

STATE OF OHIO
OFFICE OF THE INSPECTOR GENERAL

RANDALL J. MEYER, INSPECTOR GENERAL

REPORT OF
INVESTIGATION



AGENCY: OHIO DEPARTMENT OF HEALTH
FILE ID NO.: 2012-CA00027
DATE OF REPORT: OCTOBER 24, 2013

The Office of the Ohio Inspector General ... The State Watchdog

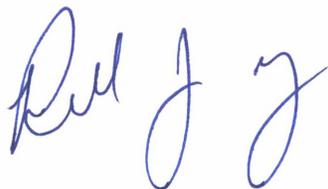
“Safeguarding integrity in state government”

The Ohio Office of the Inspector General is authorized by state law to investigate alleged wrongful acts or omissions committed by state officers or state employees involved in the management and operation of state agencies. We at the Inspector General’s Office recognize that the majority of state employees and public officials are hardworking, honest, and trustworthy individuals. However, we also believe that the responsibilities of this Office are critical in ensuring that state government and those doing or seeking to do business with the State of Ohio act with the highest of standards. It is the commitment of the Inspector General’s Office to fulfill its mission of safeguarding integrity in state government. We strive to restore trust in government by conducting impartial investigations in matters referred for investigation and offering objective conclusions based upon those investigations.

Statutory authority for conducting such investigations is defined in *Ohio Revised Code §121.41* through *121.50*. A *Report of Investigation* is issued based on the findings of the Office, and copies are delivered to the Governor of Ohio and the director of the agency subject to the investigation. At the discretion of the Inspector General, copies of the report may also be forwarded to law enforcement agencies or other state agencies responsible for investigating, auditing, reviewing, or evaluating the management and operation of state agencies. The *Report of Investigation* by the Ohio Inspector General is a public record under *Ohio Revised Code §149.43* and related sections of *Chapter 149*. It is available to the public for a fee that does not exceed the cost of reproducing and delivering the report.

The Office of the Inspector General does not serve as an advocate for either the complainant or the agency involved in a particular case. The role of the Office is to ensure that the process of investigating state agencies is conducted completely, fairly, and impartially. The Inspector General’s Office may or may not find wrongdoing associated with a particular investigation. However, the Office always reserves the right to make administrative recommendations for improving the operation of state government or referring a matter to the appropriate agency for review.

The Inspector General’s Office remains dedicated to the principle that no public servant, regardless of rank or position, is above the law, and the strength of our government is built on the solid character of the individuals who hold the public trust.



Randall J. Meyer
Ohio Inspector General



STATE OF OHIO
OFFICE OF THE INSPECTOR GENERAL
RANDALL J. MEYER, INSPECTOR GENERAL

REPORT OF INVESTIGATION

FILE ID NUMBER: 2012-CA00027

SUBJECT NAME: Edward Jones Jr.

POSITION: Infrastructure Specialist 1

AGENCY: Ohio Department of Health

BASIS FOR INVESTIGATION: Agency Referral

ALLEGATIONS: Theft of records and/or information;
Misuse or abuse of state property/equipment;
Unprofessional or improper conduct/appearance of
impropriety (other than by management).

INITIATED: March 16, 2012

DATE OF REPORT: October 24, 2013

INITIAL ALLEGATION AND COMPLAINT SUMMARY

On March 9, 2012, the Ohio Department of Administrative Services (ODAS) received an email from Viacom International, Inc. regarding allegations of the downloading of copyrighted material, specifically *Big Time Rush - Season Two*, through an IP¹ address identified as belonging to the state of Ohio. ODAS was able to determine the address was assigned to the Ohio Department of Health (ODH) who in turn traced the address to a computer assigned to Edward Jones Jr.² Jones is an Infrastructure Specialist 1 assigned to the ODH help desk located within the Office of Management Information Systems. ODH contacted the Office of the Ohio Inspector General regarding the allegations and an investigation was opened on March 16, 2012.

During the course of the investigation, additional allegations were developed after evidence was discovered indicating Jones may have jeopardized ODH computer security when he downloaded unapproved software and, in particular, downloaded computer viruses for analysis.

BACKGROUND

Ohio Department of Health

The Ohio Department of Health was established by the Ohio General Assembly in 1917. While the initial focus of ODH was to control and prevent the spread of infectious disease, the department is now responsible for providing preventative medical services, public health education and information, and providing other healthcare services and regulatory duties. The mission of ODH is “to protect and improve the health of all Ohioans by preventing disease, promoting good health, and assuring access to quality health care.”³

Office of Management Information Systems

The Office of Management Information Systems (OMIS) “is responsible for maintaining ODH computer networks and servers and for the development and implementation of strategies that support the current and future technology needs of the agency.”⁴ According to ODH officials,

¹ IP, or Internet Protocol, is a unique string of numbers separated by periods that identify a specific computer attached to a network.

² Jones was also involved in a separate investigation by the Office of the Ohio Inspector General conducted during the same time period (ROI #2011-194, released April 25, 2013).

³ Source: Biennial budget documents.

⁴ Source: Ohio Department of Health website.

the two key areas of OMIS are applications development and enterprise network solutions. Applications development includes the creation and production of various software products that support the duties of the office. Enterprise network solutions include the office's IT help desk and computer hardware support.

Copyrights

According to the United States Copyright Office, a "copyright is a form of protection provided by the laws of the United States to the authors of 'original works of authorship' including literary, dramatic, musical, artistic, and certain other intellectual works." Works protected under these laws include "motion pictures and other audiovisual works," "sound recordings," and "musical works, including any accompanying words." Copyrights are provided for the life of the author plus 70 years.

Title 17 of the United States Code, §107, allows for the "fair use" of certain copyrighted material. It lists "criticism, comment, news reporting, teaching, scholarship, and research" as areas where the limited use of copyrighted material could be permissible. Four factors have to be considered when deciding if it meets the "fair use" test:

- 1) Purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes.
- 2) The nature of the copyrighted work.
- 3) The amount and substantiality of the portion used in relation to the copyrighted work as a whole.
- 4) The effect of the use upon the potential market for, or value of, the copyrighted work.⁵

Criminal enforcement of copyright laws is provided through the U.S. Office of Homeland Security Investigation and the U.S. Department of Justice. The act of stealing, distributing, and/or selling of copyrighted material is called pirating.

⁵ Source: U.S. Copyright Office website: www.copyright.gov

Torrenting / Usenets

A common method used for obtaining pirated material, such as movies, TV show episodes, games, music, etc., is called “torrenting.” Torrenting is a file distribution network which identifies the network locations of users who are currently sharing a particular electronic file, for example a movie, through the Internet. Torrent files can be downloaded from the Internet and uploaded into torrenting client software. The client software automatically connects to all of the available users currently sharing that particular file and downloads the file in pieces from multiple users simultaneously.

Usenets or newsgroups have been around since the late 1970s as an electronic bulletin board, or Internet forum, arranged by subject matter. It was designed for users to post discussion threads and topics for other users to comment on. Registered users can post files onto the newsgroup for other users to download. However, users typically need a subscription to gain premium access in order to download posted files from the forum. Recently, independent Internet websites began indexing the content of the newsgroups. This made it easier to locate and download movies, TV shows, and games based on a user’s preferred subject matter.

The posted files are broken up into small fragments in order to be posted on the newsgroups. Users then download the file fragments which are later easily reassembled with a specific software program. This technique is called “binary assembly.” Newsgroup users rely heavily on their network performance in order to achieve extremely high download/upload speeds. Newsgroups do not receive much, if any, regulation due to the popularity of torrenting. Both newsgroups and torrenting are effective means for distributing copyrighted material.

Applicable Policies and Procedures

In addition to federal copyright laws under Title 17 of the U.S. Code, the following ODH policies and procedures were reviewed during the course of the investigation:

ODH Directive 7B, *Use and Security of Agency IT Resources*, effective June 30, 2009

[\(Exhibit 1\)](#):

- 4.2 Downloading Software - All software to be installed on a computer, including software downloaded from the Internet, must be approved as outlined in the OMIS Standard Operating Procedures (SOP) documentation. This may include authorization of individual software programs as well as an agency-wide authorization for specific products.
- 7.0 System Security – ODH staff shall follow procedures regarding access privileges, authentication methods, risk management, system hardening, network monitoring, audit logging, breach monitoring and communications/notification methods to comply with applicable laws, regulations, policies, guidelines, and standards.
- 7.6 Information Technology Code of Responsibility (ITCOR) – A yearly review and acknowledgement of ODH’s Information Technology Code of Responsibility will be performed by all ODH staff as part of the annual Employee Performance Evaluation using HEA 6200 Information Technology Code of Responsibility.
- 12.2 Establishing Network Connections – Unless the prior written approval of the chief of OMIS has been obtained, ODH staff may not establish Internet or other external network connections that could allow non-ODH users to gain access to ODH systems and information.
- 13.2 Prohibited Uses – ODH staff shall not use the Internet to disseminate or print copyrighted material (including articles and software) in violation of copyright laws. Violating or supporting and encouraging the violation of local, state or federal law is strictly prohibited.
- 15.3 Testing Controls – ODH staff shall not test or probe security mechanisms at an ODH site nor use ODH resources to test or probe security mechanisms at other Internet sites.

ODH Directive 7B makes reference to State of Ohio IT Policy ITP-E.8, *Use of Internet, E-mail and Other IT Resources*, effective March 19, 2008, which states: [\(Exhibit 2\)](#)

- 5.3 Participation in Online Communities – Any use of state-provided IT resources to operate, participate in, or contribute to an online community including, but not limited to, online forums, chat rooms, instant messaging, listservs, blogs, wikis, peer-to-peer file

sharing, and social networks, is strictly prohibited unless organized or approved by the agency.

- 5.4 Unauthorized Installation or Use of Software - Installing or using software including, but not limited to, instant messaging clients and peer-to-peer file sharing software, or personally-owned software, without proper agency approval is strictly prohibited.
- 5.6.1 Impeding Access - Impeding the state's ability to access, inspect and monitor IT resources is strictly prohibited. A public servant shall not encrypt or conceal the contents of any file or electronic communication on state computers without proper authorization. A public servant shall not set or manipulate a password on any state computer, program, file or electronic communication without proper authorization.

Jones' Employment and Training

On October 5, 1992, Edward Jones became employed with the Ohio Department of Health as a Data Systems Coordinator 1 with the Division of Quality Assurance. He subsequently became reclassified as a Minicomputer Operations Technician, a Network Services Technician 1 and 2, a Network Services Technician 4 (later demoted), and an Infrastructure Specialist in OMIS. Jones currently works for the ODH help desk.

Jones described his job duties as repairing computers at ODH. He has a degree from DeVry University related to hardware and stated he was "self-taught" when it came to his software skills. Jones has received training regarding software, ethical hacking, computer security, computer viruses, and anti-virus topics. Jones stated he received computer training "very frequently," including on-line training required by ODH. On December 11, 2011, Jones signed the ODH-IT Code of Responsibility and he acknowledged being familiar with the computer use policy.

A review of Jones personnel and training files found he received training on the following: Policies; You are the Target; Social Engineering; Email and Instant Messaging; Passwords; Encryption; Data Protections; Data Destruction; Hacked; and Confidentiality. Jones also attended a 35-hour training course entitled "Ethical Hacking and Countermeasures" approved by ODH and paid for by the Union Education Trust fund.

INVESTIGATIVE SUMMARY

On March 9, 2012, the Ohio Department of Administrative Services received an email from Viacom International, Inc., alleging an IP address identified as belonging to the state of Ohio was used to download copyrighted material. Further information provided by Viacom shows the file downloaded using BitTorrent was *Big Time Rush - Season 2*. BitTorrent is a type of software used for torrenting and sharing files over the Internet. ODAS was able to determine the IP address belonged to the Ohio Department of Health who, in turn, identified the address as belonging to a computer assigned to Edward Jones Jr. ODH notified the Office of the Ohio Inspector General and an investigation was opened on March 16, 2012.

On April 10, 2012, Jones consented to be interviewed by the Office of the Ohio Inspector General.⁶ Jones informed investigators he has been with ODH's IT division since October 1992. Jones described his current responsibilities as repairing computers and performing "a lot of software installation and configuring." During the interview, Jones was informed of the email received from Viacom and was asked to explain why the state would have received such a notice. Jones replied Viacom was "... probably looking at something, getting stuck. I do a lot of virus work, anti-virus. A tremendous amount." When investigators told Jones the email was in regard to downloading copyrighted material and not about a computer virus, Jones said, "Well, let me fully explain 'cause I've been caught at it before." Jones explained that he had a separate computer where he downloads "suspicious programs" or computer viruses for analysis. Jones said the computer is not connected to the ODH network; however, it has Internet access. Jones stated he believed what probably happened was when he downloaded one of these "suspicious programs," the file in question was obtained by his computer as a result of a virus.

Jones noted something similar had happened before and Greg Perkins, ODH's former network services supervisor,⁷ "... would have to call and jump on my case about I've done it again, you know, and there'd be processes running in the background that I'm not aware of." Investigators asked if Jones had any idea that he was downloading copyrighted material and Jones responded "I didn't download anything. It was just tunneling through my ... computer."

⁶ This interview was in relation to events surrounding a separate investigation in which Jones was involved. (File ID No. 2011-194, released April 25, 2013)

⁷ Perkins currently works for the Ohio Department of Transportation.

Jones stated it was part of his job responsibilities to download and analyze computer viruses and that Ron Ferencz (his immediate supervisor), Henry Smith (Ferencz's supervisor), and Bruce Hotte (chief of OMIS) would attest to this view. When asked what software programs he uses to perform these tasks, Jones stated he used free versions available on the Internet.

Jones confirmed ODH utilizes an anti-virus software program to detect and prevent incoming viruses, but noted the program "... unfortunately fails frequently." Jones stated he performs computer virus research while at work using the state's computer system because "I want to know where did it come from and why is everyone getting it." Jones established ODH has a network services supervisor, Jeff Swan, whose responsibilities include managing the ODH computer servers and maintaining network security. Jones stated he does not work with Swan or notify him of the computer virus research he conducts, saying he "... professionally almost never..." talks to Swan.

Jones also commented on using free software he downloaded from the Internet for ODH work-related activities, and provided an example called Logmein.com. This program allows a user to remotely access another user's computer. A user can then run any programs or access any files from a remote site without having to be physically present at the second computer's location. Jones explained ODH has licenses for a similar software application; however, there were times the licenses were all in use and so he utilized Logmein.

Jones' immediate supervisor, Ron Ferencz, was interviewed on April 18, 2012, and asked about the statements made by Jones. Ferencz verified Jones was ODH's "go-to virus guy" but was unaware of Jones downloading computer viruses for analysis. Ferencz said if Jones was in fact doing as he claimed, "That would be a compromise of our network and our security." Ferencz stated he was also unaware of Jones possessing a third ODH computer, because typically all help desk employees are assigned only two computers. However, Ferencz said it would not be suspicious if there were more than two computers in Jones' work area, as there are occasions when the help desk employees would be working on other employees' computers in their cubicles. Ferencz said if he had known Jones was utilizing a third computer, "I wouldn't have (sic) permitted him to have that."

The Office of the Ohio Inspector General inquired about the use of free software (referred to as freeware or shareware) downloaded from the Internet by ODH employees. Ferencz stated he was aware of instances where the software had been used by ODH employees. When investigators asked Ferencz whether the free software was something the employees were permitted to use, Ferencz replied, “There have been a few that have been used that I have heard of but that was not, you know, verbally said to – or in writing or something of that nature – to go ahead and use that freeware or that shareware.” When Ferencz was asked specifically about his employees using that particular software, Ferencz said “they might,” but that he had no direct knowledge of them using it. Ferencz added, “... we have never had that discussion, so to speak, in terms of using it or not using it.”

On August 9, 2012, the Office of the Ohio Inspector General interviewed Henry Smith. Smith acknowledged Jones was one of the “most knowledgeable” when it came to computer viruses and stated that he had heard Jones say he did a lot of research at home. When Smith was informed of Jones’ statements that Ferencz and Smith authorized him to do the virus research at work using ODH resources, Smith replied “absolutely, no,” he had not authorized that work. Smith further stated it would be a major security breach to conduct such work.

Smith said he was aware of the situation involving Perkins admonishing Jones for downloading copyrighted material in the past. However, Smith stated he was unaware of how the situation was resolved and what, if any, preventive measures were put into place to ensure it would not occur again.

Computer Analysis

The Office of the Ohio Inspector General took the hard drives from two computers assigned to Jones and the hard drive from the third unauthorized computer not connected to the ODH network on April 11, 2012. Additionally, an external hard drive that Jones used in his ODH work area was removed and analyzed by the Office of the Ohio Inspector General after it was confirmed by ODH officials to be their property and not the personal property of Jones. From an analysis of the hard drives conducted by the Office of the Ohio Inspector General, investigators determined that shortly after Jones’ interview ended on April 10, 2012, at approximately 3:05

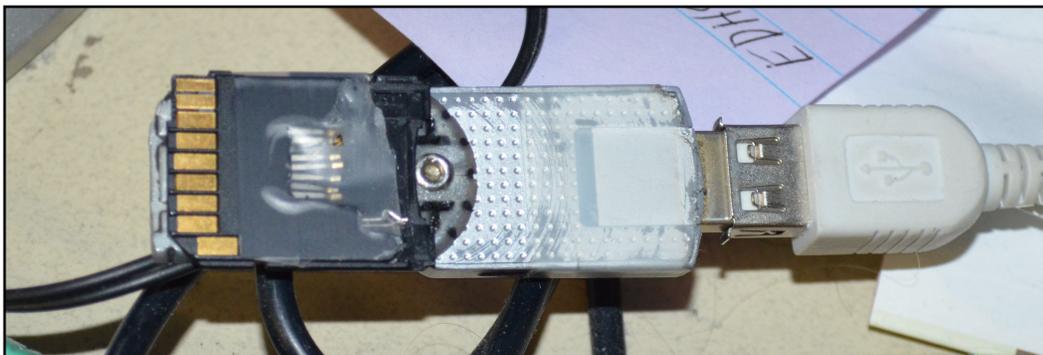
p.m., Jones returned to his work space and attempted to delete information and files from both his unauthorized computer and the external hard drive. Analysis found the following categories and number of copyrighted files that were deleted:

Type and Amount of Files Located on Seized Hard Drives

Device	Description	# of Files	Deletion Date/Time
External Hard Drive	Movie / TV	2,463	4/10/2012; 3:30 p.m.
External Hard Drive	Comic Books	2,109	4/10/2012; 3:30 p.m.
Computer Hard Drive	E-Books	438	4/10/2012; 4:00 p.m.
Computer Hard Drive	Daily Comic Strips	33	4/10/2012; 4:00 p.m.
Computer Hard Drive	Movie / TV	49	4/10/2012; 3:49 p.m.
	TOTAL	5,092	

Even though files from the two hard drives were deleted, the Office of the Ohio Inspector General was able to recover the deleted files and found the video and comic book files, most of which investigators could access to view and/or play.

In addition to the hard drives, what appeared to be a USB flash drive⁸ attached to Jones' unauthorized computer was seized. The following is a picture of the device:



The device was sent for analysis to the Ohio Bureau of Criminal Identification and Investigation (BCI), a division of the Ohio Attorney General's Office. BCI determined the device was a USB drive with a Micro SD Card Reader⁹ attached and appeared to have been made by an individual. The USB drive and card reader operated independently of each other and did not share data. Files were located on the USB drive but not the card reader. The files included anti-virus programs; video and audio copying software; torrenting programs; and what appeared to be the

⁸ An USB flash drive is a small portable electronic storage device.

⁹ SD stands for Secure Digital. A micro SD card reader is a small portable electronic memory storage device typically used in digital cameras, camcorders or audio players.

software typically installed on the computers assigned to ODH employees. The files were created between 2008 and 2012.

Investigators further determined Jones, using an online alias (also known as a “handle”), downloaded, uploaded, and torrented thousands of movies, TV shows, and comic books using state of Ohio resources, including ODH’s Internet connection. Additionally, Jones downloaded entire annual volumes of Marvel Comic Catalogs. Each single catalog contains the complete collection of all the Marvel

comic books published, in chronological order, for a calendar year. The comic books found by investigators on the state devices assigned to Jones were print-ready quality and from multiple publishers (See illustration at



right¹⁰). Jones also used comic book cataloging software to maintain the inventory of comic book collections. This comic book catalog contained more than 30,000 comic book titles, with multiple comic books for each title. ([Exhibit 3](#))

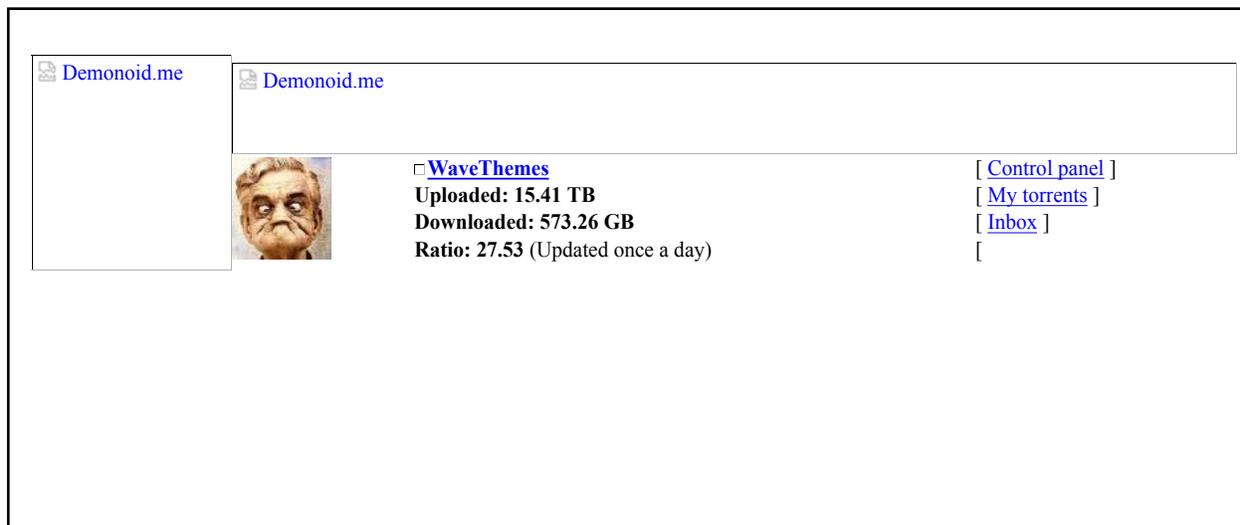
Investigators were able to determine Jones was a member of several torrenting websites where he downloaded and uploaded files. The following are two of the sites reviewed by the Office of Ohio Inspector General. On one site for Jones’ online alias, it was determined the upload to download ratio was 27:1 – meaning for every 27 gigabytes that were uploaded, 1 gigabyte of data was downloaded.

¹⁰ Citation: comic book covers used in illustration:
[Wagner, Matt (writer), and Snyder III, John K. (artist).] Zorro Rides Again. Issue #8 of 12 (February 2012), Dynamite Entertainment: Cover.
[Wells, Zeb (writer); Madureira, Joe (artist), and Daniel, Ferran (colourist).] Avenging Spider-man. Volume #1 (January 2012), Marvel Comics: Cover.
[Johns, Geoff (writer); Reis, Ivan (pencils); Prado, Joe (inks) and Ferreira, Eber (inks).] “Buried Alive!” Aquaman, the New 52, Issue 5 (March 2012), DC Comics: Cover.

Demonoid

Demonoid was a popular torrent website which facilitated in the sharing of copyrighted materials throughout the world. An analysis of Jones' temporary Internet files on his state-assigned computer found an image of an Internet webpage which showed the online alias attributed to Jones uploaded 15.41 terabytes¹¹ of data to Demonoid and downloaded 573.26 gigabytes¹² of data from Demonoid. Torrenting files from Demonoid were found on Jones' state-issued computer and external hard drive. Investigators were able to determine the site the files originated from because the site name was located in the file information. In August 2012, INTERPOL¹³ coordinated international efforts and closed the site down and police in the Ukraine seized its servers. A criminal investigation was launched, targeting its owners in Mexico, resulting in a number of arrests and a seizure of assets.

Recovered Screen of Jones' Demonoid Alias



Pirate Bay

Similar to Demonoid, Pirate Bay is a torrenting file sharing site where information was stored on Jones' unauthorized state computer. Investigators were able to establish that in 2008 and 2009, Jones hosted copyrighted materials where, at the time of this investigation, the links to the files were still active, and it was possible the files could still be downloaded by other users. The

¹¹ A terabyte is approximately one trillion bytes of data, or 1,024 gigabytes.

¹² A gigabyte is approximately one million bytes of data, or 1,024 megabytes.

¹³ INTERPOL, or the International Criminal Police Organization, is an intergovernmental organization facilitating international law enforcement cooperation.

founders of Pirate Bay were criminally prosecuted in Sweden in November 2010 for copyright infringement offenses. Jones was not as active on Pirate Bay as he was on Demonoid and the following is all of the information attributed to his known alias found by investigators on the site.

Screen Capture of Pirate Bay Uploads under Jones' Alias

Browse WaveThemes				
Type	Name (Order by: Uploaded, Size, ULed by, SE, LE)	View: Single / Double	SE	LE
Video (TV shows)	Baa Baa Black Sheep (1976)(Season1) XviD DVDRips   Uploaded 02-03 2009, Size 9.32 GiB, ULed by WaveThemes		12	7
Video (HD - TV shows)	The Addams Family (DVDRips) season 2 (1965-66)(XviD.720x480)   Uploaded 01-15 2009, Size 8.12 GiB, ULed by WaveThemes		7	5
Video (HD - TV shows)	The Addams Family (DVDRips) season 1 (1964-65)(XviD.720x480)   Uploaded 01-02 2009, Size 9.78 GiB, ULed by WaveThemes		9	6
Video (TV shows)	Power Rangers Operation Overdrive - All (RESEED) TVCap Xvid avi   Uploaded 06-06 2008, Size 7.49 GiB, ULed by WaveThemes		4	6
Video (TV shows)	Sky - Complete Series (UK-HTV 1975) XviD avi   Uploaded 04-23 2008, Size 2.92 GiB, ULed by WaveThemes		0	3
Video (TV shows)	City Beneath the Sea (British, 1962 Sci-Fi) Xvid avi   Uploaded 04-21 2008, Size 4.78 GiB, ULed by WaveThemes		0	6
Video (TV shows)	Birds of Prey (Complete with Unaired Pilot) RESEED   Uploaded 04-07 2008, Size 4.74 GiB, ULed by WaveThemes		3	3
Video (TV shows)	Young Dracula Season 2   Uploaded 02-15 2008, Size 2.95 GiB, ULed by WaveThemes		7	1

Usenet/Newsgroups

As a subscribed member of Newsguy.com, Jones used the WaveThemes alias and other aliases to post hundreds of TV and video files onto the newsgroup forums. The files that Jones uploaded onto the newsgroups were still active and available at the time of the investigation. The computer analysis was able to determine other aliases used by Jones based on information from his Internet activity and information contained in software files located on the unauthorized computer's hard drive which link one of his user names with his newsgroup aliases. Usernames and aliases used by Jones include: ejones, visit@my-domain-for-mail.org (wavethemes), see-my-dot-org@for.it (WaveThemes), and HateSpam@home&office.hr (WT-TVTube).

The analysis of the state computers assigned to Jones found or revealed:

- Internet activity to a website, later identified as created by Jones, called WaveThemes. The site was used to host TV show theme songs from the last 50 years.
- Jones uninstalled various computer programs and software from his unauthorized device. Included in the programs were various torrent clients and video “ripping” software used to capture streaming videos from the Internet and converting them to sharable video files.

Some of these programs were later determined to have been purchased by ODH for the agency's use.

- Internet activity where Jones frequented or bookmarked various TV streaming websites. Also bookmarked or visited were websites to various torrenting and newsgroup sites, different than the sites noted above.
- An online posting from 2007 where Jones, identifying himself as WaveThemes, states, "I like having 50GB of bandwidth to play with." ([Exhibit 4](#)) In 2007, this network performance was not available to residential customers and may be in reference to his Internet access at ODH.
- There was no evidence of *Big Time Rush - Season 2* on either device, but evidence was found of *Big Time Rush - Season 3*.
- BitTorrent, the program Viacom alleged was used to download *Big Time Rush - Season 2*, was located on Jones' state-issued computer.

Investigators visited the WaveThemes site and found a blog with several postings. These postings listed the dates and times of when the posts were uploaded. A comparison was made between these dates and times, with the hours reported being those in which Jones was supposed to be doing work for the state of Ohio. Jones' supervisor reported his typical work hours were 8:30 a.m. to 5:00 p.m. but Jones was known to come in early or work late, sometimes being at the office at 11:30 p.m.

Comparison of Blog Posts to Reported Hours Worked

Blog Post Date and Time	Hours Reported as Worked
Thursday, August 13, 2009; 8:00 a.m. and 8:14 a.m.	8 hours
Friday, August 14, 2009; 5:26 p.m.	8 hours
Friday, August 21, 2009; 8:23 a.m.	8 hours
Tuesday, August 2, 2011; 4:41 p.m.	7 hours + 1 hour sick leave
Friday, March 30, 2012; 9:57 a.m.	8 hours
Friday, September 14, 2012; 12:21 p.m. and 12:45 p.m.	8 hours

This comparison shows Jones was potentially updating his personal website blog during hours he was working for the state of Ohio.

Also noted on the WaveThemes site was a profile picture that was the same profile picture used on the Demonoid website. This shows that not only was Jones using the same alias, he was also using the same profile picture. ([Exhibit 5](#))

Second Interview with Jones

On July 10, 2013, the Office of the Ohio Inspector General conducted a second interview with Jones regarding the information obtained through the computer analysis. The interview was conducted with the assistance of a special agent from the U.S. Homeland Security Investigations Unit.

Hard Drives

Jones stated he purchased the external hard drive that was seized because ODH did not have the resources to "... buy big things ... back then." Immediately after making that statement, Jones said, "... that's not really a big drive." When informed the external hard drive was the property of ODH, Jones replied, "It is now, yeah. It's been their property since I got tired of it at home." Jones explained he used the drives to store ODH's laptop images.¹⁴ As there was no inventory tag on the external hard drive, the Office of the Ohio Inspector General inquired to ODH if the drive belonged to the department. ODH informed investigators they asked Jones who it belonged to and he identified it as belonging to ODH. Jones did not inform ODH of his claims that he purchased the item and donated it to the agency.

In regard to the unauthorized computer, ODH located inventory records showing the computer had been assigned to Jones in November 2009. However, Jones' supervisors did not authorize him to have this computer and believed it should have been sent to salvage. There were no records found regarding who authorized Jones to have been assigned this computer, just that it was "authorized."

When informed the computer analysis found Jones had attempted to delete almost 6,000 files containing copyrighted material from the external hard drive, Jones stated the hard drive was not

¹⁴ Images are copies of the typical software and other programs used by ODH employees that can easily be transferred to new computers.

big enough to hold that many files. Jones also could not explain why the laptop images were still on the external hard drive while only the copyrighted files were deleted.

Jones stated that on the day of his first interview, he noticed the unauthorized computer was “running” and he believed it had a virus on it that was not doing what he was expecting it to do. Jones stated he planned on “wiping” or cleaning the hard drive as he typically does when a virus he is researching starts taking over the computer. However, Jones stated that he did not get a chance to wipe or clean the hard drive, because, “I swear five minutes later you called me.” Jones said he did not do anything to either the external hard drive or the unauthorized computer other than taking them off the Internet or turning them off.

Investigators asked how the information could be deleted from the external hard drive if it was no longer connected to the computer and, therefore, was no longer receiving a signal from whoever was using it to “tunnel,” as Jones claimed someone had in his first interview. Jones replied, “... if it’s (not) receiving a signal it’s conceivable that a bomb¹⁵ would be, that was inside” and it triggered a program that removed select file types.

The computer analysis also found Jones had executed the “uninstall software” program¹⁶ on the unauthorized computer the day of the first interview. Jones was asked to explain why he executed this program if he planned on “wiping” the hard drive and that would have removed the same programs in the process. Jones said he did so because there were some programs “that I would have had to return a license.” Jones was provided a list of the programs removed, all of which were “torrenting” or media players that could be utilized to record or capture video and/or audio files, some of which Jones identified as being owned or licensed by ODH.

Computer forensic analysts with the Office of the Ohio Inspector General stated Jones’ claim of a “bomb” targeting select files types is possible. However, the external hard drive would need to be connected to a computer in order for any program on the hard drive to be activated and for the so called “bomb” to take effect.

¹⁵ A “bomb” is a malicious computer program that can wipe select files or the whole programming system from a computer. Such a program needs a processor and some type of prompt from an outside source before it is activated.

¹⁶ A utility program that removes multiple software programs from the operating system with a single command.

By shutting down and removing the external hard drive from the computer, the connection and processing capability required to execute the program would no longer exist. The computer analysis previously conducted did not find any trace evidence of such a “bomb,” as described by Jones, located on the external hard drive.

WaveThemes

Jones confirmed he owned and operated the www.WaveThemes.org website. Jones also confirmed the profile picture on the site was one he picked for the site. Jones stated the site was a “hobby” and contained a collection of TV theme songs. Jones expressed pride in the website, claiming at one point, the website “... was getting a million hits a week.”

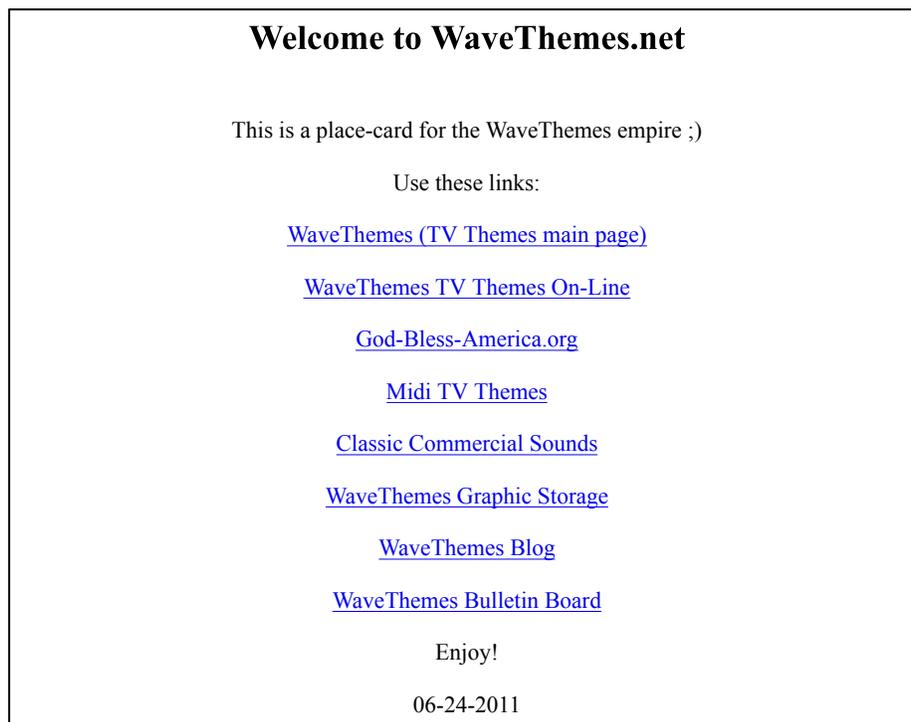
Based on the number of hits Jones claimed the website received, investigators asked Jones if he ever charged or thought about charging individuals to download the files. Jones said he did not create the site to make money but he did “... have people begging me to put banners and all that other stuff up.” Jones stated if he had, it would have violated rules and the site was “... for education and entertainment.” Jones explained that if a person was not selling the copyrighted material, but was using it for educational purposes, that use of the material would be permitted under the federal Fair Use Act. Jones also claimed that the file quality was intentionally poor and some were recorded directly from the TV and not from any CDs or DVDs. Therefore, if someone tried to make a CD using the files uploaded to the website, the sound would not be of the best quality.

The “Freedom and Innovation Revitalizing United States Entrepreneurship Act of 2007,” or the Fair Use Act, was introduced in the U.S. House of Representatives in February 2007. The act was an attempt to reform the “fair use” clause already in place based on digital media. However, the act was never voted on and never became law. Current “fair use” federal statutes allow for limited use of copyrighted material to be used for educational purposes. Including a statement that the files are copyrighted does not protect the individual under the “fair use” statutes.¹⁷

¹⁷ Source: U.S. House of Representatives and U.S. Copyright Office.

Jones also confirmed he was the individual who identified himself as “WaveThemes” and posted the comment in 2007 stating, “I like having 50GB of bandwidth to play with.” ([Exhibit 4](#)) When Jones was asked if he had the capability at home for that type of bandwidth, Jones replied “No.” Jones stated the bandwidth came from the servers that hosted his website.

Jones established other websites that were redirected from the WaveThemes site which Jones confirmed he had developed. When accessing the WaveThemes site, the following screen appears:



Comic Books

Jones stated he was “a comic book collector.” Jones said he would not “bother” having electronic copies except for some he got for his grandson so he could decorate his walls with the covers. When asked about the comic book catalog, Jones first denied having it, then later said, “I may have downloaded the list.” Jones denied downloading the actual comic books.

Jones was shown three of the covers from the thousands of files recovered from the external hard drive. Jones replied he was just downloading the covers and that was all. Investigators informed Jones that the files located on the external hard drive contained the entire book and not just the

cover. Jones stated, “All I wanted was the cover” and that he “... would take just the cover and throw the rest away.”

Investigators inquired where he was when he downloaded these items and he replied, “Everywhere. I mean at home, maybe at the office, too.” Jones stated he found the comic books by doing a basic Internet search, saying, “You just type in the name in a search and you’ll find them.” Jones admitted the downloading of the comic books was for personal use and he was not doing it to look for viruses.

Copyright Material

The Office of the Ohio Inspector General asked Jones if he was familiar with the Demonoid and Pirate Bay websites. Jones replied “Oh, sure. That’s where I pick up a lot of my viruses.” OIG computer analysts determined that Jones often bookmarked multiple torrenting websites and specific torrents through his browser. Jones said he knew the sites were “file-share sites” and admitted to going to Demonoid to watch TV shows. After downloading and watching the TV show, Jones said he would “usually delete it” but then said there were other times he would forget and when he went to download another show, he would not have the space to do so. When Jones was asked if all he did was downloading, Jones said, “Yep.”

Jones said he tried to set up an account on Demonoid using the WaveThemes alias but someone had already used it. As a result, Jones stated that he had setup an account using EJones and a number at the end that he could not remember exactly. Jones was provided a copy of the screen capture with the WaveThemes alias and profile picture. Jones again confirmed the picture was the one he used on his website. When told the picture was also used on Demonoid, Jones replied “Really? I’ll be darn.” Jones then said the WaveThemes alias had been “stolen” and used on other websites because someone was “out to get me” since he would not upload files in a better quality format. Jones also said it could not have been him as the alias on Demonoid used a capital “T” and he used a lower case “t.” However, Jones previously confirmed the WaveThemes.net website was his and the links show the capital “T” was used each time WaveThemes was listed.

Jones was also asked about the various other aliases he used on the Internet. Specifically, the “Hate Spam” account. Jones stated he did not “know anything about that” and denied using that specific alias.

Jones reviewed a list, provided by investigators, of the TV shows and movies located on the external hard drive. Jones pointed out some of the shows were British and Australian. Investigators noted on the WaveThemes blog, which Jones admitted was his blog, states the author liked these types of shows. Regarding the matter of the list of TV shows and movies being found on the hard drive, Jones explained, “I’m looking at the things to see if they’re virus infected.” Jones stated that ODH employees were viewing these shows at work and he “probably seen lists (sic) and followed after them. Some of this is my interest, but not all of it.” ODH did not provide information to the investigators regarding employees watching these TV shows at times they were working for the state, as claimed by Jones.

ODH does have a software program that can be used to monitor employees’ Internet activity. Jones is not in the chain of authority to receive a list of ODH employees who are suspected of inappropriate Internet activity and it is unknown how he would have received such a list.

Investigators asked Jones if he was downloading these shows from work. Jones replied, “No, I would use Logmein.com to go to my home PC and instruct it what to do.” In the first interview with investigators, Jones admitted to downloading this program but said it was for work purposes. When investigators presented Jones with the possibility that instead of instructing his home computer to download files, he had set his work computer to download, Jones whispered, “Oh my God. Yes.” Jones also stated he accessed his home computer through Logmein on a daily basis.

Jones was informed the computer analysis conducted by the Office of the Ohio Inspector General did not find any evidence of viruses attached to the TV shows. Jones admitted that “I’ve downloaded for my personal use” and that some of the files “probably” came from unauthorized websites. Jones said he “probably” downloaded some of the video files so he could record only the theme song. However, the computer analysis showed Jones typically downloaded entire

seasons of shows, not just one episode. Jones insisted that all he did was download, and only uploaded theme songs to his WaveThemes website.

When investigators asked Jones why these actions would not have violated copyright laws, Jones said, "I'll take ownership of being lazy. Of not caring. Not being careful." Jones insisted he did not conduct these activities for profit. When investigators pointed out to Jones that any notoriety and popularity he may have obtained by being connected to WaveThemes on the Internet could be considered a personal "gain," Jones stated, "I guess I'm in a lot of trouble but it was not intentional, but I'll own up to (it)."

CONCLUSION

Upon receiving notification from Viacom International, Inc. regarding allegations of downloading copyrighted material through an Internet connection assigned to the state of Ohio, an investigation was opened by the Office of the Ohio Inspector General. The connection was traced to an employee within the Ohio Department of Health, Edward Jones Jr. Jones initially reported the material was not downloaded but had "tunneled" through his Internet connection while he was downloading a computer virus for research purposes. This download occurred on an unauthorized computer owned by ODH, which was located in Jones' work space, and was not connected to the ODH network.

Jones claimed he had authority from his supervisors to conduct virus research work and that this function was part of his job responsibilities. Interviews conducted with the supervisors found that while they considered Jones their "go-to guy" in terms of helping remove computer viruses employees may have unintentionally downloaded, Jones did not have authorization to download computer viruses for further study. The supervisors were also unaware that Jones had access to a third computer which had Internet access and was not connected to the ODH network.

Downloading these viruses presented a security risk to ODH and was done so in violation of ODH Directive 7B, *Use and Security of Agency IT Resources*.

Accordingly, the Office of the Ohio Inspector General finds reasonable cause to believe a wrongful act or omission occurred in this instance.

The Office of the Ohio Inspector General analyzed the ODH computers and the external hard drive associated with Jones. The analysis found Jones attempted to erase various copyrighted files, computer programs, and software. Additionally, by not having the unauthorized computer connected to the ODH network, ODH officials were unable to monitor Jones' computer activity in accordance with ODH policies and procedures. By doing so, Jones attempted to impede access to files Jones had downloaded in violation of State of Ohio IT Policy ITP-E.8, *Use of Internet, E-mail and Other IT Resources*.

Accordingly, the Office of the Ohio Inspector General finds reasonable cause to believe a wrongful act or omission occurred in this instance.

Also seized was a device created by Jones that was attached to the unauthorized state computer. An analysis conducted by the Ohio Attorney General's Bureau of Criminal Identification and Investigation found anti-virus, torrenting, and ODH software programs located on the device. This device was used to image ODH computers and was also used by Jones for his virus research. Connecting this device to various ODH computers could have introduced viruses into the ODH network. This was done in violation of ODH Directive 7B, *Use and Security of Agency IT Resources*.

Accordingly, the Office of the Ohio Inspector General finds reasonable cause to believe a wrongful act or omission occurred in this instance.

Through the computer analysis and Internet research, the Office of the Ohio Inspector General was able to determine Jones was distributing numerous copyrighted materials over the Internet. This was done using ODH resources and through IP addresses associated with ODH and the state of Ohio. Jones stated the alias used was stolen from him and it was not him uploading these programs. Jones' evidence for this explanation was the use of a capital "T" in the alias' name. Jones stated he only used a lower case "t" in his name. Investigators were able to determine

from a website Jones admitted was his that Jones also used the capital “T” in various website names.

Jones initially stated he downloaded various video files for his virus research. Jones stated he downloaded specific programs because other ODH employees were viewing these shows and he wanted to determine if a virus was attached to them. Because of the large number of files uncovered during the computer analysis, it is highly unlikely ODH employees were viewing the majority of these shows without ODH becoming suspicious.

Jones admitted he downloaded copyrighted files for his personal use. Jones did so using an authorized program operating on an ODH computer used by Jones. While Jones said this program was to be used to instruct his home computer to download files on a daily basis, Jones stated it was possible he instructed the ODH computer to do so instead.

Jones utilized state resources during work hours for this activity. This was done in violation of ODH Directive 7B, *Use and Security of Agency IT Resources* and Ohio IT Policy ITP-E.8, *Use of Internet, E-mail and Other IT Resources*.

Accordingly, the Office of the Ohio Inspector General finds reasonable cause to believe a wrongful act or omission occurred in this instance.

Finally, evidence from Jones’ unauthorized state computer shows he downloaded free computer programs and software readily available on the Internet. Investigators interviewed Ron Ferencz, Jones’ immediate supervisor. During his interview, Ferencz stated he was aware of the possibility of ODH employees downloading various software programs without proper authorization. Ferencz also stated he believed the help desk employees he supervises might have also been downloading unauthorized software.

ODH Directive 7B, *Use and Security of Agency IT Resources*, states employees must be approved as outlined in the OMIS Standard Operating Procedures (SOP) documentation. State of Ohio IT Policy ITP-E.8, *Use of Internet, E-mail and Other IT Resources*, also states

“Installing or using software including, but not limited to, instant messaging clients and peer-to-peer file sharing software, or personally-owned software, without proper agency approval is strictly prohibited.” ODH supervisors were aware of the possibility of the downloading of unapproved computer programs or software had occurred but no action was taken to determine if these assumptions were true.

Accordingly, the Office of the Ohio Inspector General finds reasonable cause to believe a wrongful act or omission occurred in this instance.

RECOMMENDATION(S)

The Office of the Ohio Inspector General makes the following recommendations and asks the Ohio Department of Health to respond within 60 days with a plan detailing how the recommendations will be implemented. The Ohio Department of Health should:

- 1) Review the actions of the individuals named in this report and determine if administrative action or additional training is warranted.
- 2) Ensure the policy governing downloading of software or computer programs is adhered to by employees in OMIS and throughout the agency.
- 3) Review any free software downloaded by employees to ensure it does not comprise the security of the ODH computer network. Remove software determined to be unauthorized.

REFERRALS

A copy of this report has been provided to the U.S. Attorney for the Southern District of Ohio, the U.S. Department of Homeland Security, the Franklin County Prosecutor’s Office and the City of Columbus Prosecutor’s Office for their consideration.

[\(Click here for Exhibits 1 – 5 combined\)](#)



STATE OF OHIO
OFFICE OF THE INSPECTOR GENERAL

RANDALL J. MEYER, INSPECTOR GENERAL

NAME OF REPORT: Ohio Department of Health

FILE ID #: 2012-CA00027

KEEPER OF RECORDS CERTIFICATION

This is a true and correct copy of the report which is required to be prepared by the Office of the Ohio Inspector General pursuant to Section 121.42 of the Ohio Revised Code.

Jill Jones
KEEPER OF RECORDS

CERTIFIED
October 24, 2013

MAILING ADDRESS

OFFICE OF THE INSPECTOR GENERAL
JAMES A. RHODES STATE OFFICE TOWER
30 EAST BROAD STREET – SUITE 2940
COLUMBUS, OH 43215-3414

TELEPHONE

(614) 644-9110

IN STATE TOLL- FREE

(800) 686-1525

FAX

(614) 644-9504

E-MAIL

OIG_WATCHDOG@OIG.STATE.OH.US

INTERNET

WATCHDOG.OHIO.GOV