AAB02: OS Ressourcen unter Windows und Linux im Vergleich

Fabio Plunser
Betreuer : Walter Mueller

February 4, 2020

Inhaltsverzeichnis

Abbildungsverzeichnis

AAB02: OS Ressourcen unter Windows und Linux im Vergleich

0.1 Welche Ressourcen verwaltet ein/das Betriebssystem?

Festplattenspeicher, RAM, CPU, GPU, Netzwerk

0.2 Beschreibe den unterschied zwischen Programm / Prozess / Thread

Es gibt zwei verschiedene Arten von Threads.

- Threads im engeren Sinne, die sogenannten Kernel-Threas, laufen ab unter Steuerung durch das Betriebssystem.
- Im Gegensatz dazu stehen die sogenannten User-Threads, die das Computerprogramm des Anwenders komplett selbst verwalten muss.

Ein (Kernel-) Thread ist ein sequentieller Abarbeitungslauf innerhalb eines Prozesses und teilt sich mit den anderen vorhanden Threads (multithreading) des zugehörigen Prozesses eine Reihe von Betriebsmitteln: Jedes ausgeführte Programm ist ein Prozess, der Arbeitsspeicher belegt und bei Bedarf den Prozessor nutzt. Viele Programme wie Chrome brauchen mehrere Prozesse, da jeder Tab einen eigenen Prozess belegt. Jedoch läuft in den meisten Fällen für eine bestimmte Anwendung nur ein Prozess. Es ist egal wie oft Word geöffnet wird alle Word-Instanzen spiegeln sich in einem einzigen Prozess namens ”WINDWORD:EXE” wieder.

Auch jeder Dienst ist ein Prozess. Im Unterschied zu eine Programm wartet ein Dienst im Hintergrund darauf, dass es benötigt wird, sei es vom Anwender oder von einem anderen Programm. Prozesse, die durch aktive Dienste entstehen, erkennen Sie in der Prozessliste in der Regel am Besitzer ”System”. Außerdem hat ein Dienst keine Schnittstelle zum Benutzer, kann also nicht direkt mit im Interagieren.

In Windws heißen Prozesse Taks deswegen heißt es auch Task-Manager und nicht Prozess-Manager

0.3 Starte ein konkretes Programm unter Windows sowie unter Linux beantworte damit die folgenden Fragen

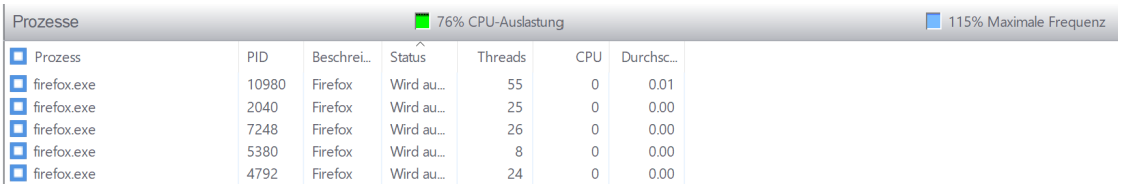
0.3.1 Welches Programm beobachtest du?

- WIN: Firefox
- Linux: Standardbrowser (Firefox)

1 Tab CPU (RM)

1.1 Was bedeuten die Spalten?

1.1.1 WIN:



Prozess	PID	Beschrei...	Status	Threads	CPU	Durchsc...
firefox.exe	10980	Firefox	Wird au...	55	0	0.01
firefox.exe	2040	Firefox	Wird au...	25	0	0.00
firefox.exe	7248	Firefox	Wird au...	26	0	0.00
firefox.exe	5380	Firefox	Wird au...	8	0	0.00
firefox.exe	4792	Firefox	Wird au...	24	0	0.00

Figure 1: RM-Spalten

- PID = Process ID
- Beschreibung = Beschreibung des Prozesses
- Status = Programm wird ausgeführt, ist angehalten
- Threads = wie viele Threads benötigt der Prozess
- CPU = auf welchem CPU-Kern der Prozess läuft
- Durchschnittliche CPU-Auslastung = genau das was es beschreibt

1.1.2 Linux:

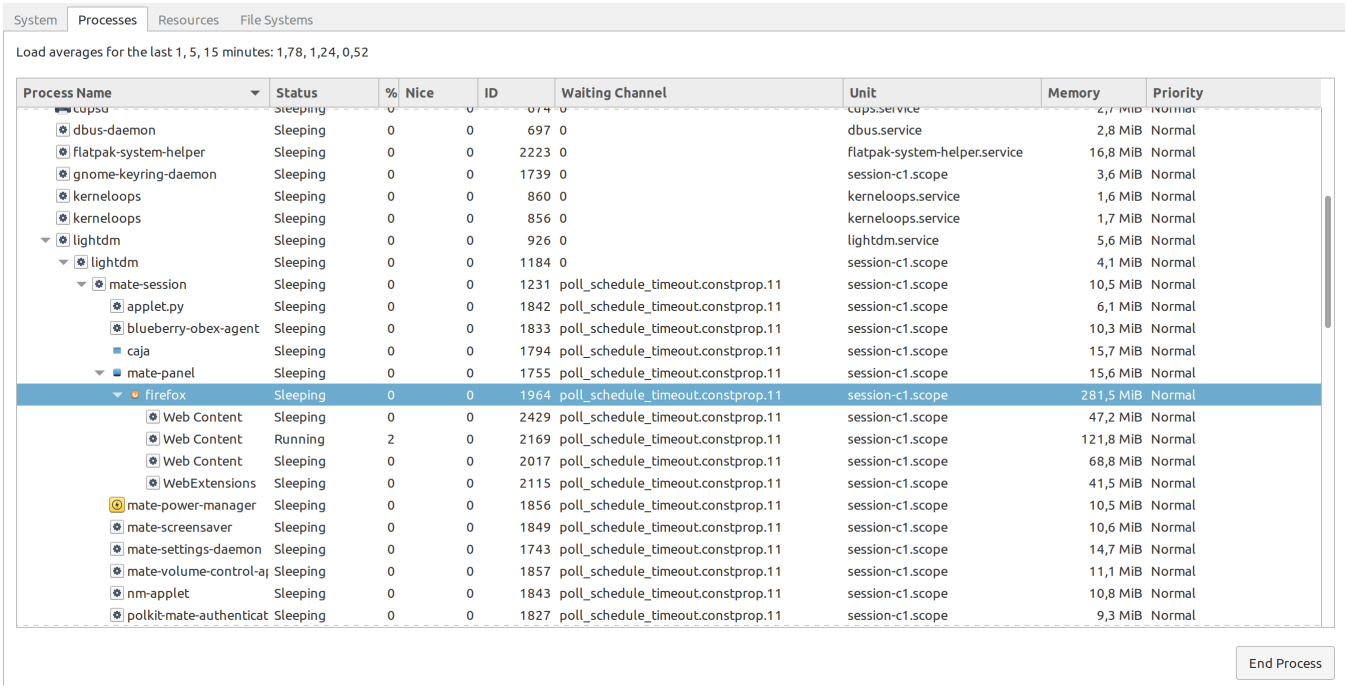


Figure 2: Linux-System-Monitor

- Status = ob das Programm läuft oder auf standby ist
- 2. Spalte = CPU = auf welchem CPU-Kern der Prozess läuft
- Nice = Priorität auf der CPU
- ID = PID bei Windows
- Waiting Channel = poll-schedule-timeout zeigt an das ein Programm auf einen IO input wartet. Entweder per Tastatur und Maus, Sound Geräte oder auch Netzwerk sockets.
- Unit = keine genaue Erklärung gefunden
- Memory = Gebrauchter RAM
- Priority = Priorität

1.2 Welche Ressourcen benötigt das von dir gestartete Programm?

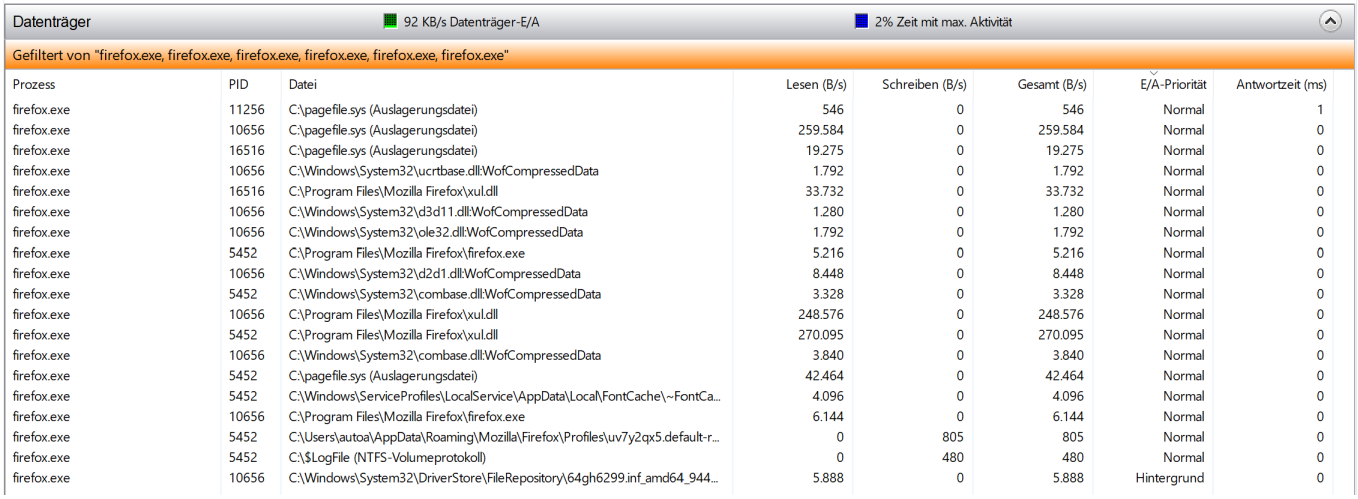
1.2.1 Win:

CPU 69% CPU-Auslastung 111% Maximale Frequenz

Prozess	PID	Beschreibung	Status	Threads	CPU	Durchschnittliche...	Benutzername
firefox.exe	5452	Firefox	Wird ausgeführt	56	0	0.01	autoa
firefox.exe	10656	Firefox	Wird ausgeführt	25	0	0.00	autoa
firefox.exe	11256	Firefox	Wird ausgeführt	24	0	0.00	autoa
firefox.exe	16516	Firefox	Wird ausgeführt	8	0	0.00	autoa
firefox.exe	12512	Firefox	Wird ausgeführt	19	0	0.00	autoa

Figure 3: Firefox-CPU

Firefox benötigt, ohne eine Seite geladen zu haben, 5 Prozesse. Mit insgesamt 152 Threads.



Datenträger — 92 KB/s Datenträger-E/A — 2% Zeit mit max. Aktivität

Gefiltert von "firefox.exe, firefox.exe, firefox.exe, firefox.exe, firefox.exe, firefox.exe"

Prozess	PID	Datei	Lesen (B/s)	Schreiben (B/s)	Gesamt (B/s)	E/A-Priorität	Antwortzeit (ms)
firefox.exe	11256	C:\pagefile.sys (Auslagerungsdatei)	546	0	546	Normal	1
firefox.exe	10656	C:\pagefile.sys (Auslagerungsdatei)	259.584	0	259.584	Normal	0
firefox.exe	16516	C:\pagefile.sys (Auslagerungsdatei)	19.275	0	19.275	Normal	0
firefox.exe	10656	C:\Windows\System32\ucrtbase.dll:WofCompressedData	1.792	0	1.792	Normal	0
firefox.exe	16516	C:\Program Files\Mozilla Firefox\xul.dll	33.732	0	33.732	Normal	0
firefox.exe	10656	C:\Windows\System32\d3d11.dll:WofCompressedData	1.280	0	1.280	Normal	0
firefox.exe	10656	C:\Windows\System32\ole32.dll:WofCompressedData	1.792	0	1.792	Normal	0
firefox.exe	5452	C:\Program Files\Mozilla Firefox\firefox.exe	5.216	0	5.216	Normal	0
firefox.exe	10656	C:\Windows\System32\d2d1.dll:WofCompressedData	8.448	0	8.448	Normal	0
firefox.exe	5452	C:\Windows\System32\combase.dll:WofCompressedData	3.328	0	3.328	Normal	0
firefox.exe	10656	C:\Program Files\Mozilla Firefox\xul.dll	248.576	0	248.576	Normal	0
firefox.exe	5452	C:\Program Files\Mozilla Firefox\xul.dll	270.095	0	270.095	Normal	0
firefox.exe	10656	C:\Windows\System32\combase.dll:WofCompressedData	3.840	0	3.840	Normal	0
firefox.exe	5452	C:\pagefile.sys (Auslagerungsdatei)	42.464	0	42.464	Normal	0
firefox.exe	5452	C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\~FontCa...	4.096	0	4.096	Normal	0
firefox.exe	10656	C:\Program Files\Mozilla Firefox\firefox.exe	6.144	0	6.144	Normal	0
firefox.exe	5452	C:\Users\autoa\AppData\Roaming\Mozilla\Firefox\Profiles\uv7y2qx5.default-r...	0	805	805	Normal	0
firefox.exe	5452	C:\$LogFile (NTFS-Volumeprotokoll)	0	480	480	Normal	0
firefox.exe	10656	C:\Windows\System32\DriverStore\FileRepository\64gh6299.inf_amd64_944...	5.888	0	5.888	Hintergrund	0

Figure 4: Firefox-Datenträger

Firefox greift gerade auf diese Verzeichnisse bzw. Dateien zu. Diese ändern sich ständig.

Netzwerk — 6 MBit/s Netzwerk-E/A — 2% Netzwerklast

Gefiltert von "firefox.exe, firefox.exe, firefox.exe, firefox.exe, firefox.exe, firefox.exe"

Prozess	PID	Adresse	Senden (B/s)	Empfangen (B/s)	Gesamt (B/s)

Figure 5: Firefox-Netzwerk

Da Firefox gerade keine Seite lädt erscheint es in der Netzwerkaktivität nicht auf.

Arbeitsspeicher — 39 Harte Fehler/s — 78% Verwendeter phys. Speicher

Gefiltert von "firefox.exe, firefox.exe, firefox.exe, firefox.exe, firefox.exe, firefox.exe"

Prozess	PID	Harte Fehler/s	Zugesichert (KB)	Arbeitssatz (KB)	Freigabe möglich...	Privat (KB)
firefox.exe	5452	0	152.988	67.216	32.912	34.304
firefox.exe	10656	1	78.068	56.180	28.464	27.716
firefox.exe	16516	0	69.548	26.676	14.696	11.980
firefox.exe	11256	0	46.460	14.860	10.468	4.392
firefox.exe	12512	0	41.824	6.500	5.700	800

Figure 6: Firefox-Arbeitssicher

Firefox benötigt ungefähr einen halben MB RAM.

1.2.2 Linux:

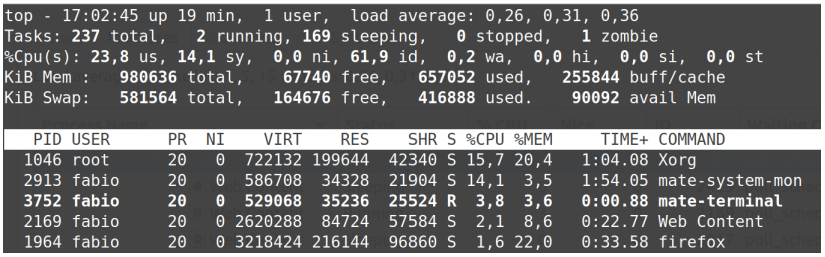


Figure 7: Linux-Firefox-Ressourcenverbrauch

Firefox benötigt:

- 1.6% CPU
- 22.0% RAM
- PID = 3752
- User= Fabio

1.3 Welchem Benutzer ist der Prozess zugeordnet? Was bedeutet das fuer den Prozess?

1.3.1 Win:

Dem Standard User des PCs = Admin

1.3.2 Linux:

Dem Standardbenutzer = Admin

1.4 Welche Betriebssystemressourcen(Handles) verwendet/belegt dein Programm?

1.4.1 Win:

- ALPC Port
- File
- Desktop
- Directory
- Event
- Key
- Mutant
- Section
- Semaphore
- WindowStation

1.4.2 Linux:

Hab dicht gefunden mit welchem Befehl man die Handles nachschauen kann.

1.5 Recherchiere im Internet einen Typ von Ressource, der dir noch unbekannt erscheint.

ALPC Port: Advanced Local Procedure Call The typical communication scenario between the server and the client is as follows:

- A server process first creates a named server connection port object, and waits for clients to connect.
- A client requests a connection to that named port by sending a connect message.
- If the server accepts the connection, two unnamed ports are created: client communication port - used by client threads to communicate with a particular server server communication port - used by the server to communicate with a particular client; one such port per client is created
- The client receives a handle to the client communication port, and server receives a handle to the server communication port, and the inter-process communication channel is established.

2 Tab Memory (RM)

2.1 Wieviel physisches Memory hat dein Computer?

2.1.1 Win:

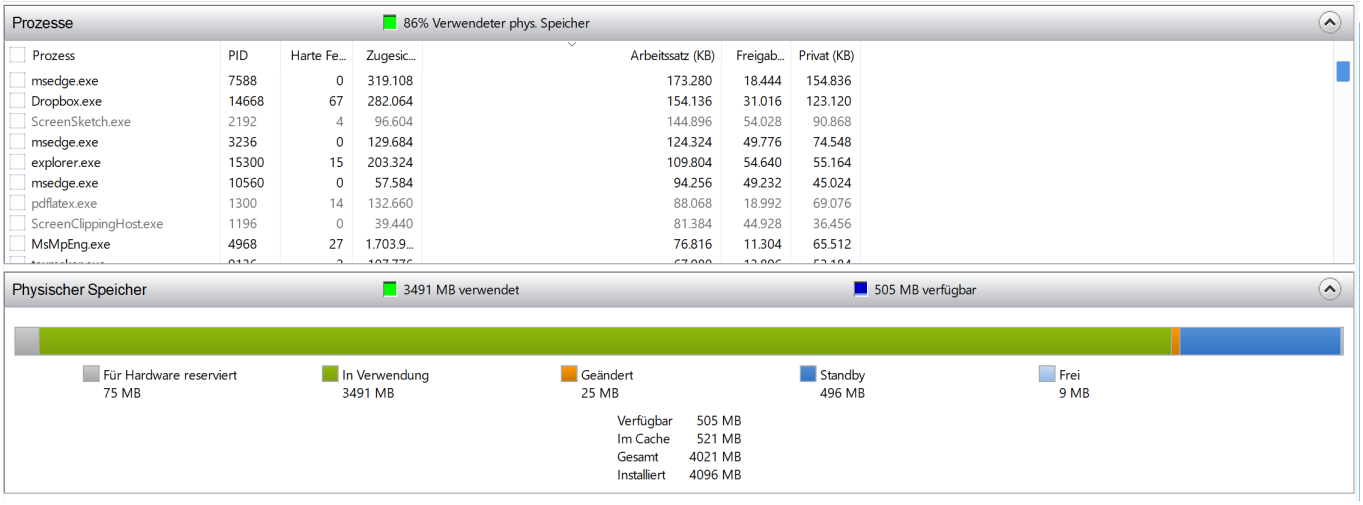


Figure 8: Arbeitssicher

4GB Ram

2.1.2 Linux:

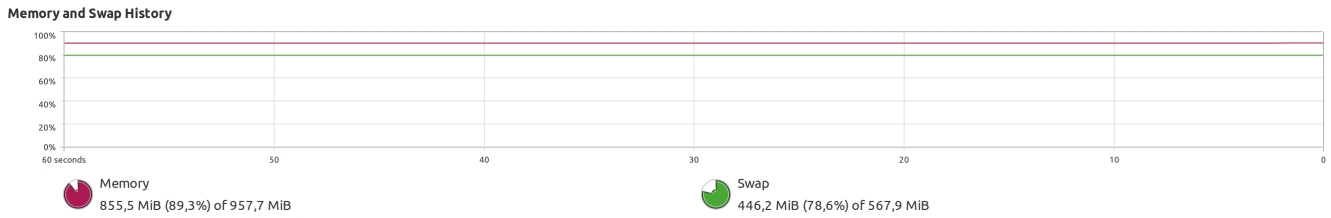


Figure 9: Linux-RAM

1GB Ram. Den ich zugewiesen habe.

2.2 Wieviel RAM ist derzeit auf deinem Computer belegt?

2.2.1 Win:

3.5GB

2.2.2 Linux:

855.5 MiB(89.3%)

2.3 Welches Programm benoetigt den meisten physikalischen Speicher?

2.3.1 Win:

Der neue (sehr tolle) Edge Browser von Microsoft.

2.3.2 Linux:

Ein Process namens Marco

2.4 Was ist eine MMU, welche Aufgaben hat die MU und wie arbeitet diese mit den Betriebssystem zusammen?

Memory Management Unit: Die Verwaltet den Zugriff auf den Arbeitsspeicher. Sie erhält Befehle und schaut ob sie valide sind und führt diese danach aus.

2.5 Was bedeutet virtuelles Memory, was ist eine Auslagerungsdatei?

Die **virtuelle Speicherverwaltung** ist eine spezielle Peicherverwaltung in einem Cmputer. Der **virutelle Speicher** bezeichnet den vom tastsächlich vorhanden Arbeitsspeicher unabghängigen Adressraum, der einem Prozess vom Betriebssystem zur Verfügung gestellt wird.

Die **Auslagerungsdatei** bzw. die **Swap-Partition** eine Partition auf einem Massenspeichermedium eines Computers, die verschiedene Betriebssysteme im Rahmen ihrer Speicherverwaltung verwenden, um Prozessen einen größeren Adressraum zur Verfügung stellen zu können als durch den physisch vorhanden Arbeitsspeicher eigentlich möglich wäre.

2.6 Was ist (Memory-)Cache? Wo befindet dieser sich meist?

Memory-Cahce ist ein kleiner super schneller Speicher (Puffer) der meistens auf extra Chips auf HDDs und SSDs sitz, oder auch direkt in der CPU. Diese Pufferspeicher der Festplatten sind vorallemfür stetige neuzugriffe auf den gleichen Prozess wichtig, da dann das Programm schneller auf die Anweisungen des Benutzer reagieren kann. Auch für Random Access auf die Datenträger wichtig, oft sind normale HDDs und SSDs zu langsa um solche Zugriffe zu Verwalten, deswegen werden sie im Cache zwischen gespeichert um die Daten danach auf die Festplatten zu schreiben.

Der Cache direkt auf der CPU ist hauptsächlich ein Puffer für den RAM. Dieser Cache Puffer ist noch sehr viel schneller wie RAM und ist in den meisten CPUs in 3 verschiedenen Layern vorhanden.

2.7 Recherchiere für deinen Prozessor wieviel Memory Cache (L1, L2, L3) verfügbar ist.

2.7.1 Win:

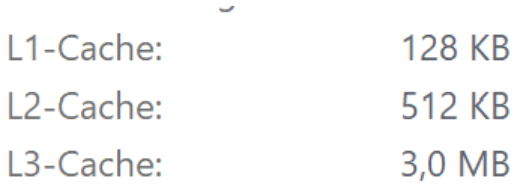


Figure 10: CPU-Cache

2.7.2 Linux:

```
Architecture:            x86_64
CPU op-mode(s):          32-bit, 64-bit
Byte Order:              Little Endian
CPU(s):                  1
On-line CPU(s) list:     0
Thread(s) per core:      1
Core(s) per socket:      1
Socket(s):               1
NUMA node(s):            1
Vendor ID:               GenuineIntel
CPU family:              6
Model:                   78
Model name:              Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz
Stepping:                3
CPU MHz:                 2495.999
BogoMIPS:                4991.99
Hypervisor vendor:       VMware
Virtualization type:     full
L1d cache:               32K
L1i cache:               32K
L2 cache:                256K
L3 cache:                3072K
NUMA node0 CPU(s):       0
Flags:                   fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_
perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hy
pervisor lahf_lm abm 3dnowprefetch cpuid_fault invpcid_single pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 hle avx2 smep bmi2 invpcid rtm mpx rdseed adx smap clflus
hopt xsaveopt xsavec xsaves arat md_clear flush_l1d arch_capabilities
```

Figure 11: Linux-Cache

- L1 cache: 32K
- L2 cache: 256K
- L3 cache: 3072K

3 Tab Datenträger (RM)

3.1 Welche Prozesse haben die höchste Datentraegeraktivität?

3.1.1 Win:

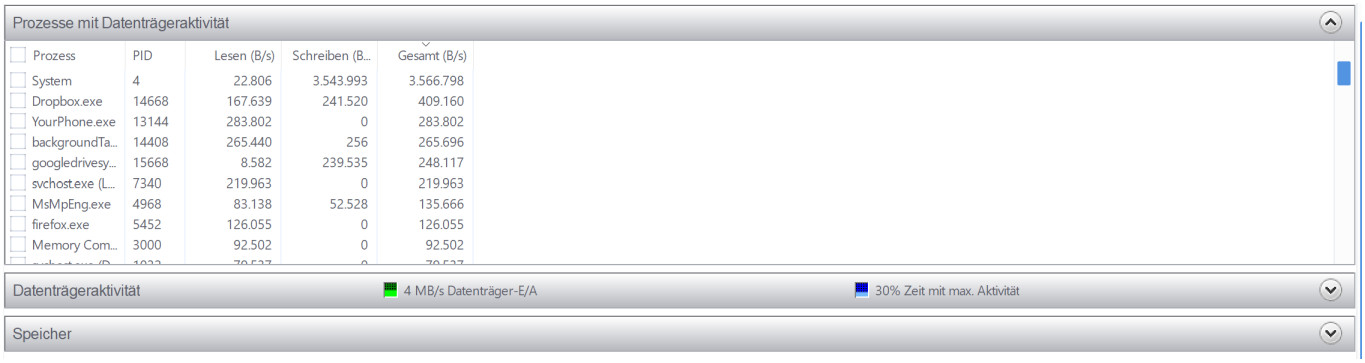


Figure 12: Datenträger-Maximale-Akitvität

Das System hat die höchste Datenträgeraktivität. Ansonsten hat es normalerweise irgendein Cloud Programm wegen Datei downloads.

3.1.2 Linux:

Weiß nicht wo ich das am besten nachschauen soll.

3.2 Dokumentiere die Aktivität des von dir gewählten Programms

3.2.1 Win:

Datenträgeraktivität — 708 KB/s Datenträger-E/A — 2% Zeit mit max. Aktivität

Gefiltert von "firefox.exe, firefox.exe, firefox.exe, firefox.exe, firefox.exe"

Prozess	PID	Datei	Lesen (B/s)	Schreiben (B...	Gesamt (B/s)	E/A-Priorität	Antwortzeit (...
firefox.exe	10980	C:\Windows\System3...	18.432	0	18.432	Normal	1
firefox.exe	10980	C:\$Mft (NTFS-Maste...	18.432	2.048	20.480	Normal	0
firefox.exe	7248	C:\Windows\System3...	10.923	0	10.923	Normal	0
firefox.exe	10980	C:\Users\autoa\AppD...	20.480	0	20.480	Normal	0
firefox.exe	10980	C:\$LogFile (NTFS-Vo...	0	41.984	41.984	Normal	0
firefox.exe	10980	C:\Windows\System3...	16.384	0	16.384	Normal	0
firefox.exe	4792	C:\pagefile.sys (Ausla...	1.118	0	1.118	Normal	0
firefox.exe	7248	C:\Windows\System3...	30.037	0	30.037	Normal	0
firefox.exe	10980	C:\Program Files\Mo...	1.126.400	0	1.126.400	Normal	0
firefox.exe	5380	C:\Program Files\Mo...	64.512	0	64.512	Normal	0
firefox.exe	7248	C:\Program Files\Mo...	2.072.576	0	2.072.576	Normal	0
firefox.exe	10980	C:\Program Files\Mo...	49.152	0	49.152	Normal	0
firefox.exe	10980	C:\Windows\System3...	6.144	0	6.144	Normal	0
firefox.exe	5380	C:\pagefile.sys (Ausla...	162.475	0	162.475	Normal	0
firefox.exe	7248	C:\Program Files\Mo...	16.384	0	16.384	Normal	0
firefox.exe	10980	C:\Windows\System3...	13.312	0	13.312	Normal	0
firefox.exe	7248	C:\pagefile.sys (Ausla...	183.987	0	183.987	Normal	0
firefox.exe	10980	C:\Program Files\Mo...	8.192	0	8.192	Normal	0
firefox.exe	7248	C:\Program Files\Mo...	466.944	0	466.944	Normal	0
firefox.exe	7248	C:\Windows\Service...	32.768	0	32.768	Normal	0
firefox.exe	10980	C:\Windows\System3...	8.192	0	8.192	Normal	0
firefox.exe	10980	C:\Windows\System3...	14.336	0	14.336	Normal	0
firefox.exe	7248	C:\Windows\System3...	32.768	0	32.768	Normal	0
firefox.exe	10980	C:\pagefile.sys (Ausla...	1.406.293	0	1.406.293	Normal	0
firefox.exe	10980	C:\Users\autoa\AppD...	10.923	0	10.923	Normal	0
firefox.exe	10980	C:\Users\autoa\AppD...	4.608	0	4.608	Normal	0
firefox.exe	7248	C:\Users\autoa\AppD...	2.048	0	2.048	Normal	0
firefox.exe	10980	C:\Users\autoa\AppD...	2.048	0	2.048	Normal	0
firefox.exe	10980	C:\Users\autoa\AppD...	0	3.072	3.072	Normal	0
firefox.exe	10980	C:\Users\autoa\AppD...	4.096	0	4.096	Normal	0

Figure 13: Firefox-Datenträgeraktivität

Ich habe zuerst die eine Seite geladen, und Firefox greift aus sehr viele Files zu. Sobald die Seite geladen wurde ist es nur mehr eine Auslagerungsdatei auf die zugegriffen wird.

3.2.2 Linux:

Weiß nicht wo ich das am besten nachschauen soll.

3.3 Kannst du dir die Bedeutung/Verwendung einzelner vom Programm verwendeter Dateien erklären?

Es werden oft auf Config files zugegriffen.

3.4 Was könnte das Programm gerade tun?

Von AppData config files laden bzw ändern. Auslagerungsdatei für RAM zuweisung.

3.5 Was findest du unter Linux über deine Datenträger heraus?

Figure 14: Linux-Datenträger

Es gibt eine Patition als ext4 die quasi die C platte ist.
Die 2GB ist eine iso9669 für eine Linux-Mint installation.

3.6 Gibt es analoges unter Windows?

Was ist gemeint mit analog? DVI und Klinke anschlüsse sind analog also muss ein Chip oder Windows die digitalen Signale übersetzen.

Was genau ist gemeint mit analoges unter Windows? Und gibt es da was? Bitte um Erklärung.

4 Tab Netzerk (RM):

4.1 Welche Netzwerkaktivitäten finden auf deinem Rechner statt?

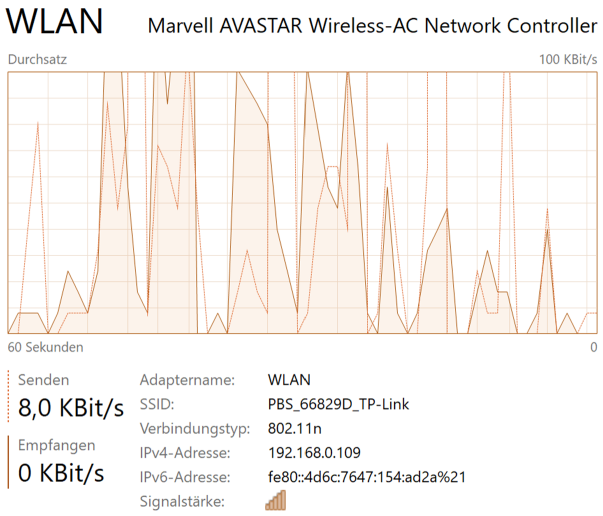


Figure 15: Win-Netzwerkaktivität

Relativ gering aber durch die durgehende Aktualisierung der Dienste im Hintergrund doch auf ompulsweise hoch.

4.1.1 Beschreibe eine TCP-Verbindung des von dir gewählten Programms.

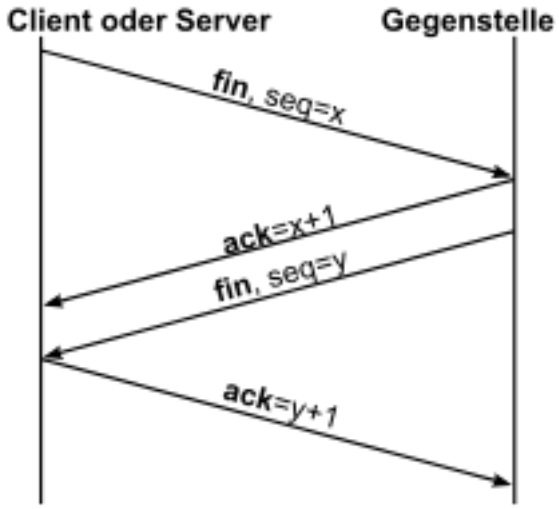
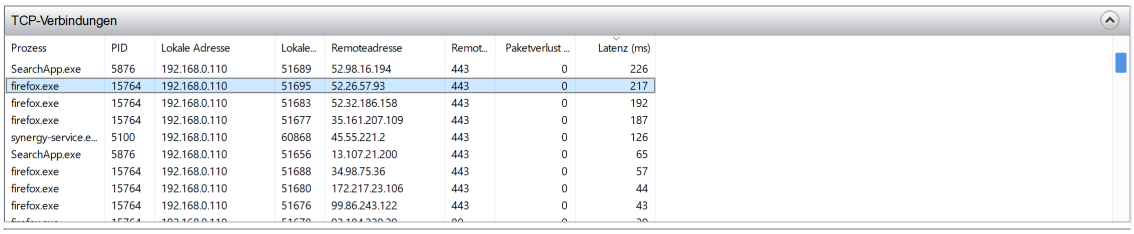


Figure 16: TCP-Verbindung

4.1.2 Beschreibe das bestimmende Quadrupel der TCP-Verbindung(SRC und DST IP, SRC und DST Port)

Verstehe die Frage nicht was ist das bestimmende Quadrupel?

4.1.3 Zwischen welchen physischen Rechnern findet die Kommunikation statt?



Prozess	PID	Lokale Adresse	Lokale...	Remoteadresse	Remot...	Paketverlust ...	Latenz (ms)
SearchApp.exe	5876	192.168.0.110	51689	52.98.16.194	443	0	226
firefox.exe	15764	192.168.0.110	51695	52.26.57.93	443	0	217
firefox.exe	15764	192.168.0.110	51683	52.32.186.158	443	0	192
firefox.exe	15764	192.168.0.110	51677	35.161.207.109	443	0	187
synergy-service.e...	5100	192.168.0.110	60868	45.55.221.2	443	0	126
SearchApp.exe	5876	192.168.0.110	51656	13.107.21.200	443	0	65
firefox.exe	15764	192.168.0.110	51688	34.98.75.36	443	0	57
firefox.exe	15764	192.168.0.110	51680	172.217.23.106	443	0	44
firefox.exe	15764	192.168.0.110	51676	99.86.243.122	443	0	43

Figure 17: TCP-Verbindungen

Lokaler Port 51695, Remoteadress 52.26.57.93, RemotePort: 443.

4.1.4 Was bedeuten die Spalten Paketverlust und Latenz?

Paketverlust = wie viele Pakete verloren gegangen sind
Latenz = die Dauer der Pakete

4.1.5 Wie viele Pakete über die gesendet oder empfangen wurden, sind verloren gegangen?

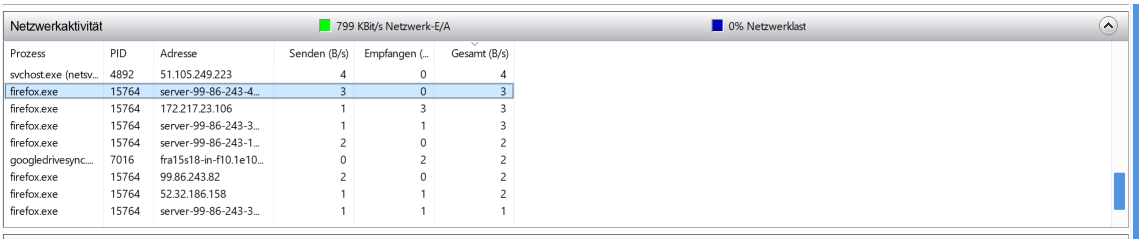


Figure 18: Gesendet und Empfangen

Ein Paar Bites wurden gesendet und Empfangen.

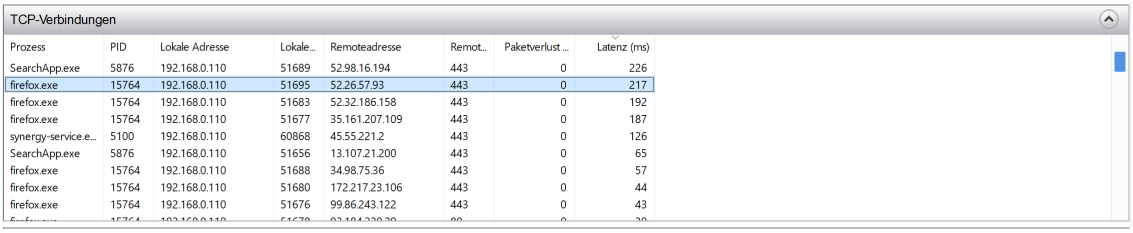


Figure 19: Paketverlust

Kein Paketverlust und 217ms Latenz.

4.1.6 Welche Art von Programme findet Ihr unter Überwachungsports?

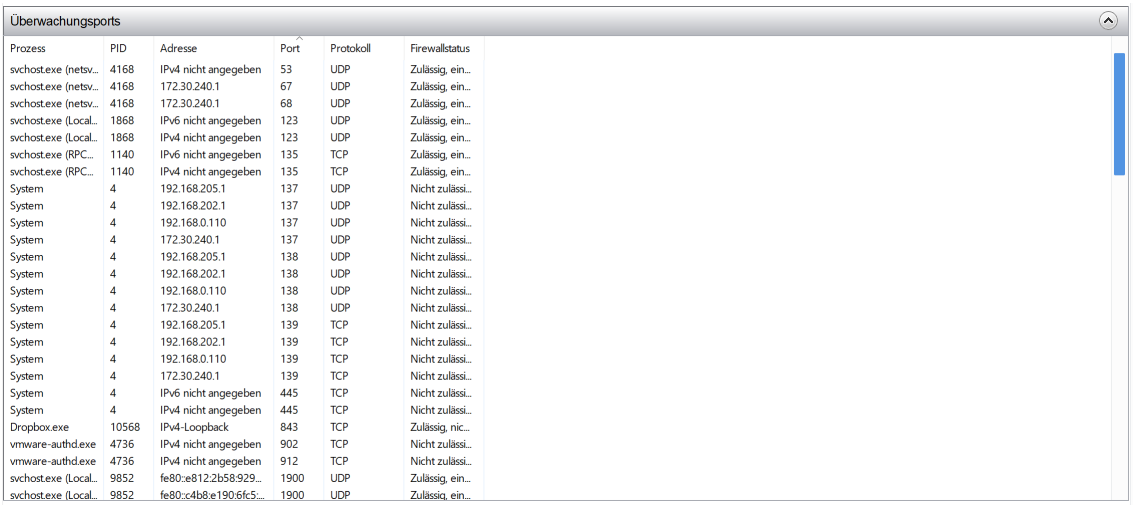


Figure 20: Überwachungsports

Überwachungsports sind Ports auf denen bestimmte Dienste warten auf Anforderungen.

4.1.7 Beschreibt eine Zeile und versucht herauszufinden welcher Dienst dahinter steckt

Hinter vmware-autd.exe steht VM Ware

4.1.8 Untersuche unter Linux den output von netstat -anp. Was findest dazu heraus?

```
fabio@fabio-virtual-machine:~$ netstat -anp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp        0      0 0.0.0.0:43264           0.0.0.0:*                           -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
udp        0      0 0.0.0.0:631             0.0.0.0:*                           -
udp        0      0 192.168.202.130:123     0.0.0.0:*                           -
udp        0      0 127.0.0.1:123           0.0.0.0:*                           -
udp        0      0 0.0.0.0:123             0.0.0.0:*                           -
udp6       0      0 :::5353                 :::*                                -
udp6       0      0 :::54304                :::*                                -
udp6       0      0 fe80::ba71:66ea:dba:123 :::*                                -
udp6       0      0 ::1:123                 :::*                                -
udp6       0      0 :::123                  :::*                                -
raw6       0      0 :::58                   :::*                    7           -
```

Figure 21: Netstat-anp

Listen = Überwachungsport