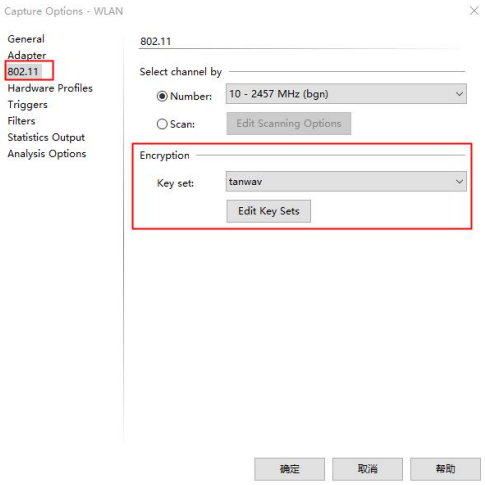
wifi 连接认证流程

如果路由器设置了密码，数据包数据会进行加密发送，所以在抓包前需要将路由器设置为开放或者在 Omnipeek 中设置路由器的密码，如果选择第二种，在 Omnipeek 工具栏中选择 Capure->Capture Options，在弹出的窗口中选择 802.11,如下图所示：



设置好密码后，需要 Omnipeek 成功抓取到对应的认证数据包后才能对数据包进行解密，否则抓取到的数据包中的数据还是会以密文显示。wifi 接入需要经过三个阶段：1）扫描阶段（SCAN）；2）认证阶段（Authentication）；3）关联（Association）。其中认证方式有 Open 和 Shared-key Authentication，Shared-key Authentication 一般采用 WEP 加密的方式，Open 一般采用 WPA/WPA2 加密方式。WEP 加密和 WPA 加密其一般流程如下：

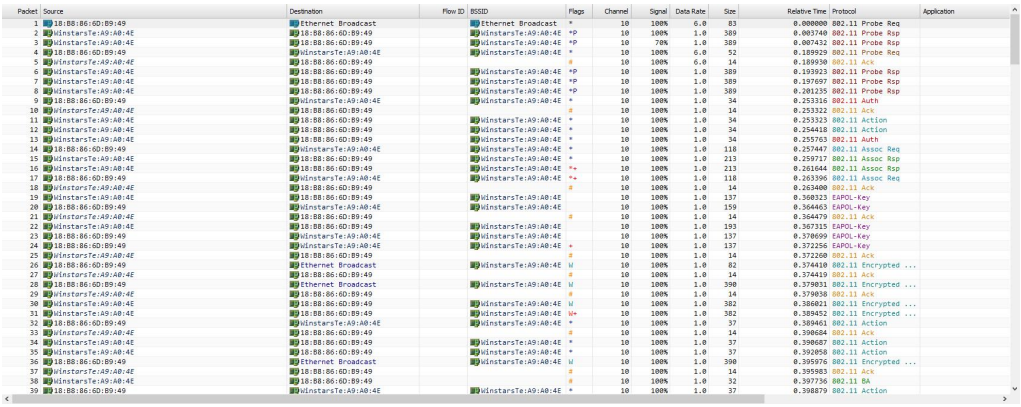
a)WEP 加密方式一般流程：

STA----(probe req)---->AP
AP ----(probe rsp)---->STA
STA----(auth)---->AP
AP ----(auth)---->STA
STA----(auth)---->AP
AP ----(auth)---->STA
STA----(assoc req)---->AP
AP ----(assoc rsp)---->STA

b)WPA 加密方式一般流程：

STA----(probe req)---->AP
AP ----(probe rsp)---->STA
STA----(auth)---->AP
AP ----(auth)---->STA
STA----(assoc req)---->AP
AP ----(assoc rsp)---->STA
AP ----(eapol)---->STA
STA ----(eapol)---->AP
AP ----(eapol)---->STA
STA ----(eapol)---->AP

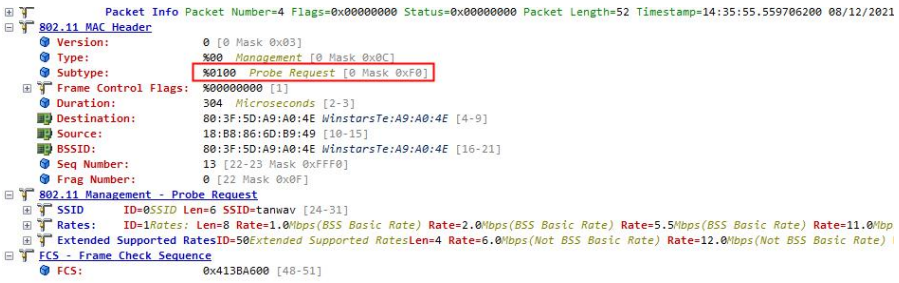
这里以 WPA 抓包为例，其 wifi 连接认证抓包如下所示。



1.扫描阶段（SCAN）

STA 发送 Probe Req，AP 回复 Probe Rsp 帧。抓包如下：

（1）sta 发出探测请求包 Probe Req



```
Packet Info Packet Number=4 Flags=0x00000000 Status=0x00000000 Packet Length=52 Timestamp=14:35:55.559706200 08/12/2021
802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %00  Management [0 Mask 0x0C]
    Subtype:                %0100  Probe Request [0 Mask 0xF0]
    Frame Control Flags:    %00000000 [1]
    Duration:               304  Microseconds [2-3]
    Destination:            80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [4-9]
    Source:                 18:B8:86:6D:B9:49 [10-15]
    BSSID:                  80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [16-21]
    Seq Number:             13 [22-23 Mask 0xFFF0]
    Frag Number:            0 [22 Mask 0x0F]
802.11 Management - Probe Request
    SSID       ID=0SSID Len=6 SSID=tanwav [24-31]
    Rates:     ID=1Rates: Len=8 Rate=1.0Mbps(BSS Basic Rate) Rate=2.0Mbps(BSS Basic Rate) Rate=5.5Mbps(BSS Basic Rate) Rate=11.0Mbp
    Extended Supported RatesID=50Extended Supported RatesLen=4 Rate=6.0Mbps(Not BSS Basic Rate) Rate=12.0Mbps(Not BSS Basic Rate)
FCS - Frame Check Sequence
    FCS:                    0x413BA600 [48-51]
```

（2）ap 发出探测响应包 Probe Rsp

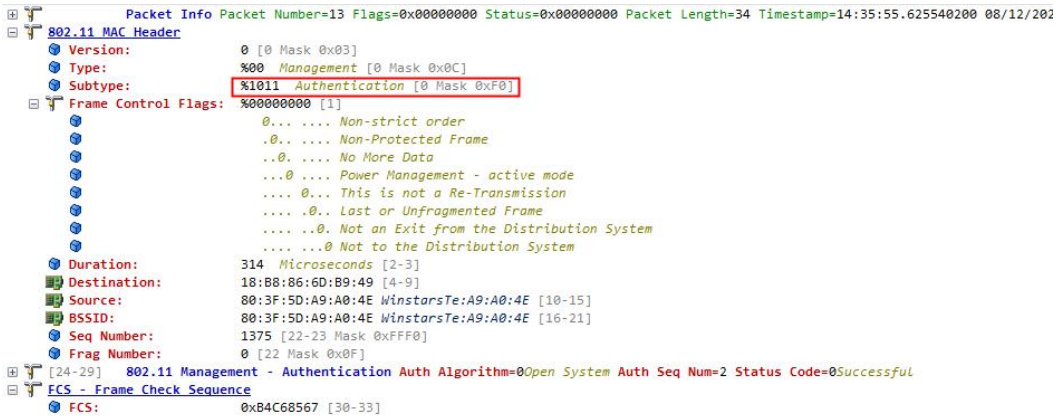
```
Packet Info Packet Number=6 Flags=0x00000000 Status=0x00000000 Packet Length=389 Timestamp=14:35:55.563700200 08/12/202
802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %00  Management [0 Mask 0x0C]
    Subtype:                %0101  Probe Response [0 Mask 0xF0]
    Frame Control Flags:    %00000000 [1]
        0... .... Non-strict order
        .0.. .... Non-Protected Frame
        ..0. .... No More Data
        ...0 .... Power Management - active mode
        .... 0... This is not a Re-Transmission
        .... .0.. Last or Unfragmented Frame
        .... ..0. Not an Exit from the Distribution System
        .... ...0 Not to the Distribution System
    Duration:               0  Microseconds [2-3]
    Destination:            18:B8:86:6D:B9:49 [4-9]
    Source:                 80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [10-15]
    BSSID:                  80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [16-21]
    Seq Number:             1369 [22-23 Mask 0xFFF0]
    Frag Number:            0 [22 Mask 0x0F]
[24-384]  Probe Rsp:  Probe Timestamp=883536223239 Beacon Interval=200 Capability Info=%0000010000010001 SSID[ID=0 Len=6 SSID=tar
FCS - Frame Check Sequence
    FCS:                    0x227DC2F0 [385-388]
```

2.认证阶段（Authentication）

（1）STA 发出链路认证请求包 Authentication Req

```
Packet Info Packet Number=9 Flags=0x00000000 Status=0x00000000 Packet Length=34 Timestamp=14:35:55.623093200 08/12/2021
802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %00  Management [0 Mask 0x0C]
    Subtype:                %1011  Authentication [0 Mask 0xF0]
    Frame Control Flags:    %00000000 [1]
        0... .... Non-strict order
        .0.. .... Non-Protected Frame
        ..0. .... No More Data
        ...0 .... Power Management - active mode
        .... 0... This is not a Re-Transmission
        .... .0.. Last or Unfragmented Frame
        .... ..0. Not an Exit from the Distribution System
        .... ...0 Not to the Distribution System
    Duration:               304  Microseconds [2-3]
    Destination:            80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [4-9]
    Source:                 18:B8:86:6D:B9:49 [10-15]
    BSSID:                  80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [16-21]
    Seq Number:             14 [22-23 Mask 0xFFF0]
    Frag Number:            0 [22 Mask 0x0F]
[24-29]   802.11 Management - Authentication Auth Algorithm=0 Auth Seq Num=1 Status Code=0
FCS - Frame Check Sequence
    FCS:                    0xBB7FCC73 [30-33]
```

（2）AP 发出链路认证响应包 Authentication Rsp



3.关联（Association）

（1）STA 发出关联请求包 Association Req

（2）AP 发出关联响应包 Association Rsp

4.EAPOL 阶段

（1）AP 发出 EAPOL-Key(ANonce, Unicast)

```
Packet Info Packet Number=19 Flags=0x00000000 Status=0x00000000 Packet Length=137 Timestamp=14:35:55.730100200 08/12/20
802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %10  Data [0 Mask 0x0C]
    Subtype:                %1000  QoS Data [0 Mask 0xF0]
    Frame Control Flags:    %00000010 [1]
                              0... .... Non-strict order
                              .0.. .... Non-Protected Frame
                              ..0. .... No More Data
                              ...0 .... Power Management - active mode
                              .... 0... This is not a Re-Transmission
                              .... .0.. Last or Unfragmented Frame
                              .... ..1. Exit from the Distribution System
                              .... ...0 Not to the Distribution System
    Duration:               314  Microseconds [2-3]
    Destination:            18:B8:86:6D:B9:49 [4-9]
    BSSID:                  80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [10-15]
    Source:                 80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [16-21]
    Seq Number:             0 [22-23 Mask 0xFFF0]
    Frag Number:            0 [22 Mask 0x0F]
    QoS Control Field:      %0000000000000000 [24-25]
                              -------- ........ AP PS Buffer State: 0
                              ........ 0....... A-MSDU: Not Present
                              ........ .00..... Ack: Normal Acknowledge
                              ........ ...0.... EOSP: Not End of Triggered Service Period
                              ........ ....0000 UP: 0 - Best Effort
802.2 Logical Link Control (LLC) Header
    Dest. SAP:              0xAA  SNAP [26]
    Source SAP:             0xAA  SNAP [27]
    Command:                0x03  Unnumbered Information [28]
    Vendor ID:              0x000000  XEROX CORPORATION [29-31]
    Protocol Type:          0x888E  IEEE Std 802.1X - Port-based network access control [32-33]
802.1x Authentication
    Protocol Version:       1 [34]
    Packet Type:            3  EAPOL - Key [35]
    Body Length:            95 [36-37]
    EAPOL - Key
        Type:               2  RSN key descriptor [38]
        Key Information:    %0000000010001010 [39-40]
                              xx...... ........ Reserved
                              ..0..... ........ SMK Handshake is not supported
                              ...0.... ........ Key Data Not Encrypted
                              ....0... ........ No Request to initiate Handshake
                              .....0.. ........ No Error
                              ......0. ........ Not Secure
                              .......0 ........ Message does NOT contain Key MIC
                              ........ 1....... Key ACK
                              ........ .0...... Install: 802.1X component shall not configure the temporal key
                              ........ ..xx.... Reserved
                              ........ ....1... Key Type: Pairwise Key
                              ........ .....010 Vers: HMAC-SHA1-128 is the EAPOL-Key MIC / NIST AES key wrap is the EAPOL-key enc
        Key Length:         16  CCMP [41-42]
        Replay Counter:     1 [43-50]
        Key Nonce:          0x50D8235D86EA1E27317A1484FC5ED7A0520B4A4EF29540394CD75A8904886CF7 [51-82]
        EAPOL-Key IV:       0x00000000000000000000000000000000 [83-98]
        Key RSC:            0x0000000000000000 [99-106]
        Key ID:             0x0000000000000000 [107-114]
        Key MIC:            0x00000000000000000000000000000000 [115-130]
        Key Data Len:       0 [131-132]
FCS - Frame Check Sequence
    FCS:                    0xCFDF4BB8 [133-136]
```

（2）STA 发出 EAPOL-Key(SNonce, Unicast, MIC)

```
Packet Info Packet Number=20 Flags=0x00000000 Status=0x00000000 Packet Length=159 Timestamp=14:35:55.734240200 08/12/20
802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %10  Data [0 Mask 0x0C]
    Subtype:                %1000  QoS Data [0 Mask 0xF0]
    Frame Control Flags:    %00000001 [1]
                              0... .... Non-strict order
                              .0.. .... Non-Protected Frame
                              ..0. .... No More Data
                              ...0 .... Power Management - active mode
                              .... 0... This is not a Re-Transmission
                              .... .0.. Last or Unfragmented Frame
                              .... ..0. Not an Exit from the Distribution System
                              .... ...1 To the Distribution System
    Duration:               202  Microseconds [2-3]
    BSSID:                  80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [4-9]
    Source:                 18:B8:86:6D:B9:49 [10-15]
    Destination:            80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [16-21]
    Seq Number:             0 [22-23 Mask 0xFFF0]
    Frag Number:            0 [22 Mask 0x0F]
    QoS Control Field:      %0000000000000000 [24-25]
                              -------- ........ AP PS Buffer State: 0
                              ........ 0....... A-MSDU: Not Present
                              ........ .00..... Ack: Normal Acknowledge
                              ........ ...0.... EOSP: Not End of Triggered Service Period
                              ........ ....0000 UP: 0 - Best Effort
802.2 Logical Link Control (LLC) Header
    Dest. SAP:              0xAA  SNAP [26]
    Source SAP:             0xAA  SNAP [27]
    Command:                0x03  Unnumbered Information [28]
    Vendor ID:              0x000000  XEROX CORPORATION [29-31]
    Protocol Type:          0x888E  IEEE Std 802.1X - Port-based network access control [32-33]
802.1x Authentication
    Protocol Version:       1 [34]
    Packet Type:            3  EAPOL - Key [35]
    Body Length:            117 [36-37]
    EAPOL - Key
        Type:               2  RSN key descriptor [38]
        Key Information:    %0000000100001010 [39-40]
                              xx...... ........ Reserved
                              ..0..... ........ SMK Handshake is not supported
                              ...0.... ........ Key Data Not Encrypted
                              ....0... ........ No Request to initiate Handshake
                              .....0.. ........ No Error
                              ......0. ........ Not Secure
                              .......1 ........ Message contains Key MIC
                              ........ 0....... No Key ACK
                              ........ .0...... Install: 802.1X component shall not configure the temporal key
                              ........ ..xx.... Reserved
                              ........ ....1... Key Type: Pairwise Key
                              ........ .....010 Vers: HMAC-SHA1-128 is the EAPOL-Key MIC / NIST AES key wrap is the EAPOL-key enc
        Key Length:         0 [41-42]
        Replay Counter:     1 [43-50]
        Key Nonce:          0x356AD4AB50A0F7590AA3468C18870E1C387057193ZD3A64C2FE965CA9428E7CE [51-82]
        EAPOL-Key IV:       0x00000000000000000000000000000000 [83-98]
        Key RSC:            0x0000000000000000 [99-106]
        Key ID:             0x0000000000000000 [107-114]
        Key MIC:            0x7F1676E75D2AC36CDAA2282A4EE37687 [115-130]
        Key Data Len:       22 [131-132]
        RSN:        ID=48RSN: Len=20 Version=1 Group Cipher OUI=00-0F-ACIEEE 802.11 Group Cipher Type=4CCMP - default in an RSN Pairw
FCS - Frame Check Sequence
    FCS:                    0x7A83AB29 [155-158]
```

（3）AP 发出 EAPOL-Key(Install PTK, Unicast, MIC, Encrypted GTK)

（4）STA 发出 EAPOL-Key(　Unicast,MIC)