

PROJ 2 : BASIC STATIC TECHNIQUES 2

Prof. Alberto LaCava

CY -640

MALWARE ANALYSIS & DEFENSE

Nikhil Patel

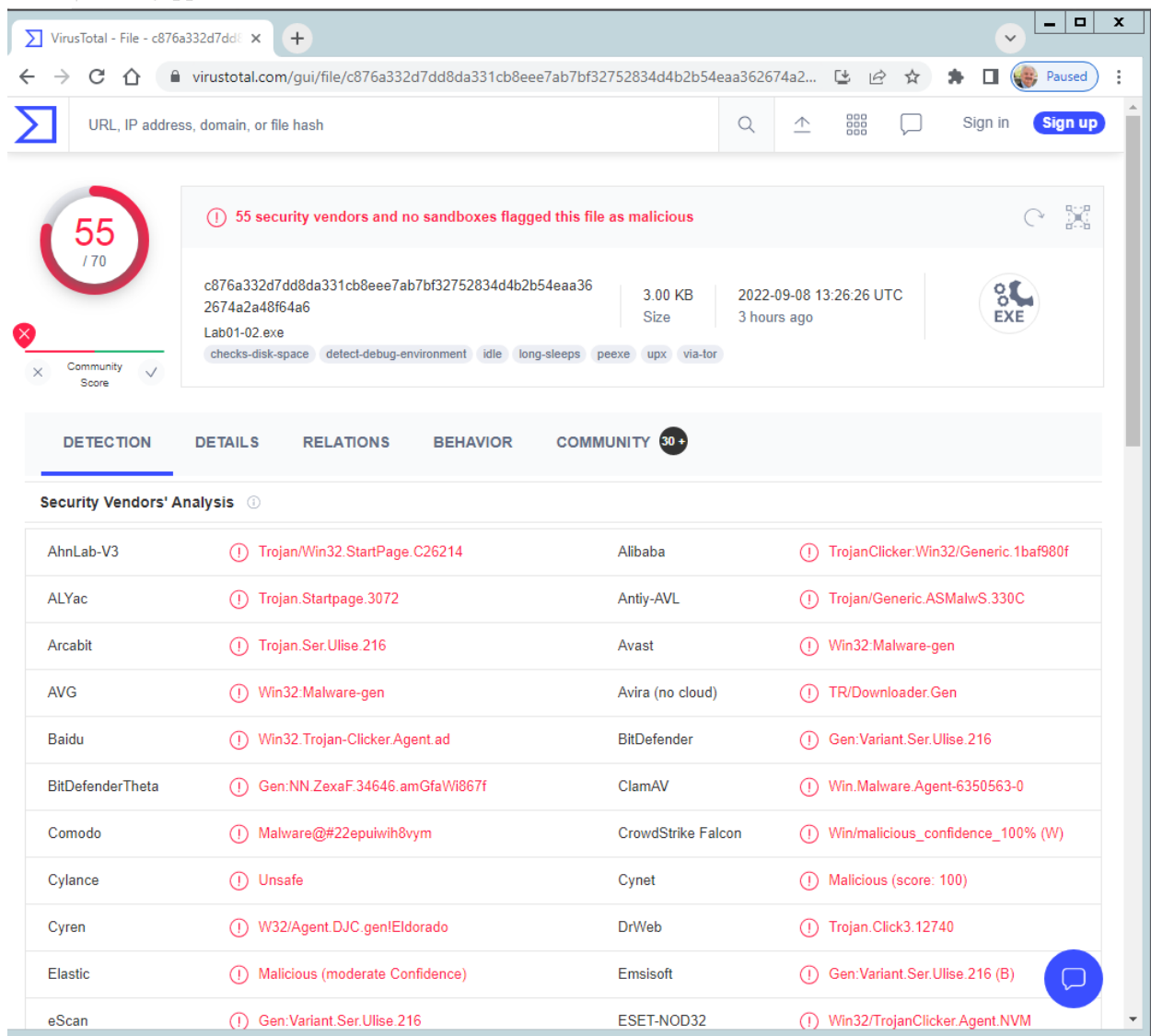
09/13/2022

Overview : In this lab we will learn how to use static methods for malware examination and we also utilized the UPX apparatus in windows.

Procedure :

Step 1: Virus Total

- Go to Browser type virustotal.com
- Click on Upload a file
- Add the file given in the folder of week 1 (Lab01-02.exe)
- You see the summary of those files you uploaded to virus total.



The screenshot shows the VirusTotal web interface for a file named 'Lab01-02.exe'. The file's SHA-256 hash is c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2... and it is 3.00 KB in size. It was uploaded on 2022-09-08 at 13:26:26 UTC. The file has a community score of 55/70, indicated by a red circle. A message states: '55 security vendors and no sandboxes flagged this file as malicious'. The file is categorized as 'EXE'. Below the file information, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (30+). The DETECTION tab is active, showing a table of security vendors and their analysis results.

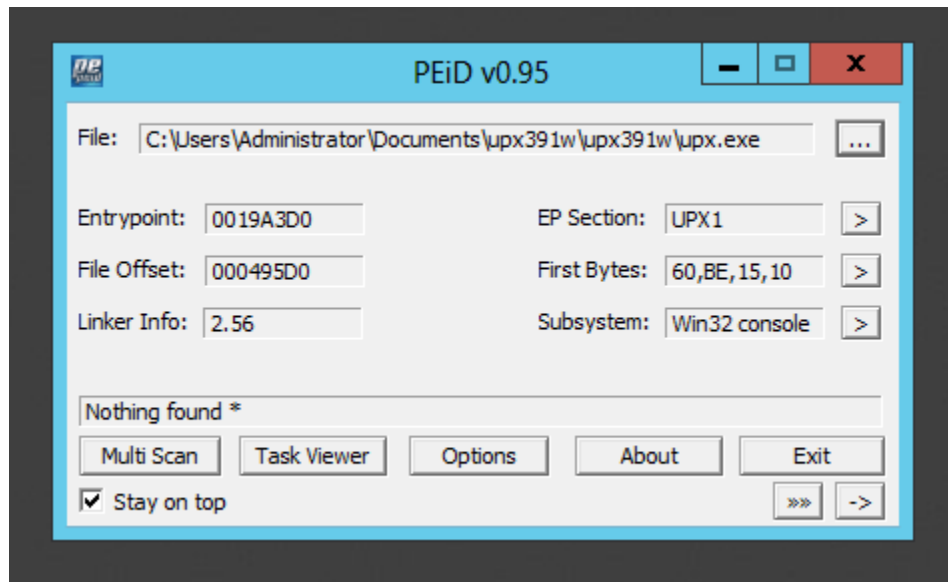
Security Vendors' Analysis			
AhnLab-V3	ⓘ Trojan.Win32.StartPage.C26214	Alibaba	ⓘ TrojanClicker.Win32/Generic.1baf980f
ALYac	ⓘ Trojan.Startpage.3072	Antiy-AVL	ⓘ Trojan/Generic.ASMalwS.330C
Arcabit	ⓘ Trojan.Ser.Ulise.216	Avast	ⓘ Win32:Malware-gen
AVG	ⓘ Win32:Malware-gen	Avira (no cloud)	ⓘ TR/Downloader.Gen
Baidu	ⓘ Win32.Trojan-Clicker.Agent.ad	BitDefender	ⓘ Gen:Variant.Ser.Ulise.216
BitDefenderTheta	ⓘ Gen:NN.ZexaF.34646.amGfaWi867f	ClamAV	ⓘ Win.Malware.Agent-6350563-0
Comodo	ⓘ Malware@#22epuiwih8vym	CrowdStrike Falcon	ⓘ Win/malicious_confidence_100% (W)
Cylance	ⓘ Unsafe	Cynet	ⓘ Malicious (score: 100)
Cyren	ⓘ W32/Agent.DJC.genIEldorado	DrWeb	ⓘ Trojan.Click3.12740
Elastic	ⓘ Malicious (moderate Confidence)	Emsisoft	ⓘ Gen:Variant.Ser.Ulise.216 (B)
eScan	ⓘ Gen:Variant.Ser.Ulise.216	ESET-NOD32	ⓘ Win32/TrojanClicker.Agent.NVM

Above Image shows the Summary of Lab01-02.exe

Step 2 : PEiD

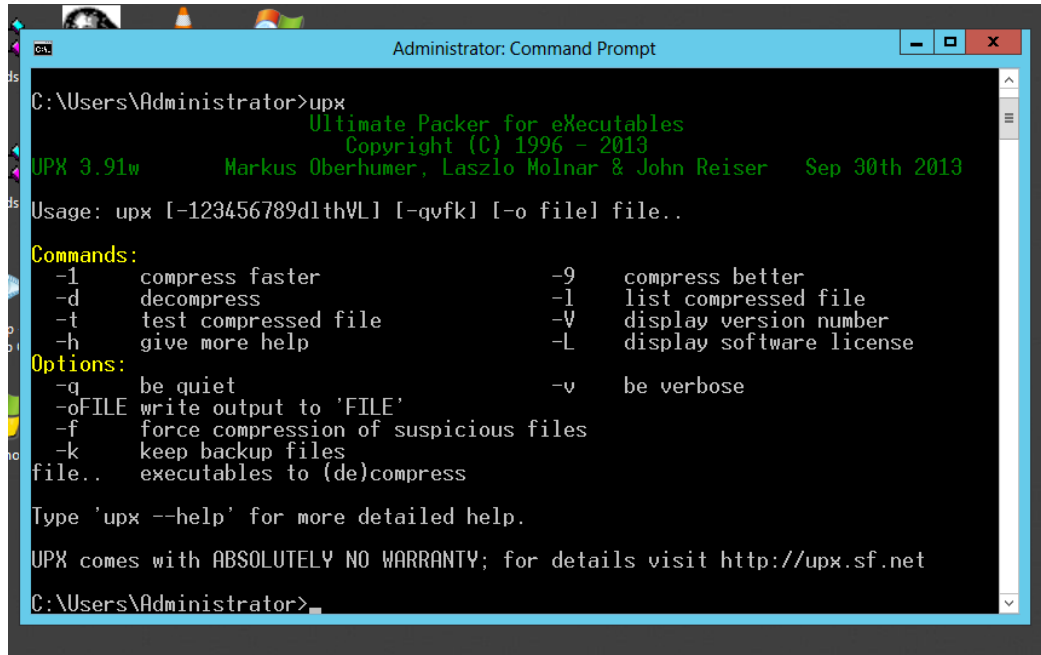
Cybercriminals generally pack their malware so deciding it is extremely challenging. This is a device that can distinguish 470 distinct structure marks in the PE document.

- Go to the Start menu and type PEiD or download it from the browser.
- Open upx.exe and it shows you the EP Section.



Step 3 : UPX

It is an executable record blower with authentic purposes to lessen the document size of convenient executable by half 70%. Upx likewise frequently uses dangerous entertainers to add a layer of confusion to their malware.



```
Administrator: Command Prompt
C:\Users\Administrator>upx
      Ultimate Packer for eXecutables
      Copyright (C) 1996 - 2013
UPX 3.91w      Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 30th 2013

Usage: upx [-123456789dlthVL] [-qvfk] [-o file] file..

Commands:
  -1      compress faster              -9      compress better
  -d      decompress                  -l      list compressed file
  -t      test compressed file        -V      display version number
  -h      give more help              -L      display software license

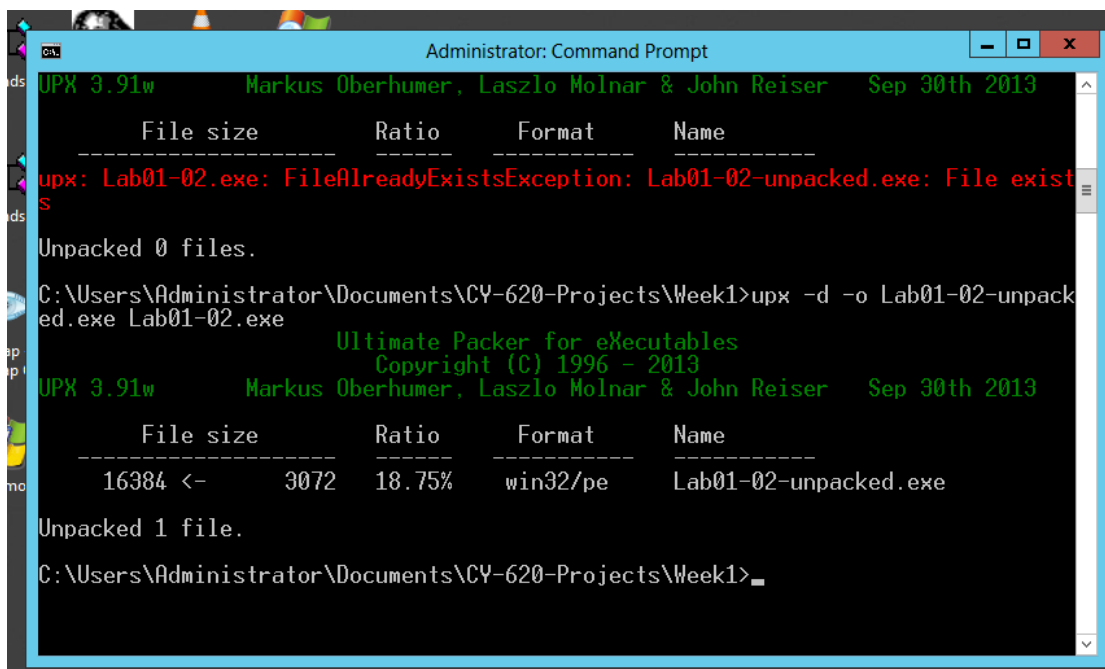
Options:
  -q      be quiet                    -v      be verbose
  -oFILE  write output to 'FILE'
  -f      force compression of suspicious files
  -k      keep backup files
file..   executables to (de)compress

Type 'upx --help' for more detailed help.

UPX comes with ABSOLUTELY NO WARRANTY; for details visit http://upx.sf.net

C:\Users\Administrator>
```

- Decompress the file using the UPX command shown below.



```
Administrator: Command Prompt
UPX 3.91w      Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 30th 2013

      File size      Ratio      Format      Name
      -----
upx: Lab01-02.exe: FileAlreadyExistsException: Lab01-02-unpacked.exe: File exists
Unpacked 0 files.

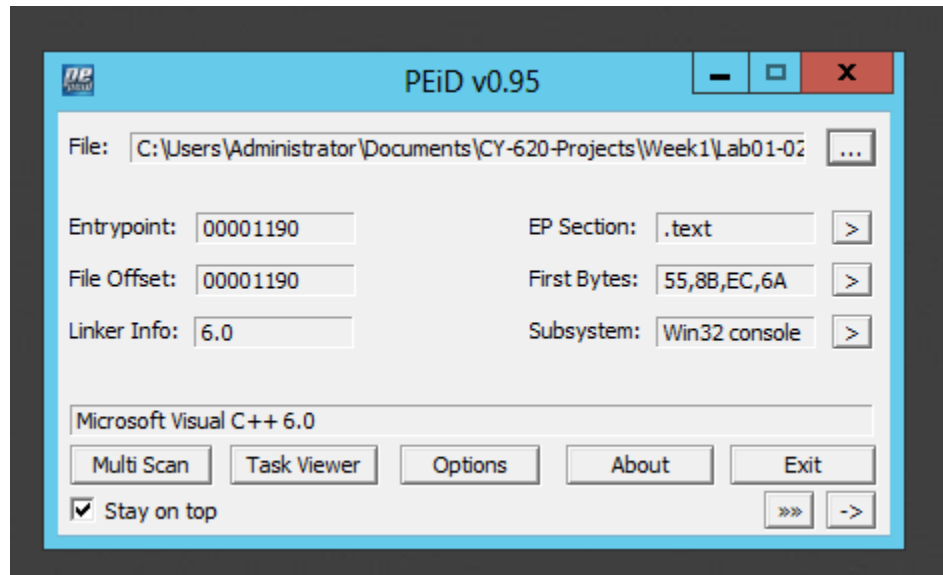
C:\Users\Administrator\Documents\CY-620-Projects\Week1>upx -d -o Lab01-02-unpacked.exe Lab01-02.exe
      Ultimate Packer for eXecutables
      Copyright (C) 1996 - 2013
UPX 3.91w      Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 30th 2013

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

Unpacked 1 file.

C:\Users\Administrator\Documents\CY-620-Projects\Week1>
```

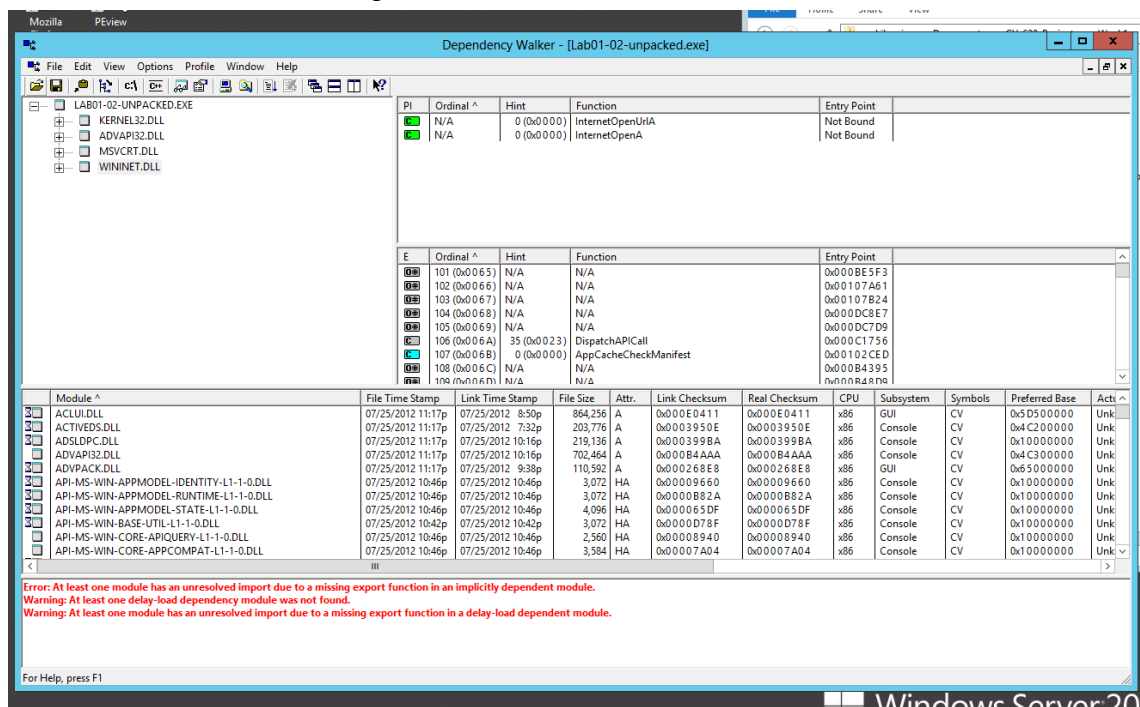
- Now unpacked the file in PEiD.



Step 4: Dependency Walker

It is utility outputs instrument which filters 32/64 pieces module(exe, dll, ocx, sys, and so on). It constructs a progressive tree chart of every single ward module. It is exceptionally valuable for investigating framework blunders related to stacking and run modules.

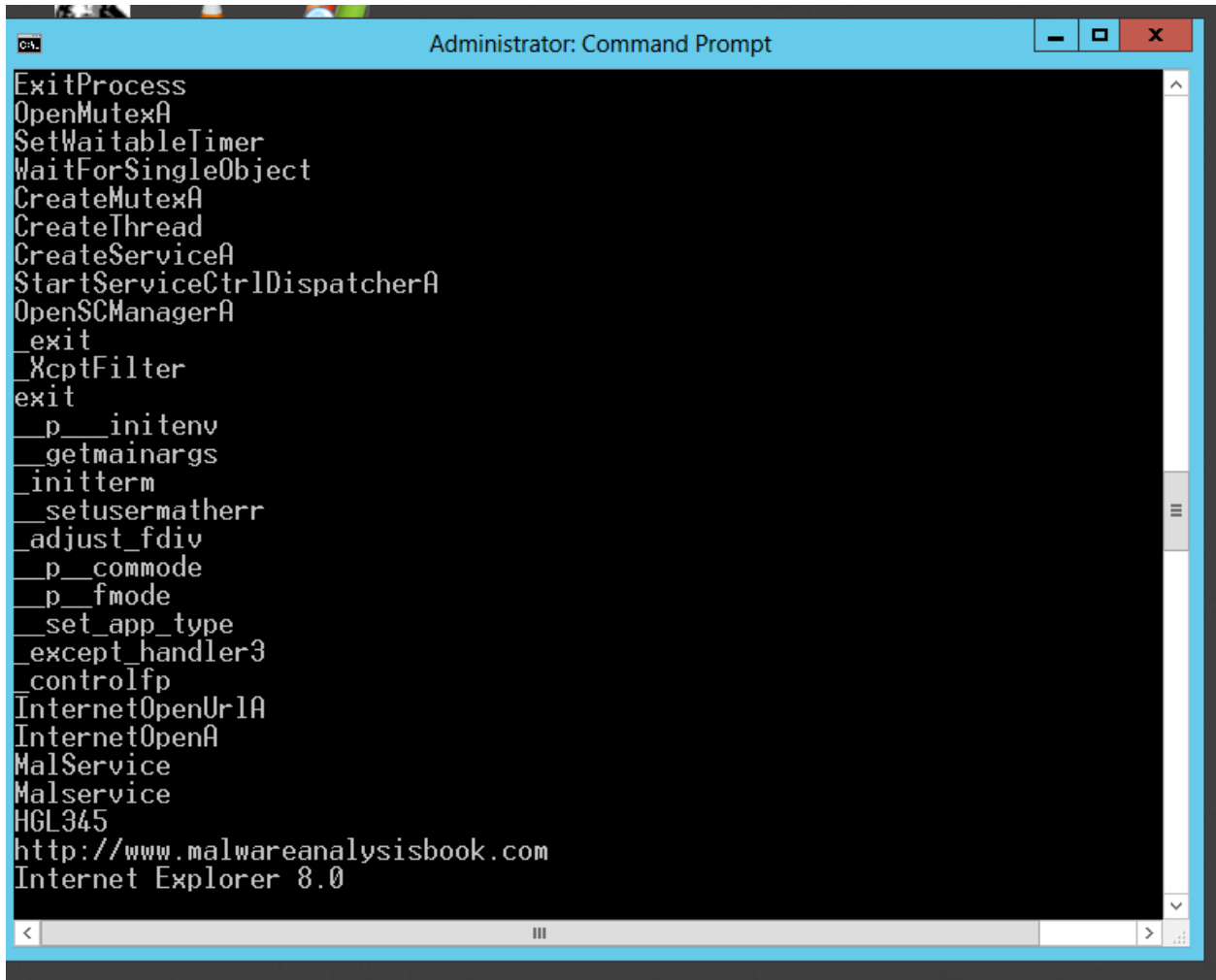
- Open Lab01-02-unpacked.exe in Dependency Walker.
- In the left panel, click WININET.DLL as shown below.



Step 5 : Strings

The strings order searches for printable strings in a document. A string is any grouping of at least 4 printable characters that end with a new-line or an invalid person. The string order is helpful for recognizing arbitrary article documents.

- Go to cmd Use strings cmd used in Proj 1. (Only difference is select other file).



```
ExitProcess
OpenMutexA
SetWaitableTimer
WaitForSingleObject
CreateMutexA
CreateThread
CreateServiceA
StartServiceCtrlDispatcherA
OpenSCManagerA
_exit
_XcptFilter
exit
_p__initenv
_getmainargs
_initterm
_setusermatherr
_adjust_fdiv
_p__commode
_p__fmode
_set_app_type
_except_handler3
_controlfp
InternetOpenUrlA
InternetOpenA
MalService
MalService
HGL345
http://www.malwareanalysisbook.com
Internet Explorer 8.0
```

Conclusion : To conclude with the lab, we have learned how to use Basic Static Techniques-2 using VirusTotal, PEiD, UPX, Dependency Walker and at the end by using Strings tools.