Proj 14: Malware Behavior (Lab 11-1) (35 pts.)

What you need:

- The Windows 2008 Server virtual machine we have been using.
- The textbook: "Practical Malware Analysis"

Purpose

You will practice the techniques in chapter 11.

Downloading the Lab Files

In a Web browser, go here:

http://practicalmalwareanalysis.com/labs/

Download and unzip the lab files.

Follow the instructions for **Lab 11-1** in the textbook. There are more detailed solutions in the back of the book. The only purpose of this document is to explain what images to turn in.

Static Analysis with Strings

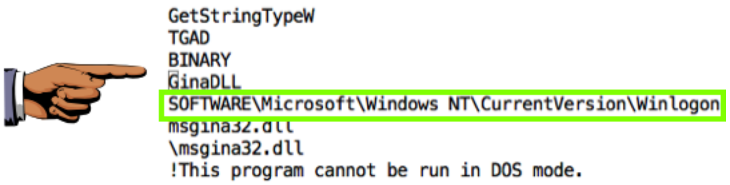
Examine the strings in Lab11-01.exe.

One handy tool to do that is **BinText**.

You should find the two items below.

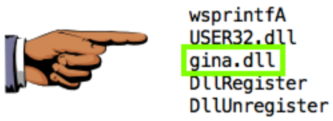
Save an image showing the string **SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon** as shown below, with the filename "**Proj 14a from YOUR NAME**".

YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT!



```
GetStringTypeW
TGAD
BINARY
GinaDLL
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
msgina32.dll
\msgina32.dll
!This program cannot be run in DOS mode.
```

Save an image showing the string **gina.DLL**, as shown below, with the filename "**Proj 14b from YOUR NAME**".



```
wsprintfA
USER32.dll
gina.dll
DllRegister
DllUnregister
```

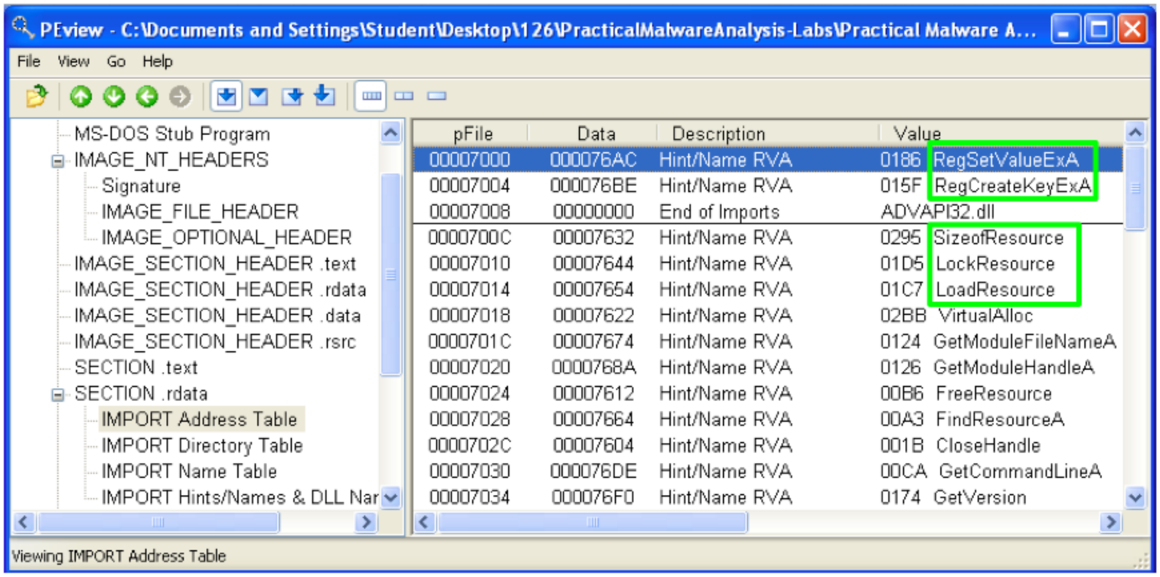
These strings suggest that this is GINA interception malware.

Static Analysis with PEview

Examine the Lab11-01.exe file in PEview. Find the items below.

Save an image showing these imports, as highlighted below:, with the filename "**Proj 14c from YOUR NAME**".

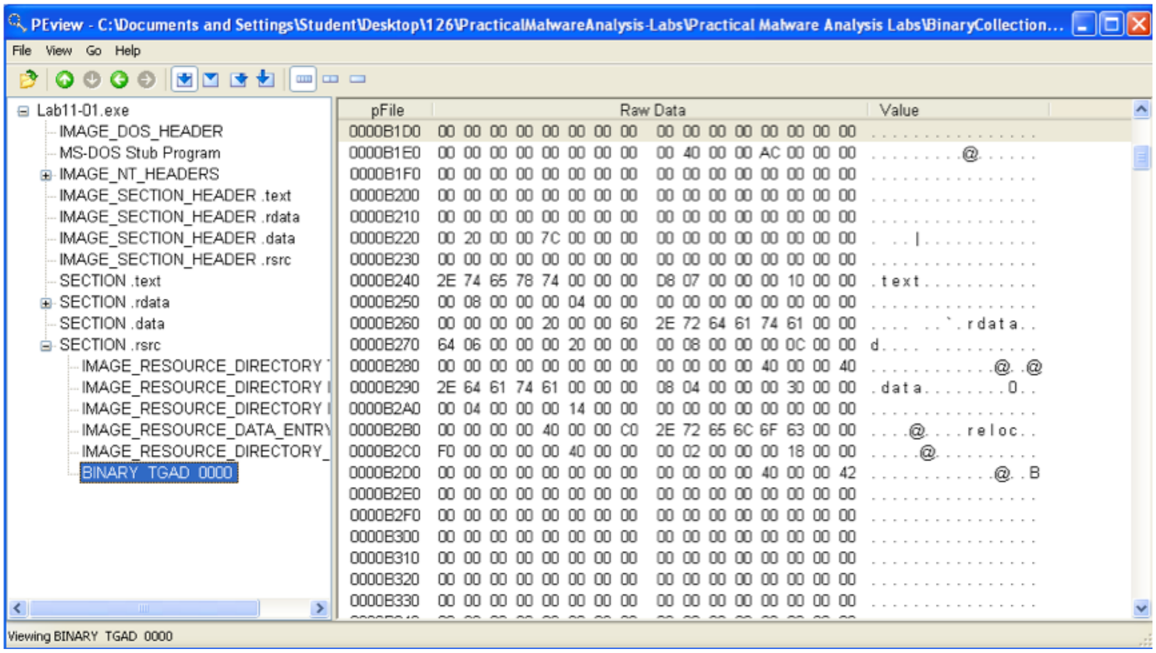
- **RegSetValueExA**
- **RegCreateKeyExA**
- **SizeofResource**
- **LockResource**
- **LoadResource**


PEview - C:\Documents and Settings\Student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware A...
File View Go Help
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .rsrc
SECTION .text
SECTION .rdata
IMPORT Address Table
IMPORT Directory Table
IMPORT Name Table
IMPORT Hints/Names & DLL Nar
Viewing IMPORT Address Table

pFile	Data	Description	Value
00007000	000076AC	Hint/Name RVA	0186 RegSetValueExA
00007004	000076BE	Hint/Name RVA	015F RegCreateKeyExA
00007008	00000000	End of Imports	ADVAPI32.dll
0000700C	00007632	Hint/Name RVA	0295 SizeofResource
00007010	00007644	Hint/Name RVA	01D5 LockResource
00007014	00007654	Hint/Name RVA	01C7 LoadResource
00007018	00007622	Hint/Name RVA	02BB VirtualAlloc
0000701C	00007674	Hint/Name RVA	0124 GetModuleFileNameA
00007020	0000768A	Hint/Name RVA	0126 GetModuleHandleA
00007024	00007612	Hint/Name RVA	00B6 FreeResource
00007028	00007664	Hint/Name RVA	00A3 FindResourceA
0000702C	00007604	Hint/Name RVA	001B CloseHandle
00007030	000076DE	Hint/Name RVA	00CA GetCommandLineA
00007034	000076F0	Hint/Name RVA	0174 GetVersion

These API calls suggest that the malware is manipulating the registry and extracting a resource section.

Save an image showing the **BINARY TGAD 0000** section, as shown below, with the filename "**Proj 14d from YOUR NAME**".


PEview - C:\Documents and Settings\Student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection...
File View Go Help
Lab11-01.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .rsrc
SECTION .text
SECTION .rdata
SECTION .data
SECTION .rsrc
IMAGE_RESOURCE_DIRECTORY
IMAGE_RESOURCE_DIRECTORY
IMAGE_RESOURCE_DIRECTORY
IMAGE_RESOURCE_DATA_ENTRY
IMAGE_RESOURCE_DIRECTORY_
BINARY TGAD 0000
Viewing BINARY TGAD 0000

```
pFile                     Raw Data                                  Value
0000B1D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0000B1E0  00 00 00 00 00 00 00 00  00 40 00 00 AC 00 00 00  .........@......
0000B1F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0000B200  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0000B210  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0000B220  00 20 00 00 7C 00 00 00  00 00 00 00 00 00 00 00  ....|...........
0000B230  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0000B240  2E 74 65 78 74 00 00 00  D8 07 00 00 00 10 00 00  .text...........
0000B250  00 08 00 00 00 04 00 00  00 00 00 00 00 00 00 00  ................
0000B260  00 00 00 00 20 00 00 60  2E 72 64 61 74 61 00 00  .......`.rdata..
0000B270  64 06 00 00 00 20 00 00  00 08 00 00 00 0C 00 00  d...............
0000B280  00 00 00 00 00 00 00 00  00 00 00 00 40 00 00 40  ............@..@
0000B290  2E 64 61 74 61 00 00 00  08 04 00 00 00 30 00 00  .data........0..
0000B2A0  00 04 00 00 00 14 00 00  00 00 00 00 00 00 00 00  ................
0000B2B0  00 00 00 00 40 00 00 C0  2E 72 65 6C 6F 63 00 00  ....@...reloc..
0000B2C0  F0 00 00 00 00 40 00 00  00 02 00 00 00 18 00 00  .....@..........
0000B2D0  00 00 00 00 00 00 00 00  00 00 00 00 40 00 00 42  ............@..B
0000B2E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0000B2F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0000B300  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0000B310  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0000B320  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0000B330  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

This is a PE file, concealed within a resource section.

Dynamic Analysis with Procmon

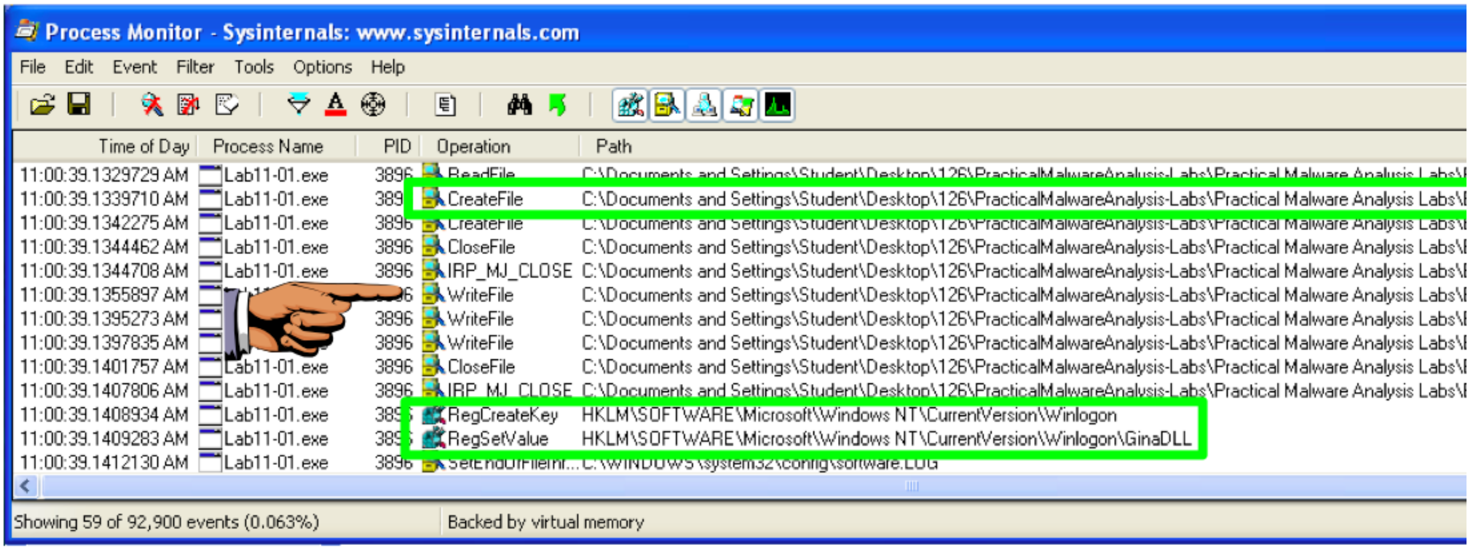
Run the malware in a virtual machine, while running Procmon to see what it does.

In Procmon, click **Filter**, "**Reset Filter**".

Click **Filter**, **Filter**. Filter for a "**Process Name**" of **Lab11-01.exe**.

Save an image showing these events, as shown below, with the filename "**Proj 14e from YOUR NAME**".

- **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**


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

```
Time of Day          Process Name   PID   Operation       Path
11:00:39.1329729 AM  Lab11-01.exe   3896  ReadFile        C:\Documents and Settings\Student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\
11:00:39.1339710 AM  Lab11-01.exe   389   CreateFile      C:\Documents and Settings\Student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\
11:00:39.1342275 AM  Lab11-01.exe   3896  CreateFile      C:\Documents and Settings\Student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\
11:00:39.1344462 AM  Lab11-01.exe   3896  CloseFile       C:\Documents and Settings\Student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\
11:00:39.1344708 AM  Lab11-01.exe   3896  IRP_MJ_CLOSE    C:\Documents and Settings\Student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\
11:00:39.1355897 AM                 6     WriteFile       C:\Documents and Settings\Student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\
11:00:39.1395273 AM                 3896  WriteFile       C:\Documents and Settings\Student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\
11:00:39.1397835 AM                 3896  WriteFile       C:\Documents and Settings\Student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\
11:00:39.1401757 AM  Lab11-01.exe   3896  CloseFile       C:\Documents and Settings\Student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\
11:00:39.1407806 AM  Lab11-01.exe   3896  IRP_MJ_CLOSE    C:\Documents and Settings\Student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\
11:00:39.1408934 AM  Lab11-01.exe   389   RegCreateKey    HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
11:00:39.1409283 AM  Lab11-01.exe   389   RegSetValue     HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL
11:00:39.1412130 AM  Lab11-01.exe   3896  SetEndOfFileInf... C:\WINDOWS\system32\config\software.LOG

Showing 59 of 92,900 events (0.063%)     Backed by virtual memory
```

These actions create a file named **msgina.dll** and insert a path to that file into registry keys that will launch the DLL when the system boots up.

Resource Hacker

Next we'll use Resource Hacker to extract the gina.dll file.

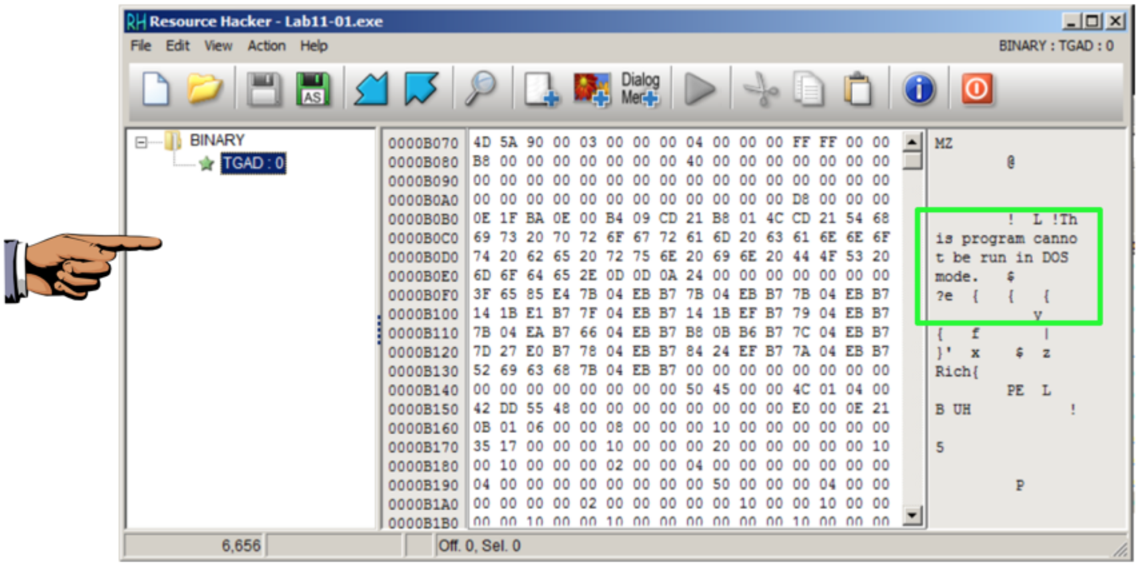
Download Resource Hacker here:

http://www.angusj.com/resourcehacker/

Open **Lab11-01.exe** in Resource Hacker.

The "**BINARY TGAD 0**" starts with **MZ** and contains the telltale text "This program cannot be run in DOS mode", as shown below--this is an EXE file.

Save an image showing the "**BINARY TGAD 0**" section, as shown below, with the filename "**Proj 14f from YOUR NAME**".



```
0000B070  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ
0000B080  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00          @
0000B090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000B0A0  00 00 00 00 00 00 00 00 00 00 00 00 D8 00 00 00
0000B0B0  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68          !  L !Th
0000B0C0  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
0000B0D0  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS
0000B0E0  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode.    $
0000B0F0  3F 65 85 E4 7B 04 EB B7 7B 04 EB B7 7B 04 EB B7  ?e  {   {   {
0000B100  14 1B E1 B7 7F 04 EB B7 14 1B EF B7 79 04 EB B7              y
0000B110  7B 04 EA B7 66 04 EB B7 B8 0B B6 B7 7C 04 EB B7  {   f       |
0000B120  7D 27 E0 B7 78 04 EB B7 84 24 EF B7 7A 04 EB B7  }'  x    $  z
0000B130  52 69 63 68 7B 04 EB B7 00 00 00 00 00 00 00 00  Rich{
0000B140  00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00          PE  L
0000B150  42 DD 55 48 00 00 00 00 00 00 00 00 E0 00 0E 21  B UH           !
0000B160  0B 01 06 00 00 08 00 00 00 10 00 00 00 00 00 00
0000B170  35 17 00 00 00 10 00 00 00 20 00 00 00 00 00 10  5
0000B180  00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00
0000B190  04 00 00 00 00 00 00 00 00 50 00 00 00 04 00 00           P
0000B1A0  00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00
0000B1B0  00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00
```

In Resource Hacker, in the left pane, click **0** to highlight it, as shown above.

Click **Action**, **Save Resource as a binary file...**".

Save the file as **YOURNAME-TGAD0.exe**, replacing the text "YOURNAME" with your own name.

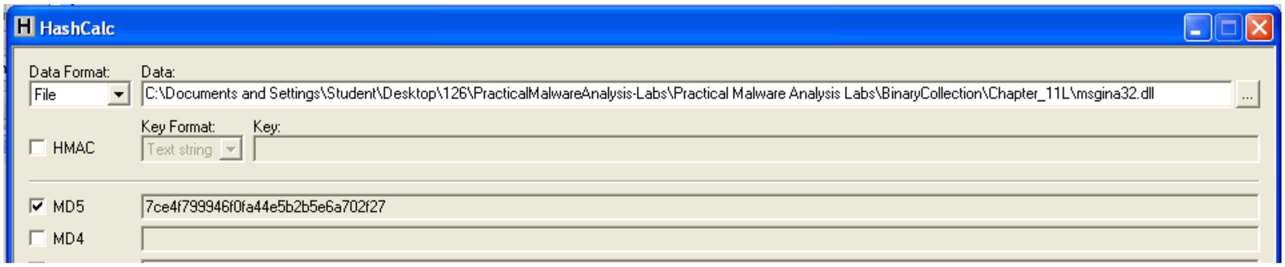
HashCalc

If you don't have it, get HashCalc here:

http://www.slavasoft.com/hashcalc/

Calculate the MD5 hash of the msgina32.dll file created by running the malware.

The MD5 hash begins with **7ce4**, as shown below.



Data Format: File

Data: C:\Documents and Settings\Student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection\Chapter_11L\msgina32.dll

□ HMAC

☑ MD5 7ce4f799946f0fa44e5b2b5e6a702f27

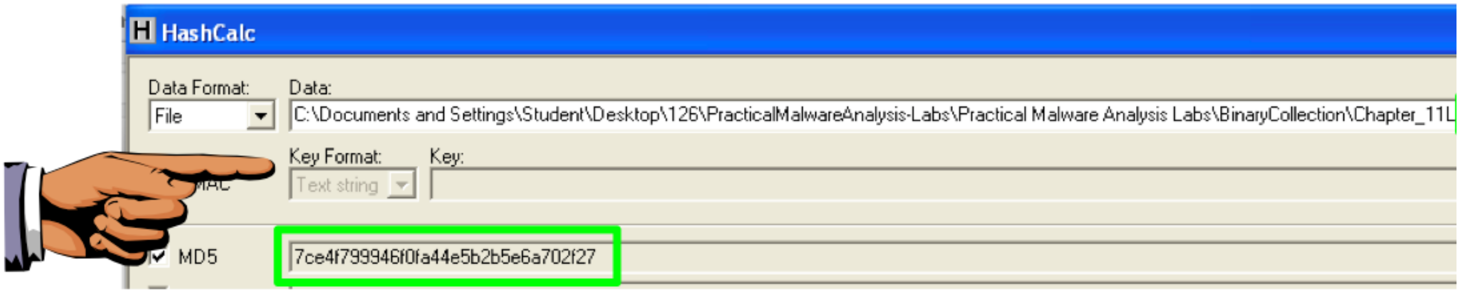
□ MD4

Calculate the MD5 hash of the **YOURNAME-TGAD0.exe** file, as shown below.

Save an image showing these elements:

- A filename containing **YOURNAME** (you will have to make the window very wide to show it if your malware samples are on your desktop like mine)
- An MD5 hash beginning with **7ce4**

Save the image with the filename "**Proj 14g from YOUR NAME**".



Data Format: File

Data: C:\Documents and Settings\Student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection\Chapter_11L

☑ MD5 7ce4f799946f0fa44e5b2b5e6a702f27

Turning in your Project

Email the images to cnit.126sam@gmail.com with the subject line: **Proj 14 from YOUR NAME**

Last modified 4-22-17