Justin Wasser

Computer Forensics Lab 2

Date of Submission: 9/19/2023

Forensic Tools Used: FTK Imager (version 4.2.1.4)

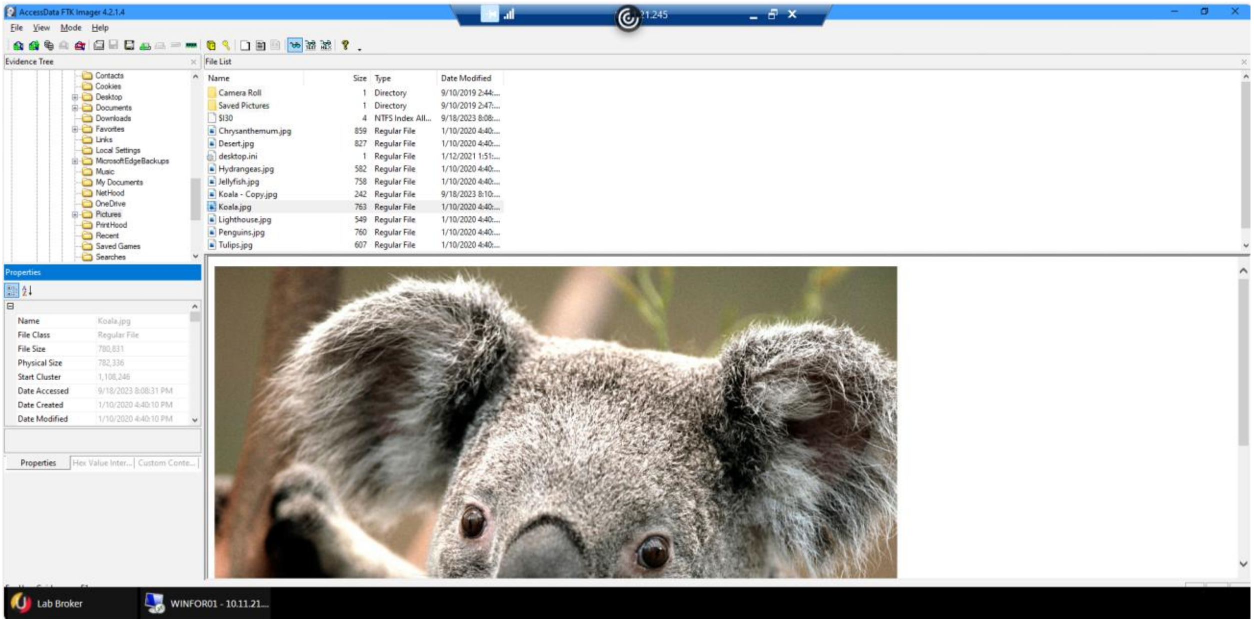
Summary:

The hard drive of a virtual machine was explored using the forensic tool FTK Imager. To that point, a graphics file was chosen (Koala.jpg), a duplicate was made of that file and then the copied/imaged file was edited. Next, the file properties of both the original graphics file and the copied and edited graphics file were examined. Furthermore, the contents that comprised each graphic were made to be displayed as text and then the file's header information was examined for each graphic file. Next, both the original graphics file and the copied/edited graphics file were hashed, and exported as a file hash list. Both hash lists produced were then edited to note the individual who created the hash list as well as the date and time that the hashing occurred. Lastly, the two hash lists produced were compared and any differences in the contents of the two lists were noted.

Description of Tasks Performed & Results with Screenshots:

The graphics file Koala.jpg was chosen for the purposes of this lab, this file and its metadata are illustrated in Figure 1.

Figure 1: Properties of Koala.jpg.

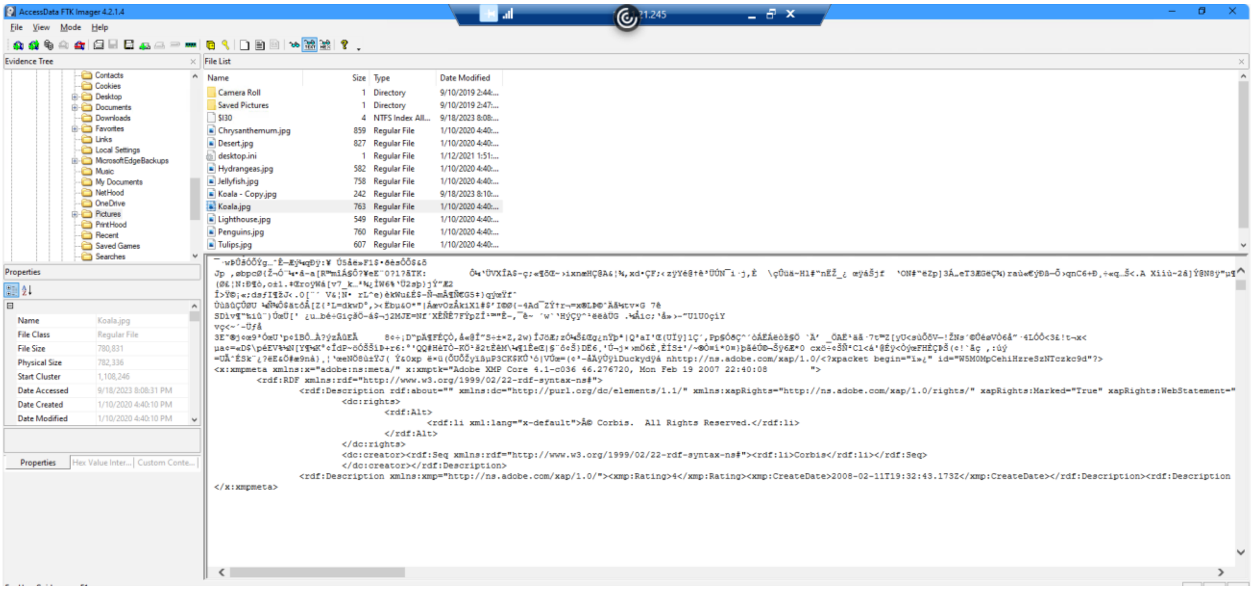


Name	Size	Type	Date Modified
Camera Roll	1	Directory	9/10/2019 2:44:...
Saved Pictures	1	Directory	9/10/2019 2:47:...
$I30	4	NTFS Index All...	9/18/2023 8:08:...
Chrysanthemum.jpg	859	Regular File	1/10/2020 4:40:...
Desert.jpg	827	Regular File	1/10/2020 4:40:...
desktop.ini	1	Regular File	1/12/2021 1:51:...
Hydrangeas.jpg	582	Regular File	1/10/2020 4:40:...
Jellyfish.jpg	758	Regular File	1/10/2020 4:40:...
Koala - Copy.jpg	242	Regular File	9/18/2023 8:10:...
Koala.jpg	763	Regular File	1/10/2020 4:40:...
Lighthouse.jpg	549	Regular File	1/10/2020 4:40:...
Penguins.jpg	760	Regular File	1/10/2020 4:40:...
Tulips.jpg	607	Regular File	1/10/2020 4:40:...

Name	Koala.jpg
File Class	Regular File
File Size	780,831
Physical Size	782,336
Start Cluster	1,108,246
Date Accessed	9/18/2023 8:08:31 PM
Date Created	1/10/2020 4:40:10 PM
Date Modified	1/10/2020 4:40:10 PM

Next, the contents of the Koala.jpg graphics file were adjusted to be displayed as text rather than as a graphic, and the file's header was then examined. Moreover, human-readable information associated with the file was located and analyzed, an illustration of which is found in Figure 2.

Figure 2: File header including human-readable data for Koala.jpg.



Name	Size	Type	Date Modified
Camera Roll	1	Directory	9/10/2019 2:44:...
Saved Pictures	1	Directory	9/10/2019 2:47:...
$I30	4	NTFS Index All...	9/18/2023 8:08:...
Chrysanthemum.jpg	859	Regular File	1/10/2020 4:40:...
Desert.jpg	827	Regular File	1/10/2020 4:40:...
desktop.ini	1	Regular File	1/12/2021 1:51:...
Hydrangeas.jpg	582	Regular File	1/10/2020 4:40:...
Jellyfish.jpg	758	Regular File	1/10/2020 4:40:...
Koala - Copy.jpg	242	Regular File	9/18/2023 8:10:...
Koala.jpg	763	Regular File	1/10/2020 4:40:...
Lighthouse.jpg	549	Regular File	1/10/2020 4:40:...
Penguins.jpg	760	Regular File	1/10/2020 4:40:...
Tulips.jpg	607	Regular File	1/10/2020 4:40:...

Name	Koala.jpg
File Class	Regular File
File Size	780,831
Physical Size	782,336
Start Cluster	1,108,246
Date Accessed	9/18/2023 8:08:31 PM
Date Created	1/10/2020 4:40:10 PM
Date Modified	1/10/2020 4:40:10 PM

```
¯·wÞÛšÓÕÝg…˜Ê–Æÿ¼qÐÿ:¥ Ú$åë»F1$•ðèsÕÕ$&õ
Jp ,øbpcØ(Ž¬Ó¨¼•å-a[R™miÁ§Õ?¥eE¨0?1?ãTK:        Ô¼'ÜVXÎA$-ç;«¶ÕŒ~›ixnæHÇ@A&¦¾,xd•ÇF;‹zÿYé@†ê³ÜÚN¯i·j,Ê  \çÛüä~H1#"nËŽ_¿ œÿáŠjf  'ON#"ëZp]3Á…eT3ÆGëÇ¾)raù«€ýÐß—Õ›qnC6+Ð,÷«q…Š<.A Xiìù~2å]Ý@N8ÿ"µ¶
(Ø£¦N:Ð¶ò,o±1.‡ŒroÿWá[v7_k…³¾¿ÌW6%'Ü2sþ)jÝ"Æ2
Î>Ÿ®¡«;dsfI¶ŽJ‹.0[¨´ V&¦N• rL^e)èkWu£É$-Ñ¬mÄ¶Ñ€G5‡)qýœŸf˜
ÙùßûÇÛØU ¼ÑÑ¾Ô$ãtÔÅ[Z(³L=dkwD°,>‹ËbµÓO*"|ÁævOzÅk1X1#$'I©Ø(-4Ad¯ZÝ†r¬=x®LÞ©˜Äå¼tv×G 7ê
SDìv¶"%iû¯)ÚœÜ[' ¿u…bé÷GiçšÖ-á$¬j2MJE=Nf´XÊÑÊ7FÝpZÎ¹™"Ê-,¯ê~ ´w`'HýÇÿ^³ëëåÜG .¼Åic;'å»›-"U1U0çiY
vç<~´-Ûfå
3E˜®j¢œ9³ÓœU'p¢ìBÔ…À?ýzÅûEÃ      8¢÷¡D"pÄ¶FÉÇÒ,å«@Î"S÷±×Z,2w)ÎJöÆ;zÔ¼Š£Œg¿nŸþª|Q³aI'Œ(UÏÿ]1Ç´,Pp§ÔðÇ^´òÁËÁëòŽ§Ö `Ä' _ÖAË¹ää·7t™Z[yU<sùÕðV—!ŽNs´©ÛéøVÒ6å"·4LÓÕ<3£!t¬x<
µa¢=«D$\péEV¾½N[Y¶¼K°¢ÎdP~öÓŠŠìÞ+r6:°'QQ#HèTÒ-KÖ³š2tÈêM\¼¶1ÊeŒ|§¨ô¢Š}DE6,'Ú¬j×›mÖ6È,ÈÎS±'/~®Ò¤ì*0¤}þãéÜÐ¬Šÿ6Æ*0 cxö÷¢ŠÑ³C1<á'@Éÿ<ÒýœFHÈÇÞŠ(¢!`ãç ,:ûý
=UÃ^ÉSk¨¿?ëE&Ö#æ9nà}¸¦'œeNÖ8ù±ŸJ( Ý&0xp ë×ü(ÕUÕŽyìßµP3CK$KÛ'ó|VÛæ=(¢³-åÄÿÛÿìDuckydÿá nhttp://ns.adobe.com/xap/1.0/<?xpacket begin="ï»¿" id="W5M0MpCehiHzreSzNTczkc9d"?>
<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 4.1-c036 46.276720, Mon Feb 19 2007 22:40:08        ">
        <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
                <rdf:Description rdf:about="" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:xapRights="http://ns.adobe.com/xap/1.0/rights/" xapRights:Marked="True" xapRights:WebStatement="
                        <dc:rights>
                                <rdf:Alt>
                                        <rdf:li xml:lang="x-default">Â© Corbis.  All Rights Reserved.</rdf:li>
                                </rdf:Alt>
                        </dc:rights>
                        <dc:creator><rdf:Seq xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:li>Corbis</rdf:li></rdf:Seq>
                        </dc:creator></rdf:Description>
                <rdf:Description xmlns:xmp="http://ns.adobe.com/xap/1.0/"><xmp:Rating>4</xmp:Rating><xmp:CreateDate>2008-02-11T19:32:43.173Z</xmp:CreateDate></rdf:Description><rdf:Description
</x:xmpmeta>
```

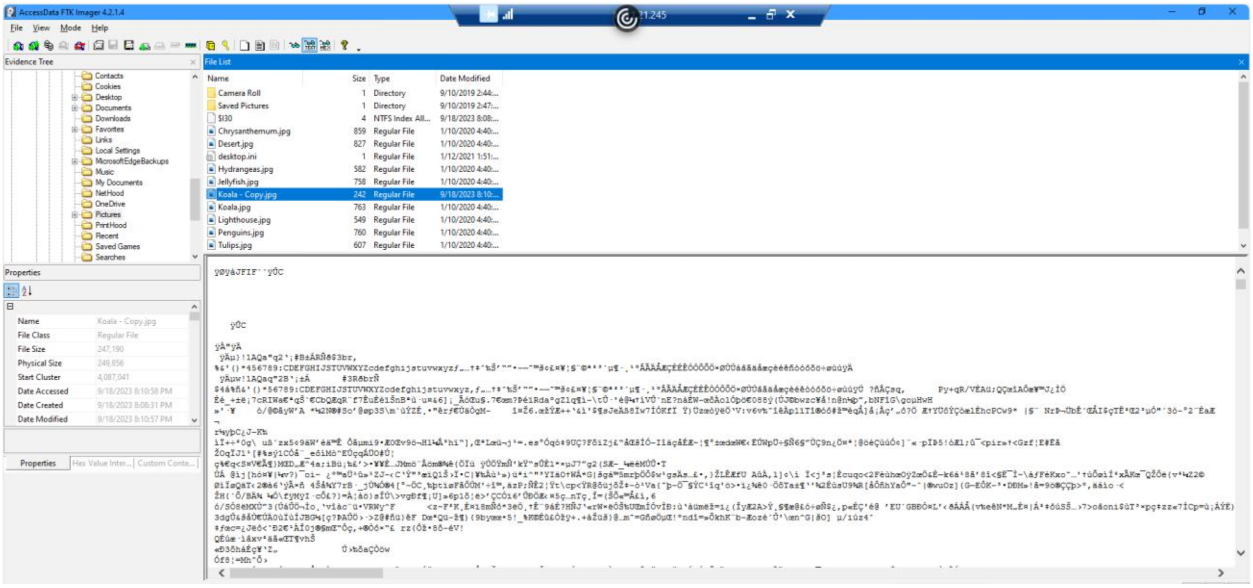
When reviewing the file header for Koala.jpg (Figure 2) there were several human-readable pieces of data of interest. These included several number strings in the very first line of data that appeared to be timestamps, the numbers displayed were as follows: '2009:03:12' '13:48:28' '2008:02:11' '11:32:432008:02:11' and '11:32:43'. Furthermore, further down in the file's header, there were what appeared to be a couple more timestamps displayed along with several URLs, all of which were as follows:

- 'Mon Feb 19 2007 22:40:08'
- 'http://www.w3.org/1999/02/22-rdf-syntax-ns#'
- 'http://purl.org/dc/elements/1.1/'
- 'http://ns.adobe.com/xap/1.0/rights/'
- 'http://pro.corbis.com/search/searchresults.asp?txt=42-15564978&amp;openImage=42-15564978'
- 'http://www.w3.org/1999/02/22-rdf-syntax-ns#'
- 'http://ns.adobe.com/xap/1.0/'
- 'CreateDate>2008-02-11T19:32:43.173Z'
- 'http://ns.microsoft.com/photo/1.0/'

This human-readable metadata found in the file header for Koala.jpg (Figure 2) contained historical data about the file such as when it was created, where it originated from on the internet, and “DCMI Metadata Terms” (*DCMI: DCMI Metadata Terms*, 2020).

Next, the copied and edited graphics file (Koala- Copy.jpg) was selected from the “File List” (UMGC, 2023), and the contents of the graphics file were displayed as text rather than as a graphic. Furthermore, the file’s header and metadata were examined, and any human-readable content associated with the file was located and analyzed, an illustration of which is found in Figure 2.

Figure 3: FTK Imager displaying the copied file



Name	Size	Type	Date Modified
Camera Roll	1	Directory	9/10/2019 2:44:...
Saved Pictures	1	Directory	9/10/2019 2:47:...
$I30	4	NTFS Index All...	9/18/2023 8:08:...
Chrysanthemum.jpg	859	Regular File	1/10/2020 4:40:...
Desert.jpg	827	Regular File	1/10/2020 4:40:...
desktop.ini	1	Regular File	1/12/2021 1:51:...
Hydrangeas.jpg	582	Regular File	1/10/2020 4:40:...
Jellyfish.jpg	758	Regular File	1/10/2020 4:40:...
Koala - Copy.jpg	242	Regular File	9/18/2023 8:10:...
Koala.jpg	763	Regular File	1/10/2020 4:40:...
Lighthouse.jpg	549	Regular File	1/10/2020 4:40:...
Penguins.jpg	760	Regular File	1/10/2020 4:40:...
Tulips.jpg	607	Regular File	1/10/2020 4:40:...

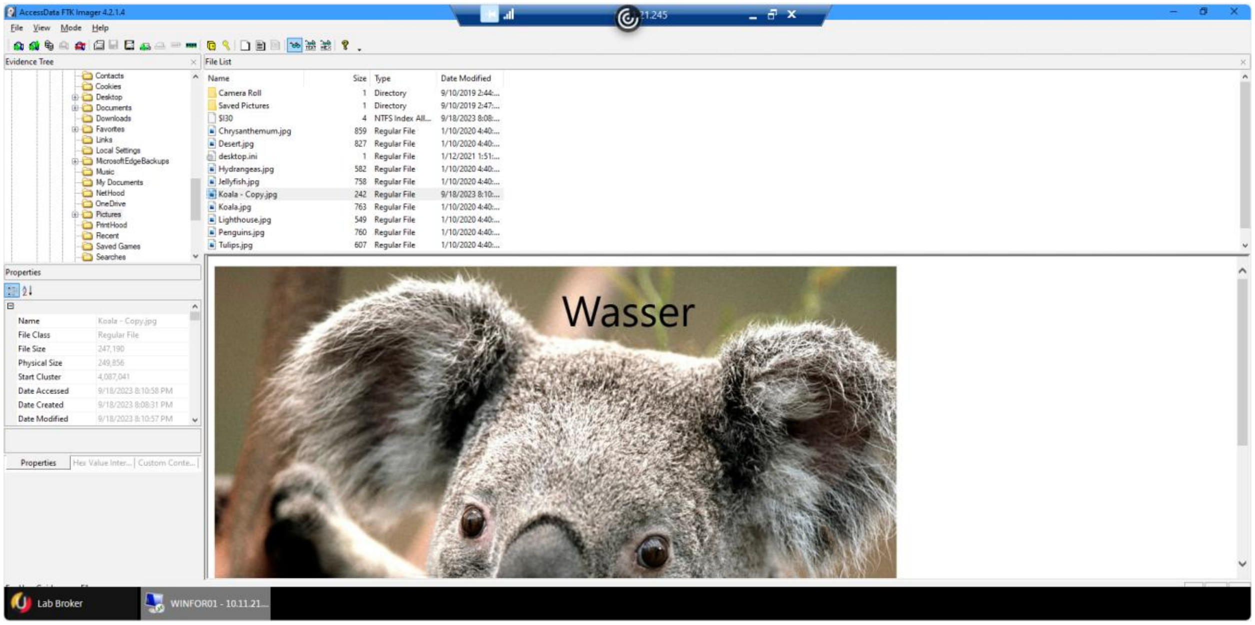
Name	Koala - Copy.jpg
File Class	Regular File
File Size	247,190
Physical Size	249,856
Start Cluster	4,087,041
Date Accessed	9/18/2023 8:10:58 PM
Date Created	9/18/2023 8:08:31 PM
Date Modified	9/18/2023 8:10:57 PM

```
ÿØÿàJFIF``ÿÛC



   ÿÛC

ÿÀ"ÿÄ
 ÿÄµ}!1AQa"q2'¡#B±ÁRÑð$3br,
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
```

When comparing the file headers for Figure 2 (original Koala.jpg) with Figure 3 (Koala- Copy.jpg), a significant difference is noted between the two headers. To that point, the file containing the copied Koala.jpg file (Figure 3) had almost no human-readable information, the only character string listed was ‘ÿØÿàJFIF``ÿÛC’. While the original Koala.jpg (Figure 2) had a plethora of human-readable information within its file header. Furthermore, the properties of the two files differed in many ways including their date created information, 1/10/2020 4:40:10 PM for the original Koala.jpg versus 9/18/2023 8:08:31 PM for the Koala- Copy.jpg; and their file size, 780,831 for Koala.jpg versus 247,190 for the Koala- Copy.jpg.

Next, the modified graphics file (Koala- Copy.jpg) was adjusted back to the "Automatic viewer" (UMGC, 2023) and the file's graphical representation was displayed in the preview section of FTK Imager as illustrated in Figure 4.

Figure 4: FTK Imager displaying the contents of the modified graphics file

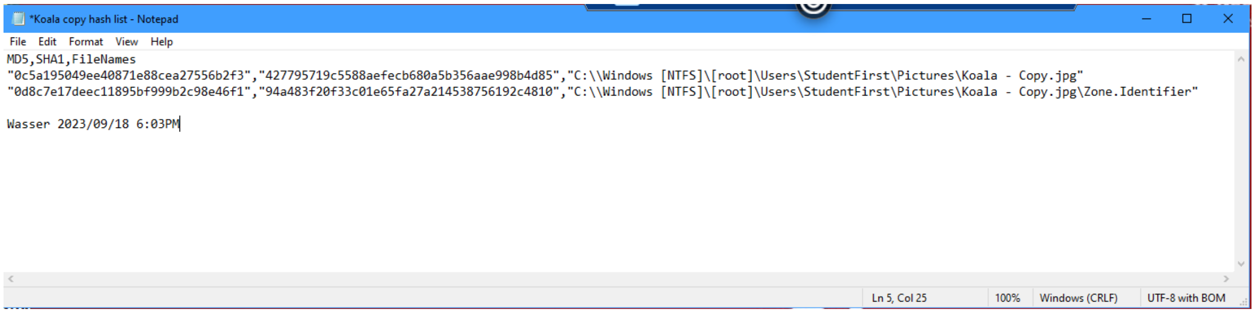


Name	Size	Type	Date Modified
Camera Roll	1	Directory	9/10/2019 2:44:...
Saved Pictures	1	Directory	9/10/2019 2:47:...
$I30	4	NTFS Index All...	9/18/2023 8:08:...
Chrysanthemum.jpg	859	Regular File	1/10/2020 4:40:...
Desert.jpg	827	Regular File	1/10/2020 4:40:...
desktop.ini	1	Regular File	1/12/2021 1:51:...
Hydrangeas.jpg	582	Regular File	1/10/2020 4:40:...
Jellyfish.jpg	758	Regular File	1/10/2020 4:40:...
Koala - Copy.jpg	242	Regular File	9/18/2023 8:10:...
Koala.jpg	763	Regular File	1/10/2020 4:40:...
Lighthouse.jpg	549	Regular File	1/10/2020 4:40:...
Penguins.jpg	760	Regular File	1/10/2020 4:40:...
Tulips.jpg	607	Regular File	1/10/2020 4:40:...

Name	Koala - Copy.jpg
File Class	Regular File
File Size	247,190
Physical Size	249,856
Start Cluster	4,087,041
Date Accessed	9/18/2023 8:10:58 PM
Date Created	9/18/2023 8:08:31 PM
Date Modified	9/18/2023 8:10:57 PM

Next, the copied and modified graphics file (Koala- Copy.jpg) was hashed, exported, and saved. Furthermore, the hash list produced was then edited to note the individual who created the hash list as well as the date and time that the hashing occurred, as shown in Figure 5.

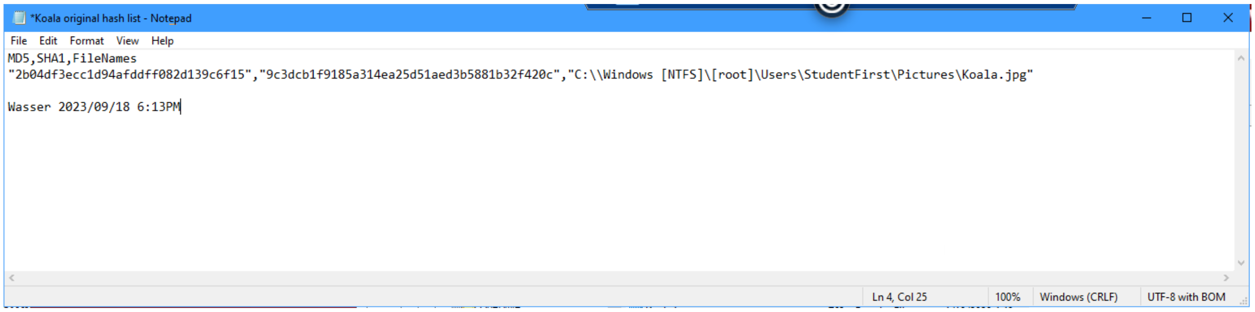
Figure 5: Hash List for koala-copy.jpg



```
MD5,SHA1,FileNames
"0c5a195049ee40871e88cea27556b2f3","427795719c5588aefecb680a5b356aae998b4d85","C:\\Windows [NTFS]\[root]\Users\StudentFirst\Pictures\Koala - Copy.jpg"
"0d8c7e17deec11895bf999b2c98e46f1","94a483f20f33c01e65fa27a214538756192c4810","C:\\Windows [NTFS]\[root]\Users\StudentFirst\Pictures\Koala - Copy.jpg\Zone.Identifier"

Wasser 2023/09/18 6:03PM
```

Next, the original graphics file (Koala.jpg) was hashed, exported, and saved. Furthermore, the hash list produced was then edited to note the individual who created the hash list as well as the date and time that the hashing occurred, as shown in Figure 6.

Figure 6: Hash List for koala.jpg


*Koala original hash list - Notepad
File Edit Format View Help
Ln 4, Col 25
100%
Windows (CRLF)
UTF-8 with BOM

```
MD5,SHA1,FileNames
"2b04df3ecc1d94afddff082d139c6f15","9c3dcb1f9185a314ea25d51aed3b5881b32f420c","C:\\Windows [NTFS]\[root]\Users\StudentFirst\Pictures\Koala.jpg"

Wasser 2023/09/18 6:13PM
```

Lastly, the two hash lists produced (Figure 5 and Figure 6) were compared and differences between the two hash lists were noted. To that point, Figure 5 contained two distinct sets of hashes, with a set meaning a pair of hashes (one MD5 hash and one SHA1 hash); put another way Figure 5 contained two different MD5 hashes and two different SHA1 hashes. While Figure 6 only contained one set of hashes. Furthermore, the extra hash set found in Figure 5 had a file name that differed from the other hashes found in Figure 5 and Figure 6, the part of the file name that differed was located at the end of the file name and was labeled '\Zone.Identifier'. Lastly, each of the three hash sets as well as the 6 total hash values found in Figures 5 and 6 were unique.

References:

DCMI: DCMI Metadata Terms. (2020, January 20). Dublincore.org. https://www.dublincore.org/specifications/dublin-core/dcmi-terms/

UMGC. (2023). *Computer Forensics Lab 2*. Learn.umgc. https://learn.umgc.edu/d2l/le/dropbox/920316/1543565/DownloadAttachment?fid=76691266