TRIPLE R

Examination Report

CASE #: 003-2022

Examiner: Zachary Rousseau

# Table of Contents

Contents

[Table of Contents 1](#_Toc122261400)

[Summation 2](#_Toc122261401)

[Background 2](#_Toc122261402)

[Summary of Findings 2](#_Toc122261403)

[Acquisition and Data Analysis Tools 2](#_Toc122261404)

[Acquisition 2](#_Toc122261405)

[Data Analysis Tools Used 3](#_Toc122261406)

[Analysis 3](#_Toc122261407)

[User Accounts 3](#_Toc122261408)

[Emails 3](#_Toc122261409)

[Documents 10](#_Toc122261410)

[Communication Accounts 15](#_Toc122261411)

[Zip Archives 18](#_Toc122261412)

[Internet Artifacts 19](#_Toc122261413)

[Attached Devices 20](#_Toc122261414)

[Kwarren-laptop 20](#_Toc122261415)

[Unallocated Data 20](#_Toc122261416)

[Recommendations 21](#_Toc122261417)

# Summation

## Background

Triple R received a request to conduct a digital forensic investigation. Frodo Baggins formed a computer forensic company known as “Hobbytes” which, as of January 2015, was valued close to $100 million. Samwize Gamgee filed suit against Mr. Baggins for back wages and damages worth over $20 million. Mr. Gamgee claims that he helped start the company before being fired over a drunken disagreement over a ring which Mr. Baggins allegedly stole from Mr. Gamgee. Further, Mr. Gamgee claims Mr. Baggins created a hostile work environment due to violent outburst and sexual harassment towards Mr. Gamgee and potential customers.

## Summary of Findings

The examination determined the drive contained data referencing Mr. Gamgee’s role in Hobbytes. Potentially sexual content was found on the drive as well as discussions of criminal activities. The following data was identified.

* User accounts including accounts for Mr. Baggins and Mr. Gamgee.
* Email exchanges and accounts including exchanges between Mr. Baggins, Mr. Gamgee, and other associates. Exchanges include Mr. Gamgee’s role at Hobbytes.
* Documents related to work conducted at Hobbytes and the relationship between Mr. Baggins and Mr. Gamgee including discussion of “the ring”
* 2 password protected Microsoft Office .xlsx documents containing unknown data.
* Communication accounts and discussions on AIM, ICQ, and Yahoo.
* Zip archives[[1]](#footnote-1) including encrypted[[2]](#footnote-2) archives and discussions between Mr. Baggins and Mr. Gamgee
* 4 USB drives and 1 network drive[[3]](#footnote-3) attached the system
* Discussion of criminal activities conducted by Pippin and Mr. Gamgee

# Acquisition and Data Analysis Tools

## Acquisition

Examiner Rousseau received a disk image, precious.img to perform analysis. The image[[4]](#footnote-4) contained an NTFS[[5]](#footnote-5) file system running on a Windows XP Operating System[[6]](#footnote-6). Utilizing QuickHash v3.3.1, the image file was verified to match the hash values contained in the log.

Acquisition and verification hashes[[7]](#footnote-7):

MD5[[8]](#footnote-8): 8E54FC1A861C072CA5C54BA8FB0CBC77

SHA-1[[9]](#footnote-9): 582C4968ED321A4E22DA7FA1E5723DD0C684AFAB

## Data Analysis Tools Used

For this examination the following tools were used, previously validated by Triple R:

* QuickHash v3.3.1
* Autopsy v4.19.3
* SysTools DBX Converter v5.0
* Registry Explorer v2.0.0.0
* John the Ripper v1.9.0

# Analysis

### User Accounts

Frodo Baggins

The user account Frodo Baggins was located and related to SID[[10]](#footnote-10) 1004. The account was created on December 9 2004 at 3:32 EST and last accessed on January 2 2005 at 10:48 EST.

Sam

The user account Frodo Baggins was located and related to SID1004. The account was created on January 3 2005 at 3:27 EST and last accessed on 3:47 of the same day.

### Emails

##### Outlook.pst

MD5: C45F431F5F6860F690FAA72D1EFF2510

SHA-1: 56AD3D718E9810C2C6A9FDFD33D90F8B52466B51

A Microsoft Outlook data file was found on the system for the email, [frodobaggi@comcast.net](mailto:frodobaggi@comcast.net). The file contained emails, calendar events and reminders for the account.

###### “RE: Training”

This email contains an exchange from between Natasha Daley ([natasha@accessdata.com](mailto:natasha@accessdata.com)), a senior regional sales manager at AccessData, and Frodo Baggins ([Frodobaggi@comcast.net](mailto:Frodobaggi@comcast.net)). The exchange began on Monday December 202004 at 10:00 AM EST and ended at 12:33 PM on the same day. In the email Mr. Baggins states that “Sam and I have started a new company specializing in Computer Forensics” and refers to himself as President of Hobbytes inc.. Mr. Baggins asks Ms. Daley for suggestions for training on Computer Forensics provided by AccessData. Samwize Gamgee’s email, [samwizgamegee@hotmail.com](mailto:samwizgamegee@hotmail.com) is carbon copied on the email. Mr. Baggins also identifies a previous company he attained called “Shire Wire” which he left to his third cousin, Keith Lockhart.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

###### “RE: Thanks for the great info!”

This email contains an exchange between Mark Stringer ([mark@accessdata.com](mailto:mark@accessdata.com)), a senior instructor at AccessData, and Frodo Baggins ([Frodobaggi@comcast.net](mailto:Frodobaggi@comcast.net)). The exchange began on Friday, December 10 2004 at 11:10 EST and ended on December 21 2004 at 1:11 PM EST. In the email Mr. Baggins states “Sam and I are starting a consulting company and specializing in Forensic Computer Analysis” referring to the company as “Hobbytes Consulting.” Mr. Stringer replies to Mr. Baggins and notes a ring that Mr. Baggins was wearing in class stating that it was “very nice.”

Graphical user interface, text, application, email

Description automatically generated

###### “An interesting Eric Clapton article from whereseric.com”

This email contains an exchange between Samwize Gamgee ([samwizgamgee@yahoo.com](mailto:samwizgamgee@yahoo.com)) and Frodo Baggins ([frodobaggi@comcast.net](mailto:frodobaggi@comcast.net)). This exchange occurred on April 29 at 1:00 PM EST. The contents include discussions regarding “Eric Clapton.”

Graphical user interface, text, application, email

Description automatically generated

###### “Add on Monster.com”

This email contains an exchange between what appears to be Keith Lockhart ([keith@accessdata.com](mailto:keith@accessdata.com)), Mr. Baggins self-proclaimed third cousin, and Frodo Baggins ([frodobaggi@comcast.net](mailto:frodobaggi@comcast.net)). The exchange occurred on Wednesday December 12 2004 at 6:15 PM EST. In the exchange Mr. Baggins introduces himself to Mr. Lockhart stating that he lives in The Shire, Utah and has previously sent his resume to Mr. Lockhart after seeing Mr. Lockhart’s “add” on Monster.com. Mr. Baggins inquiries if Mr. Lockhart’s position is still available. Mr. Baggins states that he worked in an AOL called center before they let him go for “accidentally” saying to an Elven girl “I desire you right now,” and “Your wicked” as he was just learning Elven. He also mentions a stalking charge he possesses as a result. The timeline between when he stated that [he stated Mr. Lockhart was his cousin](RE:_Training#_) on December 20 2004 and when he introduces himself to Mr. Lockhart on December 29 2004 highlights inconsistencies. Further investigation will be required to identify Mr. Baggins’ relationship with Mr. Lockhart.

Text, email

Description automatically generated

###### “RE: frodobaggin sent you this eBay item: 2 CREAM REUNION TICKET CHIOR ROW 8 CLOSE TO STAGE 5th (#6528578841)”

The email contains an exchange between Samwise Gamgee ([samwizegammgee@yahoo.com](mailto:samwizegammgee@yahoo.com)) and Frodo Baggins ([frodobaggi@comcast.net](mailto:frodobaggi@comcast.net), [baggifrodo@aol.com](mailto:baggifrodo@aol.com)). The email was sent on December 30 2004 at 4:23 AM EST and contains an email from April 29 2005 at 11:25 EST. The email contains another email from a time after the email was sent. In the email Mr. Baggins states that he bought tickets to a “Cream Reunion” and Mr. Gamgee states that he will be booking a flight to attend the concert.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated with medium confidence

##### Reminders

There are several reminders contained in this file. One reminder is “Apply for Job at AccessData” dated Friday December 31 2004. Another is “Jessica about a date!” likely referring to Jessica Parry of AccessData whom Mr. Baggins conversed with on several occasions. Additionally, there is a reminder “Talk to Pippin about his bad habbits” which reinforces discussions between Mr. Baggins and Mr. Gamgee in [“Re: It’s a Real Thing.”](Re:_Its_a#_)

A picture containing application

Description automatically generated

##### Calendar

There are several events in the calendar including “Meet with Treebrard about Hackers” on Wednesday February 2 2005 at 12:00pm EST in the Fanghorn Forest. It is unclear what the discussion about hackers includes. Further investigation will be required to reveal the details of this event.

Graphical user interface, text, application, chat or text message

Description automatically generated

##### Inbox.dbx

MD5: 2094C9BE87EC3281372609128070CD8A

SHA-1: 7D13A37930FBAB8F594202F287F8E2C2FAA1F491

Inbox.dbx contains emails contained in [Outlook.pst](#_Outlook.pst) subjected [“RE: Training”](RE:_Training#_) and [“RE: Thanks for the great info!”](RE:_Thanks_for#_) along with additional emails.

###### “Re: Its a Real Thing!”

This email contains and exchange between Samwise Gamgee ([samwizgamgee@yahoo.com](mailto:samwizgamgee@yahoo.com)) and Frodo Baggins ([frodobaggi@comcast.net](mailto:frodobaggi@comcast.net)). The exchange occurred on Friday April 29 2005 at 11:39:25 AM EST. In the exchange Mr. Baggins states that “Pippin” keeps taking his lunch money and asserts that he will be hiring an Orc for protection. Mr. Gamgee states that he will talk to Pippin about the lunch money. Mr. Gamgee also states that Pippin took his Mr. Shire trophy and pawned it.

Graphical user interface, application, Word

Description automatically generated

### Documents

###### My Buddies.doc

MD5: D21CCCC6BBB331737CF20ADA64C6C02A

SHA-1: 028650FD8458908884CF6E0166E3160F5DFC9ECE

My Buddies.doc discusses a trip Mr. Baggins took to Las Vegas. In the document Mr. Baggins writes to his mother stating that he bought a time share for $10,000 with a “cheap little gold ring” that he pawned. He attaches photos of individuals who were with him including a photo of Mr. Gamgee and Ms. Daley. This document was in Mr. Baggins’ account on the system.

Graphical user interface

Description automatically generated

###### My Love.doc

MD5: 0B0757E3321501C9D931CAE117F7540F

SHA-1: FF72D4A4917717CE89EBA3DE51E95E6C2B261ACC

My Love.doc was unable to be read and appears to be encoded with an unknown text encoding system. Further analysis will need to take place to gather information from this document. This document was in Mr. Baggins’ account on the system. There is also appears to be a deleted version of this document on the system.

###### Passwords.doc

MD5: 6041F6DD5C477BE50DB7DF0EA1F2F19A

SHA-1: 2B4C2618B81905DDAB10C05C8E6EB5BD9A2ACF22

Passwords.doc was unable to be read and appears to be encoded with an unknown text encoding system. Further analysis will need to take place to gather information from this document. This document was in Mr. Baggins’ account on the system.

###### Great Pickup Lines.doc

MD5: B286F71769BA35CB9F1452543CFCE203

SHA-1: 6B1D98CF2CCC4A7D4E1DF791A78F8319F330FAF0

Great Pickup Lines.doc was unable to be read and appears to be encoded with an unknown text encoding system. Further analysis will need to take place to gather information from this document. This document was in Mr. Baggins’ account on the system.

###### Passwords and Stuff.doc

MD5: 9FD59B4079AEBAD36586EEB52D0AB36D

SHA-1: D17E377969193CE1AC05E2F68C99C81C83619E7A

Passwords and Stuff.doc states that it was originally created to store “passwords and other devious stuff” and contains a logon password, “oneimagetorulethemall.” It states that there are no longer passwords contained in the document. Moreover, it is unclear what “devious stuff” the document was intended to include. This document was in Mr. Baggins’ account on the system. The document was authored by Mr. Baggins however was last saved by “Ken” possibly referencing [Ken Warren.](#_frodobaggi)

Graphical user interface, text, application, email

Description automatically generated

###### DEMO 1.pdf

MD5: BFEAFABA2F6819D79CDB6E8F90E5110A

SHA-1: 37F5DBD59A74F6C70C40E72343D6EE35995C5B22

DEMO 1.pdf contains an AccessData webpage regarding computer forensic training. The document was created on Saturday January 15 2005 at 8:05 PM EST. This document was in Mr. Gamgee’s account on the system.

Graphical user interface, text, application, email

Description automatically generated

###### DEMO 2.pdf

MD5: D530636BD5CF75338EDFD9D86ECE904B

SHA-1: 6AD174D13351ABDC90BE610DD218C7C622DA5F79

DEMO 2.pdf contains an AccessData webpage regarding computer forensic training. The document was created on Saturday January 15 2005 at 8:05 PM EST. This document was in Mr. Gamgee’s account on the system.

Graphical user interface

Description automatically generated

###### ACE PAGE.pdf

MD5: 497A019F0CE4F39C8CD0A0BFFE5BA6CD

SHA-1: 25960D3B05E776AA50EE2FF7DE5D0ED50E0FC7D3

ACE PAGE.pdf contains an AccessData webpage regarding computer forensic certification. The document was created on Saturday January 15 2005 at 8:05 PM EST. This document was in Mr. Gamgee’s account on the system.

Graphical user interface, text, application

Description automatically generated

###### Mortgage accounting inc escrow.xls

MD5: BEC98FD2F5864D9671F06EA2DECEE1A7

SHA-1: 717D03B574ACB92F6D68E1E0D16ECE6C4637BF60

Mortgage accounting inc escrow.xls is password protected and it is unclear the contents of this file. This document was located on Mr. Baggins’ account on the system and was last saved by Ken Warren. Further investigation will need to take place to gather additional information from this file.

###### Retire Scenario Adjustable for Tax Inflation.xls

MD5: AB945EBD976CFBA4DF6C7B8D197DE6CB

SHA-1: 57429125283BE199645CA50A7EF54998B6C2B15B

Retire Scenario Adjustable for Tax Inflation.xls is password protected and it is unclear the contents of this file. This file was located on Mr. Baggins’ account on the system and was last saved by Ken Warren. Further investigation will need to take place to gather additional information from this file.

### Communication Accounts

The following information was extracted from the NTUSER.DAT file located on Frodo Baggins’ user account on the system

###### NTUSER.DAT

MD5: 08B28B7F81D1D69E221B0F4B00E40C87

SHA-1: 455798618C30A306EEF8AB1D4098BDEDF95894BD

#### AOL Instant Messenger

AOL Instant Messenger (AIM) was previously installed however has since been deleted from the system.

##### AIM Users

The following AIM users were found on the system

* frodobaggi (Frodo Baggins)
* samwizgamgee (Samwize Gamgee)
* pimpinpipring (Pippin)

###### frodobaggi

Directory entry for the frodobaggi account states attributes the account to “Frodo Flippin Baggins” residing at 123 Shire Lane Draper, Utah 84020 in Australia.

One away message titled “Wearing the ring” is set to say, “I am off wearing my ring to spy on people I don’t like.”

Recent contacts of this account include

* samwizgamgee (Samwize Gamgee)
* pimpinpipring (Pippin)
* ADDiva92
* accessdatajessica (Jessica Parry)
* padawanken (Ken Warren)

##### accessdatajessica.log

MD5: C91BE1C95D36A51FEAC40DAC650B21E7

SHA-1: 86E51D039E76702C6D67CC40F7C8AC3AA6EA70C2

accessdatajessica.log is a chat log an exchange between Frodo Baggins (frodobaggi) and Jessica Parry (accessdatajessica). Interactions range from Friday December 17 2004 at 4:01 PM EST to 4:52 PM of the same day. The interactions include general technical support provided by Ms. Parry. Further Mr. Baggins asks Ms. Parry on a date and Ms. Parry decline however she states it is a possibility under certain conditions.

Graphical user interface, text, application

Description automatically generated

#### ICQ

Two user accounts were identified

* baggifrodo
* frodobaggi.

###### 12744045.log

MD5: E4368F43C511FF393BC6B43014FEDDEA

SHA-1: 8BD9F69CF812BD9DB15410753F932E3A704A0709

12744045.log is a chat log containing an exchange between Mr. Baggins baggifrodo and Alan (12744045). The exchange occurs from Friday December 17 2004 at 2:46 PM EST and ends at 2:55 PM of the same day. In exchange, Mr. Baggins states he started a computer forensics company in the Shire with “Sammy” called Hobbytes. The exchange also mentions crime committed by Pippin including “car prowls” and breaking into vet offices for “special K” along with doing drugs stating that he is now doing time in jail. Further Alan mentions Ecstasy dealing being done by “Ms. Gamgee.” Alan could be a reference to [Keith Lockhart](#_“RE:_Training”) as his full name may be Keith Alan Lockhart. Mr. Keith Lockhart is known to be a conductor for music associated with Mr. Baggins’ and Mr. Gamgee. Further investigation will be needed to determine the true identity of Alan.

Text

Description automatically generated

#### Yahoo

The following user accounts were identified

* bilbobaggins
* frodobaggi
* samwizgamgee
* treebeard
* wormto

### Zip Archives

###### secret.zip

MD5: 1F25734CF8A55DD1DB80A36AEE24F4F9

SHA-1: 221CBC8ACEB9EE8D1DD96AFB6B4BD3DC83E008DA

Secret.zip is a password protected archive located in Frodo Baggins’ user account. The password “ring” was cracked using John the Ripper and revealed four images. The images appear to hold no significance however, further investigation is needed.

###### tyson&orc.zip

MD5: 0A3AA19D77F97A7C6984D7D1615C6FF7

SHA-1: 20DEE83EC52B662519DB392A8C7A8D764D3B1F9B

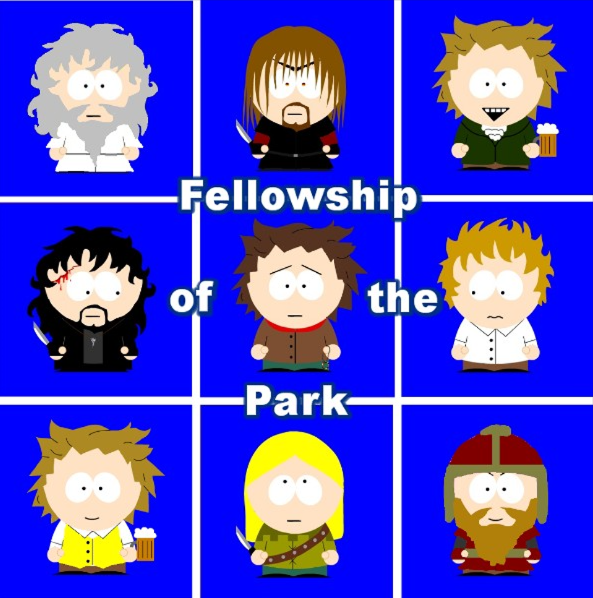
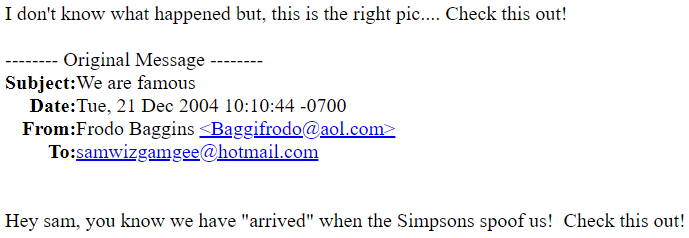
Tyson&orc.zip is a password protected archive located on the system. The password was not obtained, and further investigation will be required to reveal the content of this archive.

###### text2.zip

MD5: 23E8C1B17E90E9AC8DAAB603A2C375F6

SHA-1: 0EF2A1C4E410D123ED823D07DDEA976BAC4241E0

text2.zip contained 2 files discussing a “Simpson” spoof in exchange between Mr. Gamgee ([samwizgamgee@hotmail.com](mailto:samwizgamgee@hotmail.com)) and Mr. Baggins ([baggifrodo@aol.com](mailto:baggifrodo@aol.com)). Mr. Baggins says to Mr. Gamgee that you know “we” have “arrived when they have been spoofed.



### Internet Artifacts

#### Index.dat

MD5: 9F5EAEF82466238020A7A311026B055D

SHA-1: 965D9A3BF82ADBC6B2D0E29B850296AA1676E265

The search term “Singles in the Shire” was found in Frodo Baggins’ search history on the system in the index.dat file on his account. The search term could reveal sexual content.

#### Web Bookmarks

The bookmark “http://www.kazaalitekpp.com” was identified as an Internet Explorer favorite on Mr. Baggins account. Kazaa is a now discontinued peer-to-peer[[11]](#footnote-11) file sharing application which is used to exchange files across the internet. It is unclear what Mr. Baggins was using the site for.

### Attached Devices

#### USB Devices

The following USB drives were connected to the system

* SanDisk Corp. SDCZ2 Cruzer Mini Flash Drive (thin) (ID: SNDK4DD9B41B83E01506)
* SanDisk Corp. SDCZ2 Cruzer Mini Flash Drive (thin) (ID: SNDKAA78A427E5D06506)
* Our Technology Inc. Transcend JetFlash 2.0 / Astone USB Drive / Intellegent Stick 2.0 (ID: 233A1041593FC600)

It is unknown what the contents of these drives contain, and further analysis should be conducted to uncover the data on the drives.

### Kwarren-laptop

A network drive was found connected to the system with the path “\\Kwarren-laptop\Documents\The Precious.” Kwarren could be a reference to a [recent contact](#_frodobaggi) of Mr. Baggins, Ken Warren. It is unclear what Mr. Baggins relationship with Mr. Warren is and further what the contents of the drive contain. Further investigation should be conducted to reveal the content of the remote drive.

### Unallocated Data

A message from Pippin to Mr. Baggins was located on unallocated space[[12]](#footnote-12) on the drive. The message contains several bank account numbers as well as credit card numbers. Pippin states this is information which he stole and suggests getting everyone on board to show them the “love” they deserve.

Text

Description automatically generated

# Recommendations

Triple R recommends the following actions that could help further the investigation:

* Subpoena ICQ, AIM, and Yahoo for further chat logs and additional information.
* Subpoena AOL and comcast for Mr. Baggins’ emails.
* Subpoena Yahoo for Mr. Gamgee’s emails.
* Subpoena Kazaa for any data they may retain regarding Mr. Baggins’ activities on the site.
* Further attempts to gain the passwords for the encrypted .xlsx documents and zip archive.
* Further attempts to decode My Love.doc, Passwords.doc and Great Pickup Lines.doc.
* Locate USB drives and perform digital forensic analysis on the devices.
* Locate KWarren-laptop and perform digital forensic analysis on the device.
* Interview Jessica Parry to further discuss her relationship with Mr. Baggins.
* Interview known associates of Mr. Baggins’ including Ken Warren, Keith Lockhart, Pippin, and AccessData employees.
* Identify Alan (12744045) and his relationship with Mr. Baggins’, Mr. Gamgee and Pippin.
* Identify “Treebrard” and investigate their association with Mr. Baggins’ and hackers.
* Report on Pippin’s criminal activities and Mr. Baggins’ association.
* Investigate claims of Mr. Gamgee’s ecstasy dealing.
* There is attributing evidence that Mr. Gamgee helped start Hobbytes but further investigation is needed.
* There is attributing evidence that Mr. Baggins’ was in possession of a ring which was sold. Further investigation is needed to identify the ring.

1. ZIP is an archive file format that can compress multiple files and directories without loss [↑](#footnote-ref-1)
2. Encryption is the process of encoding data into an unreadable format until unencrypted. [↑](#footnote-ref-2)
3. A network drive is a remote drive located on another computer or server on the same network [↑](#footnote-ref-3)
4. An image is a forensic clone containing a direct bit-for-bit copy of the original system [↑](#footnote-ref-4)
5. NTFS is an acronym that stands for New Technology File System. It was first released by Microsoft in 1993 along with Windows NT 3.1 and has been the primary file system used by Microsoft Since [↑](#footnote-ref-5)
6. An operating system is the core software running on the system which all other applications run on. [↑](#footnote-ref-6)
7. A digital fingerprint generated using a one-way cryptographic algorithm [↑](#footnote-ref-7)
8. MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value [↑](#footnote-ref-8)
9. SHA-1 is an acronym that stands for Secure Hash Algorithm 1. It produces a 160-bit hash value [↑](#footnote-ref-9)
10. A security identifier (SID) is used to unique identify accounts on the Windows 10 Operating System. [↑](#footnote-ref-10)
11. Peer-to-peer file sharing allows for users to use peer-to-peer networking technology to share data where the end-user computers make up the network [↑](#footnote-ref-11)
12. Unallocated space refers to space not attributed to active files on the system [↑](#footnote-ref-12)