原创 队员编号012 酒仙桥六号部队 6月11日

这是酒仙桥六号部队的第16篇文章。

全文共计1871个字,预计阅读时长5分钟。



当我们需要对计算机进行磁盘取证时往往会发现,该台电脑之前的操作人员已经将敏感文件删 除进入回收站,并清空回收站或从回收站中彻底删除了这些文件,而这些文件很可能包含了重 要的取证信息。



从原理上,删除只是在文件上作了删除标记,而真正的文件内容仍保存在磁盘的数据区中,并 未得以删除。要等到以后的数据写入,把此数据区覆盖掉,这样才算是彻底把原来的数据删 除。因此只要将整个磁盘进行分析,就有可能将已经彻底删除的文件恢复。



目标系统: Win7SP1x86

1、首先我们在 D 盘创建几个小图片、小视频、小文档:



text_d.txt、document_d.docx。

2、右键删除

image_d.jpg、video_d.mov、text_d.txt、document_d.docx,

之后"清空回收站"。

er ► Local Disk (D:)	▼ ⁴ 7	Search Local Disk (D:)		٩
n library 🔻 Share with 👻 New folder			· • 🗊	•
Name	Date modified	Туре	Size	
🖹 document.docx	3/19/2020 1:29 AM	Office Open XML	12 KB	
🔛 image.jpg	3/19/2020 1:31 AM	JPEG image	6 KB	
i text.txt	3/19/2020 1:33 AM	Text Document	1 KB	
🔊 video.mov	3/19/2020 1:27 AM	QuickTime Movie	301 KB	



在进行磁盘取证时,为了尽量减少目标主机文件系统的变动,我们可以使用离线方式进行磁盘 取证,将目标主机的磁盘创建镜像,放在移动磁盘中存储。

3.1 在 Kali 下创建磁盘镜像

3.3.1 启动到Live模式下

1、首先启动进入取证模式;



2、接入移动硬盘, fdisk -I 确定移动硬盘的设备名为/dev/sdb1;

Disk /dev/sdb: 238.5 GiB, 256060514304 bytes, 500118192 sectors Disk model: ASM1153E Units: sectors of 1 * 512 = 512 bytes Sector size (logical/physical): 512 bytes / 4096 bytes I/O size (minimum/optimal): 4096 bytes / 33553920 bytes Disklabel type: gpt Disk identifier: 7DC1FEFE_681C-4EF0-83C2-E07C7DBDEA66 Sector size Device Start End age Sectors Size Type /dev/sdb1 4096 500117503 500113408 238.56 Microsoft basic dat

3、挂载移动硬盘。

cd /mnt

mkdir udisk

mount /dev/sdb1 /mnt/udisk



3.1.2 使用Guymager

Applications 🕶	Places 🔻	Thu 08	3:14	1) 2	🖌 =0) 🗈 -
		Q guy	Ø			
		Guymager	guymager			

1、在目标硬盘上右键 Acquire image,

设置相关信息、保存路径、文件名,开始获取磁盘镜像。

下面的hash校验我勾掉了,是为了让速度更快一些。

202

20/7/27		1	清空回收动	站'后依然在磁盘中被抓到证据!	原因竟然是.					
			Acquir	e image of /dev/sda				0	•	8
Devices	File format							^		
Rescan	O Linux dd raw ir	nage (file extensio	on .dd or	.xxx)	☑ Split in	mage files				
s	• Expert Witness	Format, sub-form	nat Guyn	nager (file extension .Exx)	Split size	2047	MiB 👻			
2042201	Case number	10086								
2G43201	Evidence number	10010							SR I	HPA:
00000000	Examiner								5B	
	Description								sв	
_	Notes	win7sp1 x86							в	
	Destination									
	Image directory		/mnt/u	disk/Forensic/						
	Image filename (w	vithout extension)	win7					וו		
	Info filename (with	nout extension)	win7							
•	Hash calculation / ve	erification								•
Size Sector si	✓ Calculate MD5		Calc	ulate SHA-1	Calcu	late SHA-2	56			
Info file	Re-read source	after acquisition	for verifi	cation (takes twice as long)						
Started Hash cal	Verify image af	fter acquisition (ta	kes twic	e as long)						
Source v Image ve	Cancel			Duplicate image		Start				

2、Start开始后,需要一段时间,由磁盘容量、速度与电脑性能决定。

Devices Misc Help		GUYMAGER 0.8.8		0 0	
Rescan					
Serial nr.	Linux device	Model	State	Size	
2G4320132832	/dev/sdb	ADATA_SU800	⊖ Idle	256.1GB	HPA
000000000000000000000000000000000000000	001 /dev/sr0	VMware_Virtual_SATA_CDRW_Drive	🔿 Idle	3.5GB	
	/dev/sda	VMware_Virtual_S	Running	42.9GB	
	/dev/loop0	filesystem.squashfs	🔿 Idle	3.2GB	
4					•
Size 4 Sector size 5 Image file /r Info file /r Current speed 2 Started 1 Hash calculation M Source verification of Image verification of	2,949,672,960 by 12 mnt/udisk/Forensi mnt/udisk/Forensi 9.92 MB/s 9. March 08:46:3: ID5 ff	rtes (40.0GiB / 42.9GB) c/win7.Exx c/win7.info 3 (00:00:03)			

3、镜像制作完成。

Serial nr.	Linux device	Model	State	Size	
2G4320132832	/dev/sdb	ADATA_SU800	🔾 Idle	256.1GB	HPA:
000000000000000000000000000000000000000	/dev/sr0	VMware_Virtual_SATA_CDRW_Drive	🔿 Idle	3.5GB	_
	/dev/sda	VMware_Virtual_S	Finished	42.9GB	
	/dev/loop0	filesystem.squashfs	◯ Idle	3.2GB	



全磁盘镜像文件大小共4.7GB。

win7.xmet	1 KB	XMET 文件
win7.info	6 KB	INFO 文件
win7.E03	727,646 KB	E03 文件
win7.E02	2,096,127	E02 文件
win7.E01	2,096,111	E01 文件

👃 guym 属性	
常规 以前	前的版本自定义
	guym
类型:	文件夹
位置:	Z:\Shared\Forensic
大小:	4.69 GB (5,037,966,140 字节)
占用空间:	4.69 GB (5,037,977,600 字节)
包含:	5 个文件,0 个文件夹

磁盘实际使用大小是这样的。

Desktop	Local D	isk (C:)	Local	Disk (D:)		1
Local Disk (C:) Pro	operties	free of 34.0 GB	Local Disk (D:) Pro	perties		Σ
Security	Previous Versions	Quota	ReadyBoost P	revious Versions	Quota	Customize
General	Tools Hardware	Sharing	General Tools	Hardware	Sharing	Security
			9			
Type: Loc File system: NTF	al Disk FS		Type: Local File system: NTFS	Disk		
Used space:	11,315,171,328 bytes	10.5 GB	Used space:	60,870,656	bytes 58	.0 MB
Free space:	25,279,078,400 bytes	23.5 GB	Free space:	6,186,541,056	bytes 5.	76 GB
Capacity:	36,594,249,728 bytes	34.0 GB	Capacity:	6,247,411,712	bytes 5.	81 GB
	Drive C:	Disk Cleanup		Drive D:	D	isk Cleanup

3.1.3 使用dd

1、fdisk -l 判断目标磁盘编号:

#if=指定需要制作映像设备, -of=指定保存的位置。

2、dd if=/dev/sda

of=/mnt/udisk/Forensic/dd/sda

root@kali:/mnt/udisk/Forensic/dd# dd if=/dev/sda of=/mnt/udisk/Forensic/dd/sda ^C2831068+0 records in 2831068+0 records out 1449506816 bytes (1:4 GB, 1.3 GiB) copied, 508.674 s, 2.8 MB/s root@kali:/mnt/udisk/Forensic/dd# dd if=/dev/sda3 of=/mnt/udisk/Forensic/dd/sda3 ^C1339327+0 records in

1339327+0 records in 1339327+0 records out 685735424 bytes (686 MB, 654 MiB) copied, 231.578 s, 3.0 MB/s

dd 速 度 非 常 慢 , 且 在 备 份 过 程 中 没 有 任 何 进 度 提 示 , 直 接 放 弃 换 用 增 强 版 dd - - - - - - dc 3 dd 。

3.1.4 使用dc3dd

dc3dd和dd参数使用是一样的,它们一样是完整备份,对备份盘容量需求比较大,这里只备 份sda3(D盘),可以看到备份了约6GB大小。

root@kali:/mnt/udisk/Forensic/dd# dc3dd if=/dev/sda3 of=/mnt/udisk/Forensic/dd/sda3
dc3dd 7.2.646 started at 2020-03-19 09:31:24 +0000
compiled options:
command line: dc3dd if=/dev/sda3 of=/mnt/udisk/Forensic/dd/sda3
device size: 12201984 sectors (probed), 6,247,415,808 bytes
sector size: 512 bytes (probed)
130580480 bytes (125 M) copied (2%), 4 s, 34 M/s

最终D盘分区镜像大小5.81GB。



3.2 在 Windows 下创建磁盘镜像

在Windows下也最好使用Live系统如WindowsPE启动盘进行取证,但是由于这里没有现成 的包含取证工具的启动盘,因此直接在系统里操作。取证工具、创建的磁盘镜像文件,都放在 虚拟机的共享磁盘上,尽可能避免改变目标文件系统。

3.2.1 使用X-Ways Forensics

这个工具就是Winhex的取证加强版,因此界面几乎都一样。

1、工具栏选择Create Disk Image。

<u>З</u> Х-	Ways	Forensics								
File	Edit	Search	Navigation	View	Tools	Specialist	Options	Window	Help	
Case	Data					🗅 🚺	2	f 👔 🗍	5	B (
File	E <u>d</u> it						Create	e Disk Image	2	

2、直接给整个磁盘创建镜像,创建分区镜像可以选择上边的。

ect Disk			×
E Salaria Logical Volu	umes/Partitions		- 1
	1 GB), HD0		
(D:, 5,8	GB), HD0		
🗄 🄜 Logical Volu	umes/Partitions without driv	ve letters	
Physical Sto	orage Devices		
I 🥪 HD0: VN	/Iware, VMware Virtual S (40),0 GB, SAS)	
list volumes that do	not have drive latter		
List volumes that do	not have drive letters		

3、选择好存储路径后点OK开始。

nage file format:	Scope: sectors 0 - 83886079
Raw image (.dd, .001, interpretable and splittable)	Converting medium
Evidence file (.e01, interpretable and compressible)	Copy entire medium
Evidence File Container	
Disk Bytes per sector: 512	Add to [active case], Refine Volume Snapshot
ath and filename: (29.7 GP free)	Connected backs MD5
I Folders/Shared/Forensic/yways/Win 7x8	Compute hash: MD5
Dverflow dir.	Compute hash(es) in a separate thread
2nd copy	
Wait for imaging in other instances to complete, if any	
Create descriptive text file	Compression: fast adaptive
xaminer(s):	+2 thread(e)
nternal description:	Church eize:
Win 7x86	Chunk size. 32 KB V
	Spir mage into segments or 0132 MB
	Encryption

4、开始创建镜像,镜像备份的速度比dd真是快的太多了。

<	Transferring sectors No. 4 615 168					
Se Disk			1	93	Sync 🔷 🤆	¢≡_
Offse	5%	12	13	14 -	Hard disk 0	
0000000	approx. 7 min. left	00	7C	BF	Model:	VMware, VMware Virtua
0000000	Shut down system after completion	FB	B9	04	Firmware Rev.:	1
0000000	Compression: fast, adaptive	01	83	C5	Bus:	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~
Compression	6.1 GB/min, read: 2.2 GB / 40.0 GB, written: 1.5 GB / 27.5 GB				Part of the	8
111						1
						•

全盘备份5.8GB,要比guymager备份的文件容量多1GB,这个结果可能是受到了在线备份镜像的影响。

2020/7/27	'清空	回收站'后依然在磁盘中被抓到证据!」	原因竟然是	
名称			大小	类型
Win7x86.e0	1		6,099,977	E01 文件
Win7x86			2 KB	文本文档
🗼 xways 属性	ŧ			x
常规以前	前的版本 自治	定义		
	xways			
类型:	文件夹			
位置:	Z:\Shared	Forensic		
大小:	5.81 GB (6,246,377,338 字章	节)	
占用空间:	5.81 GB (6,246,383,616 字章	节)	
包含:	2 个文件,	0 个文件夹		

3.2.2 使用AccessData FTK Imager

由于我找到的这个版本不支持32位系统,因此只能使用它在另外一台x64虚拟机做一个创建 镜像的演示。(D盘环境存在相同的文件读写删除操作)

AccessData FTK Imager 4.2.1.4				
<u>File View Mode H</u> elp				
🗛 🤮 🗞 🚖 🔂 🖯 🗛 🗛 🖛 🖛		≫ mi mi ? .		
Evidence Tree	File List			×
	Name	Size Type	Date Modified	
Contract Constant Constants				
Custom Content Sources				
Evidence:Pile System(Path)Pile Options				Â
·	•			
New Edit Remove Remove All Create Image				
Properties Hex Value Int Custom Conte.				-
For User Guide, press F1				

1、同样在工具栏选择Create Disk Image。

💽 Ac	cessDat	a FTK Im	ager 4.2	.1.4			
<u>F</u> ile	View	<u>M</u> ode	<u>H</u> elp				
	😭 🗣	a a		6	p 6	1 =	Ē
Evide	nce Tre	e				-	Fil
			Create	Disk	c Imag	je	N

2、选择整个磁盘或分区,这里准备备份一个分区D盘。



elect	Source Drive Selection
	Please select from the following
	D:\- [NTFS]
	🗌 Automate multiple removable media
	<上一步(B) Finish Cancel Help

3、选择备份类型,这里不建议用Raw,那样就跟dd一样创建一个和磁盘大小一样的镜像,无 视实际使用空间大小。

mage Source D:\			
D:\			
mage Destination(s)			
mage Destination(s)	Starting Evidence Number:	1	
mage Destination(s)			
Add	Edit	Remove	
		Incinove	
	Add Overflow Location		-
ct Image Type			×
Please Select the I	estination Image Type		
🔘 Raw (dd)			
SMART			
E01			
O AFF			
0			

4、按需填写证据信息。

Case Number:	10010
Evidence Number:	10011
Unique	
Examiner:	
Notes:	Win7x64Test
(c.)	
< F	

5、选择存储位置,之后开始创建镜像。

mage Destination Folder	1000	2.5
C:\Users\Lab\Desktop\Win7x64D	Brow	se
mage Filename (Excluding Extension)		
/in7x64D		
Image Fragment Size (MB) For Raw, EO1, and AFF formats: O = do not Compression (O=None, 1=Fastest, …, 9=Smallest)	1500 6	
Use AD Encryption	n 🕅	

mage Source:	D:\	
estination:	C:\Users\Lab\D	esktop\Win7x64D\Win7x64D
tatus:	Image created	successfully
Progress		
Progress	psed time:	0:00:42

D盘镜像大小21.6MB(如果使用RAW格式,将会是10GB)。

名称	^	大小	类型
Win7x64D.E	01	22,118 KB	E01 文件
Win7x64D.E	01	1 KB	文本文档
▶ Win7x64D 常规 以前	属性 前版本 自定义		×
	Win7x64D		
类型:	文件夹		
位置:	Z:\Shared\Forensic\FTK		
大小:	21.5 MB (22,649,682 字节)		
占用空间:	21.6 MB (22,654,976 字节)		



4.1 使用 X-Ways Forensics 分析证据

相较于FTK,X-Ways拥有更完善的案件、证据管理模式,可以保存案件后续再接着分析。 1、创建案件。



2、导入证据。

可以导入各类证据,这里选择镜像。

File	Edit	Search	Navigation	View	Tools
Case	Data				
File	E <u>d</u> it				
23	Creat	e New Ca	ase		
a	Open	Case			
and a	Close	Case			
	Close	(don't sa	ave)		
-1	Save	Case			
	Save	As			
	Archi	ve Case			
	Creat	e Report			
	Open	Report			
-	Add I	Medium			
	Add [Directory.			
	Add I	File			
	Add I	Memory	Dump		
	Add I	mage			

3、导入前面创建的4个镜像(包含两个全磁盘镜像、1个x86虚拟机的D盘、1个x64虚拟机的

D盘)。

🔒 X-Ways Forensics - (Guymager)			-		
Serie Edit Search Navigation Vie	w Tools Specialist Options W	indow Help			19.9 SR-4 x64 _ 8 ×
Case Data	🗋 D 🕼 🗆 😂 🕷 🖬 👔 👘		D 🗛 🗛 🙇 😂 :	S → +0 (+ → 2	2 2 2 II 2 1 1 2 II 2 II 2 II 2 II 2 II
File Edit	Guymager dd LY-Wave LET	K-W6n7v64			
A TheCase	Partitioning styles MRR	C-THEF AD-			0+0+2 flar 2 partitions
Case Root	Name		T Description	Type T S	ize Created Modified
B-Se Guymaner	Start sectors		virtual (for examination	purpo 1.0	MB
B-R Partition 1	Partition 1		partition, existing	NTFS 100	MB
D. R. Partition 2	Partition 2		partition, existing	NTFS 34,1	GB
C. R. Partition 3	Partition 3		partition, existing	NTFS 5,8	GB
	Unpartitionable space		virtual (for examination	2,0	MB
(10)					
CONCILE DIN (0)					
Surteen Volume Information (1)					
	<				•
and A ways	🗢 Disk 📄 File 📓 Pr	eview 💭 Details	🕄 Gallery 🗮 Legend	i 📜 Sync	📉 🐴 🔤 💠 🖬 file (1,0 MB)
Partition 1	Offset 0 1 2	3 4 5	6 7 8 9 10	11 12 13 14 15	[Z:\Shared\Forensic\guvm\win7.E01]
Partition 2	00000000000 33 CO 8E	D0 BC 00 7	C SE CO SE DS	BE 00 7C BF 00	(Pead only mode)
B Partition 3 (42)	0000000016 06 B9 00	02 FC F3 A	4 50 68 1C 06	CB FB B9 04 00	[Nead-only mode]
E-55 FTK-Win/x04 (41)	00000000032 BD BE 07	80 7E 00 0	0 7C 0B 0F 85	0E 01 83 C5 10	Total capacity: 40,0 GB
E-Sextend (10)	0000000048 E2 F1 CE	18 88 56 0	0 55 C6 46 11	05 C6 46 10 00	42749772760 bytes
⊕- \$RECYCLE.BIN (9)	0000000064 B4 41 BE	AA 55 CD 1	3 5D 72 OF 81	FB 55 AA 75 09	Bytes per sector: 512
	00000000080 F7 C1 01	00 74 03 F	E 46 10 66 60	80 7E 10 00 74	Surplus sectors at end: 4096
	0000000096 26 66 68	00 00 00 0	0 66 FF 76 08	68 00 00 68 00	Partition: <1
	00000000112 7C 68 01	00 68 10 0	0 B4 42 8A 56	5 00 8B F4 CD 13	Relative sector No.: n/a
	00000000128 9F 83 C4	10 9E EB 1	4 B8 01 02 BB	00 7C 8A 56 00	
	00000000144 8A 76 01	8A 4E 02 8	A 6E 03 CD 13	66 61 73 1C FE	Mode: hexadecimal
	00000000160 4E 11 75	OC 80 7E 0	0 80 OF 84 8A	00 B2 80 EB 84	Offsets: decimal
	00000000176 55 32 E4	8A 56 00 C	D 13 5D EB 9E	2 81 3E FE 7D 55	bytes per page: 1/x10=2/2
	00000000192 AA 75 6E	FF 76 00 E	8 8D 00 75 17	FA B0 D1 E6 64	Window #: 1
	00000000208 £8 83 00	BO DF E6 6	0 E8 7C 00 B0	FF E6 64 E8 75	No. of windows: 4
	00000000224 00 FB B8	00 BB CD 1	A 66 23 C0 75	3B 66 81 FB 54	Case association: Tes
	0000000240 43 50 41	75 32 81 F	9 02 01 72 20	66 68 07 BB 00	Clipboard: available
				•	TEMD folders 37.4 GB free
	Sector 0 of 83?86?80	Offset:	0	= 51 Block:	n/a Size: n/a

4、查看D盘里的文件。

可以正常显示图片,但是这里没有看到被删除的文件(被删除的文件显示为半透明)。

Guymager dd X-Ways FTK-Win7x64	Guymager, P3						
\						14+0+3	=17 file
□ ▼Name▲	T Description	Type	Y Size	Created		Modified	ł
SExtend (10)	existing		21,1 MB	12.03.2020	02:49:19	+ 12.03.2020	02:49:
SRECYCLE.BIN (9)	existing		321 KB	11.03.2020	11:53:04	+ 11.03.2020	11:53:
🗆 잂 (Root directory)	existing		5,8 GB	12.03.2020	02:49:19	+ 19.03.2020	23:33:
System Volume Information (1)	existing		20,0 KB	11.03.2020	11:53:03	+ 11.03.2020	11:53:
SAttrDef	existing		2,5 KB	12.03.2020	02:49:19	+ 12.03.2020	02:49:
SBadClus (1)	existing, already viewed		0 B	12.03.2020	02:49:19	+ 12.03.2020	02:49:
🗆 📄 \$Bitmap	existing		186 KB	12.03.2020	02:49:19	+ 12.03.2020	02:49:
🗆 📄 \$Boot	existing		8,0 KB	12.03.2020	02:49:19	+ 12.03.2020	02:49:
🗆 📄 \$LogFile	existing		31,8 MB	12.03.2020	02:49:19	+ 12.03.2020	02:49:
□	existing		256 KB	12.03.2020	02:49:19	+ 12.03.2020	02:49:
SMFTMirr	existing		4,0 KB	12.03.2020	02:49:19	+ 12.03.2020	02:49:
Secure (3)	existing, already viewed		0 B	12.03.2020	02:49:19	+ 12.03.2020	02:49:
🗆 📄 \$UpCase	existing		128 KB	12.03.2020	02:49:19	+ 12.03.2020	02:49:
💷 📄 \$Volume	existing, already viewed		0 B	12.03.2020	02:49:19	+ 12.03.2020	02:49:
document.docx	existing	docx	11,5 KB	19.03.2020	23:32:36	+ 19.03.2020	16:29>
🗉 💼 image.jpg	existing, already viewed	jpg	5,7 KB	19.03.2020	23:32:36	+ 19.03.2020	16:31:
text.txt	existing	txt	8 B	19.03.2020	23:32:36	+ 19.03.2020	16:33:
🗆 📑 video.mov	existing	mov	300 KB	19.03.2020	23:32:36	+ 19.03.2020	16:27:
Free space (net)	virtual (for examination purpo		5,8 GB				
Idle space	virtual (for examination purpo	-	?				
Volume slack	virtual (for examination purpo		4,0 KB				

Partition	📄 File 🛛 🛋 Preview	💭 Details 🚦	Gallery	Calendar 💷 Legend	VC Sync	~ A≣ 😤 ♦≣	Selected:
				我是图片 IMAGE			

]

5、寻找被删除的文件。

由于删除时,是先del进入回收站,然后清空的,因此被删除的文件会在回收站的路径中。

Guvmage	r dd	X-Wavs	FTK-Win7x64	Guymag	er, P3			
\$RECYCL	E.BIN\S-1-	5-21-3174	665540-37552	55795-414	42190488-1000)		
Nom					Description		Type	Y
□ <u>_</u> . =	\$RECYC	LE.BIN (9)			existing			
□ <u>_</u> . =	S-1-5-21	-3174665	540-375525579	95-414	existing			
🗆 📄 \$I19	O022.jpg				prev. existing,	data unchanged	recycler	
🗆 📑 \$IN3	2V8B.mov	1			prev. existing,	data unchanged	mov	
🗆 🚞 \$INI	VB43O.do	cx		0	prev. existing,	data unchanged	docx	
🗆 📄 \$IY1	1T86.txt				prev. existing,	data unchanged	txt	
🗏 💼 \$R19	90022.jpg				prev. existing,	data not neces	jpg	
🗆 📑 \$RN	32V8B.mo	v			prev. existing,	data not neces	mov	
🗆 📄 \$RN	NB43O.do	CX			prev. existing,	data not neces	docx	
\$RY1	11T86.txt				prev. existing,	data unchanged	txt	
desk	top.ini				existing		ini	

E

y 🛄 Calendar 🔠 Legend I VC
我是被删除的图片
IMAGE

6、可以将镜像中有需要的文件恢复出来进一步分析。

\\$RECYCLE.BIN\S-1-5-21	1-3174	4665540-3755255795-4	142190488-10	00		
□ ▼Name ▲			TDescription			
□ 🗀 = \$RECYCLE.B	IN (9)		existing			
□ 🗀. = S-1-5-21-31	74665	540-3755255795-414	existing			
🗆 📄 \$I19O022.jpg			prev. existing	, data unchanged	rec	
\$IN32V8B.mov			prev. existing	, data unchanged	mo	
\$INNB430.docx			prev. existing	, data unchanged	do	
\$IY11T86.txt			prev. existing	, data unchanged	txt	
📃 💼 \$R19O022.jpg	_		nrev evisting	, data not neces	jpg	
\$RN32V8B.mov	Ø	View		data not neces	mo	
\$RNNB430.docx		Viewer Programs	•	, data not neces	do	
\$RY11T86.txt		Open		, data unchanged	txt	
🗆 🔄 desktop.ini		open			ini	
		Print				
		Recover/Copy				
		Export list				
	Be	Copy "\$R190022.ing"		1		

4.2 使用 AccessData FTK Imager 分析证据

1、添加证据。



2、选择镜像文件,之后选择位置即可。



3、将4个镜像全部载入,这里不支持重命名。



4、分析文件。

FTK同样可以直接预览txt、jpg

		📭 🤇 🗋 🖹 🗎 😹 😹 🗄	2					
		File List						
	-	Name	Size	Туре	Date Modified			
Partition 2 [34899MB] Partition 3 [5958MB] NONAME [NTFS] [orphan]		System Volume Info	1	Directory	2020/3/11 3:			
		\$AttrDef	3	Regular File	2020/3/11 18			
		\$BadClus	0	Regular File	2020/3/11 18			
		SBitmap	187	Regular File	2020/3/11 18			
	Ξ	\$Boot	8	Regular File	2020/3/11 18			
E CYCLE. BIN		\$130	4	NTFS Index A	2020/3/19 15			
		\$LogFile	32,560	Regular File	2020/3/11 18			
nformation		\$MFT	256	Regular File	2020/3/11 18			
1		\$MFTMirr	4	Regular File	2020/3/11 18			
ic disk]		Secure	1	Regular File	2020/3/11 18			
	+	\$TXF_DATA	1	NTFS Logged	2020/3/19 15			
		\$UpCase	128	Regular File	2020/3/11 18			
Ontions	٦	\$Volume	0	Regular File	2020/3/11 18			
opeons	-	document.docx	12	Regular File	2020/3/19 8:			
		🔤 image.jpg	6	Regular File	2020/3/19 8:			
		text.txt	1	Regular File	2020/3/19 8:			
	- 1	R video mov	301	Regular File	2020/3/19 8:			
	nformation ic disk]	nformation ic disk]	Image.jpg	Image Image </td <td>Image: Second Second</td>	Image: Second			

5、寻找被删除的文件。

同样到回收站目录下寻找被清空的文件,这里是使用红叉表示其被删除了。

N 🚯 🕸 🕾 🕿 🖾 🖬 🖬 🖬 🗛 🕾 🕾 🖷 🖷	• 🧧 🔨 🗋 🗎 🗎 🐱 🚟 🛣	8.			
Evidence Tree	File List				
- 100 win7. 201	^ Name	Size	Туре	Date Modified	
Partition 2 [34899MB]	K \$1190022.jpg	1	Regular File	2020/3/19 15	
Partition 3 [5958MB]	\$130	4	NTFS Index A	2020/3/19 15	
-[4 NONAME [NTFS]	SIN32V8B.mov	1	Regular File	2020/3/19 15	
[orphan]	\$INNB430.docx	1	Regular File	2020/3/19 15	
4 SBadClus	X \$IV11T86.txt	1	Regular File	2020/3/19 15	
E C \$Extend	* \$R190022.jpg	12	Regular File	2020/3/19 8:	
SECTCLE. BIN	SRN32V8B.mov	296	Regular File	2020/3/19 8:	
- 3-1-5-21-5114665540-5150	SRNNB430.docx	12	Regular File	2020/3/19 8:	
System Volume Information	X \$RY11T86.txt	1	Regular File	2020/3/19 8:	
Imallocated space]	🛫 🙆 desktop.ini	1	Regular File	2020/3/11 3:	
Custom Content Sources					
Evidence:File System Path File Options					
	<mark>我是被删除的图片</mark> IMAGE				
Properties Hex Value Int Custom Conte.					
listed: 10Selected: 1win7.E01/Partition 3 [5958M	BI/NONAME [NTFS]/[root]/\$RECYCL	E.BIN/S-1	-5-21-317466554	0-3755255795-4142190488-1000/\$R19O022	ipa

6、导出文件。

FTK同样可以导出镜像内的文件。

Name		Size	Туре	Dat
K \$1190022.jpg		1	Regular File	202
\$130		4	NTFS Index A	202
SIN32V8B.mo	v	1	Regular File	202
X \$INNB430.do	ocx	1	Regular File	202
X \$IY11T86.txt		1	Regular File	202
 \$R19002 \$RN32V8 \$RNNB4: \$RV11T8 	Export <u>Files</u> Export File <u>H</u> ash Add to Custom C	List Content 1	Image (AD <u>1</u>)	02
desktop.ini		1	Regular File	202

磁盘镜像挂载

1、FTK有个特殊功能,可以把磁盘镜像映射为一个虚拟磁盘。

AccessData FTK Imager 4.2.1.4

<u>File View Mode Help</u>			
	BAAS	Mount Image To Drive	×
Evidence Tree		Add Image	
		Image File:	
		(jvmware-host(shared Poiders(shared)Forensic(pd)sda3	-
		Mount Type: Physical & Logical	
		Drive Letter: Next Available (F:)	
		Mount Method: Block Device / Read Only	
		Write Cache Folder:	
		\vmware-host\Shared Folders\Shared\Forensic\dd	
		Mount	
	Windows \$		
Custom Content Sources	您想安装这	【个设备软件吗?	
Evidence:File System Path File	1 21	条 EldoS Corporation 系统设备	-
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	存費: EldoS Corporation	
			-
	☑ 始终信任	来目 "EldoS Corporation" 的软件(A), 安裝(I) 不安裝(N)	
	● 您应仅从3	可值的发布者安装驱动程序软件。我如何确定哪些设备软件可以安全安装?	F
		Unmount	
New Edit Remove Remove A	All Create Image	Close	
Properties Hex Value I	Int Custom Con	te	
For User Guide, press F1			

2、这样就多了一个和win7x86主机里一样的分区。



3、不用的时候unmount即可。

Drive	Method	Partition	Image
PhysicalDrive 1	Block Device/Read	Image	\\vmware-host\Shared Folders\Shared\
F:	Block Device/Read	NONAME [NTFS]	\\vmware-host\Shared Folders\Shared\
•			•



使用 foremost 提取磁盘映像里的文件。

foremost -t all -i sda3

-i 指定镜像文件

-t 指定文件类型

all 是所有支持的类型,具体支持的类型查看man。

运行结果:

经过测试, jpg、mov、txt、docx四种类型的文件, 只能提取到docx和jpg两种格式的文件。

2020/7/27	
2020/1121	

	audit.txt		docx			jpg			
Open	•	/mnt/udisl	audit.tx k/Forensid	t c/dd/output	Save		•	•	8
File: so Start: Length:	da3 Thu Mar 19 09 5 GB (624743	9:42:28 20 15808 byte	20 s)						
Num 0: 1: 2: 3:	Name (bs=5: 00000336.jpg 02075360.jpg 02075312.doc 02075336.doc	12) 9 9 5x 5x 5x	Size 5 KE 11 KE 11 KE 11 KE	e F. 3 10 3 10 3 10	ile Offse 172032 062584320 062559744 062572032	et 2 9 4 2	Com	ment	
4 FILES	EXTRACTED	99:47:53 2 Plain Text ▼	020 Tab Wid	th: 8 🔻	Ln 1. C	ol 1	•	IN	s
									-



知其黑 守其白

分享知识盛宴,闲聊大院趣事,备好酒肉等你



长按二维码关注 酒仙桥六号部队