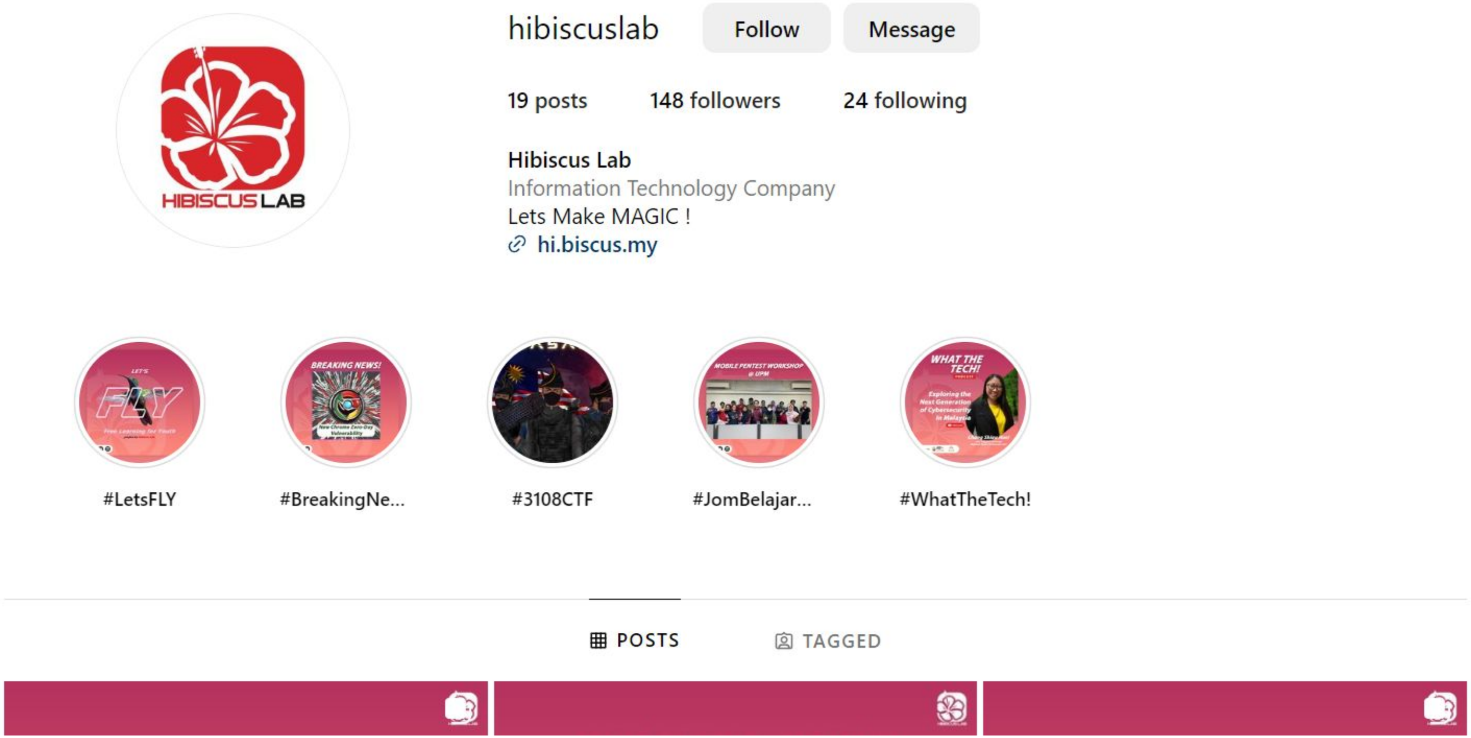
LET'S FLY WITH HIBISCUS LAB

Empower young minds with essential technical skills

HIBISCUS LAB



hibiscuslab

19 posts 148 followers 24 following

Hibiscus Lab

Information Technology Company

Lets Make MAGIC !

hi.biscus.my

#LetsFLY

#BreakingNe...

#3108CTF

#JomBelajar...

#WhatTheTech!

Legal & Ethical Agreement by Participants

- You agree to NOT misuse any of the information within to hack, whether to DDOS, deface, steal information, illegally tamper or change data or to conduct any malicious intent to any organisation or individual.
- According to **Malaysian Law, ACT 563: COMPUTER CRIMES ACT 1997 [Reprint 2002]**, will hold you liable and accountable for any misuse of the information contained within and you can be jailed and fined for any hacking offense.
- Disclaimer: Information within this Training, Workshop, document and any information and data given by our Trainer and by our Company representatives are for educational purposes ONLY and we will NOT be liable for any misuse of the information provided herein.

"ETHICS"

> whoami

•Achieved 2nd Runner Up in CYDES WARZONE CTF.

•Finalist in i-HACK 2022 in conjunction with Siber Siaga.

•Achieved Consolation Prize of Semi-Final Round in ASEAN Student Contest on Information Security (ASICS).

•Completed training courses of GCC 2022 Taiwan (the 4th Global Cybersecurity Camp).

•Participated as competitor in Enterprise Information Systems Security in WorldSkills Asia Online Friendly Skills Games 2021.

“Gentlemen, the game is Capture The Flag”

—Someone Famous

Let's Begin

01

Overview of Forensics

CTF + Forensics = ?

Forensics in the context of CTFs usually involves
some thing to do
with either recovering deleted files from an image
file or fixing
broken files to being able to find files hidden
inside of the other

Types of files you might see

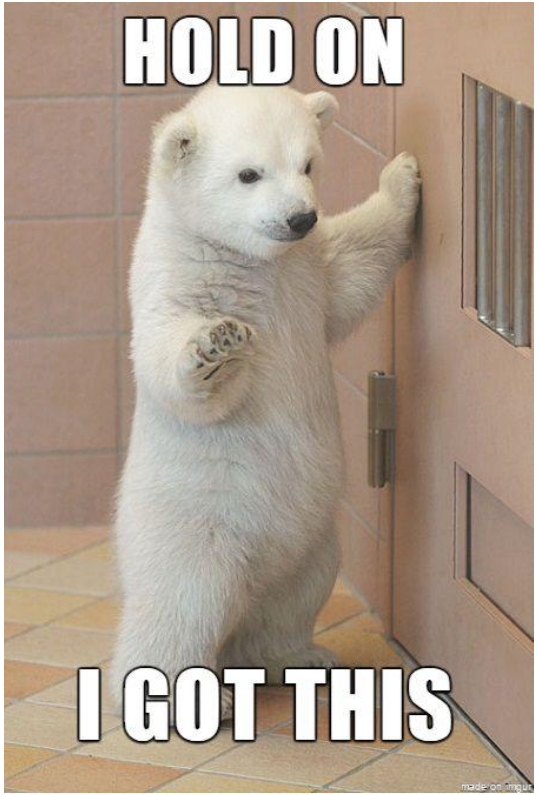
There are many different types of files you might come across but here are some important ones and the tools/programs you should try first

- .img, .raw, .e01 These should be opened with autopsy, or FTK imager
- .dmp or other memory dumps you can use volatility
- Pcap, cap uses wireshark usually

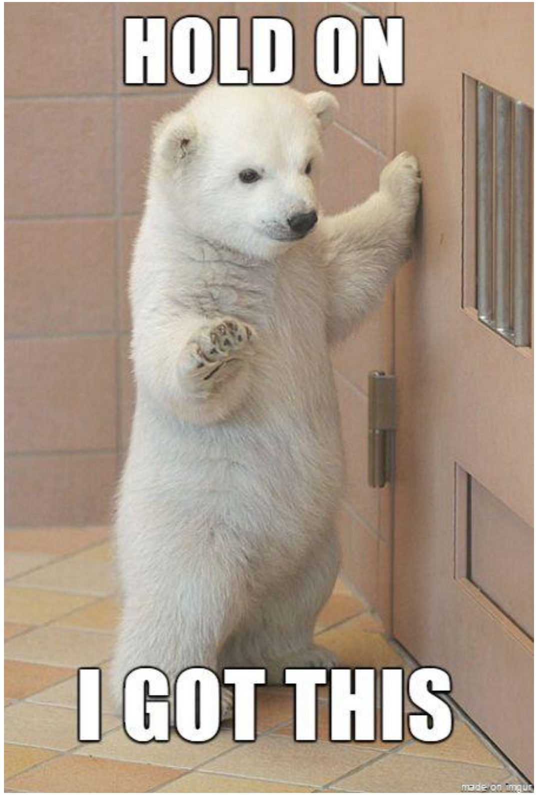
First thing first

First thing first

First thing first



First thing first



I usually use is the **file** command in linux

- This can be confused if the magic bytes are manipulated
- The file extension means nothing
- Check the file sizes

Next ...

Next …

After checking the file sizes, I want to confirm the file types.

- Using strings is very useful for finding this information.
- You can also pipe strings into grep or awk.

Then

Identifying Common File Formats at a Glance using **Magic Bytes**

Then

Identifying Common File Formats at a Glance

Sometimes people use tools that different to the challenge, leading to unsuccessful results. They often mix this up with steganography or reverse engineering challenges.

Then

Identifying Common File Formats at a Glance

Example:

Signature: 0x4D 0x5A
Signature: 0x7F 0x45 0x4C 0x46
Signature: 0x50 0x4B 0x03 0x04

Then

Identifying Common File Formats at a Glance

Example:

Signature: 0x4D 0x5A > "MZ"
Signature: 0x7F 0x45 0x4C 0x46 > ".ELF"
Signature: 0x50 0x4B 0x03 0x04 > "PK.."

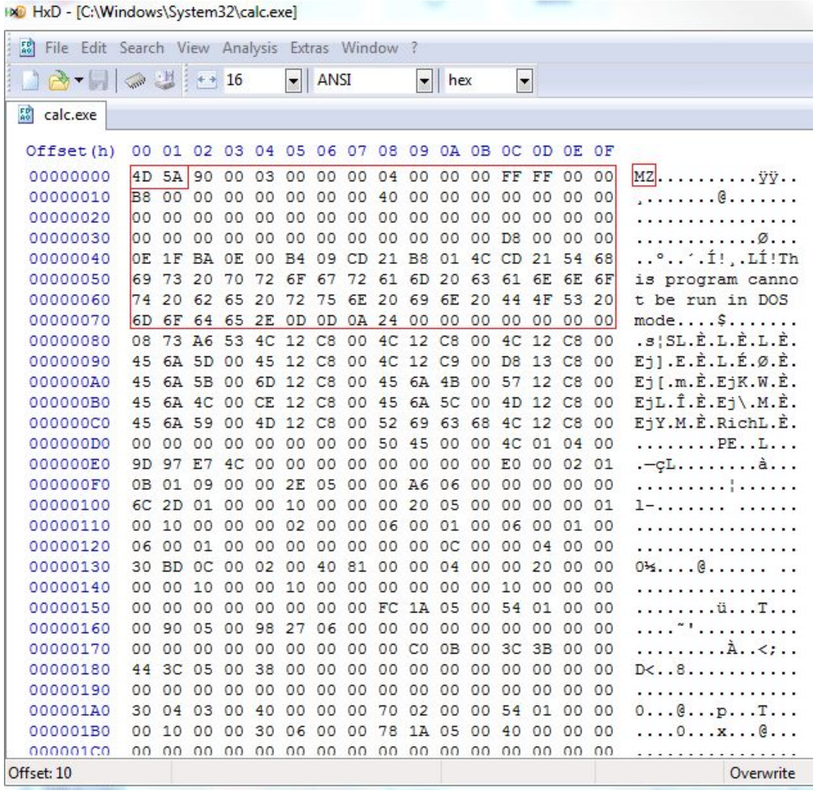
Then

Identifying Common File Formats at a Glance

Example:

Signature: 0x4D 0x5A > "MZ" > DOS
Signature: 0x7F 0x45 0x4C 0x46 > ".ELF" > ELF
Signature: 0x50 0x4B 0x03 0x04 > "PK.." > Zip

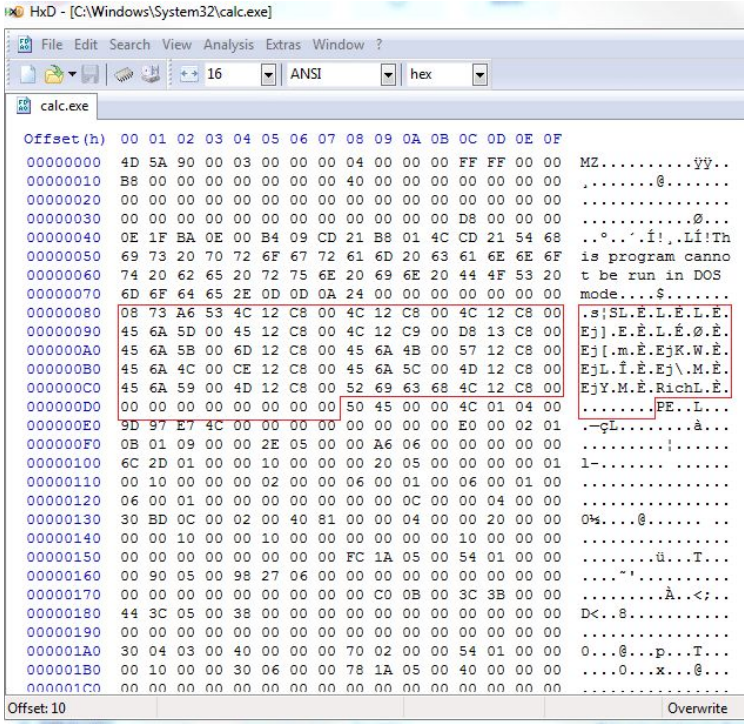
Deep dive: Calc.exe


HxD - [C:\Windows\System32\calc.exe]
File Edit Search View Analysis Extras Window ?
16
ANSI
hex
calc.exe

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 D8 00 00 00  ............Ø...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  08 73 A6 53 4C 12 C8 00 4C 12 C8 00 4C 12 C8 00  .s¦SL.È.L.È.L.È.
00000090  45 6A 5D 00 45 12 C8 00 4C 12 C9 00 D8 13 C8 00  Ej].E.È.L.É.Ø.È.
000000A0  45 6A 5B 00 6D 12 C8 00 45 6A 4B 00 57 12 C8 00  Ej[.m.È.EjK.W.È.
000000B0  45 6A 4C 00 CE 12 C8 00 45 6A 5C 00 4D 12 C8 00  EjL.Î.È.Ej\.M.È.
000000C0  45 6A 59 00 4D 12 C8 00 52 69 63 68 4C 12 C8 00  EjY.M.È.RichL.È.
000000D0  00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00  ........PE..L...
000000E0  9D 97 E7 4C 00 00 00 00 00 00 00 00 E0 00 02 01  .—çL........à...
000000F0  0B 01 09 00 00 2E 05 00 00 A6 06 00 00 00 00 00  .........¦......
00000100  6C 2D 01 00 00 10 00 00 00 20 05 00 00 00 00 01  l-....... ......
00000110  00 10 00 00 00 02 00 00 06 00 01 00 06 00 01 00  ................
00000120  06 00 01 00 00 00 00 00 00 0C 00 00 04 00 00 00  ................
00000130  30 BD 0C 00 02 00 40 81 00 00 04 00 00 20 00 00  0½....@...... ..
00000140  00 00 10 00 00 10 00 00 00 00 00 10 00 00 00 00  ................
00000150  00 00 00 00 00 00 00 00 FC 1A 05 00 54 01 00 00  ........ü...T...
00000160  00 90 05 00 98 27 06 00 00 00 00 00 00 00 00 00  ....˜'..........
00000170  00 00 00 00 00 00 00 00 00 C0 0B 00 3C 3B 00 00  .........À..<;..
00000180  44 3C 05 00 38 00 00 00 00 00 00 00 00 00 00 00  D<..8...........
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0  30 04 03 00 40 00 00 00 70 02 00 00 54 01 00 00  0...@...p...T...
000001B0  00 10 00 00 30 06 00 00 78 1A 05 00 40 00 00 00  ....0...x...@...
000001C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

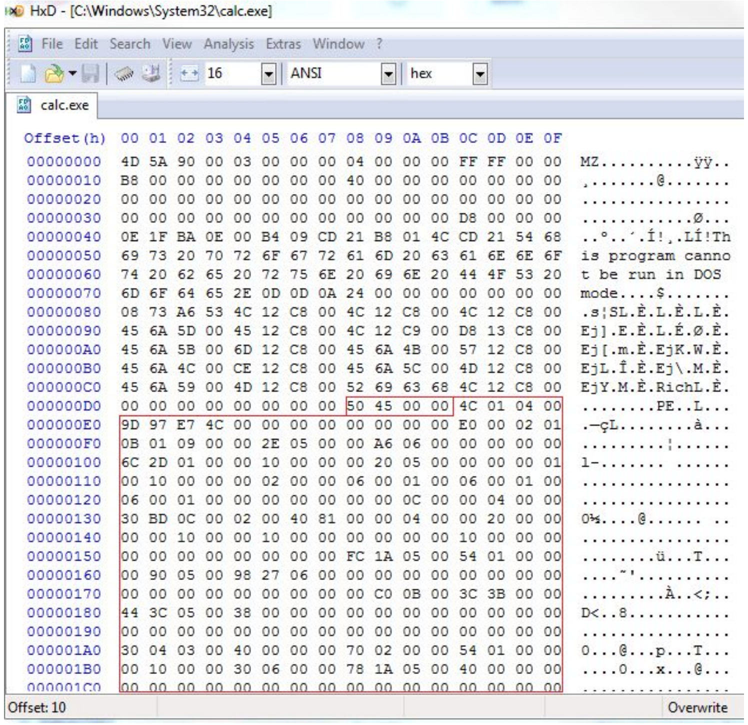
Deep dive: Calc.exe



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 D8 00 00 00  ............Ø...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  08 73 A6 53 4C 12 C8 00 4C 12 C8 00 4C 12 C8 00  .s¦SL.È.L.È.L.È.
00000090  45 6A 5D 00 45 12 C8 00 4C 12 C9 00 D8 13 C8 00  Ej].E.È.L.É.Ø.È.
000000A0  45 6A 5B 00 6D 12 C8 00 45 6A 4B 00 57 12 C8 00  Ej[.m.È.EjK.W.È.
000000B0  45 6A 4C 00 CE 12 C8 00 45 6A 5C 00 4D 12 C8 00  EjL.Î.È.Ej\.M.È.
000000C0  45 6A 59 00 4D 12 C8 00 52 69 63 68 4C 12 C8 00  EjY.M.È.RichL.È.
000000D0  00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00  ........PE..L...
000000E0  9D 97 E7 4C 00 00 00 00 00 00 00 00 E0 00 02 01  .—çL........à...
000000F0  0B 01 09 00 00 2E 05 00 00 A6 06 00 00 00 00 00  .........¦......
00000100  6C 2D 01 00 00 10 00 00 00 20 05 00 00 00 00 01  l-....... ......
00000110  00 10 00 00 00 02 00 00 06 00 01 00 06 00 01 00  ................
00000120  06 00 01 00 00 00 00 00 00 00 0C 00 00 04 00 00  ................
00000130  30 BD 0C 00 02 00 40 81 00 00 04 00 00 20 00 00  0½....@...... ..
00000140  00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00  ................
00000150  00 00 00 00 00 00 00 00 FC 1A 05 00 54 01 00 00  ........ü...T...
00000160  00 90 05 00 98 27 06 00 00 00 00 00 00 00 00 00  ....˜'..........
00000170  00 00 00 00 00 00 00 00 00 C0 0B 00 3C 3B 00 00  .........À..<;..
00000180  44 3C 05 00 38 00 00 00 00 00 00 00 00 00 00 00  D<..8...........
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0  30 04 03 00 40 00 00 00 70 02 00 00 54 01 00 00  0...@...p...T...
000001B0  00 10 00 00 30 06 00 00 78 1A 05 00 40 00 00 00  ....0...x...@...
000001C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Deep dive: Calc.exe

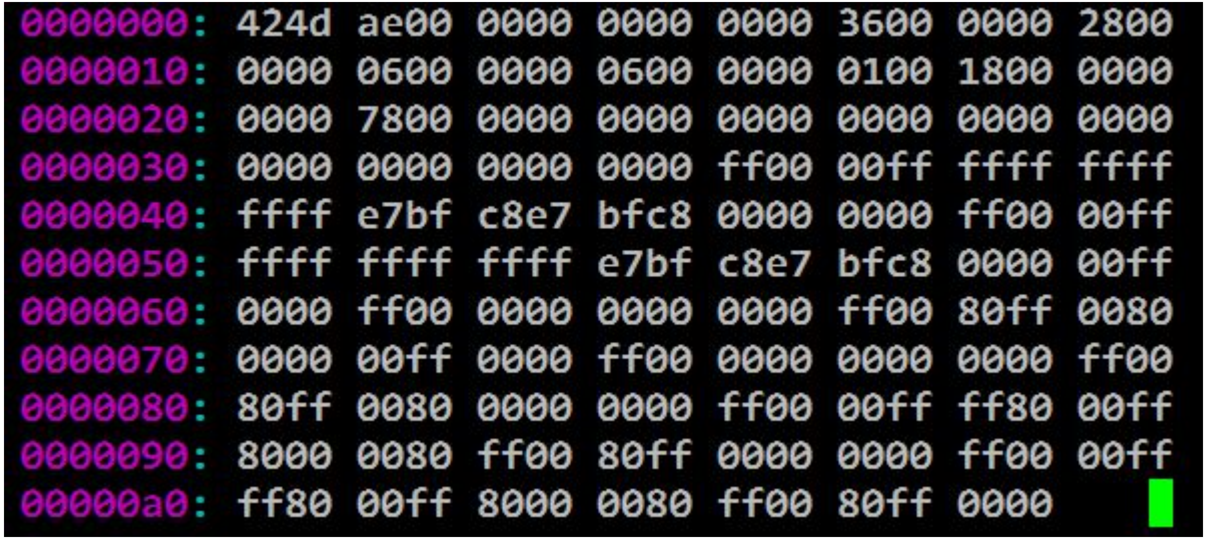

HxD - [C:\Windows\System32\calc.exe]
File Edit Search View Analysis Extras Window ?
16
ANSI
hex
calc.exe
Offset: 10
Overwrite

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 D8 00 00 00  ............Ø...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  08 73 A6 53 4C 12 C8 00 4C 12 C8 00 4C 12 C8 00  .s¦SL.È.L.È.L.È.
00000090  45 6A 5D 00 45 12 C8 00 4C 12 C9 00 D8 13 C8 00  Ej].E.È.L.É.Ø.È.
000000A0  45 6A 5B 00 6D 12 C8 00 45 6A 4B 00 57 12 C8 00  Ej[.m.È.EjK.W.È.
000000B0  45 6A 4C 00 CE 12 C8 00 45 6A 5C 00 4D 12 C8 00  EjL.Î.È.Ej\.M.È.
000000C0  45 6A 59 00 4D 12 C8 00 52 69 63 68 4C 12 C8 00  EjY.M.È.RichL.È.
000000D0  00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00  ........PE..L...
000000E0  9D 97 E7 4C 00 00 00 00 00 00 00 00 E0 00 02 01  .—çL........à...
000000F0  0B 01 09 00 00 2E 05 00 00 A6 06 00 00 00 00 00  .........¦......
00000100  6C 2D 01 00 00 10 00 00 00 20 05 00 00 00 00 01  l-....... ......
00000110  00 10 00 00 00 02 00 00 06 00 01 00 06 00 01 00  ................
00000120  06 00 01 00 00 00 00 00 00 00 0C 00 00 04 00 00  ................
00000130  30 BD 0C 00 02 00 40 81 00 00 04 00 00 20 00 00  0½....@...... ..
00000140  00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00  ................
00000150  00 00 00 00 00 00 00 00 FC 1A 05 00 54 01 00 00  ........ü...T...
00000160  00 90 05 00 98 27 06 00 00 00 00 00 00 00 00 00  ....˜'..........
00000170  00 00 00 00 00 00 00 00 00 C0 0B 00 3C 3B 00 00  .........À..<;..
00000180  44 3C 05 00 38 00 00 00 00 00 00 00 00 00 00 00  D<..8...........
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0  30 04 03 00 40 00 00 00 70 02 00 00 54 01 00 00  0...@...p...T...
000001B0  00 10 00 00 30 06 00 00 78 1A 05 00 40 00 00 00  ....0...x...@...
000001C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Exercise 1

What is the Magic Bytes based on the picture below?



```
0000000: 424d ae00 0000 0000 0000 3600 0000 2800
0000010: 0000 0600 0000 0600 0000 0100 1800 0000
0000020: 0000 7800 0000 0000 0000 0000 0000 0000
0000030: 0000 0000 0000 0000 ff00 00ff ffff ffff
0000040: ffff e7bf c8e7 bfc8 0000 0000 ff00 00ff
0000050: ffff ffff ffff e7bf c8e7 bfc8 0000 00ff
0000060: 0000 ff00 0000 0000 0000 ff00 80ff 0080
0000070: 0000 00ff 0000 ff00 0000 0000 0000 ff00
0000080: 80ff 0080 0000 0000 ff00 00ff ff80 00ff
0000090: 8000 0080 ff00 80ff 0000 0000 ff00 00ff
00000a0: ff80 00ff 8000 0080 ff00 80ff 0000
```

Try to remember common signatures

https://en.wikipedia.org/wiki/List_of_file_signatures

02

Memory Dump: Volatility

What can volatility do?

Volatility is a command-line tool that lets DFIR teams acquire and analyze the volatile data that is temporarily stored in random access memory (RAM).

Basic commands

```
python vol.py –f %image_name% imageinfo
```

- Gets the profile to continue working on the dump

```
python vol.py –f %path_to_image%
––profile=%profile_name% pstree
```

- Shows all of the running processes

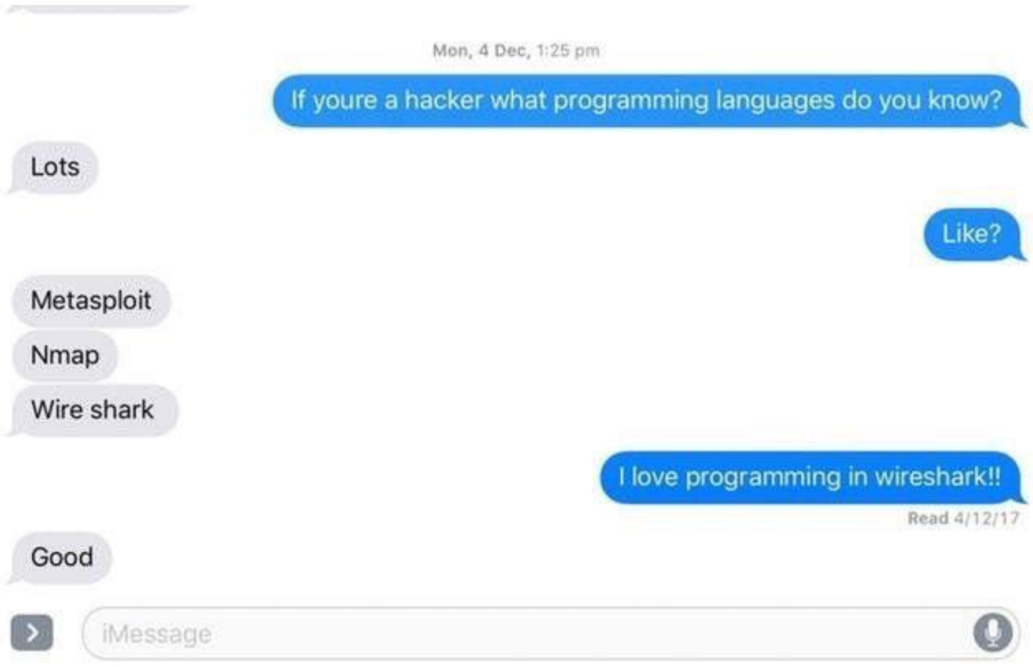
You can learn here,
a bit advanced for beginner

https://www.varonis.com/blog/how-to-use-volatility

02

Network Protocol Analyzer: Wireshark

Essential tool to be hackerz



Mon, 4 Dec, 1:25 pm

If youre a hacker what programming languages do you know?

Lots

Like?

Metasploit

Nmap

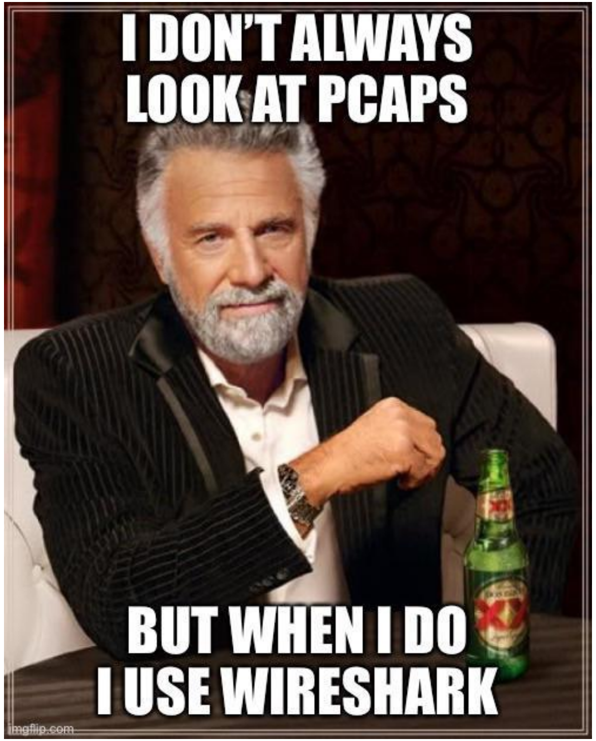
Wire shark

I love programming in wireshark!!

Read 4/12/17

Good

Lets begin


I DON'T ALWAYS LOOK AT PCAPS
BUT WHEN I DO I USE WIRESHARK
imgflip.com

Why wireshark?

Wireshark is a network protocol analyzer which is often used in CTF challenges to look at recorded network traffic. Wireshark uses a filetype called .pcap, or "packet capture", to record traffic.

‘Sniffing’ packet

Beginner Guidelines

- Things to look for include insecure protocols like **HTTP**, **FTP**, **Telnet**
- Following **tcp/http streams** can help make things more visible
- You can export things from the packet analysis using **export** and then **http objects** or you can follow the tcp steam and then save it to your desktop

Exercise 2

What can you read when you follow tcp streams

Exercise 3

What can you get when you export HTTP objects?

03

Digital Evidence Investigation

Plenty of tools you can choose

I choose ‘autopsy’

File that usually going well with autopsy :

.RAW
.E01

You can learn here,
a bit advanced for beginner

https://medium.com/@tusharcool118/autopsy-tutorial-for-digital-forensics-707ea5d5994d