

Cryptanalyse en boîte noire de chiffrement propriétaire

Pierre Capillon
ANSSI / Bureau audits et inspections



fw-c.00.bin

```

0000 00F0: 00 00 A2 8C 00 FF 03 24 C0 BF 19 3C 24 10 43 00 .....$ ...<$ .C.
0000 0100: 55 00 42 34 21 20 00 00 00 00 A2 AC 18 0E 39 37 U.B4! .. .....97
0000 0110: 08 00 20 03 00 00 00 00 3F 3D 3E 41 3A 3D 3F 3A .. .....?=>A:=?:
0000 0120: 3E 40 2D 3E 3F 47 3D 3D 47 3D 3D 1A 17 5A 4E 5B >@->?G== G==..ZN[
0000 0130: 62 53 4E 50 61 62 5F 52 5F 2D 4F 62 56 59 51 2D bSNPab_R _-0bVYQ-
0000 0140: 60 66 60 1A 17 53 76 7B 6E 79 2D 5F 72 79 72 6E `f`..Sv{ ny-_ryrn
0000 0150: 80 72 2D 4F 82 76 79 71 2D 2D 2D 2D 2D 2D 2D 2D .r-0.vyq -----
0000 0160: 2D 2D 2D 2D 2D 2D 2D 2D 83 F5 EA 21 50 07 02 00 ----- ...!P...
0000 0170: 22 40 AA 11 06 1E 36 95 33 75 83 5A AB C7 DF 50 "@....6. 3u.Z...P
0000 0180: C6 C6 C9 D4 95 D3 88 B3 06 8C 4D 4C 19 0A A8 AE ..... ..ML....

```

fw-c.00.clear

```

0000 00F0: 00 00 A2 8C 00 FF 03 24 C0 BF 19 3C 24 10 43 00 .....$ ...<$ .C.
0000 0100: 55 00 42 34 21 20 00 00 00 00 A2 AC 18 0E 39 37 U.B4! .. .....97
0000 0110: 08 00 20 03 00 00 00 00 32 30 31 34 2D 30 32 2D .. .....2014-02-
0000 0120: 31 33 20 31 32 3A 30 30 3A 30 30 0D 0A 4D 41 4E 13 12:00 :00..MAN
0000 0130: 55 46 41 43 54 55 52 45 52 20 42 55 49 4C 44 20 UFACTURE R BUILD
0000 0140: 53 59 53 0D 0A 46 69 6E 61 6C 20 52 65 6C 65 61 SYS..Fin al Relea
0000 0150: 73 65 20 42 75 69 6C 64 20 20 20 20 20 20 20 20 se Build
0000 0160: 20 20 20 20 20 20 20 20 83 F5 EA 21 50 07 02 00 ..... ...!P...
0000 0170: 22 40 AA 11 06 1E 36 95 33 75 83 5A AB C7 DF 50 "@....6. 3u.Z...P
0000 0180: C6 C6 C9 D4 95 D3 88 B3 06 8C 4D 4C 19 0A A8 AE ..... ..ML....

```

Arrow keys move	F find	RET next difference	ESC quit	T move top
C ASCII/EBCDIC	E edit file	G goto position	Q quit	B move bottom

Disclaimer

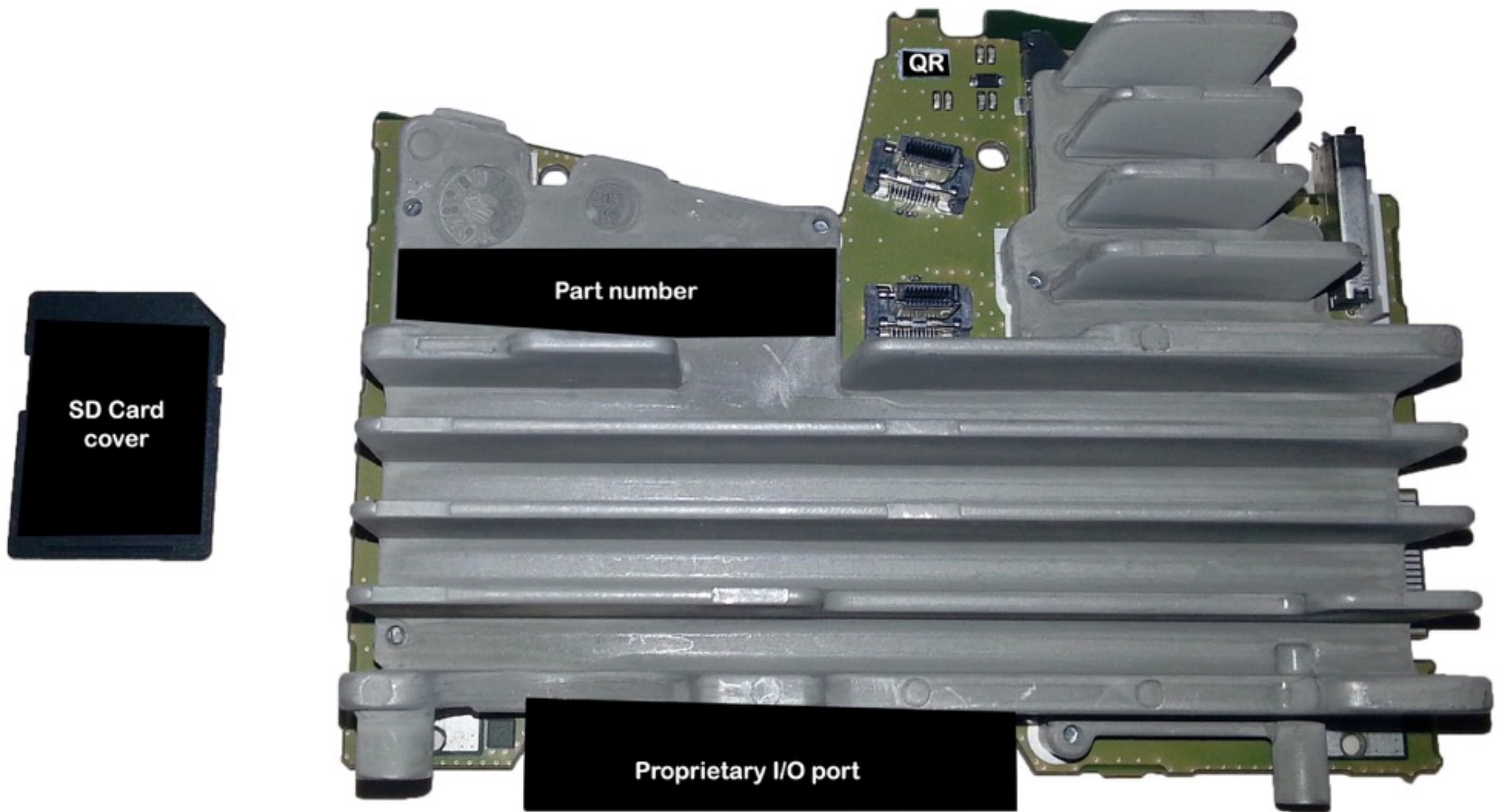
- **Aucun pré-requis mathématique**
 - algorithme propriétaire observé très simple
- **Aucun pré-requis de *reverse-engineering***
 - savoir lire de l'hexadécimal
 - connaître les opérations élémentaires (XOR, <</>>, ROL/ROR...)

Objectifs

- Montrer l'état d'esprit d'un attaquant face à un chiffré seul
- Évoquer les idées suivies et leurs impasses sur un exemple concret
- Démontrer le faux sentiment de sécurité perçu par les fabricants
- Démontrer les compétences et moyens nécessaires pour réaliser ces attaques

Contexte

- Audit d'un système embarqué en mode “*hackathon*”
 - ➔ récupération du *firmware* pour *reverse-engineering*
- Pas d'informations privilégiées
- L'équipement prêté par le constructeur doit rester en état de fonctionnement



Conséquences

- Pas d'attaque matérielle envisageable
 - Utilisation normale possible (interface web, analyse des protocoles propriétaires, outil de paramétrage)
 - Accès aux mises à jour officielles (site web public du constructeur)
- ➔ **Sans vulnérabilité sur l'équipement, seule l'analyse du fichier de mise à jour permettrait de retrouver le *firmware***

Caractéristiques

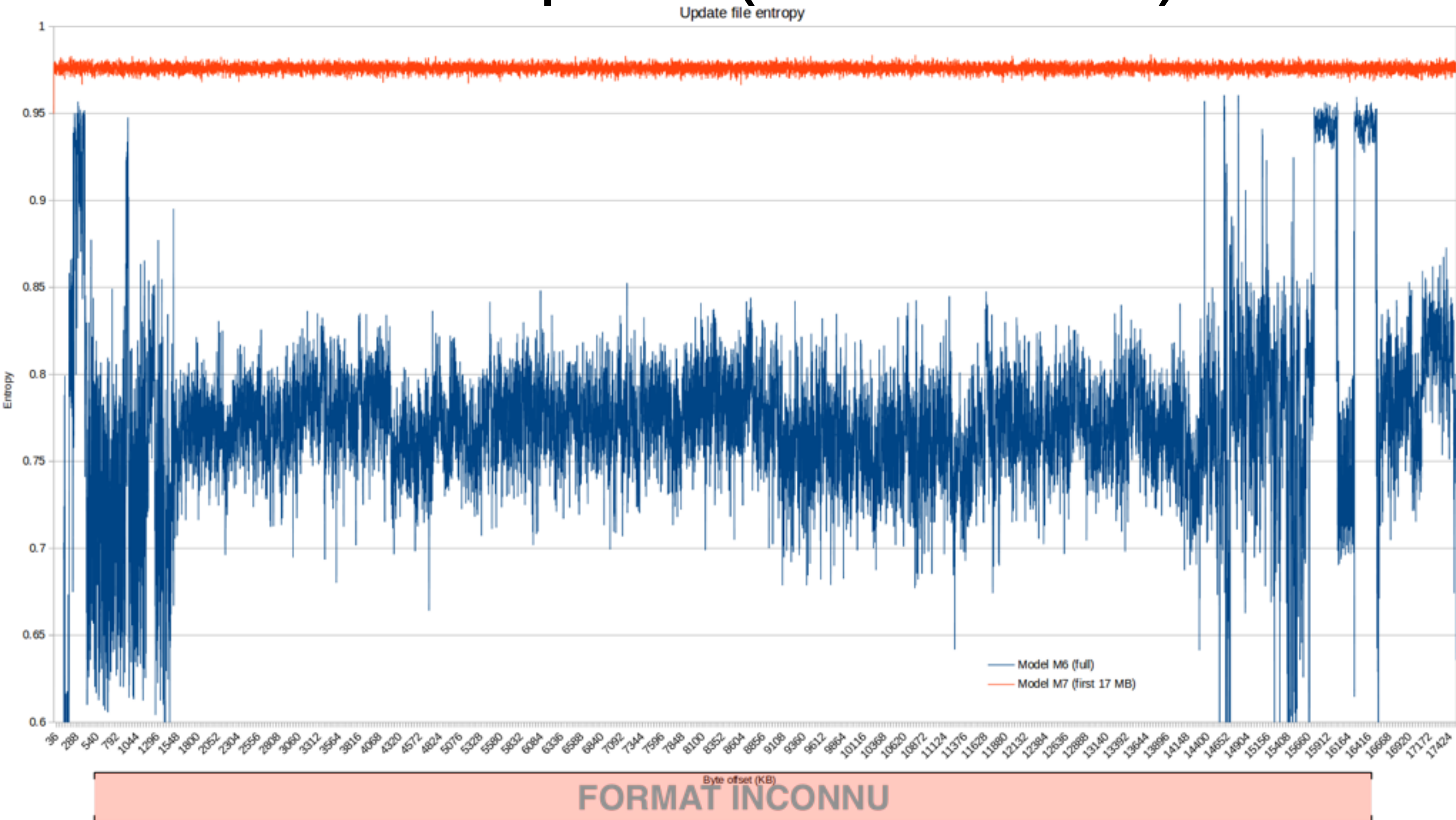
- Format de fichier propriétaire
- Architecture CPU cible inconnue
- Deux familles de modèles
 - famille A : update ~17 Mo
 - famille B : update ~50 Mo
- *Upgrade / downgrade* arbitraire supporté

Format de fichier

Identification des champs

FORMAT INCONNU

Entropie (binwalk)



Fichier de mise à jour

En-tête

```
fw-c.00.bin
0000 0000: 04 00 00 00 00 00 00 00 00 00 00 00 00 56 CC CC 00 .....V...
0000 0010: 4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 4F 4E MODEL-M6 -VERSION
0000 0020: 2D 30 31 20 00 00 00 00 00 00 00 00 20 00 00 00 -01 .....
0000 0030: A3 D2 FD FF 46 49 45 4C 44 31 00 00 00 00 FF FF ....FIEL D1.....
0000 0040: FF FF 46 49 45 4C 44 32 CA 8E 13 01 63 9C B6 8F ..FIELD2 ....c...
0000 0050: 46 49 45 4C 44 33 48 00 00 00 7A 29 EB FF 46 49 FIELD3H. ..z)..FI
0000 0060: 45 4C 44 34 46 49 45 4C 44 31 01 00 EF 00 00 00 EL D4FIEL D1.....
0000 0070: 00 00 4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 ..MODEL- M6-VERSI
0000 0080: 4F 4E 2D 30 31 20 56 00 00 00 46 49 45 4C 44 32 ON-01 V. ..FIELD2
0000 0090: 46 49 45 4C 44 33 10 02 43 6F 70 79 72 69 67 68 FIELD3.. Copyrigh
0000 00A0: 74 20 4D 41 4E 55 46 41 43 54 55 52 45 52 20 49 t MANUFA CTURER I
0000 00B0: 44 20 2D 20 32 30 31 34 20 20 20 20 E0 BF 04 3C D - 2014 ...<
0000 00C0: C8 02 85 34 32 00 03 24 32 00 02 3C 00 00 A3 AC ...42..$ 2..<....
0000 00D0: EC 03 86 34 E0 03 42 34 E4 03 84 34 10 00 03 24 ...4..B4 ...4...$
0000 00E0: A0 BF 05 3C 00 00 82 AC 5C 00 A5 34 00 00 C3 AC ...<.... \..4....
0000 00F0: 00 00 A2 8C 00 FF 03 24 C0 BF 19 3C 24 10 43 00 .....$ ...<$..C.
0000 0100: 55 00 42 34 21 20 00 00 00 00 A2 AC 18 0E 39 37 U.B4! .. .....97
0000 0110: 08 00 20 03 00 00 00 00 3F 3D 3E 41 3A 3D 3F 3A .. ..... ?=>A:=?:
0000 0120: 3E 40 2D 3E 3F 47 3D 3D 47 3D 3D 1A 17 5A 4E 5B >@->?G== G==..ZN[
0000 0130: 62 53 4E 50 61 62 5F 52 5F 2D 4F 62 56 59 51 2D bSNPab_R _-0bVYQ-
0000 0140: 60 66 60 1A 17 53 76 7B 6E 79 2D 5F 72 79 72 6E `f`..Sv{ ny-_ryrn
0000 0150: 80 72 2D 4F 82 76 79 71 2D 2D 2D 2D 2D 2D 2D 2D .r-0.vyq -----
```

```
Arrow keys move F find RET next difference ESC quit
C ASCII/EBCDIC E edit file G goto position Q quit
```

HDR

FORMAT INCONNU

En-tête

```
fw-c.00.bin
0000 0000: 04 00 00 00 00 00 00 00 00 00 00 00 00 56 CC CC 00 .....V...
0000 0010: 4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 4F 4E MODEL-M6 -VERSION
0000 0020: 2D 30 31 20 00 00 00 00 00 00 00 00 20 00 00 00 -01 ....
0000 0030: A3 D2 FD FF 46 49 45 4C 44 31 00 00 00 00 FF FF ....FIEL D1.....
0000 0040: FF FF 46 49 45 4C 44 32 CA 8E 13 01 63 9C B6 8F ..FIELD2 ....c...
0000 0050: 46 49 45 4C 44 33 48 00 00 00 7A 29 EB FF 46 49 FIELD3H. ..z)..FI
0000 0060: 45 4C 44 34 46 49 45 4C 44 31 01 00 EF 00 00 00 ELD4FIEL D1.....
0000 0070: 00 00 4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 ..MODEL- M6-VERSI
0000 0080: 4F 4E 2D 30 31 20 56 00 00 00 46 49 45 4C 44 32 ON-01 V. ..FIELD2
0000 0090: 46 49 45 4C 44 33 10 02 43 6F 70 79 72 69 67 68 FIELD3.. Copyrigh
0000 00A0: 74 20 4D 41 4E 55 46 41 43 54 55 52 45 52 20 49 t MANUFA CTURER I
0000 00B0: 44 20 2D 20 32 30 31 34 20 20 20 20 E0 BF 04 3C D - 2014 ...<
0000 00C0: C8 02 85 34 32 00 03 24 32 00 02 3C 00 00 A3 AC ...42..$ 2..<....
0000 00D0: EC 03 86 34 E0 03 42 34 E4 03 84 34 10 00 03 24 ...4..B4 ...4...$
0000 00E0: A0 BF 05 3C 00 00 82 AC 5C 00 A5 34 00 00 C3 AC ...<.... \..4....
0000 00F0: 00 00 A2 8C 00 FF 03 24 C0 BF 19 3C 24 10 43 00 .....$ ...<$.C.
0000 0100: 55 00 42 34 21 20 00 00 00 00 A2 AC 18 0E 39 37 U.B4! .. .....97
0000 0110: 08 00 20 03 00 00 00 00 3F 3D 3E 41 3A 3D 3F 3A .. ..... ?=>A:=?:
0000 0120: 3E 40 2D 3E 3F 47 3D 3D 47 3D 3D 1A 17 5A 4E 5B >@->?G== G==..ZN[
0000 0130: 62 53 4E 50 61 62 5F 52 5F 2D 4F 62 56 59 51 2D bSNPab_R _-0bVYQ-
0000 0140: 60 66 60 1A 17 53 76 7B 6E 79 2D 5F 72 79 72 6E `f`..Sv{ ny-_ryrn
0000 0150: 80 72 2D 4F 82 76 79 71 2D 2D 2D 2D 2D 2D 2D 2D .r-0.vyq -----
```

```
Arrow keys move F find RET next difference ESC quit
C ASCII/EBCDIC E edit file G goto position Q quit
```

HDR

FORMAT INCONNU

En-tête

```
fw-c.00.bin
0000 0000: 04 00 00 00 00 00 00 00 00 00 00 00 00 56 CC CC 00 .....V...
0000 0010: 4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 4F 4E MODEL-M6 -VERSION
0000 0020: 2D 30 31 20 00 00 00 00 00 00 00 00 20 00 00 00 -01 ....
0000 0030: A3 D2 FD FF 46 49 45 4C 44 31 00 00 00 00 FF FF ....FIEL D1.....
0000 0040: FF FF 46 49 45 4C 44 32 CA 8E 13 01 63 9C B6 8F ..FIELD2 ....c...
0000 0050: 46 49 45 4C 44 33 48 00 00 00 7A 29 EB FF 46 49 FIELD3H. ..z)..FI
0000 0060: 45 4C 44 34 46 49 45 4C 44 31 01 00 EF 00 00 00 ELD4FIEL D1.....
0000 0070: 00 00 4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 ..MODEL- M6-VERSI
0000 0080: 4F 4E 2D 30 31 20 56 00 00 00 46 49 45 4C 44 32 ON-01 V. ..FIELD2
0000 0090: 46 49 45 4C 44 33 10 02 43 6F 70 79 72 69 67 68 FIELD3.. Copyrigh
0000 00A0: 74 20 4D 41 4E 55 46 41 43 54 55 52 45 52 20 49 t MANUFA CTURER I
0000 00B0: 44 20 2D 20 32 30 31 34 20 20 20 20 E0 BF 04 3C D - 2014 ...<
0000 00C0: C8 02 85 34 32 00 03 24 32 00 02 3C 00 00 A3 AC ...42..$ 2..<....
0000 00D0: EC 03 86 34 E0 03 42 34 E4 03 84 34 10 00 03 24 ...4..B4 ...4...$
0000 00E0: A0 BF 05 3C 00 00 82 AC 5C 00 A5 34 00 00 C3 AC ...<.... \..4....
0000 00F0: 00 00 A2 8C 00 FF 03 24 C0 BF 19 3C 24 10 43 00 .....$ ...<$.C.
0000 0100: 55 00 42 34 21 20 00 00 00 00 A2 AC 18 0E 39 37 U.B4! .. .....97
0000 0110: 08 00 20 03 00 00 00 00 3F 3D 3E 41 3A 3D 3F 3A .. ..... ?=>A:=?:
0000 0120: 3E 40 2D 3E 3F 47 3D 3D 47 3D 3D 1A 17 5A 4E 5B >@->?G== G==..ZN[
0000 0130: 62 53 4E 50 61 62 5F 52 5F 2D 4F 62 56 59 51 2D bSNPab_R _-0bVYQ-
0000 0140: 60 66 60 1A 17 53 76 7B 6E 79 2D 5F 72 79 72 6E `f`..Sv{ ny-_ryrn
0000 0150: 80 72 2D 4F 82 76 79 71 2D 2D 2D 2D 2D 2D 2D 2D .r-0.vyq -----
```

Arrow keys move F find RET next difference ESC quit
C ASCII/EBCDIC E edit file G goto position Q quit

HDR

FORMAT INCONNU

En-tête

```
fw-c.00.bin
0000 0000: 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .. ....V...
0000 0010: 4D 4F 44 45 4C 2D 4D 36 2D 50 00 00 00 00 00 00 M6 -VERSION
0000 0020: 2D 30 31 20 00 00 00 00 00 00 00 00 00 00 20 00 00 00 -01 .....
0000 0030: A3 D2 FD FF 46 49 45 4C 44 31 00 00 00 00 FF FF ....FIEL D1.....
0000 0040: FF FF 46 49 45 4C 44 32 CA 8E 13 01 63 9C B6 8F ..FIELD2 ....c...
0000 0050: 46 49 45 4C 44 33 48 00 00 00 7A 29 EB FF 46 49 FIELD3H. ..z)..FI
0000 0060: 45 4C 44 34 46 49 45 4C 44 31 01 00 EF 00 00 00 ELD4FIEL D1.....
0000 0070: 00 00 4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 ..MODEL- M6-VERSI
0000 0080: 4F 4E 2D 30 31 20 56 00 00 00 46 49 45 4C 44 32 ON-01 V. ..FIELD2
0000 0090: 46 49 45 4C 44 6F 70 79 72 69 67 68 FIELD3.. Copyrigh
0000 00A0: 74 20 4D 41 4E 54 55 52 45 52 20 49 t MANUFA CTURER I
0000 00B0: 44 20 2D 20 32 30 31 34 20 20 20 20 E0 BF 04 3C D - 2014 ...<
0000 00C0: C8 02 85 34 32 00 03 24 32 00 02 3C 00 00 A3 AC ...42..$ 2..<....
0000 00D0: EC 03 86 34 E0 03 42 34 E4 03 84 34 10 00 03 24 ...4..B4 ...4...$
0000 00E0: A0 BF 05 3C 00 00 82 AC 5C 00 A5 34 00 00 C3 AC ...<.... \..4....
0000 00F0: 00 00 A2 8C 00 FF 03 24 C0 BF 19 3C 24 10 43 00 .....$ ...<$..C.
0000 0100: 55 00 42 34 21 20 00 00 00 00 A2 AC 18 0E 39 37 U.B4! .. .....97
0000 0110: 08 00 20 03 00 00 00 00 3F 3D 3E 41 3A 3D 3F 3A .. ..... ?=>A:=?:
0000 0120: 3E 40 2D 3E 3F 47 3D 3D 47 3D 3D 1A 17 5A 4E 5B >@->?G== G==..ZN[
0000 0130: 62 53 4E 50 61 62 5F 52 5F 2D 4F 62 56 59 51 2D bSNPab_R _-0bVYQ-
0000 0140: 60 66 60 1A 17 53 76 7B 6E 79 2D 5F 72 79 72 6E `f`..Sv{ ny-_ryrn
0000 0150: 80 72 2D 4F 82 76 79 71 2D 2D 2D 2D 2D 2D 2D 2D .r-0.vyq -----
```

```

Arrow keys move      F find          RET next difference  ESC quit
C ASCII/EBCDIC      E edit file      G goto position      Q quit

```

HDR

FORMAT INCONNU

En-tête

```
fw-c.00.bin
0000 0000: 04 00 00 00 00 00 00 00 00 00 00 00 00 56 CC CC 00 .....V...
0000 0010: 4D 4F 44 45 4C 2D 4D 36          Little endian = 0 MODEL-M6 -VERSION
0000 0020: 2D 30 31 20 00 00 00 00 -01 ....
0000 0030: A3 D2 FD FF 46 49 45 4C 44 31 00 00 00 00 FF FF ....FIEL D1.....
0000 0040: FF FF 46 49 45 4C 44 32 CA 8E 13 01 63 9C B6 8F ..FIELD2 ....c...
0000 0050: 46 49 45 4C 44 33 48 00 00 00 7A 29 EB FF 46 49 FIELD3H. ..z)..FI
0000 0060: 45 4C 44 34 46 49 45 4C 44 31 01 00 EF 00 00 00 ELD4FIEL D1.....
0000 0070: 00 00 4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 ..MODEL- M6-VERSI
0000 0080: 4F 4E 2D 30 31 20 56 00 00 00 46 49 45 4C 44 32 ON-01 V. ..FIELD2
0000 0090: 46 49 45 4C 44 33 10 02 43 6F 70 79 72 69 67 68 FIELD3.. Copyrigh
0000 00A0: 74 20 4D 41 4E 55 46 41 43 54 55 52 45 0 octets MANUFA CTURER I
0000 00B0: 44 20 2D 20 32 30 31 34 20 20 20 20 E0 - 2014 ...<
0000 00C0: C8 02 85 34 32 00 03 24 32 00 02 3C 00 00 A3 AC ...42..$ 2..<....
0000 00D0: EC 03 86 34 E0 03 42 34 E4 03 84 34 10 00 03 24 ...4..B4 ...4...$
0000 00E0: A0 BF 05 3C 00 00 82 AC 5C 00 A5 34 00 00 C3 AC ...<.... \..4....
0000 00F0: 00 00 A2 8C 00 FF 03 24 C0 BF 19 3C 24 10 43 00 .....$ ...<$..C.
0000 0100: 55 00 42 34 21 20 00 00 00 00 A2 AC 18 0E 39 37 U.B4! .. .....97
0000 0110: 08 00 20 03 00 00 00 00 3F 3D 3E 41 3A 3D 3F 3A .. ..... ?=>A:=?:
0000 0120: 3E 40 2D 3E 3F 47 3D 3D 47 3D 3D 1A 17 5A 4E 5B >@->?G== G==..ZN[
0000 0130: 62 53 4E 50 61 62 5F 52 5F 2D 4F 62 56 59 51 2D bSNPab_R _-0bVYQ-
0000 0140: 60 66 60 1A 17 53 76 7B 6E 79 2D 5F 72 79 72 6E `f`..Sv{ ny-_ryrn
0000 0150: 80 72 2D 4F 82 76 79 71 2D 2D 2D 2D 2D 2D 2D 2D .r-0.vyq -----
```

Arrow keys move F find RET next difference ESC quit
 C ASCII/EBCDIC E edit file G goto position Q quit

HDR

FORMAT INCONNU

En-tête

```
fw-c.00.bin
Version
N
04 00 00 00 00 00 00 00 00 00 00 00 00 56 CC CC 00 .....V...
4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 4F 4E MODEL-M6 -VERSION
2D 30 31 20 00 00 00 00 00 00 00 00 20 00 00 00 -01 ....
0000 0030: A3 D2 FD FF 46 49 45 4C 44 31 00 00 00 00 FF FF ....FIEL D1.....
0000 0040: FF FF 46 49 45 4C 44 32 CA 8E 13 01 63 9C B6 8F ..FIELD2 ....c...
0000 0050: 46 49 45 4C 44 33 48 00 00 00 7A 29 EB FF 46 49 FIELD3H. ..z)..FI
0000 0060: 45 4C 44 34 46 49 45 4C 44 31 01 00 EF 00 00 00 ELD4FIEL D1.....
0000 0070: 00 00 4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 ..MODEL- M6-VERSI
0000 0080: 4F 4E 2D 30 31 20 56 00 00 00 46 49 45 4C 44 32 ON-01 V. ..FIELD2
0000 0090: 46 49 45 4C 44 33 10 02 43 6F 70 79 72 69 67 68 FIELD3.. Copyright
```

```
fw-c.01.bin
Version
N+1
04 00 00 00 00 00 00 00 00 00 00 00 00 56 CC CC 01 .....V...
4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 4F 4E MODEL-M6 -VERSION
2D 30 31 20 00 00 00 00 00 00 00 00 20 00 00 00 -01 ....
0000 0030: A3 D2 FD FF 46 49 45 4C 44 31 00 00 00 00 FF FF ....FIEL D1.....
0000 0040: FF FF 46 49 45 4C 44 32 D2 92 13 01 16 B1 9F 8F ..FIELD2 .....
0000 0050: 46 49 45 4C 44 33 48 00 00 00 1C B4 F0 FF 46 49 FIELD3H. ....FI
0000 0060: 45 4C 44 34 46 49 45 4C 44 31 01 00 EF 00 00 00 ELD4FIEL D1.....
0000 0070: 00 00 4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 ..MODEL- M6-VERSI
0000 0080: 4F 4E 2D 30 31 20 56 00 00 00 46 49 45 4C 44 32 ON-01 V. ..FIELD2
0000 0090: 46 49 45 4C 44 33 10 02 43 6F 70 79 72 69 67 68 FIELD3.. Copyright
```

```
Arrow keys move F find RET next difference ESC quit T move top
C ASCII/EBCDIC E edit file G goto position Q quit B move bottom
```

HDR

FORMAT INCONNU

En-tête

```
fw-c.00.bin
0000 0000: 04 00 00 00 00 00 00 00 00 00 00 00 00 56 CC CC 00 .....V...
0000 0010: 4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 4F 4E MODEL-M6 -VERSION
0000 0020: 2D 30 31 20 00 00 00 00 00 00 00 00 20 00 00 00 -01 ....
0000 0030: A3 D2 FD FF 46 49 45 4C 44 31 00 00 00 00 FF FF ....FIEL D1.....
0000 0040: FF FF 46 49 45 4C 44 32 CA 8E 13 01 63 9C B6 8F ..FIELD2 ....c...
0000 0050: 46 49 45 4C 44 33 48 00 00 00 7A 29 EB FF 46 49 FIELD3H. ..z)..FI
0000 0060: 45 4C 44 34 46 49 45 4C 44 31 01 00 EF 00 00 00 ELD4FIEL D1.....
0000 0070: 00 00 4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 ..MODEL- M6-VERSI
0000 0080: 4F 4E 2D 30 31 20 56 00 00 00 46 49 45 4C 44 32 ON-01 V. ..FIELD2
0000 0090: 46 49 45 4C 44 33 10 02 43 6F 70 79 72 69 67 68 FIELD3.. Copyrigh
0000 00A0: 74 20 4D 41 4E 55 46 41 43 54 55 52 45 52 20 49 t MANUFA CTURER I
0000 00B0: 44 20 2D 20 32 30 31 34 20 20 20 20 E0 BF 04 3C D - 2014 ...<
0000 00C0: C8 02 85 34 32 00 03 24 32 00 02 3C 00 00 A3 AC ...42..$ 2..<....
0000 00D0: EC 03 86 34 E0 03 42 34 E4 03 84 34 10 00 03 24 ...4..B4 ...4...$
0000 00E0: A0 BF 05 3C 00 00 82 AC 5C 00 A5 34 00 00 C3 AC ...<.... \..4....
0000 00F0: 00 00 A2 8C 00 FF 03 24 C0 BF 19 3C 24 10 43 00 .....$ ...<$.C.
0000 0100: 55 00 42 34 21 20 00 00 00 00 A2 AC 18 0E 39 37 U.B4! .. .....97
0000 0110: 08 00 20 03 00 00 00 00 3F 3D 3E 41 3A 3D 3F 3A .. ..... ?=>A:=?:
0000 0120: 3E 40 2D 3E 3F 47 3D 3D 47 3D 3D 1A 17 5A 4E 5B >@->?G== G==..ZN[
0000 0130: 62 53 4E 50 61 62 5F 52 5F 2D 4F 62 56 59 51 2D bSNPab_R _-0bVYQ-
0000 0140: 60 66 60 1A 17 53 76 7B 6E 79 2D 5F 72 79 72 6E `f`..Sv{ ny-_ryrn
0000 0150: 80 72 2D 4F 82 76 79 71 2D 2D 2D 2D 2D 2D 2D 2D .r-0.vvq -----
```

Arrow keys move F find RET next difference ESC quit
 C ASCII/EBCDIC E edit file G goto position Q quit

HDR

FORMAT INCONNU

En-tête

```
fw-c.00.clear
0000 0000: 04 00 00 00 00 00 00 00 00 00 00 00 00 56 CC CC 00 .....V...
0000 0010: 4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 4F 4E MODEL-M6 -VERSION
0000 0020: 2D 30 31 20 00 00 00 00 00 00 00 00 20 00 00 00 -01 ....
0000 0030: A3 D2 FD FF 46 49 45 4C 44 31 00 00 00 00 FF FF ....FIEL D1.....
0000 0040: FF FF 46 49 45 4C 44 32 CA 8E 13 01 63 9C B6 8F ..FIELD2 ....c...
0000 0050: 46 49 45 4C 44 33 48 00 00 00 7A 29 EB FF 46 49 FIELD3H. ..z)..FI
0000 0060: 45 4C 44 34 46 49 45 4C 44 31 01 00 EF 00 00 00 ELD4FIEL D1.....
0000 0070: 00 00 4D 4F 44 45 4C 2D 4D 36 2D 56 45 52 53 49 ..MODEL- M6-VERSI
0000 0080: 4F 4E 2D 30 31 20 56 00 00 00 46 49 45 4C 44 32 ON-01 V. ..FIELD2
0000 0090: 46 49 45 4C 44 33 10 02 43 6F 70 79 72 69 67 68 FIELD3.. Copyrigh
0000 00A0: 74 20 4D 41 4E 55 46 41 43 54 55 52 45 52 20 49 t MANUFA CTURER I
0000 00B0: 44 20 2D 20 32 30 31 34 20 20 20 20 E0 BF 04 3C D - 2014 ...<
0000 00C0: C8 02 85 34 32 00 03 24 32 00 02 3C 00 00 A3 AC ...42..$ 2..<....
0000 00D0: EC 03 86 34 E0 03 42 34 E4 03 84 34 10 00 03 24 ...4..B4 ...4...$
0000 00E0: A0 BF 05 3C 00 00 82 AC 5C 00 A5 34 00 00 C3 AC ...<.... \..4....
0000 00F0: ROT 13 (pour mieux brouiller les pistes)
0000 0100:
0000 0110: 08 00 20 03 00 00 00 00 32 30 31 34 2D 30 32 2D .. ..... 2014-02-
0000 0120: 31 33 20 31 32 3A 30 30 3A 30 30 0D 0A 4D 41 4E 13 12:00 :00..MAN
0000 0130: 55 46 41 43 54 55 52 45 52 20 42 55 49 4C 44 20 UFACTURE R BUILD
0000 0140: 53 59 53 0D 0A 46 69 6E 61 6C 20 52 65 6C 65 61 SYS..Fin al Relea
0000 0150: 73 65 20 42 75 69 6C 64 20 20 20 20 20 20 20 20 se Build
```

```
Arrow keys move F find RET next difference ESC quit
C ASCII/EBCDIC E edit file G goto position Q quit
```

HDR

FORMAT INCONNU

En-tête

fw-c.00.bin																
Version N	2D	2D	2D	2D	2D	2D	2D	83	F5	EA	21	50	07	02	00	----- ...!P...
	22	40	AA	11	06	1E	36	95	33	75	83	5A	AB	C7	DF	50 "@....6. 3u.Z...P
	C6	C6	C9	D4	95	D3	88	B3	06	8C	4D	4C	19	0A	A8	AEML....
0000 0190:	A3	FB	37	3F	30	86	11	01	4D	8A	FE	BA	9D	3F	C3	25 ..7?0... M....?..%
0000 01A0:	21	27	43	87	4D	78	FF	41	BF	9B	0E	5C	E6	1A	E3	CB !'C.Mx.A ...\....
0000 01B0:	D4	CB	94	DA	93	54	C7	26	D7	E6	C9	1F	00	00	00	00T.&
0000 01C0:	E3	B0	C4	42	98	FC	1C	14	9A	FB	F4	C8	99	6F	B9	24 ...B....o.\$
0000 01D0:	27	AE	41	E4	64	9B	93	4C	A4	95	99	1B	78	52	B8	55 '.A.d..LxR.U
0000 01E0:	00	00	80	01	00	00	C0	00	00	00	00	01	12	91	14	00
0000 01F0:	00	00	80	00	80	C0	01	0E	5F	11	93	D1	40	40	00	40
fw-c.01.bin																
Version N+1	2D	2D	2D	2D	2D	2D	2D	83	F5	EA	21	50	07	02	00	----- ...!P...
	22	40	AA	11	06	1E	36	95	33	75	83	5A	AB	C7	DF	50 "@....6. 3u.Z...P
	C6	C6	C9	D4	95	D3	88	B3	06	8C	4D	4C	19	0A	A8	AEML....
0000 0190:	A3	FB	37	3F	38	8A	11	01	ED	B2	CD	C7	DC	0C	17	4A ..7?8...J
0000 01A0:	EB	26	72	95	77	FC	D3	4B	9C	90	60	99	2A	E0	FE	B2 .&r.w..K ..`.*...
0000 01B0:	BC	0D	F9	5D	8B	17	8E	DB	D7	E6	C9	1F	00	00	00	00 ...]....
0000 01C0:	E3	B0	C4	42	98	FC	1C	14	9A	FB	F4	C8	99	6F	B9	24 ...B....o.\$
0000 01D0:	27	AE	41	E4	64	9B	93	4C	A4	95	99	1B	78	52	B8	55 '.A.d..LxR.U
0000 01E0:	30	00	00	00	18	00	00	00	20	00	00	00	02	40	22	92 0..... @".
0000 01F0:	10	00	00	00	C0	01	10	38	32	FA	2B	62	00	08	08	088 2.+b....
Arrow keys move F find RET next difference ESC quit T move top C ASCII/EBCDIC E edit file G goto position Q quit B move bottom																

HDR

FORMAT INCONNU

En-tête

fw-c.00.bin															
Version N		2D	2D	2D	2D	2D	2D	2D	2D	83	F5	EA	21	50	07 02 00
		22	40	AA	11	06	1E	36	95	33	75	83	5A	AB	C7 DF 50
		C6	C6	C9	D4	95	D3	88	B3	06	8C	4D	4C	19	0A A8 AE
0000	0190:	A3	FB	37	3F	30	86	11	01	4D	8A	FE	BA	9D	3F C3 25
0000	01A0:	21	27	43	87	4D	78	FF	41	BF	9B	0E	5C	E6	1A E3 CB
0000	01B0:	D4	CB	94	DA	93	54	C7	26	D7	E6	C9	1F	00 00 00 00	
0000	01C0:	E3	B0	C4	42	98	FC	1C	14	9A	FB	F4	C8	99	6F B9 24
0000	01D0:	27	AE	41	E4	64	9B	93	4C	A4	95	99	1B	78	52 B8 55
0000	01E0:	00	00	80	01	00	00	C0	00	00	00	00	01	12	91 14 00
0000	01F0:	00	00	80	00	80	C0	01	0E	5F	11	93	D1	40	40 00 40
fw-c.01.bin															
Version N+1		2D	2D	2D	2D	2D	2D	2D	2D	83	F5	EA	21	50	07 02 00
		22	40	AA	11	06	1E	36	95	33	75	83	5A	AB	C7 DF 50
		C6	C6	C9	D4	95	D3	88	B3	06	8C	4D	4C	19	0A A8 AE
0000	0190:	A3	FB	37	3F	38	8A	11	01	ED	B2	CD	C7	DC	0C 17 4A
0000	01A0:	EB	26	72	95	77	FC	D3	4B	9C	90	60	99	2A	E0 FE B2
0000	01B0:	BC	0D	F9	5D	8B	17	8E	DB	D7	E6	C9	1F	00 00 00 00	
0000	01C0:	E3	B0	C4	42	98	FC	1C	14	9A	FB	F4	C8	99	6F B9 24
0000	01D0:	27	AE	41	E4	64	9B	93	4C	A4	95	99	1B	78	52 B8 55
0000	01E0:	30	00	00	00	18	00	00	00	20	00	00	00	02	40 22 92
0000	01F0:	10	00	00	00	C0	01	10	38	32	FA	2B	62	00	08 08 08
Arrow keys move F find RET next difference ESC quit T move top C ASCII/EBCDIC E edit file G goto position Q quit B move bottom															

SHA256 Chaîne vide

En-tête

fw-c.00.bin															
Version N	2D	2D	2D	2D	2D	2D	2D	2D	83	F5	EA	21	50	07	02 00
	22	40	AA	11	06	1E	36	95	33	75	83	5A	AB	C7	DF 50
	C6	C6	C9	D4	95	D3	88	B3	06	8C	4D	4C	19	0A	A8 AE
0000 0190:	A3	FB	37	3F	30	86	11	01	4D	8A	FE	BA	9D	3F	C3 25
0000 01A0:	21	27	43	87	4D	78	FF	41	BF	9B	0E	5C	E6	1A	E3 CB
0000 01B0:	D4	CB	94	DA	93	54	C7	26	D7	E6	C9	1F	00	00	00 00
0000 01C0:	E3	B0	C4	42	98	FC	1C	14	9A	FB	F4	C8	99	6F	B9 24
0000 01D0:	27	AE	41	E4	64	9B	93	4C	A4	95	99	1B	78	52	B8 55
0000 01E0:	00	00	80	01	00	00	C0	00	00	00	00	01	12	91	14 00
0000 01F0:	00	00	80	00	80	C0	01	0E	5F	11	93	D1	40	40	00 40
fw-c.01.bin															
Version N+1	2D	2D	2D	2D	2D	2D	2D	2D	83	F5	EA	21	50	07	02 00
	22	40	AA	11	06	1E	36	95	33	75	83	5A	AB	C7	DF 50
	C6	C6	C9	D4	95	D3	88	B3	06	8C	4D	4C	19	0A	A8 AE
0000 0190:	A3	FB	37	3F	38	8A	11	01	ED	B2	CD	C7	DC	0C	17 4A
0000 01A0:	EB	26	72	95	77	FC	D3	4B	9C	90	60	99	2A	E0	FE B2
0000 01B0:	BC	0D	F9	5D	8B	17	8E	DB	D7	E6	C9	1F	00	00	00 00
0000 01C0:	E3	B0	C4	42	98	FC	1C	14	9A	FB	F4	C8	99	6F	B9 24
0000 01D0:	27	AE	41	E4	64	9B	93	4C	A4	95	99	1B	78	52	B8 55
0000 01E0:	30	00	00	00	18	00	00	00	20	00	00	00	02	40	22 92
0000 01F0:	10	00	00	00	C0	01	10	38	32	FA	2B	62	00	08	08 08
Arrow keys move F find RET next difference ESC quit T move top C ASCII/EBCDIC E edit file G goto position Q quit B move bottom															

HDR

FORMAT INCONNU

En-tête

fw-c.00.bin															
Version N	2D	2D	2D	2D	2D	2D	2D	2D	83	F5	EA	21	50	07	02 00
	22	40	AA	11	06	1E	36	95	33	75	83	5A	AB	C7	DF 50
	C6	C6	C9	D4	95	D3	88	B3	06	8C	4D	4C	19	0A	A8 AE
0000 0190:	A3	FB	37	3F	30	86	11	01	4D	8A	FE	BA	9D	3F	C3 25
0000 01A0:	21	27	43	87	4D	78	FF	41	BF	9B	0E	5C	E6	1A	E3 CB
0000 01B0:	D4	CB	94	DA	93	54	C7	26	D7	E6	C9	1F	00	00	00 00
0000 01C0:	E3	B0	C4	42	98	FC	1C	14	9A	FB	F4	C8	99	6F	B9 24
0000 01D0:	27	AE	41	E4	64	9B	93	4C	A4	95	99	1B	78	52	B8 55
0000 01E0:	00	00	80	01	00	00	C0	00	00	00	00	01	12	91	14 00
0000 01F0:	00	00	80	00	80	C0	01	0E	5F	11	93	D1	40	40	00 40
fw-c.01.bin															
Version N+1	2D	2D	2D	2D	2D	2D	2D	2D	83	F5	EA	21	50	07	02 00
	22	40	AA	11	06	1E	36	95	33	75	83	5A	AB	C7	DF 50
	C6	C6	C9	D4	95	D3	88	B3	06	8C	4D	4C	19	0A	A8 AE
0000 0190:	A3	FB	37	3F	38	8A	11	01	ED	B2	CD	C7	DC	0C	17 4A
0000 01A0:	EB	26	72	95	77	FC	D3	4B	9C	90	60	99	2A	E0	FE B2
0000 01B0:	BC	0D	F9	5D	8B	17	8E	DB	D7	E6	C9	1F	00	00	00 00
0000 01C0:	E3	B0	C4	42	98	FC	1C	14	9A	FB	F4	C8	99	6F	B9 24
0000 01D0:	27	AE	41	E4	64	9B	93	4C	A4	95	99	1B	78	52	B8 55
0000 01E0:	30	00	00	00	18	00	00	00	20	00	00	00	02	40	22 92
0000 01F0:	10	00	00	00	C0	01	10	38	32	FA	2B	62	00	08	08 08
Arrow keys move F find RET next difference ESC quit T move top C ASCII/EBCDIC E edit file G goto position Q quit B move bottom															

HDR

FORMAT INCONNU

En-tête

fw-c.00.bin															
Version N	2D	2D	2D	2D	2D	2D	2D	2D	83	F5	EA	21	50	07	02 00
	22	40	AA	11	06	1E	36	95	33	75	83	5A	AB	C7	DF 50
	C6	C6	C9	D4	95	D3	88	B3	06	8C	4D	4C	19	0A	A8 AE
0000 0190:	A3	FB	37	3F	30	86	11	01	4D	8A	FE	BA	9D	3F	C3 25
0000 01A0:	21	27	43	87	4D	78	FF	41	BF	9B	0E	5C	E6	1A	E3 CB
0000 01B0:	D4	CB	94	DA	93	54	C7	26	D7	E6	C9	1F	00	00	00 00
0000 01C0:	E3	B0	C4	42	98	FC	1C	14	9A	FB	F4	C8	99	6F	B9 24
0000 01D0:	27	AE	41	E4	64	9B	93	4C	A4	95	99	1B	78	52	B8 55
0000 01E0:	00	00	80	01	00	00	C0	00	00	00	00	01	12	91	14 00
0000 01F0:	00	00	80	00	80	C0	01	0E	5F	11	93	D1	40	40	00 40
fw-c.01.bin															
Version N+1	2D	2D	2D	2D	2D	2D	2D	2D	83	F5	EA	21	50	07	02 00
	22	40	AA	11	06	1E	36	95	33	75	83	5A	AB	C7	DF 50
	C6	C6	C9	D4	95	D3	88	B3	06	8C	4D	4C	19	0A	A8 AE
0000 0190:	A3	FB	37	3F	38	8A	11	01	ED	B2	CD	C7	DC	0C	17 4A
0000 01A0:	EB	26	72	95	77	FC	D3	4B	9C	90	60	99	2A	E0	FE B2
0000 01B0:	BC	0D	F9	5D	8B	17	8E	DB	D7	E6	C9	1F	00	00	00 00
0000 01C0:	E3	B0	C4	42	98	FC	1C	14	9A	FB	F4	C8	99	6F	B9 24
0000 01D0:	27	AE	41	E4	64	9B	93	4C	A4	95	99	1B	78	52	B8 55
0000 01E0:	30	00	00	00	18	00	00	00	20	00	00	00	02	40	22 92
0000 01F0:	10	00	00	00	C0	01	10	38	32	FA	2B	62	00	08	08 08
Arrow keys move F find RET next difference ESC quit T move top C ASCII/EBCDIC E edit file G goto position Q quit B move bottom															

SHA256 Chunk #1 ?

SHA256 Chunk #2 ?

SHA256 Chunk #3 ?
(absent/vide)

HDR

FORMAT INCONNU

En-tête

fw-c.00.bin															
Version N	2D	2D	2D	2D	2D	2D	2D	2D	83	F5	EA	21	50	07	02 00
	22	40	AA	11	06	1E	36	95	33	75	83	5A	AB	C7	DF 50
	C6	C6	C9	D4	95	D3	88	B3	06	8C	4D	4C	19	0A	A8 AE
0000 0190:	A3	FB	37	3F	30	86	11	01	4D	8A	FE	BA	9D	3F	C3 25
0000 01A0:	21	27	43	87	4D	78	FF	41	BF	9B	0E	5C	E6	1A	E3 CB
0000 01B0:	D4	CB	94	DA	93	54	C7	26	D7	E6	C9	1F	00	00	00 00
0000 01C0:	E3	B0	C4	42	98	FC	1C	14	9A	FB	F4	C8	99	6F	B9 24
0000 01D0:	27	AE	41	E4	64	9B	93	4C	A4	95	99	1B	78	52	B8 55
0000 01E0:	00	00	80	01	00	00	C0	00	00	00	00	01	12	91	14 00
0000 01F0:	00	00	80	00	80	C0	01	0E	5F	11	93	D1	40	40	00 40
fw-c.01.bin															
Version N+1	2D	2D	2D	2D	2D	2D	2D	2D	83	F5	EA	21	50	07	02 00
	22	40	AA	11	06	1E	36	95	33	75	83	5A	AB	C7	DF 50
	C6	C6	C9	D4	95	D3	88	B3	06	8C	4D	4C	19	0A	A8 AE
0000 0190:	A3	FB	37	3F	38	8A	11	01	ED	B2	CD	C7	DC	0C	17 4A
0000 01A0:	EB	26	72	95	77	FC	D3	4B	9C	90	60	99	2A	E0	FE B2
0000 01B0:	BC	0D	F9	5D	8B	17	8E	DB	D7	E6	C9	1F	00	00	00 00
0000 01C0:	E3	B0	C4	42	98	FC	1C	14	9A	FB	F4	C8	99	6F	B9 24
0000 01D0:	27	AE	41	E4	64	9B	93	4C	A4	95	99	1B	78	52	B8 55
0000 01E0:	30	00	00	00	18	00	00	00	20	00	00	00	02	40	22 92
0000 01F0:	10	00	00	00	C0	01	10	38	32	FA	2B	62	00	08	08 08
Arrow keys move F find RET next difference ESC quit T move top C ASCII/EBCDIC E edit file G goto position Q quit B move bottom															
HDR				CHUNK #1				CHUNK #2				SIG			

SHA 256 dans l'en-tête

Model	Version	chunk #1 SHA256	chunk #2 SHA256
M3	a.01	302e7a968837c8e947a0838072e090cd31decdf43d214ce49159eb8c4e696749	7fa8e2f14f03dafb1b490e5e9433ecb403ae6c9d85afb1d04e126c3b2cc19b3d
M3	b.00	f8e7175e9468a32c93dd6fafd349ea2080b7a9eb5a355ac6688451139ccfb9a3	75860f5f64ac5c00bf821096515536ac6d2ee8a60fd883969fd277d3198abfb7
M3	b.01	f8e7175e9468a32c93dd6fafd349ea2080b7a9eb5a355ac6688451139ccfb9a3	0ece3c7b50c8970f96026e0109de951fba570700a42a48e1e4e45916de74f263
M3	b.02	f8e7175e9468a32c93dd6fafd349ea2080b7a9eb5a355ac6688451139ccfb9a3	7e812b3b993321b44c749e54d2c7ba25623b58c0921d6b095738cbe59ed13950
M3	c.00	2240aa11061e36953375835aabc7df50c6c6c9d495d388b3068c4d4c190aa8ae	4d8afeba9d3fc325212743874d78ff41bf9b0e5ce61ae3cbd4cb94da9354c726
M3	c.01	2240aa11061e36953375835aabc7df50c6c6c9d495d388b3068c4d4c190aa8ae	edb2cdc7dc0c174aeb26729577fcd34b9c9060992ae0feb2bc0df95d8b178edb
-			
M6	a.01	3ca0a9187f17d3d548ba59a6fe742eff2360b5329285056d6aec59d99e2e341f	f60c382ae3f88b7ddc8f39bd6240a2d17a47fef9ca42cac8002d4eef7f2f32dd
M6	b.00	2c084c2ca46b9df64a3ed9b8346f47020ce98e6b33895d5c0ea8865d1b92075d	3782f7fb4561b9522e59078857402976685883fb2dbe89f84b2eab7e15258581
M6	b.01	2c084c2ca46b9df64a3ed9b8346f47020ce98e6b33895d5c0ea8865d1b92075d	5dc6b540499e800d8ee2905c61486c82ae41cc3ceb7bccbbdec1e5fab24cfc10
M6	b.02	2c084c2ca46b9df64a3ed9b8346f47020ce98e6b33895d5c0ea8865d1b92075d	915b44a142fb73d7096274603f058cbf2087f48f257a2d9f6e752f009cf9009e
M6	c.00	31d0569f058654ef501820b978e55b3b7ef33fece1964d5ff6d992d48c627cf6	f32c8e97273f7b555e3a8f71c149ef90e4304408942cfc03004df6d0b20f3306
M6	c.01	31d0569f058654ef501820b978e55b3b7ef33fece1964d5ff6d992d48c627cf6	a317ae03851805d9e8cbe723d154b804bcb8bd956ab6ca88a8848574733807fa



SHA 256 dans l'en-tête

Model	Version	chunk #1 SHA256		
M3	a.01	302e7a968837c8e947a0838072e090cd31decdf43d214ce49159eb8c4e696749		7fa8e2f14f030
M3	b.00	f8e7175e9468a32c93dd6fafd349ea2080b7a9eb5a355ac6688451139ccfb9a3		75860f5f64ac5
M3	b.01	f8e7175e9468a32c93dd6fafd349ea2080b7a9eb5a355ac6688451139ccfb9a3		0ece3c7b50c89
M3	b.02	f8e7175e9468a32c93dd6fafd349ea2080b7a9eb5a355ac6688451139ccfb9a3		7e812b3b99332
M3	c.00	2240aa11061e36953375835aabc7df50c6c6c9d495d388b3068c4d4c190aa8ae		4d8afeba9d3f0
M3	c.01	2240aa11061e36953375835aabc7df50c6c6c9d495d388b3068c4d4c190aa8ae		edb2cdc7dc0c1
—				
M6	a.01	3ca0a9187f17d3d548ba59a6fe742eff2360b5329285056d6aec59d99e2e341f		f60c382ae3f88
M6	b.00	2c084c2ca46b9df64a3ed9b8346f47020ce98e6b33895d5c0ea8865d1b92075d		3782f7fb4561b
M6	b.01	2c084c2ca46b9df64a3ed9b8346f47020ce98e6b33895d5c0ea8865d1b92075d		5dc6b540499e8
M6	b.02	2c084c2ca46b9df64a3ed9b8346f47020ce98e6b33895d5c0ea8865d1b92075d		915b44a142fb7
M6	c.00	31d0569f058654ef501820b978e55b3b7ef33fece1964d5ff6d992d48c627cf6		f32c8e97273f7
M6	c.01	31d0569f058654ef501820b978e55b3b7ef33fece1964d5ff6d992d48c627cf6		a317ae0385180
HDR		CHUNK #1	CHUNK #2	SIG

SHA 256 dans l'en-tête

- Ne correspondent pas aux données réelles
 - donc on suppose qu'ils correspondent aux données en clair

1 jour écoulé



Chunk #1

Cryptanalyse



Chunk #1 : ce qui a échoué

- ❑ Recherche d'opcodes (multiples architectures)
- ❑ Recherche de motifs de conventions d'appel (push/pop)
- ❑ Fingerprinting de données (à la binwalk)
- ❑ *Reverse* du logiciel de mise à jour





Analyse du *chunk* #1

0000	0018:	32	FA	2B	62	00	08	08	08	00	00	00	00	00	00	00	00	2.+b....		
0000	0028:	00	10	00	40	00	08	00	00	5D	C4	17	08	00	A0	01	00	...@....	].....	
0000	0038:	00	40	2D	10	80	0B	80	00	01	A0	01	00	01	18	00	40	.@-.....	@	
0000	0048:	00	50	00	48	00	08	00	00	00	00	00	08	00	04	00	00	.P.H....		
0000	0058:	00	04	00	00	00	00	19	00	00	00	19	00	00	28	00	00		(.	
0000	0068:	00	00	00	08	00	08	00	00	00	00	80	0F	5D	04	80	07		]...	
0000	0078:	5D	04	80	07	00	80	9A	00	00	80	9A	00	00	38	00	00	].....	8..	
0000	0088:	00	00	00	08	00	08	00	00	00	00	80	17	5D	04	80	87		]...	
0000	0098:	5D	04	80	87	00	00	00	00	00	A0	1A	20	00	30	00	00	Version N		
0000	00A8:	00	00	00	08	00	00	00	00	00	00	00	00	00	00	00	00			
c1-11																				
0000	0018:	8C	FE	8A	98	00	02	02	02	00	00	00	00	00	00	00	00			
0000	0028:	00	04	00	10	00	02	00	00	17	F1	05	42	00	68	00	00		...B.h..	
0000	0038:	00	50	0B	04	E0	02	20	00	00	68	00	40	00	06	00	50	.P....	.h.@...P	
0000	0048:	00	14	00	12	00	02	00	00	00	00	00	02	00	01	00	00			
0000	0058:	00	01	00	00	00	40	06	00	00	40	06	00	00	0A	00	00	@..	@.....	
0000	0068:	00	00	00	02	00	02	00	00	00	00	E0	03	17	01	E0	41		A	
0000	0078:	17	01	E0	41	00	A0	26	00	00	A0	26	00	00	0E	00	00	...A..&	..&.....	
0000	0088:	00	00	00	02	00	02	00	00	00	00	E0	05	17	01	E0	61		a	
0000	0098:	17	01	E0	61	00	00	00	00	00	A8	06	08	00	0C	00	00	Version N+1		
0000	00A8:	00	00	00	02	00	00	00	00	00	00	00	00	00	00	00	00			
Arrow keys move F find RET next difference ESC quit T move top C ASCII/EBCDIC E edit file G goto position Q quit B move bottom																				

Format inconnu

Version c.00

HDR

CHUNK #1

CHUNK #2

SIG

Analyse du *chunk* #1

```

0000 0018: 32 FA 2B 62 00 08 08 08 00 00 00 00 00 00 00 00 2.+b....
0000 0028: 00 10 00 40 00 08 00 00 5D C4 17 08 00 A0 01 00 ...@... ].....
0000 0038: 00 40 2D 10 80 0B 80 00 01 A0 01 00 01 18 00 40 .@-..... @
0000 0048: 00 50 00 48 00 08 00 00 00 00 00 08 00 04 00 00 .P.H....
0000 0058: 00 04 00 00 00 00 19 00 00 00 19 00 00 28 00 00 ..... (..
0000 0068: 00 00 00 08 00 08 00 00 00 00 80 0F 5D 04 80 07 ..... ]...
0000 0078: 5D 04 80 07 00 80 9A 00 00 80 9A 00 00 38 00 00 ]..... 8..
0000 0088: 00 00 00 08 00 08 00 00 00 00 80 17 5D 04 80 87 ..... l...
0000 0098: 5D 04 80 87 00 00 00 00 00 A0 1A 20 00 30 00 00
0000 00A8: 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00
Version N

c1-11
0000 0018: 8C FF 8A 98 00 02 02 02 00 00 00 00 00 00 00 00 .....
0000 0028: 00 04 00 10 00 02 00 00 17 F1 05 42 00 68 00 00 ..... B.h..
0000 0038: 00 50 0B 04 E0 02 20 00 00 68 00 40 00 06 00 50 .P.... .h.@...P
0000 0048: 00 14 00 12 00 02 00 00 00 00 00 02 00 01 00 00 .....
0000 0058: 00 01 00 00 00 40 06 00 00 40 06 00 00 0A 00 00 .....@. .@.....
0000 0068: 00 00 00 02 00 02 00 00 00 00 E0 03 17 01 E0 41 ..... A
0000 0078: 17 01 E0 41 00 A0 26 00 00 A0 26 00 00 0E 00 00 ...A..& ..&....
0000 0088: 00 00 00 02 00 02 00 00 00 00 E0 05 17 01 E0 61 ..... a
0000 0098: 17 01 E0 61 00 00 00 00 00 A8 06 08 00 0C 00 00
0000 00A8: 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00
Version N+1

Arrow keys move F find RET next difference ESC quit T move top
C ASCII/EBCDIC E edit file G goto position Q quit B move bottom

```

Format inconnu

Version c.00

HDR

CHUNK #1

CHUNK #2

SIG

Analyse du *chunk* #1

0000	0018:	32 FA 2B 62	00 08 08 08	00 00 00 00 00 00 00 00	2.+b....		
0000	0028:	00 10 00 40	00 08 00 00	5D C4 17 08 00 A0 01 00	...@....]		
0000	0038:	00 40 2D 10	80 0B 80 00	01 A0 01 00 01 18 00 40	.@-.....@		
0000	0048:	00 50 00 48	00 08 00 00	00 00 00 08 00 04 00 00	.P.H....		
0000	0058:	00 04 00 00	00 00 19 00	00 00 19 00 00 28 00 00	(.		
0000	0068:	00 00 00 08	00 08 00 00	00 00 80 0F 5D 04 80 07	]...		
0000	0078:	5D 04 80 07	00 80 9A 00	00 80 9A 00 00 38 00 00	].....8..		
0000	0088:	00 00 00 08	00 08 00 00	00 00 80 17 5D 04 80 87	l...		
0000	0098:	5D 04 80 87	00 00 00 00	00 A0 1A 20 00 30 00 00			
0000	00A8:	00 00 00 08	00 00 00 00	00 00 00 00 00 00 00 00	Version N		
c1-11							
0000	0018:	8C FF 8A 98	00 02 02 02	00 00 00 00 00 00 00 00			
0000	0028:	00 04 00 10	00 02 00 00	17 F1 05 42 00 68 00 00	...B.h..		
0000	0038:	00 50 0B 04	E0 02 20 00	00 68 00 40 00 06 00 50	.P.... .h.@...P		
0000	0048:	00 14 00 12	00 02 00 00	00 00 00 02 00 01 00 00			
0000	0058:	00 01 00 00	00 40 06 00	00 40 06 00 00 0A 00 00	@..@.....		
0000	0068:	00 00 00 02	00 02 00 00	00 00 E0 03 17 01 E0 41	A		
0000	0078:	17 01 E0 41	00 A0 26 00	00 A0 26 00 00 0E 00 00	...A..&..&.....		
0000	0088:	00 00 00 02	00 02 00 00	00 00 E0 05 17 01 E0 61	a		
0000	0098:	17 01 E0 61	00 00 00 00	00 A8 06 08 00 0C 00 00			
0000	00A8:	00 00 00 02	00 00 00 00	00 00 00 00 00 00 00 00	Version N+1		
Arrow keys move F find RET next difference ESC quit T move top C ASCII/EBCDIC E edit file G goto position Q quit B move bottom							

Format inconnu

Version c.00

HDR

CHUNK #1

CHUNK #2

SIG

Analyse du *chunk* #1

0000	0018:	32 FA 2B 62	00 08 08 08	00 00 00 00 00 00 00 00	2.+b....
0000	0028:	00 10 00 40	00 08 00 00	5D C4 17 08 00 A0 01 00	...@....]
0000	0038:	00 40 2D 10	80 0B 80 00	01 A0 01 00 01 18 00 40	.@-.....@
0000	0048:	00 50 00 48	00 08 00 00	00 00 00 08 00 04 00 00	.P.H....
0000	0058:	00 04 00 00	00 00 19 00	00 00 19 00 00 28 00 00	(.
0000	0068:	00 00 00 08	00 08 00 00	00 00 80 0F 5D 04 80 07	]
0000	0078:	5D 04 80 07	00 80 9A 00	00 80 9A 00 00 38 00 00	].....8.
0000	0088:	00 00 00 08	00 08 00 00	00 00 80 17 5D 04 80 87	]
0000	0098:	5D 04 80 87	00 00 00 00	00 A0 1A 20 00 30 00 00	
0000	00A8:	00 00 00 08	00 00 00 00	00 00 00 00 00 00 00 00	Version N
c1-11					
0000	0018:	8C FF 8A 98	00 02 02 02	00 00 00 00 00 00 00 00	
0000	0028:	00 04 00 10	00 02 00 00	17 F1 05 42 00 68 00 00	...B.h.
0000	0038:	00 50 0B 04	E0 02 20 00	00 68 00 40 00 06 00 50	.P....h.@...P
0000	0048:	00 14 00 12	00 02 00 00	00 00 00 02 00 01 00 00	
0000	0058:	00 01 00 00	00 40 06 00	00 40 06 00 00 0A 00 00	@..@....
0000	0068:	00 00 00 02	00 02 00 00	00 00 E0 03 17 01 E0 41	A
0000	0078:	17 01 E0 41	00 A0 26 00	00 A0 26 00 00 0E 00 00	...A.&..&....
0000	0088:	00 00 00 02	00 02 00 00	00 00 E0 05 17 01 E0 61	a
0000	0098:	17 01 E0 61	00 00 00 00	00 A8 06 08 00 0C 00 00	
0000	00A8:	00 00 00 02	00 00 00 00	00 00 00 00 00 00 00 00	Version N+1
Arrow keys move F find RET next difference ESC quit T move top C ASCII/EBCDIC E edit file G goto position Q quit B move bottom					

Format inconnu

Version c.00

HDR

CHUNK #1

CHUNK #2

SIG

Analyse du *chunk* #1

0000	0018:	32 FA 2B 62	00 08 08 08	00 00 00 00 00 00 00 00	2.+b....
0000	0028:	00 10 00 40	00 08 00 00	5D C4 17 08 00 A0 01 00	...@....]
0000	0038:	00 40 2D 10	80 0B 80 00	01 A0 01 00 01 18 00 40	.@-.....@
0000	0048:	00 50 00 48	00 08 00 00	00 00 00 08 00 04 00 00	.P.H.....
0000	0058:	00 04 00 00	00 00 19 00	00 00 19 00 00 28 00 00	(.
0000	0068:	00 00 00 08	00 08 00 00	00 00 80 0F 5D 04 80 07	]...
0000	0078:	5D 04 80 07	00 80 9A 00	00 80 9A 00 00 38 00 00	].....8..
0000	0088:	00 00 00 08	00 08 00 00	00 00 80 17 5D 04 80 87	l...
0000	0098:	5D 04 80 87	00 00 00 00	00 A0 1A 20 00 30 00 00	
0000	00A8:	00 00 00 08	00 00 00 00	00 00 00 00 00 00 00 00	Version N
c1-11					
0000	0018:	8C FF 8A 98	00 02 02 02	00 00 00 00 00 00 00 00	
0000	0028:	00 04 00 10	00 02 00 00	17 F1 05 42 00 68 00 00	...B.h..
0000	0038:	00 50 0B 04	E0 02 20 00	00 68 00 40 00 06 00 50	.P.... .h.@...P
0000	0048:	00 14 00 12	00 02 00 00	00 00 00 02 00 01 00 00	
0000	0058:	00 01 00 00	00 40 06 00	00 40 06 00 00 0A 00 00	@..@.....
0000	0068:	00 00 00 02	00 02 00 00	00 00 E0 03 17 01 E0 41	A
0000	0078:	17 01 E0 41	00 A0 26 00	00 A0 26 00 00 0E 00 00	...A..&..&.....
0000	0088:	00 00 00 02	00 02 00 00	00 00 E0 05 17 01 E0 61	a
0000	0098:	17 01 E0 61	00 00 00 00	00 A8 06 08 00 0C 00 00	
0000	00A8:	00 00 00 02	00 00 00 00	00 00 00 00 00 00 00 00	Version N+1
Arrow keys move F find RET next difference ESC quit T move top C ASCII/EBCDIC E edit file G goto position Q quit B move bottom					

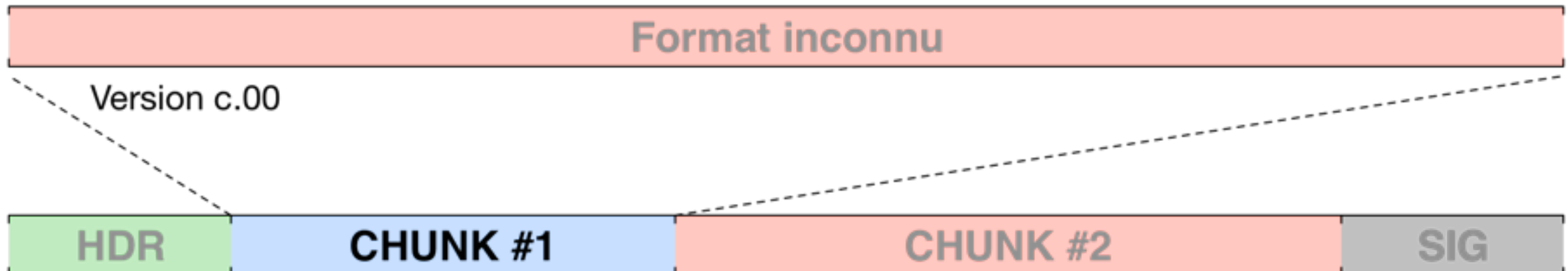
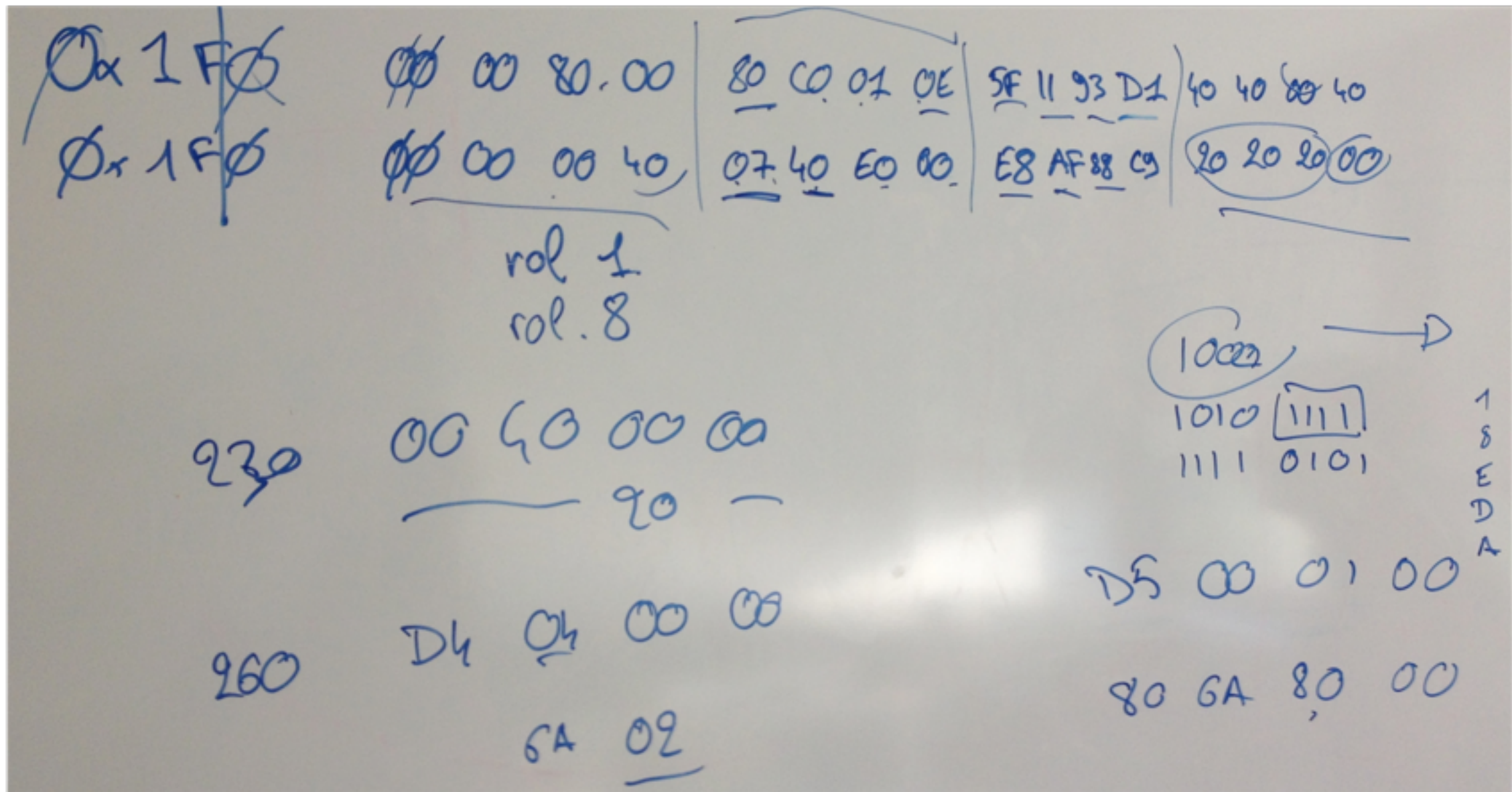
Format inconnu

Version c.00

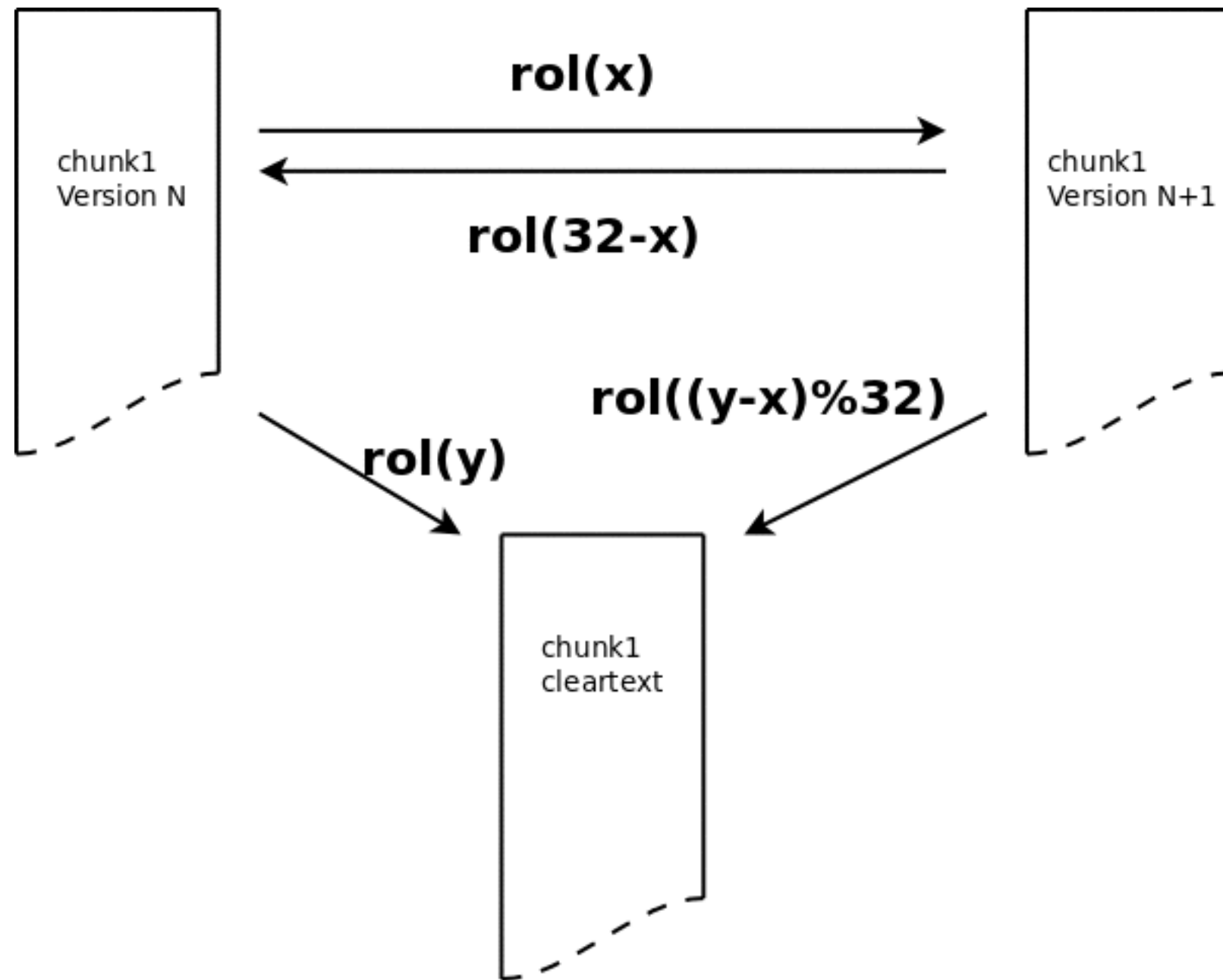


Fichier de mise à jour

Analyse du *chunk* #1



Chunk #1 : approche



Analyse du *chunk* #1

```
0000 0018: 32 FA 2B 62 00 08 08 08 00 00 00 00 00 00 00 00 2.+b....
0000 0028: 00 10 00 40 00 08 00 00 5D C4 17 08 00 A0 01 00 ...@....]....
0000 0038: 00 40 2D 10 80 0B 80 00 01 A0 01 00 01 18 00 40 .@-.....@
0000 0048: 00 50 00 48 00 08 00 00 00 00 00 08 00 04 00 00 .P.H.....
0000 0058: 00 04 00 00 00 00 19 00 00 00 19 00 00 28 00 00 .....(..
0000 0068: 00 00 00 08 00 08 00 00 00 00 80 0F 5D 04 80 07 .....]...
0000 0078: 5D 04 80 07 00 80 9A 00 00 80 9A 00 00 38 00 00 ].....8..
0000 0088: 00 00 00 08 00 08 00 00 00 00 80 17 5D 04 80 87 .....l...
0000 0098: 5D 04 80 87 00 00 00 00 00 A0 1A 20 00 30 00 00
0000 00A8: 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00
Version N
```

c1-11

```
0000 0018: 8C FE 8A 98 00 02 02 02 00 00 00 00 00 00 00 00 .....
0000 0028: 00 68 00 00 .....B.h..
0000 0038: 00 06 00 50 .P.... .h.@...P
0000 0048: 00 14 00 12 00 02 00 00 00 00 00 02 00 01 00 00 .....
0000 0058: 00 01 00 00 00 40 06 00 00 40 06 00 00 0A 00 00 .....@..@.....
0000 0068: 00 00 00 02 00 02 00 00 00 00 E0 03 17 01 E0 41 .....A
0000 0078: 17 01 E0 41 00 A0 26 00 00 A0 26 00 00 0E 00 00 ...A..&..&....
0000 0088: 00 00 00 02 00 02 00 00 00 00 E0 05 17 01 E0 61 .....a
0000 0098: 17 01 E0 61 00 00 00 00 00 A8 06 08 00 0C 00 00
0000 00A8: 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00
Version N+1
```

Arrow keys move F find RET next difference ESC quit T move top
C ASCII/EBCDIC E edit file G goto position Q quit B move bottom

Format inconnu

Version c.00



Analyse du *chunk* #1

```
0000 0018: 32 FA 2B 62 00 08 08 08 00 00 00 00 00 00 00 00 2.+b....
0000 0028: 00 10 00 40 00 08 00 00 5D C4 17 08 00 A0 01 00 ...@....]....
0000 0038: 00 40 2D 10 80 0B 80 00 01 A0 01 00 01 18 00 40 .@-.....@
0000 0048: 00 50 00 48 00 08 00 00 00 00 00 08 00 04 00 00 .P.H.....
0000 0058: 00 04 00 00 00 00 19 00 00 00 19 00 00 28 00 00 .....(..
0000 0068: 00 00 00 08 00 08 00 00 00 00 80 0F 5D 04 80 07 .....]...
0000 0078: 5D 04 80 07 00 80 9A 00 00 80 9A 00 00 38 00 00 ].....8..
0000 0088: 00 00 00 08 00 08 00 00 00 00 80 17 5D 04 80 87 .....l...
0000 0098: 5D 04 80 87 00 00 00 00 00 A0 1A 20 00 30 00 00
0000 00A8: 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00

c1-12
0000 0018: 19 FD 15 31 00 04 04 04 00 00 00 00 00 00 00 00 ...1....
ROL 11: 00000000 00000010 00000010 00000010 00 0C 00 A0 .....@.
ROL 12: 00000000 00000100 00000100 00000100 00 02 00 00 .....$.
0000 0068: 00 00 00 04 00 04 00 00 00 00 C0 07 2E 02 C0 83 .....@M..@M..
0000 0078: 2E 02 C0 83 00 40 4D 00 00 40 4D 00 00 1C 00 00 .....@M..@M..
0000 0088: 00 00 00 04 00 04 00 00 00 00 C0 0B 2E 02 C0 C3 .....
0000 0098: 2E 02 C0 C3 00 00 00 00 00 50 0D 10 00 18 00 00
0000 00A8: 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00

Version N
Version N+1

Arrow keys move F find RET next difference ESC quit T move top
C ASCII/EBCDIC E edit file G goto position Q quit B move bottom
```

Format inconnu

Version c.00



Fichier de mise à jour

Analyse du *chunk* #1

```
0000 0018: 32 FA 2B 62 00 08 08 08 00 00 00 00 00 00 00 00 2.+b....
0000 0028: 00 10 00 40 00 08 00 00 5D C4 17 08 00 A0 01 00 ...@....]....
0000 0038: 00 40 2D 10 80 0B 80 00 01 A0 01 00 01 18 00 40 .@-.....@
0000 0048: 00 50 00 48 00 08 00 00 00 00 00 08 00 04 00 00 .P.H....
0000 0058: 00 04 00 00 00 00 19 00 00 00 19 00 00 28 00 00 .....(..
0000 0068: 00 00 00 08 00 08 00 00 00 00 80 0F 5D 04 80 07 .....]...
0000 0078: 5D 04 80 07 00 80 9A 00 00 80 9A 00 00 38 00 00 ].....8..
0000 0088: 00 00 00 08 00 08 00 00 00 00 80 17 5D 04 80 87 .....]...
0000 0098: 5D 04 80 87 00 00 00 00 00 A0 1A 20 00 30 00 00
0000 00A8: 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00
```

Version N

c1-13

```
0000 0018: 32 FA 2B 62 00 08 08 08 00 00 00 00 00 00 00 00 2.+b....
0000 0028: 00 10 00 40 00 08 00 00 5D C4 17 08 00 A0 01 00 ...@....]....
0000 0038: 00 40 2D 10 80 0B 80 00 01 A0 01 00 01 18 00 40 .@-.....@
0000 0048: 00 50 00 48 00 08 00 00 00 00 00 08 00 04 00 00 .P.H....
0000 0058: 00 04 00 00 00 00 19 00 00 00 19 00 00 28 00 00 .....(..
0000 0068: 00 00 00 08 00 08 00 00 00 00 80 0F 5D 04 80 07 .....]...
0000 0078: 5D 04 80 07 00 80 9A 00 00 80 9A 00 00 38 00 00 ].....8..
0000 0088: 00 00 00 08 00 08 00 00 00 00 80 17 5D 04 80 87 .....]...
0000 0098: 5D 04 80 87 00 00 00 00 00 A0 1A 20 00 30 00 00
0000 00A8: 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00
```

ROL 11: 00000000 00000010 00000010 00000010

ROL 12: 00000000 00000100 00000100 00000100

ROL 13: 00000000 00001000 00001000 00001000

Version N+1

Arrow keys move F find RET next difference ESC quit T move top
C ASCII/EBCDIC E edit file G goto position Q quit B move bottom

Format inconnu

Version c.00

HDR

CHUNK #1

CHUNK #2

SIG

Analyse du *chunk* #1

```
0000 0018: 32 FA 2B 62 00 08 08 08 00 00 00 00 00 00 00 00 2.+b....
0000 0028: 00 10 00 40 00 08 00 00 5D C4 17 08 00 A0 01 00 ...@....]....
0000 0038: 00 40 2D 10 80 0B 80 00 01 A0 01 00 01 18 00 40 .@-.....@
0000 0048: 00 50 00 48 00 08 00 00 00 00 00 08 00 04 00 00 .P.H....
0000 0058: 00 04 00 00 00 00 19 00 00 00 19 00 00 28 00 00 .....(..
0000 0068: 00 00 00 08 00 08 00 00 00 00 80 0F 5D 04 80 07 .....]...
0000 0078: 5D 04 80 07 00 80 9A 00 00 80 9A 00 00 38 00 00 ].....8..
0000 0088: 00 00 00 08 00 08 00 00 00 00 80 17 5D 04 80 87 .....]...
0000 0098: 5D 04 80 87 00 00 00 00 00 A0 1A 20 00 30 00 00 .....]...
0000 00A8: 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00
```

Version N

c1-2

```
0000 0018: 7F 45 4C 46 01 01 01 00 00 00 00 00 00 00 00 00 .ELF....
0000 0028: 02 00 08 00 01 00 00 00 F8 02 A1 8B 34 00 00 00 .....4...
0000 0038: 03 00 28 00 .....p 4. ....(
0000 0048: 0A 00 09 00 01 00 00 00 00 00 01 00 00 00 00 00 .....
0000 0058: 05 00 00 00 .....
0000 0068: 00 F0 A0 8B .....
0000 0078: 07 00 00 00 ....P...P....
0000 0088: 00 F0 B0 8B .....
0000 0098: 00 F0 B0 8B 54 03 04 00 06 00 00 00 00 00 00 00
```

Version N+1

ROL 2: 000000001 000000001 000000001 000000000

ROL 11:

ROL 12:

ROL 13:

Arrow keys move F find RET next difference ESC quit T move top
C ASCII/EBCDIC E edit file G goto position Q quit B move bottom

Format inconnu

Version c.00

HDR

CHUNK #1

CHUNK #2

SIG

Analyse du *chunk* #1

```
0000 0018: 32 FA 2B 62 00 08 08 08 00 00 00 00 00 00 00 00 2.+b....
0000 0028: 00 10 00 40 00 08 00 00 5D C4 17 08 00 A0 01 00 ...@....]....
0000 0038: 00 40 2D 10 80 0B 80 00 01 A0 01 00 01 18 00 40 .@-.....@
0000 0048: 00 50 00 48 00 08 00 00 00 00 00 08 00 04 00 00 .P.H....
0000 0058: 00 04 00 00 00 00 19 00 00 00 19 00 00 28 00 00 .....(..
0000 0068: 00 00 00 08 00 08 00 00 00 00 80 0F 5D 04 80 07 .....]...
0000 0078: 5D 04 80 07 00 80 9A 00 00 80 9A 00 00 38 00 00 ].....8..
0000 0088: 00 00 00 08 00 08 00 00 00 00 80 17 5D 04 80 87 .....]...
0000 0098: 5D 04 80 87 00 00 00 00 00 A0 1A 20 00 30 00 00 .....]...
0000 00A8: 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00
```

Version N

c1-2

```
0000 0018: 7F 45 4C 46 01 01 01 00 00 00 00 00 00 00 00 00 .ELF....
0000 0028: 02 00 08 00 01 00 00 00 F8 02 A1 8B 34 00 00 00 .....4..
0000 0038: 03 00 28 00 .....p 4. ....
0000 0048: 0A 00 09 00 01 00 00 00 00 00 01 00 00 00 00 00 .....
0000 0058: 05 00 00 00 .....
0000 0068: 00 00 01 00 01 00 00 00 00 F0 A0 8B .....
0000 0078: 07 00 00 00 ....P...P....
0000 0088: 00 00 01 00 01 00 00 00 00 F0 B0 8B .....
0000 0098: 00 F0 B0 8B 54 03 04 00 06 00 00 00 00 00 00 00
```

Version N+1

ROL 11:

ROL 12:

ROL 13:

ROL 2: 000000001 000000001 000000001 000000000

Arrow keys move F find RET next difference ESC quit T move top
C ASCII/EBCDIC E edit file G goto position Q quit B move bottom

Format inconnu

Version c.00

HDR

CHUNK #1

CHUNK #2

SIG

2 jours écoulés

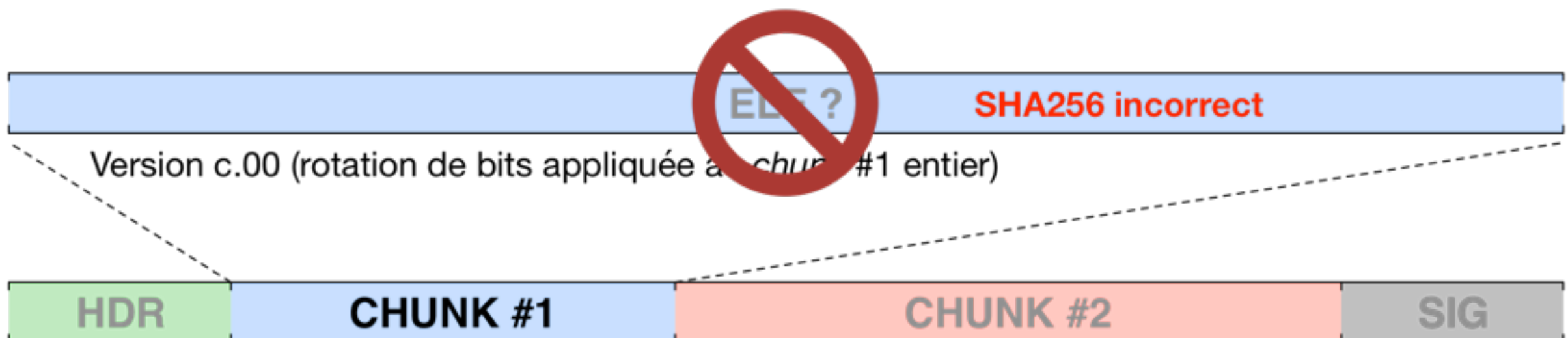


Analyse du *chunk* #1



Version c.00 (rotation de bits appliquée au *chunk* #1 entier)

Analyse du *chunk* #1



Analyse du *chunk* #1

Version c.01 (chunk 1 supposé identique)

ELF ?

ELF ?

Version c.00

**SHA256 incorrect, donc
comparaison avec d'autres versions**

ELF ?

Version c.00 (rotation de bits appliquée à *chunk* #1 entier)

HDR

CHUNK #1

CHUNK #2

SIG

Fichier de mise à jour

Analyse du *chunk* #1

fw-c.00.bin																	
0000	0018:	32	FA	2B	62	00	08	08	08	00	00	00	00	00	00	00	2.+b....
0000	0028:	00	10	00	40	00	08	00	00	5D	C4	17	08	00	A0	01	...@....].....
0000	0038:	00	40	2D	10	80	0B	80	00	01	A0	01	00	01	18	00	.@-..... @
0000	0048:	00	50	00	48	00	08	00	00	00	00	00	08	00	04	00	.P.H....
0000	0058:	00	04	00	00	00	00	19	00	00	00	19	00	00	28	00	 (..
0000	0068:	00	00	00	08	00	08	00	00	00	00	80	0F	5D	04	80	]...
0000	0078:	5D	04	80	07	00	80	9A	00	00	80	9A	00	00	38	00	]..... 8..
0000	0088:	00	00	00	08	00	08	00	00	00	00	80	17	5D	04	80	Version N
0000	0098:	5D	04	80	87	00	00	00	00	00	A0	1A	20	00	30	00	
0000	00A8:	00	00	00	08	00	00	00	00	00	00	00	00	00	00	00	
c1-13																	
0000	0018:	32	FA	2B	62	00	08	08	08	00	00	00	00	00	00	00	2.+b....
0000	0028:	00	10	00	40	00	08	00	00	5D	C4	17	08	00	A0	01	...@....].....
0000	0038:	00	40	2D	10	80	0B	80	00	01	A0	01	00	01	18	00	.@-..... @
0000	0048:	00	50	00	48	00	08	00	00	00	00	00	08	00	04	00	.P.H....
0000	0058:	00	04	00	00	00	00	19	00	00	00	19	00	00	28	00	 (..
0000	0068:	00	00	00	08	00	08	00	00	00	00	80	0F	5D	04	80	]...
0000	0078:	5D	04	80	07	00	80	9A	00	00	80	9A	00	00	38	00	]..... 8..
0000	0088:	00	00	00	08	00	08	00	00	00	00	80	17	5D	04	80	Version N+1
0000	0098:	5D	04	80	87	00	00	00	00	00	A0	1A	20	00	30	00	
0000	00A8:	00	00	00	08	00	00	00	00	00	00	00	00	00	00	00	
Arrow keys move F find RET next difference ESC quit T move top																	
C ASCII/EBCDIC E edit file G go position Q quit B move bottom																	

ELF ?

SHA256 incorrect

Version c.00 (rotation de bits appliquée à *chunk* #1 entier)

HDR

CHUNK #1

CHUNK #2

SIG

Analyse du *chunk* #1

fw-c.00.bin															
0001	0150:	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001	0160:	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001	0170:	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001	0180:	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001	0190:	00	00	00	00	00	00	00	00	00	20	88	01	00	00
0001	01A0:	F7	9E	20	FF	0A	F0	80	FF	D8	BE	A2	00	C4	BE
0001	01B0:	58	D1	50	0E	44	D1	40	0E	0A	F0	84	2E	CC	BE
0001	01C0:	C8	BE	62	00	4C	F0	3C	00	4B	91	10	F1	0B	F0
0001	01D0:	F8	BE	C2	00	DC	BE	B2	00	FC	BE	D2	00	D4	BE
0001	01E0:	D0	BE	82	00	C0	BE	42	00	78	90	04	00	5F	D1
c1-13															
0001	0150:	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001	0160:	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001	0170:	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001	0180:	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001	0190:	00	00	00	00	00	00	00	00	00	88	01	00	20	00
0001	01A0:	20	FF	F7	9E	80	FF	0A	F0	A2	00	D8	BE	52	00
0001	01B0:	50	0E	58	D1	40	0E	44	D1	84	2E	0A	F0	72	00
0001	01C0:	62	00	C8	BE	3C	00	4C	F0	10	F1	4B	91	00	FC
0001	01D0:	C2	00	F8	BE	B2	00	DC	BE	D2	00	FC	BE	92	00
0001	01E0:	82	00	D0	BE	42	00	C0	BE	04	00	78	90	00	FC
Version N															
Version N+1															
Arrow keys move F find RET next difference ESC quit T move top															
C ASCII/EBCDIC E edit file G go position Q quit B move bottom															

ELF ?

SHA256 incorrect

Version c.00 (rotation de bits appliquée à *chunk* #1 entier)

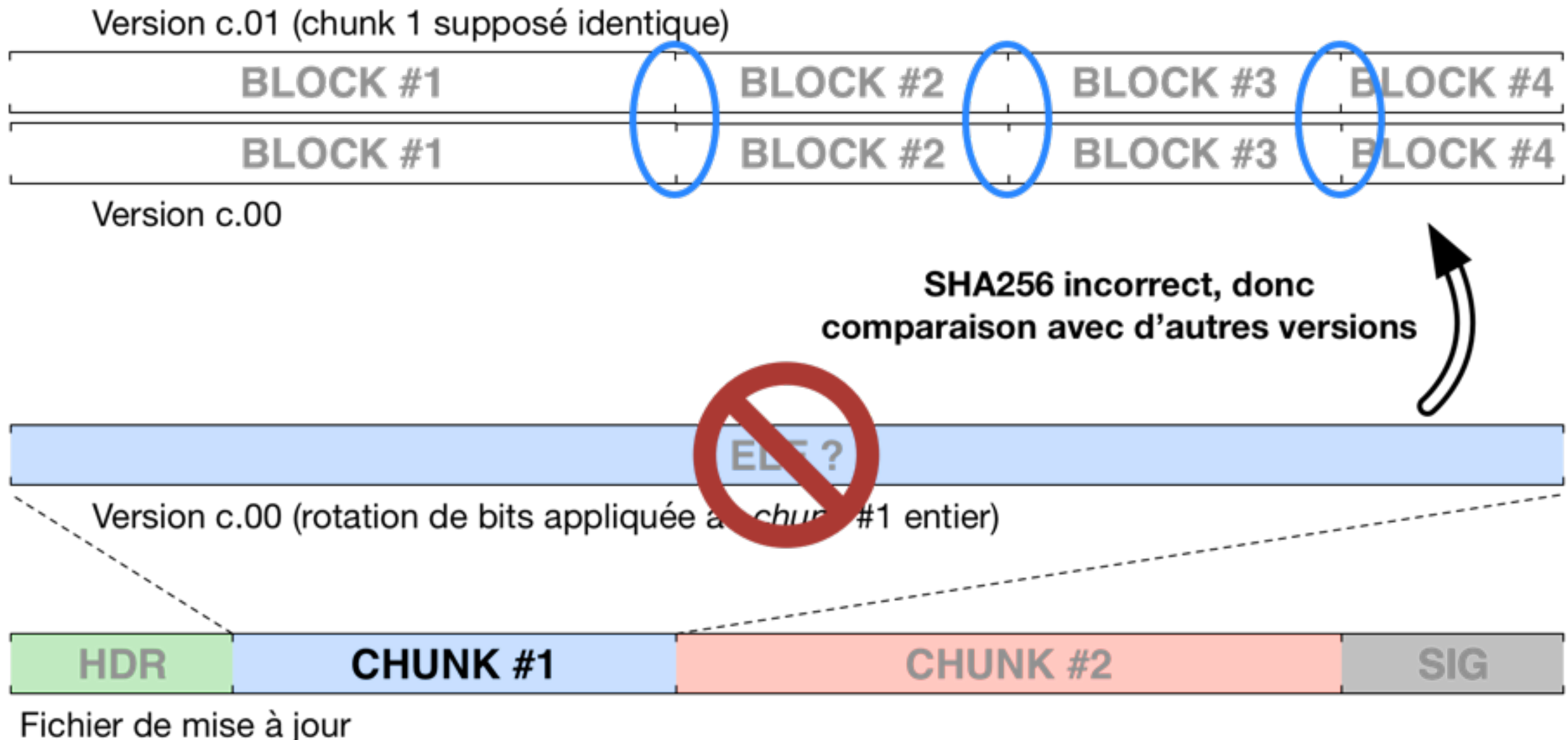
HDR

CHUNK #1

CHUNK #2

SIG

Analyse du *chunk* #1



Analyse du *chunk* #1

En-tête ELF

Strings GCC



Version c.00

Découverte de 3 changements
de distance de rotation de bits

Version c.01 (chunk 1 supposé identique)



Version c.00

SHA256 incorrect, donc
comparaison avec d'autres versions

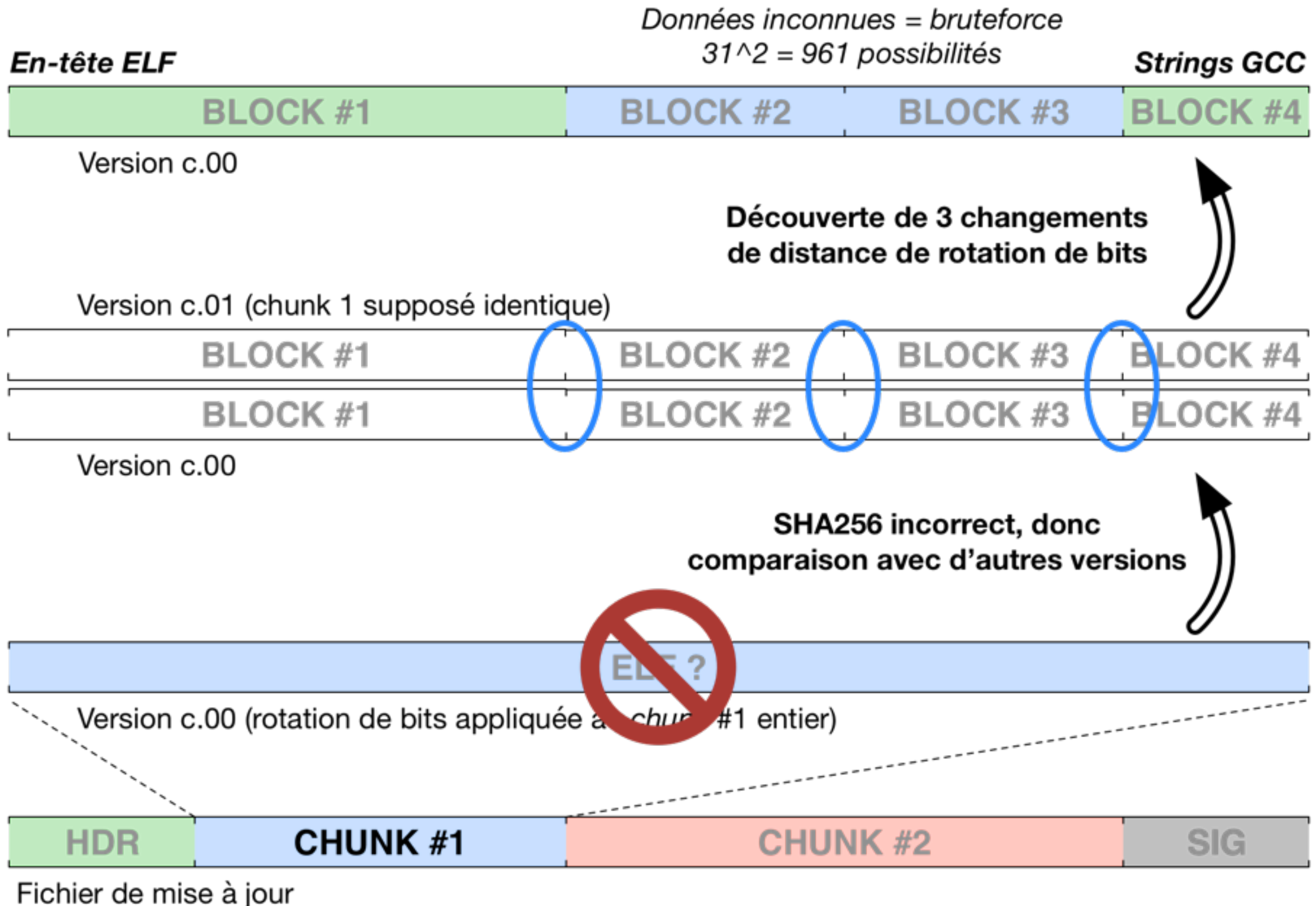


Version c.00 (rotation de bits appliquée à *chunk* #1 entier)

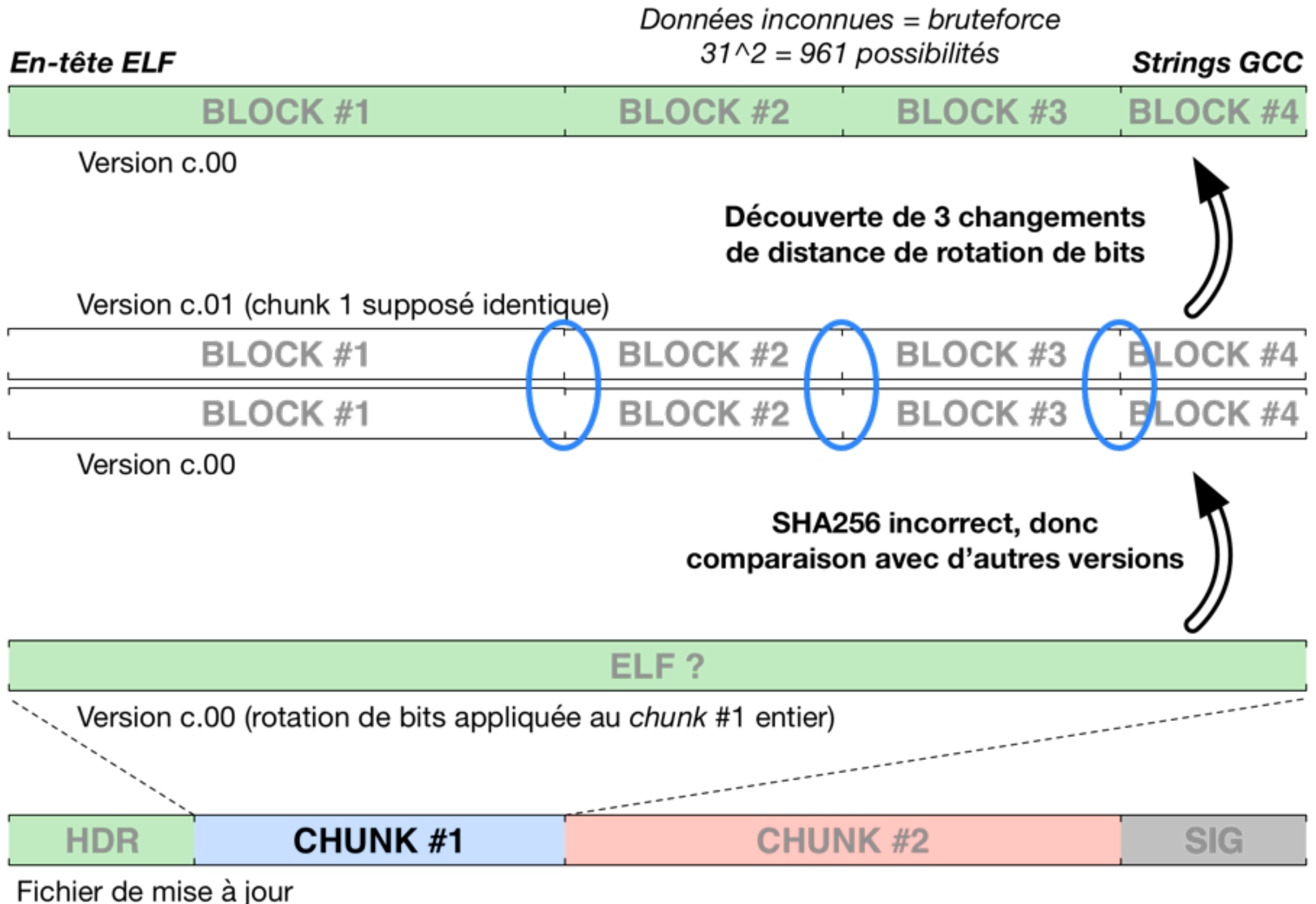


Fichier de mise à jour

Analyse du *chunk* #1



Analyse du *chunk* #1



2 semaines écoulées



Chunk #1 : conclusions

- Binaire ELF valide
- Architecture MIPS 32 bits
- Implémenté (retrouvé par *reverse-engineering*)
 - algorithme de décompression de la famille LZ
- *loader* ELF



Chunk #1 : conclusions

- 2 inconnues restantes
 - tailles de blocs
 - distance de rotation des bits pour chaque bloc



Chunk #2

Récupération



Chunk #2 : ce qui a échoué

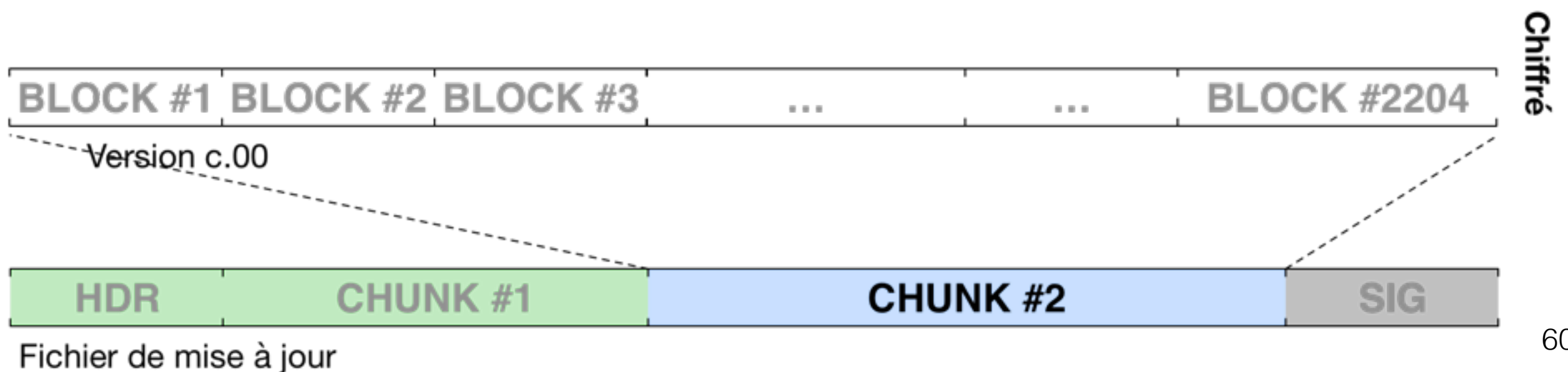
- ❑ Recherche de systèmes de fichiers existant
- ❑ Recherche de formats de stockage NAND
- ❑ Analyse statistique
- ❑ Brute-force



Analyse du *chunk* #2



Analyse du *chunk* #2



Idée

- Déchiffrer (ROL) puis décompresser (LZ)
- si la décompression progresse, c'est que l'on a bien déchiffré les blocs
- permet de valider les blocs déchiffrés les uns après les autres, linéairement



Algorithme de décompression

- Implémenté dans le chunk #1
- Appliqué sur le chunk #2
- ➔ Réimplémenté en Ruby puis en C (performances)
 - y compris les bugs découverts (c'est important)



Algorithme de compression

- Idée générale pour la décompression
 - se souvenir d'où se trouvent des motifs (octets) que l'on devra répéter



Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.	<html>	<
0x10BC	00	68	65	61	64	3E	0A	20	3C	.	head>.	<
0x10C5	00	6D	65	74	61	20	68	74	74	.	meta	htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.	p-equiv=	
0x10D7	00	27	63	6F	6E	74	65	6E	74	.	'content	
0x10E0	00	2D	74	79	70	65	27	20	63	.	-type'	c
0x10E9	10	6F	6E	74	03	3D	27	74	65	.	ont.='te	
0x10F2	20	78	74	05	3B	20	63	68	61	.	xt.; cha	
0x10FB	00	72	73	65	74	3D	55	54	46	.	rset=UTF	

0x11B94	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html>	<head>.	<
0x11BA4	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	76	3D	meta	http-equiv=	
0x11BB4	27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type'	c	
0x11BC4	6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	ontent='text/htm		
0x11BD4	6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l; charset=UTF		

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.<html> <
0x10BC	00	68	65	61	64	3E	0A	20	3C	.head>. <
0x10C5	00	6D	65	74	61	20	68	74	74	.meta htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.p-equiv=
0x10D7	00	27	63	6F	6E	74	65	6E	74	. 'content
0x10E0	00	2D	74	79	70	65	27	20	63	.-type' c
0x10E9	10	6F	6E	74	03	3D	27	74	65	.ont.='te
0x10F2	20	78	74	05	3B	20	63	68	61	.xt.; cha
0x10FB	00	72	73	65	74	3D	55	54	46	.rset=UTF

Groupes de 9 octets :

- **1 octet** de contrôle
- **8 octets** de données

0x11B94	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html> <head>. <
0x11BA4	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	76	3D	meta http-equiv=
0x11BB4	27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type' c
0x11BC4	6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	ontent='text/htm
0x11BD4	6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l; charset=UTF

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.<html> <
0x10BC	00	68	65	61	64	3E	0A	20	3C	.head>. <
0x10C5	00	6D	65	74	61	20	68	74	74	.meta htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.p-equiv=
0x10D7	00	27	63	6F	6E	74	65	6E	74	. 'content
0x10E0	00	2D	74	79	70	65	27	20	63	.-type' c
0x10E9	10	6F	6E	74	03	3D	27	74	65	.ont.='te
0x10F2	20	78	74	05	3B	20	63	68	61	.xt.; cha
0x10FB	00	72	73	65	74	3D	55	54	46	.rset=UTF

0x11B94	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html> <head>. <
0x11BA4	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	76	3D	meta http-equiv=
0x11BB4	27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type' c
0x11BC4	6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	ontent='text/htm
0x11BD4	6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l; charset=UTF

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.<html> <
0x10BC	00	68	65	61	64	3E	0A	20	3C	.head>. <
0x10C5	00	6D	65	74	61	20	68	74	74	.meta htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.p-equiv=
0x10D7	00	27	63	6F	6E	74	65	6E	74	. 'content
0x10E0	00	2D	74	79	70	65	27	20	63	.-type' c
0x10E9	10	6F	6E	74	03	3D	27	74	65	.ont.='te
0x10F2	20	78	74	05	3B	20	63	68	61	.xt.; cha
0x10FB	00	72	73	65	74	3D	55	54	46	.rset=UTF

0x11B94	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html> <head>. <
0x11BA4	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	76	3D	meta http-equiv=
0x11BB4	27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type' c
0x11BC4	6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	ontent='text/htm
0x11BD4	6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l; charset=UTF

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.<html> <
0x10BC	00	68	65	61	64	3E	0A	20	3C	.head>. <
0x10C5	00	6D	65	74	61	20	68	74	74	.meta htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.p-equiv=
0x10D7	00	27	63	6F	6E	74	65	6E	74	. 'content
0x10E0	00	2D	74	79	70	65	27	20	63	.-type' c
0x10E9	10	6F	6E	74	03	3D	27	74	65	.ont.='te
0x10F2	20	78	74	05	3B	20	63	68	61	.xt.; cha
0x10FB	00	72	73	65	74	3D	55	54	46	.rset=UTF

0x11B94	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html> <head>. <
0x11BA4	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	76	3D	meta http-equiv=
0x11BB4	27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type' c
0x11BC4	6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	ontent='text/htm
0x11BD4	6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l; charset=UTF

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.	<html>	<
0x10BC	00	68	65	61	64	3E	0A	20	3C	.	head>.	<
0x10C5	00	6D	65	74	61	20	68	74	74	.	meta	htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.	p-equiv=	
0x10D7	00	27	63	6F	6E	74	65	6E	74	.	'content	
0x10E0	00	2D	74	79	70	65	27	20	63	.	-type'	c
0x10E9	10	6F	6E	74	03	3D	27	74	65	.	ont.='te	
0x10F2	20	78	74	05	3B	20	63	68	61	.	xt.;	cha
0x10FB	00	72	73	65	74	3D	55	54	46	.	rset=UTF	

0x11B94	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html>	<head>.	<
0x11BA4	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	76	3D	meta	http-equiv=	
0x11BB4	27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type'	c	
0x11BC4	6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	content='text/htm		
0x11BD4	6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l; charset=UTF		

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.<html> <
0x10BC	00	68	65	61	64	3E	0A	20	3C	.head>. <
0x10C5	00	6D	65	74	61	20	68	74	74	.meta htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.p-equiv=
0x10D7	00	27	63	6F	6E	74	65	6E	74	. 'content
0x10E0	00	2D	74	79	70	65	27	20	63	.-type' c
0x10E9	10	6F	6E	74	03	3D	27	74	65	.ont.='te
0x10F2	20	78	74	05	3B	20	63	68	61	.xt.; cha
0x10FB	00	72	73	65	74	3D	55	54	46	.rset=UTF

index	pointeur
...	...
0x87BE	NULL
0x87BF	NULL
0x87C0	NULL
...	...

Calcul d'un HASH sur la base des
4 derniers octets décompressés

Utilisé comme **index** dans un tableau de
pointeurs

	HASH	
0x11B4	3C 68 74 6D 6C 3E 20 3C 68 65 61 64 3E 0A 20 3C	<html> <head>. <
0x11BA4	6D 65 74 61 20 68 74 74 70 2D 65 71 75 69 76 3D	meta http-equiv=
0x11BB4	27 63 6F 6E 74 65 6E 74 2D 74 79 70 65 27 20 63	'content-type' c
0x11BC4	6F 6E 74 65 6E 74 3D 27 74 65 78 74 2F 68 74 6D	ontent='text/htm
0x11BD4	6C 3B 20 63 68 61 72 73 65 74 3D 55 54 46	l; charset=UTF

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.<html> <
0x10BC	00	68	65	61	64	3E	0A	20	3C	.head>. <
0x10C5	00	6D	65	74	61	20	68	74	74	.meta htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.p-equiv=
0x10D7	00	27	63	6F	6E	74	65	6E	74	. 'content
0x10E0	00	2D	74	79	70	65	27	20	63	.-type' c
0x10E9	10	6F	6E	74	03	3D	27	74	65	.ont.='te
0x10F2	20	78	74	05	3B	20	63	68	61	.xt.; cha
0x10FB	00	72	73	65	74	3D	55	54	46	.rset=UTF

index	pointeur
...	...
0x87BE	NULL
0x87BF	0x11BB9
0x87C0	NULL
...	...

Le pointeur est renseigné pour indiquer la position suivante dans la sortie décompressée

Mémorisation de l'offset de 4 octets "vus"

	HASH	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html> <head>.
0x11BA4		6D	65	74	61	20	63	74	74	70	2D	65	71	75	69	76	3D	meta http-equiv=
0x11BB4		27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type' c
0x11BC4		6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	ontent='text/htm
0x11BD4		6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l; charset=UTF

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.<html> <
0x10BC	00	68	65	61	64	3E	0A	20	3C	.head>. <
0x10C5	00	6D	65	74	61	20	68	74	74	.meta htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.p-equiv=
0x10D7	00	27	63	6F	6E	74	65	6E	74	. 'content
0x10E0	00	2D	74	79	70	65	27	20	63	.-type' c
0x10E9	10	6F	6E	74	03	3D	27	74	65	.ont.='te
0x10F2	20	78	74	05	3B	20	63	68	61	.xt.; cha
0x10FB	00	72	73	65	74	3D	55	54	46	.rset=UTF

index	pointeur
...	...
0x87BE	NULL
0x87BF	0x11BB9
0x87C0	NULL
...	...

0x11B94	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html> <head>. <
0x11BA4	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	76	3D	meta http-equiv=
0x11BB4	27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type' c
0x11BC4	6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	ontent='text/htm
0x11BD4	6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l; charset=UTF

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C 68 74 6D 6C 3E 20 3C	.<html> <
0x10BC	00	68 65 61 64 3E 0A 20 3C	.head>. <
0x10C5	00	6D 65 74 61 20 68 74 74	.meta htt
0x10CE	00	70 2D 65 71 75 69 76 3D	.p-equiv=
0x10D7	00	27 63 6F 6E 74 65 6E 74	. 'content
0x10E0	00	2D 74 79 70 65 27 20 63	.-type' c
0x10E9	10	6F 6E 74 03 3D 27 74 65	.ont.='te
0x10F2	20	78 74 05 3B 20 63 68 61	.xt.; cha
0x10FB	00	72 73 65 74 3D 55 54 46	.rset=UTF

index	pointeur
...	...
0x87BE	NULL
0x87BF	0x11BB9
0x87C0	NULL
...	...

0x11B94	3C 68 74 6D 6C 3E 20 3C 68 65 61 64 3E 0A 20 3C	<html> <head>. <
0x11BA4	6D 65 74 61 20 68 74 74 70 2D 65 71 75 69 76 3D	meta http-equiv=
0x11BB4	27 63 6F 6E 74 65 6E 74 2D 74 79 70 65 27 20 63	'content-type' c
0x11BC4	6F 6E 74 65 6E 74 3D 27 74 65 78 74 2F 68 74 6D	ontent='text/htm
0x11BD4	6C 3B 20 63 68 61 72 73 65 74 3D 55 54 46	l; charset=UTF

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.<html> <
0x10BC	00	68	65	61	64	3E	0A	20	3C	.head>. <
0x10C5	00	6D	65	74	61	20	68	74	74	.meta htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.p-equiv=
0x10D7	00	27	63	6F	6E	74	65	6E	74	. 'content
0x10E0	00	2D	74	79	70	65	27	20	63	.-type' c
0x10E9	10	6F	6E	74	03	3D	27	74	65	.ont.='te
(bitfield) 10 = 0 0 0 1 0 0 0 0 0										.xt.; cha
										.rset=UTF

index	pointeur
...	...
0x87BE	NULL
0x87BF	0x11BB9
0x87C0	NULL
...	...

L'octet de contrôle est un bitfield :
- 0 : recopie telle quelle

0x11B94	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html> <head>. <
0x11BA4	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	76	3D	meta http-equiv=
0x11BB4	27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type' c
0x11BC4	6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	ontent='text/htm
0x11BD4	6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l; charset=UTF

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.<html> <
0x10BC	00	68	65	61	64	3E	0A	20	3C	.head>. <
0x10C5	00	6D	65	74	61	20	68	74	74	.meta htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.p-equiv=
0x10D7	00	27	63	6F	6E	74	65	6E	74	. 'content
0x10E0	00	2D	74	79	70	65	27	20	63	.-type' c
0x10E9	10	6F	6E	74	03	3D	27	74	65	.ont.='te

(bitfield) 10 = 0 0 0 1 0 0 0 0

index	pointeur
...	...
0x87BE	NULL
0x87BF	0x11BB9
0x87C0	NULL
...	...

L'octet de contrôle est un bitfield :

- 0 : recopie telle quelle

HASH IDENTIQUE

0x11B74	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html> <head>. <
0x11BA4	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	76	3D	meta http-equiv=
0x11BB4	27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type' c
0x11BC4	6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	ontent='text/htm
0x11BD4	6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l; charset=UTF

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.<html> <
0x10BC	00	68	65	61	64	3E	0A	20	3C	.head>. <
0x10C5	00	6D	65	74	61	20	68	74	74	.meta htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.p-equiv=
0x10D7	00	27	63	6F	6E	74	65	6E	74	. 'content
0x10E0	00	2D	74	79	70	65	27	20	63	.-type' c
0x10E9	10	6F	6E	74	03	3D	27	74	65	.ont.='te

(bitfield) 10	=	0	0	0	1	0	0	0	0
---------------	---	---	---	---	---	---	---	---	---

.xt.; cha
.rset=UTF

index	pointeur
...	...
0x87BE	NULL
0x87BF	0x11BB9
0x87C0	NULL
...	...

L'octet de contrôle est un bitfield :

- 0 : recopie telle quelle
- 1 : recopie X octets depuis le pointeur pour le HASH courant

HASH IDENTIQUE

0x11B74	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html> <head>. <
0x11BA4	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	76	3D	meta http-equiv=
0x11BB4	27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type' c
0x11BC4	6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	ontent='text/htm
0x11BD4	6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l; charset=UTF

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C 68 74 6D 6C 3E 20 3C	.<html> <
0x10BC	00	68 65 61 64 3E 0A 20 3C	.head>. <
0x10C5	00	6D 65 74 61 20 68 74 74	.meta htt
0x10CE	00	70 2D 65 71 75 69 76 3D	.p-equiv=
0x10D7	00	27 63 6F 6E 74 65 6E 74	. 'content
0x10E0	00	2D 74 79 70 65 27 20 63	.-type' c
0x10E9	10	6F 6E 74 03 3D 27 74 65	.ont.='te
	(bitfield) 10	= 0 0 0 1 0 0 0 0	.xt.; cha
			.rset=UTF

index	pointeur
...	...
0x87BE	NULL
0x87BF	0x11BB9
0x87C0	NULL
...	...

L'octet de contrôle est un bitfield :

- 0 : recopie telle quelle
- 1 : recopie **X octets** depuis le **pointeur** pour le **HASH courant**

HASH IDENTIQUE

0x11B94	3C 68 74 6D 6C 3E 20 3C	<html> <
0x11BA4	6D 65 74 61 20 68 74 74	<head>. <
0x11BB4	27 63 6F 6E 74 65 6E 74 2D 74 79 70 65 27 20 63	.meta http-equiv=
0x11BC4	6F 6E 74 65 6E 74 3D 27 74 65 78 74 2F 68 74 6D	'content-type' c
0x11BD4	6C 3B 20 63 68 61 72 73 65 74 3D 55 54 46	ontent='text/htm
		l; charset=UTF

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.<html> <
0x10BC	00	68	65	61	64	3E	0A	20	3C	.head>. <
0x10C5	00	6D	65	74	61	20	68	74	74	.meta htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.p-equiv=
0x10D7	00	27	63	6F	6E	74	65	6E	74	. 'content
0x10E0	00	2D	74	79	70	65	27	20	63	.-type' c
0x10E9	10	6F	6E	74	03	3D	27	74	65	.ont.='te

(bitfield) 10 = 0 0 0 1 0 0 0 0

index	pointeur
...	...
0x87BE	NULL
0x87BF	0x11BB9
0x87C0	NULL
...	...

L'octet de contrôle est un bitfield :

- 0 : recopie telle quelle
- 1 : recopie **X octets** depuis le **pointeur** pour le **HASH courant**

0x11B94	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html> <head>. <
0x11BA4	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	76	3D	meta http-equiv=
0x11BB4	27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type' c
0x11BC4	6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	ontent='text/htm
0x11BD4	6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l; charset=UTF

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.<html> <
0x10BC	00	68	65	61	64	3E	0A	20	3C	.head>. <
0x10C5	00	6D	65	74	61	20	68	74	74	.meta htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.p-equiv=
0x10D7	00	27	63	6F	6E	74	65	6E	74	. 'content
0x10E0	00	2D	74	79	70	65	27	20	63	.-type' c
0x10E9	10	6F	6E	74	03	3D	27	74	65	.ont.='te
(bitfield) 10 = 0 0 0 1 0 0 0 0 0										
										.xt.; cha
										.rset=UTF

index	pointeur
...	...
0x87BE	NULL
0x87BF	0x11BB9
0x87C0	NULL
...	...

L'octet de contrôle est un bitfield :

- 0 : recopie telle quelle
- 1 : recopie **X octets** depuis le **pointeur** pour le **HASH courant**

0x11B94	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html> <head>.
0x11BA4	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	76	3D	<meta http-equiv=
0x11BB4	27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type' c
0x11BC4	6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	content='text/htm
0x11BD4	6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l; charset=UTF

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.	<html>	<
0x10BC	00	68	65	61	64	3E	0A	20	3C	.	head>.	<
0x10C5	00	6D	65	74	61	20	68	74	74	.	meta	htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.	p-equiv=	
0x10D7	00	27	63	6F	6E	74	65	6E	74	.	'content	
0x10E0	00	2D	74	79	70	65	27	20	63	.	-type'	c
(corruption)	6F	6E	74	10	03	3D	27	74	65	.	ont.=	'te
0x10F2	20	78	74	05	3B	20	63	68	61	.	xt.;	cha
0x10FB	00	72	73	65	74	3D	55	54	46	.	rset=UTF	

index	pointeur
...	...
0x87BE	NULL
0x87BF	0x11BB9
0x87C0	NULL
...	...

0x11B94	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html>	<head>.	<
0x11BA4	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	76	3D	meta	http-equiv=	
0x11BB4	27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type'	c	
0x11BC4	6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	ontent=	'text/htm	
0x11BD4	6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l;	charset=UTF	

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.<html> <
0x10BC	00	68	65	61	64	3E	0A	20	3C	.head>. <
0x10C5	00	6D	65	74	61	20	68	74	74	.meta htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.p-equiv=
0x10D7	00	27	63	6F	6E	74	65	6E	74	. 'content
0x10E0	00	2D	74	79	70	65	27	20	63	.-type' c
(corruption)	6F	6E	74	10	03	3D	27	74	65	.ont.='te
(bitfield)	6F	=	0	1	1	0	1	1	1	.xt.; cha
										.rset=UTF

index	pointeur
...	...
0x87BE	NULL
0x87BF	0x11BB9
0x87C0	NULL
...	...

0x11B94	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html> <head>. <
0x11BA4	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	76	3D	meta http-equiv=
0x11BB4	27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type' c
0x11BC4	6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	ontent='text/htm
0x11BD4	6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l; charset=UTF

Sortie décompressée

Fichier d'entrée compressé

0x10B3	00	3C	68	74	6D	6C	3E	20	3C	.	<html>	<
0x10BC	00	68	65	61	64	3E	0A	20	3C	.	head>.	<
0x10C5	00	6D	65	74	61	20	68	74	74	.	meta	htt
0x10CE	00	70	2D	65	71	75	69	76	3D	.	p-equiv=	
0x10D7	00	27	63	6F	6E	74	65	6E	74	.	'content	
0x10E0	00	2D	74	79	70	65	27	20	63	.	-type'	c
(corruption)	6F	6E	74	10	03	3D	27	74	65	.	ont.=	'te
(bitfield)	6F	=	0	1	1	0	1	1	1	.	xt.;	cha
										.	rset=	UTF

index	pointeur
...	...
0x87BE	NULL
0x87BF	0x11BB9
0x87C0	NULL
...	...

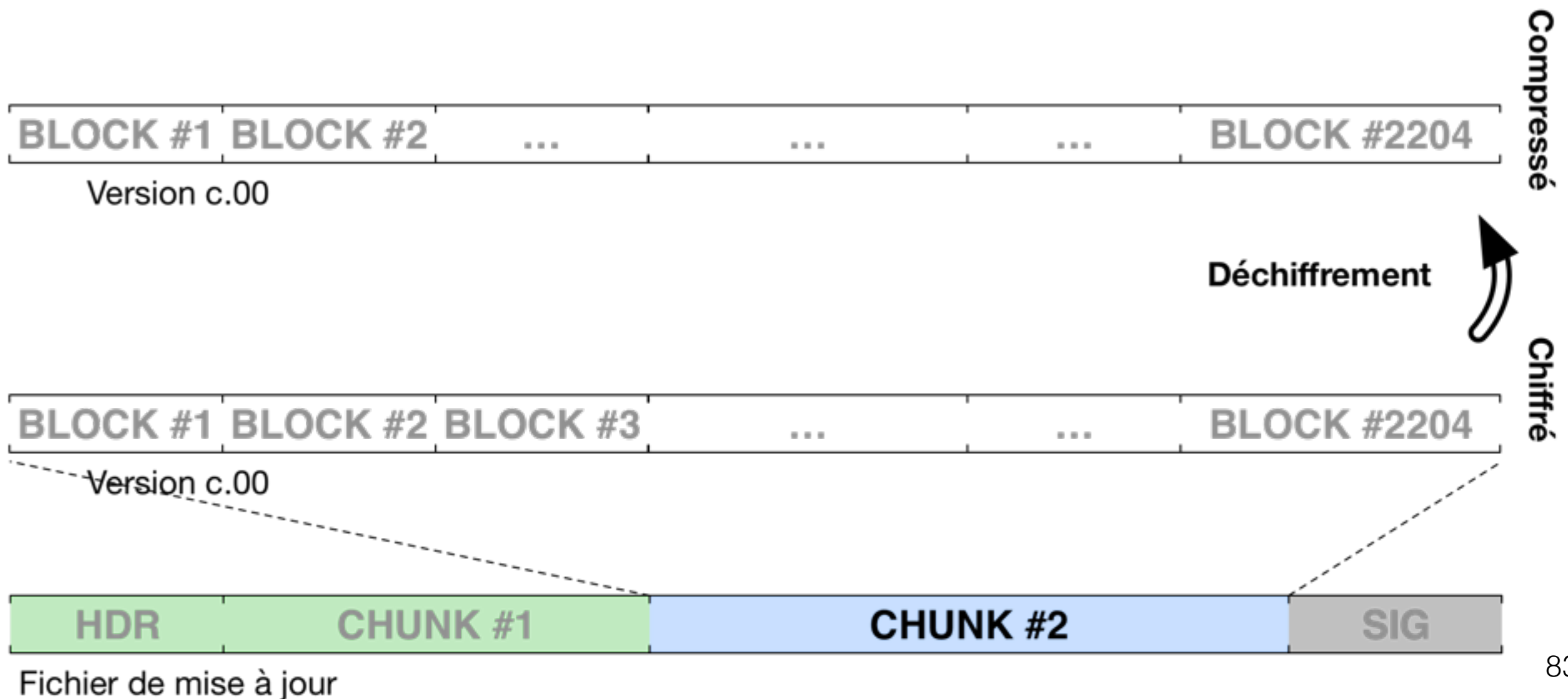
En cas de corruption des données :
HASH indiquant un pointeur NULL
= crash de l'implémentation (chunk #1)

Exploitable pour détecter les bornes de blocs dans le chiffré

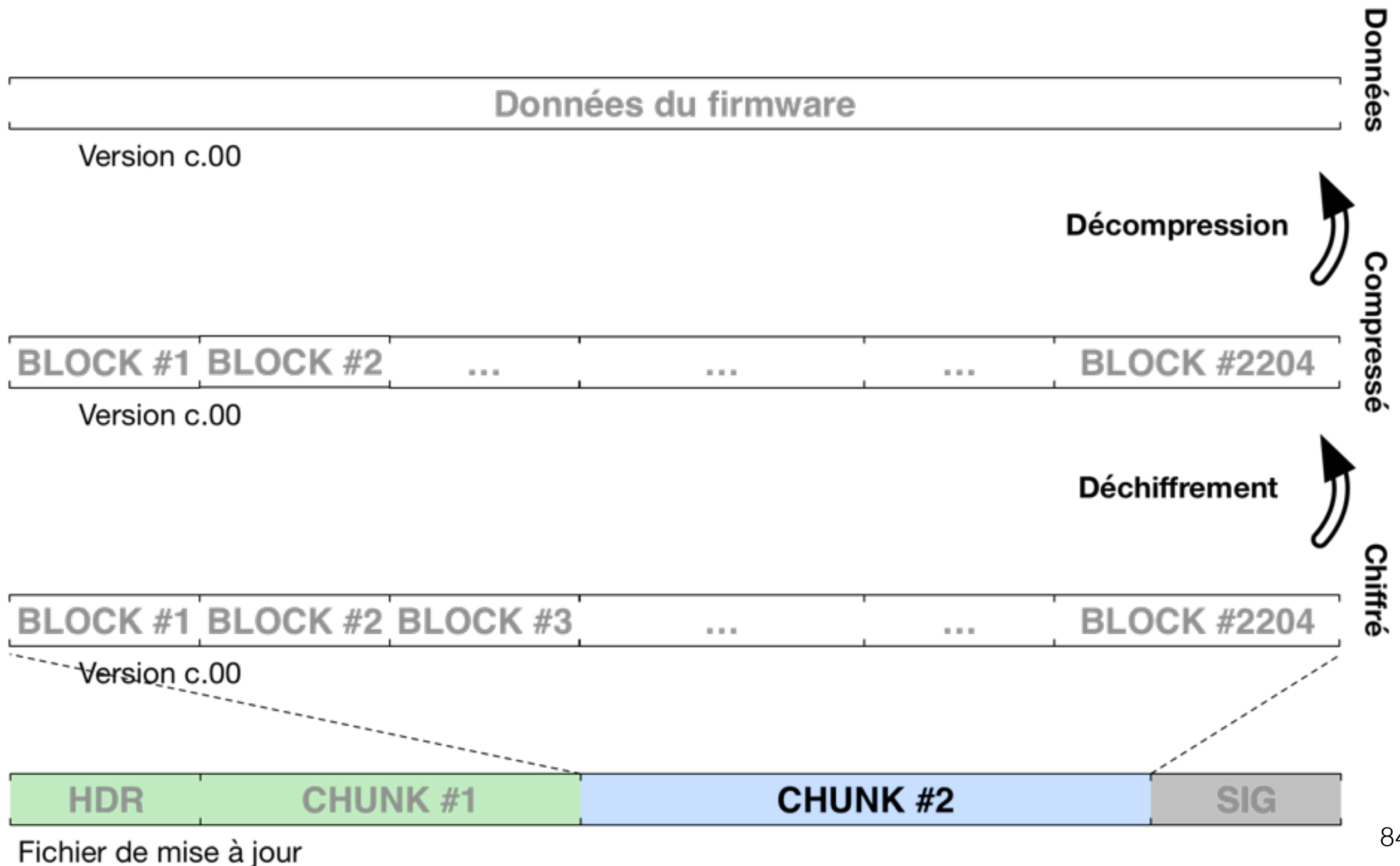
0x11B94	3C	68	74	6D	6C	3E	20	3C	68	65	61	64	3E	0A	20	3C	<html>	<head>.	<
0x11BA4	6D	65	74	61	20	68	74	74	70	2D	65	71	75	69	76	3D	meta	http-equiv=	
0x11BB4	27	63	6F	6E	74	65	6E	74	2D	74	79	70	65	27	20	63	'content-type'	c	
0x11BC4	6F	6E	74	65	6E	74	3D	27	74	65	78	74	2F	68	74	6D	ontent='text/htm		
0x11BD4	6C	3B	20	63	68	61	72	73	65	74	3D	55	54	46			l; charset=	UTF	

Sortie décompressée

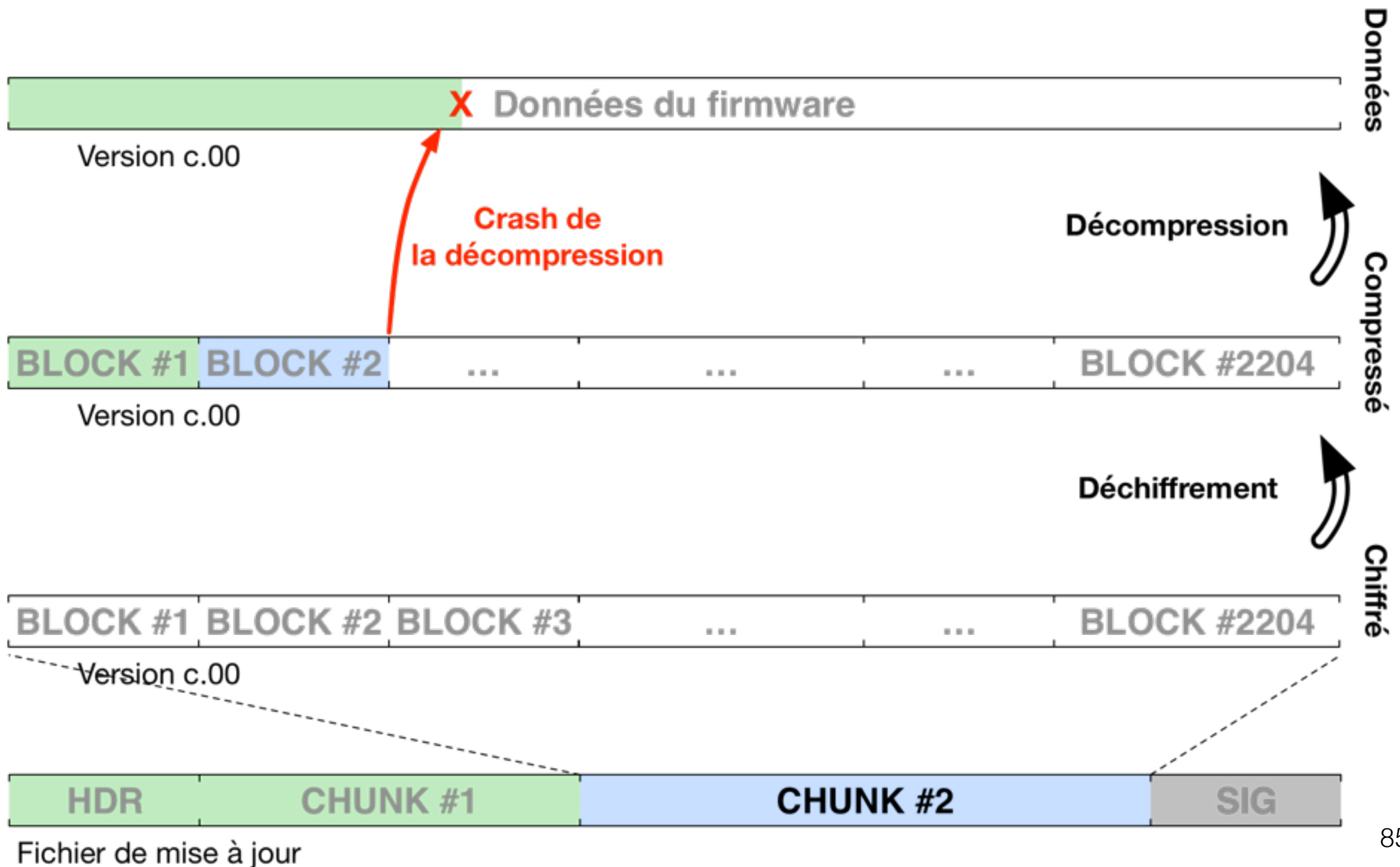
Analyse du *chunk* #2



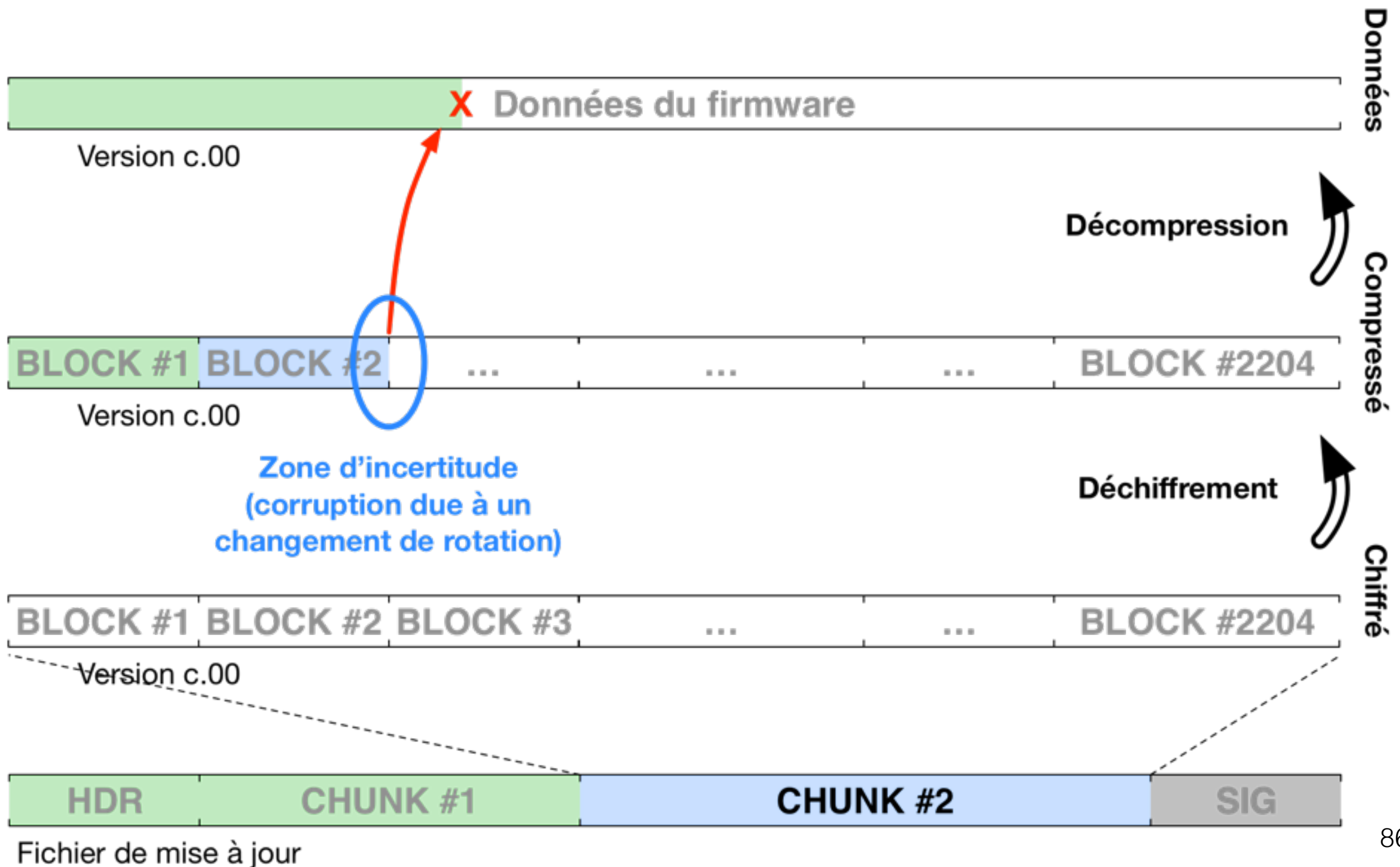
Analyse du *chunk* #2



Analyse du *chunk* #2



Analyse du *chunk* #2



Outil automatisé

```
[ - ] Declared block #001: shift=21 start: 0x00000000
[ + ] FW UPD size: XXXXXXXX (XXXXXXXX bytes)
[ + ] Chunk 1 size: 0x00020750 (132944 bytes)
[ + ] Chunk 2 size: 0x01118630 (17925680 bytes)
[ + ] SHA256 Hash #1: 2240aa11061e36953375835aabc7df50c6c6c9d495d388b3068c4d4c190aa8ae
[ + ] SHA256 Hash #2: 4d8afeba9d3fc325212743874d78ff41bf9b0e5ce61ae3cbd4cb94da9354c726
[ + ] SHA256 Hash #3: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
[ + ] Performed ROT13 on Build string
[ - ] Allocating and rotating 32 chunk2 buffers [....5....10....15....20....25....30...] done
[ - ] RAW Data:
    20930  00 00 00 06 00 00 00 03 00 00 00 04 48 44 52 00  .....HDR.
    20940  00 00 00 06 00 00 00 08 80 80 00 00 02 7e 6f f8  .....~O.
    20950  00 00 00 08 01 06 00 fc 01 06 00 fa 02 7e 6f f4  .....~O.
    20960  01 00 7f 45 4c 46 00 01 01 01 00 00 00 00 00 80  ...ELF.....
[ - ]   explore(): Step 0: guard
[ - ]   explore(): Step 1: find crash offset...
[ - ]   explore(): Step 2-5: find next shift
[ - ]   explore(): Step 6: generate candidates
[ - ]   explore(): Step 7: run stage2 on candidate boundaries
[ - ]   explore(): Step 8: discard candidates below threshold
[ - ]   explore(): found candidates:
[ + ]   | - 0x00001BA0    shift: 19    pos: 0x00005126    [depth: 1]
[ + ]   | - 0x00001B9C    shift: 19    pos: 0x00005126    [depth: 1]
[ + ]   | - 0x00001B94    shift: 19    pos: 0x00005126    [depth: 1]
[ + ]   | - 0x00001B90    shift: 19    pos: 0x00005126    [depth: 1]
[ - ]   explore(): Step 9: recurse into valid candidates
[ - ]       explore(): Step 0: guard
[ - ]       explore(): Step 1: find crash offset... 0x00005126
```



Liste cyclique des paramètres de rotation

Version n		Version n+1																														
Block offset	Bit rotation (rol)	21	19	6	9	15	29	10	26	5	11	14	23	3	31	22	1	18	27	7	25	30	17	13	2	21	19	6	9	15	29	10
		0x00000000	0x00001BA0	0x00005120	0x00006468	0x0000918C	0x0000C850	0x0000F7A0	0x00010E60	0x00013FAC	0x00014AE8	0x00018784	0x00018B50	0x00018F80	0x000193F4	0x0001B864	0x0001BAC4	0x0001EAEC	0x0001FA08	0x00022EE0	0x00026A58	0x00027610	0x00028E94	0x0002B040	0x0002CA78	0x00030800	0x00032FD4	0x00033650	0x00034AC0	0x00036C30	0x00036E54	
		0x00000000	0x00000080	0x000030A0	0x00004BCC	0x00007974	0x0000B858	0x0000D04C	0x0000D9A4	0x00010228	0x000114E0	0x00014A10	0x00016D64	0x00018F94	0x000191AC	0x00019DC4	0x0001C294	0x0001F100	0x00020FFC	0x000231C4	0x00023400	0x00024420	0x00027528	0x00029C34	0x0002DA9C	0x0002FE8C	0x00030C98	0x00031964	0x00035638	0x00039214	0x0003B9B0	
		19	6	9	15	29	10	26	5	11	14	23	3	31	22	1	18	27	7	25	30	17	13	2	21	19	6	9	15	29	10	
		21	19	6	9	15	29	10	26	5	11	14	23	3	31	22	1	18	27	7	25	30	17	13	2	21	19	6	9	15	29	10
		0x00000000	0x00001BA0	0x00005120	0x00006468	0x0000918C	0x0000C850	0x0000F7A0	0x00010E60	0x00013FAC	0x00014AE8	0x00018784	0x00018B50	0x00018F80	0x000193F4	0x0001B864	0x0001BAC4	0x0001EAEC	0x0001FA08	0x00022EE0	0x00026A58	0x00027610	0x00028E94	0x0002B040	0x0002CA78	0x00030800	0x00032FD4	0x00033650	0x00034AC0	0x00036C30	0x00036E54	
		0x00000000	0x00000080	0x000030A0	0x00004BCC	0x00007974	0x0000B858	0x0000D04C	0x0000D9A4	0x00010228	0x000114E0	0x00014A10	0x00016D64	0x00018F94	0x000191AC	0x00019DC4	0x0001C294	0x0001F100	0x00020FFC	0x000231C4	0x00023400	0x00024420	0x00027528	0x00029C34	0x0002DA9C	0x0002FE8C	0x00030C98	0x00031964	0x00035638	0x00039214	0x0003B9B0	



Fichier d'entrée compressé

0x10B3	00	3C 68 74 6D 6C 3E 20 3C	.<html> <
0x10BC	00	68 65 61 64 3E 0A 20 3C	.head>. <
0x10C5	00	6D 65 74 61 20 68 74 74	.meta htt
0x10CE	00	70 2D 65 71 75 69 76 3D	.p-equiv=
0x10D7	00	27 63 6F 6E 74 65 6E 74	. 'content
0x10E0	00	2D 74 79 70 65 27 20 63	.-type' c
0x10E9	10	6F 6E 74 03 3D 27 74 65	.ont.='te
0x10F2	20	78 74 05 3B 20 63 68 61	.xt.; cha
0x10FB	00	72 73 65 74 3D 55 54 46	.rset=UTF

index	pointeur
...	...
0x87BE	NULL
0x87BF	0x11BB9
0x87C0	NULL
...	...

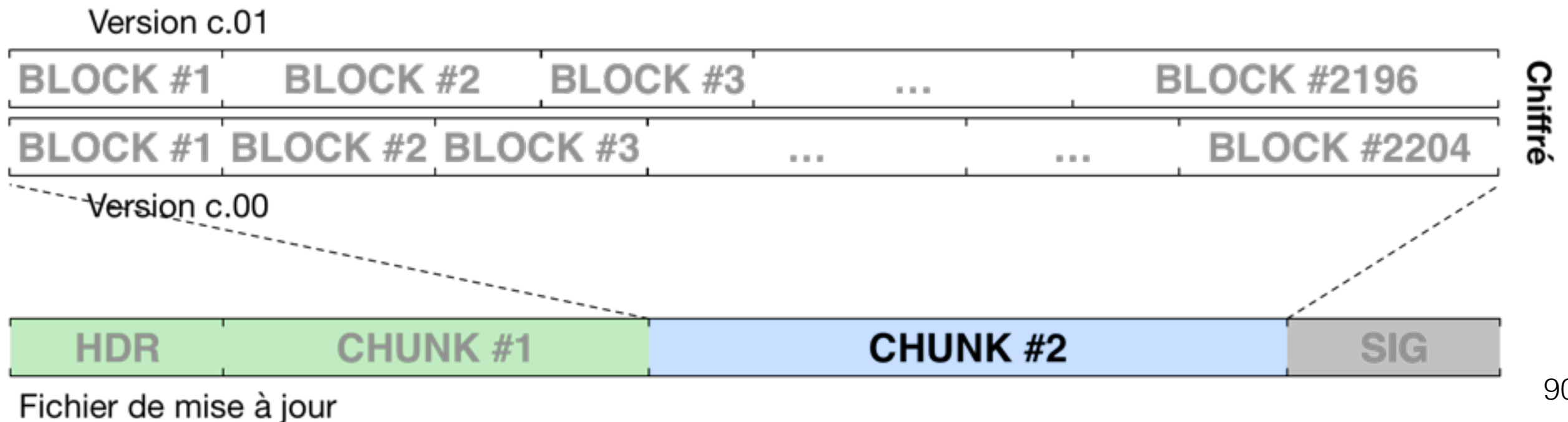
Plus on avance dans la décompression,
plus le tableau de pointeurs se remplit

Problème :
la décompression plante de moins en moins

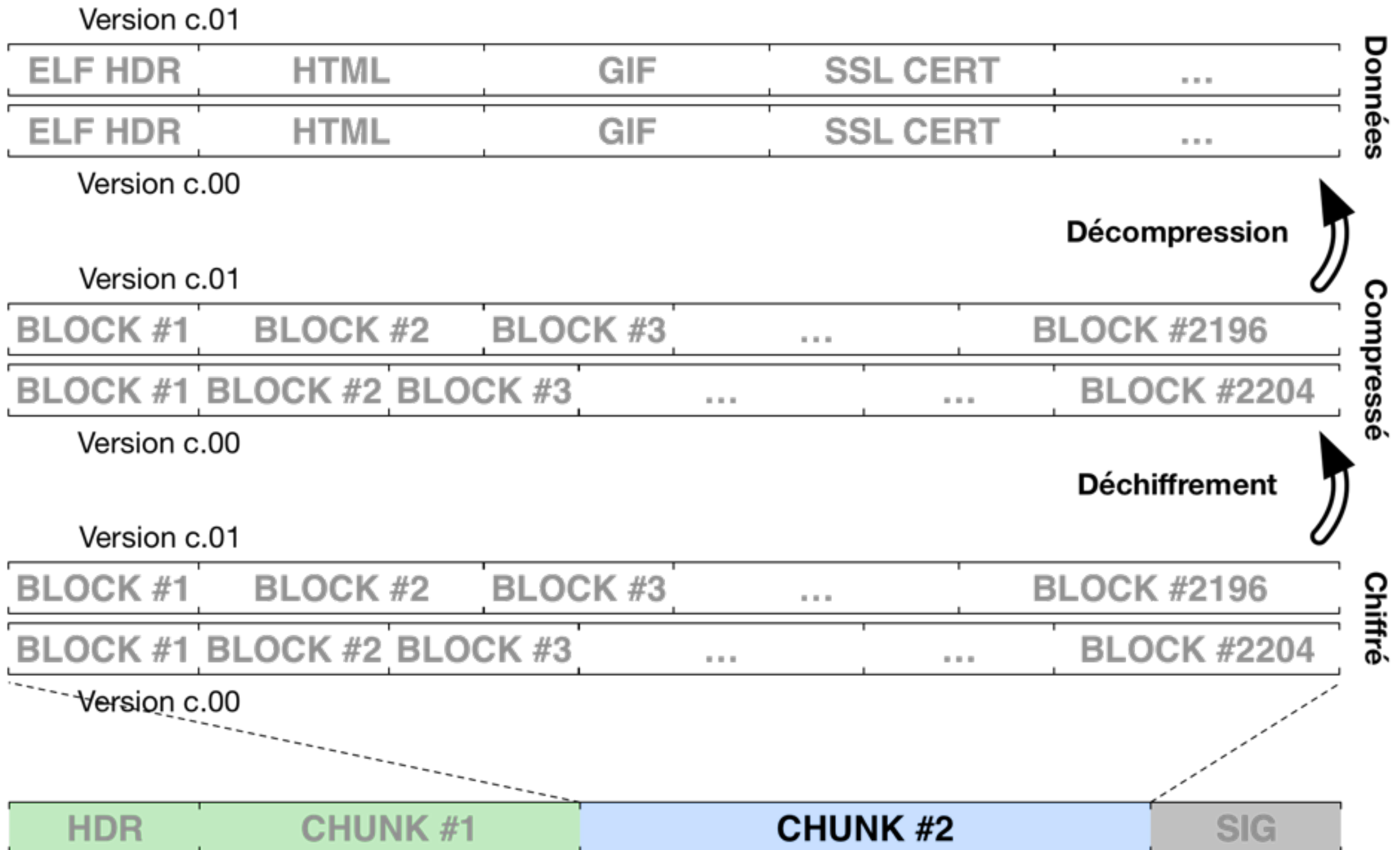
0x11B94	3C 68 74 6D 6C 3E 20 3C 68 65 61 64 3E 0A 20 3C	<html> <head>. <
0x11BA4	6D 65 74 61 20 68 74 74 70 2D 65 71 75 69 76 3D	meta http-equiv=
0x11BB4	27 63 6F 6E 74 65 6E 74 2D 74 79 70 65 27 20 63	'content-type' c
0x11BC4	6F 6E 74 65 6E 74 3D 27 74 65 78 74 2F 68 74 6D	ontent='text/htm
0x11BD4	6C 3B 20 63 68 61 72 73 65 74 3D 55 54 46	l; charset=UTF

Sortie décompressée

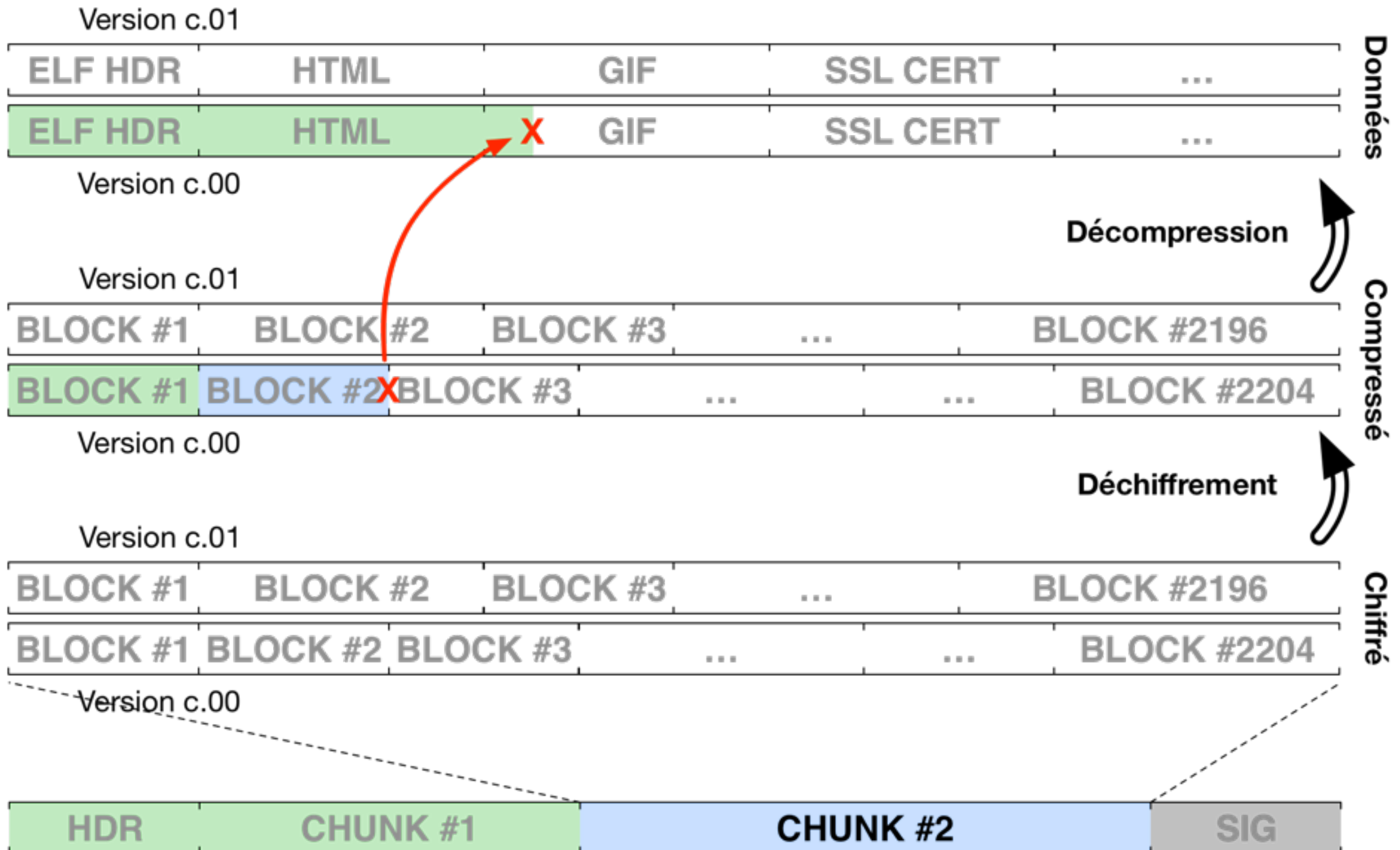
Analyse du *chunk* #2



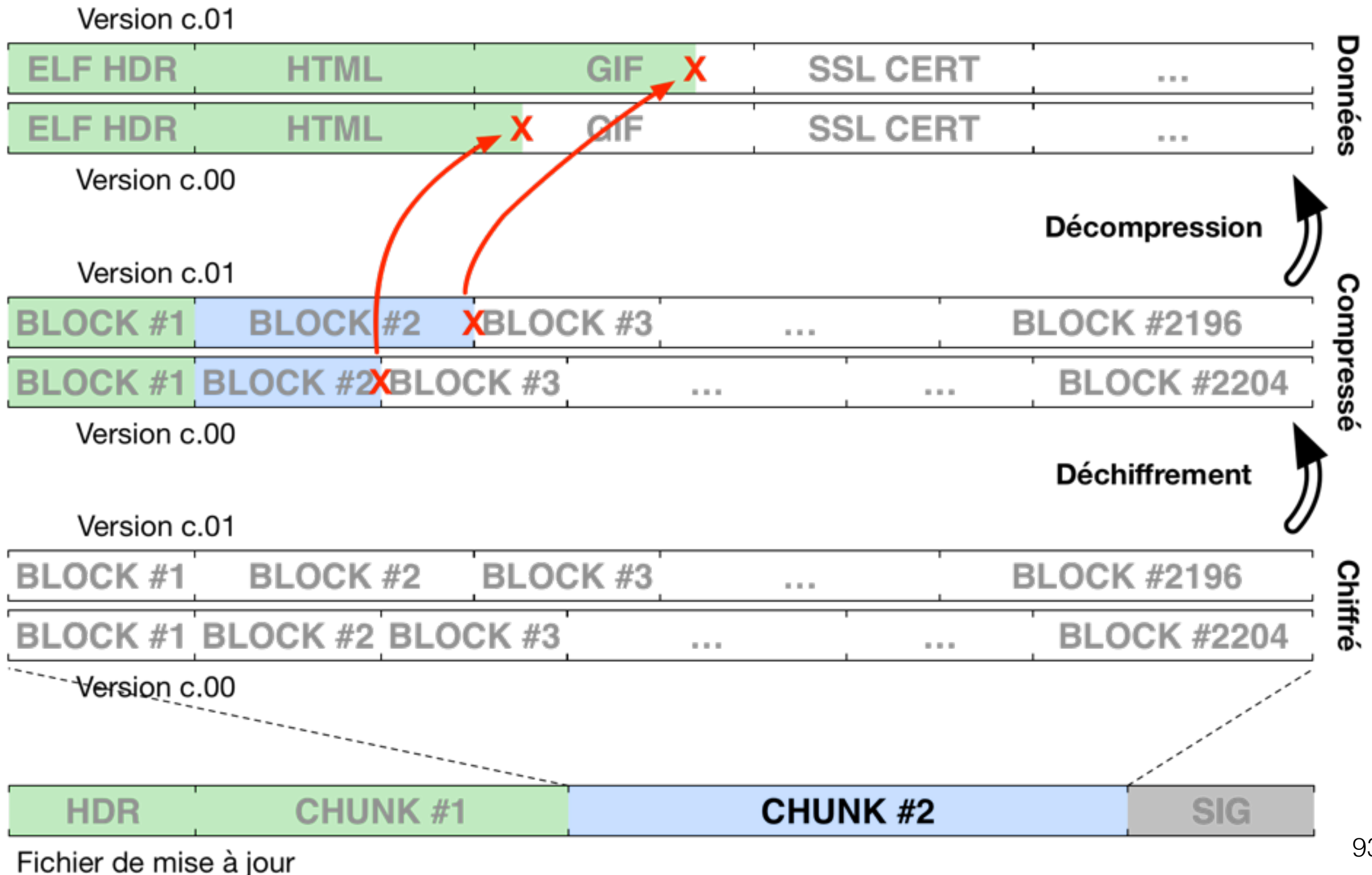
Analyse du *chunk* #2



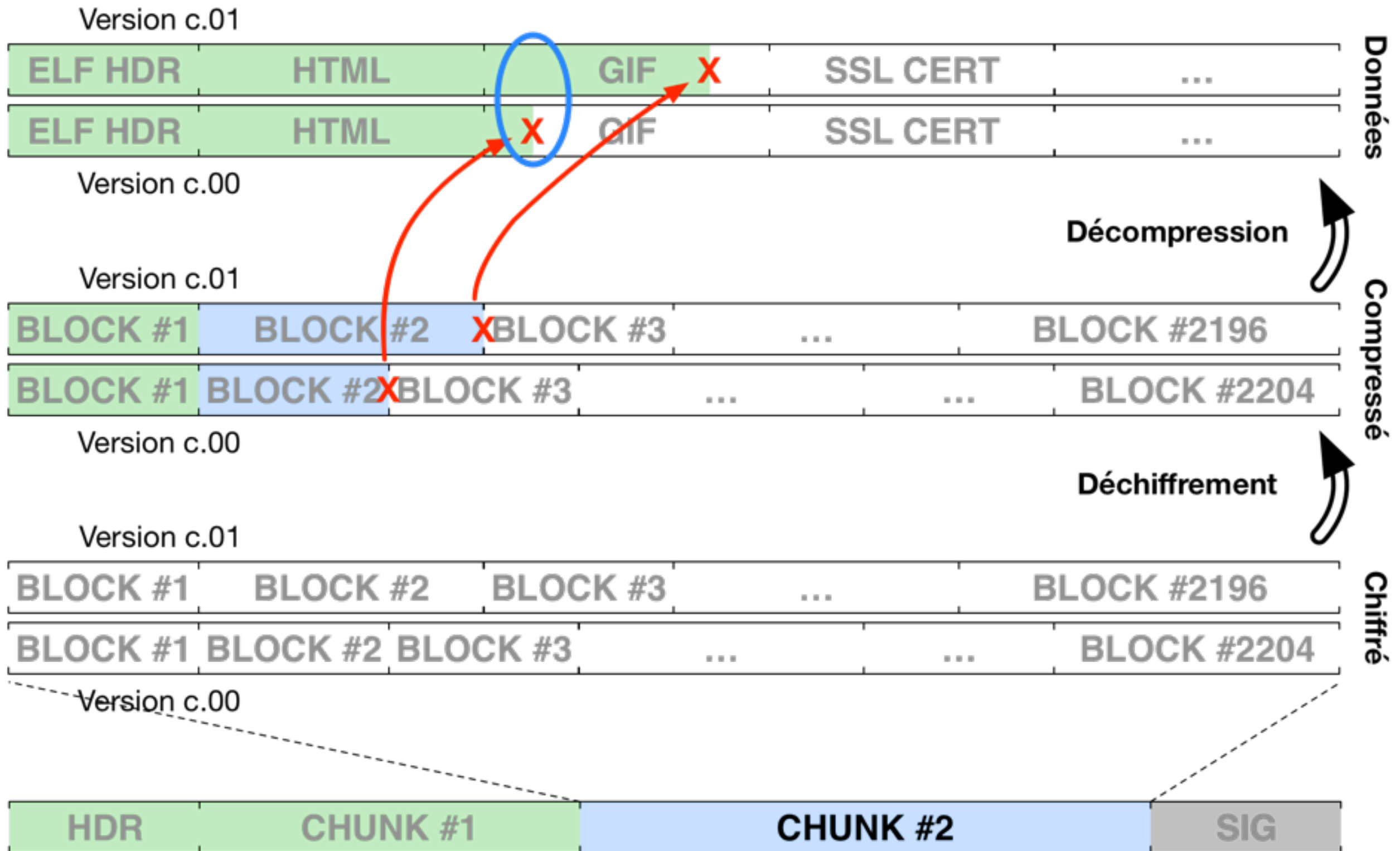
Analyse du *chunk* #2



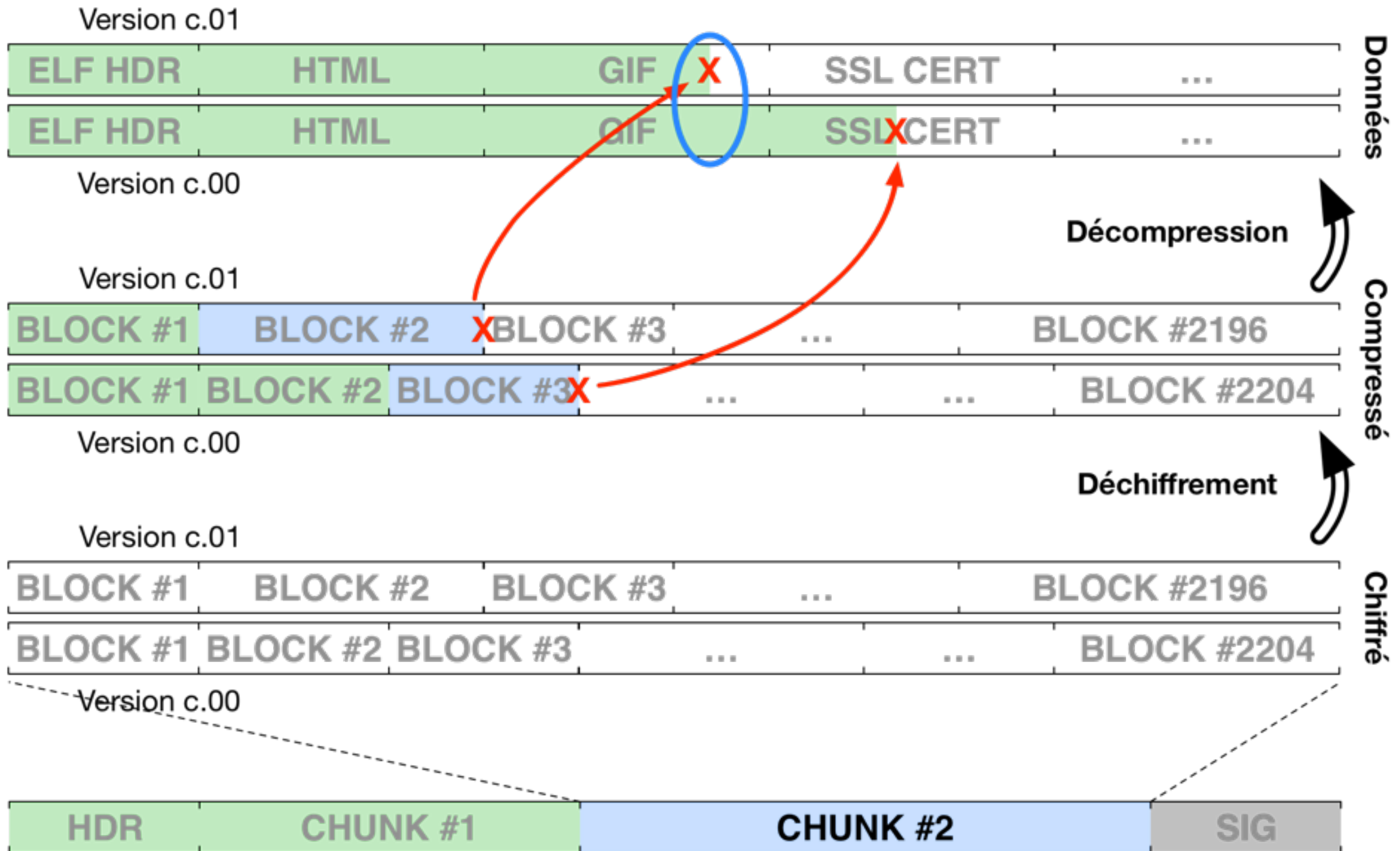
Analyse du *chunk* #2



Analyse du *chunk* #2



Analyse du *chunk* #2



Model M5

V c.00 block boundaries	V c.01	V c.00 decimal	V c.01	V c.00 block sizes (dec)	V c.01
0x00000000	0x00000000	0	0		
0x00001BA0	0x00000080	7072	128	7072	128
0x00005120	0x000030A0	20768	12448	13696	12320
0x00006468	0x00004BCC	25704	19404	4936	6956
0x0000918C	0x00007974	37260	31092	11556	11688
0x0000C850	0x0000B858	51280	47192	14020	16100
0x0000F7A0	0x0000D04C	63392	53324	12112	6132
0x00010E60	0x0000D9A4	69216	55716	5824	2392
0x00013FAC	0x00010228	81836	66088	12620	10372
0x00014AE8	0x000114E0	84712	70880	2876	4792
0x00018784	0x00014A10	100228	84496	15516	13616
0x00018B50	0x00016D64	101200	93540	972	9044
0x000193F4	0x00018F94	103412	102292	2212	8752
0x0001B864	0x000191AC	112740	102828	9328	536
0x0001BAC4	0x00019DC4	113348	105924	608	3096
0x0001EAEC	0x0001C294	125676	115348	12328	9424
0x0001FA08	0x0001F100	129544	127232	3868	11884
0x00022EE0	0x00020FFC	143072	135164	13528	7932
0x00026A58	0x000231C4	158296	143812	15224	8648
0x00027610	0x00023400	161296	144384	3000	572
0x00028E94	0x00024420	167572	148512	6276	4128
0x0002B040	0x00027528	176192	161064	8620	12552
0x0002CA78	0x00029C34	182904	171060	6712	9996
0x00030800	0x0002DA9C	198656	187036	15752	15976
0x00032FD4	0x0002FE8C	208852	196236	10196	9200
0x00033650	0x00030C98	210512	199832	1660	3596
0x00034AC0	0x00031964	215744	203108	5232	3276
0x00036C30	0x00035638	224304	218680	8560	15572
0x00036E54	0x00039214	224852	234004	548	15324
0x00039A6C	0x0003B9B0	236140	244144	11288	10140
0x0003B968	0x0003BBFC	244072	244732	7932	588
0x0003D508	0x0003E820	251144	256032	7072	11300
0x00040A88	0x0003E8A0	264840	256160	13696	128
0x00041DD0	0x000418C0	269776	268480	4936	12320
0x00044AF4	0x000433EC	281332	275436	11556	6956
0x000481B8	0x00046194	295352	287124	14020	11688
0x0004B108	0x0004A078	307464	303224	12112	16100
0x0004C7C8	0x0004B86C	313288	309356	5824	6132

HDR
CHUNK #1
CHUNK #2
SIG

6 semaines écoulées
(~3 à plein temps)
(2 pour faire les *slides*)

HDR	CHUNK #1	CHUNK #2	SIG
-----	----------	----------	-----

Pour finir

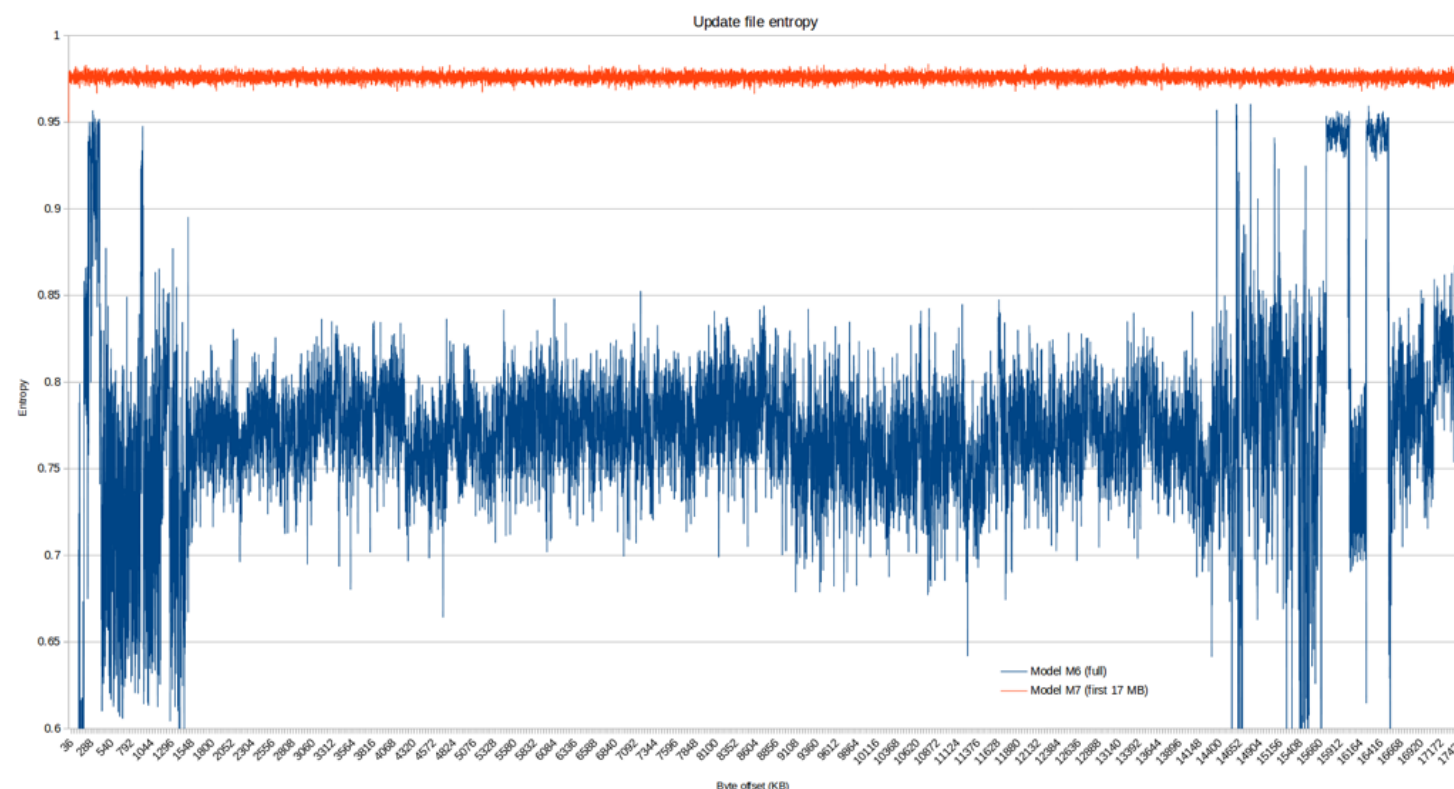
- Je ne sais pas comment l'algorithme a été imaginé
- Les faiblesses observées ne transcrivent pas forcément ce qui a été pensé par le concepteur
- L'attaquant a une vision de l'algorithme complètement différente de celle du concepteur

Pour finir

- Alors, qu'est-ce c'est ?
 - binaire ELF de 42 Mo
 - OS temps-réel complet
 - *kernel* monolithique, *filesystem*, *drivers*
 - tous propriétaires
 - équipe de développement *kernel* maison
- C++, “obfusqué”

Pour finir

- La “cryptographie fait-maison” peut s’attaquer bien plus facilement qu’on ne le croit
- y compris des implémentations “innovantes” d’AES



Pour finir

- Le *reverse-engineering* du *firmware* a permis de trouver de véritables vulnérabilités
- et d'en faire corriger
- le constructeur a également décidé de changer d'algorithme

Technique/Idea	Ref.	Comments/Relevance
Finding instruction opcodes	3.1	Unsuccessful attempt at finding executable code
Matching calling conventions	3.1	Unsuccessful attempt at finding code-like patterns in case the encryption kept symbols alike
Bitwise binary differences	3.3	Helped locate bitfields, headers, parameters, etc.
Comparing multiple samples	3.4	Helped identify static data BLOBs, enable statistical analysis, exploit potential similarities
Bruteforce	3.5	Helped recover data without known/identifiable plaintext
Reverse-engineering	3.6	Helped identify and implement the compression algorithm, helped find useful error/corner cases
Binary data fingerprinting	3.7	Unsuccessful attempt at recovering complete files from firmware image

Merci

- Greetz
 - Fabrice Desclaux
 - Camille Mougey
 - Cédric Bouhier
 - Nicolas Vivet