

Forum: [Hack Forums](#)

Thread: [\[MRT-X Academy\] FRST Tutorial](#)

Tha Sneak - February 14, 2025, 4:42 am

Farbar Recovery Scan Tool (FRST)

What is FRST?

FRST is a diagnostic and script execution tool designed for malware-infected machines. It works in normal mode, safe mode, and even in the Windows Recovery Environment (WinRE), making it a powerful tool for troubleshooting boot issues and system errors.

? Table of Contents ?

1. Introduction
2. Default Scan Areas
3. Main Scan (FRST.txt) Processes

Registry

Scheduled Tasks

Internet

Services/Drivers

NetSvcs

One month (Created/Modified)

FLock

FCheck

KnownDLLs

SigCheck

Association

Restore Points

Memory Info

Drives and MBR & Partition Table

LastRegBack

4. Additional Scan (Addition.txt) Accounts

Security Center

Installed Programs

Custom CLSID

Codecs

Shortcuts & WMI

Loaded Modules

Alternate Data Streams

Safe Mode

Association

Internet Explorer

Hosts Content

Other Areas

MSCONFIG/TASK MANAGER Disabled Items

FirewallRules

Restore Points

Faulty Device Manager Devices

Event Log Errors

Memory Info

Drives

MBR & Partition Table

5. Other Optional Scans List BCD

SigCheckExt

Shortcut.txt

90 Days Files

Search Files

Search Registry

6. Directives/Commands CloseProcesses:

CMD:

Comment:

Copy:

CreateDummy:

CreateRestorePoint:

DeleteJunctionsInDirectory:

DeleteKey: and DeleteValue:

DeleteQuarantine:

DisableService:

EmptyEventLogs:

EmptyTemp:

ExportKey: and ExportValue:

File:

FilesInDirectory: and Folder:

FindFolder:

Hosts:

ListPermissions:

Move:

Powershell:

Reboot:

Reg:

RemoveDirectory:

RemoveProxy:

Replace:

RestoreFromBackup:

RestoreMbr:

RestoreQuarantine:

SaveMbr:

SetDefaultFilePermissions:

StartBatch: — EndBatch:

StartPowershell: — EndPowershell

StartRegedit: — EndRegedit:

Symlink:

SystemRestore:

TasksDetails:

testsigning on:

Unlock:

Virusscan:

Zip:

? Introduction

? Simplicity of FRST

One of FRST's strengths is its simplicity. It is designed to be user-friendly—allowing infected items to be identified from logs, copied into Notepad, and executed with one click. This enables flexibility, as new infections appear they can be detected and removed.

? Tool Compatibility

Farbar's Recovery Scan Tool (FRST) is compatible with:?

- Windows XP

- Windows Vista

- Windows 7

- Windows 8

- Windows 10

- Windows 11

There are two versions:

- 32-bit version

- 64-bit version

[highlight]? Note: FRST64 is NOT designed to run on XP 64-bit systems.[/highlight]

? Diagnosis

FRST generates a log covering specific Windows OS areas, which can be used for initial problem analysis and system diagnostics.

? Automatic Updates:

When FRST starts, it automatically checks for updates if the PC is connected to the internet. If an update is available, users are notified to download the latest version.

? Whitelisting in FRST

To avoid overly long logs, FRST applies whitelisting by default. If a full log is needed, the whitelist option should be unchecked.

- What is Whitelisted?? Default Microsoft entries.

- Default Microsoft Services & Drivers.

- Signed Microsoft executables on the "One month (created)" list.

- What is NOT Whitelisted?? Entries with unsigned files.

- Security programs (AV or Firewalls).

? SPTD service.

If a full log is required, be prepared for large file sizes, which may need to be uploaded as an attachment.

? Preparation for Use

? Run as Administrator

Make sure FRST is run with administrator privileges. If not, it will not function properly.

? If the user lacks administrator rights, a warning will appear in the header of FRST.txt.

? Security Software Interference

Some security programs may prevent FRST from running fully.

? While this is uncommon, be aware that security software like Comodo may block FRST.

? Solution: Disable such programs before fixing to ensure FRST works properly.

? Rootkit Handling Recommendation

? When dealing with rootkits, it is best to:

? Perform one fix at a time

? Wait for the outcome before running another tool

? Registry Backup

? No need to create a registry backup—FRST automatically backs up registry hives the first time it runs.

? The backup is stored at:

%SystemDrive%\FRST\Hives (Usually C:\FRST\Hives)

? To restore, refer to the RestoreFromBackup: directive.

? Using FRST in English

FRST supports multiple languages, but helpers prefer English logs for analysis.

To run FRST in English, rename the file:

? EnglishFRST.exe

? EnglishFRST64.exe

? FRSTEnglish.exe

? FRSTEnglish64.exe

? This ensures the log is generated in English.

? Running FRST

? Download FRST to the Desktop and double-click the icon.

? Accept the disclaimer

? Start the scan

? The FRST icon looks like this:

? You must run the correct version for your system.

? If unsure, download both (32-bit & 64-bit) and run each—only one will work.

? The FRST console looks like this when opened:

? Log Files & Storage

? Once FRST completes its scan:

? Log files are saved in the same location where FRST was started.

? First and subsequent scans outside the Recovery Environment generate:

- FRST.txt log
- Addition.txt log

? Log file storage location:

? %SystemDrive%\FRST\Logs (Usually C:\FRST\Logs)

? Fixing Issues with FRST

? Very Important!

Farbar Recovery Scan Tool is non-invasive and in scan mode, it cannot harm a machine.

However, FRST is highly effective at executing commands.

? If asked to remove an item, 99% of the time, it will do so.

While built-in safeguards exist, they are broad-based to prevent interference with malware removal.

? Incorrect use (e.g., removing essential system files) can render a computer unbootable!

? If unsure about any item in an FRST report, always seek expert help before applying a fix.

? Preparing Fixlist

FRST provides multiple methods to prepare a fixlist.txt file for problem resolution.

? 1. Fixlist.txt method

? Copy and paste identified problems from FRST logs into a new text file.

? Save it as fixlist.txt in the same directory as FRST.

? Important: Always use Notepad! The fix will not work if saved in Word or another program.

? 2. Ctrl + Y Method

? Launch FRST

? Press Ctrl + Y to automatically create and open an empty file

? Paste the fix & press Ctrl + S to save

? 3. Clipboard Method

Use Start:: and End:: to encapsulate the fix.

Code Start::

script content

End::

? Have the user copy the entire block

? Click the Fix button in FRST

Tha Sneak - March 2, 2025, 8:50 am

? Handling Unicode Characters

To fix an entry containing Unicode characters, the script must be saved in Unicode format.

? Ctrl + Y automatically saves in Unicode.

? If manually creating fixlist.txt, choose UTF-8 encoding in Notepad.

? Example Unicode Entries:

Quote:S2 ?????????t; ????????????????????????????? [X]

ShortcutWithArgument: C:\Users\Public\Desktop\G??gl? ?hr?m?.lnk ->

C:\Users\User\AppData\Roaming\HPRewriter2\RewRun3.exe (QIIXU APZEDEEMFA) -> 1 0

<===== Cyrillic

2016-08-17 14:47 - 2016-08-17 16:23 - 00000000___ C:\ProgramData\Google Chrome.lnk.bat

? Correct Saving Method

? Copy and paste the entries into Notepad

? Click Save As...

? Choose UTF-8 Encoding

? Save the file as fixlist.txt

? If Notepad warns about encoding, confirm and proceed with UTF-8.

? Incorrect Encoding Output (If Notepad is not set to UTF-8):

Quote:S2 ?????????t; ????????????????????????????? [X]

C:\Users\Public\Desktop\G??gl? ?hr?m?.lnk

2016-08-17 14:47 - 2016-08-17 16:23 - 00000000___ C:\ProgramData\Google Chrome.lnk.bat

? FRST will not be able to process these entries! Always ensure UTF-8 encoding.

? Manipulated Usernames

Some users alter logs by removing or replacing a username.

To ensure that correct paths are processed, replace the potentially manipulated username in paths with:

? CurrentUserName (for the logged-in user)

? AllUserName (for all users)

FRST will automatically translate these keywords to the correct username.

? Note: CurrentUserName is not supported in the Recovery Environment.

? To prevent FRST from hanging for hours due to incorrect scripts, the CMD: and Powershell: directives execution time is limited to 60 minutes.

? Items moved by the fix are stored in %SystemDrive%\FRST\Quarantine

(In most cases: C:\FRST\Quarantine) until cleanup and deletion of FRST.

For detailed information on preparing fixes, see the sections below.

? Removing FRST

To automatically remove all files/folders created by FRST and the tool itself:

? Rename FRST.exe or FRST64.exe to uninstall.exe

? Run it

? A reboot is required.

? This works only outside the Recovery Environment.

? Default Scan Areas

? On the first and subsequent scans outside the Recovery Environment, FRST generates:

? FRST.txt log

? Addition.txt log

? Addition.txt is NOT generated in the Recovery Environment.

? Scans Run in Normal Mode:

? Main Scan:

? Processes [Digital Signature Check]

? Registry [Digital Signature Check]

? Scheduled Tasks [Digital Signature Check]

? Internet [Digital Signature Check]

? Services [Digital Signature Check]

? Drivers [Digital Signature Check]

? NetSvcs

? One month (Created) [Microsoft Digital Signature Check]

? One month (Modified)

? Files in the root of some directories

? FLock

? FCheck

? SigCheck [Digital Signature Check]

? LastRegBack

? Additional Scan:

? Accounts

? Security Center

? Installed Programs

? Custom CLSID [Digital Signature Check]

? Codecs [Digital Signature Check]

? Shortcuts & WMI

? Loaded Modules [Digital Signature Check]

- ? Alternate Data Streams
- ? Safe Mode
- ? Association
- ? Internet Explorer [Digital Signature Check]
- ? Hosts content
- ? Other Areas
- ? MSCONFIG/TASK MANAGER disabled items
- ? Firewall Rules [Digital Signature Check]
- ? Restore Points
- ? Faulty Device Manager Devices
- ? Event log errors
- ? Memory info
- ? Drives
- ? MBR & Partition Table

? Optional Scans:

- ? List BCD
- ? SigCheckExt [Digital Signature Check]
- ? Shortcut.txt
- ? Addition.txt
- ? 90 Days Files
- ? Search Files [Digital Signature Check]
- ? Search Registry

? Note: [File not signed] will be printed for files without a digital signature or with an unverifiable signature.

? Scans Run in the Recovery Environment:

? Main Scan:

- ? Registry
- ? Scheduled Tasks
- ? Services
- ? Drivers
- ? NetSvcs
- ? One month (Created)
- ? One month (Modified)
- ? KnownDLLs
- ? SigCheck
- ? Association
- ? Restore Points
- ? Memory info
- ? Drives
- ? MBR & Partition Table
- ? LastRegBack

? Optional Scans:

- ? List BCD
- ? 90 Days Files
- ? Search Files

? Note: The digital signatures check is NOT available in the Recovery Environment.

? Main Scan (FRST.txt)

? Header

Here is an example header:

Quote: Scan result of Farbar Recovery Scan Tool (FRST) (x64) Version: 28-08-2023
Ran by User (administrator) on DESKTOP-696969 (Dell Inc. Inspiron 7352) (03-09-2023 22:20:17)
Running from C:\Users\User\Desktop\FRST64.exe
Loaded Profiles: User
Platform: Windows 10 Pro Version 22H2 19045.3324 (X64) Language: English (United States)
Default browser: FF
Boot Mode: Normal

? How to Analyze the Header:

? First Line:

- Indicates whether FRST 32-bit or 64-bit was run.
- Shows FRST version identifier – ? An old version may lack recent updates.

? Second Line:

- Displays the user who ran the tool and their permission level (admin or standard).
- Shows the computer name, manufacturer, and model (if available).
- Records the scan date and time – Helps determine if a user provided an outdated log.

? Third Line:

- Shows where FRST was executed from (e.g., Desktop, USB, or another location).
- This may be relevant for fix instructions if FRST was run from an unexpected directory.

? Fourth Line:

- Lists the loaded user profile(s) (i.e., ntuser.dat and UsrClass.dat are loaded).

? Note:

If multiple accounts are active (via "Switch User" or "Log Off"), FRST will list all loaded accounts and their registry entries.

Accounts not loaded won't appear under "Loaded Profiles," but FRST will still mount their ntuser.dat hive for scanning.

? Fifth Line:

- Identifies the Windows edition, major updates (Windows 10/11 Version and OS Build), or Service Pack (Windows 7 and older).
- Useful for diagnosing update issues if the version is outdated.

? Sixth Line:

- Indicates the system's default browser.

? Seventh Line:

- Displays the scan mode used (Normal / Safe Mode / Recovery Environment).

? Note:

Headers in the Recovery Environment appear similar, but are truncated since user profiles are not loaded.

? Alerts That May Appear in the Header:

? Boot Problems:

? "ATTENTION: Could not load system hive" – This indicates a missing system hive.

? Solution: Try restoring the hive using LastRegBack:.

? Control Set Information:

? "Default: Controlset001" – Indicates which Control Set (CS) is the default.

? Why is this important?

- Normally, you don't need this info.

- But if you need to modify the CS that will be loaded at boot, this helps identify the correct CS.

- Changes to other Control Sets will have no effect on the system.

? Processes

? Process Listing Example

Quote:(cmd.exe ->) (Microsoft Windows -> Microsoft Corporation)

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

(Mozilla Corporation -> Mozilla Corporation) C:\Program Files\Mozilla Firefox\firefox.exe <8>

? Explanation of Process Notation:

- (parent process ->) Indicates the process that launched another process.

- <number> Indicates multiple instances of the same process.

? When to Stop a Process

? Stopping a Legitimate Process

- If a process interferes with fixing malware, it can be terminated safely.

? Stopping a Malicious Process

- If a process is malicious, stop it before removing its associated files or folders.

? How to Stop a Process Using FRST

? Include the process lines from FRST logs in your fixlist.

? Fixlog.txt will generate a confirmation message:

Quote:Process name => Process closed successfully

? If the process is malicious, also include the associated file/folder for removal.

? Registry Fixing

? How FRST Handles Registry Entries

- ? Registry entries (keys or values) included in the fixlist.txt will be deleted or restored by FRST.
- ? If a registry key/value resists deletion, FRST will attempt removal after reboot.
- ? Keys protected by a kernel driver will remain until the driver is removed.

? Actions Performed on Registry Entries

- ? FRST can either restore default values or delete entries.
- ? FRST automatically restores important Windows values, such as:
 - BootExecute
 - Winlogon (Userinit, Shell, System)
 - LSA
 - Applnit_DLLs (only removes bad paths, not the entire value).

? FRST does not remove files executed by registry keys! If a registry key loads a file, list the file separately for removal.

? Example: Removing a Malicious Run Entry

To remove both the registry key and its associated file, include them in the fixlist:

```
Quote:HKLM\...\RunOnce: [LT1] => C:\WINDOWS\TEMP\gA652.tmp.exe [216064 2019-04-13] ()  
[File not signed] <==== ATTENTION  
C:\WINDOWS\TEMP\gA652.tmp.exe
```

- ? First line: Removes the registry entry.
- ? Second line: Deletes the file.

? Removing Startup Entries

FRST detects Startup folder shortcuts and their target executables.
To remove both the shortcut and its target file, include both in the fixlist.

Example:

```
Quote:Startup: C:\Users\User\AppData\Roaming\Microsoft\Windows\Start  
Menu\Programs\Startup\helper.lnk [2019-03-25]  
ShortcutTarget: helper.lnk -> C:\Users\User\AppData\Roaming\WindowsServices\helper.vbs () [File  
not signed]
```

- ? First line removes the shortcut.
- ? Second line removes the executable.

? If you only remove the executable, the shortcut remains and will cause an error at startup.

? Handling Security Policy Restrictions

FRST detects Software Restriction Policies (SRP) and Untrusted Certificates that may be abused by malware.

? Example: Removing a Blocked Security Program

Quote:HKLM\ DisallowedCertificates: AD4C5429E10F4FF6C01840C20ABA344D7401209F (Avast Antivirus/Software) <==== ATTENTION

? Example: Removing a Group Policy Restriction

Quote:HKLM Group Policy restriction on software: C:\Program Files\AVAST Software <===== ATTENTION

? To unblock security programs, include these entries in the fixlist.

? Note: Some legitimate security policies may also be flagged. Review before removal!

Tha Sneak - March 3, 2025, 8:22 pm

? Group Policy Fixing

FRST detects Group Policy Objects (GPOs), including policies that restrict browsers or Windows Defender.

? Example: Resetting Group Policies

Quote:GroupPolicy: Restriction - Windows Defender <===== ATTENTION

GroupPolicyScripts: Restriction <===== ATTENTION

? To reset policies, include these lines in the fixlist.

? FRST will prune GroupPolicy folders and require a reboot.

? Example: Successful Reset Confirmation

Quote:C:\Windows\system32\GroupPolicy\Machine => moved successfully

C:\Windows\system32\GroupPolicy\GPT.ini => moved successfully

? Note: Legitimate Group Policies configured via gpedit.msc may also be flagged.

? Scheduled Tasks

? Fixing Scheduled Tasks

? When an entry is included in the fixlist, the task itself is fixed.

? FRST removes the registry entries and moves the task file.

? FRST does NOT remove the executable associated with the task. (It must be added separately for removal.)

? Example: Removing a Malicious Scheduled Task

Quote:Task: {A0DC62F9-8007-4B9C-AAA2-0AB779246E27} - System32\Tasks\csrss =>
C:\Windows\rss\csrss.exe [4925952 2019-03-19] () [File not signed] <==== ATTENTION

? What Happens When You Include It in Fixlist?

Quote:"HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Schedule\TaskCache\Plain\{A0DC62F9-8007-4B9C-AAA2-0AB779246E27}" =>
removed successfully
"HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Schedule\TaskCache\Tasks\{A0DC62F9-8007-4B9C-AAA2-0AB779246E27}" =>
removed successfully
C:\Windows\System32\Tasks\csrss => moved successfully
"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\csrss" =>
removed successfully

? Important Notes:

? FRST only removes the registry task entries and moves the task file.

? It does NOT remove the executable! (Example: csrss.exe must be listed separately for deletion.)

? Checking Executables Before Deletion

? Malware can abuse legitimate Windows executables to run malicious tasks.

? Example: Using sc.exe to create and run malicious services.

? Always verify the executable's legitimacy before removing it!

? Example of a Safe Fixlist Entry for Full Removal

Quote:Task: {A0DC62F9-8007-4B9C-AAA2-0AB779246E27} - System32\Tasks\csrss =>
C:\Windows\rss\csrss.exe [4925952 2019-03-19] () [File not signed] <==== ATTENTION
C:\Windows\rss\csrss.exe

? First line: Removes the scheduled task from the registry.

? Second line: Removes the malicious executable.

? What Should NOT Be Included in Fixlist?

? Do NOT include the following in the fixlist:

Quote:"{Random GUID}" => key was unlocked. <==== ATTENTION

? What Does This Mean?

? FRST detected broken permissions and automatically fixed them during the scan.

? A new FRST log should be taken to verify whether the unlocked task is:

- Visible -> Custom task (can be included in fixlist if needed).
- Hidden (Whitelisted) -> Standard Microsoft entry (should NOT be removed).

? Internet

? Fixing Internet-Related Entries

? Most items copied to the fixlist will be removed automatically.

- ? For registry entries involving files/folders, the files/folders must be listed separately to be moved.
- ? Exceptions apply to browser entries. (See details below.)

? Winsock Issues

- ? What Happens When a Catalog5 Entry is Fixed?
- ? If the entry is a hijacked default entry, FRST restores the default.
- ? If the entry is a custom entry, FRST removes it and re-numbers the catalog.

? What About Catalog9 Entries?

- ? Recommended Fix: Use the following command to reset Winsock:
Code cmd: netsh winsock reset
- ? If custom Catalog9 entries remain, they can be manually listed in the fixlist for removal.
- ? FRST will then remove the entries and re-number the catalog.

? Important Warning!

- ? A broken Winsock chain can prevent internet access.
- ? If your internet is not working due to Winsock issues, FRST will report it like this:

Quote:Winsock: -> Catalog5 - Broken internet access due to missing entry. <===== ATTENTION
Winsock: -> Catalog9 - Broken internet access due to missing entry. <===== ATTENTION

? How to Fix:

- ? Include the entries in the fixlist, and FRST will restore them.

? HOSTS File

? Custom HOSTS File Entries

When custom entries exist in the HOSTS file, you'll see the following line in the Internet section of the FRST.txt log:

Quote:Hosts: There are more than one entry in Hosts. See Hosts section of Addition.txt

? Missing HOSTS File

If the HOSTS file is not detected, FRST will generate a log entry stating that it couldn't be found.

? Resetting HOSTS

To reset the HOSTS file, copy and paste the line into the fixlist. After running the fix, Fixlog.txt will confirm the reset.

? TCP/IP and Other Entries

- ? Entries included in the fixlist will be deleted automatically.

? DNS Servers in the Registry (DhcpNameServer and NameServer)

These can be compared with the "DNS servers" section in Addition.txt to determine which configuration is active.

? StartMenuInternet Hijacking

- Default entries are whitelisted.
- If a non-default path appears in the log, further investigation is needed.
- If necessary, adding the entry to the fixlist will restore the default registry entry.

? Extensions Installed Outside Official Repositories

Extensions not installed via official repositories (Chrome Web Store, Firefox Add-ons, Microsoft Edge Addons, Opera Add-ons) will have an update URL detected.

? Microsoft Edge

? Windows 10+ logs both versions of Microsoft Edge:

- Classic Edge: Except for DownloadDir, entries added to the fixlist will be deleted.
- Chromium-based Edge: Follows the same rules as Google Chrome (see details below).

? Mozilla Firefox

? Firefox Entries in FRST Logs

FRST lists Firefox registry keys and profiles (if present) even if Firefox is not installed.

- All profiles are scanned for preferences and extensions.
- Non-standard profiles (e.g., created by adware) are flagged.

? Fixing Firefox Entries

? Everything except FF DefaultProfile and FF DownloadDir can be added to the fixlist for deletion.

? Unsigned Firefox Add-ons Are Flagged

Example:

Quote:FF Extension: (Adblocker for Youtube™) - C:\Program Files\Mozilla Firefox\browser\features\{A5FD4672-4D73-4F90-A1C0-2ABD39DB2565}.xpi [2018-01-18] [not signed]

? Google Chrome

? Chrome Entries in FRST Logs

FRST lists Chrome registry keys and profiles (if present) even if Chrome is not installed.

- All profiles are scanned for preferences and extensions.
- Non-standard profiles (e.g., created by adware) are flagged.

? Chrome Preferences Scan Includes:

- ? Modified HomePage and StartupUrls
- ? Session Restore settings
- ? Custom search provider settings
- ? Allowed notifications

Example:

Quote:CHR HomePage: Default -> hxxp://www.web-pl.com/

CHR StartupUrls: Default -> "hxxp://www.web-pl.com/"

CHR DefaultSearchURL: Default -> hxxp://www.web-pl.com/search?q={searchTerms}

CHR Session Restore: Default -> is enabled.

CHR Notifications: Default -> hxxps://www.speedtestace.co

? Chrome Fixes

? Adding HomePage, StartupUrls, and Notifications entries to the fixlist will remove them.

? Processing other entries may cause a partial Chrome reset.

A user may see the following message on the Chrome settings page:

? "Chrome detected that some of your settings were corrupted by another program and reset them to their original defaults."

? New Tab Redirections

FRST detects New Tab hijacks controlled by extensions.

- Find the matching extension and uninstall it manually via Chrome.

Example:

Quote:CHR NewTab: Default ->

Active:"chrome-extension://algadicmefalojnlclaalabdcjnnmclc/stubby.html"

CHR Extension: (RadioRage) - C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Extensions\algadicmefalojnlclaalabdcjnnmclc [2017-04-07]

? Removing Chrome Extensions

? CHR Extension lines are NOT processed by FRST.

? Use Chrome's built-in tools to remove extensions:

Quote:1 Open Chrome and type: chrome://extensions

2 Press Enter

3 Click Remove under the extension you want to delete

4 Confirm by clicking Remove

? Exception: Extension Installers in the Registry

If an extension is installed via HKLM or HKU, FRST can delete the registry key when included in the fixlist.

? Other Chromium-Based Browsers

? Supported Browsers:

? Brave, Opera, Vivaldi, Yandex Browser

? These browsers follow the same rules as Google Chrome.

? For other browsers not listed in FRST logs:

? Uninstall the browser completely

? Reboot your system

? Reinstall the browser

? Services and Drivers ?

The Services and Drivers are formatted as follows:

Quote: ? RunningState StartType ServiceName; ImagePath or ServiceDll [Size CreationDate]
(SignerName -> CompanyName) [? Signature Verification]

? RunningState - The letter beside the number represents the Running State:

- ? R = Running
- ? S = Stopped
- ? U = Undetermined

? StartType Numbers:

- ? 0 = Boot
- ? 1 = System
- ? 2 = Auto
- ? 3 = Demand
- ? 4 = Disabled
- ? b5 = Assigned by FRST when it is unable to read the start type

? Where you see [X] at the end of a listed entry, it indicates that FRST could not find the files associated with the particular Service or Driver and has listed the ImagePath or ServiceDll as it is in the registry instead.

? Default Microsoft Services Requiring Repair

? Example:

Quote:===== Services (Whitelisted) =====
R2 DcomLaunch; C:\Windows\system32\rpcss.dll [512512 2010-11-20] (Microsoft Corporation) [File not signed]
R2 RpcSs; C:\Windows\system32\rpcss.dll [512512 2010-11-20] (Microsoft Corporation) [File not signed]

In this case, the file needs to be replaced with a good copy. To fix, use the Replace: command.

? Removing a Bad Service or Driver

? Copy the line from the scan log to fixlist. Any associated file should be included separately.

Example:

Quote:R1 94BE3917F6DF; C:\Windows\94BE3917F6DF.sys [619880 2019-03-07]
(????????(??)???? -> VxDriver) <==== ATTENTION
C:\Windows\94BE3917F6DF.sys

The tool closes any service entry included in the fixlist and removes the service key.

? Note: FRST will report success or failure of stopping services that are running. Regardless of whether the service is stopped or not, FRST attempts to delete the service.

? If a running service is deleted, FRST will inform the user about completing the fix and the need to restart. Then FRST will restart the system.

? If a service is not running, FRST will delete it without forcing a restart.

? Exception: Hijacked Themes

Example:

Quote:S2 Themes; C:\Windows\system32\themeservice.dll [44544 2009-07-14] (Microsoft Windows -> Microsoft Corporation) [DependOnService: iThemes5] <==== ATTENTION

? When included in the fixlist, this entry will be restored to the default state.

? Do Not Include This Line in the Fixlist:

Quote:"ServiceName" => service was unlocked. <==== ATTENTION

? This message indicates that FRST detected broken permissions and automatically fixed them during a scan. A new FRST log should be taken to verify the result. If necessary, include the standard service line in the fixlist.

? NetSvcs

? NetSvc entries are listed each on a line, like this:

Quote:NETSVCx32: HpSvc -> C:\Program Files (x86)\LuDaShi\lpi\HpSvc.dll ()

NETSVCx32: WpSvc -> no filepath

? Listing Netsvc only removes the associated value from the registry. The associated service (if present under the Services section) should be listed for deletion separately.

? Example:

To remove the Netsvc value, the associated service in the registry, and the associated DLL file, the full script would look like this:

Quote:S2 HpSvc; C:\Program Files (x86)\LuDaShi\lpi\HpSvc.dll [239016 2016-07-21] (Qihoo 360 Software (Beijing) Company Limited ->) <==== ATTENTION

NETSVCx32: HpSvc -> C:\Program Files (x86)\LuDaShi\lpi\HpSvc.dll ()

C:\Program Files (x86)\LuDaShi

? One Month (Created/Modified)

The "Created" scan reports the file or folder's created date and time followed by the last modified date and time.

The "Modified" scan reports the modified date and time first, followed by the created date and time.

? Size: The number of bytes contained in the file is displayed. A folder will show 00000000 as it has no bytes.

? Scope: The scan is limited to predefined locations to prevent long scan times and large logs.

? Contents: FRST only lists custom folders, not their contents. To list the contents, use Folder: directive.

? Important Notes:

? Digital signatures check is limited to Microsoft executables (whitelisted by default).

? Other digital signatures are not checked.

? Use SigCheckExt for a list of unsigned executables.

? FRST Log Notations:

Code [C] - Compressed

[D] - Directory
[H] - Hidden
[L] - Symbolic Link
[N] - Normal (no special attributes)
[O] - Offline
[R] - Readonly
[S] - System
[T] - Temporary
[X] - No scrub (Windows 8+)

? Removing Files or Folders from the One Month List

Simply copy and paste the entire line into fixlist to remove it.

Symbolic links (L attribute) are handled properly.

Example:

Quote:2018-02-21 21:04 - 2018-02-21 21:04 - 0000000000 ____DL C:\WINDOWS\system32\Link

When added to fixlist, FRST will only delete the link, keeping the target intact:

Quote:Symbolic link found: "C:\WINDOWS\system32\Link" => "C:\Windows\System32\Target"

"C:\WINDOWS\system32\Link" => Symbolic link removed successfully

C:\WINDOWS\system32\Link => moved successfully

? Alternative: Use DeleteJunctionsInDirectory: directive.

? Fixing Files & Folders

To remove other files/folders, list their full path in fixlist (no quotes needed, even for paths with spaces).

? Example:

Code C:\Windows\System32\Drivers\bad.sys

C:\Program Files (x86)\Bad

? Using Wildcards (*) for Multiple Files

Instead of listing files one by one:

Code C:\Windows\Tasks\At1.job

C:\Windows\Tasks\At8.job

C:\Windows\Tasks\At13.job

C:\Windows\Tasks\At52.job You can use:

Code C:\Windows\Tasks\At*.job

? Note: The ? character is ignored for safety reasons and wildcards do not work for folders.

Tha Sneak - March 4, 2025, 2:09 am

? FLock - Locked Files

This section lists locked files and folders in standard directories.

? FCheck - Bad Files

This section detects bad files, such as:

? DLL Hijacking attempts

? Zero-byte executables (.exe and .dll) in standard directories

This section appears only when matching items are found.

? Fixing Bad Files

If an entry appears in fixlist, the file/folder will be moved.

? KnownDLLs

Some items in this section, if missing, patched, or corrupted, could cause boot issues.

? This scan only appears when the tool is run in Recovery Environment (RE) mode.

? Items are whitelisted unless they require attention.

? Caution: Handling these files improperly may cause system instability. It is strongly recommended to seek expert help.

? Replacing a Missing or Corrupt DLL

If a problematic file is found, a good replacement may already exist on the system. Use the FRST Search function to locate it.

Refer to the Directives section for replacement instructions.

? SigCheck - System File Verification

FRST verifies critical system files. If a file is missing or has an invalid digital signature, it will be reported.

? Outside of Recovery Mode, this section is whitelisted unless an issue is detected.

? Modified system files may indicate malware infection.

? Warning: Deleting a system file without replacement could make the system unbootable.

? Example from a Hijacker.DNS.Hosts Infection:

Quote:C:\WINDOWS\system32\dnsapi.dll

[2015-07-10 13:00] - [2015-07-10 13:00] - 0680256____ (Microsoft Corporation)

5BB42439197E4B3585EF0C4CC7411E4E

C:\WINDOWS\SysWOW64\dnsapi.dll

[2015-07-10 13:00] - [2015-07-10 13:00] - 0534064____ (Microsoft Corporation)

4F1AB9478DA2E252F36970BD4E2C643E

? Fix: Replace the file using the Replace: command.

? Safe Mode & Recovery Mode Fixes

? SmartService Infection Detection

Some versions of SmartService malware disable Recovery Mode. FRST automatically restores the BCD setting during a scan:

Quote:BCD (recoveryenabled=No -> recoveryenabled=Yes) <==== restored successfully

? Fixing Safe Mode Boot Loops

If a system is stuck in Safe Mode, users may see this warning:

Quote:safeboot: Minimal ==> The system is configured to boot to Safe Mode <===== ATTENTION

? To fix this issue: Copy and paste the above line into the fixlist.
FRST will reset the system to boot into normal mode.
? Applies to: Windows Vista and later.

? Association - EXE File Associations

The "Association" section appears in FRST.txt when running from Recovery Environment.
Outside of RE, it is logged in Addition.txt.

This scan checks .exe file associations to detect malicious hijacking.

? Example of a Hijacked EXE File Association:

Quote:HKLM\...\exefile\open\command: C:\Windows\svchost.com "%1" %* <===== ATTENTION

? Fix: Copy and paste the entry into fixlist, and FRST will restore the correct association.

? Restore Points

? "Restore Points" appear in FRST.txt when run from Recovery Environment.

? When run outside of RE, they are logged in Addition.txt.

? Windows XP: Hives can be restored using FRST.

? Windows Vista and later: Restore points must be used via Windows System Recovery Options.

? Example from a Windows XP machine:

Quote:RP: -> 2010-10-26 19:51 - 024576

_restore{3216E3D3-FBC5-40AC-B583-63C1B9EE2B6F}\RP83

RP: -> 2010-10-24 13:57 - 024576 _restore{3216E3D3-FBC5-40AC-B583-63C1B9EE2B6F}\RP82

RP: -> 2010-10-21 20:02 - 024576 _restore{3216E3D3-FBC5-40AC-B583-63C1B9EE2B6F}\RP81

? To restore a specific restore point (e.g., RP82):

Copy and paste the following into fixlist:

Code RP: -> 2010-10-24 13:57 - 024576

_restore{3216E3D3-FBC5-40AC-B583-63C1B9EE2B6F}\RP82

? Memory Info

? The Memory info section appears in FRST.txt when running in Recovery Environment (RE).

? Outside of RE, it appears in Addition.txt, containing additional details (BIOS, Motherboard, Processor).

? What It Reports:

? Total RAM installed

? Available physical memory

? Percentage of free memory

? Virtual memory & available virtual memory

? Why is this useful?

- ? Helps diagnose performance issues or hardware problems.
- ? If reported RAM is less than expected, possible reasons include:
 - Faulty RAM module
 - Motherboard slot issues
 - BIOS not recognizing all installed RAM (BIOS update may be required)
- ? 32-bit systems will only report up to 4GB RAM, even if more is installed.

? Drives and MBR & Partition Table

? The Drives and MBR & Partition Table sections appear in FRST.txt when running in Recovery Environment (RE).

? Outside of RE, they appear in Addition.txt.

? What It Does:

? Lists all fixed and removable drives detected at the time of scan.

? Unmounted volumes are identified by GUID paths.

? Example Output:

Quote:Drive c: (OS) (Fixed) (Total: 223.02 GB) (Free: 173.59 GB) (Model: Force MP500) NTFS

Drive f: (Flash drive) (Removable) (Total: 1.91 GB) (Free: 1.88 GB) FAT32

Drive g: (Recovery) (Fixed) (Total: 0.44 GB) (Free: 0.08 GB) (Model: Force MP500) NTFS

Drive x: (Boot) (Fixed) (Total: 0.5 GB) (Free: 0.49 GB) NTFS

\\?\Volume{74a80af8-ff89-444b-a7a3-09db3d90fd32}\ (Fixed) (Total: 0.09 GB) (Free: 0.07 GB) FAT32

? Partitioning Scheme Detection:

? UEFI/GPT-based partitions:

- Only the basic GPT layout is detected.
- A complete list of partitions is not available.

? Example Output:

Quote:Disk: 0 (Protective MBR) (Size: 223.6 GB) (Disk ID: 00000000)

Partition: GPT.

? BIOS/MBR-based partitions:

- The MBR code and partition entries are detected.
- Logical partitions inside extended partitions are not listed.

? Example Output:

Quote:Disk: 0 (MBR Code: Windows 7/8/10) (Size: 465.8 GB) (Disk ID: 73FD73FD)

Partition 1: (Active) - (Size = 39.1 GB) - (Type = 07 NTFS)

Partition 2: (Not Active) - (Size = 426.7 GB) - (Type = 0F Extended)

? Checking for MBR Issues:

If an issue is detected with the MBR, you may need to perform an MBR dump.

? To obtain an MBR dump, run this command in FRST:

Code SaveMbr: drive=0 (or appropriate drive number)

? This will generate MBRDUMP.txt in the same location as FRST/FRST64.

? Important:

- Some MBR infections can forge the MBR while Windows is running.
- It is recommended to run this in Recovery Environment (RE).

? LastRegBack - Last Registry Backup

FRST scans the system and lists the last registry backup created by Windows.

This backup contains all registry hives and is different from Last Known Good Configuration (LKGC).

? When to Use It?

- ? If registry corruption or loss has occurred.
- ? If FRST cannot load the system hive, you may see this error:

? Example Output:

Quote:ATTENTION: Could not load system hive.

? How to Restore the Last Registry Backup:

Include the following line in fixlist:

Code LastRegBack: >>date<< >>time<<

? Example:

Code LastRegBack: 2013-07-02 15:09

? Additional Scan Header & Malware Removal Analysis

ThenAdditional Scan Header contains a brief summary of system information relevant to malware analysis. Below is an example of how it appears:

? Example Header:

Quote:Additional scan result of Farbar Recovery Scan Tool (x64) Version: 20-10-2017

Ran by User (21-10-2017 14:16:13)

Running from C:\Users\User\Desktop

Windows 10 Pro Version 1709 16299.19 (X64) (2017-10-17 23:06:22)

Boot Mode: Normal

? How to Interpret the Header:

- ? First line: Indicates whether the FRST 32-bit or 64-bit version was used, along with the version number.
- ? Second line: Displays the user who ran the tool and the exact date/time of execution.
- ? Third line: Shows the directory from which FRST was run.
- ? Fourth line: Lists the Windows version and installation date.
- ? Fifth line: Identifies whether the scan was performed in Normal Mode or Safe Mode.

? Accounts Section

This section lists standard accounts on the system in the following format:

? Local Account Name (SID - Privileges - Enabled/Disabled) => Profile Path

? Malicious accounts can be flagged for removal.

Example:

Quote:WgaUtilAcc (S-1-5-21-1858304819-142153404-3944803098-1002 - Administrator - Enabled)
=> removed successfully

? Only the account itself is removed. The corresponding user folder in the Users directory must be deleted manually.

? Security Center Entries

Sometimes, the scan will detect leftover entries from previously uninstalled security software. These entries can be removed using a fixlist. However, if the software is still partially installed, you may see this message in the Fixlog:

Quote:Security Center Entry => The item is protected. Make sure the software is uninstalled and its services are removed.

? If removal fails, manually uninstall the security software before proceeding.

? Installed Programs

Lists all installed software, including classic desktop applications and Windows 10/11 UWP apps.

? Pre-installed Microsoft applications are whitelisted.

? Ad-supported applications are flagged with [MS Ad].

? Potentially unwanted programs (PUPs) are identified for removal.

Example:

Quote:App Radio -> C:\Program
Files\WindowsApps\34628NielsCup.AppRadio_9.1.40.6_x64__kz2v1f325crd8 [2019-06-04] (Niels
Cup) [MS Ad]

? Startup applications will be marked as [Startup Task].

? Adware programs are recommended for manual removal before using automated tools.

? Suspicious Registry Entries & ContextMenu Handlers

Malicious registry keys and shell extensions can be listed in ContextMenuHandlers or CLSID custom classes.

Example:

Quote:ContextMenuHandlers1: [SystemHelper] -> {851aab5c-2010-4157-9c5d-a28dfa7b2660} =>
C:\Windows\ExplorerPlug.dll [2018-03-03] (Unknown Publisher) [File not signed]

? If flagged as malicious, these entries can be removed via a fixlist.

? Legitimate third-party software may also create CLSID entries, so research carefully before deletion.

? Alternate Data Streams (ADS)

FRST detects hidden Alternate Data Streams, often used by malware to store malicious executables.

Example Output:

```
Quote:===== Alternate Data Streams (whitelisted) =====  
AlternateDataStreams: C:\Windows\System32\legitfile:malware.exe [134]  
AlternateDataStreams: C:\malware:malware.exe [134]
```

? If the ADS is attached to a legitimate file, only the ADS should be removed.

? If attached to a malicious file, the entire file should be deleted.

Tha Sneak - March 4, 2025, 2:09 am

? Startup & WMI Hijacks

FRST detects hijacked startup items and WMI (Windows Management Instrumentation) abuse, often used by malware to persist after reboot.

Example of WMI-Based Malware:

Quote:

```
WMI:subscription\__FilterToConsumerBinding->CommandLineEventConsumer.Name="****youmm4  
",Filter="__EventFilter.Name="****youmm3"" <==== ATTENTION  
WMI:subscription\__EventFilter->****youmm3:.[Query => SELECT * FROM  
__InstanceModificationEvent WITHIN 10800 WHERE TargetInstance ISA  
'Win32_PerfFormattedData_PerfOS_System'] <==== ATTENTION
```

? Malicious WMI entries can be removed with a fixlist.

? OEM software (such as Dell utilities) may also create custom WMI registrations—research unknown entries before removal.

? Malicious Wallpapers (Crypto Ransomware Tactics)

Ransomware sometimes replaces the desktop wallpaper with a ransom note. FRST detects such changes.

Example:

```
Quote:HKU\S-1-5-21-2507207478-166344414-3466567977-1001\Control  
Panel\Desktop\Wallpaper -> C:\Documents and Settings\User\My  
Documents\!Decrypt-All-Files.bmp
```

? The wallpaper entry should be removed, and the user should manually reset their background.

? Suspicious DNS Hijacks

FRST lists the currently used DNS servers to detect hijacked network settings.

Example Output:

Quote:DNS Servers: 213.46.228.196 - 62.179.104.196

? Use [Whois Lookup](<https://whois.domaintools.com/>) to check if these servers are legitimate. If the DNS settings appear compromised, resetting the network adapter is recommended.

? UAC (User Account Control) Settings

? Enabled (Default Setting):

Quote:HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
(ConsentPromptBehaviorAdmin: 5)
(ConsentPromptBehaviorUser: 3)
(EnableLUA: 1)

? Disabled:

Quote:HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
(ConsentPromptBehaviorAdmin: 0)
(ConsentPromptBehaviorUser: 3)
(EnableLUA: 0)

? Note:

- UAC being disabled may be a result of user action or malware activity.
- Before attempting a fix, verify whether the user has intentionally disabled it.

? SmartScreen (Windows 8+)

SmartScreen for Desktop Applications & Files:

Quote:HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
(SmartScreenEnabled: Value Data)

Supported values:

- ? Block | Warn | Off (Windows 10 Version 1703+)
- ? RequireAdmin | Prompt | Off (Older Windows versions)

Example of a missing/default value (Windows 10 Version 1703+):

Quote:HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
(SmartScreenEnabled:)

? Telephony Service Providers (TSP)

Default and some legitimate third-party entries are whitelisted. Custom entries are flagged.

Example of a Custom TSP Entry:

Quote:HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Telephony\Providers
ProviderFileName3 -> C:\Windows\system32\unknown.tsp (Publisher)

? Fixing Malicious/Broken TSP Entries:

- Manually remove the matching ProviderIDx and ProviderFileNameex entries.

- Renumber the remaining entries accordingly.

? BITS (Background Intelligent Transfer Service)

Lists BITS jobs using a notification command line.

? Reference: [Attacker Use of Windows BITS](#)

Example Output:

Quote:BITS: {Job ID} - (Job Name) -> [NotifyCmdLine: Command] [files:Remote Path -> Local Path]

? To remove all BITS jobs:

Use the EmptyTemp: directive.

? Windows Firewall

Example:

Quote:Windows Firewall is enabled.

? If Windows Firewall is enabled, it's reported in the scan.

? If disabled, this may indicate user modification or malware interference.

? If running FRST in Safe Mode, Firewall status may not be reported.

? Network Binding (Windows 8+)

Lists network adapters and non-standard components attached to them.

Compare the Drivers section to find matching elements.

Example:

Quote:inspect: COMODO Internet Security Firewall Driver

Quote:R1 inspect; C:\Windows\system32\DRIVERS\inspect.sys

[129208 2019-10-16] (Comodo Security Solutions, Inc. -> COMODO)

? If a program uninstall fails to remove these items:

- Network binding must be removed first before fixing the driver.

- Follow steps in [ESET Knowledgebase](#).

? Note:

Make sure the network binding is removed first before including the driver in a fixlist.

Removing a driver without unbinding it first may break network connectivity.

? MSCONFIG & Task Manager Disabled Items

This section is useful when users have disabled malware entries via MSCONFIG or Task Manager instead of properly removing them.

Additionally, some users disable too many services, preventing essential programs from functioning correctly.

? MSCONFIG (Windows 7 & Older)

Example Output:

Quote:MSCONFIG\Services: Quotenamron => 2

MSCONFIG\startupfolder: C:\Users\User\AppData\Roaming\Microsoft\Windows\Start

Menu\Programs\Startup\339bc1.lnk => C:\Windows\pss\339bc1.lnk.Startup

MSCONFIG\startupreg: AdAnti => C:\Program Files (x86)\AdAnti\AdAnti.exe /S

? Disabled Services:

MSCONFIG\Services: ServiceName => Original Start Type

? Disabled Items in Startup Folder:

MSCONFIG\startupfolder: Original Path => Path to Windows Backup

? Disabled Run Entries:

MSCONFIG\startupreg: ValueName => Path to File

? Task Manager (Windows 8 & Newer)

In Windows 8 and newer, MSCONFIG is used only for services, while startup items are handled by Task Manager.

Disabled items are stored in different registry keys.

Example Output:

Quote:HKLM\...\StartupApproved\Run32: => "win_en_77"

HKU\S-1-5-21-2411900937-544243709-2355068264-1001\...\StartupApproved\StartupFolder: => "SmartWeb.lnk"

HKU\S-1-5-21-2411900937-544243709-2355068264-1001\...\StartupApproved\Run: => "svchost0"

? How FRST Handles These Entries:

? Disabled Services -> FRST deletes both the MSCONFIG key & the service itself.

? Disabled Run Items -> FRST removes registry values from MSCONFIG & Task Manager.

? Startup Folder Items -> FRST deletes the entry & moves the backup file (Windows 7) or removes the file (Windows 8+).

? Important:

Fix entries from this section only if you are certain they are malware-related!

If a legitimate program was disabled, the user should re-enable it via MSCONFIG or Task Manager.

? Windows Firewall Rules

FRST lists Firewall Rules, Authorized Applications, and Globally Open Ports.

Example (Windows 10):

Quote:FirewallRules: [{E3D59A00-E41A-4AE5-AECF-E7AC117FBF83}] => (Allow) C:\Program Files (x86)\Firefox\bin\FirefoxUpdate.exe

FirewallRules: [{7FEA26C4-3ECE-4431-8FA1-E9AFE7F3B0DD}] => (Allow) C:\Program Files

(x86)\Firefox\Firefox.exe

Example (Windows XP):

Quote:StandardProfile\AuthorizedApplications: [C:\Program Files\Firefox\bin\FirefoxUpdate.exe] =>

Enabled: Update Service

StandardProfile\AuthorizedApplications: [C:\Program Files\Firefox\Firefox.exe] => Enabled: Firefox browser

StandardProfile\GloballyOpenPorts: [2900:TCP] => Enabled: ztdtqnhh

? If an entry is included in the fixlist, it will be removed from the registry.

? FRST does NOT remove the actual file, only the registry rule.

? Restore Points

FRST lists available Restore Points as follows:

Example Output:

Quote:18-04-2016 14:39:58 Windows Update

18-04-2016 22:04:49 Restore Point Created by FRST

If System Restore is disabled, FRST will indicate it:

Quote:? ATTENTION: System Restore is disabled (Total: 59.04 GB) (Free: 43.19 GB) (73%)

? System Restore Disabled via Group Policy will be reported under the Registry section in FRST.txt.

? Use CreateRestorePoint: and SystemRestore: directives to enable it.

Tha Sneak - March 4, 2025, 2:10 am

? Faulty Device Manager Entries

FRST detects broken or misconfigured devices in Device Manager.

Example:

Quote:Name: bsdriver

Description: bsdriver

Class Guid: {8ECC055D-047F-11D1-A537-0000F8753ED1}

Manufacturer:

Service: bsdriver

Problem: This device is not present, is not working properly, or does not have all its drivers installed. (Code 24)

Resolution: The device is installed incorrectly. The problem could be a hardware failure, or a new driver might be needed.

? Solution: Remove the device from Device Manager & reinstall drivers if necessary.

? Event Log Errors

FRST detects the following event log errors:

- ? Application Errors
- ? System Errors
- ? CodeIntegrity Errors
- ? Windows Defender Warnings

? MBR & Partition Table

FRST scans the Master Boot Record (MBR) and Partition Table for anomalies.

- ? A corrupt MBR can cause boot failures, and FRST can help diagnose these issues.

? Search Features

? Search Files:

Use the Search Files button to scan for specific files. Wildcards (*) are allowed.

Example searches:

Code malware.exe;virus.dll

.bat;.vbs

? Search Registry:

Use the Search Registry button to find specific registry keys or values.

- ? Avoid using wildcards (* or ?) as they will be interpreted literally.

Example searches:

Code Run;WindowsUpdate

? Find Folder:

This feature can search for specific folders.

? SearchAll:

Finds both files and registry entries matching your search term.

? FindFolder & SearchAll Directives

These directives allow searching for folders or performing a full system-wide search for files, folders, and registry entries.

? FindFolder:

To search for folders on the system drive, enter the following syntax in the Search box and press "Search Files":

Code FindFolder: term;term

? Wildcards are supported:

Code FindFolder: *term*;term*

? SearchAll:

To search for files, folders, and registry entries at once, use:

Code SearchAll: term;term

? Do NOT add wildcards — FRST automatically searches as term for files and folders.

? In Recovery Environment (RE), SearchAll: is limited to files and folders only.

? Directives & Commands

? FRST processes scripts line by line.

? All commands should be on a single line.

? Quick Reference (Directives/Commands)

? Case-insensitive

? Applicable modes:

- (N) = Normal Mode

- (S) = Safe Mode

- (RE) = Recovery Environment

? For Normal Mode only:

Code CreateRestorePoint:

SystemRestore:

TasksDetails:

? For Normal Mode & Safe Mode:

Code CloseProcesses:

EmptyEventLogs:

EmptyTemp:

Powershell:

Reboot:

RemoveProxy:

StartPowershell: — EndPowershell:

Virusscan:

Zip:

? For Normal Mode, Safe Mode, & RE:

Code cmd:

Comment:

Copy:

CreateDummy:

DeleteJunctionsInDirectory:

DeleteKey:

DeleteValue:

DeleteQuarantine:

DisableService:

ExportKey:

ExportValue:

File:

FilesInDirectory:

Folder:

FindFolder:

Hosts:

ListPermissions:

Move:

Reg:
RemoveDirectory:
Replace:
RestoreQuarantine:
SaveMbr:
SetDefaultFilePermissions:
StartBatch: — EndBatch:
StartRegedit: — EndRegedit:
Symlink:
testsigning on:
Unlock:
? For Recovery Environment (RE) only:
Code LastRegBack:
RestoreFromBackup:
RestoreMbr:

? Usage Examples

? CloseProcesses:

This directive closes all non-essential processes, speeding up malware removal.

? This directive automatically triggers a reboot—no need to use Reboot:.

? CMD:

To execute Command Prompt commands, use the CMD: directive.

? Example Syntax:

Quote:CMD: command_here

? Example - Copy Minidump files to a USB drive (E:)

Code CMD: copy /y C:\Windows\Minidump*.dmp E:\

CMD: bootrec /FixMbr? The first command copies minidump files.

? The second command repairs the MBR (Windows Vista & newer).

? Alternative: Use StartBatch: — EndBatch: instead.

? Comment:

Adds notes to explain Fixlist actions.

? Example:

Quote:Comment: The following command will remove all network proxies

RemoveProxy:

? Copy:

Copies files or folders (similar to xcopy).

? Syntax:

Quote:Copy: source_path destination_path

? Example - Backup Edge browser data:

Code Copy:

C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\DataStore\Data\nouser1\120712-0049\DBStore\spartan.edb

C:\Users\User\Desktop\EdgeBackup

? Example - Copy Minidump folder to drive F:

Code Copy: C:\Windows\Minidump F:\

? For replacing files, use Replace: instead of Copy:.

? Replace: Unlocks, moves to quarantine, and replaces the file.

? CreateDummy Directive

Creates a locked dummy folder to prevent the restoration of a malicious file/folder.

? Remove the dummy folder after malware neutralization.

? Syntax:

Code CreateDummy: path

? Example Usage:

Code CreateDummy: C:\Windows\System32\bad.exe

CreateDummy: C:\ProgramData\Bad

? CreateRestorePoint:

Creates a system restore point.

? Note:

- Works only in Normal Mode.

- Automatically enables System Restore—no need to use SystemRestore: On.

? DeleteJunctionsInDirectory:

Removes junctions (symbolic links) within a directory.

? Syntax:

Code DeleteJunctionsInDirectory: path

? Example Usage:

Code DeleteJunctionsInDirectory: C:\Program Files\Windows Defender

? DeleteKey & DeleteValue Directives

? Bypasses deletion restrictions of Reg: and StartRegedit: directives.

? 1. Delete a Registry Key:

Code DeleteKey: key_path

? 2. Delete a Registry Value:

Code DeleteValue: key_path|value_name

? Examples:

Code DeleteKey: HKLM\SOFTWARE\Microleaves

DeleteValue: HKEY_CURRENT_USER\Environment|SNF

DeleteValue:

HKU\S-1-5-21-3145329596-257967906-3285628945-1000\Software\Clients\StartMenuInternet[-HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application\Dataup]

? Advanced Deletion:

- Can remove locked registry keys/values.
- Bypasses permission restrictions & symbolic link issues.
- Does NOT require Unlock:.

? If the key is protected by active software, use Safe Mode or remove the software first.

? DeleteQuarantine:

Deletes the C:\FRST\Quarantine folder if malware files are locked.

? Note:

- Some manual deletions fail due to locked files.
- Use this command after completing malware removal.

Tha Sneak - March 4, 2025, 2:54 am

? DisableService:

Disables a Windows service or driver service.

? Syntax:

Code DisableService: ServiceName

? Example Usage:

Code DisableService: sptd

DisableService: VMware Nat Service

? FRST will set the service to "Disabled", preventing execution at next boot.

? Service name must match its registry entry. No quotes needed.

? EmptyEventLogs:

Clears Windows Event Logs.

? Total logs cleared and errors will be displayed.

? EmptyTemp:

Removes temporary files from various locations:

? Deleted Items: Windows Temp

User Temp folders

Browser caches, cookies, history (except Firefox clones)

Recently opened files cache

Discord cache

Java cache

Steam HTML cache

Explorer thumbnail & icon cache

BITS transfer queue

WinHTTP AutoProxy cache

DNS cache

Recycle Bin

? Auto-Reboot Required – no need for Reboot:.

? ? Warning: Files are permanently deleted (not moved to Quarantine).

? Disabled in Recovery Mode to prevent accidental data loss.

? ExportKey & ExportValue:

Extracts registry information for analysis.

? Syntax:

Code ExportKey: key_path

ExportValue: key_path

? Example Usage:

Code ExportKey: HKEY_LOCAL_MACHINE\SOFTWARE\SuspiciousKey

? Output Example:

Quote:===== ExportKey: =====

[HKEY_LOCAL_MACHINE\SOFTWARE\SuspiciousKey]

[HKEY_LOCAL_MACHINE\SOFTWARE\SuspiciousKey\InvalidKey]

"Hidden Value"="Hidden Data"

[HKEY_LOCAL_MACHINE\SOFTWARE\SuspiciousKey\LockedKey]

HKEY_LOCAL_MACHINE\SOFTWARE\SuspiciousKey\LockedKey => Access Denied.

=== End of ExportKey ===

? Note:

- For research only—NOT a backup or restore function.

? File Directive

Checks file properties, including metadata, MD5 checksum, and digital signature.

? Syntax:

Code File: path;path

? Example Usage:

Code File: C:\Users\User\Desktop\amtemu.v0.9.1-painter.exe

? Output Example:

Quote:===== File: C:\Users\User\Desktop\amtemu.v0.9.1-painter.exe

=====

C:\Users\User\Desktop\amtemu.v0.9.1-painter.exe
? File not signed
? MD5: A209B88B9B2CF7339BE0AC5126417875
? Creation & Modification Date: 2024-03-09 12:20 - 2017-04-10 11:44
? Size: 002546176
? Attributes: ----A
? Company Name: Painter
? Internal Name: ProxyEmu
? Original Name: emuext.exe
? Product: ProxyEmu
? Description: ProxyEmu
? File Version: 0.9.1.0
? Product Version: 0.9.1.0
? Copyright: Painter
? Virus Scan: [? Jotti Scan](#)
===== End of File: =====

? Note: The digital signature check is not available in the Recovery Environment.

? FilesInDirectory & Folder Directives

These directives list file contents within a directory.

- FilesInDirectory: Lists specific files matching wildcard patterns (*.exe, *.dll).
- Folder: Lists all files within a folder recursively (including subdirectories).

? Syntax:

Code FilesInDirectory: path\pattern;pattern

Code Folder: path

? Example Usage:

Code FilesInDirectory: C:\Windows\desktop-7ec3qg0*.exe;*.dll

Folder: C:\Windows\desktop-7ec3qg0

? Warning: Folder: is recursive, and may generate very large logs.

? FindFolder Directive

Similar to Search features, but results are recorded in Fixlog.txt.

For details, see the [Other Optional Scans](

<https://www.bleepingcomputer.com/forums/t/781976/frst-tutorial-how-to-use-farbar-recovery-scan-to-ol/#entry5468083>) section.

? Hosts Directive

Resets the Windows hosts file.

See Main scan (FRST.txt) for more details.

? ListPermissions Directive

Lists permissions for specific files, directories, or registry keys.

? Syntax:

Code ListPermissions: path/key

? Example Usage:

Code ListPermissions: C:\Windows\Explorer.exe

ListPermissions: C:\Users\User\AppData

ListPermissions: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip

ListPermissions: HKLM\SYSTEM\CurrentControlSet\services\afd

? Move Directive

Moves or renames files, useful for handling locked or system-protected files.

? Syntax:

Code Move: source destination

? Example Usage:

Code Move: C:\WINDOWS\system32\drivers\afd.sys C:\WINDOWS\system32\drivers\afd.sys.old

Move: C:\WINDOWS\system32\drivers\atapi.bak C:\WINDOWS\system32\drivers\atapi.sys

? How It Works:

1. If a file exists in the destination, FRST moves it to Quarantine.
2. Then, the source file is moved to the new location.

? Important Notes:

- Renaming is supported within the Move: directive.
- If the destination path is missing, you must include the filename in the destination.

? PowerShell Directive

Executes PowerShell commands or scripts within FRST.

1 Run a Single PowerShell Command

? Syntax:

Code Powershell: command

? Example Usage:

Code Powershell: Get-Service

? Output: Logged in Fixlog.txt.

2 Save PowerShell Output to a File

Use redirection operators (> or Out-File).

? Syntax:

Code Powershell: command > "Path to a text file"

Code Powershell: command | Out-File "Path to a text file"

? Example Usage:

Code Powershell: Get-Service > C:\log.txt

Powershell: Get-Process >> C:\log.txt

? Note: >> appends to a file instead of overwriting it.

? More Info:

- ? [Redirection Operators](#)

- ? [Out-File Cmdlet](#)

3 Run a PowerShell Script File (.ps1)

? Syntax:

Code Powershell: "Path to a script file"

? Example Usage:

Code Powershell: C:\Users\UserName\Desktop\script.ps1

Powershell: "C:\Users\User Name\Desktop\script.ps1"

? Note: Use quotes if the path contains spaces.

4 Run Multiple PowerShell Commands in One Line

Separate commands using a semicolon (;).

? Syntax:

Code Powershell: command1; command2; command3

? Example Usage:

Code Powershell: \$WebClient = New-Object System.Net.WebClient;

\$WebClient.DownloadFile("http://server/file.exe", "C:\Users\User\Desktop\file.exe")

? Alternative: StartPowershell & EndPowershell Directives

For long scripts, use:

Code StartPowershell:

(Commands here)

Code EndPowershell:

? Reboot Directive

Forces a restart after the fixlist execution.

? Syntax:

Code Reboot:

? Note: This only works in Normal & Safe Mode, not in Recovery Mode.

? Reg Directive (Registry Manipulation)

Runs reg command-line operations for modifying the Windows Registry.

? Syntax:

Code Reg: reg command

? Example Usage:

Code Reg: reg add HKLM\SYSTEM\CurrentControlSet\Services\Schedule /v Start /t REG_DWORD /d 0x2 /f

Reg: reg export "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList" C:\Users\User\Desktop\backup.reg

? Important Notes:

? Proper syntax required (use quotes " " for paths with spaces).

? This does not handle locked/invalid keys (see DeleteKey: & DeleteValue: for locked keys).

Tha Sneak - March 4, 2025, 2:54 am

? RemoveDirectory Directive

Forces deletion of stubborn or invalid directories.

? Syntax:

Code RemoveDirectory: path

? Example Usage:

Code RemoveDirectory: C:\ProgramData\BadSoftware

? Note: Works best in Safe Mode or Recovery Mode for stubborn files.

? RemoveProxy Directive

? Removes:

- Internet Explorer policy restrictions
- Proxy settings in HKLM & HKCU
- Manual Proxies & BITSAdmin proxy settings

? Syntax:

Code RemoveProxy:

? Important:

? Proxy settings may return if another program (e.g., malware) re-applies them.

? If persistent, uninstall the responsible software first.

? Replace Directive (Replace System Files)

Moves the destination file to Quarantine and replaces it with the source file.

? Syntax:

Code Replace: source destination

? Example Usage:

Code Replace: C:\WINDOWS\WinSxS\amd64_microsoft-windows-dns-client\dnsapi.dll

C:\WINDOWS\system32\dnsapi.dll

Replace: C:\WINDOWS\WinSxS\wow64_microsoft-windows-dns-client\dnsapi.dll

C:\WINDOWS\SysWOW64\dnsapi.dll

? Key Notes:

- The source file remains in its original location.
- The destination file (if present) is moved to Quarantine before replacement.
- If the destination directory is missing, this command will fail (use Copy: instead).

? RestoreFromBackup Directive

Restores Windows Registry hives from backups created in %SystemDrive%\FRST\Hives (e.g., C:\FRST\Hives).

? Key Notes:

- The first run of FRST creates backups of the System Registry Hives.
- The backup is not overwritten unless it's older than 2 months.
- If issues arise, individual hives can be restored.

? Syntax:

Code RestoreFromBackup: HiveName

? Example Usage:

Code RestoreFromBackup: software

RestoreFromBackup: system

? Restore MBR (RestoreMbr Directive)

This directive restores the Master Boot Record (MBR) from a MBR.bin backup file.

? Requirements:

- MbrFix/MbrFix64 Utility ([? Download](<https://sysint.no/mbrfix/>)).
- A valid MBR.bin backup file.
- Correct drive number.

? Syntax:

Code RestoreMbr: Drive=#

? Example Usage:

Code RestoreMbr: Drive=0

? Important Notes:

? Ensure the MBR.bin file is zipped and attached before execution.

? Restore Quarantine (RestoreQuarantine Directive)

FRST allows restoring quarantined files/folders.

? Restore the Entire Quarantine Folder:

Code RestoreQuarantine:

Code RestoreQuarantine: C:\FRST\Quarantine

? Restore a Specific File/Folder:

Code RestoreQuarantine: PathInQuarantine

? Example Usage:

Code RestoreQuarantine: C:\FRST\Quarantine\C\Program Files\Microsoft Office

RestoreQuarantine: C:\FRST\Quarantine\C\Users\User\Desktop\ANOTB.exe.xBAD

? Find Quarantined Files:

Code Folder: C:\FRST\Quarantine

Code CMD: dir /a/b/s C:\FRST\Quarantine

? Files won't be restored if they already exist at the destination.

? Rename or remove the existing file before restoring.

? Save MBR (SaveMbr Directive)

Creates a backup copy of the Master Boot Record (MBR).

? Syntax:

Code SaveMbr: Drive=#

? Example Usage:

Code SaveMbr: Drive=0

? Key Notes:

- The MBR dump is saved in MBRDUMP.txt on the flash drive.
- Users should attach MBRDUMP.txt when posting for assistance.

? SetDefaultFilePermissions Directive

? Purpose: Unlocks system files/folders by setting Administrators as the owner.

? Note: This does not restore TrustedInstaller as the owner.

? Use case: Helpful for removing malware-locked system files/folders.

? Syntax:

Code SetDefaultFilePermissions: path

? Example Usage:

Code SetDefaultFilePermissions: C:\Windows\System32\drivers\etc\hosts

? StartBatch & EndBatch Directives

? Purpose: Creates and runs a batch file within FRST.

? Output: Redirected to Fixlog.txt.

? Syntax:

Code StartBatch:

Command 1

Command 2

EndBatch:

? Example Usage:

Code StartBatch:

ipconfig /flushdns

net stop wuauserv

EndBatch:

? StartPowershell & EndPowershell Directives

? Purpose: Executes a PowerShell script with multiple lines.

? Alternative to: The Powershell: directive.

? Output: Redirected to Fixlog.txt.

? Syntax:

Code StartPowershell:

Line 1

Line 2

EndPowershell:

? Example Usage:

Code StartPowershell:

Get-Service | Select-Object Name, Status

Stop-Service -Name wuauserv -Force

EndPowershell:

? StartRegedit & EndRegedit Directives

? Purpose: Creates and imports a Registry (.reg) file.

? Output: Confirmation appears in Fixlog.txt.

? Windows Registry Editor Version 5.00 header is optional, but REGEDIT4 is required.

? Syntax:

Code StartRegedit:

Windows Registry Editor Version 5.00

[Registry_Path]

"ValueName"=dword:00000002

EndRegedit:

? Example Usage:

Code StartRegedit:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MpsSvc]

"Start"=dword:00000002

EndRegedit:

? Fixlog Output Example:

Code Registry ==> The operation completed successfully.

? Note: Errors in .reg file syntax won't be detected by FRST.

? Symlink Directive

? Purpose: Lists symbolic links & junctions in a folder.

? Recursive: Yes, it scans all subdirectories.

? Syntax:

Code Symlink: path

? Example Usage:

Code Symlink: C:\Windows

? Note: This operation may take time depending on the folder size.

? SystemRestore Directive

? Purpose: Enables or disables System Restore.

? Prerequisite: Requires sufficient free space to enable.

? Syntax:

Code SystemRestore: On

Code SystemRestore: Off

? Error occurs if the system does not meet the space requirements.

? TasksDetails Directive

? Purpose: Lists additional details about scheduled tasks (execution time, status, schedule).

? Supported OS: Windows Vista+ (Not available in Windows XP).

? Example Output:

Code ===== TasksDetails: =====

UCBrowserUpdater (LastRunTime: NA -> NextRunTime: 2024-10-13 11:32:00 -> Status: Ready ->
Schedule Type: Undefined)

Tha Sneak - March 4, 2025, 2:55 am

? testsigning Directive

? Purpose: Detects non-default test mode activation in Windows boot settings.

? Applies to: Windows Vista and later (Not available on Secure Boot enabled devices).

? Syntax:

Code testsigning: ==> 'testsigning' is set. Check for possible unsigned driver <===== ATTENTION

? Action:

- Check the Drivers section for unsigned drivers.

- If necessary, manually disable test mode.

? Unlock Directive

? Purpose: Unlocks files, directories, or registry keys by granting Administrators, Users, and SYSTEM access.

? Use case: Removing malware-locked files/folders.
? Alternative: Use SetDefaultFilePermissions: for system files.

? Syntax:
Code Unlock: path

? Example Usage:
Code Unlock: C:\Windows\System32\malware.exe

? Note: No need to unlock before deleting:
- Files/Folders -> FRST will reset permissions and move them to Quarantine.
- Registry Keys -> Use the DeleteKey: directive.

? Virusscan Directive
? Purpose: Checks files against Jotti's malware database.
? If not found: The file will be uploaded for analysis.

? Syntax:
Code Virusscan: path;path

? Example Usage:
Code Virusscan: C:\suspicious.exe;C:\Windows\System32\drivers\unknown.sys

? Zip Directive
? Purpose: Compresses files/folders into a .zip archive saved as [Date_Time].zip on the desktop.
? Useful for: Manual uploads or analysis.

? Syntax:
Code Zip: path;path

? Example Usage:
Code Zip: C:\malware.exe;C:\Windows\Minidump;C:\Windows\Logs\CBS\CBS.log

? Note:
- If multiple files have duplicate names, FRST creates separate archives.
- For file replacement, consider using Replace: instead.

Tha Sneak - March 4, 2025, 2:56 am

Clean FRST Log:

FRST Log: <https://www.mediafire.com/file/4paznxe7jrkv23i/FRST.txt/file>

Addition Log: <https://www.mediafire.com/file/ywvot7jhxbywzv4/Addition.txt/file>

Infected FRST Log:

FRST Log: <https://www.mediafire.com/file/ek81eky4lufz1u0/FRST.txt/file>

Addition Log: <https://www.mediafire.com/file/ba3id1pfcgogbsm/Addition.txt/file>