Récupération de données

Christophe GRENIER -
grenier@cgsecurity.org

SSTIC 2006

PhotoRec
Récupération de fichiers

- Logiciel OpenSource (GPL)
- Fonctionne sous
  - DOS,
  - Windows,
  - Linux,
  - FreeBSD, NetBSD, OpenBSD,
  - SunOS
  - MacOS
- Disponible sur http://www.cgsecurity.org

PhotoRec
Récupération de fichiers

- Fonctionne avec
  - les disques durs
  - CD-R/CD-RW/...
  - CompactFlash,
  - Memory Stick,
  - SecureDigital,
  - SmartMedia,
  - Microdrive,
  - MMC...

PhotoRec
Récupération de fichiers

- Travaille sur l'intégralité du média ou une partition
- Reconnaît les systèmes de partitions
  - Intel/ PC
  - Apple partition map
  - Non partitionné
  - Sun Solaris
  - XBox

PhotoRec
Récupération de fichiers

- Conçu à l'origine pour récupérer les photos effacées par mégarde sur les appareils photos numériques ou bien formatées
- Etendu pour travailler avec des supports de grande capacité

PhotoRec
Récupération de fichiers

- Reconnaît les entêtes des formats de fichiers les plus courants
  - Archives: 7z, bz2, gz, rar, tar, zip
  - Multimedia: asf, au, avi, wav, bmp, cdr, cr2, crw, ctg, dcr, dsc, fla, gif, jng, jpg, mng, mov, mp3, mp4, mpg, mrw, nef, ogg, orf, pcx, pef, png, psd, qxd, qxp, raf, raw, rdc, sit, sr2, tif, x3f, xcf
  - Office: doc, mdb, odd, odp, ods, odt, pap, ppt, rtf, sda, sdc, sdd, sdw, slk, sxc, sxd, sxi, sxw, txt, vis, xls
  - Divers: asp, bat, c, dbf, dbx, eps, exe, frm, h, html, jsp, myi, pdf, php, pl, prc, ps, pst, py, qdf,

PhotoRec
Récupération de fichiers

- Capable de récupérer des données, y compris si le système de fichier est irréparable.
- Utilise la notion de bloc de taille fixe
  - FAT
  - NTFS
  - EXT2/ EXT3
  - HFS+
- Effectue plusieurs passes pour tenter de récupérer les fichiers fragmentés

PhotoRec Comparaison

- Outils:
  - foremost 1.2
  - PhotoRec 6.4-WIP
- Challenge de « Data Carving »
  http://www.dfrws.org/2006/challenge/
  50 Mo, pas de système de fichier
  JPEG, ZIP, HTML, TXT, MS Office
  et de nombreux fragments

PhotoRec HTML

- But: 8 HTML
- Foremost 1.2
  - 5 fichiers HTML identifiés
- PhotoRec 6.4- WIP
  - 7 fichiers HTML identifiés
  - 2 fragments HTML non réassemblés mais identifiés comme HTML

PhotoRec
TXT

- But: 3 TXT
- Foremost 1.2
  - 0 fichier TXT identifié
- PhotoRec 6.4- WIP
  - 3 fichiers TXT
  - 72 fragments DOC identifiés comme txt

PhotoRec
DOC

- But: Entre 4 et 6 DOC/ XLS
- Foremost 1.2
  - 2 fichiers DOC
- PhotoRec 6.4- WIP
  - 3 fichiers DOC
  - 2 fichiers DOC illisibles
  - 1 fichier DOC illisible mais récupérable

PhotoRec
ZIP

- But: 3 ZIP
- Foremost 1.2
  - 0 fichier ZIP
- PhotoRec 6.4-WIP
  - 2 fichiers ZIP
  - 1 fichier ZIP corrompu (5/6 fichiers) mais réparable avec un petit script maison.

PhotoRec
JPG

- But: Entre 9 et 14 JPG
- Foremost 1.2
  - 4 fichiers JPG
  - 6 fichiers JPG partiels
- PhotoRec 6.4- WIP
  - 9 fichiers JPG
  - En option, 5 fichiers JPG partiels sont aussi récupérés

PhotoRec Conclusion

	Foremost 1.2	PhotoRec 6.4-WIP
HTML	5	7
TXT	0	3
DOC	2	3
ZIP	0	2
JPEG	4	9
Total	11	24