Speccy report for KAMORA-LAPTOP, [20-Mar-25 12:55:34]

Summary

Operating System
Windows 11 Pro 64-bit

CPU
Intel Core i7 8750H @ 2.20GHz 54 °C
Coffee Lake 14nm Technology

RAM
32.0GB Dual-Channel DDR4 @ 1332MHz (15-17-17-35)

Motherboard
Micro-Star International Co., Ltd. MS-17C5 (U3E1)

Graphics
Generic PnP Monitor (1920x1080@120Hz)
Intel UHD Graphics 630 (MSI)
2047MB NVIDIA GeForce GTX 1060 (MSI) 47 °C
SLI Disabled

Storage
931GB Seagate ST1000LM049-2GH172 (SATA (SSD)) 30 °C
465GB Samsung SSD 970 EVO Plus 500GB (Unknown (SSD))

Optical Drives
No optical disk drives detected

Audio
SteelSeries Sonar Virtual Audio Device

Operating System

Windows 11 Pro 64-bit
Computer type: Virtual
Installation Date: 22-Oct-24 11:41:48 AM
Serial Number: PQJDQ-C48YT-YRMBT-X8KXM-2PQGT

Windows Security Center

User Account Control (UAC)	Enabled
Notify level	2 - Default
Firewall	Enabled

Windows Update
AutoUpdate Not configured

Windows Defender
Windows Defender Enabled

Antivirus

Antivirus	Enabled
Display Name	Windows Defender
Virus Signature Database	Up to date

.NET Frameworks installed
v4.8 Full
v4.8 Client
v3.5 SP1
v3.0 SP2
v2.0 SP2

Internet Explorer
Version 11.1882.26100.0

PowerShell
Version 5.1.26100.1882
Java
Java Runtime Environment
Path C:\Program Files (x86)\Java\jre1.8.0_421\bin\java.exe
Version 8.0
Update 421
Build 09
Environment Variables
USERPROFILE C:\Users\stefa
SystemRoot C:\WINDOWS
User Variables

ChocolateyLastPathUpdate	133812348490515240
OneDrive	C:\Users\stefa\OneDrive
Path	C:\Users\stefa\AppData\Local\Programs\Python\Python312\Scripts\ C:\Users\stefa\AppData\Local\Programs\Python\Python312\ C:\Users\stefa\AppData\Local\activestate\cache\bin C:\Users\stefa\AppData\Local\ActiveState\StateTool\release\bin C:\Users\stefa\AppData\Local\Microsoft\WindowsApps C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\bin C:\Users\stefa\.dotnet\tools C:\Users\stefa\AppData\Roaming\npm
TEMP	C:\Users\stefa\AppData\Local\Temp
TMP	C:\Users\stefa\AppData\Local\Temp

Machine Variables

ChocolateyInstall	C:\ProgramData\chocolatey
ComSpec	C:\WINDOWS\system32\cmd.exe
DriverData	C:\Windows\System32\Drivers\DriverData
NUMBER_OF_PROCESSORS	12
OS	Windows_NT
Path	C:\Python313\Scripts\ C:\Python313\ C:\Program Files\Common Files\Oracle\Java\javapath C:\Program Files (x86)\Common Files\Oracle\Java\java8path C:\Program Files (x86)\Common Files\Oracle\Java\javapath C:\WINDOWS\system32 C:\WINDOWS C:\WINDOWS\System32\Wbem C:\WINDOWS\System32\WindowsPowerShell\v1.0\ C:\WINDOWS\System32\OpenSSH\ C:\Users\stefa\AppData\Local\Programs\Python\Python312

	C:\Users\stefa\AppData\Local\Programs\Python\Python312\Scripts C:\Program Files\dotnet\ C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common C:\Program Files\nodejs\ C:\ProgramData\chocolatey\bin C:\Program Files\Git\cmd C:\Program Files\NVIDIA Corporation\NVIDIA app\NvDLISR C:\Program Files\Docker\Docker\resources\bin
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.PY;.PYW
PROCESSOR_ARCHITECTURE	AMD64
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 158 Stepping 10, GenuineIntel
PROCESSOR_LEVEL	6
PROCESSOR_REVISION	9e0a
PSModulePath	%ProgramFiles%\WindowsPowerShell\Modules C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules
TEMP	C:\WINDOWS\TEMP
TMP	C:\WINDOWS\TEMP
USERNAME	SYSTEM
windir	C:\WINDOWS
ZES_ENABLE_SYSMAN	1

Battery

AC Line	Online
Battery Charge %	96 %
Battery State	High
Remaining Battery Time	Unknown

Power Profile

Active power scheme	Balanced
Hibernation	Enabled
Turn Off Monitor after: (On AC Power)	Never
Turn Off Monitor after: (On Battery Power)	3 min
Turn Off Hard Disk after: (On AC Power)	20 min
Turn Off Hard Disk after: (On Battery Power)	10 min
Suspend after: (On AC Power)	Never
Suspend after: (On Battery Power)	10 min
Screen saver	Disabled

Uptime

Current Session

Current Time	20-Mar-25 12:55:33 PM
Current Uptime	260,341 sec (3 d, 00 h, 19 m, 01 s)
Last Boot Time	17-Mar-25 12:36:32 PM

Services

Running	Adobe Acrobat Update Service
Running	Application Information
Running	AppX Deployment Service (AppXSVC)
Running	Background Tasks Infrastructure Service
Running	Base Filtering Engine
Running	Bluetooth Support Service
Running	Capability Access Manager Service
Running	Certificate Propagation
Running	Clipboard User Service_bf3c27a
Running	CNG Key Isolation
Running	COM+ Event System
Running	Connected Devices Platform Service
Running	Connected Devices Platform User Service_bf3c27a
Running	Connected User Experiences and Telemetry
Running	Contact Data_bf3c27a
Running	CoreMessaging
Running	Credential Manager
Running	Cryptographic Services
Running	Data Sharing Service
Running	Data Usage
Running	DCOM Server Process Launcher
Running	Delivery Optimization
Running	Device Association Service
Running	Device Install Service
Running	DevicesFlow_bf3c27a

Runnin DHCP Client
g
Runnin Diagnostic Policy Service
g
Runnin Diagnostic System Host
g
Runnin Display Enhancement Service
g
Runnin Display Policy Service
g
Runnin Distributed Link Tracking Client
g
Runnin DNS Client
g
Runnin Gaming Services
g
Runnin Gaming Services
g
Runnin Geolocation Service
g
Runnin Host Network Service
g
Runnin Human Interface Device Service
g
Runnin HV Host Service
g
Runnin Hyper-V Host Compute Service
g
Runnin Hyper-V Virtual Machine Management
g
Runnin IKE and AuthIP IPsec Keying Modules
g
Runnin Intel Content Protection HDCP Service
g
Runnin Intel Content Protection HECI Service
g
Runnin Intel Dynamic Application Loader Host Interface Service
g
Runnin Intel HD Graphics Control Panel Service
g
Runnin Intel Management and Security Application Local Management Service
g
Runnin Internet Connection Sharing (ICS)
g
Runnin IP Helper
g
Runnin Killer Analytics Service
g
Runnin Killer Dynamic Bandwidth Management
g

Running	Killer Network Service
Running	KillerSmartphoneSleepService
Running	LGHUB Updater Service
Running	Local Session Manager
Running	Logitech LampArray Service
Running	Microsoft Defender Antivirus Network Inspection Service
Running	Microsoft Defender Antivirus Service
Running	Microsoft Defender Core Service
Running	Microsoft Office Click-to-Run Service
Running	Microsoft Passport
Running	Microsoft Passport Container
Running	Microsoft Store Install Service
Running	Nahimic service
Running	Network Connection Broker
Running	Network Connections
Running	Network List Service
Running	Network Store Interface Service
Running	Network Virtualization Service
Running	Now Playing Session Manager Service_bf3c27a
Running	NVIDIA Display Container LS
Running	NVIDIA LocalSystem Container
Running	Plug and Play
Running	Power
Running	Print Spooler
Running	Program Compatibility Assistant Service

Runnin g Radio Management Service
Runnin g Realtek Audio Universal Service
Runnin g Remote Access Connection Manager
Runnin g Remote Desktop Configuration
Runnin g Remote Desktop Services
Runnin g Remote Desktop Services UserMode Port Redirector
Runnin g Remote Procedure Call (RPC)
Runnin g RPC Endpoint Mapper
Runnin g Secure Socket Tunneling Protocol Service
Runnin g Security Accounts Manager
Runnin g Security Center
Runnin g Server
Runnin g Shell Hardware Detection
Runnin g SSDP Discovery
Runnin g State Repository Service
Runnin g Storage Service
Runnin g Sync Host_bf3c27a
Runnin g SynTPEnhService
Runnin g SysMain
Runnin g System Event Notification Service
Runnin g System Events Broker
Runnin g Task Scheduler
Runnin g TCP/IP NetBIOS Helper
Runnin g Text Input Management Service
Runnin g Themes

Runnin Time Broker
g
Runnin Udk User Service_bf3c27a
g
Runnin Update Orchestrator Service
g
Runnin User Data Access_bf3c27a
g
Runnin User Data Storage_bf3c27a
g
Runnin User Manager
g
Runnin User Profile Service
g
Runnin Web Account Manager
g
Runnin Web Threat Defense Service
g
Runnin Web Threat Defense User Service_bf3c27a
g
Runnin Windows Audio
g
Runnin Windows Audio Endpoint Builder
g
Runnin Windows Connection Manager
g
Runnin Windows Defender Firewall
g
Runnin Windows Event Log
g
Runnin Windows Font Cache Service
g
Runnin Windows License Manager Service
g
Runnin Windows Management Instrumentation
g
Runnin Windows Mobile Hotspot Service
g
Runnin Windows Presentation Foundation Font Cache 3.0.0.0
g
Runnin Windows Push Notifications System Service
g
Runnin Windows Push Notifications User Service_bf3c27a
g
Runnin Windows Search
g
Runnin Windows Security Service
g
Runnin Windows Time
g

Runnin g	WinHTTP Web Proxy Auto-Discovery Service
Runnin g	WLAN AutoConfig
Runnin g	Workstation
Runnin g	WSL Service
Stoppe d	ActiveX Installer (AxInstSV)
Stoppe d	Agent Activation Runtime_bf3c27a
Stoppe d	AnyDesk Service
Stoppe d	App Readiness
Stoppe d	Application Identity
Stoppe d	Application Layer Gateway Service
Stoppe d	Application Management
Stoppe d	AssignedAccessManager Service
Stoppe d	Auto Time Zone Updater
Stoppe d	AVCTP service
Stoppe d	Background Intelligent Transfer Service
Stoppe d	BattlEye Service
Stoppe d	BitLocker Drive Encryption Service
Stoppe d	Block Level Backup Engine Service
Stoppe d	Bluetooth Audio Gateway Service
Stoppe d	Bluetooth User Support Service_bf3c27a
Stoppe d	BranchCache
Stoppe d	CaptureService_bf3c27a
Stoppe d	Cellular Time
Stoppe d	Client License Service (ClipSVC)
Stoppe d	Cloud Backup and Restore Service_bf3c27a

Stoppe COM+ System Application
d
Stoppe Computer Browser
d
Stoppe ConsentUX User Service_bf3c27a
d
Stoppe CredentialEnrollmentManagerUserSvc_bf3c27a
d
Stoppe Declared Configuration(DC) service
d
Stoppe Device Management Enrollment Service
d
Stoppe Device Management Wireless Application Protocol (WAP) Push message
d Routing Service
Stoppe Device Setup Manager
d
Stoppe DeviceAssociationBroker_bf3c27a
d
Stoppe DevicePicker_bf3c27a
d
Stoppe DevQuery Background Discovery Broker
d
Stoppe Diagnostic Execution Service
d
Stoppe Diagnostic Service Host
d
Stoppe DialogBlockingService
d
Stoppe Distributed Transaction Coordinator
d
Stoppe Docker Desktop Service
d
Stoppe Downloaded Maps Manager
d
Stoppe Embedded Mode
d
Stoppe Encrypting File System (EFS)
d
Stoppe Enterprise App Management Service
d
Stoppe Extensible Authentication Protocol
d
Stoppe Fax
d
Stoppe File History Service
d
Stoppe Function Discovery Provider Host
d
Stoppe Function Discovery Resource Publication
d

Stoppe GameDVR and Broadcast User Service_bf3c27a
d
Stoppe GameInput Service
d
Stoppe GameInput Service
d
Stoppe Google Chrome Elevation Service (GoogleChromeElevationService)
d
Stoppe Google Updater Internal Service (GoogleUpdaterInternalService135.0.7023.0)
d
Stoppe Google Updater Service (GoogleUpdaterService135.0.7023.0)
d
Stoppe GraphicsPerfSvc
d
Stoppe Group Policy Client
d
Stoppe Host Guardian Client Service
d
Stoppe Hyper-V Data Exchange Service
d
Stoppe Hyper-V Guest Service Interface
d
Stoppe Hyper-V Guest Shutdown Service
d
Stoppe Hyper-V Heartbeat Service
d
Stoppe Hyper-V PowerShell Direct Service
d
Stoppe Hyper-V Remote Desktop Virtualization Service
d
Stoppe Hyper-V Time Synchronization Service
d
Stoppe Hyper-V Volume Shadow Copy Requestor
d
Stoppe Intel TPM Provisioning Service
d
Stoppe Inventory and Compatibility Appraisal service
d
Stoppe IP Translation Configuration Service
d
Stoppe IPsec Policy Agent
d
Stoppe Kerberos Local Key Distribution Center
d
Stoppe Killer Provider Data Helper Service
d
Stoppe Killer Smart AP Selection Service
d
Stoppe KtmRm for Distributed Transaction Coordinator
d

Stoppe Language Experience Service
d
Stoppe Link-Layer Topology Discovery Mapper
d
Stoppe Local Profile Assistant Service
d
Stoppe McpManagementService
d
Stoppe MessagingService_bf3c27a
d
Stoppe Microsoft Account Sign-in Assistant
d
Stoppe Microsoft App-V Client
d
Stoppe Microsoft Cloud Identity Service
d
Stoppe Microsoft Edge Elevation Service (MicrosoftEdgeElevationService)
d
Stoppe Microsoft Edge Update Service (edgeupdate)
d
Stoppe Microsoft Edge Update Service (edgeupdatem)
d
Stoppe Microsoft iSCSI Initiator Service
d
Stoppe Microsoft Keyboard Filter
d
Stoppe Microsoft Software Shadow Copy Provider
d
Stoppe Microsoft Storage Spaces SMP
d
Stoppe Microsoft Windows SMS Router Service.
d
Stoppe Natural Authentication
d
Stoppe Net.Tcp Port Sharing Service
d
Stoppe Netlogon
d
Stoppe Network Connected Devices Auto-Setup
d
Stoppe Network Connectivity Assistant
d
Stoppe Network Location Awareness
d
Stoppe Network Setup Service
d
Stoppe NVIDIA FrameView SDK service
d
Stoppe Offline Files
d

Stoppe OpenSSH Authentication Agent
d
Stoppe Optimize drives
d
Stoppe P9RdrService_bf3c27a
d
Stoppe Parental Controls
d
Stoppe Payments and NFC/SE Manager
d
Stoppe PenService_bf3c27a
d
Stoppe Performance Counter DLL Host
d
Stoppe Performance Logs & Alerts
d
Stoppe Phone Service
d
Stoppe Portable Device Enumerator Service
d
Stoppe Print Device Configuration Service
d
Stoppe Printer Extensions and Notifications
d
Stoppe PrintScanBrokerService
d
Stoppe PrintWorkflow_bf3c27a
d
Stoppe Problem Reports Control Panel Support
d
Stoppe Quality Windows Audio Video Experience
d
Stoppe Recommended Troubleshooting Service
d
Stoppe ReFS Dedup Service
d
Stoppe Remote Access Auto Connection Manager
d
Stoppe Remote Procedure Call (RPC) Locator
d
Stoppe Remote Registry
d
Stoppe Retail Demo Service
d
Stoppe Rockstar Game Library Service
d
Stoppe Routing and Remote Access
d
Stoppe Secondary Logon
d

Stoppe Sensor Data Service
d
Stoppe Sensor Monitoring Service
d
Stoppe Sensor Service
d
Stoppe Shared PC Account Manager
d
Stoppe Smart Card
d
Stoppe Smart Card Device Enumeration Service
d
Stoppe Smart Card Removal Policy
d
Stoppe SNMP Trap
d
Stoppe Software Protection
d
Stoppe Spot Verifier
d
Stoppe Steam Client Service
d
Stoppe SteelSeries GG Update Service Proxy
d
Stoppe Still Image Acquisition Events
d
Stoppe Storage Tiers Management
d
Stoppe System Guard Runtime Monitor Broker
d
Stoppe Telephony
d
Stoppe UPnP Device Host
d
Stoppe User Experience Virtualization Service
d
Stoppe Virtual Disk
d
Stoppe Visual Studio Installer Elevation Service
d
Stoppe Visual Studio Standard Collector Service 150
d
Stoppe Volume Shadow Copy
d
Stoppe WaaSMedicSvc
d
Stoppe WalletService
d
Stoppe Warp JIT Service
d

Stopped	WebClient
Stopped	Wi-Fi Direct Services Connection Manager Service
Stopped	Windows Backup
Stopped	Windows Biometric Service
Stopped	Windows Camera Frame Server
Stopped	Windows Camera Frame Server Monitor
Stopped	Windows Connect Now - Config Registrar
Stopped	Windows Defender Advanced Threat Protection Service
Stopped	Windows Encryption Provider Host Service
Stopped	Windows Error Reporting Service
Stopped	Windows Event Collector
Stopped	Windows Image Acquisition (WIA)
Stopped	Windows Insider Service
Stopped	Windows Installer
Stopped	Windows Management Service
Stopped	Windows Media Player Network Sharing Service
Stopped	Windows Modules Installer
Stopped	Windows Perception Simulation Service
Stopped	Windows PushToInstall Service
Stopped	Windows Remote Management (WS-Management)
Stopped	Windows Update
Stopped	Windows Virtual Audio Device Proxy Service
Stopped	Wired AutoConfig
Stopped	WMI Performance Adapter
Stopped	Work Folders

Stoppe d	WWAN AutoConfig
Stoppe d	Xbox Accessory Management Service
Stoppe d	Xbox Live Auth Manager
Stoppe d	Xbox Live Game Save
Stoppe d	Xbox Live Networking Service

TimeZone

TimeZone	GMT +2:00 Hours
Language	English (United States)
Location	Greece
Format	English (United States)
Currency	$
Date Format	dd-MMM-yy
Time Format	h:mm:ss tt

Scheduler

20-Mar-25 1:43 PM;	MicrosoftEdgeUpdateTaskMachineUA
20-Mar-25 2:09 PM;	Opera GX scheduled Autoupdate 1726151153
20-Mar-25 2:12 PM;	update-S-1-5-21-3862043409-991023693-2464665700-1001
20-Mar-25 3:00 PM;	Adobe Acrobat Update Task
20-Mar-25 3:12 PM;	update-sys
20-Mar-25 3:31 PM;	Opera GX scheduled assistant Autoupdate 1727353882
20-Mar-25 6:13 PM;	MicrosoftEdgeUpdateTaskMachineCore
	RNIdle Task

Hotfixes

Installed

20-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.425.119.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

19-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.425.100.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

18-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.425.83.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

17-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.425.69.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

13-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.425.14.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

13-Mar-25 Realtek - SoftwareComponent - 11.0.6000.355
Realtek SoftwareComponent driver update released in January 2025

13-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.425.11.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

13-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.425.5.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

13-Mar-25 Realtek - SoftwareComponent - 1.0.821.0
Realtek SoftwareComponent driver update released in January 2025

13-Mar-25 2025-03 Cumulative Update for Windows 11 Version 24H2 for x64-based Systems (KB5053598)
Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

12-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.350.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

10-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.316.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

09-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.304.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

08-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.295.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

08-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.293.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

08-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.285.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

07-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.276.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

07-Mar-25 Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.25010.11) - Current Channel (Broad)
This package will update Microsoft Defender Antivirus antimalware platform's components on the user machine.

07-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.266.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

05-Mar-25 2025-02 Cumulative Update Preview for Windows 11 Version 24H2 for x64-based Systems (KB5052093)
Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

05-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.237.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

04-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.225.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

24-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.76.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

24-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.74.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

23-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.59.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

22-Feb-25 Logitech - USB - 1.1.55.3120
Logitech USB driver update released in April 2024
22-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.41.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.
21-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.26.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.
20-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1992.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.
19-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1979.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.
17-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1939.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.
14-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1896.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.
14-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1887.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.
13-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1873.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.
12-Feb-25 2025-02 Cumulative Update for Windows 11 Version 24H2 for x64-based Systems (KB5051987)
Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.
12-Feb-25 Windows Malicious Software Removal Tool x64 - v5.132 (KB890830)
After the download, this tool runs one time to check your computer

for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.

12-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1850.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

11-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1823.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

10-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1805.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

10-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1803.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

09-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1786.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

08-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1767.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

07-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1755.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

07-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1745.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

06-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1736.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

06-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1725.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

05-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1696.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

04-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1694.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

04-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1688.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

04-Feb-25 Realtek - SoftwareComponent - 1.0.814.0
Realtek SoftwareComponent driver update released in December 2024

04-Feb-25 Realtek - SoftwareComponent - 11.0.6000.354
Realtek SoftwareComponent driver update released in December 2024

04-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1683.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

03-Feb-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1665.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

30-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1619.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

30-Jan-25 2025-01 Cumulative Update Preview for Windows 11 Version 24H2 for x64-based Systems (KB5050094)
Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the

associated Microsoft Knowledge Base article for more information.
After you install this item, you may have to restart your computer.

30-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1612.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

29-Jan-25 2025-01 Cumulative Update Preview for .NET Framework 3.5 and 4.8.1 for Windows 11, version 24H2 for x64 (KB5050577)

Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information.
After you install this item, you may have to restart your computer.

29-Jan-25 Realtek - SoftwareComponent - 1.0.813.0

Realtek SoftwareComponent driver update released in December 2024

29-Jan-25 Realtek - AudioProcessingObject - 13.0.6000.1505

Realtek AudioProcessingObject driver update released in December 2024

29-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1590.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

27-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1553.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

25-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1542.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

25-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1534.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

24-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1519.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

24-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1516.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

23-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1506.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

23-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1498.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

22-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1484.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

21-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1465.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

20-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1446.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

18-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1426.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

18-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1422.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

17-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1407.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

17-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1404.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

16-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1391.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

16-Jan-25 Realtek - SoftwareComponent - 1.0.810.0
Realtek SoftwareComponent driver update released in November 2024

16-Jan-25 Realtek - SoftwareComponent - 11.0.6000.353
Realtek SoftwareComponent driver update released in November 2024

16-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1382.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

15-Jan-25 2025-01 Cumulative Update for Windows 11 Version 24H2 for x64-based Systems (KB5050009)
Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

15-Jan-25 Windows Malicious Software Removal Tool x64 - v5.131 (KB890830)
After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.

15-Jan-25 2025-01 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 24H2 for x64 (KB5049622)
A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.

15-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1374.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

14-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1357.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

14-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1352.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect

viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

13-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1334.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

12-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1321.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

12-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1317.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

10-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1291.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

09-Jan-25 Update for Windows Security platform - KB5007651 (Version 10.0.27703.1006)

This package will update Windows Security platform components on the user machine.

09-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1273.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

09-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1266.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

29-Dec-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1073.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

25-Dec-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.994.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

15-Dec-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.806.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once

you have installed this item, it cannot be removed.

15-Dec-24 2024-12 Cumulative Update for Windows 11 Version 24H2 for x64-based Systems (KB5048667)

Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

15-Dec-24 Realtek - SoftwareComponent - 11.0.6000.351

Realtek SoftwareComponent driver update released in October 2024

15-Dec-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.806.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

15-Dec-24 Realtek - SoftwareComponent - 1.0.801.0

Realtek SoftwareComponent driver update released in October 2024

07-Dec-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.667.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

03-Dec-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.597.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

03-Dec-24 Logitech - Image - 1.4.40.0

Logitech Image driver update released in April 2021

02-Dec-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.587.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

02-Dec-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.567.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

01-Dec-24 2024-11 Cumulative Update Preview for Windows 11 Version 24H2 for x64-based Systems (KB5046740)

Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

01-Dec-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.567.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

01-Dec-24 2024-11 Cumulative Update Preview for .NET Framework 3.5 and 4.8.1 for Windows 11, version 24H2 for x64 (KB5048162)
Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

27-Nov-24 Realtek - SoftwareComponent - 1.0.795.0
Realtek SoftwareComponent driver update released in September 2024

27-Nov-24 Realtek - SoftwareComponent - 11.0.6000.349
Realtek SoftwareComponent driver update released in September 2024

27-Nov-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.501.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

27-Nov-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.497.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

19-Nov-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.365.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

17-Nov-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.335.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

17-Nov-24 2024-11 Cumulative Update for Windows 11 Version 24H2 for x64-based Systems (KB5046617)
Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

17-Nov-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.334.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

15-Nov-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.299.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

13-Nov-24 Windows Malicious Software Removal Tool x64 - v5.130 (KB890830)
After the download, this tool runs one time to check your computer

for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.

13-Nov-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.266.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

10-Nov-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.210.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

10-Nov-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.206.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

06-Nov-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.135.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

06-Nov-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.133.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

05-Nov-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.107.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

03-Nov-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.70.0) - Current Channel (Broad)

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

02-Nov-24 Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.24090.11) - Current Channel (Broad)

This package will update Microsoft Defender Antivirus antimalware platform’s components on the user machine.

02-Nov-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.59.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

01-Nov-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.36.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

01-Nov-24 2024-10 Cumulative Update Preview for Windows 11 Version 24H2 for x64-based Systems (KB5044384)
Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

01-Nov-24 2024-10 Cumulative Update Preview for .NET Framework 3.5 and 4.8.1 for Windows 11, version 24H2 for x64 (KB5045934)
Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

26-Oct-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.419.722.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

24-Oct-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.419.676.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

23-Oct-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.419.669.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

23-Oct-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.419.668.0) - Current Channel (Broad)
Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

22-Oct-24 9NDLCLMMTMRC-AppUp.IntelGraphicsControlPanel
9NDLCLMMTMRC-1152921505689405557

22-Oct-24 Windows 11, version 24H2
Install the latest version of Windows: Windows 11, version 24H2.

Not Installed

13-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.350.0) - Current Channel (Broad)
Installation Status Failed

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

12-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.350.0) - Current Channel (Broad)

Installation Status Failed

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

12-Mar-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.350.0) - Current Channel (Broad)

Installation Status Failed

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

18-Jan-25 9PNQKHFLD2WQ-Microsoft.SunriseBaseGame

Installation Status Canceled

9PNQKHFLD2WQ-1152921505698746851

12-Jan-25 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1317.0) - Current Channel (Broad)

Installation Status Canceled

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

15-Dec-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.806.0) - Current Channel (Broad)

Installation Status Failed

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

01-Dec-24 Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.567.0) - Current Channel (Broad)

Installation Status Failed

Install this update to revise the files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

27-Nov-24 2024-11 Cumulative Update Preview for Windows 11 Version 24H2 for x64-based Systems (KB5046740)

Installation Status Failed

Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

26-Oct-24 2024-10 Cumulative Update Preview for Windows 11 Version 24H2 for x64-based Systems (KB5044384)

Installation Status Failed

Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

System Folders

Application Data	C:\ProgramData
Cookies	C:\Users\stefa\AppData\Local\Microsoft\Windows\INetCookies
Desktop	C:\Users\stefa\Desktop
Documents	C:\Users\Public\Documents
Fonts	C:\WINDOWS\Fonts
Global Favorites	C:\Users\stefa\Favorites
Internet History	C:\Users\stefa\AppData\Local\Microsoft\Windows\History
Local Application Data	C:\Users\stefa\AppData\Local
Music	C:\Users\Public\Music
Path for burning CD	C:\Users\stefa\AppData\Local\Microsoft\Windows\Burn\Burn
Physical Desktop	C:\Users\stefa\Desktop
Pictures	C:\Users\Public\Pictures
Program Files	C:\Program Files
Public Desktop	C:\Users\Public\Desktop
Start Menu	C:\ProgramData\Microsoft\Windows\Start Menu
Start Menu Programs	C:\ProgramData\Microsoft\Windows\Start Menu\Programs
Startup	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Templates	C:\ProgramData\Microsoft\Windows\Templates
Temporary Internet Files	C:\Users\stefa\AppData\Local\Microsoft\Windows\INetCache
User Favorites	C:\Users\stefa\Favorites
Videos	C:\Users\Public\Videos
Windows Directory	C:\WINDOWS
Windows/System	C:\WINDOWS\system32

Process List

AcrobatNotificationClient.exe

Process ID	7076
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\WindowsApps\ReaderNotificationClient_1.0.4.0_x86__e1rzdqpraam7r\AcrobatNotificationClient.exe
Memory Usage	12 MB
Peak Memory Usage	44 MB

AdobeCollabSync.exe

Process ID	18748
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Adobe\Acrobat DC\Acrobat\AdobeCollabSync.exe
Memory Usage	3.61 MB
Peak Memory Usage	18 MB

AdobeCollabSync.exe

Process ID	19316

User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Adobe\Acrobat DC\Acrobat\AdobeCollabSync.exe
Memory Usage	13 MB
Peak Memory Usage	28 MB

AggregatorHost.exe

Process ID	9236
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\AggregatorHost.exe
Memory Usage	17 MB
Peak Memory Usage	30 MB

API.exe

Process ID	27624
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\Desktop\DIKE Atlas\API\bin\Debug\net8.0\API.exe
Memory Usage	258 MB
Peak Memory Usage	290 MB

ApplicationFrameHost.exe

Process ID	11976
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\ApplicationFrameHost.exe
Memory Usage	35 MB
Peak Memory Usage	47 MB

AppVShNotify.exe

Process ID	25660
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Program Files\Common Files\microsoft shared\ClickToRun\AppVShNotify.exe
Memory Usage	7.99 MB
Peak Memory Usage	9.43 MB

armsvc.exe

Process ID	5128
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
Memory Usage	6.47 MB
Peak Memory Usage	7.88 MB

audiodg.exe

Process ID	24432

User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\audiodg.exe
Memory Usage	30 MB
Peak Memory Usage	35 MB

chrome.exe

Process ID	8764
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	61 MB
Peak Memory Usage	61 MB

chrome.exe

Process ID	26536
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	59 MB
Peak Memory Usage	60 MB

chrome.exe

Process ID	21556
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	167 MB
Peak Memory Usage	306 MB

chrome.exe

Process ID	9292
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	569 MB
Peak Memory Usage	672 MB

chrome.exe

Process ID	12996
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	156 MB
Peak Memory Usage	190 MB

chrome.exe

Process ID	19548
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	270 MB
Peak Memory Usage	278 MB

chrome.exe

Process ID	23352
User	stefa

Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	22 MB
Peak Memory Usage	23 MB

chrome.exe

Process ID	23308
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	232 MB
Peak Memory Usage	351 MB

chrome.exe

Process ID	20288
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	20 MB
Peak Memory Usage	29 MB

chrome.exe

Process ID	15516
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	32 MB
Peak Memory Usage	37 MB

chrome.exe

Process ID	20492
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	440 MB
Peak Memory Usage	963 MB

chrome.exe

Process ID	25632
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	57 MB
Peak Memory Usage	74 MB

chrome.exe

Process ID	15584
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	362 MB
Peak Memory Usage	543 MB

chrome.exe

Process ID	23816
User	stefa
Domain	KAMORA-LAPTOP

Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	140 MB
Peak Memory Usage	397 MB

chrome.exe

Process ID	12992
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	222 MB
Peak Memory Usage	425 MB

chrome.exe

Process ID	19952
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	8.06 MB
Peak Memory Usage	8.91 MB

chrome.exe

Process ID	19776
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	69 MB
Peak Memory Usage	69 MB

chrome.exe

Process ID	4052
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Google\Chrome\Application\chrome.exe
Memory Usage	30 MB
Peak Memory Usage	31 MB

cmd.exe

Process ID	20152
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\cmd.exe
Memory Usage	4.91 MB
Peak Memory Usage	5.65 MB

cmd.exe

Process ID	19868
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\cmd.exe
Memory Usage	5.61 MB
Peak Memory Usage	6.93 MB

cmd.exe

Process ID	20956
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\cmd.exe

Memory Usage	4.96 MB
Peak Memory Usage	5.89 MB

Code.exe

Process ID	2164
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	86 MB
Peak Memory Usage	98 MB

Code.exe

Process ID	132
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	86 MB
Peak Memory Usage	102 MB

Code.exe

Process ID	21284
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	252 MB
Peak Memory Usage	276 MB

Code.exe

Process ID	22232
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	44 MB
Peak Memory Usage	49 MB

Code.exe

Process ID	21380
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	426 MB
Peak Memory Usage	467 MB

Code.exe

Process ID	18448
User	stefa

Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	536 MB
Peak Memory Usage	567 MB

Code.exe

Process ID	22504
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	92 MB
Peak Memory Usage	131 MB

Code.exe

Process ID	15900
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	120 MB
Peak Memory Usage	180 MB

Code.exe

Process ID	26000
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	121 MB
Peak Memory Usage	131 MB

Code.exe

Process ID	12456
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	265 MB
Peak Memory Usage	333 MB

Code.exe

Process ID	24868
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	213 MB

Peak Memory Usage	281 MB

Code.exe

Process ID	22392
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	121 MB
Peak Memory Usage	153 MB

Code.exe

Process ID	23848
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	102 MB
Peak Memory Usage	164 MB

Code.exe

Process ID	20092
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	82 MB
Peak Memory Usage	128 MB

Code.exe

Process ID	12332
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	82 MB
Peak Memory Usage	111 MB

Code.exe

Process ID	23484
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	89 MB
Peak Memory Usage	112 MB

Code.exe

Process ID	10544
User	stefa

Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	27 MB
Peak Memory Usage	32 MB

Code.exe

Process ID	17308
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe
Memory Usage	140 MB
Peak Memory Usage	153 MB

com.docker.backend.exe

Process ID	26448
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Docker\Docker\resources\com.docker.backend.exe
Memory Usage	53 MB
Peak Memory Usage	61 MB

com.docker.backend.exe

Process ID	13260
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Docker\Docker\resources\com.docker.backend.exe
Memory Usage	199 MB
Peak Memory Usage	224 MB

com.docker.build.exe

Process ID	13680
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Docker\Docker\resources\com.docker.build.exe
Memory Usage	34 MB
Peak Memory Usage	38 MB

com.docker.dev-envs.exe

Process ID	17576
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Docker\Docker\resources\com.docker.dev-envs.exe
Memory Usage	9.93 MB

Peak Memory Usage	13 MB

conhost.exe

Process ID	5232
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\conhost.exe
Memory Usage	9.17 MB
Peak Memory Usage	11 MB

conhost.exe

Process ID	9816
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\conhost.exe
Memory Usage	8.78 MB
Peak Memory Usage	9.79 MB

conhost.exe

Process ID	8472
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\conhost.exe
Memory Usage	8.82 MB
Peak Memory Usage	10 MB

conhost.exe

Process ID	16888
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\conhost.exe
Memory Usage	7.40 MB
Peak Memory Usage	8.35 MB

conhost.exe

Process ID	12988
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\conhost.exe
Memory Usage	6.59 MB
Peak Memory Usage	7.33 MB

conhost.exe

Process ID	7580
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\conhost.exe
Memory Usage	8.78 MB
Peak Memory Usage	9.80 MB

conhost.exe

Process ID	20300
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\conhost.exe
Memory Usage	7.61 MB

Peak Memory Usage	8.35 MB

conhost.exe

Process ID	26572
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\conhost.exe
Memory Usage	6.59 MB
Peak Memory Usage	7.40 MB

conhost.exe

Process ID	9112
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\conhost.exe
Memory Usage	7.77 MB
Peak Memory Usage	7.89 MB

conhost.exe

Process ID	4076
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\conhost.exe
Memory Usage	7.64 MB
Peak Memory Usage	8.36 MB

conhost.exe

Process ID	15116
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\conhost.exe
Memory Usage	8.78 MB
Peak Memory Usage	9.80 MB

conhost.exe

Process ID	6620
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\conhost.exe
Memory Usage	7.77 MB
Peak Memory Usage	7.89 MB

conhost.exe

Process ID	3136
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\conhost.exe
Memory Usage	7.77 MB
Peak Memory Usage	7.89 MB

conhost.exe

Process ID	1928
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\conhost.exe
Memory Usage	6.96 MB
Peak Memory Usage	7.90 MB

conhost.exe

Process ID	5704
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\conhost.exe
Memory Usage	6.60 MB
Peak Memory Usage	7.41 MB

conhost.exe

Process ID	17344
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\conhost.exe
Memory Usage	7.09 MB
Peak Memory Usage	7.87 MB

conhost.exe

Process ID	3512
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\conhost.exe
Memory Usage	8.77 MB
Peak Memory Usage	9.77 MB

csrss.exe

Process ID	3404
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\csrss.exe
Memory Usage	8.56 MB
Peak Memory Usage	18 MB

csrss.exe

Process ID	1060
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\csrss.exe
Memory Usage	6.45 MB
Peak Memory Usage	7.49 MB

ctfmon.exe

Process ID	9232
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\ctfmon.exe
Memory Usage	30 MB
Peak Memory Usage	33 MB

DataExchangeHost.exe

Process ID	26156
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\DataExchangeHost.exe
Memory Usage	33 MB
Peak Memory Usage	46 MB

dllhost.exe

Process ID	26324
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\dllhost.exe
Memory Usage	9.33 MB
Peak Memory Usage	12 MB

dllhost.exe

Process ID	17668
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\dllhost.exe
Memory Usage	10 MB
Peak Memory Usage	12 MB

dllhost.exe

Process ID	9476
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\dllhost.exe
Memory Usage	9.13 MB
Peak Memory Usage	9.13 MB

dllhost.exe

Process ID	27472
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\dllhost.exe
Memory Usage	16 MB
Peak Memory Usage	26 MB

Docker Desktop.exe

Process ID	26912
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Docker\Docker\frontend\Docker Desktop.exe
Memory Usage	44 MB
Peak Memory Usage	49 MB

Docker Desktop.exe

Process ID	18248
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Docker\Docker\frontend\Docker Desktop.exe
Memory Usage	131 MB
Peak Memory Usage	161 MB

Docker Desktop.exe

Process ID	7868
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Docker\Docker\frontend\Docker Desktop.exe
Memory Usage	89 MB
Peak Memory Usage	213 MB

Docker Desktop.exe

Process ID	15868

User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Docker\Docker\frontend\Docker Desktop.exe
Memory Usage	144 MB
Peak Memory Usage	198 MB

docker-compose.exe

Process ID	14628
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Docker\Docker\resources\bin\docker-compose.exe
Memory Usage	36 MB
Peak Memory Usage	62 MB

docker.exe

Process ID	16004
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Docker\Docker\resources\bin\docker.exe
Memory Usage	19 MB
Peak Memory Usage	19 MB

docker.exe

Process ID	26100
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Docker\Docker\resources\bin\docker.exe
Memory Usage	19 MB
Peak Memory Usage	19 MB

docker.exe

Process ID	23480
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Docker\Docker\resources\bin\docker.exe
Memory Usage	19 MB
Peak Memory Usage	19 MB

dotnet.exe

Process ID	1908
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\dotnet\dotnet.exe
Memory Usage	96 MB
Peak Memory Usage	163 MB

dotnet.exe

Process ID	26424
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\dotnet\dotnet.exe
Memory Usage	52 MB
Peak Memory Usage	73 MB

dwm.exe

Process ID 20164
User DWM-3
Domain Window Manager
Path C:\Windows\System32\dwm.exe
Memory Usage 126 MB
Peak Memory Usage 192 MB

esbuild.exe

Process ID 25860
User stefa
Domain KAMORA-LAPTOP
Path C:\Users\stefa\Desktop\DIKE Atlas\Client\node_modules\@esbuild\win32-x64\esbuild.exe
Memory Usage 84 MB
Peak Memory Usage 102 MB

escape-node-job.exe

Process ID 2708
User stefa
Domain KAMORA-LAPTOP
Path C:\Users\stefa\.vscode\extensions\ms-dotnettools.csdevkit-1.16.6-win32-x64\components\vs-green-server\platforms\win32-x64\node_modules\@microsoft\visualstudio-code-launcher.win32-x64\escape-node-job.exe
Memory Usage 3.70 MB
Peak Memory Usage 4.13 MB

explorer.exe

Process ID 26264
User stefa
Domain KAMORA-LAPTOP
Path C:\Windows\explorer.exe
Memory Usage 432 MB
Peak Memory Usage 464 MB

fontdrvhost.exe

Process ID 1492
User UMFD-0
Domain Font Driver Host
Path C:\Windows\System32\fontdrvhost.exe
Memory Usage 6.80 MB
Peak Memory Usage 8.07 MB

fontdrvhost.exe

Process ID 7348
User UMFD-3
Domain Font Driver Host
Path C:\Windows\System32\fontdrvhost.exe

Memory Usage 9.83 MB
Peak Memory Usage 11 MB

gamingservices.exe

Process ID 24076
User SYSTEM
Domain NT AUTHORITY
Path C:\Program Files\WindowsApps\Microsoft.GamingServices_27.99.7001.0_x64__8wekyb3d8bbwe\gamingservices.exe
Memory Usage 43 MB
Peak Memory Usage 52 MB

gamingservicesnet.exe

Process ID 16072
User LOCAL SERVICE
Domain NT AUTHORITY
Path C:\Program Files\WindowsApps\Microsoft.GamingServices_27.99.7001.0_x64__8wekyb3d8bbwe\gamingservicesnet.exe
Memory Usage 9.48 MB
Peak Memory Usage 11 MB

igfxCUIService.exe

Process ID 3852
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\DriverStore\FileRepository\cui_dch.inf_amd64_9de8154b682af864\igfxCUIService.exe
Memory Usage 10 MB
Peak Memory Usage 12 MB

igfxEM.exe

Process ID 9248
User stefa
Domain KAMORA-LAPTOP
Path C:\Windows\System32\DriverStore\FileRepository\cui_dch.inf_amd64_9de8154b682af864\igfxEM.exe
Memory Usage 27 MB
Peak Memory Usage 31 MB

IntelCpHDCPSvc.exe

Process ID 4828
User SYSTEM

Domain	NT AUTHORITY
Path	C:\Windows\System32\DriverStore\FileRepository\iigd_dch.inf_amd64_de2b4d3f134dce87\IntelCpHDCPSvc.exe
Memory Usage	8.65 MB
Peak Memory Usage	10 MB

IntelCpHeciSvc.exe

Process ID	5876
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\DriverStore\FileRepository\iigd_dch.inf_amd64_de2b4d3f134dce87\IntelCpHeciSvc.exe
Memory Usage	8.22 MB
Peak Memory Usage	9.68 MB

jhi_service.exe

Process ID	5168
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\DriverStore\FileRepository\dal.inf_amd64_af50fdb80983f7bc\jhi_service.exe
Memory Usage	6.76 MB
Peak Memory Usage	8.28 MB

KillerAnalyticsService.exe

Process ID	4844
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\drivers\RivetNetworks\Killer\KillerAnalyticsService.exe
Memory Usage	9.90 MB
Peak Memory Usage	16 MB

KillerNetworkService.exe

Process ID	6124
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\drivers\RivetNetworks\Killer\KillerNetworkService.exe
Memory Usage	21 MB
Peak Memory Usage	98 MB

KNDBWM.exe

Process ID	3572
User	SYSTEM

Domain	NT AUTHORITY
Path	C:\Windows\System32\drivers\RivetNetworks\Killer\KNDBWM.exe
Memory Usage	13 MB
Peak Memory Usage	19 MB

KNDBWMService.exe

Process ID	9052
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\drivers\RivetNetworks\Killer\KNDBWMService.exe
Memory Usage	16 MB
Peak Memory Usage	20 MB

KSPS.exe

Process ID	8432
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\drivers\RivetNetworks\Killer\KSPS.exe
Memory Usage	6.50 MB
Peak Memory Usage	7.67 MB

KSPSService.exe

Process ID	6520
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\drivers\RivetNetworks\Killer\KSPSService.exe
Memory Usage	16 MB
Peak Memory Usage	20 MB

lghub_agent.exe

Process ID	1472
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\LGHUB\lghub_agent.exe
Memory Usage	60 MB
Peak Memory Usage	116 MB

lghub_system_tray.exe

Process ID	23548
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\LGHUB\system_tray\lghub_system_tray.exe
Memory Usage	78 MB
Peak Memory Usage	105 MB

lghub_updater.exe

Process ID	5280
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Program Files\LGHUB\lghub_updater.exe

Memory Usage	23 MB
Peak Memory Usage	36 MB

Lightshot.exe

Process ID	15700
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files (x86)\Skillbrains\lightshot\5.5.0.7\Lightshot.exe
Memory Usage	17 MB
Peak Memory Usage	21 MB

LMS.exe

Process ID	5272
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\DriverStore\FileRepository\lms.inf_amd64_a55aa2cd52a3429d\LMS.exe
Memory Usage	10 MB
Peak Memory Usage	12 MB

logi_lamparray_service.exe

Process ID	5248
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\DriverStore\FileRepository\logi_lamparray_usb.inf_amd64_3786a31d1dad269d\logi_lamparray_service.exe
Memory Usage	13 MB
Peak Memory Usage	16 MB

LsaIso.exe

Process ID	1252
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\LsaIso.exe
Memory Usage	3.39 MB
Peak Memory Usage	4.51 MB

lsass.exe

Process ID	1260
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\lsass.exe
Memory Usage	31 MB
Peak Memory Usage	44 MB

Memory Compression

Process ID	3868
User	SYSTEM
Domain	NT AUTHORITY
Memory Usage	1.65 GB

Peak Memory Usage 2.09 GB

Microsoft.CodeAnalysis.LanguageServer.exe

Process ID	7556
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\.vscode\extensions\ms-dotnettools.csharp-2.63.32-win32-x64\.roslyn\Microsoft.CodeAnalysis.LanguageServer.exe
Memory Usage	1.54 GB
Peak Memory Usage	3.23 GB

Microsoft.ServiceHub.Controller.exe

Process ID	10192
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\.vscode\extensions\ms-dotnettools.csdevkit-1.16.6-win32-x64\components\vs-green-server\platforms\win32-x64\node_modules\@microsoft\servicehub-controller-net60.win32-x64\Microsoft.ServiceHub.Controller.exe
Memory Usage	66 MB
Peak Memory Usage	78 MB

Microsoft.VisualStudio.Code.Server.exe

Process ID	14632
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\.vscode\extensions\ms-dotnettools.csdevkit-1.16.6-win32-x64\components\vs-green-server\platforms\win32-x64\node_modules\@microsoft\visualstudio-server.win32-x64\Microsoft.VisualStudio.Code.Server.exe
Memory Usage	117 MB
Peak Memory Usage	134 MB

Microsoft.VisualStudio.Code.ServiceHost.exe

Process ID	1852
User	stefa
Domain	KAMORA-LAPTOP

Path	C:\Users\stefa\.vscode\extensions\ms-dotnettools.csdevkit-1.16.6-win32-x64\components\vs-green-server\platforms\win32-x64\node_modules\@microsoft\visualstudio-code-servicehost.win32-x64\Microsoft.VisualStudio.Code.ServiceHost.exe
Memory Usage	147 MB
Peak Memory Usage	192 MB

Microsoft.VisualStudio.Code.ServiceHost.exe

Process ID	10520
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\.vscode\extensions\ms-dotnettools.csdevkit-1.16.6-win32-x64\components\vs-green-server\platforms\win32-x64\node_modules\@microsoft\visualstudio-code-servicehost.win32-x64\Microsoft.VisualStudio.Code.ServiceHost.exe
Memory Usage	102 MB
Peak Memory Usage	156 MB

MicrosoftStartFeedProvider.exe

Process ID	18088
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\WindowsApps\Microsoft.StartExperiencesApp_1.1.296.0_x64__8wekyb3d8bbwe\MicrosoftStartFeedProvider\MicrosoftStartFeedProvider.exe
Memory Usage	43 MB
Peak Memory Usage	51 MB

MpDefenderCoreService.exe

Process ID	5256
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25010.11-0\MpDefenderCoreService.exe
Memory Usage	24 MB

Peak Memory Usage	31 MB

msedgewebview2.exe

Process ID	21640
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\134.0.3124.72\msedgewebview2.exe
Memory Usage	1.35 MB
Peak Memory Usage	9.07 MB

msedgewebview2.exe

Process ID	15160
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\134.0.3124.72\msedgewebview2.exe
Memory Usage	4.96 MB
Peak Memory Usage	47 MB

msedgewebview2.exe

Process ID	21576
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\134.0.3124.72\msedgewebview2.exe
Memory Usage	3.12 MB
Peak Memory Usage	18 MB

msedgewebview2.exe

Process ID	14568
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\134.0.3124.72\msedgewebview2.exe
Memory Usage	13 MB
Peak Memory Usage	32 MB

msedgewebview2.exe

Process ID	12492
User	stefa
Domain	KAMORA-LAPTOP

Path	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\134.0.3124.72\msedgewebview2.exe
Memory Usage	15 MB
Peak Memory Usage	88 MB

msedgewebview2.exe

Process ID	18584
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\134.0.3124.72\msedgewebview2.exe
Memory Usage	39 MB
Peak Memory Usage	106 MB

MsMpEng.exe

Process ID	5652
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25010.11-0\MsMpEng.exe
Memory Usage	307 MB
Peak Memory Usage	1.06 GB

msrdc.exe

Process ID	27452
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\WSL\msrdc.exe
Memory Usage	37 MB
Peak Memory Usage	53 MB

NahimicService.exe

Process ID	5316
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\NahimicService.exe
Memory Usage	18 MB
Peak Memory Usage	20 MB

NgcIso.exe

Process ID	9752
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\NgcIso.exe
Memory Usage	3.60 MB
Peak Memory Usage	4.65 MB

NhNotifSys.exe

Process ID	16580

User stefa
Domain KAMORA-LAPTOP
Path C:\Windows\System32\NhNotifSys.exe
Memory Usage 24 MB
Peak Memory Usage 28 MB

NisSrv.exe
Process ID 14944
User LOCAL SERVICE
Domain NT AUTHORITY
Path C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25010.11-0\NisSrv.exe
Memory Usage 13 MB
Peak Memory Usage 18 MB

node.exe
Process ID 18328
User stefa
Domain KAMORA-LAPTOP
Path C:\Program Files\nodejs\node.exe
Memory Usage 431 MB
Peak Memory Usage 617 MB

nvcontainer.exe
Process ID 21968
User SYSTEM
Domain NT AUTHORITY
Path C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe
Memory Usage 51 MB
Peak Memory Usage 88 MB

nvcontainer.exe
Process ID 11404
User stefa
Domain KAMORA-LAPTOP
Path C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe
Memory Usage 74 MB
Peak Memory Usage 110 MB

nvcontainer.exe
Process ID 5476
User SYSTEM
Domain NT AUTHORITY
Path C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe
Memory Usage 38 MB
Peak Memory Usage 44 MB

NVDisplay.Container.exe
Process ID 13732

User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\DriverStore\FileRepository\nvmii.inf_amd64_3789e49ba4bd9327\Display.NvContainer\NVDisplay.Container.exe
Memory Usage	42 MB
Peak Memory Usage	185 MB

NVDisplay.Container.exe

Process ID	3636
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\DriverStore\FileRepository\nvmii.inf_amd64_3789e49ba4bd9327\Display.NvContainer\NVDisplay.Container.exe
Memory Usage	43 MB
Peak Memory Usage	69 MB

OfficeClickToRun.exe

Process ID	17128
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeClickToRun.exe
Memory Usage	49 MB
Peak Memory Usage	116 MB

Postman.exe

Process ID	23680
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Postman\app-11.37.1\Postman.exe
Memory Usage	176 MB
Peak Memory Usage	202 MB

Postman.exe

Process ID	15836
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Postman\app-11.37.1\Postman.exe
Memory Usage	107 MB
Peak Memory Usage	228 MB

Postman.exe

Process ID	19432
User	stefa

Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Postman\app-11.37.1\Postman.exe
Memory Usage	28 MB
Peak Memory Usage	32 MB

Postman.exe

Process ID	13132
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Postman\app-11.37.1\Postman.exe
Memory Usage	48 MB
Peak Memory Usage	66 MB

Postman.exe

Process ID	21416
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Users\stefa\AppData\Local\Postman\app-11.37.1\Postman.exe
Memory Usage	323 MB
Peak Memory Usage	493 MB

PowerToys.AlwaysOnTop.exe

Process ID	16152
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\PowerToys\PowerToys.AlwaysOnTop.exe
Memory Usage	1.48 MB
Peak Memory Usage	29 MB

PowerToys.ColorPickerUI.exe

Process ID	27344
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\PowerToys\PowerToys.ColorPickerUI.exe
Memory Usage	20 MB
Peak Memory Usage	142 MB

PowerToys.exe

Process ID	15124
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\PowerToys\PowerToys.exe
Memory Usage	26 MB
Peak Memory Usage	38 MB

PowerToys.FancyZones.exe

Process ID	18560
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\PowerToys\PowerToys.FancyZones.exe

Memory Usage	5.49 MB
Peak Memory Usage	66 MB

PowerToys.KeyboardManagerEngine.exe

Process ID	23340
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\PowerToys\KeyboardManagerEngine\PowerToys.KeyboardManagerEngine.exe
Memory Usage	1.49 MB
Peak Memory Usage	24 MB

PowerToys.Peek.UI.exe

Process ID	7528
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\PowerToys\WinUI3Apps\PowerToys.Peek.UI.exe
Memory Usage	18 MB
Peak Memory Usage	176 MB

PowerToys.PowerLauncher.exe

Process ID	6808
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\PowerToys\PowerToys.PowerLauncher.exe
Memory Usage	104 MB
Peak Memory Usage	581 MB

PowerToys.PowerOCR.exe

Process ID	9288
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\PowerToys\PowerToys.PowerOCR.exe
Memory Usage	7.05 MB
Peak Memory Usage	48 MB

PresentationFontCache.exe

Process ID	9420
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\Microsoft.NET\Framework64\v3.0\WPF\PresentationFontCache.exe
Memory Usage	20 MB
Peak Memory Usage	28 MB

Registry

Process ID	228
User	SYSTEM
Domain	NT AUTHORITY
Memory Usage	64 MB

Peak Memory Usage 253 MB

RtkAudUService64.exe

Process ID 5604
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\DriverStore\FileRepository\realtekservice.inf_amd64_7b2fe279bbb26e16\RtkAudUService64.exe
Memory Usage 13 MB
Peak Memory Usage 17 MB

RuntimeBroker.exe

Process ID 4480
User stefa
Domain KAMORA-LAPTOP
Path C:\Windows\System32\RuntimeBroker.exe
Memory Usage 35 MB
Peak Memory Usage 46 MB

RuntimeBroker.exe

Process ID 11220
User stefa
Domain KAMORA-LAPTOP
Path C:\Windows\System32\RuntimeBroker.exe
Memory Usage 22 MB
Peak Memory Usage 25 MB

RuntimeBroker.exe

Process ID 11552
User stefa
Domain KAMORA-LAPTOP
Path C:\Windows\System32\RuntimeBroker.exe
Memory Usage 49 MB
Peak Memory Usage 80 MB

RuntimeBroker.exe

Process ID 7204
User stefa
Domain KAMORA-LAPTOP
Path C:\Windows\System32\RuntimeBroker.exe
Memory Usage 23 MB
Peak Memory Usage 29 MB

RuntimeBroker.exe

Process ID 9864
User stefa
Domain KAMORA-LAPTOP
Path C:\Windows\System32\RuntimeBroker.exe
Memory Usage 10 MB
Peak Memory Usage 12 MB

SearchHost.exe

Process ID 17836
User stefa

Domain	KAMORA-LAPTOP
Path	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe
Memory Usage	131 MB
Peak Memory Usage	347 MB

SearchIndexer.exe

Process ID	25464
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\SearchIndexer.exe
Memory Usage	34 MB
Peak Memory Usage	59 MB

SearchProtocolHost.exe

Process ID	24412
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\SearchProtocolHost.exe
Memory Usage	25 MB
Peak Memory Usage	25 MB

Secure System

Process ID	188
User	SYSTEM
Domain	NT AUTHORITY
Memory Usage	124 KB
Peak Memory Usage	136 KB

SecurityHealthService.exe

Process ID	17216
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\SecurityHealthService.exe
Memory Usage	21 MB
Peak Memory Usage	37 MB

SecurityHealthSystray.exe

Process ID	16720
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\SecurityHealthSystray.exe
Memory Usage	12 MB
Peak Memory Usage	13 MB

services.exe

Process ID	1232
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\services.exe
Memory Usage	17 MB
Peak Memory Usage	21 MB

ShellExperienceHost.exe

Process ID	13436
User	stefa

Domain	KAMORA-LAPTOP
Path	C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
Memory Usage	71 MB
Peak Memory Usage	96 MB

ShellHost.exe

Process ID	22924
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\ShellHost.exe
Memory Usage	58 MB
Peak Memory Usage	66 MB

sihost.exe

Process ID	7720
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\sihost.exe
Memory Usage	34 MB
Peak Memory Usage	36 MB

smartscreen.exe

Process ID	18216
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\smartscreen.exe
Memory Usage	12 MB
Peak Memory Usage	12 MB

smss.exe

Process ID	720
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\smss.exe
Memory Usage	1.28 MB
Peak Memory Usage	1.67 MB

Speccy64.exe

Process ID	18532
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\Speccy\Speccy64.exe
Memory Usage	61 MB
Peak Memory Usage	81 MB

spoolsv.exe

Process ID	4988
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\spoolsv.exe
Memory Usage	20 MB
Peak Memory Usage	25 MB

StartMenuExperienceHost.exe

Process ID	13940

User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe
Memory Usage	115 MB
Peak Memory Usage	140 MB

svchost.exe

Process ID	19352
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	11 MB
Peak Memory Usage	14 MB

svchost.exe

Process ID	4848
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	12 MB
Peak Memory Usage	13 MB

svchost.exe

Process ID	15048
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	15 MB
Peak Memory Usage	29 MB

svchost.exe

Process ID	19448
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	20 MB
Peak Memory Usage	29 MB

svchost.exe

Process ID	19292
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	9.31 MB
Peak Memory Usage	10 MB

svchost.exe

Process ID	3380
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	16 MB

Peak Memory Usage	22 MB

svchost.exe

Process ID	16744
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	8.52 MB
Peak Memory Usage	8.74 MB

svchost.exe

Process ID	21304
User	NETWORK SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	23 MB
Peak Memory Usage	44 MB

svchost.exe

Process ID	12720
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	14 MB
Peak Memory Usage	16 MB

svchost.exe

Process ID	12596
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	33 MB
Peak Memory Usage	65 MB

svchost.exe

Process ID	13512
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\svchost.exe
Memory Usage	21 MB
Peak Memory Usage	26 MB

svchost.exe

Process ID	12896
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	24 MB
Peak Memory Usage	24 MB

svchost.exe

Process ID	7840
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	6.45 MB
Peak Memory Usage	7.23 MB

svchost.exe

Process ID	13924
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\svchost.exe
Memory Usage	14 MB
Peak Memory Usage	14 MB

svchost.exe

Process ID	11052
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	11 MB
Peak Memory Usage	12 MB

svchost.exe

Process ID	10700
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	36 MB
Peak Memory Usage	52 MB

svchost.exe

Process ID	16380
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\svchost.exe
Memory Usage	20 MB
Peak Memory Usage	28 MB

svchost.exe

Process ID	10620
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	15 MB
Peak Memory Usage	18 MB

svchost.exe

Process ID	10432
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	23 MB
Peak Memory Usage	29 MB

svchost.exe

Process ID	5936
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	5.29 MB
Peak Memory Usage	5.84 MB

svchost.exe

Process ID	10152
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	25 MB
Peak Memory Usage	27 MB

svchost.exe

Process ID	9640
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	23 MB
Peak Memory Usage	32 MB

svchost.exe

Process ID	9592
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	12 MB
Peak Memory Usage	14 MB

svchost.exe

Process ID	6916
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	8.18 MB
Peak Memory Usage	9.18 MB

svchost.exe

Process ID	6712
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	28 MB
Peak Memory Usage	70 MB

svchost.exe

Process ID	6460
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	14 MB
Peak Memory Usage	16 MB

svchost.exe

Process ID	6024
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	10 MB
Peak Memory Usage	12 MB

svchost.exe

Process ID	5660

User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	11 MB
Peak Memory Usage	13 MB

svchost.exe

Process ID	5640
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	23 MB
Peak Memory Usage	27 MB

svchost.exe

Process ID	5596
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	6.02 MB
Peak Memory Usage	7.19 MB

svchost.exe

Process ID	5488
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	7.56 MB
Peak Memory Usage	9.12 MB

svchost.exe

Process ID	5152
User	NETWORK SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	20 MB
Peak Memory Usage	72 MB

svchost.exe

Process ID	5048
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	8.41 MB
Peak Memory Usage	9.50 MB

svchost.exe

Process ID	4360
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	46 MB
Peak Memory Usage	119 MB

svchost.exe

Process ID	1452
User	SYSTEM

Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	8.94 MB
Peak Memory Usage	11 MB

svchost.exe

Process ID	5108
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	44 MB
Peak Memory Usage	194 MB

svchost.exe

Process ID	4892
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	18 MB
Peak Memory Usage	23 MB

svchost.exe

Process ID	4732
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	23 MB
Peak Memory Usage	29 MB

svchost.exe

Process ID	4464
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	12 MB
Peak Memory Usage	14 MB

svchost.exe

Process ID	4396
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	27 MB
Peak Memory Usage	52 MB

svchost.exe

Process ID	4248
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	12 MB
Peak Memory Usage	13 MB

svchost.exe

Process ID	4240
User	LOCAL SERVICE
Domain	NT AUTHORITY

Path	C:\Windows\System32\svchost.exe
Memory Usage	7.31 MB
Peak Memory Usage	8.54 MB

svchost.exe

Process ID	3484
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	7.97 MB
Peak Memory Usage	8.81 MB

svchost.exe

Process ID	1792
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	17 MB
Peak Memory Usage	18 MB

svchost.exe

Process ID	4032
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	11 MB
Peak Memory Usage	22 MB

svchost.exe

Process ID	4008
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	10 MB
Peak Memory Usage	19 MB

svchost.exe

Process ID	3988
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	9.50 MB
Peak Memory Usage	11 MB

svchost.exe

Process ID	3768
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	11 MB
Peak Memory Usage	12 MB

svchost.exe

Process ID	3760
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe

Memory Usage	17 MB
Peak Memory Usage	35 MB

svchost.exe

Process ID	3752
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	6.37 MB
Peak Memory Usage	7.30 MB

svchost.exe

Process ID	3704
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	18 MB
Peak Memory Usage	29 MB

svchost.exe

Process ID	3592
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	9.39 MB
Peak Memory Usage	10 MB

svchost.exe

Process ID	3472
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	32 MB
Peak Memory Usage	44 MB

svchost.exe

Process ID	3424
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	8.19 MB
Peak Memory Usage	9.02 MB

svchost.exe

Process ID	3296
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	11 MB
Peak Memory Usage	12 MB

svchost.exe

Process ID	3200
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	15 MB

Peak Memory Usage	17 MB

svchost.exe

Process ID	3172
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	30 MB
Peak Memory Usage	34 MB

svchost.exe

Process ID	3076
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	9.32 MB
Peak Memory Usage	10 MB

svchost.exe

Process ID	3036
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	8.71 MB
Peak Memory Usage	9.94 MB

svchost.exe

Process ID	2976
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	10 MB
Peak Memory Usage	11 MB

svchost.exe

Process ID	2900
User	NETWORK SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	11 MB
Peak Memory Usage	15 MB

svchost.exe

Process ID	2888
User	NETWORK SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	8.77 MB
Peak Memory Usage	10 MB

svchost.exe

Process ID	2632
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	8.18 MB
Peak Memory Usage	9.68 MB

svchost.exe

Process ID	2432
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	14 MB
Peak Memory Usage	19 MB

svchost.exe

Process ID	2360
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	7.18 MB
Peak Memory Usage	7.84 MB

svchost.exe

Process ID	2332
User	NETWORK SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	20 MB
Peak Memory Usage	24 MB

svchost.exe

Process ID	2200
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	13 MB
Peak Memory Usage	16 MB

svchost.exe

Process ID	2192
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	13 MB
Peak Memory Usage	14 MB

svchost.exe

Process ID	2140
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	6.32 MB
Peak Memory Usage	7.44 MB

svchost.exe

Process ID	2112
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	10 MB
Peak Memory Usage	12 MB

svchost.exe

Process ID	1272
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	20 MB
Peak Memory Usage	22 MB

svchost.exe

Process ID	1612
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	23 MB
Peak Memory Usage	24 MB

svchost.exe

Process ID	1228
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	23 MB
Peak Memory Usage	25 MB

svchost.exe

Process ID	3368
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	7.96 MB
Peak Memory Usage	9.14 MB

svchost.exe

Process ID	1936
User	NETWORK SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	29 MB
Peak Memory Usage	31 MB

svchost.exe

Process ID	12520
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\svchost.exe
Memory Usage	21 MB
Peak Memory Usage	21 MB

svchost.exe

Process ID	1920
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	13 MB
Peak Memory Usage	14 MB

svchost.exe

Process ID	1728

User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	22 MB
Peak Memory Usage	25 MB

svchost.exe

Process ID	1668
User	NETWORK SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	33 MB
Peak Memory Usage	36 MB

svchost.exe

Process ID	1424
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	68 MB
Peak Memory Usage	72 MB

svchost.exe

Process ID	8868
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	9.98 MB
Peak Memory Usage	11 MB

svchost.exe

Process ID	22944
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\svchost.exe
Memory Usage	23 MB
Peak Memory Usage	24 MB

svchost.exe

Process ID	22248
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	8.44 MB
Peak Memory Usage	9.16 MB

svchost.exe

Process ID	5776
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	18 MB
Peak Memory Usage	20 MB

svchost.exe

Process ID	2556
User	stefa

Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\svchost.exe
Memory Usage	36 MB
Peak Memory Usage	41 MB

svchost.exe

Process ID	26828
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\svchost.exe
Memory Usage	10 MB
Peak Memory Usage	11 MB

svchost.exe

Process ID	12644
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\svchost.exe
Memory Usage	30 MB
Peak Memory Usage	44 MB

svchost.exe

Process ID	25160
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\svchost.exe
Memory Usage	11 MB
Peak Memory Usage	12 MB

SynTPEnh.exe

Process ID	12028
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\SynTPEnh.exe
Memory Usage	32 MB
Peak Memory Usage	38 MB

SynTPEnhService.exe

Process ID	3464
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\SynTPEnhService.exe
Memory Usage	9.75 MB
Peak Memory Usage	13 MB

SynTPHelper.exe

Process ID	8468
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\SynTPHelper.exe
Memory Usage	7.10 MB
Peak Memory Usage	8.64 MB

System

Process ID	4
Memory Usage	13 MB
Peak Memory Usage	286 MB

System Idle Process
Process ID 0

SystemSettings.exe

Process ID	19724
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\ImmersiveControlPanel\SystemSettings.exe
Memory Usage	2.93 MB
Peak Memory Usage	195 MB

taskhostw.exe

Process ID	18896
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\taskhostw.exe
Memory Usage	19 MB
Peak Memory Usage	27 MB

taskhostw.exe

Process ID	23700
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\taskhostw.exe
Memory Usage	18 MB
Peak Memory Usage	22 MB

TextInputHost.exe

Process ID	23084
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\TextInputHost.exe
Memory Usage	130 MB
Peak Memory Usage	217 MB

unsecapp.exe

Process ID	5628
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\wbem\unsecapp.exe
Memory Usage	11 MB
Peak Memory Usage	12 MB

vmcompute.exe

Process ID	4980
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\vmcompute.exe
Memory Usage	15 MB
Peak Memory Usage	16 MB

vmmemWSL

Process ID	7268
User	CDD3B389-72E2-4228-8C43-78FD482F039A
Domain	NT VIRTUAL MACHINE

Memory Usage	1.41 GB
Peak Memory Usage	12 GB

vmms.exe

Process ID	3284
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\vmms.exe
Memory Usage	34 MB
Peak Memory Usage	40 MB

vmwp.exe

Process ID	18144
User	CDD3B389-72E2-4228-8C43-78FD482F039A
Domain	NT VIRTUAL MACHINE
Path	C:\Windows\System32\vmwp.exe
Memory Usage	21 MB
Peak Memory Usage	35 MB

WidgetBoard.exe

Process ID	7460
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\WindowsApps\MicrosoftWindows.Client.WebExperience_525.1301.30.0_x64__cw5n1h2txyewy\WidgetBoard.exe
Memory Usage	21 MB
Peak Memory Usage	23 MB

WidgetService.exe

Process ID	16344
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\WindowsApps\Microsoft.WidgetsPlatformRuntime_1.6.2.0_x64__8wekyb3d8bbwe\WidgetService\WidgetService.exe
Memory Usage	23 MB
Peak Memory Usage	25 MB

wininit.exe

Process ID	1160
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\wininit.exe
Memory Usage	7.48 MB
Peak Memory Usage	8.95 MB

winlogon.exe

Process ID	2884
User	SYSTEM

Domain	NT AUTHORITY
Path	C:\Windows\System32\winlogon.exe
Memory Usage	15 MB
Peak Memory Usage	25 MB

wlanext.exe

Process ID	21836
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\wlanext.exe
Memory Usage	6.75 MB
Peak Memory Usage	7.80 MB

WmiPrvSE.exe

Process ID	15488
User	NETWORK SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\wbem\WmiPrvSE.exe
Memory Usage	49 MB
Peak Memory Usage	54 MB

WmiPrvSE.exe

Process ID	15100
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\wbem\WmiPrvSE.exe
Memory Usage	18 MB
Peak Memory Usage	27 MB

wsl.exe

Process ID	26620
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\WSL\wsl.exe
Memory Usage	11 MB
Peak Memory Usage	12 MB

wsl.exe

Process ID	9464
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Windows\System32\wsl.exe
Memory Usage	6.57 MB
Peak Memory Usage	7.41 MB

wsl.exe

Process ID	26656
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\WSL\wsl.exe
Memory Usage	11 MB
Peak Memory Usage	12 MB

wsl.exe

Process ID	10348
User	stefa
Domain	KAMORA-LAPTOP

Path	C:\Windows\System32\wsl.exe
Memory Usage	6.56 MB
Peak Memory Usage	7.43 MB

wslhost.exe

Process ID	14408
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\WSL\wslhost.exe
Memory Usage	11 MB
Peak Memory Usage	12 MB

wslhost.exe

Process ID	15928
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\WSL\wslhost.exe
Memory Usage	11 MB
Peak Memory Usage	12 MB

wslhost.exe

Process ID	23028
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\WSL\wslhost.exe
Memory Usage	11 MB
Peak Memory Usage	11 MB

wslhost.exe

Process ID	26388
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\WSL\wslhost.exe
Memory Usage	11 MB
Peak Memory Usage	12 MB

wslrelay.exe

Process ID	15036
User	stefa
Domain	KAMORA-LAPTOP
Path	C:\Program Files\WSL\wslrelay.exe
Memory Usage	9.75 MB
Peak Memory Usage	11 MB

wslservice.exe

Process ID	5672
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Program Files\WSL\wslservice.exe
Memory Usage	30 MB
Peak Memory Usage	33 MB

WUDFHost.exe

Process ID	1500
User	LOCAL SERVICE
Domain	NT AUTHORITY
Path	C:\Windows\System32\WUDFHost.exe

Memory Usage	16 MB
Peak Memory Usage	17 MB

Security Options

@wsecedit.dll,-59058	Enabled
Accounts: Administrator account status	Disabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled

Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Not Defined
Audit: Shut down system immediately if unable to log security audits	Disabled
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined

Devices: Prevent users from installing printer drivers	Disabled
Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow computer account re-use during domain join	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure channel connections	Not Defined
Domain controller: LDAP server channel binding token requirements	Not Defined
Domain controller: LDAP server signing requirements	Not Defined

Domain controller: LDAP server signing requirements Enforcement	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain controller: Refuse setting default machine account password	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled

Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Display user information when the session is locked	Not Defined
Interactive logon: Do not require CTRL+ALT+ DEL	Not Defined
Interactive logon: Don't display last signed-in	Disabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	

Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons
Interactive logon: Prompt user to change password before expiration	5 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Require Windows Hello for Business or smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled

Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	Not Defined
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation level	Not Defined

Minimum password length audit	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled
Network access: Do not allow storage of passwords and credentials for network authentication	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions,System\CurrentControlSet\Control\Server Applications,Software\Microsoft\Windows NT\CurrentVersion

Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet\Control\Print\Printers,System\CurrentControlSet\Services\Eventlog,Software\Microsoft\OLAP Server,Software\Microsoft\Windows NT\CurrentVersion\Print,Software\Microsoft\Windows NT\CurrentVersion\Windows,System\CurrentControlSet\Control\ContentIndex,System\CurrentControlSet\Control\Terminal Server,System\CurrentControlSet\Control\Terminal Server\UserConfig,System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration,Software\Microsoft\Windows NT\CurrentVersion\Perflib,System\CurrentControlSet\Services\SysmonLog
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Restrict clients allowed to make remote calls to SAM	
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves
Network security: Allow Local System to use computer identity for NTLM	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined

Network security: Allow PKU2U authentication requests to this computer to use online identities.	Not Defined
Network security: Configure encryption types allowed for Kerberos	Not Defined
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client encryption requirements	Negotiate sealing
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require 128-bit encryption

Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require 128-bit encryption
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined

Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Recovery console: Allow automatic administrative logon	Not Defined
Recovery console: Allow floppy copy and access to all drives and all folders	Not Defined
Relax minimum password length limits	Not Defined
Shutdown: Allow system to be shut down without having to log on	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled
System settings: Optional subsystems	
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Disabled
User Account Control: Admin Approval Mode for the Built-in Administrator account	Not Defined

User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent for non-Windows binaries
User Account Control: Behavior of the elevation prompt for administrators running with Administrator protection	Prompt for credentials on the secure desktop
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials
User Account Control: Configure type of Admin Approval Mode	Legacy Admin Approval Mode (Default)
User Account Control: Detect application installations and prompt for elevation	Enabled

User Account Control: Only elevate executables that are signed and validated	Disabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

Device Tree

ACPI x64-based PC

Microsoft ACPI-Compliant System

ACPI Fixed Feature Button
ACPI Power Button
ACPI Processor Aggregator
ACPI Sleep Button
ACPI Thermal Zone
Intel Core i7-8750H CPU @ 2.20GHz
Intel Core i7-8750H CPU @ 2.20GHz
Intel Core i7-8750H CPU @ 2.20GHz
Intel Core i7-8750H CPU @ 2.20GHz

Intel Core i7-8750H CPU @ 2.20GHz
Intel Core i7-8750H CPU @ 2.20GHz
Intel Core i7-8750H CPU @ 2.20GHz
Intel Core i7-8750H CPU @ 2.20GHz
Intel Core i7-8750H CPU @ 2.20GHz
Intel Core i7-8750H CPU @ 2.20GHz
Intel Core i7-8750H CPU @ 2.20GHz
Intel Core i7-8750H CPU @ 2.20GHz
Intel Power Engine Plug-in
Microsoft Windows Management Interface for ACPI
Microsoft Windows Management Interface for ACPI
Motherboard resources
Trusted Platform Module 2.0
PCI Express Root Complex
Intel Host Bridge/DRAM Registers - 3EC4
Intel SPI (flash) Controller - A324
Intel Thermal Subsystem - A379
Microsoft Windows Management Interface for ACPI
Microsoft Windows Management Interface for ACPI
Motherboard resources
Motherboard resources
Motherboard resources
Motherboard resources
Motherboard resources
PCI standard RAM Controller
Synaptics SMBus Driver
Intel(R) Xeon(R) E3 - 1200/1500 v5/6th Gen Intel(R) Core(TM) PCIe Controller (x16) - 1901
NVIDIA GeForce GTX 1060
Intel(R) UHD Graphics 630
Integrated Monitor
Intel Graphics Control Panel
Intel Media SDK binaries
Intel(R) USB 3.1 eXtensible Host Controller - 1.10 (Microsoft)
USB Root Hub (USB 3.0)
Intel Wireless Bluetooth
Realtek USB 2.0 Card Reader
PRO WIRELESS
LIGHTSPEED Receiver
LIGHTSPEED Receiver
LIGHTSPEED Receiver
LIGHTSPEED Receiver
LIGHTSPEED Receiver
LIGHTSPEED Receiver
PRO WIRELESS
USB Input Device
HID Keyboard Device
USB Input Device
HID-compliant consumer control device
HID-compliant mouse

HID-compliant system controller
HID-compliant vendor-defined device
USB Input Device
HID-compliant vendor-defined device
HID-compliant vendor-defined device
HID-compliant vendor-defined device
Virtual HID Framework (VHF) HID device
HID-compliant device
USB Composite Device
USB Input Device
HID-compliant vendor-defined device
USB Input Device
HID-compliant consumer control device
USB Composite Device
USB Input Device
HID-compliant vendor-defined device
USB Input Device
HID-compliant consumer control device
USB Composite Device
HD Webcam
Intel(R) Wireless-AC 9560 160MHz
Microsoft Wi-Fi Direct Virtual Adapter
Microsoft Wi-Fi Direct Virtual Adapter #2
Intel(R) Management Engine Interface
Intel Dynamic Application Loader Host Interface
Intel iCLS Client
Intel Management and Security Application Local Management
Standard SATA AHCI Controller
ST1000LM049-2GH172
Intel(R) PCI Express Root Port #9 - A330
Standard NVM Express Controller
Samsung SSD 970 EVO Plus 500GB
Intel(R) PCI Express Root Port #15 - A336
Killer E2500 Gigabit Ethernet Controller
Killer Networking Software
Intel(R) 300 Series Chipset Family LPC Controller (HM370) - A30D
High precision event timer
Intel Watchdog Timer Driver (Intel WDT)
Motherboard resources
Numeric data processor
Programmable interrupt controller
System CMOS/real time clock
System timer
SteelSeries PS/2 Keyboard
SteelSeries PS/2 Keyboard Forwarding device
Synaptics SMBus TouchPad
Synaptics Service binaries
SynTP_00
Microsoft ACPI-Compliant Embedded Controller
ACPI Lid

Microsoft AC Adapter
Microsoft ACPI-Compliant Control Method Battery
Microsoft Windows Management Interface for ACPI
Radio Switch Device
HID-compliant wireless radio controls
High Definition Audio Controller
Realtek(R) Audio
A-Volute Nh3 Audio Effects Component
Microphone (Realtek Audio)
Nahimic mirroring device
Realtek Audio Effects Component
Realtek Audio Universal Service
Realtek Hardware Support Application
Speakers (Realtek Audio)
Microsoft UEFI-Compliant System
MS-17C5 SBIOS Ver.10F

CPU

Intel Core i7 8750H

Cores	6
Threads	12
Name	Intel Core i7 8750H
Code Name	Coffee Lake
Package	Socket 1440 FCBGA
Technology	14nm
Specification	Intel Core i7-8750H CPU @ 2.20GHz
Family	6
Extended Family	6
Model	E
Extended Model	9E
Stepping	A
Revision	U0
Instructions	MMX, SSE, SSE2, SSE3, SSSE3, SSE4.1, SSE4.2, Intel 64, NX, AES, AVX, AVX2, FMA3
Virtualization	Not supported
Hyperthreading	Supported, Enabled
Stock Core Speed	2200 MHz
Average Temperature	54 °C

Caches

L1 Data Cache Size	6 x 32 KBytes
L1 Instructions Cache Size	6 x 32 KBytes
L2 Unified Cache Size	6 x 256 KBytes
L3 Unified Cache Size	9216 KBytes

Cores

Core 0

Core Speed	3990.1 MHz
Multiplier	x 40.0
Bus Speed	99.8 MHz

Temperature	53 °C
Threads	APIC ID: 0, 1

Core 1

Core Speed	2194.5 MHz
Multiplier	x 22.0
Bus Speed	99.8 MHz
Temperature	54 °C
Threads	APIC ID: 2, 3

Core 2

Core Speed	3990.1 MHz
Multiplier	x 40.0
Bus Speed	99.8 MHz
Temperature	54 °C
Threads	APIC ID: 4, 5

Core 3

Core Speed	2194.5 MHz
Multiplier	x 22.0
Bus Speed	99.8 MHz
Temperature	54 °C
Threads	APIC ID: 6, 7

Core 4

Core Speed	2194.5 MHz
Multiplier	x 22.0
Bus Speed	99.8 MHz
Temperature	54 °C
Threads	APIC ID: 8, 9

Core 5

Core Speed	3990.1 MHz
Multiplier	x 40.0
Bus Speed	99.8 MHz
Temperature	52 °C
Threads	APIC ID: 10, 11

RAM

Memory slots

Total memory slots	2
Used memory slots	2
Free memory slots	0

Memory

Type	DDR4
Size	32768 MBytes
Channels #	Dual
DRAM Frequency	1330.0 MHz
CAS# Latency (CL)	15 clocks
RAS# to CAS# Delay (tRCD)	17 clocks
RAS# Precharge (tRP)	17 clocks
Cycle Time (tRAS)	35 clocks
Command Rate (CR)	2T

Physical Memory

Memory Usage	50 %

Total Physical	32 GB
Available Physical	16 GB
Total Virtual	37 GB
Available Virtual	14 GB

SPD

Number Of SPD Modules 2

Slot #1

Type	DDR4
Size	16384 MBytes
Manufacturer	Kingston
Max Bandwidth	DDR4-2666 (1333 MHz)
Part Number	KHX2666C15S4/16G
Serial Number	C69770E3
Week/year	32 / 19
SPD Ext.	XMP

Timing table

JEDEC #1

Frequency	966.7 MHz
CAS# Latency	11.0
RAS# To CAS#	13
RAS# Precharge	13
tRAS	26
tRC	44
Voltage	1.200 V

JEDEC #2

Frequency	1066.7 MHz
CAS# Latency	12.0
RAS# To CAS#	14
RAS# Precharge	14
tRAS	28
tRC	48
Voltage	1.200 V

JEDEC #3

Frequency	1166.7 MHz
CAS# Latency	13.0
RAS# To CAS#	15
RAS# Precharge	15
tRAS	31
tRC	53
Voltage	1.200 V

JEDEC #4

Frequency	1233.3 MHz
CAS# Latency	14.0
RAS# To CAS#	16
RAS# Precharge	16
tRAS	33
tRC	56
Voltage	1.200 V

JEDEC #5

Frequency	1333.0 MHz

CAS# Latency	15.0
RAS# To CAS#	17
RAS# Precharge	17
tRAS	35
tRC	60
Voltage	1.200 V

JEDEC #6

Frequency	1333.0 MHz
CAS# Latency	16.0
RAS# To CAS#	17
RAS# Precharge	17
tRAS	35
tRC	60
Voltage	1.200 V

JEDEC #7

Frequency	1333.0 MHz
CAS# Latency	17.0
RAS# To CAS#	17
RAS# Precharge	17
tRAS	35
tRC	60
Voltage	1.200 V

JEDEC #8

Frequency	1333.0 MHz
CAS# Latency	18.0
RAS# To CAS#	17
RAS# Precharge	17
tRAS	35
tRC	60
Voltage	1.200 V

XMP-2666

Frequency	1333 MHz
CAS# Latency	15.0
RAS# To CAS#	17
RAS# Precharge	17
tRAS	35
Voltage	1.200 V

Slot #2

Type	DDR4
Size	16384 MBytes
Manufacturer	Kingston
Max Bandwidth	DDR4-2666 (1333 MHz)
Part Number	KHX2666C15S4/16G
Serial Number	C29770B5
Week/year	32 / 19
SPD Ext.	XMP

Timing table

JEDEC #1

Frequency	966.7 MHz
CAS# Latency	11.0

RAS# To CAS#	13
RAS# Precharge	13
tRAS	26
tRC	44
Voltage	1.200 V

JEDEC #2

Frequency	1066.7 MHz
CAS# Latency	12.0
RAS# To CAS#	14
RAS# Precharge	14
tRAS	28
tRC	48
Voltage	1.200 V

JEDEC #3

Frequency	1166.7 MHz
CAS# Latency	13.0
RAS# To CAS#	15
RAS# Precharge	15
tRAS	31
tRC	53
Voltage	1.200 V

JEDEC #4

Frequency	1233.3 MHz
CAS# Latency	14.0
RAS# To CAS#	16
RAS# Precharge	16
tRAS	33
tRC	56
Voltage	1.200 V

JEDEC #5

Frequency	1333.0 MHz
CAS# Latency	15.0
RAS# To CAS#	17
RAS# Precharge	17
tRAS	35
tRC	60
Voltage	1.200 V

JEDEC #6

Frequency	1333.0 MHz
CAS# Latency	16.0
RAS# To CAS#	17
RAS# Precharge	17
tRAS	35
tRC	60
Voltage	1.200 V

JEDEC #7

Frequency	1333.0 MHz
CAS# Latency	17.0
RAS# To CAS#	17
RAS# Precharge	17

tRAS	35
tRC	60
Voltage	1.200 V

JEDEC #8

Frequency	1333.0 MHz
CAS# Latency	18.0
RAS# To CAS#	17
RAS# Precharge	17
tRAS	35
tRC	60
Voltage	1.200 V

XMP-2666

Frequency	1333 MHz
CAS# Latency	15.0
RAS# To CAS#	17
RAS# Precharge	17
tRAS	35
Voltage	1.200 V

Motherboard

Manufacturer	Micro-Star International Co., Ltd.
Model	MS-17C5 (U3E1)
Version	REV:1.0
Chipset Vendor	Intel
Chipset Model	Coffee Lake
Chipset Revision	07
Southbridge Vendor	Intel
Southbridge Model	HM370
Southbridge Revision	10

BIOS

Brand	American Megatrends Inc.
Version	E17C5IMS.10F
Date	20-May-19

PCI Data

Slot PCI-E

Slot Type	PCI-E
Slot Usage	In Use
Data lanes	x16
Slot Designation	J6B2
Characteristics	3.3V, Shared, PME
Slot Number	0

Slot PCI-E

Slot Type	PCI-E
Slot Usage	In Use
Data lanes	x1
Slot Designation	J6B1
Characteristics	3.3V, Shared, PME
Slot Number	1

Slot PCI-E

Slot Type	PCI-E

Slot Usage	In Use
Data lanes	x1
Slot Designation	J6D1
Characteristics	3.3V, Shared, PME
Slot Number	2

Slot PCI-E

Slot Type	PCI-E
Slot Usage	In Use
Data lanes	x1
Slot Designation	J7B1
Characteristics	3.3V, Shared, PME
Slot Number	3

Slot PCI-E

Slot Type	PCI-E
Slot Usage	In Use
Data lanes	x1
Slot Designation	J8B4
Characteristics	3.3V, Shared, PME
Slot Number	4

Graphics

Monitor

Name	Generic PnP Monitor on Intel UHD Graphics 630
Current Resolution	1920x1080 pixels
Work Resolution	1920x1027 pixels
State	Enabled, Primary
Monitor Width	1920
Monitor Height	1080
Monitor BPP	32 bits per pixel
Monitor Frequency	120 Hz
Device	\\.\DISPLAY1\Monitor0

Intel UHD Graphics 630

Manufacturer	Intel
Model	UHD Graphics 630
Device ID	8086-3E9B
Subvendor	MSI (1462)
Current Performance Level	Level 0
Voltage	0.587 V
Driver version	25.20.100.6617

Count of performance levels : 1

Level 1 - "Perf Level 0"

NVIDIA GeForce GTX 1060

Manufacturer	NVIDIA
Model	GeForce GTX 1060
Device ID	10DE-1C20
Revision	A2
Subvendor	MSI (1462)
Current Performance Level	Level 0
Current GPU Clock	139 MHz
Current Memory Clock	405 MHz

Current Shader Clock	405 MHz
Voltage	0.587 V
Technology	16 nm
Bus Interface	PCI Express x16
Temperature	47 °C
Driver version	32.0.15.7270
BIOS Version	86.06.60.00.25
Physical Memory	2047 MB
Virtual Memory	2048 MB

Count of performance levels : 3

Level 1 - "Perf Level 0"

GPU Clock	139 MHz
Shader Clock	405 MHz

Level 2 - "Base"

GPU Clock	1455 MHz
Shader Clock	4004 MHz

Level 3 - "Boost"

GPU Clock	1733 MHz
Shader Clock	4004 MHz

Storage

Hard drives

ST1000LM049-2GH172 (SSD)

Manufacturer	Seagate
Heads	16
Cylinders	121,601
Tracks	31,008,255
Sectors	1,953,520,065
SATA type	SATA-III 6.0Gb/s
Device type	Fixed
ATA Standard	ACS3
Serial Number	WGS1NPMH
Firmware Version Number	SDM1
LBA Size	48-bit LBA
Power On Count	4751 times
Power On Time	552.0 days
Speed	7200 RPM
Features	S.M.A.R.T., APM, NCQ, TRIM
Max. Transfer Mode	SATA III 6.0Gb/s
Used Transfer Mode	SATA III 6.0Gb/s
Interface	SATA
Capacity	931 GB
Real size	1,000,204,886,016 bytes
RAID Type	None

S.M.A.R.T

Status	Warning
Temperature	30 °C
Temperature Range	OK (less than 50 °C)

S.M.A.R.T attributes

01

Attribute name	Read Error Rate
Real value	0
Current	71
Worst	53
Threshold	6
Raw Value	0000AB7FF8
Status	Good

03

Attribute name	Spin-Up Time
Real value	0 ms
Current	100
Worst	99
Threshold	0
Raw Value	0000000000
Status	Good

04

Attribute name	Start/Stop Count
Real value	9,545
Current	91
Worst	91
Threshold	20
Raw Value	0000002549
Status	Good

05

Attribute name	Reallocated Sectors Count
Real value	2,264
Current	96
Worst	96
Threshold	36
Raw Value	00000008D8
Status	Good

07

Attribute name	Seek Error Rate
Real value	0
Current	85
Worst	60
Threshold	45
Raw Value	0012488554
Status	Good

09

Attribute name	Power-On Hours (POH)
Real value	551d 23h
Current	85
Worst	85
Threshold	0
Raw Value	00000033BF
Status	Good

0A

Attribute name	Spin Retry Count
Real value	0

Current	100
Worst	100
Threshold	97
Raw Value	0000000000
Status	Good

0C

Attribute name	Device Power Cycle Count
Real value	4,751
Current	96
Worst	96
Threshold	20
Raw Value	000000128F
Status	Good

B8

Attribute name	End-to-End error / IOEDC
Real value	0
Current	100
Worst	100
Threshold	99
Raw Value	0000000000
Status	Good

BB

Attribute name	Reported Uncorrectable Errors
Real value	0
Current	100
Worst	100
Threshold	0
Raw Value	0000000000
Status	Good

BC

Attribute name	Command Timeout
Real value	13
Current	100
Worst	94
Threshold	0
Raw Value	000000000D
Status	Good

BD

Attribute name	High Fly Writes (WDC)
Real value	0
Current	100
Worst	100
Threshold	0
Raw Value	0000000000
Status	Good

BE

Attribute name	Airflow Temperature
Real value	30 °C
Current	70
Worst	35

Threshold	40
Raw Value	001F0F001E
Status	Good

BF

Attribute name	G-sense error rate
Real value	33
Current	100
Worst	100
Threshold	0
Raw Value	0000000021
Status	Good

C0

Attribute name	Power-off Retract Count
Real value	41
Current	100
Worst	100
Threshold	0
Raw Value	0000000029
Status	Good

C1

Attribute name	Load/Unload Cycle Count
Real value	214,943
Current	1
Worst	1
Threshold	0
Raw Value	000003479F
Status	Good

C2

Attribute name	Temperature
Real value	30 °C
Current	30
Worst	65
Threshold	0
Raw Value	000000001E
Status	Good

C5

Attribute name	Current Pending Sector Count
Real value	0
Current	100
Worst	100
Threshold	0
Raw Value	0000000000
Status	Good

C6

Attribute name	Uncorrectable Sector Count
Real value	0
Current	100
Worst	100
Threshold	0
Raw Value	0000000000

Status	Good

C7

Attribute name	UltraDMA CRC Error Count
Real value	12
Current	200
Worst	200
Threshold	0
Raw Value	000000000C
Status	Good

F0

Attribute name	Head Flying Hours
Real value	256d 18h
Current	100
Worst	253
Threshold	0
Raw Value	0000001812
Status	Good

F1

Attribute name	Total LBAs Written
Real value	41,656,712,908
Current	100
Worst	253
Threshold	0
Raw Value	00B2EEFECC
Status	Good

F2

Attribute name	Total LBAs Read
Real value	89,234,828,645
Current	100
Worst	253
Threshold	0
Raw Value	00C6CF6D65
Status	Good

FE

Attribute name	Free Fall Protection
Real value	0
Current	100
Worst	100
Threshold	0
Raw Value	0000000000
Status	Good

Partition 0

Partition ID	Disk #0, Partition #0
Disk Letter	D:
File System	NTFS
Volume Serial Number	96FB2F16
Size	931 GB
Used Space	287 GB (30%)
Free Space	643 GB (70%)

Samsung SSD 970 EVO Plus 500GB (SSD)

Manufacturer	SAMSUNG
Interface	Unknown
Capacity	465 GB
Real size	500,107,862,016 bytes
RAID Type	None

S.M.A.R.T

S.M.A.R.T not supported

Partition 0

Partition ID	Disk #1, Partition #0
File System	FAT32
Volume Serial Number	2AE3A03D
Size	96 MB
Used Space	33.4 MB (34%)
Free Space	62 MB (66%)

Partition 1

Partition ID	Disk #1, Partition #1
Disk Letter	C:
File System	NTFS
Volume Serial Number	B8E4646A
Size	464 GB
Used Space	205 GB (44%)
Free Space	259 GB (56%)

Partition 2

Partition ID	Disk #1, Partition #2
File System	NTFS
Volume Serial Number	08A410F1
Size	738 MB
Used Space	572 MB (77%)
Free Space	166 MB (23%)

Optical Drives

No optical disk drives detected

Audio

Sound Cards

Realtek High Definition Audio
NVIDIA Virtual Audio Device (Wave Extensible) (WDM)
Nahimic mirroring device
SteelSeries Sonar Virtual Audio Device

Playback Device

Speakers (Realtek Audio)

Recording Device

Microphone (Realtek Audio)

Peripherals

HID Keyboard Device

Device Kind	Keyboard
Device Name	HID Keyboard Device
Vendor	AMP,
Location	SteelSeries Gaming Keyboard

Driver
Date 6-21-2006
Version 10.0.26100.1882
File C:\WINDOWS\system32\DRIVERS\kbdhid.sys
File C:\WINDOWS\system32\DRIVERS\kbdclass.sys

HID Keyboard Device
Device Kind Keyboard
Device Name HID Keyboard Device
Vendor Logitech
Location USB Input Device
Driver
Date 6-21-2006
Version 10.0.26100.1882
File C:\WINDOWS\system32\DRIVERS\kbdhid.sys
File C:\WINDOWS\system32\DRIVERS\kbdclass.sys

HID Keyboard Device
Device Kind Keyboard
Device Name HID Keyboard Device
Vendor Logitech
Location Logitech G HUB Virtual Keyboard
Driver
Date 6-21-2006
Version 10.0.26100.1882
File C:\WINDOWS\system32\DRIVERS\kbdhid.sys
File C:\WINDOWS\system32\DRIVERS\kbdclass.sys

SteelSeries PS/2 Keyboard
Device Kind Keyboard
Device Name SteelSeries PS/2 Keyboard
Vendor MSI
Location Intel 300 Series Chipset Family LPC Controller (HM370) - A30D
Driver
Date 6-26-2024
Version 2.3.6.0
File C:\WINDOWS\system32\DRIVERS\ssps2.sys
File C:\WINDOWS\system32\DRIVERS\i8042prt.sys
File C:\WINDOWS\system32\DRIVERS\kbdclass.sys

HID-compliant mouse
Device Kind Mouse
Device Name HID-compliant mouse
Vendor AMP,
Location SteelSeries Gaming Keyboard
Driver
Date 6-21-2006
Version 10.0.26100.1150
File C:\WINDOWS\system32\DRIVERS\mouhid.sys
File C:\WINDOWS\system32\DRIVERS\mouclass.sys

Synaptics SMBus TouchPad
Device Kind Mouse
Device Name Synaptics SMBus TouchPad
Vendor SYN

Location Intel 300 Series Chipset Family LPC Controller (HM370) - A30D

Driver

Date 7-27-2020
Version 19.5.31.21
File C:\WINDOWS\system32\DRIVERS\SynTP.sys
File C:\WINDOWS\system32\SynTPCpl.dll
File C:\WINDOWS\system32\SynCntxt.rtf
File C:\WINDOWS\system32\SynTPEnh.exe
File C:\WINDOWS\system32\SynTPRes.dll
File C:\WINDOWS\system32\SynTPAPI.dll
File C:\WINDOWS\system32\SynCOM.dll
File C:\WINDOWS\system32\SynTPHelper.exe
File C:\WINDOWS\system32\SynTPEnhService.exe
File C:\WINDOWS\system32\DRIVERS\mouclass.sys
File C:\WINDOWS\system32\DRIVERS\i8042prt.sys

HID-compliant mouse

Device Kind Mouse
Device Name HID-compliant mouse
Vendor Logitech
Location USB Input Device

Driver

Date 6-21-2006
Version 10.0.26100.1150
File C:\WINDOWS\system32\DRIVERS\mouhid.sys
File C:\WINDOWS\system32\DRIVERS\mouclass.sys

Printers

Fax

Printer Port SHRFAX:
Print Processor winprint
Availability Always
Priority 1
Duplex None
Print Quality 200 * 200 dpi Monochrome
Status Unknown

Driver

Driver Name Microsoft Shared Fax Driver (v4.00)
Driver Path C:\WINDOWS\system32\spool\DRIVERS\x64\3\FXSDRV.DLL

Microsoft Print to PDF (Default Printer)

Printer Port PORTPROMPT:
Print Processor winprint
Availability Always
Priority 1
Duplex None
Print Quality 600 * 600 dpi Color
Status Unknown

Driver

Driver Name Microsoft Print To PDF (v6.03)
Driver Path C:\WINDOWS\System32\DriverStore\FileRepository\ntprint.inf_amd64_0de5d6669dd41042\Amd64\mxdwdrv.dll

Microsoft XPS Document Writer

Printer Port	PORTPROMPT:
Print Processor	winprint
Availability	Always
Priority	1
Duplex	None
Print Quality	600 * 600 dpi Color
Status	Unknown

Driver

Driver Name	Microsoft XPS Document Writer v4 (v6.03)
Driver Path	C:\WINDOWS\System32\DriverStore\FileRepository\ntprint.inf_amd64_0de5d6669dd41042\Amd64\mxdwdrv.dll

OneNote (Desktop)

Printer Port	nul:
Print Processor	winprint
Availability	Always
Priority	1
Duplex	None
Print Quality	600 * 600 dpi Color
Status	Unknown

Driver

Driver Name	Send to Microsoft OneNote 16 Driver (v6.03)
Driver Path	C:\WINDOWS\System32\DriverStore\FileRepository\ntprint.inf_amd64_0de5d6669dd41042\Amd64\mxdwdrv.dll

---

Network

You are connected to the internet

Connected through	Intel Wireless-AC 9560 160MHz
IP Address	172.20.10.4
Subnet mask	255.255.255.240
Gateway server	172.20.10.1
Preferred DNS server	172.20.10.1
DHCP	Enabled
DHCP server	172.20.10.1
Adapter Type	IEEE 802.11 wireless
NetBIOS over TCP/IP	Enabled via DHCP
NETBIOS Node Type	Hybrid node
Link Speed	0 Bps

Computer Name

NetBIOS Name	KAMORA-LAPTOP
DNS Name	KAMORA-LAPTOP
Membership	Part of workgroup
Workgroup	WORKGROUP

Remote Desktop

Enabled

Console

State	Active
Domain	KAMORA-LAPTOP

RDP-Tcp
State Listen

WinInet Info
LAN Connection
Local system uses a local area network to connect to the Internet
Local system has RAS to connect to the Internet

Wi-Fi Info
Using native Wi-Fi API version 2
Available access points count 5

Wi-Fi ()

SSID	
Frequency	5220000 kHz
Channel Number	44
Name	No name
Signal Strength/Quality	91
Security	Enabled
State	The interface is connected to a network
Dot11 Type	Infrastructure BSS network
Network	Connectible
Network Flags	There is a profile for this network
Cipher Algorithm to be used when joining this network	AES-CCMP algorithm
Default Auth used to join this network for the first time	Not supported

Wi-Fi (DIRECT-QV-Pantum P2500 Series)

SSID	DIRECT-QV-Pantum P2500 Series
Frequency	2442000 kHz
Channel Number	7
Name	DIRECT-QV-Pantum P2500 Series
Signal Strength/Quality	53
Security	Enabled
State	The interface is connected to a network
Dot11 Type	Infrastructure BSS network
Network	Connectible
Network Flags	There is a profile for this network
Cipher Algorithm to be used when joining this network	AES-CCMP algorithm
Default Auth used to join this network for the first time	802.11i RSNA algorithm that uses PSK

Wi-Fi (HiSmart-01-ca2c4f600ce5)

SSID	HiSmart-01-ca2c4f600ce5
Frequency	2422000 kHz
Channel Number	3
Name	HiSmart-01-ca2c4f600ce5
Signal Strength/Quality	31
Security	Disabled
State	The interface is connected to a network
Dot11 Type	Infrastructure BSS network

Network	Connectible
Network Flags	There is a profile for this network
Cipher Algorithm to be used when joining this network	No Cipher algorithm is enabled/supported
Default Auth used to join this network for the first time	IEEE 802.11 Open System authentication algorithm

Wi-Fi (Kamora)

SSID	Kamora
Name	Kamora
Signal Strength/Quality	95
Security	Enabled
State	The interface is connected to a network
Dot11 Type	Infrastructure BSS network
Network	Connectible
Network Flags	Currently Connected to this network
Cipher Algorithm to be used when joining this network	AES-CCMP algorithm
Default Auth used to join this network for the first time	Not supported

Wi-Fi (Nova_2.4G_AhzSyHb)

SSID	Nova_2.4G_AhzSyHb
Frequency	2412000 kHz
Channel Number	1
Name	Nova_2.4G_AhzSyHb
Signal Strength/Quality	38
Security	Enabled
State	The interface is connected to a network
Dot11 Type	Infrastructure BSS network
Network	Connectible
Network Flags	There is a profile for this network
Cipher Algorithm to be used when joining this network	AES-CCMP algorithm
Default Auth used to join this network for the first time	802.11i RSNA algorithm that uses PSK

WinHTTPInfo

WinHTTPSessionProxyType	No proxy
Session Proxy	
Session Proxy Bypass	
Connect Retries	5
Connect Timeout (ms)	60,000
HTTP Version	HTTP 1.1
Max Connects Per 1.0 Servers	INFINITE
Max Connects Per Servers	INFINITE
Max HTTP automatic redirects	10
Max HTTP status continue	10
Send Timeout (ms)	30,000
IEProxy Auto Detect	No
IEProxy Auto Config	http://127.0.0.1:86/

IEProxy
IEProxy Bypass
Default Proxy Config Access Type No proxy
Default Config Proxy
Default Config Proxy Bypass

Sharing and Discovery

Network Discovery	Disabled
File and Printer Sharing	Disabled
File and printer sharing service	Enabled
Simple File Sharing	Enabled
Administrative Shares	Enabled
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves

Adapters List

Enabled

Intel(R) Wireless-AC 9560 160MHz

Connection Name	Wi-Fi
NetBIOS over TCPIP	Yes
DHCP enabled	Yes
MAC Address	30-24-32-C2-7E-96
IP Address	172.20.10.4
Subnet mask	255.255.255.240
Gateway server	172.20.10.1
DHCP	172.20.10.1
DNS Server	172.20.10.1

Killer E2500 Gigabit Ethernet Controller

Connection Name	Ethernet
DHCP enabled	Yes
MAC Address	30-9C-23-93-D7-1D

Network Shares

No network shares

Current TCP Connections

C:\Program Files\Adobe\Acrobat DC\Acrobat\AdobeCollabSync.exe (19316)

Local 172.20.10.4:56503 ESTABLISHED Remote 3.233.129.217:443 (Querying...) (HTTPS)

C:\Program Files\Docker\Docker\resources\com.docker.backend.exe (13260)

Local 0.0.0.0:5432 LISTEN

C:\Program Files\Google\Chrome\Application\chrome.exe (25632)

Local 127.0.0.1:55712 ESTABLISHED Remote 127.0.0.1:5000 (Querying...)

Local 172.20.10.4:55487 ESTABLISHED Remote 35.241.53.87:443 (Querying...) (HTTPS)

Local 172.20.10.4:56038 ESTABLISHED Remote 143.244.203.94:443 (Querying...) (HTTPS)

Local 172.20.10.4:56356 ESTABLISHED Remote 34.242.196.153:443 (Querying...) (HTTPS)

Local 172.20.10.4:56367 ESTABLISHED Remote 20.50.2.53:443 (Querying...) (HTTPS)

Local 172.20.10.4:56382 ESTABLISHED Remote 34.242.196.153:443 (Querying...) (HTTPS)

Local 172.20.10.4:56387 ESTABLISHED Remote 52.16.235.250:443 (Querying...) (HTTPS)
Local 172.20.10.4:56388 ESTABLISHED Remote 66.235.152.225:443 (Querying...) (HTTPS)
Local 172.20.10.4:56174 ESTABLISHED Remote 143.244.203.94:443 (Querying...) (HTTPS)
Local 172.20.10.4:56407 ESTABLISHED Remote 104.17.208.240:443 (Querying...) (HTTPS)
Local 172.20.10.4:56424 ESTABLISHED Remote 34.107.218.251:443 (Querying...) (HTTPS)
Local 172.20.10.4:56429 ESTABLISHED Remote 63.34.196.244:443 (Querying...) (HTTPS)
Local 172.20.10.4:56466 ESTABLISHED Remote 212.205.77.146:443 (Querying...) (HTTPS)
Local 172.20.10.4:56476 ESTABLISHED Remote 212.205.77.138:443 (Querying...) (HTTPS)
Local 172.20.10.4:56403 ESTABLISHED Remote 63.140.62.17:443 (Querying...) (HTTPS)

C:\Program Files\LGHUB\lghub_agent.exe (1472)

Local 127.0.0.1:49580 ESTABLISHED Remote 127.0.0.1:9100 (Querying...)
Local 127.0.0.1:9010 LISTEN
Local 127.0.0.1:9010 ESTABLISHED Remote 127.0.0.1:49578 (Querying...)
Local 127.0.0.1:9080 LISTEN
Local 127.0.0.1:56518 SYN-SENT Remote 127.0.0.1:28194 (Querying...)
Local 127.0.0.1:45654 LISTEN

C:\Program Files\LGHUB\system_tray\lghub_system_tray.exe (23548)

Local 127.0.0.1:49578 ESTABLISHED Remote 127.0.0.1:9010 (Querying...)

C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe (11404)

Local 172.20.10.4:49809 CLOSE-WAIT Remote 2.22.245.56:443 (Querying...) (HTTPS)

C:\Users\stefa\AppData\Local\Postman\app-11.37.1\Postman.exe (13132)

Local 172.20.10.4:51230 ESTABLISHED Remote 44.214.198.150:443 (Querying...) (HTTPS)
Local 172.20.10.4:51254 ESTABLISHED Remote 146.75.118.132:443 (Querying...) (HTTPS)
Local 172.20.10.4:53964 ESTABLISHED Remote 3.33.235.18:443 (Querying...) (HTTPS)
Local 172.20.10.4:56047 ESTABLISHED Remote 162.247.243.29:443 (Querying...) (HTTPS)

C:\Users\stefa\AppData\Local\Postman\app-11.37.1\Postman.exe (15836)

Local 0.0.0.0:15611 LISTEN

C:\Users\stefa\AppData\Local\Programs\Microsoft VS Code\Code.exe (22232)

Local 172.20.10.4:53291 ESTABLISHED Remote 20.42.65.94:443 (Querying...) (HTTPS)

C:\Users\stefa\Desktop\DIKE Atlas\API\bin\Debug\net8.0\API.exe (27624)

Local 0.0.0.0:5000 LISTEN
Local 127.0.0.1:5000 ESTABLISHED Remote 127.0.0.1:55712 (Querying...)

C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe (17836)

Local CLOSE-WAIT Remote 2.17.190.73:80 (Querying...)
172.20.10.4:49508 (HTTP)
lghub_updater.exe (5280)
Local 127.0.0.1:9180 LISTEN
Local 127.0.0.1:9100 ESTABLISHED Remote 127.0.0.1:49580 (Querying...)
Local 127.0.0.1:9100 LISTEN
lsass.exe (1260)
Local 0.0.0.0:49664 LISTEN
services.exe (1232)
Local 0.0.0.0:49674 LISTEN
spoolsv.exe (4988)
Local 0.0.0.0:49671 LISTEN
svchost.exe (10152)
Local 0.0.0.0:5040 LISTEN
svchost.exe (1272)
Local 0.0.0.0:49666 LISTEN
svchost.exe (1668)
Local 0.0.0.0:135 (DCE) LISTEN
svchost.exe (1936)
Local 0.0.0.0:3389 LISTEN
svchost.exe (21304)
Local 0.0.0.0:7680 LISTEN
svchost.exe (2976)
Local 0.0.0.0:49667 LISTEN
svchost.exe (3704)
Local 0.0.0.0:49669 LISTEN
System Process
Local TIME-WAIT Remote 20.50.80.214:443 (Querying...)
172.20.10.4:56012 (HTTPS)
Local TIME-WAIT Remote 172.20.10.1:53 (Querying...)
172.20.10.4:56345
Local TIME-WAIT Remote 2.22.245.106:443 (Querying...)
172.20.10.4:56104 (HTTPS)
Local TIME-WAIT Remote 20.42.65.91:443 (Querying...)
172.20.10.4:56066 (HTTPS)
System Process
Local 0.0.0.0:445 (Windows shares) LISTEN
Local 172.27.80.1:139 (NetBIOS session service) LISTEN
Local 172.20.10.4:139 (NetBIOS session service) LISTEN
Local 172.17.112.1:139 (NetBIOS session service) LISTEN
vmms.exe (3284)
Local 0.0.0.0:2179 LISTEN
wininit.exe (1160)
Local 0.0.0.0:49665 LISTEN