Internal Investigation on Tom Warner and Leslie Stowle

December 2, 2022

Prepared by: Aidan Czyryca
Price Software Company
12345 Noplace Ave.
Someplace, CA 90023

Table of Contents

Case Background

This forensic report is the result of an internal investigation of Tom Warner and Leslie Stowle on suspicion of stealing intellectual property and inappropriate workplace behavior. Tom Warner has been with Price Software since its creation and currently holds the position of Sales Manager. Due to recent growth in the company, new Vice-President positions have been created and it is well known that Mr. Warner is seeking one of these positions. Mr. Warner has not been involved in recent meetings to determine who will fill these new positions and has expressed his frustration with the company to his coworkers about not being considered for the promotion. Along with this expressed frustration, other comments from Mr. Warner to his coworkers have raised concerns of company loyalty and integrity of intellectual property from management.

Leslie Stowle is also being investigated alongside Mr. Warner for an inappropriate workplace relationship. Coworkers have also noticed these two frequently meeting up and whispering at their desks, and reported Mr. Warner and Ms. Stowle for a rumored inappropriate workplace relationship.

Price Software management has given forensic images of Mr. Warner's and Ms. Stowle's workstations, the company file server, and a company RAID array from the file server to the on-staff forensic examiner, Aidan Czyryca. The goal of this forensic report is to determine if Price Software needs to be concerned with any wrongdoing from Mr. Warner and Ms. Stowle.

Executive Summary

Purpose of Report

This investigation exposes evidence of violations of workplace integrity and inappropriate workplace behavior for Mr. Tom Warner and Ms. Leslie Stowle at Price Software. After being overlooked for a promotion, Mr. Warner has expressed discontent in the company. Several coworkers raised concerns about Mr. Warner regarding his integrity toward the company, his at-work behavior, and an inappropriate relationship with Ms. Stowle. These concerns led to the present investigation.

Methods Used

Six forensic images were obtained: (1) Mr. Warner's workstation, (2) Ms. Stowle's workstation, (3) the company file server, and (4) three parts of the company RAID5 Array from the file server. In Encase, the RAID5 Array was stitched for three seprate forensic images to create one readable forensic image. The four complete forensic images were scanned for viruses and mounted on the forensic machine. Forensic tools were then used to explore the file systems and to search for evidence of workplace integrity violations and inappropriate workplace behavior.

Major Findings

Violations of Workplace Integrity

In the case of violating workplace integrity, Mr. Warner's workstation provided evidence of having file and hard drive erasing programs (Darik's Boot and Nuke, and Eraser), an email of intent on revenge towards the company, removeable media with CD burner programs, a file encrypting protocol, and easy access to sensitve company documents. The programs found on Mr. Warner's workstation should never be in the hands of someone outside of an IT team or someone who is already experienced in its use. Mr. Warner, who is a sales employee, should not have access to these programs and the fact that he does is an active threat to the company's operations.

Inappropriate Workplace Behavior

As for the inappropriate workplace behavior, both Mr. Warner and Ms. Stowle show inappropriate behavior at work by wasting company time with MSN Gaming Zone, Windows Pinball, and inappropriate internet browsing. Secondly, by Mr. Warner and Ms. Stowle having an inappropriate workplace relationship as seen through multiple email exchanges between the two where they schedule regular lunches and dinners together and have planned a vacation together.

Conclusion

It is reasonable to conclude that Mr. Warner has the intention and means to damage company property. This is established by email communications showing Mr. Warner expressing intent to get revenge on the company for passing him by for a promotion and the multiple inappropriate and potentially dangerous programs installed on his workstation.

Secondly, it is reasonable to conclude that Mr. Warner and Ms. Stowle are in a relationship that may be inappropriate for a workplace environment. This is established by multiple email exchanges between Mr. Warner and Ms. Stowle where they schedule regular lunches and dinners together and have planned a vacation together.

Examiner Credentials

The forensic examiner for this internal investigation is Aidan Czyryca, the on-staff analyst for Price Software. Aidan Czyryca is a recent graduate of Bloomsburg University of Pennsylvania at which he earned a Bachelor of Science in Digital Forensics and Cybersecurity in the Spring of 2022. He was employed as an IT team member at a local highschool before joining Price Software Company as a Junior Analyst as of June 2022. Aidan Czyryca has been handling internal investigation cases of inappropriate workplace relationships and abuse of power for Price Software. The examiner has been trained to be able to collect and handle evidence, conduct forensic examinations, prepare comprehensive reports, and give expert testimony through the company training and his education.

Scope

The internal forensic examiner has been tasked to provide all evidence of innappropriate workplace activites and the innappropriate workplace relationship of Tom Warner and Leslie Stowle. The evidence pieces being considered in this report are forensic images of Tom Warner's workstation, Leslie Stowle's workstation, the company fileserver, and the RAID5 Array on the server.

Tom Warner's Workstation

Forensic image "PSC Tom WS.E01" is of Tom Warner's workstation.

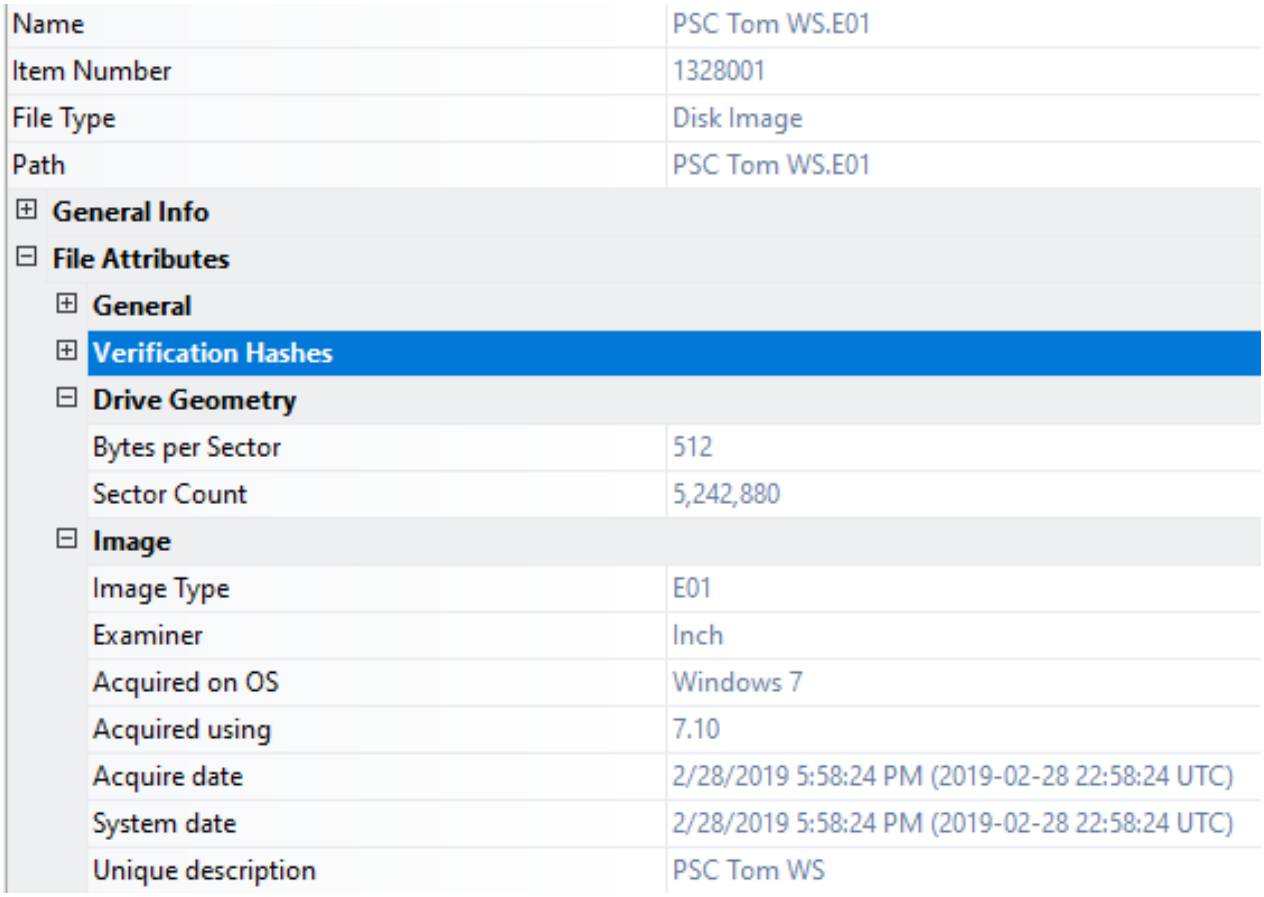


Figure 1: Image of the properties of the forensic image for Mr. Warner's workstation.

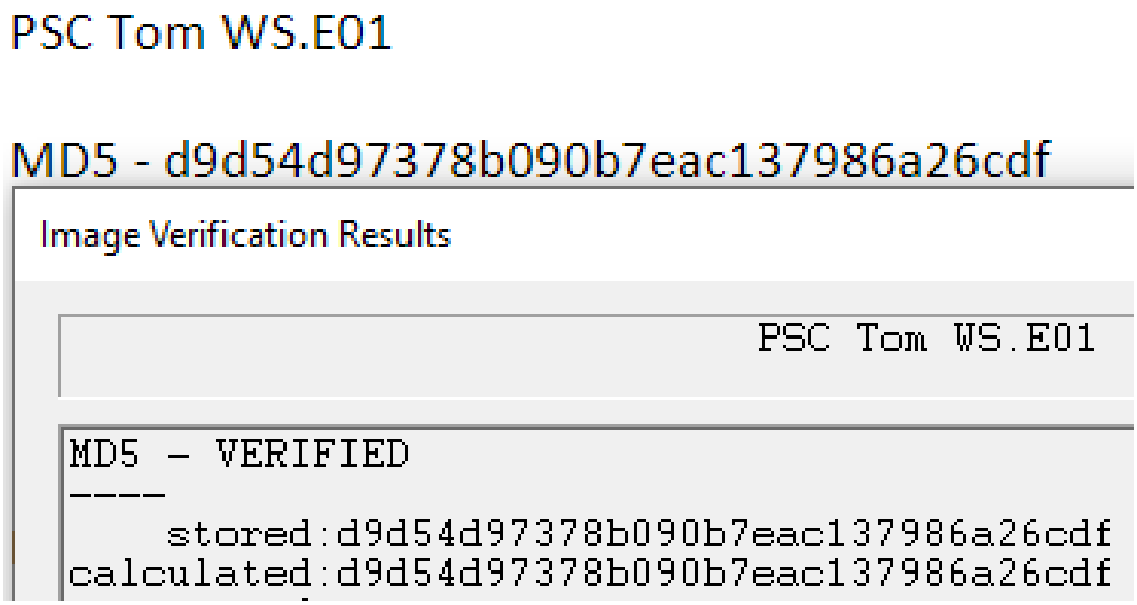
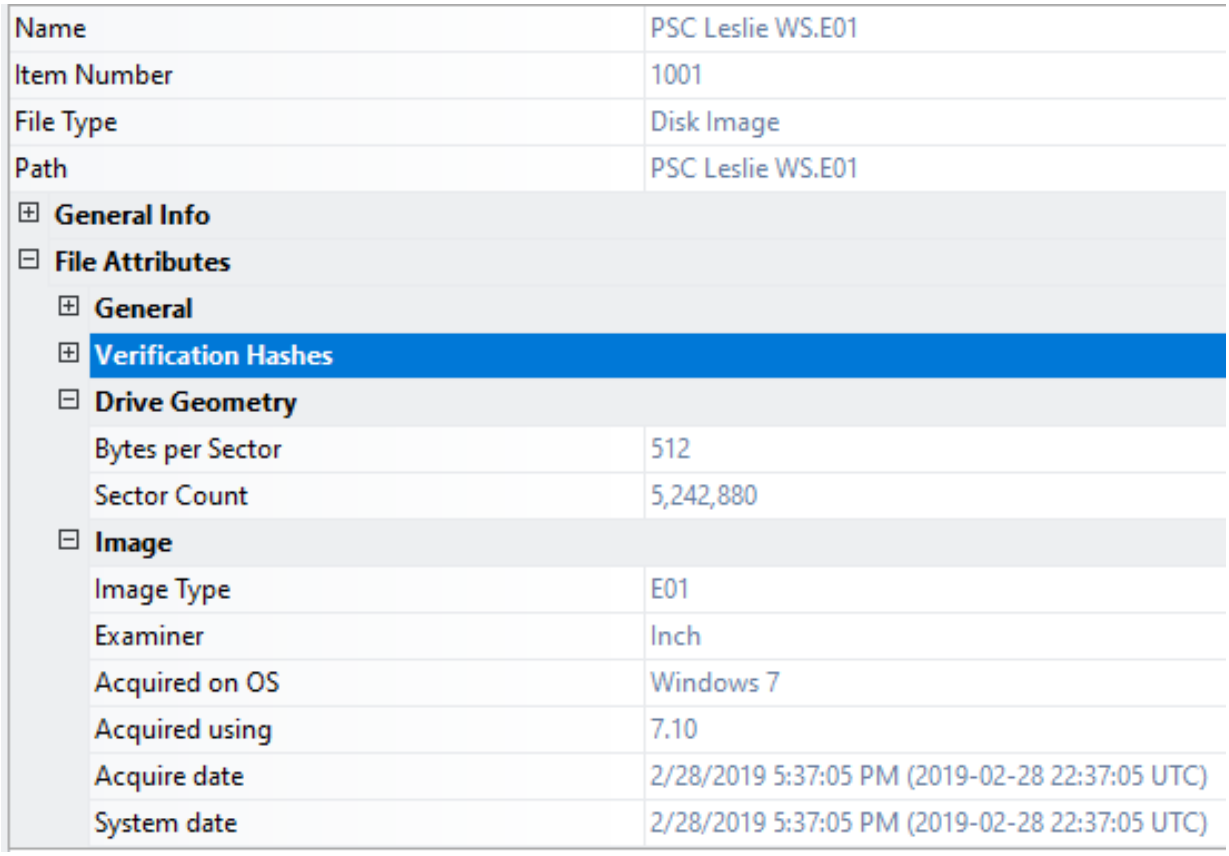


Figure 2: Image verifying that the forensic image received is the same as the image being examined.

Leslie Stowle's Workstation

Forensic image "PSC Leslie WS.E01" is of Leslie Stowle's workstation.



Name	PSC Leslie WS.E01
Item Number	1001
File Type	Disk Image
Path	PSC Leslie WS.E01
⊞ **General Info**	
⊟ **File Attributes**	
⊞ **General**	
⊞ **Verification Hashes**	
⊟ **Drive Geometry**	
Bytes per Sector	512
Sector Count	5,242,880
⊟ **Image**	
Image Type	E01
Examiner	Inch
Acquired on OS	Windows 7
Acquired using	7.10
Acquire date	2/28/2019 5:37:05 PM (2019-02-28 22:37:05 UTC)
System date	2/28/2019 5:37:05 PM (2019-02-28 22:37:05 UTC)

Figure 3: Image of the properties of the forensic image for Ms. Stowle's workstation.

PSC Leslie WS.E01

MD5 - 8f6c72fa2e31efbe2296332044d86105

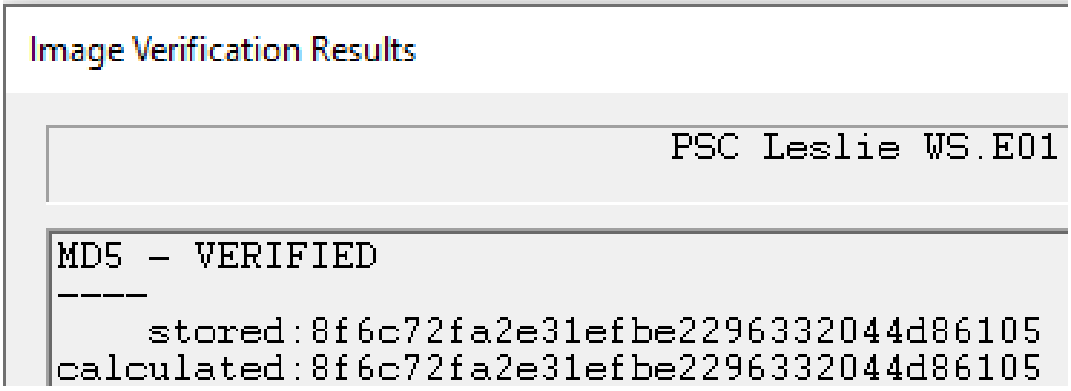
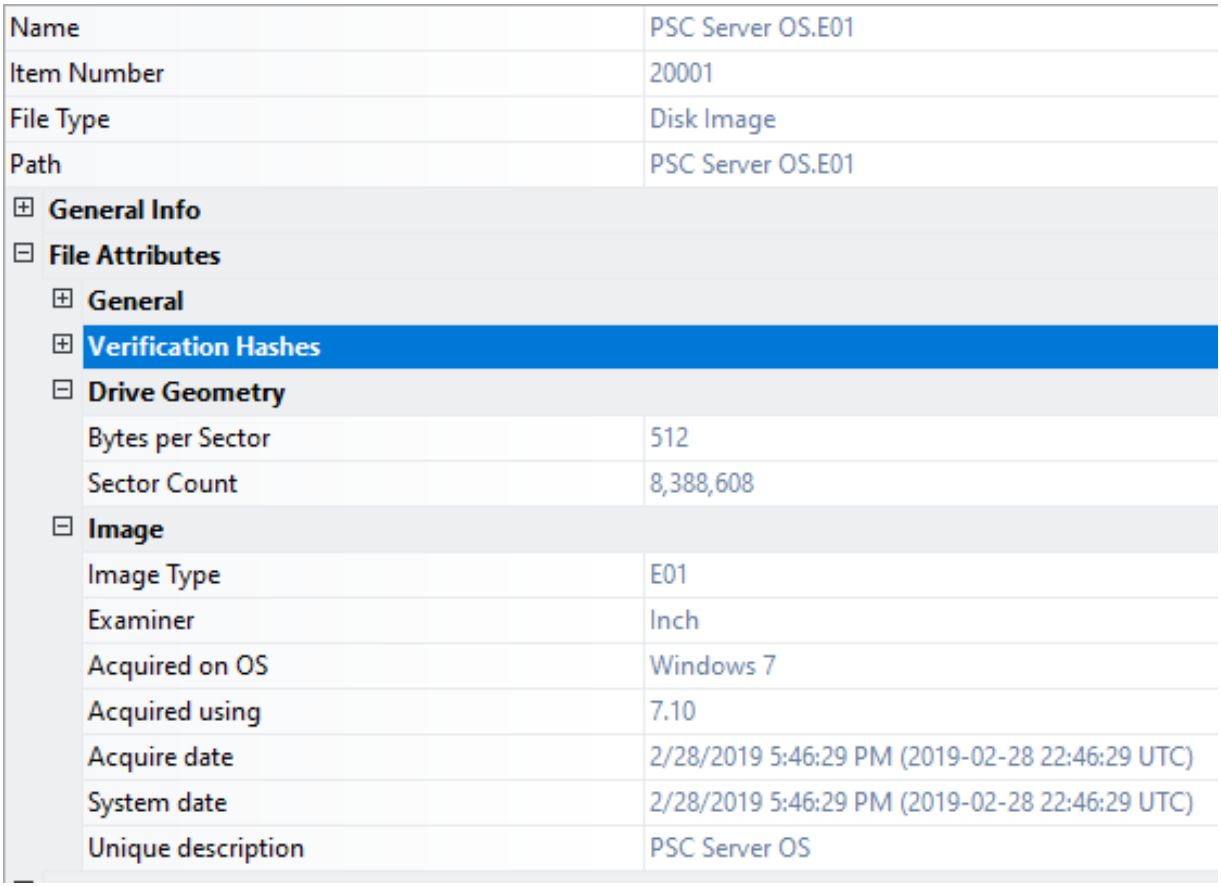


Figure 4: Image verifying that the image received is the same as the image being examined.

Price Software Server

Forensic image “PSC Server OS.E01” is of the Price Software Company server.



Name	PSC Server OS.E01
Item Number	20001
File Type	Disk Image
Path	PSC Server OS.E01
⊞ **General Info**	
⊟ **File Attributes**	
⊞ **General**	
⊞ **Verification Hashes**	
⊟ **Drive Geometry**	
Bytes per Sector	512
Sector Count	8,388,608
⊟ **Image**	
Image Type	E01
Examiner	Inch
Acquired on OS	Windows 7
Acquired using	7.10
Acquire date	2/28/2019 5:46:29 PM (2019-02-28 22:46:29 UTC)
System date	2/28/2019 5:46:29 PM (2019-02-28 22:46:29 UTC)
Unique description	PSC Server OS

Figure 5: Image of the properties of the forensic image for the company server.

PSC Server OS.E01

MD5 - 520f7fc697b730ac11f43aded0380a7a

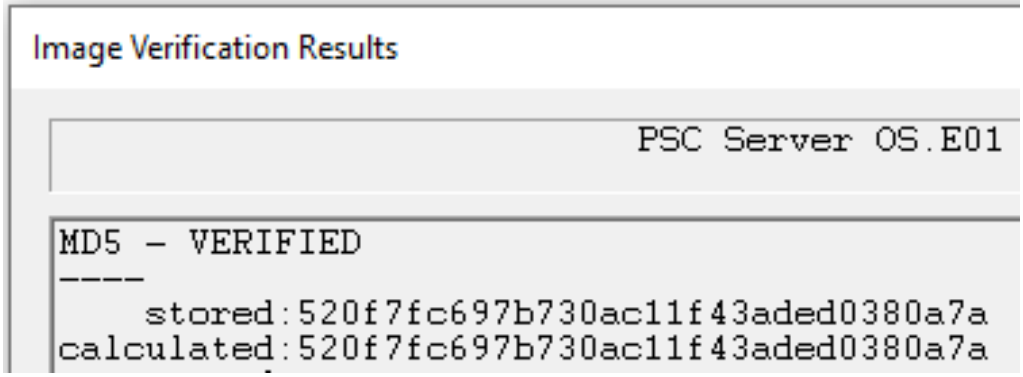
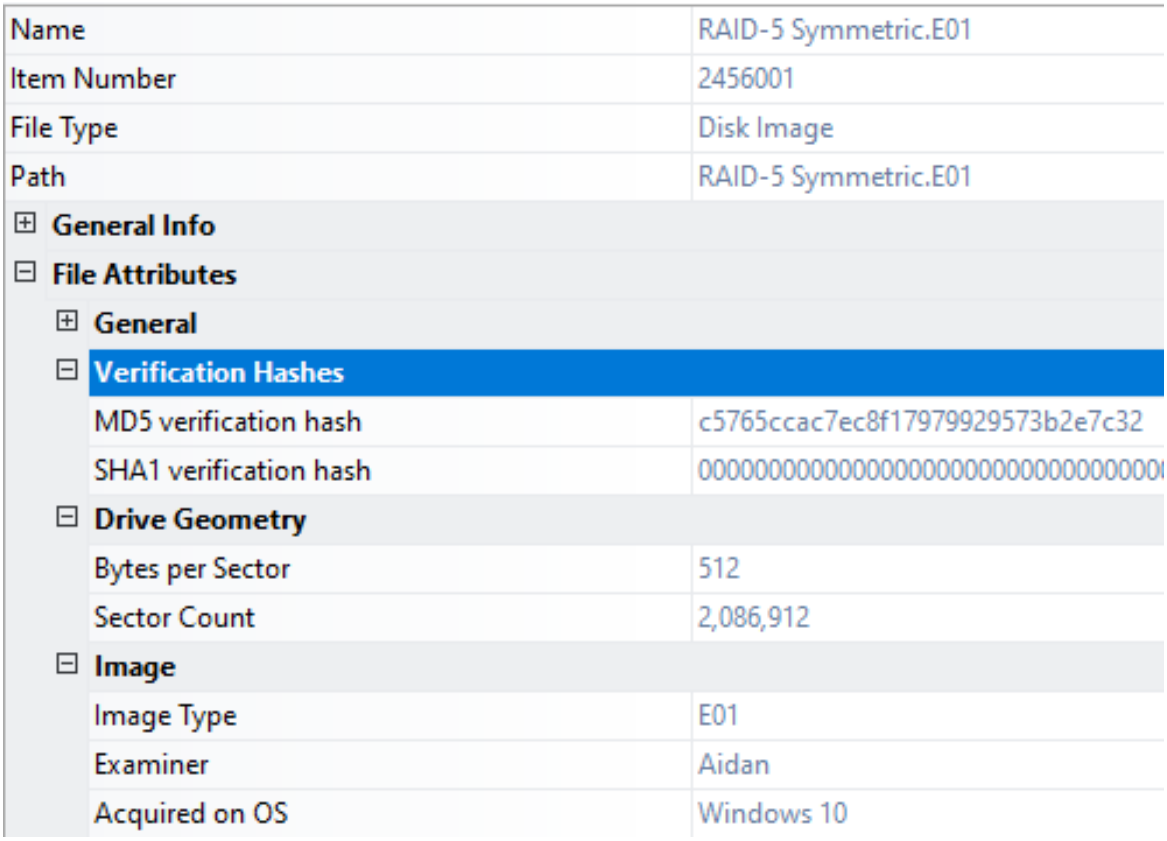


Figure 6: Image verifying that the image received is the same as the image being examined.

RAID5 Array

Forensic image “RAID-5 Symmetric.E01” is of the RAID5 Array.



Name	RAID-5 Symmetric.E01
Item Number	2456001
File Type	Disk Image
Path	RAID-5 Symmetric.E01
General Info	
File Attributes	
General	
Verification Hashes	
MD5 verification hash	c5765ccac7ec8f17979929573b2e7c32
SHA1 verification hash	0000000000000000000000000000000000
Drive Geometry	
Bytes per Sector	512
Sector Count	2,086,912
Image	
Image Type	E01
Examiner	Aidan
Acquired on OS	Windows 10

Figure 7: Image of the properties of the forensic image for the RAID5 Array.

Raid 5-1.E01

MD5 - d3281d25f1e68e8ecb1a3eba58e376ab

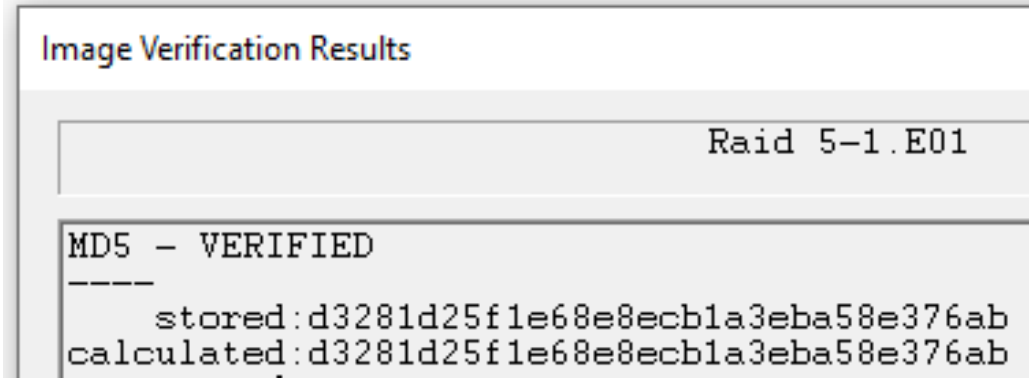


Figure 8: Image verifying that the image received is the same as the image being examined for RAID5 Array Drive #1.

Raid 5-2.E01

MD5 - 2cb2b11ceabe28afadb0f273f80331bb

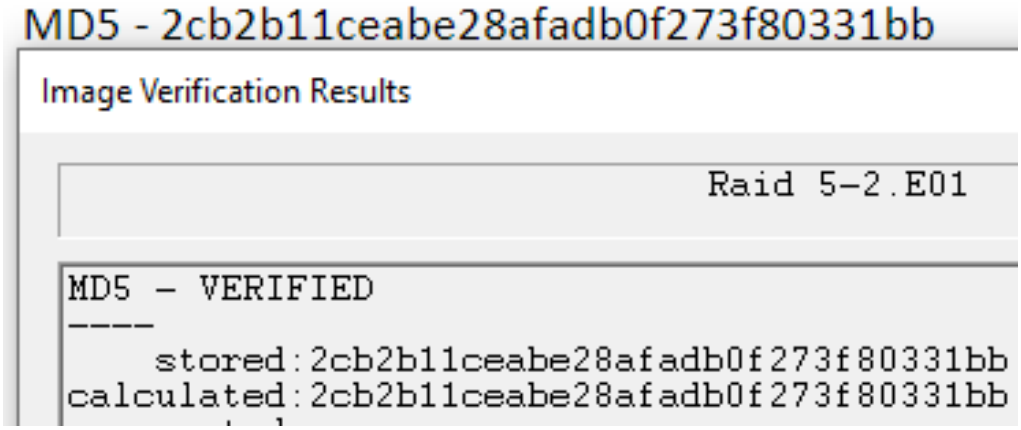


Figure 9: Image verifying that the image received is the same as the image being examined for RAID5 Array Drive #2.

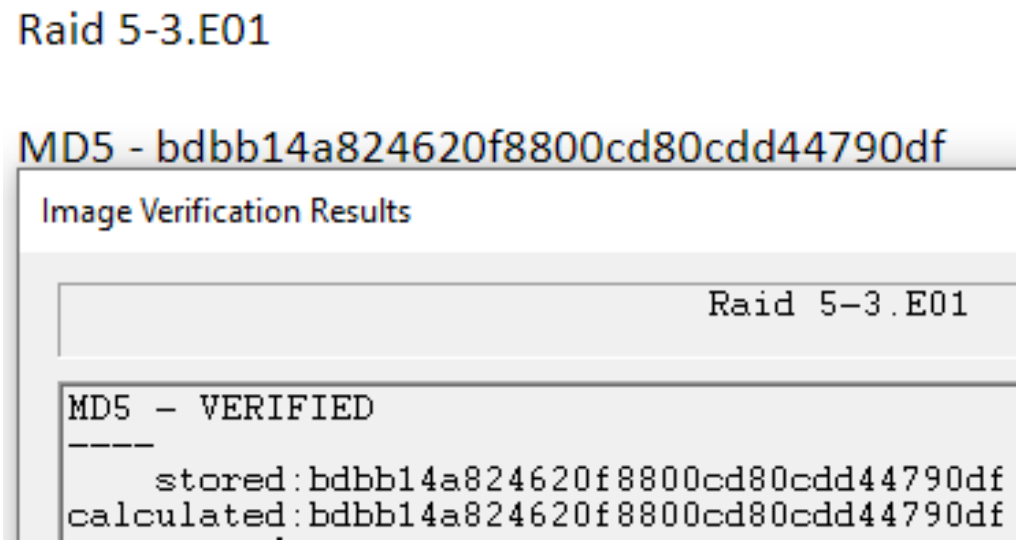


Figure 10: Image verifying that the image received is the same as the image being examined for RAID5 Array Drive #3.

Basic Computer Information

Tom Warner's Workstation

The forensic image of Mr. Warner's workstation contains one partition. The partition solely contains the Windows XP operating system which uses the NTFS file system. There are also 4,816,384 unpartitioned bytes.

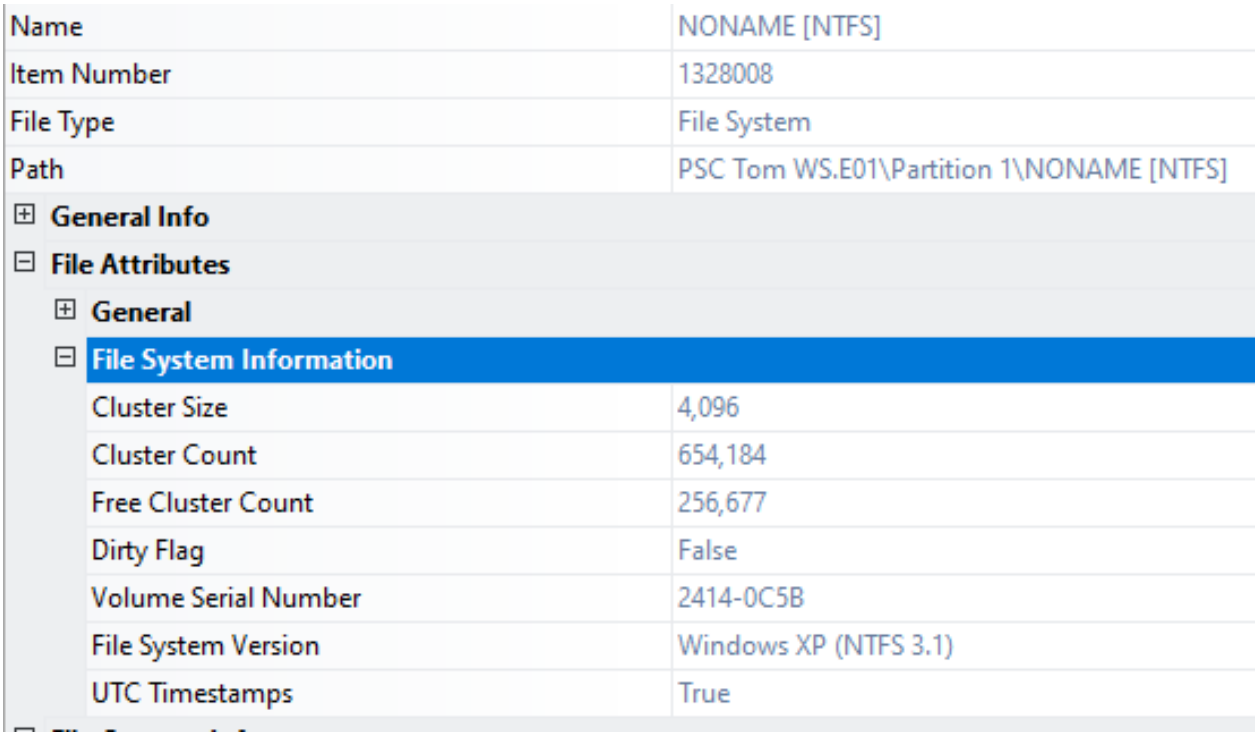


Figure 11: Image contains information about the partition on Mr. Warner's workstation.

Windows XP Partition

The partition is solely occupied by the Windows XP operating system. The file system for the operating system is NTFS. This information is found in the registry file named SOFTWARE found at “PSC Tom WS.E01\Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\config\software”.

Registry SOFTWARE Information	
Install Date	9/27/2004 1:41:59 PM -0400
Product Name	Microsoft Windows XP
Registered Organization	
Registered Owner	GS002
CSDVersion	Service Pack 1
Digital Product ID	A4 00 00 00 03 00 00 00 35 35 00 41 32 32 2D 30 30 30 30 31 00 00 D8 E1 57 41 3F EC 01 00 38 32 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Figure 12: Image contains information about the SOFTWARE registry file.

Within the operating system, the computer is named “PSC-WS-01" and runs on Pacific Standard Time. This information can be found in the SYSTEM registry file found at “PSC Tom WS.E01\Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\config\system”. This information can also be backed up by looking in the Active Control Set, ControlSet001, where the same time zone information is conveyed.

Registry SYSTEM Information	
Active Control Set	ControlSet001
Computer Name	PSC-WS-01
Shutdown Time	1/3/2005 5:03:00 PM -0500
Time Zone BIAS	480
Time Zone Active Time BIAS	480
Standard Bias	0
Daylight Bias	-60
Time Zone Standard Name	Pacific Standard Time
Time Zone Daylight Name	Pacific Standard Time

Figure 13: Image contains information about the SYSTEM registry file.

There are four local user accounts set up on this operating system: Administrator, Guest, Help, Remote Assistant. In the SAM registry file, crucial data on each user is stored. This SAM registry file is found at “PSC Tom WS.E01\Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\config\SAM”. The most important to note are the User Name, Last Logon Time, the Unique Identifier, and whether the account is enabled. Specifically, note the following: the Administrator account has never been logged on to; the Guest account has never been logged on to and is disabled; the Help account has never been logged on to and is disabled; and the Remote Assistant account has never been logged on to and is disabled.

The company workstations also have the ability to log in to users recognized by the server, not just locally created users and default users. This is how we see the user 'twarner’ not in the SAM registry file. If Mr. Warner logs in to the workstation, the server will validate the login and the workstation will create a user with the same permissions and access that user has been granted on the company server.

User Account Information		
Item	**Item Data**	**Item Des**
Last Written time	9/27/2004 5:55:09 AM -0400	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	500 (0x000001F4)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Administrator	This is the name of the user with this RID
Description	Built-in account for administering the computer/domain	The Description of this User
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	9/27/2004 5:55:09 AM -0400	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	False	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	True	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	True	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 14: Administrator account information.

Item	Item Data	Item Des
Last Written time	9/27/2004 5:46:37 AM -0400	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	501 (0x000001F5)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Guest	This is the name of the user with this RID
Description	Built-in account for guest access to the computer/domain	The Description of this User
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	N/A	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	True	This account has been disabled by the administrator
Password Required	False	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	False	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 15: Guest account information.

Item	Item Data	Item Des
Last Written time	9/27/2004 1:36:24 PM -0400	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1002 (0x000003EA)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	SUPPORT_388945a0	This is the name of the user with this RID
Full Name	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US	The full name of the user
Description	This is a vendor's account for the Help and Support Service	The Description of this User
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	9/27/2004 1:36:23 PM -0400	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	True	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	True	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 16: Local Support account information.

Item	Item Data	Item Des
Last Written time	9/27/2004 1:33:10 PM -0400	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1000 (0x000003E8)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	HelpAssistant	This is the name of the user with this RID
Full Name	Remote Desktop Help Assistant Account	The full name of the user
Description	Account for Providing Remote Assistance	The Description of this User
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	9/27/2004 1:33:10 PM -0400	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	True	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Hours Allowed	Anytime	The hours during which this user is allowed to login
Has LAN Manager Password	True	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	True	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 17: Remote Help Assistant account information.

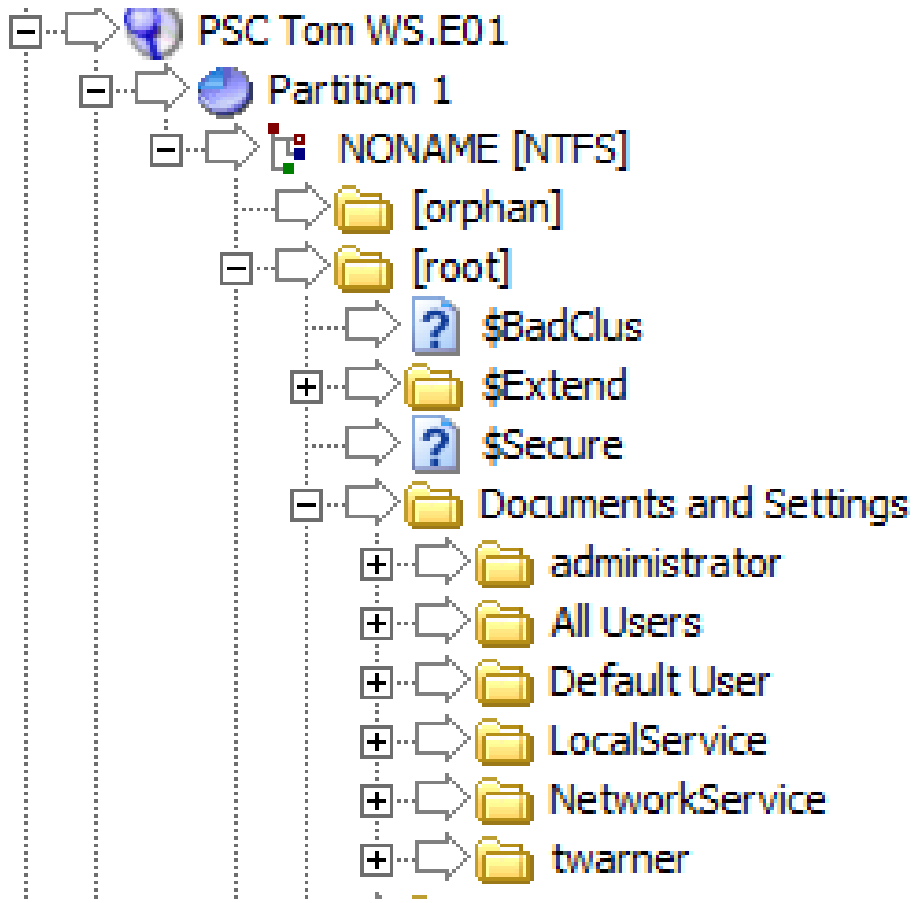
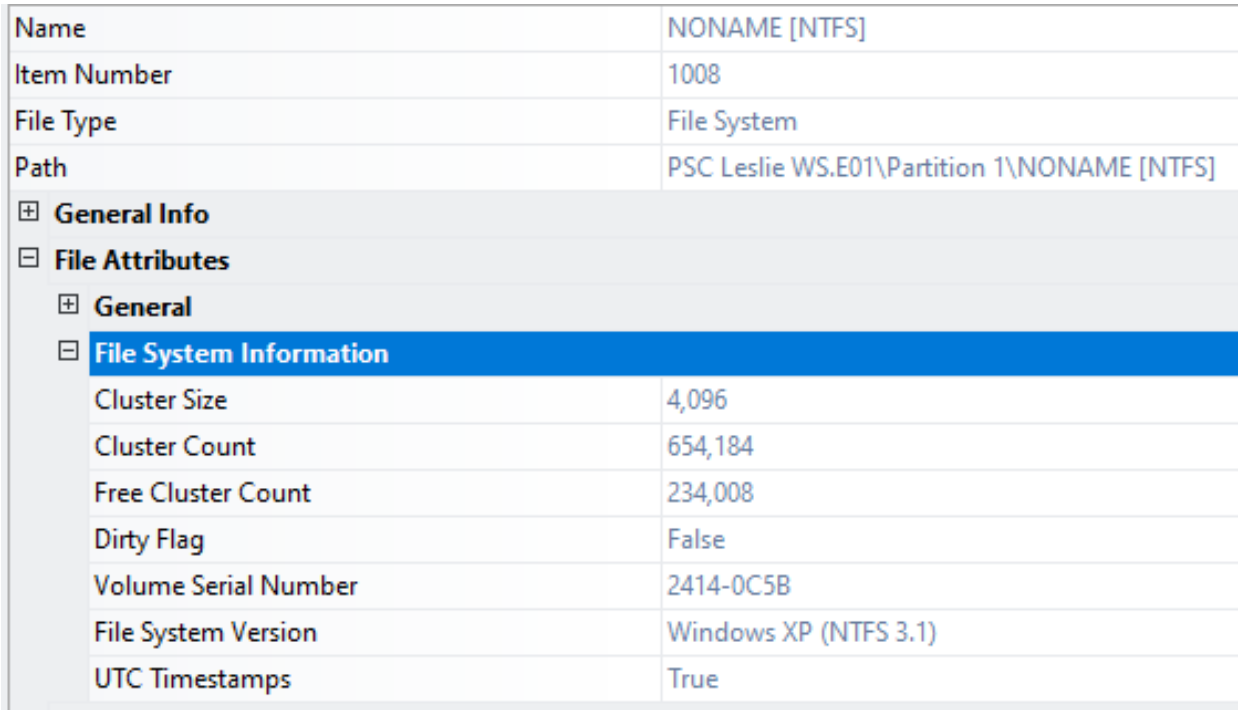


Figure 18: Shows more users than what is identified on SAM.

Leslie Stowle's Workstation

The forensic image of Ms. Stowle's workstation contains one partition. The partition solely contains the Windows XP operating system which uses the NTFS file system. There are also 4,816,384 unpartitioned bytes.



Name	NONAME [NTFS]
Item Number	1008
File Type	File System
Path	PSC Leslie WS.E01\Partition 1\NONAME [NTFS]
⊞ **General Info**	
⊟ **File Attributes**	
⊞ **General**	
⊟ **File System Information**	
Cluster Size	4,096
Cluster Count	654,184
Free Cluster Count	234,008
Dirty Flag	False
Volume Serial Number	2414-0C5B
File System Version	Windows XP (NTFS 3.1)
UTC Timestamps	True

Figure 19: Image contains information about the partition on Ms. Stowle's workstation.

Windows XP Partition

The file system is solely occupied by the Windows XP operating system. The file system for the operating system is NTFS. This information is found in the registry file named SOFTWARE found at “PSC Leslie WS.E01\Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\config\software”.

Registry SOFTWARE Information	
Install Date	9/27/2004 1:41:59 PM -0400
Product Name	Microsoft Windows XP
Registered Organization	
Registered Owner	GS002
CSDVersion	Service Pack 1
Digital Product ID	A4 00 00 00 03 00 00 00 35 3

Figure 20: Image contains information about the SOFTWARE registry.

Within the operating system, the computer is named “PSC-WS-02" and runs on the time zone of Pacific Standard Time. This information can be found in the SYSTEM registry file found at “PSC Leslie WS.E01\Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\config\system”. This information can also be backed up by looking in the Active Control Set, ControlSet001, where the same time zone information is conveyed.

Registry SYSTEM Information	
Active Control Set	ControlSet001
Computer Name	PSC-WS-02
Shutdown Time	1/3/2005 5:08:12 PM -0500
Time Zone BIAS	480
Time Zone Active Time BIAS	480
Standard Bias	0
Daylight Bias	-60
Time Zone Standard Name	Pacific Standard Time
Time Zone Daylight Name	Pacific Standard Time

Figure 21: Image contains information about the SYSTEM registry file.

There are four user accounts set up on this operating system: Administrator, Guest, Local Support, and Remote Assistant. In the SAM registry file, crucial data on each user is stored. This SAM registry file is found at “PSC Leslie WS.E01\Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\config\SAM”. The most important to note are the User Name, Last Logon Time, the Unique Identifier, and whether the account is enabled. Specifically, note the following: the Guest account has never been logged on to and is disabled; the Local Support account has never been logged on to and is disabled; and the Help Assistant account has never been logged on to and is disabled.

The company workstations also have the ability to log in to users recognized by the server, not just locally created users and default users. This is how we see the user ‘lstowle’ not in the SAM registry file. If Ms. Stowle logs in to the workstation, the server will validate the login and the workstation will create a user with the same permissions and access that user has been granted on the company server.

Item	Item Data	Item Des
Last Written time	10/4/2004 1:51:27 PM -0400	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	500 (0x000001F4)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Administrator	This is the name of the user with this RID
Description	Built-in account for administering the computer/domain	The Description of this User
Logon Count	2	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	10/4/2004 1:51:27 PM -0400	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	9/27/2004 5:55:09 AM -0400	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	False	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	True	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	True	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 22: Administrator account information

Item	Item Data	Item Des
Last Written time	9/27/2004 5:46:37 AM -0400	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	501 (0x000001F5)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Guest	This is the name of the user with this RID
Description	Built-in account for guest access to the computer/domain	The Description of this User
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	N/A	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	True	This account has been disabled by the administrator
Password Required	False	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	False	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 23: Guest account information.

Item	Item Data	Item Des
Last Written time	9/27/2004 1:36:24 PM -0400	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1002 (0x000003EA)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	SUPPORT_388945a0	This is the name of the user with this RID
Full Name	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US	The full name of the user
Description	This is a vendor's account for the Help and Support Service	The Description of this User
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	9/27/2004 1:36:23 PM -0400	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	True	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	True	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 24: Local Support account information.

Item	Item Data	Item Des
Last Written time	9/27/2004 1:33:10 PM -0400	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1000 (0x000003E8)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	HelpAssistant	This is the name of the user with this RID
Full Name	Remote Desktop Help Assistant Account	The full name of the user
Description	Account for Providing Remote Assistance	The Description of this User
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	9/27/2004 1:33:10 PM -0400	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	True	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Hours Allowed	Anytime	The hours during which this user is allowed to login
Has LAN Manager Password	True	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	True	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 25: Remote Help Assistant account information.

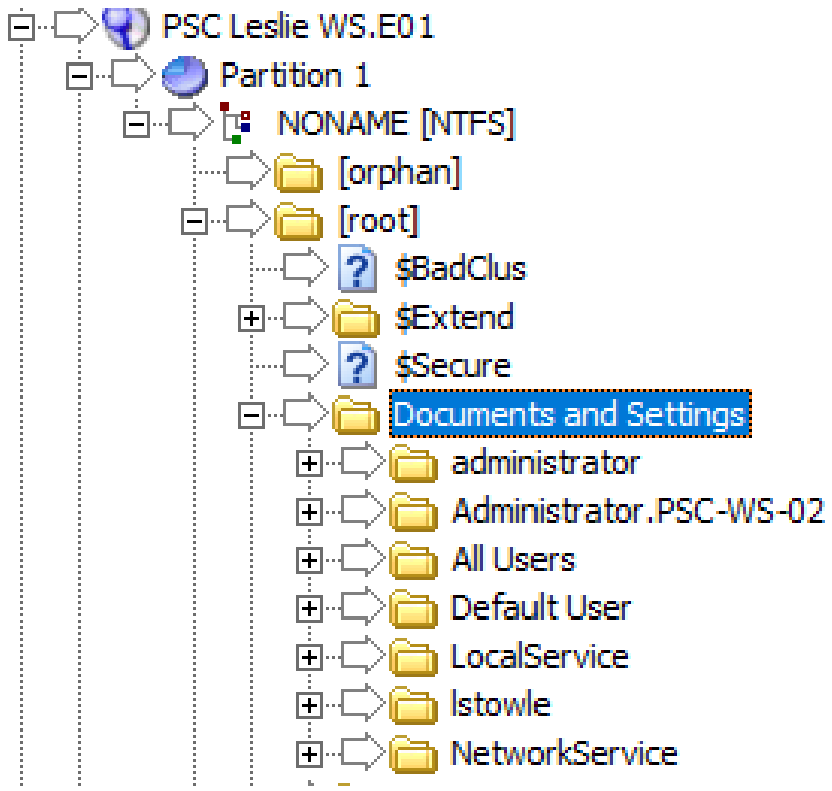
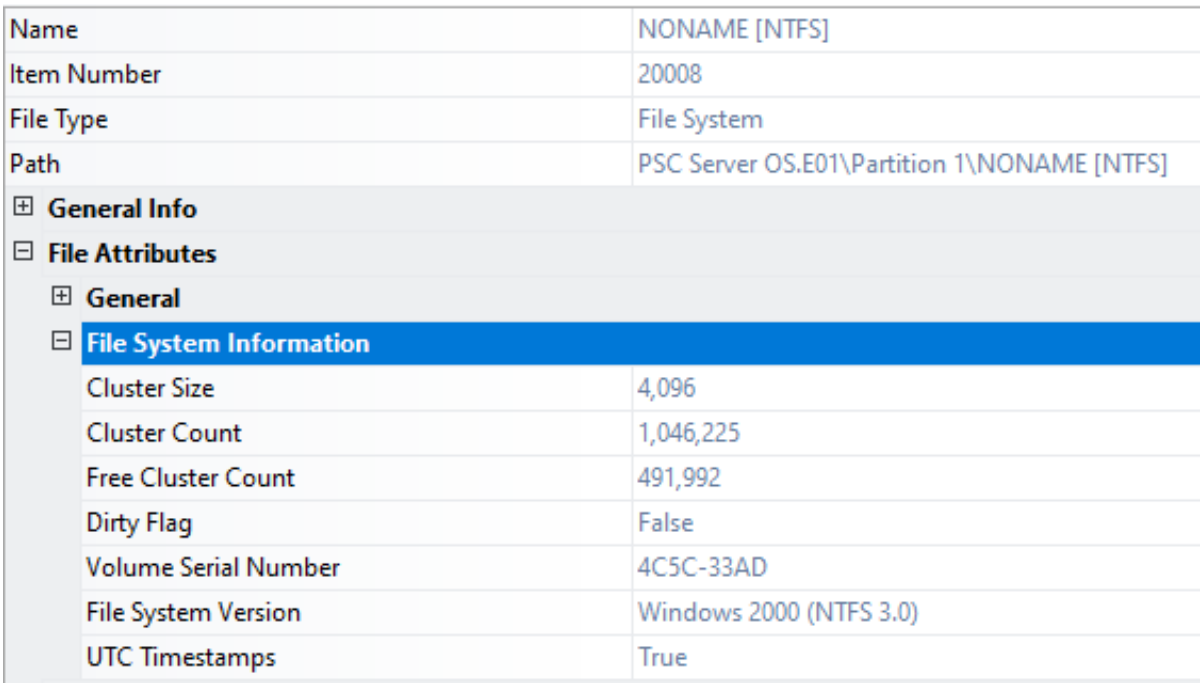


Figure 26: Shows more users than what is identified on SAM.

Price Software Server

The forensic image of the Price Software company server contains one partition. The partition solely contains the Windows 2000 operating system which uses the NTFS file system. There are also 9,628,672 unpartitioned bytes.



Name	NONAME [NTFS]
Item Number	20008
File Type	File System
Path	PSC Server OS.E01\Partition 1\NONAME [NTFS]
⊞ **General Info**	
⊟ **File Attributes**	
⊞ **General**	
⊟ **File System Information**	
Cluster Size	4,096
Cluster Count	1,046,225
Free Cluster Count	491,992
Dirty Flag	False
Volume Serial Number	4C5C-33AD
File System Version	Windows 2000 (NTFS 3.0)
UTC Timestamps	True

Figure 27: Image contains information about the partition on the Price Software coompany server.

Windows 2000 Partition

The partition is solely occupied by the Windows 2000 operating system. The file system for the operating system is NTFS. This information is found in the registry file named SOFTWARE found at “PSC Server OS.E01\Partition 1\NONAME [NTFS]\[root]\WINNT\system32\config\software”.

Registry SOFTWARE Information	
Install Date	1/7/2004 1:39:59 PM -0500
Product Name	Microsoft Windows 2000
Registered Organization	Reg
Registered Owner	Reg
CSDVersion	Service Pack 4
Digital Product ID	A4 00 00 00 03 00 00 00 35 31 38 00 43 31 30 2D 30 30 30 31 30 0(00 00 D4 E1 FB 3F 85 23 0A 00 0(36 32 30 00 00 00 00 00 00 7[00 00 00 00 00 00 00 00 00 0(

Figure 28: Image contains information about the SOFTWARE registry file.

Within the operating system, the computer is named “2KADVSERVER” and runs on the time zone of Pacific Standard Time with daylight savings. This information can be found in the SYSTEM registry file found at “PSC Server OS.E01\Partition 1\NONAME [NTFS]\[root]\WINNT\system32\config\system”. This information can also be backed up by looking in the Active Control Set, ControlSet001, where the same time zone information is conveyed.

Registry SYSTEM Information	
Active Control Set	ControlSet001
Computer Name	2KADVSERVER
Shutdown Time	10/29/2004 2:13:38 PM -0400
Time Zone BIAS	480
Time Zone Active Time BIAS	420
Standard Bias	0
Daylight Bias	-60
Time Zone Standard Name	Pacific Standard Time
Time Zone Daylight Name	Pacific Daylight Time

Figure 29: Image contains information about the SYSTEM registry file.

There are two user accounts set up on this operating system: Administrator, and Guest. In the SAM registry file, crucial data on each user is stored. This SAM registry file is found at “PSC Server OS.E01\Partition 1\NONAME [NTFS]\[root]\WINNT\system32\config\SAM”. The most important to note are the User Name, Last Logon Time, the Unique Identifier, and whether the account is enabled. Specifically, note the following: the Administrator account has never been logged on to; and the Guest account has never been logged on to and is disabled.

Item	Item Data	Item Des
Last Written time	8/27/2004 5:54:04 PM -0400	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	500 (0x000001F4)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Administrator	This is the name of the user with this RID
Description	Built-in account for administering the computer/domain	The Description of this User
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	N/A	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	False	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	True	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	True	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 30: Administrator account information.

Item	Item Data	Item Des
Last Written time	8/27/2004 5:54:04 PM -0400	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	501 (0x000001F5)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Guest	This is the name of the user with this RID
Description	Built-in account for guest access to the computer/domain	The Description of this User
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	N/A	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	True	This account has been disabled by the administrator
Password Required	False	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	False	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 31: Guest account information.

RAID5 Array

The forensic image of the RAID5 Array contains one file system. A RAID5 Array is a protocol for securely storing data by using techniques called striping and parity. Striping is splitting one file across multiple storage devices. Parity is a piece of information attached to each file that tells a system how to rebuild that file. In this case, a file placed into the RAID5 Array will have its parity calculated then the file and parity will be striped across the three storage devices. The protocol makes the hard drives participating in the RAID5 Array appear as one virtual drive to the machine that is attached to it. The virtual hard drive is attached to the Windows 2000 operating system.

This RAID5 Array is a storage device attached to the Windows 2000 server. It contains all the shared folders such as “Finance”, “Management”, and “Software” as well as the company-wide recognized users and their personal files. When one of these users logs in to a workstation, the created user will also acquire these personal files and have access to anything the server has been told the user should have access to.

Name	Users [NTFS]
Item Number	2456002
File Type	File System
Path	RAID-5 Symmetric.E01\Users [NTFS]
⊞ **General Info**	
⊟ **File Attributes**	
⊞ **General**	
⊟ **File System Information**	
Cluster Size	1,024
Cluster Count	1,043,455
Free Cluster Count	998,661
Dirty Flag	False
Volume Label	Users
Volume Serial Number	F4E8-EC10
File System Version	Windows 2000 (NTFS 3.0)
UTC Timestamps	True

Figure 32: Image contains information about the file system on the RAID5 Array.

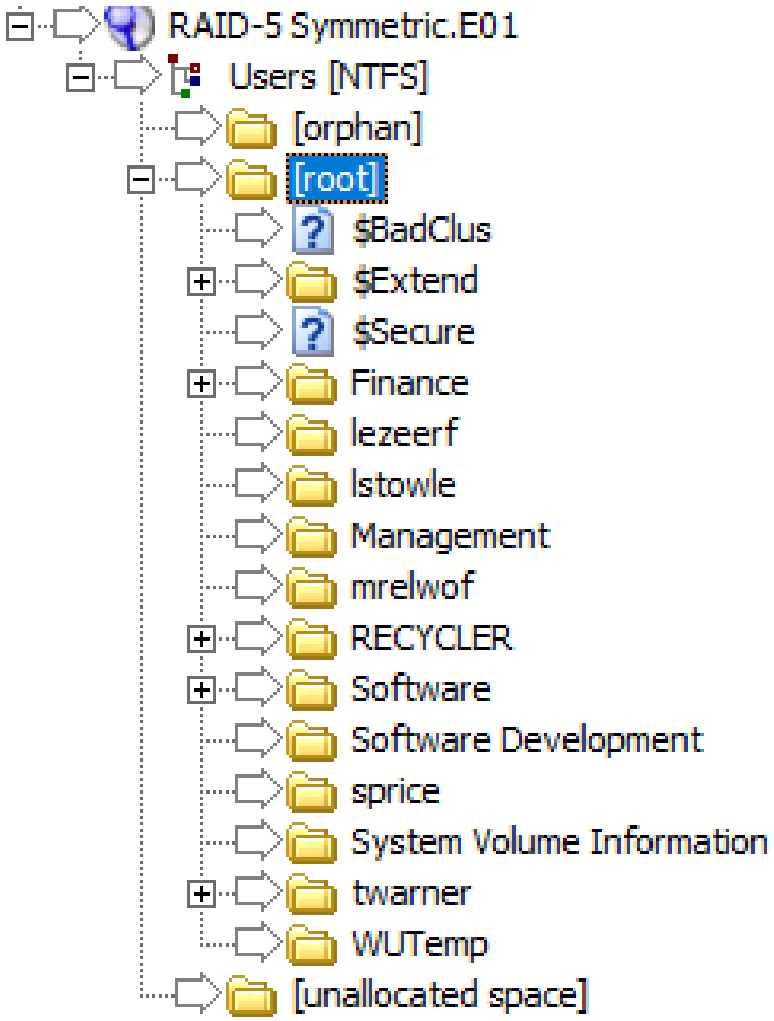


Figure 33: RAID5 Array showing shared folders and company-wide recognized users.

Procedure

Antivirus Scan

Before examining the evidence, every forensic image was scanned for viruses. The antivirus program used during this examination is called ClamWin. Each forensic image is mounted to the forensic workstation and scanned for viruses. This process does not damage the integrity of the original forensic image as the information mounted is a copy of the image and is also not allowed to be written to. Before each image was scanned, the program's virus database was updated to the current version.

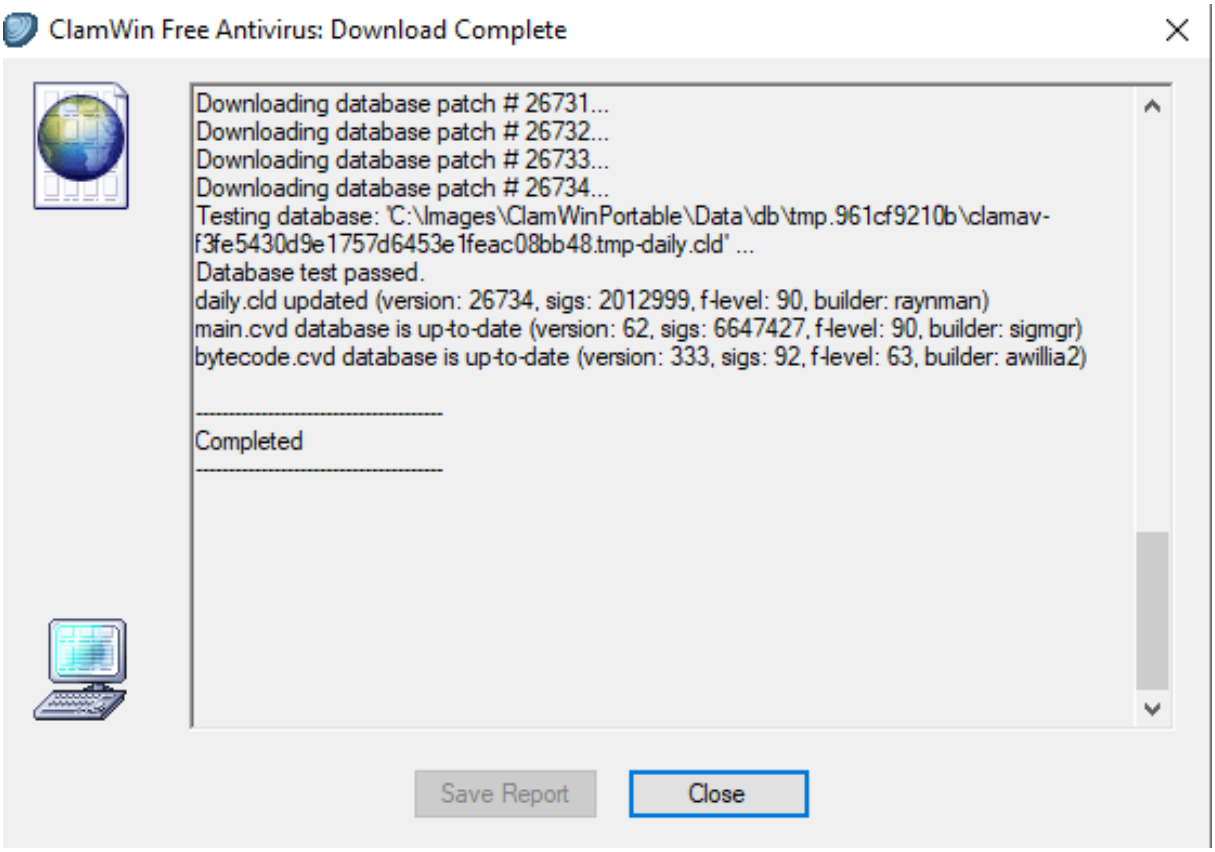


Figure 34: ClamWin Virus Scanner is up-to-date.

The image “PSC Tom WS.E01” was mounted to the forensic machine, in a read only method, physically as a simulated hard drive and logically as a distinct read only file system. One dangerous file with copies in multiple locations was detected in the Hard Drive and was recognized as “market.mar”. This file is an HTML file of the stock markets for the MSN website. The file should not have an adverse effect on the examination computer or the analysis of the evidence as it was recognized as spyware. Spyware typically does not change the information on a machine but rather collects it and sends it elsewhere. Secondly, the file was recognized on no other service to be spyware and is likely a part of the MSN website downloaded to the local machine for easier access.

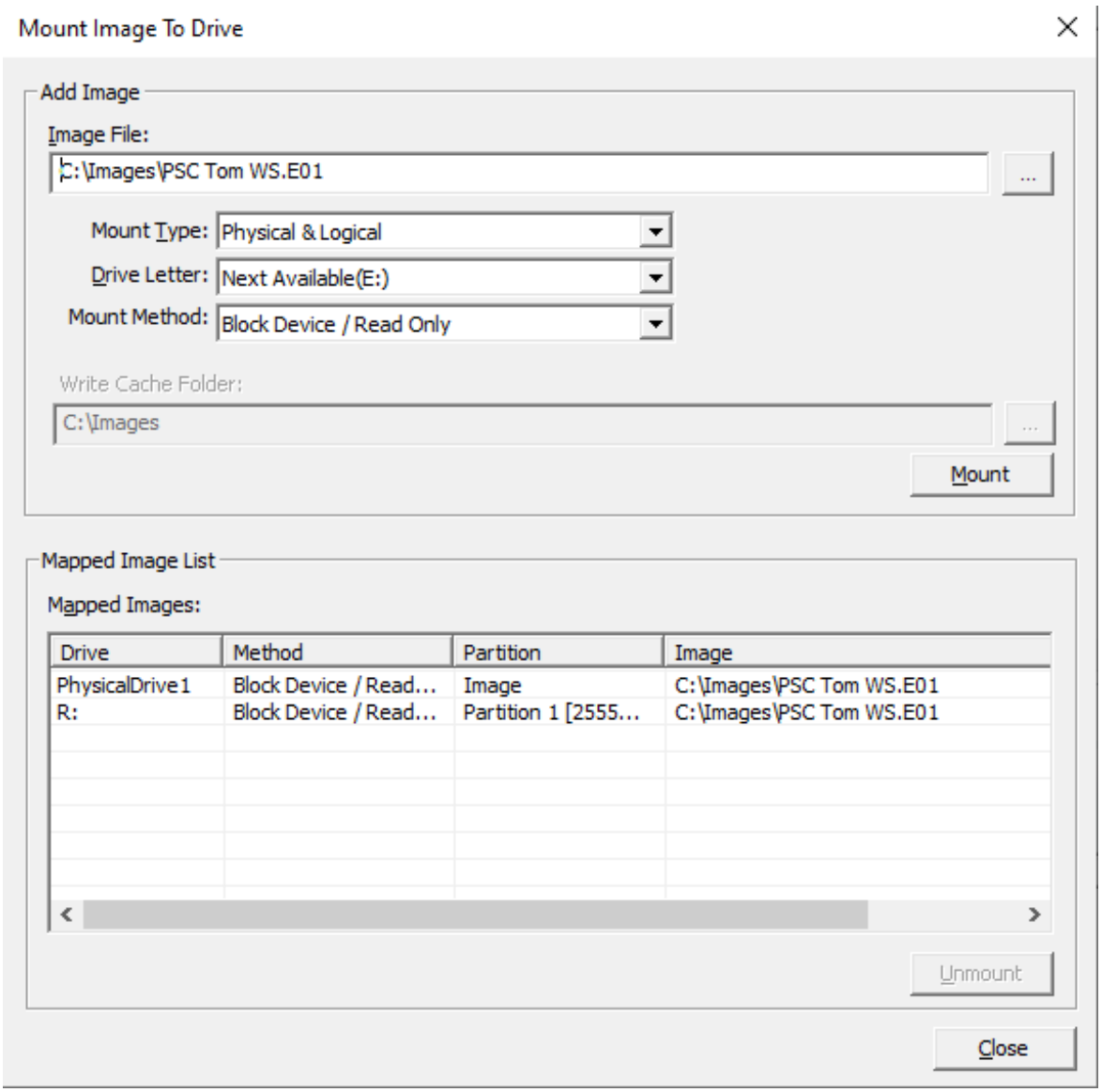


Figure 35: Mounting of "PSC Tom WS.E01".

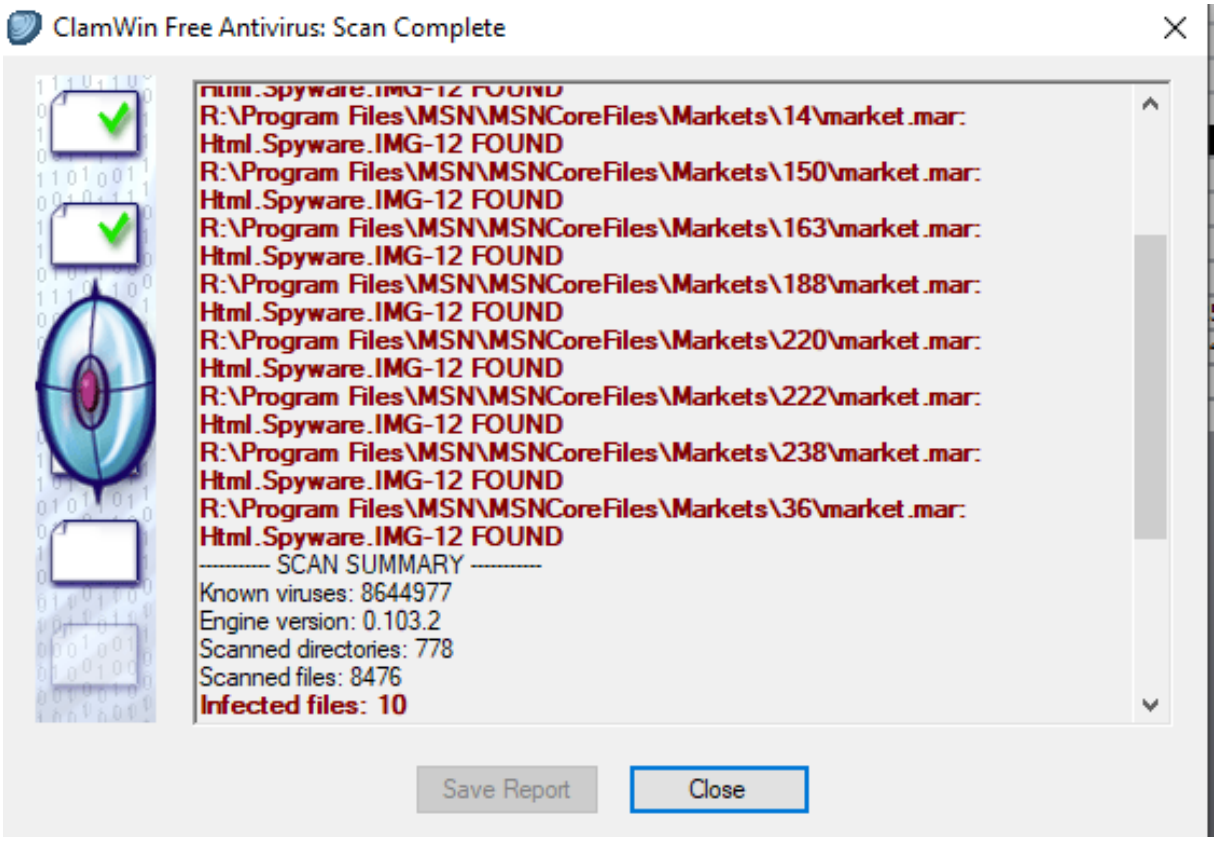


Figure 36: Virus Scan of "PSC Tom WS.E01".

The image “PSC Leslie WS.E01” was mounted to the forensic machine, in a read only method, physically as a simulated hard drive and logically as a distinct read only file system. One dangerous file with copies in multiple locations was detected in the Hard Drive and was recognized as “market.mar”. This file is an HTML file of the stock markets for the MSN website. The file should not have an adverse effect on the examination computer or the analysis of the evidence as it was recognized as spyware. Spyware typically does not change the information on a machine but rather collects it and sends it elsewhere. Secondly, the file was recognized on no other service to be spyware and is likely a part of the MSN website downloaded to the local machine for easier access. This was the same file detected on “PSC

Tom WS.E01".

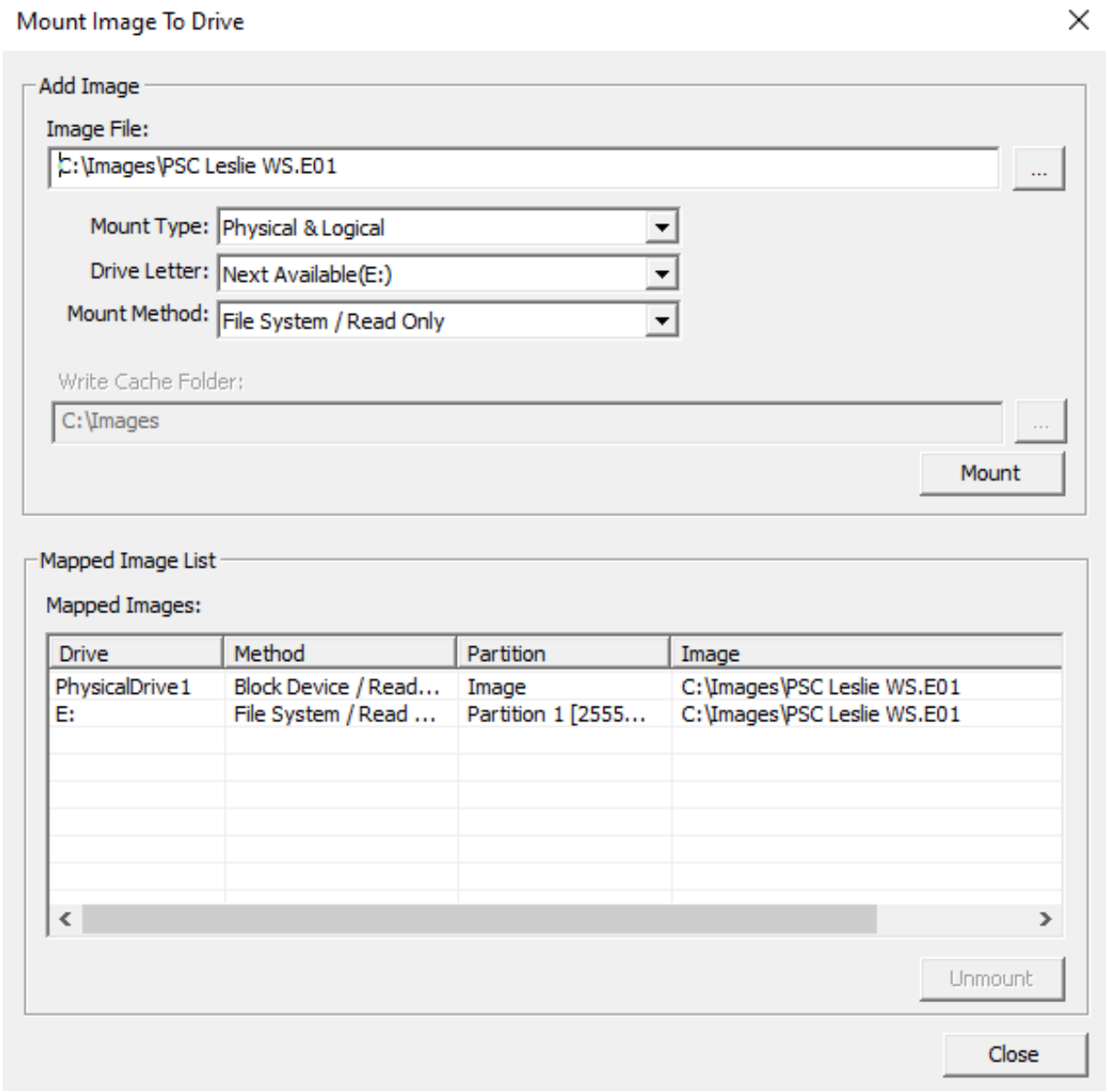


Figure 37: Mounting of "PSC Leslie WS.E01".

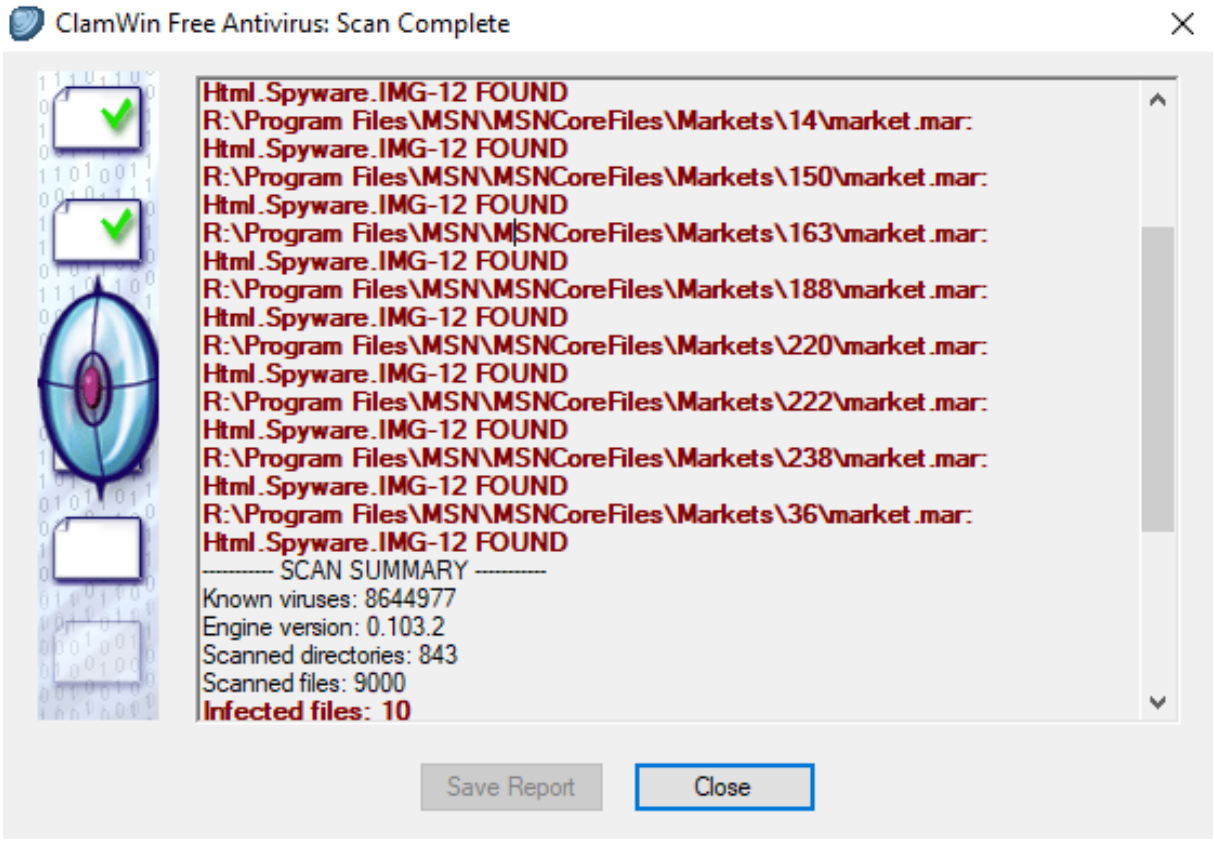


Figure 38: Virus Scan of "PSC Leslie WS.E01".

The image “PSC Server OS.E01” was mounted to the forensic machine, in a ready only method, physically as a simulated hard drive and logically as a file system. The virus scan detected no dangerous files on the hard drive.

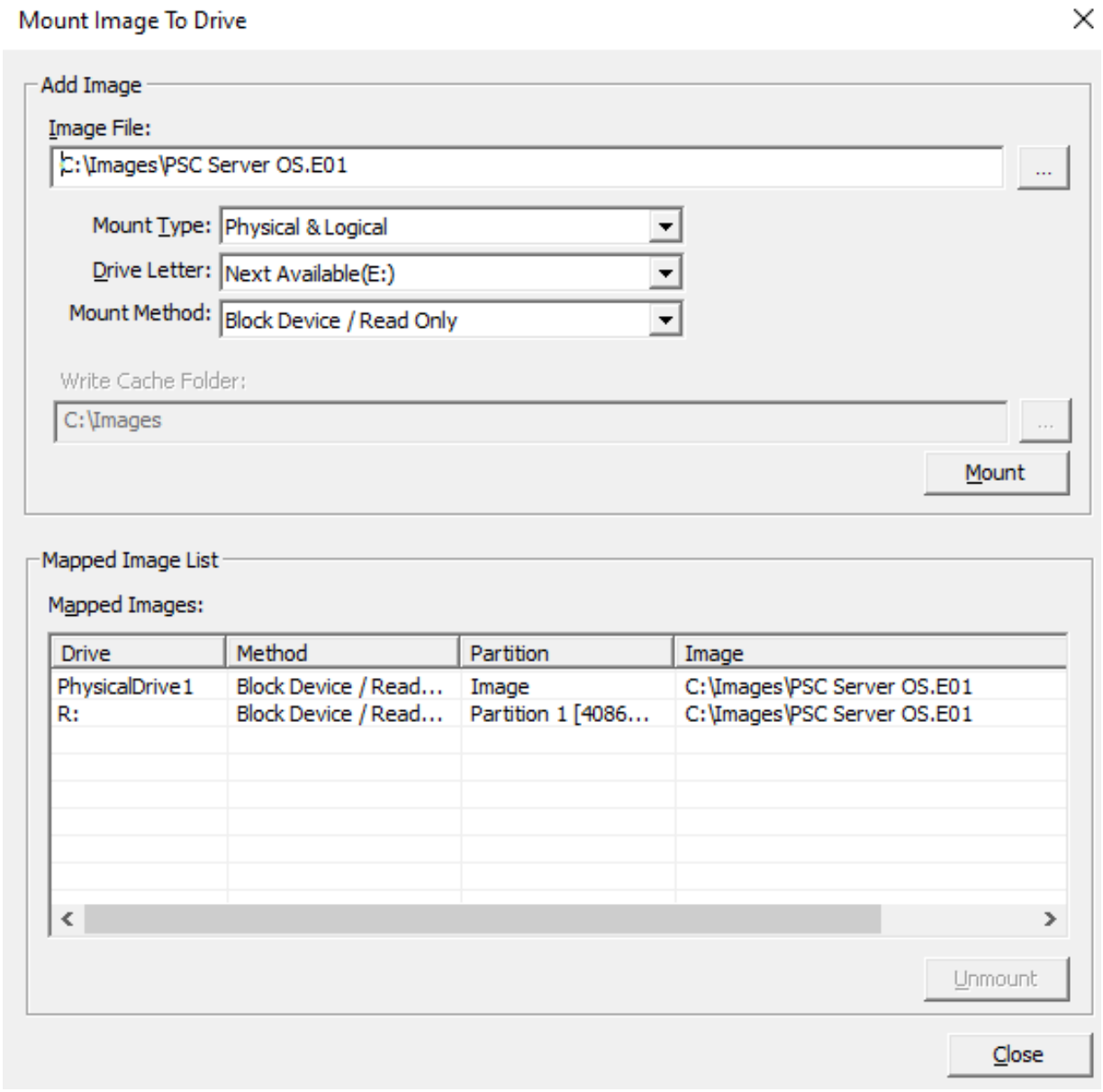


Figure 39: Mounting of “PSC Server OS.E01”.

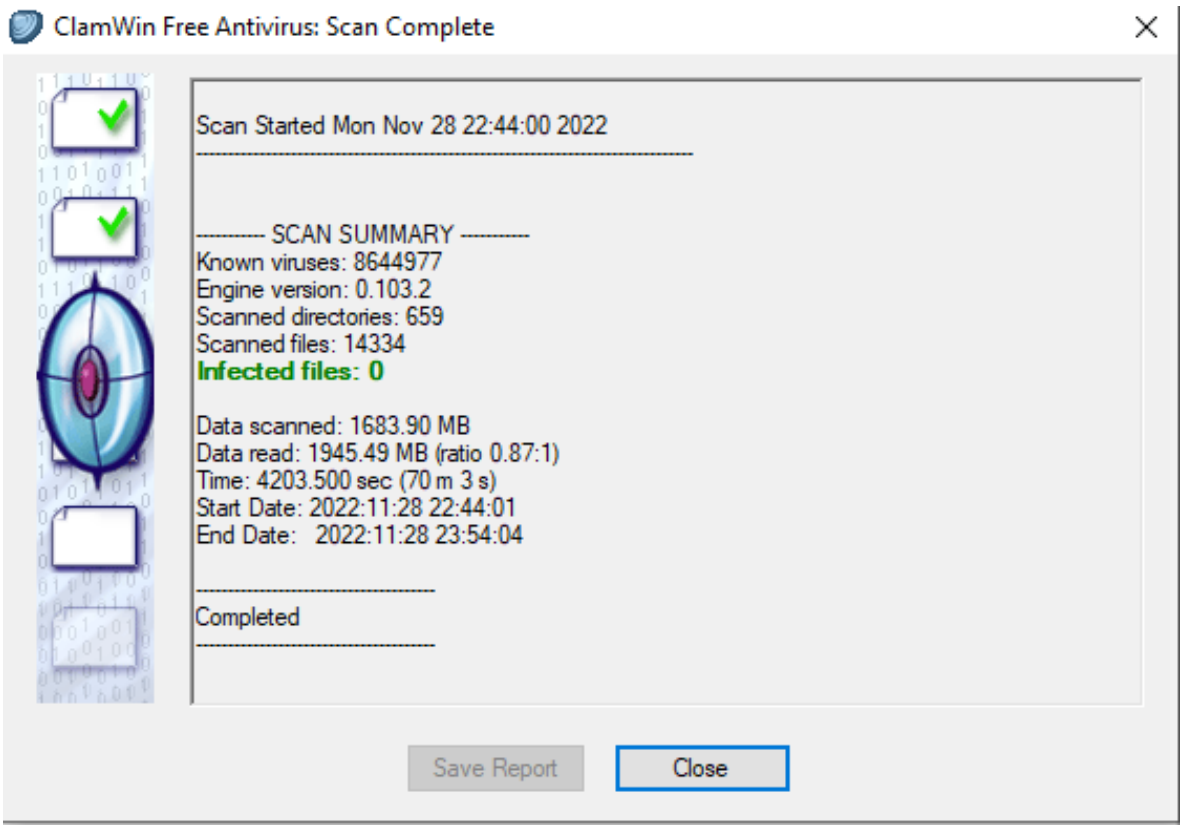


Figure 40: Virus Scan of "PSC Server OS.E01".

The image “Raid-5 Symmetric.E01” was mounted to the forensic machine, in a ready only method and logically as a file system. The virus scan detected no dangerous files on the file system.

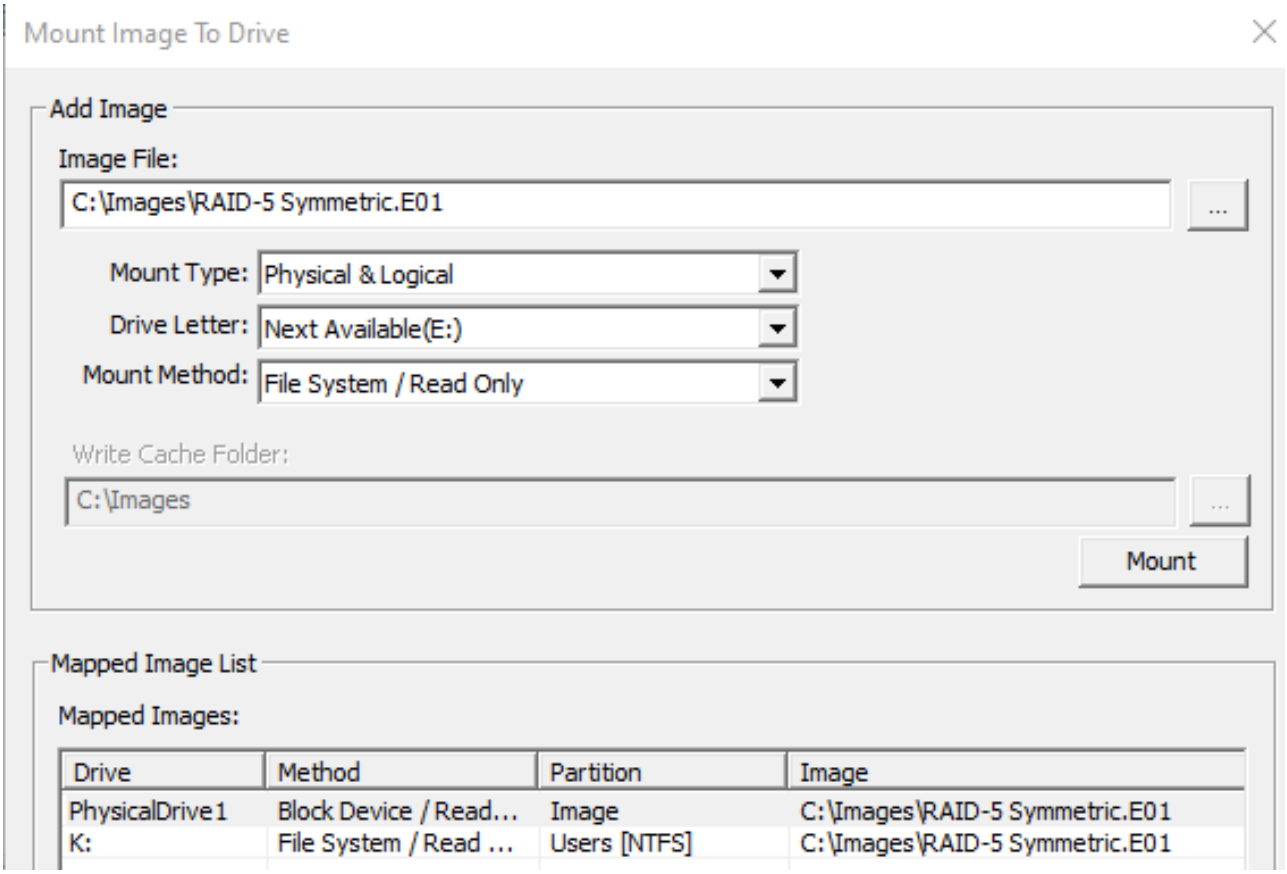


Figure 41: Mounting of "RAID-5 Symmetric.E01".

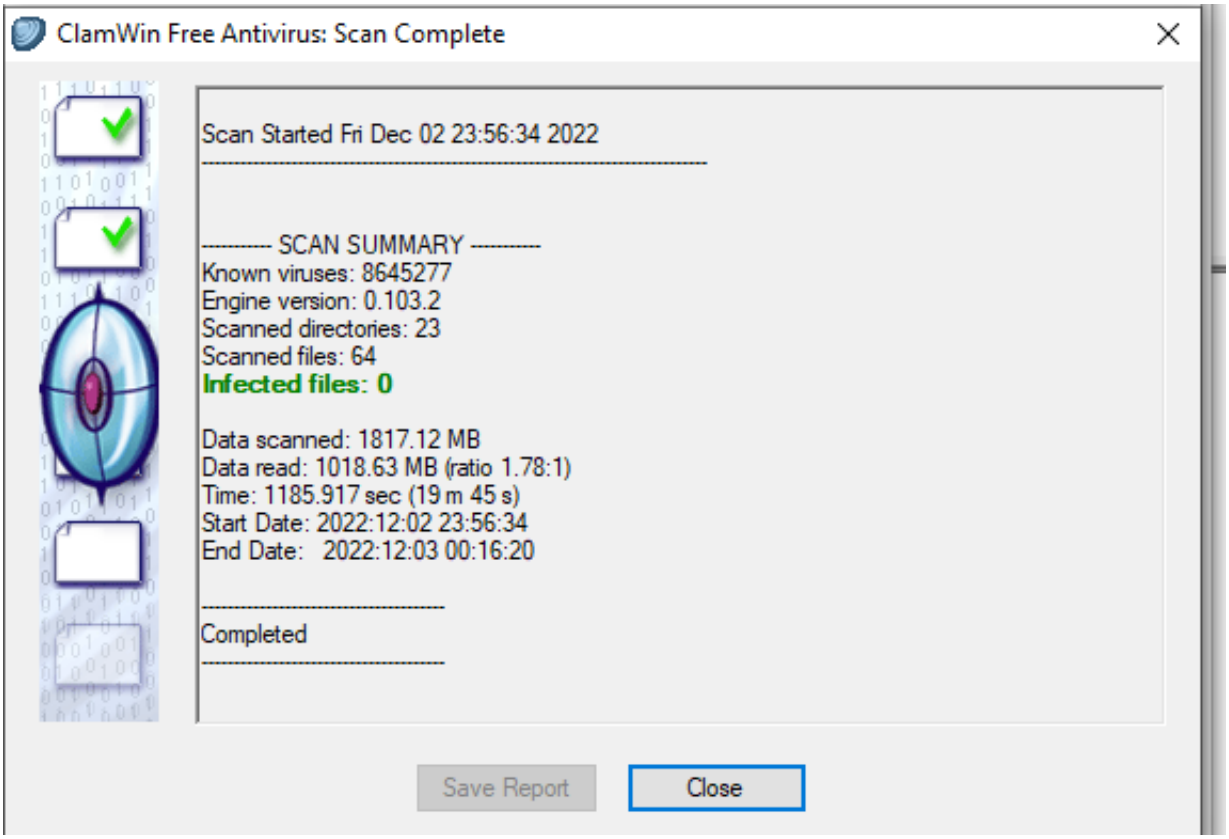


Figure 42: Virus Scan of "RAID-5 Symmetric.E01".

Processing

The analysis of the forensic images was handled in both the forensic program FTK from the company AccessData and EnCase from the company Guidance Software. EnCase was used to find evidence, search for keywords, and collect screenshots because of its ease of combing through large file systems. The FTK suite was used to mount images, extract files, examine registry files, and collect screenshots because of the way it presents registry files and how easy it is to mount and extract. The processing for all four of these forensic images failed in multiple ways and on both programs. Very little data and meta carving could be completed before EnCase and FTK gave errors that stopped all processing or crashed the program and virtual workstation. Indexing could also not be completed so potentially decryptable files may remain encrypted. See Exhibit A in the Reference section for more detailed error reports. All of these processes could be done by hand but automating them makes the forensic analysis more consistent, understandable to more people, and, most importantly, completable within a reasonable amount of time.

The stitching for the RAID5 Array from three separate forensic images into one readable forensic image of the array was done through EnCase. Inside of EnCase, the program is able to recognize the three RAID5 images, reconstruct the array, and export the virtual drive as a complete forensic image.

Decryption

There were no files found in all four of the evidence items which were decrypted. Over the course of the examination, the passwords “vmware” and “byteme@noplace.com” were found. The collected passwords were gathered by AccessData’s Password Recovery Tool Kit from the registry files NTUSER.DAT from each user and SAM from each windows operating system found inside the forensic images.

Gathering Pertinent Information

Once the forensic images were scanned for viruses, processed, and several passwords were found, the forensic analysis proceeded with the gathering of frequently useful artifacts. These artifacts include: Pictures, videos, email, calendar dates, user logon credentials, time zone information, language settings, browser history, browser cookies, browser cache, file shortcuts, personal documents, and message databases.

Findings

Tom Warner's Workstation

Workplace Integrity

On Mr. Warner's workstation, there are several pieces of evidence that demonstrate violations of workplace integrity. These include hard drive erasing programs, an email of intent regarding revenge towards the company, and unusual removable media programs and shortcuts.

Mr. Warner's workstation contains the hard drive erasing program Darik's Boot and Nuke (DBAN). This program is known for permanently erasing all data on a hard drive. DBAN is a program that should never be in the hands of someone outside of an IT team or someone who is already experienced in its use. Mr. Warner, who is a sales employee, should not have access to this program and the fact that he does is an active threat to the company's operations. The program's installation folder can be found at "PSC Tom WS\C\Program Files\Eraser\Boot\" and contains much of the information needed to know to run the program. There is a readme file in the installation folder that explains what the program is and how to use it, and it can be found at "PSC Tom WS\C\Program Files\Eraser\Boot\rea me.txt".

	Name		File Ext	Logical Size	Category
1	Lic			576	Folder
2	eBoot.exe		exe	1,418,929	Executable
3	changelog.txt		txt	5,174	Document
4	readme.txt		txt	3,945	Document
5	notes.txt		txt	1,320	Document
6	wipe.txt		txt	3,411	Document
7	Darik's Boot and Nuke.url		url	103	Windows

Figure 43: Darik's Boot and Nuke Installation folder from "PSC Tom WS.E01".

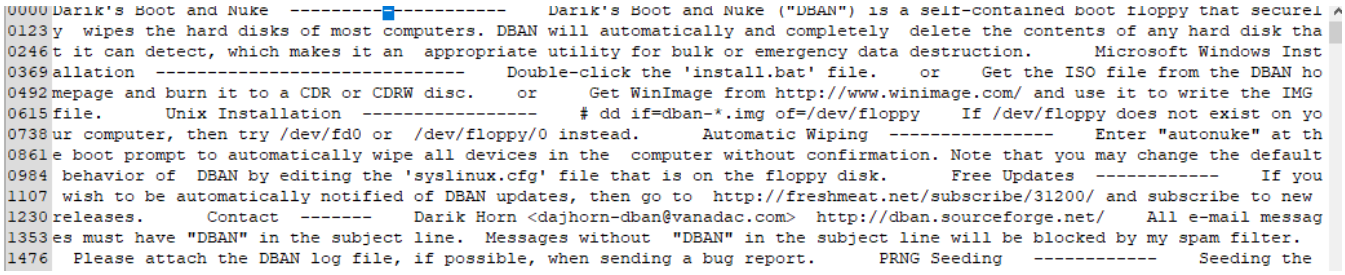
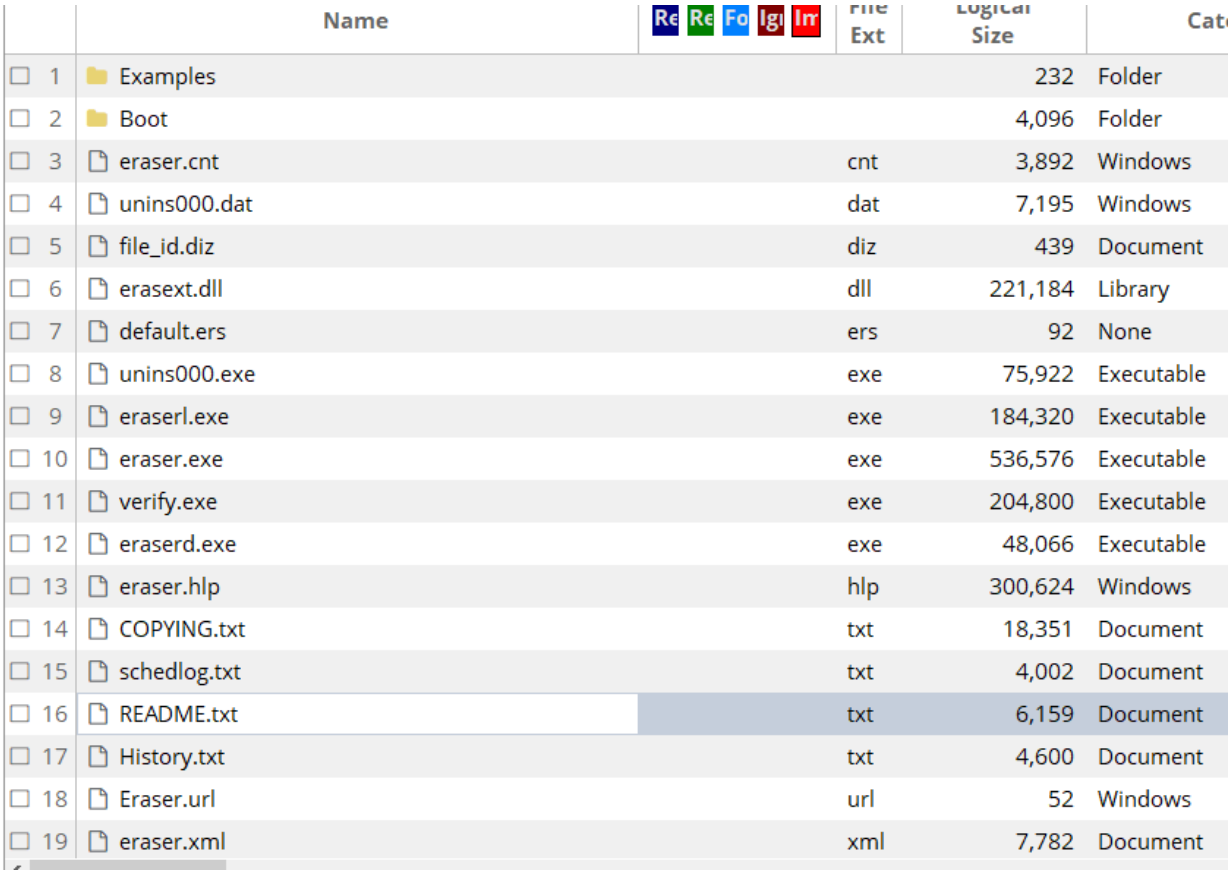


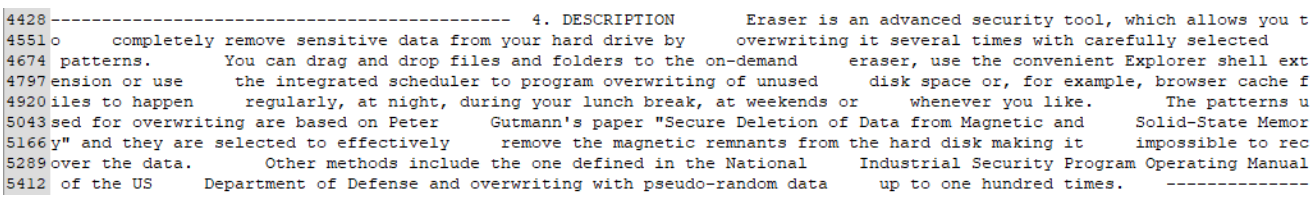
Figure 44: Darik's Boot and Nuke readme file from "PSC Tom WS.E01".

Secondly, this workstation has a file erasing program, known as Eraser. This program's installation folder can be found at "PSC Tom WS\C\Program Files\Eraser". There is a readme file in the program's folder that explains what the program is and how to use it, and it can be found at "PSC Tom WS\C\Program Files\Eraser\README.txt". The purpose of this program is to permanently delete a file and make it unrecoverable by writing over the location of a file multiple times. Other locations would be unaffected such as any shortcuts that referred to the deleted file.



	Name	File Ext	Logical Size	Cat
1	Examples		232	Folder
2	Boot		4,096	Folder
3	eraser.cnt	cnt	3,892	Windows
4	unins000.dat	dat	7,195	Windows
5	file_id.diz	diz	439	Document
6	erasext.dll	dll	221,184	Library
7	default.ers	ers	92	None
8	unins000.exe	exe	75,922	Executable
9	eraserl.exe	exe	184,320	Executable
10	eraser.exe	exe	536,576	Executable
11	verify.exe	exe	204,800	Executable
12	eraserd.exe	exe	48,066	Executable
13	eraser.hlp	hlp	300,624	Windows
14	COPYING.txt	txt	18,351	Document
15	schedlog.txt	txt	4,002	Document
16	README.txt	txt	6,159	Document
17	History.txt	txt	4,600	Document
18	Eraser.url	url	52	Windows
19	eraser.xml	xml	7,782	Document

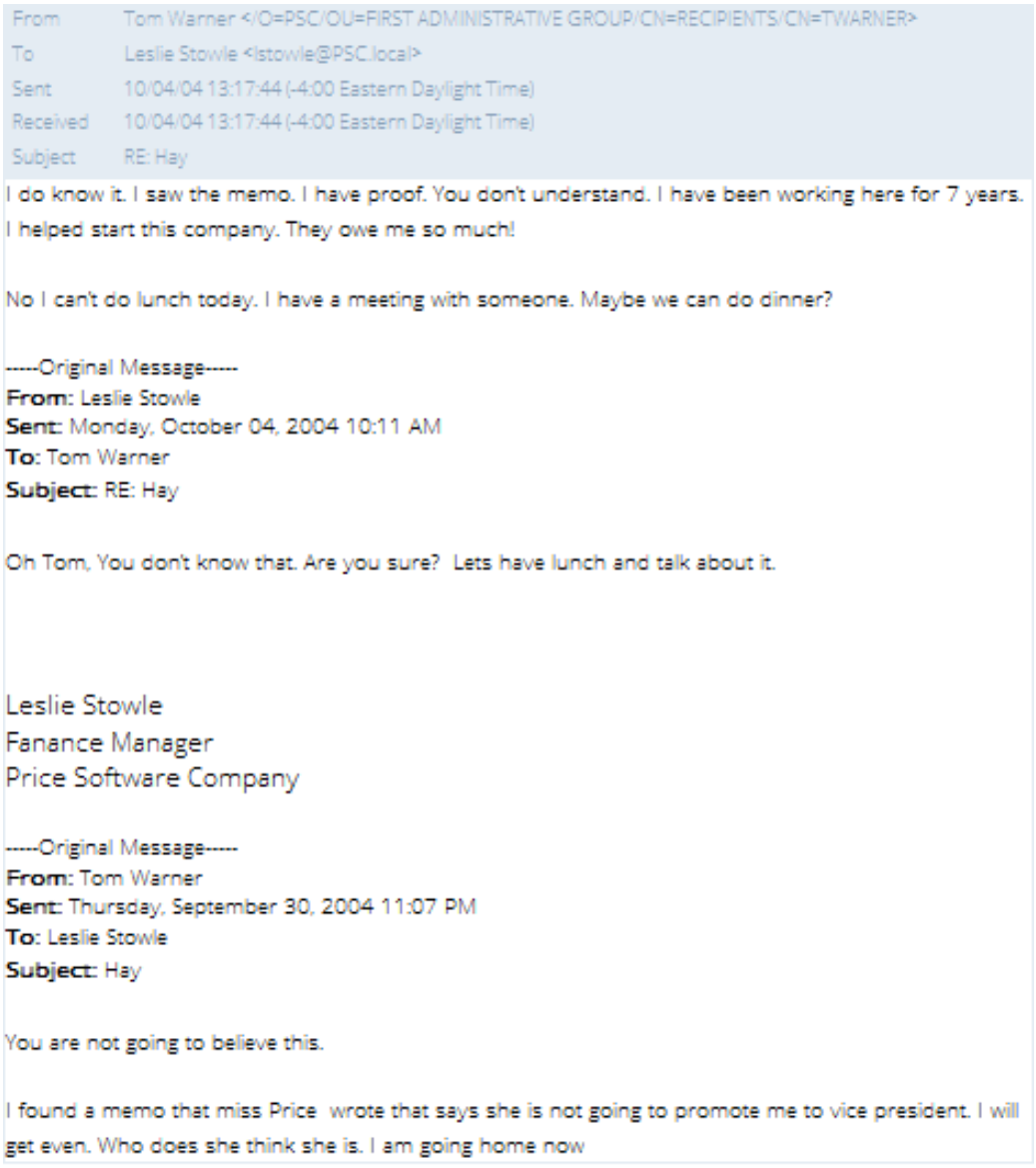
Figure 45: Eraser folder from "PSC Tom WS.E01".



```
4428 ---------------------------------------------  4. DESCRIPTION       Eraser is an advanced security tool, which allows you t
4551 o     completely remove sensitive data from your hard drive by     overwriting it several times with carefully selected
4674  patterns.       You can drag and drop files and folders to the on-demand     eraser, use the convenient Explorer shell ext
4797 ension or use     the integrated scheduler to program overwriting of unused     disk space or, for example, browser cache f
4920 iles to happen     regularly, at night, during your lunch break, at weekends or     whenever you like.       The patterns u
5043 sed for overwriting are based on Peter     Gutmann's paper "Secure Deletion of Data from Magnetic and     Solid-State Memor
5166 y" and they are selected to effectively     remove the magnetic remnants from the hard disk making it     impossible to rec
5289 over the data.       Other methods include the one defined in the National     Industrial Security Program Operating Manual
5412  of the US     Department of Defense and overwriting with pseudo-random data     up to one hundred times.    --------------
```

Figure 46: Eraser readme file from "PSC Tom WS.E01".

After discovering that he was not going to get a promotion, Mr. Warner communicated his discontent with Ms. Stowle. In an email, titled “RE: Hay”, he communicated that he will “get even” with the company, implying revenge. This email chain can be found at “PSC Tom WS\C\Documents and Settings\twarner\Local Settings\Application Data\Microsoft\Outlook\outlook.ost”.



From: Tom Warner </O=PSC/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=TWARNER>
To: Leslie Stowle <lstowle@PSC.local>
Sent: 10/04/04 13:17:44 (-4:00 Eastern Daylight Time)
Received: 10/04/04 13:17:44 (-4:00 Eastern Daylight Time)
Subject: RE: Hay

I do know it. I saw the memo. I have proof. You don't understand. I have been working here for 7 years. I helped start this company. They owe me so much!

No I can't do lunch today. I have a meeting with someone. Maybe we can do dinner?

-----Original Message-----
From: Leslie Stowle
Sent: Monday, October 04, 2004 10:11 AM
To: Tom Warner
Subject: RE: Hay

Oh Tom, You don't know that. Are you sure? Lets have lunch and talk about it.

Leslie Stowle
Fanance Manager
Price Software Company

-----Original Message-----
From: Tom Warner
Sent: Thursday, September 30, 2004 11:07 PM
To: Leslie Stowle
Subject: Hay

You are not going to believe this.

I found a memo that miss Price wrote that says she is not going to promote me to vice president. I will get even. Who does she think she is. I am going home now

Figure 47: Email communication from Mr. Warner expressing intent for revenge.

There is evidence that Mr. Warner frequently used a removeable USB storage device on his workstation. Specifically, both a desktop shortcut and a Recent shortcut can be found at “PSC Tom WS\C\Documents and Settings\twarner\Desktop\Shortcut to Removable Disk (E).lnk” and “PSC Tom WS\C\Documents and Settings\twarner\Recent\Removable Disk (E).lnk”, respectively.

There are also two removeable USB storage devices registered in the SYSTEM registry file of this machine. It is likely that Mr. Warner attached up to two USB storage devices while using this machine at work.

Figure 48: Desktop folder on the “twarner” user displaying shortcut.

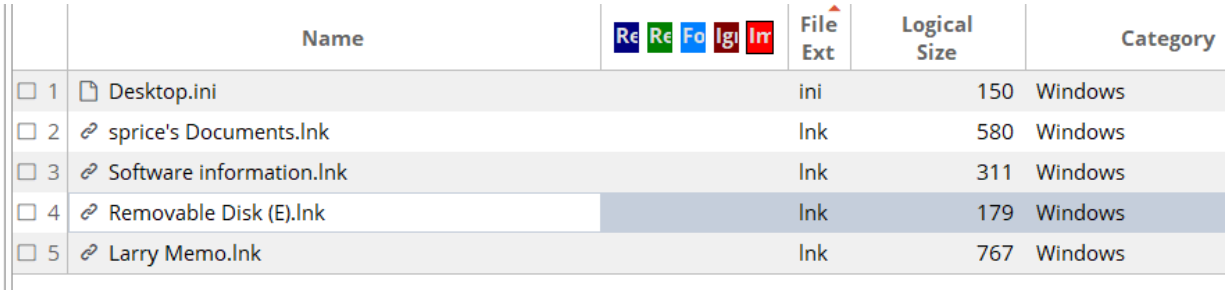


Figure 49: Recent folder on the “twarner” user displaying location shortcuts.

Name	Type	Data
DeviceDesc	REG_SZ	Disk drive
Capabilities	REG_DWORD	0x00000000 (0)
UINumber	REG_DWORD	0x00000000 (0)
HardwareID	REG_MULTI_SZ	USBSTOR\DiskNetac__OnlyDisk_____1.12 USBSTOR\DiskNetac__OnlyDisk_____ USB
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW
ClassGUID	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}
Service	REG_SZ	disk
ConfigFlags	REG_DWORD	0x00000000 (0)
ParentIdPrefix	REG_SZ	7&260c0899&0
Driver	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}\0001
Class	REG_SZ	DiskDrive
Mfg	REG_SZ	(Standard disk drives)
FriendlyName	REG_SZ	Netac OnlyDisk USB Device

Figure 50: USBSTOR section of the SYSTEM registry file showing the first USB storage device connected to this workstation.

Name	Type	Data
DeviceDesc	REG_SZ	USB Mass Storage Device
LocationInfo...	REG_SZ	USB Flash Disk
Capabilities	REG_DWORD	0x00000004 (4)
UINumber	REG_DWORD	0x00000000 (0)
HardwareID	REG_MULTI_SZ	USB\Vid_0dd8&Pid_8003&Rev_0104 USB\Vid_0dd8&Pid_8003
CompatibleIDs	REG_MULTI_SZ	USB\Class_08&SubClass_06&Prot_50 USB\Class_08&SubClass_06 USB\Class_08
ClassGUID	REG_SZ	{36FC9E60-C465-11CF-8056-444553540000}
Class	REG_SZ	USB
Driver	REG_SZ	{36FC9E60-C465-11CF-8056-444553540000}\0002
Mfg	REG_SZ	Compatible USB storage device
Service	REG_SZ	USBSTOR
ConfigFlags	REG_DWORD	0x00000000 (0)
ParentIdPrefix	REG_SZ	6&227a1c57&0

Figure 51: R USBSTOR section of the SYSTEM registry file showing the second USB storage device connected to this workstation.

Mr. Warner's workstation also has VMware installed. The installation folder for this program can be found at "PSC Tom WS\C\Program Files\VMware\". The VMware program allows you to run a virtual computer on your physical computer. A finance employee would likely not have a use for this program, but Mr. Warner could be using it to test other programs such as DBAN, Eraser, or DVD ripping tools. Unless approved by the company, a program like this likely does not belong here. This program's installing files can be found at "PSC Tom WS\C\WINDOWS\Installer\86200.mst" and "PSC Tom WS\C\WINDOWS\Installer\86203.msi".

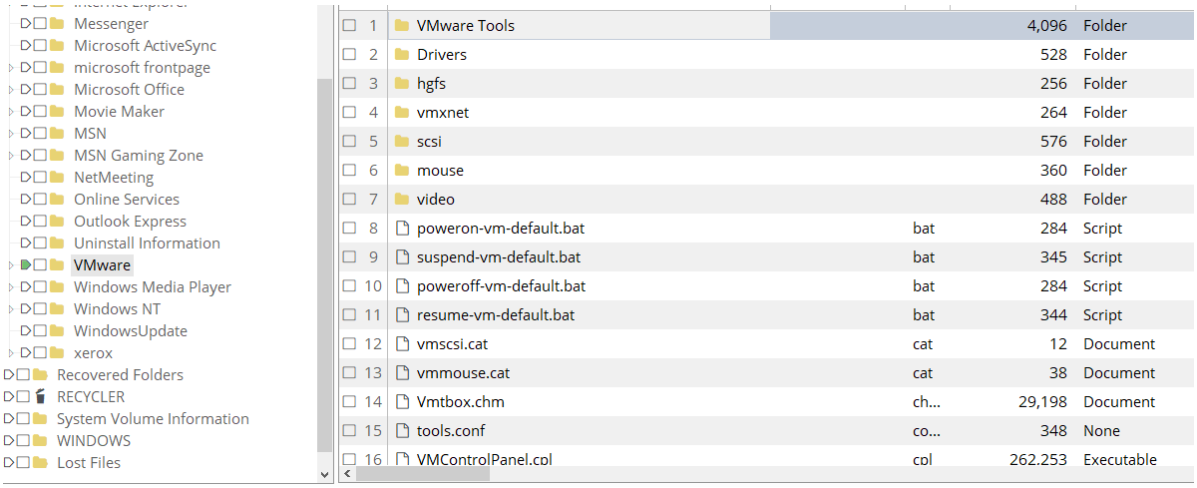


Figure 52: VMware install folder found on "PSC Tom WS.E01".

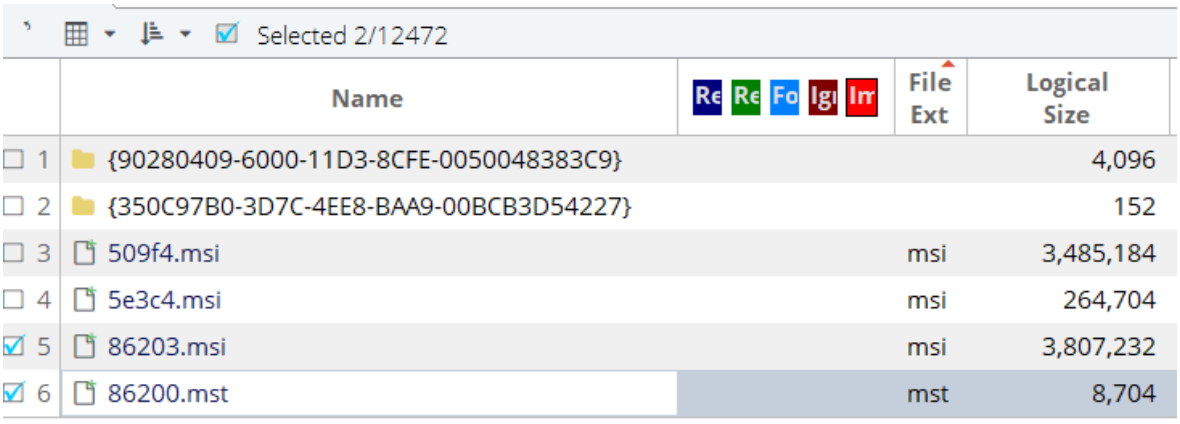


Figure 53: The VMware's install executables found on "PSC Tom WS.E01".

Mr. Warner had access to Ms. Price's personal documents. A shortcut to Ms. Price's documents can be found in the Recent folder of the user "twarner" and in the Microsoft Office Recent folder at "PSC Tom WS\C\Documents and Settings\twarner\Recent\sprice's Documents.lnk" and "PSC Tom WS\C\Documents and Settings\twarner\Application Data\Microsoft\Office\Recent\sprice's Documents.LNK", respectively. The shortcut leads to Ms. Price's documents on a different workstation at "\\psc-ws-03\c$\Documents and Settings\sprice\My Documents". A user should not be able to visit the personal documents of another user, especially one that is of a higher rank. Abusing this permission would be inappropriate and potentially damaging if Eraser was used.

This also shows that Mr. Warner frequently accessed his USB storage device as seen from the shortcuts "Removable Disk (E).lnk" and "Software Information.lnk". The software information shortcut is a link to a file found on his USB storage device. These link files can be created by the system when a user frequently accesses the same file or location. This tells us that Mr. Warner frequents these specific locations.

	Name		File Ext	Logical Size	Category
1	Desktop.ini		ini	150	Windows
2	sprice's Documents.lnk		lnk	580	Windows
3	Software information.lnk		lnk	311	Windows
4	Removable Disk (E).lnk		lnk	179	Windows
5	Larry Memo.lnk		lnk	767	Windows

Figure 54: Recent folder on the "twarner" user.

```
sprice's Documents.LNK
Name    sprice's Documents.LNK
File Ext        LNK
Logical Size    580
Category        Windows
Last Accessed   10/01/04 01:46:27 (-4:00 Eastern Daylight Time)
File Created    10/01/04 01:46:27 (-4:00 Eastern Daylight Time)
Last Written    10/01/04 01:46:27 (-4:00 Eastern Daylight Time)
Item Path       PSC Tom WS\C\Documents and Settings\twarner\Application Data\Microsoft\Office\Recent\sprice's Documents.LNK
True Path       encase attempt 3\PSC Tom WS\C\Documents and Settings\twarner\Application Data\Microsoft\Office\Recent\sprice's Documents.LNK
Description     File, Archive
Entry Modified  10/01/04 01:46:27 (-4:00 Eastern Daylight Time)

Evidence File   PSC Tom WS
File Identifier 11742
GUID    25b8bc8a9609068b86541ab7e3723dc8
Short Name      SPRICE~1.LNK
Symbolic Link   \\psc-ws-03\c$\Documents and Settings\sprice\My Documents
Share   \\psc-ws-03\c$
Mapped Name     H:
Common Path     Documents and Settings\sprice\My Documents
Machine Name    psc-ws-03
Volume Id       {589E9818-55D1-423A-8388-CCBE05D0B831}
Own Id  {4312CFA2-1340-11D9-AACB-000C29376505} (Sequence:2ACB Timestamp: 10/01/04 00:24:30 MAC:00-0C-29-37-65-05 )
Birth Volume Id {589E9818-55D1-423A-8388-CCBE05D0B831}
Birth Object Id {4312CFA2-1340-11D9-AACB-000C29376505} (Sequence:2ACB Timestamp: 10/01/04 00:24:30 MAC:00-0C-29-37-65-05 )
```

Figure 55: Microsoft Office recent folder on the "twarner" user has a shortcut to Ms. Price's documents.

OFFICE RECENT ! LINK TO sprice documents.txt - Notepad

File Edit Format View Help

```
sprice's Documents.LNK
Name    sprice's Documents.LNK
File Ext        LNK
Logical Size    580
Category        Windows
Last Accessed   10/01/04 01:46:27 (-4:00 Eastern Daylight Time)
File Created    10/01/04 01:46:27 (-4:00 Eastern Daylight Time)
Last Written    10/01/04 01:46:27 (-4:00 Eastern Daylight Time)
Item Path       PSC Tom WS\C\Documents and Settings\twarner\Application Data\Microsoft\Office\Recent\sprice's Documents.LNK
True Path       encase attempt 3\PSC Tom WS\C\Documents and Settings\twarner\Application Data\Microsoft\Office\Recent\sprice's Documents.LNK
Description     File, Archive
Entry Modified  10/01/04 01:46:27 (-4:00 Eastern Daylight Time)

Evidence File   PSC Tom WS
File Identifier 11742
GUID    25b8bc8a9609068b86541ab7e3723dc8
Short Name      SPRICE~1.LNK
Symbolic Link   \\psc-ws-03\c$\Documents and Settings\sprice\My Documents
Share   \\psc-ws-03\c$
Mapped Name     H:
Common Path     Documents and Settings\sprice\My Documents
Machine Name    psc-ws-03
Volume Id       {589E9818-55D1-423A-8388-CCBE05D0B831}
Own Id  {4312CFA2-1340-11D9-AACB-000C29376505} (Sequence:2ACB Timestamp: 10/01/04 00:24:30 MAC:00-0C-29-37-65-05 )
Birth Volume Id {589E9818-55D1-423A-8388-CCBE05D0B831}
Birth Object Id {4312CFA2-1340-11D9-AACB-000C29376505} (Sequence:2ACB Timestamp: 10/01/04 00:24:30 MAC:00-0C-29-37-65-05 )
```

Figure 56: Link to S. Price's documents on the "twarner" user.

On his workstation, Mr. Warner has installed MagicISO, a CD burner and extraction program. A program like this can be used to copy company materials to a CD or rip files off a CD onto the local machine. Neither of these actions would normally be allowed for a standard user. This program can be found at “PSC Tom WS\C\WINDOWS\Prefetch\SETUP_MAGICISO.EXE-32AD4789.pf”. The program can be found in the prefetch which means that it had to have been run before on this machine. It also has a record in NTUSER.dat registry file in the twarner user showing that it likely came from the USB storage device that is called E:\. The location of the NTUSER.dat for twarner is at “PSC Tom WS\C\Documents and Settings\twarner\NTUSER.DAT”. Unless approved by the company, a program like this likely does not belong here.

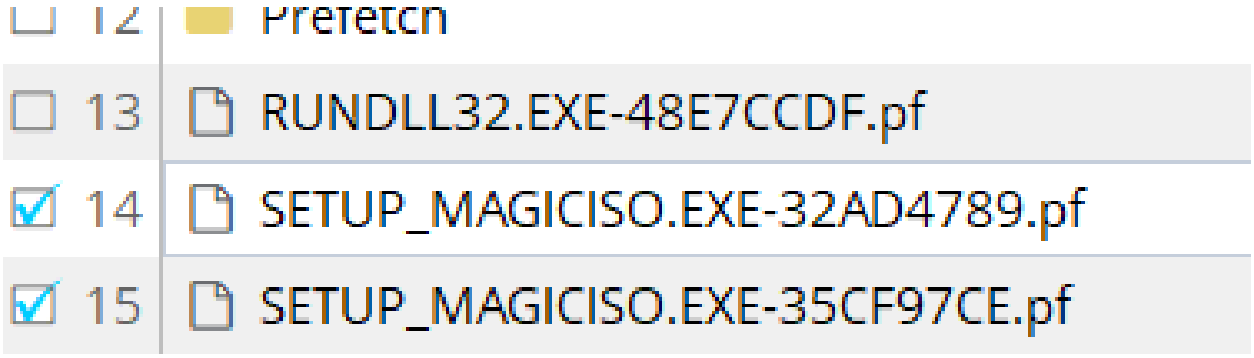


Figure 57: Magic ISO Program found under the Prefetch folder in “PSC Tom WS.E01”.

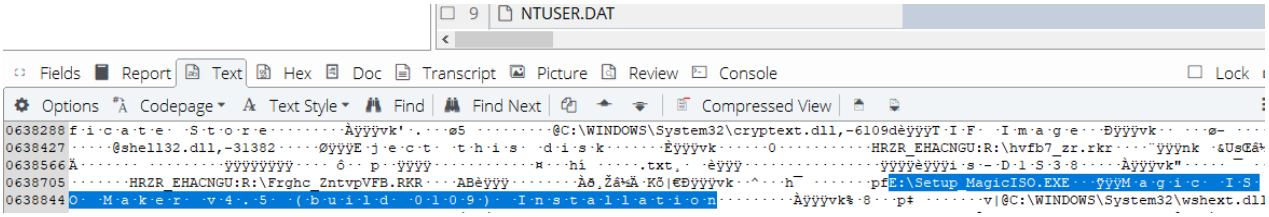


Figure 58: Magic ISO Program from USB drive as seen in NTuser.

There are files found in a folder called Protect that appear to be encrypted. In a folder called Crypto, there is an RSA key. The RSA (Rivest-Shamir-Adleman) algorithm is a system of cryptographic algorithms that are used to encrypt files and messages. The protected folder was likely encrypted with the RSA method. Unless approved by the company, privately encrypted files like this likely does not belong on a company machine. The Crypto folder can be found at "PSC Tom WS\C\Documents and Settings\twarner\Application Data\Microsoft\Crypto\" and the protected folder can be found at "PSC Tom WS\C\Documents and Settings\twarner\Application Data\Microsoft\Protect\".

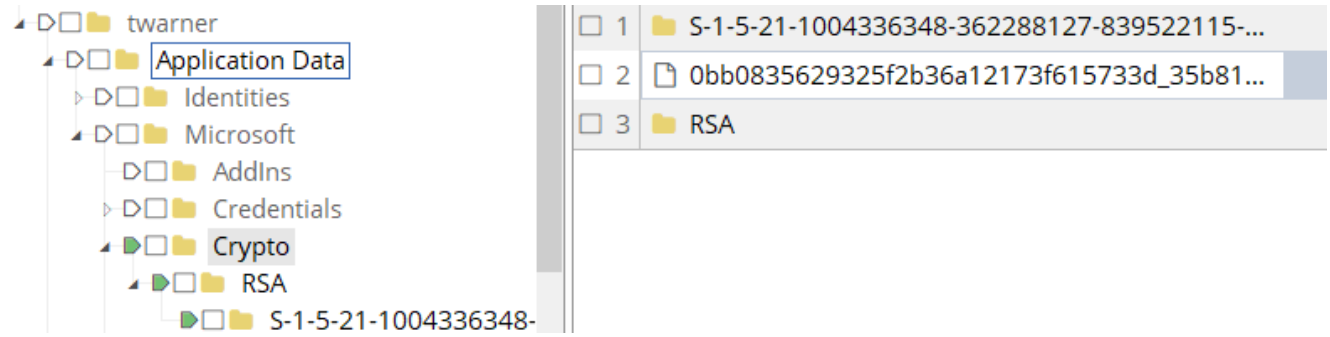


Figure 59: Crypto folder with RSA Key found in "PSC Tom WS.E01".

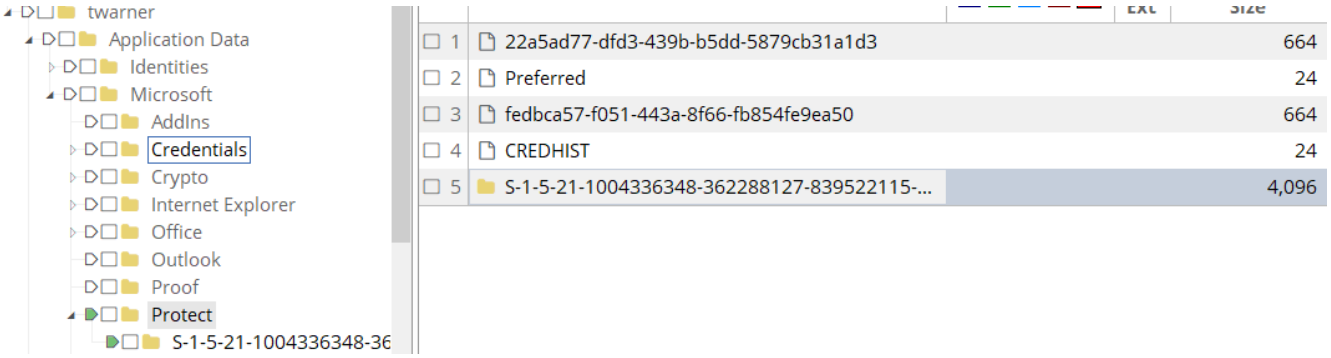


Figure 60: Protected folder found in "PSC Tom WS.E01".

Inappropriate Workplace Behavior

On Mr. Warner's workstation, there are pieces of evidence that demonstrate inappropriate workplace behavior. There are emails that imply an inappropriate relationship with coworker Ms. Stowle and the misuse of company time.

Several pieces of email evidence were found regarding the relationship between Mr. Warner and Ms. Stowle. First, several emails can be found about planning lunches together. The subjects of these emails are "RE: Vice Pres", "RE: Lunch", and "RE: Hay". These emails can be found at "PSC Tom WS\C\Documents and Settings\twarner\Local Settings\Application Data\Microsoft\Outlook\outlook.os".

Second, it appears that they are planning a vacation together. The email "RE: I like this one" provides an Expedia link regarding this vacation which can be found at "PSC Tom WS\C\Documents and Settings\twarner\Local Settings\Application Data\Microsoft\Outlook\outlook.os".

From	Leslie Stowle </O=PSC/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=LSTOWLE>
To	Tom Warner <twarner@PSC.local>
Sent	09/30/04 14:11:01 (-4:00 Eastern Daylight Time)
Received	09/30/04 14:11:01 (-4:00 Eastern Daylight Time)
Subject	RE: Vice Pres

Oh Tom I am so proud of you. I always knew you would promote.
Yes we can do lunch Mr. VP

Leslie Stowle
Fanance Manager
Price Software Company

-----Original Message-----
From: Tom Warner
Sent: Thursday, September 30, 2004 10:55 AM
To: Leslie Stowle
Subject: Vice Pres

Hay Leslie,

Did you see the e-mail about ""MY NEW JOB" Wee I can't wait, god knows I deserve it and I sure can use the x-tra money.

PS. Want to do lunch. Hee Hee

HD

Figure 61: Email communication between Mr. Warner and Ms. Stowle about a promotion and lunch from "PSC Tom WS.E01".

From	Leslie Stowle </O=PSC/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=LSTOWLE>
To	Tom Warner <twarner@PSC.local>
Sent	09/01/04 14:27:27 (-4:00 Eastern Daylight Time)
Received	09/01/04 14:27:27 (-4:00 Eastern Daylight Time)
Subject	RE: Lunch

Sure same place?

-----Original Message-----
From: Tom Warner
Sent: Wednesday, September 01, 2004 11:17 AM
To: Leslie Stowle
Subject: Lunch

Do you want to meet for lunch today?

Tom

Figure 62: Another email communication between Mr. Warner and Ms. Stowle about lunch from "PSC Tom WS.E01".

From	Tom Warner </O=PSC/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=TWARNER>
To	Leslie Stowle <lstowle@PSC.local>
Sent	10/04/04 13:32:18 (-4:00 Eastern Daylight Time)
Received	10/04/04 13:32:18 (-4:00 Eastern Daylight Time)
Subject	RE: I like this one

That looks nice. Make it happen.

-----Original Message-----
From: Leslie Stowle
Sent: Monday, October 04, 2004 10:32 AM
To: Tom Warner
Subject: RE: I like this one

&

Leslie Stowle
Fanance Manager
Price Software Company

-----Original Message-----
From: Tom Warner
Sent: Monday, October 04, 2004 10:31 AM
To: Leslie Stowle
Subject: RE: I like this one

The link does not work.

-----Original Message-----
From: Leslie Stowle
Sent: Monday, October 04, 2004 10:30 AM
To: Tom Warner
Subject: I like this one

http://www.expedia.com/pub/agent.dll?qscr=cmhi&itid=&itdx=&itty=&ecid=&from=&tpst=

Leslie Stowle
Fanance Manager
Price Software Company

Figure 63: Email communication between Mr. Warner and Ms. Stowle about a vacation.

Further evidence proving that the two are planning to vacation together, Mr. Warner visited the Expedia link which is found in his browser cookies. This cookie can be found at “PSC Tom WS\C\Documents and Settings\twarner\Cookies\twarner@expedia[2].txt”. Another piece of evidence of travel-related activity found in his cookies is a cookie to a website about passports, which can be found at “PSC Tom WS\C\Documents and Settings\twarner\Cookies\twarner@passport[1].txt”.

Name	twarner@expedia[2].txt
File Ext	txt
Logical Size	433
Category	Document
Last Accessed	10/04/04 13:30:48 (-4:00 Eastern Daylight Time)
File Created	10/04/04 13:30:48 (-4:00 Eastern Daylight Time)
Last Written	10/04/04 13:30:48 (-4:00 Eastern Daylight Time)
MD5	7d79adb8cd58ce312a8876fc56b9c0d4
SHA1	0485c136eade52319cec40c6be54a09c8eab8641
Item Path	PSC Tom WS\C\Documents and Settings\twarner\Cookies\twarner@expedia[2].txt
True Path	encase attempt 3\PSC Tom WS\C\Documents and Settings\twarner\Cookies\twarner@expedia[2].txt
Description	File, Archive

Figure 64: Expedia cookie found on “PSC Tom WS.E01”.

Name	twarner@passport[1].txt
File Ext	txt
Logical Size	89
Category	Document
Last Accessed	10/27/04 11:41:52 (-4:00 Eastern Daylight Time)
File Created	09/30/04 12:54:39 (-4:00 Eastern Daylight Time)
Last Written	09/30/04 12:54:39 (-4:00 Eastern Daylight Time)
MD5	8de6245ad1f4ba3ab9c6c8bf461e46c9
SHA1	a97c08c43638e795680bae16720658df1bf090a6
Item Path	PSC Tom WS\C\Documents and Settings\twarner\Cookies\twarner@passport[1].txt
True Path	encase attempt 3\PSC Tom WS\C\Documents and Settings\twarner\Cookies\twarner@passport[1].txt
Description	File, Archive

Figure 65: Passport cookie found on “PSC Tom WS.E01”.

Also found on Mr. Warner's workstation, there is evidence of online gaming programs. First, there is the installation of a program called MSN Gaming Zone, which allows for users to download online games and play them from their local machine. This can be found at "PSC Tom WS\C\Program Files\MSN Gaming Zone\". Second, there is the installation of Windows Pinball, which can be found at "PSC Tom WS\C\Program Files\Windows NT\Pinball\PINBALL.EXE". Having and playing these games can be a misuse of company time.

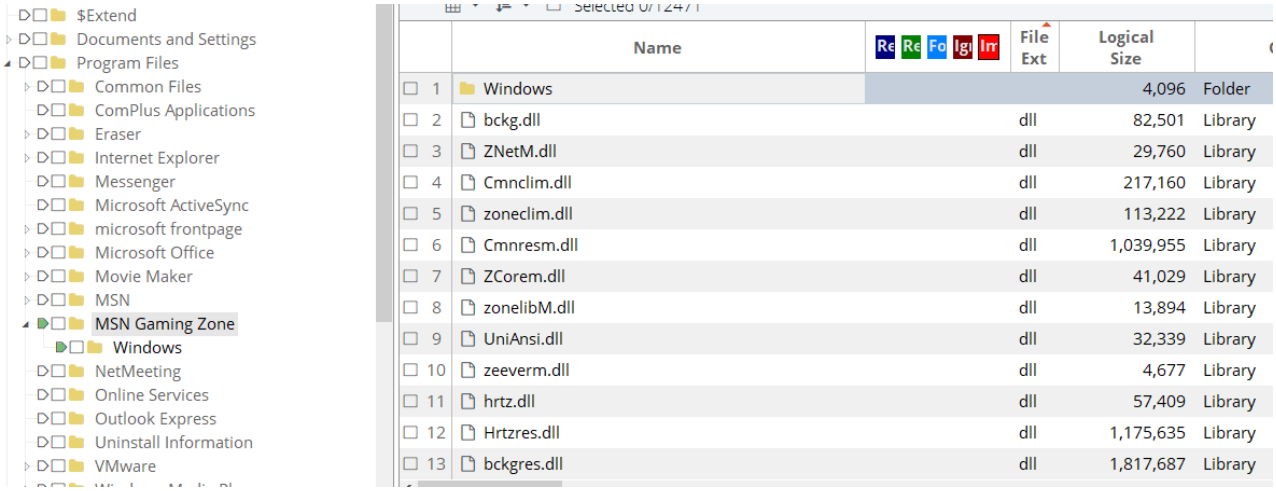
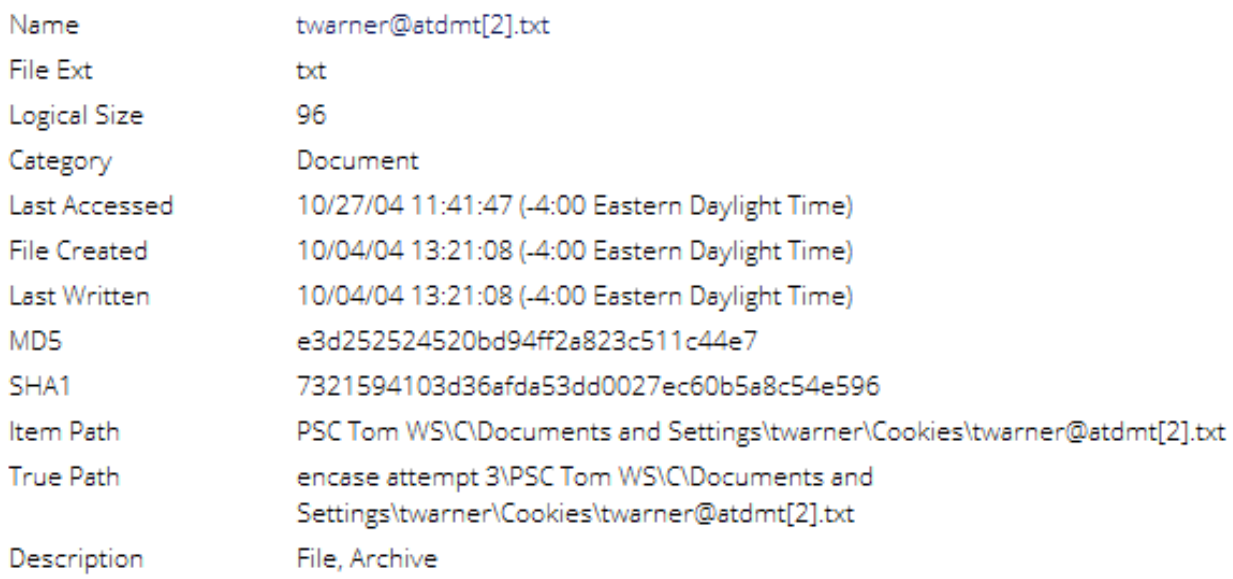


Figure 66: MSN Gaming Zone installation folder found on "PSC Tom WS.E01".

	Name	File Ext	Logical Size	Ca
1	Pinball		12,288	Folder
2	Accessories		152	Folder
3	table.bmp	b...	339,178	Picture
4	PINBALL.DAT	DAT	928,700	Windows
5	FONT.DAT	DAT	3,947	Windows
6	htrn_jis.dll	dll	13,312	Library
7	PINBALL.EXE	EXE	272,896	Executable
8	dialer.exe	exe	522,240	Executable
9	wordpad.exe	exe	200,704	Executable
10	hypertrm.exe	exe	28,160	Executable
11	wavemix.inf	inf	2,687	Windows
12	PINBALL.MID	MID	108,607	Multimedia

Figure 67: Windows Pinball installation folder found on "PSC Tom WS.E01".

In his cookies, there is the ATDMT cookie, which is most commonly acquired from visiting Facebook and tracts a lot of computer information. In fact, this specific cookie tracks so much information about the host machine that it is frequently called spyware. This cookie is evidence that Mr. Warner was on Facebook at work. This can be found at “PSC Tom WS\C\Documents and Settings\twarner\Cookies\twarner@atdmt[2].txt”.



Name	twarner@atdmt[2].txt
File Ext	txt
Logical Size	96
Category	Document
Last Accessed	10/27/04 11:41:47 (-4:00 Eastern Daylight Time)
File Created	10/04/04 13:21:08 (-4:00 Eastern Daylight Time)
Last Written	10/04/04 13:21:08 (-4:00 Eastern Daylight Time)
MD5	e3d252524520bd94ff2a823c511c44e7
SHA1	7321594103d36afda53dd0027ec60b5a8c54e596
Item Path	PSC Tom WS\C\Documents and Settings\twarner\Cookies\twarner@atdmt[2].txt
True Path	encase attempt 3\PSC Tom WS\C\Documents and Settings\twarner\Cookies\twarner@atdmt[2].txt
Description	File, Archive

Figure 68: ATDMT cookie found on “PSC Tom WS.E01”.

Leslie Stowle's Workstation

Workplace Integrity

Ms. Stowle's workstation has VMware installed. The installation folder for this program can be found at "PSC Leslie WS\C\Program Files\VMware\". The VMware program allows you to run a virtual computer on your physical computer. A finance employee would likely not have a use for this program. Unless approved by the company, a program like this likely does not belong here. This program's installing files can be found at "PSC Leslie WS\C\WINDOWS\Installer\86200.mst" and "PSC Leslie WS\C\WINDOWS\Installer\86203.msi".

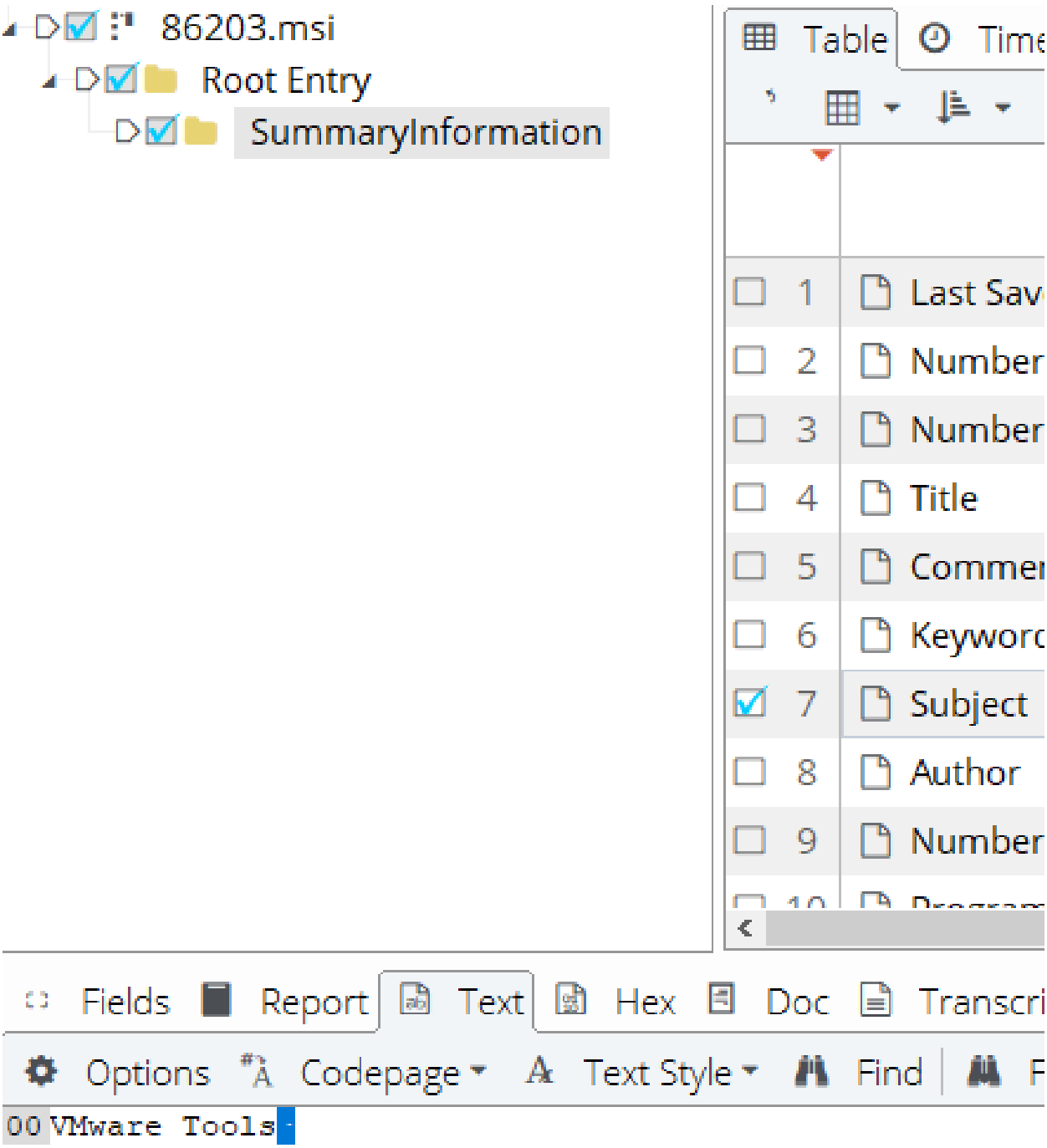


Figure 69: VMware installation exe found in Installer folder on "PSC Leslie WS.E01".

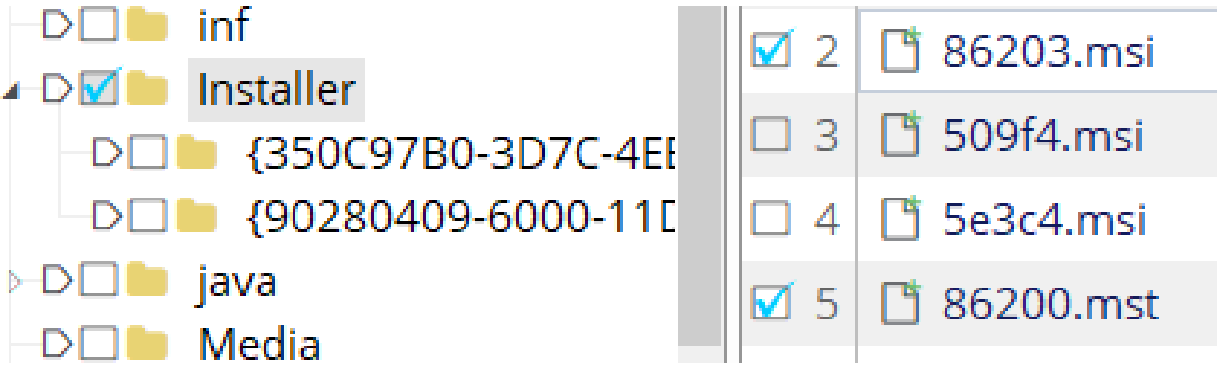


Figure 70: The VMware's installers found on "PSC Leslie WS.E01".

There are files found in a folder called Protect that appear to be encrypted. In a folder called Crypto, there is an RSA key. The RSA (Rivest-Shamir-Adleman) algorithm is a system of cryptographic algorithms that are used to encrypt files and messages. The protected folder was likely encrypted with the RSA method. Unless approved by the company, privately encrypted files like this likely does not belong on a company machine. The Crypto folder can be found at "PSC Leslie WS\C\Documents and Settings\lstowle\Application Data\Microsoft\Crypto\", and the protected folder can be found at "PSC Leslie WS\C\Documents and Settings\lstowle\Application Data\Microsoft\Protect\".

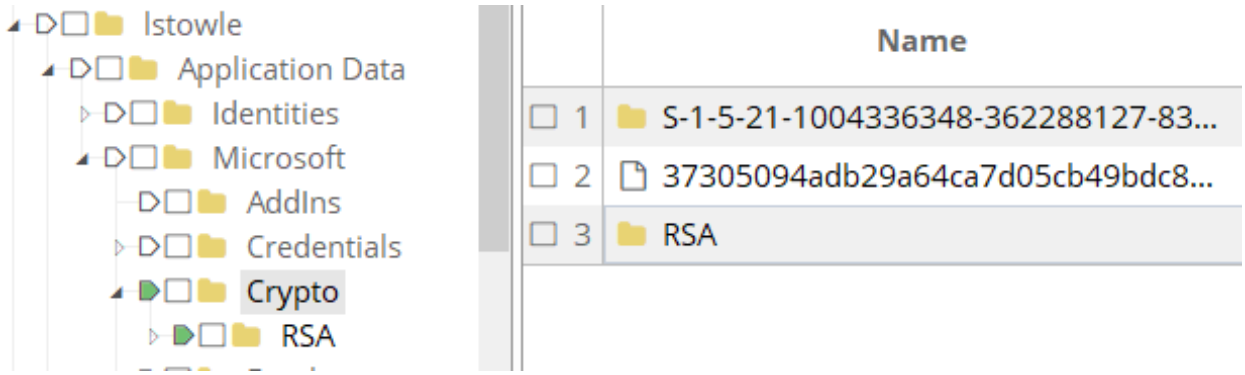


Figure 71: Crypto folder with RSA Key found in "PSC Leslie WS.E01".

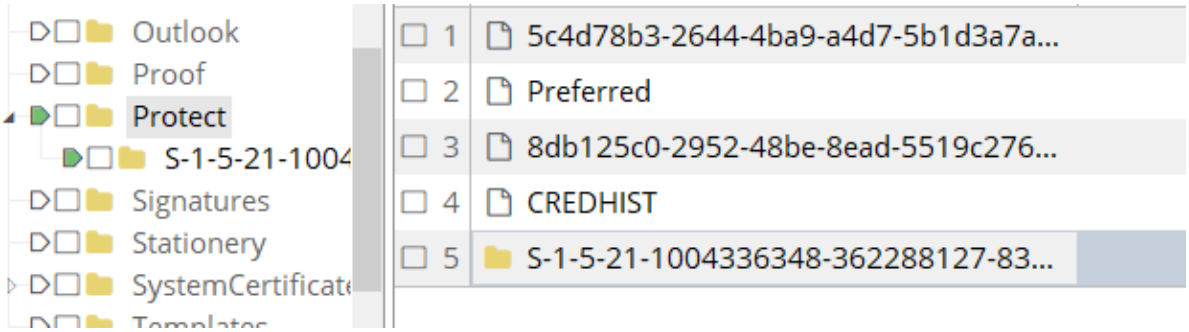


Figure 72: Protected folder found on "PSC Leslie WS.E01".

There are several useful prefetch files found on this machine. Files found in the prefetch means that it had to have been run before on this machine. Most importantly, it shows that the Eraser program has been installed and ran before on this machine. If this program was used, it is likely that some files have been deleted and cannot be seen by data carving. This is a very unusual and potentially dangerous action. The prefetch files also show that VMware has been actively used on this machine but does not give how it was used.

Figure 73: Prefetched programs found on "PSC Leslie WS.E01".

Inappropriate Workplace Behavior

Ms. Stowle's cookies folder exposes some of her activities at work. Specifically, she has cookies relating to travel such as the TripAdvisor cookie, Passport cookie, FranceGuide cookie, and the Expedia cookie show that she is viewing traveling websites at work. These cookies also back up the theory that Ms. Stowle and Mr. Warner are planning a trip together. There is also the ATDMT cookie, which is most commonly acquired from visiting Facebook and tracts a lot of computer information. In fact, this specific cookie tracks so much information about the host machine that it is frequently called spyware. This cookie is evidence that Ms. Stowle was on Facebook at work. All cookies can be found at "PSC Leslie WS\C\Documents and Settings\lstowle\Cookies\".

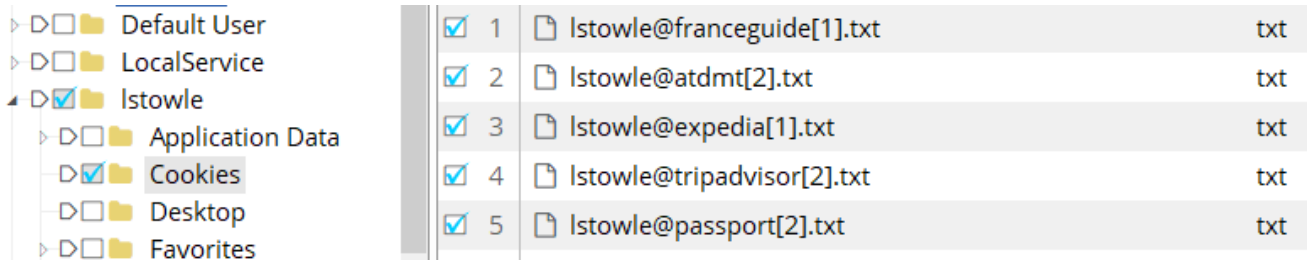


Figure 74: Cookies folder from "PSC Leslie WS.E01".

Ms. Stowle's Internet Explorer history shows various travel searches, including Expedia,

Travelocity, and several other travel related websites. This history can be found at "PSC Leslie WS\C\Documents and Settings\lstowle\Local Settings\Temporary Internet Files\Content.IE5\W1WFZXOA\search[2]".

There are also pieces of websites and images downloaded to Ms. Stowle's temporary internet files. These pieces of websites include travel deals, travel articles, and information on Hawaiian tourism. The temporary images are all related to travel websites in some way. The temporary images from travel websites can be found in Exhibit B of the References section. The named list of the images can still be found below.

These temporary internet files can be found at "PSC Leslie WS\C\Documents and Settings\lstowle\Local Settings\Temporary Internet Files\Content.IE5\".

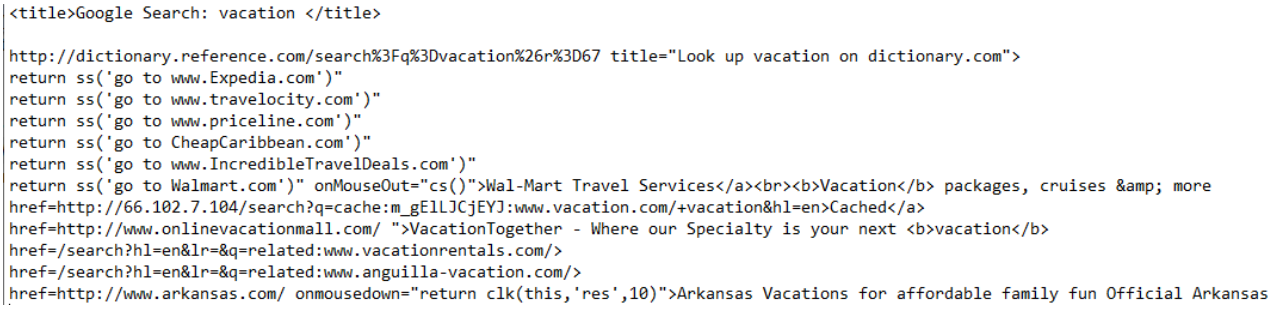


Figure 75: Filtered Internet Explorer history from "PSC Leslie WS.E01".

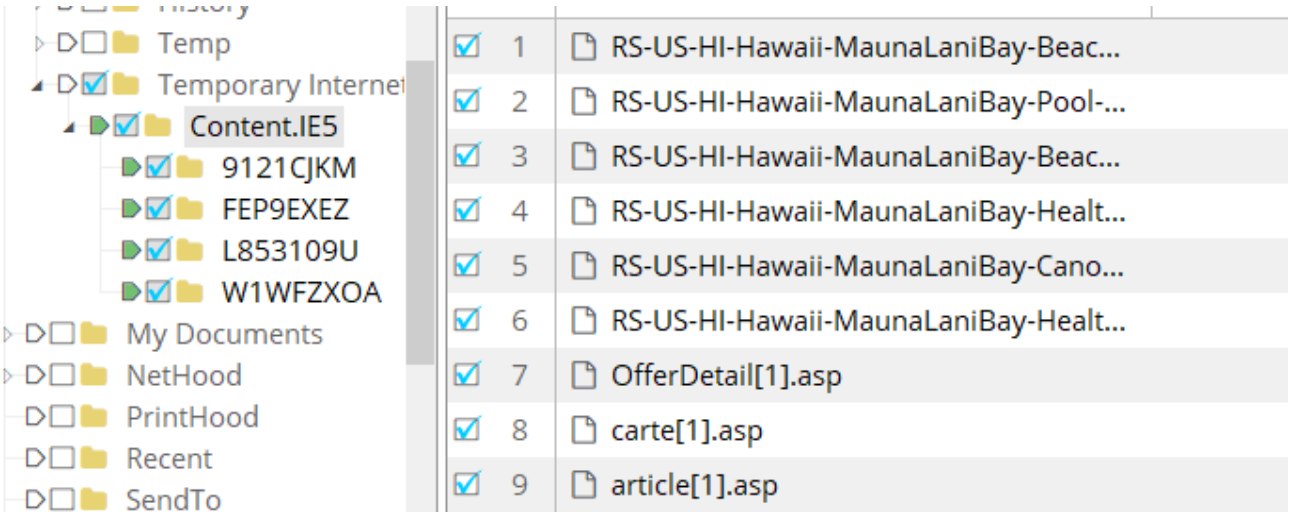


Figure 76: Temporary Internet files containing travel websites from "PSC Leslie WS.E01".

☑	1	cms_image[2].jpg	j.	6,281	Picture
☑	2	cms_image[1].gif	g	1,994	Picture
☑	3	091404_Copen_90x90[1]...	g	3,663	Picture
☑	4	DS_EUR_Acol[1].jpg	j.	11,647	Picture
☑	5	expedia-deals-120x60-d...	g	2,450	Picture
☑	6	0904_Ski_bnr[1].gif	g	10,460	Picture
☑	7	0904_PkgSave_bnr[1].gif	g	6,321	Picture
☑	8	logo_expedia_170x41[1]...	g	1,786	Picture
☑	9	pop_box_top[1].gif	g	2,616	Picture
☑	10	triplogo_sm[1].gif	g	1,659	Picture
☑	11	cms_image[2].gif	g	1,473	Picture
☑	12	cms_image[1].jpg	j.	5,041	Picture
☑	13	carte1[1].gif	g	3,163	Picture
☑	14	1004_HolSale_destopgs[...	g	2,682	Picture
☑	15	9684_28_t[1].jpg	j.	2,864	Picture
☑	16	091504_SAS_banner_90_...	g	2,360	Picture
☑	17	logo_expedia_bottom[1...	g	1,949	Picture
☑	18	d_agentnet_logo_login[...	g	1,679	Picture
☑	19	d_whois[1].gif	g	1,273	Picture
☑	20	logo[1].gif	g	2,878	Picture
☑	21	426160_15_b[1].jpg	j.	32,620	Picture
☑	22	426160_34_b[1].jpg	j.	36,452	Picture

Figure 77: Temporary Internet images relating to travel from "PSC Leslie WS.E01" - Part 1.

☑	23	426160_5_b[1].jpg	j.	36,178	Picture
☑	24	426160_10_b[1].jpg	j.	33,141	Picture
☑	25	426160_27_b[1].jpg	j.	24,029	Picture
☑	26	426160_15_t[1].jpg	j.	2,775	Picture
☑	27	426160_11_t[1].jpg	j.	2,501	Picture
☑	28	426160_13_t[1].jpg	j.	2,755	Picture
☑	29	426160_4_t[1].jpg	j.	2,594	Picture
☑	30	426160_32_t[1].jpg	j.	2,693	Picture
☑	31	426160_9_t[1].jpg	j.	2,831	Picture
☑	32	426160_14_t[1].jpg	j.	2,635	Picture
☑	33	getmap[1].gif	g	8,349	Picture
☑	34	tguin[1].gif	g	670	Picture
☑	35	logo_h[1].gif	g	2,320	Picture
☑	36	mini_carte_uk[1].gif	g	6,659	Picture
☑	37	cms_image[1].gif	g	3,316	Picture
☑	38	tz_logo[1].gif	g	1,346	Picture
☑	39	tvacn[1].gif	g	572	Picture
☑	40	i105478_big_australia_Li...	j.	10,968	Picture
☑	41	AddToTripRequest[1].gif	g	1,243	Picture
☑	42	vcom_top_logo[1].gif	g	2,687	Picture
☑	43	d_whyuse[1].gif	g	1,530	Picture
☑	44	426160_12_l[1].jpg	j.	12,105	Picture

Figure 78: Temporary Internet images relating to travel from "PSC Leslie WS.E01" - Part 2.

45	426160_35_b[1].jpg	j.	33,095	Picture
46	426160_13_b[1].jpg	j.	21,471	Picture
47	426160_33_b[1].jpg	j.	36,366	Picture
48	426160_32_b[1].jpg	j.	34,047	Picture
49	426160_28_b[1].jpg	j.	25,747	Picture
50	426160_3_t[1].jpg	j.	2,572	Picture
51	426160_8_t[1].jpg	j.	2,699	Picture
52	426160_33_t[1].jpg	j.	2,394	Picture
53	426160_10_t[1].jpg	j.	2,912	Picture
54	426160_28_t[1].jpg	j.	2,423	Picture
55	426160_27_t[1].jpg	j.	2,821	Picture
56	426160_26_s[1].jpg	j.	5,952	Picture
57	big_island[1].gif	g	10,016	Picture
58	tmapn[1].gif	g	367	Picture
59	tcrun[1].gif	g	421	Picture

Figure 79: Temporary Internet images relating to travel from "PSC Leslie WS.E01" - Part 3.

Price Software Server

On the company server, there are fewer pieces of evidence than the Workstations that display a large amount of inappropriate behavior in the workplace. Most importantly, it will show the use of inappropriate programs being installed and some online games being played.

In the Price Software Server, there is a record of a VMware installation executable which was not yet installed. The VMware program allows you to run a virtual computer on your physical computer. This can be found at “PSC Server OS\C\Documents and Settings\Administrator\Application Data\Microsoft\Installer\{B53D42E8-872B-430E-82D4-80065A31FCE1}\1033.MST”.

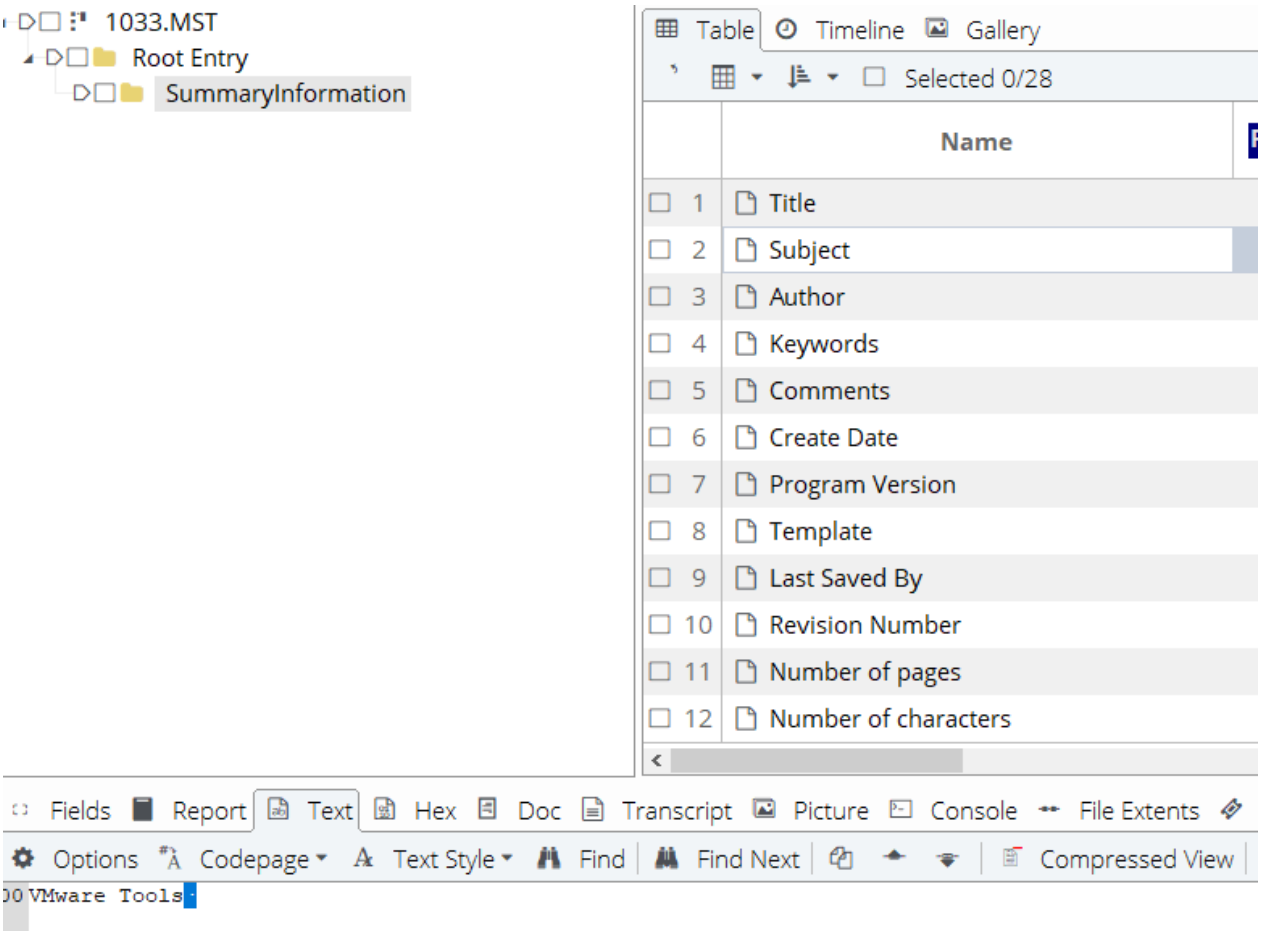


Figure 80: VMware installation executable from Installer folder.

In the folder “Lost Files” of the company server, there is a record of a piece of a website called “Eraser57Setup[2].htm” which suggests that the machine has visited the download page for the program Eraser. This can be found at “PSC Server OS\C\Lost Files\Eraser57Setup[2].htm” There is also evidence of Eraser having been downloaded before on this machine in the Internet Explorer history, which shows a visit to the program’s Source Forge page. The history can be found at “PSC Server OS\C\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012004092920040930\index.dat”.

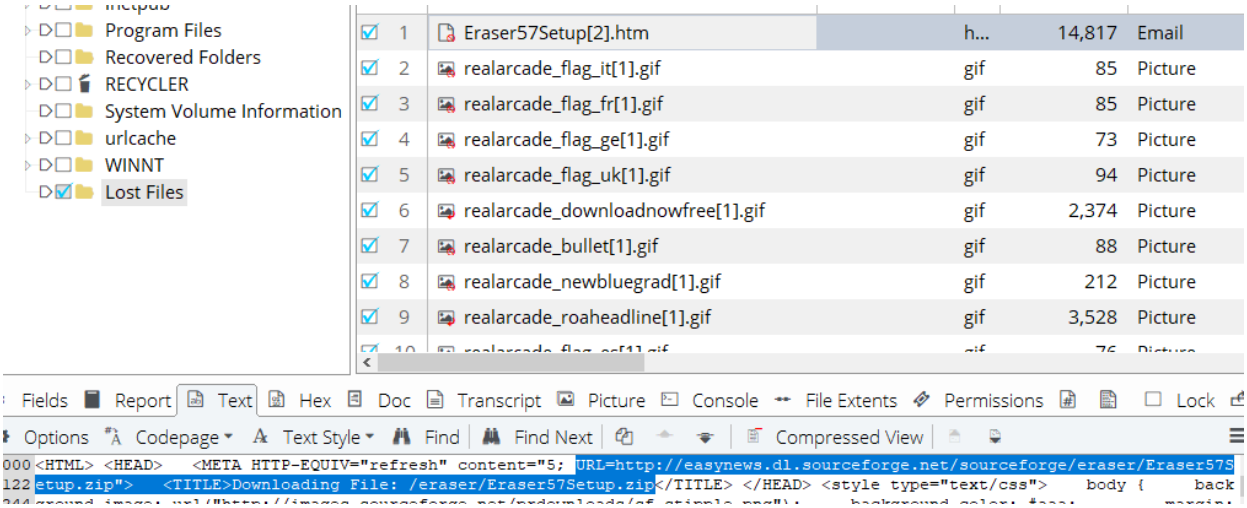


Figure 81: Eraser Setup found in Price Software’s Server.

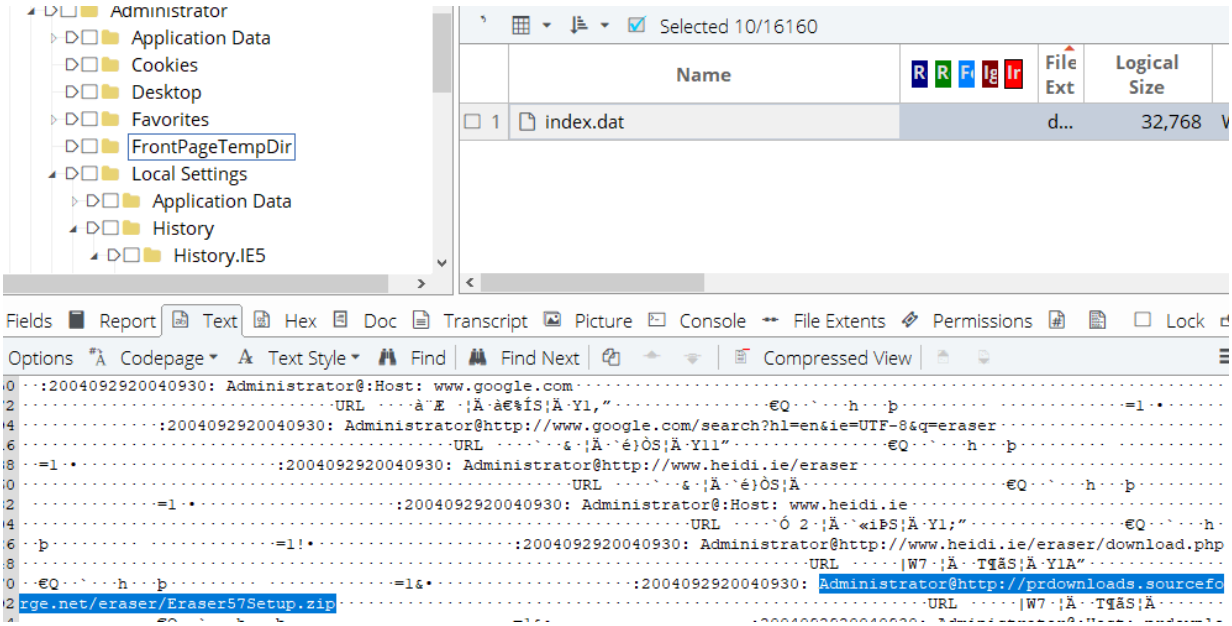


Figure 82: Eraser download found in IE history of Price Software's Server.

In the server's Recent folder, shortcuts can be found to Magic ISO's setup, to another CD burner's setup (burn4free), and to a gaming program (Real Arcade). Link files of these being created suggest that these specific files have been used on this machine before. These also be found at "\\2KADVSERVER\Users\Software\Setup_MagicISO.EXE", "\\2KADVSERVER\Users\Software\burn4free_setup.exe", and "\\2KADVSERVER\Users\Software\realarcade.exe", respectively.

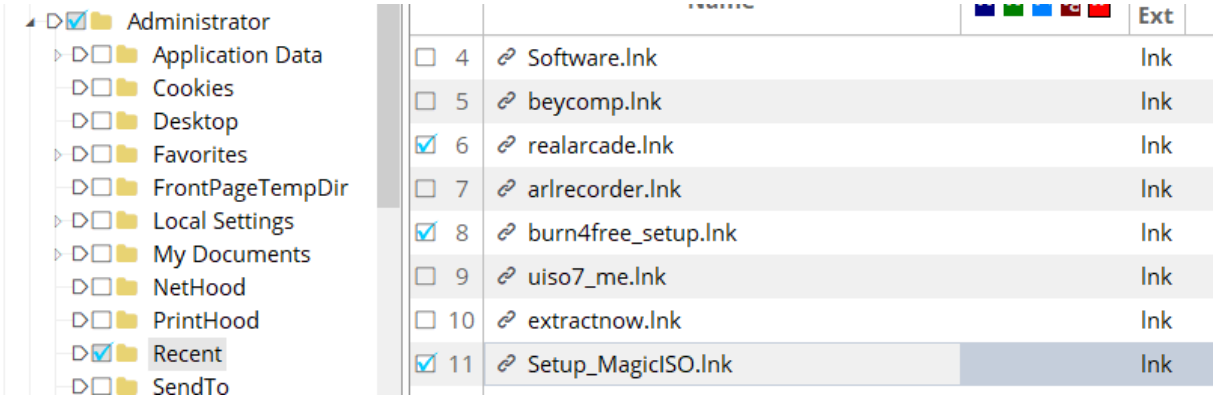


Figure 83: Recent folder program links on Price Software's Server.

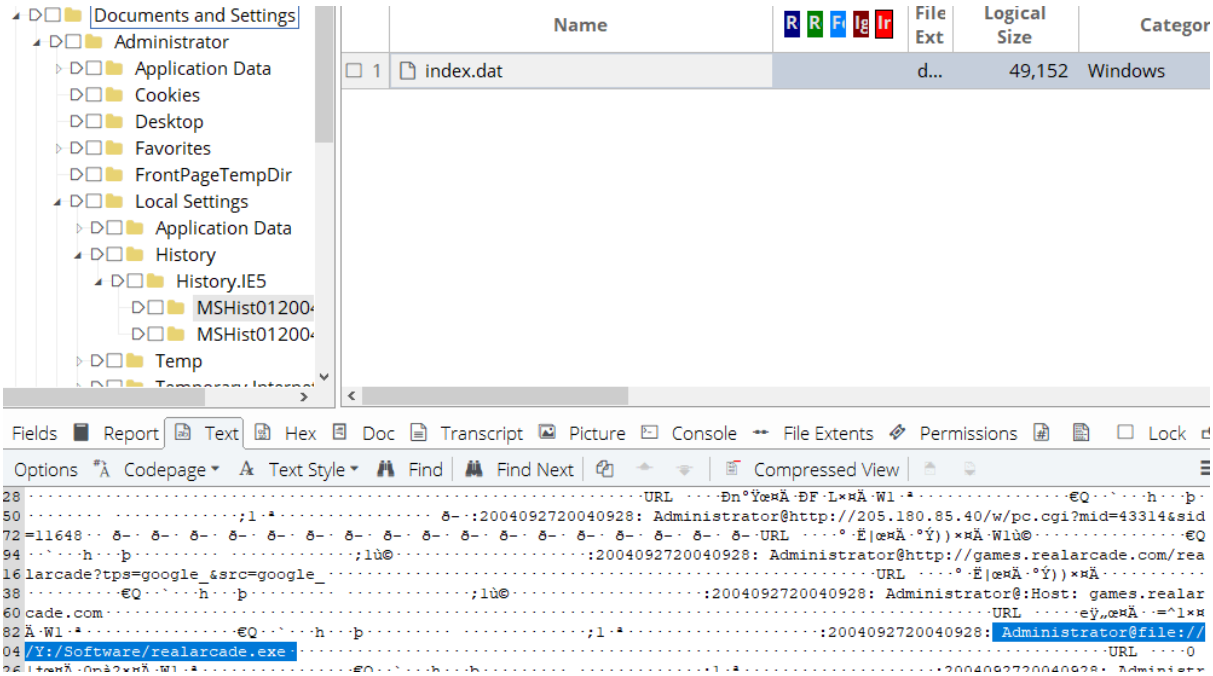


Figure 84: Download of the game program Real Arcade from Internet Explorer history.

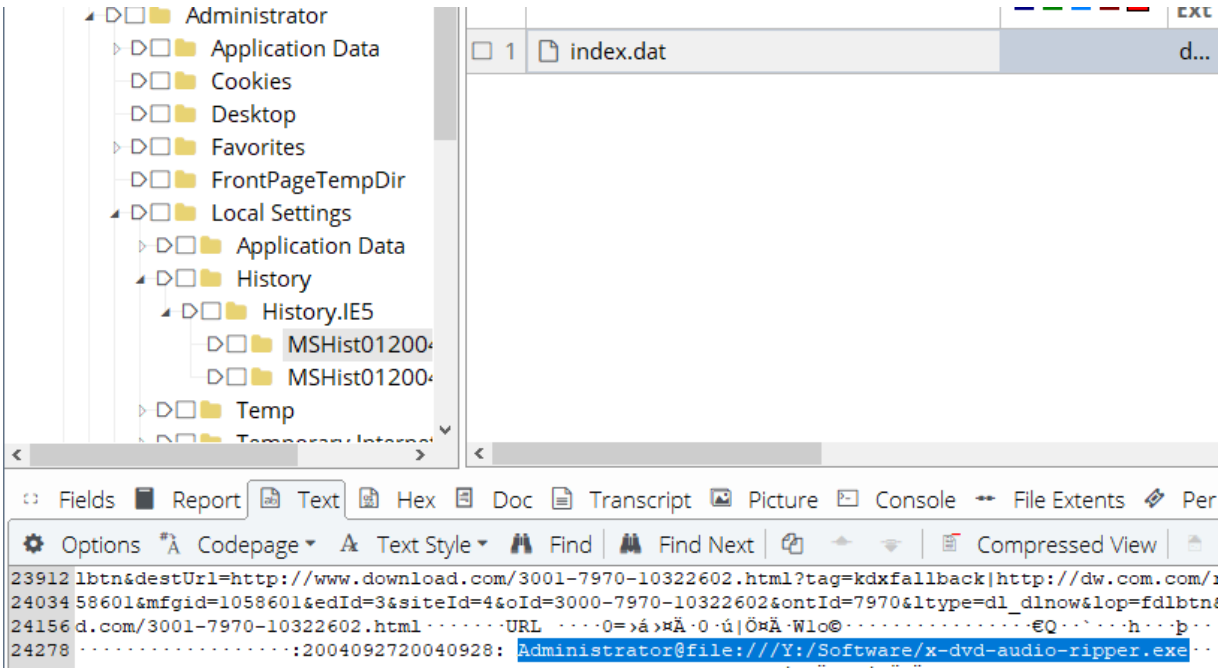
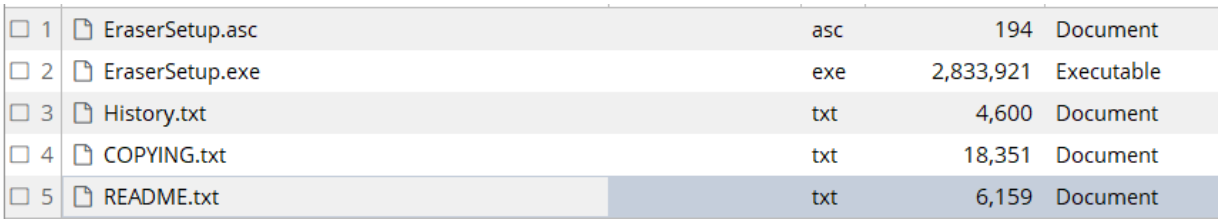


Figure 85: Download of an audio ripper for CDs from Internet Explorer History.

RAID5 Array

In the RAID5 Array that is attached to the company server, there are very few pieces evidence in displaying inappropriate behavior at work.

In the RAID5 Array, there is the file erasing program Eraser's setup which is located in the Software folder. It is inappropriate to have such a potentially dangerous program be accessible to the users. This can be found at "RAID-5 Symmetric\Software\Eraser57Setup\".



1	EraserSetup.asc	asc	194	Document
2	EraserSetup.exe	exe	2,833,921	Executable
3	History.txt	txt	4,600	Document
4	COPYING.txt	txt	18,351	Document
5	README.txt	txt	6,159	Document

Figure 86: Eraser setup found in RAID5 Array in Software folder.

Secondly, there are several executables for programs that are not suitable for the workplace such as a DVD ripper, Real Arcade game player, DVD burner, MagicISO DVD extraction and burning tool, and the Eraser file deletion program. This can be found at “RAID-5 Symmetric\Software\”.

	Name		File Ext	Logical Size	Categ
☑ 3	x-dvd-audio-ripper.exe		exe	1,058,601	Executable
☐ 4	mp3recorder.exe		exe	1,351,514	Executable
☐ 5	beycomp.exe		exe	2,006,440	Executable
☑ 6	realarcade.exe		exe	207,936	Executable
☐ 7	arlrecorder.exe		exe	2,370,536	Executable
☐ 8	uiso7_me.exe		exe	2,140,369	Executable
☑ 9	burn4free_setup.exe		exe	2,249,952	Executable
☐ 10	extractnow.exe		exe	1,228,846	Executable
☑ 11	Setup_MagicISO.EXE		EXE	1,765,022	Executable
☐ 12	ntcdtmc2.exe		exe	2,319,894	Executable
☐ 13	rminstall.exe		exe	2,414,496	Executable
☑ 14	Eraser57Setup.zip		zip	2,811,211	Archive
☐ 15	EZHSDemo.zip		zip	126,625	Archive

Figure 87: Software folder in the RAID5 Array displaying multiple executables.

Chain of Custody

Single Evidence Form

926369300001
Case No. Evidence No.

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 21/02/09 11:23 | Collected by Nick Drenel

Site Address

12345 No place Ave. Someplace, CA 90023

Section C: Evidence Details

Date/Time Stored 2008/22 10:00

Storage Location Price Software Forensic Server

Device Type Hard Drive | Capacity 500 GB

Manufacturer Western Digital | Model WD5000AAKX

Serial No. 61705668

MD5 Sum d9d54d973781b09067eac13798b92bcdf

SHA-1 Sum

Additional Information...

Note any damage, marks and scratches | Digital Image Taken ☑ Yes ☐ No

Section D: Image Details

Date/Time Imaged 02/07/09 17:34 | Imaged by Nick Drenel

Storage Location Price Software Forensics Server

Image Filename PSC Tom WS.E01 | Image Size 500 GB (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- **Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**
- **This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**
- **Further remarks can be noted overleaf in Section E: Remarks**
- **It is important that these forms are kept with the evidence at all times**
- **Upon handover or disposal please complete Section F: Evidence Handover**

Figure 88: Single Evidence Form for "PSC Tom WS.E01".

Chain of Custody Form

for use with a Single Evidence form

Digital Forensics Lab

9	2	6	3	6	9	3	0	0	0	1

Case No. Evidence No.

Page No. 02

This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER Price Software Co.	RECEIVER Price Software Co.
Name: Nick Drenel Signature: ND Evidence Modified: Date & Time: 20/08/22 10:00 Yes / (No)	Name: Scott Inch Signature: SI Date & Time: 20/08/22 11:00
SUBMITTER Price Software Co.	**RECEIVER** Price Software Co.
Name: Scott Inch Signature: SI Evidence Modified: Date & Time: 24/10/22 12:00 Yes / (No)	Name: Aidan Czyrycа Signature: AC Date & Time: 24/10/22 1:00
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: **Date & Time: Yes / No**	Name: Signature: **Date & Time:**
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:

If this form is full please continue on another page

Figure 89: Chain of Custody Form for "PSC Tom WS.E01".

Single Evidence Form

Case No. 9263693 Evidence No. 0002

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 21/07/09 11:23 | Collected by Nick Drenel

Site Address

12345 No place Ave. Someplace, CA 90023

Section C: Evidence Details

Date/Time Stored 20/08/22 10:00

Storage Location Price Software Forensic Server

Device Type Hard Drive | Capacity 500 GB

Manufacturer Western Digital | Model WD5000AAKX

Serial No. 61705569

MD5 Sum 8f6c72fa2e31cfde2296332044d8605

SHA-1 Sum

Additional Information...

Note any damage, marks and scratches

Digital Image Taken ☑ Yes ☐ No

Section D: Image Details

Date/Time Imaged 02/07/09 17:34 | Imaged by Nick Drenel

Storage Location Price Software Forensics Server

Image Filename PSC Leslie WS.E01 | Image Size 500 GB (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- **Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**
- **This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**
- **Further remarks can be noted overleaf in Section E: Remarks**
- **It is important that these forms are kept with the evidence at all times**
- **Upon handover or disposal please complete Section F: Evidence Handover**

Figure 90: Single Evidence Form for "PSC Leslie WS.E01".

Chain of Custody Form

for use with a Single Evidence form

Case No. 926369300002 Evidence No.

Page No. 02

This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER	RECEIVER
Price Software Co.	Price Software Co.
Name: Nick Drenel	Name: Scott Inch
Signature: ND	Signature: SI
Evidence Modified:	
Date & Time: 20/08/22 10:00 Yes / (No)	Date & Time: 20/08/22 11:00
SUBMITTER	**RECEIVER**
Price Software Co.	Price Software Co.
Name: Scott Inch	Name: Aidan Czyrca
Signature: SI	Signature: AC
Evidence Modified:	
Date & Time: 24/10/22 12:00 Yes / (No)	Date & Time: 24/10/22 1:00
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	**Date & Time:**
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:

If this form is full please continue on another page

Figure 91: Chain of Custody Form for "PSC Leslie WS.E01".

Single Evidence Form

Case No. 926369 Evidence No. 3003

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 21/02/09 11:23 | Collected by Nick Drenel

Site Address

12345 No place Ave. Someplace, CA 90023

Section C: Evidence Details

Date/Time Stored 20/08/22 10:00

Storage Location Price Software Forensic Server

Device Type Hard Drive | Capacity 500 GB

Manufacturer Western Digital | Model WD5000AAKX

Serial No. 6170570

MD5 Sum 520ff7fc6977673 0ac11f43adedd0380a7a

SHA-1 Sum

Additional Information...

Note any damage, marks and scratches

Digital Image Taken ☑ Yes ☐ No

Section D: Image Details

Date/Time Imaged 02/07/09 17:34 | Imaged by Nick Drenel

Storage Location Price Software Forensics Server

Image Filename PSCserver OS.E01 | Image Size 500 GB (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- **Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**
- **This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**
- **Further remarks can be noted overleaf in Section E: Remarks**
- **It is important that these forms are kept with the evidence at all times**
- **Upon handover or disposal please complete Section F: Evidence Handover**

Figure 92: Single Evidence Form for "PSC Server OS.E01".

Chain of Custody Form

for use with a Single Evidence form

Digital Forensics Lab

9	2	6	3	6	9	3	0	0	0	3

Case No. Evidence No.

Page No. 02

This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER	RECEIVER
Price Software Co.	Price Software Co.
Name: Nick Drenel	Name: Scott Inch
Signature: ND	Signature: SI
Evidence Modified:	
Date & Time: 20/08/22 10:00 Yes / (No)	Date & Time: 20/08/22 11:00
SUBMITTER	**RECEIVER**
Price Software Co.	Price Software Co.
Name: Scott Inch	Name: Aidan Czyrca
Signature: SI	Signature: AC
Evidence Modified:	
Date & Time: 24/10/22 12:00 Yes / (No)	Date & Time: 24/10/22 1:00
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	**Date & Time:**
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:

If this form is full please continue on another page

Figure 93: Chain of Custody Form for "PSC Server OS.E01".

Single Evidence Form

Case No. 926369 Evidence No. 0004

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 21/02/09 11:23 | Collected by Nick Drenel

Site Address

12345 No place Ave. Someplace, CA 90023

Section C: Evidence Details

Date/Time Stored 20/08/22 10:00

Storage Location Price Software Forensic Server

Device Type Hard Drive | Capacity 500 GB

Manufacturer Western Digital | Model WD5000AAKX

Serial No. 6170571

MD5 Sum d3281d25f1e68e8ecb1a3eba58e3766a6

SHA-1 Sum

Additional Information...

Note any damage, marks and scratches

Digital Image Taken ☑ Yes ☐ No

Section D: Image Details

Date/Time Imaged 02/07/09 17:34 | Imaged by Nick Drenel

Storage Location Price Software Forensics Server

Image Filename RAID-5 Symmetric.E01 | Image Size 500 GB (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- **Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**
- **This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**
- **Further remarks can be noted overleaf in Section E: Remarks**
- **It is important that these forms are kept with the evidence at all times**
- **Upon handover or disposal please complete Section F: Evidence Handover**

Figure 94: Single Evidence Form for "RAID 5-1".

Chain of Custody Form

for use with a Single Evidence form

Digital Forensics Lab

9	2	6	3	6	9	3	0	0	0	4

Case No. Evidence No.

Page No. 02

This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER	RECEIVER
Price Software Co.	Price Software Co.
Name: Nick Drenel	Name: Scott Inch
Signature: ND	Signature: SI
Evidence Modified:	
Date & Time: 20/08/22 10:00 Yes / (No)	Date & Time: 20/08/22 11:00
SUBMITTER	**RECEIVER**
Price Software Co.	Price Software Co.
Name: Scott Inch	Name: Aidan Czyrnca
Signature: SI	Signature: AC
Evidence Modified:	
Date & Time: 24/10/22 12:00 Yes / (No)	Date & Time: 24/10/22 1:00
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	**Date & Time:**
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:

If this form is full please continue on another page

Figure 95: Chain of Custody Form for "RAID 5-1".

Single Evidence Form

Case No. 926369 Evidence No. 0005

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 21/02/09 11:23 | Collected by Nick Drenel

Site Address

12345 No place Ave. Someplace, CA 90023

Section C: Evidence Details

Date/Time Stored 20/08/22 10:00

Storage Location Price Software Forensic Server

Device Type Hard Drive | Capacity 500 GB

Manufacturer Western Digital | Model WD5000AAKX

Serial No. 6170572

MD5 Sum 2cb2bd1c1e1a6e28afadb0f273f80331bb

SHA-1 Sum

Additional Information...

Note any damage, marks and scratches

Digital Image Taken ☑ Yes ☐ No

Section D: Image Details

Date/Time Imaged 02/07/09 17:34 | Imaged by Nick Drenel

Storage Location Price Software Forensics Server

Image Filename RAID-5 Symmetric.E01 | Image Size 500 GB (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- **Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**
- **This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**
- **Further remarks can be noted overleaf in Section E: Remarks**
- **It is important that these forms are kept with the evidence at all times**
- **Upon handover or disposal please complete Section F: Evidence Handover**

Figure 96: Single Evidence Form for "RAID 5-2".

Chain of Custody Form

for use with a Single Evidence form

Digital Forensics Lab

9	2	6	3	6	9	3	0	0	0	5

Case No. Evidence No.

Page No. 02

This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER	RECEIVER
Price Software Co.	Price Software Co.
Name: Nick Drenel	Name: Scott Inch
Signature: ND	Signature: SI
Evidence Modified:	
Date & Time: 20/08/22 10:00 Yes / (No)	Date & Time: 20/08/22 11:00
SUBMITTER	**RECEIVER**
Price Software Co.	Price Software Co.
Name: Scott Inch	Name: Aidan Czyrycа
Signature: SI	Signature: AC
Evidence Modified:	
Date & Time: 24/10/22 12:00 Yes / (No)	Date & Time: 24/10/22 1:00
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: **Yes / No**	**Date & Time:**
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:

If this form is full please continue on another page

Figure 97: Chain of Custody Form for "RAID 5-2".

Single Evidence Form

Case No. 9263693 Evidence No. 0006

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 21/02/09 11:23 | Collected by Nick Drenel

Site Address

12345 No place Ave. Someplace, CA 90023

Section C: Evidence Details

Date/Time Stored 20/08/22 10:00

Storage Location Price Software Forensic Server

Device Type Hard Drive | Capacity 500 GB

Manufacturer Western Digital | Model WD5000AAKX

Serial No. 6170573

MD5 Sum bdbb14a82462f8800cd80cdd47790df

SHA-1 Sum

Additional Information...

Note any damage, marks and scratches | Digital Image Taken ☑ Yes ☐ No

Section D: Image Details

Date/Time Imaged 02/07/09 17:34 | Imaged by Nick Drenel

Storage Location Price Software Forensics Server

Image Filename RAID-5 Symmetric.E01 | Image Size 500 GB (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- **Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**
- **This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**
- **Further remarks can be noted overleaf in Section E: Remarks**
- **It is important that these forms are kept with the evidence at all times**
- **Upon handover or disposal please complete Section F: Evidence Handover**

Figure 98: Single Evidence Form for "RAID 5-3".

Chain of Custody Form

for use with a Single Evidence form

Digital Forensics Lab

9	2	6	3	6	9	3	0	0	0	6

Case No. Evidence No.

Page No. 02

This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER Price Software Co.	RECEIVER Price Software Co.
Name: Nick Drenel	Name: Scott Inch
Signature: ND	Signature: SI
Evidence Modified:	
Date & Time: 20/08/22 10:00 Yes / (No)	Date & Time: 20/08/22 11:00
SUBMITTER Price Software Co.	**RECEIVER** Price Software Co.
Name: Scott Inch	Name: Aidan Czyrycа
Signature: SI	Signature: AC
Evidence Modified:	
Date & Time: 24/10/22 12:00 Yes / (No)	Date & Time: 24/10/22 1:00
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	**Date & Time:**
SUBMITTER	**RECEIVER**
Name:	Name:
Signature:	Signature:
Evidence Modified:	
Date & Time: Yes / No	Date & Time:

If this form is full please continue on another page

Figure 99: Chain of Custody Form for "RAID 5-3".

Conclusion

In this examination, the six forensic images provided for analysis contain sufficient information to support violations of workplace integrity from Mr. Warner and a relationship inappropriate for the workplace environment from Mr. Warner and Ms. Stowle.

Several pieces of evidence were obtained from Mr. Warner's workstation demonstrating both violations of workplace integrity and of inappropriate workplace behavior. In reference to the violations of workplace integrity, Mr. Warner's workstation provided evidence of having file and hard drive erasing programs (such as Darik's Boot and Nuke, and Eraser), an email of intent on revenge towards the company, removable media with CD burner programs, a file encrypting protocol, and easy access to sensitve company documents. As for the inappropriate workplace behavior, Mr. Warner appears to show inappropriate behavior at work by wasting company time with MSN Gaming Zone, Windows Pinball, and inappropriate internet browsing. Secondly, by having an inappropriate workplace relationship with Ms. Stowle as seen through multiple email exchanges between Mr. Warner and Ms. Stowle where the two schedule regular lunches and dinners together and have planned a vacation together.

Several pieces of evidence were obtained from Ms. Stowle's workstation demonstrating both violations of workplace integrity and of inappropriate workplace behavior. In reference to the violations of workplace integrity, Ms. Stowle's workstation provided evidence of having hard drive erasing programs (Darik's Boot and Nuke) and installation of a CD burner programs.

As for the inappropriate workplace behavior, Ms. Stowle appears to show inappropriate behavior at work by having MSN Gaming Zone, Windows Pinball, and inappropriate internet browsing. Secondly, by having an inappropriate workplace relationship with Mr. Warner as seen through multiple email exchanges between Mr. Warner and Ms. Stowle where they schedule regular lunches and dinners together and have planned a vacation together.

References

Exhibit A

The meta carving, data carving, and indexing for all four forensic images failed. They repeated through several errors and crashed the software as well as the VM multiple times. Many different combinations of options were tried but the most processing able to finish was file sorting. No concrete theory on why it failed so badly was solidified.

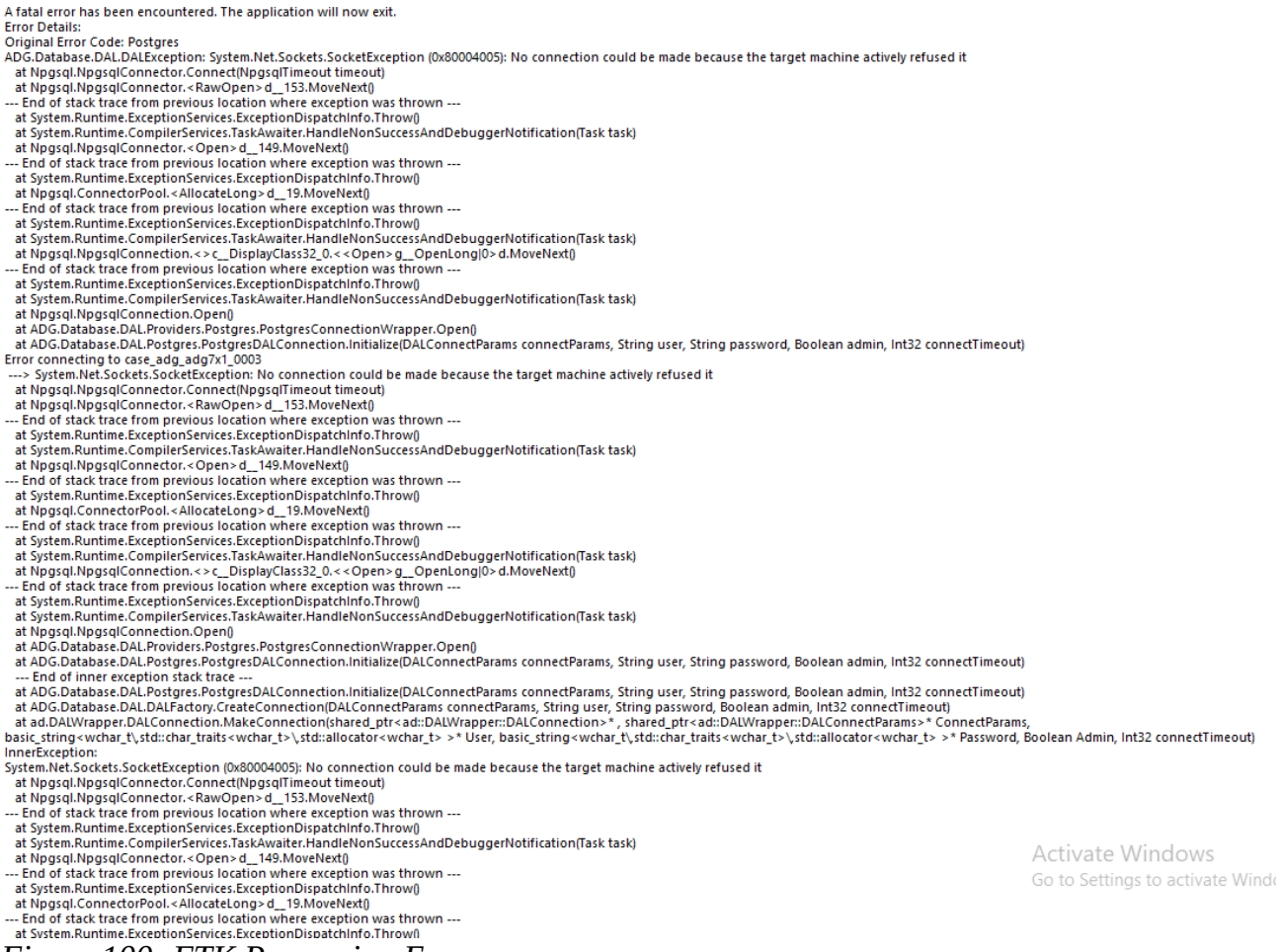


Figure 100: FTK Processing Error.

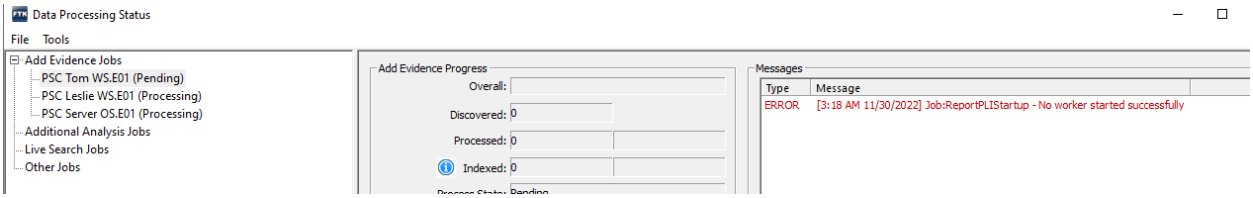


Figure 101: FTK Failure to begin processing "PSC Tom WS.E01".

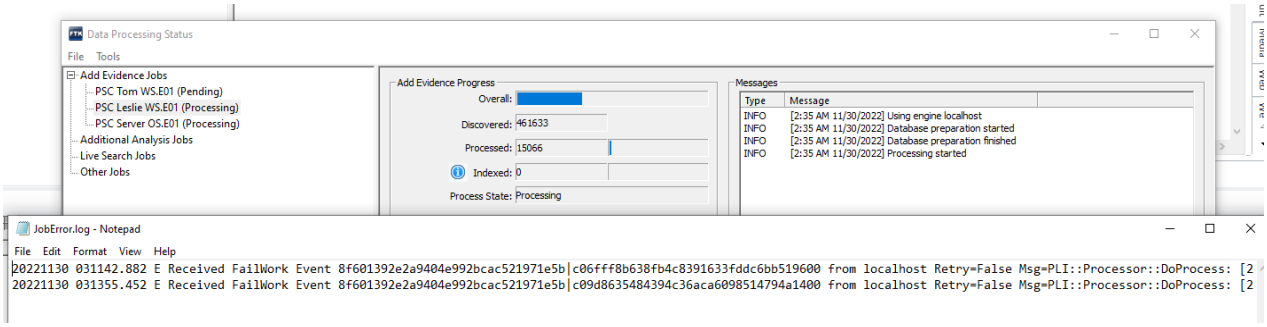


Figure 102: FTK Errors for "PSC Leslie WS.E01".

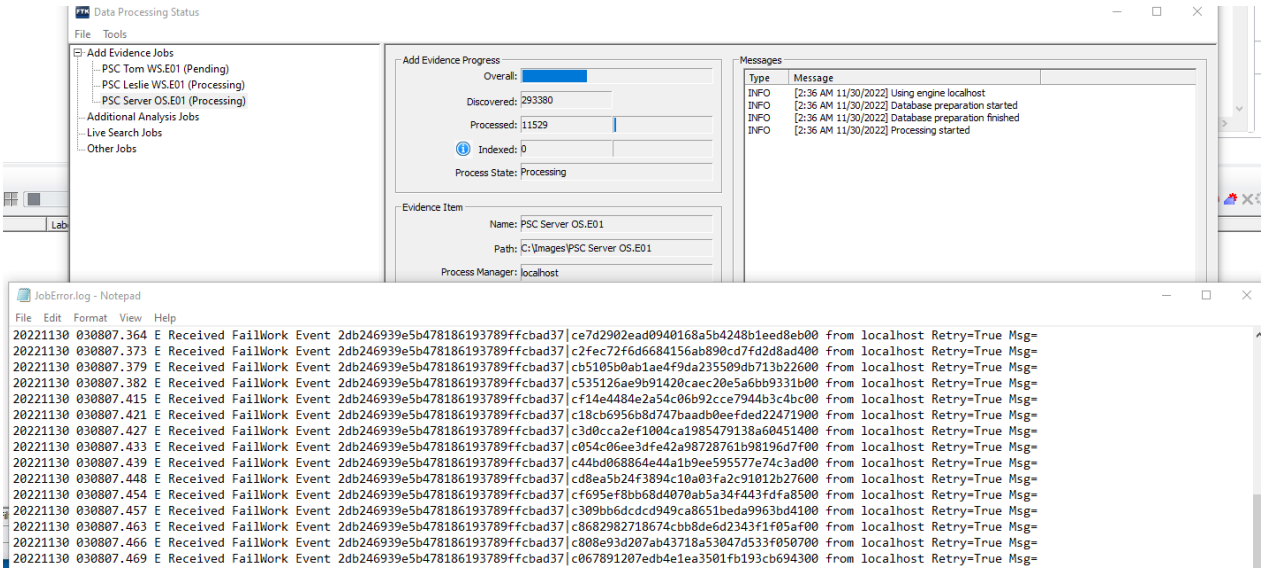


Figure 103: FTK Errors for "PSC Server OS.E01".

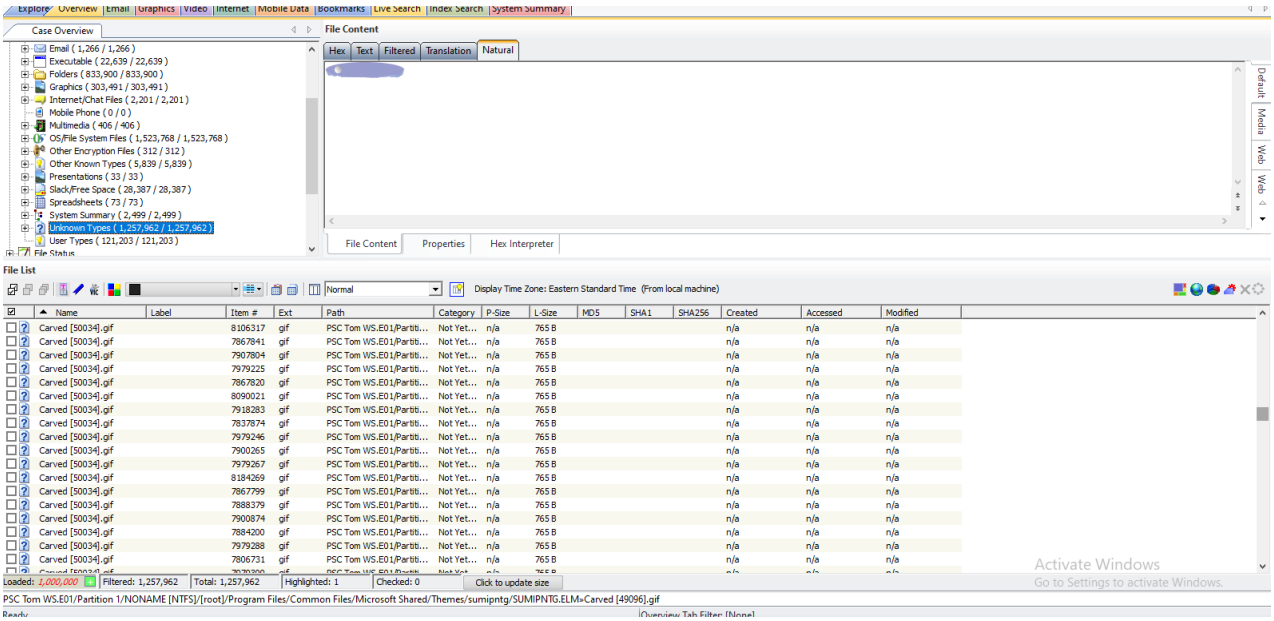


Figure 104: Example of numerous duplications for files in "PSC Tom WS.E01".

Exhibit B

On Ms. Stowle's workstation, Internet history evidence reveals various travel related images.

Figure 105: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 106: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 107: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 108: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 109: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 110: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 111: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 112: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 113: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 114: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 115: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 116: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 117: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 118: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 119: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 120: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 121: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 122: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 123: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 124: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 125: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 126: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 127: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 128: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 129: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 130: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 131: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 132: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 133: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 134: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 135: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 136: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

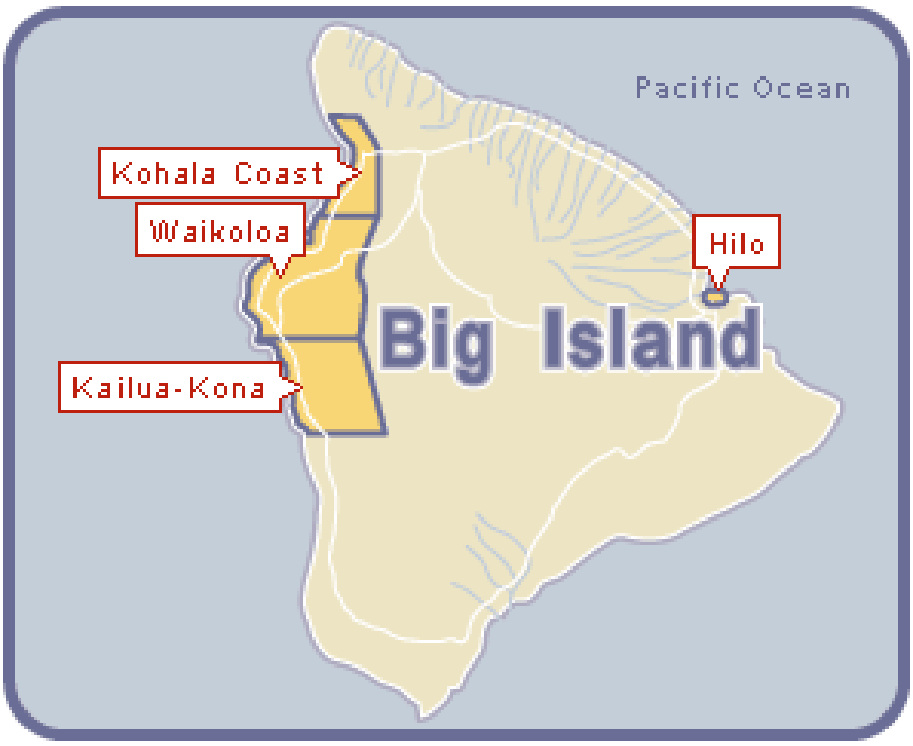


Figure 137: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

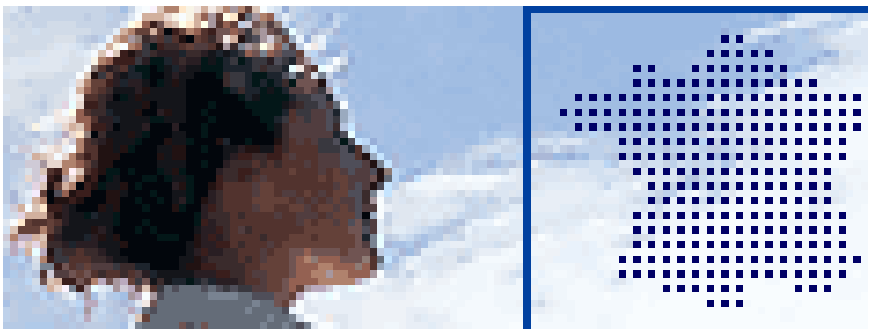


Figure 138: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 139: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 140: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

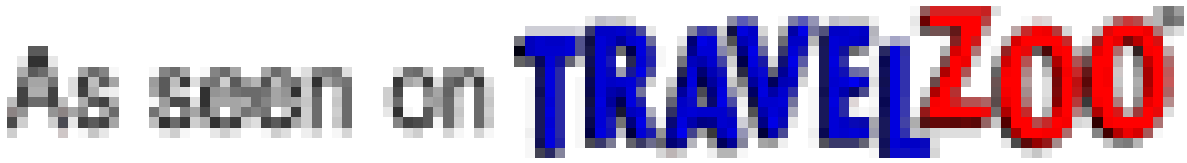


Figure 141: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 142: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 143: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 144: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 145: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 146: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 147: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 148: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 149: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 150: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

vacation.com™

Figure 151: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 152: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 153: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 154: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

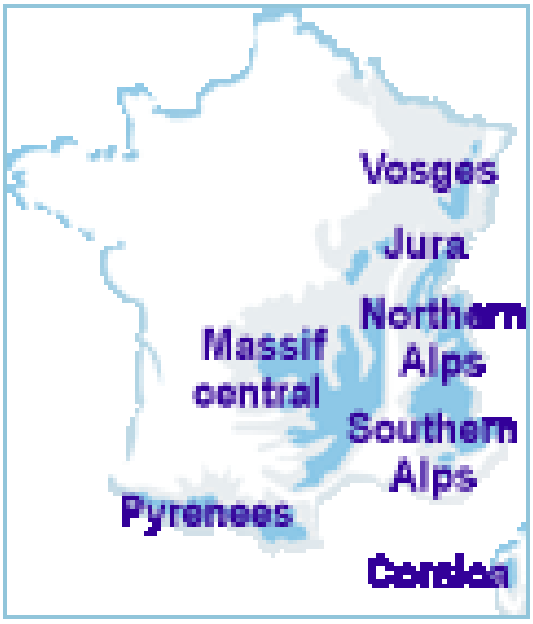


Figure 155: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

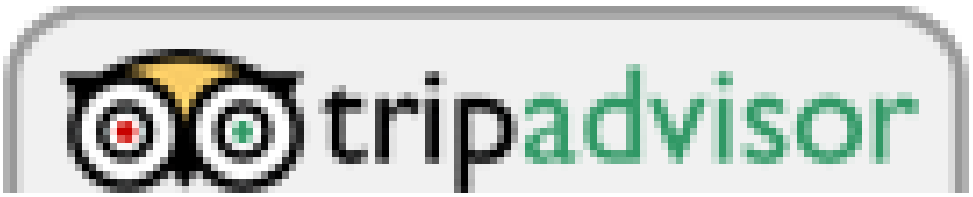


Figure 156: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 157: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

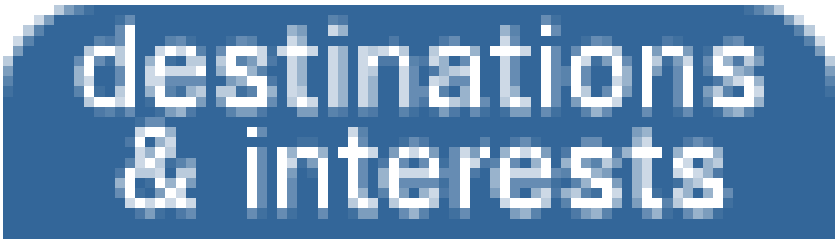


Figure 158: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 159: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 160: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 161: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

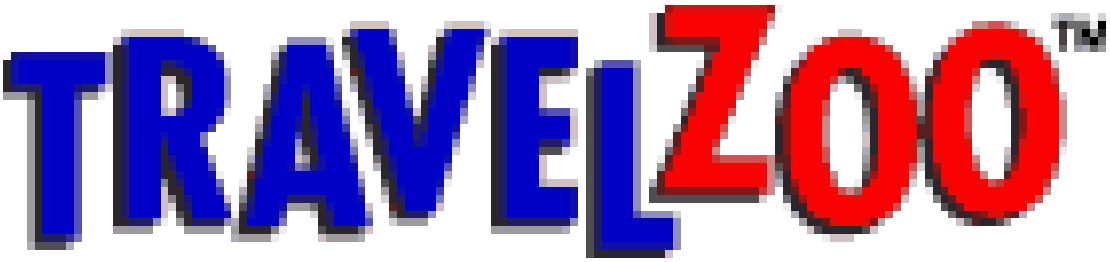


Figure 162: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".

Figure 163: Image relating to travel found in the temporary internetfile from "PSC Leslie WS.E01".