

Introduction

N

Carson High School's AP Computer Science Principles students will become more familiar with the binary, decimal and hexadecimal number systems by learning digital forensic file carving. Students will be given the opportunities to access Cyber Security protocols and concepts which will allow them to have hands-on discovery and problem solving activities.

Exploration of File Carving

Essential Questions for Lesson What does the term "File Carving" mean? File carving is a process in computer forensics to extract data from a disk drive or other storage device without the assistance of the file system that originality created the file. (https://resources.infosecinstitute.com/file-carving) What is it used for? File carving has provided law enforcement and cyber security professionals another tool they can use to recover damaged or deleted files. What is a forensic disk image? Its a bit-by-bit, sector-by-sector direct copy of a storage device, including all files, folders, and unallocated/free space. File Signatures File signature is a sequence of bytes that is used by application programs to confirm file data before loading and processing the rest of the file. File Carving Software/Tools HxD (free) - FTK Imager (free) - ExifTool (free)

File Carving Demonstration

Hands-on Teacher Lead Demo

- Students will examine image files and practice manual file carving using HxD software and Tools.
- Students will be given a variety of images, ie. PNG, JPG and GIF to discovery how each file is different from each other.

RET Site: Research Experience in Cybersecurity for Nevada Teachers (RECNT) RECNT: Digital Forensics Into the Computer Science Classroom

Sherri Kelley, Carson High School

Nancy Latourrette, Bryson Lingenfelter and Mustafa Solmaz University of Nevada, Reno Dr. Shamik Sengupta and Dr. David Feil-Seifer University of Nevada, Reno

	ľ	Ń			9	e		7	J.		
₩ HxD - [C:\Users\admin\D	esktop\	diamon 16	d.png]	Vindows	(ANSI)		hex				
File Edit Search View	Analys	is Tool	s Wind	ow Hel	lp		11.00				
📓 diamond.png			P	NG S	ignat	ure			H	IDR L	ENG
Offset(h)	00	01	02	03	04	05	06	07	80	09	0A
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00
00000010	00	00	00	E1	00	00	00	F5	08	06	00
00000020	F7	00	00	00	04	67	41	4D	41	00	00
00000030	93	00	00	00	20	63	48	52	4D	00	00
00000040	12	4 b	ytes	01	54	4 by	ytes CHT	82	2B	00	00
00000050	AF			3A	EB			14	97	08	1C
00000060	19	69	43	43	50	49	43	43	20	50	72
00000070	00	00	58	C3	AD	97	77	54	53	C9	1E
00004BB0	A8	24	AC	A8	58	30	2A	09	2B	2A	16
00004BC0	85	62	34	FA	F.F.	D6	5E	DC	ID	מט	BE
00004BD0	00	49	45	4也	44	AL	42	60	82		
				P	NGT	railer					
				•		runer					

HxD - IC:\Users\admin\Desktop\ipgtest.ipg

🗋 🚵 🕶 📊 📕 😅 📄 🕶 16 🛛 🗸 Windows (ANSI) 🖓 hex

80	File Edit Search View Analysis lools Window Help											
FD	diamond.png 📓 jpgt	JPG Hex Signature (header)										
	Offset(h)	00	01	02	03	04	05	06	07	08	09	0A
	00000000	FF	D8	FF	ΕO	00	10	4A	46	49	46	00
	00000010	00	01	00	00	FF	FE	00	3C	43	52	45
	000000000	01	01	01	01	01	01	01	01	01	01	01
	000000D0	01	01	01	01	01	01	01	01	01	01	01
	000000E0	08	01	68	01	68	03	01	22	00	02	11
	000000F0	C4	00	1F	00	00	01	05	01	01	01	01
				r	1	r						
	00008DA0	56	4 by	ytes)	14b	ytes	20	7D	4F	FE	C1	B7
	00008DB0	50	WIE	TH	I HE	GHT	14	00	51	45	14	01

🕸 HxD - [C:\Users\admin\Desktop\robot.git

🗋 🚵 🖛 📊 📲 🤩 📄 🔻 \cdots 16 🛛 🗸 🖬 Windows (ANSI) 🔗 🗸 hex

aots.png 🔤 robot.gn											
Offset(h)	00	01	02	03	04	05	06	07	80	09	0A
00000000	47	49	46	38	39	61	C8	00	C8	00	F1
00000010	30	20	20	80	FF	FF	80	80	80	21	FE
00000020	21	FF	0B	4E	45	54	53	43	41	-50	45
00000030	00	00	00	21	FE	C1	4 bytes ¹		4 bytes)		3A
00000040	2E	72	74	6C	73	6F	WIDTH ₁		HEIGHT		6F
00000050	6D	61	67	69	63	0A	0A	43	72	65	61
00003630	D8	F5	AE	23	CD	EΒ	26	F6	1A	C8	AF
00003640	66	5D	E3	5A	58	ΒE	0E	16	B1	25	15
00003650	C7	E6	F4	9D	05	00	00	3B			

GIF Trailer



Students Apply their new knowledge to a hands-on application Students will be given a USB drive with damaged or deleted images and written activities instructions.

- procedures:

 - **Use File Carving Software and Tools** \checkmark
 - The recovered results will determine which
 - damaged/deleted information is available for analysis.
 - Use correct terminology when writing the final analysis. \checkmark



File Carving Activities

Students will demonstrate mastery of the following

✓ Create a forensic disk image.

Evaluation

Pre-Assessment: Students will complete a KWL chart. The KWL chart will be used to engage students in a new topic, and activate prior knowledge. All activities will be assessed using formative and summative assessments.

Post-Assessment: Students will complete their KWL chart. Students will be given an end of unit exam based on the skills learned and trends in the real world. Students will complete an end of unit self-reflection survey.

Resources

Code.org (https://code.org)

Hex Editor (https://mh-nexus.de/en/hxd)

Practice Images Files

File Carving Resources

"This research is supported by NSF Award #1855159: RET Site: Research Experiences in Cybersecurity for Nevada Teachers (RECNT)."