Love is in the Air

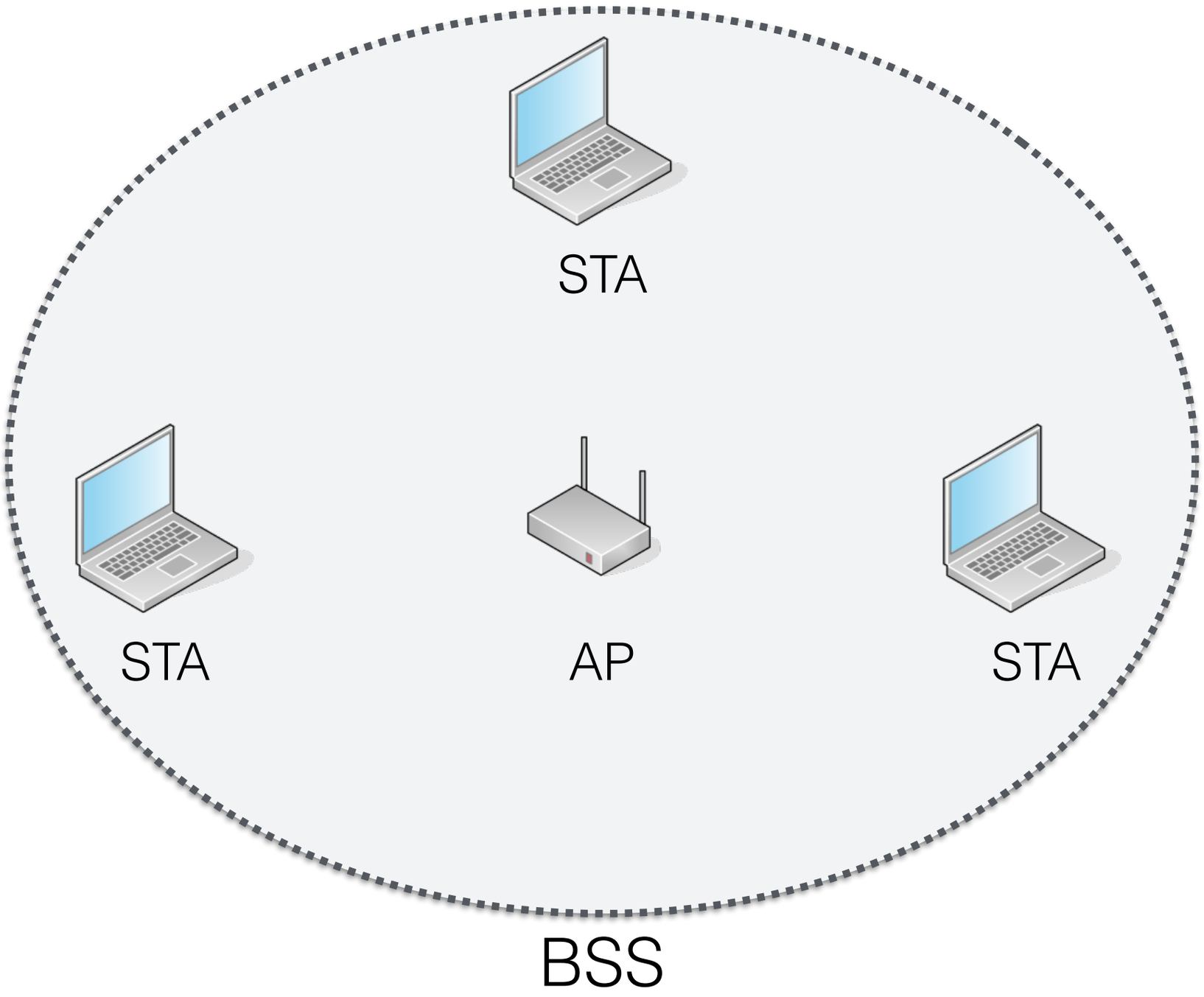
IEEE 802.11 Information Gathering

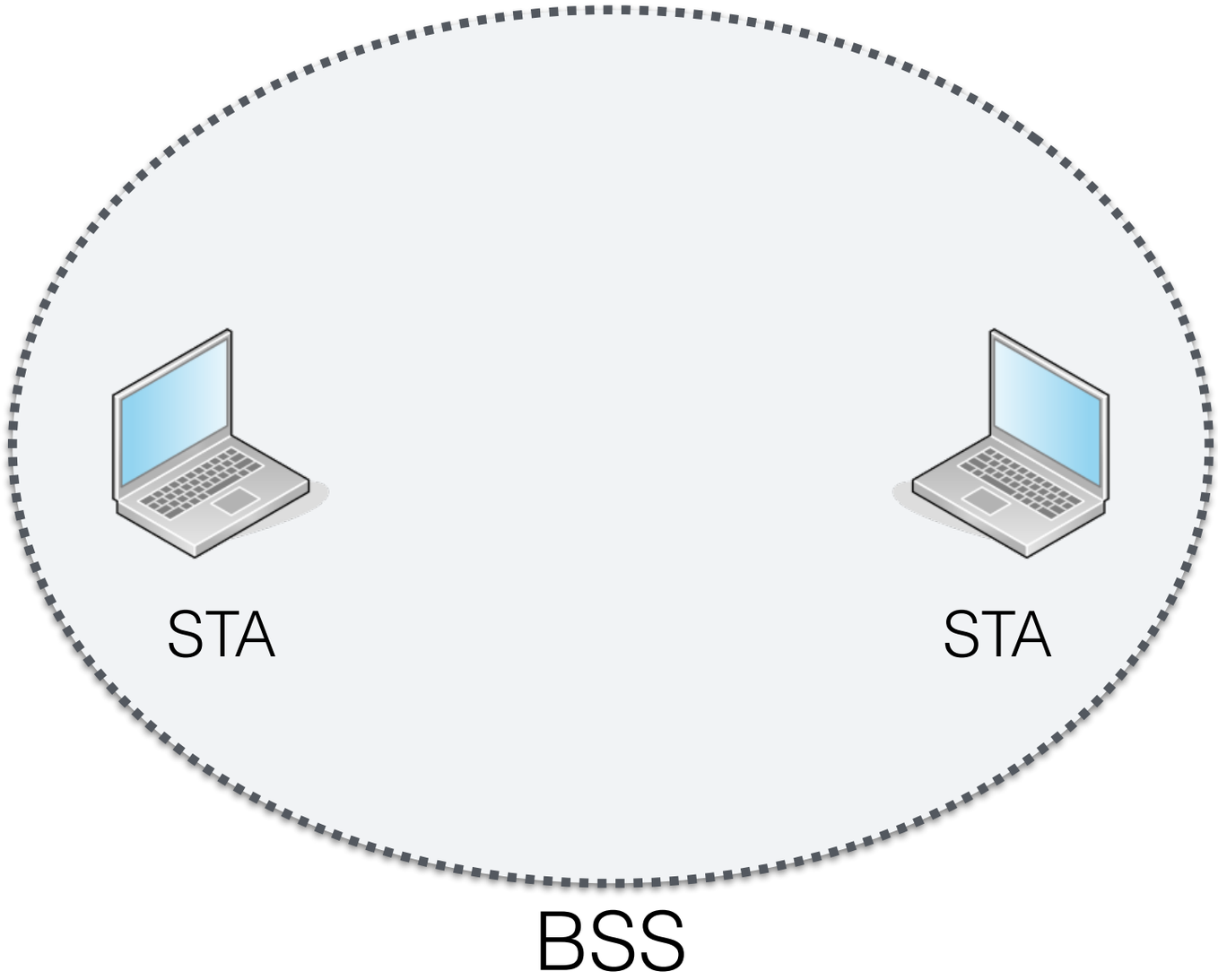
Andrés Blanco
6e726d@gmail.com
@6e726d

Whoami

Interests and expertise include network security, reverse engineering, and privacy. I enjoy playing with IEEE 802.11 security.

Infrastructure Mode





Ad Hoc Mode

IEEE 802.11 frames

Management

- Association Request
- Association Response
- Reassociation Request
- Reassociation Response
- Probe Request
- Probe Response
- Beacon
- ATIM
- Disassociation
- Authentication
- Deauthentication
- Action

Control

- Block ACK Request
- Block ACK
- PS-Poll
- RTS
- CTS
- ACK
- CF-End
- CF-End+CF-ACK

Data

- Data
- Data+CF-ACK
- Data+CF-Poll
- Data+CF-ACK+CF-Poll
- Null
- CF-ACK
- CF-Poll
- CF-ACK+CF-Poll
- QoS data
- QoS data+CF-ACK
- QoS data+CF-Poll
- QoS data+CF-ACK+CF-Poll
- QoS Null
- QoS+CF-Poll
- QoS+CF-ACK

Management frames

Management

- Association Request
- Association Response
- Reassociation Request
- Reassociation Response
- Probe Request
- Probe Response
- Beacon
- ATIM
- Disassociation
- Authentication
- Deauthentication
- Action

Control

- Block ACK Request
- Block ACK
- PS-Poll
- RTS
- CTS
- ACK
- CF-End
- CF-End+CF-ACK

Data

- Data
- Data+CF-ACK
- Data+CF-Poll
- Data+CF-ACK+CF-Poll
- Null
- CF-ACK
- CF-Poll
- CF-ACK+CF-Poll
- QoS data
- QoS data+CF-ACK
- QoS data+CF-Poll
- QoS data+CF-ACK+CF-Poll
- QoS Null
- QoS+CF-Poll
- QoS+CF-ACK

Beacon Frame

Probe Request Frame

Probe Response Frame

Action Frame

Authentication Frame

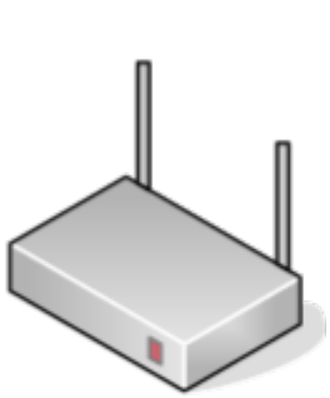
Association/Reassociation Frame

Type	Length	Value
1 byte	1 byte	1-255 byte

Information Elements

Scanning

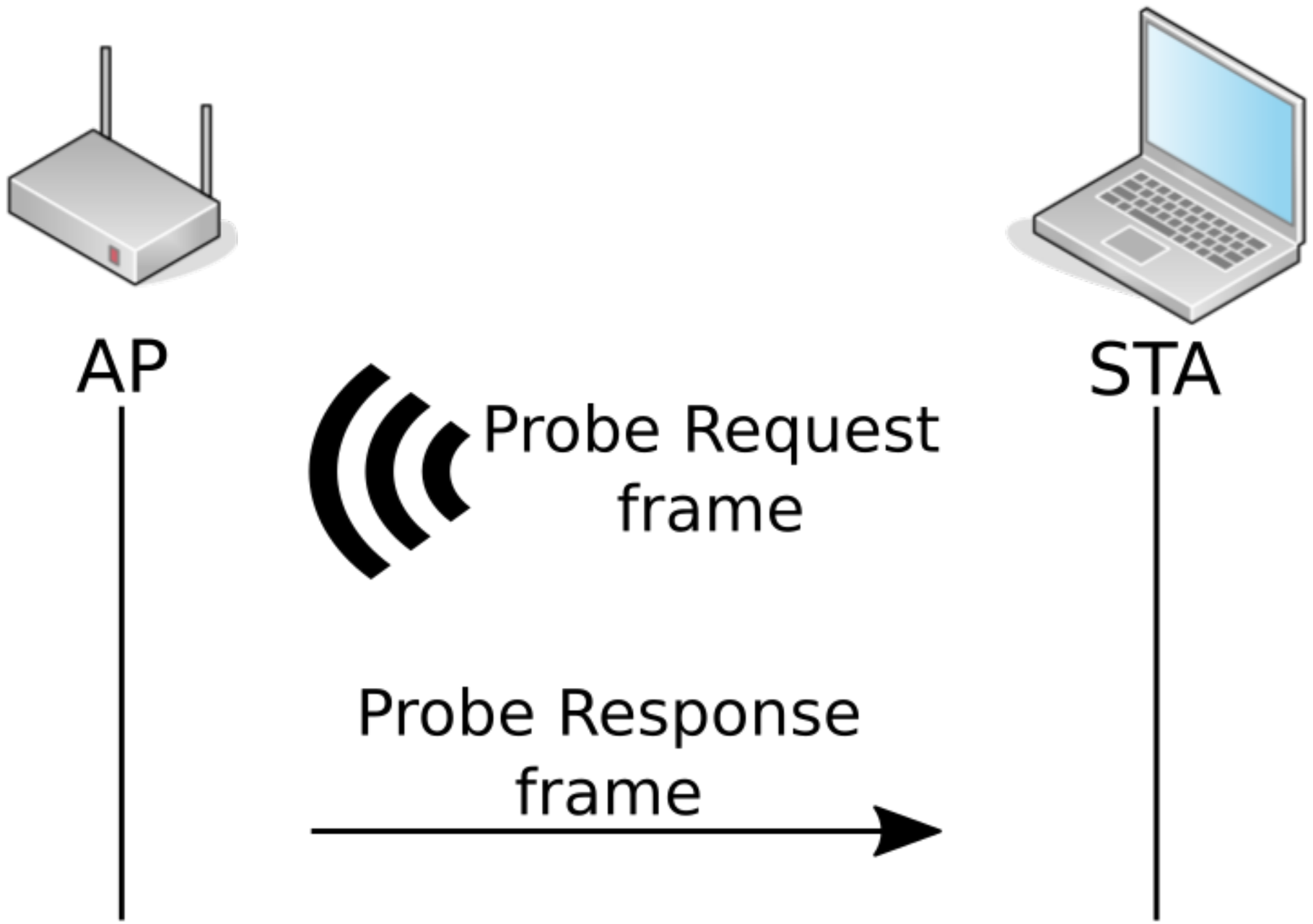
Passive



AP

Beacon frame

STA



Active

Authentication

Association

Reassociation

802.1X

WPS & WiFi-Direct

```
▸ Radiotap Header v0, Length 36
▸ 802.11 radio information
▸ IEEE 802.11 Probe Response, Flags: ....R...C
▾ IEEE 802.11 wireless LAN management frame
  ▸ Fixed parameters (12 bytes)
  ▾ Tagged parameters (319 bytes)
    ▸ Tag: SSID parameter set: (T_T)
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 10
    ▸ Tag: ERP Information
    ▸ Tag: ERP Information
    ▸ Tag: RSN Information
    ▸ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    ▸ Tag: QBSS Load Element 802.11e CCA Version
    ▸ Tag: HT Capabilities (802.11n D1.10)
    ▸ Tag: HT Information (802.11n D1.10)
    ▸ Tag: Overlapping BSS Scan Parameters: Undecoded
    ▸ Tag: Extended Capabilities (8 octets)
```

WPS Information Element

```
    ▾ Tag: Vendor Specific: Microsof: WPS
        Tag Number: Vendor Specific (221)
        Tag length: 134
        OUI: 00-50-f2
        Vendor Specific OUI Type: 4
        Type: WPS (0x04)
      ▸ Version: 0x10
      ▸ Wifi Protected Setup State: Configured (0x02)
      ▸ Ap Setup Locked: 0x01
      ▸ Response Type: AP (0x03)
      ▸ UUID E
      ▸ Manufacturer: NETGEAR, Inc.
      ▸ Model Name: R6300v2
      ▸ Model Number: R6300v2
      ▸ Serial Number: 679
      ▸ Primary Device Type
      ▸ Device Name: R6300v2
      ▸ Config Methods: 0x2008
```

```
▶ Fixed parameters (12 bytes)
▼ Tagged parameters (264 bytes)
   ▶ Tag: SSID parameter set: DIRECT-
   ▶ Tag: Supported Rates 6(B), 9(B), 12, 18, 24, 36, 48, 54, [Mbit/sec]
   ▶ Tag: DS Parameter set: Current Channel: 10
   ▼ Tag: Vendor Specific: Microsof: WPS
        Tag Number: Vendor Specific (221)
        Tag length: 163
        OUI: 00-50-f2
        Vendor Specific OUI Type: 4
        Type: WPS (0x04)
      ▶ Version: 0x10
      ▶ Wifi Protected Setup State: Not configured (0x01)
      ▶ Device Password ID: PIN (default) (0x0000)
      ▶ Response Type: Enrollee, Info only (0x00)
      ▶ UUID E
      ▶ Manufacturer: Western Digital Corporation
      ▶ Model Name: WD TV Live
      ▶ Model Number: WDBHG70000NBK
      ▶ Serial Number: WNC441203527
      ▶ Primary Device Type
      ▶ Device Name: WDTVLive
      ▶ Config Methods: 0x2388
      ▶ Vendor Extension
   ▼ Tag: Vendor Specific: Wi-FiAll: P2P
        Tag Number: Vendor Specific (221)
        Tag length: 41
        OUI: 50-6f-9a
        Vendor Specific OUI Type: 9
      ▶ P2P Capability: Device 0x23  Group 0x0
      ▶ P2P Device Info
   ▶ Tag: Vendor Specific: Wi-FiAll: Wi-Fi Display
```

WiFi-Direct

```
▶ Frame 1165: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface 0
▶ Radiotap Header v0, Length 36
▶ 802.11 radio information
▼ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▶ Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: fa:fa:fa:fa:fa:fa (fa:fa:fa:fa:fa:fa)
    Source address: fa:fa:fa:fa:fa:fa (fa:fa:fa:fa:fa:fa)
    BSS Id: fa:fa:fa:fa:fa:fa (fa:fa:fa:fa:fa:fa)
    .... .... .... 0000 = Fragment number: 0
    0111 0011 1100 .... = Sequence number: 1852
  ▶ Frame check sequence: 0xc201c58e [correct]
▼ IEEE 802.11 wireless LAN management frame
  ▶ Fixed parameters (12 bytes)
▼ Tagged parameters (43 bytes)
  ▶ Tag: SSID parameter set: fafafa
  ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
  ▶ Tag: DS Parameter set: Current Channel: 6
  ▼ Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 20
      RSN Version: 1
    ▶ Group Cipher Suite: 00-0f-ac AES (CCM)
      Pairwise Cipher Suite Count: 1
    ▶ Pairwise Cipher Suite List 00-0f-ac AES (CCM)
    ▶ Auth Key Management (AKM) Suite Count: 65535
    ▶ Auth Key Management (AKM) List 00-0f-ac PSK
    ▶ RSN Capabilities: 0x0000
```

Malformed Frames?

```
▶ Frame 600: 815 bytes on wire (6520 bits), 815 bytes captured (6520 bits)
▶ Radiotap Header v0, Length 36
▶ 802.11 radio information
▼ IEEE 802.11 Action, Flags: ........C
    Type/Subtype: Action (0x000d)
  ▶ Frame Control Field: 0xd000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: 9e:ae:17:fd:e4:3b (9e:ae:17:fd:e4:3b)
    Source address: 9e:ae:17:fd:e4:3b (9e:ae:17:fd:e4:3b)
    BSS Id: Apple_ff:94:73 (00:25:00:ff:94:73)
    .... .... .... 0000 = Fragment number: 0
    1100 1001 1001 .... = Sequence number: 3225
  ▶ Frame check sequence: 0xf3580425 [correct]
▶ IEEE 802.11 wireless LAN management frame
▶ [Malformed Packet: IEEE 802.11]
```

```
01c0  46 46 37 2c 30 78 45 08  6d 64 3d 30 2c 31 2c 32   FF7,0xE. md=0,1,2
01d0  0d 61 6d 3d 41 70 70 6c  65 54 56 33 2c 31 43 70   .am=Appl eTV3,1Cp
01e0  6b 3d 37 62 36 33 33 37  61 38 37 64 62 62 36 30   k=7b6337 a87dbb60
01f0  30 36 66 65 63 66 30 30  37 30 30 34 66 33 62 30   06fecf00 7004f3b0
0200  62 31 34 65 32 38 65 31  66 64 39 31 30 64 36 62   b14e28e1 fd910d6b
0210  63 33 33 39 64 39 31 34  39 30 39 34 65 63 62 61   c339d914 9094ecba
0220  65 64 06 73 66 3d 30 78  34 06 74 70 3d 55 44 50   ed.sf=0x 4.tp=UDP
0230  08 76 6e 3d 36 35 35 33  37 09 76 73 3d 32 32 30   .vn=6553 7.vs=220
0240  2e 36 38 04 76 76 3d 32  02 e0 00 0c 00 08 61 70   .68.vv=2 ......ap
0250  70 6c 65 20 74 76 c0 01  10 ce 00 00 00 1a 64 65   ple tv.. ......de
0260  76 69 63 65 69 64 3d 37  43 3a 44 31 3a 43 33 3a   viceid=7 C:D1:C3:
0270  32 36 3a 35 34 3a 44 31  17 66 65 61 74 75 72 65   [redacted] .feature
0280  73 3d 30 78 35 41 37 46  46 46 46 37 2c 30 78 45   s=0x5A7F FFF7,0xE
0290  09 66 6c 61 67 73 3d 30  78 34 10 6d 6f 64 65 6c   .flags=0 x4.model
02a0  3d 41 70 70 6c 65 54 56  33 2c 31 43 70 6b 3d 37   =AppleTV 3,1Cpk=7
02b0  62 36 33 33 37 61 38 37  64 62 62 36 30 30 36 66   b6337a87 dbb6006f
02c0  65 63 66 30 30 37 30 30  34 66 33 62 30 62 31 34   ecf00700 4f3b0b14
```

MAC randomization - AirPlay

```
802.11 radio information
IEEE 802.11 Action, Flags: ........C
    Type/Subtype: Action (0x000d)
  ▸ Frame Control Field: 0xd000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: 1a:ea:15:4d:c3:14 (1a:ea:15:4d:c3:14)
    Source address: 1a:ea:15:4d:c3:14 (1a:ea:15:4d:c3:14)
    BSS Id: Apple_ff:94:73 (00:25:00:ff:94:73)
    .... .... .... 0000 = Fragment number: 0
    1000 1101 0011 .... = Sequence number: 2259
  ▸ Frame check sequence: 0xf1eba79d [correct]
```

```
0000  00 00 24 00 2f 40 00 a0  20 08 00 00 00 00 00 00   ..$./@..  .......
0010  c6 e1 72 09 00 00 00 00  10 18 85 09 c0 00 0c 00   ..r..... ........
0020  00 00 0c 00 d0 00 00 00  ff ff ff ff ff ff 1a ea   ........ ........
0030  15 4d c3 14 00 25 00 ff  94 73 30 8d 7f 00 17 f2   .M...%.. .s0.....
0040  08 10 03 00 5f 42 4f 01  43 42 4f 01 04 49 00 06   ...._BO. CBO..I..
0050  36 00 95 00 10 00 b8 01  00 18 10 00 10 00 06 00   6....... ........
0060  03 03 03 03 1a ea 15 4d  c3 14 04 00 b8 00 00 00   .......M ........
0070  0f 01 00 03 ff ff 1d 97  1d 97 1d 97 1d 97 1d 97   ........ ........
0080  1d 97 2b 06 2b 06 1d 97  1d 97 1d 97 1d 97 1d 97   ..+.+... ........
0090  1d 97 2b 06 2b 06 00 00  05 25 00 01 00 00 00 00   ..+.+... .%......
00a0  1a ea 15 4d c3 14 06 01  00 00 06 01 00 00 00 00   ...M.... ........
00b0  6a b5 ee 92 bf a4 00 00  00 00 6f 51 00 00 00 00   j....... ..oQ....
00c0  12 29 00 0f 03 00 03 ff  ff 95 80 95 80 95 80 95   .)...... ........
00d0  80 95 80 95 80 06 51 06  51 95 80 95 80 95 80 95   ......Q. Q.......
00e0  80 95 80 95 80 06 51 06  51 00 00 00 0c 1b 00 27   ......Q. Q......'
00f0  0f 41 52 00 95 00 78 45  61 e0 6f 70 06 00 e8 b2   .AR...xE a.op....
0100  ac 08 b4 88 1a ea 15 4d  c3 14 06 0d 00 00 00 00   .......M ........
0110  65 00 04 00 0c 40 01 80  40 02 07 09 00 00 00 6f   e....@.. @......o
0120                                                     ........ ....M...
0130                                                     ....2... ........
0140                                                     .....Jea n-Charle
0150                                                     s-iPad.. ........
0160  03 00 c0 07 0c 0f 00 00  00 0c 33 34 35 39 65 36   ........ ..3459e6
0170  39 30 64 66 32 31 c0 00  02 30 00 10 00 0c 33 34   90df21.. .0....34
0180  35 39 65 36 39 30 64 66  32 31 c0 07 21 1a 00 00   59e690df 21..!...
0190  00 00 00 00 00 22 42 11  4a 65 61 6e 2d 43 68 61   ....."B. Jean-Cha
```

Wi-Fi Address E8:B2:AC:08:B4:88

MAC randomization - AirDrop

```
▶ Frame 244847: 417 bytes on wire (3336 bits), 417 bytes captured (3336 bits)
▶ IEEE 802.11 Beacon frame, Flags: ........
▼ IEEE 802.11 wireless LAN management frame
  ▶ Fixed parameters (12 bytes)
  ▼ Tagged parameters (381 bytes)
    ▶ Tag: SSID parameter set: DIRECT-24-HP DeskJet 3630 series
    ▶ Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 1
    ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▶ Tag: Power Constraint: 0
    ▶ Tag: TPC Report Transmit Power: 17, Link Margin: 0
    ▶ Tag: ERP Information
    ▶ Tag: ERP Information
    ▶ Tag: RSN Information
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: HT Information (802.11n D1.10)
    ▶ Tag: Vendor Specific: Broadcom
    ▶ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
    ▶ Tag: Vendor Specific: Broadcom
    ▶ Tag: Vendor Specific: Microsof: WPS
    ▼ Tag: Vendor Specific: HP
        Tag Number: Vendor Specific (221)
        Tag length: 98
        OUI: 08-00-09
        Vendor Specific OUI Type: 0
        Vendor Specific Data: 000400000017010201000314446573 6b4a65742033363330...
```

Information Elements or Information Leaks?

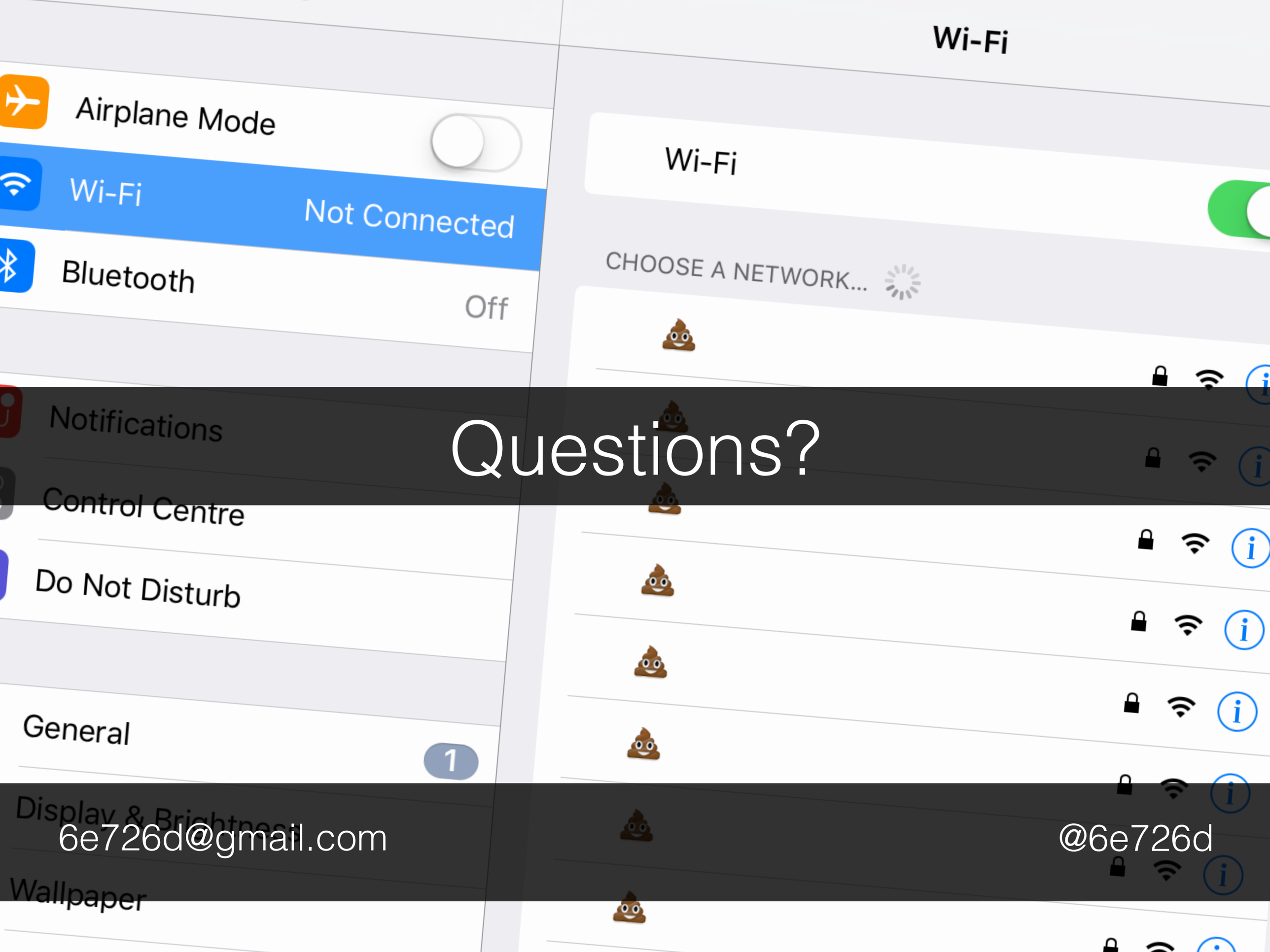
```
BSSID: FC:3F:DB:98:9D:42
0000  00 04 00 00 00 17 01 02 01 00 03 14 44 65 73 6b   ............Desk
0010  4a 65 74 20 33 36 33 30 20 73 65 72 69 65 73 00   Jet 3630 series.
0020  04 05 33 36 33 30 00 05 10 43 4e 36 33 37 33 4e   ..3630...CN6373N
0030  32 35 51 30 36 37 50 00 00 06 10 1c 85 2a 4d b8   25Q067P......*M.
0040  00 1f 08 ab cd fc 3f db 98 5f 24 07 04 c0 a8 00   ......?.._$.....
0050  99 08 02 00 c4 09 02 00 08 0a 04                  ...........

Status Bitfield: '\x00\x00\x00\x17' - 23
 - Station is on.
 - Station is configured.
 - Station is connected.
 - Station doesn't support 5GHz.
 - USB connected to host.
AWC version: 1.0
Model Name: DeskJet 3630 series
Product SKU: 3630
Serial Number: CN6373N25Q067P
UUID: 1C852A4DB8001F08ABCDFC3FDB985F24
IPv4 Address: 192.168.0.153
--------------------------------------------------------------------------------
```

Information Elements or Information Leaks?

```
▶ Frame 342226: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits)
▶ IEEE 802.11 Probe Response, Flags: ........
▼ IEEE 802.11 wireless LAN management frame
  ▶ Fixed parameters (12 bytes)
  ▼ Tagged parameters (408 bytes)
    ▶ Tag: SSID parameter set: DIRECT-R3Samsung Wireless Audio
    ▶ Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 11
    ▶ Tag: ERP Information
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: HT Information (802.11n D1.10)
    ▶ Tag: RSN Information
    ▶ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
    ▶ Tag: Vendor Specific: Microsof: WPS
    ▼ Tag: Vendor Specific: 00:2d:25
        Tag Number: Vendor Specific (221)
        Tag length: 56
        OUI: 00-2d-25 ()
        Vendor Specific OUI Type: 32
        Vendor Specific Data: 2000310010c0a80103244b0378f417264b0378f417c0ffd4...
  ▶ Tag: Vendor Specific: Wi-FiAll: P2P
```

Information Elements or Information Leaks?



Questions?

6e726d@gmail.com

@6e726d