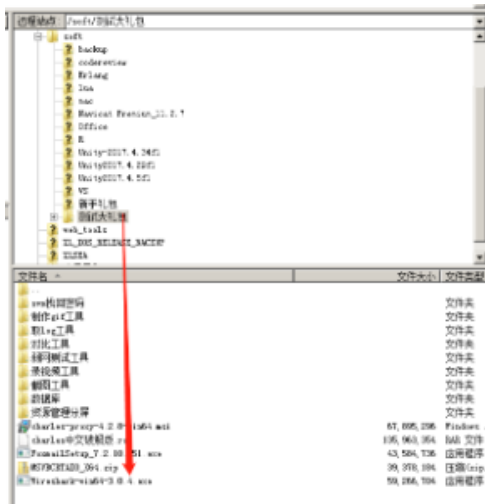


## 网络截包工具的安装使用简介 ( WireShark )

## 1, 安装

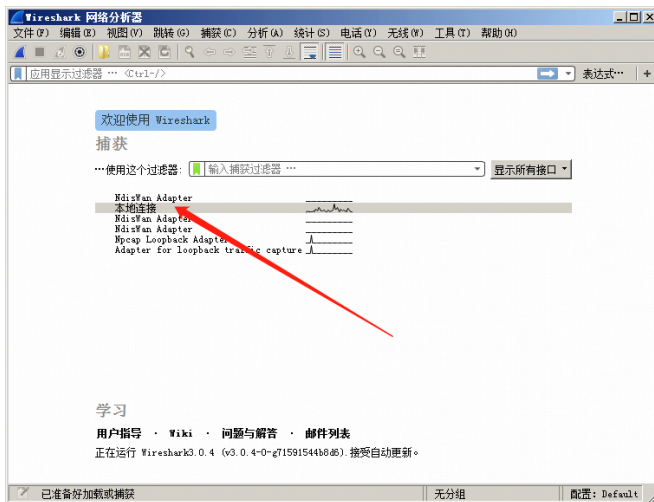
推荐使用FTP上的3.0.4版本，以下是3.04版本在FTP的目录位置：



整个安装流程可以按照默认的选项：Next->Agree->Next->Next->Next->Install->Next->Finish 顺序执行就可以完成了。

## 2, 抓包

启动后，在首页选择 双击 本地连接，就可以开始抓包了，如下图：



•本地连接

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(T) 无线(W) 工具(I) 帮助(O)

应用显示过滤器 ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
16063	265.110999	192.168.40.96	216.58.200.46	TCP	66	[TCP Retransmission] 60399 → 443 [SYN] Seq=0 Win=8192 Len=0
16172	265.721014	192.168.40.96	121.51.19.142	TCP	55	[TCP Keep-Alive] 60392 → 443 [ACK] Seq=2505 Ack=5200 Win=0 Len=0
16173	265.731295	121.51.19.142	192.168.40.96	TCP	66	[TCP Keep-Alive ACK] 443 → 60392 [ACK] Seq=5200 Ack=2505 Win=0 Len=0
16174	265.759962	192.168.40.96	121.51.19.142	TCP	55	[TCP Keep-Alive] 60391 → 443 [ACK] Seq=1532 Ack=4950 Win=0 Len=0
16175	265.779923	121.51.19.142	192.168.40.96	TCP	66	[TCP Keep-Alive ACK] 443 → 60391 [ACK] Seq=4950 Ack=1532 Win=0 Len=0
16202	266.730966	192.168.40.96	121.51.19.142	TCP	55	[TCP Keep-Alive] 60392 → 443 [ACK] Seq=2505 Ack=5200 Win=0 Len=0
16203	266.740190	121.51.19.142	192.168.40.96	TCP	66	[TCP Keep-Alive ACK] 443 → 60392 [ACK] Seq=5200 Ack=2505 Win=0 Len=0
16204	266.779948	192.168.40.96	121.51.19.142	TCP	55	[TCP Keep-Alive] 60391 → 443 [ACK] Seq=1532 Ack=4950 Win=0 Len=0
16205	266.790550	121.51.19.142	192.168.40.96	TCP	66	[TCP Keep-Alive ACK] 443 → 60391 [ACK] Seq=4950 Ack=1532 Win=0 Len=0
16230	267.375967	192.168.20.182	192.168.40.96	TCP	60	80 → 60300 [ACK] Seq=34970 Ack=59179 Win=147968 Len=0
16232	267.580902	192.168.40.96	192.168.20.182	TCP	54	60300 → 80 [ACK] Seq=59179 Ack=35317 Win=64256 Len=0
16235	267.740881	192.168.40.96	121.51.19.142	TCP	55	[TCP Keep-Alive] 60392 → 443 [ACK] Seq=2505 Ack=5200 Win=0 Len=0
16236	267.750846	121.51.19.142	192.168.40.96	TCP	66	[TCP Keep-Alive ACK] 443 → 60392 [ACK] Seq=5200 Ack=2505 Win=0 Len=0
16237	267.790881	192.168.40.96	121.51.19.142	TCP	55	[TCP Keep-Alive] 60391 → 443 [ACK] Seq=1532 Ack=4950 Win=0 Len=0
16238	267.800305	121.51.19.142	192.168.40.96	TCP	66	[TCP Keep-Alive ACK] 443 → 60391 [ACK] Seq=4950 Ack=1532 Win=0 Len=0
16244	268.110863	192.168.40.96	192.168.20.182	TCP	54	60300 → 80 [ACK] Seq=60094 Ack=35866 Win=65536 Len=0

Frame 16230: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
Ethernet II, Src: NewH3CTe\_77:d8:39 (88:df:9e:77:d8:39), Dst: AsustekC\_3d:66:9b (88:d7:f6:3d:66:9b)  
Internet Protocol Version 4, Src: 192.168.20.182, Dst: 192.168.40.96  
Transmission Control Protocol, Src Port: 80, Dst Port: 60300, Seq: 34970, Ack: 59179, Len: 0

3, 退出

抓包后，如果不想继续捕获了，可以通过CTRL+E停止捕获，再通过CTRL+W返回首页，如下图：

正在捕获 本地连接

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(T) 无线(W) 工具(I) 帮助(O)

应用显示过滤器 ... <Ctrl-/>

开始(S) Ctrl+K  
停止(T) Ctrl+E  
重新开始(R) Ctrl+R  
捕获过滤器(F) ...  
刷新接口列表 F5

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.40.96	255.255.250	Broadcast	4	
2	0.088048	Hand	255.255.250	Broadcast	4	
3	0.200405	200	255.255.250	Broadcast	4	
4	0.365170	192.168.40.96	211.139.178.49	TCP	60	
5	0.408843	fe80::415:37af:3bba...	ff02::1:2	IPv6	40	
6	0.481974	192.168.40.112	239.255.255.250	Broadcast	4	
7	0.615966	Cisco-Li_15:4c:a2	Broadcast	4		
8	0.688823	NewH3CTe_77:d8:52	Spanning-tree-(for	802.1Q	4	
9	0.730992	AsustekC_3d:66:9b	NewH3CTe_77:d8:39	ARP	42	
10	0.732019	NewH3CTe_77:d8:39	AsustekC_3d:66:9b	ARP	42	
11	0.847945	AsustekC_08:31:82	Broadcast	4		
12	0.917389	fe80::9814:488d:e0c...	ff02::1:2	IPv6	40	

•本地连接

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(T) 无线(W) 工具(I) 帮助(O)

打开(O) Ctrl+O  
打开最近(R)  
合并(M) ...  
从Hex 转码导入(I) ...  
关闭(C) Ctrl+W  
保存(S) Ctrl+S  
另存为(A) ... Ctrl+Shift+S  
文件集合  
导出特定分组...  
导出分组解析结果  
导出分组字节流(B) ... Ctrl+Shift+X  
导出 PDU 到文件...  
导出 TLS 会话密钥...  
导出对象  
打印(P) ... Ctrl+P  
退出(Q) Ctrl+Q

0000 01 00 5e 7f ff fa 2c fd a1 6e 3d 39 08 00 45  
0010 00 ca 0c 1a 00 00 01 11 d3 f1 c0 a8 28 75 e1

4, 参考

网络抓包工具wireshark入门教程详

Wireshark基本介绍和学习TCP三次握手