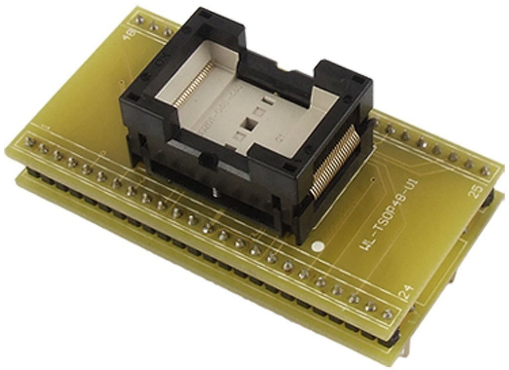
Bricked WiFi device reflashing guide

You might have an outdated version of this document. I recommend you to ***check for updates*** *if you did not download this file from my blog:* **http://blog.shibby.fr**. *Comments, suggestions and corrections are more than welcome. Please send me an e-mail if you think that this document can be improved:* ***b.l.o.g@s.h.i.b.by.f.r*** *(the e-mail address has been intentionally scrambled to avoid spam, do not copy & paste it)*

1. Bill of materials

Here is what you will need to reprogram the corrupted Flash memory:

Universal programmer



TSOP48 (most common package) to DIP adapter

I've used the picture of a Topmax 2 universal programmer because this is what I own, and I've been able to successfully reflash all chips with it so far. The supported devices list is pretty huge, but sometimes I need to find a close reference or an equivalent chip from another manufacturer in this list. The PC software “Max Loader” is available for free at EETools: http://eetools.com/index.cfm?fuseaction=category.display&category_id=38, so you can already check if you can reprogram your Flash memory before buying one of these devices. An other solution is to ask your local electronics shop if they can provide this service, or use a programmer at your university or at work. The price of these programmers is kinda expensive and it's not worth buying one just to unbrick a cheap WiFi device.
The TSOP adapter is a cheap one bought on ebay a few years ago. You should check aliexpress too if you plan to buy one.

Links to the files mentioned in this document are listed in **Annex B**.
This guide may also apply to other embedded devices.

2. Read and save the Flash memory

This might sound silly since its content is corrupted, but it can be useful if you can't find a working image. This image is a perfect copy of a non corrupted Flash memory for your device's particular hardware (same revision).
It's really important to keep a copy of the actual Flash content before doing anything else with it.

3. Get an image for the Flash

3.1.Search on forums

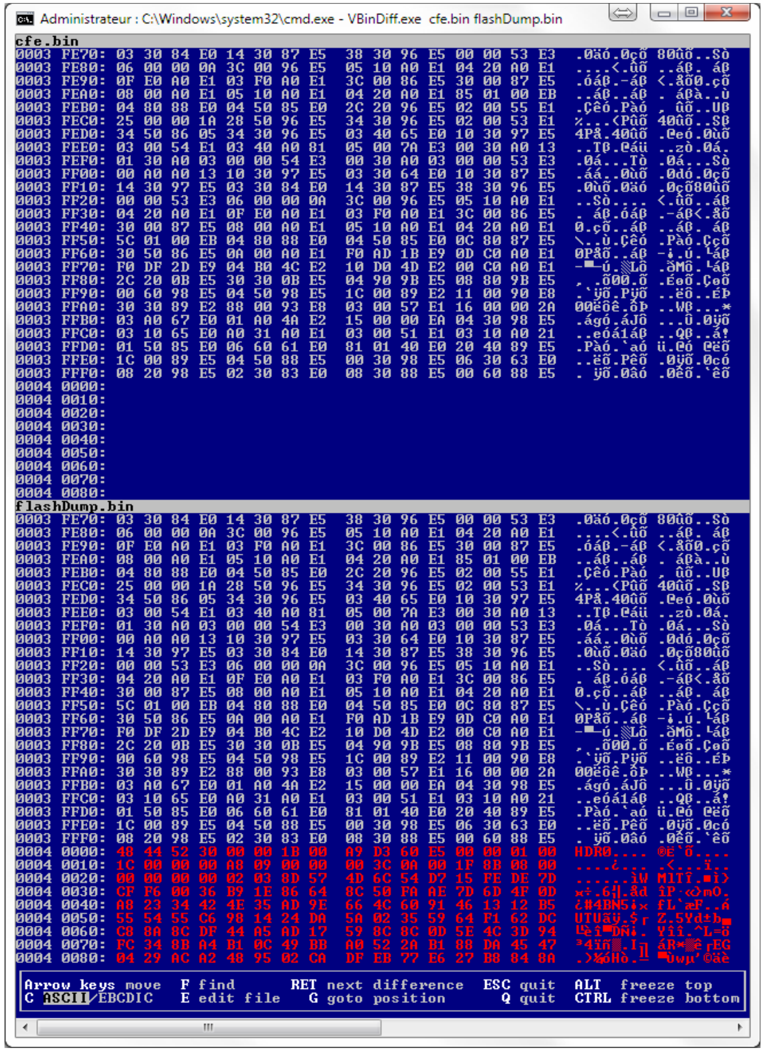
None of the manufacturers provide such files. You will have to crave unofficial forums and try to find someone who made that kind of copy. The chances to find this image will be very weak if your device is not one of the very popular ones.

3.2. Build it yourself

This is why keeping a copy of your corrupted flash is important.
Let me give you a concrete example: a corrupted Flash from a WRE54G V1.0 WiFi repeater.
I got two of these devices from someone who contacted me after reading a tutorial I poster a few years ago, explaining how I repaired my bricked WAP54G V1.0 (I'll get back to that device in **Annex A**).
The following messages was sent on its serial port console right after booting with the CFE (Common Firmware Environment):

```
Device eth0: hwaddr xx-xx-xx-xx-xx-xx, ipaddr 192.168.1.245, mask 255.255.255.0
gateway not set, nameserver not set
Boot program checksum is invalid
Reading :: Failed.: Error
CFE>
```

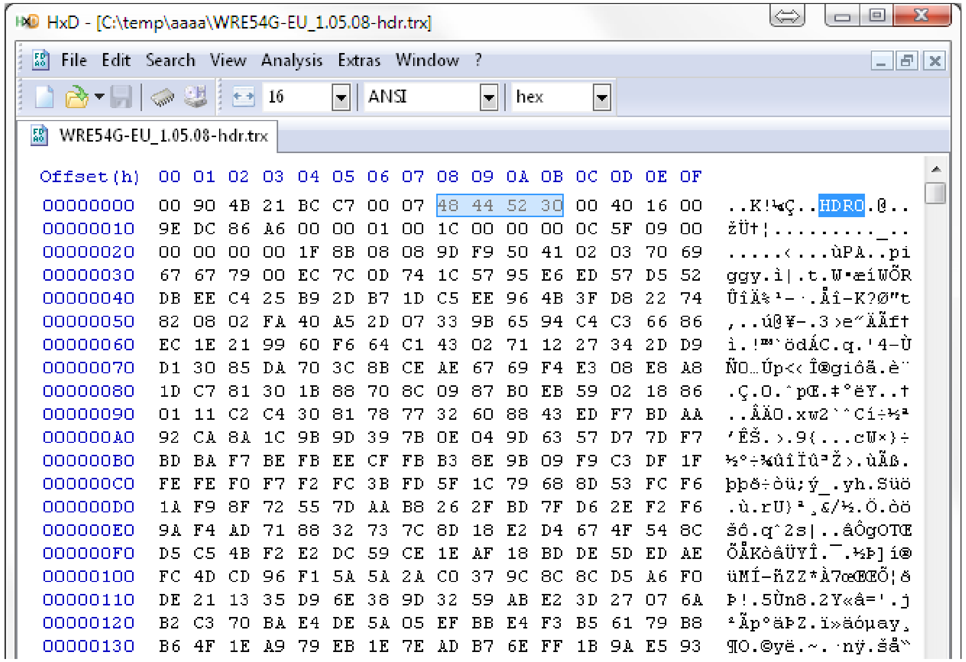
It's been quite tricky to reprogram the WRE54G V1.0 since nobody could provide an image. The only file I've been able to find was a CFE image, which only contains the boot program that starts the embedded Linux application. The CFE alone is useless since it seemed to run fin on both devices, but it helped me to define the Flash memory mapping, and see where (at which address) the Linux part is located in the chip. So I've compared the content of the corrupted memory with the CFE and here is what I've found:


Administrateur : C:\Windows\system32\cmd.exe - VBinDiff.exe cfe.bin flashDump.bin

```
cfe.bin
0003 FE70: 03 30 84 E0 14 30 87 E5  38 30 96 E5 00 00 53 E3  .0äó.0çõ 80ûõ..Sò
0003 FE80: 06 00 00 0A 3C 00 96 E5  05 10 A0 E1 04 20 A0 E1  ....<.ûõ ..áß. áß
0003 FE90: 0F E0 A0 E1 03 F0 A0 E1  3C 00 86 E5 30 00 87 E5  .óáß.-áß <.åõ0.çõ
0003 FEA0: 08 00 A0 E1 05 10 A0 E1  04 20 A0 E1 85 01 00 EB  ..áß..áß . áßà..ù
0003 FEB0: 04 80 88 E0 04 50 85 E0  2C 20 96 E5 02 00 55 E1  .Çêó.Pàó , ûõ..Uß
0003 FEC0: 25 00 00 1A 28 50 96 E5  34 30 96 E5 02 00 53 E1  %...(Pûõ 40ûõ..Sß
0003 FED0: 34 50 86 05 34 30 96 E5  03 40 65 E0 10 30 97 E5  4På.40ûõ .@eó.0ùõ
0003 FEE0: 03 00 54 E1 03 40 A0 81  05 00 7A E3 00 30 A0 13  ..Tß.@áü ..zò.0á.
0003 FEF0: 01 30 A0 03 00 00 54 E3  00 30 A0 03 00 00 53 E3  .0á...Tò .0á...Sò
0003 FF00: 00 A0 A0 13 10 30 97 E5  03 30 64 E0 10 30 87 E5  .áá..0ùõ .0dó.0çõ
0003 FF10: 14 30 97 E5 03 30 84 E0  14 30 87 E5 38 30 96 E5  .0ùõ.0äó .0çõ80ûõ
0003 FF20: 00 00 53 E3 06 00 00 0A  3C 00 96 E5 05 10 A0 E1  ..Sò.... <.ûõ..áß
0003 FF30: 04 20 A0 E1 0F E0 A0 E1  03 F0 A0 E1 3C 00 86 E5  . áß.óáß .-áß<.åõ
0003 FF40: 30 00 87 E5 08 00 A0 E1  05 10 A0 E1 04 20 A0 E1  0.çõ..áß ..áß. áß
0003 FF50: 5C 01 00 EB 04 80 88 E0  04 50 85 E0 0C 80 87 E5  \..ù.Çêó .Pàó.Ççõ
0003 FF60: 30 50 86 E5 0A 00 A0 E1  F0 AD 1B E9 0D C0 A0 E1  0Påõ..áß -¡.ú.└áß
0003 FF70: F0 DF 2D E9 04 B0 4C E2  10 D0 4D E2 00 C0 A0 E1  -▀-ú.░Lô .ðMô.└áß
0003 FF80: 2C 20 0B E5 30 30 0B E5  04 90 9B E5 08 80 9B E5  , .õ00.õ .Éøõ.Çøõ
0003 FF90: 00 60 98 E5 04 50 98 E5  1C 00 89 E2 11 00 90 E8  .`ÿõ.Pÿõ ..ëô..ÉÞ
0003 FFA0: 30 30 89 E2 88 00 93 E8  03 00 57 E1 16 00 00 2A  00ëôê.ôÞ ..Wß...*
0003 FFB0: 03 A0 67 E0 01 A0 4A E2  15 00 00 EA 04 30 98 E5  .ágó.áJô ...Û.0ÿõ
0003 FFC0: 03 10 65 E0 A0 31 A0 E1  03 00 51 E1 03 10 A0 21  ..eóá1áß ..Qß..á!
0003 FFD0: 01 50 85 E0 06 60 61 E0  81 01 40 E0 20 40 89 E5  .Pàó.`aó ü.@ó @ëõ
0003 FFE0: 1C 00 89 E5 04 50 88 E5  00 30 98 E5 06 30 63 E0  ..ëõ.Pêõ .0ÿõ.0có
0003 FFF0: 08 20 98 E5 02 30 83 E0  08 30 88 E5 00 60 88 E5  . ÿõ.0âó .0êõ.`êõ
0004 0000:
0004 0010:
0004 0020:
0004 0030:
0004 0040:
0004 0050:
0004 0060:
0004 0070:
0004 0080:
flashDump.bin
0003 FE70: 03 30 84 E0 14 30 87 E5  38 30 96 E5 00 00 53 E3  .0äó.0çõ 80ûõ..Sò
0003 FE80: 06 00 00 0A 3C 00 96 E5  05 10 A0 E1 04 20 A0 E1  ....<.ûõ ..áß. áß
0003 FE90: 0F E0 A0 E1 03 F0 A0 E1  3C 00 86 E5 30 00 87 E5  .óáß.-áß <.åõ0.çõ
0003 FEA0: 08 00 A0 E1 05 10 A0 E1  04 20 A0 E1 85 01 00 EB  ..áß..áß . áßà..ù
0003 FEB0: 04 80 88 E0 04 50 85 E0  2C 20 96 E5 02 00 55 E1  .Çêó.Pàó , ûõ..Uß
0003 FEC0: 25 00 00 1A 28 50 96 E5  34 30 96 E5 02 00 53 E1  %...(Pûõ 40ûõ..Sß
0003 FED0: 34 50 86 05 34 30 96 E5  03 40 65 E0 10 30 97 E5  4På.40ûõ .@eó.0ùõ
0003 FEE0: 03 00 54 E1 03 40 A0 81  05 00 7A E3 00 30 A0 13  ..Tß.@áü ..zò.0á.
0003 FEF0: 01 30 A0 03 00 00 54 E3  00 30 A0 03 00 00 53 E3  .0á...Tò .0á...Sò
0003 FF00: 00 A0 A0 13 10 30 97 E5  03 30 64 E0 10 30 87 E5  .áá..0ùõ .0dó.0çõ
0003 FF10: 14 30 97 E5 03 30 84 E0  14 30 87 E5 38 30 96 E5  .0ùõ.0äó .0çõ80ûõ
0003 FF20: 00 00 53 E3 06 00 00 0A  3C 00 96 E5 05 10 A0 E1  ..Sò.... <.ûõ..áß
0003 FF30: 04 20 A0 E1 0F E0 A0 E1  03 F0 A0 E1 3C 00 86 E5  . áß.óáß .-áß<.åõ
0003 FF40: 30 00 87 E5 08 00 A0 E1  05 10 A0 E1 04 20 A0 E1  0.çõ..áß ..áß. áß
0003 FF50: 5C 01 00 EB 04 80 88 E0  04 50 85 E0 0C 80 87 E5  \..ù.Çêó .Pàó.Ççõ
0003 FF60: 30 50 86 E5 0A 00 A0 E1  F0 AD 1B E9 0D C0 A0 E1  0Påõ..áß -¡.ú.└áß
0003 FF70: F0 DF 2D E9 04 B0 4C E2  10 D0 4D E2 00 C0 A0 E1  -▀-ú.░Lô .ðMô.└áß
0003 FF80: 2C 20 0B E5 30 30 0B E5  04 90 9B E5 08 80 9B E5  , .õ00.õ .Éøõ.Çøõ
0003 FF90: 00 60 98 E5 04 50 98 E5  1C 00 89 E2 11 00 90 E8  .`ÿõ.Pÿõ ..ëô..ÉÞ
0003 FFA0: 30 30 89 E2 88 00 93 E8  03 00 57 E1 16 00 00 2A  00ëôê.ôÞ ..Wß...*
0003 FFB0: 03 A0 67 E0 01 A0 4A E2  15 00 00 EA 04 30 98 E5  .ágó.áJô ...Û.0ÿõ
0003 FFC0: 03 10 65 E0 A0 31 A0 E1  03 00 51 E1 03 10 A0 21  ..eóá1áß ..Qß..á!
0003 FFD0: 01 50 85 E0 06 60 61 E0  81 01 40 E0 20 40 89 E5  .Pàó.`aó ü.@ó @ëõ
0003 FFE0: 1C 00 89 E5 04 50 88 E5  00 30 98 E5 06 30 63 E0  ..ëõ.Pêõ .0ÿõ.0có
0003 FFF0: 08 20 98 E5 02 30 83 E0  08 30 88 E5 00 60 88 E5  . ÿõ.0âó .0êõ.`êõ
0004 0000: 48 44 52 30 00 00 1B 00  A9 D3 60 E5 00 00 01 00  HDR0.... ®Ë`õ....
0004 0010: 1C 00 00 00 A8 09 00 00  00 3C 0A 00 1F 8B 08 00  ....¿... .<...ï..
0004 0020: 00 00 00 00 02 03 8D 57  4D 6C 54 D7 15 FE DE 7D  ......ìW MlTÎ.■ì}
0004 0030: CF F6 00 36 B9 1E 86 64  8C 50 FA AE 7D 6D 4F 0D  ¤÷.6╣.åd îP·«}mO.
0004 0040: A8 23 34 42 4E 35 AD 9E  66 4C 60 91 46 13 12 B5  ¿#4BN5¡× fL`æF..Á
0004 0050: 55 54 55 C6 98 14 24 DA  5A 02 35 59 64 F1 62 DC  UTUãÿ.$┌ Z.5Yd±b▄
0004 0060: C8 8A 8C DF 44 A5 AD 17  59 8C 8C 0D 5E 4C 3D 94  ╚èî▀DÑ¡. Yîî.^L=ö
0004 0070: FC 34 8B A4 B1 0C 49 BB  A0 52 2A B1 88 DA 45 47  ³4ïñ▒.I╗ áR*▒ê┌EG
0004 0080: 04 29 AC A2 48 95 02 CA  DF EB 77 E6 27 B8 84 8A  .)¼óHò.╩ ▀Ùwµ'©äè

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

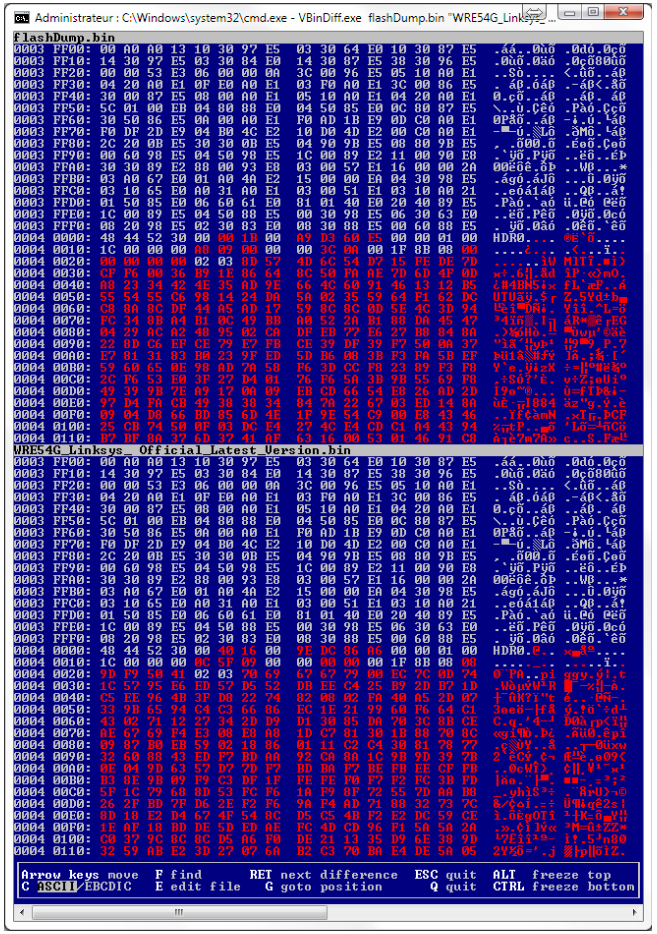
Both file's content were exactly identical from address 0x0 to 0x3FFFF.
Since there was nothing else in the CFE file (cfe.bin), I could affirm that this first block was reserved to the CFE and was not corrupted, so what bricked the repeater was only a bad firmware upgrade.
The difference, shown in red, starts at address 0x40000 on the corrupted flash memory (flashDump.bin).
It was still quite hard to understand how to repair the repeater at this point. So I've searched for a firmware update file with my favourite search engine. These files are supposed to be used with device's web interface only, to reprogram the Flash, which requires a working device.
I've opened the official firmware update to see if I could do anything with it, and found something familiar:


HxD - [C:\temp\aaaa\WRE54G-EU_1.05.08-hdr.trx]
File
Edit
Search
View
Analysis
Extras
Window
?
16
ANSI
hex
WRE54G-EU_1.05.08-hdr.trx

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  00 90 4B 21 BC C7 00 07 48 44 52 30 00 40 16 00  ..K!¼Ç..HDR0.@..
00000010  9E DC 86 A6 00 00 01 00 1C 00 00 00 0C 5F 09 00  žÜ†¦........._..
00000020  00 00 00 00 1F 8B 08 08 9D F9 50 41 02 03 70 69  .....‹...ùPA..pi
00000030  67 67 79 00 EC 7C 0D 74 1C 57 95 E6 ED 57 D5 52  ggy.ì|.t.W•æíWÕR
00000040  DB EE C4 25 B9 2D B7 1D C5 EE 96 4B 3F D8 22 74  ÛîÄ%¹-·.Åî–K?Ø"t
00000050  82 08 02 FA 40 A5 2D 07 33 9B 65 94 C4 C3 66 86  ‚..ú@¥-.3›e”ÄÃf†
00000060  EC 1E 21 99 60 F6 64 C1 43 02 71 12 27 34 2D D9  ì.!™`ödÁC.q.'4-Ù
00000070  D1 30 85 DA 70 3C 8B CE AE 67 69 F4 E3 08 E8 A8  Ñ0…Úp<‹Î®giôã.è¨
00000080  1D C7 81 30 1B 88 70 8C 09 87 B0 EB 59 02 18 86  .Ç.0.ˆpŒ.‡°ëY..†
00000090  01 11 C2 C4 30 81 78 77 32 60 88 43 ED F7 BD AA  ..ÂÄ0.xw2`ˆCí÷½ª
000000A0  92 CA 8A 1C 9B 9D 39 7B 0E 04 9D 63 57 D7 7D F7  ’ÊŠ.›.9{...cW×}÷
000000B0  BD BA F7 BE FB EE CF FB B3 8E 9B 09 F9 C3 DF 1F  ½º÷¾ûîÏû³Ž›.ùÃß.
000000C0  FE FE F0 F7 F2 FC 3B FD 5F 1C 79 68 8D 53 FC F6  þþð÷òü;ý_.yh.Süö
000000D0  1A F9 8F 72 55 7D AA B8 26 2F BD 7F D6 2E F2 F6  .ù.rU}ª¸&/½.Ö.òö
000000E0  9A F4 AD 71 88 32 73 7C 8D 18 E2 D4 67 4F 54 8C  šô.qˆ2s|..âÔgOTŒ
000000F0  D5 C5 4B F2 E2 DC 59 CE 1E AF 18 BD DE 5D ED AE  ÕÅKòâÜYÎ.¯.½Þ]í®
00000100  FC 4D CD 96 F1 5A 5A 2A C0 37 9C 8C 8C D5 A6 F0  üMÍ–ñZZ*À7œŒŒÕ¦ð
00000110  DE 21 13 35 D9 6E 38 9D 32 59 AB E2 3D 27 07 6A  Þ!.5Ùn8.2Y«â='.j
00000120  B2 C3 70 BA E4 DE 5A 05 EF BB E4 F3 B5 61 79 B8  ²ÃpºäÞZ.ï»äóµay¸
00000130  B6 4F 1E A9 79 EB 1E 7E AD B7 6E FF 1B 9A E5 93  ¶O.©yë.~.·nÿ.šå“
```

Things started to be a lot more clear when I saw that character string: HDR0.
I've assumed that the preceding data between addresses 0x0 and 0x07 was just some kind of checksum, or header needed by the web interface to check whether the file can be used on this device or not, and would then be useless in my case. So I've replaced everything from address 0x4000 on the corrupted Flash with the content of the official file from Linksys, starting from address 0x8 to the end of the file,
This may not be clear to everyone, so to make it simple, I've created a new file called "WRE54G_Linksys_ Official_Latest_Version.bin", containing the CFE followed by a truncated copy of the official firmware update file, just like it looks to be in the corrupted Flash.

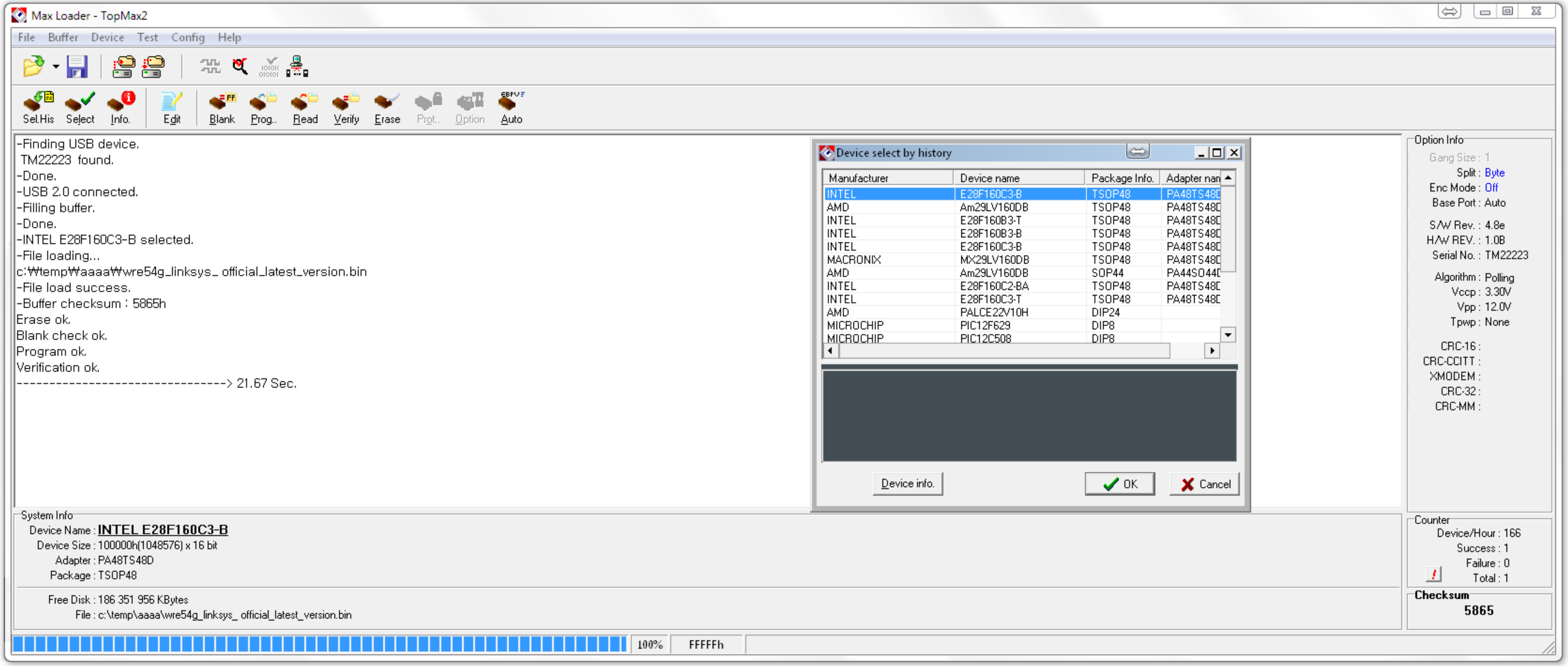

Administrateur : C:\Windows\system32\cmd.exe - VBinDiff.exe flashDump.bin "WRE54G_Linksys_...

```
flashDump.bin
0003 FF00: 00 A0 A0 13 10 30 97 E5  03 30 64 E0 10 30 87 E5  .áá..0ùõ .0dó.0çõ
0003 FF10: 14 30 97 E5 03 30 84 E0  14 30 87 E5 38 30 96 E5  .0ùõ.0äó .0çõ80ûõ
0003 FF20: 00 00 53 E3 06 00 00 0A  3C 00 96 E5 05 10 A0 E1  ..Sò.... <.ûõ..áß
0003 FF30: 04 20 A0 E1 0F E0 A0 E1  03 F0 A0 E1 3C 00 86 E5  . áß.óáß .-áß<.åõ
0003 FF40: 30 00 87 E5 08 00 A0 E1  05 10 A0 E1 04 20 A0 E1  0.çõ..áß ..áß. áß
0003 FF50: 5C 01 00 EB 04 80 88 E0  04 50 85 E0 0C 80 87 E5  \..ù.Çêó .Pàó.Ççõ
0003 FF60: 30 50 86 E5 0A 00 A0 E1  F0 AD 1B E9 0D C0 A0 E1  0Påõ..áß -¡.ú.└áß
0003 FF70: F0 DF 2D E9 04 B0 4C E2  10 D0 4D E2 00 C0 A0 E1  -▀-ú.░Lô .ðMô.└áß
0003 FF80: 2C 20 0B E5 30 30 0B E5  04 90 9B E5 08 80 9B E5  , .õ00.õ .Éøõ.Çøõ
0003 FF90: 00 60 98 E5 04 50 98 E5  1C 00 89 E2 11 00 90 E8  .`ÿõ.Pÿõ ..ëô..ÉÞ
0003 FFA0: 30 30 89 E2 88 00 93 E8  03 00 57 E1 16 00 00 2A  00ëôê.ôÞ ..Wß...*
0003 FFB0: 03 A0 67 E0 01 A0 4A E2  15 00 00 EA 04 30 98 E5  .ágó.áJô ...Û.0ÿõ
0003 FFC0: 03 10 65 E0 A0 31 A0 E1  03 00 51 E1 03 10 A0 21  ..eóá1áß ..Qß..á!
0003 FFD0: 01 50 85 E0 06 60 61 E0  81 01 40 E0 20 40 89 E5  .Pàó.`aó ü.@ó @ëõ
0003 FFE0: 1C 00 89 E5 04 50 88 E5  00 30 98 E5 06 30 63 E0  ..ëõ.Pêõ .0ÿõ.0có
0003 FFF0: 08 20 98 E5 02 30 83 E0  08 30 88 E5 00 60 88 E5  . ÿõ.0âó .0êõ.`êõ
0004 0000: 48 44 52 30 00 00 1B 00  A9 D3 60 E5 00 00 01 00  HDR0.... ®Ë`õ....
0004 0010: 1C 00 00 00 A8 09 00 00  00 3C 0A 00 1F 8B 08 00  ....¿... .<...ï..
0004 0020: 00 00 00 00 02 03 8D 57  4D 6C 54 D7 15 FE DE 7D  ......ìW MlTÎ.■Ì}
0004 0030: CF F6 00 36 B9 1E 86 64  8C 50 FA AE 7D 6D 4F 0D  ¤÷.6╣.åd îP·«}mO.
0004 0040: A8 23 34 42 4E 35 AD 9E  66 4C 60 91 46 13 12 B5  ¿#4BN5¡× fL`æF..Á
0004 0050: 55 54 55 C6 98 14 24 DA  5A 02 35 59 64 F1 62 DC  UTUãÿ.$┌ Z.5Yd±b▄
0004 0060: C8 8A 8C DF 44 A5 AD 17  59 8C 8C 0D 5E 4C 3D 94  ╚èî▀DÑ¡. Yîî.^L=ö
0004 0070: FC 34 8B A4 B1 0C 49 BB  A0 52 2A B1 88 DA 45 47  ³4ïñ▒.I╗ áR*▒ê┌EG
0004 0080: 04 29 AC A2 48 95 02 CA  DF EB 77 E6 27 B8 84 8A  .)¼óHò.╩ ▀Ùwµ'©äè
0004 0090: 22 8D C6 EF CE 79 E7 FB  CE 39 DF 39 F7 50 0A 37  "ìã´╬yþ¹ ╬9▀9÷P.7
0004 00A0: E7 81 31 83 B0 23 9F ED  5D B6 08 3B F3 FA 5B EF  þü1â░#ƒý ]Â.;¾·[´
0004 00B0: 59 60 65 0E 98 AD 7A 58  F6 3D CC F8 23 89 F3 F8  Y`e.ÿ¡zX ÷=╠°#ë¾°
0004 00C0: 2C F6 53 E0 3F 27 D4 01  76 F6 5A 3B 9B 55 69 F8  ,÷Só?'È. v÷Z;øUi°
0004 00D0: 49 39 9B 7E A9 17 0A 09  EB CD 66 54 E8 26 AD 2D  I9ø~®... Ù═fTÞ&¡-
0004 00E0: 97 D4 FA CB 49 38 38 34  84 7A 22 67 03 ED 14 8A  ùÈ·╦I884 äz"g.ý.è
0004 00F0: 09 04 D8 66 BD 85 6D 4E  1F 9E 54 C9 00 E8 43 46  ..Ïf¢àmN .×T╔.ÞCF
0004 0100: 25 CB 74 50 0F 03 DC E4  27 4C E4 CD C1 A4 43 94  %╦tP..▄õ 'LõÍ┴ñCö
0004 0110: B7 BF 8A 37 6D 37 41 AF  63 16 00 53 01 46 91 C8  À┐è7m7A» c..S.Fæ╚
WRE54G_Linksys_ Official_Latest_Version.bin
0003 FF00: 00 A0 A0 13 10 30 97 E5  03 30 64 E0 10 30 87 E5  .áá..0ùõ .0dó.0çõ
0003 FF10: 14 30 97 E5 03 30 84 E0  14 30 87 E5 38 30 96 E5  .0ùõ.0äó .0çõ80ûõ
0003 FF20: 00 00 53 E3 06 00 00 0A  3C 00 96 E5 05 10 A0 E1  ..Sò.... <.ûõ..áß
0003 FF30: 04 20 A0 E1 0F E0 A0 E1  03 F0 A0 E1 3C 00 86 E5  . áß.óáß .-áß<.åõ
0003 FF40: 30 00 87 E5 08 00 A0 E1  05 10 A0 E1 04 20 A0 E1  0.çõ..áß ..áß. áß
0003 FF50: 5C 01 00 EB 04 80 88 E0  04 50 85 E0 0C 80 87 E5  \..ù.Çêó .Pàó.Ççõ
0003 FF60: 30 50 86 E5 0A 00 A0 E1  F0 AD 1B E9 0D C0 A0 E1  0Påõ..áß -¡.ú.└áß
0003 FF70: F0 DF 2D E9 04 B0 4C E2  10 D0 4D E2 00 C0 A0 E1  -▀-ú.░Lô .ðMô.└áß
0003 FF80: 2C 20 0B E5 30 30 0B E5  04 90 9B E5 08 80 9B E5  , .õ00.õ .Éøõ.Çøõ
0003 FF90: 00 60 98 E5 04 50 98 E5  1C 00 89 E2 11 00 90 E8  .`ÿõ.Pÿõ ..ëô..ÉÞ
0003 FFA0: 30 30 89 E2 88 00 93 E8  03 00 57 E1 16 00 00 2A  00ëôê.ôÞ ..Wß...*
0003 FFB0: 03 A0 67 E0 01 A0 4A E2  15 00 00 EA 04 30 98 E5  .ágó.áJô ...Û.0ÿõ
0003 FFC0: 03 10 65 E0 A0 31 A0 E1  03 00 51 E1 03 10 A0 21  ..eóá1áß ..Qß..á!
0003 FFD0: 01 50 85 E0 06 60 61 E0  81 01 40 E0 20 40 89 E5  .Pàó.`aó ü.@ó @ëõ
0003 FFE0: 1C 00 89 E5 04 50 88 E5  00 30 98 E5 06 30 63 E0  ..ëõ.Pêõ .0ÿõ.0có
0003 FFF0: 08 20 98 E5 02 30 83 E0  08 30 88 E5 00 60 88 E5  . ÿõ.0âó .0êõ.`êõ
0004 0000: 48 44 52 30 00 40 16 00  9E DC 86 A6 00 00 01 00  HDR0.@.. ×▄åª....
0004 0010: 1C 00 00 00 0C 5F 09 00  00 00 00 00 1F 8B 08 08  ....._.. .....ï..
0004 0020: 9D F9 50 41 02 03 70 69  67 67 79 00 EC 7C 0D 74  Ø¨PA..pi ggy.ý|.t
0004 0030: 1C 57 95 E6 ED 57 D5 52  DB EE C4 25 B9 2D B7 1D  .WòµýWıR █¯─%╣-À.
0004 0040: C5 EE 96 4B 3F D8 22 74  82 08 02 FA 40 A5 2D 07  ┼¯ûK?Ï"t é...·@Ñ-.
0004 0050: 33 9B 65 94 C4 C3 66 86  EC 1E 21 99 60 F6 64 C1  3øeö─├få ý.!Ö`÷d┴
0004 0060: 43 02 71 12 27 34 2D D9  D1 30 85 DA 70 3C 8B CE  C.q.'4-┘ Ð0à┌p<ï╬
0004 0070: AE 67 69 F4 E3 08 E8 A8  1D C7 81 30 1B 88 70 8C  «gi¶Ò.Þ¿ .Ãü0.êpî
0004 0080: 09 87 B0 EB 59 02 18 86  01 11 C2 C4 30 81 78 77  .ç░ÙY..å ..┬─0üxw
0004 0090: 32 60 88 43 ED F7 BD AA  92 CA 8A 1C 9B 9D 39 7B  2`êCý÷¢¬ Æ╩è.øØ9{
0004 00A0: 0E 04 9D 63 57 D7 7D F7  BD BA F7 BE FB EE CF FB  ..ØcWÎ}÷ ¢║÷¥¹¯¤¹
0004 00B0: B3 8E 9B 09 F9 C3 DF 1F  FE FE F0 F7 F2 FC 3B FD  │Äø.¨├▀. ■■-÷=³;²
0004 00C0: 5F 1C 79 68 8D 53 FC F6  1A F9 8F 72 55 7D AA B8  _.yhìS³÷ .¨ÅrU}¬©
0004 00D0: 26 2F BD 7F D6 2E F2 F6  9A F4 AD 71 88 32 73 7C  &/¢⌂Í.=÷ Ü¶¡qê2s|
0004 00E0: 8D 18 E2 D4 67 4F 54 8C  D5 C5 4B F2 E2 DC 59 CE  ì.ÔÈgOTî ı┼K=Ô▄Y╬
0004 00F0: 1E AF 18 BD DE 5D ED AE  FC 4D CD 96 F1 5A 5A 2A  .».¢Ì]ý« ³MÍû±ZZ*
0004 0100: C0 37 9C 8C 8C D5 A6 F0  DE 21 13 35 D9 6E 38 9D  └7£îîıª- Ì!.5┘n8Ø
0004 0110: 32 59 AB E2 3D 27 07 6A  B2 C3 70 BA E4 DE 5A 05  2Y½Ô='.j ▓├p║õÌZ.
```

A quick comparison did not show a lot of similarities in the Linux memory block, but I used this new file anyway to reprogram the Flash. And guess what? It worked!

4. Flash Reprogramming

Now that you have a consistent image file, it's time to reprogram the Flash.
I had to select another device name to reprogram the WRE54G's Flash memory: E28F160 instead of TE28F160. Don't hesitate to try it too if you can't find the right device.


Max Loader - TopMax2
File Buffer Device Test Config Help
Sel.His Select Info. Edit Blank Prog.. Read Verify Erase Prot.. Option Auto
Device select by history
Device info.
OK
Cancel
Option Info
Counter
Checksum
100%
FFFFFh

```
-Finding USB device.
 TM22223  found.
-Done.
-USB 2.0 connected.
-Filling buffer.
-Done.
-INTEL E28F160C3-B selected.
-File loading...
c:₩temp₩aaaa₩wre54g_linksys_ official_latest_version.bin
-File load success.
-Buffer checksum : 5865h
Erase ok.
Blank check ok.
Program ok.
Verification ok.
-------------------------------> 21.67 Sec.
```

Manufacturer	Device name	Package Info.	Adapter nan
INTEL	E28F160C3-B	TSOP48	PA48TS48D
AMD	Am29LV160DB	TSOP48	PA48TS48D
INTEL	E28F160B3-T	TSOP48	PA48TS48D
INTEL	E28F160B3-B	TSOP48	PA48TS48D
INTEL	E28F160C3-B	TSOP48	PA48TS48D
MACRONIX	MX29LV160DB	TSOP48	PA48TS48D
AMD	Am29LV160DB	SOP44	PA44SO44D
INTEL	E28F160C2-BA	TSOP48	PA48TS48D
INTEL	E28F160C3-T	TSOP48	PA48TS48D
AMD	PALCE22V10H	DIP24	
MICROCHIP	PIC12F629	DIP8	
MICROCHIP	PIC12C508	DIP8	

Gang Size : 1
Split : Byte
Enc Mode : Off
Base Port : Auto

S/W Rev. : 4.8e
H/W REV. : 1.0B
Serial No. : TM22223

Algorithm : Polling
Vccp : 3.30V
Vpp : 12.0V
Tpwp : None

CRC-16 :
CRC-CCITT :
XMODEM :
CRC-32 :
CRC-MM :

System Info
Device Name : INTEL E28F160C3-B
Device Size : 100000h(1048576) x 16 bit
Adapter : PA48TS48D
Package : TSOP48

Free Disk : 186 351 956 KBytes
File : c:\temp\aaaa\wre54g_linksys_ official_latest_version.bin

Device/Hour : 166
Success : 1
Failure : 0
Total : 1

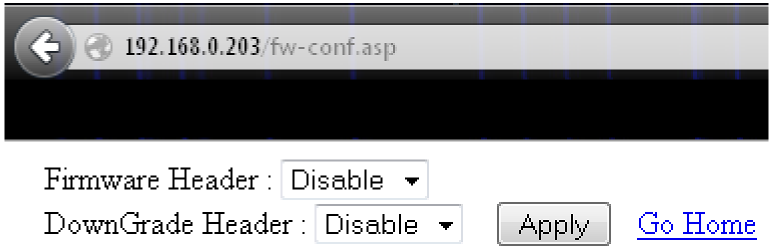
5865

As you can see, the “Auto” button takes care of everything: erasing, blank checking, programming and verifying. If everything goes well, as on this screenshot, you can then resolder the chip and admire your work.

Annex A: unbricking the WAP54G V1.0

I have to admit that I wasn't that smart when I bricked my WAP54G. Hopefully, I found someone on an unofficial Linksys forum who got a copy of his Flash memory. That's what helped me to unbrick my access point. The tutorial is available **here** [Fr].
I had to unbrick an other WAP54G V1.0 recently, and my researches led me to analyse some official firmware versions from Linksys. Despite official ".trx" for WRE54G, the ".trx" file for the WAP54G has no header and starts with the HDR0 string at address 0x0.
The boot part is also located from address 0x0 to 0x3FFF, and the Linux part also starts at address 0x4000 with HDR0.

On working devices running an official firmware, you must go to http://[your.WAP54G.IP.address]/fw-conf, select "Disable" for both "Firmware Header" and "DownGrade Header" then click "Apply". Otherwise, you won't be able to use an alternative firmware, such as dd-wrt.
This page is available on the official Linksys version 2.08 for instance:



192.168.0.203/fw-conf.asp

Firmware Header : Disable
DownGrade Header : Disable

Annex B: Links

- Hexadecimal comparator
  - VBinDiff (This is a DOS software. Usage: VBinDiff.exe FILE1 [FILE2])

- Hexadecimal editor
  - HxD

- WRE54G V1.0
  - Flash image file
    - WRE54G_Linksys_Official_Latest_Version.bin (This file must only be used to reprogram the flash chip with the universal programmer!)
  - CFE file
    - cfe.bin (for informational purposes only)
  - Genuine Linksys firmwares
    - WRE54G-EU_1.05.08-hdr.trx
    - LinksysWRE54G_1.06.05-hdr.trx
  - dd-wrt versions (only use these files to upgrade from the web interface, don't use them with the universal programmer!)
    - dd-wrt.v24_micro_generic_13064.bin
    - dd-wrt.v24_micro_generic_14896.bin (actually I did brick a repeater with one of the 14896 builds, but I may have made a mistake)
    - dd-wrt.v24_micro_olsrd_generic_14896.bin (actually I did brick a repeater with one of the 14896 builds, but I may have made a mistake)
    - Picture showing build 14896 working on a WRE54G V1 (source: http://www.dd-wrt.com/phpBB2/viewtopic.php?p=525444)

- WAP54G V1.0
  - Flash image file
    - FlashWAP54G-V10(BoardWX5541_V00)(Mustdie).BIN (This file must only be used to reprogram the flash chip with the universal programmer!)
  - Genuine Linksys firmware
    - WAP54G-fw2.08.08.trx
  - dd-wrt version (only use this file to upgrade from the web interface, don't use it with the universal programmer!)
    - WAP54G_V1.0_dd-wrt.v24-13064_VINT_micro.bin

- EETools' universal programmer software
  - Max Loader

These are mirrored files, to avoid broken links as long as my website is online.