# Application Analysis

**Disclaimer:**

*This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.*

**12/01/2017**

**http://computerforensicsblog.champlain.edu/**

**175 Lakeside Ave, Room 300A**
**Phone: (802) 865-5744**
**Fax: (802) 865-6446**

# Contents

**Introduction** **2**

Background 2

Purpose and Scope 2

Research Questions 2

Terminology 2

**Methodology and Methods** **3**

Equipment Used 4

Data Collection 4

**Analysis** **5**

**Results** **5**

LastPass 5

Steam 7

Trello 13

**Conclusion** **16**

**Further Work** **16**

**Appendix** **17**

**References** **23**

# Introduction

Web applications are an integral part of desktop computers. Everything from games to organizational applications are run on PCs every day. With desktop integration extremely common, it is essential that the apps we use everyday are secure, and in the event of wrongdoing, it is essential for investigators to know what could aid them in the investigation. Despite the concept of web applications being that most of their data is downloaded when needed, having all necessary resources being downloaded at runtime is resource intensive, and much of that can be mitigated by storing some data on the host computer. As such, these applications can leave varying artifacts on the host. This project will focus on the artifacts left behind by LastPass, Steam, and Trello, specifically.

## Background

In autumn of 2013, a project called “Cloud Forensics” was conducted by the LCDI to investigate web applications from a storage perspective, in terms of how they relate and interact with cloud services. Web applications were then explored more in depth in May of 2017, when another team from the LCDI completed a project analyzing web applications in a similar manner to this project. The previous Application Analysis project and the current one focus on the client side of web applications, as opposed to the Cloud Forensics Project. Both projects were conducted in a similar manner, however, they have different focuses. The past project focused on the applications Slack, Discord, and Dropbox, and analyzed them within the operating systems Mac OS Sierra, Windows 7, and Windows 10. In contrast, this project will focus on LastPass, Steam, and Trello, all within a Windows 10 environment.

## Purpose and Scope

The purpose of our research is to see if we can find a variety of artifacts left behind by different web applications. Even if information contained in an application has been deleted, there is always a chance that important data has been left behind. The research will provide a glimpse into the inner functions of certain web applications, the artifacts that they leave behind, and the forensic implications of these artifacts. This project in particular will focus on the applications of LastPass, Steam, and Trello in a Windows 10 environment.

## Research Questions

1. What data is recoverable in each application from Windows 10 operating systems?
2. What are the forensic implications of the revealed artifacts?

## Terminology

**Artifacts** - “Any data generated by user interaction that can be collected and examined. Any user data retrieved from the browser is considered an artifact, including cookies, caches, geolocation, search history, etc.” (“Artifacts”).

**Autopsy -** “An application that acts as a GUI to make The Sleuth Kit, an open source collection of digital forensics tools, easier to use. Created by Basics Technology Corp,” (“Autopsy”).

**Digital Evidence** - “Information of probative value that is stored or transmitted in a binary form,” (NCFS, 2012). Digital evidence not only includes computers in the traditional sense, but also digital audio, video, and pictures (“Digital Evidence”).

**Digital Forensics** - “A division of forensic science which focuses on the identification, examination, collection, preservation, and analysis of data from any device that can store electronic/digital information, such as computers and mobile phones. The science is applied in both criminal and civil investigations in a court of law, and in the private sector when investigating internal issues or intrusions,” (Digital Forensics”).

**EnCase** - “A suite of digital forensics tools created by Guidance Software. The software comes in several forms designed for forensic, cyber security, and e-discovery use,” (“EnCase”).

**FTK** - “A forensic tool made by AccessData. FTK allows users to acquire, process, and verify evidence,” (“FTK”).

**LastPass** - An application and browser extension that saves and encrypts passwords for the user.

**Steam** - A video game distribution application which offers multiplayer gaming and social networking services.

**Trello** - A productivity application in which users can have personal “Boards” as well as be on a team to share boards with lists and checklists.

**Virtual Machine (VMs)** - “A software-based computer that executes and runs programs like a physical machine,” (“Virtual Machines”).

**.VMDK** - A VMWare file format that emulates a hard drive.

**Web Application** - An application in which all or some parts of the software are downloaded from the Web each time it is run. It may refer to browser-based apps that run within the user's Web browser, or to "rich client" desktop apps that do not use a browser or to mobile apps that access the Web for additional information.

## Methodology and Methods

Before we began, our team split up into three groups and each group was assigned at least one of the applications researched. We began by establishing a virtual machine for each application, all using Windows 10. Each installation was updated then powered off. From there, the application data generation began. We worked off of a pre-made list of features for each application to ensure that as much data was generated and stored as possible. The actual data generation process was similar for each case, with each application yielding different results.

After data generation was completed, we then used the VMDK files for each VM and analyzed them using EnCase, Autopsy, and FTK Imager. We systematically looked through the evidence, verifying each artifact, and making sure there were no changes by using MD5 and SHA1 hashes that were calculated before and after analysis.

**EnCase** - One of the forensic tools we used for this project was EnCase. EnCase is a piece of software that contains multiple tools which allowed our team to look further into virtual machine files. After creating the cloned virtual machine files, the team took each file, then processed it inside of EnCase. This tool allowed us to view cache files directly. Links, pictures, and even user input that was recorded in cache were all found within the caches of the web apps that we looked at.

**FTK Imager–** FTK Imager is a piece of software which allows users to view both the text and hex data from any file uploaded, as well as generate the MD5 and SHA1 hash value of individual partitions, folders, and files. After creating the cloned virtual machine files, the team took each file and ran it through FTK Imager. This tool allowed us to receive and verify the hash values of the evidence files. Artifacts, logs, and pictures were all found within the caches of the web apps that we looked at.

**Autopsy–** An open source digital forensic platform that comes preloaded on many forensic distributions of Linux, it is a version of the Sleuth Kit with a Graphic User Interface, for ease of use. This forensic tool is useful for it's features such as timeline analysis, keyword searches, and web artifacts. It also provided hashing of files to verify integrity. This tool was only used in the forensic analysis of the LastPass Application.

**vSphere** - vSphere was our primary tool for data generation in this project. vSphere was used as a platform for our virtual machines allowing us to access our VMs from any computer in the lab. In order to start our data generation on our applications, we first had to install our Windows 10 systems on vSphere. We then used the interface to generate data for the project. Afterwards, we cloned the .vmdk file and then exported it, so that we could investigate what artifacts were on the machine.

## Equipment Used

| Device | OS Version | Comments |
|---|---|---|
| VMware vSphere Client | 6.0.0.5505 | Used to interact with VM hosted on server |
| VM | Windows 10 | Windows machines |
| Google Chrome | 61.0.3163.100 | |
| Mozilla Firefox | 55.0.3 | Browser used with LastPass |
| Steam | Sept 7th 2017 | |
| LastPass | 4.1.65 | |
| EnCase | v8.04 | Acquire and process data generated |
| Trello (Windows Store App) | 2.9.8.0 | |
| FTK Imager | 3.4.2.6 | Acquire and process data generated |
| Autopsy | 4.4.0 | Acquire and process data generated |

## Data Collection

Using EnCase, Autopsy, and FTK Imager, we systematically analyzed the VMDK files, searching for any stored information on the machine that would not be available without logging into an account, specifically any artifacts that could be relevant in a forensic investigation, or those that could indicate compromised security within any of the apps. The artifacts we collected can be found in the appendix within tables labelled by Application.

# Analysis

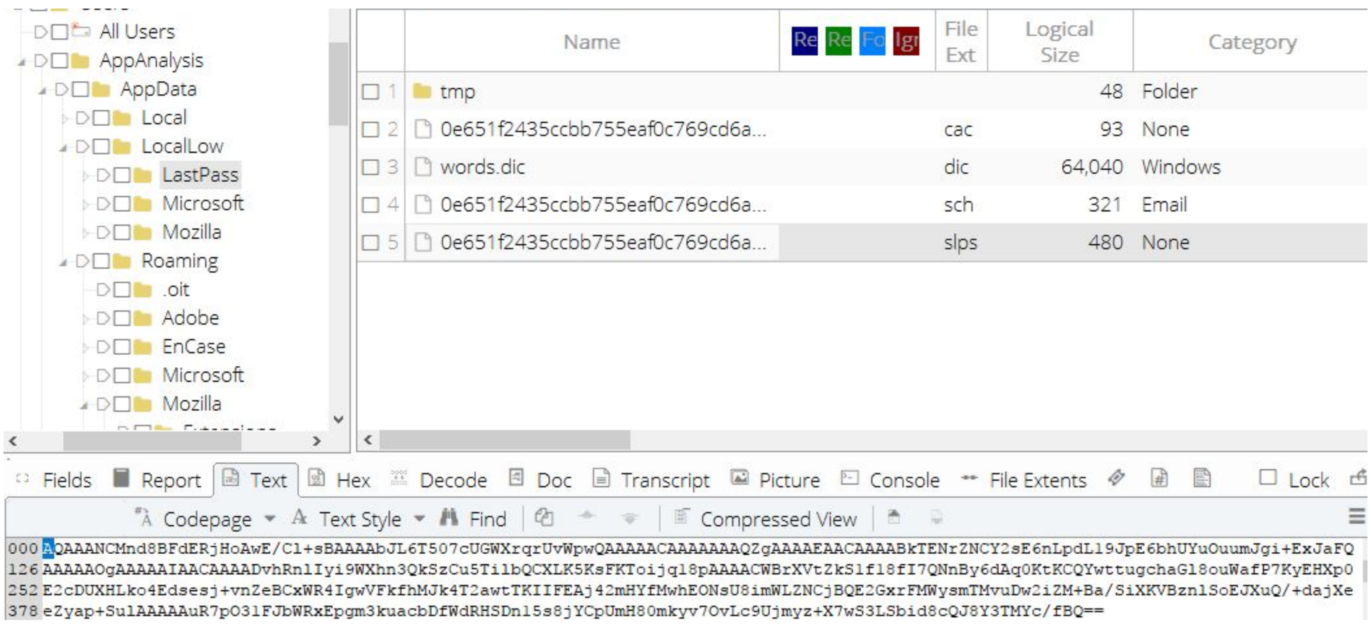
The data analyzed was acquired and processed through EnCase, Autopsy, and FTK Imager. The team focused on finding all information relevant to the app, deleted or stored, from the VMDK. We specifically attempted to search for artifacts that are not publicly accessible through profiles, as well as timestamps and hidden or deleted information. We used tables to document both the data generated as well as the analysis. These tables were color coded to separate the types of information gathered. We confirmed all evidence found by having two copies of the VMDK and doing separate but identical forensic investigations.

Based on the research questions, we expect that there will not be major breaches of information given that these apps have a very large user base and therefore, will most likely have better security as a precaution. However, there may be information that could prove critical to future forensic investigations. These applications all have the potential to store personal information, and this analysis may shed light on possible weaknesses or leakages of information within the applications.

# Results

## LastPass

Even though LastPass is a browser plugin and not a true application, it must still store some information on a computer. We used Firefox for our research. When installed on Firefox, LastPass stores its data at ***C:\Users\<username>\AppData\LocalLow\LastPass***. However, this data is encrypted.



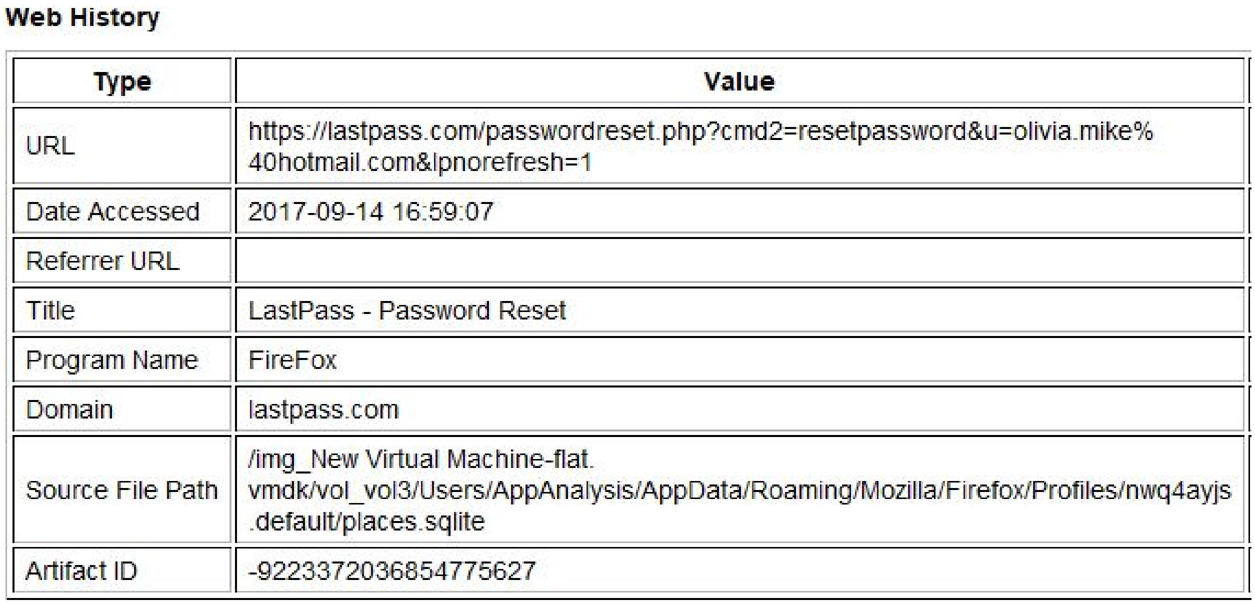
| | Name | Re | Re | Fo | Igi | File Ext | Logical Size | Category |
|---|---|---|---|---|---|---|---|---|
| □ 1 | tmp | | | | | | 48 | Folder |
| □ 2 | 0e651f2435ccbb755eaf0c769cd6a... | | | | | cac | 93 | None |
| □ 3 | words.dic | | | | | dic | 64,040 | Windows |
| □ 4 | 0e651f2435ccbb755eaf0c769cd6a... | | | | | sch | 321 | Email |
| □ 5 | 0e651f2435ccbb755eaf0c769cd6a... | | | | | slps | 480 | None |

```
000 AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAbJL6T507cUGWXrqrUvWpwQAAAAACAAAAAAAQZgAAAAEAACAAAABkTENrZNCY2sE6nLpdLl9JpE6bhUYuOuumJgi+ExJaFQ
126 AAAAAOgAAAAAIAACAAAADvhRnlIyi9WXhn3QkSzCu5TilbQCXLK5KsFKToijql8pAAAACWBrXVtZkSlfl8fI7QNnBy6dAq0KtKCQYwttugchaGl8ouWafP7KyEHXp0
252 E2cDUXHLko4Edsesj+vnZeBCxWR4IgwVFkfhMJk4T2awtTKIIFEAj42mHYfMwhEONsU8imWLZNCjBQE2GxrFMWysmTMvuDw2iZM+Ba/SiXKVBznlSoEJXuQ/+dajXe
378 eZyap+SulAAAAAuR7pO31FJbWRxEpgm3kuacbDfWdRHSDn15s8jYCpUmH80mkyv7OvLc9Ujmyz+X7wS3LSbid8cQJ8Y3TMYc/fBQ==
```

*Figure 1: Location of LastPass Encrypted Data*

All data that LastPass stores on the computer cannot be accessed. This rules out a majority of information, but some artifacts can still be found in cookies and web history. Timestamps from history and cookies can show when a user visited their vault. URLs in history were the primary type of artifacts we found.

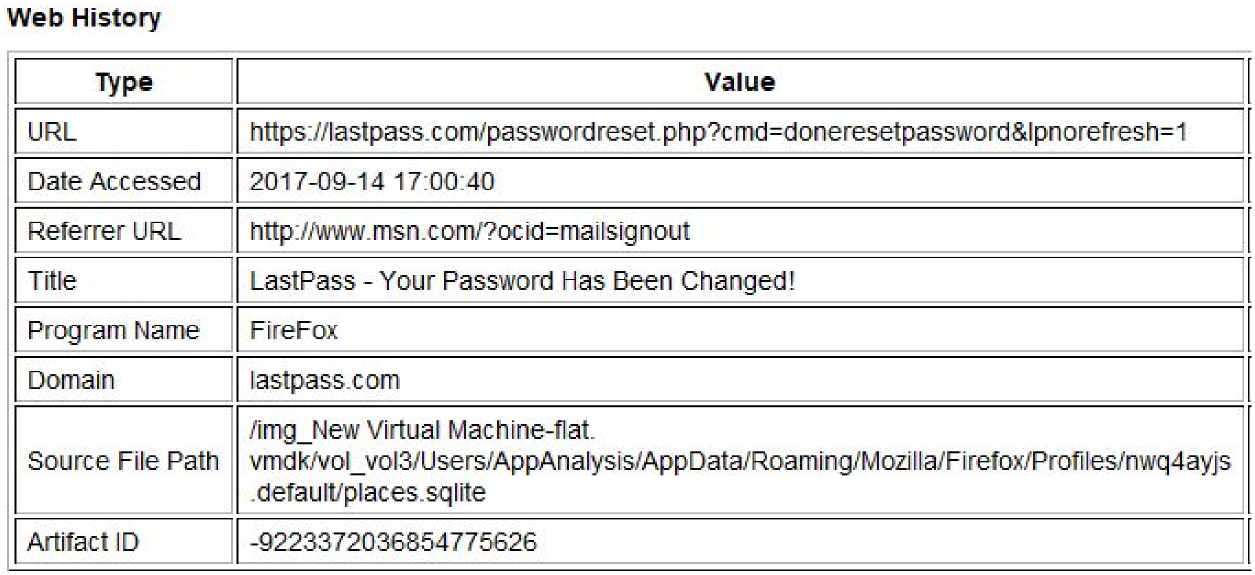
The URL of the page to reset passwords is recorded, as is the URL of the page that the user is led to when they reset their password.



**Web History**

| Type | Value |
|---|---|
| URL | https://lastpass.com/passwordreset.php?cmd2=resetpassword&u=olivia.mike%40hotmail.com&lpnorefresh=1 |
| Date Accessed | 2017-09-14 16:59:07 |
| Referrer URL | |
| Title | LastPass - Password Reset |
| Program Name | FireFox |
| Domain | lastpass.com |
| Source File Path | /img_New Virtual Machine-flat.vmdk/vol_vol3/Users/AppAnalysis/AppData/Roaming/Mozilla/Firefox/Profiles/nwq4ayjs.default/places.sqlite |
| Artifact ID | -9223372036854775627 |

*Figure 2: Password Reset*

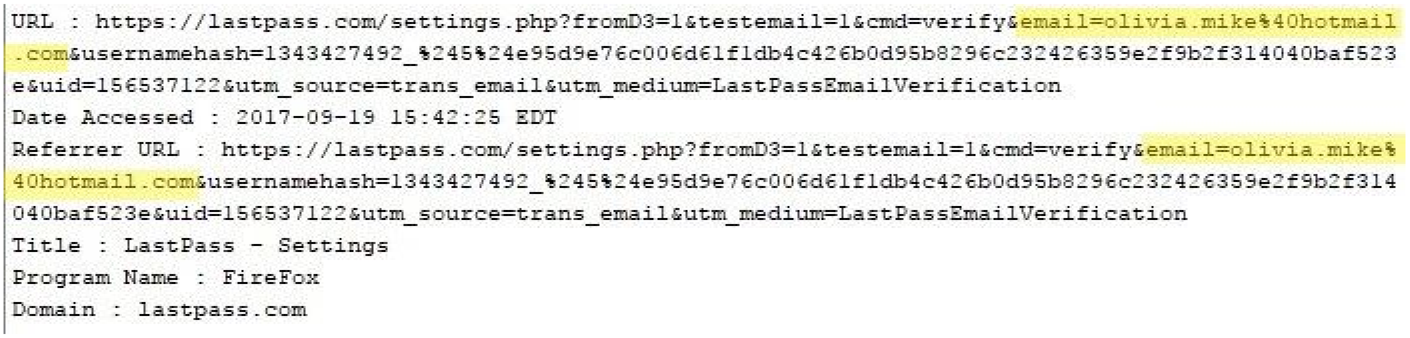


**Web History**

| Type | Value |
|---|---|
| URL | https://lastpass.com/passwordreset.php?cmd=doneresetpassword&lpnorefresh=1 |
| Date Accessed | 2017-09-14 17:00:40 |
| Referrer URL | http://www.msn.com/?ocid=mailsignout |
| Title | LastPass - Your Password Has Been Changed! |
| Program Name | FireFox |
| Domain | lastpass.com |
| Source File Path | /img_New Virtual Machine-flat.vmdk/vol_vol3/Users/AppAnalysis/AppData/Roaming/Mozilla/Firefox/Profiles/nwq4ayjs.default/places.sqlite |
| Artifact ID | -9223372036854775626 |

*Figure 3: Password Change Confirmation*

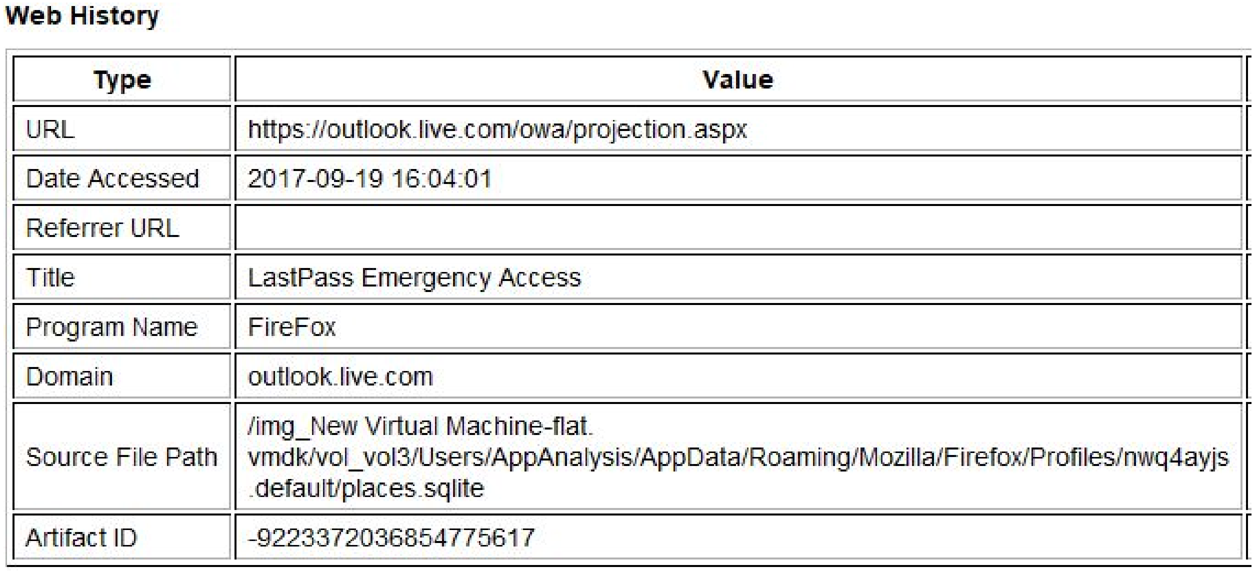
When a user verifies their email, the URL they are directed to contains the email address associated with their account, using percent encoding to represent the “@” symbol within the URL.



```
URL : https://lastpass.com/settings.php?fromD3=1&testemail=1&cmd=verify&email=olivia.mike%40hotmail
.com&usernamehash=1343427492_%245%24e95d9e76c006d61f1db4c426b0d95b8296c232426359e2f9b2f314040baf523
e&uid=156537122&utm_source=trans_email&utm_medium=LastPassEmailVerification
Date Accessed : 2017-09-19 15:42:25 EDT
Referrer URL : https://lastpass.com/settings.php?fromD3=1&testemail=1&cmd=verify&email=olivia.mike%
40hotmail.com&usernamehash=1343427492_%245%24e95d9e76c006d61f1db4c426b0d95b8296c232426359e2f9b2f314
040baf523e&uid=156537122&utm_source=trans_email&utm_medium=LastPassEmailVerification
Title : LastPass - Settings
Program Name : FireFox
Domain : lastpass.com
```

*Figure 4: Email Verification URL*

A user can give another user emergency access to their password vault. To arrange this, the recipient of emergency access must accept an invitation to receive access through an email. The title of the page containing this email indicates that emergency access has been given. However, it does not state by who or if it has been accepted.



**Web History**

| Type | Value |
|---|---|
| URL | https://outlook.live.com/owa/projection.aspx |
| Date Accessed | 2017-09-19 16:04:01 |
| Referrer URL | |
| Title | LastPass Emergency Access |
| Program Name | FireFox |
| Domain | outlook.live.com |
| Source File Path | /img_New Virtual Machine-flat.vmdk/vol_vol3/Users/AppAnalysis/AppData/Roaming/Mozilla/Firefox/Profiles/nwq4ayjs.default/places.sqlite |
| Artifact ID | -9223372036854775617 |

*Figure 5: Emergency Invitation*

LastPass allows users to share passwords and files between themselves. However, when using this feature, the email address of a user sharing with another user is stored on the recipient's system in web history.

## Steam

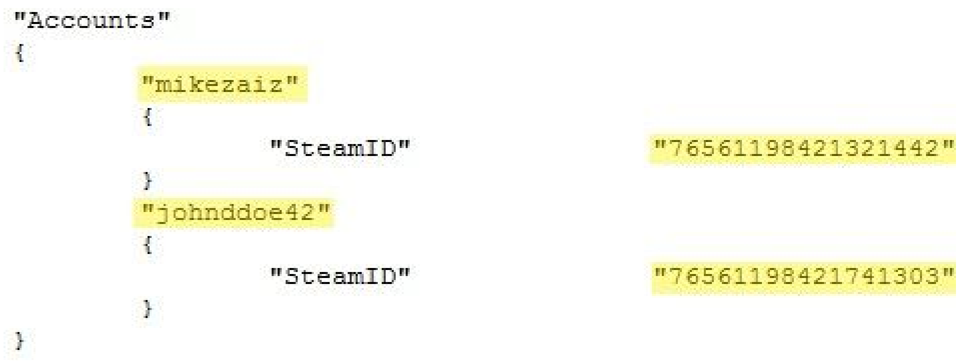
After completing the data generation phase, we started our analysis, overall finding two main places where Steam stores user information, located at: ***root\Users\<username>\Steam*** and ***root\Users\<username>\AppData\Local\Steam*** though the latter is not forensically relevant, and only contained promotional images and the HTML cache. We also noted that the games can be stored in other paths besides the default, and that is easily changed by users.

Before going into our analysis, it is important to understand the different types of Steam identification. Through our work, we learned that there are three main methods of identifying different users. The first is the profile name, which is the main name for the account, but not necessarily the username. The second is the SteamID 64, which is a number representing the Steam account, and is formatted as a seventeen digit numerical string. The third, SteamID 32, is commonly found within the host files, and is formatted as [U:#:#########] though it is commonly seen as simply the nine digit numerical string within the files of the machine.

The first relevant folder that was found within the Steam folder was the config folder within the path ***root/users/<username>/Steam/config***.

The avatarcache folder within the config folder in the path ***root/users/<username>/Steam/config /avatarcache/<Steam64 ID>.png*** contained a PNG of the avatar of the first steam account that we logged in on the computer, though the avatar for the second account that we made was not there.

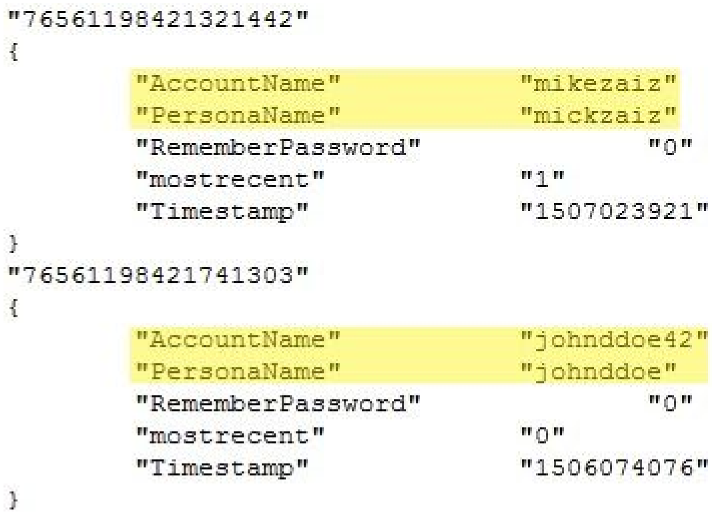
The config.vdf file contained a log of the accounts that have logged in on the computer and the associated Steam64 ID.



```
"Accounts"
{
        "mikezaiz"
        {
                "SteamID"               "76561198421321442"
        }
        "johnddoe42"
        {
                "SteamID"               "76561198421741303"
        }
}
```

*Figure 6: Users That Logged In*

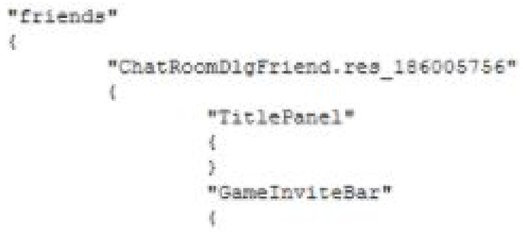
The loginusers.vdf file in ***root/users/<username>/Steam/config*** contained logs on both the user’s account and personal names, their associated Steam64 ID, whether they were the last account to be logged in, if they wanted their passwords remembered, and when they were last logged in, which is formatted in Unix.



```
"76561198421321442"
{
        "AccountName"           "mikezaiz"
        "PersonaName"           "mickzaiz"
        "RememberPassword"              "0"
        "mostrecent"            "1"
        "Timestamp"             "1507023921"
}
"76561198421741303"
{
        "AccountName"           "johnddoe42"
        "PersonaName"           "johnddoe"
        "RememberPassword"              "0"
        "mostrecent"            "0"
        "Timestamp"             "1506074076"
}
```

*Figure 7: User Information*

The DialogConfig.vdf file in ***root/users/<username>/Steam/config*** contained records of chats existing between users of this steam account. For each chat to a user, there was an entry in the file called "ChatRoomDlgFriend.res_<Steam32 ID>", which contained the configuration for that specific chat with a specific user as designated by the Steam32 ID. However, as expected, there were no actual records of the messages exchanged. Further work could explore which specific action generates this change in the file, as it could be anything from adding someone as a friend to opening up a chat window to the first message sent. It is also possible that the entry is based on the previous session rather than any chat log opened.

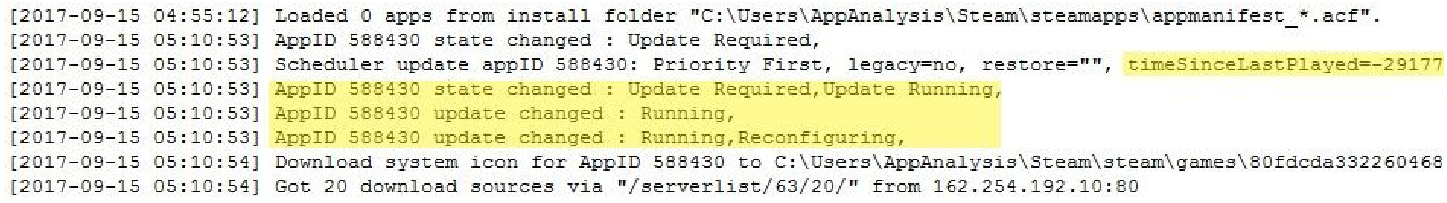


```
"friends"
{
        "ChatRoomDlgFriend.res_186005756"
        {
                "TitlePanel"
                {
                }
                "GameInviteBar"
                {
```

*Figure 8: Chat Window Configuration*

The second relevant folder that was found within the Steam folder was the logs folder. This folder contained many .txt logs of different kinds of events.

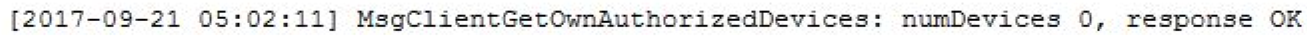
The first relevant log in the path ***root/users/<username>/Steam/logs*** was the content_log which documented each session, from login to log off, which included game updates, when an application is started, update information, game states, and more. This information can be useful in regards to timestamps, which are attached to every action. In addition, the log indicates where the apps are loaded from.



```
[2017-09-15 04:55:12] Loaded 0 apps from install folder "C:\Users\AppAnalysis\Steam\steamapps\appmanifest_*.acf".
[2017-09-15 05:10:53] AppID 588430 state changed : Update Required,
[2017-09-15 05:10:53] Scheduler update appID 588430: Priority First, legacy=no, restore="", timeSinceLastPlayed=-29177
[2017-09-15 05:10:53] AppID 588430 state changed : Update Required,Update Running,
[2017-09-15 05:10:53] AppID 588430 update changed : Running,
[2017-09-15 05:10:53] AppID 588430 update changed : Running,Reconfiguring,
[2017-09-15 05:10:54] Download system icon for AppID 588430 to C:\Users\AppAnalysis\Steam\steam\games\80fdcda332260468
[2017-09-15 05:10:54] Got 20 download sources via "/serverlist/63/20/" from 162.254.192.10:80
```

*Figure 9: Content Log*

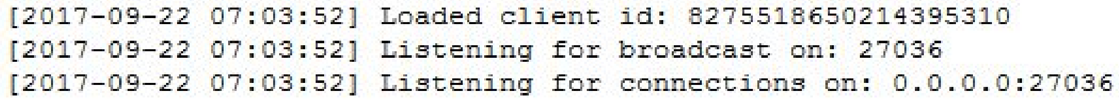
Library sharing is a feature that allows users to share their game library with other users. While we did not test this function, the librarysharing_log in ***root/users/<username>/Steam/logs*** documented the number of authorized users. However, since we did not use this feature of Steam, it is possible there is other information that will be recorded when an authorized user accesses the game library, which could prove relevant to forensic investigations. As such, further work could be done to completely explore all of the options of Steam, which includes the library sharing feature and the remote connections feature, which will be explained next.



```
[2017-09-21 05:02:11] MsgClientGetOwnAuthorizedDevices: numDevices 0, response OK
```

*Figure 10: Library Sharing Log*

The remote_connections file in ***root/users/<username>/Steam/logs*** is a log for remote connections which seemed to consistently listen on port 27036, though we did not test any remote connections in this project. The forensic importance of this log is the same as the librarysharing log.

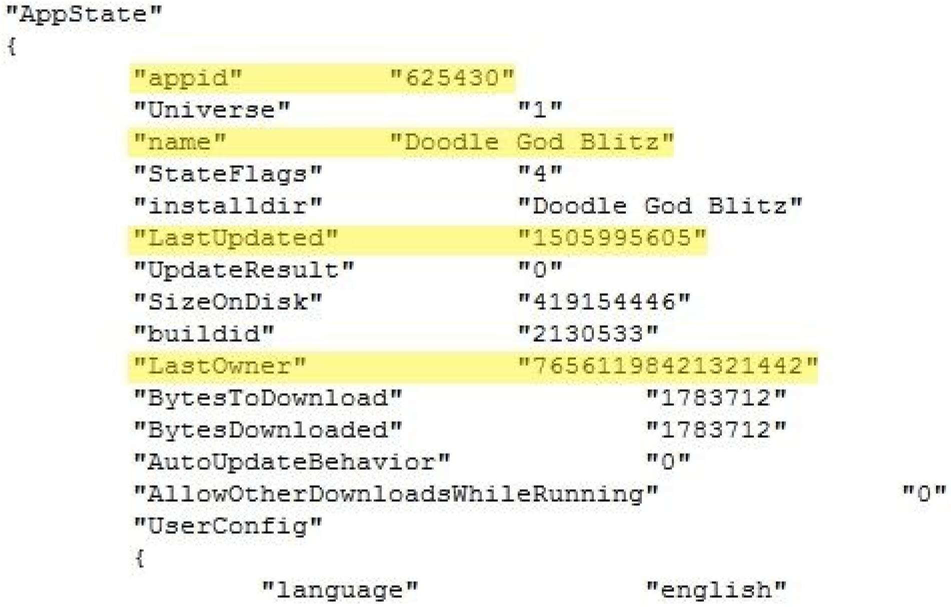


```
[2017-09-22 07:03:52] Loaded client id: 8275518650214395310
[2017-09-22 07:03:52] Listening for broadcast on: 27036
[2017-09-22 07:03:52] Listening for connections on: 0.0.0.0:27036
```

*Figure 11: Remote Connection Log*

The next folder of interest was the steamapp folder in ***root/users/<username>/Steam/steamapp***.

The file appmanifest_<App ID>.acf within the folder contained data regarding the games downloaded to Steam, like the name of a game, what language it is in, its App ID, when it was last updated, and its last owner, if it had one. There was one of these for every game that was downloaded.



```
"AppState"
{
        "appid"         "625430"
        "Universe"              "1"
        "name"          "Doodle God Blitz"
        "StateFlags"            "4"
        "installdir"            "Doodle God Blitz"
        "LastUpdated"           "1505995605"
        "UpdateResult"          "0"
        "SizeOnDisk"            "419154446"
        "buildid"               "2130533"
        "LastOwner"             "76561198421321442"
        "BytesToDownload"               "1783712"
        "BytesDownloaded"               "1783712"
        "AutoUpdateBehavior"            "0"
        "AllowOtherDownloadsWhileRunning"               "0"
        "UserConfig"
        {
                "language"              "english"
```

*Figure 12: App Information*

The steamapp folder also contained the common folder, which is the default location for where games are stored if the original settings are not changed. Our analysis of the configuration files did not reveal a list of all of the locations, and users can change the installation folder for each game, which makes it difficult to find every single game downloaded. However, there is a method to get around this, which will be explained in the next section. It is important to note here that users can change not only the location of the game, but also the name of the folder. This would make it essential to check the  appmanifest_<App ID>.acf file at ***root/users/<username>/Steam/steamapp*** as shown above to check the folder name, which is specified as the variable installdir.

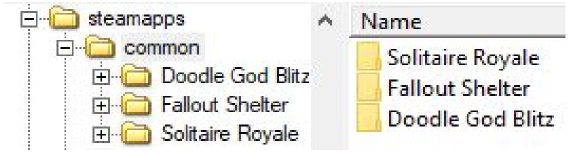
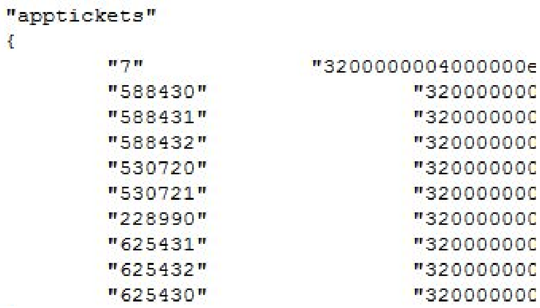


*Figure 13: Default Installation Folder*

The folder that seemed to contain the most artifacts was the userdata folder, located at r***oot/users/<username>/Steam/userdata***.

The localconfig.vdf files in the path r***oot/users/<username>/Steam/userdata/<Steam32 ID>/config*** contained the names of friends, their name history, their avatar hex number, the games they follow, and what friend groups they are in. We hypothesized that this file is used to generate the dashboard, or feed for the account based on the variety of information as well as the actual content of the feed within the app.

That file also contained a list of "apptickets" which was a list of the App IDs for all of the games installed. This can be used as a master list of games when the user downloaded the games into folders besides the default folder. It must be noted that some games have more than one App ID, usually sequentially. For example, Fallout Shelter seems to utilize App IDs 588430 through 588432. From this information, investigators can search third party databases that link App IDs to the game's common name. From there, investigators can perform a search of those names to find the folders where the game resides. It is important to note, however, that the latter sequential App IDs may not have any results attached to them as they are packages for games rather than the main App ID. For reference, the App ID "7" and "228990" refer to Steam information and is not user downloaded content.

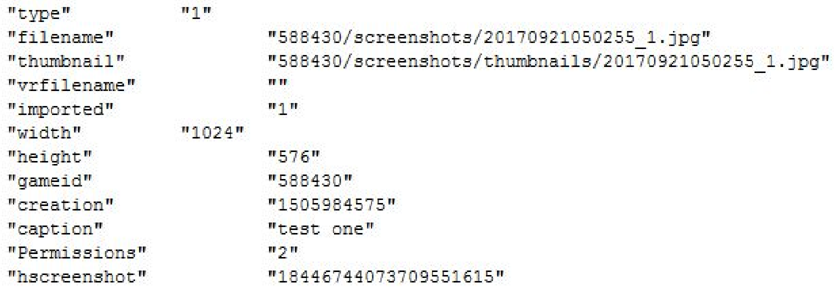


```
"apptickets"
{
        "7"             "3200000004000000e
        "588430"                "32000000C
        "588431"                "32000000C
        "588432"                "32000000C
        "530720"                "32000000C
        "530721"                "32000000C
        "228990"                "32000000C
        "625431"                "32000000C
        "625432"                "32000000C
        "625430"                "32000000C
```

*Figure 14: Game List*

The screenshots folders found in paths r***oot/users/<username>/Steam/userdata/<Steam32 ID>/760/remote/<App ID>*** from the userdata folder contained two JPEG images for screenshots taken by Steam.  It is important to note that some games may have the screenshots saved elsewhere. For Fallout Shelter, we found the screenshots at ***root/users/<username>/AppData/Local/FalloutShelter/Screenshots***.

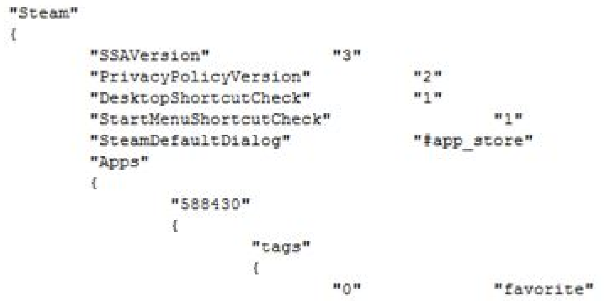
The screenshot.vdft file in the path r***oot/users/<username>/Steam/userdata/<Steam32 ID>/760*** from the userdata folder contained the filenames of screenshots taken in Steam, the thumbnails of these screenshots, their creation data, and any captions written in these screenshots.



```
"type"          "1"
"filename"              "588430/screenshots/20170921050255_1.jpg"
"thumbnail"             "588430/screenshots/thumbnails/20170921050255_1.jpg"
"vrfilename"            ""
"imported"              "1"
"width"         "1024"
"height"                "576"
"gameid"                "588430"
"creation"              "1505984575"
"caption"               "test one"
"Permissions"           "2"
"hscreenshot"           "18446744073709551615"
```

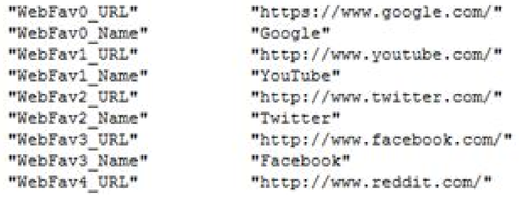
*Figure 15: Screenshot Information*

The sharedconfig.vdf file in the path ***root/users/<username>/Steam/userdata/<Steam32 ID>/7/remote*** from the userdata folder contained data on actions that were taken in Steam, like category creation, category names, and favorite URLS visited.



```
"Steam"
{
        "SSAVersion"            "3"
        "PrivacyPolicyVersion"          "2"
        "DesktopShortcutCheck"          "1"
        "StartMenuShortcutCheck"                "1"
        "SteamDefaultDialog"            "#app_store"
        "Apps"
        {
                "588430"
                {
                        "tags"
                        {
                                "0"             "favorite"
```

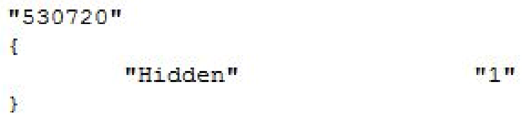
*Figure 16: Game Tags*



```
"WebFav0_URL"           "https://www.google.com/"
"WebFav0_Name"          "Google"
"WebFav1_URL"           "http://www.youtube.com/"
"WebFav1_Name"          "YouTube"
"WebFav2_URL"           "http://www.twitter.com/"
"WebFav2_Name"          "Twitter"
"WebFav3_URL"           "http://www.facebook.com/"
"WebFav3_Name"          "Facebook"
"WebFav4_URL"           "http://www.reddit.com/"
```

*Figure 17: Favorite Web Links*

That file also contained the App ID of the application Solitaire Royale, which was hidden during the data generation process.



```
"530720"
{
        "Hidden"                "1"
}
```

*Figure 18: Hidden Game*

## Trello

Upon completing the data generation phase, we began our analysis of the application which, much to our surprise, yielded much less data than expected. There are three main paths where Trello stores user information, located at:

***/root/ProgramFiles/WindowsApps/45237LiamForsyth.PawsforTrello_2.9.8.0_x64__7pb5ddty8z1pa/***

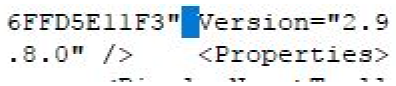
***/root/users/<username>/AppData/Local/Packages/45273LiamForsyth.PawsforTrello_7pb5ddty8z1pa/LocalCache/Roaming/Trello/***

***root/users/<username>/AppData/Local/Packages/45273LiamForsyth.PawsforTrello_7pb5ddty8z1pa/LocalCache/Roaming/com.atlassian.trello/***

The first path gave us the least amount of information, only providing Trello's version number. With that said, the two other paths did not provide as much information as we initially believed. This is unusual for an application like Trello which is designed for personal interactions. However, an explanation did present itself. Trello has no offline mode, which means that most of the data generated by user actions are stored on the Trello server.

The first relevant folder that was discovered was the folder at ***/root/ProgramFiles/WindowsApps/ 45237LiamForsyth.PawsforTrello_2.9.8.0_x64__7pb5ddty8z1pa/***

The file called AppxManifest.xml within the folder, contained the version number for the Trello App we were using. It is important to note that there are multiple places where the version can be found, the main one being in the folder name, ***45237LiamForsyth.PawsforTrello_2.9.8.0***..., though the file in that folder at ..***/app/version AppxManifest.xml*** contained an inaccurate version number. The version below is the correct one.



```
6FFD5E11F3" Version="2.9
.8.0" />    <Properties>
```

*Figure 19: Accurate Version Number*

The second relevant folder that we found was the Trello folder in the path ***/root/users/<username>/AppData/Local/Packages/45273LiamForsyth.PawsforTrello_7pb5ddty8z1pa/LocalCache/Roaming/Trello/***.

The folder *Cache* within this folder contained cached images of the backgrounds and profile pictures, as well as cached data stored in files named data_0, data_1, data_2, and data_3.

The f_00001c file in the *Cache* folder within the Trello folder contained a PNG of the profile image that was used by johnddoe124. Oddly, the profile image for the other user was not found.

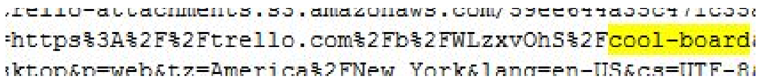
The f_00001b and f_000012 file in the *Cache* folder within the Trello folder contained a PNG of the current background image for the board we named "cool board". The main difference between these two is that f_00001b is much larger than f_000012.

The f_000019 and f_000013 file in the *Cache* folder within the Trello folder contained a PNG of the current background image for the board we named “board of nothingness”. The main difference between these two is that f_000019 is much larger than f_000013.

The f_000011 and f_000016 file in the *Cache* folder within the Trello folder contained a PNG of the current background image for the board named “testing board”. The main difference between these two is that f_000016 is much larger than f_000011.

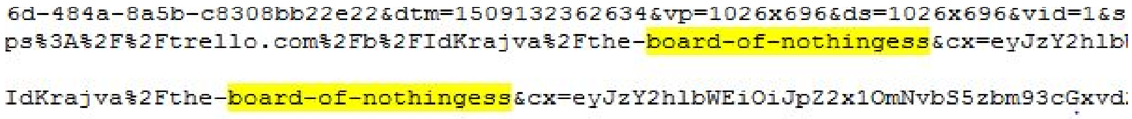
The f_00002f file in the old_Cache_000 folder within the Trello folder contained a PNG of the original background image for the board named “cool board” that was replaced with the current background image.

The data_1 file in the folder at ***/root/users/<username>/AppData/Local/Packages/45273LiamForsyth.PawsforTrello_7pb5ddty8z1pa/LocalCache/Roaming/Trello/Cache*** contained the names of the team, cards, boards, deleted boards and cards, and usernames. Most of the file, when viewed as plain text, seemed to be meaningless gibberish. However, there were URLs within this text that redirected the info to boards and text that contained a large portion of the information that was found. However, there were notable pieces of information, like certain board and card names, missing from the data. The first thing we realized is that there were many percent encoded URLs that linked to the different boards, as shown below. The board names are used as titled in the URLs with the exceptions of white spaces as dashes, and the names were all lowercase.



```
.rello-attachments.s3.amazonaws.com/59ee6f4a55c471c55
=https%3A%2F%2Ftrello.com%2Fb%2FWLzxvOhS%2Fcool-board
sktop&p=web&tz=America%2FNew York&lang=en-US&cs=UTF-8
```

*Figure 20: Found Board 1*



```
6d-484a-8a5b-c8308bb22e22&dtm=1509132362634&vp=1026x696&ds=1026x696&vid=1&s
ps%3A%2F%2Ftrello.com%2Fb%2FIdKrajva%2Fthe-board-of-nothingess&cx=eyJzY2hlb

IdKrajva%2Fthe-board-of-nothingess&cx=eyJzY2hlbWEiOiJpZ2x1OmNvbS5zbm93cGxvd
```

*Figure 21: Found Board 2*

We also found links that directed the user to the team that they were a member of. These URLs included the team ID, which consists of the original team name and possibly a numerical number to differentiate between teams of the same name.

*Figure 22: Team Name*

Not only were boards and teams present, but also the name of a card, though it is important to note that not all of the card names were present, and as such, we realized it would not be feasible for investigators to use this for any other reason besides the card names revealing intent.

*Figure 23: Found Card*

In addition to the normal boards and cards, the names of deleted boards and cards were also present.

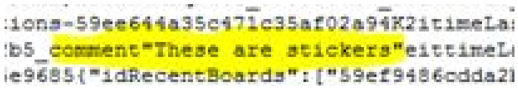
*Figure 24: Deleted Board and Card*

While we only managed to find one of the users within the data_1 file, it is worth noting that this was the user that was last logged in (and was not logged out at the end of the data generation.)

*Figure 25: Username*

While we were not able to find a way to find the names of boards or usernames easily without previous knowledge, it is still possible to find these within the URLs. It is also important to note that while there are URLs for Slack and Facebook, this does not necessarily indicate that the Trello user has accounts linked. In addition, while this file contained many artifacts, data_2 and data_3 only contained information relating to the digital certificate and the certificate authority, and data_0 contained minimal readable plaintext.

Within the LocalStorage folder within ***/root/users/<username>/AppData/Local/Packages/45273LiamForsyth.PawsforTrello_7pb5ddty8z1pa/LocalCache/Roaming/Trello/*** was the https_trello.com_0.localstorage file which contained an unsaved comment that reads "These are stickers". This is interesting because there were no records of any kind regarding the saved comments, yet the unsaved comment is cached locally, and could be of use to forensic investigators as no other comments are available.



```
:ions-59ee644a35c471c35af02a94K2itimeLa:
:b5_comment"These are stickers"eittimeL
:e9685{"idRecentBoards":["59ef9486cdda21
```

*Figure 26: Unsaved Comment*

The third relevant folder that we found was the com.atlassian.trello folder in the path ***root/users/<username>/AppData/Local/Packages/45273LiamForsyth.PawsforTrello_7pb5ddty8z1pa/LocalCache/Roaming/com.atlassian.trello***.

The main.log file in the path above contained a list of actions like refreshes, logins, and quitting the app, with each of the events containing a full timestamp. This was useful because it showed us when the account was active and what basis actions were taken on it.

*Figure 27: Main Log*

The starred-boards file at ***root/users/<username>/AppData/Local/Packages /45273LiamForsyth.PawsforTrello_7pb5ddty8z1pa/LocalCache/Roaming/com.atlassian.trello/storage/starred -boards*** contained information logs on the name of boards, if the boards are closed, the teams with access to the board, if it is pinned, the ID, the URL of the board, the permissions applied to the board, and the background images as URLs.

*Figure 28: Board Information*

## Conclusion

LastPass presented a challenge to analyze. A cursory glance at the LastPass files show no information can be gleaned from its local files. While the contents of a user's LastPass vault is secure and critical data is hidden, there is still forensically important information to be found. While seemingly secure, LastPass reveals user actions and emails through its URLs. Our research suggests that LastPass stores different amounts of data on different browsers, specifically Google Chrome. Our team found that LastPass is rather secure with Firefox, but other web browsers may be even more or substantially less secure.

For Steam, our results were congruent with our expectations. There were no major data leakages and no chat logs. However, it was interesting to find the configuration file for each chat window, and that could become relevant in an investigation. For the most part, there is no real threat posed by any of the available information, and as such, it is safe to conclude that Steam is a relatively secure application which also contains possibly relevant information that could aid in a forensic investigation.

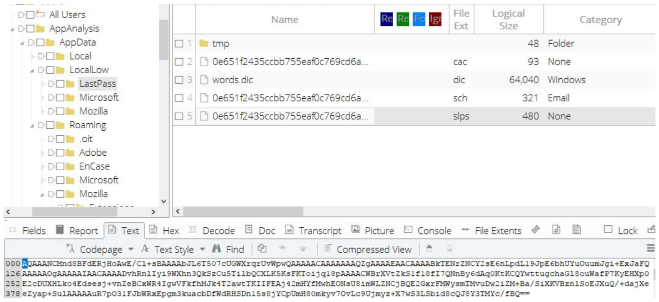
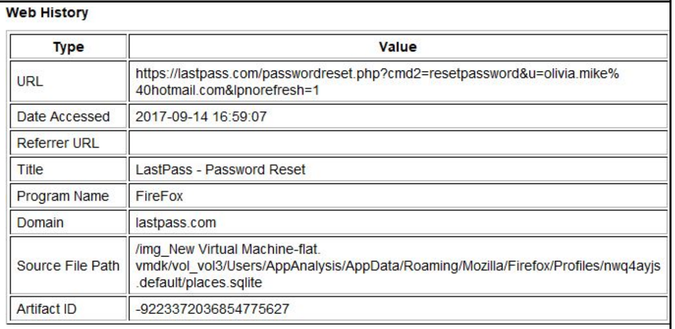
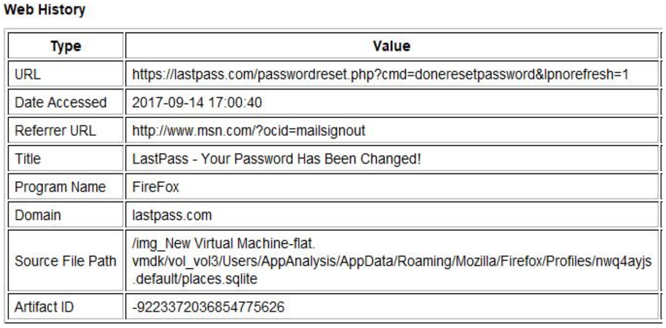
Analysis for Trello went quite differently than anticipated. Many items and artifacts that we expected to find, such as all of the cards, checklists, comments, etc., were not found. However, what we did find was more than enough to get an idea of how secure Trello is. The information made available poses no real threat, and as such, it is safe to conclude that Trello is a relatively secure application. In a forensic investigation, our conclusion is the same, that this application will not reveal much information besides timestamps or deleted boards and card names.

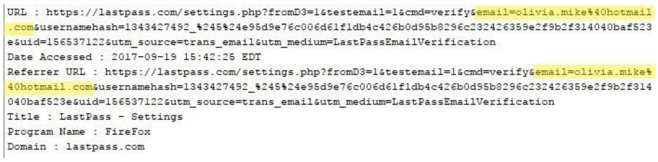
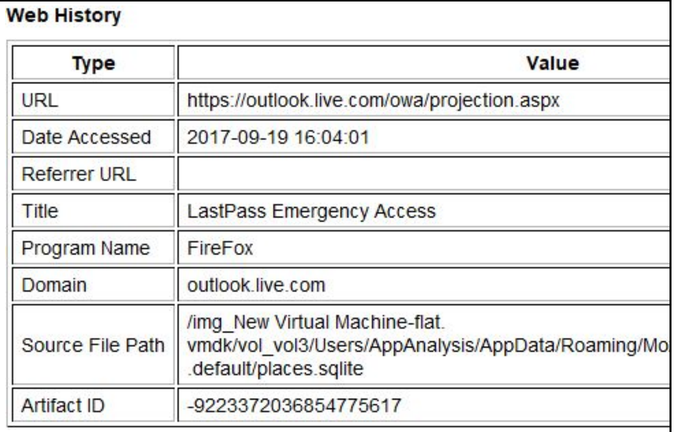
## Further Work

While the Application Analysis team covered a lot of ground, there are many more applications that could be analyzed by future iterations of this project. So far, the LCDI has analyzed seven desktop applications over varying operating systems, but there are many more popular apps that could also store relevant information on hosts. In addition, during our LastPass analysis, we found that the LastPass extension may store varying information on browsers, specifically Chrome, and in the future, it would be interesting to see a project that could analyze extension artifacts. During our initial research, our team narrowed down the list of applications to study to twelve, including Twitter, Facebook, Venmo, Google Drive, and others which we were unable to analyze due to time constraints. In general, this project can be very flexible, and subsequent teams can narrow their focus based on interest and current popularity of specific applications. gy

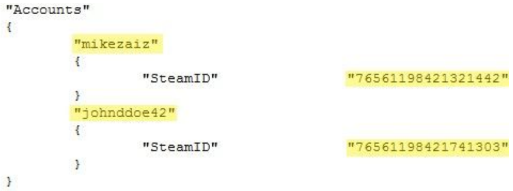
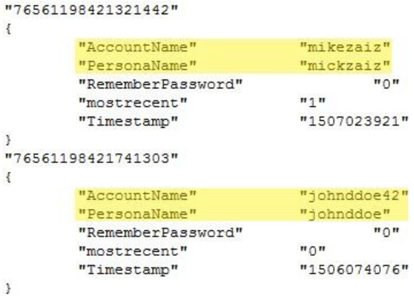
# Appendix

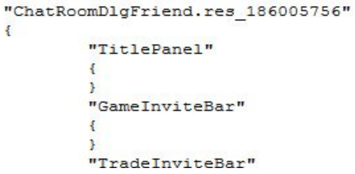
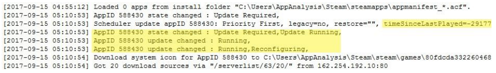
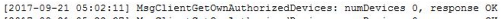
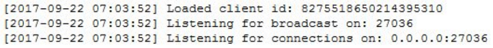
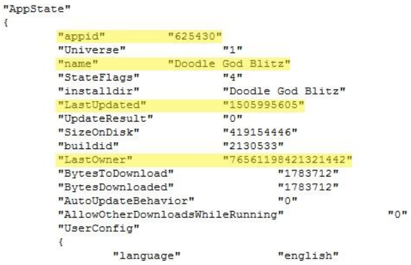
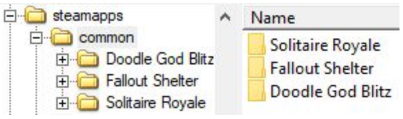
## 1: LastPass Evidence Table

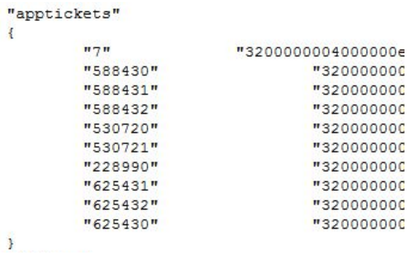
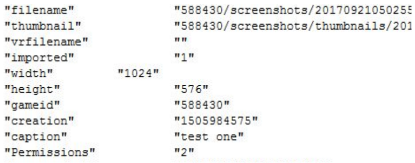
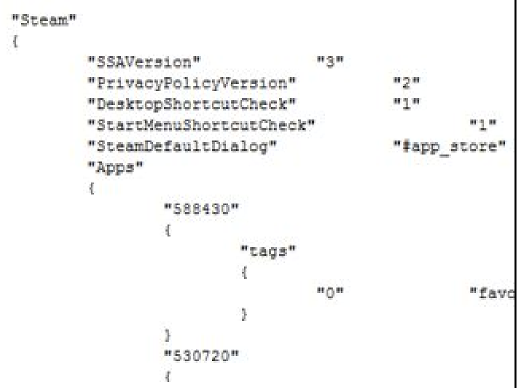
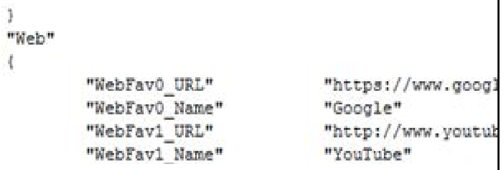
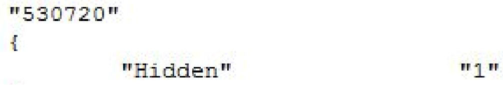
<table>
<tr><th>Evidence found</th><th>Where</th><th>Notes</th><th>Screenshot</th></tr>
<tr><td>LastPass Encrypted Data</td><td><b><i>/root/users/&lt;username&gt;/appdata/LocalLow/LastPass</i></b></td><td></td><td>

<table>
<tr><th></th><th>Name</th><th>File Ext</th><th>Logical Size</th><th>Category</th></tr>
<tr><td>1</td><td>tmp</td><td></td><td>48</td><td>Folder</td></tr>
<tr><td>2</td><td>0e651f2435ccbb755eaf0c769cd6a...</td><td>cac</td><td>93</td><td>None</td></tr>
<tr><td>3</td><td>words.dic</td><td>dic</td><td>64,040</td><td>Windows</td></tr>
<tr><td>4</td><td>0e651f2435ccbb755eaf0c769cd6a...</td><td>sch</td><td>321</td><td>Email</td></tr>
<tr><td>5</td><td>0e651f2435ccbb755eaf0c769cd6a...</td><td>slps</td><td>480</td><td>None</td></tr>
</table>
<pre>
000 AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAbJL6T507cUGWXrqrUvWpwQAAAAACAAAAAAAQZgAAAAEAACAAAABkTENrZNCY2sE6nLpdL19JpE6bhUYuOuumJgi+ExJaFQ
126 AAAAAOgAAAAAIAACAAAADvhRnlIyi9WXhn3QkSzCu5TilbQCXLK5KsFKToijql8pAAAACWBrXVtZkSlfl8fI7QNnBy6dAq0KtKCQYwttugchaGl8ouWafP7KyEHXp0
252 E2cDUXHLko4Edsesj+vnZeBCxWR4IgwVFkfhMJk4T2awtTKIIFEAj42mHYfMwhEONsU8imWLZNCjBQE2GxrFMWysmTMvuDw2iZM+Ba/SiXKVBznlSoEJXuQ/+dajXe
378 eZyap+SulAAAAAuR7pO3lFJbWRxEpgm3kuacbDfWdRHSDnl5s8jYCpUmH80mkyv7OvLc9Ujmyz+X7wS3LSbid8cQJ8Y3TMYc/fBQ==
</pre>
<i>Figure 1: Location of LastPass Encrypted Data</i></td></tr>
<tr><td>Password Reset Page</td><td></td><td>Evidence of the password reset page being accessed.</td><td>

<b>Web History</b>
<table>
<tr><th>Type</th><th>Value</th></tr>
<tr><td>URL</td><td>https://lastpass.com/passwordreset.php?cmd2=resetpassword&u=olivia.mike%40hotmail.com&lpnorefresh=1</td></tr>
<tr><td>Date Accessed</td><td>2017-09-14 16:59:07</td></tr>
<tr><td>Referrer URL</td><td></td></tr>
<tr><td>Title</td><td>LastPass - Password Reset</td></tr>
<tr><td>Program Name</td><td>FireFox</td></tr>
<tr><td>Domain</td><td>lastpass.com</td></tr>
<tr><td>Source File Path</td><td>/img_New Virtual Machine-flat.vmdk/vol_vol3/Users/AppAnalysis/AppData/Roaming/Mozilla/Firefox/Profiles/nwq4ayjs.default/places.sqlite</td></tr>
<tr><td>Artifact ID</td><td>-9223372036854775627</td></tr>
</table>
<i>Figure 2: Password Reset</i></td></tr>
<tr><td>Password Reset Complete</td><td><b><i>/root/users/&lt;username&gt;/appdata/roaming/mozilla/firefox/profiles/nwqayjs.default/places.sqlite</i></b></td><td>Result of changing a password. A URL is left behind noting the LastPass master password was changed.</td><td>

<b>Web History</b>
<table>
<tr><th>Type</th><th>Value</th></tr>
<tr><td>URL</td><td>https://lastpass.com/passwordreset.php?cmd=doneresetpassword&lpnorefresh=1</td></tr>
<tr><td>Date Accessed</td><td>2017-09-14 17:00:40</td></tr>
<tr><td>Referrer URL</td><td>http://www.msn.com/?ocid=mailsignout</td></tr>
<tr><td>Title</td><td>LastPass - Your Password Has Been Changed!</td></tr>
<tr><td>Program Name</td><td>FireFox</td></tr>
<tr><td>Domain</td><td>lastpass.com</td></tr>
<tr><td>Source File Path</td><td>/img_New Virtual Machine-flat.vmdk/vol_vol3/Users/AppAnalysis/AppData/Roaming/Mozilla/Firefox/Profiles/nwq4ayjs.default/places.sqlite</td></tr>
<tr><td>Artifact ID</td><td>-9223372036854775626</td></tr>
</table>
<i>Figure 3: Password Change Confirmation</i></td></tr>
</table>

<table>
<tr>
<td>Email Verification</td>
<td><b><i>/root/users/ &lt;username&gt; /appdata/roaming/ Mozilla /firefox/profiles/nwqayjs.default /places.sqlite</i></b></td>
<td>Email verification URL shows the email address associated with the LastPass account in plaintext.</td>
<td><br>URL : https://lastpass.com/settings.php?fromD3=1&testemail=1&cmd=verify&email=olivia.mike%40hotmail.com&usernamehash=1343427492_%245%24e95d9e76c006d61f1db4c426b0d95b8296c232426359e2f9b2f314040baf523e&uid=156537122&utm_source=trans_email&utm_medium=LastPassEmailVerification<br>Date Accessed : 2017-09-19 15:42:25 EDT<br>Referrer URL : https://lastpass.com/settings.php?fromD3=1&testemail=1&cmd=verify&email=olivia.mike%40hotmail.com&usernamehash=1343427492_%245%24e95d9e76c006d61f1db4c426b0d95b8296c232426359e2f9b2f314040baf523e&uid=156537122&utm_source=trans_email&utm_medium=LastPassEmailVerification<br>Title : LastPass - Settings<br>Program Name : FireFox<br>Domain : lastpass.com<br><i>Figure 4: Email Verification URL</i></td>
</tr>
<tr>
<td>Emergency Access</td>
<td><b><i>/root/users/&lt;username&gt;/appdata/roaming/Mozilla/firefox/profiles/nwqayjs.default /places.sqlite</i></b></td>
<td>Email indicating emergency access offered to the LastPass user.</td>
<td><br>Web History<br>
<table>
<tr><th>Type</th><th>Value</th></tr>
<tr><td>URL</td><td>https://outlook.live.com/owa/projection.aspx</td></tr>
<tr><td>Date Accessed</td><td>2017-09-19 16:04:01</td></tr>
<tr><td>Referrer URL</td><td></td></tr>
<tr><td>Title</td><td>LastPass Emergency Access</td></tr>
<tr><td>Program Name</td><td>FireFox</td></tr>
<tr><td>Domain</td><td>outlook.live.com</td></tr>
<tr><td>Source File Path</td><td>/img_New Virtual Machine-flat.vmdk/vol_vol3/Users/AppAnalysis/AppData/Roaming/Mo .default/places.sqlite</td></tr>
<tr><td>Artifact ID</td><td>-9223372036854775617</td></tr>
</table>
<i>Figure 5: Emergency Invitation</i></td>
</tr>
</table>

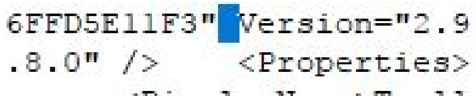
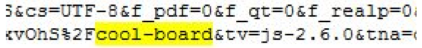
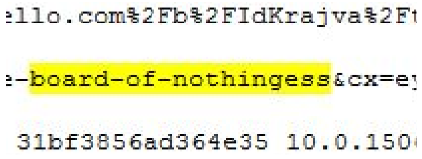
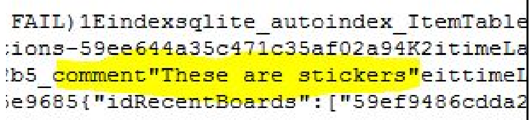
## 2: Steam Evidence Table

| Evidence found | Where | Notes | Screenshot |
|---|---|---|---|
| User config | ***root/users/ <username> /Steam /config /config.vdf.*** | User ID and Steam64 ID | <br>"Accounts"<br>{<br>"mikezaiz"<br>{<br>"SteamID" "76561198421321442"<br>}<br>"johnddoe42"<br>{<br>"SteamID" "76561198421741303"<br>}<br>}<br>*Figure 6: Users That Logged In* |
| User information | ***root/users/ <username> /Steam/config/ loginusers.vdf*** | Steam64 ID, account name, personal name, remember password option, whether they were the last account to be logged in, timestamp | <br>"76561198421321442"<br>{<br>"AccountName" "mikezaiz"<br>"PersonaName" "mickzaiz"<br>"RememberPassword" "0"<br>"mostrecent" "1"<br>"Timestamp" "1507023921"<br>}<br>"76561198421741303"<br>{<br>"AccountName" "johnddoe42"<br>"PersonaName" "johnddoe"<br>"RememberPassword" "0"<br>"mostrecent" "0"<br>"Timestamp" "1506074076"<br>}<br>*Figure 7: User Information* |

| | | | |
|---|---|---|---|
| Chatlog with friends. | ***root/users/<username> /Steam/config/ DialogConfig.vdf*** | The number 186005756 in the line ChatRoomDlgFriend.res_186005756 is the user ID32 for the user Navitri. Thus, there is proof of a chat with Navitri.<br>There was also one with Johnddoe42. |  "ChatRoomDlgFriend.res_186005756"<br>{<br>"TitlePanel"<br>{<br>}<br>"GameInviteBar"<br>{<br>}<br>"TradeInviteBar"<br>*Figure 8: Chat Window Configuration* |
| Content Log | ***root/users/ <username> /Steam /logs/ content_log.txt*** | Logs App states, downloads, install folders |  [2017-09-15 04:55:12] Loaded 0 apps from install folder "C:\Users\AppAnalysis\Steam\steamapps\appmanifest_*.acf".<br>[2017-09-15 05:10:53] AppID 588430 state changed : Update Required,<br>[2017-09-15 05:10:53] Scheduler update appID 588430: Priority First, legacy=no, restore="", timeSinceLastPlayed=-29177<br>[2017-09-15 05:10:53] AppID 588430 state changed : Update Required,Update Running,<br>[2017-09-15 05:10:53] AppID 588430 update changed : Running,<br>[2017-09-15 05:10:53] AppID 588430 update changed : Running,Reconfiguring,<br>[2017-09-15 05:10:54] Download system icon for AppID 588430 to C:\Users\AppAnalysis\Steam\steam\games\80fdcda332260468<br>[2017-09-15 05:10:54] Got 20 download sources via "/serverlist/63/20/" from 162.254.192.10:80<br>*Figure 9: Content Log* |
| Library Sharing | ***root/users/<username> /Steam /logs/ librarysharing_log .txt*** | Lists number of shared devices. May list other information when library is shared. This was not explored in the project. |  [2017-09-21 05:02:11] MsgClientGetOwnAuthorizedDevices: numDevices 0, response OK<br>*Figure 10: Library Sharing Log* |
| Remote connections list | ***root/users/<username> /Steam /logs/ remote_connections.txt*** | Lists remote connections with timestamps. Seems to consistently listen on port 27036.<br>Note: None used in this project |  [2017-09-22 07:03:52] Loaded client id: 8275518650214395310<br>[2017-09-22 07:03:52] Listening for broadcast on: 27036<br>[2017-09-22 07:03:52] Listening for connections on: 0.0.0.0:27036<br>*Figure 11: Remote Connection Log* |
| Game details | ***root/users/<username>  /Steam /steamapp/ appmanifest_<App ID>.acf*** | Game name, language, Steam App ID, last updated, last owner (formatted as Steam ID), etc. |  "AppState"<br>{<br>"appid" "625430"<br>"Universe" "1"<br>"name" "Doodle God Blitz"<br>"StateFlags" "4"<br>"installdir" "Doodle God Blitz"<br>"LastUpdated" "1505995605"<br>"UpdateResult" "0"<br>"SizeOnDisk" "419154446"<br>"buildid" "2130533"<br>"LastOwner" "76561198421321442"<br>"BytesToDownload" "1783712"<br>"BytesDownloaded" "1783712"<br>"AutoUpdateBehavior" "0"<br>"AllowOtherDownloadsWhileRunning" "0"<br>"UserConfig"<br>{<br>"language" "english"<br>*Figure 12: App Information* |
| Games downloaded | ***root/users/<username>  /Steam/ steamapps/ common<br>Or custom path*** | These folders contain the full game, however, users can change the default download path on installation. |   steamapps<br>common<br>Doodle God Blitz<br>Fallout Shelter<br>Solitaire Royale<br>Name<br>Solitaire Royale<br>Fallout Shelter<br>Doodle God Blitz<br>*Figure 13: Default Installation Folder* |

| | | | |
|---|---|---|---|
| App ID List | ***root/users/<username> /Steam /userdata/<Steam32 ID>/config/ localconfig.vdf*** | List of “apptickets” that can act as a master list of apps installed.<br>Note that one game can have more than one App ID due to game packages and DLCs. | <br>"apptickets"<br>{<br>"7" "3200000004000000e<br>"588430" "32000000C<br>"588431" "32000000C<br>"588432" "32000000C<br>"530720" "32000000C<br>"530721" "32000000C<br>"228990" "32000000C<br>"625431" "32000000C<br>"625432" "32000000C<br>"625430" "32000000C<br>}<br>*Figure 14: Game List* |
| Screenshot information | ***root/users/<username> /Steam /userdata/<Steam32 ID>/760/ screenshot.vdft*** | Screenshot filename, thumbnail, creation, and caption | <br>"filename" "588430/screenshots/20170921050255<br>"thumbnail" "588430/screenshots/thumbnails/201<br>"vrfilename" ""<br>"imported" "1"<br>"width" "1024"<br>"height" "576"<br>"gameid" "588430"<br>"creation" "1505984575"<br>"caption" "test one"<br>"Permissions" "2"<br>*Figure 15: Screenshot Information* |
| Library, web info, hidden games | ***root/users/<username> /Steam /userdata/ <Steam32 ID>/7/remote/ sharedconfig.vdf*** | Category creation, names, favorite web URL and name<br>The number 530720 is the Steam App ID for Solitaire Royale, a game hidden during data generation. | <br>"Steam"<br>{<br>"SSAVersion" "3"<br>"PrivacyPolicyVersion" "2"<br>"DesktopShortcutCheck" "1"<br>"StartMenuShortcutCheck" "1"<br>"SteamDefaultDialog" "#app_store"<br>"Apps"<br>{<br>"588430"<br>{<br>"tags"<br>{<br>"0" "favo<br>}<br>}<br>"530720"<br>{<br>*Figure 16: Game Tags*<br><br>}<br>"Web"<br>{<br>"WebFav0_URL" "https://www.googl<br>"WebFav0_Name" "Google"<br>"WebFav1_URL" "http://www.youtub<br>"WebFav1_Name" "YouTube"<br>*Figure 17: Favorite Web Links*<br><br>"530720"<br>{<br>"Hidden" "1"<br>*Figure 18: Hidden Game* |

### 3: Trello Evidence Table

| Evidence found | Where | Notes | Screenshot |
|---|---|---|---|
| Version Number | ***/root /ProgramFiles /WindowsApps /45237LiamForsyth. PawsforTrello_2.9.8.0_ x64__7pb5ddty8z1pa /AppxManifest.xml*** | | <br>`6FFD5E11F3" Version="2.9 .8.0" />    <Properties>`<br>*Figure 19: Accurate Version Number* |
| Team, Board, and Card names (not all)<br>Deleted Boards and Cards<br>Username | ***/root /users /<username>/AppData /Local /Packages /45273LiamForsyth. PawsforTrello_7pb5ddty8z1pa /LocalCache /Roaming /Trello /Cache /data_1***<br>(Data_2 and Data_3 only contain Certificate information, and Data_0 contains no relevant text) | This file in plain text seems to be meaningless, however, within it, there are URL redirects to boards and teams that contain the team and board names including deleted ones.<br>URLs are not directly accessible in a browser. | <br>`&cs=UTF-8&f_pdf=0&f_qt=0&f_realp=0`<br>`vOhS%2Fcool-board&tv=js-2.6.0&tna=`<br>*Figure 20: Found Board 1*<br><br>`llo.com%2Fb%2FIdKrajva%2F`<br>`-board-of-nothingess&cx=e`<br>`31bf3856ad364e35 10.0.150`<br>*Figure 21: Found Board 2*<br>*Figure 22: Team Name*<br>*Figure 23: Found Card*<br>*Figure 24: Deleted Board and Card*<br>*Figure 25: Username* |
| Unsaved Comment | ***/root /users /<username> /AppData /Local /Packages /45273LiamForsyth. PawsforTrello_7pb5ddty8z1pa /LocalCache /Roaming /Trello /LocalStorage /https_trello.com_0.localstorage*** | | <br>`FAIL)1Eindexsqlite_autoindex_ItemTable`<br>`ions-59ee644a35c471c35af02a94K2itimeLa`<br>`b5_comment"These are stickers"eittimeL`<br>`e9685{"idRecentBoards":["59ef9486cdda2`<br>*Figure 26: Unsaved Comment* |

| | | | |
|---|---|---|---|
| Logs and Timestamps | ***/root /users /<username> /AppData /Local /Packages /45273LiamForsyth.PawsforTrello_7pb5ddty8z1pa /LocalCache /Roaming /com.atlassian.trello /logs /main.log*** | log of actions which includes refreshes, logins, quitting app. Each event has a full timestamp. | *Figure 27: Main Log* |
| Information about board(s) | ***/root /users /<username> /AppData /Local /Packages /45273LiamForsyth.PawsforTrello_7pb5ddty8z1pa /LocalCache /Roaming /com.atlassian.trello /storage /starred-boards*** | Name of board, if closed, team, if pinned, ID, URL of board, permissions, background images as URLs | *Figure 28: Board Information* |

## References

“Artifacts.” *LCDI Wiki*, LCDI, 2 Feb. 2015, 19:11, wiki.lcdi/index.php/Artifacts.

“Autopsy.” *LCDI Wiki*, LCDI, 2 May 2016, 13:30, wiki.lcdi/index.php/Autopsy.

“Digital Evidence.” LCDI Wiki, LCDI, 28 Jan. 2015, 17:05, wiki.lcdi/index.php/Digital_Evidence.

“Digital Forensics.” *LCDI Wiki*, LCDI, 17 Feb. 2015, 11:16, wiki.lcdi/index.php/Digital_Forensics.

“EnCase.” *LCDI Wiki*, LCDI, 25 May 2016, 13:33, wiki.lcdi/index.php/EnCase.

“FTK.” *LCDI Wiki*, LCDI, 20 Apr. 2015, 16:46, wiki.lcdi/index.php/FTK.

“Virtual Machine (VM).” *LCDI Wiki*, LCDI, 14 Apr. 2015, 10:13, wiki.lcdi/index.php/Virtual_Machine_(VM).

Whitcomb, C. M. (2002). An Historical Perspective of Digital Evidence: A Forensic Scientist’s View. *International Journal of Digital Evidence,1*(1), 4. Retrieved September 25, 2017.