

Final Report on Venetian Casino Case

[Student Names]

Robert Morris University

Table of Contents

>Cover Page...	Page 1
>Table of Contents...	Page 2
>Abstract...	Page 3
>Essay...	Pages 4-6
>>Systems/Technology Examined...	Page 4
>>>Methods for Examination...	Page 4
>>Specific Files Examined...	Page 4
>>>Evidence and Content Found in First Graphic File...	Page 5
>>>Evidence and Content Found in Second Graphic File...	Page 5
>>>Maintain Integrity of Evidence...	Page 6
>>Conclusion: Expert Opinion...	Page 6
>Glossary...	Page 7
>Appendixes...	Pages 8-10
>>Appendix A...	Page 8
>>Appendix B...	Page 9
>>Appendix C...	Page 10
>Evidence Form...	Page 11
>Chain of Custody...	Page 12

Abstract

Investigator [Student Name] acquired the evidence from the Venetian County, Las Vegas head of police; it was a 32 megabyte flash drive. After turning the evidence over to investigator [Student Name], as documented on the evidence custody form, she created a forensic image of the drive. After having acquired the image and recorded the hash values, the evidence was then returned to [Student Name] to be placed in an evidence locker. Following protocol, the evidence was properly secured in the locker with high security and limited access to Investigators [Student Names]. Using the acquired image, [Student Name] identified thirty-four different evidence groups. She analyzed the graphic files which showed hidden messages found in the slack space of the image files. The hash values for the image files were taken to assure that further tampering did not occur. The following essay explains the investigation in further detail.

Systems/Technologies Examined

Investigator [Student Name] received the evidence from John Doe, head police officer of Venetian County, Las Vegas, who found the flash drive in the bathroom of the Venetian Resort Hotel Casino on August 10th, 2014. The piece of evidence examined was a solid black USB-interface flash media drive. The drive is a SanDisk-produced “cruzer mini” and is additionally marked with a capacity of 32 megabytes. The drive is 70mm long, 7mm thick and 18mm wide.

Methods for Examination. [Student Name] then submitted the evidence to investigator [Student Name], under the supervision of Lead Investigators [Student Names], for examination on October 28th, 2014. [Student Name] used a forensic-grade software programs, AccessData’s Forensic Tool Kit (FTK), in order to perform a quality analysis of the contents of the drive. [Student Name] first ensured the integrity of the evidence by making sure that the evidence would not be modified during our investigation by producing a forensic image, or acquisition, of the drive using FTK. The final product of the acquisition produced a .S01 file and a .S01.txt information file; the file utilized lossless compression to store all of the drive’s data in such a way that while the way the data was conveyed changed, the content of the data was unchanged. Immediately after creating the forensic image, [Student Name] used the evidence custody form to record the hash values, or unique digital fingerprints, for both MD5 and SHA1. Once the hash values were recorded, [Student Name] returned the evidence drive to [Student Name], who safely stored the drive in the locked evidence room with high security protocols, which has not been accessed since.

Specific Files Examined

From this point, [Student Name] sorted through the forensic image using FTK by creating a case file. From the acquisition, the following types of files were found: four documents, six folders, six graphics, three operating system files, four known types, four slack/free space files, and seven

unknown types. Overall, there were thirty-four different evidence groups. The hash value for the flash drive under MD5 Sum was f61d68c9b569d2c82b955837c37820ed and under SHA 1 Sum was 3634d08d3c14c125bc76b7f2d8c5c023odf594.

Evidence and content found in first graphic file. She first eliminated the need to search through the three operating system files and the four known types since the hash values of the files were the same. [Student Name] was able to ignore these files because they matched the Known File Filter (KFF). In other words, the files were not altered in any way by the suspects, making it unnecessary to analyze. While examining the graphic files, [Student Name] found a hidden message in the slack space of 2.JPG using the hex interpreter in FTK. These messages were within the slack space of the image files, meaning that they did not affect the outward view of the image; as a result, the messages would only be visible in a hex interpreter. The message read as follows:

“Come tonight to the casino and bet all your money and I will let you win and double your money and then we meet tmrw to get my 50% of the money.” Refer to Appendix A. The hash values were as follows: MD5 was cd76ebed171a182dfde6e58375codb93 and SHA 1 was 710bd56d6a4edfb1de507629e6a8dc13af9a18ed. Refer to Appendix B. This file was created on October 7th, 2014 at 12:15:01pm.

Evidence and content found in second graphic file. The other image that had information in it was Hawaii-Pic.JPG. The message read as follows: “In the first two times Ill let you lose but in the third time Ill wink to you to remind you to hit on number 7 all your money and do it again on the fifth time on number 17.” Refer to Appendix C. The hash value for this graphic file under MD5 Sum was 045a3f199fe62b94e88950180ea4f806 and SHA 1 was 74e9b774b622a35bee5e822adbe7c49df8ceea4e. Refer to Appendix B. This file was created on

October 7th, 2014 at 12:19:56pm. All other files on the forensic image were extraneous to the case, which was determined by [Student Name].

Maintain integrity of evidence. In order to ensure that the evidence had not been altered by [Student Name] during the investigation process, [Student Name] performed a hash value test using MD5 and SHA 1 through FTK on the image. The digital hash values for both MD5 and SHA 1 were the exact same as the values produced by FTK when the drive was first acquisitioned. As a result, since the drive and forensic image were verified to carry the exact same information, the evidence found by [Student Name] through her thorough analysis of the acquisition reflects the evidence on the original drive.

Conclusion: Expert Opinion

In the expert opinion of Investigators [Student Names], the analysis of the acquisition showed signs no signs of modification and all results should be taken as if [Student Name] had analyzed the original device. In our collective opinions, 2.JPG shows that there was a correspondence using the slack space to communicate intent to preform fraud, namely through a second party's assistance. Hawaii-Pic.JPG shows that there were messages in the slack space intended to instruct the owner of the drive how and when to gamble in order to conduct this scam. It is further within our professional opinions that because of the existence of both modified and unmodified versions of the images stored within the drive, that it is unquestionable that the owner of the drive was aware of, and almost certainly a party of these correspondences. The information provided in this report is our in our best professional opinions, and all referenced evidence is complete and accurate as confirmed by the hash value methods, MD5 and SHA 1.

Glossary

Acquisition- an exact replica of the evidence

Chain of Custody-The route the evidence takes from the time the investigator obtains it until the case is closed or goes to court

Disk-to-Image- can make one or many copies of a suspect's drive; these copies are bit-for-bit replications of the original drive

Drive Slack-Unused space in a cluster between the end of an active file and at the end of the cluster. It can contain deleted files or file fragments. Drive slack is made up of both file slack and RAM slack

Evidence custody form- a printed form indicating who has signed out and been in physical possession of evidence

File Slack- the unused space created when a file is saved. If the allocated space is larger than the file, the remaining space is slack space and can contain passwords, file fragments etc.

Forensic Tool Kit- also known as FTK; forensic-grade software produced by AccessData and used for analyzing digital evidence

FTK Imager-a Windows data acquisition program; designed for viewing evidence disks and disk-to-image files created from other proprietary formats

Hash Value- A unique hexadecimal value which identifies a file or drive. It is like a digital fingerprint to compare evidence

JPEG- Joint Photographic Experts Group, standard bitmap file format-collections of dots, or pixels, in a grid format that form a graphic

Lossless Compression- compression method in which no data is lost

MD-5-validates hash values; read and compared to the image to verify; 128 bits or 32 hex digits

SHA-1-validates hash values; compares more hash values than the MD-5; 160 bits or 40 hex digits

Steganography- A cryptographic technique for embedding information in another file for the purpose of hiding that information from casual observers

Appendix A

[illegible]

Appendix B

stl35@mail.ru x INF53120 x VMware Blast x

3/r/44AB65D4-F8CA-45FB-90A3-383A712CF85C/?vauth=2%2BPmwuKise719%2FESxanLUOe

File Explorer - Invalhnet Case.cdfn

#	Ext	Path	Category	P-Size	L-Size	MD5	SHA1
	jpg	Acquisition (1).s01/Parti...	JPEG	742.5 KB	742.1 KB	045a3f199f662b94e88950180ea4f806	74e3b7746c22a38bee5a822a1b27c4df8fcee
	doc	Acquisition (1).s01/Parti...	Unknown	4096 B	4096 B	5ecad39c470178e1b0e4932e53460fda	36dfed64995c28cf63cc63da3d153da020a88
	jpg	Acquisition (1).s01/Parti...	Microso...	74.50 KB	74.50 KB	6bb26f439031db236c22f8a4f55a1418	a17580fbd17d1cef520db7dbf507ca901f5e38
	jpg	Acquisition (1).s01/Parti...	JPEG	17.50 KB	17.42 KB	95d927c1499dd9647cfad013886e86	f6b160e5f16fbc5efddcd3754124e09ef40c4
	jpg	Acquisition (1).s01/Parti...	JPEG	39.50 KB	39.28 KB	ad1664da0c67ee78238a6ee88f637e7	78bb8eb70def2a08d63ec8ade3526765c937
	jpg	Acquisition (1).s01/Parti...	JPEG E...	38.00 KB	37.76 KB	cd76ebcd171a182dfdece5375c0db93	710bd56dca4edfb1de507629e6a80c13a9a18
	jpg	Acquisition (1).s01/Parti...	JPEG	247.0 KB	246.5 KB	d5957069ba2d9011855cde4f5561b225e	fa9bf583ad51db31d9aa2f7b88de42f5fcd908
	jpg	Acquisition (1).s01/Parti...	JPEG E...	214.0 KB	213.6 KB	f29a47495b49721356824d82a31a47	83fa8eddf3e5475993bae1ddda756ca3ae3e
		Acquisition (1).s01/Parti...	Folder	0 B	0 B		
		Acquisition (1).s01/Parti...	Folder	512 B	512 B		
		Acquisition (1).s01/Parti...	Folder	512 B	512 B		

File Explorer - Invalhnet Case.cdfn

Properties

Highlighted: 1 | Checked: 0 | Total LSize: 1376 KB

Hex Interpreter

ot2/Hawaii-PC.jpg

Explore Tab Filter: [None]

Appendix C

[illegible]

Appendix D: Evidence Forms

Single Evidence Form		 Digital Forensics Lab
1 5 0 7 8 6 3 1 0 0 1	Case No.	Evidence No.
PLEASE COMPLETE FORM IN UPPERCASE		
Section B: Evidence Collection		
Date/Time Collected	08/10/14 04:45	Collected by [REDACTED]
Site Address 3355 Las Vegas Blvd S, Las Vegas, NV, 89109 The Venetian Resort Hotel Casino		
Section C: Evidence Details		
Date/Time Stored 08/10/14 04:40		
Storage Location		
Device Type USB Drive	Capacity 32 MB	
Manufacturer SanDisk	Model Cruzer Mini	
Serial No.		
MD5 Sum f61a68c9b569a2c8ab755837c37820ed		
SHA-1 Sum 3634d98d3c142c125b476b7f2d8105cd23bdf594		
Additional Information...		
Note any damage, marks and scratches		Digital Image Taken ☒ Yes ☐ No
Section D: Image Details		
Date/Time Imaged 08/10/14 04:28		Imaged by [REDACTED]
Storage Location		
Image Filename Acquisition.s01	Image Size (inc. unit)	
Additional Information...		
This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines: - Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence - This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence - Further remarks can be noted overleaf in Section E: Remarks - It is important that these forms are kept with the evidence at all times - Upon handover or disposal please complete Section F: Evidence Handover		

Appendix E: Chain of Custody

Chain of Custody Form		for use with a Single Evidence form
1 5 0 7 8 6 3 1 0 0 1	0 1	 Digital Forensics Lab
Case No.	Evidence No.	Page No.
This form must accompany a Single Evidence form and it's respective evidence		
Chain of Custody		
SUBMITTER	RECEIVER	
Name: [REDACTED]	Name: [REDACTED]	
Signature: [REDACTED]	Signature: [REDACTED]	
Date & Time: 10/28/2014 4:20 pm	Date & Time: 10-28/14 4:28	
Evidence Modified: Yes / ☒ No		
SUBMITTER	RECEIVER	
Name: [REDACTED]	Name: [REDACTED]	
Signature: [REDACTED]	Signature: [REDACTED]	
Date & Time: 10/28/2014 4:24:26	Date & Time: 10/28/2014 4:32 pm	
Evidence Modified: Yes / ☒ No		
SUBMITTER	RECEIVER	
Name:	Name:	
Signature:	Signature:	
Date & Time:	Date & Time:	
Evidence Modified: Yes / No		
SUBMITTER	RECEIVER	
Name:	Name:	
Signature:	Signature:	
Date & Time:	Date & Time:	
Evidence Modified: Yes / No		
SUBMITTER	RECEIVER	
Name:	Name:	
Signature:	Signature:	
Date & Time:	Date & Time:	
Evidence Modified: Yes / No		
SUBMITTER	RECEIVER	
Name:	Name:	
Signature:	Signature:	
Date & Time:	Date & Time:	
Evidence Modified: Yes / No		
SUBMITTER	RECEIVER	
Name:	Name:	
Signature:	Signature:	
Date & Time:	Date & Time:	
Evidence Modified: Yes / No		
If this form is full please continue on another page		