SWEEP memory usage
Design for the Future

Dr. Jan Hruska, Sophos Plc, Oxford, England

Part # tr000084/940721

SWEEP versions 2.63 and later require extended or expanded memory or disk for storing virus information while executing. The reasons and implications are discussed in this report.

Why was the change necessary?

The number of viruses continues to grow linearly at between 100 and 200 new samples every month. Every virus is analysed and described in the proprietary Sophos Virus Description Language (VDL). Depending on the complexity of the virus, the description information is between 20 and 300 bytes long.

In order to maintain acceptable running speed, this information must reside in memory while SWEEP is executing.

Up until SWEEP version 2.62 conventional memory was used (i.e. the first 640K) to store the virus information. Since users normally run memory-resident software, the actual amount of available memory is reduced; typically to about 450K (use the DOS command *mem* to find out how much memory you have). As the number of viruses increases, we have had to find another place to store this information.

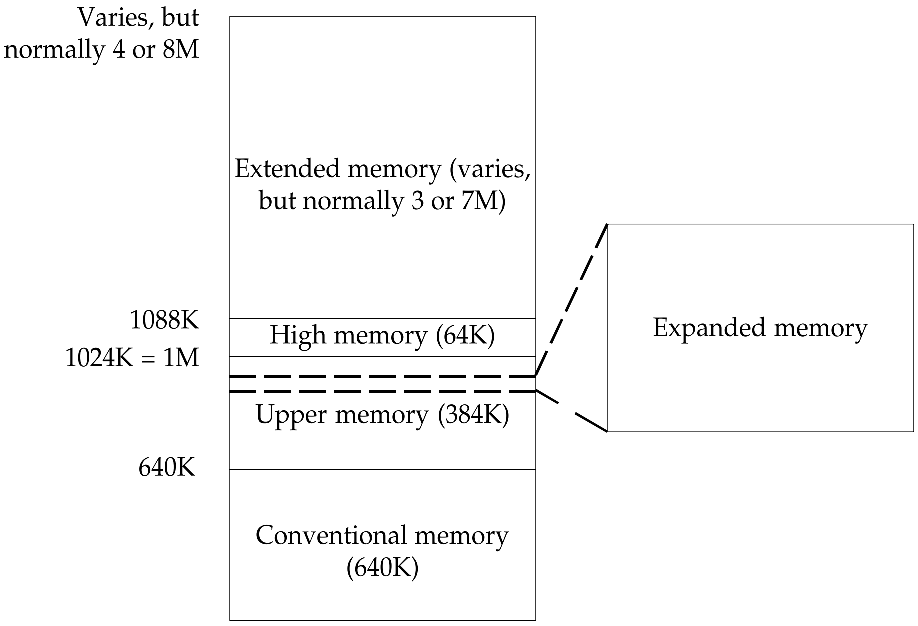
Memory types

PCs can access memory in three different ways:

- Conventional
- Extended (XMS)
- Expanded (EMS)

In addition, most 386 systems have an upper memory area which is the 384K of space adjacent to the 640K of conventional memory and which can be made to look like extended memory.

Programs which run under PC-DOS use conventional memory. In order to use extended or expanded memory, or the upper memory area, the PC must run a **memory manager**.


Varies, but normally 4 or 8M
Extended memory (varies, but normally 3 or 7M)
1088K
High memory (64K)
1024K = 1M
Upper memory (384K)
640K
Conventional memory (640K)
Expanded memory

Memory structure in a typical PC

SWEEP can use extended or expanded memory, or disk, for storing virus information while running.

Extended, expanded or disk

Extended memory

Extended memory is available on 80286 PCs and above. To use it, load the HIMEM extended memory manager through CONFIG.SYS, e.g.

```
DEVICE=HIMEM.SYS
```

If the PC is booted from floppy disk, the floppy disk should contain both HIMEM.SYS and CONFIG.SYS (see 'Preparing a clean boot disk').

Expanded memory

On 8086-based PCs SWEEP can use expanded memory, but you must use an expanded memory manager in CONFIG.SYS.

Disk

If an 8086-based PC is not fitted with expanded memory, SWEEP can use the hard disk as a swap area. SWEEP must be run (from either the floppy disk or the hard drive) with the -MD command line qualifier. The environment variable TMP must be set to wherever you wish the swap file to be stored. For example:

```
A>SET TMP=C:
A>SWEEP -MD
```

You should have at least 300K of free disk space available.

If the hard disk is not available, SWEEP can also use the floppy disk as a swap area, but this is not recommended due to the low speed of operation.

In order of preference, use extended then expanded memory and if neither is available, use disk.

Preparing a clean boot disk

First format a system disk:

```
C>FORMAT A: /S
```

Copy HIMEM.SYS to the disk:

```
C>COPY \DOS\HIMEM.SYS A:
```

Edit CONFIG.SYS on the disk to contain:

```
DEVICE=HIMEM.SYS
```

The benefits

The benefits in SWEEP versions 2.63 and later are:

- conventional memory requirement is less than 300K (version 2.63)
- SWEEP is unlikely to run out of memory for storing virus data, since most modern PCs have 4 Mbytes or more of extended memory
- more space is available to implement new features, such as automatic checking of compressed files, which may be introduced in future SWEEP releases