Lab1.1:

1,Sử dụng có chữ kí, signature

Có 56/72 engine được phát hiện

2,các tệp này được biên dịch khi nào?

Tệp lab1-02.exe được biên dịch 2011/01/19 Web 16:10:41 UTC

3,Dấu hiệu nào cho thấy bị đóng gói hay xáo trộn không? Chỉ ra

+lab1-02.exe bị đóng gói, xáo trộn vì:

+Vitual Size: 4000 >> (lớn hơn nhiều) Size of Raw data:0000

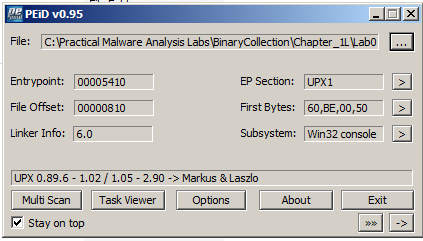
+Cả VirusTotal và PEiD đề xác định tệp này được đóng gói bằng UPX

=>file bị đóng gói

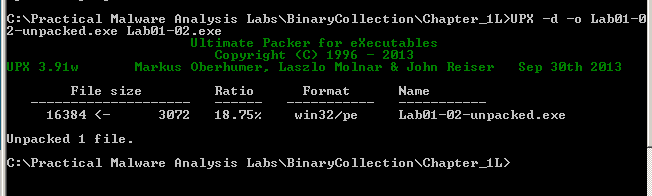
Trên VirusTotal

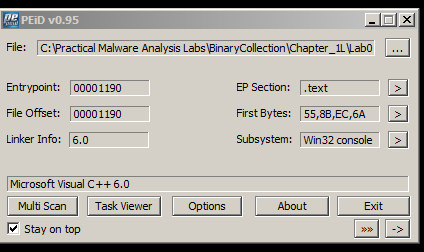


Trên PeiD



Giải nén

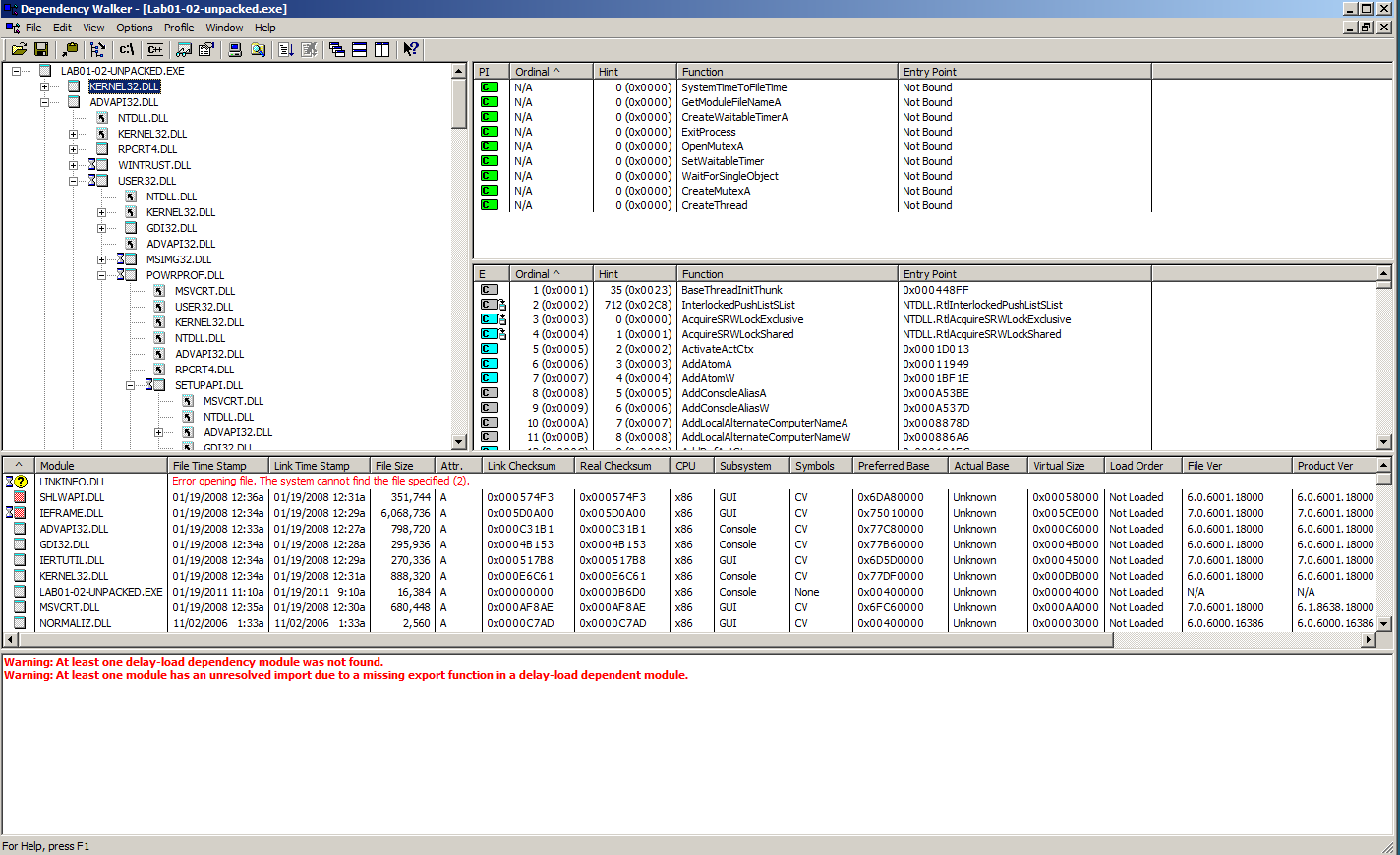




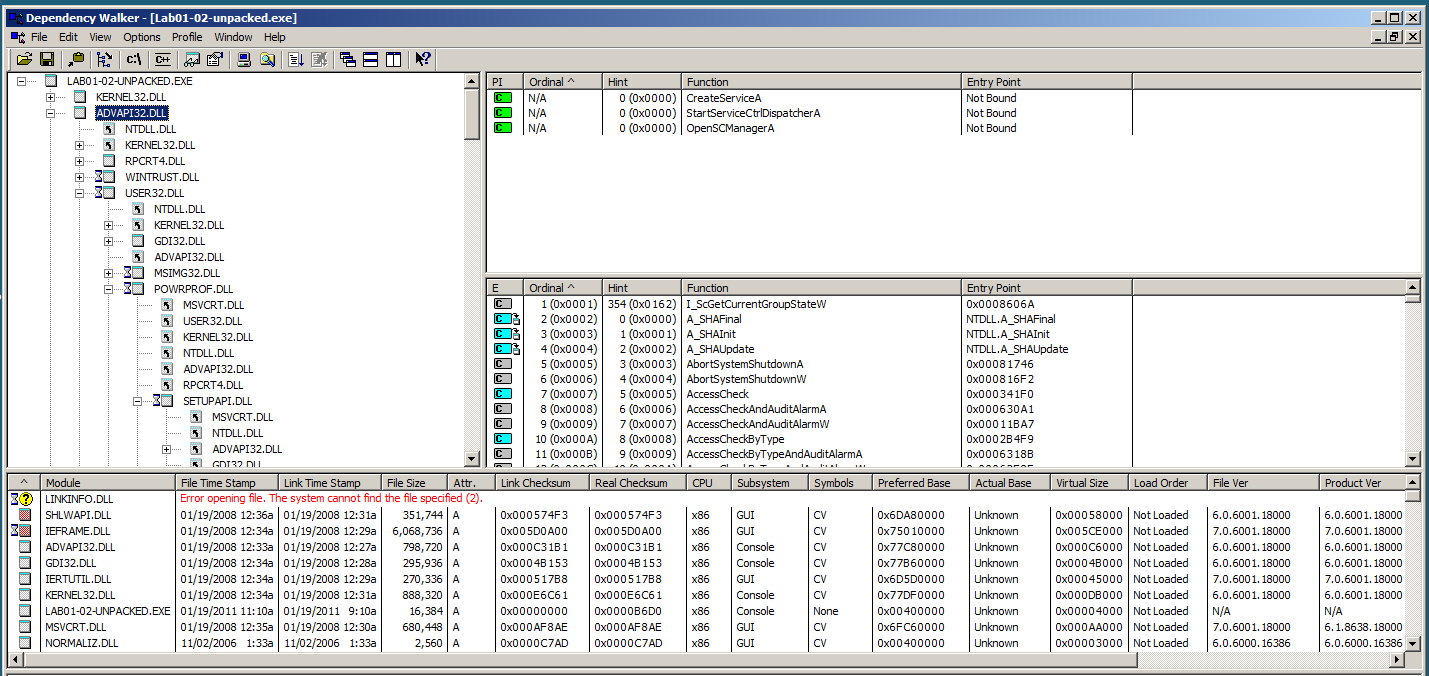
-có bất kì import nào nghi ngờ là mã độc không? nêu ra

KERNEL32.DLL

* SystemTimeToFileTime
* GetModuleFileNameA
* CreateMutexA
* CreateThread
* SetWaitableTimer

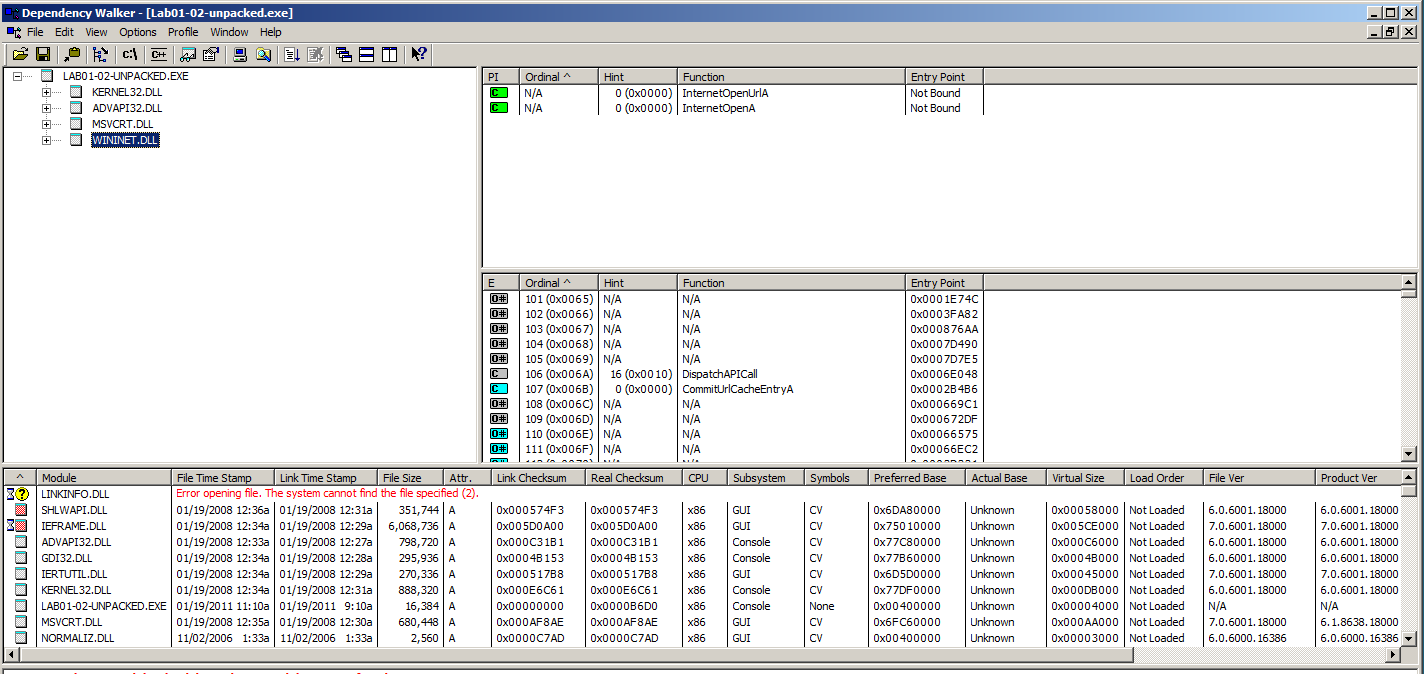


ADVAPI32.DLL

* CreateServiceA
* StartServiceCtrlDispatcherA
* OpenSCManagerA
* 

WININET.DLL

* InternetOpenUrlA
* InternetOpenA



-Có bất kì tệp nào, chỉ báo nào dựa trên máy chủ (host)

depend

1. Services or mutexes named MalService," Malservice," or HGL345
2. Network communication with http://www.malwareanalysisbook.com
3. HTTP requests with user-agentInternet Explorer 8.0

-phỏng đoán tệp tin về