Malware Analysis Lab Configuration

NCI Post Graduate Diploma Cyber Security
Semester 1

Author: Jonathon Taaffe

Title: Malware Analysis Lab Configuration
Author: Jonathon Taaffe
Copyright© 2020 Jonathon Taaffe

All rights reserved. This publication is protected by copyright, and permission must be obtained from the author prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this publication, the author assumes no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

Warning and Disclaimer
The information is provided on an “as is” basis. The author shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this publication. The opinions expressed in this publication belong to the author.

Trademark Acknowledgments
All terms mentioned in this publication that are known to be trademarks or service marks have been appropriately capitalised. The author cannot attest to the accuracy of this information. Use of a term in this publication should not be regarded as affecting the validity of any trademark or service mark.

Contents

Malware Analysis Lab Configuration

Malware Analysis Utilities Selection

As detailed in Lecture 'Malware Types & Lab Setups File'[1], Gateway OS https://REMnux.org [2] was documented as a Linux Toolkit for Reverse-Engineering and Analyzing Malware.

Virtual Network Configuration

Oracle VirtualBox[3] was chosen as the virtual platform for the Malware Analysis Lab.

VirtualBox NATNetwork

NATNetwork configured with DHCP range of 10.0.2.0/24 for initial VM install, update and configuration.

VirtualBox Host-Only Adapter

Host-Only connection configured from File Server to local host to allow for initial file transfer from local host to clients on the isolated Internal Network.

VirtualBox Internal Network

Isolated Internal Network called 'malware-analysis-network01' was configured which VM's would connect to once fully installed and configured. As DHCP services would not be available on the Internal Network, and to easily identify VM's connected to the Internal Network by IP, static IP addresses were assigned as follows:

Category	Type	Interface	Adapter	IP Range
Utilities	File Server	LAN	Host-Only Adapter	192.168.202.10
Utilities	File Server	LAN	Internal Network	10.0.0.10-19/24
Utilities	Malware Analysis	LAN	Internal Network	10.0.0.20-29/24
Client	XP	LAN	Internal Network	10.0.0.60-69/24
Client	Windows 7	LAN	Internal Network	10.0.0.70-79/24
Client	Windows 8	LAN	Internal Network	10.0.0.80-89/24
Client	Windows 10	LAN	Internal Network	10.0.0.100-109/24

Table 1. malware-analysis-network01 Static Assignments[4]

[1] Malware Types & Lab Setups File (2019) *Gateway OS Slide 24* https://moodle.ncirl.ie/mod/resource/view.php?id=59717 [Accessed 1st July 2019].
[2] REMnux.org (2019) *REMnux: A Linux Toolkit for Reverse-Engineering and Analyzing Malware* https://remnux.org/ [Accessed 1st July 2019].
[3] VirtualBox.org (2019) *VirtualBox* https://www.virtualbox.org/ [Accessed 1st July 2019].
[4] Jonathon Taaffe (2019) *Table 1. malware-analysis-network01 Static Assignments* [Created 1st July 2019].

Utilities VM Configuration

File Transfer: Windows Server 2016[5] File Server

With Automatic Windows Updates, Virus Protection and Windows Firewall disabled on the clients on which Malware was going to run, Internet connectivity from these clients was not an option. To facilitate the transfer of required Application Source files as documented in Lecture 'Malware Types & Lab Setups File'[6] ,a Windows Server 2016 File Server was installed and configured.

This File Server had 2 Network Adapters configured, a Host-Only Adapter with a static IP assigned and an Internal Network static IP assigned. This facilitated downloading the required Application Source files from the Internet to local host, transferring the files to the File Server over the Host-Only adapter and allowed the clients to connect to the File Server from the Internal Network and download the required files.

Once all Application Source files had been copied to the clients, the File Server will be powered off to ensure the Internal Network is fully isolated. Summary of the File Server VM configuration is as follows:

Name	WS2016-File-Server01		
Type	Microsoft		
Version	Windows 2016 (64-bit)		
RAM	2048MB		
Disk	VDI Dynamic		
Disk Size	C:50GB D:50GB		
Network Details	Initial VM Install	Upload from Host	Transfer to Clients
Adapter Number	01	01	02
Adapter	NATNetwork	Host-Only Adapter	Internal Network
Network	NATNetwork	Host-Only Adapter	malware-analysis-network01
Type	Intel PRO/1000MT	Intel PRO/1000MT	Intel PRO/1000MT
MAC	08:00:27:63:60:FB	08:00:27:18:93:FF	08:00:27:13:9B:15
IP	DHCP	192.168.202.10	10.0.0.20
Share Name	n/a	mw_client_files	mw_client_files
Share Location	n/a	D:\mw_client_files	D:\mw_client_files
Share Account	n/a	Administrator	MWUser01
Share Permissions	n/a	Full	Read

Table 2. Windows Server 2016 File Server VM Configuration[7]

Configuring File and Storage Services[8]

Added the File and Storage Services\ File Server Role and created a new SMB Share Quick as follows:

Share Name: MW_Client_Files
Share Settings: Enable Access-Based Enumeration
Specify Permissions: WS2016_File_Server\mwclient

---

[5] Portal.Azure.com (2019) *Windows Server 2016 Standard* http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso [Accessed 1st July 2019].
[6] Malware Types & Lab Setups File (2019) *Tools Slide 28* https://moodle.ncirl.ie/mod/resource/view.php?id=59717 [Accessed 1st July 2019].
[7] Jonathon Taaffe (2019) *Table 2. Windows Server 2016 File Server VM Configuration* [Created 1st July 2019].
[8] Tecting (2019) *How to Share Files and Folders in Windows Server 2016* https://www.tactig.com/share-files-folders-windows-server-2016/ [Accessed 1st July 2019].

Malware Analysis Utilities

As detailed in Lecture 'Malware Types & Lab Setups File' Gateway OS – REMnux[9] and FakeNet-NG[10] were recommended for Malware Analysis. Both Malware Analysis Utilities were installed and configured in the Malware Lab allowing for analysis from 2 different platforms. To use these utilities, the TCP/IP Gateway IP of the victim clients needs to be set to the static IP of the analysis utility as follows

Utility	Static IP
Gateway OS – REMnux	10.0.0.20
FakeNet-NG	10.0.0.21

Table 3. Malware Analysis Utilities Static IP Assignment[11]

Gateway OS – REMnux VM Configuration

Downloaded REMnux Virtual Appliance OVA[12] and connected it to the NATNetwork for initial appliance install, update and configuration. Successfully updated using the '`update-remnux full`' command.

Once the VM was updated and operational, the VM's network connection was changed to the isolated Internal Network 'malware-analysis-network01' and set a static IP address of 10.0.0.20/24 with no Gateway specified. Summary of the Gateway OS – REMnux VM configuration is as follows:

Name	Remnux Gateway OS	
Type	Linux	
Version	Ubuntu 14.04 (64-bit)	
RAM	1024MB	
Disk	VDI Dynamic	
Disk Size	25GB	
Network Details	Initial Install and Configuration	Isolated Network
Adapter 1	NATNetwork	Internal Network
Adapter 1 Network	NATNetwork	malware-analysis-network01
Adapter 1 Type	Intel PRO/1000MT Server (82545EM)	Intel PRO/1000MT Server (82545EM)
Adapter 1 MAC	08:00:27:93:01:19	08:00:27:93:01:19
Adapter 1 IP	DHCP	10.0.0.20

Table 4. Gateway OS – REMnux VM Configuration[13]

[9] Malware Types & Lab Setups File (2019) *Gateway OS Slide 24* https://moodle.ncirl.ie/mod/resource/view.php?id=59717 [Accessed 1st July 2019].
[10] Malware Types & Lab Setups File (2019) *FakeNet-NG Slide 25* https://moodle.ncirl.ie/mod/resource/view.php?id=59717 [Accessed 1st July 2019].
[11] Jonathon Taaffe (2019) *Table 3. Malware Analysis Utilities Static IP Assignment* [Created 1st July 2019].
[12] REMnux 6.0 OVA Public (2019) *remnux-6.0-ova-public.ova (2.0G)* https://docs.google.com/uc?id=0B6fULLT_NpxMampUWlBCQXVJZzA&export=download [Accessed 01/07/2019].
[13] Jonathon Taaffe (2019) *Table 4. Gateway OS – REMnux VM Configuration* [Created 1st July 2019].

FakeNet-NG VM Configuration[14]

Downloaded Ubuntu 18.04 ISO and installed a new VM connected to the NATNetwork for initial appliance install, update and configuration as per the following VM configuration:

Name	FakeNet-NG	
Type	Linux Ubuntu (64-bit)	
RAM	1024MB	
Disk	VDI Dynamic	
Disk Size	50GB	
Network Details	Initial Install and Configuration	Isolated Network
Adapter 1	NATNetwork	Internal Network
Adapter 1 Network	NATNetwork	malware-analysis-network01
Adapter 1 Type	Intel PRO/1000MT Server (82545EM)	Intel PRO/1000MT Server (82545EM)
Adapter 1 MAC	08:00:27:65:65:4F	08:00:27:65:65:4F
Adapter 1 IP	DHCP	10.0.0.21

Table 5. FakeNet-NG VM Configuration[15]

FakeNet-NG Installation – Pre-Requisites[16]

Completed an `apt-get update` and `apt-get upgrade` and installed all FakeNet-NG prerequisites including:

Package	Command
Git package manager	apt install git
Python 2.7 pip package manager	apt install python-pip
Python file transfer package	pip install pysendfile
Python FPTS package	pip install pyopenssl
Python 2.7 development files	apt install python-dev
OpenSSL development files	apt install libssl-dev
libffi development files	apt install libffi-dev
libnetfilterqueue development files	apt install libnetfilter-queue-dev

Table 6. FakeNet-NG Pre-Requisites[17]

FakeNet-NG Installation – Installation[18]

Once all pre-requisites were installed, fakenet-ng was cloned into the /opt directory and python installer run as follows:

```
fakenet@FakeNet-NG:/$ cd /opt
fakenet@FakeNet-NG:/opt$ git clone https://github.com/fireeye/flare-fakenet-ng/
fakenet@FakeNet-NG:/opt$ cd flare-fakenet-ng
fakenet@FakeNet-NG:/opt/flare-fakenet-ng$ python setup.py install
```

Network Adapter changed to Internet Network 'malware-analysis-network01' and configured a static IP address of 10.0.0.21/24 with no Gateway specified.

---

[14] FireEye/Flare-FakeNet-NG (2019) *FakeNet-NG - Next Generation Dynamic Network Analysis Tool* https://github.com/fireeye/flare-fakenet-ng [Accessed 1st July 2019].
[15] Jonathon Taaffe (2019) *Table 5. Gateway OS – REMnux VM Configuration* [Created 1st July 2019].
[16] FireEye/Flare-FakeNet-NG (2019) *FakeNet-NG - Next Generation Dynamic Network Analysis Tool* https://github.com/fireeye/flare-fakenet-ng [Accessed 1st July 2019].
[17] Jonathon Taaffe (2019) *Table 6. FakeNet-NG Pre-Requisites* [Created 1st July 2019].
[18] FireEye/Flare-FakeNet-NG (2019) *FakeNet-NG - Next Generation Dynamic Network Analysis Tool* https://github.com/fireeye/flare-fakenet-ng [Accessed 1st July 2019].

Client Configuration

Client VM Configuration

As the vast majority of today's malware is written for Microsoft Windows Operating Systems and to allow Malware testing on a variety of clients, 32bit versions of Windows XP, Windows 7, Windows 8.1 and Windows 10[19] were chosen as the victim clients.

As these client VM's were being installed with Automatic Windows Updates, Virus Protection and Windows Firewall disabled, they were installed and configured connected to the isolated Internal Network 'malware-analysis-network01'. VM configurations as follows:

Client	WindowsXP-01	Windows7-01	Windows8-01	Windows10-01
Type	Microsoft Windows			
OS Version	Windows XP 32bit	Windows 7 Pro 32bit	Windows 8 32bit	Windows 10 32bit
OS Build	5.1.2600 SP3	6.1.7601 SP1	6.3.9600	10.0.10240
RAM	1024MB			
Disk	VDI Dynamic			
Disk Size	50GB			
Adapter 1	Internal Network			
Network	malware-analysis-network01			
MAC	08:00:27:D2:93:84	08:00:27:1E:0F:51	08:00:27:1A:2E:5A	08:00:27:A7:A7:32
IP	10.0.0.60	10.0.0.70	10.0.0.80	10.0.0.100
Subnet	255.255.255.0			
Gateway	10.0.0.20 (Remnux Gateway OS)			

Table 7. Windows XP, 7, 8.1 and 10 VM Client Configuration[20]

Client Network Configuration

To ensure the Windows Clients were optimally configured for TCP/IPv4 on the malware-analysis-network01, the following network settings were configured:

Client	WindowsXP-01	Windows7-01	Windows8.1-01	Windows10-01
Client for MS Networks	Enabled			
QoS Packet Scheduler	Enabled			
TCP/IPv4	Enabled			
Register connection in DNS	Disabled			
Enable LMHOSTS Lookup	Disabled			
Disable NetBIOS over TCPIP	Selected			
Microsoft ISATAP Adapter	Disabled			
ISATAP Adapter	Uninstalled from Device Manager			
ISATAP Adapter Disabled	netsh interface isatap set state disabled			

Table 8. Windows XP, 7, 8.1 and 10 Network Configuration[21]

[19] Microsoft.com (2019) *Download Virtual Machines* https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/ [Accessed 2nd July 2019].
[20] Jonathon Taaffe (2019) *Table 7. Windows XP, 7, 8.1 and 10 VM Client Configuration* [Created 2nd July 2019].
[21] Jonathon Taaffe (2019) *Table 8. Windows XP, 7, 8.1 and 10 Network Configuration* [Created 2nd July 2019].

Client OS Configuration

To ensure the clients were optimally configured as per Lecture 'Malware Types & Lab Setups File'[22] and are ready for malware analysis, the following OS settings were configured:

Client	WindowsXP-01	Windows7-01	Windows8-01	Windows10-01
Automatic Updates	Off			
Virus Protection	n/a	Off	Off	Off
Windows Firewall	Off			
User Account Control	n/a	Off	Off	Off
Show File Extensions	Enabled			
Show Hidden Files	Enabled			
Disable Zone Checking*	Configured			
CMD Shortcut on Desktop	Configured			
c:\tools\bin Created	Configured			
c:\tools\bin added to %PATH%	Configured			

Table 9. Windows XP, 7, 8.1 and 10 OS Configuration[23]

***Note on Disabling Internet Explorer Zone Checking[24]:** To disable Zone Checking in Internet Explorer add the following Windows registry keys:

reg add "HKCU\Environment" /V SEE_MASK_NOZONECHECKS /T REG_SZ /D 1 /F

reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1" /v "Flags" /t REG_DWORD /d 219 /f

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment" /V SEE_MASK_NOZONECHECKS /T REG_SZ /D 1 /F

[22] Malware Types & Lab Setups File (2019) *FakeNet-NG Slide 25* https://moodle.ncirl.ie/mod/resource/view.php?id=59717 [Accessed 2nd July 2019].
[23] Jonathon Taaffe (2019*) Table 9. Windows XP, 7, 8.1 and 10 OS Configuration* [Created 2nd July 2019].
[24] Microsoft.com (2019) *Internet Explorer security zones registry entries for advanced users* https://support.microsoft.com/en-us/help/182569/internet-explorer-security-zones-registry-entries-for-advanced-users [Accessed 2nd July 2019].

Malware Analysis Lab Environment Configuration

Phase 1 Installation and Configuration

The following diagram details Phase 1 configuration of the Malware Analysis Lab which includes the Windows Server 2016[25] File Server, Gateway OS – REMnux[26] and FakeNet-NG[27] Malware Analysis Utilities and Windows XP, 7, 8.1 and 10[28] Clients network Configuration.

This configuration allows for:

1. OS install, update and configuration of the File Server and Malware Analysis Utility VM's
2. OS install and configuration of the Windows clients

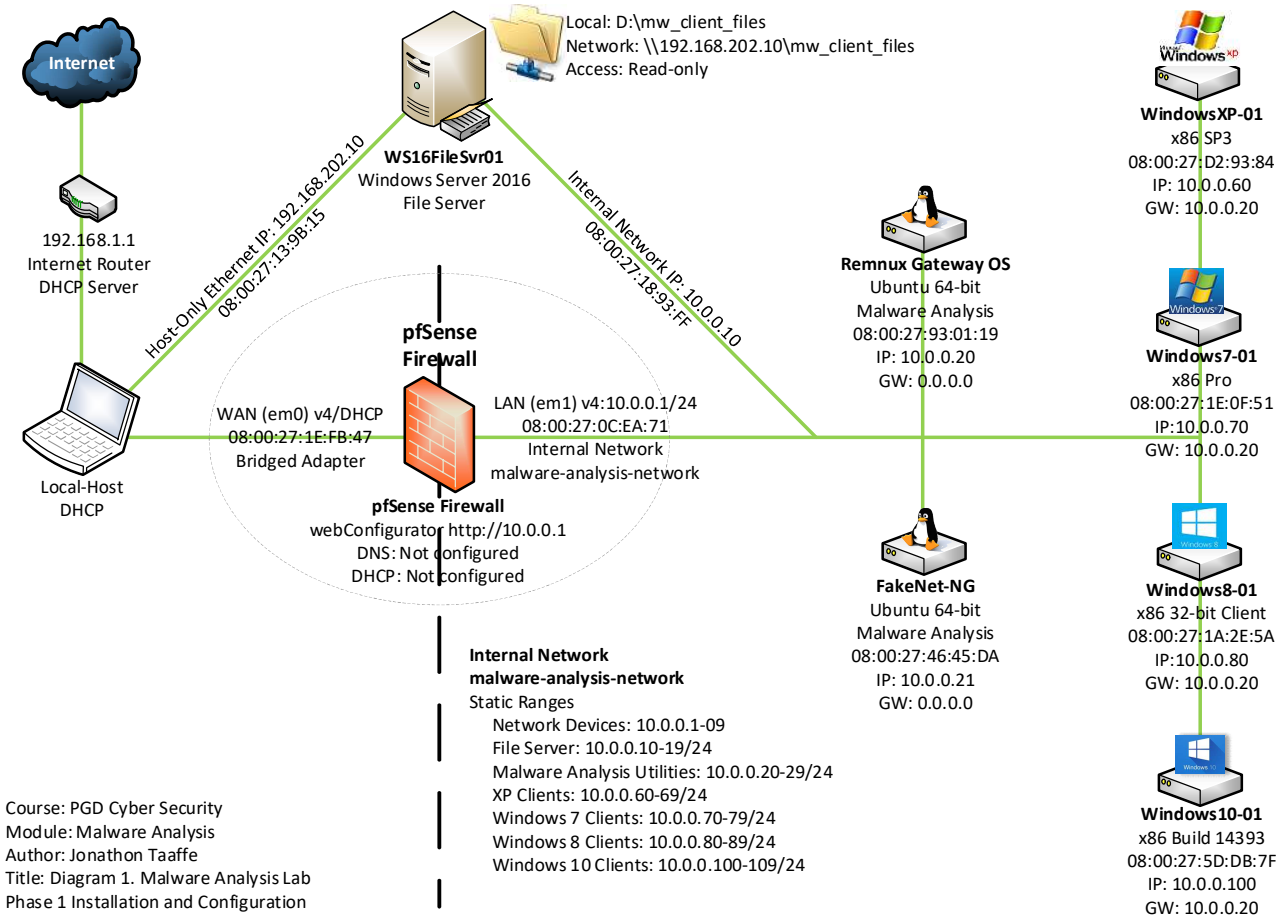


Diagram 1. Malware Analysis Lab Phase 1 Installation and Configuration [29]

[25] Portal.Azure.com (2019) *Windows Server 2016 Standard* http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso [Accessed 2nd July 2019].
[26] REMnux 6.0 OVA Public (2019) *remnux-6.0-ova-public.ova (2.0G)* https://docs.google.com/uc?id=0B6fULLT_NpxMampUWlBCQXVJZzA&export=download [Accessed 2nd July 2019].
[27] FireEye/Flare-FakeNet-NG (2019) *FakeNet-NG - Next Generation Dynamic Network Analysis Tool* https://github.com/fireeye/flare-fakenet-ng [Accessed 2nd July 2019].
[28] Microsoft.com (2019) *Download Virtual Machines* https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/ [Accessed 2nd July 2019].
[29] Jonathon Taaffe (2019) *Diagram 1. Malware Analysis Lab Phase 1 Installation and Configuration* [Created 2nd July 2019].

Phase 2 File Transfer

The following diagram details Phase 2 configuration of Lab 1 which includes the Windows Server 2016[30] File Server, Network File Share for File Transfer and the Windows XP, 7, 8.1 and 10[31] Clients network configuration.

This configuration allows for

1. Download of all required application files from the Internet to the local host
2. Transfer of files from the local host to the Windows Server 2016 File Server share mw_client_files
3. Download of files from the network share mw_client_files to each of the Windows clients

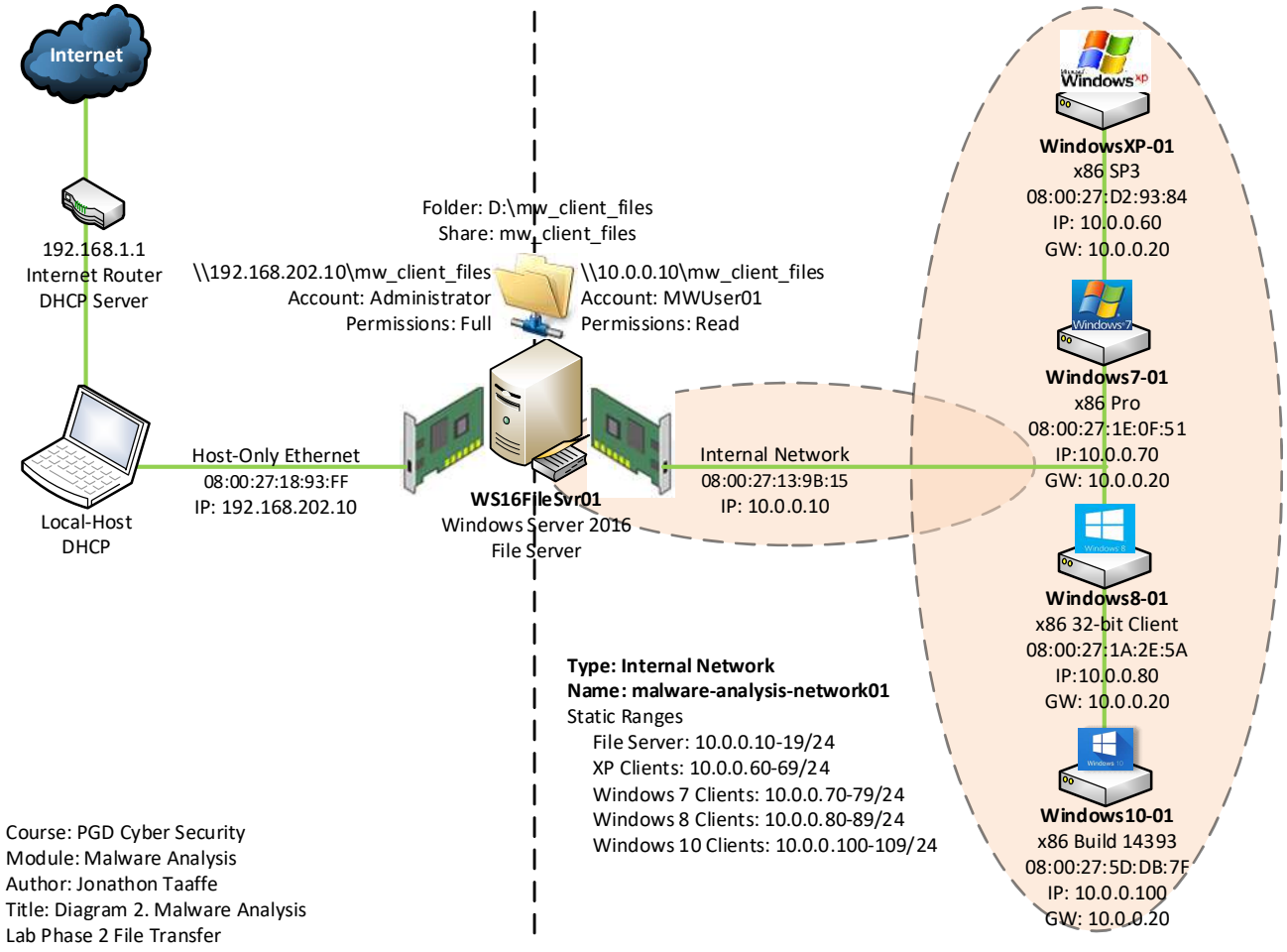


Diagram 2. Malware Analysis Lab Phase 2 File Transfer[32]

[30] Portal.Azure.com (2019) *Windows Server 2016 Standard* http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso [Accessed 2nd July 2019].
[31] Microsoft.com (2019) *Download Virtual Machines* https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/ [Accessed 2nd July 2019].
[32] Jonathon Taaffe (2019) *Diagram 2. Malware Analysis Lab Phase 2 File Transfer* [Created 2nd July 2019].

Phase 3 Client Application File Transfer

With the File Server configured allowing for File Transfer from local host to the Windows Clients on the Internal 'malware-analysis-network01' Network, the following Application Files were transferred as per Lecture 'Malware Types & Lab Setups File'[33], to C:\Temp on each Windows Client:

Application	File	OS
Microsoft .NET Framework 3.5 SP1	Microsoft_.NET_Framework_3.5_SP1_WinXP.exe	XP
Microsoft .NET Framework 4	Microsoft_.NET_Framework_4_x86_x64.exe	7,8,10
Adobe Reader 11.0.08	Adobe_Reader_11.0.08_WinXP_SP3.exe	XP
Adobe Reader 2019.012.20034	Adobe_Reader_2019.012.20034.exe	7,8,10
Chrome 1.3.34.7	ChromeStandaloneSetup_x86_WinXP.exe	XP
Chrome 49.0.2623.75 32bit	Chrome_32bit_49.0.2623.75.exe	XP
Chrome 1.3.34.7	ChromeStandaloneSetup_x86.exe	7,8,10
Firefox Setup 52.0esr.exe	Firefox_Setup_52.0esr.exe	XP
Firefox Setup 60.0b13.exe	Firefox_Setup_60.0b13.exe	XP
Firefox Setup 67.0.1 x86	Firefox_Setup_67.0.1_x86.exe	7,8,10
Java JRE 6 Windows i586	jre-6-windows-i586.exe	XP
Java JRE 8u211 Windows i586	Java_JRE_8u211_Windows_i586.exe	7,8,10
Microsoft Office 365 Home x86 x64	Office\Setup32.exe	All
Microsoft PowerShell 1.0 KB926139-v2	Microsoft_PowerShell_1.0_(KB926139-v2)_x86_WinXP	XP
Python 2.7.9 and 3.4.3 x86	Python_2.7.9_x86.msi and Python_3.4.3_x86.msi	XP
Python 3.7.3 x86	Python_3.7.3_x86.exe	7,8,10
WinRAR 561 and 571 x86	WinRAR561.exe and WinRAR571.exe	All

Table 10. Client Application File Transfer[34]

Phase 4 Client Application Installation

VirtualBox snapshots were used before and after each application install as follows

Action	Details
Snapshot 01	VM Snapshot
Application Install	Active Perl, Adobe Reader, Chrome
Snapshot 02	Post Application Install Snapshot
Application Install	Firefox, Java, Microsoft .NET
Snapshot 03	Post Application Install Snapshot
Application Install	Microsoft Office, Microsoft Powershell
Snapshot 04	Post Application Install Snapshot
Application Install	Microsoft Visual C++ 2008, C++ 2010
Snapshot 06	Post Application Install Snapshot
Application Install	Python, WinRAR
VM Clone	OS, Files and Installed Applications

Table 11. Client Application Installation[35]

[33] Malware Types & Lab Setups File (2019) *Tools Slide 28* https://moodle.ncirl.ie/mod/resource/view.php?id=59717 [Accessed 2nd July 2019].
[34] Jonathon Taaffe (2019) *Table 10. Client Application File Transfer* [Created 2nd July 2019].
[35] Jonathon Taaffe (2019) *Table 11. Client Application Installation* [Created 2nd July 2019].

Phase 5 Malware Analysis Tools File Transfer to Clients

On reviewing Lecture 'Malware Types & Lab Setups File'[36], the current version of each of the malware analysis tools listed were downloaded. All tools were transferred to each Windows client to C:\Temp\Tools.

Phase 6 Dynamic Malware Analysis Configuration

With the 2 Malware Analysis Utility VM's and all client VM's configured with required applications installed and all analysis tools copied, the Internal 'malware-analysis-network01' Network was completely isolated by powering off the Windows Server 2016[37] File Server.

Note: Malware Analysis Utility Selection

Setting Windows Client Gateway IP to 10.0.0.20, clients will communicate with REMnux (red line)
Setting Windows Client Gateway IP to 10.0.0.21, clients will communicate with FakeNet-NG (blue line)

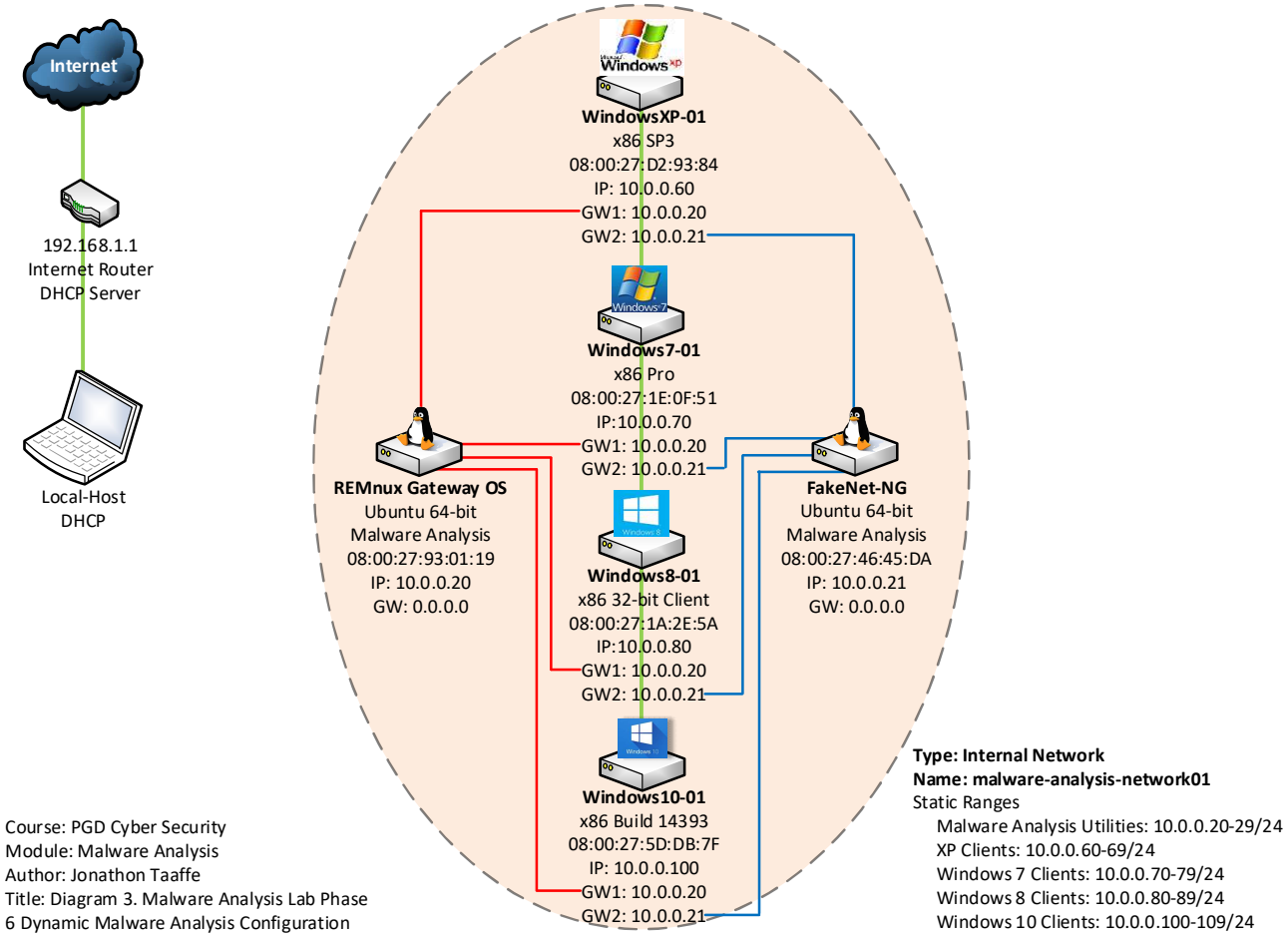


Diagram 3. Malware Analysis Lab Phase 6 Dynamic Malware Analysis Configuration[38]

[36] Malware Types & Lab Setups File (2019) *Tools Slides 28, 29, 30, 31, 32* https://moodle.ncirl.ie/mod/resource/view.php?id=59717 [Accessed 2nd July 2019].
[37] Portal.Azure.com (2019) *Windows Server 2016 Standard* http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso [Accessed 2nd July 2019].
[38] Jonathon Taaffe (2019) *Diagram 3. Malware Analysis Lab Phase 6 Dynamic Malware Analysis Configuration* [Created 2nd July 2019].

Practical Malware Analysis

Introduction

Researching Malware variants, the Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software[39] guide was reviewed. Further research resulted in locating Sam Bowne's Practical Malware Analysis website[40] which aligned to the malware analysis labs detailed in Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. Utilising these 2 resources, a Practical Malware Analysis lab was installed and configured.

Practical Malware Analysis Lab

Reviewing the labs content, the files used for analysis were not malicious. A NATNetwork was configured for the Practical Malware Analysis lab.

VirtualBox NATNetwork

NATNetwork was configured with DHCP range of 10.0.2.0/24 for initial VM install, update and configuration.

Kali Utilities VM Configuration

A Kali Linux distro was used in the labs to utilise iNetSim[41], configured as follows

Name	Kali KDE 2019.1
Type	Linux Ubuntu (64-bit)
RAM	2048MB
Disk	VDI Dynamic (50GB)
Adapter 1 Network	NATNetwork
Adapter 1 Type	Intel PRO/1000MT Server (82545EM)
Adapter 1 MAC	08:00:27:39:E6:5A
Adapter 1 NAT DHCP IP	10.0.2.3

Table 12. Kali KDE 2019.1 VM Configuration[42]

Clients Configuration

Windows XP x86 and Windows Server 2008 x86 were referenced in the labs to install and configure analysis tools on. VM's were configured as follows for analysis

VM Name	WindowsXP-01	WS2K8-x86-01
Operating System	Windows XP (32-bit)	Windows 2008 (32-bit)
RAM	2048MB	2048MB
Disk	VDI Dynamic (50GB)	VDI Dynamic (50GB)
Adapter 1 Network	NATNetwork	NATNetwork
Adapter 1 MAC	08:00:27:DB:DD:01	08:00:27:5B:95:06
Adapter 1 NAT DHCP IP	10.0.2.5	10.0.2.6
Adapter 1 Primary DNS	10.0.2.3 (Kali IP)	10.0.2.3 (Kali IP)

Table 13. Windows XP and Windows Server 2008 VM Configuration[43]

[39] Sikorski, Michael; Honig, Andrew (2012) *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software* https://library.ncirl.ie/items/32216 [Accessed 20th May 2019].
[40] Sam Bowne (2016) *CNIT 126: Practical Malware Analysis* https://samsclass.info/126/126_S16.shtml#lecture [Accessed 20th May 2019].
[41] iNetSim.org (2018) *INetSim: Internet Services Simulation Suite* https://www.inetsim.org/ [Accessed 20th May 2019].
[42] Jonathon Taaffe (2019) *Table 12. Kali KDE 2019.1 VM Configuration* [Created 20th May 2019].
[43] Jonathon Taaffe (2019) *Table 13.Windows XP and Windows Server 2008 VM Configuration* [Created 20th May 2019].

Labs, Applications and Analysis Tools Installation

The following labs, applications and analysis tools were then downloaded and installed

Type	Name	URL
Labs	Practical Malware Analysis	https://practicalmalwareanalysis.com/labs/
Labs	Practical Malware Analysis	https://github.com/mikesiko/PracticalMalwareAnalysis-Labs
App	7-zip	https://www.7-zip.org/
App	Java JRE 6 Windowsi586	https://www.oracle.com
App	.NET Framework 4	https://www.microsoft.com/en-us/download/details.aspx?id=17718
App	Microsoft Windows SDK	https://www.microsoft.com/en-us/download/details.aspx?id=8422
Browser	Firefox	https://www.mozilla.org/en-US/firefox/all
Site	Virus Total	https://www.virustotal.com
Analysis	PEView	http://wjradburn.com/software/
Analysis	PEiD 0.95	http://www.softpedia.com/
Analysis	BinText3.03	https://www.softpedia.com/get/System/File-Management/BinText.shtml
Analysis	DependencyWalker 2.2	http://www.dependencywalker.com/
Analysis	UPX 3.95	https://upx.github.io/
Analysis	Strings	https://docs.microsoft.com/en-gb/sysinternals/downloads/strings
Analysis	Nmap	http://nmap.org
Analysis	SysInternals	http://docs.microsoft.com/en-gb/sysinternals/downloads
Analysis	SysInternals Strings v2.52	https://docs.microsoft.com/en-gb/sysinternals/downloads/strings
Analysis	SysInternals Process Monitor v3.50	https://docs.microsoft.com/en-gb/sysinternals/downloads/procmon
Analysis	SysInternals Process Explorer v 16.21	https://docs.microsoft.com/en-gb/sysinternals/downloads/process-explorer
Analysis	Resource Hacker 5.1.7	http://www.angusj.com/resourcehacker/
Analysis	Wireshark (Windows Server 2008) v2.0.0	https://1.eu.dl.wireshark.org/win32/all-versions/Wireshark-win32-2.0.0.exe
Analysis	IDA Pro v5.0	https://samsclass.info/126/proj/idafree50.exe
Analysis	IDA Pro v7.0	https://www.hex-rays.com/products/ida/support/download_freeware.shtml
Analysis	OllyDbg 1.10	http://www.ollydbg.de/download.htm
Analysis	LiveKd v5.62	https://docs.microsoft.com/en-gb/sysinternals/downloads/livekd
Analysis	HashCalc 2.02	http://www.slavasoft.com/hashcalc/
Analysis	WinHex	http://winhex.com/winhex/

Table 14. Labs, Applications and Analysis Tools Installation[44]

[44] Jonathon Taaffe (2019) Table 14. Labs, Applications and Analysis Tools Installation [Created 20th May 2019].

Practical Malware Analysis Lab Environment Configuration

With the NATNetwork configured and the VM installed, the Practical Malware Analysis Lab was configured as follows:

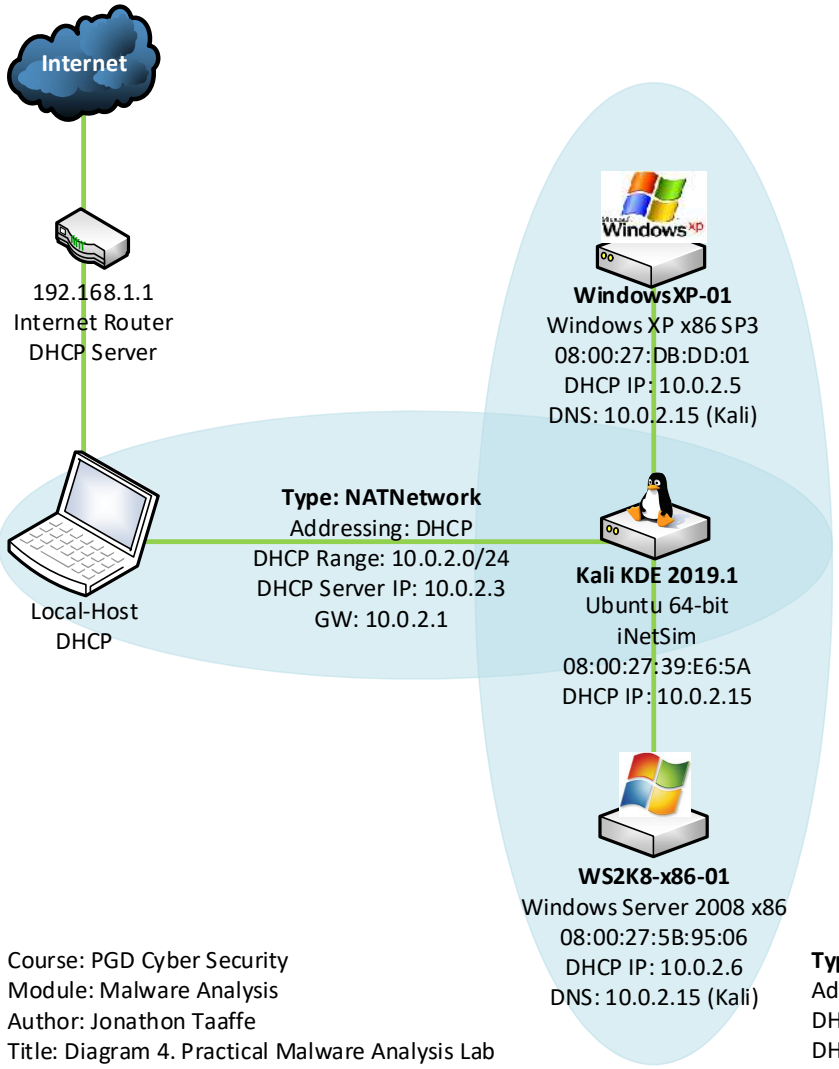


Diagram 4. Practical Malware Analysis Lab Configuration[45]

[45] Jonathon Taaffe (2019) *Diagram 4. Practical Malware Analysis Lab Configuration* [Created 20th May 2019].

Practical Malware Analysis Exercises

Referencing Practical Malware Analysis, the following lab exercises were utilised

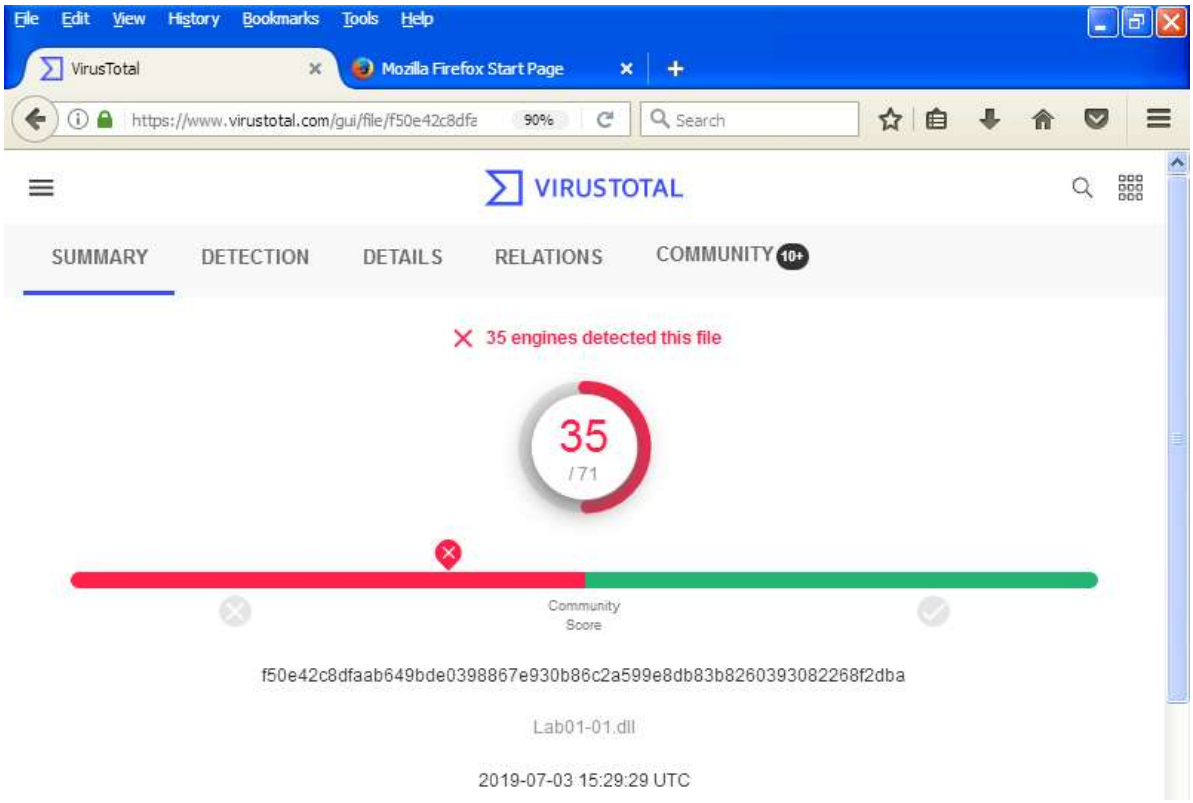
	Practical Malware Analysis Reference		
Report Section	**Chapter**	**Lab**	**Page**
2.3a	Chapter 1: Basic Static Techniques	Lab1-1	27
2.3b	Chapter 1: Basic Static Techniques	Lab1-2	27
2.3c	Chapter 3: Basic Dynamic Analysis	Lab3-1	61
2.3d	Chapter 5: Anti Reverse Engineering	Lab5-1	107
2.33	Chapter 9: OllyDBG	Lab9-1	202
2.3f	Chapter 11: Malware Behaviour	Lab11-1	251
2.3g	Chapter 12: Covert Malware Launching	Lab12-1	266
2.3h	Chapter 13: Data Encoding	Lab13-1	295

Table 15. Practical Malware Analysis Exercises[46]

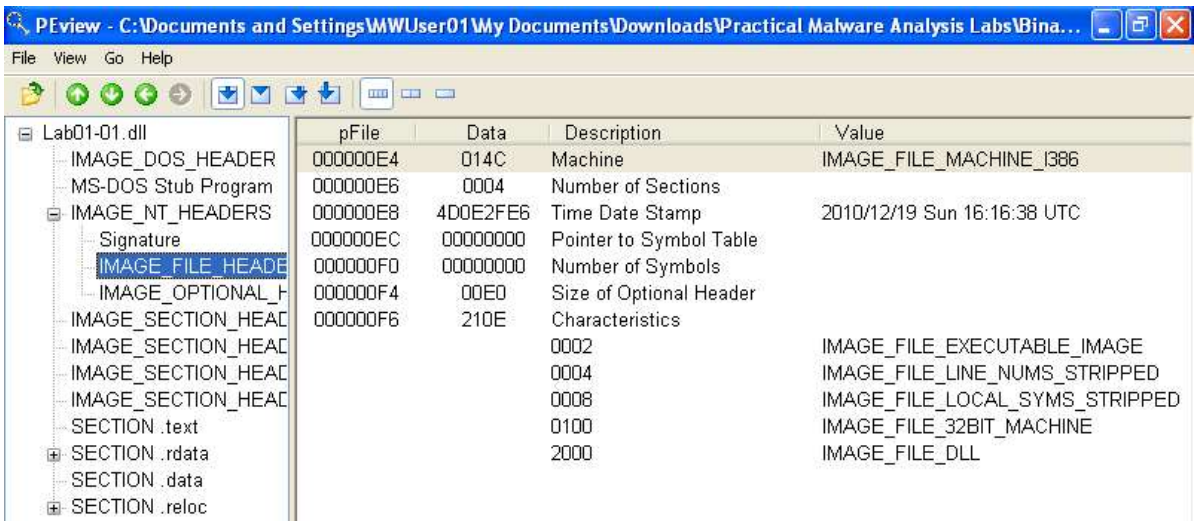
[46] Jonathon Taaffe (2019) Table 15. Practical Malware Analysis Exercises [Created 20th May 2019].

Chapter 1: Basic Static Techniques - Lab1-1
Source Files URL: https://github.com/mikesiko/PracticalMalwareAnalysis-Labs [47]

Virus Total[48] Analysis
File: Lab01-01.dll



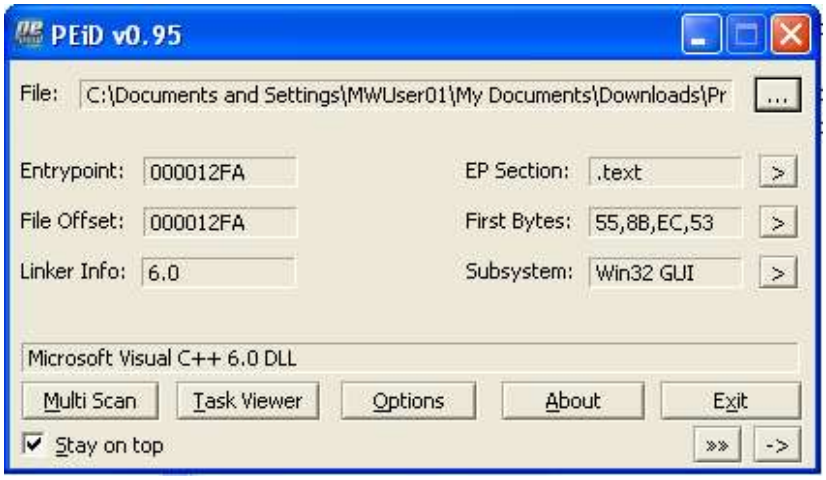
PEView[49] Analysis
File: Lab01-01.dll



[47] PracticalMalwareAnalysis-Labs (2017) *Binaries for the book Practical Malware Analysis* https://github.com/mikesiko/PracticalMalwareAnalysis-Labs [Accessed 22nd May 2019].
[48] Virus Total (2019) *Virus Total* https://www.virustotal.com [Accessed 22nd May 2019].
[49] Radburn, Wayne J. (2018) *PEview version 0.9.9 (.zip 31KB)* http://wjradburn.com/software/ [Accessed 22nd May 2019].

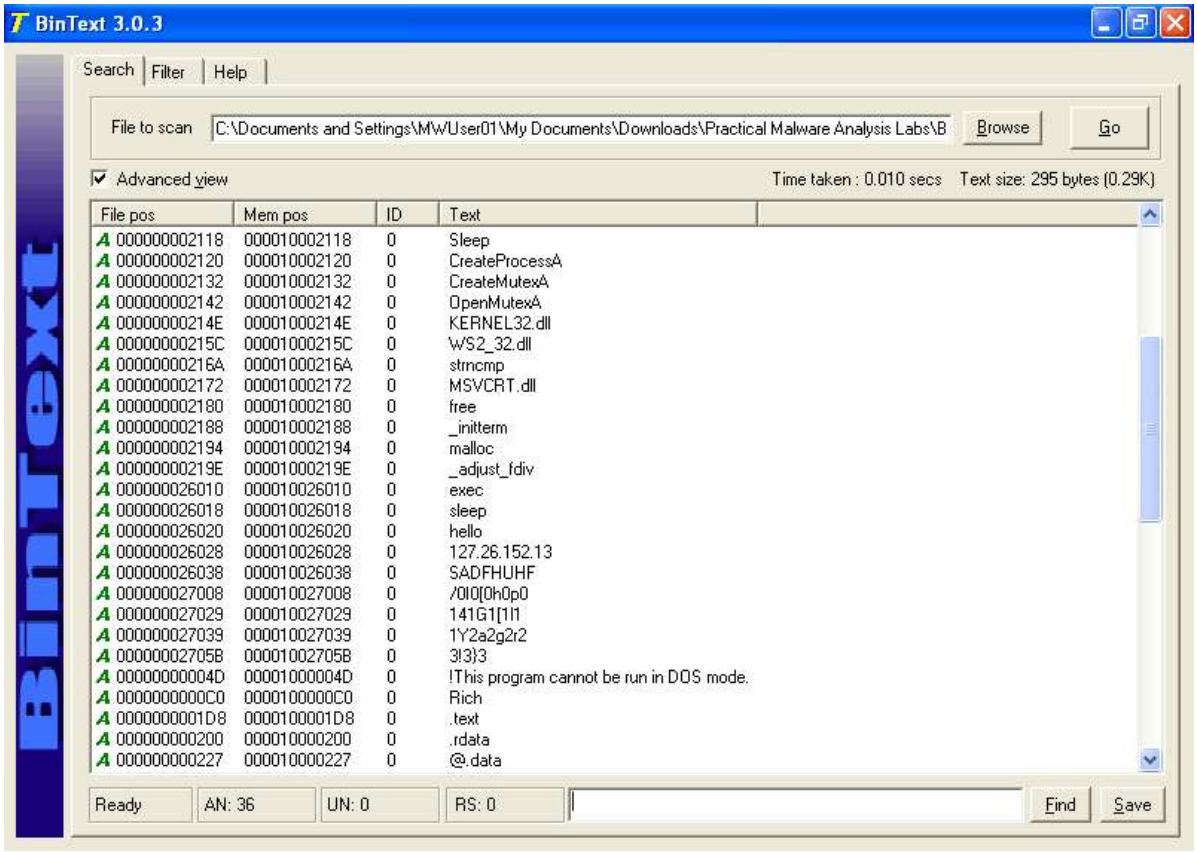
PEiD[50] Analysis

File: Lab01-01.dll



BinText3.03[51] Analysis

File: Lab01-01.dll



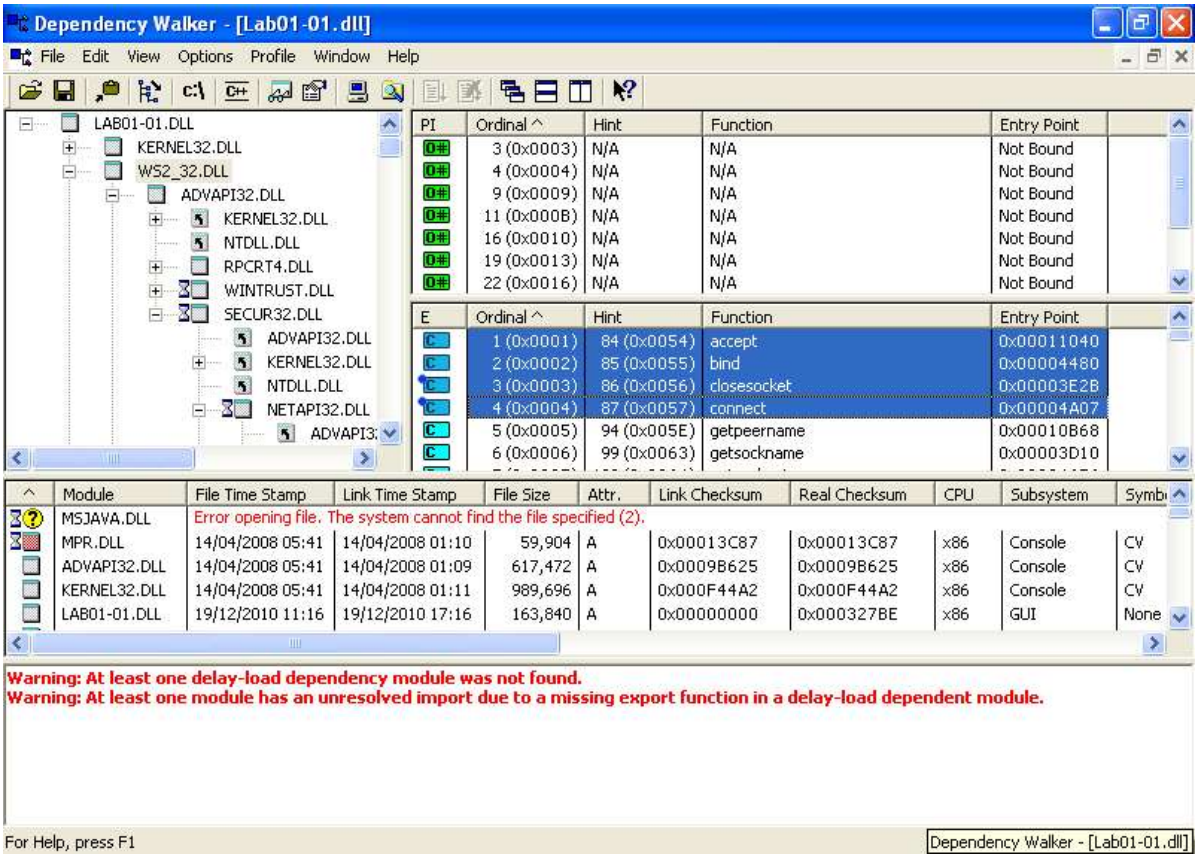
IP Address: 127.26.152.13

[50] Softpedia.com (2019) *PEiD 0.95* https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml [Accessed 22nd May 2019].

[51] Softpedia.com (2019) *BinText 3.03* https://www.softpedia.com/get/System/File-Management/BinText.shtml [Accessed 22nd May 2019].

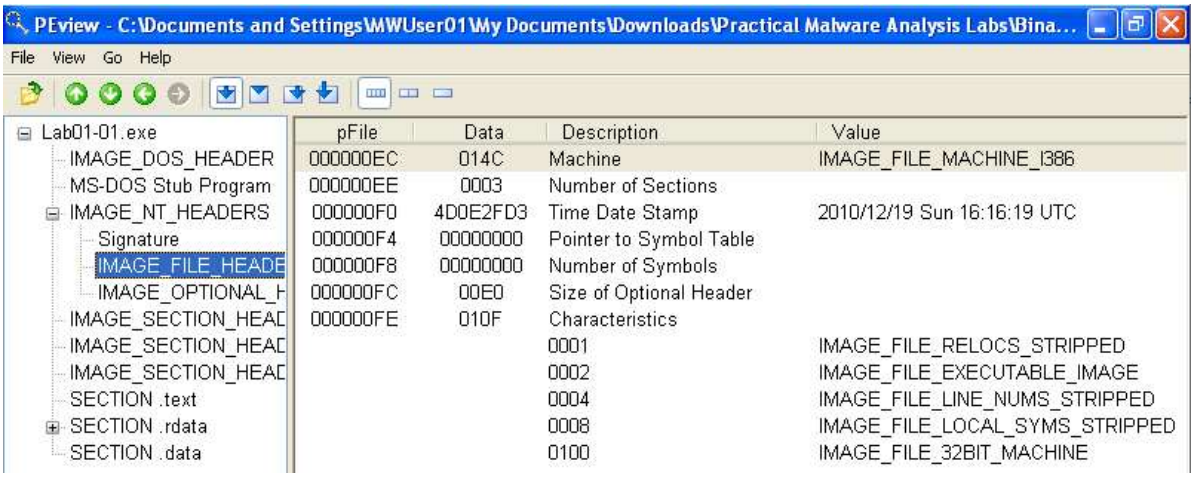
Dependency Walker 2.2[52] Analysis

File: Lab01-01.dll



PEView[53] Analysis

Lab01-01.exe

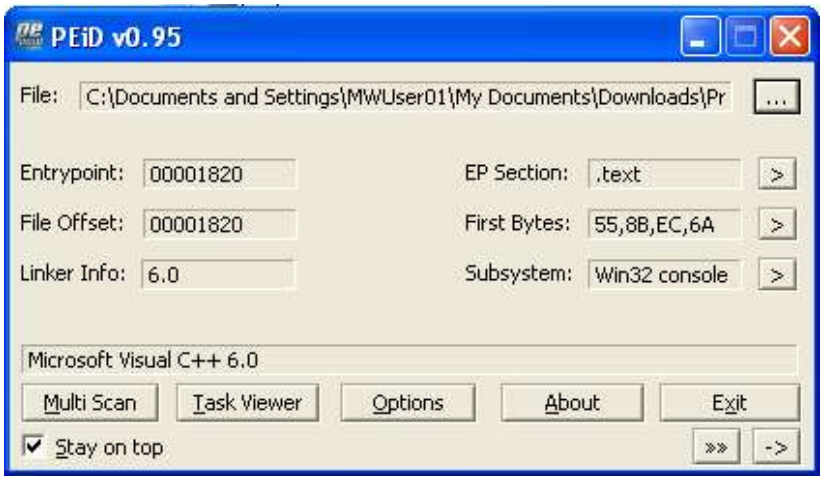


[52] Dependency Walker 2.2 (2019) *Dependency Walker 2.2* http://www.dependencywalker.com/ [Accessed 22nd May 2019].

[53] Radburn, Wayne J. (2018) *PEview version 0.9.9 (.zip 31KB)* http://wjradburn.com/software/ [Accessed 22nd May 2019].

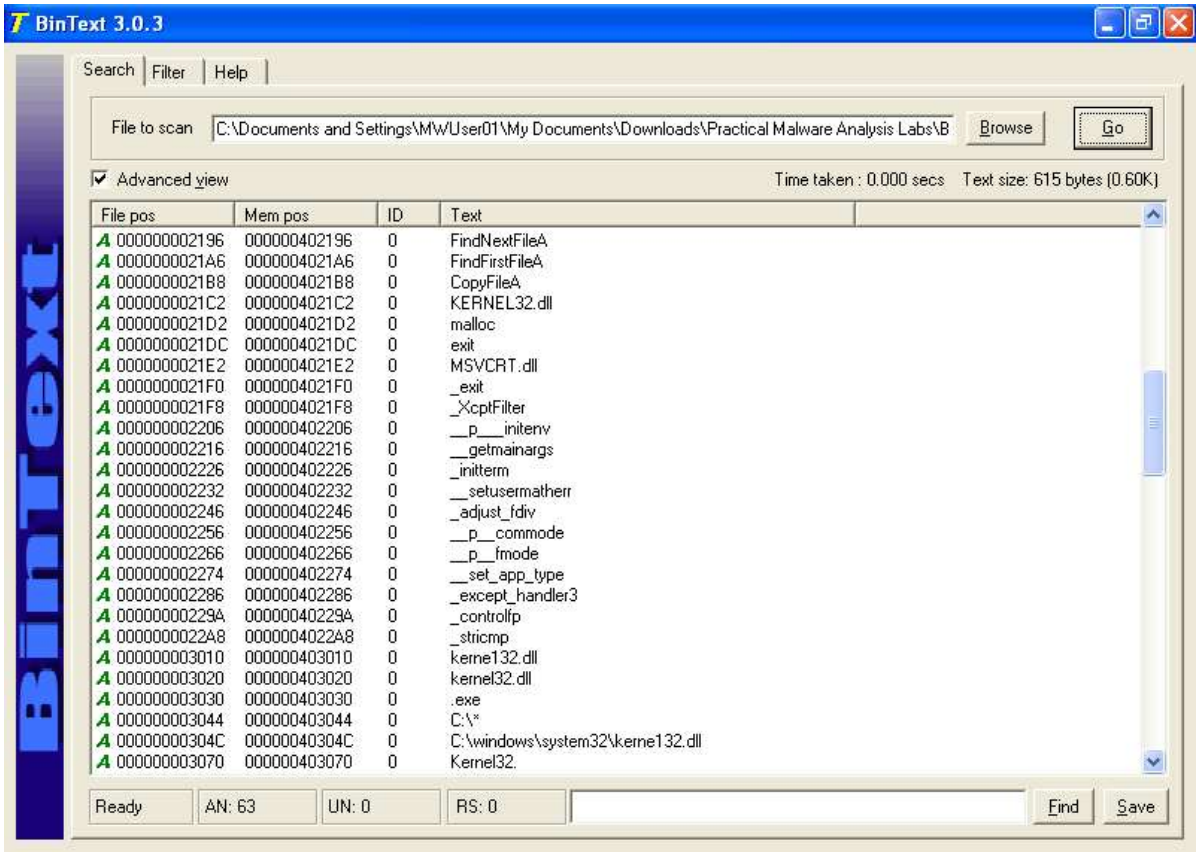
PEiD[54] Analysis

File: Lab01-01.exe



BinText3.03[55] Analysis

File: Lab01-01.exe

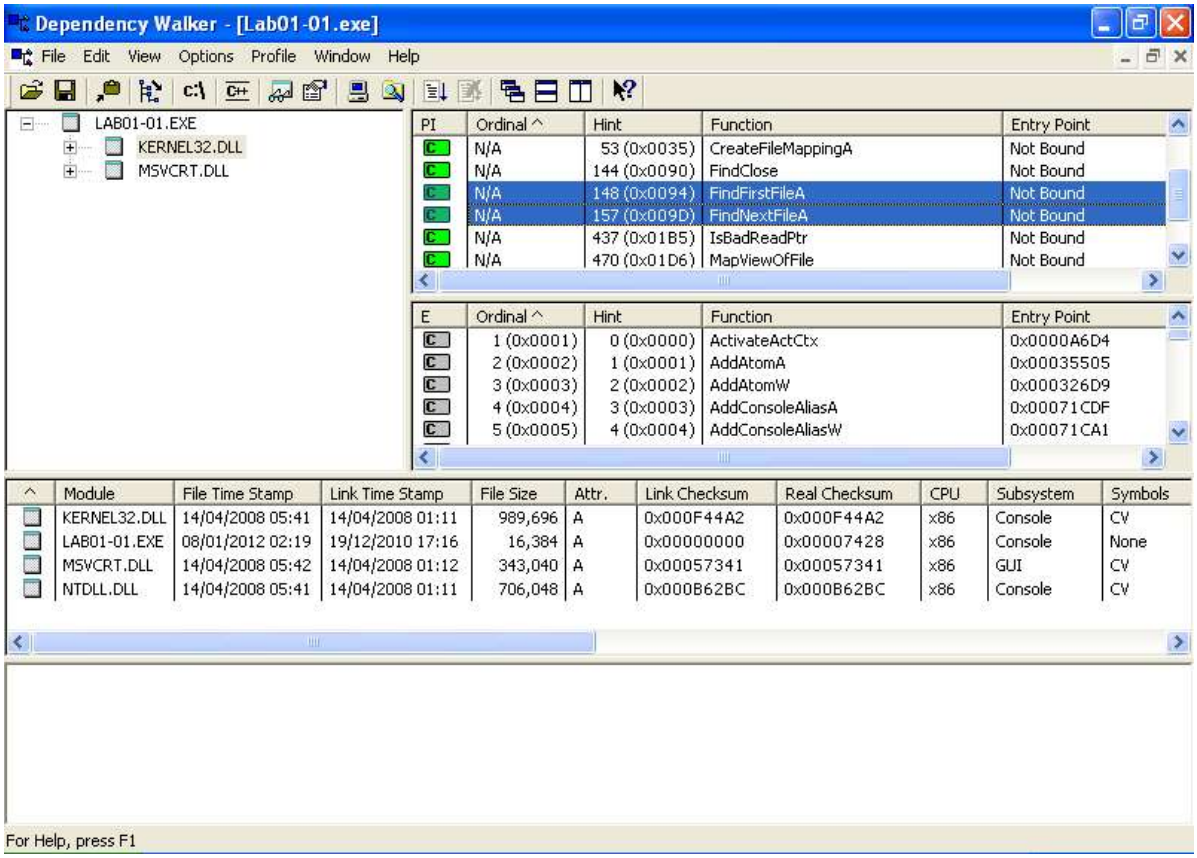


[54] Softpedia.com (2019) *PEiD 0.95* https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml [Accessed 22nd May 2019].

[55] Softpedia.com (2019) *BinText 3.03* https://www.softpedia.com/get/System/File-Management/BinText.shtml [Accessed 22nd May 2019].

Dependency Walker 2.2[56] Analysis

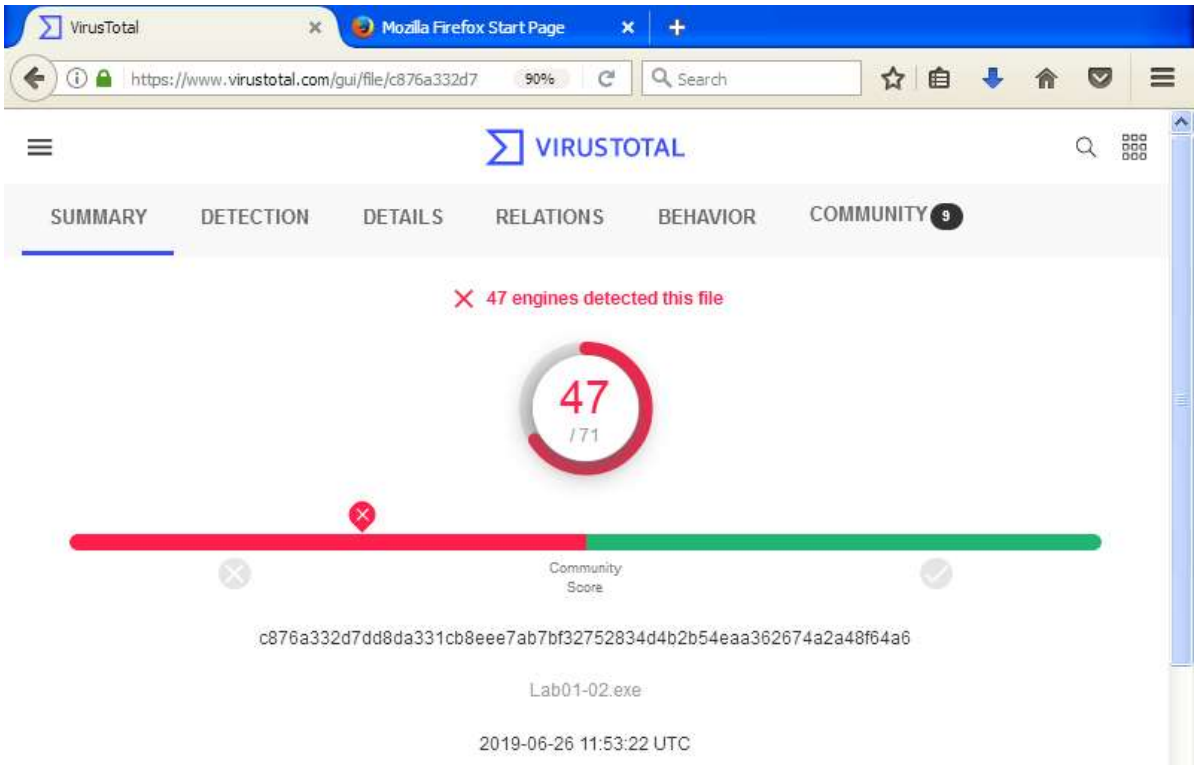
File: Lab01-01.exe



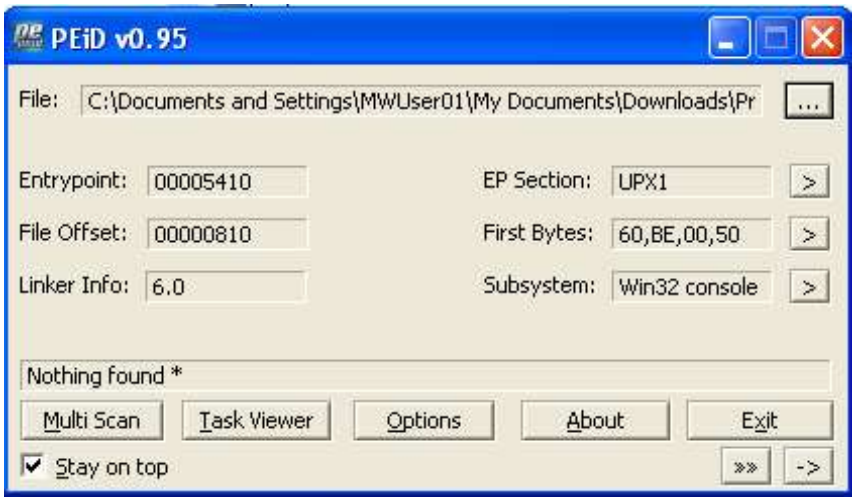
[56] Dependency Walker 2.2 (2019) *Dependency Walker 2.2* http://www.dependencywalker.com/ [Accessed 22nd May 2019].

Chapter 1: Basic Static Techniques - Lab1-2
Source Files URL: https://github.com/mikesiko/PracticalMalwareAnalysis-Labs [57]

VirusTotal[58] Analysis
File: Lab01-02.exe



PEiD[59] Analysis
File: Lab01-02.exe



Nothing found *

[57] PracticalMalwareAnalysis-Labs (2017) *Binaries for the book Practical Malware Analysis* https://github.com/mikesiko/PracticalMalwareAnalysis-Labs [Accessed 22nd May 2019].
[58] Virus Total (2019) *Virus Total* https://www.virustotal.com [Accessed 22nd May 2019].
[59] Softpedia.com (2019) *PEiD 0.95* https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml [Accessed 22nd May 2019].

UPX 3.95[60] Analysis

File: Lab01-02.exe

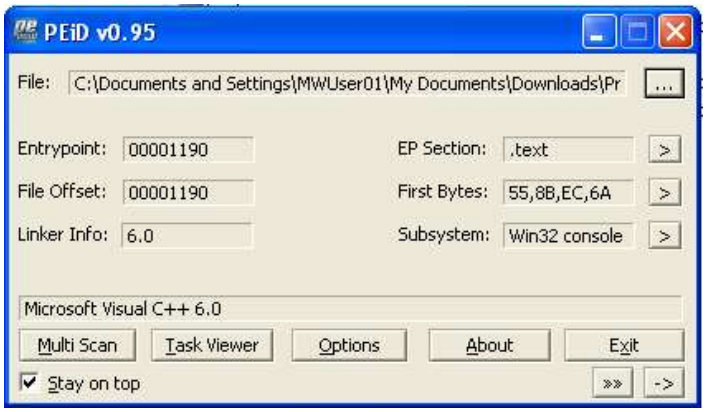
```
C:\Documents and Settings\MWUser01\My Documents\Downloads\Practical Malware Anal
ysis Labs\BinaryCollection\Chapter_1L>upx.exe -d -o Lab01-02-unpacked.exe Lab01-
02.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95w       Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     16384 <-      3072   18.75%    win32/pe     Lab01-02-unpacked.exe

Unpacked 1 file.
```

PEiD[61] Analysis

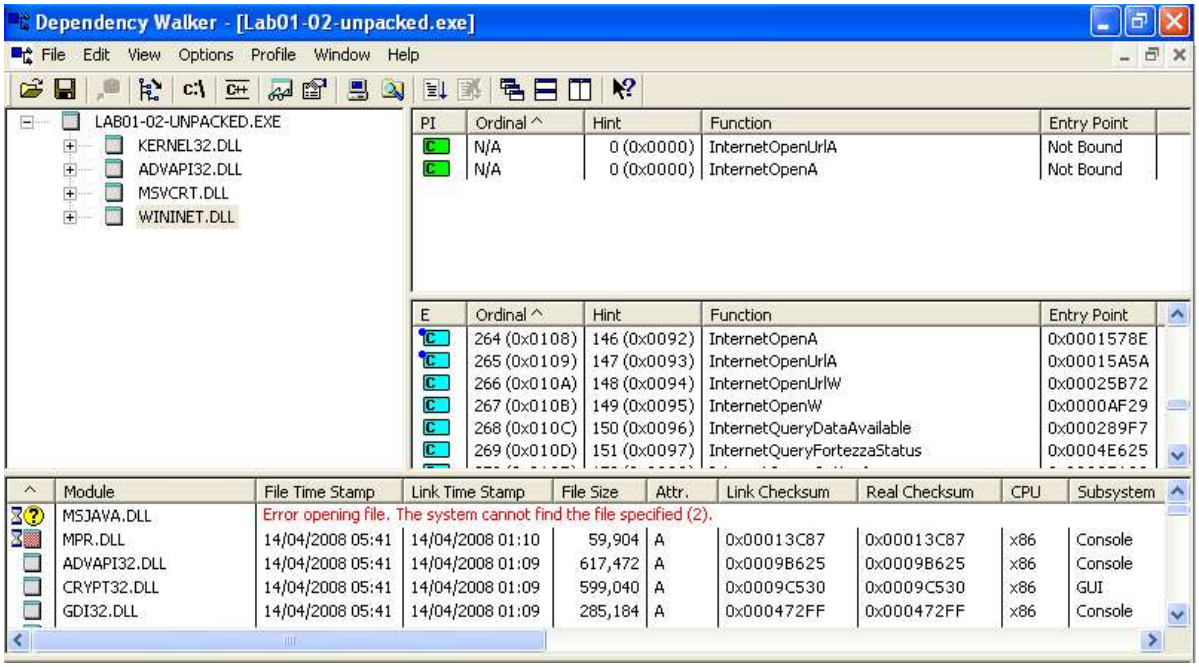
File: Lab01-02.exe



Microsoft Visual C++ 6.0

Dependency Walker[62] Analysis

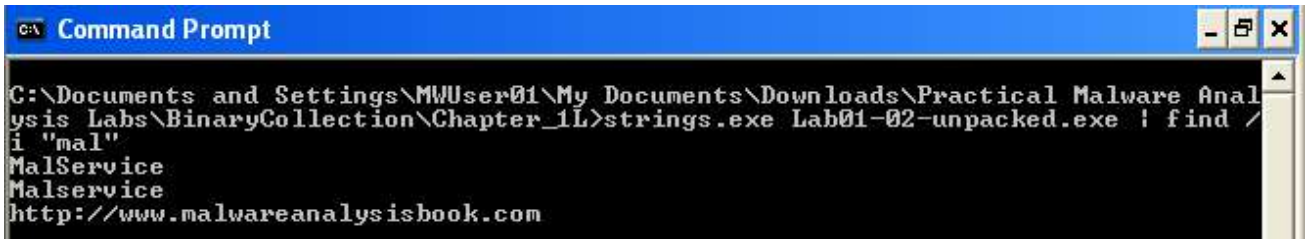
File: Lab01-02.exe



[60] UPX Ultimate Packer for eXecutables (2019) UPX 3.95 https://github.com/upx/upx/releases/tag/v3.95 [Accessed 22nd May 2019].
[61] Softpedia.com (2019) PEiD 0.95 https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml [Accessed 22nd May 2019].
[62] Dependency Walker 2.2 (2019) Dependency Walker 2.2 http://www.dependencywalker.com/ [Accessed 22nd May 2019].

Strings[63] Analysis

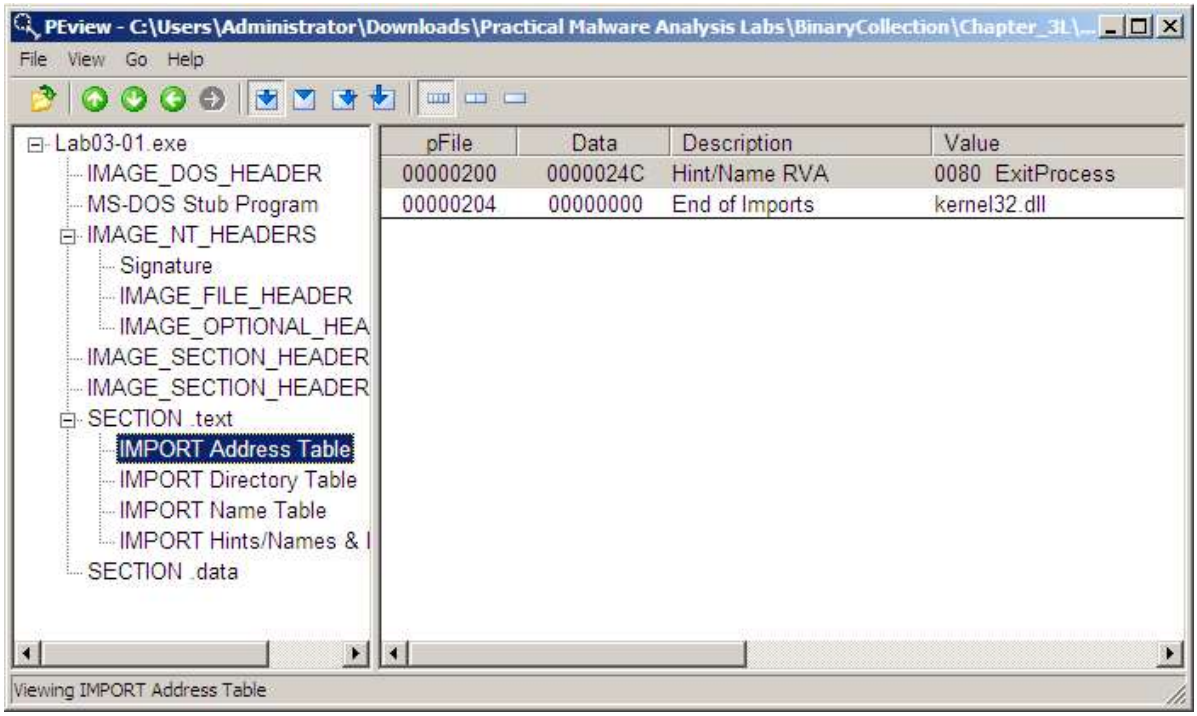
File: Lab01-02.exe



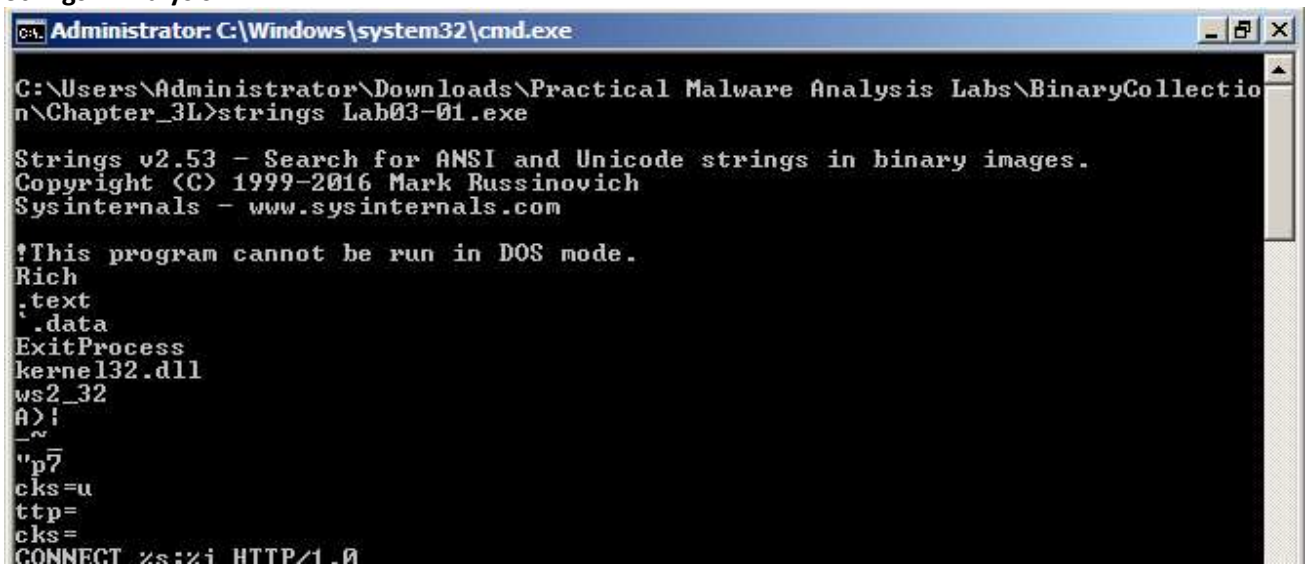
[63] Microsoft.com (2019) *Strings v2.53* https://docs.microsoft.com/en-gb/sysinternals/downloads/strings [Accessed 22nd May 2019].

Chapter 3: Basic Dynamic Analysis - Lab3-1
File: Lab03-01.exe

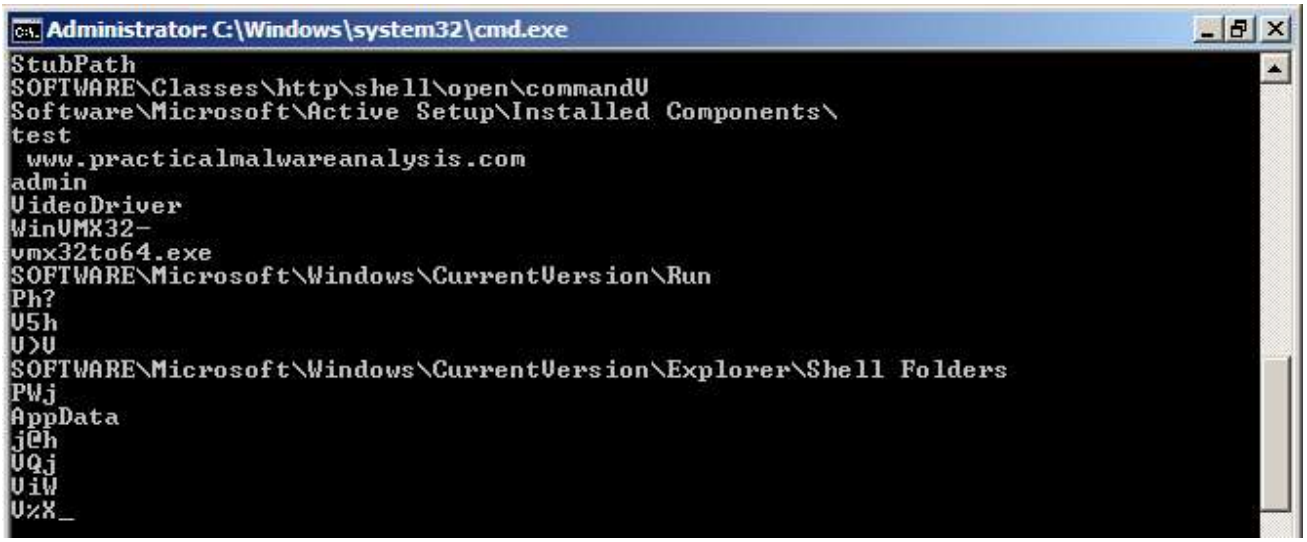
PEview[64] Analysis
File: Lab03-01.exe



Strings[65] Analysis

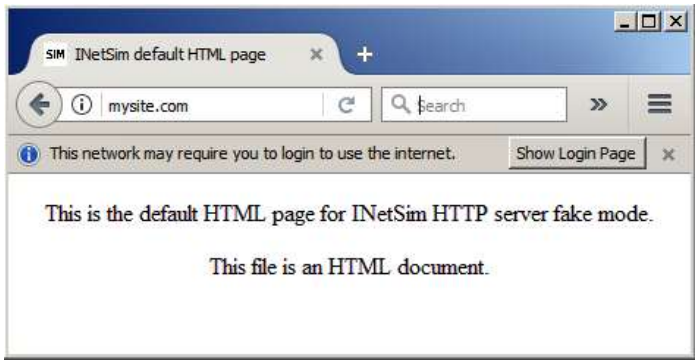


[64] Radburn, Wayne J. (2018) *PEview version 0.9.9 (.zip 31KB)* http://wjradburn.com/software/ [Accessed 22nd May 2019].
[65] Microsoft.com (2019) *Strings v2.53* https://docs.microsoft.com/en-gb/sysinternals/downloads/strings [Accessed 22nd May 2019].



Dynamic Analysis

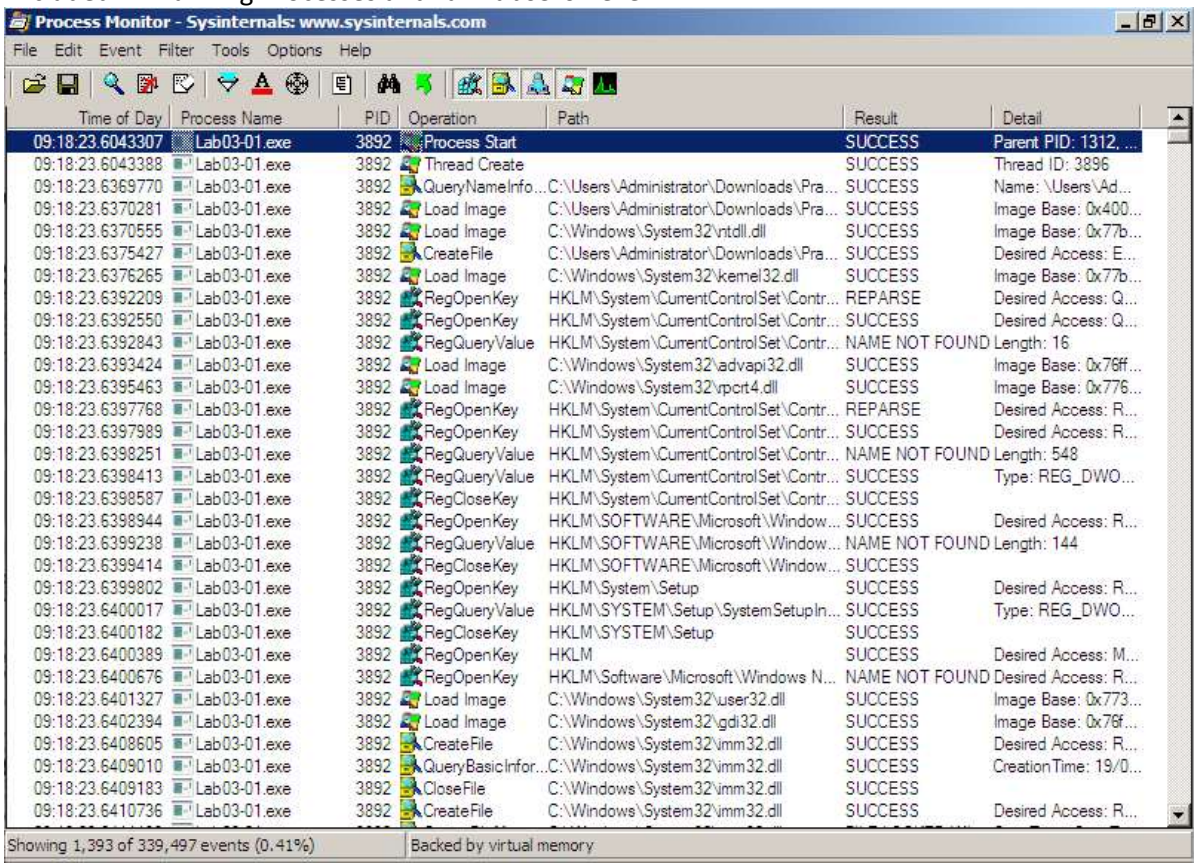
1. Started iNetSim[66] on Kali KDE 2019
2. On Windows Server 2008 set Primary DNS to 10.0.2.15 (Kali IP)
3. From Windows Server 2008 browsed through Firefox to http://mysite.com
4. Received the iNetSim HTTP server fake mode page.



[66] iNetSim.org (2018) INetSim: Internet Services Simulation Suite https://www.inetsim.org/ [Accessed 20th May 2019].

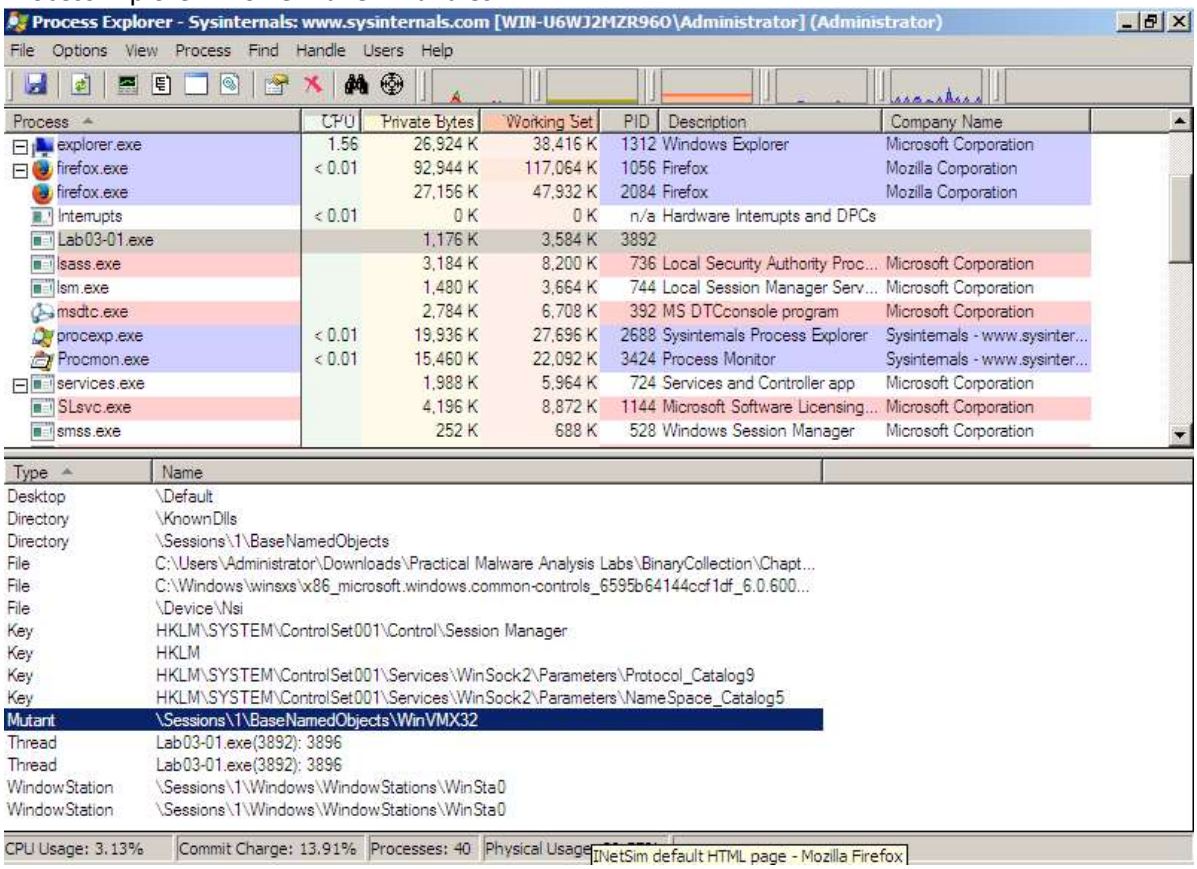
Process Explorer[67] Analysis

Excluded All Running Processes and ran Lab03-01.exe

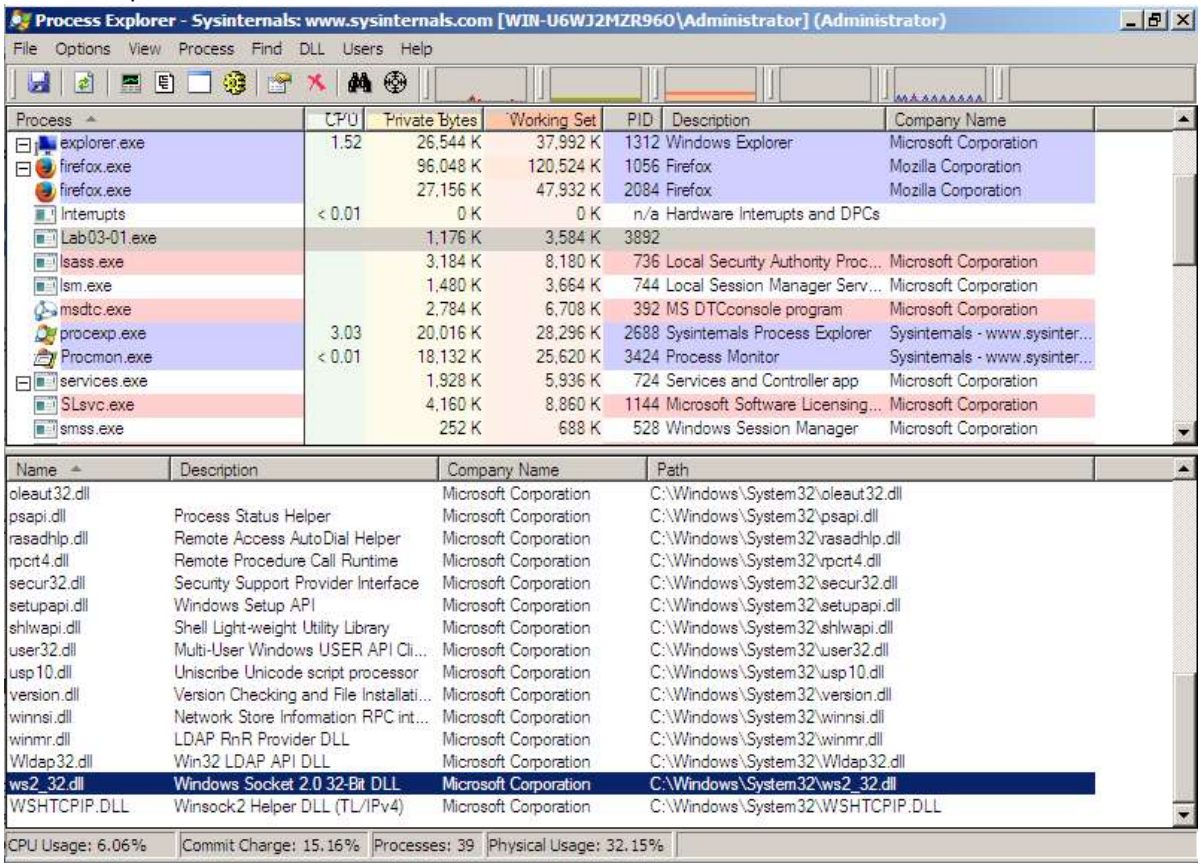


[67] Microsoft.com (2019) *Process Explorer v16.26* https://docs.microsoft.com/en-gb/sysinternals/downloads/process-explorer [Accessed 20th May 2019].

Process Explorer > Lower Pane > Handles

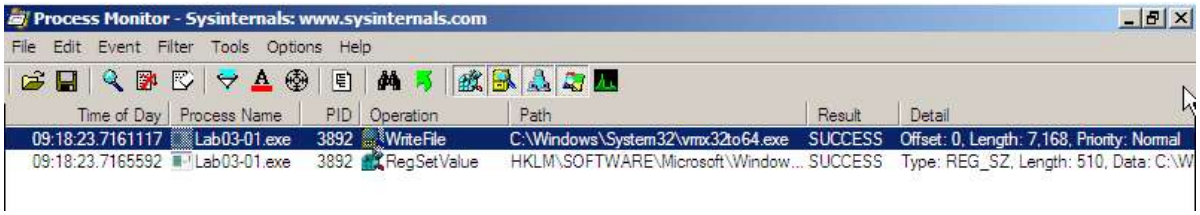


Process Explorer > Lower Pane > DLL's



Process Monitor[68]: View Malicious Process's Events

Process Monitor > Filter > Process Name > is > Lab03-01.exe > Add
Process Monitor > Filter > Operation > is > RegSetValue > Add
Process Monitor > Filter > Operation > is > WriteFile > Add

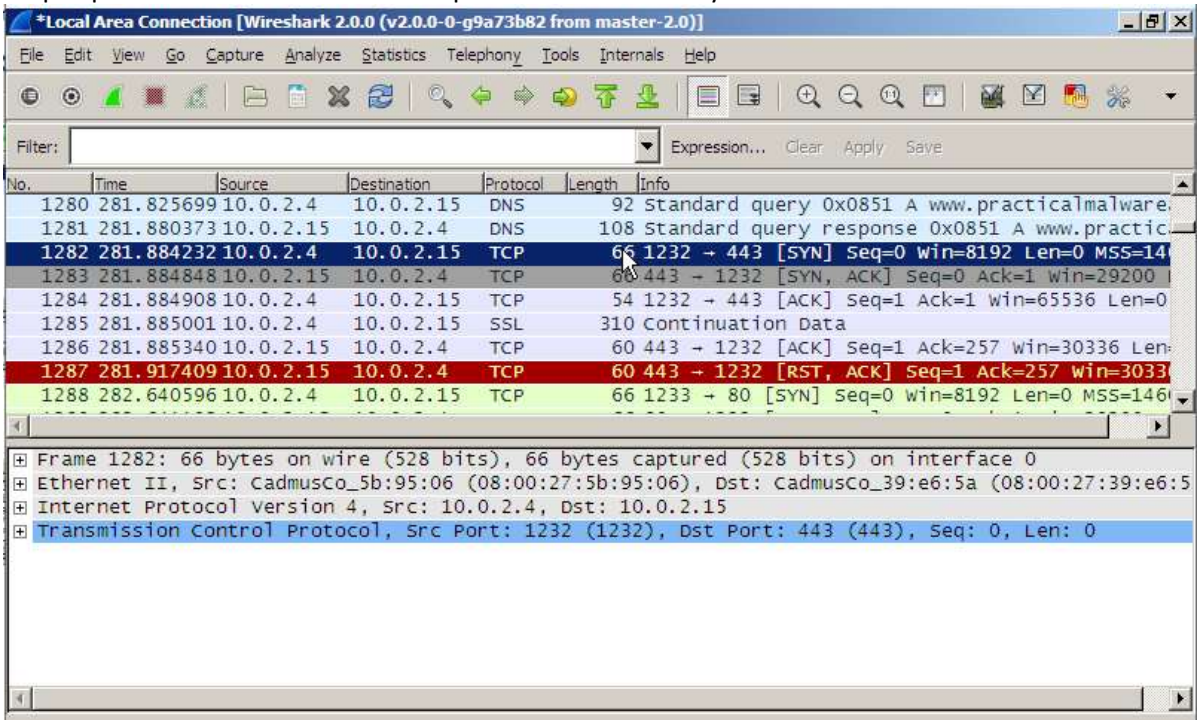


1. Double-click event with Path ending vmx32to64.exe
2. Properties sheet: this event created a file named vmx32to64.exe
3. This event copied the malware itself to a file named vmx32to64.exe, so that filename is a useful indicator of infection.
4. Double-click event with Path ending VideoDriver
5. Created new Run key in registry called "VideoDriver" with a value of "C:\WINDOWS\system32\vmx32to64.exe"
6. Persistence mechanism to re-launch the malware when the machine restarts

[68] Microsoft.com (2019) *Process Monitor v3.52* https://docs.microsoft.com/en-gb/sysinternals/downloads/procmon [Accessed 20th May 2019].

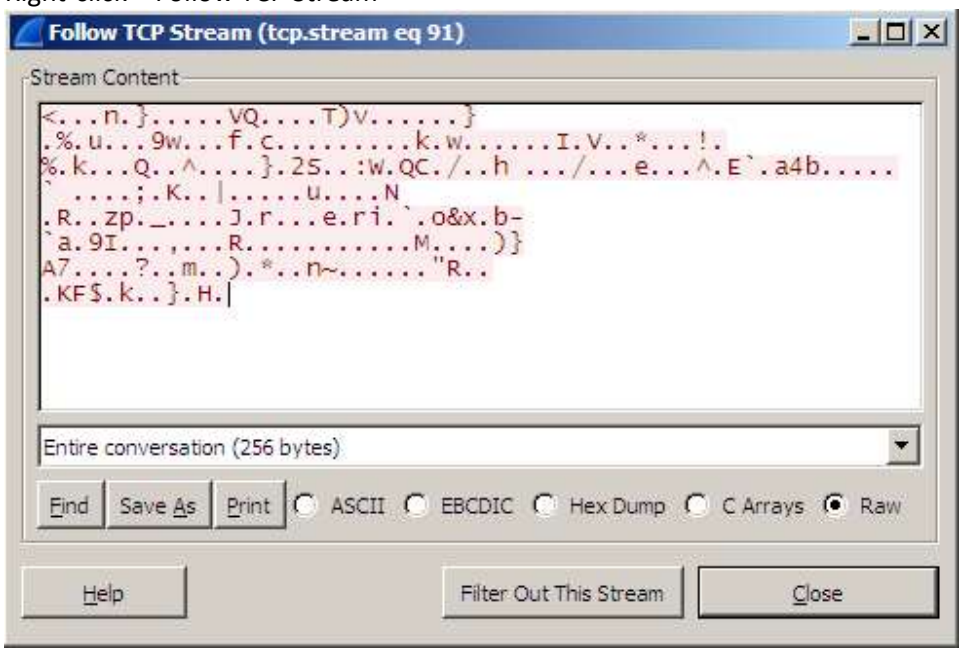
Wireshark[69] Analysis

Stop capture > Filter: 'frame contains practicalmalwareanalysis'



Packet 1282: SYN packet sent from port 1232 > https port 443

Right-click > Follow TCP Stream



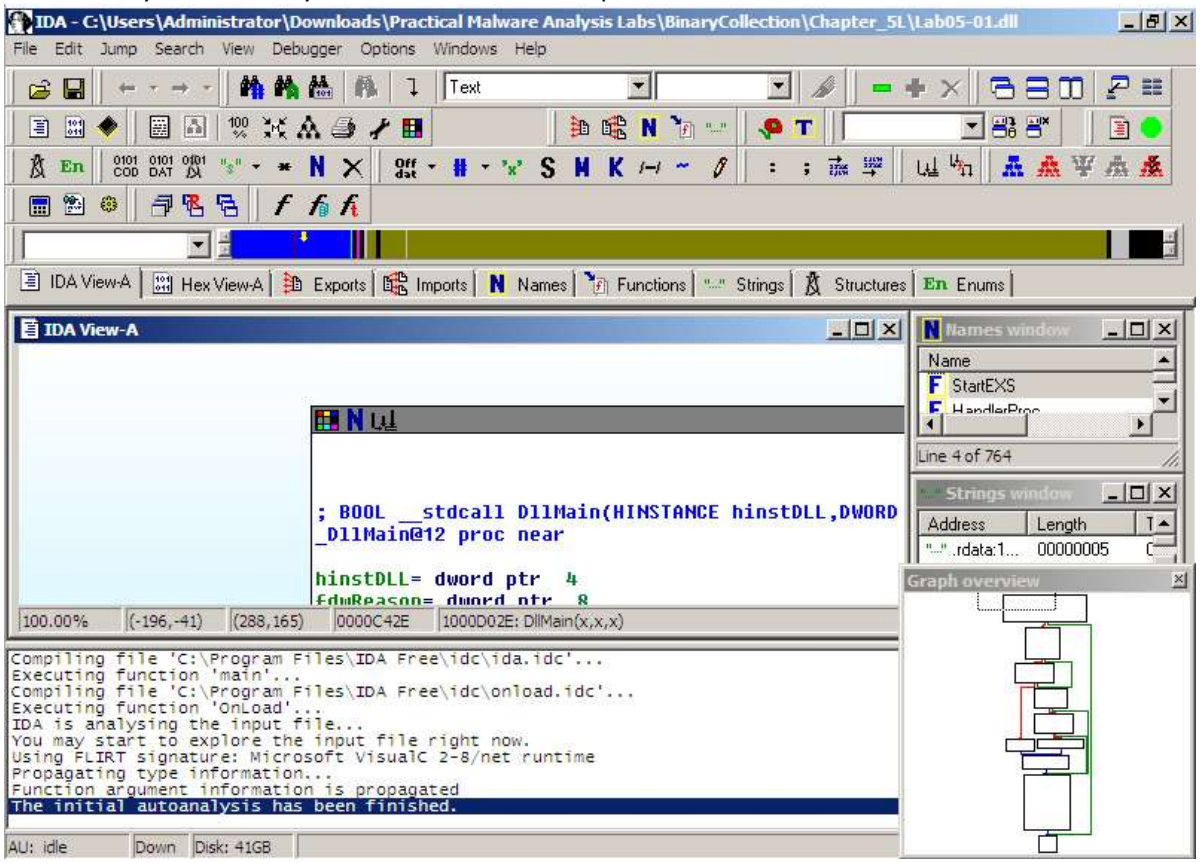
Stream Content: Entire conversation (256 bytes) of random packets

These are beacons and are used by malware to notify the Command and Control server that the machine is infected and ready to use.

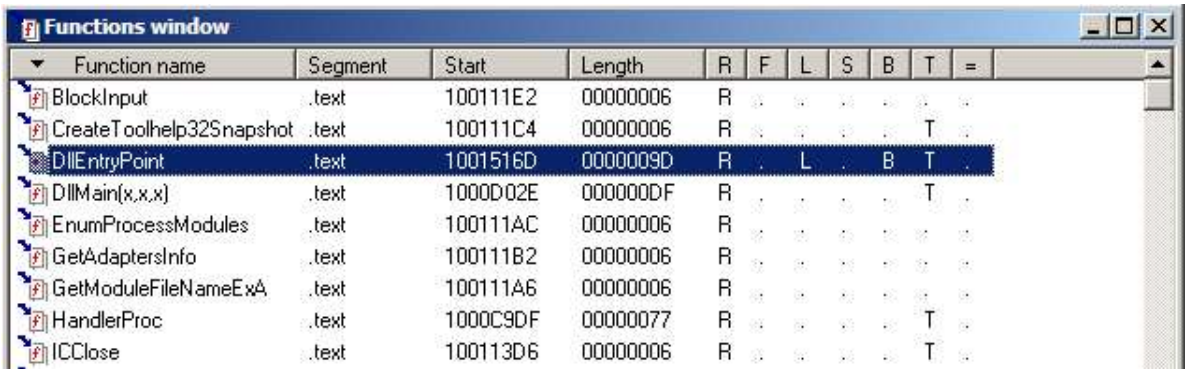
[69] Wireshark.org (2019) *Wireshark-win32-2.0.0.exe* https://1.eu.dl.wireshark.org/win32/all-versions/ [Accessed 20th May 2019].

Chapter 5: Anti Reverse Engineering - Lab5-1
Source Files URL: https://github.com/mikesiko/PracticalMalwareAnalysis-Labs [70]
File: Lab05-01.dll

IDA Pro[71] Analysis
New > PE Dynamic Library > OK > Lab05-01.dll > Open



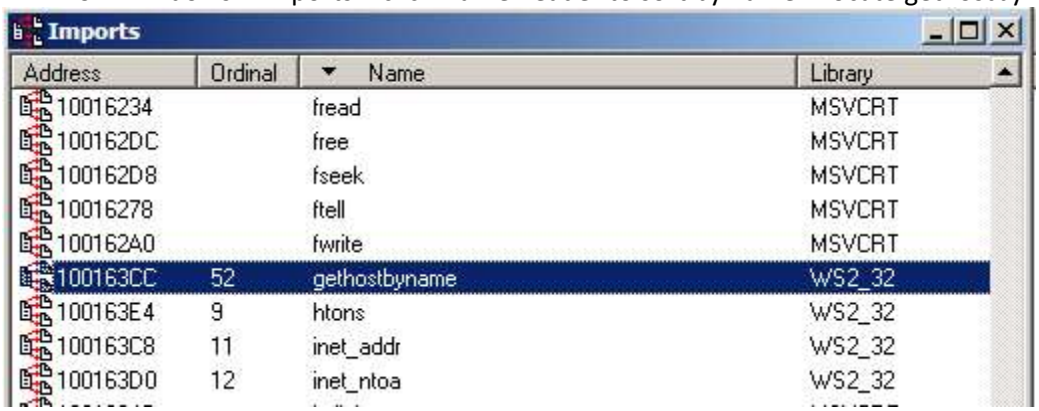
Find DLLMain Address
IDA Pro > Windows > Functions window > click "Function name" header to sort by name > locate DLLMain



[70] PracticalMalwareAnalysis-Labs (2017) *Binaries for the book Practical Malware Analysis* https://github.com/mikesiko/PracticalMalwareAnalysis-Labs [Accessed 22nd May 2019].
[71] Hex-Rays (2019) *IDA Freeware for Windows (48 MB)* https://www.hex-rays.com/products/ida/support/download_freeware.shtml [Accessed 22nd May 2019].

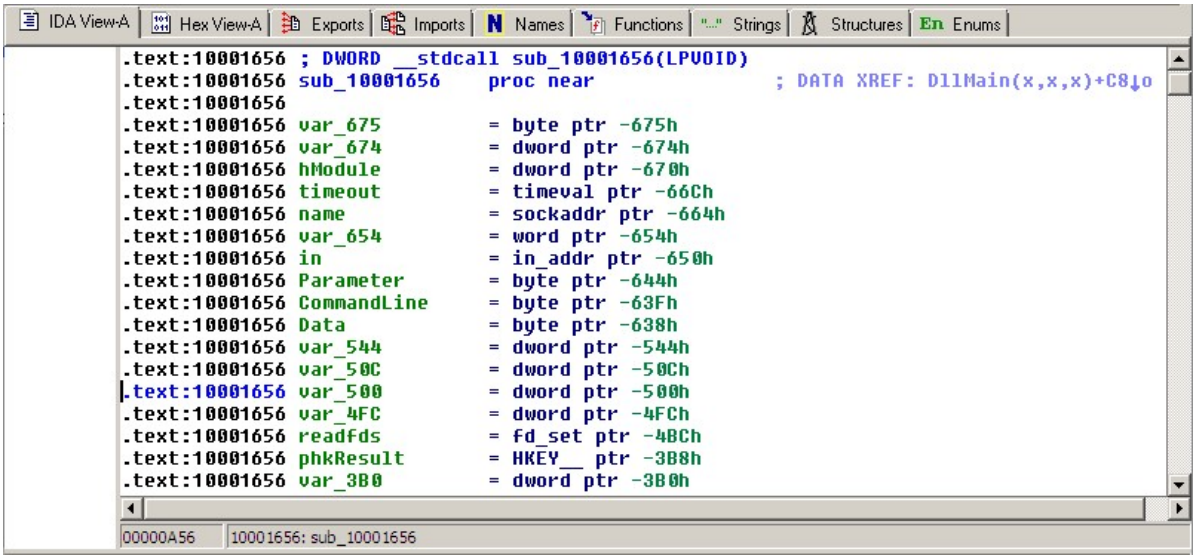
Find import for gethostbyname

IDA Pro > Windows > Imports > click Name header to sort by name > locate gethostbyname



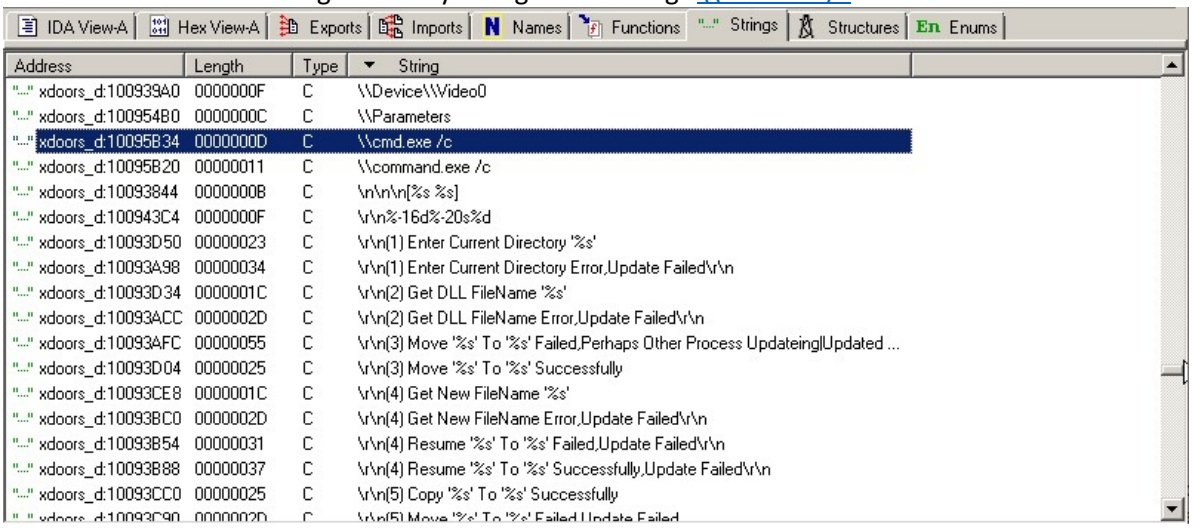
Local Variables Count for Subroutine at 0x10001656

IDA Pro > Windows > IDA View-A > press SPACEBAR for text view > press g for Go > enter address 0x10001656 > OK

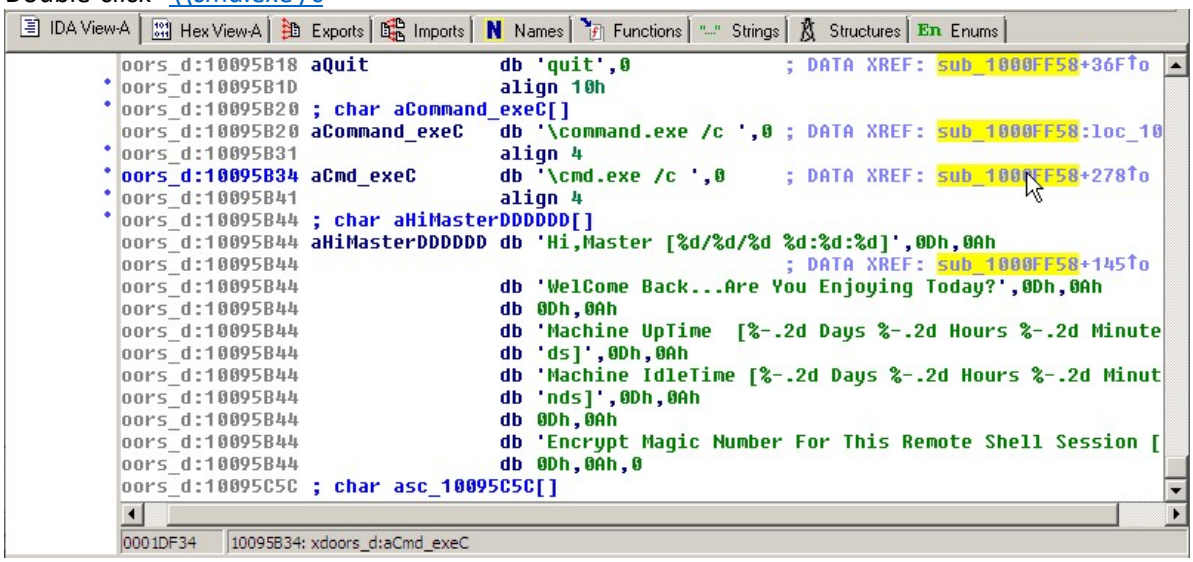


Purpose of \cmd.exe /c Code Reference

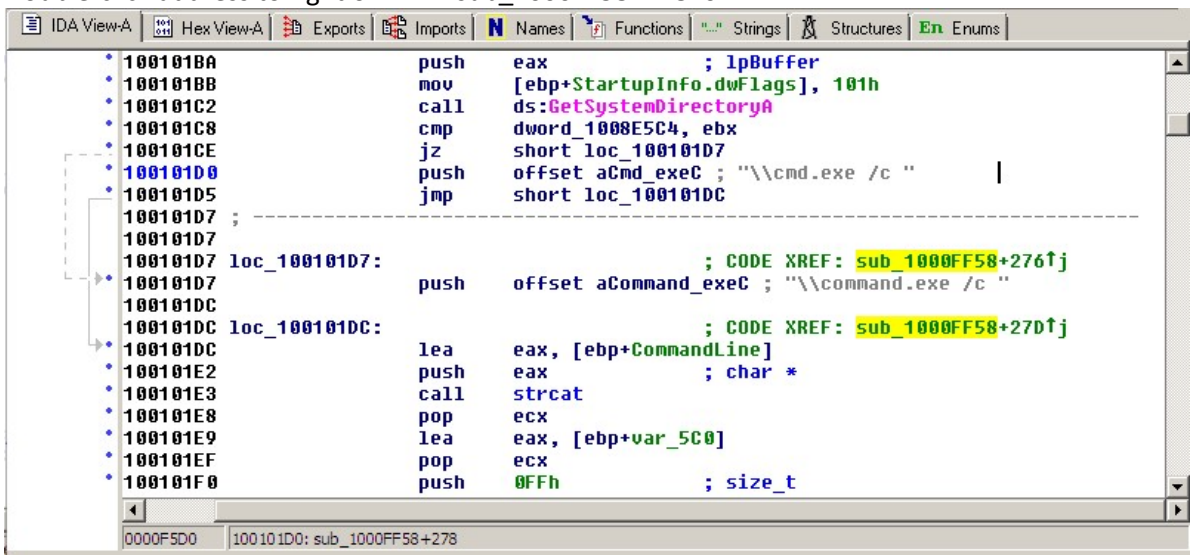
IDA Pro > Windows > Strings > sort by String > find String "\\cmd.exe /c"



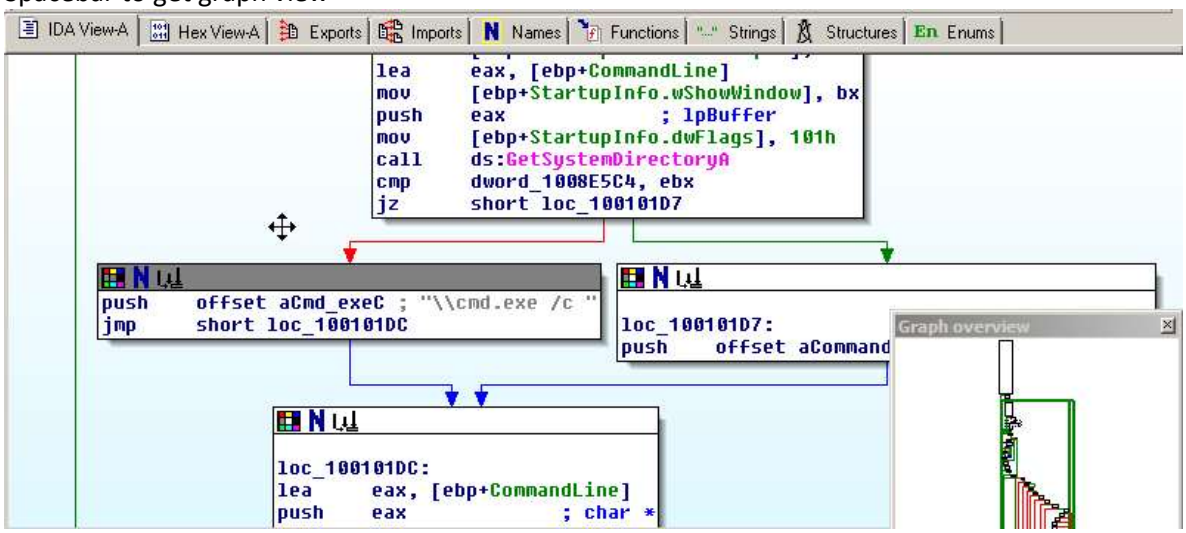
Double-click "\\cmd.exe /c"



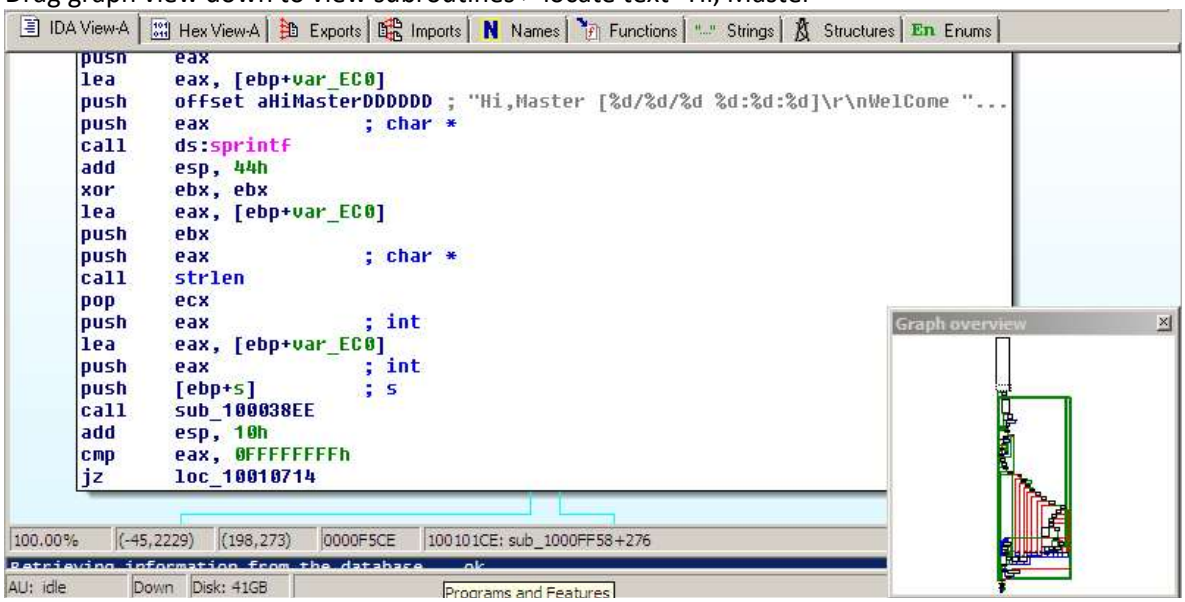
Double-click address to right of XREF: sub_1000FF58+278^0



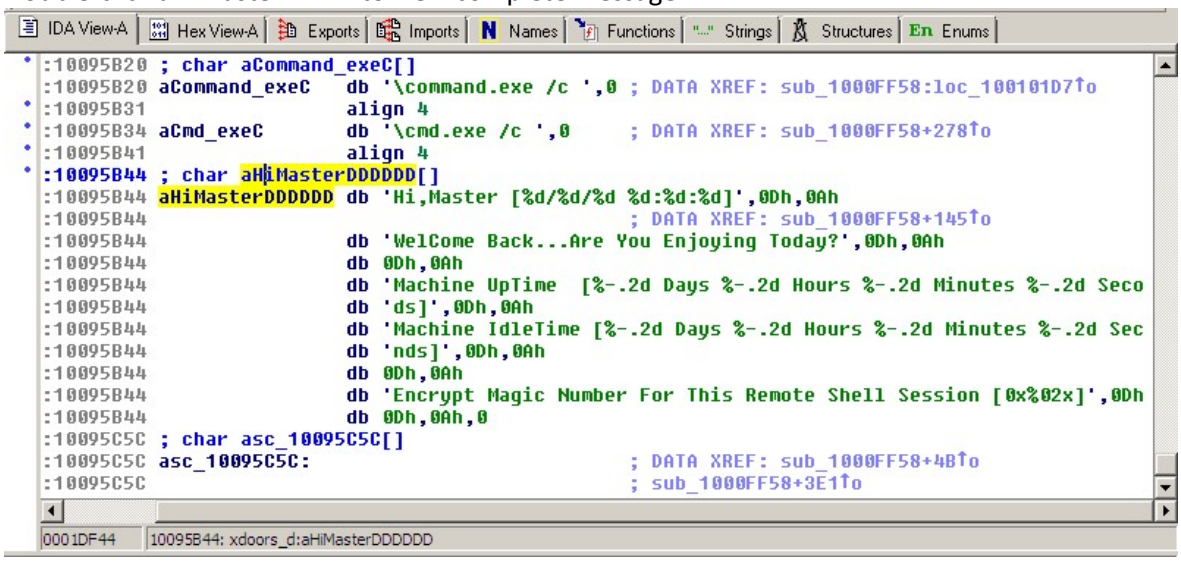
Spacebar to get graph view



Drag graph view down to view subroutines > locate text "Hi, Master"



Double-click aHiMasterDDDD to view complete message

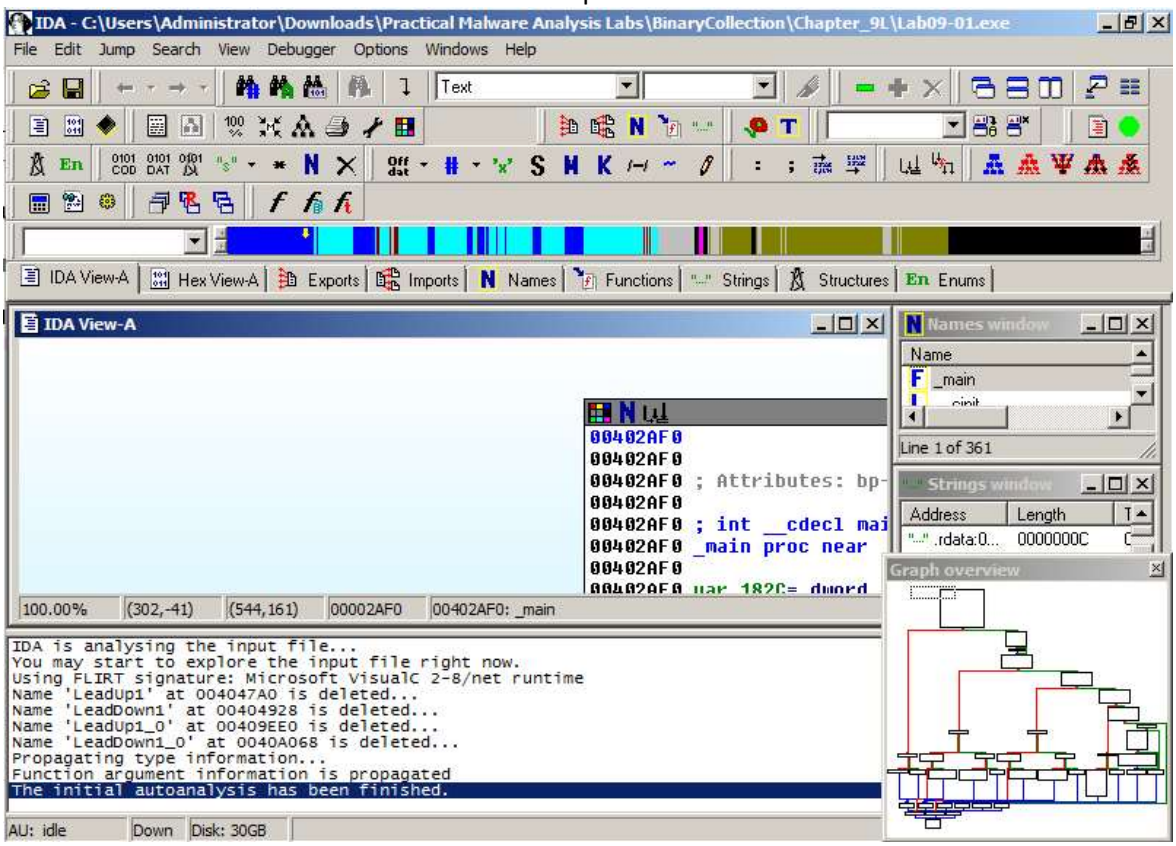


Malware purpose: Encrypt Magic Number for This Remote Shell Session [0x%02x]

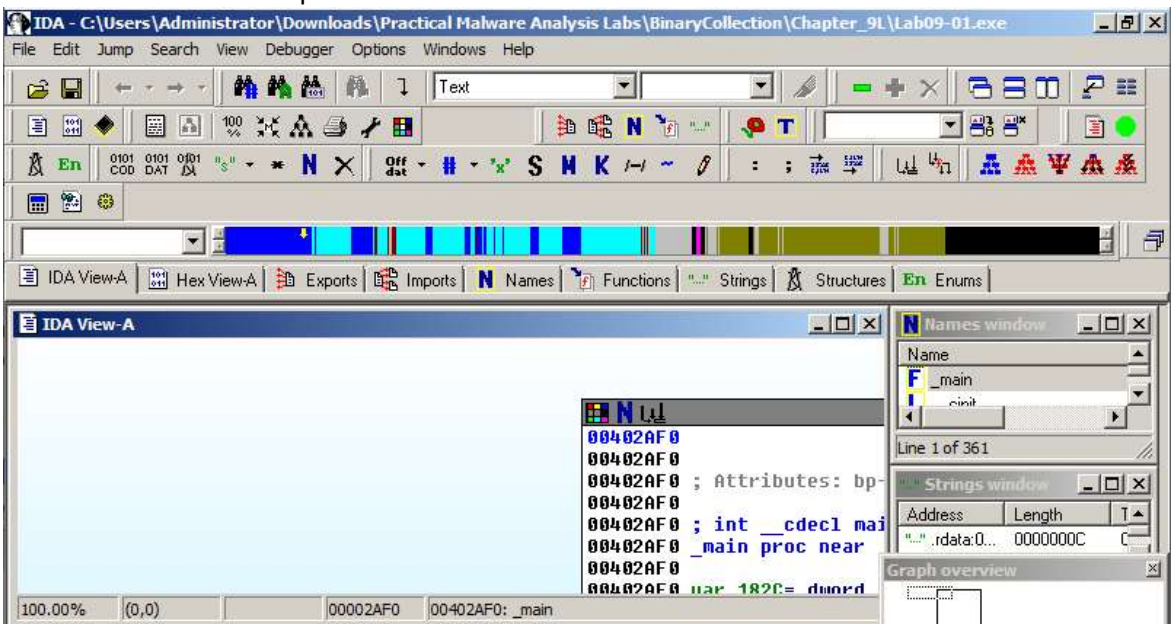
Chapter 9: OllyDBG - Lab9-1
File: Lab09-01.exe

OllyDbg 1.10[72] Analysis

Find Main Entry Point
IDA Pro Free > PE Executable > Lab09-01.exe > Options > General > check Line Prefixes > OK

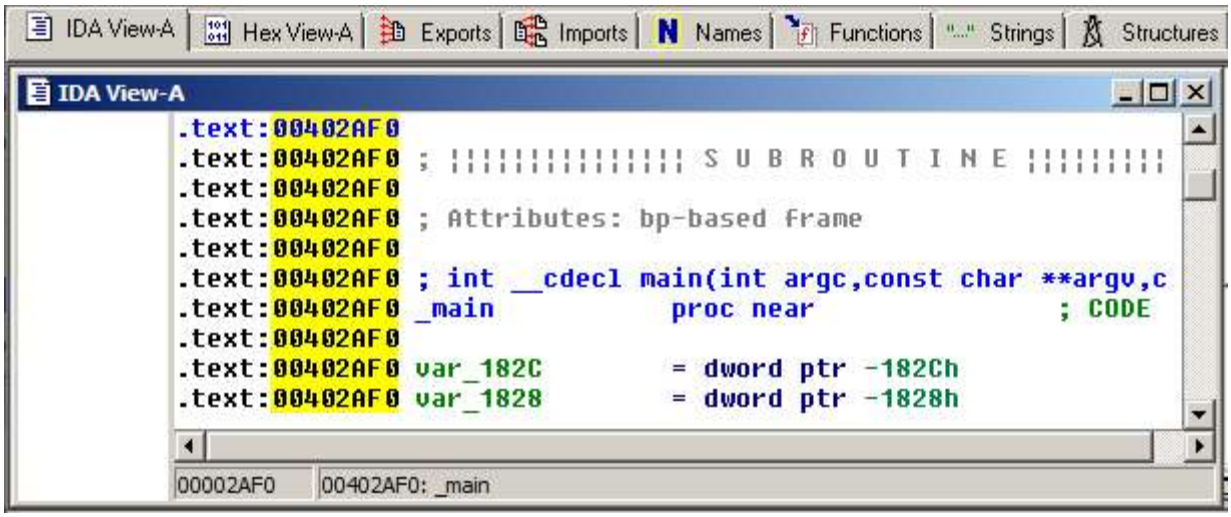


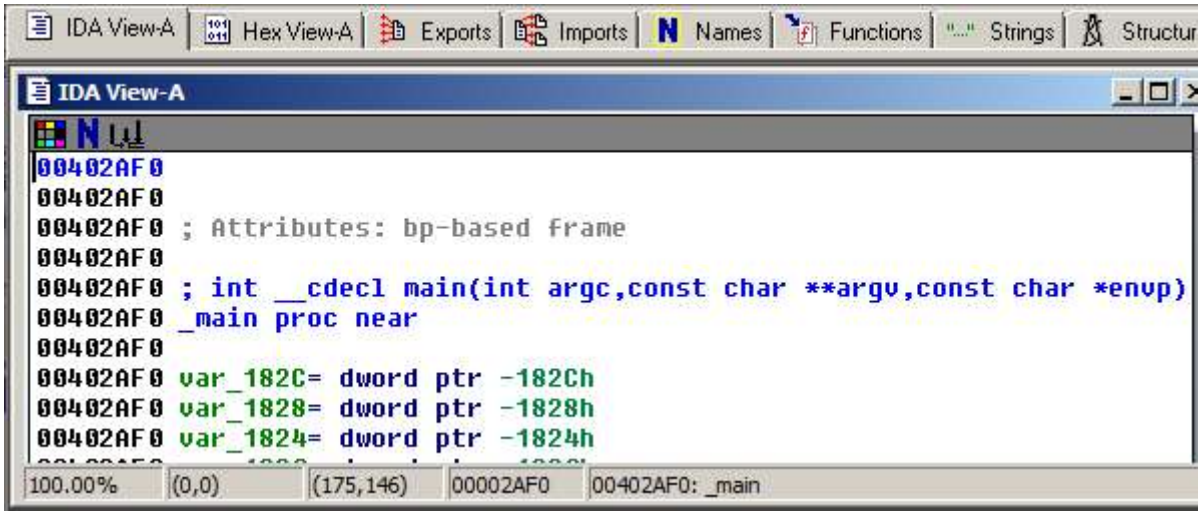
Windows > Reset Desktop



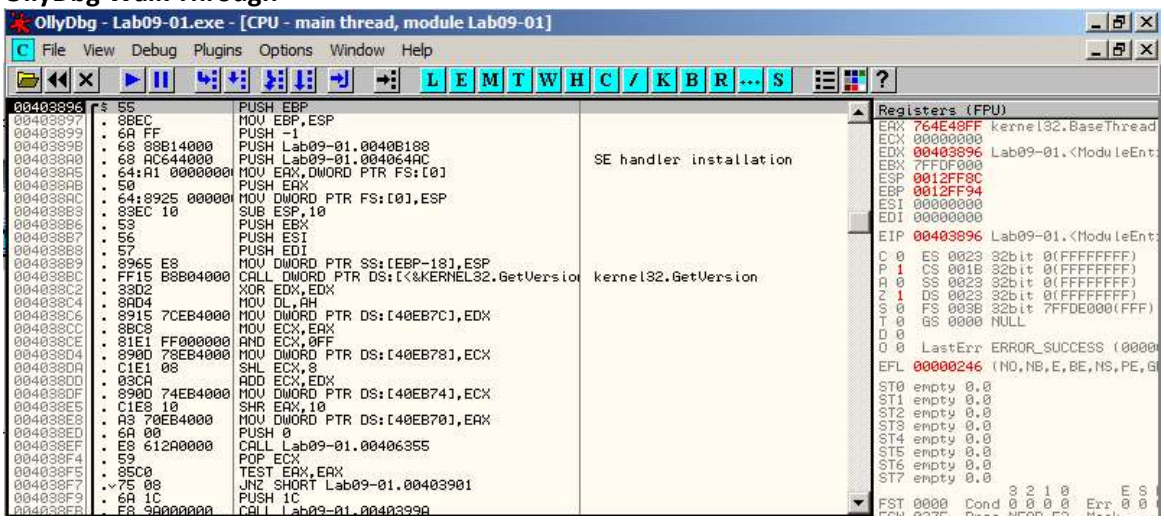
[72] OllyDBG (2019) Download OllyDbg 1.10 (final version) http://www.ollydbg.de/download.htm [Accessed 22nd May 2019].

Main starts at 0x402AF0

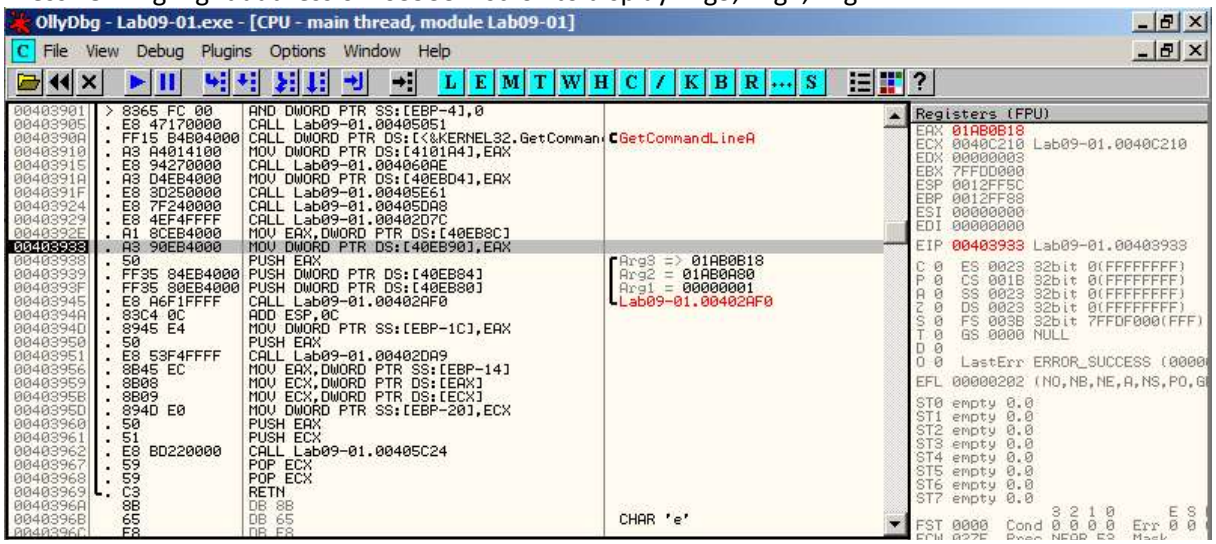




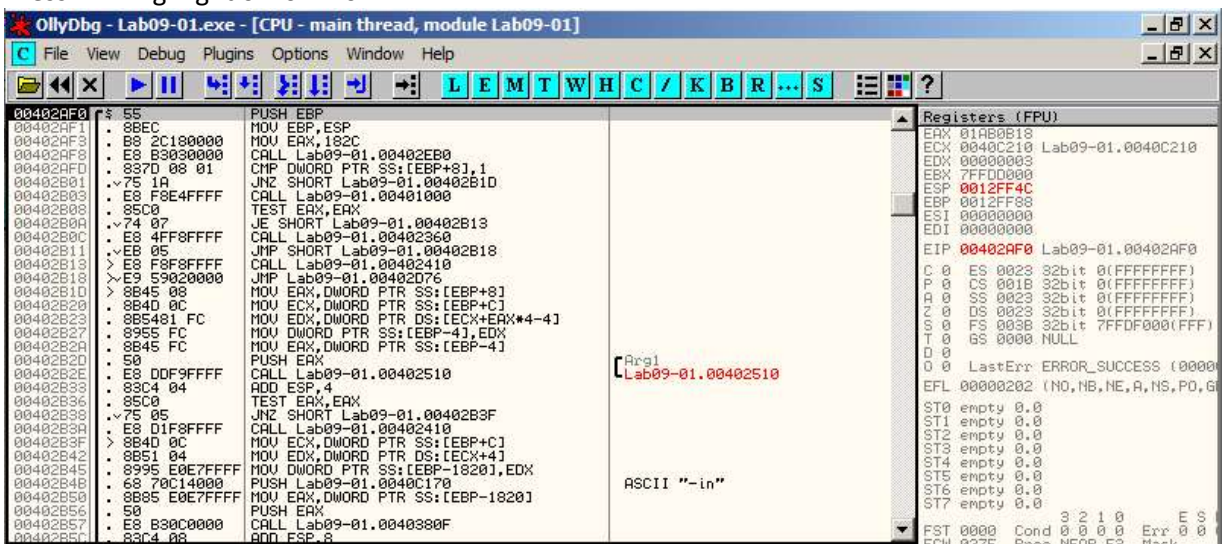
OllyDbg Walk Through



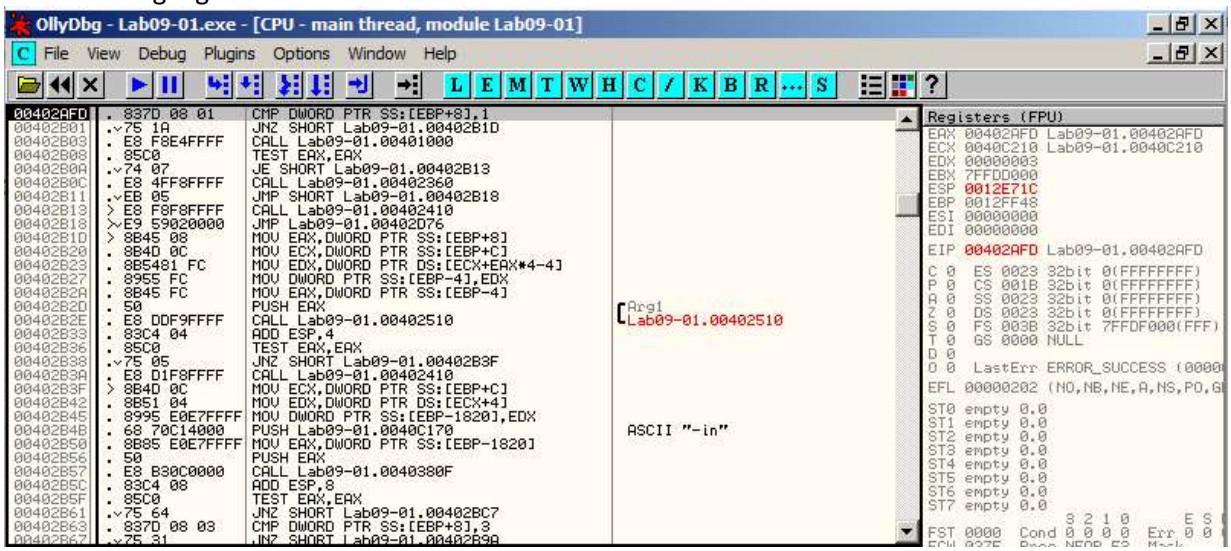
Press F8 > highlight address 0x403933 > scroll to display Arg3, Arg2, Arg1



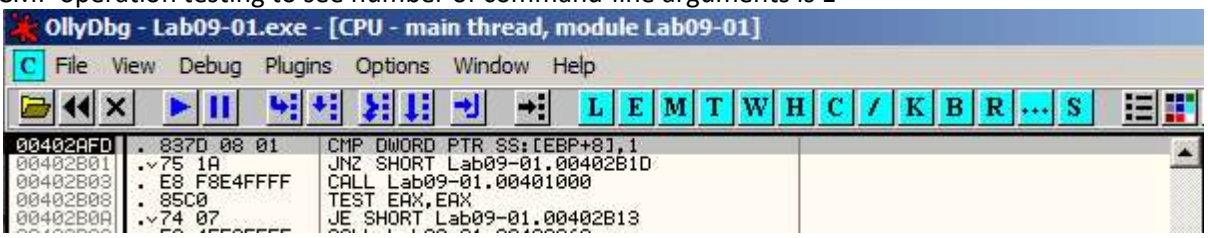
Press F7 > highlight 0x402AF0



Press F7 > highlight 0x402AFD

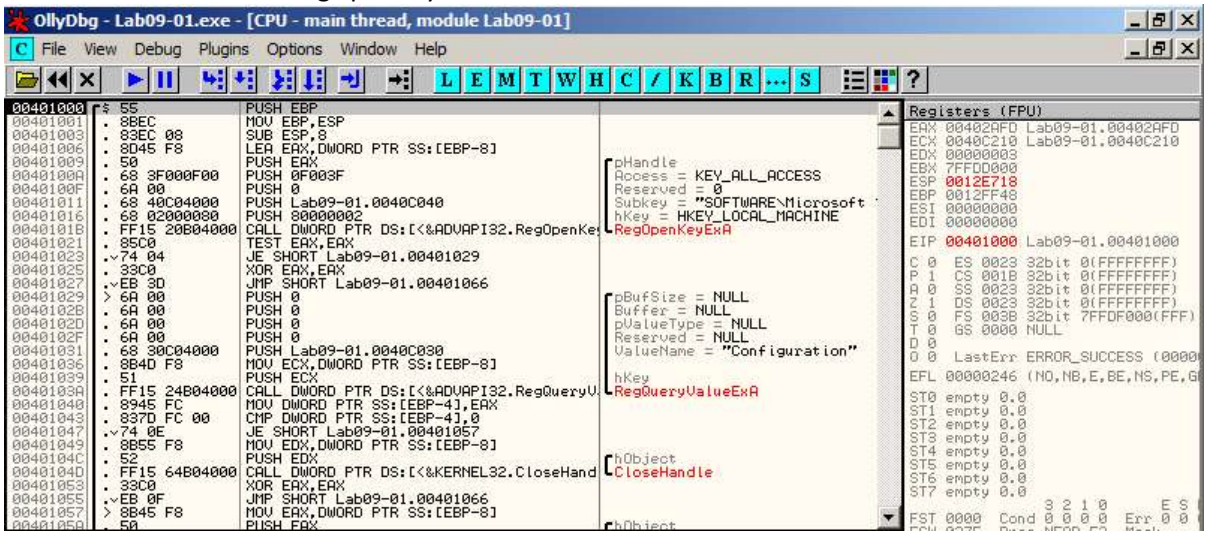


CMP operation testing to see number of command-line arguments is 1



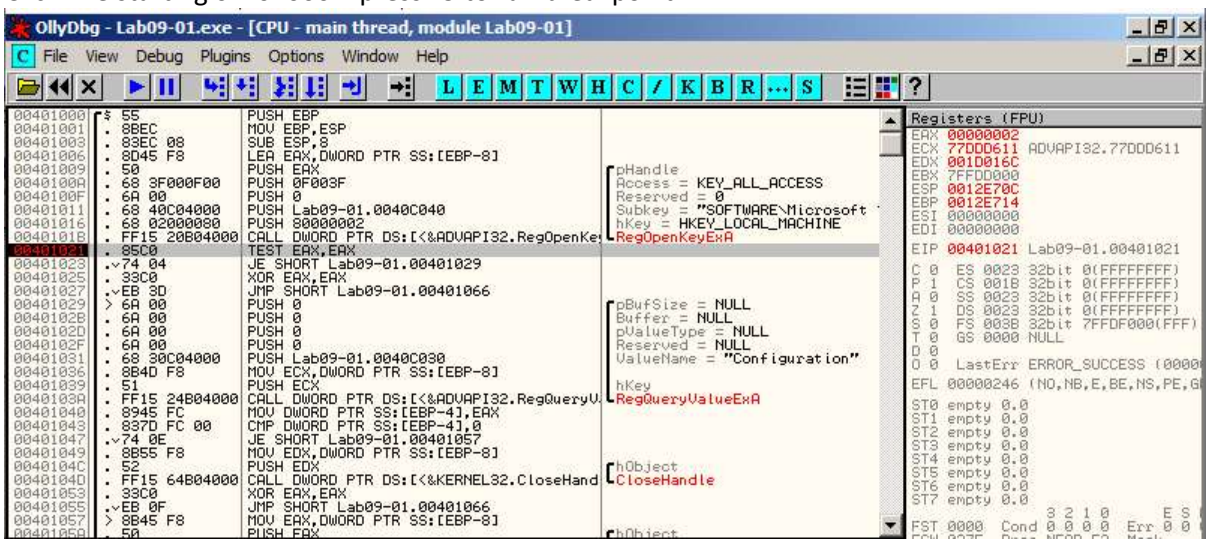
F7 x3 to pass test and go to 0x00401000

Routine 0x401000 calls RegOpenKeyExA at 0x40101B

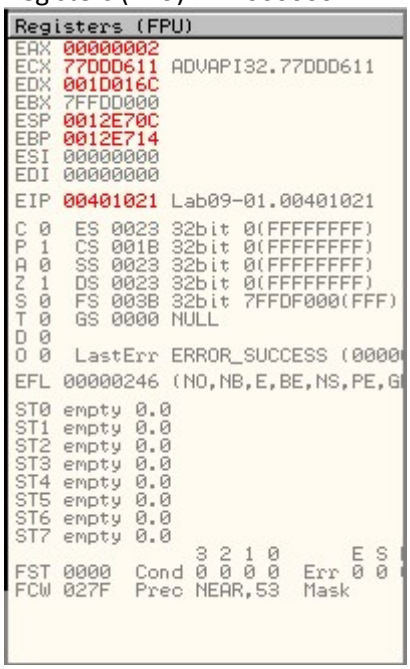


Click line starting 0x401021 > press F2 to insert breakpoint (address turns red)

Click line starting 0x401000 > press F9 to run breakpoint



Registers (FPU) EAX 0000002



Non-zero error code which means the registry key was not found

RegOpenKeyExA function[73]

Opens the specified registry key. Note that key names are not case sensitive.
To perform transacted registry operations on a key, call the RegOpenKeyTransacted function.

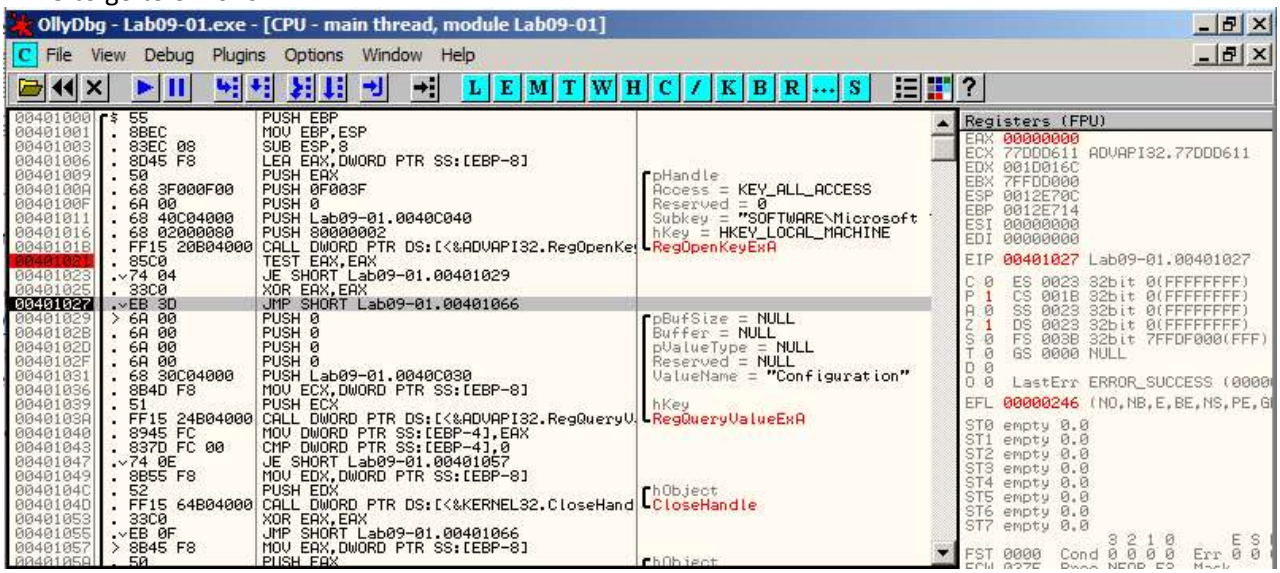
C++ Syntax

```
LSTATUS RegOpenKeyExA(
  HKEY   hKey,
  LPCSTR lpSubKey,
  DWORD  ulOptions,
  REGSAM samDesired,
  PHKEY  phkResult
);
```

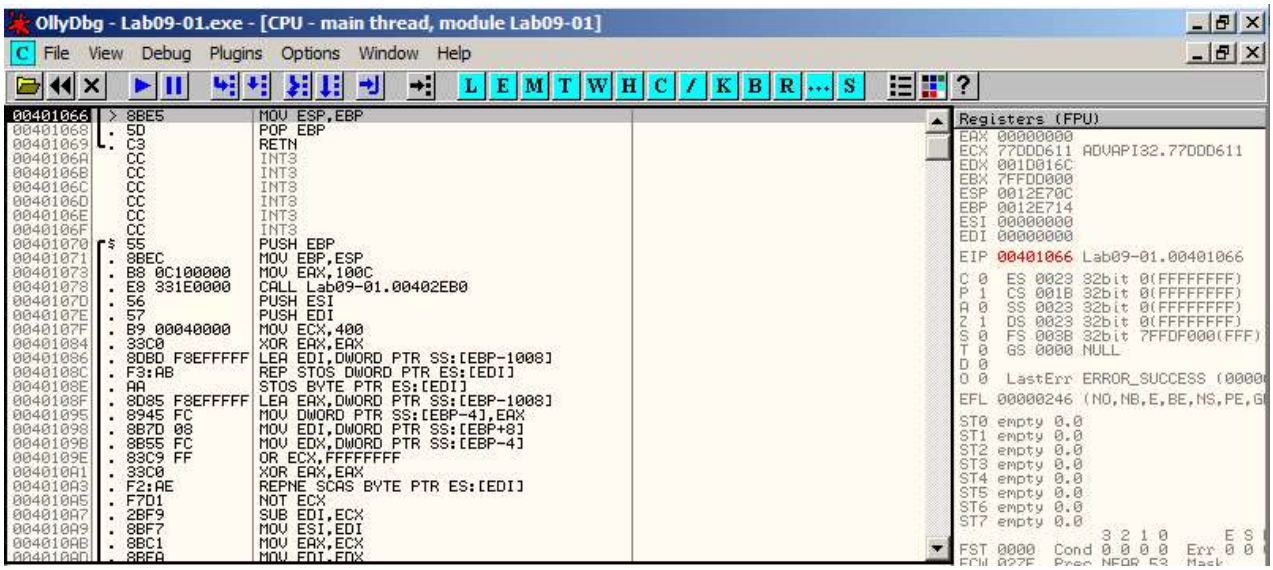
hKey: A handle to an open registry key. Predefined keys:
HKEY_CLASSES_ROOT HKEY_CURRENT_CONFIG HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE HKEY_USERS
lpSubKey: The name of the registry subkey to be opened.
ulOptions: Specifies the option to apply when opening the key
samDesired: A mask that specifies the desired access rights to the key to be opened
phkResult: A pointer to a variable that receives a handle to the opened key

[73] Microsoft.com (2019) *RegOpenKeyExA function* http://msdn.microsoft.com/en-us/library/windows/desktop/ms724897(v=vs.85).aspx [Accessed 22nd May 2019].

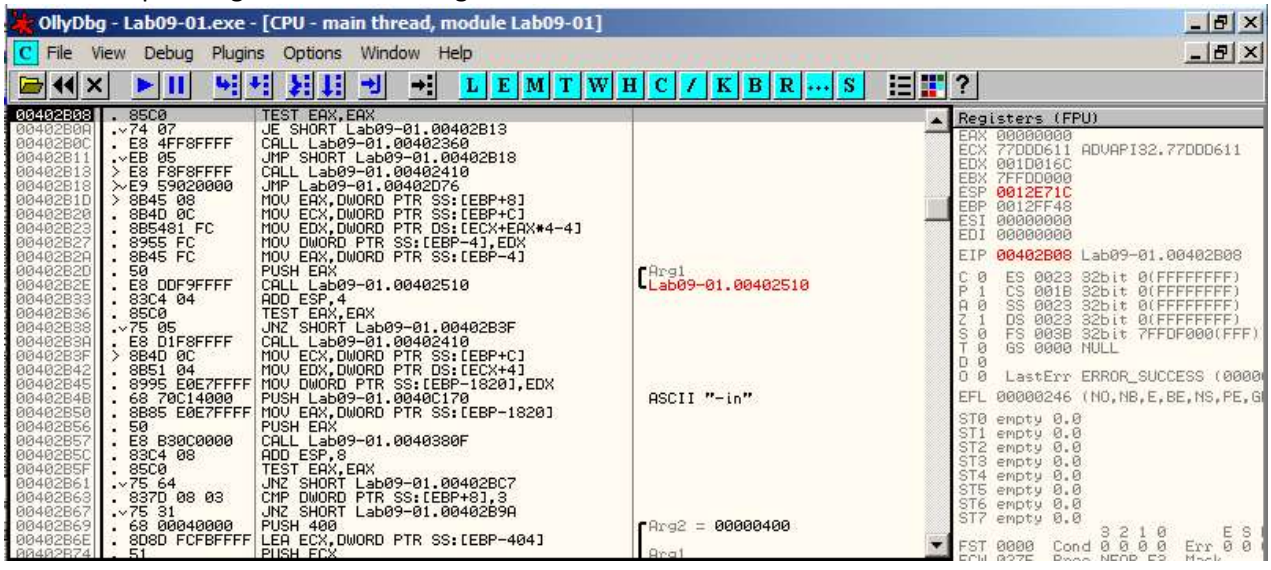
F7 x3 to go to 0x401027



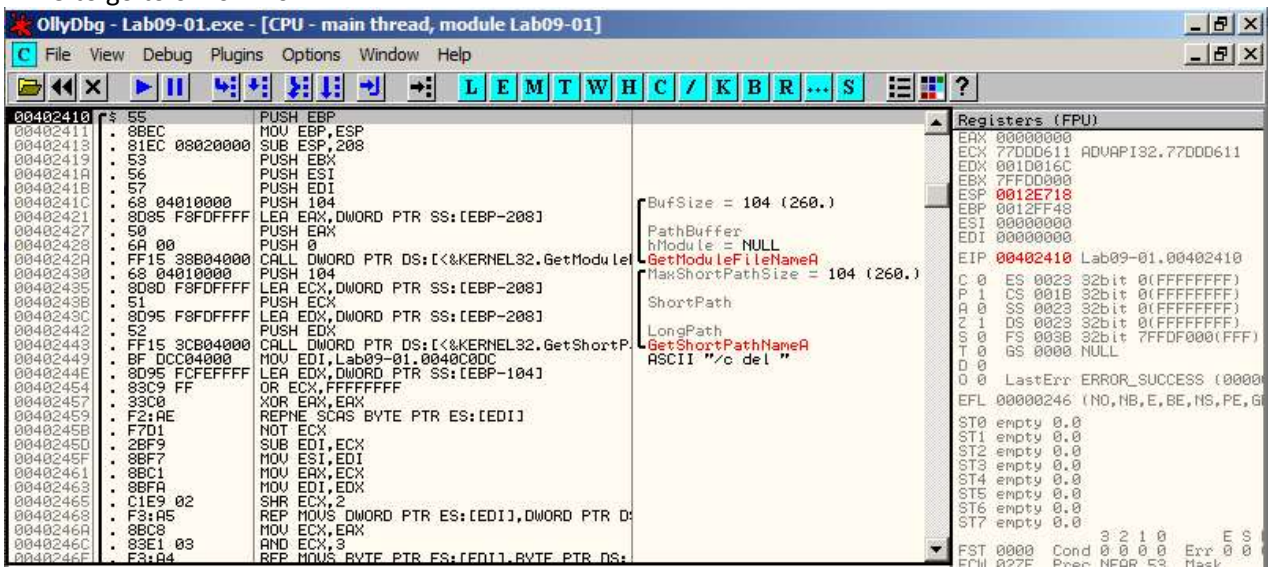
F7 to execute JMP



F7 x3 to step through subroutine and get to 0x402B08

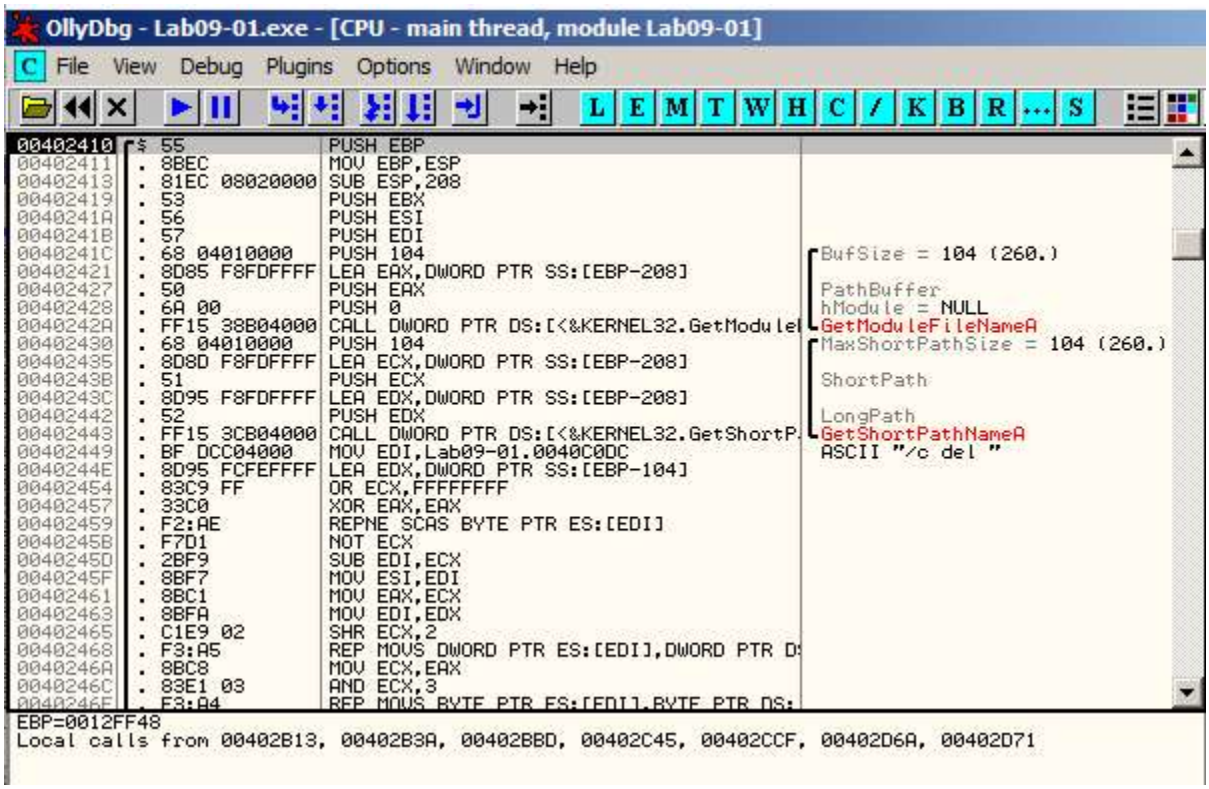


F7 x3 to go to 0x402410

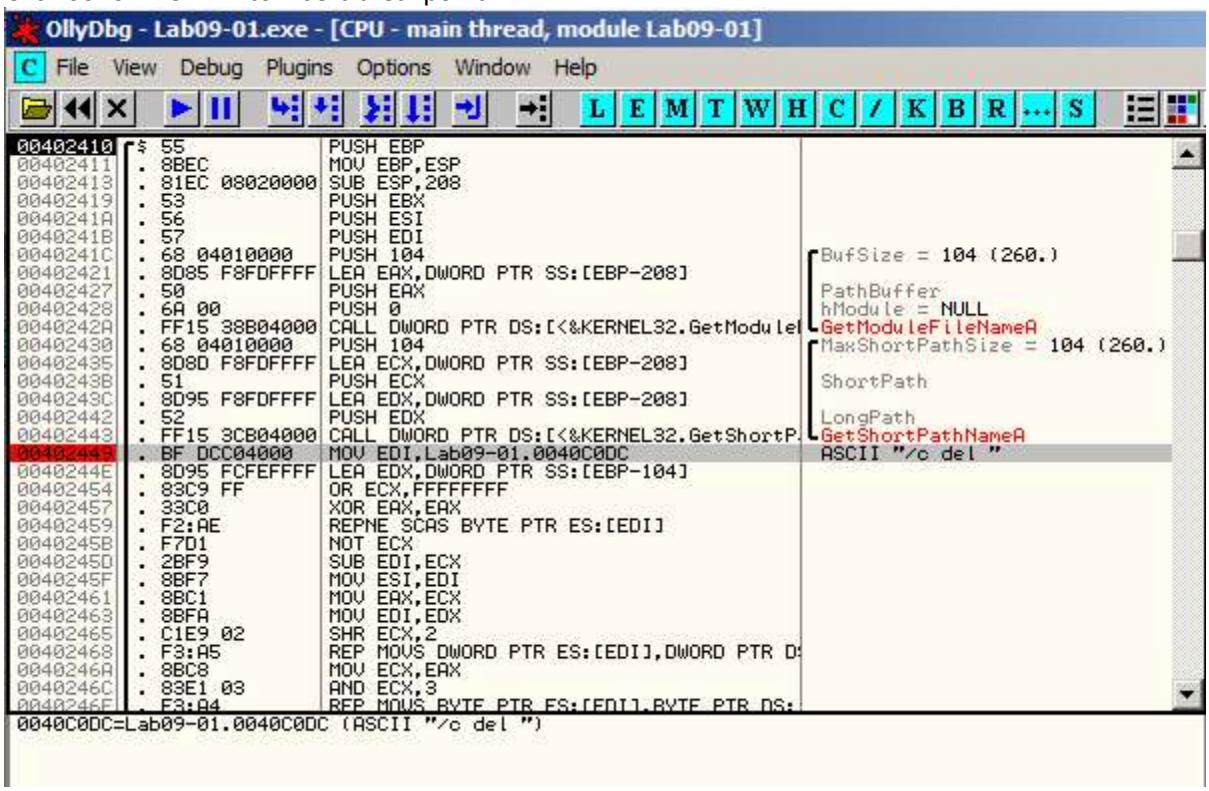


GetModuleFilename function to get path to current exe and builds ASCII string

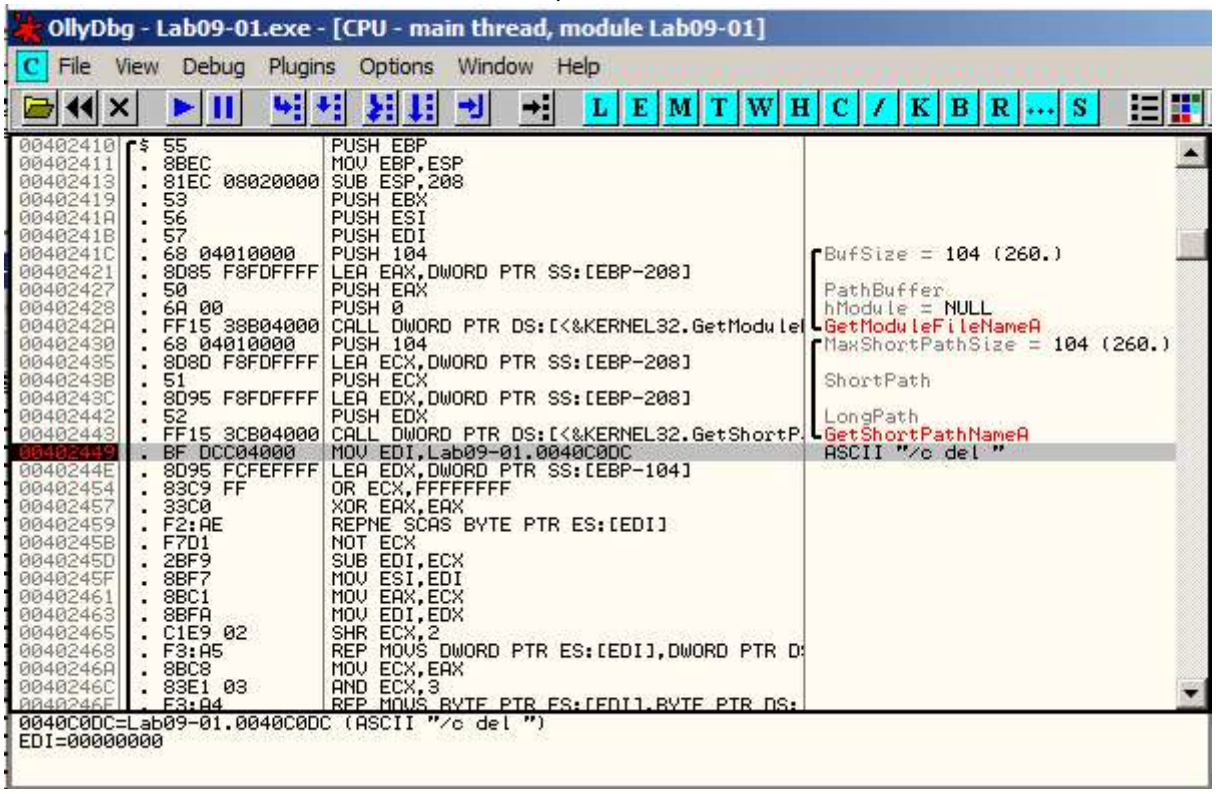
/c del path-to-executable >> NUL



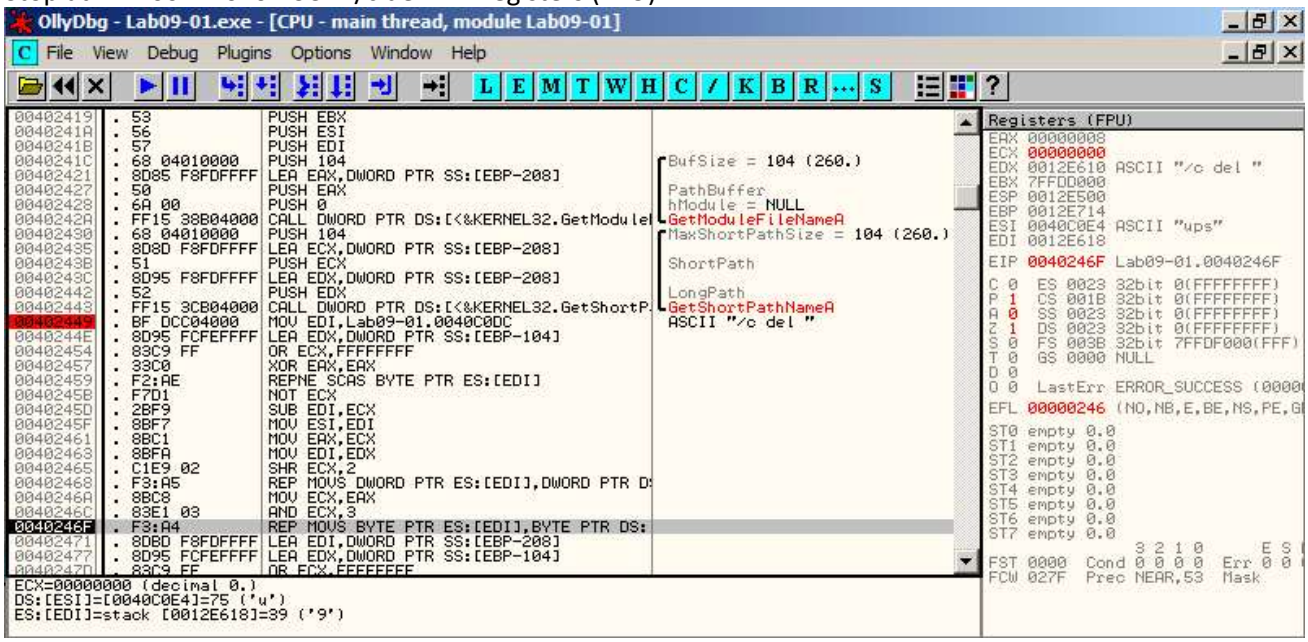
Click 00402449 > F2 to insert breakpoint



Click line 0x402410 > F9 to run breakpoint
Runs to line 00402449 which ends with ASCII "/c del "



Press F7 to 'play' the code forward
Stop at EDX 0012E610 ASCII "/c del " in Registers (FPU)



Chapter 11: Malware Behaviour - Lab11-1

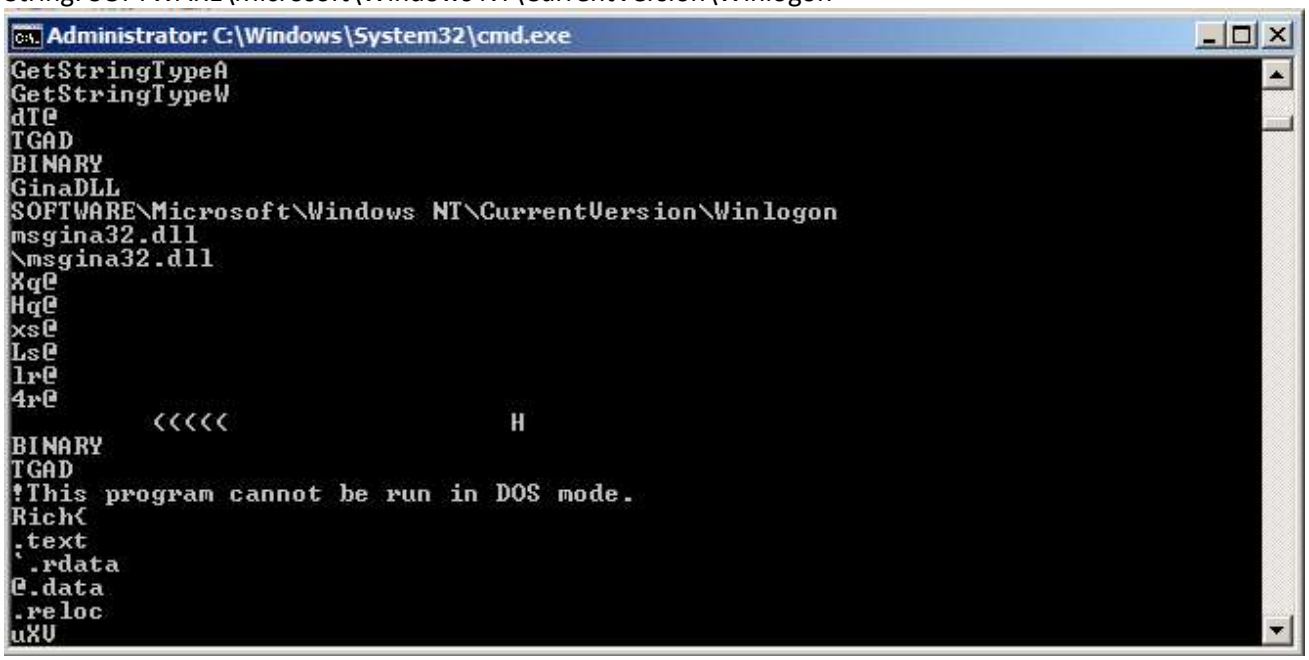
Source Files URL: https://github.com/mikesiko/PracticalMalwareAnalysis-Labs [74]

File: Chapter_11L\Lab-01.exe

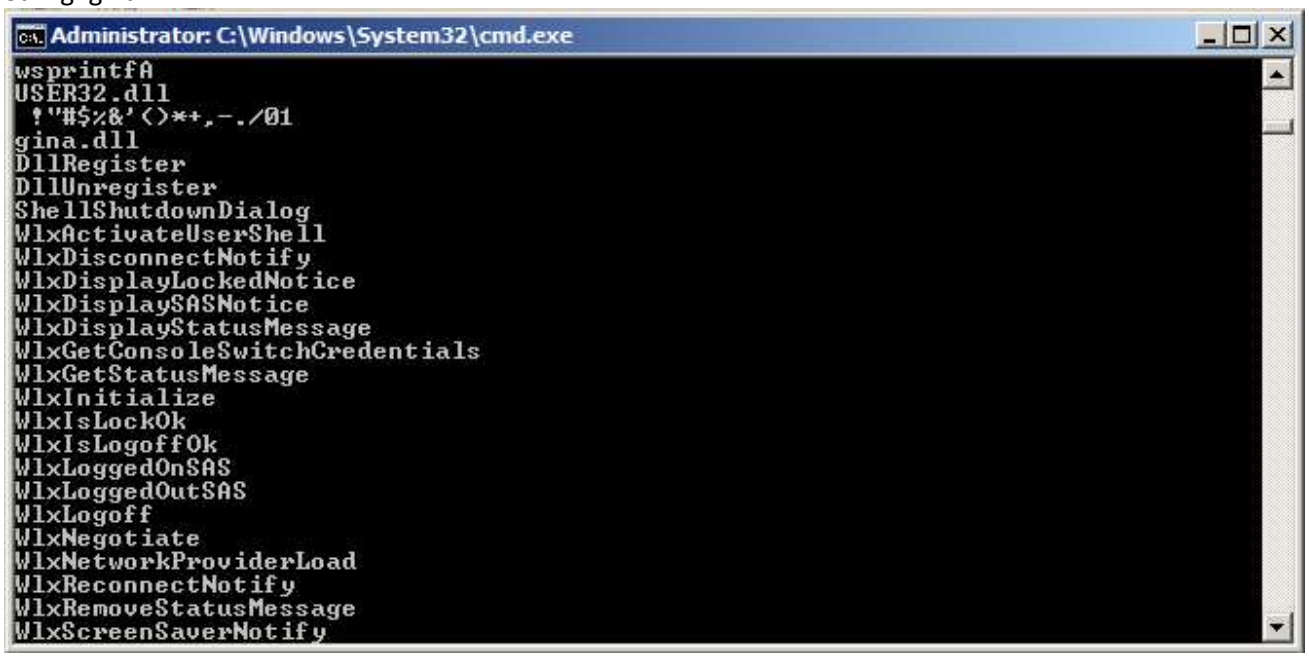
Strings[75] Analysis

(Admin)C:\>strings C:\Users\Administrator\Downloads\Practical Malware Analysis\BinaryCollection\Chapter_11L\Lab-01.exe

String: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon



String: gina.DLL



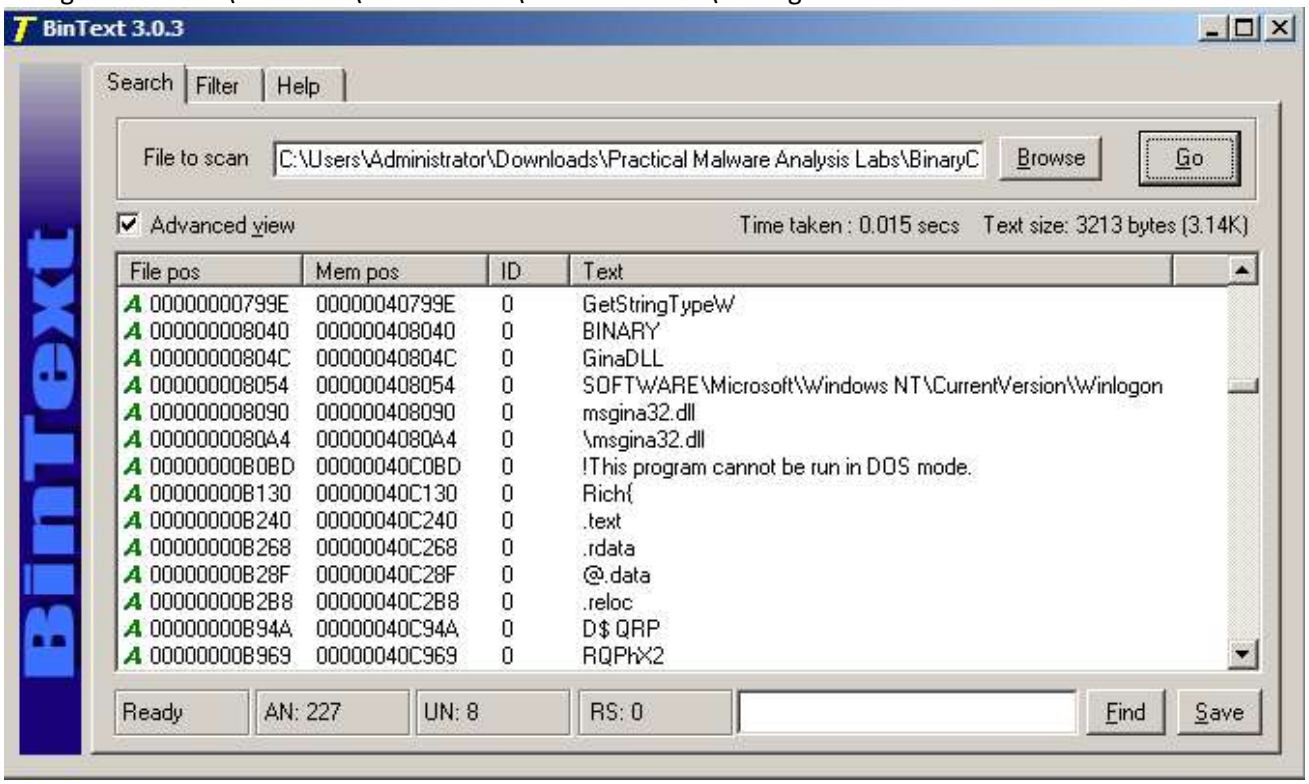
[74] PracticalMalwareAnalysis-Labs (2017) *Binaries for the book Practical Malware Analysis* https://github.com/mikesiko/PracticalMalwareAnalysis-Labs [Accessed 22nd May 2019].

[75] Microsoft.com (2019) *Strings v2.53* https://docs.microsoft.com/en-gb/sysinternals/downloads/strings [Accessed 22nd May 2019].

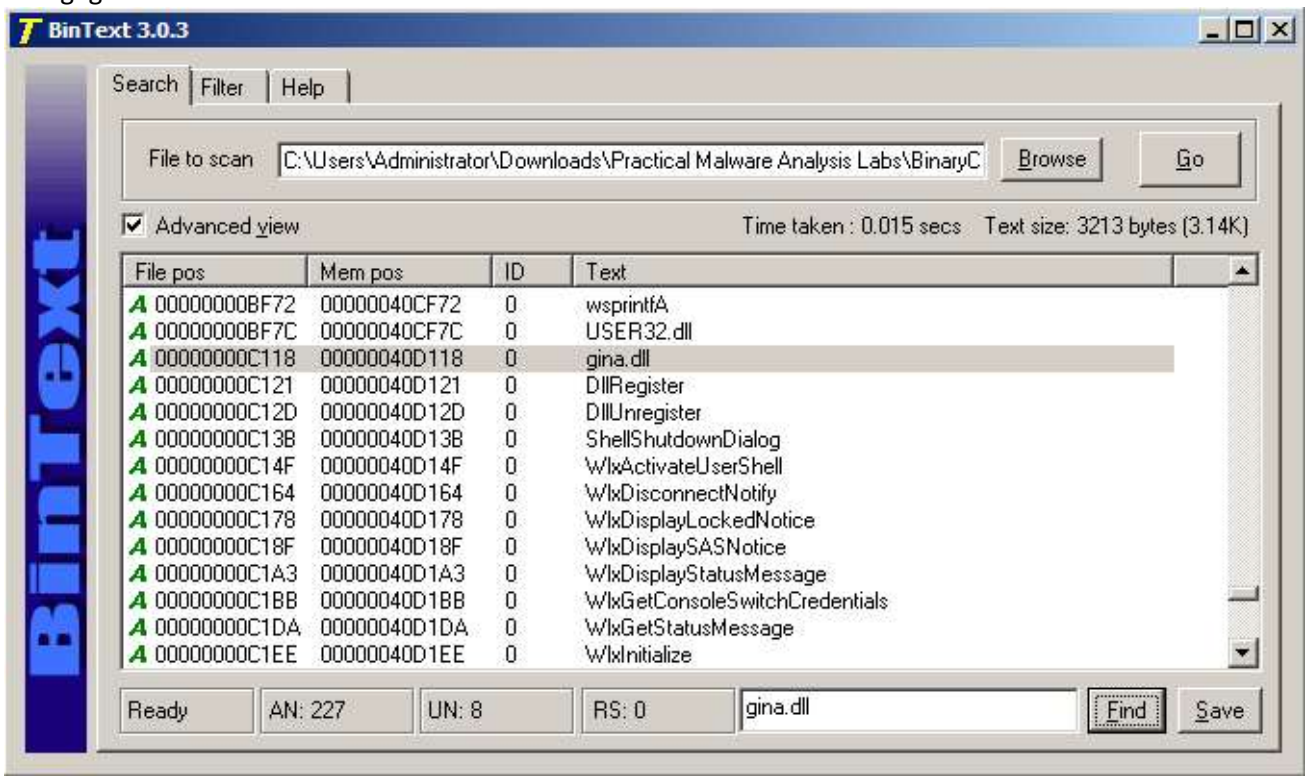
BinText 3.03[76] Analysis

C:\Users\Administrator\Downloads\Practical Malware Analysis\BinaryCollection\Chapter_11L\Lab-01.exe

String: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon



String: gina.DLL



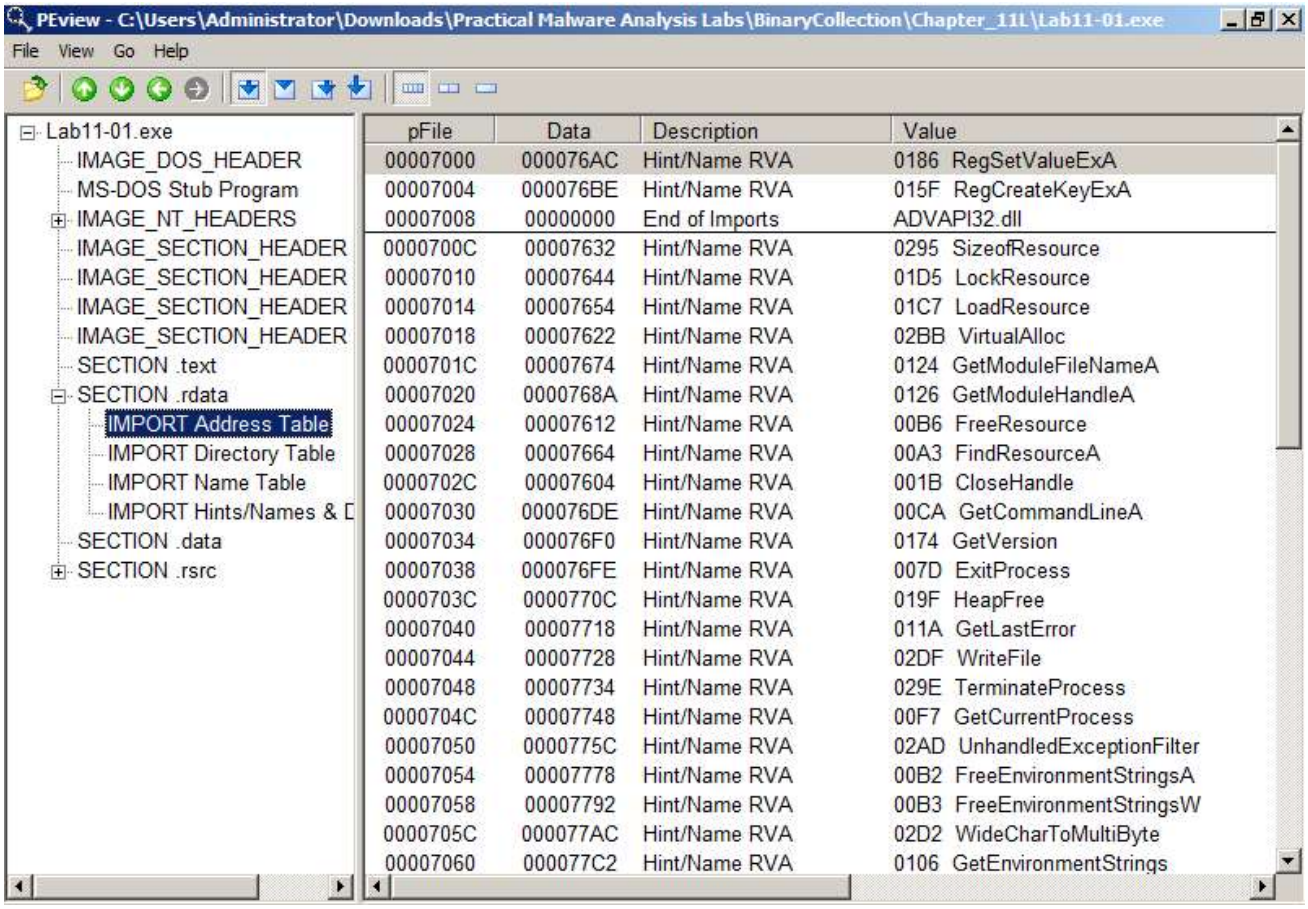
[76] Softpedia.com (2019) *BinText 3.03* https://www.softpedia.com/get/System/File-Management/BinText.shtml [Accessed 22nd May 2019].

GINA Interception Malware
GINA-Graphical Identification and Authentication [77]

The Graphical Identification and Authentication (GINA) is a component of Windows 2000, Windows XP and Windows Server 2003 that provides secure authentication and interactive logon services
GINA is discontinued in Windows Vista

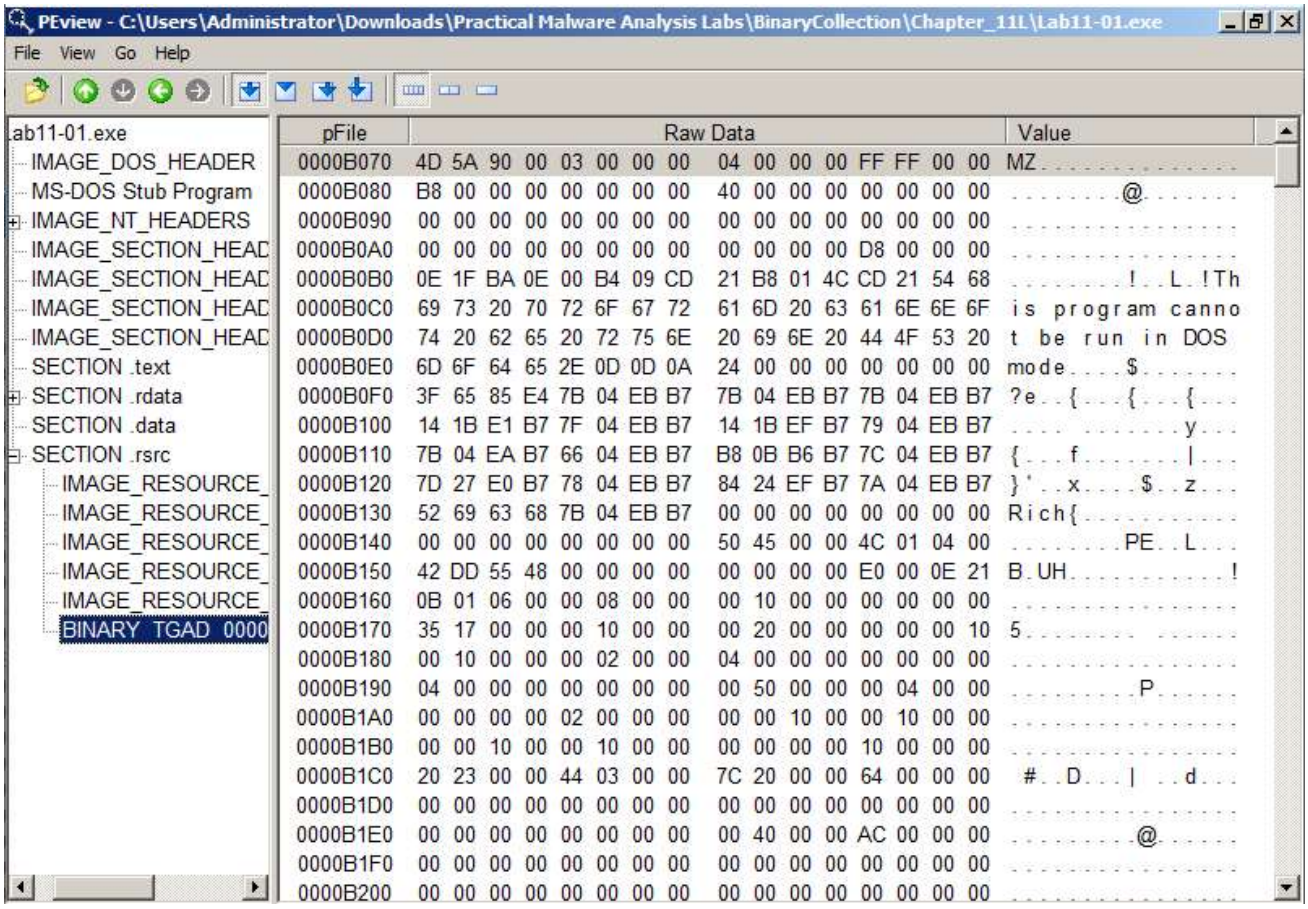
On Windows XP, GINA interception is a technique that malware uses to steal user credentials.
GINA is implemented in a DLL, msgina.dll, and is loaded by the Winlogon executable during the login process.
The GINA interception consists of injecting a malicious DLL between winlogon.exe and msgina.dll to intercept credentials

PEview[78] Static Analysis
C:\Users\Administrator\Downloads\Practical Malware Analysis\BinaryCollection\Chapter_11L\Lab-01.exe



[77] Aldeid (2019) *GINA-Graphical Identification and Authentication* https://www.aldeid.com/wiki/GINA-Graphical_Identification_and_Authentication [Accessed 22nd May 2019].
[78] Radburn, Wayne J. (2018) *PEview version 0.9.9 (.zip 31KB)* http://wjradburn.com/software/ [Accessed 22nd May 2019].

BINARY TGAD 0000

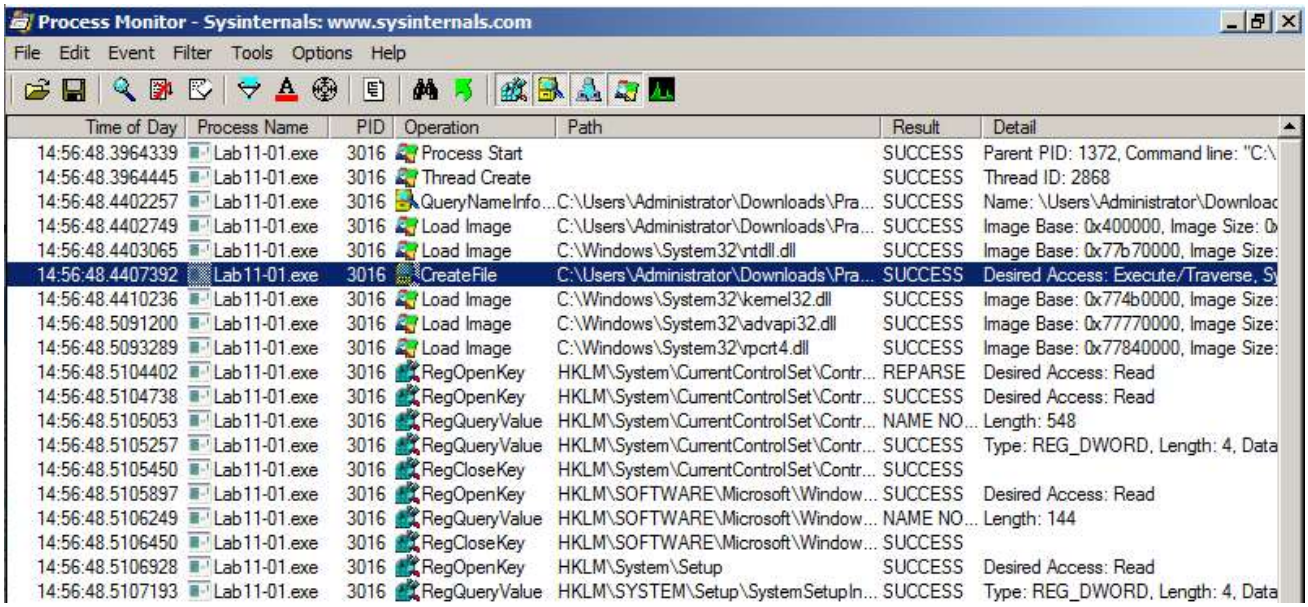


Procmon[79] Dynamic Analysis

Run C:\Users\Administrator\Downloads\Practical Malware Analysis\BinaryCollection\Chapter_11L\Lab-01.exe

Procmon > Filter > Reset Filter

Filter > Filter > Filter for: Process Name Lab11-01.exe > Add

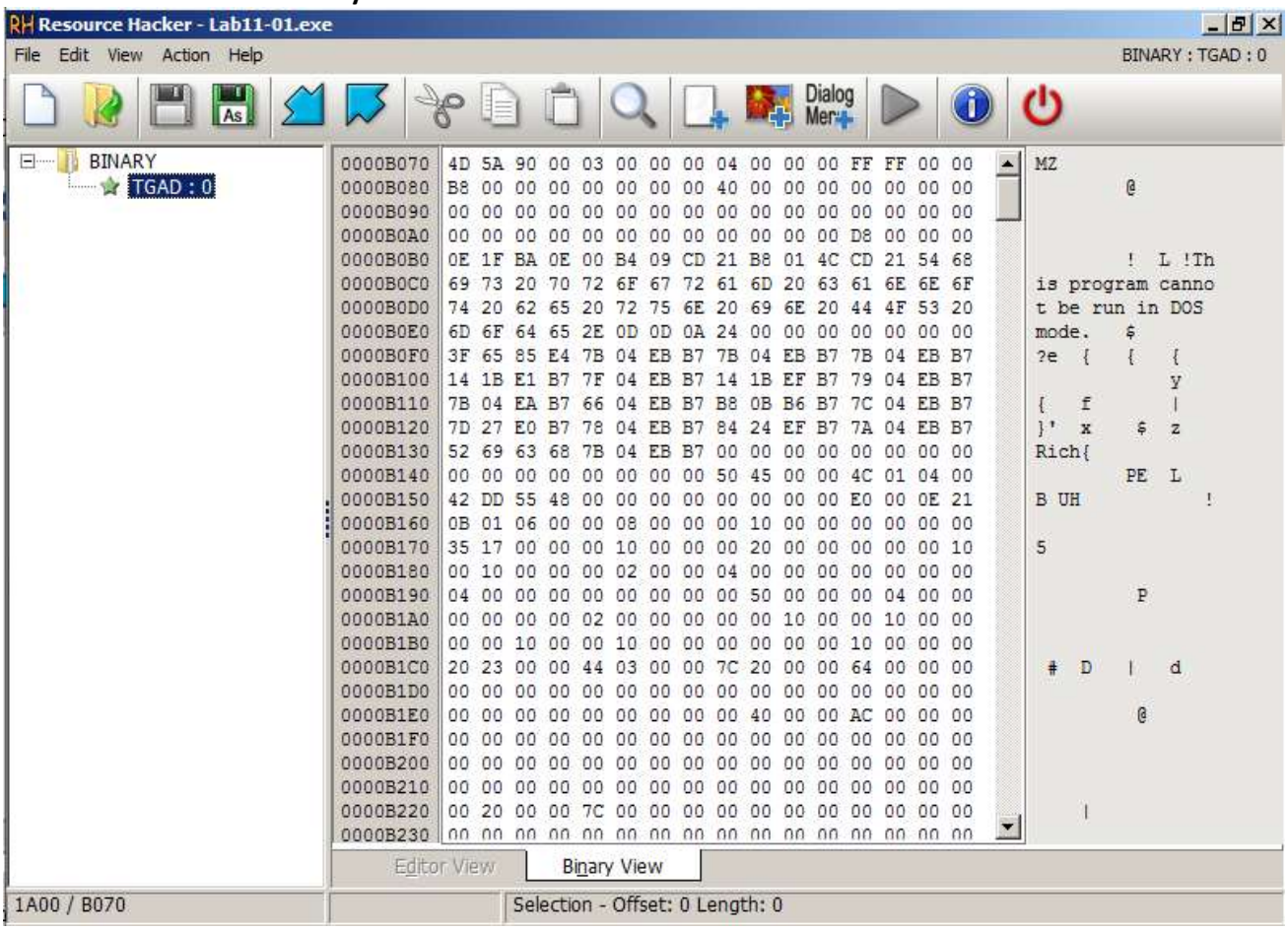


[79] Microsoft.com (2019) *Process Monitor v3.52* https://docs.microsoft.com/en-gb/sysinternals/downloads/procmon [Accessed 20th May 2019].

Key Procmon Entries
CreateFile ... msgina32.dll or IRP_MU_CREATE ... msgina.dll
RegCreateKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
RegSetValue HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL

File created called msgina.dll
Registry key created
Registry path added to key
DLL will launch on next boot

Resource Hacker 5.1.7[80] Analysis



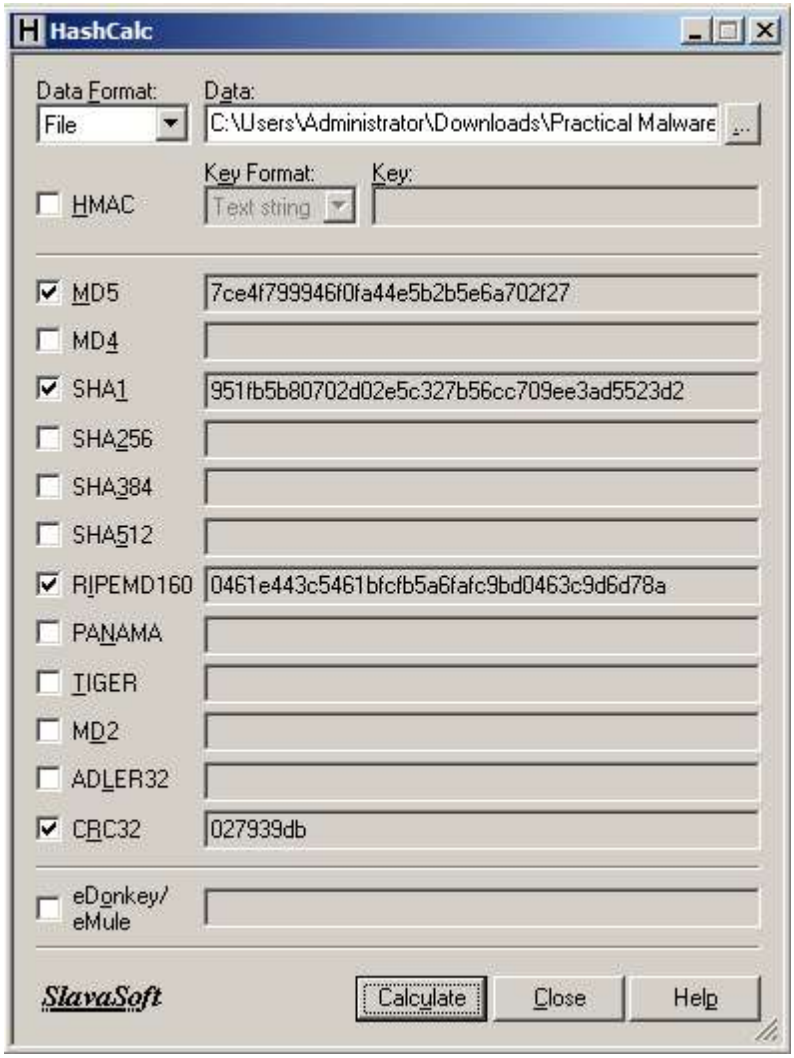
Resource Hacker > Action > Save *.bin resource... > Lab11-01-TAGD.exe

[80] Resource Hacker (2019) *Resource Hacker 5.1.7* http://www.angusj.com/resourcehacker/ [Accessed 20th May 2019].

HashCalc 2.02[81] Analysis

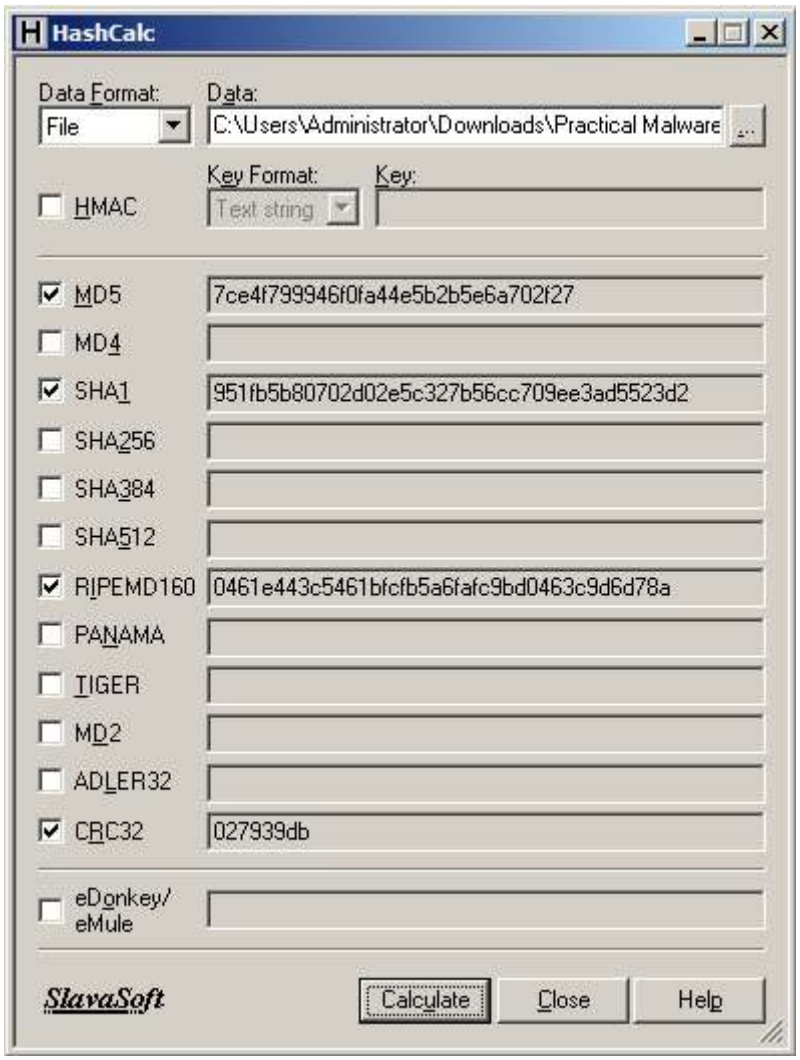
MD5 Hash of C:\Users\Administrator\Downloads\Practical Malware Analysis\BinaryCollection\Chapter_11L\msgina32.dll

MD5 hash: 7ce4f799946f0fa44e5b2b5e6a702f27



[81] SlavaSoft (2019) *HashCalc 2.02* http://www.slavasoft.com/hashcalc/ [Accessed 20th May 2019].

MD5 Hash of C:\Users\Administrator\Downloads\Practical Malware Analysis\BinaryCollection\Chapter_11L\Lab11-01-TAGD.exe
MD5 hash: 7ce4f799946f0fa44e5b2b5e6a702f27



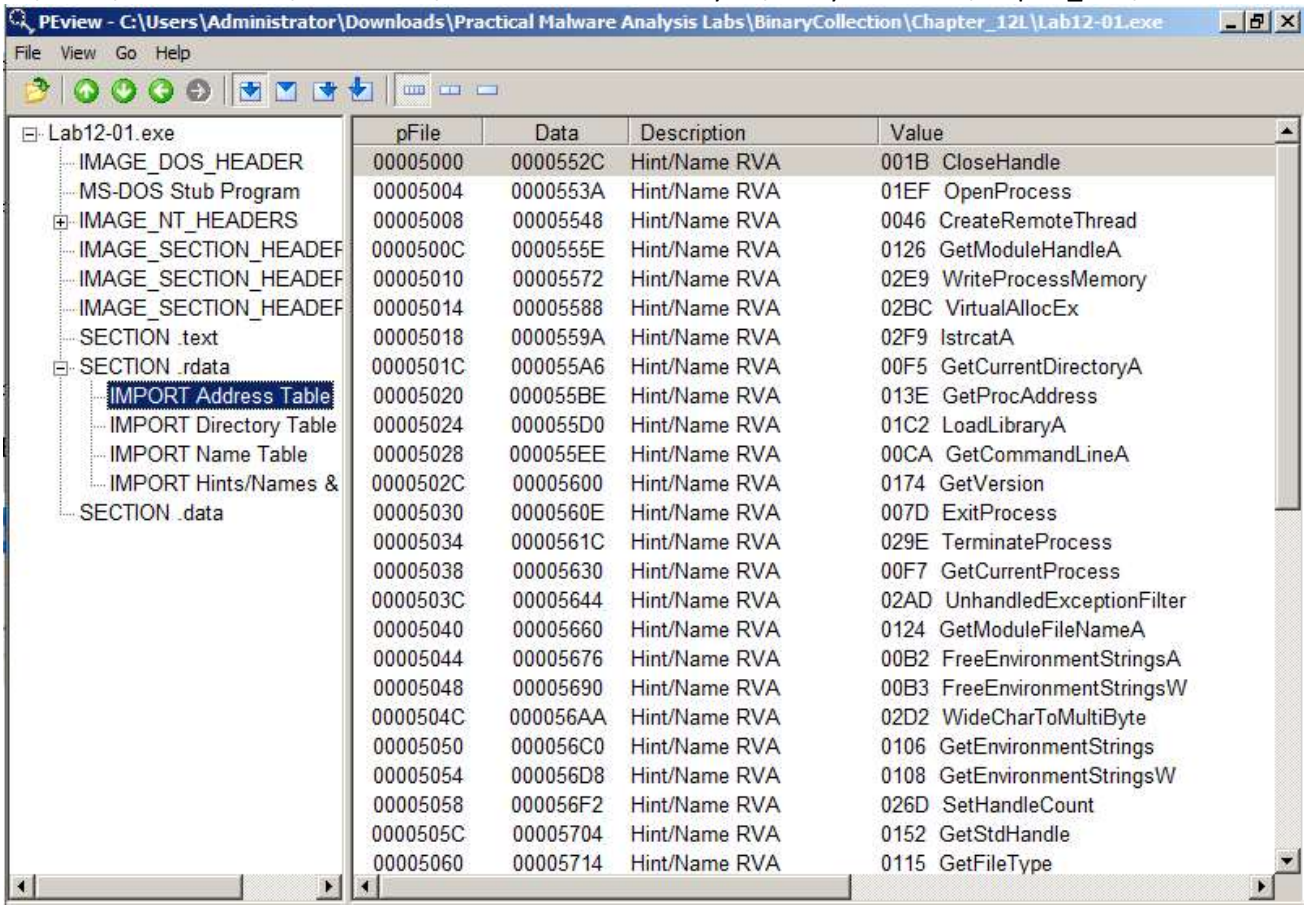
Chapter 12: Covert Malware Launching - Lab12-1

Source Files URL: https://github.com/mikesiko/PracticalMalwareAnalysis-Labs [82]

File: Lab12-01.exe

PEView[83] Analysis

C:\Users\Administrator\Downloads\Practical Malware Analysis\BinaryCollection\Chapter_11L\Lab12-01.exe

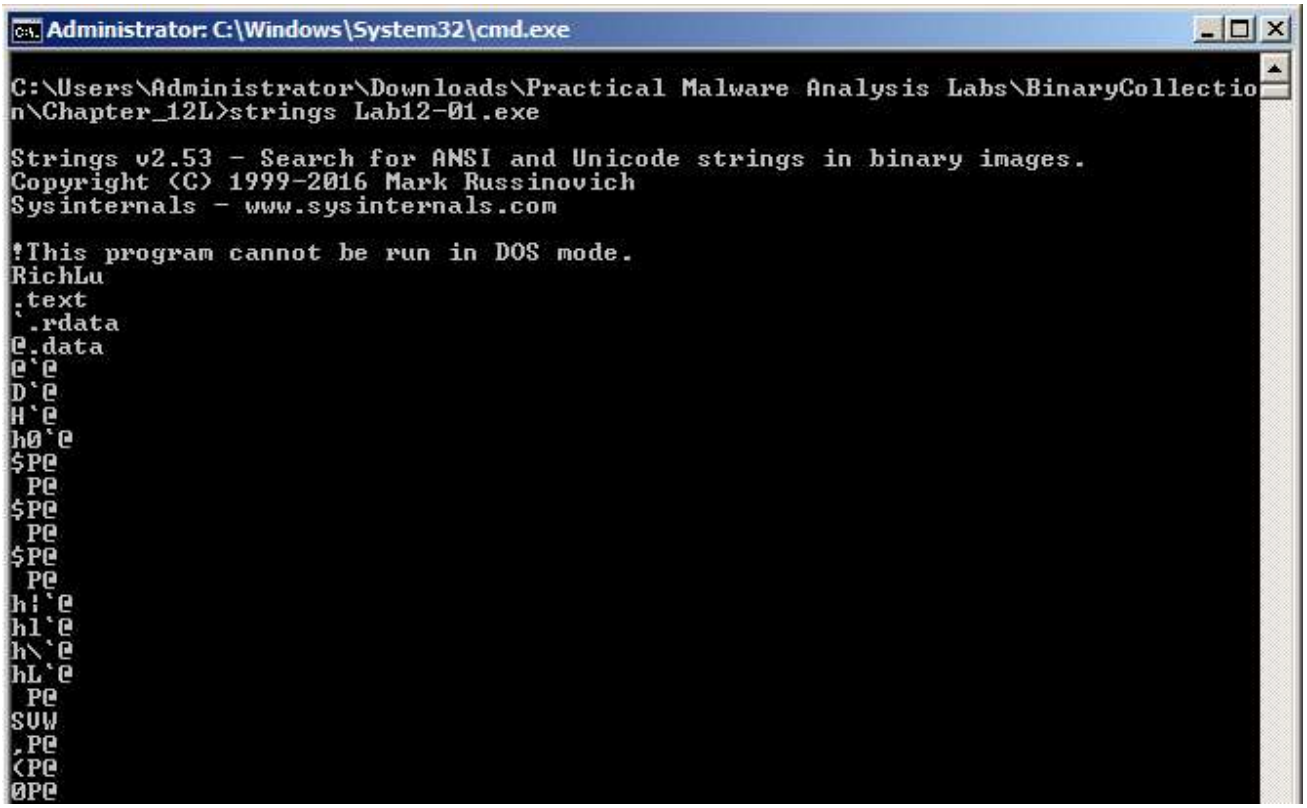


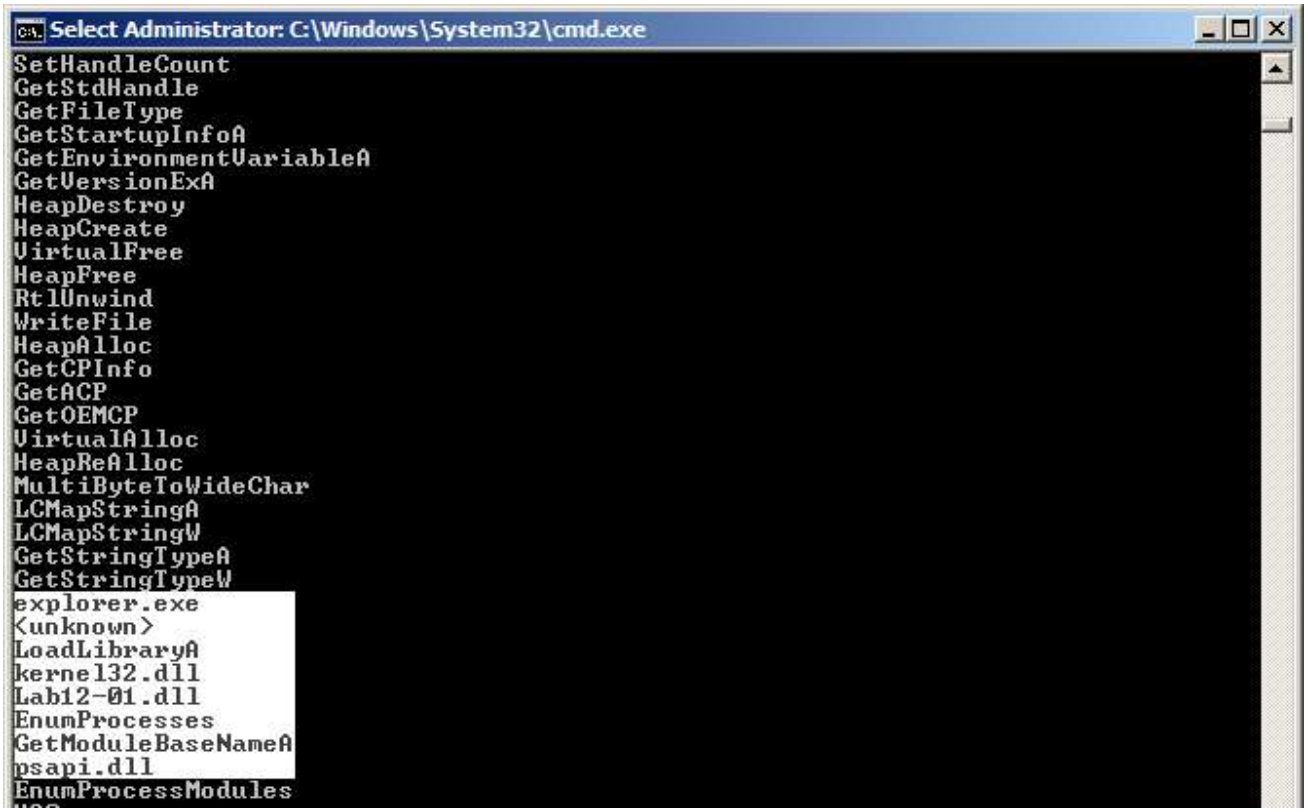
[82] PracticalMalwareAnalysis-Labs (2017) *Binaries for the book Practical Malware Analysis* https://github.com/mikesiko/PracticalMalwareAnalysis-Labs [Accessed 22nd May 2019].

[83] Radburn, Wayne J. (2018) *PEview version 0.9.9 (.zip 31KB)* http://wjradburn.com/software/ [Accessed 22nd May 2019].

Strings[84] Analysis

C:\Users\Administrator\Downloads\Practical Malware Analysis\BinaryCollection\Chapter_11L\Lab12-01.exe



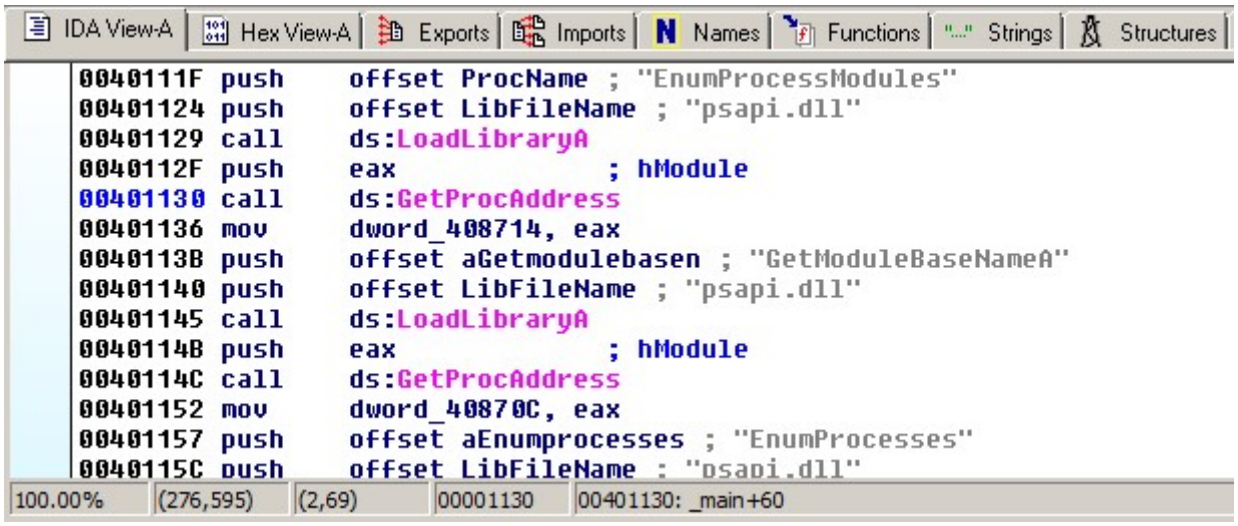


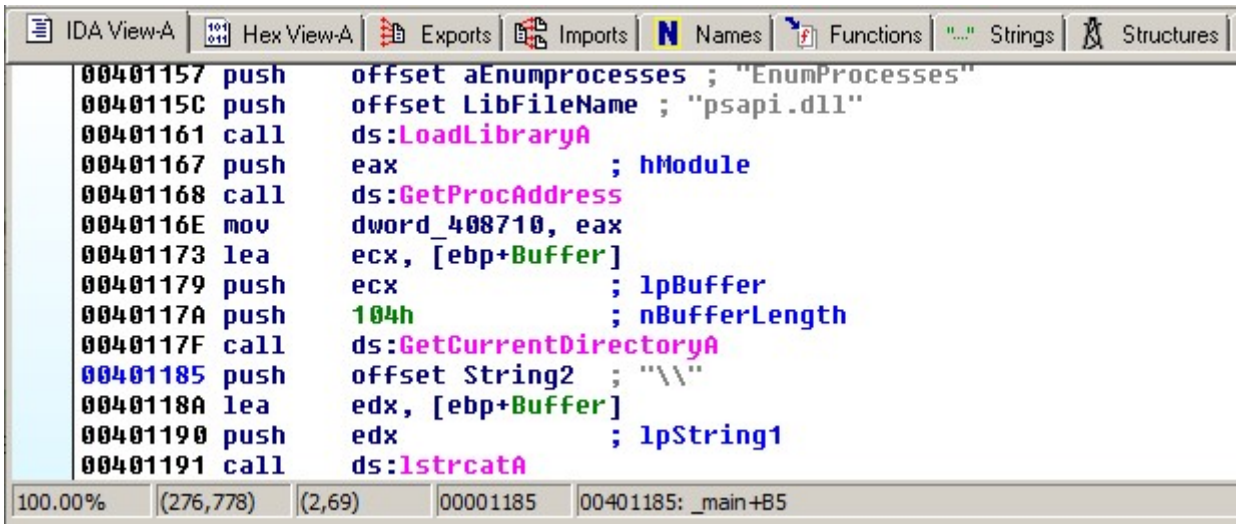
[84] Microsoft.com (2019) *Strings v2.53* https://docs.microsoft.com/en-gb/sysinternals/downloads/strings [Accessed 22nd May 2019].

IDA Pro[85] Analysis

C:\Users\Administrator\Downloads\Practical Malware Analysis\BinaryCollection\Chapter_11L\Lab12-01.exe

Options > General > Line Prefixes > Number of opcode bytes: 6





The code above references psapi three times

00401124 push offset LibFileName ; "psapi.dll"
00401140 push offset LibFileName ; "psapi.dll"
0040115C push offset LibFileName ; "psapi.dll"

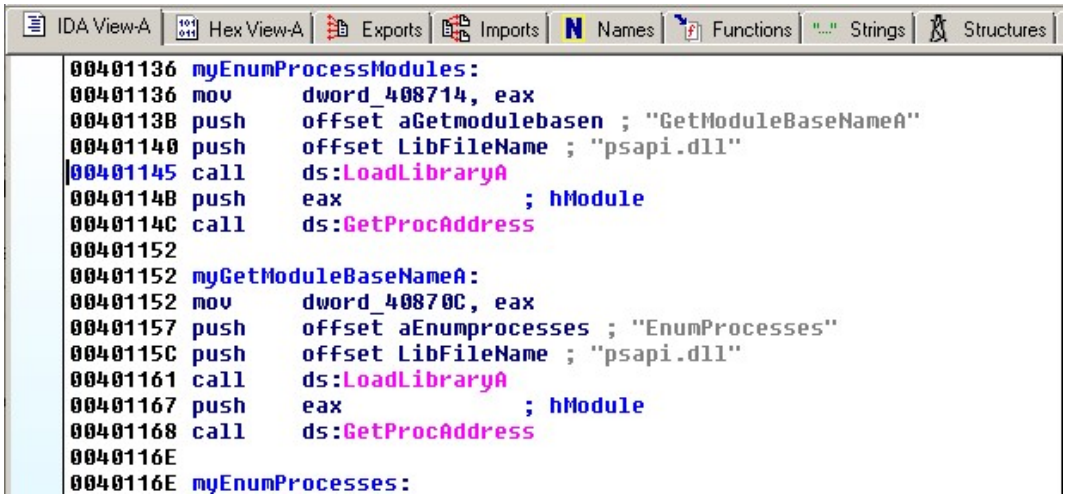
Psapi is attempting to locate a Windows API function and store its address in a numerical address
This obfuscates the code, so later calls to these functions will be difficult to recognize

[85] Hex-Rays (2019) *IDA Freeware for Windows (48 MB)* https://www.hex-rays.com/products/ida/support/download_freeware.shtml [Accessed 22nd May 2019].

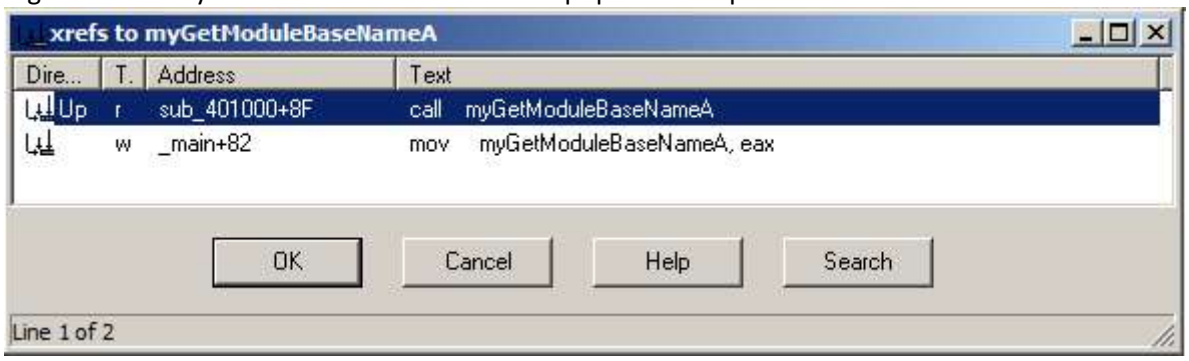
Assign Memory Addresses Labels
Address: 00401136
Data: dword_408714
Renamed to: myEnumProcessModules

Address: 00401152
Data: dword_40870C
Renamed to: myGetModuleBaseNameA

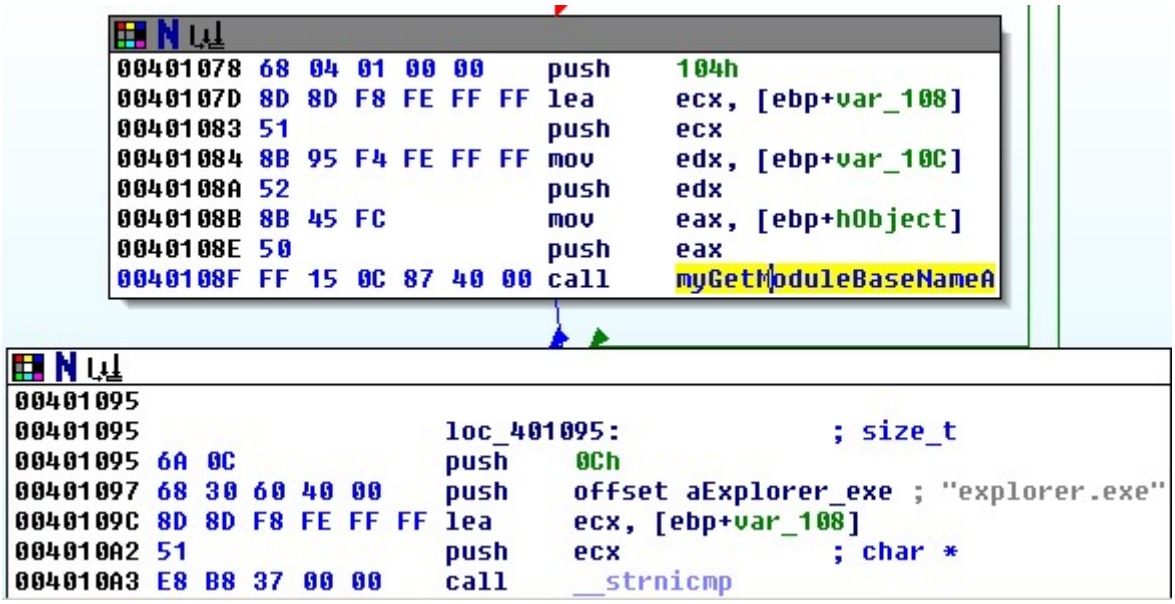
Address: 0040116E
Data: dword_408710
Renamed to: myEnumProcesses



Right-click on myGetModuleBaseNameA > Jump tp xrefs of operand

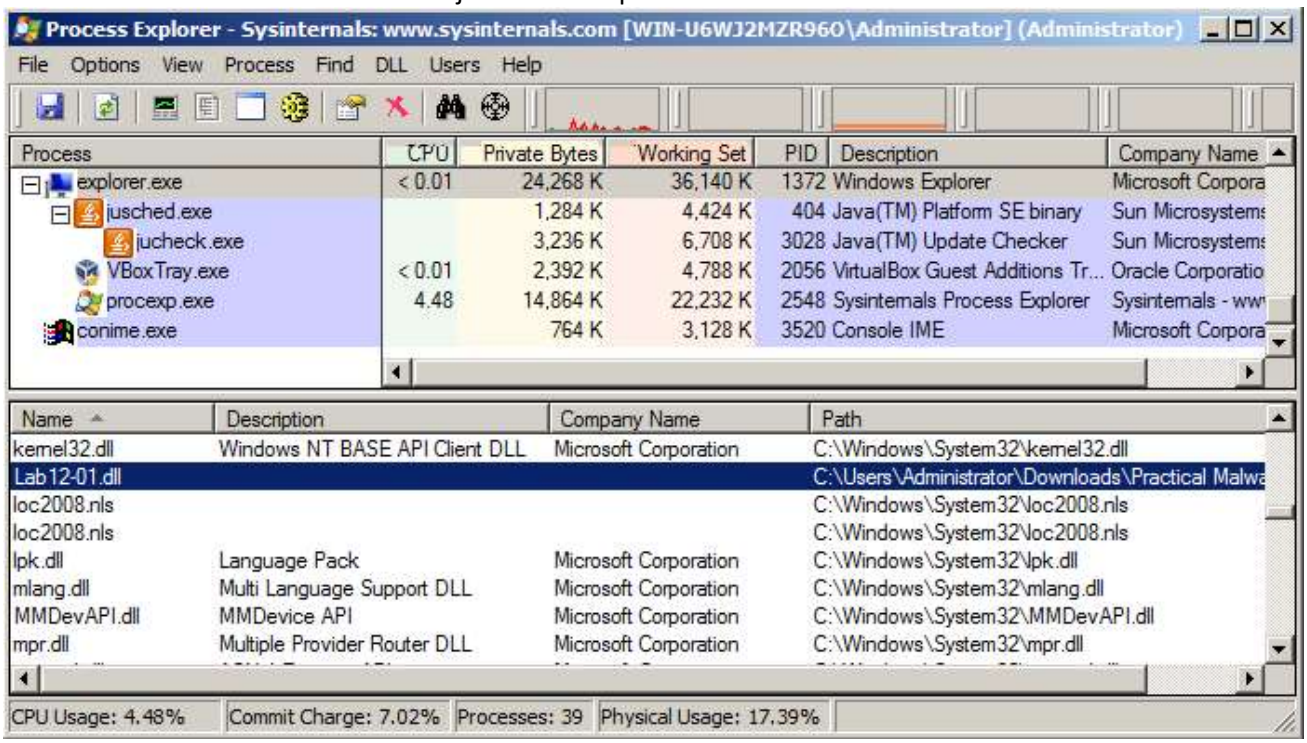


Routine enumerates modules and compares each module name to "explorer.exe", to find the module into which to inject code



Process Explorer[86] Analysis
Select explorer.exe
View > Show Lower Pane
View > Lower Pane View > DLLs

Locate Lab12-01.dll which has been injected into explorer.exe as follows

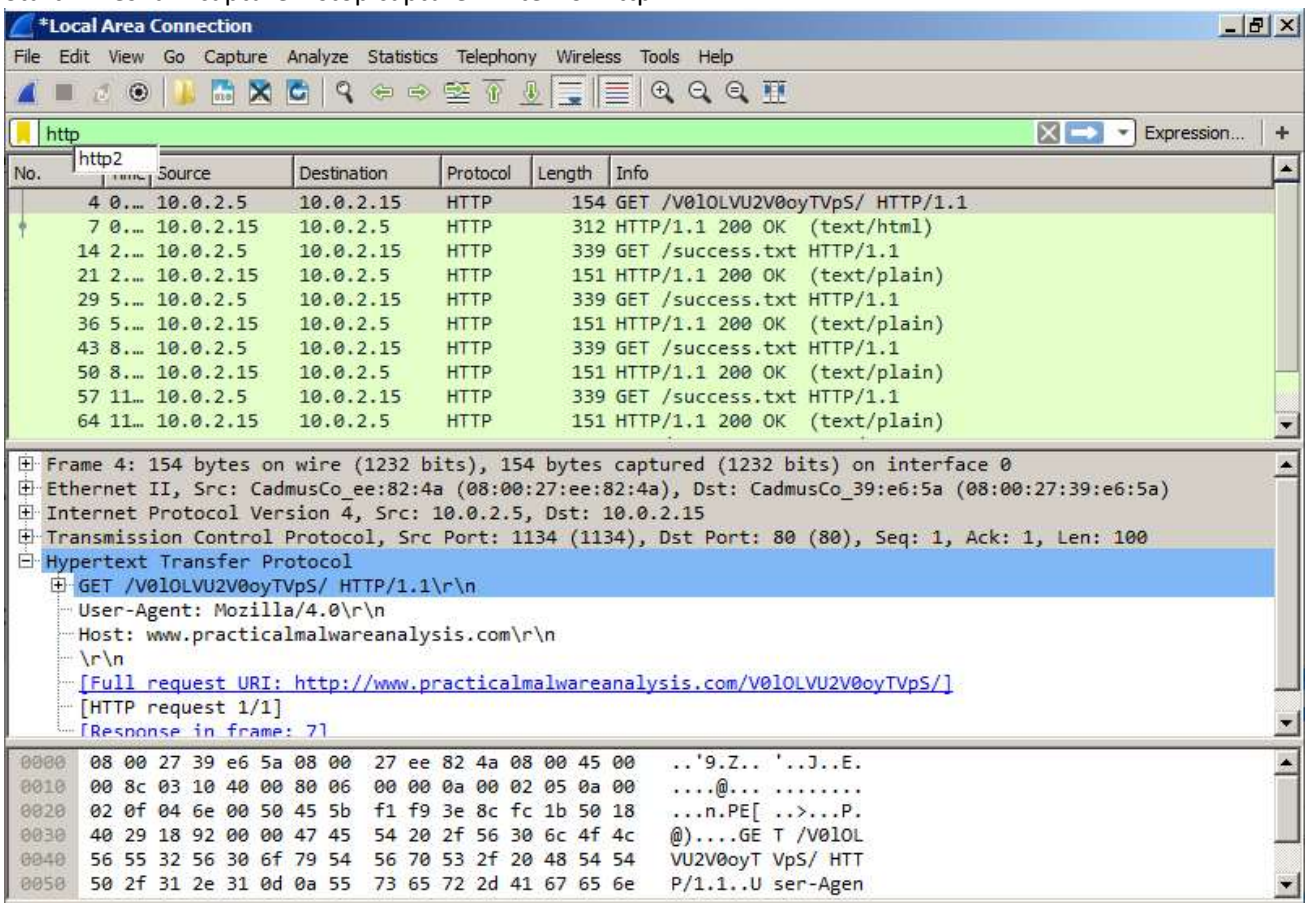


[86] Microsoft.com (2019) *Process Explorer v16.26* https://docs.microsoft.com/en-gb/sysinternals/downloads/process-explorer [Accessed 20th May 2019].

Chapter 13: Data Encoding - Lab13-1
Source Files URL: https://github.com/mikesiko/PracticalMalwareAnalysis-Labs [87]
File: Lab13-01.exe

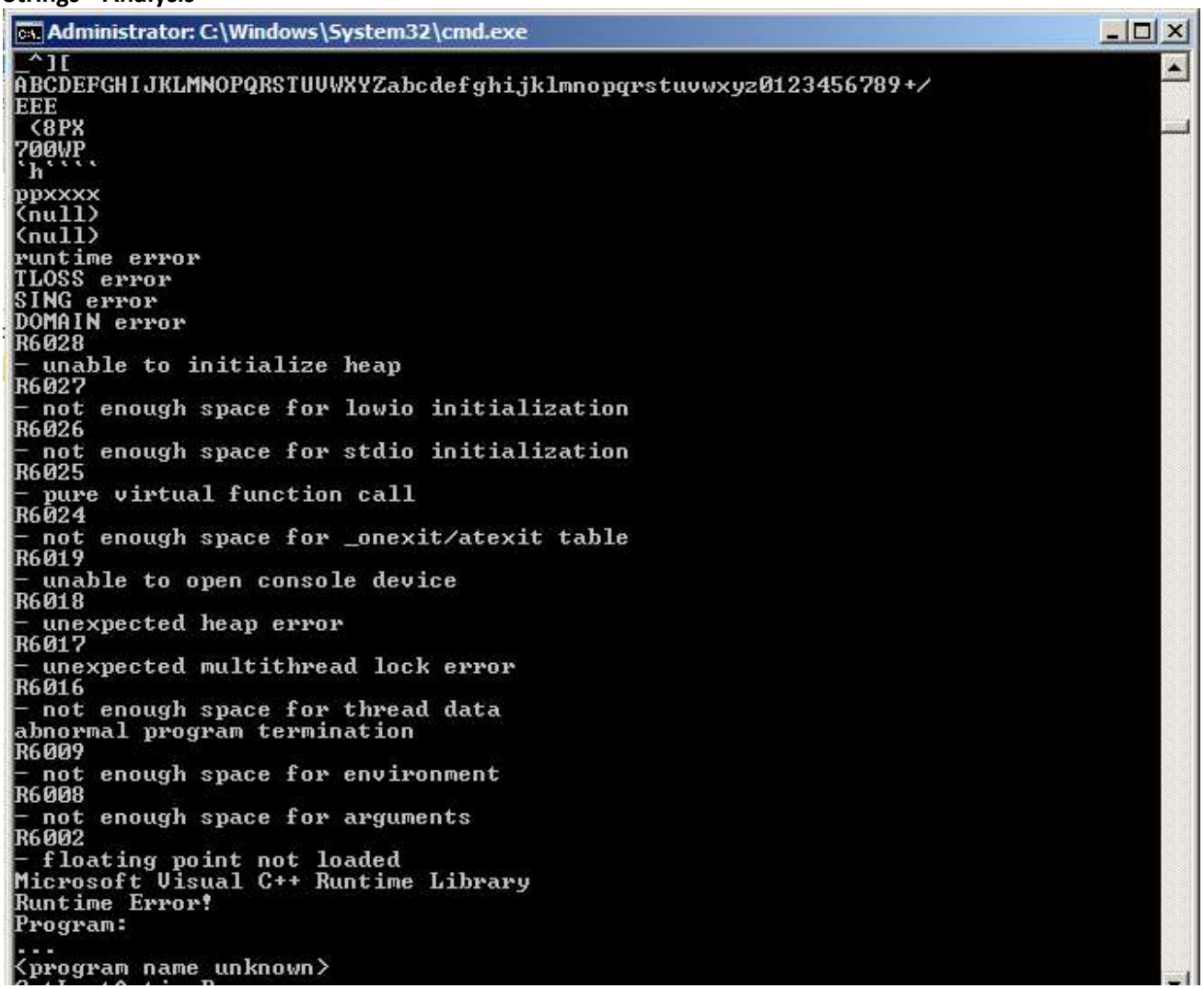
Kali KDE: start iNetSim
Windows Server 2008: set Primary DNS to Kali IP
Windows Server 2008: Firefox > http://mysite.com > INetSim default HTML page : OK

Wireshark[88] Capture
Start Wireshark capture > stop capture > filter for http



[87] PracticalMalwareAnalysis-Labs (2017) *Binaries for the book Practical Malware Analysis* https://github.com/mikesiko/PracticalMalwareAnalysis-Labs [Accessed 22nd May 2019].
[88] Wireshark.org (2019) *Wireshark-win32-2.0.0.exe* https://1.eu.dl.wireshark.org/win32/all-versions/ [Accessed 20th May 2019].

Strings[89] Analysis

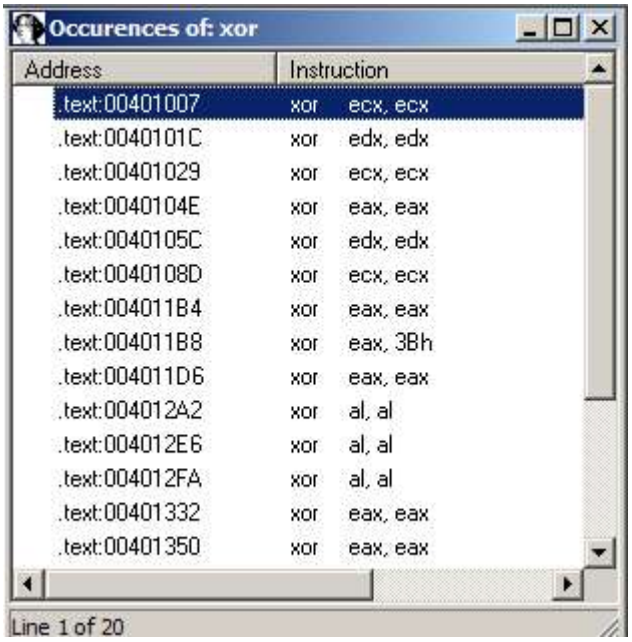


[89] Microsoft.com (2019) *Strings v2.53* https://docs.microsoft.com/en-gb/sysinternals/downloads/strings [Accessed 22nd May 2019].

IDA Pro[90] Analysis

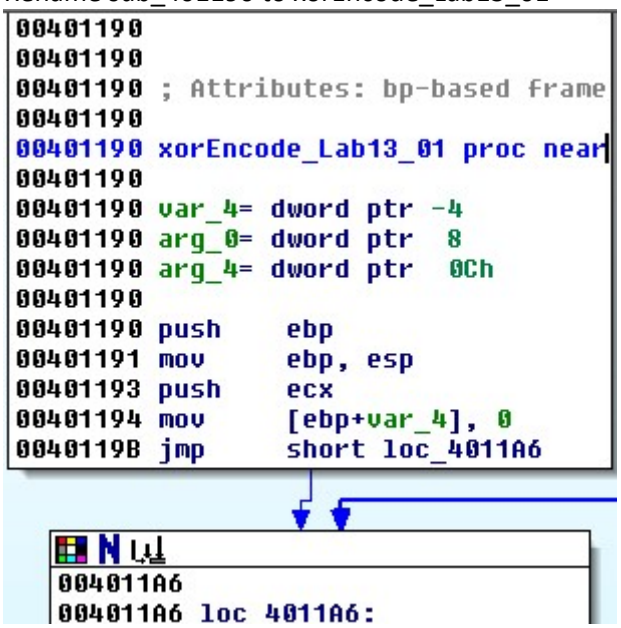
Options > General > Line Prefixes > OK

Click IDA View-A window > Search > Text > xor > Find all occurrences



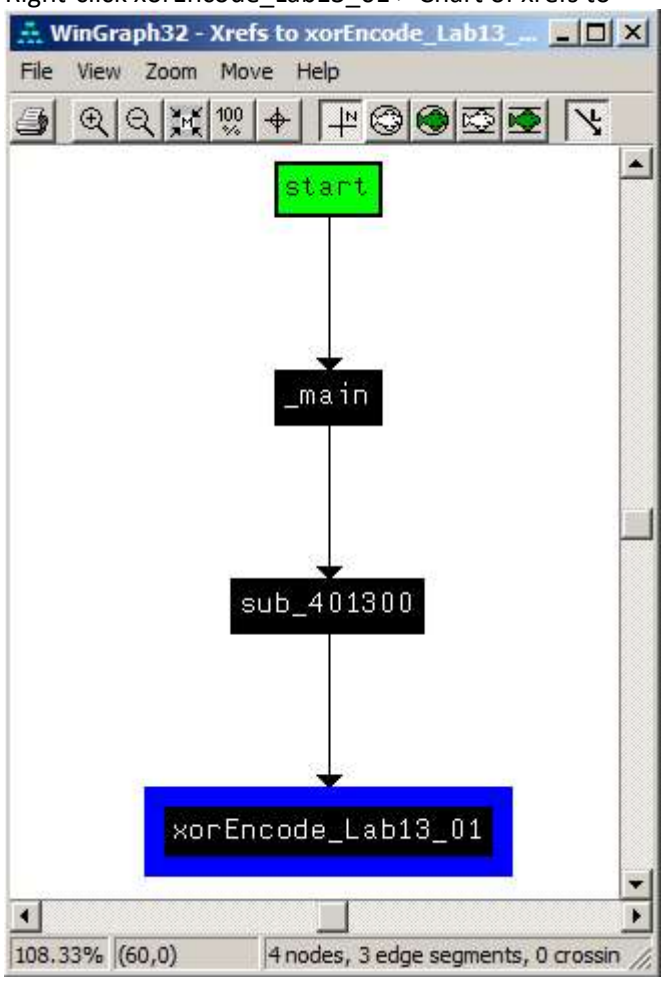
Double-click xor eax, 3Bh instruction. This function performs xor encoding

Rename sub_401190 to xorEncode_Lab13_01

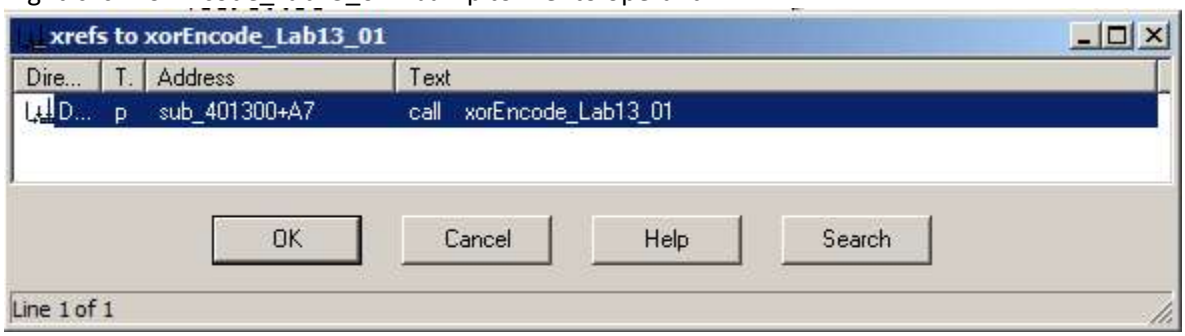


[90] Hex-Rays (2019) *IDA Freeware for Windows (48 MB)* https://www.hex-rays.com/products/ida/support/download_freeware.shtml [Accessed 22nd May 2019].

Right-click xorEncode_Lab13_01 > Chart of xrefs to



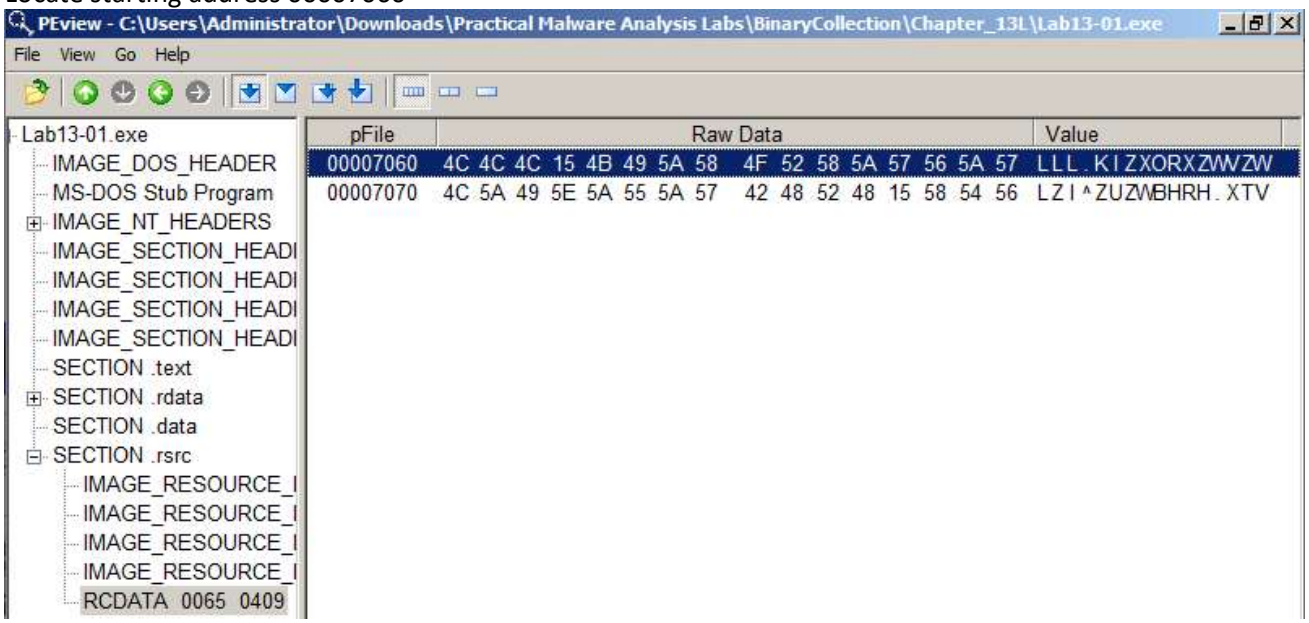
Right-click xorEncode_Lab13_01 > Jump to xref to operand



PEview[91] Analysis

PEView > SECTION .rsrc > RCDATA 0065 0409

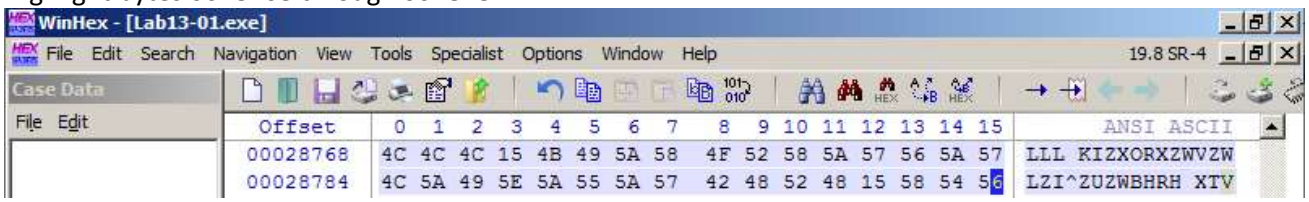
Locate starting address 00007060



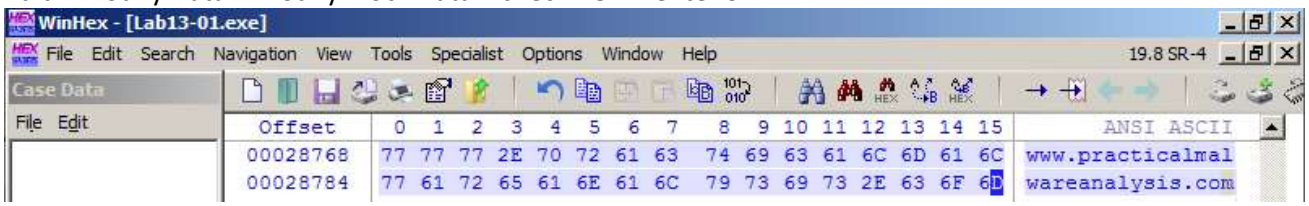
WinHex[92] Analysis

Setup.exe > File > Open > Lab13-01.exe

Highlight bytes 0028768 through 0028784



Edit > Modify Data > Modify Block Data > check XOR > enter 3B



[91] Radburn, Wayne J. (2018) *PEview version 0.9.9 (.zip 31KB)* http://wjradburn.com/software/ [Accessed 22nd May 2019].

[92] WinHex.com (2019) *WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor* http://winhex.com/winhex/ [Accessed 22nd May 2019].

References

1	Malware Types & Lab Setups File	(2019)	Gateway OS Slide 24	https://moodle.ncirl.ie/mod/resource/view.php?id=59717	[Accessed 1st July 2019].
2	REMnux.org	(2019)	REMnux: A Linux Toolkit for Reverse-Engineering and Analyzing Malware	https://remnux.org/	[Accessed 1st July 2019].
3	VirtualBox.org	(2019)	VirtualBox	https://www.virtualbox.org/	[Accessed 1st July 2019].
4	Jonathon Taaffe	(2019)	Table 1. malware-analysis-network01 Static Assignments		[Created 1st July 2019].
5	Portal.Azure.com	(2019)	Windows Server 2016 Standard	http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso	[Accessed 1st July 2019].
6	Malware Types & Lab Setups File	(2019)	Tools Slide 28	https://moodle.ncirl.ie/mod/resource/view.php?id=59717	[Accessed 1st July 2019].
7	Jonathon Taaffe	(2019)	Table 2. Windows Server 2016 File Server VM Configuration		[Created 1st July 2019].
8	Tecting	(2019)	How to Share Files and Folders in Windows Server 2016	https://www.tactig.com/share-files-folders-windows-server-2016/	[Accessed 1st July 2019].
9	Malware Types & Lab Setups File	(2019)	Gateway OS Slide 24	https://moodle.ncirl.ie/mod/resource/view.php?id=59717	[Accessed 1st July 2019].
10	Malware Types & Lab Setups File	(2019)	FakeNet-NG Slide 25	https://moodle.ncirl.ie/mod/resource/view.php?id=59717	[Accessed 1st July 2019].
11	Jonathon Taaffe	(2019)	Table 3. Malware Analysis Utilities Static IP Assignment		[Created 1st July 2019].
12	REMnux 6.0 OVA Public	(2019)	remnux-6.0-ova-public.ova (2.0G)	https://docs.google.com/uc?id=0B6fULLT_NpxMampUWlBCQXVJZzA&export=download	[Accessed 01/07/2019].
13	Jonathon Taaffe	(2019)	Table 4. Gateway OS – REMnux VM Configuration		[Created 1st July 2019].
14	FireEye/Flare-FakeNet-NG	(2019)	FakeNet-NG - Next Generation Dynamic Network Analysis Tool	https://github.com/fireeye/flare-fakenet-ng	[Accessed 1st July 2019].
15	Jonathon Taaffe	(2019)	Table 5. Gateway OS – REMnux VM Configuration		[Created 1st July 2019].
16	FireEye/Flare-FakeNet-NG	(2019)	FakeNet-NG - Next Generation Dynamic Network Analysis Tool	https://github.com/fireeye/flare-fakenet-ng	[Accessed 1st July 2019].
17	Jonathon Taaffe	(2019)	Table 6. FakeNet-NG Pre-Requisites		[Created 1st July 2019].
18	FireEye/Flare-FakeNet-NG	(2019)	FakeNet-NG - Next Generation Dynamic Network Analysis Tool	https://github.com/fireeye/flare-fakenet-ng	[Accessed 1st July 2019].
19	Microsoft.com	(2019)	Download Virtual Machines	https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/	[Accessed 2nd July 2019].
20	Jonathon Taaffe	(2019)	Table 7. Windows XP, 7, 8.1 and 10 VM Client Configuration		[Created 2nd July 2019].
21	Jonathon Taaffe	(2019)	Table 8. Windows XP, 7, 8.1 and 10 Network Configuration		[Created 2nd July 2019].
22	Malware Types & Lab Setups File	(2019)	FakeNet-NG Slide 25	https://moodle.ncirl.ie/mod/resource/view.php?id=59717	[Accessed 2nd July 2019].
23	Jonathon Taaffe	(2019)	Table 9. Windows XP, 7, 8.1 and 10 OS Configuration		[Created 2nd July 2019].
24	Microsoft.com	(2019)	Internet Explorer security zones registry entries for advanced users	https://support.microsoft.com/en-us/help/182569/internet-explorer-security-zones-registry-entries-for-advanced-users	[Accessed 2nd July 2019].
25	Portal.Azure.com	(2019)	Windows Server 2016 Standard	http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso	[Accessed 2nd July 2019].
26	REMnux 6.0 OVA Public	(2019)	remnux-6.0-ova-public.ova (2.0G)	https://docs.google.com/uc?id=0B6fULLT_NpxMampUWlBCQXVJZzA&export=download	[Accessed 2nd July 2019].
27	FireEye/Flare-FakeNet-NG	(2019)	FakeNet-NG - Next Generation Dynamic Network Analysis Tool	https://github.com/fireeye/flare-fakenet-ng	[Accessed 2nd July 2019].
28	Microsoft.com	(2019)	Download Virtual Machines	https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/	[Accessed 2nd July 2019].
29	Jonathon Taaffe	(2019)	Diagram 1. Lab Phase 1 Installation and Configuration		[Created 2nd July 2019].
30	Portal.Azure.com	(2019)	Windows Server 2016 Standard	http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso	[Accessed 2nd July 2019].
31	Microsoft.com	(2019)	Download Virtual Machines	https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/	[Accessed 2nd July 2019].
32	Jonathon Taaffe	(2019)	Diagram 2. Lab Phase 2 File Transfer		[Created 2nd July 2019].
33	Malware Types & Lab Setups File	(2019)	Tools Slide 28	https://moodle.ncirl.ie/mod/resource/view.php?id=59717	[Accessed 2nd July 2019].
34	Jonathon Taaffe	(2019)	Table 10. Client Application File Transfer		[Created 2nd July 2019].
35	Jonathon Taaffe	(2019)	Table 11. Client Application Installation		[Created 2nd July 2019].

36	Malware Types & Lab Setups File	(2019)	Tools Slides 28, 29, 30, 31, 32	https://moodle.ncirl.ie/mod/resource/view.php?id=59717	[Accessed 2nd July 2019].
37	Portal.Azure.com	(2019)	Windows Server 2016 Standard	http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso	[Accessed 2nd July 2019].
38	Jonathon Taaffe	(2019)	Diagram 3. Lab Phase 6 Dynamic Malware Analysis Configuration		[Created 2nd July 2019].
39	Sikorski, Michael; Honig, Andrew	(2012)	Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software	https://library.ncirl.ie/items/32216	[Accessed 20th May 2019].
40	Sam Bowne	(2016)	CNIT 126: Practical Malware Analysis	https://samsclass.info/126/126_S16.shtml#lecture	[Accessed 20th May 2019].
41	iNetSim.org	(2018)	INetSim: Internet Services Simulation Suite	https://www.inetsim.org/	[Accessed 20th May 2019].
42	Jonathon Taaffe	(2019)	Table 12. Kali KDE 2019.1 VM Configuration		[Created 20th May 2019].
43	Jonathon Taaffe	(2019)	Table 13.Windows XP and Windows Server 2008 VM Configuration		[Created 20th May 2019].
44	Jonathon Taaffe	(2019)	Table 14. Labs, Applications and Analysis Tools Installation		[Created 20th May 2019].
45	Jonathon Taaffe	(2019)	Diagram 4. Practical Malware Analysis Lab Configuration		[Created 20th May 2019].
46	Jonathon Taaffe	(2019)	Table 15. Practical Malware Analysis Exercises		[Created 20th May 2019].
47	PracticalMalware Analysis-Labs	(2017)	Binaries for the book Practical Malware Analysis	https://github.com/mikesiko/PracticalMalwareAnalysis-Labs	[Accessed 22nd May 2019].
48	Virus Total	(2019)	Virus Total	https://www.virustotal.com	[Accessed 22nd May 2019].
49	Radburn, Wayne J.	(2018)	PEview version 0.9.9 (.zip 31KB)	http://wjradburn.com/software/	[Accessed 22nd May 2019].
50	Softpedia.com	(2019)	PEiD 0.95	https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml	[Accessed 22nd May 2019].
51	Softpedia.com	(2019)	BinText 3.03	https://www.softpedia.com/get/System/File-Management/BinText.shtml	[Accessed 22nd May 2019].
52	Dependency Walker 2.2	(2019)	Dependency Walker 2.2	http://www.dependencywalker.com/	[Accessed 22nd May 2019].
53	Radburn, Wayne J.	(2018)	PEview version 0.9.9 (.zip 31KB)	http://wjradburn.com/software/	[Accessed 22nd May 2019].
54	Softpedia.com	(2019)	PEiD 0.95	https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml	[Accessed 22nd May 2019].
55	Softpedia.com	(2019)	BinText 3.03	https://www.softpedia.com/get/System/File-Management/BinText.shtml	[Accessed 22nd May 2019].
56	Dependency Walker 2.2	(2019)	Dependency Walker 2.2	http://www.dependencywalker.com/	[Accessed 22nd May 2019].
57	PracticalMalware Analysis-Labs	(2017)	Binaries for the book Practical Malware Analysis	https://github.com/mikesiko/PracticalMalwareAnalysis-Labs	[Accessed 22nd May 2019].
58	Virus Total	(2019)	Virus Total	https://www.virustotal.com	[Accessed 22nd May 2019].
59	Softpedia.com	(2019)	PEiD 0.95	https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml	[Accessed 22nd May 2019].
60	UPX Ultimate Packer for eXecutables	(2019)	UPX 3.95	https://github.com/upx/upx/releases/tag/v3.95	[Accessed 22nd May 2019].
61	Softpedia.com	(2019)	PEiD 0.95	https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml	[Accessed 22nd May 2019].
62	Dependency Walker 2.2	(2019)	Dependency Walker 2.2	http://www.dependencywalker.com/	[Accessed 22nd May 2019].
63	Microsoft.com	(2019)	Strings v2.53	https://docs.microsoft.com/en-gb/sysinternals/downloads/strings	[Accessed 22nd May 2019].
64	Radburn, Wayne J.	(2018)	PEview version 0.9.9 (.zip 31KB)	http://wjradburn.com/software/	[Accessed 22nd May 2019].
65	Microsoft.com	(2019)	Strings v2.53	https://docs.microsoft.com/en-gb/sysinternals/downloads/strings	[Accessed 22nd May 2019].
66	iNetSim.org	(2018)	INetSim: Internet Services Simulation Suite	https://www.inetsim.org/	[Accessed 20th May 2019].
67	Microsoft.com	(2019)	Process Explorer v16.26	https://docs.microsoft.com/en-gb/sysinternals/downloads/process-explorer	[Accessed 20th May 2019].
68	Microsoft.com	(2019)	Process Monitor v3.52	https://docs.microsoft.com/en-gb/sysinternals/downloads/procmon	[Accessed 20th May 2019].
69	Wireshark.org	(2019)	Wireshark-win32-2.0.0.exe	https://1.eu.dl.wireshark.org/win32/all-versions/	[Accessed 20th May 2019].
70	PracticalMalware Analysis-Labs	(2017)	Binaries for the book Practical Malware Analysis	https://github.com/mikesiko/PracticalMalwareAnalysis-Labs	[Accessed 22nd May 2019].
71	Hex-Rays	(2019)	IDA Freeware for Windows (48 MB)	https://www.hex-rays.com/products/ida/support/download_freeware.shtml	[Accessed 22nd May 2019].

72	OllyDBG	(2019)	Download OllyDbg 1.10 (final version)	http://www.ollydbg.de/download.htm	[Accessed 22nd May 2019].
73	Microsoft.com	(2019)	RegOpenKeyExA function	http://msdn.microsoft.com/en-us/library/windows/desktop/ms724897(v=vs.85).aspx	[Accessed 22nd May 2019].
74	PracticalMalware Analysis-Labs	(2017)	Binaries for the book Practical Malware Analysis	https://github.com/mikesiko/PracticalMalwareAnalysis-Labs	[Accessed 22nd May 2019].
75	Microsoft.com	(2019)	Strings v2.53	https://docs.microsoft.com/en-gb/sysinternals/downloads/strings	[Accessed 22nd May 2019].
76	Softpedia.com	(2019)	BinText 3.03	https://www.softpedia.com/get/System/File-Management/BinText.shtml	[Accessed 22nd May 2019].
77	Aldeid	(2019)	GINA-Graphical Identification and Authentication	https://www.aldeid.com/wiki/GINA-Graphical_Identification_and_Authentication	[Accessed 22nd May 2019].
78	Radburn, Wayne J.	(2018)	PEview version 0.9.9 (.zip 31KB)	http://wjradburn.com/software/	[Accessed 22nd May 2019].
79	Microsoft.com	(2019)	Process Monitor v3.52	https://docs.microsoft.com/en-gb/sysinternals/downloads/procmon	[Accessed 20th May 2019].
80	Resource Hacker	(2019)	Resource Hacker 5.1.7	http://www.angusj.com/resourcehacker/	[Accessed 20th May 2019].
81	SlavaSoft	(2019)	HashCalc 2.02	http://www.slavasoft.com/hashcalc/	[Accessed 20th May 2019].
82	PracticalMalware Analysis-Labs	(2017)	Binaries for the book Practical Malware Analysis	https://github.com/mikesiko/PracticalMalwareAnalysis-Labs	[Accessed 22nd May 2019].
83	Radburn, Wayne J.	(2018)	PEview version 0.9.9 (.zip 31KB)	http://wjradburn.com/software/	[Accessed 22nd May 2019].
84	Microsoft.com	(2019)	Strings v2.53	https://docs.microsoft.com/en-gb/sysinternals/downloads/strings	[Accessed 22nd May 2019].
85	Hex-Rays	(2019)	IDA Freeware for Windows (48 MB)	https://www.hex-rays.com/products/ida/support/download_freeware.shtml	[Accessed 22nd May 2019].
86	Microsoft.com	(2019)	Process Explorer v16.26	https://docs.microsoft.com/en-gb/sysinternals/downloads/process-explorer	[Accessed 20th May 2019].
87	PracticalMalware Analysis-Labs	(2017)	Binaries for the book Practical Malware Analysis	https://github.com/mikesiko/PracticalMalwareAnalysis-Labs	[Accessed 22nd May 2019].
88	Wireshark.org	(2019)	Wireshark-win32-2.0.0.exe	https://1.eu.dl.wireshark.org/win32/all-versions/	[Accessed 20th May 2019].
89	Microsoft.com	(2019)	Strings v2.53	https://docs.microsoft.com/en-gb/sysinternals/downloads/strings	[Accessed 22nd May 2019].
90	Hex-Rays	(2019)	IDA Freeware for Windows (48 MB)	https://www.hex-rays.com/products/ida/support/download_freeware.shtml	[Accessed 22nd May 2019].
91	Radburn, Wayne J.	(2018)	PEview version 0.9.9 (.zip 31KB)	http://wjradburn.com/software/	[Accessed 22nd May 2019].
92	WinHex.com	(2019)	WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor	http://winhex.com/winhex/	[Accessed 22nd May 2019].