Luca Lemnij HW2 Q1

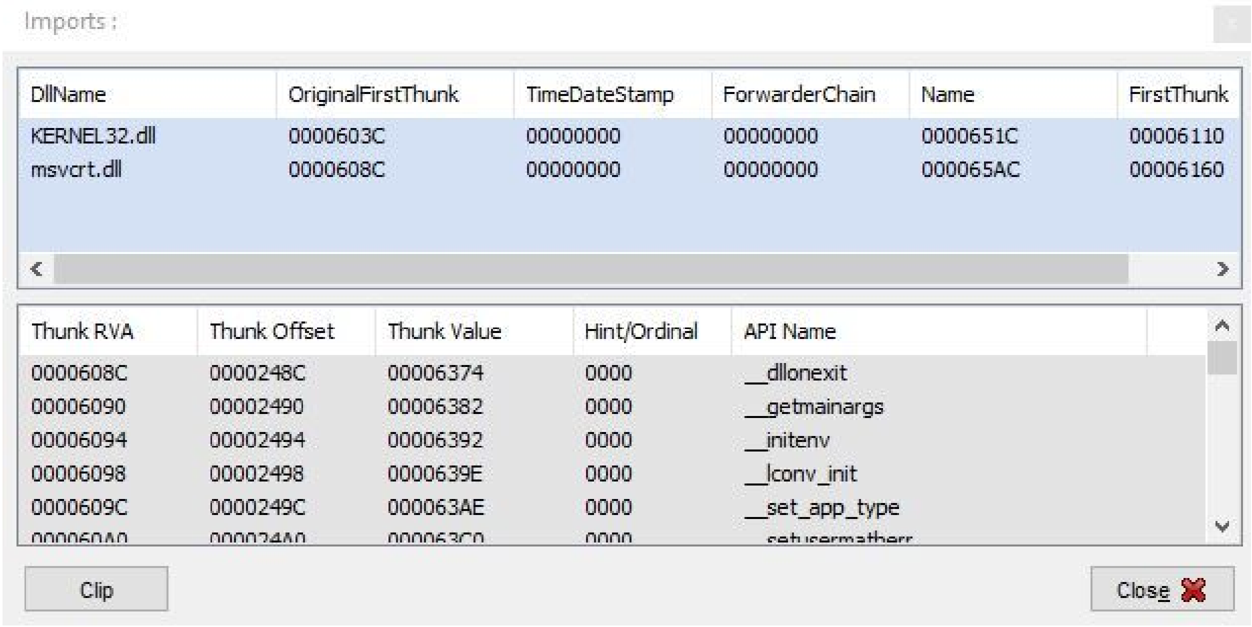
Step 1.

```
#include <stdio.h>
#include <stdlib.h>


int main(void) {
   FILE * file = fopen("C:/PE-1.txt", "w+");
   int match;
   char line[250];

          while(fgets(line, 250, file) != NULL) {
                     if(strcmp(line, "I want to learn PE file format!\n")) {
                               match = 1;
                               break;
           }
          }
           if(!match) {
                     int c = fputs("I want to learn PE file format!", file);
    }
          fclose(file);
          free(line);
 }
```

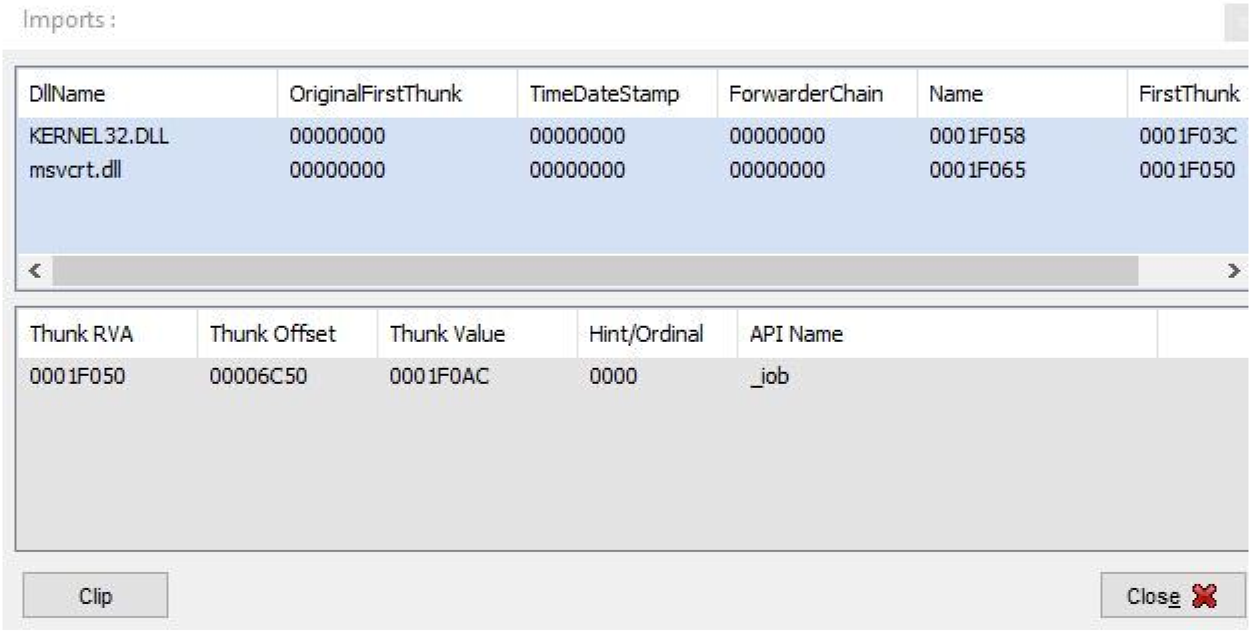
Step 2.



DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
KERNEL32.dll	0000603C	00000000	00000000	0000651C	00006110
msvcrt.dll	0000608C	00000000	00000000	000065AC	00006160

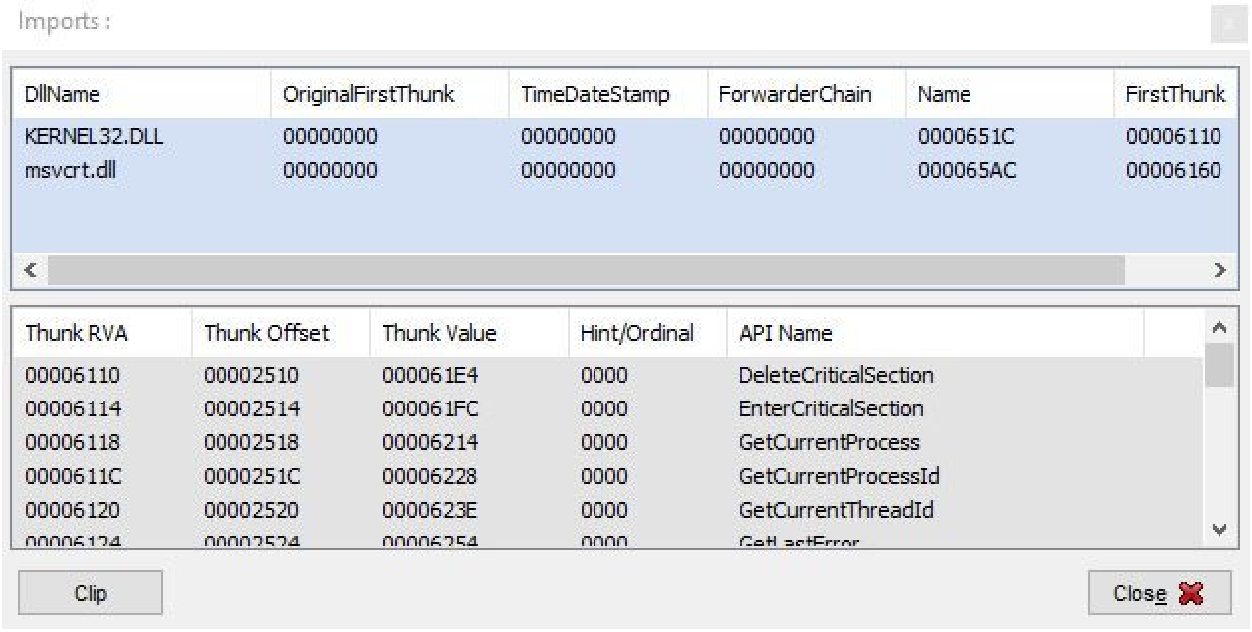
Thunk RVA	Thunk Offset	Thunk Value	Hint/Ordinal	API Name
0000608C	0000248C	00006374	0000	__dllonexit
00006090	00002490	00006382	0000	__getmainargs
00006094	00002494	00006392	0000	__initenv
00006098	00002498	0000639E	0000	__lconv_init
0000609C	0000249C	000063AE	0000	__set_app_type
000060A0	000024A0	000063C0	0000	__setusermatherr

Step 3.1 / 2 The first picture is packed, the second is unpacked.



DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
KERNEL32.DLL	00000000	00000000	00000000	0001F058	0001F03C
msvcrt.dll	00000000	00000000	00000000	0001F065	0001F050

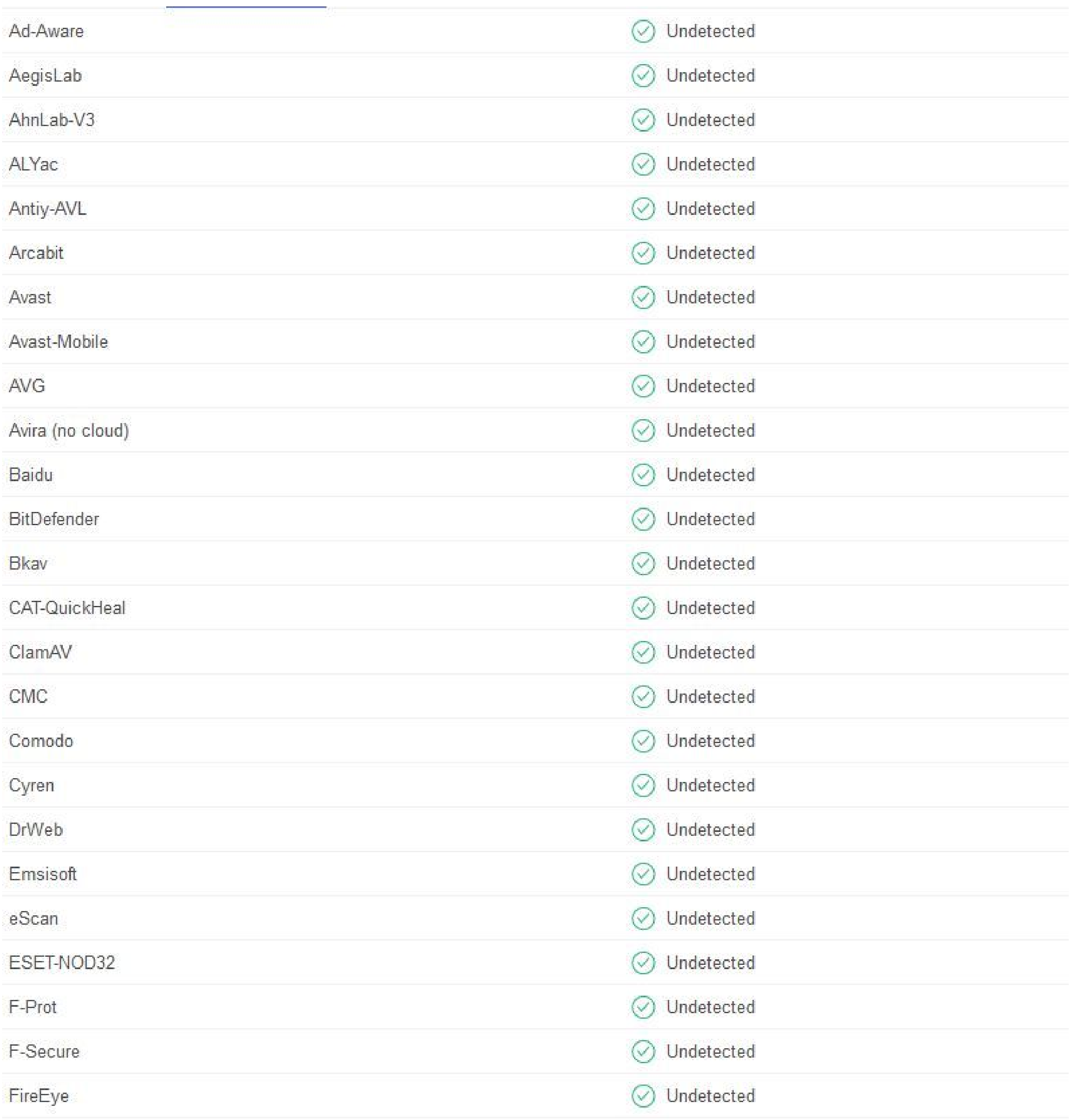
Thunk RVA	Thunk Offset	Thunk Value	Hint/Ordinal	API Name
0001F050	00006C50	0001F0AC	0000	_iob



DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
KERNEL32.DLL	00000000	00000000	00000000	0000651C	00006110
msvcrt.dll	00000000	00000000	00000000	000065AC	00006160

Thunk RVA	Thunk Offset	Thunk Value	Hint/Ordinal	API Name
00006110	00002510	000061E4	0000	DeleteCriticalSection
00006114	00002514	000061FC	0000	EnterCriticalSection
00006118	00002518	00006214	0000	GetCurrentProcess
0000611C	0000251C	00006228	0000	GetCurrentProcessId
00006120	00002520	0000623E	0000	GetCurrentThreadId
00006124	00002524	00006254	0000	GetLastError

4.I fooled it by using windows IExpress tool and then also using the packer. This is the link, and a screenshot it attached. SED file is also attached.
https://www.virustotal.com/gui/file/2b914a3797c3c7be9fa941e9302f76c7d631ebcc38212afdd4fbac2346f0bb4b/detection



Ad-Aware	✓ Undetected
AegisLab	✓ Undetected
AhnLab-V3	✓ Undetected
ALYac	✓ Undetected
Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected
Avast	✓ Undetected
Avast-Mobile	✓ Undetected
AVG	✓ Undetected
Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected
BitDefender	✓ Undetected
Bkav	✓ Undetected
CAT-QuickHeal	✓ Undetected
ClamAV	✓ Undetected
CMC	✓ Undetected
Comodo	✓ Undetected
Cyren	✓ Undetected
DrWeb	✓ Undetected
Emsisoft	✓ Undetected
eScan	✓ Undetected
ESET-NOD32	✓ Undetected
F-Prot	✓ Undetected
F-Secure	✓ Undetected
FireEye	✓ Undetected