Practical Malware Analysis — Chapter 3 — Lab03–04 — Solution

Kamran Saifullah · Follow

3 min read · Aug 29, 2019

Listen Share

This is going to be the last lab of the Chapter 3. We are provided with the Lab03–04.exe and we need to analyze it using the basic dynamic analysis technique.

The strings reveal the following strings.

> *!This program cannot be run in DOS mode.*
> *6K4*
> *6KRich*
> *.text*
> *`.rdata*
> *@.data*
> *Microsoft Visual C++ Runtime Library*
> *Runtime Error!*
> *Program:*
> *…*
> *<program name unknown>*
> ***SunMonTueWedThuFriSat***
> ***JanFebMarAprMayJunJulAugSepOctNovDec***
> *.com*
> *.bat*
> *.cmd*

user32.dll

PATH

CloseHandle

SetFileTime

GetFileTime

CreateFileA

GetSystemDirectoryA

GetLastError

ReadFile

WriteFile

Sleep

GetShortPathNameA

GetModuleFileNameA

CopyFileA

ExpandEnvironmentStringsA

DeleteFileA

KERNEL32.dll

RegQueryValueExA

RegOpenKeyExA

RegSetValueExA

RegCreateKeyExA

RegDeleteValueA

CreateServiceA

CloseServiceHandle

ChangeServiceConfigA

OpenServiceA

OpenSCManagerA

DeleteService

ADVAPI32.dll

ShellExecuteA

SHELL32.dll

WS2_32.dll

ExitProcess

TerminateProcess

GetCurrentProcess

GetTimeZoneInformation

GetSystemTime

GetLocalTime

DuplicateHandle

GetCommandLineA

GetVersion

SetStdHandle

GetFileType

SetHandleCount

GetStdHandle

GetStartupInfoA

CreatePipe

GetExitCodeProcess

WaitForSingleObject

HeapReAlloc

HeapAlloc

GetCPInfo

GetACP

GetOEMCP

UnhandledExceptionFilter

FreeEnvironmentStringsA

FreeEnvironmentStringsW

WideCharToMultiByte

GetEnvironmentStrings

GetEnvironmentStringsW

GetModuleHandleA

GetEnvironmentVariableA

GetVersionExA

HeapDestroy

HeapCreate

VirtualFree

HeapFree

RtlUnwind

MultiByteToWideChar

GetStringTypeA

GetStringTypeW

SetFilePointer

VirtualAlloc

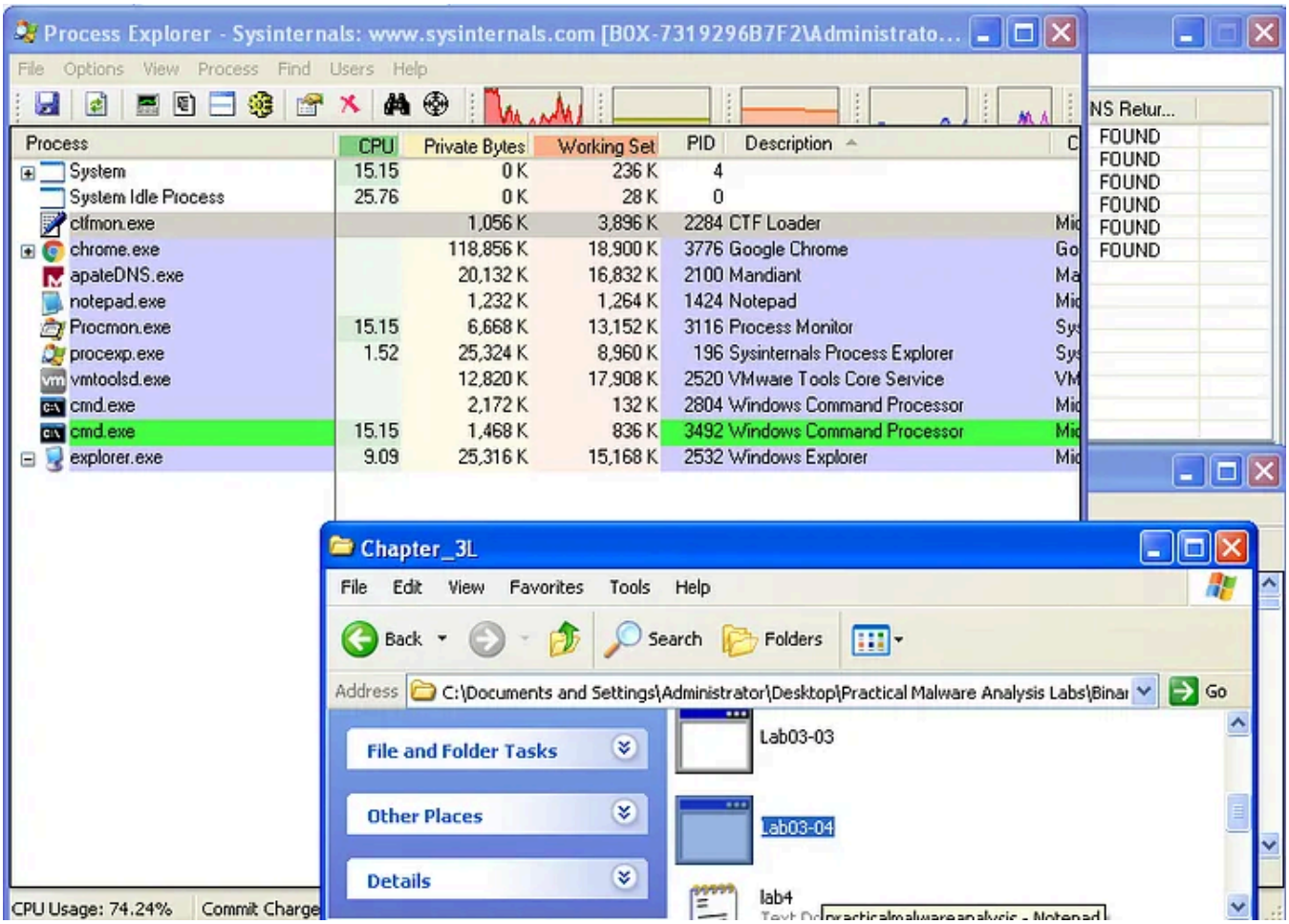
LCMapStringA

> *LCMapStringW*
> *GetProcAddress*
> ***LoadLibraryA***
> *FlushFileBuffers*
> *GetFileAttributesA*
> *CreateProcessA*
> ***CompareStringA***
> ***CompareStringW***
> *SetEnvironmentVariableA*
> *lZ@*
> *Configuration*
> ***SOFTWARE\Microsoft \XPS***
> ***\kernel32.dll***
> ***HTTP/1.0***
> ***GET***
> ‘‘’‘’
> ‘’‘’‘‘
> ***NOTHING***
> ***CMD***
> ***DOWNLOAD***
> ***UPLOAD***
> ***SLEEP***
> ***cmd.exe***
> *>> NUL*
> */c del*
> *ups*
> ***http://www.practicalmalwareanalysis.com***
> ***Manager Service***
> ***.exe***
> ***%SYSTEMROOT%\system32***
> *k:%s h:%s p:%s per:%s*

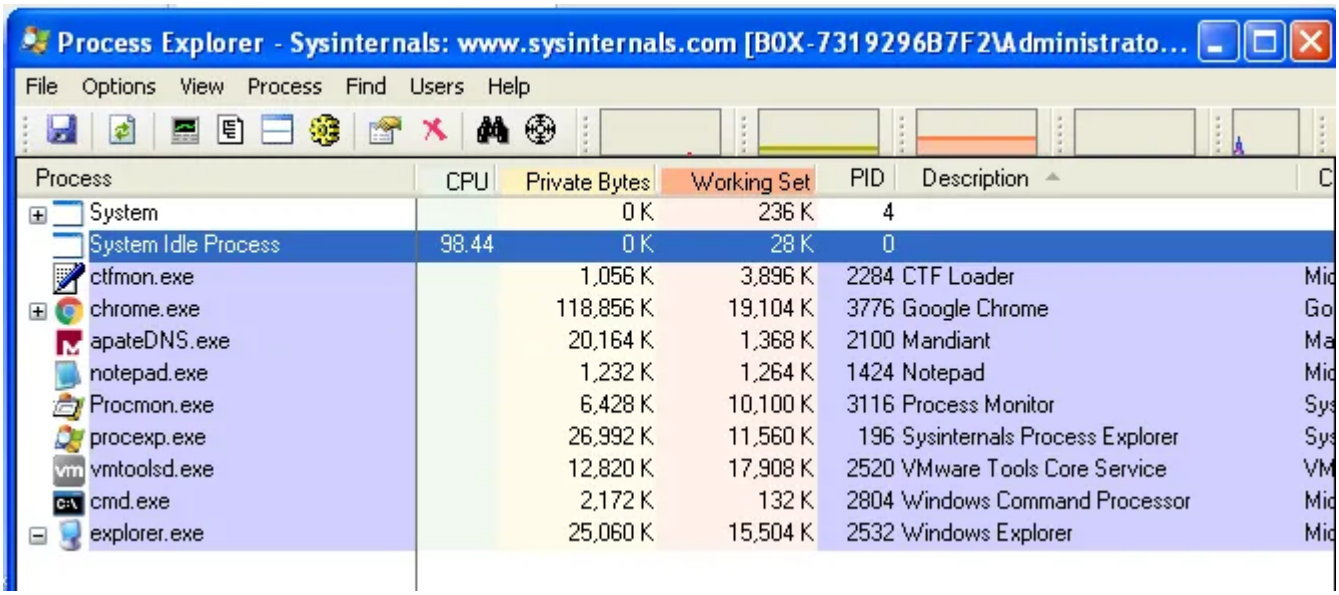
Analyzing the string we can see that we have the URL, we have something called DOWNLOAD, UPLOAD, SLEEP, CMD. Looks like a downloader. Strings are being compared both ASCII and WORD, service manager is being opened. File is being created and removed. Service is being created and removed. System directory

structure is being fetched. System Local Time is also being fetched etc. These are a lot more things this executable is doing.

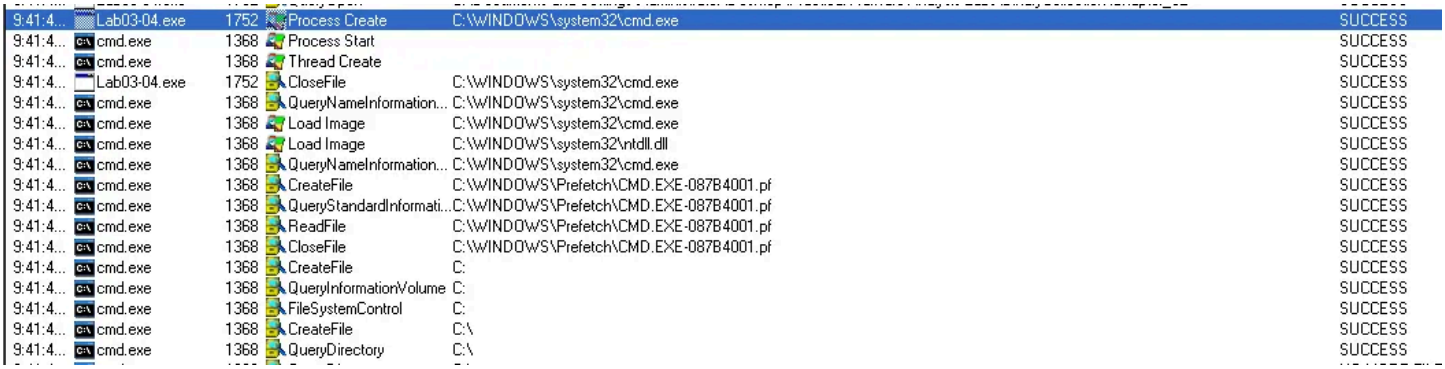
Let's analyze it using basic dynamic analysis technique.



On running the process CMD is opened and then closed. The CMD with PID 2804 is the one i have opened.



and when i tried to look into the folder the executable is gone. It means that the original executable is replacing itself somewhere else under some other name while removing itself. We can observe the processes via the process monitor and can see that CMD process was created. It did its job and then closed itself.



9:41:4...	Lab03-04.exe	1752	Process Create	C:\WINDOWS\system32\cmd.exe	SUCCESS
9:41:4...	cmd.exe	1368	Process Start		SUCCESS
9:41:4...	cmd.exe	1368	Thread Create		SUCCESS
9:41:4...	Lab03-04.exe	1752	CloseFile	C:\WINDOWS\system32\cmd.exe	SUCCESS
9:41:4...	cmd.exe	1368	QueryNameInformation...	C:\WINDOWS\system32\cmd.exe	SUCCESS
9:41:4...	cmd.exe	1368	Load Image	C:\WINDOWS\system32\cmd.exe	SUCCESS
9:41:4...	cmd.exe	1368	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS
9:41:4...	cmd.exe	1368	QueryNameInformation...	C:\WINDOWS\system32\cmd.exe	SUCCESS
9:41:4...	cmd.exe	1368	CreateFile	C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf	SUCCESS
9:41:4...	cmd.exe	1368	QueryStandardInformati...	C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf	SUCCESS
9:41:4...	cmd.exe	1368	ReadFile	C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf	SUCCESS
9:41:4...	cmd.exe	1368	CloseFile	C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf	SUCCESS
9:41:4...	cmd.exe	1368	CreateFile	C:	SUCCESS
9:41:4...	cmd.exe	1368	QueryInformationVolume	C:	SUCCESS
9:41:4...	cmd.exe	1368	FileSystemControl	C:	SUCCESS
9:41:4...	cmd.exe	1368	CreateFile	C:\	SUCCESS
9:41:4...	cmd.exe	1368	QueryDirectory	C:\	SUCCESS

On closer look we can see the command for deleting the executable as well.

Let's try to answer the questions for now.

Lab 3–4

Analyze the malware found in the file Lab03–04.exe using basic dynamic analysis tools. (This program is analyzed further in the Chapter 9 labs.)

Questions

1. **What happens when you run this file?**

When we run the file. Process is created which opens up the CMD and then deleted the original executable after making it execute and hide itself somewhere else.

2. What is causing the roadblock in dynamic analysis?

The executable is evasive and trying to evade itself by checking whether the system is VM or not. AV-Detection etc. Obviously this will make it difficult to observer the file via dynamic analysis.

3. Are there other ways to run this program?

The other ways can be to open this executable using Ollydbg or IDA pro where we can analyze it in a more efficient way.

Programming

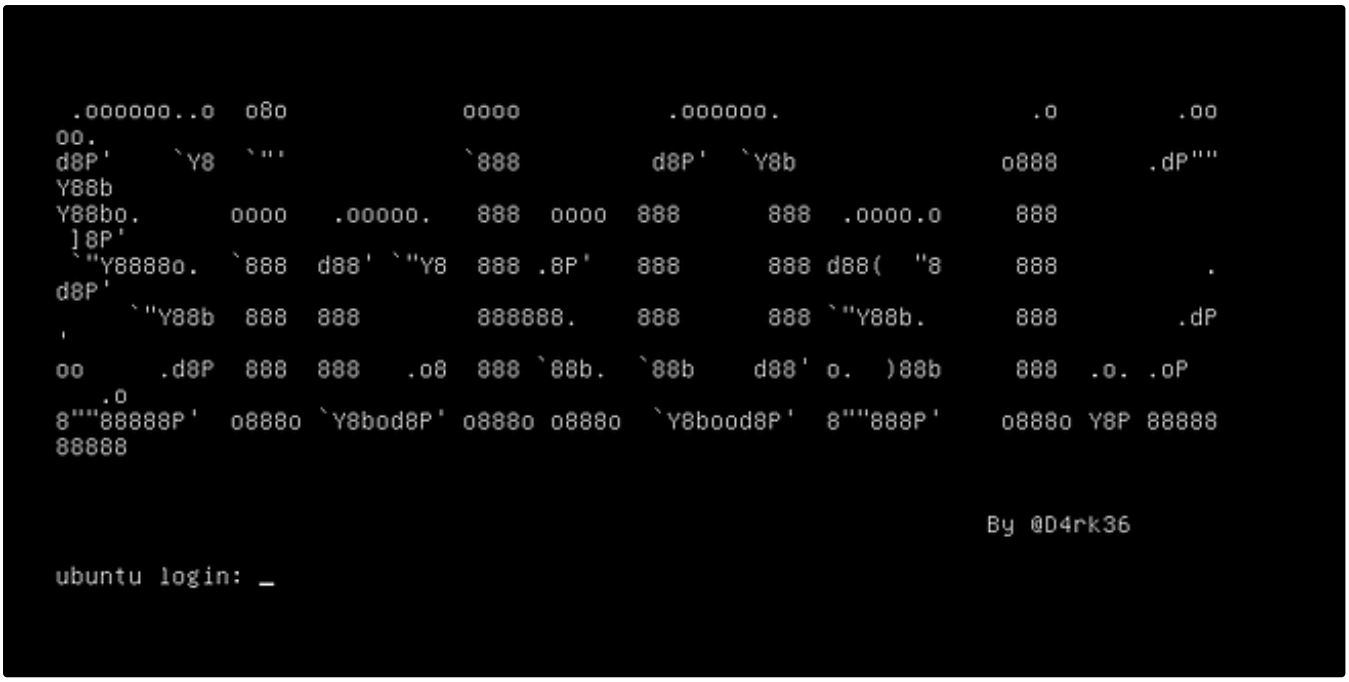
Follow

Written by Kamran Saifullah

378 Followers

Malware/RE/Firmware Analysis, App Sec/Off Sec, VAPT, Phishing Simulations/SE | Risk Management, IS Governance, Audits, ISO 27001 LI

More from Kamran Saifullah



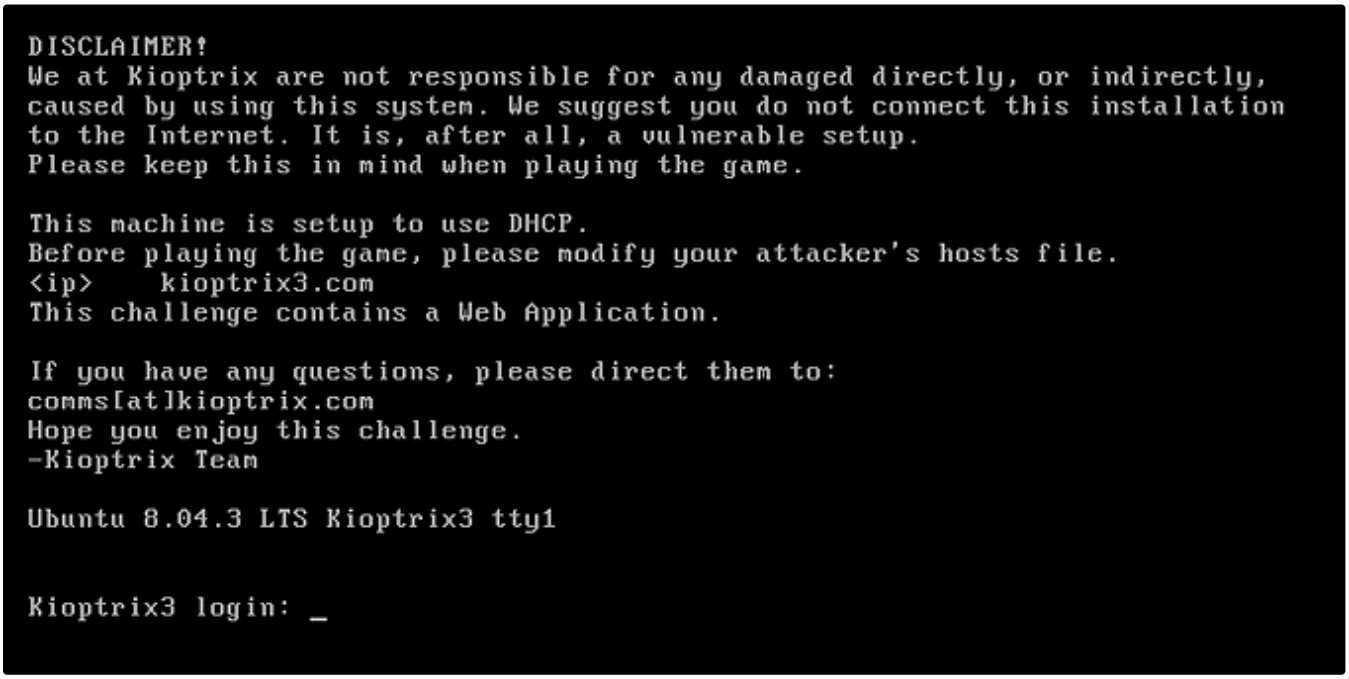
Kamran Saifullah

SickOS 1.2 WalkThrough

Hi,

5 min read · Apr 14, 2018

10



Kamran Saifullah

WalkThrough! Kioptrix — 3 By VulnHub

Hi,

8 min read · Mar 13, 2018

24

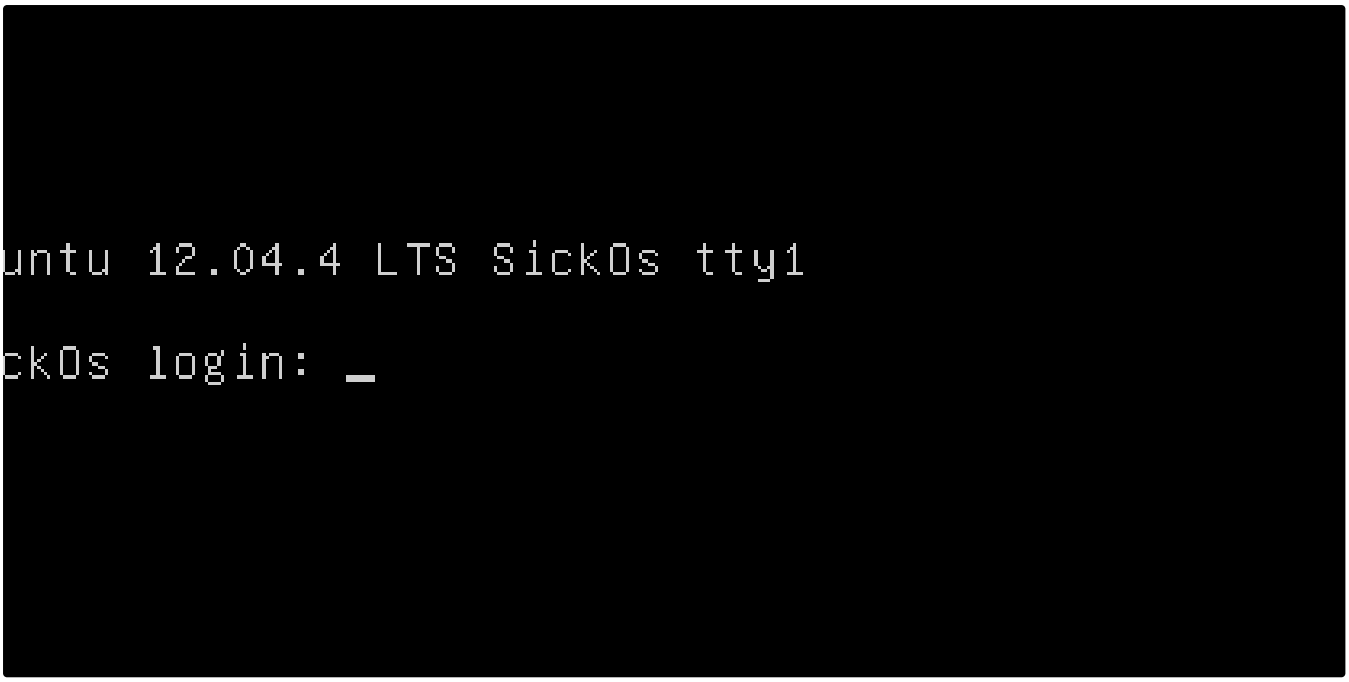
Kamran Saifullah

HSCTF 6—Forensics Challenges—Solutions

After publishing the solutions of the web challenges now it's time to move on with forensics challenges and this is all about how i solved...

5 min read · Jun 13, 2019

17

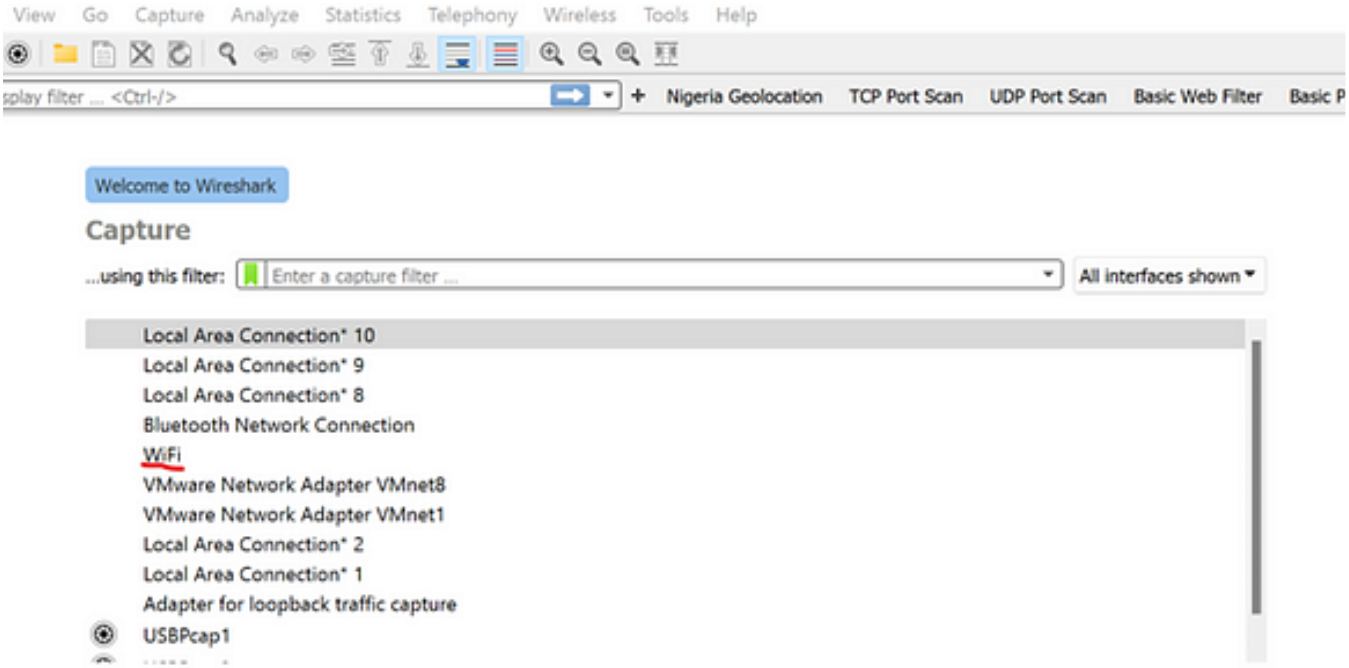


Kamran Saifullah

SickOS 1.1 Walkthrough

Hi,

5 min read · Apr 11, 2018



Kevin Moore

Analyzing PCAP Files using Wireshark

Hello, thanks for stopping by to read this blog. Its a deep-dive into the use of Wireshark to investigate captured network traffic.

6 min read · Nov 20, 2023

7

Abhay Kumar

OOPs in Python

An easy guide

10 min read · Apr 9, 2024

Lists

General Coding Knowledge

20 stories · 1148 saves

Coding & Development

11 stories · 579 saves

Stories to Help You Grow as a Software Developer

19 stories · 1007 saves

ChatGPT

21 stories · 596 saves

Yen

TryHackMe Writeups—Basic Malware RE

Are you ready to dive in the field of Malware Analysis?

3 min read · Nov 11, 2023

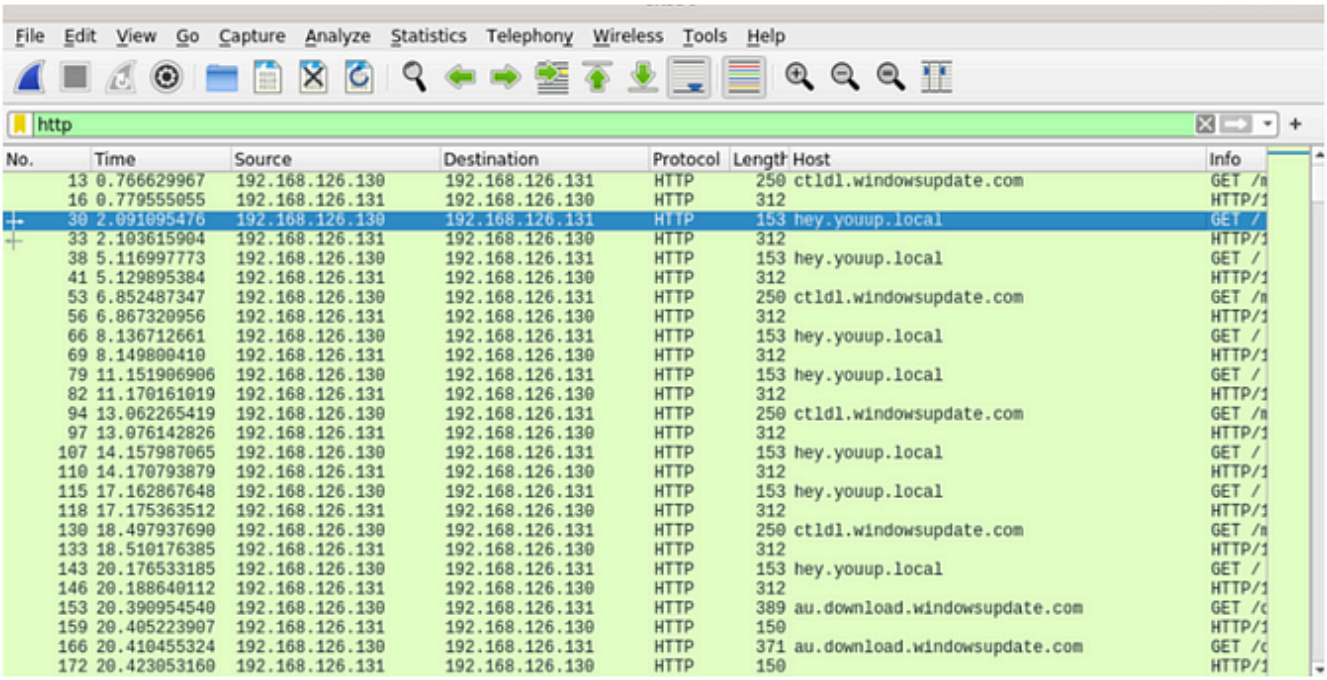
Worldsleaks

OpenWire—

CyberDefenders CTF

7 min read · Jan 25, 2024

13



Hüseyin EKŞİ

Malware Analysis of PMAT-Bonus Unknown malware

I have analyzed the Bonus malware called unknown and would like to share my findings. If you have analyzed this piece of malware please...

3 min read · Jan 21, 2024

13

Rewa Aslekar

Malware Analysis

A Beginner's guide to Malware Analysis

13 min read · Oct 31, 2023

16

See more recommendations