LINUX.CONF.AU
16–20 JANUARY 2017 HOBART
THE FUTURE OF OPEN SOURCE

Hamish Coleman

My personal fight against the modern laptop

IBM

Hewlett Packard Enterprise

My fight with modern laptops

LCA2017

Hamish Coleman - hamish@zot.org

Who am I

- Systems Programmer by trade
- Pull apart hardware as a hobby
- Just a grumpy guy, annoyed by change
- … but I want be 'constructive' about it

This talk

- What is wrong with current Laptops?
- How much can I change the hardware?
- What is needed to change the software?
- How does the firmware get flashed?
- What can we do next?

Chapter 1: Why

Why did I start my fight?

- Today's hardware is just not for me
- To be fair, I'm a small group
- New features at the of old ones?
- I want you to feel like you do something about it

Laptop evolution

- Keep getting smaller - this is good
- At the expense of ports, durability, keys - this is bad

- The Onion (2009)

The future?

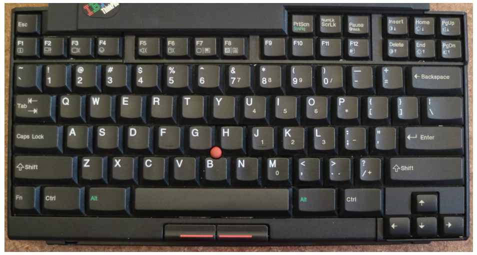
My ideal laptop

- Easily portable
- Suitable for all-day use
  - (all-day battery would be nice)
- Runs Linux
- No blobs
- Actually is a laptop
- Durable

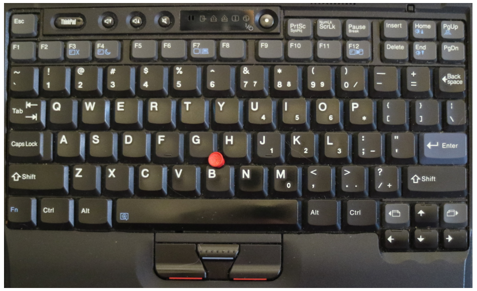
Scope

- Washing-list of changes I want
- Skills to do only one or two things
- Look at my needs and focus on the important things
- What could I do about the Keyboard on newer laptops?

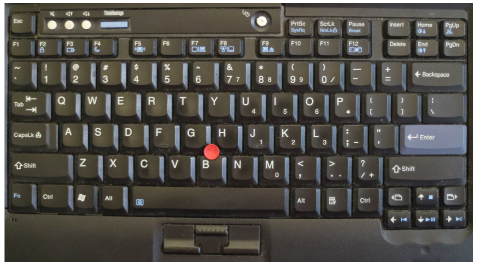
Thinkpad Keyboards - "classic"



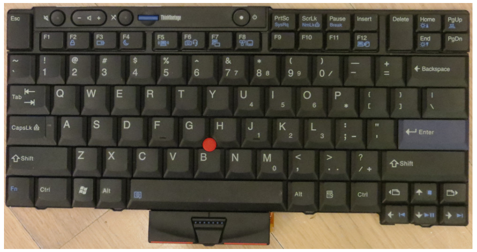
701c (1995)



x30 (2002)

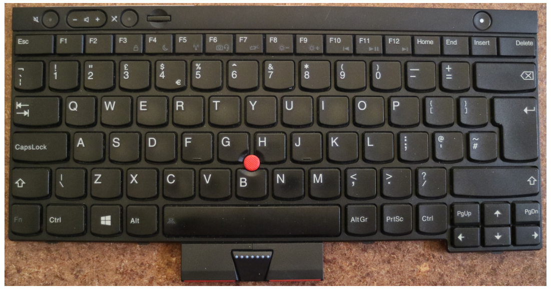


z61m (2006)

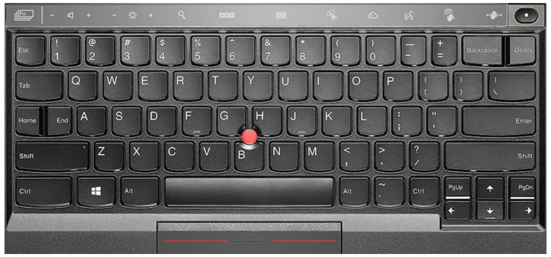


x220 (2011)

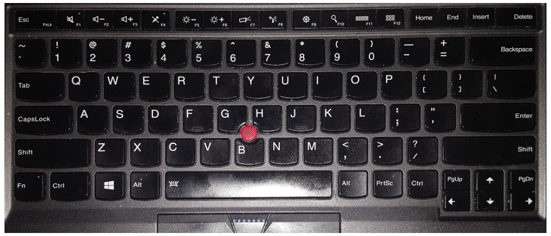
Thinkpad Keyboards - "modern"



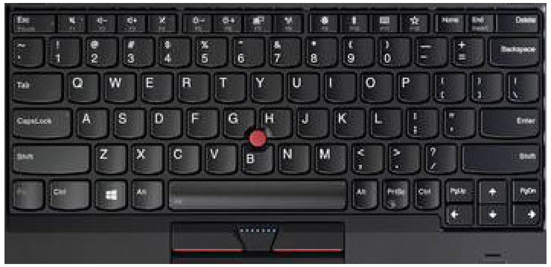
x230 (2012)



x1 gen2 (2014)

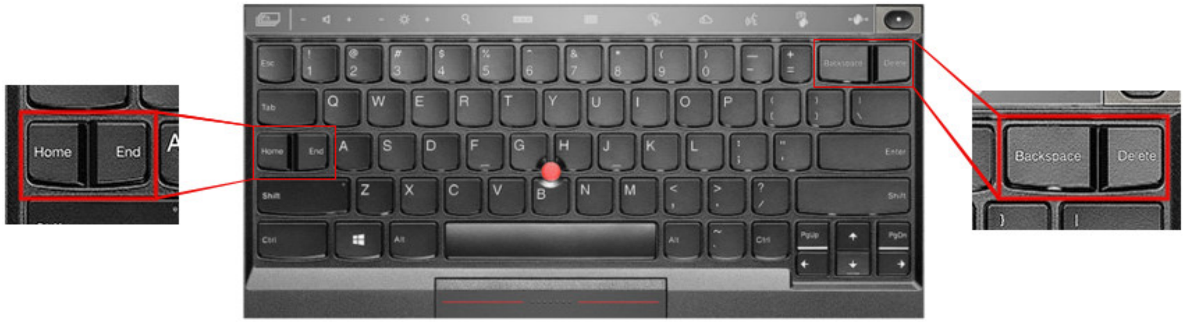


x1 gen3 (2015)



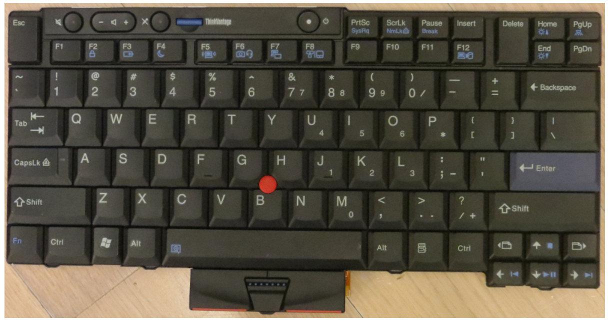
x270 (2017)

Some 'strange' design

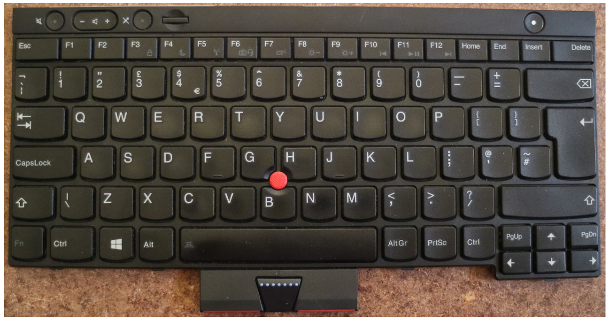


x1 gen2 (2014)

Keyboards - old and new



Thinkpad x220



Thinkpad x230

PRO:

- All the usual keys
- "Standard" layout
- Spacing helps to find keys

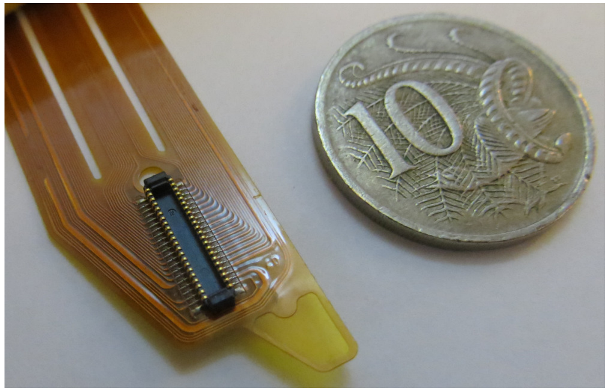
CON:

- Deleted keys / Strange locations
- Worse 'feel'
- No capslock light

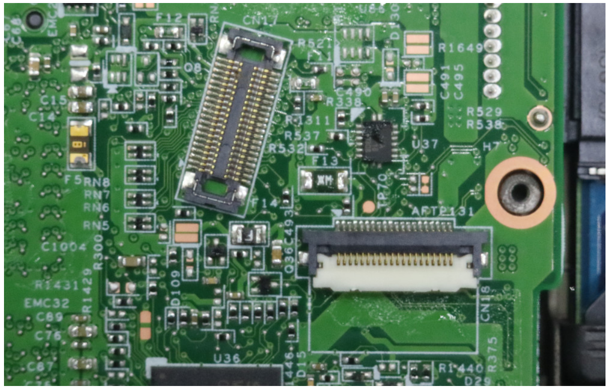
Chapter 2: Hardware replacement

Replacing the x230 keyboard

- Keyboard Connector just works…



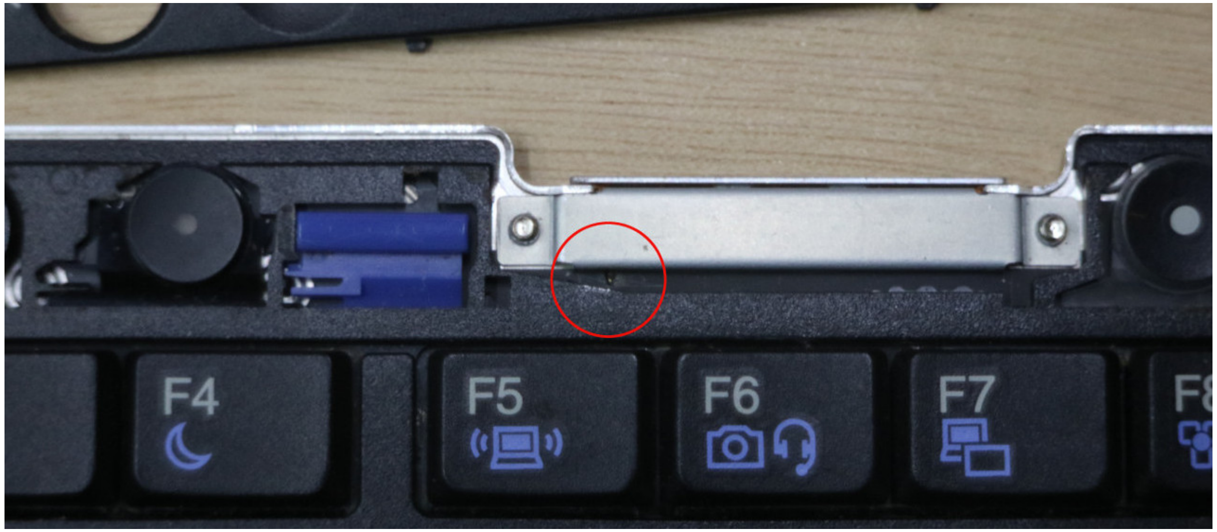
x220 Keyboard

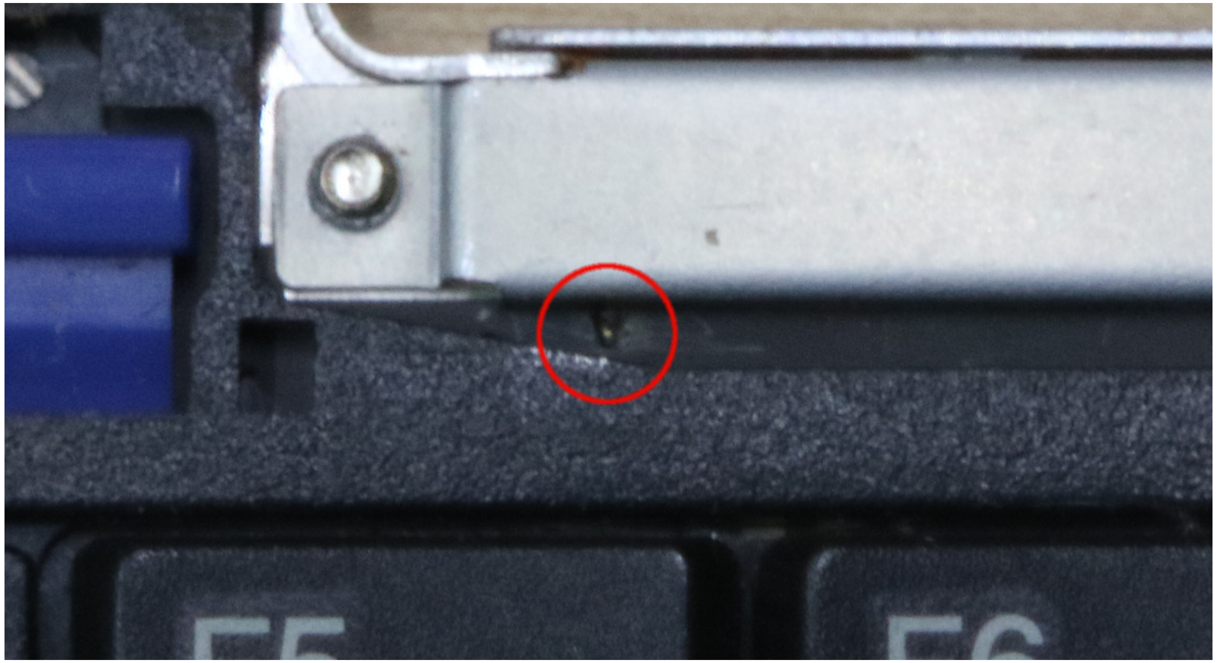


x230 Motherboard

Replacing the x230 keyboard

- but.. Backlight and Burnouts

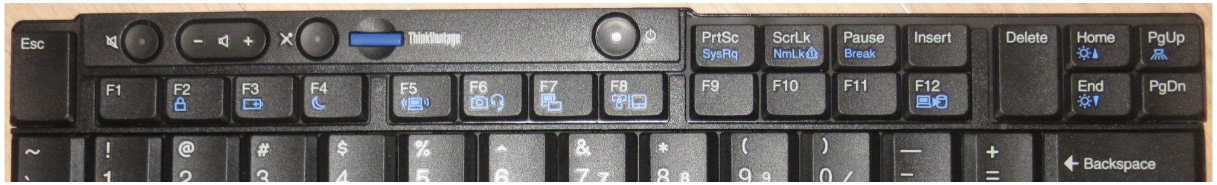




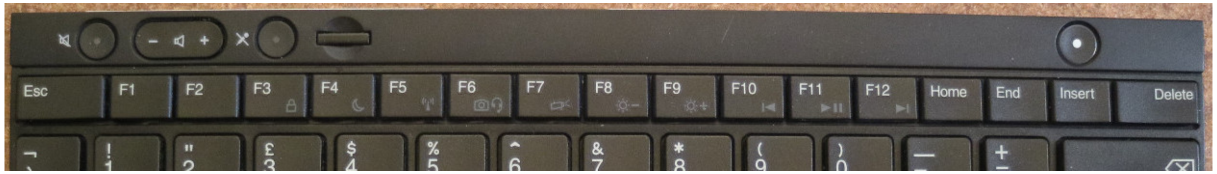
Not easy to see the burn marks

Replacing the x230 keyboard

- Many of the top-row keys dont work
- The Fn-Combos didnt match the icons



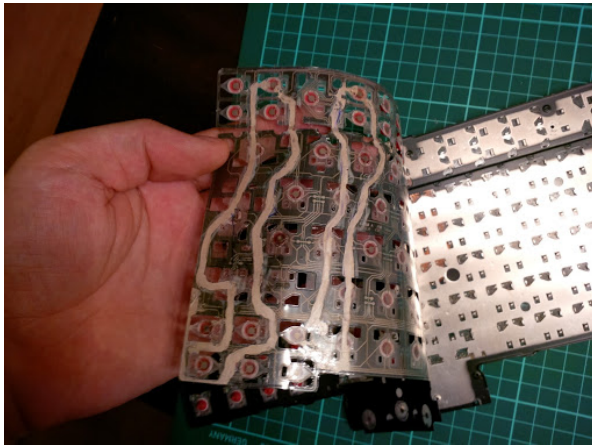
x220



x230

Replacing the x230 keyboard

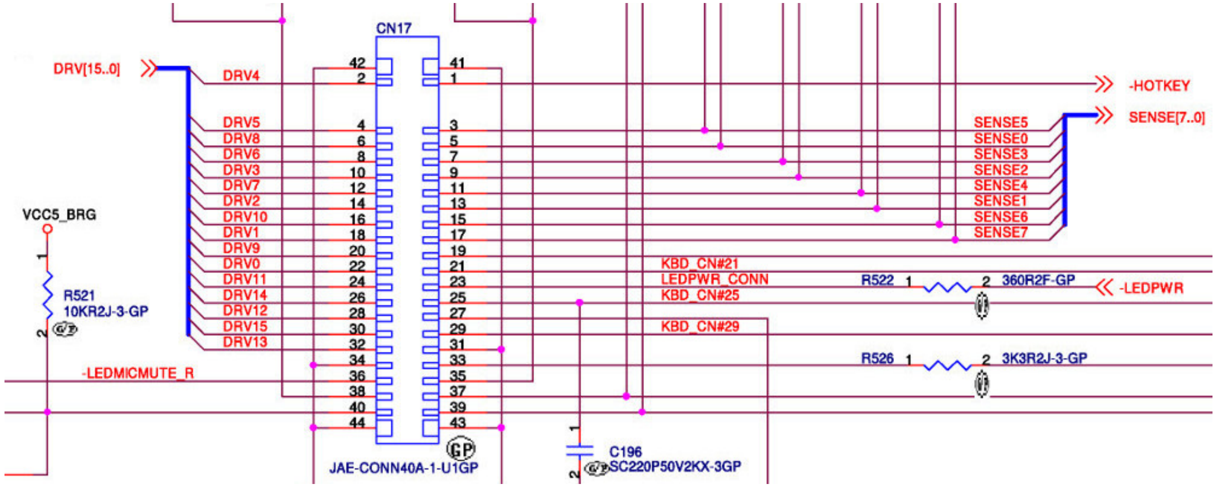
- Others have solved this…



http://forum.thinkpads.com/viewtopic.php?f=69&t=104889#p718202

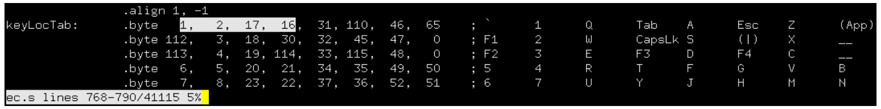
Its all just software...

- Schematics show all the dead keys are connected



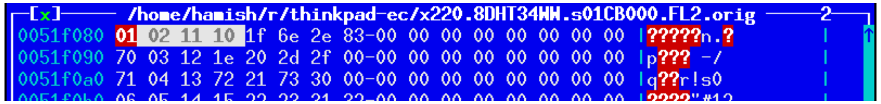
… but software sucks

- Disassembled firmware from 10 years ago exists (http://ec.gnost.info/)
- This can be used like a Rosetta stone



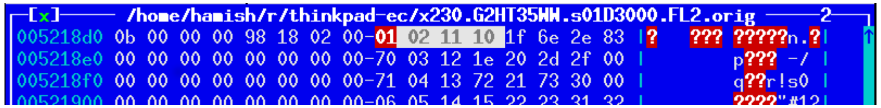
```
                .align 1, -1
keyLocTab:      .byte   1,   2,  17,  16,  31, 110,  46,  65    ; `     1     Q     Tab    A     Esc    Z     (App)
                .byte 112,   3,  18,  30,  32,  45,  47,   0    ; F1    2     W     CapsLk S     (|)    X     __
                .byte 113,   4,  19, 114,  33, 115,  48,   0    ; F2    3     E     F3     D     F4     C     __
                .byte   6,   5,  20,  21,  34,  35,  49,  50    ; 5     4     R     T      F     G      V     B
                .byte   7,   8,  23,  22,  37,  36,  52,  51    ; 6     7     U     Y      J     H      M     N
ec.s lines 768-790/41115 5%
```

T43 ec.s (viewed in less)



```
┌[x]──── /home/hamish/r/thinkpad-ec/x220.8DHT34WW.s01CB000.FL2.orig ───2─┐
0051f080 01 02 11 10 1f 6e 2e 83-00 00 00 00 00 00 00 00 |?????n.?       |
0051f090 70 03 12 1e 20 2d 2f 00-00 00 00 00 00 00 00 00 |p??? -/        |
0051f0a0 71 04 13 72 21 73 30 00-00 00 00 00 00 00 00 00 |q??r!s0        |
0051f0b0 06 05 14 15 22 23 31 32-00 00 00 00 00 00 00 00 |????"#12       |
```

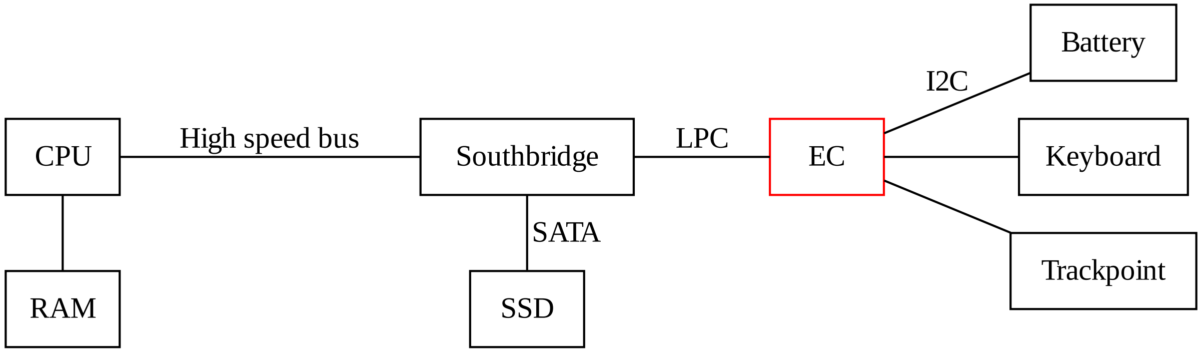
x220 EC firmware (viewed in HT Editor)



```
┌[x]──── /home/hamish/r/thinkpad-ec/x230.G2HT35WW.s01D3000.FL2.orig ───2─┐
005218d0 0b 00 00 00 98 18 02 00-01 02 11 10 1f 6e 2e 83 |?   ??? ?????n.?|
005218e0 00 00 00 00 00 00 00 00-70 03 12 1e 20 2d 2f 00 |        p??? -/ |
005218f0 00 00 00 00 00 00 00 00-71 04 13 72 21 73 30 00 |        q??r!s0 |
00521900 00 00 00 00 00 00 00 00-06 05 14 15 22 23 31 32 |        ????"#12|
```

x230 EC firmware (viewed in HT Editor)

The Embedded Controller, or "EC"



Chapter 3: Tools

Breakthrough in EC firmware

- Matthew Chapman blogs about Battery Hacking

  (See the talk before this one :-)

His mec-tools software:

- Works with Thinkpad x230 EC Firmware
- Decrypt/encrypts
- Recalculates the checksums

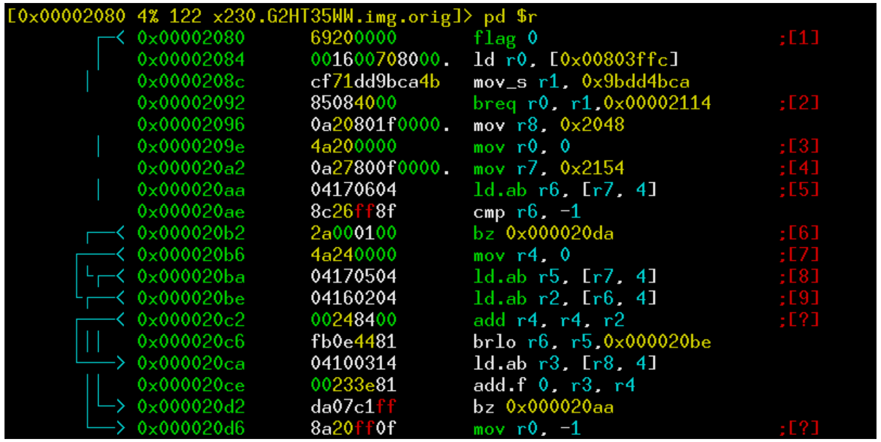
Adventures in Laptop Battery Hacking

Matthew Chapman
http://zmatt.net/
contact@zmatt.net

Presented at linux.conf.au
20th January 2017

More Reverse Engineering

- Simply patching keyLocTab doesnt fully work
- The Radare2 tool had support for the ARCompact instruction set

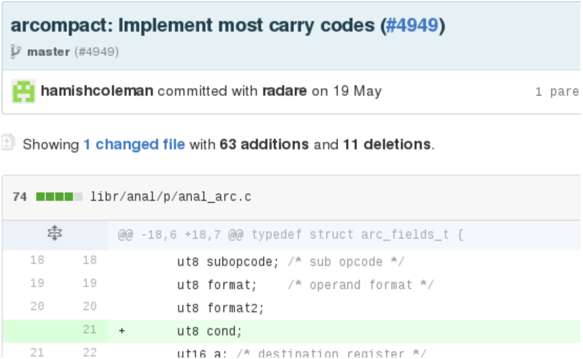


```
[0x00002080 4% 122 x230.G2HT35WW.img.orig]> pd $r
        ┌─< 0x00002080      69200000        flag 0                          ;[1]
        │   0x00002084      0016007080000.  ld r0, [0x00803ffc]
       │    0x0000208c      cf71dd9bca4b    mov_s r1, 0x9bdd4bca
            0x00002092      85084000        breq r0, r1,0x00002114          ;[2]
            0x00002096      0a20801f0000.   mov r8, 0x2048
        │   0x0000209e      4a200000        mov r0, 0                       ;[3]
            0x000020a2      0a27800f0000.   mov r7, 0x2154                  ;[4]
        │   0x000020aa      04170604        ld.ab r6, [r7, 4]               ;[5]
            0x000020ae      8c26ff8f        cmp r6, -1
       ┌──< 0x000020b2      2a000100        bz 0x000020da                   ;[6]
      ┌───< 0x000020b6      4a240000        mov r4, 0                       ;[7]
      │└┌─< 0x000020ba      04170504        ld.ab r5, [r7, 4]               ;[8]
      └┌──< 0x000020be      04160204        ld.ab r2, [r6, 4]               ;[9]
      ┌───< 0x000020c2      00248400        add r4, r4, r2                  ;[?]
      │││   0x000020c6      fb0e4481        brlo r6, r5,0x000020be
      └───> 0x000020ca      04100314        ld.ab r3, [r8, 4]
       ││   0x000020ce      00233e81        add.f 0, r3, r4
       │└─> 0x000020d2      da07c1ff        bz 0x000020aa
       └──> 0x000020d6      8a20ff0f        mov r0, -1                      ;[?]
```

Firmware excerpt - before fixing Radare2

Radare needed improvement

- Radare2 ARC support actually quite flakey
- E.G: scrolling backwards ended up going forwards!
- Worse, the ARCompact support appeared to be half missing
- Big endian only, no jump delay slot, jumps targets all wrong, no illegal instruction detection



arcompact: Implement most carry codes (#4949)

master (#4949)

hamishcoleman committed with **radare** on 19 May 1 pare

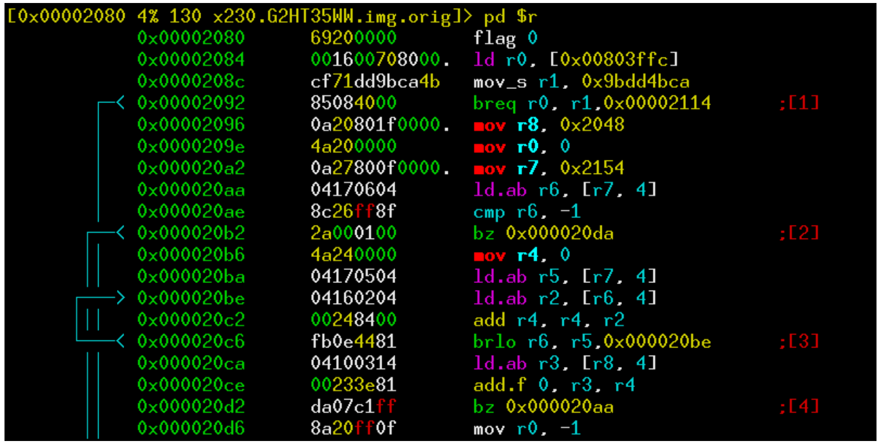
Showing **1 changed file** with **63 additions** and **11 deletions**.

74 ■■■■■ libr/anal/p/anal_arc.c

```
@@ -18,6 +18,7 @@ typedef struct arc_fields_t {
        ut8 subopcode; /* sub opcode */
        ut8 format;    /* operand format */
        ut8 format2;
+       ut8 cond;
        ut16 a; /* destination register */
```

Improvements helped

- Plenty of features still to add
- Improved enough that analysis was usable

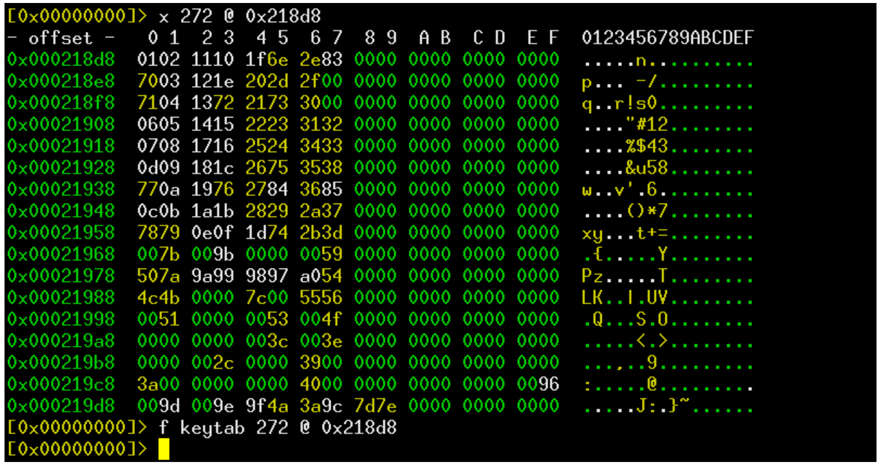


```
[0x00002080 4% 130 x230.G2HT35WW.img.orig]> pd $r
                 0x00002080       69200000        flag 0
                 0x00002084       0016007080000.  ld r0, [0x00803ffc]
                 0x0000208c       cf71dd9bca4b    mov_s r1, 0x9bdd4bca
            ┌─< 0x00002092       85084000        breq r0, r1,0x00002114       ;[1]
            │    0x00002096       0a20801f0000.  mov r8, 0x2048
            │    0x0000209e       4a200000        mov r0, 0
            │    0x000020a2       0a27800f0000.  mov r7, 0x2154
            │    0x000020aa       04170604        ld.ab r6, [r7, 4]
            │    0x000020ae       8c26ff8f        cmp r6, -1
           ┌──< 0x000020b2       2a000100        bz 0x000020da                ;[2]
           ││    0x000020b6       4a240000        mov r4, 0
           ││    0x000020ba       04170504        ld.ab r5, [r7, 4]
          ┌───> 0x000020be       04160204        ld.ab r2, [r6, 4]
          │││    0x000020c2       00248400        add r4, r4, r2
          └───< 0x000020c6       fb0e4481        brlo r6, r5,0x000020be       ;[3]
           ││    0x000020ca       04100314        ld.ab r3, [r8, 4]
           ││    0x000020ce       00233e81        add.f 0, r3, r4
           ││    0x000020d2       da07c1ff        bz 0x000020aa                ;[4]
           ││    0x000020d6       8a20ff0f        mov r0, -1
```

Same excerpt - after Radare2 fixes

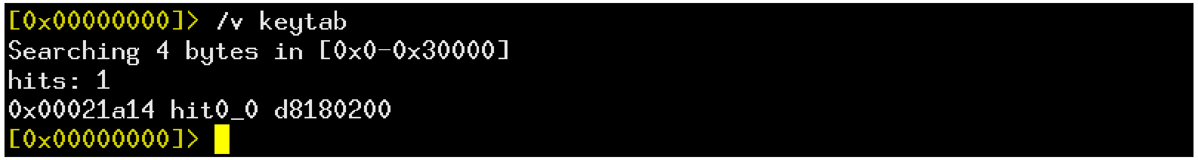
Radare is powerful

- Improving it helped me learn it
- Used it to return to looking for structures



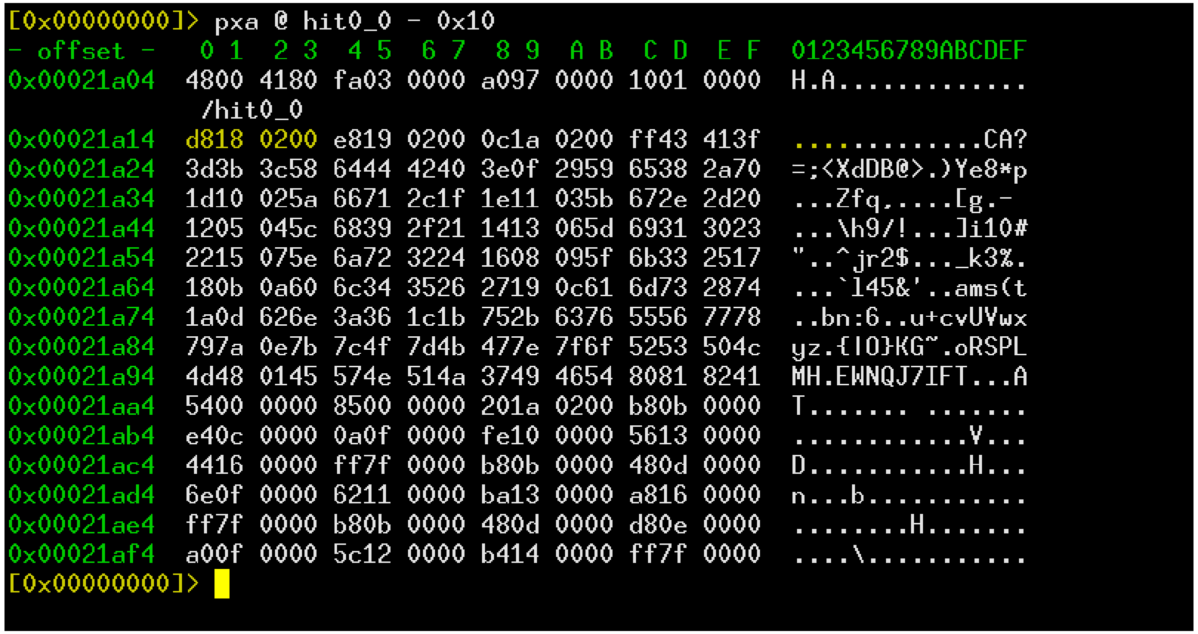
```
[0x00000000]> x 272 @ 0x218d8
- offset -   0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0x000218d8  0102 1110 1f6e 2e83 0000 0000 0000 0000  .....n..........
0x000218e8  7003 121e 202d 2f00 0000 0000 0000 0000  p... -/.........
0x000218f8  7104 1372 2173 3000 0000 0000 0000 0000  q..r!s0.........
0x00021908  0605 1415 2223 3132 0000 0000 0000 0000  ...."#12........
0x00021918  0708 1716 2524 3433 0000 0000 0000 0000  ....%$43........
0x00021928  0d09 181c 2675 3538 0000 0000 0000 0000  ....&u58........
0x00021938  770a 1976 2784 3685 0000 0000 0000 0000  w..v'.6.........
0x00021948  0c0b 1a1b 2829 2a37 0000 0000 0000 0000  ....()*7........
0x00021958  7879 0e0f 1d74 2b3d 0000 0000 0000 0000  xy...t+=........
0x00021968  007b 009b 0000 0059 0000 0000 0000 0000  .{.....Y........
0x00021978  507a 9a99 9897 a054 0000 0000 0000 0000  Pz.....T........
0x00021988  4c4b 0000 7c00 5556 0000 0000 0000 0000  LK..|.UV........
0x00021998  0051 0000 0053 004f 0000 0000 0000 0000  .Q...S.O........
0x000219a8  0000 0000 003c 003e 0000 0000 0000 0000  .....<.>........
0x000219b8  0000 002c 0000 3900 0000 0000 0000 0000  ...,..9.........
0x000219c8  3a00 0000 0000 4000 0000 0000 0000 0096  :.....@.........
0x000219d8  009d 009e 9f4a 3a9c 7d7e 0000 0000 0000  .....J:.}~......
[0x00000000]> f keytab 272 @ 0x218d8
[0x00000000]> 
```

Naming the keytab



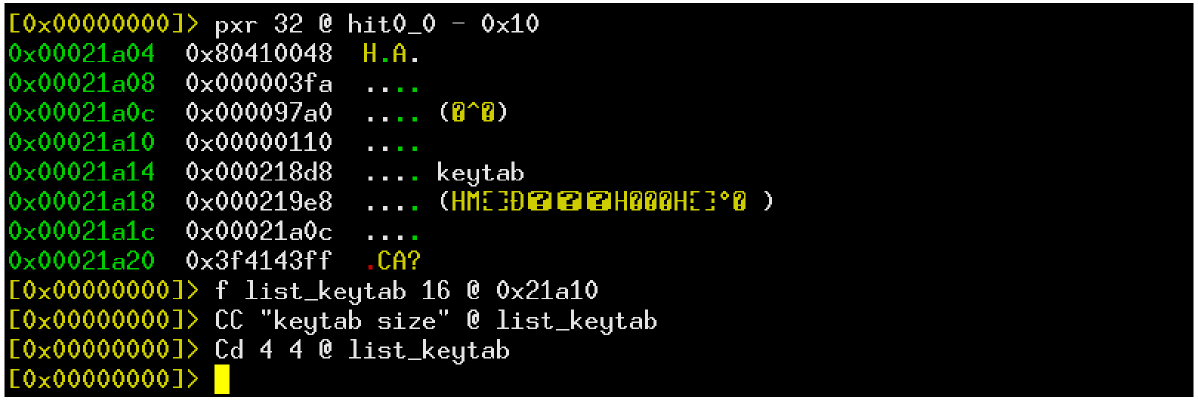
```
[0x00000000]> /v keytab
Searching 4 bytes in [0x0-0x30000]
hits: 1
0x00021a14 hit0_0 d8180200
[0x00000000]>
```

Searching for references



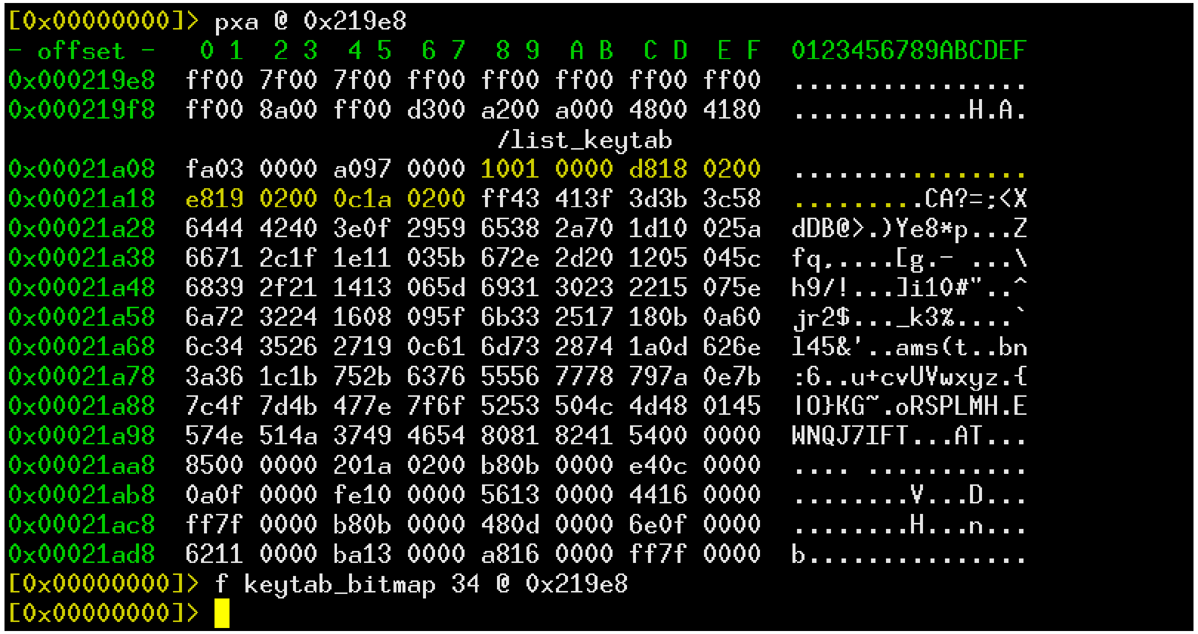
```
[0x00000000]> pxa @ hit0_0 - 0x10
- offset -   0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0x00021a04  4800 4180 fa03 0000 a097 0000 1001 0000  H.A.............
             /hit0_0
0x00021a14  d818 0200 e819 0200 0c1a 0200 ff43 413f  .............CA?
0x00021a24  3d3b 3c58 6444 4240 3e0f 2959 6538 2a70  =;<XdDB@>.)Ye8*p
0x00021a34  1d10 025a 6671 2c1f 1e11 035b 672e 2d20  ...Zfq,....[g.- 
0x00021a44  1205 045c 6839 2f21 1413 065d 6931 3023  ...\h9/!...]i10#
0x00021a54  2215 075e 6a72 3224 1608 095f 6b33 2517  "..^jr2$..._k3%.
0x00021a64  180b 0a60 6c34 3526 2719 0c61 6d73 2874  ...`l45&'..ams(t
0x00021a74  1a0d 626e 3a36 1c1b 752b 6376 5556 7778  ..bn:6..u+cvUVwx
0x00021a84  797a 0e7b 7c4f 7d4b 477e 7f6f 5253 504c  yz.{|O}KG~.oRSPL
0x00021a94  4d48 0145 574e 514a 3749 4654 8081 8241  MH.EWNQJ7IFT...A
0x00021aa4  5400 0000 8500 0000 201a 0200 b80b 0000  T....... .......
0x00021ab4  e40c 0000 0a0f 0000 fe10 0000 5613 0000  ............V...
0x00021ac4  4416 0000 ff7f 0000 b80b 0000 480d 0000  D...........H...
0x00021ad4  6e0f 0000 6211 0000 ba13 0000 a816 0000  n...b...........
0x00021ae4  ff7f 0000 b80b 0000 480d 0000 d80e 0000  ........H.......
0x00021af4  a00f 0000 5c12 0000 b414 0000 ff7f 0000  ....\...........
[0x00000000]> 
```

Dumping the found ref



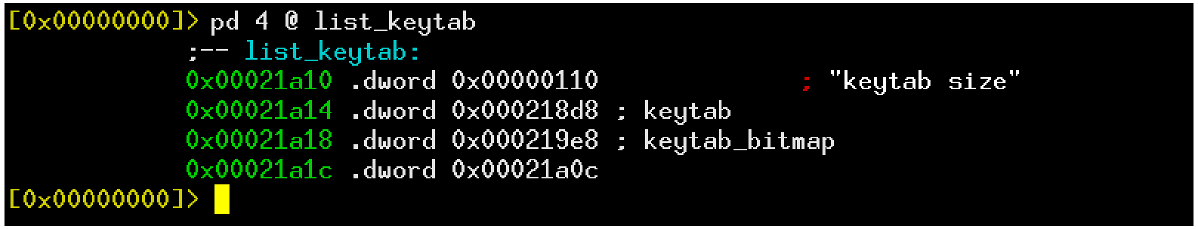
```
[0x00000000]> pxr 32 @ hit0_0 - 0x10
0x00021a04  0x80410048  H.A.
0x00021a08  0x000003fa  ....
0x00021a0c  0x000097a0  .... (�^�)
0x00021a10  0x00000110  ....
0x00021a14  0x000218d8  .... keytab
0x00021a18  0x000219e8  .... (HM[]D���H���H[]°� )
0x00021a1c  0x00021a0c  ....
0x00021a20  0x3f4143ff  .CA?
[0x00000000]> f list_keytab 16 @ 0x21a10
[0x00000000]> CC "keytab size" @ list_keytab
[0x00000000]> Cd 4 4 @ list_keytab
[0x00000000]> █
```

Different dump format



```
[0x00000000]> pxa @ 0x219e8
- offset -    0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0x000219e8   ff00 7f00 7f00 ff00 ff00 ff00 ff00 ff00  ................
0x000219f8   ff00 8a00 ff00 d300 a200 a000 4800 4180  ............H.A.
                                 /list_keytab
0x00021a08   fa03 0000 a097 0000 1001 0000 d818 0200  ................
0x00021a18   e819 0200 0c1a 0200 ff43 413f 3d3b 3c58  .........CA?=;<X
0x00021a28   6444 4240 3e0f 2959 6538 2a70 1d10 025a  dDB@>.)Ye8*p...Z
0x00021a38   6671 2c1f 1e11 035b 672e 2d20 1205 045c  fq,....[g.- ...\
0x00021a48   6839 2f21 1413 065d 6931 3023 2215 075e  h9/!...]i10#"..^
0x00021a58   6a72 3224 1608 095f 6b33 2517 180b 0a60  jr2$..._k3%....`
0x00021a68   6c34 3526 2719 0c61 6d73 2874 1a0d 626e  l45&'..ams(t..bn
0x00021a78   3a36 1c1b 752b 6376 5556 7778 797a 0e7b  :6..u+cvUVwxyz.{
0x00021a88   7c4f 7d4b 477e 7f6f 5253 504c 4d48 0145  |O}KG~.oRSPLMH.E
0x00021a98   574e 514a 3749 4654 8081 8241 5400 0000  WNQJ7IFT...AT...
0x00021aa8   8500 0000 201a 0200 b80b 0000 e40c 0000  .... ...........
0x00021ab8   0a0f 0000 fe10 0000 5613 0000 4416 0000  ........V...D...
0x00021ac8   ff7f 0000 b80b 0000 480d 0000 6e0f 0000  ........H...n...
0x00021ad8   6211 0000 ba13 0000 a816 0000 ff7f 0000  b...............
[0x00000000]> f keytab_bitmap 34 @ 0x219e8
[0x00000000]>
```

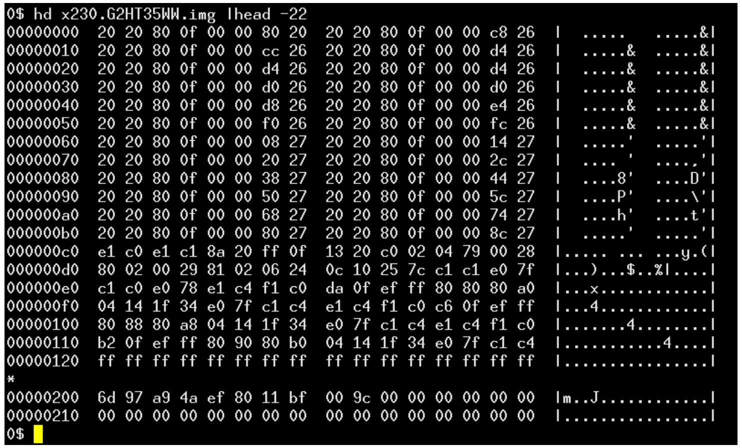
Following the next pointer



```
[0x00000000]> pd 4 @ list_keytab
            ;-- list_keytab:
            0x00021a10 .dword 0x00000110              ; "keytab size"
            0x00021a14 .dword 0x000218d8 ; keytab
            0x00021a18 .dword 0x000219e8 ; keytab_bitmap
            0x00021a1c .dword 0x00021a0c
[0x00000000]> 
```

Show the structure with known details

hd

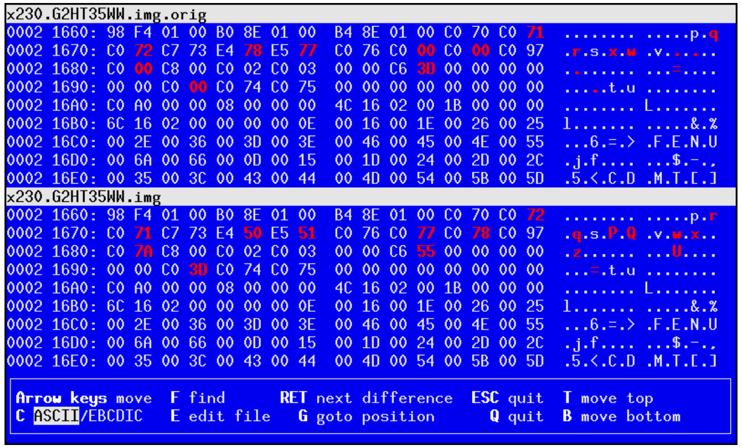


```
0$ hd x230.G2HT35WW.img |head -22
00000000  20 20 80 0f 00 00 80 20  20 20 80 0f 00 00 c8 26  |  .....   .....&|
00000010  20 20 80 0f 00 00 cc 26  20 20 80 0f 00 00 d4 26  |  .....&  .....&|
00000020  20 20 80 0f 00 00 d4 26  20 20 80 0f 00 00 d4 26  |  .....&  .....&|
00000030  20 20 80 0f 00 00 d0 26  20 20 80 0f 00 00 d0 26  |  .....&  .....&|
00000040  20 20 80 0f 00 00 d8 26  20 20 80 0f 00 00 e4 26  |  .....&  .....&|
00000050  20 20 80 0f 00 00 f0 26  20 20 80 0f 00 00 fc 26  |  .....&  .....&|
00000060  20 20 80 0f 00 00 08 27  20 20 80 0f 00 00 14 27  |  .....'  .....'|
00000070  20 20 80 0f 00 00 20 27  20 20 80 0f 00 00 2c 27  |  .... '  ....,'|
00000080  20 20 80 0f 00 00 38 27  20 20 80 0f 00 00 44 27  |  ....8'  ....D'|
00000090  20 20 80 0f 00 00 50 27  20 20 80 0f 00 00 5c 27  |  ....P'  ....\'|
000000a0  20 20 80 0f 00 00 68 27  20 20 80 0f 00 00 74 27  |  ....h'  ....t'|
000000b0  20 20 80 0f 00 00 80 27  20 20 80 0f 00 00 8c 27  |  .....'  .....'|
000000c0  e1 c0 e1 c1 8a 20 ff 0f  13 20 c0 02 04 79 00 28  |..... ... ...y.(|
000000d0  80 02 00 29 81 02 06 24  0c 10 25 7c c1 c1 e0 7f  |...)...$..%|....|
000000e0  c1 c0 e0 78 e1 c4 f1 c0  da 0f ef ff 80 80 80 a0  |...x............|
000000f0  04 14 1f 34 e0 7f c1 c4  e1 c4 f1 c0 c6 0f ef ff  |...4............|
00000100  80 88 80 a8 04 14 1f 34  e0 7f c1 c4 e1 c4 f1 c0  |.......4........|
00000110  b2 0f ef ff 80 90 80 b0  04 14 1f 34 e0 7f c1 c4  |...........4....|
00000120  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
00000200  6d 97 a9 4a ef 80 11 bf  00 9c 00 00 00 00 00 00  |m..J............|
00000210  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
0$
```

- Alias for "hexdump -C"
- Quick and simple hexdumps
- Easy to pipe into other tools

vbindiff

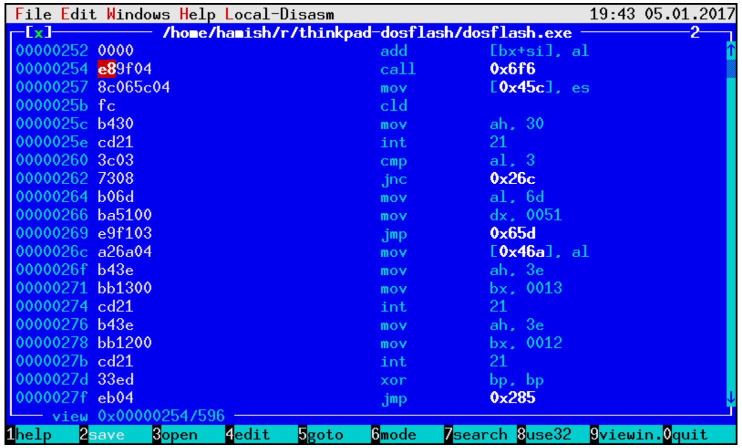
- Visualises binary diffs
- Interactive tool



```
x230.G2HT35WW.img.orig
0002 1660: 98 F4 01 00 B0 8E 01 00  B4 8E 01 00 C0 70 C0 71  ........ .....p.q
0002 1670: C0 72 C7 73 E4 78 E5 77  C0 76 C0 00 C0 00 C0 97  .r.s.x.w .v......
0002 1680: C0 00 C8 00 C0 02 C0 03  00 00 C6 3D 00 00 00 00  ........ ...=....
0002 1690: 00 00 C0 00 C0 74 C0 75  00 00 00 00 00 00 00 00  .....t.u ........
0002 16A0: C0 A0 00 00 08 00 00 00  4C 16 02 00 1B 00 00 00  ........ L.......
0002 16B0: 6C 16 02 00 00 00 00 0E  00 16 00 1E 00 26 00 25  l....... .....&.%
0002 16C0: 00 2E 00 36 00 3D 00 3E  00 46 00 45 00 4E 00 55  ...6.=.> .F.E.N.U
0002 16D0: 00 6A 00 66 00 0D 00 15  00 1D 00 24 00 2D 00 2C  .j.f.... ...$.-.,
0002 16E0: 00 35 00 3C 00 43 00 44  00 4D 00 54 00 5B 00 5D  .5.<.C.D .M.T.[.]
x230.G2HT35WW.img
0002 1660: 98 F4 01 00 B0 8E 01 00  B4 8E 01 00 C0 70 C0 72  ........ .....p.r
0002 1670: C0 71 C7 73 E4 50 E5 51  C0 76 C0 77 C0 78 C0 97  .q.s.P.Q .v.w.x..
0002 1680: C0 7A C8 00 C0 02 C0 03  00 00 C6 55 00 00 00 00  .z...... ...U....
0002 1690: 00 00 C0 3D C0 74 C0 75  00 00 00 00 00 00 00 00  ...=.t.u ........
0002 16A0: C0 A0 00 00 08 00 00 00  4C 16 02 00 1B 00 00 00  ........ L.......
0002 16B0: 6C 16 02 00 00 00 00 0E  00 16 00 1E 00 26 00 25  l....... .....&.%
0002 16C0: 00 2E 00 36 00 3D 00 3E  00 46 00 45 00 4E 00 55  ...6.=.> .F.E.N.U
0002 16D0: 00 6A 00 66 00 0D 00 15  00 1D 00 24 00 2D 00 2C  .j.f.... ...$.-.,
0002 16E0: 00 35 00 3C 00 43 00 44  00 4D 00 54 00 5B 00 5D  .5.<.C.D .M.T.[.]
```

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

hte

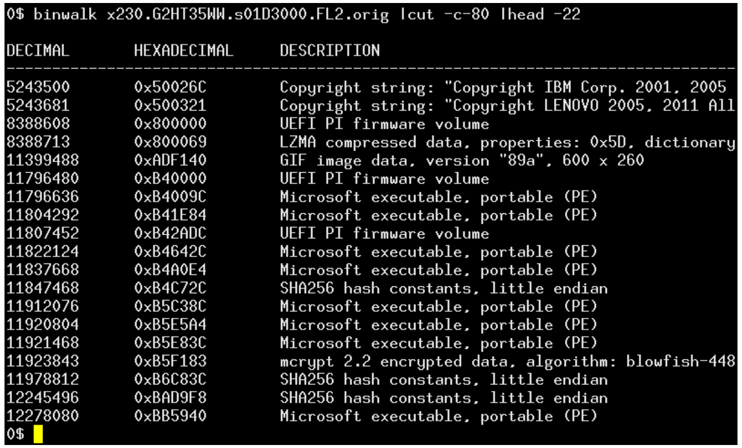


```
File Edit Windows Help Local-Disasm                                 19:43 05.01.2017
[x]        /home/hamish/r/thinkpad-dosflash/dosflash.exe        2
00000252 0000                                       add       [bx+si], al
00000254 e89f04                                     call      0x6f6
00000257 8c065c04                                   mov       [0x45c], es
0000025b fc                                         cld
0000025c b430                                       mov       ah, 30
0000025e cd21                                       int       21
00000260 3c03                                       cmp       al, 3
00000262 7308                                       jnc       0x26c
00000264 b06d                                       mov       al, 6d
00000266 ba5100                                     mov       dx, 0051
00000269 e9f103                                     jmp       0x65d
0000026c a26a04                                     mov       [0x46a], al
0000026f b43e                                       mov       ah, 3e
00000271 bb1300                                     mov       bx, 0013
00000274 cd21                                       int       21
00000276 b43e                                       mov       ah, 3e
00000278 bb1200                                     mov       bx, 0012
0000027b cd21                                       int       21
0000027d 33ed                                       xor       bp, bp
0000027f eb04                                       jmp       0x285
    view 0x00000254/596
1help   2save   3open   4edit   5goto   6mode   7search 8use32  9viewin.0quit
```

- Hex editor (as seen earlier)
- Simple disassembler
- Flexible binary search

binwalk

- Searches bin for contents
- Can extract all found



```
0$ binwalk x230.G2HT35WW.s01D3000.FL2.orig |cut -c-80 |head -22

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
5243500       0x50026C        Copyright string: "Copyright IBM Corp. 2001, 2005
5243681       0x500321        Copyright string: "Copyright LENOVO 2005, 2011 All
8388608       0x800000        UEFI PI firmware volume
8388713       0x800069        LZMA compressed data, properties: 0x5D, dictionary
11399488      0xADF140        GIF image data, version "89a", 600 x 260
11796480      0xB40000        UEFI PI firmware volume
11796636      0xB4009C        Microsoft executable, portable (PE)
11804292      0xB41E84        Microsoft executable, portable (PE)
11807452      0xB42ADC        UEFI PI firmware volume
11822124      0xB4642C        Microsoft executable, portable (PE)
11837668      0xB4A0E4        Microsoft executable, portable (PE)
11847468      0xB4C72C        SHA256 hash constants, little endian
11912076      0xB5C38C        Microsoft executable, portable (PE)
11920804      0xB5E5A4        Microsoft executable, portable (PE)
11921468      0xB5E83C        Microsoft executable, portable (PE)
11923843      0xB5F183        mcrypt 2.2 encrypted data, algorithm: blowfish-448
11978812      0xB6C83C        SHA256 hash constants, little endian
12245496      0xBAD9F8        SHA256 hash constants, little endian
12278080      0xBB5940        Microsoft executable, portable (PE)
0$ 
```

Chapter 4: Firmware Patching

Looking for structures

- EC Firmware has a large data section
- Data turns out to be a large number of lists of lists

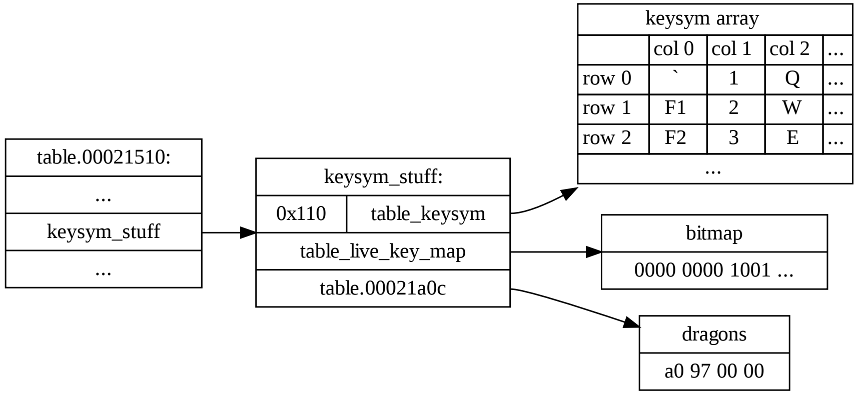


table.00021510:

…

keysym_stuff

…

keysym_stuff:

0x110	table_keysym

table_live_key_map

table.00021a0c

keysym array

	col 0	col 1	col 2	…
row 0	`	1	Q	…
row 1	F1	2	W	…
row 2	F2	3	E	…

…

bitmap

0000 0000 1001 …

dragons

a0 97 00 00

Collaboration

- Connect with Nitrocaster - points me at the 'live key bitmap'
- Together, we find the structure for "both" kinds of Fn+Combo key maps

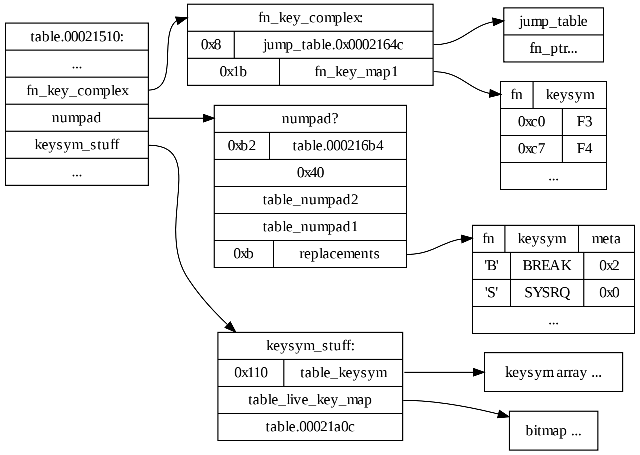


table.00021510:
...
fn_key_complex
numpad
keysym_stuff
...

fn_key_complex:
0x8 jump_table.0x0002164c
0x1b fn_key_map1

jump_table
fn_ptr...

fn	keysym
0xc0	F3
0xc7	F4
...	

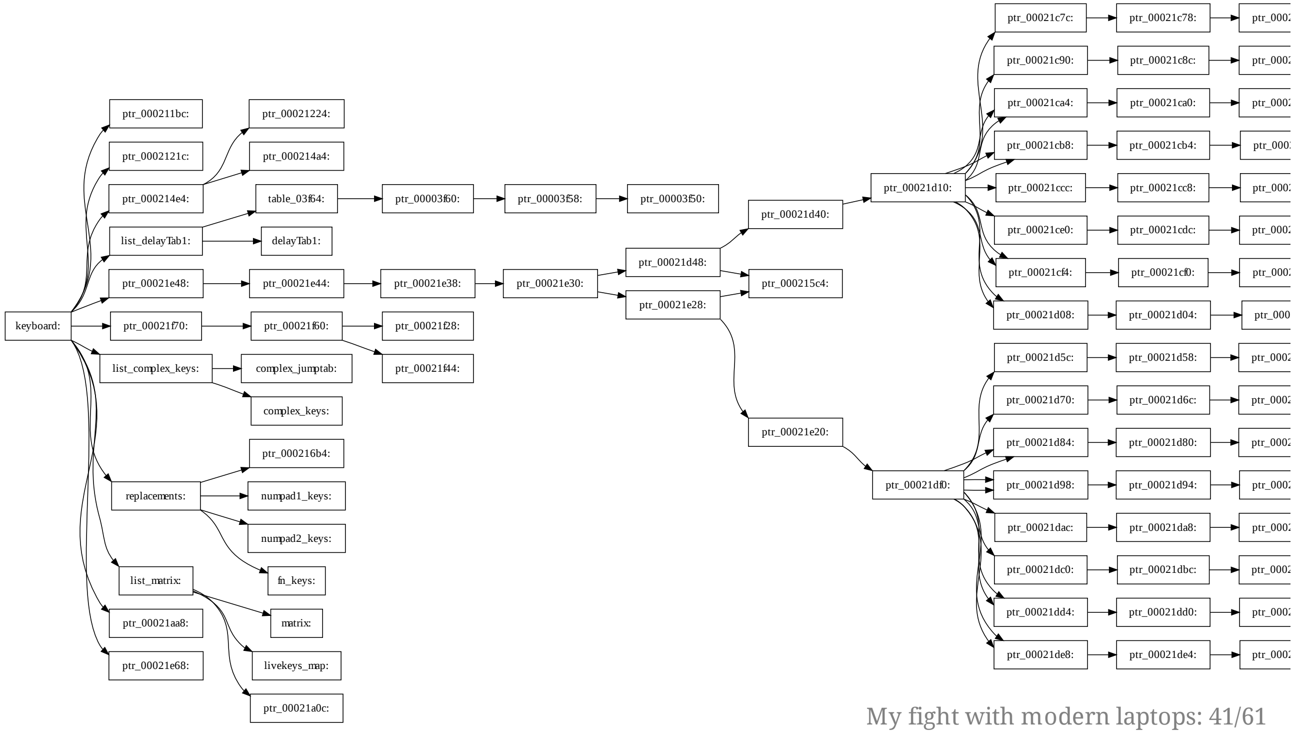
numpad?
0xb2 table.000216b4
0x40
table_numpad2
table_numpad1
0xb replacements

fn	keysym	meta
'B'	BREAK	0x2
'S'	SYSRQ	0x0
...		

keysym_stuff:
0x110 table_keysym
table_live_key_map
table.00021a0c

keysym array ...

bitmap ...



keyboard:

ptr_000211bc:
ptr_0002121c:
ptr_000214e4:
list_delayTab1:
ptr_00021e48:
ptr_00021f70:
list_complex_keys:
replacements:
list_matrix:
ptr_00021aa8:
ptr_00021e68:

ptr_00021224:
ptr_000214a4:
table_03f64:
delayTab1:
ptr_00021e44:
ptr_00021f60:
complex_jumptab:
complex_keys:
ptr_000216b4:
numpad1_keys:
numpad2_keys:
fn_keys:
matrix:
livekeys_map:
ptr_00021a0c:

ptr_00003f60:
ptr_00021e38:
ptr_00021f28:
ptr_00021f44:

ptr_00003f58:
ptr_00021e30:

ptr_00003f50:
ptr_00021d48:
ptr_00021e28:

ptr_00021d40:
ptr_000215c4:
ptr_00021e20:

ptr_00021d10:
ptr_00021df0:

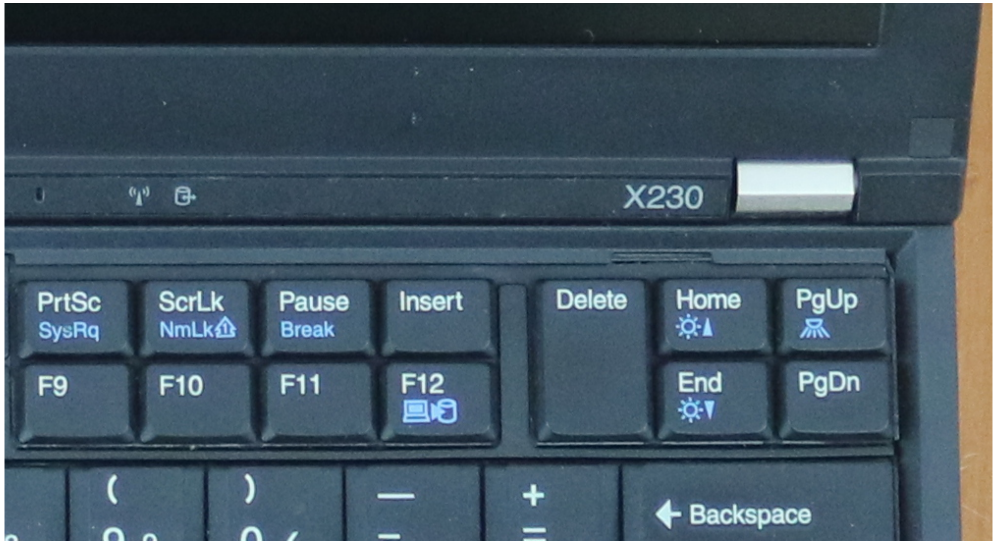
ptr_00021c7c:
ptr_00021c90:
ptr_00021ca4:
ptr_00021cb8:
ptr_00021ccc:
ptr_00021ce0:
ptr_00021cf4:
ptr_00021d08:
ptr_00021d5c:
ptr_00021d70:
ptr_00021d84:
ptr_00021d98:
ptr_00021dac:
ptr_00021dc0:
ptr_00021dd4:
ptr_00021de8:

ptr_00021c78:
ptr_00021c8c:
ptr_00021ca0:
ptr_00021cb4:
ptr_00021cc8:
ptr_00021cdc:
ptr_00021cf0:
ptr_00021d04:
ptr_00021d58:
ptr_00021d6c:
ptr_00021d80:
ptr_00021d94:
ptr_00021da8:
ptr_00021dbc:
ptr_00021dd0:
ptr_00021de4:

ptr_0002
ptr_0002
ptr_0002
ptr_0002
ptr_0002
ptr_0002
ptr_0002
ptr_000
ptr_0002
ptr_0002
ptr_0002
ptr_0002
ptr_0002
ptr_0002
ptr_0002
ptr_0002

Success!

- After patching, a functionally complete replacement

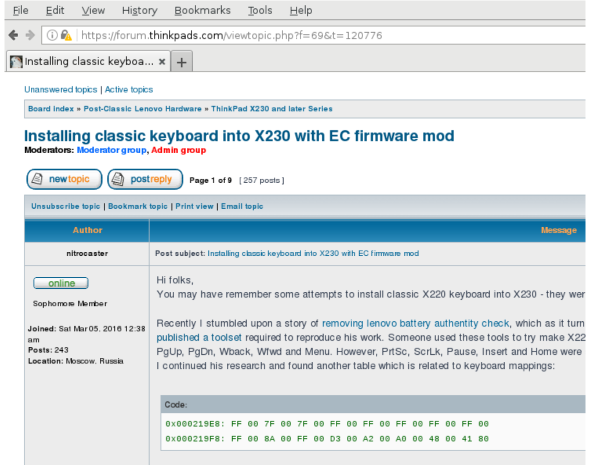


Hacked x230

Chapter 5: Community

Initial publish

- Nitrocaster starts a thinkpads.com forum thread
- We explain what we have done
- People can't really follow easily


File Edit View History Bookmarks Tools Help
https://forum.thinkpads.com/viewtopic.php?f=69&t=120776
Installing classic keyboa... ×
+
Unanswered topics | Active topics
Board index » Post-Classic Lenovo Hardware » ThinkPad X230 and later Series
newtopic
postreply
Unsubscribe topic | Bookmark topic | Print view | Email topic
online

Installing classic keyboard into X230 with EC firmware mod

Moderators: Moderator group, Admin group

Page 1 of 9 [257 posts]

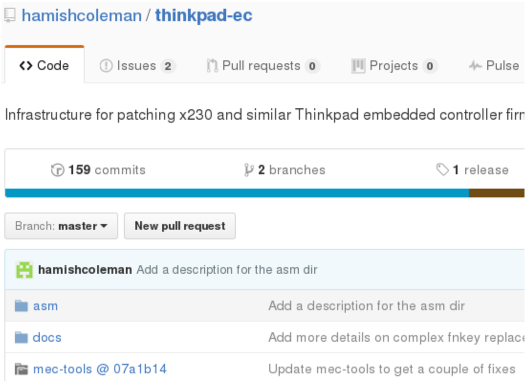
Author	Message
nitrocaster	Post subject: Installing classic keyboard into X230 with EC firmware mod
Sophomore Member Joined: Sat Mar 05. 2016 12:38 am Posts: 243 Location: Moscow. Russia	Hi folks, You may have remember some attempts to install classic X220 keyboard into X230 - they wer Recently I stumbled upon a story of removing lenovo battery authentity check, which as it turn published a toolset required to reproduce his work. Someone used these tools to try make X22 PgUp, PgDn, Wback, Wfwd and Menu. However, PrtSc, ScrLk, Pause, Insert and Home were I continued his research and found another table which is related to keyboard mappings:

Code:

```
0x000219E8: FF 00 7F 00 7F 00 FF 00 FF 00 FF 00 FF 00 FF 00
0x000219F8: FF 00 8A 00 FF 00 D3 00 A2 00 A0 00 48 00 41 80
```

Polishing the project

- Collect all the patches into a repo
- Start writing installation documentation
- Discover who my audience actually is
- Re-write the install docs
- Try to streamline the process



Infrastructure for patching x230 and similar Thinkpad embedded controller firr

hamishcoleman Add a description for the asm dir

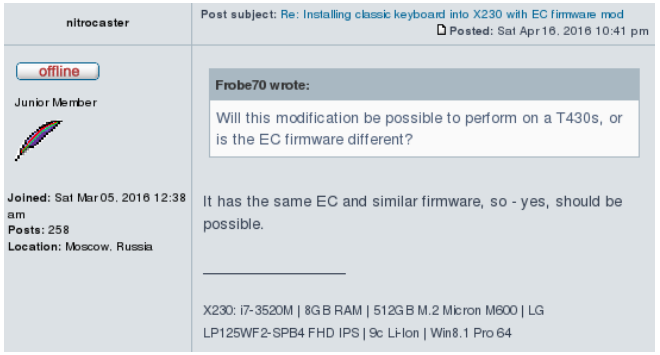
asm	Add a description for the asm dir
docs	Add more details on complex fnkey replace
mec-tools @ 07a1b14	Update mec-tools to get a couple of fixes

Issues with distribution

- What is the licence on the firmware?
- Just how much can I copy out without issues?
- How to make it easy, without infringing?
- What tools are even available?
  - on Windows?

Supporting more hardware

- Originally, just expected x230
- Forum requests kept on appearing (Everyone has their own pet model)
- In the end, support 7 different models (all of the xx30 series)
- Repo structure was assuming just one



nitrocaster

Post subject: Re: Installing classic keyboard into X230 with EC firmware mod

Posted: Sat Apr 16, 2016 10:41 pm

Joined: Sat Mar 05, 2016 12:38 am
Posts: 258
Location: Moscow, Russia

> **Frobe70 wrote:**
>
> Will this modification be possible to perform on a T430s, or is the EC firmware different?

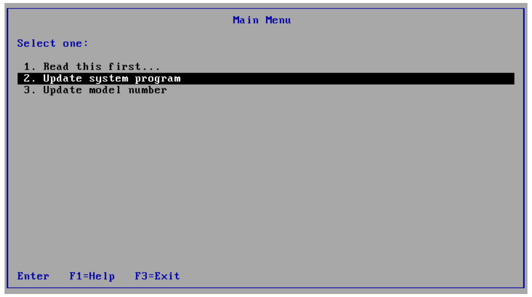
It has the same EC and similar firmware, so - yes, should be possible.

X230: i7-3520M | 8GB RAM | 512GB M.2 Micron M600 | LG LP125WF2-SPB4 FHD IPS | 9c Li-Ion | Win8.1 Pro 64

Chapter 6: Digging into DOSFLASH

Lenovo tools

- Lenovo has a Windows tool, I didn't look at it
- Bootable CD contains "dosflash.exe"
- Boot to PC-DOS, no drivers, clean config
- Runs dosflash
  - Loads firmware, *magic happens*

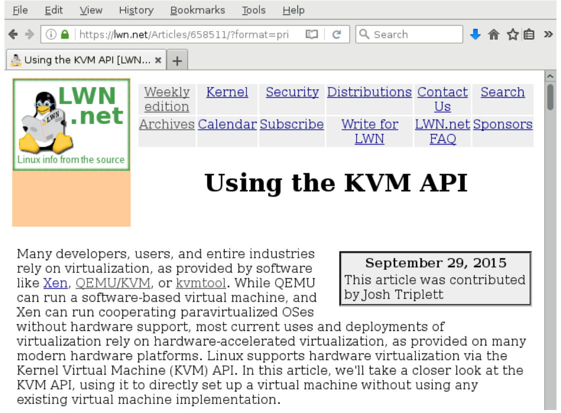


Reversing dosflash

- Need to have a DOS strace tool
- Look at binary, djgpp CWSDPMI
- Have source for djgpp
- Can unpack the flat 32bit bin
- Still no tracing, though

Writing a kvm hypervisor

- "Using the KVM API" - lwn.net
- CWSDPMI interrupt calls
- DOS interrupt calls
- BIOS interrupt calls
- Ralf Brown Interrupt List


File Edit View History Bookmarks Tools Help
https://lwn.net/Articles/658511/?format=pri
Search
Using the KVM API [LWN...
LWN .net
Linux info from the source
Weekly edition
Kernel
Security
Distributions
Contact Us
Search
Archives
Calendar
Subscribe
Write for LWN
LWN.net FAQ
Sponsors

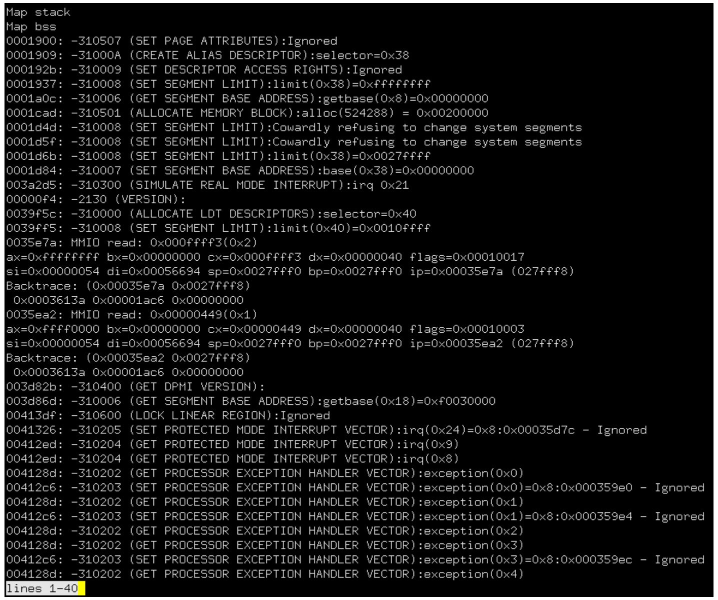
Using the KVM API

September 29, 2015
This article was contributed by Josh Triplett

Many developers, users, and entire industries rely on virtualization, as provided by software like Xen, QEMU/KVM, or kvmtool. While QEMU can run a software-based virtual machine, and Xen can run cooperating paravirtualized OSes without hardware support, most current uses and deployments of virtualization rely on hardware-accelerated virtualization, as provided on many modern hardware platforms. Linux supports hardware virtualization via the Kernel Virtual Machine (KVM) API. In this article, we'll take a closer look at the KVM API, using it to directly set up a virtual machine without using any existing virtual machine implementation.

Keep improving

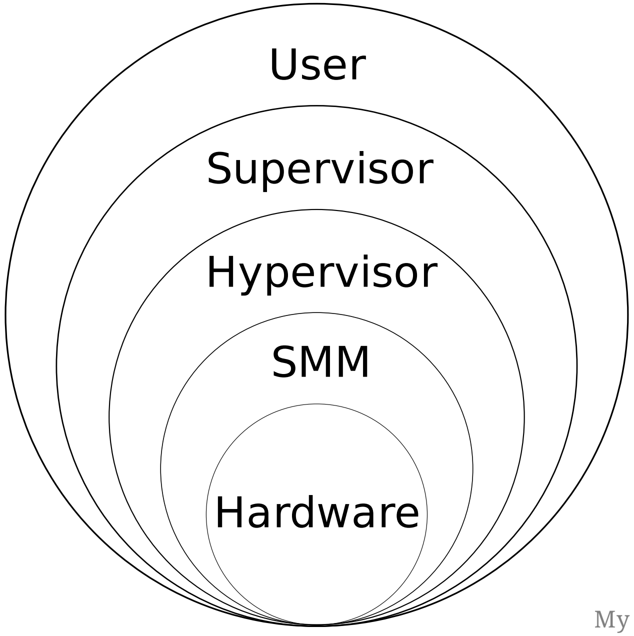
- Trace DOSFLASH.EXE
- Add missing featues (ACPI..)
- Find the SMM calls
- Document Protocol



```
Map stack
Map bss
0001900: -310507 (SET PAGE ATTRIBUTES):Ignored
0001909: -31000A (CREATE ALIAS DESCRIPTOR):selector=0x38
000192b: -310009 (SET DESCRIPTOR ACCESS RIGHTS):Ignored
0001937: -310008 (SET SEGMENT LIMIT):limit(0x38)=0xffffffff
0001a0c: -310006 (GET SEGMENT BASE ADDRESS):getbase(0x8)=0x00000000
0001cad: -310501 (ALLOCATE MEMORY BLOCK):alloc(524288) = 0x00200000
0001d4d: -310008 (SET SEGMENT LIMIT):Cowardly refusing to change system segments
0001d5f: -310008 (SET SEGMENT LIMIT):Cowardly refusing to change system segments
0001d6b: -310008 (SET SEGMENT LIMIT):limit(0x38)=0x0027ffff
0001d84: -310007 (SET SEGMENT BASE ADDRESS):base(0x38)=0x00000000
003a2d5: -310300 (SIMULATE REAL MODE INTERRUPT):irq 0x21
00000f4: -2130 (VERSION):
0039f5c: -310000 (ALLOCATE LDT DESCRIPTORS):selector=0x40
0039ff5: -310008 (SET SEGMENT LIMIT):limit(0x40)=0x0010ffff
0035e7a: MMIO read: 0x000ffff3(0x2)
ax=0xffffffff bx=0x00000000 cx=0x000ffff3 dx=0x00000040 flags=0x00010017
si=0x00000054 di=0x00056694 sp=0x0027fff0 bp=0x0027fff0 ip=0x00035e7a (027fff8)
Backtrace: (0x00035e7a 0x0027fff8)
 0x0003613a 0x00001ac6 0x00000000
0035ea2: MMIO read: 0x00000449(0x1)
ax=0xffff0000 bx=0x00000000 cx=0x00000449 dx=0x00000040 flags=0x00010003
si=0x00000054 di=0x00056694 sp=0x0027fff0 bp=0x0027fff0 ip=0x00035ea2 (027fff8)
Backtrace: (0x00035ea2 0x0027fff8)
 0x0003613a 0x00001ac6 0x00000000
003d82b: -310400 (GET DPMI VERSION):
003d86d: -310006 (GET SEGMENT BASE ADDRESS):getbase(0x18)=0xf0030000
00413df: -310600 (LOCK LINEAR REGION):Ignored
0041326: -310205 (SET PROTECTED MODE INTERRUPT VECTOR):irq(0x24)=0x8:0x00035d7c - Ignored
00412ed: -310204 (GET PROTECTED MODE INTERRUPT VECTOR):irq(0x9)
00412ed: -310204 (GET PROTECTED MODE INTERRUPT VECTOR):irq(0x8)
004128d: -310202 (GET PROCESSOR EXCEPTION HANDLER VECTOR):exception(0x0)
00412c6: -310203 (SET PROCESSOR EXCEPTION HANDLER VECTOR):exception(0x0)=0x8:0x000359e0 - Ignored
004128d: -310202 (GET PROCESSOR EXCEPTION HANDLER VECTOR):exception(0x1)
00412c6: -310203 (SET PROCESSOR EXCEPTION HANDLER VECTOR):exception(0x1)=0x8:0x000359e4 - Ignored
004128d: -310202 (GET PROCESSOR EXCEPTION HANDLER VECTOR):exception(0x2)
004128d: -310202 (GET PROCESSOR EXCEPTION HANDLER VECTOR):exception(0x3)
00412c6: -310203 (SET PROCESSOR EXCEPTION HANDLER VECTOR):exception(0x3)=0x8:0x000359ec - Ignored
004128d: -310202 (GET PROCESSOR EXCEPTION HANDLER VECTOR):exception(0x4)
lines 1-40
```

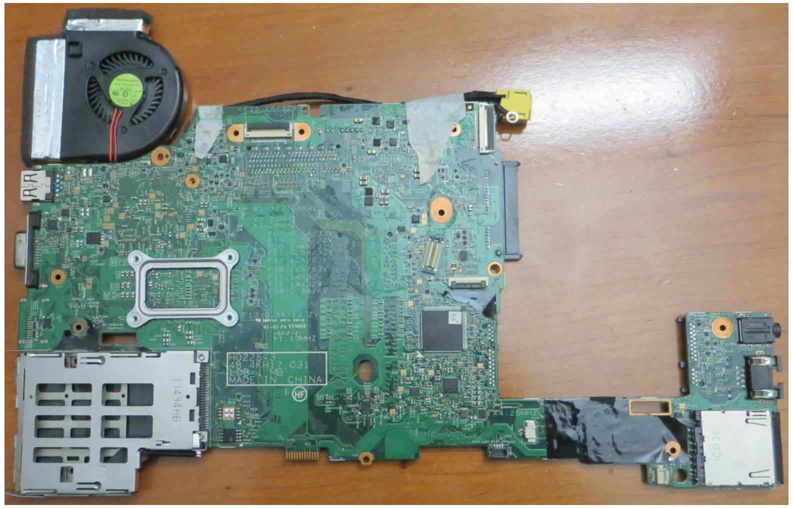
dosflash.exe Call trace

What is SMM, anyway?



Progress stalled

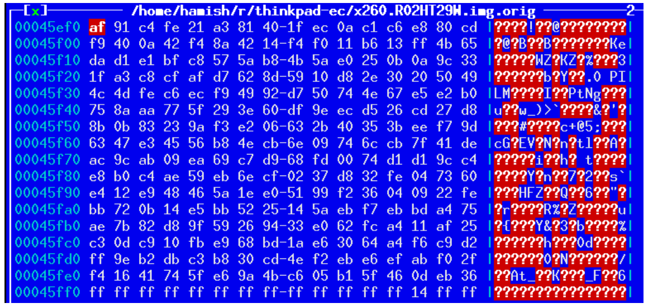
- Need a kernel driver and real hardware (dangerous)



x220 motherboard, ready for destructive testing

How is the firmware protected?

- x220, x230 - parts encrypted
- x250 - better layout, looks similar encryption
- x260 - no encryption, probably cryptographically signed



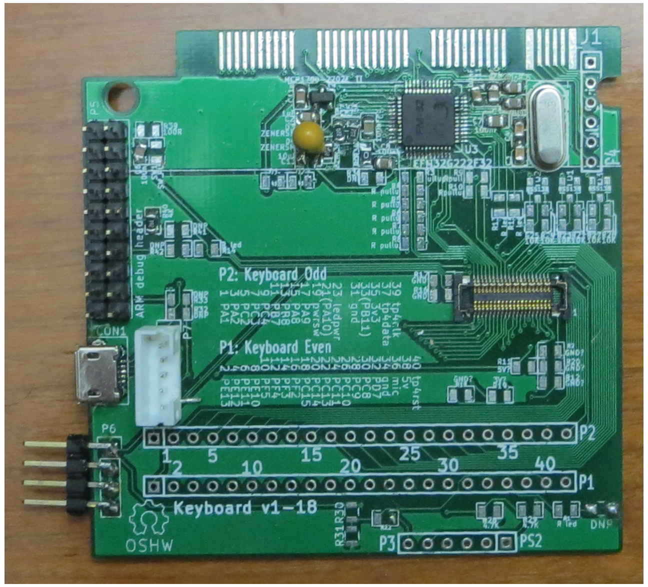
```
[x]            /home/hamish/r/thinkpad-ec/x260.R02HT29W.img.orig            2
00045ef0 af 91 c4 fe 21 a3 81 40-1f ec 0a c1 c6 e8 80 cd |????!??@????????|
00045f00 f9 40 0a 42 f4 8a 42 14-f4 f0 11 b6 13 ff 4b 65 |?@?B??B???????Ke|
00045f10 da d1 e1 bf c8 57 5a b8-4b 5a e0 25 0b 0a 9c 33 |?????WZ?KZ?%???3|
00045f20 1f a3 c8 cf af d7 62 8d-59 10 d8 2e 30 20 50 49 |??????b?Y??.0 PI|
00045f30 4c 4d fe c6 ec f9 49 92-d7 50 74 4e 67 e5 e2 b0 |LM????I??PtNg???|
00045f40 75 8a aa 77 5f 29 3e 60-df 9e ec d5 26 cd 27 d8 |u??w_)>`????&?'?|
00045f50 8b 0b 83 23 9a f3 e2 06-63 2b 40 35 3b ee f7 9d |???#????c+@5;???|
00045f60 63 47 e3 45 56 b8 4e cb-6e 09 74 6c cb 7f 41 de |cG?EV?N?n?tl??A?|
00045f70 ac 9c ab 09 ea 69 c7 d9-68 fd 00 74 d1 d1 9c c4 |?????i??h? t????|
00045f80 e8 b0 c4 ae 59 eb 6e cf-02 37 d8 32 fe 04 73 60 |????Y?n??7?2??s`|
00045f90 e4 12 e9 48 46 5a 1e e0-51 99 f2 36 04 09 22 fe |???HFZ??Q??6??"?|
00045fa0 bb 72 0b 14 e5 bb 52 25-14 5a eb f7 eb bd a4 75 |?r????R%?Z?????u|
00045fb0 ae 7b 82 d8 9f 59 26 94-33 e0 62 fc a4 11 af 25 |?{???Y&?3?b????%|
00045fc0 c3 0d c9 10 fb e9 68 bd-1a e6 30 64 a4 f6 c9 d2 |??????h???0d????|
00045fd0 ff 9e b2 db c3 b8 30 cd-4e f2 eb e6 ef ab f0 2f |??????0?N??????/|
00045fe0 f4 16 41 74 5f e6 9a 4b-c6 05 b1 5f 46 0d eb 36 |??At_??K???_F??6|
00045ff0 ff ff ff ff ff ff ff ff-ff ff ff ff ff 14 ff ff |????????????????|
```

Binary signature?

Winding up

Next Steps

- Enjoy using my 'upgraded' laptop
- Continue tracing SMM
- Build a USB keyboard adaptor
- Try to get newer hardware
- Look for alternative laptops (open?)



Homebrew keyboard-usb adaptor

Questions?

What Hardware do you want to improve?

- github projects:
  - https://github.com/hamishcoleman/thinkpad-ec
  - https://github.com/hamishcoleman/thinkpad-dosflash
  - https://github.com/hamishcoleman/thinkpad-usbkb
- talk slides:
  - http://www.zot.org/~hamish/2017lca.pdf

Hamish Coleman - hamish@zot.org

Some Additional links

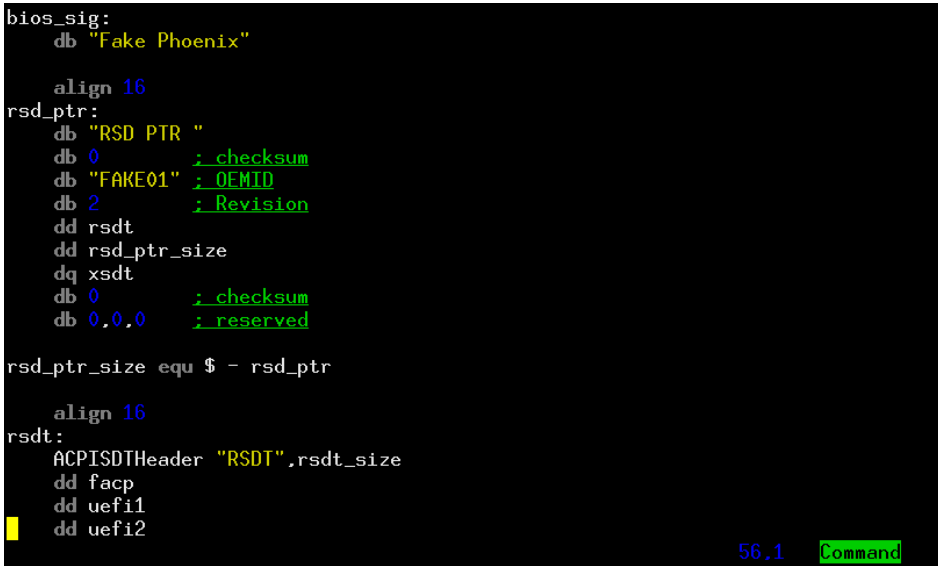
Resources

- Old thinkpad EC disassembly: http://ec.gnost.info/
- Using the KVM API: https://lwn.net/Articles/658511/
- interrupt list: https://www.cs.cmu.edu/~ralf/files.html
- forum.thinkpads.com thread: http://forum.thinkpads.com/viewtopic.php?f=69&t=120776

Tools

- mec tools: https://github.com/eigenmatt/mec-tools
- radare2: http://www.radare.org/r/
- hte: http://hte.sourceforge.net/
- binwalk: http://binwalk.org/
- vbindiff: https://github.com/madsen/vbindiff

Additional slides



```
bios_sig:
    db "Fake Phoenix"

    align 16
rsd_ptr:
    db "RSD PTR "
    db 0         ; checksum
    db "FAKE01" ; OEMID
    db 2         ; Revision
    dd rsdt
    dd rsd_ptr_size
    dq xsdt
    db 0         ; checksum
    db 0,0,0     ; reserved

rsd_ptr_size equ $ - rsd_ptr

    align 16
rsdt:
    ACPISDTHeader "RSDT",rsdt_size
    dd facp
    dd uefi1
    dd uefi2
```

Fake ACPI tables