CyberDefenders: CorporateSecrets Lab

The following writeup is for CorporateSecrets Lab on CyberDefenders, it a disk image of a Windows machine. This was a super long CTF, but it covers a lot of the foundational digital forensic knowledge, ranging from browser forensics to exploring the MFT file.

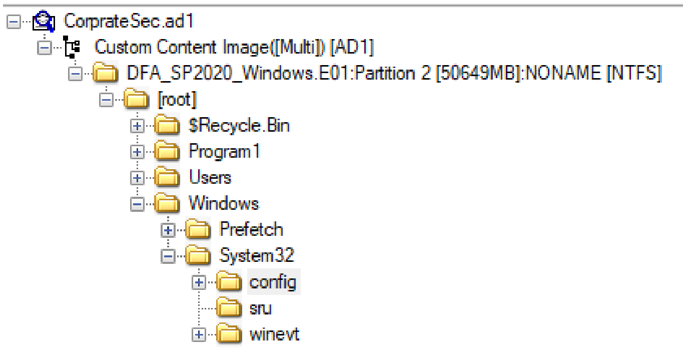
Scenario: A windows forensics challenge prepared by Champlain College Digital Forensics Association for their yearly CTF.

Windows Image Forensics Case created By AccessData® FTK® Imager 4.2.1.4

Acquired using: ADI4.2.1.4

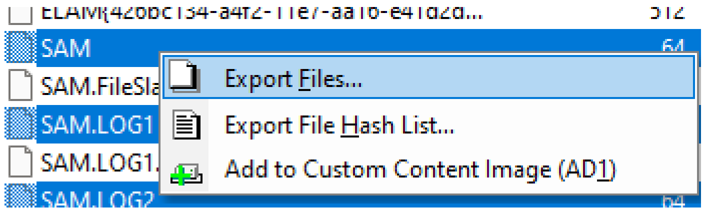
What is the current build number on the system?

In order to determine the current build number of the system, we can use FTK Imager to dump the registry hives and use Registry Explorer to look at the Software hive. Registry hives are located in Windows/System32/config:

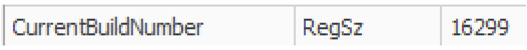


```
CrprateSec.ad1
  Custom Content Image([Multi]) [AD1]
    DFA_SP2020_Windows.E01:Partition 2 [50649MB]:NONAME [NTFS]
      [root]
        $Recycle.Bin
        Program1
        Users
        Windows
          Prefetch
          System32
            config
            sru
            winevt
```

Here we can dump hives of interest such as SYSTEM, SOFTWARE, SECURITY, and SAM.



We can now open up the Software hive in Registry Explorer and navigate to Microsoft/Windows NT/CurrentVersion:

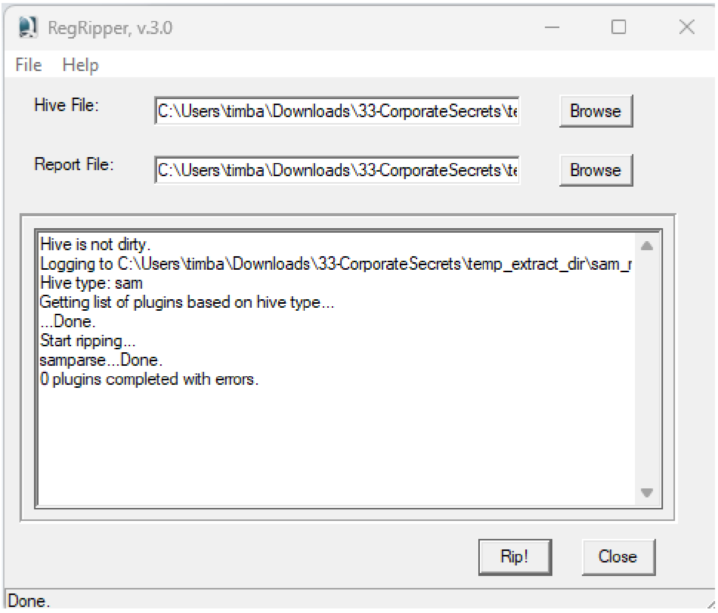


CurrentBuildNumber	RegSz	16299

Answer: 16299

How many users are there?

To determine the number of users on this system, we can run RegRipper against the SAM registry hive:



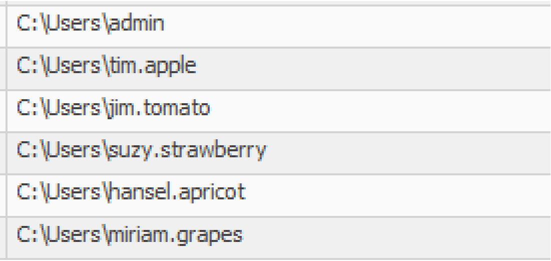
Hive File: C:\Users\timba\Downloads\33-CorporateSecrets\te

Report File: C:\Users\timba\Downloads\33-CorporateSecrets\te

```
Hive is not dirty.
Logging to C:\Users\timba\Downloads\33-CorporateSecrets\temp_extract_dir\sam_r
Hive type: sam
Getting list of plugins based on hive type...
...Done.
Start ripping...
samparse...Done.
0 plugins completed with errors.
```

Done.

Alternatively, you can navigate to Microsoft/Windows NT/CurrentVersion/ProfileList to see the number of users:

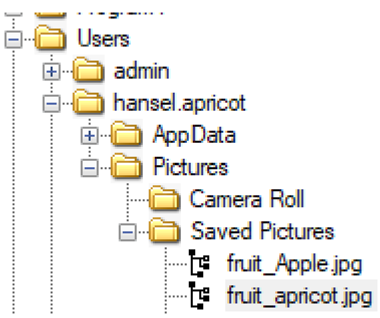


C:\Users\admin
C:\Users\tim.apple
C:\Users\jim.tomato
C:\Users\suzy.strawberry
C:\Users\hansel.apricot
C:\Users\miriam.grapes

Answer: 6

What is the CRC64 hash of the file "fruit_apricot.jpg"?

After hunting for this file, I eventually found it within the hansel.apricot users Saved Pictures directory:



After exporting the file, I then used the following tool to hash the file:

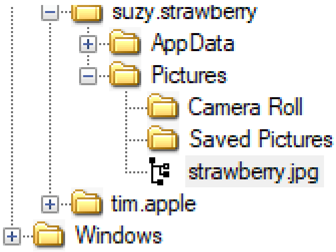
https://toolkitbay.com/tkb/tool/CRC-64

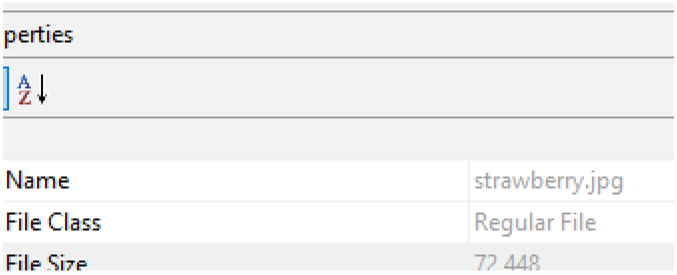
NOTE! Use ECMA table type and uncheck the padding option.

Answer: ED865AA6DFD756BF

What is the logical size of the file "strawberry.jpg" in bytes?

First, navigate to the Pictures directory for suzy.strawbery. You can then take a look at the properties tab to determine the size of the file:



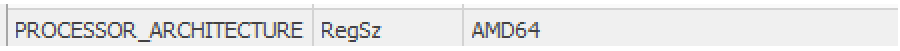


Name	strawberry.jpg
File Class	Regular File
File Size	72 448

Answer: 72448

What is the processor architecture of the system? (one word)

The processor architecture among other information can be found within the System registry hive located at CurrentControlSet\Control\Session Manager\Environment:

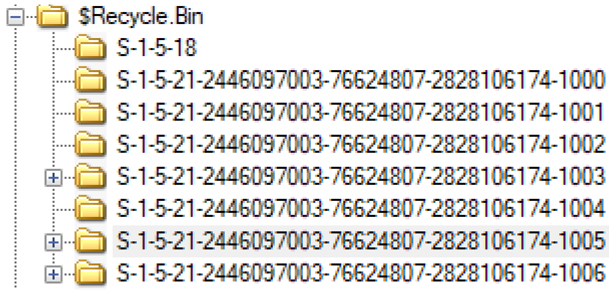


PROCESSOR_ARCHITECTURE	RegSz	AMD64

Answer: AMD64

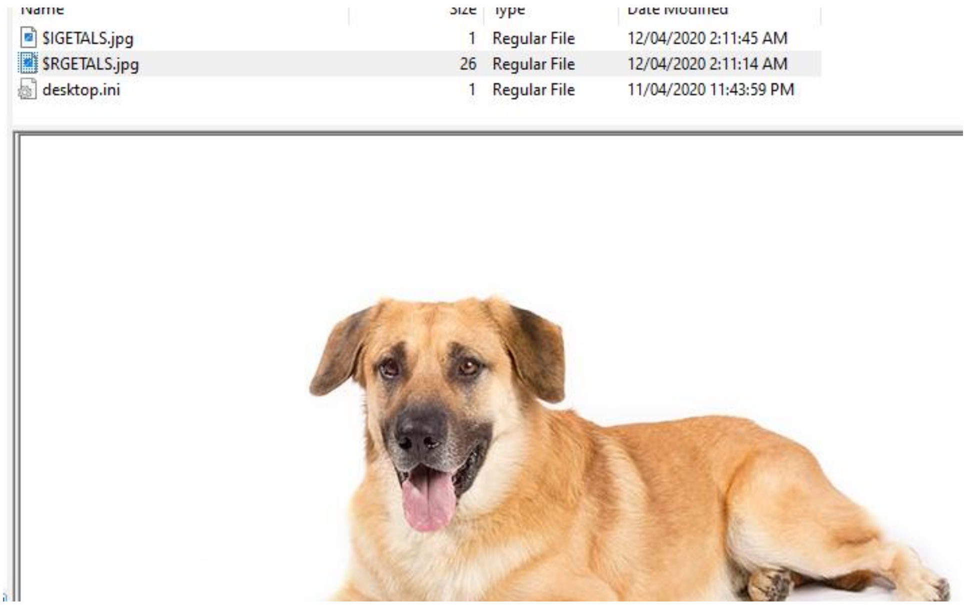
Which user has a photo of a dog in their recycling bin?

The recycle bin can be found in the root folder on disk as $Recycle.Bin:



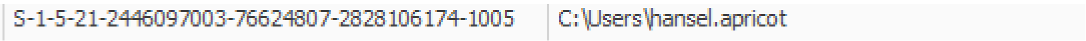
```
$Recycle.Bin
    S-1-5-18
    S-1-5-21-2446097003-76624807-2828106174-1000
    S-1-5-21-2446097003-76624807-2828106174-1001
    S-1-5-21-2446097003-76624807-2828106174-1002
    S-1-5-21-2446097003-76624807-2828106174-1003
    S-1-5-21-2446097003-76624807-2828106174-1004
    S-1-5-21-2446097003-76624807-2828106174-1005
    S-1-5-21-2446097003-76624807-2828106174-1006
```

Here we can see the user's security identifiers (SIDs). The identify ending with 1005 contains the dog photo:



Name	Size	Type	Date Modified
$IGETALS.jpg	1	Regular File	12/04/2020 2:11:45 AM
$RGETALS.jpg	26	Regular File	12/04/2020 2:11:14 AM
desktop.ini	1	Regular File	11/04/2020 11:43:59 PM

If you take a look at the ProfileList in the software hive, you can see that the user associated with this SID is hansel.apricot:

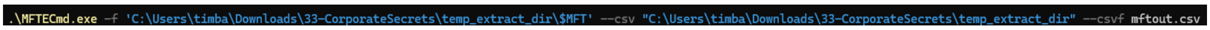


S-1-5-21-2446097003-76624807-2828106174-1005	C:\Users\hansel.apricot

Answer: hansel.apricot

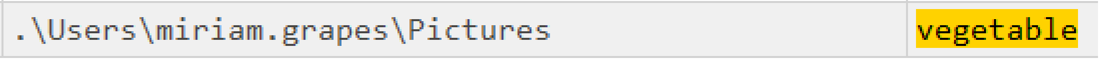
What type of file is "vegetable"? Provide the extension without a dot.

To find this file, I used MFTECmd which is an Eric Zimmerman tool that parses MFT files.



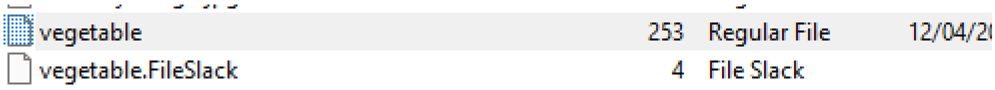
```
.\MFTECmd.exe -f 'C:\Users\timba\Downloads\33-CorporateSecrets\temp_extract_dir\$MFT' --csv "C:\Users\timba\Downloads\33-CorporateSecrets\temp_extract_dir" --csvf mftout.csv
```

After opening this csv file in Timeline Explorer (another Eric Zimmerman tool), I found that the vegetable file is located at:

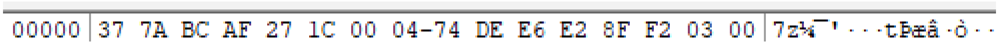


.\Users\miriam.grapes\Pictures	vegetable

Based on the file signature, we now the file type/extension to be 7z:



vegetable	253	Regular File	12/04/2
vegetable.FileSlack	4	File Slack	

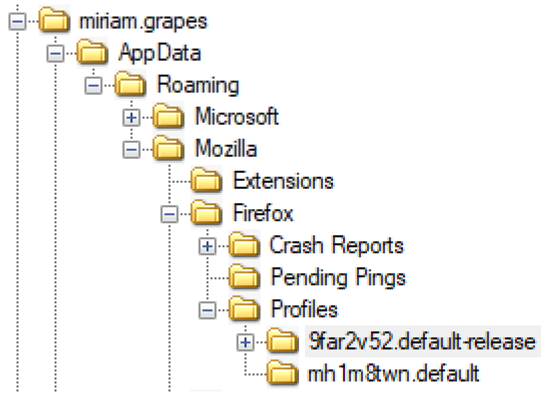


```
00000 37 7A BC AF 27 1C 00 04-74 DE E6 E2 8F F2 03 00 7z¼¯'···tÞæâ·ò··
```

Answer: 7z

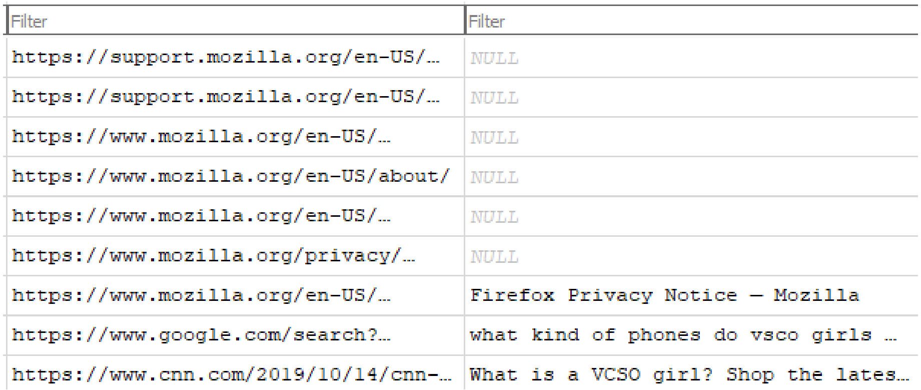
What type of girls does Miriam Grapes design phones for (Target audience)?

This question requires some browser forensics. We need to check out this users FireFox browser history. To do so, navigate to Users/Miriam.grapes/Roaming/Mozilla/Firefox/Profiles:



```
miriam.grapes
  AppData
    Roaming
      Microsoft
      Mozilla
        Extensions
        Firefox
          Crash Reports
          Pending Pings
          Profiles
            9far2v52.default-release
            mh1m8twn.default
```

Then export the places.sqlite database, open it up in a tool like DB Browser for SQLite, and view the moz_places table:



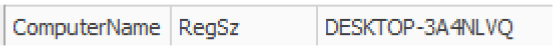
Filter	Filter
https://support.mozilla.org/en-US/…	NULL
https://support.mozilla.org/en-US/…	NULL
https://www.mozilla.org/en-US/…	NULL
https://www.mozilla.org/en-US/about/	NULL
https://www.mozilla.org/en-US/…	NULL
https://www.mozilla.org/privacy/…	NULL
https://www.mozilla.org/en-US/…	Firefox Privacy Notice — Mozilla
https://www.google.com/search?…	what kind of phones do vsco girls …
https://www.cnn.com/2019/10/14/cnn-…	What is a VCSO girl? Shop the lates…

Here you can see Miriam searching for vsco girls.

Answer: vsco

What is the name of the device?

You can find the ComputerName within the System registry hive, located at CurrentControlSet\Control\ComputerName\ComputerName\:

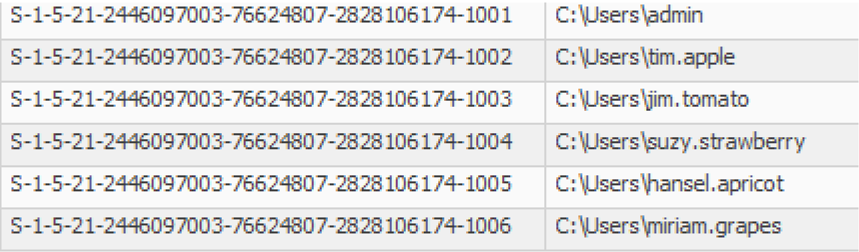


ComputerName	RegSz	DESKTOP-3A4NLVQ

Answer: DESKTOP-3A4NLVQ

What is the SID of the machine?

The SID of a user is the SID of the machine + a four-digit number which is the RID of the user. Therefore, the SID of the machine is everything before the final -:

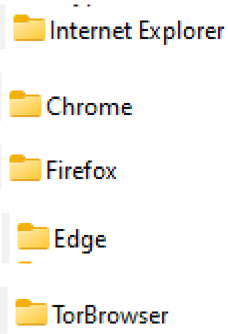


S-1-5-21-2446097003-76624807-2828106174-1001	C:\Users\admin
S-1-5-21-2446097003-76624807-2828106174-1002	C:\Users\tim.apple
S-1-5-21-2446097003-76624807-2828106174-1003	C:\Users\jim.tomato
S-1-5-21-2446097003-76624807-2828106174-1004	C:\Users\suzy.strawberry
S-1-5-21-2446097003-76624807-2828106174-1005	C:\Users\hansel.apricot
S-1-5-21-2446097003-76624807-2828106174-1006	C:\Users\miriam.grapes

Answer: S-1-5-21-2446097003-76624807-2828106174

How many web browsers are present?

After exploring the file system, I found 5 different unique browsers:



Internet Explorer

Chrome

Firefox

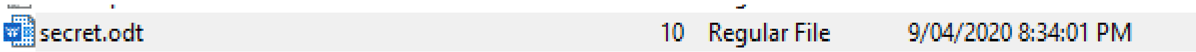
Edge

TorBrowser

Answer: 5

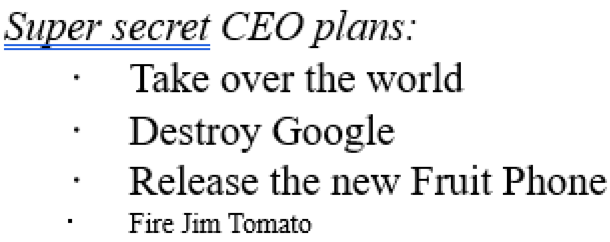
How many super secret CEO plans does Tim have? (Dr. Doofenshmirtz Type Beat)

If you go to tim.apple’s documents directory, you can see a secret.odt file:



secret.odt	10	Regular File	9/04/2020 8:34:01 PM

If you export this file and change the text font to black, you can see 4 plans:



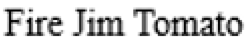
Super secret CEO plans:

- Take over the world
- Destroy Google
- Release the new Fruit Phone
- Fire Jim Tomato

Answer: 4

Which employee does Tim plan to fire? (He's Dead, Tim. Enter the full name - two words - space separated)

You can see the employee in the secret.odt file:

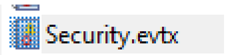


Fire Jim Tomato

Answer: Jim Tomato

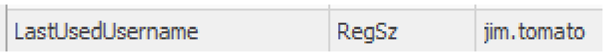
What was the last used username? (I didn't start this conversation, but I'm ending it!)

To find the last used username, we need to check the last login attempt. To do this, we can export the Security.evtx file located at Windows/System32/winevt/Logs:



Security.evtx

You can then use a tool like EvtxECmd to parse the evtx file and view the results in timeline explorer. However, I simply opened up the software hive in registry explorer and navigated to Microsoft\Windows NT\CurrentVersion\WinLogon to find the last used username:

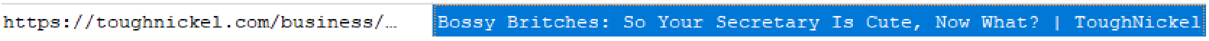


LastUsedUsername	RegSz	jim.tomato

Answer: jim.tomato

What was the role of the employee Tim was flirting with?

Answering this question requires us to take a look at Tim's FireFox browser history. Following the same process as before, all you need to do is export the place.sqlite file, open it in DB Browser for SQLite and view the moz_places table:

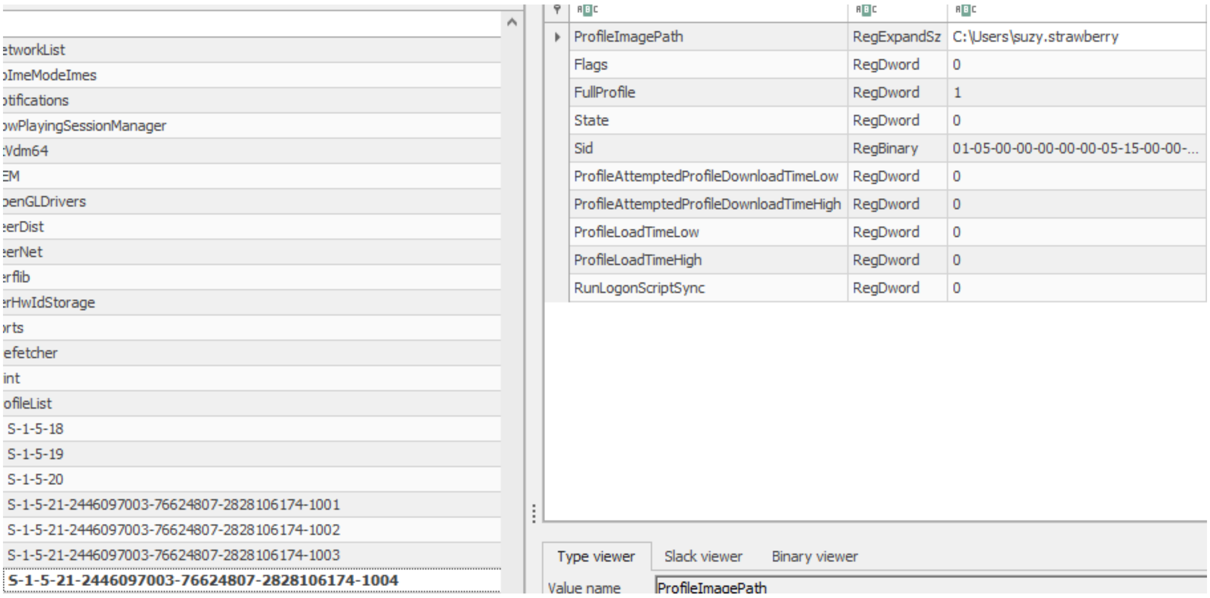


```
https://toughnickel.com/business/…   Bossy Britches: So Your Secretary Is Cute, Now What? | ToughNickel
```

Answer: Secretary

What is the SID of the user "suzy.strawberry"?

If you look at the ProfileList within the software hive, you can see the SID for suzy:



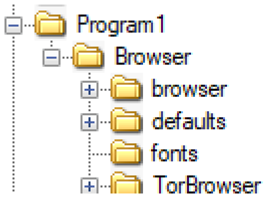
```
etworkList
oImeModeImes
otifications
owPlayingSessionManager
Vdm64
EM
penGLDrivers
erDist
erNet
rflib
rHwIdStorage
rts
efetcher
int
ofileList
 S-1-5-18
 S-1-5-19
 S-1-5-20
 S-1-5-21-2446097003-76624807-2828106174-1001
 S-1-5-21-2446097003-76624807-2828106174-1002
 S-1-5-21-2446097003-76624807-2828106174-1003
 S-1-5-21-2446097003-76624807-2828106174-1004
```

ProfileImagePath	RegExpandSz	C:\Users\suzy.strawberry
Flags	RegDword	0
FullProfile	RegDword	1
State	RegDword	0
Sid	RegBinary	01-05-00-00-00-00-00-05-15-00-00-...
ProfileAttemptedProfileDownloadTimeLow	RegDword	0
ProfileAttemptedProfileDownloadTimeHigh	RegDword	0
ProfileLoadTimeLow	RegDword	0
ProfileLoadTimeHigh	RegDword	0
RunLogonScriptSync	RegDword	0

Value name: ProfileImagePath

Answer: 1004

List the file path for the install location of the Tor Browser.

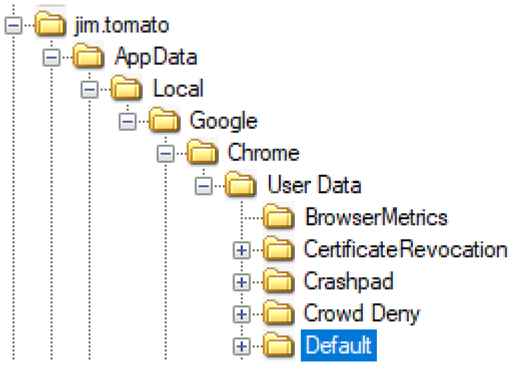


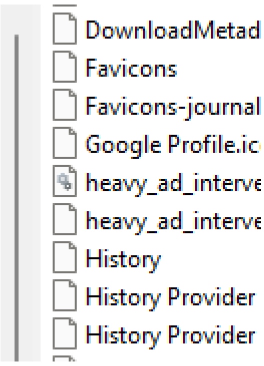
```
Program1
  Browser
    browser
    defaults
    fonts
    TorBrowser
```

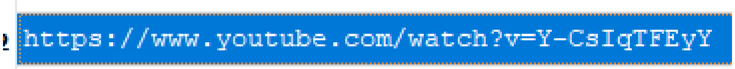
Answer: C:\Program1

What was the URL for the Youtube video watched by Jim?

Follow the same process as the other browser history questions, although this time, you want to export the History.sql file located at:



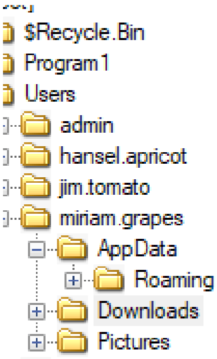


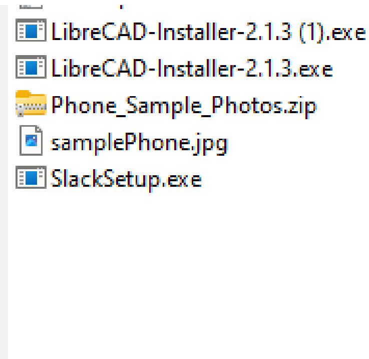

https://www.youtube.com/watch?v=Y-CsIqTFEyY

Answer: https://www.youtube.com/watch?v=Y-CsIqTFEyY

Which user installed LibreCAD on the system?

After exploring each user's directory, I was able to find two installers for LibreCAD on Miriam.grapes:

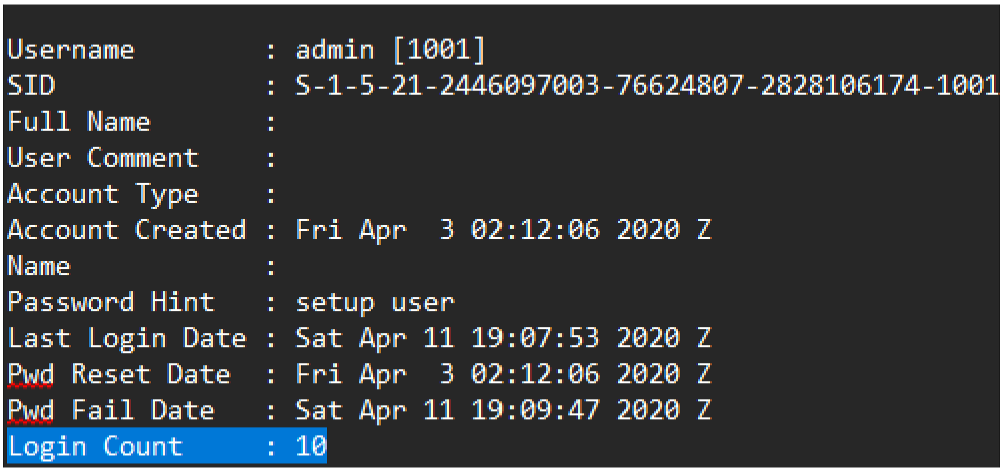



LibreCAD-Installer-2.1.3 (1).exe
LibreCAD-Installer-2.1.3.exe
Phone_Sample_Photos.zip
samplePhone.jpg
SlackSetup.exe

Answer: Miriam.grapes

How many times "admin" logged into the system?

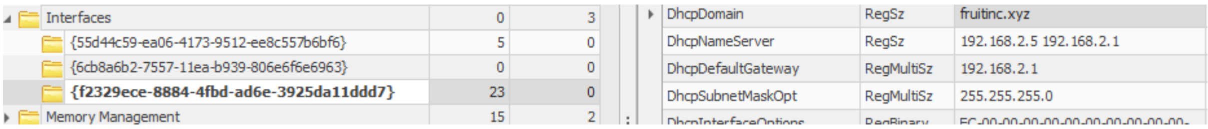
If you use regripper against the SAM registry hive, you can determine how many times a user logged in:



```
Username        : admin [1001]
SID             : S-1-5-21-2446097003-76624807-2828106174-1001
Full Name       :
User Comment    :
Account Type    :
Account Created : Fri Apr  3 02:12:06 2020 Z
Name            :
Password Hint   : setup user
Last Login Date : Sat Apr 11 19:07:53 2020 Z
Pwd Reset Date  : Fri Apr  3 02:12:06 2020 Z
Pwd Fail Date   : Sat Apr 11 19:09:47 2020 Z
Login Count     : 10
```

What is the name of the DHCP domain the device was connected to?

If you load the system registry hive into Registry Explorer, you can go to the available bookmarks tab and take a look at the interfaces. Here you will find the DHCP domain:



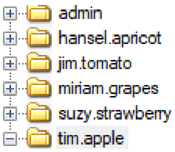
Interfaces	0	3
{55d44c59-ea06-4173-9512-ee8c557b6bf6}	5	0
{6cb8a6b2-7557-11ea-b939-806e6f6e6963}	0	0
{f2329ece-8884-4fbd-ad6e-3925da11ddd7}	23	0
Memory Management	15	2

DhcpDomain	RegSz	fruitinc.xyz
DhcpNameServer	RegSz	192.168.2.5 192.168.2.1
DhcpDefaultGateway	RegMultiSz	192.168.2.1
DhcpSubnetMaskOpt	RegMultiSz	255.255.255.0
DhcpInterfaceOptions	RegBinary	FC-00-00-00-00-00-00-00-00-00-00-

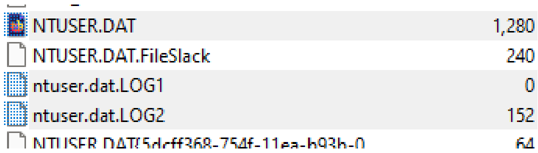
Answer: fruitinc.xyz

What time did Tim download his background image? (Oh Boy 3AM . Answer in MM/DD/YYYY HH:MM format (UTC).)

First, we need to determine what Tim's wallpaper actually. To do so, export Tim's NTUSER.DAT file:

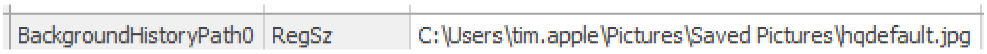


admin
hansel.apricot
jim.tomato
miriam.grapes
suzy.strawberry
tim.apple



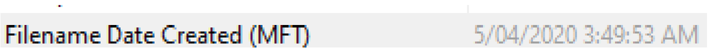
NTUSER.DAT	1,280
NTUSER.DAT.FileSlack	240
ntuser.dat.LOG1	0
ntuser.dat.LOG2	152
NTUSER.DAT{5dcff368-754f-11ea-b93b-0	64

After opening this in Registry Explorer, navigate to Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpaper:



BackgroundHistoryPath0	RegSz	C:\Users\tim.apple\Pictures\Saved Pictures\hqdefault.jpg

If you go to this file location in FTK Imager and take a look at the file properties, you can find the creation timestamp:



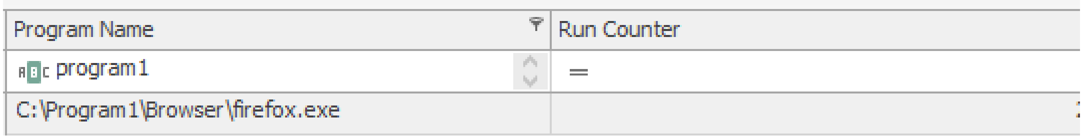
Filename Date Created (MFT)	5/04/2020 3:49:53 AM

All you need to do is convert it to the right format.

Answer: 04/05/2020 03:49

How many times did Jim launch the Tor Browser?

First, make sure to export Jim's NTUSER.dat registry hive, then you can navigate to Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist. Here we can filter for program1 (which we determined to be where Tor was installed) to determine how many times Tor was executed:



Program Name	Run Counter
program1	=
C:\Program1\Browser\firefox.exe	

Answer: 2

There is a png photo of an iPhone in Grapes's files. Find it and provide the SHA-1 hash.

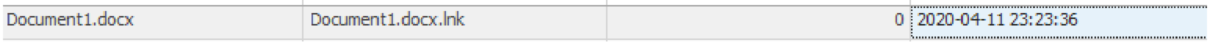
If you explore Grape's Download directory, you will come across a file called 'samplePhone.jpg'. If you export this file, you will notice that it isn't an image of an iPhone. I was stuck on this for a while so I loaded the file in aperisolve (great at steganography challenges) and was able download the Binwalk results. The file 174A from the binwalk output is an image of an iPhone:

Now all you need to do is hash the image.

Answer: 537fe19a560ba3578d2f9095dc2f591489ff2cde

When was the last time a docx file was opened on the device? (An apple a day keeps the docx away. Answer in UTC, YYYY-MM-DD HH:MM:SS)

If you dump Jim's NTUSER.dat hive and navigate to Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs, you will be able to see the last accessed docx file:



Document1.docx	Document1.docx.lnk		0	2020-04-11 23:23:36

Answer: 2020-04-11 23:23:36

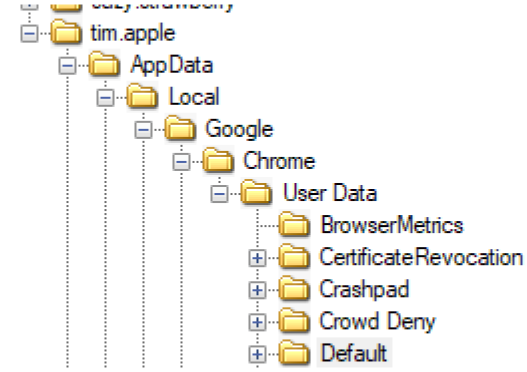
How many entries does the MFT of the filesystem have?

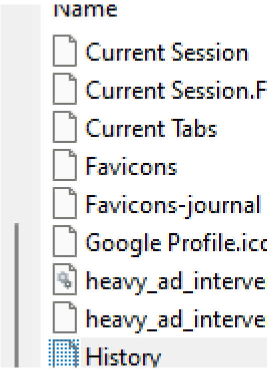
I personally cant be bothered to use the mftdump tool to count the number of entires.

Answer: 219904

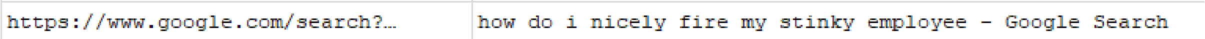
Tim wanted to fire an employee because they were ……?(Be careful what you wish for)

This is another challenge that involves investigating someone's browser history. After dumping the Google history file found here:





You can open up this sql file in DB Browser for SQLite and navigate to the urls table to determine the answer:

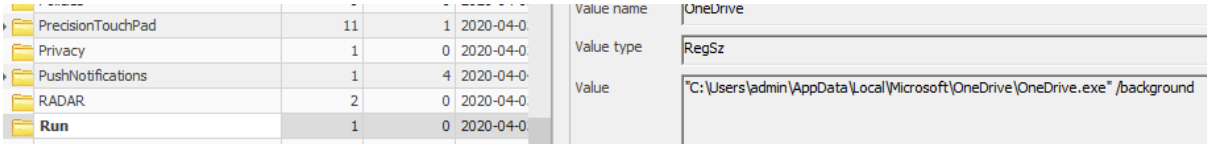


https://www.google.com/search?…	how do i nicely fire my stinky employee - Google Search

Answer: Stink

What cloud service was a Startup item for the user admin?

Startup items are located at Software\Microsoft\Windows\CurrentVersion\Run. Make sure to download the admin account's NTUSDER.DAT hive and navigate to the aforementioned location. Here you can see an entry for OneDrive:



PrecisionTouchPad	11	1	2020-04-0:
Privacy	1	0	2020-04-0:
PushNotifications	1	4	2020-04-0
RADAR	2	0	2020-04-0:
Run	1	0	2020-04-0:

Value name: OneDrive

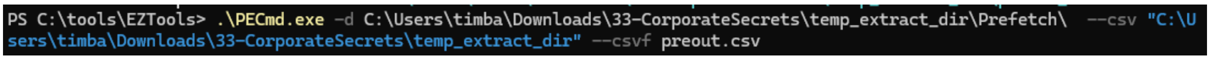
Value type: RegSz

Value: "C:\Users\admin\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background

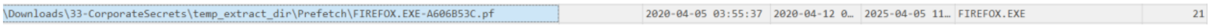
Answer: OneDrive

Which Firefox prefetch file has the most runtimes? (Flag format is)

Prefetch files are located at Windows/System32/Prefetch. We can use another Eric Zimmerman tool called PECmd to parse the prefetch files in this directory and open the output in Timeline Explorer:



```
PS C:\tools\EZTools> .\PECmd.exe -d C:\Users\timba\Downloads\33-CorporateSecrets\temp_extract_dir\Prefetch\  --csv "C:\U
sers\timba\Downloads\33-CorporateSecrets\temp_extract_dir" --csvf preout.csv
```

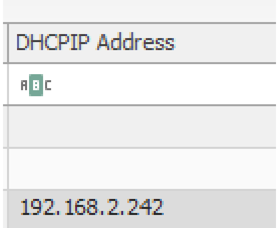


```
\Downloads\33-CorporateSecrets\temp_extract_dir\Prefetch\FIREFOX.EXE-A606B53C.pf      2020-04-05 03:55:37  2020-04-12 0…  2025-04-05 11…  FIREFOX.EXE      21
```

Answer: FIREFOX.EXE-A606B53C.pf/21

What was the last IP address the machine was connected to?

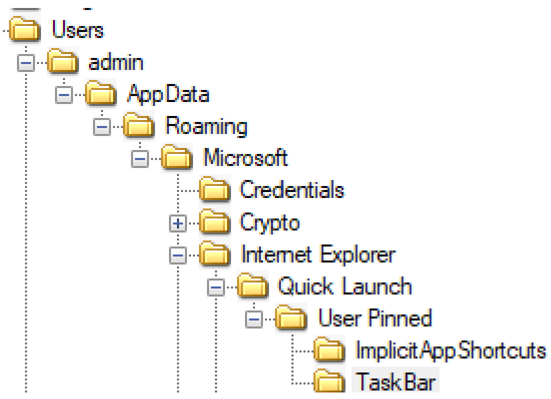
The last IP address associated with the machine can be found at SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces:



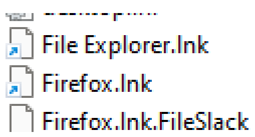
DHCPIP Address
ABC
192.168.2.242

Answer: 192.168.2.242

Which user had the most items pinned to their taskbar?



```
Users
  admin
    AppData
      Roaming
        Microsoft
          Credentials
          Crypto
          Internet Explorer
            Quick Launch
              User Pinned
                ImplicitAppShortcuts
                TaskBar
```



```
File Explorer.lnk
Firefox.lnk
Firefox.lnk.FileSlack
```

Answer: admin

What was the last run date of the executable with an MFT record number of 164885? (Format: MM/DD/YYYY HH:MM:SS (UTC).)

Answer: 04/12/2020 02:32:09

What is the log file sequence number for the file "fruit_Assortment.jpg"?

Answer: 1276820064

Jim has some dirt on the company stored in a docx file. Find it, the flag is the fourth secret, in the format of <"The flag is a sentence you put in quotes">. (Secrets, secrets are no fun)

Answer: Customer data is not stored securely

In the company Slack, what is threatened to be deactivated if the user gets their email deactivated?

Answer: kneecaps