


Digital assignment

Youssef sherif hassan

20221041587

Question 1

Q1  What is the MD5 hash value of the suspect disk?

Weight : 0 | Solved : 876 | Average Solve Time: 2min


9471e69c95d8909ae60ddff30d50ffa1

[Computed Hashes]


MD5 checksum:	9471e69c95d8909ae60ddff30d50ffa1
SHA1 checksum:	167aa08db25dfeeb876b0176ddc329a3d9f2803a

from the text file about the disk image

Question 2:

Q2  What phrase did the suspect search for on 2021-04-29 18:17:38 UTC? (three words, two spaces in between)

Weight : 0 | Solved : 720 | Average Solve Time: 1min

password cracking lists  [Submit](#)

Go to C:/Users/John Doe/AppData/Local/Google/Chrome/User Data/Default

Then open the database file and decode it to find the answer

Name	Timestamp
Apple Absolute Time (ns) (UTC)	2001-06-03 12:29:53.8589009 Z
Chromium Time Microseconds (UTC)	2021-04-29 18:17:38.9008910 Z
Microsoft Ticks (Local)	0043-01-13 01:49:45.8900891
Unix Microseconds (UTC)	2390-04-29 18:17:38.9008910 Z
Windows Filetime (UTC)	1643-01-13 01:49:45.8900891 Z

Value Input

Format:

Value:

Time Zone

Name:

Date Output

Pattern:

Sample:

Question 3

Q3 What is the IPv4 address of the FTP server the suspect connected to?

Weight : 0 | Solved : 714 | Average Solve Time: 5min

192.168.1.20

Go to [root]/Users/John Doe/AppData/Roaming/FileZilla/filezilla.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<filezilla>
  <siteManager>
    <sites>
      <site
        connected="1"
        selected="1"
        <Host>192.168.1.20</Host>
        <Port>21</Port>
        <Protocol>0</Protocol>
        <Type>0</Type>
        <User>kali</User>
        <Logontype>2</Logontype>
        <PasvMode>MODE_DEFAULT</PasvMode>
        <EncodingType>Auto</EncodingType>
        <BypassProxy>0</BypassProxy>
        <Site/>
        <RemotePath>1 0 4 home 4 kali 9 Documents</RemotePath>
        <LocalPath>C:\Users\John Doe\My Documents</LocalPath>
      </site>
    </sites>
  </siteManager>
</filezilla>
```

Question 4

Q4 What date and time was a password list deleted in UTC? (YYYY-MM-DD HH:MM:SS UTC)

Weight : 0 | Solved : 689 | Average Solve Time: 20min

2021-04-29 18:22:17 UTC




Submit

Go to [root]/\$Recycle.Bin/S-1-5-21-3061953532-2461696977-1363062292-1001/

<


Here is the time

Question 5

Q5  How many times was Tor Browser ran on the suspect's computer? (number only)


Weight : 0 | Solved : 685 | Average Solve Time: 19min

This file and use Use "WinPrefetchView.exe to analyze prefetch files


 TORBROWSER-INSTALL-WIN64-10.0-F3C...	4/29/2021 8:22 PM	PF File	26 KB
--	-------------------	---------	-------

Install PECmd.exe the command file and put the file into it to view some information about the file

Question 6

Q6  What is the suspect's email address?

Weight : 0 | Solved : 661 | Average Solve Time: 1min



Go to this location [root]/Users/John Doe/AppData/Local/Google/Chrome/User Data/Default/History"

In the history file

```
8 - Persistence in plain sight - Digital Forensic Science /%Xv<0 5=

gU;m
CKb1g1WwdSUU3qspWA6bjyQkLA==Inbox | dreammaker82@protonmail.com | ProtonMail /%}
^3YXj ;o https://protonmail.com/Secure email: ProtonMail is free
. /%ZZIdb
zip.org/download.htmlDownload /%tCÜ"g
7&sourceid=chrome&ie=UTF-8zip - Google Search /%t»iz*d 3
m/YouTube /%·ú}C†+e 5 https://youtube.com/YouTube /%·ú}C†c

10-million-password-list-top-1000000.txt /%Ö(c*

password-list-top-1000000.txt /%Ö(c*
```

Question 7

Q7

What is the FQDN did the suspect port scan?

Weight : 0 | Solved : 636 | Average Solve Time: 1min

dfir.science

Submit



Go to [root]/Users/John

Doe/AppData/Roaming/Microsoft/Windows/PowerShell/PSReadLine/ConsoleHost_history.txt


Check powershell history

```
ipconfig
ipconfig /cleardns
ipconfig /flushdns
exit
sdelete
exit
ipconfig /flushdns
ping dfir.science
nmap dfir.science
dir
cd .\Documents\
dir
sdelete .\accountNum
sdelete .\accountNum.zip
exit
cd E:\FTK_Imager_Lite_3.1.1
& '.\FTK_Imager.exe'
exit
```

Question 8

Q8  What country was picture "20210429_152043.jpg" allegedly taken in? 

Weight : 0 | Solved : 673 | Average Solve Time: 1min



Extract 20210429_152043.jpg metadata.

Install and run exiftool to find metadata about the image

```

Profile Creator      : Little CMS
Profile ID          : 0
Profile Description  : GIMP built-in sRGB
Profile Copyright   : Public Domain
Media White Point    : 0.9642 1 0.82491
Chromatic Adaptation : 1.04788 0.02292 -0.05022 0.02959 0.99048 -0.01707 -0.00925 0.01508 0.75168
Red Matrix Column    : 0.43604 0.22249 0.01392
Blue Matrix Column   : 0.14305 0.06061 0.71393
Green Matrix Column  : 0.38512 0.7169 0.09706
Red Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Green Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Blue Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Chromaticity Channels : 3
Chromaticity Colorant : Unknown
Chromaticity Channel 1 : 0.64 0.33002
Chromaticity Channel 2 : 0.3 0.60001
Chromaticity Channel 3 : 0.15001 0.06
Device Mfg Desc       : GIMP
Device Model Desc     : sRGB
Comment               : 0 AC original_brightness(123.3) bright_enhanced_level(0.0) brightness_shi
hanced_level(14.8) isOutdoor(1) lux(145.9) FM0 Prmid2 mxDrkA0.03 mxBrTA0.00 mxPkNSat6.38 dr0.05 br6.82 wd
00000bfalic 00000
Image Width           : 4160
Image Height          : 3120
Encoding Process      : Progressive DCT, Huffman coding
Bits Per Sample       : 8
Color Components      : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Aperture              : 2.2
Image Size            : 4160x3120
Megapixels            : 13.0
Shutter Speed         : 1/1419
Create Date           : 2021:04:29 15:20:43.367153
Date/Time Original    : 2021:04:29 15:20:43.367153
Modify Date           : 2021:04:29 15:33:32.367153
Thumbnail Image       : (Binary data 9000 bytes, use -b option to extract)
GPS Latitude          : 16 deg 0' 0.00" S
GPS Longitude         : 23 deg 0' 0.00" E
Focal Length          : 3.7 mm
GPS Position          : 16 deg 0' 0.00" S, 23 deg 0' 0.00" E
Light Value           : 13.7

```

Open google to know the location

Address

DD (decimal degrees)*

Latitude

Longitude

Lat,Long

Question 9

[root]\Users\John
Doe\AppData\Local\Microsoft\Windows\Usrclass.dat"

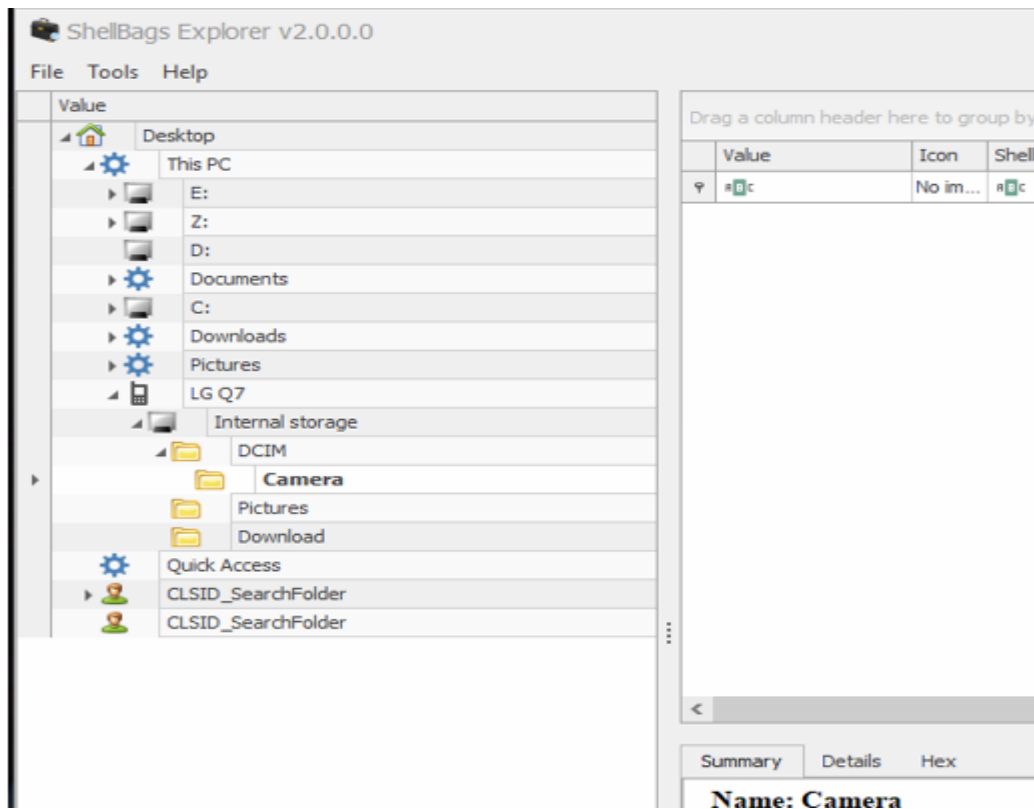
Q9 ✓ What is the parent folder name picture "20210429_151535.jpg" was in before the suspect copy it to "contact" folder on his desktop?

Weight : 0 | Solved : 604 | Average Solve Time: 7min

camera



Submit



Question 10

Q10 ✓ A Windows password hashes for an account are below. What is the user's password?
Anon:1001:aad3b435b51404eeaad3b435b51404ee:3DE1A36F6DDB8E036DFD75E8E20C4AF4:::

Weight : 0 | Solved : 579 | Average Solve Time: 18min

AFR1CA!



Submit

Use online-hashcrack.com to find the hash value

✓ Found:

3de1a36f6ddb8e036dfd75e8e20c4af4:AFR1CA!

Last question

Go to root/windows/system32/config

Q11 ✓ What is the user "John Doe's" Windows login password?

Weight : 0 | Solved : 538 | Average Solve Time: 5min

ctf2021



Submit

DRIVERS.LOG2.FileSlack	3/22/2024 9:30 PM	FILESLACK File	64 KB
ELAM	11/19/2020 9:30 AM	File	32 KB
SAM	4/30/2021 2:59 AM	File	64 KB
SAM.FileSlack	3/22/2024 9:30 PM	FILESLACK File	16 KB

✓ Found:

ecf53750b76cc9a62057ca85ff4c850e:ctf2021