Fuzzing commands

-> To Fix This: Set CPU Governor to performance

```
cd /sys/devices/system/cpu
echo performance | sudo tee cpu*/cpufreq/scaling_governor
```

-> Build Commands

1. AFL++

Compiles png_check.c using AFL++:

```
afl-clang-fast -o png_check_afl png_check.c
```

2. Honggfuzz

Compiles png_check.c using Honggfuzz compiler wrapper:

```
CC=/usr/local/bin/hfuzz-clang /usr/local/bin/hfuzz-clang -o png_check_hf png_check.c
```

3. LibFuzzer

Compiles fuzz_png_header.c using LibFuzzer:

```
clang -fsanitize=fuzzer,address -o png_check_libfuzz fuzz_png_header.c
```

-> Fuzzer Running Commands

-> **AFL++** — Run for 5 Minutes

```
AFL_SKIP_CPUFREQ=1 afl-fuzz -V 300 -i input_corpus -o afl_out -- ./png_check_afl @@
```

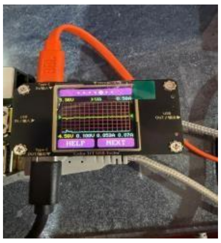
-> **Honggfuzz** — Run for 5 Minutes honggfuzz -i input_corpus
-t 300 -- ./png_check_hf ___FILE___

-> LibFuzzer — Run for 5 Minutes timeout
300 ./png_check_libfuzz

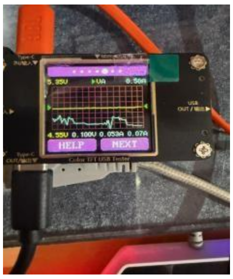
```
-> Radamsa mkdir -p
output/radamsa_out for i in
{1..100}; do

    radamsa input_corpus/seed.png > output/radamsa_out/fuzz_$i.png
./target/png_check_afl output/radamsa_out/fuzz_$i.png done
```

-> Result screenshots

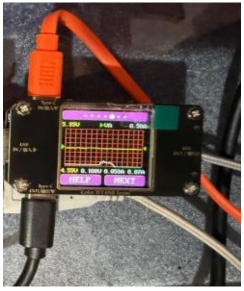
-> AFL++



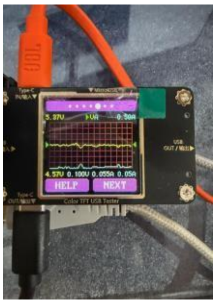
-> LibFuzz



-> HonggFuzz



-> Radamsa


JBL
Type-C
IN/输入
5.37V
VA
0.50A
4.57V 0.100V 0.055A 0.05A
HELP
NEXT
USB
OUT / 输出
Type-C
OUT/输出
Color TFT USB Tester