**1a.** 160 kB

**1b.** RW – read write

**1c.** Private – this means that me memory allocated cannot be shared by other processes.

**1d.** 0xde

**1e.**

```
VirtualAlloc(
    0xca0000,
    160000,
    MEM_COMMIT,
    PAGE_READWRITE
);
```

**2a.** RWX – read, write, execute. In addition to being able to read and write, it can also execute code.

**2b.** The memory is not committed. It is reserved. This means that no other processes can interact with it.

**2c.**

```
VirtualAlloc(
    0xab0000,
    320000,
    MEM_RESERVE,
    PAGE_EXECUTE_READWRITE
);
```

**3.** 0x760000. This is likely used to store hidden code that is to be dropped off or executed. I can see the text “this program cannot be run in dos mode” inside of the memory.

**4.**

KnownDlls: allows the system cache commonly used dlls. This increases load times. Can be used to force a system to load a dll.

ConDrv: Console Driver is a trustworthy Windows file. It is located in C:\Windows\System32\drivers. According to https://www.file.net/process/condrv.sys.html, it is likely compressed. Sometimes malware authors will drop a file of this name into another directory. The ConDrv file that was started by the original executable appears to be in the device folder which is not where it is supposed to be, so it is likely malicious.

Ntdll: contains the NT kernel functions. Flagged as a major security risk in bulletin MS03-07. Shouldn't be a problem if your system is up to date.

There are also handles opened for the original executable as well as the folder that it is in.

HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions: I cannot find any information on this one.