RSA®Conference2019
San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: SBX3-R1

Wireless Offense and Defense, Explained and Demonstrated!

Rick Mellendick
Chief Security Officer
Process Improvement Achievers, LLC
@rmellendick

piachievers

Rick Farina
Senior Product Line Manager
Aruba
@Zero_ChaosX

aruba
a Hewlett Packard Enterprise company

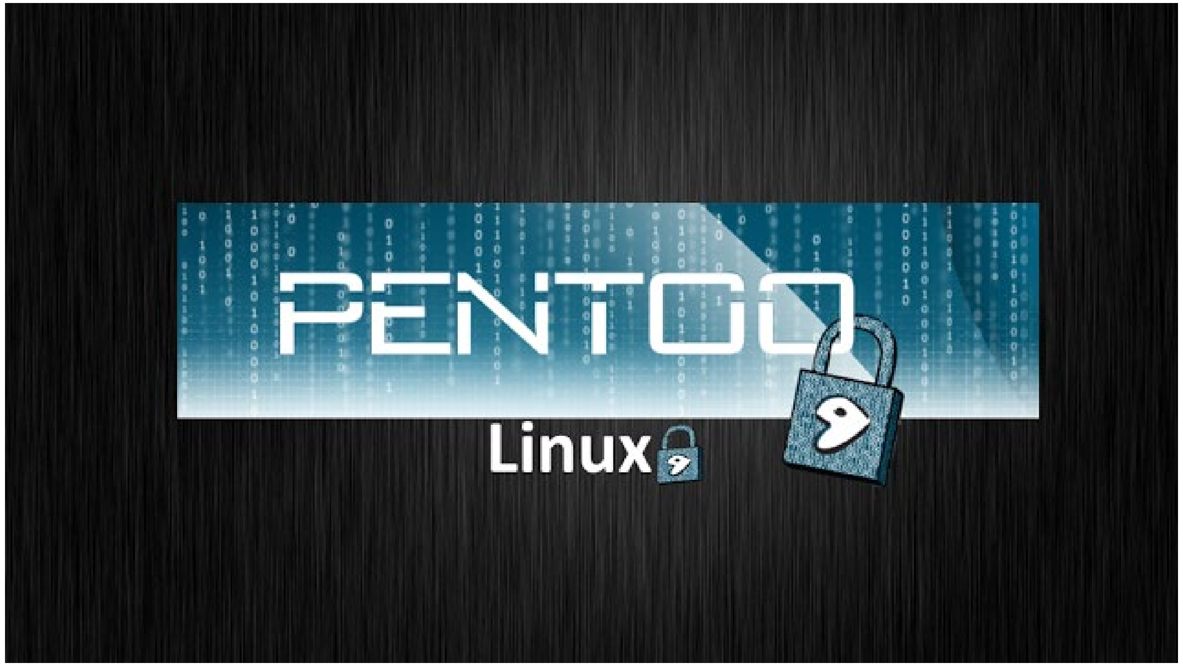
who are we

Rick is the Chief Security Officer for PI Achievers, a process improvement and security firm in Baltimore, Maryland and the developer of the Cyber Resiliency Assessment Methodology (CRAM). Rick specializes in designing and assessing networks using offensive techniques to assist in securing our client's networks.

piachievers aruba a Hewlett Packard Enterprise company

who are we

Rick is a well-known wireless expert who is a frequent speaker at a variety of security conferences including DEF CON. He also runs Wireless Capture the Flag at numerous conventions.



who is the wireless village

Twitter: @Wifi_village and @WCTF_US

Blog: https://wirelessctf.blogspot.com/

Discord: https://discordapp.com/invite/JjPQhKy

*******************DISCLAIMER******************

CAUTION

ALL YOUR RF ARE BELONG TO US!

Your proximity to this device constitues consent to be monitored on all applicable parts of the electro-magnetic spectrum.
You have no chance for privacy make your time.

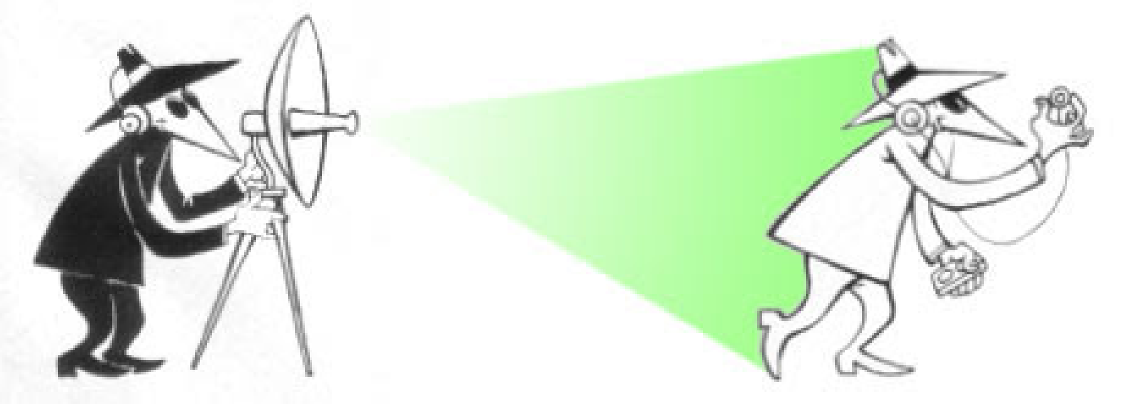
wirelessvillage.ninja WIRELESS VILLAGE www.wctf.us

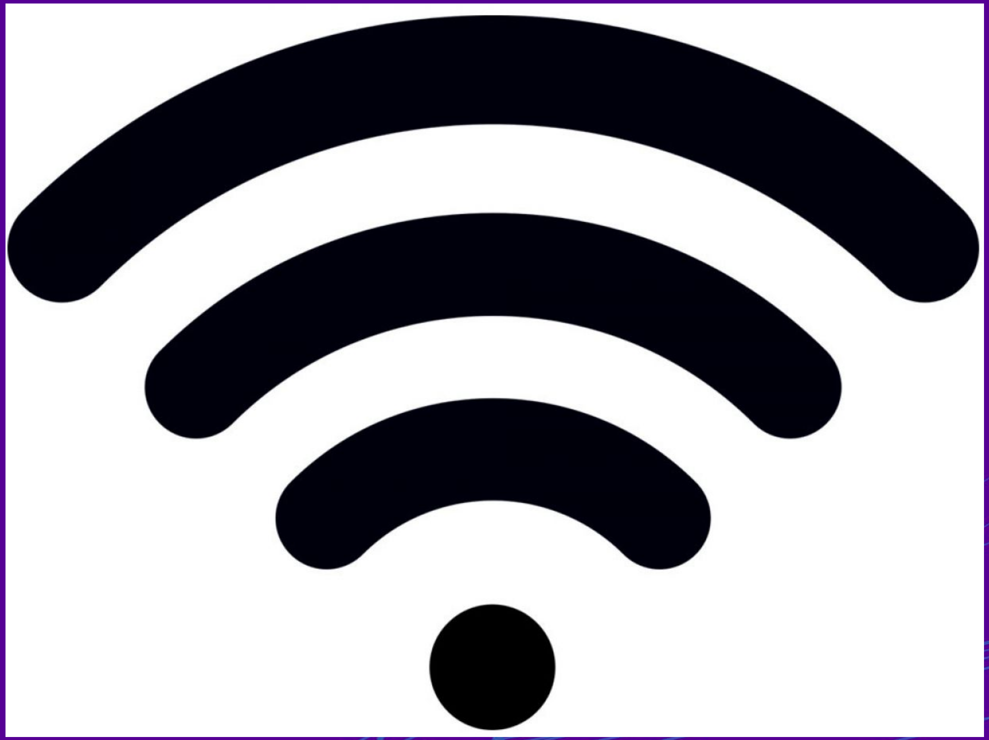
use pentoo

Does he bite?
No, but he can hurt you in other ways.
You can only use Kali in the WCTF

RSA Conference2019

Wireless and Offense Defense Steps to perform both





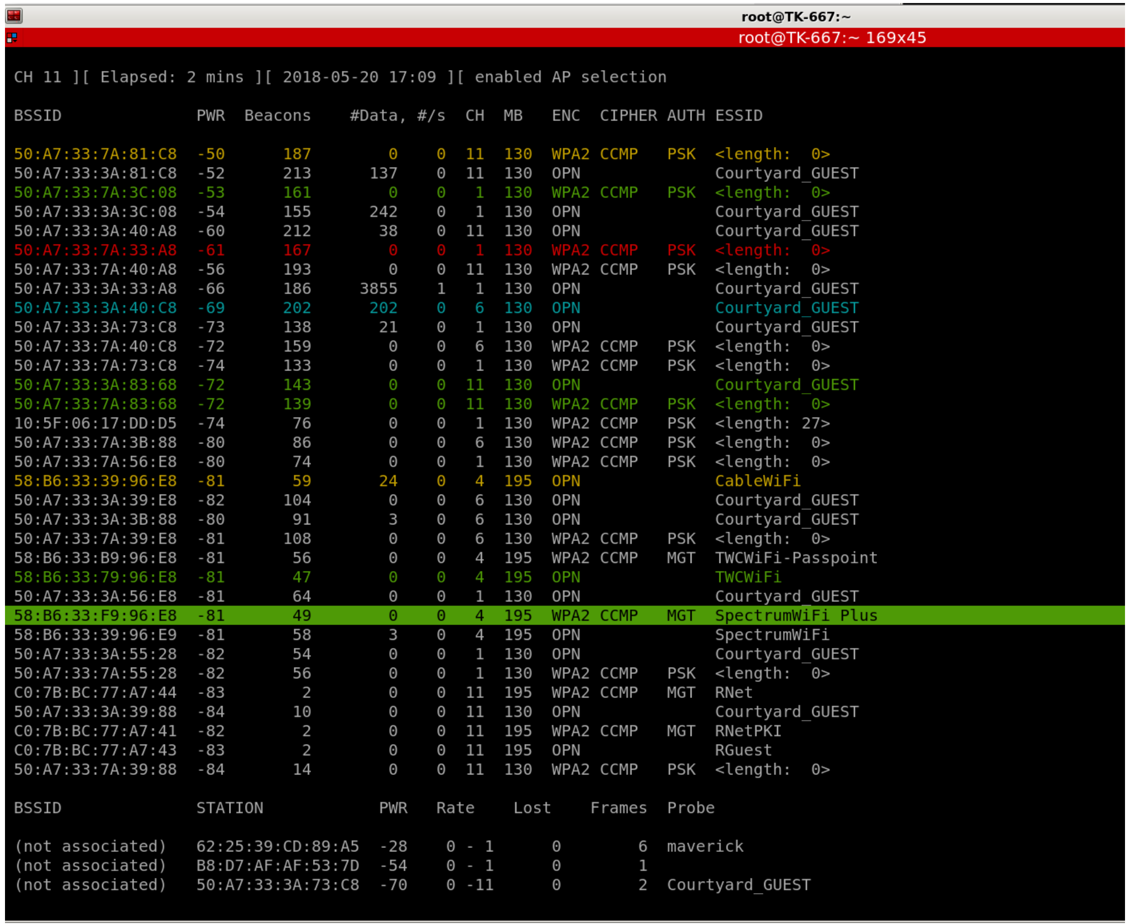
802.11 WiFi

What everyone else calls Wireless

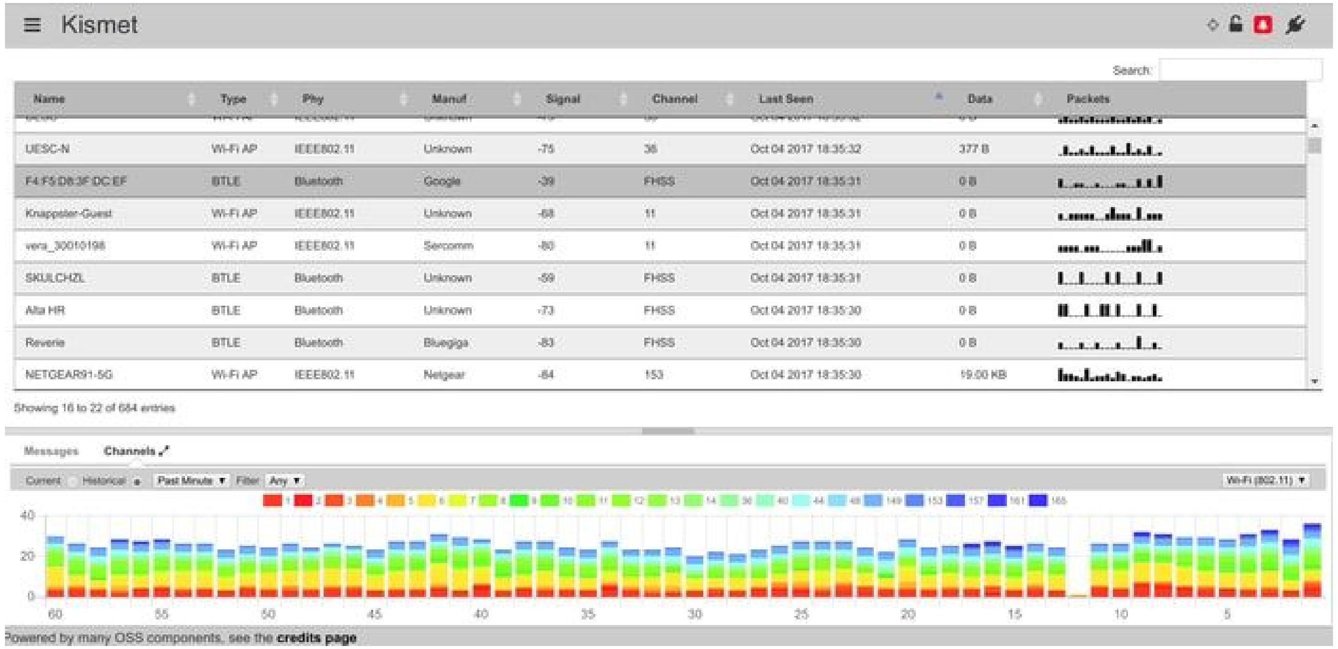
Kismet

Airodump-ng

today we are going to look at 2 wifi tools for enumeration



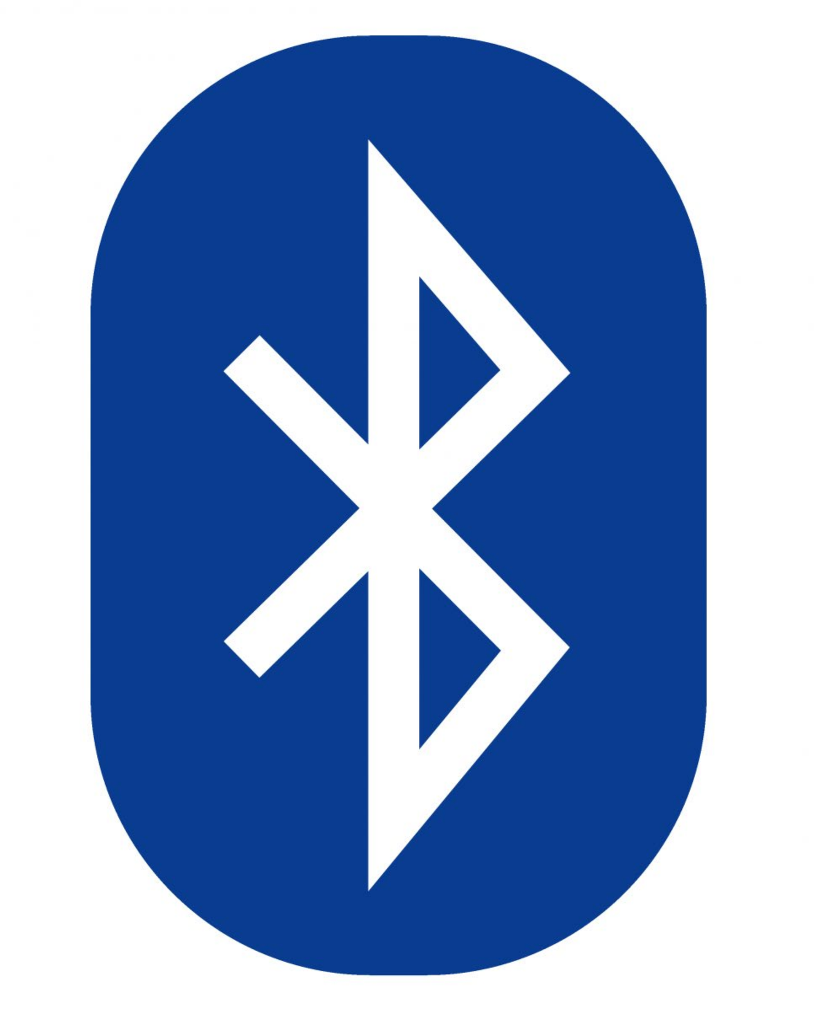
```
CH 11 ][ Elapsed: 2 mins ][ 2018-05-20 17:09 ][ enabled AP selection

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

50:A7:33:7A:81:C8  -50      187        0    0  11  130  WPA2 CCMP   PSK  <length:  0>
50:A7:33:3A:81:C8  -52      213      137    0  11  130  OPN              Courtyard_GUEST
50:A7:33:7A:3C:08  -53      161        0    0   1  130  WPA2 CCMP   PSK  <length:  0>
50:A7:33:3A:3C:08  -54      155      242    0   1  130  OPN              Courtyard_GUEST
50:A7:33:3A:40:A8  -60      212       38    0  11  130  OPN              Courtyard_GUEST
50:A7:33:7A:33:A8  -61      167        0    0   1  130  WPA2 CCMP   PSK  <length:  0>
50:A7:33:7A:40:A8  -56      193        0    0  11  130  WPA2 CCMP   PSK  <length:  0>
50:A7:33:3A:33:A8  -66      186     3855    1   1  130  OPN              Courtyard_GUEST
50:A7:33:3A:40:C8  -69      202      202    0   6  130  OPN              Courtyard_GUEST
50:A7:33:3A:73:C8  -73      138       21    0   1  130  OPN              Courtyard_GUEST
50:A7:33:7A:40:C8  -72      159        0    0   6  130  WPA2 CCMP   PSK  <length:  0>
50:A7:33:7A:73:C8  -74      133        0    0   1  130  WPA2 CCMP   PSK  <length:  0>
50:A7:33:3A:83:68  -72      143        0    0  11  130  OPN              Courtyard_GUEST
50:A7:33:7A:83:68  -72      139        0    0  11  130  WPA2 CCMP   PSK  <length:  0>
10:5F:06:17:DD:D5  -74       76        0    0   1  130  WPA2 CCMP   PSK  <length: 27>
50:A7:33:7A:3B:88  -80       86        0    0   6  130  WPA2 CCMP   PSK  <length:  0>
50:A7:33:7A:56:E8  -80       74        0    0   1  130  WPA2 CCMP   PSK  <length:  0>
58:B6:33:39:96:E8  -81       59       24    0   4  195  OPN              CableWiFi
50:A7:33:3A:39:E8  -82      104        0    0   6  130  OPN              Courtyard_GUEST
50:A7:33:3A:3B:88  -80       91        3    0   6  130  OPN              Courtyard_GUEST
50:A7:33:7A:39:E8  -81      108        0    0   6  130  WPA2 CCMP   PSK  <length:  0>
58:B6:33:B9:96:E8  -81       56        0    0   4  195  WPA2 CCMP   MGT  TWCWiFi-Passpoint
58:B6:33:79:96:E8  -81       47        0    0   4  195  OPN              TWCWiFi
50:A7:33:3A:56:E8  -81       64        0    0   1  130  OPN              Courtyard_GUEST
58:B6:33:F9:96:E8  -81       49        0    0   4  195  WPA2 CCMP   MGT  SpectrumWiFi Plus
58:B6:33:39:96:E9  -81       58        3    0   4  195  OPN              SpectrumWiFi
50:A7:33:3A:55:28  -82       54        0    0   1  130  OPN              Courtyard_GUEST
50:A7:33:7A:55:28  -82       56        0    0   1  130  WPA2 CCMP   PSK  <length:  0>
C0:7B:BC:77:A7:44  -83        2        0    0  11  195  WPA2 CCMP   MGT  RNet
50:A7:33:3A:39:88  -84       10        0    0  11  130  OPN              Courtyard_GUEST
C0:7B:BC:77:A7:41  -82        2        0    0  11  195  WPA2 CCMP   MGT  RNetPKI
C0:7B:BC:77:A7:43  -83        2        0    0  11  195  OPN              RGuest
50:A7:33:7A:39:88  -84       14        0    0  11  130  WPA2 CCMP   PSK  <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   62:25:39:CD:89:A5  -28    0 - 1      0        6  maverick
(not associated)   B8:D7:AF:AF:53:7D  -54    0 - 1      0        1
(not associated)   50:A7:33:3A:73:C8  -70    0 -11      0        2  Courtyard_GUEST
```



Name	Type	Phy	Manuf	Signal	Channel	Last Seen	Data	Packets
UESC-N	Wi-Fi AP	IEEE802.11	Unknown	-75	36	Oct 04 2017 18:35:32	377 B	
F4:F5:D8:3F:DC:EF	BTLE	Bluetooth	Google	-39	FHSS	Oct 04 2017 18:35:31	0 B	
Knappster-Guest	Wi-Fi AP	IEEE802.11	Unknown	-68	11	Oct 04 2017 18:35:31	0 B	
vera_30010198	Wi-Fi AP	IEEE802.11	Sercomm	-80	11	Oct 04 2017 18:35:31	0 B	
SKULCHZL	BTLE	Bluetooth	Unknown	-59	FHSS	Oct 04 2017 18:35:31	0 B	
Alta HR	BTLE	Bluetooth	Unknown	-73	FHSS	Oct 04 2017 18:35:30	0 B	
Reverie	BTLE	Bluetooth	Bluegiga	-83	FHSS	Oct 04 2017 18:35:30	0 B	
NETGEAR91-5G	Wi-Fi AP	IEEE802.11	Netgear	-84	153	Oct 04 2017 18:35:30	19.00 KB	

Showing 16 to 22 of 684 entries

Powered by many OSS components, see the **credits page**



Bluetooth

Bluetooth
SMART

bluetooth connections

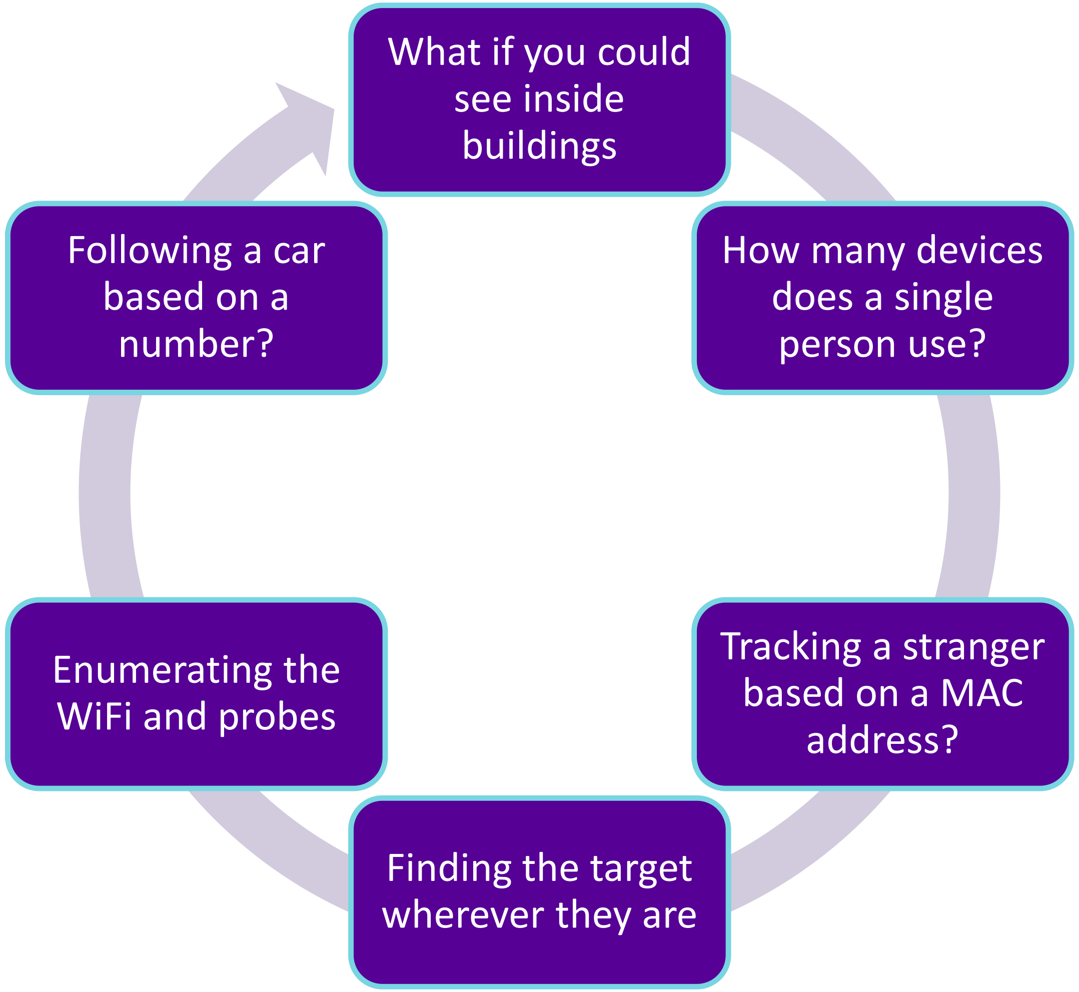
Why can’t we just easily deauth, or work with Bluetooth like we do with WiFi?

internal vs UD100 vs ubertoothone

finding and tracking

Let's just write security on the slide but talk about other things

external enumeration of internal spaces



What if you could see inside buildings

How many devices does a single person use?

Tracking a stranger based on a MAC address?

Finding the target wherever they are

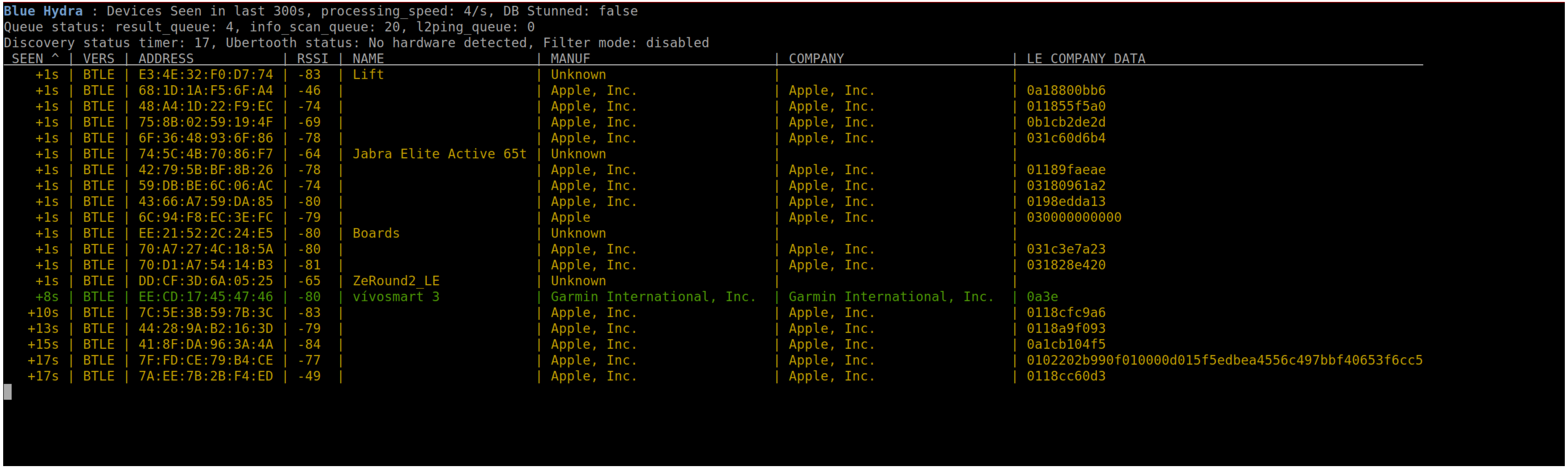
Enumerating the WiFi and probes

Following a car based on a number?

blue_hydra

https://github.com/ZeroChaos-/blue_hydra

initial bluetooth enumeration



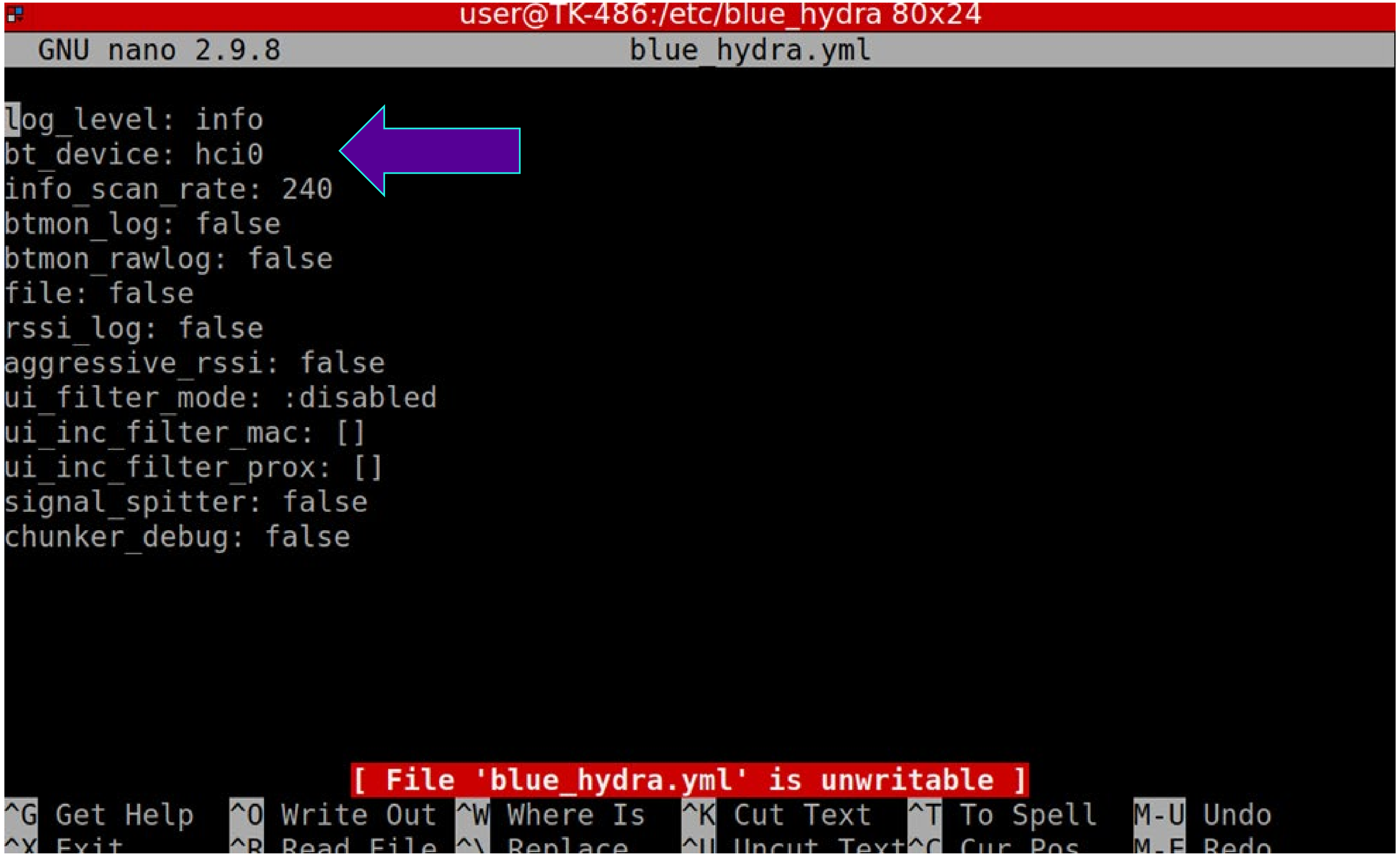
```
Blue Hydra : Devices Seen in last 300s, processing_speed: 4/s, DB Stunned: false
Queue status: result_queue: 4, info_scan_queue: 20, l2ping_queue: 0
Discovery status timer: 17, Ubertooth status: No hardware detected, Filter mode: disabled
 SEEN ^ | VERS | ADDRESS           | RSSI | NAME                   | MANUF                        | COMPANY                      | LE COMPANY DATA
    +1s | BTLE | E3:4E:32:F0:D7:74 | -83  | Lift                   | Unknown                      |                              |
    +1s | BTLE | 68:1D:1A:F5:6F:A4 | -46  |                        | Apple, Inc.                  | Apple, Inc.                  | 0a18800bb6
    +1s | BTLE | 48:A4:1D:22:F9:EC | -74  |                        | Apple, Inc.                  | Apple, Inc.                  | 011855f5a0
    +1s | BTLE | 75:8B:02:59:19:4F | -69  |                        | Apple, Inc.                  | Apple, Inc.                  | 0b1cb2de2d
    +1s | BTLE | 6F:36:48:93:6F:86 | -78  |                        | Apple, Inc.                  | Apple, Inc.                  | 031c60d6b4
    +1s | BTLE | 74:5C:4B:70:86:F7 | -64  | Jabra Elite Active 65t | Unknown                      |                              |
    +1s | BTLE | 42:79:5B:BF:8B:26 | -78  |                        | Apple, Inc.                  | Apple, Inc.                  | 01189faeae
    +1s | BTLE | 59:DB:BE:6C:06:AC | -74  |                        | Apple, Inc.                  | Apple, Inc.                  | 03180961a2
    +1s | BTLE | 43:66:A7:59:DA:85 | -80  |                        | Apple, Inc.                  | Apple, Inc.                  | 0198edda13
    +1s | BTLE | 6C:94:F8:EC:3E:FC | -79  |                        | Apple                        | Apple, Inc.                  | 030000000000
    +1s | BTLE | EE:21:52:2C:24:E5 | -80  | Boards                 | Unknown                      |                              |
    +1s | BTLE | 70:A7:27:4C:18:5A | -80  |                        | Apple, Inc.                  | Apple, Inc.                  | 031c3e7a23
    +1s | BTLE | 70:D1:A7:54:14:B3 | -81  |                        | Apple, Inc.                  | Apple, Inc.                  | 031828e420
    +1s | BTLE | DD:CF:3D:6A:05:25 | -65  | ZeRound2_LE            | Unknown                      |                              |
    +8s | BTLE | EE:CD:17:45:47:46 | -80  | vívosmart 3            | Garmin International, Inc.   | Garmin International, Inc.   | 0a3e
   +10s | BTLE | 7C:5E:3B:59:7B:3C | -83  |                        | Apple, Inc.                  | Apple, Inc.                  | 0118cfc9a6
   +13s | BTLE | 44:28:9A:B2:16:3D | -79  |                        | Apple, Inc.                  | Apple, Inc.                  | 0118a9f093
   +15s | BTLE | 41:8F:DA:96:3A:4A | -84  |                        | Apple, Inc.                  | Apple, Inc.                  | 0a1cb104f5
   +17s | BTLE | 7F:FD:CE:79:B4:CE | -77  |                        | Apple, Inc.                  | Apple, Inc.                  | 0102202b990f010000d015f5edbea4556c497bbf40653f6cc5
   +17s | BTLE | 7A:EE:7B:2B:F4:ED | -49  |                        | Apple, Inc.                  | Apple, Inc.                  | 0118cc60d3
```

blue_hydra fox mode

This will stop the info response which will make the tool much faster on the refresh…

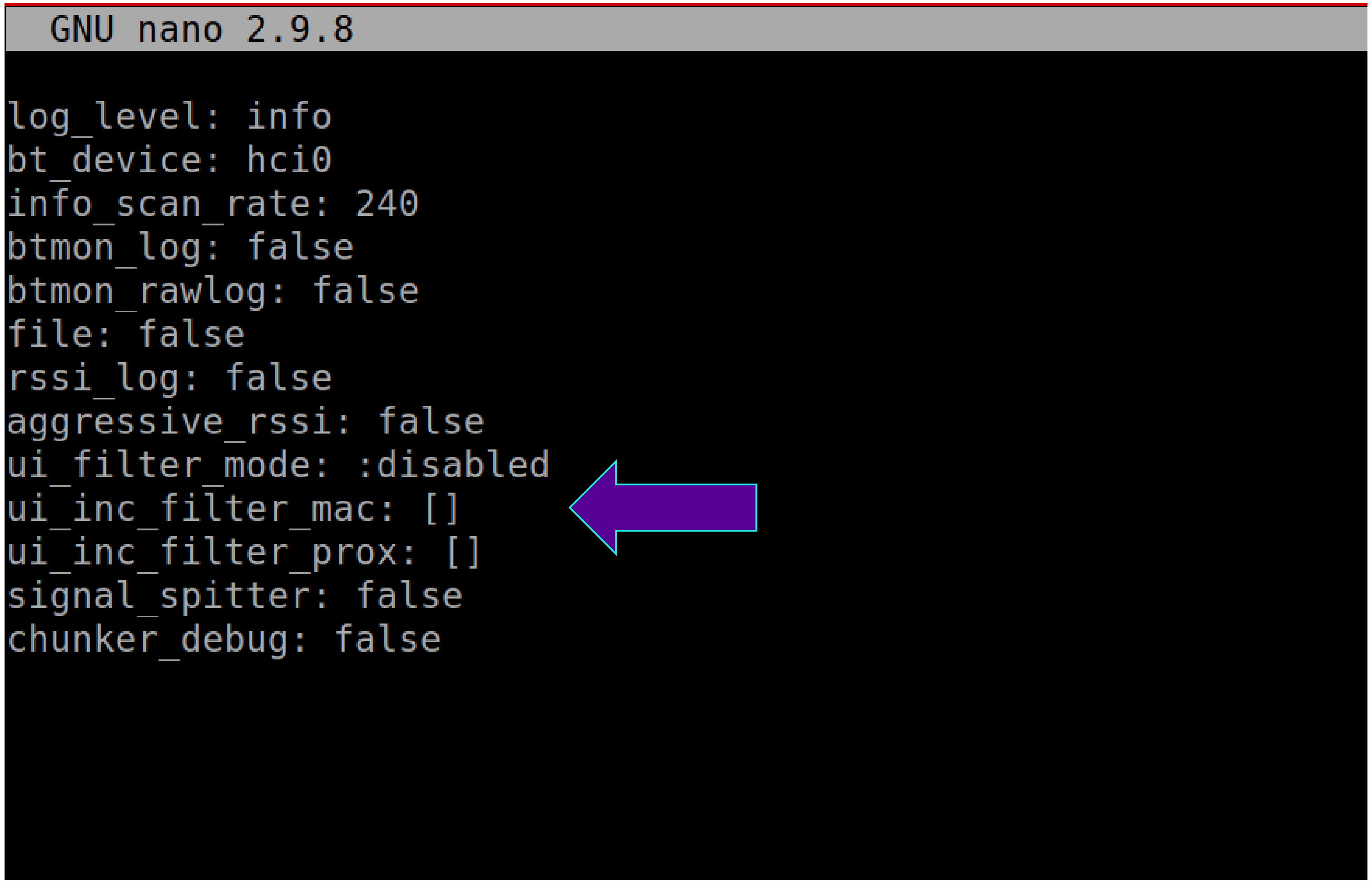
```
sudo blue_hydra –no-info
```

blue_hydra changing the bluetooth adapter



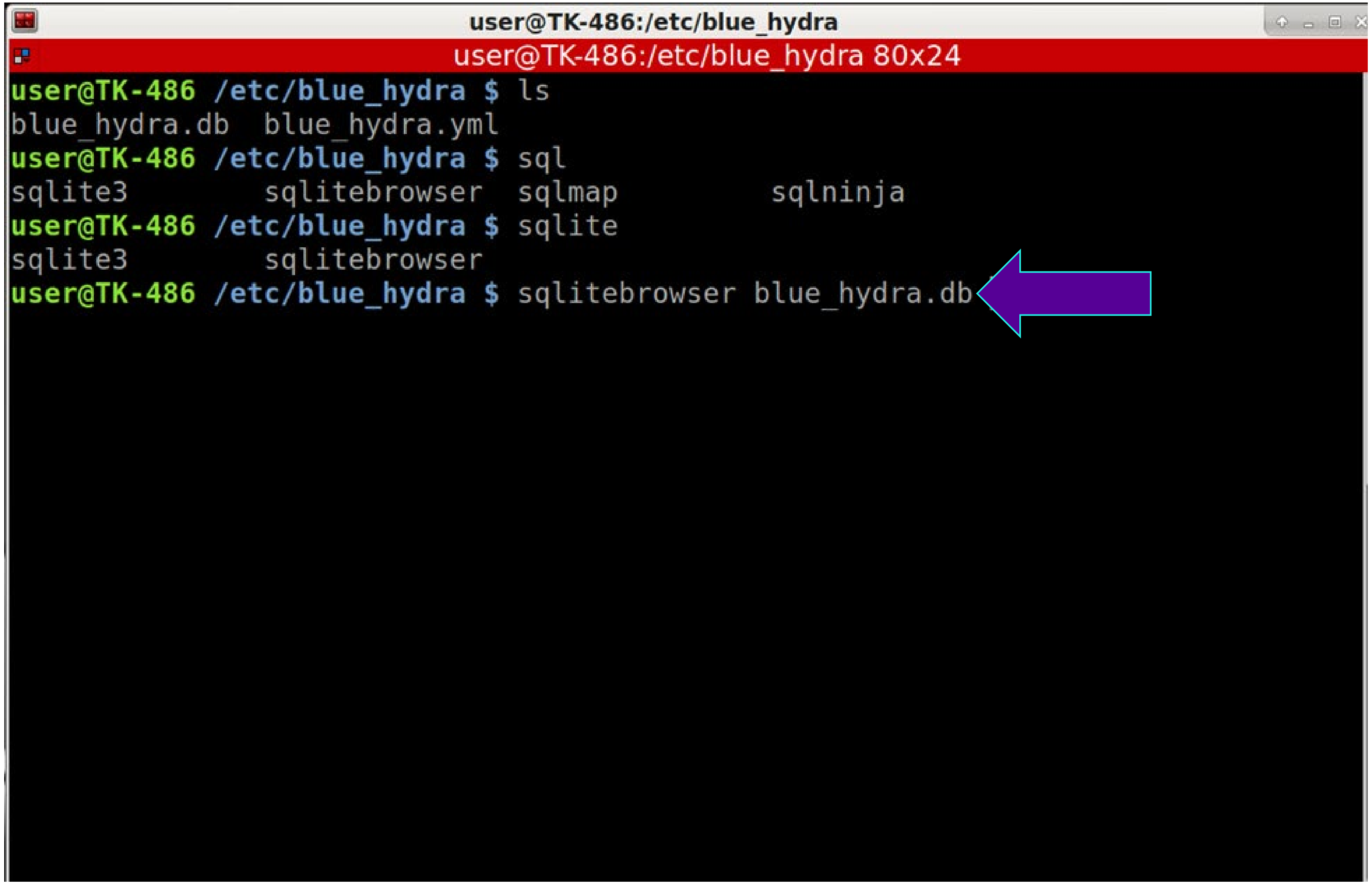
```
user@TK-486:/etc/blue_hydra 80x24
  GNU nano 2.9.8                      blue_hydra.yml

log_level: info
bt_device: hci0
info_scan_rate: 240
btmon_log: false
btmon_rawlog: false
file: false
rssi_log: false
aggressive_rssi: false
ui_filter_mode: :disabled
ui_inc_filter_mac: []
ui_inc_filter_prox: []
signal_spitter: false
chunker_debug: false




                    [ File 'blue_hydra.yml' is unwritable ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^T To Spell    M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text^C Cur Pos       M-E Redo
```

change the filters for blue_hydra
nano /etc/blue_hydra/blue_hydra.yml



```
  GNU nano 2.9.8

log_level: info
bt_device: hci0
info_scan_rate: 240
btmon_log: false
btmon_rawlog: false
file: false
rssi_log: false
aggressive_rssi: false
ui_filter_mode: :disabled
ui_inc_filter_mac: []
ui_inc_filter_prox: []
signal_spitter: false
chunker_debug: false
```

blue_hydra database backend



user@TK-486:/etc/blue_hydra
user@TK-486:/etc/blue_hydra 80x24

```
user@TK-486 /etc/blue_hydra $ ls
blue_hydra.db  blue_hydra.yml
user@TK-486 /etc/blue_hydra $ sql
sqlite3         sqlitebrowser  sqlmap          sqlninja
user@TK-486 /etc/blue_hydra $ sqlite
sqlite3         sqlitebrowser
user@TK-486 /etc/blue_hydra $ sqlitebrowser blue_hydra.db
```

blue_hydra database backend

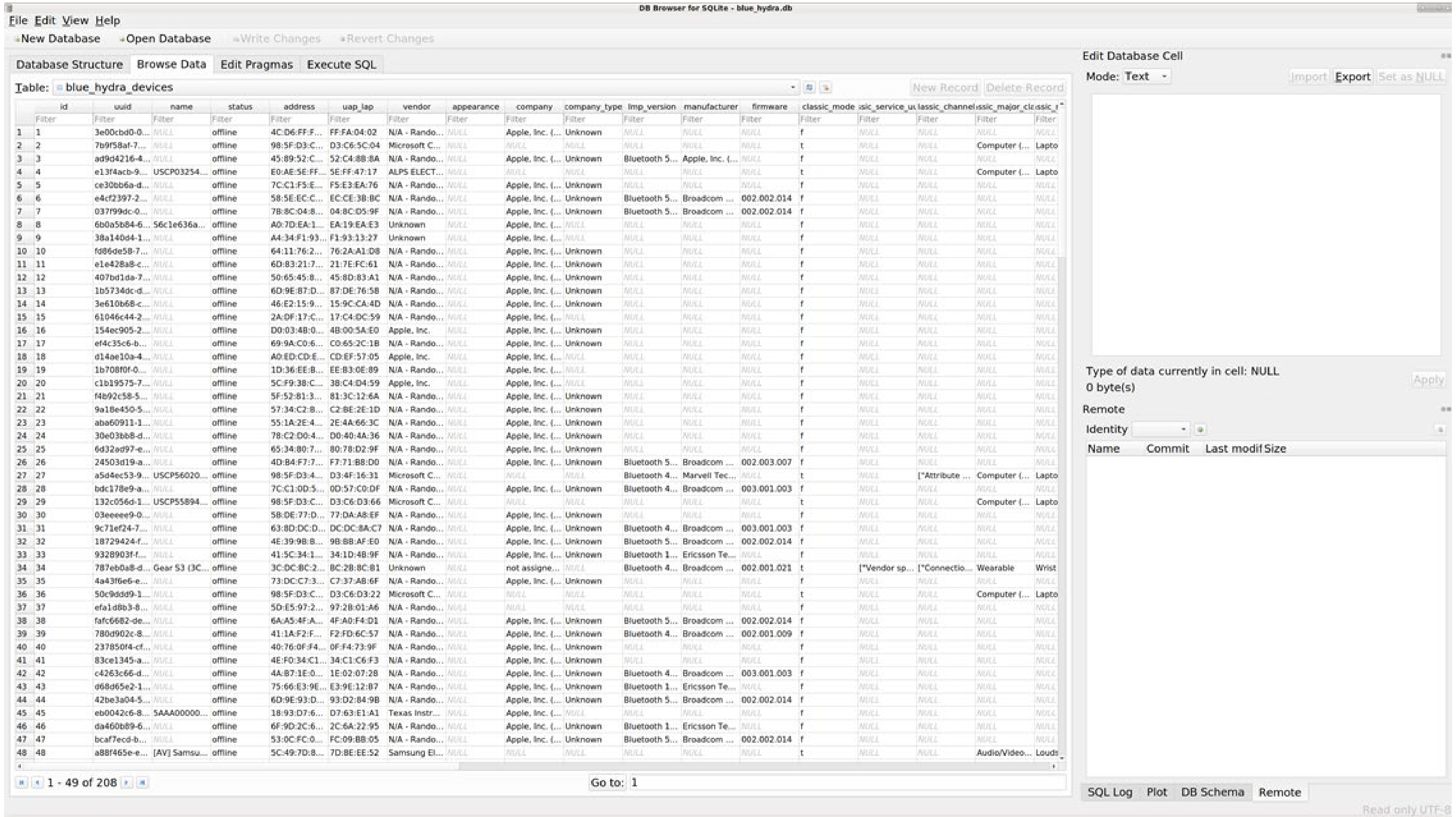


Table: blue_hydra_devices

	id	uuid	name	status	address	uap_lap	vendor	appearance	company	company_type	lmp_version	manufacturer	firmware	classic_mode	sic_service_u	lassic_channel	ssic_major_cl	ssic_r
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	3e00cbd0-0...	NULL	offline	4C:D6:FF:F...	FF:FA:04:02	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
2	2	7b9f58af-7...	NULL	offline	98:5F:D3:C...	D3:C6:5C:04	Microsoft C...	NULL	NULL	NULL	NULL	NULL	NULL	t	NULL	NULL	Computer (...	Lapto
3	3	ad9d4216-4...	NULL	offline	45:89:52:C...	52:C4:88:8A	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	Bluetooth 5...	Apple, Inc. (...	NULL	f	NULL	NULL	NULL	NULL
4	4	e13f4acb-9...	USCP03254...	offline	E0:AE:5E:FF...	5E:FF:47:17	ALPS ELECT...	NULL	NULL	NULL	NULL	NULL	NULL	t	NULL	NULL	Computer (...	Lapto
5	5	ce30bb6a-d...	NULL	offline	7C:C1:F5:E...	F5:E3:EA:76	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
6	6	e4cf2397-2...	NULL	offline	58:5E:EC:C...	EC:CE:3B:BC	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	Bluetooth 5...	Broadcom ...	002.002.014	f	NULL	NULL	NULL	NULL
7	7	037f99dc-0...	NULL	offline	7B:8C:04:8...	04:8C:D5:9F	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	Bluetooth 5...	Broadcom ...	002.002.014	f	NULL	NULL	NULL	NULL
8	8	6b0a5b84-6...	56c1e636a...	offline	A0:7D:EA:1...	EA:19:EA:E3	Unknown	NULL	Apple, Inc. (...	NULL	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
9	9	38a140d4-1...	NULL	offline	A4:34:F1:93...	F1:93:13:27	Unknown	NULL	Apple, Inc. (...	NULL	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
10	10	fd86de58-7...	NULL	offline	64:11:76:2...	76:2A:A1:D8	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
11	11	e1e428a8-c...	NULL	offline	6D:83:21:7...	21:7E:FC:61	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
12	12	407bd1da-7...	NULL	offline	50:65:45:8...	45:8D:83:A1	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
13	13	1b5734dc-d...	NULL	offline	6D:9E:87:D...	87:DE:76:58	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
14	14	3e610b68-c...	NULL	offline	46:E2:15:9...	15:9C:CA:4D	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
15	15	61046c44-2...	NULL	offline	2A:DF:17:C...	17:C4:DC:59	N/A - Rando...	NULL	Apple, Inc. (...	NULL	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
16	16	154ec905-2...	NULL	offline	D0:03:4B:0...	4B:00:5A:E0	Apple, Inc.	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
17	17	ef4c35c6-b...	NULL	offline	69:9A:C0:6...	C0:65:2C:1B	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
18	18	d14ae10a-4...	NULL	offline	A0:ED:CD:E...	CD:EF:57:05	Apple, Inc.	NULL	Apple, Inc. (...	NULL	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
19	19	1b708f0f-0...	NULL	offline	1D:36:EE:B...	EE:B3:0E:89	N/A - Rando...	NULL	Apple, Inc. (...	NULL	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
20	20	c1b19575-7...	NULL	offline	5C:F9:38:C...	38:C4:D4:59	Apple, Inc.	NULL	Apple, Inc. (...	NULL	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
21	21	f4b92c58-5...	NULL	offline	5F:52:81:3...	81:3C:12:6A	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
22	22	9a18e450-5...	NULL	offline	57:34:C2:8...	C2:8E:2E:1D	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
23	23	aba60911-1...	NULL	offline	55:1A:2E:4...	2E:4A:66:3C	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
24	24	30e03bb8-d...	NULL	offline	78:C2:D0:4...	D0:40:4A:36	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
25	25	6d32ad97-e...	NULL	offline	65:34:80:7...	80:78:D2:9F	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
26	26	24503d19-a...	NULL	offline	4D:B4:F7:7...	F7:71:B8:D0	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	Bluetooth 5...	Broadcom ...	002.003.007	f	NULL	NULL	NULL	NULL
27	27	a5d4ec53-9...	USCP56020...	offline	98:5F:D3:4...	D3:4F:16:31	Microsoft C...	NULL	NULL	NULL	Bluetooth 4...	Marvell Tec...	NULL	t	NULL	["Attribute ...	Computer (...	Lapto
28	28	bdc178e9-a...	NULL	offline	7C:C1:0D:5...	0D:57:C0:DF	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	Bluetooth 4...	Broadcom ...	003.001.003	f	NULL	NULL	NULL	NULL
29	29	132c056d-1...	USCP55894...	offline	98:5F:D3:C...	D3:C6:D3:66	Microsoft C...	NULL	NULL	NULL	NULL	NULL	NULL	t	NULL	NULL	Computer (...	Lapto
30	30	03eeeee9-0...	NULL	offline	5B:DE:77:D...	77:DA:A8:EF	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
31	31	9c71ef24-7...	NULL	offline	63:8D:DC:D...	DC:DC:8A:C7	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	Bluetooth 4...	Broadcom ...	003.001.003	f	NULL	NULL	NULL	NULL
32	32	18729424-f...	NULL	offline	4E:39:9B:B...	9B:BB:AF:E0	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	Bluetooth 5...	Broadcom ...	002.002.014	f	NULL	NULL	NULL	NULL
33	33	9328903f-f...	NULL	offline	41:5C:34:1...	34:1D:4B:9F	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	Bluetooth 1...	Ericsson Te...	NULL	f	NULL	NULL	NULL	NULL
34	34	787eb0a8-d...	Gear S3 (3C...	offline	3C:DC:BC:2...	BC:2B:8C:81	Unknown	NULL	not assigne...	NULL	Bluetooth 4...	Broadcom ...	002.001.021	t	["Vendor sp...	["Connectio...	Wearable	Wrist
35	35	4a43f6e6-e...	NULL	offline	73:DC:C7:3...	C7:37:AB:6F	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
36	36	50c9ddd9-1...	NULL	offline	98:5F:D3:C...	D3:C6:D3:22	Microsoft C...	NULL	NULL	NULL	NULL	NULL	NULL	t	NULL	NULL	Computer (...	Lapto
37	37	efa1d8b3-8...	NULL	offline	5D:E5:97:2...	97:2B:01:A6	N/A - Rando...	NULL	NULL	NULL	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
38	38	fafc6682-de...	NULL	offline	6A:A5:4F:A...	4F:A0:F4:D1	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	Bluetooth 5...	Broadcom ...	002.002.014	f	NULL	NULL	NULL	NULL
39	39	780d902c-8...	NULL	offline	41:1A:F2:F...	F2:FD:6C:57	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	Bluetooth 4...	Broadcom ...	002.001.009	f	NULL	NULL	NULL	NULL
40	40	237850f4-cf...	NULL	offline	40:76:0F:F4...	0F:F4:73:9F	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
41	41	83ce1345-a...	NULL	offline	4E:F0:34:C1...	34:C1:C6:F3	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
42	42	c4263c66-d...	NULL	offline	4A:87:1E:0...	1E:02:07:28	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	Bluetooth 4...	Broadcom ...	003.001.003	f	NULL	NULL	NULL	NULL
43	43	d68d65e2-1...	NULL	offline	75:66:E3:9E...	E3:9E:12:87	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	Bluetooth 1...	Ericsson Te...	NULL	f	NULL	NULL	NULL	NULL
44	44	42be3a04-5...	NULL	offline	6D:9E:93:D...	93:D2:84:9B	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	Bluetooth 5...	Broadcom ...	002.002.014	f	NULL	NULL	NULL	NULL
45	45	eb0042c6-8...	5AAA00000...	offline	18:93:D7:6...	D7:63:E1:A1	Texas Instr...	NULL	Apple, Inc. (...	NULL	NULL	NULL	NULL	f	NULL	NULL	NULL	NULL
46	46	da460b89-6...	NULL	offline	6F:9D:2C:6...	2C:6A:22:95	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	Bluetooth 1...	Ericsson Te...	NULL	f	NULL	NULL	NULL	NULL
47	47	bcaf7ecd-b...	NULL	offline	53:0C:FC:0...	FC:09:BB:05	N/A - Rando...	NULL	Apple, Inc. (...	Unknown	Bluetooth 5...	Broadcom ...	002.002.014	f	NULL	NULL	NULL	NULL
48	48	a88f465e-e...	[AV] Samsu...	offline	5C:49:7D:8...	7D:8E:EE:52	Samsung El...	NULL	NULL	NULL	NULL	NULL	NULL	t	NULL	NULL	Audio/Video...	Louds

1 - 49 of 208

Go to: 1

Mode: Text

Type of data currently in cell: NULL
0 byte(s)

Demonstration!

RSAConference2019

blue_sonar

https://github.com/ZeroChaos-/blue_sonar

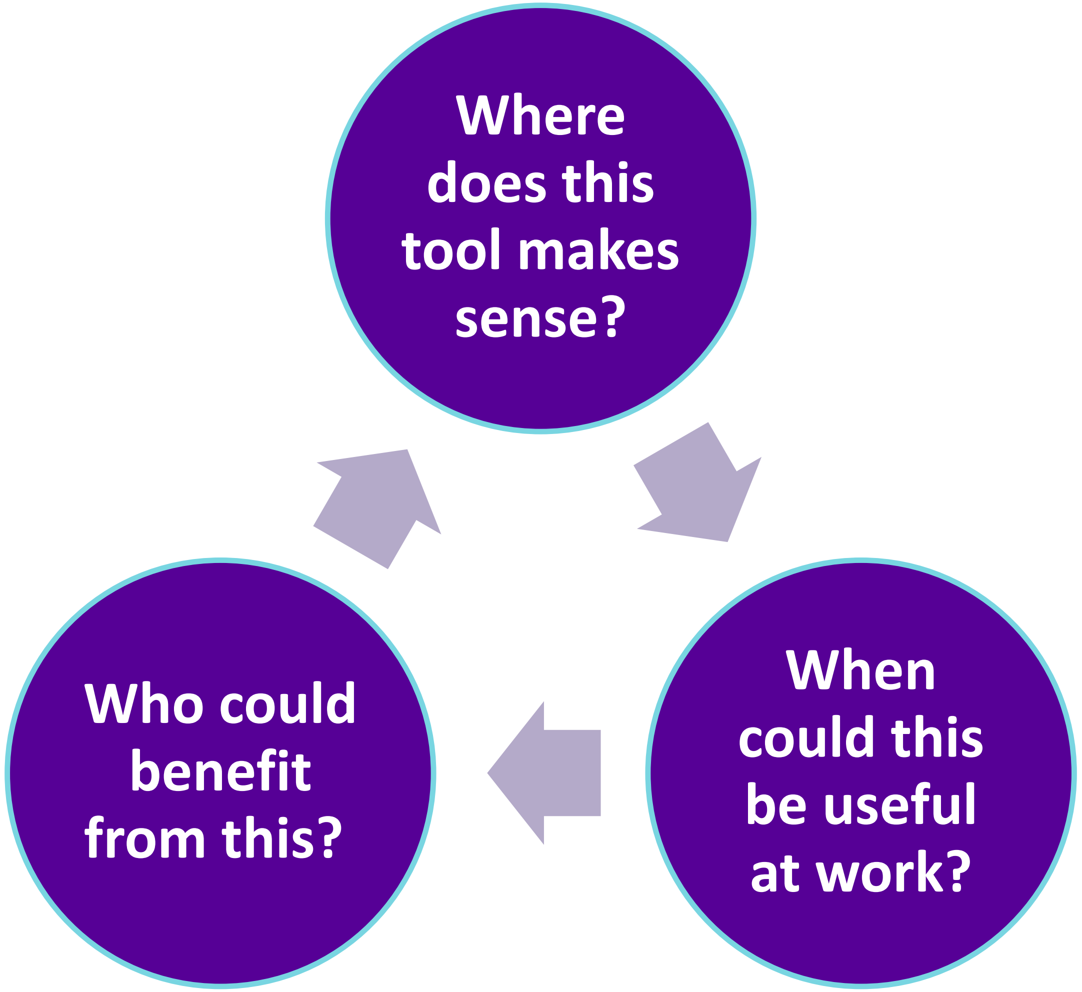
using layer 2

Bluetooth is so prevalent, and Bluetooth Classic is on all phones as we will show!

This can be used for tracking if the Layer 2 (MAC address) is known!

Demonstration!

so i was driving down the road



Where does this tool makes sense?

When could this be useful at work?

Who could benefit from this?

MouseJack

mousejack

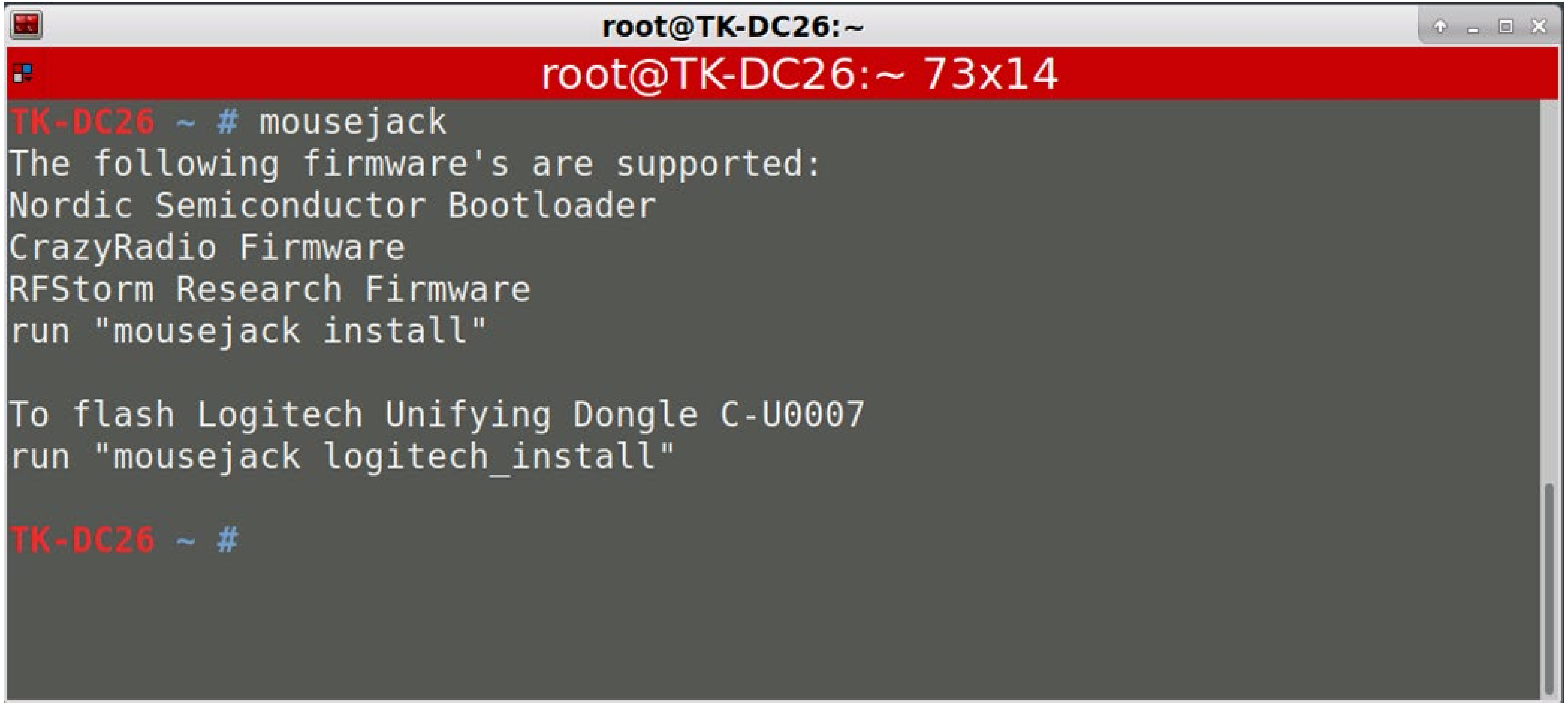
MouseJack is a class of vulnerabilities that affects most wireless, non-Bluetooth keyboards and mice.

An attacker can launch the attack from up to 100 meters away.

😈

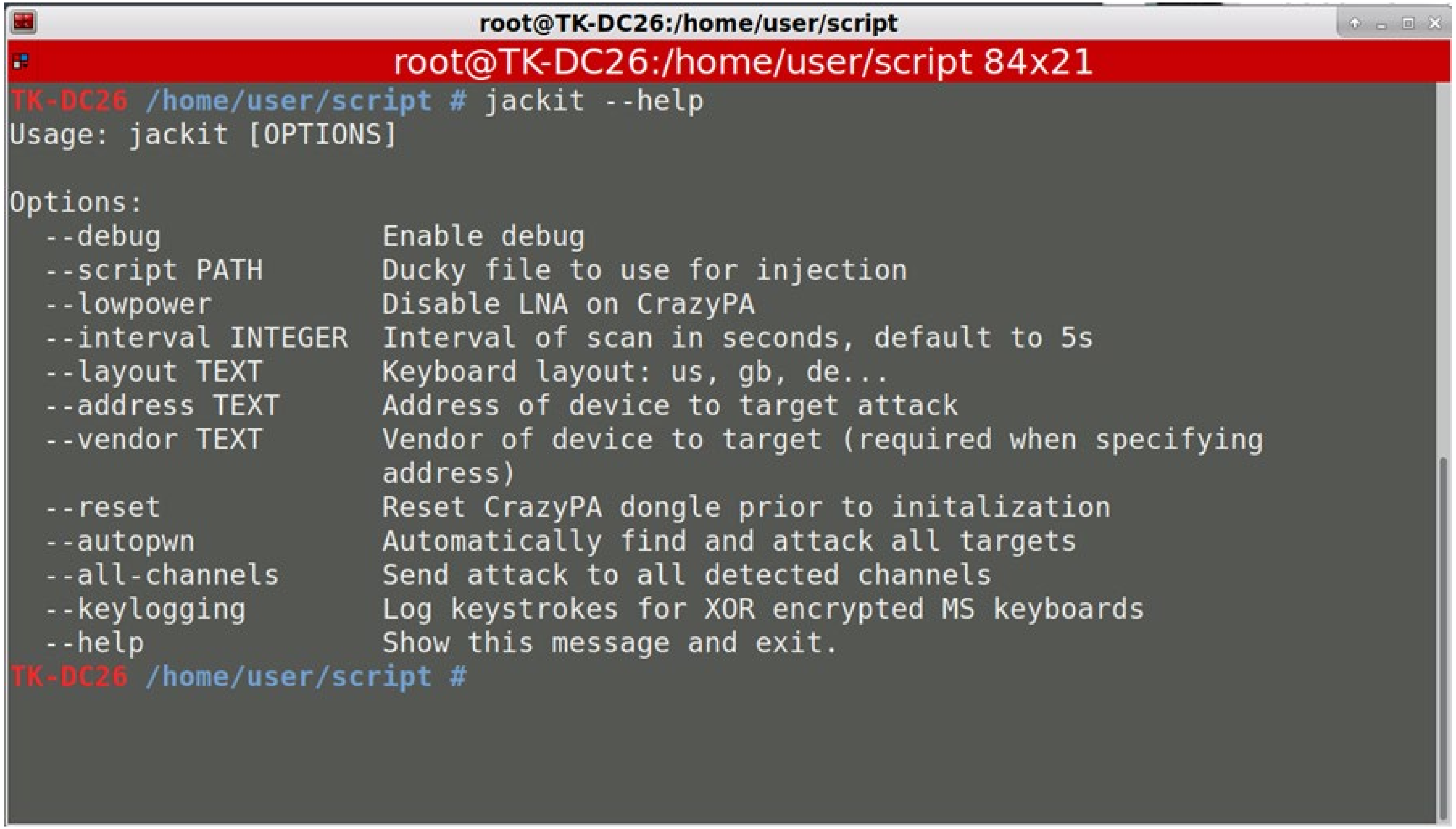
*Thanks for the amazing research Bastille

mousejack implemented in pentoo



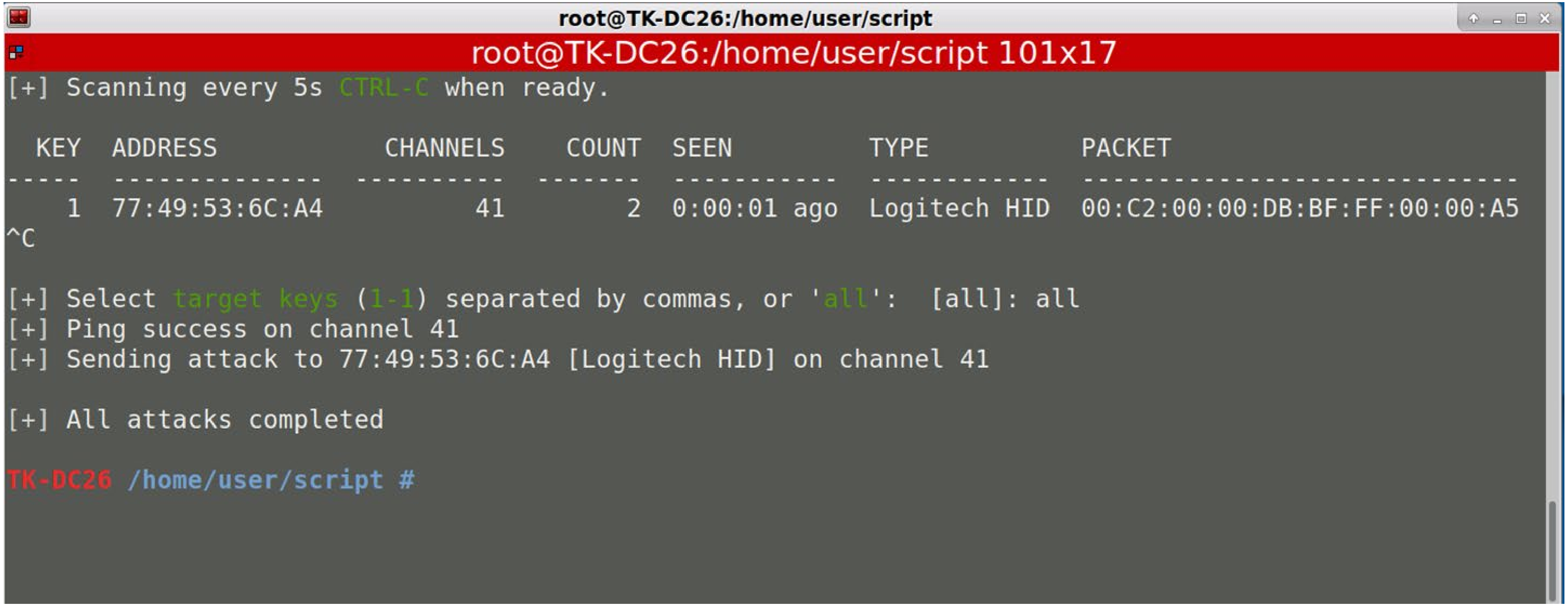
```
TK-DC26 ~ # mousejack
The following firmware's are supported:
Nordic Semiconductor Bootloader
CrazyRadio Firmware
RFStorm Research Firmware
run "mousejack install"

To flash Logitech Unifying Dongle C-U0007
run "mousejack logitech_install"

TK-DC26 ~ #
```

jackit running in pentoo


root@TK-DC26:/home/user/script
root@TK-DC26:/home/user/script 84x21

```
TK-DC26 /home/user/script # jackit --help
Usage: jackit [OPTIONS]

Options:
  --debug              Enable debug
  --script PATH        Ducky file to use for injection
  --lowpower           Disable LNA on CrazyPA
  --interval INTEGER   Interval of scan in seconds, default to 5s
  --layout TEXT        Keyboard layout: us, gb, de...
  --address TEXT       Address of device to target attack
  --vendor TEXT        Vendor of device to target (required when specifying
                       address)
  --reset              Reset CrazyPA dongle prior to initalization
  --autopwn            Automatically find and attack all targets
  --all-channels       Send attack to all detected channels
  --keylogging         Log keystrokes for XOR encrypted MS keyboards
  --help               Show this message and exit.
TK-DC26 /home/user/script #
```

attacking and enumeration with jackit



root@TK-DC26:/home/user/script
root@TK-DC26:/home/user/script 101x17

```
[+] Scanning every 5s CTRL-C when ready.

  KEY  ADDRESS          CHANNELS    COUNT  SEEN          TYPE          PACKET
-----  --------------  ----------  -------  -----------  ------------  -----------------------------
    1  77:49:53:6C:A4          41        2  0:00:01 ago  Logitech HID  00:C2:00:00:DB:BF:FF:00:00:A5
^C

[+] Select target keys (1-1) separated by commas, or 'all':  [all]: all
[+] Ping success on channel 41
[+] Sending attack to 77:49:53:6C:A4 [Logitech HID] on channel 41

[+] All attacks completed

TK-DC26 /home/user/script #
```

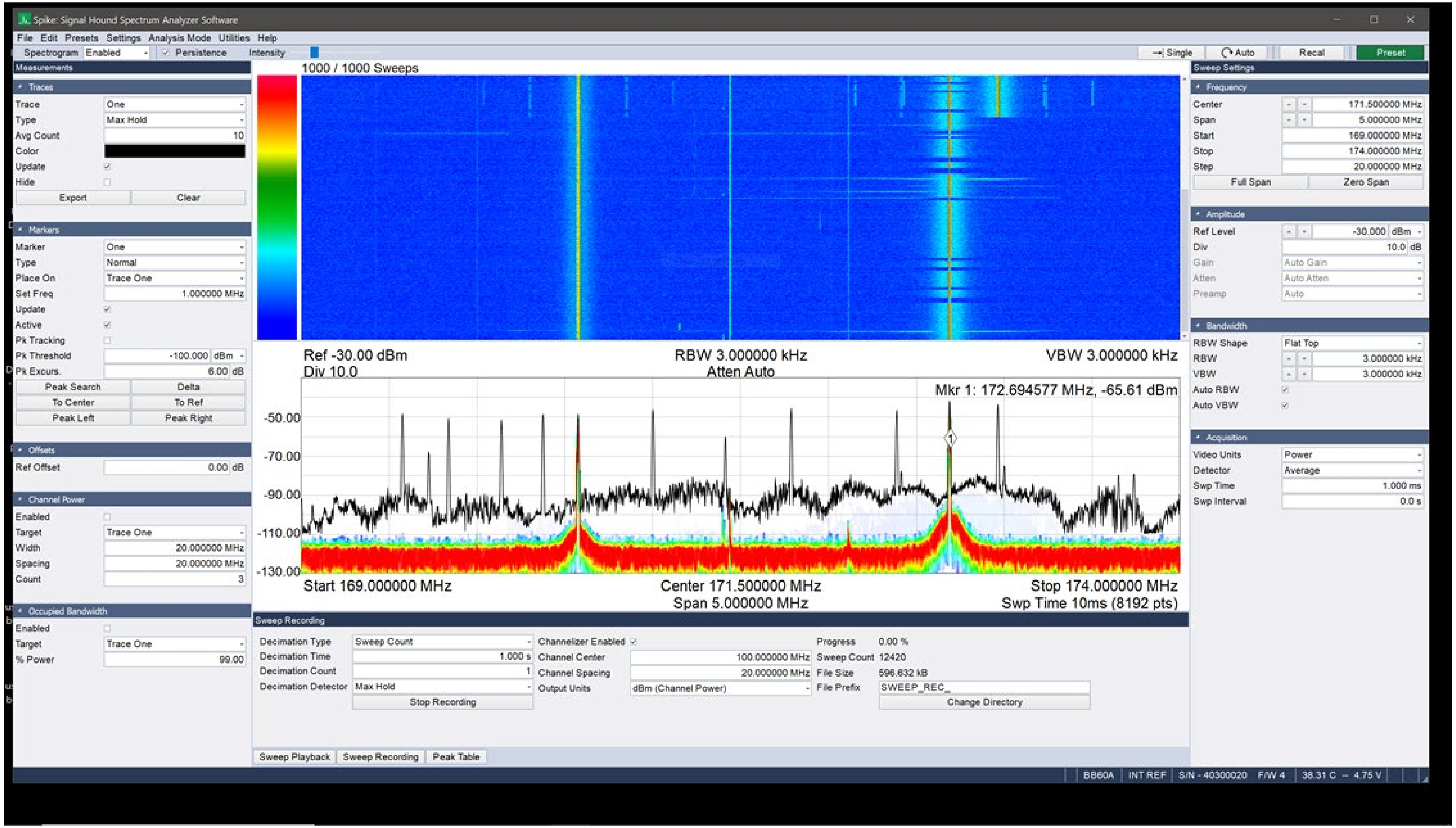
RSAConference2019

Demonstration!

RSA®Conference2019

Software Defined Radio (SDR)

10 MHz to 6 GHz spectrum



Spike: Signal Hound Spectrum Analyzer Software

Spectrogram: Enabled
☑ Persistence
Intensity

Measurements

Traces

- Trace: One
- Type: Max Hold
- Avg Count: 10
- Color: ■
- Update: ☑
- Hide: □

Export | Clear

Markers

- Marker: One
- Type: Normal
- Place On: Trace One
- Set Freq: 1.000000 MHz
- Update: ☑
- Active: ☑
- Pk Tracking: □
- Pk Threshold: -100.000 dBm
- Pk Excurs.: 6.00 dB

Peak Search | Delta
To Center | To Ref
Peak Left | Peak Right

Offsets

- Ref Offset: 0.00 dB

Channel Power

- Enabled: □
- Target: Trace One
- Width: 20.000000 MHz
- Spacing: 20.000000 MHz
- Count: 3

Occupied Bandwidth

- Enabled: □
- Target: Trace One
- % Power: 99.00

1000 / 1000 Sweeps

Ref -30.00 dBm
Div 10.0

RBW 3.000000 kHz
Atten Auto

VBW 3.000000 kHz

Mkr 1: 172.694577 MHz, -65.61 dBm

Start 169.000000 MHz

Center 171.500000 MHz
Span 5.000000 MHz

Stop 174.000000 MHz
Swp Time 10ms (8192 pts)

Sweep Settings

Frequency

- Center: 171.500000 MHz
- Span: 5.000000 MHz
- Start: 169.000000 MHz
- Stop: 174.000000 MHz
- Step: 20.000000 MHz

Full Span | Zero Span

Amplitude

- Ref Level: -30.000 dBm
- Div: 10.0 dB
- Gain: Auto Gain
- Atten: Auto Atten
- Preamp: Auto

Bandwidth

- RBW Shape: Flat Top
- RBW: 3.000000 kHz
- VBW: 3.000000 kHz
- Auto RBW: ☑
- Auto VBW: ☑

Acquisition

- Video Units: Power
- Detector: Average
- Swp Time: 1.000 ms
- Swp Interval: 0.0 s

Sweep Recording

- Decimation Type: Sweep Count
- Decimation Time: 1.000 s
- Decimation Count: 1
- Decimation Detector: Max Hold

Stop Recording

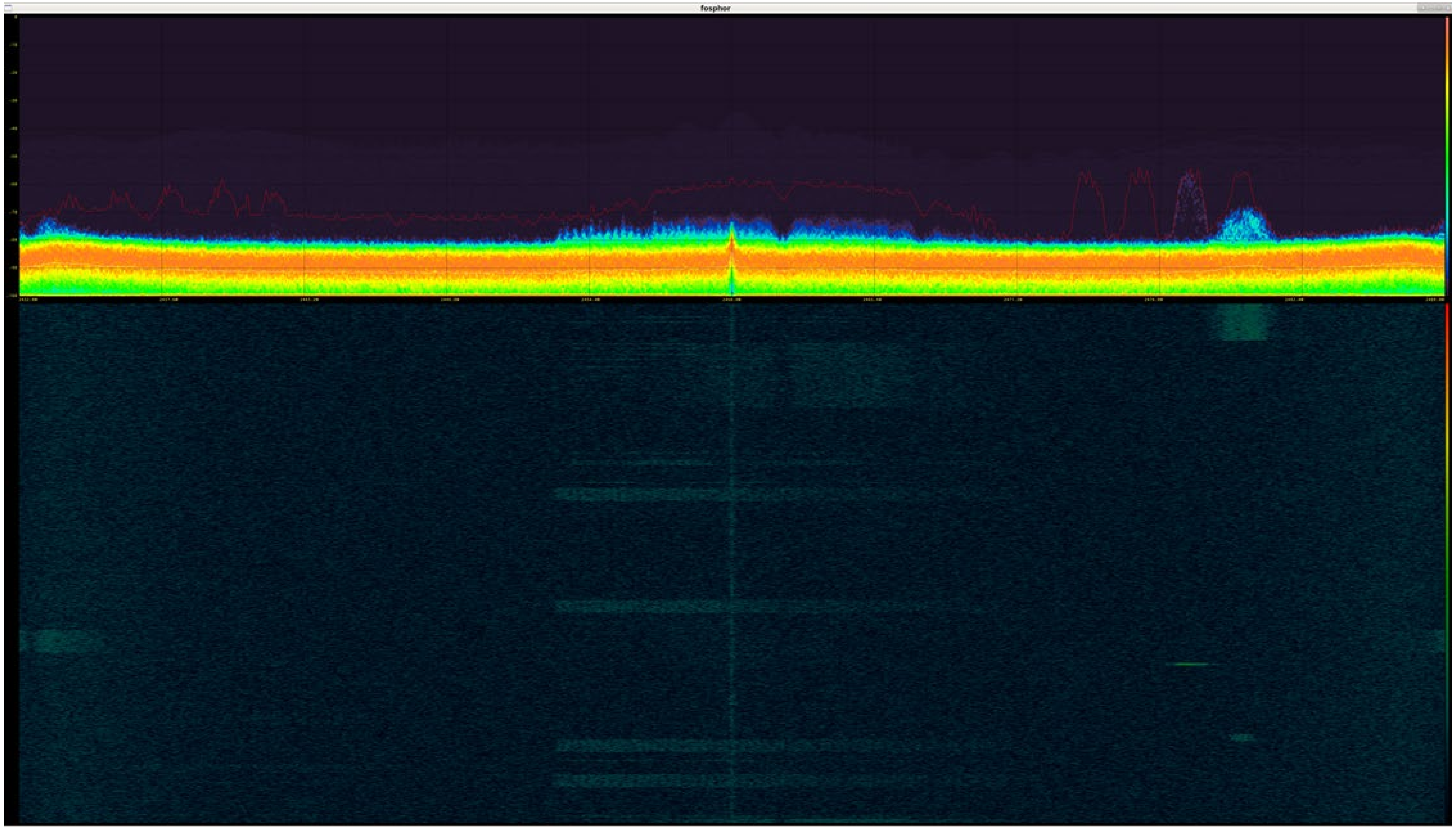
- Channelizer Enabled: ☑
- Channel Center: 100.000000 MHz
- Channel Spacing: 20.000000 MHz
- Output Units: dBm (Channel Power)

- Progress: 0.00 %
- Sweep Count: 12420
- File Size: 596.632 kB
- File Prefix: SWEEP_REC_

Change Directory

BB60A | INT REF | S/N - 40300020 F/W 4 | 38.31 C – 4.75 V

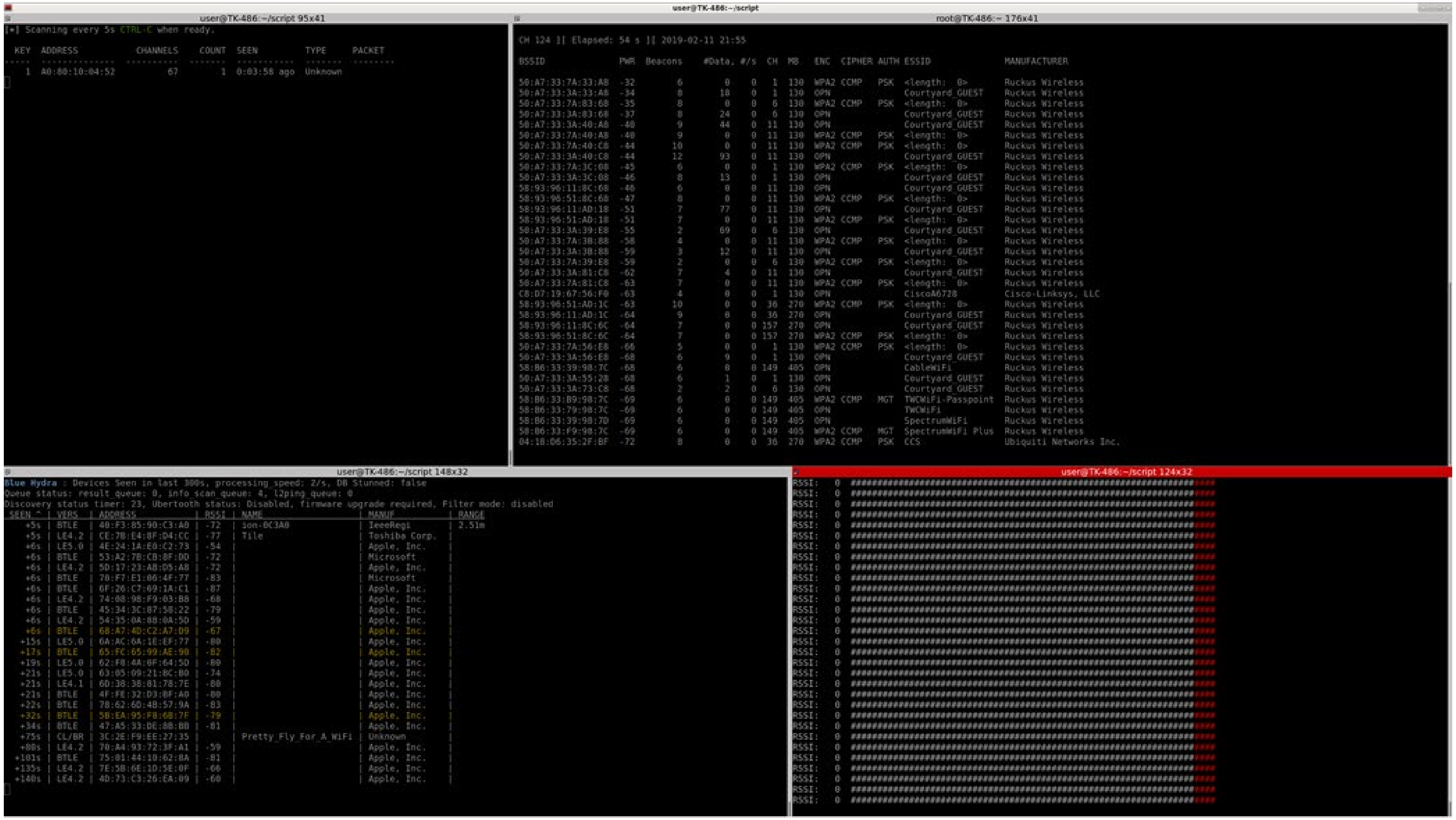
fosphor_knob in Pentoo



RSA Conference2019

Demonstration!

external enumeration of internal spaces



user@TK-486:~/script

user@TK-486:~/script 95x41

```
[*] Scanning every 5s CTRL-C when ready.

  KEY  ADDRESS            CHANNELS    COUNT  SEEN          TYPE     PACKET
-----  ---------------  ----------  -------  ------------  -------  --------
    1  A0:80:10:04:52           67        1  0:03:58 ago   Unknown
```

root@TK-486:~ 176x41

```
 CH 124 ][ Elapsed: 54 s ][ 2019-02-11 21:55

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID                 MANUFACTURER

 50:A7:33:7A:33:A8  -32        6        0    0   1  130  WPA2 CCMP   PSK  <length:  0>          Ruckus Wireless
 50:A7:33:3A:33:A8  -34        8       18    0   1  130  OPN              Courtyard_GUEST       Ruckus Wireless
 50:A7:33:7A:83:68  -35        8        0    0   6  130  WPA2 CCMP   PSK  <length:  0>          Ruckus Wireless
 50:A7:33:3A:83:68  -37        8       24    0   6  130  OPN              Courtyard_GUEST       Ruckus Wireless
 50:A7:33:3A:40:A8  -40        9       44    0  11  130  OPN              Courtyard_GUEST       Ruckus Wireless
 50:A7:33:7A:40:A8  -40        9        0    0  11  130  WPA2 CCMP   PSK  <length:  0>          Ruckus Wireless
 50:A7:33:7A:40:C8  -44       10        0    0  11  130  WPA2 CCMP   PSK  <length:  0>          Ruckus Wireless
 50:A7:33:3A:40:C8  -44       12       93    0  11  130  OPN              Courtyard_GUEST       Ruckus Wireless
 50:A7:33:7A:3C:08  -45        6        0    0   1  130  WPA2 CCMP   PSK  <length:  0>          Ruckus Wireless
 50:A7:33:3A:3C:08  -46        8       13    0   1  130  OPN              Courtyard_GUEST       Ruckus Wireless
 58:93:96:11:8C:68  -46        6        0    0  11  130  OPN              Courtyard_GUEST       Ruckus Wireless
 58:93:96:51:8C:68  -47        8        0    0  11  130  WPA2 CCMP   PSK  <length:  0>          Ruckus Wireless
 58:93:96:11:AD:18  -51        7       77    0  11  130  OPN              Courtyard_GUEST       Ruckus Wireless
 58:93:96:51:AD:18  -51        7        0    0  11  130  WPA2 CCMP   PSK  <length:  0>          Ruckus Wireless
 50:A7:33:3A:39:E8  -55        2       69    0   6  130  OPN              Courtyard_GUEST       Ruckus Wireless
 50:A7:33:7A:38:88  -58        4        0    0  11  130  WPA2 CCMP   PSK  <length:  0>          Ruckus Wireless
 50:A7:33:3A:38:88  -59        3       12    0  11  130  OPN              Courtyard_GUEST       Ruckus Wireless
 50:A7:33:7A:39:E8  -59        2        0    0   6  130  WPA2 CCMP   PSK  <length:  0>          Ruckus Wireless
 50:A7:33:3A:81:C8  -62        7        4    0  11  130  OPN              Courtyard_GUEST       Ruckus Wireless
 50:A7:33:7A:81:C8  -63        7        0    0  11  130  WPA2 CCMP   PSK  <length:  0>          Ruckus Wireless
 C8:D7:19:67:56:F0  -63        4        0    0   1  130  OPN              CiscoA6728            Cisco-Linksys, LLC
 58:93:96:51:AD:1C  -63       10        0    0  36  270  WPA2 CCMP   PSK  <length:  0>          Ruckus Wireless
 58:93:96:11:AD:1C  -64        9        0    0  36  270  OPN              Courtyard_GUEST       Ruckus Wireless
 58:93:96:11:8C:6C  -64        7        0    0 157  270  OPN              Courtyard_GUEST       Ruckus Wireless
 58:93:96:51:8C:6C  -64        7        0    0 157  270  WPA2 CCMP   PSK  <length:  0>          Ruckus Wireless
 50:A7:33:7A:56:E8  -66        5        0    0   1  130  WPA2 CCMP   PSK  <length:  0>          Ruckus Wireless
 50:A7:33:3A:56:E8  -68        6        9    0   1  130  OPN              Courtyard_GUEST       Ruckus Wireless
 58:B6:33:39:98:7C  -68        6        0    0 149  405  OPN              CableWiFi             Ruckus Wireless
 50:A7:33:3A:55:28  -68        6        1    0   1  130  OPN              Courtyard_GUEST       Ruckus Wireless
 50:A7:33:3A:73:C8  -68        2        2    0   6  130  OPN              Courtyard_GUEST       Ruckus Wireless
 58:B6:33:B9:98:7C  -69        6        0    0 149  405  WPA2 CCMP   MGT  TWCWiFi-Passpoint     Ruckus Wireless
 58:B6:33:79:98:7C  -69        6        0    0 149  405  OPN              TWCWiFi               Ruckus Wireless
 58:B6:33:39:98:7D  -69        6        0    0 149  405  OPN              SpectrumWiFi          Ruckus Wireless
 58:B6:33:F9:98:7C  -69        6        0    0 149  405  WPA2 CCMP   MGT  SpectrumWiFi Plus     Ruckus Wireless
 04:18:D6:35:2F:BF  -72        8        0    0  36  270  WPA2 CCMP   PSK  CCS                   Ubiquiti Networks Inc.
```

user@TK-486:~/script 148x32

```
Blue Hydra : Devices Seen in last 300s, processing_speed: 2/s, DB Stunned: false
Queue status: result_queue: 0, info_scan_queue: 4, l2ping_queue: 0
Discovery status timer: 23, Ubertooth status: Disabled, firmware upgrade required, Filter mode: disabled
 SEEN ^ | VERS  | ADDRESS           | RSSI | NAME                  | MANUF            | RANGE
    +5s | BTLE  | 40:F3:85:90:C3:A0 | -72  | ion-0C3A0             | IeeeRegi         | 2.51m
    +5s | LE4.2 | CE:7B:E4:8F:D4:CC | -77  | Tile                  | Toshiba Corp.    |
    +6s | LE5.0 | 4E:24:1A:E0:C2:73 | -54  |                       | Apple, Inc.      |
    +6s | BTLE  | 53:A2:7B:CB:8F:DD | -72  |                       | Microsoft        |
    +6s | LE4.2 | 5D:17:23:A8:D5:A8 | -72  |                       | Apple, Inc.      |
    +6s | BTLE  | 78:F7:E1:06:4F:77 | -83  |                       | Microsoft        |
    +6s | BTLE  | 6F:26:C7:69:1A:C1 | -87  |                       | Apple, Inc.      |
    +6s | LE4.2 | 74:08:98:F9:03:B8 | -68  |                       | Apple, Inc.      |
    +6s | BTLE  | 45:34:3C:87:58:22 | -79  |                       | Apple, Inc.      |
    +6s | LE4.2 | 54:35:0A:88:0A:5D | -59  |                       | Apple, Inc.      |
    +6s | BTLE  | 68:A7:4D:C2:A7:D9 | -67  |                       | Apple, Inc.      |
   +15s | LE5.0 | 6A:AC:6A:1E:EF:77 | -80  |                       | Apple, Inc.      |
   +17s | BTLE  | 65:FC:65:99:AE:90 | -82  |                       | Apple, Inc.      |
   +19s | LE5.0 | 62:F8:4A:0F:64:5D | -80  |                       | Apple, Inc.      |
   +21s | LE5.0 | 63:05:09:21:8C:80 | -74  |                       | Apple, Inc.      |
   +21s | LE4.1 | 6D:38:38:81:78:7E | -80  |                       | Apple, Inc.      |
   +21s | BTLE  | 4F:FE:32:D3:8F:A0 | -80  |                       | Apple, Inc.      |
   +22s | BTLE  | 78:62:6D:4B:57:9A | -83  |                       | Apple, Inc.      |
   +32s | BTLE  | 5B:EA:95:F8:6B:7F | -79  |                       | Apple, Inc.      |
   +34s | BTLE  | 47:A5:33:DE:88:B8 | -81  |                       | Apple, Inc.      |
   +75s | CL/BR | 3C:2E:F9:EE:27:35 |      | Pretty_Fly_For_A_WiFi | Unknown          |
   +80s | LE4.2 | 70:A4:93:72:3F:A1 | -59  |                       | Apple, Inc.      |
  +101s | BTLE  | 75:01:44:10:62:8A | -81  |                       | Apple, Inc.      |
  +135s | LE4.2 | 7E:5B:6E:1D:5E:0F | -66  |                       | Apple, Inc.      |
  +140s | LE4.2 | 4D:73:C3:26:EA:09 | -60  |                       | Apple, Inc.      |
```

user@TK-486:~/script 124x32

```
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
RSSI:   0   #####################################################################
```

a Hewlett Packard
Enterprise company

RSA Conference2019

Questions?

Rick Mellendick
PIAchievers, LLC
@rmellendick

Rick Farina
Aruba
@Zero_ChaosX