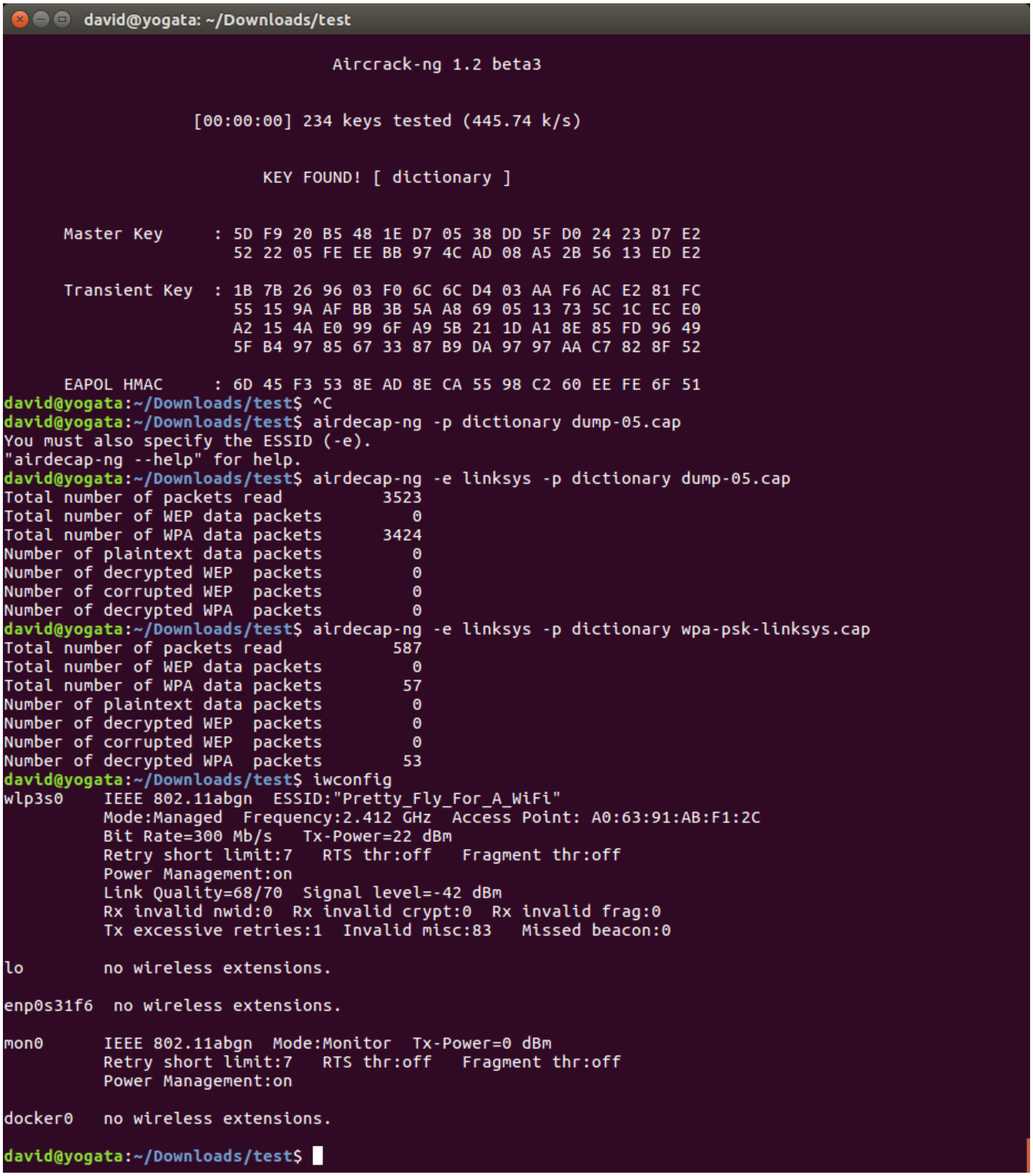
<p style="page-break-after:always;"></p>

Network Security Lab 18

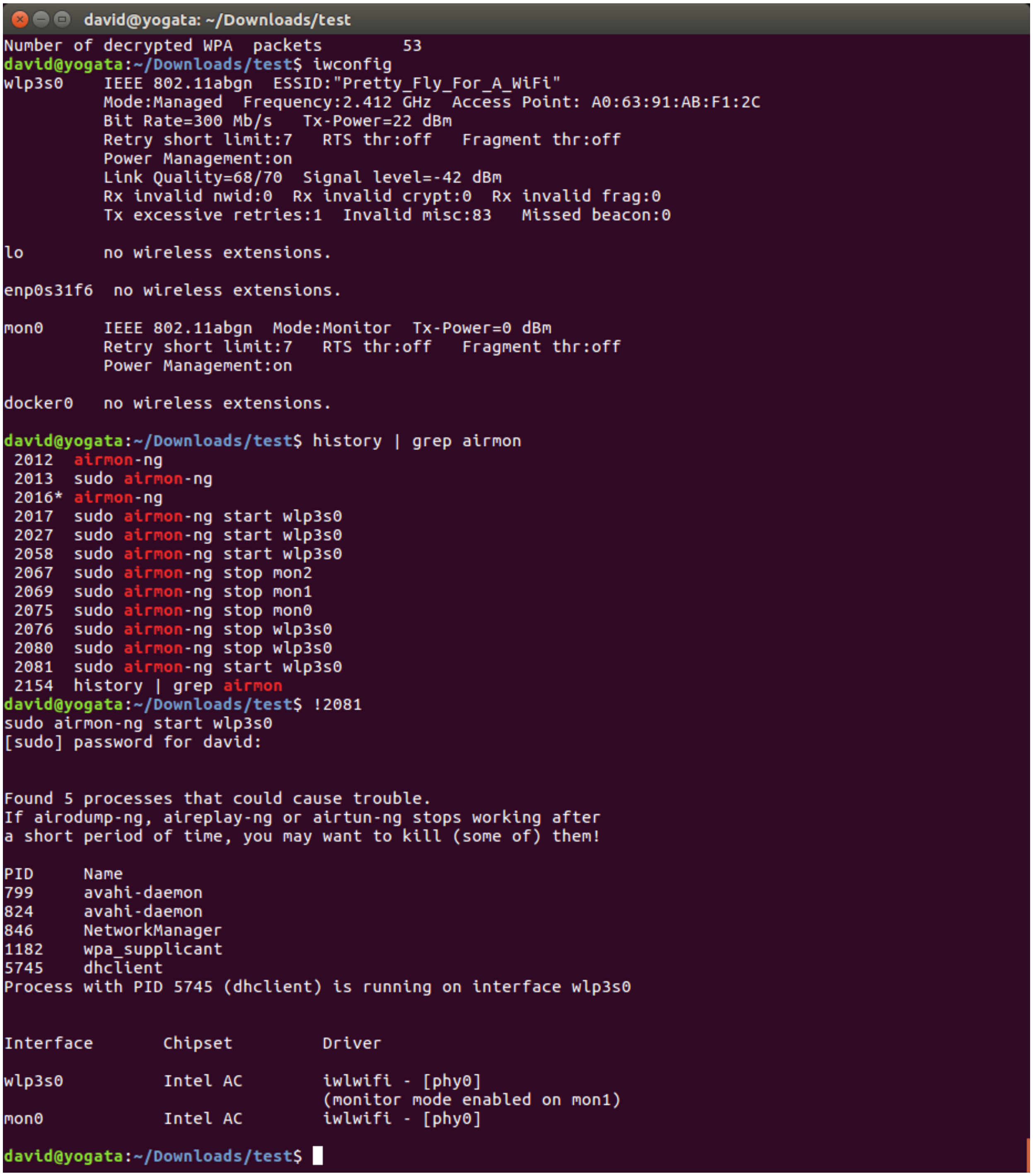
<p><!-- pagebreak --></p>

Network Security Lab 18

David Ayeke April 10. 2017

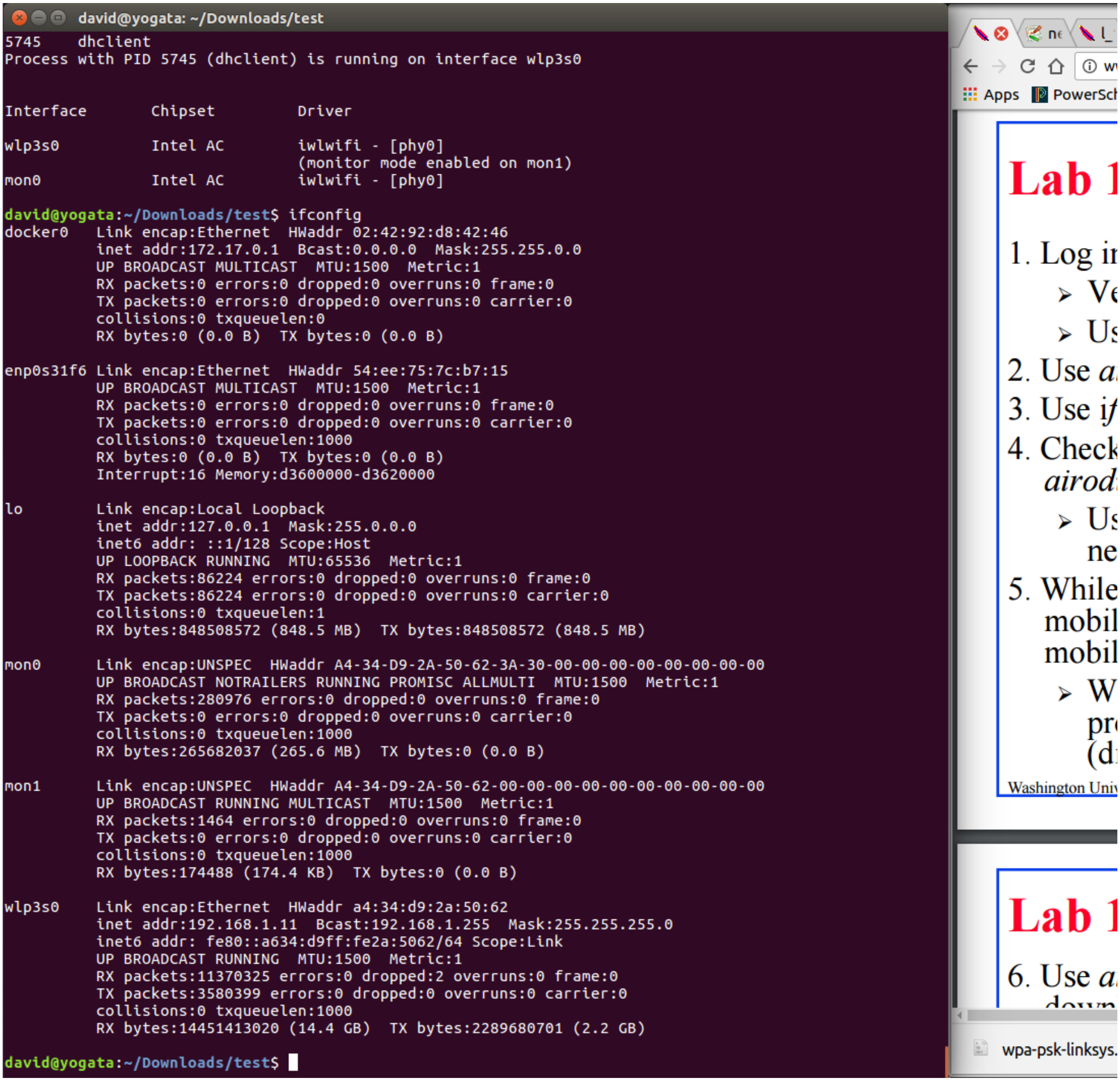
1. 

```
                                 Aircrack-ng 1.2 beta3


                   [00:00:00] 234 keys tested (445.74 k/s)


                          KEY FOUND! [ dictionary ]


      Master Key     : 5D F9 20 B5 48 1E D7 05 38 DD 5F D0 24 23 D7 E2
                       52 22 05 FE EE BB 97 4C AD 08 A5 2B 56 13 ED E2

      Transient Key  : 1B 7B 26 96 03 F0 6C 6C D4 03 AA F6 AC E2 81 FC
                       55 15 9A AF BB 3B 5A A8 69 05 13 73 5C 1C EC E0
                       A2 15 4A E0 99 6F A9 5B 21 1D A1 8E 85 FD 96 49
                       5F B4 97 85 67 33 87 B9 DA 97 97 AA C7 82 8F 52

      EAPOL HMAC     : 6D 45 F3 53 8E AD 8E CA 55 98 C2 60 EE FE 6F 51
david@yogata:~/Downloads/test$ ^C
david@yogata:~/Downloads/test$ airdecap-ng -p dictionary dump-05.cap
You must also specify the ESSID (-e).
"airdecap-ng --help" for help.
david@yogata:~/Downloads/test$ airdecap-ng -e linksys -p dictionary dump-05.cap
Total number of packets read          3523
Total number of WEP data packets         0
Total number of WPA data packets      3424
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets         0
david@yogata:~/Downloads/test$ airdecap-ng -e linksys -p dictionary wpa-psk-linksys.cap
Total number of packets read           587
Total number of WEP data packets         0
Total number of WPA data packets        57
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets        53
david@yogata:~/Downloads/test$ iwconfig
wlp3s0    IEEE 802.11abgn  ESSID:"Pretty_Fly_For_A_WiFi"
          Mode:Managed  Frequency:2.412 GHz  Access Point: A0:63:91:AB:F1:2C
          Bit Rate=300 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=68/70  Signal level=-42 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:1  Invalid misc:83   Missed beacon:0

lo        no wireless extensions.

enp0s31f6  no wireless extensions.

mon0      IEEE 802.11abgn  Mode:Monitor  Tx-Power=0 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

docker0   no wireless extensions.

david@yogata:~/Downloads/test$ 
```

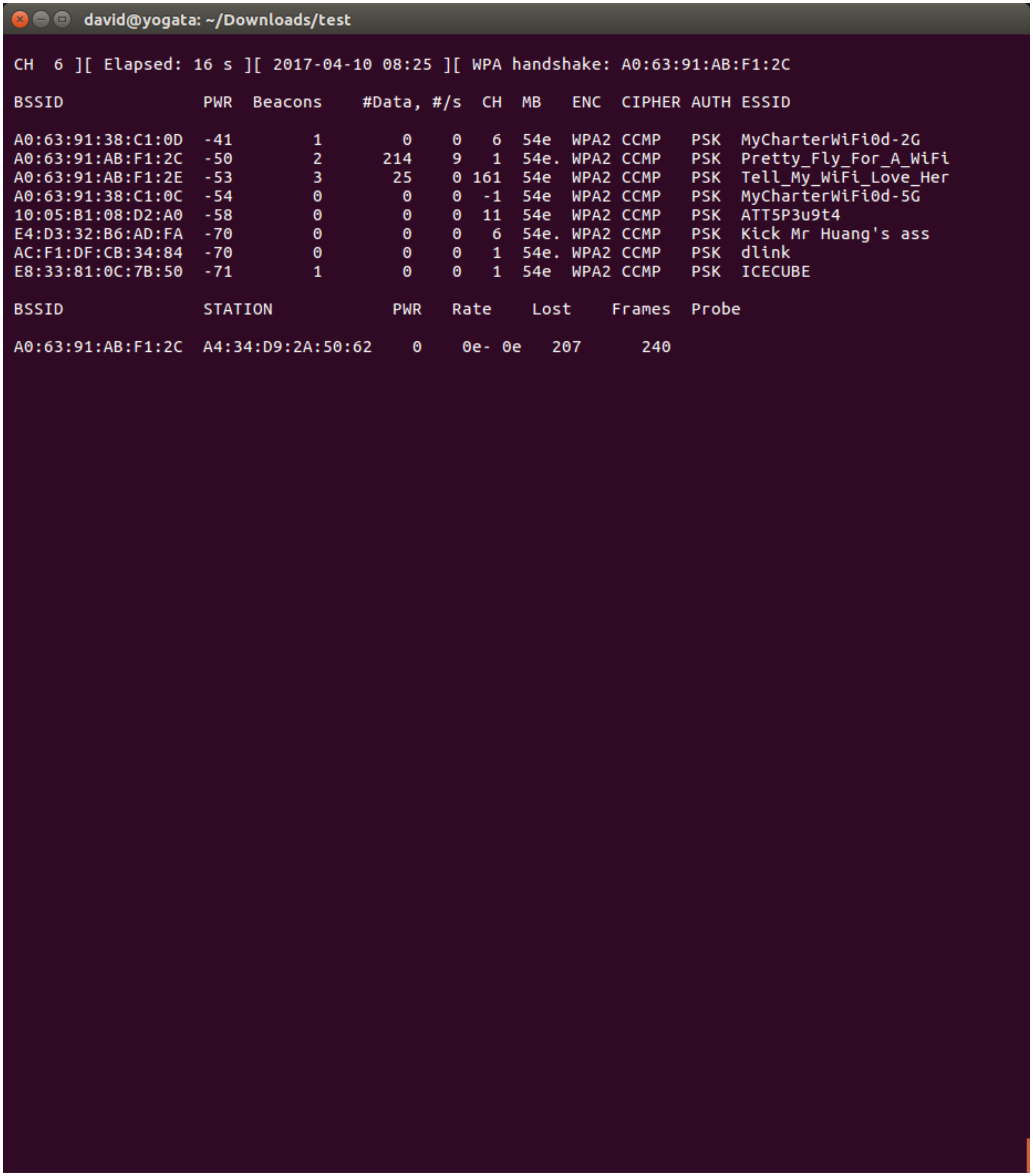
2. 

```
Number of decrypted WPA  packets         53
david@yogata:~/Downloads/test$ iwconfig
wlp3s0    IEEE 802.11abgn  ESSID:"Pretty_Fly_For_A_WiFi"
          Mode:Managed  Frequency:2.412 GHz  Access Point: A0:63:91:AB:F1:2C
          Bit Rate=300 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=68/70  Signal level=-42 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:1  Invalid misc:83   Missed beacon:0

lo        no wireless extensions.

enp0s31f6  no wireless extensions.

mon0      IEEE 802.11abgn  Mode:Monitor  Tx-Power=0 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

docker0   no wireless extensions.

david@yogata:~/Downloads/test$ history | grep airmon
 2012  airmon-ng
 2013  sudo airmon-ng
 2016* airmon-ng
 2017  sudo airmon-ng start wlp3s0
 2027  sudo airmon-ng start wlp3s0
 2058  sudo airmon-ng start wlp3s0
 2067  sudo airmon-ng stop mon2
 2069  sudo airmon-ng stop mon1
 2075  sudo airmon-ng stop mon0
 2076  sudo airmon-ng stop wlp3s0
 2080  sudo airmon-ng stop wlp3s0
 2081  sudo airmon-ng start wlp3s0
 2154  history | grep airmon
david@yogata:~/Downloads/test$ !2081
sudo airmon-ng start wlp3s0
[sudo] password for david:


Found 5 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 kill (some of) them!

PID     Name
799     avahi-daemon
824     avahi-daemon
846     NetworkManager
1182    wpa_supplicant
5745    dhclient
Process with PID 5745 (dhclient) is running on interface wlp3s0


Interface       Chipset         Driver

wlp3s0          Intel AC        iwlwifi - [phy0]
                                (monitor mode enabled on mon1)
mon0            Intel AC        iwlwifi - [phy0]

david@yogata:~/Downloads/test$ 
```

3.



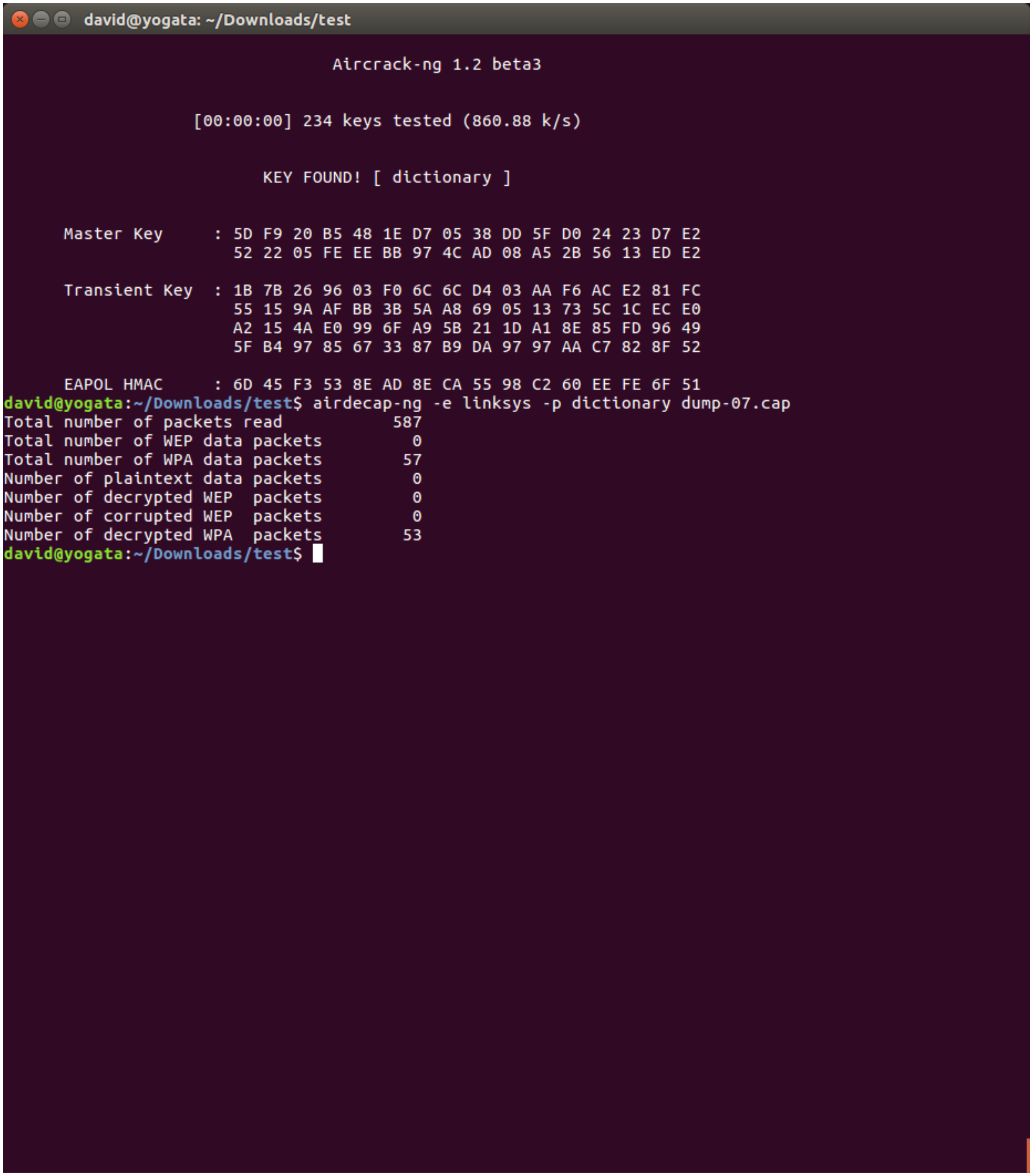
```
5745    dhclient
Process with PID 5745 (dhclient) is running on interface wlp3s0


Interface       Chipset         Driver

wlp3s0          Intel AC        iwlwifi - [phy0]
                                (monitor mode enabled on mon1)
mon0            Intel AC        iwlwifi - [phy0]

david@yogata:~/Downloads/test$ ifconfig
docker0   Link encap:Ethernet  HWaddr 02:42:92:d8:42:46
          inet addr:172.17.0.1  Bcast:0.0.0.0  Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

enp0s31f6 Link encap:Ethernet  HWaddr 54:ee:75:7c:b7:15
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:16 Memory:d3600000-d3620000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:86224 errors:0 dropped:0 overruns:0 frame:0
          TX packets:86224 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:848508572 (848.5 MB)  TX bytes:848508572 (848.5 MB)

mon0      Link encap:UNSPEC  HWaddr A4-34-D9-2A-50-62-3A-30-00-00-00-00-00-00-00-00
          UP BROADCAST NOTRAILERS RUNNING PROMISC ALLMULTI  MTU:1500  Metric:1
          RX packets:280976 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:265682037 (265.6 MB)  TX bytes:0 (0.0 B)

mon1      Link encap:UNSPEC  HWaddr A4-34-D9-2A-50-62-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1464 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:174488 (174.4 KB)  TX bytes:0 (0.0 B)

wlp3s0    Link encap:Ethernet  HWaddr a4:34:d9:2a:50:62
          inet addr:192.168.1.11  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a634:d9ff:fe2a:5062/64 Scope:Link
          UP BROADCAST RUNNING  MTU:1500  Metric:1
          RX packets:11370325 errors:0 dropped:2 overruns:0 frame:0
          TX packets:3580399 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14451413020 (14.4 GB)  TX bytes:2289680701 (2.2 GB)

david@yogata:~/Downloads/test$
```

4. 

```
CH  6 ][ Elapsed: 16 s ][ 2017-04-10 08:25 ][ WPA handshake: A0:63:91:AB:F1:2C

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

A0:63:91:38:C1:0D  -41        1        0    0   6  54e  WPA2 CCMP   PSK  MyCharterWiFi0d-2G
A0:63:91:AB:F1:2C  -50        2      214    9   1  54e. WPA2 CCMP   PSK  Pretty_Fly_For_A_WiFi
A0:63:91:AB:F1:2E  -53        3       25    0 161  54e  WPA2 CCMP   PSK  Tell_My_WiFi_Love_Her
A0:63:91:38:C1:0C  -54        0        0    0  -1  54e  WPA2 CCMP   PSK  MyCharterWiFi0d-5G
10:05:B1:08:D2:A0  -58        0        0    0  11  54e  WPA2 CCMP   PSK  ATT5P3u9t4
E4:D3:32:B6:AD:FA  -70        0        0    0   6  54e. WPA2 CCMP   PSK  Kick Mr Huang's ass
AC:F1:DF:CB:34:84  -70        0        0    0   1  54e. WPA2 CCMP   PSK  dlink
E8:33:81:0C:7B:50  -71        1        0    0   1  54e  WPA2 CCMP   PSK  ICECUBE

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

A0:63:91:AB:F1:2C  A4:34:D9:2A:50:62    0    0e- 0e   207      240
```

5. 5

6. 6

7. 

```
                                 Aircrack-ng 1.2 beta3


                   [00:00:00] 234 keys tested (860.88 k/s)


                          KEY FOUND! [ dictionary ]


      Master Key     : 5D F9 20 B5 48 1E D7 05 38 DD 5F D0 24 23 D7 E2
                       52 22 05 FE EE BB 97 4C AD 08 A5 2B 56 13 ED E2

      Transient Key  : 1B 7B 26 96 03 F0 6C 6C D4 03 AA F6 AC E2 81 FC
                       55 15 9A AF BB 3B 5A A8 69 05 13 73 5C 1C EC E0
                       A2 15 4A E0 99 6F A9 5B 21 1D A1 8E 85 FD 96 49
                       5F B4 97 85 67 33 87 B9 DA 97 97 AA C7 82 8F 52

      EAPOL HMAC     : 6D 45 F3 53 8E AD 8E CA 55 98 C2 60 EE FE 6F 51
david@yogata:~/Downloads/test$ airdecap-ng -e linksys -p dictionary dump-07.cap
Total number of packets read           587
Total number of WEP data packets         0
Total number of WPA data packets        57
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets        53
david@yogata:~/Downloads/test$ 
```