

Digital Forensics Report

August 20, 2023

Executive Summary

On July 12, 2023, Campbell Forensics LLC was contracted by P&G Law to provide forensics on two internal hard drives. The digital forensics examination aimed to determine if the devices contained any artifacts supporting the dissolution of marriage for client Winnifred Cynthia Campino. The digital forensics process was also to discover any possible hidden assets for property distribution.

Based on the digital forensics examination of both devices, some evidence may support the dissolution of the marriage. This evidence is in the form of pictures, websites, and voice messages on the devices. There is minimal evidence to support hidden assets. This report will provide details on the relevant artifacts and the methods to obtain the requested evidence.

Background

P&G Law is representing Winnifred Cynthia Campino in a marriage dissolution case. Ms. Campino co-owns a business with her husband, James Wilson Campino. Ms. Campino presented two internal hard drives to the P & G Law firm. The hard drives were removed from a home office closet. Ms. Campino stated that the hard drives were stored as part of information technology upgrades to the couple's business. It has been approximately ten years since the upgrades. Mr. and Mrs. Campino shared login credentials to make it easier to access business documents.

Digital Forensics Process

The following details the digital forensics process used by Campbell Forensics, LLC. The framework used is discussed to ensure the methodology meets the Daubert standard. The

extraction and processing are also discussed to allow a third party to recreate the process.

Finally, the examination and evidence are provided to support the P&G Law firm's efforts in the Campino vs. Campino marriage dissolution case.

Framework

The Digital Forensic methodology utilized is provided by the National Institute of Justice (NIJ) Forensic Examination of Digital Evidence: A Guide for Law Enforcement and the Department of Justice Computer Crime and Intellectual Property Section Computer Crime Lab. The primary methods utilized are evidence assessment, acquisition, and examination (National Institute of Justice, 2004).

Initial Contact and Intake

P & G Law Firm contacted Jonathan Campbell of Campbell Forensics, LLC, to investigate two internal hard drives they had in their possession. Paul Jones of the P & G Law Firm personally provided the internal hard drives at the Campbell Forensics LLC, place of business on July 12, 2023, at 15:15. Chain-of-Custody documents were completed, and the hard drives were received by the digital forensic analyst, Jonathan Campbell. Mr. Campbell then moved the hard drives into a secure, clean laboratory location for processing.

Evidence Assessment

The evidence assessment is based on the NIJ digital forensic guidelines. The policy for the evaluation is primarily associated with Kentucky laws and defining the scope of the investigation. Since the hard drives were delivered to Campbell Forensics, LLC, no site assessment was required by the digital forensic team.

Legal Background

To ensure the scope of the investigation is appropriately defined, Kentucky rules for marriage dissolution, property distribution, and evidence in court are provided. Also provided are issues related to the 4th Amendment regarding privacy.

Kentucky Rules for Marriage Dissolution

Chapter 403 of the Kentucky revised statutes (Kentucky General Assembly, 2023a) contains the rules governing the dissolution of marriage. Rule 403.140 (Kentucky General Assembly, 2023a) states that the Circuit Court can enter a degree of dissolution if one party resides in the state, the marriage is irretrievably broken, and child custody provisions have been made. Under rule 403.170 (Kentucky General Assembly, 2023b), irretrievable breakdown is defined. If one of the parties denies an irretrievable breakdown, the court can consider evidence supporting it. Under rule 403.170, no decree of dissolution of marriage is granted until the "*parties have lived apart for 60 days*". Rule 403.050, divorce from bed and board, can speed up the dissolution of marriage. The *Bed and Board* is a separation option in abuse, adultery, or mistreatment situations.

Adultery is not a crime in Kentucky; therefore, it cannot be used in the disposition of property. However, it can be considered in the court decreeing a dissolution of marriage due to an irretrievable breakdown. Rule 403.190 (Kentucky General Assembly, 2023c) provides for the disposition of property. The rule states the court shall "*divide the marital property without regard to marital misconduct.*" Rule 403.190 also states that relevant factors in property distribution include:

- "*Contribution of each spouse to the acquisition of the marital property, including the contribution of a spouse as a homemaker.*"
- "*Value of the property set apart to each spouse.*"

- *"Duration of the marriage."*
- *"Economic circumstances of each spouse when the property division is to become effective."*

Kentucky Rules on Evidence

Rule 401 Relevant evidence (Kentucky General Assembly, 2023) defines evidence as *"having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."* In other words, the evidence presented must support or disprove claims by a spouse in a dissolution of marriage case. Rule 702, Testimony by experts, states that evidence must be provided and analyzed using sound scientific methods, and the expert witness must have the experience, knowledge, and education to support the findings (Kentucky General Assembly, 2023e). Three conditions must be met under the Kentucky statutes Rule 702 (Kentucky General Assembly, 2023e). These conditions are:

1. *"The testimony is based upon sufficient facts or data."*
2. *"The testimony is the product of reliable principles and methods."*
3. *"The witness has reliably applied the principles and methods to the case facts."*

As we can see from the above conditions, sound digital forensics methodology must be applied to present the evidence in court.

One factor that may limit an investigation is the expectation of privacy. While a spouse can use evidence retrieved from a shared computer, they cannot use evidence found on a spouse's password-protected device. According to the Association of Certified E-Discovery Specialists (2022), permission must be received from the device's owner to search for a password-protected device, or there must be a court order.

Scope

Based on the marriage dissolution rules, artifacts that support Rule 403.170 regarding irretrievable breakdown to include evidence of an alternative lifestyle, such as infidelity, were analyzed. Regarding Kentucky rule 403.190 property distribution, an analysis of artifacts associated with property to include unknown spouse finances was performed. Finally, to support Kentucky Rules 103, 401, and 703 regarding evidence, sound digital forensics methodology was used based on the National Institute of Justice digital forensics guidelines for law enforcement.

Evidence Acquisition

The following steps were taken to identify and acquire the device images for digital forensic analysis. The acquisition steps are based on the NIJ digital forensics guideline for law enforcement. Digital forensic platforms and tools are also identified.

Identification

To ensure that the devices are correctly identified for digital forensic purposes, the devices were annotated correctly on the Chain-of-custody forms. Table 1 provides the identification information for each device acquired and examined for artifacts associated with the case.

Table 1

Device Identification Information

Identification	Device 1	Device 2
Make	Hitachi	Seagate
Model	DK23EA-40	ST380013 AS
Serial Number	2Y460159PC0CY2	3MR04728

Interface Type	2.5 IDE	3.5 SATA
Capacity	40 Gigabytes	80 Gigabytes
Drive Type	Spinning	Spinning
(Spinning/SSD/USB)		

Note: The table displays information associated with devices that were investigated

Preparation

To prepare for the acquisition and analysis of the hard drive images, an Apple MAC model A2141 was installed with VMWare Fusion version 12.2.5. Fusion was used to install a Windows SANS Investigative Forensic Toolkit (SIFT) virtual machine. The resources given to the virtual machine consisted of 32 gigabytes of RAM, six core processes, and 500 gigabytes of hard disk space. A WeibeTech Forensic Ultradock was also prepared to ensure no data would be written to the original hard drives. Table 2 details the platforms and tools used for acquisition and analysis.

Table 2

Tools and Platforms for Digital Forensic Investigation

Platform/Tool	Version/Manufacturer	Description
Host Workstation	macOS 13.4.1/Apple	Primary workstation. 64GB RAM. 4TB SSD. i9 Core
Forensic Ultradock	V5.5/WeibeTech	Write blocker used to image drives and ensure no changes are made to original devices.

VMware Fusion	v12.2.5/VMware	Virtual platform to provide resources for SIFT
Windows SIFT	SANS/Microsoft	Virtual Machine providing digital forensics tools
FTK Imager	Exterro	Image creation for hard drives
Axiom	Magnet	Evidence processing and analysis
RegRipper	Eric Zimmerman	Registry processing and analysis
Browsing History Viewer	Nirsoft	Browser history examination
Kernel OST Viewer	v21.1/nucleustechnologies.com	Outlook email examination
Arsenal Image Mounter	v3.9.223/Arsenal Recon	Mount HD image as Windows share

Note: The table displays information about the tools and platforms used to perform the digital forensics investigation.

Acquisition Methods

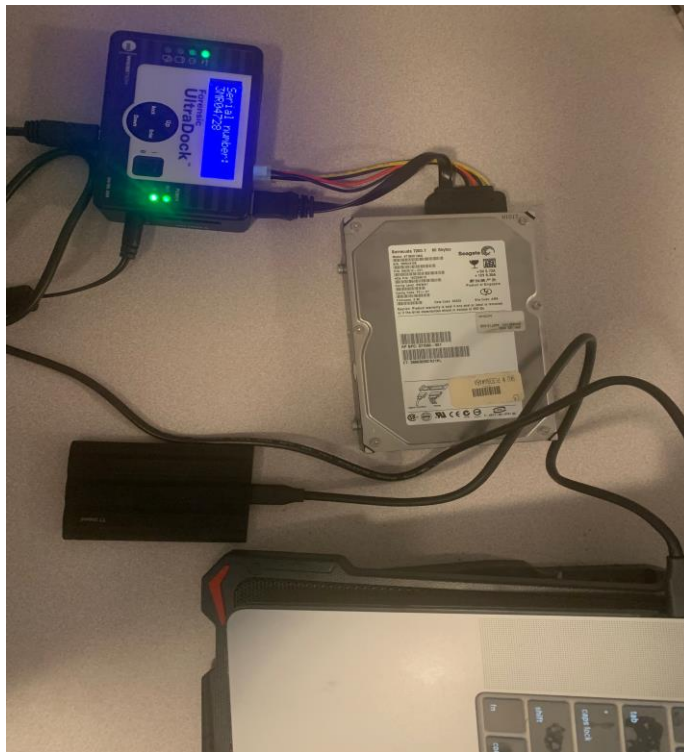
The following describes the steps to acquire the images from the hard drives. The acquisition methods include configuring the digital forensic workstation, implementing write blockers, hashing the images, and storing the images.

FTK Imager Acquisition Steps

To ensure that changes are not made to the hard drives, a WiebeTech Forensic UltraDock write blocker was used, as seen in Exhibit 1. The hard drive is connected to the write blocker's SATA port. The write blocker is then connected to the Apple macOS host. Turning on the write blocker, we see that the display provides information about the connected hard drive.

Exhibit 1

Physical Configuration for Digital Forensics Imaging



The Windows SIFT digital forensics virtual platform was configured with 32 gigabytes of random access memory (RAM) and six CPU cores, ensuring enough resources were available to process and analyze evidence. As seen in Exhibit 2, the WiebeTech write blocker is connected to the Windows SIFT platform along with two Samsung T7 external SSD drives. One T7 drive was used to store the images, and the second Samsung T7 device was used to store the processed evidence.

Exhibit 2

WiebeTech Device Connection to Windows SIFT



Once the devices were connected, FTK Imager was used to image both hard drives into a .E01 format. The .E01 format efficiently creates multiple image files and stores the metadata associated with the imaging process. A physical image of the hard drives was performed to ensure that all data was collected. Table 3 provides the metadata associated with the hard drives and images supplied by FTK Imager.

Table 3

FTK Imager Computed and Verified Hashes

Metadata	HITACHI DK23EA-40	SEAGATE ST380013 AS
Computed MD5	19602baf98063cc6d445d5e831743673	a2b7c1d18de93e84a4b7f0e5cd2b9583
Computed SHA1	5e7681e009315b87081b9c06a1f05688	6ca881ca3d481b777ee0ac74ecd06016
Verified MD5	586bde13	59285a65
Verified MD5	19602baf98063cc6d445d5e831743673	a2b7c1d18de93e84a4b7f0e5cd2b9583

Image	5e7681e009315b87081b9c06a1f05688	6ca881ca3d481b777ee0ac74ecd06016
Verified	586bde13	59285a65
SHA1		

Evidence Examination

The evidence examination section describes in detail how the evidence was processed and analyzed based on the scope of the digital forensic investigation. A variety of tools were used. Multiple tools were used to examine like data for validation. A timeline of events associated with the analysis was also developed to explore a possible pattern of behavior.

Processing Methods

Multiple processing methods were utilized to examine the evidence. The first processing method used Magnet Axion Process to select and explore the evidence to be examined. The second processing method was to mount the two device images as virtual drives for validation. Multiple tools were used to validate the Windows Registry, Email, and Browser History.

Processing Goals

Processing goals were defined based on the investigation scope. To provide evidence to support a dissolution of marriage, various media types such as audio, video, and pictures were processed to examine suspect behavior related to extramarital activity. Web browser data was also processed to examine evidence related to patterns of behavior associated with extramarital and financial activity. Documents were also processed for examination of possible financial activity. Finally, the Windows registry was processed that could provide evidence of activity associated with external devices, network shares, document activity, and user activity.

Magnet Axiom was used to process all data within partitioned and unpartitioned spaces to ensure all evidence was available for examination. As seen in Exhibit 3, unallocated space, volume shadow copy, hiberfil.sys, file slack space, and the pagefile.sys were processed for examination. Each one of these areas provides evidence that may have either been hidden or deleted.

Exhibit 3

Example of Magnet Axiom Drive Search Parameters

EVIDENCE SOURCES

The screenshot shows the 'EVIDENCE SOURCES' window in Magnet Axiom. It has a title bar 'WINDOWS' and a subtitle 'SELECT SEARCH TYPE'. Below this is a table with two columns: 'Source location' and 'Search type'. The first source is 'DivorceCase.E01 - Partition 1 (Microsoft NTFS, 37.25 GB)', which is expanded to show a list of search types: 'pagefile.sys / swapfile.sys', '\$LogFile', '\$MFT', 'All files and folders', 'Volume Shadow Copy', 'Unallocated space', 'File slack space', 'hiberfil.sys', and 'Uninitialized file area'. The second source is 'DivorceCase.E01 - Unpartitioned space', which is also expanded to show 'Unpartitioned space'.

Source location	Search type
DivorceCase.E01 - Partition 1 (Microsoft NTFS, 37.25 GB)	pagefile.sys / swapfile.sys
	\$LogFile
	\$MFT
	All files and folders
	Volume Shadow Copy
	Unallocated space
	File slack space
	hiberfil.sys
	Uninitialized file area
DivorceCase.E01 - Unpartitioned space	Unpartitioned space

The artifact process selection was then performed. All possible artifacts were selected for processing to ensure the scope of the investigation was complete. Exhibit 4 displays the types of artifacts available for processing by Magnet Axiom. The memory artifact was not selected because no memory evidence file was available for processing.

Exhibit 4

Magnet Axiom Artifact Selection

SELECT ARTIFACTS TO INCLUDE IN CASE

COMPUTER ARTIFACTS

[CLEAR ALL](#)

☒ ADDITIONAL SOURCES (4 of 4)

☒ APPLICATION USAGE (7 of 7)

☒ CLOUD STORAGE (6 of 6)

☒ COMMUNICATION (39 of 39)

☒ CONNECTED DEVICES (9 of 9)

☒ CUSTOM ARTIFACTS (5 of 5)

☒ DOCUMENTS (17 of 17)

☒ EMAIL & CALENDAR (14 of 14)

☒ ENCRYPTION & CREDENTIALS (5 of 5)

☒ LOCATION & TRAVEL (1 of 1)

☒ MEDIA (13 of 13)

☐ MEMORY (0 of 21)

☒ OPERATING SYSTEM (71 of 71)


☒ PEER TO PEER (11 of 11)


☒ SOCIAL NETWORKING (9 of 9)


☒ VOLATILE ARTIFACTS (1 of 1)


☒ WEB RELATED (19 of 19)


ALL COMPUTER ARTIFACTS


☒  \$LogFile Analysis
Operating System

☒  AIM
Communication

☐  API Hooks (ap
Memory
OPTIONS

☒  Apple Keychain
Encryption &
OPTIONS

☒  Ares
Peer to Peer

☒  Bebo
Social Network

Overall, the Hitachi 40-gigabyte hard drive image took 3.5 hours to complete processing. The Seagate 80-gigabyte hard drive image, completed processing in approximately 12 hours. Once both images were processed, Arsenal Image Mounter was used to mount the images as local drives for manual examination.

Analysis

Once all artifacts were processed for examination, Magnet Axiom Examiner was used to perform the initial analysis. As seen in Table 4, numerous artifact categories were discovered on both device images. The analysis addresses the who, what, where, and when of the discovered evidence (Computer Crime and Intellectual Property Section, 2007) The focus of the analysis was on artifacts that supported the scope of the investigation.

Table 4

Magnet Axiom Artifact Count

Artifacts	40G	80G
Web Related	48,523	29,027
Communication	272	343
Social Networking	2	1
Media	25,565	99,573
Email & Calendar	131	280,853
Documents	2771	12,043
Additional Sources	22	30
Peer to Peer	0	2
Cloud Storage	0	1
Application Usage	321	441
Operating Systems	1,194,212	120,771
Encryption & Credentials	23	381
Connected Devices	47	77
Location & Travel	21	12
Custom	193	3090

Both device images were mounted using Arsenal Image Mounter. RegRipper was then used to extract both images' software hives to discover the installed operating system. Exhibit 4 shows the Hitachi 40-gigabyte hard drive operating system product name and build as Microsoft Windows XP Service Pack 2. Exhibit 5 shows the exact product name and build on the Seagate 80-gigabyte hard drive; however, the patch level differs based on the BuildLab value.

Exhibit 4

RegRipper Hitachi 40G Hard Drive Product Name Output

```
Microsoft\WBEM\CIMOM
LastWrite Time 1980-01-04 05:05:40Z

Autorecover MOFs: C:\WINNT\system32\WBEM\cimwin32.mof C:\WI
-----
winver v.20200525
(Software) Get Windows version & build info

ProductName             Microsoft Windows XP
CSDVersion              Service Pack 2
BuildLab                2600.xpsp_sp2_gdr.090206-1233
RegisteredOrganization  FirstHe
RegisteredOwner         Authorized User
InstallDate             2004-05-10 20:13:39Z
-----
wow64 v.20200515
(Software) Gets contents of WOW64\x86 key

WOW64
Microsoft\WOW64\x86 not found.
Microsoft\WOW64\arm not found.
-----
```

Exhibit 5

RegRipper Seagate 80G Hard Drive Product Name Output

```
-----
winver v.20200525
(Software) Get Windows version & build info

ProductName             Microsoft Windows XP
CSDVersion              Service Pack 2
BuildLab                2600.xpsp_sp2_gdr.100216-1441
RegisteredOrganization  FirstHe
RegisteredOwner         Authorized User
InstallDate             2008-02-07 16:57:18Z
-----
wow64 v.20200515
(Software) Gets contents of WOW64\x86 key

WOW64
Microsoft\WOW64\x86 not found.
Microsoft\WOW64\arm not found.
-----
wsh_settings v.20200517
(Software) Gets WSH Settings

Microsoft\Windows Script Host\Settings
Key LastWrite: 2005-02-14 19:34:05Z
DisplayLogo      1
ActiveDebugging  1
SilentTerminate  0
UseWINSAFER      1

Analysis Tip: If Remote value is set to 1, system may be WSH Remoting target
-----
```

Next, we wanted to discover a timeline of usage for both devices. Utilizing Magnet Axiom, timelines for both devices were constructed. The browser activity was measured since web browsers are the most active application on Windows clients. Exhibit 6 shows that the primary web browsing activity for the Hitachi 40-gigabyte drive occurred between January 2004 and May 2009.

Exhibit 6

Browser Timeline of Hitachi 40G drive

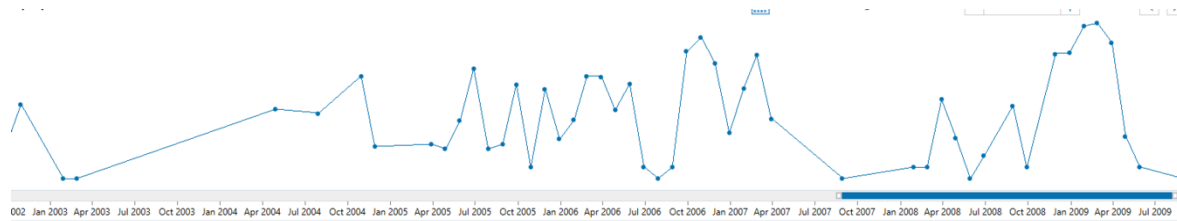
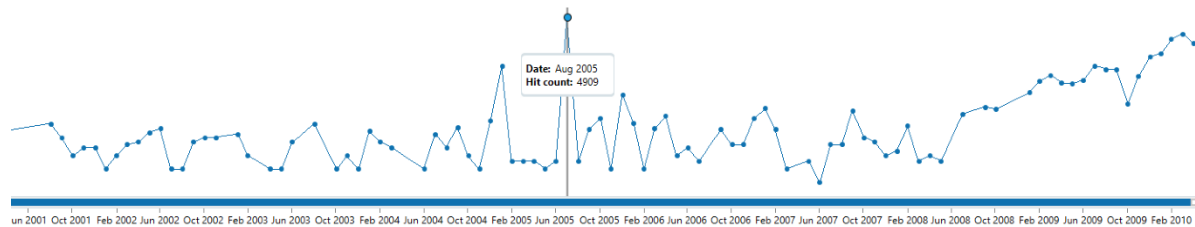


Exhibit 7 shows the browser activity for the Seagate 80-gigabyte drive. Here, we see the most activity in August 2005, but we also see a steady increase in browser activity between June 2008 and March 2010. Both Exhibit 6 and Exhibit 7 show that the devices were taken offline or replaced in the years 2009 and 2010.

Exhibit 7

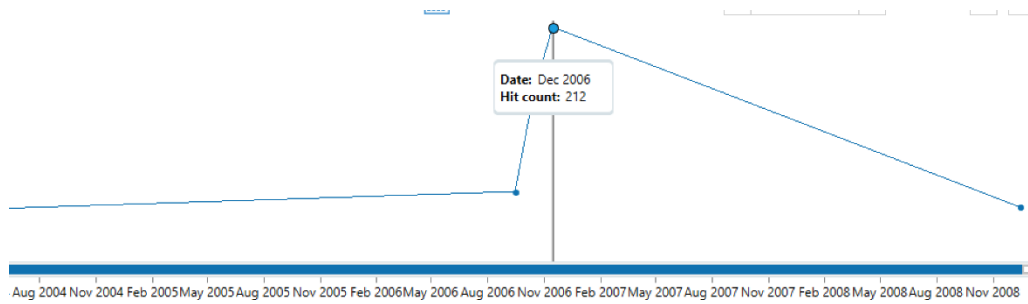
Browser Timeline of Seagate 80G Drive



Email activity was then measured on both devices. In Exhibit 8, we see most of the email activity on the Hitachi 40-gigabyte drive occurring in December 2006; a gradual decline follows this in email activity.

Exhibit 8

Email Activity Timeline of Hitachi 40G Drive



The Outlook OST file is accessed for analysis using the Kernel OST Viewer tool. Exhibit 9 displays the Email client as it would appear on the original device. As seen in Exhibit 9, most of the email activity occurred in December 2006. The emails appear to be business related.

Exhibit 9

Outlook .OST File Located on Hitachi 40G Drive

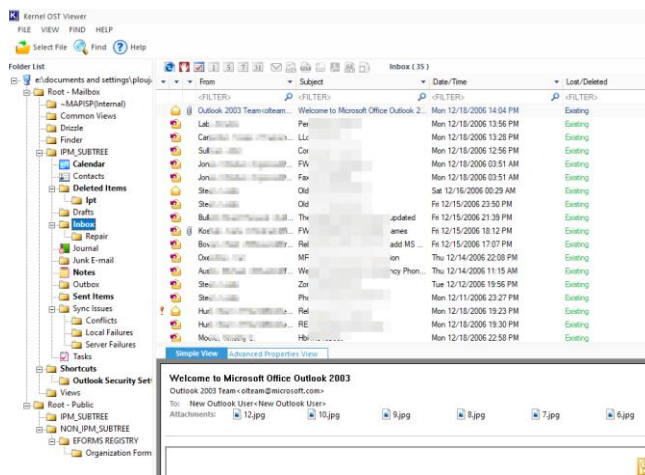
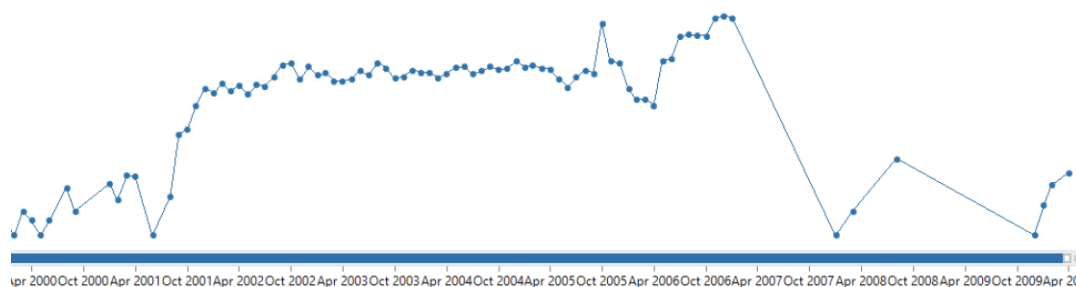


Exhibit 10 displays the email activity on the Seagate 80-gigabyte drive. We see a longer timeline for activity between October 2001 and May 2007. This timeline of email activity is contrary to the timeframe of browser activity. As email activity decreases, browser activity increases. We discovered that the user used a Thunderbird email client. A hypothesis for this explanation could be the user switching to a browser-based email client instead of a locally installed one.

Exhibit 10

Email Activity Timeline of Seagate 80G Drive



We also discovered voice messages within emails. These voice messages appear as attachments where the sender is Unity Messaging System. The Unity Messaging System is a voicemail product manufactured by Cisco and may be the business voicemail system. Exhibit 11 displays the outcome of a Magnet Axiom Unity Messaging filter on email artifacts.

Exhibit 11

Magnet Axiom Email Filtering of Seagate 80G Drive

Camp	"Unity Messaging System - UNITY-1"	2/23/2007 2:49:50 AM	Message from an
Camp	"Unity Messaging System - UNITY-1"	2/24/2007 4:24:44 AM	Message from 911
Camp	"Unity Messaging System - UNITY-1"	2/23/2007 11:47:33 PM	Message from 911
Camp	"Unity Messaging System - UNITY-1"	2/22/2007 1:20:25 AM	Message from 671
Camp	"Unity Messaging System - UNITY-1"	7/19/2006 1:42:04 AM	Message from on
Camp	"Unity Messaging System - UNITY-1"	2/25/2004 12:30:59 AM	Message from an
Camp	"Unity Messaging System - UNITY-1"	9/19/2006 12:03:17 AM	Message from 911
Camp	"Unity Messaging System - UNITY-1"	11/25/2006 1:39:43 AM	Message from 911
Camp	"Unity Messaging System - UNITY-1"	11/25/2006 9:04:14 PM	Message from 331
Camp	"Unity Messaging System - UNITY-1"	11/25/2006 8:48:37 PM	Message from 30
Camp	"Unity Messaging System - UNITY-1"	11/25/2006 7:52:38 PM	Message from an
Camp	"Unity Messaging System - UNITY-1"	11/27/2006 11:50:45 PM	Message from an
Camp	"Unity Messaging System - UNITY-1"	11/20/2006 11:30:48 PM	Message from 331
Camp	"Unity Messaging System - UNITY-1"	11/20/2006 10:36:27 PM	Message from 911
Camp	"Unity Messaging System - UNITY-1"	11/17/2006 9:46:13 PM	Message from 331
Camp	"Unity Messaging System - UNITY-1"	11/15/2006 3:32:18 AM	Message from 80
Camp	"Unity Messaging System - UNITY-1"	11/14/2006 8:56:58 PM	Message from 331
Camp	"Unity Messaging System - UNITY-1"	11/13/2006 10:05:40 PM	Message from 911
Camp	"Unity Messaging System - UNITY-1"	11/10/2006 2:09:52 AM	Message from 911
Camp	"Unity Messaging System - UNITY-1"	11/10/2006 2:01:54 AM	Message from 331
Camp	"Unity Messaging System - UNITY-1"	11/5/2006 6:18:39 PM	Message from 25
Camp	"Unity Messaging System - UNITY-1"	11/9/2006 11:14:57 PM	Message from on
Camp	"Unity Messaging System - UNITY-1"	12/22/2006 1:10:03 AM	Message from 911
Camp	"Unity Messaging System - UNITY-1"	12/21/2006 11:09:11 PM	Message from 911

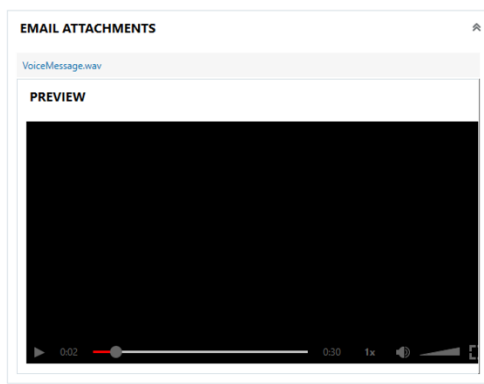
Upon further analysis of the voice messages, a suspect voice message was found, as shown in Exhibit 12. The voice message contains a female voice. The voice message was

received on November 28, 2006, with a UTC timestamp of 8:48:37 PM. The following is a transcript of the message.

Are we still on for the Cricket Inn tonight at seven? I sure hope so. I have a special surprise for you. See you tonight.

Exhibit 12

Email Voice Message Attachment Seagate 80G Drive



Note: The location of the voice message is "Documents and Settings\campjw\Application Data\Thunderbird\Profiles\kgh88r0j.default\Mail\Local Folders\Outlook Mail.sbd\Personal Folders.sbd\overage"

Expanding our analysis, we began to focus on web browser activity. Exhibit 13 focused on financial activity and any activity showing possible extramarital affairs. Magnet Axiom did discover artifacts associated with this activity, but not in browser history. The activity was found in the pagefile.sys file and an Adobe Distiller log file. The pagefile.sys contains items moved from memory to more efficiently utilize the random-access memory (RAM) (Said et al., 2011). Adobe Distiller can be used to convert files or pages to PDF format.

Exhibit 13

Magnet Axiom Seagate 80G Drive Browser Activity

Site...	URL	Date...	Artifact	Artifact type	Source
Friend Finder	http://adulthoodfinder.com/go/g664880...		Potential Browser Activity	Dating Sites URLs	DivorceCase0010.E01 - Partition 1 (Microsoft NTFS, 74.53 GB)\pagefile.sys
Friend Finder	http://adulthoodfinder.com/search/p360...		Potential Browser Activity	Dating Sites URLs	DivorceCase0010.E01 - Partition 1 (Microsoft NTFS, 74.53 GB)\pagefile.sys
Friend Finder	http://adulthoodfinder.com/go/p73081		Potential Browser Activity	Dating Sites URLs	DivorceCase0010.E01 - Partition 1 (Microsoft NTFS, 74.53 GB)\pagefile.sys
eHarmony	http://www.eharmony.com/singles/servle...		WebKit Browser Web History (Carved)	Dating Sites URLs	DivorceCase0010.E01 - Partition 1 (Microsoft NTFS, 74.53 GB)\Documents and Settings\campjw\Appl...

Exhibit 14 displays the Adobe Distiller log file. The source file is the eharmony.com website. The destinations are two generated PDF files. The generation of the PDFs occurs within a few minutes of each other and may indicate the user is creating a dating profile.

Exhibit 14

Adobe Distiller Log File

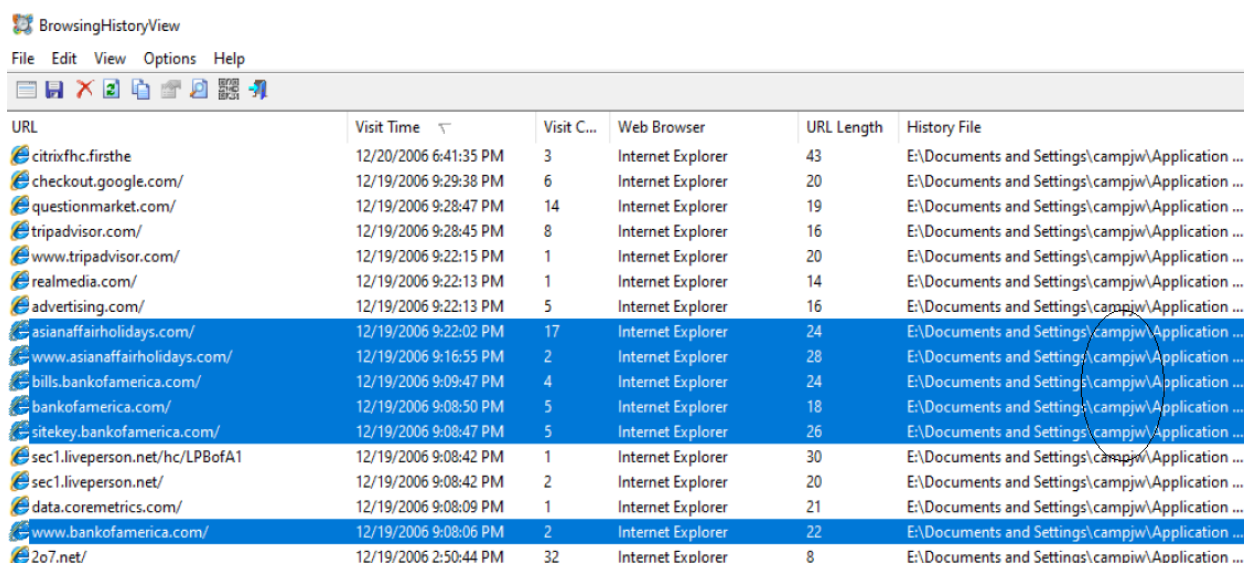
```
Start Time: Wednesday, October 29, 2008 at 13:06:32
Source: P:\toDistiller_ID_2:http://www.eharmony.com/singles/servlet/user/ppr/view?sectionIn
Destination: C:\Documents and Settings\campjw\My Documents\Personalprofile-agreeable.pdf
Adobe PDF Settings: C:\Documents and Settings\All Users\Documents\Adobe PDF\Settings\Standard.joboptions
C:\Documents and Settings\campjw\My Documents\Personalprofile-agreeable.log
%%[ ProductName: Distiller ]%%
%%[ Page: 1 ]%%
%%[ Page: 2 ]%%
%%[ Page: 3 ]%%
%%[ Page: 4 ]%%
%%[ Page: 5 ]%%
%%[ Page: 6 ]%%
%%[ Page: 7 ]%%
%%[ Page: 8 ]%%
%%[ Page: 9 ]%%
%%[ Page: 10 ]%%
%%[ LastPage ]%%
Distill Time: 4 seconds (00:00:04)
**** End of Job ****
```

```
Start Time: Wednesday, October 29, 2008 at 13:09:13
Source: P:\toDistiller_ID_3:http://www.eharmony.com/singles/servlet/user/ppr/view?sectionIn
Destination: C:\Documents and Settings\campjw\My Documents\Personalprofile-openness.pdf
Adobe PDF Settings: C:\Documents and Settings\All Users\Documents\Adobe PDF\Settings\Standard.joboptions
C:\Documents and Settings\campjw\My Documents\Personalprofile-openness.log
%%[ ProductName: Distiller ]%%
%%[ Page: 1 ]%%
%%[ Page: 2 ]%%
%%[ Page: 3 ]%%
%%[ Page: 4 ]%%
%%[ Page: 5 ]%%
```

Next, we reviewed the browsing history of the 40-gigabyte image to uncover any artifacts associated with extramarital activity or finances. In Exhibit 15, we discovered two possible artifacts. One artifact is a website on Asian Affairs, and the second artifact is a banking site, Bank of America. These activities occurred within the UTC at 9 pm on December 19, 2006.

Exhibit 15

Browser History View Hitachi 40G Drive



The screenshot shows the 'BrowsingHistoryView' window in Internet Explorer. It contains a table with the following columns: URL, Visit Time, Visit C..., Web Browser, URL Length, and History File. The table lists various websites visited, including citrixfhc.firsthe, checkout.google.com/, questionmarket.com/, tripadvisor.com/, www.tripadvisor.com/, realmedia.com/, advertising.com/, asianaffairholidays.com/, www.asianaffairholidays.com/, bills.bankofamerica.com/, bankofamerica.com/, sitekey.bankofamerica.com/, sec1.liveperson.net/hc/LPBofA1, sec1.liveperson.net/, data.coremetrics.com/, www.bankofamerica.com/, and 2o7.net/. The 'Visit C...' column shows the number of visits, and the 'History File' column shows the path to the history file in the user's profile.

URL	Visit Time	Visit C...	Web Browser	URL Length	History File
citrixfhc.firsthe	12/20/2006 6:41:35 PM	3	Internet Explorer	43	E:\Documents and Settings\campjw\Application ...
checkout.google.com/	12/19/2006 9:29:38 PM	6	Internet Explorer	20	E:\Documents and Settings\campjw\Application ...
questionmarket.com/	12/19/2006 9:28:47 PM	14	Internet Explorer	19	E:\Documents and Settings\campjw\Application ...
tripadvisor.com/	12/19/2006 9:28:45 PM	8	Internet Explorer	16	E:\Documents and Settings\campjw\Application ...
www.tripadvisor.com/	12/19/2006 9:22:15 PM	1	Internet Explorer	20	E:\Documents and Settings\campjw\Application ...
realmedia.com/	12/19/2006 9:22:13 PM	1	Internet Explorer	14	E:\Documents and Settings\campjw\Application ...
advertising.com/	12/19/2006 9:22:13 PM	5	Internet Explorer	16	E:\Documents and Settings\campjw\Application ...
asianaffairholidays.com/	12/19/2006 9:22:02 PM	17	Internet Explorer	24	E:\Documents and Settings\campjw\Application ...
www.asianaffairholidays.com/	12/19/2006 9:16:55 PM	2	Internet Explorer	28	E:\Documents and Settings\campjw\Application ...
bills.bankofamerica.com/	12/19/2006 9:09:47 PM	4	Internet Explorer	24	E:\Documents and Settings\campjw\Application ...
bankofamerica.com/	12/19/2006 9:08:50 PM	5	Internet Explorer	18	E:\Documents and Settings\campjw\Application ...
sitekey.bankofamerica.com/	12/19/2006 9:08:47 PM	5	Internet Explorer	26	E:\Documents and Settings\campjw\Application ...
sec1.liveperson.net/hc/LPBofA1	12/19/2006 9:08:42 PM	1	Internet Explorer	30	E:\Documents and Settings\campjw\Application ...
sec1.liveperson.net/	12/19/2006 9:08:42 PM	2	Internet Explorer	20	E:\Documents and Settings\campjw\Application ...
data.coremetrics.com/	12/19/2006 9:08:09 PM	1	Internet Explorer	21	E:\Documents and Settings\campjw\Application ...
www.bankofamerica.com/	12/19/2006 9:08:06 PM	2	Internet Explorer	22	E:\Documents and Settings\campjw\Application ...
2o7.net/	12/19/2006 2:50:44 PM	32	Internet Explorer	8	E:\Documents and Settings\campjw\Application ...

We then examined both devices for media. No explicit media was found on the Hitachi 40-gigabyte drive, but photographs of the spouse (James Campino) and an unknown female were discovered on the 80-gigabyte image. Exhibit 16 is an example of the photograph found.

Exhibit 16

Picture on Seagate 80G Drive



We further examined the photograph for metadata. In Exhibit 17, we used the Exif tool to discover the metadata. We found the camera used was a Kodak CX7525 model, and the photograph was taken on July 25, 2007, at 21:19:35. No geolocation information was found in the metadata.

Exhibit 17

EXIF Data Associated with Exhibit 16 Artifact

```
File Type Extension      : jpg
MIME Type                : image/jpeg
Exif Byte Order          : Big-endian (Motorola, MM)
Make                    : EASTMAN KODAK COMPANY
Camera Model Name       : KODAK CX7525 ZOOM DIGITAL CAMERA
Orientation              : Horizontal (normal)
X Resolution             : 230
Y Resolution             : 230
Resolution Unit          : inches
Y Cb Cr Positioning     : Centered
Exposure Program        : Program AE
Exif Version             : 0221
Date/Time Original      : 2007:07:25 21:19:35
Create Date              : 2007:07:25 21:19:35
Components Configuration : Y, Cb, Cr, -
Shutter Speed Value      : 1/64
Aperture Value           : 2.7
Max Aperture Value       : 2.7
Light Source             : Unknown
Flash                   : Auto, Fired
Focal Length             : 5.6 mm
Kodak Model              : CX7525
Quality                  : Fine
Burst Mode               : Off
Kodak Image Width        : 2560
Kodak Image Height       : 1920
Year Created             : 2007
Month Day Created        : 07:25
Time Created             : 21:19:35.67
```

After browser and media artifacts were analyzed, the investigation continued focusing on Word, Excel, PDF, and text documents. No documents supporting any hidden finances or assets were discovered. Some Word documents were found that appeared unusual under the administrator account. Exhibit 18 is an example of a poem or song lyrics. The document refers to a person named Kate. The poem-song was under the administrator user's My Documents directory with similar documents.

Exhibit 18

Example of poem-song

Why run from Fate Kate?

Verse1/ This town is getting boring
So let's go and have some fun
Drop your cigarette quit the habit of
Hesitating
I know you regret your life
And all the shit you made
So tell me why can't you
Get away?
Why can't you just
Tell me why,
You stepped down
From your position
Of trouble and mischief maker
Why do you run?
Chorus
From a life
We could have made together
A chance to be forever
To spend with each other
All we could have made?

The documents in question had timestamps of January 4, 1980. Exhibit 19 is an example of the master file table with the associated document. At first appearance, the document appeared to be a Time Stomp.

Exhibit 19

Why run from Fate Kate.doc	1980-01-04 08:38:41	1980-01-04 08:38:42	1980-01-04 08:38:42
----------------------------	---------------------	---------------------	---------------------

The timestamp issue was examined further by analyzing the ntuser.dat registry hive of the administrator user. Exhibit 20 shows that the MRU List for the .doc extensions has a LastWrite time of 1980-01-31 06:14:36Z. The timestamp suggests that the system clock was changed or a system failure occurred.

Exhibit 20

Administrator ntuser.dat RecentDocs\.doc Registry Key

```
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ .chm
LastWrite Time 2008-12-02 15:54:16Z
MRUListEx = 0
    0 = ProduKey.chm

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ .doc
LastWrite Time 1980-01-31 06:14:36Z
MRUListEx = 9,8,6,3,5,0,4,2,7,1
    9 = To August.doc
    8 = Kill Switch.doc
    6 = Actions and Feelings.doc
    3 = A promise.doc
    5 = A Time to live.doc
    0 = Two sides to a thing called Love.doc
    4 = Magic.doc
    2 = Warriors.doc
    7 = SUMMER GREEN.doc
    1 = A reaction.doc

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ .jpg
LastWrite Time 2008-07-07 18:31:39Z
```

Examining the master file table further aided in verifying the hypothesis of either a manual timestamp change or system failure. Exhibit 21 displays other files with a timestamp of January 4, 1980. These files are associated with web browsing.

Exhibit 21

\$MFT File Example of Hitachi 40G Image

administrator@foxsports[2].txt	1980-01-04 04:04:43	1980-01-04 04:05:13	1980-01-04 04:05:13
administrator@opt.fimserve[2].txt	1980-01-04 04:04:43	1980-01-04 04:04:43	1980-01-04 04:04:43
REGSVR32.EXE-29C480B8.pf	1980-01-04 04:04:48	1980-01-05 03:01:31	1980-01-05 03:01:31
administrator@c.foxsports[1].txt	1980-01-04 04:05:02	1980-01-04 04:05:02	1980-01-04 04:05:02
administrator@scorecardresearch[1].txt	1980-01-04 04:05:04	1980-01-04 04:05:04	1980-01-04 04:05:04
administrator@quantserve[1].txt	1980-01-04 04:05:14	1980-01-04 04:05:14	1980-01-04 04:05:14
administrator@msn.foxsports[1].txt	1980-01-04 04:05:15	1980-01-04 04:05:15	1980-01-04 04:05:15
administrator@www.clickmanage[2].txt	1980-01-04 04:05:56	1980-01-04 05:03:47	1980-01-04 05:03:47
frmall_jinit.jar-4b61cf0-235345d2.idx	1980-01-04 04:07:08	1980-01-04 04:07:08	1980-01-04 04:07:08
esis.jar-5c68126d-73a8aceb.idx	1980-01-04 04:07:08	1980-01-04 04:07:08	1980-01-04 04:07:08
web_icons.jar-69b38008-6d5416ee.idx	1980-01-04 04:07:09	1980-01-04 04:07:09	1980-01-04 04:07:09
administrator@www.compasscove[2].txt	1980-01-04 04:08:25	1980-01-04 04:08:25	1980-01-04 04:08:25
administrator@counter.hitslink[1].txt	1980-01-04 04:08:28	1980-01-04 04:08:28	1980-01-04 04:08:28
administrator@fuelinteractive[1].txt	1980-01-04 04:08:45	1980-01-04 04:08:45	1980-01-04 04:08:45
comment_sprite[1].htm	1980-01-04 04:09:01	1980-01-04 04:09:01	1980-01-04 04:09:01
A0039794.que	1980-01-04 04:09:10	1980-01-04 04:09:10	1980-01-04 06:14:14
comment_sprite[1].htm	1980-01-04 04:10:32	1980-01-04 04:10:32	1980-01-04 04:10:32
administrator@blogger[1].txt	1980-01-04 04:11:39	1980-01-04 04:11:39	1980-01-04 04:11:39
administrator@milnetconsulting[1].txt	1980-01-04 04:11:50	1980-01-04 04:11:50	1980-01-04 04:11:50
image402[1].png	1980-01-04 04:11:53	1980-01-04 04:12:01	1980-01-04 04:12:01

Based on the January 4, 1980 timestamp, it appears that the laptop in which the hard drive was housed had issues maintaining its settings. According to Biersdorfer (2000), once a computer loses its settings, the BIOS defaults the date/time to January 4, 1980.

Conclusion

Based on the digital forensic examination, evidence suggests the spouse either had an extramarital affair or was planning to have an extramarital affair. This evidence would support a request for dissolution of marriage. There is minor evidence of hidden assets. There were no documents found displaying holdings outside of the business. The one exception is a visit to a Bank of America site, which needs to be investigated for a possible hidden financial account. Table 5 describes the timeline of events for the discovered evidence.

Table 5

Timeline of Discovered Evidence

TimeStamp	Artifact	Description
12/19/2006 21:08:47 UTC	BankofAmerica.com	Possible banking activity. Visit count: 5
12/19/2006 21:16:55 UTC	AsianAffairs.com	Possible hookup Site. Visit count: 17
2/27/2007 16:29:46 UTC	Voice Message	Voice message from suspect female. Phone: 5552613738
7/25/2007 21:19:35 Local	Photographs	Photos of spouse and unknown female

10/29/2008 13:06:32 Local	eHarmony Profile	Build timestamp of PDF associated with the dating website profile
---------------------------	------------------	---

Table 6 displays the evidence found with either unreliable timestamps or no timestamps. Although the pagefile.sys file does not hold timestamp data and is not deleted; data is removed over a period to ensure the file does not grow beyond its configured size, suggesting the AdultFriendFinder.com artifact may have occurred within one year of the hard drive being removed from service.

Table 6

Evidence with Timestamps Unknown

Artifact	Reason Timestamp Unknown	Description
Poem-Song Documents	System Clock Failure	Documents seem to be written for persons unknown
AdultFriendFinder.com	Pagefile.sys	Dating site. Possibly InPrivate Browsing is used to hide activity.

References

- Association of Certified E-Discovery Specialists. (2022). *Digital forensics: Revealing data in family law cases*. <https://aceds.org/digital-forensics-revealing-data-in-family-law-cases/>.
- Biersdorfer, J.D., (2000, January 20). *Q & A; Beginning of time: January 4, 1980*.
<https://www.nytimes.com/2000/01/20/technology/q-a-beginning-of-time-jan-4-1980.html>
- Computer Crime and Intellectual Property Section. (2007, August 22). *Digital forensics analysis methodology*. Department of Justice. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/03/26/forensics_chart.pdf
- Kentucky General Assembly. (2023a). *.140 Marriage -- Court may enter decree of dissolution or separation*. <https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=1447>
- Kentucky General Assembly. (2023b). *.170 Marriage -- Irretrievable breakdown*.
<https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=1450>
- Kentucky General Assembly. (2023c). *.190 Disposition of property*.
<https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=1452>
- Kentucky General Assembly. (2023d). *.401 Rule 401 Definition of "relevant evidence."*.
<https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=20363>
- Kentucky General Assembly. (2023e). *.702 Rule 702 Testimony by experts*.
<https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=20402>
- National Institute of Justice. (2004, April). *Forensic examination of digital evidence: a guide for law enforcement*. Department of Justice. <https://www.ojp.gov/pdffiles1/nij/199408.pdf>
- Said, H., Al Mutawa, N., Al Awadhi, I., & Guimaraes, M. (2011, April 25-27). *Forensic analysis of private browsing artifacts* [Paper Presentation]. 7th International Conference on Innovations in Information Technology. Abu Dhabi, UAE.