Summary

 Operating System

 Windows 10 Enterprise LTSC 64-bit

 CPU

 Intel Core i5 7500 @ 3.40GHz 50 °C

 Kaby Lake 14nm Technology

 RAM

 8.00GB Single-Channel Unknown @ 1197MHz (17-17-17-39)

 Motherboard

 Dell Inc. 0W0CHX (U3E1)

 Graphics

 DHL22-F600 (1920x1080@59Hz)

 DHL22-F600 (1920x1080@59Hz)

 Intel HD Graphics 630 (Dell)

 Storage

 465GB Seagate ST500DM009-2F110A (SATA ) 38 °C

 Optical Drives

 PLDS DVD+-RW DU-8A5LH

 Audio

 Realtek Audio

Operating System

 Windows 10 Enterprise LTSC 64-bit

 Computer type: Desktop

 Installation Date: 6/14/2019 3:48:15 PM

 Serial Number: VTM4Q-R69FP-94GBM-DRHTR-2KD8Q

 Windows Security Center

 User Account Control (UAC) Disabled

 Firewall Enabled

 Windows Update

 AutoUpdate Not configured

 Windows Defender

 Windows Defender Disabled

 Antivirus

 McAfee Endpoint Security

 Antivirus Enabled

 Virus Signature Database Up to date

 Windows Defender

 Antivirus Disabled

 Virus Signature Database Up to date

 .NET Frameworks installed

 v4.7 Full

 v4.7 Client

 v3.5 SP1

 v3.0 SP2

 v2.0 SP2

 Internet Explorer

 Version 11.864.17763.0

 PowerShell

 Version 5.1.17763.1

 Environment Variables

 USERPROFILE C:\Users\Dahua

 SystemRoot C:\WINDOWS

 User Variables

 OneDrive C:\Users\Dahua\OneDrive

 Path C:\Users\Dahua\AppData\Local\Microsoft\WindowsApps

 TEMP C:\Users\Dahua\AppData\Local\Temp

 TMP C:\Users\Dahua\AppData\Local\Temp

 Machine Variables

 ComSpec C:\WINDOWS\system32\cmd.exe

 DEFLOGDIR C:\ProgramData\McAfee\Endpoint Security\Logs

 DriverData C:\Windows\System32\Drivers\DriverData

 NUMBER\_OF\_PROCESSORS 4

 OS Windows\_NT

 Path C:\WINDOWS\system32

 C:\WINDOWS

 C:\WINDOWS\System32\Wbem

 C:\WINDOWS\System32\WindowsPowerShell\v1.0\

 C:\WINDOWS\System32\OpenSSH\

 C:\Program Files (x86)\Intel\Intel Management Engine Components\DAL

 C:\Program Files\Intel\Intel Management Engine Components\DAL

 C:\Program Files\PuTTY\

 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC

 PROCESSOR\_ARCHITECTURE AMD64

 PROCESSOR\_IDENTIFIER Intel64 Family 6 Model 158 Stepping 9, GenuineIntel

 PROCESSOR\_LEVEL 6

 PROCESSOR\_REVISION 9e09

 PSModulePath %ProgramFiles%\WindowsPowerShell\Modules

 C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules

 TEMP C:\WINDOWS\TEMP

 TMP C:\WINDOWS\TEMP

 USERNAME SYSTEM

 windir C:\WINDOWS

 Power Profile

 Active power scheme Power

 Hibernation Enabled

 Turn Off Monitor after: (On AC Power) 15 min

 Turn Off Hard Disk after: (On AC Power) 20 min

 Suspend after: (On AC Power) Never

 Screen saver Disabled

 Uptime

 Current Session

 Current Time 11/22/2019 8:44:24 AM

 Current Uptime 5,367 sec (0 d, 01 h, 29 m, 27 s)

 Last Boot Time 11/22/2019 7:14:57 AM

 Services

 Running Adobe Acrobat Update Service

 Running AnyDesk DahuaTechnologyUSATechnicalSupport Service

 Running AnyDesk Service

 Running AppX Deployment Service (AppXSVC)

 Running Background Intelligent Transfer Service

 Running Background Tasks Infrastructure Service

 Running Base Filtering Engine

 Running BitLocker Drive Encryption Service

 Running Cisco AnyConnect Secure Mobility Agent

 Running Clipboard User Service\_ba84e

 Running CNG Key Isolation

 Running COM+ Event System

 Running COM+ System Application

 Running Connected Devices Platform Service

 Running Connected Devices Platform User Service\_ba84e

 Running Connected User Experiences and Telemetry

 Running CoreMessaging

 Running Credential Manager

 Running Cryptographic Services

 Running Data Usage

 Running DCOM Server Process Launcher

 Running Dell Client Management Service

 Running Dell Data Vault Processor

 Running Dell Data Vault Service API

 Running Dell Hardware Support

 Running Dell SupportAssist

 Running Device Association Service

 Running DHCP Client

 Running Diagnostic Policy Service

 Running Diagnostic Service Host

 Running Diagnostic System Host

 Running Distributed Transaction Coordinator

 Running DNS Client

 Running DSS Express

 Running Function Discovery Provider Host

 Running Function Discovery Resource Publication

 Running Geolocation Service

 Running Group Policy Client

 Running Human Interface Device Service

 Running iNode DAM Agent

 Running iNode Service

 Running Intel Content Protection HDCP Service

 Running Intel Content Protection HECI Service

 Running Intel Dynamic Application Loader Host Interface Service

 Running Intel HD Graphics Control Panel Service

 Running Intel Management and Security Application Local Management Service

 Running Intel Rapid Storage Technology

 Running Intel Storage Middleware Service

 Running IP Helper

 Running Local Session Manager

 Running McAfee Agent Backwards Compatibility Service

 Running McAfee Agent Common Services

 Running McAfee Agent Service

 Running McAfee Endpoint Security Web Control Service

 Running McAfee Service Controller

 Running McAfee Validation Trust Protection Service

 Running McAfee WebAdvisor

 Running Microsoft iSCSI Initiator Service

 Running Net Driver HPZ12

 Running Network Connected Devices Auto-Setup

 Running Network Connection Broker

 Running Network List Service

 Running Network Location Awareness

 Running Network Store Interface Service

 Running Peer Name Resolution Protocol

 Running Peer Networking Identity Manager

 Running Plug and Play

 Running Pml Driver HPZ12

 Running Power

 Running Print Spooler

 Running Program Compatibility Assistant Service

 Running Radio Management Service

 Running Realtek Audio Service

 Running Remote Access Connection Manager

 Running Remote Procedure Call (RPC)

 Running RPC Endpoint Mapper

 Running Secure Socket Tunneling Protocol Service

 Running Security Accounts Manager

 Running Security Center

 Running Server

 Running Shell Hardware Detection

 Running Splashtop Software Updater Service

 Running Splashtop Remote Service

 Running SSDP Discovery

 Running State Repository Service

 Running Storage Service

 Running Sync Host\_ba84e

 Running SysMain

 Running System Event Notification Service

 Running System Events Broker

 Running System Guard Runtime Monitor Broker

 Running Task Scheduler

 Running TCP/IP NetBIOS Helper

 Running Telephony

 Running Themes

 Running Time Broker

 Running Touch Keyboard and Handwriting Panel Service

 Running Update Orchestrator Service

 Running User Manager

 Running User Profile Service

 Running Waves Audio Services

 Running Web Account Manager

 Running Windows Audio

 Running Windows Audio Endpoint Builder

 Running Windows Connection Manager

 Running Windows Defender Firewall

 Running Windows Event Log

 Running Windows Font Cache Service

 Running Windows Image Acquisition (WIA)

 Running Windows Management Instrumentation

 Running Windows Presentation Foundation Font Cache 3.0.0.0

 Running Windows Push Notifications System Service

 Running Windows Push Notifications User Service\_ba84e

 Running Windows Search

 Running Windows Security Service

 Running Windows Update

 Running WinHTTP Web Proxy Auto-Discovery Service

 Running WLAN AutoConfig

 Running WMI Performance Adapter

 Running Workstation

 Stopped ActiveX Installer (AxInstSV)

 Stopped AllJoyn Router Service

 Stopped App Readiness

 Stopped Application Identity

 Stopped Application Information

 Stopped Application Layer Gateway Service

 Stopped Application Management

 Stopped AssignedAccessManager Service

 Stopped Auto Time Zone Updater

 Stopped AVCTP service

 Stopped Block Level Backup Engine Service

 Stopped Bluetooth Audio Gateway Service

 Stopped Bluetooth Support Service

 Stopped Bluetooth User Support Service\_ba84e

 Stopped BranchCache

 Stopped Brave Update Service (brave)

 Stopped Brave Update Service (bravem)

 Stopped Capability Access Manager Service

 Stopped CaptureService\_ba84e

 Stopped Certificate Propagation

 Stopped Client License Service (ClipSVC)

 Stopped Computer Browser

 Stopped ConsentUX\_ba84e

 Stopped Contact Data\_ba84e

 Stopped Data Sharing Service

 Stopped Delivery Optimization

 Stopped Dell Data Vault Collector

 Stopped Device Install Service

 Stopped Device Management Enrollment Service

 Stopped Device Management Wireless Application Protocol (WAP) Push message Routing Service

 Stopped Device Setup Manager

 Stopped DevicePicker\_ba84e

 Stopped DevicesFlow\_ba84e

 Stopped DevQuery Background Discovery Broker

 Stopped Diagnostic Execution Service

 Stopped Display Enhancement Service

 Stopped Distributed Link Tracking Client

 Stopped Downloaded Maps Manager

 Stopped Embedded Mode

 Stopped Encrypting File System (EFS)

 Stopped Enterprise App Management Service

 Stopped Extensible Authentication Protocol

 Stopped Fax

 Stopped File History Service

 Stopped GameDVR and Broadcast User Service\_ba84e

 Stopped Google Chrome Elevation Service

 Stopped Google Update Service (gupdate)

 Stopped Google Update Service (gupdatem)

 Stopped GraphicsPerfSvc

 Stopped HV Host Service

 Stopped Hyper-V Data Exchange Service

 Stopped Hyper-V Guest Service Interface

 Stopped Hyper-V Guest Shutdown Service

 Stopped Hyper-V Heartbeat Service

 Stopped Hyper-V PowerShell Direct Service

 Stopped Hyper-V Remote Desktop Virtualization Service

 Stopped Hyper-V Time Synchronization Service

 Stopped Hyper-V Volume Shadow Copy Requestor

 Stopped IKE and AuthIP IPsec Keying Modules

 Stopped Infrared monitor service

 Stopped Intel Capability Licensing Service TCP IP Interface

 Stopped Intel Optane Memory Service

 Stopped Intel RST HFC Disable Service

 Stopped Intel TPM Provisioning Service

 Stopped Internet Connection Sharing (ICS)

 Stopped IP Translation Configuration Service

 Stopped IPsec Policy Agent

 Stopped KtmRm for Distributed Transaction Coordinator

 Stopped Language Experience Service

 Stopped Link-Layer Topology Discovery Mapper

 Stopped Local Profile Assistant Service

 Stopped McAfee Firewall Core Service

 Stopped MessagingService\_ba84e

 Stopped Microsoft Diagnostics Hub Standard Collector Service

 Stopped Microsoft Account Sign-in Assistant

 Stopped Microsoft App-V Client

 Stopped Microsoft Passport

 Stopped Microsoft Passport Container

 Stopped Microsoft Software Shadow Copy Provider

 Stopped Microsoft Storage Spaces SMP

 Stopped Microsoft Store Install Service

 Stopped Microsoft Windows SMS Router Service.

 Stopped Mozilla Maintenance Service

 Stopped Natural Authentication

 Stopped Net.Tcp Port Sharing Service

 Stopped Netlogon

 Stopped Network Connections

 Stopped Network Connectivity Assistant

 Stopped Network Setup Service

 Stopped Office 64 Source Engine

 Stopped Offline Files

 Stopped OpenSSH Authentication Agent

 Stopped Optimize drives

 Stopped Parental Controls

 Stopped Payments and NFC/SE Manager

 Stopped Peer Networking Grouping

 Stopped Performance Counter DLL Host

 Stopped Performance Logs & Alerts

 Stopped Phone Service

 Stopped PNRP Machine Name Publication Service

 Stopped Portable Device Enumerator Service

 Stopped Printer Extensions and Notifications

 Stopped PrintWorkflow\_ba84e

 Stopped Problem Reports and Solutions Control Panel Support

 Stopped Quality Windows Audio Video Experience

 Stopped Remote Access Auto Connection Manager

 Stopped Remote Desktop Configuration

 Stopped Remote Desktop Services

 Stopped Remote Desktop Services UserMode Port Redirector

 Stopped Remote Procedure Call (RPC) Locator

 Stopped Remote Registry

 Stopped Retail Demo Service

 Stopped Routing and Remote Access

 Stopped Secondary Logon

 Stopped Sensor Data Service

 Stopped Sensor Monitoring Service

 Stopped Sensor Service

 Stopped Shared PC Account Manager

 Stopped Smart Card

 Stopped Smart Card Device Enumeration Service

 Stopped Smart Card Removal Policy

 Stopped SNMP Trap

 Stopped Software Protection

 Stopped Spatial Data Service

 Stopped Spot Verifier

 Stopped Still Image Acquisition Events

 Stopped Storage Tiers Management

 Stopped UPnP Device Host

 Stopped User Data Access\_ba84e

 Stopped User Data Storage\_ba84e

 Stopped User Experience Virtualization Service

 Stopped Virtual Disk

 Stopped Volume Shadow Copy

 Stopped Volumetric Audio Compositor Service

 Stopped WalletService

 Stopped WarpJITSvc

 Stopped WebClient

 Stopped Wi-Fi Direct Services Connection Manager Service

 Stopped Windows Backup

 Stopped Windows Biometric Service

 Stopped Windows Camera Frame Server

 Stopped Windows Connect Now - Config Registrar

 Stopped Windows Defender Advanced Threat Protection Service

 Stopped Windows Defender Antivirus Network Inspection Service

 Stopped Windows Defender Antivirus Service

 Stopped Windows Encryption Provider Host Service

 Stopped Windows Error Reporting Service

 Stopped Windows Event Collector

 Stopped Windows Insider Service

 Stopped Windows Installer

 Stopped Windows License Manager Service

 Stopped Windows Management Service

 Stopped Windows Media Player Network Sharing Service

 Stopped Windows Mobile Hotspot Service

 Stopped Windows Modules Installer

 Stopped Windows Perception Service

 Stopped Windows Perception Simulation Service

 Stopped Windows PushToInstall Service

 Stopped Windows Remote Management (WS-Management)

 Stopped Windows Time

 Stopped Windows Update Medic Service

 Stopped Wired AutoConfig

 Stopped Work Folders

 Stopped WWAN AutoConfig

 Stopped Xbox Accessory Management Service

 Stopped Xbox Live Auth Manager

 Stopped Xbox Live Game Save

 Stopped Xbox Live Networking Service

 TimeZone

 TimeZone GMT -8:00 Hours

 Language English (United States)

 Location United States

 Format English (United States)

 Currency $

 Date Format M/d/yyyy

 Time Format h:mm:ss tt

 Scheduler

 11/22/2019 8:44 AM; GoogleUpdateTaskMachineUA

 11/22/2019 8:47 AM; BraveSoftwareUpdateTaskMachineUA

 11/22/2019 8:53 AM; G2MUploadTask-S-1-5-21-1410435651-646996757-2559596686-1001

 11/22/2019 9:31 AM; G2MUpdateTask-S-1-5-21-1410435651-646996757-2559596686-1001

 11/22/2019 4:08 PM; Adobe Flash Player PPAPI Notifier

 11/22/2019 5:44 PM; GoogleUpdateTaskMachineCore

 11/23/2019 6:47 AM; BraveSoftwareUpdateTaskMachineCore

 11/23/2019 7:00 AM; Adobe Acrobat Update Task

 11/24/2019 10:26 AM; Dell SupportAssistAgent AutoUpdate

 CCleanerSkipUAC

 Hotfixes

 Installed

 11/13/2019 Update for Microsoft Word 2016 (KB4484135) 64-Bit Edition

 Microsoft has released an update for Microsoft Word 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Word

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 11/13/2019 Update for Microsoft PowerPoint 2016 (KB4484134) 64-Bit Edition

 Microsoft has released an update for Microsoft PowerPoint 2016

 64-Bit Edition. This update provides the latest fixes to Microsoft

 PowerPoint 2016 64-Bit Edition. Additionally, this update contains

 stability and performance improvements.

 11/13/2019 Update for Microsoft Outlook 2016 (KB4484139) 64-Bit Edition

 Microsoft has released an update for Microsoft Outlook 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Outlook

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 11/13/2019 Update for Microsoft Office 2016 (KB4484145) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 11/13/2019 Update for Microsoft Office 2016 (KB4475552) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 11/13/2019 Update for Microsoft Access 2016 (KB4475539) 64-Bit Edition

 Microsoft has released an update for Microsoft Access 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Access

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 11/13/2019 Update for Microsoft Office 2016 (KB4484138) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 11/13/2019 Update for Microsoft Office 2016 (KB4475588) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 11/13/2019 Update for Microsoft Office 2016 (KB4484137) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 11/13/2019 Windows Malicious Software Removal Tool x64 - November 2019 (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.

 11/13/2019 Security Update for Microsoft Office 2016 (KB4484148) 64-Bit Edition

 A security vulnerability exists in Microsoft Office 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 11/13/2019 Security Update for Microsoft Excel 2016 (KB4484144) 64-Bit Edition

 A security vulnerability exists in Microsoft Excel 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 11/13/2019 Security Update for Microsoft Office 2016 (KB4484113) 64-Bit Edition

 A security vulnerability exists in Microsoft Office 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 11/13/2019 2019-11 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB4523205)

 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.

 10/29/2019 Acer Incorporated. - Other hardware - USB Ethernet/RNDIS Gadget

 Acer Incorporated. Other hardware software update released in

 January, 2010

 10/17/2019 Security Update for Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package (KB2565063)

 A security issue has been identified leading to MFC application

 vulnerability in DLL planting due to MFC not specifying the full

 path to system/localization DLLs. You can protect your computer

 by installing this update from Microsoft. After you install this

 item, you may have to restart your computer.

 10/9/2019 Windows Malicious Software Removal Tool x64 - October 2019 (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.

 10/9/2019 Security Update for Microsoft Office 2016 (KB4475554) 64-Bit Edition

 A security vulnerability exists in Microsoft Office 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 10/9/2019 Security Update for Microsoft Excel 2016 (KB4484112) 64-Bit Edition

 A security vulnerability exists in Microsoft Excel 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 10/9/2019 2019-10 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB4519338)

 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.

 10/3/2019 2019-09 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB4524148)

 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.

 10/1/2019 Update for Microsoft Word 2016 (KB4484105) 64-Bit Edition

 Microsoft has released an update for Microsoft Word 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Word

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 10/1/2019 Update for Microsoft Project 2016 (KB4484116) 64-Bit Edition

 Microsoft has released an update for Microsoft Project 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Project

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 10/1/2019 Update for Microsoft PowerPoint 2016 (KB4475578) 64-Bit Edition

 Microsoft has released an update for Microsoft PowerPoint 2016

 64-Bit Edition. This update provides the latest fixes to Microsoft

 PowerPoint 2016 64-Bit Edition. Additionally, this update contains

 stability and performance improvements.

 10/1/2019 Update for Microsoft Outlook 2016 (KB4484107) 64-Bit Edition

 Microsoft has released an update for Microsoft Outlook 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Outlook

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 10/1/2019 Update for Microsoft Office 2016 (KB4484114) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 10/1/2019 Update for Skype for Business 2016 (KB4484102) 64-Bit Edition

 Microsoft has released an update for Skype for Business 2016

 64-Bit Edition. This update provides the latest fixes to Skype

 for Business 2016 64-Bit Edition. Additionally, this update contains

 stability and performance improvements.

 10/1/2019 Update for Microsoft Office 2016 (KB4475585) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 10/1/2019 2019-09 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64 (KB4516550)

 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.

 10/1/2019 2019-09 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB4516077)

 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.

 9/24/2019 Update for Windows Defender Antivirus antimalware platform - KB4052623 (Version 4.18.1909.5)

 This package will update Windows Defender Antivirus antimalware

 platform’s components on the user machine.

 9/24/2019 Security Intelligence Update for Windows Defender Antivirus - KB2267602 (Version 1.303.25.0)

 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.

 9/11/2019 2019-09 Security Update for Adobe Flash Player for Windows 10 Version 1809 for x64-based Systems (KB4516115)

 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.

 9/11/2019 2019-09 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64 (KB4514601)

 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.

 9/11/2019 2019-09 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB4512578)

 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.

 9/10/2019 Update for Microsoft Word 2016 (KB4475592) 64-Bit Edition

 Microsoft has released an update for Microsoft Word 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Word

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 9/10/2019 Update for Microsoft Office 2016 (KB3114852) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 9/10/2019 Update for Microsoft Outlook 2016 (KB4475593) 64-Bit Edition

 Microsoft has released an update for Microsoft Outlook 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Outlook

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 9/10/2019 Update for Microsoft Office 2016 (KB4475580) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 9/10/2019 Update for Microsoft Office 2016 (KB4464531) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 9/10/2019 Update for Microsoft Office 2016 (KB4464584) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 9/10/2019 Update for Skype for Business 2016 (KB4475577) 64-Bit Edition

 Microsoft has released an update for Skype for Business 2016

 64-Bit Edition. This update provides the latest fixes to Skype

 for Business 2016 64-Bit Edition. Additionally, this update contains

 stability and performance improvements.

 9/10/2019 Update for Microsoft Office 2016 (KB4011629) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 9/10/2019 Security Update for Microsoft Office 2016 (KB4475591) 64-Bit Edition

 A security vulnerability exists in Microsoft Office 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 9/10/2019 Security Update for Microsoft Excel 2016 (KB4475579) 64-Bit Edition

 A security vulnerability exists in Microsoft Excel 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 9/10/2019 Security Update for Microsoft Office 2016 (KB4475583) 64-Bit Edition

 A security vulnerability exists in Microsoft Office 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 9/10/2019 Security Update for Microsoft Project 2016 (KB4475589) 64-Bit Edition

 A security vulnerability exists in Microsoft Project 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 8/14/2019 Update for Microsoft Office 2016 (KB4475551) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 8/14/2019 Update for Microsoft PowerPoint 2016 (KB4464577) 64-Bit Edition

 Microsoft has released an update for Microsoft PowerPoint 2016

 64-Bit Edition. This update provides the latest fixes to Microsoft

 PowerPoint 2016 64-Bit Edition. Additionally, this update contains

 stability and performance improvements.

 8/14/2019 Update for Microsoft Office 2016 (KB4032254) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 8/14/2019 Update for Skype for Business 2016 (KB4475548) 64-Bit Edition

 Microsoft has released an update for Skype for Business 2016

 64-Bit Edition. This update provides the latest fixes to Skype

 for Business 2016 64-Bit Edition. Additionally, this update contains

 stability and performance improvements.

 8/14/2019 Update for Microsoft Office 2016 (KB4464535) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 8/14/2019 Update for Microsoft Office 2016 (KB3141456) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 8/14/2019 Update for Microsoft OneNote 2016 (KB4092450) 64-Bit Edition

 Microsoft has released an update for Microsoft OneNote 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft OneNote

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 8/14/2019 Update for Microsoft Office 2016 (KB4464588) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 8/14/2019 Update for Microsoft Office 2016 (KB4475542) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 8/14/2019 Update for Microsoft Project 2016 (KB4475544) 64-Bit Edition

 Microsoft has released an update for Microsoft Project 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Project

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 8/14/2019 Windows Malicious Software Removal Tool x64 - August 2019 (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.

 8/13/2019 Update for Microsoft Office 2016 (KB3114528) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 8/13/2019 Update for Microsoft Excel 2016 (KB4475550) 64-Bit Edition

 Microsoft has released an update for Microsoft Excel 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Excel

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 8/13/2019 Update for Microsoft Office 2016 (KB4475516) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 8/13/2019 2019-08 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB4511553)

 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.

 8/13/2019 Security Update for Microsoft Word 2016 (KB4475540) 64-Bit Edition

 A security vulnerability exists in Microsoft Word 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 8/13/2019 Security Update for Microsoft Outlook 2016 (KB4475553) 64-Bit Edition

 A security vulnerability exists in Microsoft Outlook 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 8/13/2019 Security Update for Microsoft Office 2016 (KB4475538) 64-Bit Edition

 A security vulnerability exists in Microsoft Office 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 7/25/2019 9NB9SRTL2KPT-WavesAudio.WavesMaxxAudioProforDell

 9NB9SRTL2KPT-1152921505688042297

 7/25/2019 9NZM7B1BB5TR-Microsoft.NET.Native.Framework.1.7

 9NZM7B1BB5TR-1152921505688395033

 7/25/2019 9MTW6RN84LVM-Microsoft.NET.Native.Runtime.1.7

 9MTW6RN84LVM-1152921504626672001

 7/25/2019 Waves - SoftwareComponent - 11/29/2018 12:00:00 AM - 3.2.0.81

 Waves SoftwareComponent driver update released in November 2018

 7/25/2019 Dell - Extension - 5/22/2019 12:00:00 AM - 1.3.2.276

 Dell Extension driver update released in May 2019

 7/10/2019 Update for Microsoft Word 2016 (KB4475521) 64-Bit Edition

 Microsoft has released an update for Microsoft Word 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Word

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 7/10/2019 Update for Microsoft Project 2016 (KB4475518) 64-Bit Edition

 Microsoft has released an update for Microsoft Project 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Project

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 7/10/2019 Update for Microsoft Office 2016 (KB4464582) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 7/10/2019 Update for Microsoft Access 2016 (KB4462237) 64-Bit Edition

 Microsoft has released an update for Microsoft Access 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Access

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 7/10/2019 Update for Microsoft Office 2016 (KB4464595) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 7/10/2019 2019-07 Cumulative Update for .NET Framework 3.5, 4.7.2, 4.8 for Windows 10 Version 1809 for x64 (KB4507419)

 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.

 7/10/2019 Windows Malicious Software Removal Tool x64 - July 2019 (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.

 7/10/2019 2019-07 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB4507469)

 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.

 7/9/2019 Security Update for Microsoft Outlook 2016 (KB4475517) 64-Bit Edition

 A security vulnerability exists in Microsoft Outlook 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 7/9/2019 Security Update for Microsoft Office 2016 (KB4464534) 64-Bit Edition

 A security vulnerability exists in Microsoft Office 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 7/9/2019 Security Update for Microsoft Office 2016 (KB4475514) 64-Bit Edition

 A security vulnerability exists in Microsoft Office 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 7/9/2019 Security Update for Skype for Business 2016 (KB4475545) 64-Bit Edition

 A security vulnerability exists in Skype for Business 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 7/9/2019 Security Update for Microsoft Office 2016 (KB4461539) 64-Bit Edition

 A security vulnerability exists in Microsoft Office 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 7/9/2019 Security Update for Microsoft Excel 2016 (KB4475513) 64-Bit Edition

 A security vulnerability exists in Microsoft Excel 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 6/26/2019 2019-06 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB4503327)

 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.

 6/25/2019 Elgato - Media - 7/7/2014 12:00:00 AM - 2.1.1.3

 Elgato Media driver update released in July 2014

 6/25/2019 Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.295.1460.0)

 Install this update to revise the definition files that are used

 to detect viruses, spyware, and other potentially unwanted software.

 Once you have installed this item, it cannot be removed.

 6/25/2019 Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.295.1457.0)

 Install this update to revise the definition files that are used

 to detect viruses, spyware, and other potentially unwanted software.

 Once you have installed this item, it cannot be removed.

 6/25/2019 Realtek Semiconductor Corp. - Net - 5/28/2019 12:00:00 AM - 1030.38.328.2019

 Realtek Semiconductor Corp. Net driver update released in May

 2019

 6/25/2019 Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.295.1457.0)

 Install this update to revise the definition files that are used

 to detect viruses, spyware, and other potentially unwanted software.

 Once you have installed this item, it cannot be removed.

 6/24/2019 Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.295.1381.0)

 Install this update to revise the definition files that are used

 to detect viruses, spyware, and other potentially unwanted software.

 Once you have installed this item, it cannot be removed.

 6/21/2019 Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.295.1180.0)

 Install this update to revise the definition files that are used

 to detect viruses, spyware, and other potentially unwanted software.

 Once you have installed this item, it cannot be removed.

 6/21/2019 Security Update for Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package (KB2538243)

 A security issue has been identified leading to MFC application

 vulnerability in DLL planting due to MFC not specifying the full

 path to system/localization DLLs. You can protect your computer

 by installing this update from Microsoft. After you install this

 item, you may have to restart your computer.

 6/21/2019 Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.295.1177.0)

 Install this update to revise the definition files that are used

 to detect viruses, spyware, and other potentially unwanted software.

 Once you have installed this item, it cannot be removed.

 6/19/2019 Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.295.1037.0)

 Install this update to revise the definition files that are used

 to detect viruses, spyware, and other potentially unwanted software.

 Once you have installed this item, it cannot be removed.

 6/19/2019 2019-02 Update for Windows 10 Version 1809 for x64-based Systems (KB4465065)

 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.

 6/19/2019 Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.295.1025.0)

 Install this update to revise the definition files that are used

 to detect viruses, spyware, and other potentially unwanted software.

 Once you have installed this item, it cannot be removed.

 6/18/2019 2019-06 Security Update for Adobe Flash Player for Windows 10 Version 1809 for x64-based Systems (KB4503308)

 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.

 6/18/2019 Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.295.959.0)

 Install this update to revise the definition files that are used

 to detect viruses, spyware, and other potentially unwanted software.

 Once you have installed this item, it cannot be removed.

 6/18/2019 HP - Printers - HP Universal Printing PCL 6

 HP Printers software update released in January, 2013

 6/17/2019 Realtek Semiconductor Corp. - MEDIA - 10/17/2018 12:00:00 AM - 6.0.1.8555

 Realtek Semiconductor Corp. MEDIA driver update released in October

 2018

 6/17/2019 Security Update for Microsoft Word 2016 (KB4464596) 64-Bit Edition

 A security vulnerability exists in Microsoft Word 2016 64-Bit

 Edition that could allow arbitrary code to run when a maliciously

 modified file is opened. This update resolves that vulnerability.

 6/17/2019 Update for Microsoft Project 2016 (KB4464589) 64-Bit Edition

 Microsoft has released an update for Microsoft Project 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Project

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 6/17/2019 Update for Microsoft Office 2016 (KB4464579) 64-Bit Edition

 Microsoft has released an update for Microsoft Office 2016 64-Bit

 Edition. This update provides the latest fixes to Microsoft Office

 2016 64-Bit Edition. Additionally, this update contains stability

 and performance improvements.

 6/17/2019 2019-05 Security Update for Adobe Flash Player for Windows 10 Version 1809 for x64-based Systems (KB4497932)

 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.

 6/17/2019 2019-05 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64 (KB4499405)

 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.

 6/17/2019 Update for Adobe Flash Player for Windows 10 Version 1809 for x64-based Systems (KB4462930)

 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.

 6/17/2019 Update for Windows Defender Antivirus antimalware platform - KB4052623 (Version 4.18.1905.4)

 This package will update Windows Defender Antivirus antimalware

 platform’s components on the user machine.

 6/17/2019 Apple, Inc. - USBDevice - 5/7/2018 12:00:00 AM - 423.36

 Apple, Inc. USBDevice driver update released in May 2018

 Not Installed

 8/29/2019 Feature update to Windows 10, version 1903

 Installation Status Failed

 Install the latest update for Windows 10: Windows 10, version

 1903.

 8/29/2019 Feature update to Windows 10, version 1903

 Installation Status Failed

 Install the latest update for Windows 10: Windows 10, version

 1903.

 8/29/2019 Feature update to Windows 10, version 1903

 Installation Status Failed

 Install the latest update for Windows 10: Windows 10, version

 1903.

 6/17/2019 Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.295.897.0)

 Installation Status Canceled

 Install this update to revise the definition files that are used

 to detect viruses, spyware, and other potentially unwanted software.

 Once you have installed this item, it cannot be removed.

 System Folders

 Application Data C:\ProgramData

 Cookies C:\Users\Dahua\AppData\Local\Microsoft\Windows\INetCookies

 Desktop C:\Users\Dahua\Desktop

 Documents C:\Users\Public\Documents

 Fonts C:\WINDOWS\Fonts

 Global Favorites C:\Users\Dahua\Favorites

 Internet History C:\Users\Dahua\AppData\Local\Microsoft\Windows\History

 Local Application Data C:\Users\Dahua\AppData\Local

 Music C:\Users\Public\Music

 Path for burning CD C:\Users\Dahua\AppData\Local\Microsoft\Windows\Burn\Burn

 Physical Desktop C:\Users\Dahua\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\Dahua\AppData\Local\Microsoft\Windows\INetCache

 User Favorites C:\Users\Dahua\Favorites

 Videos C:\Users\Public\Videos

 Windows Directory C:\WINDOWS

 Windows/System C:\WINDOWS\system32

 Process List

 AnyDesk-b067a865.exe

 Process ID 3872

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\AnyDesk-b067a865\AnyDesk-b067a865.exe

 Memory Usage 7.76 MB

 Peak Memory Usage 19 MB

 AnyDesk-b067a865.exe

 Process ID 15924

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\AnyDesk-b067a865\AnyDesk-b067a865.exe

 Memory Usage 9.43 MB

 Peak Memory Usage 20 MB

 AnyDesk.exe

 Process ID 3668

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\AnyDesk\AnyDesk.exe

 Memory Usage 10 MB

 Peak Memory Usage 25 MB

 AnyDesk.exe

 Process ID 3864

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\AnyDesk\AnyDesk.exe

 Memory Usage 8.30 MB

 Peak Memory Usage 24 MB

 armsvc.exe

 Process ID 3856

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe

 Memory Usage 4.82 MB

 Peak Memory Usage 6.67 MB

 audiodg.exe

 Process ID 2132

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\audiodg.exe

 Memory Usage 20 MB

 Peak Memory Usage 68 MB

 brave.exe

 Process ID 20760

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe

 Memory Usage 65 MB

 Peak Memory Usage 135 MB

 brave.exe

 Process ID 6628

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe

 Memory Usage 86 MB

 Peak Memory Usage 164 MB

 brave.exe

 Process ID 17728

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe

 Memory Usage 14 MB

 Peak Memory Usage 20 MB

 brave.exe

 Process ID 7468

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe

 Memory Usage 4.94 MB

 Peak Memory Usage 6.56 MB

 brave.exe

 Process ID 13180

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe

 Memory Usage 99 MB

 Peak Memory Usage 248 MB

 brave.exe

 Process ID 19940

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe

 Memory Usage 111 MB

 Peak Memory Usage 190 MB

 brave.exe

 Process ID 18588

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe

 Memory Usage 29 MB

 Peak Memory Usage 45 MB

 brave.exe

 Process ID 20616

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe

 Memory Usage 32 MB

 Peak Memory Usage 53 MB

 brave.exe

 Process ID 18768

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe

 Memory Usage 9.25 MB

 Peak Memory Usage 12 MB

 brave.exe

 Process ID 18544

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe

 Memory Usage 22 MB

 Peak Memory Usage 32 MB

 brave.exe

 Process ID 13140

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe

 Memory Usage 8.80 MB

 Peak Memory Usage 11 MB

 brave.exe

 Process ID 20116

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe

 Memory Usage 30 MB

 Peak Memory Usage 49 MB

 browserhost.exe

 Process ID 3020

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files\McAfee\WebAdvisor\O005CBA.tmp

 Memory Usage 11 MB

 Peak Memory Usage 18 MB

 CCleaner64.exe

 Process ID 1160

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files\CCleaner\CCleaner64.exe

 Memory Usage 36 MB

 Peak Memory Usage 50 MB

 chrome.exe

 Process ID 18388

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 35 MB

 Peak Memory Usage 38 MB

 chrome.exe

 Process ID 17144

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 61 MB

 Peak Memory Usage 61 MB

 chrome.exe

 Process ID 7396

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 35 MB

 Peak Memory Usage 37 MB

 chrome.exe

 Process ID 15608

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 74 MB

 Peak Memory Usage 76 MB

 chrome.exe

 Process ID 17264

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 34 MB

 Peak Memory Usage 36 MB

 chrome.exe

 Process ID 11788

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 35 MB

 Peak Memory Usage 37 MB

 chrome.exe

 Process ID 19356

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 61 MB

 Peak Memory Usage 73 MB

 chrome.exe

 Process ID 20344

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 26 MB

 Peak Memory Usage 36 MB

 chrome.exe

 Process ID 20040

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 66 MB

 Peak Memory Usage 106 MB

 chrome.exe

 Process ID 18552

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 205 MB

 Peak Memory Usage 294 MB

 chrome.exe

 Process ID 436

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 36 MB

 Peak Memory Usage 37 MB

 chrome.exe

 Process ID 16188

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 12 MB

 Peak Memory Usage 13 MB

 chrome.exe

 Process ID 2348

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 22 MB

 Peak Memory Usage 30 MB

 chrome.exe

 Process ID 20824

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 45 MB

 Peak Memory Usage 64 MB

 chrome.exe

 Process ID 15612

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 35 MB

 Peak Memory Usage 37 MB

 chrome.exe

 Process ID 20932

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 37 MB

 Peak Memory Usage 46 MB

 chrome.exe

 Process ID 21424

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 167 MB

 Peak Memory Usage 211 MB

 chrome.exe

 Process ID 17672

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 6.89 MB

 Peak Memory Usage 8.63 MB

 chrome.exe

 Process ID 21136

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 5.49 MB

 Peak Memory Usage 6.62 MB

 chrome.exe

 Process ID 20424

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 150 MB

 Peak Memory Usage 171 MB

 chrome.exe

 Process ID 20648

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 40 MB

 Peak Memory Usage 48 MB

 chrome.exe

 Process ID 16908

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 38 MB

 Peak Memory Usage 39 MB

 chrome.exe

 Process ID 12572

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 42 MB

 Peak Memory Usage 43 MB

 chrome.exe

 Process ID 5668

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 54 MB

 Peak Memory Usage 55 MB

 chrome.exe

 Process ID 17160

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 83 MB

 Peak Memory Usage 97 MB

 chrome.exe

 Process ID 1992

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 108 MB

 Peak Memory Usage 143 MB

 chrome.exe

 Process ID 18604

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 33 MB

 Peak Memory Usage 35 MB

 chrome.exe

 Process ID 17092

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

 Memory Usage 20 MB

 Peak Memory Usage 20 MB

 cmd.exe

 Process ID 19892

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\cmd.exe

 Memory Usage 2.70 MB

 Peak Memory Usage 3.79 MB

 cmd.exe

 Process ID 5876

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\SysWOW64\cmd.exe

 Memory Usage 3.17 MB

 Peak Memory Usage 4.82 MB

 CompatTelRunner.exe

 Process ID 8324

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\CompatTelRunner.exe

 Memory Usage 14 MB

 Peak Memory Usage 14 MB

 conhost.exe

 Process ID 8528

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 5.89 MB

 Peak Memory Usage 12 MB

 conhost.exe

 Process ID 8572

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 9.61 MB

 Peak Memory Usage 12 MB

 conhost.exe

 Process ID 8612

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 6.14 MB

 Peak Memory Usage 12 MB

 conhost.exe

 Process ID 8512

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 6.02 MB

 Peak Memory Usage 12 MB

 conhost.exe

 Process ID 8380

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 5.73 MB

 Peak Memory Usage 12 MB

 conhost.exe

 Process ID 8344

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 5.54 MB

 Peak Memory Usage 12 MB

 conhost.exe

 Process ID 8316

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 5.88 MB

 Peak Memory Usage 12 MB

 conhost.exe

 Process ID 15020

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 3.77 MB

 Peak Memory Usage 10 MB

 conhost.exe

 Process ID 18168

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 3.95 MB

 Peak Memory Usage 10 MB

 conhost.exe

 Process ID 8244

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 5.84 MB

 Peak Memory Usage 12 MB

 conhost.exe

 Process ID 1672

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 12 MB

 Peak Memory Usage 12 MB

 conhost.exe

 Process ID 9196

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 5.53 MB

 Peak Memory Usage 12 MB

 conhost.exe

 Process ID 7408

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 4.06 MB

 Peak Memory Usage 11 MB

 conhost.exe

 Process ID 6600

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 3.94 MB

 Peak Memory Usage 11 MB

 conhost.exe

 Process ID 9012

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 6.43 MB

 Peak Memory Usage 12 MB

 conhost.exe

 Process ID 18596

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\conhost.exe

 Memory Usage 5.95 MB

 Peak Memory Usage 13 MB

 conhost.exe

 Process ID 6568

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 4.02 MB

 Peak Memory Usage 11 MB

 conhost.exe

 Process ID 6552

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 4.01 MB

 Peak Memory Usage 11 MB

 conhost.exe

 Process ID 6396

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 5.72 MB

 Peak Memory Usage 12 MB

 conhost.exe

 Process ID 15696

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 5.77 MB

 Peak Memory Usage 12 MB

 conhost.exe

 Process ID 5040

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\conhost.exe

 Memory Usage 3.93 MB

 Peak Memory Usage 11 MB

 conhost.exe

 Process ID 13800

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\conhost.exe

 Memory Usage 5.61 MB

 Peak Memory Usage 13 MB

 csrss.exe

 Process ID 832

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\csrss.exe

 Memory Usage 4.07 MB

 Peak Memory Usage 5.72 MB

 csrss.exe

 Process ID 936

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\csrss.exe

 Memory Usage 4.84 MB

 Peak Memory Usage 21 MB

 ctfmon.exe

 Process ID 13632

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\ctfmon.exe

 Memory Usage 14 MB

 Peak Memory Usage 16 MB

 DamAgent.exe

 Process ID 14056

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\iNode DAM Agent\A96B1E2F2FA4EB41A2EECF23B35902FF\DamAgent.exe

 Memory Usage 11 MB

 Peak Memory Usage 15 MB

 DamAgentTray.exe

 Process ID 14640

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\iNode DAM Agent\A96B1E2F2FA4EB41A2EECF23B35902FF\DamAgentTray.exe

 Memory Usage 7.32 MB

 Peak Memory Usage 10 MB

 dasHost.exe

 Process ID 3424

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\dasHost.exe

 Memory Usage 15 MB

 Peak Memory Usage 19 MB

 DDVCollectorSvcApi.exe

 Process ID 20404

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\Dell\DellDataVault\DDVCollectorSvcApi.exe

 Memory Usage 5.66 MB

 Peak Memory Usage 7.06 MB

 DDVRulesProcessor.exe

 Process ID 2944

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\Dell\DellDataVault\DDVRulesProcessor.exe

 Memory Usage 12 MB

 Peak Memory Usage 15 MB

 dllhost.exe

 Process ID 2088

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\dllhost.exe

 Memory Usage 11 MB

 Peak Memory Usage 12 MB

 dllhost.exe

 Process ID 18004

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\dllhost.exe

 Memory Usage 9.87 MB

 Peak Memory Usage 13 MB

 dllhost.exe

 Process ID 22324

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\dllhost.exe

 Memory Usage 6.27 MB

 Peak Memory Usage 6.28 MB

 DSAPI.exe

 Process ID 15516

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\Dell\SupportAssistAgent\PCDr\SupportAssist\6.0.7033.2285\DSAPI.exe

 Memory Usage 40 MB

 Peak Memory Usage 61 MB

 DSS\_ADS.exe

 Process ID 8196

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\ADS\DSS\_ADS.exe

 Memory Usage 10 MB

 Peak Memory Usage 21 MB

 DSS\_CLog.exe

 Process ID 1316

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\LogTool\DSS\_CLog.exe

 Memory Usage 6.16 MB

 Peak Memory Usage 8.01 MB

 DSS\_DMS.exe

 Process ID 8216

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\DMS\DSS\_DMS.exe

 Memory Usage 7.86 MB

 Peak Memory Usage 51 MB

 DSS\_HRS.exe

 Process ID 8264

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\MachineDiscovery\DSS\_HRS.exe

 Memory Usage 5.48 MB

 Peak Memory Usage 11 MB

 DSS\_MCDAlarm.exe

 Process ID 8284

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\MCDALARM\DSS\_MCDAlarm.exe

 Memory Usage 6.34 MB

 Peak Memory Usage 32 MB

 DSS\_MCDDoor.exe

 Process ID 8336

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\MCDDOOR\DSS\_MCDDoor.exe

 Memory Usage 7.61 MB

 Peak Memory Usage 41 MB

 DSS\_MCDLed.exe

 Process ID 8360

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\MCDLED\DSS\_MCDLed.exe

 Memory Usage 7.23 MB

 Peak Memory Usage 33 MB

 DSS\_MGW.exe

 Process ID 8452

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\MGW\DSS\_MGW.exe

 Memory Usage 5.61 MB

 Peak Memory Usage 12 MB

 DSS\_MQ.exe

 Process ID 11240

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\jre\bin\DSS\_MQ.exe

 Memory Usage 76 MB

 Peak Memory Usage 87 MB

 DSS\_MQWrapper.exe

 Process ID 10420

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\activemq\bin\win32\DSS\_MQWrapper.exe

 Memory Usage 3.97 MB

 Peak Memory Usage 5.20 MB

 DSS\_MTS.exe

 Process ID 8476

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\MTS\DSS\_MTS.exe

 Memory Usage 7.92 MB

 Peak Memory Usage 48 MB

 DSS\_OSS.exe

 Process ID 8236

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\OSS\DSS\_OSS.exe

 Memory Usage 7.12 MB

 Peak Memory Usage 15 MB

 DSS\_PCPS.exe

 Process ID 8504

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\PCPS\DSS\_PCPS.exe

 Memory Usage 8.07 MB

 Peak Memory Usage 36 MB

 DSS\_PES.exe

 Process ID 8544

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\PES\DSS\_PES.exe

 Memory Usage 6.65 MB

 Peak Memory Usage 13 MB

 DSS\_PTS.exe

 Process ID 10072

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\PTS\DSS\_PTS.exe

 Memory Usage 9.08 MB

 Peak Memory Usage 69 MB

 DSS\_SC.exe

 Process ID 9024

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\SwitchCenter\DSS\_SC.exe

 Memory Usage 6.73 MB

 Peak Memory Usage 17 MB

 DSS\_Service.exe

 Process ID 4084

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\DSS Service\DSS\_Service.exe

 Memory Usage 12 MB

 Peak Memory Usage 19 MB

 DSS\_SOSO.exe

 Process ID 8628

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\SearchDevice\DSS\_SOSO.exe

 Memory Usage 8.96 MB

 Peak Memory Usage 53 MB

 DSS\_SS.exe

 Process ID 10372

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\SS\DSS\_SS.exe

 Memory Usage 8.85 MB

 Peak Memory Usage 48 MB

 DSS\_VMS.exe

 Process ID 9596

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\VMS\DSS\_VMS.exe

 Memory Usage 6.51 MB

 Peak Memory Usage 31 MB

 DSS\_WEB.exe

 Process ID 4996

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\jre\bin\DSS\_WEB.exe

 Memory Usage 532 MB

 Peak Memory Usage 863 MB

 dwm.exe

 Process ID 1208

 User DWM-1

 Domain Window Manager

 Path C:\Windows\System32\dwm.exe

 Memory Usage 99 MB

 Peak Memory Usage 125 MB

 explorer.exe

 Process ID 14632

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\explorer.exe

 Memory Usage 128 MB

 Peak Memory Usage 157 MB

 fontdrvhost.exe

 Process ID 744

 User UMFD-0

 Domain Font Driver Host

 Path C:\Windows\System32\fontdrvhost.exe

 Memory Usage 2.48 MB

 Peak Memory Usage 4.74 MB

 fontdrvhost.exe

 Process ID 300

 User UMFD-1

 Domain Font Driver Host

 Path C:\Windows\System32\fontdrvhost.exe

 Memory Usage 13 MB

 Peak Memory Usage 18 MB

 IAStorDataMgrSvc.exe

 Process ID 18100

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\Intel\Intel Rapid Storage Technology\IAStorDataMgrSvc.exe

 Memory Usage 55 MB

 Peak Memory Usage 72 MB

 IAStorIcon.exe

 Process ID 17300

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files\Intel\Intel Rapid Storage Technology\IAStorIcon.exe

 Memory Usage 30 MB

 Peak Memory Usage 39 MB

 iexplore.exe

 Process ID 1592

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Internet Explorer\iexplore.exe

 Memory Usage 119 MB

 Peak Memory Usage 154 MB

 iexplore.exe

 Process ID 488

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Internet Explorer\iexplore.exe

 Memory Usage 141 MB

 Peak Memory Usage 152 MB

 iexplore.exe

 Process ID 3284

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files\internet explorer\iexplore.exe

 Memory Usage 46 MB

 Peak Memory Usage 57 MB

 iexplore.exe

 Process ID 13332

 User Dahua

 Domain WIN10-CARLOSESP

 Memory Usage 264 KB

 Peak Memory Usage 268 KB

 igfxCUIService.exe

 Process ID 1680

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\DriverStore\FileRepository\ki132842.inf\_amd64\_e968a65c52333922\igfxCUIService.exe

 Memory Usage 6.36 MB

 Peak Memory Usage 8.50 MB

 igfxEM.exe

 Process ID 15092

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\DriverStore\FileRepository\ki132842.inf\_amd64\_e968a65c52333922\igfxEM.exe

 Memory Usage 16 MB

 Peak Memory Usage 24 MB

 iNode Client.exe

 Process ID 4532

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\iNode\iNode Client\iNode Client.exe

 Memory Usage 19 MB

 Peak Memory Usage 36 MB

 iNodeCmn.exe

 Process ID 6528

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\iNode\iNode Client\iNodeCmn.exe

 Memory Usage 11 MB

 Peak Memory Usage 17 MB

 iNodeImg.exe

 Process ID 4672

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\iNode\iNode Client\iNodeImg.exe

 Memory Usage 5.64 MB

 Peak Memory Usage 8.36 MB

 iNodeMon.exe

 Process ID 4032

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\iNode\iNode Client\iNodeMon.exe

 Memory Usage 6.11 MB

 Peak Memory Usage 13 MB

 iNodePortal.exe

 Process ID 6576

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\iNode\iNode Client\iNodePortal.exe

 Memory Usage 9.05 MB

 Peak Memory Usage 15 MB

 iNodeSec.exe

 Process ID 6536

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\iNode\iNode Client\iNodeSec.exe

 Memory Usage 12 MB

 Peak Memory Usage 18 MB

 IntelCpHDCPSvc.exe

 Process ID 3884

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\DriverStore\FileRepository\ki132842.inf\_amd64\_e968a65c52333922\IntelCpHDCPSvc.exe

 Memory Usage 5.22 MB

 Peak Memory Usage 6.99 MB

 IntelCpHeciSvc.exe

 Process ID 4568

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\DriverStore\FileRepository\ki132842.inf\_amd64\_e968a65c52333922\IntelCpHeciSvc.exe

 Memory Usage 4.82 MB

 Peak Memory Usage 6.54 MB

 jhi\_service.exe

 Process ID 2916

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\Intel\Intel Management Engine Components\DAL\jhi\_service.exe

 Memory Usage 4.45 MB

 Peak Memory Usage 6.11 MB

 LMS.exe

 Process ID 16252

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\Intel\Intel Management Engine Components\LMS\LMS.exe

 Memory Usage 10 MB

 Peak Memory Usage 14 MB

 lsass.exe

 Process ID 348

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\lsass.exe

 Memory Usage 20 MB

 Peak Memory Usage 22 MB

 macmnsvc.exe

 Process ID 3352

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Program Files\McAfee\Agent\macmnsvc.exe

 Memory Usage 8.93 MB

 Peak Memory Usage 13 MB

 macompatsvc.exe

 Process ID 13208

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\McAfee\Agent\x86\macompatsvc.exe

 Memory Usage 12 MB

 Peak Memory Usage 14 MB

 masvc.exe

 Process ID 4108

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\McAfee\Agent\masvc.exe

 Memory Usage 20 MB

 Peak Memory Usage 23 MB

 mcshield.exe

 Process ID 6488

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\Common Files\McAfee\AVSolution\mcshield.exe

 Memory Usage 237 MB

 Peak Memory Usage 438 MB

 mctray.exe

 Process ID 15016

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files\McAfee\Agent\x86\mctray.exe

 Memory Usage 1.95 MB

 Peak Memory Usage 16 MB

 Memory Compression

 Process ID 1916

 User SYSTEM

 Domain NT AUTHORITY

 Memory Usage 564 MB

 Peak Memory Usage 565 MB

 mfecanary.exe

 Process ID 14964

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\Common Files\McAfee\SystemCore\mfecanary.exe

 Memory Usage 4.28 MB

 Peak Memory Usage 7.13 MB

 mfeensppl.exe

 Process ID 6984

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\McAfee\Endpoint Security\Threat Prevention\mfeensppl.exe

 Memory Usage 7.62 MB

 Peak Memory Usage 12 MB

 mfeesp.exe

 Process ID 6684

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\mfeesp.exe

 Memory Usage 27 MB

 Peak Memory Usage 33 MB

 mfefire.exe

 Process ID 6712

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\Common Files\McAfee\SystemCore\mfefire.exe

 Memory Usage 8.08 MB

 Peak Memory Usage 11 MB

 mfehcs.exe

 Process ID 6848

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\Common Files\McAfee\SystemCore\mfehcs.exe

 Memory Usage 5.74 MB

 Peak Memory Usage 9.09 MB

 mfemactl.exe

 Process ID 13276

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\McAfee\Agent\x86\mfemactl.exe

 Memory Usage 9.98 MB

 Peak Memory Usage 13 MB

 mfemms.exe

 Process ID 4176

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\Common Files\McAfee\SystemCore\mfemms.exe

 Memory Usage 7.11 MB

 Peak Memory Usage 9.81 MB

 mfetp.exe

 Process ID 7004

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\McAfee\Endpoint Security\Threat Prevention\mfetp.exe

 Memory Usage 30 MB

 Peak Memory Usage 48 MB

 mfevtps.exe

 Process ID 5044

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\mfevtps.exe

 Memory Usage 13 MB

 Peak Memory Usage 23 MB

 mfevtps.exe

 Process ID 4908

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\mfevtps.exe

 Memory Usage 4.72 MB

 Peak Memory Usage 7.54 MB

 mfewc.exe

 Process ID 6900

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\McAfee\Endpoint Security\Web Control\mfewc.exe

 Memory Usage 23 MB

 Peak Memory Usage 30 MB

 mfewch.exe

 Process ID 14028

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\McAfee\Endpoint Security\Web Control\mfewch.exe

 Memory Usage 3.24 MB

 Peak Memory Usage 4.47 MB

 msdtc.exe

 Process ID 17504

 User NETWORK SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\msdtc.exe

 Memory Usage 7.27 MB

 Peak Memory Usage 12 MB

 msfeedssync.exe

 Process ID 6184

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\msfeedssync.exe

 Memory Usage 7.58 MB

 Peak Memory Usage 7.71 MB

 mysqld.exe

 Process ID 9688

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\DSS Express\Server\mysql\bin\mysqld.exe

 Memory Usage 36 MB

 Peak Memory Usage 114 MB

 ONENOTEM.EXE

 Process ID 8308

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files\Microsoft Office\Office16\ONENOTEM.EXE

 Memory Usage KB

 Peak Memory Usage 6.97 MB

 OUTLOOK.EXE

 Process ID 14628

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files\Microsoft Office\Office16\OUTLOOK.EXE

 Memory Usage 170 MB

 Peak Memory Usage 205 MB

 pcdrwi.exe

 Process ID 18076

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\Dell\SupportAssistAgent\PCDr\SupportAssist\6.0.7033.2285\pcdrwi.exe

 Memory Usage 43 MB

 Peak Memory Usage 139 MB

 PresentationFontCache.exe

 Process ID 12828

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\Microsoft.NET\Framework64\v3.0\WPF\PresentationFontCache.exe

 Memory Usage 7.02 MB

 Peak Memory Usage 19 MB

 PrintIsolationHost.exe

 Process ID 18084

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\PrintIsolationHost.exe

 Memory Usage 7.19 MB

 Peak Memory Usage 7.23 MB

 RAVBg64.exe

 Process ID 6748

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe

 Memory Usage 8.91 MB

 Peak Memory Usage 13 MB

 RAVBg64.exe

 Process ID 2704

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe

 Memory Usage 9.30 MB

 Peak Memory Usage 15 MB

 RAVBg64.exe

 Process ID 2712

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe

 Memory Usage 10 MB

 Peak Memory Usage 14 MB

 Registry

 Process ID 104

 User SYSTEM

 Domain NT AUTHORITY

 Memory Usage 40 MB

 Peak Memory Usage 98 MB

 RstMwService.exe

 Process ID 4336

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\DriverStore\FileRepository\iastorac.inf\_amd64\_eea3cf789013ad4f\RstMwService.exe

 Memory Usage 5.04 MB

 Peak Memory Usage 8.18 MB

 RtkAudioService64.exe

 Process ID 2104

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe

 Memory Usage 5.85 MB

 Peak Memory Usage 8.13 MB

 RtkNGUI64.exe

 Process ID 11944

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files\Realtek\Audio\HDA\RtkNGUI64.exe

 Memory Usage 12 MB

 Peak Memory Usage 14 MB

 RuntimeBroker.exe

 Process ID 16140

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\RuntimeBroker.exe

 Memory Usage 15 MB

 Peak Memory Usage 24 MB

 RuntimeBroker.exe

 Process ID 15616

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\RuntimeBroker.exe

 Memory Usage 35 MB

 Peak Memory Usage 72 MB

 RuntimeBroker.exe

 Process ID 14464

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\RuntimeBroker.exe

 Memory Usage 27 MB

 Peak Memory Usage 29 MB

 SearchFilterHost.exe

 Process ID 17860

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\SearchFilterHost.exe

 Memory Usage 5.95 MB

 Peak Memory Usage 6.03 MB

 SearchIndexer.exe

 Process ID 10392

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\SearchIndexer.exe

 Memory Usage 42 MB

 Peak Memory Usage 47 MB

 SearchProtocolHost.exe

 Process ID 18700

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\SearchProtocolHost.exe

 Memory Usage 12 MB

 Peak Memory Usage 30 MB

 SearchProtocolHost.exe

 Process ID 15188

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\SearchProtocolHost.exe

 Memory Usage 9.62 MB

 Peak Memory Usage 13 MB

 SearchUI.exe

 Process ID 15444

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\SystemApps\Microsoft.Windows.Cortana\_cw5n1h2txyewy\SearchUI.exe

 Memory Usage 139 MB

 Peak Memory Usage 157 MB

 SecurityHealthService.exe

 Process ID 12820

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\SecurityHealthService.exe

 Memory Usage 12 MB

 Peak Memory Usage 15 MB

 SecurityHealthSystray.exe

 Process ID 11776

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\SecurityHealthSystray.exe

 Memory Usage 6.82 MB

 Peak Memory Usage 8.46 MB

 servicehost.exe

 Process ID 4844

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\McAfee\WebAdvisor\O00E03E.tmp

 Memory Usage 22 MB

 Peak Memory Usage 25 MB

 services.exe

 Process ID 1000

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\services.exe

 Memory Usage 8.18 MB

 Peak Memory Usage 10 MB

 ServiceShell.exe

 Process ID 17960

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\Dell\UpdateService\ServiceShell.exe

 Memory Usage 37 MB

 Peak Memory Usage 53 MB

 SgrmBroker.exe

 Process ID 19476

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\SgrmBroker.exe

 Memory Usage 5.17 MB

 Peak Memory Usage 6.82 MB

 ShellExperienceHost.exe

 Process ID 5892

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\SystemApps\ShellExperienceHost\_cw5n1h2txyewy\ShellExperienceHost.exe

 Memory Usage 57 MB

 Peak Memory Usage 92 MB

 sihost.exe

 Process ID 13112

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\sihost.exe

 Memory Usage 23 MB

 Peak Memory Usage 24 MB

 slack.exe

 Process ID 4160

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Users\Dahua\AppData\Local\slack\app-4.1.2\slack.exe

 Memory Usage 122 MB

 Peak Memory Usage 127 MB

 slack.exe

 Process ID 3248

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Users\Dahua\AppData\Local\slack\app-4.1.2\slack.exe

 Memory Usage 214 MB

 Peak Memory Usage 289 MB

 slack.exe

 Process ID 5960

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Users\Dahua\AppData\Local\slack\app-4.1.2\slack.exe

 Memory Usage 204 MB

 Peak Memory Usage 248 MB

 smartscreen.exe

 Process ID 1384

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\smartscreen.exe

 Memory Usage 25 MB

 Peak Memory Usage 31 MB

 smss.exe

 Process ID 464

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\smss.exe

 Memory Usage 844 KB

 Peak Memory Usage 34 MB

 SoundCapture.exe

 Process ID 13144

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files\Elgato\SoundCapture\SoundCapture.exe

 Memory Usage 70 MB

 Peak Memory Usage 96 MB

 Speccy64.exe

 Process ID 22416

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files\Speccy\Speccy64.exe

 Memory Usage 22 MB

 Peak Memory Usage 23 MB

 spoolsv.exe

 Process ID 3516

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\spoolsv.exe

 Memory Usage 16 MB

 Peak Memory Usage 24 MB

 spsetup132.exe

 Process ID 20016

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Users\Dahua\Downloads\spsetup132.exe

 Memory Usage 38 MB

 Peak Memory Usage 38 MB

 SRAgent.exe

 Process ID 12304

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\Splashtop\Splashtop Remote\Server\SRAgent.exe

 Memory Usage 13 MB

 Peak Memory Usage 13 MB

 SRFeature.exe

 Process ID 15300

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\Splashtop\Splashtop Remote\Server\SRFeature.exe

 Memory Usage 7.61 MB

 Peak Memory Usage 11 MB

 SRManager.exe

 Process ID 4964

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\Splashtop\Splashtop Remote\Server\SRManager.exe

 Memory Usage 13 MB

 Peak Memory Usage 17 MB

 SRServer.exe

 Process ID 800

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\Splashtop\Splashtop Remote\Server\SRServer.exe

 Memory Usage 12 MB

 Peak Memory Usage 18 MB

 SRService.exe

 Process ID 4372

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\Splashtop\Splashtop Remote\Server\SRService.exe

 Memory Usage 4.99 MB

 Peak Memory Usage 6.77 MB

 SSUService.exe

 Process ID 4412

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\Splashtop\Splashtop Software Updater\SSUService.exe

 Memory Usage 6.62 MB

 Peak Memory Usage 9.09 MB

 SupportAssistAgent.exe

 Process ID 20072

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files\Dell\SupportAssistAgent\bin\SupportAssistAgent.exe

 Memory Usage 88 MB

 Peak Memory Usage 123 MB

 svchost.exe

 Process ID 1532

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\svchost.exe

 Memory Usage 14 MB

 Peak Memory Usage 16 MB

 svchost.exe

 Process ID 4316

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 5.13 MB

 Peak Memory Usage 6.63 MB

 svchost.exe

 Process ID 4296

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 3.86 MB

 Peak Memory Usage 5.45 MB

 svchost.exe

 Process ID 4268

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 5.04 MB

 Peak Memory Usage 5.40 MB

 svchost.exe

 Process ID 4252

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 3.91 MB

 Peak Memory Usage 5.51 MB

 svchost.exe

 Process ID 4072

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 11 MB

 Peak Memory Usage 13 MB

 svchost.exe

 Process ID 3976

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 39 MB

 Peak Memory Usage 218 MB

 svchost.exe

 Process ID 3944

 User NETWORK SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 15 MB

 Peak Memory Usage 16 MB

 svchost.exe

 Process ID 3936

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 19 MB

 Peak Memory Usage 20 MB

 svchost.exe

 Process ID 3724

 User NETWORK SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 6.86 MB

 Peak Memory Usage 8.15 MB

 svchost.exe

 Process ID 3656

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 6.85 MB

 Peak Memory Usage 8.32 MB

 svchost.exe

 Process ID 8228

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 8.59 MB

 Peak Memory Usage 10 MB

 svchost.exe

 Process ID 3604

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 21 MB

 Peak Memory Usage 24 MB

 svchost.exe

 Process ID 3564

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 7.36 MB

 Peak Memory Usage 8.86 MB

 svchost.exe

 Process ID 2380

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\svchost.exe

 Memory Usage 9.31 MB

 Peak Memory Usage 12 MB

 svchost.exe

 Process ID 3452

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 12 MB

 Peak Memory Usage 14 MB

 svchost.exe

 Process ID 3360

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 5.48 MB

 Peak Memory Usage 6.98 MB

 svchost.exe

 Process ID 3196

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 5.30 MB

 Peak Memory Usage 6.74 MB

 svchost.exe

 Process ID 1460

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 10 MB

 Peak Memory Usage 11 MB

 svchost.exe

 Process ID 3024

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 18 MB

 Peak Memory Usage 21 MB

 svchost.exe

 Process ID 2948

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 8.89 MB

 Peak Memory Usage 10 MB

 svchost.exe

 Process ID 2900

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 5.75 MB

 Peak Memory Usage 6.91 MB

 svchost.exe

 Process ID 2836

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 12 MB

 Peak Memory Usage 15 MB

 svchost.exe

 Process ID 2828

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 8.21 MB

 Peak Memory Usage 9.79 MB

 svchost.exe

 Process ID 2668

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 6.28 MB

 Peak Memory Usage 7.38 MB

 svchost.exe

 Process ID 2532

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 8.23 MB

 Peak Memory Usage 8.38 MB

 svchost.exe

 Process ID 2392

 User NETWORK SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 12 MB

 Peak Memory Usage 12 MB

 svchost.exe

 Process ID 2276

 User NETWORK SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 8.58 MB

 Peak Memory Usage 10 MB

 svchost.exe

 Process ID 2268

 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 19756

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 7.03 MB

 Peak Memory Usage 8.57 MB

 svchost.exe

 Process ID 2260

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 5.27 MB

 Peak Memory Usage 6.45 MB

 svchost.exe

 Process ID 4524

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 18 MB

 Peak Memory Usage 21 MB

 svchost.exe

 Process ID 2232

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 7.00 MB

 Peak Memory Usage 7.66 MB

 svchost.exe

 Process ID 2140

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 12 MB

 Peak Memory Usage 13 MB

 svchost.exe

 Process ID 1588

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 45 MB

 Peak Memory Usage 100 MB

 svchost.exe

 Process ID 1284

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 8.36 MB

 Peak Memory Usage 8.60 MB

 svchost.exe

 Process ID 2024

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 8.35 MB

 Peak Memory Usage 9.73 MB

 svchost.exe

 Process ID 1892

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 7.92 MB

 Peak Memory Usage 11 MB

 svchost.exe

 Process ID 1884

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 7.15 MB

 Peak Memory Usage 8.41 MB

 svchost.exe

 Process ID 1840

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 12 MB

 Peak Memory Usage 15 MB

 svchost.exe

 Process ID 1796

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 107 MB

 Peak Memory Usage 142 MB

 svchost.exe

 Process ID 1788

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 4.63 MB

 Peak Memory Usage 5.77 MB

 svchost.exe

 Process ID 1780

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 8.98 MB

 Peak Memory Usage 11 MB

 svchost.exe

 Process ID 1728

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 15 MB

 Peak Memory Usage 22 MB

 svchost.exe

 Process ID 1624

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 7.81 MB

 Peak Memory Usage 8.71 MB

 svchost.exe

 Process ID 1520

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 7.73 MB

 Peak Memory Usage 8.75 MB

 svchost.exe

 Process ID 1496

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 4.50 MB

 Peak Memory Usage 5.96 MB

 svchost.exe

 Process ID 1400

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 4.39 MB

 Peak Memory Usage 5.59 MB

 svchost.exe

 Process ID 1392

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 4.92 MB

 Peak Memory Usage 5.75 MB

 svchost.exe

 Process ID 1352

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 8.80 MB

 Peak Memory Usage 10 MB

 svchost.exe

 Process ID 1148

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 6.57 MB

 Peak Memory Usage 8.18 MB

 svchost.exe

 Process ID 1104

 User NETWORK SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 14 MB

 Peak Memory Usage 15 MB

 svchost.exe

 Process ID 824

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 21 MB

 Peak Memory Usage 23 MB

 svchost.exe

 Process ID 860

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 2.93 MB

 Peak Memory Usage 3.92 MB

 svchost.exe

 Process ID 20612

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 8.30 MB

 Peak Memory Usage 8.59 MB

 svchost.exe

 Process ID 4420

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 5.98 MB

 Peak Memory Usage 8.00 MB

 svchost.exe

 Process ID 7400

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\iNode DAM Agent\A96B1E2F2FA4EB41A2EECF23B35902FF\svchost.exe

 Memory Usage 2.78 MB

 Peak Memory Usage 3.66 MB

 svchost.exe

 Process ID 7012

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 9.49 MB

 Peak Memory Usage 11 MB

 svchost.exe

 Process ID 12840

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\svchost.exe

 Memory Usage 18 MB

 Peak Memory Usage 21 MB

 svchost.exe

 Process ID 12764

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\svchost.exe

 Memory Usage 28 MB

 Peak Memory Usage 31 MB

 svchost.exe

 Process ID 14836

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 4.73 MB

 Peak Memory Usage 6.08 MB

 svchost.exe

 Process ID 13088

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 9.75 MB

 Peak Memory Usage 14 MB

 svchost.exe

 Process ID 14908

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 8.00 MB

 Peak Memory Usage 17 MB

 svchost.exe

 Process ID 5336

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 9.48 MB

 Peak Memory Usage 13 MB

 svchost.exe

 Process ID 17368

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 19 MB

 Peak Memory Usage 19 MB

 svchost.exe

 Process ID 16812

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 6.12 MB

 Peak Memory Usage 6.17 MB

 svchost.exe

 Process ID 5824

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 5.59 MB

 Peak Memory Usage 5.73 MB

 svchost.exe

 Process ID 13344

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 6.26 MB

 Peak Memory Usage 7.84 MB

 svchost.exe

 Process ID 15164

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 6.57 MB

 Peak Memory Usage 9.96 MB

 svchost.exe

 Process ID 15220

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 12 MB

 Peak Memory Usage 19 MB

 svchost.exe

 Process ID 14096

 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 12004

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 18 MB

 Peak Memory Usage 31 MB

 svchost.exe

 Process ID 12844

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 11 MB

 Peak Memory Usage 11 MB

 svchost.exe

 Process ID 4580

 User NETWORK SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 5.79 MB

 Peak Memory Usage 7.17 MB

 svchost.exe

 Process ID 20924

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\svchost.exe

 Memory Usage 6.34 MB

 Peak Memory Usage 6.57 MB

 System

 Process ID 4

 Memory Usage 3.64 MB

 Peak Memory Usage 25 MB

 System Idle Process

 Process ID 0

 taskhostw.exe

 Process ID 12956

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\taskhostw.exe

 Memory Usage 15 MB

 Peak Memory Usage 19 MB

 Taskmgr.exe

 Process ID 19288

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\System32\Taskmgr.exe

 Memory Usage 39 MB

 Peak Memory Usage 59 MB

 uihost.exe

 Process ID 12944

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files\McAfee\WebAdvisor\O01E10E.tmp

 Memory Usage 7.58 MB

 Peak Memory Usage 15 MB

 unsecapp.exe

 Process ID 3164

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\wbem\unsecapp.exe

 Memory Usage 5.45 MB

 Peak Memory Usage 6.75 MB

 unsecapp.exe

 Process ID 17496

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\wbem\unsecapp.exe

 Memory Usage 5.73 MB

 Peak Memory Usage 7.19 MB

 UpdaterUI.exe

 Process ID 15120

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files\McAfee\Agent\x86\UpdaterUI.exe

 Memory Usage 5.75 MB

 Peak Memory Usage 14 MB

 vpnagent.exe

 Process ID 2540

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\vpnagent.exe

 Memory Usage 13 MB

 Peak Memory Usage 21 MB

 vpnui.exe

 Process ID 6260

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\vpnui.exe

 Memory Usage 39 MB

 Peak Memory Usage 43 MB

 WavesSvc64.exe

 Process ID 920

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Program Files\Waves\MaxxAudio\WavesSvc64.exe

 Memory Usage 12 MB

 Peak Memory Usage 32 MB

 WavesSysSvc64.exe

 Process ID 4500

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\DriverStore\FileRepository\wavesapo75de.inf\_amd64\_5ff36f834a6d461a\WavesSysSvc64.exe

 Memory Usage 4.95 MB

 Peak Memory Usage 17 MB

 WerFault.exe

 Process ID 19980

 User Dahua

 Domain WIN10-CARLOSESP

 Path C:\Windows\SysWOW64\WerFault.exe

 Memory Usage 15 MB

 Peak Memory Usage 27 MB

 wininit.exe

 Process ID 924

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\wininit.exe

 Memory Usage 4.50 MB

 Peak Memory Usage 6.78 MB

 winlogon.exe

 Process ID 636

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\winlogon.exe

 Memory Usage 8.87 MB

 Peak Memory Usage 29 MB

 WmiApSrv.exe

 Process ID 19868

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\wbem\WmiApSrv.exe

 Memory Usage 8.31 MB

 Peak Memory Usage 8.37 MB

 WmiPrvSE.exe

 Process ID 19796

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\wbem\WmiPrvSE.exe

 Memory Usage 13 MB

 Peak Memory Usage 33 MB

 WmiPrvSE.exe

 Process ID 3508

 User LOCAL SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\SysWOW64\wbem\WmiPrvSE.exe

 Memory Usage 7.94 MB

 Peak Memory Usage 9.19 MB

 WmiPrvSE.exe

 Process ID 3272

 User SYSTEM

 Domain NT AUTHORITY

 Path C:\Windows\System32\wbem\WmiPrvSE.exe

 Memory Usage 44 MB

 Peak Memory Usage 44 MB

 WmiPrvSE.exe

 Process ID 5488

 User NETWORK SERVICE

 Domain NT AUTHORITY

 Path C:\Windows\System32\wbem\WmiPrvSE.exe

 Memory Usage 32 MB

 Peak Memory Usage 35 MB

 Security Options

 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 server operators to schedule tasks Not Defined

 Domain controller: LDAP server signing requirements Not Defined

 Domain controller: Refuse machine account password changes 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

 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 Enabled

 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: Do not store LAN Manager hash value on next password change Enabled

 Network security: Force logoff when logon hours expire Disabled

 Network security: LAN Manager authentication level Not Defined

 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

 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 Disabled

 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 Elevate without prompting

 User Account Control: Behavior of the elevation prompt for standard users Prompt for credentials on the secure desktop

 User Account Control: Detect application installations and prompt for elevation Disabled

 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 Disabled

 User Account Control: Switch to the secure desktop when prompting for elevation Disabled

 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 Fan

 ACPI Fan

 ACPI Fan

 ACPI Fan

 ACPI Fan

 ACPI Fixed Feature Button

 ACPI Power Button

 ACPI Processor Aggregator

 ACPI Sleep Button

 ACPI Thermal Zone

 ACPI Thermal Zone

 Intel Core i5-7500 CPU @ 3.40GHz

 Intel Core i5-7500 CPU @ 3.40GHz

 Intel Core i5-7500 CPU @ 3.40GHz

 Intel Core i5-7500 CPU @ 3.40GHz

 Intel Power Engine Plug-in

 Microsoft Windows Management Interface for ACPI

 Motherboard resources

 Trusted Platform Module 2.0

 PCI Express Root Complex

 Intel Management Engine Interface

 Intel PMC - A2A1

 Intel SMBUS - A2A3

 Intel Thermal subsystem - A2B1

 Intel Xeon E3 - 1200 v6/7th Gen Intel Core Host Bridge/DRAM Registers - 591F

 Motherboard resources

 Motherboard resources

 Motherboard resources

 Motherboard resources

 Intel(R) HD Graphics 630

 Generic PnP Monitor

 Generic PnP Monitor

 Intel(R) USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)

 USB Root Hub (USB 3.0)

 Realtek RTL8811AU Wireless LAN 802.11ac USB 2.0 Network Adapter

 Microsoft Wi-Fi Direct Virtual Adapter

 Microsoft Wi-Fi Direct Virtual Adapter #2

 USB Input Device

 Logicool HID-compliant TrackMan Wheel Mouse

 Logitech HID Device

 Logitech Pointing Device

 USB Composite Device

 USB Input Device

 HID Keyboard Device

 USB Input Device

 HID-compliant consumer control device

 Intel(R) Chipset SATA/PCIe RST Premium Controller

 Intel Pinning Shell Extensions

 PLDS DVD+-RW DU-8A5LH

 ST500DM009-2F110A

 Intel(R) PCI Express Root Port #5 - A294

 Realtek PCIe GbE Family Controller

 Intel(R) 200 Series Chipset Family LPC Controller (B250) - A2C8

 Communications Port (COM1)

 High precision event timer

 Legacy device

 Motherboard resources

 Motherboard resources

 Motherboard resources

 Motherboard resources

 Numeric data processor

 Programmable interrupt controller

 System CMOS/real time clock

 System timer

 High Definition Audio Controller

 Realtek(R) Audio

 Jack Mic (Realtek Audio)

 Speakers / Headphones (Realtek Audio)

 Waves Audio Effects Component

 Intel(R) Display Audio

 DHL22-F600 (Intel Display Audio)

 DHL22-F600 (Intel Display Audio)

 Microsoft UEFI-Compliant System

 System Firmware

CPU

 Intel Core i5 7500

 Cores 4

 Threads 4

 Name Intel Core i5 7500

 Code Name Kaby Lake

 Package Socket 1151 LGA

 Technology 14nm

 Specification Intel Core i5-7500 CPU @ 3.40GHz

 Family 6

 Extended Family 6

 Model E

 Extended Model 9E

 Stepping 9

 Revision B0

 Instructions MMX, SSE, SSE2, SSE3, SSSE3, SSE4.1, SSE4.2, Intel 64, NX, VMX, AES, AVX, AVX2, FMA3

 Virtualization Supported, Enabled

 Hyperthreading Not supported

 Bus Speed 99.8 MHz

 Stock Core Speed 3400 MHz

 Stock Bus Speed 100 MHz

 Average Temperature 50 °C

 Caches

 L1 Data Cache Size 4 x 32 KBytes

 L1 Instructions Cache Size 4 x 32 KBytes

 L2 Unified Cache Size 4 x 256 KBytes

 L3 Unified Cache Size 6144 KBytes

 Cores

 Core 0

 Core Speed 3691.9 MHz

 Multiplier x 37.0

 Bus Speed 99.8 MHz

 Temperature 50 °C

 Threads APIC ID: 0

 Core 1

 Core Speed 3691.9 MHz

 Multiplier x 37.0

 Bus Speed 99.8 MHz

 Temperature 52 °C

 Threads APIC ID: 2

 Core 2

 Core Speed 3592.1 MHz

 Multiplier x 36.0

 Bus Speed 99.8 MHz

 Temperature 48 °C

 Threads APIC ID: 4

 Core 3

 Core Speed 3691.9 MHz

 Multiplier x 37.0

 Bus Speed 99.8 MHz

 Temperature 48 °C

 Threads APIC ID: 6

RAM

 Memory slots

 Total memory slots 2

 Used memory slots 1

 Free memory slots 1

 Memory

 Type Unknown

 Size 8192 MBytes

 Channels # Single

 DRAM Frequency 1197.4 MHz

 CAS# Latency (CL) 17 clocks

 RAS# to CAS# Delay (tRCD) 17 clocks

 RAS# Precharge (tRP) 17 clocks

 Cycle Time (tRAS) 39 clocks

 Command Rate (CR) 2T

 Physical Memory

 Memory Usage 84 %

 Total Physical 7.73 GB

 Available Physical 1.22 GB

 Total Virtual 13 GB

 Available Virtual 2.52 GB

 SPD

 Number Of SPD Modules 1

 Slot #1

 Type Unknown

 Size 8192 MBytes

 Manufacturer Hyundai Electronics

 Max Bandwidth DDR4-2400 (1200 MHz)

 Part Number HMA81GU6AFR8N-UH

 Serial Number 2177031635

 Week/year 39 / 17

 Timing table

 JEDEC #1

 Frequency 727.3 MHz

 CAS# Latency 10.0

 RAS# To CAS# 10

 RAS# Precharge 10

 tRAS 24

 tRC 34

 Voltage 1.200 V

 JEDEC #2

 Frequency 800.0 MHz

 CAS# Latency 11.0

 RAS# To CAS# 11

 RAS# Precharge 11

 tRAS 26

 tRC 37

 Voltage 1.200 V

 JEDEC #3

 Frequency 872.7 MHz

 CAS# Latency 12.0

 RAS# To CAS# 12

 RAS# Precharge 12

 tRAS 28

 tRC 40

 Voltage 1.200 V

 JEDEC #4

 Frequency 945.5 MHz

 CAS# Latency 13.0

 RAS# To CAS# 13

 RAS# Precharge 13

 tRAS 31

 tRC 44

 Voltage 1.200 V

 JEDEC #5

 Frequency 1018.2 MHz

 CAS# Latency 14.0

 RAS# To CAS# 14

 RAS# Precharge 14

 tRAS 33

 tRC 47

 Voltage 1.200 V

 JEDEC #6

 Frequency 1090.9 MHz

 CAS# Latency 15.0

 RAS# To CAS# 15

 RAS# Precharge 15

 tRAS 35

 tRC 50

 Voltage 1.200 V

 JEDEC #7

 Frequency 1163.6 MHz

 CAS# Latency 16.0

 RAS# To CAS# 16

 RAS# Precharge 16

 tRAS 38

 tRC 54

 Voltage 1.200 V

 JEDEC #8

 Frequency 1200.5 MHz

 CAS# Latency 17.0

 RAS# To CAS# 17

 RAS# Precharge 17

 tRAS 39

 tRC 55

 Voltage 1.200 V

 JEDEC #9

 Frequency 1200.5 MHz

 CAS# Latency 18.0

 RAS# To CAS# 17

 RAS# Precharge 17

 tRAS 39

 tRC 55

 Voltage 1.200 V

Motherboard

 Manufacturer Dell Inc.

 Model 0W0CHX (U3E1)

 Version A00

 Chipset Vendor Intel

 Chipset Model Kaby Lake

 Chipset Revision 05

 Southbridge Vendor Intel

 Southbridge Model B250

 Southbridge Revision 00

 BIOS

 Brand Dell Inc.

 Version 1.12.1

 Date 5/9/2019

 PCI Data

 Slot PCI-E

 Slot Type PCI-E

 Slot Usage Available

 Data lanes x1

 Slot Designation SLOT1

 Characteristics 3.3V, PME

 Slot Number 0

 Slot PCI-E Gen 3

 Slot Type PCI-E Gen 3

 Slot Usage Available

 Data lanes x16

 Slot Designation SLOT2

 Characteristics 3.3V, PME

 Slot Number 1

 Slot PCI-E

 Slot Type PCI-E

 Slot Usage Available

 Data lanes x1

 Slot Designation SLOT3

 Characteristics 3.3V, PME

 Slot Number 2

 Slot PCI-E

 Slot Type PCI-E

 Slot Usage Available

 Data lanes x1

 Slot Designation SLOT4

 Characteristics 3.3V, PME

 Slot Number 3

 Slot Unknown

 Slot Type Unknown

 Slot Usage Available

 Data lanes x4

 Slot Designation SLOT5

 Characteristics 3.3V, PME

 Slot Number 4

Graphics

 Monitor 1

 Name DHL22-F600 on Intel HD Graphics 630

 Current Resolution 1920x1080 pixels

 Work Resolution 1920x1040 pixels

 State Enabled

 Multiple displays Extended, Primary, Enabled

 Monitor Width 1920

 Monitor Height 1080

 Monitor BPP 32 bits per pixel

 Monitor Frequency 59 Hz

 Device \\.\DISPLAY1\Monitor0

 Monitor 2

 Name DHL22-F600 on Intel HD Graphics 630

 Current Resolution 1920x1080 pixels

 Work Resolution 1920x1040 pixels

 State Enabled

 Multiple displays Extended, Secondary, Enabled

 Monitor Width 1920

 Monitor Height 1080

 Monitor BPP 32 bits per pixel

 Monitor Frequency 59 Hz

 Device \\.\DISPLAY2\Monitor0

 Intel HD Graphics 630

 Manufacturer Intel

 Model HD Graphics 630

 Device ID 8086-5912

 Revision 5

 Subvendor Dell (1028)

 Current Performance Level Level 0

 Current GPU Clock 0 MHz

 Driver version 26.20.100.6951

 Count of performance levels : 1

 Level 1 - "Perf Level 0"

Storage

 Hard drives

 ST500DM009-2F110A

 Manufacturer Seagate

 Heads 16

 Cylinders 60,801

 Tracks 15,504,255

 Sectors 976,768,065

 SATA type SATA-III 6.0Gb/s

 Device type Fixed

 ATA Standard ATA8-ACS

 Serial Number ZA47MDRQ

 Firmware Version Number CC43

 LBA Size 48-bit LBA

 Power On Count 215 times

 Power On Time 102.7 days

 Speed 7200 RPM

 Features S.M.A.R.T., APM, NCQ

 Max. Transfer Mode SATA III 6.0Gb/s

 Used Transfer Mode SATA III 6.0Gb/s

 Interface SATA

 Capacity 465 GB

 Real size 500,107,862,016 bytes

 RAID Type None

 S.M.A.R.T

 Status Good

 Temperature 38 °C

 Temperature Range OK (less than 50 °C)

 S.M.A.R.T attributes

 01

 Attribute name Read Error Rate

 Real value 0

 Current 77

 Worst 63

 Threshold 6

 Raw Value 000351A593

 Status Good

 03

 Attribute name Spin-Up Time

 Real value 0 ms

 Current 98

 Worst 97

 Threshold 0

 Raw Value 0000000000

 Status Good

 04

 Attribute name Start/Stop Count

 Real value 216

 Current 100

 Worst 100

 Threshold 20

 Raw Value 00000000D8

 Status Good

 05

 Attribute name Reallocated Sectors Count

 Real value 0

 Current 100

 Worst 100

 Threshold 10

 Raw Value 0000000000

 Status Good

 07

 Attribute name Seek Error Rate

 Real value 0

 Current 81

 Worst 60

 Threshold 45

 Raw Value 00078C3E7A

 Status Good

 09

 Attribute name Power-On Hours (POH)

 Real value 102d 17h

 Current 98

 Worst 98

 Threshold 0

 Raw Value 00000009A1

 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 215

 Current 100

 Worst 100

 Threshold 20

 Raw Value 00000000D7

 Status Good

 B7

 Attribute name SATA Downshift Error Count

 Real value 0

 Current 100

 Worst 100

 Threshold 0

 Raw Value 0000000000

 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 0

 Current 100

 Worst 100

 Threshold 0

 Raw Value 0000000000

 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 38 °C

 Current 62

 Worst 59

 Threshold 40

 Raw Value 0027150026

 Status Good

 C1

 Attribute name Load/Unload Cycle Count

 Real value 290

 Current 100

 Worst 100

 Threshold 0

 Raw Value 0000000122

 Status Good

 C2

 Attribute name Temperature

 Real value 38 °C

 Current 38

 Worst 16

 Threshold 0

 Raw Value 0000000026

 Status Good

 C3

 Attribute name Hardware ECC Recovered

 Real value 0

 Current 8

 Worst 1

 Threshold 0

 Raw Value 000351A593

 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 0

 Current 200

 Worst 200

 Threshold 0

 Raw Value 0000000000

 Status Good

 F0

 Attribute name Head Flying Hours

 Real value 102d 10h

 Current 100

 Worst 253

 Threshold 0

 Raw Value 000000099A

 Status Good

 F1

 Attribute name Total LBAs Written

 Real value 7,739,468,519

 Current 100

 Worst 253

 Threshold 0

 Raw Value 00CD4EEAE7

 Status Good

 F2

 Attribute name Total LBAs Read

 Real value 11,185,860,160

 Current 100

 Worst 253

 Threshold 0

 Raw Value 009ABAAE40

 Status Good

 Partition 0

 Partition ID Disk #0, Partition #0

 File System NTFS

 Volume Serial Number 14CADF85

 Size 449 MB

 Used Space 16.1 MB (3%)

 Free Space 433 MB (97%)

 Partition 1

 Partition ID Disk #0, Partition #1

 File System FAT32

 Volume Serial Number D0CC969C

 Size 96 MB

 Used Space 44 MB (46%)

 Free Space 51 MB (54%)

 Partition 2

 Partition ID Disk #0, Partition #2

 Disk Letter C:

 File System NTFS

 Volume Serial Number 50DDDFA8

 Size 464 GB

 Used Space 83 GB (17%)

 Free Space 381 GB (83%)

 Partition 3

 Partition ID Disk #0, Partition #3

 File System NTFS

 Volume Serial Number 6EB90513

 Size 834 MB

 Used Space 496 MB (59%)

 Free Space 338 MB (41%)

Optical Drives

 PLDS DVD+-RW DU-8A5LH

 Media Type DVD Writer

 Name PLDS DVD+-RW DU-8A5LH

 Availability Running/Full Power

 Capabilities Random Access, Supports Writing, Supports Removable Media

 Read capabilities CD-R, CD-RW, CD-ROM, DVD-ROM, DVD-R, DVD-RW, DVD+R, DVD+RW, DVD-R DL, DVD+R DL

 Write capabilities CD-R, CD-RW, DVD-R, DVD-RW, DVD+R, DVD+RW, DVD-R DL, DVD+R DL

 Config Manager Error Code Device is working properly

 Config Manager User Config FALSE

 Drive D:

 Media Loaded FALSE

 SCSI Bus 0

 SCSI Logical Unit 0

 SCSI Port 0

 SCSI Target Id 1

 Status OK

Audio

 Sound Cards

 Intel Display Audio

 Elgato Sound Capture

 Realtek Audio

 Playback Devices

 Speakers / Headphones (Realtek Audio) (default)

 DHL22-F600 (Intel Display Audio)

 DHL22-F600 (Intel Display Audio)

 Recording Devices

 Jack Mic (Realtek Audio) (default)

 Line (Elgato Sound Capture)

 Speaker Configuration

 Speaker type Stereo

Peripherals

 HID Keyboard Device

 Device Kind Keyboard

 Device Name HID Keyboard Device

 Vendor Microsoft

 Location USB Input Device

 Driver

 Date 6-21-2006

 Version 10.0.17763.348

 File C:\WINDOWS\system32\DRIVERS\kbdhid.sys

 File C:\WINDOWS\system32\DRIVERS\kbdclass.sys

 Logicool HID-compliant TrackMan Wheel Mouse

 Device Kind Mouse

 Device Name Logicool HID-compliant TrackMan Wheel Mouse

 Vendor Logitech

 Location USB Input Device

 Driver

 Date 6-9-2015

 Version 5.90.38.0

 File C:\WINDOWS\system32\DRIVERS\LHidFilt.Sys

 File C:\WINDOWS\system32\DRIVERS\LMouFilt.Sys

 File C:\WINDOWS\system32\DRIVERS\mouhid.sys

 File C:\WINDOWS\system32\DRIVERS\mouclass.sys

 File C:\WINDOWS\system32\LkmdfCoInst.dll

 File C:\WINDOWS\system32\LMouFiltCoInst.dll

 HP Universal Printing PCL 6

 Device Kind Printer

 Device Name HP Universal Printing PCL 6

 Vendor HP

 Location http://172.16.16.207:3911/

 Driver

 Date 12-3-2013

 Version 61.160.1.17508

 File C:\WINDOWS\system32\spool\PRTPROCS\x64\1\hpcpp160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcui160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcpe160.dll

 File C:\WINDOWS\SysWOW64\hpcdmc32.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcdmc64.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpbcfgre.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcpu160.cfg

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpc6r160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcsm160.gpd

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpc6m160.gpd

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcst160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcur160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcpn160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcu1606.hpx

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcsc160.dtd

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcev160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpchl160.cab

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcu160.dem

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpmux160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpmur160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpmpm081.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpmpw081.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpmdp160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpmsn160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpmsl160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcsat20.dll

 File C:\WINDOWS\system32\hpmpm081.dll

 File C:\WINDOWS\system32\hpmpw081.dll

 File C:\WINDOWS\system32\hpmtp160.dll

 File C:\WINDOWS\system32\hpmja160.dll

 File C:\WINDOWS\system32\hpmml160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcu1606.gpd

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcu160u.ini

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcu1606.xml

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcls160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcss160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\pjl.gpd

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\pclxl.gpd

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\stdnames.gpd

 File C:\WINDOWS\system32\hpmco160.dll

 File C:\WINDOWS\system32\hpmprein.dll

 File C:\WINDOWS\system32\difxapi.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\FxCompChannel\_x64.dll

 File C:\WINDOWS\system32\FxCompChannel\_x64.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\cioum.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\cioum64.msi

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcpn160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcpp160.dll

 File C:\WINDOWS\system32\hpcpn160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\pclxl.DLL

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\unidrv.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\unires.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\unidrvui.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\unidrv.hlp

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\stddtype.gdl

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\stdschem.gdl

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\stdschmx.gdl

 File C:\WINDOWS\system32\hpmlm135.dll

 File C:\WINDOWS\SysWOW64\hpcc3160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpcc6160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpbdrvjct1004.dll

 File C:\WINDOWS\SysWOW64\hppccompio.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hppdcompio.dll

 File C:\WINDOWS\system32\hppdcompio.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpbuio64.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpfxcomw.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpfie160.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpsysobj.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\HPSecurePrint64.dll

 File C:\WINDOWS\system32\spool\DRIVERS\x64\{13433F41-64FF-4D84-9369-625DF24DFFA9}\hpspw160.dll

 File C:\WINDOWS\system32\hpcjpm.dll

 Printers

 \\172.16.16.211\Main Office Printer - Sharp MX3570 (Default Printer)

 Share Name Main Office Printer - Sharp MX3570

 Printer Port 172.16.16.201

 Print Processor winprint

 Availability Always

 Priority 1

 Duplex Long-edge binding

 Print Quality 600 \* 600 dpi Monochrome

 Status Unknown

 Driver

 Driver Name SHARP MX-3570N PCL6 (v7.01)

 Driver Path C:\WINDOWS\system32\spool\DRIVERS\x64\3\SU0E2DRV.DLL

 AnyDesk Printer

 Printer Port AD\_Port

 Print Processor winprint

 Availability Always

 Priority 1

 Duplex None

 Print Quality 600 \* 600 dpi Color

 Status Unknown

 Driver

 Driver Name AnyDesk v4 Printer Driver (v6.03)

 Driver Path C:\WINDOWS\System32\DriverStore\FileRepository\ntprint.inf\_amd64\_9543832f82bb474f\Amd64\mxdwdrv.dll

 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

 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\_9543832f82bb474f\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\_9543832f82bb474f\Amd64\mxdwdrv.dll

 NPI351FE8 (HP Color LaserJet CP5225n)

 Printer Port WSD-2791bf55-b716-4696-af73-4c60be220dee

 Print Processor hpcpp160

 Availability Always

 Priority 1

 Duplex None

 Print Quality 600 \* 600 dpi Color

 Status Unknown

 Driver

 Driver Name HP Universal Printing PCL 6 (v6.03)

 Driver Path C:\WINDOWS\system32\spool\DRIVERS\x64\3\unidrv.dll

 Send To OneNote 16

 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\_9543832f82bb474f\Amd64\mxdwdrv.dll

Network

 You are connected to the internet

 Connected through Realtek PCIe GbE Family Controller

 IP Address 172.16.16.79

 Subnet mask 255.255.255.0

 Gateway server 172.16.16.1

 Preferred DNS server 172.16.8.1

 DHCP Enabled

 DHCP server 172.16.16.1

 External IP Address 70.165.50.210

 Adapter Type Ethernet

 NetBIOS over TCP/IP Enabled via DHCP

 NETBIOS Node Type Hybrid node

 Link Speed 1.4 KBps

 Computer Name

 NetBIOS Name WIN10-CARLOSESP

 DNS Name WIN10-CARLOSESP

 Membership Part of workgroup

 Workgroup WORKGROUP

 Remote Desktop

 Disabled

 Console

 State Active

 Domain WIN10-CARLOSESP

 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 13

 Wi-Fi ()

 SSID

 Frequency 2462000 kHz

 Channel Number 11

 Name No name

 Signal Strength/Quality 100

 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 (DH-Guest)

 SSID DH-Guest

 Frequency 5180000 kHz

 Channel Number 36

 Name DH-Guest

 Signal Strength/Quality 70

 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 (DH-Guest 2.4)

 SSID DH-Guest 2.4

 Frequency 2437000 kHz

 Channel Number 6

 Name DH-Guest 2.4

 Signal Strength/Quality 47

 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 (DH-OFFICE)

 SSID DH-OFFICE

 Frequency 5785000 kHz

 Channel Number 157

 Name DH-OFFICE

 Signal Strength/Quality 100

 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 (DH-Repair 2.4)

 SSID DH-Repair 2.4

 Frequency 2437000 kHz

 Channel Number 6

 Name DH-Repair 2.4

 Signal Strength/Quality 46

 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 (DHT-WAREHOUSE)

 SSID DHT-WAREHOUSE

 Frequency 2437000 kHz

 Channel Number 6

 Name DHT-WAREHOUSE

 Signal Strength/Quality 0

 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 (FBI Van)

 SSID FBI Van

 Frequency 5180000 kHz

 Channel Number 36

 Name FBI Van

 Signal Strength/Quality 57

 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 802.11i RSNA algorithm that uses PSK

 Wi-Fi (Mobile AP 2.4)

 SSID Mobile AP 2.4

 Frequency 2457000 kHz

 Channel Number 10

 Name Mobile AP 2.4

 Signal Strength/Quality 62

 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 (Mobile AP 5)

 SSID Mobile AP 5

 Frequency 5785000 kHz

 Channel Number 157

 Name Mobile AP 5

 Signal Strength/Quality 60

 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 (Product\_Test)

 SSID Product\_Test

 Frequency 2462000 kHz

 Channel Number 11

 Name Product\_Test

 Signal Strength/Quality 62

 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 (Product\_Test\_5G)

 SSID Product\_Test\_5G

 Frequency 5785000 kHz

 Channel Number 157

 Name Product\_Test\_5G

 Signal Strength/Quality 68

 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 (Vetting No Internet)

 SSID Vetting No Internet

 Frequency 2412000 kHz

 Channel Number 1

 Name Vetting No Internet

 Signal Strength/Quality 72

 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 (Vetting No Internet-5G)

 SSID Vetting No Internet-5G

 Frequency 5200000 kHz

 Channel Number 40

 Name Vetting No Internet-5G

 Signal Strength/Quality 70

 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 Yes

 IEProxy Auto Config

 IEProxy

 IEProxy Bypass

 Default Proxy Config Access Type No proxy

 Default Config Proxy

 Default Config Proxy Bypass

 Sharing and Discovery

 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

 Private profile

 Network Discovery Enabled

 File and Printer Sharing Disabled

 Public profile

 Network Discovery Disabled

 File and Printer Sharing Disabled

 Adapters List

 Enabled

 Cisco AnyConnect Secure Mobility Client Virtual Miniport Adapter for Windows x64

 Connection-specific DNS Suffix Lorex.com

 Connection Name Ethernet 3

 NetBIOS over TCPIP Yes

 DHCP enabled No

 MAC Address 00-05-9A-3C-7A-00

 IP Address 10.137.221.59

 Subnet mask 255.255.255.0

 DNS Server 10.137.150.80

 Realtek PCIe GbE Family Controller

 Connection-specific DNS Suffix dahuasecurity.com

 Connection Name Ethernet

 NetBIOS over TCPIP Yes

 DHCP enabled Yes

 MAC Address 8C-EC-4B-50-40-85

 IP Address 172.16.16.79

 Subnet mask 255.255.255.0

 Gateway server 172.16.16.1

 DHCP 172.16.16.1

 DNS Server 172.16.8.1

 Realtek RTL8811AU Wireless LAN 802.11ac USB 2.0 Network Adapter

 Connection Name Wi-Fi

 NetBIOS over TCPIP Yes

 DHCP enabled Yes

 MAC Address 16-88-11-C3-73-C6

 IP Address 192.168.2.174

 Subnet mask 255.255.255.0

 Gateway server 192.168.2.1

 DHCP 192.168.2.1

 DNS Server 192.168.1.1

 8.8.8.8

 Network Shares

 No network shares

 Current TCP Connections

 \Device\HarddiskVolume4\Users\Dahua\Downloads\spsetup132.exe (20016)

 Local 172.16.16.79:51537 ESTABLISHED Remote 151.101.184.64:80 (Querying... ) (HTTP)

 C:\DSS Express\Server\activemq\bin\win32\DSS\_MQWrapper.exe (10420)

 Local 127.0.0.1:32000 LISTEN

 Local 127.0.0.1:32000 ESTABLISHED Remote 127.0.0.1:31000 (Querying... )

 C:\DSS Express\Server\ADS\DSS\_ADS.exe (8196)

 Local 192.168.2.174:55642 ESTABLISHED Remote 192.168.2.174:9400 (Querying... )

 Local 192.168.2.174:55641 ESTABLISHED Remote 192.168.2.174:9200 (Querying... )

 Local 127.0.0.1:36089 ESTABLISHED Remote 127.0.0.1:9000 (Querying... )

 Local 127.0.0.1:33601 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:33626 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:33627 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:33628 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:33629 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:33630 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 C:\DSS Express\Server\DMS\DSS\_DMS.exe (8216)

 Local 0.0.0.0:9200 LISTEN

 Local 0.0.0.0:9201 LISTEN

 Local 192.168.2.174:9200 ESTABLISHED Remote 192.168.2.174:55707 (Querying... )

 Local 192.168.2.174:9200 ESTABLISHED Remote 192.168.2.174:55641 (Querying... )

 Local 127.0.0.1:36070 ESTABLISHED Remote 127.0.0.1:9000 (Querying... )

 C:\DSS Express\Server\DSS Service\DSS\_Service.exe (4084)

 Local 0.0.0.0:7701 LISTEN

 C:\DSS Express\Server\jre\bin\DSS\_MQ.exe (11240)

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:34100 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:35854 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:35855 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:35856 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:35857 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:35858 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:35859 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:35860 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:35864 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:35865 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:35866 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:54866 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:54867 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:54868 (Querying... )

 Local 0.0.0.0:1883 LISTEN

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:54908 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:54909 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:55008 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:55009 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:34101 (Querying... )

 Local 127.0.0.1:33677 ESTABLISHED Remote 127.0.0.1:33676 (Querying... )

 Local 127.0.0.1:33676 ESTABLISHED Remote 127.0.0.1:33677 (Querying... )

 Local 127.0.0.1:33674 ESTABLISHED Remote 127.0.0.1:33675 (Querying... )

 Local 127.0.0.1:33675 ESTABLISHED Remote 127.0.0.1:33674 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:33626 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:33627 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:54907 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:33628 (Querying... )

 Local 127.0.0.1:31000 ESTABLISHED Remote 127.0.0.1:32000 (Querying... )

 Local 127.0.0.1:8161 LISTEN

 Local 0.0.0.0:61616 LISTEN

 Local 0.0.0.0:61613 LISTEN

 Local 0.0.0.0:33378 LISTEN

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:55006 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:33629 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:33630 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:34034 (Querying... )

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:34035 (Querying... )

 Local 0.0.0.0:5672 LISTEN

 Local 127.0.0.1:61616 ESTABLISHED Remote 127.0.0.1:33601 (Querying... )

 C:\DSS Express\Server\jre\bin\DSS\_WEB.exe (4996)

 Local 0.0.0.0:443 (HTTPS) LISTEN

 Local 127.0.0.1:54738 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:35970 ESTABLISHED Remote 127.0.0.1:35971 (Querying... )

 Local 127.0.0.1:54737 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54736 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 0.0.0.0:9000 LISTEN

 Local 0.0.0.0:9005 LISTEN

 Local 127.0.0.1:54735 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:55694 ESTABLISHED Remote 127.0.0.1:55695 (Querying... )

 Local 127.0.0.1:55695 ESTABLISHED Remote 127.0.0.1:55694 (Querying... )

 Local 127.0.0.1:55696 ESTABLISHED Remote 127.0.0.1:55698 (Querying... )

 Local 127.0.0.1:55698 ESTABLISHED Remote 127.0.0.1:55696 (Querying... )

 Local 127.0.0.1:54734 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:55699 ESTABLISHED Remote 127.0.0.1:55700 (Querying... )

 Local 127.0.0.1:55700 ESTABLISHED Remote 127.0.0.1:55699 (Querying... )

 Local 127.0.0.1:54733 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54732 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54731 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:55701 ESTABLISHED Remote 127.0.0.1:55702 (Querying... )

 Local 127.0.0.1:55702 ESTABLISHED Remote 127.0.0.1:55701 (Querying... )

 Local 127.0.0.1:55703 ESTABLISHED Remote 127.0.0.1:55704 (Querying... )

 Local 127.0.0.1:55704 ESTABLISHED Remote 127.0.0.1:55703 (Querying... )

 Local 127.0.0.1:54730 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 0.0.0.0:80 (HTTP) LISTEN

 Local 127.0.0.1:54729 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54728 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54727 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54726 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:35971 ESTABLISHED Remote 127.0.0.1:35970 (Querying... )

 Local 127.0.0.1:35995 ESTABLISHED Remote 127.0.0.1:35996 (Querying... )

 Local 127.0.0.1:35996 ESTABLISHED Remote 127.0.0.1:35995 (Querying... )

 Local 127.0.0.1:35997 ESTABLISHED Remote 127.0.0.1:35998 (Querying... )

 Local 127.0.0.1:35998 ESTABLISHED Remote 127.0.0.1:35997 (Querying... )

 Local 127.0.0.1:35999 ESTABLISHED Remote 127.0.0.1:36000 (Querying... )

 Local 127.0.0.1:36000 ESTABLISHED Remote 127.0.0.1:35999 (Querying... )

 Local 127.0.0.1:36001 ESTABLISHED Remote 127.0.0.1:36002 (Querying... )

 Local 127.0.0.1:36002 ESTABLISHED Remote 127.0.0.1:36001 (Querying... )

 Local 127.0.0.1:36003 ESTABLISHED Remote 127.0.0.1:36004 (Querying... )

 Local 127.0.0.1:36004 ESTABLISHED Remote 127.0.0.1:36003 (Querying... )

 Local 127.0.0.1:36005 ESTABLISHED Remote 127.0.0.1:36006 (Querying... )

 Local 127.0.0.1:36006 ESTABLISHED Remote 127.0.0.1:36005 (Querying... )

 Local 127.0.0.1:36007 ESTABLISHED Remote 127.0.0.1:36008 (Querying... )

 Local 127.0.0.1:36036 ESTABLISHED Remote 127.0.0.1:36035 (Querying... )

 Local 127.0.0.1:36008 ESTABLISHED Remote 127.0.0.1:36007 (Querying... )

 Local 127.0.0.1:36009 ESTABLISHED Remote 127.0.0.1:36010 (Querying... )

 Local 127.0.0.1:36010 ESTABLISHED Remote 127.0.0.1:36009 (Querying... )

 Local 127.0.0.1:36011 ESTABLISHED Remote 127.0.0.1:36012 (Querying... )

 Local 127.0.0.1:36012 ESTABLISHED Remote 127.0.0.1:36011 (Querying... )

 Local 127.0.0.1:36013 ESTABLISHED Remote 127.0.0.1:36014 (Querying... )

 Local 127.0.0.1:36014 ESTABLISHED Remote 127.0.0.1:36013 (Querying... )

 Local 127.0.0.1:36015 ESTABLISHED Remote 127.0.0.1:36016 (Querying... )

 Local 127.0.0.1:36016 ESTABLISHED Remote 127.0.0.1:36015 (Querying... )

 Local 127.0.0.1:36017 ESTABLISHED Remote 127.0.0.1:36018 (Querying... )

 Local 127.0.0.1:36018 ESTABLISHED Remote 127.0.0.1:36017 (Querying... )

 Local 127.0.0.1:36019 ESTABLISHED Remote 127.0.0.1:36020 (Querying... )

 Local 127.0.0.1:36020 ESTABLISHED Remote 127.0.0.1:36019 (Querying... )

 Local 127.0.0.1:36021 ESTABLISHED Remote 127.0.0.1:36022 (Querying... )

 Local 127.0.0.1:36022 ESTABLISHED Remote 127.0.0.1:36021 (Querying... )

 Local 127.0.0.1:36023 ESTABLISHED Remote 127.0.0.1:36024 (Querying... )

 Local 127.0.0.1:36024 ESTABLISHED Remote 127.0.0.1:36023 (Querying... )

 Local 127.0.0.1:36025 ESTABLISHED Remote 127.0.0.1:36026 (Querying... )

 Local 127.0.0.1:36026 ESTABLISHED Remote 127.0.0.1:36025 (Querying... )

 Local 127.0.0.1:36027 ESTABLISHED Remote 127.0.0.1:36028 (Querying... )

 Local 127.0.0.1:36028 ESTABLISHED Remote 127.0.0.1:36027 (Querying... )

 Local 127.0.0.1:36029 ESTABLISHED Remote 127.0.0.1:36030 (Querying... )

 Local 127.0.0.1:36030 ESTABLISHED Remote 127.0.0.1:36029 (Querying... )

 Local 127.0.0.1:36031 ESTABLISHED Remote 127.0.0.1:36032 (Querying... )

 Local 127.0.0.1:36032 ESTABLISHED Remote 127.0.0.1:36031 (Querying... )

 Local 127.0.0.1:36033 ESTABLISHED Remote 127.0.0.1:36034 (Querying... )

 Local 127.0.0.1:36034 ESTABLISHED Remote 127.0.0.1:36033 (Querying... )

 Local 127.0.0.1:36035 ESTABLISHED Remote 127.0.0.1:36036 (Querying... )

 Local 127.0.0.1:8005 LISTEN

 Local 127.0.0.1:52396 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:9000 ESTABLISHED Remote 127.0.0.1:36037 (Querying... )

 Local 127.0.0.1:9000 ESTABLISHED Remote 127.0.0.1:36039 (Querying... )

 Local 127.0.0.1:9000 ESTABLISHED Remote 127.0.0.1:36040 (Querying... )

 Local 127.0.0.1:9000 ESTABLISHED Remote 127.0.0.1:36041 (Querying... )

 Local 127.0.0.1:9000 ESTABLISHED Remote 127.0.0.1:36042 (Querying... )

 Local 127.0.0.1:9000 ESTABLISHED Remote 127.0.0.1:36043 (Querying... )

 Local 127.0.0.1:9000 ESTABLISHED Remote 127.0.0.1:36044 (Querying... )

 Local 127.0.0.1:9000 ESTABLISHED Remote 127.0.0.1:36049 (Querying... )

 Local 127.0.0.1:9000 ESTABLISHED Remote 127.0.0.1:36050 (Querying... )

 Local 127.0.0.1:9000 ESTABLISHED Remote 127.0.0.1:36051 (Querying... )

 Local 127.0.0.1:9000 ESTABLISHED Remote 127.0.0.1:36052 (Querying... )

 Local 127.0.0.1:9000 ESTABLISHED Remote 127.0.0.1:36070 (Querying... )

 Local 127.0.0.1:9000 ESTABLISHED Remote 127.0.0.1:36089 (Querying... )

 Local 127.0.0.1:55705 ESTABLISHED Remote 127.0.0.1:55706 (Querying... )

 Local 127.0.0.1:55706 ESTABLISHED Remote 127.0.0.1:55705 (Querying... )

 Local 192.168.2.174:55707 ESTABLISHED Remote 192.168.2.174:9200 (Querying... )

 Local 192.168.2.174:55697 ESTABLISHED Remote 192.168.2.174:9400 (Querying... )

 Local 127.0.0.1:52395 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:38919 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:35858 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:36046 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:36045 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:33804 ESTABLISHED Remote 127.0.0.1:33805 (Querying... )

 Local 127.0.0.1:33805 ESTABLISHED Remote 127.0.0.1:33804 (Querying... )

 Local 127.0.0.1:33817 ESTABLISHED Remote 127.0.0.1:33818 (Querying... )

 Local 127.0.0.1:33818 ESTABLISHED Remote 127.0.0.1:33817 (Querying... )

 Local 127.0.0.1:34034 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:34035 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:34100 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:34101 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:35854 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:35855 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:35856 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:35857 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:35859 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:35860 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:35864 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:35865 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:35866 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:35923 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:35964 ESTABLISHED Remote 127.0.0.1:35965 (Querying... )

 Local 127.0.0.1:35965 ESTABLISHED Remote 127.0.0.1:35964 (Querying... )

 Local 127.0.0.1:35966 ESTABLISHED Remote 127.0.0.1:35967 (Querying... )

 Local 127.0.0.1:35967 ESTABLISHED Remote 127.0.0.1:35966 (Querying... )

 Local 127.0.0.1:35968 ESTABLISHED Remote 127.0.0.1:35969 (Querying... )

 Local 127.0.0.1:35969 ESTABLISHED Remote 127.0.0.1:35968 (Querying... )

 Local 127.0.0.1:54739 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54740 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54741 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54742 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54743 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54744 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54866 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:54867 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:54868 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:54907 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:54908 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:54909 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:54913 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54914 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54915 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54916 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:54917 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:55006 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:55008 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:55009 ESTABLISHED Remote 127.0.0.1:61616 (Querying... )

 Local 127.0.0.1:55015 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:55016 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:55017 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:55018 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:55019 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:55046 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:55047 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:55455 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:55456 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:55457 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:55674 ESTABLISHED Remote 127.0.0.1:55675 (Querying... )

 Local 127.0.0.1:55675 ESTABLISHED Remote 127.0.0.1:55674 (Querying... )

 Local 127.0.0.1:55676 ESTABLISHED Remote 127.0.0.1:55677 (Querying... )

 Local 127.0.0.1:55677 ESTABLISHED Remote 127.0.0.1:55676 (Querying... )

 Local 127.0.0.1:55678 ESTABLISHED Remote 127.0.0.1:55679 (Querying... )

 Local 127.0.0.1:55679 ESTABLISHED Remote 127.0.0.1:55678 (Querying... )

 Local 127.0.0.1:55680 ESTABLISHED Remote 127.0.0.1:55681 (Querying... )

 Local 127.0.0.1:55681 ESTABLISHED Remote 127.0.0.1:55680 (Querying... )

 Local 127.0.0.1:55682 ESTABLISHED Remote 127.0.0.1:55683 (Querying... )

 Local 127.0.0.1:55683 ESTABLISHED Remote 127.0.0.1:55682 (Querying... )

 Local 127.0.0.1:55684 ESTABLISHED Remote 127.0.0.1:55685 (Querying... )

 Local 127.0.0.1:55685 ESTABLISHED Remote 127.0.0.1:55684 (Querying... )

 Local 127.0.0.1:55686 ESTABLISHED Remote 127.0.0.1:55687 (Querying... )

 Local 127.0.0.1:55687 ESTABLISHED Remote 127.0.0.1:55686 (Querying... )

 Local 127.0.0.1:55688 ESTABLISHED Remote 127.0.0.1:55689 (Querying... )

 Local 127.0.0.1:55689 ESTABLISHED Remote 127.0.0.1:55688 (Querying... )

 Local 127.0.0.1:55690 ESTABLISHED Remote 127.0.0.1:55691 (Querying... )

 Local 127.0.0.1:55691 ESTABLISHED Remote 127.0.0.1:55690 (Querying... )

 Local 127.0.0.1:55692 ESTABLISHED Remote 127.0.0.1:55693 (Querying... )

 Local 127.0.0.1:55693 ESTABLISHED Remote 127.0.0.1:55692 (Querying... )

 C:\DSS Express\Server\MCDALARM\DSS\_MCDAlarm.exe (8284)

 Local 127.0.0.1:36052 ESTABLISHED Remote 127.0.0.1:9000 (Querying... )

 C:\DSS Express\Server\MCDDOOR\DSS\_MCDDoor.exe (8336)

 Local 127.0.0.1:33340 ESTABLISHED Remote 127.0.0.1:33341 (Querying... )

 Local 127.0.0.1:36042 ESTABLISHED Remote 127.0.0.1:9000 (Querying... )

 Local 127.0.0.1:33341 ESTABLISHED Remote 127.0.0.1:33340 (Querying... )

 Local 127.0.0.1:33338 ESTABLISHED Remote 127.0.0.1:33339 (Querying... )

 Local 127.0.0.1:33339 ESTABLISHED Remote 127.0.0.1:33338 (Querying... )

 C:\DSS Express\Server\MCDLED\DSS\_MCDLed.exe (8360)

 Local 127.0.0.1:36043 ESTABLISHED Remote 127.0.0.1:9000 (Querying... )

 C:\DSS Express\Server\MGW\DSS\_MGW.exe (8452)

 Local 0.0.0.0:9090 LISTEN

 Local 127.0.0.1:36040 ESTABLISHED Remote 127.0.0.1:9000 (Querying... )

 C:\DSS Express\Server\MTS\DSS\_MTS.exe (8476)

 Local 0.0.0.0:9099 LISTEN

 Local 0.0.0.0:9100 LISTEN

 Local 0.0.0.0:9102 LISTEN

 Local 127.0.0.1:36039 ESTABLISHED Remote 127.0.0.1:9000 (Querying... )

 Local 127.0.0.1:33369 ESTABLISHED Remote 127.0.0.1:33370 (Querying... )

 Local 127.0.0.1:33348 ESTABLISHED Remote 127.0.0.1:33347 (Querying... )

 Local 127.0.0.1:33347 ESTABLISHED Remote 127.0.0.1:33348 (Querying... )

 Local 127.0.0.1:33370 ESTABLISHED Remote 127.0.0.1:33369 (Querying... )

 C:\DSS Express\Server\mysql\bin\mysqld.exe (9688)

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:38919 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:52395 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:52396 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54726 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54727 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54728 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54729 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54730 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54732 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54733 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54734 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54735 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54736 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54737 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54738 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54739 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54740 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54741 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54742 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54743 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54744 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54913 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54914 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54915 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54916 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54917 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:55015 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:55016 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:55017 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:55018 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:55019 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:55046 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:55047 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:55455 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:55456 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:55457 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:54731 (Querying... )

 Local 0.0.0.0:3306 LISTEN

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:33757 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:33759 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:35923 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:35946 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:36045 (Querying... )

 Local 127.0.0.1:3306 ESTABLISHED Remote 127.0.0.1:36046 (Querying... )

 C:\DSS Express\Server\OSS\DSS\_OSS.exe (8236)

 Local 0.0.0.0:9900 LISTEN

 Local 0.0.0.0:9901 LISTEN

 C:\DSS Express\Server\PCPS\DSS\_PCPS.exe (8504)

 Local 127.0.0.1:33344 ESTABLISHED Remote 127.0.0.1:33343 (Querying... )

 Local 127.0.0.1:33343 ESTABLISHED Remote 127.0.0.1:33344 (Querying... )

 Local 127.0.0.1:33360 ESTABLISHED Remote 127.0.0.1:10504 (Querying... )

 Local 127.0.0.1:33359 ESTABLISHED Remote 127.0.0.1:10503 (Querying... )

 Local 127.0.0.1:36050 ESTABLISHED Remote 127.0.0.1:9000 (Querying... )

 Local 127.0.0.1:10504 ESTABLISHED Remote 127.0.0.1:33360 (Querying... )

 Local 127.0.0.1:10504 LISTEN

 Local 127.0.0.1:10503 ESTABLISHED Remote 127.0.0.1:33359 (Querying... )

 Local 127.0.0.1:10503 LISTEN

 C:\DSS Express\Server\PES\DSS\_PES.exe (8544)

 Local 127.0.0.1:36044 ESTABLISHED Remote 127.0.0.1:9000 (Querying... )

 Local 192.168.2.174:9400 ESTABLISHED Remote 192.168.2.174:55642 (Querying... )

 Local 192.168.2.174:9400 ESTABLISHED Remote 192.168.2.174:55697 (Querying... )

 Local 0.0.0.0:9400 LISTEN

 C:\DSS Express\Server\PTS\DSS\_PTS.exe (10072)

 Local 127.0.0.1:36041 ESTABLISHED Remote 127.0.0.1:9000 (Querying... )

 Local 127.0.0.1:33757 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 0.0.0.0:18081 LISTEN

 Local 0.0.0.0:9115 LISTEN

 C:\DSS Express\Server\SearchDevice\DSS\_SOSO.exe (8628)

 Local 127.0.0.1:33334 ESTABLISHED Remote 127.0.0.1:33333 (Querying... )

 Local 127.0.0.1:33333 ESTABLISHED Remote 127.0.0.1:33334 (Querying... )

 Local 127.0.0.1:33331 ESTABLISHED Remote 127.0.0.1:33332 (Querying... )

 Local 0.0.0.0:12366 LISTEN

 Local 127.0.0.1:33332 ESTABLISHED Remote 127.0.0.1:33331 (Querying... )

 C:\DSS Express\Server\SS\DSS\_SS.exe (10372)

 Local 127.0.0.1:33442 ESTABLISHED Remote 127.0.0.1:33443 (Querying... )

 Local 127.0.0.1:36037 ESTABLISHED Remote 127.0.0.1:9000 (Querying... )

 Local 127.0.0.1:33358 ESTABLISHED Remote 127.0.0.1:33357 (Querying... )

 Local 127.0.0.1:33443 ESTABLISHED Remote 127.0.0.1:33442 (Querying... )

 Local 127.0.0.1:33357 ESTABLISHED Remote 127.0.0.1:33358 (Querying... )

 Local 0.0.0.0:9322 LISTEN

 Local 0.0.0.0:9320 LISTEN

 Local 0.0.0.0:9319 LISTEN

 C:\DSS Express\Server\SwitchCenter\DSS\_SC.exe (9024)

 Local 127.0.0.1:35946 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:33354 ESTABLISHED Remote 127.0.0.1:10502 (Querying... )

 Local 127.0.0.1:33759 ESTABLISHED Remote 127.0.0.1:3306 (Querying... )

 Local 127.0.0.1:33353 ESTABLISHED Remote 127.0.0.1:10501 (Querying... )

 Local 127.0.0.1:36051 ESTABLISHED Remote 127.0.0.1:9000 (Querying... )

 Local 127.0.0.1:10502 ESTABLISHED Remote 127.0.0.1:33354 (Querying... )

 Local 127.0.0.1:10502 LISTEN

 Local 127.0.0.1:10501 ESTABLISHED Remote 127.0.0.1:33353 (Querying... )

 Local 127.0.0.1:10501 LISTEN

 C:\DSS Express\Server\VMS\DSS\_VMS.exe (9596)

 Local 127.0.0.1:33346 ESTABLISHED Remote 127.0.0.1:33345 (Querying... )

 Local 127.0.0.1:33345 ESTABLISHED Remote 127.0.0.1:33346 (Querying... )

 Local 127.0.0.1:36049 ESTABLISHED Remote 127.0.0.1:9000 (Querying... )

 C:\Program Files (x86)\AnyDesk-b067a865\AnyDesk-b067a865.exe (3872)

 Local 0.0.0.0:7071 LISTEN

 Local 172.16.16.79:33289 ESTABLISHED Remote 23.111.187.173:80 (Querying... ) (HTTP)

 C:\Program Files (x86)\AnyDesk\AnyDesk.exe (3864)

 Local 0.0.0.0:7070 LISTEN

 Local 172.16.16.79:33288 ESTABLISHED Remote 148.72.171.164:80 (Querying... ) (HTTP)

 C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe (18544)

 Local 172.16.16.79:55668 ESTABLISHED Remote 172.217.165.14:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:36981 ESTABLISHED Remote 35.201.97.85:443 (Querying... ) (HTTPS)

 C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\vpnagent.exe (2540)

 Local 127.0.0.1:62522 ESTABLISHED Remote 127.0.0.1:33861 (Querying... )

 Local 127.0.0.1:62522 LISTEN

 C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\vpnui.exe (6260)

 Local 127.0.0.1:33861 ESTABLISHED Remote 127.0.0.1:62522 (Querying... )

 C:\Program Files (x86)\Google\Chrome\Application\chrome.exe (20932)

 Local 172.16.16.79:49988 ESTABLISHED Remote 104.18.226.52:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:49991 ESTABLISHED Remote 184.84.40.149:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:49992 ESTABLISHED Remote 184.84.40.149:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:49931 ESTABLISHED Remote 162.248.19.147:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:43935 ESTABLISHED Remote 151.101.185.253:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:50000 ESTABLISHED Remote 104.88.157.237:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:43936 ESTABLISHED Remote 104.88.157.64:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:43939 ESTABLISHED Remote 104.88.157.64:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:50013 ESTABLISHED Remote 172.106.143.54:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:50018 ESTABLISHED Remote 172.217.164.226:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:50020 ESTABLISHED Remote 184.84.40.149:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:50021 ESTABLISHED Remote 104.88.157.64:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:50034 ESTABLISHED Remote 23.111.8.18:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:50036 ESTABLISHED Remote 23.74.9.29:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:43945 ESTABLISHED Remote 35.244.172.133:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:50040 ESTABLISHED Remote 172.217.164.226:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:43946 ESTABLISHED Remote 104.98.197.93:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:51526 ESTABLISHED Remote 99.84.167.81:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:51527 ESTABLISHED Remote 52.4.74.49:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:51529 ESTABLISHED Remote 104.17.65.4:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:51531 ESTABLISHED Remote 23.73.168.49:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:51532 ESTABLISHED Remote 23.73.168.49:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:43948 ESTABLISHED Remote 172.217.1.174:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:43958 ESTABLISHED Remote 74.119.119.151:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:51539 ESTABLISHED Remote 151.139.128.10:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:51540 ESTABLISHED Remote 205.185.216.42:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:51541 ESTABLISHED Remote 205.185.216.10:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:51542 ESTABLISHED Remote 3.91.171.244:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:53307 ESTABLISHED Remote 35.244.186.129:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:53308 ESTABLISHED Remote 185.167.164.49:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:53311 ESTABLISHED Remote 23.74.8.61:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:53312 ESTABLISHED Remote 184.24.145.135:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:53316 ESTABLISHED Remote 107.178.246.49:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:53317 ESTABLISHED Remote 151.101.186.49:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:43960 ESTABLISHED Remote 172.217.164.230:443 (Querying... ) (HTTPS)

 Local 10.137.221.59:36760 ESTABLISHED Remote 170.14.88.5:8443 (Querying... )

 Local 172.16.16.79:49930 ESTABLISHED Remote 35.190.72.21:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:55650 ESTABLISHED Remote 74.125.69.188:5228 (Querying... )

 Local 172.16.16.79:49937 ESTABLISHED Remote 35.244.140.139:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:49938 ESTABLISHED Remote 151.101.184.166:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56017 ESTABLISHED Remote 172.217.0.238:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56019 ESTABLISHED Remote 172.217.1.14:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56022 ESTABLISHED Remote 35.244.172.133:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56025 ESTABLISHED Remote 151.101.186.133:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56026 ESTABLISHED Remote 151.101.186.133:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56038 ESTABLISHED Remote 99.84.249.86:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56039 ESTABLISHED Remote 74.119.119.131:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56040 ESTABLISHED Remote 23.192.42.68:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56044 ESTABLISHED Remote 99.84.251.94:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56046 ESTABLISHED Remote 104.88.157.163:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56048 ESTABLISHED Remote 99.84.249.86:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56050 ESTABLISHED Remote 99.84.251.8:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56052 ESTABLISHED Remote 151.101.186.2:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56055 ESTABLISHED Remote 74.119.119.150:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56060 ESTABLISHED Remote 99.84.251.8:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56064 ESTABLISHED Remote 104.88.157.64:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56065 ESTABLISHED Remote 172.217.165.14:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56069 ESTABLISHED Remote 172.217.0.225:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56071 ESTABLISHED Remote 104.88.157.64:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56072 ESTABLISHED Remote 104.98.198.31:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56073 ESTABLISHED Remote 104.98.198.31:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56075 ESTABLISHED Remote 104.98.198.31:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:56078 ESTABLISHED Remote 184.87.52.72:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:49942 ESTABLISHED Remote 185.86.138.114:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:49943 ESTABLISHED Remote 74.119.119.139:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:49944 ESTABLISHED Remote 35.227.197.177:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:49954 ESTABLISHED Remote 184.84.40.149:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:49961 ESTABLISHED Remote 151.101.186.202:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:49965 ESTABLISHED Remote 50.97.40.233:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:49976 ESTABLISHED Remote 104.88.157.237:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:49977 ESTABLISHED Remote 50.97.40.233:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:49979 ESTABLISHED Remote 184.27.66.251:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:49982 ESTABLISHED Remote 151.101.186.202:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:50039 ESTABLISHED Remote 172.217.5.227:443 (Querying... ) (HTTPS)

 C:\Program Files (x86)\iNode\iNode Client\iNode Client.exe (4532)

 Local 127.0.0.1:33521 ESTABLISHED Remote 127.0.0.1:8900 (Querying... )

 C:\Program Files (x86)\iNode\iNode Client\iNodeCmn.exe (6528)

 Local 127.0.0.1:33321 ESTABLISHED Remote 127.0.0.1:8900 (Querying... )

 C:\Program Files (x86)\iNode\iNode Client\iNodeImg.exe (4672)

 Local 127.0.0.1:33310 ESTABLISHED Remote 127.0.0.1:33311 (Querying... )

 Local 127.0.0.1:33311 ESTABLISHED Remote 127.0.0.1:33310 (Querying... )

 Local 127.0.0.1:8900 ESTABLISHED Remote 127.0.0.1:33293 (Querying... )

 Local 127.0.0.1:8900 ESTABLISHED Remote 127.0.0.1:33521 (Querying... )

 Local 127.0.0.1:8900 ESTABLISHED Remote 127.0.0.1:33324 (Querying... )

 Local 127.0.0.1:8900 ESTABLISHED Remote 127.0.0.1:33321 (Querying... )

 Local 127.0.0.1:8900 ESTABLISHED Remote 127.0.0.1:33319 (Querying... )

 Local 0.0.0.0:8900 LISTEN

 C:\Program Files (x86)\iNode\iNode Client\iNodeMon.exe (4032)

 Local 127.0.0.1:33293 ESTABLISHED Remote 127.0.0.1:8900 (Querying... )

 C:\Program Files (x86)\iNode\iNode Client\iNodePortal.exe (6576)

 Local 127.0.0.1:33324 ESTABLISHED Remote 127.0.0.1:8900 (Querying... )

 C:\Program Files (x86)\iNode\iNode Client\iNodeSec.exe (6536)

 Local 127.0.0.1:33319 ESTABLISHED Remote 127.0.0.1:8900 (Querying... )

 C:\Program Files (x86)\Internet Explorer\iexplore.exe (488)

 Local 172.16.16.79:51538 CLOSE-WAIT Remote 132.148.21.102:443 (Querying... ) (HTTPS)

 C:\Program Files (x86)\Splashtop\Splashtop Remote\Server\SRManager.exe (4964)

 Local 0.0.0.0:6783 LISTEN

 Local 172.16.16.79:33586 ESTABLISHED Remote 35.212.195.47:443 (Querying... ) (HTTPS)

 Local 127.0.0.1:9527 LISTEN

 C:\Program Files\Common Files\McAfee\AVSolution\mcshield.exe (6488)

 Local 172.16.16.79:43965 ESTABLISHED Remote 8.18.25.28:443 (Querying... ) (HTTPS)

 C:\Program Files\Dell\SupportAssistAgent\bin\SupportAssistAgent.exe (20072)

 Local 0.0.0.0:9012 LISTEN

 C:\Program Files\Dell\SupportAssistAgent\PCDr\SupportAssist\6.0.7033.2285\DSAPI.exe (15516)

 Local 127.0.0.1:34118 ESTABLISHED Remote 127.0.0.1:34104 (Querying... )

 Local 127.0.0.1:54850 LISTEN

 C:\Program Files\Dell\SupportAssistAgent\PCDr\SupportAssist\6.0.7033.2285\pcdrwi.exe (18076)

 Local 127.0.0.1:34104 ESTABLISHED Remote 127.0.0.1:34118 (Querying... )

 Local 127.0.0.1:34104 LISTEN

 C:\Program Files\McAfee\Agent\macmnsvc.exe (3352)

 Local 0.0.0.0:8081 LISTEN

 C:\Program Files\Microsoft Office\Office16\OUTLOOK.EXE (14628)

 Local 172.16.16.79:34084 ESTABLISHED Remote 13.57.81.62:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:34119 ESTABLISHED Remote 13.57.81.62:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:38641 ESTABLISHED Remote 13.57.81.62:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:38642 ESTABLISHED Remote 13.57.81.62:443 (Querying... ) (HTTPS)

 C:\Users\Dahua\AppData\Local\slack\app-4.1.2\slack.exe (4160)

 Local 172.16.16.79:55107 ESTABLISHED Remote 34.194.201.2:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:43951 ESTABLISHED Remote 99.84.174.165:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:55669 ESTABLISHED Remote 13.249.92.165:443 (Querying... ) (HTTPS)

 C:\Windows\System32\lsass.exe (348)

 Local 0.0.0.0:33323 LISTEN

 C:\Windows\System32\spoolsv.exe (3516)

 Local 172.16.16.79:33386 ESTABLISHED Remote 172.16.16.211:50610 (Querying... )

 Local 0.0.0.0:33283 LISTEN

 C:\Windows\System32\svchost.exe (1104)

 Local 0.0.0.0:135 (DCE) LISTEN

 C:\Windows\System32\svchost.exe (14096)

 Local 0.0.0.0:5040 LISTEN

 C:\Windows\System32\svchost.exe (1728)

 Local 0.0.0.0:33281 LISTEN

 C:\Windows\System32\svchost.exe (1840)

 Local 0.0.0.0:33282 LISTEN

 C:\Windows\System32\svchost.exe (4524)

 Local 172.16.16.79:54269 ESTABLISHED Remote 52.242.211.89:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:55649 ESTABLISHED Remote 52.179.224.121:443 (Querying... ) (HTTPS)

 services.exe (1000)

 Local 0.0.0.0:33322 LISTEN

 System Process

 Local 127.0.0.1:8884 LISTEN

 Local 172.16.16.79:139 (NetBIOS session service) LISTEN

 Local 0.0.0.0:445 (Windows shares) LISTEN

 Local 172.16.16.79:33382 ESTABLISHED Remote 172.16.16.211:445 (Querying... ) (Windows shares)

 Local 0.0.0.0:5357 LISTEN

 Local 0.0.0.0:5700 LISTEN

 Local 192.168.2.174:139 (NetBIOS session service) LISTEN

 Local 10.137.221.59:139 (NetBIOS session service) LISTEN

 System Process

 Local 172.16.16.79:58091 TIME-WAIT Remote 72.21.81.240:80 (Querying... ) (HTTP)

 Local 172.16.16.79:33384 TIME-WAIT Remote 172.16.16.211:135 (Querying... ) (DCE)

 Local 172.16.16.79:49993 TIME-WAIT Remote 52.109.88.37:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:49975 TIME-WAIT Remote 139.178.69.23:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:51525 TIME-WAIT Remote 172.16.8.1:53 (Querying... )

 Local 172.16.16.79:50005 TIME-WAIT Remote 23.34.203.27:80 (Querying... ) (HTTP)

 Local 172.16.16.79:50003 TIME-WAIT Remote 23.34.203.27:80 (Querying... ) (HTTP)

 Local 172.16.16.79:49994 TIME-WAIT Remote 52.109.124.18:443 (Querying... ) (HTTPS)

 Local 172.16.16.79:58088 TIME-WAIT Remote 172.16.8.1:53 (Querying... )

 wininit.exe (924)

 Local 0.0.0.0:33280 LISTEN

Generated with Speccy v1.32.740