

# Forum:[Hack Forums](#)

Thread: [My Laptop is laggy as hell](#)

**King 69** - March 16, 2020, 7:14 pm

I think that I am infected because before I downloaded heaps of movies unaware of it can be infected. Also cracked programs (Adobe). I was wondering if there is any program that could help me mass uninstall programs with a program and can help me check if I am infected?

**Charger** - March 16, 2020, 7:18 pm

You installed cracked adobe. Congrats, you're 100% infected.

**King 69** - March 16, 2020, 7:19 pm

(Mar 16, 2020 07:18 PM)Charger Wrote: [\[CITE\]](#) You installed cracked adobe. Congrats, you're 100% infected.

Good day, I was unaware/innocent of viruses before. This is why I am asking for help.

**Klonopin** - March 16, 2020, 8:44 pm

(Mar 16, 2020 07:19 PM)King 69 Wrote: [\[CITE\]](#) Good day, I was unaware/innocent of viruses before. This is why I am asking for help.

Download malwarebytes and check your task manager for unwanted processes and go through your startup ect.

**BeautifulTime** - March 19, 2020, 4:25 pm

yeah...your gunna want to bring it to someone who knows what theyre doing. trust me, its wayyy safer this way

**SIM-4199941** - March 20, 2020, 2:42 pm

(Mar 16, 2020 07:14 PM)King 69 Wrote: [\[CITE\]](#) I think that I am infected because before I downloaded heaps of movies unaware of it can be infected. Also cracked programs (Adobe). I was wondering if there is any program that could help me mass uninstall programs with a program and can help me check if I am infected?

You've hidden miner, i think.

Download a good antivirus, or reset your pc (BETTER).

**SoulZeh** - March 20, 2020, 2:46 pm

I honestly feel like you should probably wait for someone that actually has decent knowledge on what could be wrong instead of listening to some of these fulls, however.. I would for sure install malwarebytes and run a full scan.

**DAMINK** - March 20, 2020, 2:50 pm

Download an illegal copy of windows then fresh install mate, lol.

I kid i kid.

Fresh install is whats needed mate.

**SoulZeh** - March 20, 2020, 2:51 pm

(Mar 20, 2020 02:50 PM)DAMINK Wrote: [\[CITE\]](#) Download an illegal copy of windows then fresh install mate, lol.

I kid i kid.

Fresh install is whats needed mate.

How even is it? I hate how people legit jump to that conclusion instantly, don't be a moron and listen to this guy, like I said in my post, just wait for someone with actual knowledge on this to post and you'll be sorted OP.

**DAMINK** - March 20, 2020, 2:52 pm

(Mar 20, 2020 02:51 PM)SoulZeh Wrote: [\[CITE\]](#) How even is it? I hate how people legit jump to that conclusion instantly, don't be a moron and listen to this guy, like I said in my post, just wait for someone with actual knowledge on this to post and you'll be sorted OP.

I did not jump to any conclusion mate, perhaps you miss read.

I SUGGESTED he get an illegal copy of windows as a joke, did not imply he already has one.

Then suggested what he really should do. Fresh install.

**SoulZeh** - March 20, 2020, 2:54 pm

(Mar 20, 2020 02:52 PM)DAMINK Wrote: [\[CITE\]](#) I did not jump to any conclusion mate, perhaps you miss read.

I SUGGESTED he get an illegal copy of windows as a joke, did not imply he already has one.

Then suggested what he really should do. Fresh install.

I wasn't even commenting on the fact you "joked" about him installing a copy of windows, I was commenting on the fact you instantly said to fresh install which is so dumb.

**DAMINK** - March 20, 2020, 2:56 pm

(Mar 20, 2020 02:54 PM)SoulZeh Wrote: [\[CITE\]](#) I wasn't even commenting on the fact you "joked" about him installing a copy of windows, I was commenting on the fact you instantly said to fresh install which is so dumb.

Given some infections pass through AV i suggested it.

A fresh install can be quicker than trying to clear infections.

Not only that windows tends to bloat on a good day so a fresh install nearly always gets the system up to speed again.

A simple answer perhaps but certainly not dumb. Cheers.

**9756502033875746737731550** - March 22, 2020, 7:35 pm

Yeah don't download cr4cked programs. Just get the original version or a trial or something.

**King 69** - March 27, 2020, 12:44 am

Hello thank you for the help everyone! I am currently running a scan on my malwarebytes premium trial since I cannot afford the premium one!

**Bastille** - March 27, 2020, 4:17 am

(Mar 27, 2020 12:44 AM)King 69 Wrote: [\[CITE\]](#) Hello thank you for the help everyone! I am currently running a scan on my malwarebytes premium trial since I cannot afford the premium one!

Hello buddy,

Let me know (in the thread) if you need further help after the Malwarebytes scan

Have a nice day

**King 69** - March 29, 2020, 5:25 am

(Mar 27, 2020 04:17 AM)Yseurk Wrote: [\[CITE\]](#) Hello buddy,

Let me know (in the thread) if you need further help after the Malwarebytes scan

Have a nice day

hello my scan showed me I have 34 infections which about 5 of them were malware. I have no idea what the files are and since my malwarebytes is free I couldn't remove virus. help

**Bastille** - March 29, 2020, 5:59 am

You can remove those viruses even with the the non premium version.

Can you send me the report of malwarebytes please ?

Can you also run Adwcleaner <https://fr.malwarebytes.com/adwcleaner/>

Send me the report as well and remove all things shown by malwarebytes and adwcleaner (except bloatware for adwcleaner)

**King 69** - March 29, 2020, 9:22 pm

I wasn't sure how to send the report but here is a screenshot

<http://prntscr.com/rp6eyz>

<http://prntscr.com/rp6fi3>

one of several

<https://pastebin.com/EYLy1Sp2>

<http://prntscr.com/rp6gb2>

should I be also quarantining these files?

**Bastille** - March 30, 2020, 12:07 am

(Mar 29, 2020 09:22 PM)King 69 Wrote: [\[CITE\]](#) I wasn't sure how to send the report but here is a screenshot

<http://prntscr.com/rp6eyz>

<http://prntscr.com/rp6fi3>

one of several

<https://pastebin.com/EYLy1Sp2>

<http://prntscr.com/rp6gb2>

should I be also quarantining these files?

Please quote me when you reply, like I do now, otherwise I'll not be notified by your reply.

Thanks for the report, pastebin is a good way to do that. Seems malwarebytes and adwcleaner found lot of things, good.

Concerning the bloatware it's not a have to, I mean : a bloatware is a preinstalled software from the company which can causes lags, open lot of pop-ups regarding their products, or warranties, etc ... So adwcleaner can uninstall them, however in these bloatware there is useful utilities to manage some components, so I wouldn't recommend to uninstall them.

If you didn't already do, please delete all elements in quarantine now.

Regarding uTorrent please use qBittorrent instead.

I see a "Virus/Joke" folder, don't know what you are trying to do but be aware that dealing with malware is not a safe thing, the proof is you are asking help here. Even if sometimes people

propose you "fake malware" , just to prank your friends or whatever, avoid. Most of them seems fake but are real and your computer is infected.

**King 69** - March 30, 2020, 3:39 am

(Mar 30, 2020 12:07 AM)Yseurk Wrote: [\[CITE\]](#) Please quote me when you reply, like I do now, otherwise I'll not be notified by your reply.

Thanks for the report, pastebin is a good way to do that. Seems malwarebytes and adwcleaner found lot of things, good.

Concerning the bloatware it's not a have to, I mean : a bloatware is a preinstalled software from the company which can causes lags, open lot of pop-ups regarding their products, or warranties, etc ... So adwcleaner can uninstall them, however in these bloatware there is useful utilities to manage some components, so I wouldn't recommend to uninstall them.

If you didn't already do, please delete all elements in quarantine now.

Regarding uTorrent please use qBittorent instead.

I see a "Virus/Joke" folder, don't know what you are trying to do but be aware that dealing with malware is not a safe thing, the proof is you are asking help here. Even if sometimes people propose you "fake malware" , just to prank your friends or whatever, avoid. Most of them seems fake but are real and your computer is infected.

Ah yes it's my folder name I was unable to change it because some of my downloads are directly downloaded there and if I change the name of the folder, a new folder will automatically appear.

How do I get the malware out of my computer without reformatting it? I can't reformat now because first I do not know how and I don't have a cd that has microsoft and second I have photo memories that I cannot transfer since I cannot afford to buy a external hardware.

**Bastille** - March 30, 2020, 3:50 am

(Mar 30, 2020 03:39 AM)King 69 Wrote: [\[CITE\]](#) Ah yes it's my folder name I was unable to change it because some of my downloads are directly downloaded there and if I change the name of the folder, a new folder will automatically appear.

How do I get the malware out of my computer without reformatting it? I can't reformat now because first I do not know how and I don't have a cd that has microsoft and second I have photo memories that I cannot transfer since I cannot afford to buy a external hardware.

Don't remember exactly the process but when Malwarebytes find something you can select it and then place it in quarantine I guess, then go to quarantine, select every junks, and then click delete

Don't have to reformat your computer

**Tilcayo** - March 30, 2020, 12:10 pm

(Mar 29, 2020 09:22 PM)King 69 Wrote: [\[CITE\]](#) I wasn't sure how to send the report but here is a screenshot

<http://prntscr.com/rp6eyz>

<http://prntscr.com/rp6fi3>

one of several

<https://pastebin.com/EYLy1Sp2>

<http://prntscr.com/rp6gb2>

should I be also quarantining these files?

Additionally, go to cmd and run it as admin, type "netstat -bo" and wait a few minutes, then either

screenshot the results or copy-paste it here in a code block so we can see if there's any weird process with a connection.

Some rootkits can hide their use of the network and may not show in a tcpview/netstat, there's a way around this though if you also have another device, you can run wireshark on that and see if you're getting lots of suspicious packets outbound from your infected device that don't correspond with a local listening port, for example if you're seeing alot of packets from a remote port 32,000 to port 4444 on your infected device, but the infected device says it isn't listening on 4444, then you most likely have a kernel rootkit problem, hopefully that's not the case and Malwarebytes killed everything.

King 69 - March 31, 2020, 12:45 am

(Mar 30, 2020 12:10 PM)size\_t Wrote: [\[CITE\]](#) Additionally, go to cmd and run it as admin, type "netstat -bo" and wait a few minutes, then either screenshot the results or copy-paste it here in a code block so we can see if there's any weird process with a connection.

Some rootkits can hide their use of the network and may not show in a tcpview/netstat, there's a way around this though if you also have another device, you can run wireshark on that and see if you're getting lots of suspicious packets outbound from your infected device that don't correspond with a local listening port, for example if you're seeing alot of packets from a remote port 32,000 to port 4444 on your infected device, but the infected device says it isn't listening on 4444, then you most likely have a kernel rootkit problem, hopefully that's not the case and Malwarebytes killed everything. Good day! I wasn't able to understand the last instruction that you gave about wireshark thing but here is the code of the cmd

Code Microsoft Windows [Version 10.0.17134.1246]

(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat -bo

#### Active Connections

| Proto                       | Local Address       | Foreign Address         | State       | PID  |
|-----------------------------|---------------------|-------------------------|-------------|------|
| TCP                         | 192.168.100.6:49686 | 52.139.250.253:https    | ESTABLISHED | 4536 |
| WpnService<br>[svchost.exe] |                     |                         |             |      |
| TCP                         | 192.168.100.6:49746 | 172.217.194.188:5228    | ESTABLISHED | 8804 |
| [chrome.exe]                |                     |                         |             |      |
| TCP                         | 192.168.100.6:49748 | 40.119.211.203:https    | ESTABLISHED | 8664 |
| [OneDrive.exe]              |                     |                         |             |      |
| TCP                         | 192.168.100.6:49764 | 40.81.91.45:https       | TIME_WAIT   | 0    |
| TCP                         | 192.168.100.6:49772 | 74:https                | ESTABLISHED | 7072 |
| [Video.UI.exe]              |                     |                         |             |      |
| TCP                         | 192.168.100.6:49773 | 40.81.30.101:https      | TIME_WAIT   | 0    |
| TCP                         | 192.168.100.6:49779 | kul09s12-in-f2:https    | TIME_WAIT   | 0    |
| TCP                         | 192.168.100.6:49784 | kul08s10-in-f10:https   | ESTABLISHED | 8804 |
| [chrome.exe]                |                     |                         |             |      |
| TCP                         | 192.168.100.6:49785 | gap-prime-finance:https | TIME_WAIT   | 0    |
| TCP                         | 192.168.100.6:49791 | 117.18.237.29:http      | TIME_WAIT   | 0    |
| TCP                         | 192.168.100.6:49792 | 52.114.75.149:https     | TIME_WAIT   | 0    |
| TCP                         | 192.168.100.6:49793 | 20.189.73.166:https     | TIME_WAIT   | 0    |
| TCP                         | 192.168.100.6:49794 | 52.114.128.9:https      | TIME_WAIT   | 0    |
| TCP                         | 192.168.100.6:49795 | gap-prime-finance:https | TIME_WAIT   | 0    |
| TCP                         | 192.168.100.6:49796 | 52.114.128.9:https      | TIME_WAIT   | 0    |

```

TCP 192.168.100.6:49799 23.102.236.172:https TIME_WAIT 0
TCP 192.168.100.6:49801 a23-67-57-201:http TIME_WAIT 0
TCP 192.168.100.6:49803 67.24.9.254:http TIME_WAIT 0
TCP 192.168.100.6:49804 67.24.15.254:http TIME_WAIT 0
TCP 192.168.100.6:49805 52.229.174.29:https ESTABLISHED 4116
DoSvc
[svchost.exe]
TCP 192.168.100.6:49808 kul06s11-in-f42:https ESTABLISHED 8804
[chrome.exe]
TCP 192.168.100.6:49811 67.27.41.254:http TIME_WAIT 0
TCP 192.168.100.6:49813 67.24.11.254:http TIME_WAIT 0
^C
C:\WINDOWS\system32>

```

Tilcayo - March 31, 2020, 12:57 am

(Mar 31, 2020 12:45 AM)King 69 Wrote: [CITE](#) Good day! I wasn't able to understand the last instruction that you gave about wireshark thing but here is the code of the cmd  
Code Microsoft Windows [Version 10.0.17134.1246]  
(c) 2018 Microsoft Corporation. All rights reserved.

```
C:\WINDOWS\system32>netstat -bo
```

#### Active Connections

```

Proto Local Address          Foreign Address         State           PID
TCP 192.168.100.6:49686 52.139.250.253:https ESTABLISHED    4536
WpnService
[svchost.exe]
TCP 192.168.100.6:49746 172.217.194.188:5228 ESTABLISHED    8804
[chrome.exe]
TCP 192.168.100.6:49748 40.119.211.203:https ESTABLISHED    8664
[OneDrive.exe]
TCP 192.168.100.6:49764 40.81.91.45:https TIME_WAIT      0
TCP 192.168.100.6:49772 74:https ESTABLISHED    7072
[Video.UI.exe]
TCP 192.168.100.6:49773 40.81.30.101:https TIME_WAIT      0
TCP 192.168.100.6:49779 kul09s12-in-f2:https TIME_WAIT      0
TCP 192.168.100.6:49784 kul08s10-in-f10:https ESTABLISHED    8804
[chrome.exe]
TCP 192.168.100.6:49785 gap-prime-finance:https TIME_WAIT      0
TCP 192.168.100.6:49791 117.18.237.29:http TIME_WAIT      0
TCP 192.168.100.6:49792 52.114.75.149:https TIME_WAIT      0
TCP 192.168.100.6:49793 20.189.73.166:https TIME_WAIT      0
TCP 192.168.100.6:49794 52.114.128.9:https TIME_WAIT      0
TCP 192.168.100.6:49795 gap-prime-finance:https TIME_WAIT      0
TCP 192.168.100.6:49796 52.114.128.9:https TIME_WAIT      0
TCP 192.168.100.6:49799 23.102.236.172:https TIME_WAIT      0
TCP 192.168.100.6:49801 a23-67-57-201:http TIME_WAIT      0
TCP 192.168.100.6:49803 67.24.9.254:http TIME_WAIT      0
TCP 192.168.100.6:49804 67.24.15.254:http TIME_WAIT      0
TCP 192.168.100.6:49805 52.229.174.29:https ESTABLISHED    4116
DoSvc
[svchost.exe]

```

```
TCP 192.168.100.6:49808 kul06s11-in-f42:https ESTABLISHED 8804
[chrome.exe]
TCP 192.168.100.6:49811 67.27.41.254:http TIME_WAIT 0
TCP 192.168.100.6:49813 67.24.11.254:http TIME_WAIT 0
^C
```

C:\WINDOWS\system32>

Great, how long did you wait though as I can see you canceled it, hopefully you gave it 5 minutes or so.. everything looks good there, but you should reset your chrome browser incase you have some malicious addons, but other than that it looks clean, you're good. :)

EDIT: You need to update windows, you're using a build from January 14, 2020, make sure you keep updating windows when prompted, they're not doing it to annoy you they're doing it because their product is defective and they want to fix it!

If you notice any suspicious behavior make sure you post back here.

**King 69** - March 31, 2020, 12:59 am

(Mar 31, 2020 12:57 AM)size\_t Wrote: [\[CITE\]](#) Great, how long did you wait though as I can see you canceled it, hopefully you gave it 5 minutes or so.. everything looks good there, but you should reset your chrome browser incase you have some malicious addons, but other than that it looks clean, you're good. :)

If you notice any suspicious behavior make sure you post back here.  
I thought it was the end already but it wasn't moving when I saw it thats why.  
Thank you for the help!

**Bastille** - March 31, 2020, 1:56 am

(Mar 31, 2020 12:59 AM)King 69 Wrote: [\[CITE\]](#) I thought it was the end already but it wasn't moving when I saw it thats why.  
Thank you for the help!  
Your welcome

If you feel the problem is solved, please don't forget to close the thread :)