The Forensic Analysis of KeePass and Password Safe:

An Evaluation of Open Source Password Managers

By

Daryl R. Middleton
Graduate Student
Capstone Project for Information Security and Intelligence
Ferris State University

Advisor:
Dr. Greg Gogolin, Ph.D.
Full Professor
Department of Information Security and Intelligence

Spring, 2017
Ferris State University
Big Rapids, MI

ACKNOWLEDGEMENTS

The process of completing a Capstone Project is one that builds on many semesters of hard work. It is a compilation of skillsets that have accumulated over the course of study and experiences crafted by talented instructors. I would like to thank Professor Greg Gogolin, Ph.D. for his ability to teach the technical aspects of Digital Forensics; yet emphasize the importance of people as part of the equation and how they are affected by the investigators findings. The deep knowledge that Professor Gogolin possesses in each subject area provided a broad platform from which to integrate disparate ideas and creative solutions. His rapid response to questions and academic guidance was critical to the success of this project.

I would also like to thank Associate Professor Jim Furstenberg for his enthusiastic approach to learning especially where group collaboration is essential. His insight into time management, gathering intelligence and documenting research material was so helpful in maintaining an organized methodology from the very beginning of the project.

I would like to thank Professor Hwee-Joo Kam D.Sc. for her knowledge and teaching skills pertaining to database design and security that was instrumental in helping me understand the importance of those concepts. The concept of database security, establishment of trust and data integrity were directly applicable to this project.

Last but not least I would like to thank my wife Joni who placed many of our plans on hold for several months so that I could dedicate the time and resources required to complete the Capstone Project. Each of you contributed immensely to the success of this experience.

Table of Contents

Page

List of Tables

Page

List of Figures

Page

Abstract

Access control elements such as identification and authentication form part of the initial security landscape when integrated into a defense in depth strategy. Identification allows a user to profess an identity with a username while authentication with a password provides a challenge to that claimed identity. Identification and authentication credentials that are too easy to guess will lead to unauthorized access to network resources. Credentials that are based on business security policies have established requirements for complexity and change management that many times produce unintended consequences for users. Password management programs can help mitigate some of the complexities of access control but there must be trust in the processes ability to assure data integrity. This project systematically challenges two popular open source password management tools that are intentionally subjected to low memory resources within pre-configured virtual machines. Subsequent examination of forensic images and digital artifacts obtained from the prototype virtual machine architecture reveal that constrained memory resources seem to affect the efficiency of the underlying encryption algorithm. This phenomenon causes the Master Key and underlying database credentials in some cases to be captured by forensic software in plain text format from virtual memory and deleted files that remain on disk.

Keywords: Password Managers, Authentication, Digital Forensics, Virtual Machines

Chapter 1- Introduction

Background

Rapid developments in technology have created new challenges to the field of cybersecurity especially in the area of effective password management as part of the authentication process. The problem is that adequate user authentication has become an enigmatic process that requires passwords to be changed at a greater frequency and generated with higher complexity requirements. This process can generate unintended consequences.

IT management is tasked with establishing security policies at every level of the system to protect business assets but the painful truth is that the computer user is still the weakest link in the security chain. Information security is not only a technical issue but also a behavioral issue involving users (Bang, Lee, Bae & Ahn, 2012, p. 409). IT Security professionals turn to password management systems as an affordable, important component of access control in an attempt to help users remain compliant with company Information Security policies. A robust password manager has the ability to generate passphrases of configurable complexity, store them in an encrypted state, providing user auto fill capabilities on form field data while simultaneously protected by a Master Key (Gray, Franqueira & Yu, 2016, p. 2). KeePass version 2.35 and Password Safe 3.41 are popular open source password managers that have these capabilities and are the subject of this project.

Users of computer information systems often times do not understand threat models or known vulnerabilities and view security protocols as something that they have to work around. As an IT Specialist employed in industry I witnessed how the demands of a highly regulated environment placed a great deal of responsibility on the workforce to remain compliant with company Information Security policies. One area of technical support that surfaced frequently dealt with the employee’s ability to manage all of the passwords that they needed to utilize efficiently on a daily basis. Those individuals with elevated privileges had even more difficulty in managing their passwords due to the security policy that required a higher level of complexity for each password and greater frequency for changing them.

Employees routinely utilized spreadsheets or text files to create a system to help recall the passwords when they were needed. Some unintended consequences surfaced included password files that were not backed up to a server and eventually lost, inadequate password encryption and the lack of a password generation function that was designed to comply with the company Information Security Policy. “Users must understand that they are the last bastion of defense in any security design and that they need to make tradeoffs for better security (McGraw, 2006, p. 38).

Confusion and chaos that develops due to poor password management practices can quickly become a compliance issue in most industries. The problem for the IT Security manager is deciding on what password management package will be a good fit for the operation when considering usability, industry best practice and product trust based on testing.

Problem Statement

The problem to be evaluated in this project is focused on discovering digital artifacts that may surface during the forensic investigation of two open source password managers tested on virtual machines configured with differing RAM resources. Included in the testing process are the KeePass and Password Safe systems. The digital artifacts to be searched for include the Master Key and any underlying protected data assets they may reside within the secured vaults. The Master Key does not have a recovery option so if a user forgets the key there is no way to access the accounts contained within the encrypted vault. However, the inadvertent discovery of the Master Key by a nefarious individual provides unlimited access to all of the underlying account credentials stored in the encrypted vault.

The decision was made to restrict the scope of this project to that of the KeePass and Password Safe products since they are open source, free and similar in functionality. This allows for a comprehensive investigation of specific user initiated events; which are also referred to as Trial Events that may create digital artifacts in the presence of constrained memory resources. There will also be research into potential differences when the password manager files are synchronized from a Dropbox cloud server instead of a local machine installation. Digital artifacts will be examined that may reside on host hard drive, virtual machines, physical and virtual memory. The examination of a similar class of password managers allowed time to experiment with a broad range of tools including VMWare Workstation, Wireshark, Python Volatility, FTK, FTK Imager, Encase 7 and forensic imaging with a Tableau Write Blocker.

An important aspect that will not be covered within the scope of this project pertains to the security testing of any mobile app. Previous studies of the Android operating system disclosed vulnerabilities when certain apps are decompiled causing authentication credentials to appear in plain text (Trujano, F., Chan, B., Beams, G. et al., 2016, p.7). The examination of the Android operating system as it interacts with the KeePass app on mobile devices could be the subject of its own project and investigation.

Purpose of the Study

The main purpose of this study is to determine if the popular open source KeePass and Password Safe password managers Master Key or underlying secured credentials become vulnerable to discovery within digital artifacts as a result of low memory resources when subjected to specified user initiated events. The goal is to create a virtual test environment which facilitates the utilization of as many tools and skills learned in our program; to thoroughly investigate the processes involved during and after the password management software has been used for authentication under structured conditions. The hope is that the prototype VMWare architecture created for this project could be reproduced by any IT Department. This could assist in the testing and selection of a password manager of their choice and allow users to evaluate various user interfaces without affecting enterprise network operations.

Rationale

The results obtained from this project may help indicate how much trust should be placed on the password manager system and the effect it may have on the enterprise and system managers that implement them. IT Security personnel must have some metric to evaluate the functionality and vulnerabilities of any new system that will be integrated into the existing workflow. Specifically, a password managing process that utilizes a Master Key to create an encrypted vault containing important business assets.

Research Questions:

1. Does the Master Key or underlying secured credentials for databases protected by the KeePass and Password Safe software become vulnerable to discovery within digital artifacts on disk when there are low memory resources?
2. Does moving the database from the local machine to a cloud environment such as Dropbox elicit observable differences in the discovery of digital artifacts?
3. Is there recoverable data from memory while utilizing FTK or Volatility when examining VMWare Snapshots?

4. Will KeePass with AES/Rijndael and Password Safe with Two Fish algorithms perform equally in protecting underlying data when subjected to the scheduled Trial Events?

Nature of the Study

This paper is one of the final deliverables that documents a project involving the development of eight virtual machines designed to capture and identify digital artifacts. The digital artifacts may be discovered through forensic examination as a result of routine user initiated events (Trial Events). The Trial Events include entering login data with a Master Key, random password generation, perform auto-type in form fields, copy to clipboard, copy/paste, export database, print a password database and delete a database.

Significance of the Project

It is important that a password manager be able to protect the Master Key since it has the potential to decrypt any underlying password database. This project and paper will help provide insight into the trustworthiness of the popular KeePass and Password Safe's password managing capabilities. Especially, as it pertains to effectively protecting the Master Key when operating in environments with constrained system and memory resources.

To maintain the integrity of this study it is important to establish guidelines as they pertain to scientific process. Three aspects of the scientific process that need to be addressed involve defining a research question, formulating a hypothesis and being able to verify the findings (Gogolin, 2013, p. 2). The main research question previously mentioned is "Does the Master Key or underlying secured credentials for databases protected by the KeePass and Passware Safe become vulnerable to discovery within digital artifacts when there are low memory resources?"

The hypothesis is that when physical RAM has been exhausted there may be digital artifacts that can be recovered from the host hard drive. This did occur in a previous study during the use of virtual machines configured with only 1 Gig of RAM and an older version of Keepass 2.28, Password Safe version 3.35 and RoboForm version 7.9.12 (Gray, Franqueira, & Yu, 2016, p. 2). That study was not able to test memory constraints and compare results between variable RAM configurations on password management efficiency since all of the virtual machines had been configured with 1 Gig of RAM.

Therefore the relationship between low RAM resources and inadvertent exposure of sensitive data were not able to be verified during the (Gray, 2016) study. Previous studies limited the use of KeePass and Passware Safe as a database located on a local machine where this project will also test the password database efficiency when synchronized and executed from a cloud server such as Dropbox.

The scientific process of this study includes the utilization of VMWare Workstation 12 to facilitate the creation of eight virtual machines. They will be configured according to the password manager used, memory allocated and local or cloud based execution. Please see the virtual machine architectural diagram and user initiated event (Trial Event) flowchart listed as Figure 25 and Figure 26 in Appendix A. This project will allow each test to be run in its own virtual environment in accordance to specific parameters and user initiated events that help create the digital artifacts. The hope is that by creating virtual machines with intentionally low RAM memory capacity (1Gig) and adequate RAM memory capacity (4Gig) that it will provide insight into some relationship of the quality of service from the KeePass and Password Safe.

Virtual Memory. Virtual memory is created by the operating system to provide each process its own private virtual address space. This abstraction creates a separation between the logical memory that a process sees and the actual physical memory installed on the machine (VMWare, 2017).

A successful measured outcome for this project would be the discovery of the KeePass or Password Safe Master Key and underlying protected credentials in a readable format within the examined digital artifacts. The final deliverable will include a paper documenting the research and a technology video created using SnagIt and Camtasia Studio.

Assumptions and Limitations

A major assumption is that previous studies were conducted with only low memory virtual machines and recent software patches have addressed some issues that deal with better encryption and security.

In particular are substantial differences in encryption algorithms between KeePass version 2.28 and 2.35 (Reichl, 2016, p.1). This project will utilize KeePass version 2.35 but with the default AES-KDF key derivation encryption algorithm that accompanies the KDBX 3.1 file structure. KeePass 2.35 allows the user to select a newer KDBX 4 file structure with the award winning Argon2 encryption algorithm. Argon 2 provides better resistance to GPU/ASIC brute force attacks in case the database was exported for password cracking (Reichl, 2016). The limitation with the Argon 2 encryption algorithm is that it is new and not ported to all services at this time.

Similarly, Password Safe version 3.41 is the latest release of this open source password manager and has also undergone code modifications since the (Gray, 2016) study. Password

Safe utilizes the Two Fish encryption algorithm for securing the Master Key and underlying databases (Schneier, 2016, p. 1).

The naming convention of virtual machines in this project will follow a specific format so when large amounts of data are processed it can be easily associated with a specific machine and process. For example virtual machine #2 is named VM2-PS-1G-local and indicates that VM2 is utilizing Password Safe (PS) with 1Gig of RAM and is initiated from the local machine.

In contrast virtual machine #7 is named VM7-IE-4G-cloud which indicates that VM7 is utilizing KeePass (IE) with 4 Gig of RAM and is initiated from a cloud server such as Dropbox. That way when a VMWare Snapshot is taken of the virtual machine for evidence the Snapshot Manager will include the virtual machine name in each snapshot. An example of a captured memory image from a virtual machine would look like VM2-PS-1G-local – [snapshot name].vmem. This is the best case scenario from a forensic standpoint since physical memory is written to disk as a .vmem file when taking a snapshot of the virtual machine (Ruff, 2008, p. 85).

Chapter 2 – Literature Review

Method of Review

This project is a causal study designed to determine whether one or more variables can affect an outcome that will be measured by the presence of digital forensic artifacts. The variables include a virtual environment that replicates constrained memory resources while executing the password managers as a local machine and then from a cloud server. The methodology utilized to formulate a basis for the final project involved serious consideration of a topic that is currently of interest to the business community from an Information Security perspective and could be considered complimentary to previous studies. Literature review was constructed in such a way that it would help to provide a conceptual framework for a logical scientific process that is repeatable and verifiable (Gogolin, 2013, p. 3).

The process of selecting previous works included the utilization of search criteria that limited the queried returns within established guidelines. This included setting the queries to filter only works that specifically identified research on password management software systems within the last four years. Information was obtained from scholarly sources such as the Ferris State University library system, Google Scholar, paid subscriptions to the Association of Computing Machinery and the American Health Information Management Association. The scholarly literature was stored in a document research tool named Mendeley Desktop.

Information Security Implications

The underlying security of information systems cannot be reliant upon casual review but more upon proven industry best practice and established protocols. Therefore the confidentiality, integrity and availability of the information systems must remain first and foremost (Stewart, Chapple & Gibson, 2012, p. 3). Controlling legitimate access to information systems is critical and requires a well thought out process for the authentication of users whom will be allowed access to the information systems.

Authentication can involve multiple steps also known as multi-factor authentication for increased security but in its simplest form is a two step process that is set up to establish access control to network resources. The first step is to identify the individual by an assigned username which also assists in determining the role of the user. The second step is authorization where the user must enter a secret password or phrase referred to as “something you know” to complete the authentication process (Stewart, Chapple & Gibson, 2012, p. 9).

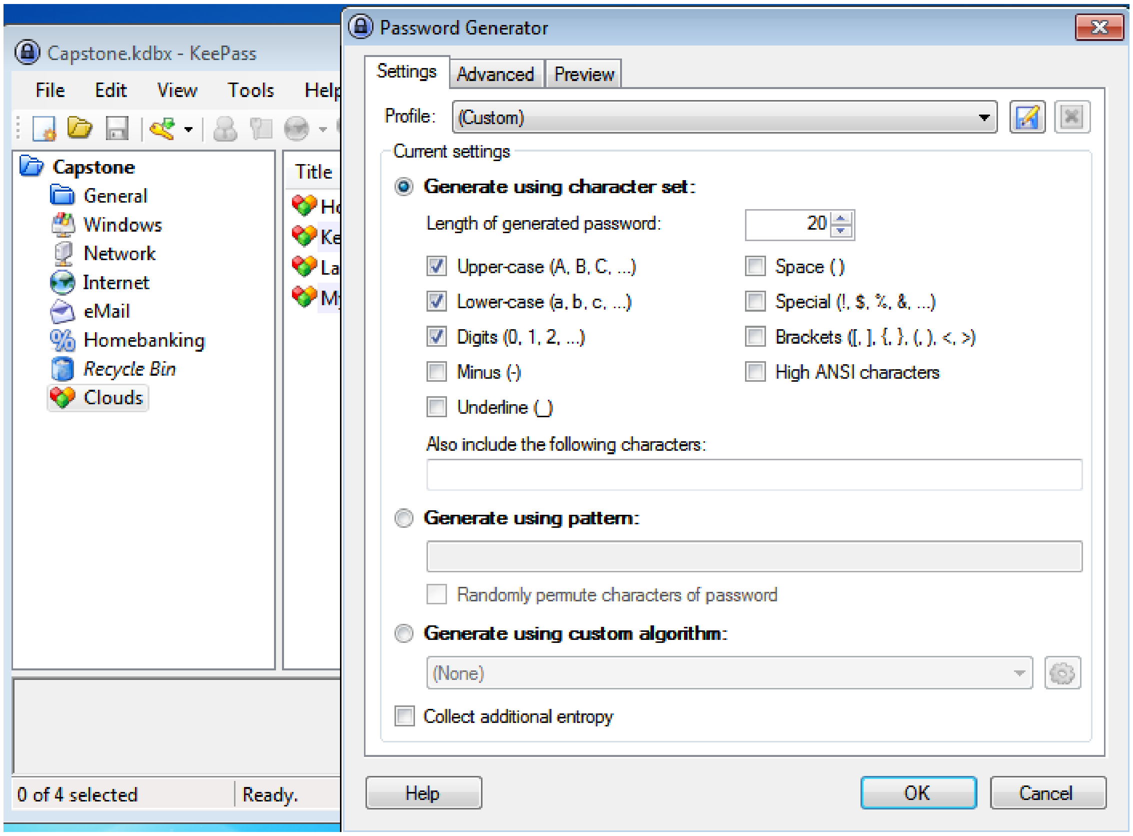
The authentication process can provide additional layers of security by requiring the user to provide “something you have” like a key card and “something you are” such as a biometric requirement (Stewart, Chapple & Gibson, 2012, p. 10). This simple form of authentication is still used because it can be effective if implemented properly and it is certainly affordable to any organization. Researchers have been engineering alternatives to text passwords such as graphical processes however conventional password authentication will be around for the foreseeable future (Blocki & Sridhar, 2016, p. 167).

KeePass Password Manager Features

There are many features that are common to password managers which assist users in managing security while improving usability. The KeePass password manager provides some valuable features as an OSI Certified Open Source Software (KeePass, 2017).

Password Generator. The password generator is the recommended method of generating random passwords while using the KeePass password manager (KeePass, 2017). The user has the ability to access the password generator from the menu bar and selecting Tools > Generate Password.

This option allows the user to create a user profile with preset attributes such as character set requirements or a design pattern. The character sets that can be selected to generate the passwords include upper case, lower case, digits, minus sign, underline, spaces, special characters and brackets (KeePass, 2017). These characters can be used in any combination creating a password length that would meet any logical scenario. An example of the Password Generator dialog can be viewed in Fig 1.



Profile: (Custom)

Current settings

● Generate using character set:

Length of generated password: 20

☑ Upper-case (A, B, C, ...)

☑ Lower-case (a, b, c, ...)

☑ Digits (0, 1, 2, ...)

□ Minus (-)

□ Underline (_)

□ Space ( )

□ Special (!, $, %, &, ...)

□ Brackets ([,], {, }, (,), <, >)

□ High ANSI characters

Also include the following characters:

○ Generate using pattern:

□ Randomly permute characters of password

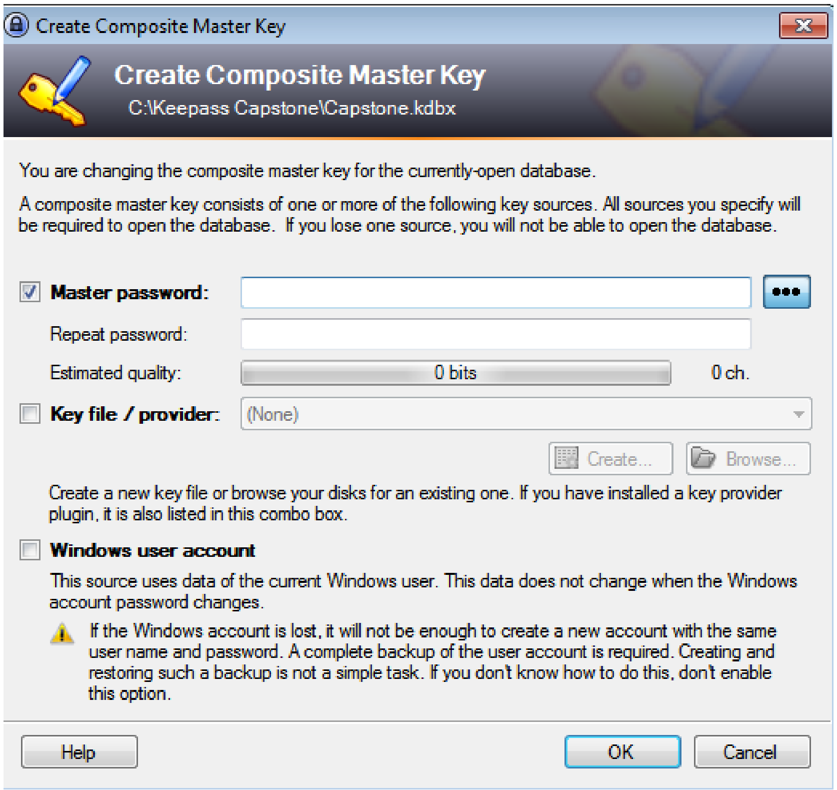
○ Generate using custom algorithm:

(None)

□ Collect additional entropy

Figure 1. This screenshot depicts the Password Generator dialog box for KeePass.

Change Master Key. The user is able to change the Master Key password at any time by using the main menu bar and selecting File > Change Master Key which brings up a dialog box for completing the process.



Create Composite Master Key
Create Composite Master Key
C:\Keepass Capstone\Capstone.kdbx

You are changing the composite master key for the currently-open database.

A composite master key consists of one or more of the following key sources. All sources you specify will be required to open the database. If you lose one source, you will not be able to open the database.

☑ **Master password:**

Repeat password:

Estimated quality: 0 bits 0 ch.

□ **Key file / provider:** (None)

Create a new key file or browse your disks for an existing one. If you have installed a key provider plugin, it is also listed in this combo box.

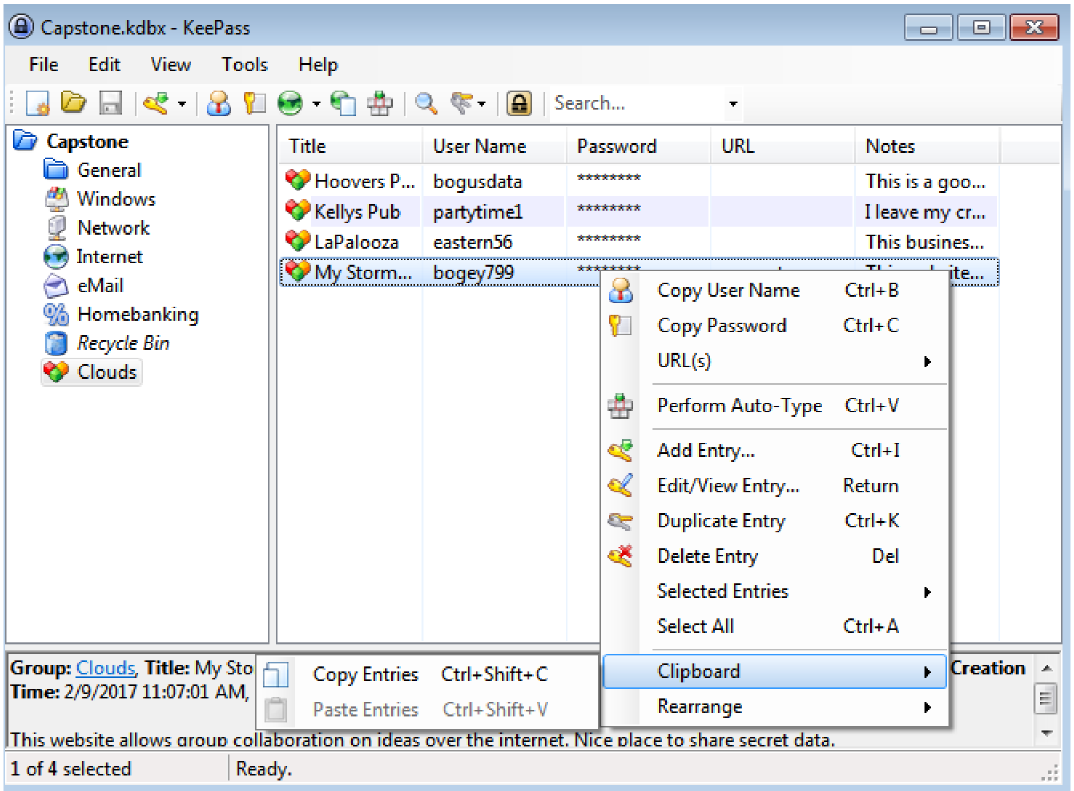
□ **Windows user account**

This source uses data of the current Windows user. This data does not change when the Windows account password changes.

⚠ If the Windows account is lost, it will not be enough to create a new account with the same user name and password. A complete backup of the user account is required. Creating and restoring such a backup is not a simple task. If you don't know how to do this, don't enable this option.

Figure 2. This screenshot depicts the Create Composite Master Key dialog box which is used to change the Master Key password and add a secret Key File or Windows User Account for extra levels of authentication protection.

Copy to Clipboard. When a user wants to copy data or a password to place in another database it can be copied to the clipboard. The user highlights the attribute that needs to be copied then Right Click > Clipboard > Copy Entries and the data base information can be placed in an alternate location.



Title	User Name	Password	URL	Notes
Hoovers P...	bogusdata	********		This is a goo...
Kellys Pub	partytime1	********		I leave my cr...
LaPalooza	eastern56	********		This busines...
My Storm...	bogey799	********		ite...

Group: Clouds, **Title:** My Sto **Creation**
Time: 2/9/2017 11:07:01 AM,

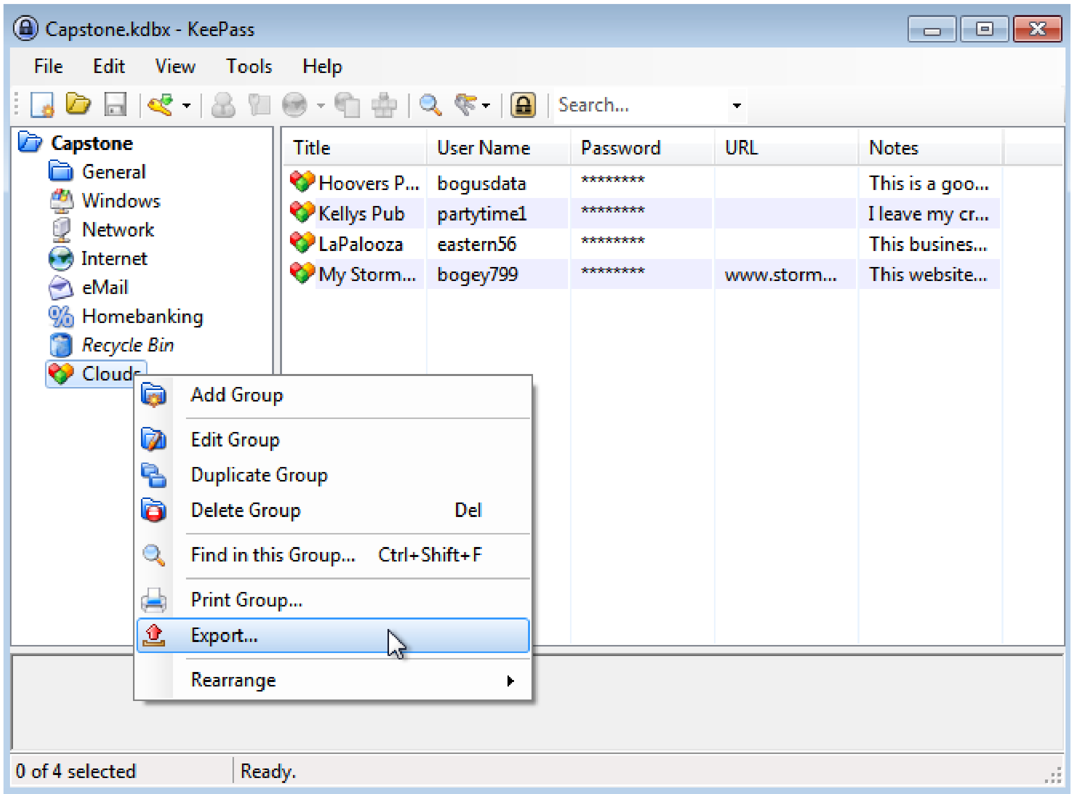
This website allows group collaboration on ideas over the internet. Nice place to share secret data.

1 of 4 selected Ready.

Figure 3. This screenshot depicts a database entity named My Stormboard that is highlighted and a Right Click menu provides the Clipboard > Copy Entries command.

Perform Auto-Type. The Auto-Type feature allows pre-configured data to be automatically entered into web forms. The previous screenshot displays a menu that has two additional options, one is URL(s) which brings up the web page and a command labeled “Perform Auto-Type” which types the pre-established form data into the field.

Export Data. The Export Data feature allows the contents of any database in the KeePass password manager to be exported to CSV, HTML, KeePass 2.x (KDBX) and KeePass 2.x XML file types. This feature is for an entire database and not just a single entry within the database.



Title	User Name	Password	URL	Notes
Hoovers P...	bogusdata	********		This is a goo...
Kellys Pub	partytime1	********		I leave my cr...
LaPalooza	eastern56	********		This busines...
My Storm...	bogey799	********	www.storm...	This website...

Figure 4. This screenshot depicts the Clouds database (KeePass) which was created for this project. Right Click menu dialog box presents the Export function.

Delete Database. Once a database is no longer needed it can be deleted from the KeePass password manager. The menu from the previous screenshot contains an option named "Delete Group". When this is executed it will delete the highlighted database in the left pane and all of its associated attributes.

The above listed features are commonly utilized and are applicable to this project test. There are many more features that can be utilized in KeePass and can be viewed as screenshots in Appendix C or on the KeePass website (KeePass, 2017).

Password Safe Features

As mentioned previously there are many features common to password managers which assist users in maintaining security while improving usability. The Password Safe password manager also provides valuable features as an OSI Certified Open Source Software product (Schneier, 2016). Among the many features that Password Safe offers include login with a master key, random password generation, auto-type form data, copy to clipboard, copy/paste export a database and delete the database. Two unique security features of Password Safe is the requirement to enter the master key prior to exporting data from the system and no print option available for the database. Screenshots of various Password Safe features are in Appendix D.

Importance of Password Configuration

There have been decades of research dedicated to the development of alternatives for using a password as an access control. The familiarity of using passwords, easy implementation and affordability are barriers to utilizing other access control systems. Creating secure passwords is essential in a secure network solution and equally important is that the passwords are changed at regular intervals. Passwords have long been the security hole on networks most often due to the fact that they did not meet a specific complexity level and were easily guessed. To help plug this hole there are some password security guidelines that can be followed. Common password security guidelines include:

- *Minimum length of password* – this sets the minimum number of characters in a password. The minimum number of characters is eight but the longer the better. Best practice suggests combining words together so the password becomes more of a passphrase (Harwood, 2011, p.157).

- *Password duration* – this establishes how long the password or passphrase can be used on the network. This can vary from 1 month to several months depending on the network administration policy.
- *Password reuse* – this option prohibits the use of the same password more than once. This requires that a new password or passphrase be created in accordance with the time frame established by the network administration policy (Harwood, 2011, p.157).

Maintaining the complexity of a password along with the ability to change it frequently are critical processes to any information security program. The reason for that is the presence of scalable computing hardware and password cracking programs available on the internet. The dilemma for the computer user is that the number of passwords they require between work and home is increasing. Job requirements and time constraints can lead to employees developing bad habits such as writing passwords down on paper or in notepads. There was some interesting research accomplished at Carnegie Mellon University in the area of password security.

Dr. Lorrie Cranor, Professor of Computer Engineering and Public Policy at Carnegie Mellon University conducted research on password security (Hu, 2015, p. 1). Professor Cranor indicated that research on password security has always been difficult since people are taught to not disclose their password. To solve this issue a repository of current and expired passwords were approved to be used in a black box (secret) computer system that would never be human readable. In addition, surveys were conducted where people were asked to submit what they would consider to be secure passwords that consisted of eight or sixteen characters. Professor Cranor advised that she was looking for a balance between password security and usability. The research conducted by Dr. Cranor suggests that an efficient balance in password development include passwords that are 12 characters long, at least two character classes with special characters in the middle of the password (Hu, 2015, p. 1).

The balance between creating secure passwords and users having the ability to remember the passwords is not an easy task. A key component of password security is to make them more computationally expensive so they cannot be easily guessed by password cracking software. The new capabilities of graphical processing units (GPU) and modern password cracking software can assist hackers in guessing passwords 10^{14} times within a 3 day period. (Ur et al, 2015, p.463). Securing passwords so they cannot be easily guessed helps to improve access control but complicates the issue of usability. This suggests that the use of a password manager like KeePass or Password Safe may be beneficial to users so their password choices can be complex, random, secure and organized. It also emphasizes the importance of testing the password manager software to assure that the goals of the IT Security team are being consistently met and that the password manager does not become a single point of failure.

Previous Password Manager Evaluations

Password manager software systems can be classified by the environment in which they are executed whether it is from a web browser, a remote cloud server or a local machine. Google Chrome, Firefox, Internet Explorer, Safari and Opera all offer browser based password management with limited functionality (Gray, Franqueira & Yu, 2016, p. 3). Cloud based password managers that are popular include LastPass and 1Password but there are many more that can be found with a simple web search for best password managers for 2017. An important consideration when using browser or cloud based password managers is that there are assurances that they are free of common web application vulnerabilities (Zhao & Yue, 2013, p. 335).

The password management software that is executed from a local machine includes those password managers like Roboform, Password Safe and KeePass. The most recent study available was based on the forensic evaluation of these three local password managers and how they compared from a security perspective (Gray, Franqueira & Yu, 2016, p. 8). The scope of this project is limited to the KeePass and Password Safe systems since they are locally installed systems that are open source and free. Roboform can also be a cloud based product.

The (Gray, Franqueira & Yu, 2016) study advised that all of their testing was conducted utilizing local machines within VMWare Workstation 9 virtual machines configured with Windows 7, 60 GB hard disk and 1 Gigabyte of RAM. The study indicated that the forensic tool of choice was EnCase (no version mentioned) and that several vulnerabilities were noted in the KeePass version 2.28. The first issue included the appearance of the Master Key in plain text that had been stored within the pagefile.sys when data was transferred due to low physical memory availability. However this could not be confirmed since the virtual machine environment was only configured with 1 Gigabyte of RAM.

Another vulnerability identified in the study concluded that exporting the database in HTML format made it viewable in Google Chrome and Internet Explorer (Gray, Franqueira & Yu, 2016, p. 7). When the user saved the exported database to a flash drive then deleted the database which seems like a logical sequence of events, EnCase detected the deleted database in the Recycle Bin. There was some confusion in the study as it pertains to printing the database and having it appear in plain text within a Temp file. The print process may have to be unsuccessful or interrupted for the database file to appear in a Temp file.

Some important software patches for the KeePass 2.28 password manager have occurred since the (Gray, Franqueira & Yu, 2016) study. Improvements and new features are documented in versions 2.34 and 2.35 (Reichl, 2016, p. 1). The list of software changes include:

1. Added support for opening entry URLs with Firefox/Opera in Private Mode.
2. When closing a database, KeePass now searches and deletes any temporary files that may have been created and forgotten by MSHTML when printing failed. (Noted this problem in Gray Study).
3. ChaCha20 – is the new encryption algorithm for database files and as a fallback process memory encryption with a 256 bit key and a 96 bit Nonce.
4. The new KDBX 4file (not default) type has the inner random stream cipher ID and Key that support process memory protection now stored in the inner header.
5. Argon2 (only works if KDBX 4 file type is selected) can be used as a *Password Hashing option* in the "Security" tab of the Database Settings Dialog box. (Strong protection against GPU/ASIC Dictionary Attack)
6. Improved header and data authentication in KDBX 4 files by (HMAC-SHA-256, Encrypt –then MAC scheme).

The implications of these software patches are significant for two reasons; the first is that the change was accomplished through an open source software project that occurred quite rapidly and second is that forensic analysis of KeePass version 2.35 may not replicate the same vulnerabilities that were present in version 2.28 just a few months ago.

Another password manager product evaluated in the previous study was Password Safe version 3.35.1 (Gray, Franqueira & Yu, 2016, p. 1). This version when tested had a tendency to disclose sensitive information in the pagefile.sys if the data had been copied to the clipboard and the machine experienced a hard shutdown that was imitated by suspending the virtual machine (Gray, Franqueira & Yu, 2016, p. 8). This vulnerability was discovered utilizing a keyword search during the forensic examination of the Password Safe product with EnCase.

This project will expand the investigation beyond the local hard drive to include digital artifacts that may appear through forensic analysis of memory while the synchronized database is executed from a Dropbox server. Additionally, it will be running tests with variable memory resources and the most updated version of KeePass 2.35 released on January 9, 2017 and Password Safe 3.41.0 released on November 26, 2016.

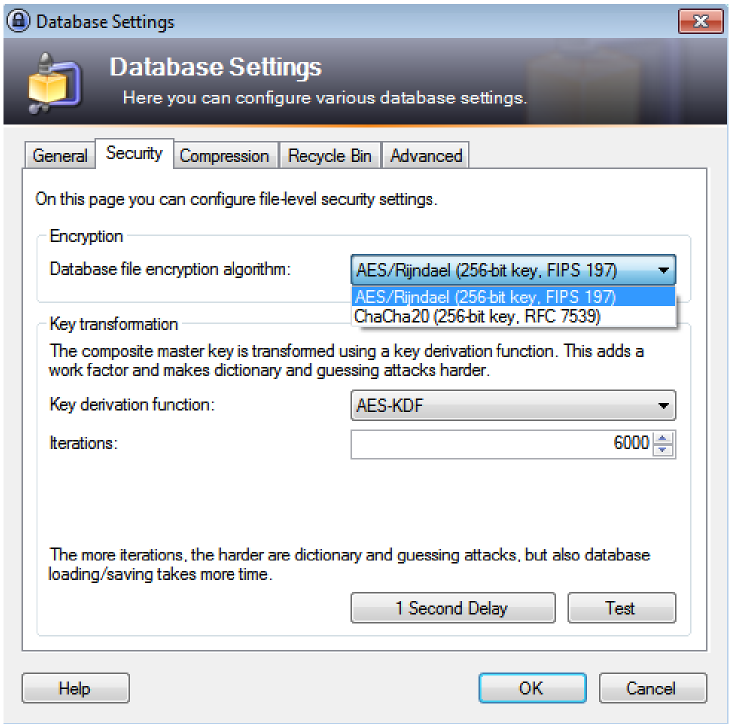
KeePass Encryption Algorithms

The encryption algorithm is responsible for maintaining the secrecy of a Master Key and the data stored within the KeePass password manager. The National Institute of Standards and Technology (NIST) announced in 2001 that the Federal Information Processing Standard (FIPS-197) directed the use of a new Advanced Encryption Standard (AES) as the latest cryptographic algorithm for securing communications (Stewart, Chapple & Gibson, 2012, p. 391). The AES cipher is a symmetric encryption algorithm which allows the use of three key strengths in the form of 128 bits, 192 bits and 256 bits with 128 bit blocks of data. When Daemen and Rijmen exceeded the 128 bit block size limit for the AES so that it could equal the key length, the algorithm became known as AES/Rijndael (Stewart, Chapple & Gibson, 2012, p. 391).

The Advanced Encryption Standard (AES) is constructed with two basic design principles in mind, *confusion* and *diffusion*. Where confusion denotes a lack of information concerning the dependence of a key on the plain text and ciphertext; and diffusion is meant to frustrate statistical analysis through a quantitative spreading of information so that simple structures in plain text and simple structures in the cipher do not have a statistical dependence (Hellekalek & Wegenkitti, 2003, p. 324). Another symmetric key encryption algorithm is a stream cipher utilized by the KeePass password manager named ChaCha20.

In 2004 ECRYPT, the European Network of Excellence in Cryptology requested proposals for the development of Stream Ciphers under Project eSTREAMS. The idea was to create a platform for the development of stream ciphers that could find universal applicability to software systems with high throughput requirements and hardware applications with restricted resources (Sobti & Ganesan, 2016, p.1). The eSTREAM initiative produced several stream ciphers but two that are applicable to the KeePass password manager are Salsa20 discovered in 2004 and updated version ChaCha20 that was adopted in 2008.

The popular TwoFish block chain algorithm was used in KeePass 1.x versions while KeePass 2.x versions utilize the Modified ChaCha Core (MCC) in ChaCha20 which is able to change parameter values for better data diffusion (Sobti & Ganesan, 2016, p.1). ChaCha20 is a stream cipher that involves an encryption method where encryption and decryption occurs one symbol (character or bit) at a time (Sobti & Ganesan, 2016, p.1). The mathematics and technology that make up the latest ChaCha20 cipher stream is beyond the scope of this project but highlights the fact that it is offered as an option in the latest versions of the KeePass password manager.



Database Settings

Here you can configure various database settings.

On this page you can configure file-level security settings.

Encryption

Database file encryption algorithm: AES/Rijndael (256-bit key, FIPS 197)

AES/Rijndael (256-bit key, FIPS 197)
ChaCha20 (256-bit key, RFC 7539)

Key transformation

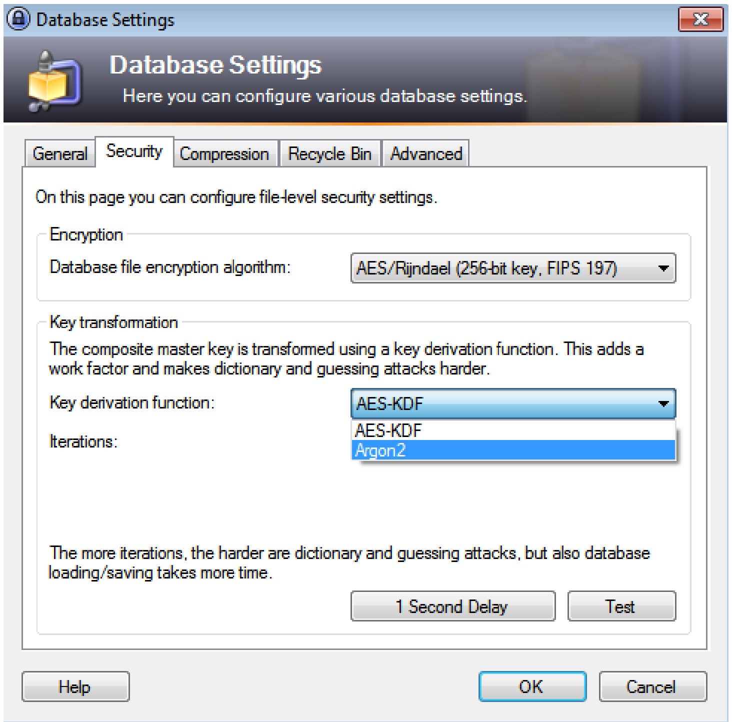
The composite master key is transformed using a key derivation function. This adds a work factor and makes dictionary and guessing attacks harder.

Key derivation function: AES-KDF

Iterations: 6000

The more iterations, the harder are dictionary and guessing attacks, but also database loading/saving takes more time.

Figure 5. This screenshot highlights the database encryption options for KeePass version 2.35 with the default of AES/Rijndael (256-bit key FIPS 197).



Database Settings

Here you can configure various database settings.

On this page you can configure file-level security settings.

Encryption

Database file encryption algorithm: AES/Rijndael (256-bit key, FIPS 197)

Key transformation

The composite master key is transformed using a key derivation function. This adds a work factor and makes dictionary and guessing attacks harder.

Key derivation function: AES-KDF

AES-KDF
Argon2

Iterations:

The more iterations, the harder are dictionary and guessing attacks, but also database loading/saving takes more time.

Figure 6. This screenshot highlights the Key Derivation Function encryption options for KeePass 2.35 with the default of AES-KDF or Argon 2 with a KDBX 4 file structure.

The data authentication encryption methodology utilized by the KeePass password manager is SHA-256-MAC-then Encrypt for version 2.x and the HMAC-SHA-256 hash of the ciphertext (Encrypt-then-MAC scheme) is available as an option in version 2.35 (Reichl,2016, p.1). The Hashed Message Authentication Code (HMAC) algorithm implements a partial digital signature that guarantees the integrity of the message during transmission based on a shared secret key (Stewart, Chapple & Gibson, 2012, p. 414).

The purpose of the HMAC is to *authenticate* the source of the message and its *integrity* by attaching a Message Authentication Code (MAC) to the message which is generated by distinct parameters that include the message input, the secret key and HMACs SHA-256 hash function (Michail, Athanasiou, Kelefouras, Theodoridis & Goutis, 2012, p.5). The Encrypt-then-MAC scheme describes how the input data is processed by encryption first and then the creation of the message authentication code. This scheme of authentication is thought to be more resistant to Denial of Service attacks as compared to an Authenticate-then-Encrypt operation (Maurer &Tackman, 2010, p. 507). The main purpose of the MAC can be regarded as" transforming an insecure channel into an authenticated channel and encryption then corresponds to transforming an authenticated channel into a fully secure channel; this is the well known Encrypt-then Authenticate paradigm" (Maurer &Tackman, 2010, p. 505).

Password Safe Encryption Algorithm

The Password Safe system utilizes the TwoFish encryption algorithm which was one of the original finalists in the Advanced Encryption Standard (AES) program of 1997 (Schneier, Kelsey, Whiting, Wagner, Hall & Ferguson, 1998, p. 3). The TwoFish algorithm utilized by Password Safe was designed to incorporate the AES requirements such as a 128 bit symmetric block cipher, key lengths of 128 bit, 192 bit and 256 bits with no weak keys. A unique characteristic of the TwoFish algorithm was a whitening process that involved the XORing of key material before the first round of encryption and then again after the last round (Schneier, et al, 1997, p. 5). Exclusive OR (XOR) is a logical function commonly used in cryptographic applications that returns a true value when only one of the input values is true.

Prewhitening. This process involves the XORing of plain text with a separate sub-key before the first round of encryption (Stewart, et al, 2012, p. 392).

Postwhitening. The postwhitening involves the XORing of plain text with a separate sub-key after the 16th round of encryption (Stewart, et al, 2012, p. 392).

Table 1

Summary of Encryption Algorithms

Password Manager	Algorithm	Key Size	Standard/ Ref.	Key Derivation Function
KeePass Version 1.x	Advanced Encryption Standard (AES/Rijndael)	256 bits	NIST/FIPS 197	AES-KDF
	TwoFish	128 bits - 256bits		

KeePass Version 2.x	Advanced Encryption Standard (AES/Rijndael)	256 bits	NIST/FIPS 197	AES-KDF
	ChaCha20	256 bits	RFC 7539	
	Data Authentication		SHA-256- MAC-then-Encrypt	
KeePass Version 2.35 (Latest Version)	Advanced Encryption Standard (AES/Rijndael)	256 bits	NIST/FIPS 197	AES-KDF (***Optional*** **Argon2** with KDBX 4 File Type)
	ChaCha20	256 bits	RFC 7539	
	Data Authentication		HMAC-SHA256-Encrypt –then-MAC	
Password Safe Version 3.41	TwoFish	128 bits, 192 bits or 256bits	NIST/FIPS 197	

Screenshots of the database encryption algorithms utilized for KeePass and Password Safe are displayed in Table 1. KeePass version 2.35 uses the AES\Rijndael algorithm while Password Safe 3.41 utilizes TwoFish.

Guidelines for Digital Forensic Analysis

Some example guidelines for digital forensic investigations can be found in the National Institute of Standards and Technology (NIST), specifically in documents such as SP 800-86 titled Guide to Integrating Forensic Techniques into Incident Response. Some agencies set up their own guidelines such as the American Chief of Police Officers:

1. Principle One – Don't cause anything to alter data during tests
2. Principle Two – Accessing the original data at any time must be documented
3. Principle Three – Audit trails must be available to third party requests
4. Principle Four – The case officer in charge is responsible for all applicable laws and assures these principles are followed (Gogolin, 2013, p. 15).

The NIST SP 800-86 provides general guidance toward establishing acceptable procedures for conducting digital forensic investigations. The guide breaks the investigative process down into four categories that include collection, examination, analysis and reporting (Kent, Chevalier, Grance & Dang, 2006, p. 9).

Collection. The collection of relevant digital data involves identifying, labeling, recording and acquiring the data while following established professional guidelines that will assure the integrity of the collections are maintained throughout the process.

Examination. This process requires the forensically processing of collected data using a combination of automated and manual methods to extract specific items of interest while maintaining the integrity of the data samples throughout the examination process.

Analysis. The analysis of resulting data must have been accomplished in accordance to acceptable legal methods at all phases of the investigation with the goal of obtaining useful information that will help answer the original questions that were the motivating force behind the investigation.

Reporting. Completing the final reports should provide detailed descriptions of results of the analysis that describe actions used, tools that were implemented, procedures that were selected and what may still need to be accomplished to improve on those actions, tools and procedures.

The NIST SP 800-86 provides a unique perspective on the evidence collection, examination, analysis and reporting categories as they are applied to the transformation of digital media, to data, information and finally the evidence.

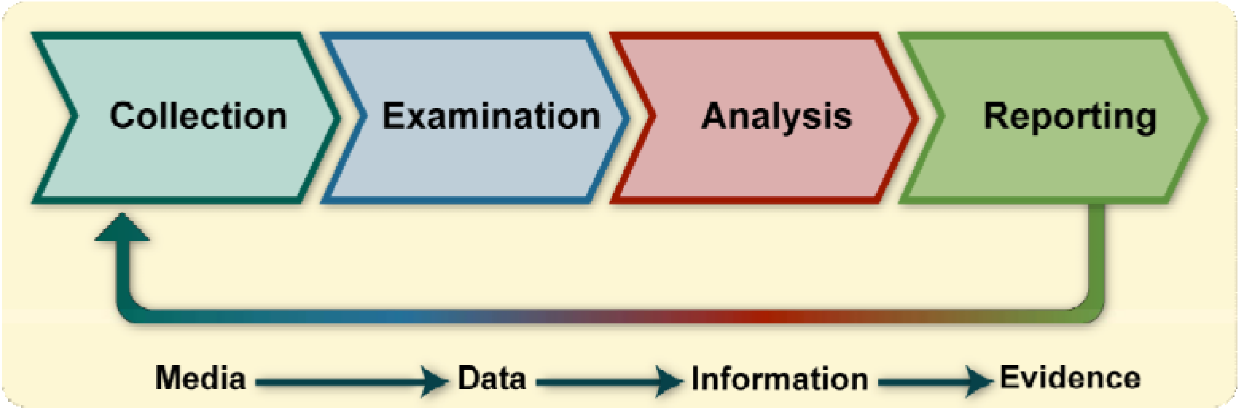


Figure 7. This screenshot was obtained from NIST SP 800-86, p. 5. It depicts a graphic representation of the relationship between digital media and how after the application of scientific methodology the data is transformed into evidence.

Virtual Machines as Forensic Tools

Conducting a forensic examination on a virtual machine follows the same scientific processes as that of a hard disk as long as the virtual machine is exported into an acceptable forensic file format (Shavers, 2008, p. 26). FTK Imager and EnCase are tools especially useful in this process since they can readily accept the VMWare .vmdk file format for a specific virtual machine and create a forensic disk image of that virtual machine (Shavers, 2008, p. 26). The disk image created by FTK Imager can then be saved as a forensic file format such as dd, Encase .E01 or a Smart image imported as evidence files into Encase and FTK.

This project will be using the Snapshot feature of VMWare that creates an additional file with the extension .vmem. The .vmem file that is created will capture the state of the machine at that point in time including data in live memory and it is stored in the directory on the host with all of the other files for that specific virtual machine. This allows the Snapshots (.vmem) files to be imaged (write blocker utilized) with the rest of the hard disk in an unaltered forensically sound state (Hirwani, Pan, Stackpole & Johnson, 2012, p.4).

Chapter 3 – Methodology

Introduction

The scientific methodology of how this experimental project was conducted is described in this section. The object of this investigation is not to conduct a penetration test on the password manager software but to record expected and unexpected outputs that may occur during routine use of the system. These outputs can be utilized to assess the trustworthiness of the KeePass and Password Safe password managers in reference to their ability to maintain confidentiality, data integrity and a reduced digital footprint.

To maintain the integrity of this study it was important to establish guidelines as they pertain to scientific process that helped to answer research questions, formulate multiple hypotheses and verify the findings (Gogolin, 2013, p. 2). "The beauty of systems research is that while there may be many "wrong" answers there can also be multiple "right" answers (Mahajan, 2010, p. 62). The remaining portion of this chapter is dedicated to describing the methodology, design of the study, design description, technical review and design requirements.

Description of Methodology

This project is a causal study and experiment designed to determine whether one or more independent variables (random access memory and database location) can affect the output that will be measured by the presence of a dependent variable (digital forensic artifacts) in the form of identifiable secret data. A methodology was developed through a systematic process of building a research system that included picking the topic domain carefully, being familiar with the underlying problem, articulating a central idea, minimizing complexity and identifying some real world impact (Mahajan, 2010, p. 61). The outputs from this project will be the result of

Black Box testing. A definition of Black Box testing was obtained from (Stewart, Chapple & Gibson, 2012, p. 315).

Black Box Testing. Black Box testing examines the program from a user perspective by providing a wide variety of input scenarios and inspecting the output. Black Box testers do not have access to the internal code.

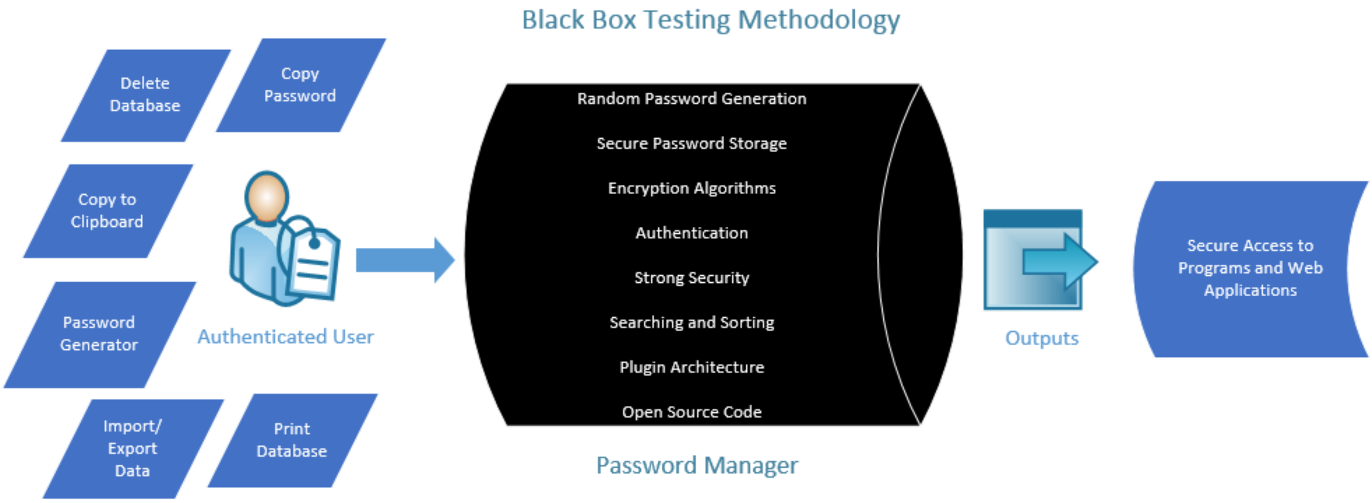


Figure 8. This is a representation of the Black Box testing methodology that depicts user inputs in the password manager, data processed by the software and outputs assumed to be in the form of secure access to programs and web applications.

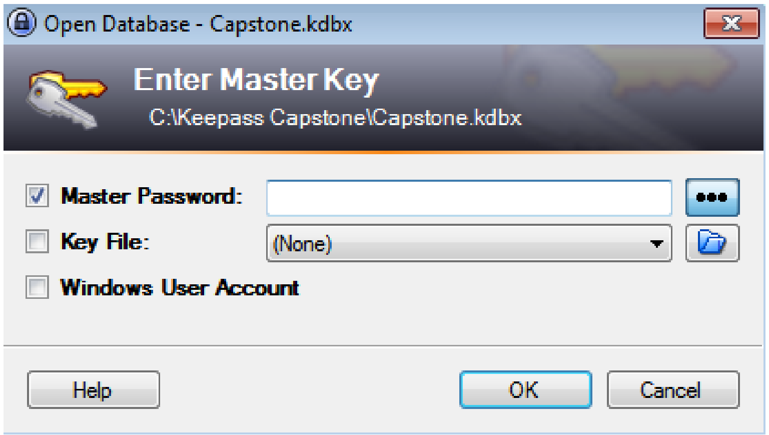
The scientific process of this study includes the utilization of VMWare Workstation 12 to facilitate the creation of eight virtual machines that are configured according to the memory, location of execution and password database requirements. Please see the virtual machine architectural diagram and user initiated (Trial Event) flowchart listed as Figure 25 and Figure 26 in Appendix A. This project was designed so each test could be run in its own virtual environment. This is in accordance to specific parameters and user initiated events that help create digital artifacts. The hope is that by creating virtual machines with intentionally low

RAM memory capacity (1Gig) and adequate RAM memory capacity (4 Gig); that it may provide insight into some relationship of the quality of service from the KeePass and Password Safe password managers as user initiated testing events occur during variable memory resource allocation.

A successful measured outcome for this project would be the discovery of the KeePass and Password Safe Master Key or underlying protected credentials in a readable format within the examined digital artifacts.

Describing the scientific methodology in a stepwise fashion would include:

1. Start the Host Machine running the virtual machines
2. Check for current software updates and patches to the Host Machine
3. Execute the VMWare Workstation 12 virtual machine test environment
4. Each virtual machine is named in the format VM1-IE-1G-local which identifies VM1 = VM number, IE = KeePass, 1G = 1 Gig of RAM and local = password database is located on the local machine. Other options include PS = Password Safe, 4G = 4 Gig of RAM and cloud = database is located on Dropbox. See Fig. 25, the VM Architectural Diagram in Appendix A.
5. Start a virtual machine that is appropriate for the test (VM1 –VM8).
6. Log into the Windows 7 instance for that virtual machine.
7. Click on the KeePass/Password Safe icon located on the Taskbar or as a Desktop Shortcut. This will present the password manager login screen that requests the user to enter the secret Master Key.



Open Database - Capstone.kdbx

Enter Master Key

C:\Keepass Capstone\Capstone.kdbx

☑ Master Password:

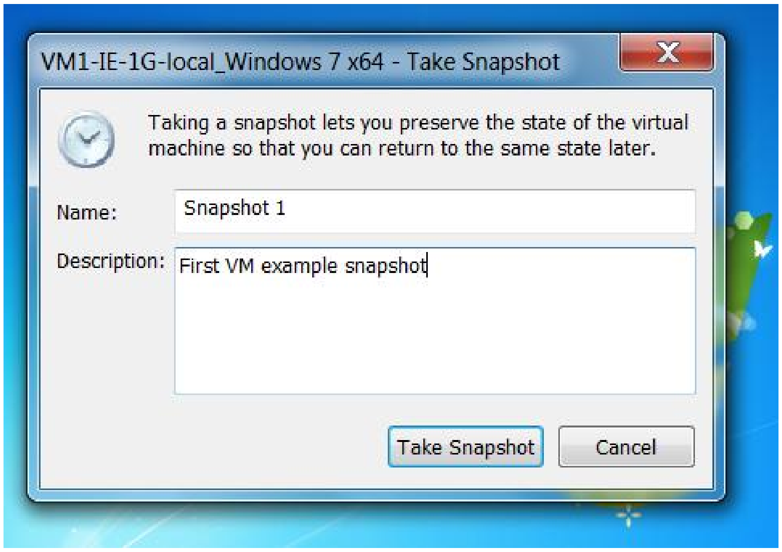
□ Key File: (None)

□ Windows User Account

Figure 9. This screenshot displays the KeePass Master Key login screen that enables access to the password manager and all of the accounts and notes located there.

8. Enter the Master Key password (Authentication). A secret key file (placed on a flash drive) and the Windows User Account can also be added to the authentication process.
9. Take a Snapshot with the VMWare Snapshot Manager to record the machine state and document when the Master Key was entered into the Login screen.

VMWare Snapshot Manager. VMWare has the capability to take a snapshot at any point while the virtual machine is running. The Snapshot is then captured by the Snapshot Manager and appears on disk in the directory that is assigned to that specific virtual machine. The screenshot below (Fig. 10) depicts the dialog box that appears which allows the user to explicitly label the snapshot so that it can be located for further examination. The Snapshot captures the current state of the virtual machine including power state and data states on disk and memory. The Snapshot would appear on disk with a file name in the format of *VM1-IE-1G-local [Snapshot Name].vmem* (VMWare, 2017). The Snapshot Manager also provides a visual representation of all recorded Snapshots in sequence of the actual Trial Event tests. A screen shot of the Snapshot Manager can be viewed as Fig. 28 in Appendix B.



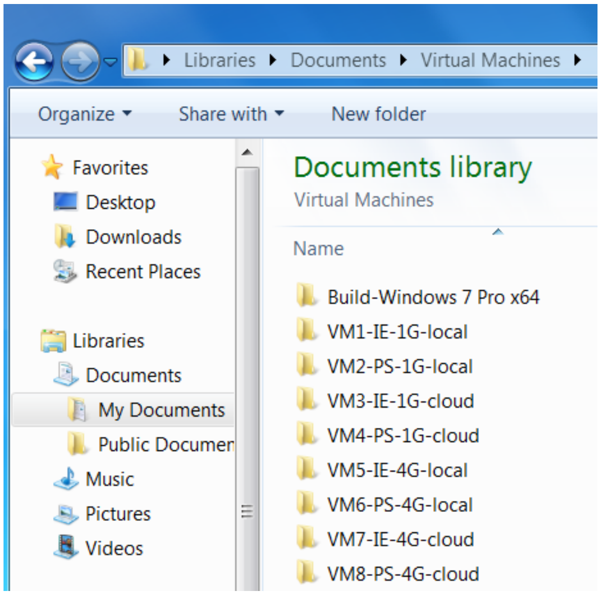
Taking a snapshot lets you preserve the state of the virtual machine so that you can return to the same state later.

Name: Snapshot 1

Description: First VM example snapshot

Figure 10. This screenshot depicts the VMWare Snapshot dialog box that allows you to label each snapshot so that it can be identified later for analysis.

10. Once the Snapshot of the user initiated event has been recorded it will appear in the appropriate virtual machine directory on the Host Machine disk.



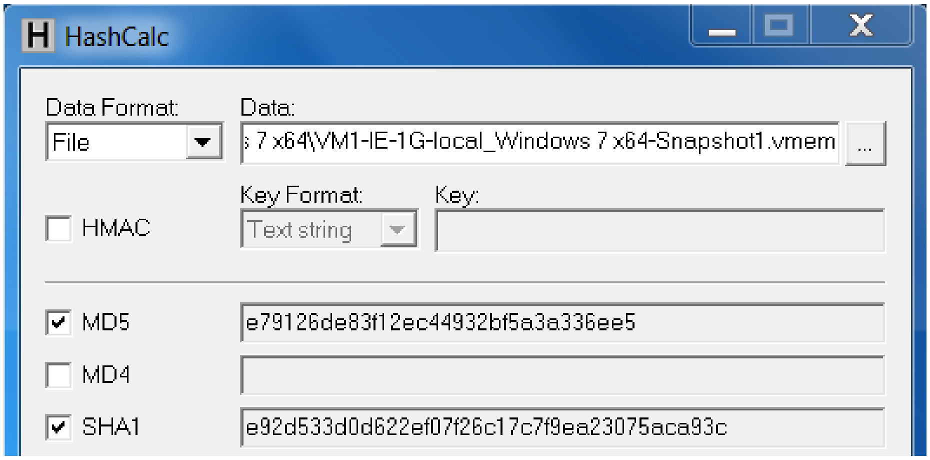
Documents library
Virtual Machines

Name

Build-Windows 7 Pro x64
VM1-IE-1G-local
VM2-PS-1G-local
VM3-IE-1G-cloud
VM4-PS-1G-cloud
VM5-IE-4G-local
VM6-PS-4G-local
VM7-IE-4G-cloud
VM8-PS-4G-cloud

Figure 11. This screenshot depicts the location where a Snapshot can be located within the explicit VM directory that was used to capture the machine state.

11. Locate the Snapshot that will appear in the form VM1-IE-1G-local [Snapshot Name].vmem and run the file in HashCalc to obtain hash values for integrity. HashCalc is a freeware type program that helps to calculate hash values to assure that data has not changed due through the digital processing phases.



Data Format: File

Data: ; 7 x64\VM1-IE-1G-local_Windows 7 x64-Snapshot1.vmem

□ HMAC

Key Format: Text string

Key:

☑ MD5 e79126de83f12ec44932bf5a3a336ee5

□ MD4

☑ SHA1 e92d533d0d622ef07f26c17c7f9ea23075aca93c

Figure 12. This screenshot depicts the Snapshot1.vmem file that was obtained and it was processsed by HashCalc to obtain an MD5 and a SHA1 hash value.

12. Compare the MD5 and SHA1 hash values of the Snapshots to assure data integrity.
13. Once the Snapshot has been properly recorded for this user iniated event which in this first example is the logging in and entering the Master Key. Now close the password manager, restart the Windows 7 instance to clear the memory which is especially important in the 1 Gig RAM configurations to prevent the OS from locking up.
14. Now repeat steps 5-13 for user initiated events (Trial Events) that include:
    a. Authentication with the Master Key (used for previous example)
    b. Password Generator to create a password
    c. Auto-Type credentials in a web form
    d. Copy credentials to the clipboard

   e. Copy and Paste
   f. Export database to several formats
   g. Print database (Not an option for Password Safe)
   h. Delete a database

15. Capture each Snapshot .vmem file created during step # 14 in FTK and Volitility for examination.
16. Run HashCalc on the Snapshot.vmem files to assure that they have not been altered and document it in the hashes spreadsheet.
17. Once all of the user initiated (Trial Events) and data captures from the virtual machine have been accomplished shut down the virtual machine and repeat the process for the remaining virutal machinesVM2 – VM8.
18. When all tests and data captures of the virtual machines have been accomplished then utilize FTK Imager to create a forensic image of each individual VM. This will produce eight forensic images, one for each VM1 – VM8 that can be added as evidence once the hard drive is imaged.
19. Storage of the imaged virtual machines will be on an external USB drive.
20. Shut down the host machine, disconnect the power source and remove the battery.
21. Remove the hard disk from the Host Machine so that it can be imaged with Encase 7 and FTK Imager. Tableau Write Blocker was used during the hard drive imaging process.
22. Analyze the data obtained from each Snapshot.vmem file created by the user initiated event with EnCase, FTK and Volatility memory analysis tools.

23. Analyze the forensic images created by EnCase 7 and FTK Imager which provides a comprehensive investigative environment of both the Windows 7 Operating System and interactivity with the VMWare Virtual Machines.

MD5 Hash. The MD5 Message Digest algorithm produces a 128 bit value that is represented by a 32 digit hexadecimal number. Files that have been hashed have unique values and do not change even if the file extension or file name has been changed. Searching with hash values is very useful in the field of digital forensics. An example MD5 hash value = de9277ffb9be5bc1cbc364ecd7340dab (Gogolin, 2013, p. 53).

SHA1 Hash. The SHA1 is the Secure Hash Algorithm 1 and produces a 160 bit value that is represented by a 40 digit hexadecimal number. SHA1 is commonly used in addition to the MD5 as evidence that a specific file or set of files have retained their integrity. An example SHA1hash value = 9069e8ba02b6a369e7c16c1e31e1064e843e52d6 (Gogolin, 2013, p. 53).

File System. The file system is a collection of data structures that allow an application to perform operations on stored data. Memory forensics attempts to locate file system artifacts that reside in volatile memory, main memory artifacts that you find within the file system and how you combine these sources of data for a more comprehensive analysis.

Design of the Study

A Dell Precision M-4800 mobile engineering workstation designed to work with virtual machine architecture was selected for this project. It includes a SATA 500 GB hard drive, Intel I-7 4610M processor and 16 GB of RAM. The host operating system consists of a fresh install of Windows 7 Pro x64. System Information report written at: 02/13/17 12:22:02 indicates the following system configuration for the Host machine.

Host System Hardware Configuration. System Name: INVESTIGATOR

OS Name - Microsoft Windows 7 Professional, Version - 6.1.7601 Service Pack 1 Build 7601

OS Manufacturer - Microsoft Corporation System Name - INVESTIGATOR

System Manufacturer Dell Inc. System Model Precision M4800

System Type x64-based PC

Processor - Intel(R) Core(TM) i7-4610M CPU @ 3.00GHz, 3001 Mhz, 2Core(s),

4 Logical Processor(s) BIOS Version/Date - Dell Inc. A16, 12/1/2015

Windows Directory C:\Windows System Directory - C:\Windows\system32

Boot Device \Device\HarddiskVolume1 (500 GB SATA)

Locale United States Time Zone - Eastern Standard Time

Hardware Abstraction Layer Version = "6.1.7601.17514"

Installed Physical Memory (RAM) 16.0 GB Total Physical Memory - 15.9 GB

Available Physical Memory 12.9 GB Total Virtual Memory - 31.8 GB

Available Virtual Memory 28.7 GB Page File Space - 15.9 GB

Page File C:\pagefile.sys

Host System Software Configuration. Programs that were added to the host machine include current updates to Windows 7, Microsoft Security Essentials for A/V protection, Microsoft Firewall activation, VMWare Workstation 12, Internet Explorer 11, Mozilla Firefox, Notepad ++ , Python 2.7, Volatility 2.6 and Wireshark network protocol analyzer. Microsoft Office 2013 was also added to assist in reporting processes. Virtual Machines were stored in separate folders to reduce the chance of comingled data.

Virtual Machine Naming Convention. Virtual machines were named in accordance with a strategic naming convention and will describe the virtual machine number, password manager used, memory capacity and database location.

Virtual Machine Number – VM1 – VM8

Password Manager – KeePass (IE) or Password Safe (PS)

Memory Capacity – One Gigabyte (1G), Four Gigabyte (4G)

Database Location – Local Database (local), Cloud Based Dropbox account (cloud).

A base virtual machine was created for the 1Gig of RAM configurations and another for the 4 Gig RAM which then each was cloned for consistency. Each VM include Windows 7 Pro x64 and appears in the format VM1-IE-1G-local. See the Virtual Machine Architecture diagram as Fig. 25 in Appendix A.

Base Windows 7 1G-Build with 1G of RAM. This template was created by:

1. Utilized VMWare Workstation 12 to create a new VM
2. Select “Typical Installation”
3. Select “I will install the OS later”
4. Select OS as Microsoft Windows and Version Windows 7 x64
5. Named the VM “1G-Build-Windows 7 x64”
6. Maximum Disk Size = 60GB
7. Store virtual disk as a single file
8. “Customize hardware” and set this VM to 1024MB= 1GB Processor = 2 Core=2
9. Click on CD/DVD and select radio button for “Use ISO Image”

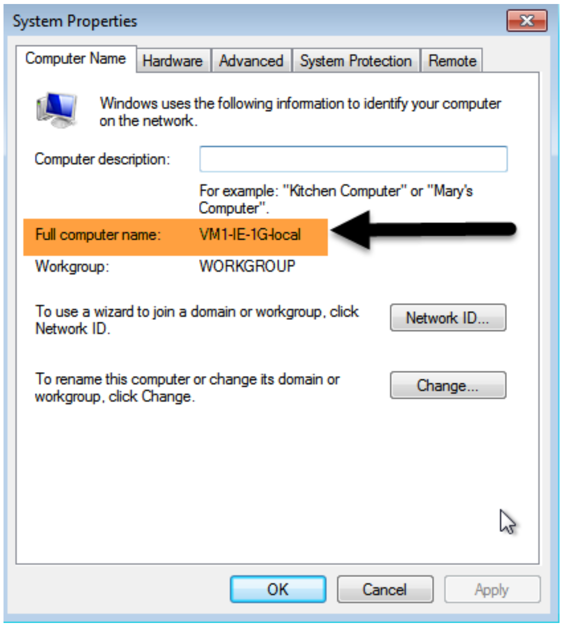
10. OS is from a Windows 7 Pro SP1x64 .iso file (Download Directory)
11. Virtual Machine is stored in C:\Users\Daryl\Documents\Virtual Machines\
12. Username = MISI799 Computer Name = 1G-Build-Windows 7x64
13. Password = P@ssword56
14. Installed IE version 11 for Windows 7 x64 and Microsoft Defaults for Firewall and Microsoft Security Essentials for antivirus protection.

Base Windows 7 4G-Build with 4G of RAM. This template was created by:

1. Utilized VMWare Workstation 12 to create a new VM
2. Select "Typical Installation"
3. Select "I will install the OS later"
4. Select OS as Microsoft Windows and Version Windows 7 x64
5. Named the VM "4G-Build-Windows 7 x64"
6. Maximum Disk Size = 60GB
7. Store virtual disk as a single file
8. "Customize hardware" and set this VM to 4096MB= 4GB Processor = 2 Core=2
9. Click on CD/DVD and select radio button for "Use ISO Image"
10. OS is from a Windows 7 Pro SP1x64 .iso file (Download Directory)
11. Virtual Machine is stored in C:\Users\Daryl\Documents\Virtual Machines\
12. Username = MISI799 Computer Name = 4G-Build-Windows 7 x64
13. Password = P@ssword56
14. Installed IE version 11 for Windows 7 x64 and Microsoft Defaults for Firewall and Microsoft Security Essentials for antivirus protection.

The names of the virtual machines created for this project are: VM1-IE-1G-local, VM2-PS-1G-local, VM3-IE-1G-cloud, VM4-PS-1G-cloud, VM5-IE-4G-local VM6-PS-4G-local, VM7-IE-4G-cloud and VM8-PS-4G-cloud. The Cloning takes about 30 minutes for each of the eight VM's for this project. Each VM was then individually configured in accordance to a specific need for the project based on the original clone.

Once the Cloning of a specific VM is completed, power on the VM and go into the Computer "Properties" Screen. Change the Computer Name so it matches the name of the virtual machine. This will help in tracking data since it will be assigned to a specific virtual machine instance in the project. Then restart the VM to assure that it is working properly and that the new Computer Name has registered.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: VM1-IE-1G-local

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

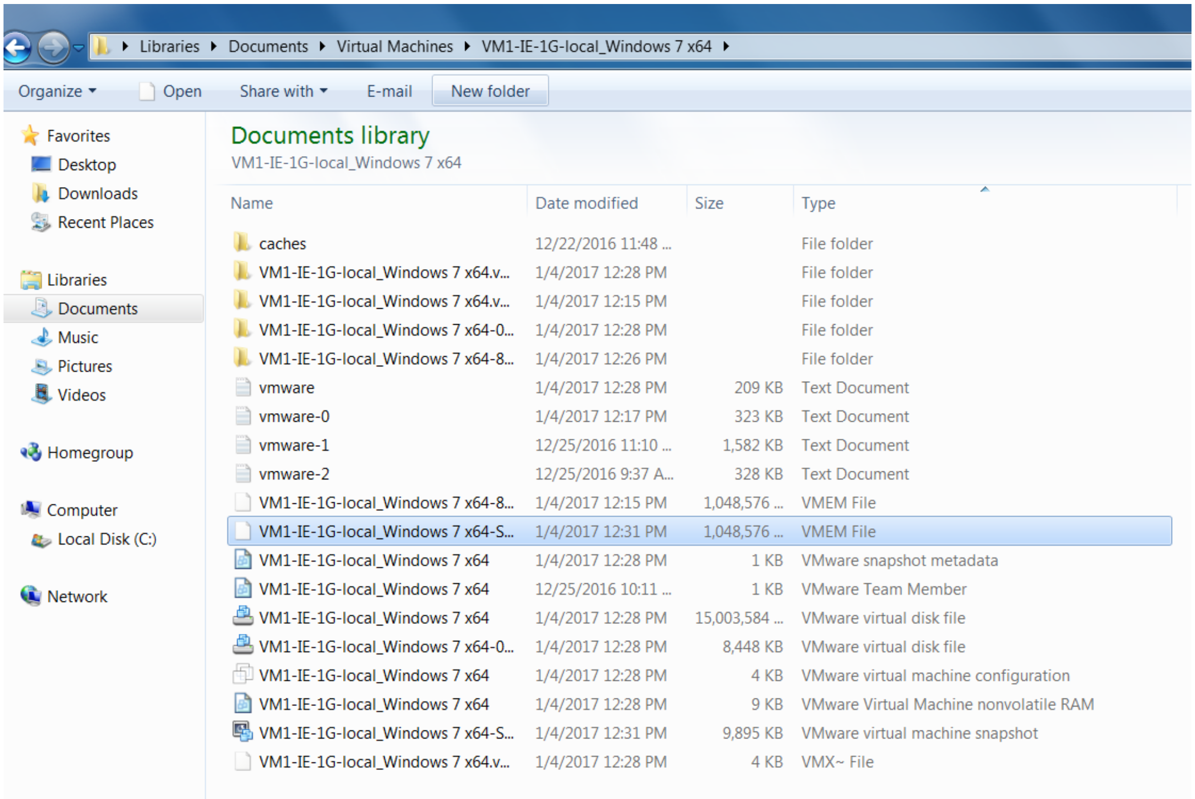
To rename this computer or change its domain or workgroup, click Change.

Figure 13. The Computer Name for each virtual machine was set to match the specific VM.

Once all of the virtual machines were tested for functionality a Restore Point was created on the Host machine to preserve the state in case a problem developed later in the project. If disaster recovery were required during the processing of data; the Restore Point is configured by the Windows 7 operating system and provides a methodology to reset the operating system back to a specific time and date prior to the disaster.

Establish a Baseline for VM file structure. Once the virtual machines were created a baseline was established to document the file types that should occur within each virtual machine prior to any Snapshots taken during the experiment phase of the project. The list below depicts the file structure of the virtual machines and a functional description of the file. These files exist prior to any Snapshots taken during the testing process.

Libraries > Documents > Virtual Machines >
VM1-IE-1G-local
Caches – file folder
Vmware – txt (.log file) [Most recent log file]
Vmware –0- txt (.log file)
Vmware –1- txt (.log file)
Vmware –2- txt (.log file) [Oldest log file]
VM1-IE-1G-local**.vmsd** (Snapshot Metadata)
VM1-IE-1G-local**.vmxf** (VMware Team Member)
VM1-IE-1G-local**.vmdk** (VMware Virtual Disk File)
VM1-IE-1G-local**.vmx** VMware Virtual Machine Configuration)
VM1-IE-1G-local**.nvram** (VMware Virtual Mach. Non-Volatile RAM)



Name	Date modified	Size	Type
caches	12/22/2016 11:48 ...		File folder
VM1-IE-1G-local_Windows 7 x64.v...	1/4/2017 12:28 PM		File folder
VM1-IE-1G-local_Windows 7 x64.v...	1/4/2017 12:15 PM		File folder
VM1-IE-1G-local_Windows 7 x64-0...	1/4/2017 12:28 PM		File folder
VM1-IE-1G-local_Windows 7 x64-8...	1/4/2017 12:26 PM		File folder
vmware	1/4/2017 12:28 PM	209 KB	Text Document
vmware-0	1/4/2017 12:17 PM	323 KB	Text Document
vmware-1	12/25/2016 11:10 ...	1,582 KB	Text Document
vmware-2	12/25/2016 9:37 A...	328 KB	Text Document
VM1-IE-1G-local_Windows 7 x64-8...	1/4/2017 12:15 PM	1,048,576 ...	VMEM File
VM1-IE-1G-local_Windows 7 x64-S...	1/4/2017 12:31 PM	1,048,576 ...	VMEM File
VM1-IE-1G-local_Windows 7 x64	1/4/2017 12:28 PM	1 KB	VMware snapshot metadata
VM1-IE-1G-local_Windows 7 x64	12/25/2016 10:11 ...	1 KB	VMware Team Member
VM1-IE-1G-local_Windows 7 x64	1/4/2017 12:28 PM	15,003,584 ...	VMware virtual disk file
VM1-IE-1G-local_Windows 7 x64-0...	1/4/2017 12:28 PM	8,448 KB	VMware virtual disk file
VM1-IE-1G-local_Windows 7 x64	1/4/2017 12:28 PM	4 KB	VMware virtual machine configuration
VM1-IE-1G-local_Windows 7 x64	1/4/2017 12:28 PM	9 KB	VMware Virtual Machine nonvolatile RAM
VM1-IE-1G-local_Windows 7 x64-S...	1/4/2017 12:31 PM	9,895 KB	VMware virtual machine snapshot
VM1-IE-1G-local_Windows 7 x64.v...	1/4/2017 12:28 PM	4 KB	VMX~ File

Figure 14. This screenshot highlights a .VMEM file that had been created after a Snapshot was taken. Notice that it does not appear in the baseline list of files from the previous page.

Design Description

The design of this experimental project involves the development of scientific conclusions from digital artifacts based on observations of commonly utilized password management features. KeePass version 2.35 and Password Safe 3.41 are the password management software systems that are the subject of this project. Trial Event testing was focused toward those features that would be frequently utilized by a user with the greatest potential for creating digital artifacts. Features such as Authentication with the Master Key, Password Generator to create a password, Auto-Type credentials in a web form, Copy credentials to the clipboard, Copy and Paste data, Export database to csv/html format, Print database and Delete a database are considered to be user initiated (Trial Events) during this project. Each of these events will be captured during Trial Event testing using a VMWare Snapshot that is executed on all of the eight virtual machines that contain fictitious password databases developed for this project.

The VMWare Snapshots that have the .vmem file type will be analyzed with forensic tools and Python Volatility for the presence of the Master Key. Once all of the VMWare Snapshots have been captured then FTK Imager will be utilized to image each of the eight virtual machines so they can be added as evidence to FTK.. The final phase after all of the tests have been accomplished is to obtain a forensic image of the entire Host machine hard drive with FTK Imager. This will allow a complete examination with FTK and EnCase of host activity that may be related to the individual virtual machines containing the test environment.

Framework Design Methodology

The scientific methodology that will be utilized for conducting the experimental trials in this project will follow the Black Box Methodology that was described earlier in Chapter 3. This methodology allows the focus to be directly on user initiated input events so observations can be made and documented of digital artifacts that are the output data points. This will be accomplished without having to interact with the password management software code. Each test will be executed within a specially designed virtual machine that possesses its own computer name and configuration encapsulated by the VMWare 12 Workstation environment.

The virtual machine architectural framework that makes up the operating environment of this project can be viewed as Fig. 25 in Appendix A. The framework consists of eight virtual machines; VM1 – VM4 that were cloned from Windows 7 Pro 64x 1G-Build with 1G of RAM and VM5 – VM8 from Windows 7 Pro 64x 4G-Build with 4G of RAM. Each were built with the default VMWare settings with 60 Gig of hard disk space and configured as a single file. The virtual machines can be used as a forensic operating system as a matter of convenience because they can be easily cloned and a completely new machine re-created if problems develop during the analysis process (Shavers, 2008, p. 15). Virtual machine technology facilitates the integration of software packages within each machine required for testing and yet remain independent of one another. This is especially true since each virtual machine file structure was inspected to assure that it is stored in its own file directory.

Trial Event Framework

The Trial Event Framework in Table 3 provides a detailed description of what user initiated event will be tested and documents:

1. The virtual machine utilized for the test (VM1 –VM-8)
2. The password manager (KeePass 2.35 or Password Safe 3.41)
3. RAM configuration (1G or 4G)
4. Database location (Local machine or Cloud base with Dropbox)
5. VMWare Snapshot Name.vmem assigned to the Trial Event
6. Resources utilized for each Trial Event

Specific Trial Events that will be initiated multiple times in succession to exhaust system resources against each of the eight virtual machines include:

Trial Event #1- ***Authentication with the Master Key***. This will be the first user initiated event to be tested since this security method is responsible for the underlying integrity of stored databases. Authentication with the Master Key can be executed from the local desktop where the database resides or as an alternative from a synchronized Dropbox account. This trial is designed to determine if the Master Key which is assigned the value WX[secretp@assword]YZ for the KeePass virtual machines and AB[n0accesshere]CD for the Password Safe virtual machines can be identified within digital artifacts that are forensically examined.

Trial Event #2 - *Password Generator.* The KeePass and Password Safe Password Generator will be utilized to generate random passwords and the test will be conducted prior to the process being saved and once again after it is saved.

Trial Event #3 - *Auto-Type credentials in a web form.* This trial involves utilizing the KeePass and Password Safe feature that accesses a pre-set URL and then Auto-Types the username and password into a web form.

Trial Event #4 - *Copy data to the clipboard.* The process of copying data to the clipboard will be tested to determine if protected information becomes inadverantly exploited during the process. This is a separate command from the Copy/Paste option on the menu. The data will be in the form of user credentials and also some notes that can be typed within any of the database entries.

Trial Event #5 - *Copy and Paste.* The process of copying data to the clipboard will be tested to determine if protected information becomes inadverantly exploited during the process. This is a separate command from the Copy to Clipboard option on the menu. The data will be in the form of user credentials and also some notes that can be typed within any of the database entries.

Trial Event #6 - *Export database.* This trial event involves exporting a database named "Clouds" in the KeePass configuration and "Bluesky" in the Password Safe. The database will be exported as .csv, html and also as the native file format that is associated with the KeePass and Password Safe password managers.

Trial Event #7 - *Print database*. The "Clouds" database in KeePass will be subjected to the Print command and observations will be made to see if the database is visible during examination of digital artifacts. Password Safe does not allow any print functions.

Trial Event #8 - *Delete a database.* At the conclusion of the previous seven trial events the "Clouds" and "Bluesky" databases will be subjected to a delete process that is not saved and one that is committed. Observations will be made to determine if any portions of the database are recoverable in a readable format during the forensic examination.

Resources for Design Requirements

Table 2

Program Resources Utilized

KeePass ver. 2.35 (Recently patched version)	FTK Imager	EnCase 7
Password Safe (Version 3.41.0)	VMWare Workstation 12 (Creating 8 virtual machines)	FTK6
Volatility 2.6	HashCalc	Python 2.7
Wireshark	Camtasia Studio	Snag It
Dropbox	Microsoft Office, Powerpoint, Project, OneNote and Visio	Internet Explorer 11
Notepad ++	Tableau Write Blocker	Mozilla Firefox

Data Analysis

The success of this project is dependent on the proper forensic processing of digital evidence in accordance with NIST SP 800-86 for the collection, examination, analysis and reporting the results (Kent, Chevalier, Grance, & Dang, 2006, p.16). If the greatest of care is not afforded the digital evidence, it may become altered which makes any subsequent decisions based on that data very questionable. Once the data integrity issue is resolved then the collected data can be organized, reviewed, classified and presented. One affective method to accomplish data analysis is through the recording of events presented in tables that help visualize solutions for the original research questions.

1. Does the Master Key or underlying secured credentials for databases protected by the KeePass and Password Safe software become vulnerable to discovery within digital artifacts on disk when there are low memory resources?
2. Does moving the database from the local machine to a cloud environment such as Dropbox elicit observable differences in the discovery of digital artifacts?
3. Is there recoverable data from memory while using FTK or Volatility when examining VMWare Snapshots?
4. Will KeePass AES/Rijndael and Password Safe Two Fish algorithms perform equally?

All Trial Events will be tested on each of the eight virtual machines (VM1 – VM8) and the results will be documented similar to Table 3 shown on the next page.

Table 3

Trial Events Systematically Executed On Each Virtual Machine

Trial ID	Test Description	Expected Results	Actual Results
Trial Event #1	Authentication with the Master Key will occur on VMs with 1 Gig of RAM and 4 Gig of RAM configurations.	Previous study indicated that when RAM is limited the Master Key can be found in the Windows Page File (pagefile.sys). However that was reportedly fixed in KeePass ver. 2.34.	
Trial Event #2	Password Generator will be used to create complex passwords.	Passwords will remain in an encrypted state throughout all phases of the test.	
Trial Event #3	Perform Auto-Type on form fields to enter login data on local database and from Dropbox.	Passwords will remain in an encrypted state throughout all phases of the test.	
Trial Event #4	Copy data to Clipboard in the form of Notes and Login data.	Expectations are that all of the data within the database will remain encrypted both in memory and on disk.	
Trial Event #5	Copy and Paste operation for login data. It is a different menu item than Copy to Clipboard	Passwords will remain in an encrypted state throughout all phases of the test.	
Trial Event #6	Export database to CSV, HTML and Native KeePass and Password Safe formats.	Previous studies indicated that exports in HTML could be viewed with a web browser and that after deletion it remained in the Recycle Bin.	
Trial Event #7	Print database entries and also disrupt a Print function.	Failed Print operation allowed the database to appear in the Temp Folder in plain text.	

Trial Event **#8**	Delete the database named "Clouds" or "Bluesky" that were created for this project.	Expectations are that all of the data within the database will remain encrypted both in memory and on disk.	

Research question #1 is applicable to all eight virtual machine configurations because VM 1 – VM 4 will allow the Trial Events to be tested in a 1 Gig of RAM environment while VM 5 – VM 8 will operate with 4 Gig of RAM. Previous research suggests that earlier versions of KeePass and Password Safe occasionally allow unencrypted data to become exploitable in the pagefile.sys when operated with reduced memory capacity (Gray, Franqueira & Yu, 2016, p. 7). However, the earlier study occurred while using KeePass version 2.28 and according to the KeePass website should have been addressed and updated in version 2.35 (Reichl, 2016, p.1).

Research question #2 is unique to any studies since it involves the use of KeePass and Password Safe in their native form as a database operated from a local machine. In this project the database in VM-3, VM-4, VM-7 and VM-8 will be executed from a synchronized Dropbox. These specific virtual machines were chosen as the Trial Event testing for the cloud environment where the local database is synchronized from a Dropbox account. In addition, the Trial Events tested on these virtual machines will utilize the network protocol analyzer Wireshark in an attempt to capture network traffic during synchronization of the database between the local machine and Dropbox.

Research question #3 pertains to the forensic analysis of Snapshot data recorded by the VMWare 12 Workstation. The Snapshot data will appear in the results with a specific format such as VM1-IE-1G-local-master_key.vmem. Each of the snapshots will be labeled with a descriptive identifier that is specific to the Trial Event that it is testing. This will assist in the location and identification of the Snapshot data during the analysis phase of the project and in the isolation of the data specific to the appropriate virtual machine utilized during the test.

The host hard disk was imaged in a forensically sound manner utilizing a Tableau Write Blocker to assure data integrity. The Snapshot data was processed with EnCase 7, Python Volatility Memory Analysis Framework and FTK 6 which facilitated keyword searches for strategically named data sets incorporated into each Trial Event.

Research question #4 pertains to the efficiency and effectiveness of each underlying encryption algorithm that secures data within KeePass and Password Safe. Both password managers utilize algorithms that are Advanced Encryption Standard (AES) compliant but have different underlying mechanisms. The mathematics describing the functionality of KeePass that utilizes AES/Rijndael while Password Safe uses TwoFish is beyond the scope of this project.

The consistent application of scientific methodology during this project for each Trial Event used to test KeePass and Password Safe is accomplished in isolated virtual environments which may provide some useful measurement and insight between the two encryption methods.

Chapter 4 – Results

Overview

This section of the paper will provide an overview of the scientific processes utilized to develop the project prototype used for testing the Trial Events. Every attempt was made during the project to protect data and computing processes from being altered as tests were conducted on the various configurations isolated within each virtual machine. Particular attention was directed at preserving the tested states of the virtual machines by protecting power sources with an uninterruptable power supply to assure consistent current flow, frequent data backup routines and following industry standards for collecting and processing digital forensic artifacts.

Establishing Forensic Processing Prototype

The project required a robust host computing environment and obtained a Dell Precision M-4800 mobile engineering workstation designed to work with virtual machine architecture. It included a SATA 500 GB hard drive, Intel I-7 4610M processor and 16 GB of RAM. The operating system is Windows 7 Pro X64 that was a fresh install specific to this project.

Programs that were added to the host machine include current updates to Windows 7 Pro x64, Microsoft Security Essentials for A/V protection, Microsoft Firewall activation, VMWare Workstation 12, Internet Explorer 11, Mozilla Firefox, Notepad ++, Volatility Memory Forensic Framework, Python 2.7 and Wireshark network protocol analyzer. Microsoft Office 2013 was also added to assist in reporting processes.

Once the Trial Events described in chapter 3 were accomplished on each of the specifically configured virtual machines there began the preparation for examining forensic images and memory samples. This process involved preparing the Host Drive for forensic imaging that included:

1. Conducted a graceful shutdown of all programs on the host machine (Dell M-4800)
2. Disconnecting the host machine from the power source.
3. Removed the battery pack on the back of the laptop
4. Utilized anti-static and electro-magnetic discharge precautions
5. Removed screws holding the back plate of the host machine
6. Removed the back plate to access the hard drive carriage
7. Removed the lock bolt securing the hard drive along with hard drive screws
8. Removed the hard drive and place it in an anti-static storage bag
9. Prepared the Tableau T35u Forensic IDE\SATA Bridge Write Blocker by connecting the power, data and USB 3 cables. Confirmed Read Only without Write capability.
10. Utilized an Uninterruptable Power Supply to assure consistent current flow and reduce the chance of a power loss/surge during the imaging process. (APC Battery Backup).
11. Connected the Host Hard Drive to the Tableau device
12. Connected the USB 3 cable from the Tableau T35u to the laptop that would be used to create the HostHardDrive.E01 image.
13. Waited for confirmation from the Windows 7 Pro OS that the Tableau device was identified as the new F:\ and could be accessed by FTK Imager.

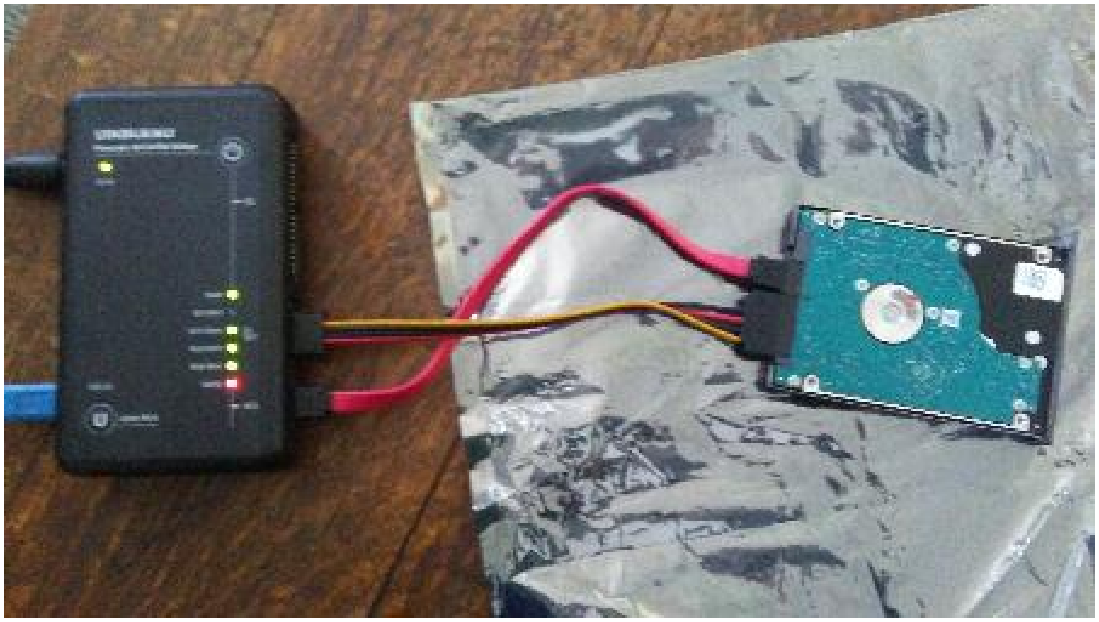


Figure 15. This image shows the T35u Forensic IDE/SATA Bridge Write Blocker attached to the host hard drive while obtaining a forensically sound image. The red cable is for data while the four wire cable is used to supply power to the hard drive.

Prepared FTK Imager to create the hard drive image:

1. Started FTK Imager
2. Selected Create New Image from a Disk Drive
3. Selected Image Source as F:\\Physical Drive 3 (Tableau and SATA Host Drive)
4. Selected the Destination for the stored image as E:\FTK Imager\HostHardDrive\HostHardDrive.E01.
5. Completed the imaging process with MD5 and SHA-1 hash confirmations
6. Image was verified along with an FTK Imager verification and Image Summary

Created a New Case with FTK 6 and add the image as evidence:

1. Click on Cases on the menu bar and then select “New”.

2. Enter the Case Name or Number "MISI799_Capstone_middleton
3. Complete the form fields to help identify the new case
4. Click the Evidence tab on the Menu Bar and Select "Add New Evidence"
5. Select the Destination for the stored image as E:\FTK Imager\HostHardDrive\HostHardDrive.E01.
6. Select the "Refinement Options" button to select additional processing options like .CSV files and deselecting like SHA-256 hashing.
7. When completed, continue and allow FTK 6 to acquire the HostHardDrive.E01 image.
8. This will add HostHardDrive.E01 as an evidence item to the MISI799_Capstone_middleton case within the FTK forensic processing tool.
9. Access to the HostHardDrive.E01 evidence file was successful with FTK 6.

Created a new case in Encase 7 and add the image as evidence:

1. Start EnCase 7
2. Create new case named MISI799_Capstone_2017.
3. Confirm proper NAS and DATA configuration for EnCase Forensic Training mode.
4. Select Evidence > Add Evidence and migrate to the HostHardDrive.E01 file.
5. EnCase7 will load the file and begin a complete file integrity check.
6. Once the evidence file had been verified then Select Process Evidence > Acquire Evidence. Once Acquired Select Process Evidence > Process Evidence.
7. Configure the Evidence Processing dialog box and assure that all of the options desired are included. One additionally added for this project was the Keyword Search that allowed many keywords used during the project to be searched during initial processing.

Once the HostHardDrive.E01 image was successfully acquired into FTK 6 and Encase 7, the host hard drive was re-installed back into the host machine so Volatility tools could be utilized to examine the virtual machine memory files created during the Trial Testing. HashCalc was utilized to track the hash values of the Host Hard Drive and virtual machines as compared to those obtained by FTK 6 and EnCase 7.

Database Content for Keyword Search

During the previous chapters there is mention of a "Clouds" database that was developed to be used with the KeePass system and "Bluesky" that was designed for use in the Password Safe. The contents of these password databases are distinct from one another by design so that keyword searches may provide more insight into answering the research questions. The appearance of specific keywords during the examination phase would help to identify which password management system was affected and help identify a specific virtual machine that may need further investigation. The following table helps to identify the root keywords used for searching in FTK and EnCase on the HostHardDrive.E01 forensic image. These root keywords were also used to create a list of 60 words that were entered into various Note sections of the KeePass and Password Safe password managers. Table 4 and Table 5 provide a visual representation of the keywords available for search during this project.

Table 4

Database Contents Created for Developing Keyword Searches

Software Product	Master Key Password	Database Name	Database Entries

KeePass 2.35	**WX[secretp@ssword]YZ**	**Clouds**	**Hoovers Place**
			User=bogusdata
			Password = T00easy
			
			Kellys Pub
			User = partytime1
			Password = 0nthec0rner
			
			Lapalooza
			User = eastern56
			Password = n3wpass2017
			
			Stormboard
			User = bogey799
			Password = mislead666^)

Password Safe 3.41	**AB[n0accesshere]CD**	**Bluesky**	**Alphonses**
			User = bigal
			Password = r3alm3an17
			
			Benny Jets
			User = coolhand
			Password = M0respeed
			
			Franco Nursery
			User = bossman1
			Password = l0veplants
			
			Stormboard
			User = bogey799
			Password = mislead666^)

Table 5

List of keywords for this project including those created by the Password Generation function of KeePass and Password Safe.

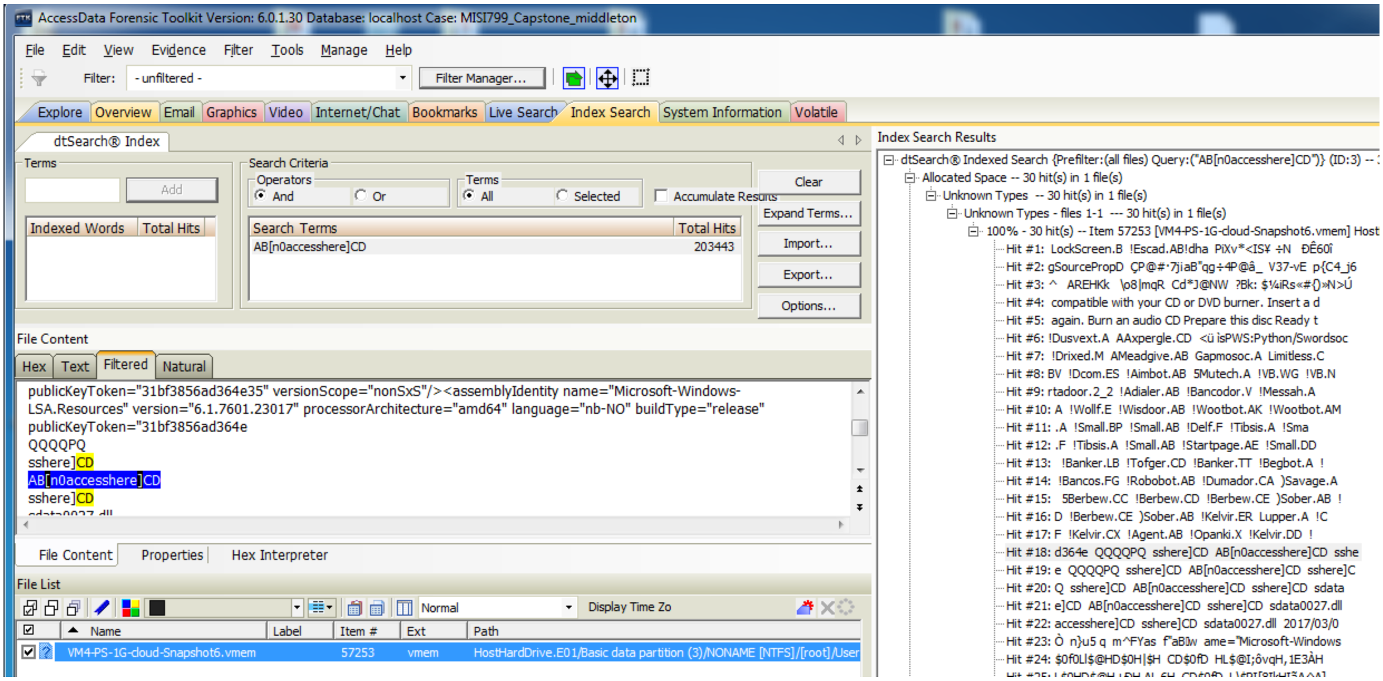
	Total List of Keywords Available for Search		
username	partytime1	12345	l0veplants
user	0nthec0rner	Password	Harry
User	eastern56	Bluesky	Hawk
password	n3wpass2017	bluesky	DOB
MISI799	bogey799	Alphonses	906-623-9475
P@ssword56	T00easy	Alphonse	Phone
GDYCQ-	mislead666^)	bigal	Te<vUqj(*QM4Kts0,}~^
6DWY6-	1234-6789-4321-9876	r3alm3an17	HhvCunJrA0QHtWI zKZL
Capstone	Hoovers	Benny	vsiHf}Mz9w}xs2105MWb
Capstone2	Place	Jets	b6HJSi94iekfACD} TOdK
WX[secretp@ssword]YZ	Kelly	coolhand	29A]GV@&72t
AB[n0accesshere]CD	Pubs	m0respeed	C0=3P<h60f:4
Clouds	LaPalooza	Franco	0^5-J8>FJjo
clouds	Stormboard	Nursery	a3cLd2t7W7uH
bogusdata	Michael321	bossman1	

Examination of HostHardDriv.E01 with FTK 6

Examination of the hard drive utilized in the study named HostHardDrive.E01 began with a cursory review of data classifications that are collected during evidence processing within the FTK 6 forensic software. These can be accessed by selecting tabs located at the top of the page. One of the options is labeled dtSearch which allow Indexed Searches based on keywords that were indexed during the processing phase of the hard drive. The first logical search was for the Master Key Passwords listed in Table 4 that would allow access to all of the underlying databases for KeePass 2.35 and Password Safe 3.41. Once FTK 6 was started and the capstone case was opened, the HostHardDrive.E01 file was selected for examination.

Master Key Keyword Search for Password Safe 3.41

The Master Key **AB[n0accesshere]CD** was entered into the FTK dtSearch Index dialog box so the HostHardDrive.E01 evidence file would be examined for the presence of this string data in plain text anywhere on the hard drive. When the dtSearch results returned it indicated that there were 22 hits on the search criteria and they were found at VM4-PS-1G-cloud-Snapshot6.vmem as seen in Fig. 16.


AccessData Forensic Toolkit Version: 6.0.1.30 Database: localhost Case: MISI799_Capstone_middleton
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
dtSearch® Index
Terms
Add
Indexed Words Total Hits
Search Criteria
Operators
● And ○ Or
Terms
● All ○ Selected
□ Accumulate Results
Clear
Expand Terms...
Import...
Export...
Options...
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Normal
Display Time Zo
Index Search Results

Search Terms	Total Hits
AB[n0accesshere]CD	203443

```
publicKeyToken="31bf3856ad364e35" versionScope="nonSxS"/><assemblyIdentity name="Microsoft-Windows-
LSA.Resources" version="6.1.7601.23017" processorArchitecture="amd64" language="nb-NO" buildType="release"
publicKeyToken="31bf3856ad364e
QQQQPQ
sshere]CD
AB[n0accesshere]CD
sshere]CD
```

☑	Name	Label	Item #	Ext	Path
☑	VM4-PS-1G-cloud-Snapshot6.vmem		57253	vmem	HostHardDrive.E01/Basic data partition (3)/NONAME [NTFS]/[root]/User

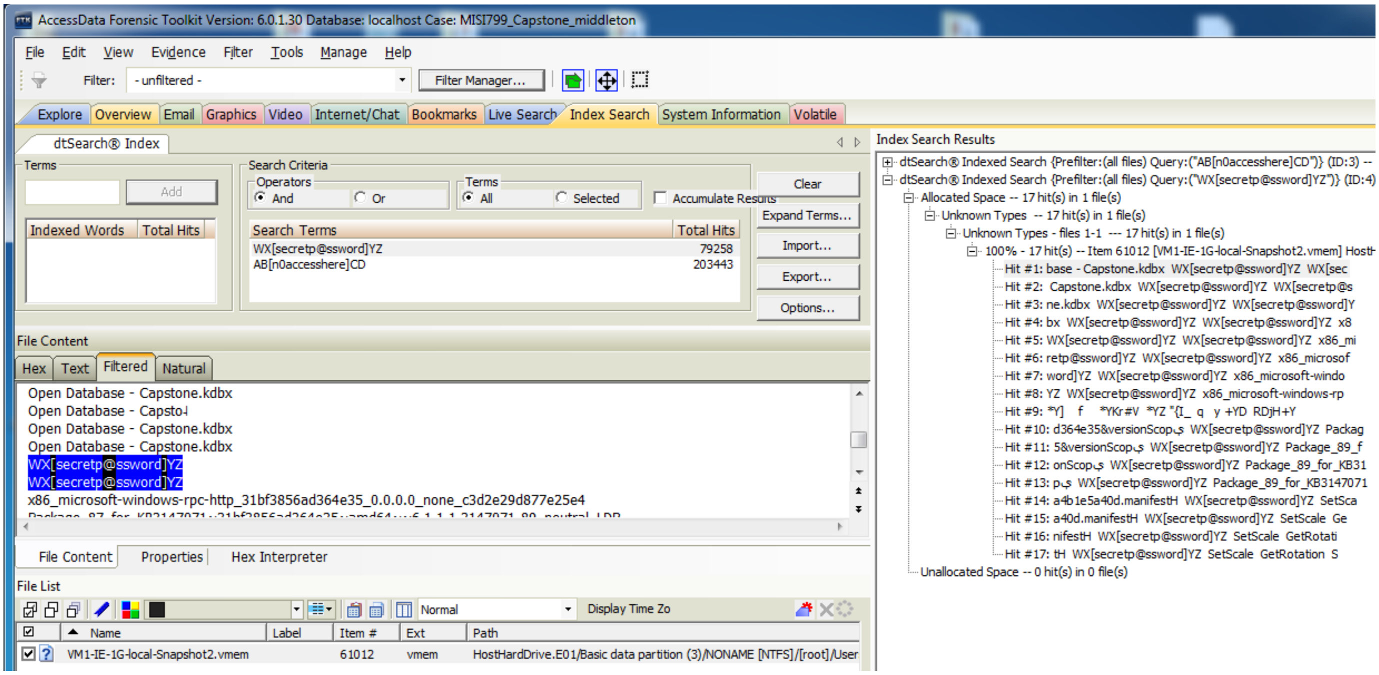
```
dtSearch® Indexed Search {Prefilter:(all files) Query:("AB[n0accesshere]CD")} (ID:3) --
  Allocated Space -- 30 hit(s) in 1 file(s)
    Unknown Types  -- 30 hit(s) in 1 file(s)
      Unknown Types - files 1-1  --- 30 hit(s) in 1 file(s)
        100% - 30 hit(s) -- Item 57253 [VM4-PS-1G-cloud-Snapshot6.vmem] Host
          Hit #1:  LockScreen.B  !Escad.AB!dha  PiXv*<IS¥ ÷N   ĐÊ60î
          Hit #2: gSourcePropD  ÇP@#·7jiaB"qg÷4P@â_  V37-vE  p{C4_j6
          Hit #3: ^   AREHKk   \o8|mqR  Cd*J@NW  ?Bk: $¼iRs«#{}»N>Ú
          Hit #4:  compatible with your CD or DVD burner. Insert a d
          Hit #5:  again. Burn an audio CD Prepare this disc Ready t
          Hit #6: !Dusvext.A  AAxpergle.CD  <ü ìsPWS:Python/Swordsoc
          Hit #7:  !Drixed.M  AMeadgive.AB  Gapmosoc.A  Limitless.C
          Hit #8: BV  !Dcom.ES  !Aimbot.AB  5Mutech.A  !VB.WG  !VB.N
          Hit #9: rtadoor.2_2  !Adialer.AB  !Bancodor.V  !Messah.A
          Hit #10: A  !Wollf.E  !Wisdoor.AB  !Wootbot.AK  !Wootbot.AM
          Hit #11: .A  !Small.BP  !Small.AB  !Delf.F  !Tibsis.A  !Sma
          Hit #12: .F  !Tibsis.A  !Small.AB  !Startpage.AE  !Small.DD
          Hit #13:   !Banker.LB  !Tofger.CD  !Banker.TT  !Begbot.A  !
          Hit #14:  !Bancos.FG  !Robobot.AB  !Dumador.CA  )Savage.A
          Hit #15:   5Berbew.CC  !Berbew.CD  !Berbew.CE  )Sober.AB  !
          Hit #16: D  !Berbew.CE  )Sober.AB  !Kelvir.ER  Lupper.A  !C
          Hit #17: F  !Kelvir.CX  !Agent.AB  !Opanki.X  !Kelvir.DD  !
          Hit #18: d364e  QQQQPQ  sshere]CD  AB[n0accesshere]CD  sshe
          Hit #19: e  QQQQPQ  sshere]CD  AB[n0accesshere]CD  sshere]C
          Hit #20: Q  sshere]CD  AB[n0accesshere]CD  sshere]CD  sdata
          Hit #21: e]CD  AB[n0accesshere]CD  sshere]CD  sdata0027.dll
          Hit #22: accesshere]CD  sshere]CD  sdata0027.dll  2017/03/0
          Hit #23: Ò  n}u5 q  m^FYas  f"aBw  ame="Microsoft-Windows
          Hit #24: $0f0Ll$@HD$0H|$H  CD$0fD  HL$@I;ôvqH,1E3ÀH
```

Figure 16. This is the FTK dtSearch results when the Master Key Password for Password Safe was entered and it shows that the password is in plain text. It was located in VM4-PS-1G-cloud-Snapshot6.vmem captured during Trial Event 6 (Export Database).

This dtSearch result was marked as a Bookmarked item in FTK 6 that is available for export when assembling the final report. Documenting the evidence location for future reference with a bookmark assists in the verification protocol for scientific processes.

Master Key Keyword Search for KeePass 2.35

The Master Key **WX[secretp@ssowrd]YZ** was entered into the FTK dtSearch Index dialog box so the HostHardDrive.E01 evidence file would be examined for the presence of this string data in plain text anywhere on the hard drive. When the dtSearch results returned it indicated that there were 17 hits on the search criteria and they were found at VM1-IE-1G-localSnapshot2.vmem as seen in Figure 17.



Operators: ● And ○ Or Terms: ● All ○ Selected □ Accumulate Results

Search Terms	Total Hits
WX[secretp@ssword]YZ	79258
AB[n0accesshere]CD	203443

```
Open Database - Capstone.kdbx
Open Database - Capsto⫞
Open Database - Capstone.kdbx
Open Database - Capstone.kdbx
WX[secretp@ssword]YZ
WX[secretp@ssword]YZ
x86_microsoft-windows-rpc-http_31bf3856ad364e35_0.0.0.0_none_c3d2e29d877e25e4
```

Index Search Results

```
⊞ dtSearch® Indexed Search {Prefilter:(all files) Query:("AB[n0accesshere]CD")} (ID:3) --
⊟ dtSearch® Indexed Search {Prefilter:(all files) Query:("WX[secretp@ssword]YZ")} (ID:4)
  ⊟ Allocated Space -- 17 hit(s) in 1 file(s)
    ⊟ Unknown Types  -- 17 hit(s) in 1 file(s)
      ⊟ Unknown Types - files 1-1  --- 17 hit(s) in 1 file(s)
        ⊟ 100% - 17 hit(s) -- Item 61012 [VM1-IE-1G-local-Snapshot2.vmem] HostH
            Hit #1: base - Capstone.kdbx  WX[secretp@ssword]YZ  WX[sec
            Hit #2:  Capstone.kdbx  WX[secretp@ssword]YZ  WX[secretp@s
            Hit #3: ne.kdbx  WX[secretp@ssword]YZ  WX[secretp@ssword]Y
            Hit #4: bx  WX[secretp@ssword]YZ  WX[secretp@ssword]YZ  x8
            Hit #5: WX[secretp@ssword]YZ  WX[secretp@ssword]YZ  x86_mi
            Hit #6: retp@ssword]YZ  WX[secretp@ssword]YZ  x86_microsof
            Hit #7: word]YZ  WX[secretp@ssword]YZ  x86_microsoft-windo
            Hit #8: YZ  WX[secretp@ssword]YZ  x86_microsoft-windows-rp
            Hit #9: *Y]   f    *YKr#V  *YZ "{I_  q   y +YD  RDjH+Y
            Hit #10: d364e35&versionScopڀ  WX[secretp@ssword]YZ  Packag
            Hit #11: 5&versionScopڀ  WX[secretp@ssword]YZ  Package_89_f
            Hit #12: onScopڀ  WX[secretp@ssword]YZ  Package_89_for_KB31
            Hit #13: pڀ  WX[secretp@ssword]YZ  Package_89_for_KB3147071
            Hit #14: a4b1e5a40d.manifestH  WX[secretp@ssword]YZ  SetSca
            Hit #15: a40d.manifestH  WX[secretp@ssword]YZ  SetScale  Ge
            Hit #16: nifestH  WX[secretp@ssword]YZ  SetScale  GetRotati
            Hit #17: tH  WX[secretp@ssword]YZ  SetScale  GetRotation  S
  Unallocated Space -- 0 hit(s) in 0 file(s)
```

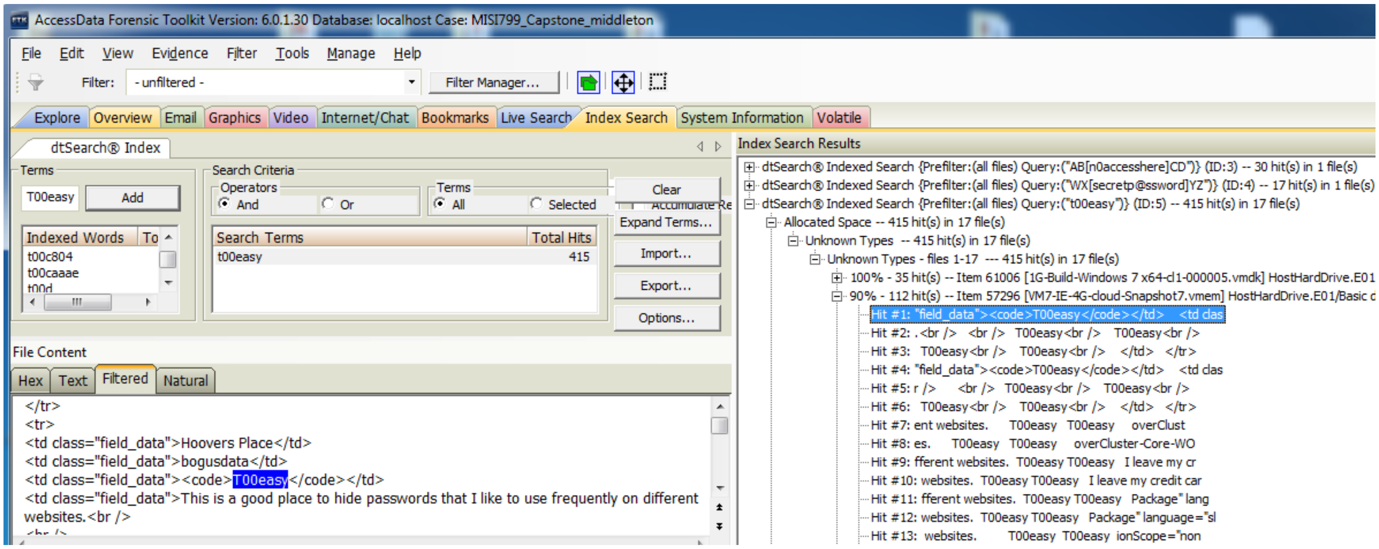
☑	Name	Label	Item #	Ext	Path
☑	VM1-IE-1G-local-Snapshot2.vmem		61012	vmem	HostHardDrive.E01/Basic data partition (3)/NONAME [NTFS]/[root]/User

Figure 17. This is the FTK dtSearch results when the Master Key Password for KeePass was entered and it shows the password in plain text. It was located in VM1-IE-1G-local-Snapshot2.vmem during Trial Event 1 (Logon with Master Key).

This dtSearch result was marked as a Bookmarked item in FTK 6 that is available for export when assembling the final report. Documenting the evidence location for future reference with a bookmark assists in the verification protocol for scientific processes.

Password Search for KeePass 2.35

The next step involved searching with the FTK dtSearch tool for the presence of passwords that appear in a readable format as summarized in Table 6. Virtual machines used for the KeePass testing process involved VM1, VM3, VM5 and VM7. The Capstone database created for use during the Trial Tests with KeePass included an entry named “Hoovers Place” with a user name “bogusdata” and the associated password of “T00easy”. The password **T00easy** was entered into the FTK dtSearch Index dialog box so the HostHardDrive.E01 evidence file would be examined for the presence of this string data in plain text anywhere on the hard drive. This resulted in locating 415 hits within 17 fields. Nine of the fields were the virtual memory files (.vmem) and the other eight fields were the associated virtual disk (.vdmk) files that are created after each snapshot was taken. The data returned indicated that VM1-IE-1G-local-Snapshot5 (Copy to Clipboard) provided 7 hits where VM1-IE-1G-local-Snapshot6 (Copy and Paste) yielded 22 hits on the “T00easy’ password in plain text.



Filter: - unfiltered -

Terms: T00easy

Indexed Words	To
t00c804	
t00caaae	
t00d	

Search Criteria
Operators: ● And ○ Or
Terms: ● All ○ Selected

Search Terms	Total Hits
t00easy	415

```
</tr>
<tr>
<td class="field_data">Hoovers Place</td>
<td class="field_data">bogusdata</td>
<td class="field_data"><code>T00easy</code></td>
<td class="field_data">This is a good place to hide passwords that I like to use frequently on different
websites.<br />
```

Index Search Results

```
⊞ dtSearch® Indexed Search {Prefilter:(all files) Query:("AB[n0accesshere]CD")} (ID:3) -- 30 hit(s) in 1 file(s)
⊞ dtSearch® Indexed Search {Prefilter:(all files) Query:("WX[secretp@ssword]YZ")} (ID:4) -- 17 hit(s) in 1 file(s)
⊟ dtSearch® Indexed Search {Prefilter:(all files) Query:("t00easy")} (ID:5) -- 415 hit(s) in 17 file(s)
  ⊟ Allocated Space -- 415 hit(s) in 17 file(s)
    ⊟ Unknown Types  -- 415 hit(s) in 17 file(s)
      ⊟ Unknown Types - files 1-17  --- 415 hit(s) in 17 file(s)
        ⊞ 100% - 35 hit(s) -- Item 61006 [1G-Build-Windows 7 x64-cl1-000005.vmdk] HostHardDrive.E01
        ⊟ 90% - 112 hit(s) -- Item 57296 [VM7-IE-4G-cloud-Snapshot7.vmem] HostHardDrive.E01/Basic d
            Hit #1: "field_data"><code>T00easy</code></td>    <td clas
            Hit #2: .<br />   <br />   T00easy<br />   T00easy<br />
            Hit #3:   T00easy<br />   T00easy<br />    </td>   </tr>
            Hit #4: "field_data"><code>T00easy</code></td>    <td clas
            Hit #5: r />      <br />   T00easy<br />   T00easy<br />
            Hit #6:   T00easy<br />   T00easy<br />    </td>   </tr>
            Hit #7: ent websites.     T00easy   T00easy    overClust
            Hit #8: es.     T00easy   T00easy    overCluster-Core-WO
            Hit #9: fferent websites.  T00easy T00easy   I leave my cr
            Hit #10: websites.  T00easy T00easy   I leave my credit car
            Hit #11: fferent websites.  T00easy T00easy   Package" lang
            Hit #12: websites.  T00easy T00easy   Package" language="sl
            Hit #13:  websites.       T00easy  T00easy  ionScope="non
```

Figure 18. This screenshot displays the result of an FTK dtSearch for the password “T00easy”.

Due to the amount of space that the screenshots utilize the remaining figures associated with the FTK dtSearches are located in Appendix E. The VM3-IE-1G-cloud-Snapshot5.vmem (Copy and Paste) provided 13 hits while VM3-IE-1G-cloud-Snapshot6.vmem (Export) had 59 hits for the “T00easy” password search. VM5-IE-4G-local-Snapshot8.vmem (Delete Database) indicated 74 hits and VM5-IE-4G-local-Snapshot4.vmem (Copy to Clipboard) had 2 hits. The most hits recorded during this search occurred in VM7-IE-4G-cloud-Snapshot7 (Print) Trial Event testing with VM7-IE-4G-cloud-Snapshot3 (Perform Auto-Type) at 4 hits and VM7-IE-4G-cloud-Snapshot4 ((Copy To Clipboard) with 6 hits on the “T00easy” password search. This dtSearch result was marked in FTK as a Bookmarked item named “Search for T00easy” that will be available when assembling the final report.

A dtSearch on "n3wpass2017" that is the password for the LaPalooza database entry with username eastern56 in the Capstone database for the KeePass configuration indicated 378 hits in 15 fields. The greatest number of hits was identified in the VM7-IE-4G-cloud-Snapshot7.vmem (Print) feature that yielded 152 hits. The next virtual machine that had the highest number of hits for “n3wpass2017” was VM5-IE-4G-local-Snapshot8.vmem (Delete Database) feature that returned 74 hits. VM3-IE-1G-cloud-Snapshot6 (Export Database) recorded 62 hits on the password while the (Copy and Paste) feature produced 16 hits. Finally, the virtual machine VM1-IE-1G-local-Snapshots 5 and 6 only produced 1 hit for (Copy to Clipboard) and 2 hits for (Copy and Paste) respectfully. The next KeePass database entry to be searched was that named as “Kellys Pub”.

Kellys Pub was also created within the Capstone database file with a username = partytime1 and a password = “0nthec0rner”. A dtSearch on “0nthec0rner” produced 354 hits in 15 files. Once again the greatest number of hits on the password appeared in VM7-IE-4G-cloud-

Snapshot7 (Print) Trial Event test with 114 hits and 2 hits during the (Copy to Clipboard) test. The next virtual machine to register a large number of hits on the password was VM3-IE-1G-cloud-Snapshot6 (Export Database) Trial Test Event test which recorded 60 hits and 11 hits for the (Copy and Paste) feature. VM5-IE-4G-local-Snapshot8 (Delete Database) Trial Event test yielded 49 hits and only 1 hit for the (Copy to Clipboard) feature. Finally, the virtual machine VM1-IE-1G-local-Snapshot6 (Export Database) registered 17 hits on the password while the (Copy to Clipboard) feature had 1 hit.

Password Search for Password Safe 3.41

The next step involved searching with the FTK dtSearch tool for the presence of passwords that appear in a readable format. Virtual machines used for the Password Safe testing process involved VM2, VM4, VM6 and VM8. An important aspect is that the Password Safe 3.41 version does not have a (Print) feature for security reasons and will not have results to show for that portion of the Trial Event tests. The Capstone2 database created for use during the Trial Tests with Password Safe included an entry named “Alphonses” with a user name “bigal” and the associated password of “r3alm3an17”.

The password **r3alm3an17** was entered into the FTK dtSearch Index dialog box so the HostHardDrive.E01 evidence file would be examined for the presence of this string data in plain text anywhere on the hard drive. This resulted in locating 269 hits within 13 files. Nine of the files were the virtual memory files (.vmem) and the other 4 files were the associated virtual disk (.vdmk) files that are created after each snapshot was taken.

The virtual machine named VM4-PS-1G-cloud-Snapshot6 (Export Database) Trial Event test indicated 51 hits while (Delete Database) had 41 hits and (Copy to Clipboard) produced 6 hits on the password. VM2-PS-1G-local-Snapshot6 (Export Database) Trial Event test indicated that there were 47 hits on this process. VM-8-PS-4G-cloud-Snapshot3 (Auto-Type) Trial Event test provided 19 hits while the (Copy to Clipboard) Trial Event test produced 24 hits on the “r3alm3an17” password. The virtual machine VM6-PS-4G-local-Snapshot4 (Copy to Clipboard) Trial Event test produced 1 hit with the (Copy and Paste) feature producing 5 hits on the previously mentioned password.

The next FTK dtSearch pertained to a database entry called “Benny Jets” which had a username of “coolhand” and an associated password of “m0respeed”. The password **m0respeed** was entered into the FTK dtSearch Index dialog box so the HostHardDrive.E01 evidence file would be examined for the presence of this string data in plain text anywhere on the hard drive. This resulted in locating 188 hits within 11 files. Seven of the files were the virtual memory files (.vmem) and the other four files were the associated virtual disk (.vdmk) files that are created after each snapshot was taken.

The virtual machine VM2-PS-1G-local-Snapshot6 (Export Database) Trial Event test produced 46 hits on the **m0respeed** password while the (Delete Database) process recorded 31 hits on the password. VM4-PS-1G-cloud-Snapshot6 (Export Database) Trial Event test produced 21 hits when the (Delete Database) process had 18 hits. VM6-PS-4G-local-Snapshot 5 (Copy and Paste) Trial Event test produced 3 hits. VM8-PS-4G-cloud-Snapshot3 (Auto-Type) Trial Event test had 10 hits while the (Copy to Clipboard) operation recorded 15 hits on the password.

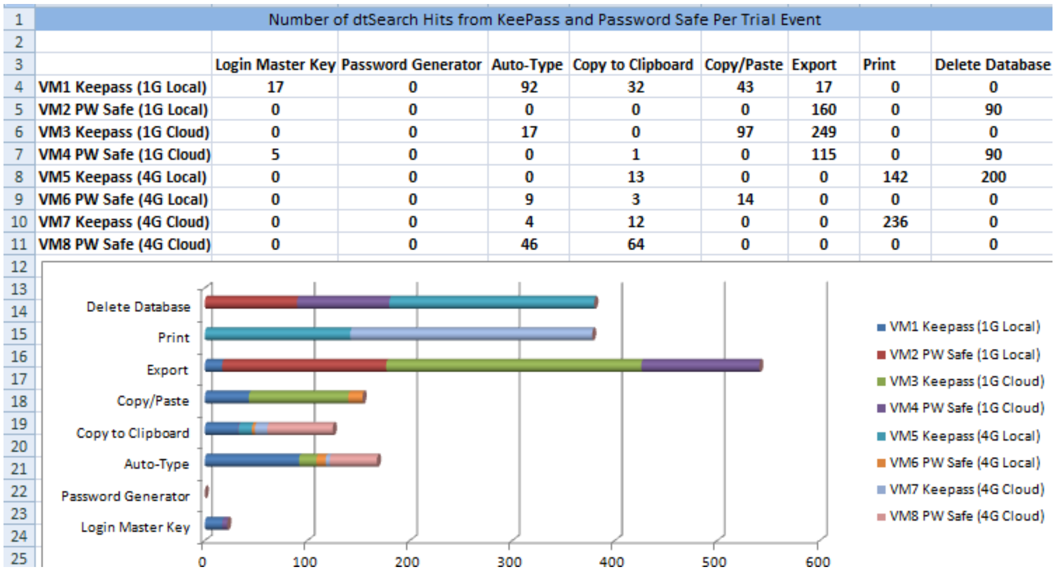
The next FTK dtSearch pertained to a database entry called “Franco Nursery” which had a username of “bossman1” and an associated password of “l0veplants”. The password **l0veplants** was entered into the FTK dtSearch Index dialog box so the HostHardDrive.E01 evidence file would be examined for the presence of this string data in plain text anywhere on the hard drive. This resulted in locating 168 hits within 12 files. Eight of the files were the virtual memory files (.vmem) and the other four files were the associated virtual disk (.vdmk) files that are created after each snapshot was taken.

The virtual machine with the greatest number of hits in this dataset was VM2-PS-1G-local-Snapshot6 (Export Database) Trial Event test with 52 hits and a subsequent (Delete Database) Trial Event that produced 21 hits on the password. VM4-PS-1G-cloud-Snapshot4 (Copy to Clipboard) Trial Event test had only 1 hit while the (Export Database) had 18 hits and the (Delete Database) test provided 13 hits on the password. VM-PS4G-local-Snapshot5 (Copy and Paste) Trial Event had 2 hits while VM8-PS-4G-cloud-Snapshot3 (Auto-Type) provided 8 hits and the (Copy to Clipboard) test produced 13 hits.

See Table 6 below for total hits returned on FTK dtSearches. Note that while examining data in FTK it was observed that each hit returned did not correlate to one unique password. The hits included fragments of passwords or a couple segments of the same password which tended to artificially inflate the total number of hit values.

Table 6

Total Number of Returned FTK dtSearch Hits on Passwords



Number of dtSearch Hits from KeePass and Password Safe Per Trial Event

	Login Master Key	Password Generator	Auto-Type	Copy to Clipboard	Copy/Paste	Export	Print	Delete Database
VM1 Keepass (1G Local)	17	0	92	32	43	17	0	0
VM2 PW Safe (1G Local)	0	0	0	0	0	160	0	90
VM3 Keepass (1G Cloud)	0	0	17	0	97	249	0	0
VM4 PW Safe (1G Cloud)	5	0	0	1	0	115	0	90
VM5 Keepass (4G Local)	0	0	0	13	0	0	142	200
VM6 PW Safe (4G Local)	0	0	9	3	14	0	0	0
VM7 Keepass (4G Cloud)	0	0	4	12	0	0	236	0
VM8 PW Safe (4G Cloud)	0	0	46	64	0	0	0	0

Password Search for KeePass 2.35 and Password Safe 3.41

The next step involved searching with the FTK dtSearch tool for the presence of passwords that appear in a readable format that may occur in all of the virtual machines. Since this database entry was used in both the “Clouds” and “Bluesky” data sets; Virtual machines used for this KeePass and Password Safe testing process included VM1, VM2, VM3, VM4, VM5, VM6, VM7 and VM8. The reason for this was to have one sample website that would be common to all virtual machines for testing Trial Event 3 (Auto-Type) on form fields within a web application.

The database entry created for use during the Trial Tests with this process included an entry named “Stormboard” with a user name “bogey799” and the associated password of “misi605^)”. The password **misi605^)** was entered into the FTK dtSearch Index dialog box so the HostHardDrive.E01 evidence file would be examined for the presence of this string data in plain text anywhere on the hard drive. This resulted in locating 826 hits within 35 files. Twenty three of the files were the virtual memory files (.vmem) and the other 8 files were the associated virtual disk (.vdmk) files that are created after each snapshot was taken.

Starting with VM1-IE-1G-local-Snapshot4 (Auto-Type) Trial Event produced 92 hits followed by (Copy to Clipboard) with 23 hits and (Copy and Paste) producing 17 hits on the misi605^) password. VM2-PS-1G-local-Snapshot6 (Export Database) had 15 hits with the (Delete Database) Trial Event having 8 hits. VM3-IE-1G-cloud-Snapshot6 (Export Database) produced 68 hits with the (Copy and Paste) operation at 67 hits and the (Auto-Type) process producing 17 hits on the misi605^) password. VM4-PS-1G-cloud-Snapshot6 (Export Database) had 26 hits with the (Delete Database) process yielding 18 hits and the (Copy to Clipboard) operation having 1 hit on the password.

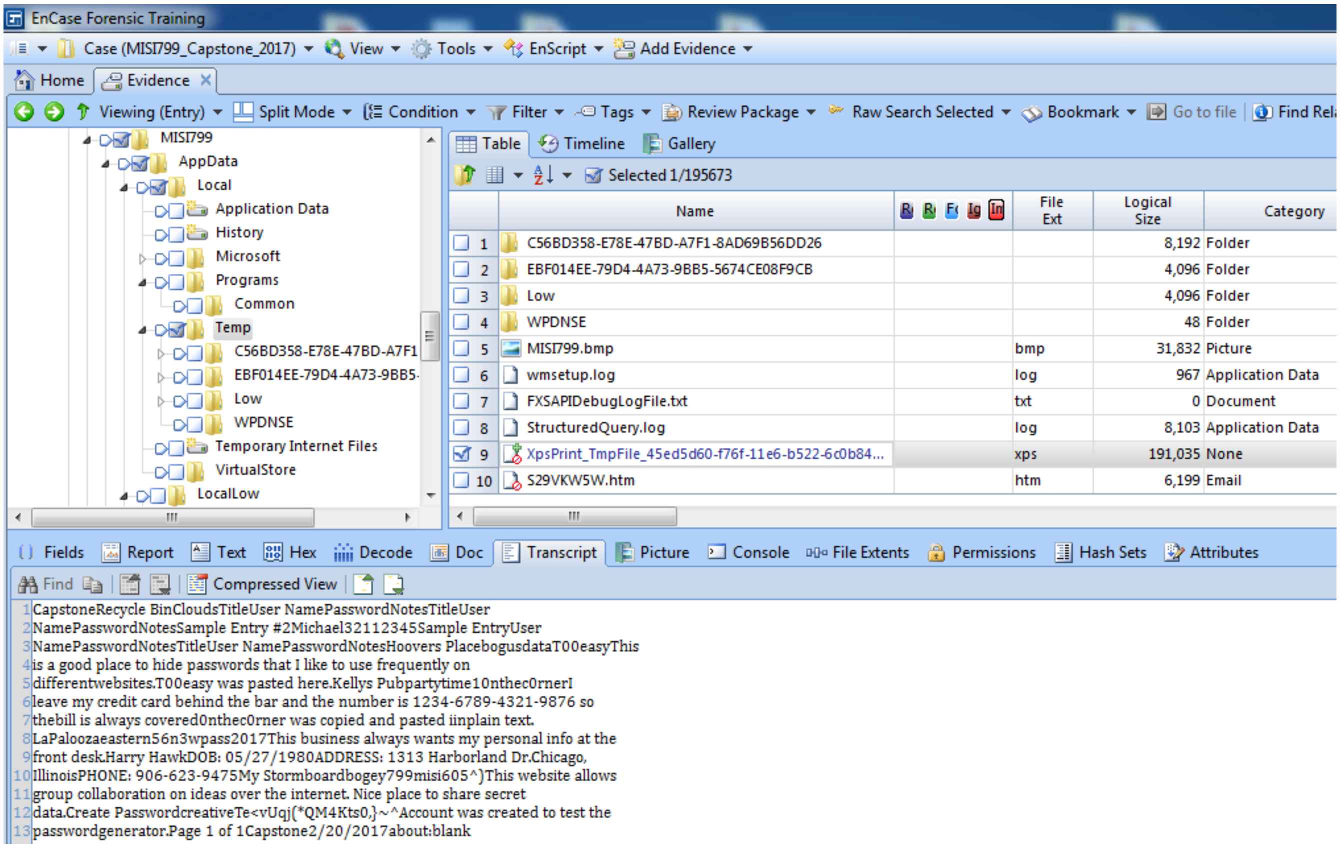
The final set of virtual machines started with VM5-IE-4G-local-Snapshot8 (Delete Database) with 52 hits, (Copy to Clipboard) at 6 hits and an (Auto-Type) Trial Event that produce 3 hits. VM6-PS-4G-local-Snapshot3 (Auto-Type) had 9 hits where (Copy and Paste) produced 4 hits and (Copy to Clipboard) had 1 hit on the password. VM7-IE-4G-cloud-Snapshot7 (Print Database) produced 143 hits with (Auto-Type) and (Copy to Clipboard) each producing 1 hit apiece. Finally, VM8-PS-4G-cloud-Snapshot4 (Copy to Clipboard) produced 12 hits and the (Auto-Type) process had 9 hits on the pass misi605^) password. See Table 6 for total number of dtSearch hits across all of the virtual machines. Screenshots for most of the above listed FTK dtSearches can be viewed in Appendix E.

Examination of HostHardDriv.E01 with EnCase 7

Examination of the hard drive utilized in the study named HostHardDrive.E01 began with a cursory review of data classifications that are collected during evidence processing within the EnCase forensic software. The virtual machines utilized in the Trial Event testing were accessible as virtual memory (.vmem) files however EnCase seemed to have a difficult time differentiating the Snapshot data sets. To overcome this obstacle, each virtual disk file (.vmdk) Snapshot representing a specific Trial Event such as VM1-IE-1G-local-Snapshot7.vmem (Print Database) was imaged individually using FTK Imager and then added as a separate evidence item to EnCase Forensic. One specific image was named **vm1_kp_print-db.E01** to identify its origin and Trial Event functionality. This allowed each specific Snapshot item to be available for examination as a separate instance of the hard disk.

Review of the evidence files indicated that KeePass and Password Safe left little in the form of unencrypted data on the hard disk. This was the case whether the virtual machine was configured with 1 Gig or 4 Gig of RAM. The most significant finding was that where the print database feature in KeePass was utilized to create an XPS document or a Fax, even upon deletion there was a complete plain text copy of the document in the TEMP directory. However these items would most likely not be retrievable without forensic software and Password Safe does not provide a database printing feature.

Referring to Fig. 19 below it can be seen in KeePass evidence image **vm1_kp_print-db.E01** that item #9 in the right sided pane is an XPS Print Temporary file that had been deleted after being printed to the XPS format. The lower pane displays the content of the printed item that was recovered by EnCase Examiner. The file was bookmarked so it could be exported later.

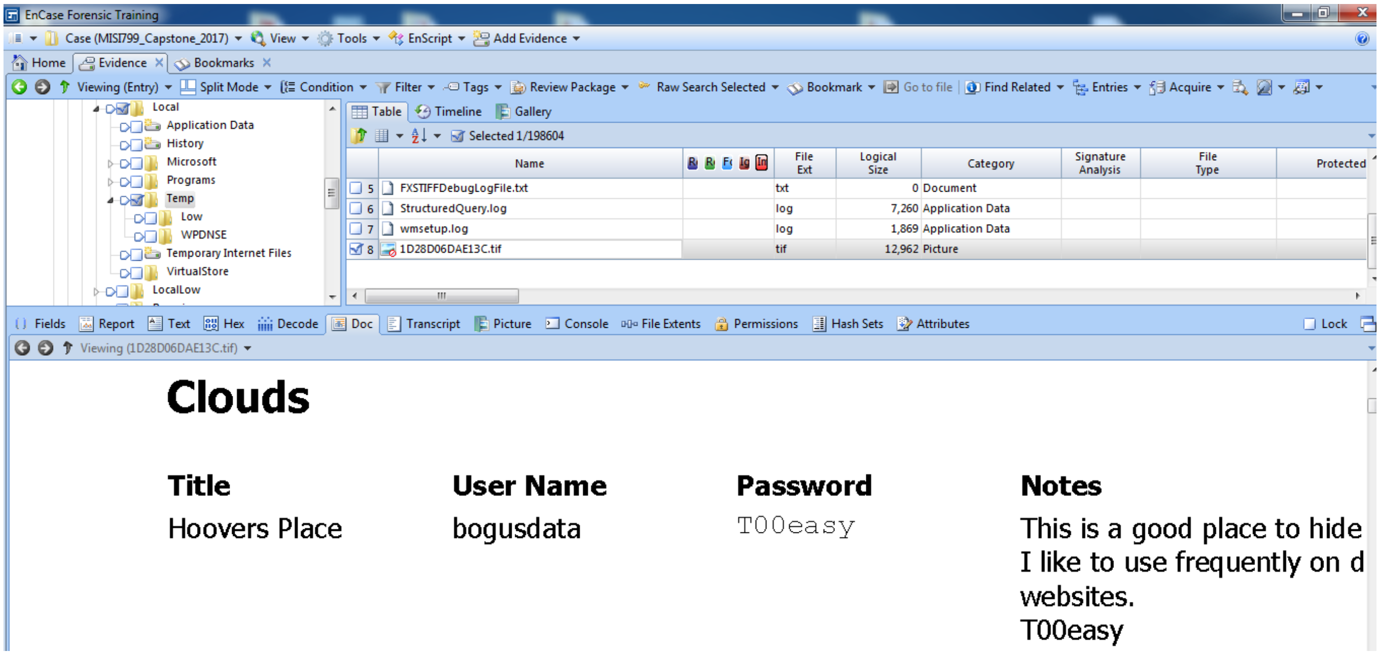


		Name	R R Fi Ig In	File Ext	Logical Size	Category
☐	1	C56BD358-E78E-47BD-A7F1-8AD69B56DD26			8,192	Folder
☐	2	EBF014EE-79D4-4A73-9BB5-5674CE08F9CB			4,096	Folder
☐	3	Low			4,096	Folder
☐	4	WPDNSE			48	Folder
☐	5	MISI799.bmp		bmp	31,832	Picture
☐	6	wmsetup.log		log	967	Application Data
☐	7	FXSAPIDebugLogFile.txt		txt	0	Document
☐	8	StructuredQuery.log		log	8,103	Application Data
☑	9	XpsPrint_TmpFile_45ed5d60-f76f-11e6-b522-6c0b84...		xps	191,035	None
☐	10	S29VKW5W.htm		htm	6,199	Email

```
CapstoneRecycle BinCloudsTitleUser NamePasswordNotesTitleUser
NamePasswordNotesSample Entry #2Michael32112345Sample EntryUser
NamePasswordNotesTitleUser NamePasswordNotesHoovers PlacebogusdataT00easyThis
is a good place to hide passwords that I like to use frequently on
differentwebsites.T00easy was pasted here.Kellys Pubpartytime10nthec0rnerI
leave my credit card behind the bar and the number is 1234-6789-4321-9876 so
thebill is always covered0nthec0rner was copied and pasted iinplain text.
LaPaloozaeastern56n3wpass2017This business always wants my personal info at the
front desk.Harry HawkDOB: 05/27/1980ADDRESS: 1313 Harborland Dr.Chicago,
IllinoisPHONE: 906-623-9475My Stormboardbogey799misi605^)This website allows
group collaboration on ideas over the internet. Nice place to share secret
data.Create PasswordcreativeTe<vUqj(*QM4Kts0,}~^Account was created to test the
passwordgenerator.Page 1 of 1Capstone2/20/2017about:blank
```

Figure 19. This EnCase 7 screenshot depicts the Temp directory containing XPSPrint_Temp file (marked with a checkmark) which was KeePass Trial Event 7 (Print Database) on VM1.

The second document type that appeared in the Temp directory was located in the **vm5_kp_print-db.E01** evidence image. Recall that this evidence image was created with FTK Imager by processing the virtual machine disk (.vmdk) file created from the Snapshot used to capture the (Print Database) feature. Examination of the image utilizing EnCase facilitated the isolation of a previously deleted fax that had been printed during the Trial Event (Print Database) on VM5. When the command to print the database from within KeePass was presented the option selected included the ability to print to a fax format. The process had been repeated a couple of times including cancelling the print process and deleting the fax document.



	Name	File Ext	Logical Size	Category	Signature Analysis	File Type	Protected
□ 5	FXSTIFFDebugLogFile.txt	txt	0	Document			
□ 6	StructuredQuery.log	log	7,260	Application Data			
□ 7	wmsetup.log	log	1,869	Application Data			
☑ 8	1D28D06DAE13C.tif	tif	12,962	Picture			

Clouds

Title	User Name	Password	Notes
Hoovers Place	bogusdata	T00easy	This is a good place to hide I like to use frequently on d websites. T00easy

Figure 20. This screenshot depicts the previously deleted (Print Database to Fax) shown as item #8 in the upper right pane of EnCase 7. The recovered contents from **vm5_kp_print-db.E01** are displayed in the lower pane.

Printing of the database in KeePass allowed the entire “Clouds” information set including the entries for Title, User Name, Password and all contents in the Notes section to appear in plain text as a deleted file from within the TEMP directory. It should be noted at this point that the

Trial Events for the Print Database test were repeated many times in an attempt to exhaust memory resources and precipitate unusual behavior of residual digital artifacts. This evidence item was bookmarked within EnCase 7 so it could be exported at a later time. The Password Safe management system does not offer a print database function and could not be tested.

Configuring Volatility Memory Analysis Framework

Volatility is located at the (**Path= C:\Python27\volatility-master\vol.py**). After activating the Command Prompt **C:\Windows\system32** the directory was changed to **C:\Python27\volatility-master** which provides the command prompt and allows access to the **volatility-master** directory. Volatility is initialized by the command **vol.py**. The command that was tested was the "**pslist**" module for processes and it was configured as:

C:\Python27\volatility-master> vol.py pslist –f path to VM1-IE-1G-local-Snapshot1**.vmem --profile=Win7SP1x64.**

When executed it provides a comprehensive list of processes recorded in the memory image. The module can be listed before or after the **–f** (file). To obtain the proper path=file location highlight the VM1-IE-1G-local-Snapshot1**.vmem** file, **Shift + R Click and Select "Copy for Path".** Once it is in the clipboard it can be pasted in the Command Prompt which eliminates typing errors and saves a great deal of time. Useful commands for this project include:

1. $ **python vol.py clipboard -f image_name.vmem --profile=Win7SP1x86** which was very useful in identifying data that had been copied to the clipboard.
2. $ **python vol.py clipboard –v -f image_name.vmem --profile=Win7SP1x86** (Verbose displays Hex Values and also a text field).
3. $ **python vol.py imageinfo –f image_name.vmem --profile=Win7SP1x86**

4. $ **python vol.py pslist –f image_name.vmem --profile=Win7SP1x86**
5. $ **python vol.py dlllist -f image_name.vmem --profile=Win7SP1x86**
6. $ **python vol.py verinfo –f image_name.vmem --profile=Win7SP1x86**

Exporting a Volatile Command to an Output File includes:

1. Open the Command Prompt Window
2. **C:\Python27\volatility-master> vol.py –f " Path to vmem file" - - profile= Win7SP1x64 ldrmodules - - output-file= "Path to Desktop Folder\something.txt"**
3. The memory file and output file were both entered by highlighting them, then **select Shift + R Click and Select "Copy to Path"** and paste them in the Command Line.
4. The output file "something.txt" is created and can be placed in the Desktop Folder named "Command Line Exports".

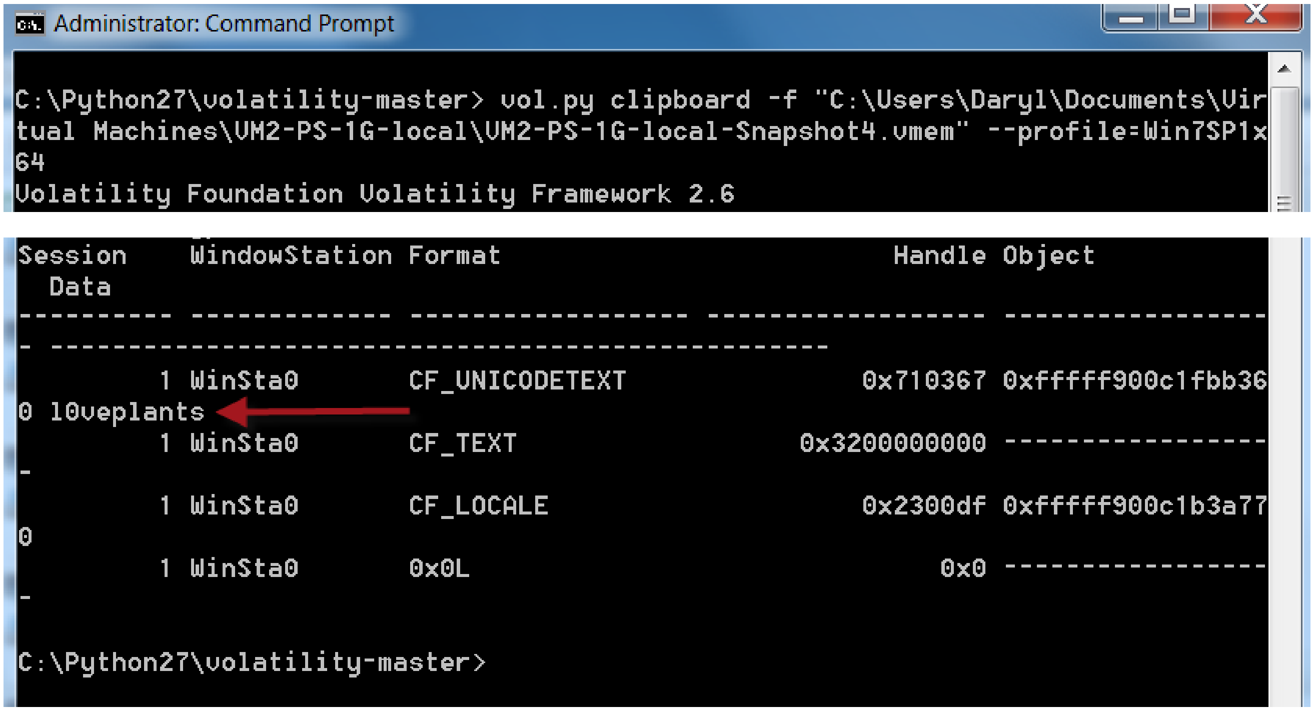
Executing Volatility Commands

The process of executing Volatility commands on the virtual machines in this project involved testing a variety of modules to see which would produce usable data sets. One of the most useful Python Volatility modules was the "clipboard". It would scan the virtual memory file created from each Trial Event and return data that had been stored from the Copy to Clipboard or Copy and Paste routines.

While testing the KeePass virtual machines VM1, VM3, VM5 and VM7 with the Volatility-Clipboard module it was observed that no data sets that had been processed with "Copy to Clipboard" would appear. This was consistent with what was observed during Trial Test 4 (Copy to Clipboard). While using KeePass since the Copy command displays a message in the user interface window indicating there are 10 seconds to copy. If the item is not pasted within that time frame the data is no longer available within the Clipboard. It was very difficult to copy an item in KeePass to the clipboard and have enough time to create the appropriate Snapshot within the virtual machine to capture that data from the clipboard.

However, while testing VM2, VM4, VM6 and VM8 Password Safe did not delete the data from the Copy to Clipboard process which provided enough time to complete Trial Event 4 (Copy to Clipboard) and create the corresponding Snapshot for the test. Several passwords from the Bluesky database were repeatedly copied to the clipboard, one after the other in an attempt to challenge the memory resources.

It was discovered that since Password Safe allowed the data to remain on the clipboard long enough during repeated commands for (Copy to Clipboard), the 1 Gig of RAM configuration caused the program to fail and allowed a password “l0veplants” to appear in plain text. The password was associated with Franco Nursery and user name bossman1. See Fig.21 below for a screenshot of this activity.

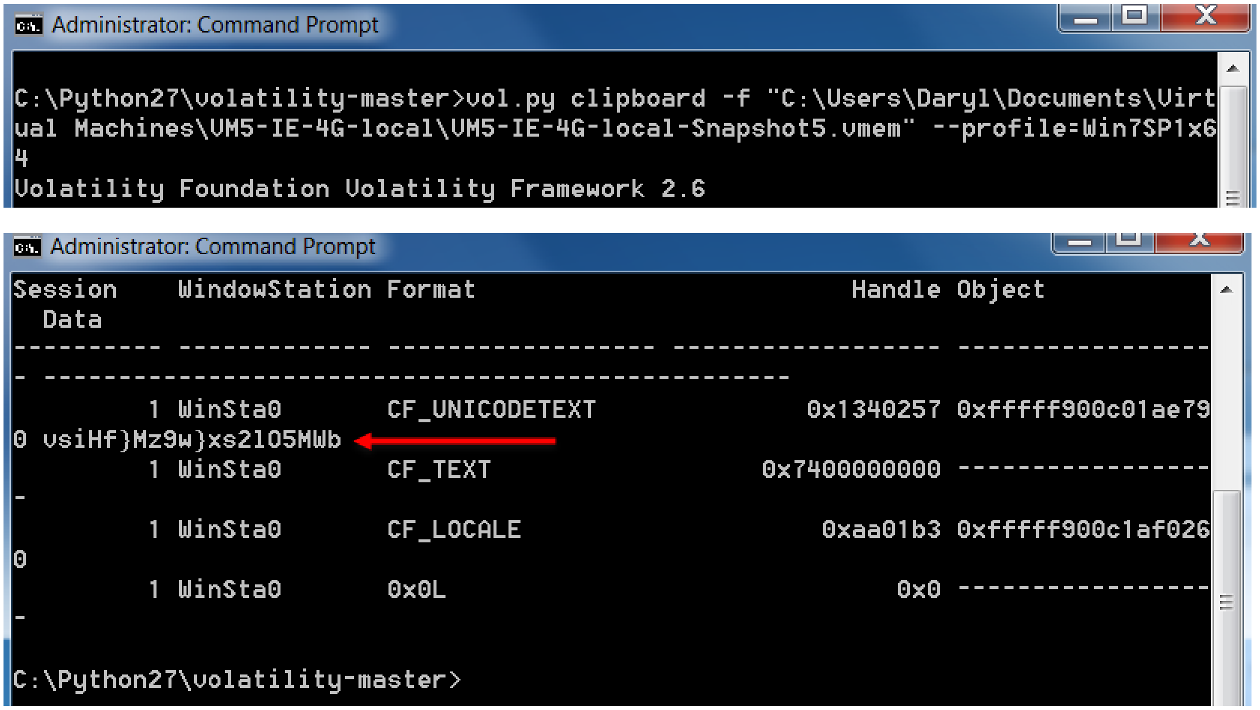


```
C:\Python27\volatility-master> vol.py clipboard -f "C:\Users\Daryl\Documents\Vir
tual Machines\VM2-PS-1G-local\VM2-PS-1G-local-Snapshot4.vmem" --profile=Win7SP1x
64
Volatility Foundation Volatility Framework 2.6
```

```
Session    WindowStation Format                         Handle Object
  Data
---------- ------------- ------------------ ------------------ -----------------
- --------------------------------------------------
         1 WinSta0       CF_UNICODETEXT               0x710367 0xfffff900c1fbb36
0 l0veplants
         1 WinSta0       CF_TEXT                  0x3200000000 -----------------
-
         1 WinSta0       CF_LOCALE                    0x2300df 0xfffff900c1b3a77
0
         1 WinSta0       0x0L                              0x0 -----------------
-

C:\Python27\volatility-master>
```

Figure 21. This is a Volatility Command Line screenshot depicting Password Safe VM2-PS-1G-local-Snapshot4.vmem (Copy to Clipboard) with “l0veplants” appearing in plain text.

The KeePass (Copy and Paste) operation was also tested with the Volatility Framework to see if it too could avoid disclosing previously encrypted passwords. This involved VM5-IE-4G-local-Snapshot5 (Copy and Paste). In this Trial Event the test involved sequential copying of passwords and pasting them into the Notes section of the KeePass user interface. This was done fast and repetitive with the intent of overloading memory resources.



```
C:\Python27\volatility-master>vol.py clipboard -f "C:\Users\Daryl\Documents\Virt
ual Machines\VM5-IE-4G-local\VM5-IE-4G-local-Snapshot5.vmem" --profile=Win7SP1x6
4
Volatility Foundation Volatility Framework 2.6
```

```
Session    WindowStation Format                  Handle Object
  Data
---------- ------------- ------------------ ------------------ ----------------
- --------------------------------------------------
         1 WinSta0       CF_UNICODETEXT           0x1340257 0xfffff900c01ae79
0 vsiHf}Mz9w}xs2105MWb
         1 WinSta0       CF_TEXT              0x7400000000 ----------------
-
         1 WinSta0       CF_LOCALE                0xaa01b3 0xfffff900c1af026
0
         1 WinSta0       0x0L                          0x0 ----------------
-

C:\Python27\volatility-master>
```

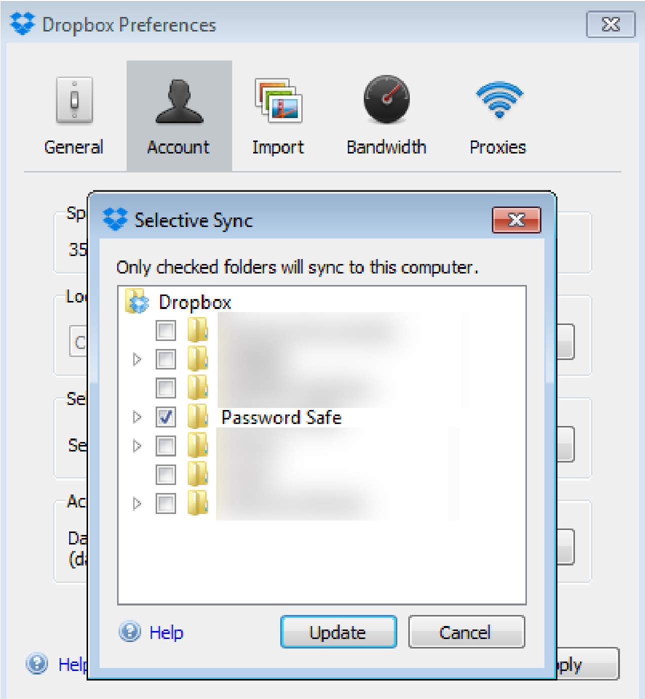
Figure 22. This is a Volatility "clipboard" screenshot depicting KeePass VM5-IE-4G-local-Snapshot5.vmem (Copy and Paste) with "vsiHf}Mz9w}xs2105MWb" appearing in plain text.

The Notes section usually remains encrypted and unavailable to users that are not authenticated. Reviewing Fig. 22 above indicates that a password "vsiHf}Mz9w}xs2105MWb" previously generated by the Password Generator and then copied and pasted into the Notes section does appear in plain text.

Wireshark Network Protocol Analysis

The network protocol analyzer Wireshark version 2.2.5 was utilized to record KeePass and Password Safe data as it was synchronized between the Dropbox cloud server and the corresponding virtual machine. Virtual machines VM3, VM4, VM7 and VM8 were configured to have the password manager's data stored on the Dropbox server and synchronized to a Dropbox folder. A specific scientific methodology was utilized to assure that the synchronizing data was handled uniformly which included configuring Dropbox to only allow the KeePass or

Password Safe databases to be transferred as seen in Fig. 23. This helped to control the amount and type of data transferred during the synchronization process that needed be filtered by Wireshark.



Only checked folders will sync to this computer.

☑ Password Safe

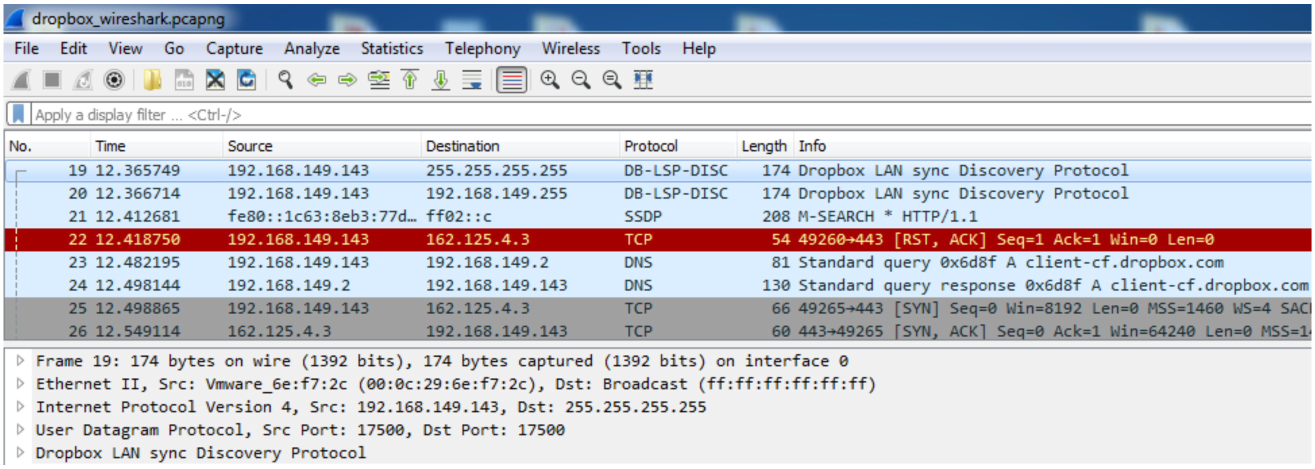
Figure 23. This process allowed only the desired database manager to be synchronized with Dropbox which in this case the box checked is for Password Safe.

Another important aspect was to assure that the current Dropbox directory on the virtual machine was empty so the specific password manager files would synchronize when the process was initiated. The specific process can be described as:

1. Click on the Dropbox icon in the System Tray.
2. Pause or stop the Dropbox Syncing process until Wireshark is active.
3. Click on the gear icon to adjust Sync Settings.
4. Select "Preferences" and then the "Accounts" tab.
5. Click on the "Selective Sync" button which brings up the dialog box in Fig. 23.

6. Place a checkmark on only the folder that is desired to be synchronized.
7. Close the open windows and assure that the System Tray icon is still “Paused”.
8. Check the Dropbox directory on the virtual machine remains empty.
9. Start Wireshark and begin capturing network traffic.
10. Click on the Dropbox System Tray icon to start the synchronization of the password manager located on the Dropbox cloud server.
11. Note that Dropbox will alert when the synchronization begins and confirm when completed.
12. Stop Wireshark from capturing network traffic.
13. Check the Dropbox directory on the virtual machine contains the proper password manager.
14. Save the captured Wireshark network traffic for analysis.

See Figure 24 below for example of a captured Wireshark network traffic sample at the time that Dropbox was executed to begin the synchronization of Password Safe and the virtual machine.


dropbox_wireshark.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source                  Destination      Protocol    Length Info
   19 12.365749  192.168.149.143         255.255.255.255  DB-LSP-DISC    174 Dropbox LAN sync Discovery Protocol
   20 12.366714  192.168.149.143         192.168.149.255  DB-LSP-DISC    174 Dropbox LAN sync Discovery Protocol
   21 12.412681  fe80::1c63:8eb3:77d…    ff02::c          SSDP           208 M-SEARCH * HTTP/1.1
   22 12.418750  192.168.149.143         162.125.4.3      TCP             54 49260→443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   23 12.482195  192.168.149.143         192.168.149.2    DNS             81 Standard query 0x6d8f A client-cf.dropbox.com
   24 12.498144  192.168.149.2           192.168.149.143  DNS            130 Standard query response 0x6d8f A client-cf.dropbox.com
   25 12.498865  192.168.149.143         162.125.4.3      TCP             66 49265→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACI
   26 12.549114  162.125.4.3             192.168.149.143  TCP             60 443→49265 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1

▷ Frame 19: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface 0
▷ Ethernet II, Src: Vmware_6e:f7:2c (00:0c:29:6e:f7:2c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Internet Protocol Version 4, Src: 192.168.149.143, Dst: 255.255.255.255
▷ User Datagram Protocol, Src Port: 17500, Dst Port: 17500
▷ Dropbox LAN sync Discovery Protocol
```

Figure 24. This Wireshark network traffic sample was captured when Dropbox Synchronization was initiated on VM8 to allow the virtual machine access to the password manager residing on the Dropbox cloud server.

The objective was to assure that the original desktop Dropbox folder was empty prior to executing the Wireshark analyzer. Once Wireshark was actively capturing network traffic then Dropbox Synch was initiated.

Capturing of network traffic between the Dropbox cloud server and the virtual machine that was accessing the password manager database was accomplished to assure protocol integrity. It was important to evaluate the client-server processes that were occurring during the time that the password manager databases were synchronizing between the virtual machine and the Dropbox cloud server. No malformed data packets were observed and standard client – server responses were present. Additional Dropbox and Wireshark screenshots can be viewed in Appendix H.

Chapter 5 – Analysis

Summary of Findings

The execution of Trial Events captured within each virtual machine snapshot provided some insight into processes that were occurring behind the scenes. One important aspect that surfaced is that as the progression was made from Trial Event 1 to Trial Event 8 within each virtual machine there was an accumulated strain on system resources. This was due to the way in which VMWare Snapshots capture events and machine state prior to taking the next Snapshot. The following passage will help summarize the findings and answer research questions.

Research question #1. Does the Master Key or underlying secured credentials for databases protected by the KeePass and Password Safe software become vulnerable to discovery within digital artifacts on disk when there are low memory resources?

The information gathered from FTK dtSearches on passwords are displayed in Table 6 from Chapter 4 and help visualize the accumulating password hits as you examine the data from left (Trial Event 1) to right (Trial Event 8). Key insights include that a greater number of password hits from FTK dtSearch occur early in the process within the 1G RAM configurations of both KeePass and Password Safe; but then as 4G RAM resources are consumed those configurations indicate an increasing number of password hits. This suggests that the 1G RAM configurations may fail early and expose protected data but as the resources are increasingly strained, eventually a 4G RAM configuration may also fail to provide full encryption of data.

A rather significant finding was when an FTK dtSearch was executed on the Master Key passwords for KeePass “WX[secretp@ssword]YZ” and Password Safe “AB[n0accesshere]CD” they were located in plain text within the 1G RAM configurations. The KeePass Master Key was identified during the initial login of Trial Event 1 however the Password Safe Master Key was identified during Trial Event 6 (Export Database). Password Safe 1G RAM configurations did not yield the plain text Master Key until late in the process where Password Safe requires re-authentication prior to exporting data. No Master Keys from either KeePass or Password Safe were located in 4G RAM configurations from FTK, EnCase or Volatility.

Research question #2. Is there recoverable data from memory while utilizing FTK or Volatility when examining VMWare Snapshots? Discovering the digital artifacts with FTK from (.vmem) files created by VMWare Snapshots was productive and documented in Chapter 4. Additional interesting processes were discovered utilizing the Python Volatility Memory Analysis Framework. Volatility helped to identify data that was processed by Copy to Clipboard or the Copy and Paste Trial Event. The "clipboard" module in Volatility was instrumental in locating data within memory that had been placed on the Clipboard as seen in Figure 21.

Since KeePass restricted the amount of time data can remain on the Clipboard it was difficult to capture before it was automatically deleted. Volatility was able to capture passwords in plain text from Password Safe within a 1 G RAM configuration Figure 21 and from KeePass on a 4 G RAM configuration Figure 22.

Research question #3. Does moving the database from the local machine to a cloud environment such as Dropbox elicit observable differences in the discovery of digital artifacts? There was a noticeable delay in processing when any of the 1G RAM configurations were used to synchronize the password database to the virtual machine from Dropbox. This was especially true when Trial Event 6 (Export Database) was executed.

However, once adequate memory and system resources were allocated to the virtual machine there was no detectable difference between running KeePass and Password Safe locally or from a synchronized folder on Dropbox. One additional test that was performed on the 4G configurations of KeePass and Password Safe was to utilize Wireshark network protocol analyzer within the virtual machine. This allowed all of the network traffic to be captured during the synchronization process and assure that proper client-server communication was consistent between the virtual machine being tested and the Dropbox cloud server. The expected connection protocols completing a three way handshake between the client and cloud server existed. There were no malformed data packets to indicate a problem during synchronization.

Research question #4. Will KeePass with AES/Rijndael and Password Safe with Two Fish algorithms perform equally in protecting underlying data when subjected to the scheduled Trial Events? Finally there is the issue of whether KeePass with AES/Rijndael and Password Safe with Two Fish algorithms performed equally well under similar conditions. The answer to that question is both of these password managers performed equally well. Each system had one occasion while under intense system processing and low memory resources that it failed to fully encrypt the Master Key Password. Verification of this anomaly can be viewed in Figure16 and Figure17 which was discovered with FTK dtSearch.

KeePass has the benefit of restricting the time that data is available for Copy to Clipboard operations and therefore making it more difficult to capture. Password Safe requires re-authentication for data Export and does not allow Print operations on any database. These attributes help to prevent digital artifacts from being stored on disk and located with forensic tools. See Table 7 below which helps to visualize the summary of findings and the Trial Events.

Table 7

Trial Event Summary of Findings Table

Trial ID	Test Description	Expected Results	Actual Results
Trial Event #1	Authentication with the Master Key will occur on VMs with 1 Gig of RAM and 4 Gig of RAM configurations.	Previous study indicated that when RAM is limited the Master Key can be found in the Windows Page File (pagefile.sys). However that was reportedly fixed in KeePass ver. 2.34.	Master Key for KeePass was discovered in memory only during Login with Master Key and 1G RAM on VM1.
Trial Event #2	Password Generator will be used to create complex passwords.	Passwords will remain in an encrypted state throughout all phases of the test.	None of the passwords created by the KeePass or Password Safe password generators were detected except those Copy and Pasted to the Notes section.
Trial Event #3	Perform Auto-Type on form fields to enter login data on local database and from Dropbox.	Passwords will remain in an encrypted state throughout all phases of the test.	Passwords were detected in memory for KeePass and Password Safe especially in the 1g RAM configurations.
Trial Event #4	Copy data to Clipboard in the form of Notes and Login data.	Expectations are that all of the data within the database will remain encrypted both in memory and on disk.	KeePass Copy to Clipboard had a time limit which when expired, deleted the contents. Password Safe did not have such constraints and allowed more data to be copied.
Trial Event #5	Copy and Paste operation for login data and Notes. It is a different menu item than Copy to Clipboard.	Passwords will remain in an encrypted state throughout all phases of the test.	The rapid Copy and Paste required by KeePass to defeat the deletion from Clipboard was replicated in Password Safe with both 1G RAM configurations exposing data.
Trial Event #6	Export database to CSV, HTML, Native KeePass and Password Safe formats.	Previous studies indicated that exports in HTML could be viewed with a web browser and that after deletion it remained in the Recycle Bin.	Master Key for Password Safe was discovered in memory only during Database Export with 1G RAM on VM4. Password Safe requires a second login during Export. Deleted Exports of both databases could be recovered from TEMP files.

Trial Event **#7**	Print database entries and also disrupt a Print function.	Failed Print operation allows the database to appear in the Temp Folder in plain text.	Password Safe does not offer a Print Database option. KeePass automatically deletes Temp Folders however they can be recovered by EnCase Forensic Examiner producing the entire database.
Trial Event **#8**	Delete the database named “Clouds” or “Bluesky” that were created for this project.	Expectations are that all of the data within the database will remain encrypted both in memory and on disk.	Deleting the Databases for KeePass and Password Safe did not disclose new information. They could not be located in Recycle Bins.

Lessons Learned

Consider a robust VM architecture. During the initial planning of the project there was a great deal of time expended on estimating the amount of computing resources that would be required to run eight virtual machines. The host machine was selected based on these estimations. One specific area that was overlooked in the initial project planning was the enormous amount of space would be required to store the VMWare Snapshot data. Once the testing phase had begun it became clear that every time a Snapshot was recording an event test it was also creating an entirely new instance of the Windows 7 Pro operating system. Even though this was only a 6-7 Gigabyte requirement per Snapshot, there were eight snapshots to record the Trial Events consuming approximately 50 Gig of disk space for each VM. The eight VM configurations in this project consumed approximately 400 Gig of total disk space.

EnCase, FTK and Volatility. Guidance Software’s EnCase 7 requires a robust internet connection to maintain authentication services or a licensed dongle. Interruption of internet service and connection for authentication of EnCase will cause a “Dongle Removed” alert, stopping all evidence processing. In many cases the acquisition and processing may have to be started from the beginning which can mean hours of lost processing time.

AccessDatas's FTK and FTK Imager were very handy tools since FTK Imager was easily able to image the host machine and each individual virtual machine disk file created by a VMWare Snapshot. FTK processed the image files quickly and provided excellent search capabilities for data located in the (.vmem) virtual memory files.

The Python Volatility Memory Analysis Framework was also helpful in analyzing the (.vmem) files created during snapshot sessions. Volatility modules such as imageinfo, verinfo, pslist and especially clipboard were helpful in providing insight from the same memory files.

Potential Data Duplication. Once the Copy and Paste Trial Event 5 is accomplished all subsequent Trial Events may contain that data located in the Notes section where it was pasted. Even though the Notes section is supposed to be encrypted it may appear if content from that section is printed or exported in plain text and may cause a duplication of dtSearch hits. One way to mitigate this issue would be to move Copy to Clipboard, Copy/Paste and Print so they are the last Trial Event tests to be conducted or conduct them as isolated tests.

Conclusion

In this paper, a project is presented that creates a robust virtual test environment designed specifically to evaluate the KeePass and Password Safe open source password management features. The design includes constructing a host machine that houses eight VMWare Workstation virtual machines (VM) configured to test the effectiveness of the software products features under variable conditions. In particular, the VM configurations consist of cloned Windows7 Pro instances of 1G and 4G RAM; these configurations also included running the password manager from the local machine or as a synchronized Dropbox folder.

Each VM was assigned an independent Computer Name that corresponded to the specific VM name to help identify computer processes during the examination phase. Specific test methods defined as Trial Events were integrated into the file name to further assist in the identification of searching data. Once the design of the VM architecture has been established, the Trial Event testing criteria and specific needs of an organization can be easily modified.

This project design allows the testing of password management tools isolated from the business network and can help employees provide input pertaining to the software efficiency and usability. Data files that are created by the virtual machines during the testing process can be easily integrated into popular forensic analytical tools. This provides an independent test environment for password managers that can be evaluated for operational fit and integrity.

Next Steps for Further Study

Further study in the future could include a forensic comparison of the KDBX/KDBX4 file system. Starting with the KeePass 2.35 version the user is able to select which file system and encryption algorithm that they would prefer to use with the password management scheme (Reichl, 2016). KDBX version 3.1 utilizes the AES-KDF encryption algorithm (default) for key derivation. KDBX 4 – utilizes Argon 2 as the key derivation function but you must deselect AES-KDF which is the default file structure even in KeePass 2.35. Argon 2 provides better resistance to GPU/ASIC brute force attacks (Reichl, 2016).

Another area of study that may prove to be fruitful would include a similar virtual machine platform utilized in this study but with a focus on relevant malware directed at password manager products. This could also include malware that affects a mobile app. Specifically, those intended to install keylogger type malware in an attempt to obtain the Master Key during the user login session. A password manager that is vulnerable to a keylogger attack would negate any benefit from the development of a password protection strategy.

References

Bang, Y., Lee, D., Bae, Y. & Ahn, J. (2012). Improving information security management: An analysis of ID-password usage and a new login vulnerability measure. *International Journal of Information Management*, 32, (5), p. 409-418. Retrieved from http://dx.doi.org/10.1016/j.ijinfomgt.2012.01.001

Blocki, J. & Sridhar, A. (2016). Client-CASH: Protecting master passwords against offline attacks. *The Association of Computing Machinery – Asia CCS*, p.165-176. DOI: 10.1145/2897845.2897876

Gray, J., Franqueira, V. & Yu, Y. (2016). Forensically sound analysis of security risks when using local password managers. *1st International Workshop on Requirements Engineering for Investigating and Countering Crime, 5, p. 114-121.* Retrieved from http://oro.open.ac.uk/46871/

Gogolin, G. (2013). *Digital forensics explained*. Boca Raton, FL: CRC Press Taylor & Francis Group.

Harwood, M. (2011). *Security strategies in web applications and social networking*. Burlington, MA: Jones and Bartlett Learning.

Hirwani, M., Pan, Y., Stackpole, B. & Johnson,D. (2012). Forensic acquisition and analysis of VMWare virtual hard disks. *Rochester Institute of Technology RIT Scholar Works*, p. 255-259. Retrieved from http://scholarworks.rit.edu/other/297

Hellekalek, P. & Wegenkitti, S. (2003). Empirical evidence concerning AES. *ACM Transactions on Modeling and Computer Simulations*, 13 (4), p. 322-333. doi:http://doi.acm.org/10.1145/945511.945

Hu, D. (2015). *Professor Lorrie Cranor gives a lecture on password security*. Carnegie Mellon Student Newspaper: The Tartan. Retrieved from http://thetartan.org/2015/2/23/scitech/passwords

Kent, K., Chevalier, S., Grance, T. & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *National Institute of Standards and Technology (Special Publication 800-86).* DOI 10.6028/NIST.SP.800-86

Mahajan, R. (2010). Microsoft Research: How to build a research system in your spare time. *ACM SIGCOMM Computer Communication Review,* 40, (2), p. 60-65. DOI 10.1145/1764873.1764884

Maurer, U. & Tackman, B. (2010). On the soundness of authenticate-then-encrypt. *Proceedings of the 17th ACM Conference on Computer and Communications Security*, p. 505-515. DOI: 10.1145/1866307.1866364

McGraw, G. (2006). Software security: Building security in. Boston, MA: Pearson Education.

Michail, H., Athanasiou, G., Kelefouras, V., Theodoridis, G. & Goutis, C. (2012). On the exploitation of a high throughput SHA-256 FPGA design for HMAC. *ACM Transactions on Reconfigurable Technology and Systems*, 5 (1), p. 1-28. DOI: 10.1145/2133352.2133354

Reichl, D. (2016). *KeePass Help Center: Changes in KeePass 2.35*. Retrieved from http://keepass.info/news/n170109_2.35.html

Reichl, D. (2016). *KeePass Help Center: Changes from the kdbx 3.1 file format to kdbx 4*. Retrieved from http://keepass.info/help/kb/kdbx_4.html#argon2.

Ruff, N. (2008). Windows memory forensics. *Journal in Computer Virology*, (4), 2, p. 83-100. DOI: 10.1007/s11416-007-0070-0

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C. & Ferguson, N. (1998). TwoFish: A 128 bit block cipher. *NIST AES Approval*, (15), 1, p. 1-27. DOI: 10.1.1.35.1273

Schneier, B. (2016). *Schneier on security: Password Safe.* Retrieved from https://www.schneier.com/academic/passsafe/

Shavers, B. (2008). Virtual Forensics: A discussion of virtual machines related to forensics analysis. *Forensic Focus*, 1-35. Retrieved from http://www.forensicfocus.com/downloads/virtual-machines-forensics-analysis.pdf

Stewart, J., Chapple, M., & Gibson, D. (2012). *CISSP: Certified information security professional study guide (6th ed.)*. Indianapolis, IN: John Wiley & Sons Inc.

Sobti, R. & Ganesan, G. (2016). Analysis of quarter rounds of Salsa and ChaCha core and proposal of an alternative design to maximize diffusion. *Indian Journal of Science and Technology*, 9, (3), p. 1-10. Retrieved from http://www.indjst.org/index.php/indjst/article/view/80087/67062

Trujano, F., Chan, B., Beams, G. et al. (2016). *Security analysis of DJI Phantom Standard*. Retrieved from https://courses.csail.mit.edu/6.857/2016/files/9.pdf

Ur, B., Segreti, S., Bauer, L., Christin, N., Cranor, L. et al (2015). *Measuring real world accuracies and biases in modeling password guessability*. 24th Usenix Security Symposium. Retrieved from https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-ur.pdf

VMWare. (2017). VMWare Knowledgebase. Understanding vm snapshots. Retrieved from https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1015180 .

Zhao, R. & Yue, C. (2013). All of your browser based passwords could belong to us: A security analysis and a new cloud based design. *CodaSpy* , p. 333-340. Retrieved from http://dl.acm.org/citation.cfm?id=2435397

Appendix A

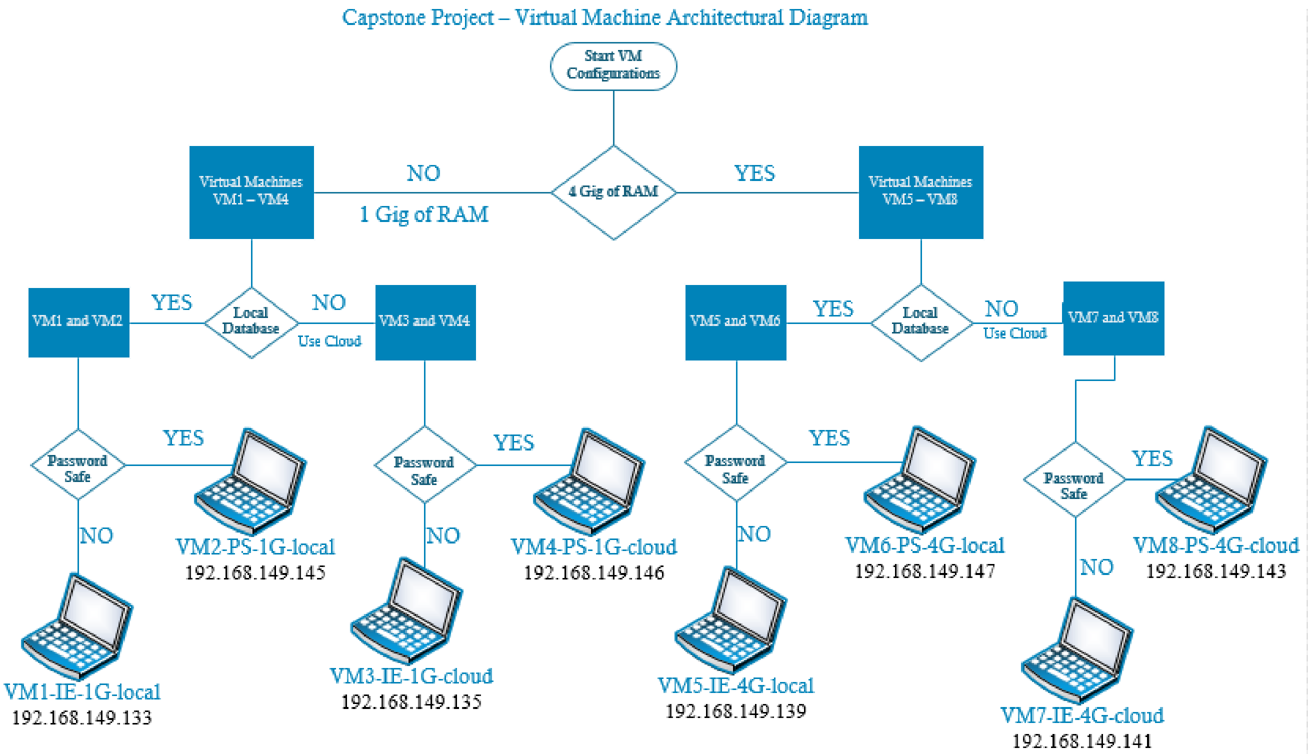


Figure 25. This diagram depicts the variations in virtual machine configurations that were used to conduct Trial Event testing of the KeePass and Password Safe password managers. Note the naming convention of the virtual machines include **IE**= KeePass, **PS** = Password Safe **1G** = 1 Gig RAM, **4G** = 4 Gig RAM, **local** = local database and **cloud** = cloud database (Dropbox).

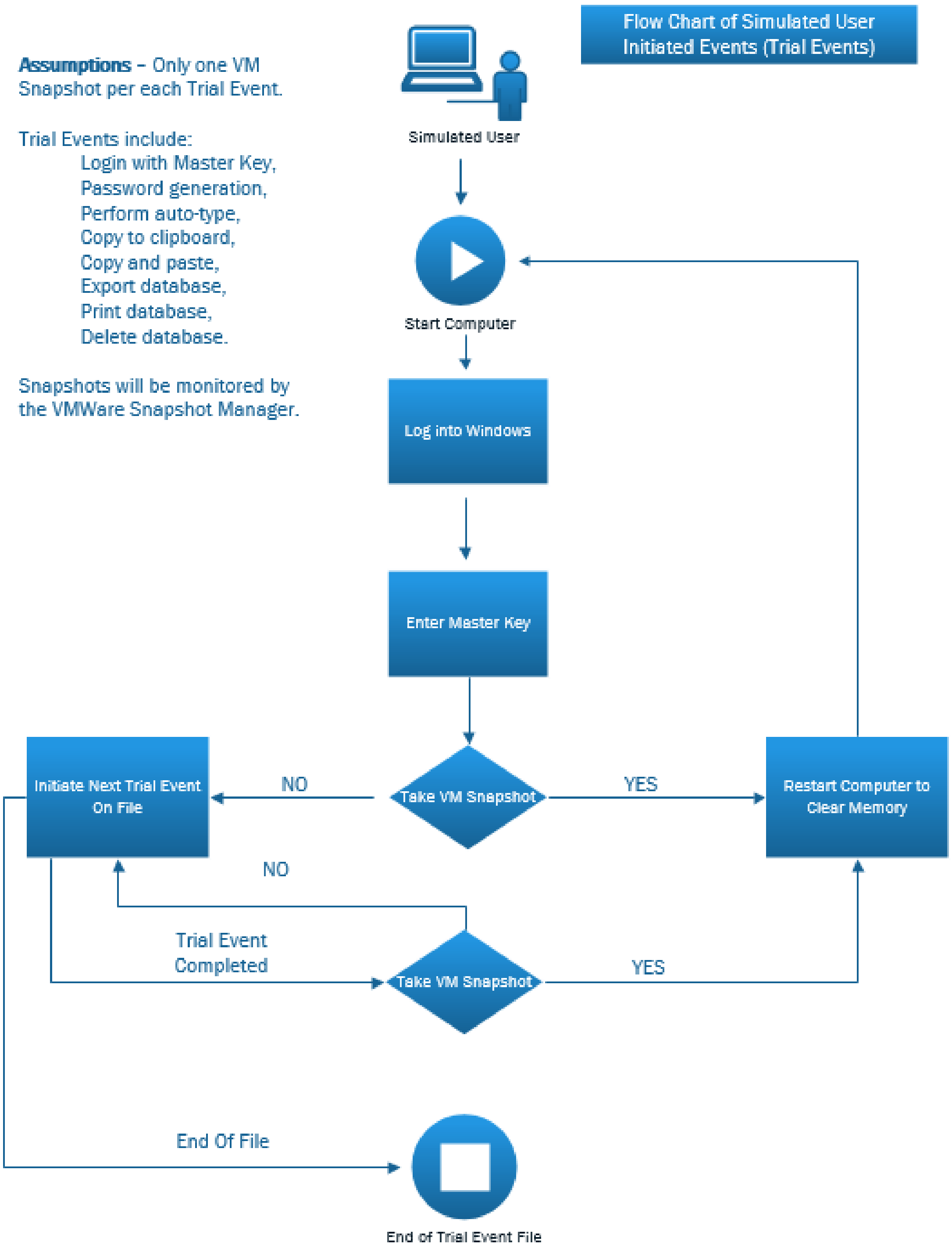


Figure 26. Flowchart of simulated user initiated events (Trial Events) that represent part of the scientific process for assuring that actions were consistently captured within each of the virtual machines during the testing process.

Table 8

VMWare Virtual Machine IP Addresses

Virtual Machine	IP Address	Gateway	Subnet Mask
VM1-IE-1G-local	192.168.149.133	192.168.149.2	255.255.255.0
VM2-PS-1G-local	192.168.149.145	192.168.149.2	255.255.255.0
VM3-IE-1G-cloud	192.168.149.135	192.168.149.2	255.255.255.0
VM4-PS-1G-cloud	192.168.149.146	192.168.149.2	255.255.255.0
VM5-IE-4G-local	192.168.149.139	192.168.149.2	255.255.255.0
VM6-PS-4G-local	192.168.149.147	192.168.149.2	255.255.255.0
VM7-IE-4G-cloud	192.168.149.141	192.168.149.2	255.255.255.0
VM8-PS-4G-cloud	192.168.149.143	192.168.149.2	255.255.255.0

Appendix B

This Depicts a Series of VMWare Virtual Machine Screenshots

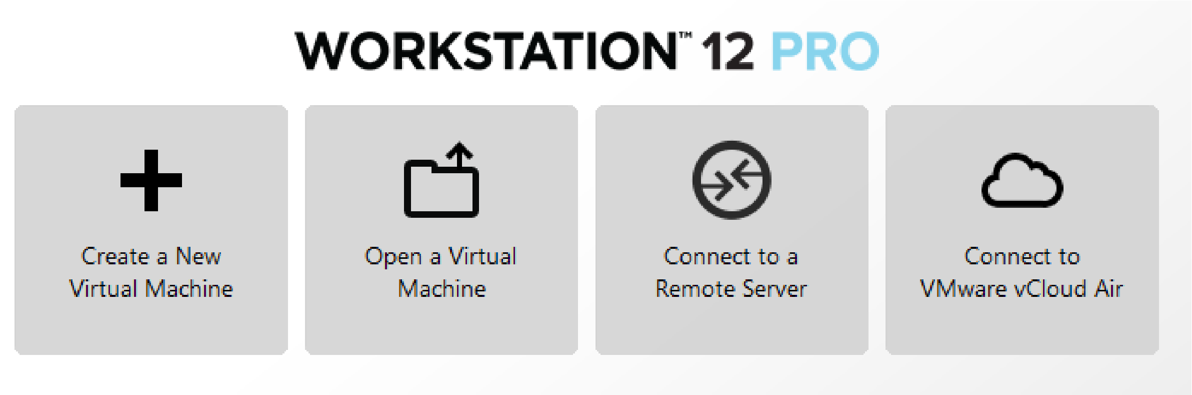
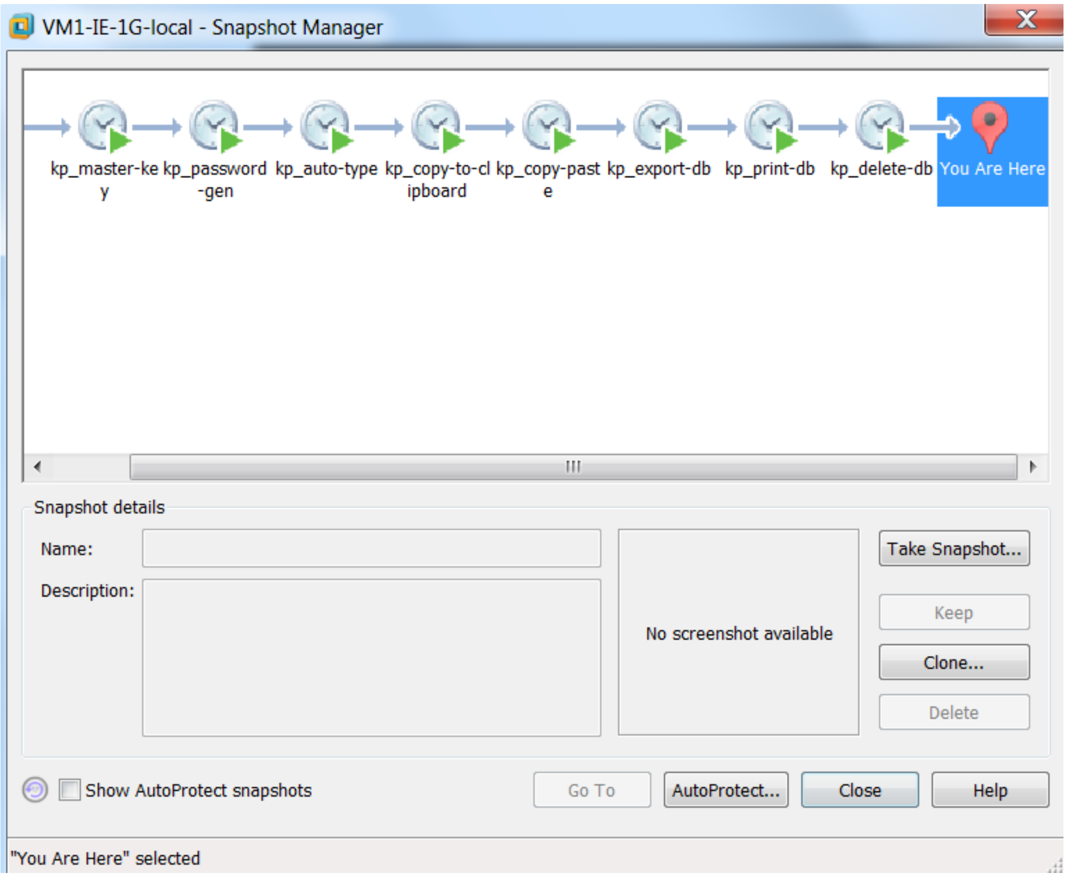

WORKSTATION™ 12 PRO
Create a New Virtual Machine
Open a Virtual Machine
Connect to a Remote Server
Connect to VMware vCloud Air

Figure 27. Initial screen for access to VMWare Workstation 12 Pro.



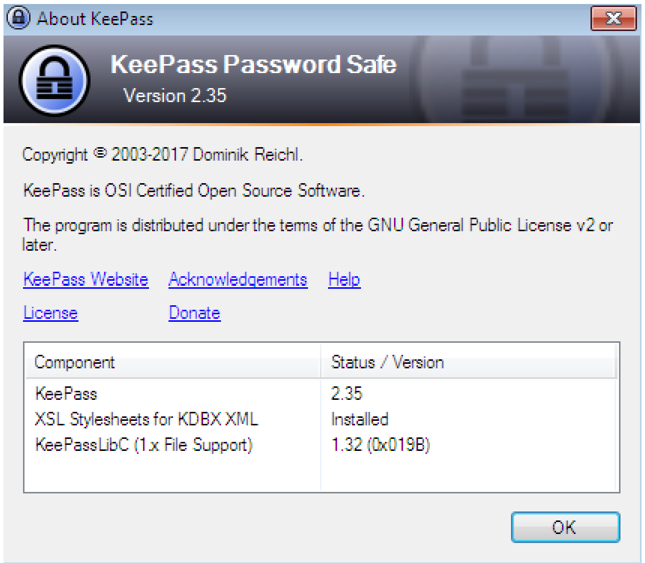
No screenshot available

"You Are Here" selected

Figure 28. This screenshot visualizes the testing process of Snapshots that are recorded with the VMWare Snapshot Manager during the execution of Trial Events.

Appendix C

This Depicts a Series of KeePass Screenshots



About KeePass

KeePass Password Safe

Version 2.35

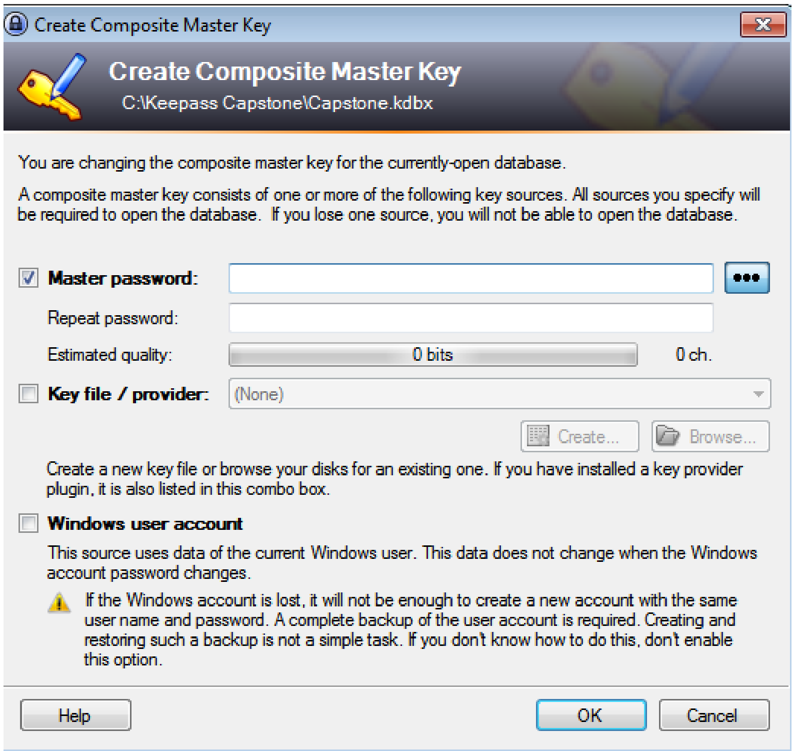
Copyright © 2003-2017 Dominik Reichl.

KeePass is OSI Certified Open Source Software.

The program is distributed under the terms of the GNU General Public License v2 or later.

Component	Status / Version
KeePass	2.35
XSL Stylesheets for KDBX XML	Installed
KeePassLibC (1.x File Support)	1.32 (0x019B)

Figure 29. This screenshot provides version and Open Source information about KeePass 2.35.



Create Composite Master Key

Create Composite Master Key

C:\Keepass Capstone\Capstone.kdbx

You are changing the composite master key for the currently-open database.

A composite master key consists of one or more of the following key sources. All sources you specify will be required to open the database. If you lose one source, you will not be able to open the database.

☑ **Master password:**

Repeat password:

Estimated quality: 0 bits 0 ch.

□ **Key file / provider:** (None)

Create a new key file or browse your disks for an existing one. If you have installed a key provider plugin, it is also listed in this combo box.

□ **Windows user account**

This source uses data of the current Windows user. This data does not change when the Windows account password changes.

If the Windows account is lost, it will not be enough to create a new account with the same user name and password. A complete backup of the user account is required. Creating and restoring such a backup is not a simple task. If you don't know how to do this, don't enable this option.

Figure 30. Dialog box in KeePass for creating the Composite Master Key.

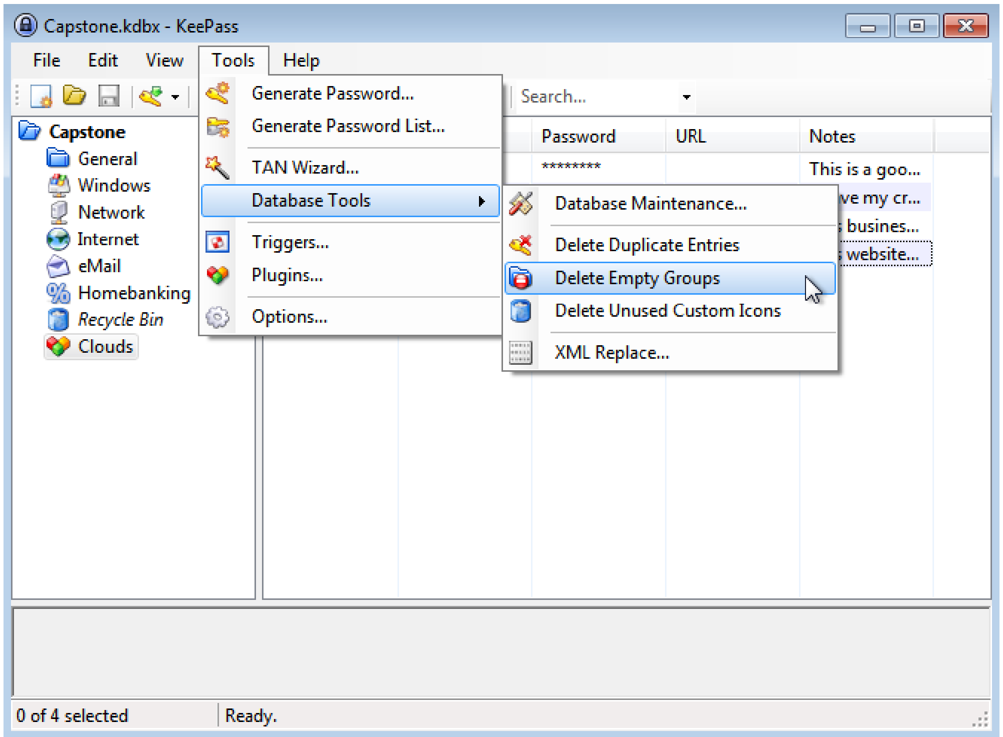
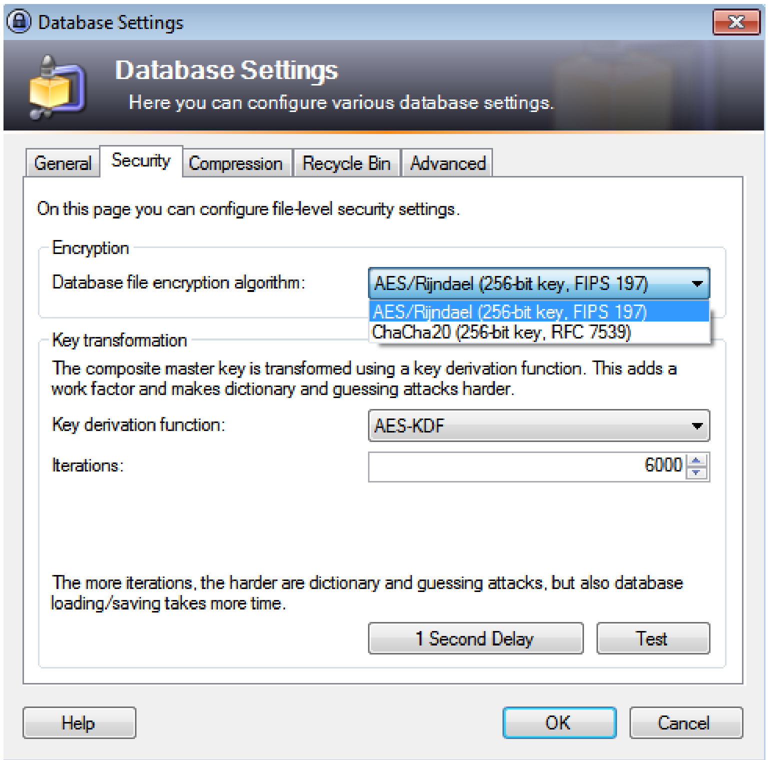


Figure 31. KeePass Database Tools menu options.



Database Settings

Here you can configure various database settings.

On this page you can configure file-level security settings.

Encryption

Database file encryption algorithm: AES/Rijndael (256-bit key, FIPS 197)

AES/Rijndael (256-bit key, FIPS 197)
ChaCha20 (256-bit key, RFC 7539)

Key transformation

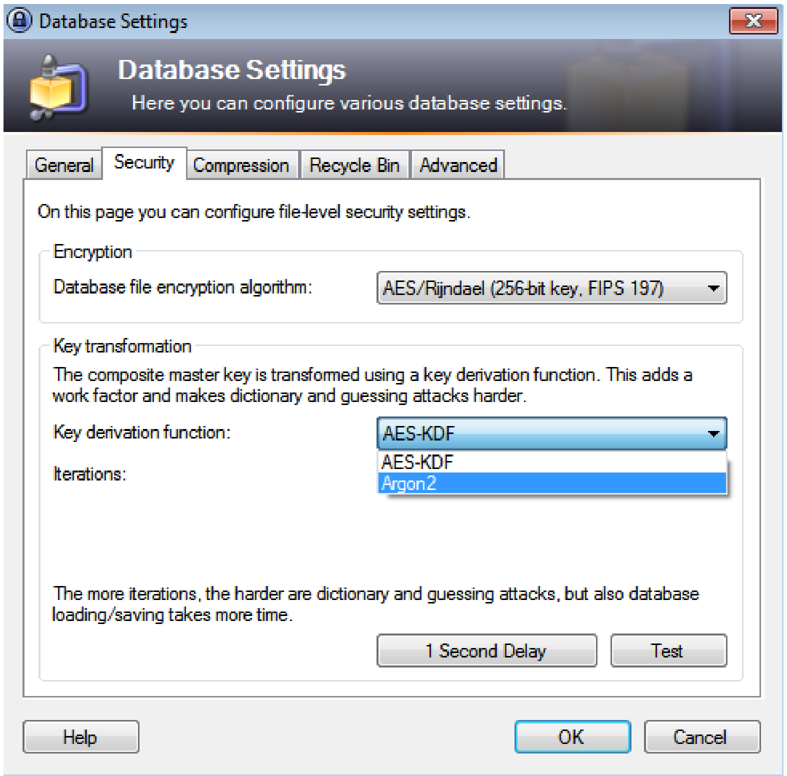
The composite master key is transformed using a key derivation function. This adds a work factor and makes dictionary and guessing attacks harder.

Key derivation function: AES-KDF

Iterations: 6000

The more iterations, the harder are dictionary and guessing attacks, but also database loading/saving takes more time.

Figure 32. Database settings in KeePass for file encryption.



Database Settings

Here you can configure various database settings.

On this page you can configure file-level security settings.

Encryption

Database file encryption algorithm: AES/Rijndael (256-bit key, FIPS 197)

Key transformation

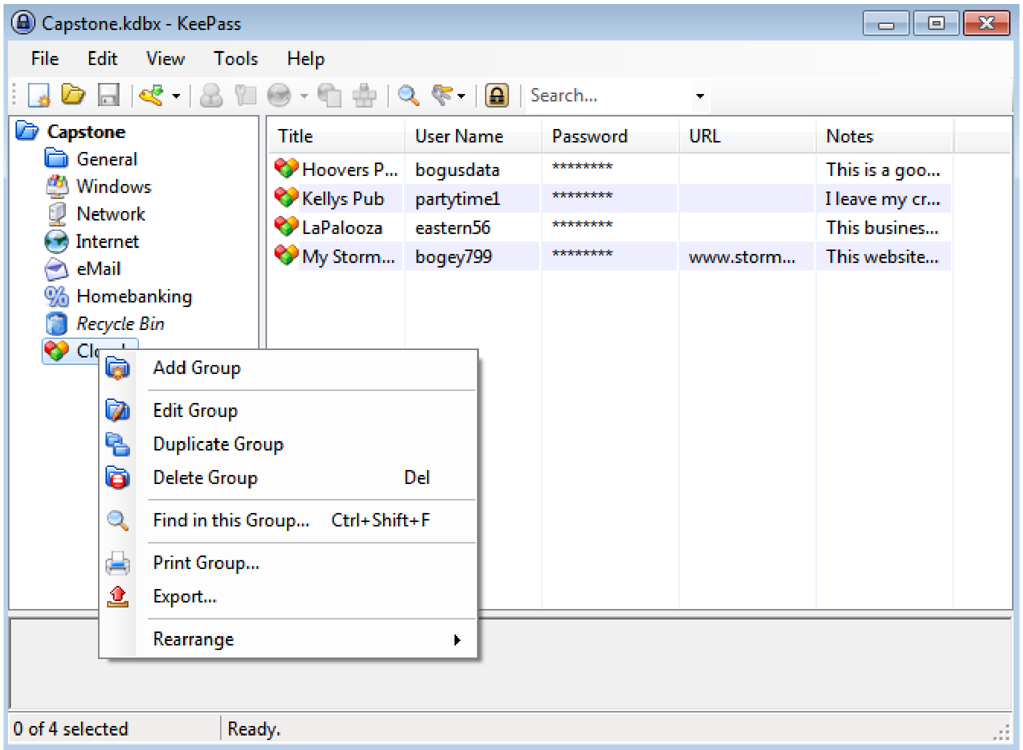
The composite master key is transformed using a key derivation function. This adds a work factor and makes dictionary and guessing attacks harder.

Key derivation function: AES-KDF

Iterations:

The more iterations, the harder are dictionary and guessing attacks, but also database loading/saving takes more time.

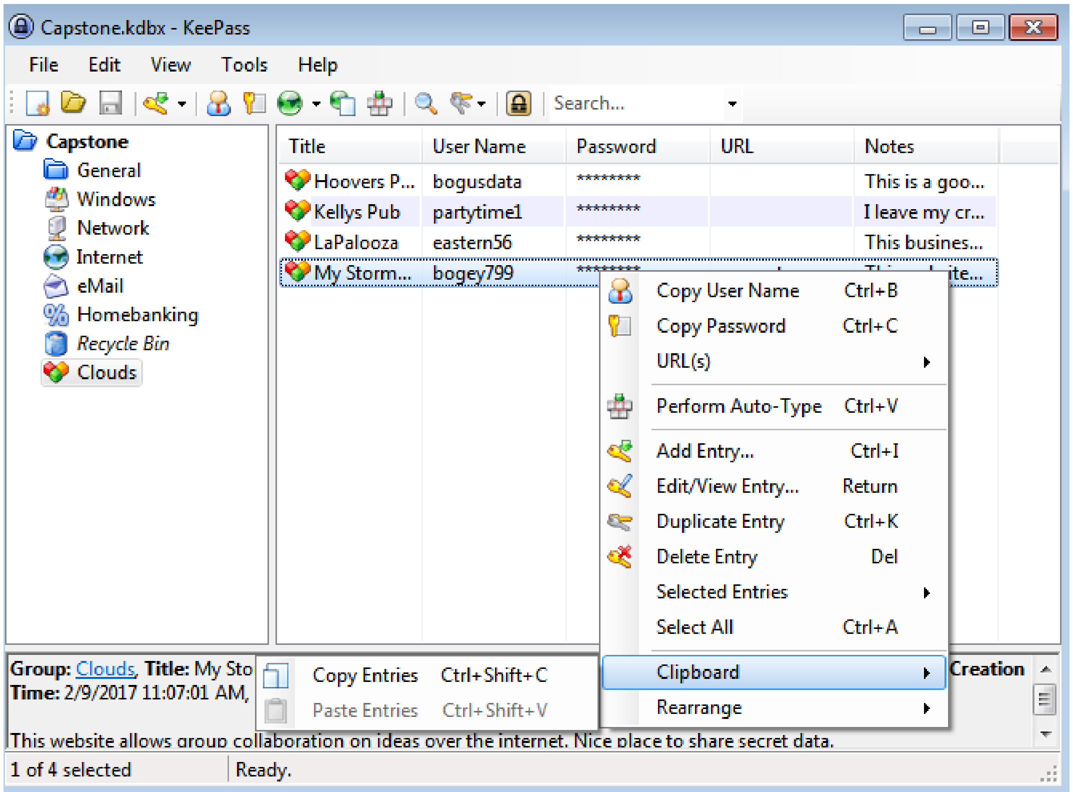
Figure 33. Database settings for KeePass Key Derivation.



Title	User Name	Password	URL	Notes
Hoovers P...	bogusdata	********		This is a goo...
Kellys Pub	partytime1	********		I leave my cr...
LaPalooza	eastern56	********		This busines...
My Storm...	bogey799	********	www.storm...	This website...

0 of 4 selected Ready.

Figure 34. KeePass menu for adding a new database group.



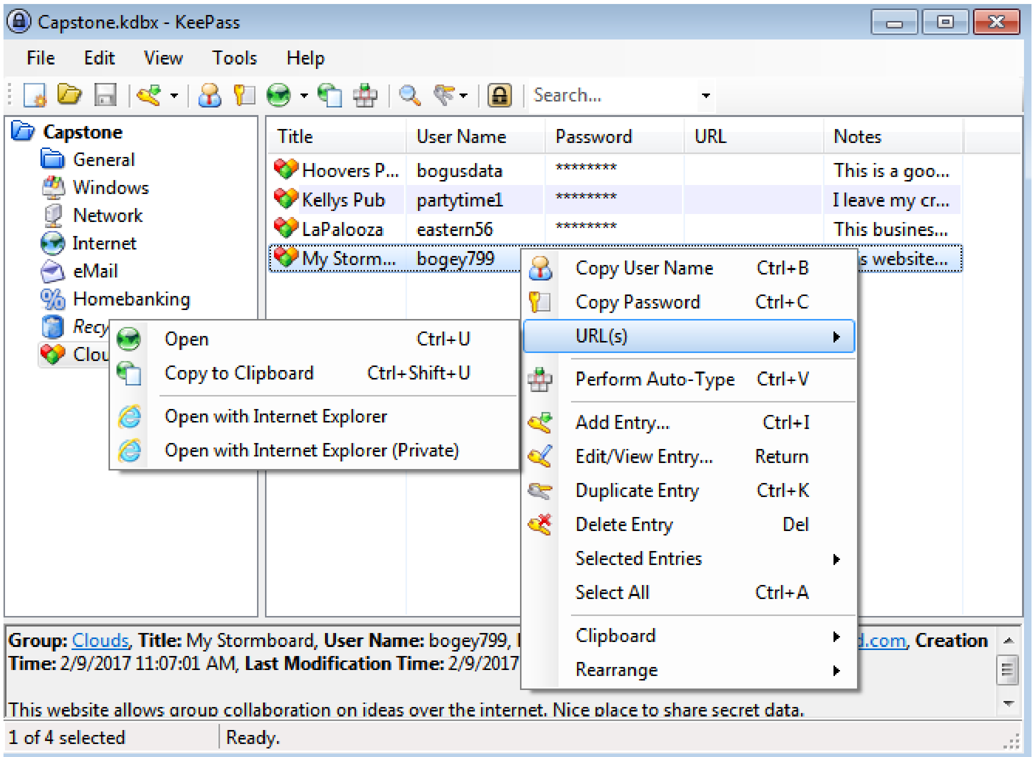
Title	User Name	Password	URL	Notes
Hoovers P...	bogusdata	********		This is a goo...
Kellys Pub	partytime1	********		I leave my cr...
LaPalooza	eastern56	********		This busines...
My Storm...	bogey799	********		ite...

Group: Clouds, **Title:** My Sto **Creation**
Time: 2/9/2017 11:07:01 AM,

This website allows group collaboration on ideas over the internet. Nice place to share secret data.

1 of 4 selected Ready.

Figure 35. KeePass menu for Copy to Clipboard feature.



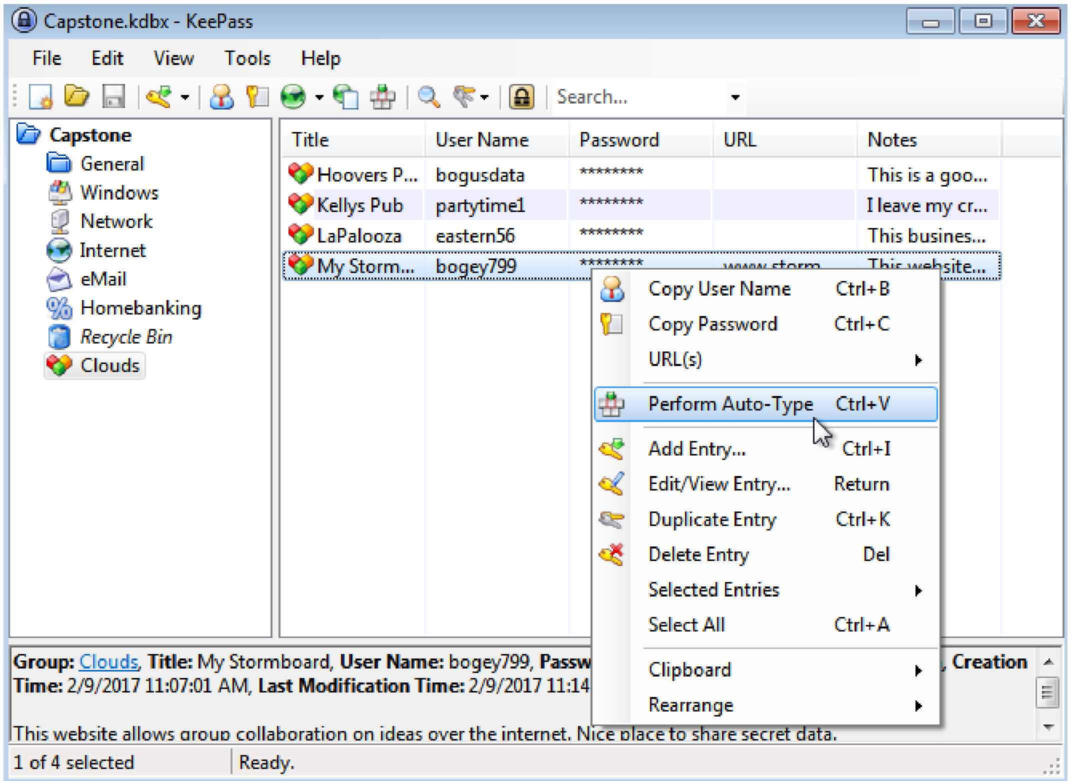
Title	User Name	Password	URL	Notes
Hoovers P...	bogusdata	********		This is a goo...
Kellys Pub	partytime1	********		I leave my cr...
LaPalooza	eastern56	********		This busines...
My Storm...	bogey799			s website...

Group: Clouds, **Title:** My Stormboard, **User Name:** bogey799, l d.com, **Creation**
Time: 2/9/2017 11:07:01 AM, **Last Modification Time:** 2/9/2017

This website allows group collaboration on ideas over the internet. Nice place to share secret data.

1 of 4 selected Ready.

Figure 36. KeePass menu option to select URL for a website.



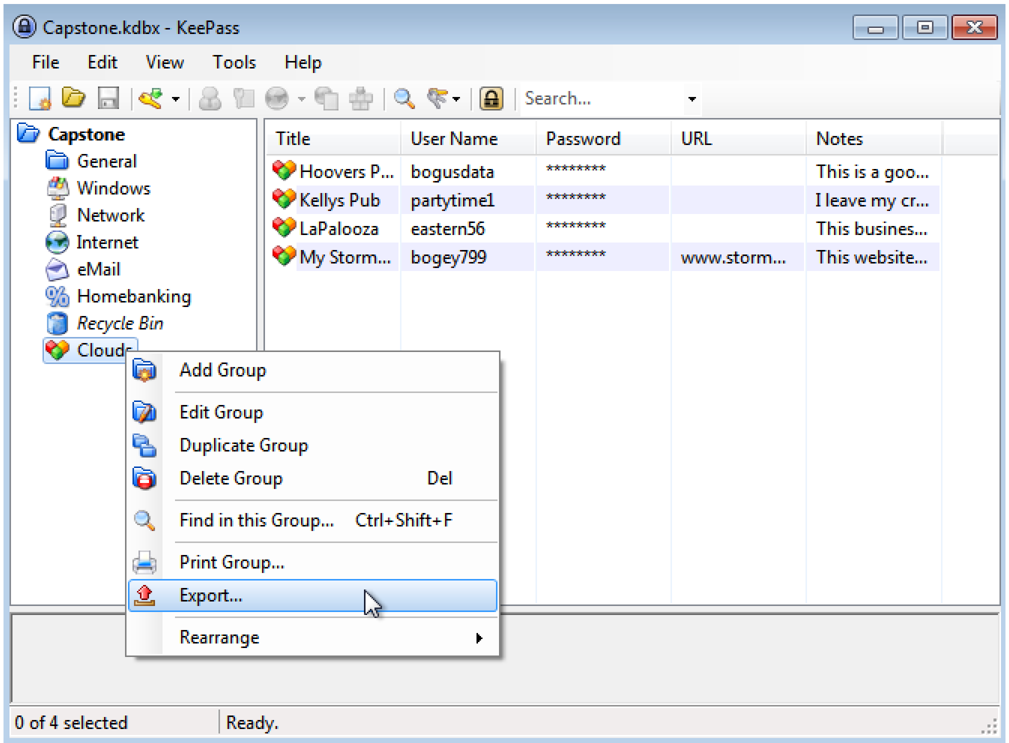
Title	User Name	Password	URL	Notes
Hoovers P...	bogusdata	********		This is a goo...
Kellys Pub	partytime1	********		I leave my cr...
LaPalooza	eastern56	********		This busines...
My Storm...	bogey799	********	www.storm...	This website...

Group: Clouds, **Title:** My Stormboard, **User Name:** bogey799, **Passw** , **Creation Time:** 2/9/2017 11:07:01 AM, **Last Modification Time:** 2/9/2017 11:14

This website allows group collaboration on ideas over the internet. Nice place to share secret data.

1 of 4 selected Ready.

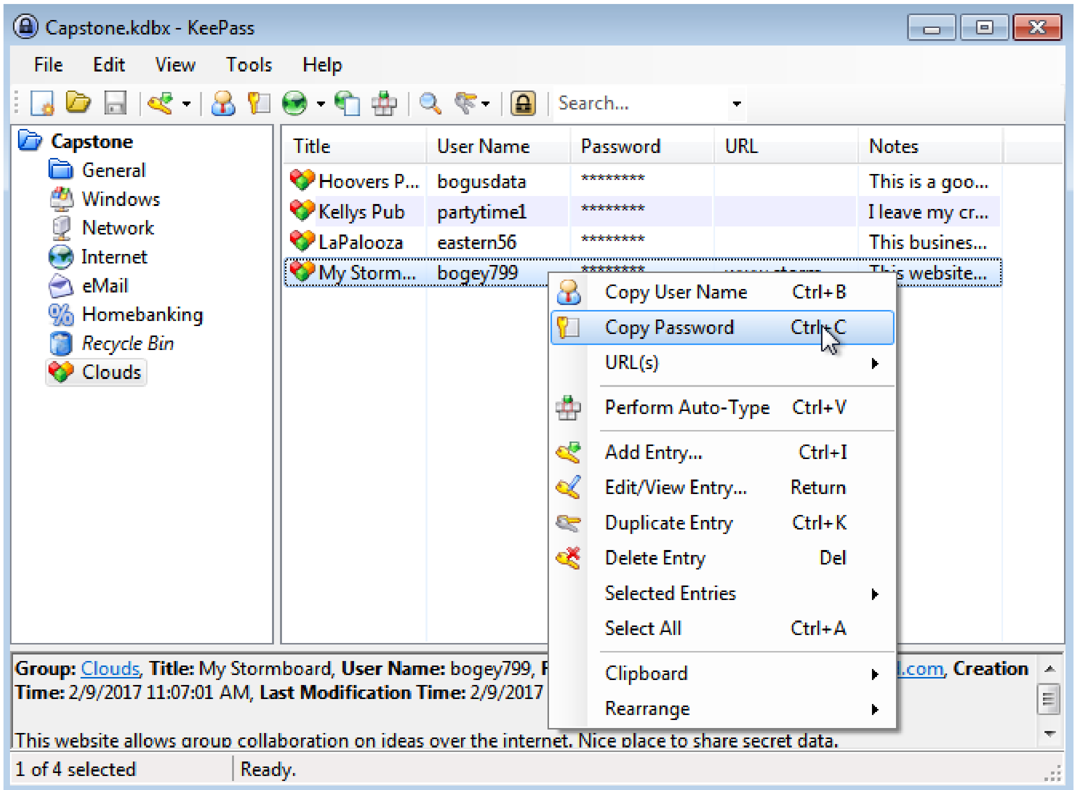
Figure 37. KeePass menu for utilizing the Auto-Type feature in form fields.



Title	User Name	Password	URL	Notes
Hoovers P...	bogusdata	********		This is a goo...
Kellys Pub	partytime1	********		I leave my cr...
LaPalooza	eastern56	********		This busines...
My Storm...	bogey799	********	www.storm...	This website...

0 of 4 selected Ready.

Figure 38. KeePass menu option for utilizing the Export database feature.



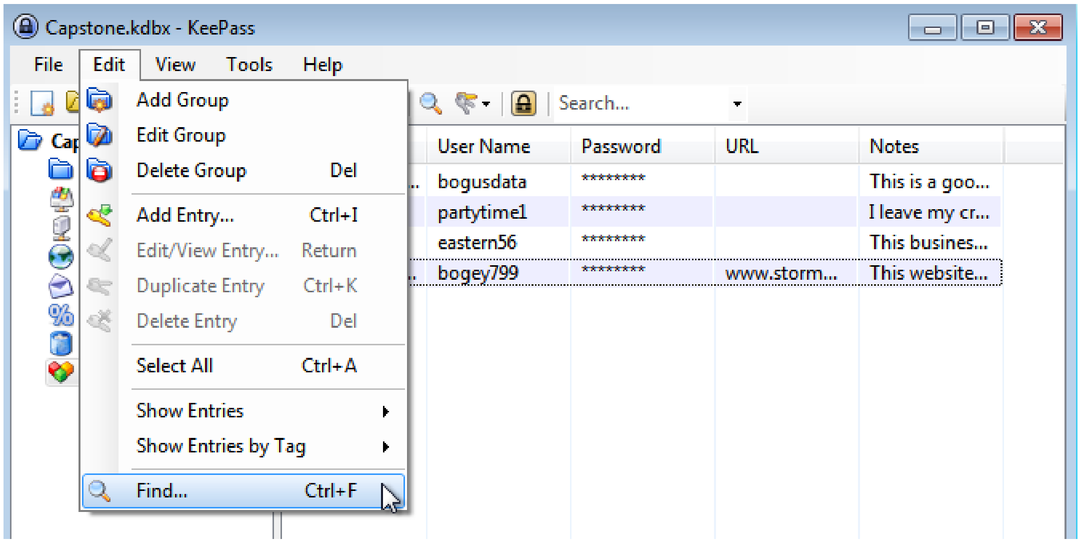
Title	User Name	Password	URL	Notes
Hoovers P...	bogusdata	********		This is a goo...
Kellys Pub	partytime1	********		I leave my cr...
LaPalooza	eastern56	********		This busines...
My Storm...	bogey799	********	www.storm...	This website...

Group: Clouds, **Title:** My Stormboard, **User Name:** bogey799, **F** .com, **Creation Time:** 2/9/2017 11:07:01 AM, **Last Modification Time:** 2/9/2017

This website allows group collaboration on ideas over the internet. Nice place to share secret data.

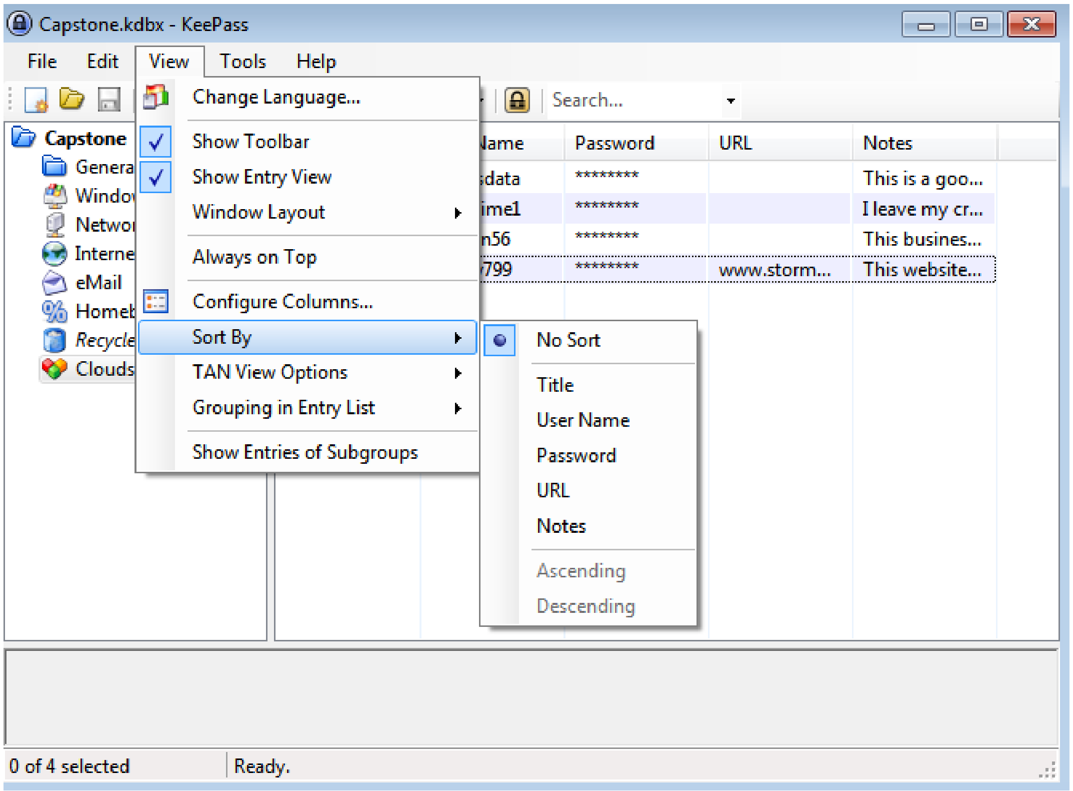
1 of 4 selected | Ready.

Figure 39. KeePass menu option for the Copy Password feature.



User Name	Password	URL	Notes
bogusdata	********		This is a goo...
partytime1	********		I leave my cr...
eastern56	********		This busines...
bogey799	********	www.storm...	This website...

Figure 40. KeePass menu option Find feature for conducting a search in the database.



Name	Password	URL	Notes
data	********		This is a goo...
ime1	********		I leave my cr...
n56	********		This busines...
799	********	www.storm...	This website...

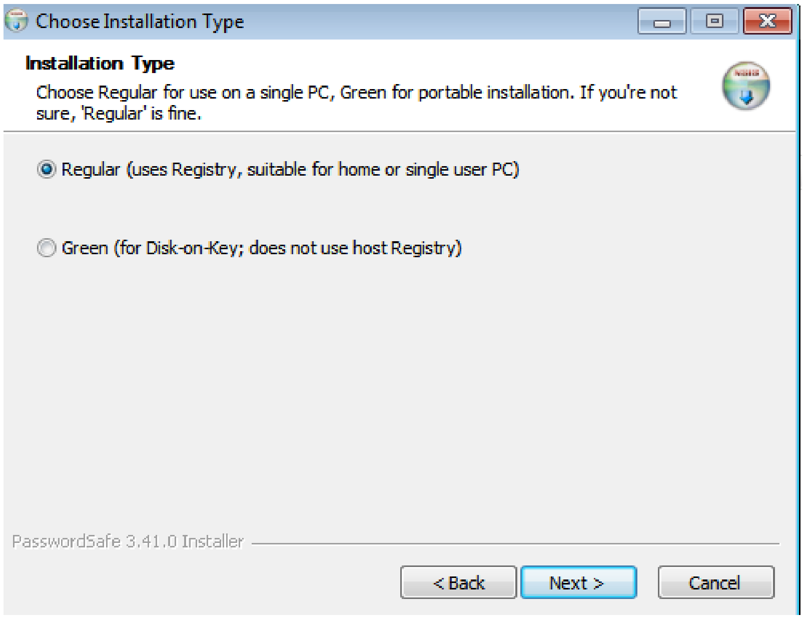
0 of 4 selected

Ready.

Figure 41. KeePass menu option for the Sort feature with the database.

Appendix D

This Depicts a Series of Password Safe Screenshots



Choose Installation Type

Installation Type

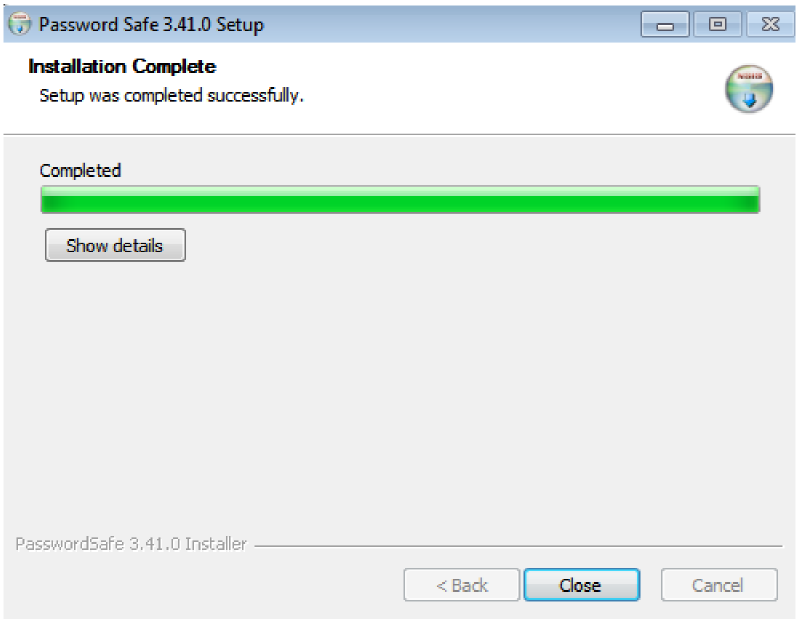
Choose Regular for use on a single PC, Green for portable installation. If you're not sure, 'Regular' is fine.

● Regular (uses Registry, suitable for home or single user PC)

○ Green (for Disk-on-Key; does not use host Registry)

PasswordSafe 3.41.0 Installer

Figure 42. Password Safe installation type dialog box.



Password Safe 3.41.0 Setup

Installation Complete

Setup was completed successfully.

Completed

PasswordSafe 3.41.0 Installer

Figure 43. Password Safe successful installation dialog box.

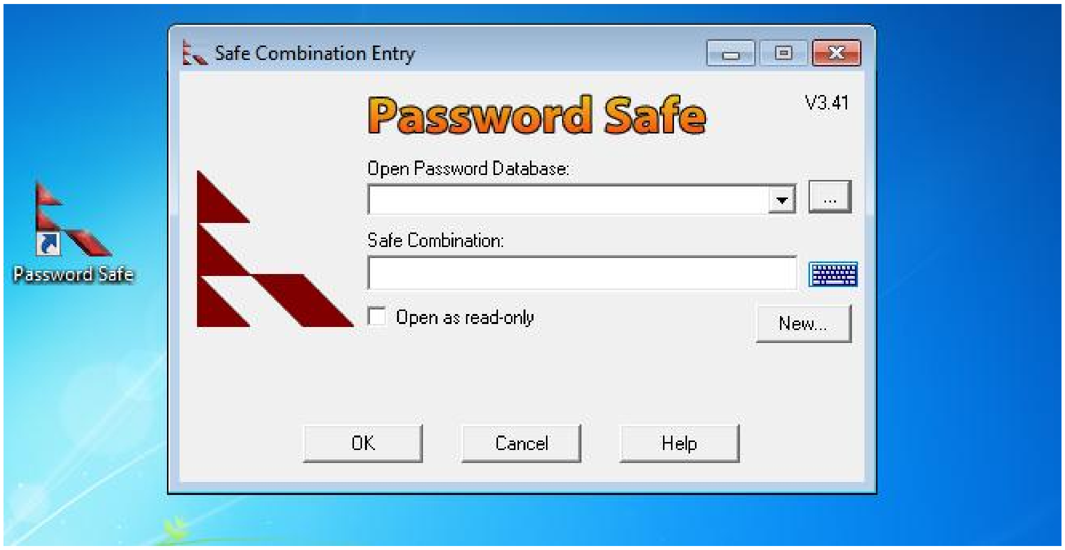
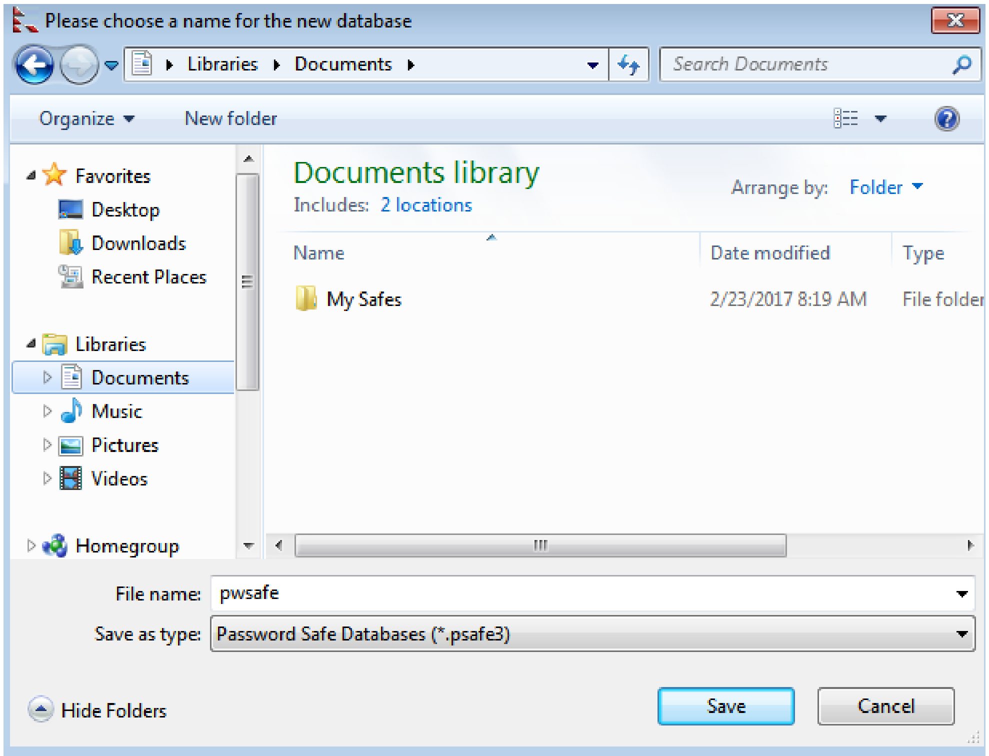


Figure 44. Password Safe login screen and the Safe Combination is the Master Key.

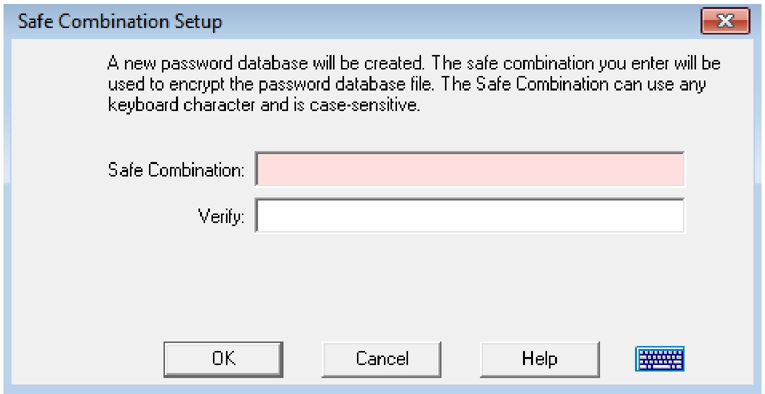


Name	Date modified	Type
My Safes	2/23/2017 8:19 AM	File folder

File name: pwsafe

Save as type: Password Safe Databases (*.psafe3)

Figure 45. Password Safe default storage location and file type.



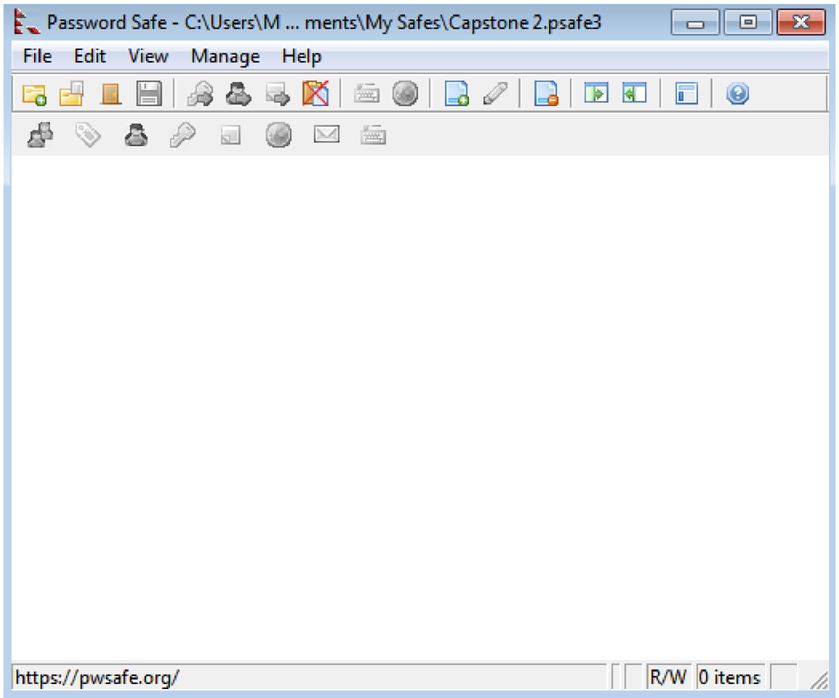
Safe Combination Setup

A new password database will be created. The safe combination you enter will be used to encrypt the password database file. The Safe Combination can use any keyboard character and is case-sensitive.

Safe Combination:

Verify:

Figure 46. Password Safe (Safe Combination) setup screen.



Password Safe - C:\Users\M ... ments\My Safes\Capstone 2.psafe3

https://pwsafe.org/ R/W 0 items

Figure 47. New empty Password Safe ready to add database entries.

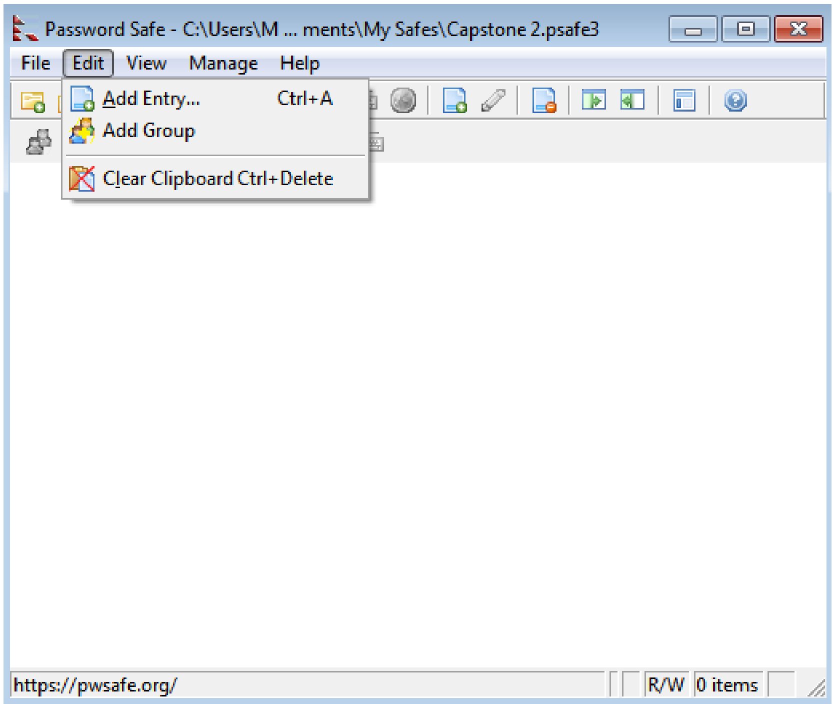

Password Safe - C:\Users\M ... ments\My Safes\Capstone 2.psafe3
File
Edit
View
Manage
Help
Add Entry... Ctrl+A
Add Group
Clear Clipboard Ctrl+Delete
https://pwsafe.org/
R/W
0 items

Figure 48. Password Safe Edit menu to Add Group to database.

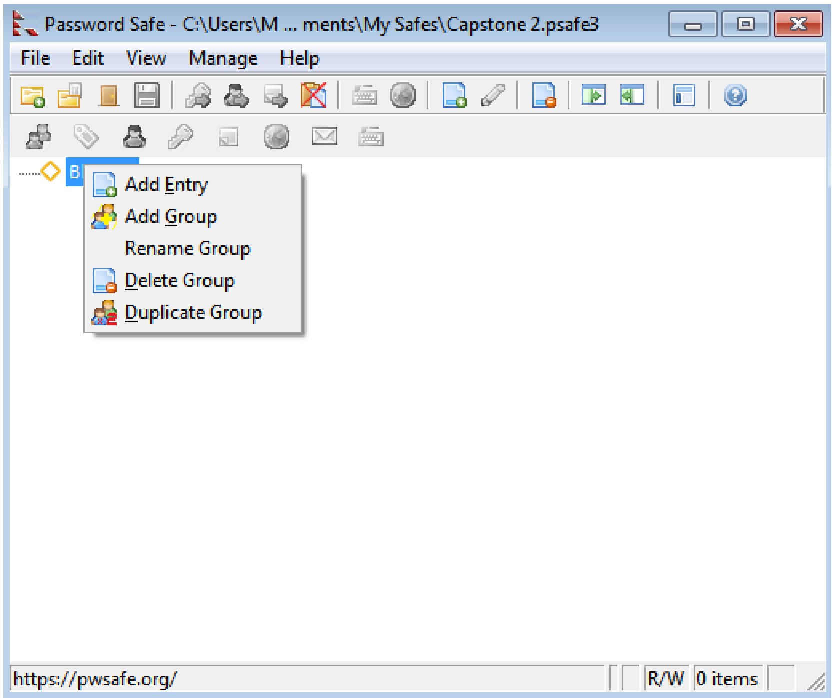
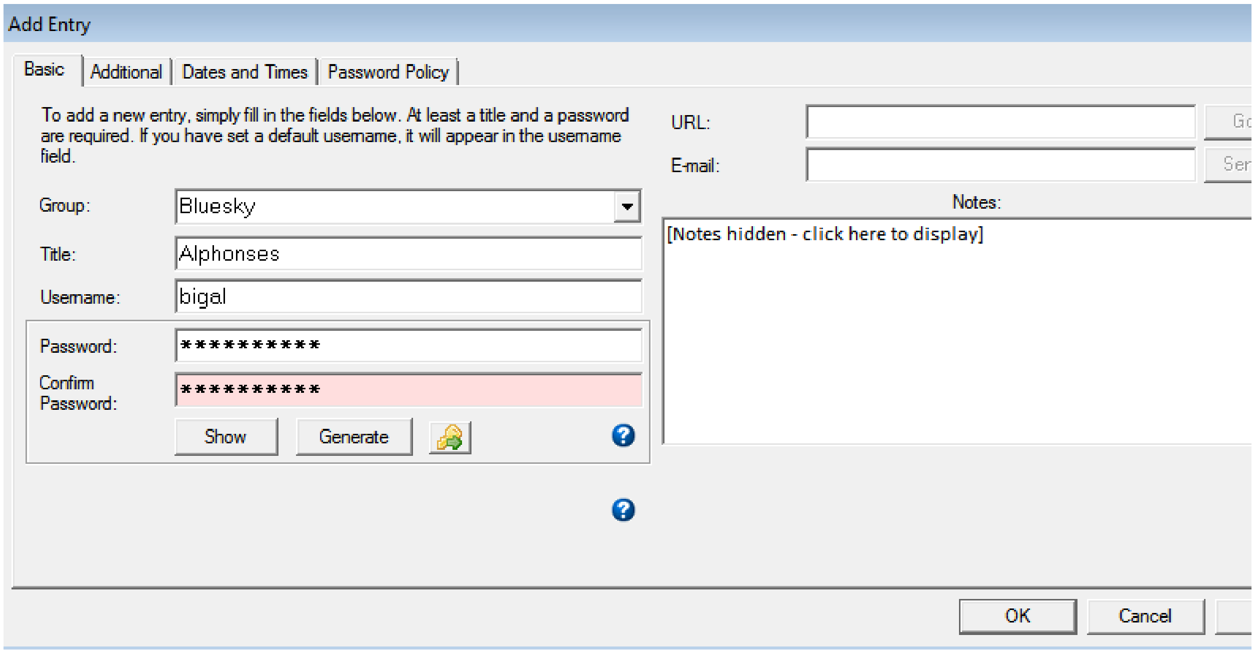


Figure 49. Password Safe menu to Add Entry to the new “Bluesky” group.



To add a new entry, simply fill in the fields below. At least a title and a password are required. If you have set a default username, it will appear in the username field.

Group: Bluesky

Title: Alphonses

Username: bigal

Password: **********

Confirm Password: **********

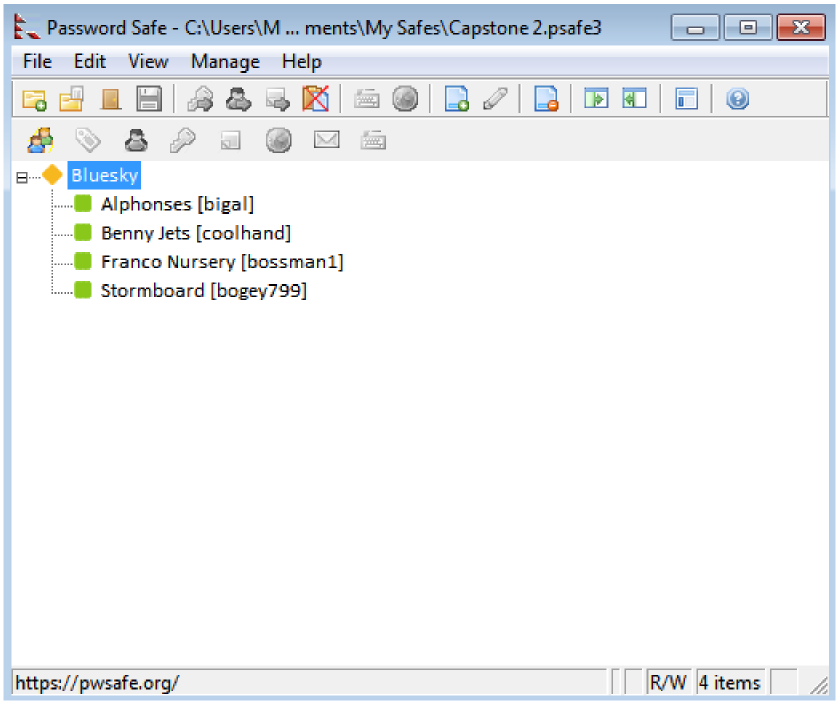
URL:

E-mail:

Notes:

[Notes hidden - click here to display]

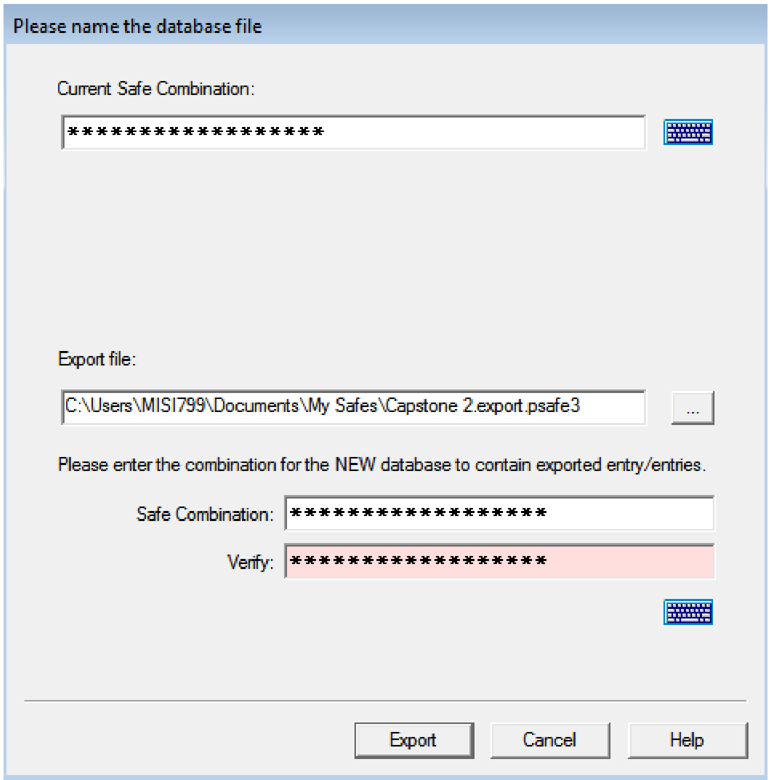
Figure 50. Password Safe menu to Add Entry with assigned username and password.



Password Safe - C:\Users\M ... ments\My Safes\Capstone 2.psafe3

- Bluesky
  - Alphonses [bigal]
  - Benny Jets [coolhand]
  - Franco Nursery [bossman1]
  - Stormboard [bogey799]

Figure 51. Password Safe interface depicting the completed entries for “Bluesky” database.



Please name the database file

Current Safe Combination:

****

Export file:

C:\Users\MISI799\Documents\My Safes\Capstone 2.export.psafe3

Please enter the combination for the NEW database to contain exported entry/entries.

Safe Combination: ******************

Verify: ******************

Figure 52. This unique feature of Password Safe requires the Master Key password to be entered before authorization is granted for a database Export function.

Appendix E

Forensic Tool Kit (FTK) Screenshots

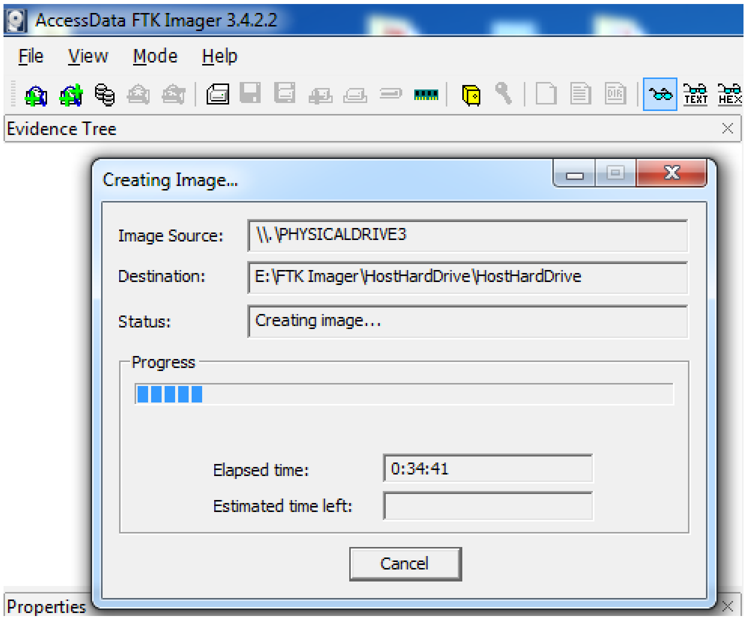


Image Source: \\.\PHYSICALDRIVE3

Destination: E:\FTK Imager\HostHardDrive\HostHardDrive

Status: Creating image...

Elapsed time: 0:34:41

Estimated time left:

Figure 53. This screenshot depicts the process where the hard drive connected to the Tableau Write Blocker is creating the evidence image HostHardDrive.E01.

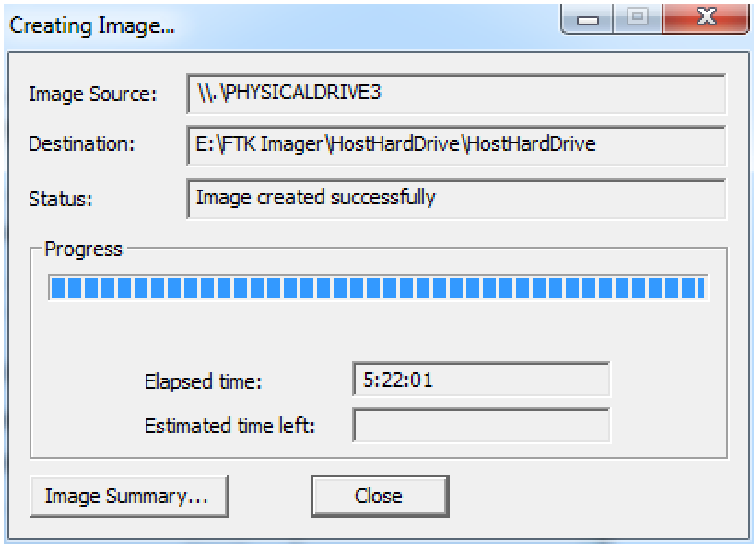


Image Source: \\.\PHYSICALDRIVE3

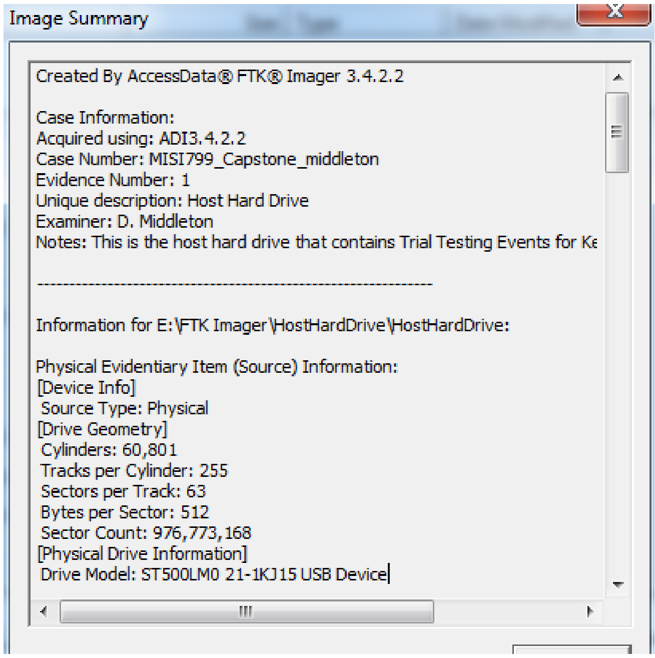
Destination: E:\FTK Imager\HostHardDrive\HostHardDrive

Status: Image created successfully

Elapsed time: 5:22:01

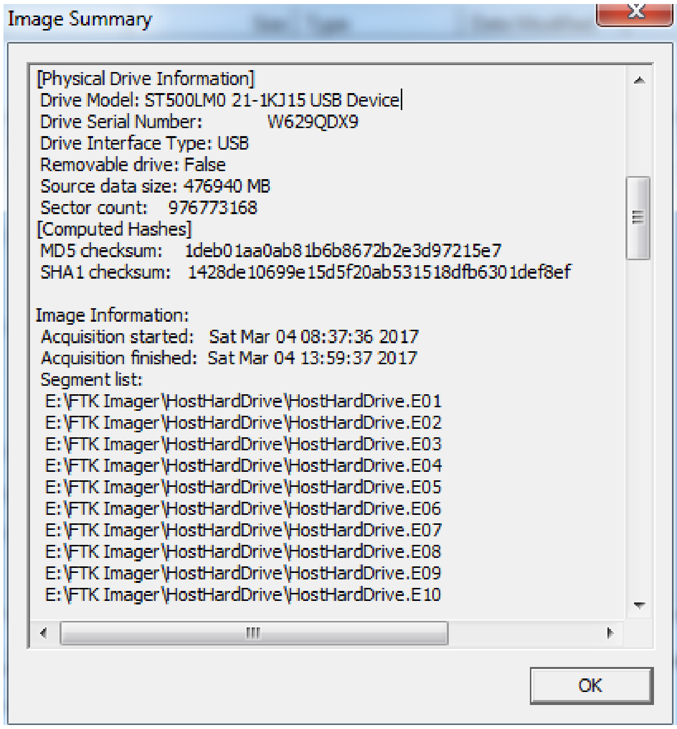
Estimated time left:

Figure 54. The evidence image named HostHardDrive.E01 was created successfully by FTK Imager.



```
Created By AccessData® FTK® Imager 3.4.2.2

Case Information:
Acquired using: ADI3.4.2.2
Case Number: MISI799_Capstone_middleton
Evidence Number: 1
Unique description: Host Hard Drive
Examiner: D. Middleton
Notes: This is the host hard drive that contains Trial Testing Events for Ke

----------------------------------------------------------------

Information for E:\FTK Imager\HostHardDrive\HostHardDrive:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60,801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976,773,168
[Physical Drive Information]
 Drive Model: ST500LM0 21-1KJ15 USB Device
```

Figure 55. This is the Image Summary created for the HostHardDrive.E01.



```
[Physical Drive Information]
 Drive Model: ST500LM0 21-1KJ15 USB Device
 Drive Serial Number:         W629QDX9
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    1deb01aa0ab81b6b8672b2e3d97215e7
 SHA1 checksum:   1428de10699e15d5f20ab531518dfb6301def8ef

Image Information:
 Acquisition started:  Sat Mar 04 08:37:36 2017
 Acquisition finished:  Sat Mar 04 13:59:37 2017
 Segment list:
  E:\FTK Imager\HostHardDrive\HostHardDrive.E01
  E:\FTK Imager\HostHardDrive\HostHardDrive.E02
  E:\FTK Imager\HostHardDrive\HostHardDrive.E03
  E:\FTK Imager\HostHardDrive\HostHardDrive.E04
  E:\FTK Imager\HostHardDrive\HostHardDrive.E05
  E:\FTK Imager\HostHardDrive\HostHardDrive.E06
  E:\FTK Imager\HostHardDrive\HostHardDrive.E07
  E:\FTK Imager\HostHardDrive\HostHardDrive.E08
  E:\FTK Imager\HostHardDrive\HostHardDrive.E09
  E:\FTK Imager\HostHardDrive\HostHardDrive.E10
```

Figure 56. This is the 2nd half of the Image Summary created for the HostHardDrive.E01.

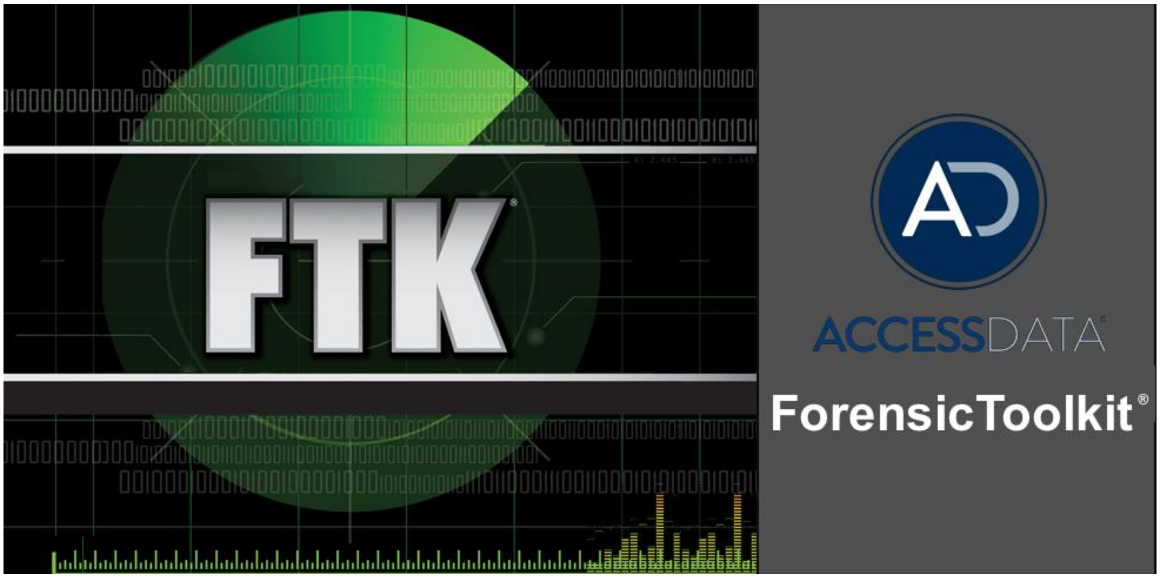
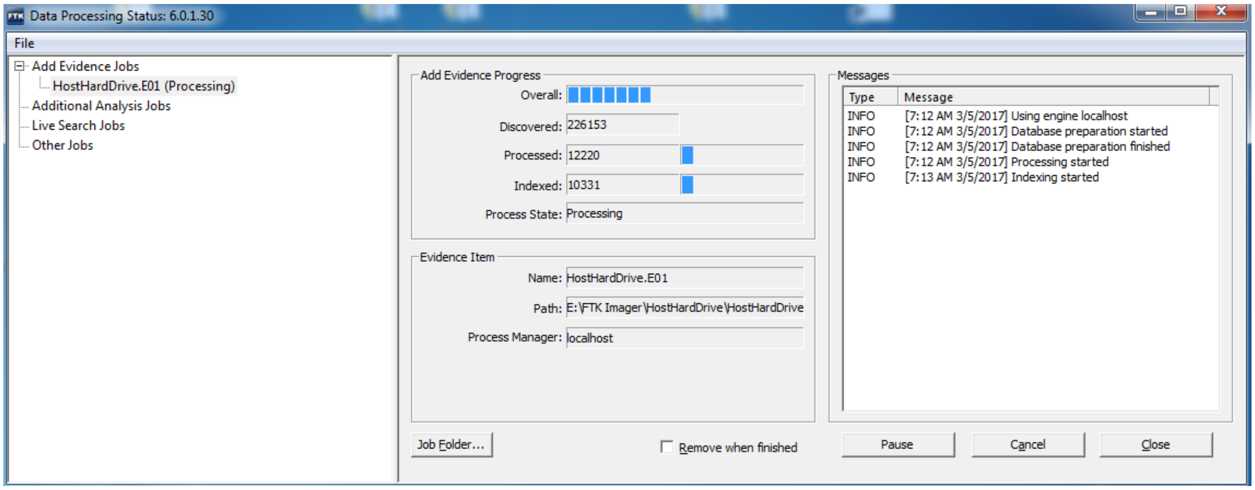


Figure 57. This logo appears when FTK is activated for processing evidence.



- Add Evidence Jobs
  - HostHardDrive.E01 (Processing)
- Additional Analysis Jobs
- Live Search Jobs
- Other Jobs

Add Evidence Progress

Overall:

Discovered: 226153

Processed: 12220

Indexed: 10331

Process State: Processing

Evidence Item

Name: HostHardDrive.E01

Path: E:\FTK Imager\HostHardDrive\HostHardDrive

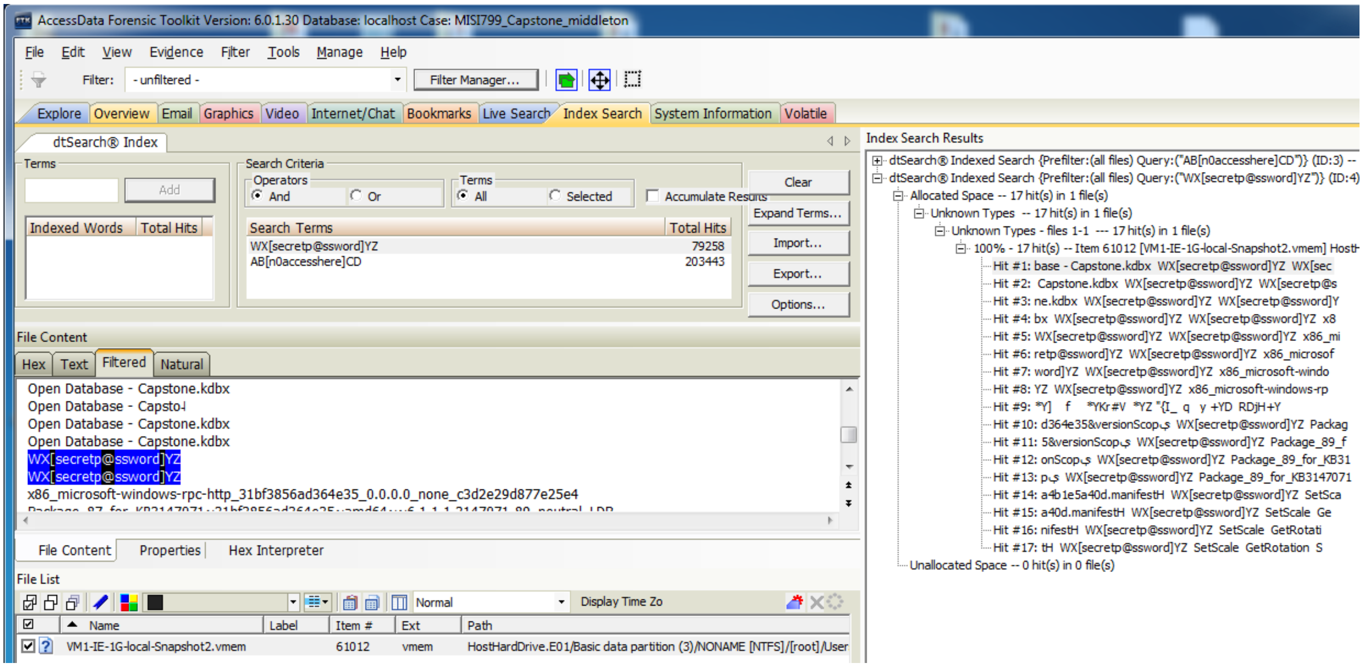
Process Manager: localhost

□ Remove when finished

Messages

```
Type  Message
INFO  [7:12 AM 3/5/2017] Using engine localhost
INFO  [7:12 AM 3/5/2017] Database preparation started
INFO  [7:12 AM 3/5/2017] Database preparation finished
INFO  [7:12 AM 3/5/2017] Processing started
INFO  [7:13 AM 3/5/2017] Indexing started
```

Figure 58. This is FTK processing the HostHardDrive.E01 evidence file that was created using FTK Imager.



AccessData Forensic Toolkit Version: 6.0.1.30 Database: localhost Case: MISI799_Capstone_middleton

Filter: - unfiltered -

Search Terms	Total Hits
WX[secretp@ssword]YZ	79258
AB[n0accesshere]CD	203443

Operators: ● And ○ Or — Terms: ● All ○ Selected — □ Accumulate Results

File Content

```
Open Database - Capstone.kdbx
Open Database - Capsto
Open Database - Capstone.kdbx
Open Database - Capstone.kdbx
WX[secretp@ssword]YZ
WX[secretp@ssword]YZ
x86_microsoft-windows-rpc-http_31bf3856ad364e35_0.0.0.0_none_c3d2e29d877e25e4
```

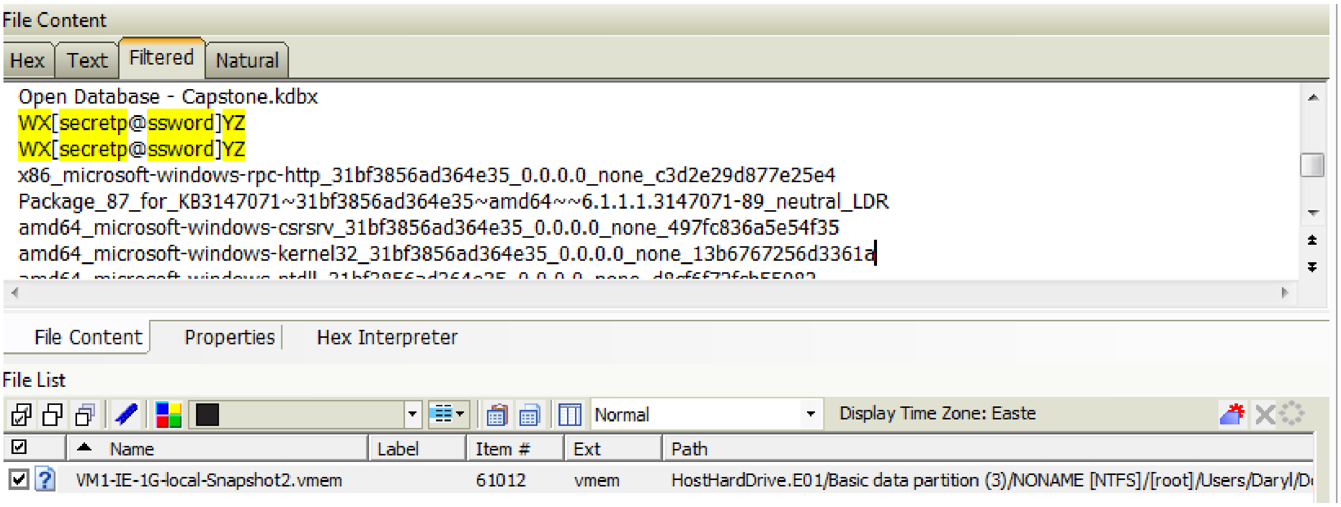
☑	Name	Label	Item #	Ext	Path
☑	VM1-IE-1G-local-Snapshot2.vmem		61012	vmem	HostHardDrive.E01/Basic data partition (3)/NONAME [NTFS]/[root]/User

Index Search Results

```
dtSearch® Indexed Search {Prefilter:(all files) Query:("AB[n0accesshere]CD")} (ID:3) --
dtSearch® Indexed Search {Prefilter:(all files) Query:("WX[secretp@ssword]YZ")} (ID:4)
  Allocated Space -- 17 hit(s) in 1 file(s)
    Unknown Types  -- 17 hit(s) in 1 file(s)
      Unknown Types - files 1-1  --- 17 hit(s) in 1 file(s)
        100% - 17 hit(s) -- Item 61012 [VM1-IE-1G-local-Snapshot2.vmem] Host
          Hit #1: base - Capstone.kdbx  WX[secretp@ssword]YZ  WX[sec
          Hit #2:  Capstone.kdbx  WX[secretp@ssword]YZ  WX[secretp@s
          Hit #3: ne.kdbx  WX[secretp@ssword]YZ  WX[secretp@ssword]Y
          Hit #4: bx  WX[secretp@ssword]YZ  WX[secretp@ssword]YZ  x8
          Hit #5: WX[secretp@ssword]YZ  WX[secretp@ssword]YZ  x86_mi
          Hit #6: retp@ssword]YZ  WX[secretp@ssword]YZ  x86_microsof
          Hit #7: word]YZ  WX[secretp@ssword]YZ  x86_microsoft-windo
          Hit #8: YZ  WX[secretp@ssword]YZ  x86_microsoft-windows-rp
          Hit #9: *Y]   f    *YKr#V  *YZ "{I_  q   y +YD  RDjH+Y
          Hit #10: d364e35&versionScopي  WX[secretp@ssword]YZ  Packag
          Hit #11: 5&versionScopي  WX[secretp@ssword]YZ  Package_89_f
          Hit #12: onScopي  WX[secretp@ssword]YZ  Package_89_for_KB31
          Hit #13: pي  WX[secretp@ssword]YZ  Package_89_for_KB3147071
          Hit #14: a4b1e5a40d.manifestH  WX[secretp@ssword]YZ  SetSca
          Hit #15: a40d.manifestH  WX[secretp@ssword]YZ  SetScale  Ge
          Hit #16: nifestH  WX[secretp@ssword]YZ  SetScale  GetRotati
          Hit #17: tH  WX[secretp@ssword]YZ  SetScale  GetRotation  S
  Unallocated Space -- 0 hit(s) in 0 file(s)
```

File Edit View Evidence Filter Tools Manage Help
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
dtSearch® Index
Terms
Add
Indexed Words
Total Hits
Search Criteria
Clear
Expand Terms...
Import...
Export...
Options...
Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Normal
Display Time Zo

Figure 59. This screenshot is the first series of FTK dtSearches that was specific to locating the Master Key **WX[secretp@ssword]YZ** that was used within the KeePass password manager. The Path to the evidence file is also included in the screenshot and Bookmarked for reporting.



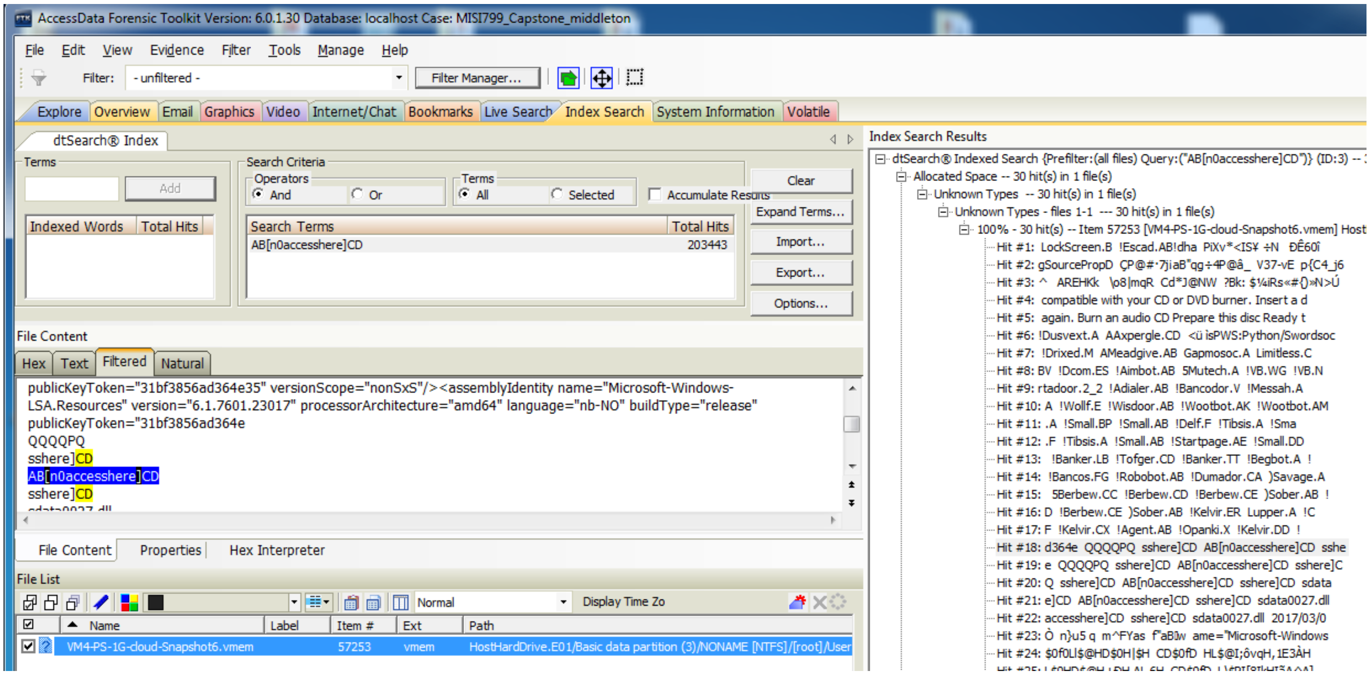
File Content

```
Open Database - Capstone.kdbx
WX[secretp@ssword]YZ
WX[secretp@ssword]YZ
x86_microsoft-windows-rpc-http_31bf3856ad364e35_0.0.0.0_none_c3d2e29d877e25e4
Package_87_for_KB3147071~31bf3856ad364e35~amd64~~6.1.1.1.3147071-89_neutral_LDR
amd64_microsoft-windows-csrsrv_31bf3856ad364e35_0.0.0.0_none_497fc836a5e54f35
amd64_microsoft-windows-kernel32_31bf3856ad364e35_0.0.0.0_none_13b6767256d3361a
```

☑	Name	Label	Item #	Ext	Path
☑	VM1-IE-1G-local-Snapshot2.vmem		61012	vmem	HostHardDrive.E01/Basic data partition (3)/NONAME [NTFS]/[root]/Users/Daryl/D

Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Normal
Display Time Zone: Easte

Figure 60. This item is a closer view of the previous figure showing the captured Master Key assigned to the KeePass password manager highlighted in yellow.



AccessData Forensic Toolkit Version: 6.0.1.30 Database: localhost Case: MISI799_Capstone_middleton

Filter: - unfiltered -

Operators: ● And ○ Or

Terms: ● All ○ Selected

□ Accumulate Results

Indexed Words	Total Hits

Search Terms	Total Hits
AB[n0accesshere]CD	203443

```
publicKeyToken="31bf3856ad364e35" versionScope="nonSxS"/><assemblyIdentity name="Microsoft-Windows-
LSA.Resources" version="6.1.7601.23017" processorArchitecture="amd64" language="nb-NO" buildType="release"
publicKeyToken="31bf3856ad364e
QQQQPQ
sshere]CD
AB[n0accesshere]CD
sshere]CD
```

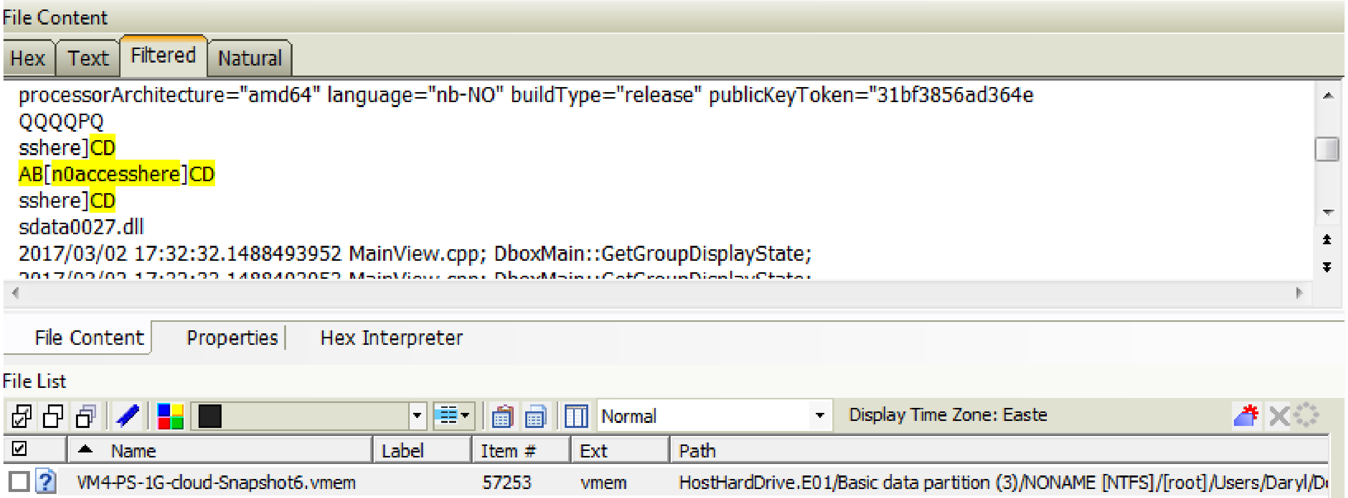
Normal

☑	Name	Label	Item #	Ext	Path
☑	VM4-PS-1G-cloud-Snapshot6.vmem		57253	vmem	HostHardDrive.E01/Basic data partition (3)/NONAME [NTFS]/[root]/User

Index Search Results

```
⊟ dtSearch® Indexed Search {Prefilter:(all files) Query:("AB[n0accesshere]CD")} (ID:3) --
  ⊟ Allocated Space -- 30 hit(s) in 1 file(s)
    ⊟ Unknown Types  -- 30 hit(s) in 1 file(s)
      ⊟ Unknown Types - files 1-1  --- 30 hit(s) in 1 file(s)
        ⊟ 100% - 30 hit(s) -- Item 57253 [VM4-PS-1G-cloud-Snapshot6.vmem] Host
            Hit #1:  LockScreen.B  !Escad.AB!dha  PiXv*<IS¥ ÷N   ÐÊ60î
            Hit #2: gSourcePropD  ÇP@#·7jiaB"qg÷4P@â_  V37-vE  p{C4_j6
            Hit #3: ^   AREHKk   \p8|mqR  Cd*J@NW  ?Bk: $¼iRs«#{}»N>Ú
            Hit #4:  compatible with your CD or DVD burner. Insert a d
            Hit #5:  again. Burn an audio CD Prepare this disc Ready t
            Hit #6: !Dusvext.A  AAxpergle.CD  <ü ìsPWS:Python/Swordsoc
            Hit #7:  !Drixed.M  AMeadgive.AB  Gapmosoc.A  Limitless.C
            Hit #8: BV  !Dcom.ES  !Aimbot.AB  5Mutech.A  !VB.WG  !VB.N
            Hit #9: rtadoor.2_2  !Adialer.AB  !Bancodor.V  !Messah.A
            Hit #10: A  !Wollf.E  !Wisdoor.AB  !Wootbot.AK  !Wootbot.AM
            Hit #11: .A  !Small.BP  !Small.AB  !Delf.F  !Tibsis.A  !Sma
            Hit #12: .F  !Tibsis.A  !Small.AB  !Startpage.AE  !Small.DD
            Hit #13:   !Banker.LB  !Tofger.CD  !Banker.TT  !Begbot.A  !
            Hit #14:  !Bancos.FG  !Robobot.AB  !Dumador.CA  )Savage.A
            Hit #15:   5Berbew.CC  !Berbew.CD  !Berbew.CE  )Sober.AB  !
            Hit #16: D  !Berbew.CE  )Sober.AB  !Kelvir.ER  Lupper.A  !C
            Hit #17: F  !Kelvir.CX  !Agent.AB  !Opanki.X  !Kelvir.DD  !
            Hit #18: d364e  QQQQPQ  sshere]CD  AB[n0accesshere]CD  sshe
            Hit #19: e  QQQQPQ  sshere]CD  AB[n0accesshere]CD  sshere]C
            Hit #20: Q  sshere]CD  AB[n0accesshere]CD  sshere]CD  sdata
            Hit #21: e]CD  AB[n0accesshere]CD  sshere]CD  sdata0027.dll
            Hit #22: accesshere]CD  sshere]CD  sdata0027.dll  2017/03/0
            Hit #23: Ò  n}u5 q  m^FYas  f"aBÌw  ame="Microsoft-Windows
            Hit #24: $0f0Ll$@HD$0H|$H  CD$0fD  HL$@I;ôvqH,1E3ÀH
```

Figure 61. This screenshot is the first series of FTK dtSearches that was specific to locating the Master Key **AB[n0accesshere]CD** that was used within the Password Safe password manager. The Path to the evidence file is also included in the screenshot and Bookmarked for reporting.

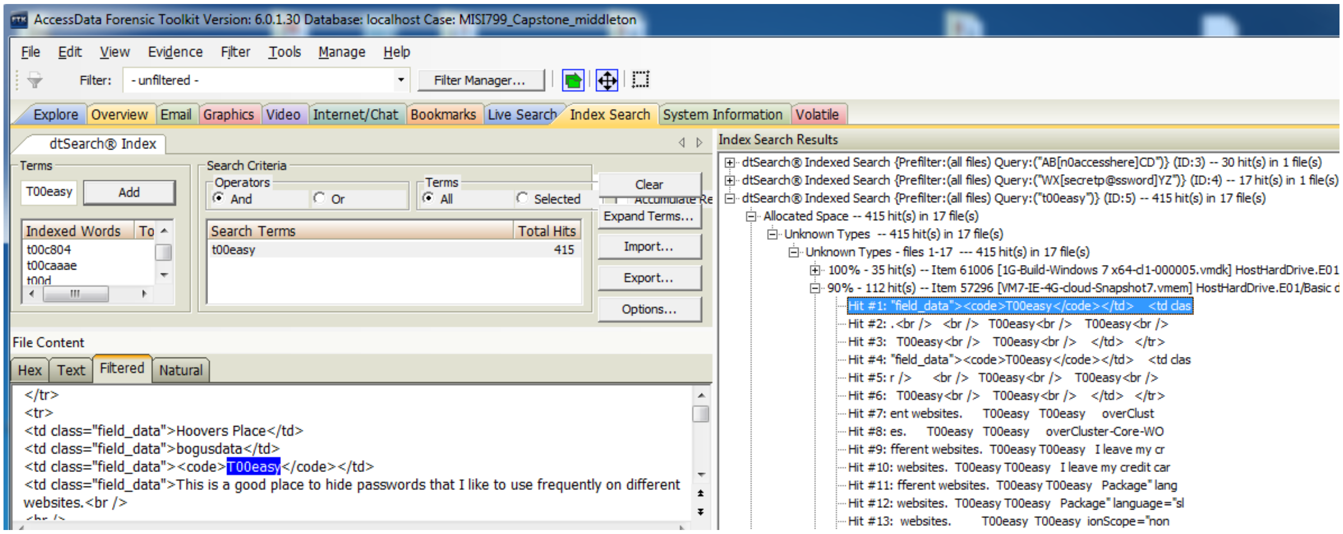


```
processorArchitecture="amd64" language="nb-NO" buildType="release" publicKeyToken="31bf3856ad364e
QQQQPQ
sshere]CD
AB[n0accesshere]CD
sshere]CD
sdata0027.dll
2017/03/02 17:32:32.1488493952 MainView.cpp; DboxMain::GetGroupDisplayState;
```

Normal

☑	Name	Label	Item #	Ext	Path
□	VM4-PS-1G-cloud-Snapshot6.vmem		57253	vmem	HostHardDrive.E01/Basic data partition (3)/NONAME [NTFS]/[root]/Users/Daryl/D

Figure 62. This item is a closer view of the previous figure showing the captured Master Key assigned to the Password Safe password manager highlighted in yellow.


AccessData Forensic Toolkit Version: 6.0.1.30 Database: localhost Case: MISI799_Capstone_middleton
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
dtSearch® Index
Terms
Add
Indexed Words To
Search Criteria
Operators
● And ○ Or
Terms
● All ○ Selected
Clear
Expand Terms...
Import...
Export...
Options...
Search Terms Total Hits
File Content
Hex Text Filtered Natural
Index Search Results

T00easy

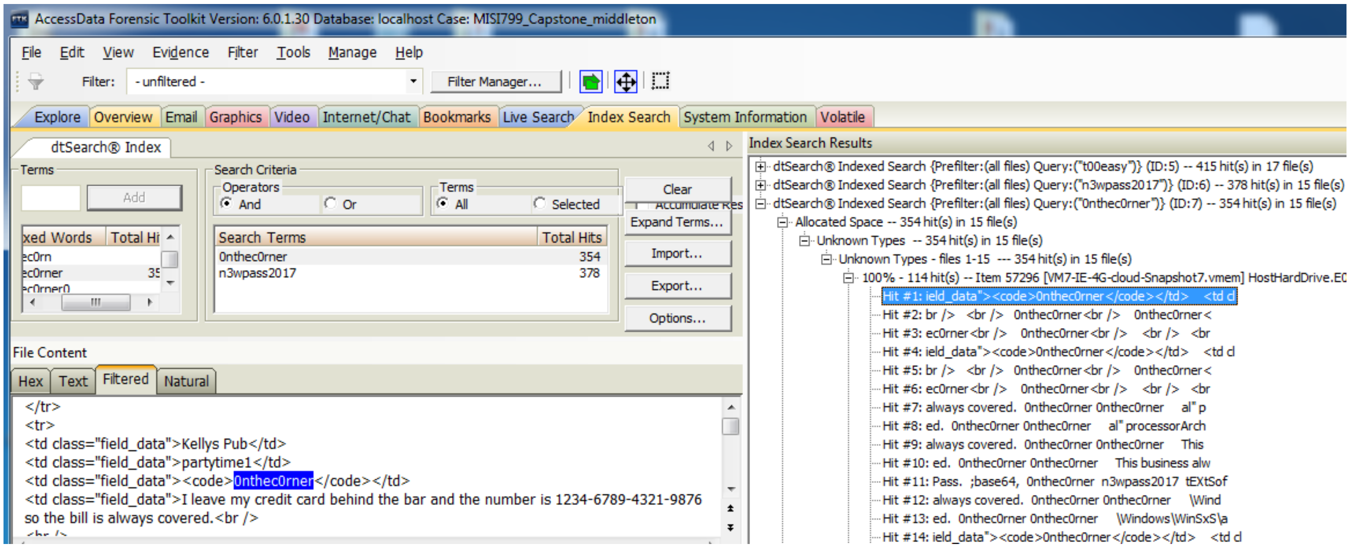
Indexed Words	To
t00c804	
t00caaae	
t00d	

Search Terms	Total Hits
t00easy	415

```
</tr>
<tr>
<td class="field_data">Hoovers Place</td>
<td class="field_data">bogusdata</td>
<td class="field_data"><code>T00easy</code></td>
<td class="field_data">This is a good place to hide passwords that I like to use frequently on different
websites.<br />
```

```
dtSearch® Indexed Search {Prefilter:(all files) Query:("AB[n0accesshere]CD")} (ID:3) -- 30 hit(s) in 1 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("WX[secretp@ssword]YZ")} (ID:4) -- 17 hit(s) in 1 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("t00easy")} (ID:5) -- 415 hit(s) in 17 file(s)
  Allocated Space -- 415 hit(s) in 17 file(s)
    Unknown Types  -- 415 hit(s) in 17 file(s)
      Unknown Types - files 1-17  --- 415 hit(s) in 17 file(s)
        100% - 35 hit(s) -- Item 61006 [1G-Build-Windows 7 x64-cl1-000005.vmdk] HostHardDrive.E01
        90% - 112 hit(s) -- Item 57296 [VM7-IE-4G-cloud-Snapshot7.vmem] HostHardDrive.E01/Basic d
          Hit #1: "field_data"><code>T00easy</code></td>    <td clas
          Hit #2: .<br />   <br />  T00easy<br />   T00easy<br />
          Hit #3:  T00easy<br />   T00easy<br />   </td>  </tr>
          Hit #4: "field_data"><code>T00easy</code></td>    <td clas
          Hit #5: r />      <br />  T00easy<br />   T00easy<br />
          Hit #6:  T00easy<br />   T00easy<br />   </td>  </tr>
          Hit #7: ent websites.     T00easy  T00easy    overClust
          Hit #8: es.     T00easy  T00easy    overCluster-Core-WO
          Hit #9: fferent websites.  T00easy T00easy  I leave my cr
          Hit #10: websites.  T00easy T00easy  I leave my credit car
          Hit #11: fferent websites.  T00easy T00easy  Package" lang
          Hit #12: websites.  T00easy T00easy  Package" language="sl
          Hit #13:  websites.       T00easy  T00easy  ionScope="non
```

Figure 63. This screenshot depicts one of the returned values during a dtSearch for the“**T00easy**” password from the Hoovers Place entry on the KeePass Database (Clouds).


AccessData Forensic Toolkit Version: 6.0.1.30 Database: localhost Case: MISI799_Capstone_middleton
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
dtSearch® Index
Terms
Add
xed Words Total Hi
Search Criteria
Operators
● And ○ Or
Terms
● All ○ Selected
Clear
Expand Terms...
Import...
Export...
Options...
Search Terms Total Hits
File Content
Hex Text Filtered Natural
Index Search Results

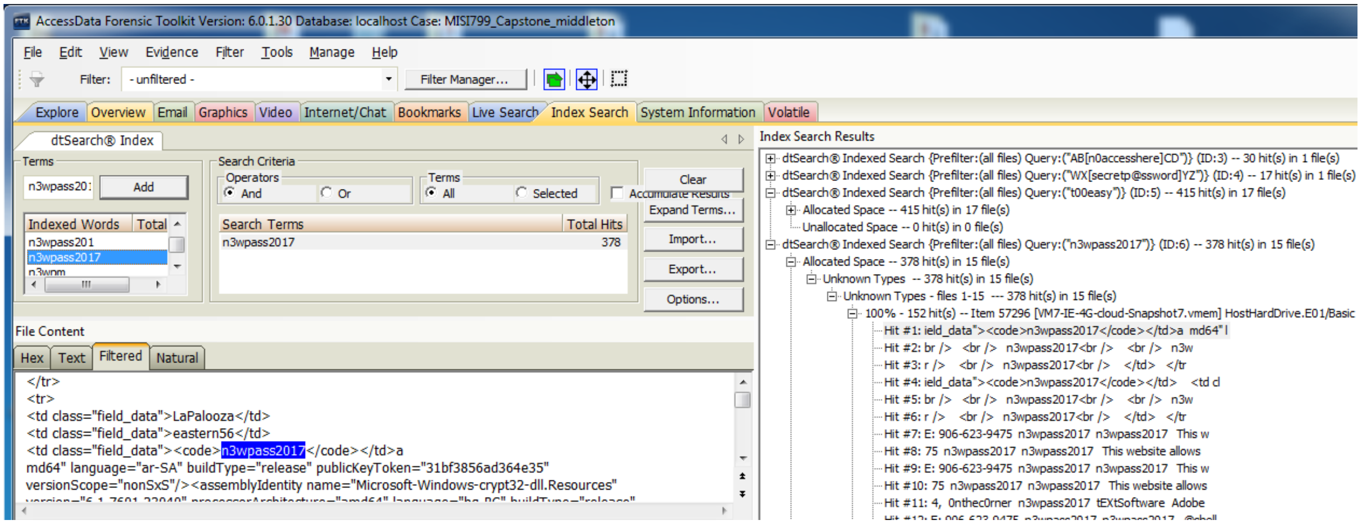
xed Words	Total Hi
ec0rn	
ec0rner	35
c0rner0	

Search Terms	Total Hits
0nthec0rner	354
n3wpass2017	378

```
</tr>
<tr>
<td class="field_data">Kellys Pub</td>
<td class="field_data">partytime1</td>
<td class="field_data"><code>0nthec0rner</code></td>
<td class="field_data">I leave my credit card behind the bar and the number is 1234-6789-4321-9876
so the bill is always covered.<br />
```

```
dtSearch® Indexed Search {Prefilter:(all files) Query:("t00easy")} (ID:5) -- 415 hit(s) in 17 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("n3wpass2017")} (ID:6) -- 378 hit(s) in 15 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("0nthec0rner")} (ID:7) -- 354 hit(s) in 15 file(s)
  Allocated Space -- 354 hit(s) in 15 file(s)
    Unknown Types  -- 354 hit(s) in 15 file(s)
      Unknown Types - files 1-15  --- 354 hit(s) in 15 file(s)
        100% - 114 hit(s) -- Item 57296 [VM7-IE-4G-cloud-Snapshot7.vmem] HostHardDrive.E0
          Hit #1: ield_data"><code>0nthec0rner</code></td>    <td cl
          Hit #2: br />   <br />  0nthec0rner<br />   0nthec0rner<
          Hit #3: ec0rner<br />   0nthec0rner<br />   <br />   <br
          Hit #4: ield_data"><code>0nthec0rner</code></td>    <td cl
          Hit #5: br />   <br />  0nthec0rner<br />   0nthec0rner<
          Hit #6: ec0rner<br />   0nthec0rner<br />   <br />   <br
          Hit #7: always covered.  0nthec0rner 0nthec0rner    al" p
          Hit #8: ed.  0nthec0rner 0nthec0rner    al" processorArch
          Hit #9: always covered.  0nthec0rner 0nthec0rner    This
          Hit #10: ed.  0nthec0rner 0nthec0rner    This business alw
          Hit #11: Pass.  ;base64,  0nthec0rner  n3wpass2017  tEXtSof
          Hit #12: always covered.  0nthec0rner 0nthec0rner    \Wind
          Hit #13: ed.  0nthec0rner 0nthec0rner    \Windows\WinSxS\a
          Hit #14: ield_data"><code>0nthec0rner</code></td>    <td cl
```

Figure 64. This screenshot depicts one of the returned values during a dtSearch for the “**0nthec0rner**” password from the Kellys Pub entry on the KeePass Database (Clouds).



AccessData Forensic Toolkit Version: 6.0.1.30 Database: localhost Case: MISI799_Capstone_middleton

Filter: - unfiltered -

Terms: n3wpass201

Indexed Words	Total
n3wpass201	
n3wpass2017	

Search Criteria — Operators: ● And ○ Or; Terms: ● All ○ Selected; □ Accumulate Results

Search Terms	Total Hits
n3wpass2017	378

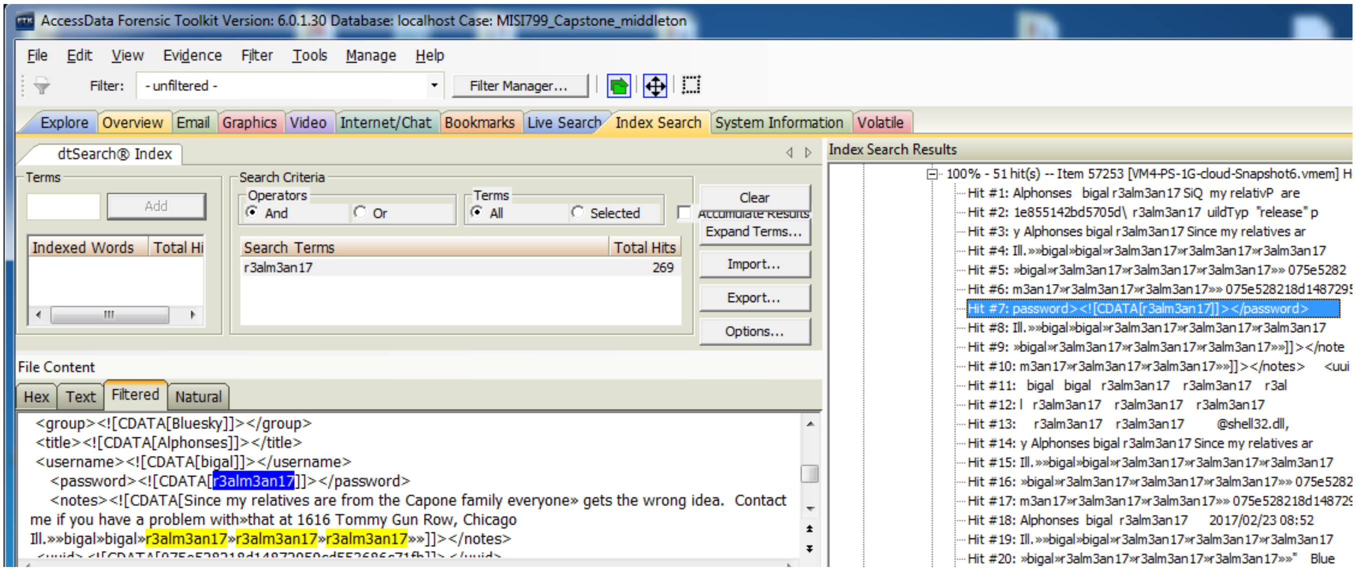
File Content (Filtered)

```
</tr>
<tr>
<td class="field_data">LaPalooza</td>
<td class="field_data">eastern56</td>
<td class="field_data"><code>n3wpass2017</code></td>a
md64" language="ar-SA" buildType="release" publicKeyToken="31bf3856ad364e35"
versionScope="nonSxS"/><assemblyIdentity name="Microsoft-Windows-crypt32-dll.Resources"
```

Index Search Results

```
⊞ dtSearch® Indexed Search {Prefilter:(all files) Query:("AB[n0accesshere]CD")} (ID:3) -- 30 hit(s) in 1 file(s)
⊞ dtSearch® Indexed Search {Prefilter:(all files) Query:("WX[secretp@ssword]YZ")} (ID:4) -- 17 hit(s) in 1 file(s)
⊟ dtSearch® Indexed Search {Prefilter:(all files) Query:("t00easy")} (ID:5) -- 415 hit(s) in 17 file(s)
   ⊞ Allocated Space -- 415 hit(s) in 17 file(s)
     Unallocated Space -- 0 hit(s) in 0 file(s)
⊟ dtSearch® Indexed Search {Prefilter:(all files) Query:("n3wpass2017")} (ID:6) -- 378 hit(s) in 15 file(s)
   ⊟ Allocated Space -- 378 hit(s) in 15 file(s)
      ⊟ Unknown Types  -- 378 hit(s) in 15 file(s)
         ⊟ Unknown Types - files 1-15  --- 378 hit(s) in 15 file(s)
            ⊟ 100% - 152 hit(s) -- Item 57296 [VM7-IE-4G-cloud-Snapshot7.vmem] HostHardDrive.E01/Basic
                 Hit #1: ield_data"><code>n3wpass2017</code></td>a  md64" l
                 Hit #2: br />   <br />   n3wpass2017<br />    <br />   n3w
                 Hit #3: r />    <br />   n3wpass2017<br />    </td>   </tr
                 Hit #4: ield_data"><code>n3wpass2017</code></td>    <td cl
                 Hit #5: br />   <br />   n3wpass2017<br />    <br />   n3w
                 Hit #6: r />    <br />   n3wpass2017<br />    </td>   </tr
                 Hit #7: E: 906-623-9475  n3wpass2017  n3wpass2017   This w
                 Hit #8: 75  n3wpass2017  n3wpass2017   This website allows
                 Hit #9: E: 906-623-9475  n3wpass2017  n3wpass2017   This w
                 Hit #10: 75  n3wpass2017  n3wpass2017   This website allows
                 Hit #11: 4,  0nthec0rner  n3wpass2017  tEXtSoftware  Adobe
```

Figure 65. This screenshot depicts one of the returned values during a dtSearch for the“**n3wpass17**” password from the LaPalooza entry on the KeePass Database (Clouds).



AccessData Forensic Toolkit Version: 6.0.1.30 Database: localhost Case: MISI799_Capstone_middleton

Filter: - unfiltered -

Indexed Words	Total Hi

Search Criteria — Operators: ● And ○ Or; Terms: ● All ○ Selected; □ Accumulate Results

Search Terms	Total Hits
r3alm3an17	269

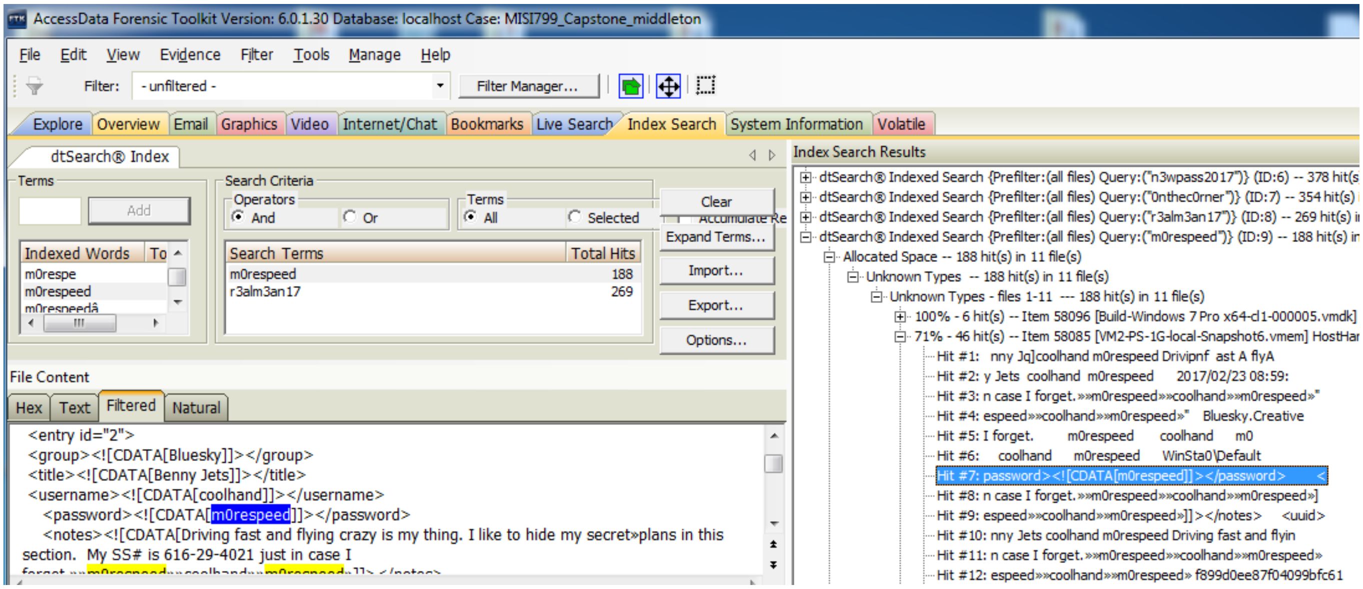
File Content (Filtered)

```
 <group><![CDATA[Bluesky]]></group>
 <title><![CDATA[Alphonses]]></title>
 <username><![CDATA[bigal]]></username>
   <password><![CDATA[r3alm3an17]]></password>
   <notes><![CDATA[Since my relatives are from the Capone family everyone» gets the wrong idea.  Contact
me if you have a problem with»that at 1616 Tommy Gun Row, Chicago
Ill.»»bigal»bigal»r3alm3an17»r3alm3an17»r3alm3an17»»]]></notes>
```

Index Search Results

```
⊟ 100% - 51 hit(s) -- Item 57253 [VM4-PS-1G-cloud-Snapshot6.vmem] H
     Hit #1: Alphonses   bigal r3alm3an17 SiQ  my relativP  are
     Hit #2: 1e855142bd5705d\  r3alm3an17  uildTyp  "release" p
     Hit #3: y Alphonses bigal r3alm3an17 Since my relatives ar
     Hit #4: Ill.»»bigal»bigal»r3alm3an17»r3alm3an17»r3alm3an17
     Hit #5: »bigal»r3alm3an17»r3alm3an17»r3alm3an17»» 075e5282
     Hit #6: m3an17»r3alm3an17»r3alm3an17»» 075e528218d148729
     Hit #7: password><![CDATA[r3alm3an17]]></password>
     Hit #8: Ill.»»bigal»bigal»r3alm3an17»r3alm3an17»r3alm3an17
     Hit #9: »bigal»r3alm3an17»r3alm3an17»r3alm3an17»»]]></note
     Hit #10: m3an17»r3alm3an17»r3alm3an17»»]]></notes>     <uui
     Hit #11:   bigal   bigal   r3alm3an17    r3alm3an17    r3al
     Hit #12: l   r3alm3an17    r3alm3an17    r3alm3an17
     Hit #13:     r3alm3an17    r3alm3an17        @shell32.dll,
     Hit #14: y Alphonses bigal r3alm3an17 Since my relatives ar
     Hit #15: Ill.»»bigal»bigal»r3alm3an17»r3alm3an17»r3alm3an17
     Hit #16: »bigal»r3alm3an17»r3alm3an17»r3alm3an17»» 075e5282
     Hit #17: m3an17»r3alm3an17»r3alm3an17»» 075e528218d14872
     Hit #18: Alphonses  bigal  r3alm3an17      2017/02/23 08:52
     Hit #19: Ill.»»bigal»bigal»r3alm3an17»r3alm3an17»r3alm3an17
     Hit #20: »bigal»r3alm3an17»r3alm3an17»r3alm3an17»»"   Blue
```

Figure 66. This screenshot depicts one of the returned values during a dtSearch for the“**r3alm3an17**” password from the Alphonses entry on the Password Safe Database (Bluesky).


AccessData Forensic Toolkit Version: 6.0.1.30 Database: localhost Case: MISI799_Capstone_middleton
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
dtSearch® Index
Terms
Add
Search Criteria
Operators
● And ○ Or
Terms
● All ○ Selected
Clear
Expand Terms...
Import...
Export...
Options...
File Content
Hex Text Filtered Natural
Index Search Results

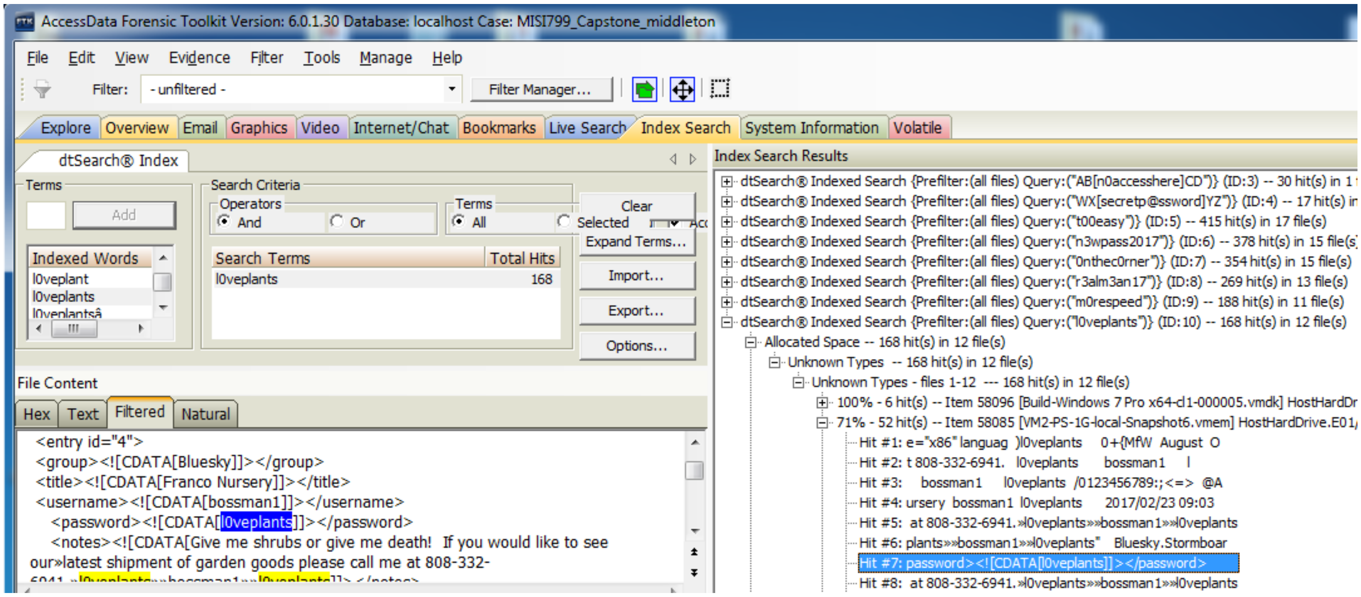
Indexed Words
m0respe
m0respeed
m0respeedâ

Search Terms	Total Hits
m0respeed	188
r3alm3an17	269

```
<entry id="2">
<group><![CDATA[Bluesky]]></group>
<title><![CDATA[Benny Jets]]></title>
<username><![CDATA[coolhand]]></username>
  <password><![CDATA[m0respeed]]></password>
  <notes><![CDATA[Driving fast and flying crazy is my thing. I like to hide my secret»plans in this
section.  My SS# is 616-29-4021 just in case I
```

```
dtSearch® Indexed Search {Prefilter:(all files) Query:("n3wpass2017")} (ID:6) -- 378 hit(s
dtSearch® Indexed Search {Prefilter:(all files) Query:("0nthec0rner")} (ID:7) -- 354 hit(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("r3alm3an17")} (ID:8) -- 269 hit(s) i
dtSearch® Indexed Search {Prefilter:(all files) Query:("m0respeed")} (ID:9) -- 188 hit(s) ir
  Allocated Space -- 188 hit(s) in 11 file(s)
    Unknown Types  -- 188 hit(s) in 11 file(s)
      Unknown Types - files 1-11  --- 188 hit(s) in 11 file(s)
        100% - 6 hit(s) -- Item 58096 [Build-Windows 7 Pro x64-cl1-000005.vmdk]
        71% - 46 hit(s) -- Item 58085 [VM2-PS-1G-local-Snapshot6.vmem] HostHar
          Hit #1:  nny Jq]coolhand m0respeed Drivipnf  ast A flyA
          Hit #2: y Jets  coolhand  m0respeed     2017/02/23 08:59:
          Hit #3: n case I forget.»»m0respeed»»coolhand»»m0respeed»"
          Hit #4: espeed»»coolhand»»m0respeed»"   Bluesky.Creative
          Hit #5: I forget.       m0respeed     coolhand     m0
          Hit #6:    coolhand     m0respeed     WinSta0\Default
          Hit #7: password><![CDATA[m0respeed]]></password>       <
          Hit #8: n case I forget.»»m0respeed»»coolhand»»m0respeed»]
          Hit #9: espeed»»coolhand»»m0respeed»]]></notes>     <uuid>
          Hit #10: nny Jets coolhand m0respeed Driving fast and flyin
          Hit #11: n case I forget.»»m0respeed»»coolhand»»m0respeed»
          Hit #12: espeed»»coolhand»»m0respeed» f899d0ee87f04099bfc61
```

Figure 67. This screenshot depicts one of the returned values during a dtSearch for the“**m0respeed**” password from the Benny Jets entry on the Password Safe Database (Bluesky).


AccessData Forensic Toolkit Version: 6.0.1.30 Database: localhost Case: MISI799_Capstone_middleton
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
dtSearch® Index
Terms
Add
Search Criteria
Operators
● And ○ Or
Terms
● All ○ Selected
Clear
Expand Terms...
Import...
Export...
Options...
File Content
Hex Text Filtered Natural
Index Search Results

Indexed Words
l0veplant
l0veplants
l0veplantsâ

Search Terms	Total Hits
l0veplants	168

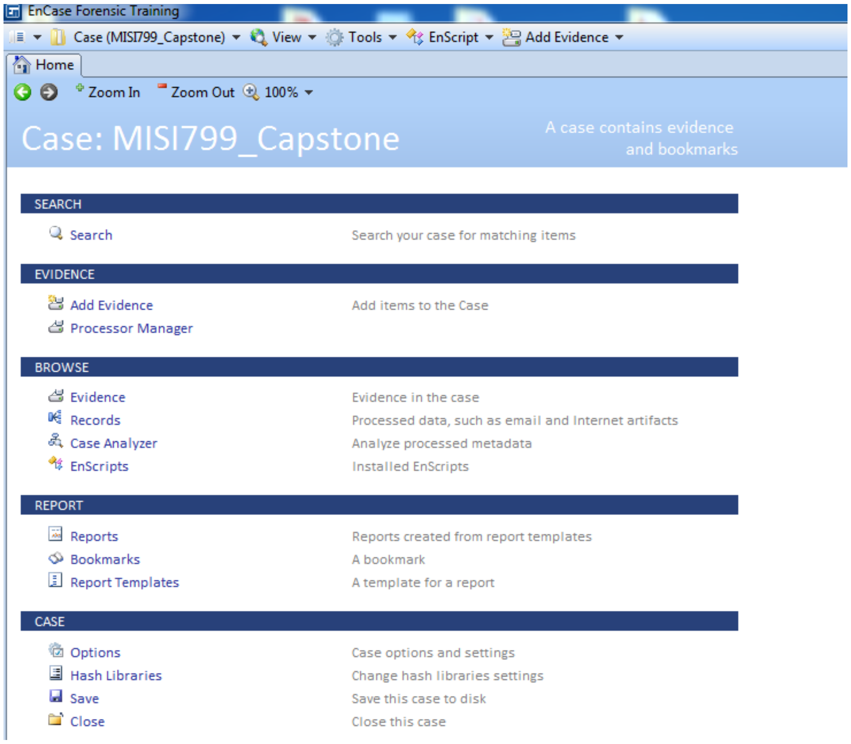
```
<entry id="4">
<group><![CDATA[Bluesky]]></group>
<title><![CDATA[Franco Nursery]]></title>
<username><![CDATA[bossman1]]></username>
  <password><![CDATA[l0veplants]]></password>
  <notes><![CDATA[Give me shrubs or give me death!  If you would like to see
our»latest shipment of garden goods please call me at 808-332-
```

```
dtSearch® Indexed Search {Prefilter:(all files) Query:("AB[n0accesshere]CD")} (ID:3) -- 30 hit(s) in 1
dtSearch® Indexed Search {Prefilter:(all files) Query:("WX[secretp@ssword]YZ")} (ID:4) -- 17 hit(s) ir
dtSearch® Indexed Search {Prefilter:(all files) Query:("t00easy")} (ID:5) -- 415 hit(s) in 17 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("n3wpass2017")} (ID:6) -- 378 hit(s) in 15 file(s
dtSearch® Indexed Search {Prefilter:(all files) Query:("0nthec0rner")} (ID:7) -- 354 hit(s) in 15 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("r3alm3an17")} (ID:8) -- 269 hit(s) in 13 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("m0respeed")} (ID:9) -- 188 hit(s) in 11 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("l0veplants")} (ID:10) -- 168 hit(s) in 12 file(s)
  Allocated Space -- 168 hit(s) in 12 file(s)
    Unknown Types  -- 168 hit(s) in 12 file(s)
      Unknown Types - files 1-12  --- 168 hit(s) in 12 file(s)
        100% - 6 hit(s) -- Item 58096 [Build-Windows 7 Pro x64-cl1-000005.vmdk] HostHardDr
        71% - 52 hit(s) -- Item 58085 [VM2-PS-1G-local-Snapshot6.vmem] HostHardDrive.E01/
          Hit #1: e="x86" languag  )l0veplants    0+{MfW  August  O
          Hit #2: t 808-332-6941.  l0veplants      bossman1     l
          Hit #3:    bossman1     l0veplants  /0123456789:;<=>  @A
          Hit #4: ursery  bossman1  l0veplants     2017/02/23 09:03
          Hit #5:  at 808-332-6941.»l0veplants»»bossman1»»l0veplants
          Hit #6: plants»»bossman1»»l0veplants"   Bluesky.Stormboar
          Hit #7: password><![CDATA[l0veplants]]></password>
          Hit #8:  at 808-332-6941.»l0veplants»»bossman1»»l0veplants
```

Figure 68. This screenshot depicts one of the returned values during a dtSearch for the“**l0veplants**” password Franco Nursery entry on the Password Safe Database (Bluesky).

Appendix F

EnCase Forensic Examiner Screenshots



Case: MISI799_Capstone

A case contains evidence and bookmarks

SEARCH

Search	Search your case for matching items

EVIDENCE

Add Evidence	Add items to the Case
Processor Manager	

BROWSE

Evidence	Evidence in the case
Records	Processed data, such as email and Internet artifacts
Case Analyzer	Analyze processed metadata
EnScripts	Installed EnScripts

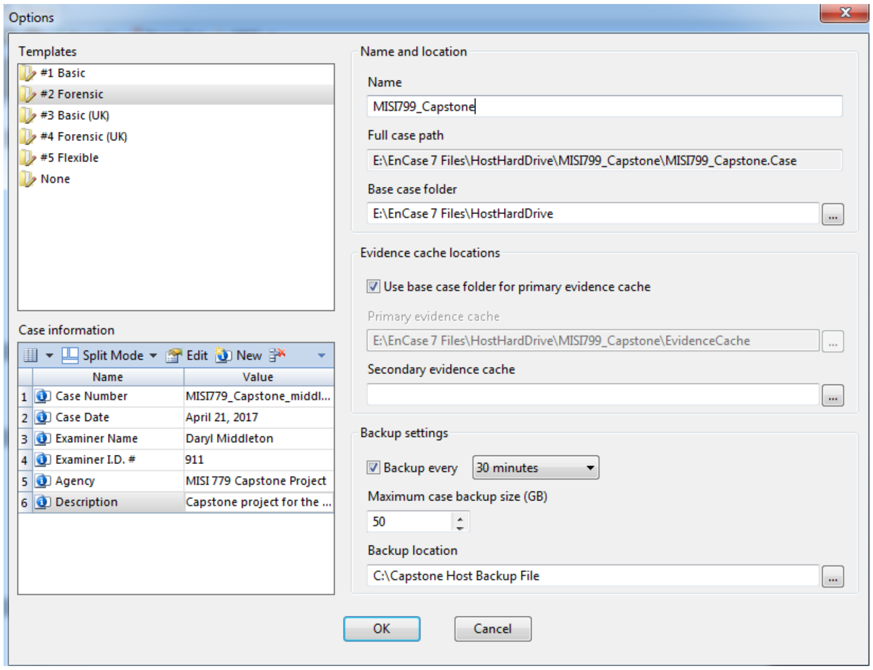
REPORT

Reports	Reports created from report templates
Bookmarks	A bookmark
Report Templates	A template for a report

CASE

Options	Case options and settings
Hash Libraries	Change hash libraries settings
Save	Save this case to disk
Close	Close this case

Figure 69. This is the start page to access the MISI799_Capstone Case



Templates

- #1 Basic
- #2 Forensic
- #3 Basic (UK)
- #4 Forensic (UK)
- #5 Flexible
- None

Case information

	Name	Value
1	Case Number	MISI779_Capstone_middl...
2	Case Date	April 21, 2017
3	Examiner Name	Daryl Middleton
4	Examiner I.D. #	911
5	Agency	MISI 779 Capstone Project
6	Description	Capstone project for the ...

Name and location

Name: MISI799_Capstone

Full case path: E:\EnCase 7 Files\HostHardDrive\MISI799_Capstone\MISI799_Capstone.Case

Base case folder: E:\EnCase 7 Files\HostHardDrive

Evidence cache locations

☑ Use base case folder for primary evidence cache

Primary evidence cache: E:\EnCase 7 Files\HostHardDrive\MISI799_Capstone\EvidenceCache

Secondary evidence cache:

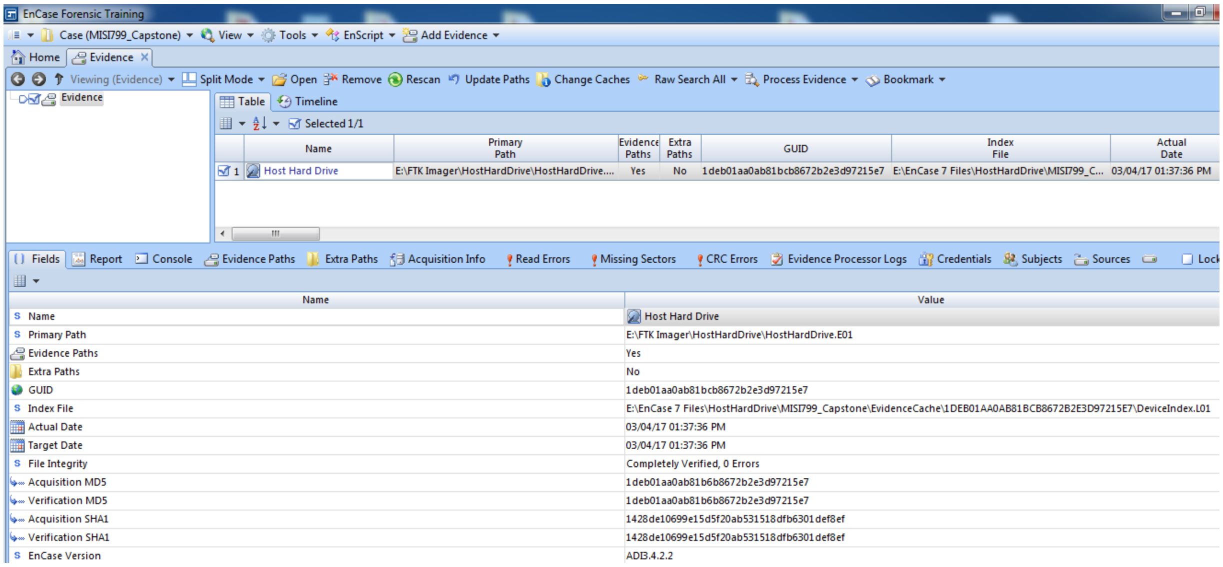
Backup settings

☑ Backup every 30 minutes

Maximum case backup size (GB): 50

Backup location: C:\Capstone Host Backup File

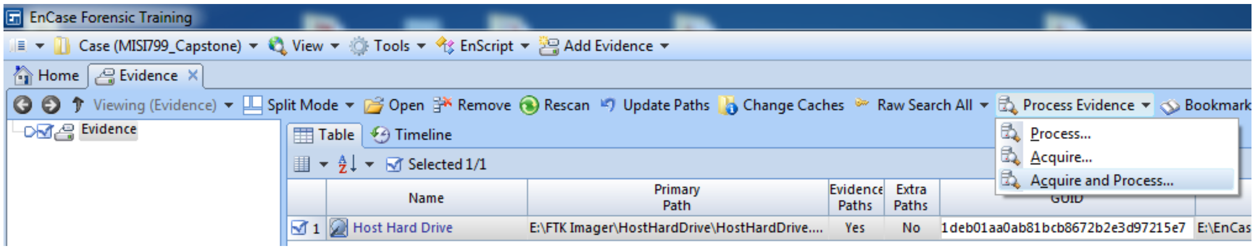
Figure 70. Options page to setup Name, Case Path, Backup and Report Template



	Name	Primary Path	Evidence Paths	Extra Paths	GUID	Index File	Actual Date
☑ 1	Host Hard Drive	E:\FTK Imager\HostHardDrive\HostHardDrive....	Yes	No	1deb01aa0ab81bcb8672b2e3d97215e7	E:\EnCase 7 Files\HostHardDrive\MISI799_C...	03/04/17 01:37:36 PM

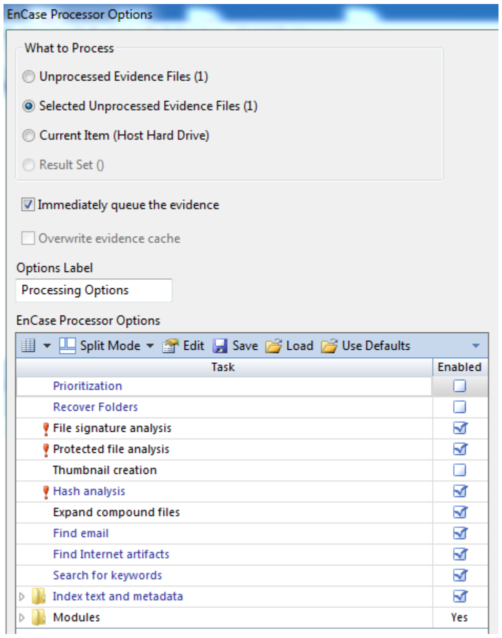
Name	Value
Name	Host Hard Drive
Primary Path	E:\FTK Imager\HostHardDrive\HostHardDrive.E01
Evidence Paths	Yes
Extra Paths	No
GUID	1deb01aa0ab81bcb8672b2e3d97215e7
Index File	E:\EnCase 7 Files\HostHardDrive\MISI799_Capstone\EvidenceCache\1DEB01AA0AB81BCB8672B2E3D97215E7\DeviceIndex.L01
Actual Date	03/04/17 01:37:36 PM
Target Date	03/04/17 01:37:36 PM
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	1deb01aa0ab81b6b8672b2e3d97215e7
Verification MD5	1deb01aa0ab81b6b8672b2e3d97215e7
Acquisition SHA1	1428de10699e15d5f20ab531518dfb6301def8ef
Verification SHA1	1428de10699e15d5f20ab531518dfb6301def8ef
EnCase Version	ADI3.4.2.2

Figure 71. Image verification results for HostHardDrive.E01 including file integrity hashes.



	Name	Primary Path	Evidence Paths	Extra Paths	GUID	
☑ 1	Host Hard Drive	E:\FTK Imager\HostHardDrive\HostHardDrive....	Yes	No	1deb01aa0ab81bcb8672b2e3d97215e7	E:\EnCas

Figure 72. The evidence processing begins by selecting the evidence and then Acquire and Process.


EnCase Processor Options

What to Process

○ Unprocessed Evidence Files (1)

● Selected Unprocessed Evidence Files (1)

○ Current Item (Host Hard Drive)

○ Result Set ()

☑ Immediately queue the evidence

☐ Overwrite evidence cache

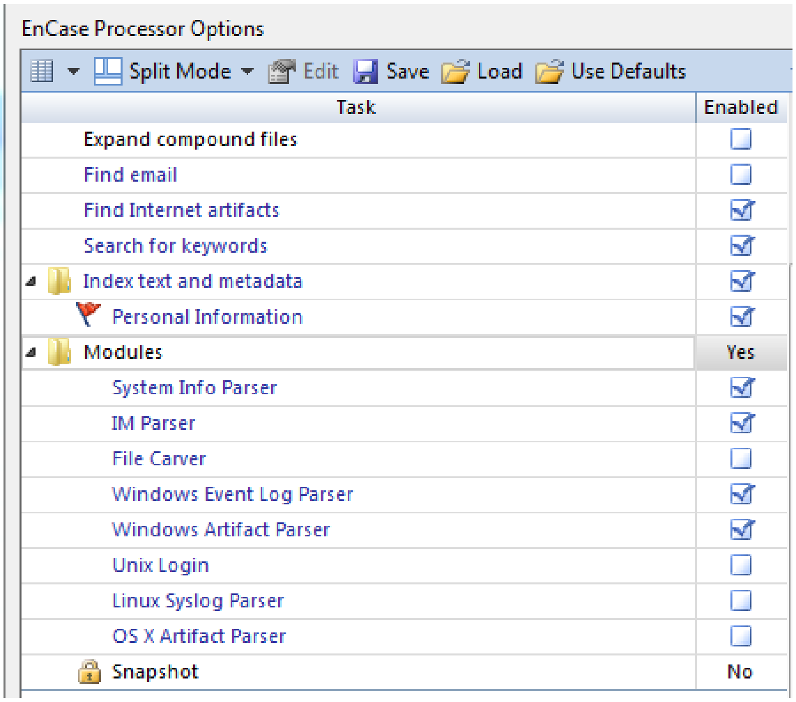
Options Label

Processing Options

EnCase Processor Options

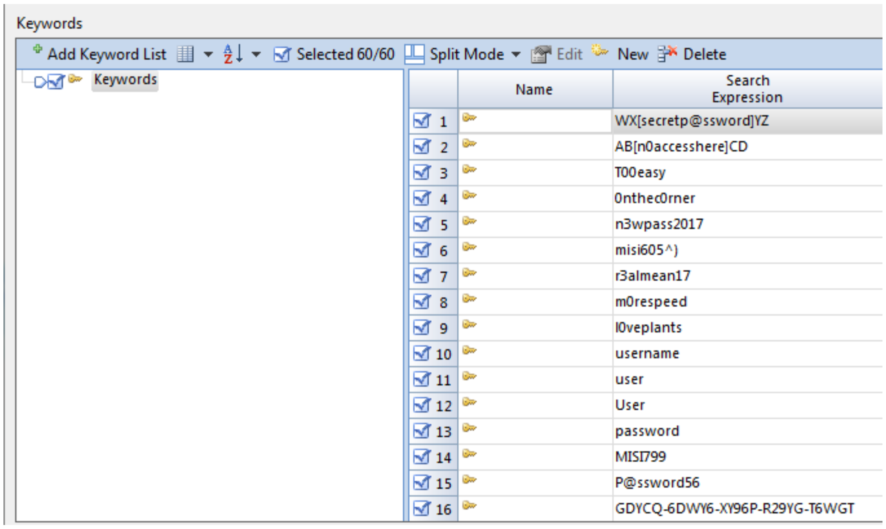
Task	Enabled
Prioritization	☐
Recover Folders	☐
File signature analysis	☑
Protected file analysis	☑
Thumbnail creation	☐
Hash analysis	☑
Expand compound files	☑
Find email	☑
Find Internet artifacts	☑
Search for keywords	☑
Index text and metadata	☑
Modules	Yes

Figure 73. This is the first section of the EnCase Processor Options that are available.



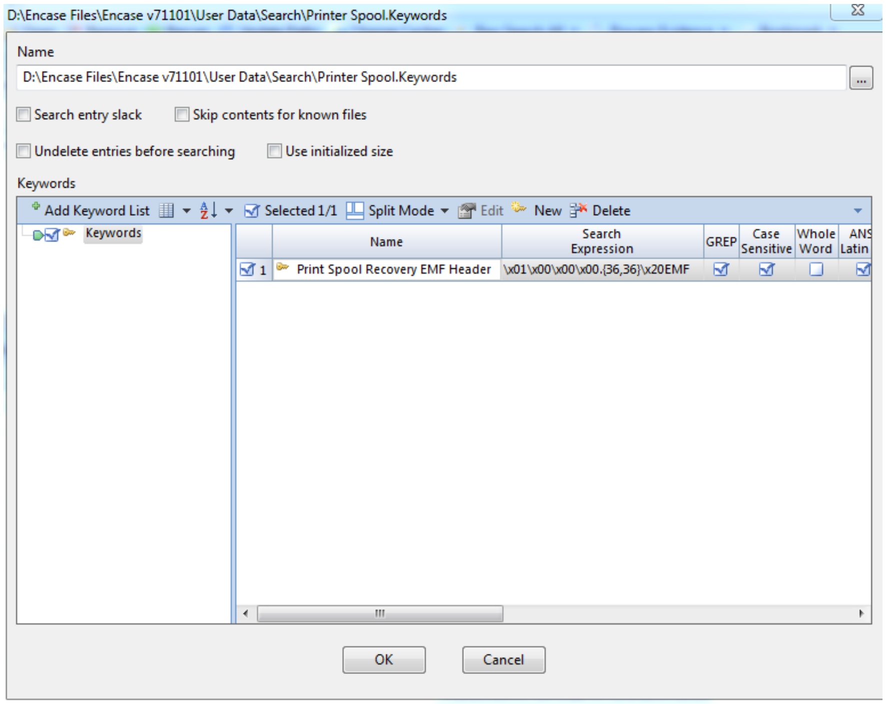
Task	Enabled
Expand compound files	□
Find email	□
Find Internet artifacts	☑
Search for keywords	☑
Index text and metadata	☑
Personal Information	☑
Modules	Yes
System Info Parser	☑
IM Parser	☑
File Carver	□
Windows Event Log Parser	☑
Windows Artifact Parser	☑
Unix Login	□
Linux Syslog Parser	□
OS X Artifact Parser	□
Snapshot	No

Figure 74. Expanded evidence processing modules in EnCase Processor Options.



	Name	Search Expression
☑ 1		WX[secretp@ssword]YZ
☑ 2		AB[n0accesshere]CD
☑ 3		T00easy
☑ 4		0nthec0rner
☑ 5		n3wpass2017
☑ 6		misi605^)
☑ 7		r3almean17
☑ 8		m0respeed
☑ 9		l0veplants
☑ 10		username
☑ 11		user
☑ 12		User
☑ 13		password
☑ 14		MISI799
☑ 15		P@ssword56
☑ 16		GDYCQ-6DWY6-XY96P-R29YG-T6WGT

Figure 75. This is a keyword list to search the hard drive images for significant data.



D:\Encase Files\Encase v71101\User Data\Search\Printer Spool.Keywords

Name

D:\Encase Files\Encase v71101\User Data\Search\Printer Spool.Keywords

☐ Search entry slack ☐ Skip contents for known files

☐ Undelete entries before searching ☐ Use initialized size

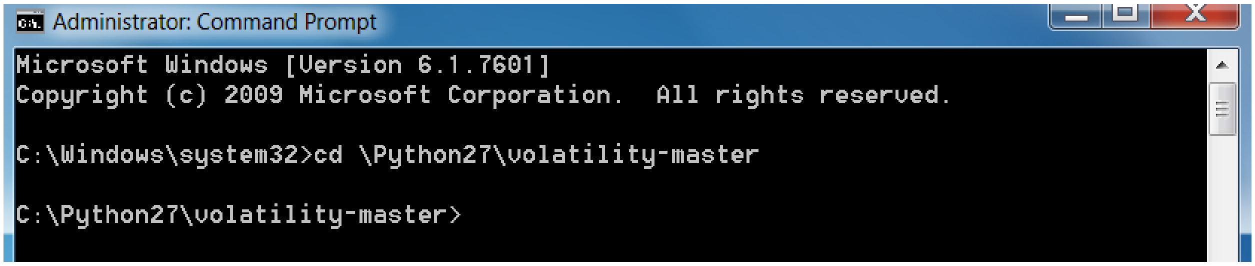
Keywords

	Name	Search Expression	GREP	Case Sensitive	Whole Word	ANS Latin
☑ 1	Print Spool Recovery EMF Header	\x01\x00\x00\x00.{36,36}\x20EMF	☑	☑	☐	☑

Figure 76. Developing a Search Expression for Print Spool Recovery.

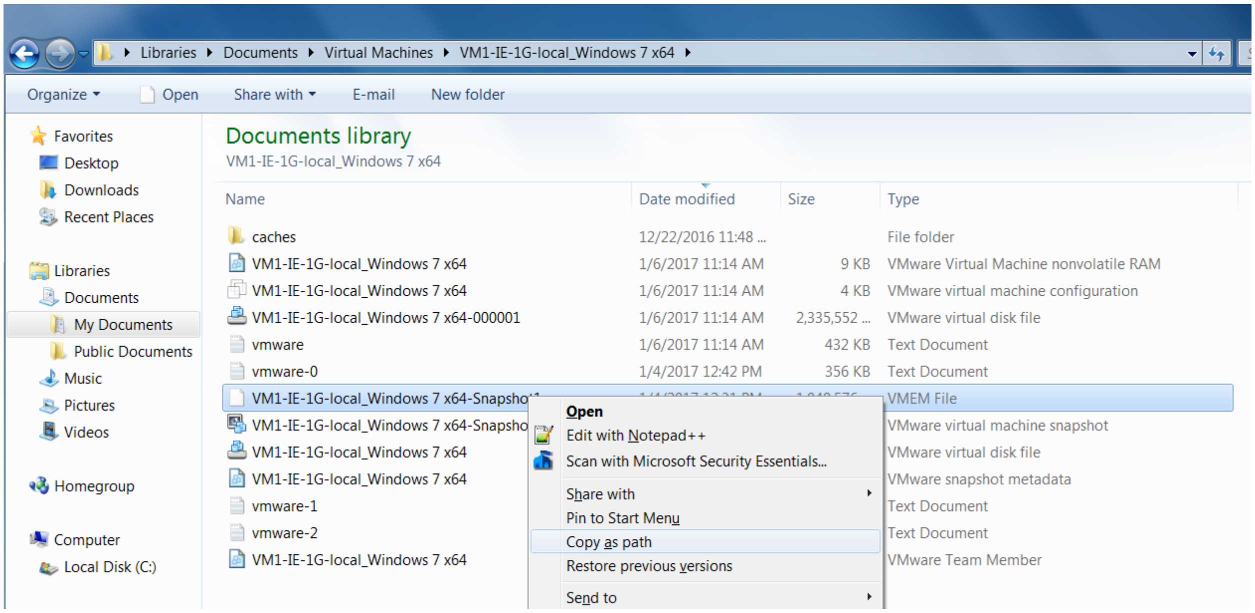
Appendix G

This Depicts a Series of Python Volatility Screenshots



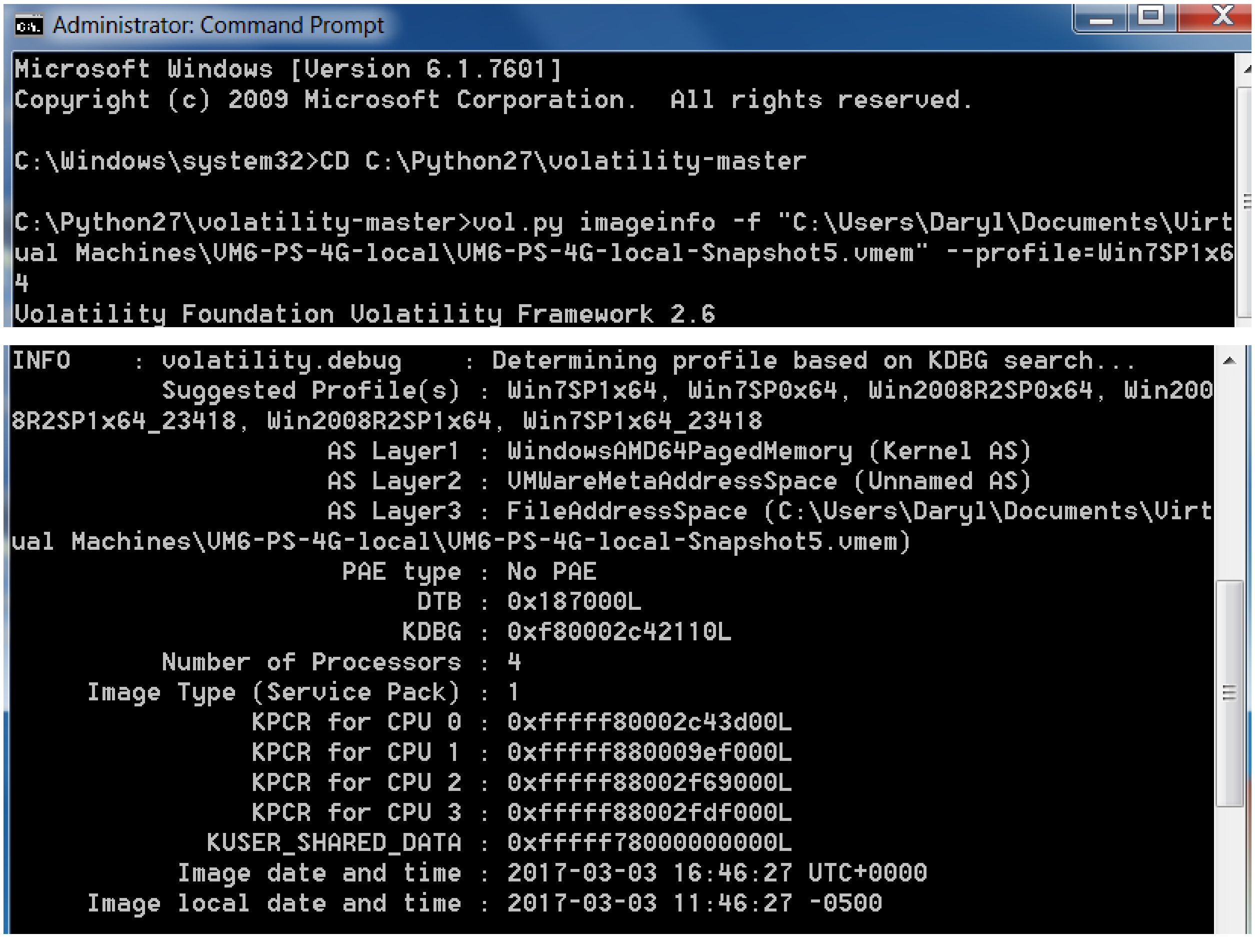
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd \Python27\volatility-master

C:\Python27\volatility-master>
```

Figure 77. The command prompt utilized to access Python Volatility Memory Analysis Framework.



Name	Date modified	Size	Type
caches	12/22/2016 11:48 ...		File folder
VM1-IE-1G-local_Windows 7 x64	1/6/2017 11:14 AM	9 KB	VMware Virtual Machine nonvolatile RAM
VM1-IE-1G-local_Windows 7 x64	1/6/2017 11:14 AM	4 KB	VMware virtual machine configuration
VM1-IE-1G-local_Windows 7 x64-000001	1/6/2017 11:14 AM	2,335,552 ...	VMware virtual disk file
vmware	1/6/2017 11:14 AM	432 KB	Text Document
vmware-0	1/4/2017 12:42 PM	356 KB	Text Document
VM1-IE-1G-local_Windows 7 x64-Snapshot1			VMEM File
VM1-IE-1G-local_Windows 7 x64-Snapsho			VMware virtual machine snapshot
VM1-IE-1G-local_Windows 7 x64			VMware virtual disk file
VM1-IE-1G-local_Windows 7 x64			VMware snapshot metadata
vmware-1			Text Document
vmware-2			Text Document
VM1-IE-1G-local_Windows 7 x64			VMware Team Member

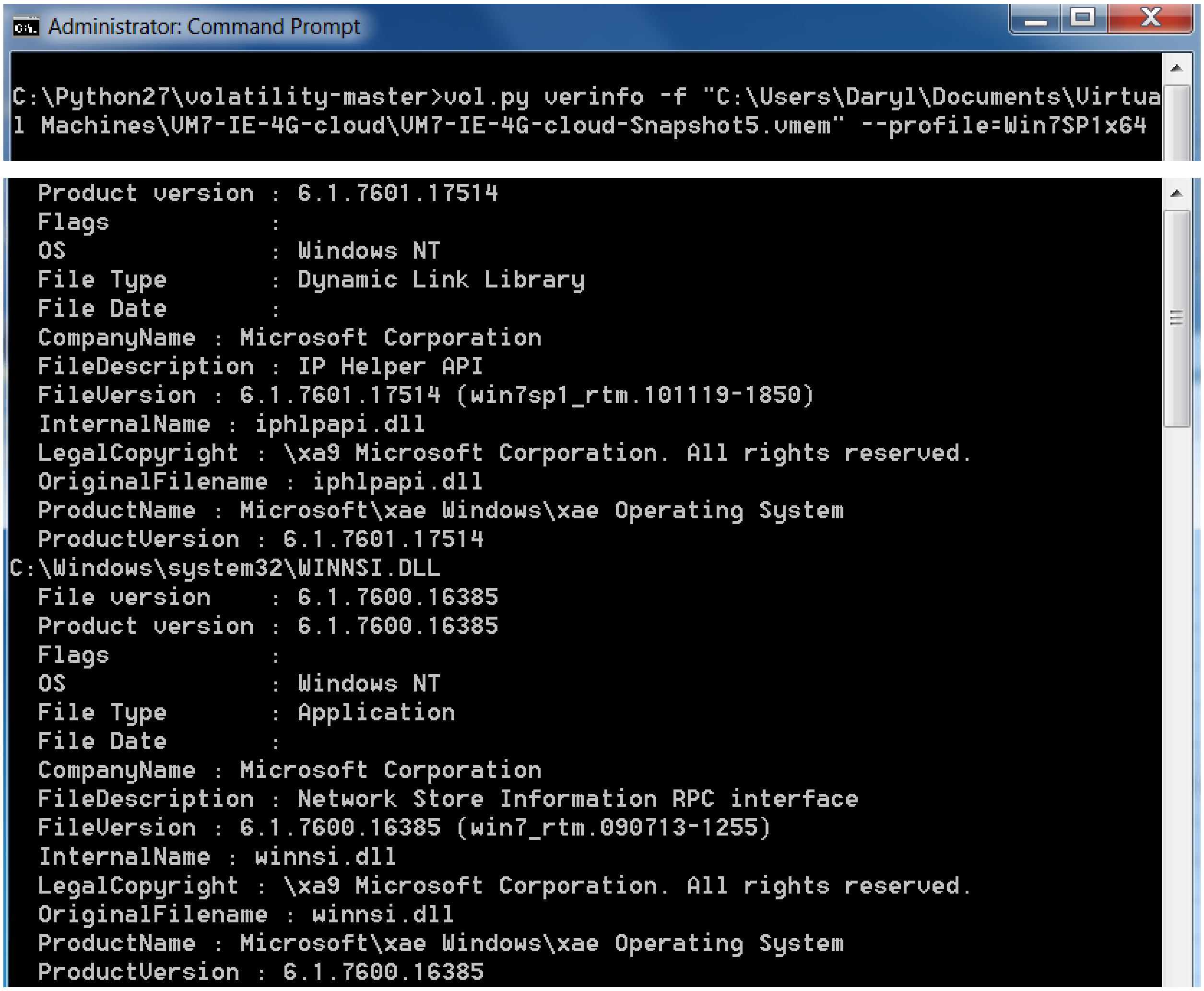
Figure 78. The “Copy as Path” selection allows the explicit path to be pasted in a Command Line which is much faster and reduces errors in typing each command for testing.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>CD C:\Python27\volatility-master

C:\Python27\volatility-master>vol.py imageinfo -f "C:\Users\Daryl\Documents\Virt
ual Machines\VM6-PS-4G-local\VM6-PS-4G-local-Snapshot5.vmem" --profile=Win7SP1x6
4
Volatility Foundation Volatility Framework 2.6
```

```
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win200
8R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : VMWareMetaAddressSpace (Unnamed AS)
                     AS Layer3 : FileAddressSpace (C:\Users\Daryl\Documents\Virt
ual Machines\VM6-PS-4G-local\VM6-PS-4G-local-Snapshot5.vmem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002c42110L
          Number of Processors : 4
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002c43d00L
                KPCR for CPU 1 : 0xfffff880009ef000L
                KPCR for CPU 2 : 0xfffff88002f69000L
                KPCR for CPU 3 : 0xfffff88002fdf000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2017-03-03 16:46:27 UTC+0000
     Image local date and time : 2017-03-03 11:46:27 -0500
```

Figure 79. Volatility “imageinfo” module with sample output.

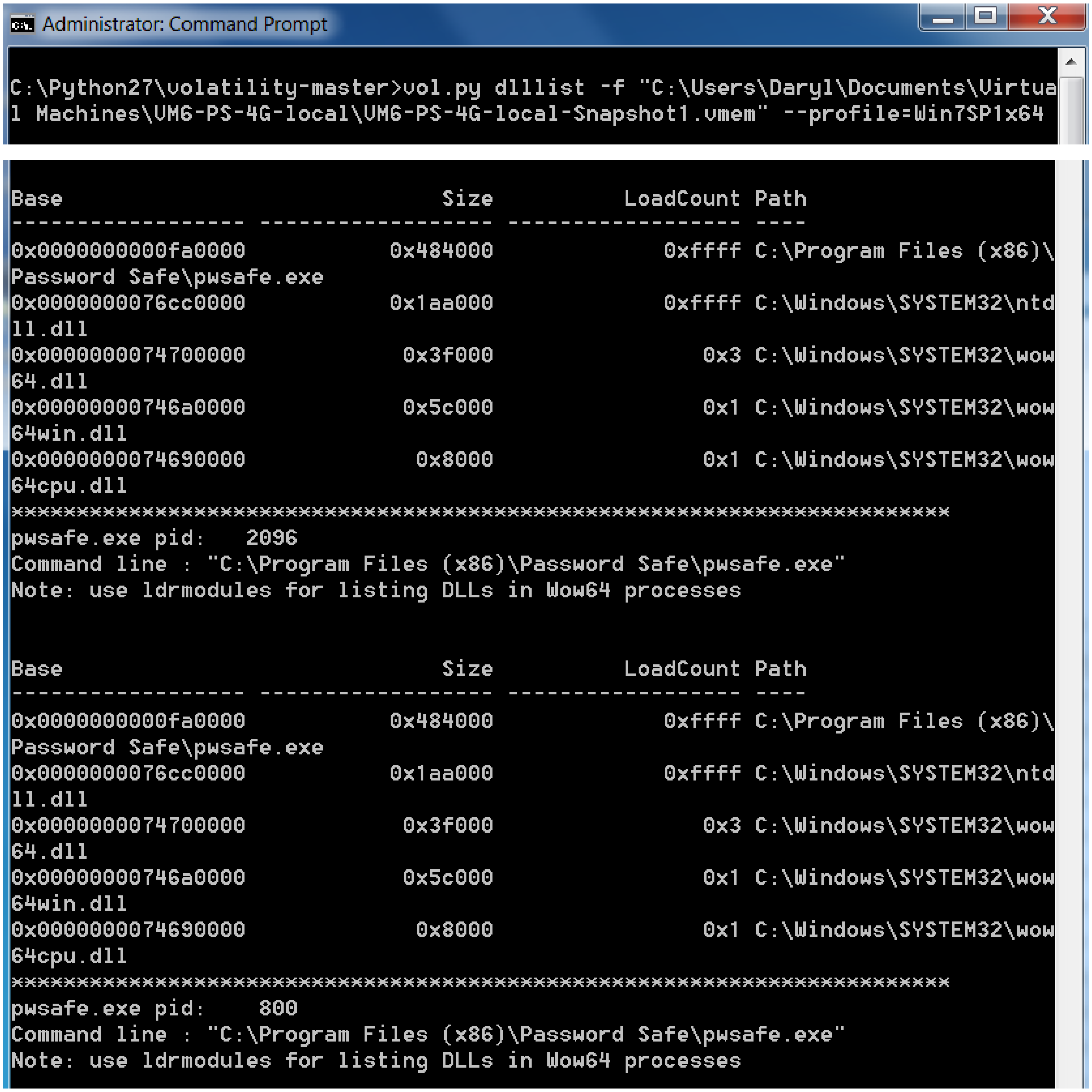


Administrator: Command Prompt

```
C:\Python27\volatility-master>vol.py verinfo -f "C:\Users\Daryl\Documents\Virtua
l Machines\VM7-IE-4G-cloud\VM7-IE-4G-cloud-Snapshot5.vmem" --profile=Win7SP1x64
```

```
  Product version : 6.1.7601.17514
  Flags           :
  OS              : Windows NT
  File Type       : Dynamic Link Library
  File Date       :
  CompanyName : Microsoft Corporation
  FileDescription : IP Helper API
  FileVersion : 6.1.7601.17514 (win7sp1_rtm.101119-1850)
  InternalName : iphlpapi.dll
  LegalCopyright : \xa9 Microsoft Corporation. All rights reserved.
  OriginalFilename : iphlpapi.dll
  ProductName : Microsoft\xae Windows\xae Operating System
  ProductVersion : 6.1.7601.17514
C:\Windows\system32\WINNSI.DLL
  File version    : 6.1.7600.16385
  Product version : 6.1.7600.16385
  Flags           :
  OS              : Windows NT
  File Type       : Application
  File Date       :
  CompanyName : Microsoft Corporation
  FileDescription : Network Store Information RPC interface
  FileVersion : 6.1.7600.16385 (win7_rtm.090713-1255)
  InternalName : winnsi.dll
  LegalCopyright : \xa9 Microsoft Corporation. All rights reserved.
  OriginalFilename : winnsi.dll
  ProductName : Microsoft\xae Windows\xae Operating System
  ProductVersion : 6.1.7600.16385
```

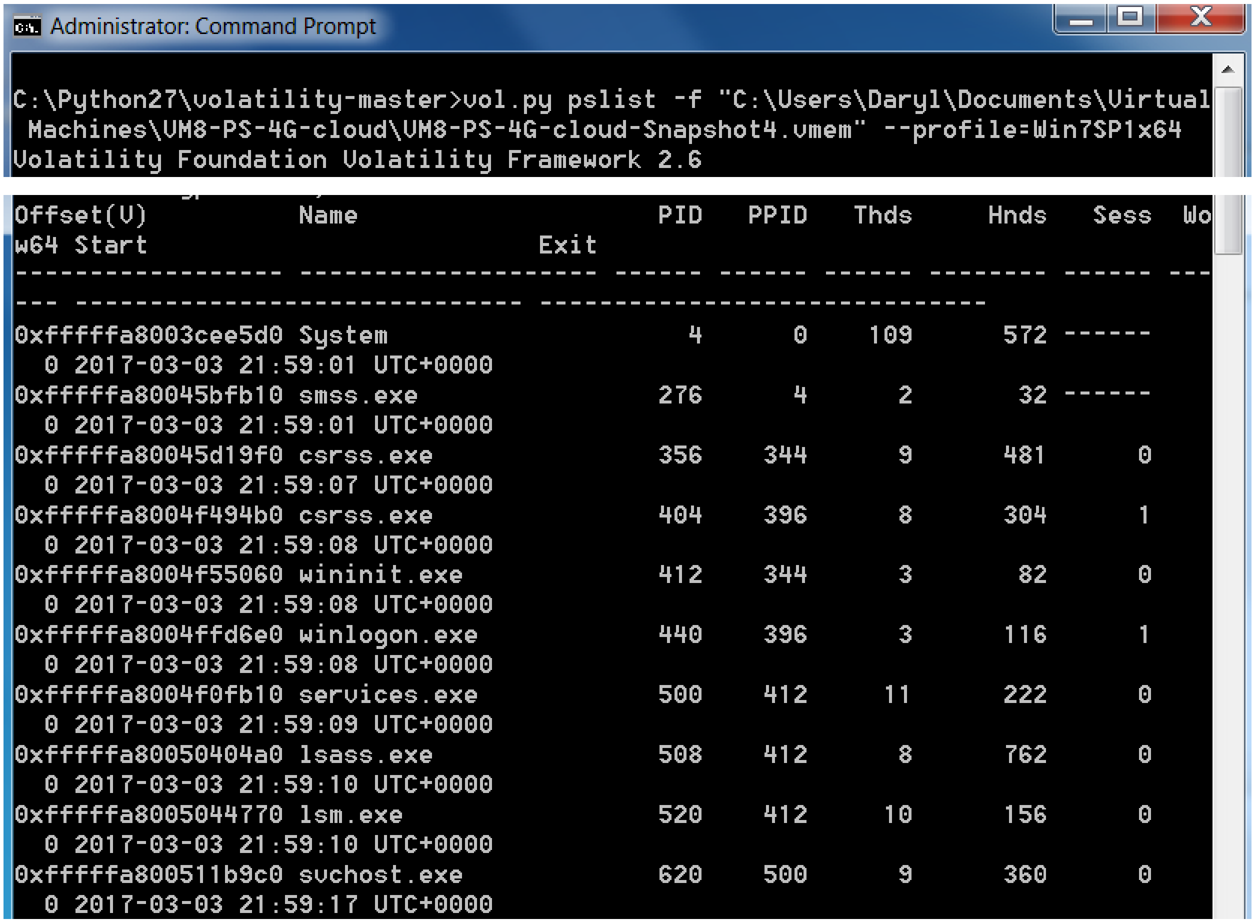
Figure 80. Volatility “verinfo” module with sample output.



```
C:\Python27\volatility-master>vol.py dlllist -f "C:\Users\Daryl\Documents\Virtua
l Machines\VM6-PS-4G-local\VM6-PS-4G-local-Snapshot1.vmem" --profile=Win7SP1x64
```

```
Base                             Size          LoadCount Path
------------------ ------------------ ------------------ ----
0x0000000000fa0000           0x484000             0xffff C:\Program Files (x86)\
Password Safe\pwsafe.exe
0x0000000076cc0000           0x1aa000             0xffff C:\Windows\SYSTEM32\ntd
ll.dll
0x0000000074700000            0x3f000                0x3 C:\Windows\SYSTEM32\wow
64.dll
0x00000000746a0000            0x5c000                0x1 C:\Windows\SYSTEM32\wow
64win.dll
0x0000000074690000             0x8000                0x1 C:\Windows\SYSTEM32\wow
64cpu.dll
************************************************************************
pwsafe.exe pid:   2096
Command line : "C:\Program Files (x86)\Password Safe\pwsafe.exe"
Note: use ldrmodules for listing DLLs in Wow64 processes


Base                             Size          LoadCount Path
------------------ ------------------ ------------------ ----
0x0000000000fa0000           0x484000             0xffff C:\Program Files (x86)\
Password Safe\pwsafe.exe
0x0000000076cc0000           0x1aa000             0xffff C:\Windows\SYSTEM32\ntd
ll.dll
0x0000000074700000            0x3f000                0x3 C:\Windows\SYSTEM32\wow
64.dll
0x00000000746a0000            0x5c000                0x1 C:\Windows\SYSTEM32\wow
64win.dll
0x0000000074690000             0x8000                0x1 C:\Windows\SYSTEM32\wow
64cpu.dll
************************************************************************
pwsafe.exe pid:    800
Command line : "C:\Program Files (x86)\Password Safe\pwsafe.exe"
Note: use ldrmodules for listing DLLs in Wow64 processes
```

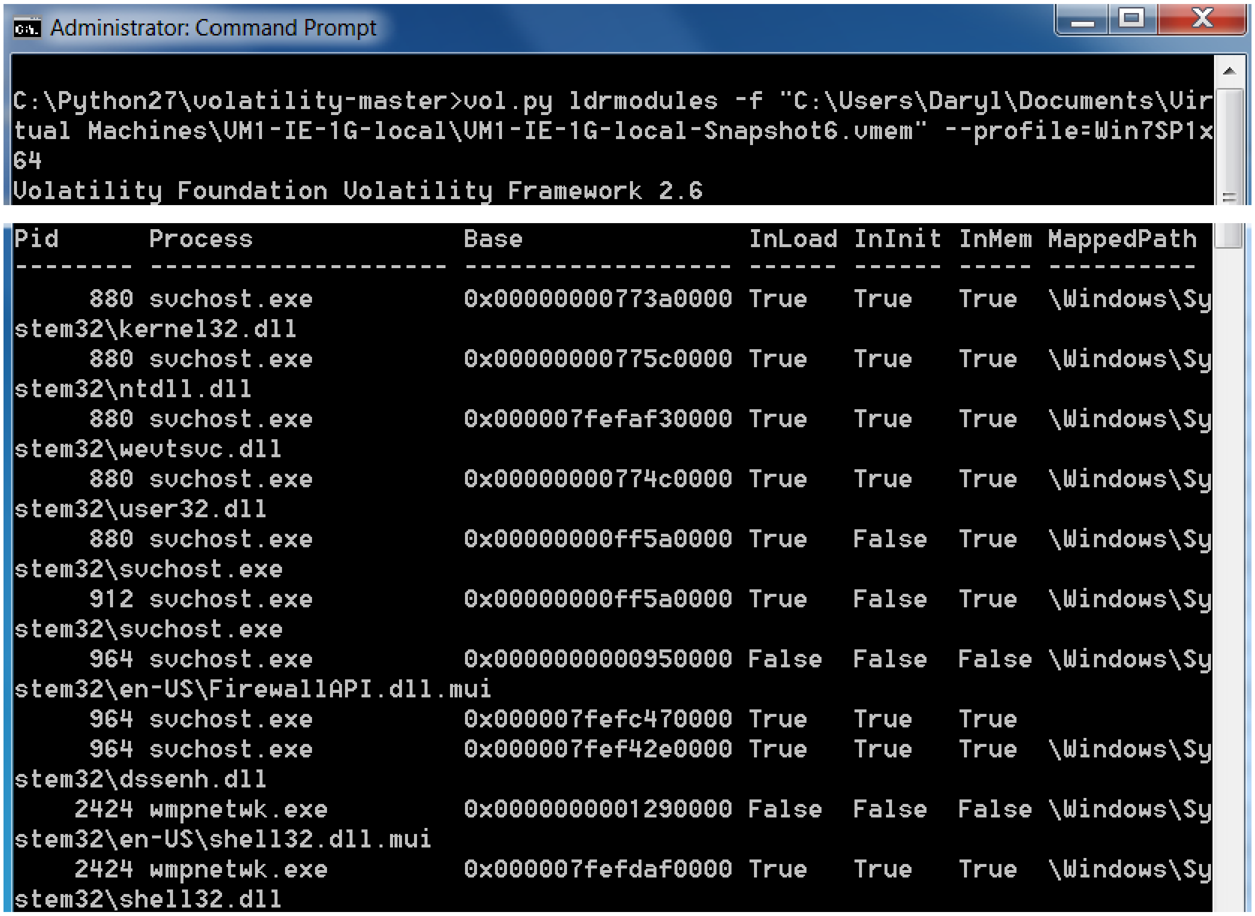
Figure 81. Volatility “dlllist” module with sample output.



```
C:\Python27\volatility-master>vol.py pslist -f "C:\Users\Daryl\Documents\Virtual
 Machines\VM8-PS-4G-cloud\VM8-PS-4G-cloud-Snapshot4.vmem" --profile=Win7SP1x64
Volatility Foundation Volatility Framework 2.6
```

```
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wo
w64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ---
--- ------------------------------ ------------------------------
0xfffffa8003cee5d0 System                    4      0    109      572 ------
  0 2017-03-03 21:59:01 UTC+0000
0xfffffa80045bfb10 smss.exe                276      4      2       32 ------
  0 2017-03-03 21:59:01 UTC+0000
0xfffffa80045d19f0 csrss.exe               356    344      9      481      0
  0 2017-03-03 21:59:07 UTC+0000
0xfffffa8004f494b0 csrss.exe               404    396      8      304      1
  0 2017-03-03 21:59:08 UTC+0000
0xfffffa8004f55060 wininit.exe             412    344      3       82      0
  0 2017-03-03 21:59:08 UTC+0000
0xfffffa8004ffd6e0 winlogon.exe            440    396      3      116      1
  0 2017-03-03 21:59:08 UTC+0000
0xfffffa8004f0fb10 services.exe            500    412     11      222      0
  0 2017-03-03 21:59:09 UTC+0000
0xfffffa80050404a0 lsass.exe               508    412      8      762      0
  0 2017-03-03 21:59:10 UTC+0000
0xfffffa8005044770 lsm.exe                 520    412     10      156      0
  0 2017-03-03 21:59:10 UTC+0000
0xfffffa800511b9c0 svchost.exe             620    500      9      360      0
  0 2017-03-03 21:59:17 UTC+0000
```

Figure 82. Volatility “pslist” module with sample output.



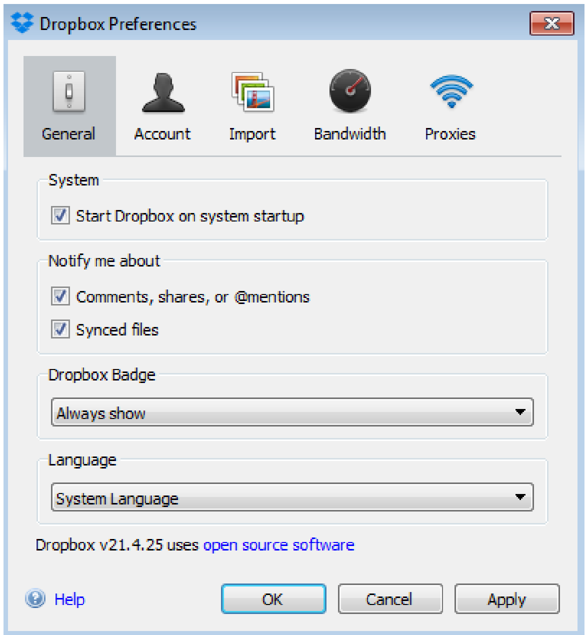
```
C:\Python27\volatility-master>vol.py ldrmodules -f "C:\Users\Daryl\Documents\Vir
tual Machines\VM1-IE-1G-local\VM1-IE-1G-local-Snapshot6.vmem" --profile=Win7SP1x
64
Volatility Foundation Volatility Framework 2.6
```

```
Pid      Process              Base               InLoad InInit InMem MappedPath
-------- -------------------- ------------------ ------ ------ ----- ----------
     880 svchost.exe          0x00000000773a0000 True   True   True  \Windows\Sy
stem32\kernel32.dll
     880 svchost.exe          0x00000000775c0000 True   True   True  \Windows\Sy
stem32\ntdll.dll
     880 svchost.exe          0x000007fefaf30000 True   True   True  \Windows\Sy
stem32\wevtsvc.dll
     880 svchost.exe          0x00000000774c0000 True   True   True  \Windows\Sy
stem32\user32.dll
     880 svchost.exe          0x00000000ff5a0000 True   False  True  \Windows\Sy
stem32\svchost.exe
     912 svchost.exe          0x00000000ff5a0000 True   False  True  \Windows\Sy
stem32\svchost.exe
     964 svchost.exe          0x0000000000950000 False  False  False \Windows\Sy
stem32\en-US\FirewallAPI.dll.mui
     964 svchost.exe          0x000007fefc470000 True   True   True
     964 svchost.exe          0x000007fef42e0000 True   True   True  \Windows\Sy
stem32\dssenh.dll
    2424 wmpnetwk.exe         0x0000000001290000 False  False  False \Windows\Sy
stem32\en-US\shell32.dll.mui
    2424 wmpnetwk.exe         0x000007fefdaf0000 True   True   True  \Windows\Sy
stem32\shell32.dll
```

Figure 83. Volatility “ldrmodules” module with sample output.

Appendix H

Wireshark and Dropbox Screenshots



System

☑ Start Dropbox on system startup

Notify me about

☑ Comments, shares, or @mentions

☑ Synced files

Dropbox Badge

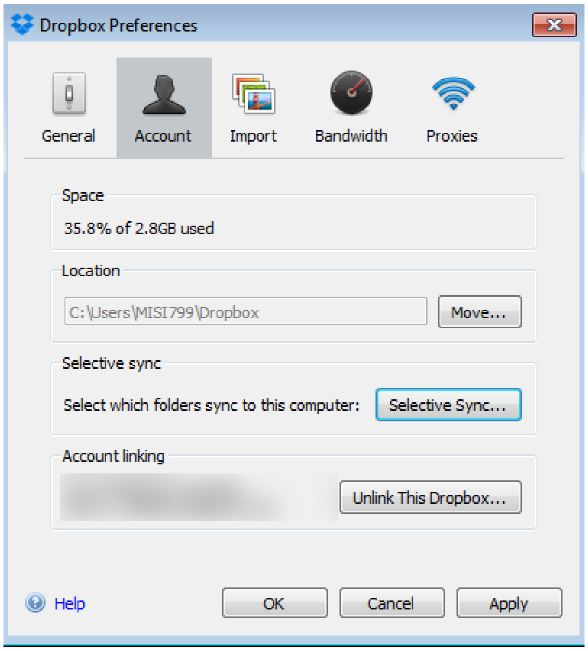
Always show

Language

System Language

Dropbox v21.4.25 uses open source software

Figure 84. General Dropbox Configuration Settings.



Space

35.8% of 2.8GB used

Location

C:\Users\MISI799\Dropbox

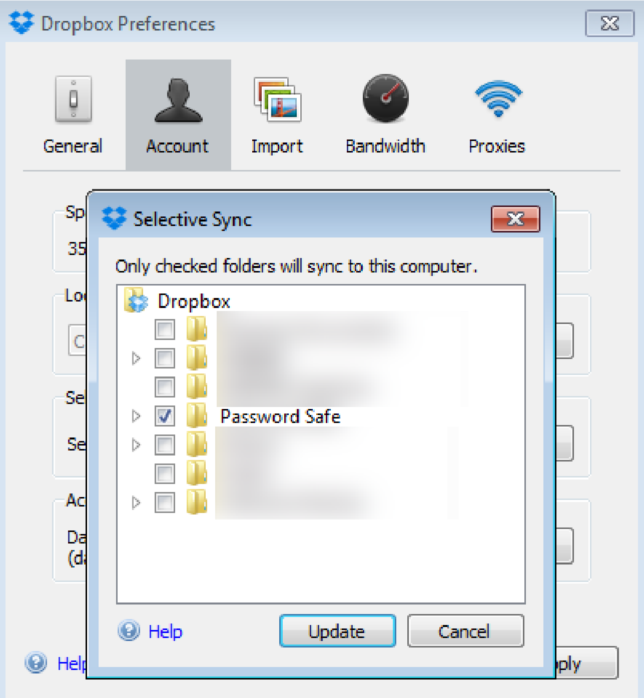
Selective sync

Select which folders sync to this computer:

Account linking

[redacted]

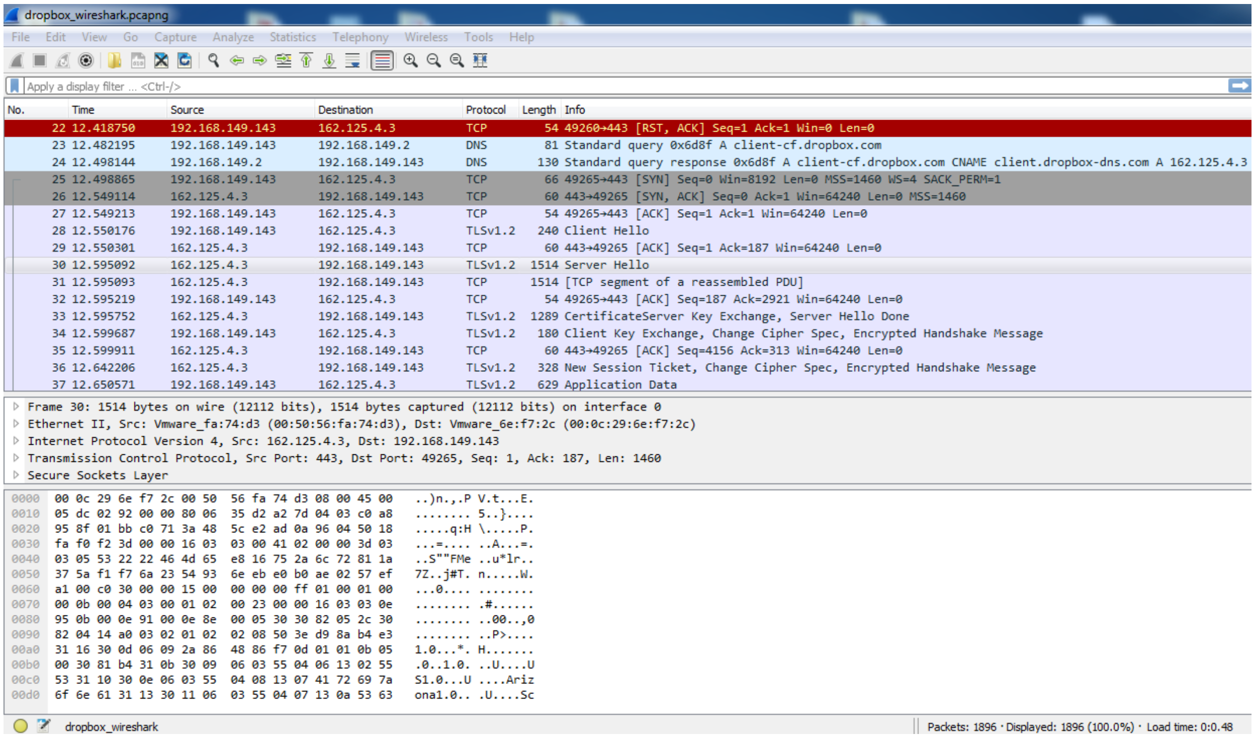
Figure 85. Account Configuration for accessing Selective Sync in Dropbox.



Only checked folders will sync to this computer.

- Dropbox
  - □
  - □
  - □
  - ☑ Password Safe
  - □
  - □
  - □

Figure 86. Configuring Selective Sync in Dropbox to control which password manager is synchronized to the virtual machine.


dropbox_wireshark.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time          Source            Destination       Protocol  Length Info
   22 12.418750     192.168.149.143   162.125.4.3       TCP         54 49260→443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   23 12.482195     192.168.149.143   192.168.149.2     DNS         81 Standard query 0x6d8f A client-cf.dropbox.com
   24 12.498144     192.168.149.2     192.168.149.143   DNS        130 Standard query response 0x6d8f A client-cf.dropbox.com CNAME client.dropbox-dns.com A 162.125.4.3
   25 12.498865     192.168.149.143   162.125.4.3       TCP         66 49265→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
   26 12.549114     162.125.4.3       192.168.149.143   TCP         60 443→49265 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   27 12.549213     192.168.149.143   162.125.4.3       TCP         54 49265→443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   28 12.550176     192.168.149.143   162.125.4.3       TLSv1.2    240 Client Hello
   29 12.550301     162.125.4.3       192.168.149.143   TCP         60 443→49265 [ACK] Seq=1 Ack=187 Win=64240 Len=0
   30 12.595092     162.125.4.3       192.168.149.143   TLSv1.2   1514 Server Hello
   31 12.595093     162.125.4.3       192.168.149.143   TCP       1514 [TCP segment of a reassembled PDU]
   32 12.595219     192.168.149.143   162.125.4.3       TCP         54 49265→443 [ACK] Seq=187 Ack=2921 Win=64240 Len=0
   33 12.595752     162.125.4.3       192.168.149.143   TLSv1.2   1289 CertificateServer Key Exchange, Server Hello Done
   34 12.599687     192.168.149.143   162.125.4.3       TLSv1.2    180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   35 12.599911     162.125.4.3       192.168.149.143   TCP         60 443→49265 [ACK] Seq=4156 Ack=313 Win=64240 Len=0
   36 12.642206     162.125.4.3       192.168.149.143   TLSv1.2    328 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
   37 12.650571     192.168.149.143   162.125.4.3       TLSv1.2    629 Application Data
```

```
▷ Frame 30: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▷ Ethernet II, Src: Vmware_fa:74:d3 (00:50:56:fa:74:d3), Dst: Vmware_6e:f7:2c (00:0c:29:6e:f7:2c)
▷ Internet Protocol Version 4, Src: 162.125.4.3, Dst: 192.168.149.143
▷ Transmission Control Protocol, Src Port: 443, Dst Port: 49265, Seq: 1, Ack: 187, Len: 1460
▷ Secure Sockets Layer
```

```
0000  00 0c 29 6e f7 2c 00 50  56 fa 74 d3 08 00 45 00   ..)n.,.P V.t...E.
0010  05 dc 02 92 00 00 80 06  35 d2 a2 7d 04 03 c0 a8   ........ 5..}....
0020  95 8f 01 bb c0 71 3a 48  5c e2 ad 0a 96 04 50 18   .....q:H \.....P.
0030  fa f0 f2 3d 00 00 16 03  03 00 41 02 00 00 3d 03   ...=.... ..A...=.
0040  03 05 53 22 22 46 4d 65  e8 16 75 2a 6c 72 81 1a   ..S""FMe ..u*lr..
0050  37 5a f1 f7 6a 23 54 93  6e eb e0 b0 ae 02 57 ef   7Z..j#T. n.....W.
0060  a1 00 c0 30 00 00 15 00  00 00 00 ff 01 00 01 00   ...0.... ........
0070  00 0b 00 04 03 00 01 02  00 23 00 00 16 03 03 0e   ........ .#......
0080  95 0b 00 0e 91 00 0e 8e  00 05 30 30 82 05 2c 30   ........ ..00..,0
0090  82 04 14 a0 03 02 01 02  02 08 50 3e d9 8a b4 e3   ........ ..P>....
00a0  31 16 30 0d 06 09 2a 86  48 86 f7 0d 01 01 0b 05   1.0...*. H.......
00b0  00 30 81 b4 31 0b 30 09  06 03 55 04 06 13 02 55   .0..1.0. ..U....U
00c0  53 31 10 30 0e 06 03 55  04 08 13 07 41 72 69 7a   S1.0...U ....Ariz
00d0  6f 6e 61 31 13 30 11 06  03 55 04 07 13 0a 53 63   ona1.0.. .U....Sc
```

dropbox_wireshark | Packets: 1896 · Displayed: 1896 (100.0%) · Load time: 0:0.48

Figure 87. The initial Wireshark capture of Password Safe from Dropbox cloud server.