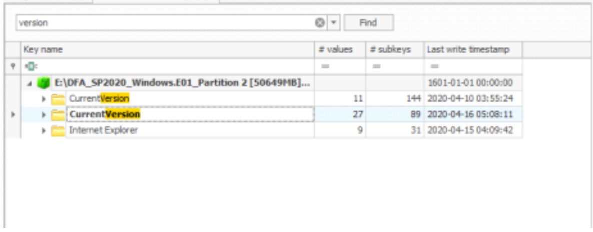
# CorporateSecrets Lab (Cyber Defenders) - Walkthrough

Wednesday, September 25, 2024 10:36 AM

Story:
A windows forensics challenge prepared by Champlain College Digital Forensics Association for their yearly CTF.
Your objective as a SOC analyst is to analyze the image and answer the question.

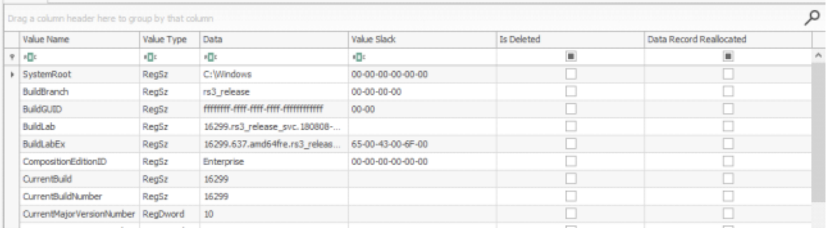
**Q1: What is the current build number on the system?**

- I loaded all the registry hives into 'Registry Explorer'.
  In the 'Software' hive, I searched for the 'CurrentVersion' key and found that the current build of the machine is **16299.**



version | Find

| Key name | # values | # subkeys | Last write timestamp |
|---|---|---|---|
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]... | | | 1601-01-01 00:00:00 |
| CurrentVersion | 11 | 144 | 2020-04-10 03:55:24 |
| CurrentVersion | 27 | 89 | 2020-04-16 05:08:11 |
| Internet Explorer | 9 | 31 | 2020-04-15 04:09:42 |

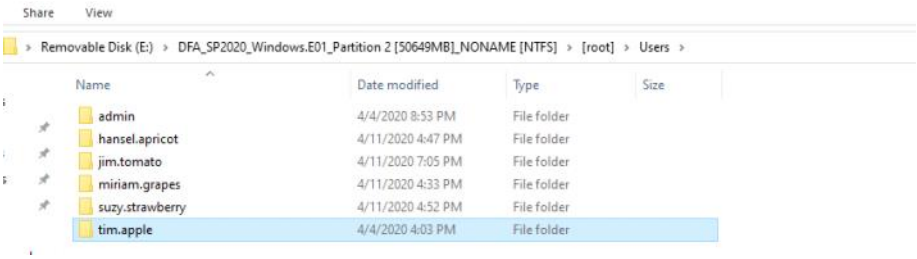


Drag a column header here to group by that column

| Value Name | Value Type | Data | Value Slack | Is Deleted | Data Record Reallocated |
|---|---|---|---|---|---|
| SystemRoot | RegSz | C:\Windows | 00-00-00-00-00-00 | □ | □ |
| BuildBranch | RegSz | rs3_release | 00-00-00-00 | □ | □ |
| BuildGUID | RegSz | ffffffff-ffff-ffff-ffff-ffffffffffff | 00-00 | □ | □ |
| BuildLab | RegSz | 16299.rs3_release_svc.180808-... | | □ | □ |
| BuildLabEx | RegSz | 16299.637.amd64fre.rs3_releas... | 65-00-43-00-6F-00 | □ | □ |
| CompositionEditionID | RegSz | Enterprise | 00-00-00-00-00-00 | □ | □ |
| CurrentBuild | RegSz | 16299 | | □ | □ |
| CurrentBuildNumber | RegSz | 16299 | | □ | □ |
| CurrentMajorVersionNumber | RegDword | 10 | | □ | □ |

**Q2: How many users are there?**

- I accessed to the 'Users' directory and counted the number of the users.
  The answer is **6**

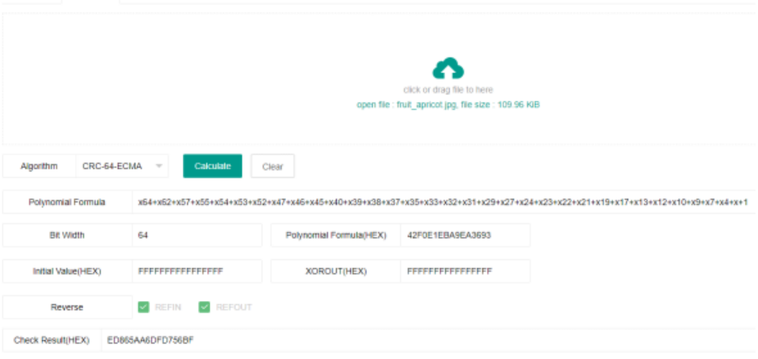


Removable Disk (E:) › DFA_SP2020_Windows.E01_Partition 2 [50649MB]_NONAME [NTFS] › [root] › Users ›

| Name | Date modified | Type | Size |
|---|---|---|---|
| admin | 4/4/2020 8:53 PM | File folder | |
| hansel.apricot | 4/11/2020 4:47 PM | File folder | |
| jim.tomato | 4/11/2020 7:05 PM | File folder | |
| miriam.grapes | 4/11/2020 4:33 PM | File folder | |
| suzy.strawberry | 4/11/2020 4:52 PM | File folder | |
| tim.apple | 4/4/2020 4:03 PM | File folder | |

**Q3: What is the CRC64 hash of the file "fruit_apricot.jpg"?**

- I searched for the file using the search box and uploaded it to this site, where I calculated the hash using the CRC-64-ECMA algorithm.

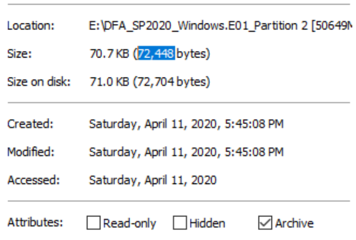


click or drag file to here
open file : fruit_apricot.jpg, file size : 109.96 KiB

| | | | |
|---|---|---|---|
| Algorithm | CRC-64-ECMA | | |
| Polynomial Formula | x64+x62+x57+x55+x54+x53+x52+x47+x46+x45+x40+x39+x38+x37+x35+x33+x32+x31+x29+x27+x24+x23+x22+x21+x19+x17+x13+x12+x10+x9+x7+x4+x+1 | | |
| Bit Width | 64 | Polynomial Formula(HEX) | 42F0E1EBA9EA3693 |
| Initial Value(HEX) | FFFFFFFFFFFFFFFF | XOROUT(HEX) | FFFFFFFFFFFFFFFF |
| Reverse | ☑ REFIN ☑ REFOUT | | |
| Check Result(HEX) | ED865AA6DFD756BF | | |

**Q4: What is the logical size of the file "strawberry.jpg" in bytes?**

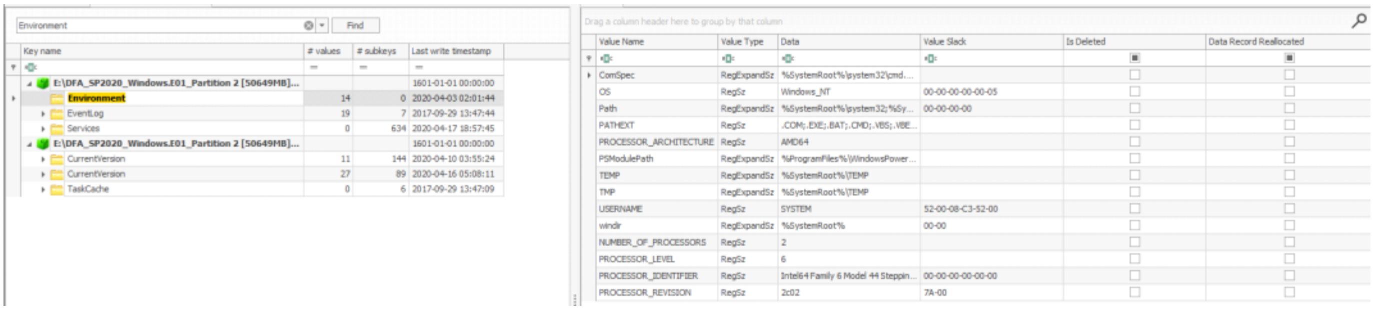
- I searched the file by the same method like before, I accessed the 'Properties' of the file and found the byte size of the file.



| | |
|---|---|
| Location: | E:\DFA_SP2020_Windows.E01_Partition 2 [50649M |
| Size: | 70.7 KB (72,448 bytes) |
| Size on disk: | 71.0 KB (72,704 bytes) |
| Created: | Saturday, April 11, 2020, 5:45:08 PM |
| Modified: | Saturday, April 11, 2020, 5:45:08 PM |
| Accessed: | Saturday, April 11, 2020 |
| Attributes: | □ Read-only □ Hidden ☑ Archive |

**Q5: What is the processor architecture of the system? (one word)**

- To address this question, I used Registry Explorer again and search in the 'System' Hive the key ControlSet001\Control\Session Manager\E**nvironment** which retrieved OS information including the processor architecture.



Environment ⊗ ▾ Find

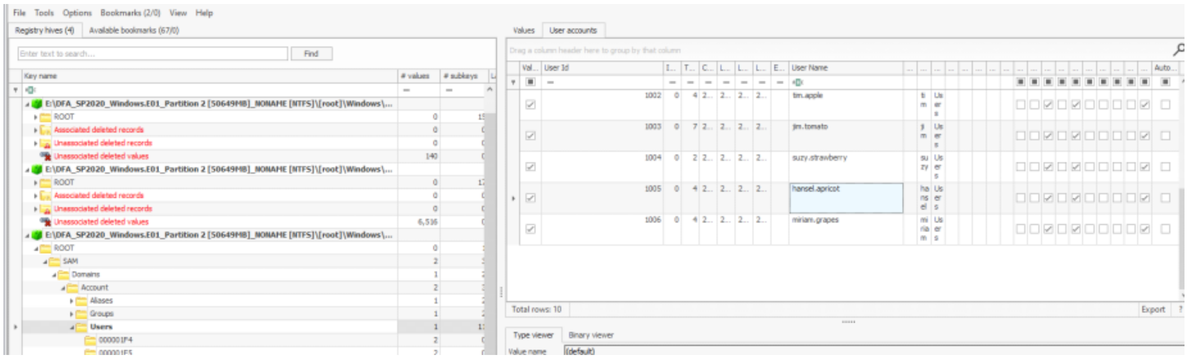
| Key name | # values | # subkeys | Last write timestamp |
|---|---|---|---|
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]... | | | 1601-01-01 00:00:00 |
| Environment | 14 | 0 | 2020-04-03 02:01:44 |
| EventLog | 19 | 7 | 2017-09-29 13:47:44 |
| Services | 0 | 634 | 2020-04-17 18:57:45 |
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]... | | | 1601-01-01 00:00:00 |
| CurrentVersion | 11 | 144 | 2020-04-10 03:55:24 |
| CurrentVersion | 27 | 89 | 2020-04-16 05:08:11 |
| TaskCache | 0 | 6 | 2017-09-29 13:47:09 |

Drag a column header here to group by that column

| Value Name | Value Type | Data | Value Slack | Is Deleted | Data Record Reallocated |
|---|---|---|---|---|---|
| ComSpec | RegExpandSz | %SystemRoot%\system32\cmd.... | | ☐ | ☐ |
| OS | RegSz | Windows_NT | 00-00-00-00-00-05 | ☐ | ☐ |
| Path | RegExpandSz | %SystemRoot%\system32;%Sy... | 00-00-00-00 | ☐ | ☐ |
| PATHEXT | RegSz | .COM;.EXE;.BAT;.CMD;.VBS;.VBE... | | ☐ | ☐ |
| PROCESSOR_ARCHITECTURE | RegSz | AMD64 | | ☐ | ☐ |
| PSModulePath | RegExpandSz | %ProgramFiles%\WindowsPower... | | ☐ | ☐ |
| TEMP | RegExpandSz | %SystemRoot%\TEMP | | ☐ | ☐ |
| TMP | RegExpandSz | %SystemRoot%\TEMP | | ☐ | ☐ |
| USERNAME | RegSz | SYSTEM | 52-00-08-C3-52-00 | ☐ | ☐ |
| windir | RegExpandSz | %SystemRoot% | 00-00 | ☐ | ☐ |
| NUMBER_OF_PROCESSORS | RegSz | 2 | | ☐ | ☐ |
| PROCESSOR_LEVEL | RegSz | 6 | | ☐ | ☐ |
| PROCESSOR_IDENTIFIER | RegSz | Intel64 Family 6 Model 44 Steppin... | 00-00-00-00-00-00 | ☐ | ☐ |
| PROCESSOR_REVISION | RegSz | 2c02 | 7A-00 | ☐ | ☐ |

**Q6:Which user has a photo of a dog in their recycling bin?**

- I navigated through the Recycle Bin of all users until I found some JPGs in the Recycle Bin of the user associated with the SID S-1-5-21-2446097003-76624807-2828106174-1005.
  I then loaded the SAM hive, navigated to SAM\Domains\Account\Users, and found that SID 1005 was related to **'hansel.apricot'.**



File Tools Options Bookmarks (2/0) View Help
Registry hives (4) Available bookmarks (67/0)
Enter text to search... Find
Values User accounts

| Key name | # values | # subkeys |
|---|---|---|
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]_NONAME [NTFS]\[root]\Windows\... | | |
| ROOT | 0 | 15 |
| Associated deleted records | 0 | 0 |
| Unassociated deleted records | 0 | 0 |
| Unassociated deleted values | 140 | 0 |
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]_NONAME [NTFS]\[root]\Windows\... | | |
| ROOT | 0 | 17 |
| Associated deleted records | 0 | 0 |
| Unassociated deleted records | 0 | 0 |
| Unassociated deleted values | 6,516 | 0 |
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]_NONAME [NTFS]\[root]\Windows\... | | |
| ROOT | 0 | [illegible] |
| SAM | 2 | [illegible] |
| Domains | 1 | [illegible] |
| Account | 2 | [illegible] |
| Aliases | 1 | [illegible] |
| Groups | 1 | [illegible] |
| Users | 1 | 11 |
| 000001F4 | 2 | 0 |
| 000001F5 | 2 | 0 |

Drag a column header here to group by that column

| Val... | User Id | I... | T... | C... | L... | L... | L... | E... | User Name | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | Auto... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | 1002 | 0 | 4 | 2... | 2... | 2... | 2... | | tim.apple | | tim | Users | | | | | | ☐ | ☐ | ☑ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ |
| ☑ | 1003 | 0 | 7 | 2... | 2... | 2... | 2... | | jim.tomato | | jim | Users | | | | | | ☐ | ☐ | ☑ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ |
| ☑ | 1004 | 0 | 2 | 2... | 2... | 2... | 2... | | suzy.strawberry | | suzy | Users | | | | | | ☐ | ☐ | ☑ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ |
| ☑ | 1005 | 0 | 4 | 2... | 2... | 2... | 2... | | hansel.apricot | | hansel | Users | | | | | | ☐ | ☐ | ☑ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ |
| ☑ | 1006 | 0 | 4 | 2... | 2... | 2... | 2... | | miriam.grapes | | miriam | Users | | | | | | ☐ | ☐ | ☑ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ |

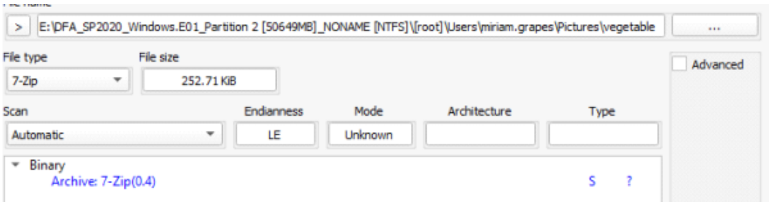
Total rows: 10

Value name (default)

**Note:** You are able to find via SID with the associated username via Microsoft\Windows NT \CurrentVersion\ProfileList

**Q7: What type of file is "vegetable"? Provide the extension without a dot.**

- I searched via the search box the file and used 'Detect It Easy' to find the file extension



> E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]_NONAME [NTFS]\[root]\Users\miriam.grapes\Pictures\vegetable

File type: 7-Zip

File size: 252.71 KiB

☐ Advanced

Scan: Automatic

Endianness: LE

Mode: Unknown

Architecture:

Type:

Binary

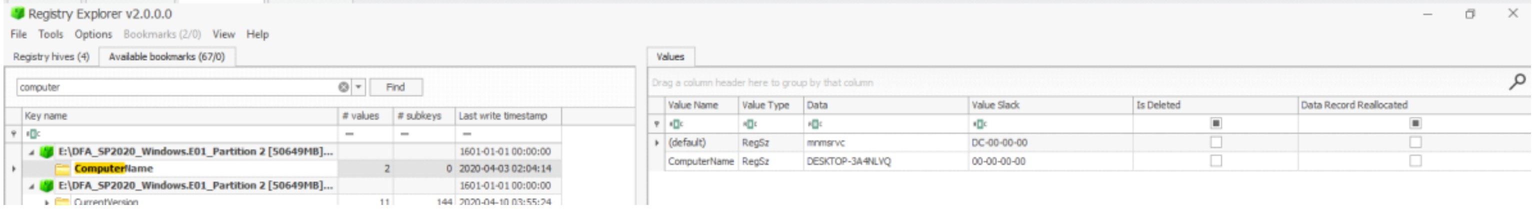
Archive: 7-Zip(0.4)

**Q8: What type of girls does Miriam Grapes design phones for (Target audience)?**

- I investigated the browsing history of the user and found Miriam searched via Firefox 'What is VCSO girl? Shop the latest teen trend'
  The answer is **'VSCO'**

**Q9: What is the name of the device?**

- **I searched in the 'SYSTEM' hive the 'ComputerName' key which located at** 'ControlSet001 \Control\ComputerName\' to find the hostname



Registry Explorer v2.0.0.0
File Tools Options Bookmarks (2/0) View Help
Registry hives (4) Available bookmarks (67/0)
Values

computer ⊗ ▾ Find

| Key name | # values | # subkeys | Last write timestamp |
|---|---|---|---|
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]... | | | 1601-01-01 00:00:00 |
| ComputerName | 2 | 0 | 2020-04-03 02:04:14 |
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]... | | | 1601-01-01 00:00:00 |
| CurrentVersion | 11 | 144 | 2020-04-10 03:55:24 |

Drag a column header here to group by that column

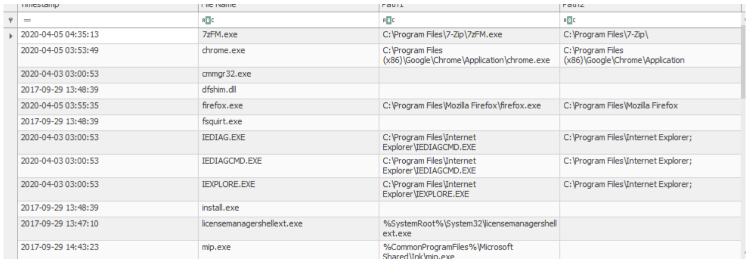
| Value Name | Value Type | Data | Value Slack | Is Deleted | Data Record Reallocated |
|---|---|---|---|---|---|
| (default) | RegSz | mnmsrvc | DC-00-00-00 | ☐ | ☐ |
| ComputerName | RegSz | DESKTOP-3A4NLVQ | 00-00-00-00 | ☐ | ☐ |

**Q10: What is the SID of the machine?**

- We already found it the question 6 **(S-1-5-21-2446097003-76624807-2828106174**)

**Q11: How many web browsers are present?**

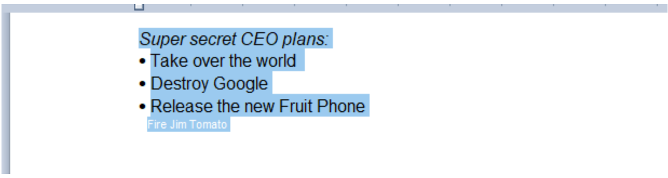
- I accessed the SOFTWARE\Microsoft\Windows\CurrentVersion\**App Paths** key to identify the installed web browsers and found only three: Internet Explorer, Firefox, and Google Chrome. However, the expected total is five. I couldn't find any information online to explain this discrepancy.



| Timestamp | File Name | Path1 | Path2 |
|---|---|---|---|
| 2020-04-05 04:35:13 | 7zFM.exe | C:\Program Files\7-Zip\7zFM.exe | C:\Program Files\7-Zip\ |
| 2020-04-05 03:53:49 | chrome.exe | C:\Program Files (x86)\Google\Chrome\Application\chrome.exe | C:\Program Files (x86)\Google\Chrome\Application |
| 2020-04-03 03:00:53 | cmmgr32.exe | | |
| 2017-09-29 13:48:39 | dfshim.dll | | |
| 2020-04-05 03:55:35 | firefox.exe | C:\Program Files\Mozilla Firefox\firefox.exe | C:\Program Files\Mozilla Firefox |
| 2017-09-29 13:48:39 | fsquirt.exe | | |
| 2020-04-03 03:00:53 | IEDIAG.EXE | C:\Program Files\Internet Explorer\IEDIAGCMD.EXE | C:\Program Files\Internet Explorer; |
| 2020-04-03 03:00:53 | IEDIAGCMD.EXE | C:\Program Files\Internet Explorer\IEDIAGCMD.EXE | C:\Program Files\Internet Explorer; |
| 2020-04-03 03:00:53 | IEXPLORE.EXE | C:\Program Files\Internet Explorer\IEXPLORE.EXE | C:\Program Files\Internet Explorer; |
| 2017-09-29 13:48:39 | install.exe | | |
| 2017-09-29 13:47:10 | licensemanagershellext.exe | %SystemRoot%\System32\licensemanagershellext.exe | |
| 2017-09-29 14:43:23 | mip.exe | %CommonProgramFiles%\Microsoft Shared\Ink\mip.exe | |

**Q12: How many super-secret CEO plans does Tim have? (Dr. Doofenshmirtz Type Beat)**

- I navigated in Tim directory and accessed to 'Documents' folder, I identified a file named 'Secret' I opened it and found the answer (4).
  We are able to see only 3, but if you are copying the secrets there is an hidden one.



Super secret CEO plans:
- Take over the world
- Destroy Google
- Release the new Fruit Phone

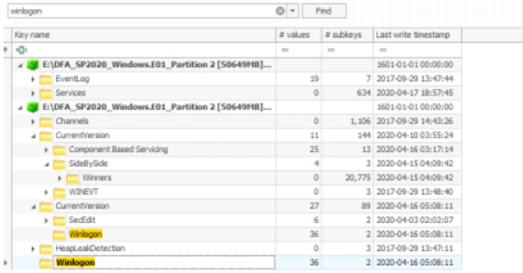
Fire Jim Tomato

**Q13: Which employee does Tim plan to fire? (He's Dead, Tim. Enter the full name- two words - space separated)**

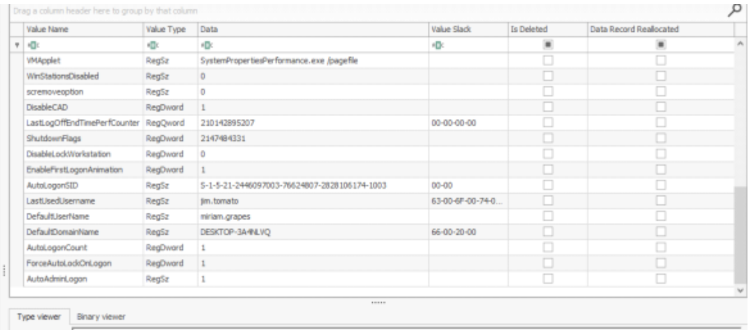
- The answer is the hidden secret - **Jim Tomato**

**Q14: What was the last used username? (I didn't start this conversation, but I'm ending it!)**

- I just found a registry key I didn't know about, the 'Winlogon' key, which is located in the 'Software' hive at Microsoft\Windows NT\CurrentVersion\Winlogon.
  This key provides the last used username, in our case, it's '**Jim.Tomato**'.



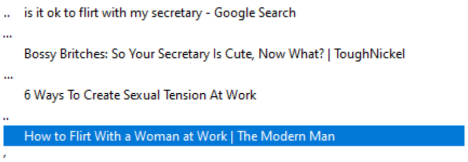
| Key name | # values | # subkeys | Last write timestamp |
|---|---|---|---|
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]... | | | 1601-01-01 00:00:00 |
| EventLog | 19 | 7 | 2017-09-29 13:47:44 |
| Services | 0 | 634 | 2020-04-17 18:57:45 |
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]... | | | 1601-01-01 00:00:00 |
| Channels | 0 | 1,106 | 2017-09-29 14:43:26 |
| CurrentVersion | 11 | 144 | 2020-04-10 03:55:24 |
| Component Based Servicing | 25 | 13 | 2020-04-16 03:17:14 |
| SideBySide | 4 | 3 | 2020-04-15 04:09:42 |
| Winners | 0 | 20,775 | 2020-04-15 04:09:42 |
| WINEVT | 0 | 3 | 2017-09-29 13:48:40 |
| CurrentVersion | 27 | 89 | 2020-04-16 05:08:11 |
| SecEdit | 6 | 2 | 2020-04-03 02:02:07 |
| Winlogon | 36 | 2 | 2020-04-16 05:08:11 |
| HeapLeakDetection | 0 | 3 | 2017-09-29 13:47:11 |
| Winlogon | 36 | 2 | 2020-04-16 05:08:11 |



| Value Name | Value Type | Data | Value Slack | Is Deleted | Data Record Reallocated |
|---|---|---|---|---|---|
| VMApplet | RegSz | SystemPropertiesPerformance.exe /pagefile | | □ | □ |
| WinStationsDisabled | RegSz | 0 | | □ | □ |
| scremoveoption | RegSz | 0 | | □ | □ |
| DisableCAD | RegDword | 1 | | □ | □ |
| LastLogOffEndTimePerfCounter | RegQword | 210142895207 | 00-00-00-00 | □ | □ |
| ShutdownFlags | RegDword | 2147484331 | | □ | □ |
| DisableLockWorkstation | RegDword | 0 | | □ | □ |
| EnableFirstLogonAnimation | RegDword | 1 | | □ | □ |
| AutoLogonSID | RegSz | S-1-5-21-2446097003-76624807-2828106174-1003 | 00-00 | □ | □ |
| LastUsedUsername | RegSz | jim.tomato | 63-00-6F-00-74-0... | □ | □ |
| DefaultUserName | RegSz | miriam.grapes | | □ | □ |
| DefaultDomainName | RegSz | DESKTOP-3A4NLVQ | 66-00-20-00 | □ | □ |
| AutoLogonCount | RegDword | 1 | | □ | □ |
| ForceAutoLockOnLogon | RegDword | 1 | | □ | □ |
| AutoAdminLogon | RegSz | 1 | | □ | □ |

**Q15: What was the role of the employee Tim was flirting with?**

- I used "Browsing History" by Nirsoft and found that Tim searched for: **The answer is 'Secretary.'**



is it ok to flirt with my secretary - Google Search

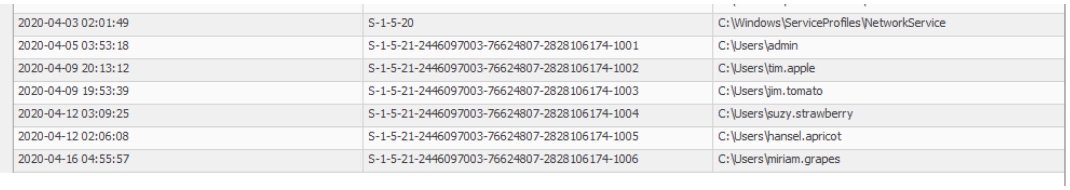
Bossy Britches: So Your Secretary Is Cute, Now What? | ToughNickel

6 Ways To Create Sexual Tension At Work

How to Flirt With a Woman at Work | The Modern Man

**Q16: What is the SID of the user "suzy.strawberry"?**

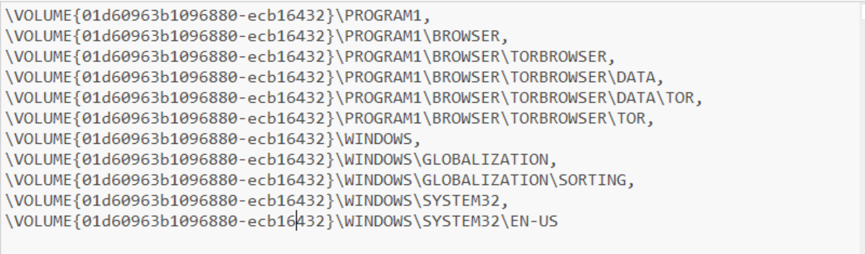
- As before, I accessed to Microsoft\Windows NT\CurrentVersion\ProfileList and found the SID of the mentioned user.



| | | |
|---|---|---|
| 2020-04-03 02:01:49 | S-1-5-20 | C:\Windows\ServiceProfiles\NetworkService |
| 2020-04-05 03:53:18 | S-1-5-21-2446097003-76624807-2828106174-1001 | C:\Users\admin |
| 2020-04-09 20:13:12 | S-1-5-21-2446097003-76624807-2828106174-1002 | C:\Users\tim.apple |
| 2020-04-09 19:53:39 | S-1-5-21-2446097003-76624807-2828106174-1003 | C:\Users\jim.tomato |
| 2020-04-12 03:09:25 | S-1-5-21-2446097003-76624807-2828106174-1004 | C:\Users\suzy.strawberry |
| 2020-04-12 02:06:08 | S-1-5-21-2446097003-76624807-2828106174-1005 | C:\Users\hansel.apricot |
| 2020-04-16 04:55:57 | S-1-5-21-2446097003-76624807-2828106174-1006 | C:\Users\miriam.grapes |

**Q17: List the file path for the install location of the Tor Browser.**

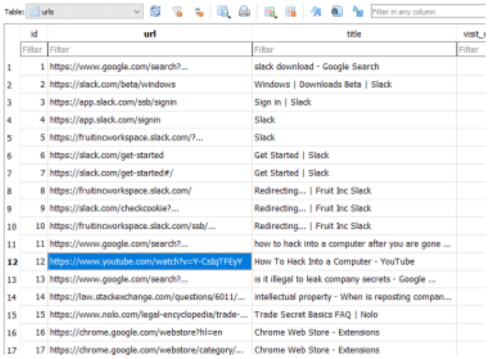
- To address this question, I parsed the Prefetch directory via 'PECmd' by Eric Zimmerman.
  I searched the keyword 'Tor' and found the directory is **'C:\Program1'**



```
\VOLUME{01d60963b1096880-ecb16432}\PROGRAM1,
\VOLUME{01d60963b1096880-ecb16432}\PROGRAM1\BROWSER,
\VOLUME{01d60963b1096880-ecb16432}\PROGRAM1\BROWSER\TORBROWSER,
\VOLUME{01d60963b1096880-ecb16432}\PROGRAM1\BROWSER\TORBROWSER\DATA,
\VOLUME{01d60963b1096880-ecb16432}\PROGRAM1\BROWSER\TORBROWSER\DATA\TOR,
\VOLUME{01d60963b1096880-ecb16432}\PROGRAM1\BROWSER\TORBROWSER\TOR,
\VOLUME{01d60963b1096880-ecb16432}\WINDOWS,
\VOLUME{01d60963b1096880-ecb16432}\WINDOWS\GLOBALIZATION,
\VOLUME{01d60963b1096880-ecb16432}\WINDOWS\GLOBALIZATION\SORTING,
\VOLUME{01d60963b1096880-ecb16432}\WINDOWS\SYSTEM32,
\VOLUME{01d60963b1096880-ecb16432}\WINDOWS\SYSTEM32\EN-US
```

**Q18: What was the URL for the Youtube video watched by Jim?**

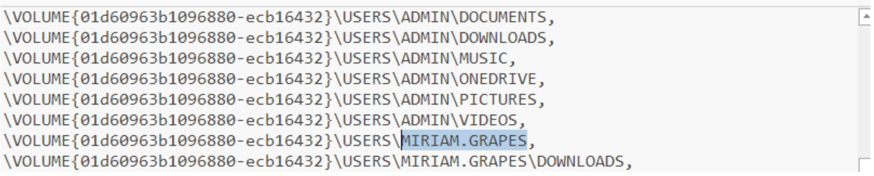
- **I loaded the 'Hisotory' file of Google Chrome via SQLite DB and found the YouTube URL Jim watched**
  How To Hack Into a Computer



| | id | url | title | visit_ |
|---|---|---|---|---|
| | Filter | Filter | Filter | Filter |
| 1 | 1 | https://www.google.com/search?... | slack download - Google Search | |
| 2 | 2 | https://slack.com/beta/windows | Windows \| Downloads Beta \| Slack | |
| 3 | 3 | https://app.slack.com/ssb/signin | Sign in \| Slack | |
| 4 | 4 | https://app.slack.com/signin | Slack | |
| 5 | 5 | https://fruitincworkspace.slack.com/?... | Slack | |
| 6 | 6 | https://slack.com/get-started | Get Started \| Slack | |
| 7 | 7 | https://slack.com/get-started#/ | Get Started \| Slack | |
| 8 | 8 | https://fruitincworkspace.slack.com/ | Redirecting... \| Fruit Inc Slack | |
| 9 | 9 | https://slack.com/checkcookie?... | Redirecting... \| Fruit Inc Slack | |
| 10 | 10 | https://fruitincworkspace.slack.com/ssb/... | Redirecting... \| Fruit Inc Slack | |
| 11 | 11 | https://www.google.com/search?... | how to hack into a computer after you are gone ... | |
| 12 | 12 | https://www.youtube.com/watch?v=Y-CsIqTFEyY | How To Hack Into a Computer - YouTube | |
| 13 | 13 | https://www.google.com/search?... | is it illegal to leak company secrets - Google ... | |
| 14 | 14 | https://law.stackexchange.com/questions/6011/... | intellectual property - When is reposting compan... | |
| 15 | 15 | https://www.nolo.com/legal-encyclopedia/trade-... | Trade Secret Basics FAQ \| Nolo | |
| 16 | 16 | https://chrome.google.com/webstore?hl=en | Chrome Web Store - Extensions | |
| 17 | 17 | https://chrome.google.com/webstore/category/... | Chrome Web Store - Extensions | |

**Q19: Which user installed LibreCAD on the system?**

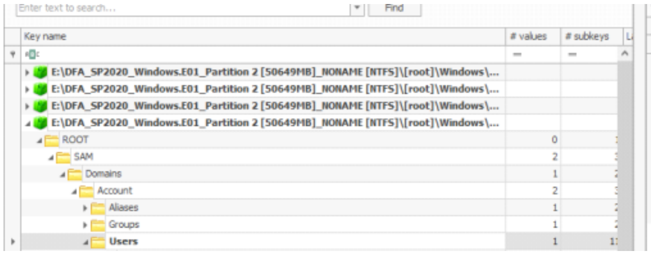
- I used the parsed Prefetch CSV to search for 'LibreCAD' and found the installation file.
  I accessed the 'Directories' and discovered that the file was located in the 'Downloads' directory of MIRIAM.GRAPES.



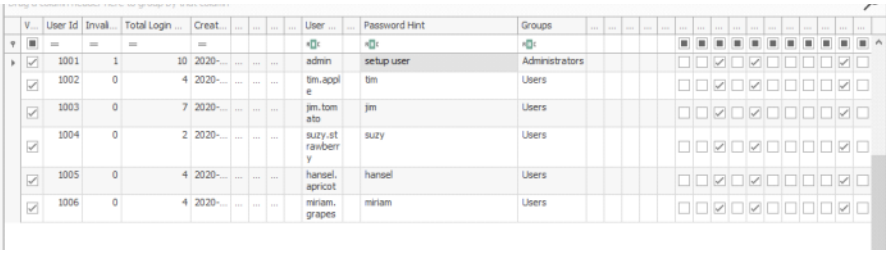
```
\VOLUME{01d60963b1096880-ecb16432}\USERS\ADMIN\DOCUMENTS,
\VOLUME{01d60963b1096880-ecb16432}\USERS\ADMIN\DOWNLOADS,
\VOLUME{01d60963b1096880-ecb16432}\USERS\ADMIN\MUSIC,
\VOLUME{01d60963b1096880-ecb16432}\USERS\ADMIN\ONEDRIVE,
\VOLUME{01d60963b1096880-ecb16432}\USERS\ADMIN\PICTURES,
\VOLUME{01d60963b1096880-ecb16432}\USERS\ADMIN\VIDEOS,
\VOLUME{01d60963b1096880-ecb16432}\USERS\MIRIAM.GRAPES,
\VOLUME{01d60963b1096880-ecb16432}\USERS\MIRIAM.GRAPES\DOWNLOADS,
```

**Q20: How many times "admin" logged into the system?**

- To address this question, I accessed to the SAM hive to 'Users' key.
  By Registry Explorer you are able to see the number of the loggings that performed by the user.



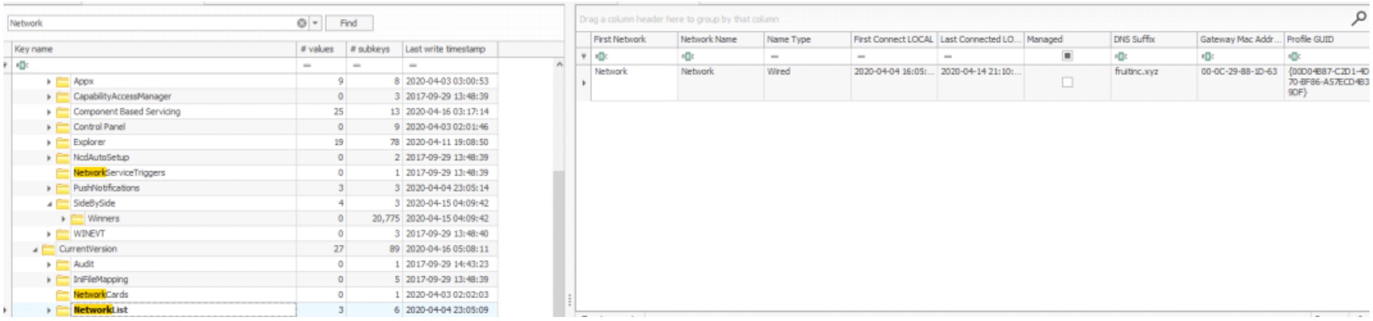
| Key name | # values | # subkeys |
|---|---|---|
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]_NONAME [NTFS]\[root]\Windows\... | | |
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]_NONAME [NTFS]\[root]\Windows\... | | |
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]_NONAME [NTFS]\[root]\Windows\... | | |
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]_NONAME [NTFS]\[root]\Windows\... | | |
| ROOT | 0 | |
| SAM | 2 | |
| Domains | 1 | |
| Account | 2 | |
| Aliases | 1 | |
| Groups | 1 | |
| Users | 1 | |



| V... | User Id | Invali... | Total Login ... | Creat... | ... | ... | ... | ... | User ... | ... | Password Hint | Groups | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | 1001 | 1 | 10 | 2020-... | ... | ... | ... | | admin | | setup user | Administrators | | | | | | □ | □ | ☑ | □ | ☑ | □ | □ | □ | □ | ☑ | □ |
| ☑ | 1002 | 0 | 4 | 2020-... | ... | ... | ... | | tim.apple | | tim | Users | | | | | | □ | □ | ☑ | □ | ☑ | □ | □ | □ | □ | ☑ | □ |
| ☑ | 1003 | 0 | 7 | 2020-... | ... | ... | ... | | jim.tomato | | jim | Users | | | | | | □ | □ | ☑ | □ | ☑ | □ | □ | □ | □ | ☑ | □ |
| ☑ | 1004 | 0 | 2 | 2020-... | ... | ... | ... | | suzy.strawberry | | suzy | Users | | | | | | □ | □ | ☑ | □ | ☑ | □ | □ | □ | □ | ☑ | □ |
| ☑ | 1005 | 0 | 4 | 2020-... | ... | ... | ... | | hansel.apricot | | hansel | Users | | | | | | □ | □ | ☑ | □ | ☑ | □ | □ | □ | □ | ☑ | □ |
| ☑ | 1006 | 0 | 4 | 2020-... | ... | ... | ... | | miriam.grapes | | miriam | Users | | | | | | □ | □ | ☑ | □ | ☑ | □ | □ | □ | □ | ☑ | □ |

**Q21: What is the name of the DHCP domain the device was connected to?**

- In the 'Software' hive, within the 'NetworkList' key located at Microsoft\Windows NT \CurrentVersion\NetworkList, you can find the DHCP domain in the 'DNS Suffix' section.



Network

| Key name | # values | # subkeys | Last write timestamp |
|---|---|---|---|
| Appx | 9 | 8 | 2020-04-03 03:00:53 |
| CapabilityAccessManager | 0 | 3 | 2017-09-29 13:48:39 |
| Component Based Servicing | 25 | 13 | 2020-04-16 03:17:14 |
| Control Panel | 0 | 9 | 2020-04-03 02:01:46 |
| Explorer | 19 | 78 | 2020-04-11 19:08:50 |
| NcdAutoSetup | 0 | 2 | 2017-09-29 13:48:39 |
| NetworkServiceTriggers | 0 | 1 | 2017-09-29 13:48:39 |
| PushNotifications | 3 | 3 | 2020-04-04 23:05:14 |
| SideBySide | 4 | 3 | 2020-04-15 04:09:42 |
| Winners | 0 | 20,775 | 2020-04-15 04:09:42 |
| WINEVT | 0 | 3 | 2017-09-29 13:48:40 |
| CurrentVersion | 27 | 89 | 2020-04-16 05:08:11 |
| Audit | 0 | 1 | 2017-09-29 14:43:23 |
| IniFileMapping | 0 | 5 | 2017-09-29 13:48:39 |
| NetworkCards | 0 | 1 | 2020-04-03 02:02:03 |
| NetworkList | 3 | 6 | 2020-04-04 23:05:09 |

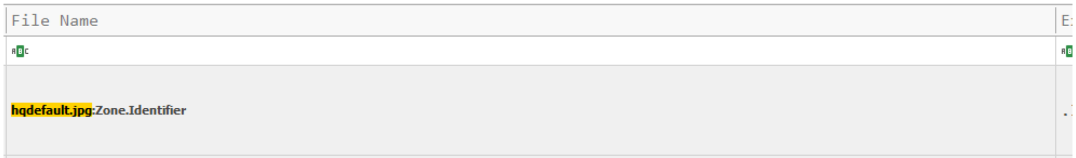
Drag a column header here to group by that column

| First Network | Network Name | Name Type | First Connect LOCAL | Last Connected LO... | Managed | DNS Suffix | Gateway Mac Addr... | Profile GUID |
|---|---|---|---|---|---|---|---|---|
| Network | Network | Wired | 2020-04-04 16:05:... | 2020-04-14 21:10:... | □ | fruitinc.xyz | 00-0C-29-88-1D-63 | {00D04B87-C2D1-4D70-BF86-A57ECD4B39DF} |

**Q22: What time did Tim download his background image? (Oh Boy 3AM . Answer in MM/DD/YYYY HH:MM format (UTC).)**

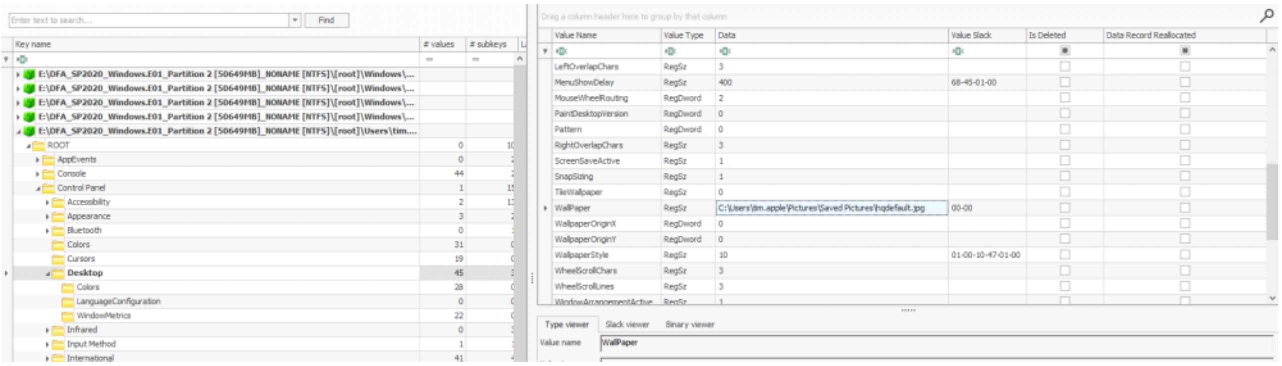
- I loaded NTUSER.dat into Registry Explorer and accessed the \Control Panel\Desktop key. Within this key, we can see the wallpaper image, which in our case is named 'hqdefault.jpg'.

  I then parsed the $MFT to determine when the image was downloaded by the user. I searched for the image name and found an entry with the 'Zone Identifier', which indicates that the file was downloaded from the web. The file was created on the system at: **2020-04-05 03:49:53**.



File Name

hqdefault.jpg:Zone.Identifier



Enter text to search...

| Key name | # values |
|---|---|
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]_NONAME [NTFS]\[root]\Windows\... | |
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]_NONAME [NTFS]\[root]\Windows\... | |
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]_NONAME [NTFS]\[root]\Windows\... | |
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]_NONAME [NTFS]\[root]\Windows\... | |
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]_NONAME [NTFS]\[root]\Users\tim.... | |
| ROOT | 0 |
| AppEvents | 0 |
| Console | 44 |
| Control Panel | 1 |
| Accessibility | 2 |
| Appearance | 3 |
| Bluetooth | 0 |
| Colors | 31 |
| Cursors | 19 |
| Desktop | 45 |
| Colors | 28 |
| LanguageConfiguration | 0 |
| WindowMetrics | 22 |
| Infrared | 0 |
| Input Method | 1 |
| International | 41 |

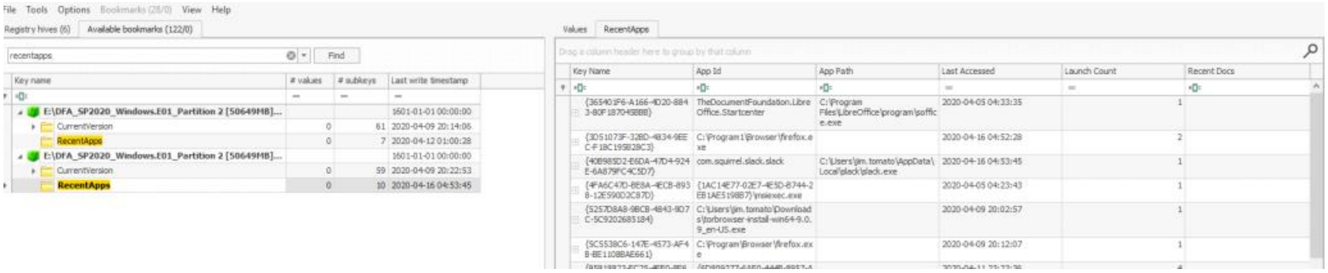
Drag a column header here to group by that column

| Value Name | Value Type | Data | Value Slack | Is Deleted | Data Record Reallocated |
|---|---|---|---|---|---|
| LeftOverlapChars | RegSz | 3 | | □ | □ |
| MenuShowDelay | RegSz | 400 | 68-45-01-00 | □ | □ |
| MouseWheelRouting | RegDword | 2 | | □ | □ |
| PaintDesktopVersion | RegDword | 0 | | □ | □ |
| Pattern | RegDword | 0 | | □ | □ |
| RightOverlapChars | RegSz | 3 | | □ | □ |
| ScreenSaveActive | RegSz | 1 | | □ | □ |
| SnapSizing | RegSz | 1 | | □ | □ |
| TileWallpaper | RegSz | 0 | | □ | □ |
| WallPaper | RegSz | C:\Users\tim.apple\Pictures\Saved Pictures\hqdefault.jpg | 00-00 | □ | □ |
| WallpaperOriginX | RegDword | 0 | | □ | □ |
| WallpaperOriginY | RegDword | 0 | | □ | □ |
| WallpaperStyle | RegSz | 10 | 01-00-10-47-01-00 | □ | □ |
| WheelScrollChars | RegSz | 3 | | □ | □ |
| WheelScrollLines | RegSz | 3 | | □ | □ |
| WindowArrangementActive | RegSz | 1 | | □ | □ |

Value name: WallPaper

**Q23: How many times did Jim launch the Tor Browser?**

- This was a tricky one, I used the hint to find the answer.
  Initially, I accessed the 'UserAssist' key, which indicates how many times the user interacted with the shell or applications. I found the launch of Tor, but it was not the answer. After using the hint, I searched the 'RecentApps' key and found 'Firefox.exe,' which is located in the directory of the Tor Browser. It was executed two times.



recentapps

| Key name | # values | # subkeys | Last write timestamp |
|---|---|---|---|
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]... | | | 1601-01-01 00:00:00 |
| CurrentVersion | 0 | 61 | 2020-04-09 20:14:06 |
| RecentApps | 0 | 7 | 2020-04-12 01:00:28 |
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]... | | | 1601-01-01 00:00:00 |
| CurrentVersion | 0 | 59 | 2020-04-09 20:22:53 |
| RecentApps | 0 | 10 | 2020-04-16 04:53:45 |

Drag a column header here to group by that column

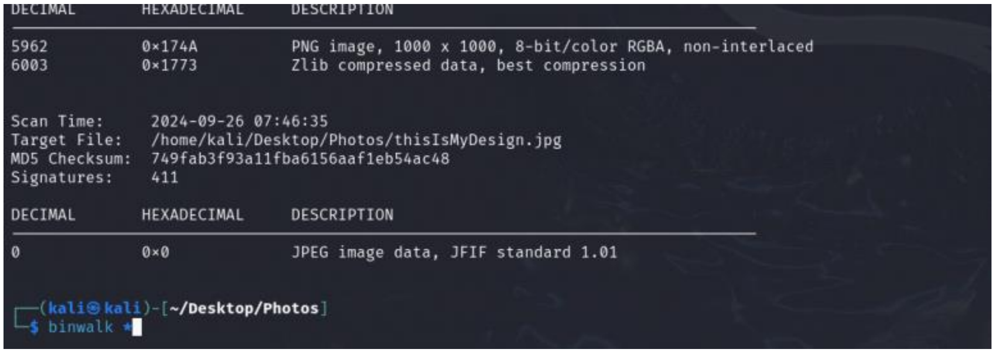
| Key Name | App Id | App Path | Last Accessed | Launch Count | Recent Docs |
|---|---|---|---|---|---|
| {365401F6-A166-4D20-8843-80F18704S8B8} | TheDocumentFoundation.LibreOffice.Startcenter | C:\Program Files\LibreOffice\program\soffice.exe | 2020-04-05 04:33:35 | 1 | |
| {3D51073F-32BD-4834-9EEC-F1BC195B28C3} | C:\Program1\Browser\firefox.exe | | 2020-04-16 04:52:28 | 2 | |
| {40B985D2-E6DA-47D4-924E-6A879FC4C5D7} | com.squirrel.slack.slack | C:\Users\jim.tomato\AppData\Local\slack\slack.exe | 2020-04-16 04:53:45 | 1 | |
| {4FA6C47D-BE8A-4ECB-8938-12E590D2C87D} | {1AC14E77-02E7-4E5D-8744-2EB1AE5198B7}\msiexec.exe | | 2020-04-05 04:23:43 | 1 | |
| {5257D8A8-9BCB-4843-9D7C-5C9202685184} | C:\Users\jim.tomato\Downloads\torbrowser-install-win64-9.0.9_en-US.exe | | 2020-04-09 20:02:57 | 1 | |
| {5C5538C6-147E-4573-AF4B-BE1108BAE661} | C:\Program\Browser\firefox.exe | | 2020-04-09 20:12:07 | 1 | |

**Q24:There is a png photo of an iPhone in Grapes's files. Find it and provide the SHA-1 hash.**

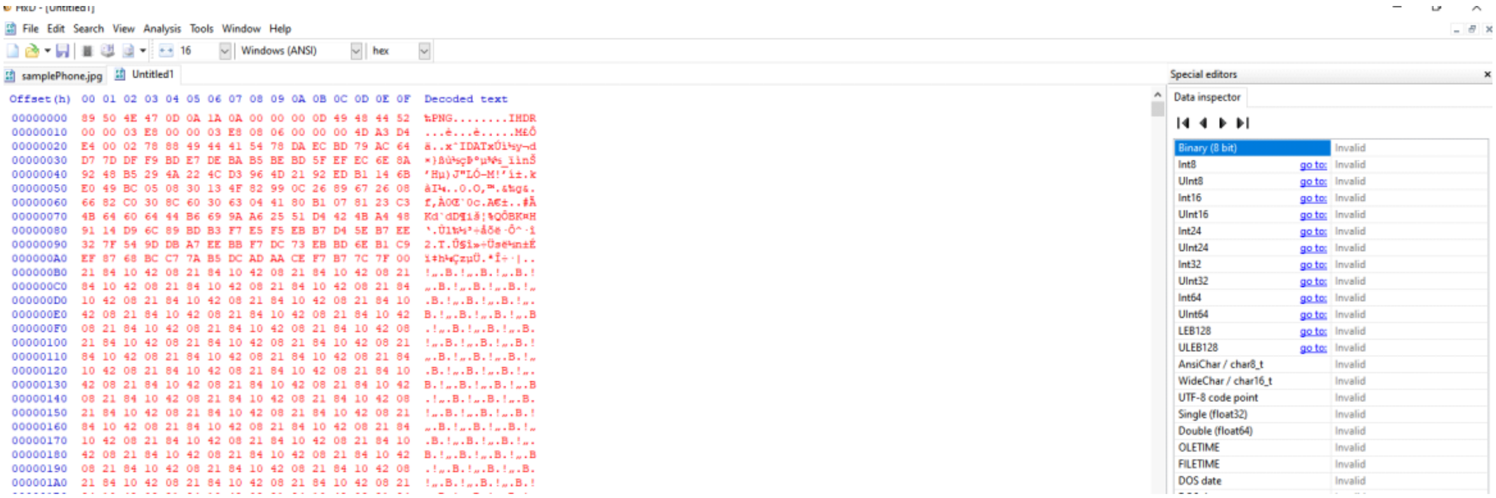
- I extracted all the photos found in the user's folder and used 'Binwalk' to check for any hidden data. During the analysis, I discovered that the image 'thisismyDesign' contained an embedded PNG file.

  Using 'HxD', I opened the file and searched for the PNG signature (89 50 4E 47 0D 0A 1A 0A), which I referenced from Gary Kasler's site.
  I found the signature and identified that the PNG file extended to the end of the image, indicated by the text 'IEND®B'.

  I then copied this section into a new file using 'HxD' and saved it as a PNG.
  Success! The extracted image turned out to be an iPhone photo. Finally, I used the 'Certutil' utility to extract its SHA1 hash.

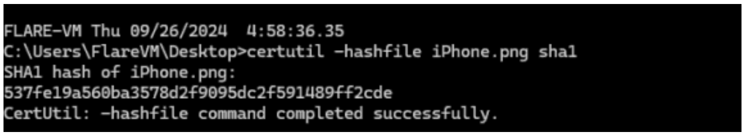


```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
5962          0x174A          PNG image, 1000 x 1000, 8-bit/color RGBA, non-interlaced
6003          0x1773          Zlib compressed data, best compression


Scan Time:     2024-09-26 07:46:35
Target File:   /home/kali/Desktop/Photos/thisIsMyDesign.jpg
MD5 Checksum:  749fab3f93a11fba6156aaf1eb54ac48
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01


┌──(kali㉿kali)-[~/Desktop/Photos]
└─$ binwalk *
```



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

00000000  89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  ‰PNG........IHDR
00000010  00 00 03 E8 00 00 03 E8 08 06 00 00 00 4D A3 D4  ...è...è.....M£Ô
00000020  E4 00 02 78 88 49 44 41 54 78 DA EC BD 79 AC 64  ä..xˆIDATxÚì½y¬d
00000030  D7 7D DF F9 BD E7 DE BA B5 BE BD 5F EF EC 6E 8A  ×}ßù½çÞºµ¾½_ïìnŠ
00000040  92 48 B5 29 4A 22 4C D3 96 4D 21 92 ED B1 14 6B  ’Hµ)J"LÓ–M!’í±.k
00000050  E0 49 BC 05 08 30 13 4F 82 99 0C 26 89 67 26 08  àI¼..0.O‚™.&‰g&.
00000060  66 82 C0 30 8C 60 30 63 04 41 80 B1 07 81 23 C3  f‚À0Œ`0c.A€±..#Ã
00000070  4B 64 60 64 44 B6 69 9A A6 25 51 D4 42 4B A4 48  Kd`dD¶iš¦%QÔBK¤H
00000080  91 14 D9 6C 89 BD B3 F7 E5 F5 EB B7 D4 5E B7 EE  ‘.Ùl‰½³÷åõë·Ô^·î
00000090  32 7F 54 9D DB A7 EE BB F7 DC 73 EB BD 6E B1 C9  2.T.Û§î»÷Üsë½n±É
000000A0  EF 87 68 BC C7 7A B5 DC AD AA CE F7 B7 7C 7F 00  ï‡h¼ÇzµÜ.ªÎ÷·|..
000000B0  21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21  !„.B.!„.B.!„.B.!
000000C0  84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84  „.B.!„.B.!„.B.!„
000000D0  10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10  .B.!„.B.!„.B.!„.
000000E0  42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42  B.!„.B.!„.B.!„.B
000000F0  08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08  .!„.B.!„.B.!„.B.
00000100  21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21  !„.B.!„.B.!„.B.!
00000110  84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84  „.B.!„.B.!„.B.!„
00000120  10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10  .B.!„.B.!„.B.!„.
00000130  42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42  B.!„.B.!„.B.!„.B
00000140  08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08  .!„.B.!„.B.!„.B.
00000150  21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21  !„.B.!„.B.!„.B.!
00000160  84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84  „.B.!„.B.!„.B.!„
00000170  10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10  .B.!„.B.!„.B.!„.
00000180  42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42  B.!„.B.!„.B.!„.B
00000190  08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08  .!„.B.!„.B.!„.B.
000001A0  21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21  !„.B.!„.B.!„.B.!
```

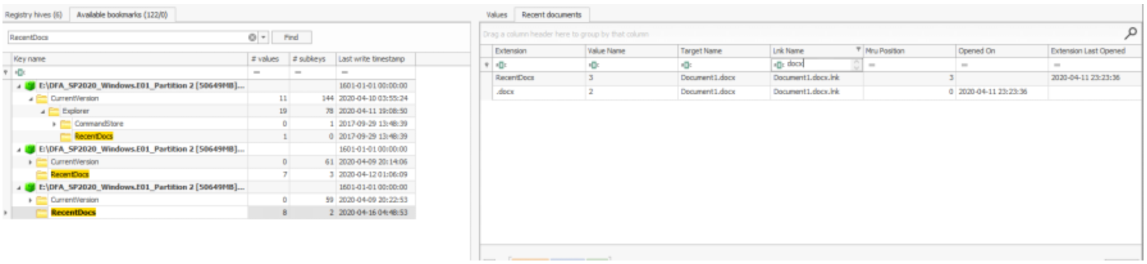
| | | |
|---|---|---|
| Binary (8 bit) | | Invalid |
| Int8 | go to: | Invalid |
| UInt8 | go to: | Invalid |
| Int16 | go to: | Invalid |
| UInt16 | go to: | Invalid |
| Int24 | go to: | Invalid |
| UInt24 | go to: | Invalid |
| Int32 | go to: | Invalid |
| UInt32 | go to: | Invalid |
| Int64 | go to: | Invalid |
| UInt64 | go to: | Invalid |
| LEB128 | go to: | Invalid |
| ULEB128 | go to: | Invalid |
| AnsiChar / char8_t | | Invalid |
| WideChar / char16_t | | Invalid |
| UTF-8 code point | | Invalid |
| Single (float32) | | Invalid |
| Double (float64) | | Invalid |
| OLETIME | | Invalid |
| FILETIME | | Invalid |
| DOS date | | Invalid |



```
FLARE-VM Thu 09/26/2024  4:58:36.35
C:\Users\FlareVM\Desktop>certutil -hashfile iPhone.png sha1
SHA1 hash of iPhone.png:
537fe19a560ba3578d2f9095dc2f591489ff2cde
CertUtil: -hashfile command completed successfully.
```

**Q25: 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)**

- I used Registry Explorer again and searched the '**RecentDocs**' key which indicate recently used Applications and files by a user.
  I found Jim last opened a docx file named 'Document1' at **2020-04-11 23:23:36**



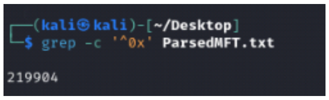
Registry hives (6)
Available bookmarks (122/0)
RecentDocs
Find
Values
Recent documents
Drag a column header here to group by that column

| Key name | # values | # subkeys | Last write timestamp |
|---|---|---|---|
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]... | | | 1601-01-01 00:00:00 |
| CurrentVersion | 11 | 144 | 2020-04-10 03:55:24 |
| Explorer | 19 | 78 | 2020-04-11 19:08:50 |
| CommandStore | 0 | 1 | 2017-09-29 13:48:39 |
| RecentDocs | 1 | 0 | 2017-09-29 13:48:39 |
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]... | | | 1601-01-01 00:00:00 |
| CurrentVersion | 0 | 61 | 2020-04-09 20:14:06 |
| RecentDocs | 7 | 3 | 2020-04-12 01:06:09 |
| E:\DFA_SP2020_Windows.E01_Partition 2 [50649MB]... | | | 1601-01-01 00:00:00 |
| CurrentVersion | 0 | 59 | 2020-04-09 20:22:53 |
| RecentDocs | 8 | 2 | 2020-04-16 04:48:53 |

| Extension | Value Name | Target Name | Lnk Name | Mru Position | Opened On | Extension Last Opened |
|---|---|---|---|---|---|---|
| | | | docx | | | |
| RecentDocs | 3 | Document1.docx | Document1.docx.lnk | 3 | | 2020-04-11 23:23:36 |
| .docx | 2 | Document1.docx | Document1.docx.lnk | 0 | 2020-04-11 23:23:36 | |

**Q26:How many entries does the MFT of the filesystem have?**

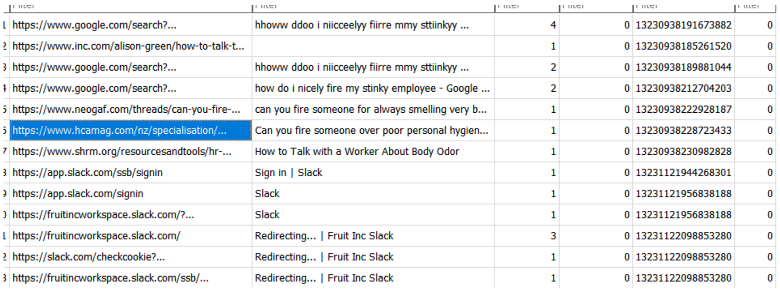
I usually use 'MFTECmd' to parse the MFT, which counts the number of entries.
However, the count was incorrect, so I used **MFTDump.py** and counted the number of entries manually.
I saved the output to a TXT file, then used the command grep -c '^0x' ParsedMFT.txt to count the entries. This command searches for lines that start with 0x, which corresponds to the record offsets in the MFT.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ grep -c '^0x' ParsedMFT.txt

219904
```

**Q27: Tim wanted to fire an employee because they were ......?(Be careful what you wish for)**

- We already have an indication that Tim wanted to fire Jim so at first I tried to find any evidence of something Jim did in his personal directory and don't found anything.
  Next, I loaded Tim Chrome history and found he wanted to fire Jim because he is **stinky**



| | | | | | |
|---|---|---|---|---|---|
| https://www.google.com/search?... | hhoww ddoo i niicceelyy fiirre mmy sttiinkyy ... | 4 | 0 | 13230938191673882 | 0 |
| https://www.inc.com/alison-green/how-to-talk-t... | | 1 | 0 | 13230938185261520 | 0 |
| https://www.google.com/search?... | hhoww ddoo i niicceelyy fiirre mmy sttiinkyy ... | 2 | 0 | 13230938189881044 | 0 |
| https://www.google.com/search?... | how do i nicely fire my stinky employee - Google ... | 2 | 0 | 13230938212704203 | 0 |
| https://www.neogaf.com/threads/can-you-fire-... | can you fire someone for always smelling very b... | 1 | 0 | 13230938222928187 | 0 |
| https://www.hcamag.com/nz/specialisation/... | Can you fire someone over poor personal hygien... | 1 | 0 | 13230938228723433 | 0 |
| https://www.shrm.org/resourcesandtools/hr-... | How to Talk with a Worker About Body Odor | 1 | 0 | 13230938230982828 | 0 |
| https://app.slack.com/ssb/signin | Sign in \| Slack | 1 | 0 | 13231121944268301 | 0 |
| https://app.slack.com/signin | Slack | 1 | 0 | 13231121956838188 | 0 |
| https://fruitincworkspace.slack.com/?... | Slack | 1 | 0 | 13231121956838188 | 0 |
| https://fruitincworkspace.slack.com/ | Redirecting... \| Fruit Inc Slack | 3 | 0 | 13231122098853280 | 0 |
| https://slack.com/checkcookie?... | Redirecting... \| Fruit Inc Slack | 1 | 0 | 13231122098853280 | 0 |
| https://fruitincworkspace.slack.com/ssb/... | Redirecting... \| Fruit Inc Slack | 1 | 0 | 13231122098853280 | 0 |

**Q28:What cloud service was a Startup item for the user admin?**

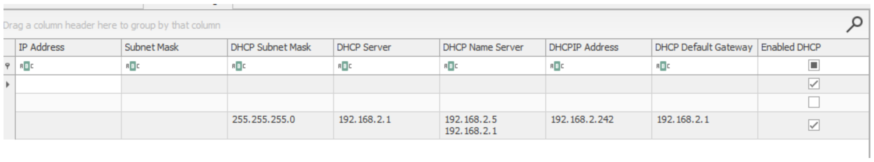
- I accessed to 'C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs' and found **'OneDrive'** on admin user startup folder.

**Q29: Which Firefox prefetch file has the most runtimes? (Flag format is )**

- I accessed to the parsed Prefetch CSV and search 'firefox' found 'FIREFOX.EXE-A606B53C.pf' executed 21 times.
  The answer is **'FIREFOX.EXE-A606B53C.pf/21'**

**Q30: What was the last IP address the machine was connected to?**

- We are able to identified the last DHCP IP address at 'System' HIVE by ControlSet001\Services \Tcpip\Parameters\**Interfaces** key.



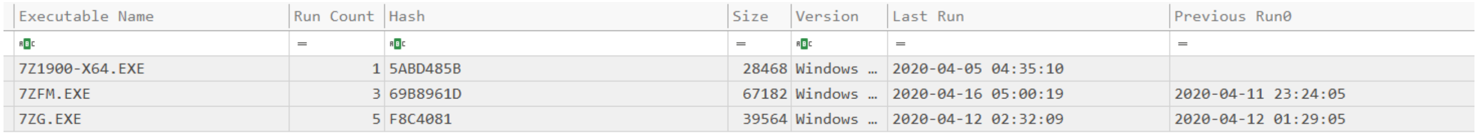
| IP Address | Subnet Mask | DHCP Subnet Mask | DHCP Server | DHCP Name Server | DHCPIP Address | DHCP Default Gateway | Enabled DHCP |
|---|---|---|---|---|---|---|---|
| | | | | | | | ☑ |
| | | | | | | | ☐ |
| | | 255.255.255.0 | 192.168.2.1 | 192.168.2.5<br>192.168.2.1 | 192.168.2.242 | 192.168.2.1 | ☑ |

**Q31: Which user had the most items pinned to their taskbar?**

- We can see pinned applications in the taskbar at C:\Users\<USER>\AppData\Roaming\Microsoft \Internet Explorer\Quick Launch\User Pinned\TaskBar.
  I examined all users and identified that the '**Admin**' user has the most pinned applications.

**Q32: What was the last run date of the executable with an MFT record number of 164885? (Format: MM/DD/YYYY HH:MM:SS (UTC).)**

- I searched in the parsed MFT file the entry number, I found the entry number related to '7zG.exe' I searched the executable in the parsed Prefetch and found the last run was at '12/04/2020 02:32:09'



| Executable Name | Run Count | Hash | Size | Version | Last Run | Previous Run0 |
|---|---|---|---|---|---|---|
| 7Z1900-X64.EXE | 1 | 5ABD485B | 28468 | Windows ... | 2020-04-05 04:35:10 | |
| 7ZFM.EXE | 3 | 69B8961D | 67182 | Windows ... | 2020-04-16 05:00:19 | 2020-04-11 23:24:05 |
| 7ZG.EXE | 5 | F8C4081 | 39564 | Windows ... | 2020-04-12 02:32:09 | 2020-04-12 01:29:05 |

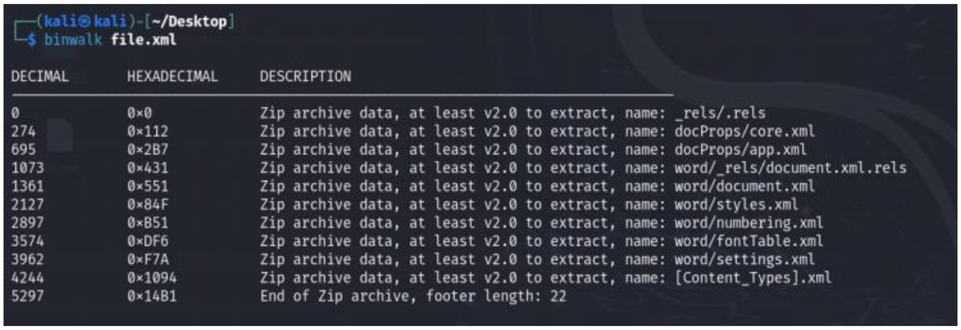
**Q33: What is the log file sequence number for the file "fruit_Assortment.jpg"?**

- II had an issue with MFTEcmd where I didn't see all the available fields. So, I used this walkthrough: Corporate Secret Challenge - CyberDefenders.org by Azad and found that the answer is 1276820064.

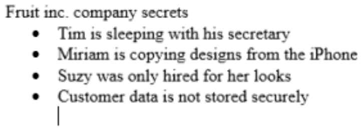
**Q34: Jim has some dirt on the company stored in a docx file. Find it, the flag is the fourth secret, in the format of <"The flag is a sentence you put in quotes">. (Secrets, secrets are no fun)**

- I accessed Jim's directory and found a DOCX file named 'Document1'. Inside, the content simply read, "There is nothing to see!" I used 'binwalk' to extract all files from the ZIP archive but found nothing.
  Next, I checked the Recycle Bin for Jim (SID:1003) and extracted all its contents. Despite several operations, no significant results appeared.

  Drawing from previous experience and [1], I renamed the DOCX file to a ZIP file and decompressed it.
  Among the extracted files, only one—'file.xml'—stood out.
  Running 'binwalk' on it revealed that it was actually a DOC file.
  After renaming it, I uncovered the hidden secrets!



```
┌──(kali㉿kali)-[~/Desktop]
└─$ binwalk file.xml

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, name: _rels/.rels
274           0x112           Zip archive data, at least v2.0 to extract, name: docProps/core.xml
695           0x2B7           Zip archive data, at least v2.0 to extract, name: docProps/app.xml
1073          0x431           Zip archive data, at least v2.0 to extract, name: word/_rels/document.xml.rels
1361          0x551           Zip archive data, at least v2.0 to extract, name: word/document.xml
2127          0x84F           Zip archive data, at least v2.0 to extract, name: word/styles.xml
2897          0xB51           Zip archive data, at least v2.0 to extract, name: word/numbering.xml
3574          0xDF6           Zip archive data, at least v2.0 to extract, name: word/fontTable.xml
3962          0xF7A           Zip archive data, at least v2.0 to extract, name: word/settings.xml
4244          0x1094          Zip archive data, at least v2.0 to extract, name: [Content_Types].xml
5297          0x14B1          End of Zip archive, footer length: 22
```



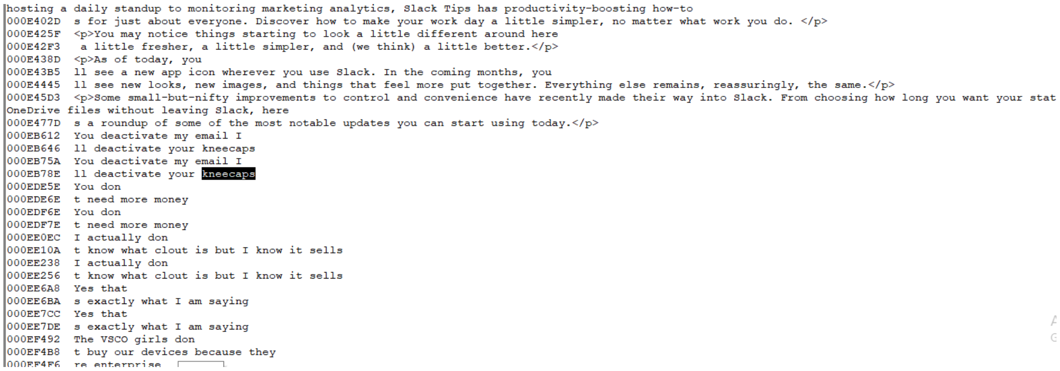
Fruit inc. company secrets

- Tim is sleeping with his secretary
- Miriam is copying designs from the iPhone
- Suzy was only hired for her looks
- Customer data is not stored securely

**Q35: In the company Slack, what is threatened to be deactivated if the user gets their email deactivated?**

- **I found 'Slack' directory in 'Hansel' Appdata directory.**  
  **I never investigated 'Slack' application before I read here** [https://medium.com/@jeroenverhaeghe/forensics-finding-slack-chat-artifacts-d5eeffd31b9c](https://medium.com/@jeroenverhaeghe/forensics-finding-slack-chat-artifacts-d5eeffd31b9c) **how to investigate Slack files.**  
  **Slack underlyingly uses Chromium (google chrome based browser). Slack stores the recent chats and the recently viewed user data in these files.**  
  **So we are can open these files via 'GoogleChromeCache' view.**

  **In C:\**Users\hansel.apricot\AppData\Roaming\Slack\IndexedDB\https_app.slack.com_0.indexeddb.leveldb\00003.log file you are able to see all the chats decrypted.  
  I used strings to find the answer.



```
hosting a daily standup to monitoring marketing analytics, Slack Tips has productivity-boosting how-to
000E402D  s for just about everyone. Discover how to make your work day a little simpler, no matter what work you do. </p>
000E425F  <p>You may notice things starting to look a little different around here
000E42F3   a little fresher, a little simpler, and (we think) a little better.</p>
000E438D  <p>As of today, you
000E43B5  ll see a new app icon wherever you use Slack. In the coming months, you
000E4445  ll see new looks, new images, and things that feel more put together. Everything else remains, reassuringly, the same.</p>
000E45D3  <p>Some small-but-nifty improvements to control and convenience have recently made their way into Slack. From choosing how long you want your stat
OneDrive files without leaving Slack, here
000E477D  s a roundup of some of the most notable updates you can start using today.</p>
000EB612  You deactivate my email I
000EB646  ll deactivate your kneecaps
000EB75A  You deactivate my email I
000EB78E  ll deactivate your kneecaps
000EDE5E  You don
000EDE6E  t need more money
000EDF6E  You don
000EDF7E  t need more money
000EE0EC  I actually don
000EE10A  t know what clout is but I know it sells
000EE238  I actually don
000EE256  t know what clout is but I know it sells
000EE6A8  Yes that
000EE6BA  s exactly what I am saying
000EE7CC  Yes that
000EE7DE  s exactly what I am saying
000EF492  The VSCO girls don
000EF4B8  t buy our devices because they
000EF4F6  re enterprise
```