

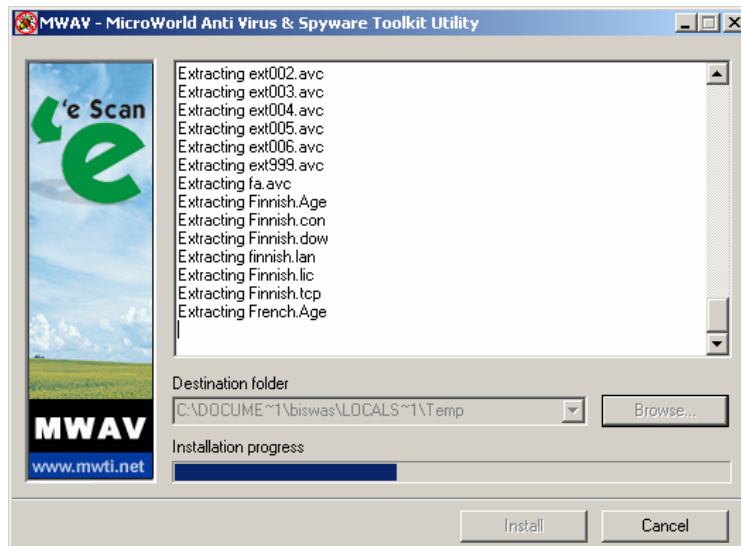
MWAV - User Guide

MWAV is an intelligent and powerful AntiVirus Utility, enabling fast and hassle-free scanning of computers for a range of malwares. The new MWAV comes with the power of detection and disinfection of Viruses, Worms, Rootkits, Trojans, Backdoors and other malice, dramatically improving the system performance and stability. It also detects Spyware and Adware, to clear your system of all harmful and suspicious programs.


Features

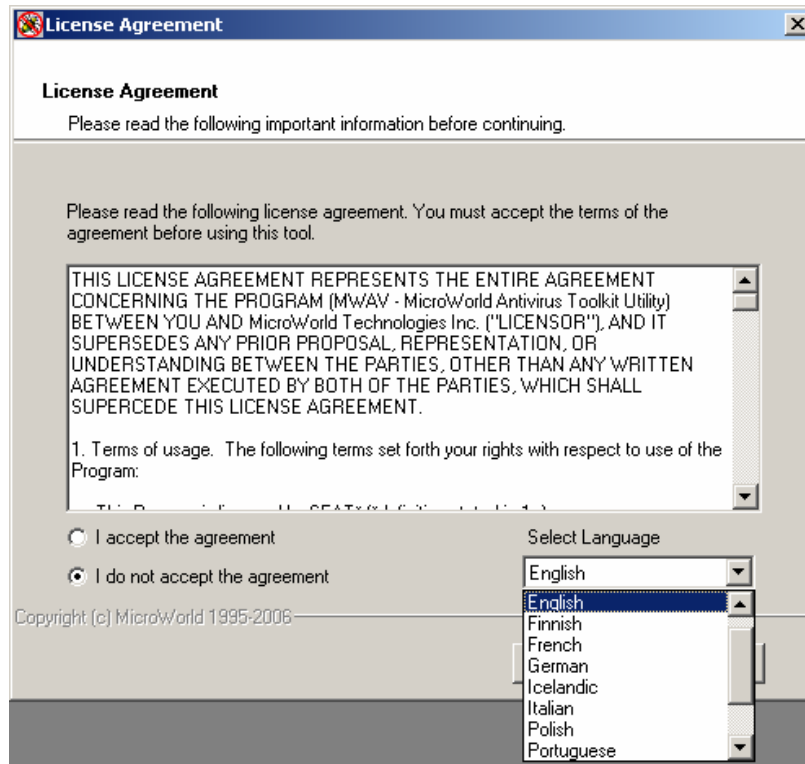
- Scans your computer completely to catch all types of Viruses and Worms.
- Informs you of any background sniffers or tools like spyware, adware, keyloggers etc, running in the memory of your computer.
- You can add this utility to the startup list of programs on your computer so that it scans your computer every time it's started.
- The utility comes with the latest updated list of all viruses in the wild.
- No Installation is required for this utility. Just download and run the MWAV toolkit to scan for viruses.
- MWAV 8.x provides multi-language support.

How to initialize MWAV



1.1 Extracting Files

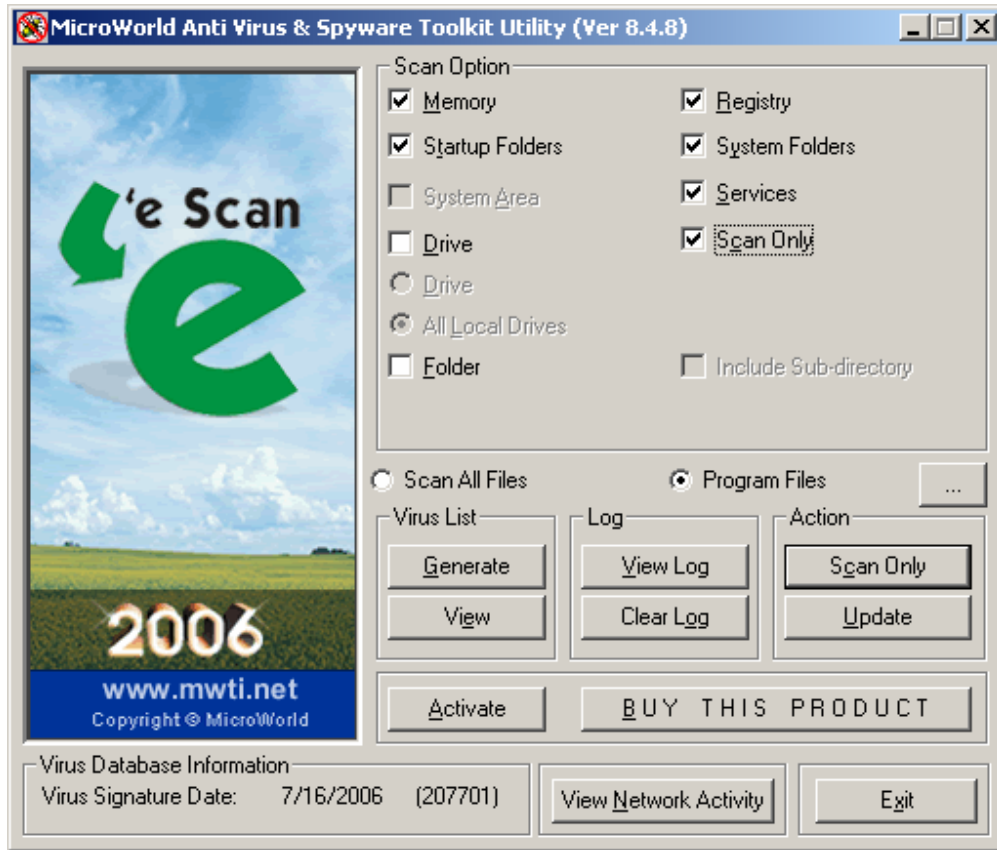
After downloading the MWAV Utility, click on the  icon to launch the program. The process of extracting the files takes a few seconds before it launches the main screen.



1.2 Language Selection

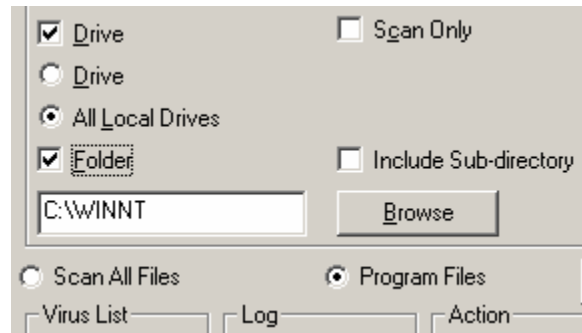
MWAV comes in 12 different languages. They are Chinese, English, Finnish, French, German, Icelandic, Italian, Polish, Portuguese, Romanian, Spanish and Spanish Latin.

How To Perform Virus Scanning



1.3 MWAV Main Screen

At the default level, MWAV scans the **Memory**, **Start-Up Folders**, **Registry**, **System Folder** and **Services**. Any kind of Virus, Worm, Trojan, Backdoor, Rootkit, Spyware, Adware and Keylogger will be detected and removed by MWAV.



1.4 Scan Drives

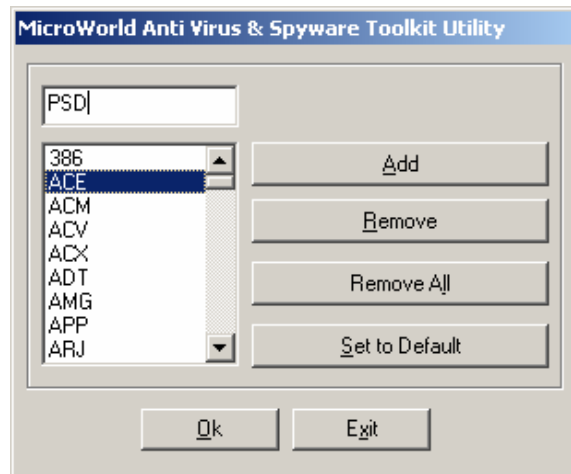
Options are also available for you to scan and clean **Drives** and **Folders** (Fig 1.5). These options can be selected by choosing the 'Drives' and 'Folders' options.

You can select either '**Scan All Files**' or '**Scan Program Files**' option according to the requirement.



1.5 Scan Files

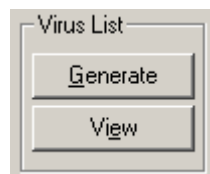
By activating the '**Scan Program Files**' option you can scan for specific file types.



1.6 File Types

Option is available to add new file extensions or remove existing ones from the list. 'Set to Default' option brings the list back to its default levels.

Virus List



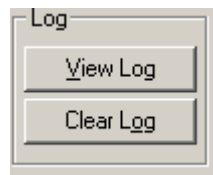
1.7 Virus List

It gives you a comprehensive list of Viruses and Worms that MWAV is updated with.

```
Virus Count: 201751
KL
x86emu
Py2Exe
pfp
Email-worm.BAT.Alcobul.a
Email-worm.BAT.Alcobul.b
Email-worm.BAT.Arica.a
Email-worm.BAT.Baatezu
Email-worm.BAT.Barabat
Email-worm.BAT.Batwin
Email-worm.BAT.Bh.a
Email-worm.BAT.Bong
Email-worm.BAT.Bulbas
Email-worm.BAT.BWG.a
Email-worm.BAT.BWG.b
Email-worm.BAT.BWG.c
Email-worm.BAT.BWG.d
Email-worm.BAT.BWG.e
Email-worm.BAT.BWG.f
Email-worm.BAT.BWG.g
Email-worm.BAT.BWG.h
Email-worm.BAT.BWG.i
Email-worm.BAT.BWG.j
Email-worm.BAT.Calhob
Email-worm.BAT.Cct.a
Email-worm.BAT.CodeFive
Email-worm.BAT.Darf.a
Email-worm.BAT.Darf.b
Email-worm.BAT.Erma.a
Email-worm.BAT.Eversaw
```

1.8 Virus List

Log



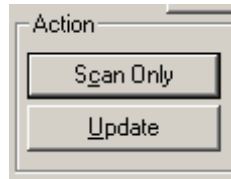
1.9 Log Button

The log gives you detailed description of the scan results. It also provides valuable information on user's computer like;

- MWAV Version Info
- Registration Status
- OS Type
- MWAV Mode
- Date of Virus Database
- Spyware Database Size
- User Account Info
- Windows Fixed Drives
- Options Selected
- Date and Time etc.

Action

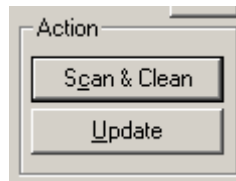
You can choose 'Scan' or 'Scan & Clean' options. While 'Scan' feature simply scans and finds out Viruses & Malwares, the 'Scan & Clean' option removes the same.



2.0 Action Scan

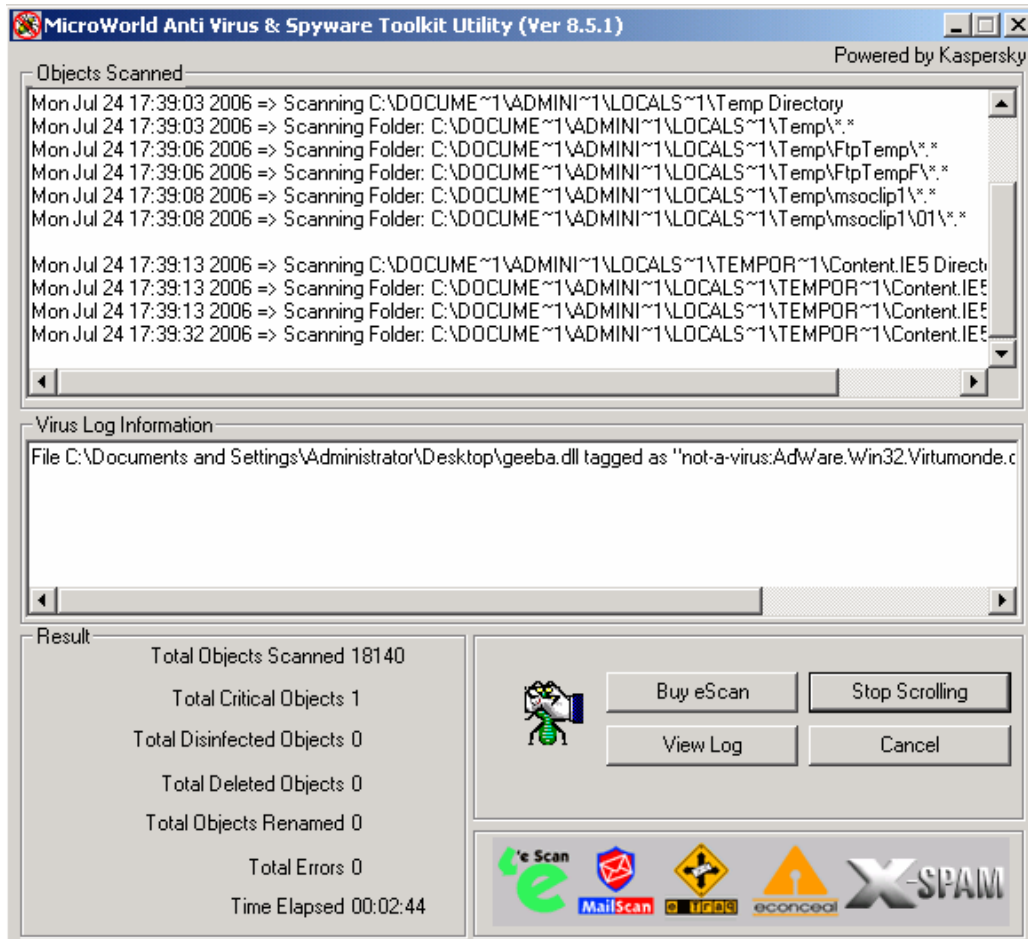
Important: It is strongly recommended to check the 'Scan Only' option initially, as you can view the list of Viruses & Malwares that are found by MWAIV and subsequently you can decide to clean the same.

If you uncheck the 'Scan Only' field, the button will display 'Scan & Clean' option.



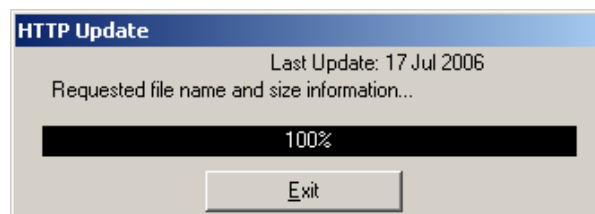
2.1 Scan & Clean

Clicking the 'Scan & Clean' button will activate the process of Scanning and Disinfection.



2.2 Scanning Process

Once you click on the **Update** button, it starts updating new Virus signatures from the Server.



2.3 Signature Update

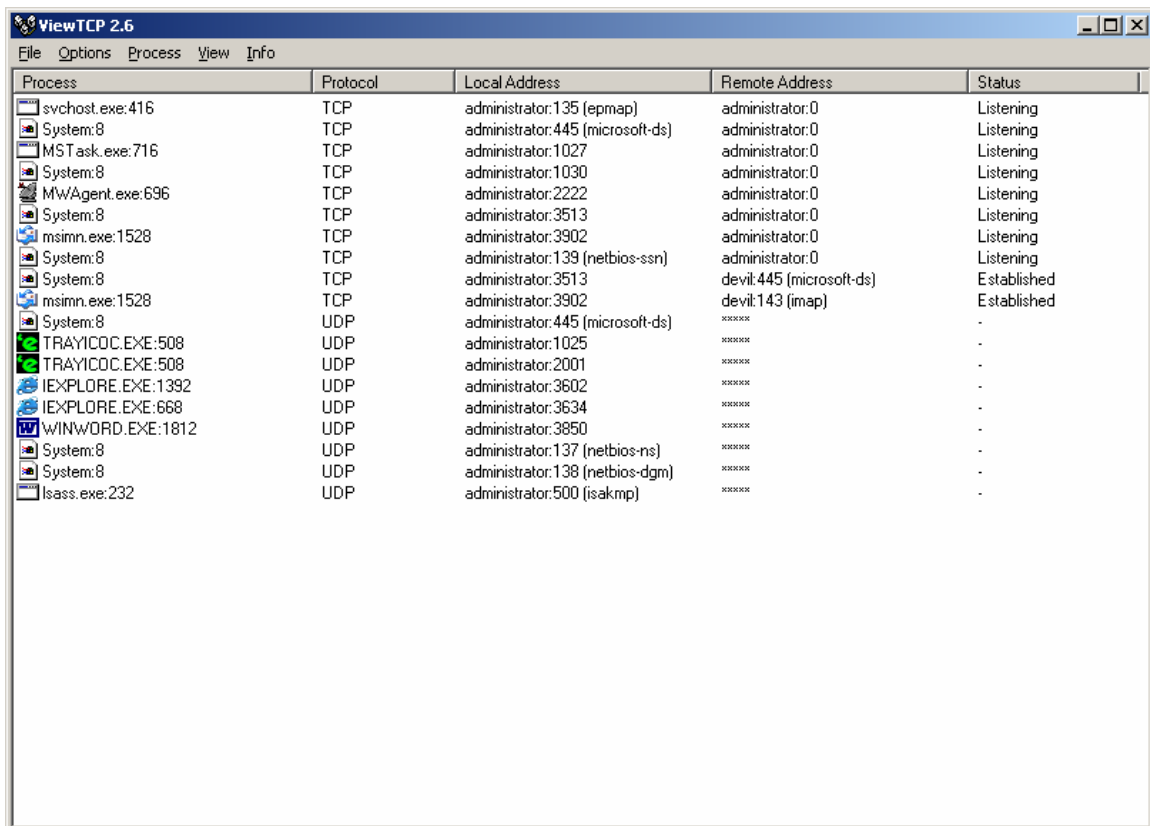
Activate

If you click on the Activate button, a box will be displayed asking you to put the license key.



2.4 Enter Key

TCP View

A screenshot of the "ViewTCP 2.6" application window. The window has a menu bar with "File", "Options", "Process", "View", and "Info". Below the menu bar is a table with five columns: "Process", "Protocol", "Local Address", "Remote Address", and "Status". The table lists various system processes and their network connections. For example, "svchost.exe:416" is shown listening on "administrator:135 (epmap)". Other processes like "System:8" are shown listening on various ports. Some connections are established, such as "devil:445 (microsoft-ds)" and "devil:143 (imap)".

Process	Protocol	Local Address	Remote Address	Status
svchost.exe:416	TCP	administrator:135 (epmap)	administrator:0	Listening
System:8	TCP	administrator:445 (microsoft-ds)	administrator:0	Listening
MSTask.exe:716	TCP	administrator:1027	administrator:0	Listening
System:8	TCP	administrator:1030	administrator:0	Listening
MWAgent.exe:696	TCP	administrator:2222	administrator:0	Listening
System:8	TCP	administrator:3513	administrator:0	Listening
msimn.exe:1528	TCP	administrator:3902	administrator:0	Listening
System:8	TCP	administrator:139 (netbios-ssn)	administrator:0	Listening
System:8	TCP	administrator:3513	devil:445 (microsoft-ds)	Established
msimn.exe:1528	TCP	administrator:3902	devil:143 (imap)	Established
System:8	UDP	administrator:445 (microsoft-ds)	xxxxxx	-
TRAYICOC.EXE:508	UDP	administrator:1025	xxxxxx	-
TRAYICOC.EXE:508	UDP	administrator:2001	xxxxxx	-
IEXPLORE.EXE:1392	UDP	administrator:3602	xxxxxx	-
IEXPLORE.EXE:668	UDP	administrator:3634	xxxxxx	-
WINWORD.EXE:1812	UDP	administrator:3850	xxxxxx	-
System:8	UDP	administrator:137 (netbios-ns)	xxxxxx	-
System:8	UDP	administrator:138 (netbios-dgm)	xxxxxx	-
lsass.exe:232	UDP	administrator:500 (isakmp)	xxxxxx	-

2.5 TCP View

TCP View is an inbuilt Network Monitoring Tool that examines TCP/IP activity on Windows computers. This feature gives you information on all TCP and UDP endpoints on

your PC, including the remote address with domain names and the state of TCP connections.

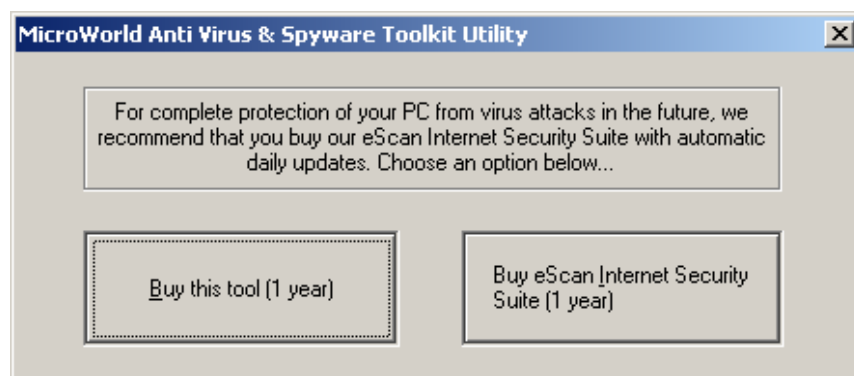
It translates all IP addresses to the respective domain names. TCP Connections will display processes related to each endpoint in Windows NT, 2000 and XP. Default updating Works per second; however you can set timings of your convenience too.

Command Line Scanning

You can also use various commands given below as an alternative to the GUI to perform Virus Scanning.

/MEM	Scan Memory	/FS	Full Silent Mode
/REG	Scan Registry	/NoLog	Do not create logs
/STARTUP	Scan Startup Folder	DELETE_IF_NOT_CLEANABLE	If the Virus infected file is not cleanable, delete it.
/SysFolder	Scan System Folder	/DELETE_ALL_INFECTED	Delete all infected files.
/DRIVE	Scan Local Drives	/LowPriority	Run in low priority.
/SNOC	Scan Only	/NoSelfCheck	Do not perform Self Check
/SC	Scan and Clean	/CheckRegErrors	Check for Registry errors
/WaitToExit	Wait for users to press OK	/riskware	Forcefully delete Riskware tagged as 'not-a-virus:' by MWAV
/s	Silent Mode		

‘BUY THIS PRODUCT’ button gives you directions to buy and license **MWAV**.



2.6 Buy MWAV

Happy Using MWAV!