Faut-il acheter un outil de file carving ?

SSTIC #0x0D

4 juin 2015

Christophe GRENIER
grenier@cgsecurity.org

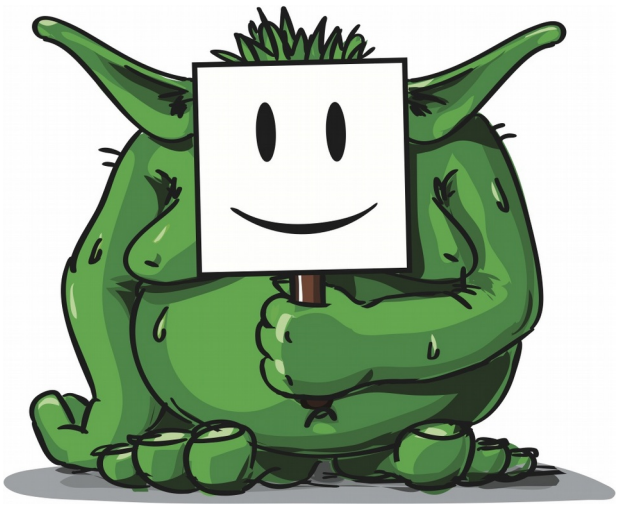
Tests du NIST

- NIST : National Institute of Standards and Technology
- Outils : Forensic File Carving

- Périmètre des tests :
  - fichiers graphiques : gif, bmp, png, jpg, tiff
  - fichiers vidéos : mp4, mov, avi, wmv, 3gp, ogv

Pourquoi acheter un outil de file carving ?

- File carving= récupération de fichiers effacés de formats connus
- But : récupérer des fichiers effacés pour lesquels un « Undelete » n'est pas/plus possible
- Payer un outil pour gagner du temps/réduire le coût humain



Fichiers graphiques contigus

But : récupérer 40 fichiers et 7 miniatures

Test: No Padding	Total Carved	Viewable-Complete	Viewable-Incomplete	Not viewable	False Positive
Adroit Photo Forensics 2013 v3.1d	54	26+7		14	7
EnCase Forensic v6.18.0.59	62	23+7	3	4	25
EnCase Forensic v7.09.05	8946	29+0		2	8915
FTK v4.1	39	26+7		3	3
iLook v2.2.7	0				
PhotoRec v7.0-WIP	47	**40+7**			
Recover My Files v5.2.1	38	38+0			
R-Studio v6.2	38	38+0			
Scalpel v2.0	186	12+0	2	7	165
X-Ways Forensics v17.6	47	**40+7**			

Fichiers vidéos contigus

But : récupérer 36 vidéos

Test: No Padding	Total Carved	Viewable-Complete	Viewable-Incomplete	Not viewable	False Positive
Defraser v1.3	36	25		8	3
Encase v7.09.05	44	16	11	11	6
iLook v.2.2.7	43	2	11	5	25
PhotoRec 7.0-WIP	**37**	**36**		**1**	
R-Studio v6.2	56	31		25	
Recover My Files v5.2.1	34	33		1	
Scalpel v2.0	73	13	10	22	28
X-Ways v17.6	30	27	1	2	