

Fisher Case File

Lead Black Mesa Investigator: Colin Van Alstine

Comment [DW1]: Ouch, I think you got him. Good write up on this case. I want to use it as an example in the future if I have your permission. I will be happy to leave your name on or off as you wish. Some minor problems and overstatements but you did an outstanding job of digging through the files and toasting the guy. Try and transfer more of that information into your summation to make it more thorough. 100.

**Confidential Material Contained Within
Employees and Sworn Officials ONLY
Property of Black Mesa Research Facility**

SUMMATION: 3
ANALYSIS: 3
PHYSICAL EVIDENCE: 3
DATA EVIDENCE: 4

 INCONCLUSIVE FILES: 4
 JPEG_9879438[71304].jpg: 4
 SIGNIFICANT HARASSMENT FILES: 4
 Compose[2].htm: 4
 Yellowtail02[1].JPG: 4
 Dc1.JPG: 5
 INFO2: 5
 Investigation.eml: 5
 SUPPORTING HARASSMENT FILES: 5
 CAIUIKV4.htm: 5
 Compose[1].htm, Compose[2].htm, Compose[5].htm, Compose[6].htm, Untitled0: 6
 id_check[1].htm: 6
 Message0001: 6
 Message0001: 6
 Message0002: 6
 Message0002: 6
 SIGNIFICANT ILLEGAL FILES: 6
 559834046[1].jpg, 684392941.jpg, 710380003.jpg, 859614749.jpg: 6
 Compose[3].htm: 7
 Compose[4].htm: 7
 Compose[5].htm: 7
 doug.white.vcf: 7
 fate_50x50[1].jpg, merlot_chardonny[1].jpg, neko[1].jpg, ray_pugsley_mewmew[1].jpg: 7
 ShowFolder[1].htm, ShowFolder[2].htm, ShowFolder[3].htm: 8
 ShowLetter[1].htm: 8
 thalia[1].jpg: 8
 SUPPORTING ILLEGAL FILES: 8
 CAIUIKV4, id_check[1].htm: 8
 Compose[3].htm, Compose[7].htm, Untitled0: 8
 Appendices: 9
 Glossary of Terms: 9
 Common Business Practices: 9
 FTK Report: 9

Summation:

After reviewing the files contained on the hard drive brought to us by the Bank Of Edison we found that not only was David Fisher responsible for the online harassment of fellow coworker Gloria Costa, but he also was engaging in the sharing of illegal child pornography at the workplace. Email files were found on his hard drive that show that David Fisher owned the account bigd2466@yahoo.com that was used to email a pornographic image that resembled himself to Ms. Costa. This same email account was used to make contact with Doug White and for the trading of known child pornography through email with this Doug White. Upon finding these illegal pornographic images the authorities were contacted and a full investigation of David Fisher, separate from the harassment case, will soon commence. In addition to the illegal pornography, a large amount of legal pornographic images were found on the hard drive, calling into doubt the validity of Mr. Fisher's wrongful termination suit. In short, there was evidence found on Mr. Fisher's computer in the form of emails and images that shows that Mr. Fisher was engaging in non-work related activities prohibited by the company policy, that Mr. Fisher was responsible for the email harassment of Ms. Costa, and that Mr. Fisher owns several known illegal pornographic images of children.

Comment [DW2]: Eek, you just claimed you held the trial. You can't say things like this. Just present the facts. You can have an expert opinion on the facts but that is all.

Comment [DW3]: How do you prove this??

Comment [DW4]: Never include information about other cases you have not been asked to examine. You have no knowledge of any other charges and if an officer of the court revealed such information to you they would have just endangered their case.

Comment [DW5]: You need to mention that you reported the illegal images to the proper authorities.

Analysis:

Physical Evidence:

First Municipal Trust Bank of Edison contacted Black Mesa Research Facility on the 1st of September, 2005 and Black Mesa was hired to investigate this case of harassment. The only recovered media in the case was the work computer belonging to the man suing the Bank of Edison, David Fisher. The hard drive was manufactured by Sea Gate and is the 10GB model with the product number ST310014ACE. There were no unique identifying marks found on the outside of this drive. The hard drive was brought to Black Mesa Research Facility by corporate security where it was logged as evidence. The drive was immediately placed within a secure storage closet and signed in by the security officer. The disk was removed from the storage closet for investigation by Black Mesa on the 4th of September, 2005. A DOD wiped hard drive of comparable size was removed from storage and images of the original media were created both on the new drive and the computer assembled and maintained solely for computer forensics work (as detailed in our company policy). The images were created using a Forensics Examination Toolkit and the MD5 hashes of the images were compared and deemed identical to the original medium. After the creation and comparison of the images, the original hard drive and the newly created copy were placed back into the security closet and signed in. The rest of Black Mesa's examination would be conducted using a licensed copy of Access Data Forensics Toolkit.

Comment [DW6]: One word.

Comment [DW7]: It should have been logged as evidence when you got it not when it was returned to your offices. You need to have a chain of custody document and appendix explaining your approach. This just caused a problem with your case.

Comment [DW8]: It's nice to refer to the appendix.

Data Evidence:

Inconclusive Files:

With a media source as large as a hard drive from a computer at a place of work, there were quite a few files that could be discarded as irrelevant to this case. Also, since this is a bootable drive and not just a storage medium, there were many files belonging to applications that were not suspect (Open Office and Microsoft Frontpage for example). For the most part, the files under the 'Program Files' and 'Windows' folder hierarchies were rather benign, with all of the relevant files coming from the 'Temporary Internet Files' folders in the 'Documents and Settings' folder hierarchy or from the 'Recycling Bin'. Another interesting fact that should be mentioned before any of the specific files are analyzed is that FTK has reported a bad cluster of data on the drive. This appears to have not corrupted any of the files found on the drive, but there has been damage done to this drive and the IT department at the Bank of Edison does not know how this occurred.

Comment [DW9]: You just don't really need this. If they are inconclusive or irrelevant, just skip it. Just make sure they are really irrelevant.

JPEG_9879438[71304].jpg:

This file is but one of many such pornographic files found on this hard drive. Using data carving to restore the information saved in hidden parts of the drive, a great deal of image files were recovered, most of them pornographic in nature. While not illegal for a man of David Fisher's age, these files were certainly prohibited by the Code of Conduct agreements that he signed while being hired into his position and they are inappropriate for viewing in the workplace. They also establish the veracity of the statements made by the Bank of Edison; there were pornographic images on Mr. Fisher's computer and they potentially could have been used to decorate his desktop, causing this entire incident to be started.

Significant Harassment Files:

Compose[2].htm:

This file is a hypertext page made by a server-side email provider, in this case, Yahoo Mail, which was automatically stored into the 'Temporary Internet Files' folder on Mr. Fisher's computer. This page is identical to the one that Ms. Costa received after Mr. Fisher was made to apologize to her for following Ms. Costa into the restroom. Attached to the email is an image titled Yellowtail02.jpg which will be discussed momentarily. There is no evidence found inside this email that would point to Mr. Fisher being responsible for creating and sending this email to Ms. Costa. All we can be sure about from this file is that the inappropriate email originated from this machine and that the user bigd2466@yahoo.com was responsible for sending it.

Comment [DW10]: Good.

Yellowtail02[1].JPG:

This is the file of the unidentified nude man cropped above the shoulders that was connected to the harassing email as an attachment. The IT department of the Bank of Edison had previously determined that the picture was not sent though email, but was instead placed on a public network drive within the company and then linked to the email that was sent to Ms. Costa. This is the file that was found on the public network drive, and again there is no evidence found that would directly place this file as the property of

Comment [DW11]: What? How was this determined.

Mr. Fisher, but it is true that it was found upon his hard drive and it was connected to an email sent from the yahoo account of bigd2466.

Dc1.JPG:

This is the same image as the Yellowtail02[1].JPG that was previously analyzed, but it's location was in the Recycling Bin on the computer. The file was automatically renamed Dc1.jpg upon being placed into the folder. For the purposes of this case, this image is identical in all but location to Yellowtail02[1].JPG.

INFO2:

This is the Recycling Bin information file that holds the previous location of all the files currently in the Recycling Bin. This is used by Windows to restore files when the user decides not to remove them from their computer. The information found in this file confirms that the image Dc1.JPG is the same as Yellowtail02[1].JPG and it includes a date and time as to when the user decided that they wanted to remove Yellowtail02[1].JPG from their computer. The image was still in the Recycling Bin slated to be deleted the next time the user confirmed that they wished all the files in the Bin to be deleted.

Investigation.eml:

Investigation.eml is an email file found in a folder named Legal on Mr. Fisher's computer. It appears that the First Municipal Trust Bank of Edison had previously contacted a security firm to investigate Mr. Fisher on the behalf of Ms. Costa's hostile workplace suit. Mr. Fisher saved the email that this firm, Secure Technologies LLC, to his hard drive. This normally would not be a noteworthy file to investigate, Black Mesa sent out their own notifications to the involved parties before this investigation was undertaken, but the name of the lead investigator is shocking. Doug White originally contacted Mr. Fisher on the behalf of Secure Technologies and as our investigation of the known child pornography files was developed, the name of the other individual with whom Mr. Fisher was trading the illegal files with was Doug White. The police investigation into Mr. Fisher for the disseminating of known child pornography will uncover the identity of his cohort, but it is a shock to see the suspected name of a child pornography peddler in an email from an information security **company**.

Comment [DW12]: Well, be careful, there are a lot of people named Doug White. In fact, there were two Doug Whites and a David White at my high school. But, you are right there is something fishy here (No Pun Intended).

Supporting Harassment Files:

CAIUIKV4.htm:

This file is another hypertext file that was created by Yahoo Mail and then stored on to the hard drive. This hypertext deals with a user that was registered using this computer. The user name selected was bigd2466@yahoo.com and this file stored personal information about the user to be used if a password ever needed to be retrieved. This personal information includes an area code (80634), a birthday (March 3rd, 1970), and the name of a pet (mrcat). This information might give us a better understanding of who created this email account, assuming that it is all **true**.

Comment [DW13]: Outstanding. You really hurt him with this one. You don't know it but Fisher's birthday is March 3rd, 1970. I don't think anyone else so far has found this file. This desperately needs to find its way to your summation.

Compose[1].htm, Compose[2].htm, Compose[5].htm, Compose[6].htm, Untitled0:

These are basic hypertext files that are confirming that an unknown message has been sent to Ms. Costa's email address from this Yahoo Account. It establishes that bigd2466@yahoo.com has been in contact with Ms. Costa on numerous occasions.

id_check[1].htm:

Here we have another hypertext file that is related to the registration of the user name bigd2446 with Yahoo Mail. This page simply states that the desired user name is available if the user wants to continue registering for the email account with this name. The file's existence on this computer shows that not only was the account accessed from Mr. Fisher's computer, but it also was created on his machine and had information saved on this hard drive.

Message0001:

This reply email is rather odd considering the lack of surprise that Mr. Fisher is expressing after seeing an email arrive from a security firm that will be investigating him for a hostile workplace suit and undoubtedly recognizing the name of the sender. The contents of this email are rather mundane and involve legal power plays, and the only thing of note is that the conversation stays on legal topics even though the investigator from Secure Technologies has the same name and address as the person with whom Fisher is trading known child pornography.

Message0001:

This is another email file that involves David Fisher approaching a fellow coworker. He appears to have affections for a Brenda Bridgeman and has been sending anonymous gifts to her for some time. While not directly related to the case of harassment, it does show his preference to remain hidden while dealing with his emotions. It does speak in his favor, and possibly against his character, when he offers to leave Ms. Bridgeman alone if she does not desire his affections. This email was deleted.

Comment [DW14]: This needs to get in your summation.

Message0002:

This is an email version of the file found in the Legal folder on Mr. Fisher's hard drive. The file that this email is related to is Investigation.eml and can be found under the Significant Harassment Files section of this report.

Message0002:

This file mirrors the other email file that was sent to Ms. Bridgeman regarding Mr. Fisher's interest in her. This version seems to have been reduced in length and does not have line spacing found in the top portion of the deleted version.

Significant Illegal Files:

559834046[1].jpg, 684392941.jpg, 710380003.jpg, 859614749.jpg:

These are image files that depict sexual relations between a minors and adults. These files and all their iterations have all been positively identified as illegal images of child pornography by the National Center for Missing and Exploited Children. These

images were found within the 'Temporary Internet Files' folder, signifying that they had been downloaded and viewed **recently**.

Comment [DW15]: Be sure and include your Authorities were notified and permission to proceed was obtained here.

Compose[3].htm:

This hypertext file is a snapshot of an email written to Doug White by Mr. Fisher on the Yahoo Mail account suspected of being used to harass Ms. Costa. It also appears from this email that Mr. Fisher was soliciting pornographic images from other individuals over the internet. This particular email looks to be the start of one such online relationship in which Mr. Fisher asks what type of images Mr. White would like to exchange. Mr. White responded using a metaphor commonly found in email pornography trading rings that he would be most interested in trading child pornography.

Compose[4].htm:

This is a follow up to the email found in file Compose[3].htm. The relationship between Mr. Fisher and Mr. White has developed and they have supposedly started to exchange images. Mr. Fisher expressed an interest in the child pornography that Mr. White offered and Mr. White implies through the text of his response email that he has attached images for Mr. Fisher to view. This cannot be confirmed because the snapshot that the computer saved was only of the text and not the rest of the email.

Compose[5].htm:

The conversation between Mr. Fisher and Mr. White continues in this hypertext file. In this particular email Mr. Fisher has responded by saying that he has received several images from Mr. White and that while "some of those" (the individuals in the photos are assumed to be the subject of the sentence) were too young for his tastes, he did enjoy a file with an image of one Thalia. An image of illegal pornography was found with the filename of thalia[1].jpg and it is assumed that the name mentioned in the email and this file are one and the same. This file also shows that Mr. Fisher had attached a file to the response that he was writing and was planning on completing the exchange by sending an image file. The file attached, dog3.jpg, was found on the hard drive and it is a legal pornographic image.

doug.white.vcf:

This file is of the vCard type and it containing various personal details and can be attached to an email. This enables the transmission of selected information without retyping it each time a message is sent. In this specific case, the information found within pertains to Mr. White. This information has no impact on the case of harassment, but it will be useful in the impending investigation of the known child pornography found on Mr. Fisher's **computer**.

Comment [DW16]: Awesome.

fate_50x50[1].jpg, merlot_chardonny[1].jpg, neko[1].jpg, ray_pugsley_mewmew[1].jpg:

These are image files containing known child pornography. These files and all their iterations have all been positively identified as illegal images of child pornography by the National Center for Missing and Exploited Children. These images were found within the 'Temporary Internet Files' folder, signifying that they had been downloaded and viewed recently.

Comment [DW17]: Again, on the notification thing.

ShowFolder[1].htm, ShowFolder[2].htm, ShowFolder[3].htm:

These three hypertext files are again snapshots of the Yahoo Mail account that was used for the harassment of Ms. Costa and for the exchange of pornographic images with Mr. White. The folder shown is the 'Inbox' which is used by the email provider to sort mail that has been received by the user. These files show the Inbox in a different state each time as Mr. Fisher has received more email from Mr. White. There is progressively more mail stored here as their relationship develops. The dates and file sizes are particularly interesting as the dates provide a time line and the file sizes will tell if there is a possibility of an image file being attached to the email.

ShowLetter[1].htm:

There are three distinct hypertext files that have been assigned this same name. The first of these files is an email with the text contents having been previously removed, and it is a text-free shell of the first email sent from Mr. White to Mr. Fisher. The second file is a snapshot of the Yahoo Mail client's anti-virus screening procedure. Yahoo Mail scans an attachment for common viruses before you are allowed to open it and view the contents. The attachment being scanned is the known child pornographic image named thalia[1].jpg. The analysis of the image found no viruses and helpfully displayed the file type (image/jpeg) and the size of the file (11kb). This removes any doubts about Mr. Fisher and Mr. White; a known pornographic image of a child was received from Mr. White by Mr. Fisher and was downloaded and viewed by Mr. Fisher. Mr. Fisher thanked Mr. White for the image in a following email response. The third file that shares this name is just as inconsequential as the first file, and only documents the conversations between Mr. White and Mr. Fisher.

Comment [DW18]: What do you think, is he going down or what? I think you nailed him with this.

thalia[1].jpg:

This is the known image of child pornography that we have evidence of Mr. White and Mr. Fisher exchanging, downloading, viewing, and discussing. This file has positively identified as an illegal image of a child by the National Center for Missing and Exploited Children.

Supporting Illegal Files:

CAIUIKV4, id_check[1].htm:

These files were previously reviewed and the original analysis of the files can be found above under the section titled Supporting Harassment Files. The files were included again in this section because it is important to establish the identity of the owner of the bigd2446@yahoo.com account in regards to the illegal files as well as the files related to the harassment of Ms. Costa. The information found within these files is personal and specific and is helpful in establishing the identity of the user.

Compose[3].htm, Compose[7].htm, Untitled0:

These are basic hypertext files that are confirming that an unknown message or reply has been sent to Mr. White from this Yahoo Account. It establishes that the emails that we have found written by bigd2466@yahoo.com were actually sent to Mr. White.

Appendices:

Glossary of Terms



Glossary Of Terms

Common Business Practices:



Common Practices

FTK Report:

Case Information

12/11/2005

FTK Version	Version 1.60, build 05.06.30
Case Number	2005004
Forensic Examiner	Colin Van Alstine
Agency	Black Mesa Research Facility

File Overview

12/11/2005

Evidence Items

Evidence Items: 2

File Items

Total File Items: 81,906
Flagged Thumbnails: 0
Other Thumbnails: 20,149

File Status

KFF Alert Files: 0
Bookmarked Items: 51
Bad Extension: 11,392
Encrypted Files: 0
From E-mail: 202
Deleted Files: 5,732
From Recycle Bin: 2
Duplicate Items: 47,630
OLE Subitems: 433

Flagged Ignore: 1
KFF Ignorable: 9,362

File Category

Documents: 14,339
Spreadsheets: 14
Databases: 7
Graphics: 20,149
E-mail Messages: 77
Executables: 8,999
Archives: 2,278
Folders: 1,285
Slack/Free Space: 11,048
Other Known Type: 1,793
Unknown Type: 21,917

Evidence List

12/11/2005

Display Name: fisher\Part_1\NONAME-NTFS

Evidence File Name: fisher.E01
Evidence Path: C:\Documents and Settings\User\Desktop\Case4 - Fisher
Identification Name/Number: 001
Evidence Type: NTFS
Added: 12/2/2005 2:32:50 PM
Children: 173
Descendants: 83,788

Display Name: fisher\UnpartSpace

Evidence File Name: fisher.E01
Evidence Path: C:\Documents and Settings\User\Desktop\Case4 - Fisher
Identification Name/Number: 001
Evidence Type: Unpartitioned Space
Added: 12/2/2005 4:06:13 PM
Children: 2
Descendants: 2