KERNEL

```
PSIONICS FILE - KERNEL
======================
Kernel memory organisation
Last modified 1997-09-09
=========================
Kernel memory can be examined with the system call GenGetOsData, or in blocksof assembler with
the system call GenDataSegment. Some useful information isavailable at known offsets. In
addition, a handle is actually the offset, inkernel memory, of the start of a data structure,
which can therefore also be
examined.
Constant offsets
----------------
Offset 1036 (word): number of seconds before auto power-offOffset 1052 (word): increments every
1/32 second, but is not synchronized
                    to the real time clock (it drifts)Offset 1056 (word): delay in 1/32 seconds
until current time next changes
Offset 1058 (long): current abstime
Data structures
---------------
The bottom 12 bits of a process ID are actually the address of the process'scontrol block. This
has the following format:
  Offset  0 (word): pointer to next process in the same queue  Offset  2 (word): pointer to
previous process in the same queue
  Offset  4 (word): @@ queKey
  Offset  6 (word): @@ queData
  Offset  8 (byte): @@ deltaType
  Offset  9 (byte): @@ addressTrap
  Offset 10 (byte): process status:
       1 = running (there is only one running process)
       2 = ready to run
       3 = waiting for a timer to expire
       4 = suspended
```

```
      5 = waiting for a semaphore
    255 = entry not in use
  Offset 11 (byte): non-zero if the process is to be suspended
  Offset 12 (byte): @@ priority
  Offset 13 (byte): @@ priorityH  Offset 14 (byte): zero if executing ROM code, non-zero if
executing RAM code
  Offset 15 (byte): zero for processes, non-zero for sub-tasks
  Offset 16 (cstr): process name
  Offset 29 (byte): zero if non-active, non-zero if active  Offset 30 (word): handle of the
semaphore of the process
  Offset 32 (word): @@ *semHead
  Offset 34 (word): address of the start of the heap  Offset 36 (word): amount to grow heap by,
in 16 byte units
  Offset 38 (word): address of the message control block (0 if none set up)  Offset 40 (word):
minimum heap size, in 16 byte units  Offset 42 (word): file server's handle for the process (0
if not using files)  Offset 44 (word): handle of the process's data segment (used for DS and
SS)
  Offset 46 (word): handle of the process's code segment (used for CS)  Offset 48 (word): @@
*saveSP
  Offset 50 (word): @@ *saveBP
  Offset 52 (byte): 0 = unattended, 1 = notify  Offset 53 (byte): non-zero if waiting for the
sound semaphore
  Offset 54 (word): top 4 bits of the process ID @@ in which bits ?  Offset 56 (word): checksum
of code
  Offset 58 (word): ProcOnTerminate message type
One queue (offsets 0 and 2) is maintained for ready processes, in priorityorder, one for
processes waiting for a timer, in timer order, and one for
each semaphore.
The checksum (offset 56) is used to determine whether two programs of the samename are running
the same code, which can then be shared between them.
The battery status data structure has an address returned by the system callHwGetBatData. It has
the following format: @@@@
    Offset  0 (byte): main battery level
    Offset  1 (byte): main battery status
    Offset  2 (byte): backup battery level
    Offset  3 (byte): mains power status
    Offset  4 (word): warning flags
```

```
    Offset  6 (????): insertion date
    Offset  @       : ticks in use battery
    Offset  @       : ticks in use mains power    Offset  @       : milliamp-ticks
```

Revision #1

Created Thu, Jan 24, 2019 10:26 AM by Alex

Updated Thu, Jan 24, 2019 10:26 AM by Alex