

About Heap Watch

This utility is used to view *Windows 95* Win32 application heaps and monitor them for memory leaks. The interface has three levels to view the appropriate information. The first level, the Summary-view window, shows a list of the heaps for all of the Win32 applications running in the system at that given time. Next, the Details-view windows, shows all of the memory object in the selected heap. Finally, the Object-view window, show the allocated memory block for the given object. Memory leaks are searched for by taking snapshots from the Details-view windows, before and after a given operation is performed. Memory objects that exist after the post operation snapshot are potential memory leaks and can be further investigated.

Using Heap Watch with the kernel debugger

If you are running debug *Windows 95* under the wdeb386 debugger HW32 will display, on the debug terminal, the function address that allocated the object. If symbols for the allocator are loaded, type the *ln* command with the address of the allocator found by HW32 to display the symbol name. Otherwise, use the linker generated .map file to locate the allocator.

Command line options

Log file options:

- la LOGFILENAME The name of the log file used to dump summary heap info when the *Update* menu item is selected from the Summary-view window.
- lh LOGFILENAME The name of the log file used to dump heap snapshot info when the *Update* or *Snapshot* menu item is selected from the Details-view window.

When either of these command line parameters have been selected, a description dialog will appear when snapshots are taken. This gives the user the opportunity to enter a description that will be entered into the log file.

Automation options:

- aa MS Auto-All snapshot interval in milliseconds. This option automatically takes a summary view snapshot at the given time interval.
- ah MS Auto-Heap snapshot interval in milliseconds. This option automatically takes a details view snapshot at the given time interval.

To view a given memory object

1. From the Summary-view window, Dbl-click on the process' heap you wish to watch. This gives you the Details-view window.
2. From the Details-view window, Dbl-click on the address in heap of the memory object you wish to view.

To watch for memory leaks

1. From the Summary-view window, Dbl-click on the process' heap you wish to watch. This gives you the Details-view window.
2. Perform the operation where you are trying to find the memory leak.
3. Select the **Snapshot** menu item from the Details-view window. The snapshot count will be incremented. Allocations that took place during this snapshot and still exist, are possible candidates for a memory leak.
4. Look for allocated memory objects that belong only to the current snapshot. Objects that belong to the current snapshot will be automatically sorted to the top of the list.

- Repeat 2 through 4 as necessary.

- The **Update** menu option will take another snapshot of the heap and reset the snapshot count to one.

HeapWatch32						
File Update!						
Process Id	Module Name	Heap Id	Bytes Alloc	Obj Count	Bytes Free	
ffffe0241	EXCHNG32.EXE	7f74b055	496	3	1047920	
ffffe0241	EXCHNG32.EXE	7f44b055	0	0	1048428	
ffffe0241	EXCHNG32.EXE	7f54b055	436	3	1047980	
ffffe0241	EXCHNG32.EXE	7ca4b055	200	1	1048224	
ffffe0241	EXCHNG32.EXE	7cb4b055	200	1	1048212	
ffffe0241	EXCHNG32.EXE	7c84b055	200	1	1048212	
ffffe0241	EXCHNG32.EXE	7c94b055	200	1	1048224	
ffffe3af5	HCW.EXE	7ee5b055	5824	112	1045848	
ffffed84d	SPOOL32.EXE	7eecb055	0	0	1052448	
fffff0d85	EXPLORER.EXE	7ee9b055	63008	1358	982524	
fffff432d	WINWORD.EXE	7ed4b055	333544	778	714944	
fffff4535	KERNEL32.DLL	7eecb055	0	0	1048428	
fffff4f11	HW32.EXE	7eefb055	1792	38	1050580	
fffffd21d	KERNEL32.DLL	7eedb055	0	0	1048428	
fffffde61	MPREXE.EXE	7efcb055	164	2	1052264	
fffffe995	KERNEL32.DLL	7eedb055	0	0	1048428	
fffffb69	KERNEL32.DLL	7eecb055	0	0	1048428	

HW32(Details) EXPLORER.EXE PID:0xffff0d85 HID:0x7ee9b055					
File Update! Snapshot!					
Address	Size	Flags	Lock Count	Snapshot	
00440830	1252	Alloc	0	1	
00440d18	168	Alloc	0	1	
00440dc4	36	Alloc	0	1	
00440dec	68	Alloc	0	1	
00440e34	20	Alloc	0	1	
00440e4c	256	Alloc	0	1	
00440f50	200	Alloc	0	1	
0044101c	56	Alloc	0	1	
00441058	24	Alloc	0	1	
00441074	16	Alloc	0	1	
004410a4	16	Alloc	0	1	
004410b8	12	Alloc	0	1	
004410c8	24	Alloc	0	1	
004410e4	12	Alloc	0	1	
004410f4	12	Alloc	0	1	
00441104	56	Alloc	0	1	
Snapshot	Alloc	Objs	Delta Alloc	Delta Objs	
1	68164	1477			

```
HW32(Object) 0x447ba0 EXPLORER.EXE PID:0xffff0d85 HID:0x7ee9b055
0000 14 00 1f 00 e0 4f d0 20-ea 3a 69 10 a2 d8 08 00 ...O...i.....
0010 2b 30 30 9d 19 00 23 43-3a 5c 00 00 00 00 00 +00...#C:\.....
0020 10 0a 54 00 20 14 03 00-d8 09 54 31 2c 17 00 31 ..T.....T1...1
0030 00 00 00 00 00 93 1d 6e-a6 10 80 57 69 6e 64 6f .....In...Windo
0040 77 73 00 00 20 00 31 00-00 00 00 00 3b 1e 35 bc ws...1.....|5.
0050 10 00 50 72 6f 66 69 6c-65 73 00 50 52 4f 46 49 ..Profiles.PROFI
0060 4c 45 53 00 20 00 31 00-00 00 00 00 3b 1e 35 bc LES...1.....|5.
0070 10 00 76 69 6e 63 65 6e-74 72 00 56 49 4e 43 45 ...rtnecniv.....
0080 4e 54 52 00 22 00 31 00-00 00 00 00 3b 1e 44 bc NTR."..1.....|D.
0090 10 00 53 74 61 72 74 20-4d 65 6e 75 00 53 54 41 ..Start Menu STA
00a0 52 54 4d 7e 31 00 20 00-31 00 00 00 00 00 3b 1e RTM~1...1.....|
00b0 44 bc 10 00 50 72 6f 67-72 61 6d 73 00 50 52 4f D...Programs PRO
```

