

How to reflash the onboard T.S.O.P. in your V1.2/1.3 Xbox

WITHOUT OPENING IT

This is a document for those of you that want to reflash the bios in your xbox without opening it. WARNING this procedure CAN be dangerous to the health of your Xbox if something goes wrong or you are not CAREFUL. Please read ALL of this document BEFORE attempting anything contained herein.

INGREDIENTS:

1 virgin Xbox with a “SGS – M29F002” flash chip

Plenty of patience

A good set of eyes

A good knowledge of what the inside of an Xbox looks like

A work area that can be dimmed (do it at night helps)

An original of 007 Agent Under Fire (original – We don’t like pirate software now do we)

A xbox memory card (anything that works is ok – I used a USB keyring drive)

A copy of flashbox.zip (should be available where you got this document)

A friend with a modded Xbox (or a way to get the save game on the memory card)

A small (read tiny) light globe about 2 mm in diameter

2 pieces of fine insulated wire about 40 cm each

Some tape to insulate the wiring with

Batteries to suit the globe you are using

A small file and a small pair of needle nose pliers

EITHER:

2 pieces of stiff wire about 1.4 mm in diameter

OR:

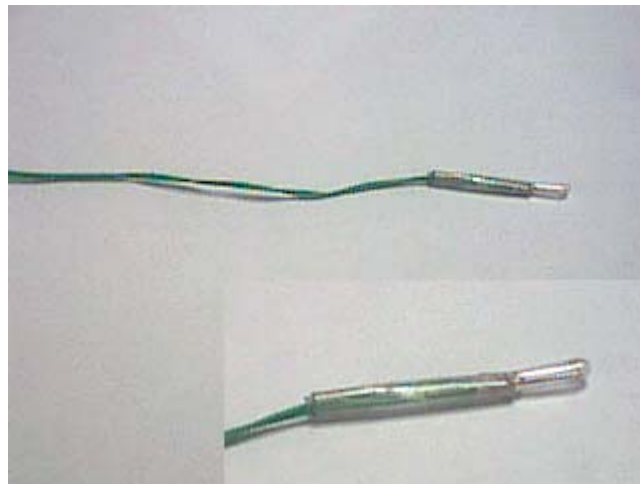
A small piece of metal pipe no bigger than 1.4 mm in diameter about 40 cm

A small piece of rubber or plastic pipe to suit the metal pipe above

A conductive paint pen or similar

The very first thing you need to do is unzip and copy the save game to your memory card, or get a friend to do it for you. A modded Xbox is the easiest way I know – I have one on hand. Once you get the save game on your

The globe should be available from most electronics suppliers – mine actually came out of an old pager that was going to be thrown away. Here is a picture of the globe I used.



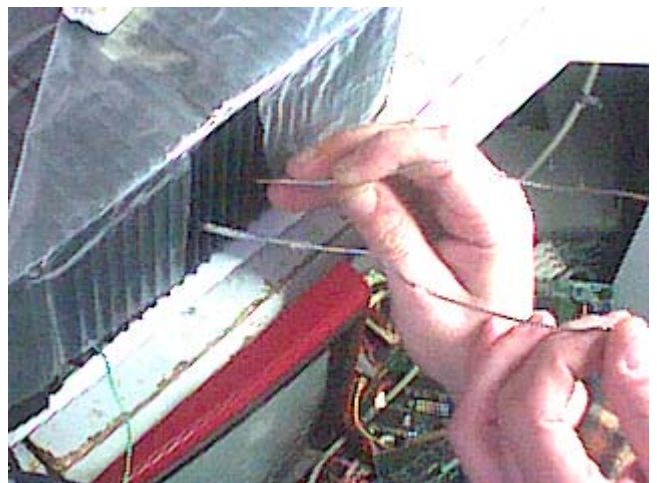
Now you have your light ready you can insert it, in the side of the Xbox, under the DVD through one of the ventilation slots CAREFULLY. You will need to play around with the position a bit to get the right amount light you need. You need to illuminate the area in the following picture that has the red circles.



NOTE: this picture was shamelessly copied from xbox scene.
Here is how it looks to my crappy camera !

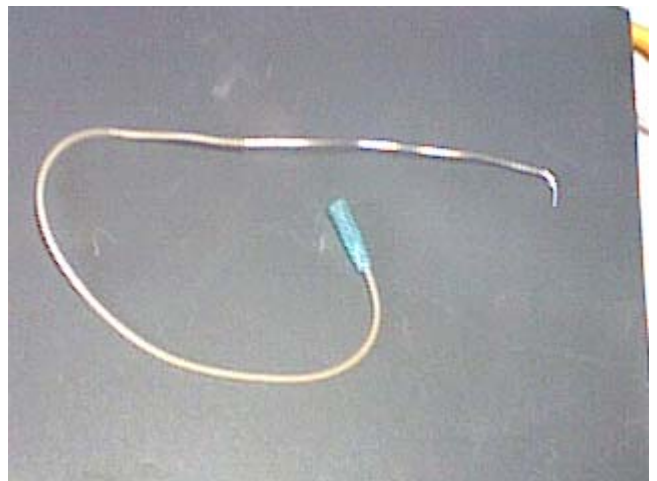
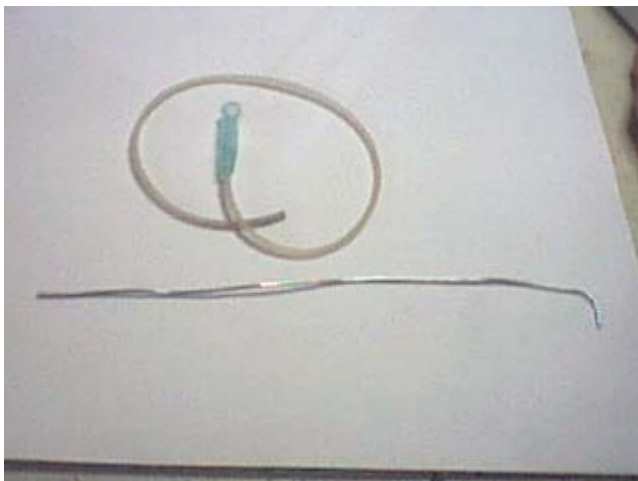


Okay now you have an Xbox ready to attack one of two ways. The first method uses two metal probes made from stiff wire. With this method, you can reflash the bios while the probes are in place, but once they are removed the bios will not be flashable. This can be useful when you are modding an Xbox for someone who is prone to tinkering – the bios can't be killed so even if they screw up the files on the hard drive, a boot disk will fix it. Now to make the probes. I used a whisk (from a kitchen shop for \$2) it is made of stainless steel and is really stiff so is perfect. I cut two pieces to length and bent them so they will fit through the vents and bridge the two jumpers on top of the PCB. **IMPORTANT** you must wrap the probe with insulation tape where it goes through the vent. Just inside the plastic slot in the side of the Xbox is a metal plate with slots in it - which the probe must pass through. If the metal probes touch the metal plate you **CAN** damage your Xbox, hence the tape. Here is a picture of the probes I made, and a picture of them being used.

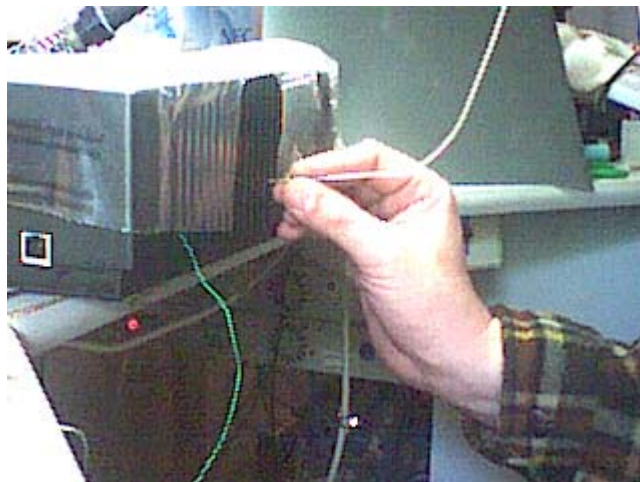


Use the pliers to bend the wire to shape, and use a file to shape the end of the probes. Don't forget the tape !!! Now with the Xbox UNPLUGGED insert the probes into the side and use the end of them to bridge the two jumpers. It will take some practice to get it right. But be VERY CAREFUL – you can break components and damage the PCB with a single slip of the probes. But how do I see where the probes are going to ? That's what the light inside the Xbox is for. You need to carefully peer through the vents to aim the probes. This method will take at least two people to perform as one person has to hold the probes in place, while the other person has to operate the software. WARNING – If one or both of the probes move during an erase or programming cycle, the bios in the Xbox will no longer work until it is correctly reflashed. This method is VERY DANGEROUS and is not recommended. It is here only for the purpose of showing it can be done. I have done it several times and DO NOT recommend anyone else try it unless they are prepared to dismantle their Xbox and solder a mod in to enable recovery – if it fails. If you really want to try this method, good luck and move on to the software section.

Now for the second method. This is a slight variation of the first method but is quite a bit safer. Instead of holding two probes through the vents to bridge the jumpers points, we will be bridging them with conductive paint instead. The advantage to this method is that once it is done, it can be reflashed again and again with nothing more than software and some common sense. But hang on you ask, just how am I supposed to get the paint out of the paint pen and onto the link points on the PCB ? Well I'm glad you asked. The idea is to get a piece of extremely thin metal pipe with a small bend on one end, and use it to deposit the paint in the right spots. First you need to find some suitable pipe. I got mine out of an old mechanical thermostat. It is called capillary tube and measures 0.9 mm in diameter. I cut a piece to about 35 cm and bent one end. See the following picture.



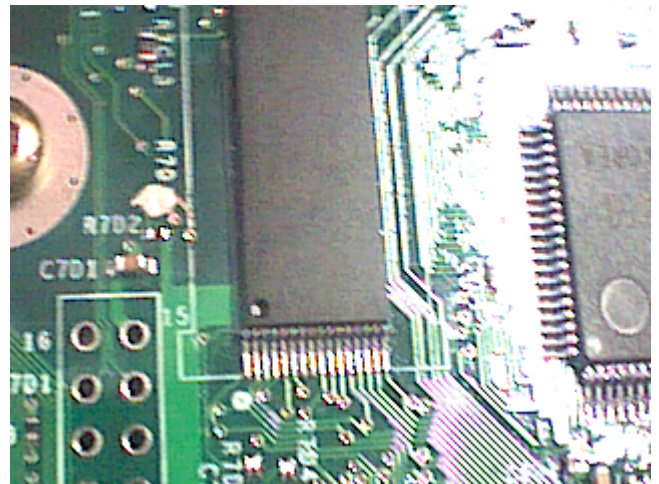
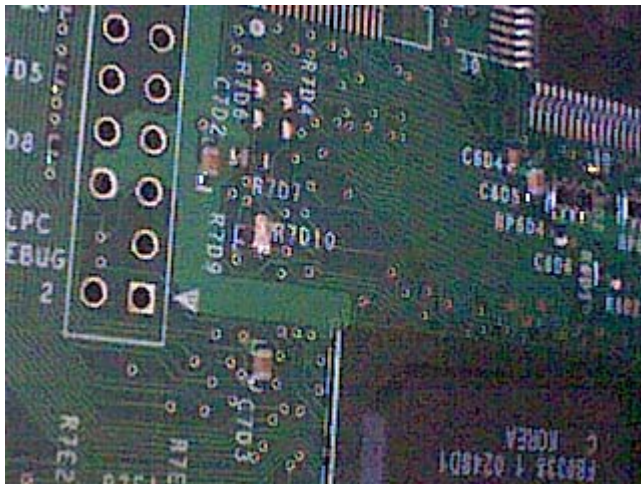
Also in the picture is a piece of rubber tube that I got from a chemist. It was a part of a “butterfly needle” that I asked the chemist to cut off the needle and dispose of it for me. Any kind of flexible tube will do that will fit over the metal pipe. See the picture above right to see how they fit together. Okay you now have the tool you need to bridge those jumpers. The first thing you need to do is to practice using it on an old PCB or similar to deposit the paint. All that is required is to squeeze out a small blob of paint from the pen onto a clean piece of scrap plastic. Follow the instructions on the pen for more info. Working reasonably quickly (before the paint dries !) place the rubber end of the hose in your mouth and the metal end into the paint blob you made. GENTLY suck the paint up into the pipe – it won’t take very much for the two jumpers. Now insert the pipe into the vents of the Xbox and position it over one of the jumper points. GENTLY blow and watch the paint come out, and regulate the pressure you apply to regulate the paint flow. It doesn’t take much paint to cover the jumper points so be careful. Once both points are linked, you can remove the pipe and TAKE A GOOD LOOK at your work – or should I say squint! Make sure that the paint joins only the points in the red circles AND NOTHING ELSE. If you Mess up and get paint in the wrong spot – don’t worry all is not lost. If you are careful, the paint can be scraped off with a piece of stiff wire VERY CAREFULLY. Any bits of paint can be picked up with a very fine artists paint brush dipped in metho. Yes you can get brushes that small ! However I don’t really recommend trying to clean through the vents – you might miss something – which is not good. That is why I recommend that you practice as much as you can before you attempt this. Here is a picture of what the procedure looks like – minus the head peering into the box to see where the pipe is going of course.



This is what the paint looks like to my camera Through the vents.



This is how the paint looks after it is in place (with lid removed so you can see what it looks like)

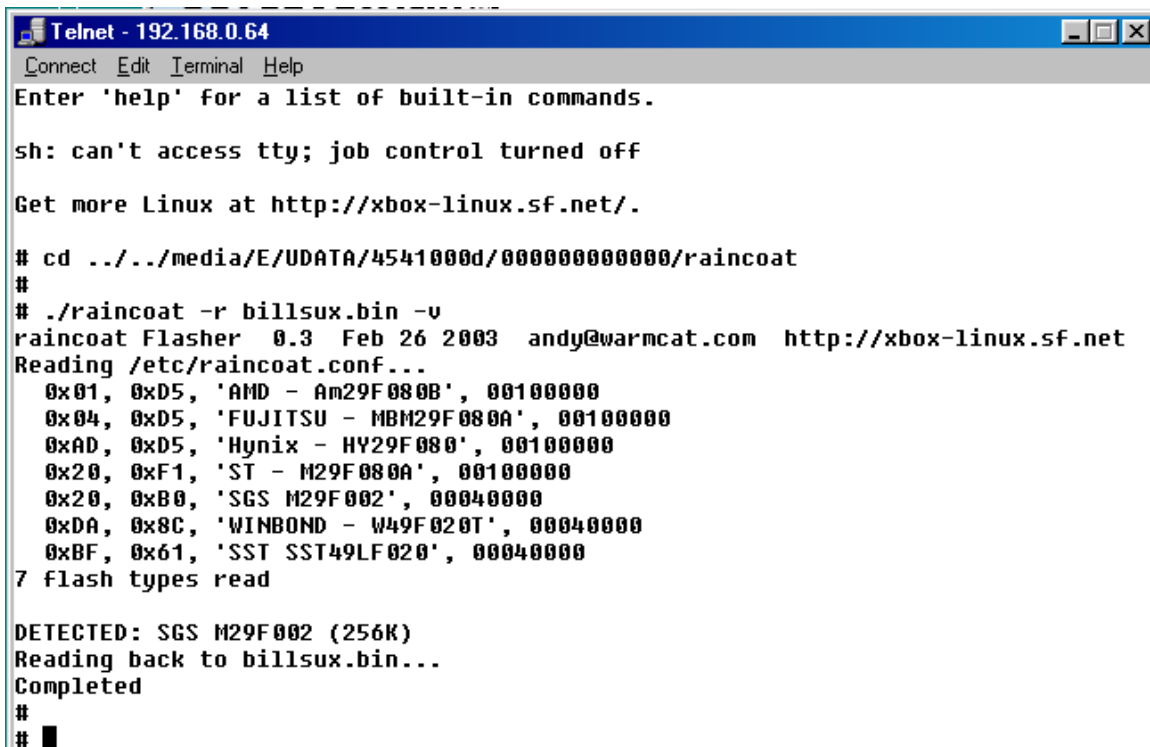


SOFTWARE:

After you load the save game from your hard disk using the 007 disk, the screen will go black and the Xbox will make some sounds. Once it is quiet (won't take very long) go to your PC and TELNET to 192.168.0.64. Log in with a user name of root and the password of xbox (what else did you expect?).

Now type in “cd ../../media/E/UDATA/4541000d/000000000000/raincoat” (without the quotes of course) and press enter. Now you need to backup your old Xbox bios for two reasons. First so you have a backup of the original bios so the box can be restored to the original operating condition. Second to test that the points that you linked on the PCB are correctly connected. If they are not correct, you can't backup the original bios and you should go and fix the links so the backup works. To backup the bios you need to type “./raincoat -r billsux.bin -v” and press enter. Note billsux.bin is the name I used for my bios backup – change that bit to the name you want it called – usually backup.bin or similar. If all goes well you should get a screen like the following.

If you don't get the chip type detected properly, either your jumpers aren't installed properly or the entry in raincoat.conf is missing.



```
Telnet - 192.168.0.64
Connect Edit Terminal Help
Enter 'help' for a list of built-in commands.

sh: can't access tty; job control turned off

Get more Linux at http://xbox-linux.sf.net/.

# cd ../../media/E/UDATA/4541000d/000000000000/raincoat
#
# ./raincoat -r billsux.bin -v
raincoat Flasher 0.3 Feb 26 2003 andy@warmcat.com http://xbox-linux.sf.net
Reading /etc/raincoat.conf...
 0x01, 0xD5, 'AMD - Am29F080B', 00100000
 0x04, 0xD5, 'FUJITSU - MBM29F080A', 00100000
 0xAD, 0xD5, 'Hynix - HY29F080', 00100000
 0x20, 0xF1, 'ST - M29F080A', 00100000
 0x20, 0xB0, 'SGS M29F002', 00040000
 0xDA, 0x8C, 'WINBOND - W49F020T', 00040000
 0xBF, 0x61, 'SST SST49LF020', 00040000
7 flash types read

DETECTED: SGS M29F002 (256K)
Reading back to billsux.bin...
Completed
#
# █
```

Okay now you have the bios backed up you can proceed with the flashing. Type in “./raincoat -p bios.bin -v” (without quotes) and press enter. You should see the following screens as the bios is erased, reprogrammed and verified.

```
Telnet - 192.168.0.64
Connect Edit Terminal Help
0x20, 0xF1, 'ST - M29F080A', 00100000
0x20, 0xB0, 'SGS M29F002', 00040000
0xDA, 0x8C, 'WINBOND - W49F020T', 00040000
0xBF, 0x61, 'SST SST49LF020', 00040000
7 flash types read

DETECTED: SGS M29F002 (256K)
Completed
#
# ./raincoat -p bios.bin -v
raincoat Flasher 0.3 Feb 26 2003 andy@warmcat.com http://xbox-linux.sf.net
Reading /etc/raincoat.conf...
0x01, 0xD5, 'AMD - Am29F080B', 00100000
0x04, 0xD5, 'FUJITSU - MBM29F080A', 00100000
0xAD, 0xD5, 'Hynix - HY29F080', 00100000
0x20, 0xF1, 'ST - M29F080A', 00100000
0x20, 0xB0, 'SGS M29F002', 00040000
0xDA, 0x8C, 'WINBOND - W49F020T', 00040000
0xBF, 0x61, 'SST SST49LF020', 00040000
7 flash types read

DETECTED: SGS M29F002 (256K)
Programming with bios.bin...Read 262144 bytes from file
Erasing...
14% .:(*****.....):.
```

```
Telnet - 192.168.0.64
Connect Edit Terminal Help
Enter 'help' for a list of built-in commands.

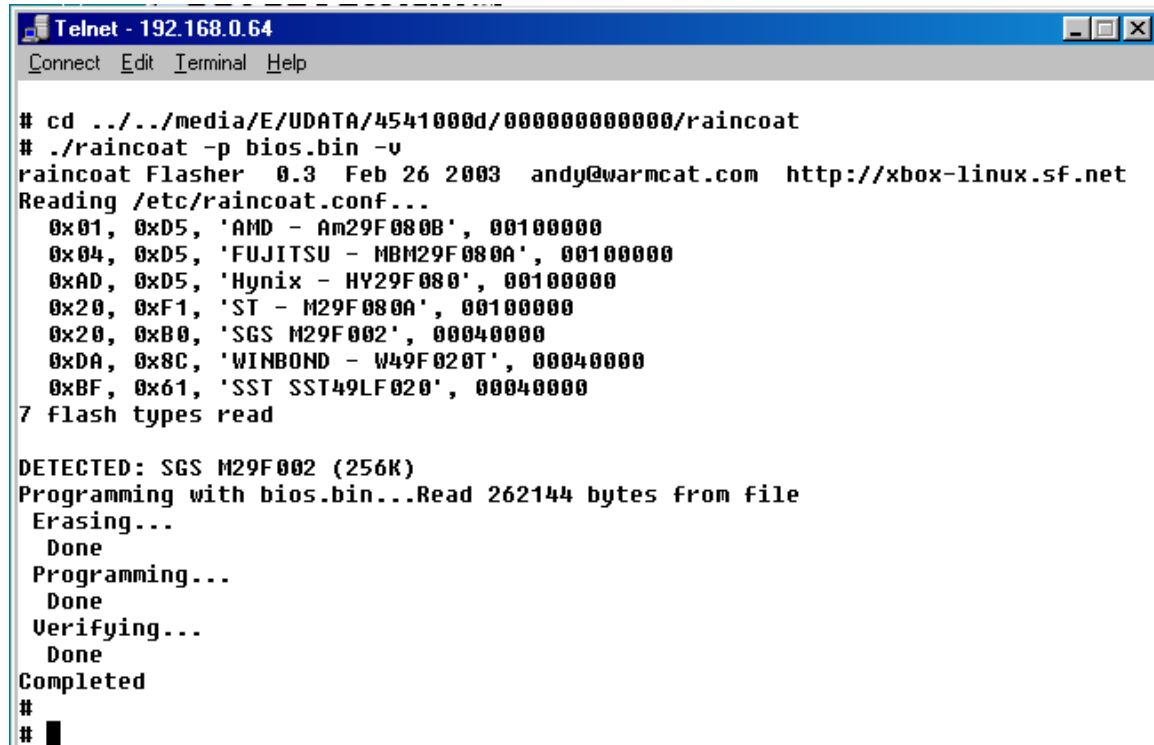
sh: can't access tty; job control turned off

Get more Linux at http://xbox-linux.sf.net/.

# cd ../../media/E/UDATA/4541000d/000000000000/raincoat
# ./raincoat -p bios.bin -v
raincoat Flasher 0.3 Feb 26 2003 andy@warmcat.com http://xbox-linux.sf.net
Reading /etc/raincoat.conf...
0x01, 0xD5, 'AMD - Am29F080B', 00100000
0x04, 0xD5, 'FUJITSU - MBM29F080A', 00100000
0xAD, 0xD5, 'Hynix - HY29F080', 00100000
0x20, 0xF1, 'ST - M29F080A', 00100000
0x20, 0xB0, 'SGS M29F002', 00040000
0xDA, 0x8C, 'WINBOND - W49F020T', 00040000
0xBF, 0x61, 'SST SST49LF020', 00040000
7 flash types read

DETECTED: SGS M29F002 (256K)
Programming with bios.bin...Read 262144 bytes from file
Erasing...
Done
Programming...
22% .:(*****.....):█
```


AND FINALLY this screen.



```
Telnet - 192.168.0.64
Connect Edit Terminal Help

# cd ../../media/E/UDATA/4541000d/000000000000/raincoat
# ./raincoat -p bios.bin -v
raincoat Flasher 0.3 Feb 26 2003 andy@warmcat.com http://xbox-linux.sf.net
Reading /etc/raincoat.conf...
0x01, 0xD5, 'AMD - Am29F080B', 00100000
0x04, 0xD5, 'FUJITSU - MBM29F080A', 00100000
0xAD, 0xD5, 'Hynix - HY29F080', 00100000
0x20, 0xF1, 'ST - M29F080A', 00100000
0x20, 0xB0, 'SGS M29F002', 00040000
0xDA, 0x8C, 'WINBOND - W49F020T', 00040000
0xBF, 0x61, 'SST SST49LF020', 00040000
7 flash types read

DETECTED: SGS M29F002 (256K)
Programming with bios.bin...Read 262144 bytes from file
Erasing...
Done
Programming...
Done
Verifying...
Done
Completed
#
# █
```

Success at last. This means that your new bios is now flashed into the Xbox. Make sure you keep the backup bios safe incase you ever need it. Now for a note on flash chips. This method will currently work on all boxes with a SGS flash, the Winbonds don't seem to work. This seems to be a minor bug in raincoat. You can use a hacked Micro\$oft dashboard and it will work with both the SGS and Winbond chips – but who wants to do that !!! A word on the way raincoat works. For some reason I'm not sure about it will only see seven entries in its config file and you MUST use the default name of bios.bin when you flash your bios or it can really spit the dummy and leave you with an Xbox with an incomplete bios. It's probably just something I'm doing wrong – but I found it easier to use the default name and put up with only seven flash types. The file bios.bin contained in flashbox.zip is a Cromwell bios ready for linux use. If you want to use a different bios you will have to replace it with your own.

Now you have read the whole document, you might be asking yourself why would anyone want to mod an Xbox in this way. Well I'll tell you. Once you have done a few with this method you won't want to do it any other way – I can reflash a V1.2/1.3 in under 5 minutes from start to finish !

HAPPY FLASHING !
THE BASTARD

