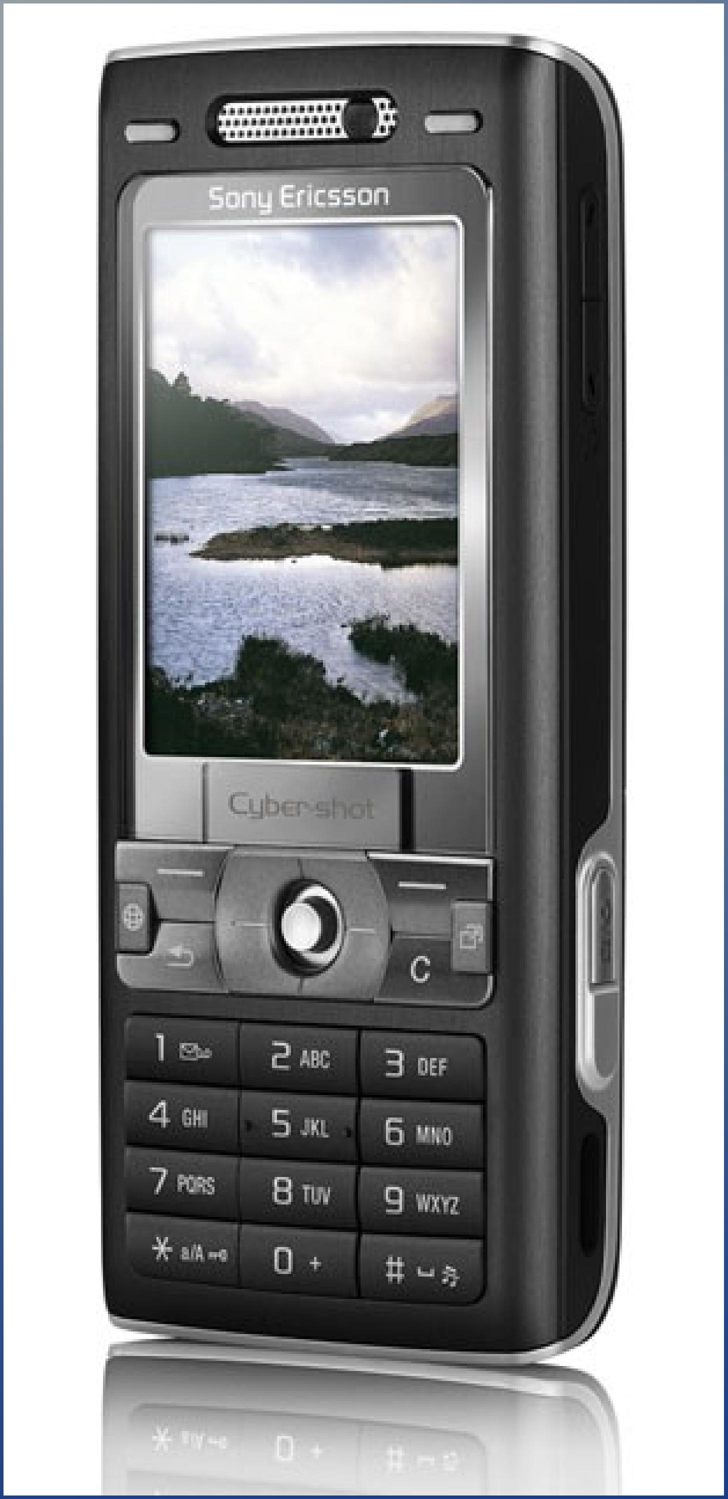
Analyse de la mémoire Flash d'un téléphone portable

SSTIC 2010

Christophe GRENIER - grenier@cgsecurity.org

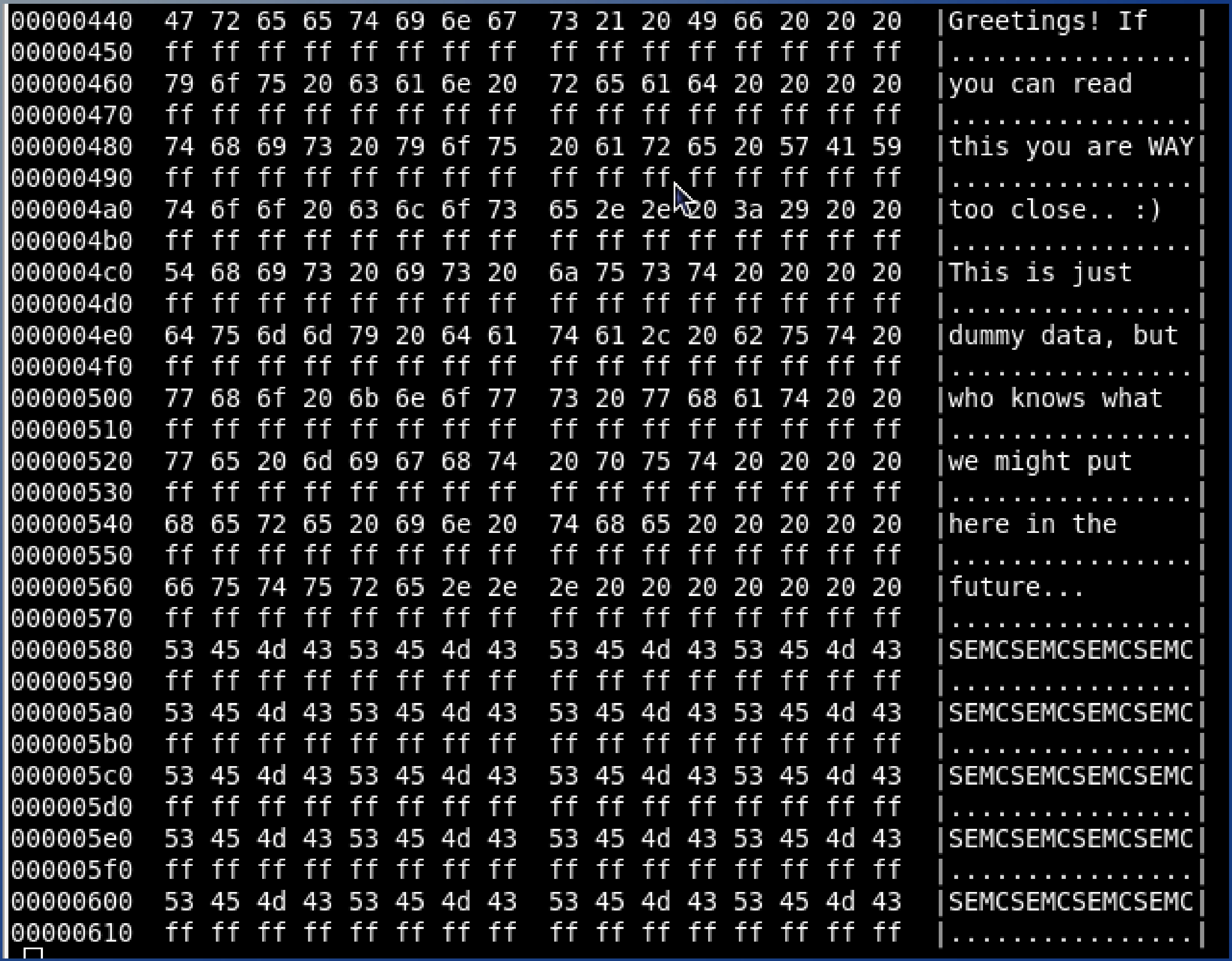


Scenario

In the current operation, undercover investigators arranged an arms deal through one of Mr. Victor's front companies, Smurf Celtic. To convince him that the deal was real, an initial down payment was made by electronic funds transfer to Smelt Bank in France into an account owned by another front company named RipTide Security.

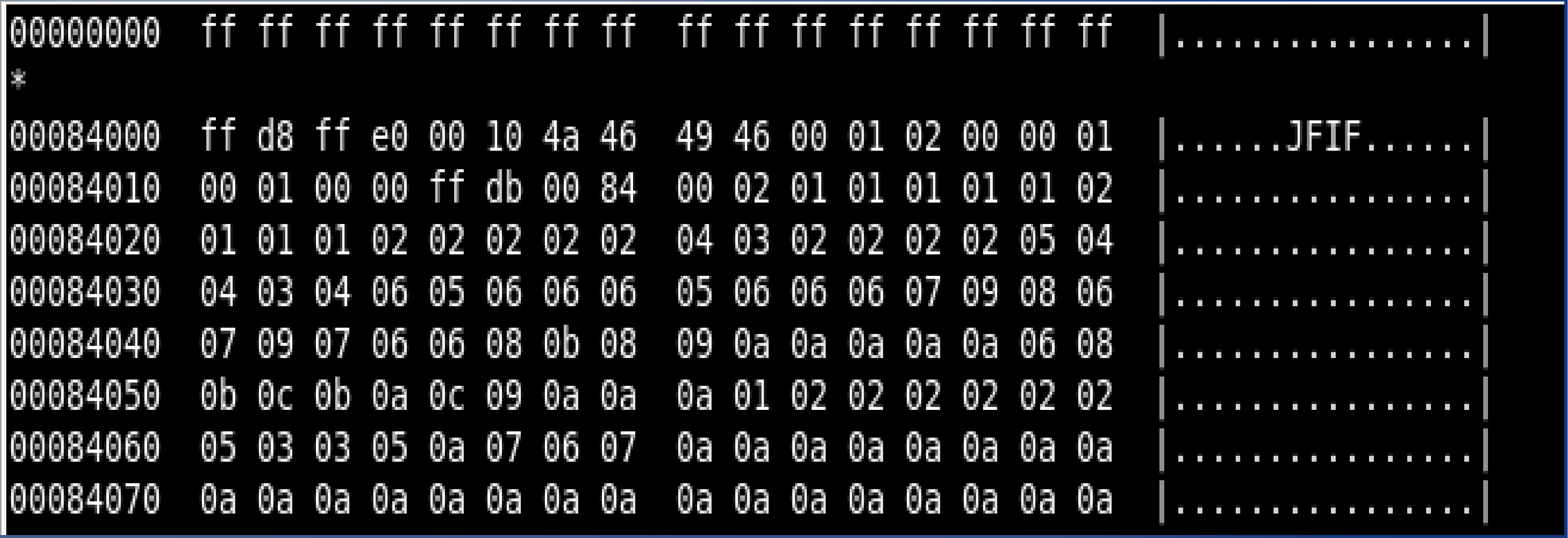
http://www.dfrws.org/2010/challenge/

SonyEricsson_K800i_Norflash_PF38F5060M0Y0BE.dmp



```
00000440  47 72 65 65 74 69 6e 67  73 21 20 49 66 20 20 20  |Greetings! If   |
00000450  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
00000460  79 6f 75 20 63 61 6e 20  72 65 61 64 20 20 20 20  |you can read    |
00000470  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
00000480  74 68 69 73 20 79 6f 75  20 61 72 65 20 57 41 59  |this you are WAY|
00000490  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
000004a0  74 6f 6f 20 63 6c 6f 73  65 2e 2e 20 3a 29 20 20  |too close.. :)  |
000004b0  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
000004c0  54 68 69 73 20 69 73 20  6a 75 73 74 20 20 20 20  |This is just    |
000004d0  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
000004e0  64 75 6d 6d 79 20 64 61  74 61 2c 20 62 75 74 20  |dummy data, but |
000004f0  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
00000500  77 68 6f 20 6b 6e 6f 77  73 20 77 68 61 74 20 20  |who knows what  |
00000510  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
00000520  77 65 20 6d 69 67 68 74  20 70 75 74 20 20 20 20  |we might put    |
00000530  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
00000540  68 65 72 65 20 69 6e 20  74 68 65 20 20 20 20 20  |here in the     |
00000550  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
00000560  66 75 74 75 72 65 2e 2e  2e 20 20 20 20 20 20 20  |future...       |
00000570  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
00000580  53 45 4d 43 53 45 4d 43  53 45 4d 43 53 45 4d 43  |SEMCSEMCSEMCSEMC|
00000590  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
000005a0  53 45 4d 43 53 45 4d 43  53 45 4d 43 53 45 4d 43  |SEMCSEMCSEMCSEMC|
000005b0  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
000005c0  53 45 4d 43 53 45 4d 43  53 45 4d 43 53 45 4d 43  |SEMCSEMCSEMCSEMC|
000005d0  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
000005e0  53 45 4d 43 53 45 4d 43  53 45 4d 43 53 45 4d 43  |SEMCSEMCSEMCSEMC|
000005f0  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
00000600  53 45 4d 43 53 45 4d 43  53 45 4d 43 53 45 4d 43  |SEMCSEMCSEMCSEMC|
00000610  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
```

SonyEricsson_K800i_NAND_NAND512R3A.bin



```
00000000  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
00084000  ff d8 ff e0 00 10 4a 46  49 46 00 01 02 00 00 01  |......JFIF......|
00084010  00 01 00 00 ff db 00 84  00 02 01 01 01 01 01 02  |................|
00084020  01 01 01 02 02 02 02 02  04 03 02 02 02 02 05 04  |................|
00084030  04 03 04 06 05 06 06 06  05 06 06 06 07 09 08 06  |................|
00084040  07 09 07 06 06 08 0b 08  09 0a 0a 0a 0a 0a 06 08  |................|
00084050  0b 0c 0b 0a 0c 09 0a 0a  0a 01 02 02 02 02 02 02  |................|
00084060  05 03 03 05 0a 07 06 07  0a 0a 0a 0a 0a 0a 0a 0a  |................|
00084070  0a 0a 0a 0a 0a 0a 0a 0a  0a 0a 0a 0a 0a 0a 0a 0a  |................|
```

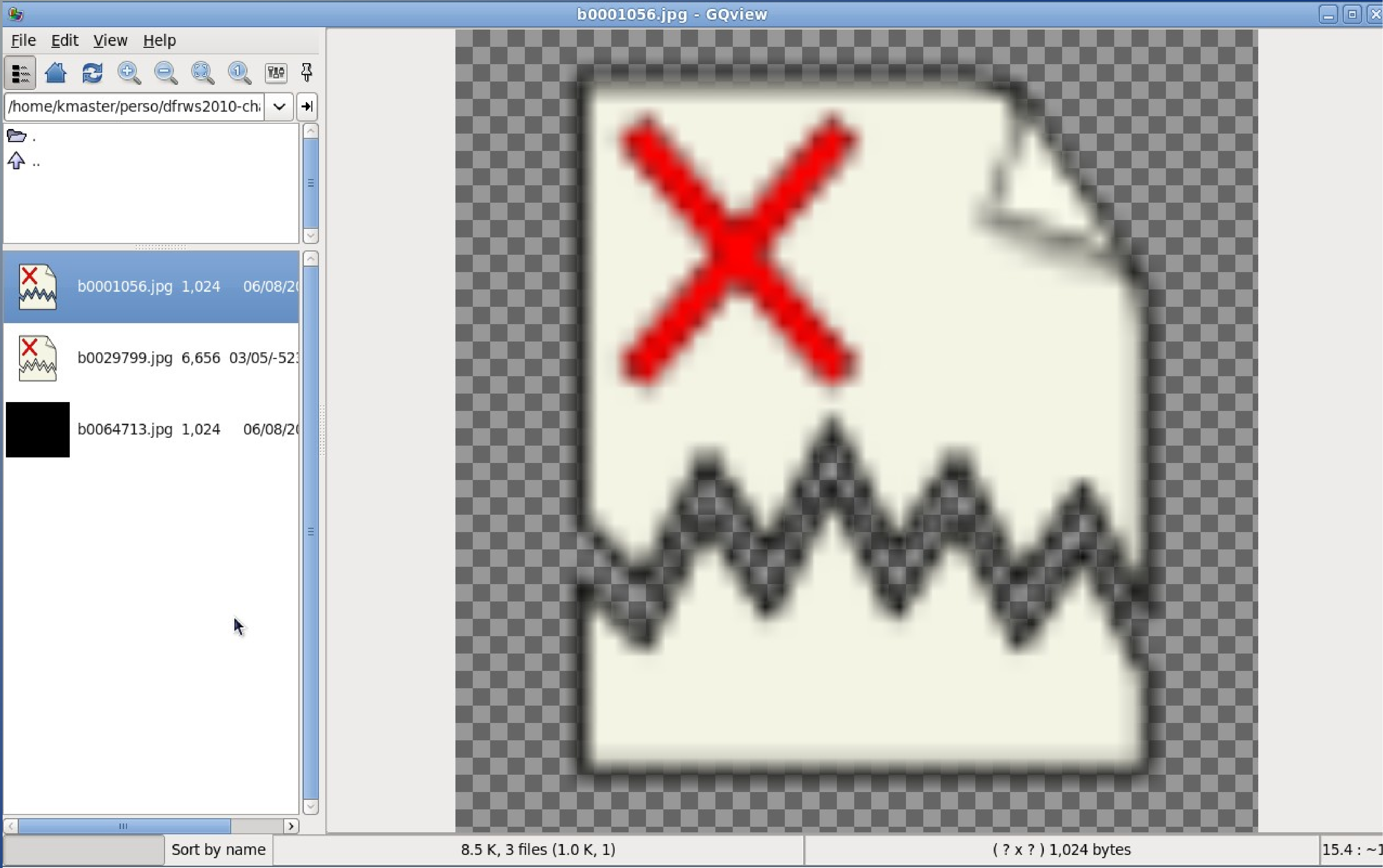
http://www.cgsecurity.org

PhotoRec
Récupération de fichiers

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

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, sh, wab



b0001056.jpg - GQview

/home/kmaster/perso/dfrws2010-ch

.
..

b0001056.jpg	1,024	06/08/2
b0029799.jpg	6,656	03/05/-52
b0064713.jpg	1,024	06/08/2

Sort by name

8.5 K, 3 files (1.0 K, 1)

(? x ?) 1,024 bytes

15.4 : ~1

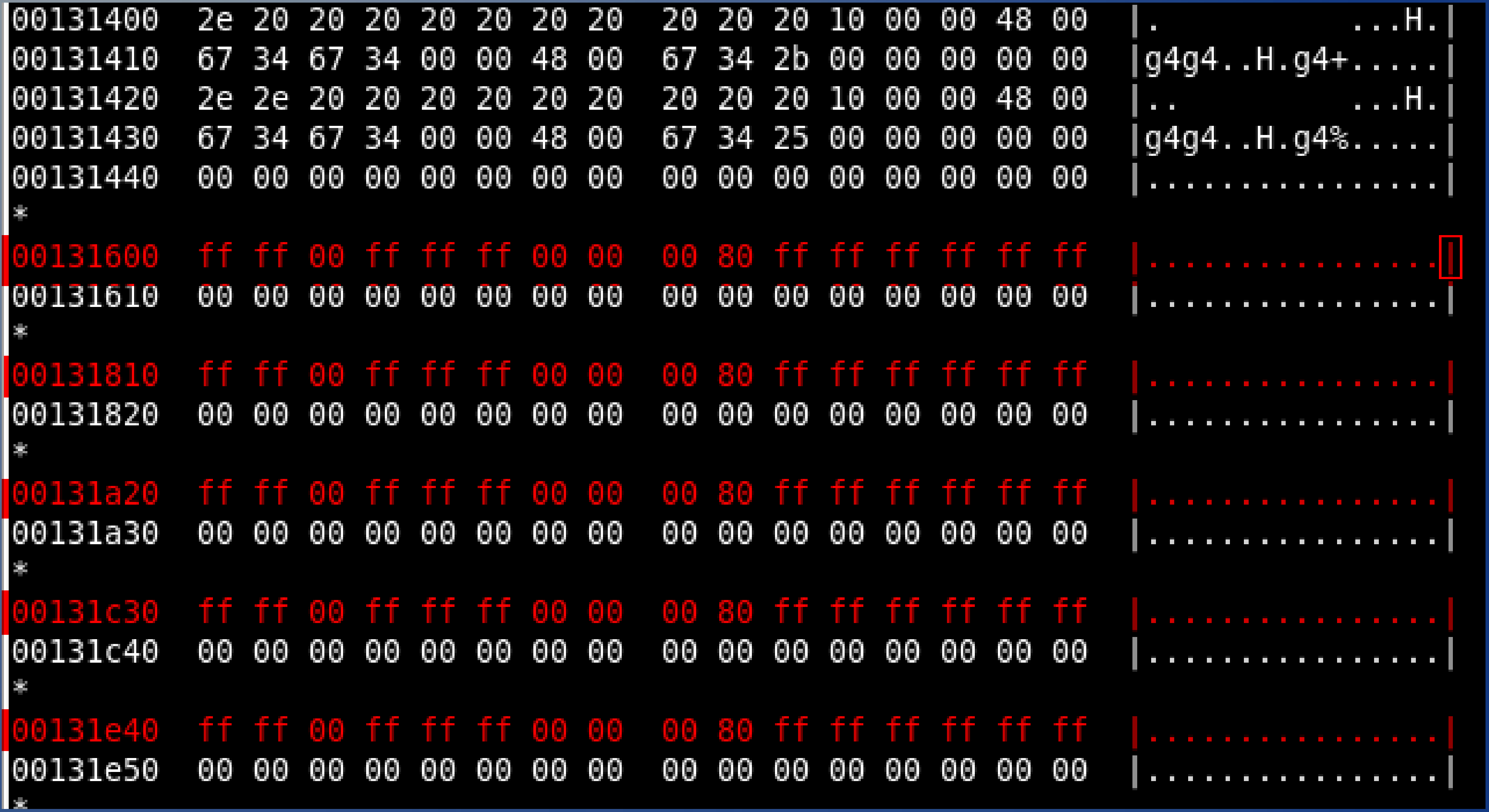
Du secteur à la mémoire flash

Une zone d'une mémoire Flash supporte 100000 cycles d'effacement/écriture

Solutions des fabricants:

- Présence de checksum (CRC) ou code de correction d'erreurs (ECC)
- Wear levelling: ne pas toujours utiliser les mêmes zones pour stocker les nouvelles informations

Des intrus dans le répertoire!



```
00131400  2e 20 20 20 20 20 20 20  20 20 20 10 00 00 48 00  |.          ...H.|
00131410  67 34 67 34 00 00 48 00  67 34 2b 00 00 00 00 00  |g4g4..H.g4+.....|
00131420  2e 2e 20 20 20 20 20 20  20 20 20 10 00 00 48 00  |..         ...H.|
00131430  67 34 67 34 00 00 48 00  67 34 25 00 00 00 00 00  |g4g4..H.g4%.....|
00131440  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00131600  ff ff 00 ff ff ff 00 00  00 80 ff ff ff ff ff ff  |................|
00131610  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00131810  ff ff 00 ff ff ff 00 00  00 80 ff ff ff ff ff ff  |................|
00131820  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00131a20  ff ff 00 ff ff ff 00 00  00 80 ff ff ff ff ff ff  |................|
00131a30  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00131c30  ff ff 00 ff ff ff 00 00  00 80 ff ff ff ff ff ff  |................|
00131c40  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00131e40  ff ff 00 ff ff ff 00 00  00 80 ff ff ff ff ff ff  |................|
00131e50  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
```

Coding skills!

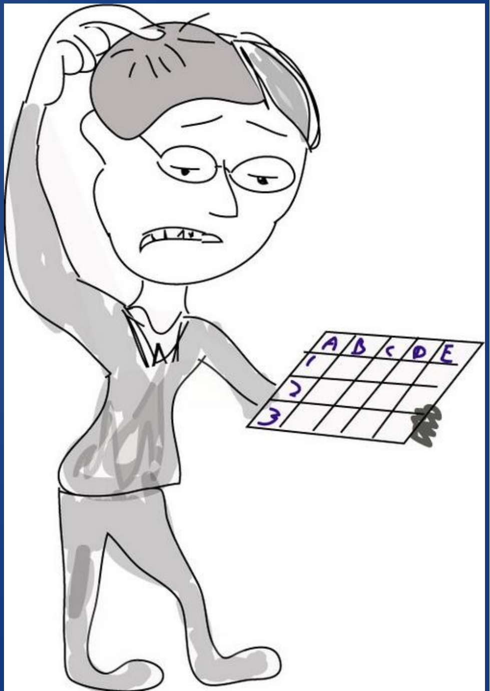
Solution pour supprimer ces données supplémentaires:

```
 while(fread(buffer, 0x210, 1, in)>0)
  {
    fwrite(buffer, 0x200, 1, out);
  }
```

Wear levelling en action

```
offset 0x9bb80 - cluster 46
offset 0xa9200 - cluster 3858
offset 0xab300 - cluster 527
offset 0xaf500 - cluster 527
offset 0xb1600 - cluster 527
offset 0xb4780 - cluster 3855
offset 0xc2e80 - cluster 3148
offset 0xc4f80 - cluster 141
```

C'est compliqué, ignorons le problème!

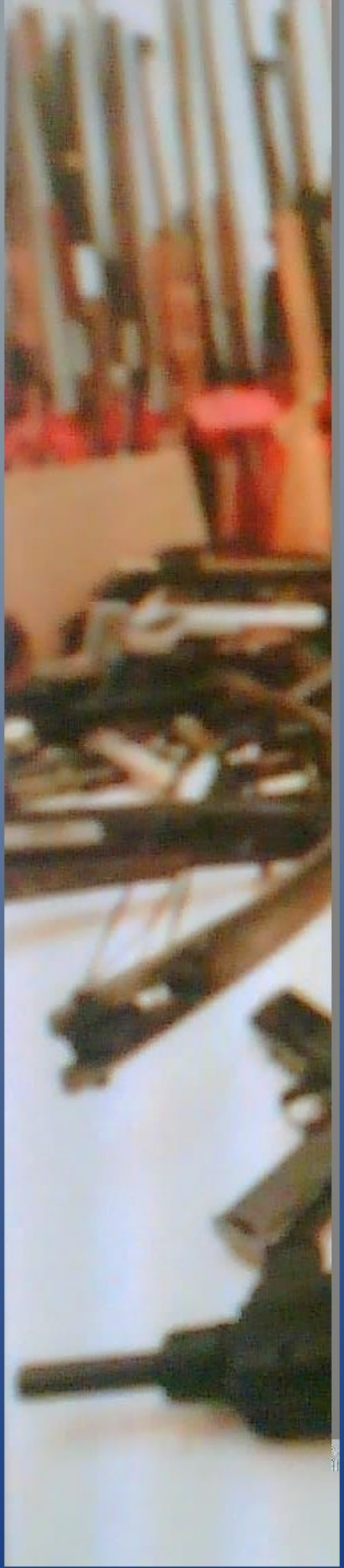


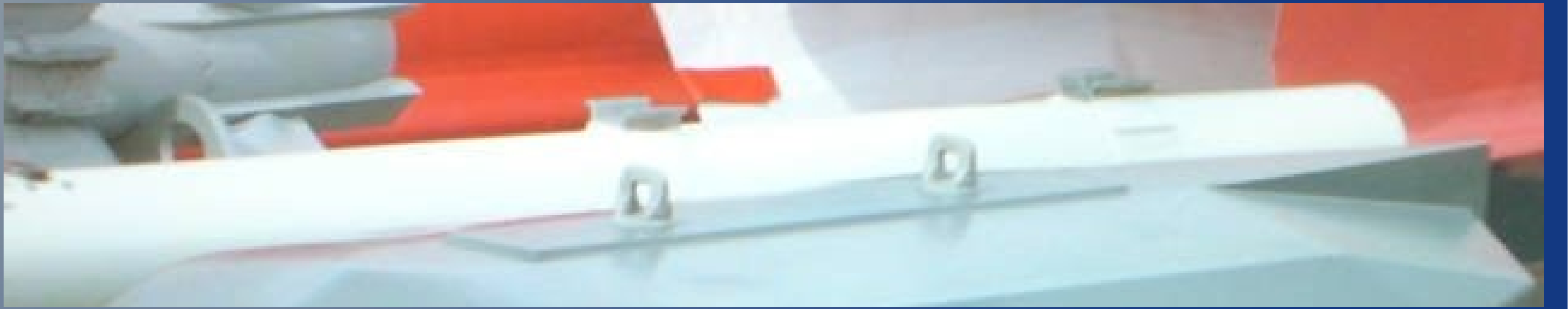
emails

recup_dir.1/f0030856.utf16
Hi,
Make sure 100 J85-21 replacement engines are bought. I will arrange further air deployment for customer.
Best regards,
M.V.

recup_dir.1/f0056032.utf16
Sir is going to contact you about some rockets

recup_dir.1/f0057992.utf16
Arrange for a delivery of some stuff from Germany to Iraq. Not via normal ways.
M.V.





Avantage d'ignorer le wear levelling:
- Résultats rapides
- Le plus long est de faire les slides

Inconvénients:
- Fragment de fichiers, d'images...

http://www.cgsecurity.org