Rogue AP Finder C9800

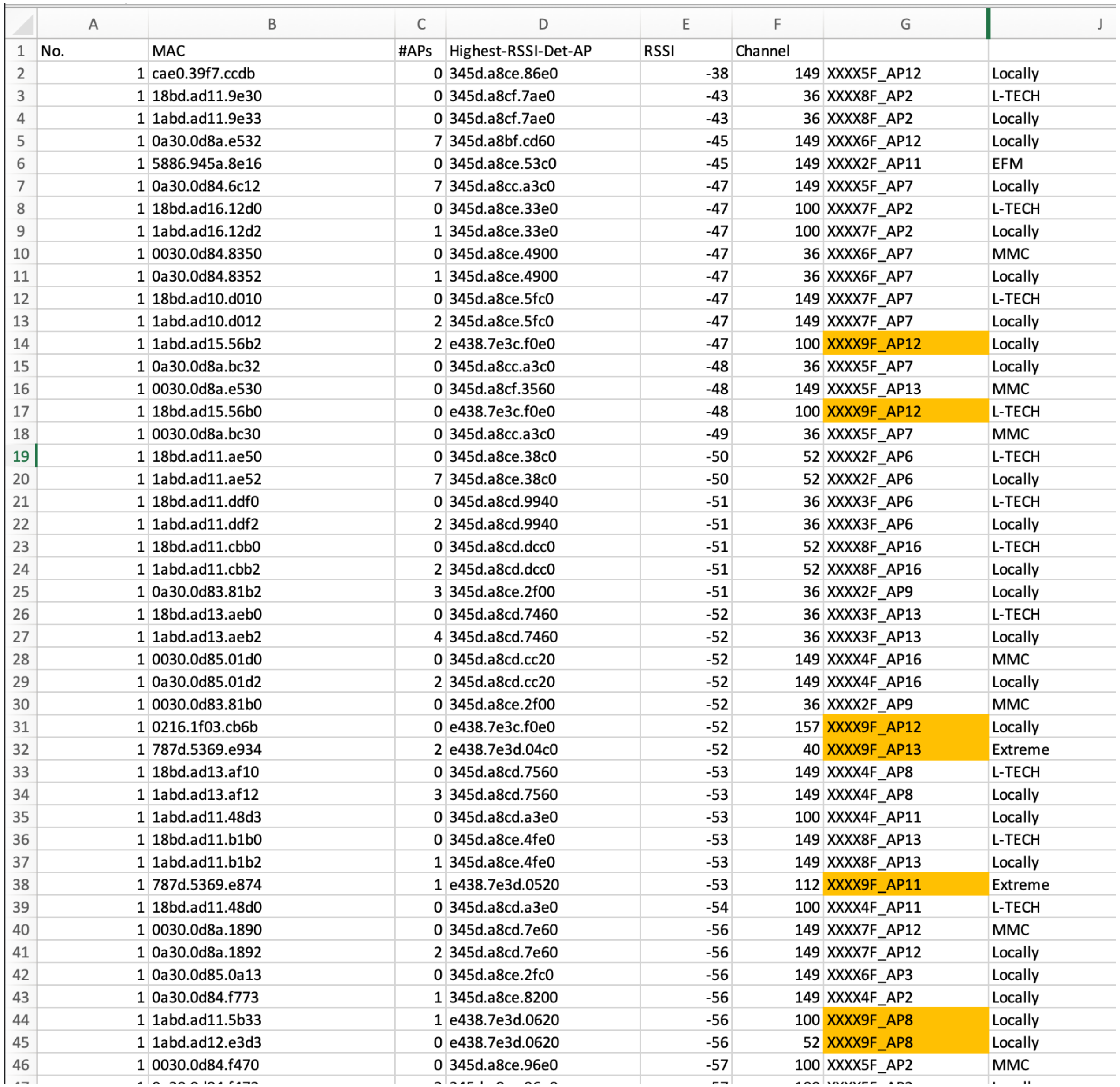
2024. 5.

Customer Request

Want to Find the Rogue AP

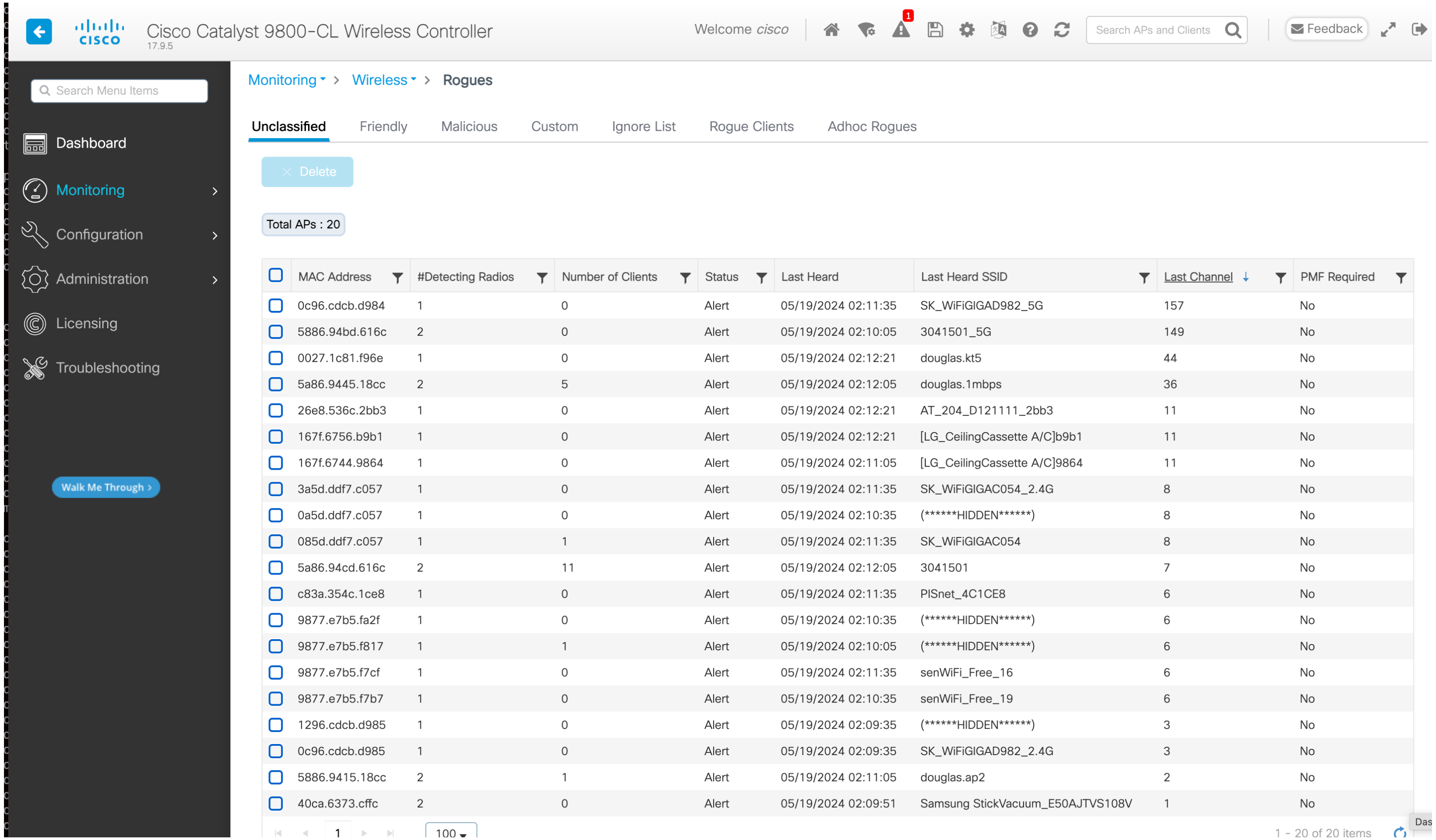
Location and Vendor information is required.

EXCEL



	A	B	C	D	E	F	G	J
1	No.	MAC	#APs	Highest-RSSI-Det-AP	RSSI	Channel		
2	1	cae0.39f7.ccdb	0	345d.a8ce.86e0	-38	149	XXXX5F_AP12	Locally
3	1	18bd.ad11.9e30	0	345d.a8cf.7ae0	-43	36	XXXX8F_AP2	L-TECH
4	1	1abd.ad11.9e33	0	345d.a8cf.7ae0	-43	36	XXXX8F_AP2	Locally
5	1	0a30.0d8a.e532	7	345d.a8bf.cd60	-45	149	XXXX6F_AP12	Locally
6	1	5886.945a.8e16	0	345d.a8ce.53c0	-45	149	XXXX2F_AP11	EFM
7	1	0a30.0d84.6c12	7	345d.a8cc.a3c0	-47	149	XXXX5F_AP7	Locally
8	1	18bd.ad16.12d0	0	345d.a8ce.33e0	-47	100	XXXX7F_AP2	L-TECH
9	1	1abd.ad16.12d2	1	345d.a8ce.33e0	-47	100	XXXX7F_AP2	Locally
10	1	0030.0d84.8350	0	345d.a8ce.4900	-47	36	XXXX6F_AP7	MMC
11	1	0a30.0d84.8352	1	345d.a8ce.4900	-47	36	XXXX6F_AP7	Locally
12	1	18bd.ad10.d010	0	345d.a8ce.5fc0	-47	149	XXXX7F_AP7	L-TECH
13	1	1abd.ad10.d012	2	345d.a8ce.5fc0	-47	149	XXXX7F_AP7	Locally
14	1	1abd.ad15.56b2	2	e438.7e3c.f0e0	-47	100	XXXX9F_AP12	Locally
15	1	0a30.0d8a.bc32	0	345d.a8cc.a3c0	-48	36	XXXX5F_AP7	Locally
16	1	0030.0d8a.e530	0	345d.a8cf.3560	-48	149	XXXX5F_AP13	MMC
17	1	18bd.ad15.56b0	0	e438.7e3c.f0e0	-48	100	XXXX9F_AP12	L-TECH
18	1	0030.0d8a.bc30	0	345d.a8cc.a3c0	-49	36	XXXX5F_AP7	MMC
19	1	18bd.ad11.ae50	0	345d.a8ce.38c0	-50	52	XXXX2F_AP6	L-TECH
20	1	1abd.ad11.ae52	7	345d.a8ce.38c0	-50	52	XXXX2F_AP6	Locally
21	1	18bd.ad11.ddf0	0	345d.a8cd.9940	-51	36	XXXX3F_AP6	L-TECH
22	1	1abd.ad11.ddf2	2	345d.a8cd.9940	-51	36	XXXX3F_AP6	Locally
23	1	18bd.ad11.cbb0	0	345d.a8cd.dcc0	-51	52	XXXX8F_AP16	L-TECH
24	1	1abd.ad11.cbb2	2	345d.a8cd.dcc0	-51	52	XXXX8F_AP16	Locally
25	1	0a30.0d83.81b2	3	345d.a8ce.2f00	-51	36	XXXX2F_AP9	Locally
26	1	18bd.ad13.aeb0	0	345d.a8cd.7460	-52	36	XXXX3F_AP13	L-TECH
27	1	1abd.ad13.aeb2	4	345d.a8cd.7460	-52	36	XXXX3F_AP13	Locally
28	1	0030.0d85.01d0	0	345d.a8cd.cc20	-52	149	XXXX4F_AP16	MMC
29	1	0a30.0d85.01d2	2	345d.a8cd.cc20	-52	149	XXXX4F_AP16	Locally
30	1	0030.0d83.81b0	0	345d.a8ce.2f00	-52	36	XXXX2F_AP9	MMC
31	1	0216.1f03.cb6b	0	e438.7e3c.f0e0	-52	157	XXXX9F_AP12	Locally
32	1	787d.5369.e934	2	e438.7e3d.04c0	-52	40	XXXX9F_AP13	Extreme
33	1	18bd.ad13.af10	0	345d.a8cd.7560	-53	149	XXXX4F_AP8	L-TECH
34	1	1abd.ad13.af12	3	345d.a8cd.7560	-53	149	XXXX4F_AP8	Locally
35	1	1abd.ad11.48d3	0	345d.a8cd.a3e0	-53	100	XXXX4F_AP11	Locally
36	1	18bd.ad11.b1b0	0	345d.a8ce.4fe0	-53	149	XXXX8F_AP13	L-TECH
37	1	1abd.ad11.b1b2	1	345d.a8ce.4fe0	-53	149	XXXX8F_AP13	Locally
38	1	787d.5369.e874	1	e438.7e3d.0520	-53	112	XXXX9F_AP11	Extreme
39	1	18bd.ad11.48d0	0	345d.a8cd.a3e0	-54	100	XXXX4F_AP11	L-TECH
40	1	0030.0d8a.1890	0	345d.a8cd.7e60	-56	149	XXXX7F_AP12	MMC
41	1	0a30.0d8a.1892	2	345d.a8cd.7e60	-56	149	XXXX7F_AP12	Locally
42	1	0a30.0d85.0a13	0	345d.a8ce.2fc0	-56	149	XXXX6F_AP3	Locally
43	1	0a30.0d84.f773	1	345d.a8ce.8200	-56	149	XXXX4F_AP2	Locally
44	1	1abd.ad11.5b33	1	e438.7e3d.0620	-56	100	XXXX9F_AP8	Locally
45	1	1abd.ad12.e3d3	0	e438.7e3d.0620	-56	52	XXXX9F_AP8	Locally
46	1	0030.0d84.f470	0	345d.a8ce.96e0	-57	100	XXXX5F_AP2	MMC

WLC C9800 Rogue AP UI – not enough!



□	MAC Address	#Detecting Radios	Number of Clients	Status	Last Heard	Last Heard SSID	Last Channel	PMF Required
□	0c96.cdcb.d984	1	0	Alert	05/19/2024 02:11:35	SK_WiFiGIGAD982_5G	157	No
□	5886.94bd.616c	2	0	Alert	05/19/2024 02:10:05	3041501_5G	149	No
□	0027.1c81.f96e	1	0	Alert	05/19/2024 02:12:21	douglas.kt5	44	No
□	5a86.9445.18cc	2	5	Alert	05/19/2024 02:12:05	douglas.1mbps	36	No
□	26e8.536c.2bb3	1	0	Alert	05/19/2024 02:12:21	AT_204_D121111_2bb3	11	No
□	167f.6756.b9b1	1	0	Alert	05/19/2024 02:12:21	[LG_CeilingCassette A/C]b9b1	11	No
□	167f.6744.9864	1	0	Alert	05/19/2024 02:11:05	[LG_CeilingCassette A/C]9864	11	No
□	3a5d.ddf7.c057	1	0	Alert	05/19/2024 02:11:35	SK_WiFiGIGAC054_2.4G	8	No
□	0a5d.ddf7.c057	1	0	Alert	05/19/2024 02:10:35	(******HIDDEN******)	8	No
□	085d.ddf7.c057	1	1	Alert	05/19/2024 02:11:35	SK_WiFiGIGAC054	8	No
□	5a86.94cd.616c	2	11	Alert	05/19/2024 02:12:05	3041501	7	No
□	c83a.354c.1ce8	1	0	Alert	05/19/2024 02:11:35	PISnet_4C1CE8	6	No
□	9877.e7b5.fa2f	1	0	Alert	05/19/2024 02:10:35	(******HIDDEN******)	6	No
□	9877.e7b5.f817	1	1	Alert	05/19/2024 02:10:05	(******HIDDEN******)	6	No
□	9877.e7b5.f7cf	1	0	Alert	05/19/2024 02:11:35	senWiFi_Free_16	6	No
□	9877.e7b5.f7b7	1	0	Alert	05/19/2024 02:10:35	senWiFi_Free_19	6	No
□	1296.cdcb.d985	1	0	Alert	05/19/2024 02:09:35	(******HIDDEN******)	3	No
□	0c96.cdcb.d985	1	0	Alert	05/19/2024 02:09:35	SK_WiFiGIGAD982_2.4G	3	No
□	5886.9415.18cc	2	1	Alert	05/19/2024 02:11:05	douglas.ap2	2	No
□	40ca.6373.cffc	2	0	Alert	05/19/2024 02:09:51	Samsung StickVacuum_E50AJTVS108V	1	No

WLC C9800 Rogue AP CLI – Need to Improve

```
v9800_17.9.5#show wireless wps rogue ap summary

Rogue Location Discovery Protocol            : Disabled
Validate rogue APs against AAA               : Disabled
Rogue Security Level                         : Custom
Rogue on wire Auto-Contain                   : Disabled
Rogue using our SSID Auto-Contain            : Disabled
Valid client on rogue AP Auto-Contain        : Disabled
Rogue AP timeout                             : 1200
Rogue init timer                             : 180

Total Number of Rogue APs             : 20
MAC Address     Classification  State        #APs  #Clients  Last Heard           Highest-RSSI-Det-AP  RSSI  Channel GHz
------------------------------------------------------------------------------------------------------------------------
0027.1c81.f96e  Unclassified    Alert        1     0         05/19/2024 02:12:21  c4f7.d5e9.5560       -78   44      5
085d.ddf7.c057  Unclassified    Alert        1     1         05/19/2024 02:11:35  286f.7fff.9420       -76   8       2.4
0a5d.ddf7.c057  Unclassified    Alert        1     0         05/19/2024 02:10:35  286f.7fff.9420       -78   8       2.4
```

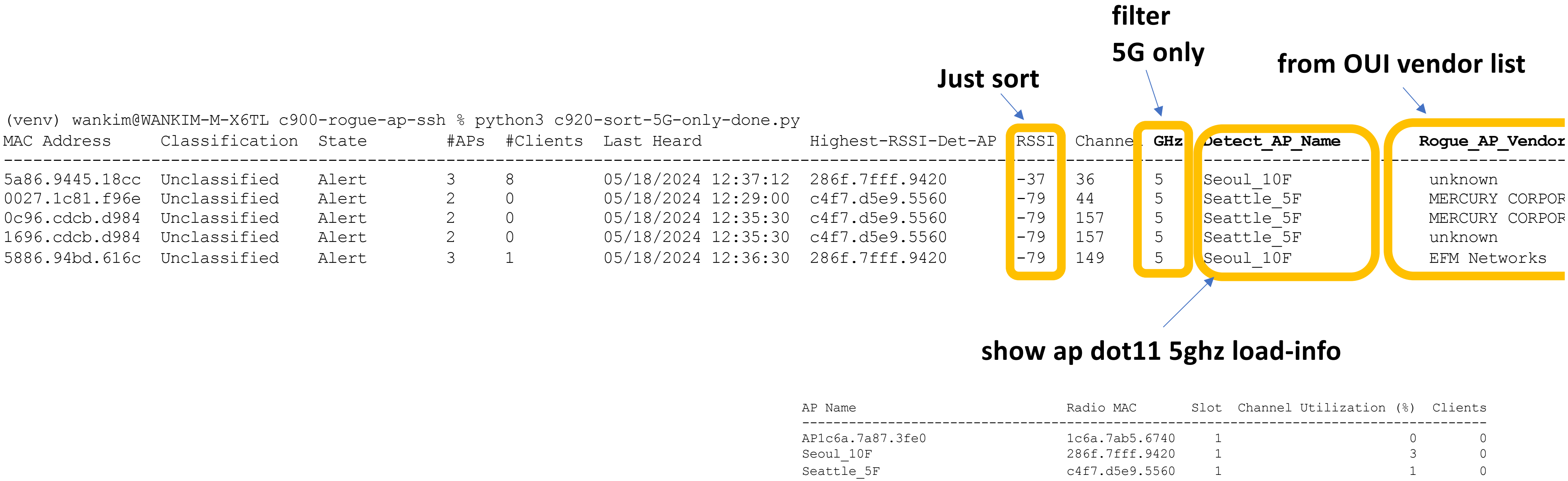
Sorting RSSI

Display 5Ghz Only

Convert into AP MAC vendor

Convert into AP Host Name

Final Goal



Just sort

filter
5G only

from OUI vendor list

```
(venv) wankim@WANKIM-M-X6TL c900-rogue-ap-ssh % python3 c920-sort-5G-only-done.py
MAC Address       Classification   State          #APs   #Clients   Last Heard           Highest-RSSI-Det-AP   RSSI   Channel  GHz   Detect_AP_Name            Rogue_AP_Vendor
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------
5a86.9445.18cc    Unclassified     Alert          3      8          05/18/2024 12:37:12  286f.7fff.9420        -37    36       5     Seoul_10F                  unknown
0027.1c81.f96e    Unclassified     Alert          2      0          05/18/2024 12:29:00  c4f7.d5e9.5560        -79    44       5     Seattle_5F                 MERCURY CORPOR
0c96.cdcb.d984    Unclassified     Alert          2      0          05/18/2024 12:35:30  c4f7.d5e9.5560        -79    157      5     Seattle_5F                 MERCURY CORPOR
1696.cdcb.d984    Unclassified     Alert          2      0          05/18/2024 12:35:30  c4f7.d5e9.5560        -79    157      5     Seattle_5F                 unknown
5886.94bd.616c    Unclassified     Alert          3      1          05/18/2024 12:36:30  286f.7fff.9420        -79    149      5     Seoul_10F                  EFM Networks
```

show ap dot11 5ghz load-info

```
AP Name                            Radio MAC        Slot  Channel Utilization (%)  Clients
-----------------------------------------------------------------------------------------
AP1c6a.7a87.3fe0                   1c6a.7ab5.6740     1                         0        0
Seoul_10F                          286f.7fff.9420     1                         3        0
Seattle_5F                         c4f7.d5e9.5560     1                         1        0
```

FLOW

```
netmiko
    save <c901_ap_list.txt> from <show ap dot11 5ghz load-info> and <show ap dot11 24ghz load-info>
    save <c902_rogue_AP_list.txt> from <'show wireless wps rogue ap summary’>
```

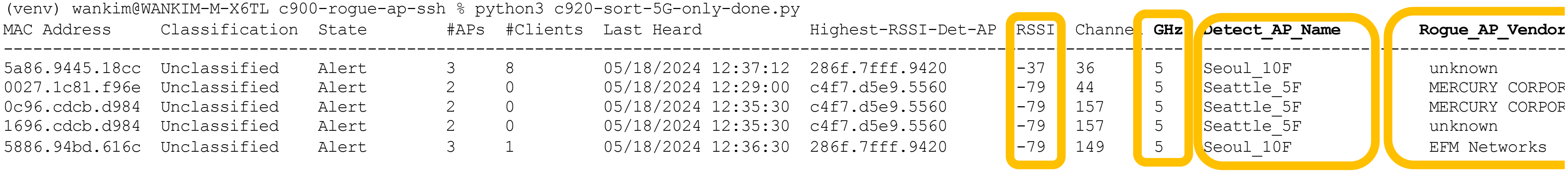
```
read < c902_rogue_AP_list.txt>
    add <rogue AP vendor> using ModC920MacVendorFinder / MAC_VENDOR_FINDER according to <c900-mac-vendor
    add <detect AP hostname> using ModC910FindApName / AP_NAME_FINDER
    write < c903_result_for_sort.txt>
```

```
read < c903_result_for_sort.txt >
    sorting based on RSSI
    dictionaries in list are used
```

Files

- c920-sort-5G-only-done.py
- ModC910FindApName.py
- ModC920MacVendorFinder.py
- c900-mac-vendor.txt

Result



```
(venv) wankim@WANKIM-M-X6TL c900-rogue-ap-ssh % python3 c920-sort-5G-only-done.py
MAC Address     Classification  State          #APs  #Clients  Last Heard                 Highest-RSSI-Det-AP  RSSI  Channel GHz Detect_AP_Name        Rogue_AP_Vendor
-------------------------------------------------------------------------------------------------------------------------------------------------------------
5a86.9445.18cc  Unclassified    Alert          3     8         05/18/2024 12:37:12  286f.7fff.9420       -37   36      5    Seoul_10F             unknown
0027.1c81.f96e  Unclassified    Alert          2     0         05/18/2024 12:29:00  c4f7.d5e9.5560       -79   44      5    Seattle_5F            MERCURY CORPOR
0c96.cdcb.d984  Unclassified    Alert          2     0         05/18/2024 12:35:30  c4f7.d5e9.5560       -79   157     5    Seattle_5F            MERCURY CORPOR
1696.cdcb.d984  Unclassified    Alert          2     0         05/18/2024 12:35:30  c4f7.d5e9.5560       -79   157     5    Seattle_5F            unknown
5886.94bd.616c  Unclassified    Alert          3     1         05/18/2024 12:36:30  286f.7fff.9420       -79   149     5    Seoul_10F             EFM Networks
```

Run on C9800-40

want to do but I don’t have it.

- C9800-40 runs guestshell, which is CentOS/Linux.
- If you have it, you can convert into guestshell code and run C9800 CLI.