wireshark抓包实验 分析 详解

转载

淘豆豆么 于 2011-10-11 20:21:26 发布 8816 收藏 3
分类专栏： Tool 常用debug 文章标签： dst internet networking url class 网络

Tool 同时被 2 个专栏收录
31 篇文章 0 订阅
订阅专栏

常用debug
14 篇文章 0 订阅
订阅专栏

Wireshark(Formerly Ethereal) is an award-winning network protocol analyzer developed by an international team of networking experts.

WireShark是一款很好的抓包工具，我们今天用它来做几个实验，复习一下网络基础知识。

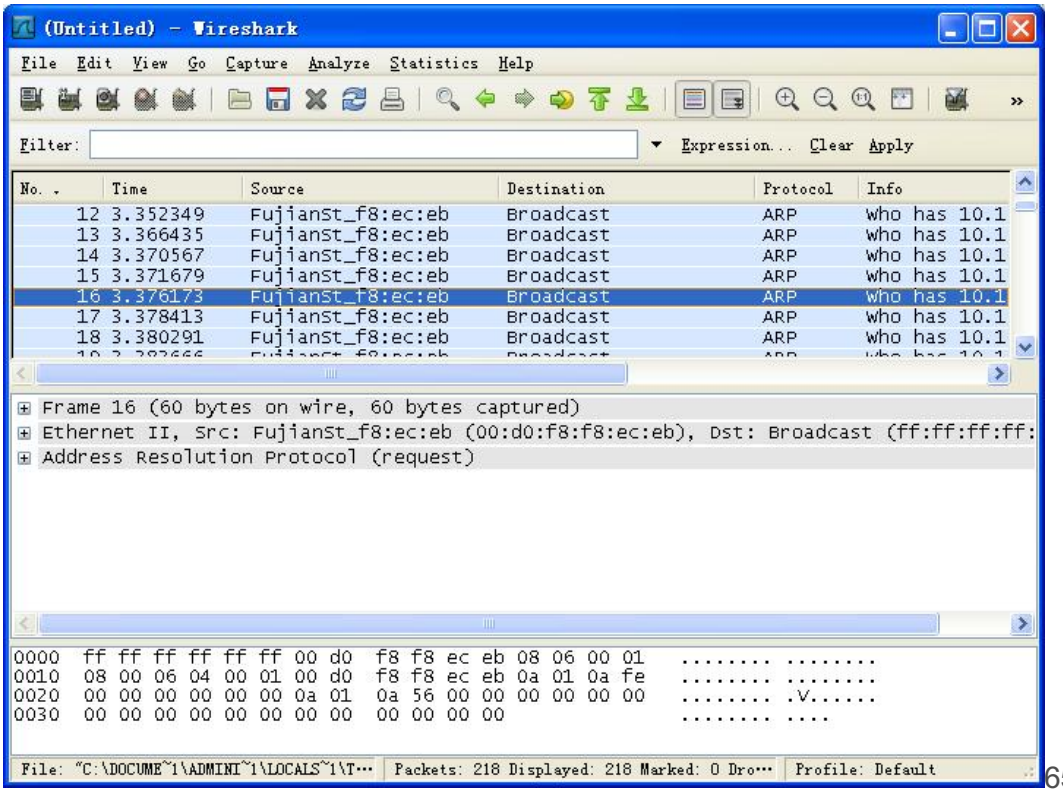
1、安装WireShark。这个不用说了，中间会提示安装WinPcap,一切都是默认。

2、实验前把网络断一下（关掉联网的软件），防止产生一些不必要的流量，不利于分析。

3、ok。打开WireShark,选择"Capture>>Interfaces",选择自己的网卡（物理网卡，如果装了，VM或是VPN软件，会产生很多虚拟网卡，但软件不使用时，流量是零）。选择"Start"开始监控流量。

4.HTTP协议分析。迅速打开一个网页，因为我是在局域网环境下，ARP广播较多。然后选择"Stop The running live capture"停止抓包。 截图一。

点击图片查看大图！



650) this.width=650;"<

抓包过程中发现UDP组播、ARP广播等。

A.组播分析.

Ethernet II帧,

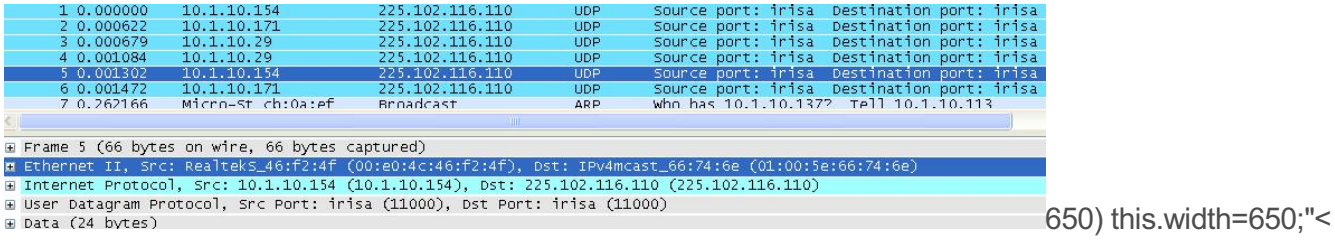
Src: RealtekS_46:f2:4f (00:e0:4c:46:f2:4f), Dst:IPv4mcast_66:74:6e (01:00:5e:66:74:6e)。

源地址RealtekS，目的地址IPv4mcast 66:74:6e。

Internet Protocol(IP数据包),

Src: 10.1.10.154 (10.1.10.154), Dst: 225.102.116.110(225.102.116.110)这个不用说吧。

User Datagram Protocol(UDP数据包), Src Port: irisa (11000), Dst Port: irisa (11000)。



650) this.width=650;"<

B.ARP广播。

Ethernet II帧,

Src: FujianSt_f8:ec:eb (00:d0:f8:f8:ec:eb)[锐捷网络的交换机，这里显示"福建实达网 络"], Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)(ARP数据包)

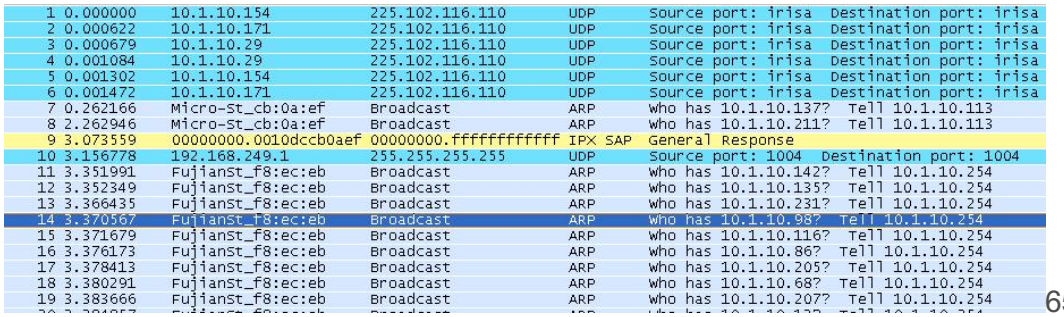
Sender MAC address: FujianSt_f8:ec:eb (00:d0:f8:f8:ec:eb)

Sender IP address: 10.1.10.254 (10.1.10.254)

Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

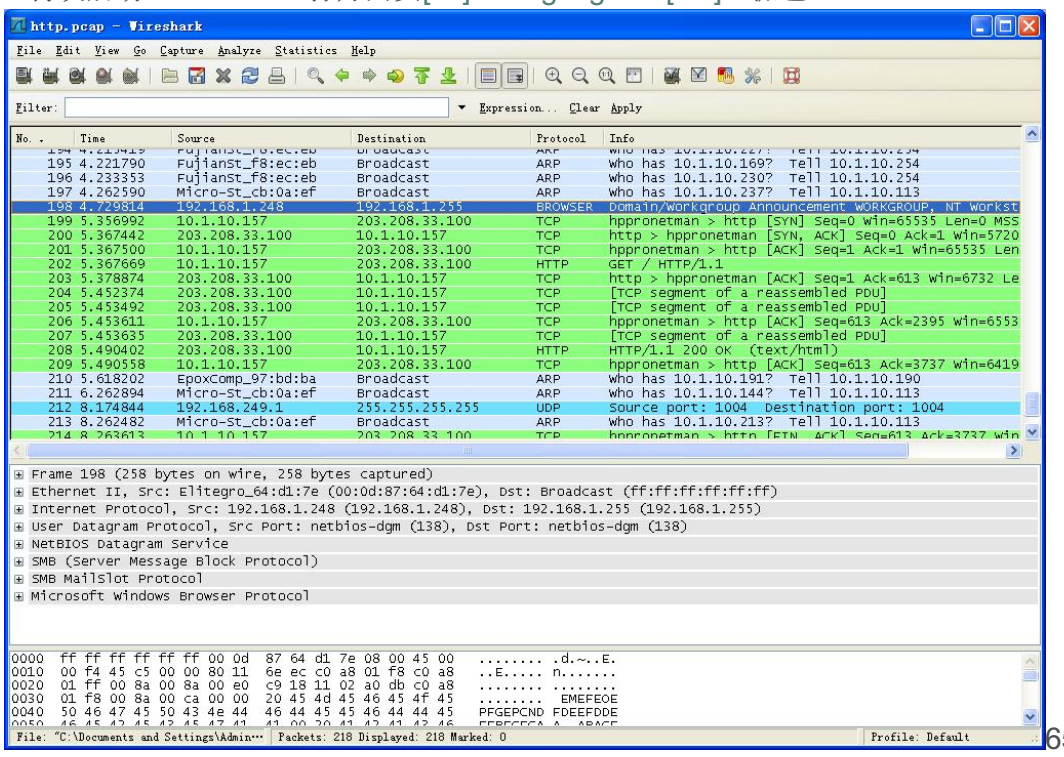
Target IP address: 10.1.10.135 (10.1.10.135)

ARP是一个三层的协议，直接跑在Frame之上



650) this.width=650;"<

5.再次启动WireShark，打开网页[url]www.google.cn[/url]，抓包。



650) this.width=650;"<

C.HTTP数据包分析。

Ethernet II Frame,

Src: Elitegro_59:a7:88 (00:16:ec:59:a7:88)【VIA的网卡，这里显示Elitegro】,

Dst: FujianSt_f8:ec:eb (00:d0:f8:f8:ec:eb)

Internet Protocol,

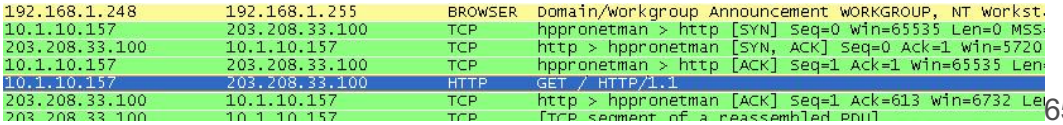
Src: 10.1.10.157 (10.1.10.157), Dst: 203.208.33.100 (203.208.33.100)

【Google.cn的IP地址】

Transmission Control Protocol,

Src Port: hppronetman (3908), Dst Port: http (80), Seq: 0, Len: 0

从抓的包中可以看到TCP的连接建立过程(Three-way Handshake).[syn][syn,ack][ack]

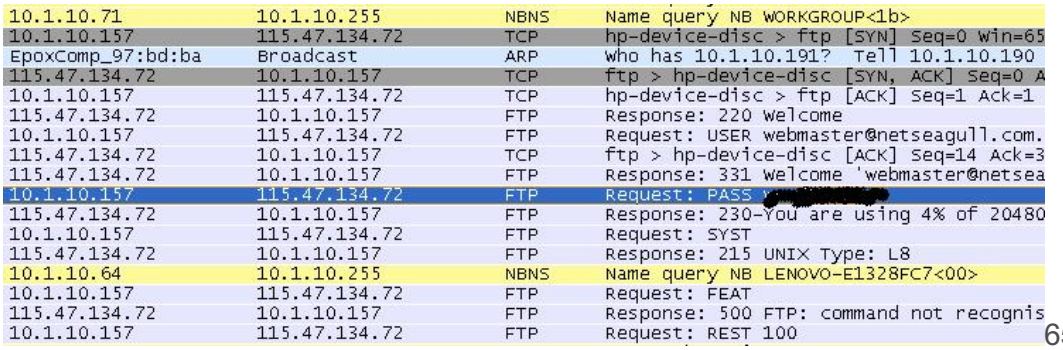


650) this.width=650;"<

6.再次启动WireShark，启动FlashFXP连接远程服务器，抓包。

D.FTP数据包分析

先建立TCP的链接，然后传送密码，命令。不多说了。密码以明文方式传送（涂黑的部分）。



650) this.width=650;"<

7.再次启动WireShark，打开cmd,ping [url]www.g.cn[/url]，抓包。

E.PING [url]www.g.cn[/url] 【DNS和ICMP】

DNS服务走的53端口UDP

Internet Protocol,

Src: 192.168.175.5 (192.168.175.5)【这是我们内部的DNS】,

Dst: 10.1.10.157 (10.1.10.157)

User Datagram Protocol,

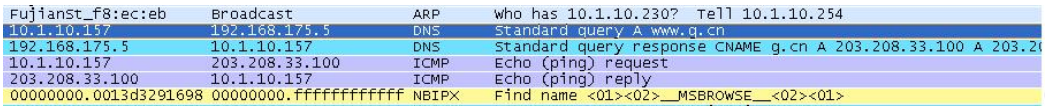
Src Port: domain (53), Dst Port: 59161 (59161)

[url]www.g.cnDNS[/url]查询的返回值[url]www.g.cn[/url]: type CNAME, class IN, cname g.cn

g.cn: type A, class IN, addr 203.208.33.100

g.cn: type A, class IN, addr 203.208.33.101

而ICMP走的是IP协议。



650) this.width=650;"<

总结：我们一共抓了组播、ARP、HTTP、FTP、DNS、ICMP，通过实验复习下网络的基础知识。WireShark的功能很强大，需要仔细研究。要继续努力呀！

转自：海鸥博客