过滤：协议+源mac

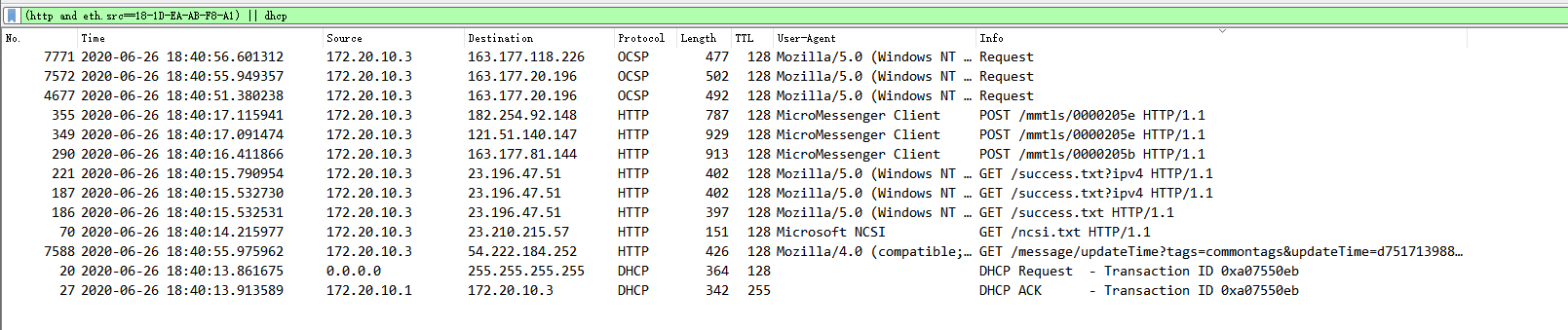
判断：

无线帧IEE802.1X数据建议在linux系统下抓取，windows抓取的基本都是在此基础上封包后的数据。

过滤条件：

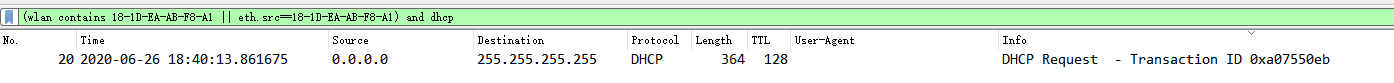
* (http and eth.src==18-1D-EA-AB-F8-A1) || dhcp

满足(http and eth.src==18-1D-EA-AB-F8-A1) 或者 dhcp 的数据包



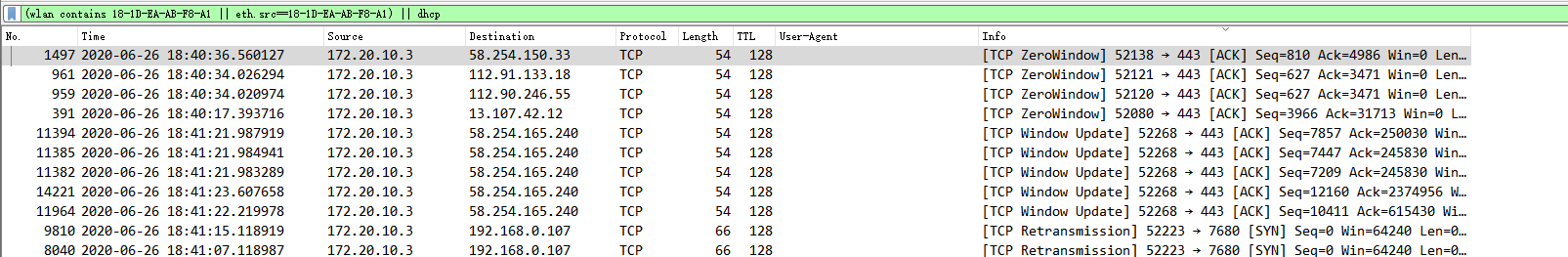
* (wlan contains 18-1D-EA-AB-F8-A1 || eth.src==18-1D-EA-AB-F8-A1) and dhcp

满足 (wlan contains 18-1D-EA-AB-F8-A1 || eth.src==18-1D-EA-AB-F8-A1) 和dhcp的数据包



* (wlan contains 18-1D-EA-AB-F8-A1 || eth.src==18-1D-EA-AB-F8-A1) || dhcp

满足(wlan contains 18-1D-EA-AB-F8-A1 || eth.src==18-1D-EA-AB-F8-A1) 或 dhcp的数据包

* 

## wireshark中无线帧的类型和过滤规则对照表

|  |  |
| --- | --- |
| 帧类型 | 过滤器语法 |
| Management frame | wlan.fc.type == 0 |
| Control frame | wlan.fc.type == 1 |
| Data frame | wlan.fc.type == 2 |
| Association request | wlan.fc.type\_subtype == 0x00 |
| Association response | wlan.fc.type\_subtype == 0x01 |
| Reassociation request | wlan.fc.type\_subtype == 0x02 |
| Reassociation response | wlan.fc.type\_subtype == 0x03 |
| Probe request | wlan.fc.type\_subtype == 0x04 |
| Probe response | wlan.fc.type\_subtype == 0x05 |
| Beacon | wlan.fc.type\_subtype == 0x08 |
| Disassociate | wlan.fc.type\_subtype == 0x0A |
| Authentication | wlan.fc.type\_subtype == 0x0B |
| Deauthentication | wlan.fc.type\_subtype == 0x0C |
| Action frame | wlan.fc.type\_subtype == 0x0D |
| Block ACK requests | wlan.fc.type\_subtype == 0x18 |
| Block ACK | wlan.fc.type\_subtype == 0x19 |
| Power save poll | wlan.fc.type\_subtype == 0x1A |
| Request to send | wlan.fc.type\_subtype == 0x1B |
| Clear to send | wlan.fc.type\_subtype == 0x1C |
| ACK | wlan.fc.type\_subtype == 0x1D |
| Contention free period end | wlan.fc.type\_subtype == 0x1E |
| NULL data | wlan.fc.type\_subtype == 0x24 |
| QoS data | wlan.fc.type\_subtype == 0x28 |
| Null QoS data | wlan.fc.type\_subtype == 0x2C |