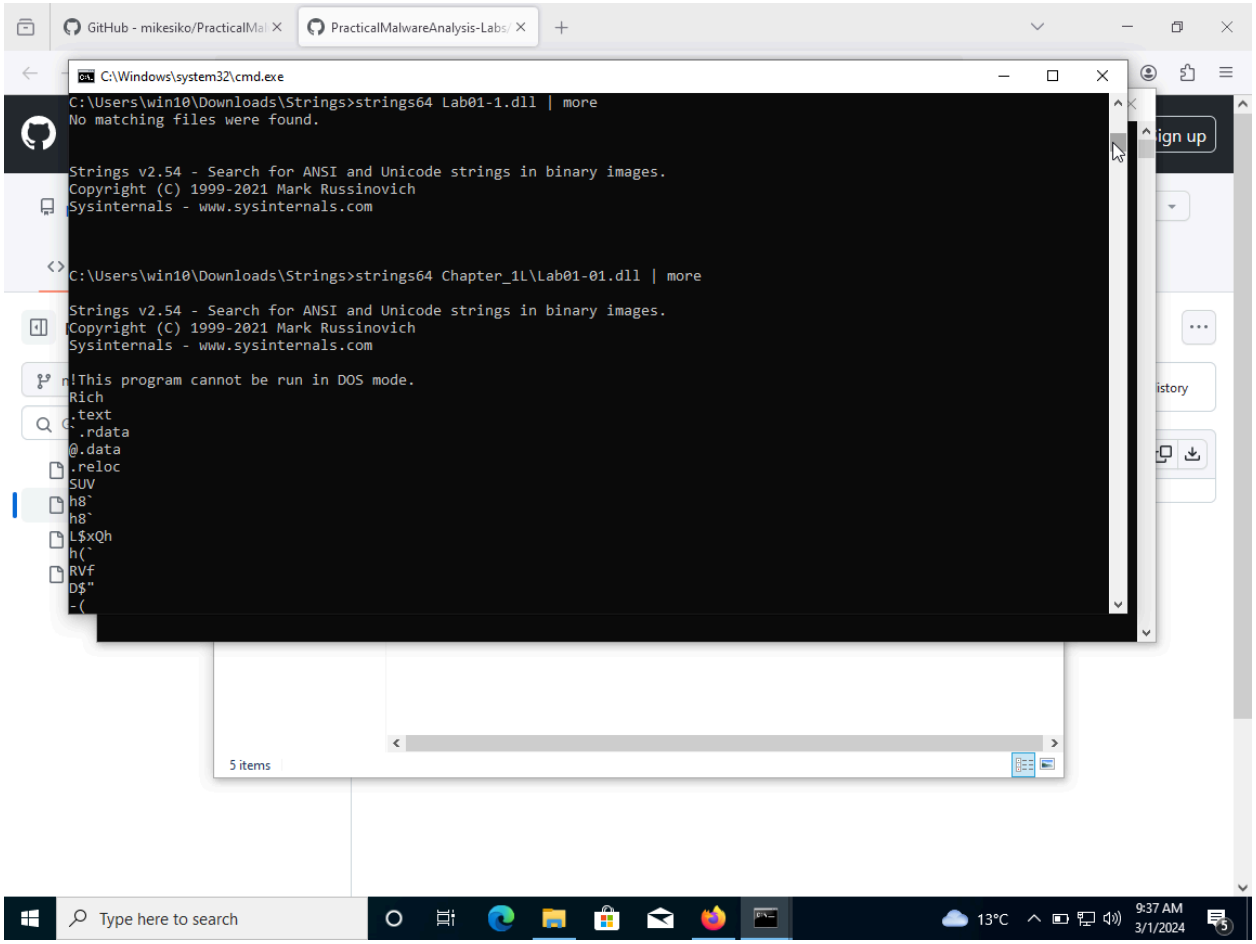
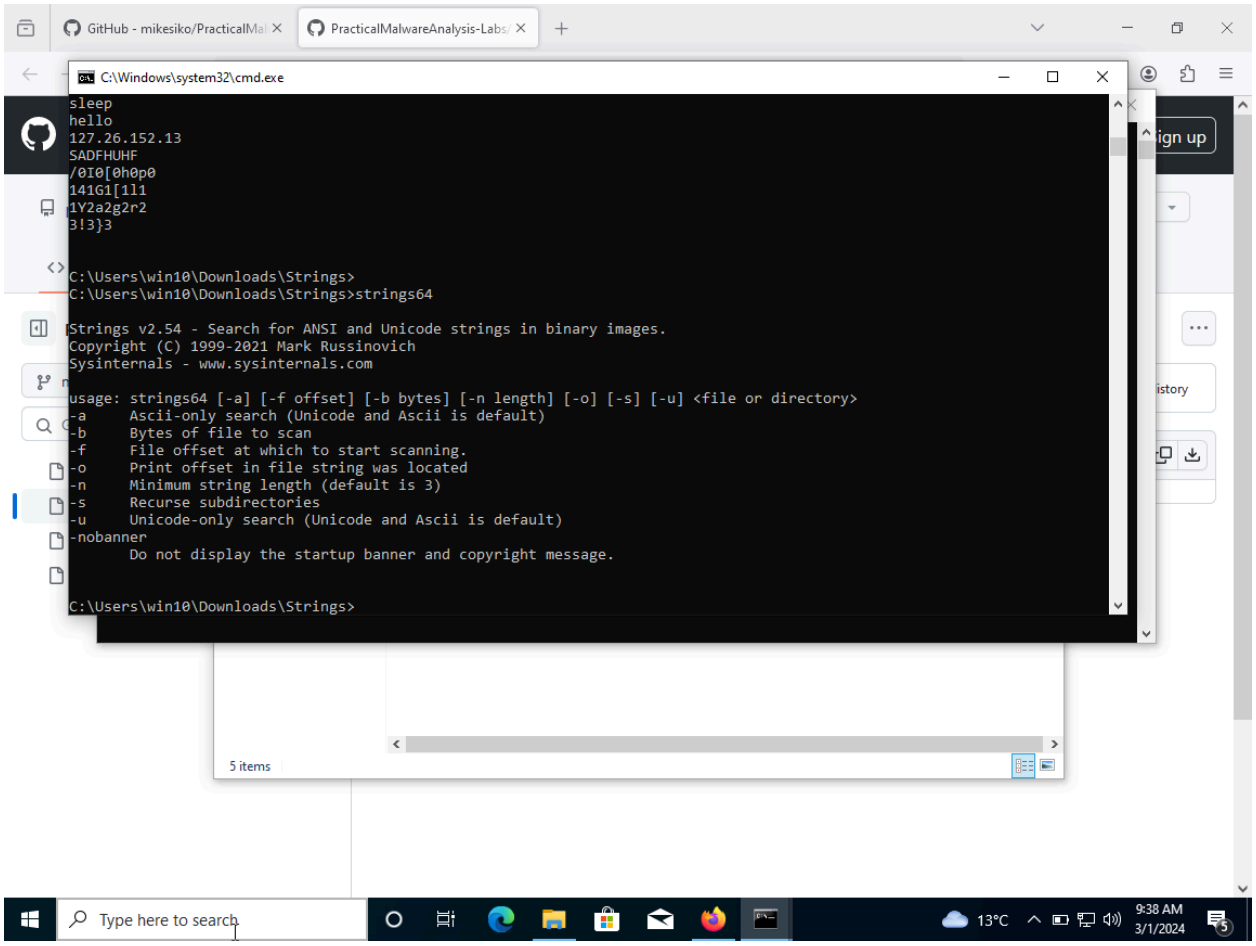
Lab 15.01

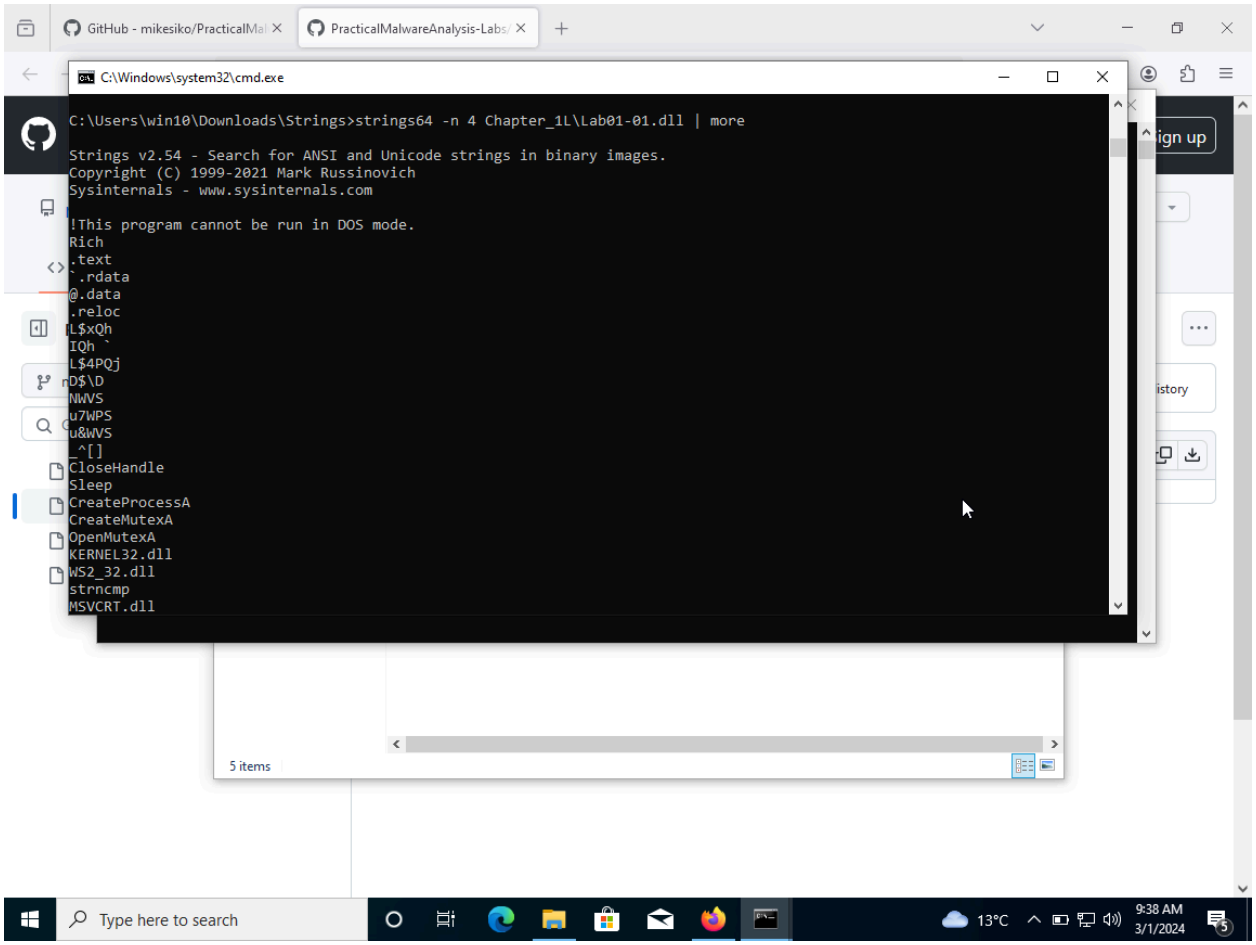
1a,


GitHub - mikesiko/PracticalMal
PracticalMalwareAnalysis-Labs/
C:\Windows\system32\cmd.exe
C:\Users\win10\Downloads\Strings>strings64 Lab01-1.dll | more
No matching files were found.
Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com
C:\Users\win10\Downloads\Strings>strings64 Chapter_1L\Lab01-01.dll | more
Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.reloc
SUV
h8`
h8`
L$xQh
h(`
RVf
D$"
-(
5 items
Type here to search
13°C
9:37 AM
3/1/2024

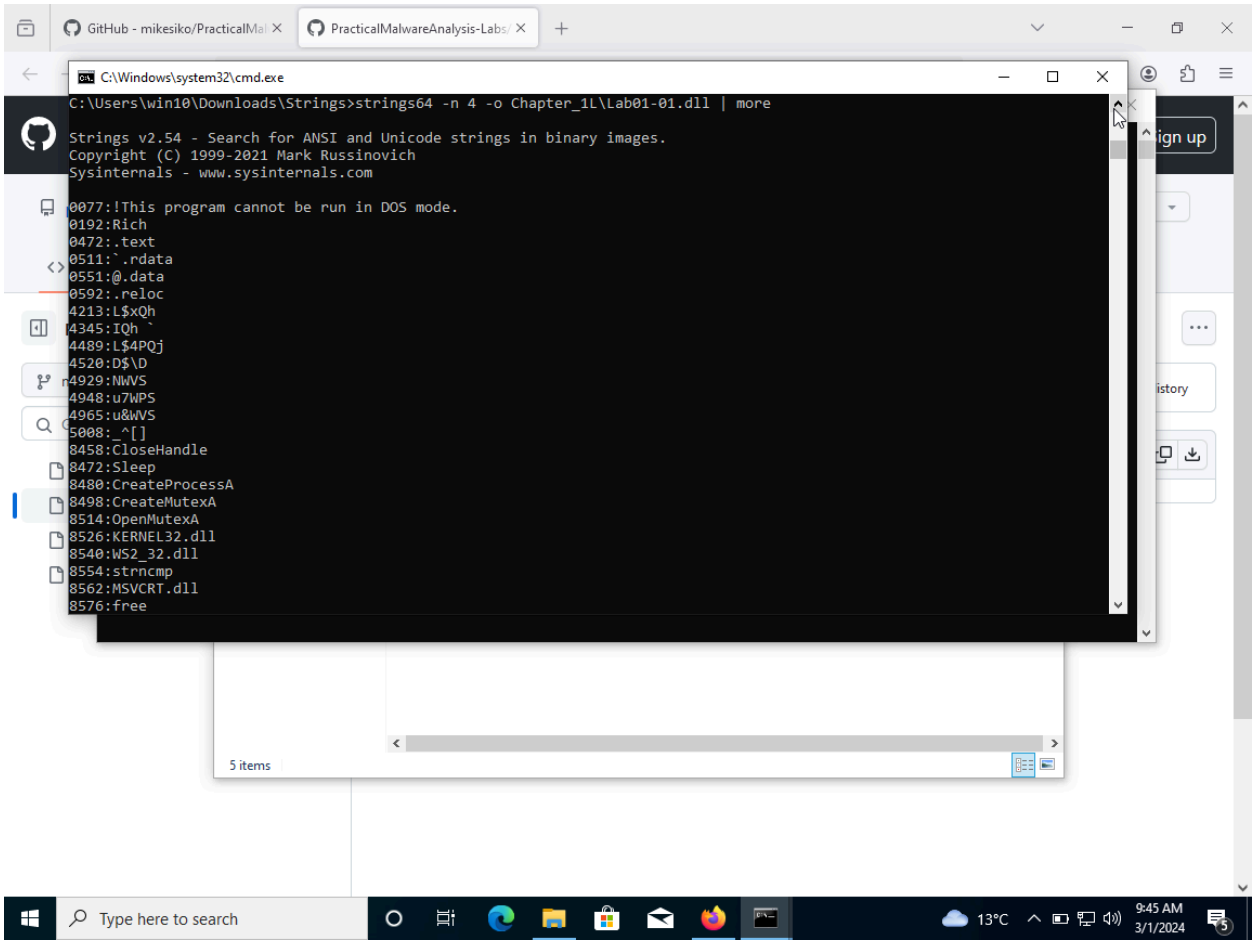
1b,


GitHub - mikesiko/PracticalMal
PracticalMalwareAnalysis-Labs/
C:\Windows\system32\cmd.exe
sleep
hello
127.26.152.13
SADFHUHF
/0I0[0h0p0
141G1[1l1
1Y2a2g2r2
3!3}3
C:\Users\win10\Downloads\Strings>
C:\Users\win10\Downloads\Strings>strings64
Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com
usage: strings64 [-a] [-f offset] [-b bytes] [-n length] [-o] [-s] [-u] <file or directory>
-a Ascii-only search (Unicode and Ascii is default)
-b Bytes of file to scan
-f File offset at which to start scanning.
-o Print offset in file string was located
-n Minimum string length (default is 3)
-s Recurse subdirectories
-u Unicode-only search (Unicode and Ascii is default)
-nobanner
Do not display the startup banner and copyright message.
C:\Users\win10\Downloads\Strings>
5 items
Type here to search
13°C
9:38 AM
3/1/2024

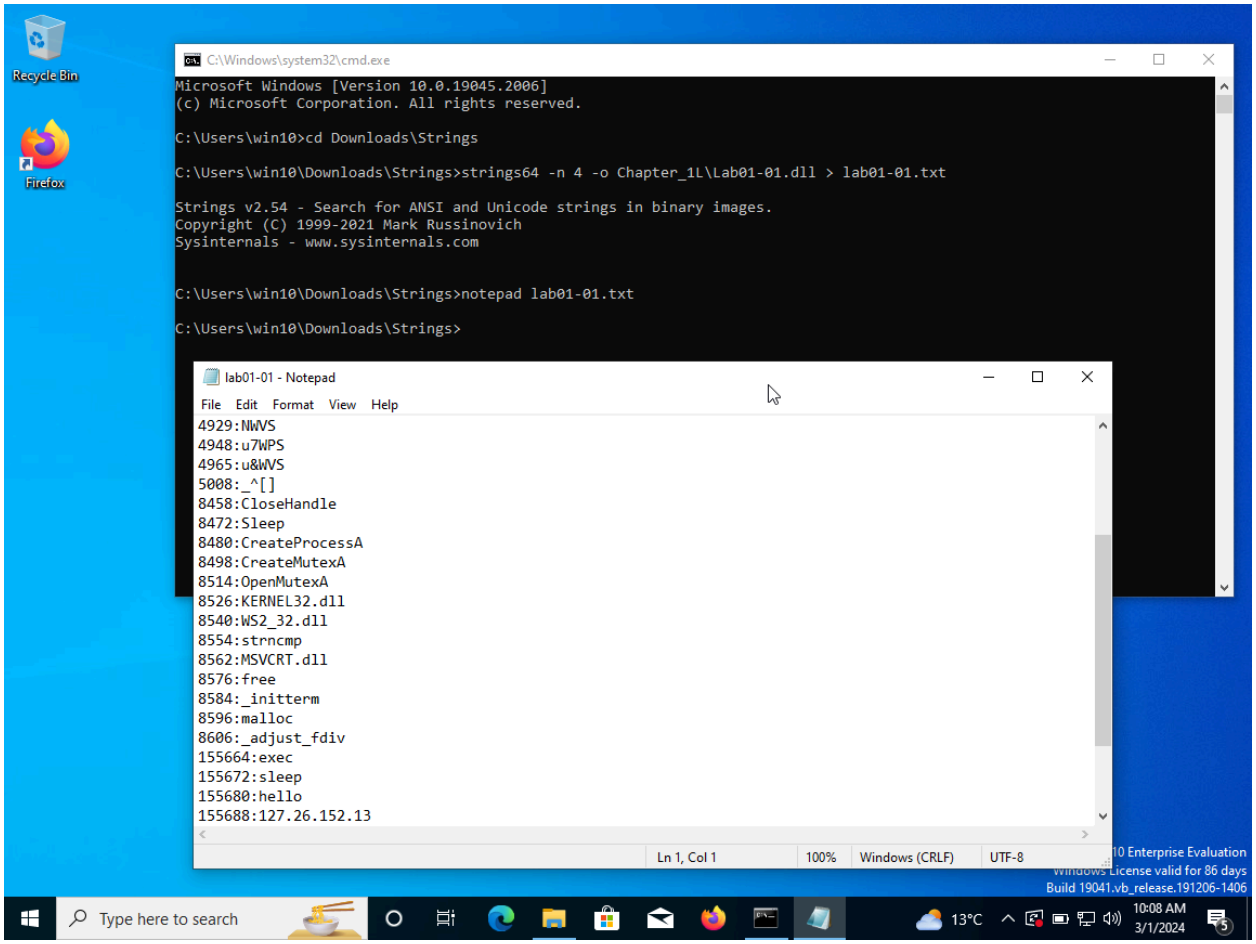
1c,


GitHub - mikesiko/PracticalMal
PracticalMalwareAnalysis-Labs/
C:\Windows\system32\cmd.exe
C:\Users\win10\Downloads\Strings>strings64 -n 4 Chapter_1L\Lab01-01.dll | more
Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.reloc
L$xQh
IQh `
L$4PQj
D$\D
NWVS
u7WPS
u&WVS
_^[]
CloseHandle
Sleep
CreateProcessA
CreateMutexA
OpenMutexA
KERNEL32.dll
WS2_32.dll
strncmp
MSVCRT.dll
5 items
Type here to search
13°C
9:38 AM
3/1/2024

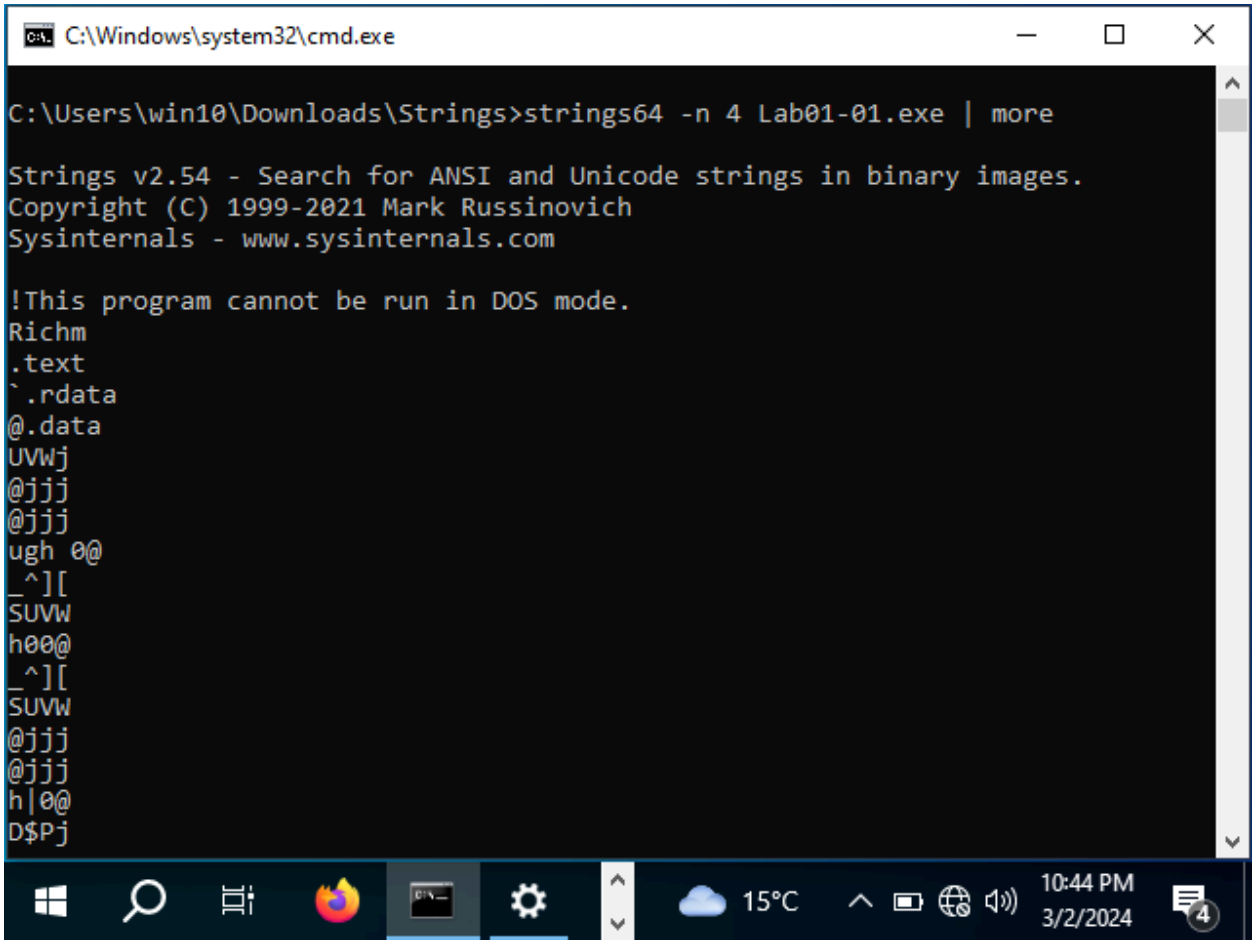
1d,


GitHub - mikesiko/PracticalMal
PracticalMalwareAnalysis-Labs/
C:\Windows\system32\cmd.exe
C:\Users\win10\Downloads\Strings>strings64 -n 4 -o Chapter_1L\Lab01-01.dll | more
Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com
0077:!This program cannot be run in DOS mode.
0192:Rich
0472:.text
0511:`.rdata
0551:@.data
0592:.reloc
4213:L$xQh
4345:IQh `
4489:L$4PQj
4520:D$\D
4929:NWVS
4948:u7WPS
4965:u&WVS
5008:_^[]
8458:CloseHandle
8472:Sleep
8480:CreateProcessA
8498:CreateMutexA
8514:OpenMutexA
8526:KERNEL32.dll
8540:WS2_32.dll
8554:strncmp
8562:MSVCRT.dll
8576:free
5 items
Type here to search
13°C
9:45 AM
3/1/2024

1e,


Recycle Bin
Firefox
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.
C:\Users\win10>cd Downloads\Strings
C:\Users\win10\Downloads\Strings>strings64 -n 4 -o Chapter_1L\Lab01-01.dll > lab01-01.txt
Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com
C:\Users\win10\Downloads\Strings>notepad lab01-01.txt
C:\Users\win10\Downloads\Strings>
lab01-01 - Notepad
File Edit Format View Help
4929:NWVS
4948:u7WPS
4965:u&WVS
5008:_^[]
8458:CloseHandle
8472:Sleep
8480:CreateProcessA
8498:CreateMutexA
8514:OpenMutexA
8526:KERNEL32.dll
8540:WS2_32.dll
8554:strncmp
8562:MSVCRT.dll
8576:free
8584:_initterm
8596:malloc
8606:_adjust_fdiv
155664:exec
155672:sleep
155680:hello
155688:127.26.152.13
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8
Type here to search
13°C
10:08 AM
3/1/2024

2a,

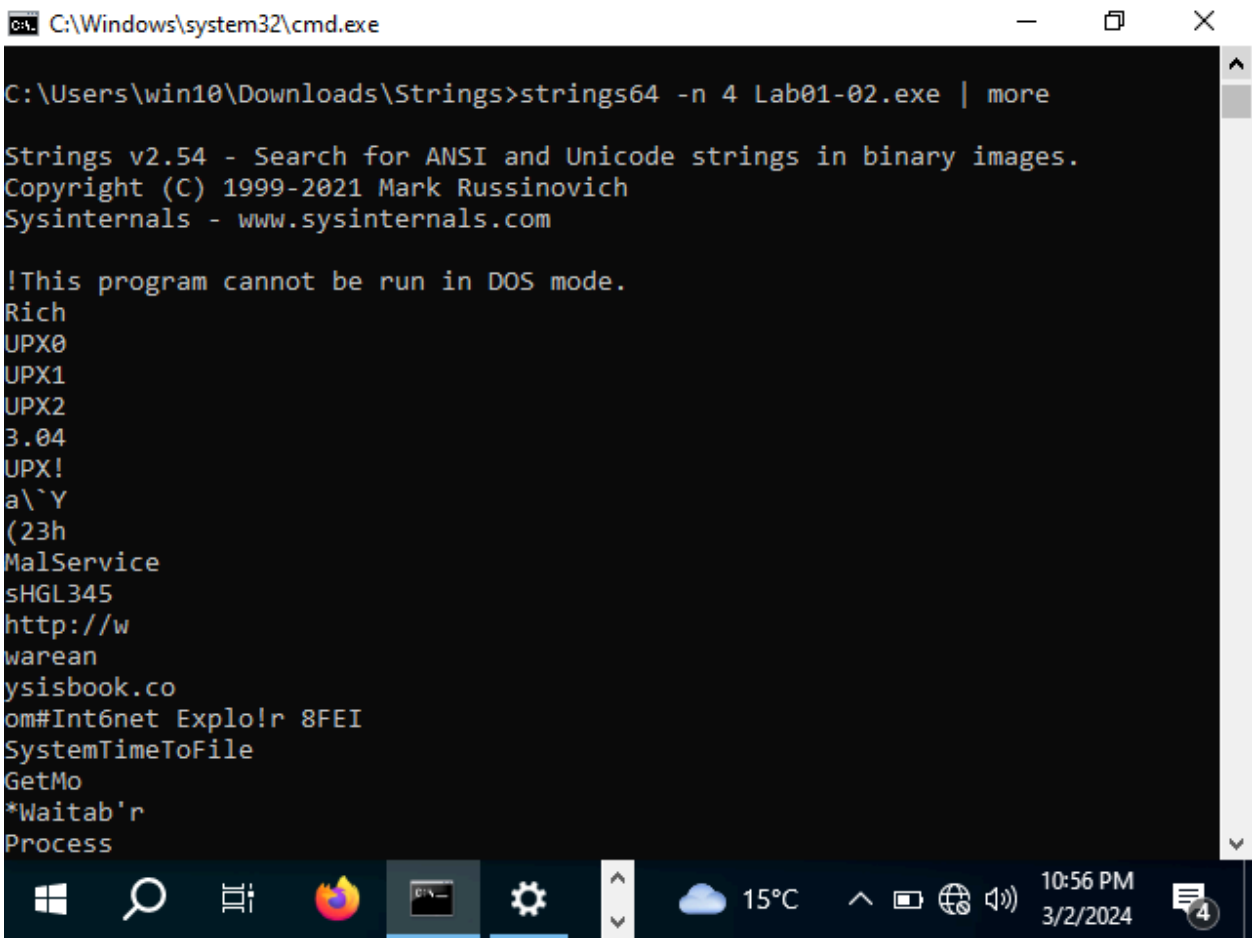


2b, các hàm mở, tìm và chỉnh sửa file là UnmapViewOfFile, MapViewOfFile, FindClose, FindNextFileA, FIndFirstFileA, CopyFIleA

2c, các xâu thể hiện loại file mà phần mềm này tìm là KERNEL32.dll và MSVCRT.dll

2d, Xâu được dùng để spoof là C:\windows\system32\kerne132.dll với số 1 thay cho ký tự l. 2 vấn đề khác trong sâu là windows và system32 viết thường. Xâu đúng mà xâu spoof đang cố gắng giả mạo là C:\Windows\System32\kernel32.dll

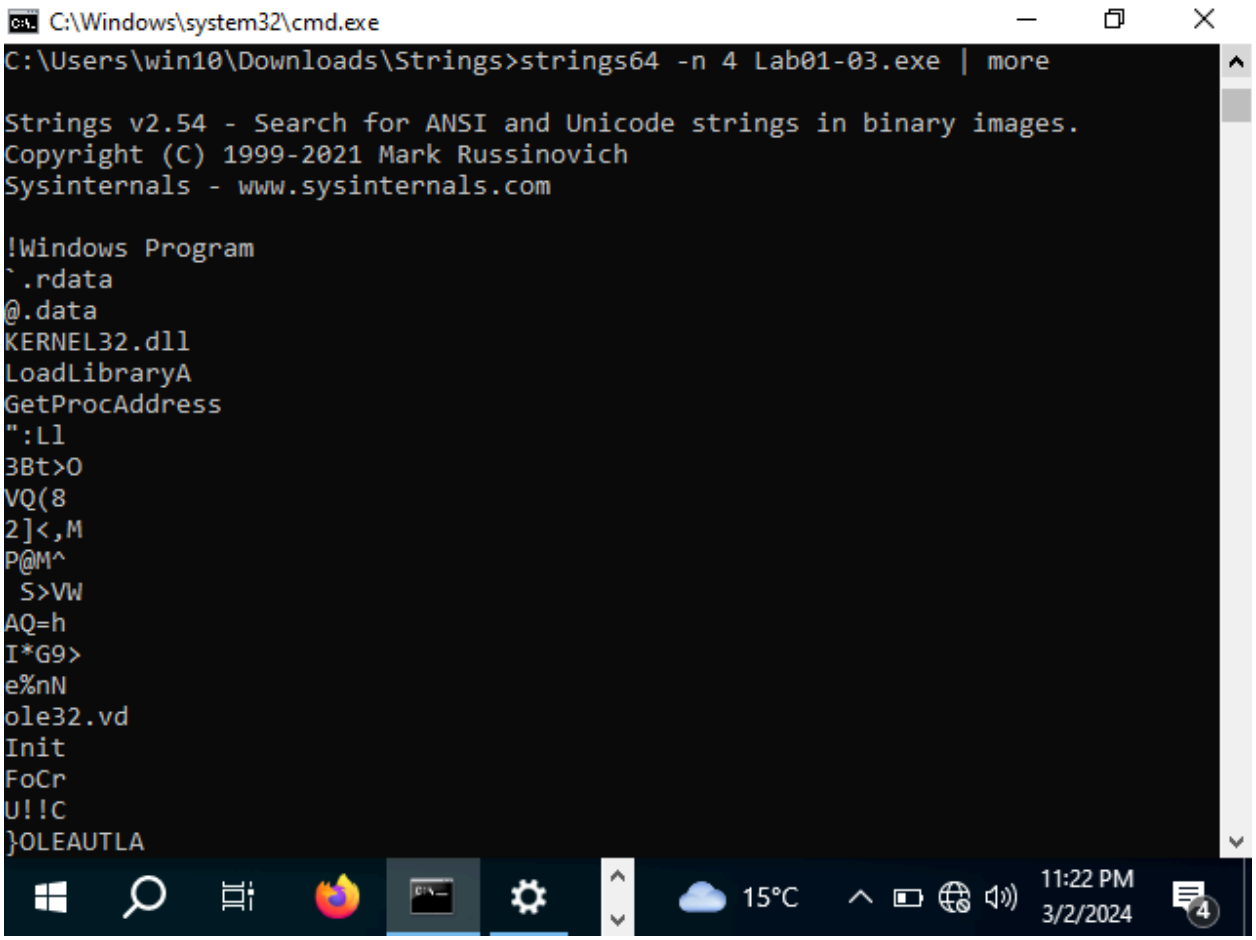
3a



3b, DLL và hàm để truy cập Internet là WININET.dll là InternetOpenA

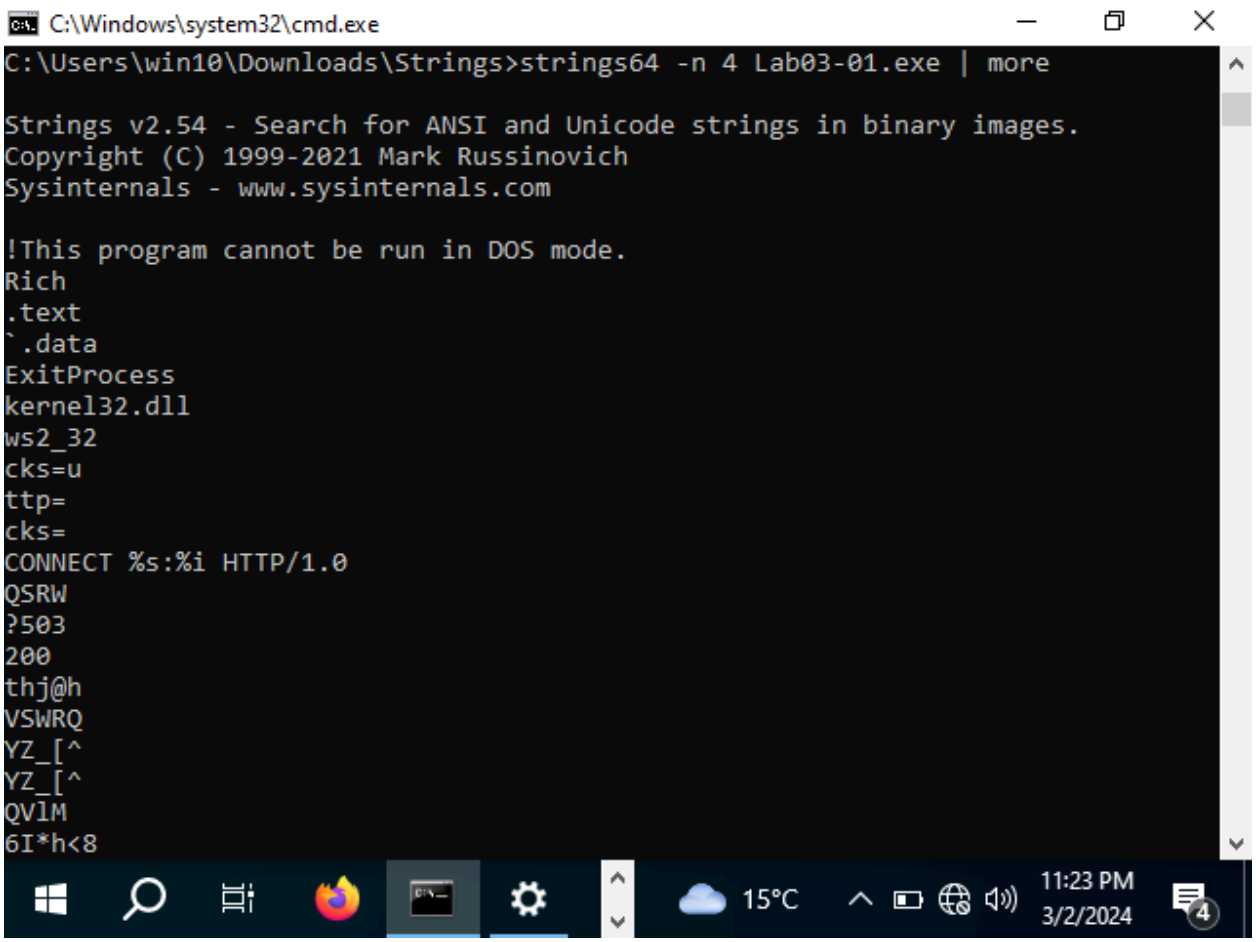
3c, UPX là phần mềm nén file executable nâng cao. UPX có thể giảm kích cỡ file từ 50 đến 70%, che dấu code mà không bị phạt trong bộ nhớ hoặc trong thời gian chạy. UPX quan trọng trong quá trình phân tích file nhị phân này vì ta có thể giải đóng gói phần mềm để hỗ trợ quá trình dịch ngược

4a,



4b, Có ít xâu có giá trị hơn các file nhị phân trước. Điều này thể hiện phần mềm này đã được đóng gói hoàn toàn.

5a,



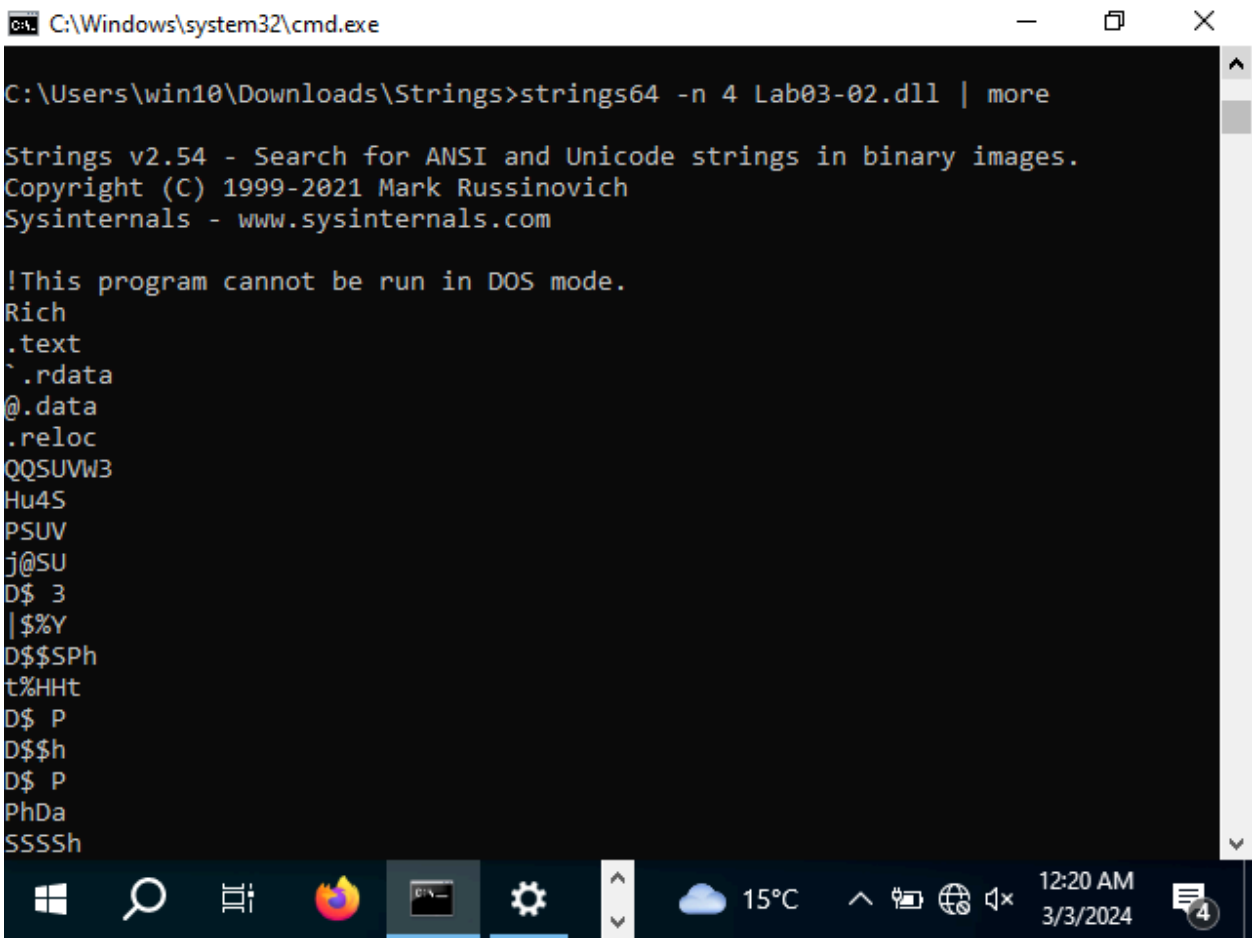
5b,Địa điểm của registry là : SOFTWARE\Microsoft\Windows\CurrentVersion\Run và SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

5c, FQDN là www.practicalmalwareanalysis.com

5d, Xâu liên quan đến video là VideoDriver

5e, Xâu có thể sử dụng làm tên người dùng mà kẻ tấn công có thể sử dụng là admin

6a,



6b, Xâu là hàm để thao túng dịch vụ là RegisterServiceCtrlHandlerA,CloseServiceHandle,CreateServiceA, DeleteService, OpenSCManagerA,DeleteService.SetServiceStatus,ServiceMain, UninstallService

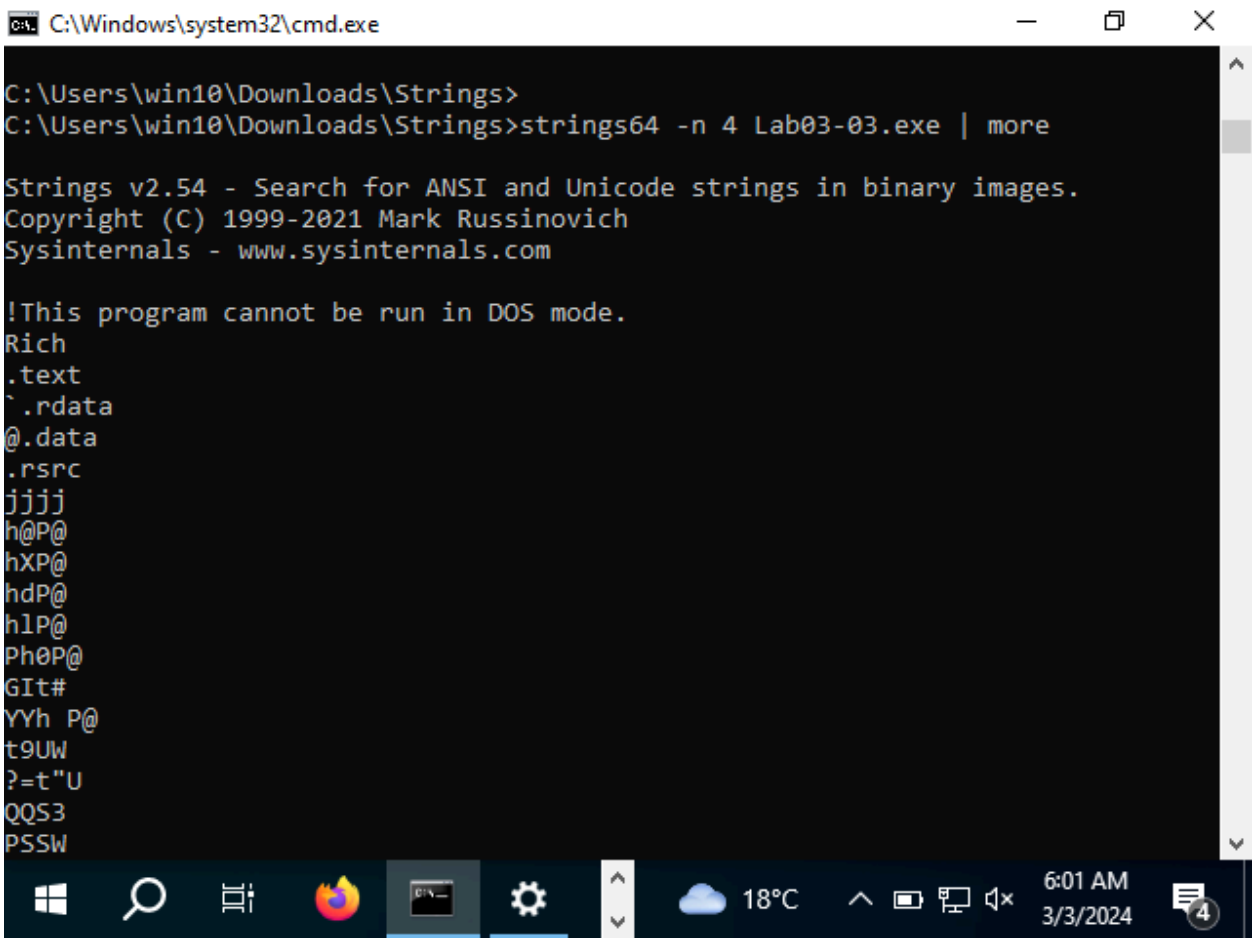
6c, Xâu để thao túng Registry là RegSetValueExA, RegCreateKeyA, RegCloseKey, RegQueryValueExA,RegOpenKeyExA,

6d, Xâu liên quan đến hàm thao tác với mạng là InternetReadFIle, HttpQueryInfoA, HttpSendRequestA, HttpOpenRequestA, Int như nhiernetConnectA, InternetOpenA,InternetCloseHandle

6e, Tùy chọn được sử dụng trong xâu chứa cmd là /c. Nó đáng nghi vì lựa chọn này cho phép ta thực hiện xâu sau lựa chọn này rồi hủy cmd, khiến cho cmd thực hiện các thao tác được mã độc đề ra rồi hủy cmd để che dấu vết.

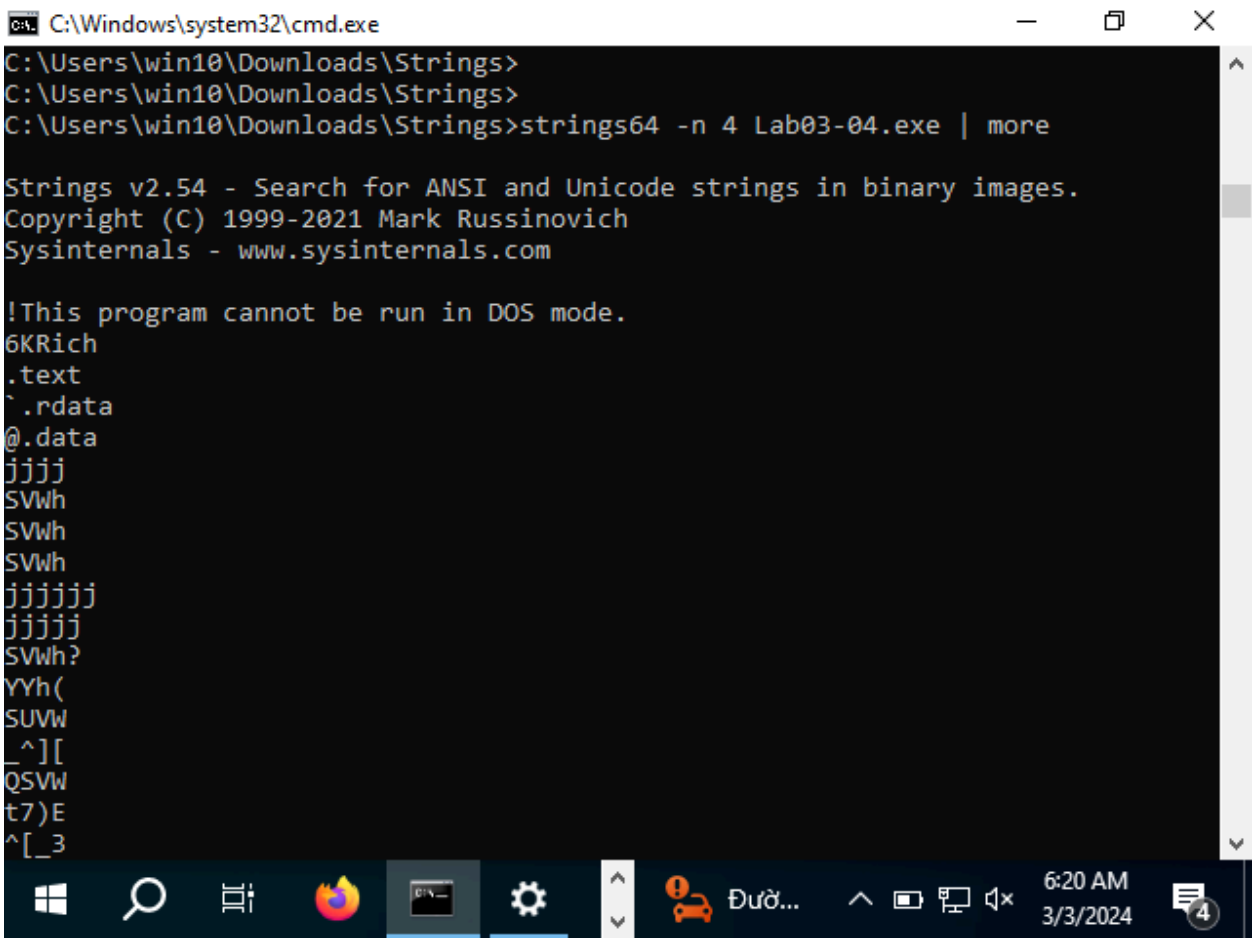
6f, Xâu có chữ cái viết hoa, viết thường, số và 1 vài ký tự là “ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/”, nó đáng nghi vì nó là tất cả các ký tự trong chuỗi Base64, từ đó ta có thể đoán kẻ tấn công sử dụng Base64 để che dấu thông tin trong mã độc mình.

7a,



7b,Chương trình có báo lỗi là không thể khởi tạo heap cũng như nhiều chức năng cơ bản của hệ điều hành gặp lỗi để rồi Microsoft Visual C++ Runtime Library gặp lỗi Runtime. Thêm nữa trong phần báo lỗi thì ta có thể thấy input có chứa nhiều xâu gồm nhiều chữ A được lặp lại, từ đó ta có thể đoán là chương trình này muốn làm tràn heap để thực hiện các chương trình được đóng gói ở sau các xâu A.

8a,



8b, Xâu cho thấy tùy chọn cmd là /c

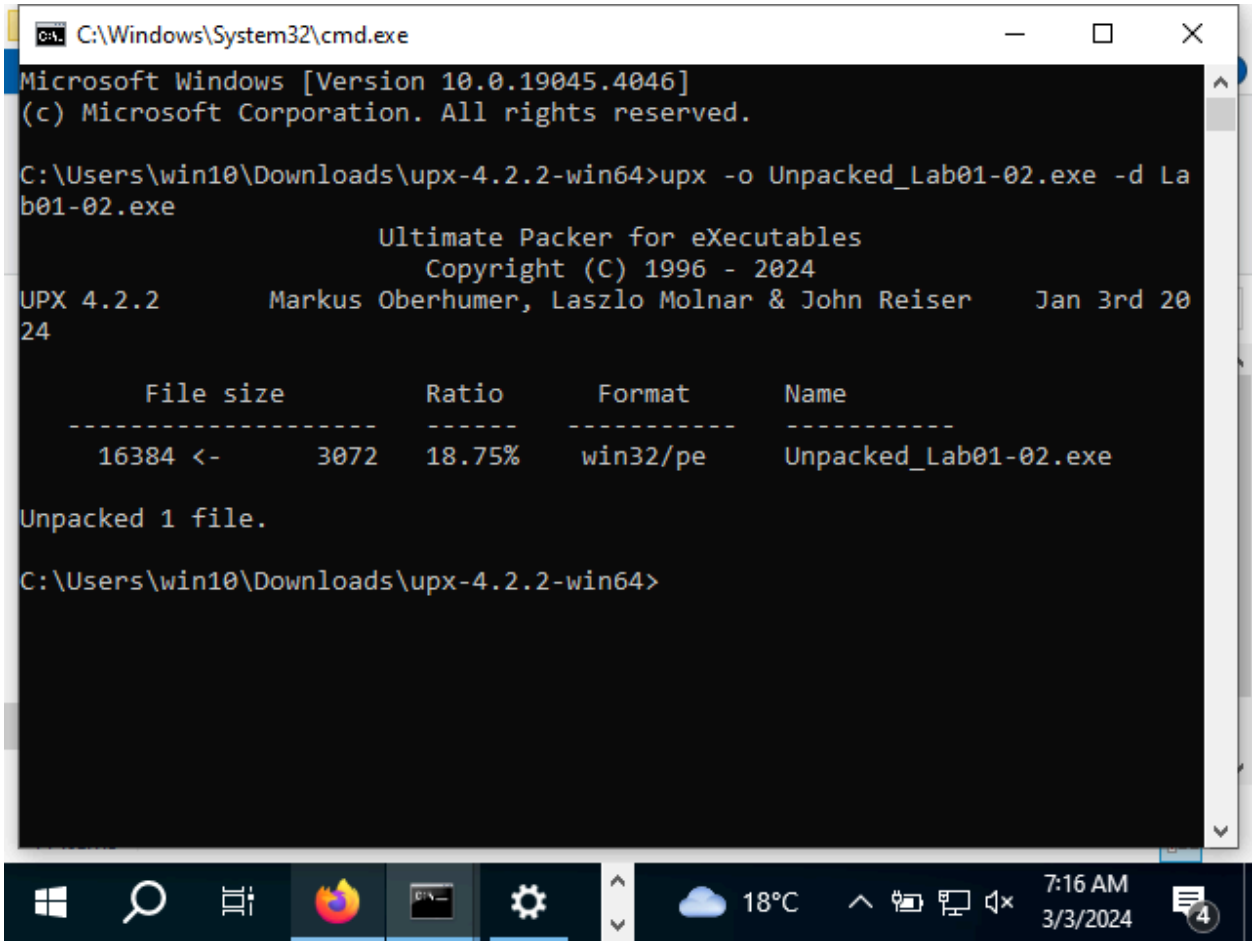
8c, Xâu cho thấy chương trình sẽ xóa một cái gì đó là cmd.exe /c del

8d, Xâu kìm hãm đầu ra là >> NULL

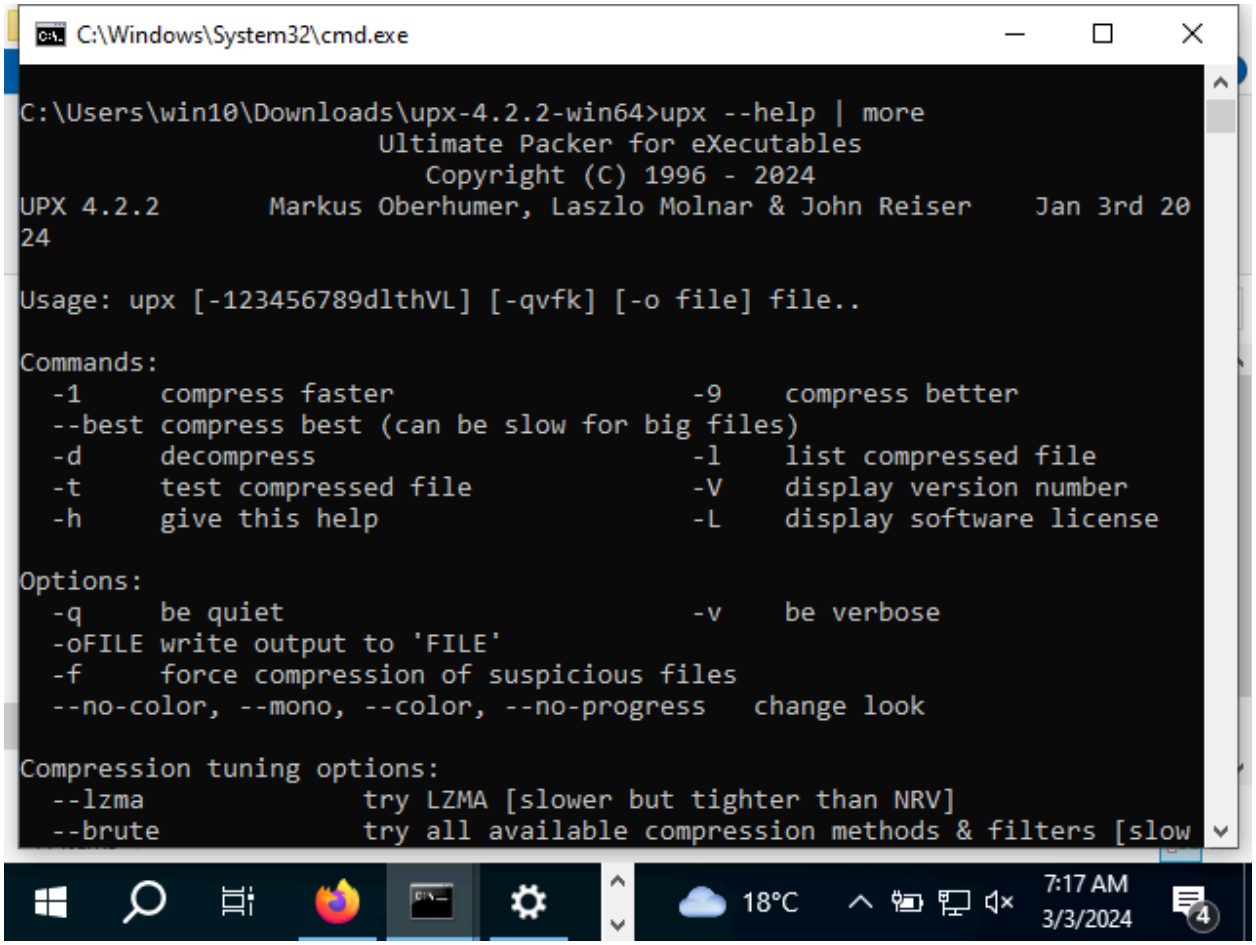
8e, Xâu thể hiện các lựa chọn menu kẻ tấn công có thể chọn là NOTHING, DOWNLOAD ,UPLOAD, SLEEP

Lab 15.02

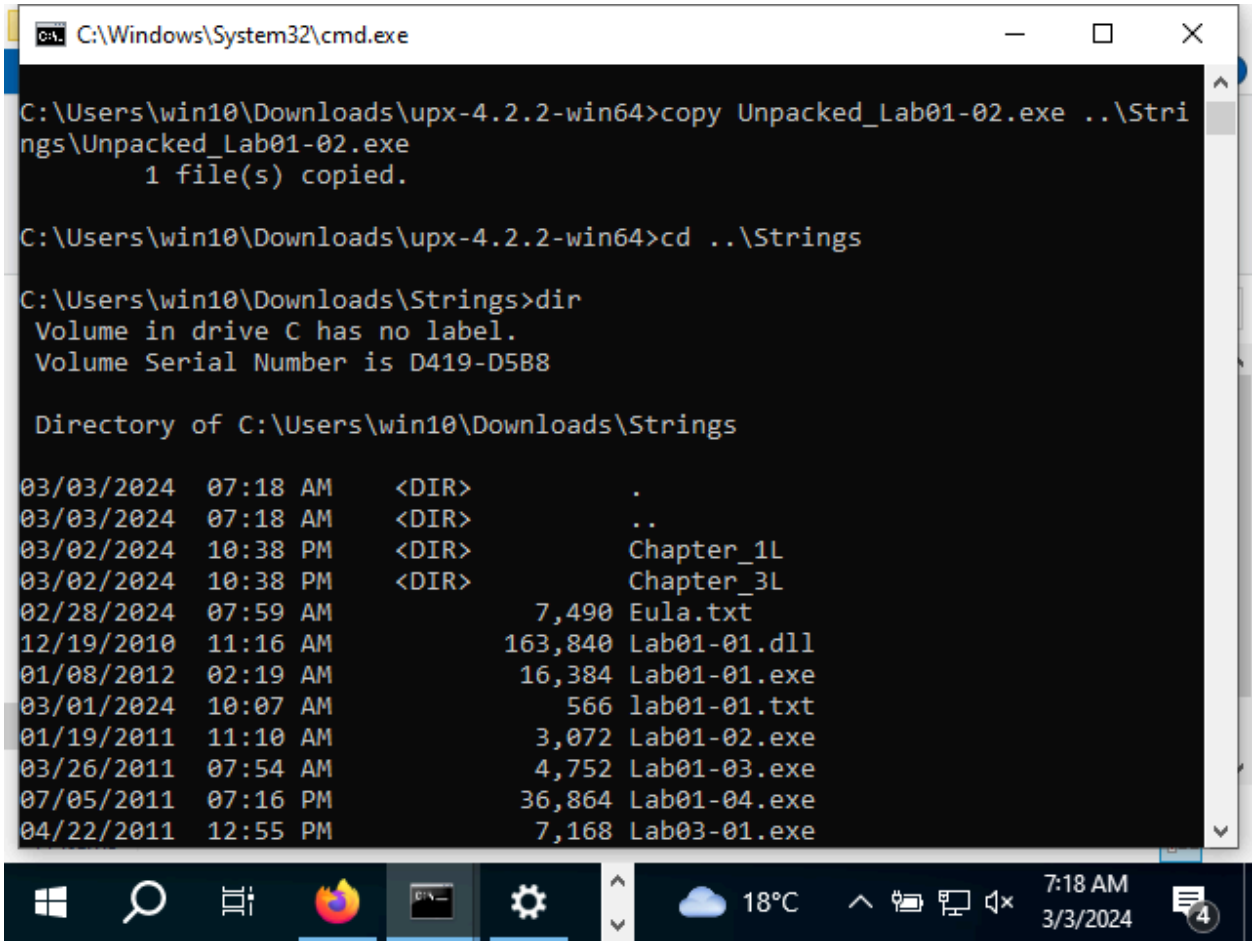
1a,


C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.4046]
(c) Microsoft Corporation. All rights reserved.
C:\Users\win10\Downloads\upx-4.2.2-win64>upx -o Unpacked_Lab01-02.exe -d Lab01-02.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2024
UPX 4.2.2 Markus Oberhumer, Laszlo Molnar & John Reiser Jan 3rd 2024
File size Ratio Format Name
16384 <- 3072 18.75% win32/pe Unpacked_Lab01-02.exe
Unpacked 1 file.
C:\Users\win10\Downloads\upx-4.2.2-win64>
18°C
7:16 AM
3/3/2024

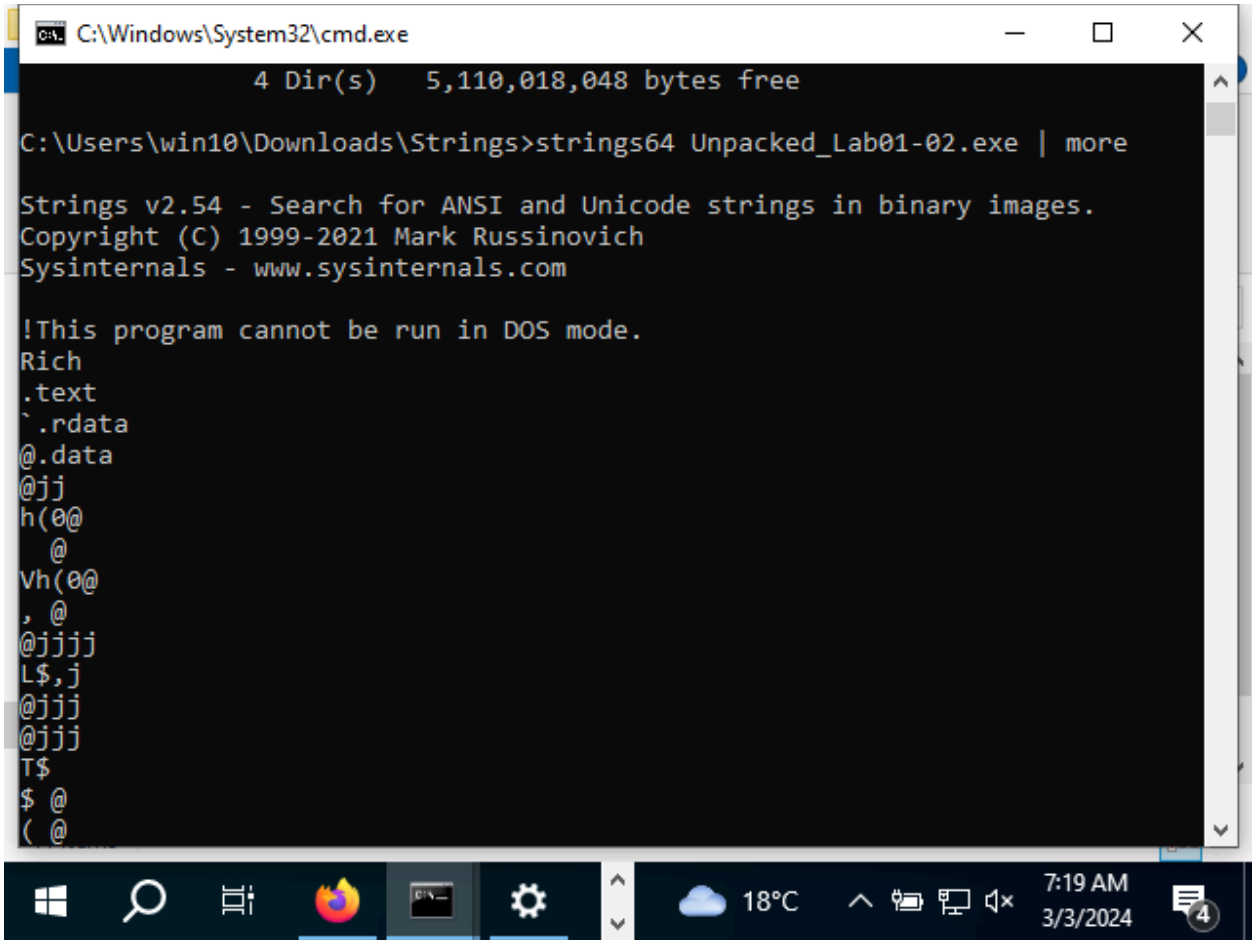
1b,


C:\Windows\System32\cmd.exe
C:\Users\win10\Downloads\upx-4.2.2-win64>upx --help | more
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2024
UPX 4.2.2 Markus Oberhumer, Laszlo Molnar & John Reiser Jan 3rd 20
24
Usage: upx [-123456789dlthVL] [-qvfk] [-o file] file..
Commands:
-1 compress faster -9 compress better
--best compress best (can be slow for big files)
-d decompress -l list compressed file
-t test compressed file -V display version number
-h give this help -L display software license
Options:
-q be quiet -v be verbose
-oFILE write output to 'FILE'
-f force compression of suspicious files
--no-color, --mono, --color, --no-progress change look
Compression tuning options:
--lzma try LZMA [slower but tighter than NRV]
--brute try all available compression methods & filters [slow
18°C
7:17 AM
3/3/2024

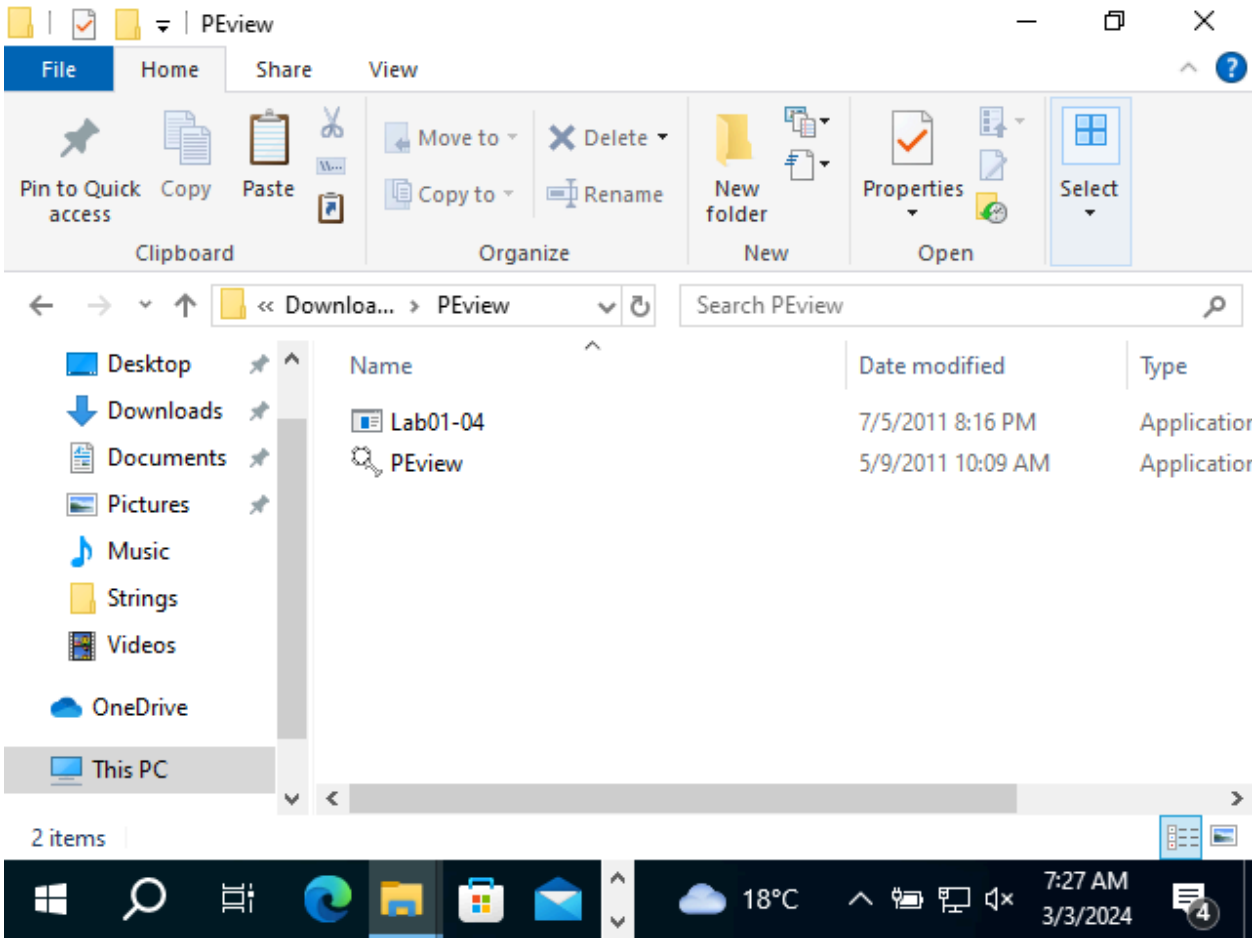
1c,


C:\Windows\System32\cmd.exe
C:\Users\win10\Downloads\upx-4.2.2-win64>copy Unpacked_Lab01-02.exe ..\Strings\Unpacked_Lab01-02.exe
1 file(s) copied.
C:\Users\win10\Downloads\upx-4.2.2-win64>cd ..\Strings
C:\Users\win10\Downloads\Strings>dir
Volume in drive C has no label.
Volume Serial Number is D419-D5B8
Directory of C:\Users\win10\Downloads\Strings
03/03/2024 07:18 AM <DIR> .
03/03/2024 07:18 AM <DIR> ..
03/02/2024 10:38 PM <DIR> Chapter_1L
03/02/2024 10:38 PM <DIR> Chapter_3L
02/28/2024 07:59 AM 7,490 Eula.txt
12/19/2010 11:16 AM 163,840 Lab01-01.dll
01/08/2012 02:19 AM 16,384 Lab01-01.exe
03/01/2024 10:07 AM 566 lab01-01.txt
01/19/2011 11:10 AM 3,072 Lab01-02.exe
03/26/2011 07:54 AM 4,752 Lab01-03.exe
07/05/2011 07:16 PM 36,864 Lab01-04.exe
04/22/2011 12:55 PM 7,168 Lab03-01.exe
18°C
7:18 AM
3/3/2024

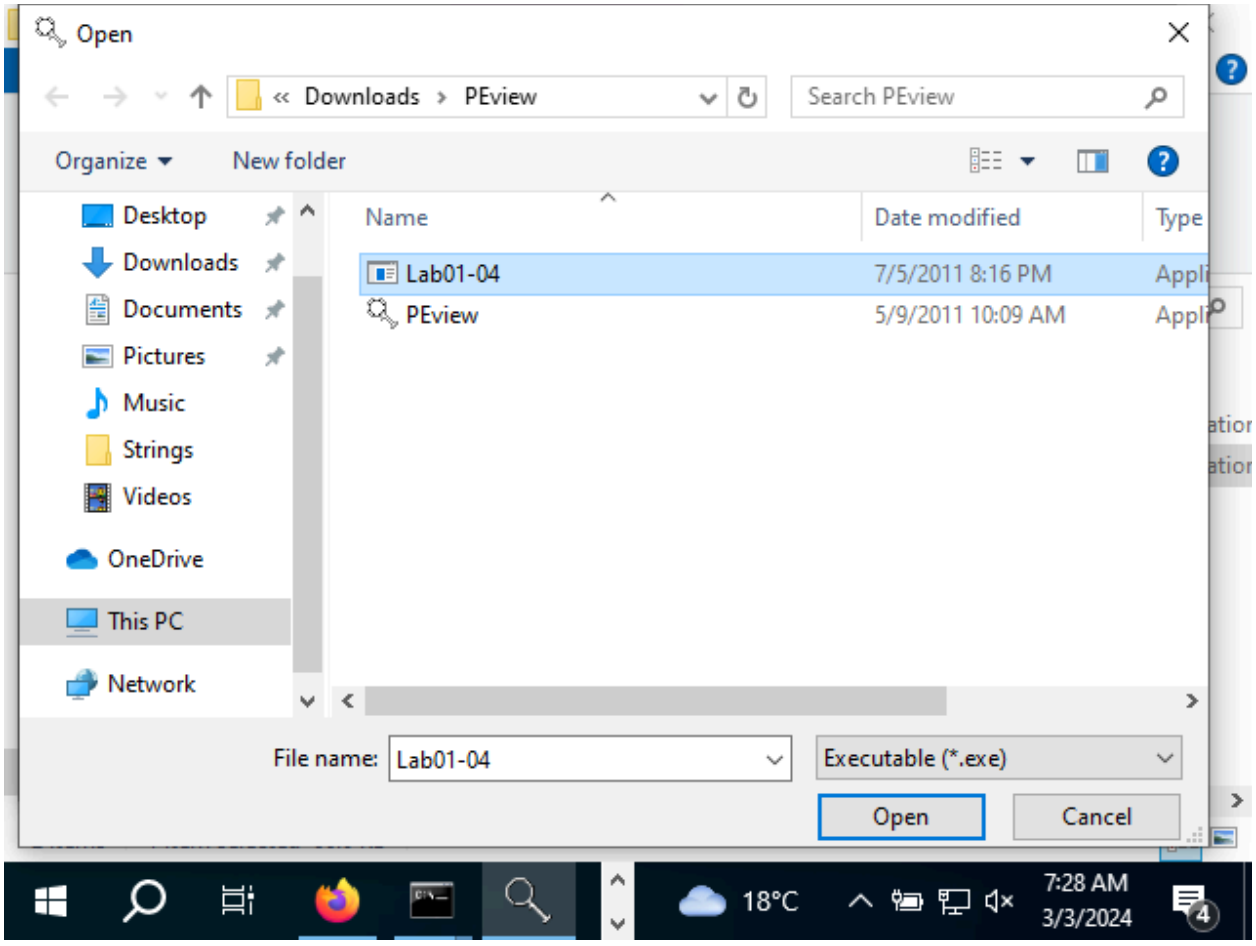
2a,

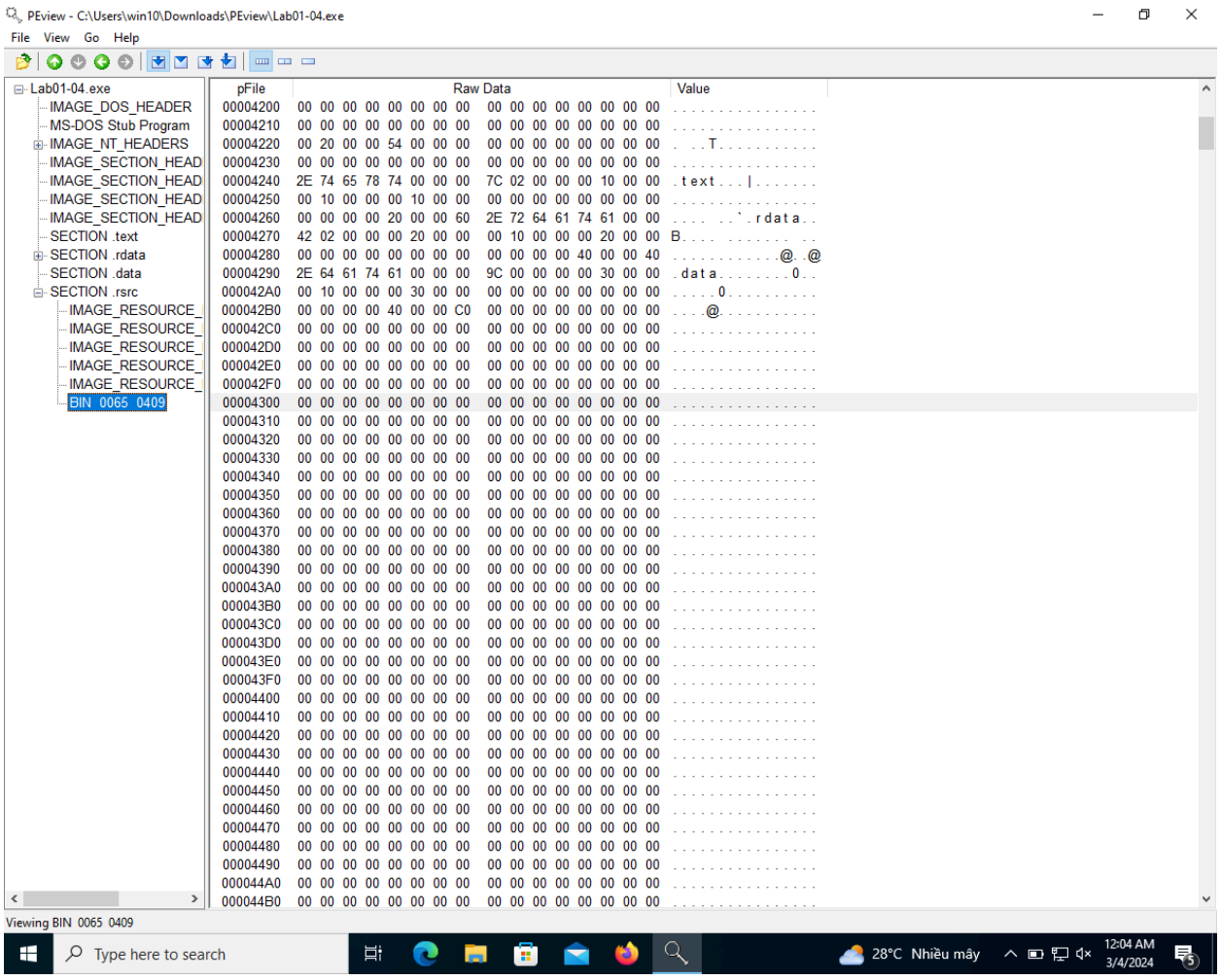


2b,URL hiện lên là http://www.malwareanalysisbook.com
2c, Một số hàm liên quan đến URL là InternetOpenUrlA và InternetOpenA
2d, DLL mà các hàm này đến từ WININET.dll
Lab 15.03
1a,

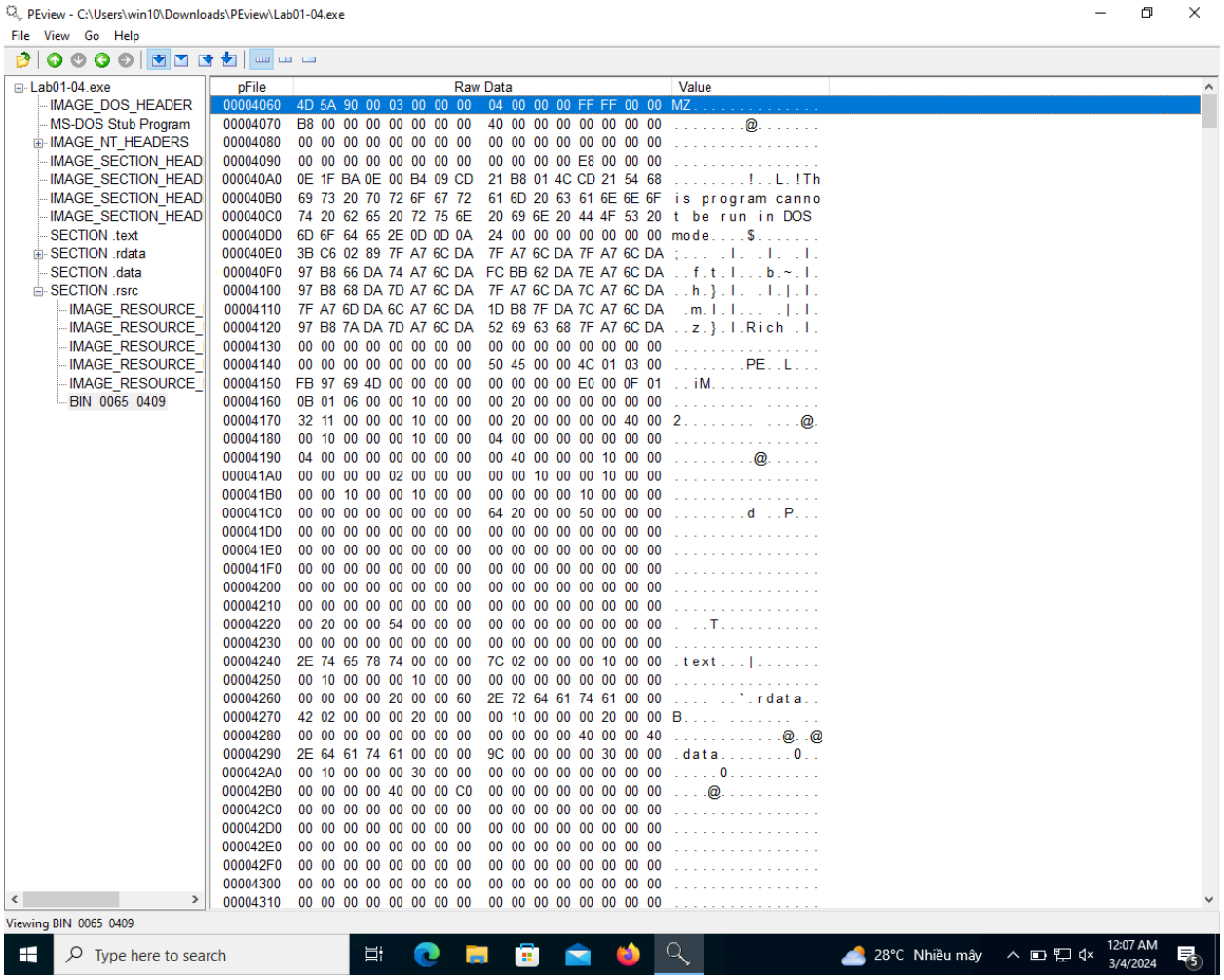

PEview
File
Home
Share
View
Pin to Quick access
Copy
Paste
Clipboard
Move to
Delete
Copy to
Rename
Organize
New folder
New
Properties
Open
Select
« Downloa... › PEview
Search PEview
Desktop
Downloads
Documents
Pictures
Music
Strings
Videos
OneDrive
This PC
Name
Date modified
Type
Lab01-04
7/5/2011 8:16 PM
Application
PEview
5/9/2011 10:09 AM
Application
2 items
18°C
7:27 AM
3/3/2024

1b & c,

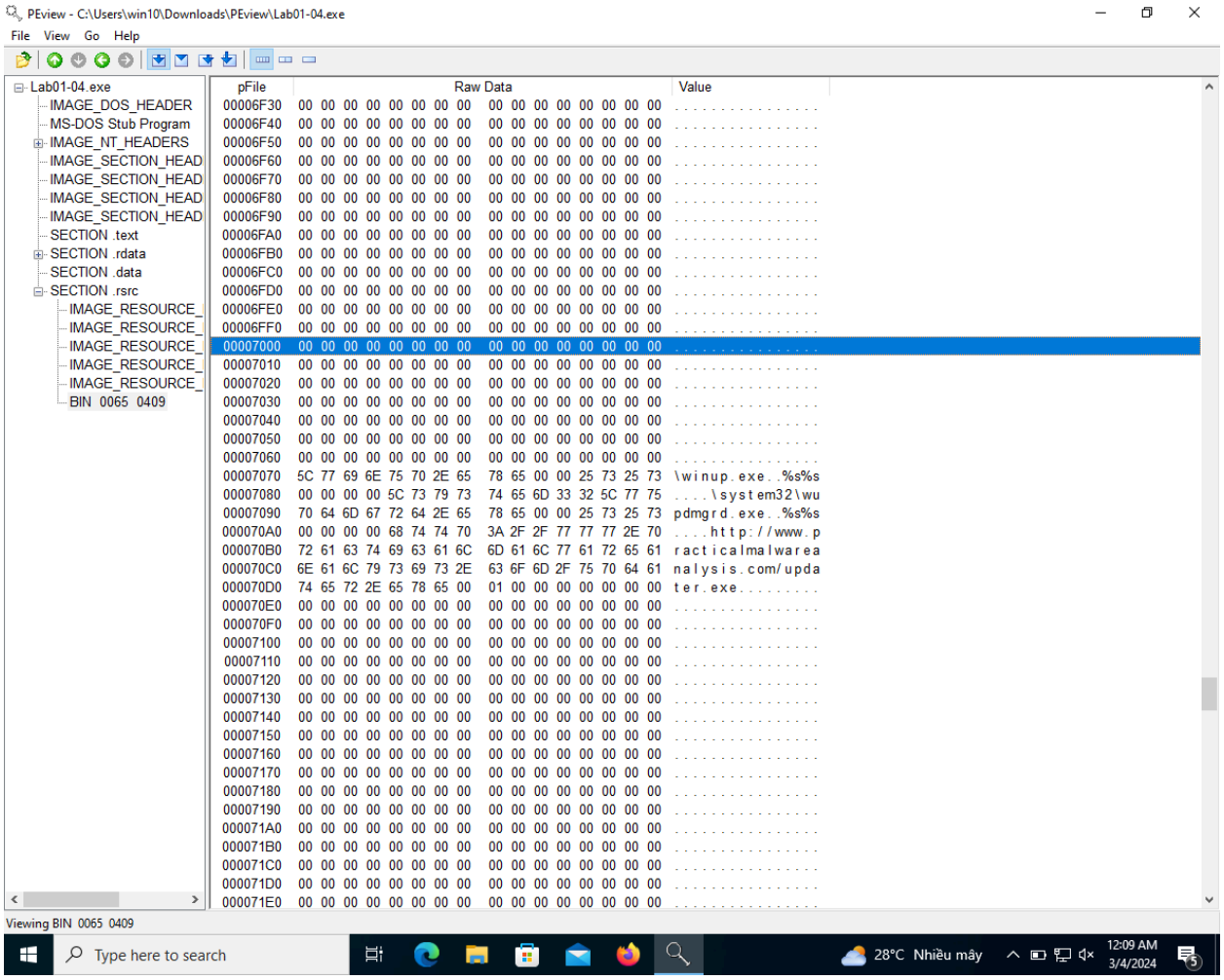

Open
« Downloads › PEview
Search PEview
Organize
New folder
Desktop
Downloads
Documents
Pictures
Music
Strings
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Lab01-04
7/5/2011 8:16 PM
PEview
5/9/2011 10:09 AM
File name:
Lab01-04
Executable (*.exe)
Open
Cancel
18°C
7:28 AM
3/3/2024


PEview - C:\Users\win10\Downloads\PEview\Lab01-04.exe
File View Go Help
Lab01-04.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEAD
IMAGE_SECTION_HEAD
IMAGE_SECTION_HEAD
IMAGE_SECTION_HEAD
SECTION .text
SECTION .rdata
SECTION .data
SECTION .rsrc
IMAGE_RESOURCE_
IMAGE_RESOURCE_
IMAGE_RESOURCE_
IMAGE_RESOURCE_
IMAGE_RESOURCE_
BIN 0065 0409
pFile
Raw Data
Value
00004200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004220 00 20 00 00 54 00 00 00 00 00 00 00 00 00 00 00 ...T...
00004230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004240 2E 74 65 78 74 00 00 00 7C 02 00 00 00 10 00 00 .text...|.....
00004250 00 10 00 00 00 10 00 00 00 00 00 00 00 00 00 00
00004260 00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00 .... ..`.rdata..
00004270 42 02 00 00 00 20 00 00 00 10 00 00 00 20 00 00 B.... ....
00004280 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 ....@..@
00004290 2E 64 61 74 61 00 00 00 9C 00 00 00 00 30 00 00 .data.....0..
000042A0 00 10 00 00 00 30 00 00 00 00 00 00 00 00 00 00 .....0..........
000042B0 00 00 00 00 40 00 00 C0 00 00 00 00 00 00 00 00 ....@...........
000042C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000042D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000042E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000042F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004330 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004340 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004350 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004370 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004380 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004390 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000043A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000043B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000043C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000043D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000043E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000043F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004410 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004420 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004430 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004440 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004450 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004460 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004470 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004480 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004490 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000044A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000044B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Viewing BIN 0065 0409
Type here to search
28°C Nhiều mây
12:04 AM
3/4/2024

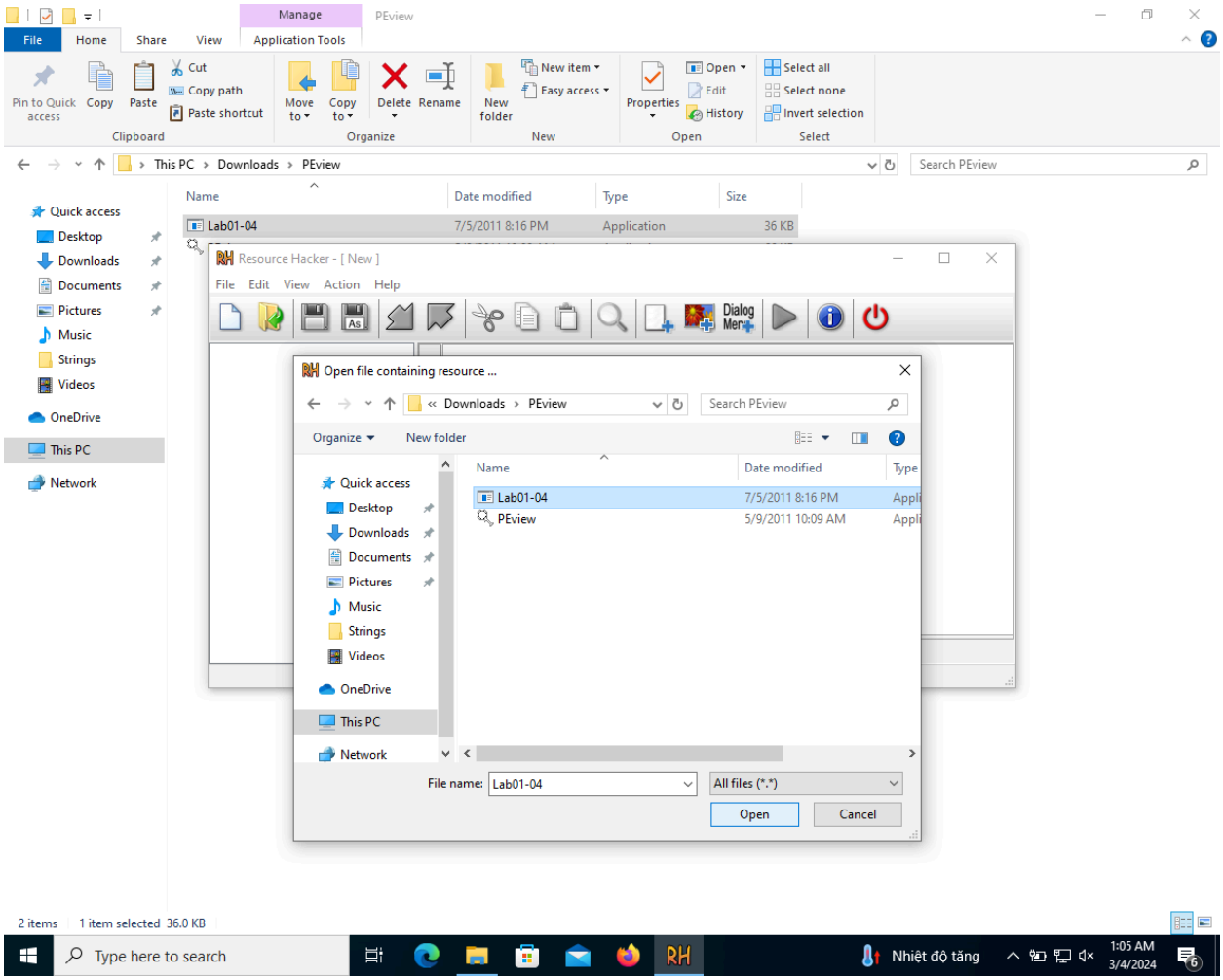
1e,


PEview - C:\Users\win10\Downloads\PEview\Lab01-04.exe
File View Go Help
Lab01-04.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEAD
IMAGE_SECTION_HEAD
IMAGE_SECTION_HEAD
IMAGE_SECTION_HEAD
SECTION .text
SECTION .rdata
SECTION .data
SECTION .rsrc
IMAGE_RESOURCE_
IMAGE_RESOURCE_
IMAGE_RESOURCE_
IMAGE_RESOURCE_
IMAGE_RESOURCE_
BIN 0065 0409
pFile Raw Data Value
00004060 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ
00004070 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 @
00004080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004090 00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00
000040A0 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 !..L.!Th
000040B0 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
000040C0 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
000040D0 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$
000040E0 3B C6 02 89 7F A7 6C DA 7F A7 6C DA 7F A7 6C DA ;....l...l...l.
000040F0 97 B8 66 DA 74 A7 6C DA FC BB 62 DA 7E A7 6C DA ..f.t.l...b.~.l.
00004100 97 B8 68 DA 7D A7 6C DA 7F A7 6C DA 7C A7 6C DA ..h.}.l...l.|.l.
00004110 7F A7 6D DA 6C A7 6C DA 1D B8 7F DA 7C A7 6C DA ..m.l.l.....|.l.
00004120 97 B8 7A DA 7D A7 6C DA 52 69 63 68 7F A7 6C DA ..z.}.l.Rich..l.
00004130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004140 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 03 00 ........PE..L...
00004150 FB 97 69 4D 00 00 00 00 00 00 00 00 E0 00 0F 01 ..iM
00004160 0B 01 06 00 00 10 00 00 00 20 00 00 00 00 00 00
00004170 32 11 00 00 00 10 00 00 00 20 00 00 00 00 40 00 2.... ....@.
00004180 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00
00004190 04 00 00 00 00 00 00 00 00 40 00 00 00 10 00 00 .....@
000041A0 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00
000041B0 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00
000041C0 00 00 00 00 00 00 00 00 64 20 00 00 50 00 00 00 ....d ..P...
000041D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000041E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000041F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004220 00 20 00 00 54 00 00 00 00 00 00 00 00 00 00 00 ...T
00004230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004240 2E 74 65 78 74 00 00 00 7C 02 00 00 00 10 00 00 .text...|.....
00004250 00 10 00 00 00 10 00 00 00 00 00 00 00 00 00 00
00004260 00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00 .... ..`.rdata..
00004270 42 02 00 00 00 20 00 00 00 10 00 00 00 20 00 00 B.... .....
00004280 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 ....@..@
00004290 2E 64 61 74 61 00 00 00 9C 00 00 00 00 30 00 00 .data.....0..
000042A0 00 10 00 00 00 30 00 00 00 00 00 00 00 00 00 00 0
000042B0 00 00 00 00 40 00 00 C0 00 00 00 00 00 00 00 00 ....@
000042C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000042D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000042E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000042F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Viewing BIN 0065 0409
Type here to search
28°C Nhiều mây
12:07 AM
3/4/2024

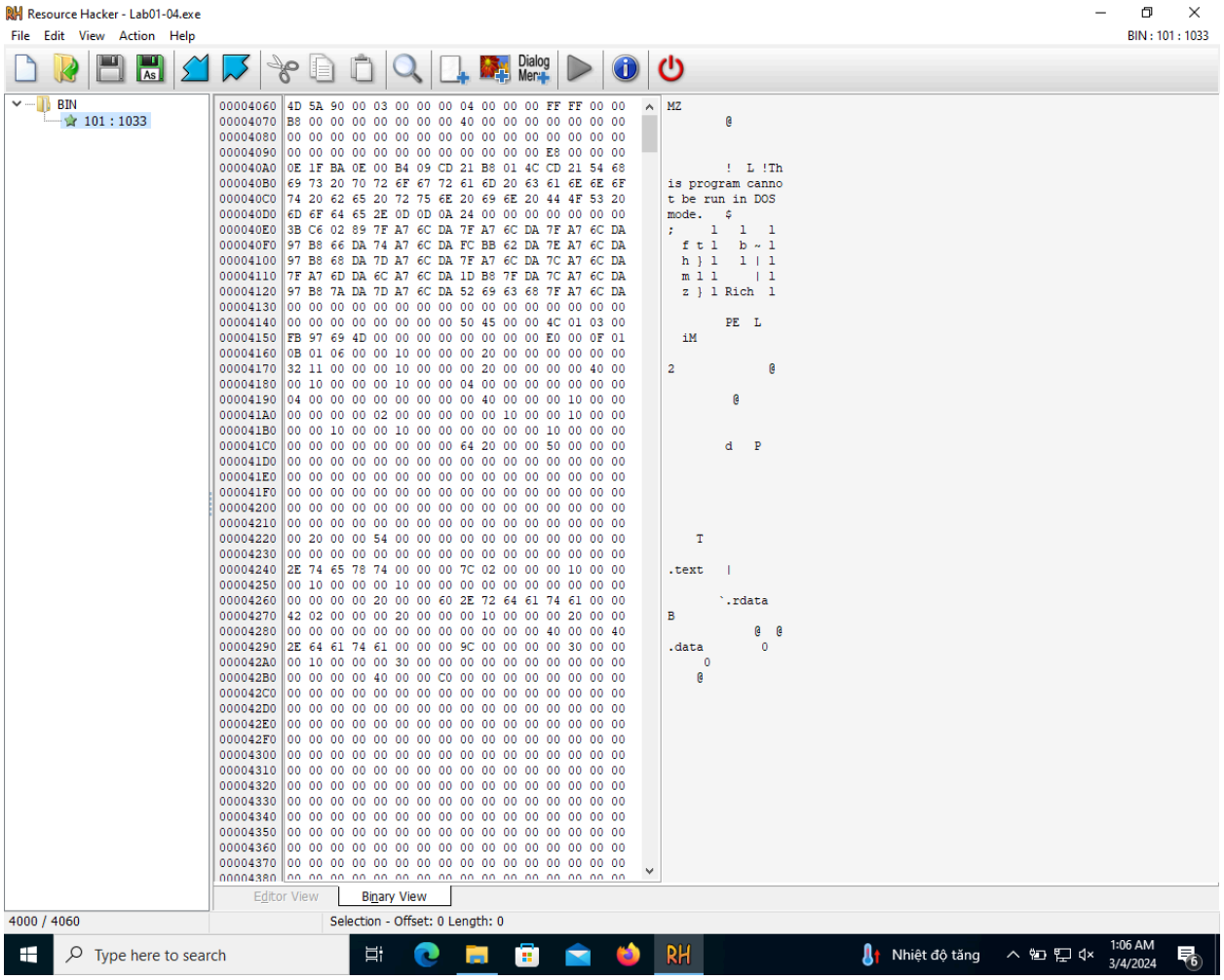
1f,


PEview - C:\Users\win10\Downloads\PEview\Lab01-04.exe
File View Go Help
Lab01-04.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEAD
IMAGE_SECTION_HEAD
IMAGE_SECTION_HEAD
IMAGE_SECTION_HEAD
SECTION .text
SECTION .rdata
SECTION .data
SECTION .rsrc
IMAGE_RESOURCE_
IMAGE_RESOURCE_
IMAGE_RESOURCE_
IMAGE_RESOURCE_
IMAGE_RESOURCE_
BIN 0065 0409
pFile
Raw Data
Value
00006F30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00006F40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00006F50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00006F60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00006F70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00006F80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00006F90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00006FA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00006FB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00006FC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00006FD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00006FE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00006FF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007070 5C 77 69 6E 75 70 2E 65 78 65 00 00 25 73 25 73 \winup.exe..%s%s
00007080 00 00 00 00 5C 73 79 73 74 65 6D 33 32 5C 77 75 ....\system32\wu
00007090 70 64 6D 67 72 64 2E 65 78 65 00 00 25 73 25 73 pdmgrd.exe..%s%s
000070A0 00 00 00 00 68 74 74 70 3A 2F 2F 77 77 77 2E 70 ....http://www.p
000070B0 72 61 63 74 69 63 61 6C 6D 61 6C 77 61 72 65 61 racticalmalwarea
000070C0 6E 61 6C 79 73 69 73 2E 63 6F 6D 2F 75 70 64 61 nalysis.com/upda
000070D0 74 65 72 2E 65 78 65 00 01 00 00 00 00 00 00 00 ter.exe.........
000070E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
000070F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
00007190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
000071A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
000071B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
000071C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
000071D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
000071E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . . .
Viewing BIN 0065 0409
Type here to search
28°C Nhiều mây
12:09 AM
3/4/2024

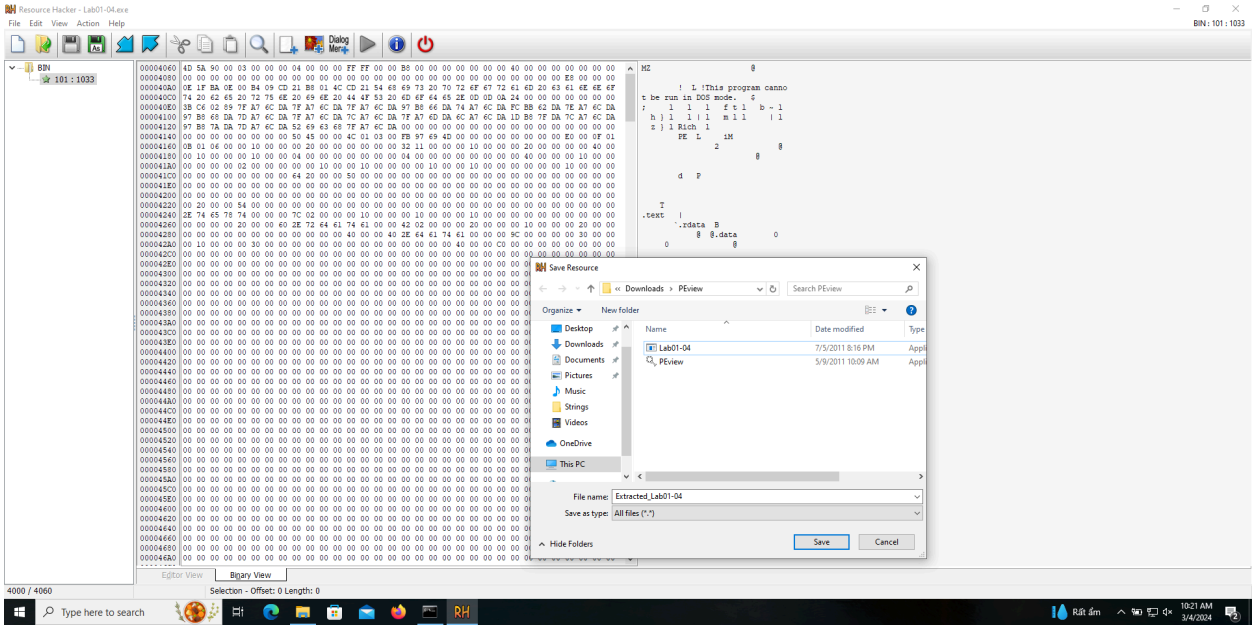
2a&b,


Manage
PEview
File
Home
Share
View
Application Tools
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › Downloads › PEview
Search PEview
Quick access
Desktop
Downloads
Documents
Pictures
Music
Strings
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Lab01-04
7/5/2011 8:16 PM
Application
36 KB
Resource Hacker - [New]
File Edit View Action Help
Open file containing resource ...
Downloads › PEview
Search PEview
Organize
New folder
Lab01-04
7/5/2011 8:16 PM
PEview
5/9/2011 10:09 AM
File name: Lab01-04
All files (*.*)
Open
Cancel
2 items
1 item selected 36.0 KB
Type here to search
Nhiệt độ tăng
1:05 AM
3/4/2024

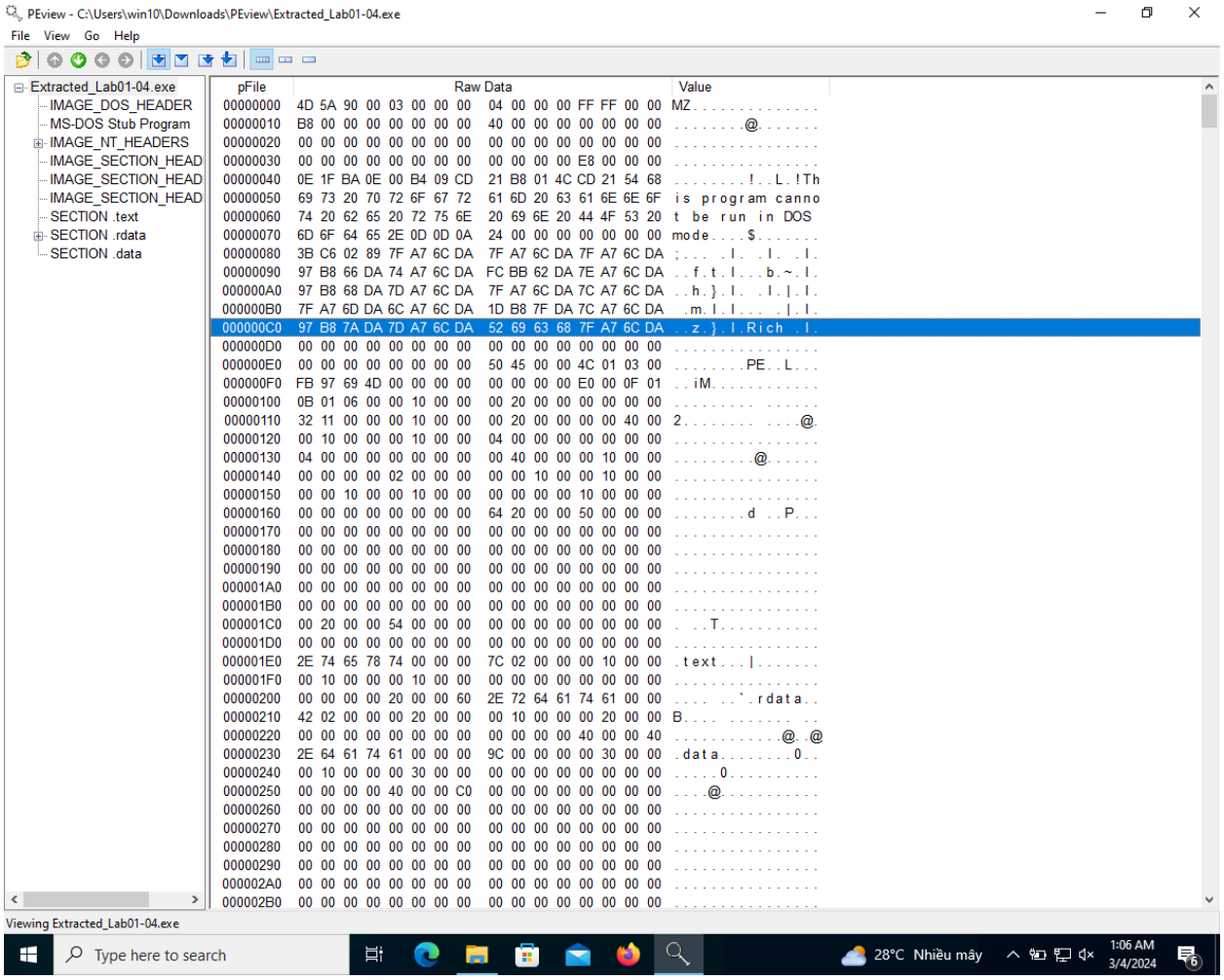
2c,


Resource Hacker - Lab01-04.exe
File Edit View Action Help
BIN : 101 : 1033
BIN
101 : 1033
Editor View
Binary View
4000 / 4060
Selection - Offset: 0 Length: 0
Type here to search
Nhiệt độ tăng
1:06 AM
3/4/2024

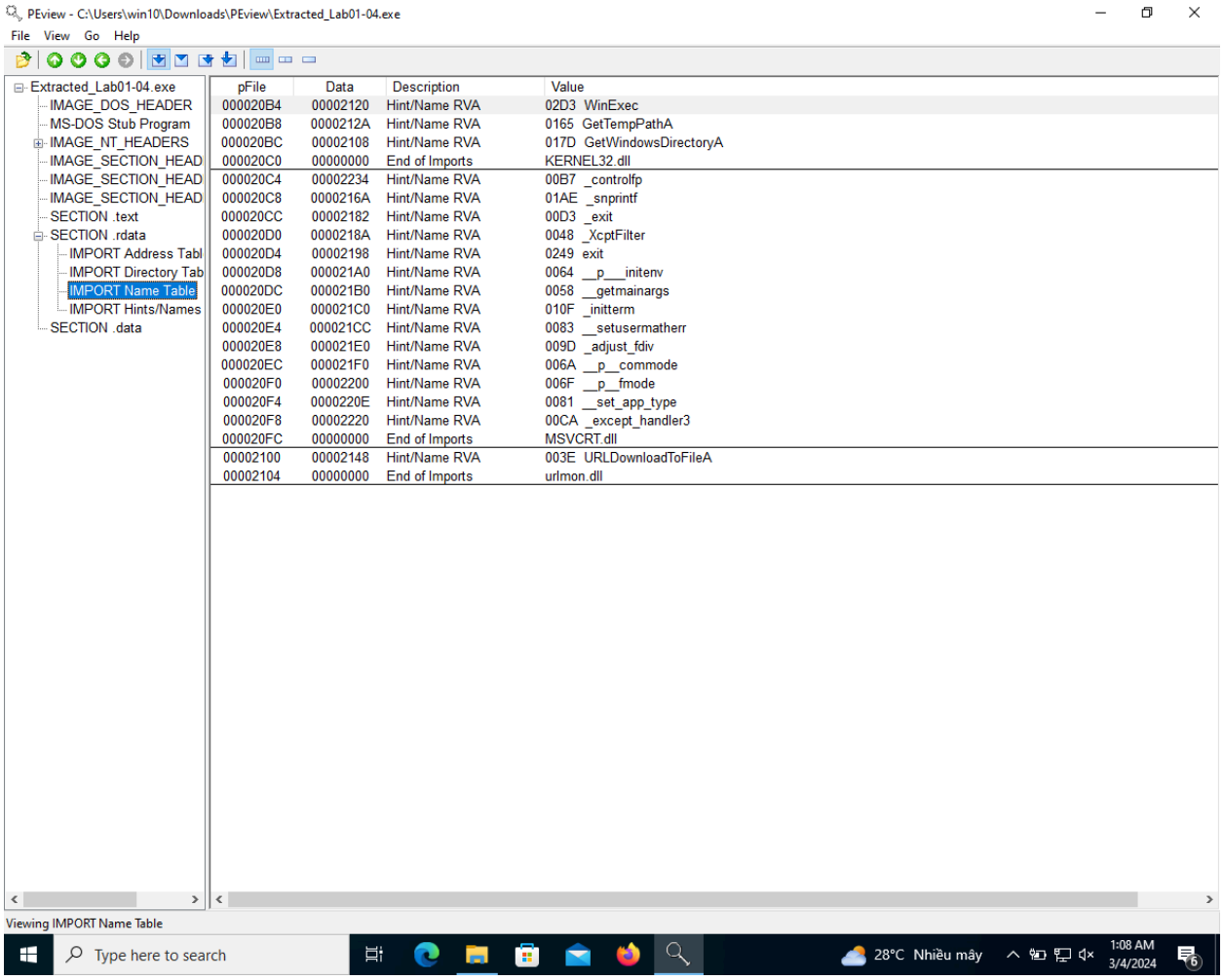
2d&e,


Save Resource
Downloads › PEview
Search PEview
Organize
New folder
Desktop
Downloads
Documents
Pictures
Music
Strings
Videos
OneDrive
This PC
Name
Date modified
Lab01-04
7/5/2011 8:16 PM
PEview
5/9/2011 10:09 AM
File name: Extracted_Lab01-04
Save as type: All files (*.*)
Hide Folders
Save
Cancel

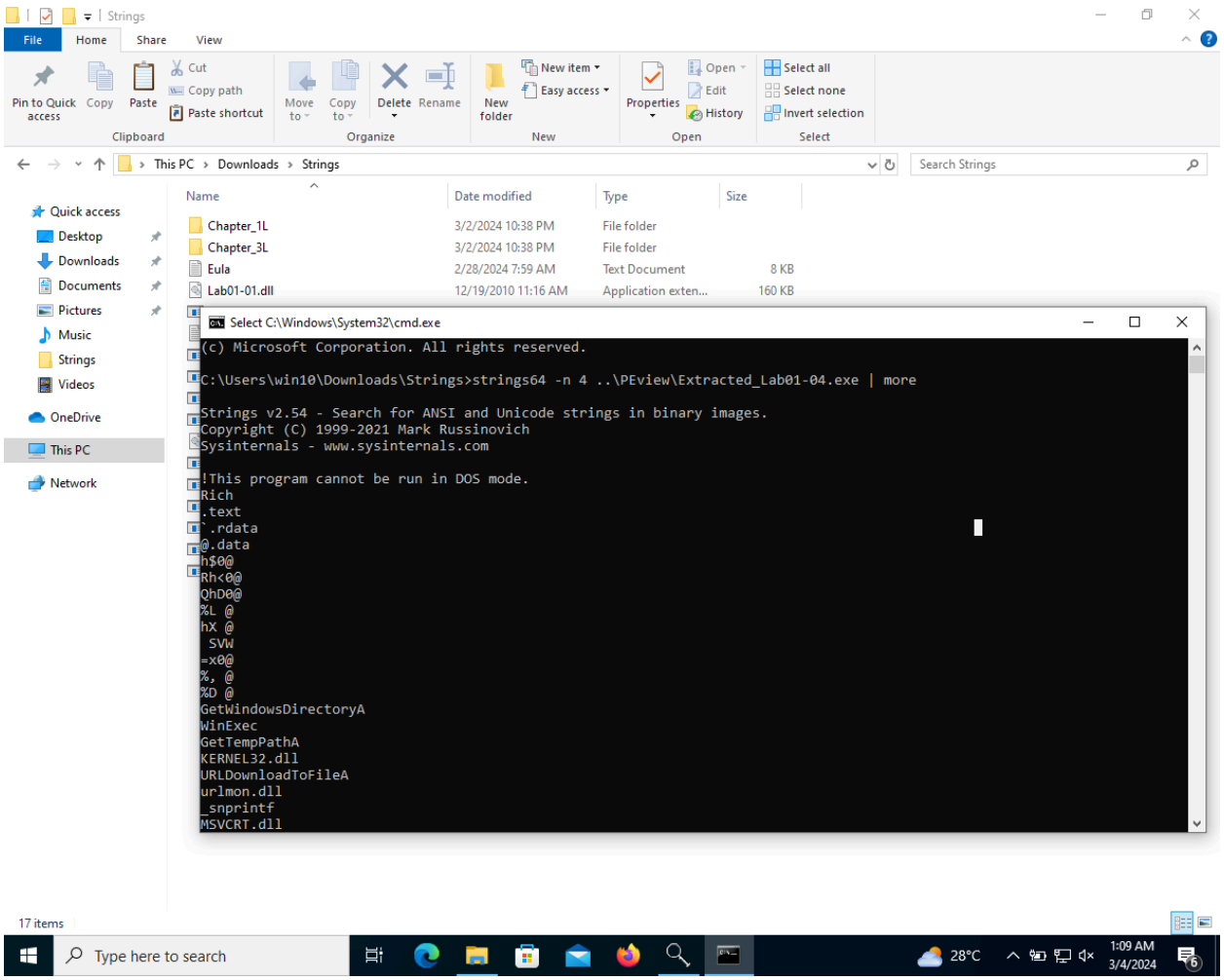
3a,


PEview - C:\Users\win10\Downloads\PEview\Extracted_Lab01-04.exe
File View Go Help
Extracted_Lab01-04.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEAD
IMAGE_SECTION_HEAD
IMAGE_SECTION_HEAD
SECTION .text
SECTION .rdata
SECTION .data
pFile Raw Data Value
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ
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 E8 00 00 00
00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 !..L.!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 3B C6 02 89 7F A7 6C DA 7F A7 6C DA 7F A7 6C DA ;....l...l...l.
00000090 97 B8 66 DA 74 A7 6C DA FC BB 62 DA 7E A7 6C DA ..f.t.l...b.~.l.
000000A0 97 B8 68 DA 7D A7 6C DA 7F A7 6C DA 7C A7 6C DA ..h.}.l...l.|.l.
000000B0 7F A7 6D DA 6C A7 6C DA 1D B8 7F DA 7C A7 6C DA ..m.l.l.....|.l.
000000C0 97 B8 7A DA 7D A7 6C DA 52 69 63 68 7F A7 6C DA ..z.}.l.Rich..l.
000000D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000E0 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 03 00 ........PE..L...
000000F0 FB 97 69 4D 00 00 00 00 00 00 00 00 E0 00 0F 01 ..iM............
00000100 0B 01 06 00 00 10 00 00 00 20 00 00 00 00 00 00 ....
00000110 32 11 00 00 00 10 00 00 00 20 00 00 00 00 40 00 2..... ....@.
00000120 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00 ....
00000130 04 00 00 00 00 00 00 00 00 40 00 00 00 10 00 00 .....@......
00000140 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 ....
00000150 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 ....
00000160 00 00 00 00 00 00 00 00 64 20 00 00 50 00 00 00 ....d ..P...
00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000001A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000001B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000001C0 00 20 00 00 54 00 00 00 00 00 00 00 00 00 00 00 ...T............
000001D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000001E0 2E 74 65 78 74 00 00 00 7C 02 00 00 00 10 00 00 .text...|.......
000001F0 00 10 00 00 00 10 00 00 00 00 00 00 00 00 00 00 ....
00000200 00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00 .... ..`.rdata..
00000210 42 02 00 00 00 20 00 00 00 10 00 00 00 20 00 00 B.... ....
00000220 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 ....@..@
00000230 2E 64 61 74 61 00 00 00 9C 00 00 00 00 30 00 00 .data........0..
00000240 00 10 00 00 00 30 00 00 00 00 00 00 00 00 00 00 .....0..........
00000250 00 00 00 00 40 00 00 C0 00 00 00 00 00 00 00 00 ....@...........
00000260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000270 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000002A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000002B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
Viewing Extracted_Lab01-04.exe
Type here to search
28°C Nhiều mây
1:06 AM
3/4/2024

3b,


PEview - C:\Users\win10\Downloads\PEview\Extracted_Lab01-04.exe
File View Go Help
Extracted_Lab01-04.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEAD
IMAGE_SECTION_HEAD
IMAGE_SECTION_HEAD
SECTION .text
SECTION .rdata
IMPORT Address Tabl
IMPORT Directory Tab
IMPORT Name Table
IMPORT Hints/Names
SECTION .data
pFile Data Description Value
000020B4 00002120 Hint/Name RVA 02D3 WinExec
000020B8 0000212A Hint/Name RVA 0165 GetTempPathA
000020BC 00002108 Hint/Name RVA 017D GetWindowsDirectoryA
000020C0 00000000 End of Imports KERNEL32.dll
000020C4 00002234 Hint/Name RVA 00B7 _controlfp
000020C8 0000216A Hint/Name RVA 01AE _snprintf
000020CC 00002182 Hint/Name RVA 00D3 _exit
000020D0 0000218A Hint/Name RVA 0048 _XcptFilter
000020D4 00002198 Hint/Name RVA 0249 exit
000020D8 000021A0 Hint/Name RVA 0064 __p___initenv
000020DC 000021B0 Hint/Name RVA 0058 __getmainargs
000020E0 000021C0 Hint/Name RVA 010F _initterm
000020E4 000021CC Hint/Name RVA 0083 __setusermatherr
000020E8 000021E0 Hint/Name RVA 009D _adjust_fdiv
000020EC 000021F0 Hint/Name RVA 006A __p__commode
000020F0 00002200 Hint/Name RVA 006F __p__fmode
000020F4 0000220E Hint/Name RVA 0081 __set_app_type
000020F8 00002220 Hint/Name RVA 00CA _except_handler3
000020FC 00000000 End of Imports MSVCRT.dll
00002100 00002148 Hint/Name RVA 003E URLDownloadToFileA
00002104 00000000 End of Imports urlmon.dll
Viewing IMPORT Name Table
Type here to search
28°C Nhiều mây
1:08 AM
3/4/2024

4a,

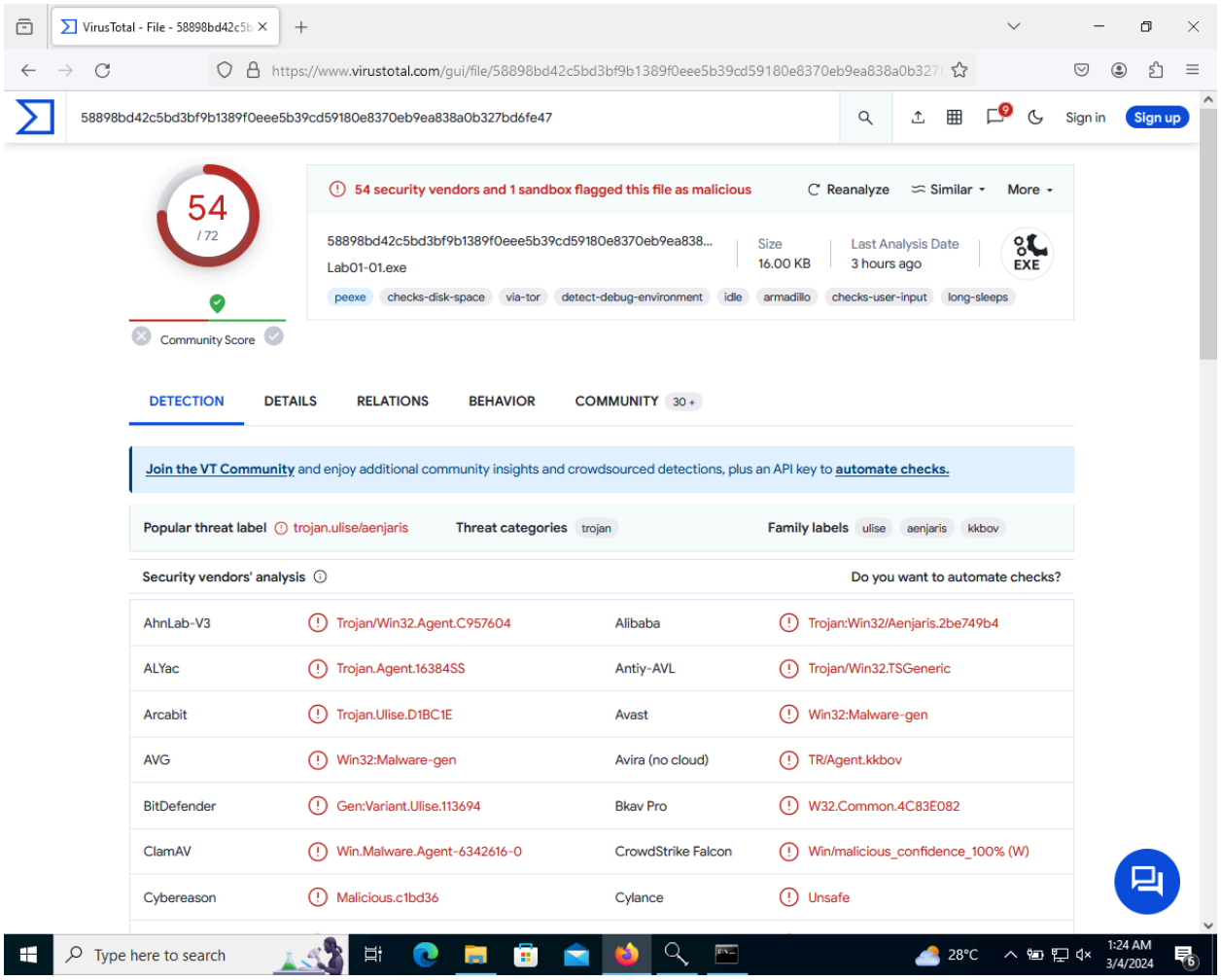


4b, Xâu liên quan đến URL đáng chú ý là http://www.practicalmalwareanalysis.com/updater.exe

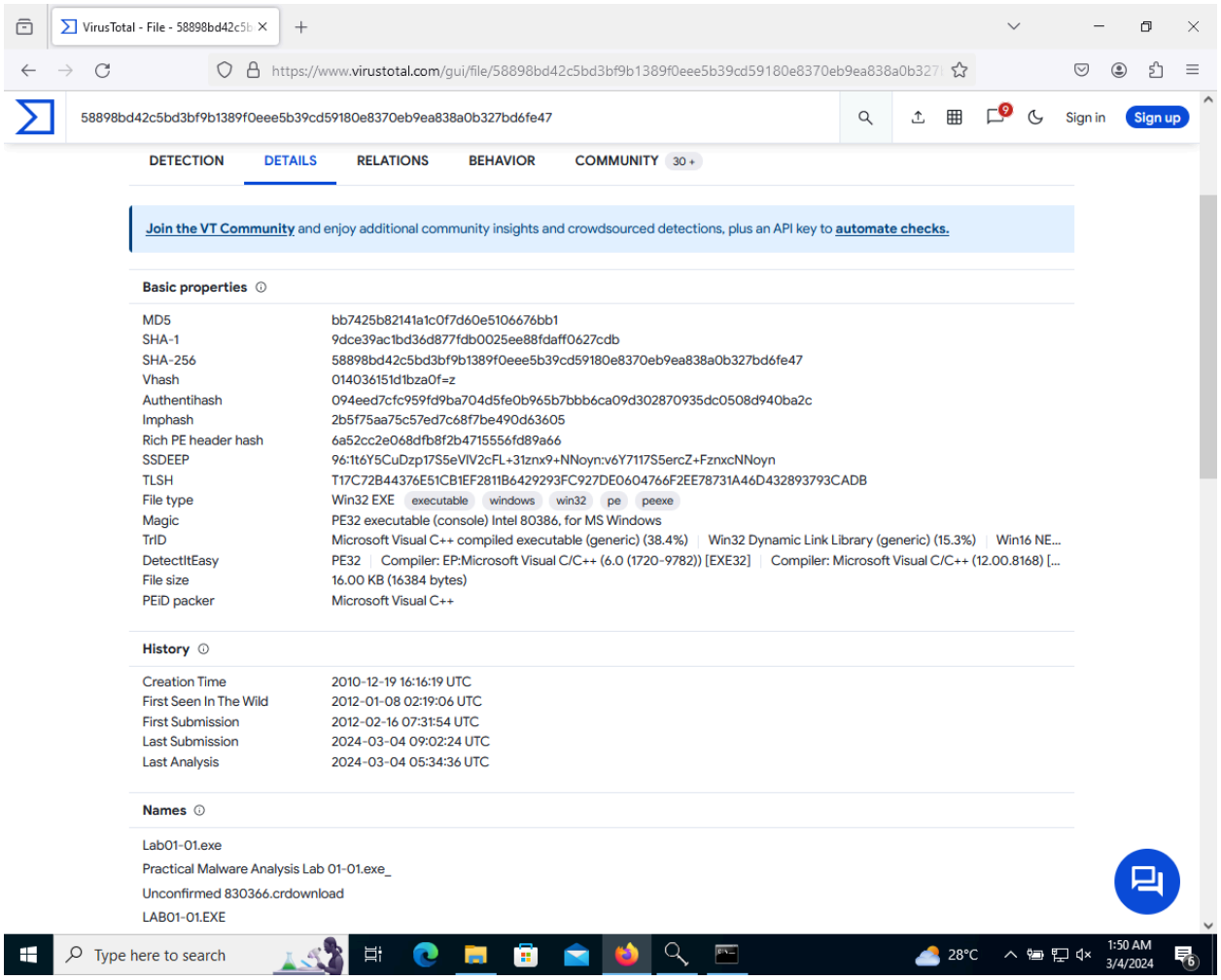
4c, Xâu liên quan đến quá trình cập nhật là \winup.exe, \system32\wupdmgrd.exe, http://www.practicalmalwareanalysis.com/updater.exe

Lab 15.04:

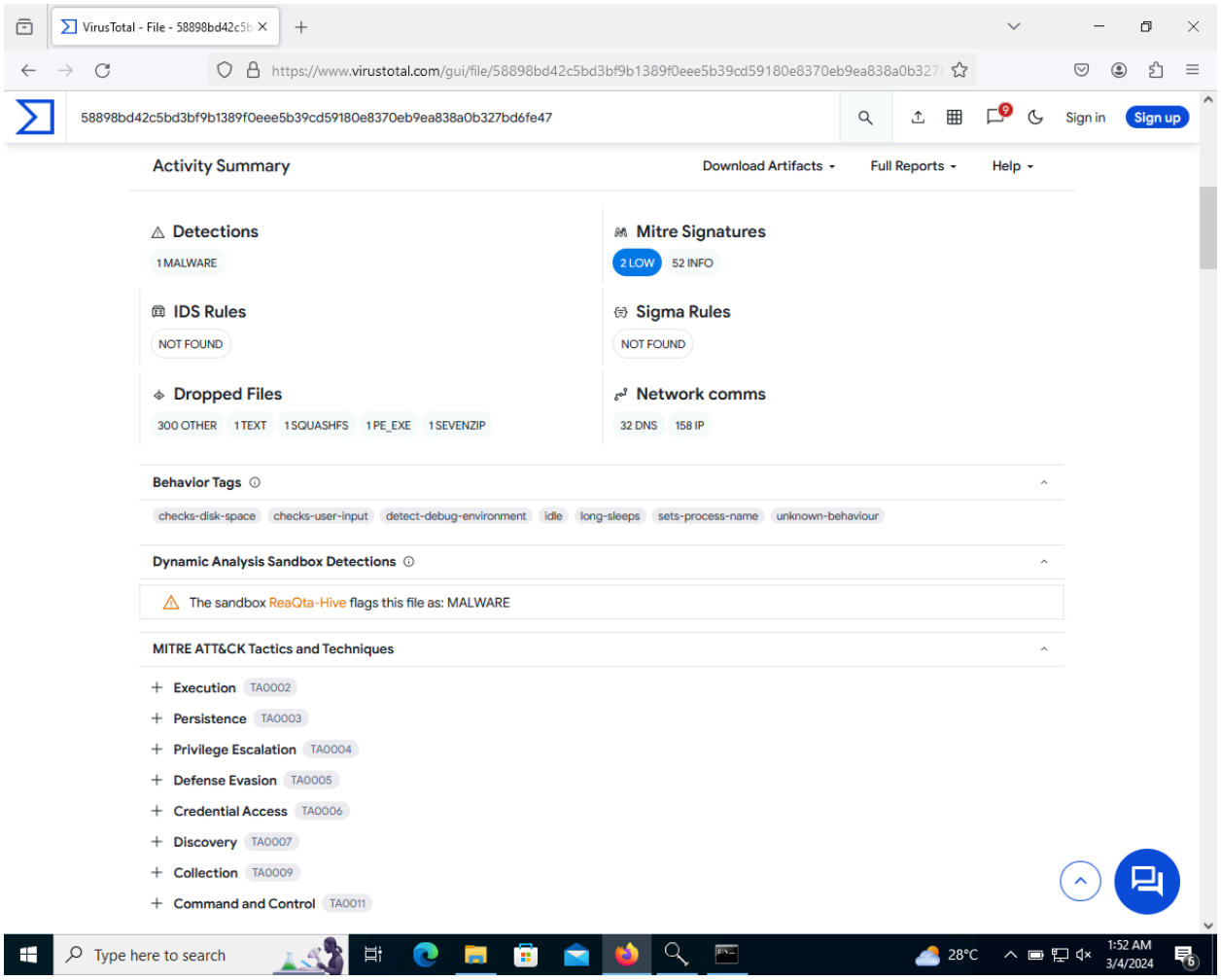
1a&b,


VirusTotal - File - 58898bd42c5b
https://www.virustotal.com/gui/file/58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327
58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Sign in
Sign up
54
/ 72
Community Score
54 security vendors and 1 sandbox flagged this file as malicious
Reanalyze
Similar
More
58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838...
Lab01-01.exe
Size
16.00 KB
Last Analysis Date
3 hours ago
EXE
peexe
checks-disk-space
via-tor
detect-debug-environment
idle
armadillo
checks-user-input
long-sleeps
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 30 +
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.ulise/aenjaris
Threat categories trojan
Family labels ulise aenjaris kkbov
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3 Trojan/Win32.Agent.C957604
Alibaba Trojan:Win32/Aenjaris.2be749b4
ALYac Trojan.Agent.16384SS
Antiy-AVL Trojan/Win32.TSGeneric
Arcabit Trojan.Ulise.D1BC1E
Avast Win32:Malware-gen
AVG Win32:Malware-gen
Avira (no cloud) TR/Agent.kkbov
BitDefender Gen:Variant.Ulise.113694
Bkav Pro W32.Common.4C83E082
ClamAV Win.Malware.Agent-6342616-0
CrowdStrike Falcon Win/malicious_confidence_100% (W)
Cybereason Malicious.c1bd36
Cylance Unsafe
Type here to search
28°C
1:24 AM
3/4/2024

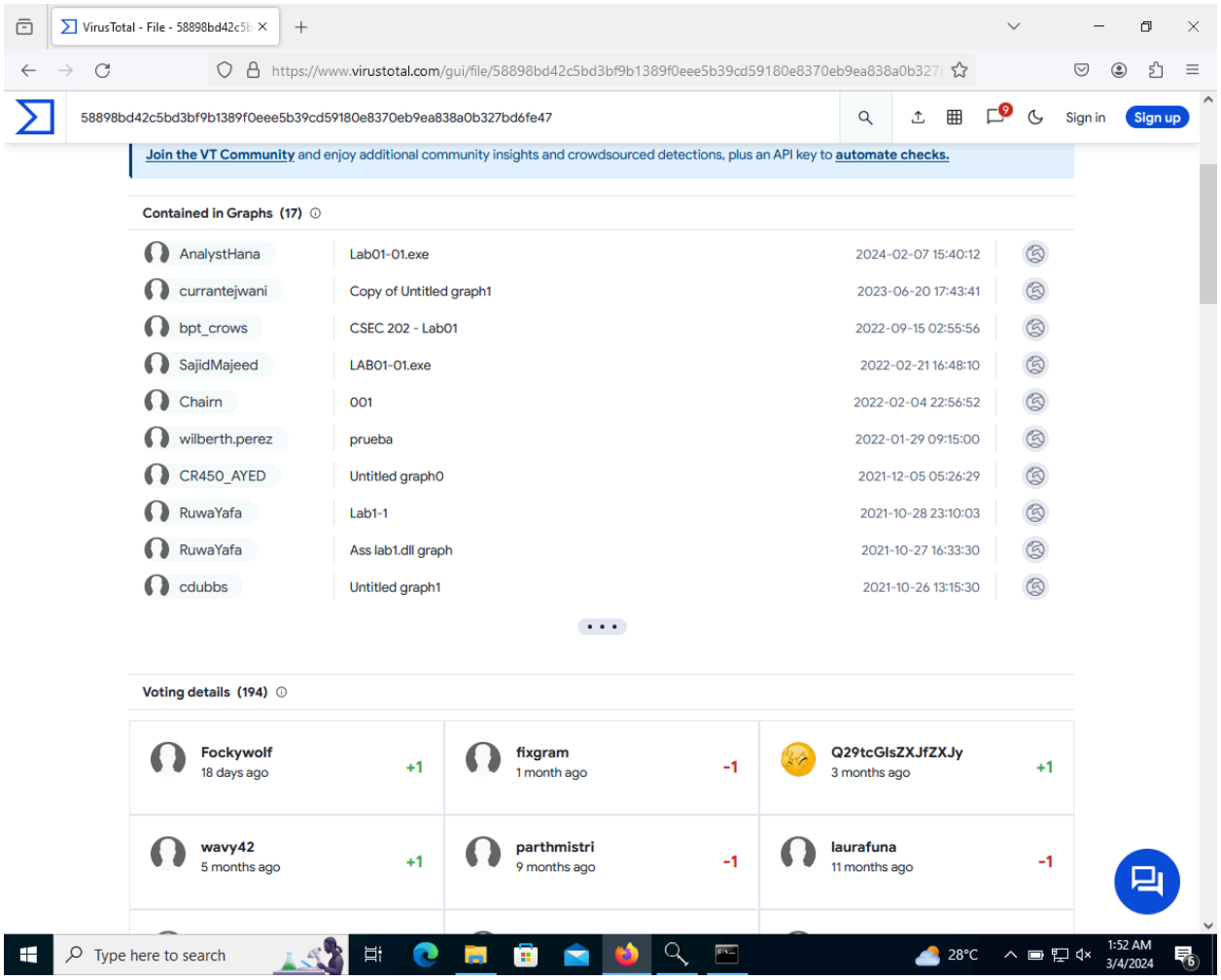
1c,


VirusTotal - File - 58898bd42c5b
https://www.virustotal.com/gui/file/58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327
58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Sign in
Sign up
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 30 +
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Basic properties
MD5 bb7425b82141a1c0f7d60e5106676bb1
SHA-1 9dce39ac1bd36d877fdb0025ee88fdaff0627cdb
SHA-256 58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Vhash 014036151d1bza0f=z
Authentihash 094eed7cfc959fd9ba704d5fe0b965b7bbb6ca09d302870935dc0508d940ba2c
Imphash 2b5f75aa75c57ed7c68f7be490d63605
Rich PE header hash 6a52cc2e068dfb8f2b4715556fd89a66
SSDEEP 96:1t6Y5CuDzp17S5eVIV2cFL+31znx9+NNoyn:v6Y7117S5ercZ+FznxcNNoyn
TLSH T17C72B44376E51CB1EF2811B6429293FC927DE0604766F2EE78731A46D432893793CADB
File type Win32 EXE executable windows win32 pe peexe
Magic PE32 executable (console) Intel 80386, for MS Windows
TrID Microsoft Visual C++ compiled executable (generic) (38.4%) | Win32 Dynamic Link Library (generic) (15.3%) | Win16 NE...
DetectItEasy PE32 | Compiler: EP:Microsoft Visual C/C++ (6.0 (1720-9782)) [EXE32] | Compiler: Microsoft Visual C/C++ (12.00.8168) [...
File size 16.00 KB (16384 bytes)
PEiD packer Microsoft Visual C++
History
Creation Time 2010-12-19 16:16:19 UTC
First Seen In The Wild 2012-01-08 02:19:06 UTC
First Submission 2012-02-16 07:31:54 UTC
Last Submission 2024-03-04 09:02:24 UTC
Last Analysis 2024-03-04 05:34:36 UTC
Names
Lab01-01.exe
Practical Malware Analysis Lab 01-01.exe_
Unconfirmed 830366.crdownload
LAB01-01.EXE
Type here to search
28°C
1:50 AM
3/4/2024

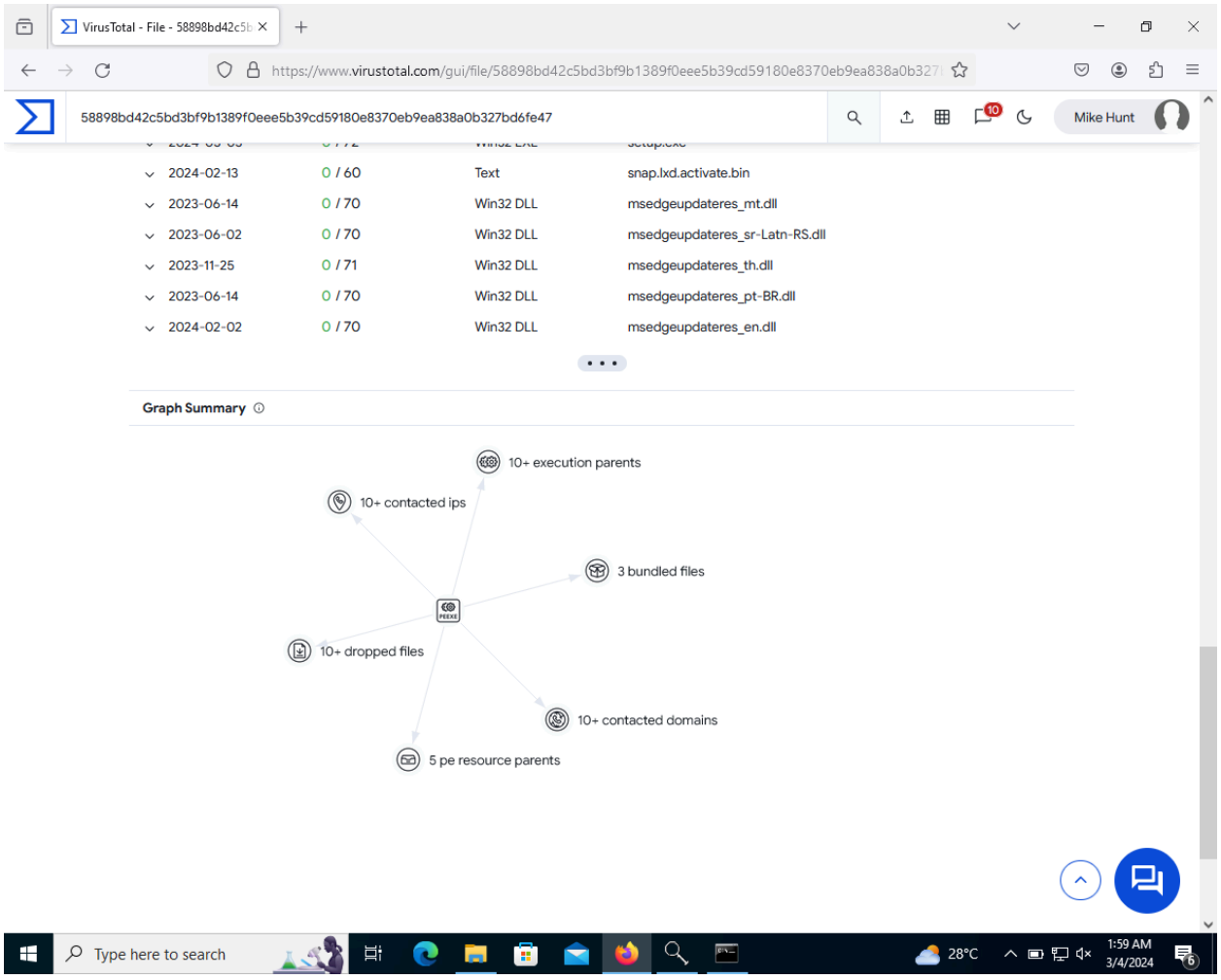
1d,


VirusTotal - File - 58898bd42c5b
https://www.virustotal.com/gui/file/58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327
58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Sign in
Sign up
Activity Summary
Download Artifacts
Full Reports
Help
Detections
1 MALWARE
Mitre Signatures
2 LOW
52 INFO
IDS Rules
NOT FOUND
Sigma Rules
NOT FOUND
Dropped Files
300 OTHER
1 TEXT
1 SQUASHFS
1 PE_EXE
1 SEVENZIP
Network comms
32 DNS
158 IP
Behavior Tags
checks-disk-space
checks-user-input
detect-debug-environment
idle
long-sleeps
sets-process-name
unknown-behaviour
Dynamic Analysis Sandbox Detections
The sandbox ReaQta-Hive flags this file as: MALWARE
MITRE ATT&CK Tactics and Techniques
Execution TA0002
Persistence TA0003
Privilege Escalation TA0004
Defense Evasion TA0005
Credential Access TA0006
Discovery TA0007
Collection TA0009
Command and Control TA0011
Type here to search
28°C
1:52 AM
3/4/2024

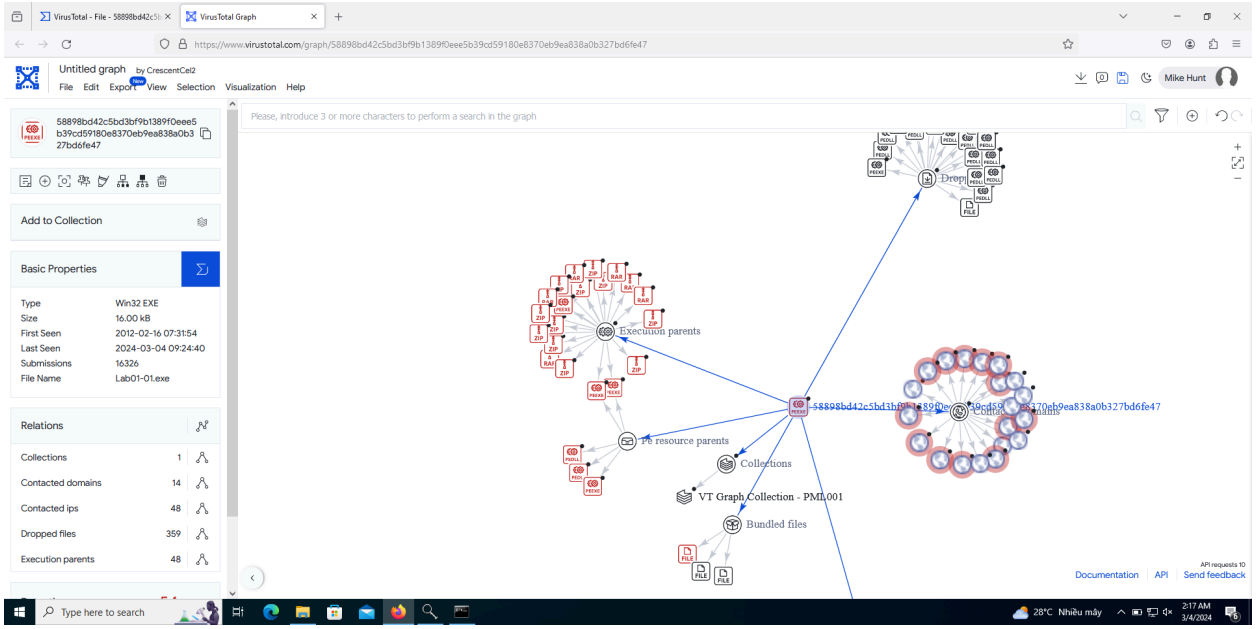
1e,


VirusTotal - File - 58898bd42c5b
https://www.virustotal.com/gui/file/58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327
58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Sign in
Sign up
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Contained in Graphs (17)
AnalystHana Lab01-01.exe 2024-02-07 15:40:12
currantejwani Copy of Untitled graph1 2023-06-20 17:43:41
bpt_crows CSEC 202 - Lab01 2022-09-15 02:55:56
SajidMajeed LAB01-01.exe 2022-02-21 16:48:10
Chairn 001 2022-02-04 22:56:52
wilberth.perez prueba 2022-01-29 09:15:00
CR450_AYED Untitled graph0 2021-12-05 05:26:29
RuwaYafa Lab1-1 2021-10-28 23:10:03
RuwaYafa Ass lab1.dll graph 2021-10-27 16:33:30
cdubbs Untitled graph1 2021-10-26 13:15:30
Voting details (194)
Fockywolf 18 days ago +1
fixgram 1 month ago -1
Q29tcGlsZXJfZXJy 3 months ago +1
wavy42 5 months ago +1
parthmistri 9 months ago -1
laurafuna 11 months ago -1
Type here to search
28°C
1:52 AM
3/4/2024

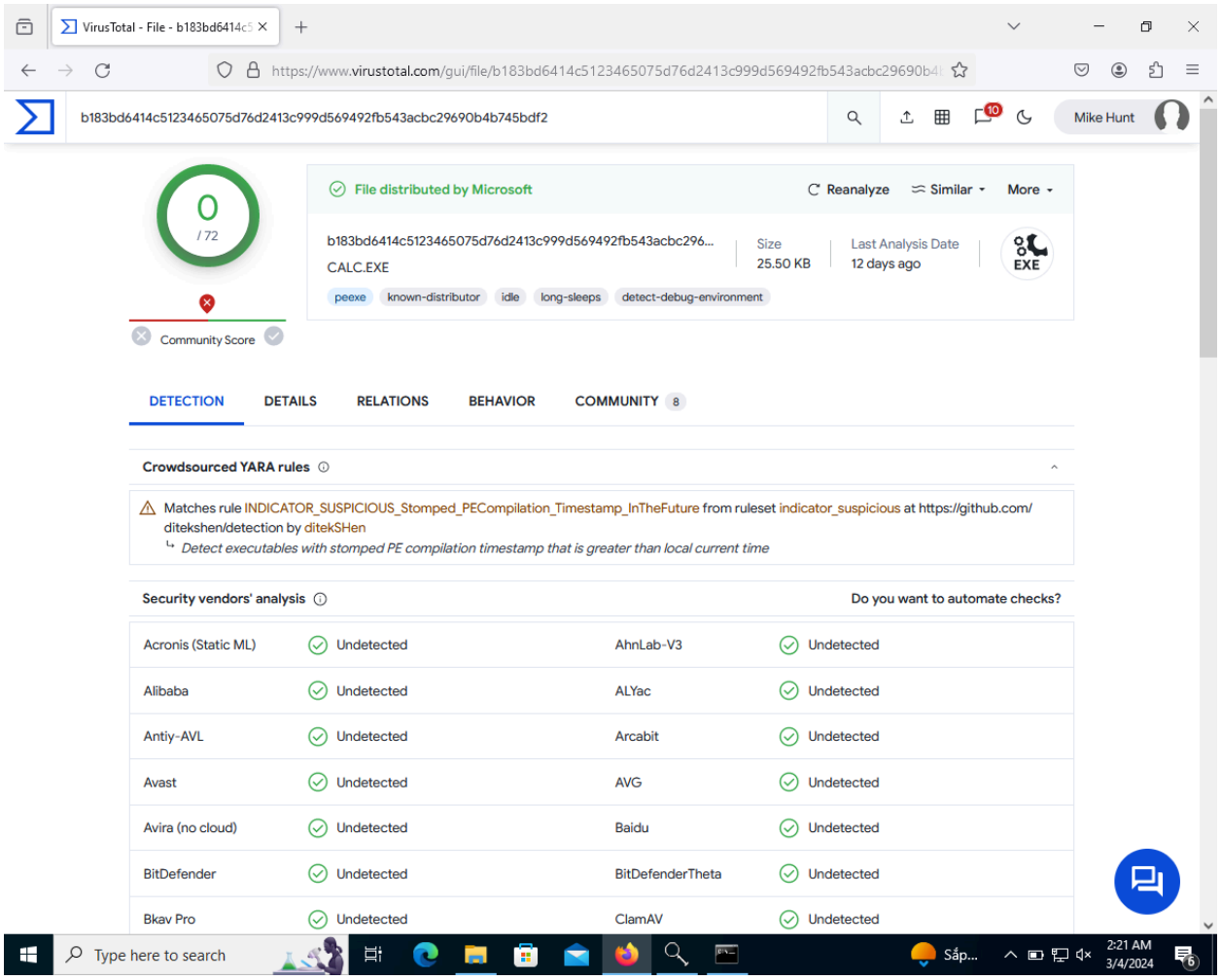
2a,


VirusTotal - File - 58898bd42c5b
https://www.virustotal.com/gui/file/58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Mike Hunt
2024-02-13 0 / 60 Text snap.lxd.activate.bin
2023-06-14 0 / 70 Win32 DLL msedgeupdateres_mt.dll
2023-06-02 0 / 70 Win32 DLL msedgeupdateres_sr-Latn-RS.dll
2023-11-25 0 / 71 Win32 DLL msedgeupdateres_th.dll
2023-06-14 0 / 70 Win32 DLL msedgeupdateres_pt-BR.dll
2024-02-02 0 / 70 Win32 DLL msedgeupdateres_en.dll
Graph Summary
10+ execution parents
10+ contacted ips
3 bundled files
10+ dropped files
10+ contacted domains
5 pe resource parents
Type here to search
28°C
1:59 AM
3/4/2024

2b&c,

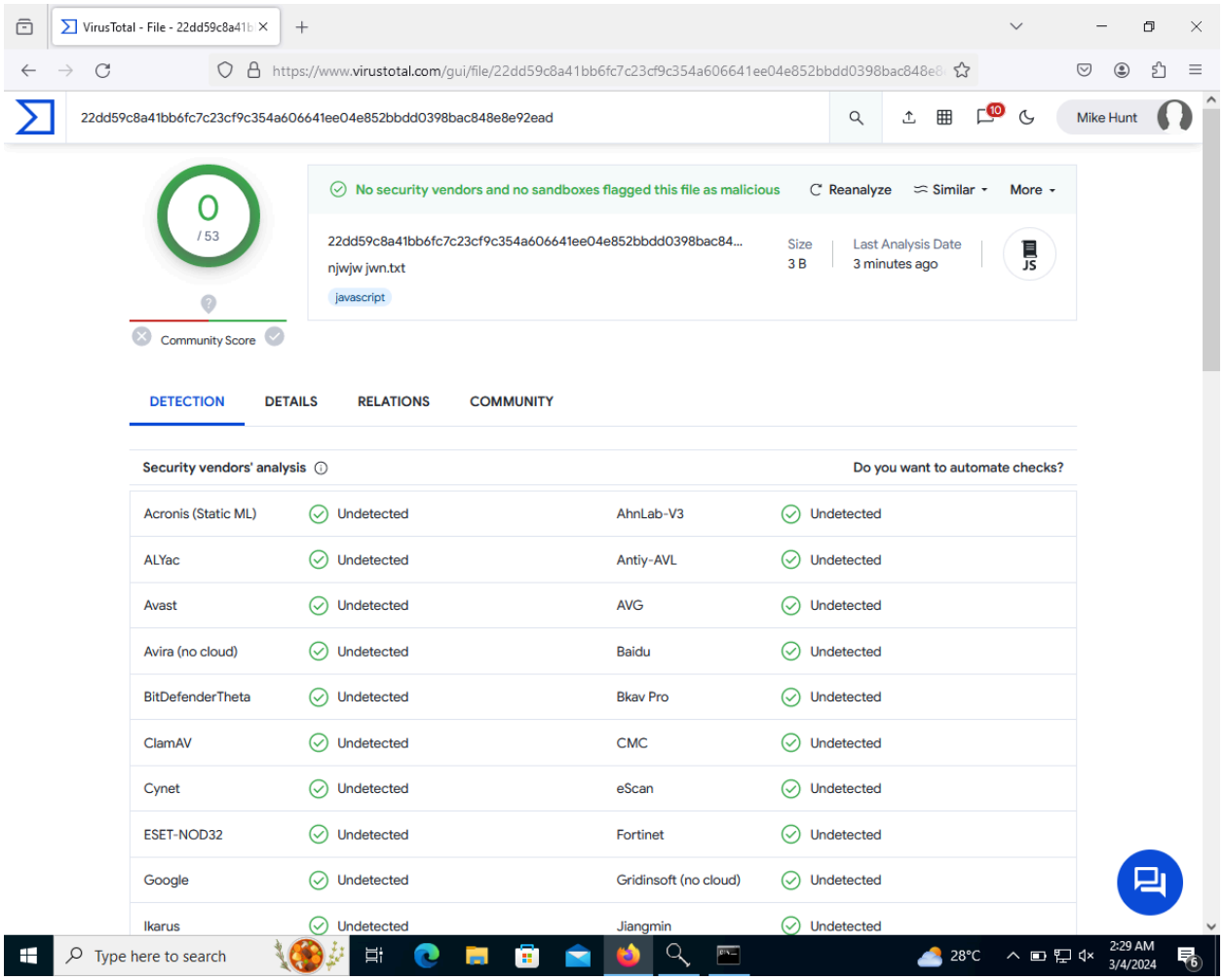

VirusTotal Graph
Untitled graph
Mike Hunt
Add to Collection
Basic Properties
Type Win32 EXE
Size 16.00 kB
First Seen 2012-02-16 07:31:54
Last Seen 2024-03-04 09:24:40
Submissions 16326
File Name Lab01-01.exe
Relations
Collections 1
Contacted domains 14
Contacted ips 48
Dropped files 359
Execution parents 48
Execution parents
Collections
VT Graph Collection - PML001
Bundled files
Documentation
API
Send feedback
28°C Nhiều mây
2:17 AM
3/4/2024

3a,

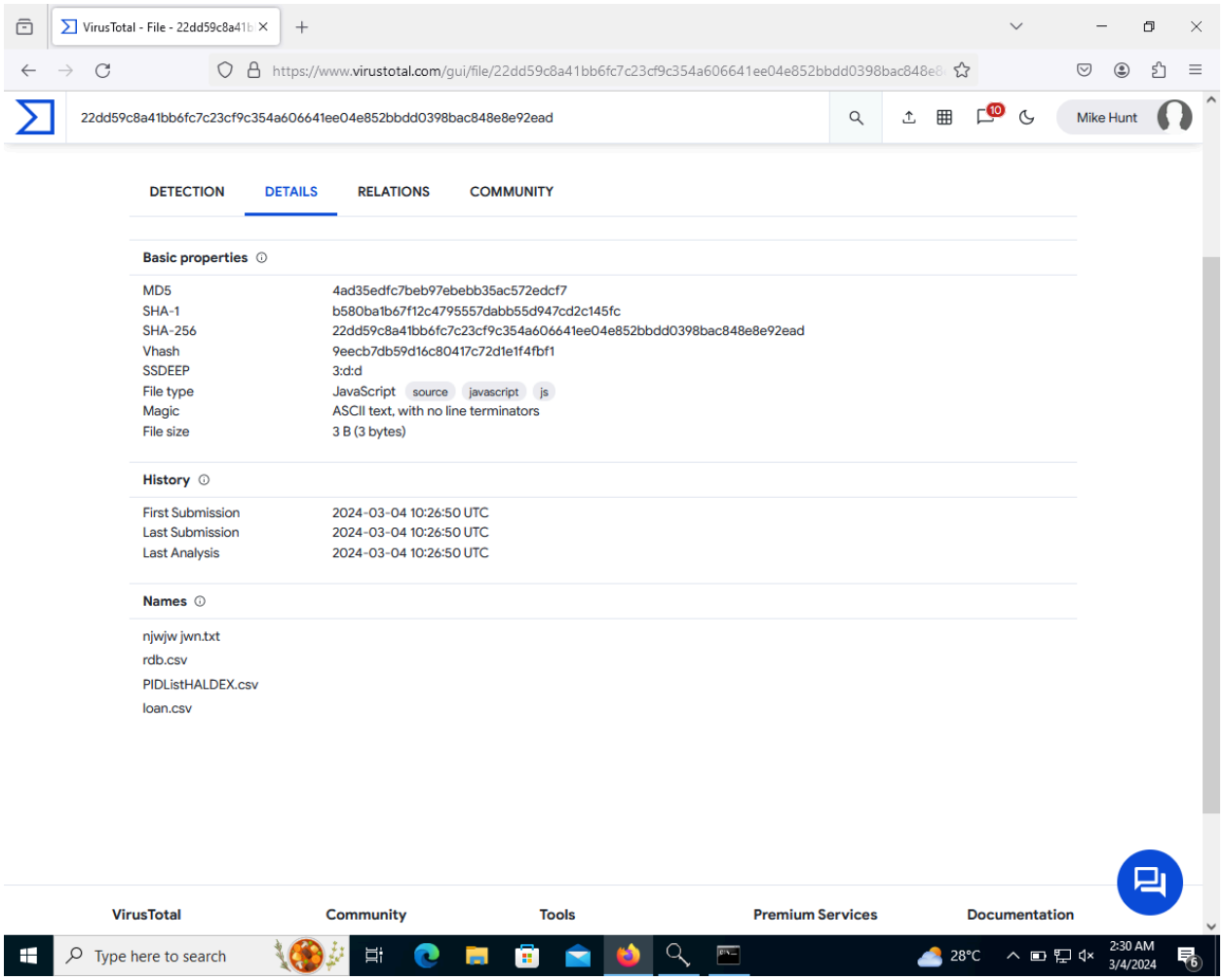


3b, 0/72 vendor coi calc.exe là độc hại

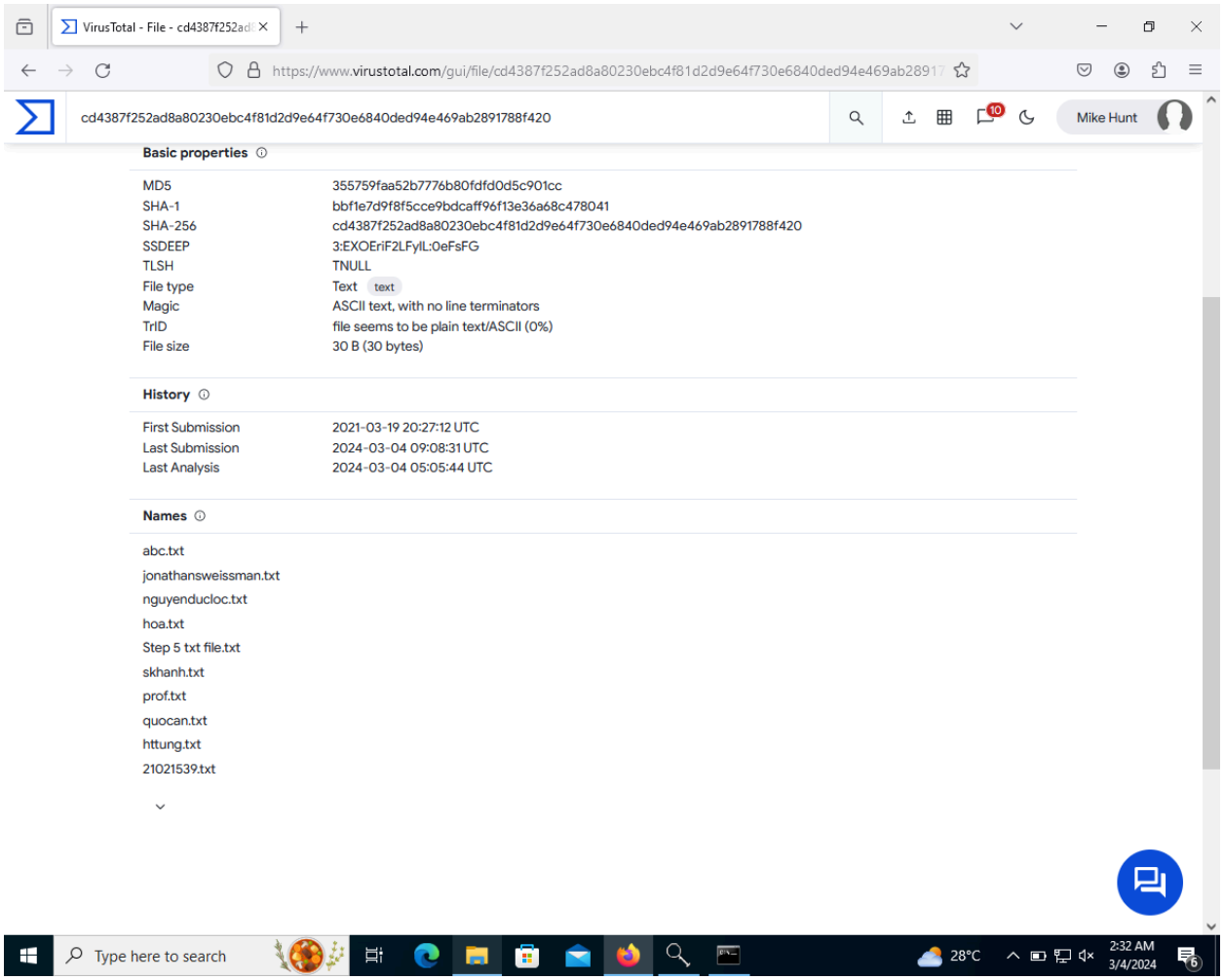
4a,


VirusTotal - File - 22dd59c8a41b
https://www.virustotal.com/gui/file/22dd59c8a41bb6fc7c23cf9c354a606641ee04e852bbdd0398bac848e8
22dd59c8a41bb6fc7c23cf9c354a606641ee04e852bbdd0398bac848e8e92ead
Mike Hunt
0
/ 53
Community Score
No security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
22dd59c8a41bb6fc7c23cf9c354a606641ee04e852bbdd0398bac84...
njwjw jwn.txt
javascript
Size
3 B
Last Analysis Date
3 minutes ago
JS
DETECTION
DETAILS
RELATIONS
COMMUNITY
Security vendors' analysis
Do you want to automate checks?
Acronis (Static ML) Undetected
AhnLab-V3 Undetected
ALYac Undetected
Antiy-AVL Undetected
Avast Undetected
AVG Undetected
Avira (no cloud) Undetected
Baidu Undetected
BitDefenderTheta Undetected
Bkav Pro Undetected
ClamAV Undetected
CMC Undetected
Cynet Undetected
eScan Undetected
ESET-NOD32 Undetected
Fortinet Undetected
Google Undetected
Gridinsoft (no cloud) Undetected
Ikarus Undetected
Jiangmin Undetected
Type here to search
28°C
2:29 AM
3/4/2024

4b,

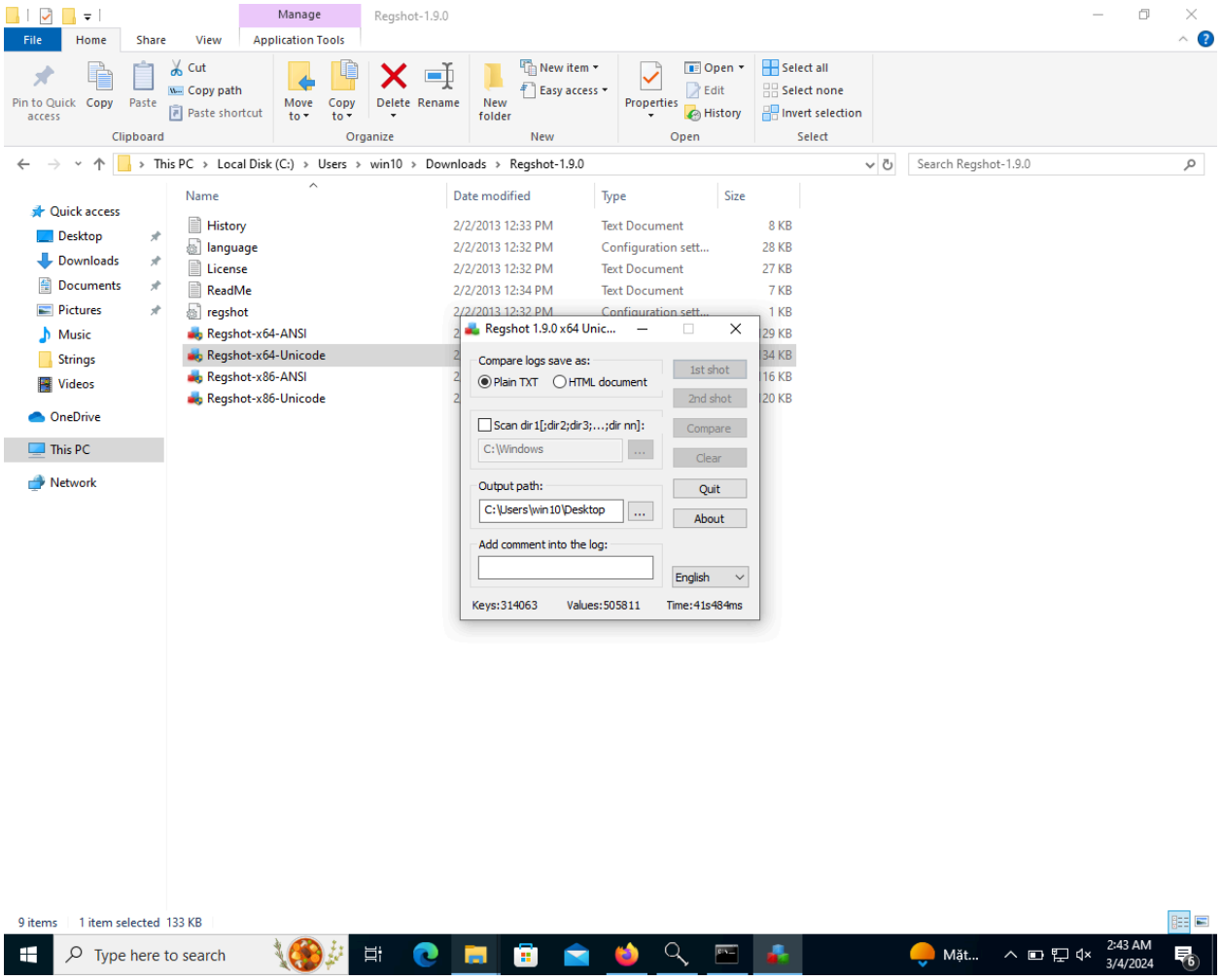

VirusTotal - File - 22dd59c8a41b
https://www.virustotal.com/gui/file/22dd59c8a41bb6fc7c23cf9c354a606641ee04e852bbdd0398bac848e8
22dd59c8a41bb6fc7c23cf9c354a606641ee04e852bbdd0398bac848e8e92ead
Mike Hunt
DETECTION
DETAILS
RELATIONS
COMMUNITY
Basic properties
MD5 4ad35edfc7beb97ebebb35ac572edcf7
SHA-1 b580ba1b67f12c4795557dabb55d947cd2c145fc
SHA-256 22dd59c8a41bb6fc7c23cf9c354a606641ee04e852bbdd0398bac848e8e92ead
Vhash 9eecb7db59d16c80417c72d1e1f4fbf1
SSDEEP 3:d:d
File type JavaScript source javascript js
Magic ASCII text, with no line terminators
File size 3 B (3 bytes)
History
First Submission 2024-03-04 10:26:50 UTC
Last Submission 2024-03-04 10:26:50 UTC
Last Analysis 2024-03-04 10:26:50 UTC
Names
njwjw jwn.txt
rdb.csv
PIDListHALDEX.csv
loan.csv
VirusTotal
Community
Tools
Premium Services
Documentation
Type here to search
28°C
2:30 AM
3/4/2024

5c,

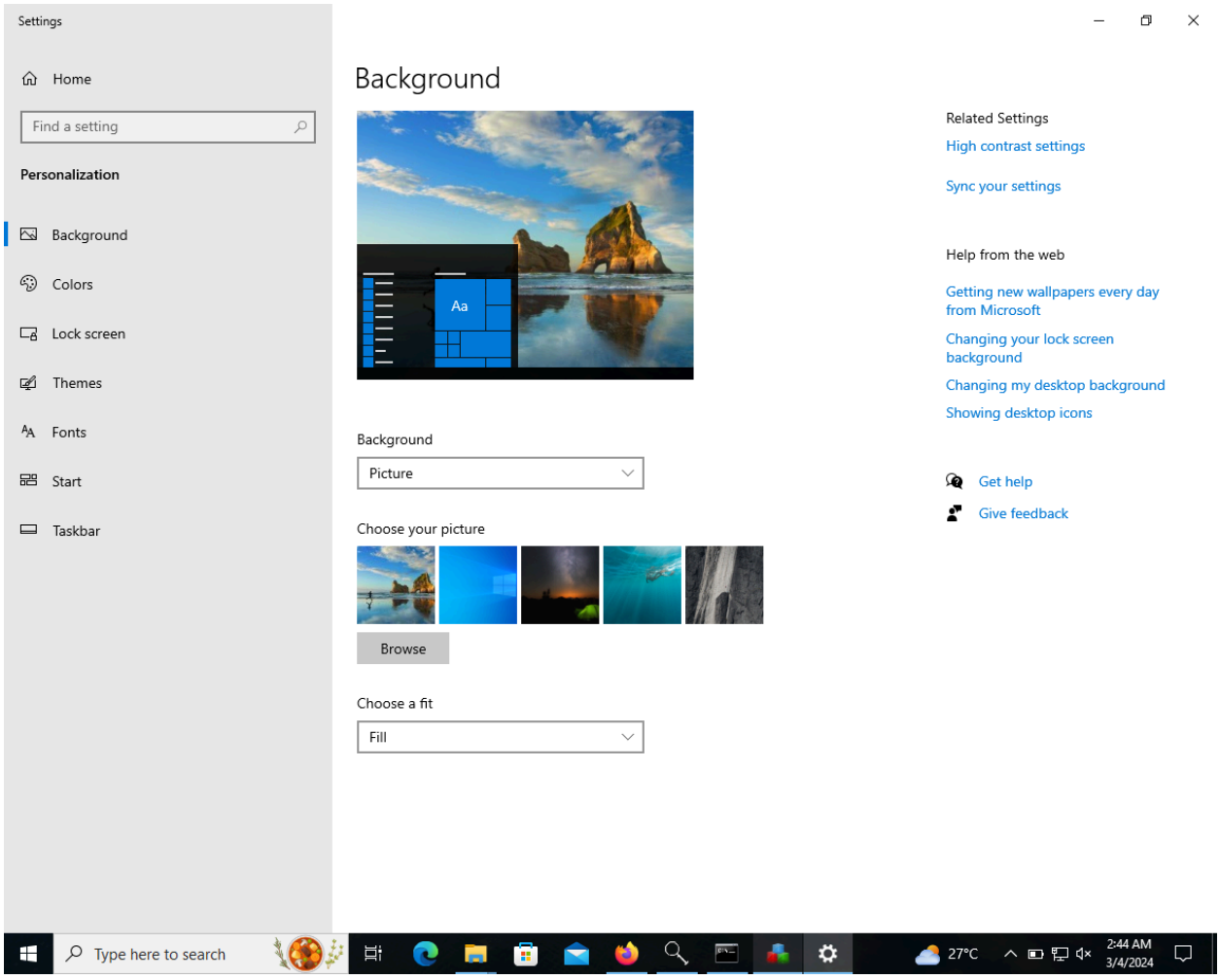

VirusTotal - File - cd4387f252ad
https://www.virustotal.com/gui/file/cd4387f252ad8a80230ebc4f81d2d9e64f730e6840ded94e469ab28917
cd4387f252ad8a80230ebc4f81d2d9e64f730e6840ded94e469ab2891788f420
Mike Hunt
Basic properties
MD5 355759faa52b7776b80fdfd0d5c901cc
SHA-1 bbf1e7d9f8f5cce9bdcaff96f13e36a68c478041
SHA-256 cd4387f252ad8a80230ebc4f81d2d9e64f730e6840ded94e469ab2891788f420
SSDEEP 3:EXOEriF2LFylL:0eFsFG
TLSH TNULL
File type Text text
Magic ASCII text, with no line terminators
TrID file seems to be plain text/ASCII (0%)
File size 30 B (30 bytes)
History
First Submission 2021-03-19 20:27:12 UTC
Last Submission 2024-03-04 09:08:31 UTC
Last Analysis 2024-03-04 05:05:44 UTC
Names
abc.txt
jonathansweissman.txt
nguyenducloc.txt
hoa.txt
Step 5 txt file.txt
skhanh.txt
prof.txt
quocan.txt
httung.txt
21021539.txt
Type here to search
28°C
2:32 AM
3/4/2024

Lab 15.05

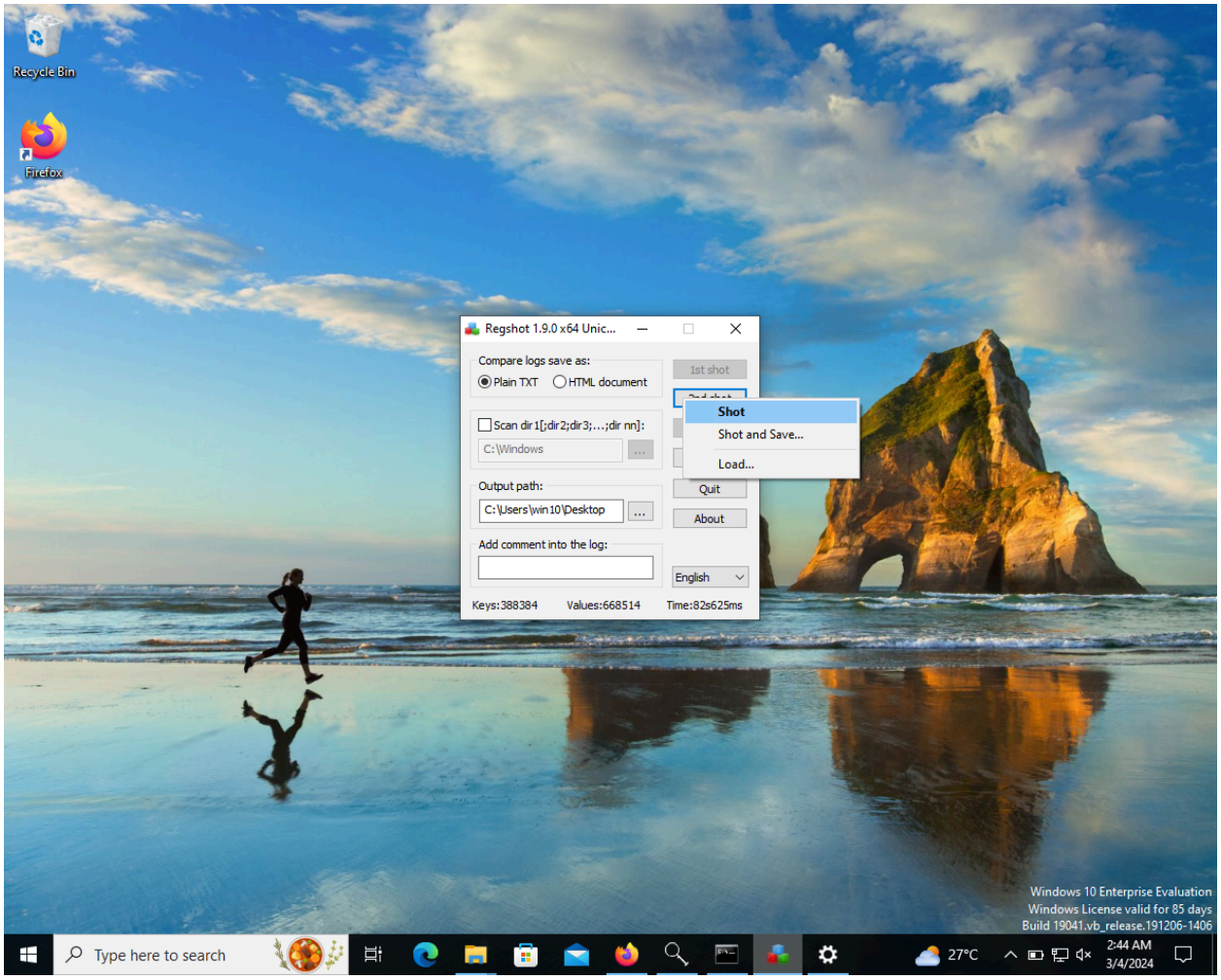
1a,


Manage
Regshot-1.9.0
File
Home
Share
View
Application Tools
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New item
Easy access
New folder
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › Local Disk (C:) › Users › win10 › Downloads › Regshot-1.9.0
Search Regshot-1.9.0
Quick access
Desktop
Downloads
Documents
Pictures
Music
Strings
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
History 2/2/2013 12:33 PM Text Document 8 KB
language 2/2/2013 12:32 PM Configuration sett... 28 KB
License 2/2/2013 12:32 PM Text Document 27 KB
ReadMe 2/2/2013 12:34 PM Text Document 7 KB
regshot 2/2/2013 12:32 PM Configuration sett... 1 KB
Regshot-x64-ANSI
Regshot-x64-Unicode
Regshot-x86-ANSI
Regshot-x86-Unicode
Regshot 1.9.0 x64 Unic...
Compare logs save as:
Plain TXT
HTML document
1st shot
2nd shot
Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows
Compare
Clear
Output path:
C:\Users\win10\Desktop
Quit
About
Add comment into the log:
English
Keys:314063
Values:505811
Time:41s484ms
9 items
1 item selected 133 KB
Type here to search
Mặt...
2:43 AM
3/4/2024

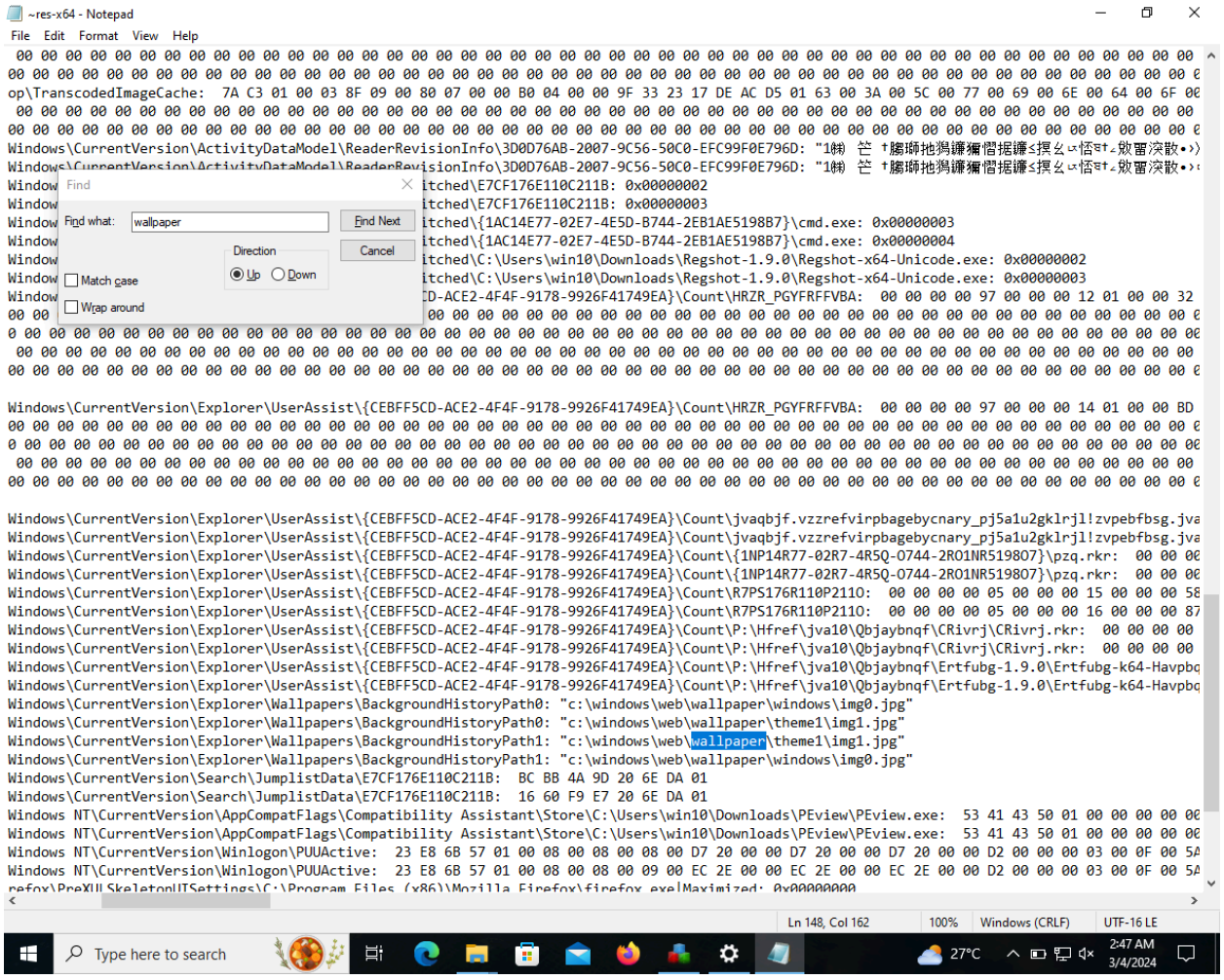
1b&c,


Settings
Home
Find a setting
Personalization
Background
Colors
Lock screen
Themes
Fonts
Start
Taskbar
Background
Aa
Background
Picture
Choose your picture
Browse
Choose a fit
Fill
Related Settings
High contrast settings
Sync your settings
Help from the web
Getting new wallpapers every day from Microsoft
Changing your lock screen background
Changing my desktop background
Showing desktop icons
Get help
Give feedback
Type here to search
27°C
2:44 AM
3/4/2024

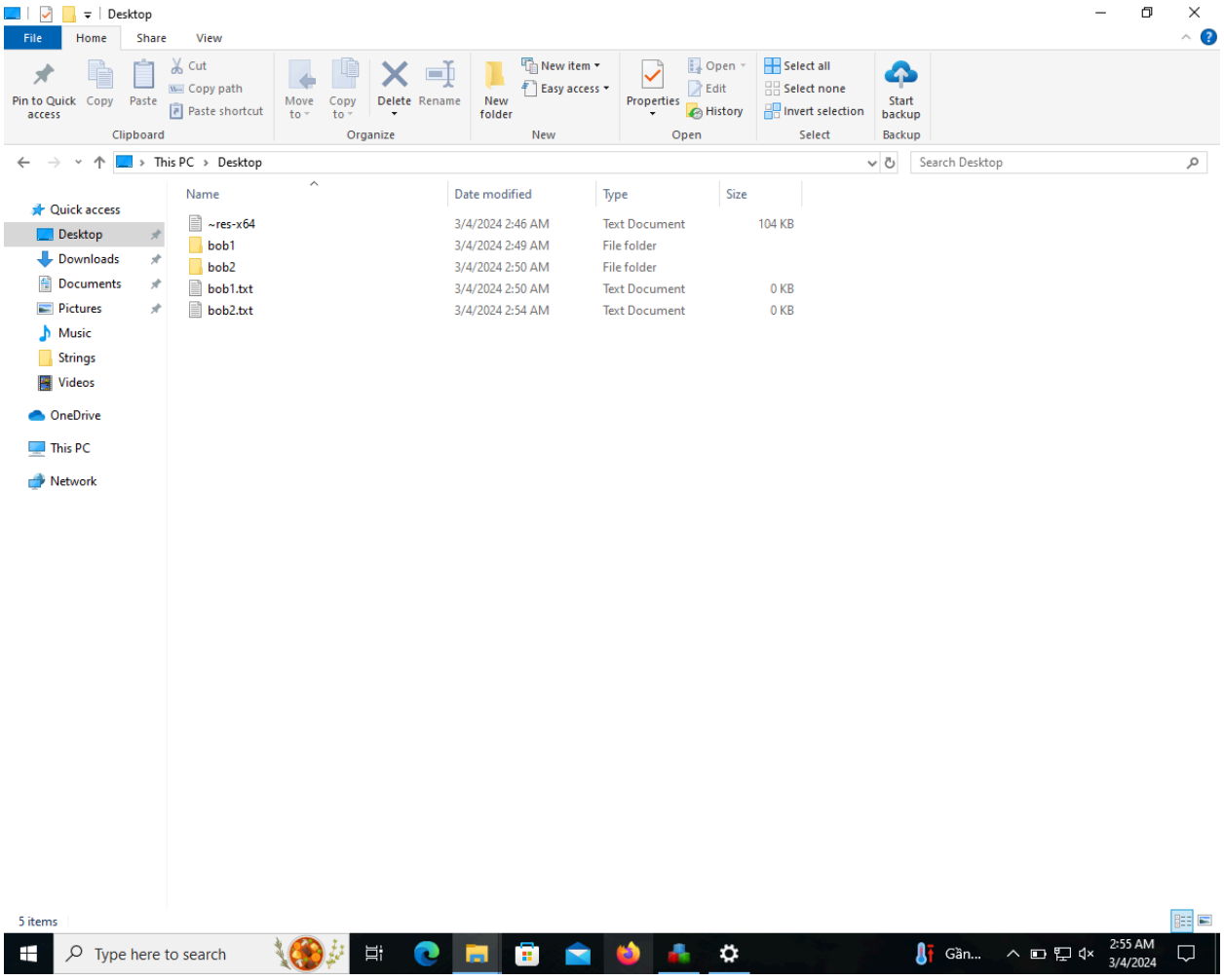
1d,


Recycle Bin
Firefox
Regshot 1.9.0 x64 Unic...
Compare logs save as:
Plain TXT
HTML document
1st shot
Shot
Shot and Save...
Load...
Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows
Output path:
C:\Users\win10\Desktop
Quit
About
Add comment into the log:
English
Keys:388384
Values:668514
Time:82s625ms
Windows 10 Enterprise Evaluation
Windows License valid for 85 days
Build 19041.vb_release.191206-1406
Type here to search
27°C
2:44 AM
3/4/2024

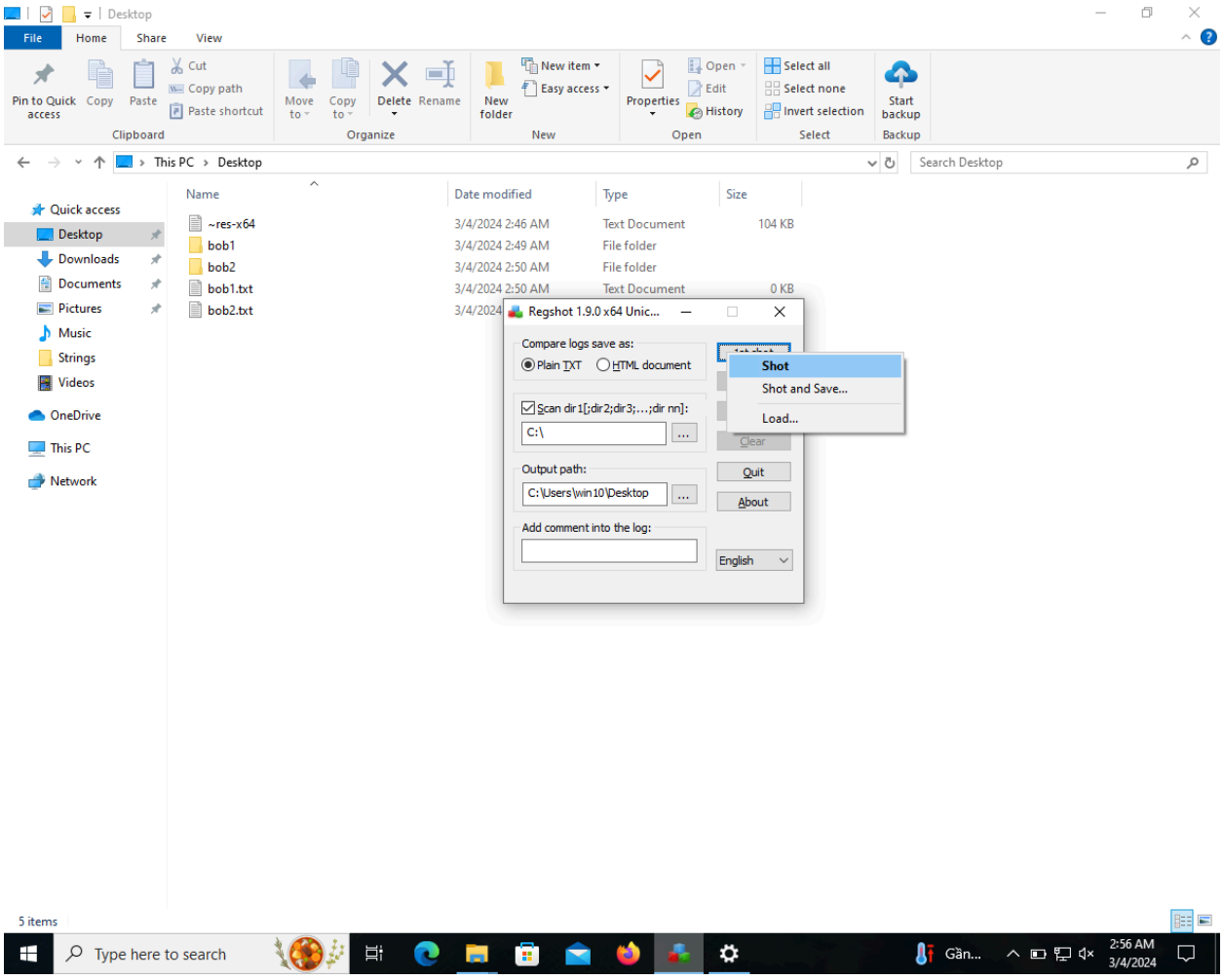
1e&f,

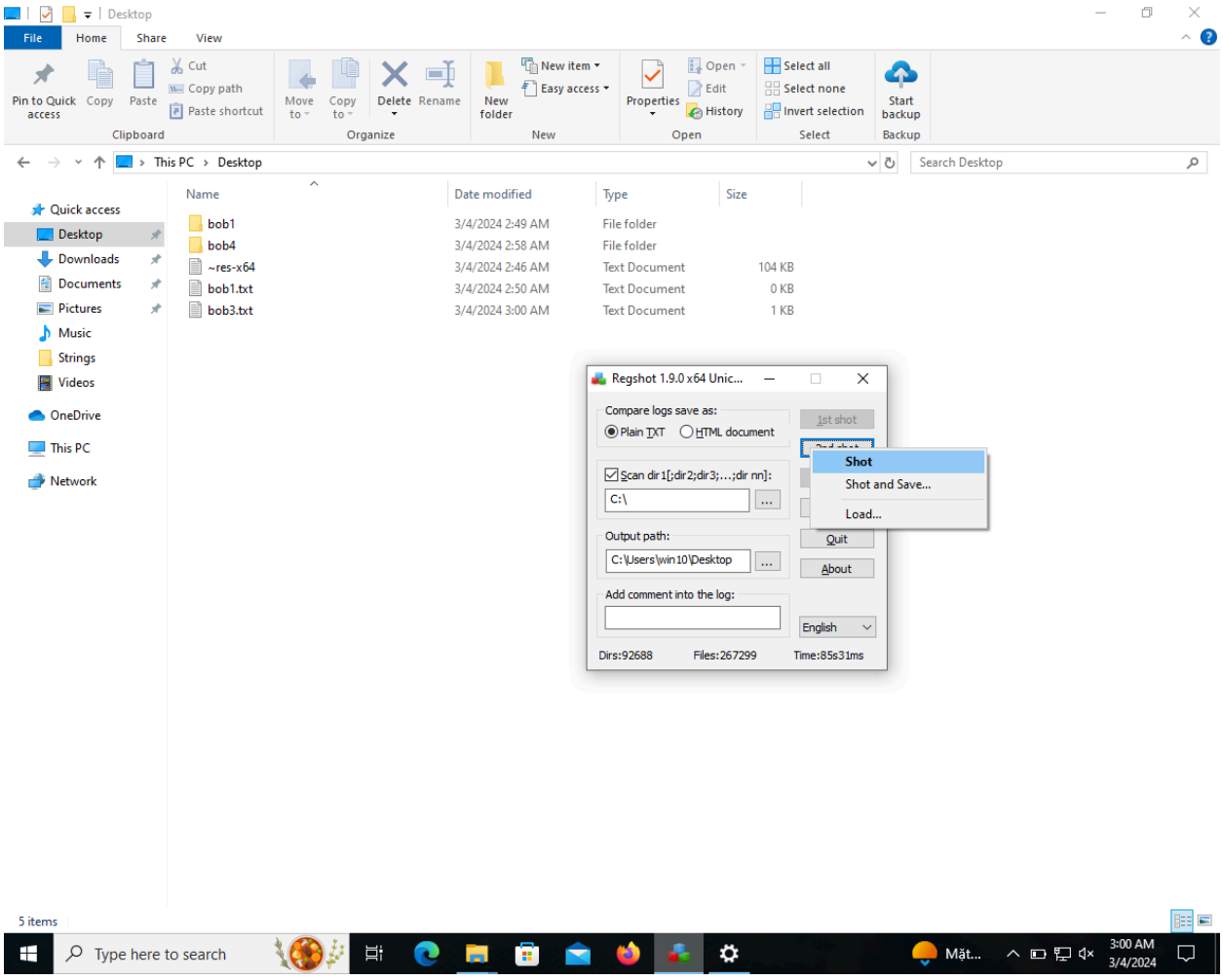

~res-x64 - Notepad
File Edit Format View Help
Find
Find what: wallpaper
Find Next
Cancel
Direction
Up Down
Match case
Wrap around
Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath0: "c:\windows\web\wallpaper\windows\img0.jpg"
Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath0: "c:\windows\web\wallpaper\theme1\img1.jpg"
Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath1: "c:\windows\web\wallpaper\theme1\img1.jpg"
Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath1: "c:\windows\web\wallpaper\windows\img0.jpg"
Ln 148, Col 162
100%
Windows (CRLF)
UTF-16 LE
Type here to search
27°C
2:47 AM
3/4/2024

2a-f,

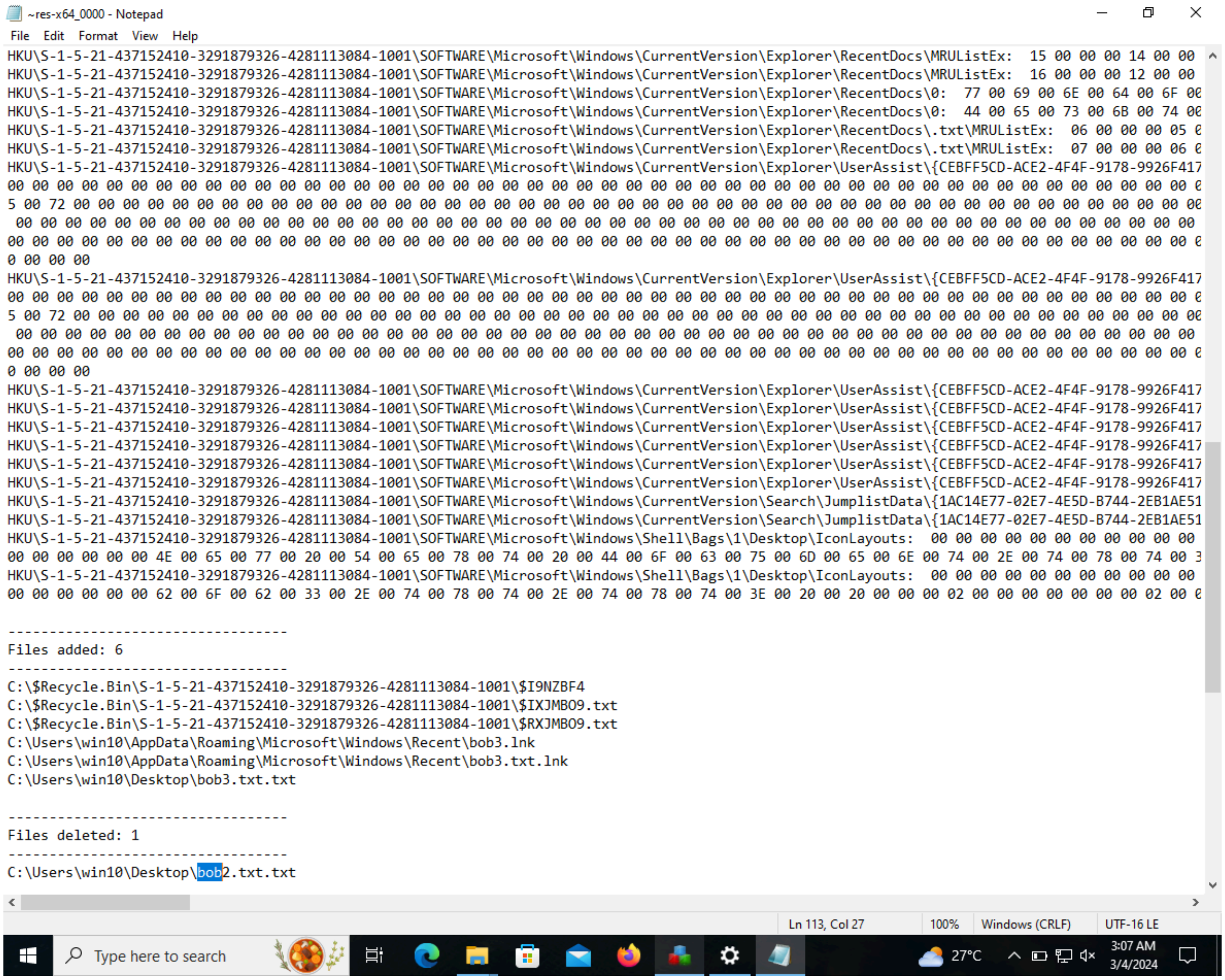

Desktop
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
Start backup
Backup
This PC › Desktop
Search Desktop
Quick access
Desktop
Downloads
Documents
Pictures
Music
Strings
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
~res-x64 3/4/2024 2:46 AM Text Document 104 KB
bob1 3/4/2024 2:49 AM File folder
bob2 3/4/2024 2:50 AM File folder
bob1.txt 3/4/2024 2:50 AM Text Document 0 KB
bob2.txt 3/4/2024 2:54 AM Text Document 0 KB
5 items
Type here to search
Gần...
2:55 AM
3/4/2024

2g-l,


Desktop
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
Start backup
Backup
This PC › Desktop
Search Desktop
Quick access
Desktop
Downloads
Documents
Pictures
Music
Strings
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
~res-x64
3/4/2024 2:46 AM
Text Document
104 KB
bob1
3/4/2024 2:49 AM
File folder
bob2
3/4/2024 2:50 AM
File folder
bob1.txt
3/4/2024 2:50 AM
Text Document
0 KB
bob2.txt
Regshot 1.9.0 x64 Unic...
Compare logs save as:
Plain TXT
HTML document
Scan dir1[;dir2;dir3;...;dir nn]:
C:\
Output path:
C:\Users\win10\Desktop
Add comment into the log:
1st shot
Shot
Shot and Save...
Load...
Clear
Quit
About
English
5 items
Type here to search
Gần...
2:56 AM
3/4/2024


Desktop
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
Start backup
Backup
This PC › Desktop
Search Desktop
Quick access
Desktop
Downloads
Documents
Pictures
Music
Strings
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
bob1 3/4/2024 2:49 AM File folder
bob4 3/4/2024 2:58 AM File folder
~res-x64 3/4/2024 2:46 AM Text Document 104 KB
bob1.txt 3/4/2024 2:50 AM Text Document 0 KB
bob3.txt 3/4/2024 3:00 AM Text Document 1 KB
Regshot 1.9.0 x64 Unic...
Compare logs save as:
Plain TXT
HTML document
1st shot
Shot
Shot and Save...
Load...
Scan dir1[;dir2;dir3;...;dir nn]:
C:\
Output path:
C:\Users\win10\Desktop
Quit
About
Add comment into the log:
English
Dirs:92688
Files:267299
Time:85s31ms
5 items
Type here to search
Mặt...
3:00 AM
3/4/2024

5m,



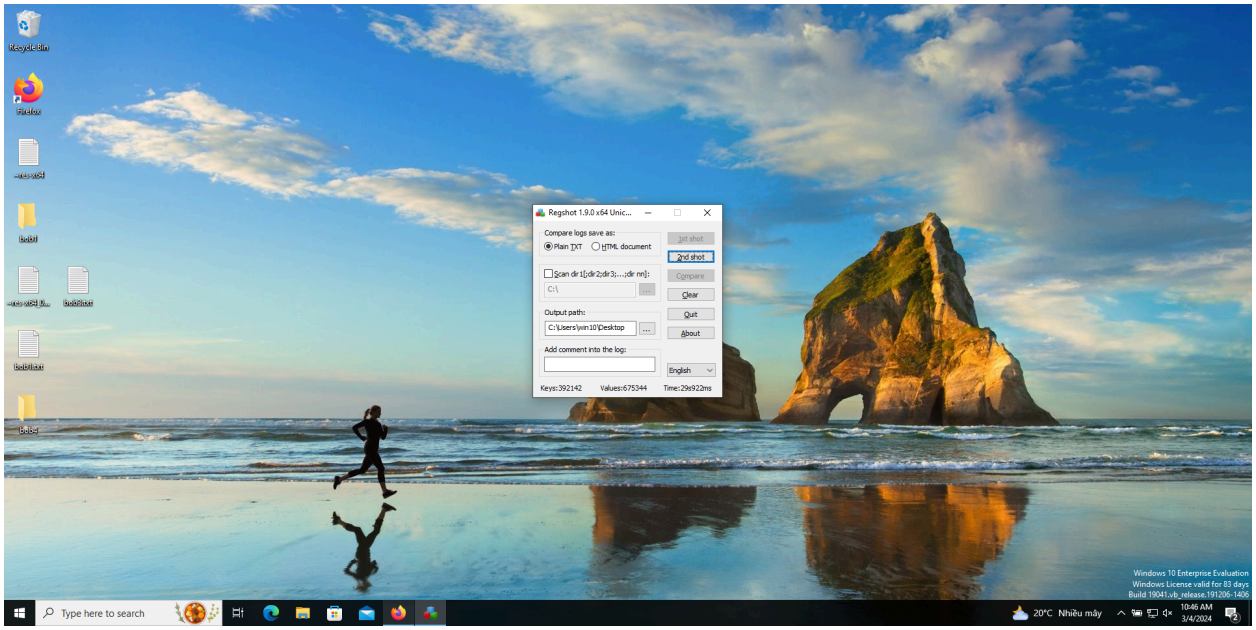
~res-x64_0000 - Notepad

File Edit Format View Help

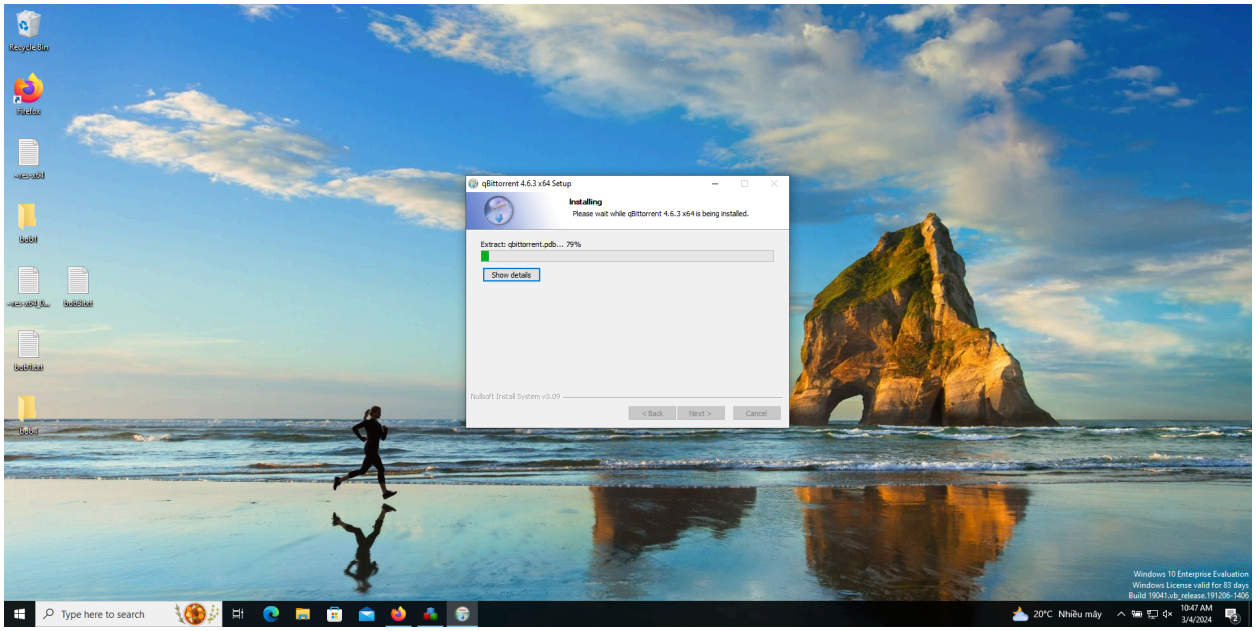
```
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\MRUListEx:  15 00 00 00 14 00 00
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\MRUListEx:  16 00 00 00 12 00 00
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\0:  77 00 69 00 6E 00 64 00 6F 00
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\0:  44 00 65 00 73 00 6B 00 74 00
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt\MRUListEx:  06 00 00 00 05 0
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt\MRUListEx:  07 00 00 00 06 0
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F417
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
5 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
0 00 00 00
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F417
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
5 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
0 00 00 00
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F417
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F417
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F417
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F417
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F417
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F417
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData\{1AC14E77-02E7-4E5D-B744-2EB1AE51
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData\{1AC14E77-02E7-4E5D-B744-2EB1AE51
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\Shell\Bags\1\Desktop\IconLayouts:  00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 4E 00 65 00 77 00 20 00 54 00 65 00 78 00 74 00 20 00 44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2E 00 74 00 78 00 74 00 3
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\Shell\Bags\1\Desktop\IconLayouts:  00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 62 00 6F 00 62 00 33 00 2E 00 74 00 78 00 74 00 2E 00 74 00 78 00 74 00 3E 00 20 00 20 00 00 00 02 00 00 00 00 00 00 00 02 00 0

----------------------------------
Files added: 6
----------------------------------
C:\$Recycle.Bin\S-1-5-21-437152410-3291879326-4281113084-1001\$I9NZBF4
C:\$Recycle.Bin\S-1-5-21-437152410-3291879326-4281113084-1001\$IXJMBO9.txt
C:\$Recycle.Bin\S-1-5-21-437152410-3291879326-4281113084-1001\$RXJMBO9.txt
C:\Users\win10\AppData\Roaming\Microsoft\Windows\Recent\bob3.lnk
C:\Users\win10\AppData\Roaming\Microsoft\Windows\Recent\bob3.txt.lnk
C:\Users\win10\Desktop\bob3.txt.txt

----------------------------------
Files deleted: 1
----------------------------------
C:\Users\win10\Desktop\bob2.txt.txt
```

Ln 113, Col 27 | 100% | Windows (CRLF) | UTF-16 LE

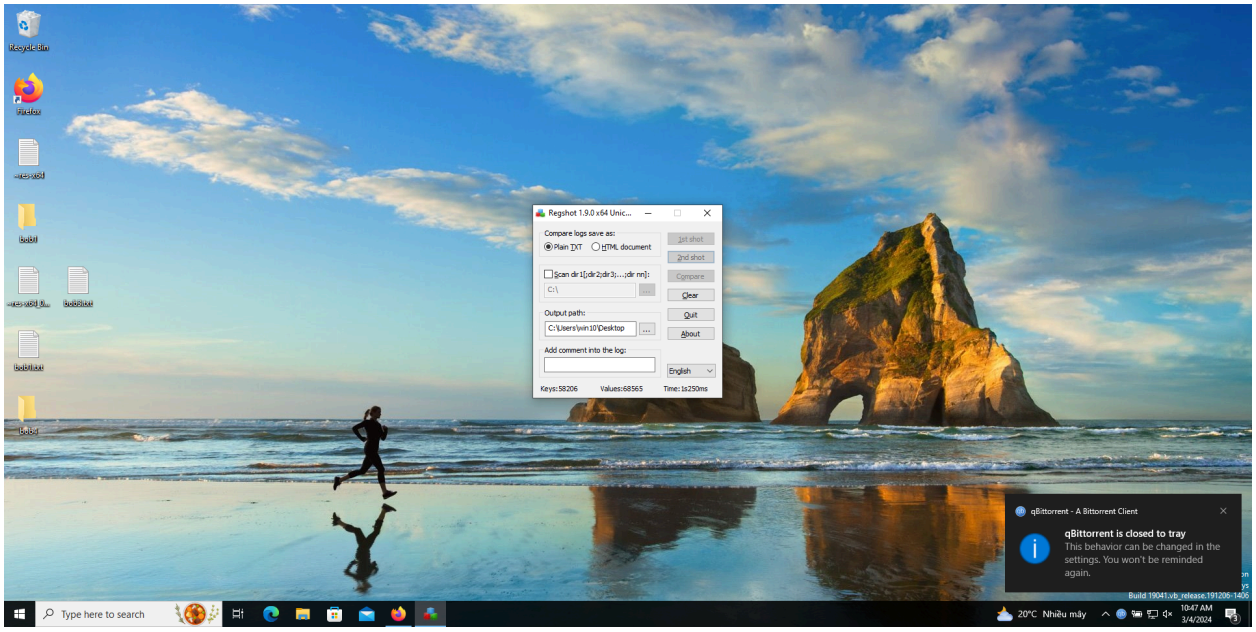
3a,


Regshot 1.9.0 x64 Unic...
Compare logs save as:
Plain TXT
HTML document
1st shot
2nd shot
Compare
Clear
Quit
About
Output path:
C:\Users\win10\Desktop
Add comment into the log:
English
Keys:392142
Values:675344
Time:29m922ms
Type here to search
20°C Nhiều mây
10:46 AM
3/4/2024

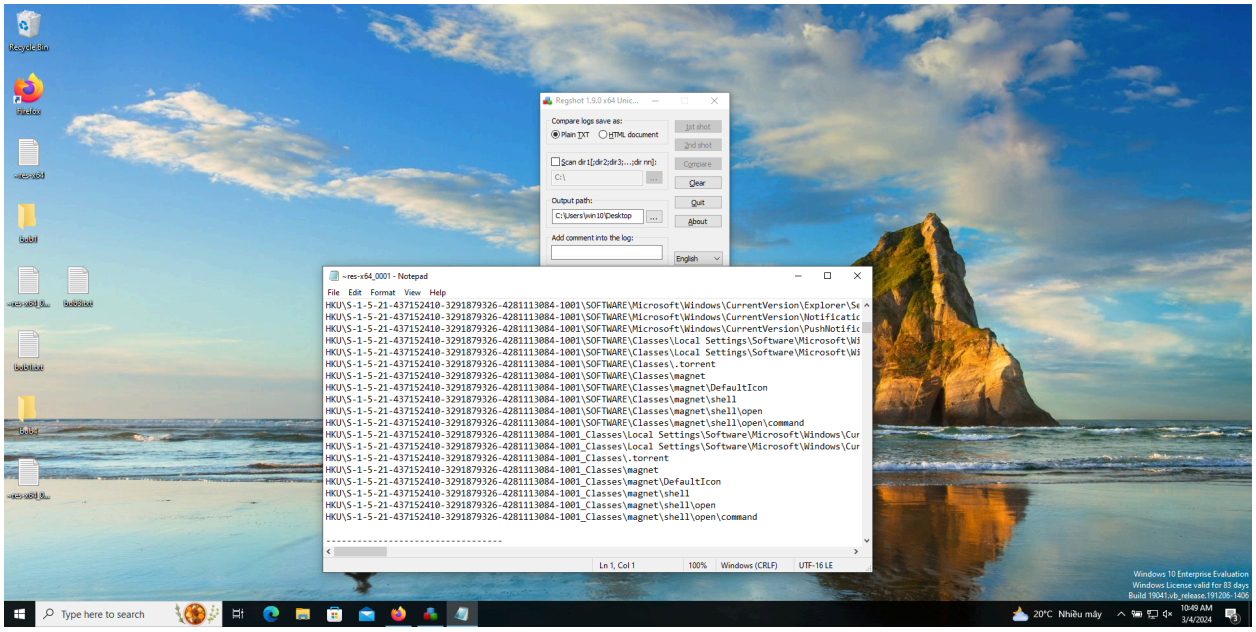
3b,


qBittorrent 4.6.3 x64 Setup
Installing
Please wait while qBittorrent 4.6.3 x64 is being installed.
Extract: qbittorrent.pdb... 79%
Show details
Nullsoft Install System v3.09
< Back
Next >
Cancel
Type here to search
20°C Nhiều mây
10:47 AM
3/4/2024

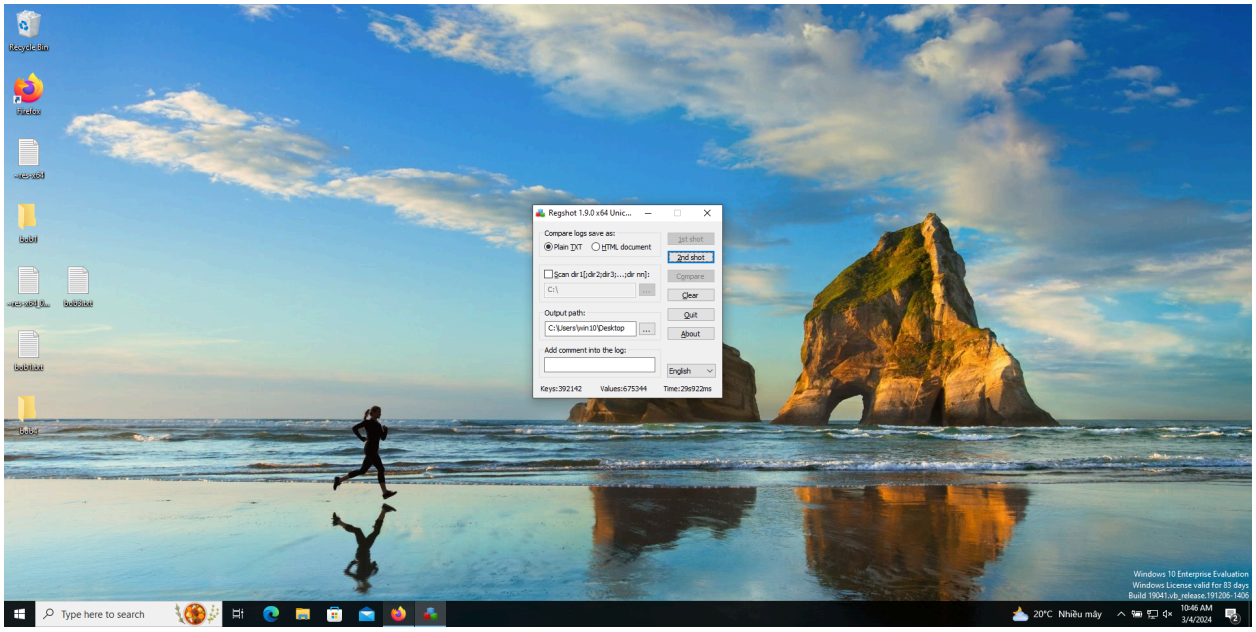
3c,


Regshot 1.9.0 x64 Unic...
Compare logs save as:
Plain TXT
HTML document
1st shot
2nd shot
Compare
Clear
Quit
About
Output path:
C:\Users\win10\Desktop
Add comment into the log:
English
Keys:58206
Values:68565
Time: 1s250ms
qBittorrent - A Bittorrent Client
qBittorrent is closed to tray
This behavior can be changed in the settings. You won't be reminded again.
Type here to search
20°C Nhiều mây
10:47 AM
3/4/2024

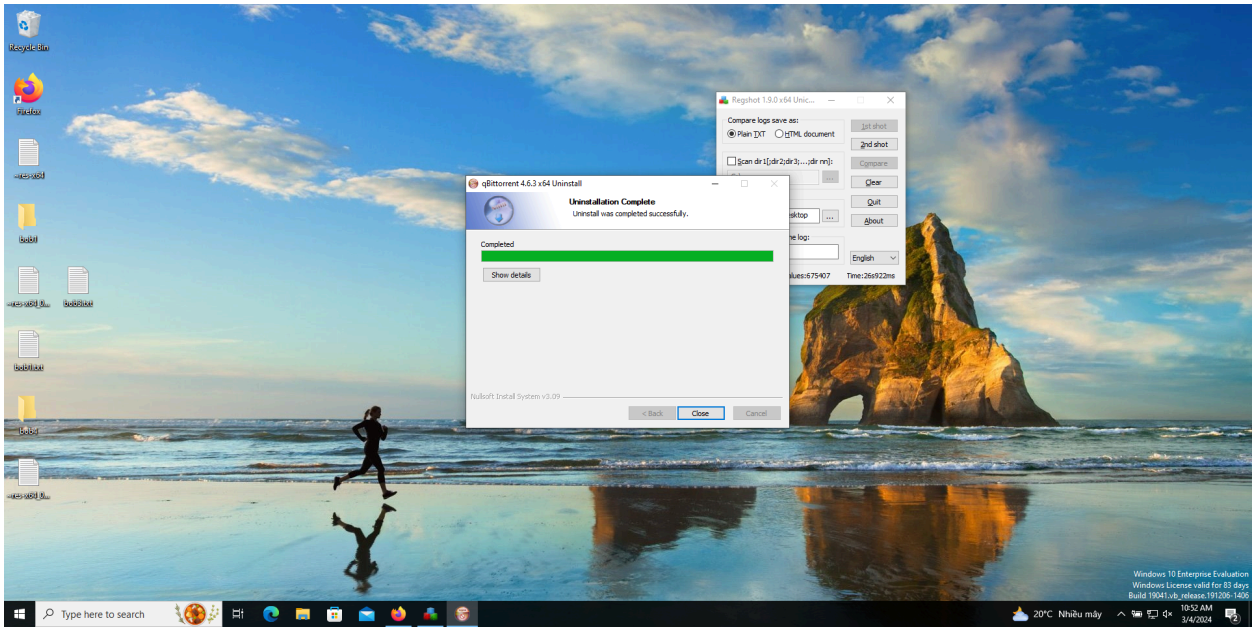
3d,


Regshot 1.9.0 x64 Unic...
~res-x64_0001 - Notepad
File Edit Format View Help
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Se
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Notificatic
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\PushNotific
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Wi
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Wi
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Classes\.torrent
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Classes\magnet
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Classes\magnet\DefaultIcon
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Classes\magnet\shell
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Classes\magnet\shell\open
HKU\S-1-5-21-437152410-3291879326-4281113084-1001\SOFTWARE\Classes\magnet\shell\open\command
HKU\S-1-5-21-437152410-3291879326-4281113084-1001_Classes\Local Settings\Software\Microsoft\Windows\Cur
HKU\S-1-5-21-437152410-3291879326-4281113084-1001_Classes\Local Settings\Software\Microsoft\Windows\Cur
HKU\S-1-5-21-437152410-3291879326-4281113084-1001_Classes\.torrent
HKU\S-1-5-21-437152410-3291879326-4281113084-1001_Classes\magnet
HKU\S-1-5-21-437152410-3291879326-4281113084-1001_Classes\magnet\DefaultIcon
HKU\S-1-5-21-437152410-3291879326-4281113084-1001_Classes\magnet\shell
HKU\S-1-5-21-437152410-3291879326-4281113084-1001_Classes\magnet\shell\open
HKU\S-1-5-21-437152410-3291879326-4281113084-1001_Classes\magnet\shell\open\command
Ln 1, Col 1
100%
Windows (CRLF)
UTF-16 LE
Windows 10 Enterprise Evaluation
Windows License valid for 83 days
Build 19041.vb_release.191206-1406
Type here to search
20°C Nhiều mây
10:49 AM
3/4/2024

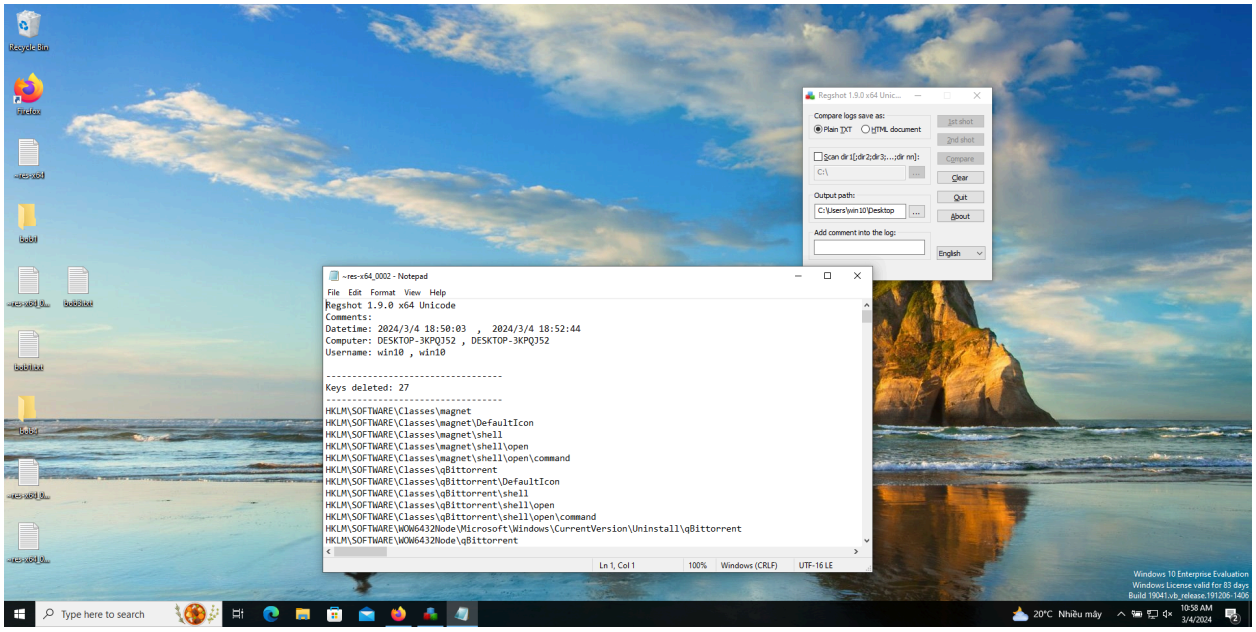
3e,


Regshot 1.9.0 x64 Unic...
Compare logs save as:
Plain TXT
HTML document
1st shot
2nd shot
Compare
Clear
Quit
About
Output path:
C:\Users\win10\Desktop
Add comment into the log:
English
Keys:392142
Values:675344
Time:29s922ms
Type here to search
20°C Nhiều mây
10:46 AM
3/4/2024

3f,

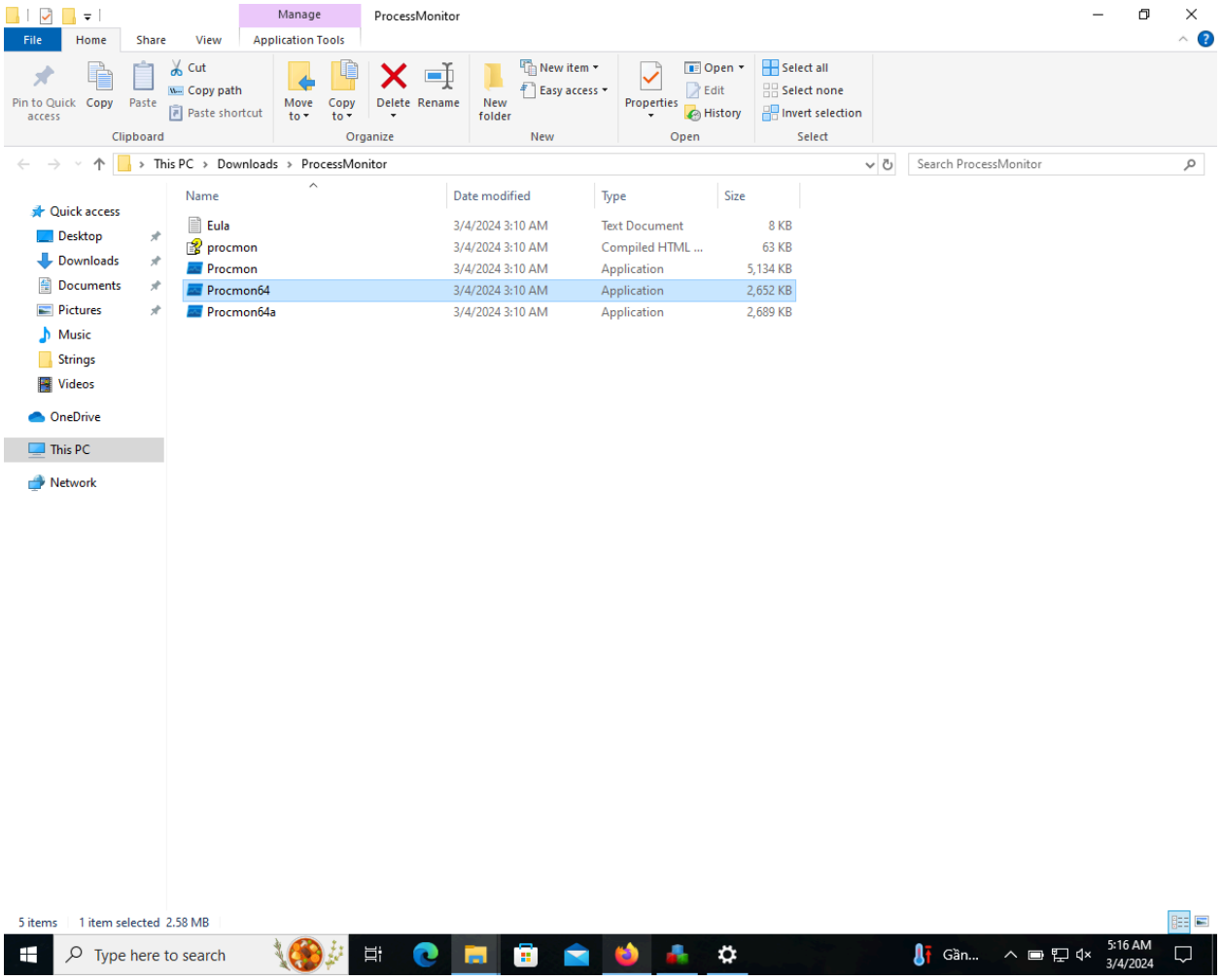

qBittorrent 4.6.3 x64 Uninstall
Uninstallation Complete
Uninstall was completed successfully.
Completed
Show details
Nullsoft Install System v3.09
< Back
Close
Cancel
Regshot 1.9.0 x64 Unic...
Compare logs save as:
Plain TXT
HTML document
1st shot
2nd shot
Compare
Clear
Quit
About
English
Time:26s922ms
Type here to search
20°C Nhiều mây
10:52 AM
3/4/2024

3g & h,

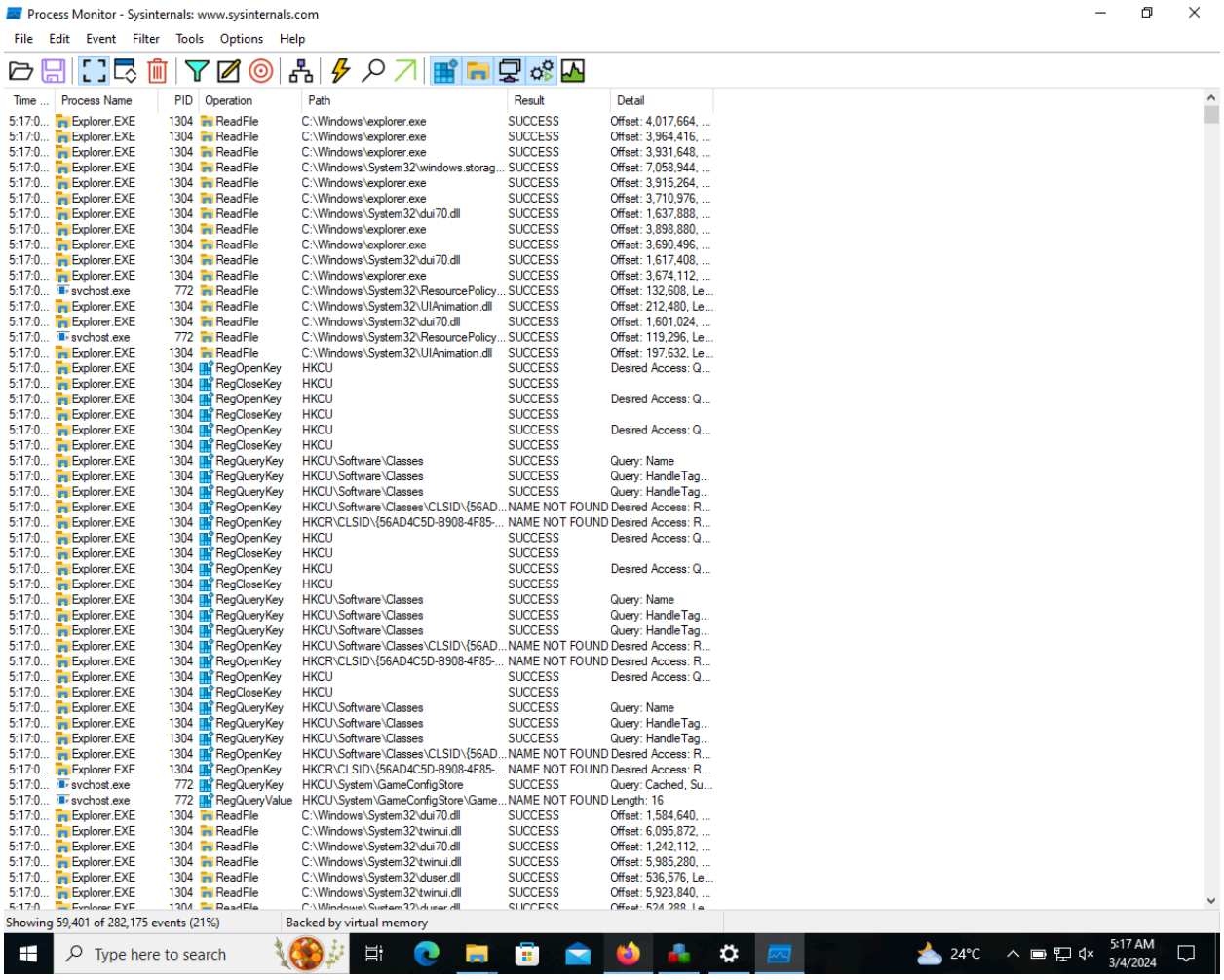

Recycle Bin
Firefox
Regshot 1.9.0 x64 Unic...
Compare logs save as:
Plain TXT
HTML document
1st shot
2nd shot
Compare
Clear
Quit
About
Output path:
C:\Users\win10\Desktop
Add comment into the log:
English
~res-x64_0002 - Notepad
File Edit Format View Help
Regshot 1.9.0 x64 Unicode
Comments:
Datetime: 2024/3/4 18:50:03 , 2024/3/4 18:52:44
Computer: DESKTOP-3KPQJ52 , DESKTOP-3KPQJ52
Username: win10 , win10
Keys deleted: 27
HKLM\SOFTWARE\Classes\magnet
HKLM\SOFTWARE\Classes\magnet\DefaultIcon
HKLM\SOFTWARE\Classes\magnet\shell
HKLM\SOFTWARE\Classes\magnet\shell\open
HKLM\SOFTWARE\Classes\magnet\shell\open\command
HKLM\SOFTWARE\Classes\qBittorrent
HKLM\SOFTWARE\Classes\qBittorrent\DefaultIcon
HKLM\SOFTWARE\Classes\qBittorrent\shell
HKLM\SOFTWARE\Classes\qBittorrent\shell\open
HKLM\SOFTWARE\Classes\qBittorrent\shell\open\command
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\qBittorrent
HKLM\SOFTWARE\WOW6432Node\qBittorrent
Ln 1, Col 1
100%
Windows (CRLF)
UTF-16 LE
Type here to search
20°C Nhiều mây
10:58 AM
3/4/2024
Windows 10 Enterprise Evaluation
Windows License valid for 83 days
Build 19041.vb_release.191206-1406

Lab 15.06:

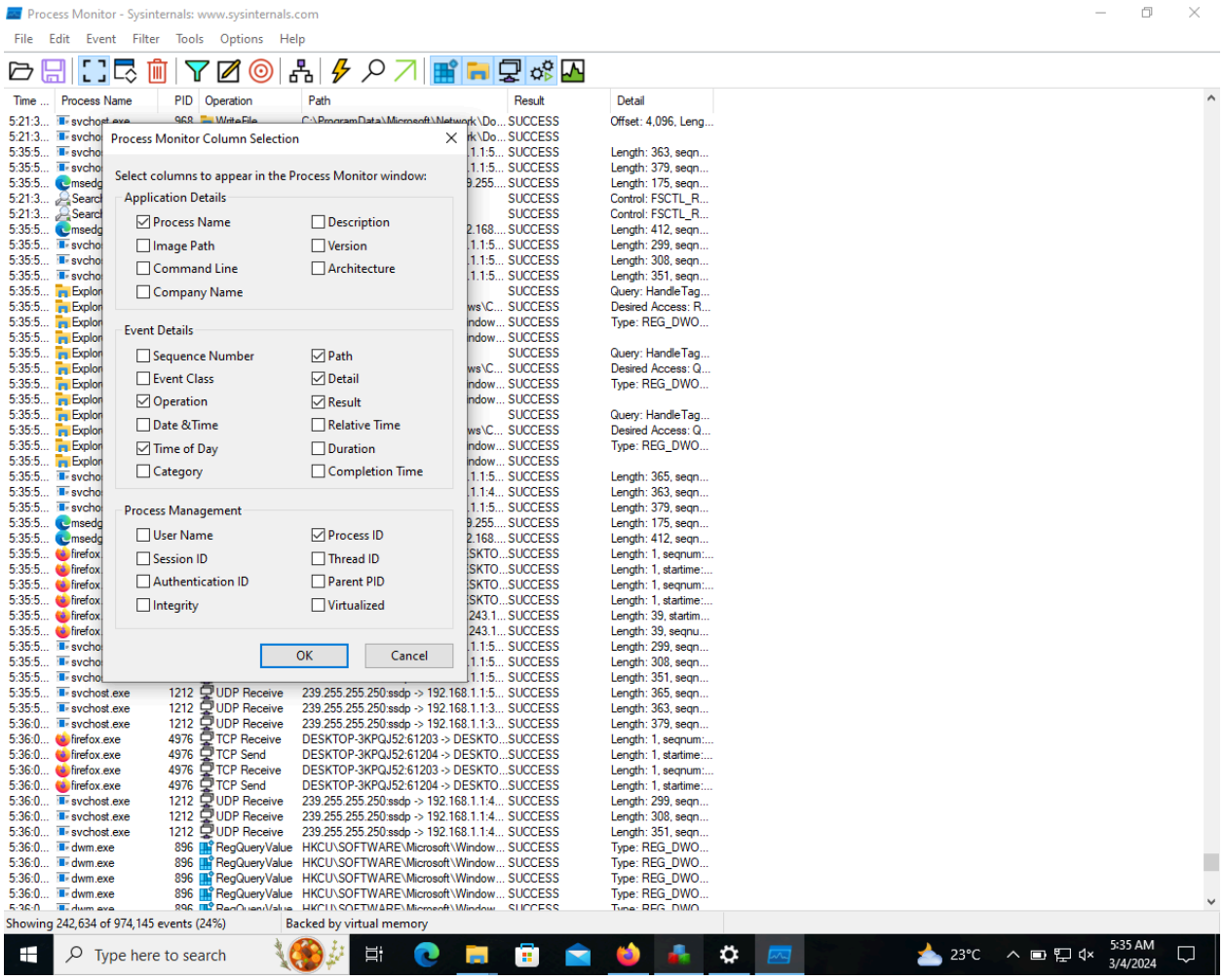
1a&b,


Manage
ProcessMonitor
File
Home
Share
View
Application Tools
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New item
Easy access
New folder
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › Downloads › ProcessMonitor
Search ProcessMonitor
Quick access
Desktop
Downloads
Documents
Pictures
Music
Strings
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Eula 3/4/2024 3:10 AM Text Document 8 KB
procmon 3/4/2024 3:10 AM Compiled HTML ... 63 KB
Procmon 3/4/2024 3:10 AM Application 5,134 KB
Procmon64 3/4/2024 3:10 AM Application 2,652 KB
Procmon64a 3/4/2024 3:10 AM Application 2,689 KB
5 items
1 item selected 2.58 MB
Type here to search
Gần...
5:16 AM
3/4/2024

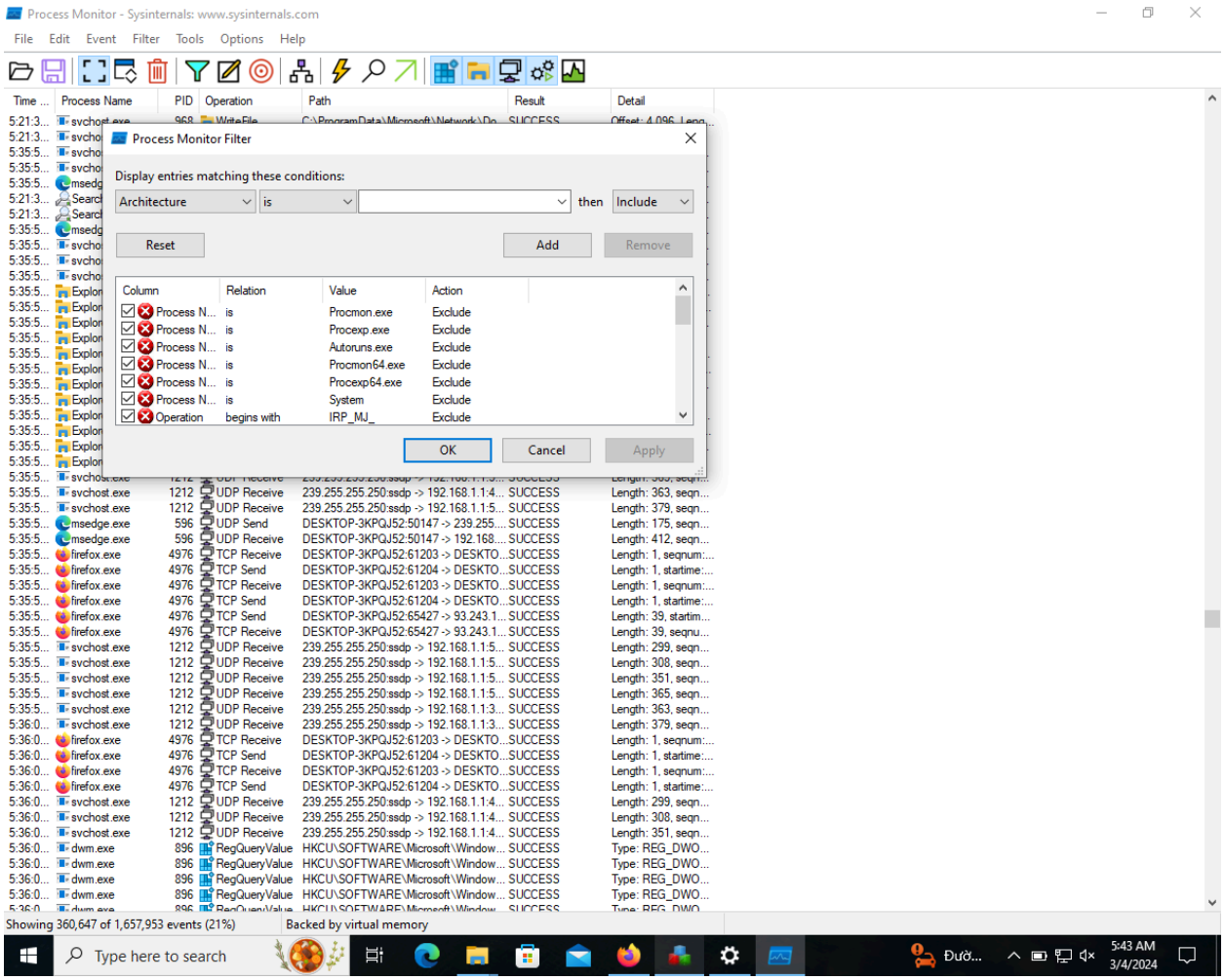
1c&d,


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\explorer.exe SUCCESS Offset: 4,017,664, ...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\explorer.exe SUCCESS Offset: 3,964,416, ...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\explorer.exe SUCCESS Offset: 3,931,648, ...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\System32\windows.storag... SUCCESS Offset: 7,058,944, ...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\explorer.exe SUCCESS Offset: 3,915,264, ...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\explorer.exe SUCCESS Offset: 3,710,976, ...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\System32\dui70.dll SUCCESS Offset: 1,637,888, ...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\explorer.exe SUCCESS Offset: 3,898,880, ...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\explorer.exe SUCCESS Offset: 3,690,496, ...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\System32\dui70.dll SUCCESS Offset: 1,617,408, ...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\explorer.exe SUCCESS Offset: 3,674,112, ...
5:17:0... svchost.exe 772 ReadFile C:\Windows\System32\ResourcePolicy... SUCCESS Offset: 132,608, Le...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\System32\UIAnimation.dll SUCCESS Offset: 212,480, Le...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\System32\dui70.dll SUCCESS Offset: 1,601,024, ...
5:17:0... svchost.exe 772 ReadFile C:\Windows\System32\ResourcePolicy... SUCCESS Offset: 119,296, Le...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\System32\UIAnimation.dll SUCCESS Offset: 197,632, Le...
5:17:0... Explorer.EXE 1304 RegOpenKey HKCU SUCCESS Desired Access: Q...
5:17:0... Explorer.EXE 1304 RegCloseKey HKCU SUCCESS
5:17:0... Explorer.EXE 1304 RegOpenKey HKCU SUCCESS Desired Access: Q...
5:17:0... Explorer.EXE 1304 RegCloseKey HKCU SUCCESS
5:17:0... Explorer.EXE 1304 RegOpenKey HKCU SUCCESS Desired Access: Q...
5:17:0... Explorer.EXE 1304 RegCloseKey HKCU SUCCESS
5:17:0... Explorer.EXE 1304 RegQueryKey HKCU\Software\Classes SUCCESS Query: Name
5:17:0... Explorer.EXE 1304 RegQueryKey HKCU\Software\Classes SUCCESS Query: HandleTag...
5:17:0... Explorer.EXE 1304 RegQueryKey HKCU\Software\Classes SUCCESS Query: HandleTag...
5:17:0... Explorer.EXE 1304 RegOpenKey HKCU\Software\Classes\CLSID\{56AD... NAME NOT FOUND Desired Access: R...
5:17:0... Explorer.EXE 1304 RegOpenKey HKCR\CLSID\{56AD4C5D-B908-4F85-... NAME NOT FOUND Desired Access: R...
5:17:0... Explorer.EXE 1304 RegOpenKey HKCU SUCCESS Desired Access: Q...
5:17:0... Explorer.EXE 1304 RegCloseKey HKCU SUCCESS
5:17:0... Explorer.EXE 1304 RegOpenKey HKCU SUCCESS Desired Access: Q...
5:17:0... Explorer.EXE 1304 RegCloseKey HKCU SUCCESS
5:17:0... Explorer.EXE 1304 RegQueryKey HKCU\Software\Classes SUCCESS Query: Name
5:17:0... Explorer.EXE 1304 RegQueryKey HKCU\Software\Classes SUCCESS Query: HandleTag...
5:17:0... Explorer.EXE 1304 RegQueryKey HKCU\Software\Classes SUCCESS Query: HandleTag...
5:17:0... Explorer.EXE 1304 RegOpenKey HKCU\Software\Classes\CLSID\{56AD... NAME NOT FOUND Desired Access: R...
5:17:0... Explorer.EXE 1304 RegOpenKey HKCR\CLSID\{56AD4C5D-B908-4F85-... NAME NOT FOUND Desired Access: R...
5:17:0... Explorer.EXE 1304 RegOpenKey HKCU SUCCESS Desired Access: Q...
5:17:0... Explorer.EXE 1304 RegCloseKey HKCU SUCCESS
5:17:0... Explorer.EXE 1304 RegQueryKey HKCU\Software\Classes SUCCESS Query: Name
5:17:0... Explorer.EXE 1304 RegQueryKey HKCU\Software\Classes SUCCESS Query: HandleTag...
5:17:0... Explorer.EXE 1304 RegQueryKey HKCU\Software\Classes SUCCESS Query: HandleTag...
5:17:0... Explorer.EXE 1304 RegOpenKey HKCU\Software\Classes\CLSID\{56AD... NAME NOT FOUND Desired Access: R...
5:17:0... Explorer.EXE 1304 RegOpenKey HKCR\CLSID\{56AD4C5D-B908-4F85-... NAME NOT FOUND Desired Access: R...
5:17:0... svchost.exe 772 RegQueryKey HKCU\System\GameConfigStore SUCCESS Query: Cached, Su...
5:17:0... svchost.exe 772 RegQueryValue HKCU\System\GameConfigStore\Game... NAME NOT FOUND Length: 16
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\System32\dui70.dll SUCCESS Offset: 1,584,640, ...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\System32\twinui.dll SUCCESS Offset: 6,095,872, ...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\System32\dui70.dll SUCCESS Offset: 1,242,112, ...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\System32\twinui.dll SUCCESS Offset: 5,985,280, ...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\System32\duser.dll SUCCESS Offset: 536,576, Le...
5:17:0... Explorer.EXE 1304 ReadFile C:\Windows\System32\twinui.dll SUCCESS Offset: 5,923,840, ...
Showing 59,401 of 282,175 events (21%)
Backed by virtual memory
Type here to search
24°C
5:17 AM
3/4/2024

1e,


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Process Monitor Column Selection
Select columns to appear in the Process Monitor window:
Application Details
Process Name
Description
Image Path
Version
Command Line
Architecture
Company Name
Event Details
Sequence Number
Path
Event Class
Detail
Operation
Result
Date &Time
Relative Time
Time of Day
Duration
Category
Completion Time
Process Management
User Name
Process ID
Session ID
Thread ID
Authentication ID
Parent PID
Integrity
Virtualized
OK
Cancel
Showing 242,634 of 974,145 events (24%)
Backed by virtual memory
Type here to search
23°C
5:35 AM
3/4/2024

2a&b&c,

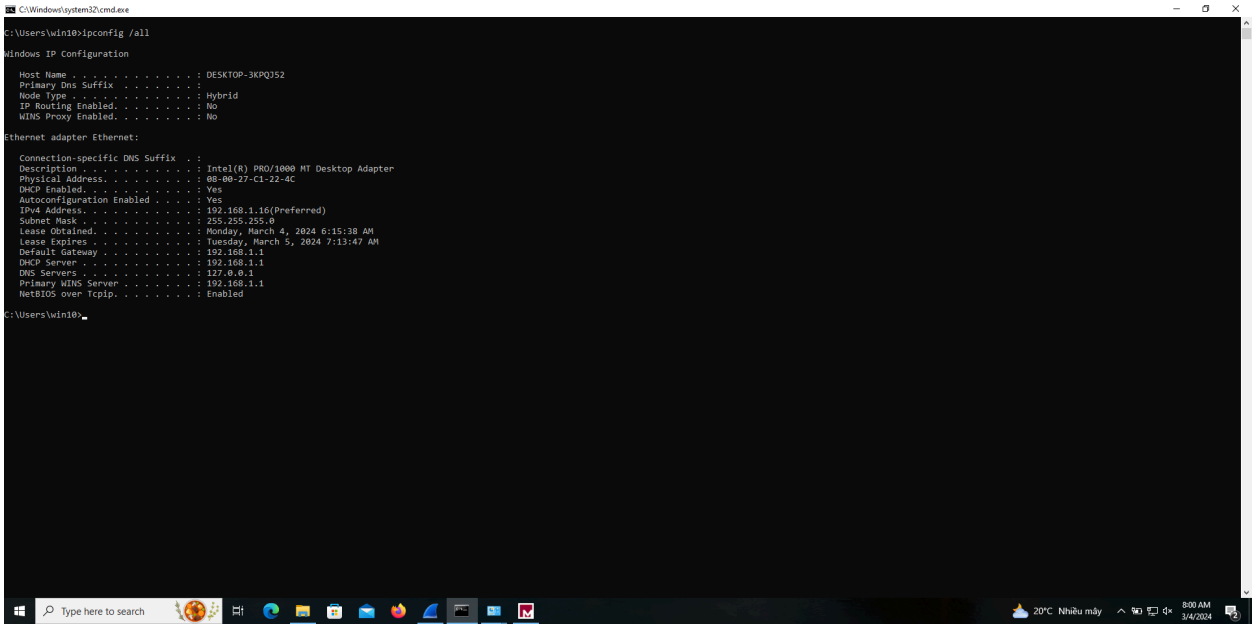


2d, Bộ lọc là “Event Class is Registry then Include”. Bộ lọc này được chọn để kiểm tra xem có thay đổi nào trong Registry và theo dõi hoạt động bất thường liên quan đến Registry

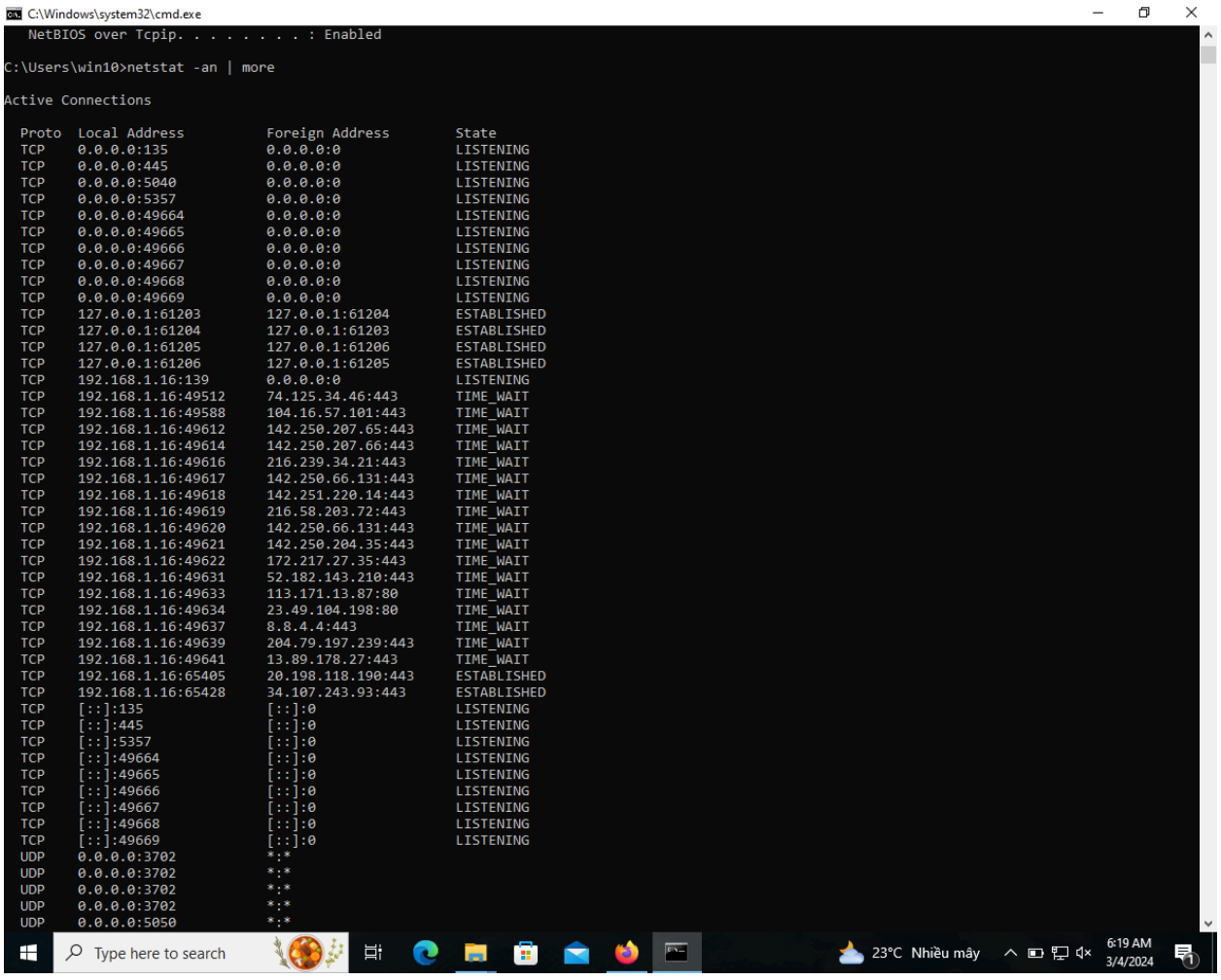
2e, 3 bộ lọc được sử dụng là “Event Class is Registry then Include”, “Architecture is 65 bit then Include” và “Date & Time more than 3/4/2024 6:00:00 AM then Exclude”. Bộ lọc này được sử dụng khi ta biết máy bị tấn công vào ngày 4/3/2024 6h sáng và mục tiêu sử dụng kiến trúc 64 bit thì ta lần tìm sự kiện trước đó với các tiến trình 64 bit và kiểm tra Event Class là Registry

Lab 15.07:

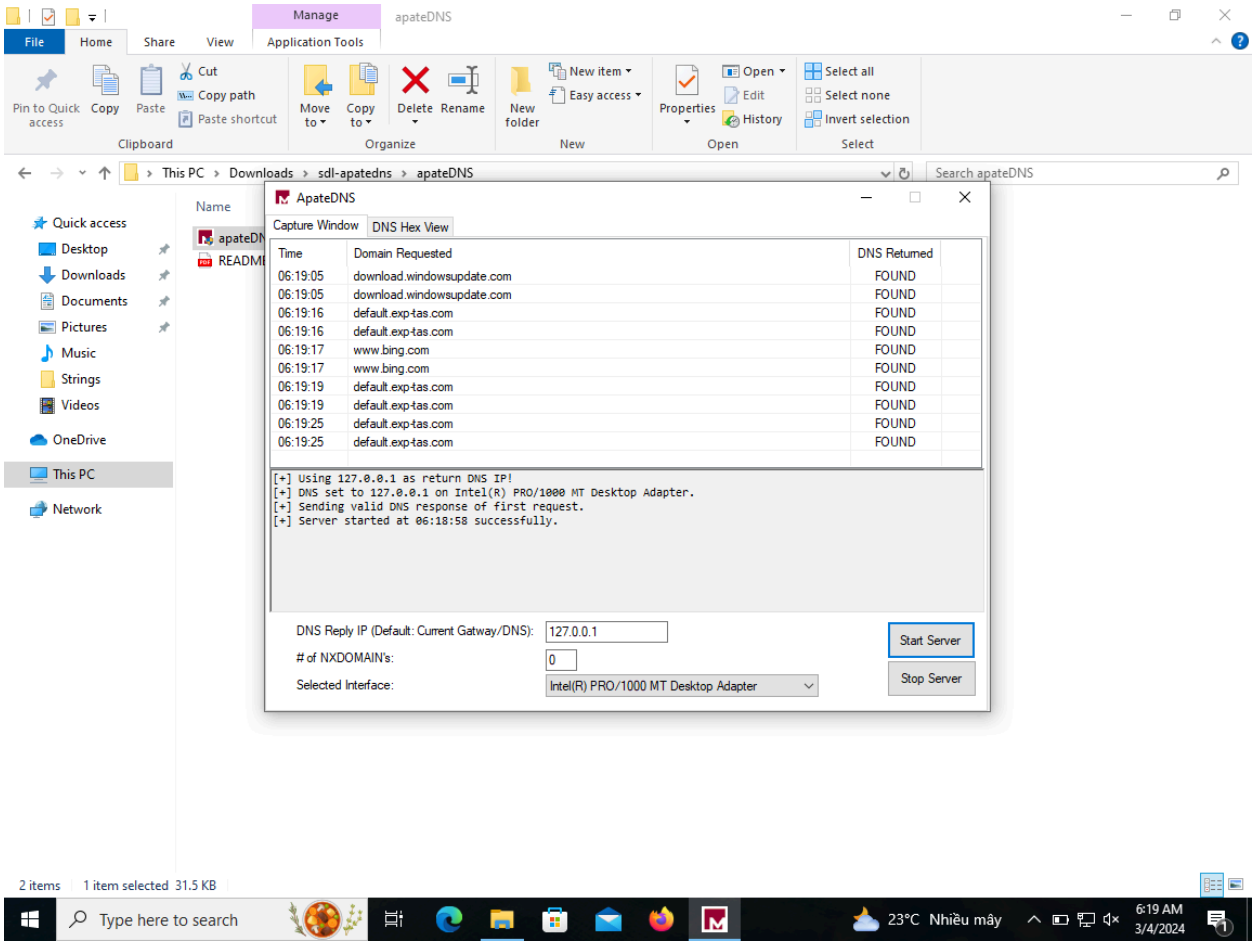
1a,


C:\Windows\system32\cmd.exe
C:\Users\win10>ipconfig /all
Windows IP Configuration
Host Name . . . . . : DESKTOP-3KPQJ52
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-C1-22-4C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.1.16(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, March 4, 2024 6:15:38 AM
Lease Expires . . . . . : Tuesday, March 5, 2024 7:13:47 AM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 127.0.0.1
Primary WINS Server . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
C:\Users\win10>
Type here to search
20°C Nhiều mây
8:00 AM
3/4/2024

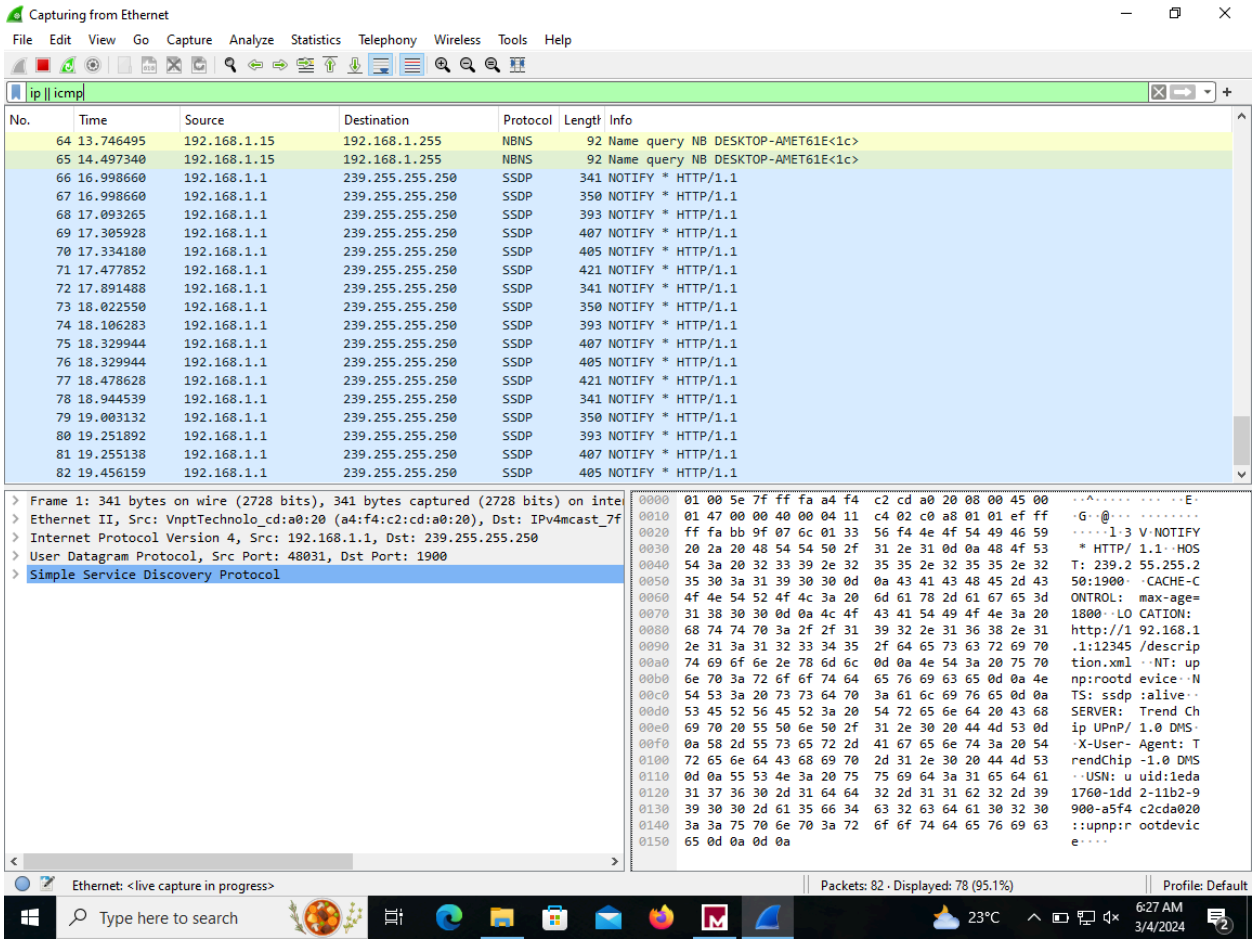
1b,


C:\Windows\system32\cmd.exe
NetBIOS over Tcpip. . . . . : Enabled
C:\Users\win10>netstat -an | more
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49669 0.0.0.0:0 LISTENING
TCP 127.0.0.1:61203 127.0.0.1:61204 ESTABLISHED
TCP 127.0.0.1:61204 127.0.0.1:61203 ESTABLISHED
TCP 127.0.0.1:61205 127.0.0.1:61206 ESTABLISHED
TCP 127.0.0.1:61206 127.0.0.1:61205 ESTABLISHED
TCP 192.168.1.16:139 0.0.0.0:0 LISTENING
TCP 192.168.1.16:49512 74.125.34.46:443 TIME_WAIT
TCP 192.168.1.16:49588 104.16.57.101:443 TIME_WAIT
TCP 192.168.1.16:49612 142.250.207.65:443 TIME_WAIT
TCP 192.168.1.16:49614 142.250.207.66:443 TIME_WAIT
TCP 192.168.1.16:49616 216.239.34.21:443 TIME_WAIT
TCP 192.168.1.16:49617 142.250.66.131:443 TIME_WAIT
TCP 192.168.1.16:49618 142.251.220.14:443 TIME_WAIT
TCP 192.168.1.16:49619 216.58.203.72:443 TIME_WAIT
TCP 192.168.1.16:49620 142.250.66.131:443 TIME_WAIT
TCP 192.168.1.16:49621 142.250.204.35:443 TIME_WAIT
TCP 192.168.1.16:49622 172.217.27.35:443 TIME_WAIT
TCP 192.168.1.16:49631 52.182.143.210:443 TIME_WAIT
TCP 192.168.1.16:49633 113.171.13.87:80 TIME_WAIT
TCP 192.168.1.16:49634 23.49.104.198:80 TIME_WAIT
TCP 192.168.1.16:49637 8.8.4.4:443 TIME_WAIT
TCP 192.168.1.16:49639 204.79.197.239:443 TIME_WAIT
TCP 192.168.1.16:49641 13.89.178.27:443 TIME_WAIT
TCP 192.168.1.16:65405 20.198.118.190:443 ESTABLISHED
TCP 192.168.1.16:65428 34.107.243.93:443 ESTABLISHED
TCP [::]:135 [::]:0 LISTENING
TCP [::]:445 [::]:0 LISTENING
TCP [::]:5357 [::]:0 LISTENING
TCP [::]:49664 [::]:0 LISTENING
TCP [::]:49665 [::]:0 LISTENING
TCP [::]:49666 [::]:0 LISTENING
TCP [::]:49667 [::]:0 LISTENING
TCP [::]:49668 [::]:0 LISTENING
TCP [::]:49669 [::]:0 LISTENING
UDP 0.0.0.0:3702 *:*
UDP 0.0.0.0:3702 *:*
UDP 0.0.0.0:3702 *:*
UDP 0.0.0.0:3702 *:*
UDP 0.0.0.0:5050 *:*
Type here to search
23°C Nhiều mây
6:19 AM
3/4/2024

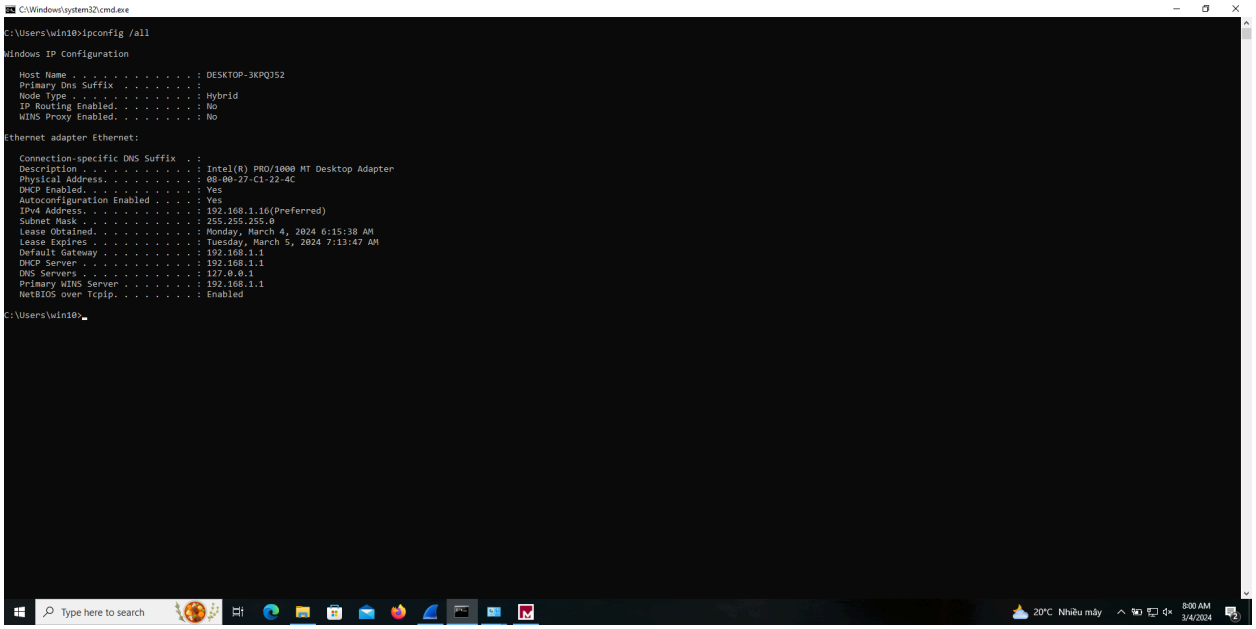
1c,

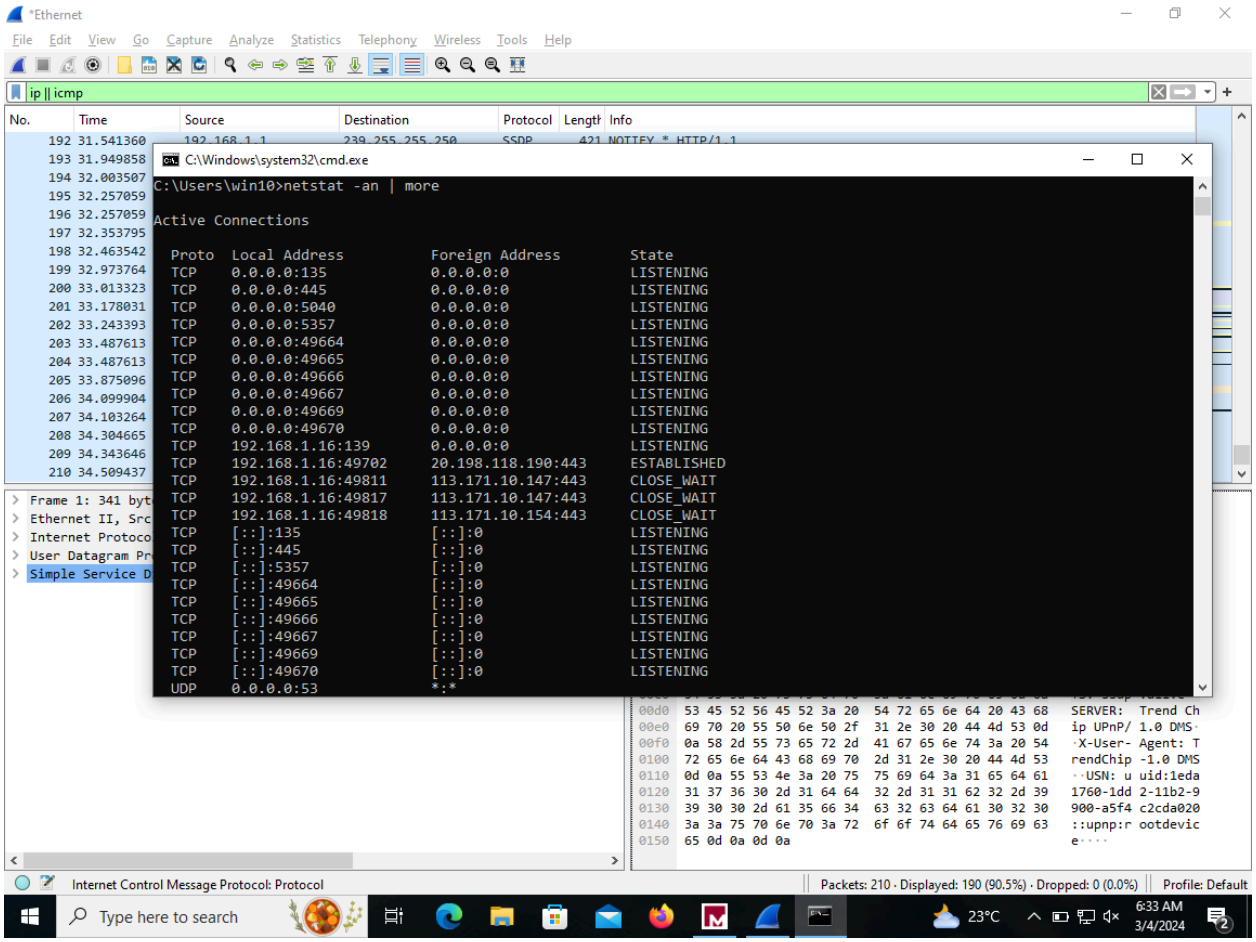

Manage
apateDNS
File
Home
Share
View
Application Tools
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New item
Easy access
New folder
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › Downloads › sdl-apatedns › apateDNS
Search apateDNS
Quick access
Desktop
Downloads
Documents
Pictures
Music
Strings
Videos
OneDrive
This PC
Network
Name
apateDN
READM
ApateDNS
Capture Window
DNS Hex View
Time
Domain Requested
DNS Returned
06:19:05 download.windowsupdate.com FOUND
06:19:05 download.windowsupdate.com FOUND
06:19:16 default.exp-tas.com FOUND
06:19:16 default.exp-tas.com FOUND
06:19:17 www.bing.com FOUND
06:19:17 www.bing.com FOUND
06:19:19 default.exp-tas.com FOUND
06:19:19 default.exp-tas.com FOUND
06:19:25 default.exp-tas.com FOUND
06:19:25 default.exp-tas.com FOUND
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Desktop Adapter.
[+] Sending valid DNS response of first request.
[+] Server started at 06:18:58 successfully.
DNS Reply IP (Default: Current Gatway/DNS):
127.0.0.1
# of NXDOMAIN's:
0
Selected Interface:
Intel(R) PRO/1000 MT Desktop Adapter
Start Server
Stop Server
2 items
1 item selected 31.5 KB
Type here to search
23°C Nhiều mây
6:19 AM
3/4/2024

2a,

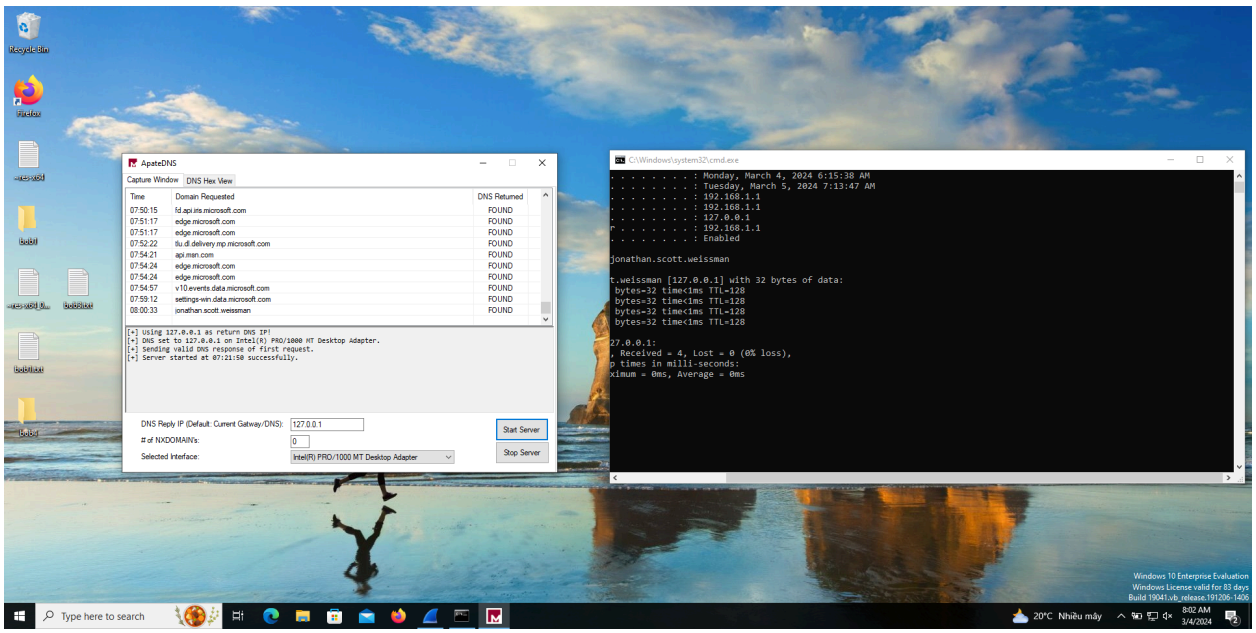

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip || icmp
No. Time Source Destination Protocol Length Info
64 13.746495 192.168.1.15 192.168.1.255 NBNS 92 Name query NB DESKTOP-AMET61E<1c>
65 14.497340 192.168.1.15 192.168.1.255 NBNS 92 Name query NB DESKTOP-AMET61E<1c>
66 16.998660 192.168.1.1 239.255.255.250 SSDP 341 NOTIFY * HTTP/1.1
67 16.998660 192.168.1.1 239.255.255.250 SSDP 350 NOTIFY * HTTP/1.1
68 17.093265 192.168.1.1 239.255.255.250 SSDP 393 NOTIFY * HTTP/1.1
69 17.305928 192.168.1.1 239.255.255.250 SSDP 407 NOTIFY * HTTP/1.1
70 17.334180 192.168.1.1 239.255.255.250 SSDP 405 NOTIFY * HTTP/1.1
71 17.477852 192.168.1.1 239.255.255.250 SSDP 421 NOTIFY * HTTP/1.1
72 17.891488 192.168.1.1 239.255.255.250 SSDP 341 NOTIFY * HTTP/1.1
73 18.022550 192.168.1.1 239.255.255.250 SSDP 350 NOTIFY * HTTP/1.1
74 18.106283 192.168.1.1 239.255.255.250 SSDP 393 NOTIFY * HTTP/1.1
75 18.329944 192.168.1.1 239.255.255.250 SSDP 407 NOTIFY * HTTP/1.1
76 18.329944 192.168.1.1 239.255.255.250 SSDP 405 NOTIFY * HTTP/1.1
77 18.478628 192.168.1.1 239.255.255.250 SSDP 421 NOTIFY * HTTP/1.1
78 18.944539 192.168.1.1 239.255.255.250 SSDP 341 NOTIFY * HTTP/1.1
79 19.003132 192.168.1.1 239.255.255.250 SSDP 350 NOTIFY * HTTP/1.1
80 19.251892 192.168.1.1 239.255.255.250 SSDP 393 NOTIFY * HTTP/1.1
81 19.255138 192.168.1.1 239.255.255.250 SSDP 407 NOTIFY * HTTP/1.1
82 19.456159 192.168.1.1 239.255.255.250 SSDP 405 NOTIFY * HTTP/1.1
Frame 1: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on inte
Ethernet II, Src: VnptTechnolo_cd:a0:20 (a4:f4:c2:cd:a0:20), Dst: IPv4mcast_7f
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 48031, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa a4 f4 c2 cd a0 20 08 00 45 00
0010 01 47 00 00 40 00 04 11 c4 02 c0 a8 01 01 ef ff
0020 ff fa bb 9f 07 6c 01 33 56 f4 4e 4f 54 49 46 59
0030 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 4f 53
0040 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 2e 32
0050 35 30 3a 31 39 30 30 0d 0a 43 41 43 48 45 2d 43
0060 4f 4e 54 52 4f 4c 3a 20 6d 61 78 2d 61 67 65 3d
0070 31 38 30 30 0d 0a 4c 4f 43 41 54 49 4f 4e 3a 20
0080 68 74 74 70 3a 2f 2f 31 39 32 2e 31 36 38 2e 31
0090 2e 31 3a 31 32 33 34 35 2f 64 65 73 63 72 69 70
00a0 74 69 6f 6e 2e 78 6d 6c 0d 0a 4e 54 3a 20 75 70
00b0 6e 70 3a 72 6f 6f 74 64 65 76 69 63 65 0d 0a 4e
00c0 54 53 3a 20 73 73 64 70 3a 61 6c 69 76 65 0d 0a
00d0 53 45 52 56 45 52 3a 20 54 72 65 6e 64 20 43 68
00e0 69 70 20 55 50 6e 50 2f 31 2e 30 20 44 4d 53 0d
00f0 0a 58 2d 55 73 65 72 2d 41 67 65 6e 74 3a 20 54
0100 72 65 6e 64 43 68 69 70 2d 31 2e 30 20 44 4d 53
0110 0d 0a 55 53 4e 3a 20 75 75 69 64 3a 31 65 64 61
0120 31 37 36 30 2d 31 64 64 32 2d 31 31 62 32 2d 39
0130 39 30 30 2d 61 35 66 34 63 32 63 64 61 30 32 30
0140 3a 3a 75 70 6e 70 3a 72 6f 6f 74 64 65 76 69 63
0150 65 0d 0a 0d 0a
Ethernet: <live capture in progress>
Packets: 82 · Displayed: 78 (95.1%)
Profile: Default
Type here to search
23°C
6:27 AM
3/4/2024

2b,

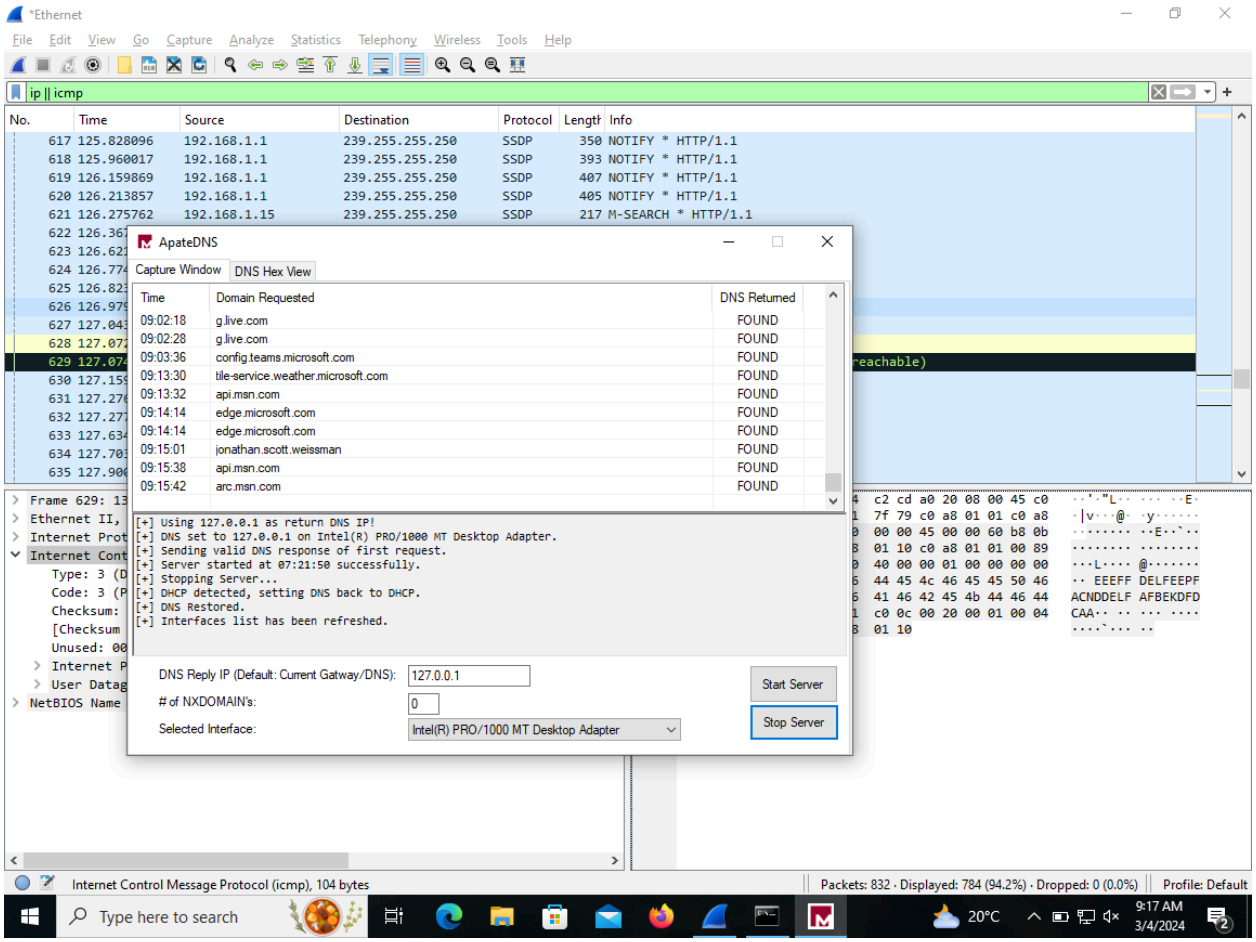

C:\Windows\system32\cmd.exe
C:\Users\win10>ipconfig /all
Windows IP Configuration
Host Name . . . . . : DESKTOP-3KPQJ52
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-C1-22-4C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.1.16(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, March 4, 2024 6:15:38 AM
Lease Expires . . . . . : Tuesday, March 5, 2024 7:13:47 AM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 127.0.0.1
Primary WINS Server . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
C:\Users\win10>
Type here to search
20°C Nhiều mây
8:00 AM
3/4/2024


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip || icmp
No. Time Source Destination Protocol Lengt Info
192 31.541360 192.168.1.1 239.255.255.250 SSDP 421 NOTIFY * HTTP/1.1
193 31.949858
194 32.003507
195 32.257059
196 32.257059
197 32.353795
198 32.463542
199 32.973764
200 33.013323
201 33.178031
202 33.243393
203 33.487613
204 33.487613
205 33.875096
206 34.099904
207 34.103264
208 34.304665
209 34.343646
210 34.509437
C:\Windows\system32\cmd.exe
C:\Users\win10>netstat -an | more
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49669 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49670 0.0.0.0:0 LISTENING
TCP 192.168.1.16:139 0.0.0.0:0 LISTENING
TCP 192.168.1.16:49702 20.198.118.190:443 ESTABLISHED
TCP 192.168.1.16:49811 113.171.10.147:443 CLOSE_WAIT
TCP 192.168.1.16:49817 113.171.10.147:443 CLOSE_WAIT
TCP 192.168.1.16:49818 113.171.10.154:443 CLOSE_WAIT
TCP [::]:135 [::]:0 LISTENING
TCP [::]:445 [::]:0 LISTENING
TCP [::]:5357 [::]:0 LISTENING
TCP [::]:49664 [::]:0 LISTENING
TCP [::]:49665 [::]:0 LISTENING
TCP [::]:49666 [::]:0 LISTENING
TCP [::]:49667 [::]:0 LISTENING
TCP [::]:49669 [::]:0 LISTENING
TCP [::]:49670 [::]:0 LISTENING
UDP 0.0.0.0:53 *:*
Frame 1: 341 byt
Ethernet II, Src
Internet Protoco
User Datagram Pr
Simple Service D
00d0 53 45 52 56 45 52 3a 20 54 72 65 6e 64 20 43 68 SERVER: Trend Ch
00e0 69 70 20 55 50 6e 50 2f 31 2e 30 20 44 4d 53 0d ip UPnP/ 1.0 DMS·
00f0 0a 58 2d 55 73 65 72 2d 41 67 65 6e 74 3a 20 54 ·X-User- Agent: T
0100 72 65 6e 64 43 68 69 70 2d 31 2e 30 20 44 4d 53 rendChip -1.0 DMS
0110 0d 0a 55 53 4e 3a 20 75 75 69 64 3a 31 65 64 61 ··USN: u uid:1eda
0120 31 37 36 30 2d 31 64 64 32 2d 31 31 62 32 2d 39 1760-1dd 2-11b2-9
0130 39 30 30 2d 61 35 66 34 63 32 63 64 61 30 32 30 900-a5f4 c2cda020
0140 3a 3a 75 70 6e 70 3a 72 6f 6f 74 64 65 76 69 63 ::upnp:r ootdevic
0150 65 0d 0a 0d 0a e····
Internet Control Message Protocol: Protocol
Packets: 210 · Displayed: 190 (90.5%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
23°C
6:33 AM
3/4/2024

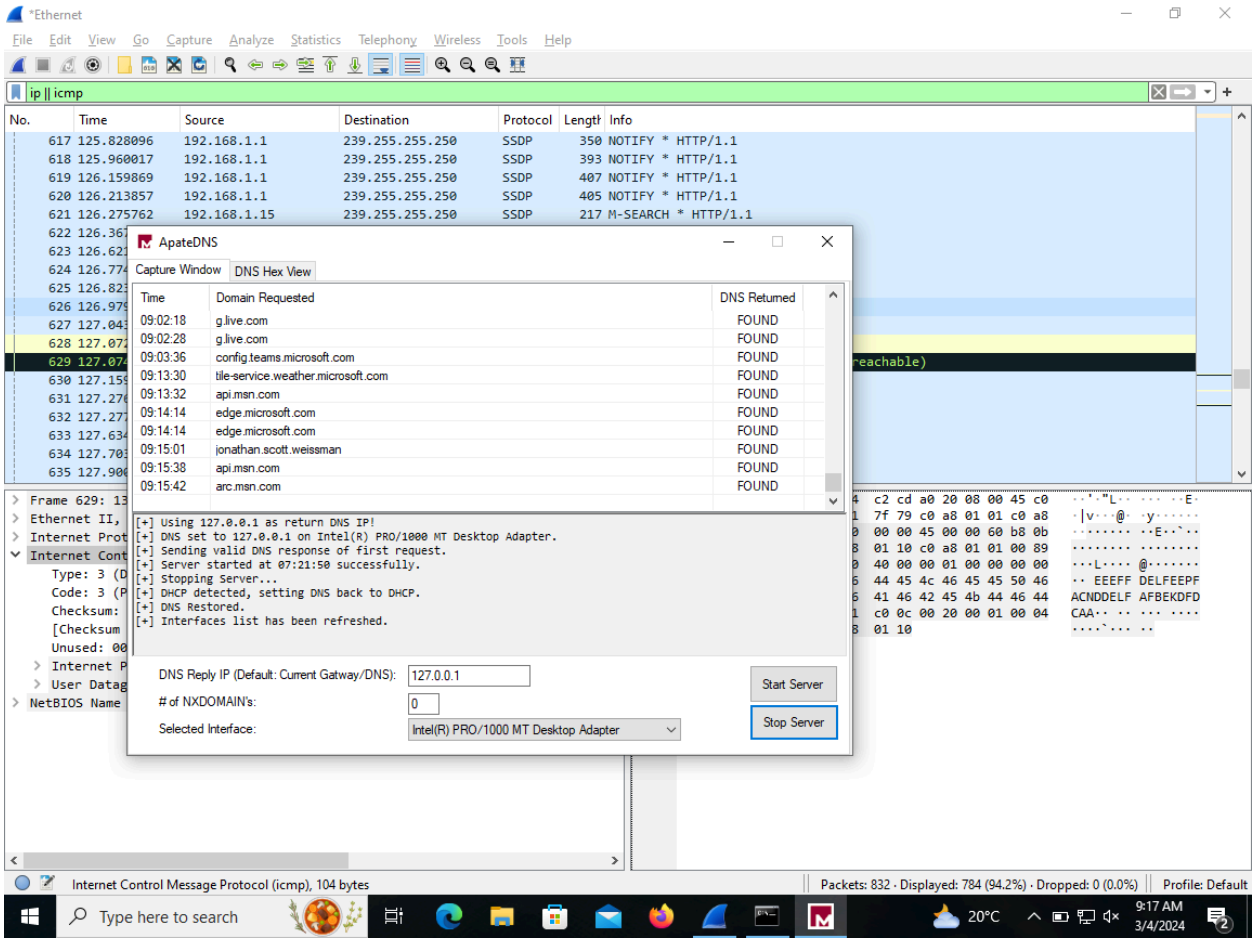
3a,


ApateDNS
Capture Window DNS Hex View
Time Domain Requested DNS Returned
07:50:15 fd.api.iris.microsoft.com FOUND
07:51:17 edge.microsoft.com FOUND
07:51:17 edge.microsoft.com FOUND
07:52:22 ftu.dl.delivery.mp.microsoft.com FOUND
07:54:21 api.msn.com FOUND
07:54:24 edge.microsoft.com FOUND
07:54:24 edge.microsoft.com FOUND
07:54:57 v10.events.data.microsoft.com FOUND
07:59:12 settings-win.data.microsoft.com FOUND
08:00:33 jonathan.scott.weissman FOUND
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Desktop Adapter.
[+] Sending valid DNS response of first request.
[+] Server started at 07:21:58 successfully.
DNS Reply IP (Default: Current Gatway/DNS): 127.0.0.1
# of NXDOMAINs: 0
Selected Interface: Intel(R) PRO/1000 MT Desktop Adapter
Start Server
Stop Server
C:\Windows\system32\cmd.exe
. . . . . : Monday, March 4, 2024 6:15:38 AM
. . . . . : Tuesday, March 5, 2024 7:13:47 AM
. . . . . : 192.168.1.1
. . . . . : 192.168.1.1
. . . . . : 127.0.0.1
r . . . . . : 192.168.1.1
. . . . . : Enabled
jonathan.scott.weissman
t.weissman [127.0.0.1] with 32 bytes of data:
bytes=32 time<1ms TTL=128
bytes=32 time<1ms TTL=128
bytes=32 time<1ms TTL=128
bytes=32 time<1ms TTL=128
27.0.0.1:
, Received = 4, Lost = 0 (0% loss),
p times in milli-seconds:
ximum = 0ms, Average = 0ms
Windows 10 Enterprise Evaluation
Windows License valid for 83 days
Build 19041.vb_release.191206-1406
Type here to search
20°C Nhiều mây
8:02 AM
3/4/2024

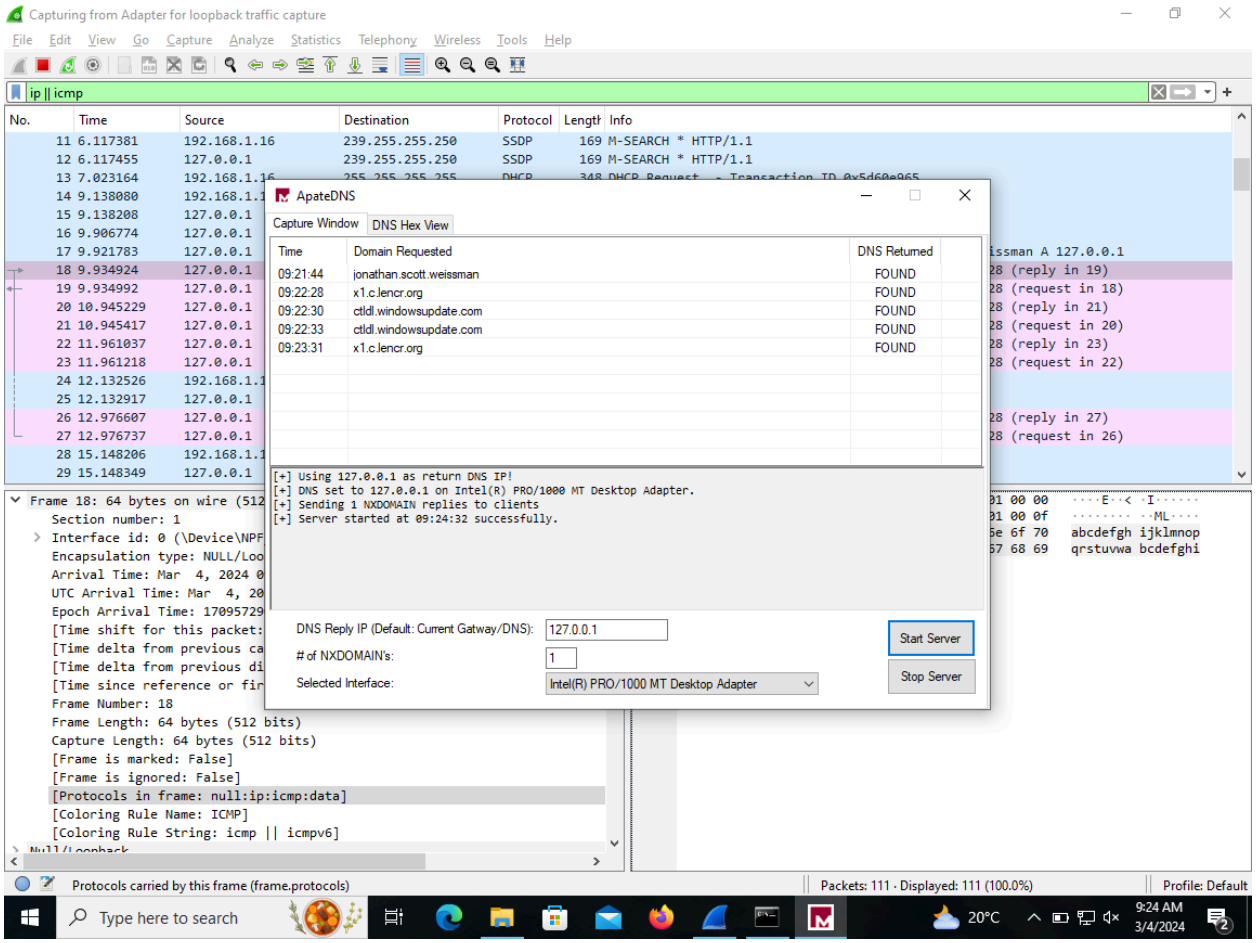
3b,


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip || icmp
No. Time Source Destination Protocol Length Info
617 125.828096 192.168.1.1 239.255.255.250 SSDP 350 NOTIFY * HTTP/1.1
618 125.960017 192.168.1.1 239.255.255.250 SSDP 393 NOTIFY * HTTP/1.1
619 126.159869 192.168.1.1 239.255.255.250 SSDP 407 NOTIFY * HTTP/1.1
620 126.213857 192.168.1.1 239.255.255.250 SSDP 405 NOTIFY * HTTP/1.1
621 126.275762 192.168.1.15 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
ApateDNS
Capture Window
DNS Hex View
Time Domain Requested DNS Returned
09:02:18 g.live.com FOUND
09:02:28 g.live.com FOUND
09:03:36 config.teams.microsoft.com FOUND
09:13:30 tile-service.weather.microsoft.com FOUND
09:13:32 api.msn.com FOUND
09:14:14 edge.microsoft.com FOUND
09:14:14 edge.microsoft.com FOUND
09:15:01 jonathan.scott.weissman FOUND
09:15:38 api.msn.com FOUND
09:15:42 arc.msn.com FOUND
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Desktop Adapter.
[+] Sending valid DNS response of first request.
[+] Server started at 07:21:50 successfully.
[+] Stopping Server...
[+] DHCP detected, setting DNS back to DHCP.
[+] DNS Restored.
[+] Interfaces list has been refreshed.
DNS Reply IP (Default: Current Gatway/DNS): 127.0.0.1
# of NXDOMAIN's: 0
Selected Interface: Intel(R) PRO/1000 MT Desktop Adapter
Start Server
Stop Server
Internet Control Message Protocol (icmp), 104 bytes
Packets: 832 · Displayed: 784 (94.2%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
20°C
9:17 AM
3/4/2024

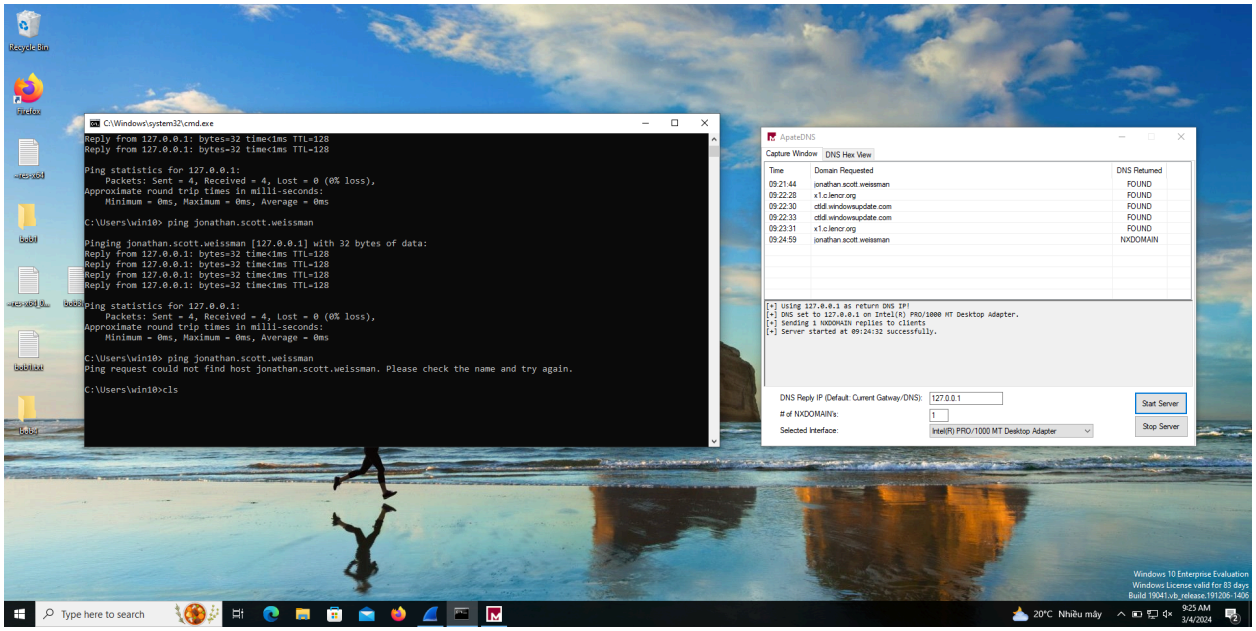
3c,


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip || icmp
No. Time Source Destination Protocol Length Info
617 125.828096 192.168.1.1 239.255.255.250 SSDP 350 NOTIFY * HTTP/1.1
618 125.960017 192.168.1.1 239.255.255.250 SSDP 393 NOTIFY * HTTP/1.1
619 126.159869 192.168.1.1 239.255.255.250 SSDP 407 NOTIFY * HTTP/1.1
620 126.213857 192.168.1.1 239.255.255.250 SSDP 405 NOTIFY * HTTP/1.1
621 126.275762 192.168.1.15 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
ApateDNS
Capture Window
DNS Hex View
Time Domain Requested DNS Returned
09:02:18 g.live.com FOUND
09:02:28 g.live.com FOUND
09:03:36 config.teams.microsoft.com FOUND
09:13:30 tile-service.weather.microsoft.com FOUND
09:13:32 api.msn.com FOUND
09:14:14 edge.microsoft.com FOUND
09:14:14 edge.microsoft.com FOUND
09:15:01 jonathan.scott.weissman FOUND
09:15:38 api.msn.com FOUND
09:15:42 arc.msn.com FOUND
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Desktop Adapter.
[+] Sending valid DNS response of first request.
[+] Server started at 07:21:50 successfully.
[+] Stopping Server...
[+] DHCP detected, setting DNS back to DHCP.
[+] DNS Restored.
[+] Interfaces list has been refreshed.
DNS Reply IP (Default: Current Gatway/DNS): 127.0.0.1
# of NXDOMAIN's: 0
Selected Interface: Intel(R) PRO/1000 MT Desktop Adapter
Start Server
Stop Server
Internet Control Message Protocol (icmp), 104 bytes
Packets: 832 · Displayed: 784 (94.2%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
20°C
9:17 AM
3/4/2024

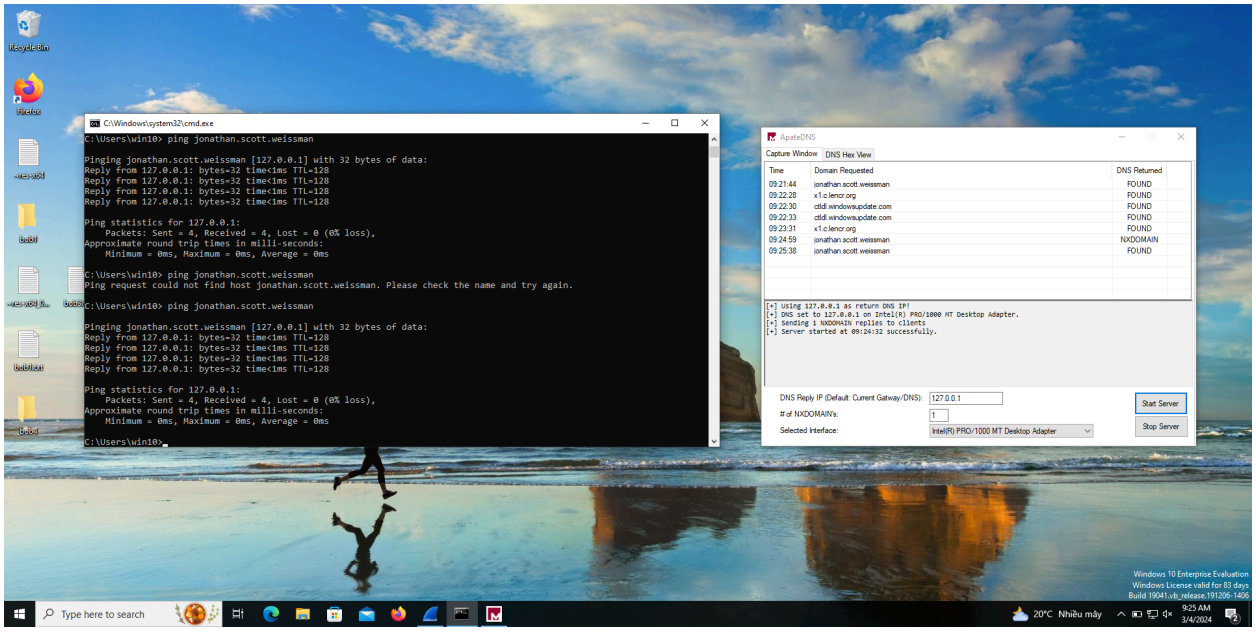
4a,


Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip || icmp
No. Time Source Destination Protocol Length Info
11 6.117381 192.168.1.16 239.255.255.250 SSDP 169 M-SEARCH * HTTP/1.1
12 6.117455 127.0.0.1 239.255.255.250 SSDP 169 M-SEARCH * HTTP/1.1
13 7.023164 192.168.1.16
14 9.138080 192.168.1.1
15 9.138208 127.0.0.1
16 9.906774 127.0.0.1
17 9.921783 127.0.0.1
18 9.934924 127.0.0.1
19 9.934992 127.0.0.1
20 10.945229 127.0.0.1
21 10.945417 127.0.0.1
22 11.961037 127.0.0.1
23 11.961218 127.0.0.1
24 12.132526 192.168.1.1
25 12.132917 127.0.0.1
26 12.976607 127.0.0.1
27 12.976737 127.0.0.1
28 15.148206 192.168.1.1
29 15.148349 127.0.0.1
ApateDNS
Capture Window
DNS Hex View
Time Domain Requested DNS Returned
09:21:44 jonathan.scott.weissman FOUND
09:22:28 x1.c.lencr.org FOUND
09:22:30 ctldl.windowsupdate.com FOUND
09:22:33 ctldl.windowsupdate.com FOUND
09:23:31 x1.c.lencr.org FOUND
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Desktop Adapter.
[+] Sending 1 NXDOMAIN replies to clients
[+] Server started at 09:24:32 successfully.
DNS Reply IP (Default: Current Gatway/DNS): 127.0.0.1
# of NXDOMAIN's: 1
Selected Interface: Intel(R) PRO/1000 MT Desktop Adapter
Start Server
Stop Server
Frame 18: 64 bytes on wire (512
Section number: 1
Interface id: 0 (\Device\NPF
Encapsulation type: NULL/Loo
Arrival Time: Mar 4, 2024 0
UTC Arrival Time: Mar 4, 20
Epoch Arrival Time: 17095729
[Time shift for this packet:
[Time delta from previous ca
[Time delta from previous di
[Time since reference or fir
Frame Number: 18
Frame Length: 64 bytes (512 bits)
Capture Length: 64 bytes (512 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: null:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Protocols carried by this frame (frame.protocols)
Packets: 111 · Displayed: 111 (100.0%)
Profile: Default
Type here to search
20°C
9:24 AM
3/4/2024

4b,


C:\Windows\system32\cmd.exe
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\win10> ping jonathan.scott.weissman
Pinging jonathan.scott.weissman [127.0.0.1] with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\win10> ping jonathan.scott.weissman
Ping request could not find host jonathan.scott.weissman. Please check the name and try again.
C:\Users\win10>cls
ApateDNS
Capture Window
DNS Hex View
Time Domain Requested DNS Returned
09:21:44 jonathan.scott.weissman FOUND
09:22:28 x1.c.lencr.org FOUND
09:22:30 ctldl.windowsupdate.com FOUND
09:22:33 ctldl.windowsupdate.com FOUND
09:23:31 x1.c.lencr.org FOUND
09:24:59 jonathan.scott.weissman NXDOMAIN
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Desktop Adapter.
[+] Sending 1 NXDOMAIN replies to clients
[+] Server started at 09:24:32 successfully.
DNS Reply IP (Default: Current Gatway/DNS): 127.0.0.1
# of NXDOMAIN's: 1
Selected Interface: Intel(R) PRO/1000 MT Desktop Adapter
Start Server
Stop Server
Windows 10 Enterprise Evaluation
Windows License valid for 83 days
Build 19041.vb_release.191206-1406
Type here to search
20°C Nhiều mây
9:25 AM
3/4/2024

4c,


Recycle Bin
Firefox
C:\Windows\system32\cmd.exe
C:\Users\win10> ping jonathan.scott.weissman
Pinging jonathan.scott.weissman [127.0.0.1] with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\win10> ping jonathan.scott.weissman
Ping request could not find host jonathan.scott.weissman. Please check the name and try again.
C:\Users\win10> ping jonathan.scott.weissman
Pinging jonathan.scott.weissman [127.0.0.1] with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\win10>
ApateDNS
Capture Window
DNS Hex View
Time
Domain Requested
DNS Returned
09:21:44 jonathan.scott.weissman FOUND
09:22:28 x1.c.lencr.org FOUND
09:22:30 ctldl.windowsupdate.com FOUND
09:22:33 ctldl.windowsupdate.com FOUND
09:23:31 x1.c.lencr.org FOUND
09:24:59 jonathan.scott.weissman NXDOMAIN
09:25:38 jonathan.scott.weissman FOUND
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Desktop Adapter.
[+] Sending 1 NXDOMAIN replies to clients
[+] Server started at 09:24:32 successfully.
DNS Reply IP (Default: Current Gatway/DNS):
127.0.0.1
# of NXDOMAIN's:
1
Selected Interface:
Intel(R) PRO/1000 MT Desktop Adapter
Start Server
Stop Server
Type here to search
20°C Nhiều mây
9:25 AM
3/4/2024
Windows 10 Enterprise Evaluation
Windows License valid for 83 days
Build 19041.vb_release.191206-1406