Lab 1-1:

* This program was matched with many virus signatures
* The files were compiled on December 19th 2010, at 5:16 PM
* The files are not packed or obfuscated because when you run strings on the program it shows many relevant strings
* The dll file might be obfuscated but it does not seem to be because it has legible strings in the file.
* The file looks for a file, copies it and it creates processes and also uses sleep
* There is an IP address in the dll file.

Lab1-2:

* The file is labeled as a Trojan
* The file is packed, when you put it in virustotal it is listed as packed
* This malware imports KERNEL32.dll, ADVAPI32.dll, MSVCRT.dll, WININET.dll, these imports tell us that it changes files in system32, it creates a service and it connects to the internet
* In the strings of the file it has a url and a version number for what web browser to use.

Lab3-1:

* The file imports KERNEL32.dll and it has an IP listed as a string and it creates a new shell for the proposed backdoor that it has a signature for. It also connects over HTTP version 1.0
* The file makes the mutex WinVMX32 and it connects to 192.0.78.25 over https

Lab5-1:

* The address of D11Main is, 1000D02E
* The import of gethostbyname is at .idata:100163CC
* The function was called 9 times