Commonwealth of Pennsylvania

v.

Weiwu Zhao

No.: CP-48-CR-665-2016

Information Technology Investigation – Final Report

November 9, 2017

Submitted to: Weiwu Zhao

Written by:
Steve Simpson CCE, CISSP, CPTC, CSFA, PMP
S2 Forensics, LLC

Introduction:

This report is a response to a request from Mr. Weiwu Zhao made through his daughter and interpreter Ms. Qing Zhao. The opinions and conclusion of this report are based on my interviews conducted with Ms. Qing Zhao, many of which included Mr. Weiwu Zhao; the case related documents forwarded by Ms. Qing Zhao; and findings made at the Zhao family residence in Easton, Pennsylvania. A listing of the documents used for this report and provided by Ms. Zhao can be found in *Appendix A: Case related documents.* The request for this report was made via email dated September 30, 2017 sent by Ms. Qing Zhao to Steve Simpson of S2 Forensics, LLC.

The charges against Mr. Zhao stem from accusations made by the Commonwealth of Pennsylvania against Mr. Weiwu Zhao that include the possession and distribution of child pornography (CP).

It should be noted that this report does not include any findings from the analysis of Mr. Zhao's computer. To date no 3rd party entity has been allowed to analyze the hard drive, including files or metadata residing on the hard drive, used to charge Mr. Zhao.

Report Summary:

This report will examine the possibility that the computer used by Mr. Zhao likely contained the images and video of CP for which Mr. Zhao is accused. The report also explores the ease with which the Zhao family computer network, and in particular Mr. Zhao's computer could have been compromised using either physical or online means. Additionally, this report will explore a number of discrepancies pertaining to police evidence regarding the files acquired from Mr. Zhao's computer. Lastly, this report will propose the possibility that individuals other than Mr. Zhao could have easily compromised and used the computer for the storage and distribution of child pornography.

Specifically, this report will address:

- Why it is likely that Mr. Zhao's computer contained up to 14 CP images/videos at the time Mr. Zhao's retrieved the computer from a pile of refuse
- The peer to peer software found on Mr. Zhao's computer that enabled the distribution of CP was installed prior to Mr. Zhao's use
- That people other than Mr. Zhao and including Ms. Qing Zhao's her ex-husband used the computer on multiple occasions
- Discrepancies and inaccuracies found in the police report documents that may indicate evidence files from other cases have been used against Mr. Zhao
- That Mr. Zhao's computer and network equipment had little to no protection against unauthorized use or intrusion by malicious individuals allowing anyone with physical or online access total control of the computer

Based on interviews with Ms. Qing Zhao, the documentation received regarding this case, and the network investigation conducted at the Zhao residence it is my conclusion that the computer equipment used by Mr. Zhao contained no less than five, and possibly up to 14 CP images and videos when Mr. Zhao retrieved the computer from the refuse pile. Additionally, due to a lack of common computer security practices implemented on Mr. Zhao's computer as well as the Zhao family network equipment it is highly possible that any individual with malicious intent could have gained both access and control of Mr. Zhao's computer through physical use of the machine or remote online network and computer access. This access could have then led to the malicious use of Mr. Zhao's computer for the storage and distribution of the child pornography videos found on the computer.

Discussion:

Timeline of events:
The following is a timeline of events that relate to the charges against Mr. Zhao. This timeline reflects the order of events as told to me by Ms. Qing Zhao. In some cases the timeline events are confirmed with various documents.

- December 22, 2014 through January 3, 2015 – a total of 14 videos classified as child pornography (CP) were loaded onto the computer later found and retrieved by Mr. Zhao. The loading date and time of the files can be established by the file creation time
- Sometime between December 30, 2014 and December 31, 2014 Mr. Zhao found and retrieved the PC from a pile of refuse near his home
- "Within a few days" as reported by Ms. Qing Zhao and likely between January 4, 2015 and January 5, 2015 Ms. Qing Zhao loaded the Microsoft-XP operating system (OS) onto the PC retrieved by Mr. Zhao
- Computer log reports from police indicating that file downloads were attempted multiple times daily between December 23, 2014 and January 7, 2015. A majority of the log files indicate that either the police were unable to download any data that any attempted file transferred ceased due to "time limit to wait for data was exceeded". Log files report that the remote IP address connection was 65.78.83.141
- January 5, 2015 – Police connect to Mr. Zhao's PC and download images.
- April 20, 2015 – Application for Search Warrant and Authorization for the search and seizure of computer and computer related items from the home of Weiwu Zhao
- April 21, 2015 - The Pennsylvania State Police executed a search warrant at the home of Weiwu Zhao

Mr. Zhao's computer:

Per the timeline listed above, the testimony presented by Pennsylvania State Trooper James Ford at Mr. Zhao's preliminary hearing (see document *1-11 preliminary hearing transcript.pdf*), and the police computer forensics reports titled *a1.pdf* and *a2.pdf* all files listed below were created on the computer prior to the date on which Ms. Qing Zhao installed the Microsoft-XP OS and prior to Mr. Zhao's use of the computer.

A summary of the files loaded and the file creation dates are listed in Table 1, below.

File name	File Creation Date	File Last Access Date	File Last Written Date
Preteen-Daphne (Blond Rasta).avi	12/22/2014 01:54:18AM	12/30/2014 05:34:38PM	12/30/2014 02:05:27PM
L1(20).avi	12/22/2014 01:54:18AM	01/02/2015 07:45:34AM	12/30/2014 02:05:27PM
o(29).mp4	12/22/2014 01:55:20AM	12/24/2014 05:24:47PM	12/22/2014 09:29:49PM
o(66).avi	12/24/2014 07:31:37AM	12/28/2014 07:23:26AM	12/24/2014 08:47:33PM
o(70).rmvb	12/24/2014 07:31:50AM	12/28/2014 01:02:31PM	12/28/2014 12:25:29PM
o(50).avi	12/24/2014 09:30:00AM	12/24/2014 05:38:33AM	12/24/2014 10:06:49AM
o(65).avi	12/24/2014 10:04:10AM	12/28/2014 02:12:56AM	12/28/2014 01:01:25PM
o(81).avi	12/24/2014 10:06:15AM	12/28/2014 01:01:39PM	12/28/2014 11:50:51AM
o(23).gif	12/27/2014 10:29:05AM	12/27/2014 10:29:05AM	12/27/2014 10:29:05AM
L1(1).mp4	01/01/2015 08:14:11PM	01/02/2015 10:13:21AM	01/01/2015 08:19:00PM
k(7).avi	01/03/2015 08:36:29AM	01/03/2015 09:56:02AM	01/03/2015 09:50:0AM
处女 破处 强奸 血腥.mpeg	01/03/2015 08:37:58AM	01/03/2015 08:37:58AM	01/03/2015 10:53:02AM
女西欧阴唇 教师 强奸 潮吹 尿尿 美女 内射 无码 制 .mpg	01/03/2015 08:39:04AM	01/03/2015 08:39:04AM	01/03/2015 10:40:34AM
苏联惹小女孩 （3分钟） （1） 大乳 奶 精品 收藏 无码 穴 女 少妇 强奸 另类 后门 暴 迷药.avi	01/03/2015 08:39:46AM	01/03/2015 08:39:46AM	01/03/2015 10:26:48AM

Table 1

Note the highlighted entries of the above table have identical dates for File Creation Date, File Last Access Date, and File Last Written indicating that it is unlikely that the files were ever opened or viewed.

During the preliminary hearing testimony Trooper James Ford also identified the file sharing software eMule as resident on Mr. Zhao's computer. During his testimony Trooper James Ford stated that the software was important to him because the eMule software was the "… pin to our client – that was the client that was used as the peer-to-peer to share these files." However, neither in the testimony during the preliminary hearing, nor in any of police forensic reports submitted by Pennsylvania State computer examiners Brian Mengel (see documents *1-7 forensic report submitted on June 13 2016.pdf* and *1-15 forensic report submitted on Aug 23 2017.pdf*) or Cpl. G.M. Goodyear (see document *1.pdf*) identify the creation date of the eMule software. Trooper Ford and the two state computer examiners all identified either eMule or eDonkey as the file sharing software, but there is no record of the eMule installation date in any of the reports provided to Ms. Qing Zhao. Per discussions with both Ms. Qing Zhao and Mr. Weiwu Zhao neither stated that they were responsible for downloading and/or installing the eDonkey200, Kademila, or eMule on the computer found by Mr. Zhao.

One would think that if the Pennsylvania State Police would go to the trouble of cataloging and documenting the creation date of any file identified as child pornography, and that they were using the eMule software to pin the use of file sharing software on Mr. Zhao, one would also think that the creation date of the eMule software would also be important. However, since the police did not document the creation date(s) of the file sharing software one can conclude that it is likely that the file sharing software was resident on the computer prior to Mr. Zhao's use.

Even though it is unlikely that Mr. Weiwu Zhao or Ms. Qing Zhao loaded any file sharing software onto the PC Ms. Qing Zhao did install the Microsoft XP operating system (OS) software onto the computer a few days after Mr. Zhao found the discarded computer. Since Mr. Zhao found the computer on either December 30 or December 31, 2014 installation of the Microsoft XP OS would have likely occurred on anytime between January 4 and January 5, 2015. Per a conversation with Ms. Qing Zhao the Microsoft XP OS software replaced the Microsoft Vista software that was resident on the machine at the time of the machine's retrieval. However, when setting up the new OS Ms. Qing Zhao installed the Microsoft XP OS with no login password requirement. This lack of a password requirement enabled anyone who had physical of online access to log into the computer making it susceptible to any illicit use.

It should be noted that the choice to the Microsoft-XP OS is a poor choice with regards to data and computer security. Microsoft-XP is notorious as an OS vulnerable to data hacking, computer intrusion, and unauthorized access and control. The software is so vulnerable that computers loaded with the Microsoft XP OS are often used as targets for cybersecurity students learning the methods and techniques of computer compromise. Industry knowledge regarding the vulnerability of the Microsoft XP OS is also attested to by Young Zhang, Ph.D., an Associate professor of Computer Science at Kutztown University of PA (see document *4-1 professor zhang.pdf*).

Mr. Zhao's router:

Not only was the computer found to be susceptible to unauthorized access, but so was the router used to connect the Zhao computer to the internet. Reportedly Mr. Zhao used a Mercury router to connect his found computer to the internet. A photo of this router's information panel is shown in *Image 1: Zhao family router*.

While much of the text on the router's information panel is in Asian characters the factory default values for the router's Internet Protocol (IP) address, username, and password are clearly visible. These listings inform the owner of the router's default values and provide the owner with a means to configure the router's settings to protect their home network from anonymous or unwanted intrusion.

Usual owner configurable settings provide for home network privacy and add a layer of device protection. These configurable settings include the home network gateway/IP address, the network's Service Set Identifier (SSID), the username, the password, various firewall rules, network access control, as well as other settings. Leaving the IP address, the username, and the password in the factory default setting allows anyone with physical access to the router, or anyone within range of the router's wireless signal an easy method of logging into the router. This access provides the intruder a method to not only compromise the network, but also lists the IP address and the media access control (MAC) address of all devices connected to the network. With both the IP and MAC addresses of the connected devices the intruder has all the information needed to compromise both the network and any unprotected devices (i.e. Mr. Zhao's unprotected computer) connected to the network.

To illustrate how easy it would have been to compromise the Zhao family network an informal test of the network's wireless coverage was conducted. Inside the ground floor of the Zhao's residence the home network SSID was observed as Mercury_23893E. This reading was verified by logging into the router and observing the SSID directly – see *Image 2: Zhao Family Router Login Page*.

The wireless broadcast signal was measured as full strength from within the Zhao residence using a popular smartphone. To test the range of the Zhao's home router five additional signal strength measurements were taken, one at each of the locations indicated on the Google Satellite Image of the Zhao residence, identified by the address 230 West Madison Street as shown in *Image 3: Wireless Signal Strength Test Points.*

Image 1: Zhao family router

home network SSID was observed as Mercury_23893E. This reading was verified by logging into the router and observing the SSID directly – see *Image 2: Zhao Family Router Login Page*.

The wireless broadcast signal was measured as full strength from within the Zhao residence using a popular smartphone. To test the range of the Zhao's home router five additional signal strength measurements were taken, one at each of the locations indicated on the Google Satellite Image of the Zhao residence, identified by the address 230 West Madison Street as shown in *Image 3: Wireless Signal Strength Test Points.*

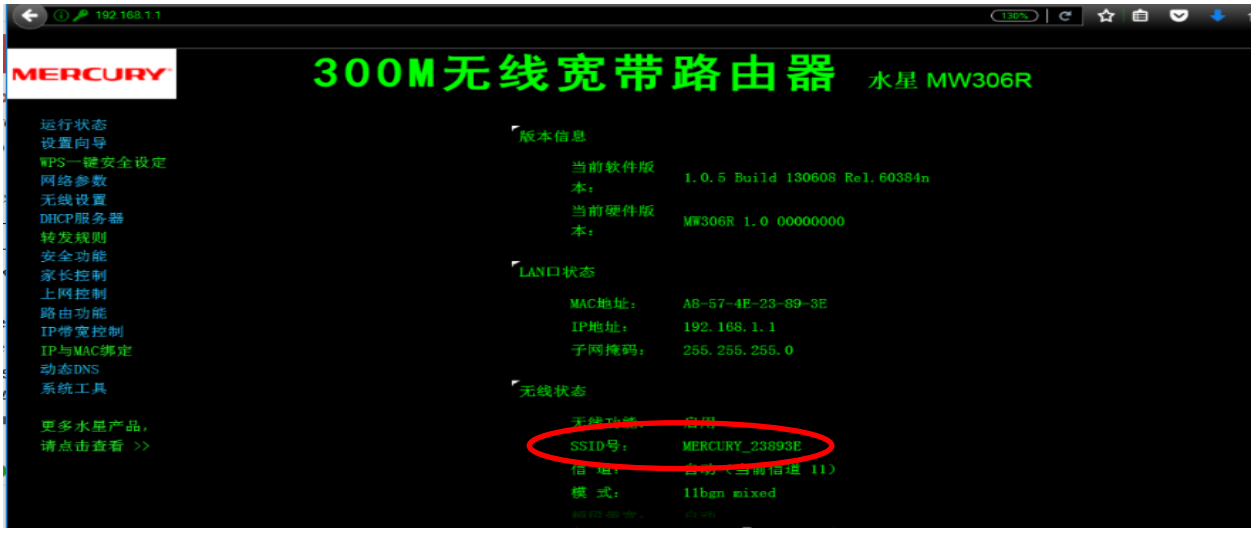

Image 2: Zhao Family Router Login Page

The test point indicated by the numeral 1 is on the street parking area directly in front of the Zhao family house. The wireless signal strength showed no degradation at this location and the network SSID was readable by the same smartphone used when measuring the signal inside the residence. Test points indicated by the numerals 3 and 4 were again taking from the street parking locations directly in front of the houses immediately to the left and right of the Zhao's residence and also showed no wireless signal degradation. As with test point 1 the SSID of the network was also clearly visible at test points 3 and 4.

The test point signified by the numeral 2 was across on the sidewalk directly across the street from the Zhao residence. In contrast to the previous measurements this location showed a degradation of the wireless signal, but only a slight degradation.

The last test point as indicated by the numeral 5 is directly behind the Zhao residence on Orchard Street. The location of this test point is similar to test point 2 with regards to the approximate distance from the Zhao residence and with the signal strength reading. While there was a slight degradation of the strength of the signal the network's SSID was clearly readable.

From all five test points the SSID was clearly visible and the signal strength has ample strength for a network connection. Given the above information it should be apparent that it would have been easy to connect to the router. Additionally, since the router still remained in the factory default configuration with respect to the login IP address, username, and password compromising the router would only require a simple Google search for the default information for the Mercury router. *Image 4: Mercury Router Defaults* shows the results of a Google search for the phrase "Mercury router default username and password". As can be seen the results of the search yield the default username of "admin", the default password of "admin", and the default IP address of 192.168.1.1.

Image 3: Wireless Signal Strength Test Points

Another point of vulnerability to the Zhao family network is their IP address. Ms. Qing Zhao reported that the Zhao family network had kept the same external IP address of 65.78.83.141 for a number of years making the IP address an easier target for a would-be hacker.

With the information of the router's manufacturer available by reading the router's SSID and the default IP address, username, and password taken from the results of the Google search, and an external IP address that remains stable even the most unsophisticated user can is able to login to the router to gain any information needed to easily compromise both the network and any device logged onto the network at any given time.

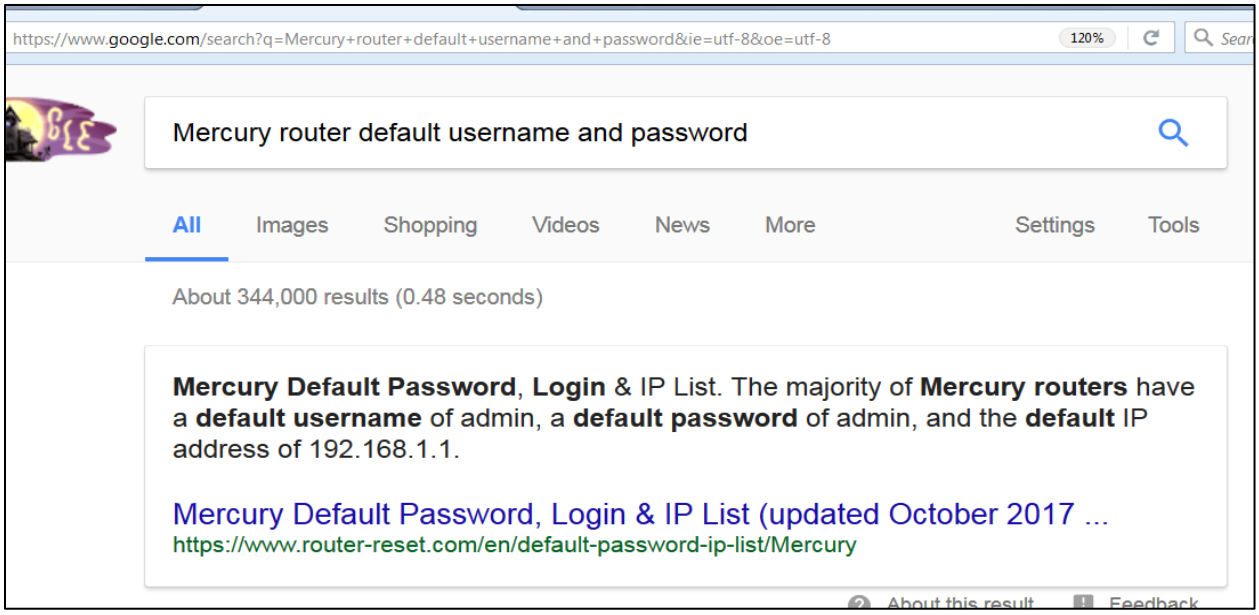

Image 4: Mercury Router Defaults

Physical access to Mr. Zhao's computer:

As discussed with both Mr. Weiwu Zhao and Ms. Qing Zhao, at least four individuals had physical access to Mr. Zhao's computer. These individuals included Mr. Weiwu Zhao, Mr. Zhao's wife, Mr. Zhao's daughter Ms. Qing Zhao, and MS. Qing Zhao's ex-husband, Jason Nicholas Veres. As reported by Ms. Qing Zhao and substantiated by Mrs. Zhao, Mr. Veres not only had physical access to the computer but had used the computer on many occasions. Further, it is reported that Mr. Veres used the computer unattended and while Mr. Zhao was absent. Unattended computer use could easily allow for the downloading and installation of both malicious computer content and provide ample time to reconfigure both Mr. Zhao's computer and the Zhao family router allowing remote access.

Discrepancies of evidence related to Mr. Zhao:

The discrepancies and possible inaccuracies found in the documents provided to Ms. Qing Zhao are very concerning.

Initially Trooper James Ford testified in Mr. Zhao's preliminary hearing on February, 18, 2016 that a total of seven files alleged to be child pornography were located on Mr. Zhao's computer. These file included Preteen-Daphne (Blond Rasta).avi, k7.avi, o(50).avi, o(66).avi, o(70).rmvb, o(65).avi, and a file Trooper Ford identified as file with a Japanese extension created on 1/03/2015 (see file *1-11 preliminary hearing transcript.pdf*). However, a second report dated July 26, 2017 found an additional seven files including L1(20).avi, o(29).mp4, o(81).avi, o(23).gif, L1(1).mp4, and two additional files that include Asian titles. The question must be raised as to why all 14 files were not located during initial analysis of Mr. Zhao's hard drive.

The normal method used by computer forensic analysts is to submit the suspect hard drive to software that will index, catalogue, and list all files on the hard drive. For an unknown and unexplained reason seven files reported on July 26, 2017 were found sometime after the initial files were found and testified to in the February 18, 2016 preliminary hearing.

Additionally, the police have listed a computer and hard drive that does was not confiscated from Mr. Zhao as evidence against him. Page 18 of file *4.pdf*, which is a copy of the Application for Search Warrant and Authorization, dated May 18, 2015, lists Evidence Description of an Acer laptop sn NXM6VAA0013220730C6600, a generic flash drive, a Western Digital external hard drive sn WMC1T0591522, and a Samsung Galaxy phone among other items. However, as recorded in document *1-7 forensic report submitted on June 13 2016.pdf*, investigating office Brian Mengel lists the computer seized and analyzed as a Dell Inspiron sn: BPXZ5J1 and a Western Digital hard drive with sn WMAV25256156. These are obviously two distinct and unique computers and hard drives. However, the question must be asked if files from a different computer were used as evidence against Mr. Weiwu Zhao.

Conclusion:

Mr. Weiwu Zhao is charged with crimes relating to the possession and distribution of child pornography, but as explained in this report he may be a victim of unfortunate circumstances that were either beyond his technical knowledge or beyond his control. While this report does not challenge the finding of child pornography on Mr. Zhao's computer it does offer plausible explanations that may exonerate Mr. Zhao from any wrong doing.

Mr. Zhao found an old discarded personal computer that very likely could have contained images of child pornography on the computer when found. As shown, the creation dates of the CP files used as evidence are prior to the retrieval and use of an abandoned PC by Mr. Zhao. The timeline of events as reported by Ms. Qing Zhao show that it was impossible for Mr. Zhao to have downloaded the CP files as charged.

Mr. Zhao's computer and home network were also extremely vulnerable to attack. Ms. Qing Zhao loaded the Microsoft-XP operating system on the computer approximately eight months after support for the OS ended. In addition to using an operating system that has well-known data security risks, Ms. Zhao also loaded the software without the requirement of a password for use. This left the OS operating on Mr. Zhao's computer totally vulnerable to anyone who had access to the computer.

As discussed in the body of this report multiple people had physical access to the computer including at least one person who was no longer considered a trusted family member. As discussed Ms. Zhao's ex-

husband used the computer on a number of occasions many times while not under the supervision of Mr. Zhao.

In addition to a vulnerable computer and the physical access by a non-family member the Zhao family home network was extremely vulnerable to remote wireless connections. Anyone within close proximity to the Zhao family home had easy and likely total access to the Zhao family network and their devices. This access could have easily been used to compromise Mr. Zhao's computer to be used for the storage and or distribution of child pornography.

There is also the question of discrepancies in the evidence presented by the police. While the police took the time to catalogue and determine the creation times of the CP files, they did not do the same for the file sharing software (i.e. eMule) which they used to download files they claimed were from Mr. Zhao's computer. One possible conclusion for this omission is that the creation time of the eMule software would show that Mr. Zhao is not responsible for its download, installation or use.

Another troubling conclusion to be drawn from the police discrepancies is the lack of consistency with the evidence. The police have reported the seizure of two different computers and hard drives from Mr. Zhao to use evidence against him. From the documents provided as evidence against Mr. Zhao it is difficult to determine what files came from which PC and if any actually came by the PC being used by Mr. Zhao.

Lastly, it must be noted that the defendant's motion to have a 3rd party complete an analysis of the hard drive was denied by the courts. It is likely that if such an analysis could be completed that many of the questions posed by this report could be answered and be used as a legal defense for Mr. Weiwu Zhao.

Appendix A: Case related documents:

The files listed in this appendix maintain the original filename as sent to S2 Forensics, LLC. It is unknown who named each file or the significance of any filename.

1.pdf A collection of police reports regarding the Weiwu Zhao case including a Pennsylvania State Police Incident Report, a Supplemental Investigation Report (2 reports), and a Pennsylvania State Police General Investigation Report – Request for assistance (Forensic Services)

1-4 search warrant submitted on Apr 21 2015.pdf An application for search warrant and Authorization to seize and examine all computer and computer related items from the residence Weiwu Zhao

1-7 forensic report submitted on June 13 2016.pdf Forensic examination synopsis report dated 05/20/2015 for forensic investigation of computer seized from Weiwu Zhao's home

1-8 police criminal complaint submitted on Dec 8 2015.pdf A copy of the Police Criminal Complaint Commonwealth of Pennsylvania vs. Weiwu (NMN) Zhao.

1-9 incident report submitted on Aug 23 2017.pdf A police incident report for incident no. X43-50966 including the description of the incident history

1-11 preliminary hearing transcript.pdf Transcript of the preliminary transcript taken on February 18, 2016, Commonwealth of Pennsylvania vs. Weiwu Zhao, OTN # T730555-0.

1-13 forensic report submitted on Dec 20 2016.pdf Document titled Zhao Report and listed as Exhibit "A" to Attorney Santos sent by the state police analyst via the Assistant District Attorney Anthony L. Casola The document lists seven files identified as CP Video with the file name, Modified, Accessed and Created (MAC) times, file status – deleted, logical size, physical; size and location path. This file looks to be identical to file a1.pdf listed above.

1-15 forensic report submitted on Aug 23 2017.pdf Request for further examination of item seized

2.pdf Forensic Analysis Worksheet Document lists the Model numbers and serial numbers of the PC and hard drive seized from Weiwu Zhao

2-15.docx: Defendant's pre-trial motion, Commonwealth of Pennsylvania v. Weiwu Zhao No.: CP-48-CR-665-2016

3.pdf Police Criminal Complaint including an Affidavit of Probable Cause Formal complaint against Weiwu Zhao

4.pdf Application for Search Warrant and Authorization, dated April 20, 2015

4-1 professor zhang.pdf Letter written by Professor Young Zhang, Ph.D. on behalf of Mr. Weiwu Zhao stating the conditions of his PC seized by the police.

5.pdf Request from police and response from RCN Telecom Services, LLC Case #AP8761 regarding subscriber information for customer records of an IP Address of 65.78.83.141 assigned to account of Ms. Qing Zhao at 230 W. Madison St, FL 1, Easton, PA 18042

5-1 facebook published by defendant's enemy on Nov 20 2014.pdf Three pages of Facebook conversations and photos of toddler girls. Facebook conversation includes narration by Qing Zhao's ex-mother-in-law bemoaning not having access to her granddaughters.

5-11.pdf A chart showing the "Relationship Network among Facebook People and the legal officials involved.

6.pdf A letter from the Commonwealth of Pennsylvania Office of Inspector General to Colonel Tyree C. Blocker of the Pennsylvania State Police forwarding the Referral of Complaint 15-0496-C made by Ms. Qing Zhao outlining the charges of corruption against the Pennsylvania State Police.

7.pdf Arrest data of Weiwu Zhao dated April 11, 2016

7-4.pdf A denial of the three motions to "compel forensic report of computer filed in September of 2016, as well as the motion to compel discovery investigation into the notes of Trooper Ford, … and the defendant's pro se motion to unseal records filed on or about August 31, 2017

8-1.pdf Supplemental Investigation Report regarding incident X43-0050966 for the offense of Sexual Abuse of Children including the narrative of investigative actions taken between 12/07/2015 and 7/20/2017

8-2.pdf This file is a collection of 3 photos of toddlers, assumed to be the two children of Ms. Qing Zhao.

10.pdf An Encase evidence examination report listing the forensic image MD5 hash values, a photo of an airline ticket for a flight on Continental Airlines, and file listing (including file name, hard drive path location, MAC times, and hash values for some, but not all the evidence files) for some, but not all, the files used as evidence against Mr. Weiwu Zhao

a1.pdf Document titled Zhao Report and listed as Exhibit "A" to Attorney Santos sent by the state police analyst via the Assistant District Attorney Anthony L. Casola The document lists seven files identified as CP Video with the file name, Modified, Accessed and Created (MAC) times, file status – deleted, logical size, physical; size and location path.

a2.pdf A second copy of the Encase report. The file appears identical to file 10.pdf, but a test for file uniqueness was not conducted

a3.pdf A copy of the slide show that the prosecutor planned on using during the trial of Mr. Weiwu Zhao.

a4.pdf preliminary hearing transcript The transcript of the preliminary hearing of the Commonwealth of Pennsylvania vs. Weiwu Zhao, Defendant – OTN # T730555-0 and conducted on February 18, 2016 in the office of Magisterial District Judge Daniel Corpora

a4.pdf A copy of the supplemental report of the police investigation into Case Number 665-2016 against Mr. Weiwu Zhao dated October 27, 2017 sent to Mr. Zhao

a5.pdf A copy of the ECD Technical Assistance Request report from the National Center for Missing and Exploited Children provided to the Commonwealth of Pennsylvania on the morning of October 26, 2017 and provided to Mr. Weiwu Zhao

CD screenshot 1.png, CD screenshot 2.png, CD screenshot 3.png Screenshots showing the contents of three CD of files provided by the Commonwealth of Pennsylvania in support of the case again Mr. Weiwu Zhao

D-13.pdf A copy of the three pages of Facebook postings, conversations and photos of two toddler girls. The Facebook conversation includes the narration by Qing Zhao's ex-mother-in-law bemoaning not having access to her granddaughters

D-53.docx A collection of statements with purported evidence accusing the Pennsylvania State Police and the "Facebook People" (a term used by Mr. Weiwu Zhao in reference to the

family of her ex-husband, Jason Nicholas Veres) of collision and "… having a conflict of interest with Defendant to lie and falsify the evidence in order to falsify case facts."

list.pdf List of items of discovery sent to Attorney Gamburg on August 23, 2017

nature of weiwu zhao case 10172017.docx Summary of strategy for Weiwu Zhao case.

Router weiwu zhao home.jpg A photo of the home router used by Weiwu Zhao and family.

Syslog.txt A copy of the log files taken from the Zhao family router showing a brief logging of events dated 2002-01-01 8:47:33 2858s. It is unknown and very doubtful if the time/date stamp of the log file was accurate.

65.78.83.141_56663_PA_Easton A collection of compressed log files showing the attempts, failures, and downloads from the IP address 65.78.83.141, which is the IP address associated with the Zhao family home. The individual file names are not listed in thos appendix

CD 2 The file structure including the files and folders of CD 2 are displayed below:

```
CD 2
|  X43A5-8668 FORD - GI.pdf
|  X43A5-8668 FORD Digital Forensic Worksheet 2.pdf
|
├──Encase Report
|  |  frame view.html
|  |  gallery.html
|  |  toc.html
|  |  X43A5-8668 Item 1 Report.html
|  |
|  └──X43A5-8668 Item 1 Report_files
└──HTML Export 2015-05-18_06-14-35
   |  index.html
   |
   ├──Resources
   |  |  front.html
   |  |  jquery-2.1.1.min.js
   |  |  jquery.floatThead.js
   |  |  jquery.tablesorter.js
   |  |  Logo.png
   |  |  respond.js
```

```
|   |   script.js
|   |   style.css
|   |   style_eo_pdf.css
|   |   style_print.css
|   |   toc.html
|   |
|   └──images
|           asc.gif
|           desc.gif
|           printer_white.png
|           sort.gif
|
└──Webpages
      Emule Known.met Records.html
      Emule StoredSearches.met Records.html
```

CD 3 The file structure including the files and folders of CD 3 are displayed below:

```
CD 3
|   X43A5-8668 FORD Zhao Supplemental Digital Forensic Worksheet.pdf
|   X43A5-8668 FORD Zhao Supplemental GI.pdf
|
├──X43A5-8668 Encase 8 Supplemental Report
|   |   X43A5-8668 FORD Zhao EnCase Report.html
|   |
|   └──Links
|           2a269c052cc01c409dd008cf6033a353.jpg
|           d5ee7d28ca0a044ca52d1d54c612d11c.jpg
|           e90da64cdbffbd8188a212c1781752d0.jpg
|
└──X43A5-8668 FORD Zhoa IEF supplemental report
    |   index.html
    |
    ├──Resources
    |   |   front.html
    |   |   jquery-2.1.1.min.js
    |   |   jquery.floatThead.js
    |   |   jquery.tablesorter.js
    |   |   Logo.png
    |   |   respond.js
    |   |   script.js
```

```
|   |   style.css
|   |   style_eo_pdf.css
|   |   style_print.css
|   |   toc.html
|   |
|   └───images
|           asc.gif
|           desc.gif
|           printer_white.png
|           sort.gif
|
└───Webpages
    |   EML(X) Files.html
    |   Facebook URLs.html
    |   Identifiers.html
    |   Outlook Webmail Inbox.html
    |   Skype Accounts.html
    |
    └───Fragments
            File0.htm
            File1.txt
            File2.jpeg
            File3.jpeg
```