Disk Drive Investigation for John Brinkley Fake Driver's License Case

Kollin Labowski

kkl0009@mix.wvu.edu

December 11, 2021

Abstract

A computer forensic investigation was completed on a disk drive seized from the home of John Brinkley with a valid search warrant. Access to the drive was accomplished using a tool called Hiren's BootCD PE, which allowed access into the Windows 7 disk while bypassing the password. In the investigation, several files were recovered containing personal information such as email addresses, home addresses, social security numbers, and dates of birth for various individuals. An HTML file was found which appears to have hosted a website for a company called "IDs 'R' Us". Additionally, several images were recovered, some of which contain fake driver's licenses (licenses marked with the words "Fake Driver's License"), and some of which are just pictures of various people. The files recovered during the investigation range in the time of their creation from 2001 to 2016. Also, several emails were recovered during the investigation, many of which specifically mention this "IDs 'R' Us" business. Most of these emails are either addressed to or sent from an individual by the name of Ira Aubrey Badun.

Table of Contents

Affiant's Background

Kollin Labowski is a Computer Science student in the class of 2022 at West Virginia University. He has over 5 years of experience in computer programming, particularly with Java, C, Python, and PHP. He is currently pursuing an area of emphasis in Cybersecurity and has experience penetration testing with Kali Linux. Kollin has used a wide variety of computer forensic tools, including but not limited to, Nmap, Wireshark, Dirbuster, John the Ripper, and Ghidra. Additionally, Kollin is currently enrolled in CPE 435, Computer Incident Response, at West Virginia University. In this class, Kollin gained a solid understanding of the forensic investigation process, and the government policies relating to them. This class is also where Kollin as introduced to many of the forensic tools he had used, particularly as part of the National Cyber League competition, where he ranked within the top 98 percent of the country.

Incident Material

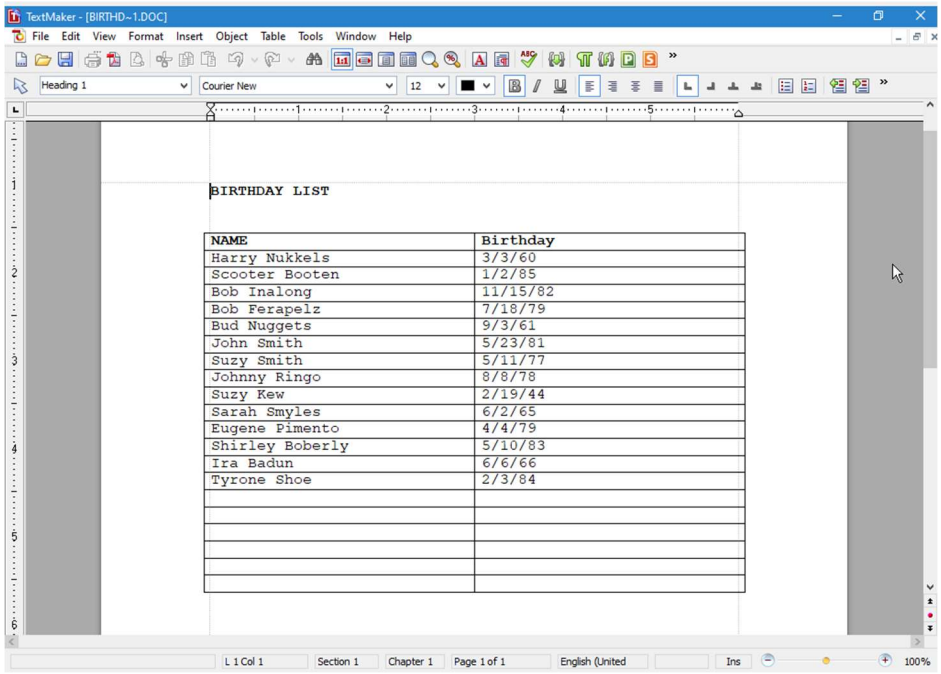
The following section contains images and documents recovered from the disk drive. All files are displayed here in chronological order, based on their "Modified" date. Each image or document displayed here is followed by a screenshot of its metadata. Each document also has its name listed, in addition to a time stamp of the time the file was modified (with accuracy of within a minute). Finally, the directory each of the files were found in can be found by viewing the nearest directory listed above the screenshot of the file (ex: the first file can be found in the directory *C:\Documents and Settings\rsn\My Documents\LOOT* as seen below).

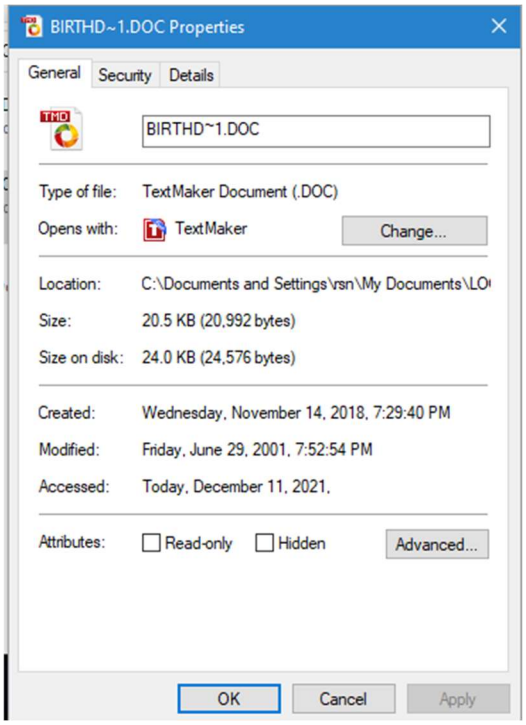
June 29, 2001

On this day, a list of 14 individuals and their birthdays were added to the system.

In directory *C:\Documents and Settings\rsn\My Documents\LOOT*

7:52 PM: *BirthD~1.DOC*



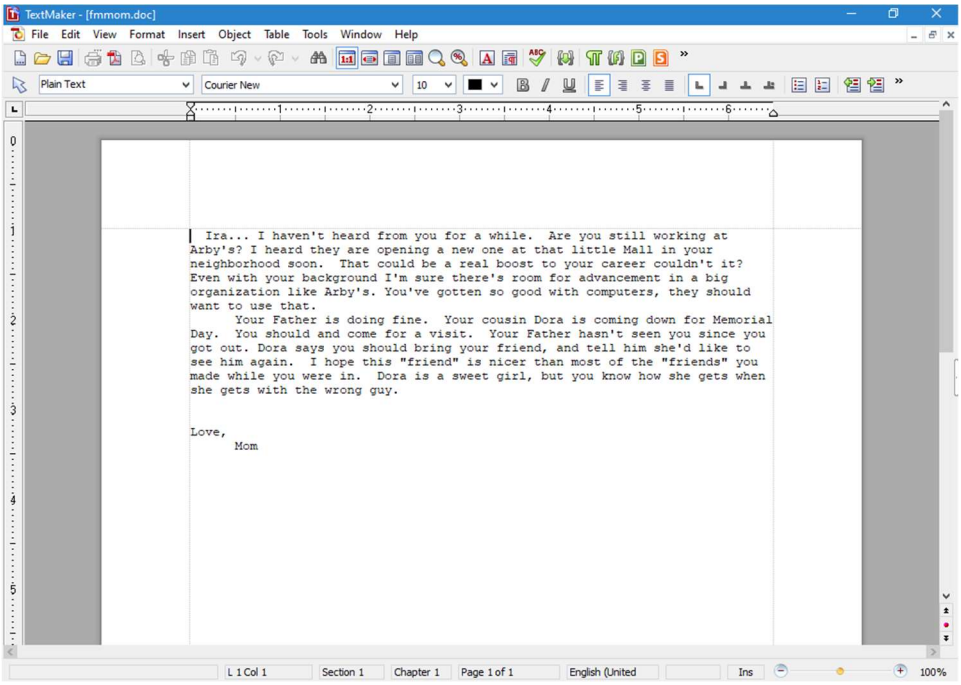


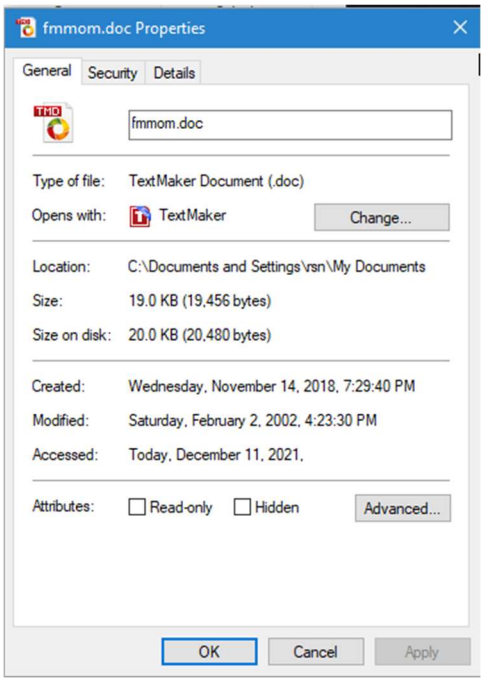
February 2, 2002

On this day, an email was received addressed to an individual named Ira. The email appears to have been sent by this individual's mother.

In directory *C:\Documents and Settings\rsn\My Documents*

4:23 PM: *fmmom.doc*



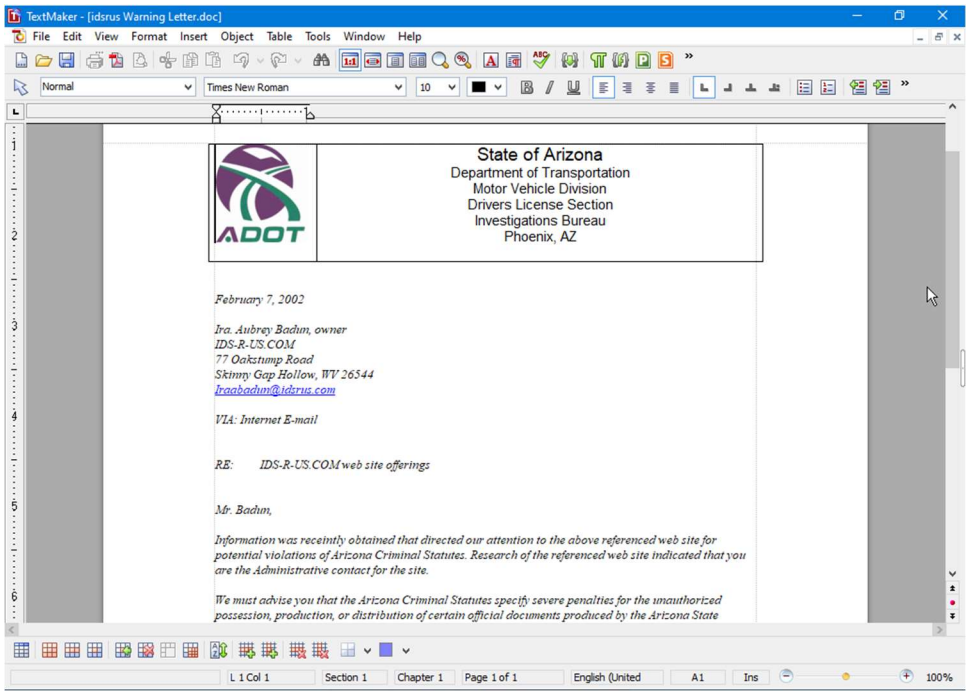


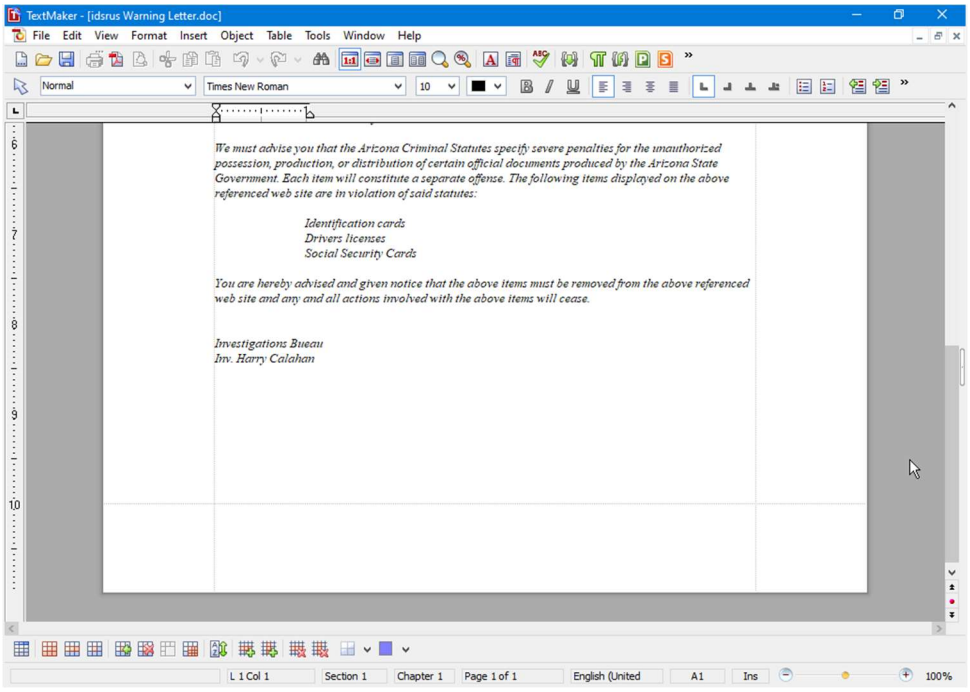
February 7, 2002

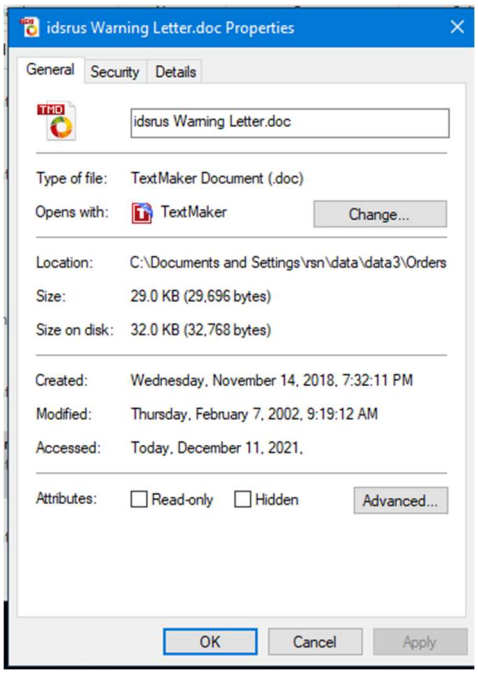
On this day, the State of Arizona Department of Transportation sent a letter to an individual named Ira Aubrey Badun. The letter was regarding some alleged activities that the addressed individual was doing which violated their policies.

In directory *C:\Documents and Settings\rsn\data\data3\Orders and Records*

9:19 AM: *idsrus Warning Letter.doc*





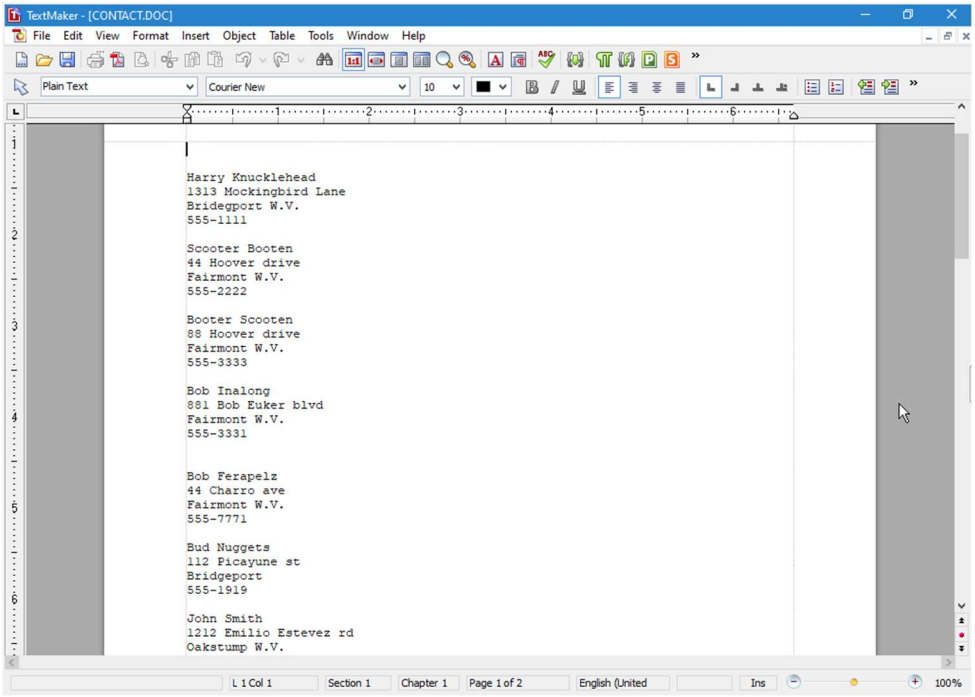

idsrus Warning Letter.doc Properties
General
Security
Details
idsrus Warning Letter.doc
Type of file: TextMaker Document (.doc)
Opens with: TextMaker
Change...
Location: C:\Documents and Settings\rsn\data\data3\Orders
Size: 29.0 KB (29,696 bytes)
Size on disk: 32.0 KB (32,768 bytes)
Created: Wednesday, November 14, 2018, 7:32:11 PM
Modified: Thursday, February 7, 2002, 9:19:12 AM
Accessed: Today, December 11, 2021,
Attributes: Read-only Hidden
Advanced...
OK
Cancel
Apply

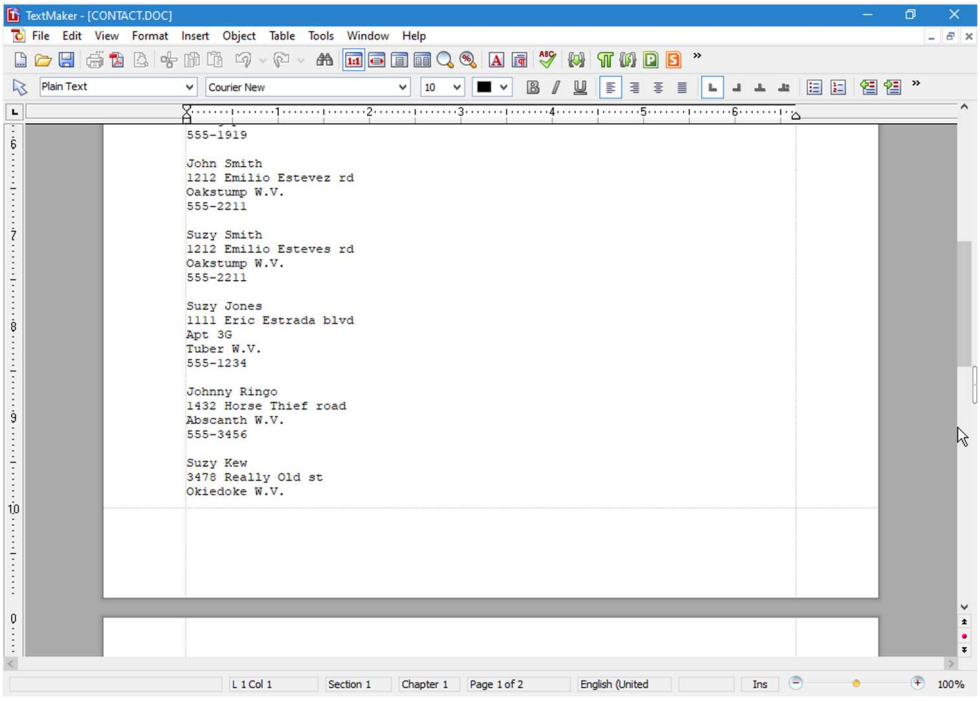
February 11, 2002

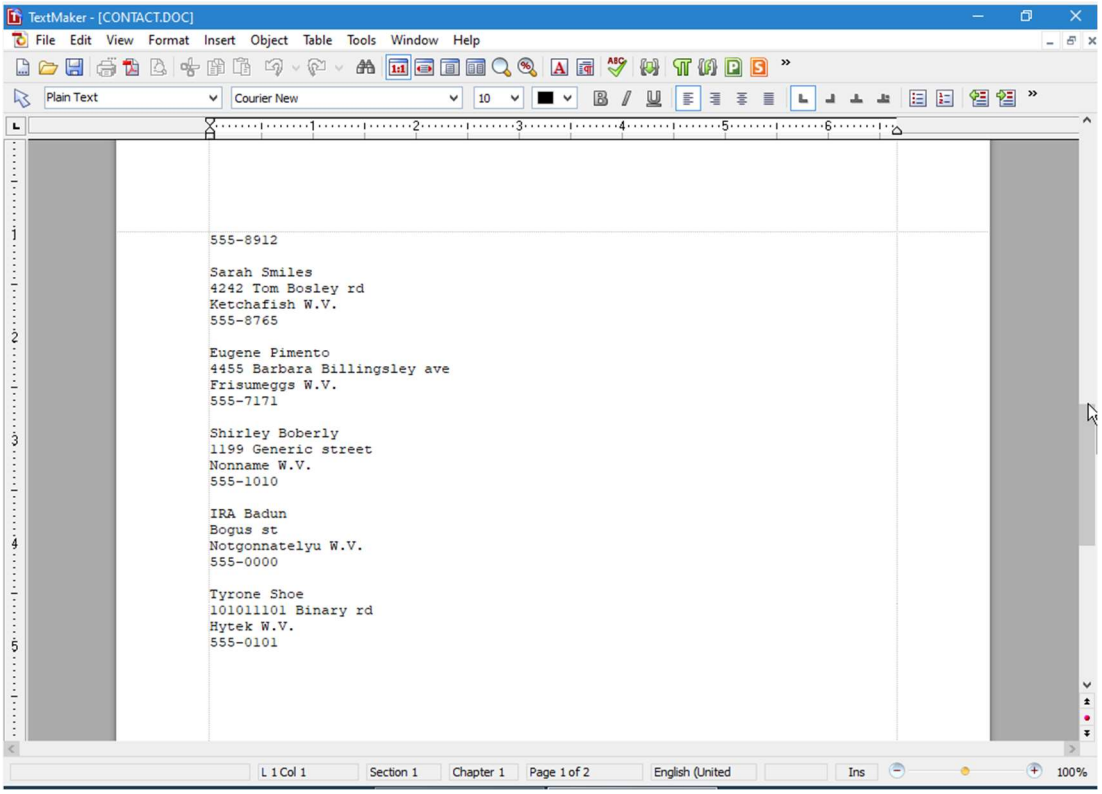
On this day, a list of 16 individuals and what appear to be their home addresses were added to the system.

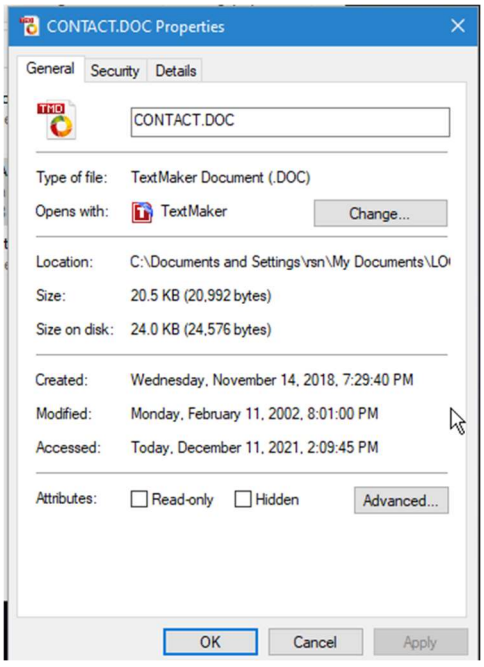
In directory *C:\Documents and Settings\rsn\My Documents\LOOT*

8:01 PM: *CONTACT.DOC*






TextMaker - [CONTACT.DOC]
File Edit View Format Insert Object Table Tools Window Help
Plain Text
Courier New
10
555-8912
Sarah Smiles
4242 Tom Bosley rd
Ketchafish W.V.
555-8765
Eugene Pimento
4455 Barbara Billingsley ave
Frisumeggs W.V.
555-7171
Shirley Boberly
1199 Generic street
Nonname W.V.
555-1010
IRA Badun
Bogus st
Notgonnatelyu W.V.
555-0000
Tyrone Shoe
101011101 Binary rd
Hytek W.V.
555-0101
L 1 Col 1
Section 1
Chapter 1
Page 1 of 2
English (United
Ins
100%

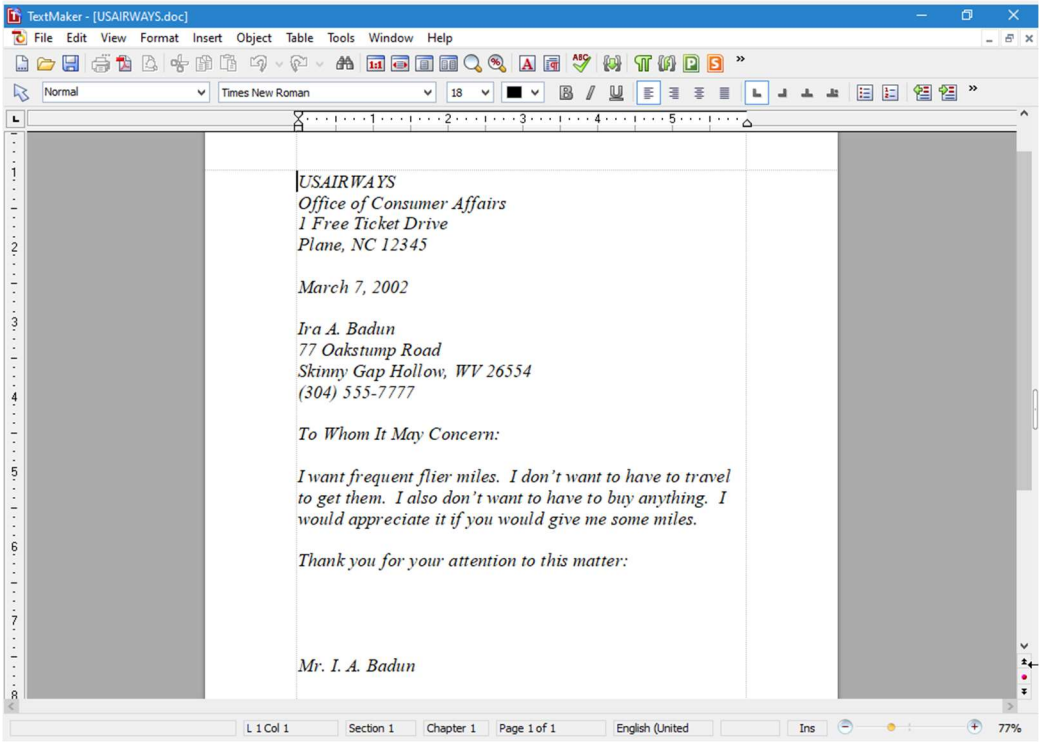

CONTACT.DOC Properties
General
Security
Details
CONTACT.DOC
Type of file: TextMaker Document (.DOC)
Opens with: TextMaker
Change...
Location: C:\Documents and Settings\vsn\My Documents\LO
Size: 20.5 KB (20,992 bytes)
Size on disk: 24.0 KB (24,576 bytes)
Created: Wednesday, November 14, 2018, 7:29:40 PM
Modified: Monday, February 11, 2002, 8:01:00 PM
Accessed: Today, December 11, 2021, 2:09:45 PM
Attributes: Read-only Hidden
Advanced...
OK
Cancel
Apply

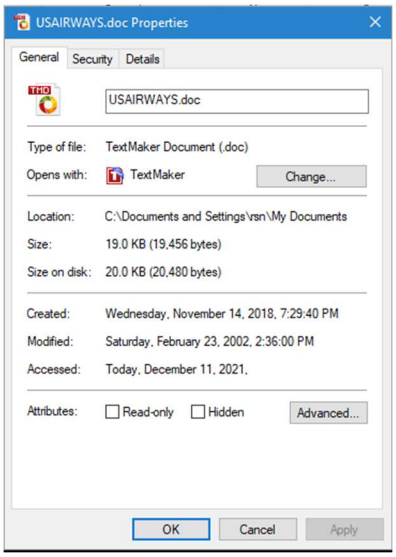
February 23, 2002

On this day, an individual named Ira A. Badun (likely the same individual mentioned in previous documents) sent an email to USAIRWAYS to request frequent flier miles.

In directory *C:\Documents and Settings\rsn\My Documents*

2:36 PM: *USAIRWAYS.doc*



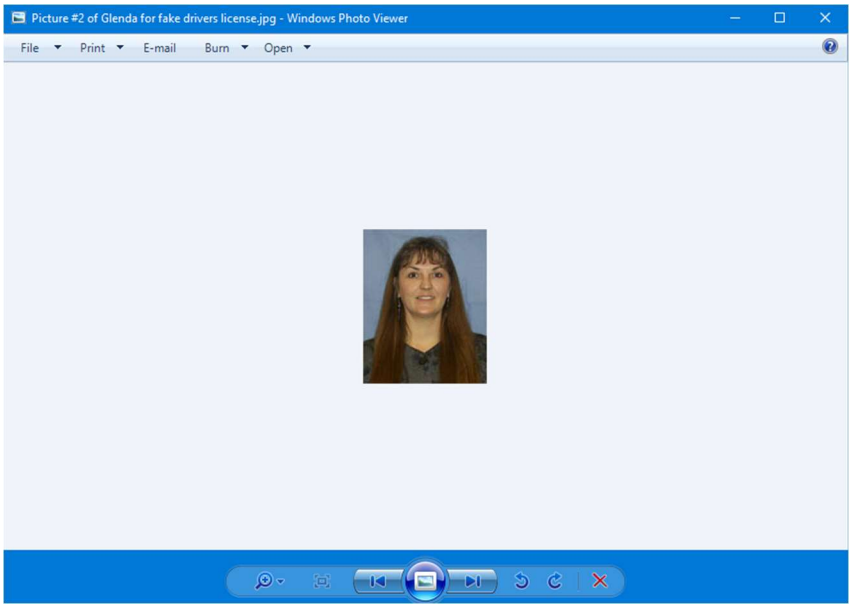


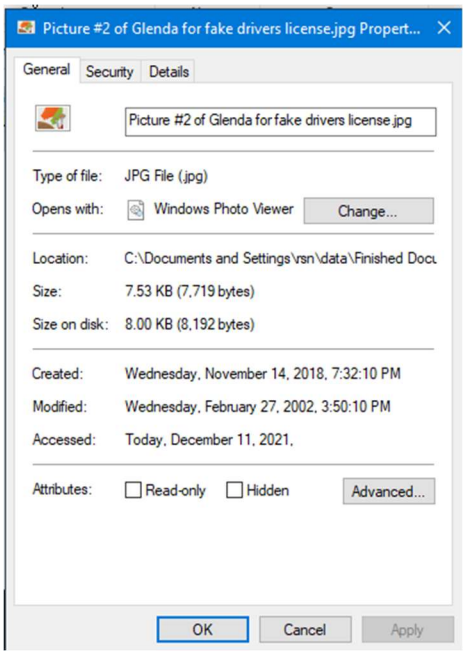
February 27, 2002

On this day, 2 images of different individuals were added onto the system. Both file names contain the term “fake drivers license”.

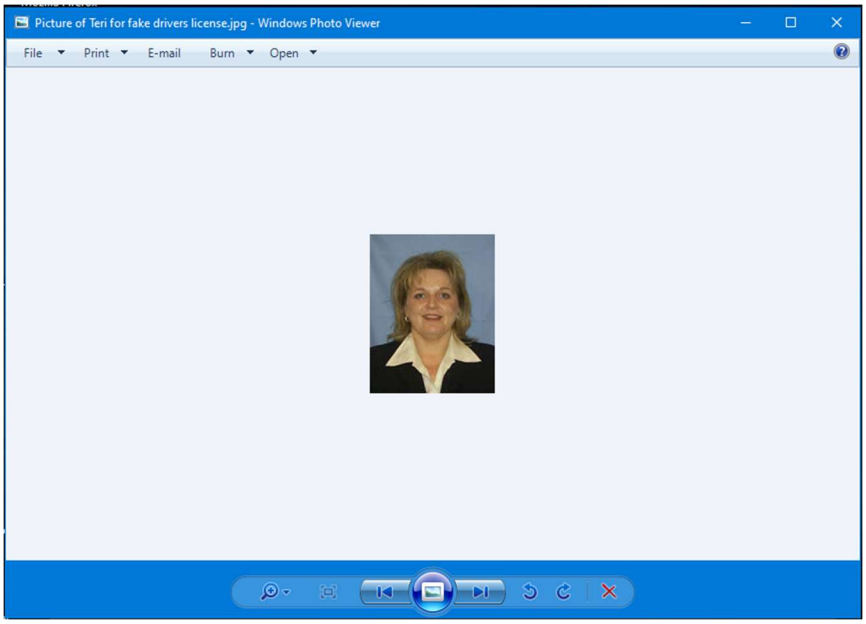
In directory *C:\Documents and Settings\rsn\data\Finished Documents\Stuff for Mikey*

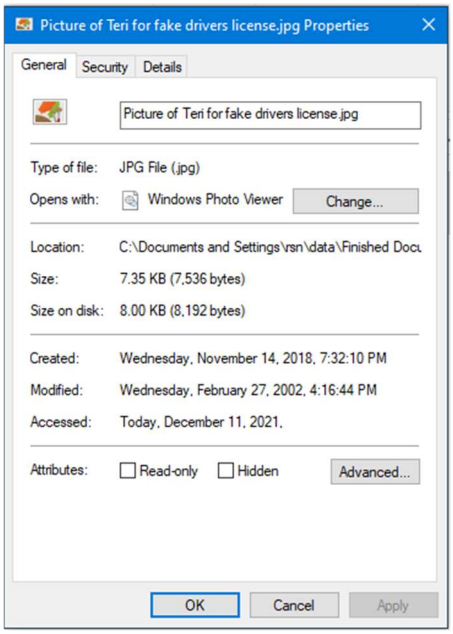
3:50 PM: *Picture #2 of Glenda for fake drivers license.jpg*





4:16 PM: *Picture of Teri for fake drivers license.jpg*



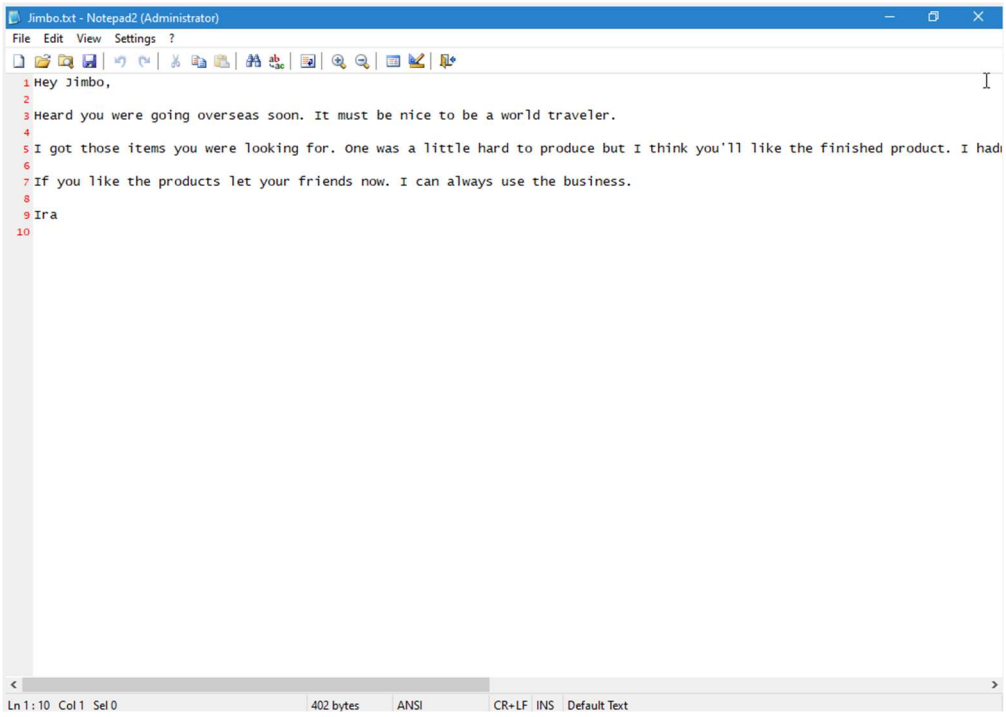


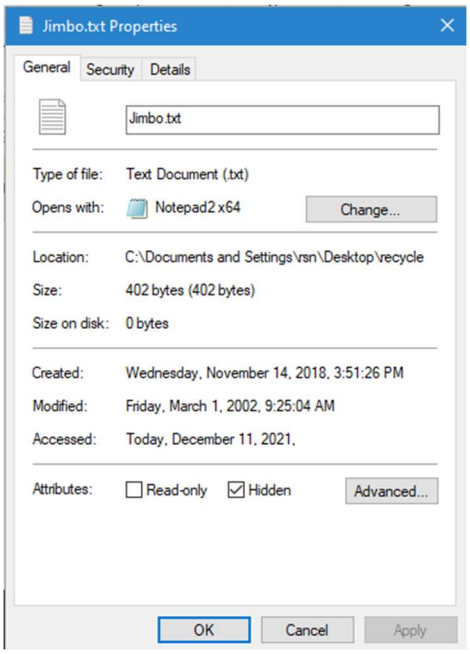
March 1, 2002

On this day, a message appears to have been drafted by the individual named Ira, and the message was to be sent to someone who goes by “Jimbo”. The message mentions some “items”, however it is unclear what specifically this might be referring to.

In directory *C:\Documents and Settings\rsn\Desktop\recycle*

9:25 AM: *Jimbo.txt*



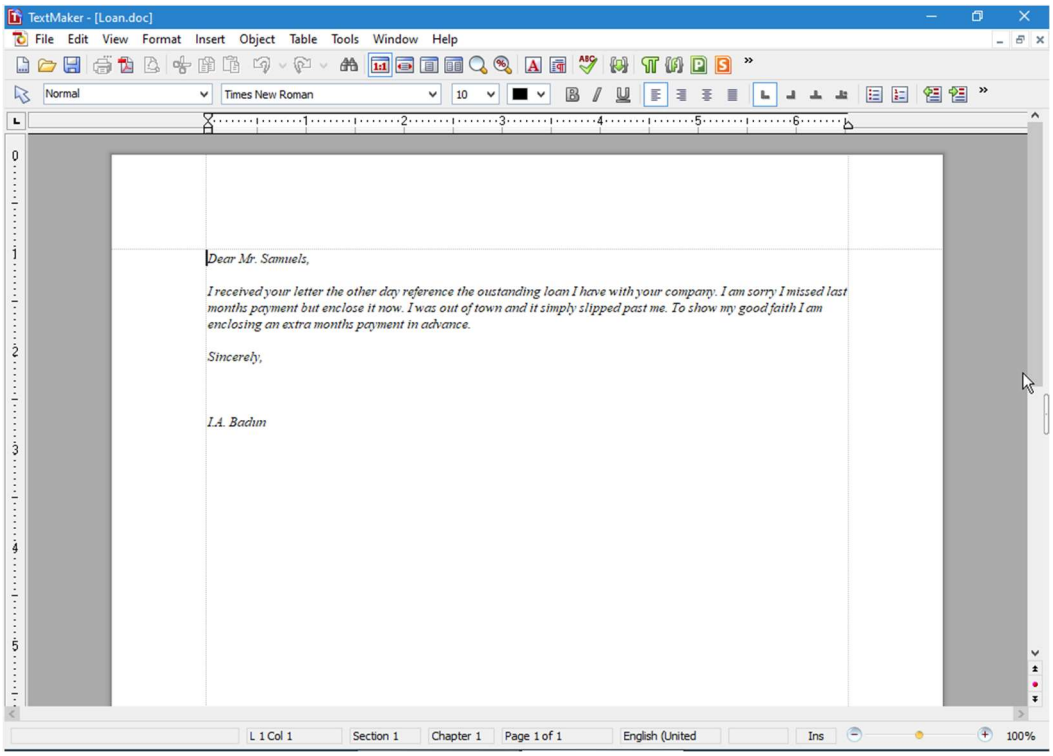


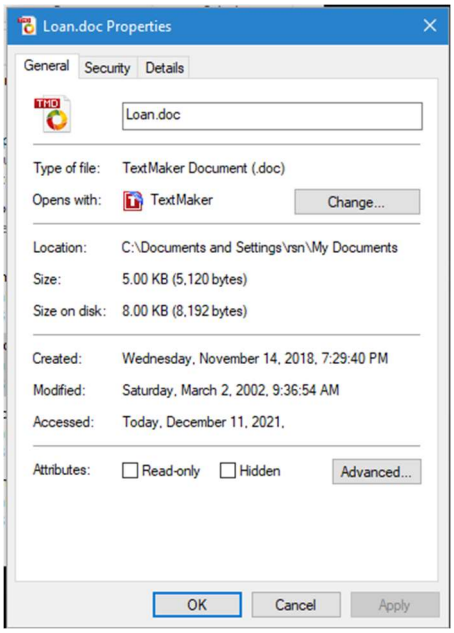
March 2, 2002

On this day, it appears that the individual Ira Badun has sent a message to someone named Mr. Samuels regarding a loan.

In directory *C:\Documents and Settings\rsn\My Documents*

9:36 AM: *Loan.doc*



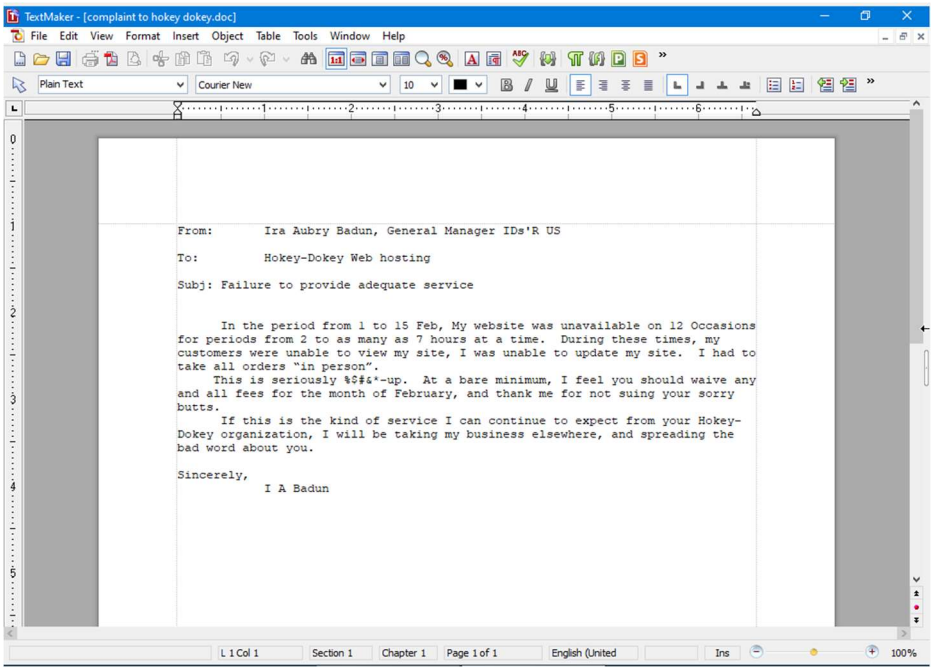


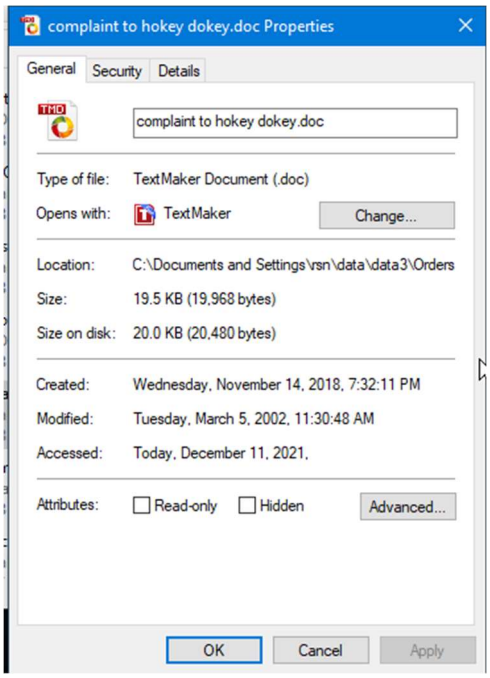
March 5, 2002

On this day, the individual Ira Badun appears to have sent a message to a business called Hokey-Dokey Web Hosting. The message appears to be regarding a loss of availability for some website.

In directory *C:\Documents and Settings\rsn\data\data3\Orders and Records*

11:30 AM: *complaint to hokey dokey.doc*



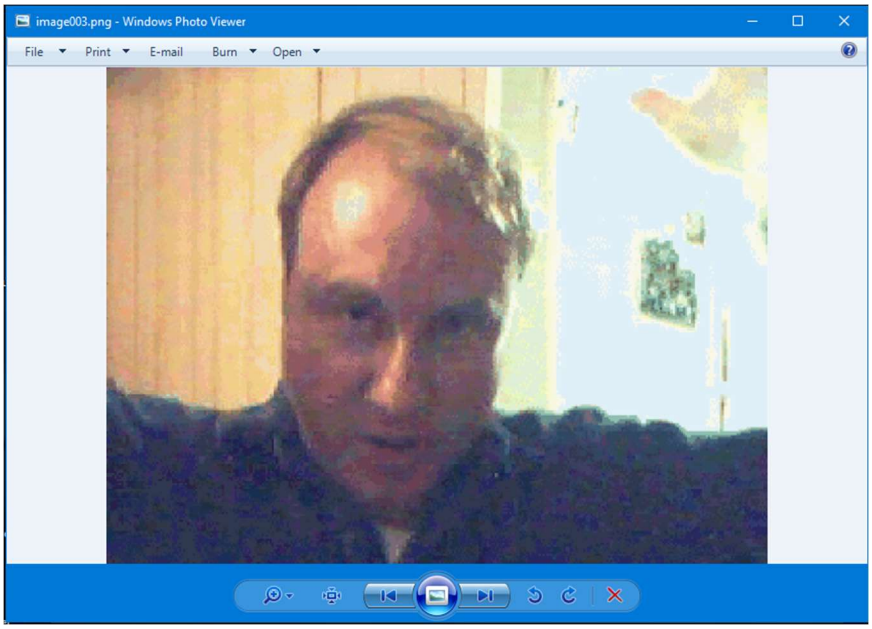


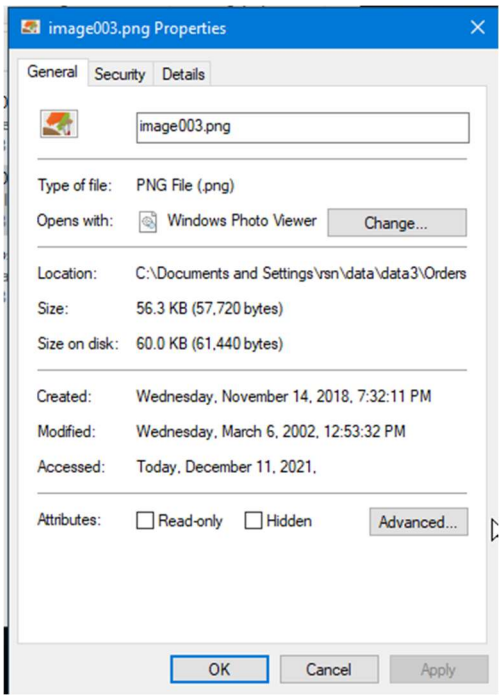
March 6, 2002

On this day, images and HTML files were added for a website which appears to be titled “IDS ‘R’ US”. Additionally, an email addressed to “IDsRUs” from someone named Jack Morton was found on the server.

In directory *C:\Documents and Settings\rsn\data\data3\Orders and Records\IDsrus_files*

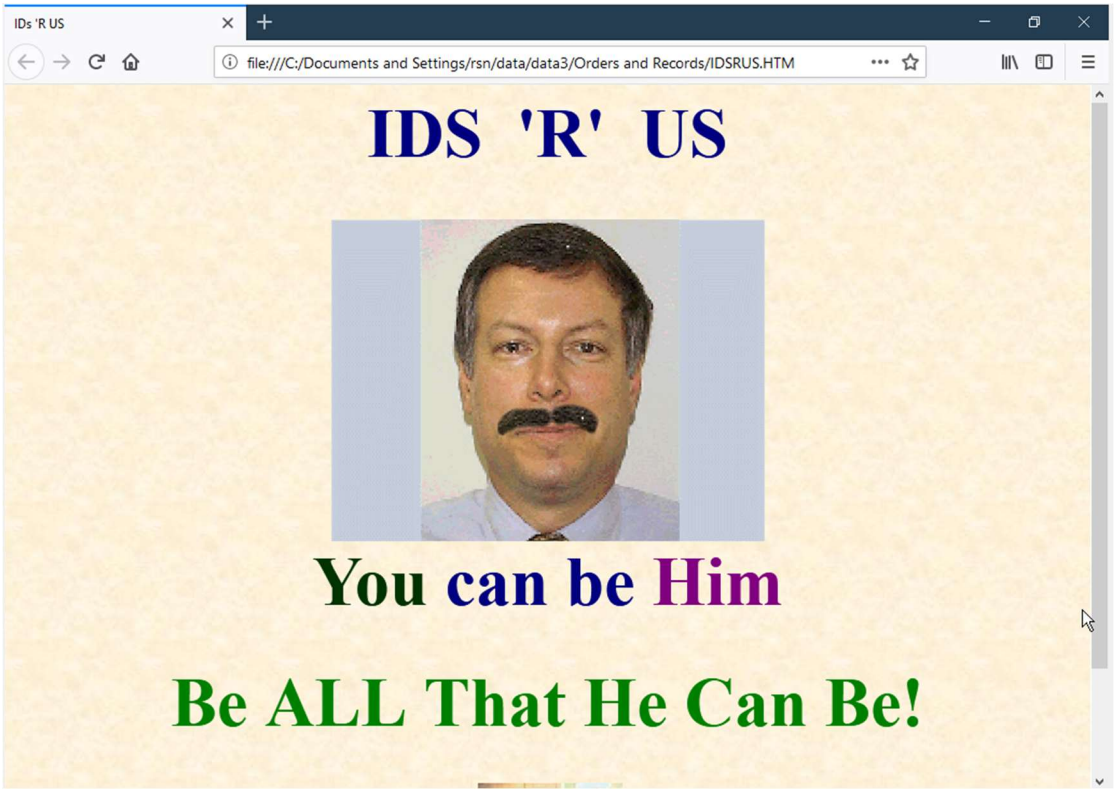
12:53 PM: *image003.png*

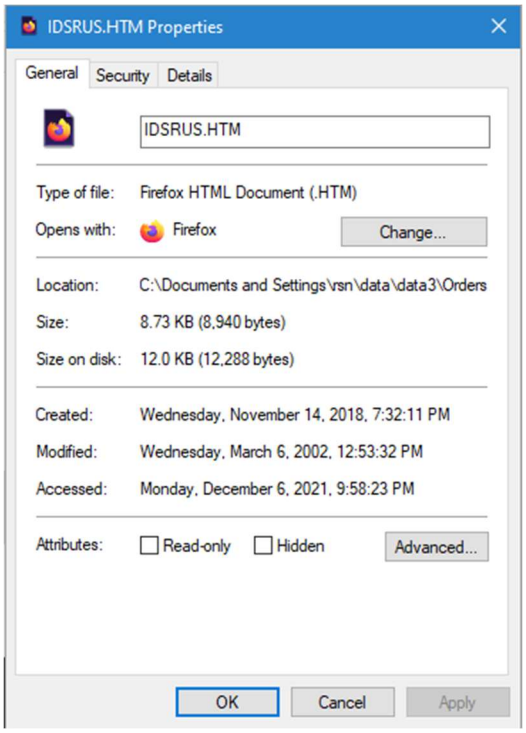




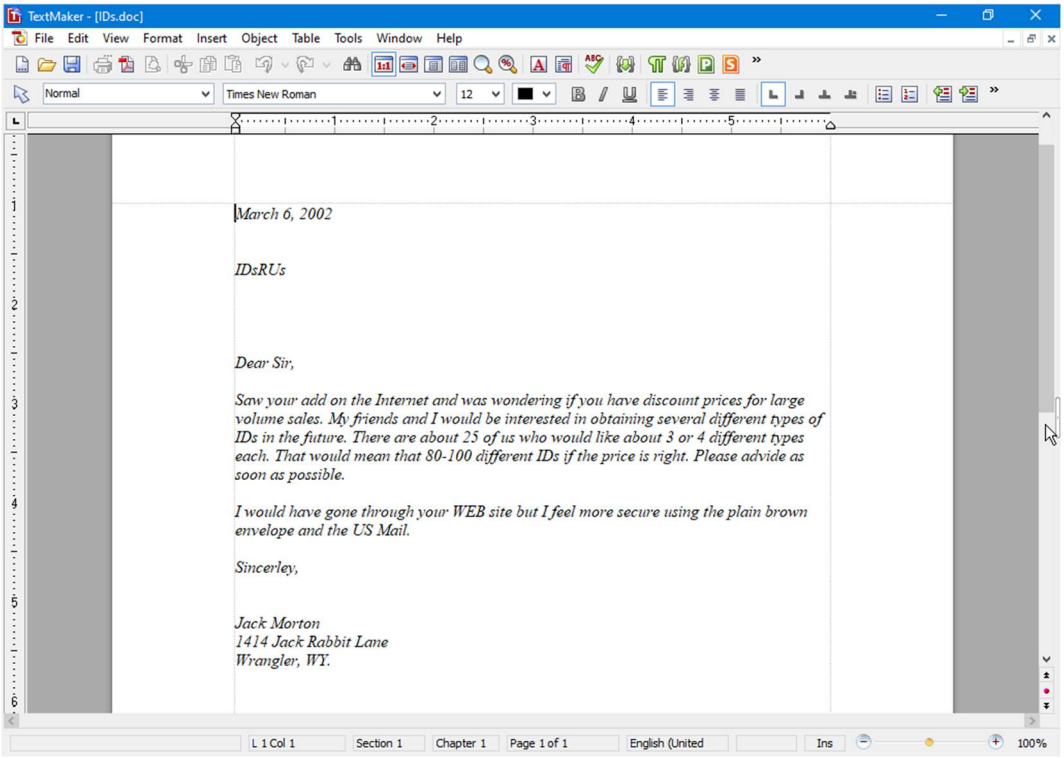
In directory *C:\Documents and Settings\rsn\data\data3\Orders and Records*

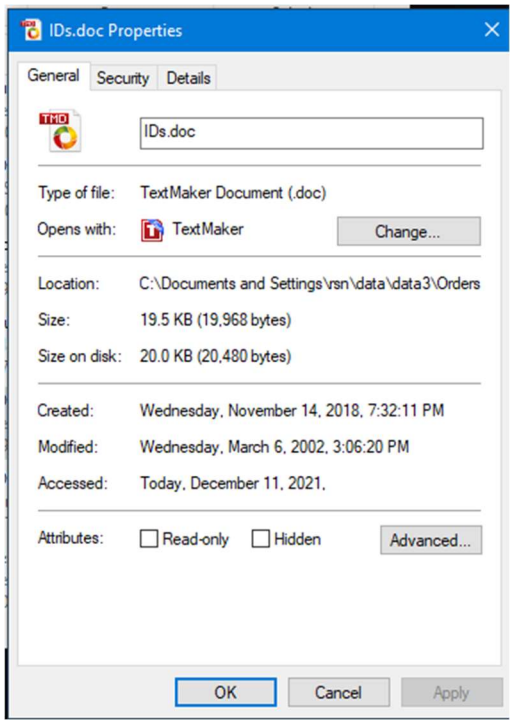
12:53 PM: *IDSRUS.HTM*





3:06 PM: *IDs.doc*



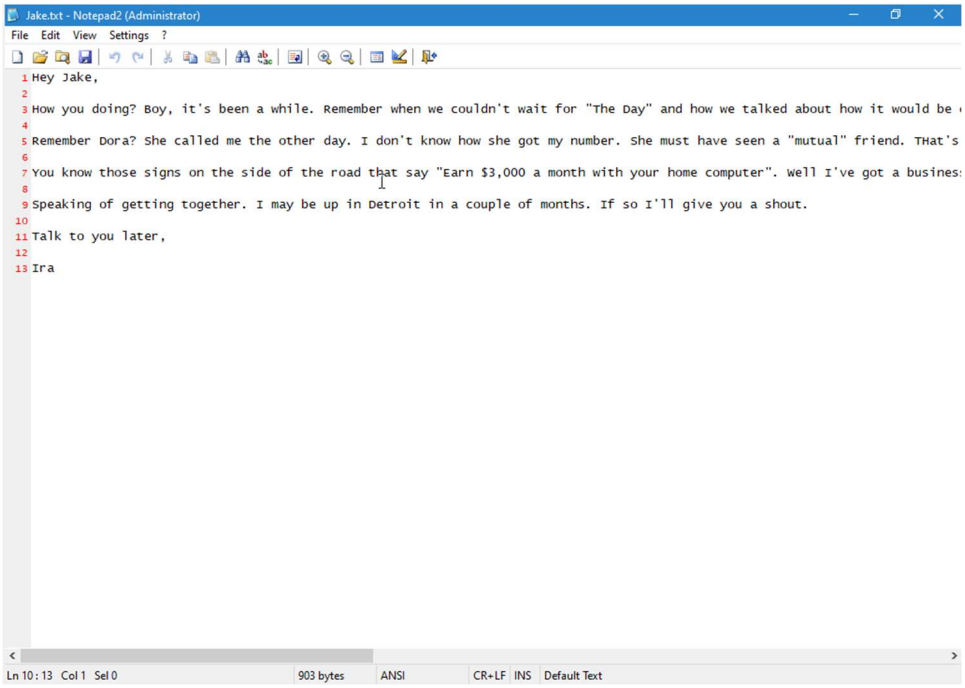


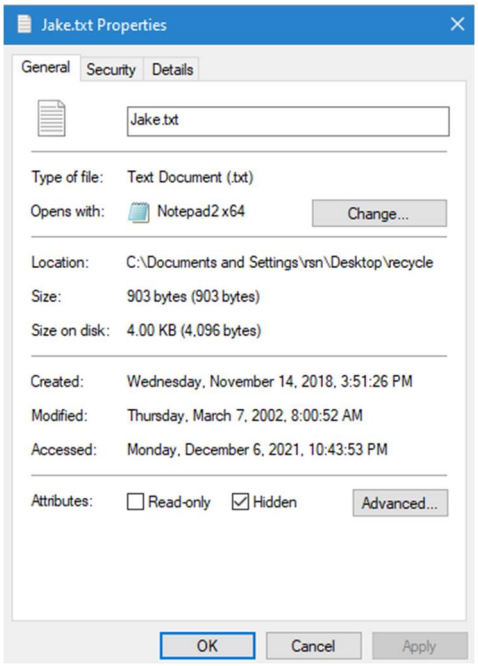
March 7, 2002

On this day, several messages which appear to be coming either to or from the individual Ira Badun appear in the server discussing various topics.

In directory *C:\Documents and Settings\rsn\Desktop\recycle*

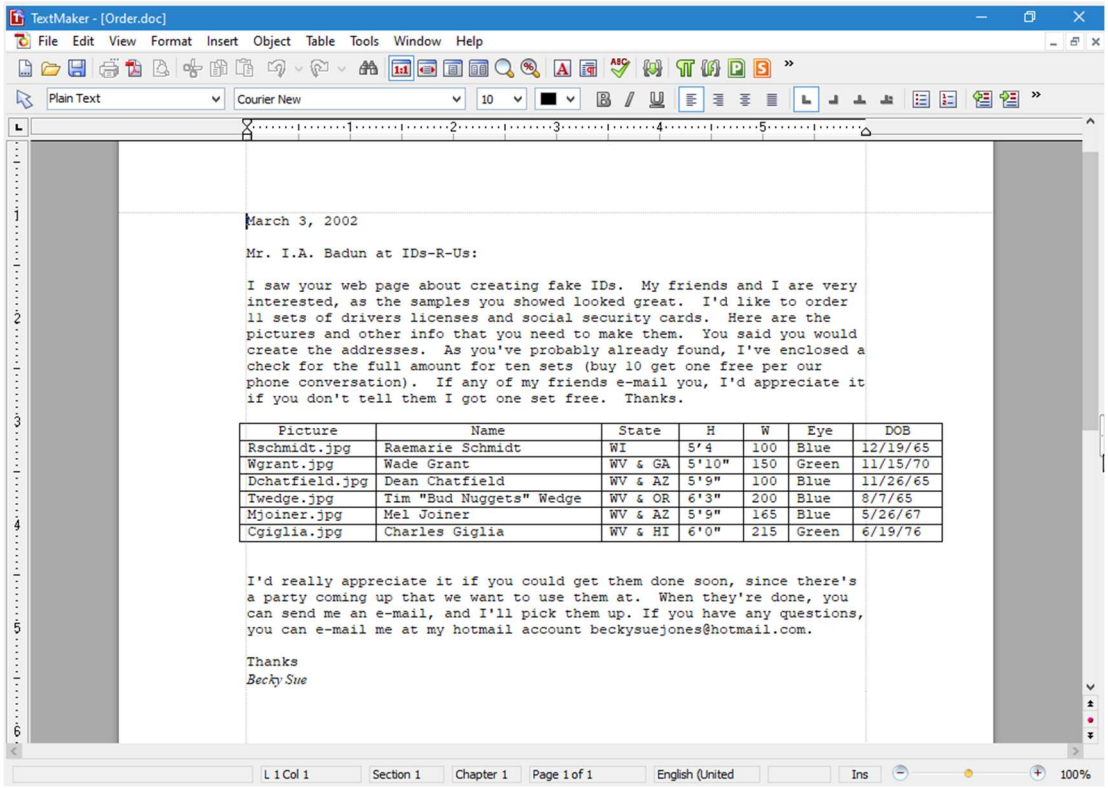
8:00 AM: *Jake.txt*

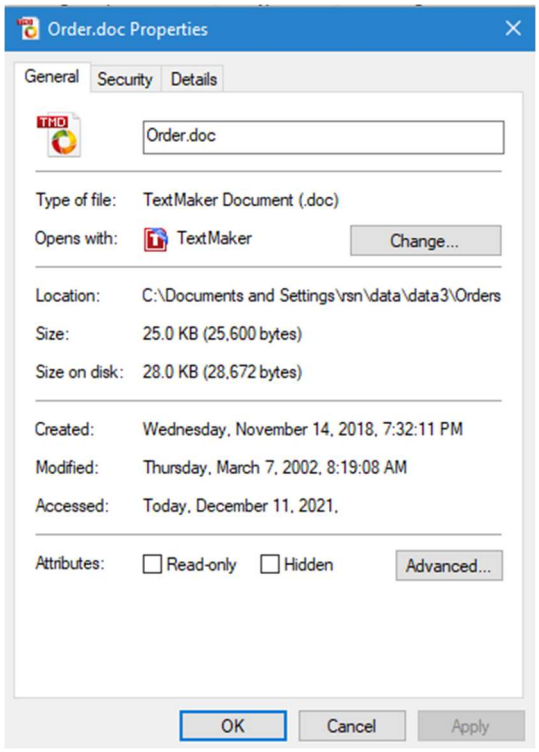




In directory *C:\Documents and Settings\rsn\data\data3\Orders and Records*

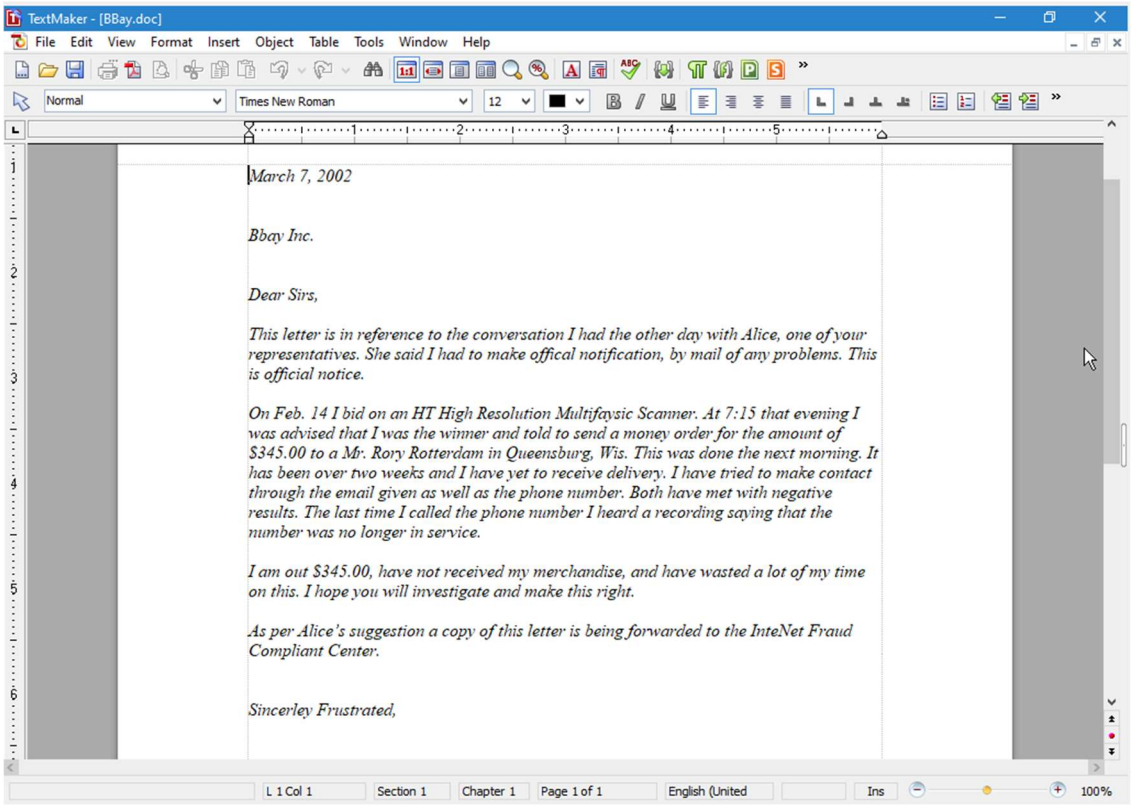
8:19 AM: *Order.doc*

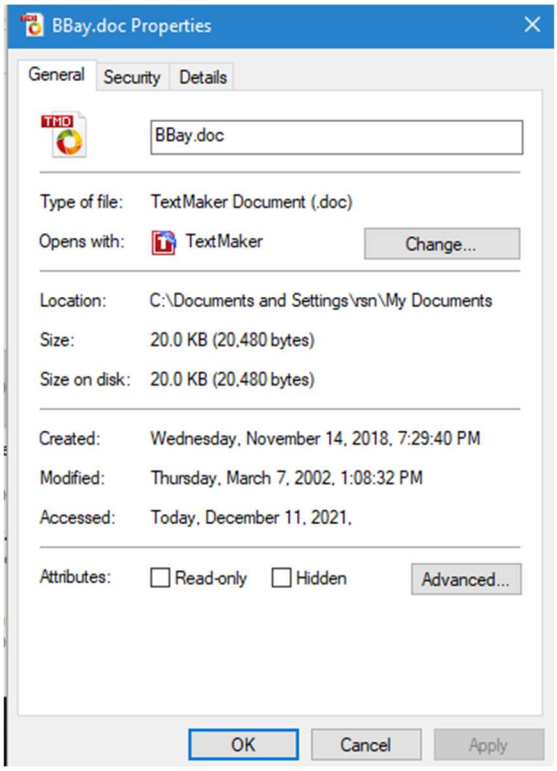




In directory *C:\Documents and Settings\rsn\My Documents*

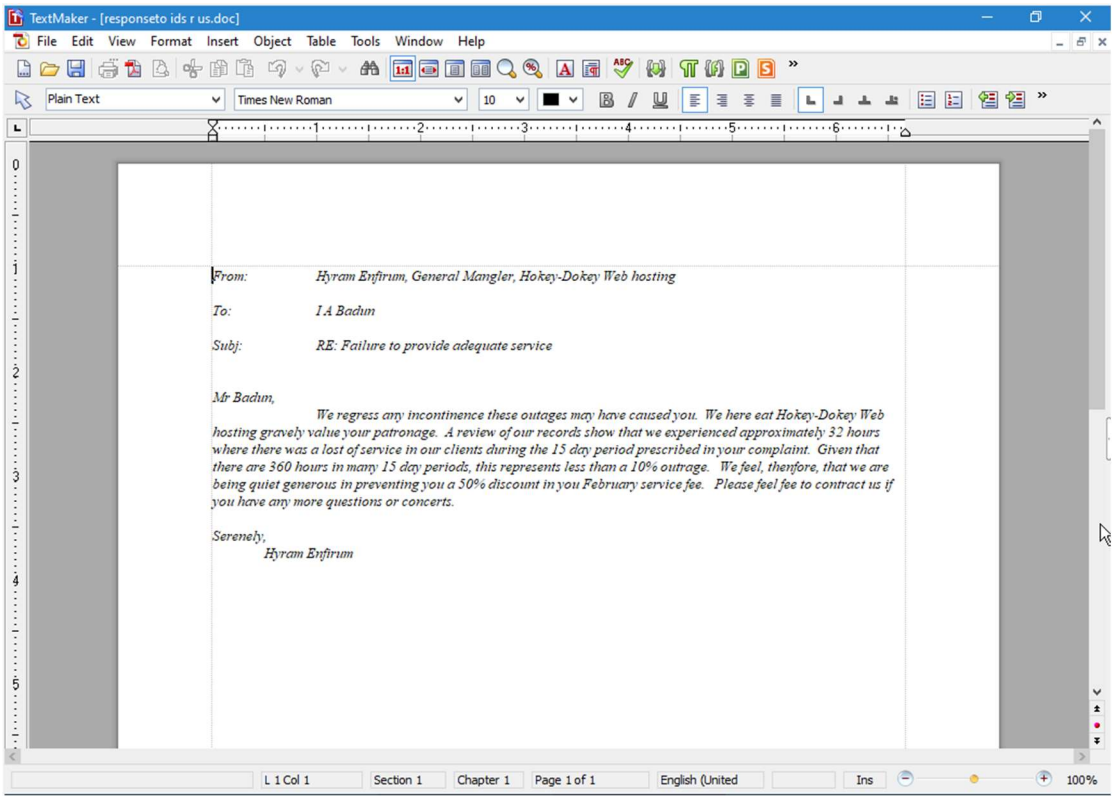
1:08 PM: *BBay.doc*

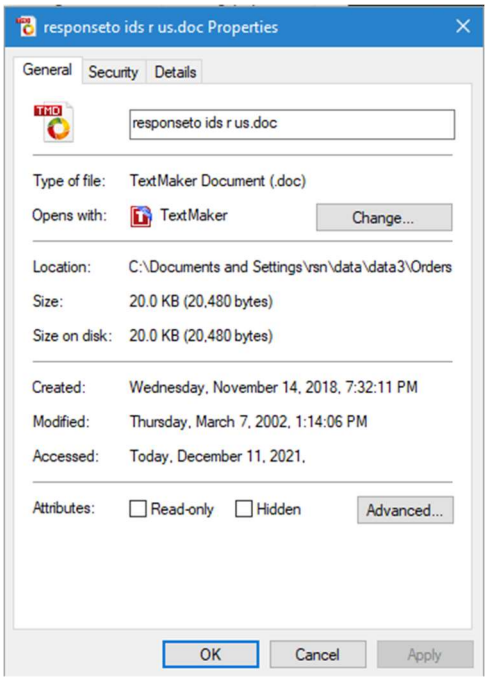




In directory *C:\Documents and Settings\rsn\data\data3\Orders and Records*

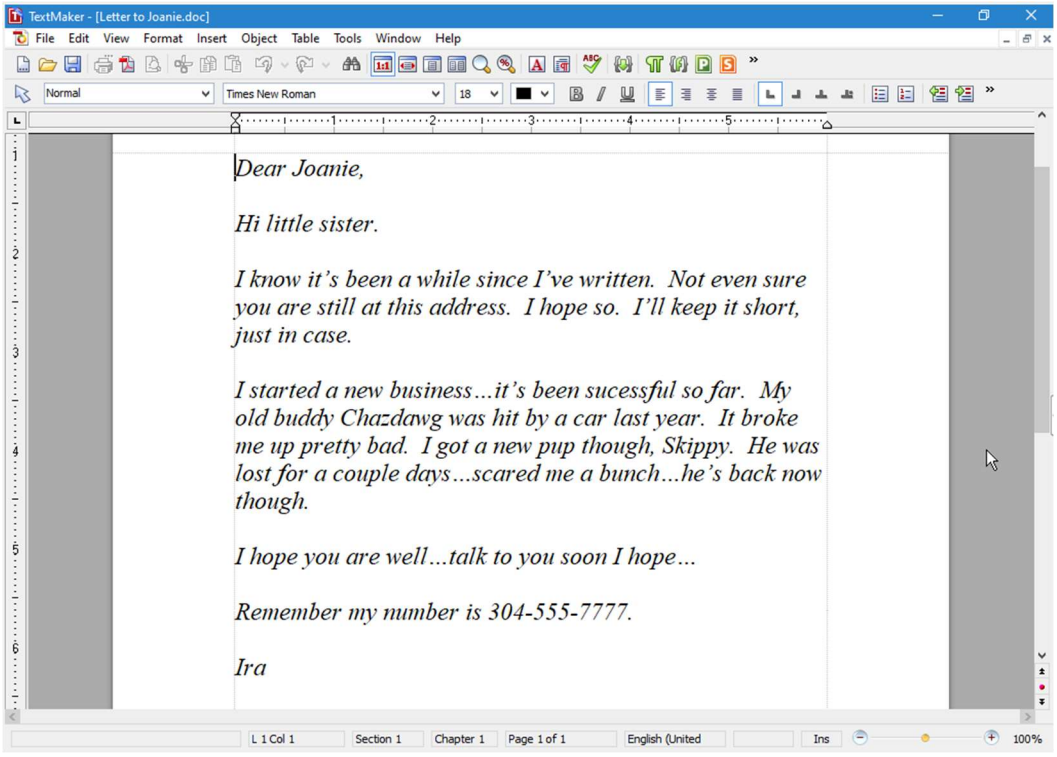
1:14 PM: *responseto ids r us.doc*

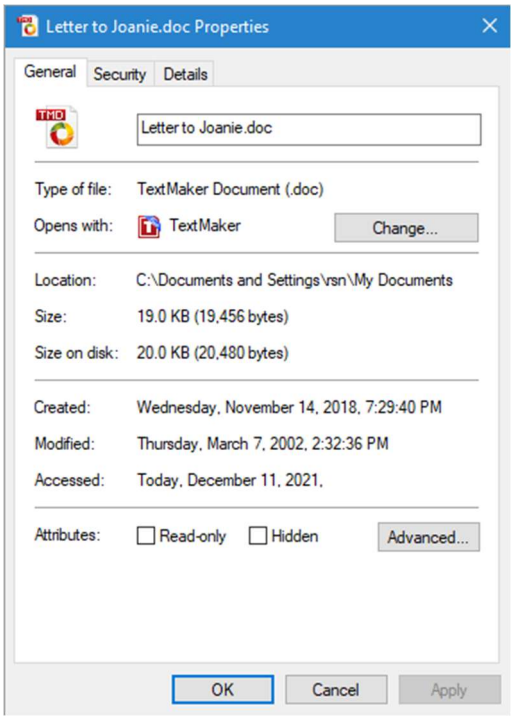




In directory *C:\Documents and Settings\rsn\My Documents*

2:32 PM: *Letter to Joanie.doc*

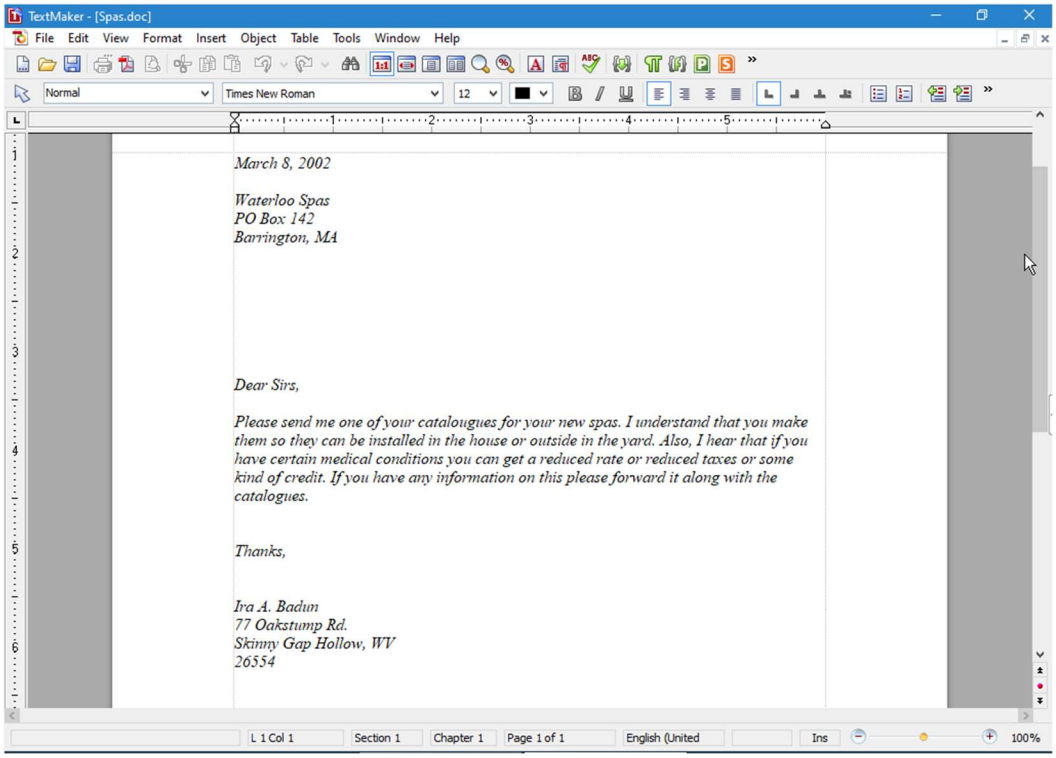


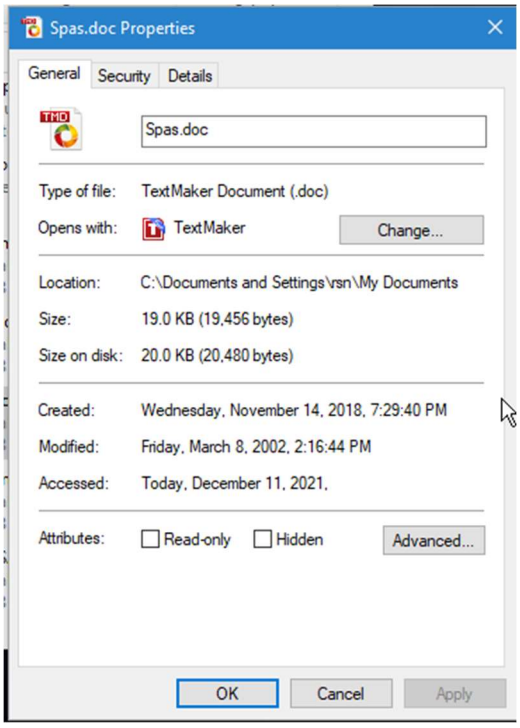


March 8, 2002

On this day, the individual Ira Badun sent an email to Waterloo Spas, inquiring about their spa catalogue.

In directory *C:\Documents and Settings\rsn\My Documents*



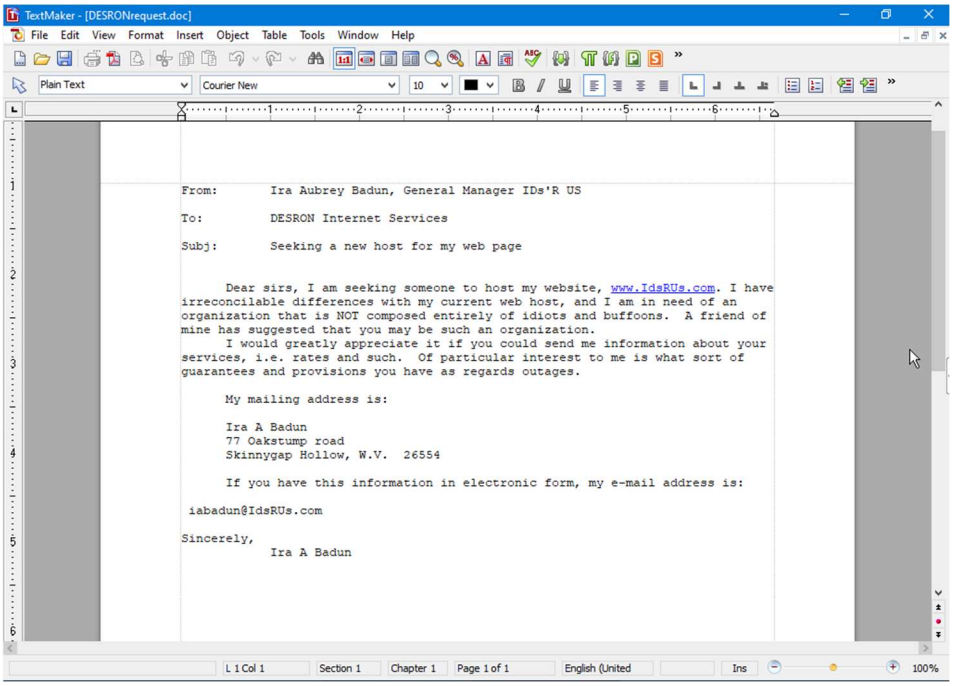


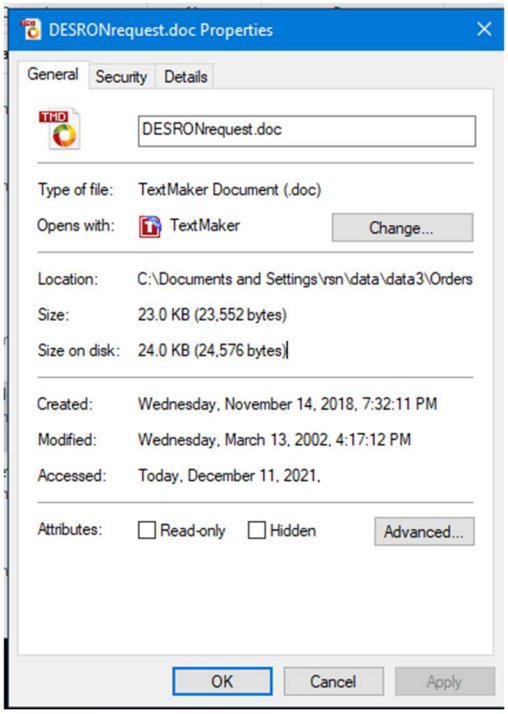
March 13, 2002

On this day, it appears that an email was sent from the individual Ira Badun to DESRON Internet Services. The email is inquiring about hosting a website with the URL www.IdsRUs.com.

In directory *C:\Documents and Settings\rsn\data\data3\Orders and Records*

4:17 PM: *DESRONrequest.doc*



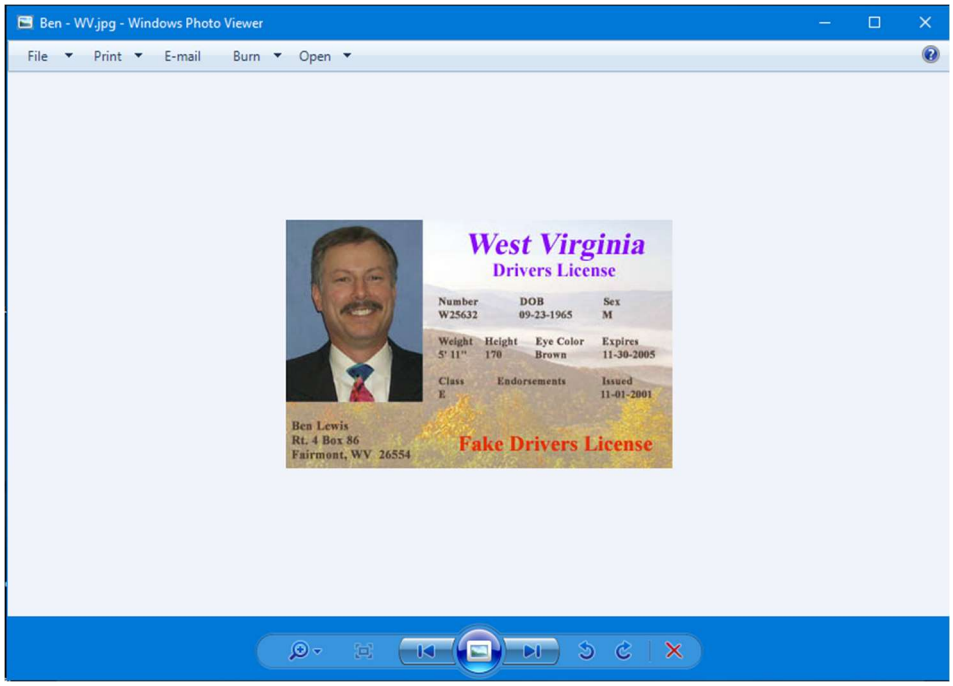


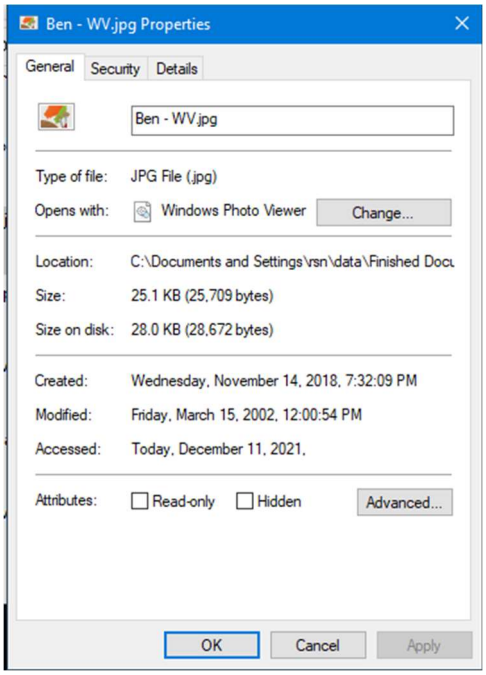
March 15, 2002

On this day, 11 images containing what appear to be driver's licenses were added to the system.

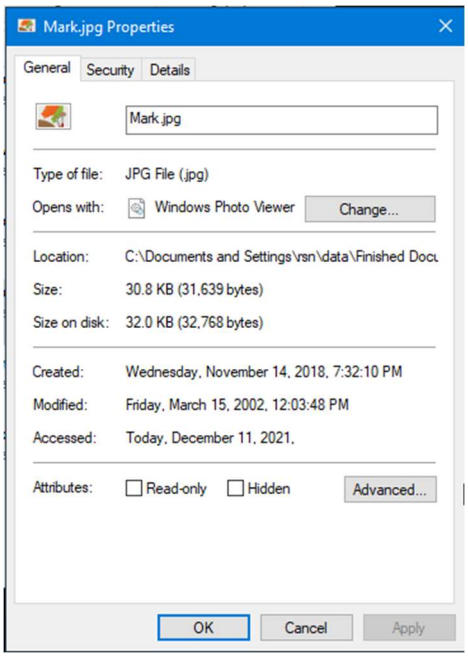
In directory *C:\Documents and Settings\rsn\data\Finished Documents*

12:00 PM: *Ben – WV.jpg*

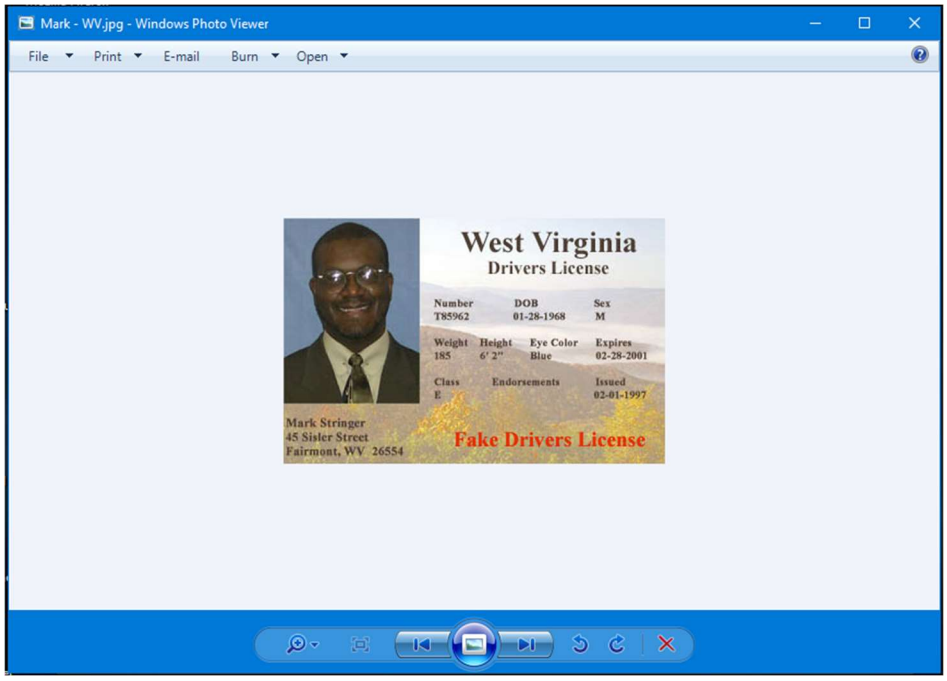


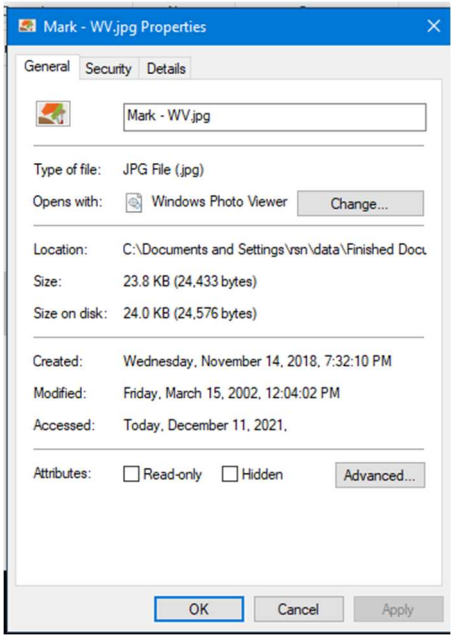


12:03 PM: *Mark.jpg*

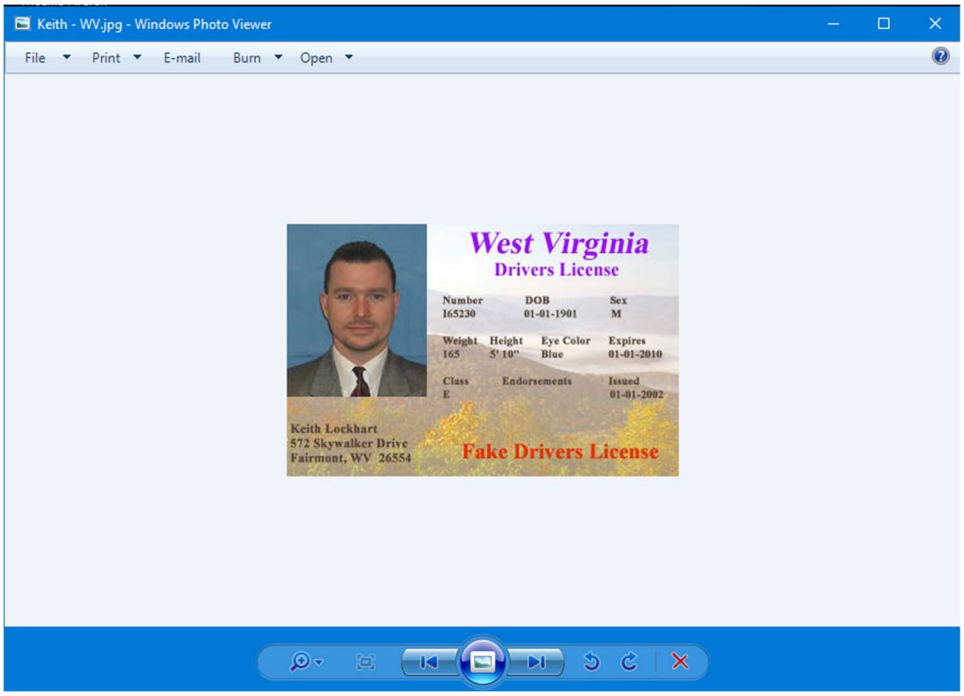


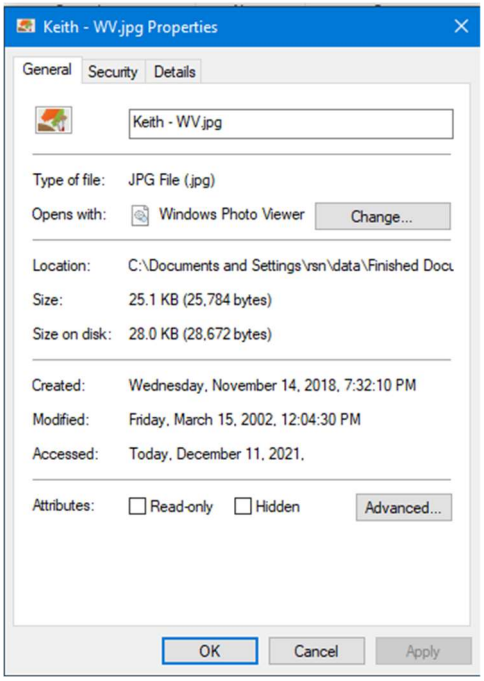
12:04 PM: *Mark – WV.jpg*



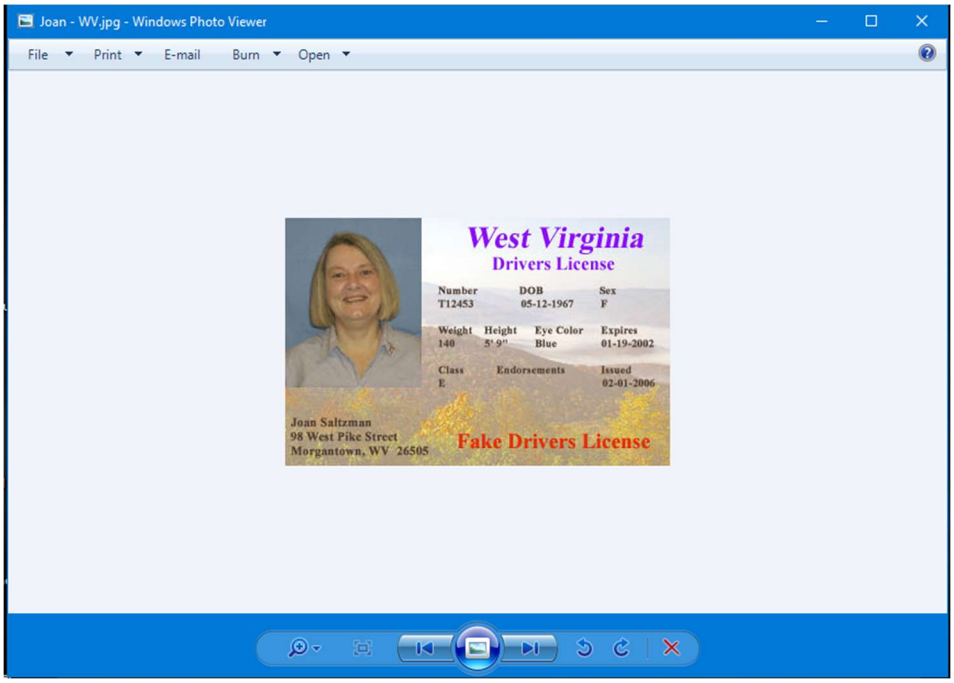


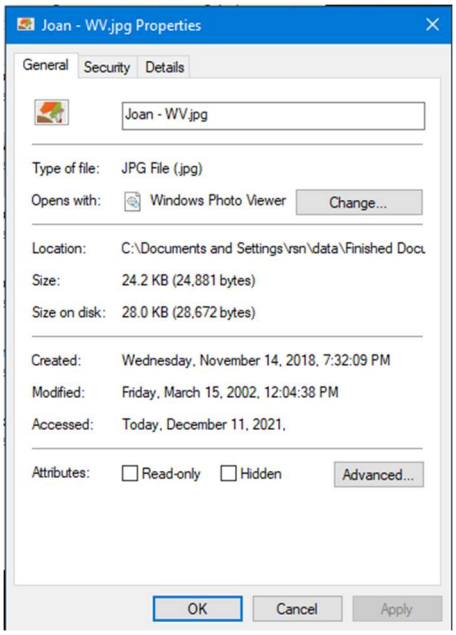
12:04 PM: *Keith – WV.jpg*



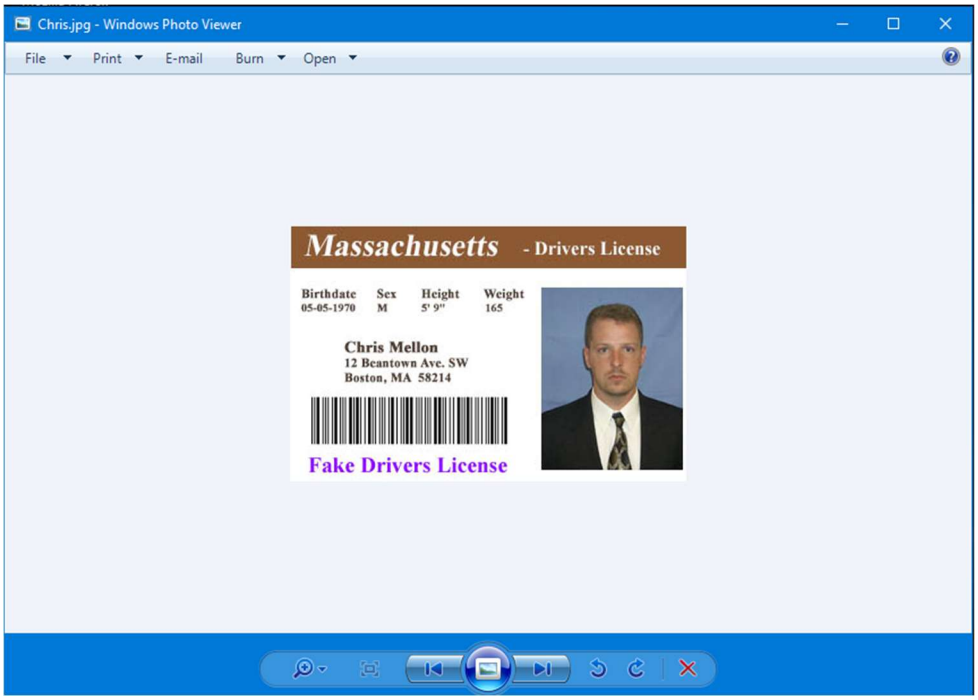


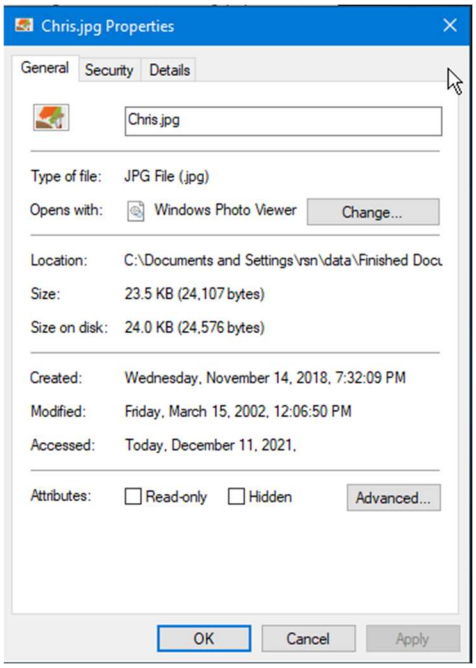
12:04 PM: *Joan – WV.jpg*



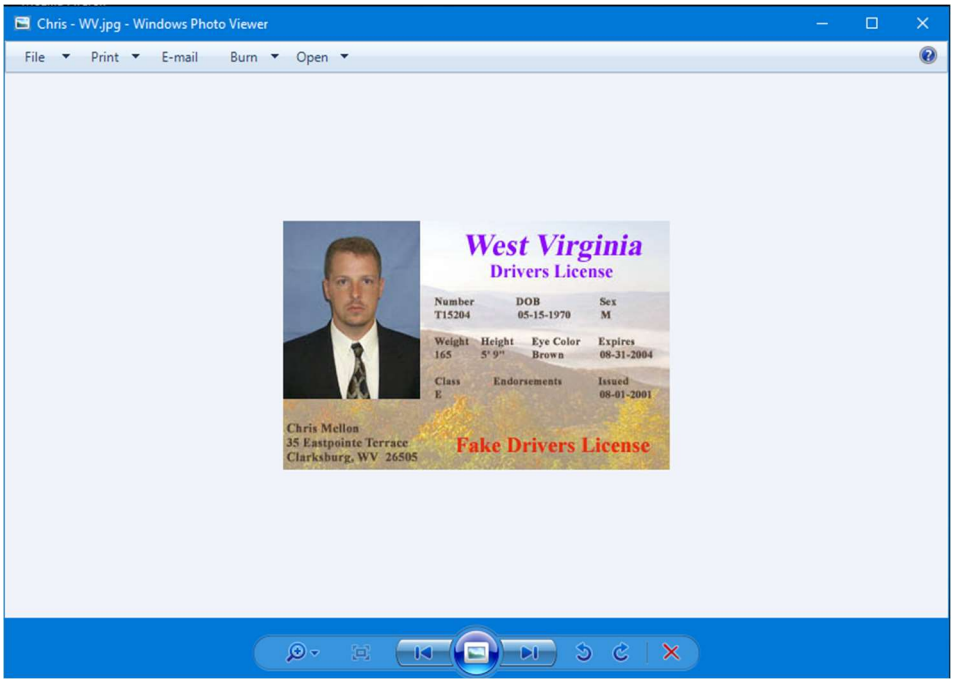


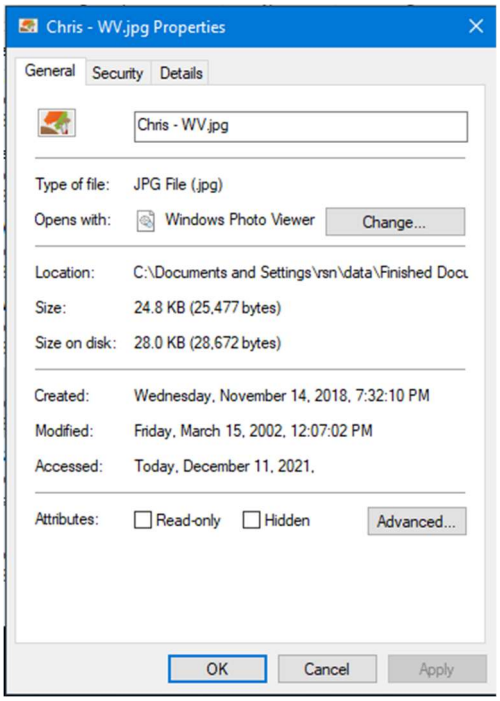
12:06 PM: *Chris.jpg*



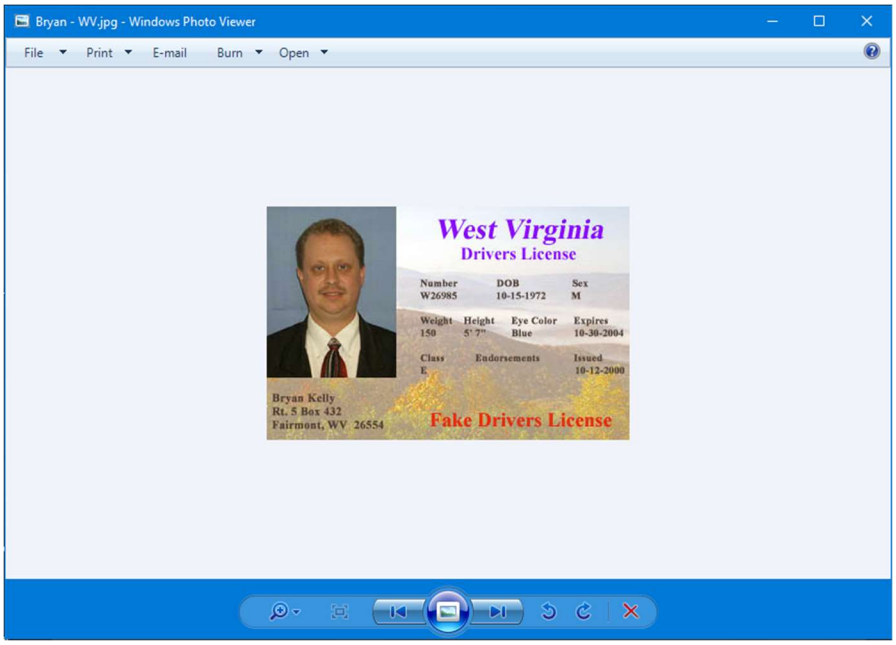


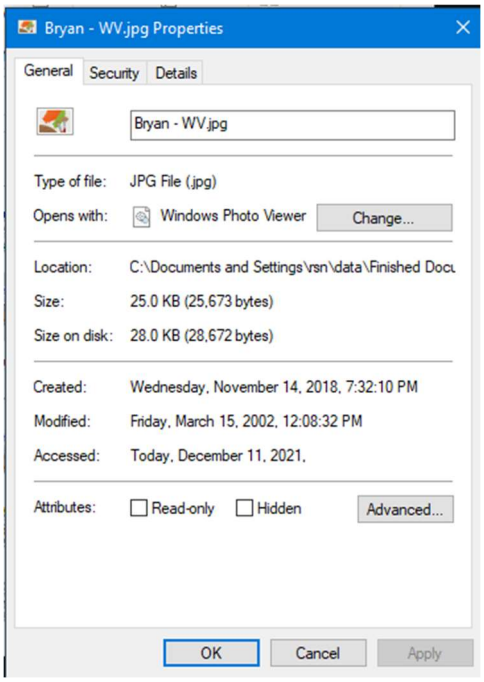
12:07 PM: *Chris – WV.jpg*



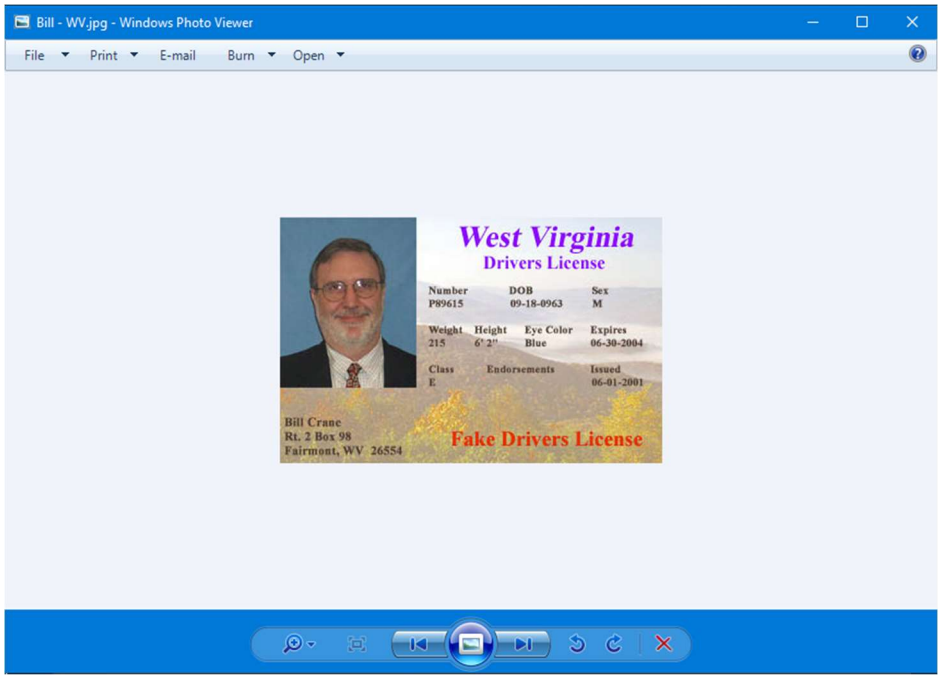


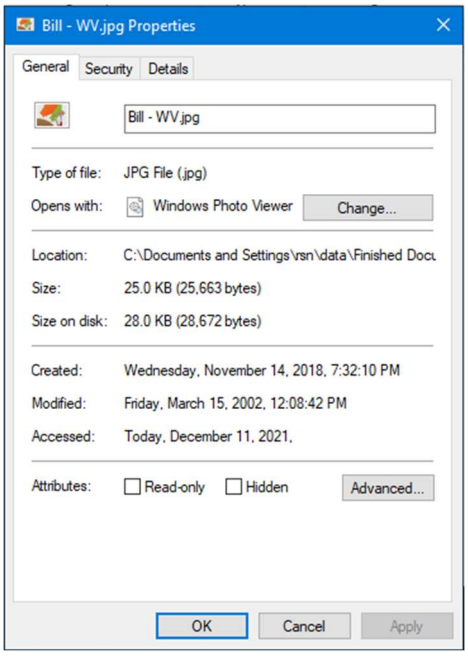
12:08 PM: *Bryan – WV.jpg*



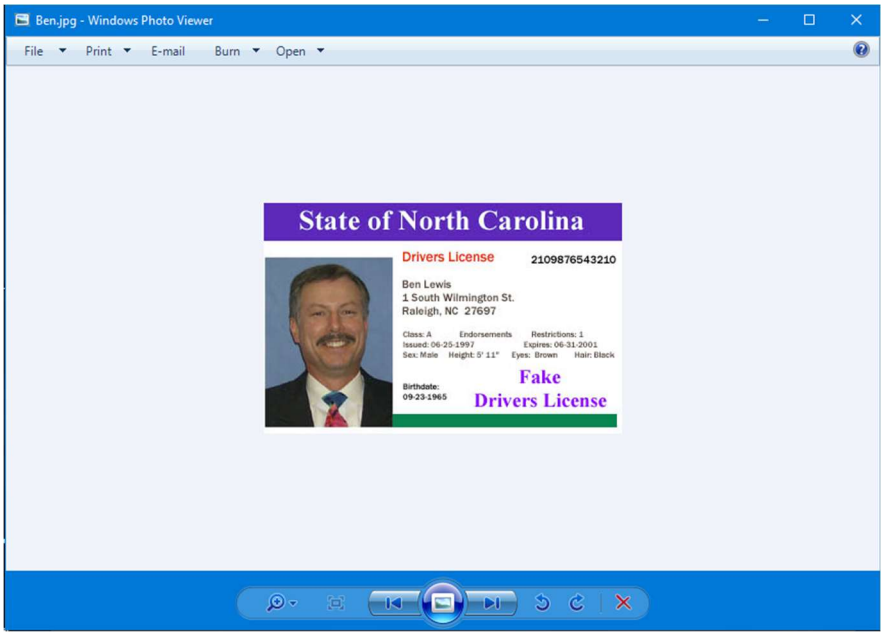


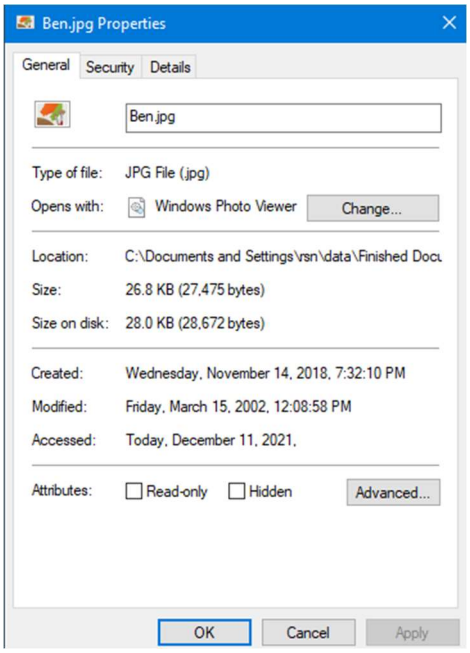
12:08 PM: *Bill – WV.jpg*



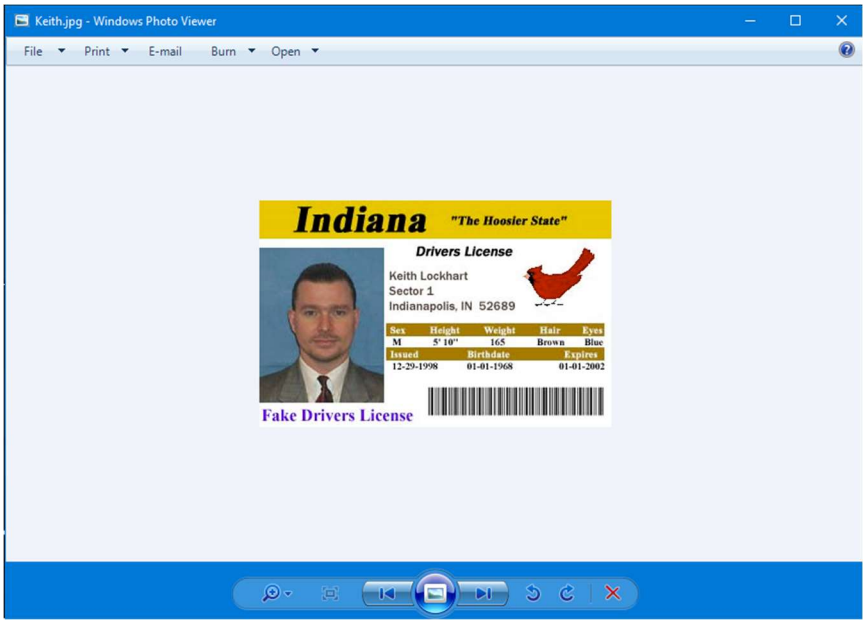


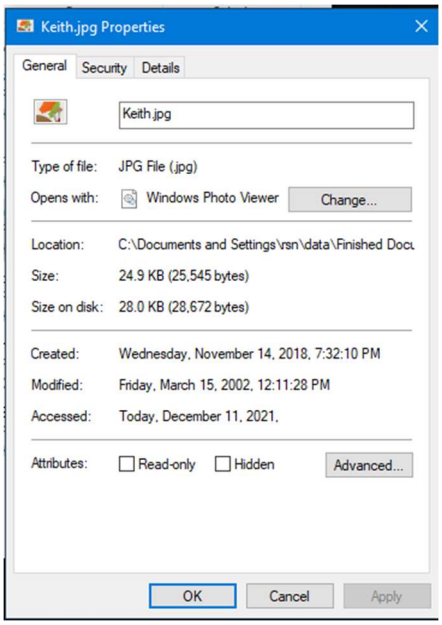
12:08 PM: *Ben.jpg*





12:11 PM: *Keith.jpg*



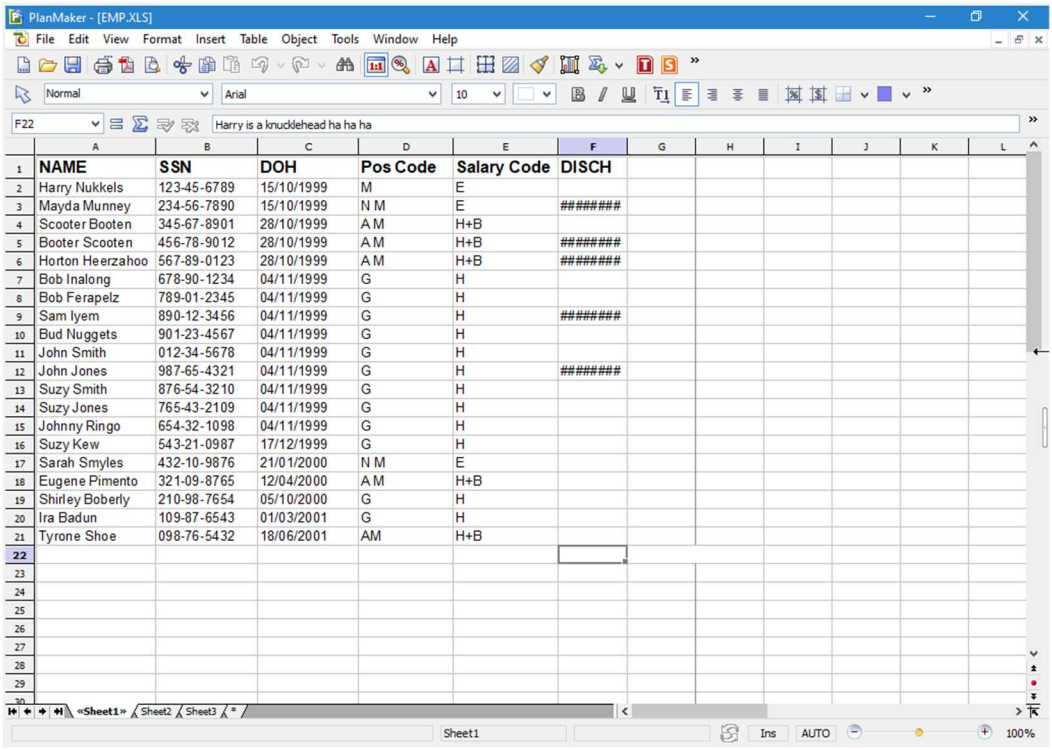


March 16, 2002

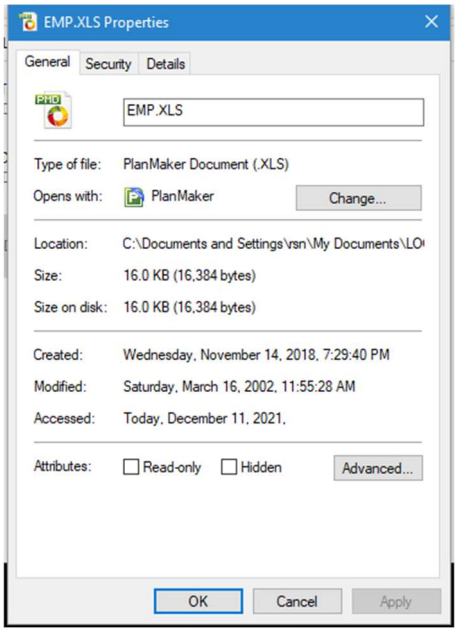
On this day, a new spreadsheet was added, containing 20 names, and what appears to be social security numbers along with some additional information.

In directory *C:\Documents and Settings\rsn\My Documents\LOOT*

11:55 AM: *EMP.XLS*



	NAME	SSN	DOH	Pos Code	Salary Code	DISCH
2	Harry Nukkels	123-45-6789	15/10/1999	M	E	
3	Mayda Munney	234-56-7890	15/10/1999	N M	E	########
4	Scooter Booten	345-67-8901	28/10/1999	A M	H+B	
5	Booter Scooten	456-78-9012	28/10/1999	A M	H+B	########
6	Horton Heerzahoo	567-89-0123	28/10/1999	A M	H+B	########
7	Bob Inalong	678-90-1234	04/11/1999	G	H	
8	Bob Ferapelz	789-01-2345	04/11/1999	G	H	
9	Sam Iyem	890-12-3456	04/11/1999	G	H	########
10	Bud Nuggets	901-23-4567	04/11/1999	G	H	
11	John Smith	012-34-5678	04/11/1999	G	H	
12	John Jones	987-65-4321	04/11/1999	G	H	########
13	Suzy Smith	876-54-3210	04/11/1999	G	H	
14	Suzy Jones	765-43-2109	04/11/1999	G	H	
15	Johnny Ringo	654-32-1098	04/11/1999	G	H	
16	Suzy Kew	543-21-0987	17/12/1999	G	H	
17	Sarah Smyles	432-10-9876	21/01/2000	N M	E	
18	Eugene Pimento	321-09-8765	12/04/2000	A M	H+B	
19	Shirley Boberly	210-98-7654	05/10/2000	G	H	
20	Ira Badun	109-87-6543	01/03/2001	G	H	
21	Tyrone Shoe	098-76-5432	18/06/2001	AM	H+B	

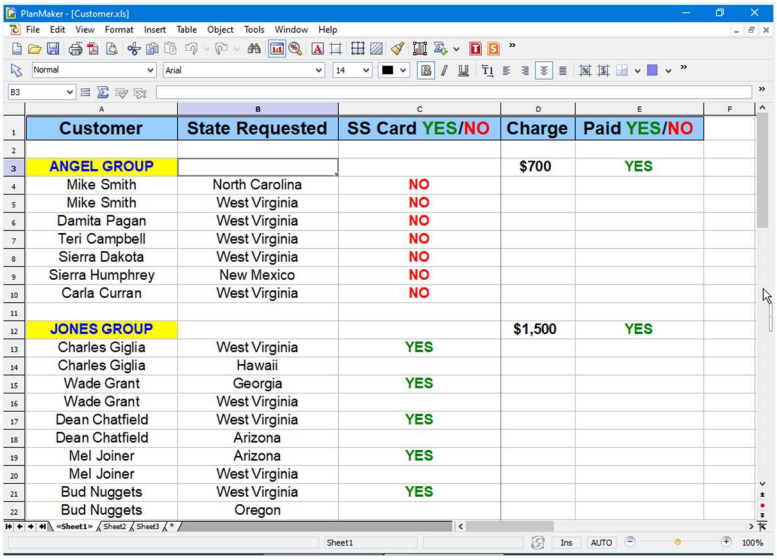


May 24, 2005

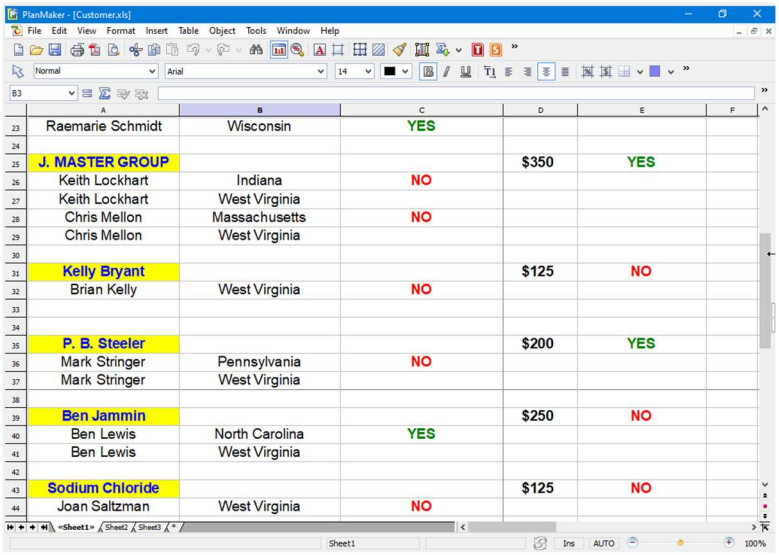
On this day, a spreadsheet was added to the disk drive containing the names of several individuals, along with other information about them.

In directory *C:\Documents and Settings\rsn\data\data3\Orders and Records*

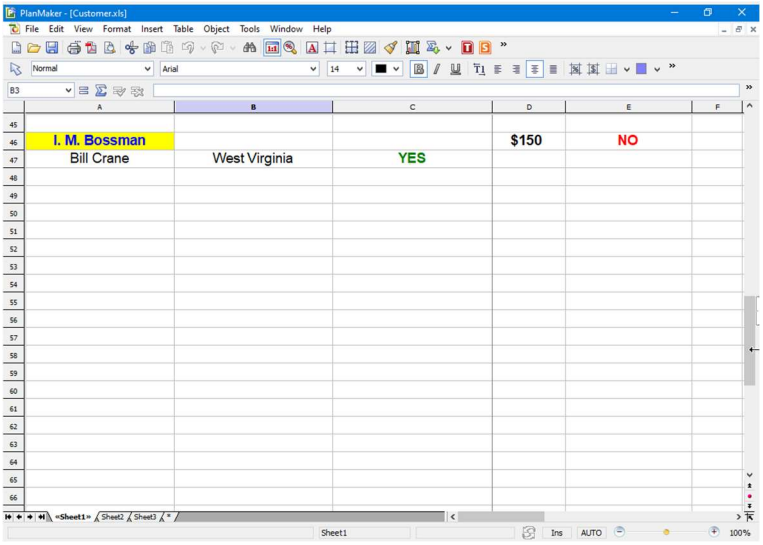
11:44 AM: *Customer.xls*

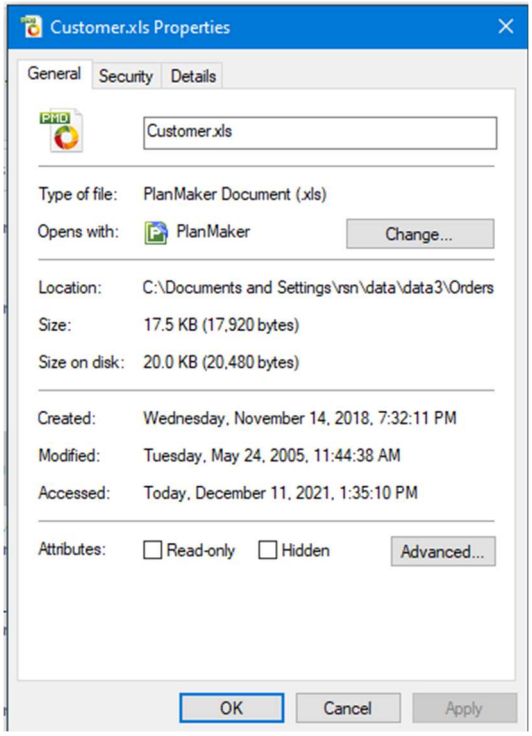


	Customer	State Requested	SS Card YES/NO	Charge	Paid YES/NO
1					
2					
3	ANGEL GROUP			$700	YES
4	Mike Smith	North Carolina	NO		
5	Mike Smith	West Virginia	NO		
6	Damita Pagan	West Virginia	NO		
7	Teri Campbell	West Virginia	NO		
8	Sierra Dakota	West Virginia	NO		
9	Sierra Humphrey	New Mexico	NO		
10	Carla Curran	West Virginia	NO		
11					
12	JONES GROUP			$1,500	YES
13	Charles Giglia	West Virginia	YES		
14	Charles Giglia	Hawaii			
15	Wade Grant	Georgia	YES		
16	Wade Grant	West Virginia			
17	Dean Chatfield	West Virginia	YES		
18	Dean Chatfield	Arizona			
19	Mel Joiner	Arizona	YES		
20	Mel Joiner	West Virginia			
21	Bud Nuggets	West Virginia	YES		
22	Bud Nuggets	Oregon			



23	Raemarie Schmidt	Wisconsin	YES		
24					
25	J. MASTER GROUP			$350	YES
26	Keith Lockhart	Indiana	NO		
27	Keith Lockhart	West Virginia			
28	Chris Mellon	Massachusetts	NO		
29	Chris Mellon	West Virginia			
30					
31	Kelly Bryant			$125	NO
32	Brian Kelly	West Virginia	NO		
33					
34					
35	P. B. Steeler			$200	YES
36	Mark Stringer	Pennsylvania	NO		
37	Mark Stringer	West Virginia			
38					
39	Ben Jammin			$250	NO
40	Ben Lewis	North Carolina	YES		
41	Ben Lewis	West Virginia			
42					
43	Sodium Chloride			$125	NO
44	Joan Saltzman	West Virginia	NO		


PlanMaker - [Customer.xls]
File Edit View Format Insert Table Object Tools Window Help
I. M. Bossman
$150
NO
Bill Crane
West Virginia
YES
Sheet1 Sheet2 Sheet3
Ins AUTO 100%

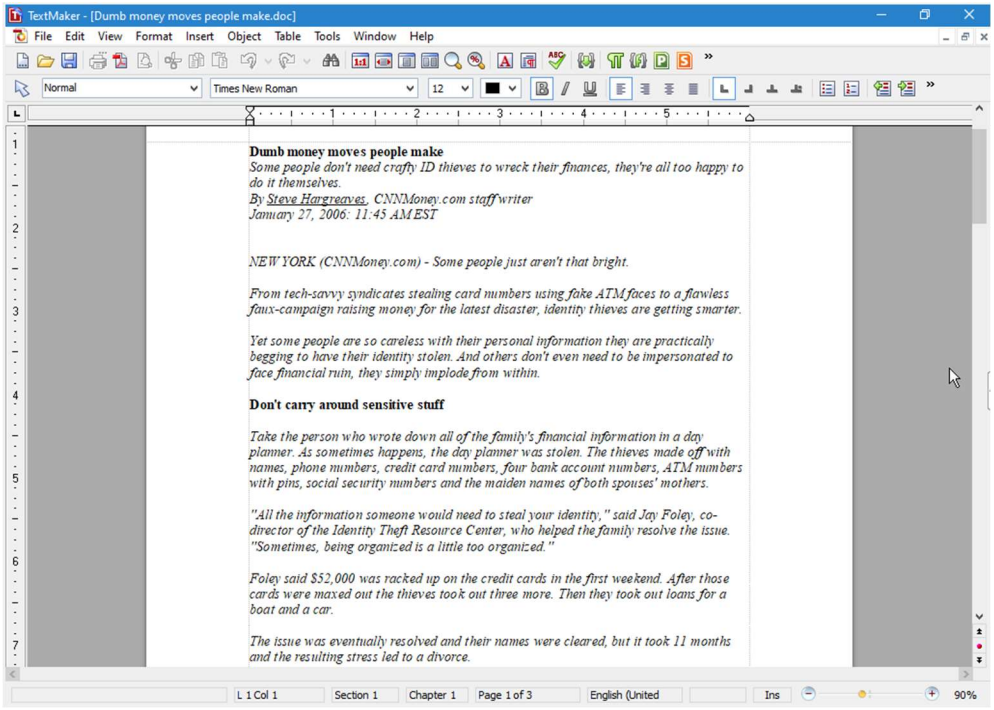

Customer.xls Properties
General Security Details
Customer.xls
Type of file: PlanMaker Document (.xls)
Opens with: PlanMaker
Change...
Location: C:\Documents and Settings\vsn\data\data3\Orders
Size: 17.5 KB (17,920 bytes)
Size on disk: 20.0 KB (20,480 bytes)
Created: Wednesday, November 14, 2018, 7:32:11 PM
Modified: Tuesday, May 24, 2005, 11:44:38 AM
Accessed: Today, December 11, 2021, 1:35:10 PM
Attributes: Read-only Hidden
Advanced...
OK
Cancel
Apply

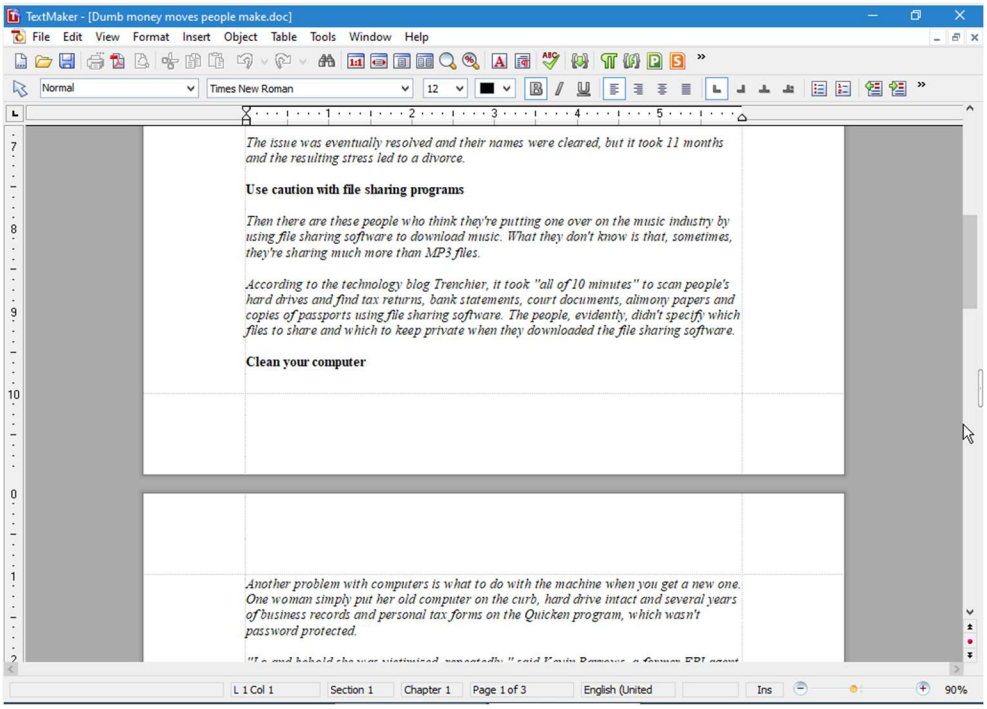
February 6, 2006

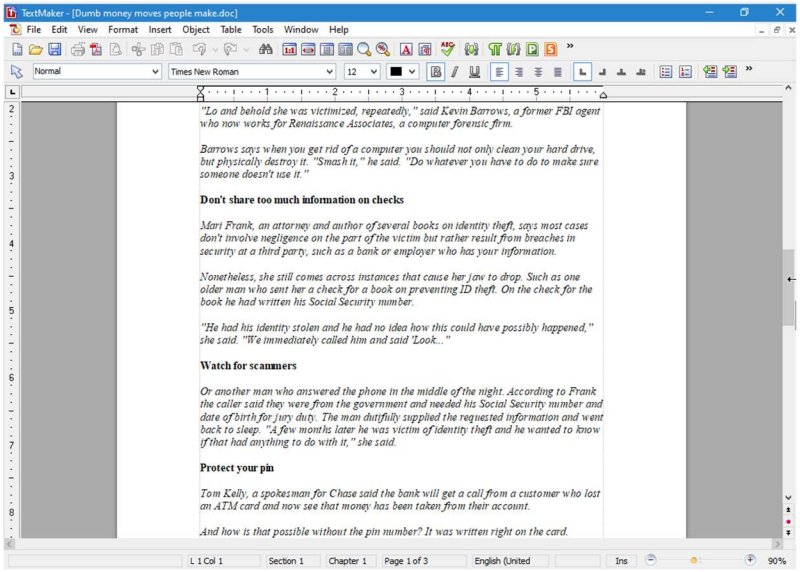
On this day, an article from CNNMoney.com was saved to the system regarding money management.

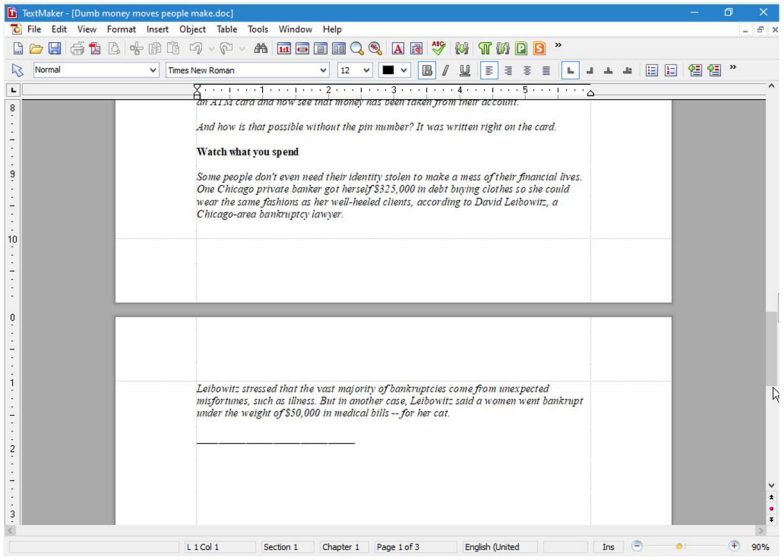
In directory *C:\Documents and Settings\rsn\My Documents*

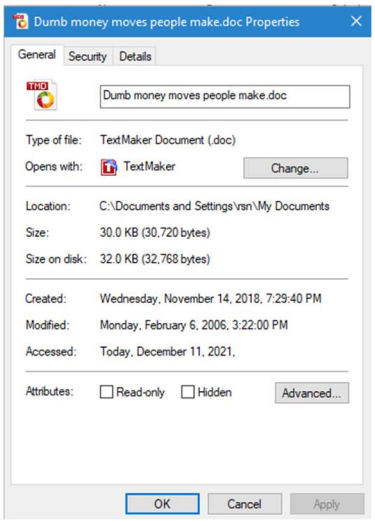
3:22 PM: *Dumb money moves people make.doc*






TextMaker - [Dumb money moves people make.doc]
File Edit View Format Insert Object Table Tools Window Help
Normal
Times New Roman
12
"Lo and behold she was victimized, repeatedly," said Kevin Barrows, a former FBI agent who now works for Renaissance Associates, a computer forensic firm.
Barrows says when you get rid of a computer you should not only clean your hard drive, but physically destroy it. "Smash it," he said. "Do whatever you have to do to make sure someone doesn't use it."
Don't share too much information on checks
Mari Frank, an attorney and author of several books on identity theft, says most cases don't involve negligence on the part of the victim but rather result from breaches in security at a third party, such as a bank or employer who has your information.
Nonetheless, she still comes across instances that cause her jaw to drop. Such as one older man who sent her a check for a book on preventing ID theft. On the check for the book he had written his Social Security number.
"He had his identity stolen and he had no idea how this could have possibly happened," she said. "We immediately called him and said 'Look...'"
Watch for scammers
Or another man who answered the phone in the middle of the night. According to Frank the caller said they were from the government and needed his Social Security number and date of birth for jury duty. The man dutifully supplied the requested information and went back to sleep. "A few months later he was victim of identity theft and he wanted to know if that had anything to do with it," she said.
Protect your pin
Tom Kelly, a spokesman for Chase said the bank will get a call from a customer who lost an ATM card and now see that money has been taken from their account.
And how is that possible without the pin number? It was written right on the card.
L 1 Col 1
Section 1
Chapter 1
Page 1 of 3
English (United
Ins
90%


TextMaker - [Dumb money moves people make.doc]
File Edit View Format Insert Object Table Tools Window Help
Normal
Times New Roman
12
an ATM card and now see that money has been taken from their account.
And how is that possible without the pin number? It was written right on the card.
Watch what you spend
Some people don't even need their identity stolen to make a mess of their financial lives. One Chicago private banker got herself $325,000 in debt buying clothes so she could wear the same fashions as her well-heeled clients, according to David Leibowitz, a Chicago-area bankruptcy lawyer.
Leibowitz stressed that the vast majority of bankruptcies come from unexpected misfortunes, such as illness. But in another case, Leibowitz said a women went bankrupt under the weight of $50,000 in medical bills -- for her cat.
L 1 Col 1
Section 1
Chapter 1
Page 1 of 3
English (United
Ins
90%

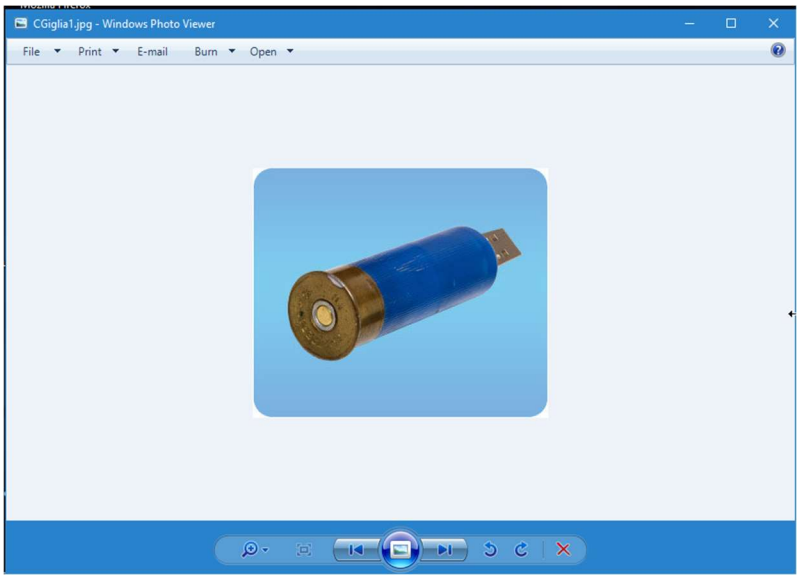

Dumb money moves people make.doc Properties
General
Security
Details
Dumb money moves people make.doc
Type of file: TextMaker Document (.doc)
Opens with: TextMaker
Change...
Location: C:\Documents and Settings\vsn\My Documents
Size: 30.0 KB (30,720 bytes)
Size on disk: 32.0 KB (32,768 bytes)
Created: Wednesday, November 14, 2018, 7:29:40 PM
Modified: Monday, February 6, 2006, 3:22:00 PM
Accessed: Today, December 11, 2021,
Attributes: Read-only Hidden
Advanced...
OK
Cancel
Apply

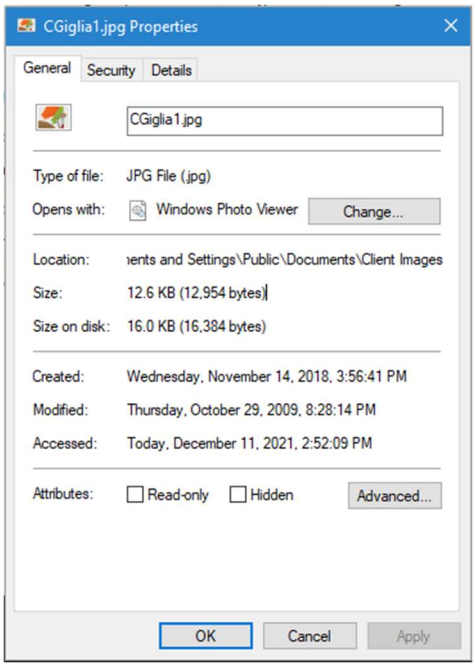
October 29, 2009

On this day, an image appeared on the system that appears to picture some type of flash drive.

In directory *C:\Documents and Settings\Public\Documents\Client Images*

8:28 PM: *CGiglia1.jpg*

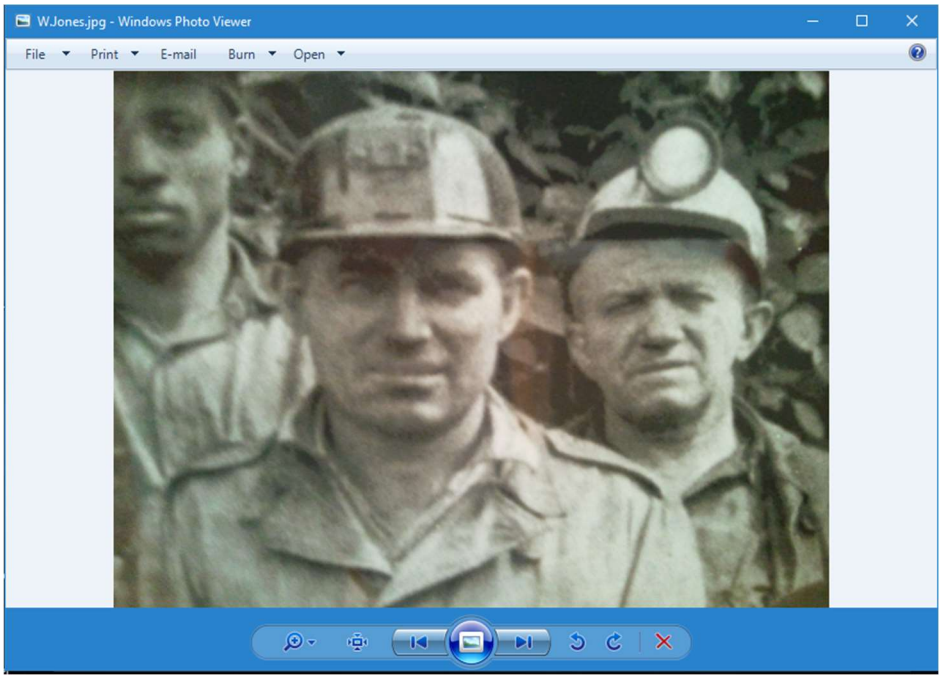


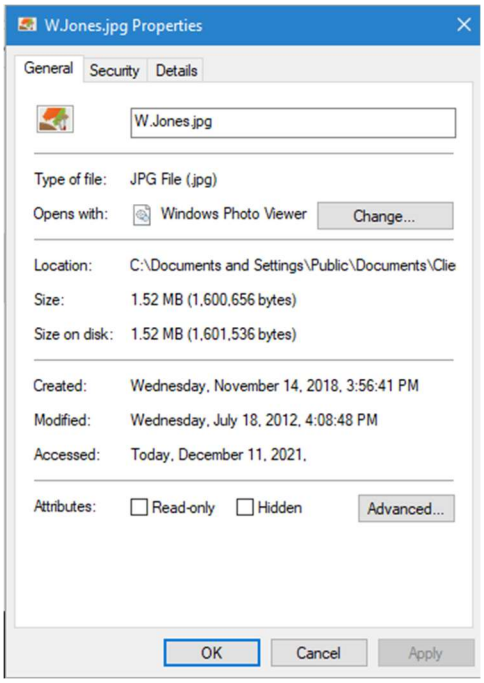


July 18, 2012

On this day, an image appeared on the system of 3 individuals.

In directory *C:\Documents and Settings\Public\Documents\Client Images*



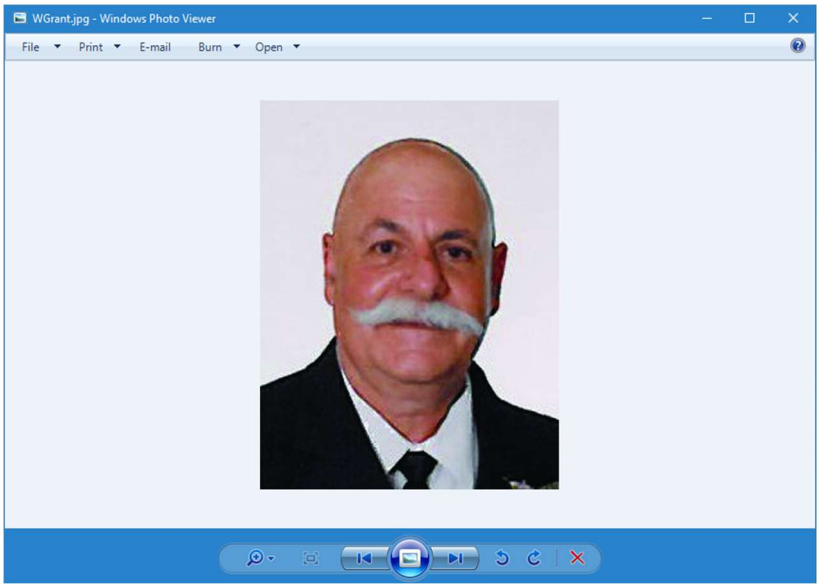


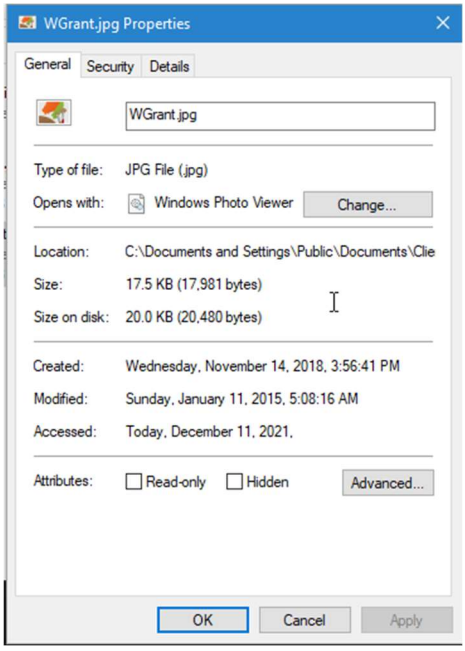
January 11, 2015

On this day, 4 images appeared on the system of various individuals.

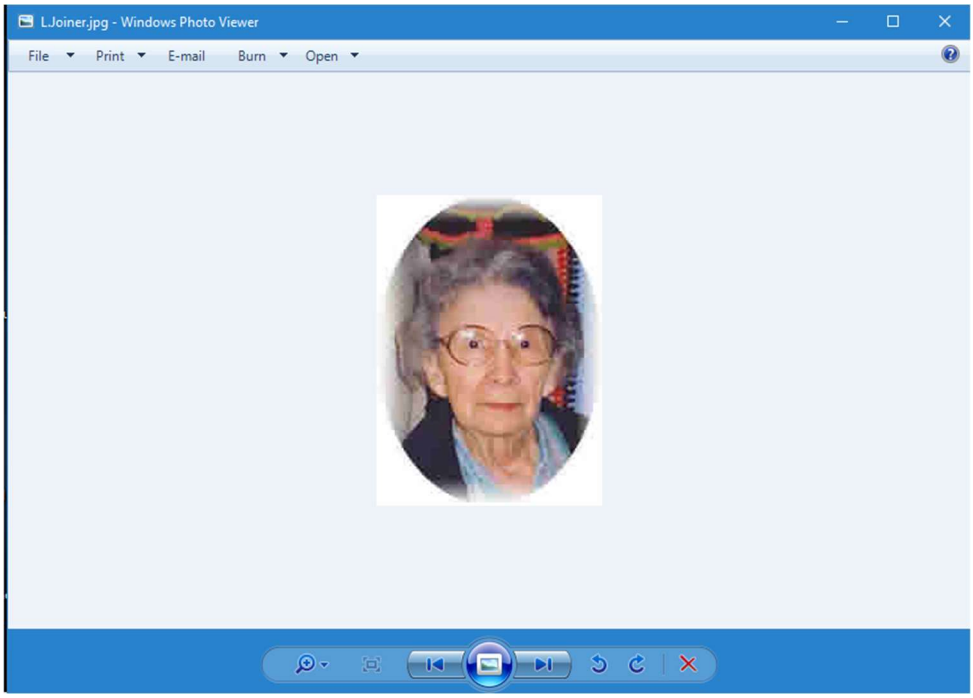
In directory *C:\Documents and Settings\Public\Documents\Client Images*

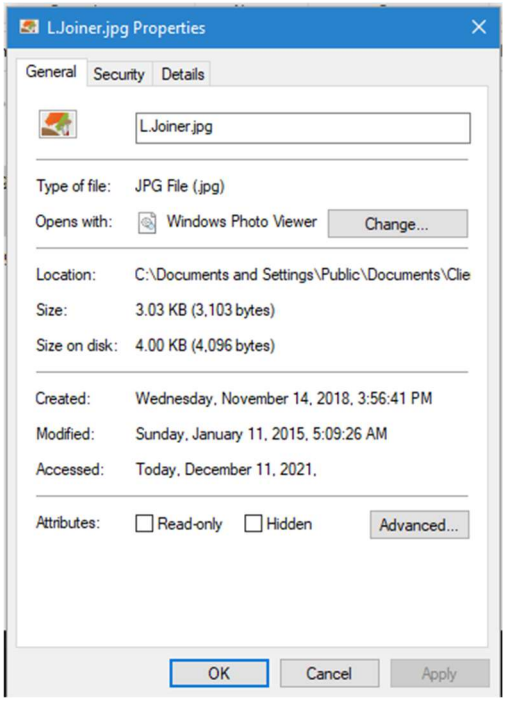
5:08 AM: *WGrant.jpg*



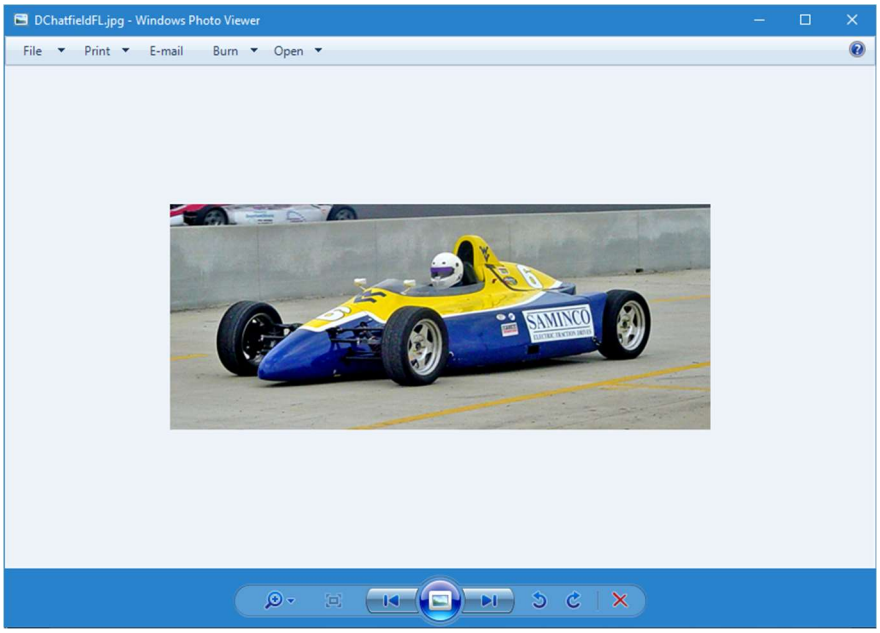


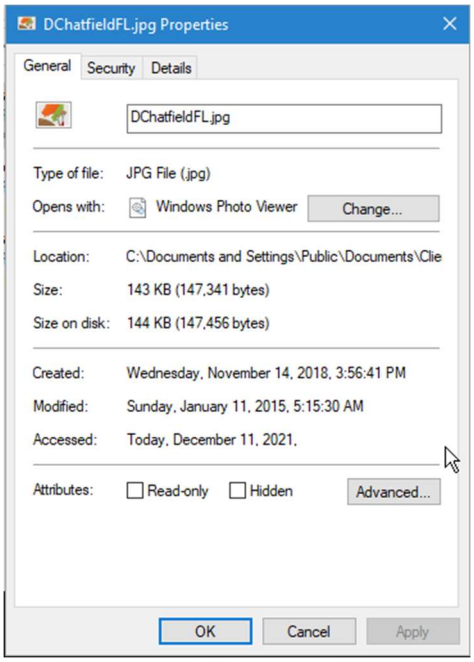
5:09 AM: *L.Joiner.jpg*



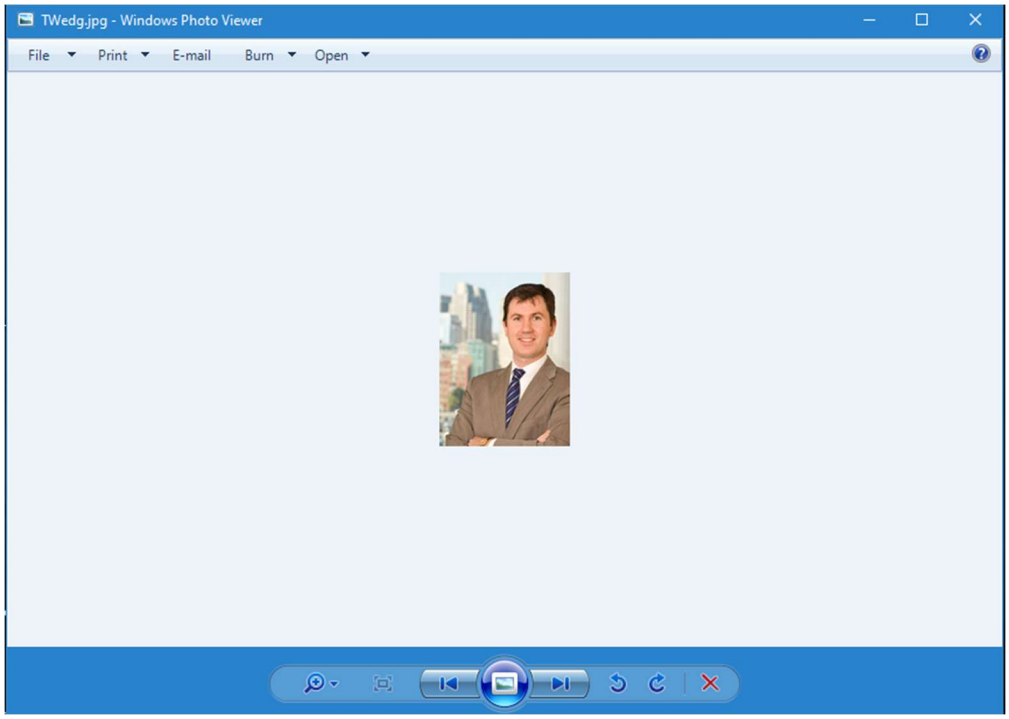


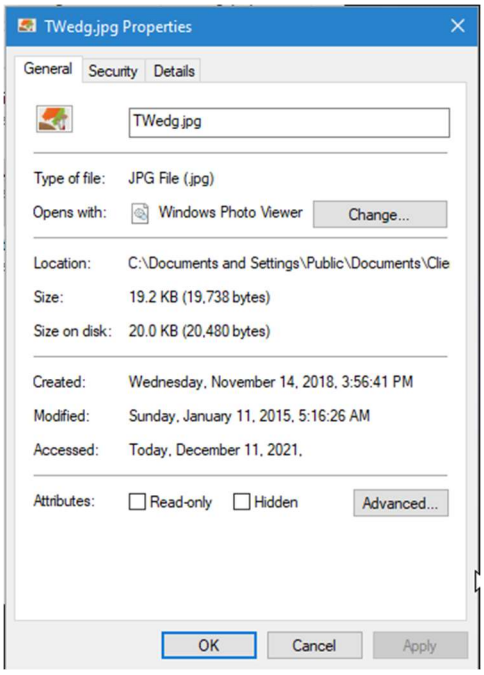
5:15 AM: *DChatfieldFL.jpg*





5:16 AM: *TWedg.jpg*



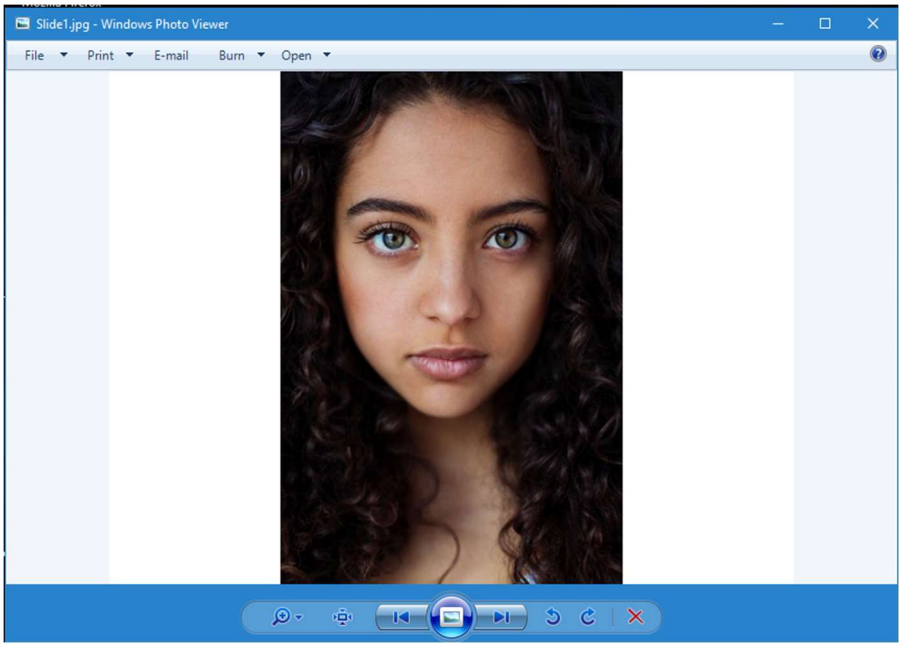


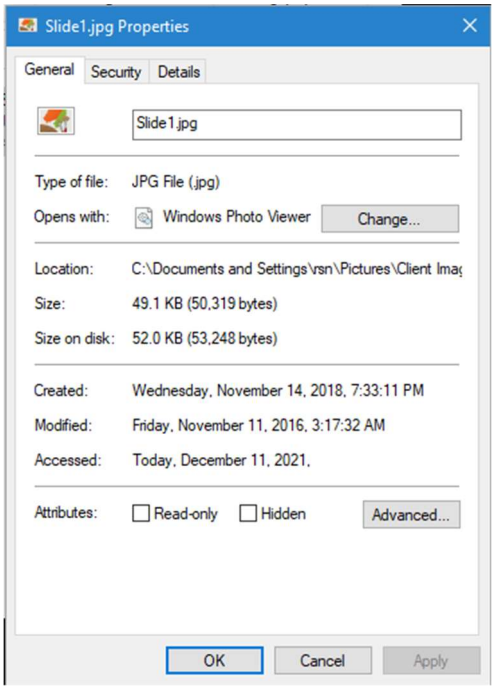
November 11, 2016

On this day, 10 images of various people appeared on the system.

In directory *C:\Documents and Settings\rsn\Pictures\Client Images\CGiglia*

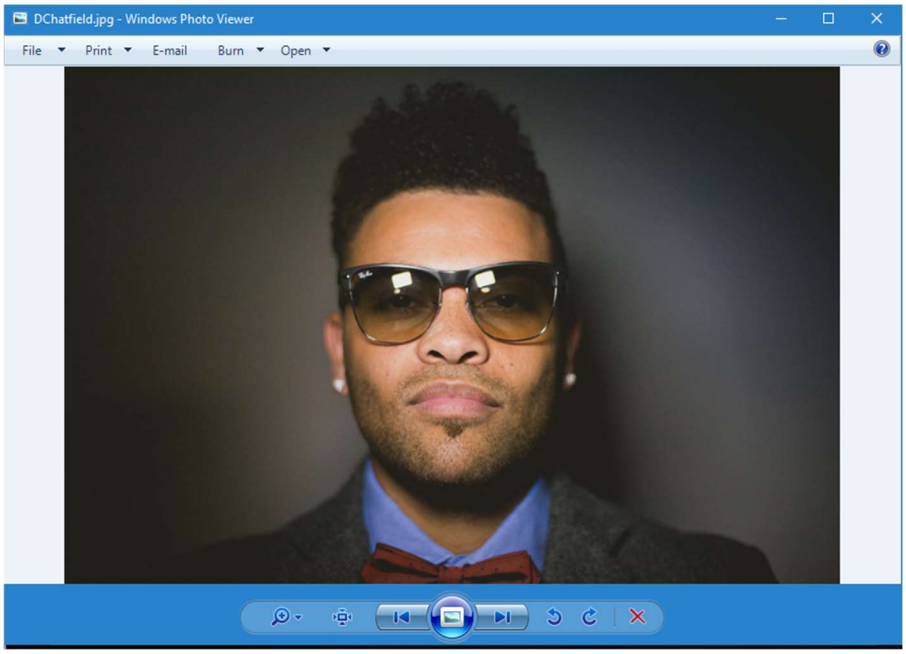
3:17 AM: *Slide1.jpg*

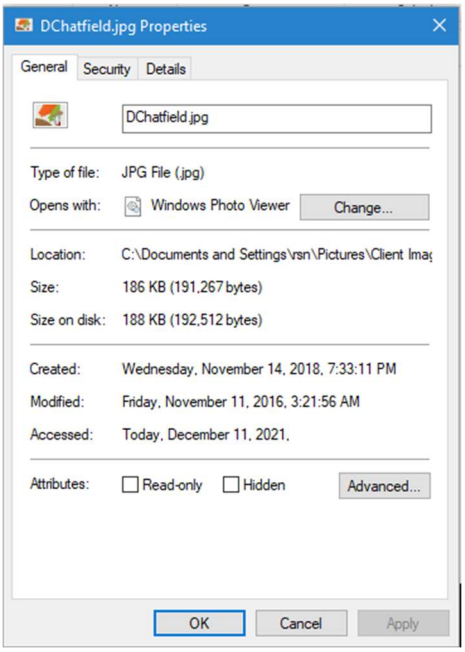




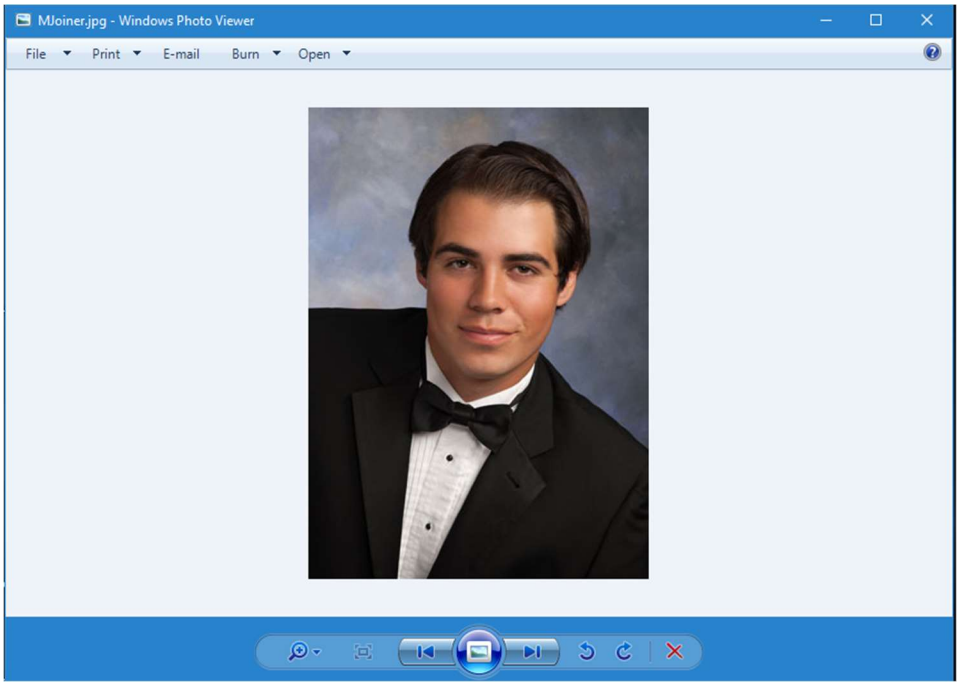
In directory *C:\Documents and Settings\rsn\Pictures\Client Images*

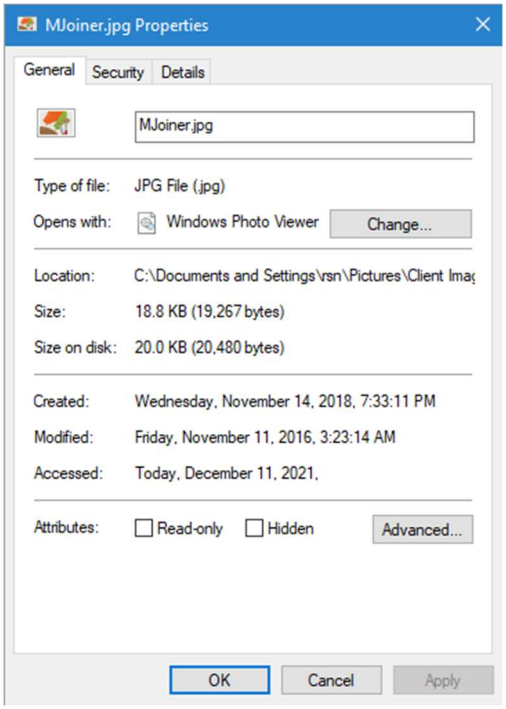
3:21 AM: *DChatfield.jpg*



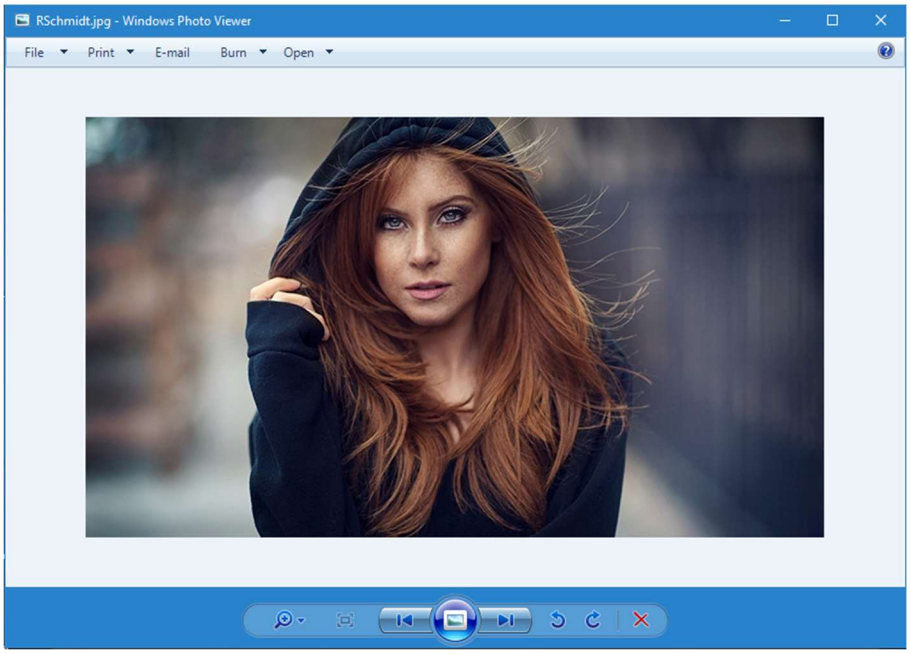


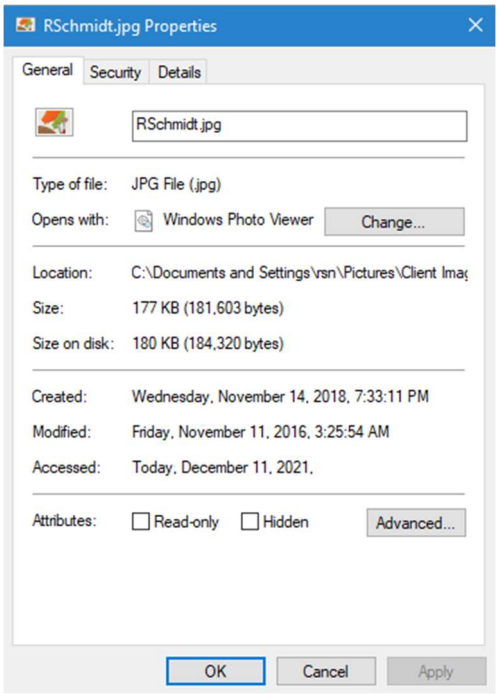
3:23 AM: *MJoiner.jpg*



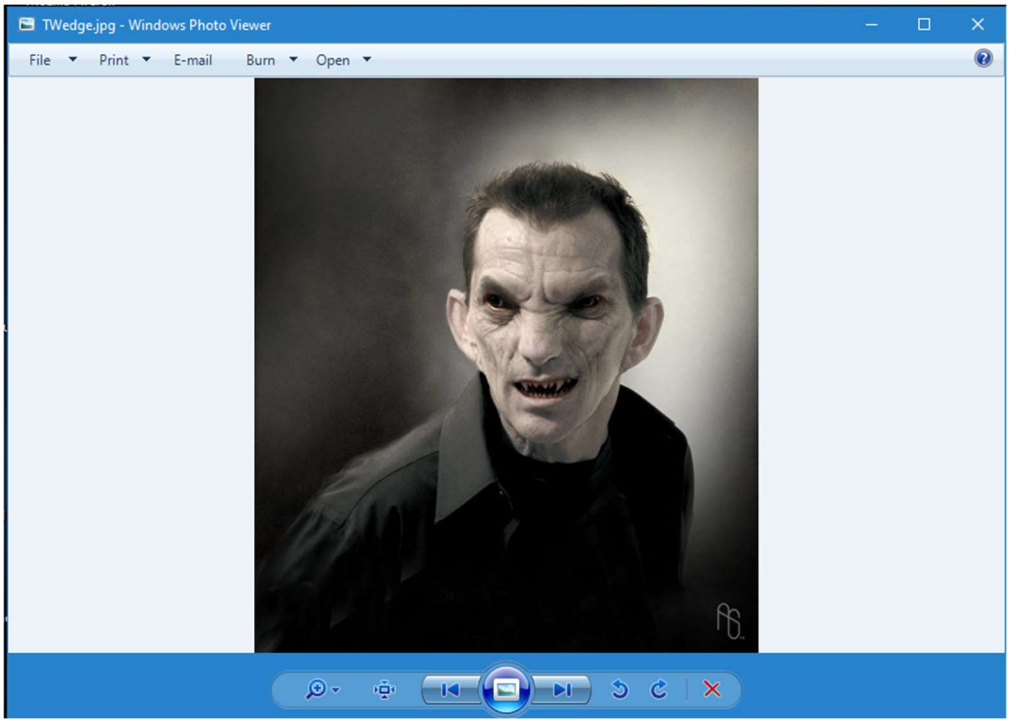


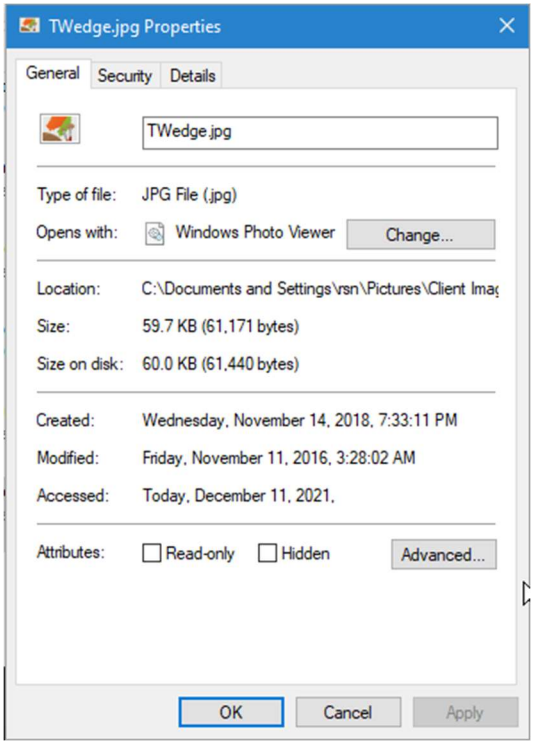
3:25 AM: *RSchmidt.jpg*



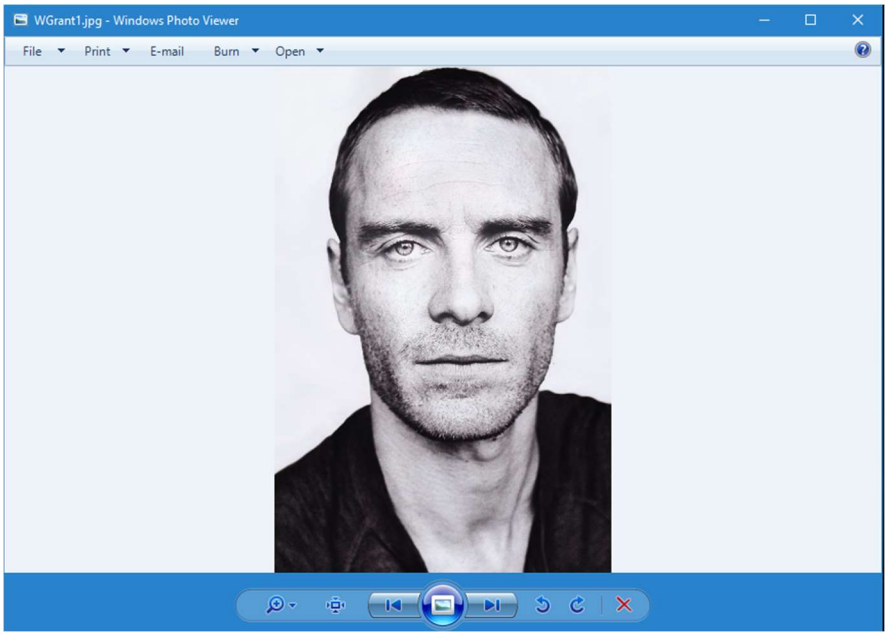


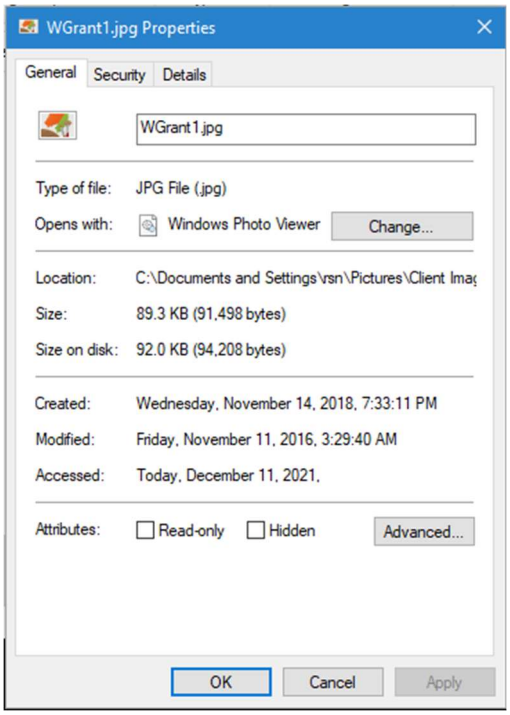
3:28 AM: *TWedge.jpg*





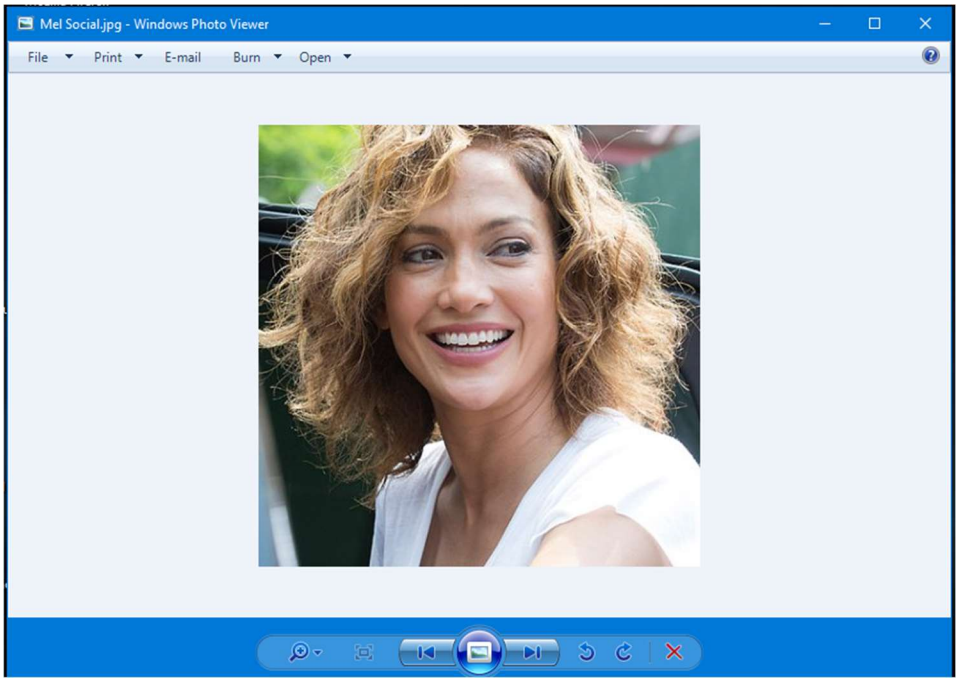
3:29 AM: *WGrant1.jpg*

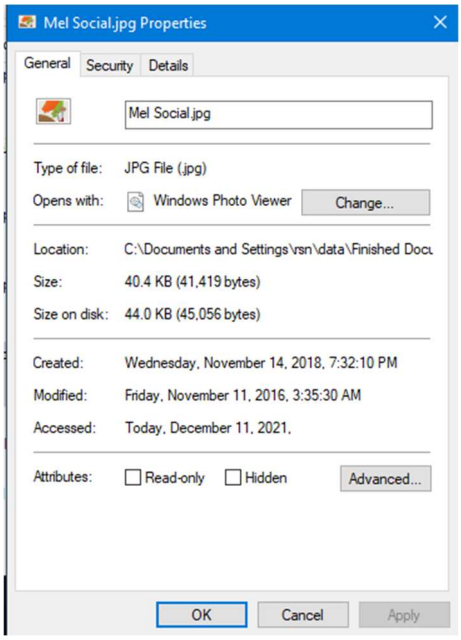




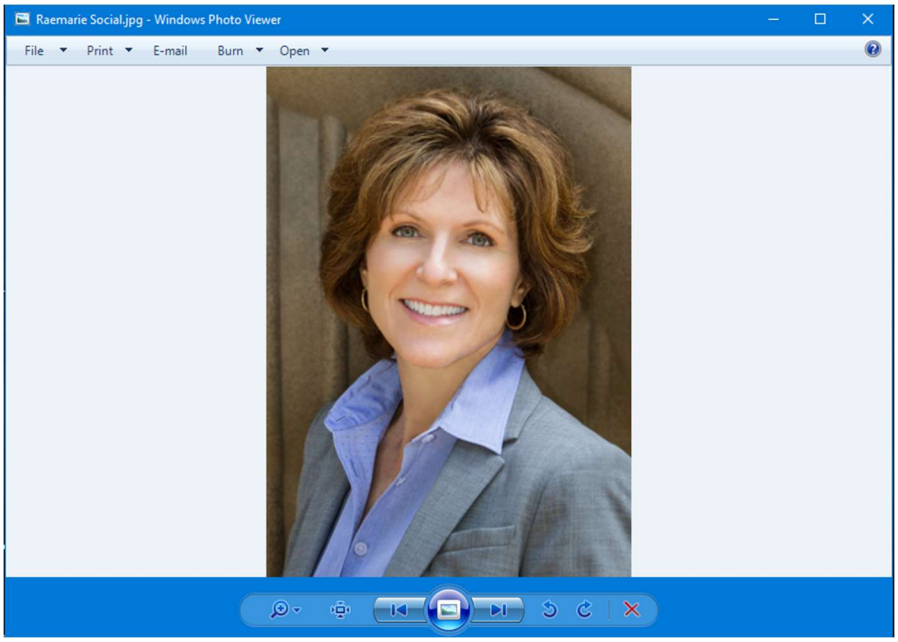
In directory *C:\Documents and Settings\rsn\data\Finished Documents*

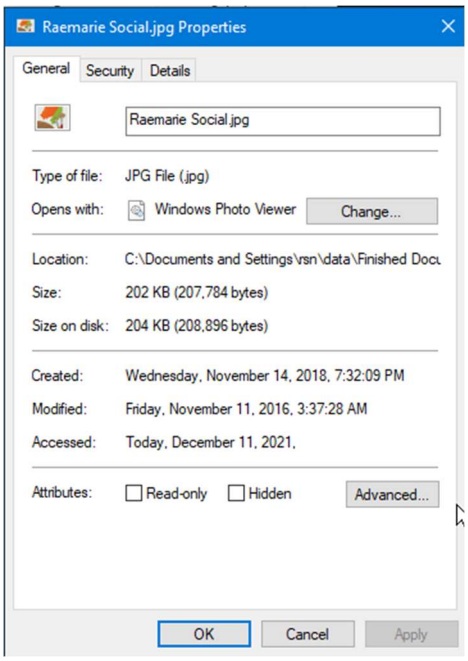
3:35 AM: *Mel Social.jpg*



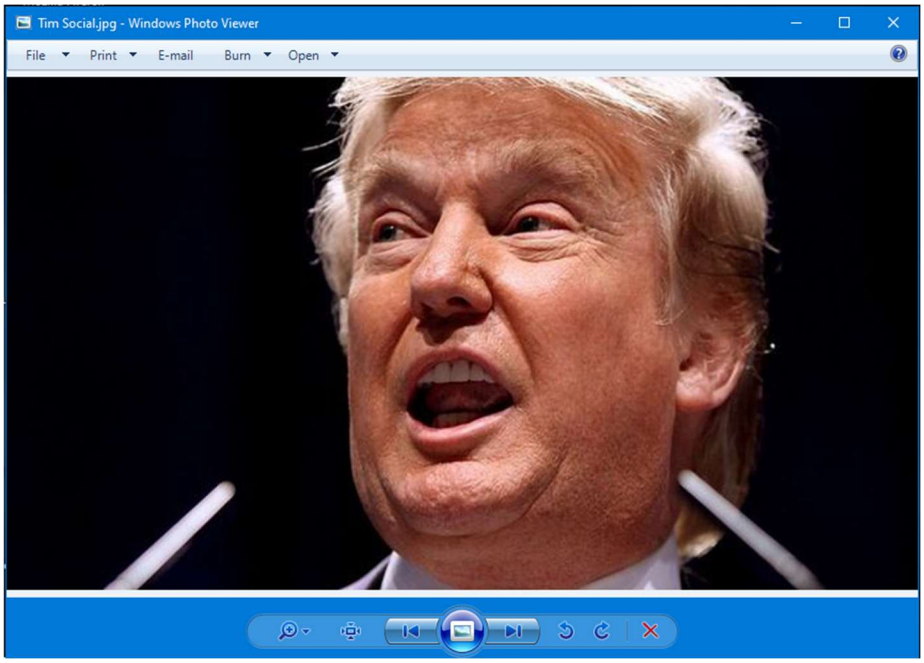


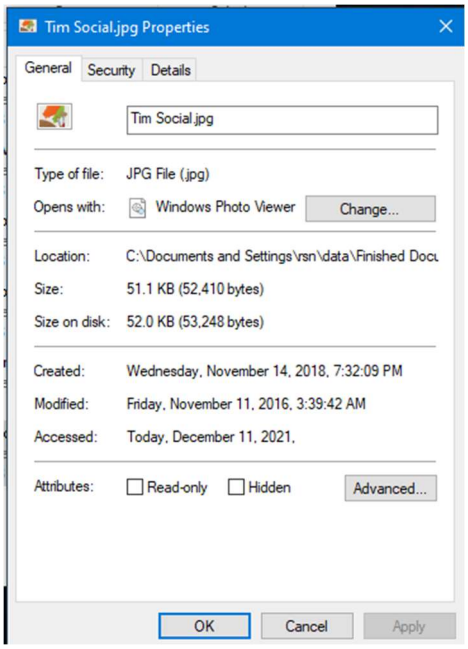
3:37 AM: *Raemarie Social.jpg*



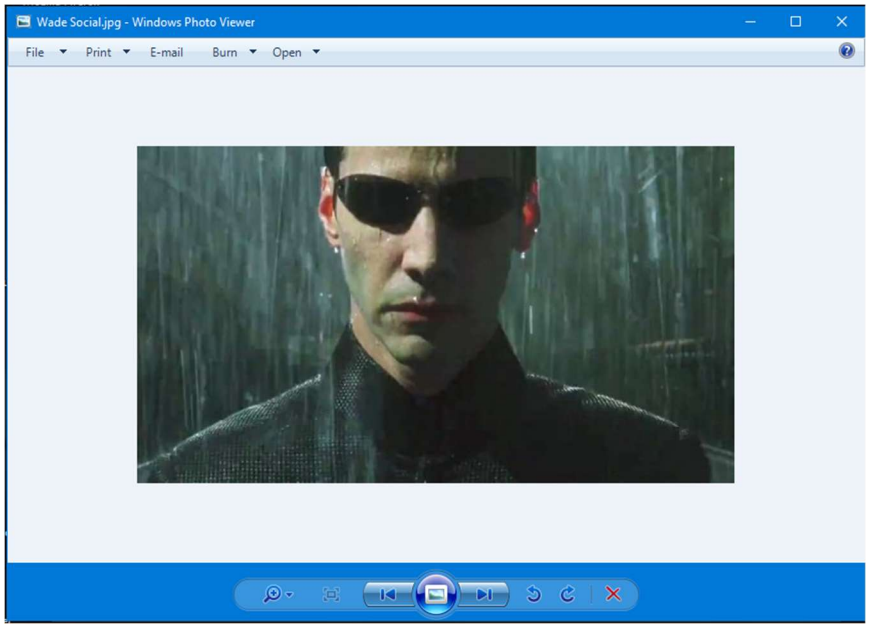


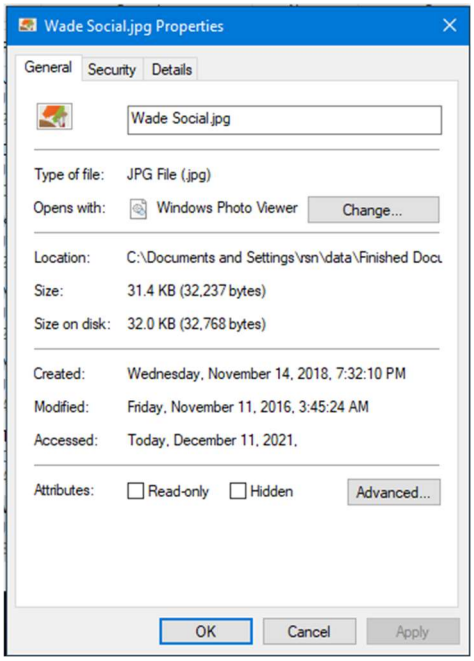
3:39 AM: *Tim Social.jpg*





3:45 AM: *Wade Social.jpg*





List of Documents

C:\Documents and Settings\rsn\Desktop\recycle

1) Jake.txt
2) Jimbo.txt

C:\Documents and Settings\rsn\My Documents

1) BBay.doc
2) Dumb money moves people make.doc
3) fmmom.doc
4) Letter to Joanie.doc
5) Loan.doc
6) Spas.doc
7) ToMom.doc
8) USAIRWAYS.doc

C:\Documents and Settings\rsn\My Documents\LOOT

1) BIRTHD~1.DOC
2) CONTACT.DOC
3) EMP.XLS

C:\Documents and Settings\rsn\data\data3\Orders and Records

1) complaint to hokey dokey.doc
2) Customer.xls
3) DESRONrequest.doc
4) IDs.doc
5) idsrus Warning Letter.doc
6) IDSRUS.HTM
7) Order.doc
8) responseto ids r us.doc

List of Images

C:\Documents and Settings\Public\Public Documents\Client Images

1) CGiglia1.jpg
2) DChatfieldFL.jpg
3) LJoiner.jpg
4) TWedg.jpg
5) WJones.jpg
6) WGrant.jpg

C:\Documents and Settings\rsn\Pictures\Client Images

1) DChatfield.jpg
2) MJoiner.jpg
3) RSchmidt.jpg
4) TWedge.jpg
5) WGrant1.jpg

C:\Documents and Settings\rsn\Pictures\Client Images\CGiglia

1) Slide1.jpg

C:\Documents and Settings\rsn\data\Finished Documents

1) Ben – WV.jpg
2) Ben.jpg
3) Bill – WV.jpg
4) Bryan – WV.jpg
5) Chris – WV.jpg
6) Chris.jpg
7) Joan – WV.jpg
8) Keith – WV.jpg
9) Keith.jpg
10) Mark – WV.jpg
11) Mark.jpg
12) Mel Social.jpg
13) Raemarie Social.jpg
14) Tim Social.jpg
15) Wade Social.jpg

C:\Documents and Settings\rsn\data\Finished Documents\Stuff for Mikey

1) Picture #2 of Glenda for fake drivers license.jpg
2) Pictures for Teri for fake drivers license.jpg

C:\Documents and Settings\rsn\data\data3\Orders and Records\IDsrus_files

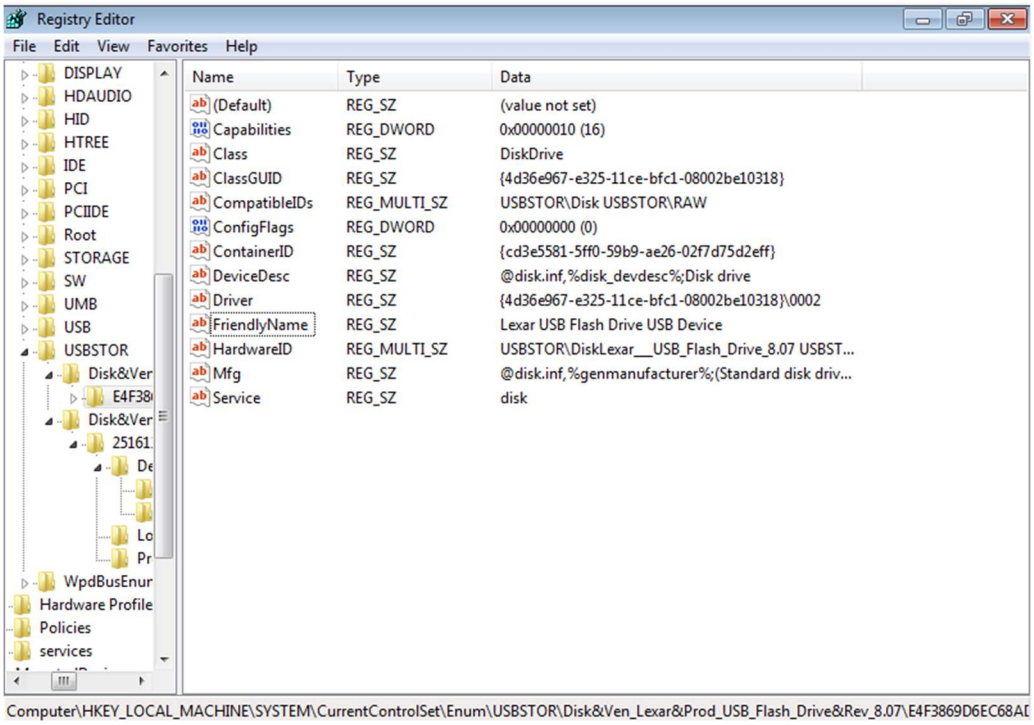
1) image003.png

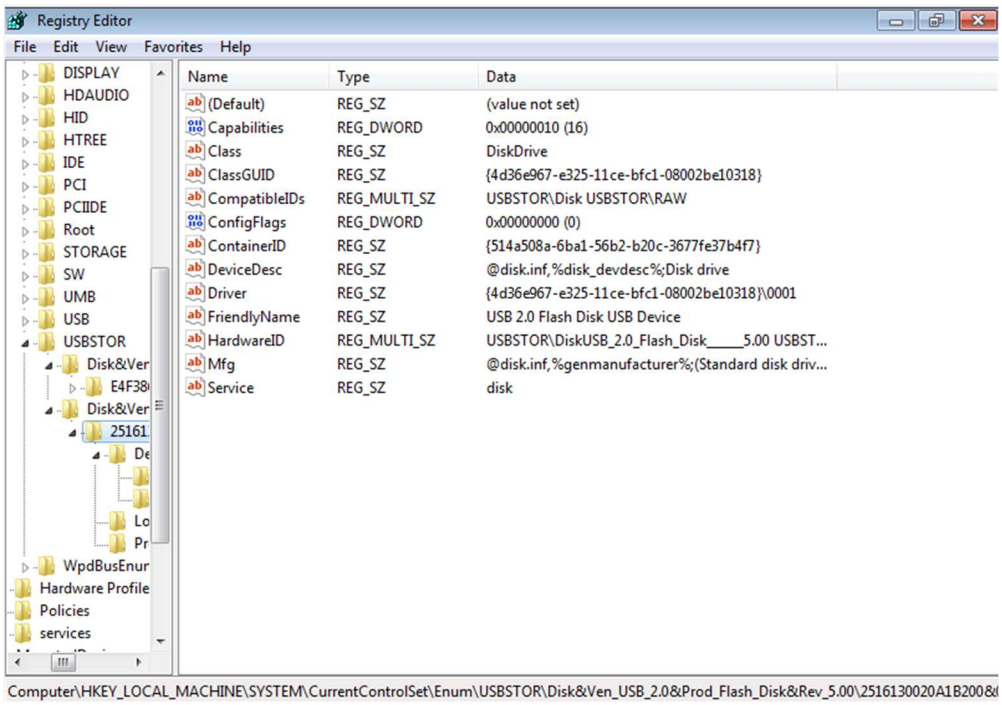
List of Tools

Tool Name	Tool Source
VirtualBox	https://www.virtualbox.org/wiki/Downloads
Hiren's BootCD PE	https://www.hirensbootcd.org/download/

Connected Flash Drives

The investigation found that there had been 2 flash drives connected to the machine. The first of these flash drives was a Lexar USB Flash Drive USB Device, as can be seen in the FriendlyName field of the first screenshot below. The second flash drive was a USB 2.0 Flash Disk USB Device, and its information can be seen the second screenshot below. This information was found by entering the Registry Editor and navigating to HKEY_LOCAL_MACHINE -> SYSTEM -> CurrentControlSet -> Enum -> USBSTOR. The screenshots with information about the 2 flash drives can be seen below.





NOTE: While most of the investigation was completed using Hiren's BootCD PE to access the file system, a different means of access was required to find the flash drives that were connected to the system. An exploit in the Window 7 crash recovery procedure allowed access to the Windows file system. This vulnerability was used to overwrite a file called "sethc" to instead call a new command prompt in place of its original function, which was related to sticky keys. Using this exploit, a new command prompt was brought up on the login menu by pressing shift 5 times, and this command prompt was used to change the password of the user "rsn" to log in to the machine without using Hiren's BootCD PE. With this new level of access gained, the flash drives appeared in the registry as expected.