



南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异

# 恶意代码分析与防治技术

## 第2章 基本静态分析技术

王志

zwang@nankai.edu.cn

南开大学 网络空间安全学院

2023-2024学年

# 新型冠状病毒 与网络安全病毒特点分析

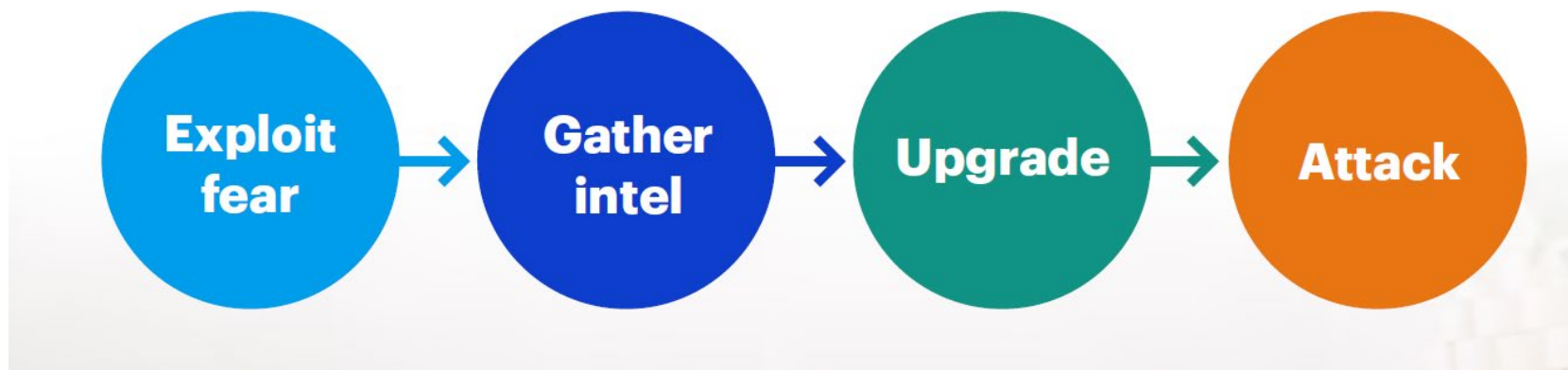
新型冠状病毒	病毒名称	永恒之蓝 (WannaCry) 勒索病毒
野生动物-中华菊头蝠	传染源	影子经纪人-利用美军NSA 网络攻击武器库工具
人	感染对象	服务器终端
经呼吸道飞沫传播 亦可通过接触传播 存在粪-口传播可能性	传播途径	利用MS17-010漏洞攻击微软 SMB服务， 通过139和445端口感染
人传人、人通过路网 交通，各地爆发	传染路线	机器之间互相传染 通过网络复制传播
发热、乏力、干咳， 逐渐呼吸困难	症状	文件全部加密，变更文件名， 桌面背景包含勒索语言和支付方式
传染强度高于非典	传染强度	传染强度大，一个机器中招， 几个小时同网全部机器被加密
严重， 致死率目前在2~3%左右	严重性	严重， 最核心数据全部被加密
人群普遍易感	易感群体	系统版本较老，未升级MS17-010 补丁的，开放139、445端口的， 后期主要感染非互联网系统
尚无	特效药物	尚无很好的手段 被加密后破解难度很大
3~7天，最长14天	潜伏期	永恒之蓝演变成潜伏挖矿病毒





允公允能 日新月异

# COVID-19 changed the threat landscape




南开大学  
Nankai University




允公允能 日新月异

# Exploit fear

RE: Disposable Face Mask and Forehead Thermometer

 Fujian Joy Solar Technology Corporation <geral@fcristino.com>  
To undisclosed-recipients:

 IMG\_0585032857.zip  
44 KB

Dear,

Nice day!

This is Bella Huang from Fujian Joy Solar Technology Corporation. Currently, the Coronavirus has spread all over the world.


Attached are the item images In order to fight against the epidemic, our company has developed established two production lines for disposable face mask and forehead thermometer.


Now we have started mass production but demand exceeds supply.

Kindly contact us if interested.

Thanks and best regards,  
FRADAH MOHAMED  
Customer Service  
1-888-3M HELPS (1-888-364-3577)

UNICEF COVID-19 TIPS APP


 UNICEF Inc <swift@allcounty.com>  
To Recipients

 UNICEF COVID-19 APP.parj  
1 KB

Find attached presentation & APP regarding COVID-19 for your reference and dissemination. kindly download and install on your system for dearlly update and guide line on how to protect your self and staff from this current deadly virus

Kindly pass it on, Let join hand together and fight this virus to the last.

Thanks  
1-760-597-2966 ext 135

  
**unicef**  
Jennifer Debeer

3/16/2020

In April, Google reported it was blocking 18 million spam emails related to COVID-19 per day!



南开大学  
Nankai University



允公允能 日新月异

# Malware as a business

- Malware Distribution Services
  - On November 23, GootKit pushing the Revil ransomware to machines only in Germany.







允公允能 日新月异

# 本章知识点

1. Antivirus Scanning
2. Hashes
3. Finding Strings
4. Packed and Obfuscated Malware
5. Portable Executable File Format
6. Linked Libraries and Functions
7. Dependency Walker
8. The PE File Headers and Sections





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異



# Basic Static Analysis

有哪些恶意代码的识别方法？

作答





允公允能 日新月异

# Static Analysis

- **Reverse engineering** the code or structure of a binary executable to understand its functionality.
- Static analysis:
  - The program is **not run** at this time.





允公允能 日新月异

# Basic Static Analysis

- **No** disassembly
- Provides good **pointers** to guide dynamic and advanced analysis
- Lots of **tools** involved!





允公允能 日新月异

# Techniques

- Antivirus scanning
- Hashes
- A file's strings, functions, and headers



使用基本静态分析我们能够获得哪些恶意代码的特征？

- ☒ A URLs
- ☒ B File Names
- ☒ C Registry Keys
- ☒ D API functions

提交





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異

# Antivirus Scanning

列出大家知道的杀毒软件名称。

正常使用主观题需2.0以上版本雨课堂

作答







允公允能 日新月异

# 杀毒软件



南开大学  
Nankai University



允公允能 日新月异

# Antivirus Scanning

- Known malware
  - File signatures
  - Heuristics
- Unknown malware
  - Obfuscation
  - Polymorphic: syntax obfuscation
  - Metamorphic: semantic obfuscation





允公允能 日新月异

# Collection of Antivirus Tools



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

No file selected

Choose File

Maximum file size: 64MB



南开大学  
Nankai University



允公允能 日新月异



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

File

URL

Search

1eae1e2-fad8-4ef0-b20f-1863e02100e1.doc

Choose File

Maximum file size: 128MB

By clicking 'Scan it!', you consent to our [Terms of Service](#) and allow VirusTotal to share this file with the security community. See our [Privacy Policy](#) for details.

Scan it!



SHA256: 7a371cc054ee14f0614b90cd6797001b5fd18c70c45c463f9f1a161ba08498ec

File name: 1eae1e2-fad8-4ef0-b20f-1863e02100e1.doc

Detection ratio: 0 / 55

Analysis date: 2017-02-15 04:46:13 UTC ( 0 minutes ago )



- Analysis
- File detail
- Additional information
- Comments
- Votes

Antivirus	Result	Update
ALYac	✓	20170215
AVG	✓	20170215
AVware	✓	20170215
Ad-Aware	✓	20170215







南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異

A light blue world map is centered in the background of the slide.

# Hashing



为什么文件哈希值可以用来作为杀毒软件的特征？  
有哪些优点和缺点？

正常使用主观题需2.0以上版本雨课堂

作答





允公允能 日新月异

# Hashing

- Method to uniquely identify malware
- MD5
  - Message-Digest Algorithm
  - 128-bit hash
- SHA1
  - Secure Hash Algorithm
  - 160-bit hash





允公允能 日新月异

# Hashes

- Input:
  - A file or string with arbitrary length
- Output:
  - fixed-length hash
- Uniquely identifies a file well in practice
  - MD5 collisions but they are not common
  - Collision: two different files with the same hash





# HashCalc

**H HashCalc** [Minimize] [Maximize] [Close]

Data Format: File ▼ Data: C:\Users\student\Desktop\p3.pcap ...

☐ HMAC Key Format: Text string ▼ Key:

---

☒ MD5 52583b5e2c99d19c046915181fd7b29b

☐ MD4

☒ SHA1 991d4e880832dd6aaebadb8040798a6b9f163194

☐ SHA256





允公允能 日新月异

# Hash Uses

- Label a malware file
- Share the hash with other analysts to identify malware
- Search the hash online to see if someone else has already identified the file



南开大学  
Nankai University



南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異

# Finding Strings





允公允能 日新月异

# Strings

- String: a sequence of printable characters.
- Computer can only understand 0 and 1
- Use 0 and 1 to represent characters
  - **ASCII**
  - **UNICODE**



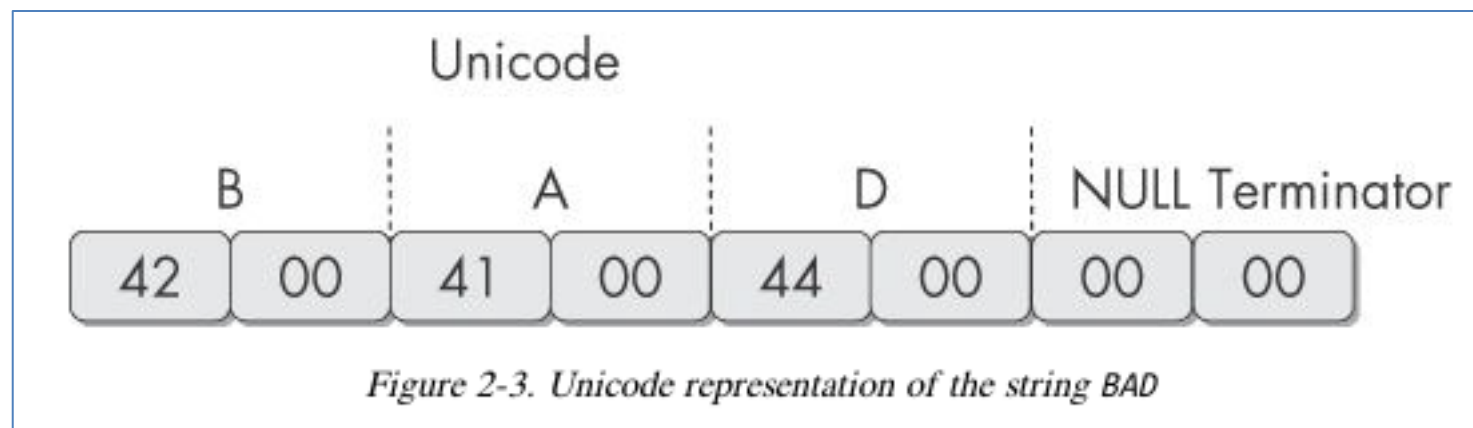
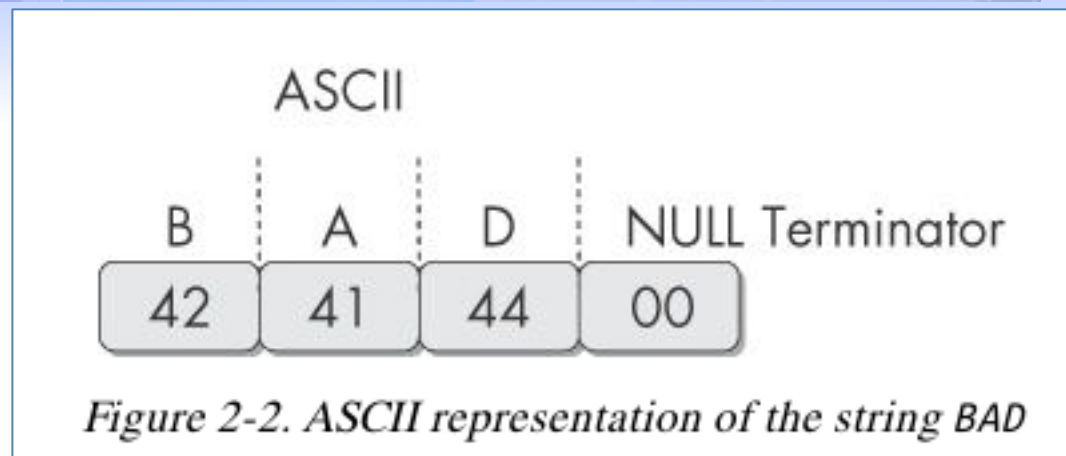


允公允能 日新月异

# Strings

- **ASCII**
  - American Standard Code for Information Interchange
  - 8 bits long
- **UNICODE**
  - Universal Coded Character Set
  - 135 modern or historic scripts
  - 16 bits long







允公允能 日新月异

# The strings Command

- Search binary executable for ASCII and Unicode strings
- Three or greater sequence of characters
- Followed by a terminator





允公允能 日新月异

# The strings Command

```
C:>strings bp6.ex_  
VP3  
VW3  
t$@  
D$4  
99.124.22.1 4  
e-@  
GetLayout 1  
GDI32.DLL 3  
SetLayout 2  
M}C  
Mail system DLL is invalid.!Send Mail failed to  
send message. 5
```



字符串是否可以隐藏？ 躲避基于字符串的杀毒软件查杀。

正常使用主观题需2.0以上版本雨课堂

作答







南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異

# Packed and Obfuscated Malware



允公允能 日新月异

# Packed and Obfuscated Malware

- Goals: Make malware more difficult to reverse engineering and detect
- Obfuscation: conceal execution information
- Packer: compress the size of binary file
  - a subset of obfuscation



南开大学  
Nankai University



允公允能 日新月异

# Packer and Obfuscation

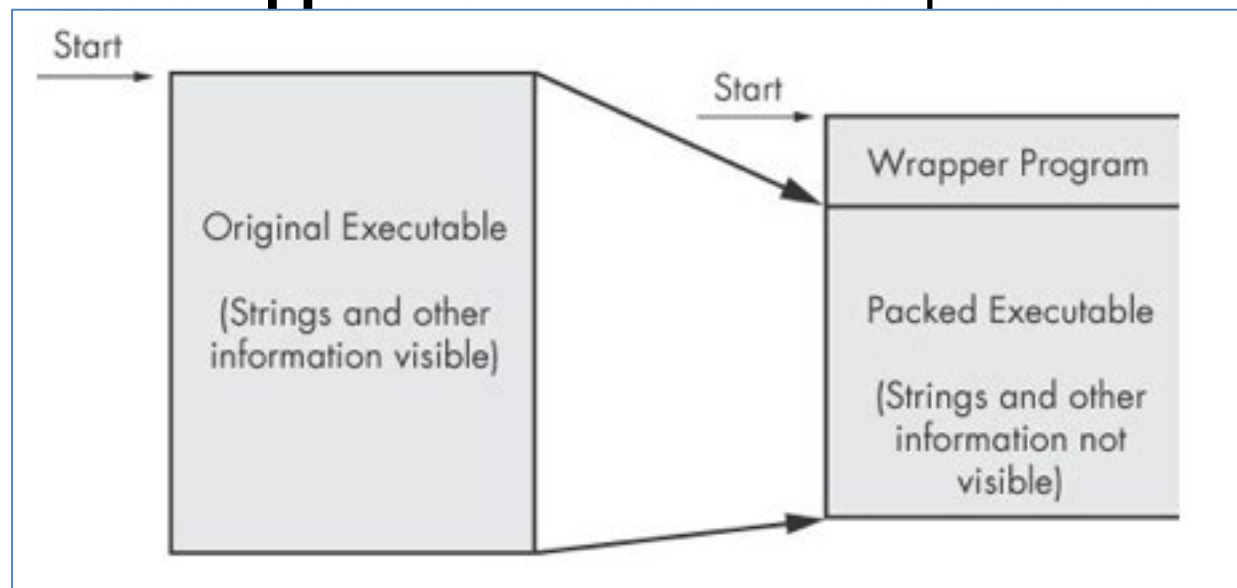
- Legitimate Program
  - Many strings
- Packed or Obfuscated Malware
  - few strings





# Packing Files

- The code is compressed, like a Zip or RAR file
- This makes the strings and instructions unreadable
- All you'll see is the **wrapper** – small code that unpacks the file when it is running





允公允能 日新月异

# Demo: UPX

```
root@kali: ~/126
File Edit View Search Terminal Help
root@kali:~/126# cat chatty.c
#include <stdio.h>
main()
{
char name[10];
printf("This program contains readable strings\n");
printf("Enter your name: ");
scanf("%s", name);
printf("Hello %s\n", name);
}

root@kali:~/126# gcc -static chatty.c -o chatty
root@kali:~/126# upx -o chatty-packed chatty
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2011
UPX 3.08      Markus Oberhumer, Laszlo Molnar & John Reiser   Dec 12th 2011

File size      Ratio      Format      Name
-----
592800 ->    272588    45.98%    linux/elf386    chatty-packed

Packed 1 file.
root@kali:~/126# ls -l
total 852
-rwxr-xr-x 1 root root 592800 Aug 16 20:34 chatty
-rw-r--r-- 1 root root 174 Aug 16 20:27 chatty.c
-rwxr-xr-x 1 root root 272588 Aug 16 20:34 chatty-packed
root@kali:~/126#
```



南开大学  
Nankai University

# Detecting Packers with PEiD

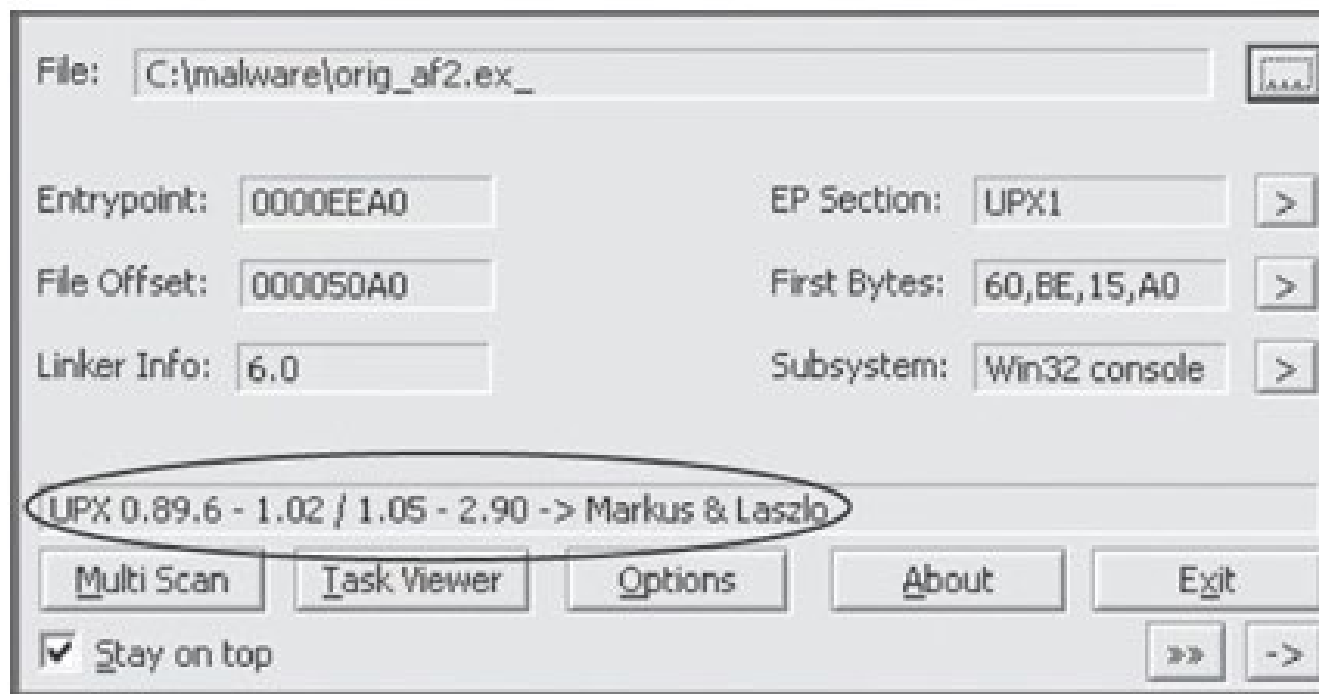


Figure 2-5. The PEiD program



允公允能 日新月异

# Packing Obfuscates Strings

```
root@kali:~/126# strings chatty | wc
1962    4498    33817
root@kali:~/126# strings chatty-packed | wc
3950    4290    23623
root@kali:~/126#
```



加壳技术和混淆技术有哪些作用？

- ☒ A Compress file size
- ☒ B Hide URL and IPs
- ☒ C Conceal significant strings
- ☐ D Change code behaviors

提交







## NOTE

*Many PEiD plug-ins will run the malware executable without warning! (See **Chapter 3** to learn how to set up a safe environment for running malware.) Also, like all programs, especially those used for malware analysis, PEiD can be subject to vulnerabilities. For example, PEiD version 0.92 contained a buffer overflow that allowed an attacker to execute arbitrary code. This would have allowed a clever malware writer to write a program to exploit the malware analyst's machine. Be sure to use the latest version of PEiD.*





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異



# Portable Executable File Format

文件头中有哪些信息可以作为恶意代码的特征？

作答



允公允能 日新月异

# PE Files

- Portable Executable File Format
- Used by Windows executable files, and DLLs
- Contains the information necessary for Windows to load the binary executable
- Almost every file executed on Windows is in PE format





允公允能 日新月异

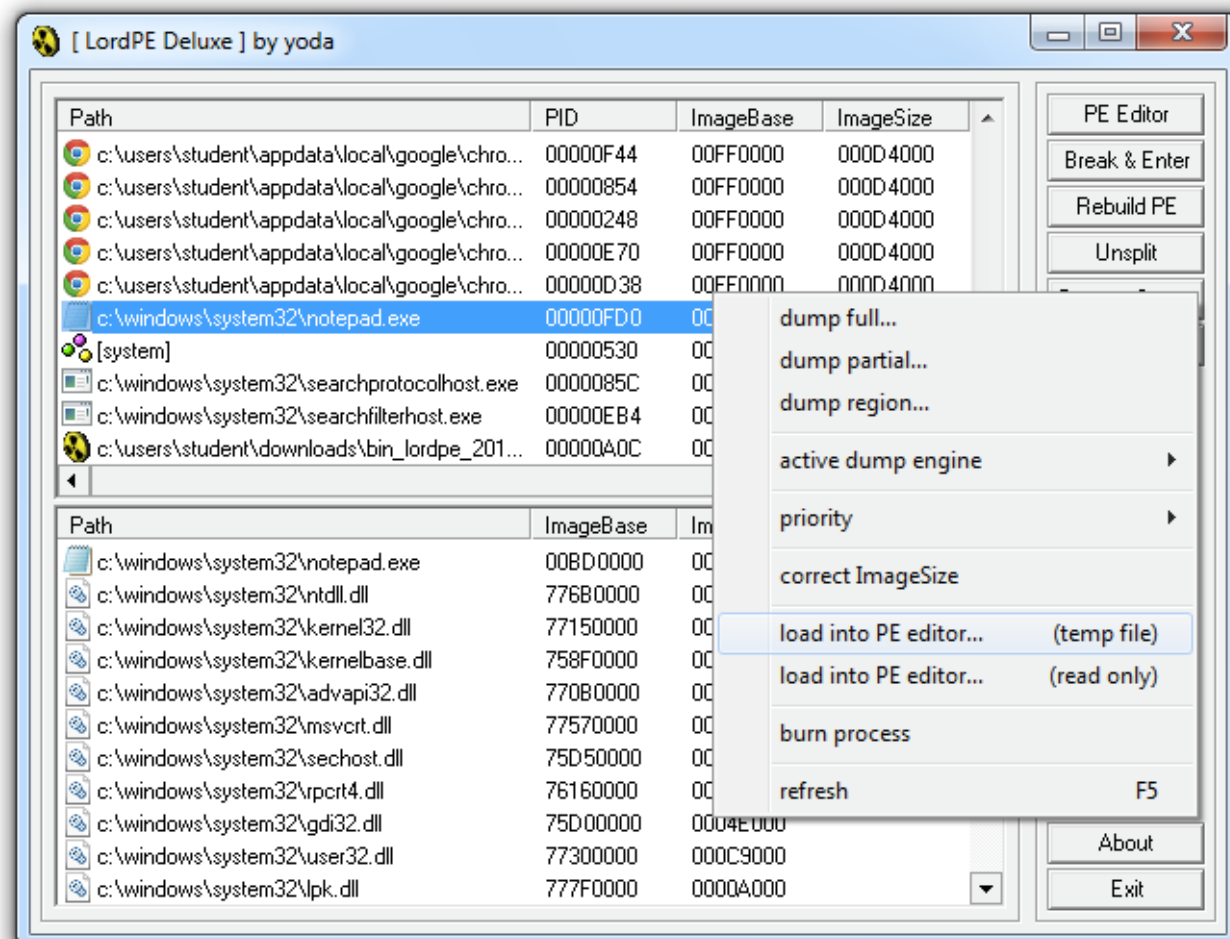
# PE Header

- Information about the code
- Type of application
- Required library functions
- Space requirements



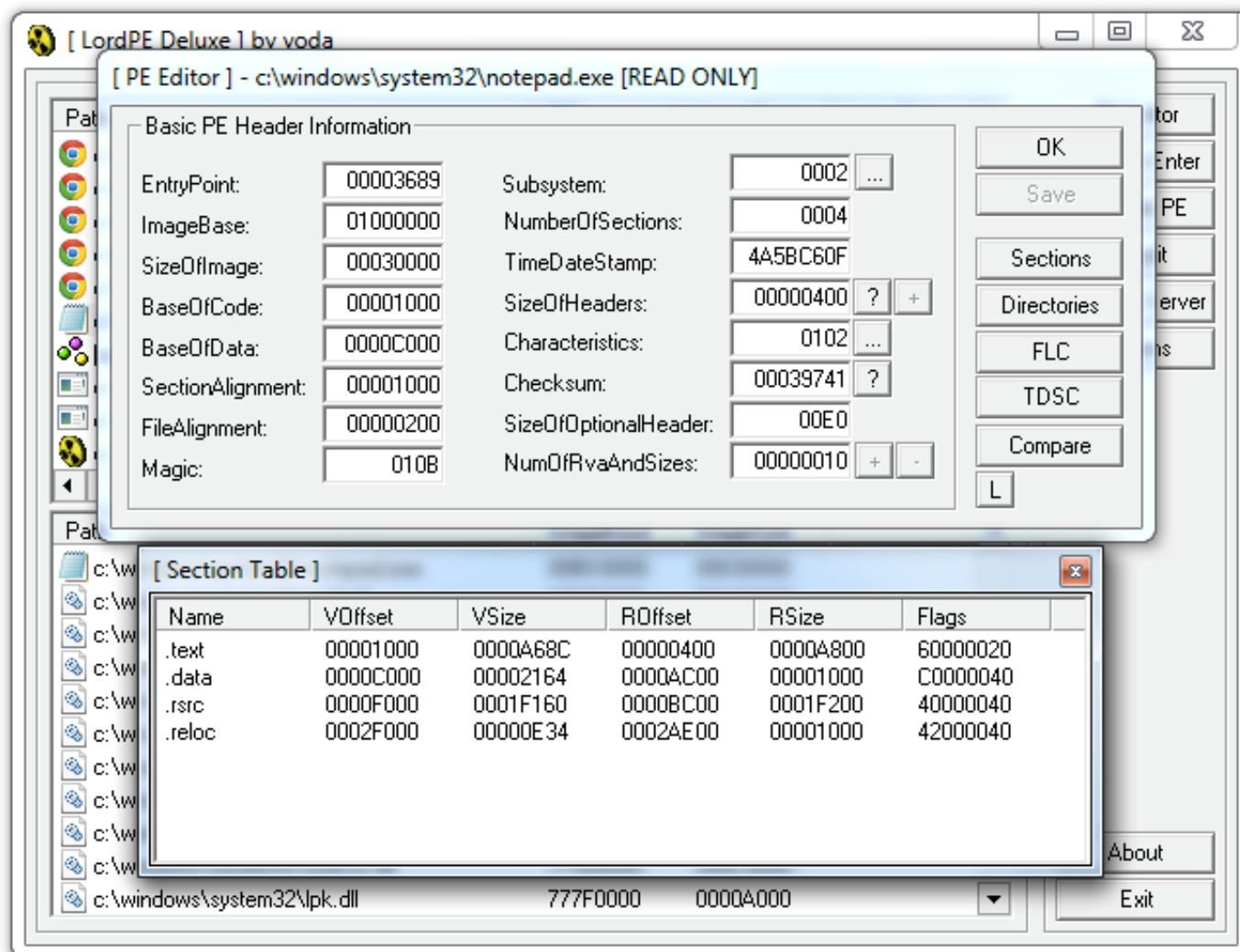
允公允能 日新月异

# LordPE Demo



允公允能 日新月异

# Main Sections



There are a lot more sections

- But the main ones are enough for now

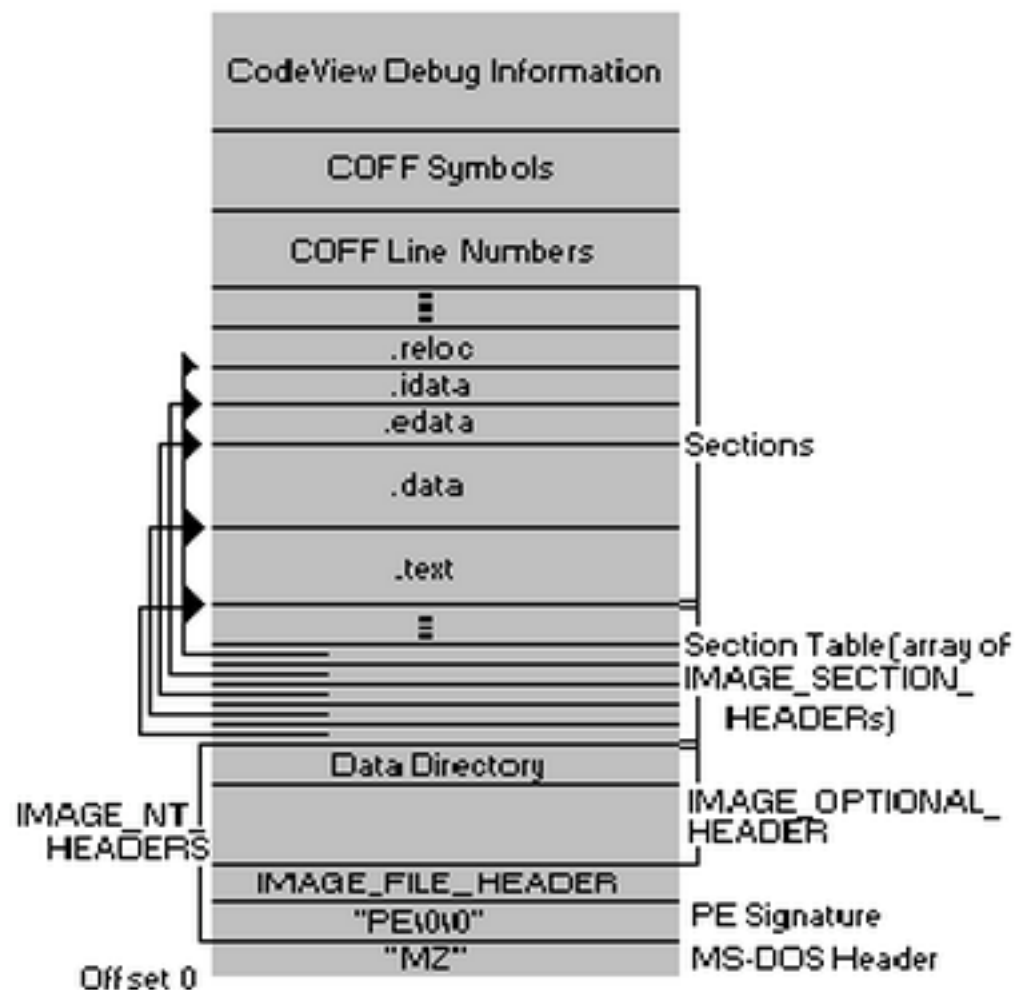


Figure 1. The PE file format



在PE文件头中可以提取到哪些信息？

- ☒ A Type of application
- ☒ B Required library functions
- ☒ C Space requirements
- ☒ D Code entry point

提交





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異

# Linked Libraries and Functions



允公允能 日新月异

# Imports

- Functions used by a program that are stored in a different program, such as library
- Connected to the main EXE by **Linking**
- Can be linked three ways
  - **Statically**
  - **At Runtime**
  - **Dynamically**





允公允能 日新月异

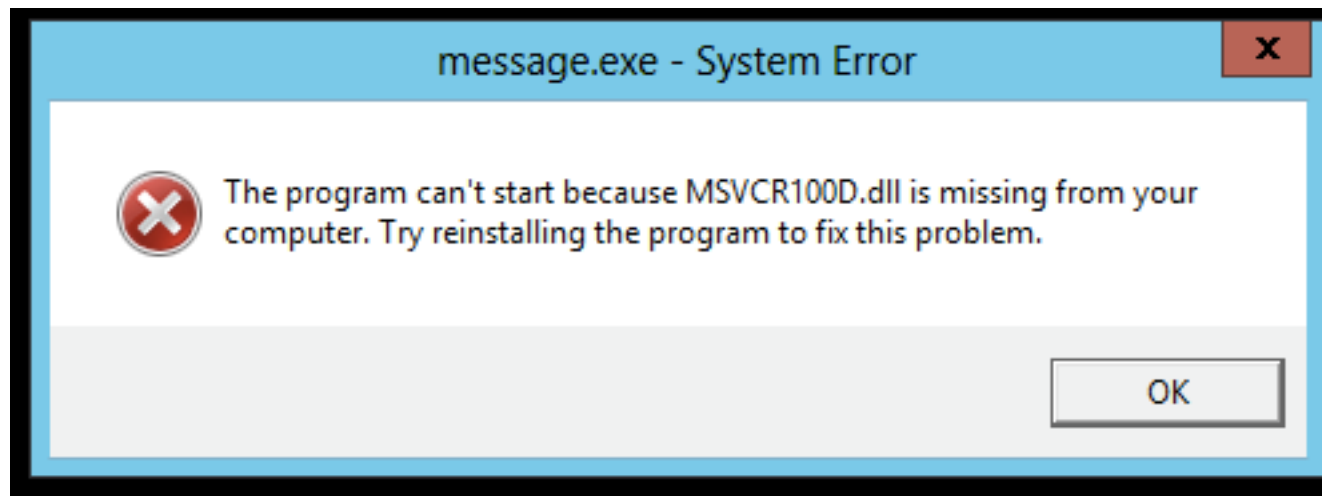
# Static Linking

- Rarely used for Windows executables
- Common in Unix and Linux
- All code from the library is copied into the executable
- Bigger file size
- More memory space



# Dynamic Linking

- Most common method
- Host OS searches for necessary libraries when the program is loaded





允公允能 日新月异

# Runtime Linking

- Unpopular in friendly programs
- Common in malware, especially packed or obfuscated malware
- Connect to libraries only when needed, not when the program starts
- Most commonly done with the **LoadLibrary** and **GetProcAddress** functions





允公允能 日新月异

# Clues in Libraries

- The PE header lists every library and function that will be loaded
- Their names can reveal what the program does
- **URLDownloadToFile** indicates that the program downloads something





库文件有哪些装载的方式?

- ☒ A Static
- ☒ B Runtime
- ☒ C Dynamic
- ☐ D Obfuacated

提交



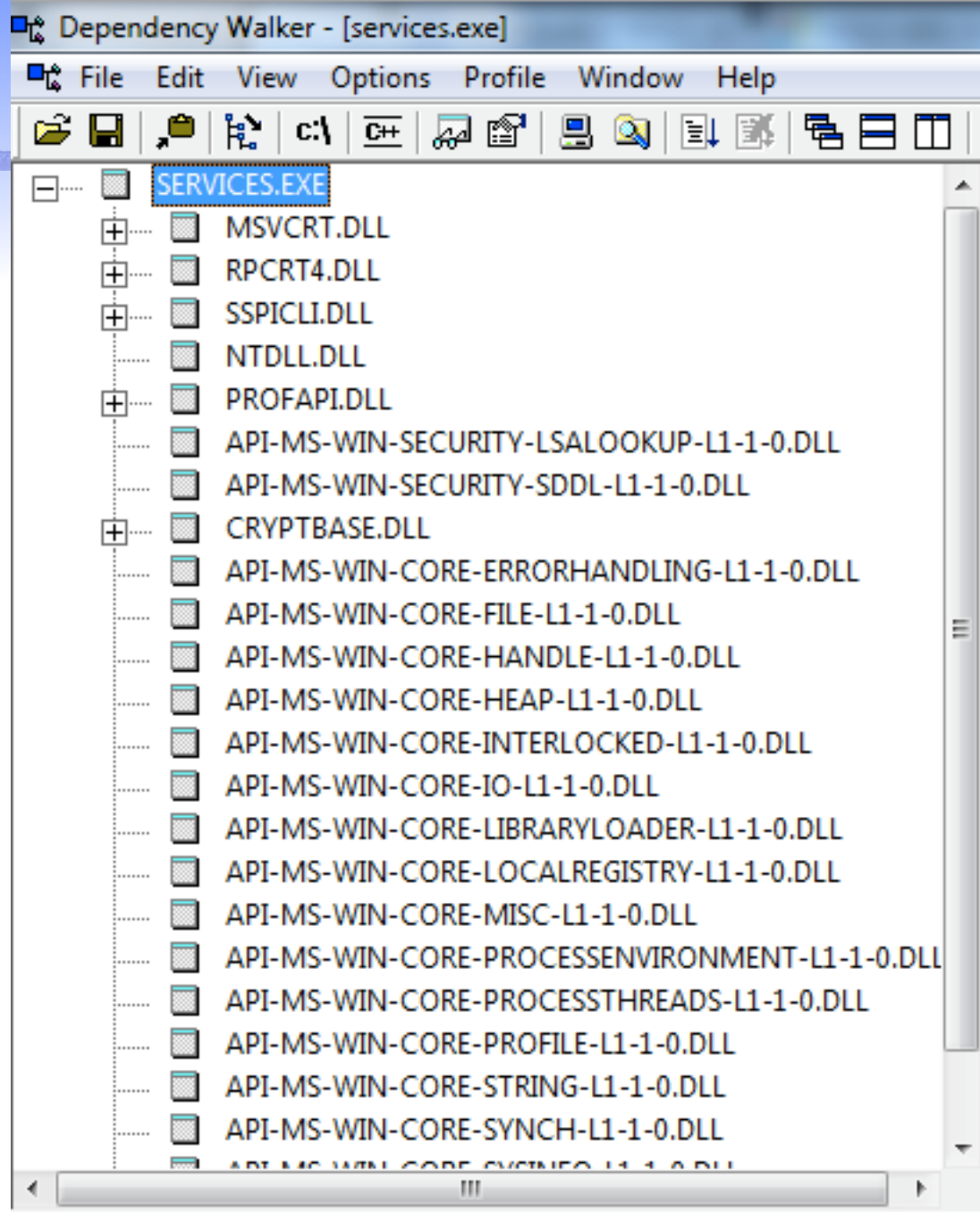


南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異

# Dependency Walker



Dependency Walker - [services.ex\_]

File Edit View Options Profile Window Help

Services.Ex\_ 1

- Kernel32.Dll 2
- WS2\_32.Dll

PI	Ordinal ^	Hint	Function	Entry Point
<input checked="" type="checkbox"/>	N/A	27 (0x001B)	CloseHandle	Not Bound
<input checked="" type="checkbox"/>	N/A	68 (0x0044)	CreateProcessA	Not Bound
<input checked="" type="checkbox"/>	N/A	125 (0x007D)	ExitProcess	Not Bound
<input checked="" type="checkbox"/>	N/A	385 (0x0181)	GlobalAlloc	Not Bound
<input checked="" type="checkbox"/>	N/A	392 (0x0188)	GlobalFree	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
<input checked="" type="checkbox"/>	1 (0x0001)	0 (0x0000)	ActivateActCtx	0x0000A6E4
<input checked="" type="checkbox"/>	2 (0x0002)	1 (0x0001)	AddAtomA	0x0003551D
<input checked="" type="checkbox"/>	3 (0x0003)	2 (0x0002)	AddAtomW	0x000326F1
<input checked="" type="checkbox"/>	4 (0x0004)	3 (0x0003)	AddConsoleAliasA	0x00071DFF

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem
ADVAPI32.DLL	02/09/2009 1:10p	02/09/2009 1:10p	617,472	A	0x000A5BB8	0x000A5BB8	x86	Console
KERNEL32.DLL	03/21/2009 3:06p	03/21/2009 3:06p	989,696	A	0x000FE572	0x000FE572	x86	Console
MSVCRT.DLL	04/14/2008 1:12a	04/14/2008 1:12a	343,040	A	0x00057341	0x00057341	x86	GUI
NTDLL.DLL	02/09/2009 1:10p	02/09/2009 1:10p	714,752	A	0x000BC674	0x000BC674	x86	Console

6

For Help, press F1



允公允能 日新月异

# Shows Dynamically Linked Functions

- Normal programs have a lot of DLLs
- Malware often has very few DLLs



南开大学  
Nankai University



*Table 2-1. Common DLLs*

DLL	Description
<i>Kernel32.dll</i>	This is a very common DLL that contains core functionality, such as access and manipulation of memory, files, and hardware.
<i>Advapi32.dll</i>	This DLL provides access to advanced core Windows components such as the Service Manager and Registry.
<i>User32.dll</i>	This DLL contains all the user-interface components, such as buttons, scroll bars, and components for controlling and responding to user actions.
<i>Gdi32.dll</i>	This DLL contains functions for displaying and manipulating graphics.





*Ntdll.dll*

This DLL is the interface to the Windows kernel. Executables generally do not import this file directly, although it is always imported indirectly by *Kernel32.dll*. If an executable imports this file, it means that the author intended to use functionality not normally available to Windows programs. Some tasks, such as hiding functionality or manipulating processes, will use this interface.

*WSock32.dll* and *Ws2\_32.dll* These are networking DLLs. A program that accesses either of these most likely connects to a network or performs network-related tasks.

*Wininet.dll* This DLL contains higher-level networking functions that implement protocols such as FTP, HTTP, and NTP.







允公允能 日新月异

# Exports

- DLLs **export** functions
- EXEs **import** functions
- Both exports and imports are listed in the PE header



南开大学  
Nankai University



S

Kernel32.dll	User32.dll	User32.dll (continued)
CreateDirectoryW	BeginDeferWindowPos	ShowWindow
CreateFileW	CallNextHookEx	ToUnicodeEx
CreateThread	CreateDialogParamW	TrackPopupMenu
DeleteFileW	CreateWindowExW	TrackPopupMenuEx
ExitProcess	DefWindowProcW	TranslateMessage
FindClose	DialogBoxParamW	UnhookWindowsHookEx
FindFirstFileW	EndDialog	UnregisterClassW
FindNextFileW	GetMessageW	UnregisterHotKey
GetCommandLineW	GetSystemMetrics	
GetCurrentProcess	GetWindowLongW	<b>GDI32.dll</b>
GetCurrentThread	GetWindowRect	GetStockObject
GetFileSize	GetWindowTextW	SetBkMode
GetModuleHandleW	InvalidateRect	SetTextColor
GetProcessHeap	IsDlgButtonChecked	
GetShortPathNameW	IsWindowEnabled	<b>Shell32.dll</b>
HeapAlloc	LoadCursorW	CommandLineToArgvW
HeapFree	LoadIconW	SHChangeNotify
IsDebuggerPresent	LoadMenuW	SHGetFolderPathW
MapViewOfFile	MapVirtualKeyW	ShellExecuteExW
OpenProcess	MapWindowPoints	ShellExecuteW
ReadFile	MessageBoxW	
SetFilePointer	RegisterClassExW	<b>Advapi32.dll</b>
WriteFile	RegisterHotKey	RegCloseKey
	SendMessageA	RegDeleteValueW
	SetClipboardData	RegOpenCurrentUser
	SetDlgItemTextW	RegOpenKeyExW
	SetWindowTextW	RegQueryValueExW
	SetWindowsHookExW	RegSetValueExW

e





允公允能 日新月异

# Ex: A Packed Program

*Table 2-3. DLLs and Functions Imported from PackedProgram.exe*

Kernel32.dll	User32.dll
GetModuleHandleA	MessageBoxA
LoadLibraryA	
GetProcAddress	
ExitProcess	
VirtualAlloc	
VirtualFree	



下面哪些函数可以被加壳代码用来动态加载其它的API函数?

- ☒ A LoadLibrary
- ☒ B GetProcAddress
- ☐ C FindFirstFile
- ☐ D ShowWindow



南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異



# The PE File Headers and Sections



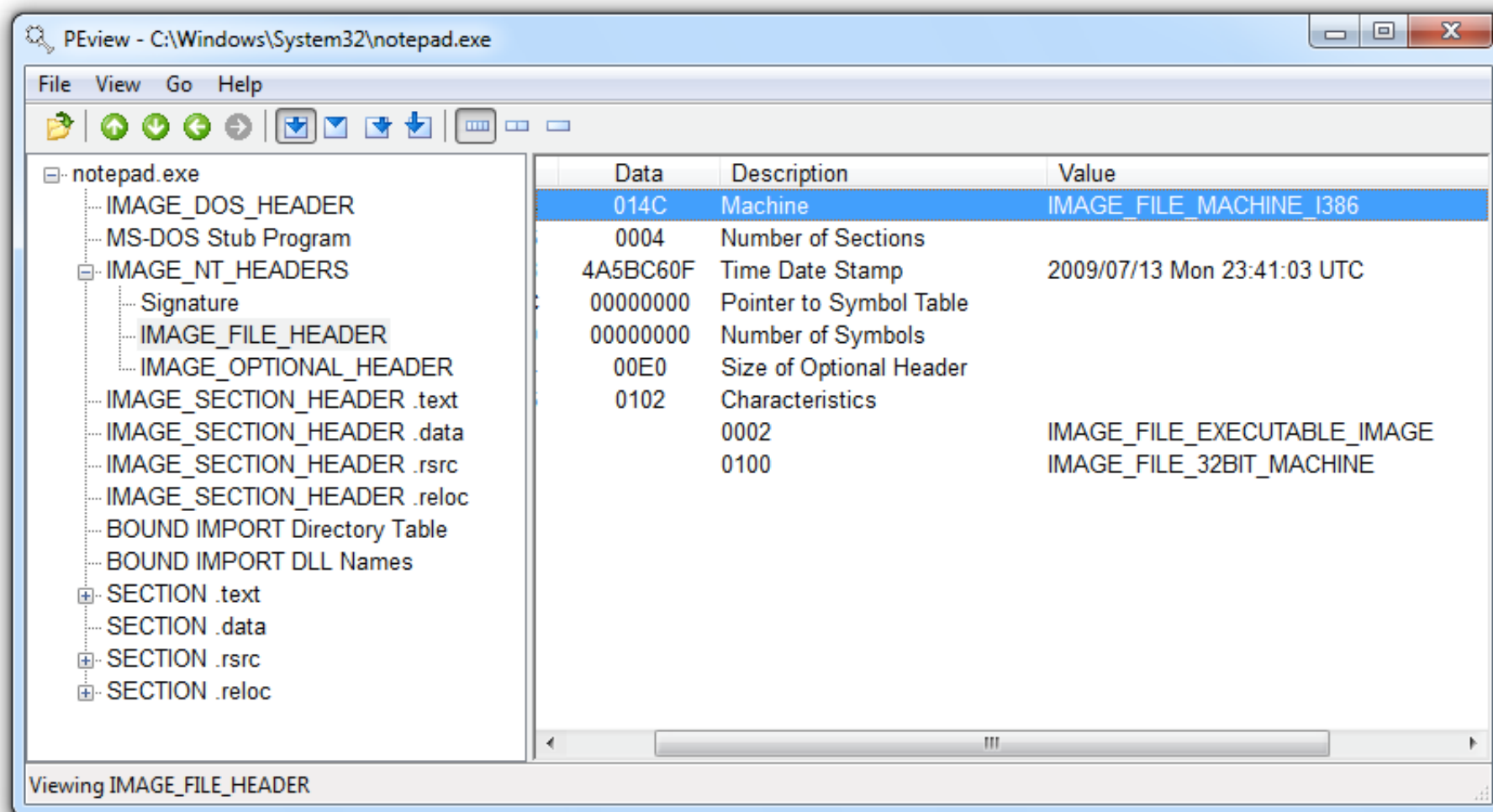
允公允能 日新月异

# Important PE Sections

- **.text** -- instructions for the CPU to execute
- **.rdata** -- imports & exports
- **.data** – global data
- **.rsrc** – strings, icons, images, menus



# PEView



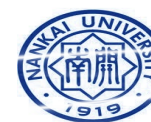




允公允能 日新月异

# Time Date Stamp

- Shows when this executable was compiled
- Older programs are more likely to be known to antivirus software
- But sometimes the date is wrong
  - All Delphi programs show June 19, 1992
  - Date can also be faked



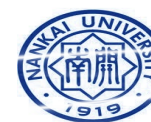


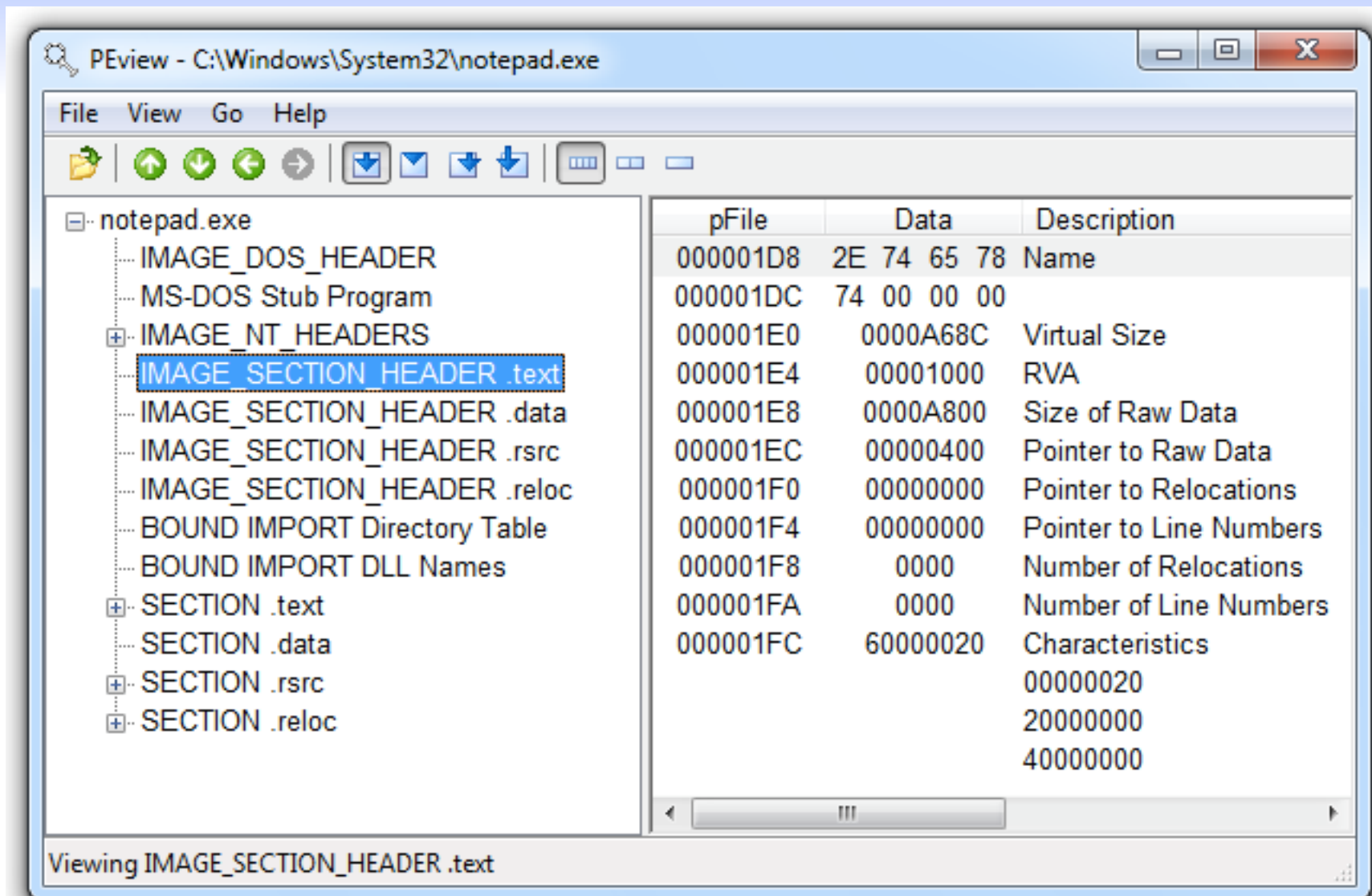


允公允能 日新月异

# IMAGE\_SECTION\_HEADER

- Virtual Size – RAM
- Size of Raw Data – DISK
- For **.text** section, normally equal, or nearly equal
- Packed executables show Virtual Size much larger than Size of Raw Data for **.text** section







*Table 2-6. Section Information for PackedProgram.exe*

Name	Virtual size	Size of raw data
.text	A000	0000
.data	3000	0000
.rdata	4000	0000
.rsrc	19000	3400
Dijfpds	20000	0000
.sdfuok	34000	3313F
Kijijl	1000	0200





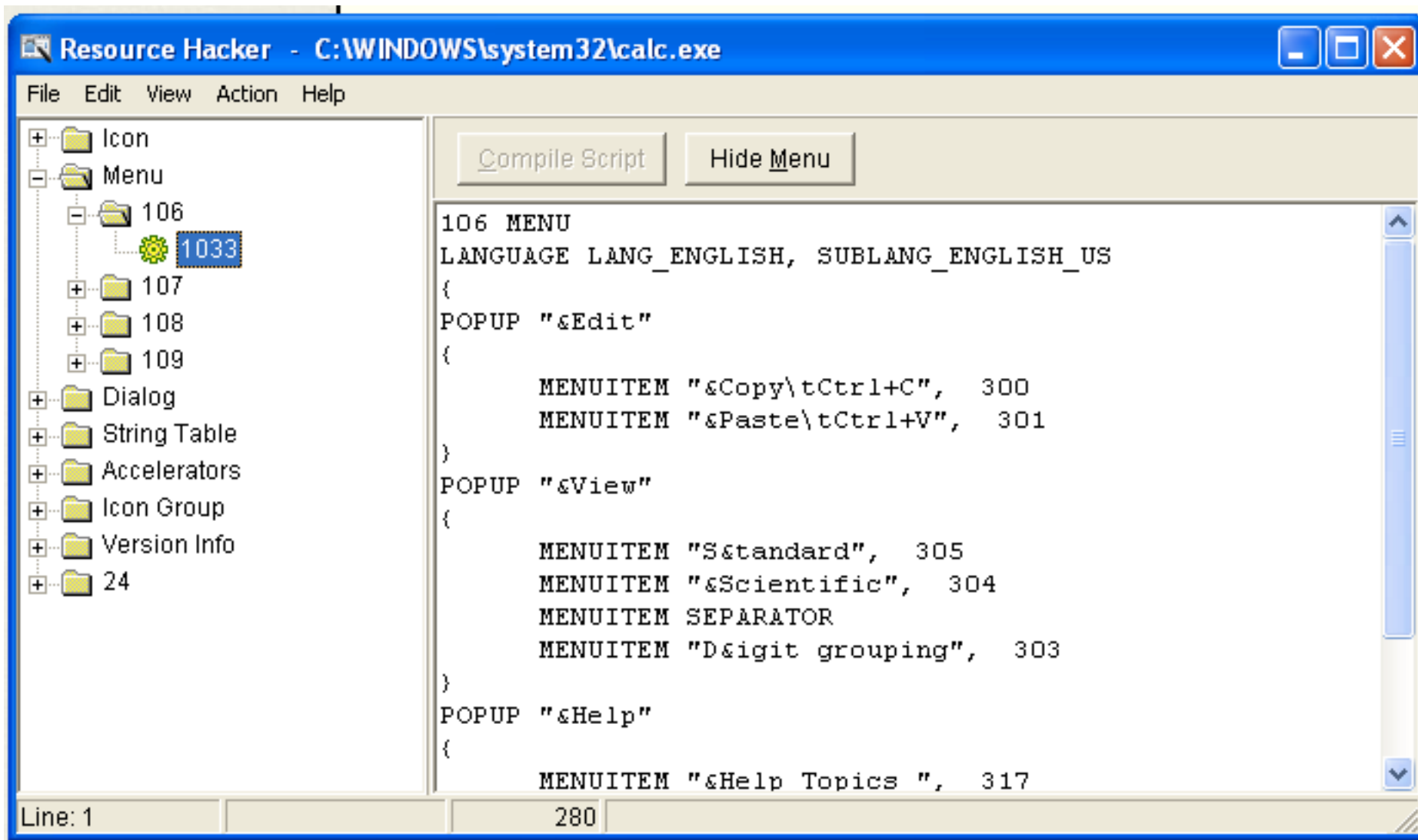
允公允能 日新月异

# Resource Hacker

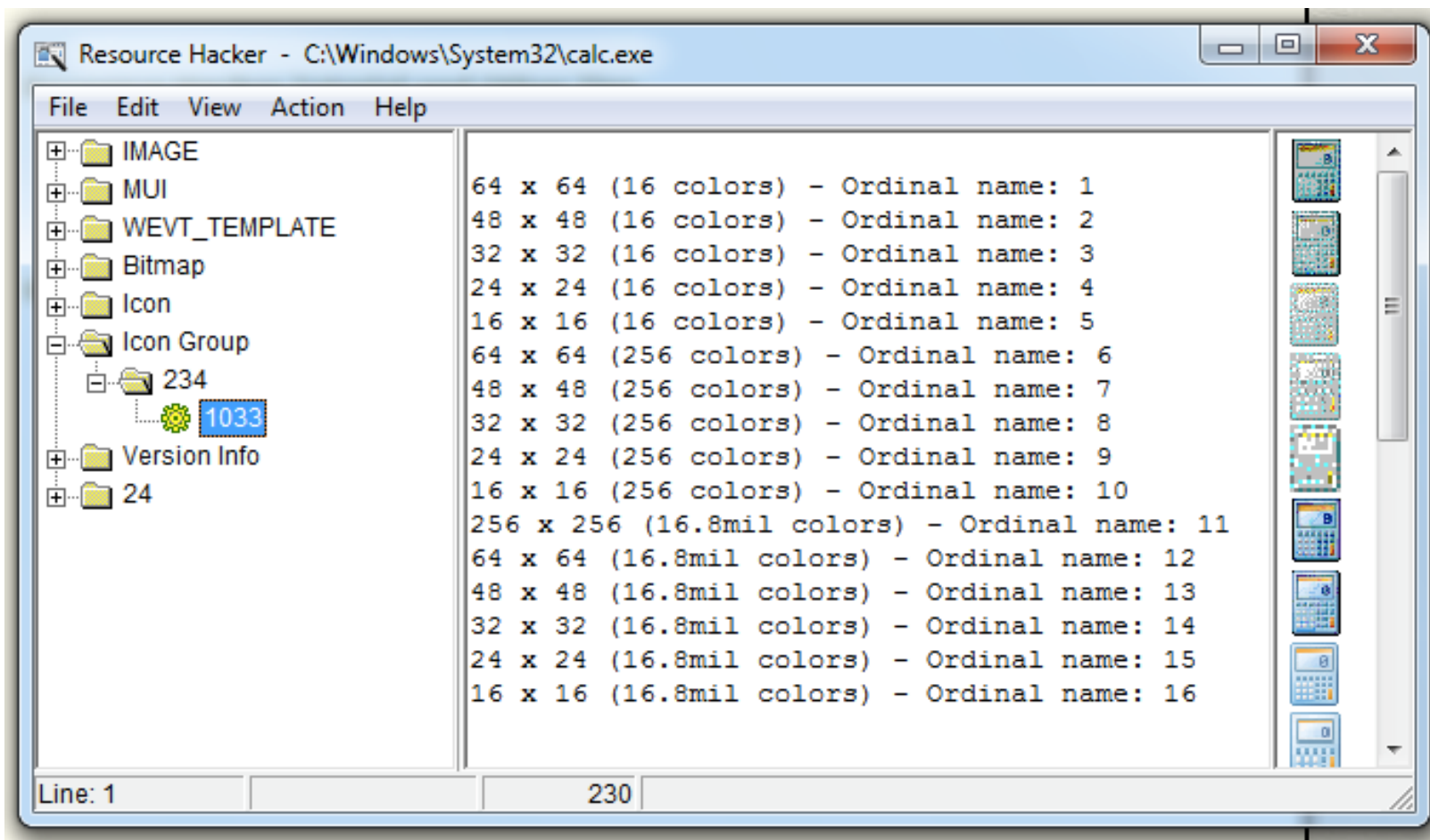
- Lets you browse the **.rsrc** section
- Strings, icons, and menus



# Resource Hacker in Windows XP



# Resource Hacker in Windows 7





允公允能 日新月异

# Labs

- Practice our skills
- In order to simulate realistic malware analysis, little or no information about the program is given.
  - generic names
  - meaningless or misleading names



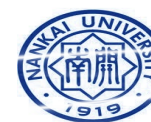




允公允能 日新月异

# Labs

- Each lab consists
  - a malicious file
  - a few questions
  - short answers to the questions
  - a detailed analysis of the malware
- The solutions are included in Appendix C





允公允能 日新月异

# Lab 1 - 1

This lab uses the files *Lab01-01.exe* and *Lab01-01.dll*. Use the tools and techniques described in the chapter to gain information about the files and answer the questions below.

## Questions

1. Upload the files to <http://www.VirusTotal.com/> and view the reports. Does either file match any existing antivirus signatures?
2. When were these files compiled?
3. Are there any indications that either of these files is packed or obfuscated? If so, what are these indicators?
4. Do any imports hint at what this malware does? If so, which imports are they?
5. Are there any other files or host-based indicators that you could look for on infected systems?
6. What network-based indicators could be used to find this malware on infected machines?
7. What would you guess is the purpose of these files?



允公允能 日新月异

# Lab 1-2

## Questions

1. Upload the *Lab01-02.exe* file to <http://www.VirusTotal.com/>. Does it match any existing antivirus definitions?
2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.
3. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
4. What host- or network-based indicators could be used to identify this malware on infected machines?



南开大学  
Nankai University



允公允能 日新月异

# Lab 1-3

Analyze the file *Lab01-03.exe*.

## Questions

1. Upload the *Lab01-03.exe* file to <http://www.VirusTotal.com/>. Does it match any existing antivirus definitions?
2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.
3. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
4. What host- or network-based indicators could be used to identify this malware on infected machines?



允公允能 日新月异

# Lab 1- 4

Analyze the file *Lab01-04.exe*.

## Questions

1. Upload the *Lab01-04.exe* file to <http://www.VirusTotal.com/>. Does it match any existing antivirus definitions?
2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.
3. When was this program compiled?
4. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
5. What host- or network-based indicators could be used to identify this malware on infected machines?
6. This file has one resource in the resource section. Use Resource Hacker to examine that resource, and then use it to extract the resource. What can you learn from the resource?





允公允能 日新月异

# 实验报告提交

- 实验报告以附件的形式在雨课堂上提交。







南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异

恶意代码分析与防治技术

## 第2章 基本静态分析技术

王志

zwang@nankai.edu.cn

南开大学 网络空间安全学院

2023-2024学年