3. 在 Linux 下，汉字用（ D ）个字节编码。

A. 2　　B. 3　　C. 4　　D. >=3

这道题的 A 项应该也可以算对。

原因：本题说的是“在 Linux 下，汉字用几个字节编码”，而 **Linux 下并不一定非要用 UTF-8 编码**。去百度上搜，**发现有可以把 Linux 的编码改为 gbk 的教程。**而根据 GBK 的编码规则，**一个汉字占用 2 个字节**。

本题更严谨的提问方式应当是“在 Linux 的**默认**情况下……”。既然没提默认，就不能有默认的假设。

（来源：https://www.cnblogs.com/dengmeinan/p/10821640.html）

9. 进程的虚拟地址空间到磁盘文件的映射通过（ D ）

A. fork　　B. execve　　C.loader　　D.mmap

这道题的 C 项应该也可以算对。

原因：把题目中的“磁盘文件”理解为“**该程序的可执行文件**”，即**被加载器加载的可执行文件**。

这里引用 CSAPP 教材的原话（第 485 页旁注的第 2 段）：

……加载器删除子进程现有的虚拟内存段，并创建一组新的代码、数据、堆和栈段。新的栈和堆段被初始化为零。通过**将虚拟地址空间中的页映射到可执行文件的页大小的片**(chunk), 新的代码和数据段被初始化为可执行文件的内容。……

15. 库打桩不会发生在（ C ）

A.编译时　　B.静态链接时　　C.静态链接/运行时　　D.动态链接/运行时

这道题应该没有答案。

原因：对于 C、D 项中**对“/”的理解是有歧义的**。有以下两种理解：

（1）“/”的前后内容**无关**。所以选 C 的意思是，库打桩不会发生在静态链接时，也不会发生在**任何情况下的**运行时。D 同理。

（2）“/”的前后内容**有关**。所以选 C 的意思是，库打桩不会发生在静态链接时，也不会发生在**静态链接后的**运行时。D 同理。

36.（ √ ）Ubuntu 中数据段、代码段在内存的起始地址（段基址）是一样的。

建议×、√均可。

原因：**数据段**在内存的起始地址**并不是固定的**。

这里引用 CSAPP 教材原话（第 484 页倒数第二段）：

为了简洁，我们把堆、数据和代码段画得彼此相邻，并且把栈顶放在了最大的合法用户地址处。**实际上，由于.data 段有对齐要求**（见 7.8 节），所以**代码段和数据段之间是有间隙的**。同时，在分配栈、共享库和堆段运行时地址的时候，链接器还会使用**地址空间布局随机化**(ASLR, 参见 3.10.4 节)。虽然每次程序运行时这些区域的地址都会改变，它们的相对位置是不变的。

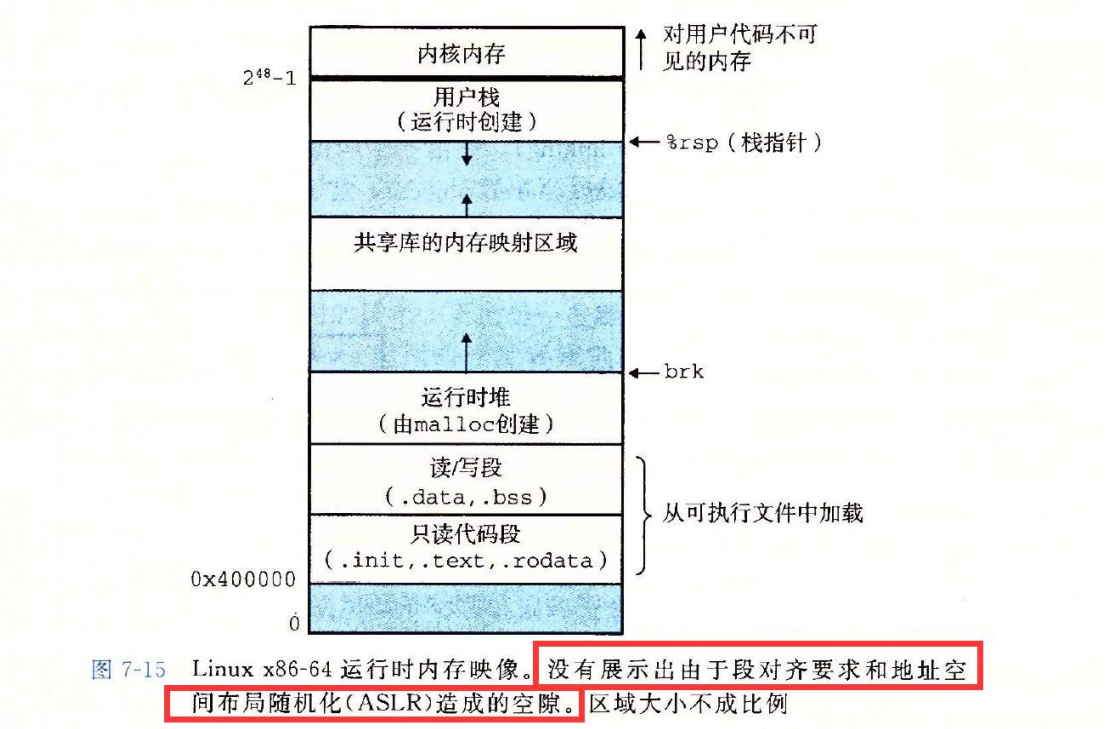

图 7-15 Linux x86-64 运行时内存映像。没有展示出由于段对齐要求和地址空间布局随机化(ASLR)造成的空隙。区域大小不成比例

（图片来自 CSAPP 教材第 485 页）