

The image features a highly expressive and abstract painting of a sailboat. The sailboat is the central focus, rendered with bold, energetic brushstrokes in a variety of colors including red, yellow, white, and black. The sails are full, and the boat is tilted as if catching the wind. The background is a dense, textured composition of warm colors like orange, red, and brown, with swirling and scribbled lines that create a sense of movement and intensity. The overall style is reminiscent of expressive abstract art or digital painting.

**JP** Software

Take Command 9  
Tutorial 3 -- Using Triggers

# Tutorial 3

## Using Triggers In Take Command 9

*Take Command 9 provides a set of 7 "trigger" commands that allow you to monitor activities on your computer and to trigger your computer to take an action based on changes occurring in the computer. This tutorial teaches you how to use them.*

### Overview

Take Command 9.0 features seven new internal commands to allow you to do real-time monitoring of your system. These command are:

- **FOLDERMONITOR** - Monitor folder and/or file creation, modification, and deletion
- **EVENTMONITOR** - Monitor event logs
- **NETMONITOR** - Monitor network connections and execute a command when a network is connected or disconnected
- **PROCESSMONITOR** - monitor processes and execute a command when a process is started or ended
- **SERVICEMONITOR** - monitor Windows services and execute a command when a service is started, paused, or stopped
- **USBMONITOR** - monitor USB connections and execute a command when a device is connected or disconnected
- **FIREWIREMONITOR** - monitor FireWire connections and execute a command when a device is connected or disconnected

Using these commands, you can easily watch most activity going on in your computer and provide alerts, such as emails or take actions, such as triggering a batch process if a monitored event occurs.

You can have up to 100 monitoring commands running simultaneously in a single Take Command 9.0 tab window. The examples below show how simple it is to set up triggers and give you an idea about some of the things you can do with triggers.

### Example 1 -- FOLDERMONITOR

FOLDERMONITOR lets you monitor directory and file creation, deletion, renaming, and modification. Let's say you want to watch for a file called "FinalResult.htm" to be created in the "d:\Results" subdirectory, and then copy it to "<http://mycompany.com/results/FinalResult.htm>"

The traditional approach would be to create a script file that waited forever for the file:

```
(4NT Syntax) FINAL.CMD:
do forever
  iff exist "d:\results\FinalResult.htm" then
    copy "d:\results\FinalResult.htm" "http://mycompany.com/results/FinalResult.htm"
    del FinalResult.htm
    rem Wait for the file again
  endif
  Delay 10
enddo
```

This creates a separate 4NT session, wasting memory and continuously requiring a small amount of CPU time.

In Take Command 9.0 you can do the same thing with (on one line):

```
foldermonitor d:\results /i"FinalResult.htm" created forever
(copy "d:\results\FinalResult.htm" "http://mycompany.com/results/FinalResult.htm" &
del d:\results\FinalResult.htm)
```

Here is what is happening:

1. **Foldermonitor d:\results** -- causes the command to watch the subdirectory d:\results
2. **/i"FinalResult.htm"** -- says to include (watch) only files with the name FinalResult.htm in the monitoring
3. **created forever** -- means that we are looking only for files that are newly created and that we will do this in a continuous loop that will execute forever
4. **(copy "d:\results\FinalResult.htm" "<http://mycompany.com/results/FinalResult.htm>" & del d:\results\FinalResult.htm)** - will copy the new file to a website and deletes the file from the d:\results directory after it has been copied. You could execute a batch file here instead of creating a command group as we have done.

This command creates a separate thread in the current Take Command session.

FOLDERMONITOR also creates four environment variables when a file or folder is created, deleted, modified, or renamed that can be queried by the command. The variables are deleted after the command is executed.

- **\_folderaction** -- The type of change to the file or folder. The possible values are:  
CREATED  
DELETED  
MODIFIED This includes changing the file size, attributes or the date/time stamp.  
RENAMED
- **\_foldername** -- The name of the folder being monitored
- **\_folderfile1** -- The name of the file or folder that was created/deleted/modified/renamed. If the file was renamed, folderfile1 is the old name.
- **\_folderfile2** -- If a file was renamed, folderfile2 is the new name

If you want to test for multiple changes, you should put the condition tests in a single FOLDERMONITOR command; otherwise FOLDERMONITOR will create a thread for each command (wasting your memory and CPU time).

For example, the following command will wait for any file to be created or changed in the d:\results directory and copy them to the web directory:

```
foldermonitor d:\results created modified forever
(copy "%_folderfile1" "http://mycompany.com/results/")
```

## **Example 2 -- PROCESSMONITOR**

PROCESSMONITOR monitors program starts and exits.

For example, if you want to be alerted with an email whenever a particular application exits:

```
processmonitor myapp* ended forever
(sendmail bob@abc.com myapp Myapp just shut down!)
```

Here is what is happening:

1. **processmonitor myapp\*** -- looks for any process with a name beginning with "myapp"
2. **ended forever** -- means that we are looking only for processes that have terminated (for any reason)
3. **(sendmail bob@abc.com myapp Myapp just shut down!)** - creates and sends an email using the internal TC9 Sendmail command to [bob@abc.com](mailto:bob@abc.com) with a subject of "myapp" and message text of ""myapp just shut down"

This is good for making sure that key production processes are operating as expected.

You can also use processmonitor to watch for specific processes being started. Maybe there is a virus that has escaped in your company that executes a malicious process -- call it malproc. The following script will look for the process running on a machine, kill it and send you an email saying its on the machine, so you know where the infection is.

```
processmonitor malproc started forever
(taskend /F malproc & sendmail bob@abc.com malproc I have malproc on my
computer!)
```

This code does the following:

4. **processmonitor malproc** -- looks for any process with a name malproc
5. **started forever** -- means that we are looking only for processes that have just started (for any reason)
6. **(taskend /F malproc & sendmail bob@abc.com malproc I have malproc on my computer)** - uses the TC9 taskend command to force (/F) malproc to terminate immediately and then creates and sends an email using the internal TC9 Sendmail command to [bob@abc.com](mailto:bob@abc.com) with a subject of "malproc" and message text of ""I have malproc on my machine"

The seven new Take Command 9 triggers are exceptionally powerful and flexible commands that give you the ability to monitor and manage your computers like never before.