

Anti-Forensic

Breaking Encase with FILE0 and
Winhex

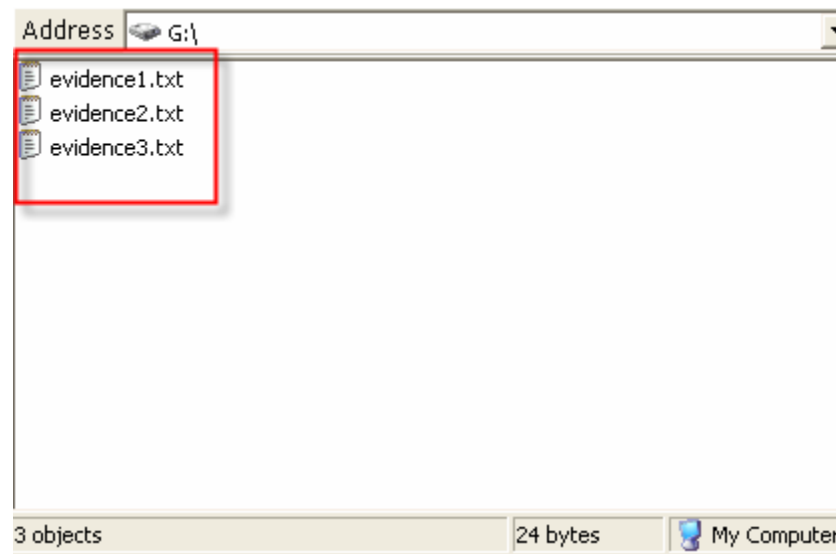
Adonis a.K.a. NtWaK0
www.safehack.com

No Innovation

- ⊙ No real innovation in the anti-forensics field. We need the followings:
 - New ways to hide stuff
 - New ways to erase stuff
 - New ways to exploit stuff e.g. log corruption
 - New ways to exploit commercial tool e.g. encase, FTK.
- ⊙ Forensic Investigator depend to much on commercial tools. Break these tools and you break the investigation , the investigator moral and the investigation budget.

Start by creating Evidence files

⦿ Created files on Drive G:\



Deleting a file leave evidence

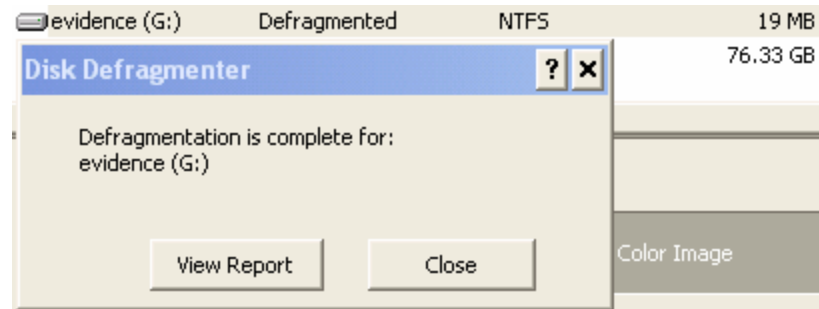
- ⦿ We delete the files without sending to recycler, then we grab the drive using encase.
- ⦿ Encase was able to located all deleted files
- ⦿ Running Disk Defrag does not help U!!!



	Name	Filter	In Report	File Ext
<input type="checkbox"/>	10	🚫 \$ObjId		
<input type="checkbox"/>	11	🚫 \$Quota		
<input type="checkbox"/>	12	🚫 \$Reparse		
<input type="checkbox"/>	13	🔒 \$Secure		
<input type="checkbox"/>	14	\$Secure:\$SDS		
<input type="checkbox"/>	15	🔒 \$UpCase		
<input type="checkbox"/>	16	🔒 \$Volume		
<input type="checkbox"/>	17	🚫 evidence1.txt		txt
<input type="checkbox"/>	18	🚫 evidence2.txt		txt
<input type="checkbox"/>	19	🚫 evidence3.txt		txt
<input type="checkbox"/>	20	🔒 Unallocated Clusters		

Deleting a file leave evidence

- Now we defrag the G: drive and grab it again with encase. Encase still see the deleted files.



A screenshot of Windows Explorer showing the contents of drive G:. The left pane shows a tree view with "Cases", "Case 1", and "G:". The right pane displays a list of files and folders. The list includes a volume label, several temporary files, and evidence files. The "File Ext" column shows the file extensions.

	Name	Filter	In Report	File Ext
<input type="checkbox"/> 16	\$Volume			
<input type="checkbox"/> 17	DFR407.tmp			tmp
<input type="checkbox"/> 18	evidence.exe			exe
<input type="checkbox"/> 19	evidence1.txt			txt
<input type="checkbox"/> 20	evidence2.txt			txt
<input type="checkbox"/> 21	evidence3.txt			txt
<input type="checkbox"/> 22	evidence4.txt			txt
<input type="checkbox"/> 23	evidence5.txt			txt
<input type="checkbox"/> 24	evidence6.exe			exe
<input type="checkbox"/> 25	evidence7.exe			exe
<input type="checkbox"/> 26	Unallocated Clusters			

Removing Evidence Commercial Tools

- ⊙ There are some tools that can help you erasing the file but most of them leave traces.
- ⊙ Here I have deleted two files and I have used SecureClean a very good tool. BUT!!!



**Will deleted these files
and use Secureclean**



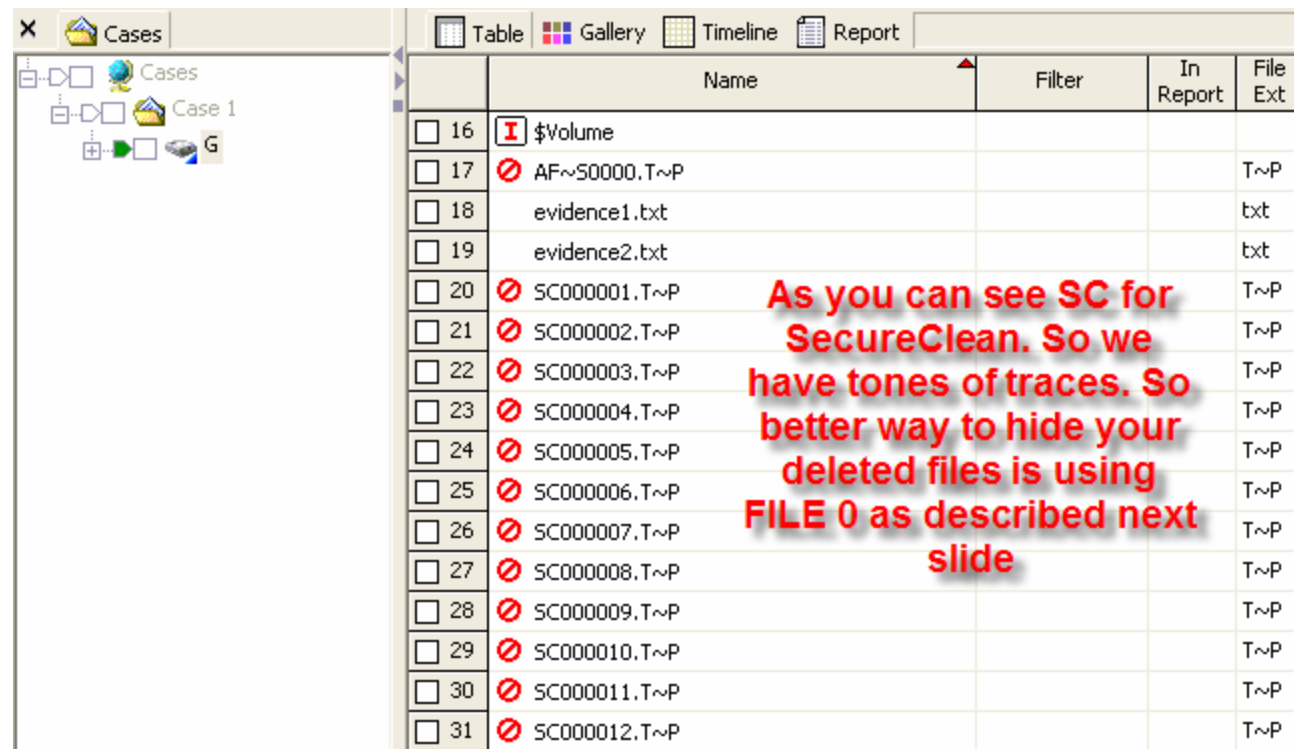
Removing Evidence Commercial Tools

⦿ Running SecureClean on G:\



Removing Evidence Commercial Tools

- As you can see SC for SecureClean. So we have tones of traces. So better way to hide your deleted files is using FILE 0 as described next slide

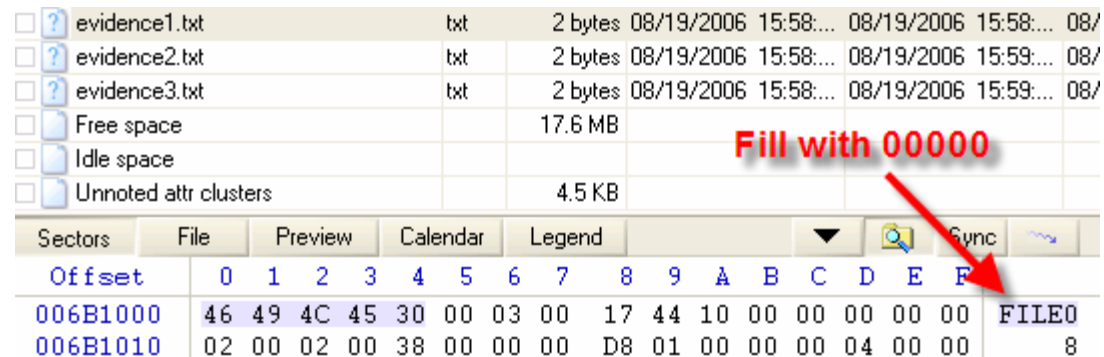


	Name	Filter	In Report	File Ext
<input type="checkbox"/> 16	I \$Volume			
<input type="checkbox"/> 17	AF~S0000.T~P			T~P
<input type="checkbox"/> 18	evidence1.txt			txt
<input type="checkbox"/> 19	evidence2.txt			txt
<input type="checkbox"/> 20	SC000001.T~P			T~P
<input type="checkbox"/> 21	SC000002.T~P			T~P
<input type="checkbox"/> 22	SC000003.T~P			T~P
<input type="checkbox"/> 23	SC000004.T~P			T~P
<input type="checkbox"/> 24	SC000005.T~P			T~P
<input type="checkbox"/> 25	SC000006.T~P			T~P
<input type="checkbox"/> 26	SC000007.T~P			T~P
<input type="checkbox"/> 27	SC000008.T~P			T~P
<input type="checkbox"/> 28	SC000009.T~P			T~P
<input type="checkbox"/> 29	SC000010.T~P			T~P
<input type="checkbox"/> 30	SC000011.T~P			T~P
<input type="checkbox"/> 31	SC000012.T~P			T~P

As you can see SC for SecureClean. So we have tones of traces. So better way to hide your deleted files is using FILE 0 as described next slide

BREAKING ENCASE - Hiding deleted files from Encase

- ⊙ We Open the Disk in Winhex we click on the file name that we like to hide from Encase.
- ⊙ We locate the string FILE 0 and we replace it with 00



The screenshot shows the Winhex interface. The top part is a file list with columns for checkboxes, file names, extensions, sizes, and dates. Below that is a hex editor window with a toolbar and a data grid. A red arrow points to the 'FILE0' string in the hex editor, with the text 'Fill with 00000' above it.

Sectors	File	Preview	Calendar	Legend	▼	🔍	Sync	⚡									
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
006B1000	46	49	4C	45	30	00	03	00	17	44	10	00	00	00	00	00	FILE0
006B1010	02	00	02	00	38	00	00	00	D8	01	00	00	00	04	00	00	8

BREAKING ENCASE - Hiding deleted files from Encase

- ⊙ We dump our disk again using encase. Sure enough we do not see our deleted files.



	Name	Filter	In Report	File Ext
<input type="checkbox"/>	1 I \$AttrDef			
<input type="checkbox"/>	2 I \$BadClus			
<input type="checkbox"/>	3 \$BadClus:\$Bad			
<input type="checkbox"/>	4 I \$Bitmap			
<input type="checkbox"/>	5 I \$Boot			
<input type="checkbox"/>	6 I \$Extend			
<input type="checkbox"/>	7 I \$LogFile			
<input type="checkbox"/>	8 I \$MFT			
<input type="checkbox"/>	9 I \$MFTMirr			
<input type="checkbox"/>	10 I \$ObjId			
<input type="checkbox"/>	11 I \$Quota			
<input type="checkbox"/>	12 I \$Reparse			
<input type="checkbox"/>	13 I \$Secure			
<input type="checkbox"/>	14 \$Secure:\$SDS			
<input type="checkbox"/>	15 I \$UpCase			
<input type="checkbox"/>	16 I \$Volume			
<input type="checkbox"/>	17 I Unallocated Clusters			

Evidence files = Gone. This is a clear issue in Encase. If we use Winhex we can see the file name. But encase does not show anything. This will break encase and sure will break your investigation

BREAKING ENCASE - Hiding deleted files from Encase

- ⊙ HO HO HO as you see the file name was removed and the investigator wont be able to create his timeline or file search using the file name.
- ⊙ So this is one way to break Encase.
- ⊙ Just imagine the investigator face when he does not see your hidden files in ENCASE.