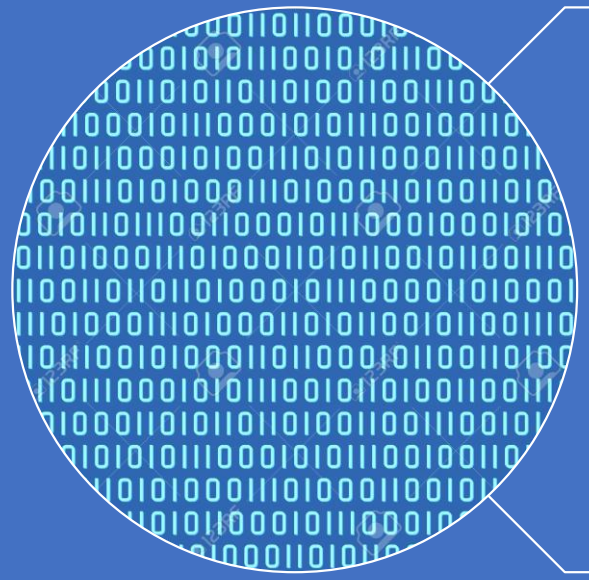


# Para além dos processos

Acássio Moura
Bruno Siqueira
Igor Carvalho
Leonardo Cararo

# Preview

- 8.1 : Introdução;
- 8.2: Os princípios básicos da memoria virtual;
- 8.3: Os princípios básicos das páginas de memória;
- 8.4: Arquivos e páginas de memória;
- 8.5 : Paginas de memória anônima;
- 8.6 : Capturando memória;
- 8.7 : O comando savecore;
- 8.8 : Análise estática: Reconhecendo arquivos na memória;
- 8.9 : Recuperando conteúdo de arquivo criptografado sem chaves;
- 8.10 : Blocos do sistema de arquivos versus a técnica de página de memória;
- 8.11 : Reconhecendo arquivos de memória;
- 8.12 : Análise dinâmica;
- 8.13 : Persistência de arquivos em memória;
- 8.14 : A persistência de dados não associados com arquivo ou dados anônimos;
- 8.15 : Persistência no espaço de troca;
- 8.16 : A persistência da memória após o processo de inicialização;
- 8.17 : A confiabilidade e a tenacidade dos dados na memória;

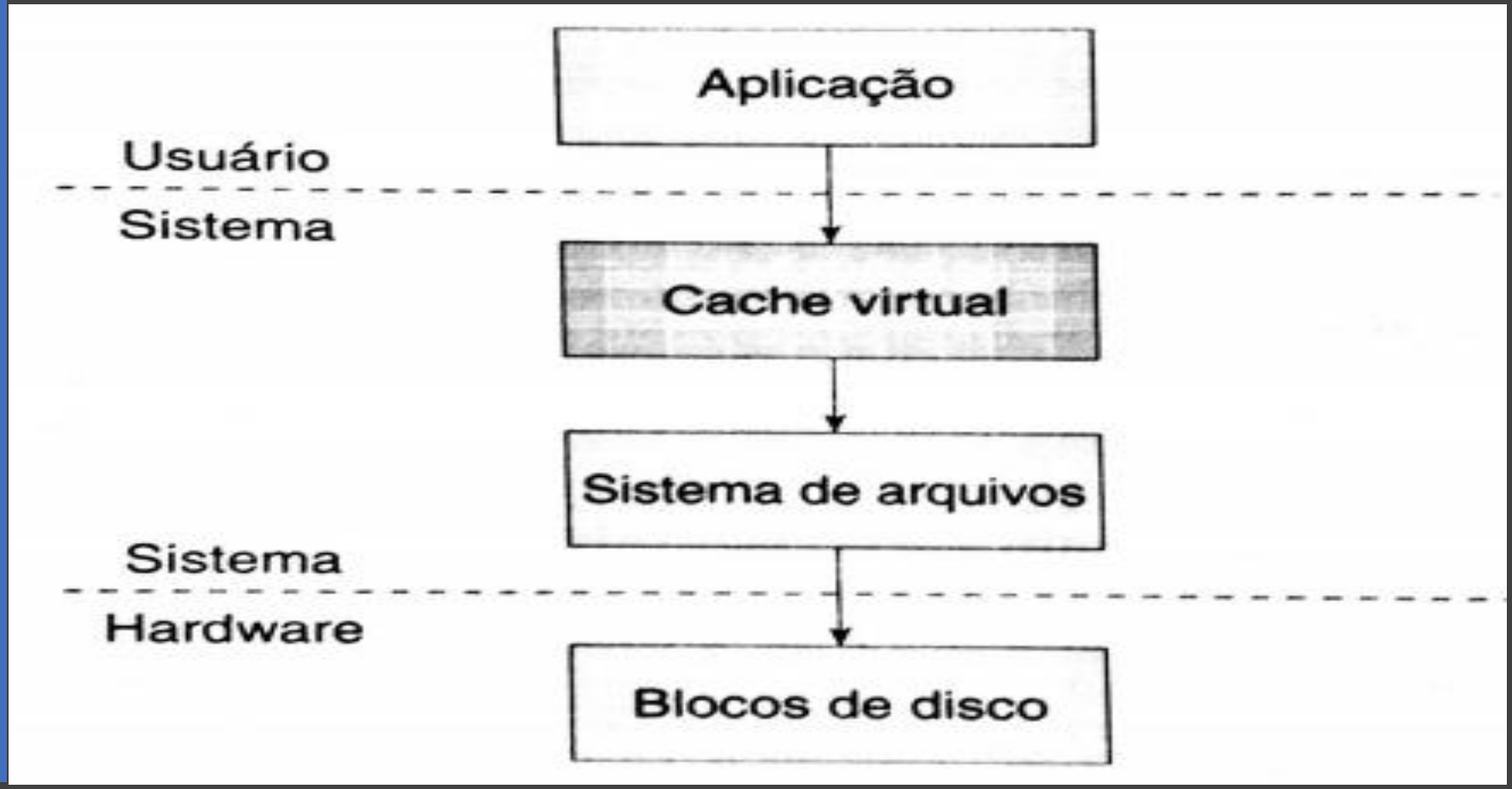
# Capitulo 8.1

# Introdução

# Capitulo 8.2

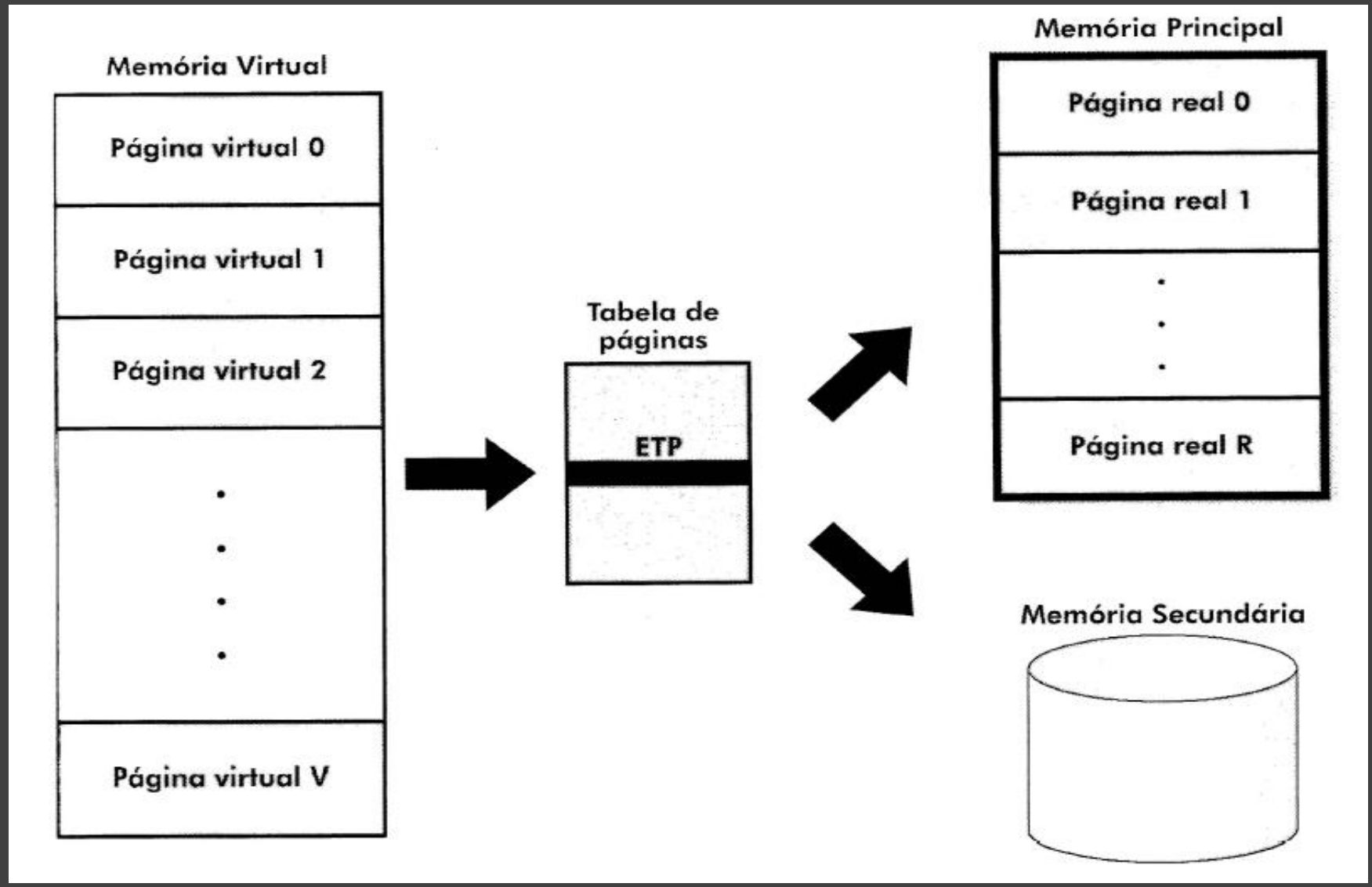
## Os princípios básicos da memoria virtual;

- Todos os sistemas operacionais modernos usam memoria virtual como abstração para tratar combinações da RAM;
- O sistema de arquivos sempre foi armazenado em cache ate certo ponto;



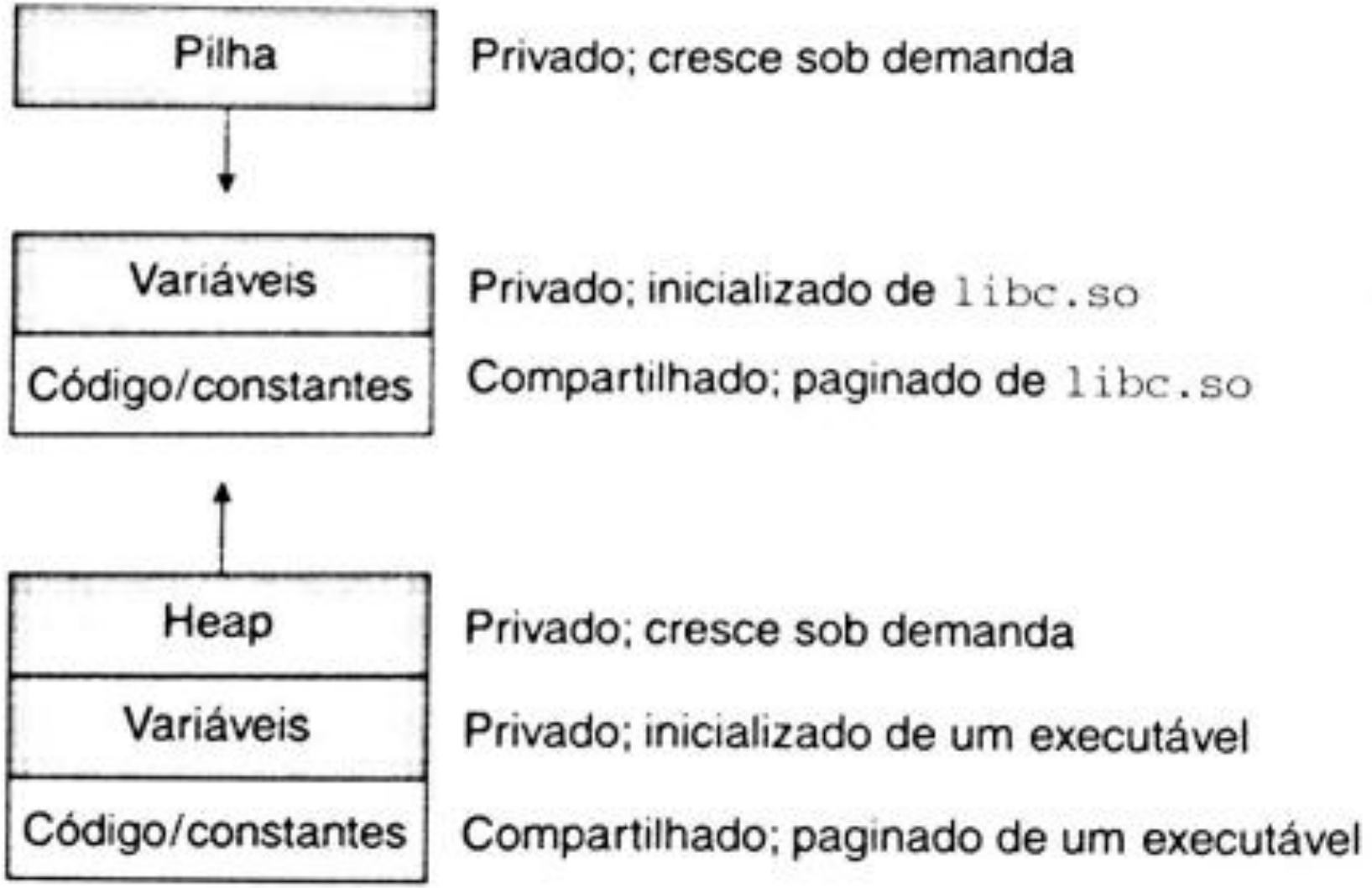
# Capitulo 8.3

Os princípios básicos das páginas de memória;



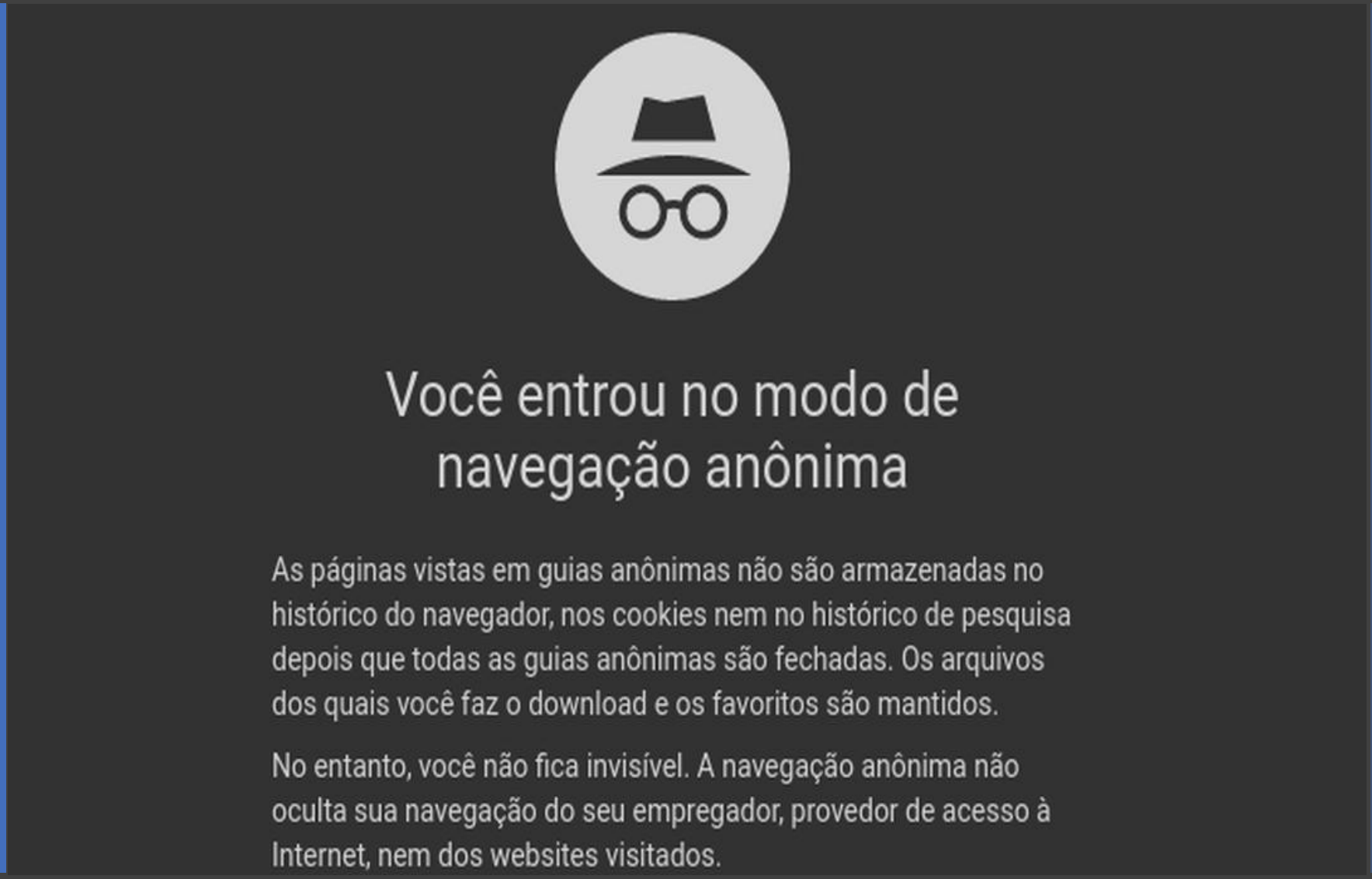
# Capitulo 8.4

## Arquivos e páginas de memória



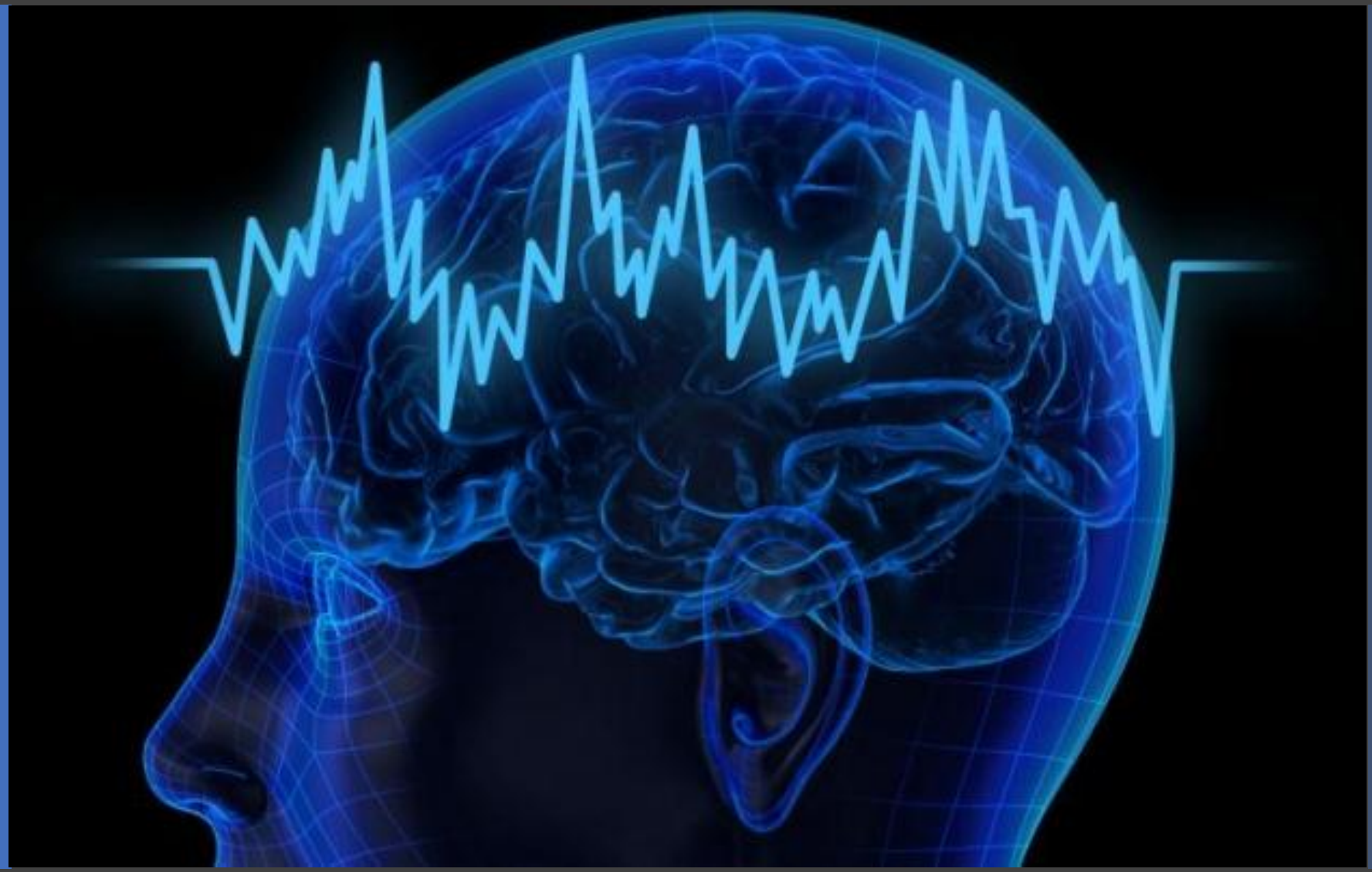
# Capitulo 8.5

## Páginas de memórias anônimas



# Capitulo 8.6

## Capturando memória



# Capitulo 8.7

## O comando : Savecore

Savecore: salva parte, se não toda a memoria principal da memoria.

```
solaris # dumpadm
      Dump content: all pages
       Dump device: /dev/dsk/c0t4d0s1 (dedicated)
Savecore directory: /foo/savecore
  Savecore enabled: yes
solaris # savecore -v -L
dumping to /dev/dsk/c0t4d0s1, offset 65536
100% done: 16384 pages dumped, compression ratio 2.29, dump succeeded
System dump time: Mon Dec 30 14:57:30 2002
Constructing namelist /foo/savecore/unix.1
Constructing corefile /foo/savecore/vmcore.1
100% done: 16384 of 16384 pages saved
solaris # ls -asl /foo/savecore/
total 264354
   2 drwxr-xr-x   2 root     other        512 Dec 30 14:57 ./
   2 drwxr-xr-x   4 root     root         512 Oct 22 22:44 ../
   2 -rwxr-xr-x   1 root     sys            2 Dec 30 14:58 bounds*
 704 -rw-------   1 root     sys       349164 Dec 30 14:57 unix.1
263472 -rw-------   1 root     sys    134905856 Dec 30 14:58 vmcore.1
```

# Capitulo 8.7

# O comando : Savecore

```
#!/usr/local/bin/perl -s
#
# Open /dev/mem or /dev/kmem and read page-size chunks.
# Ignore errors; just seek and read one page at a time.
#
#       Usage: $0 [-k] N
#
# Where "N" is the number of pages to read. The -k flag tells
# it to read from kmem (dangerous!); else it reads /dev/mem.
#

$page_length = 4096;                    # some pages are longer . . .
$ARGV[0] = "262144" unless $#ARGV >= 0;    # get 1 Gbyte of memory
if ($k) { $MEMORY = "/dev/kmem"; }
else    { $MEMORY = "/dev/mem"; }

die "Can't open $MEMORY\n" unless open(MEMORY, $MEMORY);

# for this many megabytes of data
for $n (0..($ARGV[0]-1)) {
        $position = $n * $page_length;
        seek(MEMORY,$position,0);
        if (($bytes_read = sysread(MEMORY, $page, $page_length))) {
         print $page;
         $total_bytes_read += $bytes_read;
         }
        }
warn "successfully read $total_bytes_read bytes from $MEMORY\n";
```

# Capitulo 8.8

## Análise estática: reconhecendo arquivos na memoria

```
freebsd # ./dump-mem.pl > giga-mem-img-1
successfully read 1073741824 bytes
freebsd # strings giga-mem-img-1 | fgrep "Supercalif"
freebsd # cat helloworld
Supercalifragilisticexpialidocious
freebsd # ./dump-mem.pl > giga-mem-img-2
successfully read 1073741824 bytes
freebsd # strings giga-mem-img-2 | fgrep "Supercalifr"
Supercalifragilisticexpialidocious
Supercalifragilisticexpialidocious
freebsd #
```

# Capitulo 8.9

Recuperando conteúdo de arquivo criptografado sem chaves

# Capitulo 8.10

## Blocos do Sistema de arquivos
## VS
## Técnica de página de memória

| Memória disponível (em Mb) | Corresp. de páginas | | Páginas NULL | | Não-reconhecidas | |
|---|---|---|---|---|---|---|
| | % | MB | % | MB | % | MB |
| *FreeBSD 5.0 e KDE 2.1* | | | | | | |
| 128 | 20,6 | 26,4 | 44,3 | 56,7 | 35,1 | 44,9 |
| 192 | 19,9 | 38,2 | 53,0 | 101,8 | 27,1 | 52,0 |
| 256 | 11,7 | 30,0 | 73,3 | 187,6 | 15,0 | 38,4 |
| 384 | 8,6 | 33,0 | 79,9 | 306,8 | 11,5 | 44,2 |
| *SuSe 7.1 e KDE 2.1* | | | | | | |
| 128 | 31,2 | 39,9 | 32,3 | 41,3 | 36,5 | 46,7 |
| 192 | 20,7 | 39,7 | 56,0 | 107,5 | 23,3 | 44,7 |
| 256 | 15,9 | 40,7 | 65,8 | 168,4 | 18,3 | 46,8 |
| 384 | 12,9 | 49,5 | 74,4 | 285,7 | 12,7 | 48,8 |
| *Solaris 2.51 e OpenWindows* | | | | | | |
| 128 | 39,3 | 50,3 | 15,3 | 19,6 | 45,4 | 58,1 |
| 192 | 37,6 | 72,2 | 15,0 | 28,8 | 47,4 | 91,0 |
| 256 | 37,3 | 95,5 | 13,1 | 33,5 | 49,6 | 127,0 |
| 384 | 38,4 | 147,5 | 16,3 | 62,6 | 45,3 | 174,0 |

# Capitulo 8.11

# Reconhecendo arquivos na memória

- Hash MD5.
- Certificado Digital
- Reconhecimento de arquivos atravez do Hash MD5.

```
/kernel                    (80.7% found, 3814504 bytes)
/modules/ng_socket.ko      (84.6%,      12747)
/modules/ng_ether.ko       (81.8%,      10899)
/modules/ng_bridge.ko      (84.6%,      13074)
/modules/netgraph.ko       (94.7%,      38556)
/modules/linprocfs.ko      (92.8%,      27843)
/var/run/ppp               (100%,         512)
/var/run/syslog.pid        (100%,           3)
/var/run/dev.db            (25.0%,      65536)
/var/run/ld-elf.so.hints   (100%,         203)
/var/log/sendmail.st       (100%,         628)
/var/log/auth.log          (66.7%,      15345)
[. . . 500 mais linhas omitidas. . .]
```

# Capitulo 8.12

# Análise dinâmica: a persistência dos dados na memória

- Persistência de dados na memoria
- Recuperação dos dados com programas simples
- Excluir completamente os dados da memória

# Capitulo 8.13

## Persistência de arquivos na memória

- Encriptar arquivos para perícia
- Rastro digital
- Porcentagem recuperavel de arquivos

# Capitulo 8.14

A persistência de dados não associados com arquivo ou dados anônimos

- Pequena parte recuperavel de arquivo
- Arquivo sobrescrito
- Ilegivel

# 8.15

# Persistência no espaço de troca

- Arquivos deletados mantidos a salvo em espaço em disco.

# 8.16 Persistência de memória após processo de inicialização

- Duração dos dados após reinicialização

# 8.17 Confiabilidade e a tenacidade dos dados.

- Os dados são ou não confiáveis ?

# Perguntas ?