption	Mean
AES	85 MB/s	83 MB/s	84 MB/s
Twofish	75 MB/s	66 MB/s	70 MB/s
AES-Twofish	40 MB/s	37 MB/s	38 MB/s
Serpent	31 MB/s	40 MB/s	36 MB/s
Serpent-AES	24 MB/s	28 MB/s	26 MB/s
Twofish-Serpent	23 MB/s	26 MB/s	25 MB/s
Serpent-Twofish-AES	18 MB/s	20 MB/s	19 MB/s
AES-Twofish-Serpent	17 MB/s	20 MB/s	19 MB/s

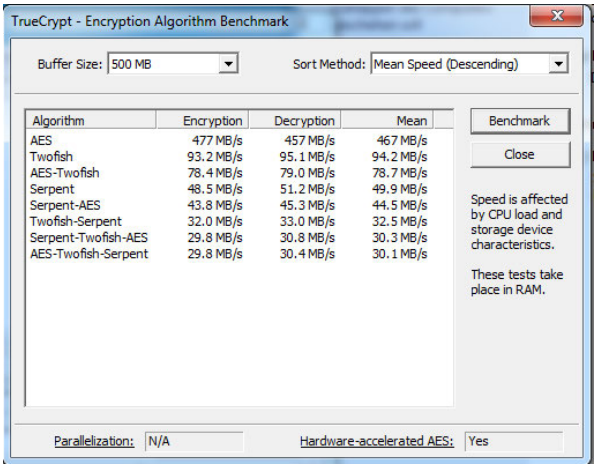
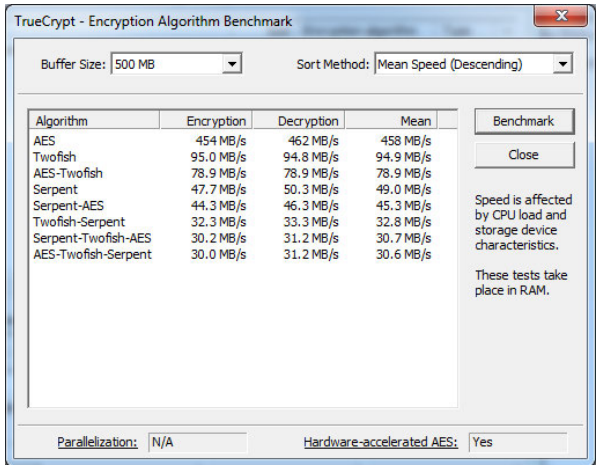
Windows QuadCore 64-Bit mit AES-NI

Höchstleistungsmodus	Energiesparmodus
	

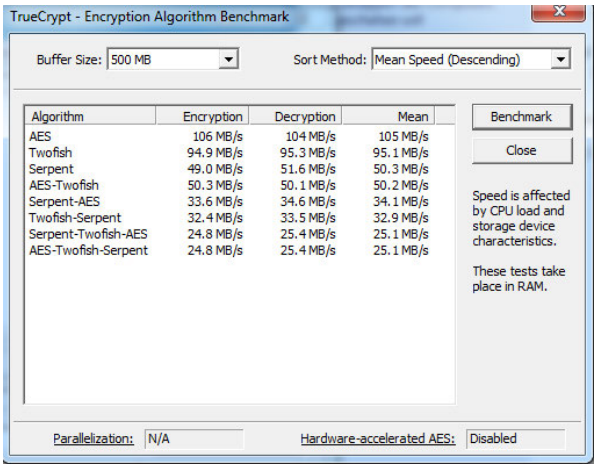
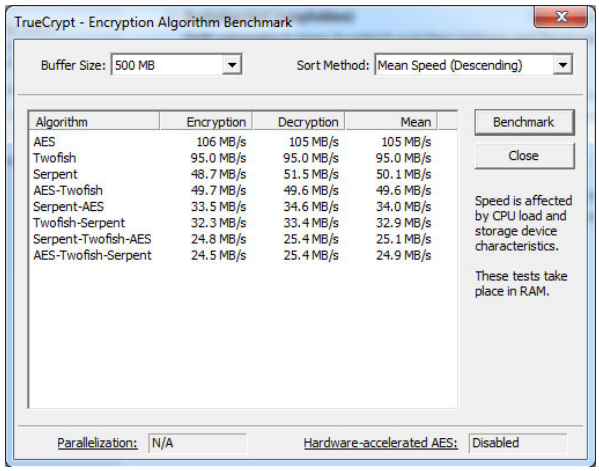
Windows QuadCore 64-Bit ohne AES-NI

Höchstleistungsmodus	Energiesparmodus
	

Windows SingleCore 64-Bit mit AES-NI

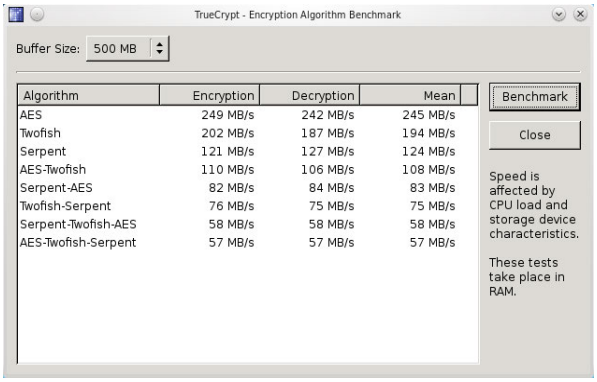
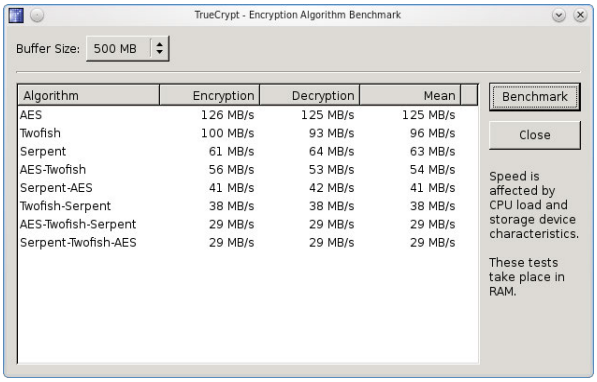
Höchstleistungsmodus	Energiesparmodus
	

Windows SingleCore 64-Bit ohne AES-NI

Höchstleistungsmodus	Energiesparmodus
	

5.2.4 xPC Shuttle-PC G2

Linux DualCore

Performance	Powersave
	

5.3 Linux-Messungen ohne TrueCrypt-interne Krypto

5.3.1 Acer Aspire one D250-1Bk

Name:	***Acer Aspire One***
32-Bit / 64-Bit:	32-Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Performance
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	98,9
Blockgröße: 1024 Byte	165,0
Blockgröße: 2048 Byte	244,0
Blockgröße: 4096 Byte	317,0
Blockgröße: 8192 Byte	367,0
Blockgröße: 16384 Byte	387,0
Blockgröße: 32768 Byte	402,0
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	40,5
Blockgröße: 1024 Byte	50,4
Blockgröße: 2048 Byte	56,5
Blockgröße: 4096 Byte	191,0
Blockgröße: 8192 Byte	212,0
Blockgröße: 16384 Byte	207,0
Blockgröße: 32768 Byte	243,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	9,8
Blockgröße: 1024 Byte	10,3
Blockgröße: 2048 Byte	10,5
Blockgröße: 4096 Byte	24,0
Blockgröße: 8192 Byte	23,9
Blockgröße: 16384 Byte	24,0
Blockgröße: 32768 Byte	24,0
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	8,2
Blockgröße: 1024 Byte	8,2
Blockgröße: 2048 Byte	8,4
Blockgröße: 4096 Byte	19,0
Blockgröße: 8192 Byte	19,0
Blockgröße: 16384 Byte	19,0
Blockgröße: 32768 Byte	18,9

Name:	***Acer Aspire One***
32-Bit / 64-Bit:	32-Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Powersave
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	59,7
Blockgröße: 1024 Byte	104,0
Blockgröße: 2048 Byte	153,0
Blockgröße: 4096 Byte	207,0
Blockgröße: 8192 Byte	240,0
Blockgröße: 16384 Byte	259,0
Blockgröße: 32768 Byte	272,0
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	27,6
Blockgröße: 1024 Byte	34,6
Blockgröße: 2048 Byte	37,8
Blockgröße: 4096 Byte	126,0
Blockgröße: 8192 Byte	129,0
Blockgröße: 16384 Byte	134,0
Blockgröße: 32768 Byte	148,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	6,0
Blockgröße: 1024 Byte	6,2
Blockgröße: 2048 Byte	6,4
Blockgröße: 4096 Byte	14,6
Blockgröße: 8192 Byte	14,6
Blockgröße: 16384 Byte	14,4
Blockgröße: 32768 Byte	14,7
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	4,9
Blockgröße: 1024 Byte	5,0
Blockgröße: 2048 Byte	5,2
Blockgröße: 4096 Byte	11,3
Blockgröße: 8192 Byte	11,3
Blockgröße: 16384 Byte	11,4
Blockgröße: 32768 Byte	11,3

Name:	***Acer Aspire One***
32-Bit / 64-Bit:	32-Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Performance
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	87,7
Blockgröße: 1024 Byte	158,0
Blockgröße: 2048 Byte	225,0
Blockgröße: 4096 Byte	314,0
Blockgröße: 8192 Byte	359,0
Blockgröße: 16384 Byte	362,0
Blockgröße: 32768 Byte	386,0
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	42,8
Blockgröße: 1024 Byte	60,0
Blockgröße: 2048 Byte	70,6
Blockgröße: 4096 Byte	121,0
Blockgröße: 8192 Byte	139,0
Blockgröße: 16384 Byte	123,0
Blockgröße: 32768 Byte	144,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	10,1
Blockgröße: 1024 Byte	10,6
Blockgröße: 2048 Byte	8,7
Blockgröße: 4096 Byte	20,0
Blockgröße: 8192 Byte	22,2
Blockgröße: 16384 Byte	22,5
Blockgröße: 32768 Byte	22,1
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	8,2
Blockgröße: 1024 Byte	8,5
Blockgröße: 2048 Byte	8,6
Blockgröße: 4096 Byte	17,7
Blockgröße: 8192 Byte	19,2
Blockgröße: 16384 Byte	16,5
Blockgröße: 32768 Byte	19,3

Name:	***Acer Aspire One***
32-Bit / 64-Bit:	32-Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Powersave
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	60,0
Blockgröße: 1024 Byte	103,0
Blockgröße: 2048 Byte	155,0
Blockgröße: 4096 Byte	208,0
Blockgröße: 8192 Byte	244,0
Blockgröße: 16384 Byte	260,0
Blockgröße: 32768 Byte	275,0
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	29,6
Blockgröße: 1024 Byte	38,7
Blockgröße: 2048 Byte	45,1
Blockgröße: 4096 Byte	81,8
Blockgröße: 8192 Byte	91,6
Blockgröße: 16384 Byte	95,7
Blockgröße: 32768 Byte	97,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	6,0
Blockgröße: 1024 Byte	6,4
Blockgröße: 2048 Byte	6,5
Blockgröße: 4096 Byte	13,3
Blockgröße: 8192 Byte	14,5
Blockgröße: 16384 Byte	12,7
Blockgröße: 32768 Byte	13,5
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	4,9
Blockgröße: 1024 Byte	5,1
Blockgröße: 2048 Byte	5,2
Blockgröße: 4096 Byte	11,3
Blockgröße: 8192 Byte	9,8
Blockgröße: 16384 Byte	11,6
Blockgröße: 32768 Byte	10,0

5.3.2 Lenovo x61s

Name:	***Lenovo X61s***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Performance
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	326,0
Blockgröße: 1024 Byte	507,0
Blockgröße: 2048 Byte	672,0
Blockgröße: 4096 Byte	864,0
Blockgröße: 8192 Byte	932,0
Blockgröße: 16384 Byte	917,0
Blockgröße: 32768 Byte	921,0
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	92,9
Blockgröße: 1024 Byte	109,0
Blockgröße: 2048 Byte	117,0
Blockgröße: 4096 Byte	462,0
Blockgröße: 8192 Byte	439,0
Blockgröße: 16384 Byte	463,0
Blockgröße: 32768 Byte	473,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	24,9
Blockgröße: 1024 Byte	26,0
Blockgröße: 2048 Byte	26,2
Blockgröße: 4096 Byte	77,3
Blockgröße: 8192 Byte	79,2
Blockgröße: 16384 Byte	76,1
Blockgröße: 32768 Byte	80,1
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	18,3
Blockgröße: 1024 Byte	22,2
Blockgröße: 2048 Byte	22,4
Blockgröße: 4096 Byte	62,2
Blockgröße: 8192 Byte	62,6
Blockgröße: 16384 Byte	62,4
Blockgröße: 32768 Byte	61,1

Name:	***Lenovo X61s***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Powersave
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	159,0
Blockgröße: 1024 Byte	249,0
Blockgröße: 2048 Byte	353,0
Blockgröße: 4096 Byte	443,0
Blockgröße: 8192 Byte	486,0
Blockgröße: 16384 Byte	479,0
Blockgröße: 32768 Byte	443,0
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	51,0
Blockgröße: 1024 Byte	62,5
Blockgröße: 2048 Byte	75,1
Blockgröße: 4096 Byte	243,0
Blockgröße: 8192 Byte	246,0
Blockgröße: 16384 Byte	251,0
Blockgröße: 32768 Byte	249,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	13,8
Blockgröße: 1024 Byte	14,5
Blockgröße: 2048 Byte	14,6
Blockgröße: 4096 Byte	40,4
Blockgröße: 8192 Byte	39,7
Blockgröße: 16384 Byte	40,1
Blockgröße: 32768 Byte	40,7
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	11,6
Blockgröße: 1024 Byte	12,0
Blockgröße: 2048 Byte	12,3
Blockgröße: 4096 Byte	32,1
Blockgröße: 8192 Byte	31,7
Blockgröße: 16384 Byte	31,0
Blockgröße: 32768 Byte	32,0

5.3.3 HP EliteBook 8540p

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	ja
Anzahl Kerne:	QuadCore
Betriebsmodus:	Performance
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	760,0
Blockgröße: 1024 Byte	1,1 GB/s
Blockgröße: 2048 Byte	1,5 GB/s
Blockgröße: 4096 Byte	1,8 GB/s
Blockgröße: 8192 Byte	2,0 GB/s
Blockgröße: 16384 Byte	2,1 GB/s
Blockgröße: 32768 Byte	2,1 GB/s
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	228,0
Blockgröße: 1024 Byte	247,0
Blockgröße: 2048 Byte	295,0
Blockgröße: 4096 Byte	891,0
Blockgröße: 8192 Byte	946,0
Blockgröße: 16384 Byte	968,0
Blockgröße: 32768 Byte	970,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	90,6
Blockgröße: 1024 Byte	103,0
Blockgröße: 2048 Byte	94,8
Blockgröße: 4096 Byte	271,0
Blockgröße: 8192 Byte	272,0
Blockgröße: 16384 Byte	270,0
Blockgröße: 32768 Byte	270,0
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	88,6
Blockgröße: 1024 Byte	87,6
Blockgröße: 2048 Byte	88,1
Blockgröße: 4096 Byte	259,0
Blockgröße: 8192 Byte	235,0
Blockgröße: 16384 Byte	267,0
Blockgröße: 32768 Byte	269,0

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	ja
Anzahl Kerne:	QuadCore
Betriebsmodus:	Powersave
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	317,0
Blockgröße: 1024 Byte	489,0
Blockgröße: 2048 Byte	685,0
Blockgröße: 4096 Byte	886,0
Blockgröße: 8192 Byte	1,0 GB/s
Blockgröße: 16384 Byte	1,1 GB/s
Blockgröße: 32768 Byte	1,1 GB/s
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	110,0
Blockgröße: 1024 Byte	110,0
Blockgröße: 2048 Byte	109,0
Blockgröße: 4096 Byte	435,0
Blockgröße: 8192 Byte	520,0
Blockgröße: 16384 Byte	552,0
Blockgröße: 32768 Byte	484,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	37,9
Blockgröße: 1024 Byte	43,6
Blockgröße: 2048 Byte	45,5
Blockgröße: 4096 Byte	126,0
Blockgröße: 8192 Byte	127,0
Blockgröße: 16384 Byte	128,0
Blockgröße: 32768 Byte	121,0
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	34,3
Blockgröße: 1024 Byte	37,4
Blockgröße: 2048 Byte	36,2
Blockgröße: 4096 Byte	99,2
Blockgröße: 8192 Byte	110,0
Blockgröße: 16384 Byte	109,0
Blockgröße: 32768 Byte	110,0

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	QuadCore
Betriebsmodus:	Performance
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	766,0
Blockgröße: 1024 Byte	1,1 GB/s
Blockgröße: 2048 Byte	1,5 GB/s
Blockgröße: 4096 Byte	1,8 GB/s
Blockgröße: 8192 Byte	1,9 GB/s
Blockgröße: 16384 Byte	2,1 GB/s
Blockgröße: 32768 Byte	2,1 GB/s
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	244,0
Blockgröße: 1024 Byte	275,0
Blockgröße: 2048 Byte	294,0
Blockgröße: 4096 Byte	924,0
Blockgröße: 8192 Byte	949,0
Blockgröße: 16384 Byte	932,0
Blockgröße: 32768 Byte	977,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	56,4
Blockgröße: 1024 Byte	59,7
Blockgröße: 2048 Byte	57,3
Blockgröße: 4096 Byte	148,0
Blockgröße: 8192 Byte	148,0
Blockgröße: 16384 Byte	134,0
Blockgröße: 32768 Byte	149,0
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	46,0
Blockgröße: 1024 Byte	48,2
Blockgröße: 2048 Byte	47,8
Blockgröße: 4096 Byte	115,0
Blockgröße: 8192 Byte	108,0
Blockgröße: 16384 Byte	107,0
Blockgröße: 32768 Byte	111,0

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	QuadCore
Betriebsmodus:	Powersave
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	320,0
Blockgröße: 1024 Byte	492,0
Blockgröße: 2048 Byte	684,0
Blockgröße: 4096 Byte	889,0
Blockgröße: 8192 Byte	1,0 GB/s
Blockgröße: 16384 Byte	1,0 GB/s
Blockgröße: 32768 Byte	1,1 GB/s
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	106,0
Blockgröße: 1024 Byte	130,0
Blockgröße: 2048 Byte	140,0
Blockgröße: 4096 Byte	495,0
Blockgröße: 8192 Byte	534,0
Blockgröße: 16384 Byte	550,0
Blockgröße: 32768 Byte	546,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	22,9
Blockgröße: 1024 Byte	24,8
Blockgröße: 2048 Byte	23,5
Blockgröße: 4096 Byte	58,6
Blockgröße: 8192 Byte	59,6
Blockgröße: 16384 Byte	55,9
Blockgröße: 32768 Byte	53,9
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	18,2
Blockgröße: 1024 Byte	19,1
Blockgröße: 2048 Byte	19,5
Blockgröße: 4096 Byte	45,1
Blockgröße: 8192 Byte	46,5
Blockgröße: 16384 Byte	46,2
Blockgröße: 32768 Byte	46,4

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	ja
Anzahl Kerne:	SingleCore
Betriebsmodus:	Performance
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	740,0
Blockgröße: 1024 Byte	1,1 GB/s
Blockgröße: 2048 Byte	1,5 GB/s
Blockgröße: 4096 Byte	1,6 GB/s
Blockgröße: 8192 Byte	2,0 GB/s
Blockgröße: 16384 Byte	2,0 GB/s
Blockgröße: 32768 Byte	2,1 GB/s
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	324,0
Blockgröße: 1024 Byte	384,0
Blockgröße: 2048 Byte	361,0
Blockgröße: 4096 Byte	586,0
Blockgröße: 8192 Byte	720,0
Blockgröße: 16384 Byte	733,0
Blockgröße: 32768 Byte	739,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	105,0
Blockgröße: 1024 Byte	111,0
Blockgröße: 2048 Byte	115,0
Blockgröße: 4096 Byte	227,0
Blockgröße: 8192 Byte	230,0
Blockgröße: 16384 Byte	231,0
Blockgröße: 32768 Byte	232,0
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	94,9
Blockgröße: 1024 Byte	100,0
Blockgröße: 2048 Byte	103,0
Blockgröße: 4096 Byte	203,0
Blockgröße: 8192 Byte	206,0
Blockgröße: 16384 Byte	206,0
Blockgröße: 32768 Byte	207,0

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	ja
Anzahl Kerne:	SingleCore
Betriebsmodus:	Powersave
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	717,0
Blockgröße: 1024 Byte	1,0 GB/s
Blockgröße: 2048 Byte	1,5 GB/s
Blockgröße: 4096 Byte	1,8 GB/s
Blockgröße: 8192 Byte	2,0 GB/s
Blockgröße: 16384 Byte	2,1 GB/s
Blockgröße: 32768 Byte	2,1 GB/s
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	273,0
Blockgröße: 1024 Byte	338,0
Blockgröße: 2048 Byte	444,0
Blockgröße: 4096 Byte	687,0
Blockgröße: 8192 Byte	723,0
Blockgröße: 16384 Byte	733,0
Blockgröße: 32768 Byte	745,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	105,0
Blockgröße: 1024 Byte	112,0
Blockgröße: 2048 Byte	115,0
Blockgröße: 4096 Byte	228,0
Blockgröße: 8192 Byte	230,0
Blockgröße: 16384 Byte	232,0
Blockgröße: 32768 Byte	231,0
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	95,0
Blockgröße: 1024 Byte	101,0
Blockgröße: 2048 Byte	103,0
Blockgröße: 4096 Byte	204,0
Blockgröße: 8192 Byte	206,0
Blockgröße: 16384 Byte	207,0
Blockgröße: 32768 Byte	207,0

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Performance
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	683,0
Blockgröße: 1024 Byte	1,1 GB/s
Blockgröße: 2048 Byte	1,5 GB/s
Blockgröße: 4096 Byte	1,8 GB/s
Blockgröße: 8192 Byte	2,0 GB/s
Blockgröße: 16384 Byte	2,1 GB/s
Blockgröße: 32768 Byte	2,1 GB/s
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	324,0
Blockgröße: 1024 Byte	359,0
Blockgröße: 2048 Byte	393,0
Blockgröße: 4096 Byte	693,0
Blockgröße: 8192 Byte	731,0
Blockgröße: 16384 Byte	745,0
Blockgröße: 32768 Byte	753,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	59,3
Blockgröße: 1024 Byte	59,8
Blockgröße: 2048 Byte	63,5
Blockgröße: 4096 Byte	127,0
Blockgröße: 8192 Byte	128,0
Blockgröße: 16384 Byte	128,0
Blockgröße: 32768 Byte	129,0
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	48,9
Blockgröße: 1024 Byte	50,3
Blockgröße: 2048 Byte	51,0
Blockgröße: 4096 Byte	103,0
Blockgröße: 8192 Byte	103,0
Blockgröße: 16384 Byte	103,0
Blockgröße: 32768 Byte	104,0

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Powersave
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	690,0
Blockgröße: 1024 Byte	1,1 GB/s
Blockgröße: 2048 Byte	1,5 GB/s
Blockgröße: 4096 Byte	1,8 GB/s
Blockgröße: 8192 Byte	2,0 GB/s
Blockgröße: 16384 Byte	2,1 GB/s
Blockgröße: 32768 Byte	2,1 GB/s
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	336,0
Blockgröße: 1024 Byte	381,0
Blockgröße: 2048 Byte	422,0
Blockgröße: 4096 Byte	695,0
Blockgröße: 8192 Byte	723,0
Blockgröße: 16384 Byte	741,0
Blockgröße: 32768 Byte	747,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	58,7
Blockgröße: 1024 Byte	61,8
Blockgröße: 2048 Byte	61,9
Blockgröße: 4096 Byte	127,0
Blockgröße: 8192 Byte	128,0
Blockgröße: 16384 Byte	129,0
Blockgröße: 32768 Byte	129,0
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	49,1
Blockgröße: 1024 Byte	50,5
Blockgröße: 2048 Byte	51,1
Blockgröße: 4096 Byte	103,0
Blockgröße: 8192 Byte	103,0
Blockgröße: 16384 Byte	103,0
Blockgröße: 32768 Byte	104,0

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	32-Bit
Hardware-AES:	nein
Anzahl Kerne:	QuadCore
Betriebsmodus:	Performance
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	569,0
Blockgröße: 1024 Byte	956,0
Blockgröße: 2048 Byte	1,3 GB/s
Blockgröße: 4096 Byte	1,6 GB/s
Blockgröße: 8192 Byte	1,7 GB/s
Blockgröße: 16384 Byte	1,8 GB/s
Blockgröße: 32768 Byte	1,8 GB/s
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	224,0
Blockgröße: 1024 Byte	271,0
Blockgröße: 2048 Byte	294,0
Blockgröße: 4096 Byte	1,2 GB/s
Blockgröße: 8192 Byte	1,2 GB/s
Blockgröße: 16384 Byte	1,2 GB/s
Blockgröße: 32768 Byte	1,2 GB/s
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	51,2
Blockgröße: 1024 Byte	53,4
Blockgröße: 2048 Byte	52,0
Blockgröße: 4096 Byte	127,0
Blockgröße: 8192 Byte	127,0
Blockgröße: 16384 Byte	127,0
Blockgröße: 32768 Byte	127,0
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	42,4
Blockgröße: 1024 Byte	42,6
Blockgröße: 2048 Byte	42,6
Blockgröße: 4096 Byte	99,7
Blockgröße: 8192 Byte	99,8
Blockgröße: 16384 Byte	99,8
Blockgröße: 32768 Byte	95,9

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	32-Bit
Hardware-AES:	nein
Anzahl Kerne:	QuadCore
Betriebsmodus:	Powersave
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	241,0
Blockgröße: 1024 Byte	396,0
Blockgröße: 2048 Byte	590,0
Blockgröße: 4096 Byte	780,0
Blockgröße: 8192 Byte	872,0
Blockgröße: 16384 Byte	907,0
Blockgröße: 32768 Byte	907,0
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	95,0
Blockgröße: 1024 Byte	127,0
Blockgröße: 2048 Byte	120,0
Blockgröße: 4096 Byte	594,0
Blockgröße: 8192 Byte	673,0
Blockgröße: 16384 Byte	692,0
Blockgröße: 32768 Byte	694,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	19,7
Blockgröße: 1024 Byte	20,6
Blockgröße: 2048 Byte	21,5
Blockgröße: 4096 Byte	49,1
Blockgröße: 8192 Byte	50,8
Blockgröße: 16384 Byte	50,8
Blockgröße: 32768 Byte	46,7
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	15,9
Blockgröße: 1024 Byte	16,7
Blockgröße: 2048 Byte	17,4
Blockgröße: 4096 Byte	39,3
Blockgröße: 8192 Byte	38,6
Blockgröße: 16384 Byte	37,1
Blockgröße: 32768 Byte	37,1

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	32-Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Performance
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	569,0
Blockgröße: 1024 Byte	933,0
Blockgröße: 2048 Byte	1,3 GB/s
Blockgröße: 4096 Byte	1,2 GB/s
Blockgröße: 8192 Byte	1,8 GB/s
Blockgröße: 16384 Byte	1,9 GB/s
Blockgröße: 32768 Byte	1,8 GB/s
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	319,0
Blockgröße: 1024 Byte	397,0
Blockgröße: 2048 Byte	455,0
Blockgröße: 4096 Byte	688,0
Blockgröße: 8192 Byte	713,0
Blockgröße: 16384 Byte	732,0
Blockgröße: 32768 Byte	729,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	52,4
Blockgröße: 1024 Byte	53,9
Blockgröße: 2048 Byte	55,2
Blockgröße: 4096 Byte	110,0
Blockgröße: 8192 Byte	111,0
Blockgröße: 16384 Byte	111,0
Blockgröße: 32768 Byte	111,0
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	42,8
Blockgröße: 1024 Byte	43,7
Blockgröße: 2048 Byte	44,6
Blockgröße: 4096 Byte	88,6
Blockgröße: 8192 Byte	89,1
Blockgröße: 16384 Byte	89,3
Blockgröße: 32768 Byte	89,3

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	32-Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Powersave
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	593,0
Blockgröße: 1024 Byte	935,0
Blockgröße: 2048 Byte	1,3 GB/s
Blockgröße: 4096 Byte	1,1 GB/s
Blockgröße: 8192 Byte	1,5 GB/s
Blockgröße: 16384 Byte	1,9 GB/s
Blockgröße: 32768 Byte	1,8 GB/s
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	319,0
Blockgröße: 1024 Byte	401,0
Blockgröße: 2048 Byte	453,0
Blockgröße: 4096 Byte	690,0
Blockgröße: 8192 Byte	721,0
Blockgröße: 16384 Byte	735,0
Blockgröße: 32768 Byte	736,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	52,4
Blockgröße: 1024 Byte	54,3
Blockgröße: 2048 Byte	55,2
Blockgröße: 4096 Byte	110,0
Blockgröße: 8192 Byte	111,0
Blockgröße: 16384 Byte	111,0
Blockgröße: 32768 Byte	111,0
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	42,8
Blockgröße: 1024 Byte	43,6
Blockgröße: 2048 Byte	44,4
Blockgröße: 4096 Byte	88,6
Blockgröße: 8192 Byte	85,8
Blockgröße: 16384 Byte	88,1
Blockgröße: 32768 Byte	83,8

5.3.4 xPC Shuttle-PC G2

Name:	***xPC Shuttle***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Performance
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	450,0
Blockgröße: 1024 Byte	820,0
Blockgröße: 2048 Byte	1,1 GB/s
Blockgröße: 4096 Byte	1,3 GB/s
Blockgröße: 8192 Byte	1,4 GB/s
Blockgröße: 16384 Byte	1,4 GB/s
Blockgröße: 32768 Byte	1,5 GB/s
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	208,0
Blockgröße: 1024 Byte	214,0
Blockgröße: 2048 Byte	210,0
Blockgröße: 4096 Byte	562,0
Blockgröße: 8192 Byte	569,0
Blockgröße: 16384 Byte	569,0
Blockgröße: 32768 Byte	568,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	49,6
Blockgröße: 1024 Byte	51,7
Blockgröße: 2048 Byte	53,7
Blockgröße: 4096 Byte	117,0
Blockgröße: 8192 Byte	128,0
Blockgröße: 16384 Byte	128,0
Blockgröße: 32768 Byte	127,0
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	40,8
Blockgröße: 1024 Byte	43,9
Blockgröße: 2048 Byte	44,9
Blockgröße: 4096 Byte	103,0
Blockgröße: 8192 Byte	105,0
Blockgröße: 16384 Byte	105,0
Blockgröße: 32768 Byte	104,0

Name:	***xPC Shuttle***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Powersave
RAM-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	287,0
Blockgröße: 1024 Byte	412,0
Blockgröße: 2048 Byte	646,0
Blockgröße: 4096 Byte	792,0
Blockgröße: 8192 Byte	865,0
Blockgröße: 16384 Byte	814,0
Blockgröße: 32768 Byte	911,0
Device-Mapper-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	126,0
Blockgröße: 1024 Byte	136,0
Blockgröße: 2048 Byte	139,0
Blockgröße: 4096 Byte	354,0
Blockgröße: 8192 Byte	368,0
Blockgröße: 16384 Byte	387,0
Blockgröße: 32768 Byte	397,0
Linux-Crypto-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	27,0
Blockgröße: 1024 Byte	28,1
Blockgröße: 2048 Byte	29,0
Blockgröße: 4096 Byte	69,2
Blockgröße: 8192 Byte	68,8
Blockgröße: 16384 Byte	65,4
Blockgröße: 32768 Byte	70,2
TrueCrypt-Geschwindigkeit	**in MB/s**
Blockgröße: 512 Byte	23,4
Blockgröße: 1024 Byte	23,9
Blockgröße: 2048 Byte	23,6
Blockgröße: 4096 Byte	57,2
Blockgröße: 8192 Byte	57,3
Blockgröße: 16384 Byte	56,4
Blockgröße: 32768 Byte	56,9

5.4 Windows-Messungen mit TrueCrypt-interner Krypto

5.4.1 Acer Aspire One

Name:	***Acer Aspire One***
32-Bit / 64-Bit:	32- Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Höchstleistungsmodus
Betriebssystem:	Windows 7 Professional 32-Bit
RAM-Durchsatz:	700 MB/s
Festplattendurchsatz:	65 MB/s
TrueCrypt auf FAT-Ramdisk:	25 MB/s
TrueCrypt auf NTFS-Ramdisk:	25 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	150 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	150 Sekunden
Extrahieren von Eclipse (NTFS auf TC-RD):	150 Sekunden

Name:	***Acer Aspire One***
32-Bit / 64-Bit:	32- Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Energiesparmodus
Betriebssystem:	Windows 7 Professional 32-Bit
RAM-Durchsatz:	700 MB/s
Festplattendurchsatz:	65 MB/s
TrueCrypt auf FAT-Ramdisk:	25 MB/s
TrueCrypt auf NTFS-Ramdisk:	25 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	150 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	180 Sekunden
Extrahieren von Eclipse (NTFS auf TC-RD):	180 Sekunden

Name:	*Acer Aspire One*
32-Bit / 64-Bit:	32- Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Höchstleistungsmodus
Betriebssystem:	Windows 7 Professional 32-Bit
RAM-Durchsatz:	750 MB/s
Festplattendurchsatz:	50 MB/s
TrueCrypt auf FAT-Ramdisk:	15 MB/s
TrueCrypt auf NTFS-Ramdisk:	15 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	200 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	215 Sekunden
Extrahieren von Eclipse (NTFS auf TC-RD):	215 Sekunden

Name:	*Acer Aspire One*
32-Bit / 64-Bit:	32- Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Energiesparmodus
Betriebssystem:	Windows 7 Professional 32-Bit
RAM-Durchsatz:	720 MB/s
Festplattendurchsatz:	50 MB/s
TrueCrypt auf FAT-Ramdisk:	15 MB/s
TrueCrypt auf NTFS-Ramdisk:	15 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	200 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	215 Sekunden
Extrahieren von Eclipse (NTFS auf TC-RD):	215 Sekunden

5.4.2 Lenovo x61s

Name:	*Lenovo X61s*
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Höchstleistungsmodus
Betriebssystem:	Windows Vista Ultimate 64-Bit SP1
RAM-Durchsatz:	1,3 GB/s
Festplattendurchsatz:	35 MB/s
TrueCrypt auf FAT-Ramdisk:	110 MB/s
TrueCrypt auf NTFS-Ramdisk:	110 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	50 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	55 Sekunden

Name:	*Lenovo X61s*
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Energiesparmodus
Betriebssystem:	Windows Vista Ultimate 64-Bit SP1
RAM-Durchsatz:	700 MB/s
Festplattendurchsatz:	30 MB/s
TrueCrypt auf FAT-Ramdisk:	55 MB/s
TrueCrypt auf NTFS-Ramdisk:	55 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	95 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	90 Sekunden

Name:	*Lenovo X61s*
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Höchstleistungsmodus
Betriebssystem:	Windows Vista Ultimate 64-Bit SP1
RAM-Durchsatz:	1,3 GB/s
Festplattendurchsatz:	35 MB/s
TrueCrypt auf FAT-Ramdisk:	70 MB/s
TrueCrypt auf NTFS-Ramdisk:	65 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	70 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	75 Sekunden

Name:	*Lenovo X61s*
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Energiesparmodus
Betriebssystem:	Windows Vista Ultimate 64-Bit SP1
RAM-Durchsatz:	1,3 GB/s
Festplattendurchsatz:	25 MB/s
TrueCrypt auf FAT-Ramdisk:	70 MB/s
TrueCrypt auf NTFS-Ramdisk:	65 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	85 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	80 Sekunden
Extrahieren von Eclipse (NTFS auf TC-RD):	70 Sekunden

5.4.3 HP EliteBook 8540p

Name:	*HP EliteBook 8540p*
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	ja
Anzahl Kerne:	QuadCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows 7 64-Bit
RAM-Durchsatz:	2,7 GB/s
Festplattendurchsatz:	80 – 95 MB/s
TrueCrypt auf FAT-Ramdisk:	860 MB/s
TrueCrypt auf NTFS-Ramdisk:	850 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	12 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	25 Sekunden
Extrahieren von Eclipse (NTFS auf TC-RD):	25 Sekunden

Name:	*HP EliteBook 8540p*
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	ja
Anzahl Kerne:	QuadCore
Betriebsmodus:	Energiesparmodus
Betriebssystem:	Windows 7 64-Bit
RAM-Durchsatz:	2,5 GB/s
Festplattendurchsatz:	80 – 95 MB/s
TrueCrypt auf FAT-Ramdisk:	370 MB/s
TrueCrypt auf NTFS-Ramdisk:	350 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	21 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	57 Sekunden
Extrahieren von Eclipse (NTFS auf TC-RD):	62 Sekunden

Name:	*HP EliteBook 8540p*
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	QuadCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows 7 64-Bit
RAM-Durchsatz:	2,7 GB/s
Festplattendurchsatz:	80 – 95 MB/s
TrueCrypt auf FAT-Ramdisk:	235 MB/s
TrueCrypt auf NTFS-Ramdisk:	235 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	12 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	25 Sekunden
Extrahieren von Eclipse (NTFS auf TC-RD):	26 Sekunden

Name:	*HP EliteBook 8540p*
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	QuadCore
Betriebsmodus:	Energiesparmodus
Betriebssystem:	Windows 7 64-Bit
RAM-Durchsatz:	2,5 GB/s
Festplattendurchsatz:	80 – 95 MB/s
TrueCrypt auf FAT-Ramdisk:	235 MB/s
TrueCrypt auf NTFS-Ramdisk:	235 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	21 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	59 Sekunden
Extrahieren von Eclipse (NTFS auf TC-RD):	63 Sekunden

Name:	*HP EliteBook 8540p*
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	ja
Anzahl Kerne:	SingleCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows 7 64-Bit
RAM-Durchsatz:	2,9 GB/s
Festplattendurchsatz:	80 – 90 MB/s
TrueCrypt auf FAT-Ramdisk:	420 MB/s
TrueCrypt auf NTFS-Ramdisk:	420 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	31 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	27 Sekunden
Extrahieren von Eclipse (NTFS auf TC-RD):	28 Sekunden

Name:	*HP EliteBook 8540p*
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	ja
Anzahl Kerne:	SingleCore
Betriebsmodus:	Energiesparmodus
Betriebssystem:	Windows 7 64-Bit
RAM-Durchsatz:	2,9 GB/s
Festplattendurchsatz:	80 – 85 MB/s
TrueCrypt auf FAT-Ramdisk:	420 MB/s
TrueCrypt auf NTFS-Ramdisk:	420 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	30 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	27 Sekunden
Extrahieren von Eclipse (NTFS auf TC-RD):	28 Sekunden

Name:	*HP EliteBook 8540p*
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows 7 64-Bit
RAM-Durchsatz:	2,9 GB/s
Festplattendurchsatz:	80 – 90 MB/s
TrueCrypt auf FAT-Ramdisk:	115 MB/s
TrueCrypt auf NTFS-Ramdisk:	115 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	31 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	28 Sekunden
Extrahieren von Eclipse (NTFS auf TC-RD):	29 Sekunden

Name:	*HP EliteBook 8540p*
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Energiesparmodus
Betriebssystem:	Windows 7 64-Bit
RAM-Durchsatz:	2,9 GB/s
Festplattendurchsatz:	80 – 85 MB/s
TrueCrypt auf FAT-Ramdisk:	115 MB/s
TrueCrypt auf NTFS-Ramdisk:	115 MB/s
Extrahieren von Eclipse (FAT auf unverschlüsselter RD):	30 Sekunden
Extrahieren von Eclipse (FAT auf TC-RD):	28 Sekunden
Extrahieren von Eclipse (NTFS auf TC-RD):	30 Sekunden

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows 7 64-Bit
Full-Disc-Encryption:	ein
Starten von Windows:	27 Sekunden
Herunterfahren von Windows:	9 Sekunden
Starten von Firefox.	5 Sekunden
Extrahieren von Eclipse:	25 Sekunden
Starten von Eclipse:	27 Sekunden
Starten von OpenOffice:	5 Sekunden

5.5 Full-Disc-Encryption Tests (nur Windows)

5.5.1 Acer Aspire one D250-1Bk

Ohne Full-Disc-Encryption

Name:	***Acer Aspire One***
32-Bit / 64-Bit:	32- Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows 7 Professional 32-Bit
Full-Disc-Encryption:	aus
Starten von Windows:	40 Sekunden
Herunterfahren von Windows:	13-15 Sekunden
Starten von Firefox.	14 Sekunden
Extrahieren von Eclipse:	160 Sekunden
Starten von Eclipse:	30 Sekunden
Starten von OpenOffice:	8 Sekunden

Name:	***Acer Aspire One***
32-Bit / 64-Bit:	32- Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows 7 Professional 32-Bit
Full-Disc-Encryption:	aus
Starten von Windows:	40 Sekunden
Herunterfahren von Windows:	13-15 Sekunden
Starten von Firefox.	19 Sekunden
Extrahieren von Eclipse:	240 Sekunden
Starten von Eclipse:	35 Sekunden
Starten von OpenOffice:	8 Sekunden

Mit Full-Disc-Encryption

Name:	***Acer Aspire One***
32-Bit / 64-Bit:	32- Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows 7 Professional 32-Bit
Full-Disc-Encryption:	ein
Starten von Windows:	30 Sekunden
Herunterfahren von Windows:	18 Sekunden
Starten von Firefox.	10 Sekunden
Extrahieren von Eclipse:	200 Sekunden
Starten von Eclipse:	40 Sekunden
Starten von OpenOffice:	11 Sekunden

Name:	***Acer Aspire One***
32-Bit / 64-Bit:	32- Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows 7 Professional 32-Bit
Full-Disc-Encryption:	ein
Starten von Windows:	37 Sekunden
Herunterfahren von Windows:	13-15 Sekunden
Starten von Firefox.	10 Sekunden
Extrahieren von Eclipse:	260 Sekunden
Starten von Eclipse:	35 Sekunden
Starten von OpenOffice:	14 Sekunden

5.5.2 Lenovo x61s

Ohne Full-Disc-Encryption

Name:	***Lenovo X61s***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows Vista Ultimate 64-Bit S
Full-Disc-Encryption:	aus
Starten von Windows:	25 Sekunden
Herunterfahren von Windows:	20 Sekunden
Starten von Firefox.	8 Sekunden
Extrahieren von Eclipse:	62 Sekunden
Starten von Eclipse:	22 Sekunden
Starten von OpenOffice:	8 Sekunden

Name:	***Lenovo X61s***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows Vista Ultimate 64-Bit S
Full-Disc-Encryption:	aus
Starten von Windows:	25 Sekunden
Herunterfahren von Windows:	15 Sekunden
Starten von Firefox.	10 Sekunden
Extrahieren von Eclipse:	75 Sekunden
Starten von Eclipse:	20 Sekunden
Starten von OpenOffice:	8 Sekunden

Mit Full-Disc-Encryption

Name:	***Lenovo X61s***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows Vista Ultimate 64-Bit S
Full-Disc-Encryption:	ein
Starten von Windows:	30 Sekunden
Herunterfahren von Windows:	20 Sekunden
Starten von Firefox.	8 Sekunden
Extrahieren von Eclipse:	150 Sekunden
Starten von Eclipse:	50 Sekunden
Starten von OpenOffice:	8 Sekunden

Name:	***Lenovo X61s***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows Vista Ultimate 64-Bit S
Full-Disc-Encryption:	ein
Starten von Windows:	35 Sekunden
Herunterfahren von Windows:	15 Sekunden
Starten von Firefox.	10 Sekunden
Extrahieren von Eclipse:	90 Sekunden
Starten von Eclipse:	45 Sekunden
Starten von OpenOffice:	8 Sekunden

5.5.3 HP EliteBook 8540p

Ohne Full-Disc-Encryption

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	QuadCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows 7 64-Bit
Full-Disc-Encryption:	aus
Starten von Windows:	23 – 25 Sekunden
Herunterfahren von Windows:	8-10 Sekunden
Starten von Firefox.	4 Sekunden
Extrahieren von Eclipse:	14 Sekunden
Starten von Eclipse:	22 Sekunden
Starten von OpenOffice:	5 Sekunden

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows 7 64-Bit
Full-Disc-Encryption:	aus
Starten von Windows:	23 – 25 Sekunden
Herunterfahren von Windows:	10 Sekunden
Starten von Firefox.	7 Sekunden
Extrahieren von Eclipse:	21 Sekunden
Starten von Eclipse:	23 Sekunden
Starten von OpenOffice:	5 Sekunden

Mit Full-Disc-Encryption

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	QuadCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows 7 64-Bit
Full-Disc-Encryption:	ein
Starten von Windows:	23 – 25 Sekunden
Herunterfahren von Windows:	11 Sekunden
Starten von Firefox.	7 Sekunden
Extrahieren von Eclipse:	30 Sekunden
Starten von Eclipse:	30 Sekunden
Starten von OpenOffice:	8 Sekunden

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	SingleCore
Betriebsmodus:	Höchstleistung
Betriebssystem:	Windows 7 64-Bit
Full-Disc-Encryption:	ein
Starten von Windows:	27 Sekunden
Herunterfahren von Windows:	9 Sekunden
Starten von Firefox.	5 Sekunden
Extrahieren von Eclipse:	25 Sekunden
Starten von Eclipse:	27 Sekunden
Starten von OpenOffice:	5 Sekunden

5.6 Dateisystem-Benchmarks (nur Linux)

5.6.1 Bonnie++

Acer Aspire one D250-1Bk

Name:	***Acer Aspire One***
32-Bit / 64-Bit:	32-Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Performance
Filesystem-Bonnie-Tests	**in KB/s pro Block**
EXT3 plain	51.284,00
EXT3 TrueCrypt	13.870,00
REISERFS plain	110.516,00
REISERFS TrueCrypt	17.951,00
VFAT plain	164.150,00
VFAT TrueCrypt	18.278,00
XFS plain	165.603,00
XFS TrueCrypt	19.722,00

Lenovo x61s

Name:	***Lenovo X61s***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Performance
Filesystem-Bonnie-Tests	**in KB/s pro Block**
EXT3 plain	44.948,00
EXT3 TrueCrypt	117.680,00
REISERFS plain	219.636,00
REISERFS TrueCrypt	56.294,00
VFAT plain	293.877,00
VFAT TrueCrypt	60.320,00
XFS plain	353.467,00
XFS TrueCrypt	60.510,00

HP EliteBook 8540p – 64Bit

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	ja
Anzahl Kerne:	QuadCore
Betriebsmodus:	Performance
Filesystem-Bonnie-Tests	**in KB/s pro Block**
EXT3 plain	271.176,00
EXT3 TrueCrypt	129.989,00
REISERFS plain	+++++
REISERFS TrueCrypt	220.484,00
VFAT plain	+++++
VFAT TrueCrypt	243.524,00
XFS plain	+++++
XFS TrueCrypt	254.997,00

HP EliteBook 8540p – 32Bit

Name:	***HP EliteBook 8540p***
32-Bit / 64-Bit:	32-Bit
Hardware-AES:	nein
Anzahl Kerne:	QuadCore
Betriebsmodus:	Performance
Filesystem-Bonnie-Tests	**in KB/s pro Block**
EXT3 plain	309.186,00
EXT3 TrueCrypt	75.137,00
REISERFS plain	+++++
REISERFS TrueCrypt	92.848,00
VFAT plain	+++++
VFAT TrueCrypt	93.446,00
XFS plain	+++++
XFS TrueCrypt	96.702,00

xPC Shuttle-PC G2

Name:	***xPC Shuttle***
32-Bit / 64-Bit:	64-Bit
Hardware-AES:	nein
Anzahl Kerne:	DualCore
Betriebsmodus:	Performance
Filesystem-Bonnie-Tests	**in KB/s pro Block**
EXT3 plain	180.178,00
EXT3 TrueCrypt	59.224,00
REISERFS plain	341.465,00
REISERFS TrueCrypt	94.811,00
VFAT plain	+++++
VFAT TrueCrypt	110.387,00
XFS plain	+++++
XFS TrueCrypt	109.803,00

5.6.2 Iozone

Acer Aspire one D250-1Bk

Name:	***Acer Aspire One***		
32-Bit / 64-Bit:	32-Bit		
Hardware-AES:	nein		
Anzahl Kerne:	DualCore		
Betriebsmodus:	Performance		
	plain	**TrueCrypt**	**Verlust**
	(in KB/s pro 16k-Datei)		
	EXT3	**EXT3**	
Blockgröße: 512 Byte	61.861,00	13.222,00	78,63%
Blockgröße: 1024 Byte	62.153,00	12.882,00	79,27%
Blockgröße: 2048 Byte	65.532,00	13.527,00	79,36%
Blockgröße: 4096 Byte	63.704,00	13.541,00	78,74%
Blockgröße: 8192 Byte	64.123,00	12.738,00	80,14%
Blockgröße: 16384 Byte	65.653,00	13.065,00	80,10%
	REISERFS	**REISERFS**	
Blockgröße: 512 Byte	64.022,00	13.927,00	78,25%
Blockgröße: 1024 Byte	74.603,00	15.037,00	79,84%
Blockgröße: 2048 Byte	99.619,00	15.556,00	84,38%
Blockgröße: 4096 Byte	99.963,00	17.001,00	82,99%
Blockgröße: 8192 Byte	108.603,00	17.016,00	84,33%
Blockgröße: 16384 Byte	111.346,00	17.151,00	84,60%
	VFAT	**VFAT**	
Blockgröße: 512 Byte	159.603,00	18.639,00	88,32%
Blockgröße: 1024 Byte	168.246,00	18.886,00	88,77%
Blockgröße: 2048 Byte	169.013,00	19.005,00	88,76%
Blockgröße: 4096 Byte	169.616,00	18.983,00	88,81%
Blockgröße: 8192 Byte	172.281,00	18.999,00	88,97%
Blockgröße: 16384 Byte	179.558,00	19.092,00	89,37%
	XFS	**XFS**	
Blockgröße: 512 Byte	145.633,00	17.994,00	87,64%
Blockgröße: 1024 Byte	136.945,00	18.329,00	86,62%
Blockgröße: 2048 Byte	149.587,00	18.551,00	87,60%
Blockgröße: 4096 Byte	165.984,00	17.746,00	89,31%
Blockgröße: 8192 Byte	182.335,00	17.771,00	90,25%
Blockgröße: 16384 Byte	200.700,00	18.720,00	90,67%

Lenovo x61s

Name:	***Lenovo X61s***		
32-Bit / 64-Bit:	64-Bit		
Hardware-AES:	nein		
Anzahl Kerne:	DualCore		
Betriebsmodus:	Performance		
	plain	**TrueCrypt**	**Verlust**
	(in KB/s pro 16k-Datei)		
	EXT3	**EXT3**	
Blockgröße: 512 Byte	113.578,00	37.315,00	67,15%
Blockgröße: 1024 Byte	115.468,00	37.820,00	67,25%
Blockgröße: 2048 Byte	116.254,00	40.264,00	65,37%
Blockgröße: 4096 Byte	116.233,00	40.788,00	64,91%
Blockgröße: 8192 Byte	114.812,00	42.218,00	63,23%
Blockgröße: 16384 Byte	113.903,00	42.265,00	62,89%
	REISERFS	**REISERFS**	
Blockgröße: 512 Byte	162.278,00	45.880,00	71,73%
Blockgröße: 1024 Byte	191.316,00	48.032,00	74,89%
Blockgröße: 2048 Byte	204.544,00	49.694,00	75,70%
Blockgröße: 4096 Byte	220.043,00	49.863,00	77,34%
Blockgröße: 8192 Byte	216.241,00	50.410,00	76,69%
Blockgröße: 16384 Byte	223.355,00	54.045,00	75,80%
	VFAT	**VFAT**	
Blockgröße: 512 Byte	310.092,00	59.475,00	80,82%
Blockgröße: 1024 Byte	301.038,00	59.669,00	80,18%
Blockgröße: 2048 Byte	296.876,00	60.628,00	79,58%
Blockgröße: 4096 Byte	291.852,00	61.218,00	79,02%
Blockgröße: 8192 Byte	263.904,00	61.863,00	76,56%
Blockgröße: 16384 Byte	284.222,00	56.925,00	79,97%
	XFS	**XFS**	
Blockgröße: 512 Byte	378.943,00	60.950,00	83,92%
Blockgröße: 1024 Byte	376.956,00	62.745,00	83,35%
Blockgröße: 2048 Byte	366.991,00	62.544,00	82,96%
Blockgröße: 4096 Byte	359.812,00	62.373,00	82,67%
Blockgröße: 8192 Byte	348.796,00	62.550,00	82,07%
Blockgröße: 16384 Byte	346.311,00	63.203,00	81,75%

HP EliteBook 8540p – 64Bit

Name:	***HP EliteBook 8540p***		
32-Bit / 64-Bit:	64-Bit		
Hardware-AES:	ja		
Anzahl Kerne:	QuadCore		
Betriebsmodus:	Performance		
	plain	**TrueCrypt**	**Verlust**
	(in KB/s pro 16k-Datei)		
	EXT3	**EXT3**	
Blockgröße: 512 Byte	278.786,00	138.358,00	50,37%
Blockgröße: 1024 Byte	266.601,00	138.024,00	48,23%
Blockgröße: 2048 Byte	262.437,00	138.670,00	47,16%
Blockgröße: 4096 Byte	259.138,00	137.415,00	46,97%
Blockgröße: 8192 Byte	252.914,00	139.636,00	44,79%
Blockgröße: 16384 Byte	253.175,00	140.646,00	44,45%
	REISERFS	**REISERFS**	
Blockgröße: 512 Byte	46.818,00	48.182,00	-2,91%
Blockgröße: 1024 Byte	91.014,00	86.154,00	5,34%
Blockgröße: 2048 Byte	163.858,00	96.324,00	41,21%
Blockgröße: 4096 Byte	413.164,00	126.185,00	69,46%
Blockgröße: 8192 Byte	419.574,00	149.847,00	64,29%
Blockgröße: 16384 Byte	464.597,00	155.831,00	66,46%
	VFAT	**VFAT**	
Blockgröße: 512 Byte	726.307,00	231.033,00	68,19%
Blockgröße: 1024 Byte	695.922,00	228.234,00	67,20%
Blockgröße: 2048 Byte	642.533,00	230.426,00	64,14%
Blockgröße: 4096 Byte	627.473,00	232.935,00	62,88%
Blockgröße: 8192 Byte	624.394,00	235.003,00	62,36%
Blockgröße: 16384 Byte	631.515,00	236.087,00	62,62%
	XFS	**XFS**	
Blockgröße: 512 Byte	900.426,00	247.799,00	72,48%
Blockgröße: 1024 Byte	842.927,00	243.404,00	71,12%
Blockgröße: 2048 Byte	632.660,00	150.288,00	76,25%
Blockgröße: 4096 Byte	727.114,00	222.484,00	69,40%
Blockgröße: 8192 Byte	759.643,00	249.539,00	67,15%
Blockgröße: 16384 Byte	709.810,00	252.178,00	64,47%

HP EliteBook 8540p – 32Bit

Name:	***HP EliteBook 8540p***		
32-Bit / 64-Bit:	32-Bit		
Hardware-AES:	nein		
Anzahl Kerne:	QuadCore		
Betriebsmodus:	Performance		
	plain	**TrueCrypt**	**Verlust**
	(in KB/s pro 16k-Datei)		
	EXT3	**EXT3**	
Blockgröße: 512 Byte	277.318,00	60.018,00	78,36%
Blockgröße: 1024 Byte	263.611,00	70.802,00	73,14%
Blockgröße: 2048 Byte	249.843,00	59.243,00	76,29%
Blockgröße: 4096 Byte	252.839,00	72.408,00	71,36%
Blockgröße: 8192 Byte	250.973,00	72.283,00	71,20%
Blockgröße: 16384 Byte	256.842,00	72.741,00	71,68%
	REISERFS	**REISERFS**	
Blockgröße: 512 Byte	123.960,00	63.949,00	48,41%
Blockgröße: 1024 Byte	256.452,00	63.926,00	75,07%
Blockgröße: 2048 Byte	274.209,00	73.108,00	73,34%
Blockgröße: 4096 Byte	345.602,00	78.823,00	77,19%
Blockgröße: 8192 Byte	421.953,00	83.990,00	80,09%
Blockgröße: 16384 Byte	475.879,00	84.143,00	82,32%
	VFAT	**VFAT**	
Blockgröße: 512 Byte	650.522,00	87.974,00	86,48%
Blockgröße: 1024 Byte	617.891,00	87.547,00	85,83%
Blockgröße: 2048 Byte	571.131,00	87.667,00	84,65%
Blockgröße: 4096 Byte	563.779,00	87.705,00	84,44%
Blockgröße: 8192 Byte	552.896,00	87.894,00	84,10%
Blockgröße: 16384 Byte	517.483,00	87.365,00	83,12%
	XFS	**XFS**	
Blockgröße: 512 Byte	854.805,00	91.654,00	89,28%
Blockgröße: 1024 Byte	799.569,00	91.509,00	88,56%
Blockgröße: 2048 Byte	722.524,00	91.436,00	87,34%
Blockgröße: 4096 Byte	697.991,00	91.719,00	86,86%
Blockgröße: 8192 Byte	707.916,00	92.195,00	86,98%

xPC Shuttle-PC G2

Name:	***xPC Shuttle***		
32-Bit / 64-Bit:	64-Bit		
Hardware-AES:	nein		
Anzahl Kerne:	DualCore		
Betriebsmodus:	Performance		
	plain	**TrueCrypt**	**Verlust**
	(in KB/s pro 16k-Datei)		
	EXT3	**EXT3**	
Blockgröße: 512 Byte	153.779,00	57.662,00	62,50%
Blockgröße: 1024 Byte	145.779,00	58.712,00	59,73%
Blockgröße: 2048 Byte	144.320,00	59.787,00	58,57%
Blockgröße: 4096 Byte	148.589,00	60.028,00	59,60%
Blockgröße: 8192 Byte	148.541,00	57.288,00	61,43%
Blockgröße: 16384 Byte	176.637,00	59.915,00	66,08%
	REISERFS	**REISERFS**	
Blockgröße: 512 Byte	51.211,00	51.188,00	0,04%
Blockgröße: 1024 Byte	102.699,00	51.196,00	50,15%
Blockgröße: 2048 Byte	205.359,00	68.297,00	66,74%
Blockgröße: 4096 Byte	206.254,00	82.068,00	60,21%
Blockgröße: 8192 Byte	278.762,00	82.338,00	70,46%
Blockgröße: 16384 Byte	332.899,00	82.234,00	75,30%
	VFAT	**VFAT**	
Blockgröße: 512 Byte	467.699,00	104.008,00	77,76%
Blockgröße: 1024 Byte	502.607,00	103.510,00	79,41%
Blockgröße: 2048 Byte	486.172,00	102.229,00	78,97%
Blockgröße: 4096 Byte	460.911,00	104.094,00	77,42%
Blockgröße: 8192 Byte	451.128,00	104.753,00	76,78%
Blockgröße: 16384 Byte	425.516,00	103.004,00	75,79%
	XFS	**XFS**	
Blockgröße: 512 Byte	485.482,00	98.580,00	79,69%
Blockgröße: 1024 Byte	455.845,00	102.380,00	77,54%
Blockgröße: 2048 Byte	500.397,00	105.996,00	78,82%
Blockgröße: 4096 Byte	523.298,00	103.363,00	80,25%
Blockgröße: 8192 Byte	526.054,00	106.158,00	79,82%
Blockgröße: 16384 Byte	516.812,00	96.645,00	81,30%

6 Zusammenfassung und Empfehlungen

Ziel dieses Arbeitspaketes war es, die Auswirkungen durch den Einsatz der Festplattenverschlüsselung TrueCrypt hinsichtlich der benötigten Ressourcen als auch der zusätzlichen zeitlichen Aufwände zu untersuchen. Hierzu wurden verschiedene Tests auf unterschiedlich performanten Plattformen (Netbook, Laptop, Desktop-PC) unter den Betriebssystemen Windows und Linux durchgeführt.

Im Rahmen mehrerer Testszenarien wurden sowohl reine Benchmarks durchgeführt, als auch die für einen Benutzer merkbaren Auswirkungen durch den Einsatz einer Verschlüsselungssoftware – insbesondere während des Einsatzes einer Full-Disc-Encryption – untersucht.

Folgende Ergebnisse sind dabei hervorzuheben:

- Es zeigt sich, dass mit dem Einsatz von Verschlüsselung und dem damit einhergehenden Verlust von DMA ein erheblicher Performanceverlust in Höhe von >90% einhergeht. Dies gilt für alle Plattformen und beide Betriebssysteme Windows und Linux.
- Je nach eingesetztem Dateisystem reduziert sich der Performance-Verlust auf 50-80%. Vor allem interessant sind hier Dateisysteme mit einer großen Blockgröße (d.h. >512 Byte).
- Beim Einsatz von TrueCrypt zur Full-Disc-Encryption unter Windows:
  - Das Hoch- und Herunterfahren von Windows ist nahezu unabhängig von dem Einsatz einer Verschlüsselung.
  - Das Starten von Anwendungen aus dem Benutzerkontext bedeutet einen zeitlichen Mehraufwand in der Größenordnung von 30-50%.
  - Ebenso sind Dateizugriffe um diesen Faktor langsamer.
- Der Einsatz von AES-Hardwarebeschleunigung bringt einen Geschwindigkeitsvorteil von ca. 500% bei der reinen Ausführung der Algorithmen. Im echten Einsatz auf Dateisystemebene liegt der Geschwindigkeitsvorteil zwar nur noch bei 70-80%, für den Benutzer bedeutet dies jedoch, dass der Einsatz von Verschlüsselung subjektiv nicht bemerkbar ist.
- Der Geschwindigkeitsvorteil beim Einsatz von MultiCore-Systemen liegt im Schnitt bei 80-120%. Es gibt allerdings Ausnahmen, in denen der Overhead durch den Einsatz von MultiCore zu einer langsameren Performance führt. Dies ist immer dann der Fall, wenn auf Daten zugegriffen wird, die kleiner sind als eine Kernelseite (in der Regel 4096 Byte = 4kB). So sind automatisch Dateisysteme mit einer Blockgröße in Höhe einer Sektorgröße (512 Byte) für den Einsatz bei MultiCore-Systemen inperformanter als bei SingleCore-Systemen.
- Das Verhältnis des Datendurchsatzes in Abhängigkeit von der CPU-Taktrate ist nahezu linear.
- Der Speicherbedarf von TrueCrypt auf der Festplatte ist vernachlässigbar.

Einzige Ausnahme stellt der Einsatz in einer Initrd unter Linux dar. Hier sollte TrueCrypt manuell so kompiliert werden, dass ein statisches Programm erzeugt wird.

- Der Arbeitsspeicherbedarf von TrueCrypt liegt grob bei ca. 20-30 MB RAM.

Die Benchmark-Ergebnisse zeigen, dass der Datendurchsatz bei Computern mit modernen CPUs (wie bei HP EliteBook oder xPC Shuttle) groß genug ist, um eine Festplattenverschlüsselung einzusetzen, da hier jeweils der Datendurchsatz über dem der jeweiligen Festplatte liegt, sodass kaum Performanceeinbußen vor allem beim Einsatz einer Full-Disc-Encryption zu erwarten sind. Auf der anderen Seite zeigt sich aber auch, dass bei langsamen Systemen wie Netbooks (Acer Aspire One) der Einsatz von Verschlüsselung das System extrem ausbremsen kann, vor allem wenn das System batterieschonend betrieben wird.

Solange die effektive Geschwindigkeit durch den Einsatz von Verschlüsselung dennoch höher ist als die Geschwindigkeit der verwendeten Festplatte, ist der Einsatz einer Verschlüsselung ohne merkbare Verluste für den Benutzer möglich.

In jedem Falle ist der Einsatz einer Hardwarebeschleunigung zu empfehlen, um die Performanceverluste durch den Wegfall von DMA einigermaßen wieder auszugleichen.