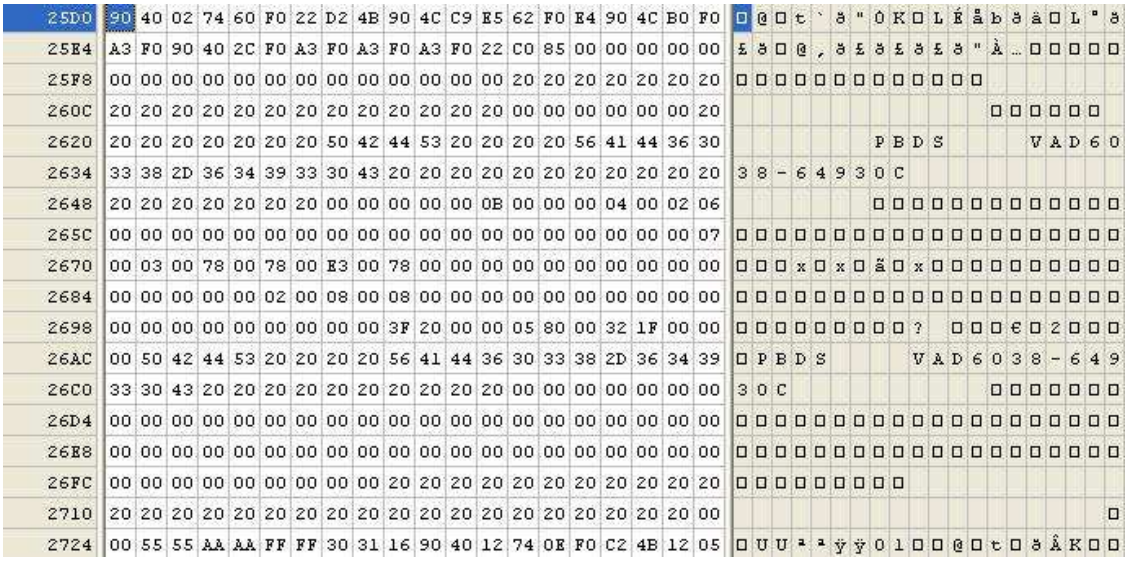
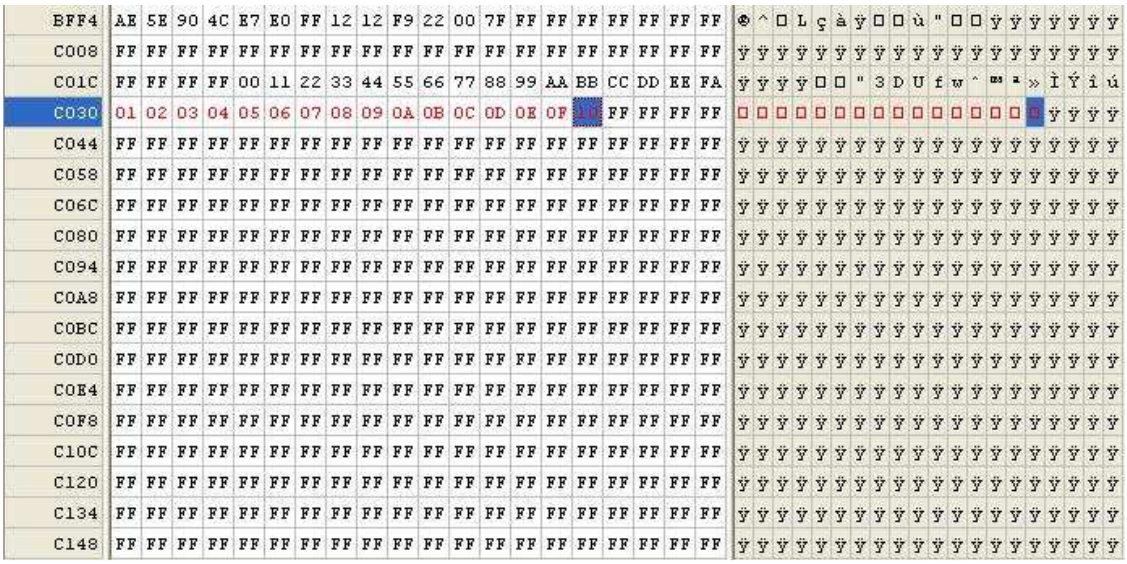
BenQ Firmware Verification with a Hex Editor

1) Open your dumped firmware with a hex editor of your choice
2) Check for your version strings between $2000-2FFF



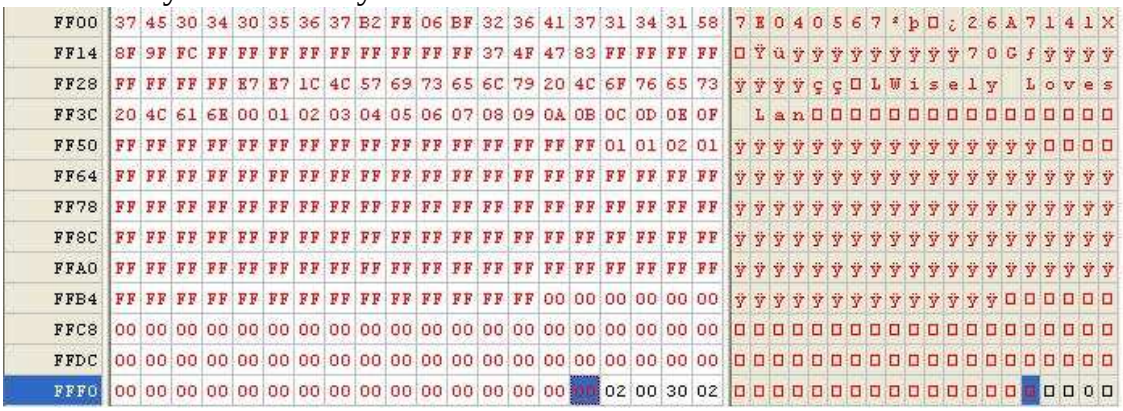
25D0	90	40	02	74	60	F0	22	D2	4B	90	4C	C9	E5	62	F0	E4	90	4C	B0	F0
25E4	A3	F0	90	40	2C	F0	A3	F0	A3	F0	A3	F0	22	C0	85	00	00	00	00	00
25F8	00	00	00	00	00	00	00	00	00	00	00	00	00	20	20	20	20	20	20	20
260C	20	20	20	20	20	20	20	20	20	20	20	20	20	00	00	00	00	00	00	20
2620	20	20	20	20	20	20	20	50	42	44	53	20	20	20	20	56	41	44	36	30
2634	33	38	2D	36	34	39	33	30	43	20	20	20	20	20	20	20	20	20	20	20
2648	20	20	20	20	20	20	20	00	00	00	00	00	0B	00	00	00	04	00	02	06
265C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	07
2670	00	03	00	78	00	78	00	E3	00	78	00	00	00	00	00	00	00	00	00	00
2684	00	00	00	00	00	02	00	08	00	08	00	00	00	00	00	00	00	00	00	00
2698	00	00	00	00	00	00	00	00	00	3F	20	00	00	05	80	00	32	1F	00	00
26AC	00	50	42	44	53	20	20	20	20	56	41	44	36	30	33	38	2D	36	34	39
26C0	33	30	43	20	20	20	20	20	20	20	20	20	20	00	00	00	00	00	00	00
26D4	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
26E8	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
26FC	00	00	00	00	00	00	00	00	00	20	20	20	20	20	20	20	20	20	20	20
2710	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	00
2724	00	55	55	AA	AA	FF	FF	30	31	16	90	40	12	74	0E	F0	C2	4B	12	05

3) Find your drive key section $A000, $B000, $C000, $D000, $E000, that looks like the section below. In this screenshot, 0102030405060708090A0B0C0D0E0F10 is the key. It will always be before the long string of ‘FF’s to the end of the corresponding section. In this shot, FF’s go from the end of the key to $CFFF.



BFF4	AE	5E	90	4C	E7	E0	FF	12	12	F9	22	00	7F	FF	FF	FF	FF	FF	FF	FF
C008	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
C01C	FF	FF	FF	FF	00	11	22	33	44	55	66	77	88	99	AA	BB	CC	DD	EE	FA
C030	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	FF	FF	FF	FF
C044	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
C058	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
C06C	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
C080	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
C094	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
C0A8	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
C0BC	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
C0D0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
C0E4	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
C0F8	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
C10C	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
C120	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
C134	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
C148	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

4) Check the drive serial number. This will be stated at $FF00 and run until $FFFF. This is unique to each drive, so it is just as important to note as your drive key is.



FF00	37	45	30	34	30	35	36	37	B2	FE	06	BF	32	36	41	37	31	34	31	58
FF14	8F	9F	FC	FF	FF	FF	FF	FF	FF	FF	FF	FF	37	4F	47	83	FF	FF	FF	FF
FF28	FF	FF	FF	FF	E7	E7	1C	4C	57	69	73	65	6C	79	20	4C	6F	76	65	73
FF3C	20	4C	61	6E	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
FF50	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	01	01	02	01
FF64	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
FF78	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
FF8C	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
FFA0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
FFB4	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	00	00	00	00
FFC8	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FFDC	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FFF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	02	00	30	02	

Hope this helps,

Caster420.